Junos® OS 12.1X45 Release Notes

Release 12.1X45-D15
21 October 2013
Revision 4

These release notes accompany Release 12.1X45-D15 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, J Series Services Routers, and LN Series 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 6
New and Changed Features in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers 6
Software Features 7
Changes in Behavior and Syntax in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers 21
AppSecure 21
Application Firewall 22
Command-Line Interface (CLI) 23
Compatibility 25
Flow and Processing 25
Hardware 26
Interfaces and Routing 26
Intrusion Detection and Prevention (IDP) 26
J-Web 27
Screen 28
Simple Network Management Protocol (SNMP) 28
System Logs 28
Virtual Private Network (VPN) 29

Known Behavior in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers . . . 30
AppSecure . . . 30
AX411 Access Points . . . 31
Chassis Cluster . . . 31
Command-Line Interface (CLI) . . . 32
Connectivity Fault Management (CFM) . . . 32
Dynamic Host Configuration Protocol (DHCP) . . . 32
Flow and Processing . . . 33
Interfaces and Routing . . . 34
Intrusion Detection and Prevention (IDP) . . . 38
IPv6 . . . 40
J-Web . . . 40
Layer 2 Transparent Mode . . . 42
Network Address Translation (NAT) . . . 42
Power over Ethernet (PoE) . . . 43
Security Policies . . . 43
Simple Network Management Protocol (SNMP) . . . 44
Switching . . . 44
Unified Threat Management (UTM) . . . 45
Upgrade and Downgrade . . . 45
USB . . . 45
Virtual Private Network (VPN) . . . 45
Unsupported CLI for Branch SRX Series Services Gateways and J Series Services Routers . . . 47
Known Issues in Junos OS Release 12.1X45-D15 for Branch SRX Series Services Gateways and J Series Services Routers . . . 58
Application Layer Gateways (ALG) . . . 58
Chassis Cluster . . . 58
Dynamic Host Configuration Protocol (DHCP) . . . 58
Flow and Processing . . . 58
Interfaces and Routing . . . 59
Intrusion Detection and Prevention (IDP) . . . 59
J-Web . . . 59
Network Address Translation (NAT) . . . 60
Network Management and Monitoring . . . 60
Platform and Infrastructure . . . 60
Screen . . . 61
Switching . . . 61
System Logs . . . 61
Unified Threat Management (UTM) . . . 61
Virtual Private Network (VPN) . . . 61
Resolved Issues in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers . . . 63
Resolved Issues in Junos OS Release 12.1X45-D15 for Branch SRX Series Services Gateways . . . 63
Resolved Issues in Junos OS Release 12.1X45-D10 for Branch SRX Series Services Gateways . . . 66

Documentation Updates for Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers . . . 74
Documentation Updates for the Junos OS Software Documentation . . . 74
Documentation Updates for the Junos OS Hardware Documentation . . . 78
Migration, Upgrade, and Downgrade Instructions for Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers . . . 81
Upgrading and Downgrading among Junos OS Releases . . . 81
Upgrading an AppSecure Device . . . 83
Upgrade and Downgrade Scripts for Address Book Configuration . . . 83
Hardware Requirements for Junos OS Release 12.1X45 for SRX Series Services Gateways and J Series Services Routers . . . 86
Junos OS Release Notes for High-End SRX Series Services Gateways . . . 89
New and Changed Features in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways . . . 89
Release 12.1x45-D15 Software Features . . . 89
Release 12.1x45-D10 Software Features . . . 90
Changes in Behavior and Syntax in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways . . . 105
AppSecure . . . 106
Application Firewall . . . 107
Command-Line Interface (CLI) . . . 108
Compatibility . . . 111
Flow and Processing . . . 111
Intrusion Detection and Prevention (IDP) . . . 111
Management Information Base (MIB) . . . 113
Screen . . . 113
Session Timeout for Reroute Failure . . . 113
SNMP . . . 113
System Logs . . . 113
Unified In-Service Software Upgrade (ISSU) . . . 114
Virtual Private Network (VPN) . . . 114
Known Behavior in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways . . . 116
AppSecure . . . 116
Chassis Cluster . . . 116
Dynamic Host Configuration Protocol (DHCP) . . . 118
Flow and Processing . . . 118
General Packet Radio Service (GPRS) . . . 118
Interfaces and Routing . . . 121
Intrusion Detection and Prevention (IDP) . . . 122
IPv6 . . . 125
J-Web . . . 126
Logical Systems . . . 126
Network Address Translation (NAT) . . . 127
Security Policies . . . 129
Services Offloading . . . 130

Simple Network Management Protocol (SNMP) . . . 131
In-Service Software Upgrade (ISSU) . . . 131
Virtual Private Network (VPN) . . . 131
Known Issues in Junos OS Release 12.1X45-D15 for High-End SRX Series Services Gateways . . . 133
Application Layer Gateways (ALG) . . . 133
Certificate Authority (CA) Profile . . . 133
Chassis Cluster . . . 133
Dynamic Host Configuration Protocol (DHCP) . . . 134
Flow and Processing . . . 134
J-Web . . . 134
Interfaces and Routing . . . 134
Network Address Translation (NAT) . . . 135
Platform and Infrastructure . . . 135
Screen . . . 135
SNMP . . . 135
System Logs . . . 135
Virtual Private Network (VPN) . . . 136
Resolved Issues in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways . . . 136
Resolved Issues in Junos OS Release 12.1X45-D15 for High-End SRX Series Services Gateways . . . 136
Resolved Issues in Junos OS Release 12.1X45-D10 for High-End SRX Series Services Gateways . . . 139
Documentation Updates for Junos OS Release 12.1X45 for High-End SRX Series Services Gateways . . . 148
Documentation Updates for the Junos OS Software Documentation . . . 148
Migration, Upgrade, and Downgrade Instructions for Junos OS Release 12.1X45 for High-End SRX Series Services Gateways . . . 152
Upgrading and Downgrading among Junos OS Releases . . . 152
Upgrading an AppSecure Device . . . 154
Upgrade and Downgrade Scripts for Address Book Configuration . . . 154
Upgrade Policy for Junos OS Extended End-Of-Life Releases . . . 157
Hardware Requirements for Junos OS Release 12.1X45 for High-End SRX Series Services Gateways . . . 157
Junos OS Release Notes for LN Series Routers . . . 158
New and Changed Features in Junos OS Release 12.1X45-D15 for LN Series Routers . . . 158
Hardware Features . . . 158
Known Behavior in Junos OS Release 12.1X45 for LN Series Routers . . . 159
LN Series . . . 159
Product Compatibility . . . 160
Hardware Compatibility . . . 160
Third-Party Components . . . 160
Finding More Information . . . 160
Junos OS Documentation and Release Notes . . . 160
Documentation Feedback . . . 161
Requesting Technical Support . . . 161

Revision History 163

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 and Changed Features in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 6
- Changes in Behavior and Syntax in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 21
- Known Behavior in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 30
- Known Issues in Junos OS Release 12.1X45-D15 for Branch SRX Series Services Gateways and J Series Services Routers on page 58
- Resolved Issues in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 63
- Documentation Updates for Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 74
- Migration, Upgrade, and Downgrade Instructions for Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 81

New and Changed Features in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers

The following features have been added to Junos OS Release 12.1X45. Following the description is the title of the manual or manuals to consult for further information.

NOTE: **For the latest updates about support and issues on Junos Pulse, see the** Junos Pulse Release Notes**.**

- Software Features on page 7

Software Features

Application Layer Gateways (ALG)

- **DDNS support**—Junos OS Release 12.1X45-D10 supports dynamic DNS (DDNS). This feature is supported on all branch SRX Series devices.

  DDNS is an addition to the DNS ALG standard. The main difference between DNS and DDNS is in the message format of the header section and the update message.

  Compared with DNS messages, DDNS messages are processed differently. Message parsing is rewritten for DDNS. DDNS performs NAT and NAT-PT in the query part of the message and DNS performs NAT and NAT-PT in the response part of the message.

  DDNS updates a DNS server with new or changed records for IP addresses without the need for human intervention. Unlike DNS that only works with static IP addresses, DDNS is also designed to support dynamic IP addresses, such as those assigned by a DHCP server. DDNS is a good option for home networks, which often receive dynamic public IP addresses from their Internet provider that occasionally change.

  DDNS ALG does not support:

  - DNS packet over TCP
  - Reverse lookup
  - Logical systems

  [*Junos OS Application Layer Gateways (ALGs) Library for Security Devices*]

  [*DNS ALG Overview*]

- **Logging improvements for ALGs**—Junos OS Release 12.1X45-D10 introduces system log messages for all ALGs. These messages are supported on all branch SRX Series and J Series devices.

  During ALG processing, every error and failure has a system log.

  There are 12 predefined tags and four levels of log options that can be utilized. The four levels at which system logs are captured during ALG processing are error, warning, notification, and debug.

  For example, when there is an open gate failure with the SUNRPC ALG, the log level for this event is **ERR**, the tag is **RT_ALG_ERR_GATE**, and the system log message is SUNRPC ALG open gate failed.

  The ALG system log messages are:

LOG Level	TAG	System Log Messages
LOG_ERR	RT_ALG_ERR_INIT	ALG initialization failed.
LOG_ERR	RT_ALG_ERR_MEM_ALLOC	Call context allocated by ALG failed.
LOG_ERR	RT_ALG_ERR_RES_ALLOC	ASL resource created by ALG failed.

LOG Level	TAG	System Log Messages
LOG_ERR	RT_ALG_ERR_NAT	NAT for ALG data session failed.
LOG_ERR	RT_ALG_ERR_GATE	ALG open gate failed.
LOG_WARNING	RT_ALG_WRN_CFG_NEED	ALG detected unusual traffic to let it pass through. Need extra configuration.
LOG_WARNING	RT_ALG_WRN_CAPACITY_LMT	ALG exceeded capacity limitation.
LOG_WARNING	RT_ALG_WRN_FLOOD	ALG messages flooding.
LOG_NOTICE	RT_ALG_NTC_FSM_DROP	ALG finite state machine mismatch.
LOG_NOTICE	RT_ALG_NTC_PKT_MALFORMED	ALG packet payload malformed.
LOG_NOTICE	RT_ALG_NTC_PARSE_ERR	ALG packet decode error.
LOG_DEBUG	RT_ALG_DEBUG	There are different debug system log messages output at this level. Example: junos-alg - RT_ALG_DEBUG [junos@2636.1.1.1.2.35 alg-name="SQL" details="detect message with packet length more than 3K, bypass"] SQL ALG detected message with packet length more than 3K, bypass.

[*Junos OS Application Layer Gateways (ALGs) Library for Security Devices*]

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

  Beginning with Junos OS Release 12.1X45-D10, 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 Transparent Mode Feature Guide for Security Devices*]

AppSecure

- **AppTrack supports IPv6 address format**—This feature is supported on all branch SRX Series devices.

  AppTrack now recognizes and logs IP addresses using the appropriate IPv4 or IPv6 format. There is no additional configuration needed to enable IPv6 support. When AppTrack is enabled, IPv6 is automatically supported for all relevant traffic.

  [*Understanding AppTrack*]

- **HTTP traffic can be redirected when denied or rejected by application firewall**—This feature is supported on all branch SRX Series devices.

  A new **block-message** option for a deny or reject policy action in an application firewall redirects the user to a splash page. By default, the following message informs the user that their traffic has been denied or rejected.

  "*username*, Application Firewall has blocked your request to application *appname* at *dst-ip*:*dst-port* accessed from *src-ip*:*src-port*\n"

  To customize this message, you can define one or more block message profiles that contain either custom text to be added to the default message or a URL to redirect users to an informative webpage. The redirection URL uses the following format:

  "*http(s)://custom-redirect-url*?JNI_SRCIP=*src-ip*
  &JNI_SRCPORT=*src-port*&JNI_DSTIP=*dst-ip*
  &JNI_DSTPORT=*dst-port*&JNI_APPNAME=*appname*
  &JNI_USER=*username*&JNI_ROLES=*rolename*
  &JNI_POLICY=*policy-id*"

  A new **profile** option in the **rule-sets** configuration identifies which profile to use for applicable rules within that rule set.

  NOTE: This option only applies to HTTP traffic on branch SRX Series devices.

  [*Application Firewall Overview*]

Chassis Cluster

- **Chassis cluster extended cluster ID**—This feature is supported on all branch SRX Series devices through CLI configuration.

  The chassis cluster feature uses cluster ID to identify a cluster in a Layer 2 domain. Fifteen separate clusters are supported with the cluster ID range of 1 through 15 (cluster ID 0 is reserved).

  With Junos OS Release 12.1X45-D10, the new range for cluster IDs using the **set chassis cluster cluster-id** command is now 1 through 255 (cluster ID 0 is reserved).

  NOTE:
  - If you create a cluster with cluster IDs greater than 16, and then decide to roll back to a previous release image that does not support extended cluster IDs, the system comes up as standalone.
  - If you have a cluster set up and running with an earlier release of Junos OS, you can upgrade to Junos OS Release 12.1X45-D10 and re-create a cluster with extended cluster IDs greater than 16. However, if for any reason you decide to revert to the previous version of Junos OS that did not support extended cluster IDs, the system comes up with standalone devices after you reboot.

DHCP

- **DHCPv6 client**—This feature is supported on all branch SRX Series and J Series devices.

  The Dynamic Host Configuration Protocol (DHCP) client feature has been enhanced to include IPv6 support. DHCPv6 client support includes the following features:

  - Identity association for nontemporary addresses (IA_NA)
  - Identity association for prefix delegation (IA_PD)
  - Rapid commit
  - TCP/IP propagation
  - Auto-prefix delegation
  - Autoconfig mode (stateful and stateless)

  To configure the DHCPv6 client on the device, include the **dhcpv6-client** statement at the [**edit interfaces**] hierarchy level.

  NOTE: To configure a DHCPv6 client in a routing instance, add the interface in a routing instance using the [**edit routing-instances**] hierarchy.

[*Administration Guide for Security Devices*]

Dual-Root Partitioning

- **Automatic recovery of primary root**—This feature is supported on all branch SRX Series devices. The auto-snapshot repairs the corrupted primary root when the device reboots from the alternate root. This is accomplished by taking a snapshot of the alternate root onto the primary root automatically rather than manually from the CLI.

  NOTE: **We recommend performing the snapshot once all the processes start. This is done to avoid any increase in the reboot time.**

  Enable this feature with the **set system auto-snapshot** command. Once the primary root partition is recovered using this method, the device will successfully boot from the primary root partition on the next reboot.

  Execute the **delete system auto-snapshot** command to delete all backed up data and disable auto-snapshot, if required.

  Use the **show system auto-snapshot** command to check the auto-snapshot status.

  When auto-snapshot is in progress, you cannot run a manual snapshot command concurrently and the following error message appears:

  ```
  Snapshot already in progress. Please try after sometime
  ```

Flow and Processing

- **Flow and route Scaling**—This feature is supported on all branch SRX Series devices.

  This feature provides enhanced route scaling configuration for better route scalability for SRX240H2 (2 GB RAM), SRX550 (2 GB RAM), and SRX650 (2 GB RAM) devices.

- **Juniper flow monitoring IPv6 version 9 (V9) support**—This feature is supported on all branch SRX Series and J Series devices.

  The existing flow monitoring IPv4 version 9 is enhanced to include the flow monitoring IPv6 version 9 support.

  When you configure the collector IP address using the **forwarding-options sampling family inet flow server** command, the flow server might be IPv4 or IPv6, but only IPv4 sampling works. Similarly, when you configure the collector IP address using the **forwarding-options sampling family inet6 flow server** command, the flow server might be IPv4 or IPv6, but only IPv6 sampling works.

  IPv6 flow monitoring V9 provides an extensible and flexible method for using IPv6 templates to export records. Each template indicates the format in which the device exports data.

  Table 1 on page 11 shows a comparison between IPv4 and IPv6 template elements.

Table 1: Flow Selector Fields

Filed Name	IPv4 (Length)	IPv6 (Length)

Table 1: Flow Selector Fields *(continued)*

Source IP Address	4 bytes	16 byte
Destination IP Address	4 bytes	16 byte
Source Port	2 bytes	2 bytes
Destination Port	2 bytes	2 bytes
Protocol	1 byte	1 byte
TOS	1 byte	1 byte
IIF	20 bits	20 bits
ICMP Type	2 bytes	2 bytes

Interfaces

- **IPv6 Support on ADSL, G.SHDSL, and VDSL2 Interfaces**—This feature is supported on SRX210, SRX220, SRX240, SRX550, and SRX650 devices.

  The DSL encapsulations feature has been enhanced to include IPv6 support. The following DSL encapsulations are supported:

  - ATM physical interface encapsulations
    - atm-pvc
    - ethernet-over-atm
  - ATM logical interface encapsulations
    - atm-snap
    - atm-ppp-vc-mux
    - atm-nlpid
    - atm-cisco-nlpid
    - atm-ppp-llc
    - ether-over-atm-llc

[*DSL Interfaces Feature Guide for Security Devices*]

Logical Systems

- **Support for source NAT interface in logical systems**—This feature is supported on all high-end SRX Series devices for both IPv4 and IPv6 configurations.

  In previous Junos OS releases, all NAT configurations, except for source NAT interface, were supported for logical systems.

  A new option has been added to configure interface NAT port overloading in a root or logical system. To configure the **port-overloading-factor** option, use the **nat source interface** statement in the **[security nat]**hierarchy.

  The value entered for the port overloading factor (a number from 1 through the maximum port capacity) is multiplied by the maximum port capacity to set the port overloading threshold. For example, if the port overloading factor for an SRX3400 device is set to 2, it is multiplied by the maximum port capacity of 63,486, making the port overloading threshold 126972(2*63486).

  The existing **port-overloading** option is not supported for logical systems and should not be used in conjunction with **port-overloading factor**, because the statements can overwrite each other. For example, if **port-overloading** has been set to **off** to disable interface port overloading, and subsequently **port-overloading-factor** is configured with any value greater than 1, the **port-overloading-factor** will override the **port-overloading** setting.

  Use the new **all** option for the **show security nat interface-nat-ports logical-systems** command to display all port usage information for the master and user logical system.

  [*Junos OS Logical Systems Library for Security Devices*]

Mini-PIM Ethernet Switching

- **Ethernet port switching**—This feature is supported on the 1-port Gigabit Ethernet SFP Mini-PIM ports on SRX210, SRX220, SRX240, and SRX550 devices. Switching between the SFP Mini-PIM ports is supported on SRX220, SRX240, and SRX550 devices, and switching between the Mini-PIM and the GPIM is supported on SRX550 devices. This feature is also supported in chassis cluster mode and the Mini-PIM can be configured as a fabric link but it cannot be configured as a switch fabric interface link.

