Junos® OS 12.1X44-D20 Release Notes

Release 12.1X44-D20
08 August 2013
Revision 2

These release notes accompany Release 12.1X44-D20 of the Junos® OS. They describe device documentation and known problems with the software. Junos OS runs on all Juniper® Networks SRX Series Services Gateways and J Series Services Routers.

For the latest, most complete information about outstanding and resolved issues with the Junos OS software, see the Juniper Networks online software defect search application at http://www.juniper.net/prsearch.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, which is located at https://www.juniper.net/techpubs/software/junos/.

Contents

Junos OS Release Notes for Branch SRX Series Services Gateways and J Series Services Routers

Powered by Junos OS, Juniper Networks SRX Series Services Gateways provide robust networking and security services. SRX Series Services Gateways range from lower-end branch devices designed to secure small distributed enterprise locations to high-end devices designed to secure enterprise infrastructure, data centers, and server farms. The branch SRX Series Services Gateways include the SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, and SRX650 devices.

Juniper Networks J Series Services Routers running Junos OS provide stable, reliable, and efficient IP routing, WAN and LAN connectivity, and management services for small to medium-sized enterprise networks. These routers also provide network security features, including a stateful firewall with access control policies and screens to protect against attacks and intrusions, and IPsec VPNs. The J Series Services Routers include the J2320, J2350, J4350, and J6350 devices.

- New Features in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 6
- Changes in Default Behavior and Syntax in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 25
- Known Limitations in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 34
- Outstanding Issues in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 62
- Resolved Issues in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 65
- Errata and Changes in Documentation for Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 80
- Upgrade and Downgrade Instructions for Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 90

New Features in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers

The following features have been added to Junos OS Release 12.1X44. Following the description is the title of the topics and pathway pages to consult for more information on the feature.

- Release 12.1X44-D20 Software Features on page 7
- Release 12.1X44-D15 Hardware Features on page 8
- Release 12.1X44-D15 Software Features on page 9
- Release 12.1X44-D10 Hardware Features on page 9
- Release 12.1X44-D10 Software Features on page 11

Release 12.1X44-D20 Software Features

Application Layer Gateways (ALG)

- **Transparent mode support for ALGs**—This feature is supported on all branch SRX Series devices.

  Beginning with Junos OS Release 12.1X44-D20, Avaya H.323, G-H323, IKE, MGCP, MSRPC, PPTP, RSH, SUN RPC, SCCP, SIP, SQL, and TALK ALGs support layer 2 transparent mode. Transparent mode on SRX Series devices provides standard Layer 2 switching capabilities and full security services.

  In transparent mode, the SRX Series device filters packets that traverse the device without modifying any of the source or destination information in the packet MAC headers. Transparent mode is useful for protecting servers that mainly receive traffic from untrusted sources because there is no need to reconfigure the IP settings of routers or protected servers.

  NOTE: **Transparent mode is supported on all data and VOIP ALGs.**

  A device operates in Layer 2 transparent mode when all physical interfaces on the device are configured as Layer 2 interfaces. There is no command to define or enable transparent mode on the device. The device operates in transparent mode when there are interfaces defined as Layer 2 interfaces. The device operates in route mode (the default mode) if there are no physical interfaces configured as Layer 2 interfaces.

  - [*Layer 2 Bridging and Transparent Mode Overview*]
  - [*Layer 2 Bridging and Switching for Security Devices*]

- [*Layer 2 Bridging and Transparent Mode for Security Devices*]
- [*Transparent Mode*]

IPsec VPN

- **AutoVPN RIP support for unicast traffic**—AutoVPN hubs are supported on SRX240, SRX550, and SRX650 devices. AutoVPN spokes are supported on SRX100, SRX210, SRX220, SRX240, SRX550, and SRX650 devices.

  Junos OS Release 12.1X44-D20 adds support for configuring the RIP dynamic routing protocol with AutoVPN for unicast traffic. In addition to RIP, OSPF and BGP are supported with AutoVPN for unicast traffic.

  For AutoVPN configuration examples with RIP, go to the Juniper Networks Knowledge Base (KB): http://kb.juniper.net/ and search for KB27720.

  [*AutoVPNs for Security Devices*]

Release 12.1X44-D15 Hardware Features

Hardware Features - SRX100 Services Gateway

This release introduces the following model of the SRX100 Services Gateway with increased memory. The features for the new model are the same as that of the existing models. For information on the specification changes, refer to the relevant product datasheet.

Model	Description
SRX100H2	SRX100 Services Gateway with 8 Fast Ethernet ports, 2 GB DRAM, and 2 GB NAND Flash memory

Hardware Features - SRX110 Services Gateway

This release introduces the following models of the SRX110 Services Gateway with increased memory. The features for the new model are the same as that of the existing models. For information on the specification changes, refer to the relevant product datasheet.

Model	Description
SRX110H2-VA	SRX110 Services Gateway with 8 Fast Ethernet ports, 2 GB DRAM, 2 GB CompactFlash memory, and 1 VDSL/ADSL-POTS port
SRX110H2-VB	SRX110 Services Gateway with 8 Fast Ethernet ports, 2 GB DRAM, 2 GB CompactFlash memory, and 1 VDSL/ADSL-ISDN port

Hardware Features – SRX210 Services Gateway

This release introduces the following models of the SRX210 Services Gateway with increased memory. The features for the new model are the same as that of the existing models. For information on the specification changes, refer to the relevant product datasheet.

Model	Description
SRX210HE2	SRX210 Services Gateway with 1 Mini-PIM slot, 2 GB DRAM, and 2 GB NAND Flash memory
SRX210HE2-POE	SRX210 Services Gateway with 1 Mini-PIM slot, 2 GB DRAM, 2 GB NAND Flash memory, and 4 Power over Ethernet (PoE) ports

Hardware Features – SRX220 Services Gateway

This release introduces the following models of the SRX220 Services Gateway with increased memory. The features for the new model are the same as that of the existing models. For information on the specification changes, refer to the relevant product datasheet.

Model	Description
SRX220H2	SRX220 Services Gateway with 2 Mini-PIM slots, 2 GB DRAM, and 2 GB CompactFlash memory
SRX220H2-POE	SRX220 Services Gateway with 2 Mini-PIM slots, 2 GB DRAM, 2 GB CompactFlash memory, and 8 PoE ports

Release 12.1X44-D15 Software Features

Hardware

- **2G Memory Upgrade**— This feature is supported on SRX100, SRX110, SRX210, and SRX220 devices. See Hardware Features section for more details.

Release 12.1X44-D10 Hardware Features

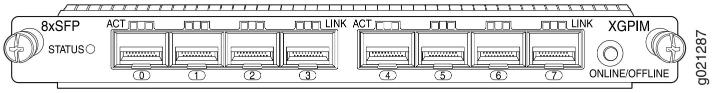
This topic includes the following sections:

- 8-Port Gigabit Ethernet SFP XPIM on page 9

8-Port Gigabit Ethernet SFP XPIM

The ports of the 8-Port Gigabit Ethernet small form-factor pluggable (SFP) XPIM can be used for connecting to Ethernet WAN service as well as for local server connectivity at Gigabit Ethernet speeds. The XPIM enables Layer 2 line-rate Gigabit switching and system-processor dependent Layer 3 service with connection of up to eight SFP Gigabit Ethernet ports. The 8-Port Gigabit Ethernet SFP XPIM complements the on-board 10/100/1000 Mbps Ethernet interfaces with extended WAN connectivity. It supports a variety of transceivers. This XPIM can be used in copper and optical environments to provide maximum flexibility when upgrading from an existing infrastructure to Metro Ethernet. Figure 1 on page 10 shows the front panel of 8-port Gigabit Ethernet XPIM.

Figure 1: 8-Port Gigabit Ethernet SFP XPIM Front Panel



Hardware Specifications

Table 1 on page 10 gives the physical specifications of the 8-Port Gigabit Ethernet small form-factor pluggable (SFP) XPIM.

Table 1: 8-Port Gigabit Ethernet SFP XPIM Physical Specifications

Description	Value
Dimensions (H x W x L)	0.78 in. x 6.72 in. x 8.1 in. (1.98 cm x 17.1 cm x 20.57 cm)
Weight	17.6 oz (0.499 kg)
Connector type	SFP
Form factor	XPIM
Environmental operating temperature	32°F through 113°F (0°C through 45°C)
Relative humidity	5% to 90% noncondensing
Altitude	Up to 10,000 ft (3000 m)

Network Interface Specifications

Table 2 on page 10 gives the network interface specifications of the 8-Port Gigabit Ethernet small form-factor pluggable (SFP) XPIM.

Table 2: 8-Port Gigabit Ethernet SFP XPIM Network Interface Specifications

Network Interface Specification	Value
Operating modes	Full-duplex and half-duplex
Operating speed	10/100/1000 Mbps
VLAN support	802.1Q virtual LANs
Class-of-service support	Supported
Encapsulations	DIX, LLC/SNAP, CCC, TCC, and VLAN-CCC
Loopback diagnostic feature	Supported
Autonegotiation	Supported

Release 12.1X44-D10 Software Features

Application Layer Gateways (ALG)

- **Real-Time Streaming Protocol (RTSP) interleave mode—** This feature is supported on all branch SRX Series and J Series devices.

  This feature is an enhancement to the current RTSP ALG. In most use cases the network carries UDP media streams based on an RTSP TCP connection, but there has been an increase in demand for the use of interleaving mode in which both media and control share the same TCP connection. The key reason to use interleaving is the ability to traverse firewalls. Because of the lower security restrictions around TCP port 80 to support Web traffic, RTSP makes use of interleaving mode for including media in the same connection to traverse firewalls.

  [*Understanding ALG Types*]

AppSecure

- **AppFW rule set features expanded**—This feature is supported on all branch SRX Series devices.

  NOTE: On the SRX100, SRX110, and SRX210 platforms, this feature is only supported on the High Memory versions.

  AppFW is enhanced to broaden the rule set options for defining an application-aware firewall, you can now:

  - Choose to close a TCP connection when matching traffic is rejected.
  - Define explicit, coexisting permit rules and deny rules in a single rule set.
  - Display session logs to view new session create, deny, and close messages that describe the AppFW actions that have been taken.
  - Display AppFW rules that are shadowed by others in the same rule set so that you can remove redundancy and avoid errors.

  [*Application Firewall*]

- **Application identification at Layer 3 and Layer 4**—This feature is supported on all branch SRX Series devices.

  NOTE: This feature is supported on only the High Memory versions of SRX100, SRX110, and SRX210 devices.

  New **services application-identification** configuration options allow the ICMP type or code, the IP protocol, and the source or destination addresses that are available at Layer 3 or Layer 4 to be mapped to an application. When implementing AppSecure services, such as AppFW, AppTrack, or AppQoS, you can apply Layer 3 or Layer 4 mapping techniques when applicable to bypass Layer 7 signature-based mapping and improve the efficiency of the network. The mapping techniques work as follows:

- Address mapping associates traffic to or from particular addresses with a known application.
- ICMP mapping associates the type or code of ICMP messages with a known application.
- IP protocol mapping applies to IP traffic only and associates a particular IP protocol with a known application.

[*Application Identification for Security Devices*]

Chassis Cluster

- **Logical interface scaling**—On SRX Series devices, chassis cluster failover performance has been optimized to scale with more logical interfaces.

  During redundancy group failover, Generic Attribute Registration Protocol (GARP) is sent on each logical interface to steer the traffic to the appropriate node. GARP was sent by the Juniper Services Redundancy Protocol (jsrpd) process running in the Routing Engine in the previous release of Junos OS.

  With logical interface scaling, the Routing Engine becomes the checkpoint and GARP is directly sent from the Services Processing Unit (SPU).

  [*Understanding Chassis Cluster Redundancy Group Failover*]

DNS

- **DNS enhancements**—This feature is supported on all branch SRX Series and J Series devices.

  Junos OS Domain Name System (DNS) support allows you to use domain names as well as IP addresses to identify locations.

  DNS enhancements include:

  - **DNS proxy**—The device proxies hostname resolution requests on behalf of the clients behind the J Series or SRX Series device.
  - **DNS proxy with split DNS**— You can configure your proxy server to split the DNS query based on both the interface and the domain name. You can also configure a set of name servers and associate them with a given domain name.
  - **Dynamic DNS (DDNS) client**—Servers protected by the device remain accessible despite dynamic IP address changes.

  [*DNS Proxy Overview*]

  [*Configuring the Device as a DNS Proxy*]

[*Junos OS CLI Reference*]

Ethernet OAM Connectivity Fault Management

- **Ethernet OAM connectivity fault management**—This feature is supported on SRX210, SRX220, SRX240, SRX550, and SRX650 devices.

  Ethernet interfaces on branch SRX Series devices support the IEEE 802.1ag standard for Operation, Administration, and Management (OAM). The 802.1ag is an IEEE standard for connectivity fault management (CFM). The IEEE 802.1ag provides a specification for Ethernet CFM. The Ethernet network can consist of one or more service instances. A service instance could be a VLAN or a concatenation of VLANs. The goal of CFM is to provide a mechanism to monitor, locate, and isolate faulty links.

  CFM support includes the following features:

  - Fault monitoring using the Continuity Check Protocol. This is a neighbor discovery and health check protocol that discovers and maintains adjacencies at the VLAN or link level.
  - Path discovery and fault verification using the Linktrace protocol.
  - Fault isolation using the Loopback protocol.

    The Loopback protocol is used to check access to maintenance association end points (MEPs) under the same maintenance association (MA). The Loopback messages are triggered by an administrator using the **ping ethernet** command.

  [*Understanding Ethernet OAM Connectivity Fault Management*]

  [*Junos OS CLI Reference*]

Ethernet OAM Link Fault Management

- **802.3ah OAM link fault management**—This feature is supported on SRX100, SRX210, SRX220, SRX240, SRX550, and SRX650 devices.

  The Ethernet interfaces on these SRX Series devices support the IEEE 802.3ah standard for Operation, Administration, and Maintenance (OAM). The standard defines OAM link fault management (LFM). You can configure IEEE 802.3ah OAM LFM on point-to-point Ethernet links that are connected either directly or through Ethernet repeaters. The IEEE 802.3ah standard meets the requirement for OAM capabilities as Ethernet moves from being solely an enterprise technology to a WAN and access technology, and the standard remains backward-compatible with existing Ethernet technology.

  The following OAM LFM features are supported:

  - Discovery and link monitoring
  - Remote fault detection
  - Remote loopback

[*Understanding Ethernet OAM Link Fault Management for SRX Series Services Gateways*]

Interfaces and Routing

- **8-Port Gigabit Ethernet SFP XPIM**—The 8-Port Gigabit Ethernet small form-factor pluggable (SFP) XPIM is supported on SRX550 and SRX650 Services Gateways.

  An XPIM is a network interface card (NIC) that installs in the front slots of the SRX550 or SRX650 Services Gateway to provide physical connections to a LAN or a WAN.

  Small form-factor pluggables (SFPs) are hot-pluggable modular interface transceivers for Gigabit Ethernet and Fast Ethernet connections. The 8-port SFP Gigabit Ethernet interface enables customers to connect to Ethernet WAN services as well as to local servers at gigabit speed.

  Supported Features

  The following features are supported on the 8-Port Gigabit Ethernet SFP XPIM:

  - Pluggable on standard SFP Gigabit Ethernet ports
  - Operates in tri-rate (10/100/1000 Mbps) mode with copper SFPs
  - Routing and switched mode operation
  - Layer 2 protocols
    - LACP
    - LLDP
    - GVRP
    - IGMP snooping (v1 and v2)
    - STP, RSTP, and MSTP
    - 802.1x
  - Encapsulation (supported at the Physical Layer)
    - ethernet-bridge
    - ethernet-ccc
    - ethernet-tcc
    - ethernet-vpls
    - extended-vlan-ccc
    - extended-vlan-tcc
    - flexible-ethernet-services
    - vlan-ccc
  - Q in Q VLAN tagging
  - Integrated routing and bridging (IRB)
  - Jumbo frames (9192-byte size)

- Chassis cluster switching
- Chassis cluster fabric link using Gigabit Ethernet ports

NOTE:
The following Layer 2 switching features are not supported when the 8-Port Gigabit Ethernet SFP XPIM is plugged in slots with speed less than 1 Gigabit:

- Q in Q VLAN tagging
- Link aggregation using ports across multiple XPIMs

Interface Names and Settings

The following format is used to represent the 8-Port Gigabit Ethernet SFP XPIM:

type-fpc/pic/port

Where:

- type—Media type (ge)
- fpc—Number of the Flexible PIC Concentrator (FPC) card where the physical interface resides
- pic—Number of the PIC where the physical interface resides (0)
- port—Specific port on a PIC (0)

Examples: **ge-1/0/0** and **ge-2/0/0**

By default, the interfaces on the ports on the uplink module installed on the device are enabled. You can also specify the MTU size for the XPIM. Junos OS supports values from 256 through 9192. The default MTU size for the 8-Port Gigabit Ethernet SFP XPIM is 1514.

[*Understanding the 8-Port Gigabit Ethernet SFP XPIM*]

- **8-Port serial GPIM**—The 8-Port synchronous serial GPIM is supported on SRX550 and SRX650 devices. This GPIM provides 8 ports that operate in synchronous mode and supports a line rate of 64 Mbps or 8 Mbps per port.

  The 8-Port synchronous serial GPIM supports the following features:

  - Operation modes (autoselect based on cable, no configuration required)
    - DTE (data terminal equipment)
    - DCE (data communication equipment)
  - Clocking
  - Clock rates (baud rates) from 1.2 KHz to 8.0 MHz

  NOTE: RS-232 serial interfaces might cause an error with a clock rate greater than 200 KHz.

  - MTU—9192 bytes, default value is 1504 bytes
  - HDLC
  - Line encoding—NRZ and NRZI
  - Invert data
  - Line protocol—EIA530/EIA530A, X.21, RS-449, RS-232, V.35
  - Data cables—Separate cable for each line protocol (both DTE/DCE mode)
  - Error counters (conformance to ANSI specification)
  - Alarms and defects
  - Data signal—Rx clock
  - Control signals
  - Serial autoresync
  - Diagnostic feature
  - Layer 2
  - SNMP
  - Anticounterfeit check

  [*Understanding the 8-Port Synchronous Serial GPIM*]

- **Ethernet in the First Mile support on G.SHDSL Mini-PIMs**—This feature is supported on SRX210, SRX220, SRX240, and SRX550 devices. This feature supports single-port EFM mode in SHDSL 2-wire mode, without disrupting the existing functionality of the PIC. Currently the G.SHDSL Mini-PIM supports ATM interfaces toward DSL lines in various modes like 2-wire, 4-wire, and 8-wire.

  NOTE: EFM is not supported in 4-wire and 8-wire modes.

  The following key features are supported on EFM mode on G.SHDSL Mini-PIMs:

  - IEEE 802.3-2004 compliant
  - VLAN over G.SHDSL EFM
  - Chassis cluster
  - IPV6 over EFM
  - Annexes A/B/F/G/Auto
  - Dying gasp
  - Line coding of 16- and 32-TCPAM (trellis coded pulse amplitude modulation)

  [*DSL Interfaces*]

- **Q-in-Q support on Layer 3 interfaces**—This feature is supported on all branch SRX Series and J Series devices.

The Q-in-Q feature is supported in both packet mode and flow mode. This feature allows you to configure flexible VLANs at the Ethernet port level. Flexible VLAN tagging is supported only in plain encapsulation and on Fast Ethernet/Gigabit Ethernet/10-Gigabit Ethernet interfaces.

The flexible VLAN is enabled to accept the following VLAN packets on the same physical Interface:

- Untagged VLAN packets (using native-vlan-id)
- Single VLAN packets
- Double VLAN packets

[*Configuring VLAN Tagging*]

[*Junos OS CLI Reference*]

Intrusion Detection and Prevention (IDP)

- **IDP policy compilation improvements**—This feature is supported on all SRX branch devices. On SRX100, SRX210, SRX240 these improvements are supported only on the high-memory variants.

  The IDP policy compilation process has been optimized to provide significant reductions in compilation time and memory utilization.

  [*Security IDP*]

J-Web

- **New Setup Wizard**—This feature is supported on all branch SRX Series devices.

  The New Setup wizard simplifies device configuration by guiding you through the process of setting up a device from start to finish.

  You can select one of the following modes:

  - Guided Setup — Default mode that takes you through the complete configuration process. Using Guided Setup mode, you can customize options for the Internet, DMZ, internal zones, policies, RVPN, and NAT.
  - Default Setup — Quick way to configure basic device elements. Using Default Setup mode, you can configure the device name, root password, user accounts, device time, and license details.

The New Setup wizard has the following advantages:

- Input validation
- Context-sensitive Help
- Smart navigation bar
- Pending changes review
- Accelerated quick start
- Can be relaunched from J-Web

Monitoring

- **System health monitoring**—This feature is supported on all branch SRX Series devices.

  The system health monitor can monitor resources such as CPU, memory, storage, open-file-descriptor, process-count, and temperature. Tracking critical resources utilization ensures that all parameters stay within normal limits and the system remains functional. In the event of a malfunction caused by abnormal resource usage, system health monitoring provides the diagnostic information required to identify the source of the problem.

  To enable the system health monitor, run the **set snmp health-monitor routing engine** CLI command.

  [*Monitoring System Resources for Branch SRX Series Devices*]

  [*Junos OS CLI Reference*]

Network Address Translation (NAT)

- **Increase in the maximum sessions allowed for a persistent NAT binding**—This feature is supported on all branch SRX Series devices.

  Previously, the maximum number of sessions allowed for a persistent NAT binding was 100. This limit is now 65,536. You can now configure the maximum number of sessions ranging from 8 through 65,536.

  [*max-session-number*]

  [*Junos OS CLI Reference*]

- **Static NAT support for port mapping**—This feature is supported on all branch SRX Series and J Series devices.

  Static NAT defines a one-to-one mapping from one IP subnet to another IP subnet. The existing static NAT functionality is enhanced to support the following types of translation:

  - To map multiple IP addresses and specified ranges of ports to the same IP address and a different range of ports
  - To map a specific IP address and port to a different IP address and port

  The new CLI statements **destination-port *low* to *high*** and **mapped-port *low* to *high*** are introduced as part of this enhancement.

  [*Example: Configuring Static NAT for Port Mapping*]

Security Profiles

- **New match criteria for user role firewall policies**—This feature is supported on all branch SRX Series devices.

  User role firewall policies can now specify the username as match criteria in the source-identity field. In the previous release, roles were the only valid input for the source-identity field. Roles are now considered optional.

Two additional show commands display the users and the combined users and roles that are specified in the user identification tables (UITs) and available for user and role provisioning:

- **show security user-identification user-provision all**
- **show security user-identification source-identity-provision all**

In addition, the connection setup rate has been improved when a user role firewall is enabled.

[*Understanding User Role Firewalls*]

- **Shadow policy check**—This feature is supported on SRX100, SRX210, SRX220, SRX240, and SRX650 devices.

  You can now check if there is any policy shadowing in the policy list using the following CLI commands:

  - For logical systems, run the **show security shadow-policies logical-system** ***lsys-name*** **from-zone** ***from-zone-name*** **to-zone** ***to-zone-name*** **policy** ***policy-name*** **reverse** command.
  - For global policies, run the **show security shadow-policies logical-system** ***lsys-name*** **global policy** ***policy-name*** **reverse** command.

    The CLI commands can be used to display:

    - All shadow policies within a context
    - If a given policy shadows one or more policies
    - If a given policy is shadowed by one or more policies

  [*Understanding Security Policy Ordering*]

  [*Verifying Shadow Policies*]

  [*show security shadow-policies logical-system*]

  [*Junos OS CLI Reference*]

System Logs

The following system logs are introduced in Junos OS Release 12.1X44-D10:

- **PKID_CERT_BASIC_CNSTRS_MISSING**—Certificate does not have the basic constraints field.
- **PKID_CERT_BASIC_CNSTRS_INV_CA**—Certificate does not have a valid CA flag.
- **ERRMSG(PKID_CERT_BASIC_CNSTRS_MISSING, LOG_ERR**—Basic constraints field is missing for the CA certificate <certificate-subject>.
- **ERRMSG(PKID_CERT_BASIC_CNSTRS_INV_CA, LOG_ERR**—Basic constraints field contains an invalid CA flag for the CA certificate <certificate-subject>.
- **PKID_CERT_NOT_BEFORE_FAIL**—Certificate /C=US/DC=juniper/ST=CA/L=Sunnyvale/O=PKI/OU=SSD/CN=bubba is not valid until 06-12-2012 21:44.

- **PKID_CERT_NOT_AFTER_FAIL**—Certificate /C=US/DC=juniper/ST=CA/L=Sunnyvale/O=PKI/OU=SSD/CN=bubba has expired, not valid after 06-12-2014 .21:44
- **PKID_CERT_ID_LOOKUP_FAIL**—Certificate chain does not contain certificate with ID 30.1.1.31 and Type IPSEC_ID_IPV4_ADDR.
- **PKID_CERT_ID_LOOKUP_FAIL**—Certificate chain does not contain certificate with ID /C=US/DC=juniper/ST=CA/L=Sunnyvale/O=PKI/OU=SSD/CN=bubba and Type IPSEC_ID_DER_ASN1_DN.
- **PKID_CERT_ID_LOOKUP_FAIL**—Certificate chain does not contain certificate with ID bubba@juniper.net and Type IPSEC_ID_USER_FQDN.
- **PKID_CERT_ID_LOOKUP_FAIL**—Certificate chain does not contain certificate with ID bubba.juniper.net and Type IPSEC_ID_FQDN.

Unified Threat Management (UTM)

- **UTM Enhanced Web Filtering - action on site reputation score**—This feature is supported on all branch SRX Series devices.

  In previous releases of Junos OS, the Threat Seeker Cloud (TSC) returned site reputation information to a device only if there was no category match found for a particular URL.

  With the introduction of this feature, TSC returns site reputation information for both categorized and uncategorized URLs. In addition, the UTM Enhanced Web Filtering supports configuring actions such as permit, log-and-permit, block, or quarantine on the site-reputation returned by TSC for both categorized and uncategorized URLs.

  [*UTM Web Filtering for Security Devices*]

  [*Junos OS CLI Reference Guide*]

- **UTM Enhanced Web Filtering - quarantine action**—This feature is supported on all branch SRX Series devices.

  In previous releases of Junos OS, UTM Enhanced Web filtering supported block, log-and-permit, and permit actions for HTTP/HTTPS requests. The block option restricted access to websites that did not adhere to organizations' security policies.

  With the introduction of this feature, UTM Enhanced Web filtering now also supports a quarantine action. When a user attempts to access a quarantined website, a warning message appears. Based on the user's response to the message, UTM Enhanced Web filtering allows or denies access to the site.

  [*UTM Web Filtering for Security Devices*]

  [*Junos OS CLI Reference Guide*]

USB

- **USB enable/disable feature**—This feature is supported on all branch SRX Series and on J Series devices.

  This feature allows the administrator to disable all USB ports on the device to block users from connecting a USB to the device. If a USB device is already mounted and connected, this feature unmounts and disables the device. Any transactions in progress on the USB device are aborted.

  Table 3 on page 21 lists the supported CLI commands:

Table 3: CLI Commands and Description

CLI Command	Description
show chassis usb storage	Displays the current status of any USB mass storage device and whether it is enabled or disabled.
set chassis usb storage disable	Disables mass storage devices that are connected on the USB ports.
delete chassis usb storage disable	Enables the use of USB mass storage devices on USB ports.

NOTE:

- The USB ports on a services gateway or services router are functional by default.
- Even if the USB ports are disabled, the USB LEDs still light up when the device is plugged in.
- This feature is supported only in Junos OS and is not supported in the uboot or loader phase.
- When Junos OS is booted from a USB storage device, this feature is unavailable.
- If a USB port is disabled, the **request system reboot media usb** command is not supported.
- If the kernel is configured to boot from USB, the kernel checks if USB is disabled early in the boot process. If USB is disabled, then the kernel might reboot.

[*Junos OS CLI Reference*]

Virtual Private Network (VPN)

- **AutoVPN**—AutoVPN hubs are supported on SRX240, SRX550, and SRX650 devices. AutoVPN spokes are supported on all branch SRX Series devices.

  AutoVPN allows network administrators to configure the hub in a hub-and-spoke IPsec VPN topology for current and future client device connections. No configuration changes are required on the hub when spoke devices are added or deleted, thus allowing administrators flexibility in managing large-scale network deployments.

  AutoVPN is supported on route-based IPsec VPNs. AutoVPN traffic must be IPv4. Dynamic routing protocols are supported to forward packets through the VPN tunnels.

  NOTE: The RIP dynamic routing protocol is not supported with AutoVPN in Junos OS Release 12.1X44-D10 and 12.1X44-D15.

  The supported authentication for AutoVPN hubs and spokes is X.509 public key infrastructure (PKI) certificates. The group IKE user type configured on the hub allows you to specify strings, to match the alternate subject field in spoke certificates. Partial matches for the subject fields in spoke certificates can also be specified.

  AutoVPN is configured and managed on SRX Series devices using the CLI. Multiple AutoVPN hubs can be configured on a single SRX Series device. The maximum spokes supported by a configured hub is specific to the model of the SRX Series device. AutoVPN supports VPN monitoring and dead peer detection.

  [*AutoVPNs for Security Devices*]

- **Dynamic VPN enhancement**—This feature is supported on SRX100, SRX210, SRX220, SRX240, and SRX650 devices.

  Dynamic VPN (DVPN) includes the following enhancements:

  - **Grouping of users**—The duplication of the list of users configured under the **[dynamic vpn]** hierarchy and under the **[access]** hierarchy has been removed, and the configuration of DVPN users and the association of the users with client VPN has been simplified. Users are now grouped under the **[access]** hierarchy alone.

    A reference from security dynamic VPN to the configured user group under **[access]** hierarchy still needs to be configured under **[security dynamic vpn]** hierarchy so that you can associate a user with a client configuration.

  - **IKE and IPsec configuration validation**—There is no restriction on the set of IKE and IPsec parameters needed. IKE and IPsec configuration validation is done through commit checks.

    A commit time check is performed by the httpd gk to verify if all IKE and IPsec parameters needed for DVPN are correctly configured. If the configuration is invalid for IKE or IPsec, the commit fails and an error message is displayed.

    NOTE: The commit checks are turned off by default. You can enable the commit checks by using the **security dynamic vpn commit checks** command.

- **Removal of the requirement to configure Web management services**—Begining with Junos OS Release 12.1X44 D10, you do not have to configure Web management services to enable DVPN.

  NOTE: **Previous configurations that had the loopback interface set to disable Web management now enables Web management on the loopback interface.**

  The Appweb webserver is started when Web management is not configured. All other Web management configuration parameters such as https (by default, a system-generated certificate must be used) and debug level limits (by default, this is be 9 for the webserver) that are needed to start the Appweb webserver now have the default values.

  Traceoptions is added under **[security dynamic vpn]** hierarchy to log dvpn related messages. You need to configure taceoptions to view the DVPN trace log messages.

[*Example: Configuring Dynamic VPN*]

[*Example: Configuring Unique URLs for J-Web and Dynamic VPN*]

[*Dynamic VPN Configuration Overview*]

[*Dynamic Virtual Private Network (DVPN) Enhancement*]

[*dynamic-vpn*]

[*show security dynamic-vpn users*]

[*show security dynamic-vpn users terse*]

[*interface (Security Dynamic VPN)*]

[*user-groups (Security Dynamic VPN)*]

[*traceoptions (Security Dynamic VPN)*]

[*clients (Security)*]

[*config-check (Security Dynamic VPN)*]

- **Improvements in VPN debugging capabilities**— This feature is supported on all branch SRX Series devices.

  The following enhancements are now available to improve the VPN debugging capabilities:

  - Previously, debugging of tunnels was limited to the policy manager; which is now extended to include QuickSec software stacks.
  - The **show security ipsec security-associations detail** command is enhanced to provide information such as VPN name, tunnel ID, and bind interface in the security associations (SA) output.
  - The **show security ike security-associations detail** command is enhanced to provide gateway name and Diffie-Hellman (DH) group information in the SA output.

- The **show security ipsec security-associations vpn-name** ***vpn-name*** command displays the IPsec SA based on the VPN name. For policy-based VPNs and dial-up VPNs, the output displays multiple SAs because the VPN names are shared.
- The new **show security ipsec inactive-tunnels** command displays security information about the inactive tunnels.
- The new **request security ike (debug-enable | debug-disable)** command enables IKE debugging through operational mode commands.
- The common log location for all SRX Series devices is now **/var/log/*log-filename***.

NOTE: If you do not specify the log filename for the *log-filename* field, then all logs are written to the kmd log.

[*Junos OS CLI Reference*]

- **Loopback interface for chassis cluster VPN**—This feature is supported on all SRX Series devices.

  An Internet Key Exchange (IKE) gateway needs an external interface to communicate with a peer device. In a chassis cluster setup, the node on which the external interface is active selects a Services Processing Unit (SPU) to support the VPN tunnel. IKE and IPsec packets are processed on that SPU. Therefore, the active external interface determines the anchor SPU.

  In a chassis cluster setup, this external interface can be the redundant Ethernet (reth) interface or a standalone interface. These interfaces can go down when the physical interfaces are down. Therefore, loopback interfaces can be used to reach the peer gateway because the loopback interfaces are alternate physical interfaces.

  This feature allows the loopback interface to be configured for any redundancy group. This redundancy group configuration is only checked for VPN packets, because only VPN packets must find the anchor SPU through the active interface.

  On branch SRX Series devices, the lo0 pseudointerface can be configured in any redundancy group; for example, RG0, RG1, RG2, and so on.

  You can use the **show chassis cluster interfaces** command to view the redundant pseudointerface information.

  [*VPN for Security Devices*]

  [*Junos OS CLI Reference*]

Related Documentation

- Changes in Default Behavior and Syntax in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 25
- Known Limitations in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 34
- Outstanding Issues in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 62

- Resolved Issues in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 65
- Errata and Changes in Documentation for Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 80
- Upgrade and Downgrade Instructions for Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 90

Changes in Default Behavior and Syntax in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers

The following current system behavior, configuration statement usage, and operational mode command usage might not yet be documented in the Junos OS documentation:

Application Firewall

- Prior to Junos OS release 11.4R6, when a rule specifies **dynamic-application junos:HTTP** without specifying any other nested application, the rule matches all HTTP traffic whether the traffic contains a nested application or not.

  In Junos OS release 11.4R6 and later, that functionality has changed. When a rule specifies **dynamic-application junos:HTTP**, only HTTP traffic with no nested members is matched.

  Consider the following application firewall ruleset:

  ```
  rule-sets http-ruleset {
     rule rule1 {
        match {
           dynamic-application [junos:FACEBOOK];
        }
        then {
           deny;
        }
     }
     rule rule2 {
        match {
           dynamic-application [junos:HTTP];
        }
        then {
           permit;
        }
     }
     default-rule {
        deny;
     }
  }
  ```

  Prior to Junos OS release 11.4R6, the sample rules would be applied to traffic as shown in the following list:

  - HTTP traffic with junos:FACEBOOK as a nested application would be denied by rule1.
  - HTTP traffic with no nested application would be permitted by rule2.

- HTTP traffic with a nested application other than junos:FACEBOOK, such as junos:TWITTER, would be permitted by rule2 because it is HTTP traffic that does not match any previous rule.

After Junos OS release 11.4R6, the dynamic application junos:HTTP matches only the traffic that does not contain a recognizable nested application. The sample rules would now be applied differently:

- HTTP traffic with junos:FACEBOOK as a nested application would be denied by rule1.
- HTTP traffic with no nested application would be permitted by rule2.
- However, HTTP traffic with a nested application other than junos:FACEBOOK, such as junos:TWITTER, would no longer match rule2. Instead, the traffic would be denied by the default rule.

AppSecure

- On all branch SRX Series devices, application tracking is enabled by default. You can disable application tracking with the **set security application-tracking disable** command. This command allows you to disable and reenable application tracking without modifying your existing zone selections.

Command-Line Interface (CLI)

New or Changed CLI

- On all branch SRX Series and J Series devices, the following commands are now supported:

CLI Command	Description
show pppoe interfaces	List all Point-to-Point Protocol over Ethernet (PPPoE) sessions.
request pppoe connect	Connect to all sessions that are down.
request pppoe connect ***pppoe interface name***	Connect only to the specified session.
request pppoe disconnect	Disconnect all sessions that are up.
request pppoe disconnect ***session id*** **or** ***pppoe interface name***	Disconnect only the specified session, identified by either a session ID or a PPPoE interface name.

- On all branch SRX Series devices, the **show security flow session extensive** command has been updated to show the predefined application name.

Deprecated Items for Security Hierarchy

Table 4 on page 27 lists deprecated items (such as CLI statements, commands, options, and interfaces).

CLI statements and commands are deprecated—rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration. We strongly recommend that you phase out deprecated items and replace them with supported alternatives.

Table 4: Items Deprecated in Release 12.1

Deprecated Item	Replacement	Hierarchy Level or Command Syntax	Additional Information
download-timeout	-	**download-timeout timeout**	On all branch SRX Series devices, the **download-timeout** command is deprecated. If the configuration is present, then that configuration will be ignored. The idpd daemon internally triggers the security package to install when an automatic download is completed. There is no need to configure any download timeout.
node	-	**request security idp security-package download**	On all branch SRX Series devices operating in a chassis cluster, the **request security idp security-package download** command with the **node** option is not supported: **request security idp security-package download node primary** **request security idp security-package download node local** **request security idp security-package download node all**

Compatibility

- **Version Compatibility for Junos SDK**—Beginning with Junos OS Release 12.1X44-D10, Junos OS applications will install on the Junos OS only if the application is built with the same release as the Junos OS Release on which the application is being installed.

  For example, an application built with Junos OS Release 12.1R2 will only install on Junos OS Release 12.1R2 and will not install on Junos OS Release 12.1R1 or Junos OS Release 12.1R3.

Flow and Processing

- The minimum value you can configure for TCP session initialization is 4 seconds. The default value is 20 seconds; if required you can set the TCP session initialization value to less than 20 seconds.

- On all branch SRX Series devices, the default value of Type of Service (ToS) for IKE packets is changed from 0x00 to 0xc0.

Hardware

- On SRX550 devices, the mini-USB console cable provides a “break” message to the Windows application whenever the console cable is unplugged and re-plugged. If you have configured “debugger-on-break”, the system goes to the **db>** prompt because the system receives a break character. This behavior is specific to the mini-USB console.

Interfaces and Routing

- On SRX240 and SRX650 devices, for the Layer 2 link aggregation group (LAG) interface, the hash algorithm for load balancing is now based on source IP address and destination IP address instead of source MAC address and destination MAC address.

Intrusion Detection and Prevention (IDP)

- New sensor configuration options have been added to log run conditions as IDP session capacity and memory limits are approached, and to analyze traffic dropped by IDP and application identification due to exceeding these limitations.
  - At start up, traffic is ignored by IDP by default if the IDP policy is not yet loaded. The **drop-if-no-policy-loaded** option changes this behavior so that all sessions are dropped before the IDP policy is loaded.

    Use the following configuration command to drop traffic before the IDP policy is loaded:

    ```
    set security idp sensor-configuration flow drop-if-no-policy-loaded
    ```

    The following new counters have been added to the **show security idp counters flow** command output to analyze dropped traffic due to the **drop-if-no-policy-loaded** option:

    ```
    Sessions dropped due to no policy                    0
    ```
  - By default, IDP ignores failover sessions in an SRX chassis cluster deployment. The **drop-on-failover** option changes this behavior and automatically drops sessions that are in the process of being inspected on the primary node when a failover to the secondary node occurs.

    Use the following configuration command to drop failover sessions:

    ```
    set security idp sensor-configuration flow drop-on-failover
    ```

    The following new counter has been added to the **show security idp counters flow** command output to analyze dropped failover traffic due to the **drop-on-failover** option:

    ```
    Fail-over sessions dropped                           0
    ```
  - By default, sessions are not dropped if the IDP session limit or resource limits are exceeded. In this case, IDP and other sessions are dropped only when the device’s session capacity or resources are depleted. The **drop-on-limit** option changes this behavior and drops sessions when resource limits are exceeded.

Use the following configuration commands to set or remove the **drop-on-limit** option:

```
set security idp sensor-configuration flow drop-on-limit
delete security idp sensor-configuration flow drop-on-limit
```

The following new counters have been added to the **show security idp counters flow** command output to analyze dropped IDP traffic due to the **drop-on-limit** option:

```
SM Sessions encountered memory failures              0
SM Packets on sessions with memory failures          0
SM Sessions dropped                                  0
Both directions flows ignored                        0
IDP Stream Sessions dropped due to memory failure    0
IDP Stream Sessions ignored due to memory failure    0
IDP Stream Sessions closed due to memory failure     0
Number of times Sessions exceed high mark            0
Number of times Sessions drop below low mark         0
Memory of Sessions exceeds high mark                 0
Memory of Sessions drops below low mark              0
```

The following counters have also been added to the **show security idp counters application-identification** command output to analyze dropped application identification traffic due to the **drop-on-limit** option:

```
AI-session dropped due to malloc failure before session create       0
AI-Sessions dropped due to malloc failure after create               0
AI-Packets received on sessions marked for drop due to malloc failure 0
```

The following options have been added to trigger informative log messages about current run conditions. When set, the log messages are triggered whether the **drop-on-limit** option is set or not.