  The following features are supported:

  - L2 Learning, Aging, and VLAN membership
  - STP
  - MSTP
  - RSTP
  - 802.1x
  - IGMP snooping
  - IRB

- LLDP
- MAC limiting

The following features are not supported in Junos OS Release 12.1X45-D10:

- Q-in-Q
- L2 LAG
- LACP
- CFM/LFM
- GVRP

[*Junos OS Layer 2 Bridging and Switching Library for Security Devices*]

Negated Address Support

- **Negated address support** —This feature is supported on all branch SRX Series and J Series devices.

  Users can exclude source, destination, or both addresses from the policy by configuring them as a negated address.

  [*Understanding Negated Address Support*, *Example: Configuring Negated Addresses*]

  [*source-address-excluded*, *destination-address-excluded*]

Network Address Translation (NAT)

- **NAT resource utilization**—This feature is supported on all branch SRX Series devices.

  This feature enables you to improve management of Network Address Translation (NAT) pool addresses and rules.

  - **Source NAT pool usage**—You can view information about source NAT pool resources for all configured source NAT pools or for a specific source NAT pool. In pools without Port Address Translation (PAT), information about IP addresses is displayed; and in pools with PAT, information about ports is displayed.

    Use the **show security nat resource-usage source-pool** command to view resource information, including the number of available resources and the number of used resources in the pool.

  - **Source NAT pool utilization alarm**—This option enables you to define utilization alarm thresholds for a specific NAT source pool. When pool utilization exceeds the upper (raise) threshold or falls below the lower (clear) threshold, an SNMP trap is triggered.

    To configure the **pool-utilization-alarm** option, use the **source pool *pool-name*** statement in the **[edit security nat]** hierarchy.

  - **NAT rule sessions**—You can view real-time information about the number of sessions, both successful and failed, for specific source, destination NAT rules, and static NAT rules.

Use the **show security nat source rule**, **show security destination nat rule**, and **show security static nat rule** commands to view session information.

- **NAT rule session count alarm**—This option enables you to define session count alarm thresholds for a specific NAT source rule. When the session count exceeds the upper (raise) threshold or falls below the lower (clear) threshold, an SNMP trap is triggered.

  To configure the **rule-session-count-alarm** option for source NAT, use the **rule-set** ***rule-set-name*** **rule** ***rule-name*** **then source-nat** statement in the **[edit security nat]** hierarchy.

  To configure the **rule-session-count-alarm** option for destination NAT, use the **rule-set** ***rule-set-name*** **rule** ***rule-name*** **then destination-nat** statement in the **[edit security nat]** hierarchy.

  To configure the **rule-session-count-alarm** option for static NAT, use the **static rule-set** ***rule-set-name*** **rule** ***rule-name*** **then static-nat**statement in the **[edit security nat]** hierarchy.

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

- **Single IP address in a source NAT pool without PAT**—This feature is supported on all branch SRX Series and J Series devices.

  This feature allows you to configure a single IP address in a source NAT pool with no Port Address Translation (PAT), and enables you to use two new options: **address-shared** and **address-pooling** (**paired** or **no-paired**).

  - **Address sharing**—This option enables you to map multiple source IP addresses to one external IP address. Use this option to increase NAT resources and improve traffic when you are configuring a source NAT pool without PAT.

    To configure the **address-shared** option, use the **nat source pool** statement in the **[edit security nat]** hierarchy.

  - **Address pooling**—The **address-pooling-paired** and **address-pooling-no-paired** options enable you to associate one internal IP address with the same external IP address for the duration of a session or not. For applications that require this type of mapping, use the **pooling-paired** option when you are configuring a source NAT pool..

    To configure the **address-pooling** option, use the **nat source pool** statement in the **[edit security nat]** hierarchy.

  The number of hosts that a source NAT pool with out PAT can support is limited to the number of addresses in the pool. When you have a pool with a single IP address, only one host can be supported, and traffic from other hosts is blocked, because there are no resources available.

  If a single IP address is configured for a source NAT pool without PAT when NAT resource assignment is not in active-backup mode in a chassis cluster, traffic through node 1 will be blocked.

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

- **Static NAT rule match for source address and source port**—This feature is supported on all branch SRX Series devices.

  In addition to specifying the destination address as a match condition for a rule, static Network Address Translation (NAT) also supports source address, source address name, and source port match conditions. These new options enable you to target specific traffic for static NAT processing.

  To configure the **source-address**, **source-address-name**, and **source-port** options, use the **static rule-set** *rule-set-name* **rule** *rule-name* **match** statement in the **[edit security nat]** hierarchy.

  Use the **show security nat static rule** command to view source address and source port information.

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

- **Source NAT rule match for source port**—This feature is supported on all branch SRX Series devices.

  In addition to specifying the destination address, the destination address name, the destination port, the source address, the source address name, and the protocol, source Network Address Translation (NAT) also supports source port match conditions. This new option enables you to target specific traffic for source NAT processing.

  To configure the **source-port** option, use the **source rule-set** *rule-set-name* **rule** *rule-name* **match** statement in the **[edit security nat]** hierarchy.

  Use the **show security nat source rule** command to view source port information.

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

Security Policies

- **Security policy firewall authentication now provides user identities for user role firewall provisioning**—This feature is supported on all branch SRX Series devices.

  User identity information, maintained by firewall authentication, can also be mapped to the user's IP address and used for user role firewall enforcement.

  A new UIT, the firewall authentication table, provides firewall authentication data for username and role retrieval. When users authenticate to the firewall, usernames and roles (groups) are mapped to IP addresses and written to the firewall authentication table. The following command enables the firewall authentication table as an authentication source and specifies its priority among other available UITs:

  ```
  set security user-identification authentication-source firewall-authentication priority
    priority
  ```

  The firewall authentication table is propagated when a security policy permits firewall authentication and specifies the new type, **user-firewall**. Users are authenticated based on the access-profile configured for the policy. To trigger firewall authentication for HTTPS traffic, you also need to specify the SSL termination profile. This option is not needed for HTTP traffic.

set security policies from-zone *zone* to-zone *zone* policy *policy-name* then permit firewall-authentication user-firewall access-profile *profile-name* ssl-termination-profile *profile-name*

NOTE: The access profile is configured in the [edit access profile] hierarchy as with other firewall authentication types. The SSL termination profile is configured in the [edit services ssl] hierarchy.

set access profile *profile-name* client *client-name* firewall-user password *pwd*
set services ssl termination profile *ssl-profile-name* server-certificate *certificate-type*

[*Understanding User Role Firewalls*, *Firewall User Authentication Overview*]

System Health Management

- **System Health Management**—This feature is supported on all branch SRX Series devices.

  The system health management feature is enhanced to support preventive and recovery action. This enhancement helps prevent system breakdowns by applying appropriate actions. By default, only preventive actions are taken; user configuration has been added to restrict the system to monitor or allow recovery. Recovery actions include intrusive operations like process restart, file deletion, and so on.

  [*Junos OS Monitoring and Troubleshooting Library for Security Devices*]

Virtual Private Network (VPN)

- **AutoVPN Protocol Independent Multicast (PIM) point-to-multipoint mode**—AutoVPN hubs are supported on SRX240, SRX550, and SRX650 devices. AutoVPN spokes are supported on SRX100, SRX210, SRX220, SRX240, SRX550, and SRX650 devices.

  In hub-and-spoke topologies, multicast data is used for applications such as video streaming or the music-on-hold function for VoIP systems. The multicast sender is typically located behind the hub, although the sender could also be located behind a spoke or a set of spokes. Junos OS Release 12.1X45-D10 supports multicast traffic in an AutoVPN hub-and-spoke network.

  AutoVPN secure tunnel st0 logical interfaces on hub-and-spoke devices are configured for PIM point-to-multipoint mode. This allows devices in the network to replicate multicast data packets to neighbors that join the multicast group. PIM and multipoint must be enabled on multicast sending and receiving interfaces on the devices. To enable PIM on an st0 logical interface, use the **set protocols pim interface st0.*x*** configuration statement. To enable multipoint on an st0 logical interface, use the **multipoint** configuration statement at the [**edit interfaces st0 unit *x***] hierarchy level.

  NOTE: AutoVPN multicast deployments support a maximum of 500 PIM neighbors. The st0 interface that hosts PIM on the hub can support a maximum of 500 spokes.

Configure dynamic routing protocols to support multicast traffic:

- OSPF—Configure the st0 logical interface as an OSPF interface at the [**edit protocols ospf area *area-id* interface**] hierarchy level and specify the **interface-type p2mp** and **dynamic-neighbor** options.
- BGP—On the hub, configure the **local-address** option at the [**edit protocols bgp group bgp-group**] hierarchy level with the address of the st0 logical interface; configure the **neighbor** or the **allow** option to match the st0 addresses on the spokes. On the spoke, configure the **local-address** option at the [**edit protocols bgp group bgp-group**] hierarchy level with the address of the st0 logical interface; configure the **neighbor** option to match the st0 address on the hub. Configure policy statements at the [**edit policy-options**] hierarchy level to limit the number of advertised routes.

NOTE: **The RIP dynamic routing protocol is not supported with AutoVPN for multicast traffic.**

[*AutoVPNs Feature Guide for Security Devices*]

- 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 12.1X45-D10 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 Feature Guide for Security Devices*]

- **Certificate chaining**—This feature is supported on all branch SRX Series devices.

  Certificate-based authentication is an authentication method supported on SRX Series devices during IKE negotiation. In large networks, multiple certificate authorities (CAs) can issue end entity (EE) certificates to their respective end devices. It is common to have separate CAs for individual locations, departments, and organizations.

  With a single-level hierarchy for certificate-based authentication, all EE certificates in the network must be signed by the same CA. All firewall devices must have the same CA certificate enrolled for peer certificate validation. The certificate payload sent during IKE negotiation only contains EE certificates.

  In Junos OS Release 12.1X45-D10, the certificate payload sent during IKE negotiation can contain a chain of EE and CA certificates. A certificate chain is the list of certificates required to certify the subject in the EE certificate. The certificate chain includes the EE certificate, intermediate CA certificates, and the root CA certificate. CA certificates can be enrolled using Simple Certificate Enrollment Process (SCEP) or loaded manually. There is no new CLI configuration statement or command for certificate chains; however, every end device must be configured with a CA profile for each CA in the certificate chain.

The network administrator needs to ensure that all peers participating in IKE negotiation have at least one common trusted CA in their respective certificate chains. The common trusted CA does not have to be the root CA. The number of certificates in the chain, including certificates for EEs and the topmost CA in the chain, cannot exceed 10.

[*Certificates and Public Key Infrastructure Feature Guide for Security Devices*]

- **Suite B cryptographic suites**—This feature is supported on all branch SRX Series devices.

  Suite B is a set of cryptographic algorithms designated by the U.S. National Security Agency to allow commercial products to protect traffic that is classified at secret or top secret levels. Suite B protocols are defined in RFC 6379, *Suite B Cryptographic Suites for IPsec*. The Suite B cryptographic suites supported in Junos OS Release 12.1X45-D10 provide Encapsulating Security Payload (ESP) integrity and confidentiality and should be used when ESP integrity protection and encryption are both required.

  The following Suite B cryptographic suites are supported in Junos OS Release 12.1X45-D10:

  - Suite-B-GCM-128
    - ESP: Advanced Encryption Standard (AES) encryption with 128-bit keys and 16-octet integrity check value (ICV) in Galois/Counter Mode (GCM).
    - IKE: AES encryption with 128-bit keys in cipher block chaining (CBC) mode, integrity using SHA-256 authentication, and key establishment using Diffie-Hellman (DH) group 19 and authentication using Elliptic Curve Digital Signature Algorithm (ECDSA) 256-bit elliptic curve signatures.
  - Suite-B-GCM-256
    - ESP: AES encryption with 256-bit keys and 16-octet ICV in GCM for ESP.
    - IKE: AES encryption with 256-bit keys in CBC mode, integrity using SHA-384 authentication, and key establishment using DH group 20 and authentication using ECDSA 384-bit elliptic curve signatures.

  IKEv1 and IKEv2 configuration are supported.

  NOTE: **Suite B is not supported with the group VPN feature.**

  In Junos OS Release 12.1X45-D10, new and existing options support Suite B compliance in IKE and IPsec proposal configuration:

  - For IKE proposals configured at the [**edit security ike proposal** ***proposal-name***] hierarchy level:
    - **authentication-algorithm** options include **sha-256** and **sha-384**
    - **authentication-method** options include **ecdsa-signatures-256** and **ecdsa-signatures-384**

    - **dh-group** options include **group19** and **group20**

- For IPsec proposals configured at the [**edit security ipsec proposal** ***proposal-name***] hierarchy level, **encryption-algorithm** options include **aes-128-gcm**, **aes-192-gcm**, and **aes-256-gcm**.
- For IPsec policies configured at the [**edit security ipsec policy** ***policy-name***] hierarchy level, the **perfect-forward-secrecy keys** options include **group19** and **group20**.
- For convenience, predefined proposals that provide Suite B compliance—**suiteb-gcm-128** and **suiteb-gcm-256**—are available at the [**edit security ike policy** ***policy-name***] and [**edit security ipsec policy** ***policy-name***] hierarchy levels.

[*IPsec VPNs Feature Guide for Security Devices*]

Related Documentation

- Changes in Behavior and Syntax in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 21
- Known Behavior in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 30
- Known Issues in Junos OS Release 12.1X45-D15 for Branch SRX Series Services Gateways and J Series Services Routers on page 58
- Resolved Issues in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 63
- Documentation Updates for Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 74
- Migration, Upgrade, and Downgrade Instructions for Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 81

Changes in Behavior and Syntax in Junos OS Release 12.1X45 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:

AppSecure

- The following new counters have been added to the **show services application-identification counter** command output:
  - Application Identification Module Statistics

    Sessions that triggered interest callback

    Sessions that triggered create callback

    Sessions that triggered packet process callback

    Sessions that triggered session close callback

    Client-to-server flows ignored

    Server-to-client flows ignored

    Negative cache hits

    Cache inserted

    Cache expired

    Session ignored due to disabled AppId

    Session ignored due to unsupported protocol

    Session ignored due to no active signature set

    Session ignored due to max concurrent session reached
  - Application Identification TCP Reordering Statistics

    Stream constructed

    Stream destructed

    Segment allocated

    Segment freed

    Packet cloned

    Packet freed

    Fast path segment

    Segment case 1

    Segment case 2

    Segment case 3

    Segment case 4

Segment case 5

Segment case 6

- Application Identification Decoder Statistics

  Session state constructed

  Session state destructed

  Packet decoded

  HTTP session state constructed

  HTTP session state destructed

  HTTP packet decoded

- Application Identification Heuristics Statistics

  Unspecified encrypted sessions called

  Encrypted P2P sessions called

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:HTTP];
    }
    then {
      deny;
    }
  }
  default-rule {
    permit;
  }
}
```

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

  - HTTP traffic with or without nested applications would be denied by rule1.
  - HTTP traffic with a nested application, such as junos:FACEBOOK or junos:TWITTER, would be denied by rule1.
  - All other traffic would be permitted by the default rule.

After Junos OS release 11.4R6 and later, the dynamic application junos:HTTP matches only the traffic that does not contains no recognizable nested application. The sample rules would now be applied differently:

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

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.

Deprecated Items for Security Hierarchy

Table 2 on page 24 and Table 3 on page 25 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 2: 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 IDP process 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**

Table 3: Items Deprecated in Release 12.1x45-D10

Deprecated Item	Replacement	Hierarchy Level or Command Syntax	Additional Information
max-packet-mem	**max-packet-memory-ratio**	**security idp sensor-configuration re-assembler**	On all branch SRX Series devices, the **max-packet-mem** command is not supported.
max-packet-memory	**max-packet-memory-ratio** **max-reass-packet-memory-ratio**	**security idp sensor-configuration application-identification**	On all branch SRX Series devices, the **max-packet-memory** 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

- 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 has been 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)

- 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-memory-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-memory-ratio ***percentage-value***

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

  - 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.

- When certain TCP error packets (packets with anomalies) during or after the three-way handshake are forwarded to IDP for processing, IDP TCP reassembly stops the reassembly. Once the reassembly is stopped, IDP does not continue the stream-based attack detection and TCP error packets are not dropped. The **action-on-reassembly-failure** option changes this behavior so that you can configure the action to be initiated when a reassembly failure occurs.
  - Use the following configuration command to drop the error packets when a reassembly failure occurs:

    set security idp sensor-configuration re-assembler action-on-reassembly-failure drop

    Use the following configuration command to drop the session when a reassembly failure occurs:

    set security idp sensor-configuration re-assembler action-on-reassembly-failure drop-session

    If you do not require any action to be taken, then use the following configuration command:

    set security idp sensor-configuration re-assembler action-on-reassembly-failure ignore

    By default, **action-on-reassembly-failure** is set to drop.
  - The **tcp-error-logging** and **no-tcp-error-logging** options enable or disable TCP error logging.

    Use the following commands to enable or disable TCP error logging:

    set security idp sensor-configuration re-assembler tcp-error-logging

    set security idp sensor-configuration re-assembler no-tcp-error-logging

    By default, TCP error logging is disabled.

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 >
  ```

Screen

- The TCP SYN flood counter for a SYN cookie or a SYN proxy attack incorrectly counted every second, thus incrementing the counter every second. This issue has been rectified so that every TCP SYN packet is counted for each SYN cookie or SYN proxy attack. Now every time you receive a SYN packet that is greater than the threshold value, the counter is incremented.

Simple Network Management Protocol (SNMP)

- On all branch SRX Series and J Series devices, the screen SNMP trap **jnxJsScreenCfgChange** will not be sent during reboot.

System Logs

On all branch SRX Series devices, the following system log messages have been updated to include the **certificate ID**:

- 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 12.1X45-D10, an IPsec policy for a VPN can contain proposals with different protocol types (ESP or AH). This means that an IPsec SA can be established with either ESP or AH, depending on the protocol type in the peer's proposal.
- 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)

- For each VPN tunnel, both Encapsulating Security Payload (ESP) and Authentication Header (AH) tunnel sessions are installed on Services Processing Units (SPUs) and the control plane. In previous Junos OS releases, two tunnel sessions of the same protocol (ESP or AH) were installed for each VPN tunnel. For branch SRX Series devices, tunnel sessions are updated with the negotiated protocol after negotiation is completed. For high-end SRX Series devices, tunnel sessions on anchor SPUs are updated with the negotiated protocol while non-anchor SPUs retain ESP and AH tunnel sessions.

  The ESP and AH tunnel sessions are displayed in the outputs for the **show security flow session** and **show security flow cp-session** operational mode commands.

- 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.

- 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.

Related Documentation

- New and Changed Features in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 6
- Known Behavior in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 30
- Known Issues in Junos OS Release 12.1X45-D15 for Branch SRX Series Services Gateways and J Series Services Routers on page 58
- Resolved Issues in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 63
- Documentation Updates for Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 74
- Migration, Upgrade, and Downgrade Instructions for Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 81

Known Behavior in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers

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 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, SRX220, SRX240, and SRX650 devices, you can configure and manage a 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, SRX220, SRX240, SRX550, 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 are not supported in chassis cluster.
  - 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 the 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 the lt-0/0/0 interface, CoS for real-time performance monitoring (RPM) is not supported.
- The factory default configuration for SRX100 and SRX110 devices automatically enables Layer 2 Ethernet switching. Layer 2 Ethernet switching is not supported in chassis cluster mode for SRX100 and SRX110 devices. If you use the factory default configuration, you must delete 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 the 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 J Series devices, the **clear services flow** command is not supported.
- On all J Series devices, RADIUS accounting is not supported.
- On SRX210, SRX220, 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 round 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 the Ethernet switching family.

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-Server and DHCP-Client are not supported in a chassis cluster.
- On all branch SRX Series devices, DHCPv6 client does not support:
  - Temporary addresses
  - Reconfigure messages

- Multiple identity association for nontemporary addresses (IA_NA)
- Multiple prefixes in a single identity association for prefix delegation (IA_PD)
- Multiple prefixes in a single router advertisement

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, 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 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, SRX220, SRX240, SRX550, SRX650 and J Series devices, broadcast TFTP is not supported when flow is enabled on the device.
- On SRX100, SRX110, SRX210, SRX220, SRX240, SRX550 and SRX650 devices, the maximum number of concurrent sessions for SSH, Telnet, Console, and Web is as follows:

Sessions	SRX210	SRX240	SRX650
Console	1	1	-
SSH	3	5	5
Telnet	3	5	5
Web	3	5	5

NOTE: These defaults are provided for performance reasons.

- 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.

Interfaces and Routing

- On all J Series devices, the flow monitoring version 9 has the following limitations:
  - Routing Engine based flow monitoring V5 or V8 mode is mutually exclusive with inline flow monitoring V9.
  - High-end SRX Series devices do not support multiple collectors like branch SRX Series devices. Only one V9 collector per IPv4 or IPv6 is supported.
  - Flow aggregation for V9 export is not supported.
  - Only UDP over IPv4 or IPv6 protocol can be used as the transport protocol.
  - Only the standard IPv4 or IPv6 template is supported for exporting flow monitoring records.
  - User-defined or special templates are not supported for exporting flow monitoring records.
- On all branch SRX Series and J Series devices, flow monitoring IPv6 version 9 has the following limitations:
  - MPLS in not supported.
  - User-defined version 9 templates are not supported.
  - Routing Engine based flow monitoring version 9 is not supported.
  - Flow monitoring and accounting are not supported in chassis cluster mode.
  - Flow monitoring and accounting are not supported on an aggregated Ethernet interface.
  - J-Web for IPv6 sampled packets is not supported.
  - SNMP queries for IPv6 sampled packets are not supported
  - Flow monitoring can be configured in version 5, version 8, or version 9 export mode. Up to eight version 9 collectors are supported in export mode.
  - Scope of accounting of IPv6 flow monitoring version 9 packets associated with pseudointerfaces (such as IRB, ML, LAG, VLAN, and GRE) is not supported.
  - Creation of a Stream Control Transmission Protocol (SCTP) session (parallel to TCP) between an exporter and a collector for gathering flow monitoring information is not supported.
  - Maximum flow sessions that might be supported include:
    - A device with 1-GB RAM, support up to 15,000 flow monitoring sessions at a time.

    - A device with 2-GB RAM, support up to 59,900 flow monitoring sessions at a time.
    - Changes in source autonomous system (AS) and destination AS are not immediately reflected in exported flows.

- 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.
- The ATM interface takes more than 5 minutes to come 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 the 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 the following 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, the 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 an 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, SRX110, SRX210, SRX220, SRX240, SRX550, and SRX650 devices, on 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 the Ethernet switching family.
- 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
  - 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)

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 Release 11.2 or later, a migration of IDP security package files needs to be performed. This is done automatically on upgrade when the IDP process comes up. Similarly, when the image is downgraded, a migration (secDb install) is automatically performed when the IDP process 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 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 fail over or fail back.
  - 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.

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:
    - Language support—English-version browsers
    - Supported OS—Microsoft Windows XP Service Pack 3
    - Supported browsers

Device	Application	Supported Browsers	Recommended Browser
SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, SRX650	J-Web	• Mozilla Firefox version 3.x • · Microsoft Internet Explorer version 7.0 NOTE: The New Setup wizard and the PPPoE wizard works best with Mozilla Firefox version 15.x or later.	Mozilla Firefox version 3.x

  - 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 all branch SRX Series 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 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 while underlying Web management interface changes, you do not receive a response about the commit status.
- Images, buttons, and spinner (indicating that the configuration is being applied) on the wizard screen do not initially appear when the browser cache is cleared.

Layer 2 Transparent Mode

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

Network Address Translation (NAT)

- **Single IP address in a source NAT pool without PAT**—The number of hosts that a source NAT pool without PAT can support is limited to the number of addresses in the pool. When you have a pool with a single IP address, only one host can be supported, and traffic from other hosts is blocked because there are no resources available.

  If a single IP address is configured for a source NAT pool without PAT when NAT resource assignment is not in active-backup mode in a chassis cluster, traffic through node 1 will be blocked.

- For all ALG traffic, except FTP, we recommend that you not use the static NAT rule options **source-address** or **source-port**. Data session creation can fail if these options are used, because the IP address and the source port value, which is a random value, might not match the static NAT rule. For the same reason, we also recommend that you not use the source NAT rule option **source-port** for ALG traffic.

  For FTP ALG traffic, the **source-address** option can be used because an IP address can be provided to match the source address of a static NAT rule.

  Additionally, because static NAT rules do not support overlapping addresses and ports, they should not be used to map one external IP address to multiple internal IP addresses for ALG traffic. For example, if different sites want to access two different FTP servers, the internal FTP servers should be mapped to two different external IP addresses.

- 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 (high memory devices)	1024	1024	64M	1024
SRX650 (low memory devices)	256	256	16M	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 (63,488 through 65,535), 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 (63,488 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 4 on page 43. The limitation on the number of destination-rule-set and static-rule-set has been increased.

  Table 4 on page 43 provides the requirements per device to increase the configuration limitation as well as to scale the capacity for each device.

Table 4: 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
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

- On all branch SRX Series and J Series devices, you cannot configure the following IP addresses as negated addresses in a policy:
  - Wildcard addresses
  - IPv6 addresses

  - Addresses such as any, any-ipv4, any-ipv6, and 0.0.0.0

- When a range of addresses or a single address is negated, it can be divided into multiple addresses. These negated addresses are shown as a prefix or a length that requires more memory for storage on a Packet Forwarding Engine.
- Each platform has a limited number of policies with negated addresses. A policy can contain 10 source or destination addresses. The capacity of the policy depends on the maximum number of policies that the platform supports.
- 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**.

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, SRX550, and SRX650 devices, the following features are not supported for Layer 2 transparent mode:
  - Gratuitous-ARP (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, SRX220, SRX240, SRX550, and SRX650 devices, change of authorization is not supported with 802.1x.
- On SRX100, SRX210, SRX220, SRX240, SRX550, 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)

- 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 and Changed Features in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 6
- Changes in Behavior and Syntax in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 21
- Known Issues in Junos OS Release 12.1X45-D15 for Branch SRX Series Services Gateways and J Series Services Routers on page 58
- Resolved Issues in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 63
- Documentation Updates for Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 74

- Migration, Upgrade, and Downgrade Instructions for Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 81

Known Issues in Junos OS Release 12.1X45-D15 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.

NOTE: 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.

Application Layer Gateways (ALG)

- When an RTSP TCP segment cannot be processed because it is too small or incomplete, the RTSP ALG holds it and waits for the next segment. An RTSP endpoint does not receive an ACK for segments that are too small, so it retransmits the segment several times. Eventually, the RTSP endpoint resets the TCP connection. [PR887601]
- The SUN RPC ALG might not work properly when the SUN RPC server replies with a get-address packet to the client. This might wrongly truncate the server's address, which causes the SUN RPC connection to fail. [PR901205]

Chassis Cluster

- When Layer 2 bridging is configured, both the nodes must be rebooted. After you reboot the primary node, the secondary node goes into a disabled state because of a fabric link failure. As a workaround, reboot both the nodes (including the one running as primary). Rebooting only the disabled node does not resolve the issue. [PR892374]

Dynamic Host Configuration Protocol (DHCP)

- Prior to Junos OS Release 11.4R9, DHCP option 125 cannot be configured for use as the **byte-stream** option. With Junos OS Release 11.4R9 and later releases, DHCP option 125 can be used for the **byte-stream** option. [PR895055]

Flow and Processing

- When reverse path forwarding (RPF) is enabled along with real-time performance monitoring (RPM), the device changes to the db prompt and loses the reach ability when you delete some configurations. [PR869528]
- On devices with 1 GB of memory, if the advanced services license is configured with the **reduce-dp-memory** option, memory is not released from the data plane to the control plane. As a workaround, when the advanced services license is configured, do not configure the **reduce-dp-memory** option. [PR895648]

Interfaces and Routing

- The counter for incoming traffic on a fabric interface (used for chassis cluster) always shows zero (0). [PR520962]
- On SRX210 High Memory devices, the state of the cl-0/0/8 interface reflects only the output packets sent but does not show the input packets received over the Dialer interface (dl0). [PR662813]
- On SRX550 devices, the Virtual Router Redundancy Protocol (VRRP) does not work when it is connected through integrated routing and bridging (IRB). [PR834766]
- When there is high CPU utilization, Link Aggregation Control Protocol (LACP) might flap and consequently the aggregated Ethernet (ae) interface link might sometimes go down. [PR860129]

Intrusion Detection and Prevention (IDP)

- When you disable idp policy-optimizer by using the **set security idp sensor-configuration no-policy-optimizer** command, the policy fails to load after reboot. [PR883258]

J-Web

- On devices in a chassis cluster, the LACP cannot be configured on redundant Ethernet (reth) interfaces using J-Web. [PR590387]
- In J-Web, drag and drop reverse functionality is not available for UTM pages. As a workaround, use the arrow tabs provided. [PR613238]
- On SRX100, SRX210, SRX240, and SRX650 devices, you cannot access the Help page for Monitor>Wireless LAN. As a workaround, navigate to Monitor>Interfaces and select Help>HelpContents. On the Help Page, click the WLAN link in the list of items under Monitor Node. [PR691915]
- When wireless LAN access point is configured through Configure>WirelessLAN>Settings, and an existing name is provided for the new access point, no error occurs, but the existing access point's configuration is overwritten. [PR691924]
- On SRX100, SRX210, SRX240, and SRX650 devices, the country code configured for an AX411 Wireless LAN access point connected to the device through Configure >Wireless LAN >Settings does not reflect properly on Monitor >Wireless LAN. [PR692740]
- In J-Web, the PPPoE wizard is not supported on Microsoft Internet Explorer version 9.0. As a workaround, use Microsoft Internet Explorer version 7 or version 8, or use Mozilla Firefox version 3 and later, up to version 6.0. [PR694026]
- The J-Web interface and the New Setup wizard do not work properly when PHP request is not served by MGD. [PR797542]
- In J-Web, you might not be able to commit configurations after launching and closing the PPPoE wizard. After you launch the PPPoE wizard and close, the commit preference changes from Validate configuration changes to Validate and commit configuration

changes. If you do some configuration from other screens in J-Web, the configuration might be pushed into the CLI but is not committed and the J-Web interface might not show any pending commit. As a workaround, after launching and closing the PPPoE wizard, change the commit preference manually and then configure through J-Web. You can also commit the configurations through the CLI. [PR804273]

- In J-Web, the Edit Existing Configuration option of the New Setup wizard works only when the configuration is delivered using the wizard. As a workaround, use the Create New Configuration option, which overwrites the existing configuration with a wizard configuration. [PR806035]
- The Layer 2 Transparent Mode feature does not work with the groups configuration. [PR815225]

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]
- On devices in a chassis cluster, the chassis cluster rule number of sessions in the SNMP query or walk result is the sum of the real number of sessions of the primary node and the secondary node. [PR908206]

Network Management and Monitoring

- The SNMP query or walk on ipNetToMediaPhysAddress does not match the **show arp** command output. [PR850051]

Platform and Infrastructure

- There is a mismatch between the version displayed in the **show configuration** and **show version** commands. [PR790714]
- When forwarding restarts on the primary node or when the primary node is rebooted, occasionally, the Flexible PIC Concentrator (FPC) on that node might not come online. Multiple reboots of the node are required to bring the FPC online. [PR868792]
- J-Flow is not working as expected. The cflowd packets are not seen for V5 and V8 sampled flows. [PR916986]

Screen

- On SRX Series devices with teardrop Screen enabled, the teardrop attack traffic is not intermittently detected, and it is forwarded out of the device. [PR906811]

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 the 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)

- When full file-based scanning of antivirus is enabled with Kaspersky scanning, some websites are not accessible. [PR853516]
- Webpages become unavailable and do not display any content when you enable Sophos antivirus for HTTP traffic. As a workaround, use Kaspersky or Express antivirus instead of Sophos antivirus when both antivirus and content filtering are required for HTTP traffic. [PR906534]

Virtual Private Network (VPN)

- If the VPN external interface configuration changes from static IP address assignment to DHCP-based dynamic address assignment, along with any VPN configuration change in the same commit, the IPsec Key management process (daemon) might restart. As a workaround, change the external interface configuration (from static IP to DHCP based) and perform the VPN configuration change in two different commits. [PR837943]
- When a device is configured to support remote access VPN clients with a local address pool, memory usage of the general authentication service process (authd) increases slowly over time. As a workaround, execute the **restart general-authentication-service** command to prevent the memory usage from reaching a critical level. [PR894232]
- For IKEv2, when an SRX Series device running Junos OS Release 12.1X45-D15 is in negotiation with a peer SRX Series device running Junos OS Release 11.4 or 12.1X44-D10, a kmd core file is generated on the peer device during IPsec child SA rekey. However,

this does not impact any IKEv1 scenarios. As a workaround, upgrade the peer SRX Series device to either Junos OS Release 12.1X44-D25 or later or Junos OS Release 11.4R10 or later. [PR915376]

Related Documentation

- New and Changed Features in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 6
- Changes in Behavior and Syntax in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 21
- Known Behavior in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 30
- Resolved Issues in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 63
- Documentation Updates for Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 74
- Migration, Upgrade, and Downgrade Instructions for Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 81

Resolved Issues in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers

The following are the issues that have been resolved in Junos OS Release 12.1X45 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.

NOTE: 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.

Resolved Issues in Junos OS Release 12.1X45-D15 for Branch SRX Series Services Gateways

Application Layer Gateways (ALG)

- In certain circumstances, if the OPTIONS method is used to create a call, and the INVITE method is used to reuse the call, the SIP ALG would apply an incorrect state. As a result, the device might drop the ACK of 200-OK. [PR898956]
- On devices enabled with the MSRPC ALG, the flowd process might crash frequently when heavy MSRPC traffic is processed by the MSRPC ALG. [PR907288]

Flow and Processing

- When DNS ALG was enabled, the rewrite rules applied on the egress interface might not work for DNS messages. [PR785099]
- After enabling IPv6 in flow mode, IPv6 routes are not active. [PR824563]
- Periodic multicast packets such as NTP do not refresh the route, and packets are dropped intermittently. [PR869291]
- On SRX Series devices, during ARP floods of the data plane Packet Forwarding Engine, the CPU spikes might impact transit and host-bound traffic. [PR871704]
- On devices in a chassis cluster, after data plane RG1 failover, the RTSP data packet is queued, and a duplicate RTSP data packet is processed by the device; the flowd process crashes and generates core files. [PR883397]
- On J Series devices, the self-originating outbound traffic always uses the first logical unit queue. [PR887283]
- When flow trace options are enabled, all the traffic that flows between logical systems through the logical-tunnel (lt-0/0/0) generates unexpected messages and floods the flow trace. These messages cannot be filtered and are difficult to read and use. [PR891689]

Interfaces and Routing

- On devices in a chassis cluster, when you execute the **clear system commit** command, it clears commit only from the local node. [PR821957]
- When a symmetric high-speed DSL (SHDSL) Mini-PIM is configured in 2-wire mode with annex mode as Annex B/G, one of the physical interfaces does not come up. [PR882035]
- On devices in a chassis cluster, when a session created as the incoming interface is a VPN secure tunnel interface (ST interface) and the outgoing interface is a logical tunnel interface (LT interface), this session is incorrectly marked as active on the secondary node. When this session expires on the secondary node, the sessions on both cluster nodes might get deleted and interrupt the traffic. [PR896299]
- When there is a configuration change in the VDSL profile from one to another, the VDSL line does not retrain and come up with the with the newly configured VDSL profile. [PR898775]

Intrusion Detection and Prevention (IDP)

- On SRX Series devices with IDP enabled, if IDP exempt rule is configured, a change of the IDP rule configuration (such as a change to source or destination, action, or signature) might cause the flowd process to crash and core files are generated. [PR877865]
- When there are a large number of ASC entries (100,000 or more), and the entries are listed using CLI command, the flowd process might crash. [PR886173]

J-Web

- The ASN.1 buffered I/O functions in OpenSSL before 0.9.8v do not properly interpret integer data, which allows remote attackers to conduct buffer overflow attacks and causes a denial of service (memory corruption). J-Web is explicitly not affected by this vulnerability, because J-Web is a server and this is a client-side vulnerability. However, many other functions in Junos OS use these buffered I/O routines and can trigger fetches of untrusted X.509 certificates. Refer to PSN-2012-07-645 for more information. [PR770702]
- J-Web fails to display the member in the application set after adding it to the nested application set. [PR883391]
- In J-Web, the configured 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]

Network Address Translation (NAT)

- In a root system, the destination and static NAT rule cannot send system log and trap messages when the number of sessions reaches the threshold value. In a logical-system, the source, destination, and static NAT rule cannot send system log and trap messages when the number of sessions reaches the threshold value. [PR905359]

Network Management and Monitoring

- Under certain conditions, a duplicate SNMP index might be assigned to different interfaces by the kernel to the mib2d (Management Information Base II daemon). This might cause mib2d and other processes such as lacpd (LACP daemon) to crash and generate core files. [PR836823]

Platform and Infrastructure

- There is no specific CLI command to display the count of sessions allowed, denied, or terminated because of UAC enforcement. [PR733995]
- Event scripts, part of Junos OS automation infrastructure, run at high priority compared to other system-critical processes. This can result in resource contention and high CPU readings. [PR512315]
- When you enable **Change password every time the user logs out** on the active directory, you cannot change your password. [PR740869]
- On SRX240 devices, when a nonstandard HTTPS port is set, the Uniform Resource Identifier (URI) changes to the IP address and port. [PR851741]

Security Group

- Multiple vulnerabilities are reported in earlier versions of OpenSSL in Junos OS. [PR853724]

Unified Threat Management (UTM)