- The **max-sessions-offset** option sets an offset for the maximum IDP session limit. When the number of IDP sessions exceeds the maximum session limit, a warning is logged that conditions exist where IDP sessions could be dropped. When the number of IDP sessions drops below the maximum IDP session limit minus the offset value, a message is logged that conditions have returned to normal.

  ```
  Jul 19 04:38:13 4.0.0.254 RT_IDP: IDP_SESSION_LOG_EVENT: IDP: at 1374233893,
   FPC 4 PIC 1 IDP total sessions pass through high mark 100000. IDP may drop
   new sessions. Total sessions dropped 0.

  Jul 19 04:38:21 4.0.0.254 RT_IDP: IDP_SESSION_LOG_EVENT: IDP: at 1374233901,
   FPC 4 PIC 1 IDP total sessions drop below low mark 99000. IDP working in
  normal mode. Total sessions dropped 24373.
  ```

  Use the following configuration command to set the **max-sessions-offset** option:

  ```
  set security idp sensor-configuration flow max-sessions-offset offset-value
  ```

- The **min-objcache-limit-lt** option sets a lower threshold for available cache memory. The threshold value is expressed as a percentage of available IDP cache memory. If the available cache memory drops below the lower threshold level, a message is logged stating that conditions exist where IDP sessions could be dropped because of memory allocation failures. For example, the following message shows that the IDP cache memory has dropped below the lower threshold and that a number of sessions have been dropped:

  ```
  Jul 19 04:07:33 4.0.0.254 RT_IDP: IDP_SESSION_LOG_EVENT: IDP: at 1374232053,
   FPC 4 PIC 1 IDP total available objcache(used 4253368304, limit 7247757312)
   drops below low mark 3986266515. IDP may drop new sessions. Total sessions
   dropped 1002593.
  ```

  Use the following configuration command to set the **min-objcache-limit-lt** option:

  ```
  set security idp sensor-configuration flow min-objcache-limit-lt
    lower-threshold-value
  ```

  - The **min-objcache-limit-ut** option sets an upper threshold for available cache memory. The threshold value is expressed as a percentage of available IDP cache memory. If available IDP cache memory returns to the upper threshold level, a message is logged stating that available cache memory has returned to normal. For example, the following message shows that the available IDP cache memory has increased above the upper threshold and that it is now performing normally:

    ```
    Jul 19 04:13:47 4.0.0.254 RT_IDP: IDP_SESSION_LOG_EVENT: IDP: at 1374232428,
     FPC 4 PIC 1 IDP total available objcache(used 2782950560, limit 7247757312)
     increases above high mark 4348654380. IDP working in normal mode. Total
    sessions dropped 13424632.
    ```

    NOTE: **This message is triggered only if the lower threshold has been reached and the available memory has returned above the upper threshold. Fluctuations in available memory that dropped below the upper threshold but did not fall below the lower threshold would not trigger the message.**

    Use the following configuration commands to set the **min-objcache-limit-ut** option:

    ```
    set security idp sensor-configuration flow min-objcache-limit-ut
      upper-threshold-value
    ```

- By default, values for IDP reassembler packet memory and application identification packet memory used by IDP are established as percentages of all memory. In most cases, these default values are adequate.

  - If a deployment exhibits an excessive number of dropped TCP packets or retransmissions resulting in high IDP reassembly memory usage, use the following option:

    The **max-packet-mem-ratio** option to reset the percentage of available IDP memory for IDP reassembly packet memory. Acceptable values are between 5% and 40%.

    ```
    set security idp sensor-configuration re-assembler max-packet-mem-ratio
      percentage-value
    ```

  - If a deployment exhibits an excessive number of ignored IDP sessions due to reassembler and application identification memory allocation failures, use the following options:

- The **max-packet-memory-ratio** option sets application identification packet memory limit as a percentage of available IDP memory. This memory is only used by IDP in cases where application identification delays identifying an application. Acceptable values are between 5% and 40%.

  ```
  set security idp sensor-configuration application-identification
    max-packet-memory-ratio percentage-value
  ```

- The **max-reass-packet-memory-ratio** option sets the reassembly packet memory limit for application identification as a percentage of available IDP memory. Acceptable values are between 5% and 40%.

  ```
  set security idp sensor-configuration application-identification
    max-reass-packet-memory-ratio percentage-value
  ```

NOTE: The **max-packet-memory** option has been deprecated and replaced by the new **max-packet-memory-ratio** and **max-reass-packet-memory-ratio** options.

Junos OS Federal Information Processing Standard (FIPS)

- On all SRX Series devices, the secure Junos OS software environment does not permit DSA key pairs with modulus greater than 1024 bits.

Junos Pulse

- On all branch SRX Series devices, the Junos Pulse client is updated from Release 2.0R3 to 4.0R2. If you are using an older version of Junos Pulse client then it will get upgraded automatically to the newer version during next login.

J-Web

- On all branch SRX Series and J Series devices, the username field does not accept HTML tags or the “<” and “>” characters. The following error message appears:

  ```
  A username cannot include certain characters, including < and >
  ```

Layer 2 Transparent Mode

- On SRX550 devices with Hitachi configurations, Unified Threat Management (UTM) Kaspersky full antivirus protection is supported in Layer 2 transparent mode.

System Logs

On all branch SRX Series devices, the following system log messages have been updated to include the **certificate ID** in Junos OS Release 12.1X44-D10:

- PKID_PV_KEYPAIR_DEL

  Existing message: **Key-Pair deletion failed**

  New message: **Key-Pair deletion failed for <cert-id>**

- PKID_PV_CERT_DEL

  Existing message: **Certificate deletion has occurred**

  New message: **Certificate deletion has occurred for <cert-id>**

- PKID_PV_CERT_LOAD

  Existing message: **Certificate has been successfully loaded**

  New message: **Certificate <cert-id> has been successfully loaded**

- PKID_PV_KEYPAIR_GEN

  Existing message: **Key-Pair has been generated**

  New message: **Key-Pair has been generated for <cert-id>**

Virtual Private Network (VPN)

- As of Junos OS Release 11.4, checks are performed to validate the IKE ID received from the VPN peer device. By default, SRX Series and J Series devices validate the IKE ID received from the peer with the IP address configured for the IKE gateway. In certain network setups, the IKE ID received from the peer (which can be an IPv4 or IPv6 address, fully qualified domain name, distinguished name, or e-mail address) does not match the IKE gateway configured on the SRX Series or J Series device. This can lead to a Phase 1 validation failure.

  To modify the configuration of the SRX Series or J Series device or the peer device for the IKE ID that is used:

  - On the SRX Series or J Series device, configure the **remote-identity** statement at the [**edit security ike gateway *gateway-name***] hierarchy level to match the IKE ID that is received from the peer. Values can be an IPv4 or IPv6 address, fully qualified domain name, distinguished name, or e-mail address.

    NOTE: If you do not configure **remote-identity**, the device uses the IPv4 or IPv6 address that corresponds to the remote peer by default.

  - On the peer device, ensure that the IKE ID is the same as the **remote-identity** configured on the SRX Series or J Series device. If the peer device is an SRX Series or J Series device, configure the **local-identity** statement at the [**edit security ike gateway *gateway-name***] hierarchy level. Values can be an IPv4 or IPv6 address, fully qualified domain name, distinguished name, or e-mail address.

- On all branch SRX Series devices, for Path Maximum Transmission Unit (PMTU) calculations, the IPsec authentication data length is fixed at 16 bytes. However, the authentication data length for packets going through the IPsec tunnel is in accordance with the authentication algorithm negotiated for that tunnel.

  The authentication data lengths for the different algorithms are:

  - hmac-md5-96 (12 bytes)
  - hmac-sha-256-128 (16 bytes)
  - hmac-sha1-96 (12 bytes)

- The subject fields of a digital certificate can include Domain Component (DC), Common Name (CN), Organization Unit (OU), Organization (O), Location (L), State (ST), and Country (C).

  In earlier releases, the **show security pki ca-certificate** and **show security pki local-certificate** CLI operational commands displayed only a single entry for each subject field, even if the certificate contained multiple entries for a field. For example, a certificate with two OU fields such as “OU=Shipping Department,OU=Priority Mail” displayed with only the first entry “OU=Shipping Department.” The **show security pki ca-certificate** and **show security pki local-certificate** CLI commands now display the entire contents of the subject field, including multiple field entries.

  The commands also display a new subject string output field that shows the contents of the subject field as it appears in the certificate.

- When a remote user launches newly installed client software, the link to close the Web browser window does not appear in the VPN client launch page. The user must close the browser window by clicking the browser’s close button.

- On all branch SRX Series devices, the secure Junos OS software environment does not permit DSA key pairs with modulus greater than 1024 bits.

Related Documentation

- New Features in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 6
- Known Limitations in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 34
- Outstanding Issues in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 62
- Resolved Issues in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 65
- Errata and Changes in Documentation for Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 80

- Upgrade and Downgrade Instructions for Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 90

Known Limitations in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers

AppSecure

- J-Web pages for AppSecure are preliminary.
- When you create custom application or nested application signatures for Junos OS application identification, the order value must be unique among all predefined and custom application signatures. The order value determines the application matching priority of the application signature.

  The order value is set with the **set services application-identification application application-name signature order** command. You can also view all signature order values by entering the **show services application-identification | display set | match order** command. You will need to change the order number of the custom signature if it conflicts with another application signature.
- Custom application signatures and custom nested application signatures are not currently supported by J-Web.
- When ALG is enabled, application identification includes the ALG result to identify the application of the control sessions. Application firewall permits ALG data sessions whenever control sessions are permitted. If the control session is denied, there will be no data sessions. When ALG is disabled, application identification relies on its signatures to identify the application of the control and data sessions. If a signature match is not found, the application is considered unknown. Application firewall handles applications based on the application identification result.

AX411 Access Points

- On SRX210, SRX240, and SRX650 devices, you can configure and mange maximum of four access points.
- On all branch SRX Series devices, managing AX411 WLAN Access Points through a Layer 3 aggregated Ethernet (ae) interface is not supported.

Chassis Cluster

- SRX100, SRX210, SRX240, and SRX650 devices have the following chassis cluster limitations:
  - Virtual Router Redundancy Protocol (VRRP) is not supported.
  - Unified in-service software upgrade (ISSU) is not supported.
  - The 3G dialer interface is not supported.
  - On SRX Series device failover, access points on the Layer 2 switch reboot and all wireless clients lose connectivity for 4 to 6 minutes.

  - On very-high-bit-rate digital subscriber line (VDSL) Mini-PIMs, chassis cluster is not supported for VDSL mode.
  - Queuing on the aggregated Ethernet (ae) interface is not supported.
  - Group VPN is not supported.
  - Sampling features such as flow monitoring, packet capture, and port mirror on the redundant Ethernet (reth) interfaces are not supported.
  - Switching is not supported in chassis cluster mode for SRX100 Series devices.
  - The Chassis Cluster MIB is not supported.
  - Any packet-based services such as MPLS and CLNS are not supported.
  - On lsq-0/0/0 interface, Link services Multilink Point-to-Point Protocol (MLPPP), Multilink Frame Relay (MLFR), and Compressed Real-Time Transport Protocol (CRTP) are not supported.
  - On lt-0/0/0 interface, CoS for real-time performance monitoring (RPM) is not supported.
- Packet-based forwarding for MPLS and International Organization for Standardization (ISO) protocol families is not supported.
- The factory default configuration for SRX100 devices automatically enables Layer 2 Ethernet switching. Layer 2 Ethernet switching is not supported in chassis cluster mode for SRX100 devices. If you use the factory default configuration, you must delete the Ethernet switching before you enable chassis clustering.
- On all J Series devices, a Fast Ethernet port from a 4-port Ethernet PIM cannot be used as a fabric link port in a chassis cluster.
- On all branch SRX Series devices, redundant Ethernet (reth) interfaces and lo0 interface are supported for IKE external interface configuration in IPsec VPN. Other interface types can be configured, but IPsec VPN might not work.
- On all J Series devices, the ISDN feature on chassis cluster is not supported.

Command-Line Interface (CLI)

- On all branch SRX Series and all J Series devices, the **clear services flow** command is not supported.
- On all J Series devices, RADIUS accounting is not supported.
- On SRX210 and SRX240 devices, J-Web crashes if more than nine users log in to the device by using the CLI. The number of users allowed to access the device is limited as follows:
  - For SRX210 devices: four CLI users and three J-Web users
  - For SRX240 devices: six CLI users and five J-Web users
- On J6350 devices, there is a difference in the power ratings provided by user documentation (*J Series Services Routers Hardware Guide* and PIM, uPIM, and ePIM Power and Thermal Calculator) and the power ratings displayed by CLI (by a unit of

1). The CLI display rounds off the value to a lower integer and the ratings provided in user documentation rounds off the value to the higher integer. As a workaround, follow the user documentation for accurate ratings.

- On all branch SRX Series devices, the tunnel-queuing option is not supported in chassis cluster mode.

Connectivity Fault Management (CFM)

- CFM is not supported on the following interfaces:
  - 8-Port Gigabit Ethernet small form-factor pluggable (SFP) XPIM
  - 2-Port 10-Gigabit Ethernet XPIM
  - 1-Port SFP Mini-PIM
- CFM is supported only on interfaces with family Ethernet switching.

Dynamic Host Configuration Protocol (DHCP)

- On all branch SRX Series and J Series devices, DHCPv6 client authentication is not supported.
- On all branch SRX Series and J Series devices, DHCP is not supported in a chassis cluster.

Flow and Processing

- On all branch SRX Series and J Series devices, a mismatch between the Firewall Counter Packet and Byte Statistics values, and between the Interface Packet and Byte Statistics values, might occur when the rate of traffic increases above certain rates of traffic.
- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, due to a limit on the number of large packet buffers, Routing Engine based sampling might run out of buffers for packet sizes greater than or equal to 1500 bytes and hence those packets will not be sampled. The Routing Engine could run out of buffers when the rate of the traffic stream is high.
- On SRX100 and SRX240 devices, the data file transfer rate for more than 20 Mbps is reduced by 60 percent with the introduction of Junos Pulse 1.0 client as compared to the Acadia client that was used before Junos OS Release 11.1.
- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, the default authentication table capacity is 10,000; the administrator can increase the capacity to a maximum of 15,000.
- On all branch SRX Series and J Series devices, when devices are operating in flow mode, the Routing Engine side cannot detect the path maximum transmission unit (PMTU) of an IPv6 multicast address (with a large size packet).
- On all branch SRX Series devices, you cannot configure route policies and route patterns in the same dial plan.
- On all J Series devices, even when forwarding options are set to drop packets for the ISO protocol family, the device forms End System-to-Intermediate System (ES-IS)

adjacencies and transmits packets because ES-IS packets are Layer 2 terminating packets.

- On all branch SRX Series and J Series devices, high CPU utilization triggered for reasons such as CPU intensive commands and SNMP walks causes the Bidirectional Forwarding Detection (BFD) protocol to flap while processing large BGP updates.
- On SRX210, SRX240, and J Series devices, broadcast TFTP is not supported when flow is enabled on the device.
- On SRX210, SRX240, and SRX650 devices, the maximum number of concurrent sessions for SSH, Telnet, and Web is as follows:

Sessions	SRX210	SRX240	SRX650
SSH	3	5	5
Telnet	3	5	5
Web	3	5	5

NOTE: These defaults are provided for performance reasons.

- On SRX210 and SRX240 devices, for optimized efficiency, we recommend that you limit use of CLI and J-Web to the numbers of sessions listed in the following table:

Device	CLI	J-Web	Console
SRX210	3	3	1
SRX240	5	5	1

- On SRX100 devices, Layer 3 control protocols (OSPF, using multicast destination MAC address) on the VLAN Layer 3 interface work only with access switch ports.

Group VPN Interoperability with Cisco's GET VPN for Juniper Networks Security Devices that Support Group VPN

Cisco's implementation of the Group Domain of Interpretation (GDOI) is called *Group Encryption Transport (GET) VPN*. While group VPN in Junos OS and Cisco's GET VPN are both based on RFC 3547, *The Group Domain of Interpretation*, there are some implementation differences that you need to be aware of when deploying GDOI in a networking environment that includes both Juniper Networks security devices and Cisco routers. This topic discusses important items to note when using Cisco routers with GET VPN and Juniper Networks security devices with group VPN.

Cisco GET VPN members and Juniper Group VPN members can interoperate as long as the server role is played by a Cisco GET VPN server, Juniper Networks security devices are group members.

The group VPN in Release 12.1 of Junos OS has been tested with Cisco GET VPN servers running Version 12.4(22)T and Version 12.4(24)T.

To avoid traffic disruption, do not enable rekey on a Cisco server when the VPN group includes a Juniper Networks security device. The Cisco GET VPN server implements a proprietary ACK for unicast rekey messages. If a group member does not respond to the unicast rekey messages, the group member is removed from the group and is not able to receive rekeys. An out-of-date key causes the remote peer to treat IPsec packets as bad security parameter indexes (SPIs). The Juniper Networks security device can recover from this situation by reregistering with the server and download the new key.

Antireplay must be disabled on the Cisco server when a VPN group of more than two members includes a Juniper Networks security device. The Cisco server supports time-based antireplay by default. A Juniper Networks security device will not interoperate with a Cisco group member if time-based antireplay is used because the timestamp in the IPsec packet is proprietary. Juniper Networks security devices are not able to synchronize time with the Cisco GET VPN server and Cisco GET VPN members because the sync payload is also proprietary. Counter-based antireplay can be enabled if there are only two group members.

According to Cisco documentation, the Cisco GET VPN server triggers rekeys 90 seconds before a key expires, and the Cisco GET VPN member triggers rekeys 60 seconds before a key expires. When interacting with a Cisco GET VPN server, a Juniper Networks security device member needs to match Cisco behavior.

A Cisco GET VPN member accepts all keys downloaded from the GET VPN server. Policies associated with the keys are dynamically installed. A policy does not have to be configured on a Cisco GET VPN member locally, but a deny policy can optionally be configured to prevent certain traffic from passing through the security policies set by the server. For example, the server can set a policy to have traffic between subnet A and subnet B be encrypted by key 1. The member can set a deny policy to allow OSPF traffic between subnet A and subnet B not to be encrypted by key 1. However, the member cannot set a permit policy to allow more traffic to be protected by the key. The centralized security policy configuration does not apply to the Juniper Networks security device.

On a Juniper Networks security device, the **ipsec-group-vpn** configuration statement in the permit tunnel rule in a scope policy references the group VPN. This allows multiple policies referencing a VPN to share an SA. This configuration is required to interoperate with Cisco GET VPN servers.

Logical key hierarchy (LKH), a method for adding and removing group members, is not supported with group VPN on Juniper Networks security devices.

GET VPN members can be configured for cooperative key servers (COOP KSs), an ordered list of servers with which the member can register or reregister. Multiple group servers cannot be configured on group VPN members.

Hardware

On SRX100, SRX110, SRX210, and SRX220 devices:

- DRAM memory is not supported.

- Chassis cluster on devices with 1GB of memory is not supported because of different capacity numbers between 1 GB and 2 GB models.

Interfaces and Routing

- On all branch SRX Series devices, IPv6 traffic transiting over IPv4 based IP over IP tunnel (for example, IPv6-over-IPv4 using ip-x/x/x interface) is not supported.
- ATM interface takes more than 5 minutes to show up when CPE is configured in ANSI-DMT mode and CO is configured in automode. This occurs only with ALU 7300 DSLAM, due to limitation in current firmware version running on the ADSL Mini-PIM.
- On SRX650 devices, you can only create a maximum of 63 physical interface devices with 1 GB RAM capacity. Therefore, we recommend that you use only 7-octal serial cards to create physical interface devices. To optimally use the 8-octal serial cards, and to create 64 physical interface devices, you require an SRX650 device with 2 GB RAM capacity.
- On SRX100 and J Series devices, dynamic VLAN assignments and guest VLANs are not supported.
- On all branch SRX Series devices, the subnet directed broadcast feature is not supported.
- On SRX650 devices, Ethernet switching is not supported on Gigabit Ethernet interfaces (ge-0/0/0 through ge-0/0/3 ports).
- On SRX210, SRX220, SRX240, and SRX650 devices, logs cannot be sent to NSM when logging is configured in the stream mode. Logs cannot be sent because the security log does not support configuration of the source IP address for the fxp0 interface and the security log destination in stream mode cannot be routed through the fxp0 interface. This implies that you cannot configure the security log server in the same subnet as the fxp0 interface and route the log server through the fxp0 interface.
- On all branch SRX Series devices, the number of child interfaces per node is restricted to 4 on the redundant Ethernet (reth) interface and the number of child interfaces per reth interface is restricted to 8.
- On SRX240 High Memory devices, traffic might stop between the SRX240 device and the Cisco switch due to link mode mismatch. We recommend setting same value to the autonegotiation parameters on both ends.
- On SRX100 devices, the link goes down when you upgrade FPGA on 1xGE SFP. As a workaround, run the **restart fpc** command and restart the FPC.
- On SRX210 devices with VDLS2, ATM COS VBR-related functionality cannot be tested.
- On SRX210 devices, Internet Group Management Protocol version 2 (IGMPv2) JOINS messages are dropped on an integrated routing and bridging (IRB) interface. As a workaround, enable IGMP snooping to use IGMP over IRB interfaces.
- On all J Series devices, the DS3 interface does not have an option to configure multilink-frame-relay-uni-nni (MFR).

- On SRX210, SRX220, and SRX240 devices, every time the VDSL2 Mini-PIM is restarted in the asymmetric digital subscriber line (ADSL) mode, the first packet passing through the Mini-PIM is dropped.
- On SRX240 Low Memory devices and SRX240 High Memory devices, the RPM server operation does not work when the probe is configured with the option **destination-interface**.
- On all J Series devices, Link Layer Discovery Protocol (LLDP) is not supported on routed ports.
- In J Series xDSL PIMs, mapping between IP CoS and ATM CoS is not supported. If the user configures IP CoS in conjunction with ATM CoS, the logical interface level shaper matching the ATM CoS rate must be configured to avoid congestion drops in segmentation and reassembly (SAR) as shown in following examples:

  Example:

  ```
  set interfaces at-5/0/0 unit 0 vci 1.110
  set interfaces at-5/0/0 unit 0 shaping cbr 62400 ATM COS
  set class-of-service interfaces at-5/0/0 unit 0 scheduler-map sche_map IP COS
  set class-of-service interfaces at-5/0/0 unit 0 shaping-rate 62400 ADD IFL SHAPER
  ```
- On SRX210, SRX220, and SRX240 devices, 1-Port Gigabit Ethernet SFP Mini-PIM does not support switching.
- On SRX650 devices, MAC pause frame and frame check sequence (FCS) error frame counters are not supported for the interfaces ge-0/0/0 through ge-0/0/3.
- On SRX240 and SRX650 devices, the VLAN range from 3967 to 4094 falls under the reserved VLAN address range, and the user is not allowed any configured VLANs from this range.
- On SRX650 devices, the last four ports of a 24-Gigabit Ethernet switch GPIM can be used either as RJ-45 or small form-factor pluggable transceiver (SFP) ports. If both are present and providing power, the SFP media is preferred. If the SFP media is removed or the link is brought down, then the interface will switch to the RJ-45 medium. This can take up to 15 seconds, during which the LED for the RJ-45 port might go on and off intermittently. Similarly, when the RJ-45 medium is active and a SFP link is brought up, the interface will transition to the SFP medium, and this transition could also take a few seconds.
- On SRX210 devices, the USB modem interface can handle bidirectional traffic of up to 19 Kbps. On oversubscription of this amount (that is, bidirectional traffic of 20 Kbps or above), keepalives do not get exchanged, and the interface goes down.
- On SRX100, SRX210, SRX240, and SRX650 devices, on the Layer 3 aggregated Ethernet (ae) interface, the following features are not supported:
  - Encapsulations (such as CCC, VLAN CCC, VPLS, and PPPoE)
  - J-Web
  - 10-Gigabit Ethernet
- On SRX100 devices, the multicast data traffic is not supported on IRB interfaces.

- On SRX240 High Memory devices, when the **system login deny-sources** statement is used to restrict the access, it blocks a remote copy (rcp) between nodes, which is used to copy the configuration during the commit routine. Use a firewall filter on the lo0.0 interface to restrict the Routing Engine access, However, if you choose to use the **system login deny-sources** statement, check the private addresses that were automatically on lo0.x and sp-0/0/0.x and exclude them from the denied list.
- On SRX100, SRX210, SRX220, SRX240, SRX650, and all J Series devices, on VLAN-tagged routed interfaces, LLDP is not supported.
- On SRX210 devices, the DOCSIS Mini-PIM delivers speeds up to a maximum of 100 Mbps throughput in each direction.
- On SRX550 and SRX650 devices, the aggregate Ethernet (ae) interface with XE member interface cannot be configured with family Ethernet switching.
- On all branch SRX Series and J Series devices, the Q-in-Q support on a Layer 3 interface has the following limitations:
  - Double tagging is not supported on redundant Ethernet (reth) and aggregate Ethernet (ae) interfaces.
  - Multitopology routing is not supported in flow mode and in chassis clusters.
  - Dual tagged frames are not supported on encapsulations (such as CCC, TCC, VPLS, and PPPoE).
  - On Layer 3 logical interfaces, input-vlan-map, output-vlan-map, inner-range, and inner-list are not applicable
  - Only TPIDS with 0x8100 are supported and the maximum number of tags is 2.
  - Dual tagged frames are accepted only for logical interfaces with IPV4 and IPV6 families.
- On SRX650 devices, Link Layer Discovery Protocol (LLDP) is not supported on the base ports of the device and on the 2-Port 10 Gigabit Ethernet XPIM.
- On SRX100, SRX110, SRX210, SRX220, SRX240, and SRX550 devices, Link Aggregation Control Protocol (LACP) is not supported on the 1-Port Gigabit Ethernet Small Form-Factor Pluggable (SFP) Mini-PIM.
- On all branch SRX Series devices, IKEv2 does not include support for:
  - Policy-based tunnels
  - Dial-up tunnels
  - Network Address Translation-Traversal (NAT-T)
  - VPN monitoring
  - Next-Hop Tunnel Binding (NHTB) for st0—Reusing the same tunnel interface for multiple tunnels
  - Extensible Authentication Protocol (EAP)
  - IPv6
  - Multiple child SAs for the same traffic selectors for each QoS value

- Proposal enhancement features
- Reuse of Diffie-Hellman (DH) exponentials
- Configuration payloads
- IP Payload Compression Protocol (IPComp)
- Dynamic Endpoint (DEP)

Intrusion Detection and Prevention (IDP)

- On all branch SRX Series devices, from Junos OS Release 11.2 and later, the IDP security package is based on the Berkeley database. Hence, when the Junos OS image is upgraded from Junos OS Release 11.1 or earlier to Junos OS 11.2 or later, a migration of IDP security package files needs to be performed. This is done automatically on upgrade when the IDP daemon comes up. Similarly, when the image is downgraded, a migration (secDb install) is automatically performed when the IDP daemon comes up, and previously installed database files are deleted.

  However, migration is dependent on the XML files for the installed database present on the device. For first-time installation, completely updated XML files are required. If the last update on the device was an incremental update, migration might fail. In such a case, you have to manually download and install the IDP security package using the **download** or **install** CLI command before using the IDP configuration with predefined attacks or groups.

  As a workaround, use the following CLI commands to manually download the individual components of the security package from the Juniper Security Engineering portal and install the full update:

  - **request security idp security-package download full-update**
  - **request security idp security-package install**

- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, the **request services application-identification uninstall** command will uninstall all predefined signatures.
- On all branch SRX Series devices, IDP does not allow header checks for nonpacket contexts.
- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, the maximum supported number of entries in the ASC table is 100,000 entries. Because the user land buffer has a fixed size of 1 MB as a limitation, the table displays a maximum of 38,837 cache entries.
- The maximum number of IDP sessions supported is 16,384 on SRX210 devices, 32,768 on SRX240 devices, and 131,072 on SRX650 devices.
- On all branch SRX Series devices, all IDP policy templates are supported except All Attacks. There is a 100 MB policy size limit for integrated mode and a 150 MB policy size limit for dedicated mode. The current supported IDP policy templates are dynamic based on the attack signatures added. Therefore, be aware that supported templates might eventually grow past the policy size limit.

On all branch SRX Series devices, the following IDP policies are supported:

  - DMZ_Services
  - DNS_Service
  - File_Server
  - Getting_Started
  - IDP_Default
  - Recommended
  - Web_Server

- On all branch SRX Series devices, IDP deployed in both active/active and active/passive chassis clusters has the following limitations:
  - No inspection of sessions that failover or failback.
  - The IP action table is not synchronized across nodes.
  - The Routing Engine on the secondary node might not be able to reach networks that are reachable only through a Packet Forwarding Engine.
  - The SSL session ID cache is not synchronized across nodes. If an SSL session reuses a session ID and it happens to be processed on a node other than the one on which the session ID is cached, the SSL session cannot be decrypted and will be bypassed for IDP inspection.
- On all branch SRX Series devices, IDP deployed in active/active chassis clusters has a limitation that for time-binding scope source traffic, if attacks from a source (with more than one destination) have active sessions distributed across nodes, then the attack might not be detected because time-binding counting has a local-node-only view. Detecting this sort of attack requires an RTO synchronization of the time-binding state that is not currently supported.

  NOTE: **On SRX100 devices, IDP chassis cluster is supported in active/backup mode.**

- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, the IDP policies for each user logical system are compiled together and stored on the data plane memory. To estimate adequate data plane memory for a configuration, consider these two factors:
  - IDP policies applied to each user logical system are considered unique instances because the ID and zones for each user logical system are different. Estimates need to take into account the combined memory requirements for all user logical systems.
  - As the application database increases, compiled policies will require more memory. Memory usage should be kept below the available data plane memory to accommodate increase in database size.

Layer 2 Transparent Mode

- DHCP server propagation is not supported in Layer 2 transparent mode.

License

- When you have Junos OS Release 12.1X45 or later with advanced license installed, if you downgrade to Junos OS Release 12.1X44 and delete the license, upgrading back to Junos OS Release 12.1X45 might lead to a decrease in the session capacity.

IPv6

- NSM—Consult the Network and Security Manager (NSM) release notes for version compatibility, required schema updates, platform limitations, and other specific details regarding NSM support for IPv6 addressing on SRX Series and J Series devices.

J-Web

- SRX Series and J Series browser compatibility
  - To access the J-Web interface, your management device requires the following software:
    - Supported browsers—Microsoft Internet Explorer version 7.0 or Mozilla Firefox version 3.0
    - Language support—English-version browsers
    - Supported OS—Microsoft Windows XP Service Pack 3
  - If the device is running the worldwide version of the Junos OS and you are using the Microsoft Internet Explorer Web browser, you must disable the Use SSL 3.0 option in the Web browser to access the device.
  - To use the Chassis View, a recent version of Adobe Flash that supports ActionScript and AJAX (Version 9) must be installed. Also note that the Chassis View is displayed by default on the Dashboard page. You can enable or disable it using options in the Dashboard Preference dialog box, but clearing cookies in Internet Explorer also causes the Chassis View to be displayed.
- On all branch SRX Series devices, in the J-Web interface, there is no support for changing the T1 interface to an E1 interface or vice versa. As a workaround, use the CLI to convert from T1 to E1 and vice versa.
- On all branch SRX Series and J Series devices, users cannot differentiate between Active and Inactive configurations on the System Identity, Management Access, User Management, and Date & Time pages.
- On SRX210 devices, there is no maximum length when the user commits the hostname in CLI mode; however, only 58 characters, maximum, are displayed in the J-Web System Identification panel.
- On all J Series devices, some J-Web pages for new features (for example, the Quick Configuration page for the switching features on J Series devices) display content in

one or more modal pop-up windows. In the modal pop-up windows, you can interact only with the content in the window and not with the rest of the J-Web page. As a result, online Help is not available when modal pop-up windows are displayed. You can access the online Help for a feature only by clicking the **Help** button on a J-Web page.

- On all branch SRX Series devices, you cannot use J-Web to configure a VLAN interface for an IKE gateway. VLAN interfaces are not currently supported for use as IKE external interfaces.

The PPPoE wizard has the following limitations:

- While you use the load and save functionality, the port details are not saved in the client file.
- The Non Wizard connection option cannot be edited or deleted through the wizard. Use the CLI to edit or delete the connections.
- The PPPoE wizard cannot be launched if the backend file is corrupted.
- The PPPoE wizard cannot be loaded from the client file if non-wizard connections share the same units.
- The PPPoE wizard cannot load the saved file from one platform to another platform.
- There is no backward compatibility between PPPoE wizard Phase 2 to PPPoE wizard Phase 1. As a result, the PPPoE connection from Phase 2 will not be shown in Phase 1 when you downgrade to an earlier release.

The New Setup wizard has the following limitations:

- The Existing Edit mode might not work as expected if you previously configured the device manually, without using the wizard.
- Edit mode might overwrite outside configurations such as Custom Application, Policy Name, and zone inbound services.
- In create new mode, when you commit your configuration changes, your changes will overwrite the existing configuration.
- VPN and NAT wizards are not compatible with the New Setup wizard; therefore the VPN or NAT wizard configuration will not be reflected in the New Setup wizard or vice versa.
- By default, 2 minutes are required to commit a configuration using the New Setup wizard.
- On SRX650 devices, the default mode configures only the ge-0/0/1 interface under the internal zone.
- You might encounter usability issues if you use Internet Explorer version 7 or 8 to launch the New Setup wizard.
- If you refresh your browser after you download the license, the factory mode wizard is not available.

- When you commit the configuration, the underlying Web management interface changes, and you do not receive a response about the commit status.
- Web server ports 80 (HTTP) and 443 (HTTPS) on the DMZ or internal zone are overshadowed if Web management is enabled on the Internet zone not configured for destination NAT. As a workaround, change the Web server port numbers for HTTP and HTTPS by editing the recommended policies on the Security policies page.
- Images, buttons, and spinner (applying configuration) on wizard screen does not render or appear for the first time when browser cache is cleared.

Network Address Translation (NAT)

- Maximum capacities for source pools and IP addresses have been extended on SRX650 devices, as follows:

Devices	Source NAT Pools	PAT Maximum Address Capacity	Pat Port Number	Source NAT rules number
SRX650	1024	1024	64M	1024

  Increasing the capacity of source NAT pools consumes memory needed for port allocation. When source NAT pool and IP address limits are reached, port ranges should be reassigned. That is, the number of ports for each IP address should be decreased when the number of IP addresses and source NAT pools is increased. This ensures NAT does not consume too much memory. Use the **port-range** statement in configuration mode in the CLI to assign a new port range or the **pool-default-port-range** statement to override the specified default.

  Configuring port overloading should also be done carefully when source NAT pools are increased.

  For source pool with port address translation (PAT) in range (64,510 through 65,533), two ports are allocated at one time for RTP/RTCP applications, such as SIP, H.323, and RTSP. In these scenarios, each IP address supports PAT, occupying 2048 ports (64,512 through 65,535) for Application Layer Gateway (ALG) module use.

- **NAT rule capacity change**—To support the use of large scale NAT (LSN) at the edge of the carrier network, the device wide NAT rule capacity has been changed.

  The number of destination and static NAT rules has been incremented as shown in Table 5 on page 46. The limitation on the number of destination-rule-set and static-rule-set has been increased.

  Table 5 on page 46 provides the requirements per device to increase the configuration limitation as well as to scale the capacity for each device.

Table 5: Number of Rules on SRX Series and J Series Devices

NAT Rule Type	SRX100	SRX210	SRX240	SRX650	J Series
Source NAT rule	512	512	1024	1024	512

Table 5: Number of Rules on SRX Series and J Series Devices *(continued)*

NAT Rule Type	SRX100	SRX210	SRX240	SRX650	J Series
Destination NAT rule	512	512	1024	1024	512
Static NAT rule	512	512	1024	6144	512

The restriction on the number of rules per rule set has been increased so that there is only a device wide limitation on how many rules a device can support. This restriction is provided to help you better plan and configure the NAT rules for the device.

Power over Ethernet (PoE)

- On SRX210-PoE devices, SDK packages might not work.

Security Policies

- J Series devices do not support the authentication order **password radius** or **password ldap** in the **edit access profile** ***profile-name*** **authentication-order** command. Instead, use **order radius password** or **ldap password**.
- On all branch SRX Series and J Series devices, the limitation on the number of addresses in an address-set has been increased. The number of addresses in an address-set now depends on the device and is equal to the number of addresses supported by the policy.

Table 6: Number of Addresses in an address-set on SRX Series and J Series Devices

Device	address-set
Default	1024
SRX100 High Memory	1024
SRX100 Low Memory	512
SRX210 High Memory	1024
SRX210 Low Memory	512
SRX240 High Memory	1024
SRX240 Low Memory	512
SRX650	1024
J Series	1024

Simple Network Management Protocol (SNMP)

- On all J Series devices, the SNMP NAT related MIB is not supported.

Switching

- **Layer 2 transparent mode support**—On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, the following features are not supported for Layer 2 transparent mode:
  - Gateway-Address Resolution Protocol (G-ARP) on the Layer 2 interface
  - Spanning Tree Protocol (STP)
  - IP address monitoring on any interface
  - Transit traffic through integrated routing and bridging (IRB)
  - IRB interface in a routing instance
  - Chassis clustering
  - IRB interface handling of Layer 3 traffic

  NOTE: **The IRB interface is a pseudointerface and does not belong to the reth interface and redundancy group.**

- On SRX100, SRX210, SRX240, and SRX650 devices, change of authorization is not supported with 802.1x.
- On SRX100, SRX210, SRX240, and SRX650 devices, on the routed VLAN interface, the following features are not supported:
  - IPv6 (family inet6)
  - IS-IS (family ISO)
  - Class of service
  - Encapsulations (Ether circuit cross-connect [CCC], VLAN CCC, VPLS, PPPoE, and so on) on VLAN interfaces
  - Connectionless network Service (CLNS)
  - Protocol Independent Multicast (PIM)
  - Distance Vector Multicast Routing Protocol (DVMRP)
  - VLAN interface MAC change
  - Gateway-Address Resolution Protocol (G-ARP)
  - Change VLAN-Id for VLAN interface

Unified Threat Management (UTM)

- On all J Series devices, UTM requires 1 GB of memory. If your J2320, J2350, or J4350 device has only 512 MB of memory, you must upgrade the memory to 1 GB to run UTM.
- The quarantine action is supported only for UTM Enhanced Web Filtering or Juniper-Enhanced type of Web Filtering.

Upgrade and Downgrade

- On all J Series devices, the Junos OS upgrade might fail due to insufficient disk space if the CompactFlash is smaller than 1 GB in size. We recommend using a 1GB compact flash for Junos OS Release 10.0 and later.
- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, when you connect a client running Junos Pulse 1.0 to an SRX Series device that is a running a later version of Junos Pulse, the client will not be upgraded automatically to the later version. You must uninstall Junos Pulse 1.0 from the client and then download the later version of Junos Pulse from the SRX Series device.

USB

- On all branch SRX Series devices, frequent plug and play of USB keys is not supported. You must wait for the device node creation before removing the USB key.

Virtual Private Network (VPN)

The IPv6 IPsec implementation has the following limitations:

- Devices with IPv6 addressing do not perform fragmentation. IPv6 hosts should either perform path maximum transmission unit (PMTU) discovery or send packets smaller than the IPv6 minimum MTU size of 1280 bytes.
- Because IPv6 addresses are 128 bits long compared to IPv4 addresses, which are 32-bits long, IPv6 IPsec packet processing requires more resources. Therefore, a small performance degradation is observed.
- IPv6 uses more memory to set up the IPsec tunnel. Therefore, the IPsec IPv4 tunnel scalability numbers might drop.
- The addition of IPv6 capability might cause a drop in the IPsec IPv4-in-IPv4 tunnel throughput performance.
- The IPv6 IPsec VPN does not support the following functions:
  - 4in6 and 6in4 policy-based site-to-site VPN, IKE
  - 4in6 and 6in4 route-based site-to-site VPN, IKE
  - 4in6 and 6in4 policy-based site-to-site VPN, Manual Key
  - 4in6 and 6in4 route-based site-to-site VPN, Manual Key
  - 4in4, 6in6, 4in6, and 6in4 policy-based dial-up VPN, IKE
  - 4in4, 6in6, 4in6, and 6in4 policy-based dial-up VPN, Manual Key

  - Remote Access—XAuth, config mode, and shared IKE identity with mandatory XAuth
  - IKE authentication—public key infrastructure/digital signature algorithm (PKI/DSA)
  - IKE peer type—Dynamic IP
  - Chassis cluster for basic VPN features
  - IKE authentication—PKI/RSA
  - Network Address Translation-Traversal (NAT-T)
  - VPN monitoring
  - Hub-and-spoke VPNs
  - Next Hop Tunnel Binding Table (NHTB)
  - Dead Peer Detection (DPD)
  - Simple Network Management Protocol (SNMP) for IPsec VPN MIBs
  - Chassis cluster for advanced VPN features
  - IPv6 link-local address

- On all branch SRX Series devices, when you enable VPN, overlapping of the IP addresses across virtual routers is supported with following limitations:
  - An IKE external interface address cannot overlap with any other virtual router.
  - An internal/trust interface address can overlap across virtual routers.
  - An st0 interface address cannot overlap in route-based VPN in point-to-multipoint tunnels such as NHTB.
  - An st0 interface address can overlap in route-based VPN in point-to-point tunnels.

SRX100, SRX210, and SRX240 devices have the following limitations:

- The IKE configuration for the Junos Pulse client does not support the hexadecimal preshared key.
- The Junos Pulse client IPsec does not support the Authentication Header (AH) protocol and the Encapsulating Security Payload (ESP) protocol with NULL authentication.
- When you log in through the Web browser (instead of logging in through the Junos Pulse client) and a new client is available, you are prompted for a client upgrade even if the **force-upgrade** option is configured. Conversely, if you log in using the Junos Pulse client with the **force-upgrade** option configured, the client upgrade occurs automatically (without a prompt).
- On all branch SRX Series devices, when you download the Pulse client using the Mozilla browser, the “Launching the VPN Client” page is displayed when Junos Pulse is still downloading. However, when you download the Pulse client using Internet Explorer,

"Launching the VPN Client" page is displayed after Junos Pulse has been downloaded and installed.

- On SRX100, SRX210, SRX240, and SRX650 devices, while configuring dynamic VPN using the Junos Pulse client, when you select the authentication-algorithm as sha-256 in the IKE proposal, the IPsec session might not get established.