- The flowd process might crash when traffic is processed by Unified Thread Management (UTM). [PR854880]

Virtual Private Network (VPN)

- On all branch SRX Series devices, the Junos Pulse client is updated from Release 2.0R3 to 4.0R2. [PR868101]
- File Descriptor (FD) leak occurs during the network-security-trace process when commit configuration changes are made in the **edit security ike** configuration. Eventually, the system reaches the maximum file limit, which results in a system-unmanageable condition. [PR893017]

Resolved Issues in Junos OS Release 12.1X45-D10 for Branch SRX Series Services Gateways

Application Layer Gateway (ALG)

- On devices with Media Gateway Control Protocol (MGCP) ALG enabled, flowd core files were generated. [PR684653]
- The Microsoft remote procedure call (MSRPC) ALG feature did not include support for NDR64 parsing and DCOM interface, which is used by applications such as WMIC, IIS, and so on. [PR700049]
- The TCP proxy module used by the ALG was deficient in handling a TCP stream with large packets. [PR727649]
- The total SIP call values were incorrect, and the ALG feature could not be verified. [PR839190]
- The Session Initiation Protocol (SIP) ALG implementation used within the SRX Series in Junos OS Release 11.2 and later releases had a firewall bypass vulnerability, which allowed sessions to be created for connections (SIP calls) that should not have been allowed by the policy. An untrusted remote user caused a denial of service by exhausting session resources. [PR821623]

Authentication

- When devices were configured to use RADIUS authentication, if the user-permission string sent from the RADIUS server was longer than 129 characters, the device failed to process the user-permission string. This resulted in user permissions being set incorrectly. [PR736331]
- On all branch SRX Series devices configured with firewall authentication, if a user was already authenticated, and then when a subsequent user initiated authentication using the same IP address as the first user, the subsequent user inherited the first authenticated user's "Access time remaining" value. [PR843591]

Chassis Cluster

- During an IP monitoring failover condition, the IP monitoring policy status changed to INIT from FAIL and the interface and route actions were reset to MARKED-DOWN and NOT-APPLIED. [PR729022]
- After reboot of both chassis cluster nodes and RG1 failover, one redundant Ethernet member was held in the Spanning Tree Protocol (STP) Learn state, and when the cable was unplugged multiple times, the link went down and did not recover. [PR811002]
- On devices in a chassis cluster, the child link of the link aggregation group (LAG) redundant Ethernet (reth) interface flapped frequently, which corrupted the memory on the next-hop pointer and the Routing Engine generated vmcore files. [PR821833]
- On devices in a chassis cluster, when Layer 2 Ethernet switching was configured and the created session was related to the Layer 3 VLAN interface (the session's ingress or egress interface), the session was deleted on the primary node when the backup session timed out on the backup node.[PR839290]

- On devices in a chassis cluster, during cold synchronization, if the flow sessions were synchronized before the application identification configuration synchronization, then after the backup node was rebooted, the application identification module bypassed the flow sessions and the application names for those sessions were marked as unknown. [PR843742]
- The primary node changed to db mode and generated vmcore files when there was a change in the redundant Ethernet (reth) interface configuration that caused the deletion of the logical interface of reth. [PR850897]
- On all branch SRX Series devices, when you used aggregated redundant Ethernet (chassis cluster redundant Ethernet interface with multiple link members per node), traffic loss was observed when the link member failed. [PR858519]
- On SRX210, SRX220, and SRX240 devices, the maximum transmission unit (MTU) value on the SRX-MP-1SFP-GE Mini-PIM interface is 9010, if the Mini-PIM interface was configured as a chassis cluster fabric interface, the chassis cluster fabric interface automatically sets the MTU value to 9014 to support jumbo frames. Setting the MTU value fails on the Mini-PIM interface configured as a chassis cluster fabric interface, and the Mini-PIM interface retained the default MTU setting (1514). The packets that were larger than the 1514-byte frame were dropped because the chassis cluster fabric interface did not support fragmentation.

  NOTE: Prior to Junos OS release 11.4R1, the SFP interfaces on Mini-PIMs are not supported to use as the fabric link in a chassis cluster.

  [PR865975]

Command-Line Interface (CLI)

- 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]
- On SRX210 devices, you could not configure **0.0.0.0/0** in **dialer-options watch-list**. The **set interfaces dl0 unit 0 dialer-options watch-list 0.0.0.0/0** command failed. [PR841371]

Flow and Processing

- On J2350 devices, the CPU utilization increased sharply with 3000 connections per second because rtlogd and eventd daemons consumed high CPU resources. [PR586224]
- On all branch SRX Series devices, when multicast traffic was received, changes in policer, filter, or sampling configuration resulted in the generation of core files. [PR613782]
- Special crafted kernel routes that were generated based on directly connected networks (clone routes) introduced reference count inconsistencies when the link flapped, if the clone routes were rewired to a different interface. This occurred because the longest prefix match found another destination for the IP address of the flapped interface.

When the parent reference count was reduced to zero, the kernel crashed when deleting the remaining child routes. [PR685941]

- Occasionally, flowd core files were generated when the wrong packets were processed. [PR730921]
- When you configured the **nas-ip-address** option using the command **system radius-options attributes nas-ip-address** and committed, the **nas-ip-address** was not correctly set unless you rebooted the device. [PR786467]
- Destination port information was missing for IPv6 packets when the firewall was in packet mode. [PR805986]
- When a device forwarded traffic, flowd core files were generated. [PR831480]
- On devices with increased ALG or proxy traffic, memory leaks in global data plane memory were observed, and traffic (FTP, MSRPC, AppID, and so on) was dropped. [PR859956]
- If Virtual Router Redundancy Protocol (VRRP) was configured with the preempt option on an aggregated Ethernet link aggregation group (LAG) interface, the device did not send Gateway-Address Resolution Protocol (G-ARP). [PR863549]
- When an active route changed from multiple-next-hop to single-next-hop, one of the internal structures was incorrectly updated. This resulted in route lookup failure and caused traffic drops even though the new active route was correctly displayed in both the routing and forwarding tables. [PR879726]

Infrastructure

- When the **commit | display xml** command was used, if a commit error occurred because of a missing configured event script file, the returned XML code had an incorrect closing tag. [PR694658]

Interfaces and Routing

- On J Series devices, E1 LCP links could not be recovered after BERT tests. [PR600846]
- On receipt of a BGP UPDATE message that contained a crafted flow specification, NLRI caused the RPD to crash. The update created an invalid inetflow prefix, which caused the RPD process to allocate memory until it reached its assigned memory limit. After trying to exceed the process memory limit, RPD crashed and restarted.The system recovered after the crash; however, a constant stream of malformed updates caused an extended outage. [PR734453]
- When you committed a configuration change, the routing protocol process (rpd) was reinitialized. When multiple reinitializations occurred while OSPF was running on the router, the periodic refresh of the OSPF LSAs stopped. If the LSAs were not refreshed, the router did not participate in the OSPF routing domain. The output of the **show ospf database router advertising-router router-id extensive | match timer** command did not include the Gen timer field. [PR744280]
- When a TAR file was created, a user with super user class privileges could not access the core TAR file. [PR772809]

- Configuring multicast addresses (inet6) on an interface resulted in the generation of RPD core (mc_ssm_add) files. [PR780751]
- By default, the Physical Interface Module (PIM) interface is in the self zone. When the PIM interface was UP, it triggered the tunnel session creation function. However, when a device was running in packet mode, there were no session-related resources reserved or allocated in the packet mode (packet mode does not create sessions). The tunnel session creation failed and then looped. In this case, the logs did not indicate any impact on the production traffic. [PR792271]
- 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 through the equal-cost multipath (ECMP) to the aggregate interface was dropped. [PR809383]
- When the Flexible PIC Concentrator (FPC) was removed or made to go offline, the FPC status was not getting detected. [PR818363]
- Crafted Generic Routing Encapsulation (GRE) packets received on a multicast tunnel (mt- or gr-) interface that were allowed to reach the Routing Engine caused the Junos OS kernel to crash. [PR821503]
- On a very-high-bit-rate digital subscriber line (VDSL) Mini-PIM or integrated module, when the VDSL profile was selected as Auto and the address acquisition method was selected as DHCP in the pt mode, the physical interface link flapped. [PR827144]
- When you attempted to create a dial backup interface, * and # symbols were not accepted. [PR834042]
- High-priority Routing Protocol Daemon (RPD) tasks were scheduled more frequently, halting the progress of low-priority RPD tasks. Low-priority tasks could not be completed until all the scheduled high-priority tasks were completed. [PR836197]
- When the signal to noise ratio on the DSL line was low, the DSL line dropped and retrained. The DSL interface stopped transmission after multiple line drop events. [PR837557]
- The Junos OS kernel crashed when a specifically crafted TCP packet was received by the Routing Engine on a listening TCP port. TCP traffic traversing the router did not trigger this crash. The TCP packets destined to the router that successfully reached the Routing Engine through existing edge and control plane filtering, caused the crash. This issue could be triggered by both IPv4 and IPv6 TCP packets destined to the Routing Engine. [PR839412]
- 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 the SRX-GP-24GE PIM were disabled, the laser remained turned on. This caused the link on the peer side to remain up and resulted 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)

- If you configured only custom attacks without installing the IDP security package, the default detector was used. If the default detector version contained the date 110307, the detector was not compatible with the engine and resulted in the generation of flowd core files. [PR795400]
- You could not configure the memory limit using the configuration statement **security sensor-configuration global memory-limit-percent** because an invalid range was expected. [PR830467]
- Signatures with negate attacks did not work as expected with hardware DFA based pattern matching and led to many false positives. [PR848659]
- IDP signature database update was not synchronized between node 0 and node 1. [PR859196]

IPv6

- Certain IPv6 packets matching an IPv6 egress filter with a discard or reject term applied on the lo0 interface triggered a buffer leak, which caused MBUF exhaustion and a kernel crash. The rate of the leak was proportional to the number of these specific IPv6 packets hitting the discard term, reject term, or both. This issue only affected IPv6 egress filters with a discard or reject action. [PR816666]
- Rewriting DSCP bits for IPv6 Neighbor advertisements was not supported. [PR827740]

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]
- On devices 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]
- In J-Web, an insufficient validation vulnerability allowed an authenticated user to execute arbitrary commands. This allowed a user with low privilege (such as read-only access) complete administrative access. The scope of this vulnerability was limited to only those users with valid, authenticated login credentials. [PR826518]
- In J-Web, after you upgraded a device to Junos OS Release 11.4 R4 or later, downloading configuration files using Internet Explorer failed. [PR830482]
- In J-Web, the session expired when the idle-timeout value was set too low. [PR830644]
- 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]
- In J-Web, custom defined applications were presented as “pre-defined”. [PR837820]
- In J-Web, the value of POLO was not visible when you configured security zones using the CLI or J-Web. [PR839749]
- In J-Web, when you edited a PPPoE connection that was loaded from the load and save client file option using Internet Explorer, the following error message was displayed:

unknown runtime error pppoeFunctions.js

[PR844282]

- In J-Web, if the policy name was "0", the penultimate-hop popping (PHP) function treated it as empty, and traffic log output could not be viewed. [PR853093]
- In J-Web, you could not specify the global address book object when configuring a security policy in an untrust zone. [PR853325]
- In J-Web, when you selected Configure > Security > Policy> Apply Policy section, after applying the From and To Zone filter, the configured zones were not listed. [PR854285]
- The New Setup wizard failed to commit the configuration if the Password Authentication Protocol (PAP) or the Challenge Handshake Authentication Protocol (CHAP) password was missing, and if the PPPoE account contained the character “@” in the account name. [PR856746]
- In J-Web, on devices in a chassis cluster, the "switch to L2 mode" button was not functional. [PR857147]
- In J-Web, if dynamic VPN was configured, when you logged out, the following error message was displayed:

  404 page not found error

  [PR857419]
- On devices in a chassis cluster, the security zone was not populated properly on the J-Web interface port configuration page. [PR859200]
- In J-Web, information on routes was not listed under the Configure > Routing > Static Routing section. [PR864324]
- In J-Web, when 200 or more users were listed under Access Profile, all the users were not displayed. [PR872103]

Logical Systems

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

Network Address Translation (NAT)

- On all branch SRX Series devices, 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]
- On devices enabled with static NAT and configured with multiple routing instances, reverse static NAT did not work when both the ingress interface and egress interface were in the root routing instance. [PR834145]

SNMP

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

Switching

- On SRX650 devices, the dot1x:mode:Multiple:Supplicants were authenticated even after a disconnect message was sent from the RADIUS server. [PR786731]
- The Internet Group Management Protocol (IGMP) leave messages received on a port of an 8-Port Gigabit Ethernet small form-factor pluggable (SFP) XPIM that was configured with family Ethernet switching, were not processed by the IGMP Snooping module. [PR824557]

System Logs

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

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

  [PR747002]

- New system log messages were added for the following PKI Daemon failures:
  - Missing basic constraints in a CA certificate
  - Invalid CA=TRUE flag in CA certificate

  [PR831995.]

Unified Access Control (UAC)

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

Unified Threat Management (UTM)

- On SRX210 and SRX240 devices, performance drop of the Kaspersky antivirus solution was observed during testing. [PR704838.]
- When antivirus was enabled on a system, Web search using search engines such as yahoo.co.jp failed, if the content size limit was set to 20. [PR722652]
- When antivirus was enabled, an FTP connection failed, if the name of the folder contained the term “quit”. [PR739635.]
- When there were huge number of pending UTM enhanced Web filtering requests, the CPU utilization was high on the utmd process. [PR841047.]
- A security policy configured with antivirus showed incorrect count of bytes and packets in the policy statistics. [PR841923.]

- On all branch SRX Series devices with UTM antivirus enabled, flowd core files were generated if files exceeding 1 GB were transferred using FTP. [PR846655]
- On devices in a chassis cluster, the antivirus database was not synchronized on both the cluster nodes. [PR863181]
- On all branch SRX Series devices, new categories for Enhanced Web filtering were added. [PR866160]
- The **sessions-per-client** option, which imposes a session throttle to prevent a malicious user from generating large amounts of traffic simultaneously, was supported only with antispam, content filtering, and antivirus UTM features, but was not supported with the Web filtering feature. [PR872385]

Upgrade and Downgrade

- When you upgraded a 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 was not accepted. [PR806750]
- On SRX550 devices, the **request system firmware upgrade re bios** command to upgrade the BIOS was missing. [PR809921]
- On all branch SRX Series devices, if the NVRAM was corrupted, upgrade still continued and you were prompted to reboot the device. However, the affected device booted up with the earlier software version, which in a cluster led to both devices running different software releases. This led to traffic loss. [PR843888]

Virtual Private Networks (VPNs)

- Occasionally, devices configured with policy-based IPsec VPN did not allow traffic to the protected resources. [PR718057]
- The Key Manager Daemon (kmd) process crashed and generated core files. This caused disruptions in the IPsec VPN traffic and made the IPsec VPN tunnel unstable. [PR725765]
- 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]
- IKE SA failed to install the responder during Phase 2 rekey. [PR809219]

Related Documentation

- New and Changed Features in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 6
- Changes in Behavior and Syntax in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 21
- Known Behavior in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 30
- Known Issues in Junos OS Release 12.1X45-D15 for Branch SRX Series Services Gateways and J Series Services Routers on page 58

- Documentation Updates for Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 74
- Migration, Upgrade, and Downgrade Instructions for Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 81

Documentation Updates for Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers

This section lists the errata and changes in Junos OS Release 12.1X45 documentation.

Documentation Updates for the Junos OS Software Documentation

This section lists improvements and outstanding issues with the software documentation.

Security Policy Applications Feature Guide for Security Devices

- On the Overview tab, under IP-Related Predefined Policy Applications, in the topic entitled "Understanding IP-Related Predefined Policy Applications," the Port column for both TCP-ANY and UDP-ANY should indicate 0-65535. The lead-in sentence should read, "Each entry includes the port and a description of the application." TCP-ANY means any application that is using TCP, so there is no default port for it. The same is true for UDP-ANY.
- In the topic entitled "Understanding Miscellaneous Predefined Policy Applications," table "Predefined Miscellaneous Applications" is incomplete. Under the RADIUS row, add a new row:

Table 5: Predefined Miscellaneous Applications

Application	Port	Description
RADIUS Accounting	1813	Enables the collecting of statistical data about users logging in to or out from a LAN and sending the data to a RADIUS Accounting server.

In table "Predefined Miscellaneous Applications" replace the IPsec-NAT row with the following:

Table 6: Predefined Miscellaneous Applications

Application	Port	Description
IKE	500	Internet Key Exchange is the protocol that sets up a security association in the IPsec protocol suite.

Table 6: Predefined Miscellaneous Applications *(continued)*

Application	Port	Description
IKE-NAT	4500	Helps to perform Layer 3 NAT for S2C IKE traffic.

Application	Port	Description
VoIP	389	Internet Locator Service (ILS)
	522	User Location Service (ULS)
	1503	T.120 Data sharing
	1719	H.225 RAS message
	1720	Q.931 Call Setup
	1731	Audio Call Control
	5060	SIP protocol

Certificates and Public Key Infrastructure Feature Guide for Security Devices

- In "Example: Using SCEP to Automatically Renew a Local Certificate," the overview states that you can configure when the device is to send out the certificate renewal request as the number of days and minutes before the certificate's expiration date. This is incorrect. The trigger for the device to send out a certificate renewal request is a specified percentage of the certificate's lifetime that remains before the certificate expires. For example, if the renewal request is to be sent when the certificate's remaining lifetime is 10%, then configure 10 for the reenrollment trigger.

Junos OS UTM Library for Security Devices

- The "Understanding UTM Support for Active/Active Chassis Cluster" topic incorrectly indicates that Sophos antivirus scanning is not supported as part of the active/active chassis cluster implementation. The correct information is: Sophos antivirus scanning is supported in the active/active chassis cluster implementation as of Junos OS Release 12.1.
- Multiple topics in the UTM task-based, tabbed webpages are missing information about SRX550 support in the "Supported Platforms" list. All UTM features are supported on the SRX550 as of Junos OS Release 12.1.

Security Zones and Interfaces Feature Guide for Security Devices

- The section "Configuring the Device as a DNS Proxy" incorrectly states that when you set a default domain name, and specify global name servers, that an interface option needs to be configured on the forwarders. The step should be as follows:

Set a default domain name, and specify global name servers according to their IP addresses.

```
[edit system services]
user@host# set dns dns-proxy default-domain * forwarders 172.17.28.100
```

Junos OS for SRX Series Documentation

The Junos OS for SRX Series technical documentation set has been expanded, restructured, and retitled in this release to make it more comprehensive, easy-to-use, and intuitive. Highlights:

- (New) The Complete Software Guide consolidates all of the release-specific content that applies to Junos OS for SRX Series devices (except release notes) into a three volume set of PDFs that you can download and view offline. The first volume contains getting started and administration information; the second contains feature information; the third contains developer information. You can find the PDFs in the Downloads box on the right side of the *Junos OS for SRX Series Services Gateways, Release 12.1X45* index page.
- (New) The *Getting Started Guide for Branch SRX Series* describes how to get up and running with branch SRX Series devices.
- (Expanded) The *Junos OS Monitoring and Troubleshooting Library for Security Devices* contains significantly more content to help network and security managers keep their SRX Series devices running smoothly in their production environments.
- (Expanded) The *Junos OS for SRX Series Services Gateways, Release 12.1X45* index page has been expanded to serve as a "one stop shop" for all of your Junos OS for SRX Series technical documentation needs.