Unsupported CLI for Branch SRX Series Services Gateways and J Series Services Routers

Dynamic Profiles Hierarchy

- On all branch SRX Series and all J Series devices, the following Firewall hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set dynamic-profiles interfaces interface container-options container-type aps
 fast-aps-switch

set dynamic-profiles interfaces interface fastether-options no-source-filtering

set dynamic-profiles interfaces interface fastether-options source-filtering

set dynamic-profiles interfaces interface services-options close-timeout

set dynamic-profiles interfaces interface services-options fragment-limit

set dynamic-profiles interfaces interface services-options reassembly-timeout

set dynamic-profiles interfaces interface sonet-options aps fast-aps-switch

set dynamic-profiles interfaces interface-range container-options container-type
 aps fast-aps-switch

set dynamic-profiles interfaces interface-range fastether-options
no-source-filtering

set dynamic-profiles interfaces interface-range fastether-options
source-filtering

set dynamic-profiles interfaces interface-range services-options close-timeout

set dynamic-profiles interfaces interface-range services-options fragment-limit

set dynamic-profiles interfaces interface-range services-options
reassembly-timeout

set dynamic-profiles interfaces interface-range sonet-options aps fast-aps-switch

set dynamic-profiles profile-variable-set junos-action-profile

set dynamic-profiles profile-variable-set junos-ccm-interval

set dynamic-profiles profile-variable-set junos-loss-threshold

set dynamic-profiles profile-variable-set junos-ma-name-format

set dynamic-profiles profile-variable-set junos-md-name-format
```

Interfaces Hierarchy

- On all branch SRX Series and all J Series devices, the following interface hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set interfaces interface container-options container-type aps fast-aps-switch
set interfaces interface fastether-options no-source-filtering

set interfaces interface fastether-options source-filtering

set interfaces interface services-options close-timeout

set interfaces interface services-options fragment-limit

set interfaces interface services-options reassembly-timeout

set interfaces interface sonet-options aps fast-aps-switch

set interfaces interface-range container-options container-type aps
fast-aps-switch

set interfaces interface-range fastether-options no-source-filtering

set interfaces interface-range fastether-options source-filtering

set interfaces interface-range services-options close-timeout

set interfaces interface-range services-options fragment-limit

set interfaces interface-range services-options reassembly-timeout

set interfaces interface-range sonet-options aps fast-aps-switch
```

Logical Systems Hierarchy

- On all branch SRX Series and all J Series devices, the following interface hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set logical-systems protocols pim dense-groups dynamic-reject

set logical-systems protocols pim dense-groups pim-dense-group-type

set logical-systems protocols pim dense-groups pim-dense-group-type announce

set logical-systems protocols pim dense-groups pim-dense-group-type name

set logical-systems protocols pim dense-groups pim-dense-group-type reject

set logical-systems routing-instances instance protocols l2vpn associate-profile

set logical-systems routing-instances instance protocols l2vpn associate-profile
 profile-name

set logical-systems routing-instances instance protocols l2vpn associate-profile
 profile-variable-set

set logical-systems routing-instances instance protocols l2vpn mesh-group
associate-profile

set logical-systems routing-instances instance protocols l2vpn mesh-group
associate-profile profile-name

set logical-systems routing-instances instance protocols l2vpn mesh-group
associate-profile profilevariable-set

set logical-systems routing-instances instance protocols l2vpn mesh-group
mac-flush

set logical-systems routing-instances instance protocols l2vpn mesh-group
mac-flush any-interface

set logical-systems routing-instances instance protocols l2vpn mesh-group
mac-flush any-spoke

set logical-systems routing-instances instance protocols l2vpn mesh-group
mac-flush propagate
```

```
set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor associate-profile

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor associate-profile profile-name

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor associate-profile profile-variable-set

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor backup-neighbor

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor backup-neighbor community

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor backup-neighbor name

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor backup-neighbor psn-tunnel-endpoint

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor backup-neighbor standby

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor backup-neighbor static

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor backup-neighbor static incoming-label

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor backup-neighbor static outgoing-label

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor community

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor connection-protection

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor encapsulation-type

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor ignoreencapsulation-mismatch

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor name

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor pseudowirestatus-tlv

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor psn-tunnelendpoint

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor revert-time

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor static

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor static
incoming-label

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor static
outgoing-label
```

```
set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor switchover-delay

set logical-systems routing-instances instance protocols l2vpn mesh-group
route-distinguisher

set logical-systems routing-instances instance protocols l2vpn mesh-group
route-distinguisher rd-type

set logical-systems routing-instances instance protocols l2vpn mesh-group
vrf-export

set logical-systems routing-instances instance protocols l2vpn mesh-group
vrf-import

set logical-systems routing-instances instance protocols l2vpn mesh-group
vrf-target

set logical-systems routing-instances instance protocols l2vpn mesh-group
vrf-target community

set logical-systems routing-instances instance protocols l2vpn mesh-group
vrf-target export

set logical-systems routing-instances instance protocols l2vpn mesh-group
vrf-target import

set logical-systems routing-instances instance protocols l2vpn neighbor
associate-profile

set logical-systems routing-instances instance protocols l2vpn neighbor
associate-profile
profile-name

set logical-systems routing-instances instance protocols l2vpn neighbor
associate-profile profilevariable-set

set logical-systems routing-instances instance protocols pim dense-groups
dynamic-reject

set logical-systems routing-instances instance protocols pim dense-groups
pim-dense-group-type

set logical-systems routing-instances instance protocols pim dense-groups
pim-dense-group-type announce

set logical-systems routing-instances instance protocols pim dense-groups
pim-dense-group-type
name

set logical-systems routing-instances instance protocols pim dense-groups
pim-dense-group-type reject

set logical-systems routing-instances instance protocols vpls associate-profile

set logical-systems routing-instances instance protocols vpls associate-profile
 profile-name

set logical-systems routing-instances instance protocols vpls associate-profile
 profile-variable-set

set logical-systems routing-instances instance protocols vpls mesh-group
associate-profile

set logical-systems routing-instances instance protocols vpls mesh-group
associate-profile
profile-name

set logical-systems routing-instances instance protocols vpls mesh-group
associate-profile profilevariable-set
```

```
set logical-systems routing-instances instance protocols vpls mesh-group
mac-flush

set logical-systems routing-instances instance protocols vpls mesh-group
mac-flush any-interface

set logical-systems routing-instances instance protocols vpls mesh-group
mac-flush any-spoke

set logical-systems routing-instances instance protocols vpls mesh-group
mac-flush propagate

set logical-systems routing-instances instance protocols vpls mesh-group neighbor

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 associate-profile

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 associate-profile profile-name

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 associate-profile profile-variable-set

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 backup-neighbor

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 backup-neighbor community

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 backup-neighbor name

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 backup-neighbor psn-tunnel-endpoint

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 backup-neighbor standby

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 backup-neighbor static

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 backup-neighbor static incoming-label

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 backup-neighbor static outgoing-label

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 community

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 connection-protection

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 encapsulation-type

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 ignore-encapsulation-mismatch

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 name

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 pseudowirestatus-tlv

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 psn-tunnelendpoint

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 revert-time
```

```
set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 static

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 static
incoming-label

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 static
outgoing-label

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 switchover-delay

set logical-systems routing-instances instance protocols vpls mesh-group
route-distinguisher

set logical-systems routing-instances instance protocols vpls mesh-group
route-distinguisher rd-type

set logical-systems routing-instances instance protocols vpls mesh-group
vrf-export

set logical-systems routing-instances instance protocols vpls mesh-group
vrf-import

set logical-systems routing-instances instance protocols vpls mesh-group
vrf-target

set logical-systems routing-instances instance protocols vpls mesh-group
vrf-target community

set logical-systems routing-instances instance protocols vpls mesh-group
vrf-target export

set logical-systems routing-instances instance protocols vpls mesh-group
vrf-target import

set logical-systems routing-instances instance protocols vpls neighbor
associate-profile

set logical-systems routing-instances instance protocols vpls neighbor
associate-profile profile-name

set logical-systems routing-instances instance protocols vpls neighbor
associate-profile profile-variable-set

set logical-systems routing-instances instance system services dhcp-local-server
 duplicate-clients-on-interface

set logical-systems routing-instances instance system services dhcp-local-server
 forward-snooped-clients

set logical-systems routing-instances instance system services dhcp-local-server
 forward-snooped-clients all-interfaces

set logical-systems routing-instances instance system services dhcp-local-server
 forward-snooped-clients configured-interfaces

set logical-systems routing-instances instance system services dhcp-local-server
 forward-snooped-clients non-configured-interfaces

set logical-systems system services dhcp-local-server
duplicate-clients-on-interface

set logical-systems system services dhcp-local-server forward-snooped-clients

set logical-systems system services dhcp-local-server forward-snooped-clients
all-interfaces
```

```
set logical-systems system services dhcp-local-server forward-snooped-clients
configured-interfaces
```

```
set logical-systems system services dhcp-local-server forward-snooped-clients
non-configured-interfaces
```

Protocols Hierarchy

- On all branch SRX Series and all J Series devices, the following CLI commands are not supported. However, if you enter these commands in the CLI editor, they will appear to succeed and will not display an error message.

```
set protocols pim dense-groups dynamic-reject

set protocols pim dense-groups pim-dense-group-type

set protocols pim dense-groups pim-dense-group-type announce

set protocols pim dense-groups pim-dense-group-type name

set protocols pim dense-groups pim-dense-group-type reject
```

Routing Hierarchy

- On all branch SRX Series and all J Series devices, the following routing hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set routing-instances instance protocols l2vpn associate-profile

set routing-instances instance protocols l2vpn associate-profile profile-name

set routing-instances instance protocols l2vpn associate-profile
profile-variable-set

set routing-instances instance protocols l2vpn mesh-group associate-profile

set routing-instances instance protocols l2vpn mesh-group associate-profile
profile-name

set routing-instances instance protocols l2vpn mesh-group associate-profile
profile-variable-set

set routing-instances instance protocols l2vpn mesh-group mac-flush

set routing-instances instance protocols l2vpn mesh-group mac-flush any-interface

set routing-instances instance protocols l2vpn mesh-group mac-flush any-spoke

set routing-instances instance protocols l2vpn mesh-group mac-flush propagate

set routing-instances instance protocols l2vpn mesh-group neighbor

set routing-instances instance protocols l2vpn mesh-group neighbor
associate-profile

set routing-instances instance protocols l2vpn mesh-group neighbor
associate-profile profile-name

set routing-instances instance protocols l2vpn mesh-group neighbor
associate-profile profile-variable-set

sset routing-instances instance protocols l2vpn mesh-group neighbor
backup-neighbor

set routing-instances instance protocols l2vpn mesh-group neighbor
backup-neighbor community
```

```
set routing-instances instance protocols l2vpn mesh-group neighbor
backup-neighbor name

set routing-instances instance protocols l2vpn mesh-group neighbor
backup-neighbor psn-tunnel-endpoint

set routing-instances instance protocols l2vpn mesh-group neighbor
backup-neighbor standby

set routing-instances instance protocols l2vpn mesh-group neighbor
backup-neighbor static

set routing-instances instance protocols l2vpn mesh-group neighbor
backup-neighbor static incoming-label

set routing-instances instance protocols l2vpn mesh-group neighbor
backup-neighbor static outgoing-label

set routing-instances instance protocols l2vpn mesh-group neighbor community

set routing-instances instance protocols l2vpn mesh-group neighbor
connection-protection

set routing-instances instance protocols l2vpn mesh-group neighbor
encapsulation-type

set routing-instances instance protocols l2vpn mesh-group neighbor
ignore-encapsulation-mismatch

set routing-instances instance protocols l2vpn mesh-group neighbor name

set routing-instances instance protocols l2vpn mesh-group neighbor
pseudowire-status-tlv

set routing-instances instance protocols l2vpn mesh-group neighbor
psn-tunnel-endpoint

set routing-instances instance protocols l2vpn mesh-group neighbor revert-time

set routing-instances instance protocols l2vpn mesh-group neighbor static

set routing-instances instance protocols l2vpn mesh-group neighbor static
incoming-label

set routing-instances instance protocols l2vpn mesh-group neighbor static
outgoing-label

set routing-instances instance protocols l2vpn mesh-group neighbor
switchover-delay

set routing-instances instance protocols l2vpn mesh-group route-distinguisher

set routing-instances instance protocols l2vpn mesh-group route-distinguisher
rd-type

set routing-instances instance protocols l2vpn mesh-group vrf-export

set routing-instances instance protocols l2vpn mesh-group vrf-import

set routing-instances instance protocols l2vpn mesh-group vrf-target

set routing-instances instance protocols l2vpn mesh-group vrf-target community

set routing-instances instance protocols l2vpn mesh-group vrf-target export

set routing-instances instance protocols l2vpn mesh-group vrf-target import

set routing-instances instance protocols l2vpn neighbor associate-profile

set routing-instances instance protocols l2vpn neighbor associate-profile
profile-name
```

```
set routing-instances instance protocols l2vpn neighbor associate-profile
profile-variable-set

set routing-instances instance protocols pim dense-groups dynamic-reject

set routing-instances instance protocols pim dense-groups pim-dense-group-type

set routing-instances instance protocols pim dense-groups pim-dense-group-type
 announce

set routing-instances instance protocols pim dense-groups pim-dense-group-type
 name

set routing-instances instance protocols pim dense-groups pim-dense-group-type
 reject

set routing-instances instance protocols vpls associate-profile

set routing-instances instance protocols vpls associate-profile profile-name

set routing-instances instance protocols vpls associate-profile
profile-variable-set

set routing-instances instance protocols vpls mesh-group associate-profile

set routing-instances instance protocols vpls mesh-group associate-profile
profile-name

set routing-instances instance protocols vpls mesh-group associate-profile
profile-variable-set

set routing-instances instance protocols vpls mesh-group mac-flush

set routing-instances instance protocols vpls mesh-group mac-flush any-interface

set routing-instances instance protocols vpls mesh-group mac-flush any-spoke

set routing-instances instance protocols vpls mesh-group mac-flush propagate

set routing-instances instance protocols vpls mesh-group neighbor

set routing-instances instance protocols vpls mesh-group neighbor
associate-profile

set routing-instances instance protocols vpls mesh-group neighbor
associate-profile profile-name

set routing-instances instance protocols vpls mesh-group neighbor
associate-profile profile-variable-set

set routing-instances instance protocols vpls mesh-group neighbor backup-neighbor

set routing-instances instance protocols vpls mesh-group neighbor backup-neighbor
 community

set routing-instances instance protocols vpls mesh-group neighbor backup-neighbor
 name

set routing-instances instance protocols vpls mesh-group neighbor backup-neighbor
 psn-tunnel-endpoint

set routing-instances instance protocols vpls mesh-group neighbor backup-neighbor
 standby

set routing-instances instance protocols vpls mesh-group neighbor backup-neighbor
 static

set routing-instances instance protocols vpls mesh-group neighbor backup-neighbor
 static incoming-label

set routing-instances instance protocols vpls mesh-group neighbor backup-neighbor
 static outgoing-label
```

```
set routing-instances instance protocols vpls mesh-group neighbor community

set routing-instances instance protocols vpls mesh-group neighbor connection-protection

set routing-instances instance protocols vpls mesh-group neighbor encapsulation-type

set routing-instances instance protocols vpls mesh-group neighbor ignore-encapsulation-mismatch

set routing-instances instance protocols vpls mesh-group neighbor name

set routing-instances instance protocols vpls mesh-group neighbor pseudowire-status-tlv

set routing-instances instance protocols vpls mesh-group neighbor psn-tunnel-endpoint

set routing-instances instance protocols vpls mesh-group neighbor revert-time

set routing-instances instance protocols vpls mesh-group neighbor static

set routing-instances instance protocols vpls mesh-group neighbor static incoming-label

set routing-instances instance protocols vpls mesh-group neighbor static outgoing-label

set routing-instances instance protocols vpls mesh-group neighbor switchover-delay

set routing-instances instance protocols vpls mesh-group route-distinguisher

set routing-instances instance protocols vpls mesh-group route-distinguisher rd-type

set routing-instances instance protocols vpls mesh-group vrf-export

set routing-instances instance protocols vpls mesh-group vrf-import

set routing-instances instance protocols vpls mesh-group vrf-target

set routing-instances instance protocols vpls mesh-group vrf-target community

set routing-instances instance protocols vpls mesh-group vrf-target export

set routing-instances instance protocols vpls mesh-group vrf-target import

set routing-instances instance protocols vpls neighbor associate-profile

set routing-instances instance protocols vpls neighbor associate-profile profile-name

set routing-instances instance protocols vpls neighbor associate-profile profile-variable-set

set routing-instances instance system services dhcp-local-server duplicate-clients-on-interface

set routing-instances instance system services dhcp-local-server forward-snooped-clients

set routing-instances instance system services dhcp-local-server forward-snooped-clients all-interfaces

set routing-instances instance system services dhcp-local-server forward-snooped-clients configured-interfaces

set routing-instances instance system services dhcp-local-server forward-snooped-clients non-configured-interfaces
```

Security Hierarchy

- On all branch SRX Series and all J Series devices, the following services hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

  ```
  set security idp sensor-configuration application-identification
  application-system-cache
  ```

  ```
  set security idp sensor-configuration application-identification
  application-system-cache-timeout
  ```

  ```
  set security idp sensor-configuration application-identification disable
  ```

  ```
  set security idp sensor-configuration application-identification max-sessions
  ```

  ```
  set security idp sensor-configuration application-identification
  no-application-system-cache
  ```

System Hierarchy

- On all branch SRX Series and all J Series devices, the following system hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

  ```
  set system services dhcp-local-server duplicate-clients-on-interface
  ```

  ```
  set system services dhcp-local-server forward-snooped-clients
  ```

  ```
  set system services dhcp-local-server forward-snooped-clients all-interfaces
  ```

  ```
  set system services dhcp-local-server forward-snooped-clients
  configured-interfaces
  ```

  ```
  set system services dhcp-local-server forward-snooped-clients
  non-configured-interfaces
  ```

Related Documentation

- New Features in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 6
- Changes in Default Behavior and Syntax in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 25
- Outstanding Issues in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 62
- Resolved Issues in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 65
- Errata and Changes in Documentation for Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 80
- Upgrade and Downgrade Instructions for Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 90

Outstanding Issues in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers

The following problems currently exist in Juniper Networks branch SRX Series Services Gateways and J Series Services Routers. The identifier following the description is the tracking number in the Juniper Networks Problem Report (PR) tracking system.

For the latest, most complete information about outstanding and resolved issues with the Junos OS software, see the Juniper Networks online software defect search application at http://www.juniper.net/prsearch.

NOTE: If there is no device listed in the PR description, then that issue applies to all branch SRX Series and J Series devices.

Outstanding Issues in Junos OS Release 12.1X44-D20 for Branch SRX Series Services Gateways and J Series Services Routers

Authentication

- On all branch SRX Series devices configured with firewall authentication, if a user has already been authenticated, and then a subsequent user initiates authentication using the same IP address as the first user, the subsequent user inherites the first authenticated user’s **Access time remaining** value. [PR843591]

Certificate Authority (CA)

- When the PKI certificate expires at a later date, the output of the **show security pki ca-certificate detail** command incorrectly shows the “Not after” field in the Validity date as “Not determined”. [PR878036]

Chassis Cluster

- On SRX210, SRX220, and SRX240 devices, the maximum MTU on the SRX-MP-1SFP-GE Mini-PIM interface is 9010. If the Mini-PIM interface is configured as a chassis cluster fabric interface, the fabric interface automatically sets a MTU to 9014 to support jumbo frames. So, the MTU setting fails in the Mini-PIM interface that is configured as a chassis cluster fabric interface, and the Mini-PIM interface stays in the default MTU setting (1514). As a result, packets that are larger than 1514-byte frames are dropped because the chassis cluster fabric interface does not support fragmentation.

  NOTE: For chassis clusters made up of SRX210, SRX220, or SRX240 devices, the SFP interfaces on Mini-PIMs cannot be used as the fabric link.

  [PR865975]

- On J Series devices in a chassis cluster, when you manually trigger the restart forwarding on the primary node, the secondary node might go to disabled status and cannot be recovered back to normal state without rebooting both the nodes. [PR895614]

Command-Line Interface (CLI)

- On SRX650 devices, when you execute the **show security nat static rule all** command continuously, the following message is displayed:

  kern.maxfiles limit exceeded by uid 0

  [PR721715]

- On SRX210 devices, the **set interfaces dl0 unit 0 dialer-options watch-list 0.0.0.0/0** command fails when you try to configure 0.0.0.0/0 in dialer-options watch-list. [PR841371]

Dynamic Host Configuration Protocol (DHCP)

- The DHCPv6 server application might not process DHCPv6 packets properly when Option 18 (DHCPv6 Interface-ID) and Option 37 (DHCPv6 Relay Agent Remote-ID) are received in the same packet. [PR774631]

Flow and Processing

- After enabling IPv6 in flow mode, IPv6 routes are not active. [PR824563]

Infrastructure

- On SRX240 devices, when a nonstandard HTTPS port is set, the Uniform Resource Identifier (URI) is changed to the IP address and port.[PR851741]

Interfaces and Routing

- On J Series devices, E1 LCP links cannot be recovered after BERT tests. [PR600846]
- When the Flexible PIC Concentrator (FPC) is removed or made to go offline, the FPC status does not get detected. [PR818363]
- When reverse path forwarding (RPF) is enabled along with real-time performance monitoring (RPM), the device goes to db prompt and loses the reach ability when you delete some configurations. [PR869528]
- The new configuration of the VDSL profile might not take effect until you restart FPC manually. [PR898775]

Intrusion Detection and Prevention (IDP)

- On all branch SRX Series devices, in the output of the **show services application-identification application-system-cache** command, the “application-system-cache” table for P2P encrypted traffic is incorrectly marked as “Encrypted: No” instead of “Encrypted:Yes”. [PR704023]
- If you configure only custom attacks without installing the IDP security package, the default detector is used. If the default detector version contains the date 110307, the detector is not compatible with the engine and flowd core files are generated. [PR795400]

J-Web

- The AppSecure Settings page might take more time to load the applications when there are many applications to load. In such cases, the following error message might appear:

  The device is taking too long to respond. Please check the connectivity again. [PR728995]

- In J-Web, the maximum flow memory value key **max-flow-mem** is marked as deprecated and hidden. Therefore, the maximum flow memory value cannot be fetched or displayed in J-Web. [PR894787]

Software

- On all branch SRX Series devices, if you enable **Change password every time the user logs out** on the active directory, you cannot change your password. [PR740869]

Switching

- On SRX650 devices in a chassis cluster, when the fabric link is disabled manually using the CLI, the secondary node remains in the secondary mode. As a result, in the active/active mode, the Z-traffic is dropped even when the secondary node is up and the fabric link status is down. [PR839193]

System Logs

- Memory leak is observed with periodic packet management process (ppmd), and the following logs are generated:

  /kernel: Process (1413,ppmd) has exceeded 85% of RLIMIT_DATA: used 115596 KB Max 131072 KB

  As a workaround, reset the ppmd process. [PR747002]

- On all branch SRX Series devices, when the source address is specified for a particular host, eventd core files are generated.

  As a workaround, do not limit the source address to a particular host. [PR769855]

Unified Threat Management (UTM)

- Invalid notification options are displayed in antivirus fallback-block notification. [PR787063]

Related Documentation

- New Features in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 6
- Changes in Default Behavior and Syntax in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 25
- Known Limitations in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 34

Resolved Issues in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers

The following are the issues that have been resolved in Junos OS Release 12.1X44 for Juniper Networks SRX Series Services Gateways. The identifier following the description is the tracking number in the Juniper Networks Problem Report (PR) tracking system.

For the latest, most complete information about outstanding and resolved issues with the Junos OS software, see the Juniper Networks online software defect search application at http://www.juniper.net/prsearch.

NOTE: If there is no device listed in the PR description, then that issue applies to all branch SRX Series and J Series devices.

Resolved Issues in Junos OS Release 12.1X44-D20 for Branch SRX Series Services Gateways

Application Layer Gateway (ALG)

- The TCP proxy module used by the ALG is deficient in handling a TCP stream with large packets. [PR727649]

Chassis Cluster

- During an IP monitoring failover condition, the IP monitoring policy status changes to INIT from FAIL and the interface and route actions are reset to MARKED-DOWN and NOT-APPLIED. [PR729022]
- On devices in a chassis cluster, when Layer 2 Ethernet switching is configured and the created session is related to the Layer 3 VLAN interface (the session's ingress or egress interface), the session is deleted on the primary node when the backup session times out on the backup node. [PR839290]
- On devices in a chassis cluster, during cold synchronization, if the flow sessions are synchronized before the application identification configuration synchronization, then after the backup node is rebooted, the application identification module bypasses the flow sessions and the application names for those sessions are marked as unknown. [PR843742]

- On all branch SRX Series devices, when you use aggregated redundant Ethernet (chassis cluster redundant Ethernet interface with multiple link members per node), traffic loss is observed when the link member fails. [PR858519]
- On devices in a chassis cluster, the security zone is not populated properly on the J-Web interface port configuration page. [PR859200]

Command-Line Interface (CLI)

- The **show interface pp0.x** command triggers memory leakage for interface statistics. [PR854658.]

Dynamic Host Configuration Protocol (DHCP)

- Only the first three options present in the Request option of a DHCPv6 Solicit/Request was correctly populated from the dhcp-attributes specified within a local inet6 pool. [PR741823]

Flow and Processing

- When a large number of logs are archived to a remote site, event core files are generated. [PR771228]
- When you configure the **nas-ip-address** option using the command **system radius-options attributes nas-ip-address** and commit, the **nas-ip-address** is not correctly set unless you reboot the device. [PR786467]
- Destination port information is missing for IPv6 packets when the firewall is in packet mode. [PR805986]
- When a device forwards traffic, flowd core files are generated. [PR831480]
- On devices with increased ALG or proxy traffic, memory leaks in global data plane memory are observed, and traffic (FTP, MSRPC, AppID, and so on) drops. [PR859956]
- If Virtual Router Redundancy Protocol (VRRP) is configured with the preempt option on an aggregated Ethernet link aggregation group (LAG) interface, the device might not send Gateway-Address Resolution Protocol (G-ARP). [PR863549]
- When reverse path forwarding (RPF) is enabled along with real-time performance monitoring (RPM), the device changes to db prompt and loses the reach ability when you delete some configurations. [PR869528]
- When an active route changes from multiple-next-hop to single-next-hop, one of the internal structure is incorrectly updated. This results in route lookup failure and causes traffic drops even though the new active routes are correctly displayed in both the routing and forwarding tables. [PR879726]

Infrastructure

- When you archive a file using the file-archive rpc option, the following error is displayed:

  Operation allowed only from CLI

  [PR831865]

Interfaces and Routing

- When a process generates a vmcore or core-tarball file, users with super-user class privileges cannot access or retrieve the file. [PR772809]
- Configuring multicast addresses (inet6) on an interface results in the generation of RPD core (mc_ssm_add) files. [PR780751]
- When you attempt to create a dial backup interface, * and # symbols are not accepted. [PR834042]
- On the asymmetric digital subscriber line (ADSL) Mini-PIM, the Asynchronous Transfer Mode (ATM) Operation, Administration, and Management (OAM) feature is not supported. [PR835677]
- When the signal to noise ratio on the DSL line is low, the DSL line drops and is retrained. The DSL interface stops transmission after multiple line drop events. [PR837557]
- In an invalid subnet configuration on a multicast group, when you performed a commit or commit check, the routing protocol process (rpd) crashed and generated core files. [PR856925]
- Even when optical interfaces on SRX-GP-24GE PIM are disabled, the laser remains turned on. This causes the link on the peer side to remain up and results in a unidirectional link. [PR872916]
- When a symmetric high-speed DSL (SHDSL) Mini-PIM was configured in 2-wire mode with annex mode as Annex B/G, one of the physical interfaces did not come up. [PR882035]

Intrusion Detection and Prevention (IDP)

- You might not be able to configure the memory limit using the configuration statement **security sensor-configuration global memory-limit-percent** because an invalid range is expected. [PR830467]
- IDP signature database update was not synchronized between node 0 and node 1. [PR859196]

J-Web

- In J-Web, you can configure content-size-limit to a maximum range of 20 to 20,000 on the Configure>Security>UTM>Antivirus>ADD page, but the maximum range is 20 to 40,000. [PR725946]
- In J-Web, reboot does not work. [PR741014]

- On SRX550 devices, the “External storage” option is not supported. Therefore do not select the "External storage" option from the list on the Maintain>reboot and snapshot page. [PR741593]
- In J-Web, when more than one security policy is configured on a device, the first policy is not listed in the Apply-Policy section. [PR837799]
- In J-Web, if the policy name is "0", the penultimate-hop popping (PHP) function treats it as empty, and traffic log output cannot be viewed. [PR853093]
- In J-Web, you might not be able to specify the global address book object when configuring a security policy in an untrust zone. [PR853325]
- In J-Web, if dynamic VPN is configured, when you log out, the following error message is displayed: “404 page not found error”. [PR857419]
- In J-Web, information on routes is not listed under the Configure > Routing > Static Routing section. [PR864324]
- In J-Web, when 200 or more users are listed under Access Profile, all the users are not displayed. [PR872103]

Logical Systems

- In a logical system, you cannot use snmpwalk for Simple Network Management Protocol (SNMP) polling. [PR791859]

Network Address Translation (NAT)

- On all branch SRX Series devices, NAT might not function as expected because the configuration changes to source NAT, destination NAT, or both are not properly pushed to the forwarding plane. [PR744344]
- On devices enabled with static NAT and configured with multiple routing instances, reverse static NAT might not work when both the ingress interface and egress interface are in the root routing instance. [PR834145]

SNMP

- On all branch SRX Series and J Series devices, the SNMP jnxJsScreenCfgChange traps are rebooted even if there are no changes to the screen configuration. [PR835290]

Switching

- On SRX650 devices, the dot1x:mode:Multiple:Supplicants are authenticated even after a disconnect message is sent from the RADIUS server. [PR786731]

Unified Access Control (UAC)

- When a branch SRX Series device is deployed as a Unified Access Control (UAC) enforcer with session logging enabled for UAC enforced security policies in a UAC network, and the UAC authentication table contains users with many roles associated, traffic match for these policies generate flowd core files. [PR849805]

Unified Threat Management (UTM)

- When antivirus is enabled on a system, Web search using search engines such as yahoo.co.jp fails, if the content size limit is set to 20. [PR722652]
- When large numbers of UTM Enhanced Web filtering requests are pending, the CPU utilization is high on the utmd process. [PR841047]
- A security policy configured with antivirus shows incorrect count of bytes and packets in the policy statistics. [PR841923]
- On all branch SRX Series devices with UTM antivirus enabled, flowd core files are generated if files exceeding 1 GB are transferred using FTP. [PR846655]
- On devices in a chassis cluster, the antivirus database is not synchronized on both the cluster nodes. [PR863181]
- On all branch SRX Series device with Unified Threat Management (UTM) full antivirus (Kaspersky lab engine) enabled, traffic might drop intermittently when there is heavy traffic load to antivirus. This is because the cache space of antivirus (MFS disk) is marked as full once it is filled and the full flag is never cleared later even though the cache space is 100 percent free. As a result, traffic to the antivirus engine is flagged as out-of-resource and the connection resets. [PR864775]
- On all branch SRX Series devices, new categories for Enhanced Web filtering have been added. [PR866160]

Virtual Private Network (VPN)

- Occasionally, devices configured with policy-based IPsec VPN might not allow traffic to the protected resources. [PR718057]
- Network Address Translation-Traversal (NAT-T) might not work when the VPN is with Cisco and if the VPN is initiated from a Cisco peer. The VPN negotiates using port UDP 500 instead of UDP 4500 when NAT is involved. [PR869458]

Resolved Issues in Junos OS Release 12.1X44-D15 for Branch SRX Series Services Gateways

Chassis Cluster

- On a device in a chassis cluster, the primary node would go to **db** mode and generated vmcore file when you changed the configuration of the redundant Ethernet (reth) interface that caused the deletion of the logical interface of reth. [PR850897: This issue has been resolved.]

Command-Line Interface (CLI)

- When you upgrade an SRX Series device to Junos OS Release 11.4, NSM showed an error that a space in the full-name parameter of the **set system login user test-name full-name test name** command statement is not accepted. [PR806750: This issue has been resolved.]
- On SRX550 devices, the **request system firmware upgrade re bios** command to upgrade bios was missing. [PR809921: This issue has been resolved.]
- When you executed the **request system zeroize** command, the configuration was not deleted. As a result, the rescue configuration was loaded instead of the factory default configuration. [PR835687: This issue has been resolved.]

Flow and Processing

- Rewriting DiffServ code point (DSCP) bits for IPv6 neighbor advertisements was not supported. [PR827740: This issue has been resolved.]
- When a device forwarded traffic, a flowd core file was generated. This was a generic issue and was not related to any specific feature [PR831480: This issue has been resolved.]

Interfaces and Routing

- The routing protocol process (rpd) was reinitialized when you committed a configuration change. When multiple reinitializations occurred while OSPF was running on the router, the periodic refresh of OSPF router link-state advertisements (LSAs) stopped. If the LSAs were not refreshed, the router no longer participated in the OSPF routing domain. You could issue the **show ospf database router advertising-router router-id extensive | match timer"** command to see evidence of the issue. In the error state, the output did not include the Gen timer field. [PR744280: This issue has been resolved.]
- When the Flexible PIC Concentrator (FPC) restarted after performing a master Routing Engine switchover, the aggregate interface flag was set to **down**. Any traffic that entered this FPC and traversed the equal-cost multipath (ECMP) to the aggregate interface was dropped. [PR809383: This issue has been resolved.]
- On devices with a VDSL Mini-PIM or an integrated module, when you selected the VDSL profile as auto and the address acquisition method as DHCP in pt mode, the physical interface link flapped. [PR827144: This issue has been resolved.]

Intrusion Detection Prevention (IDP)

- The issue of false positives with negate attacks when using hardware DFA based pattern matching has been fixed. [PR848659: This issue has been resolved.]

J-Web

- On J Series devices, the initial setup tab was missing when you logged in to the device using the factory default setup method. [PR823306: This issue has been resolved.]
- On a device in a chassis cluster, the message “Configuring chassis cluster in non-cluster mode is not allowed” was displayed when you accessed J-Web using Internet Explorer. [PR825952: This issue has been resolved.]
- In J-Web, the value was set low in the “session expired when the idle-timeout” option. [PR830644: This issue has been resolved.]
- In J-Web, when more than one security policy was configured on a device, the first policy was not listed in the “Apply-Policy” section. [PR837799: This issue has been resolved.]
- In J-Web, custom-defined applications were presented as predefined. [PR837820: This issue has been resolved.]
- In J-Web, when you configured using the CLI or J-Web, you could not see the value of POL0. [PR839749: This issue has been resolved.]
- The New Setup wizard failed to commit the configuration because of a missing password for PAP/CHAP when the PPPoE wizard account contained "@" in it. [PR856746: This issue has been resolved.]
- On a device in a chassis cluster, the “switch to L2 mode” button from J-Web interface is non-functional. [PR857147: This issue has been resolved.]

Network Address Translation (NAT)

- NAT was not functioning as expected because the configuration changes to source NAT, destination NAT, or both were not properly pushed to the forwarding plane. [PR744344: This issue has been resolved.]

Switching

- IGMP leave messages received on a port of an 8-Port Gigabit Ethernet small form-factor pluggable (SFP) XPIM that was configured with Ethernet switching family were not processed by the IGMP Snooping module. [PR824557: This issue has been resolved.]

Unified Access Control (UAC)

- On a SRX device when captive portal is used along with UAC enforcement, the device ran into problems with authentication table state because of which IC-SRX connection broke continuously. [PR847180: This issue has been resolved.]
- On a device deployed as a Unified Access Control (UAC) enforcer in a UAC network, if session logging was enabled for UAC-enforced security policies and the UAC authentication table contained users that had many roles associated, traffic matched

these policies and caused the flowd process to crash and to generate a core file. [PR849805: This issue has been resolved.]

Unified Threat Management (UTM)

- When there were huge pending UTM enhanced Web filtering (EWF) requests, the CPU utilization was high on the utmd process. [PR841047: This issue has been resolved.]
- A security policy configured with antivirus showed incorrect count of bytes and packets in the policy statistics. [PR841923: This issue has been resolved.]

Virtual Private Networks (VPNs)

- IKE SA failed to install the responder during Phase 2 rekey. [PR809219: This issue has been resolved.]

Resolved Issues in Junos OS Release 12.1X44-D10 for Branch SRX Series Services Gateways

Application Layer Gateway (ALG)

- The forwarding process crashed, resulting in generation of a core file due to abnormal MGCP traffic. [PR684653: This issue has been resolved.]
- The EPRT command did not work with FTP ALGs on port 0, which were not valid. [PR769444: This issue has been resolved.]
- During ALG traffic processing, the device generated a core file. [PR780007: This issue has been resolved.]
- When the TNS RESEND (type 11) was 8 bytes long, the SQL ALG did not work properly. [PR806893: This issue has been resolved.]
- The MSRPC ALG dropped some big packets under the Kerberos authentication environment, because the Kerberos ticket token size and the MS-RPC bind packet were too large for ALG to handle. [PR817453: This issue has been resolved.]

Authentication

- The Web authentication page was not displayed properly when you tried to reauthenticate after an idle time. [PR741973: This issue has been resolved.]
- When the local or radius user password contained a percent character (%), firewall authentication through the Web portal failed due to an issue in processing the percent sign. [PR778891: This issue has been resolved.]

Command-Line Interface (CLI)

- The **show interface at < > extensive** command did not display the correct value when the at interface was up on the SHDSL Mini-PIM. [PR738322: This issue has been resolved.]
- On devices in a chassis cluster, the **set chassis usb storage disable** command did not work. [PR793844: This issue has been resolved.]

- On SRX220 PoE devices, the smtp-profile junos-as-defaults failed to load. [PR791575: This issue has been resolved.]
- The **ssl-encryption** option under the **edit security application-firewall rulesets *name* rule *name*** was irrelevant. [PR817232: This issue has been resolved.]

Dynamic Host Configuration Protocol (DHCP)

- When the devices acted as DHCP servers and the DHCP requests were forwarded to the SRX Series devices by a DHCP relay, the devices sent responses to DHCP requests to an incorrect UDP destination port. [PR774541: This issue has been resolved.]

Flow and Processing

- On SRX240 devices, when fragments with MTU value larger than 1514 were received, some of the fragments were dropped. [PR595955: This issue has been resolved.]
- Changes in policer, filter, or sampling configuration caused a core file to be generated during receipt of multicast traffic. [PR613782: This issue has been resolved.]
- Activating and deactivating logical interfaces a number of times resulted in flowd core files. [PR691907: This ssue has been resolved.]
- When the syn-cookie feature was enabled along with the syn-flood screen with a low timeout value, high-latency TCP sessions failed to establish successfully. The client sessions received unresponsive connections because the SRX Series device timed out the flow for the session. The device also dropped subsequent packets from the client due to the state not being found. [PR692484: This issue has been resolved.]
- The content filter for the SMTP block extension did not work when the name of the attached file was in Japanese. [PR724960: This issue has been resolved.]
- When making configuration changes to delete virtual router instances that included multicast interfaces, the Routing Protocol Daemon (RPD) crashed. [PR727357: This issue has been resolved.]
- The commands after STARTTLS were encrypted and could not be understood by the SMTP parser. These commands caused the session to hang until the TCP session was closed and no packets were forwarded. [PR750047: This issue has been resolved.]
- When the device sent a broadcast ARP to a Layer 3 VLAN interface that was restarting, it caused the forwarding to restart, resulting in traffic loss and generation of a flowd_octeon_hm core file. [PR755204: This issue has been resolved.]
- When SYN flooded packets per second (pps) over the screen attack-threshold, a SYN cookie was triggered by default. The SRX Series device sent SYN ACK to the client with ISN, and once the correct ACK was received, the device sent SYN to the server. However, the ACK packet (from the client) created a session and forwarded it to the server. Because the client received an ACK instead of a SYN packet, the server sent RST and RST was forwarded to the client, and the connection was reset. [PR755727: This issue has been resolved.]
- The httpd task was high. [PR768952: This issue has been resolved.]
- The traffic shaping did not work correctly when the shaping rate was configured on virtual channels. [PR769244: This issue has been resolved.]

- The SYN proxy (Syn-I) held the jbuf before SYN-ACK was received from the server. If the server was unreachable, SYN-PROXY held the jbuf until the session timed out. [PR769828: This issue has been resolved.]
- When the device processed a large amount of traffic, performing an AppID security package update caused the flowd process to generate a core file. [PR769832: This issue has been resolved.]
- For IKEv2, when the device attempted a dpd exchange during an existing exchange, a core file was generated. [PR771234 : This issue has been resolved.]
- On a device in a chassis cluster, the forwarding module became unresponsive when the redundant Ethernet (reth) interface was deleted while traffic was flowing through the device. Sometimes flowd generated a core file. [PR771273: This issue has been resolved.]
- The routing protocol daemon (rpd) generated a core file while processing a malformed RIP or RIP message from a neighbor during adjacency establishment. [PR772601: This issue has been resolved.]
- When passing GVPN multicast traffic, flowd core files were generated when the GVPN packet was encapsulated in the PIM register message. [PR774133: This issue has been resolved.]
- ICMP redirect did not work for FTP traffic. [PR776388: This issue has been resolved.]
- On a device in a chassis cluster, flowd core files were generated with Layer 2 Transparent configuration when the system was being shut down. [PR782579: This issue has been resolved.]
- The changes made to the VPI and VCI values of ADSL interfaces did not take effect until the chassis was rebooted. [PR783992: This issue has been resolved.]
- When the DNS ALG was enabled, the rewrite rules applied on the egress interface did not work for DNS messages. [PR785099: This issue has been resolved.]
- The session creation per second was always zero in the **show security monitoring fpc 0** output. [PR787343: This issue has been resolved.]
- When the DHCP client was configured on a routing instance in JSRP setup, after failover, device remained in secondary hold indefinitely. [PR790872: This issue has been resolved.]
- The flowd core files were generated during the IDP security-package update. [PR793417: This issue has been resolved.]
- On a device in a chassis cluster, long pauses and timeouts were seen for SNMP walk/query. This was caused by a delay in querying the gr-0/0/0 (GRE) interface by the kernel. [PR800735: This issue has been resolved.]
- The generation of a flowd core file was triggered by cache errors. [PR805975: This issue has been resolved.]
- There was an unexpectedly lower bandwidth through a scheduler queue that was configured with a small buffer size on an interface faster than 2 Mbps. [PR806745: This issue has been resolved.]