For more information about technical documentation improvements in this release, see Getting the Content You Need. To see a detailed mapping of how 12.1X44 Junos OS for SRX Series content maps to the new 12.1X45 guides, see Where's My Content Now? Junos OS Release 12.1X45.

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.

WLAN Feature Guide for Security Devices

- This guide is missing information that the AX411 Access Point can be managed from SRX100 and SRX110 devices.

Network Address Translation

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

show security nat source persistent–nat–table internal-ip internal-port

```
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
```

show security nat source persistent–nat–table all

```
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
```

show security nat source persistent-nat-table summary

```
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
```

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 Feature Explorer: http://pathfinder.juniper.net/feature-explorer/select-software.html?swName=Junos+OS&typ=1.
- Some Junos OS 12.1X45 user, reference, and configuration guides and topics still include references to discontinued guides such as the *Feature Support Reference for SRX Series and J Series Devices* and the *Junos OS CLI Reference*. Please disregard those erroneous references. For more information about documentation changes implemented in 12.1X45 and which guides have been discontinued or moved, please see Where's My Content Now? Junos OS Release 12.1X45.

Documentation Updates 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.

- 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 and Changed Features in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 6
- Changes in Behavior and Syntax in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 21
- Known Behavior in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 30
- Known Issues in Junos OS Release 12.1X45-D15 for Branch SRX Series Services Gateways and J Series Services Routers on page 58
- Resolved Issues in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 63
- Migration, Upgrade, and Downgrade Instructions for Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 81

Migration, Upgrade, and Downgrade Instructions for Junos OS Release 12.1X45 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 81
- Upgrading an AppSecure Device on page 83
- Upgrade and Downgrade Scripts for Address Book Configuration on page 83
- Hardware Requirements for Junos OS Release 12.1X45 for SRX Series Services Gateways and J Series Services Routers on page 86

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 1 on page 85).

- About Upgrade and Downgrade Scripts on page 84
- Running Upgrade and Downgrade Scripts on page 85
- Upgrade and Downgrade Support Policy for Junos OS Releases on page 86

About Upgrade and Downgrade Scripts

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

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

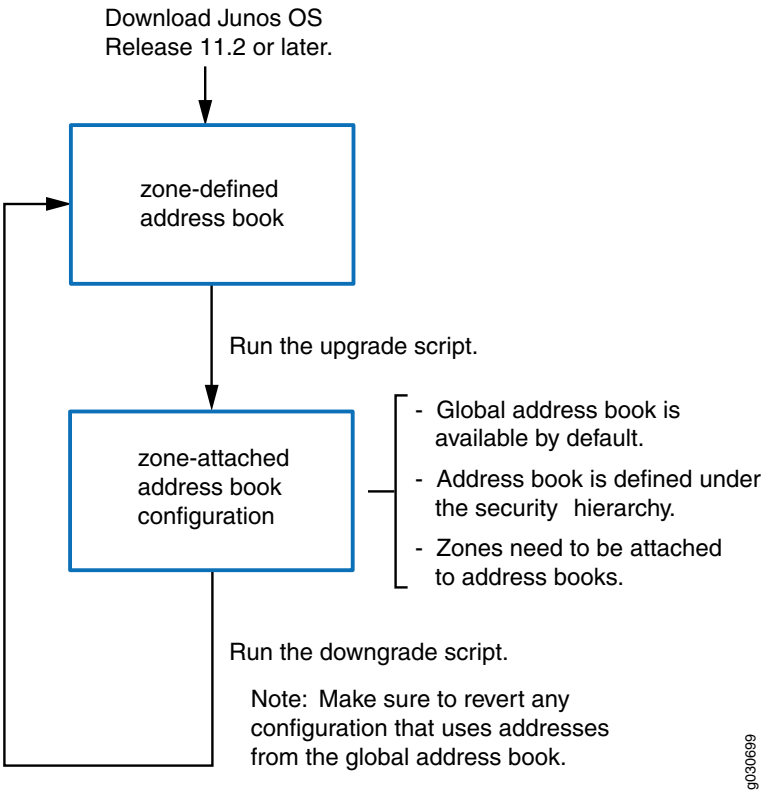
  After upgrading to the zone-attached address book configuration:

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

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

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

Figure 1: Upgrade and Downgrade Scripts for Address Books



Running Upgrade and Downgrade Scripts

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

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

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

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

Upgrade and Downgrade Support Policy for Junos OS Releases

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 12.1X45 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 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 7 on page 87 lists the USB and CompactFlash card devices supported for use with the J Series Services Routers.

Table 7: 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 8 on page 88 lists the CompactFlash card and DRAM requirements for J Series Services Routers.

Table 8: 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 and Changed Features in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 6
- Changes in Behavior and Syntax in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 21
- Known Behavior in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 30
- Known Issues in Junos OS Release 12.1X45-D15 for Branch SRX Series Services Gateways and J Series Services Routers on page 58
- Resolved Issues in Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 63
- Documentation Updates for Junos OS Release 12.1X45 for Branch SRX Series Services Gateways and J Series Services Routers on page 74

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 and Changed Features in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 89
- Changes in Behavior and Syntax in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 105
- Known Behavior in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 116
- Known Issues in Junos OS Release 12.1X45-D15 for High-End SRX Series Services Gateways on page 133
- Resolved Issues in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 136
- Documentation Updates for Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 148
- Migration, Upgrade, and Downgrade Instructions for Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 152

New and Changed Features in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways

The following features have been added to Junos OS Release 12.1X45. Following the description is the title of the manual or manuals to consult for further information.

NOTE: For the latest updates about support and issues on Junos Pulse, see the Junos Pulse Release Notes.

Release 12.1x45-D15 Software Features

- **IPsec VPN performance enhancements**—Starting in Junos OS Release 12.1X45-D15, a new configuration statement, **ipsec-performance-acceleration**, has been introduced under the **[edit security flow]** hierarchy to enable IPsec VPN performance acceleration. This feature is supported on all SRX Series high-end devices.

  By default, VPN performance acceleration is disabled on SRX Series devices. Enabling VPN performance acceleration can improve VPN throughput under certain conditions.

  The following functions are not supported:

  - VPN traffic ACL accounting on physical egress and ingress interface
  - VPN traffic physical interface filter-based policer

- VPN traffic physical interface QoS feature (classifier, remarking, scheduling, and shaping)

Release 12.1x45-D10 Software Features

Application Layer Gateways (ALG)

- **DDNS support**—Junos OS Release 12.1X45-D10 supports dynamic DNS (DDNS). This feature is supported on all high-end SRX Series devices.

  DDNS is an addition to the DNS ALG standard. The main difference between DNS and DDNS is in the message format of the header section and the update message.

  Compared with DNS messages, DDNS messages are processed differently. Message parsing is rewritten for DDNS. DDNS performs NAT and NAT-PT in the query part of the message and DNS performs NAT and NAT-PT in the response part of the message.

  DDNS updates a DNS server with new or changed records for IP addresses without the need for human intervention. Unlike DNS that only works with static IP addresses, DDNS is also designed to support dynamic IP addresses, such as those assigned by a DHCP server. DDNS is a good option for home networks, which often receive dynamic public IP addresses from their Internet provider that occasionally change.

  DDNS ALG does not support:

  - DNS packet over TCP
  - Reverse lookup
  - Logical systems

  [*Junos OS Application Layer Gateways (ALGs) Library for Security Devices*]

  [*DNS ALG Overview*]

- **Logging improvements for ALGs**—Junos OS Release 12.1X45-D10 introduces system log messages for all ALGs. These messages are supported on all high-end SRX Series devices.

  During ALG processing, every error and failure has a system log.

  There are 12 predefined tags and four levels of log options that can be utilized. The four levels at which system logs are captured during ALG processing are error, warning, notification, and debug.

  For example, when there is an open gate failure with the SUNRPC ALG, the log level for this event is **ERR**, the tag is **RT_ALG_ERR_GATE**, and the system log message is SUNRPC ALG open gate failed.

The ALG system log messages are:

LOG Level	TAG	System Log Messages
LOG_ERR	RT_ALG_ERR_INIT	ALG initialization failed.
LOG_ERR	RT_ALG_ERR_MEM_ALLOC	Call context allocated by ALG failed.
LOG_ERR	RT_ALG_ERR_RES_ALLOC	ASL resource created by ALG failed.
LOG_ERR	RT_ALG_ERR_NAT	NAT for ALG data session failed.
LOG_ERR	RT_ALG_ERR_GATE	ALG open gate failed.
LOG_WARNING	RT_ALG_WRN_CFG_NEED	ALG detected unusual traffic, to let it pass through. Need extra configuration.
LOG_WARNING	RT_ALG_WRN_CAPACITY_LMT	ALG exceeded capacity limitation.
LOG_WARNING	RT_ALG_WRN_FLOOD	ALG messages flooding.
LOG_NOTICE	RT_ALG_NTC_FSM_DROP	ALG finite state machine mismatch.
LOG_NOTICE	RT_ALG_NTC_PKT_MALFORMED	ALG packet payload malformed.
LOG_NOTICE	RT_ALG_NTC_PARSE_ERR	ALG packet decode error.
LOG_DEBUG	RT_ALG_DEBUG	There are different debug system log messages output at this level. Example: junos-alg - RT_ALG_DEBUG [junos@2636.1.1.1.2.35 alg-name="SQL" details="detect message with packet length more than 3K, bypass"] SQL ALG detected message with packet length more than 3K, bypass.

[*Junos OS Application Layer Gateways (ALGs) Library for Security Devices*]

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

  Beginning with Junos OS Release 12.1X45-D10, 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 Transparent Mode Feature Guide for Security Devices*]

AppSecure

- **AppTrack supports IPv6 address format**—This feature is supported on all high-end SRX Series devices.

  AppTrack now recognizes and logs IP addresses using the appropriate IPv4 or IPv6 format. There is no additional configuration needed to enable IPv6 support. When AppTrack is enabled, IPv6 is automatically supported for all relevant traffic.

  [*Understanding AppTrack*]

- **HTTP/HTTPS traffic can be redirected when denied or rejected by application firewall**—This feature is supported on all high-end SRX Series devices.

  A new **block-message** option for a deny or reject policy action in an application firewall redirects the user to a splash page. By default, the following message informs the user that their traffic has been denied or rejected.

  "*username*, Application Firewall has blocked your request to application *appname* at *dst-ip*:*dst-port* accessed from *src-ip*:*src-port*\n"

  To customize this message, you can define one or more block message profiles that contain either custom text to be added to the default message or a URL to redirect users to an informative webpage. The redirection URL uses the following format:

  "*http(s)://custom-redirect-url*?JNI_SRCIP=*src-ip*
  &JNI_SRCPORT=*src-port*&JNI_DSTIP=*dst-ip*
  &JNI_DSTPORT=*dst-port*&JNI_APPNAME=*appname*
  &JNI_USER=*username*&JNI_ROLES=*rolename*&JNI_POLICY=*policy-id*"

  A new **profile** option in the **rule-sets** configuration identifies which profile to use for applicable rules within that rule set.

  [*Application Firewall Overview*]

Chassis Cluster

- **Chassis cluster extended cluster ID**—This feature is supported on SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices through CLI configuration.

  The chassis cluster feature uses cluster ID to identify a cluster in a Layer 2 domain. Fifteen separate clusters are supported with the cluster ID range of 1 through 15 (cluster ID 0 is reserved).

  With Junos OS Release 12.1X45-D10, the new range for cluster IDs using the **set chassis cluster cluster-id** command is now 1 through 255 (cluster ID 0 is reserved).

  NOTE:
  - If you create a cluster with cluster IDs greater than 16, and then decide to roll back to a previous release image that does not support extended cluster IDs, the system comes up as standalone.
  - If you have a cluster set up and running with an earlier release of Junos OS, you can upgrade to Junos OS Release 12.1X45-D10 and re-create a cluster with extended cluster IDs greater than 16. However, if for any reason you decide to revert to the previous version of Junos OS that did not support extended cluster IDs, the system comes up with standalone devices after you reboot.

- **Chassis cluster secure login**—This feature is supported on all high-end SRX Series devices.

  High-end SRX series devices have a chassis cluster control port that is used to connect two SRX Series devices to form a chassis cluster. To refrain attackers from gaining privileged access through this control port, an internal IPsec SA is installed using the **request security internal-security-association refresh** command.

  Use the **show chassis cluster interfaces** CLI command to verify that internal SA is enabled:

```
user@host> show chassis cluster interfaces
  Control link status: Up

  Control interfaces:
      Index   Interface        Status        Internal SA <- new column
      0       em0              Up              enabled
      1       em1              Down            enabled
```

  See Example: Configuring an SRX Series Services Gateway for the High-End as a Chassis Cluster

Flow and Processing

- **Juniper flow monitoring IPv6 version 9 (V9) support**—This feature is supported on all high-end SRX Series devices.
  - IPv4 flow monitoring V9 provides an extensible and flexible method for using IPv4 templates to export records. Each template indicates the format in which the device exports data.

- When you configure the collector IP address using the **forwarding-options sampling family inet flow server** command, the flow server might be IPv4 or IPv6, but only IPv4 sampling works. Similarly, when you configure the collector IP address using the **forwarding-options sampling family inet6 flow server** command, the flow server might be IPv4 or IPv6, but only IPv6 sampling works.

  IPv6 flow monitoring V9 provides an extensible and flexible method for using IPv6 templates to export records. Each template indicates the format in which the device exports data.

Table 9 on page 94 shows a comparison between IPv4 and IPv6 template elements.

Table 9: Flow Selector Fields

Filed Name	IPv4 (Length)	IPv6 (Length)
Source IP Address	4 bytes	16 byte
Destination IP Address	4 bytes	16 byte
Source Port	2 bytes	2 bytes
Destination Port	2 bytes	2 bytes
Protocol	1 byte	1 byte
TOS	1 byte	1 byte
IIF	20 bits	20 bits
ICMP Type	2 bytes	2 bytes

- **IPv6 support for network processor offloading**—This feature is supported on SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices.

  As of Junos OS Release 12.1X45-D10, network processor offloading is supported on both IPv4 and IPv6 traffic.

  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 the central point. To enable network processor offloading, use the **set security forwarding-process application-services session-distribution-mode hash-based** command. You must reboot the device for the configuration to take effect.

  [*SRX5600 and SRX5800 Services Gateways Processing Overview*]

General Packet Radio Service (GPRS)

- **GTP control message path rate limit**—This feature is supported on all high-end SRX Series devices.

  You can now restrict the maximum packets per second for specific control messages on a path. These GTP messages include **create-req**, **delete-req** and other GTP messages.

However, you can restrict the maximum packets per minute for an **echo-req** GTP message.

The **path-rate-limit** function controls specific GTP messages in both the inbound and outbound directions. A drop threshold and an alarm threshold can be configured for each control message in the inbound and outbound direction for one path. If the control messages on one path reach the alarm threshold, an alarm log is generated. If the number of control messages received reaches the drop threshold, a packet drop log is generated and all other control messages of this type received later are dropped.

To control message traffic in the inbound and outbound directions, configure a policy on the device such that the direction that is consistent with the configured policy is defined as forward, and the opposite direction is defined as reverse. Use the **set security gprs gtp profile <profile-name> path-rate-limit** statement to restrict the maximum packets per second for specific control messages on a path.

- **General Packet Radio Service (GPRS) tunneling protocol, user plane (GTP-U)**—This feature is supported on all high-end SRX Series devices.

  GTP-U carries user data between the radio access network and the GPRS core network. The transported user data can be an IPv4 or IPv6 packet type.

  GTP firewall performs security checks on the GTP-U packets, including packet sanity checking, stateful inspection, sequence checking, and end-user address checking of GTP-U packets.

  At the **[edit security gprs gtp profile <*profile-name*>]** hierarchy level:

  - **u-tunnel-validated**—When enabled, GTP-PDU packets must match one of the existing GTP-U tunnels; otherwise the packet is dropped.
  - **seq-number-validated**—When enabled, GTP-PDU packets must match one of the existing GTP-U tunnels and its sequence number is checked. The packet is dropped if there is a tunnel mismatch or an incorrect sequence number. GTP-PDU without a sequence number will pass without a sequence check.
  - **end-user-address-validated**—When enabled , GTP-PDU packets must match one of the existing GTP-U tunnels and the end-user address (only an IPv4 user address is supported) is checked. The packet is dropped if there is a tunnel mismatch or an IPV4 end user address mismatch.
  - **log gtp-u**—When enabled, GTP-U inspection log is generated. If **log gtp-u** is set to **all**, then every GTP-U packet will generate a system log message. If **log gtp-u** is set to **dropped**, then only dropped GTP-U packets will generate a system log message.

  GTP-U packet inspection includes these four CLI configuration statements and the existing **set security gprs gtp profile <*profile_name*> gtp-in-gtp-denied** configuration statement.

  Use the **show security gprs gtp tunnels detail** CLI statement to display details of each GTP tunnel.

- **SCTP enhancements**—These feature enhancements are supported on all high-end SRX Series devices.

  The enhancements include the following:

- **Control message retransmission**—This enhancement was added to better support retransmission. A retransmitted cookie-echo/cookie-ack can pass after an association is established on the firewall, but it cannot pass after the configured handshake timeout. (For example, if a handshake timeout is configured for 20 seconds, the packets can pass through the 4-way handshake process only within the configured 20 seconds.) When the association is shut down completely, there are 2 seconds for packet (shutdown, shutdown-ack, shutdown-complete) retransmission.
- **Debugging and troubleshooting** —These enhancements include additional **show** command filter options, a new command for clearing associations, an additional trace flag option, and additional system log messages.

  Use the **detail** option of the **show security gprs sctp counters** command to view detailed debugging counters for SCTP packets.

  Use the **show security gprs sctp association** command to view established associations, and use additional options to filter the output.

  Use the **clear security gprs sctp association** command to clear SCTP associations.

  To configure debugging traces using the **detail** option, use the **sctp traceoptions flag** statement in the **[edit security gprs]** hierarchy.

  To configure the output of system log messages using the new **association**, **data-message-drop**, **control-message-drop**, **control-message-all** and **rate-limit** options, use the **sctp log** statement in the **[edit security gprs]** hierarchy.
- **Clearing deleted policy sessions and associations**—This enhancement clears all related sessions and associations when a policy is deleted.
- **SCTP inspection**—This enhancement enables you to use policy configuration to control the SCTP state inspection. If no profile is attached to a policy, SCTP packets are forwarded without any inspection. If a profile is attached to a policy, the SCTP packets that match the policy are inspected.

  To configure a policy with the **nat-only** option so that the payload IP addresses are translated but not inspected, use the **sctp profile** statement in the **[edit security gprs]** hierarchy.
- **Rate-limit setting**—This enhancement specifies that the rate limit for SCCP, SSP, and SST packets is per association. It is not a global messages rate limit. The rate limit is configured using the **sctp profile** statement in the **[edit security gprs]** hierarchy.
- **Default living timer**—This enhancement shortens the default living timer from 24 hours to 5 hours. When an association is established, its default idle timeout is 5 hours, but you can configure the timeout value from 10 minutes through 100 hours.

[*General Packet Radio Service Feature Guide for Security Devices*]

Logical Systems

- **Support for source NAT interface in logical systems**—This feature is supported on all high-end SRX Series devices for both IPv4 and IPv6 configurations.

  In previous Junos OS releases, all NAT configurations, except for source NAT interface, were supported for logical systems.

  A new option has been added to configure interface NAT port overloading in a root or logical system. To configure the **port-overloading-factor** option, use the **nat source interface** statement in the **[security nat]**hierarchy.

  The value entered for the port overloading factor (a number from 1 through the maximum port capacity) is multiplied by the maximum port capacity to set the port overloading threshold. For example, if the port overloading factor for an SRX3400 device is set to 2, it is multiplied by the maximum port capacity of 63,486, making the port overloading threshold 126972(2*63486).

  The existing **port-overloading** option is not supported for logical systems and should not be used in conjunction with **port-overloading factor**, because the statements can overwrite each other. For example, if **port-overloading** has been set to **off** to disable interface port overloading, and subsequently **port-overloading-factor** is configured with any value greater than 1, the **port-overloading-factor** will override the **port-overloading** setting.

  Use the new **all** option for the **show security nat interface-nat-ports logical-systems** command to display all port usage information for the master and user logical system.

  Junos OS Logical Systems Library for Security Devices

Negated Address Support

- **Negated address support** —This feature is supported on all high-end SRX Series devices.

  Users can exclude source, destination, or both addresses from the policy by configuring them as a negated address.

  [*Understanding Negated Address Support*, *Example: Configuring Negated Addresses*]

  [*source-address-excluded*, *destination-address-excluded*]

Network Address Translation (NAT)

- **NAT resource utilization**—This feature is supported on all high-end SRX Series devices.

  This feature enables you to improve management of Network Address Translation (NAT) pool addresses and rules.

- **Source NAT pool usage**—You can view information about source NAT pool resources for all configured source NAT pools or for a specific source NAT pool. In pools without Port Address Translation (PAT), information about IP addresses is displayed; and in pools with PAT, information about ports is displayed.

  Use the **show security nat resource-usage source-pool** command to view resource information, including the number of available resources and the number of used resources in the pool.

- **Source NAT pool utilization alarm**—This option enables you to define utilization alarm thresholds for a specific NAT source pool. When pool utilization exceeds the upper (raise) threshold or falls below the lower (clear) threshold, an SNMP trap is triggered.

  To configure the **pool-utilization-alarm** option, use the **source pool *pool-name*** statement in the **[edit security nat]** hierarchy.

- **NAT rule sessions**—You can view real-time information about the number of sessions, both successful and failed, for specific source, destination NAT rules, and static NAT rules.

  Use the **show security nat source rule**, **show security destination nat rule**, and **show security static nat rule** commands to view session information.

- **NAT rule session count alarm**—This option enables you to define session count alarm thresholds for a specific NAT source rule. When the session count exceeds the upper (raise) threshold or falls below the lower (clear) threshold, an SNMP trap is triggered.

  To configure the **rule-session-count-alarm** option for source NAT, use the **rule-set *rule-set-name* rule *rule-name* then source-nat** statement in the **[edit security nat]** hierarchy.

  To configure the **rule-session-count-alarm** option for destination NAT, use the **rule-set *rule-set-name* rule *rule-name* then destination-nat** statement in the **[edit security nat]** hierarchy.

  To configure the **rule-session-count-alarm** option for static NAT, use the **static rule-set *rule-set-name* rule *rule-name* then static-nat**statement in the **[edit security nat]** hierarchy.

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

- **Single IP address in a source NAT pool without PAT**—This feature is supported on all high-end SRX Series devices.

  This feature allows you to configure a single IP address in a source NAT pool with no Port Address Translation (PAT), and enables you to use two new options: **address-shared** and **address-pooling** (**paired** or **no-paired**).

  - **Address sharing**—This option enables you to map multiple source IP addresses to one external IP address. Use this option to increase NAT resources and improve traffic when you are configuring a source NAT pool without PAT.

    To configure the **address-shared** option, use the **nat source pool** statement in the **[edit security nat]** hierarchy.

- **Address pooling**—The **address-pooling-paired** and **address-pooling-no-paired** options enable you to associate one internal IP address with the same external IP address for the duration of a session or not. For applications that require this type of mapping, use the **pooling-paired** option when you are configuring a source NAT pool.

  To configure the **address-pooling** option, use the **nat source pool** statement in the **[edit security nat]** hierarchy.

The number of hosts that a source NAT pool with out PAT can support is limited to the number of addresses in the pool. When you have a pool with a single IP address, only one host can be supported, and traffic from other hosts is blocked, because there are no resources available.

If a single IP address is configured for a source NAT pool without PAT when NAT resource assignment is not in active-backup mode in a chassis cluster, traffic through node 1 will be blocked.

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

- **Static NAT rule match for source address and source port**—This feature is supported on all high-end SRX Series devices.

  In addition to specifying the destination address as a match condition for a rule, static Network Address Translation (NAT) also supports source address, source address name, and source port match conditions. These new options enable you to target specific traffic for static NAT processing.

  To configure the **source-address**, **source-address-name**, and **source-port** options, use the **static rule-set** *rule-set-name* **rule** *rule-name* **match** statement in the **[edit security nat]** hierarchy.

  Use the **show security nat static rule** command to view source address and source port information.

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

- **Source NAT rule match for source port**—This feature is supported on all high-end SRX Series devices.

  In addition to specifying the destination address, the destination address name, the destination port, the source address, the source address name, and the protocol, source Network Address Translation (NAT) also supports source port match conditions. This new option enables you to target specific traffic for source NAT processing.

  To configure the **source-port** option, use the **source rule-set** *rule-set-name* **rule** *rule-name* **match** statement in the **[edit security nat]** hierarchy.

  Use the **show security nat source rule** command to view source port information.

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

Security Policies

- **Per-policy support for 3072 application items**—This feature is supported on all high-end SRX Series devices.

The total number of application items that can be configured in one security policy has been increased to 3072.

[*Best Practices for Defining Policies on High-End SRX Series Devices*]

- **Security policy firewall authentication now provides user identities for user role firewall provisioning**—This feature is supported on all high-end SRX Series devices.

  User identity information, maintained by firewall authentication, can also be mapped to the user's IP address and used for user role firewall enforcement.

  A new UIT, the firewall authentication table, provides firewall authentication data for username and role retrieval. When users authenticate to the firewall, usernames and roles (groups) are mapped to IP addresses and written to the firewall authentication table. The following command enables the firewall authentication table as an authentication source and specifies its priority among other available UITs:

  set security user-identification authentication-source firewall-authentication priority *priority*

  The firewall authentication table is propagated when a security policy permits firewall authentication and specifies the new type, **user-firewall**. Users are authenticated based on the access-profile configured for the policy. To trigger firewall authentication for HTTPS traffic, you also need to specify the SSL termination profile. This option is not needed for HTTP traffic.

  set security policies from-zone *zone* to-zone *zone* policy *policy-name* then permit firewall-authentication user-firewall access-profile *profile-name* ssl-termination-profile *profile-name*

  NOTE: The access profile is configured in the [edit access profile] hierarchy as with other firewall authentication types. The SSL termination profile is configured in the [edit services ssl] hierarchy.

  set access profile *profile-name* client *client-name* firewall-user password *pwd*
  set services ssl termination profile *ssl-profile-name* server-certificate *certificate-type*

[*Understanding User Role Firewalls*, *Firewall User Authentication Overview*]

Services Processing Card SRX5K-SPC-4-15-320 Features

- **Central point session capacity**—This feature is supported on SRX5600 and SRX5800 devices with next-generation SPCs. This enhancement increases the central point session capacity to 100 million for both IPv4 and IPv6 sessions.

  [*Processing Overview Feature Guide for Security Devices*]

- **Packet-ordering function enhancements**—This feature is supported on SRX5800 and SRX5600 devices with next-generation SPCs.

  This feature improves the performance of the device by activating the packet-ordering function of the Packet Ordering Engine on the XLP processor on the central point. When you activate the packet-ordering function, the load-balancing thread (LBT) and packet-ordering thread (POT) are removed and their core is used to run the flow thread.

By increasing the number of cores for running the flow thread, the central point gains more CPU power, resulting in improved performance.

[*Processing Overview Feature Guide for Security Devices*]

- **System session distribution mechanism in adaptive mode**—This feature enhancement is supported on SRX5800 and SRX5600 devices with next-generation SPCs and existing SPCs installed.

  This enhancement provides implementation of adaptive mode where sessions are distributed based on the real-time session and CPU power usage of each SPU.

  In adaptive mode, the system resources are utilized to the maximum degree because the sessions distributed among the different types of SPUs are variable rather than based on a fixed ratio.

  By default, the device operates in adaptive mode.

  [*Processing Overview Feature Guide for Security Devices*]

System Logs

The following system logs are introduced in Junos OS Release 12.1X45-D10:

- **RT_GTP_CFG_PROFILE_PATH_RATE_LIMIT**—Configure GPRS Tunnelling Protocol (GTP) path rate limit.
- **RT_GTP_PATH_RATE_ALARM** —Displays GTP path control messages.
- **RT_GTP_PATH_RATE_DROP**—Displays GTP path control messages exceed path rate limit.
- **RT_GTP_U_PKT**—Displays GTP-U packet information.

Virtual Private Network (VPN)

- AutoVPN Protocol Independent Multicast (PIM) point-to-multipoint mode—AutoVPN hubs are supported on SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices. AutoVPN spokes are supported only on SRX1400 devices.

  In hub-and-spoke topologies, multicast data is used for applications such as video streaming or the music-on-hold function for VoIP systems. The multicast sender is typically located behind the hub, although the sender could also be located behind a spoke or a set of spokes. Junos OS Release 12.1X45-D10 supports multicast traffic in an AutoVPN hub-and-spoke network.

  AutoVPN secure tunnel st0 logical interfaces on hub-and-spoke devices are configured for PIM point-to-multipoint mode. This allows devices in the network to replicate multicast data packets to neighbors that join the multicast group. PIM and multipoint must be enabled on multicast sending and receiving interfaces on the devices. To enable PIM on an st0 logical interface, use the **set protocols pim interface st0.*x*** configuration statement. To enable multipoint on an st0 logical interface, use the **multipoint** configuration statement at the [**edit interfaces st0 unit *x***] hierarchy level.

NOTE: AutoVPN multicast deployments support a maximum of 500 PIM neighbors. The st0 interface that hosts PIM on the hub can support a maximum of 500 spokes.

Configure dynamic routing protocols to support multicast traffic:

- OSPF—Configure the st0 logical interface as an OSPF interface at the [**edit protocols ospf area *area-id* interface**] hierarchy level and specify the **interface-type p2mp** and **dynamic-neighbor** options.
- BGP—On the hub, configure the **local-address** option at the [**edit protocols bgp group bgp-group**] hierarchy level with the address of the st0 logical interface; configure the **neighbor** or the **allow** option to match the st0 addresses on the spokes. On the spoke, configure the **local-address** option at the [**edit protocols bgp group bgp-group**] hierarchy level with the address of the st0 logical interface; configure the **neighbor** option to match the st0 address on the hub. Configure policy statements at the [**edit policy-options**] hierarchy level to limit the number of advertised routes.

NOTE: The RIP dynamic routing protocol is not supported with AutoVPN for multicast traffic.

[*AutoVPNs Feature Guide for Security Devices*]

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

  Junos OS Release 12.1X45-D10 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 Feature Guide for Security Devices*]

- **Certificate chaining**—This feature is supported on all high-end SRX Series devices.

  Certificate-based authentication is an authentication method supported on SRX Series devices during IKE negotiation. In large networks, multiple certificate authorities (CAs) can issue end entity (EE) certificates to their respective end devices. It is common to have separate CAs for individual locations, departments, and organizations.

  With a single-level hierarchy for certificate-based authentication, all EE certificates in the network must be signed by the same CA. All firewall devices must have the same CA certificate enrolled for peer certificate validation. The certificate payload sent during IKE negotiation only contains EE certificates.

  In Junos OS Release 12.1X45-D10, the certificate payload sent during IKE negotiation can contain a chain of EE and CA certificates. A certificate chain is the list of certificates required to certify the subject in the EE certificate. The certificate chain includes the

EE certificate, intermediate CA certificates, and the root CA certificate. CA certificates can be enrolled using Simple Certificate Enrollment Process (SCEP) or loaded manually. There is no new CLI configuration statement or command for certificate chains; however, every end device must be configured with a CA profile for each CA in the certificate chain.

The network administrator needs to ensure that all peers participating in IKE negotiation have at least one common trusted CA in their respective certificate chains. The common trusted CA does not have to be the root CA. The number of certificates in the chain, including certificates for EEs and the topmost CA in the chain, cannot exceed 10.

[*Certificates and Public Key Infrastructure Feature Guide for Security Devices*]

- **Suite B cryptographic suites**—This feature is supported on SRX5600 and SRX5800 devices with the Next-Generation Services Processing Card (NG-SPC) installed.

  Suite B is a set of cryptographic algorithms designated by the U.S. National Security Agency to allow commercial products to protect traffic that is classified at secret or top secret levels. Suite B protocols are defined in RFC 6379, *Suite B Cryptographic Suites for IPsec*. The Suite B cryptographic suites supported in Junos OS Release 12.1X45-D10 provide Encapsulating Security Payload (ESP) integrity and confidentiality and should be used when ESP integrity protection and encryption are both required.

  The following Suite B cryptographic suites are supported in Junos OS Release 12.1X45-D10:

  - Suite-B-GCM-128
    - ESP: Advanced Encryption Standard (AES) encryption with 128-bit keys and 16-octet integrity check value (ICV) in Galois/Counter Mode (GCM).
    - IKE: AES encryption with 128-bit keys in cipher block chaining (CBC) mode, integrity using SHA-256 authentication, and key establishment using Diffie-Hellman (DH) group 19 and authentication using Elliptic Curve Digital Signature Algorithm (ECDSA) 256-bit elliptic curve signatures.
  - Suite-B-GCM-256
    - ESP: AES encryption with 256-bit keys and 16-octet ICV in GCM for ESP.
    - IKE: AES encryption with 256-bit keys in CBC mode, integrity using SHA-384 authentication, and key establishment using DH group 20 and authentication using ECDSA 384-bit elliptic curve signatures.

  IKEv1 and IKEv2 configuration are supported.

  NOTE: Suite B is not fully supported on the SRX1400, SRX3400, SRX3600, and on SRX5600 and SRX5800 devices that do not have the NG-SPC installed. You can configure IKE with Suite B options on these devices, but AES-GCM options are not supported. If you configure IKE with Suite B options on these devices, VPN establishment is slower because the devices do not have the hardware processors that can accelerate Suite B algorithm processing.

NOTE: Suite B is not supported with the group VPN feature.

In Release 12.1.X45-D10, new and existing options support Suite B compliance in IKE and IPsec proposal configuration:

- For IKE proposals configured at the [**edit security ike proposal** *proposal-name*] hierarchy level:
  - **authentication-algorithm** options include **sha-256** and **sha-384**
  - **authentication-method** options include **ecdsa-signatures-256** and **ecdsa-signatures-384**
  - **dh-group** options include **group19** and **group20**
- For IPsec proposals configured at the [**edit security ipsec proposal** *proposal-name*] hierarchy level, **encryption-algorithm** options include **aes-128-gcm**, **aes-192-gcm**, and **aes-256-gcm**.
- For IPsec policies configured at the [**edit security ipsec policy** *policy-name*] hierarchy level, the **perfect-forward-secrecy keys** options include **group19** and **group20**.
- For convenience, predefined proposals that provide Suite B compliance—**suiteb-gcm-128** and **suiteb-gcm-256**—are available at the [**edit security ike policy** *policy-name*] and [**edit security ipsec policy** *policy-name*] hierarchy levels.