- ARP requests on the link aggregation interface failed under certain conditions. [PR819816: This issue has been resolved.]
- On devices with an SFP port on PIM, IP monitoring failed. [PR823643: This issue has been resolved.]
- On J Series devices, IDP initialization failed and the policy did not load. As a result, IDP inspection did not work. [PR833071: This issue has been resolved.]

Infrastructure

- The **services ip-monitoring** CLI command was not working. [PR771344: This issue has been resolved.]

Interfaces and Routing

- The egress queues were not supported on VLAN or IRB interfaces. [PR510568: This issue has been resolved.]
- For the VLAN-tagged redundant Ethernet interface, the Track IP (ipmon) feature was not supported. [PR575754: This issue has been resolved.]
- On J Series devices, when you used ISDN connections, an error appeared stating that a BAD_PAGE_FAULT had occurred and the ISDN connection had stopped working. [PR669297: This issue has been resolved.]
- On SRX550 devices, online insertion and removal of GPIMs or XPIMS was not supported. [PR719882: This issue has been resolved.]
- The service status of the 3G modem did not change from “Emergency calls only”. [PR746400: This issue has been resolved.]
- You could not use the words “management” or its variants as the security zone name. [PR754585: This issue has been resolved.]
- When interface VLAN was configured as a Layer 3 interface and redirected an IP packet, it did not reply with the ICMP redirect message. [PR754616: This issue has been resolved.]
- When automatic installation was enabled, the interface-control (dcd) process stopped and interfaces could not be configured. [PR773616: This issue has been resolved.]
- When the DHCP client was configured with VLAN, the DHCP leases were not acquired by the client and unicast messages were dropped. [PR776525: This issue has been resolved.]
- Interfaces with no cable connected and configured with the loopback option did not come up. [PR788395: This issue has been resolved.]
- After reboot, sometimes the VLAN interface was down while its physical interface member was up. [PR791610: This issue has been resolved.]

Intrusion Detection and Prevention (IDP)

- When the device was in low-memory condition on the control plane, it rebooted suddenly during the IDP security-package update. [PR776947: This issue has been resolved.]
- The detector was not updated in the control plane when the update-attack-database-only flag was used during security package installation. [PR778816: This issue has been resolved.]
- During IDP policy compile, the failure message “idp policy parser compile failed” was displayed due to a memory leak in the application identification configuration load. [PR787970: This issue has been resolved.]
- IDP policy load failed though there was sufficient memory (heap) available. This issue occurred when there was not enough contiguous memory block available in kernel heap memory. [PR789146: This issue has been resolved.]
- When you changed the configuration, the **show security idp policy-commit-status** command showed the message “Failed to add connection for dataplane”. [PR789542: This issue has been resolved.]
- The help and system logs on the terminal did not match. [PR794743: This issue has been resolved.]
- The policy push was not clearing SSL counters, and the SSL sessions-inspected counter kept increasing for every policy push. If the maximum SSL session limit configured was low, then SSL sessions were not inspected if the maximum limit was reached. [PR831611: This issue has been resolved.]
- The forwarding module crashed as a result of IDP processing. [PR832608: This issue has been resolved.]

J-Web

- In J-Web, policies configured under group global could not be edited or deleted in the NAT and firewall wizards. [PR552519: This issue has been resolved.]
- The J-Web interface incorrectly displayed the Session Expired pop-up window whenever flash storage was full. [PR569931: This issue has been resolved.]
- The PPPoE wizard support was not available in Junos OS Release 12.1X44-D10. [PR681083: This issue has been resolved.]
- In J-Web, you could not edit or delete the PPPoE connections set using the wizard. [PR688421: This issue has been resolved.]
- While editing the radio settings for an AX411 Wireless LAN Access Point on Configure >Wireless LAN > Setting, you could not edit the virtual access point, for which the security options configured were static-wep and dot1x. [PR692195: This issue has been resolved.]
- Add and Update buttons were not available on the License page when the 30 days or 1 day trial license was installed. [PR735174: This issue has been resolved.]

- On a device in a chassis cluster, when you configured ANNEX details of the SHDSL interface through J-Web, the existing configuration was deleted. Editing the configuration of SHDSL and the T1 card was not possible if it involved pushing chassis information. [PR737643: This issue has been resolved.]
- The Global options > Proxy screen was blank for the first time when you accessed it using Internet Explorer version 7.0. [PR737675: This issue has been resolved.]
- The EZ-Setup (J-Web Initialization setup) failed with the following error: “Fetching setup configuration....Please wait”. [PR748173: This issue has been resolved.]
- On SRX210 devices, Junos OS failed to import node configurations when chassis cluster setup was configured using J-Web. [PR753533: This issue has been resolved.]
- Using J-Web, when you clicked Enable Log on the Monitor > Security > IDP > Attacks page, the page was disabled and not accessible. [PR768559: This issue has been resolved.]
- When the httpd process restarted, the old httpd was deleted and the new httpd started. In certain circumstances, however, the old httpd and the new httpd existed at the same time, causing high CPU usage. [PR772701: This issue has been resolved.]
- J-Web displayed the following misleading error message when it reached memory limit when opening a large policy_session security log file: “The configuration on the Switch is too large for J-Web to handle. Please use the CLI to manipulate the configuration”. [PR777539: This issue has been resolved.]
- Logging in to J-Web resulted in the following error message: “JWEB is not supported on this platform”. [PR781659: This issue has been resolved.]
- In J-Web, when the device was in cluster mode after RG failover the primary node was displayed as a secondary hold in the Dashboard > System-identification > Cluster details. This was due to an RPC get data error. [PR786700: This issue has been resolved.]
- The Action > Compare in Dashboard page did not display output properly. [PR790557: This issue has been resolved.]
- On all branch SRX Series devices, an httpd-gk core file was generated when DVPN was enabled with FTP traffic. [PR791661: This issue has been resolved.]
- The Help page was not available for the Configure >Interface > Ports page. [PR792544: This issue has been resolved.]
- When you ran the S2J tool to convert a configuration from ScreenOS to Junos OS, the S2J tool automatically added annotations in the Junos OS configurations. J-Web had issues with creating or managing security policies when these annotations were in the Junos OS configuration. [PR793159: This issue has been resolved.]
- The default radio buttons did not work after you configured the Configure > Security > UTM > Web Filtering > Add profile > Fallback options. [PR794441: This issue has been resolved.]
- The Help page was not available for the Troubleshoot > CLI terminal page. [PR806027: This issue has been resolved.]

- The J-Web security logging tab was not working. [PR806442: This issue has been resolved.]
- The httpd task was high. [PR809061: This issue has been resolved.]
- Sometime the firewall policy wizard would not run. [PR816393: This issue has been resolved.]
- When you upgraded using the Partition command, if the Junos OS image was corrupted, the system rebooted with no available Junos OS image. [PR819505: This issue has been resolved.]
- The dashboard refresh rate changed. Refresh rates of 15, 30, and 60 seconds were removed. The minimum refresh rate available was 2 minutes. [PR826053: This issue has been resolved.]

License

- Erroneous messages were printed from liblicense during commit. [PR826158: This issue has been resolved.]

Network Address Translation (NAT)

- The commit of static NAT rules failed when logical system interfaces, security zone, and NAT were committed at the same time. Similarly, there were problems with committing static rules when you committed security zone and NAT at the same time. [PR756240: This issue has been resolved.]
- Static NAT rules were not being enforced when Ethernet switching family was used. [PR785106: This issue has been resolved.]

Security

- The captive portal redirect did not work with the strict SYN checking option enabled in the firewall. [PR743466: This issue has been resolved.]
- The configuration control link between the control and data planes was not reliable. In some conditions, the connection to the secondary node broke, in which case the application firewall rule could not be pushed to the secondary node. [PR810946: This issue has been resolved.]

SNMP

- When a default IP address was used as SNMP engine ID, after the device was rebooted or power cycled, the SNMP local engine ID was incorrectly set to 80 00 0a 4c 01 00 00 00 00. [PR613625: This issue has been resolved.]

SNMP MIBs

- The value for mib jnxJsIdp LastSignatureUpdateTime.0 always had the same value. [PR691785: This issue has been resolved.]
- SNMP OID jnxOperatingCPU.9 (Routing Engine CPU usage) always returned 100, although Routing Engine CPU usage was not 100 percent. [PR739591: This issue has been resolved.]

System Logs

- When an idle session is closed based on timeout expiration, the close reason shown in logs displayed "idle Timeout", instead of "unset" as it appeared before. [PR746572: This issue has been resolved.]

Unified Access Control (UAC)

- The device acted as a Unified Access Control (UAC) enforcer in a UAC network to ensure only qualified end users could access protected resources scenarios. However, when there were many users requiring authentication, users were redirected to the login portal and the IC server reported redirect loops. [PR817764: This issue has been resolved.]

Unified Threat Management (UTM)

- When Express AV (antivirus) was enabled, traffic from the server and client was buffered at the device. Sometimes the buffer resource ran out because the traffic arrived faster than the buffer resources were released, and the device detected an out-of-resource condition and took a fallback action. [PR556309: This issue has been resolved.]
- In the UTM feature “Content filter for SMTP Block Extension List,” the notify e-mail was not sent to the sender. [PR732182: This issue has been resolved.]
- The SMTP session was suspended, and the AV counters showed incorrect increments when a 20-MB file was transferred. [PR792518: This issue has been resolved.]
- UTM mbuf leaks were observed after several hours of traffic load. [PR795681: This issue has been resolved.]
- The traffic processed by a UTM antivirus that was configured with trickling caused JBUFs (MBUFs) memory leak and resulted in traffic outage. [PR799859: This issue has been resolved.]
- On the devices, there used to be a requirement for the support of both “STARTTLS” and “X-ANONYMOUSTLS” cases for the SMTP parser. [PR824027: This issue has been resolved.]
- The Juniper enhanced Web filtering feature experienced default, timeout, and connectivity fallback actions under sustained bursts of high traffic. [PR833768: This issue has been resolved.]

Virtual Private Network (VPN)

- Dynamic VPN users were unable to connect because the previous dynamic VPN user license had not been removed. [PR710519: This issue has been resolved.]
- When there were many IKE SAs, the SNMP MIB “jnxIpSecFlowMonPhaseOne” returned only the first IKE SA. [PR734797: This issue has been resolved.]
- The dynamic VPN license was not getting released when old dynamic VPN connections were terminated. [PR735615, PR774877: This issue has been resolved.]

- The error “Failed to connect to server” was displayed when multiple clients were connected to the device through dynamic VPN and when some configurations related to IKE negotiation changed on the device. [PR737787: This issue has been resolved.]
- IKE Phase 1 and Phase 2 logs erroneously reported that the renegotiation retry limit had been reached, even though the VPN build succeeded. [PR741751: This issue has been resolved.]
- When using IPsec VPN, the “IKE Phase-2 Failure: IKE Phase-2 negotiation retry limit reached?” message was logged even though no failure had actually occurred. [PR768466: This issue has been resolved.]
- If the version 2 IKE SA lifetime was more than 65,535 seconds, the IKE SA never rekeyed. It expired, and the corresponding tunnel flapped, causing traffic outage. [PR775595: This issue has been resolved.]
- When using SIP on a dynamic VPN client, the voice stream did not reach the client. [PR776883: This issue has been resolved.]
- The maximum number of custom categories should be 50 and maximum number of URL lists per custom category should be 30. [PR789538: This issue has been resolved.]
- The IPsec Phase 2 negotiation failed when you used authentication-algorithm hmac-sha-256-128. [PR793760: This issue has been resolved.]
- When you used hmac-sha-256-128 at the group VPN server for the IPsec authentication-algorithm, a gkmd core file was generated for the group VPN member. [PR800719: This issue has been resolved.]

Related Documentation

- New Features in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 6
- Changes in Default Behavior and Syntax in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 25
- Known Limitations in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 34
- Outstanding Issues in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 62
- Errata and Changes in Documentation for Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 80
- Upgrade and Downgrade Instructions for Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 90

Errata and Changes in Documentation for Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers

Errata for the Junos OS Software Documentation

This section lists outstanding issues with the software documentation.

Feature Support Reference for SRX Series and J Series Devices

- In this guide, in Table 14: DHCP Support, the "Dynamic Host Configuration Protocol" section incorrectly states that DHCPV6 relay agent is supported on SRX100, SRX110, SRX210 SRX220, SRX240, and SRX650 devices. The DHCPV6 relay agent is not supported on Branch SRX Series devices.
- The Chassis Cluster table incorrectly indicates that Layer 2 Ethernet switching capability in chassis cluster mode is supported on SRX100 devices. Layer 2 Ethernet switching capability in chassis cluster mode is not supported on SRX100 devices.
- The "IPv6 Support" table lists that IPv6 is supported only for TFTP ALG. The correct information is IPv6 is supported for DNS, FTP, and TFTP ALGs.

J Series Services Router Advanced WAN Access Configuration Guide

- The example given in the "Configuring Full-Cone NAT" section in the guide available at http://www.juniper.net/techpubs/software/jseries/junos85/index.html is incorrect. The correct and updated example is given in the revised guide available at http://www.juniper.net/techpubs/software/jseries/junos90) .

J2320, J2350, J4350, and J6350 Services Router Getting Started Guide

- The "Connecting to the CLI Locally" section states that the required adapter type is DB-9 female to DB-25 male. This is incorrect; the correct adapter type is DB-9 male to DB-25 male.

J-Web

- **J-Web Security Package Update Help page**—This Help page does not contain information about the download status.
- **J-Web pages for stateless firewall filters**—There is no documentation describing the J-Web pages for stateless firewall filters. To find these pages in J-Web, go to **Configure>Security>Firewall Filters**, and then select **IPv4 Firewall Filters** or **IPv6 Firewall Filters**. After configuring the filters, select **Assign to Interfaces** to assign your configured filters to interfaces.
- **J-Web configuration Instructions**— Because of ongoing J-Web interface enhancements, some of the J-Web configuration example instructions in the Junos administration and configuration guides became obsolete and thus were removed. For examples that are missing J-Web instructions, use the provided CLI instructions.

Junos OS CLI Reference

- In the "show security policies" topic, the "show security policies Output Fields" table includes the following incorrect information:

Applications	**ALG**: If an ALG is associated with the session, the name of the ALG. Otherwise, 0.

The correct information is:

Applications	**ALG**: If an ALG is explicitly associated with the policy, the name of the ALG is displayed. If **application-protocol ignore** is configured, ignore is displayed. Otherwise, 0 is displayed. However, even if this command shows ALG: 0, ALGs might be triggered for packets destined to well-known ports on which ALGs are listening, unless ALGs are explicitly disabled or when **application-protocol ignore** is not configured for custom applications.

- In this guide, the **source-threshold** statement incorrectly shows a default value of 1024 per second for number in the Options section. The correct default value is 4000 per second.
- The **edit applications application** ***application-name*** **term** ***term-name*** hierarchy level for the alg (Applications) configuration statement is incorrect. The correct hierarchy level is **edit applications application** ***application-name*****<term** ***term-name*****>**.

Junos OS Layer 2 Bridging and Switching Configuration Guide for Security Devices

- In this guide, the section “Configuring Layer 2 Bridging and Transparent Mode” includes an incorrect example, “Example: Configuring Layer 2 Trunk Interfaces with Multiple Units.” The example is in error because the SRX Series devices do not support multiple units.

Junos OS Interfaces Configuration Guide for Security Devices

- In this guide, Table 11, “MTU Values for the SRX Series Services Gateways PIMs,” does not specify the maximum MTU and default IPMTU values for the following PIMs:
  - 2-Port 10 Gigabit Ethernet XPIM
  - 16-Port Gigabit Ethernet XPIM
  - 24-Port Gigabit Ethernet XPIM

  The following table lists these values:

Table 7: MTU Values for the SRX Series Services Gateways PIMs

PIM	Default Media MTU (Bytes)	Maximum MTU (Bytes)	Default IP MTU (Bytes)
2-Port 10 Gigabit Ethernet XPIM	1514	9192	1500
16-Port Gigabit Ethernet XPIM	1514	9192	1500

Table 7: MTU Values for the SRX Series Services Gateways PIMs *(continued)*

24-Port Gigabit Ethernet XPIM	1514	9192	1500

Junos OS Security Basics

- The topic Understanding Policy Application Timeouts Contingencies under **Security Basics > Security Policy Applications for Security Devices > Policy Application Timeout**, contains erroneous information. It should read as follows:

  When setting timeouts, be aware of the following contingencies:

  - If an application contains several application rule entries, all rule entries share the same timeout. You need to define the application timeout only once. For example, if you create an application with two rules, the following commands will set the timeout to **20** seconds for both rules:

    ```
    user@host# set applications application test protocol tcp destination-port 1035-1035
    inactivity-timeout 20
    user@host# set applications application test term test protocol udp
    user@host# set applications application test term test source-port 1-65535
    user@host# set applications application test term test destination-port 1111-1111
    ```

  - If multiple custom applications are configured with custom timeouts, then each application will have its own custom application timeout. For example:

    ```
    user@host# set applications application ftp-1 protocol tcp source-port 0-65535
    destination-port 2121-2121 inactivity-timeout 10
    user@host# set applications application telnet-1 protocol tcp source-port 0-65535
    destination-port 2300-2348 inactivity-timeout 20
    ```

    With this configuration, Junos OS applies a 10-second timeout for destination port **2121** and a 20-second timeout for destination port **2300** in an application group.

Junos OS Security Configuration Guide

- In "Example: Configuring AppTrack," of the *Junos OS Security Configuration Guide for Security Devices*, the **set security log mode stream** statement was omitted from the log configuration statements. The updated log configuration should read:

  ```
  user@host# set security log mode stream
  user@host# set security log format sd-syslog
  user@host# set security log source-address 5.0.0.254
  user@host# set security log stream app-track-logs host 5.0.0.1
  ```

- In the "Understanding SIP ALGs and NAT" topic, information in the following sections is incorrect:

  - **Call Re-INVITE Messages**

    This section incorrectly states:

    When one or more media sessions are removed from a call, pinholes are closed and bindings released just as with a BYE message.

    The correct information is:

    When all the media sessions or media pinholes are removed from a call, the call is removed when a BYE message is received.

- **Call Session Timers**

  This section incorrectly states:

  The SIP ALG uses the **session-expires** value to time out a session if a Re-INVITE or UPDATE message is not received. The ALG receives the **session-expires** value, if present, from the 200 OK responses to the INVITE and uses this value for signaling timeout. If the ALG receives another INVITE before the session times out, the ALG resets all timeout values to this new INVITE or to default values, and the process is repeated. As a precautionary measure, the SIP ALG uses hard timeout values to set the maximum amount of time a call can exist.

  The correct information is (The **session-expires** value is not supported on SRX Series devices):

  As a precautionary measure, the SIP ALG uses hard timeout values to set the maximum amount of time a call can exist.

- **Table Requesting Messages with NAT Table**

  This table incorrectly states:

Outbound Request (from private to public	Route:	Replace ALG address with local address

  The correct information is:

Outbound Request (from private to public	Route:	Replace local address with ALG address

- This guide incorrectly lists the following topics. These commands are not supported:
  - **disable-call-id-hiding**
  - **show security alg sip transactions**

Junos OS Security interfaces

- The "Example: Configuring Multilink Frame Relay FRF.16" topic provides the following incorrect configuration information:

  Step: Set device R0 as a DCE device.

  ```
  [edit interfaces lsq-0/0/0]
  user@host# set dce
  ```

  The correct configuration information is

  Step: Set device R0 as a DCE device.

  ```
  [edit interfaces lsq-0/0/0:0]
  user@host# set dce
  ```

Junos OS Security Network Address Translation

- In Example: Configuring NAT for Mulitple ISPs under Network Address Translation for Security Devices > Configuration > NAT for Multiple ISPs the statement **set**

routing-options rib-groups isp import-rib inet.0 was omitted from the configuration. The updated configuration should read:

```
set routing-options rib-groups isp import-rib inet.0
set routing-options rib-groups isp import-rib isp1.inet.0
set routing-options rib-groups isp import-rib isp2.inet.0
```

In addition, because zone based address-book for NAT rules is unsupported, you should not use the statements provided in the example; use global address book instead.

- The command **show security nat source persistent-nat-table** under **Network Address Translation > Administration > Source NAT Operational Commands** is:
  - Missing the option:**summary**—Display persistent NAT bindings summary.
  - Contains incomplete sample output. The corrected sample output is as follows:

```
user@host> show security nat source persistent–nat–table internal-ip 9.9.9.1 internal-port
60784


Internal                        Reflective        Source     Type
Left_time/  Curr_Sess_Num/ Source
 In_IP  In_Port I_Proto Ref_IP    Ref_Port R_Proto NAT Pool
Conf_time   Max_Sess_Num  NAT Rule
9.9.9.1  60784   udp  66.66.66.68  60784     udp   dynamic-customer-source
any-remote-host  254/300  0/30 105
```

```
user@host> show security nat source persistent–nat–table all
 Internal             Reflective                  Source     Type
Left_time/  Curr_Sess_Num/  Source
 In_IP     In_Port I_Proto Ref_IP       Ref_Port R_Proto NAT Pool
       Conf_time   Max_Sess_Num    NAT Rule
9.9.9.1    63893   tcp    66.66.66.68   63893     tcp    dynamic-customer-source
 any-remote-host  192/300   0/30 105
9.9.9.1    64014   udp    66.66.66.68   64014     udp    dynamic-customer-source
 any-remote-host  244/300   0/30 105
9.9.9.1    60784   udp    66.66.66.68   60784     udp    dynamic-customer-source
 any-remote-host  254/300   0/30 105
9.9.9.1    57022   udp    66.66.66.68   57022     udp    dynamic-customer-source
 any-remote-host  264/300   0/30 105
9.9.9.1    53009   udp    66.66.66.68   53009     udp    dynamic-customer-source
 any-remote-host  268/300   0/30 105
9.9.9.1    49225   udp    66.66.66.68   49225     udp    dynamic-customer-source
 any-remote-host  272/300   0/30 105
9.9.9.1    52150   udp    66.66.66.68   52150     udp    dynamic-customer-source
 any-remote-host  274/300   0/30 105
9.9.9.1    59770   udp    66.66.66.68   59770     udp    dynamic-customer-source
 any-remote-host  278/300   0/30 105
9.9.9.1    61497   udp    66.66.66.68   61497     udp    dynamic-customer-source
 any-remote-host  282/300   0/30 105
9.9.9.1    56843   udp    66.66.66.68   56843     udp    dynamic-customer-source
 any-remote-host    -/300   1/30 105
```

```
user@host> show security nat source persistent-nat-table summary
Persistent NAT Table Statistics on FPC5 PIC0:
binding total : 65536
binding in use : 0
enode total : 524288
enode in use : 0
```

User Role Firewall

- In *Example: Configuring a User Role Firewall on an SRX Series Device* and *Acquiring User Role Information from an Active Directory Authentication Server*, the **redirect-url** option in step 2 of the redirection procedure is incorrect. The URL and variables should be enclosed in quotation marks.

  ```
  [edit]
  user@host# set services unified-access-control captive-portal acs-device
  redirect-url “https://%ic-url%/?target=%dest-url%&enforcer=%enforcer-id%”
  ```

VPN for Security Devices

- In “Example: Configuring a Route-Based VPN,” the **show security zones** output for the SRX Series device erroneously shows host-inbound-traffic configured for the vpn-chicago zone; this configuration is not included in the CLI Quick Configuration and the Step-by-Step Procedure.

Junos OS WLAN Configuration and Administration Guide

- This guide is missing information that the AX411 Access Point can be managed from SRX100 and SRX110 devices.
- This guide is missing the information that on all branch SRX devices, managing AX411 WLAN Access Points through an Layer 3 Aggregated Ethernet (ae) interface is not supported.

Various Guides

- 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 the Junos OS Feature Support Reference for SRX Series and J Series Devices.

Errata for the Junos OS Hardware Documentation

This section lists outstanding issues with the hardware documentation.

J Series Services Routers Hardware Guide

- The procedure “Installing a DRAM Module” omits the following condition:

  All DRAM modules installed in the router must be the same size (in megabytes), type, and manufacturer. The router might not work properly when DRAM modules of different sizes, types, or manufacturer are installed.
- This guide incorrectly states that only the J2350 Services Router complies with Network Equipment Building System (NEBS) criteria. It should state that the J2350, J4350, and J6350 routers comply with NEBS criteria.
- This guide is missing information about 100Base-LX connector support for 1-port and 6-port Gigabit Ethernet uPIMs.

SRX Series Services Gateways for the Branch Physical Interface Modules Hardware Guide

- This guide incorrectly documents that slot 3 of the SRX550 Services Gateway can be used to install GPIMs. The correct information is:
  - In Table 10: “SRX Series Services Gateway Interface Port Number Examples”, for 2-Port 10 Gigabit Ethernet XPIM, you can install the XPIM only in slot 6 of the SRX550 Services Gateway.
  - In Table 44: “Slots for 20-Gigabit GPIMs, for 20-Gigabit GPIM slots”, you can install the GPIM only in slot 6 of the SRX550 Services Gateway.

SRX100 Services Gateway Hardware Guide

- In the “Connecting an SRX100 Services Gateway to the J-Web Interface” section, the following information is missing in the note:

  NOTE: **Microsoft Internet Explorer version 6.0 is also supported as backward compatible from Microsoft Internet Explorer version 7.0.**

SRX210 Services Gateway Hardware Guide

- In the “Connecting an SRX210 Services Gateway to the J-Web Interface” section, the following information is missing in the note:

  NOTE: **Microsoft Internet Explorer version 6.0 is also supported as backward compatible from Microsoft Internet Explorer version 7.0.**

- The “SRX210 Services Gateway Specifications” table lists the values for chassis height, chassis width, chassis depth, chassis weight, and noise level incorrectly. The correct values are as follows:
  - Chassis height—1.73 in. (44 mm)
  - Chassis width—11.02 in. (280 mm)
  - Chassis depth—7.13 in. (181 mm)
  - Chassis weight:
    - 3.46 lb (1.57 kg) for SRX210 Services Gateway without PoE (no interface modules)
    - 3.55 lb (1.61 kg) for SRX210 Services Gateway with PoE (no interface modules)
  - Noise level—29.1 dB per EN ISO 7779

SRX220 Services Gateway Hardware Guide

- The “SRX220 Services Gateway Specifications” table lists the values for chassis height, chassis width, chassis depth, chassis weight, and noise level incorrectly. The correct values are as follows:

- Chassis height—1.73 in. (44 mm)
- Chassis width—14.29 in. (363 mm)
- Chassis depth—7.13 in. (181 mm)
- Chassis weight:
  - 4.52 lb (2.05 kg) for SRX220 models without PoE (no interface modules)
  - 4.62 lb (2.10 kg) for SRX220 models with PoE (no interface modules)
- Noise level—51.1 dB per EN ISO 7779

SRX240 Services Gateway Hardware Guide

- In the "Connecting the SRX240 Services Gateway to the J-Web Interface" section, the following information is missing in the note:

  NOTE: **Microsoft Internet Explorer version 6.0 is also supported as backward compatible from Microsoft Internet Explorer version 7.0.**

SRX550 Services Gateway Hardware Guide

- The "SRX550 Services Gateway Front Panel" section incorrectly states that the SanDisk Micro Cruzer 2GB to 32GB USB storage devices are supported on SRX550 devices. The SanDisk Micro Cruzer 2GB to 32GB USB storage devices are not supported on SRX550 devices.

SRX650 Services Gateway Hardware Guide

- The "Maintaining the SRX650 Services Gateway Power Supply" section incorrectly states that the status of the power supplies on the SRX650 Services Gateway can be checked by issuing the **show chassis environment pem** command. The **show chassis environment pem** command is not supported on the SRX650 Services Gateway.

SRX110 Services Gateway 3G USB Modem Quick Start

- The SRX110 Services Gateway 3G USB Modem Quick Start has been updated with the J-Web procedures, and it is available on the Juniper Networks website.

SRX210 Services Gateway 3G ExpressCard Quick Start

- Several tasks are listed in the wrong order. "Task 6: Connect the External Antenna" should appear before "Task 3: Check the 3G ExpressCard Status," because the user needs to connect the antenna before checking the status of the 3G ExpressCard. The correct order of the tasks is as follows:

  1. Install the 3G ExpressCard
  2. Connect the External Antenna
  3. Check the 3G ExpressCard Status

4. Configure the 3G ExpressCard
5. Activate the 3G ExpressCard Options

- In “Task 6: Connect the External Antenna,” the following sentence is incorrect and redundant: “The antenna has a magnetic mount, so it must be placed far away from radio frequency noise sources including network components.”
- In the “Frequently Asked Questions” section, the answer to the following question contains an inaccurate and redundant statement:

  Q: Is an antenna required? How much does it cost?

  A: The required antenna is packaged with the ExpressCard in the SRX210 Services Gateway 3G ExpressCard kit at no additional charge. The antenna will have a magnetic mount with ceiling and wall mount kits within the package.

  In the answer, the sentence “The antenna will have a magnetic mount with ceiling and wall mount kits within the package” is incorrect and redundant.

SRX210 Services Gateway Quick Start Guide

- The section on installing software packages is missing the following information:

  On SRX210 devices, the **/var** hierarchy is hosted in a separate partition (instead of the *root* partition). If Junos OS installation fails as a result of insufficient space:

  1. Use the **request system storage cleanup** command to delete temporary files.
  2. Delete any user-created files both in the *root* partition and under the **/var** hierarchy.

Related Documentation

- New Features in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 6
- Changes in Default Behavior and Syntax in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 25
- Known Limitations in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 34
- Outstanding Issues in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 62
- Resolved Issues in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 65
- Upgrade and Downgrade Instructions for Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 90

Upgrade and Downgrade Instructions for Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers

This section includes the following topics:

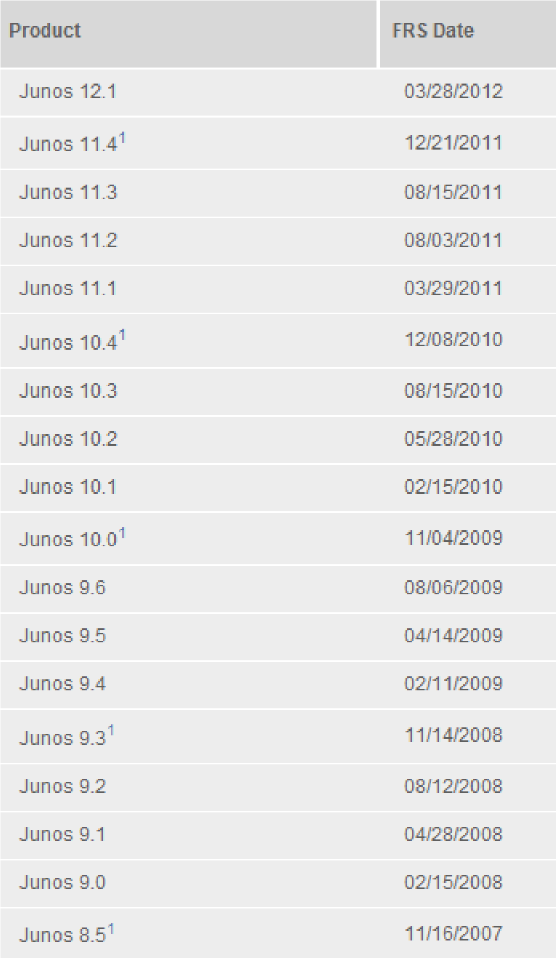
- Upgrading and Downgrading among Junos OS Releases on page 90
- Upgrading an AppSecure Device on page 92
- Upgrade and Downgrade Scripts for Address Book Configuration on page 92
- Hardware Requirements for Junos OS Release 12.1X44 for SRX Series Services Gateways and J Series Services Routers on page 95

Upgrading and Downgrading among Junos OS Releases

All Junos OS releases are listed in sequence on the JUNOS Software Dates & Milestones web page:

http://www.juniper.net/support/eol/junos.html

To help in understanding the examples that are presented in this section, a portion of that table is replicated here. Note that releases footnoted with a 1 are Extended End-of-Life (EEOL) releases.



Product	FRS Date
Junos 12.1	03/28/2012
Junos 11.4[1]	12/21/2011
Junos 11.3	08/15/2011
Junos 11.2	08/03/2011
Junos 11.1	03/29/2011
Junos 10.4[1]	12/08/2010
Junos 10.3	08/15/2010
Junos 10.2	05/28/2010
Junos 10.1	02/15/2010
Junos 10.0[1]	11/04/2009
Junos 9.6	08/06/2009
Junos 9.5	04/14/2009
Junos 9.4	02/11/2009
Junos 9.3[1]	11/14/2008
Junos 9.2	08/12/2008
Junos 9.1	04/28/2008
Junos 9.0	02/15/2008
Junos 8.5[1]	11/16/2007

You can directly upgrade or downgrade between any two Junos OS releases that are within three releases of each other.

- Example: Direct release upgrade

  Release 10.3 → *(bypassing Releases 10.4 and 11.1)* Release 11.2

To upgrade or downgrade between Junos OS releases that are more than three releases apart, you can upgrade or downgrade first to an intermediate release that is within three releases of the desired release, and then upgrade or downgrade from that release to the desired release.

- Example: Multistep release downgrade

  Release 11.3 → *(bypassing Releases 11.2 and 11.1)* Release 10.4 → Release 10.3

Juniper Networks has also provided an even more efficient method of upgrading and downgrading using the Junos OS EEOL releases. EEOL releases generally occur once a calendar year and can be more than three releases apart. For a list of, EEOL releases, go to http://www.juniper.net/support/eol/junos.html

You can directly upgrade or downgrade between any two Junos OS EEOL releases that are within three EEOL releases of each other.

- Example: Direct EEOL release upgrade

  Release 9.3 (EEOL) → *(bypassing Releases 10.0 [EEOL] and 10.4 [EEOL])* Release 11.4 (EEOL)

To upgrade or downgrade between Junos OS EEOL releases that are more than three EEOL releases apart, you can upgrade first to an intermediate EEOL release that is within three EEOL releases of the desired EEOL release, and then upgrade from that EEOL release to the desired EEOL release.

- Example: Multistep release upgrade using intermediate EEOL release

  Release 8.5 (EEOL) → *(bypassing Releases 9.3 [EEOL] and 10.0 [EEOL])* Release 10.4 (EEOL) → Release 11.4 (EEOL)

You can even use a Junos OS EEOL release as an intermediate upgrade or downgrade step if your desired release is several releases later than your current release.

- Example: Multistep release upgrade using intermediate EEOL release

  Release 9.6 → Release 10.0 (EEOL) → Release 10.2

For additional information about how to upgrade and downgrade, see the *Junos OS Installation and Upgrade Guide*.

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 2 on page 94).

- About Upgrade and Downgrade Scripts on page 93
- Running Upgrade and Downgrade Scripts on page 94
- Upgrade and Downgrade Support Policy for Junos OS Releases on page 95

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.

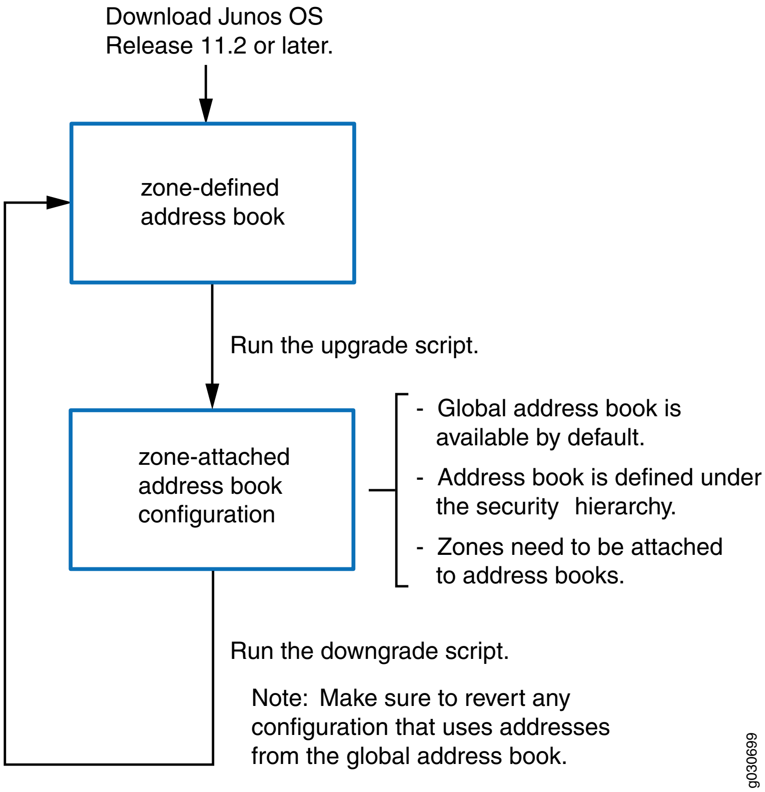
  After upgrading to the zone-attached address book configuration:

  - 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 2: Upgrade and Downgrade Scripts for Address Books


Download Junos OS
Release 11.2 or later.
zone-defined
address book
Run the upgrade script.
zone-attached
address book
configuration
- Global address book is available by default.
- Address book is defined under the security hierarchy.
- Zones need to be attached to address books.
Run the downgrade script.
Note: Make sure to revert any configuration that uses addresses from the global address book.
g030699

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

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 .

Hardware Requirements for Junos OS Release 12.1X44 for SRX Series Services Gateways and J Series Services Routers

Transceiver Compatibility for SRX Series and J Series Devices

We strongly recommend that only transceivers provided by Juniper Networks be used on SRX Series and J Series interface modules. Different transceiver types (long-range, short-range, copper, and others) can be used together on multiport small form-factor pluggable (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.

Power and Heat Dissipation Requirements for J Series PIMs

On J Series Services Routers, the system monitors the PIMs and verifies that the PIMs fall within the power and heat dissipation capacity of the chassis. If power management is enabled and the capacity is exceeded, the system prevents one or more of the PIMs from becoming active.

CAUTION: Disabling the power management can result in hardware damage if you overload the chassis capacities.

You can also use CLI commands to choose which PIMs are disabled. For details about calculating the power and heat dissipation capacity of each PIM and for troubleshooting procedures, see the *J Series Services Routers Hardware Guide*.

Supported Third-Party Hardware

The following third-party hardware is supported for use with J Series Services Routers running Junos OS.

- **USB Modem**

  We recommend using a U.S. Robotics USB 56K V.92 Modem, model number USR 5637.

- **Storage Devices**

  The USB slots on J Series Services Routers accept a USB storage device or USB storage device adapter with a CompactFlash card installed, as defined in the *CompactFlash Specification* published by the CompactFlash Association. When the USB device is installed and configured, it automatically acts as a secondary boot device if the primary CompactFlash card fails on startup. Depending on the size of the USB storage device, you can also configure it to receive any core files generated during a router failure. The USB device must have a storage capacity of at least 256 MB.

  Table 8 on page 96 lists the USB and CompactFlash card devices supported for use with the J Series Services Routers.

Table 8: Supported Storage Devices on the J Series Services Routers

Manufacturer	Storage Capacity	Third-Party Part Number
SanDisk—Cruzer Mini 2.0	256 MB	SDCZ2-256-A10
SanDisk	512 MB	SDCZ3-512-A10
SanDisk	1024 MB	SDCZ7-1024-A10
Kingston	512 MB	DTI/512KR
Kingston	1024 MB	DTI/1GBKR
SanDisk—ImageMate USB 2.0 Reader/Writer for CompactFlash Type I and II	N/A	SDDR-91-A15
SanDisk CompactFlash	512 MB	SDCFB-512-455
SanDisk CompactFlash	1 GB	SDCFB-1000.A10

J Series CompactFlash and Memory Requirements

Table 9 on page 97 lists the CompactFlash card and DRAM requirements for J Series Services Routers.

Table 9: J Series CompactFlash Card and DRAM Requirements

Model	Minimum CompactFlash Card Required	Minimum DRAM Required	Maximum DRAM Supported
J2320	1 GB	1 GB	1 GB
J2350	1 GB	1 GB	1 GB
J4350	1 GB	1 GB	2 GB
J6350	1 GB	1 GB	2 GB

Related Documentation

- New Features in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 6
- Changes in Default Behavior and Syntax in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 25
- Known Limitations in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 34
- Outstanding Issues in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 62
- Resolved Issues in Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 65
- Errata and Changes in Documentation for Junos OS Release 12.1X44 for Branch SRX Series Services Gateways and J Series Services Routers on page 80

Junos OS Release Notes for High-End SRX Series Services Gateways

Powered by Junos OS, Juniper Networks high-end SRX Series Services Gateways provide robust networking and security services. High-end SRX Series Services Gateways are designed to secure enterprise infrastructure, data centers, and server farms. The high-end SRX Series Services Gateways include the SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices.

New Features in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways

The following features have been added to Junos OS Release 12.1X44. Following the description is the title of the topics and pathway pages to consult for more information on the feature.

Release 12.1X44-D20 Software Features

Application Layer Gateways (ALG)

- **Transparent mode support for ALGs**—This feature is supported on all high-end SRX Series devices.