[*IPsec VPNs Feature Guide for Security Devices*]

Related Documentation

- Known Issues in Junos OS Release 12.1X45-D15 for High-End SRX Series Services Gateways on page 133
- Resolved Issues in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 136
- Documentation Updates for Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 148
- Changes in Behavior and Syntax in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 105
- Known Behavior in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 116

Changes in Behavior and Syntax in Junos OS Release 12.1X45 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:

AppSecure

- The following new counters have been added to the **show services application-identification counter** command output:
  - Application Identification Module Statistics

    Sessions that triggered interest callback

    Sessions that triggered create callback

    Sessions that triggered packet process callback

    Sessions that triggered session close callback

    Client-to-server flows ignored

    Server-to-client flows ignored

    Negative cache hits

    Cache inserted

    Cache expired

    Session ignored due to disabled AppId

    Session ignored due to unsupported protocol

    Session ignored due to no active signature set

    Session ignored due to max concurrent session reached
  - Application Identification TCP Reordering Statistics

    Stream constructed

    Stream destructed

    Segment allocated

    Segment freed

    Packet cloned

    Packet freed

    Fast path segment

    Segment case 1

    Segment case 2

    Segment case 3

    Segment case 4

    Segment case 5

    Segment case 6
  - Application Identification Decoder Statistics

    Session state constructed

Session state destructed

Packet decoded

HTTP session state constructed

HTTP session state destructed

HTTP packet decoded

- Application Identification Heuristics Statistics

  Unspecified encrypted sessions called

  Encrypted P2P sessions called

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:HTTP];
    }
    then {
      deny;
    }
  }
  default-rule {
    permit;
  }
}
```

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

  - HTTP traffic with or without nested applications would be denied by rule1.
  - HTTP traffic with a nested application, such as junos:FACEBOOK or junos:TWITTER, would be denied by rule1.
  - All other traffic would be permitted by the default rule.

  After Junos OS release 11.4R6 and later, the dynamic application junos:HTTP matches only the traffic that does not contains no recognizable nested application. The sample rules would now be applied differently:

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

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 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 10 on page 109 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 10: 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 IDP process 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 are 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 11: Items Deprecated in Junos OS Release 12.1X45-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.
max-packet-mem	**max-packet-memory-ratio**	**security idp sensor-configuration re-assembler**	On all high-end SRX Series devices, the **max-packet-mem** command is not supported.
max-packet-memory	**max-packet-memory-ratio** **max-reass-packet-memory-ratio**	**security idp sensor-configuration application-identification**	On all high-end SRX Series devices, the **max-packet-memory** command is not supported.

Table 12 on page 110 lists the deprecated system log messages in Junos OS Release 12.1X45-D10.

Table 12: Deprecated System Log Messages in Junos OS Release 12.1X45-D10

Deprecated Item	Replacement
RT_GTP_PKT_ECHO_REQUEST	RT_GTP_V0_PKT_ECHO_REQUEST
RT_GTP_PKT_ECHO_REPONSE	RT_GTP_V0_PKT_ECHO_RESPONSE
	RT_GTP_V1_PKT_ECHO_REQUEST
	RT_GTP_V1_PKT_ECHO_RESPONSE
	RT_GTP_V2_PKT_ECHO_REQUEST
	RT_GTP_V2_PKT_ECHO_RESPONSE

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 and Prevention (IDP)

- 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-memory-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-memory-ratio ***percentage-value***

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

  - 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.

- When certain TCP error packets (packets with anomalies) during or after the three-way handshake are forwarded to IDP for processing, IDP TCP reassembly stops the reassembly. Once the reassembly is stopped, IDP does not continue the stream-based attack detection and TCP error packets are not dropped. The **action-on-reassembly-failure** option changes this behavior so that you can configure the action to be initiated when a reassembly failure occurs.

  - Use the following configuration command to drop the error packets when a reassembly failure occurs:

    set security idp sensor-configuration re-assembler action-on-reassembly-failure drop

    Use the following configuration command to drop the session when a reassembly failure occurs:

    set security idp sensor-configuration re-assembler action-on-reassembly-failure drop-session

    If you do not require any action to be taken, then use the following configuration command:

    set security idp sensor-configuration re-assembler action-on-reassembly-failure ignore

    By default, **action-on-reassembly-failure** is set to drop.

  - The **tcp-error-logging** and **no-tcp-error-logging** options enable or disable TCP error logging.

    Use the following commands to enable or disable TCP error logging:

    set security idp sensor-configuration re-assembler tcp-error-logging

    set security idp sensor-configuration re-assembler no-tcp-error-logging

    By default, TCP error logging is disabled.

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.

  [*SNMP MIBS and Traps Reference for SRX1400 and SRX3000 Line Services Gateways*]

  [*SNMP MIBS and Traps Reference for SRX5000 Line Services Gateways*]

Screen

- The TCP SYN flood counter for a SYN cookie or a SYN proxy attack incorrectly counted every second, thus incrementing the counter every second. This issue has been rectified so that every TCP SYN packet is counted for each SYN cookie or SYN proxy attack. Now every time you receive a SYN packet that is greater than the threshold value, the counter is incremented.

Session Timeout for Reroute Failure

- The **route-change-timeout** configuration statement at the [**edit security flow**] hierarchy level sets the timeout when a session is rerouted but there is a reroute failure (for example, the new route uses a different egress zone from the previous route). In previous releases, the **route-change-timeout** statement was disabled by default. In Release 12.1X45D10, the **route-change-timeout** configuration is enabled by default and the default timeout value is 6 seconds.

SNMP

- On all high-end SRX Series devices, the screen SNMP trap **jnxJsScreenCfgChange** will not be sent during reboot.

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_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**:

- 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 12.1X45-D10, an IPsec policy for a VPN can contain proposals with different protocol types (ESP or AH). This means that an IPsec SA can be established with either ESP or AH, depending on the protocol type in the peer's proposal.
- For each VPN tunnel, both Encapsulating Security Payload (ESP) and Authentication Header (AH) tunnel sessions are installed on Services Processing Units (SPUs) and the control plane. In previous Junos OS releases, two tunnel sessions of the same protocol (ESP or AH) were installed for each VPN tunnel. For branch SRX Series devices, tunnel sessions are updated with the negotiated protocol after negotiation is completed. For high-end SRX Series devices, tunnel sessions on anchor SPUs are updated with the negotiated protocol while non-anchor SPUs retain ESP and AH tunnel sessions.

  The ESP and AH tunnel sessions are displayed in the outputs for the **show security flow session** and **show security flow cp-session** operational mode commands.

- 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 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>

Related Documentation

- New and Changed Features in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 89
- Known Issues in Junos OS Release 12.1X45-D15 for High-End SRX Series Services Gateways on page 133
- Resolved Issues in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 136
- Documentation Updates for Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 148
- Known Behavior in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 116

Known Behavior in Junos OS Release 12.1X45 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 SRX1400, 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-Server and DHCP-Client
  - GPRS, GTP, and SCTP

  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 SRX1400, 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 SRX1400, 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, 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 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.

- 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.
- On all high-end SRX Series devices, the GPRS tunneling protocol (GTP) module competes with other modules for memory allocation during runtime because it has dynamic memory allocation for tunnel management.
- On all high-end SRX Series devices, GTP-U inspection has the following limitations:
  - When GTP-U inspection is enabled, GTP-U throughput drops.
  - GTP-U inspection only affects the new flow sessions that are created after enabling the GTP-U inspection.

NOTE: When GTP-U inspection is disabled, the GTP module ignores the traffic on which the corresponding flow sessions were created. When GTP-U inspection is reenabled, the GTP module continues to ignore the traffic during the lifetime of the flow sessions that were created before the GTP-U inspection was reenabled.

  - The ramp-up rate of GTP tunnel management messages decreases slightly (the decrease rate is less than 10 percent) when the GTP control (GTP-C) tunnel and GTP-U tunnel are created on different Services Processing Units (SPUs), whether GTP-U inspection is enabled or not.

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 reenabled; doing this will avoid any impact caused by the old SCTP sessions on the new SCTP communications.
- Only established SCTP associations will be synchronized 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 fails over 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, and 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
- 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:
  - The forwarding class is the 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 all high-end SRX Series devices, the flow monitoring version 9 has the following limitations:
  - Routing Engine based flow monitoring V5 or V8 mode is mutually exclusive with inline flow monitoring V9.
  - High-end SRX Series devices do not support multiple collectors like branch SRX Series devices. Only one V9 collector per IPv4 or IPv6 is supported.
  - Flow aggregation for V9 export is not supported.
  - Only UDP over IPv4 or IPv6 protocol can be used as the transport protocol.
  - Only the standard IPv4 or IPv6 template is supported for exporting flow monitoring records.
  - User-defined or special templates are not supported for exporting flow monitoring records.
  - Chassis cluster is supported without flow monitoring session synchronization.
- 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, the 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 Release 11.2 or later, a migration of IDP security package files needs to be performed. This is done automatically on upgrade when the IDP process comes up. Similarly, when the image

is downgraded, a migration (secDb install) is automatically performed when the IDP process 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 fail over or fail back.
  - 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 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

- The following table indicates browser compatibility:

Table 13: Browser Compatibility on High-End SRX Series Devices

Device	Application	Supported Browsers	Recommended Browser
SRX1400, SRX3400, SRX3600, SRX5600, SRX5800	J-Web	• Mozilla Firefox version 3.6 or later • Microsoft Internet Explorer version 7.0	Mozilla Firefox version 3.6 or later

- 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 the 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.
- 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)

- **Single IP address in a source NAT pool without PAT**—The number of hosts that a source NAT pool without PAT can support is limited to the number of addresses in the pool. When you have a pool with a single IP address, only one host can be supported, and traffic from other hosts is blocked because there are no resources available.

  If a single IP address is configured for a source NAT pool without PAT when NAT resource assignment is not in active-backup mode in a chassis cluster, traffic through node 1 will be blocked.

- For all ALG traffic, except FTP, we recommend that you not use the static NAT rule options **source-address** or **source-port**. Data session creation can fail if these options are used, because the IP address and the source port value, which is a random value, might not match the static NAT rule. For the same reason, we also recommend that you not use the source NAT rule option **source-port** for ALG traffic.

  For FTP ALG traffic, the **source-address** option can be used because an IP address can be provided to match the source address of a static NAT rule.

Additionally, because static NAT rules do not support overlapping addresses and ports, they should not be used to map one external IP address to multiple internal IP addresses for ALG traffic. For example, if different sites want to access two different FTP servers, the internal FTP servers should be mapped to two different external IP addresses.

- 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	12,288
IP addresses supporting port translation	8192	8192	12,288
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 (63,488 through 65,535), 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 (63,488 through 65,535) for Application Layer Gateway (ALG) module use. On SRX5600 and SRX5800 devices, if all of the 12288 source pool is configured, a port allocation of 2M 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, static, and source NAT rules has been incremented as shown in Table 14 on page 129. The limitation on the number of destination rule sets and static rule sets has been increased.

  Table 14 on page 129 provides the requirements per device to increase the configuration limitation as well as to scale the capacity for each device.

Table 14: 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 SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices.

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	20,480	30,720
Total NAT rules per rule set	20,480	30,720

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, you cannot configure the following IP addresses as negated addresses in a policy:
  - Wildcard addresses
  - IPv6 addresses
  - Addresses such as **any**, **any-ipv4** , **any-ipv6** and **0.0.0.0**
- When a range of addresses or a single address is negated, it can be divided into multiple addresses. These negated addresses are shown as a prefix or a length that requires more memory for storage on a Packet Forwarding Engine.
- Each platform has a limited number of policies with negated addresses. A policy can contain 10 source or destination addresses. The capacity of the policy depends on the maximum number of policies that the platform supports.

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.

In-Service Software Upgrade (ISSU)

- On all high-end SRX Series devices that support unified in-service software upgrade (ISSU), when unified ISSU is performed from an earlier release (earlier than the releases listed below) to any SRX Series special releases (12.1X44-D10 or later), it does not proceed after the first node is upgraded and becomes secondary.
  - Junos OS Release 10.4R9 and later
  - Junos OS Release 11.1R7 and later
  - Junos OS Release 11.2R5 and later
  - Junos OS Release 11.3R4 and later
  - Junos OS Release 11.4R1.7 and later
  - Junos OS Release 12.1R1 and later

  As a workaround, do the following:

  First perform unified ISSU from the earlier image to any of the aforementioned listed images.

  After the unified ISSU is successful, perform it once again to the targeted Junos OS SRX Series special release (Junos OS Release 12.1X44-D10 or later).

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)
- VPN monitoring and Suite B cryptographic configuration options **ecdsa-signatures-384** (for IKE authentication) and Diffie-Hellman **group20** consume considerable CPU resources. If VPN monitoring and the **ecdsa-signatures-384** and **group20** options are used on an SRX Series device with a large number of tunnels configured, the device must have the Next-Generation SPC installed.
- 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 and Changed Features in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 89

- Resolved Issues in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 136
- Known Issues in Junos OS Release 12.1X45-D15 for High-End SRX Series Services Gateways on page 133
- Documentation Updates for Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 148
- Changes in Behavior and Syntax in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 105

Known Issues in Junos OS Release 12.1X45-D15 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.

NOTE: 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.

Application Layer Gateways (ALG)

- When an RTSP TCP segment cannot be processed because it is too small or incomplete, the RTSP ALG holds it and waits for the next segment. An RTSP endpoint does not receive an ACK for segments that are too small, so it retransmits the segment several times. Eventually, the RTSP endpoint resets the TCP connection. [PR887601]
- The SUN RPC ALG might not work properly when the SUN RPC server replies with a get-address packet to the client. This might wrongly truncate the server's address, which causes the SUN RPC connection to fail. [PR901205]

Certificate Authority (CA) Profile

- The **show security pki *-certificate** shows the time without a time zone. [PR746785]

Chassis Cluster

- On SRX1400, SRX3400, and SRX3600 Series devices, under certain conditions, the em0 (tsec1) detection and recovery mechanism is not working as expected. This might cause the chassis cluster to fail or split-brain condition or all FPCs reset on the local node. As a workaround, use the **set chassis cluster heartbeat-threshold 8** command.

  NOTE: Do not use the security policy count and make sure trace options are disabled. Do not use set security log mode event command; instead use mode stream (default mode). [PR877604]

- On devices in a chassis cluster, the chassisd log outputs are flooded with the following message: **LCC: fru_is_present: out of range slot -1 for SCB**. [PR889776]

Dynamic Host Configuration Protocol (DHCP)

- On all high-end SRX Series devices, the Dynamic Host Configuration Protocol version 6 (DCHPv6) server did not create any server binding. [PR799829]
- Prior to Junos OS Reease 11.4R9, DHCP option 125 cannot be configured for use as the **byte-stream** option. With Junos OS Release 11.4R9 and later releases, DHCP option 125 can be used for the **byte-stream** option. [PR895055]

Flow and Processing

- When packets must be routed out from the same interface they are received from, the following log messages are logged:

  nh_walk_chek_max_num_tag: unexpected NH type 17 [PR837471]

J-Web

- In J-Web, the LSYS operation might cause MGD to generate a core file, and "compare before commit" does not work. [PR889029]
- All fields in the edit policy window are empty in the logical systems. [PR900975]
- On SRX3400, SRX3600, SRX5600, and SRX5800 devices; when you use the Microsoft Internet Explorer browser to open reports from the following pages in the J-Web interface, the reports open in the same browser session:
  - Files page (Maintain > Files)
  - History page (Maintain > Config Management > History)
  - Port Troubleshooting page (Troubleshoot > Troubleshoot > Troubleshoot Port)
  - Static Routing page (Monitor > Routing > Route Information)
  - Support Information page (Maintain > Customer Support > Support Information)
  - View Events page (Monitor > Events and Alarms > View Events) [PR433883]

Interfaces and Routing

- When you configure and commit IPv6 addresses on a logical interface, the output of the **show interface terse** command does not reflect the change immediately. [PR802229]
- On SRX550 devices, the Virtual Router Redundancy Protocol (VRRP) does not work when it is connected through integrated routing and bridging (IRB). [PR834766]

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]
- On devices in a chassis cluster, the chassis cluster rule number of sessions in snmpwalk result is the sum of the real number of sessions of the primary node and the secondary node.[PR908206]

Platform and Infrastructure

- On all high-end SRX series device, when fragmented jumbo frames are reassembled in Services Processing Unit (Reassembling might be required by IDP feature, ALG feature, ESP/AH packets, and L2TP packets) and if the size of the reassembled packet becomes larger than 9712 bytes, the packet is dropped in device internal, and the device reports XLR egress packets corruption issues. As a workaround, use the cli command **set security flow reordering-mixed-traffic disable** to resolve the issue. [PR819621]
- When the backup Routing Engine kernel fails, some devices send a message to the master Routing Engine to generate a core file. [PR854501]
- During every failover of redundancy-group 0, the /etc/ssh and /var/db/certs directories are copied from primary node to secondary node. However, the directories are not copied correctly and nested directories such as /etc/ssh/ssh, /etc/ssh/ssh/ssh are created. [PR878436]
- All input parameters for the command **show security match-policies global source-ip <source IP> destination-ip <destination IP> source-port <source port> destination-port <destination port> protocol <protocol>** are not provided, it might trigger the mgd process into an infinite loop, resulting in high CPU utilization on the Routing Engine. [PR893721]
- The CRL download fails for fragmented LDAP packets. [PR910947]
- J-Flow is not working as expected. The cflowd packets are not seen for V5 and V8 sampled flows. [PR916986]
- E2edebug traces are not generated for all the events. [PR919471]

Screen

- On SRX Series devices with teardrop Screen enabled, the teardrop attack traffic is not intermittently detected, and it is forwarded out of the device. [PR906811]

SNMP

- The SNMP query or walk on ipNetToMediaPhysAddress does not match the **show arp** command output. [PR850051]

System Logs

- On SRX3400 and SRX3600 devices, the following system logs are seen in the messages file:

sfchip_show_rates_pfe: Fchip Plane 0, dpc 0, pfe <1/2/3>: Invalid dpc

These system logs do not affect the device. [PR738199]

- Memory leak is observed with the 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]

Virtual Private Network (VPN)

- On a high-scale RIP deployment, frequent flap of tunnels might cause a small number of RIP routes to be missed. These routes are eventually recovered. [PR802078]
- In a site-to-site IPsec VPN deployments using IKEv2, when tunnels are removed through configuration change, the information is not propagated to the remote peer. Later, when the peer initiates a normal Phase-1 re-key process, the kmd process crashes and core files are generated. [PR898198]

Related Documentation

- New and Changed Features in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 89
- Known Behavior in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 116
- Documentation Updates for Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 148

Resolved Issues in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways

The following are the issues that have been resolved in Junos OS Release 12.1X45 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.

NOTE: **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.

Resolved Issues in Junos OS Release 12.1X45-D15 for High-End SRX Series Services Gateways

Application Layer Gateways (ALG)

- In certain circumstances, if the OPTIONS method is used to create a call, and the INVITE method is used to reuse the call, the SIP ALG would apply an incorrect state. As a result, the device might drop the ACK of 200-OK. [PR898956]
- The SCTP module drops the SCCP packet when the received SCCP pointer goes out of order. [PR901584]

- On devices enabled with the MSRPC ALG, the flowd process might crash frequently when heavy MSRPC traffic is processed by the MSRPC ALG. [PR907288]