  Beginning with Junos OS Release 12.1X44-D20, Avaya H.323, G-H323, IKE, MGCP, MSRPC, PPTP, RSH, SUN RPC, SCCP, SIP, SQL, and TALK ALGs support layer 2 transparent mode. Transparent mode on SRX Series devices provides standard Layer 2 switching capabilities and full security services.

  In transparent mode, the SRX Series device filters packets that traverse the device without modifying any of the source or destination information in the packet MAC headers. Transparent mode is useful for protecting servers that mainly receive traffic from untrusted sources because there is no need to reconfigure the IP settings of routers or protected servers.

  NOTE: **Transparent mode is supported on all data and VOIP ALGs.**

A device operates in Layer 2 transparent mode when all physical interfaces on the device are configured as Layer 2 interfaces. There is no command to define or enable transparent mode on the device. The device operates in transparent mode when there are interfaces defined as Layer 2 interfaces. The device operates in route mode (the default mode) if there are no physical interfaces configured as Layer 2 interfaces.

- [*Layer 2 Bridging and Transparent Mode Overview*]
- [*Layer 2 Bridging and Switching for Security Devices*]
- [*Layer 2 Bridging and Transparent Mode for Security Devices*]
- [*Transparent Mode*]

IPsec VPN

- **AutoVPN RIP support for unicast traffic**—AutoVPN hubs are supported on SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices. AutoVPN spokes are supported on SRX1400 devices.

  Junos OS Release 12.1X44-D20 adds support for configuring the RIP dynamic routing protocol with AutoVPN for unicast traffic. In addition to RIP, OSPF and BGP are supported with AutoVPN for unicast traffic.

  For AutoVPN configuration examples with RIP, go to the Juniper Networks Knowledge Base (KB): http://kb.juniper.net/ and search for KB27720.

  [*AutoVPNs for Security Devices*]

Release 12.1X44-D15 Hardware Features

Chassis Grounding for SRX1400 Through SRX5800 Services Gateways

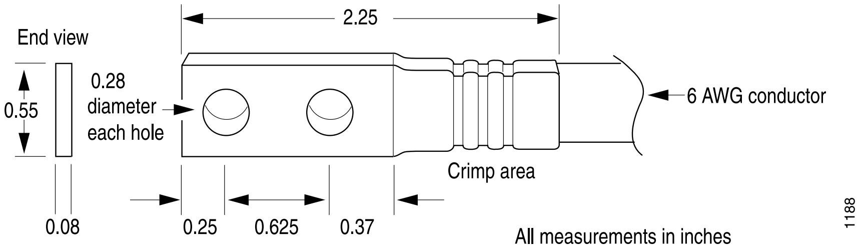
WARNING:

In order to meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, you must properly ground the services gateway chassis before connecting power. This requirement applies to the following services gateway models without exception:

- SRX1400 Services Gateway
- SRX3400 Services Gateway
- SRX3600 Services Gateway
- SRX5600 Services Gateway
- SRX5800 Services Gateway

For all services gateway models, the accessory box shipped with the device includes one cable lug that attaches the grounding cable to the services gateway chassis. The cable lug is shown in Figure 3 on page 100.

Figure 3: Grounding Cable Lug



Before services gateway installation begins, a licensed electrician must attach the cable lug to the grounding cable that you supply. A cable with an incorrectly attached lug can damage the services gateway. The grounding cable must be no smaller than specified in Table 10 on page 100, or as required by local electrical codes:

Table 10: Grounding Cable Wire Specification

Services Gateway Type	Grounding Cable Wire Specification
SRX1400 Services Gateway	14-AWG (2.1 mm^2), minimum 60ºC wire
SX3400 Services Gateway	10-AWG (5.3 mm^2), minimum 60ºC wire
SRX3600 Services Gateway	10-AWG (5.3 mm^2), minimum 60ºC wire
SRX5600 Services Gateway	6-AWG (13.3 mm^2), minimum 60ºC wire
SRX5800 Services Gateway	6-AWG (13.3 mm^2), minimum 60ºC wire

NOTE: For the SRX5800 services gateway models, we previously specified 10-AWG wire for the grounding cable. Where you have installed such grounding cables, you can safely leave them in service. However, all new installations of SRX5800 Services Gateways must have grounding cables sized according to Table 10 on page 100.

If you have lost the grounding cable lug supplied with the services gateway, contact your Juniper Networks representative to obtain a replacement.

Figure 4 on page 101 through Figure 8 on page 103 show the locations of the chassis grounding points on the listed SRX Series Services Gateway models. We recommend that you confirm that your services gateway chassis is properly grounded as soon as practical. For full instructions on grounding the services gateway chassis, see the hardware documentation for your services gateway.

Figure 4: Connecting the Grounding Cable, SRX1400 Services Gateway

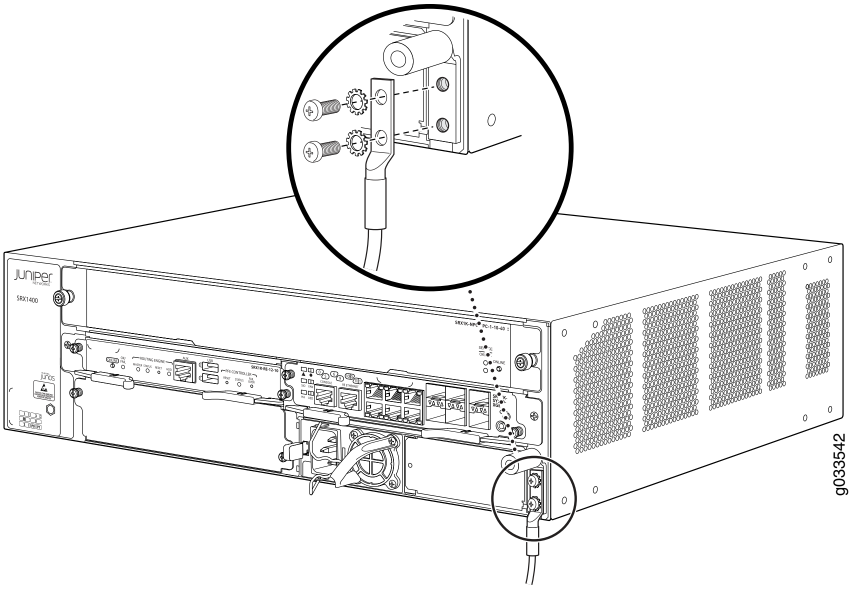


Figure 5: Connecting the Grounding Cable, SRX3400 Services Gateway

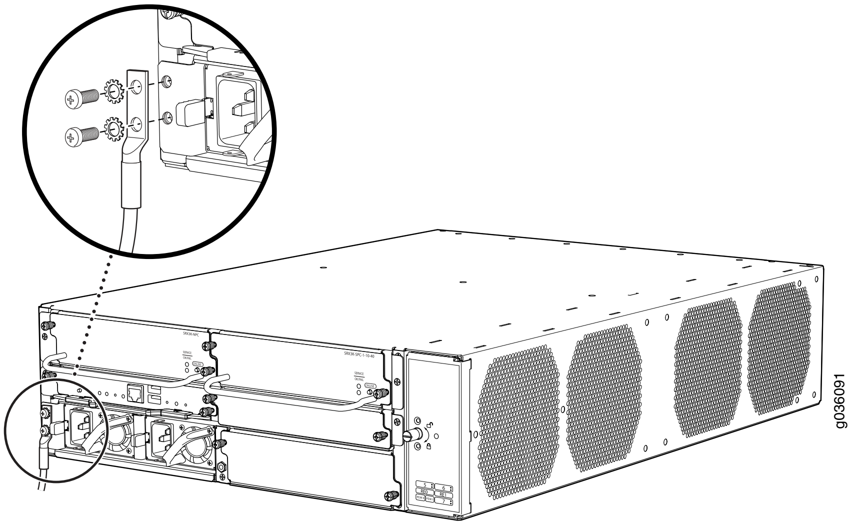


Figure 6: Connecting the Grounding Cable, SRX3600 Services Gateway

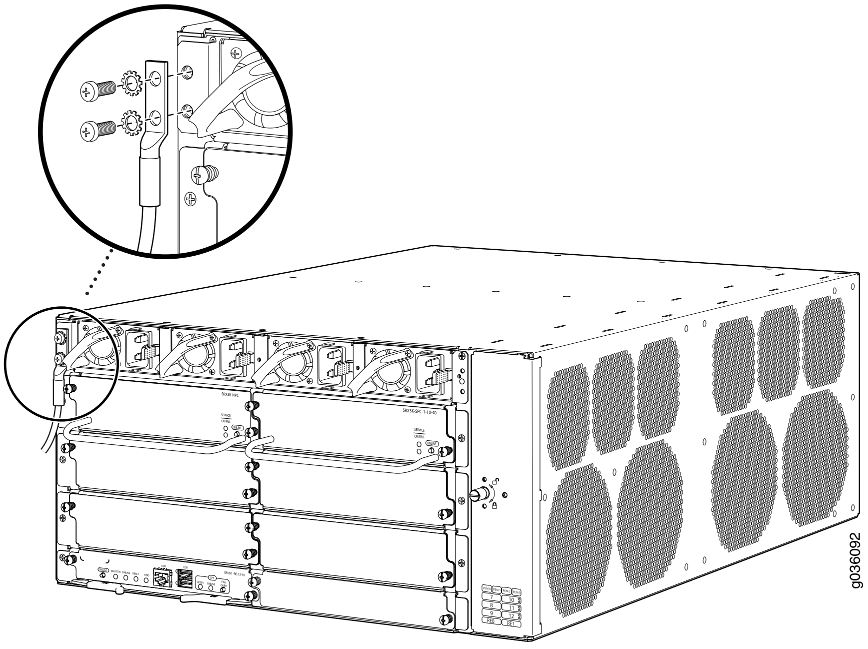


Figure 7: Connecting the Grounding Cable, SRX5600 Services Gateway

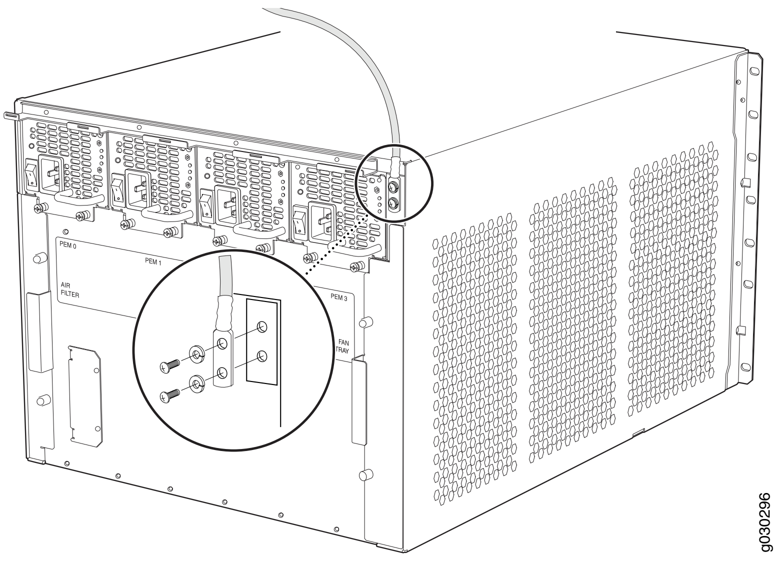
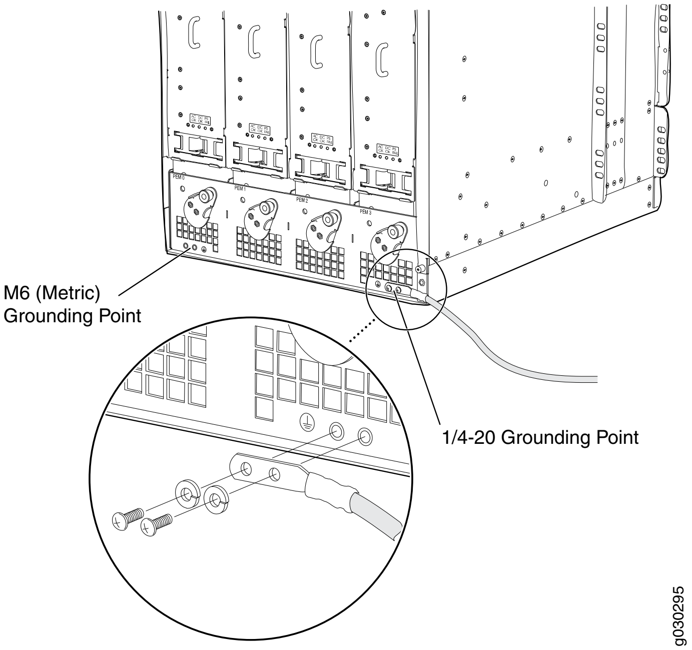


Figure 8: Connecting the Grounding Cable, SRX5800 Services Gateway



Release 12.1X44-D15 Software Features

The following features are supported on next-generation SPCs on SRX5600 and SRX5800 devices:

- Intrusion detection and prevention (IDP)—Next-generation SPCs support IDP and Appsecure functionality.
- Application firewall and user firewall—Support for application firewall rule sets and rules and user firewall policies have been increased as follows:

Maximum AppFW Rule Sets	Maximum AppFW Rules	Maximum Network Policies
56,000	112,000	80,000

Maximum UserFW Policies	Maximum Network Policies
64,000	80,000

Release 12.1X44-D10 Hardware Features

- **Chassis cluster SPC insert**—For services gateways from the SRX3000 line or the SRX5000 line configured in a chassis cluster, you can install additional Services Processing Cards (SPCs) in the services gateways in the cluster without incurring downtime on your network.

To perform such an installation, your devices must meet the following conditions:

- If the chassis cluster is in active/active mode, you must transition it to active/passive mode before using this procedure. You transition the cluster to active/passive mode by making one node primary for all redundancy groups.
- Both of the services gateways in the cluster must be running Junos OS Release 11.4R2-S1, 12.1X44-D10, or later.
- You must install SPCs of the same type in both of the services gateways in the cluster.
- You must install the SPCs in the same slots in each chassis.
- You must install the SPCs so that they are not the SPCs with the lowest-numbered slots in the chassis. For example, if the chassis already has two SPCs with one SPC each in slots 2 and 3, you cannot install additional SPCs in slots 0 or 1 using this procedure.

NOTE: **During this installation procedure, you must shut down both devices one at a time. During the period when one device is shut down, the remaining device is operating without a backup. If that remaining device fails for any reason, you incur network downtime until you restart at least one of the devices.**

[*SRX3400 Services Gateway Hardware Guide*]

[*SRX3600 Services Gateway Hardware Guide*]

[*SRX5600 Services Gateway Hardware Guide*]

[*SRX5800 Services Gateway Hardware Guide*]

- **Second Services Processing Card in SRX1400 Services Gateway**—When running Junos OS Release 12.1X44-D10 or later, the SRX1400 Services Gateway supports a Services Processing Card (SPC) installed in the front panel slot labeled 2, which acts as the central point (CP). Installing an SPC in slot 2 improves the services gateway performance and increases the session capacity from 500,000 to 1,500,000.

  [*Understanding Chassis Cluster Control Links*]

  [*Understanding Chassis Cluster Formation*]

  [*Understanding Chassis Cluster Redundancy Group IP Address Monitoring*]

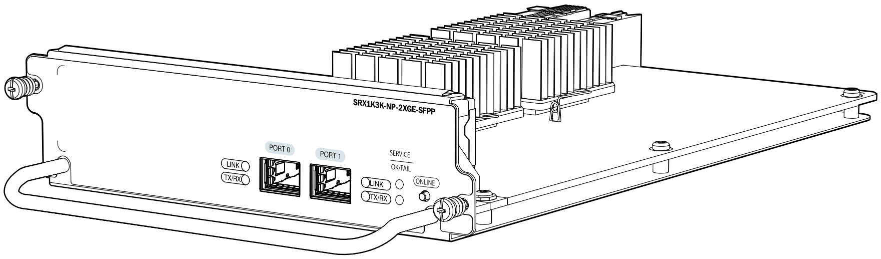
  [*Connecting Dual Control Links for SRX Series Devices in a Chassis Cluster*]

  [*show chassis fpc (View)*]

  [*SRX1400 Services Gateway Hardware Guide*]

- **Network Processing I/O Card SRX1K3K-NP-2XGE-SFPP for SRX1400, SRX3400, and SRX3600 Services Gateways**—Junos OS Release 12.1X44-D10 supports the new Network Processing I/O card (NP-IOC) SRX1K3K-NP-2XGE-SFPP (Figure 9 on page 105). The NP-IOC is an IOC that includes its own Network Processing Unit (NPU), so that traffic traversing the NP-IOC does not have to also traverse the services gateway bus to a remote NPC. This feature makes the NP-IOC well-suited to low-latency applications. The NP-IOC is inserted horizontally into the midplane of the services gateway to communicate with the Switch Fabric Board (SFB) and to receive power. To use fiber interface media, install enhanced small form-factor pluggable plus (SFP+) transceivers on the desired ports. LEDs on the faceplate of the NP-IOC indicate port status and connectivity. The SFP+ ports are numbered 0 through 1 from left to right.

Figure 9: NP-IOC SRX1K3K-NP-2XGE-SFPP



The NP-IOC is supported in the following slots in the SRX1400, SRX3400, and SRX3600 Services Gateways:

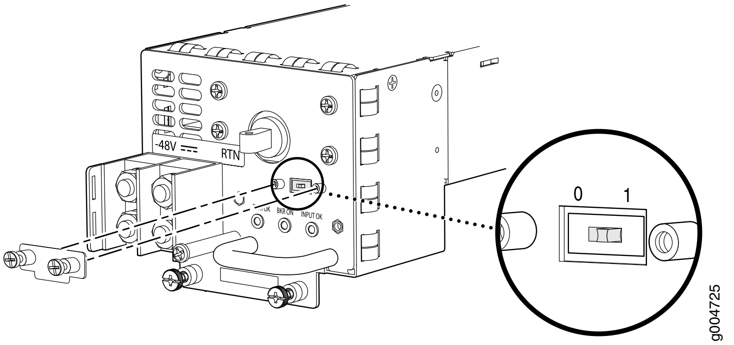
- SRX1400: Front slot labeled **2**
- SRX3400: Front slots labeled **1-4** and rear slots labeled **5-7**.
- SRX3600: Front slots labeled **1-6** and rear slots labeled **7-12**.

NOTE: You can install NP-IOCs instead of NPCs and IOCs in the SRX3400 or SRX3600 Services Gateway. However, if no NPCs are present, the Ethernet ports on the SFB are not functional.

- **SRX5600 Services Gateway high-capacity power supplies and fan tray**—With Junos OS Release 12.1X44-D10, the SRX5600 Services Gateway supports new high-capacity AC and DC power supplies, and also a new high-capacity fan tray. These components increase the power and cooling capacity so that the services gateway can support high-performance cards such as the SRX5K-SPC-4-15-320 next-generation SPC.

  The high-capacity AC power supply and the high-capacity fan tray are similar in appearance to their standard-capacity counterparts. The high-capacity DC power supply has an added DIP switch on its faceplate that lets you configure the device for either 60 A or 70 A maximum input current. See Figure 10 on page 106.

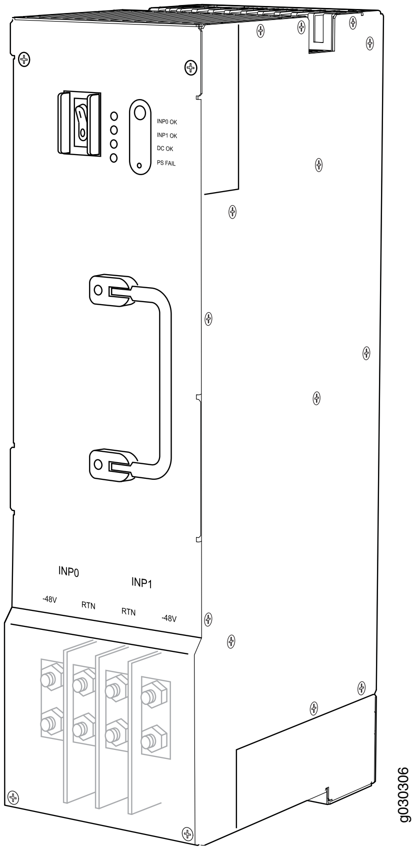
Figure 10: DC High-Capacity Power Supply Input Mode Switch



- **SRX5800 Services Gateway high-capacity DC power supply**—Starting with Junos OS Relase 10.4, the SRX5800 Services Gateway supported high-capacity AC power supplies and also high-capacity fan trays and air filters. With Junos OS Release 12.1X44-D10, the services gateway also supports high-capacity DC power supplies (Figure 11 on page 107). These components increase the power and cooling capacity of the services gateway so that it can support high-performance cards such as the SRX5K-SPC-4-15-320 next-generation SPC.

  High-capacity DC power supplies provide a maximum power of 4100 W. Two high-capacity DC power supplies are required, and you can install four high-capacity DC power supplies for redundancy. Each high-capacity DC power supply has inlets for two DC power feeds. The four power connectors (-48V and RTN for each of the two inlets) are located behind a clear plastic cover near the bottom of the power supply. Each DC power inlet you use requires a dedicated DC power feed and a dedicated 15 A (250 VAC) circuit breaker.

Figure 11: SRX5800 Services Gateway High-Capacity DC Power Supply



NOTE:

- The services gateway cannot be powered from standard-capacity and high-capacity DC power supplies simultaneously. The one exception is during the process of replacing standard-capacity DC power supplies with high- capacity DC power supplies, when it is permissible to have both types installed briefly.
- The high-capacity DC power supply will operate with only one of its two DC inlets connected to a DC power feed. However, the DC output will be limited to a maximum of 1700 W. We recommend that you connect two DC power feeds to each high-capacity DC power supply.

Release 12.1X44-D10 Software Features

Application Layer Gateways (ALGs)

- **Real-Time Streaming Protocol (RTSP) interleave mode**—This feature is supported on all high-end SRX Series devices.

  This feature is an enhancement to the current RTSP ALG. In most use cases the network carries UDP media streams based on an RTSP TCP connection, but there has been an increase in demand for the use of interleaving mode in which both media and control share the same TCP connection. The key reason to use interleaving is the ability to traverse firewalls. Because of the lower security restrictions around TCP port 80 to support Web traffic, RTSP makes use of interleaving mode for including media in the same connection to traverse firewalls.

[*Understanding ALG Types*]

- On SRX3600 devices, the new application **junos-sun-rpc-any** has been added. This CLI provides you a simple way to enable all the Sun RPC applications. You do not have to configure any specific Sun RPC applications.

  [*Understanding Sun RPC ALGs*]

AppSecure

- **AppFW rule set features expanded**—This feature is supported on all high-end SRX Series devices.

  AppFW has been enhanced to broaden the rule set options for defining an application-aware firewall. With the new enhancements you can:

  - Choose to close a TCP connection when matching traffic is rejected.
  - Define explicit, coexisting permit rules and deny rules in a single rule set.
  - Control SSL traffic more effectively with cleartext or encrypted options in AppFW rules.
  - Display session logs to view new session create, deny, and close messages that describe the AppFW actions that have been taken.
  - Display AppFW rules that are shadowed by others in the same rule set so that you can remove redundancy and avoid errors.

  [*Application Firewall*]

- **Application identification at Layer 3 and Layer 4**—This feature is supported on all high-end SRX Series devices.

  New **services application-identification** configuration options allow the ICMP type or code, the IP protocol, and the source or destination addresses that are available at Layer 3 or Layer 4 to be mapped to an application. When implementing AppSecure services, such as AppFW, AppTrack, or AppQoS, you can apply Layer 3 or Layer 4 mapping techniques to bypass Layer 7 signature-based mapping whenever applicable and improve the efficiency of the network. The mapping techniques work as follows:

  - Address mapping associates traffic to or from particular addresses with a known application.
  - ICMP mapping associates the type or code of ICMP messages with a known application.
  - IP protocol mapping applies to IP traffic only and associates a particular IP protocol with a known application.

  [*Application Identification for Security Devices*]

- **Session resumption and renegotiation with SSL proxy**—This feature is supported on all high-end SRX Series devices.

  The computational overhead for a complete SSL handshake and master key generation can be considerable. To reduce overhead, you can use session resumption with SSL proxy to cache session parameters such as the pre-master secret key, selected ciphers, and so forth. When a subsequent connection is attempted, the client and server can resume the previous session by specifying its session ID.

  With session renegotiation, you can modify SSL parameters for a connection. Session renegotiation can be used to refresh cipher keys for a prolonged SSL session.

  [*SSL Proxy Overview*]

Chassis Cluster

- **Logical interface scaling**—On all high-end SRX Series devices, chassis cluster failover performance has been optimized to scale with more logical interfaces.

  During redundancy group failover, Generic Attribute Registration Protocol (GARP) is sent on each logical interface to steer the traffic to the appropriate node. GARP was sent by the Juniper Services Redundancy Protocol (jsrpd) process running in the Routing Engine in the previous release of Junos OS.

  With logical interface scaling, the Routing Engine becomes the checkpoint and GARP is directly sent from the Services Processing Unit (SPU).

  [*Understanding Chassis Cluster Redundancy Group Failover*]

Flow and Processing

- **Network processor offloading**—This feature is supported on SRX3400, SRX3600, SRX5600, and SRX5800 devices.

  With this feature, when a network processor fails to identify a session for a packet, it sends the packet to a selected SPU instead of forwarding the packet to a central point. The network processor forwards packets to SPUs based on certain algorithms. This approach avoids overloading of the central point. To enable network processor offloading, use the **set security forwarding-process application-services session-distribution-mode hash-based** command.

  NOTE:
  - You must reboot the device for the configuration to take effect.
  - Currently network processor offloading is supported only on IPv4 traffic.

  [*SRX5600 and SRX5800 Services Gateways Processing Overview*]

  [*Junos OS CLI Reference*]

- **Transparent mode support for IPv6 flows**—This feature is supported on all high-end SRX Series devices.

  In transparent mode, the SRX Series device filters packets that traverse the device without modifying any of the source or destination information in the packet MAC headers. Transparent mode is useful for protecting servers that mainly receive traffic from untrusted sources because there is no need to reconfigure the IP settings of routers or protected servers. In Junos OS Release 12.1X44-D10, IPv6 traffic is supported for transparent mode on the specified SRX Series devices.

A device operates in Layer 2 transparent mode when all physical interfaces on the device are configured as Layer 2 interfaces. There is no command to define or enable transparent mode on the device. The device operates in transparent mode when there are interfaces defined as Layer 2 interfaces. The device operates in route mode (the default mode) if there are no physical interfaces configured as Layer 2 interfaces.

By default, IPv6 flows are dropped on security devices. To enable processing by security features such as zones, screens, and firewall policies, you must enable flow-based forwarding for IPv6 traffic with the **mode flow-based** configuration option at the [**edit security forwarding-options family inet6**] hierarchy level. A device reboot is required when you change the mode.

Configuring bridge domains and Layer 2 logical interfaces for IPv6 flows is the same as configuring bridge domains and Layer 2 logical interfaces for IPv4 flows. You can optionally configure an integrated routing and bridging (IRB) interface for management traffic in a bridge domain. The IRB interface is the only Layer 3 interface allowed in transparent mode. The IRB interface on the SRX Series device does not support traffic forwarding or routing. The IRB interface can be configured with both IPv4 and IPv6 addresses.

[*Understanding IPv6 Flows in Transparent Mode*]

- **64-bit support for Junos OS security features**—This feature is supported on all high-end SRX Series devices.

  The 64-bit support increases the session scalability for both the SPC and the central point. The exact increase in the session scalability also depends on whether IDP is enabled or not for the application and on the configuration such as combo Services Processing Unit (SPU). The 64-bit support also increases the capacity for various services such as NAT, ALG, GTP, and so on.

General Packet Radio Service (GPRS)

- This feature is supported on all high-end SRX Series devices.

  A GPRS support node (GSN) identifies a Mobile Station (MS) by its International Mobile Subscriber Identity (IMSI). An IMSI consists of three elements: the mobile country code (MCC), the mobile network code (MNC), and the Mobile Subscriber Identification Number (MSIN). The MCC and MNC combined constitute the IMSI prefix and identify the mobile subscriber’s home network, or public land mobile network (PLMN).

  By setting IMSI prefixes, you can configure the device to deny GPRS tunneling protocol (GTP) traffic coming from nonroaming partners. By default, a device does not perform IMSI prefix filtering on GTP packets.

  This feature extends the length of the IMSI filter length from 5 or 6 digits to 15 digits, which is the full length for the IMSI filter. You can set the IMSI prefix as a wildcard character (*) or enter any digit from 0 to 9.

NOTE: If the IMSI prefix string is less than 15 digits, then the wildcard character (*) automatically appends to the string. For example, if you enter 12345*, then the device displays an invalid entry.

- **GTP APN filtering**—A device can filter GTP packets based on the combination of an IMSI prefix and an access point name (APN). When you filter GTP packets based on an IMSI prefix, you must also specify an APN.

  An APN string is case-insensitive. For instance, in the following example you set two APN strings, WWW.SINA.COM.CN and www.sina.com.cn, with the same IMSI prefix value, the lowercase string will display after the uppercase string, and the packet will be dropped.

  ```
  user@host# edit security gprs gtp profile test apn WWW.SINA.COM.CN imsi-prefix *
    action pass
  user@host# edit security gprs gtp profile test apn www.sina.com.cn imsi-prefix *
    action drop
  ```

  To view the output, use the following command:

  ```
  user@host> show configuration security gprs gtp profile test
  ```

  If an APN is configured with two IMSI prefix entries, then the IMSI prefix with the longest match takes priority. For example, see the following configuration:

  ```
  user@host# edit security gprs gtp profile test apn WWW.SINA.COM.CN imsi-prefix
    12345678 action pass
  user@host# edit security gprs gtp profile test apn www.sina.com.cn imsi-prefix 12345
    action drop
  ```

  To view the output, use the following command:

  ```
  user@host> show configuration security gprs gtp profile test
  ```

  If an incoming packet value matches the IMSI prefix value 12345678, then the packet will pass. The IMSI prefix value 12345678 takes precedence over the IMSI prefix value 12345, because the longest matched IMSI prefix takes priority.

[*General Packet Radio Service for Security Devices*]

- **SCTP optimization for carriers (packet drop and stability)**—This feature is supported on all high-end SRX Series devices.

  Stream Control Transmission Protocol (SCTP) is used in carrier networks for the transport of telephony (Signaling System 7) protocols over IP addresses, with the goal of duplicating some of the reliability attributes of the SS7 signaling network in IP addresses.

  SCTP optimization is done to:

  - Avoid the multithread infrastructure problems, when the traffic is high
  - Improve the SCTP association searching rate (association lookup process speed is increased) by SCTP hash table optimization on the SPU
  - Improve finite state machine (FSM) for retransmission cases

NOTE: Because there is no dynamic policy for SCTP, you must configure all policies for the required SCTP sessions.

To view the SCTP associations, use the **show security gprs sctp association** command.

[*Understanding Stream Control Transmission Protocol*]

[*show security gprs sctp association*]

[*Junos OS CLI Reference*]

- **SGSN roaming in GGSN pooling scenarios**—This feature is supported on all high-end SRX Series devices.

  This feature allows the General Packet Radio Service (GPRS) tunneling protocol (GTP) to support different Gateway GPRS Support Node (GGSN) IP addresses when creating tunnels.

  This feature supports the following two pooling scenarios:

  Scenario 1: GGSN uses a response packet's source IP address that is different from the request packet's destination IP address to send a response message to the Serving GPRS Support Node (SGSN).

  Scenario 2: SGSN or GGSN uses a response packet's source IP address that is different from the payload GSN IP address for the GGSN tunneling protocol, control (GTP-C) and GGSN tunneling protocol, user plane (GTP-U) tunnel creation procedures.

  [*General Packet Radio Service*]

  [*General Packet Radio Service for Security Devices*]

Services Processing Card SRX5K-SPC-4-15-320 Features

- **Next-generation Services Processing Card (SPC)**—Junos OS Release 12.1X44-D10 supports a next-generation Services Processing Card (SPC) (SRX5K-SPC-4-15-320) on SRX5600 and SRX5800 devices.

  The next-generation SPC uses a high-performance, multicore and multithreaded processor to enhance firewall, IPsec, and IDP services to scale in capacity and performance.

  The SRX5K-SPC-4-15-320 is a next-generation Services Processing Card (SPC). It contains four Services Processing Units (SPUs), as opposed to the two SPUs of the earlier SRX5K-SPC-2-10-40 SPC. It also offers higher per-SPU performance than the older SPC.

  If your services gateway contains a mix of SRX5K-SPC-4-15-320 SPCs and SRX5K-SPC-2-10-40 SPCs, an SRX5K-SPC-4-15-320 SPC must occupy the lowest-numbered slot of any SPC in the chassis. This configuration ensures that the central point (CP) function is performed by the faster and higher-performance SPC type.

NOTE:

- You must have high-capacity power supplies (either AC or DC) and high-capacity fan trays installed in the services gateway in order to install and use SRX5K-SPC-4-15-320 SPCs. On the SRX5800 Services Gateway, you must also install the high-capacity air filter. If you do not have high-capacity power supplies and fan trays installed, the services gateway will log an alarm condition when it recognizes the SRX5K-SPC-4-15-320 SPCs.
- On SRX5600 Services Gateways with AC power supplies, we recommend that you use high-line (220v) input power to ensure the device has adequate power to support SRX5K-SPC-4-15-320 SPCs.

SPCs are common form-factor module (CFM) cards that provide the processing power to run integrated services such as firewall, IPsec, and IDP. All traffic traversing the services gateway is passed to an SPC to have services processing applied to it. Traffic is intelligently distributed by Network Processing Cards (NPCs) to SPCs for services processing, including session setup based on policies, fast-packet processing for packets that match a session, encryption and decryption, and IKE negotiation.

Note the following specifics about next-generation SPCs:

- Next-generation SPCs have four SPUs per card. The central point (CP) and Services Processing Unit (SPU) combo mode is not supported.
- Next-generation SPCs must always be plugged into the lowest-numbered slot of the SRX-series device.
- Combination of next-generation SPC and existing SPCs is supported. Make sure that the first SPC in the lowest slot of the chassis should be a next-generation SPC. This could be followed by existing SPCs or other next-generation SPCs in any order.

Next-generation SPCs support all the existing chassis cluster functionality. If your SRX5600 or SRX5800 device is part of a chassis cluster:

- Junos OS software upgrade cannot be done at the same time as SPC hardware upgrade. If both software and hardware need to be upgraded, the software update must be done first before proceeding to the hardware upgrade.
- Installing additional NG-SPC on the devices in the cluster without incurring downtime on the network is supported. However, during this installation procedure, you must shut down both nodes, one at a time.
- Replacing a next-generation SPC with an earlier SPC is not supported.
- Removal of any type of SPC from a chassis cluster setup is not supported without traffic disruption.
- SPC expansion should be added to a slot that has a higher number than the central point slot.

The following features are enhanced on SRX5600 and SRX5800 devices with the introduction of the next-generation SPC:

- Enhanced performance and increased scaling capacity
- Support for dynamic tunnel distribution scheme
- Enhanced NAT scaling capacity as follows:
  - NAT rule set and rule:

Table 11: NAT Rule Set and Rule

Objects	Scaling Capacity
Total NAT rule sets per system	30,720
Total NAT rules per rule set	30,720

  - Persistent NAT binding capacity:

Table 12: Persistent NAT Binding Capacity

Objects	Scaling Capacity
CP bindings on CP	2,097,152
SPU bindings on SPU	524,288

- Increase in maximum number of supported security policies (up to 80,000), address-books (up to 2000 for SRX5600 and up to 4000 for SRX5800) and zones (up to 2000 for SRX5600 and up to 4000 for SRX5800).
- Increase in maximum number of allowed firewall authentication entries to 50,000
- Increased ALGs session capacity as follows:

Table 13: Increased ALGs Session Capacity

ALGs	Maximum Supported Sessions
FTP/TFTP Layer 2 and Layer 3 for ALG per SPU	50,000
RTSP Layer 2 Mode for ALG per SPU	50,000
RTSP Layer 3 Mode for ALG per SPU	50,000

- In-service software upgrade (ISSU) support
- J-Web support

You can use the **show chassis hardware** and **show chassis fpc** commands to display the information about NG-SPC.

[*SRX5600 Services Gateway Hardware Guide*]

[*SRX5800 Services Gateway Hardware Guide*]

J-Web

- **J-Web webserver upgrade to 3.2**—This feature is supported on all high-end SRX Series devices.

  The internal J-Web webserver version is upgraded, providing both security and performance improvements.

Logical Systems

- **Display and clear the DNS cache in the master logical system**—This feature is supported on all high-end SRX Series devices.

  The master administrator can use the CLI operational command **show security dns-cache** to display all DNS cache information or to display DNS cache information for a specific name. The master administrator can use the **clear security dns-cache** command to clear all DNS cache information or clear DNS cache information for a specific name. The master administrator can use these commands to verify the resolved IP address of a DNS name and invalidate the addresses if needed.

  NOTE: These commands are not available in user logical systems or on devices that are not configured for logical systems.

  [*Junos OS CLI Reference*]

Network Address Translation (NAT)

- **Increase in the maximum sessions allowed for a persistent NAT binding**—This feature is supported on all high-end SRX Series devices.

  Previously, the maximum number of sessions allowed for a persistent NAT binding was 100. This limit is now 65,536. You can now configure the maximum number of sessions ranging from 8 through 65,536.

  [*max-session-number*]

  [*Junos OS CLI Reference*]

- **Scalability improvements to persistent NAT**—This feature is supported on all high-end SRX Series devices.

  Users can now increase the persistent NAT binding capacity to a maximum of 2 million on the central point and 275,000 per SPU on the SRX5800 device.

  To maximize the persistent NAT binding capacity, use the **set security forwarding-process application-services maximize-persistent-nat-capacity** command.

  If you want to achieve maximum value of 2 million binding capacity, then you need to enable central point session maximum using the **set security forwarding-process application-services maximize-cp-session** command.

  To restore the persistent NAT binding capacity to default value, use the **delete security forwarding-process application-services maximize-persistent-nat-capacity** command.

You must reboot the device for the configuration to take effect. Using this optimization technique reduces the number of flow sessions on both the central point and the SPU.

[*Example: Setting Maximum Persistent NAT Bindings*]

[*Junos OS CLI Reference*]

- **Static NAT support for port mapping**—This feature is supported on all high-end SRX Series devices.

  Static NAT defines a one-to-one mapping from one IP subnet to another IP subnet. The existing static NAT functionality is enhanced to support the following types of translation:

  - To map multiple IP addresses and specified ranges of ports to the same IP address and a different range of ports
  - To map a specific IP address and port to a different IP address and port

  The new CLI statements **destination-port *low* to *high*** and **mapped-port *low* to *high*** are introduced as part of this enhancement.

  [*Example: Configuring Static NAT for Port Mapping*]

Security Policies

- **Firewall authentication support for HTTPS traffic**—This feature is supported on all high-end SRX Series devices.

  Firewall authentication now supports the HTTPS protocol along with FTP, HTTP, and Telnet. This feature enhances HTTPS support for Web authentication. Unauthenticated HTTPS traffic is redirected to the Web authentication IP addresses of the incoming interfaces.

  The following new CLI statements are part of this feature:

  - **ssl-termination-profile**—Specify the name of the SSL termination profile used for SSL offloading.
  - **web-redirect-to-https**—Redirect unauthenticated HTTP requests to the device's internal HTTPS webserver. If **web-redirect-to-https** is configured, the firewall redirects the unauthenticated HTTP traffic to the HTTPS Web authentication server's incoming interface .
  - **https**—Enable authentication through HTTPS. If **https** is selected, the system allows Web authentication for HTTPS traffic.
  - **redirect-to-https**—Redirect the HTTP Web authentication traffic to the HTTPS Web authentication service.

  [*Firewall User Authentication for Security Devices*]

- **New match criteria for user role firewall policies**—This feature is supported on all high-end SRX Series devices.

  User role firewall policies can now specify the username as match criteria in the source-identity field. In the previous release, roles were the only valid input for the source-identity field. Roles are now considered optional.

Two additional show commands display the users and the combined users and roles that are specified in the user identification tables (UITs) and available for user and role provisioning:

- **show security user-identification user-provision all**
- **show security user-identification source-identity-provision all**

In addition, the connection setup rate has been improved when a user role firewall is enabled.

[*Understanding User Role Firewalls*]

- **Shadow policy check**—This feature is supported on all high-end SRX Series devices.

  You can now check if there is any policy shadowing in the policy list using the following CLI commands:

  - For logical systems, run the **show security shadow-policies logical-system *lsys-name* from-zone *from-zone-name* to-zone *to-zone-name* policy *policy-name* reverse** command.
  - For global policies, run the **show security shadow-policies logical-system *lsys-name* global policy *policy-name* reverse** command.

    The CLI commands can be used to display:

    - All shadow policies within a context
    - If a given policy shadows one or more policies
    - If a given policy is shadowed by one or more policies

  [*Understanding Security Policy Ordering*]

  [*Verifying Shadow Policies*]

  [*show security shadow-policies logical-system*]

  [*Junos OS CLI Reference*]

Services Offloading

This feature is supported on SRX1400, SRX3400, and SRX3600 devices.

Services offloading now supports the following:

- Per-wing statistics counters—The network processor in services-offload mode provides the option for each flow entry to keep a per-wing bytes counter. The counter captures the number of bytes that the network processor sends out over the wing. You can configure the statistics counter feature for each PIC.
- Services-offload traffic across different network processors—Services offloading now provides additional cross-network-processor support; therefore, it is not restricted to the ports of the same network processor.
- NP-IOC support—The NP-IOC is a new type of card that integrates an existing IOC with a Network Processing Card (NPC) in one card with simplified Layer 2 functions in the hardware.

- Session scale up for NP-IOC in services-offload mode—The NP-IOC has a larger static RAM (SRAM) to accommodate session resources, thus hosting more sessions per PIC.
- End-to-end debugging in services-offload mode—For regular flow packets, end-to-end debugging functions are the same as in the non-services-offload mode; packet filter and action items are supported in this flow mode. For traffic that matches services-offload sessions, the end-to-end debugging function supports one packet copy to host CPU when the filter and the action are both affirmative in the end-to-end search results.

System Logs

The following system logs are introduced in Junos OS Release 12.1X44-D10:

- **PKID_CERT_BASIC_CNSTRS_MISSING**—Certificate does not have the basic constraints field.
- **PKID_CERT_BASIC_CNSTRS_INV_CA**—Certificate does not have a valid CA flag.
- **ERRMSG(PKID_CERT_BASIC_CNSTRS_MISSING, LOG_ERR**—Basic constraints field is missing for the CA certificate <certificate-subject>.
- **ERRMSG(PKID_CERT_BASIC_CNSTRS_INV_CA, LOG_ERR**—Basic constraints field contains an invalid CA flag for the CA certificate <certificate-subject>.
- **PKID_CERT_NOT_BEFORE_FAIL**—Certificate /C=US/DC=juniper/ST=CA/L=Sunnyvale/O=PKI/OU=SSD/CN=bubba is not valid until 06-12-2012 21:44.
- **PKID_CERT_NOT_AFTER_FAIL**—Certificate /C=US/DC=juniper/ST=CA/L=Sunnyvale/O=PKI/OU=SSD/CN=bubba has expired, not valid after 06-12-2014 .21:44
- **PKID_CERT_ID_LOOKUP_FAIL**—Certificate chain does not contain certificate with ID 30.1.1.31 and Type IPSEC_ID_IPV4_ADDR.
- **PKID_CERT_ID_LOOKUP_FAIL**—Certificate chain does not contain certificate with ID /C=US/DC=juniper/ST=CA/L=Sunnyvale/O=PKI/OU=SSD/CN=bubba and Type IPSEC_ID_DER_ASN1_DN.
- **PKID_CERT_ID_LOOKUP_FAIL**—Certificate chain does not contain certificate with ID bubba@juniper.net and Type IPSEC_ID_USER_FQDN.
- **PKID_CERT_ID_LOOKUP_FAIL**—Certificate chain does not contain certificate with ID bubba.juniper.net and Type IPSEC_ID_FQDN.

Virtual Private Network (VPN)

- **AutoVPN**—AutoVPN hubs are supported on all high-end SRX Series devices. AutoVPN spokes are supported on SRX1400 devices.

  AutoVPN allows network administrators to configure the hub in a hub-and-spoke IPsec VPN topology for current and future client device connections. Configuration changes are not required on the hub when spoke devices are added or deleted, thus allowing administrators flexibility in managing large-scale network deployments.

  AutoVPN is supported on route-based IPsec VPNs. AutoVPN traffic must be IPv4. Dynamic routing protocols are supported to forward packets through the VPN tunnels.

  NOTE: The RIP dynamic routing protocol is not supported with AutoVPN in Junos OS Release 12.1X44-D10 and 12.1X44-D15.

  The supported authentication for AutoVPN hubs and spokes is X.509 public key infrastructure (PKI) certificates. The group IKE user type configured on the hub allows strings to be specified to match the alternate subject field in spoke certificates. Partial matches for the subject fields in spoke certificates can also be specified.

  AutoVPN is configured and managed on SRX Series devices using the CLI. Multiple AutoVPN hubs can be configured on a single SRX Series device. The maximum number of spokes supported by a configured hub is specific to the model of the SRX Series device. AutoVPN supports VPN monitoring and dead peer detection.

  [*AutoVPNs for Security Devices*]

- **Improvements in VPN debugging capabilities**—This feature is supported on all high-end SRX Series devices.

  The following enhancements are now available to improve the VPN debugging capabilities:

  - The debugging of tunnels was limited to the policy manager previously, is now extended to include QuickSec software stacks.
  - The **show security ipsec security-associations detail** command is enhanced to provide information such as VPN name, tunnel ID, and bind interface in the security associations (SAs) output.
  - The **show security ike security-associations detail** command is enhanced to provide gateway name and Diffie-Hellman (DH) group information in the SA output.
  - The **show security ipsec security-associations vpn-name *vpn-name*** command displays the IPsec SA based on the VPN name. For policy-based VPNs and dial-up VPNs, the output displays multiple SAs because VPN names are shared.
  - The new **show security ipsec inactive-tunnels** command displays security information about the inactive tunnels.
  - The new **request security ike (debug-enable | debug-disable)** command enables IKE debugging through operational mode commands.
  - The common log location for all SRX Series devices is now **/var/log/*log-filename***.

NOTE: If you do not specify the log filename for the *log-filename* field, then all logs are written to the kmd log.

[*Junos OS CLI Reference*]

- **VPN session affinity**—This feature is supported on all high-end SRX Series devices.

  VPN session affinity occurs when a cleartext session is located in a Services Processing Unit (SPU) that is different from the SPU where the IPsec tunnel session is located. The goal of VPN session affinity is to locate the cleartext and IPsec tunnel session in the same SPU.

  Without VPN session affinity, a cleartext session created by a flow might be located in one SPU and the tunnel session created by IPsec might be located in another SPU. An SPU to SPU forward or hop is needed to route cleartext packets to the IPsec tunnel.

  By default, VPN session affinity is disabled on SRX Series devices. When VPN session affinity is enabled, a new cleartext session is placed on the same SPU as the IPsec tunnel session. Existing cleartext sessions are not affected.

  Enabling VPN session affinity can improve VPN throughput under the following traffic conditions:

  - A number of IPsec tunnels are needed and the tunnels are distributed evenly among SPUs. If IPsec tunnels are already concentrated on several SPUs, then enabling VPN session affinity allows all cleartext SPUs to also use those SPUs. This can cause those SPUs to be overutilized while other SPUs might be underutilized.

    To display active tunnel sessions on SPUs, use the **show security ipsec security-association** command and specify the Flexible PIC Concentrator (FPC) and Physical Interface Card (PIC) slots that contain the SPU.

  - Cleartext sessions passing through the tunnels should be at the highest volume for the longest periods of time as possible. Applying VPN session affinity to cleartext sessions of small volumes and short periods (for example, DNS sessions) will decrease the effect of session affinity and might even have a negative impact on VPN throughput under certain conditions.

  [*IPsec VPNs for Security Devices*]

- **VPN support for inserting Services Processing Cards**—This feature is supported on SRX3400, SRX3600, SRX5600, and SRX5800 devices.

  These high-end SRX Series devices have a chassis-based distributed processor architecture. The flow processing power is shared and is based on the number of Services Processing Cards (SPCs). You can scale the processing power of the device by installing a new SPC. Previously, whenever you installed a new SPC on a device either in standalone mode or in chassis cluster mode, the distributed VPNs on the device were disrupted.

  This feature enables you to insert an SPC on a device in a chassis cluster without disrupting the traffic on the existing VPN tunnels created by the IKE and IPsec workload.

Now when you insert a new SPC in each chassis of the cluster, the existing tunnels are not affected and traffic continues to flow over them without any disruption.

However, existing tunnels cannot use the processing power of the new SPC and redistribute it to the new SPC. The newly inserted SPC can anchor the newly configured site-to-site tunnels and dynamic tunnels. The newly configured tunnels are not guaranteed to be anchored on the new SPC.

Site-to-site tunnels are anchored on different SPCs based on a load-balancing algorithm. For site-to-site tunnels, the least-loaded SPC is chosen as the anchor SPC. If multiple SPCs have the same smallest load, then any SPC can be chosen as the anchor SPC. The newly configured site-to-site tunnels are guaranteed as primary on the new SPC only if the load of the old SPCs is all greater than 0. The load corresponds to the number of site-to-site gateways or manual VPN tunnels anchored on an SPC.

Dynamic tunnels are anchored on different SPCs based on a round-robin algorithm. The newly configured dynamic tunnels are not guaranteed to be anchored on the new SPC.

After inserting the SPC in a chassis cluster, you can view the tunnel mapping on different Services Processing Units (SPUs) using the **show security ike tunnel-map** command. You can only display the primary information of site-to-site VPN tunnels and manual VPN tunnels with this command.

After the dynamic tunnel is established, you can display the primary information of dynamic tunnels using the **show security ike sa detail** command.

[*VPN for Security Devices*]

- **Loopback interface for chassis cluster VPN**—This feature is supported on all high-end SRX Series devices.

  An Internet Key Exchange (IKE) gateway needs an external interface to communicate with a peer device. In a chassis cluster setup, the node on which the external interface is active selects a Services Processing Unit (SPU) to support the VPN tunnel. IKE and IPsec packets are processed on that SPU. Therefore, the active external interface determines the anchor SPU.

  In a chassis cluster setup, this external interface can be the redundant Ethernet interface or a standalone interface. These interfaces can go down when the physical interfaces are down. Therefore, loopback interfaces can be used to reach the peer gateway because the loopback interfaces are alternate physical interfaces.

  This feature allows the loopback interface to be configured for any redundancy group. This redundancy group configuration is only checked for VPN packets, because only VPN packets must find the anchor SPU through the active interface.

  On high-end SRX Series devices, the lo0 pseudointerface cannot be configured in RG0 when it is used as an IKE gateway external interface. Because a VPN is only supported in an active/passive chassis cluster environment on high-end SRX Series devices, the lo0 pseudointerface can be configured in such a setup for RG1. In a chassis cluster setup, the node on which the external interface is active selects an SPU to anchor the VPN tunnel. IKE and IPsec packets are processed on that SPU. Thus an active external interface determines the anchor SPU.

You can use the **show chassis cluster interfaces** command to view the redundant pseudointerface information.

[*VPN for Security Devices*]

Related Documentation

- Outstanding Issues in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 150
- Resolved Issues in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 153
- Errata and Changes in Documentation for Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 172
- Changes in Default Behavior and Syntax in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 123
- Known Limitations in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 134

Changes in Default Behavior and Syntax in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways

The following current system behavior, configuration statement usage, and operational mode command usage might not yet be documented in the Junos OS documentation:

Application Firewall

- Prior to Junos OS release 11.4R6, when a rule specifies **dynamic-application junos:HTTP** without specifying any other nested application, the rule matches all HTTP traffic whether the traffic contains a nested application or not.

  In Junos OS release 11.4R6 and later, that functionality has changed. When a rule specifies **dynamic-application junos:HTTP**, only HTTP traffic with no nested members is matched.

  Consider the following application firewall ruleset:

  ```
  rule-sets http-ruleset {
     rule rule1 {
        match {
           dynamic-application [junos:FACEBOOK];
        }
        then {
           deny;
        }
     }
     rule rule2 {
        match {
           dynamic-application [junos:HTTP];
        }
        then {
           permit;
        }
     }
     default-rule {
        deny;
     }
  }
  ```

  Prior to Junos OS release 11.4R6, the sample rules would be applied to traffic as shown in the following list:

  - HTTP traffic with junos:FACEBOOK as a nested application would be denied by rule1.
  - HTTP traffic with no nested application would be permitted by rule2.
  - HTTP traffic with a nested application other than junos:FACEBOOK, such as junos:TWITTER, would be permitted by rule2 because it is HTTP traffic that does not match any previous rule.

  After Junos OS release 11.4R6, the dynamic application junos:HTTP matches only the traffic that does not contain a recognizable nested application. The sample rules would now be applied differently:

  - HTTP traffic with junos:FACEBOOK as a nested application would be denied by rule1.
  - HTTP traffic with no nested application would be permitted by rule2.
  - However, HTTP traffic with a nested application other than junos:FACEBOOK, such as junos:TWITTER, would no longer match rule2. Instead, the traffic would be denied by the default rule.

AppSecure Application Package Upgrade Changes

- **Application signatures removed after upgrading to Junos OS Release 11.4**—This change applies to all high-end SRX Series devices that use the application identification signature package.

  As of Junos OS Release 11.4, the application signature package is downloaded and installed in a separate database, not in the Junos OS configuration file as in previous Junos OS releases.

  When you upgrade an SRX Series device from Junos OS Release 11.2 to Junos OS Release 11.4 or later, any predefined application signatures and signature groups from the Junos OS Release 11.2 configuration will be removed when you install the latest predefined signatures and signature groups by using the **request services application-identification install** command. However, the upgrade will not remove custom signatures and signature groups from the Junos OS configuration.

  For information about using the **request services application-identification download** and **request services application-identification install** commands, see the *Junos OS CLI Reference*.

Command-Line Interface (CLI)

New or Changed CLI

- The **client-match** ***match-name*** option under security hierarchy [**edit security policies from-zone** ***zone-name*** **to-zone** ***zone-name*** **policy** ***policy-name*** **then permit firewall-authentication**] now supports a maximum of 64 users or user groups in the policy.
- On all high-end SRX Series devices, the **show interface** ***interface-name*** **statistics detail** command was showing incorrect FCS statistics. Additional 4 bytes in the FCS were counted in input statistics but not counted in output statistics. Now the FCS is included in both input and output Ethernet statistics and the **show interface** ***interface-name*** **statistics detail** command displays correct output.
- On all high-end SRX Series devices, a new command, **clear security flow statistics**, has been introduced to clear the flow-related system statistics.
- On all branch SRX Series devices, the **show security flow session extensive** command has been updated to show the predefined application name.
- On all high-end SRX Series devices, on Services Processing Cards (SPC) and next-generation SPCs, IDP dedicated modes are supported only with the **inline-tap** option. In the inline-tap mode option, the **weight equal** option is not supported.

  Other IDP dedicated mode configurations such as dedicated weight IDP, dedicated firewall, and dedicated equal are not supported.

  The following IDP dedicated mode configuration statements are not supported:

  - **set security forwarding-process application-services maximize-idp-sessions weight firewall**
  - **set security forwarding-process application-services maximize-idp-sessions weight idp**
  - **set security forwarding-process application-services maximize-idp-sessions weight equal**
  - **set security forwarding-process application-services maximize-idp-sessions inline-tap weight equal**

- The following configuration statements are supported:
  - **set security forwarding-process application-services maximize-idp-sessions inline-tap weight firewall**
  - **set security forwarding-process application-services maximize-idp-sessions inline-tap weight idp**

Deprecated Items for High-End SRX Series Services Gateways

Table 14 on page 126 lists deprecated items (such as CLI statements, commands, options, and interfaces).

CLI statements and commands are deprecated—rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration. We strongly recommend that you phase out deprecated items and replace them with supported alternatives.

Table 14: Items Deprecated in Release 12.1

Deprecated Item	Replacement	Hierarchy Level or Command Syntax	Additional Information
download-timeout	-	download-timeout timeout	On all high-end SRX Series devices, the **download-timeout** command is deprecated. If the configuration is present, then the configuration is ignored. The idpd daemon internally triggers the security package to install when an automatic download is completed. There is no need to configure any download timeout.
node	-	request security idp security-package download	On all high-end SRX Series devices operating in a chassis cluster, the following **request security idp security-package download** commands with the **node** option is not supported: • **request security idp security-package download node primary** • **request security idp security-package download node local** • **request security idp security-package download node all**

Table 15: Items Deprecated in Junos OS Release 12.1X44-D10

Deprecated Item	Replacement	Hierarchy Level or Command Syntax	Additional Information
mcc-mnc	imsi-prefix	**edit security gprs gtp profile profile-name apn pattern-string**	On all high-end SRX Series devices, the **mcc-mnc** command is not supported.

Compatibility

- **Version Compatibility for Junos SDK**—Beginning with Junos OS Release 12.1X44-D10, Junos OS applications will install on the Junos OS only if the application is built with the same release as the Junos OS Release on which the application is being installed.

  For example, an application built with Junos OS Release 12.1R2 will only install on Junos OS Release 12.1R2 and will not install on Junos OS Release 12.1R1 or Junos OS Release 12.1R3.

Flow and Processing

SPU software changes for the SPC—The following changes apply to all high-end SRX Series devices:

- Each SPU runs a 64-bit FreeBSD kernel instead of the 32-bit FreeBSD kernel.
- Each SPU runs a 64-bit flowd instead of the 32-bit version for increased scalability.
- With the 64-bit OS, ksynd and ifstates on the SPU run in 64-bit mode.

- **TCP initial timeout enhancement**–The minimum value you can configure for TCP session initialization is 4 seconds. The default value is 20 seconds; if required you can set the TCP session initialization value to less than 20 seconds.

Intrusion Detection Prevention (IDP)

- On all high-end SRX Series devices, unsupported IDP dedicated mode commands, which are supported in releases earlier than Junos OS Release 12.1X44, allow a blank password for Telnet, J-Web, or Console access connections; and accept any random password for SSH connection after upgrading to Junos OS Release 12.1X44-D10 or 12.1X44-D11.

  As a workaround:

  - Before upgrading to Junos OS Release 12.1X44-D10, remove the unsupported IDP dedicated mode commands and then upgrade the release to Junos OS Release 12.1X44-D10.
  - Check the configuration compatibility between releases earlier than Junos OS Release 12.1X44 and Junos OS Release 12.1X44-D10 using the **request system software validate <12.1X44-install-package>**command.

  - Remove the unsupported IDP dedicated mode commands or change the IDP mode from dedicated mode to in-line tap mode.
  - Upgrade to Junos OS Release 12.1X44 using the **request system software add no-copy junos-srx1k3k-12.1X44-D11.5-domestic.tgz reboot** command.

- New sensor configuration options have been added to log run conditions as IDP session capacity and memory limits are approached, and to analyze traffic dropped by IDP and application identification due to exceeding these limitations.

  - At start up, traffic is ignored by IDP by default if the IDP policy is not yet loaded. The **drop-if-no-policy-loaded** option changes this behavior so that all sessions are dropped before the IDP policy is loaded.

    Use the following configuration command to drop traffic before the IDP policy is loaded:

    ```
    set security idp sensor-configuration flow drop-if-no-policy-loaded
    ```

    The following new counters have been added to the **show security idp counters flow** command output to analyze dropped traffic due to the **drop-if-no-policy-loaded** option:

    ```
    Sessions dropped due to no policy                    0
    ```

  - By default, IDP ignores failover sessions in an SRX chassis cluster deployment. The **drop-on-failover** option changes this behavior and automatically drops sessions that are in the process of being inspected on the primary node when a failover to the secondary node occurs.

    Use the following configuration command to drop failover sessions:

    ```
    set security idp sensor-configuration flow drop-on-failover
    ```

    The following new counter has been added to the **show security idp counters flow** command output to analyze dropped failover traffic due to the **drop-on-failover** option:

    ```
    Fail-over sessions dropped                           0
    ```

  - By default, sessions are not dropped if the IDP session limit or resource limits are exceeded. In this case, IDP and other sessions are dropped only when the device's session capacity or resources are depleted. The **drop-on-limit** option changes this behavior and drops sessions when resource limits are exceeded.

    Use the following configuration commands to set or remove the **drop-on-limit** option:

    ```
    set security idp sensor-configuration flow drop-on-limit
    delete security idp sensor-configuration flow drop-on-limit
    ```

    The following new counters have been added to the **show security idp counters flow** command output to analyze dropped IDP traffic due to the **drop-on-limit** option:

    ```
    SM Sessions encountered memory failures              0

    SM Packets on sessions with memory failures          0

    SM Sessions dropped                                  0

    Both directions flows ignored                        0
    ```

```
IDP Stream Sessions dropped due to memory failure      0
IDP Stream Sessions ignored due to memory failure      0
IDP Stream Sessions closed due to memory failure       0
Number of times Sessions exceed high mark              0
Number of times Sessions drop below low mark           0
Memory of Sessions exceeds high mark                   0
Memory of Sessions drops below low mark                0
```

The following counters have also been added to the **show security idp counters application-identification** command output to analyze dropped application identification traffic due to the **drop-on-limit** option:

```
AI-session dropped due to malloc failure before session create       0
AI-Sessions dropped due to malloc failure after create               0
AI-Packets received on sessions marked for drop due to malloc failure 0
```

The following options have been added to trigger informative log messages about current run conditions. When set, the log messages are triggered whether the **drop-on-limit** option is set or not.

- The **max-sessions-offset** option sets an offset for the maximum IDP session limit. When the number of IDP sessions exceeds the maximum session limit, a warning is logged that conditions exist where IDP sessions could be dropped. When the number of IDP sessions drops below the maximum IDP session limit minus the offset value, a message is logged that conditions have returned to normal.

  ```
  Jul 19 04:38:13 4.0.0.254 RT_IDP: IDP_SESSION_LOG_EVENT: IDP: at 1374233893,
   FPC 4 PIC 1 IDP total sessions pass through high mark 100000. IDP may drop
   new sessions. Total sessions dropped 0.
  Jul 19 04:38:21 4.0.0.254 RT_IDP: IDP_SESSION_LOG_EVENT: IDP: at 1374233901,
   FPC 4 PIC 1 IDP total sessions drop below low mark 99000. IDP working in
  normal mode. Total sessions dropped 24373.
  ```

  Use the following configuration command to set the **max-sessions-offset** option:

  set security idp sensor-configuration flow max-sessions-offset ***offset-value***

- The **min-objcache-limit-lt** option sets a lower threshold for available cache memory. The threshold value is expressed as a percentage of available IDP cache memory. If the available cache memory drops below the lower threshold level, a message is logged stating that conditions exist where IDP sessions could be dropped because of memory allocation failures. For example, the following message shows that the IDP cache memory has dropped below the lower threshold and that a number of sessions have been dropped:

  ```
  Jul 19 04:07:33 4.0.0.254 RT_IDP: IDP_SESSION_LOG_EVENT: IDP: at 1374232053,
   FPC 4 PIC 1 IDP total available objcache(used 4253368304, limit 7247757312)
   drops below low mark 3986266515. IDP may drop new sessions. Total sessions
   dropped 1002593.
  ```

  Use the following configuration command to set the **min-objcache-limit-lt** option:

  set security idp sensor-configuration flow min-objcache-limit-lt ***lower-threshold-value***

    - The **min-objcache-limit-ut** option sets an upper threshold for available cache memory. The threshold value is expressed as a percentage of available IDP cache memory. If available IDP cache memory returns to the upper threshold level, a message is logged stating that available cache memory has returned to normal. For example, the following message shows that the available IDP cache memory has increased above the upper threshold and that it is now performing normally:

      ```
      Jul 19 04:13:47 4.0.0.254 RT_IDP: IDP_SESSION_LOG_EVENT: IDP: at 1374232428,
       FPC 4 PIC 1 IDP total available objcache(used 2782950560, limit 7247757312)
       increases above high mark 4348654380. IDP working in normal mode. Total
      sessions dropped 13424632.
      ```

      NOTE: **This message is triggered only if the lower threshold has been reached and the available memory has returned above the upper threshold. Fluctuations in available memory that dropped below the upper threshold but did not fall below the lower threshold would not trigger the message.**

      Use the following configuration commands to set the **min-objcache-limit-ut** option:

      ```
      set security idp sensor-configuration flow min-objcache-limit-ut
        upper-threshold-value
      ```

- By default, values for IDP reassembler packet memory and application identification packet memory used by IDP are established as percentages of all memory. In most cases, these default values are adequate.

  - If a deployment exhibits an excessive number of dropped TCP packets or retransmissions resulting in high IDP reassembly memory usage, use the following option:

    The **max-packet-mem-ratio** option to reset the percentage of available IDP memory for IDP reassembly packet memory. Acceptable values are between 5% and 40%.

    ```
    set security idp sensor-configuration re-assembler max-packet-mem-ratio
      percentage-value
    ```

  - If a deployment exhibits an excessive number of ignored IDP sessions due to reassembler and application identification memory allocation failures, use the following options:

    - The **max-packet-memory-ratio** option sets application identification packet memory limit as a percentage of available IDP memory. This memory is only used by IDP in cases where application identification delays identifying an application. Acceptable values are between 5% and 40%.

      ```
      set security idp sensor-configuration application-identification
        max-packet-memory-ratio percentage-value
      ```

    - The **max-reass-packet-memory-ratio** option sets the reassembly packet memory limit for application identification as a percentage of available IDP memory. Acceptable values are between 5% and 40%.

      ```
      set security idp sensor-configuration application-identification
        max-reass-packet-memory-ratio percentage-value
      ```

NOTE: The **max-packet-memory** option has been deprecated and replaced by the new **max-packet-memory-ratio** and **max-reass-packet-memory-ratio** options.

Junos OS Federal Information Processing Standard (FIPS)

- On all SRX Series devices, the secure Junos OS software environment does not permit DSA key pairs with modulus greater than 1024 bits.

Logical Systems

- The **logical-systems all** option can now be specified for the **show security screen statistics** operational command.

Management Information Base (MIB)

- On all high-end SRX Series devices in a chassis cluster, the calculation of the primary and secondary node sessions in the JnxJsSPUMonitoringObjectsTable object of the SPU monitoring MIB is incorrect. The MIB jnxJsSPUMonitoringCurrentTotalSession incorrectly displays total sessions.

  A doubled session count is displayed because the active and backup nodes are treated as separate sessions, although these nodes are not separate sessions.

  Count only the session numbers on the local node, thereby avoiding a double count, and local total sessions are displayed.

  The SPUMonitoringCurrentTotalSession object of the MIB adds information per each SPU from the local node.

  [*MIB Reference for SRX1400, SRX3400, and SRX3600 Services Gateways*]

  [*MIB Reference for SRX5600 and SRX5800 Services Gateways*]

Security Policies

- Security policies are stored in both the Routing Engine and the Packet Forwarding Engine. When you modify the policies on the Routing Engine side, the policies are synchronized to the Packet Forwarding Engine side when you commit the configuration.

  The policies in the Routing Engine and Packet Forwarding Engine must always be in synchronization for the configuration to commit successfully. Under certain circumstances, policies in the Routing Engine and the Packet Forwarding Engine might be out of sync resulting in generation of system core files upon commit completion. As of Junos OS 11.2R6 and Junos OS 11.4R3, when the policy configuration is modified and policies are out of sync, the following error message will be displayed when you attempt to commit a configuration:

```
Policy is out of sync between RE and PFE <SPU-name(s)>. Please resync before
commit.
```

```
error: configuration check-out failed
```

To synchronize policies between the Routing Engine and the Packet Forwarding Engine, you must:

- Reboot the device (device in standalone mode)
- Reboot both devices (devices in a chassis cluster mode)

System Logs

- On all high-end SRX Series devices, the attribute type of **packets-from-client** and **packets-from-server** options in the system logs of the following modules have been changed from uint to string:
  - App Track module— APPTRACK_SESSION_APP_UPDATE, APPTRACK_SESSION_APP_UPDATE_LS, APPTRACK_SESSION_CLOSE, APPTRACK_SESSION_CLOSE_LS, APPTRACK_SESSION_VOL_UPDATE and APPTRACK_SESSION_VOL_UPDATE_LS
  - Session module—RT_FLOW_SESSION_CLOSE and RT_FLOW_SESSION_CLOSE_LS

On all high-end SRX Series devices, the following system log messages have been updated to include the **certificate ID** in Junos OS Release 12.1X44-D10:

- PKID_PV_KEYPAIR_DEL

  Existing message: **Key-Pair deletion failed**

  New message: **Key-Pair deletion failed for <cert-id>**
- PKID_PV_CERT_DEL

  Existing message: **Certificate deletion has occurred**

  New message: **Certificate deletion has occurred for <cert-id>**
- PKID_PV_CERT_LOAD

  Existing message: **Certificate has been successfully loaded**

  New message: **Certificate <cert-id> has been successfully loaded**
- PKID_PV_KEYPAIR_GEN

  Existing message: **Key-Pair has been generated**

  New message: **Key-Pair has been generated for <cert-id>**

Unified In-Service Software Upgrade (ISSU)

On all high-end SRX Series devices, at the beginning of a chassis cluster unified ISSU, the system automatically fails over all RG-1+ redundancy groups that are not primary on the node from which you start the ISSU. This action ensures that the redundancy groups are all active on only the RG-0 primary node. You no longer need to fail over redundancy groups manually.

After the system fails over all RG-1+ redundancy groups, the system sets the manual failover bit and changes all RG-1+ primary node priorities to 255, regardless of whether the redundancy group failed over to the RG-0 primary node.

Virtual Private Network (VPN)

- As of Junos OS Release 11.4, checks are performed to validate the IKE ID received from the VPN peer device. By default, SRX Series and J Series devices validate the IKE ID received from the peer with the IP address configured for the IKE gateway. In certain network setups, the IKE ID received from the peer (which can be an IPv4 or IPv6 address, fully qualified domain name, distinguished name, or e-mail address) does not match the IKE gateway configured on the SRX Series or J Series device. This can lead to a Phase 1 validation failure.

  To modify the configuration of the SRX Series or J Series device or the peer device for the IKE ID that is used:

  - On the SRX Series or J Series device, configure the **remote-identity** statement at the [**edit security ike gateway *gateway-name***] hierarchy level to match the IKE ID that is received from the peer. Values can be an IPv4 or IPv6 address, fully qualified domain name, distinguished name, or e-mail address.

    NOTE: If you do not configure remote-identity, the device uses the IPv4 or IPv6 address that corresponds to the remote peer by default.

  - On the peer device, ensure that the IKE ID is the same as the **remote-identity** configured on the SRX Series or J Series device. If the peer device is an SRX Series or J Series device, configure the **local-identity** statement at the [**edit security ike gateway *gateway-name***] hierarchy level. Values can be an IPv4 or IPv6 address, fully qualified domain name, distinguished name, or e-mail address.

- On all high-end SRX Series devices, the subject fields of a digital certificate can include Domain Component (DC), Common Name (CN), Organization Unit (OU), Organization (O), Location (L), State (ST), and Country (C).

  In earlier releases, the **show security pki ca-certificate** and **show security pki local-certificate** CLI operational commands displayed only a single entry for each subject field, even if the certificate contained multiple entries for a field.

  For example, a certificate with two OU fields such as “OU=Shipping Department,OU=Priority Mail” displayed with only the first entry “OU=Shipping Department.” The **show security pki ca-certificate** and **show security pki local-certificate** CLI commands now display the entire contents of the subject field, including multiple field entries. The commands also display a new subject string output field that shows the contents of the subject field as it appears in the certificate.

- Public key infrastructure (PKI) objects include certificates, key pairs, and certificate revocation lists (CRLs). PKI objects are read from the PKI database when the PKI Daemon starts. The PKI Daemon database loads all certificates into memory at boot time.

When an object is read into memory from the PKI database, the following new log message is created:

PKID_PV_OBJECT_READ: A PKI object was read into memory from <location>

- On all high-end SRX Series devices, the secure Junos OS software environment does not permit DSA key pairs with modulus greater than 1024 bits.

Related Documentation

- New Features in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 98
- Outstanding Issues in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 150
- Resolved Issues in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 153
- Errata and Changes in Documentation for Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 172
- Known Limitations in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 134

Known Limitations in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways

AppSecure

- J-Web pages for AppSecure are preliminary.
- Custom application signatures and custom nested application signatures are not currently supported by J-Web.
- When ALG is enabled, application identification includes the ALG result to identify the application of the control sessions. Application firewall permits ALG data sessions whenever control sessions are permitted. If the control session is denied, there are no data sessions.

  When ALG is disabled, application identification relies on its signatures to identify the application of the control and data sessions. If a signature match is not found, the application is considered unknown. Application firewall handles applications based on the application identification result.

Chassis Cluster

- On all high-end SRX Series devices, IPsec VPN is not supported in active/active chassis cluster configuration (that is, when there are multiple RG1+ redundancy groups).

The following list describes the limitations for inserting an SPC on SRX3400, SRX3600, SRX5600, and SRX5800 devices in chassis cluster mode:

- The chassis cluster must be in active/passive mode before and during the SPC insert procedure.
- A different number of SPCs cannot be inserted in two different nodes.

- A new SPC must be inserted in a slot that is higher than the central point slot.

  NOTE: **The existing combo central point cannot be changed to a full central point after the new SPC is inserted.**

- During an SPC insert procedure, the IKE and IPsec configurations cannot be modified.
- Users cannot specify the SPU and the IKE instance to anchor a tunnel.
- After a new SPC is inserted, the existing tunnels cannot use the processing power of the new SPC and redistribute it to the new SPC.
- Dynamic tunnels cannot load-balance across different SPCs.
- The manual VPN name and the site-to-site gateway name cannot be the same.
- In a chassis cluster scaling environment, the heartbeat-threshold must always be set to 8.
- An APN or an IMSI filter must be limited to 600 for each GTP profile. The number of filters is directly proportional to the number of IMSI prefix entries. For example, if one APN is configured with two IMSI prefix entries, then the number of filters is two.
- Eight QoS queues are supported per aggregated Ethernet (ae) interface.
- The first recommended unified ISSU *from* release is Junos OS Release 10.4R4. If you intend to upgrade from a release earlier than Junos OS Release 10.4R4, see the release notes for the release that you are upgrading from for information about limitations and issues related to upgrading.
- ISSUs do not support the following features:
  - DHCP
  - GPRS, GTP, and SCTP
  - Flow monitoring

  For the latest unified ISSU support status, go to the Juniper Networks Knowledge Base (KB): http://kb.juniper.net/ and search for KB17946.
- In large chassis cluster configurations on SRX3400 or SRX3600 devices, you need to increase the wait time before triggering failover. In a full-capacity implementation, we recommend increasing the wait to 8 seconds by modifying **heartbeat-threshold** and **heartbeat-interval** values in the **[edit chassis cluster]** hierarchy.

  The product of the **heartbeat-threshold** and **heartbeat-interval** values defines the time before failover. The default values (**heartbeat-threshold** of 3 beats and **heartbeat-interval** of 1000 milliseconds) produce a wait time of 3 seconds.

  To change the wait time, modify the option values so that the product equals the desired setting. For example, setting the **heartbeat-threshold** to 8 and maintaining the default value for the **heartbeat-interval** (1000 milliseconds) yields a wait time of 8 seconds. Likewise, setting the **heartbeat-threshold** to 4 and the **heartbeat-interval** to 2000 milliseconds also yields a wait time of 8 seconds.

- Packet-based forwarding for MPLS and International Organization for Standardization (ISO) protocol families is not supported.
- On SRX5600 and SRX5800 devices, only two of the 10 ports on each PIC of 40-port 1-Gigabit Ethernet I/O cards (IOCs) can simultaneously enable IP address monitoring. Because there are four PICs per IOC, this permits a total of eight ports per IOC to be monitored. If more than two ports per PIC on 40-port 1-Gigabit Ethernet IOCs are configured for IP address monitoring, the commit will succeed but a log entry will be generated, and the accuracy and stability of IP address monitoring cannot be ensured. This limitation does not apply to any other IOCs or devices.
- IP address monitoring is not supported on redundant Ethernet interface link aggregation groups (LAGs) or on child interfaces of redundant Ethernet interface LAGs.
- Screen statistics data can be gathered on the primary device only.
- Unified ISSU does not support version downgrading.
- Only redundant Ethernet (reth) interfaces are supported for IKE external interface configuration in IPsec VPN. Other interface types can be configured, but IPsec VPN might not work.

Dynamic Host Configuration Protocol (DHCP)

- On all high-end SRX Series devices, DHCPv6 client authentication is not supported.
- On all high-end SRX Series devices, DHCP is not supported in a chassis cluster.

Flow and Processing

- On all high-end SRX Series devices, when packet-logging functionality is configured with an improved pre-attack configuration parameter value, the resource usage increases proportionally and might affect the performance.
- On SRX3400, SRX3600, SRX5600, and SRX5800 devices, the default authentication table capacity is 45,000; the administrator can increase the capacity to a maximum of 50,000.

  On SRX1400 devices, the default authentication table capacity is 10,000; the administrator can increase the capacity to a maximum of 15,000.
- On all high-end SRX Series devices, when devices are operating in flow mode, the Routing Engine side cannot detect the path maximum transmission unit (PMTU) of an IPv6 multicast address (with a large size packet).
- On all high-end SRX Series devices, you cannot configure route policies and route patterns in the same dial plan.
- On all high-end SRX Series devices, high CPU utilization triggered for reasons such as CPU intensive commands and SNMP walks causes the Bidirectional Forwarding Detection (BFD) protocol to flap while processing large BGP updates.

- On all high-end SRX Series devices, downgrading is not supported in low-impact unified ISSU chassis cluster upgrades (LICU).
- On SRX5800 devices, network processing bundling is not supported in Layer 2 transparent mode.

General Packet Radio Service (GPRS)

The following Gateway GPRS Support Node (GGSN) and Packet Data Network Gateway (PGW) limitations are applicable for all high-end SRX Series devices.

- GGSN and PGW traffic must pass through the GPRS tunneling protocol (GTP) framework; otherwise, the tunnel status is updated incorrectly.
- The central point distributes all GTP packets to Services Processing Units (SPUs) according to upstream endpoints for GGSN or PGW (one GGSN or PGW is the upstream endpoint of the GTP tunnels). Information is checked on the upstream endpoint IP and GTP packets in the GGSN pool network in the following way:
  - If the upstream endpoint source IP address in the Create-PDP-Context-Response or Create-Session-Response message is different from the upstream endpoint destination IP address in the Create-PDP-Context-Request/Create-Session-Request message, tunnels are not created. The related source and destination IP addresses are distributed to two Services Processing Units (SPUs).
  - If the upstream endpoint source IP address in the Create-PDP-Context-Response or Create-Session-Response message is different from the IP address of the upstream endpoint, tunnels are created on one SPU. According to the IP address of the upstream endpoint for GGSN or PGW, an incoming GTP tunnel message is moved to a second SPU, and the GTP packets are dropped because no tunnel is found.

NOTE: In the GGSN pool scenario, GGSN can reply with a Create-PDP-Context-Request or Create-Session-Request message using another IP address that differs from the one received. Therefore the request and the response can run on two different flow sessions, and these two flow sessions can be distributed to different SPUs.

The following GTP firewall limitations are applicable on all high-end SRX Series devices.

- GGSN tunneling protocol, user plane (GTP-U) inspection is not supported.
- GTP firewall does not support hot-insertable and hot-removable hardware.
- In-service software upgrade (ISSU) is not supported from an earlier release to the current release.
- The GTP firewall needs to learn the network’s GSN table and install the table for the central point and the Services Processing Unit (SPU). Otherwise, some GTP traffic is blocked when the firewall is inserted in the network.
- Recovery might not clear tunnels in GGSN-pooling scenarios, because recovery broadcast between SPUs is not supported.

The following SCTP limitations are applicable on all high-end SRX Series devices:

- Dynamic policy is not supported for SCTP. You must configure all policies for needed SCTP sessions.
- SCTP modules only inspect IPv4 traffic. IPv6 traffic will be passed or dropped by flow-based or policy-based processing directly, and no SCTP module inspection will occur.
- Only the first chunk in each SCTP packet is checked.
- For static NAT to work, the interfaces packets (from one side: client or server side) coming in must belong to the same zone.
- For multihome cases, only IPv4 Address Parameter (5) in INIT or INI-ACK is supported.
- Only static NAT is supported for SCTP.
- SCTP enable or disable is controlled by whether there is a SCTP profile configured. When you disable the SCTP feature, all associations are deleted and later SCTP packets will pass or drop according to the policy.

  If you want to enable SCTP again, all the running SCTP communications will be dropped, because no associations exist. New SCTP communications can establish an association and perform the inspections.

  Clear old SCTP sessions when SCTP is re-enabled, doing this will avoid any impact caused by the old SCTP sessions on the new SCTP communications.
- Only established SCTP associations will be synced to peer node.
- A maximum of eight source IP addresses and eight destination IP addresses are allowed in an SCTP communication.
- One SPU supports a maximum of 5000 associations and a maximum of 320, 000 SCTP sessions.
- The 4-way handshake process should be done in one node of a cluster. If the SCTP 4-way handshake process is handled on two nodes (for example, two sessions on two nodes in active/active mode) or the cluster is failover before the 4-way handshake is finished, the association cannot be established successfully.
- If you configure different policies for each session belonging to one association, there will be multiple policies related to one association. The SCTP packet management (drop, rate limit, and so on) will use the profile attached to the handling SCTP session's policy.

  The association's timeout will only use the profile attached to its INIT packet’s policy. If the INIT packet’s policy changes the attached profile, the old profile is deleted, and the association will refresh the timeout configuration. However, if the INIT packet’s policy changes its attached profile without deleting the old profile, the association will not refresh the timeout configuration.
- Unified in-service software upgrade (ISSU) to earlier Junos OS releases is not supported.
- In some cases, the associations might not be distributed to SPUs very evenly because the port’s hash result on the central point is uneven. For example, this event can occur

when only two peers of ports are used, and one peer has 100 associations, but another peer has only one association. In this case, the associations cannot be distributed evenly on the firewall with more than one SPU.

- SCTP sessions will not be deleted with associations, the sessions will time out in 30 minutes, which is the default value. If you need the session to time out soon, you can preconfigure the SCTP application timeout value.
- M3UA or SCCP message parsing is checked , but the M3UA or SCCP stateful inspection is not checked.
- Only ITU-T Rec. Q.711-Q.714 (07 or 96) standard is supported. ANSI, ETSI, China, and other standards are not supported.
- Only RFC 4960 is supported.

Interfaces and Routing

This section covers filter and policing limitations.

- On SRX1400, SRX3400, and SRX3600 devices, the following feature is not supported by a simple filter:
  - Forwarding class as match condition
- The loopback (lo0) and redundant Ethernet (reth) interfaces are supported for an IKE external interface configuration in an IPsec VPN. Other interface types can be configured, but IPsec VPN might not work.
- On all high-end SRX Series devices, IPv6 traffic transiting over IPv4 based IP over IP tunnel (for example, IPv6-over-IPv4 using ip-x/x/x interface) is not supported.
- On SRX1400, SRX3400 and SRX3600, devices, the following features are not supported by a policer or a three-color-policer:
  - Color-aware mode of a three-color-policer
  - Filter-specific policer
  - Forwarding class as action of a policer
  - Logical interface policer
  - Logical interface three-color policer
  - Logical interface bandwidth policer
  - Packet loss priority as action of a policer
  - Packet loss priority as action of a three-color-policer
- On all high-end SRX Series devices, the following features are not supported by a firewall filter:
  - Policer action
  - Egress filter-based forwarding (FBF)

  - Forwarding table filter (FTF)

- SRX3400 and SRX3600 devices have the following limitations of a simple filter:
  - Forwarding class as match condition
  - In the packet processor on an IOC, up to 400 logical interfaces can be applied with simple filters.
  - In the packet processor on an IOC, the maximum number of terms of all simple filters is 2000.
  - In the packet processor on an IOC, the maximum number of policers is 2000.
  - In the packet processor on an IOC, the maximum number of three-color-policers is 2000.
  - The maximum burst size of a policer or three-color-policer is 16 MB.

- On SRX3400 and SRX3600 devices, when you enable the monitor traffic option using the **monitor traffic** command to monitor the FXP interface traffic, interface bounce occurs. You must use the **monitor traffic interface fxp0 no-promiscuous** command to avoid the issue.
- On all high-end SRX Series devices, lo0 logical interface cannot be configured with RG0 if used as an IKE gateway external interface.
- On all high-end SRX Series devices, the **set protocols bgp family inet flow** and **set routing-options flow** CLI statements are no longer available, because BGP flow spec functionality is not supported on these devices.
- On all high-end SRX Series devices, the Link Aggregation Control Protocol (LACP) is not supported on Layer 2 interfaces.
- On all high-end SRX Series devices, BGP-based virtual private LAN service (VPLS) works on child ports and physical interfaces, but not over aggregated Ethernet (ae) interfaces.

Intrusion Detection and Prevention (IDP)

- On all high-end SRX Series devices, from Junos OS Release 11.2 and later, the IDP security package is based on the Berkeley database. Hence, when the Junos OS image is upgraded from Junos OS Release 11.1 or earlier to Junos OS 11.2 or later, a migration of IDP security package files needs to be performed. This is done automatically on upgrade when the IDP daemon comes up. Similarly, when the image is downgraded, a migration (secDb install) is automatically performed when the IDP daemon comes up, and previously installed database files are deleted.

  However, migration is dependent on the XML files for the installed database present on the device. For first-time installation, completely updated XML files are required. If the last update on the device was an incremental update, migration might fail. In such a case, you have to manually download and install the IDP security package using the **download** or **install** CLI commands before using the IDP configuration with predefined attacks or groups.

As a workaround, use the following CLI commands to manually download the individual components of the security package from the Juniper Security Engineering portal and install the full update:

- **request security idp security-package download full-update**
- **request security idp security-package install**

- On all high-end SRX Series devices, the IDP policies for each user logical system are compiled together and stored on the data plane memory. To estimate adequate data plane memory for a configuration, consider these two factors:
  - IDP policies applied to each user logical system are considered unique instances because the ID and zones for each user logical system are different. Estimates need to consider the combined memory requirements for all user logical systems.
  - As the application database increases, compiled policies requires more memory. Memory usage should be kept below the available data plane memory to allow for database increases.
- On all high-end SRX Series devices, ingress as ge-0/0/2 and egress as ge-0/0/2.100 works with flow showing both source and destination interface as ge-0/0/2.100.
- IDP does not allow header checks for nonpacket contexts.
- On all high-end SRX Series devices, application-level distributed denial-of-service (application-level DDoS) detection does not work if two rules with different application-level DDoS applications process traffic going to a single destination application server. When setting up application-level DDoS rules, make sure that you do not configure rulebase-ddos rules that have two different application-ddos objects when the traffic destined to one application server can process more than one rule. Essentially, for each protected application server, you have to configure the application-level DDoS rules so that traffic destined for one protected server processes only one application-level DDoS rule.

  NOTE: **Application-level DDoS rules are terminal, which means that once traffic is processed by one rule, it will not be processed by other rules.**

  The following configuration options can be committed, but they will not work properly:

source-zone	destination-zone	destination-ip	service	application-ddos	Application Server
source-zone-1	dst-1	any	http	http-appddos1	1.1.1.1:80
source-zone-2	dst-1	any	http	http-appddos2	1.1.1.1:80

- On all high-end SRX Series devices, application-level DDoS rule base (rulebase-ddos) does not support port mapping. If you configure an application other than default, and if the application is from either predefined Junos OS applications or a custom application that maps an application service to a nonstandard port, application-level DDoS detection will not work.

When you configure the application setting as default, IDP uses application identification to detect applications running on standard and nonstandard ports; thus, the application-level DDoS detection would work properly.

- On all high-end SRX Series devices, all IDP policy templates are supported except All Attacks. There is a 100 MB policy size limit for integrated mode and a 150 MB policy size limit for dedicated mode. The current IDP policy templates supported are dynamic, based on the attack signatures being added. Therefore, be aware that supported templates might eventually grow past the policy size limit.

  On all high-end SRX Series devices, the following IDP policies are supported:

  - DMZ_Services
  - DNS_Service
  - File_Server
  - Getting_Started
  - IDP_Default
  - Recommended
  - Web_Server

- IDP deployed in both active/active and active/passive chassis clusters has the following limitations:

  - No inspection of sessions that failover or failback.
  - The IP action table is not synchronized across nodes.
  - The Routing Engine on the secondary node might not be able to reach networks that are reachable only through a Packet Forwarding Engine.
  - The SSL session ID cache is not synchronized across nodes. If an SSL session reuses a session ID and it happens to be processed on a node other than the one on which the session ID is cached, the SSL session cannot be decrypted and will be bypassed for IDP inspection.

- IDP deployed in active/active chassis clusters has a limitation that for time-binding scope source traffic, if attacks from a source (with more than one destination) have active sessions distributed across nodes, then the attack might not be detected because time-binding counting has a local-node-only view. Detecting this sort of attack requires an RTO synchronization of the time-binding state that is not currently supported.

IPv6

IPv6 IPsec implementation has the following limitations:

- Devices with IPv6 addressing do not perform fragmentation. IPv6 hosts should either perform path maximum transmission unit (PMTU) discovery or send packets smaller than the IPv6 minimum MTU size of 1280 bytes.
- Because IPv6 addresses are 128 bits long compared to IPv4 addresses, which are 32-bits long, IPv6 IPsec packet processing requires more resources. Therefore, a small performance degradation is observed.
- IPv6 uses more memory to set up the IPsec tunnel. Therefore, the IPsec IPv4 tunnel scalability numbers might drop.
- The addition of IPv6 capability might cause a drop in the IPsec IPv4-in-IPv4 tunnel throughput performance.
- The IPv6 IPsec VPN does not support the following functions:
  - 4in6 and 6in4 policy-based site-to-site VPN, IKE
  - 4in6 and 6in4 route-based site-to-site VPN, IKE
  - 4in6 and 6in4 policy-based site-to-site VPN, Manual Key
  - 4in6 and 6in4 route-based site-to-site VPN, Manual Key
  - 4in4, 6in6, 4in6, and 6in4 policy-based dial-up VPN, IKE
  - 4in4, 6in6, 4in6, and 6in4 policy-based dial-up VPN, Manual Key
  - Remote Access—XAuth, config mode, and shared IKE identity with mandatory XAuth
  - IKE authentication—public key infrastructure or digital signature algorithm (PKI or DSA)
  - IKE peer type—dynamic IP
  - Chassis cluster for basic VPN features
  - IKE authentication—PKI or RSA
  - Network Address Translation-Traversal (NAT-T)
  - VPN monitoring
  - Hub-and-spoke VPNs
  - Next Hop Tunnel Binding Table (NHTB)
  - Dead Peer Detection (DPD)
  - Simple Network Management Protocol (SNMP) for IPsec VPN MIBs
  - Chassis cluster for advanced VPN features
  - IPv6 link-local address

- **NSM**—Consult the Network and Security Manager (NSM) release notes for version compatibility, required schema updates, platform limitations, and other specific details regarding NSM support for IPv6 addressing on all high-end SRX Series devices.
- **Security policy**—Only IDP for IPv6 sessions is supported only for all high-end SRX Series devices. UTM for IPv6 sessions is not supported. If your current security policy uses rules with the IP address wildcard any, and UTM features are enabled, you will encounter configuration commit errors because UTM features do not yet support IPv6 addresses. To resolve the errors, modify the rule returning the error so that the any-ipv4 wildcard is used; and create separate rules for IPv6 traffic that do not include UTM features.

J-Web

- On all high-end SRX Series devices, if the device is running the worldwide version of the Junos OS and you are using the Microsoft Internet Explorer Web browser, you must disable the Use SSL 3.0 option in the Web browser to access the device.
- To use the Chassis View, a recent version of Adobe Flash that supports ActionScript and AJAX (Version 9) must be installed. Also note that the Chassis View is displayed by default on the Dashboard page. You can enable or disable chassis view using options in the dashboard Preference dialog box, but clearing cookies in Internet Explorer also causes the Chassis View to be displayed.
- On all high-end SRX Series devices, users cannot differentiate between Active and Inactive configurations on the System Identity, Management Access, User Management, and Date & Time pages.

Logical Systems

- The master logical system must not be bound to a security profile that is configured with a 0 percent reserved CPU quota because traffic loss could occur. When upgrading all high-end SRX Series devices from Junos OS Release 11.2, make sure that the reserved CPU quota in the security profile that is bound to the master logical system is configured for 1 percent or more. After upgrading from Junos OS Release 11.2, the reserved CPU quota is added to the default security profile with a value of 1 percent.
- Starting with Junos OS Release 11.2, address books can be defined under the [**security**] hierarchy level instead of the [**security zones**] hierarchy level. This enhancement makes configuring your network simpler by allowing you to share IP addresses in address books when configuring features such as security policies and NAT. You can attach zones to address books—this is known as zone-attached configuration.

  Junos OS Release 12.1 continues to support address book configuration under the [**security zones**] hierarchy level—this is known as zone-defined configuration. However, we recommend that zone-attached address book configuration be used in the master logical system and user logical systems.

  If you upgraded your high-end SRX Series devices to this Junos OS Release 12.1, and are configuring logical systems on the device, 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 zone-defined configuration to zone-attached configuration. The upgrade script converts all zone-defined configurations in the master logical system and user logical systems. See the section, "Upgrade and Downgrade Scripts for Address Book Configuration" of "Upgrade and Downgrade Instructions for Junos OS Release 12.1X44 for High-End SRX Series Services Gateways" on page 177.

- On all high-end SRX Series devices, the logical systems feature does not support ALGs for user logical systems because ALGs are configured globally. If you enable ALGs at the root master logical system level, they are also enabled for user logical systems in Junos OS Release 12.1. In this case, user logical system traffic is processed by the ALGs, and corresponding ALG flow sessions are initiated under the user logical system. You can only enable and disable ALGs at the root master logical system level.
- On all high-end SRX Series devices, quality-of-service (QoS) classification across interconnected logical systems does not work.
- On all high-end SRX Series devices, the number of logical system security profiles you can create is constrained by an internal limit on security profile IDs. The security profile ID range is from 1 through 32 with ID 0 reserved for the internally configured default security profile. When the maximum number of security profiles is reached, if you want to add a new security profile, you must first delete one or more existing security profiles, commit the configuration, and then create the new security profile and commit it. You cannot add a new security profile and remove an existing one within a single configuration commit.

  If you want to add more than one new security profile, the same rule is true. You must first delete the equivalent number of existing security profiles, commit the configuration, and then create the new security profiles and commit them.
- **User and administrator configuration for logical systems**—Configuration for users for all logical systems and all user logical systems administrators must be done at the root level by the master administrator. A user logical system administrator cannot create other user logical system administrators or user accounts for their logical systems.
- **Name-space separation**—The same name cannot be used in two logical systems. For example, if logical-system1 includes the username "Bob" then other logical systems on the device cannot include the username "Bob".
- **Commit rollback**—Commit rollback is supported at the root level only.
- **Trace and debug**—Trace and debug are supported at the root level only.
- **Class of service**—You cannot configure class of service on logical tunnel (lt-0/0/0) interfaces.
- **ALGs**—The master administrator can configure ALGs at the root level. The configuration is inherited by all user logical systems. It cannot be configured discretely for user logical systems.

Network Address Translation (NAT)

- On all high-end SRX Series devices, in case of SSL proxy, sessions are whitelisted based on the actual IP address and not on the translated IP address. Because of this, in the whitelist configuration of the SSL proxy profile, the actual IP address should be provided and not the translated IP addresses.

Example:

Consider a destination NAT rule that translates destination IP address 20.20.20.20 to 5.0.0.1 using the following commands:

- **set security nat destination pool d1 address 5.0.0.1/32**
- **set security nat destination rule-set dst-nat rule r1 match destination-address 20.20.20.20/32**
- **set security nat destination rule-set dst-nat rule r1 then destination-nat pool d1**

In the above scenario, to exempt a session from SSL proxy inspection, the following IP address should be added to the whitelist:

- **set security address-book global address ssl-proxy-exempted-addr 20.20.20.20/32**
- **set services ssl proxy profile ssl-inspect-profile whitelist ssl-proxy-exempted-addr**

- Maximum capacities for source pools and IP addresses have been extended on all high-end SRX Series devices as follows:

Pool/PAT Maximum Address Capacity	SRX1400	SRX3400 SRX3600	SRX5600 SRX5800
Source NAT pools	8192	8192	12288
IP addresses supporting port translation	8192	8192	12288
PAT port number	256M	256M	384M

Increasing the capacity of source NAT pools consumes memory needed for port allocation. When source NAT pool and IP address limits are reached, port ranges should be reassigned. That is, the number of ports for each IP address should be decreased when the number of IP addresses and source NAT pools is increased. This ensures NAT does not consume too much memory. Use the **port-range** statement in configuration mode in the CLI to assign a new port range or the **pool-default-port-range** statement to override the specified default.

Configuring port overloading should also be done carefully when source NAT pools are increased.

For source pool with port address translation (PAT) in range (64,510 through 65,533), two ports are allocated at one time for RTP or RTCP applications, such as SIP, H.323, and RTSP. In these scenarios, each IP address supports PAT, occupying 2048 ports (64,512 through 65,535) for Application Layer Gateway (ALG) module use. On SRX5600 and SRX5800 devices, if all of the 4096 source pool is configured, a port allocation of 8,388,608 is reserved for twin port use.

- **NAT rule capacity change**—To support the use of largescale NAT (LSN) at the edge of the carrier network, the devicewide NAT rule capacity has been changed.

The number of destination and static NAT rules has been incremented as shown in Table 16 on page 147. The limitation on the number of destination rule set and static rule set has been increased.

Table 16 on page 147 provides the requirements per device to increase the configuration limitation as well as to scale the capacity for each device.

Table 16: Number of Rules on all High-End SRX Series Devices

NAT Rule Type	SRX1400	SRX3400 SRX3600	SRX5600 SRX5800
Source NAT rule	8192	20480	30720
Destination NAT rule	8192	20480	30720
Static NAT rule	8192	20480	30720

The restriction on the number of rules per rule set has been increased so that there is only a devicewide limitation on how many rules a device can support. This restriction is provided to help you better plan and configure the NAT rules for the device.

For memory consumption, there is no guarantee to support these numbers (maximum source rule or rule set + maximum destination rule or rule set + maximum static rule or rule-set) at the same time for SRX3400, SRX3600, SRX5600, and SRX5800.

The suggested total number of rules and rule sets is listed in following table:

Objects	SRX3400 SRX3600	SRX5600 SRX5800
Total NAT rule sets per system	20,000	30,000
Total NAT rules per rule set	20,000	30,000

Security Policies

- On all high-end SRX Series devices, the current SSL proxy implementation has the following connectivity limitations:
  - The SSLv2 protocol is not supported. SSL sessions using SSLv2 are dropped.
  - SSL sessions where client certificate authentication is mandatory are dropped.
  - SSL sessions where renegotiation is requested are dropped.
- On all high-end SRX Series devices, for a particular session, the SSL proxy is only enabled if a relevant feature related to SSL traffic is also enabled. Features that are related to SSL traffic are Intrusion Detection and Prevention (IDP), application identification, application firewall, and application tracking. If none of the above listed features are active on a session, the SSL proxy bypasses the session and logs are not generated in this scenario.

- On all high-end SRX Series devices, the limitation on the number of addresses in an address set has been increased to 1024. The default value of an address set is 1024. The number of addresses in an address set, which depends on the device, is equal to the number of addresses supported by the policy.

Services Offloading

- Services offloading has the following limitations:
  - Transparent mode is not supported. If transparent mode is configured, a normal session is installed.
  - Link aggregation group (LAG) is not supported. If a LAG is configured, a normal session is installed.
  - Only multicast sessions with one fan-out are supported. If a multicast session with more than one fan-out exists, a normal session is installed.
  - Only active/passive chassis cluster configuration is supported. Active/active chassis cluster configuration is not supported.
  - Fragmented packets are not supported. If fragmented packets exist, a normal session is installed.
  - IP version 6 (IPv6) is not supported. If IPv6 is configured, a normal session is installed.

  NOTE: A normal session forwards packets from the network processor to the Services Processing Unit (SPU) for fast-path processing. A services-offload session processes fast-path packets in the network processor and the packets exit out of the network processor itself.

- For Non-Services-Offload Sessions:
  - When services offloading is enabled, for normal sessions, the performance can drop by approximately 20 percent for connections per second (CPS) and 15 percent for packets per second (PPS) when compared with non-services-offload mode.
  - For Services-Offload Sessions

    When services offloading is enabled, for fast-forward sessions, the performance can drop by approximately 13 percent for connections per second (CPS).

Simple Network Management Protocol (SNMP)

- On all high-end SRX Series devices, the **show snmp mib** CLI command will not display the output for security related MIBs. We recommend that you use an SNMP client and prefix **logical-system-name@** to the community name. For example, if the community is **public**, use **default@public** for default root logical system.

Virtual Private Network (VPN)

On all high-end SRX Series devices, IKEv2 does not include support for:

- Policy-based tunnels
- Dial-up tunnels
- Network Address Translation-Traversal (NAT-T)
- VPN monitoring
- Next-Hop Tunnel Binding (NHTP) for st0—Reusing the same tunnel interface for multiple tunnels
- Extensible Authentication Protocol (EAP)
- IPv6
- Multiple child SAs for the same traffic selectors for each QoS value
- Proposal enhancement features
- Reuse of Diffie-Hellman (DH) exponentials
- Configuration payloads
- IP Payload Compression Protocol (IPComp)
- Dynamic Endpoint (DEP)

- On all high-end SRX Series devices, DH-group 14 is not supported for dynamic VPN.
- On all high-end SRX Series devices, when you enable VPN, overlapping of the IP addresses across virtual routers is supported with the following limitations:
  - An IKE external interface address cannot overlap with any other virtual router.
  - An internal or trust interface address can overlap across any other virtual router.
  - An st0 interface address cannot overlap in route-based VPN in point-to-multipoint tunnels such as NHTB.
  - An st0 interface address can overlap in route-based VPN in point-to-point tunnels.
- On all high-end SRX Series devices, the DF-bit configuration for VPN only works if the original packet size is smaller than the st0 interface MTU, and larger than the **external interface-ipsec overhead**.
- The local IP feature is not supported on the following:
  - All SRX Series devices in chassis cluster configuration

  - All high-end SRX Series devices

- On all high-end SRX Series devices, the IPsec NAT-T tunnel scaling and sustaining issues are as follows:
  - For a given private IP address, the NAT device should translate both 500 and 4500 private ports to the same public IP address.
  - The total number of tunnels from a given public translated IP cannot exceed 1000 tunnels.

Related Documentation

- New Features in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 98
- Resolved Issues in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 153
- Outstanding Issues in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 150
- Errata and Changes in Documentation for Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 172
- Changes in Default Behavior and Syntax in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 123

Outstanding Issues in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways

The following problems currently exist in Juniper Networks SRX Series Services Gateways. The identifier following the descriptions is the tracking number in the Juniper Networks Problem Report (PR) tracking system.

For the latest, most complete information about outstanding and resolved issues with the Junos OS software, see the Juniper Networks online software defect search application at http://www.juniper.net/prsearch.

NOTE: If there is no device listed in the PR description, then that issue applies to all high-end SRX Series devices.

Outstanding Issues in Junos OS Release 12.1X44-D20 for High-End SRX Series Services Gateways

Certificate Authority (CA)

- The output of the **show security pki ca-certificate detail** command includes the "Auto-re-enrollment" section. This is incorrect because automatic reenrollment is not supported for CA certificates. [PR877574]

Chassis Cluster

- On devices in a chassis cluster, Layer 2 node 1 does not change to disable state, if node 0 is RG-0 primary and node 1 is RG1+ primary node with fabric link failure. [PR821704]
- On devices in a chassis cluster, if the secondary node is rebooted with new Web authentication requests coming into the chassis cluster continuously, the Web authentication entry ID is not the same between the two nodes when testing in-service hardware upgrade (ISHU). [PR826100]

Flow and Processing

- When end-to-end debugging is enabled, if the traffic rate is 1000 packets per second (pps) or higher, packet loss is observed. [PR786406]
- When NP hash is enabled, traffic loss is observed for IPv6 fragmented traffic (UDP and TCP). [PR818279]
- When re-route fails for an existing session (for example, because of zone mismatch between the new and the old best route), the session remains active and all the traffic is black-holed. [PR852316]
- The correct http service timeout should be 300 seconds by default, but the SRX device sets http session timeout to 1800 seconds. [PR858621]

Infrastructure

- Superfluous accounts are present in Junos OS on SRX Series devices. [PR719750]
- On SRX Series devices in a chassis cluster, after control plane Redundancy Group (RG0) failover, in a race condition SPUs might have more if states than the new master Routing Engine. This difference leads to sequence number mismatch and causes cold synchronization failure, and all FPCs might reboot. After the FPCs reboot , a "split brain" situation occurs in which both nodes become primary. [PR885889]

Interfaces and Routing

- When you change interface configurations, the interface is deleted from the Routing Engine kernel and added back. Applications that are asynchronously listening to kernel state changes might receive delete requests and add out of order events. Some Layer 2 applications might not be able to handle these out of order events and applications might restart and resynchronize kernel states again. [PR771748]

- When a nonrendezvous point (RP) device is configured as RP for a specific group, the auto-rendezvous feature fails to elect RP for the specific group. [PR774844]
- Multicast stream is not redirected to other member links on the aggregated Ethernet interface even when the link in use is disabled. [PR867529]

Intrusion Detection and Prevention (IDP)

- On XLP platforms, setting the **max-sessions** option in an application identification configuration does not impact the attack traffic. [PR809384]
- After the Junos image is upgraded, we recommend you, download a full update of the IDP security package and then perform the installation. Subsequent incremental updates (default) work fine. If a full update is not performed, the device might end up adding only the new signatures downloaded in incremental order, leaving the device unprotected from a large set of signatures. [PR876764]
- On all high-end SRX Series devices, maximize sessions inline-tap equal mode is not supported in Junos OS Release 12.1X44-D20. If the maximize sessions inline-tap equal mode is configured in releases earlier than release Junos OS Release 12.1X44-D20, when you upgrade to Junos OS Release 12.1X44-D20, the configuration changes to maximize sessions inline-tap firewall mode. [PR889597]

Network Address Translation (NAT)

- On devices in a chassis cluster, some persistent NAT table entries cannot be removed on the Services Processing Unit (SPU) when the device is under heavy traffic with multiple failovers. [PR834823]

System Logs

- Occasionally, the following SPU message is displayed, causing the kernel system log buffer to overflow:

  Nexthop XXXX on ifl XXX. Ignoring

  [PR726580]
- Memory leak is observed with periodic packet management process (ppmd), and the following logs are generated:

  /kernel: Process (1413,ppmd) has exceeded 85% of RLIMIT_DATA: used 115596 KB Max 131072 KB

  As a workaround, reset the ppmd process. [PR747002]
- When you set a Network Processing I/O card (NP-IOC) as offline, error messages are seen in the /var/log/message folder. [PR833413]
- When you reboot the device, cyclic redundancy check (CRC) error logs recorded in chassis log file might appear. However, this does not affect the normal operation of the device and can be ignored. [PR877722]

Related Documentation

- New Features in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 98
- Known Limitations in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 134
- Errata and Changes in Documentation for Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 172

Resolved Issues in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways

The following are the issues that have been resolved in Junos OS Release 12.1X44 for Juniper Networks SRX Series Services Gateways. The identifier following the description is the tracking number in the Juniper Networks Problem Report (PR) tracking system.

For the latest, most complete information about outstanding and resolved issues with the Junos OS software, see the Juniper Networks online software defect search application at http://www.juniper.net/prsearch.

NOTE: If there is no device listed in the PR description, then that issue applies to all high-end SRX Series devices.

Resolved Issues in Junos OS Release 12.1X44-D20 for High-End SRX Series Services Gateways

Application Identification

- On all high-end SRX Series devices, when AI handles Secure Socket Layer (SSL) encrypted sessions with SSLFP are enabled, if the client sends a large amount of data to the server in a single transaction, core files are generated. [PR859951]

Application Layer Gateway (ALG)

- The TCP proxy module used by the ALG is deficient in handling a TCP stream with large packets. [PR727649]
- On SRX3400 devices, the TCP proxy incorrectly acknowledges the SYN packet when the session is in close wait state for RSH ALG. The register suppression time (RST) packet creates a session with a timeout value of 1800 when RSH ALG is enabled. [PR742317]
- If the Microsoft Remote Procedure Call (MS-RPC) or Sun Microsystems Remote Procedure Call (SUN-RPC) ALG is disabled when there are other open MS-RPC or SUN-RPC gates, the traffic that hit the previously opened gates is dropped by ALG even after the ALG is completely disabled. This is because of an ALG behavior change ntroduced in Junos OS Release 11.4. [PR865851]

- The b attribute (pertaining to bandwidth) in a Session Initiation Protocol (SIP) Session Description Protocol (SDP) message is not carried forward after the SIP ALG processes the packet. [PR875211]
- If a static route is configured and exported into OSPF, and if the static route has the same subnet as an OSPF interface address, then committing configuration changes (even unrelated to OSPF, such as a device's hostname) results in the removal of the static route related to OSPF type-5 link-state advertisement (LSA) from the OSPF database. [PR875481]

Authentication

- On SRX Series devices configured with the user role firewall feature, if the length of the source-identity role name in the security policy is more than 64 bytes, the devices are unstable and flowd core files are generated. [PR855386]

Chassis Cluster

- On all high-end SRX Series devices, operating in a chassis cluster, a maximum 8 queues per interface configuration is not reflected on the interface part of the cluster setup. [PR389451]
- On devices in a chassis cluster with the second control link connected, when CRM is installed, and the primary node is power-cycled, the primary node takes over RG-0 ownership when the primary node is rebooted. [PR679634]
- On devices in a chassis cluster, the flowd process crashes if packets received on the chassis cluster data links are corrupted. The device drops these corrupted packets. [PR680209]
- Occasionally, during RG1 failover, the priority of node 1 stuck at zero (0). Attempts to fail over to node 1 are unsuccessful, and the cluster bounces back to node 0 because the priority of node 1 remains zero. [PR750708]
- On devices in chassis cluster, to save the configuration on a remote file server, you have to specify the absolute/relative path for storing the file. If the path is not specified, the save operation fails. However, this issue might not affect devices operating in a stand-alone mode. [PR752363]
- On devices in a chassis cluster, massive amounts of MAC addresses are generated on the fabric link switch port. [PR833609]
- On SRX3600 devices, in certain circumstances one of the Services Processing Cards (SPCs) is stuck due to a hardware fault, and the following error message is displayed in the jsrpd log: “Jan 17 23:07:22 Index: 16 PFE Id: 16, Error_code: 0x01 - Loopback”. [PR851317]
- On all high-end SRX Series devices, when aggregated redundant Ethernet (chassis cluster redundant Ethernet interface with multiple link members per node) is used, traffic loss is observed when the link member fails. [PR858519]
- On devices in a chassis cluster, Juniper Services Redundancy Protocol (jsrpd) process log messages are displayed even though the cluster is stable with no failover events. [PR861704]

Command-Line Interface (CLI)

- On SRX3400 and SRX3600 devices, in standalone mode, when the device is rebooted using the request system reboot command, some of the interfaces are up during the reboot. This results in slow traffic failover in the static routing environment. [PR732733]
- An escalation of privileges occurrs when the **load factory-default** command fails in the exclusive edit mode. When the command fails, the user is not subjected to any command or configuration restrictions. The escalation is limited to authenticated users with the privilege to edit the configuration. The privilege bypass is specific to configured CLI users with restrictions on commands such as **allow-commands**, **deny-commands**, and **deny-configuration**. [PR743545]
- On all high-end SRX Series devices, running the **show security screen statistics logical-system all zone** X command generates core files, if the X zone does not have screens enabled and if it is part of a logical system. [PR866559]
- The **request chassis fabric plane offline/online** command might not work as expected. [PR877776]

Dynamic Host Configuration Protocol (DHCP)

- On all high-end SRX Series devices, the Dynamic Host Configuration Protocol version 6 (DCHPv6) server might not create any server binding. [PR799829]

Flow and Processing

- Special crafted kernel routes that are generated based on directly connected networks (clone routes) introduce reference count inconsistencies when the link flaps, if the clone routes are rewired to a different interface. This occurs because the longest prefix match finds another destination for the IP address of the flapped interface. When the parent reference count is reduced to zero, the kernel crashes when deleting the remaining child routes. [PR685941]
- On all high-end SRX Series devices, flowd core files are generated during the Layer 2 mode stress test. [PR704482]
- On all high-end SRX Series devices, the graceful restart mechanism might not abort even if the link to the upstream neighbor is down. This leads to a higher routing protocol convergence time because the route might not fail over to an alternate path until the graceful restart timer expires. [PR751640]
- When a large number of logs are archived to a remote site, event core files are generated. [PR771228]
- An illegal pointer address generates eventd core files. [PR784037]
- When a device forwards traffic, flowd core files are generated. [PR831480]
- SYN packets are dropped if TCP ports are reused within 2 seconds. [PR836554]
- When you configure a wildcard address and use it in more than seven security policies, the Services Processing Unit (SPU) crashes. [PR847632]

- In the output of the **show security flow session extensive** command, if the flow session references a custom application with the **application-protocol ignore** option configured, the application field is incorrectly set. [PR852081]
- When you commit security policy changes, under certain load conditions (based on the Services Processing Unit (SPU) usage and number of active sessions) and in situations where policy rematch must be performed (either when policy rematch is configured or new policies are added, or the order is changed), SPU usage increase and partial packet drops are observed. [PR854412]
- When a TCP server sends more bytes than the receiver’s window size, a TCP segment can pass the SRX Series TCP sequence check even if it exceeds the receiver's window size. This is because the current TCP sequence check does not consider the size of the TCP segment when validating against the receiver's window size. However, the SRX Series device drops the ACK on the other direction for this TCP segment. [PR855056]
- On devices enabled with SYN cookie protection, after the SYN cookie function is triggered, the SYN cookie might not send ACK to the client to update the TCP window size after a handshake with the server. When the client sends ACK with a PSH flag to the device as the third TCP ACK during the TCP three-way hand shake, the device might not recognize the ACK. This results in TCP connection failure. [PR859222]
- When TCP SYN flood protection is enabled and triggered, and if the Window Scaling option is used between a TCP client and server, TCP communication is reset abnormally. [PR886204]

General Packet Radio Service (GPRS)

- On SRX1400 devices, the number of GPRS support node (GSN) entries is expanded from 6000 entries to 18,000 entries on each Services Processing Unit (SPU). [PR787028]

Infrastructure

- When you archive a file using the file-archive rpc option, the following error is displayed:

  Operation allowed only from CLI

  [PR831865]
- When the backup Routing Engine kernel fails, some devices send a message to the master Routing Engine to generate a core file. This causes problems. [PR854501]

Interfaces and Routing

- Configuring multicast addresses (inet6) on an interface results in the generation of RPD core (mc_ssm_add) files. [PR780751]

Intrusion Detection and Prevention (IDP)

- Occasionally, when the Service Processing Units (SPUs) are not recovered completely and when the device handles messages related to Secure Sockets Layer (SSL), traffic drops and core files are generated. [PR856132].
- On all high-end SRX Series devices with IDP application-level distributed denial-of-service (DDoS) feature enabled, if the binary analysis report function is enabled, the device generating IDP application-level DDoS attack logs crashes the flowd process and core files are generated. [PR865469]
- On SRX Series devices with IDP enabled, if IDP exempt rule is configured, a change of the IDP rule configuration (such as, change source/destination address or change action or change signature) might cause the flowd process to crash and core files are generated. [PR877865]
- When the no-reset-on-policy option is set and there are two active policies in a dataplane, and only one session referred to the older policy; flowd core files are generated, if application identification indicates a change in application (from the default one, for example, FTP running on Telnet port), because of policy re-lookup. [PR880408]
- On all high-end SRX Series devices, maximize sessions inline-tap equal mode is not supported in Junos OS Release 12.1X44-D20. If the maximize sessions inline-tap equal mode is configured in releases earlier than Junos OS Release 12.1X44-D20, when you upgrade to Junos OS Release 12.1X44-D20, the configuration changes to maximize sessions inline-tap firewall mode. [PR889597]

J-Web

- On all high-end SRX Series devices, when using the CLI you might not be able to configure only an AppQoS rule set without configuring any other diff-services. However, in J-Web, you can configure at least one diff-service for a new AppQoS rule set configuration. [PR686462]
- In J-Web, if the policy name is "0", the penultimate-hop popping (PHP) function treats it as empty, and traffic log output cannot be viewed. [PR853093]

Logical Systems

- In a logical system, you cannot use snmpwalk for Simple Network Management Protocol (SNMP) polling. [PR791859]
- On SRX1400 devices, commit on configuration with the lt-0/0/0 interface failed. [PR845837]

Network Address Translation (NAT)

- On all high-end SRX Series devices, NAT might not function as expected because the configuration changes to source NAT, destination NAT, or both are not properly pushed to the forwarding plane. [PR744344]
- On devices enabled with static NAT and configured with multiple routing instances, reverse static NAT might not work when both the ingress interface and egress interface are in the root routing instance. [PR834145]
- On devices in a chassis cluster, NAT proxy-ndp might not work as expected after a failover because the related multicast routes are deleted. [PR841618]
- On devices enabled with the Protocol Independent Multicast (PIM) protocol, the flowd process crashed and generated core files, when there was a unicast PIM register message received with encapsulated multicast data; and if NAT process was involved in the session for the received PIM packet. This issue was observed on standalone high-end SRX Series devices, and on devices in a chassis cluster. In the case of devices in a chassis cluster, the flowd process crashed on both node 0 and node 1. [PR842253]

System Logs

- On SRX5800 devices, when configuration messages exceed the interprocess communication message (IPC) maximum transmission unit (MTU), occasionally the following error message is displayed:

  ipc_msg_write: %PFE-3: IPC message type: 27, subtype: 2 exceeds MTU, mtu 3216, length 3504. [PR612757]
- In certain configurations, the following message is displayed in the logs: [ ]

  PFEMAN: Sent Resync request to Master. [PR802355]

Upgrade and Downgrade

- After you upgrade to Junos OS Release 11.4R2, RTSP ALG might not open a pinhole for IXIA because "/r/n" characters are added to the packet. [PR842470]

Virtual Private Network (VPN)

- Occasionally, devices configured with policy-based IPsec VPN might not allow traffic to the protected resources. [PR718057]
- Manual (static) next-hop tunnel binding (NHTB) with DEP is not supported. [PR725462]
- On a high-scale RIP deployment, frequent flap of tunnels leads to missing a small number of RIP routes. These routes eventually recover. [PR802078]
- When traffic is fragmented over an IPsec tunnel, the first fragment is the smallest fragment. This is done because the first fragment has to be copied into a separate memory buffer and a smaller first fragment results in faster copying and a faster fragmentation process. [PR807216]
- On devices in a chassis cluster, some VPN system log messages are not generated. [PR837983]

- Automatic enrollment of PKI certificates might not work as expected. [PR860923]
- When an IPsec tunnel is established from a routing instance, the enable VPN session affinity (SA) features cause VPN traffic drop in the anchor Services Processing Unit (SPU). If the clear-text session is located in a SPU that is different from the anchor SPU, the routing instance ID is lost when the packet is forwarded from the central point to the anchor SPU in the first path processing, and causes the routing lookup to occur in the wrong routing table (inet.0 table). [PR866220]

Resolved Issues in Junos OS Release 12.1X44-D15 for High-End SRX Series Services Gateways

Application Layer Gateways (ALG)

- On SRX5600 and SRX5800 devices, if next-generation Services Processing Card (NG-SPC) is used, under heavy traffic, Application Layer Gateways (ALGs) might receive duplicate Juniper Message Passing Interface (JMPI) messages. This causes the flowd process to crash and a core file is generated. PR844041: This issue has been resolved.]

NOTE: JMPI message is an internal message used for communications between internal components of the device.

- When the user firewall was enabled for ALG traffic, the system crashed when the user firewall tried to log in the session-close for the ALG data (child) session. [PR845501: This issue has been resolved.]

Chassis Cluster

- On devices in a chassis cluster, the flowd process crashed if packets received on the chassis cluster data links were corrupted. The device dropped these corrupted packets. [PR680209: This issue has been resolved.]
- After multiple node failovers, the chassis cluster LEDs showed as unlit even if the cluster was stable. [PR789190: This issue has been resolved.]
- On devices in a chassis cluster, when the kernel memory was exhausted because of dead if states, the recovery caused an outage. [PR799831: This issue has been resolved.]
- On SRX5600 devices in a chassis cluster, after rebooting the primary node, the connection for the user firewall or application firewall between the new primary Routing Engine and new primary Packet Forwarding Engine was lost. The configuration for the user firewall or application firewall could not be pushed to the primary Packet Forwarding Engine. [PR816911: This issue has been resolved.]
- On devices in a chassis cluster, some VPN system log messages were not generated. [PR837983: This issue has been resolved.]
- On a device in a chassis cluster, the primary node would go to **db** mode and generated a vmcore file when you changed the configuration of the redundant Ethernet (reth) interface that caused the deletion of logical interface of reth. [PR850897: This issue has been resolved.]

Command-Line Interface (CLI)

- When you upgraded an SRX Series device to Junos OS Release 11.4, NSM showed an error that a space in the full-name parameter of the **set system login user test-name full-name test name** command statement is not accepted. [PR806750: This issue has been resolved.]

Flow and Processing

- When a device forwarded traffic, a flowd core file was generated. This was a generic issue and was not related to any specific feature. [PR831480: This issue has been resolved.]
- When you configured a security policy using the DNS name, traffic was dropped and the security policy did not function as expected. [PR841682: This issue has been resolved.]
- When the data size was smaller than 128 bytes, the certificate revocation list (CRL) failed to install using the Lightweight Directory Access Protocol (LDAP) server. [PR847868: This issue has been resolved.]

Hardware

- On devices with next-generation SPCs, boot up delayed because of SPC boot ROM running into unknown state. This recovered by automatic power sequence but added additional delay of around 5 minutes for the next-generation-SPC to boot up. [PR833691: This issue has been resolved.]

Infrastructure

- On SRX3600 devices, a change bit was set for a gencfg client after the client closed. A change bit was set on an **ifstate** before the client changed to the next state. The function rts_ifstate_client_close moved the client from the next location to the end of the chain and cleared all the bits. [PR786080: This issue has been resolved.]

Interfaces and Routing

- The routing protocol process (rpd) was reinitialized when you committed a configuration change. When multiple reinitializations occurred while OSPF was running on the router, the periodic refresh of OSPF router link-state advertisements (LSAs) stopped. If the LSAs were not refreshed, the router no longer participated in the OSPF routing domain. You could issue the **show ospf database router advertising-router router-id extensive | match timer** command to see evidence of the issue. In the error state, the output did not include the Gen timer field. [PR744280: This issue has been resolved.]
- Transmit (Tx) and receive (Rx) lockup of the tsec1 (em0) controller caused the em0 interface to go down and all the field-replaceable units (FRUs) to go offline. [PR820210: This issue has been resolved.]

Intrusion Detection and Prevention (IDP)

- Occasionally, when the Service Processing Units (SPUs) were not recovered completely and when the device handled messages related to Secure Sockets Layer (SSL), traffic dropped and core files were generated. [PR856132: This issue has been resolved].
- On all high-end SRX Series devices with the IDP application-level distributed denial-of-service (DDoS) feature enabled, if the binary analysis report function was enabled, the device generating IDP application-level DDoS attack logs crashed the flowd process and core files were generated. [PR865469: This issue has been resolved.]

J-Web

- In J-Web, when you tried to commit for logical systems configurations, the following error was received even if configuration changes were made: “You have pending changes from previous commit”. [PR812896: This issue has been resolved.]
- In J-Web, there was no support for the XLP-based card. [PR826605: This issue has been resolved.]
- In J-Web, the value was set low in the “session expired when the idle-timeout” option. [PR830644: This issue has been resolved.]

Network Address Translation (NAT)

- NAT was not functioning as expected because the configuration changes to source NAT, destination NAT, or both were not properly pushed to the forwarding plane. [PR744344: This issue has been resolved.]
- On devices in chassis cluster Z mode, a flowd core file was generated while handling mass persistent NAT traffic. [PR834821: This issue has been resolved.]

Security Policies

- During configuration and maintenance of a device, occasionally the security match policies did not synchronize between the Packet Forwarding Engine and the Routing Engine. In most cases, an error message was displayed during the attempt to commit the configuration. [PR836489: This issue has been resolved.]

Upgrade and Downgrade

- After you upgraded to Junos OS Release 11.4R2, , RTSP ALG did not open a pinhole for IXIA because "/r/n" characters were added to the packet. [PR842470: This issue has been resolved.]

Virtual Private Network (VPN)

- If all the IPsec tunnels in a configuration used the predefined IKE proposal set, and no custom proposals were present in the configuration, the IPsec tunnels flapped when you committed any configuration changes under the IKE or IPsec hierarchy. [PR812433: This issue has been resolved.]
- If IPsec VPN was configured, vmcore files were generated on Services Processing Units (SPUs). [PR824931: This issue has been resolved.]

- Occasionally, you could commit an incomplete configuration, where a VPN object referenced a missing "st" interface under the bind-interface statement. The missing interface reference was detected when the configuration was displayed using the **show security ipsec vpn** command. However, it was still possible to commit the configuration in some cases because the commit check did not consistently detect configuration errors. [PR834238: This issue has been resolved.]
- If the loopback interface was chosen as the external interface in the IKE gateway, the interface had to be in the same zone as the outgoing interface. Otherwise, packets were dropped because the packets could not be routed. [PR840182: This issue has been resolved.]
- Dynamic VPN on Windows 7, 64-bit operating system (OS) did not work in some environments. [PR842607: This issue has been resolved.]
- When a certificate revocation list (CRL) file was loaded using the **request security pki crl load ca-profile ca-profile filename *filename*** command, the CRL checking worked as expected until a PKID Daemon restarted. Once a PKID Daemon was restarted, the CRL file needed to be reloaded manually for CRL checking to continue working. [PR845459: This issue has been resolved.]

Resolved Issues in Junos OS Release 12.1X44-D10 for High-End SRX Series Services Gateways

Application Layer Gateways (ALGs)

- When the device was processing several thousands of transit IPsec sessions through ike-esp-nat ALG, occasionally, new sessions failed. [PR671074: This issue has been resolved.
- Abnormal SQL traffic caused the flowd process to crash when the SQL ALG was enabled. [PR737468: This issue has been resolved.]
- The flowd process crashed and generated core files when processing NAT-translated H.323 traffic using the H.323 ALG. [PR737507: This issue has been resolved.]
- The ALG module did not initialize properly due to a last-minute regression, preventing protocols such as FTP, RTSP, SIP, and RPC from working properly. This caused traffic drop and affected all the ALG related features. [PR749366: This issue has been resolved.]
- The fragmented packets with the DF bit set (do not fragment) might be dropped by the device when processed by ALG. This problem might occur when the fragmented packet was set to DF when it should not be fragmented anymore. [PR754504: This issue has been resolved.]
- ALG processing of traffic could result in generation of a core file. [PR780007: This issue has been resolved.]
- SIP ALG dropped SIP acknowledgement messages when messages used the folding format. [PR787879: This issue has been resolved.]

- When using the IKE-ESP-NAT ALG to pass through for the Cisco EZ-VPN client, the IKE handshake might not be successful, because the IKE packet coming from the VPN server got dropped. [PR791549: This issue has been resolved.]
- At initialization one wing was updated with client IPs, and at INIT-ACK the other wing was updated with server IPs. However, abort occurred after initialization, so only one wing of the association was filled with IP information. Because the association strictly matched both the wings, it failed and returned the message “no association”. [PR822829: This issue has been resolved.]

Chassis Cluster

- On devices in a chassis cluster, some central point binding entries did not age out after stress test. [PR611827: This issue has been resolved.]
- There was a timing error at the SYSIO interface, which connects to an IOC in slot 2. [PR680832: This issue has been resolved.]
- The AI cache could not synchronize successfully for chassis cluster cold synchronization. [PR682090: This issue has been resolved.]
- After the secondary node was upgraded, rebooted, and joined to the cluster, its priority node was restored before it completed cold synchronization. This was purely a cosmetic issue because the infrastructure actually waits until cold synchronization is completed before it proceeds further. [PR693933: This issue has been resolved.]
- On devices in a chassis cluster, if an equal-cost multipath (ECMP) route had both local and remote interfaces, then the local interface was favored for the next hop to avoid the performance-related issues that involved forwarding the traffic across the fabric link. [PR718807: This issue has been resolved.]
- On devices in a chassis cluster, the system crashed while changing the MTU of the redundant Ethernet interface. [PR720927: This issue has been resolved.]
- On devices in a chassis cluster, when the secondary node was rebooted or shut down, there could be a transient traffic drop on the primary node. The amount of drop depended on the number of active sessions. After the route change and RTO cold synchronization was complete, the traffic returned to normal state and the drop time window might be a few seconds. [PR734966: This issue has been resolved.]
- Distributed BFD was enabled by default, which could cause BFD flaps in case of chassis cluster failover. [PR747363: This issue has been resolved.]
- On devices in a chassis cluster, the forwarding module was not responsive when the redundant Ethernet interface was deleted while traffic was flowing through the device. Sometimes flowd generated a core file. [PR771273: This issue has been resolved.]
- LACP failed due to problems with distributed PPM not working properly. [PR781736: This issue has been resolved.]
- DHCP option 82 commit failed. The device generated a core file, and the configurations failed. [PR794522: This issue has been resolved.]

Command-Line Interface (CLI)

- For naming a security zone, usage of word management and its variants were not supported. [PR754585: This issue has been resolved.]
- The **set chassis fpc pic services-offload** command did not work. [PR787526: This issue has been resolved.]

Flow and Processing

- The diagnostic script failed for recb_i2c_rep_clk_generator functionality. [PR602621: This issue has been resolved.]
- Changes in policer, filter, or sampling configuration caused core files when multicast traffic was received. [PR613782: This issue has been resolved.]
- On SRX3400 and SRX3600 devices, CPU utilization was high at 75 to 85 percent on FPCs when 4000 IFLs were configured on redundant Ethernet (reth) interfaces. [PR670925: This issue has been resolved.]
- The **Link failure happened for DPC%d PFE%d** log message displayed an incorrect FPC number. [PR683371: This issue has been resolved.]
- When the syn-cookie feature was enabled along with syn-flood screen with a low timeout value, high-latency TCP sessions might fail to establish successfully. The client sessions received unresponsive connections because the SRX Series device timed out the flow for the session. The device also dropped subsequent packets from the client due to the state not being found. [PR692484: This issue has been resolved.]
- The content filter for the SMTP block extension did not work when the name of the attached file was in Japanese. [PR724960: This issue has been resolved.]
- High CPU use due to the mgd process might result when the **run show config** command was specified during configuration mode. In addition, the httpd process was high. [PR729617: This issue has been resolved.]
- The flow bytes counters tracked on a per-interface basis were incorrect for IPv6 flows, and flow output bytes statistics were reversed to the source or destination interfaces. [PR740911: This issue has been resolved.
- After upgrading to Junos OS Release 12.1, if a commit was tried after a commit was confirmed, the following error message was displayed:

  error: problem checking file: No such file or directory.

  [PR741239: This issue has been resolved.]
- For the loopback interface traffic, if the traffic processed by IDP or ALGs that require serialized packet processing, traffic dropped due to serialization bit loss in session creation stage. [PR741743: This issue has been resolved.]
- The captive portal redirect did not work with the strict synchronization checking option enabled in the firewall. [PR743466: This issue has been resolved.]
- The **show security pki *-certificate** command showed the time without the time zone. [PR746785: This issue has been resolved.]

- Commands after STARTTLS were encrypted, and could not be understood by the SMTP parser. These commands caused the session to hang until the TCP session was closed, so packets were not forwarded. [PR750047: This issue has been resolved.]
- Inbound "to-self" SSH traffic was accepted by the device even though "ssh" was not explicitly included in the "host-inbound-traffic" configuration for the ingress interface within the security zone. [PR754392: This issue has been resolved.]
- A timing issue in the ttymodem() internal I/O processing routine caused the Junos OS kernel to crash. The crash was triggered by simple remote access (for example, Telnet, SSH) to the device. [PR755448: This issue has been resolved.]
- When SYN flood packets per second (pps) over the screen attack-threshold, a synchronization cookie was triggered by default. [PR755727: This issue has been resolved.]
- When an FPC restart was performed, some of the PICs and IFDs were unable to be created by chassisd due to an EBUSY error returned by the kernel. The kernel was unable to process the new requests until the previous states of the same object (PIC, IFD in one case) were consumed by all peers. [PR769632: This issue has been resolved.]
- SYN-PROXY held the jbuf before SYN-ACK was received from the server. If the server was unreachable, SYN-PROXY held the jbuf until the session was timed out. In addition, firewall authentication generated a core file if a GET request that contained a long Uniform Resource Identifier (URI) was received. [PR769828: This issue has been resolved.]
- In certain cases, when the device was processing a large amount of traffic, performing an AppID security package update might cause the flowd process to generate a core file. [PR769832: This issue has been resolved.]
- When an RLAG was configured with an active LACP and the SRX Series high-end firewall cluster was upgraded through ISSU, there was traffic and session loss. The traffic drop time was dependent on the number of links per node for an RLAG, and also the type of active LACP used (that is, fast or slow).

  [PR770653: This issue has been resolved.]
- For IKEv2 only, when the device attempted a dpd exchange when an existing exchange was in progress, a core file might have been generated. [PR771234: This issue has been resolved.]
- The routing protocol daemon (rpd) generated a core file while processing a malformed RIP or RIP message from a neighbor during adjacency establishment. [PR772601: This issue has been resolved.]
- When the HTTPD process restarted, the HTTPD process was deleted and new was started. In certain circumstances, however, the old and the new HTTPD processes existed at the same time, causing high CPU usage. [PR772701: This issue has been resolved.]
- When syn-flood and session limitation screen features were enabled, and when there were 16,000 or more source or destination IP addresses, the connections per second data might drop 50 percent. [PR773162: This issue has been resolved.]

- If an IKEv2 SA lifetime was more than 65,535 seconds, the IKE SA would not rekey. It expired and the corresponding tunnel flapped, causing traffic outage. [PR775595: This issue has been resolved.]
- When there was heavy traffic, the FIOC interface did not respond. [PR776179: This issue has been resolved.]
- The message log was too granular, indicating blower speed changes frequently from normal to intermediate speed. As a result, logs were overfilled, making it difficult to troubleshoot them. [PR776254: This issue has been resolved.]
- RPD memory leak occurred when SNMP polled BGP and BGP was not configured. [PR776637: This issue has been resolved.]
- When data path debugging was configured, fragmented traffic was dropped. [PR777381: This issue has been resolved.]
- The session creation per second was always zero in the **show security monitoring fpc 0** output. [PR787343: This issue has been resolved.]
- After a Routing Engine switchover, LACP and MIB process (mib2d) core files were created. [PR790966: This issue has been resolved.]
- When LACP was configured in fast mode, interface flapping might occur if the SPC's central point CPU utilization was very high (over 90 percent). [PR792513: This issue has been resolved.]
- If security policies were configured with a large number of applications using the same source and destination ports, then policy configuration updates might not work as expected. [PR793151: This issue has been resolved.]
- Core files might be generated when Stream Control Transmission Protocol (SCTP) packets were processed. [PR793303: This issue has been resolved.]
- When the SPU booted up (at the time of device start or after any other kind of SPU reset), the device logged messages on the Routing Engine with the wrong timestamp. [PR803286: This issue has been resolved.]
- When application QoS was configured, and if traffic did not match the configured AppQoS rules, a flowd core was generated. [PR805562: This issue has been resolved.]
- The INET MTU on the secure tunnel interface did not return to the default value. [PR805883: This issue has been resolved.]
- When you committed any changes under logical system configuration, the security policy failed to resolve the DNS objects that were in the security address book. As a result, the traffic hit other unexpected security policies, or default-deny instead, causing a traffic outage. [PR810723: This issue has been resolved.]
- The TCP sessions and the processing of FIN and RST packets did not work correctly. [PR814370: This issue has been resolved.]
- If traffic was fragmented and had to be reassembled, and when the reassembled data was larger than the path maximum transmission unit (PMTU) of an IPv6 multicast address (with a large size packet), the “IPv6 Too Big” message was returned to the sender and traffic was dropped. [PR818898: This issue has been resolved.]

General Packet Radio Service (GPRS)

- When GTP inspection was globally enabled, the GTP sanity check was dropped, resulting in badly formatted GTP packets, even if GTP inspection had not been configured on the security policy. [PR790143: This issue has been resolved.]

Hardware

- In Junos OS Release 11.2R7, CL73-AN was inadvertently enabled for ports 7, 8, and 9 on the 1 Gigabit Ethernet SYSIO card. As a result, links failed to come up on these ports. [PR787010: This issue has been resolved.]

Installation and Upgrade

- When you installed AI Scripts (part of the Service Now product) on a device with a very large configuration (more than 100,000 lines), the cscript daemon might crash, resulting in a core file. [PR736138: This issue has been resolved.]

Interfaces and Routing

- On devices in a chassis cluster, a maximum of 8 queues per interface configuration were not reflected on the interface part of the cluster setup. [PR389451: This issue has been resolved]
- Egress queues were not supported on VLAN or IRB interfaces. [PR510568: This issue has been resolved.]
- The Track IP (ipmon) feature was not working for VLAN tagged redundant Ethernet interfaces. (PR575754: This issue has been resolved.]
- When a defective 16-Port SFP Gigabit Ethernet IOC was inserted on the device, all other SFP cards were no longer recognized. [PR711461: This issue has been resolved.]
- The ICMP redirect did not work for redundant Ethernet interfaces. [PR746374: This issue has been resolved.]
- The aggregated Ethernet interface might go down after users configured Active LACP on the back-to-back connected AE bundles. [PR770998: This issue has been resolved.]
- When multiple interfaces were bound to the same security zone, if the first fragmented packet and the second fragmented packet arrived in different interfaces, the second fragmented packet was dropped. [PR777343: This issue has been resolved.]
- Interfaces without cable connected and configured with the loopback option were not coming up. [PR788395: This issue has been resolved.]
- After reboot, sometimes the interface VLAN was down when the member physical interface was up. [PR795363: This issue has been resolved.]

- With a large number of tunnel routes added, memory utilization could become very high. [PR797845: This issue has been resolved.]
- After upgrading to Junos OS Release 11.4R5, if OSPF was enabled for any of the st0 interfaces, an internal processing error prevented the default route from being advertised out. [PR822352: This issue has been resolved.]

Intrusion Detection and Prevention (IDP)

- The application groups statistics were shown as **unassigned** and **unknown** for the **show services application-identification statistics application-groups** command output without displaying the details. [PR740014: This issue has been resolved.]
- After 24 hours of a slt4 stress run with a huge number of sessions generated, IDP sessions were not increasing along with flow sessions. [PR742882: This issue has been resolved.]
- The detector was not updated in the control plane when the update-attack-database-only flag was used during security package installation. [PR778816: This issue has been resolved.]
- A new filter was added in dynamic attack groups in the CLI. The two flags under filters are **recommended** (which means true) and **not-recommended** (which means false). Only the **recommended=true** flag was supported. [PR828494: This issue has been resolved.]

IPv6

- The NP hash feature did not work with IPv6 for the cross virtual router (VR) traffic. [PR738812: This issue has been resolved.]

J-Web

- If multiple J-Web clients were connected to a single device, it caused high CPU utilization on the Routing Engine. [PR741432: This issue has been resolved.]
- The source interface for IP monitoring must be a logical interface. However, the corresponding configuration screen on J-Web did not list logical interface and only listed physical interface. [PR754523: This issue has been resolved.]
- Users could not add custom applications that had the substring “any” in the name to a policy with other applications. [PR755495: This issue has been resolved.]
- If a configuration error was made on the J-Web CLI editor after the user had already committed changes in the same editor, the validation failed and previous committed changes would be lost in the editor. All previous changes had to be reentered in the CLI editor to avoid an incorrect commit anytime the J-Web CLI editor was used. [PR771660: This issue has been resolved.]

- On devices with more than one SPC installed, in J-Web, you could only view the flow sessions from one SPC. Flow sessions on the other SPCs could not be displayed. [PR777520: This issue has been resolved.]
- When you logged in to J-Web, the message, "J-WEB is not supported on this platforms" was displayed. [PR781659: This issue has been resolved.]

Logical Systems

- The BFD session on routing protocols for logical systems was not working. [PR671444: This issue has been resolved.]
- Fragmentation was affected when traffic passed through logical systems LT and/or GRE interface in the routing instance. [PR738449: This issue has been resolved.]
- On devices running Junos OS Release 11.2, when a logical system feature was added, diagnostic information was sent to a specific file without rotation control, causing core files to be generated. [PR721104: This issue has been resolved.]
- When two or more IDP policies were configured in the root logical system and one policy was active in the root logical system and a different policy was active in the custom logical system, the referenced logical system policy might not get compiled properly after a signature update. [PR749126: This issue has been resolved.]
- The flowd process (the process responsible for traffic forwarding in SRX Series devices) might crash when running on a logical system. [PR780019: This issue has been resolved.]

Network Address Translation (NAT)

- On devices in a chassis cluster, some central point binding entries did not age out after a stress test. [PR611827: This issue has been resolved.]
- IDP SSL proxy AI displayed two AI cache entries with single SSL session when destination NAT was enabled on the device. [PR687311: This issue has been resolved.]
- Flowd core files were generated when persistent NAT binding entries were cleared. [PR697856: This issue has been resolved.]
- NAT resources (address and port) were not fully utilized when port range was specified. [PR754886: This issue has been resolved.]
- It was possible to configure a security zone in the format a.b.c.d. However, when the same zone name was referenced while configuring NAT, a configuration error occurred. [PR748621: This issue has been resolved.]
- Commit of static NAT rules might fail when you committed interfaces, security zone, and NAT at same time in the root or logical system. In addition, the commit of static NAT rules might fail when you committed for security zone and NAT at the same time. [PR756240: This issue has been resolved.]
- Sometimes cone-NAT binding was released extremely slowly when clear sessions and bindings had too many sessions and there were close to 65,536 bindings. [PR747777: This issue has been resolved.]

- Static NAT rules were not being enforced when the Ethernet switching family was used. [PR785106: This issue has been resolved.]
- Persistent NAT table entries could not be removed on the central point when the device was under heavy traffic. [PR807524 , PR819603: This issue has been resolved.]

Security Policies

- Logical systems with policy count option displayed the statistics after a while following a **show** command, or the counters stopped to increment if both redundant groups were not on same node as a result of failover. [PR782546: This issue has been resolved.]

SNMP

- SNMP OID jnxOperatingCPU.9 (Routing Engine CPU usage) always returned 100, although Routing Engine CPU usage was not 100 percent. [PR739591: This issue has been resolved.]
- On devices in a chassis cluster, long pauses and timeout were seen during SNMP walk or query of the device. A delay occurred in the kernel's query of the gr-0/0/0 (GRE) interface. [PR800735: This issue has been resolved.]
- Routing Engine failover occurred due to possible out-of-sync information about already allocated SNMP interface index values, and duplicate SNMP interface index values might be allocated. As a result, the mib2d process might crash or the SNMP interface index value of zero might be allocated for newly created interfaces. [PR806098: This issue has been resolved.]
- SNMP query for maximum total session (jnxJsSPUMonitoringMaxTotalSession) was taking the maximum value, that is, max-cp-session value. [PR838214: This issue has been resolved.]

System Logs

- When an idle session is closed based on timeout expiration, the close reason shown in logs displayed "idle Timeout", instead of "unset" as it appeared before. [PR746572: This issue has been resolved.]
- The performance monitor message format has been changed. The message format previously generated a rtlogd core file and rtlogd restarted automatically after 1 or 2 seconds. [PR819700: This issue has been resolved.]
- Session-close system log messages were not as expected. [PR822509: This issue has been resolved.]

Unified Threat Management (UTM)

- On the devices, there used to be a requirement for the support of both “STARTTLS” and “X-ANONYMOUSTLS” cases for the SMTP parser. [PR824027: This issue has been resolved.]

- The Juniper Networks enhanced Web filtering feature experienced default, timeout, and connectivity fallback actions under sustained bursts of high traffic. [PR833768: This issue has been resolved.]

Virtual Private Network (VPN)

- The dynamic VPN license was not released when the old dynamic VPN connections were terminated. [PR735615: This issue has been resolved.]
- An error "Failed to connect to server" was displayed when multiple clients were connected to the device through dynamic VPN and when some configurations related to IKE negotiation changed on the device. [PR737787: This issue has been resolved.]
- IKE Phase 1 and Phase 2 logs erroneously reported that the renegotiation retry limit had been reached, even though the VPN build was successful. [PR741751: This issue has been resolved.]
- In some IPsec VPN scenarios where RG1+ failover occurred consecutively and in short periods of time (less than 5 minutes), sometimes the ESP sequence number would not be synchronized on the other cluster node. As a consequence, after failover, traffic was sent inside the IPsec tunnel with an incorrect ESP sequence number. When antireplay functionality was enabled on the remote peer, traffic blocking occurred on the remote VPN. [PR753683: This issue has been resolved.]
- When **load override** was used to load a new VPN configuration, flow and IKE daemons might generate core files and VPN tunnels might not be established. [PR773482: This issue has been resolved.]
- The following IKE traceoption messages were printed while debugging VPN tunnels:

  ```
  Aug 2 09:27:03 srx-5800-1 (FPC Slot 0, PIC Slot 1) SPC0_PIC1 kmd[213]: IKE Phase-1
  Failure: (null) [spi=75ffd1a8, src_ip=<none>, dst_ip=A.A.A.A]
  Aug 2 09:27:06 srx-5800-1 (FPC Slot 0, PIC Slot 1) SPC0_PIC1 kmd[214]: IKE Phase-1
  Failure: (null) [spi=75ffd1a8, src_ip=<none>, dst_ip=B.B>B>B]
  ```

  The same SPI value was printed for two different peer IP addresses, which should not be the case. A memory address of SPI was printed instead of SPI address itself. Also, the invalid cookie reason was not printed due to this message. [PR803294: This issue has been resolved.]
- When building a GRE over an IPsec VPN tunnel, the device did not use GRE protocol 47 in the proxy-id for IKE Phase 2 negotiation. [PR806233: This issue has been resolved.]
- The tcp-proxy in flowd hangs while processing TCP RST packets with data padding. This resulted in the mbuf pool getting filled up. [PR806269: This issue has been resolved.]

Related Documentation

- New Features in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 98
- Known Limitations in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 134

Errata and Changes in Documentation for Junos OS Release 12.1X44 for High-End SRX Series Services Gateways

Errata for the Junos OS Software Documentation

This section lists outstanding issues with the software documentation.

Feature Support Reference for SRX Series and J Series Devices

- The “IPv6 Support“ table lists that IPv6 is supported only for TFTP ALG. The correct information is IPv6 is supported for DNS, FTP, and TFTP ALGs.

J-Web

- **J-Web pages for stateless firewall filters**—There is no documentation describing the J-Web pages for stateless firewall filters. To find these pages in J-Web, go to **Configure>Security>Firewall Filters**, and then select **IPv4 Firewall Filters** or **IPv6 Firewall Filters**. After configuring the filters, select **Assign to Interfaces** to assign your configured filters to interfaces.

Junos OS Layer 2 Bridging and Switching Configuration Guide for Security Devices

- In this guide, the section “Configuring Layer 2 Bridging and Transparent Mode” includes an incorrect example, “Example: Configuring Layer 2 Trunk Interfaces with Multiple Units.” SRX Series devices do not support multiple units.

Junos OS CLI Reference

- In the “show security policies” topic, the “show security policies Output Fields” table includes the following incorrect information:

Applications	**ALG**: If an ALG is associated with the session, the name of the ALG. Otherwise, 0.

The correct information is:

Applications	**ALG**: If an ALG is explicitly associated with the policy, the name of the ALG is displayed. If **application-protocol ignore** is configured, ignore is displayed. Otherwise, 0 is displayed. However, even if this command shows ALG: 0, ALGs might be triggered for packets destined to well-known ports on which ALGs are listening, unless ALGs are explicitly disabled or when **application-protocol ignore** is not configured for custom applications.

- In this guide, the **source-threshold** statement incorrectly shows a default value of 1024 per second for number in the Options section. The correct default value is 4000 per second.
- The **edit applications application *application-name* term *term-name*** hierarchy level for the alg (Applications) configuration statement is incorrect. The correct hierarchy level is **edit applications application *application-name*<term *term-name*>**.

Junos OS Security Basics

- The topic Understanding Policy Application Timeouts Contingencies under **Security Basics > Security Policy Applications for Security Devices > Policy Application Timeout**, contains erroneous information. It should read as follows:

  When setting timeouts, be aware of the following contingencies:

  - If an application contains several application rule entries, all rule entries share the same timeout. You need to define the application timeout only once. For example, if you create an application with two rules, the following commands will set the timeout to **20** seconds for both rules:

    ```
    user@host# set applications application test protocol tcp destination-port 1035-1035
    inactivity-timeout 20
    user@host# set applications application test term test protocol udp
    user@host# set applications application test term test source-port 1-65535
    user@host# set applications application test term test destination-port 1111-1111
    ```

  - If multiple custom applications are configured with custom timeouts, then each application will have its own custom application timeout. For example:

    ```
    user@host# set applications application ftp-1 protocol tcp source-port 0-65535
    destination-port 2121-2121 inactivity-timeout 10
    user@host# set applications application telnet-1 protocol tcp source-port 0-65535
    destination-port 2300-2348 inactivity-timeout 20
    ```

    With this configuration, Junos OS applies a 10-second timeout for destination port **2121** and a 20-second timeout for destination port **2300** in an application group.

Junos OS Security Configuration Guide

- In “Example: Configuring AppTrack,” of the *Junos OS Security Configuration Guide for Security Devices*, the **set security log mode stream** statement was omitted from the log configuration statements. The updated log configuration should read:

  ```
  user@host# set security log mode stream
  user@host# set security log format sd-syslog
  user@host# set security log source-address 5.0.0.254
  user@host# set security log stream app-track-logs host 5.0.0.1
  ```

- In the “Understanding SIP ALGs and NAT” topic, information in the following sections is incorrect:

  - **Call Re-INVITE Messages**

    This section incorrectly states:

    When one or more media sessions are removed from a call, pinholes are closed and bindings released just as with a BYE message.

The correct information is:

When all the media sessions or media pinholes are removed from a call, the call is removed when a BYE message is received.

  - **Call Session Timers**

    This section incorrectly states:

    The SIP ALG uses the **session-expires** value to time out a session if a Re-INVITE or UPDATE message is not received. The ALG receives the **session-expires** value, if present, from the 200 OK responses to the INVITE and uses this value for signaling timeout. If the ALG receives another INVITE before the session times out, the ALG resets all timeout values to this new INVITE or to default values, and the process is repeated. As a precautionary measure, the SIP ALG uses hard timeout values to set the maximum amount of time a call can exist.

    The correct information is (The **session-expires** value is not supported on SRX Series devices):

    As a precautionary measure, the SIP ALG uses hard timeout values to set the maximum amount of time a call can exist.

  - **Table Requesting Messages with NAT Table**

    This table incorrectly states:

Outbound Request (from private to public	Route:	Replace ALG address with local address

    The correct information is:

Outbound Request (from private to public	Route:	Replace local address with ALG address

- This guide incorrectly lists the following topics. These commands are not supported:
  - **disable-call-id-hiding**
  - **show security alg sip transactions**

Junos OS Security interfaces

- The "Example: Configuring Multilink Frame Relay FRF.16" topic provides the following incorrect configuration information:

  Step: Set device R0 as a DCE device.

```
[edit interfaces lsq-0/0/0]
user@host# set dce
```

  The correct configuration information is

  Step: Set device R0 as a DCE device.

```
[edit interfaces lsq-0/0/0:0]
user@host# set dce
```

Junos OS Security Network Address Translation

- In Example: Configuring NAT for Mulitple ISPs under Network Address Translation for Security Devices > Configuration > NAT for Multiple ISPs the statement **set routing-options rib-groups isp import-rib inet.0** was omitted from the configuration. The updated configuration should read:

  ```
  set routing-options rib-groups isp import-rib inet.0
  set routing-options rib-groups isp import-rib isp1.inet.0
  set routing-options rib-groups isp import-rib isp2.inet.0
  ```

  In addition, because zone based address-book for NAT rules is unsupported, you should not use the statements provided in the example; use global address book instead.

- The command **show security nat source persistent-nat-table** under **Network Address Translation > Administration > Source NAT Operational Commands** is:

  - Missing the option:**summary**—Display persistent NAT bindings summary.
  - Contains incomplete sample output. The corrected sample output is as follows:

```
user@host> show security nat source persistent–nat–table internal-ip 9.9.9.1 internal-port
60784


Internal                        Reflective        Source     Type
Left_time/  Curr_Sess_Num/ Source
 In_IP  In_Port I_Proto Ref_IP    Ref_Port R_Proto NAT Pool
Conf_time   Max_Sess_Num    NAT Rule
9.9.9.1  60784   udp  66.66.66.68  60784     udp   dynamic-customer-source
any-remote-host  254/300  0/30 105
```

```
user@host> show security nat source persistent–nat–table all
 Internal             Reflective                  Source     Type
Left_time/  Curr_Sess_Num/  Source
 In_IP     In_Port I_Proto Ref_IP       Ref_Port R_Proto NAT Pool
       Conf_time   Max_Sess_Num    NAT Rule
9.9.9.1    63893   tcp    66.66.66.68   63893     tcp    dynamic-customer-source
 any-remote-host  192/300   0/30 105
9.9.9.1    64014   udp    66.66.66.68   64014     udp    dynamic-customer-source
 any-remote-host  244/300   0/30 105
9.9.9.1    60784   udp    66.66.66.68   60784     udp    dynamic-customer-source
 any-remote-host  254/300   0/30 105
9.9.9.1    57022   udp    66.66.66.68   57022     udp    dynamic-customer-source
 any-remote-host  264/300   0/30 105
9.9.9.1    53009   udp    66.66.66.68   53009     udp    dynamic-customer-source
 any-remote-host  268/300   0/30 105
9.9.9.1    49225   udp    66.66.66.68   49225     udp    dynamic-customer-source
 any-remote-host  272/300   0/30 105
9.9.9.1    52150   udp    66.66.66.68   52150     udp    dynamic-customer-source
 any-remote-host  274/300   0/30 105
9.9.9.1    59770   udp    66.66.66.68   59770     udp    dynamic-customer-source
 any-remote-host  278/300   0/30 105
9.9.9.1    61497   udp    66.66.66.68   61497     udp    dynamic-customer-source
 any-remote-host  282/300   0/30 105
9.9.9.1    56843   udp    66.66.66.68   56843     udp    dynamic-customer-source
 any-remote-host    -/300   1/30 105
```

```
user@host> show security nat source persistent-nat-table summary
Persistent NAT Table Statistics on FPC5 PIC0:
binding total : 65536
```

```
binding in use : 0
enode total : 524288
enode in use : 0
```

Junos OS Security Policies

The “Best Practices for Defining Policies on High-End SRX Series Devices” topic states that the SRX Series devices support up to 1024 source and destination address objects.

NOTE: The number of source and destination address objects allowed per firewall rule is 1024. The systemwide maximum allowed is 32,000 address objects.

Junos OS System Log Messages Reference

- The *AV System Log Messages* topic lists incorrect facilities for the systems logs.

  On all SRX Series devices, antivirus (AV) system logs are generated with the facility **LOG_USER** or **LOG_DAEMON**.

  Table 17 on page 176 shows the correct facilities for the system logs.

Table 17: Antivirus System Logs

System Logs	Incorrect Facility	Correct Facility
AV_PATTERN_GET_FAILED	LOG_FIREWALL	LOG_DAEMON
AV_PATTERN_KEY_EXPIRED	LOG_FIREWALL	LOG_DAEMON
AV_PATTERN_KL_CHECK_FAILED	LOG_FIREWALL	LOG_DAEMON
AV_PATTERN_TOO_BIG	LOG_FIREWALL	LOG_DAEMON
AV_PATTERN_UPDATED	LOG_FIREWALL	LOG_DAEMON
AV_PATTERN_WRITE_FS_FAILED	LOG_FIREWALL	LOG_DAEMON
AV_SCANNER_READY	LOG_FIREWALL	LOG_DAEMON
AV_VIRUS_DETECTED_MT	LOG_PFE	LOG_USER

User Role Firewall

- In *Example: Configuring a User Role Firewall on an SRX Series Device* and *Acquiring User Role Information from an Active Directory Authentication Server*, the **redirect-url** option in step 2 of the redirection procedure is incorrect. The URL and variables should be enclosed in quotation marks.

  ```
  [edit]
  user@host# set services unified-access-control captive-portal acs-device
  redirect-url “https://%ic-url%/?target=%dest-url%&enforcer=%enforcer-id%”
  ```

VPN for Security Devices

- In “Example: Configuring a Route-Based VPN,” the **show security zones** output for the SRX Series device erroneously shows host-inbound-traffic configured for the vpn-chicago zone; this configuration is not included in the CLI Quick Configuration and the Step-by-Step Procedure.

Various Guides

- 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 the *Junos OS Feature Support Reference for SRX Series and J Series Devices*.

Related Documentation

- New Features in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 98
- Known Limitations in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 134
- Outstanding Issues in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 150
- Resolved Issues in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 153

Upgrade and Downgrade Instructions for Junos OS Release 12.1X44 for High-End SRX Series Services Gateways

This section includes the following topics:

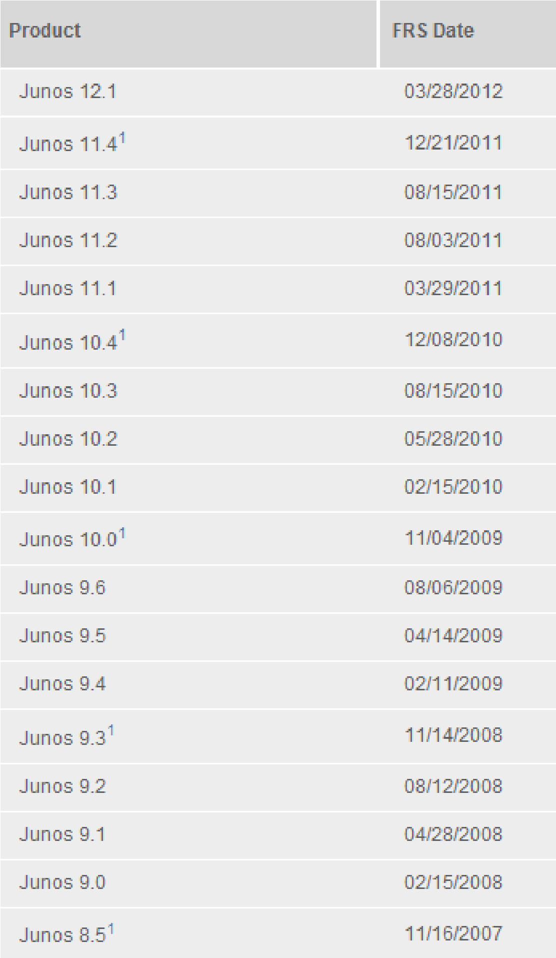
- Upgrading and Downgrading among Junos OS Releases on page 177
- Upgrading an AppSecure Device on page 179
- Upgrade and Downgrade Scripts for Address Book Configuration on page 179
- Upgrade Policy for Junos OS Extended End-Of-Life Releases on page 182
- Hardware Requirements for Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 182

Upgrading and Downgrading among Junos OS Releases

All Junos OS releases are listed in sequence on the JUNOS Software Dates & Milestones webpage:

http://www.juniper.net/support/eol/junos.html

To help in understanding the examples that are presented in this section, a portion of that table is replicated here. Note that releases footnoted with a 1 are Extended End-of-Life (EEOL) releases.



Product	FRS Date
Junos 12.1	03/28/2012
Junos 11.4[1]	12/21/2011
Junos 11.3	08/15/2011
Junos 11.2	08/03/2011
Junos 11.1	03/29/2011
Junos 10.4[1]	12/08/2010
Junos 10.3	08/15/2010
Junos 10.2	05/28/2010
Junos 10.1	02/15/2010
Junos 10.0[1]	11/04/2009
Junos 9.6	08/06/2009
Junos 9.5	04/14/2009
Junos 9.4	02/11/2009
Junos 9.3[1]	11/14/2008
Junos 9.2	08/12/2008
Junos 9.1	04/28/2008
Junos 9.0	02/15/2008
Junos 8.5[1]	11/16/2007

You can directly upgrade or downgrade between any two Junos OS releases that are within three releases of each other.

- Example: Direct release upgrade

  Release 10.3 → *(bypassing Releases 10.4 and 11.1)* Release 11.2

To upgrade or downgrade between Junos OS releases that are more than three releases apart, you can upgrade or downgrade first to an intermediate release that is within three releases of the desired release, and then upgrade or downgrade from that release to the desired release.

- Example: Multistep release downgrade

  Release 11.3 → *(bypassing Releases 11.2 and 11.1)* Release 10.4 → Release 10.3

Juniper Networks has also provided an even more efficient method of upgrading and downgrading using the Junos OS EEOL releases. EEOL releases generally occur once a calendar year and can be more than three releases apart. For a list of, EEOL releases, go to http://www.juniper.net/support/eol/junos.html

You can directly upgrade or downgrade between any two Junos OS EEOL releases that are within three EEOL releases of each other.

- Example: Direct EEOL release upgrade

  Release 9.3 (EEOL) → *(bypassing Releases 10.0 [EEOL] and 10.4 [EEOL])* Release 11.4 (EEOL)

To upgrade or downgrade between Junos OS EEOL releases that are more than three EEOL releases apart, you can upgrade first to an intermediate EEOL release that is within three EEOL releases of the desired EEOL release, and then upgrade from that EEOL release to the desired EEOL release.

- Example: Multistep release upgrade using intermediate EEOL release

  Release 8.5 (EEOL) → *(bypassing Releases 9.3 [EEOL] and 10.0 [EEOL])* Release 10.4 (EEOL) → Release 11.4 (EEOL)

You can even use a Junos OS EEOL release as an intermediate upgrade or downgrade step if your desired release is several releases later than your current release.

- Example: Multistep release upgrade using intermediate EEOL release

  Release 9.6 → Release 10.0 (EEOL) → Release 10.2

For additional information about how to upgrade and downgrade, see the *Junos OS Installation and Upgrade Guide*.

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 11.4, 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 12 on page 181).

- About Upgrade and Downgrade Scripts on page 180
- Running Upgrade and Downgrade Scripts on page 181

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.

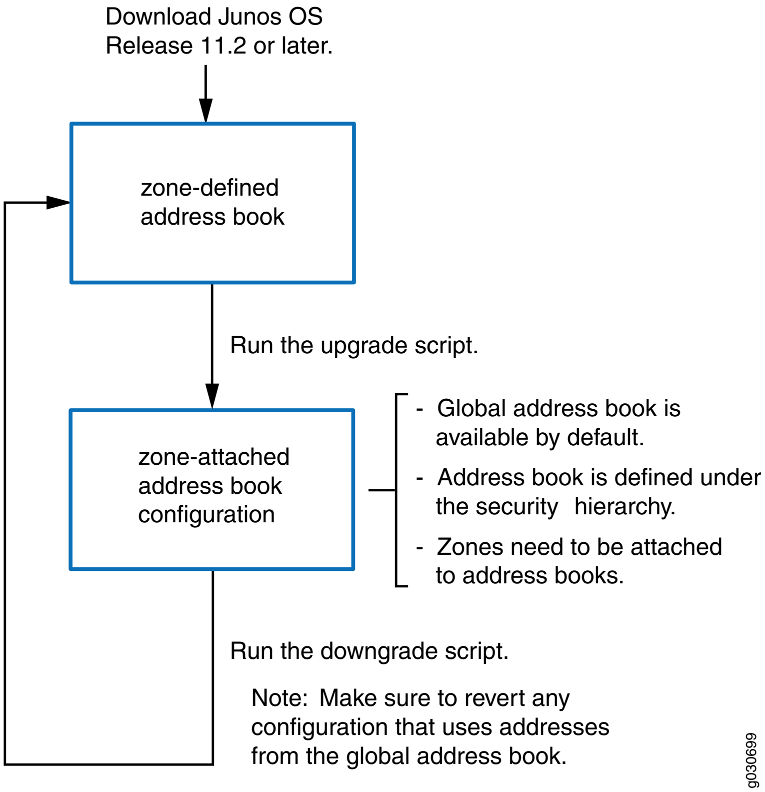
  After upgrading to the zone-attached address book configuration:

  - 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 11.4 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 12: 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 11.4 or later 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 Policy for Junos OS 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 on EEOL releases and to review a list of EEOL releases, see http://www.juniper.net/support/eol/junos.html .

Hardware Requirements for Junos OS Release 12.1X44 for High-End SRX Series Services Gateways

Transceiver Compatibility for SRX Series Devices

We strongly recommend that only transceivers provided by Juniper Networks be used on high-end SRX Series Services Gateways 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.

Related Documentation

- New Features in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 98
- Errata and Changes in Documentation for Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 172
- Changes in Default Behavior and Syntax in Junos OS Release 12.1X44 for High-End SRX Series Services Gateways on page 123

Junos OS Documentation and Release Notes

For a list of related Junos OS documentation, see http://www.juniper.net/techpubs/software/junos/.

If the information in the latest release notes differs from the information in the documentation, follow the *Junos OS Release Notes.*

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

Juniper Networks supports a technical book program to publish books by Juniper Networks engineers and subject matter experts with book publishers around the world. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration using the Junos operating system (Junos OS) and Juniper Networks devices. In addition, the Juniper Networks Technical Library, published in conjunction with O'Reilly Media, explores improving network security, reliability, and availability using Junos OS configuration techniques. All the books are for sale at technical bookstores and book outlets around the world. The current list can be viewed at http://www.juniper.net/books.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to **techpubs-comments@juniper.net**, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number
- Software release version

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/.

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/ .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, visit us at http://www.juniper.net/support/requesting-support.html.

If you are reporting a hardware or software problem, issue the following command from the CLI before contacting support:

```
user@host> request support information | save filename
```

To provide a core file to Juniper Networks for analysis, compress the file with the **gzip** utility, rename the file to include your company name, and copy it to **ftp.juniper.net:pub/incoming**. Then send the filename, along with software version information (the output of the **show version** command) and the configuration, to **support@juniper.net**. For documentation issues, fill out the bug report form located at https://www.juniper.net/cgi-bin/docbugreport/.

Revision History

08 August 2013—Revision 2, Junos OS 12.1X44-D20 – High End SRX Series, Branch SRX Series, and J Series.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.