Flow and Processing

- Periodic multicast packets such as NTP do not refresh the route, and packets are dropped intermittently. [PR869291]
- On SRX Series devices, during ARP floods of the data plane Packet Forwarding Engine, the CPU spikes might impact transit and host-bound traffic. [PR871704]
- On devices in a chassis cluster, after data plane RG1 failover, the RTSP data packet is queued, and a duplicate RTSP data packet is processed by the device; the flowd process crashes and generates core files. [PR883397]
- 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]
- On all high-end SRX Series devices, due to incorrect computation of central point IPv6 sessions, the output of the total central point sessions is incorrect for the **show security monitoring fpc number** command. This is only a display issue and does not affect actual central point sessions or the traffic passing through. [PR888890]
- When flow trace options are enabled, all the traffic that flows between logical systems through the logical-tunnel (lt-0/0/0) generates unexpected messages and floods the flow trace. These messages cannot be filtered and are difficult to read and use. [PR891689]

Interfaces and Routing

- On devices in a chassis cluster, when you execute the **clear system commit** command, it clears commit only from the local node. [PR821957]
- Multicast stream is redirected to other member links on the aggregated Ethernet interface or on the Redundant Ethernet (Reth) Link Aggregation Group (LAG) even when the link in use is disabled. [PR867529]
- On devices in a chassis cluster, when a session created as the incoming interface is a VPN secure tunnel interface (ST interface) and the outgoing interface is a logical tunnel interface (LT interface), this session is incorrectly marked as active on the secondary node. When this session expires on the secondary node, the sessions on both cluster nodes might get deleted and interrupt the traffic. [PR896299]

Intrusion Detection and Prevention (IDP)

- After the Junos image is upgraded, we recommend that you download a completely updated IDP security package and then perform the installation. Subsequent incremental updates (default) work fine. If a complete 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 SRX Series devices with IDP enabled, if IDP exempt rule is configured, a change of the IDP rule configuration (such as a change to source or destination, action, or

signature) might cause the flowd process to crash and core files are generated. [PR877865]

- When there are a large number of ASC entries (100,000 or more), and the entries are listed using CLI command, the flowd process might crash. [PR886173]

J-Web

- The ASN.1 buffered I/O functions in OpenSSL before 0.9.8v do not properly interpret integer data, which allows remote attackers to conduct buffer overflow attacks and causes a denial of service (memory corruption). J-Web is explicitly not affected by this vulnerability, because J-Web is a server and this is a client-side vulnerability. However, many other functions in Junos OS use these buffered I/O routines and can trigger fetches of untrusted X.509 certificates. Refer to PSN-2012-07-645 for more information. [PR770702]
- J-Web fails to display the member in the application set after adding it to the nested application set. [PR883391]

Network Address Translation (NAT)

- In a root system, the destination and static NAT rule cannot send system log and trap messages when the number of sessions reaches the threshold value. In a logical-system, the source, destination, and static NAT rule cannot send system log and trap messages when the number of sessions reaches the threshold value. [PR905359]

Network Management and Monitoring

- Under certain conditions, a duplicate SNMP index might be assigned to different interfaces by the kernel to the mib2d (Management Information Base II daemon). This might cause mib2d and other processes such as lacpd (LACP daemon) to crash and generate core files. [PR836823]

Platform and Infrastructure

- There is no specific CLI command to display the count of sessions allowed, denied, or terminated because of UAC enforcement. [PR733995]
- Event scripts, part of Junos OS automation infrastructure, run at high priority compared to other system-critical processes. This can result in resource contention and high CPU readings. [PR512315]
- When you enable **Change password every time the user logs out** on the active directory, you cannot change your password. [PR740869]
- On devices in a chassis cluster, after control plane Redundancy Group (RG0) failover, Occasionally, 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]

Routing Policy and Firewall Filters

- If more than 10 virtual routers (routing instances) or logical systems (LSYS) are configured on a device, Domain Name System (DNS) fails to resolve addresses. A maximum of only 10 routing instances and LSYS can be configured per DNS name server. [PR896174]

Security Group

- Multiple vulnerabilities are reported in earlier versions of OpenSSL in Junos OS. [PR853724]

System Logs

- SRX5600 and SRX5800 devices with an SRX5K-SPC-4-15-320 (NG-SPC) might generate one of the following system logs on the messages file:
  - spu_mac_get_linkstate:spu (<fpc#>/<pic#>) – phy link <link#> failed
  - spu_mac_get_linkstate: %PFE-3: (<fpc#>/<pic#>) – MAC layer link failed

  In this condition, the affected SPU cannot do any flow processing until the system is rebooted. [PR914736]

Virtual Private Network (VPN)

- File Descriptor (FD) leak occurs during the network-security-trace process when commit configuration changes are made in the **edit security ike** configuration. Eventually, the system reaches the maximum file limit, which results in a system-unmanageable condition. [PR893017]

Resolved Issues in Junos OS Release 12.1X45-D10 for High-End SRX Series Services Gateways

Application Identification

- On all high-end SRX Series devices, when AI handled Secure Socket Layer (SSL) encrypted sessions with SSLFP enabled, if the client sent a large amount of data to the server in a single transaction, core files were generated. [PR859951]

Application Layer Gateways (ALGs)

- The Microsoft remote procedure call (MSRPC) ALG feature did not include support for NDR64 parsing and DCOM interface, which is used by applications such as WMIC, IIS, and so on. [PR700049]
- The TCP proxy module used by the ALG was deficient in handling a TCP stream with large packets. [PR727649]
- On SRX3400 devices, the TCP proxy incorrectly acknowledged the SYN packet when the session was in close wait state for RSH ALG. The register suppression time (RST) packet created a session with a timeout value of 1800 when RSH ALG was enabled. [PR742317]

- Failover under heavy traffic caused H.323 ALG packets to drop and resulted in a call connection failure. [PR792051]
- On SRX5600 devices, under heavy traffic, ALGs received duplicate JMPI messages and generated core files. [PR844041]
- When firewall was enabled for ALG traffic, the system crashed when attempting to log **session-close** for ALG data (child) session. [PR845501]
- If the Microsoft Remote Procedure Call (MS-RPC) or Sun Microsystems Remote Procedure Call (SUN-RPC) ALG was disabled when there were other open MS-RPC or SUN-RPC gates, the traffic that hit the previously opened gates were dropped by ALG even after the ALG was completely disabled. This was because of an ALG behavior change that was introduced in Junos OS Release 11.4. [PR865851]
- The b attribute (pertaining to bandwidth) in a Session Initiation Protocol (SIP) Session Description Protocol (SDP) message was not carried forward after SIP ALG processed the packet. [PR875211]
- If a static route was configured and exported into OSPF, and if the static route had the same subnet as an OSPF interface address, then committing configuration changes (even unrelated to OSPF, such as a device's hostname) resulted 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 was more than 64 bytes, the devices were unstable and flowd core files were generated. [PR855386]

Chassis Cluster

- On devices in a chassis cluster with the second control link connected, when CRM was installed, and the primary node was power-cycled, the primary node took over RG-0 ownership when the primary node was rebooted. [PR679634]
- On devices in a chassis cluster, when LACP was configured on a remote switch connected to a redundant Ethernet (reth) interface, and the control link between the nodes were lost, both the nodes changed to primary. [PR733335]
- Occasionally, during RG1 failover, the priority of node 1 was stuck at zero (0). Attempts to fail over to node 1 were unsuccessful, and the cluster bounced back to node 0 because the priority of node 1 remained zero. [PR750708]
- On devices in a chassis cluster, to save the configuration on a remote file server, you had to specify the absolute/relative path for storing the file. If the path was not specified, the save operation failed. However, this issue did not affect devices operating in a stand-alone mode. [PR752363]
- After multiple node failovers, the chassis cluster LEDs were unlit even if the cluster was stable. [PR789190]
- After you rebooted the device, the interface counters on the secondary node were not accurate. [PR790807]

- On 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]
- On devices in a chassis cluster, the child link of the link aggregation group (LAG) redundant Ethernet (reth) interface flapped frequently, which corrupted the memory on the next-hop pointer and the Routing Engine generated vmcore files. [PR821833]
- On devices in a chassis cluster, massive amounts of MAC addresses were generated on the fabric link switch port. [PR833609]
- On SRX5600 and SRX5800 devices in a chassis cluster, occasionally, when a fully loaded device with next-generation Services Processing Cards was powered on, there was a delay in boot because the SPC boot ROM reached an unknown state. [PR833691]
- FPCs could not be brought online because of a communication failure with the Switch Fabric Board (SFB) component. [PR847705]
- The primary node changed to db mode and generated vmcore files when there was a change in the redundant Ethernet (reth) interface configuration that caused the deletion of the logical interface of reth. [PR850897]
- On SRX3600 devices, in certain circumstances one of the Services Processing Cards (SPCs) was stuck due to a hardware fault, and the following error message was 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) was used, traffic loss was observed when the link member failed. [PR858519]

Command-Line Interface (CLI)

- On all high-end SRX Series devices, under certain conditions, the session numbers displayed by the **show security flow session summary** and **show security flow session services-offload** commands were not consistent. The services-offload session was correct. [PR700461]
- On SRX3400 and SRX3600 devices, in standalone mode, when the device was rebooted using the **request system reboot** command, some of the interfaces were up during the reboot. This resulted in slow traffic failover in the static routing environment. [PR732733]
- An escalation of privileges occurred when the **load factory-default** command failed in the exclusive edit mode. When the command failed, the user was not subjected to any command or configuration restrictions. The escalation was limited to authenticated users with the privilege to edit the configuration. The privilege bypass was 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 generated core files, if the **X** zone did not have screens enabled and if it was part of a logical system. [PR866559]
- The **request chassis fabric plane offline/online** command did 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 did not create any server binding. [PR799829]

Flow and Processing

- On all high-end SRX Series devices, when multicast traffic was received, changes in policer, filter, or sampling configuration resulted in the generation of core files. [PR613782]
- Special crafted kernel routes that were generated based on directly connected networks (clone routes) introduced reference count inconsistencies when the link flapped, if the clone routes were rewired to a different interface. This occurred because the longest prefix match found another destination for the IP address of the flapped interface. When the parent reference count was reduced to zero, the kernel crashed when deleting the remaining child routes. [PR685941]
- On all high-end SRX Series devices, flowd core files were generated during the Layer 2 mode stress test. [PR704482]
- Occasionally, traffic sent by authenticated users (authenticated by Web authentication) was not passing through the firewall. This was because the authentication entry created in the central point was not passed to the Services Processing Unit (SPU). [PR734869]
- When a security policy was configured using J-Web, incorrect address objects were displayed. [PR747318]
- On all high-end SRX Series devices, the graceful restart mechanism did not abort even if the link to the upstream neighbor was down. This led to a higher routing protocol convergence time because the route did not fail over to an alternate path until the graceful restart timer expired. [PR751640]
- An illegal pointer address generated eventd core files. [PR784037]
- The "XLR ingress paused" condition caused traffic drops and latency processed the traffic. [PR818621]
- When a device forwarded traffic, flowd core files were generated. [PR831480]
- During configuration and maintenance of a high-end SRX Series device, occasionally the security match policies were out of sync 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]
- SYN packets were dropped if TCP ports were reused within 2 seconds. [PR836554]
- When you configured a security policy using the DNS name, traffic was dropped and the security policy did not function as expected. [PR841682]

- When you configured a wildcard address and used it in more than seven security policies, the Services Processing Unit (SPU) crashed. [PR847632]
- In the output of the **show security flow session extensive** command, if the flow session referenced a custom application with the **application-protocol ignore** option configured, the application field was incorrectly set. [PR852081]
- When you committed 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 was configured or new policies were added, or the order was changed), SPU usage increased and partial packet drops were observed. [PR854412]
- On all high-end SRX Series devices, the Services Processing Unit (SPU) level kernel crashed and generated vmcore files when processing traffic that required serialized packet processing in some application modules such as IDP, ALGs, application security, and so on. [PR855397]
- On devices enabled with SYN cookie protection, after the SYN cookie function was triggered, the SYN cookie did not send ACK to the client to update the TCP window size after a handshake with the server. When the client sent ACK with a PSH flag to the device as the third TCP ACK during the TCP three-way hand shake, the device did not recognize the ACK. This resulted in TCP connection failure. [PR859222]
- The Routing Engine control plane showed the HTTPS timeout value as 1800 seconds as opposed to the actual value of 300 seconds. [PR858621]

General Packet Radio Service (GPRS)

- On SRX1400 devices, the number of GPRS support node (GSN) entries was expanded from 6000 entries to 18,000 entries on each Services Processing Unit (SPU). [PR787028]

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]
- On devices in a chassis cluster, occasionally, when the kernel memory reached exhaustion because of dead **ifstates**, recovery of the devices caused an outage. [PR799831]

In-Service Software Upgrade (ISSU)

- The unified in-service software upgrade (ISSU) from Junos OS Release 11.4R3.6 to Junos OS Release 12.1R1.9 failed with the following error:

  ISSU not supported due to rt request TLV for target table address family

  [PR770478]

Interfaces and Routing

- On receipt of a BGP UPDATE message that contained a crafted flow specification, NLRI caused the RPD to crash. The update created an invalid inetflow prefix, which caused the RPD process to allocate memory until it reached its assigned memory limit. After trying to exceed the process memory limit, RPD crashed and restarted. The system recovered after the crash; however, a constant stream of malformed updates caused an extended outage. [PR734453]
- When you committed a configuration change, the routing protocol process (rpd) was reinitialized. When multiple reinitializations occurred while OSPF was running on the router, the periodic refresh of the OSPF LSAs stopped. If the LSAs were not refreshed, the router did not participate in the OSPF routing domain. The output of the **show ospf database router advertising-router router-id extensive | match timer** command did not include the Gen timer field. [PR744280]
- Configuring multicast addresses (inet6) on an interface resulted in the generation of RPD core (mc_ssm_add) files. [PR780751]
- On SRX1400, SRX3400, and SRX3600 devices, Tx and Rx lockup of the tsec1 (em0) controller caused em0 interface failure, and all the field-replaceable units (FRUs) went offline. [PR820210]
- Crafted Generic Routing Encapsulation (GRE) packets received on a multicast tunnel (mt- or gr-) interface that were allowed to reach the Routing Engine caused the Junos OS kernel to crash. [PR821503]
- High-priority Routing Protocol Daemon (RPD) tasks were scheduled more frequently, halting the progress of low-priority RPD tasks. Low-priority tasks could not be completed until all the scheduled high-priority tasks were completed. [PR836197]
- The Junos OS kernel crashed when a specifically crafted TCP packet was received by the Routing Engine on a listening TCP port. TCP traffic traversing the router did not trigger this crash. The TCP packets destined to the router that successfully reached the Routing Engine through existing edge and control plane filtering, caused the crash. This issue could be triggered by both IPv4 and IPv6 TCP packets destined to the Routing Engine. [PR839412]
- Multicast stream was not redirected to other member links on the aggregated Ethernet interface even when the link in use was disabled. [PR867529]

Intrusion Detection and Prevention (IDP)

- On devices in a chassis cluster, application identification information was not synchronized. [PR682090]
- In Junos OS Release 11.4, if Intrusion Detection and Prevention (IDP) was configured, the output of the command **show security idp policy-commit-status** incorrectly displayed the message **Active policy not configured** even when the active policy was configured. [PR741736]
- On XLP platforms, setting the **max-sessions** option in an application identification configuration did not impact the attack traffic. [PR809384]
- On devices configured with IDP, the serialization bit was cleared by IDP, and the traffic processed by IDP that required serialized packet processing was dropped, if the session was idle for more than 5 minutes before data transmission resumed. [PR810247]
- 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]
- 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]
- When the **no-reset-on-policy** option was set and there were two active policies in a dataplane, and only one session referred to the older policy; flowd core files were generated, if application identification indicated a change in application (from the default one, for example, FTP running on Telnet port), because of policy re-lookup. [PR880408]

IPv6

- Certain IPv6 packets matching an IPv6 egress filter with a discard or reject term applied on the lo0 interface triggered a buffer leak, which caused MBUF exhaustion and a kernel crash. The rate of the leak was proportional to the number of these specific IPv6 packets hitting the discard term, reject term, or both.. This issue only affected IPv6 egress filters with a discard or reject action. [PR816666]

J-Web

- On all high-end SRX Series devices, when using the CLI you could configure only an AppQoS rule set without configuring any other diff-services. However, in J-Web, you could configure at least one diff-service for a new AppQoS rule set configuration. [PR686462]
- The J-Web interface was vulnerable to HTML cross-site scripting attacks, also called XST or cross-site tracing. [PR752398]
- In J-Web, when you tried to commit a logical systems configuration, the following message was displayed even if there were no configuration changes:

  You have pending changes from previous commit

[PR812896]

- J-Web did not support XLP-based cards. [PR826605]
- In J-Web, after you upgraded a device to Junos OS Release 11.4 R4 or later, downloading configuration files using Internet Explorer failed. [PR830482]
- In J-Web, the Chassis View could not be dragged under the Dashboard tab. [PR842034]
- You could not edit the source NAT configuration using J-Web. [PR850506]
- In J-Web, if the policy name was "0", the penultimate-hop popping (PHP) function treated it as empty, and traffic log output could not be viewed. [PR853093]

Logical Systems

- On SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices, the BFD session on routing protocols for LSYS was not working. [PR671444]
- In a logical system, you could not use snmpwalk for Simple Network Management Protocol (SNMP) polling. [PR791859]
- When you performed a commit full on a lt-0/0/0 interface configuration, the commit failed. Subsequent commits also failed. [PR845837]

Network Address Translation (NAT)

- On all high-end SRX Series devices, 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]
- On devices in a chassis cluster Z mode, flowd core files were generated while handling mass persistent mass traffic. [PR834821]
- On SRX Series devices with Protocol-Independent Multicast (PIM) is enabled, certain PIM packets subject to Network Address Translation (NAT) might causes the flow process (flowd) to crash. [PR842253]

System Logs

- Occasionally, the following SPU message was displayed, causing the kernel system log buffer to overflow:

  Nexthop XXXX on ifl XXX. Ignoring

  [PR726580]

- In certain configurations, the following message was displayed in the logs: **PFEMAN: Sent Resync request to Master**. [PR802355]
- On SRX5800 devices, when configuration messages exceeded the interprocess communication message (IPC) maximum transmission unit (MTU), occasionally the following error message was displayed:

  ipc_msg_write: %PFE-3: IPC message type: 27, subtype: 2 exceeds MTU, mtu 3216, length 3504

[PR612757]

- New system log messages were added for the following PKI Daemon failures:
  - Missing basic constraints in a CA certificate
  - Invalid CA=TRUE flag in CA certificate

  [PR831995]

Upgrade and Downgrade

- When you upgraded a 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 was not accepted. [PR806750]
- 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]

Virtual Private Network (VPN)

- When a firewall filter was configured on the lo0 interface, the firewall log displayed the wrong address and port information for the IKE packets. [PR695288]
- Occasionally, devices configured with policy-based IPsec VPN did not allow traffic to the protected resources. [PR718057]
- Manual (static) next-hop tunnel binding (NHTB) with DEP was not supported. [PR725462]
- 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]
- On a high-scale RIP deployment, frequent flap of tunnels led to missing a small number of RIP routes. These routes eventually recovered. [PR802078]
- When traffic was fragmented over an IPsec tunnel, the first fragment was the smallest fragment. This was done because the first fragment had to be copied into a separate memory buffer and a smaller first fragment resulted in faster copying and a faster fragmentation process. [PR807216]
- If all the IPsec tunnels in a configuration used the pre defined IKE proposal set, and no custom proposal was present in the configuration, the IPsec tunnels flapped when configuration changes were committed under the IKE or IPsec hierarchy. [PR812433]
- On all high-end SRX Series devices, if IPsec VPN was configured, vmcore files were generated on Services Processing Units (SPUs). [PR824931]
- 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]

- On devices in a chassis cluster, some VPN system log messages were not generated. [PR837983]
- Dynamic VPN on Microsoft Windows 7, 64-bit operating system (OS) did not work in some environments. [PR842607]
- When a certificate revocation list (CRL) file was loaded using the **request security pki crl load ca-profile *ca-profile* filename *filename*** command, CRL checking worked as expected until a PKID Daemon restarted. After the PKID Daemon restarted, the CRL file had to be reloaded manually for CRL checking to continue working. [PR845459]
- When the data size was smaller than 128 bytes, certificate revocation list (CRL) installation using the Lightweight Directory Access Protocol (LDAP) server failed. [PR847868]
- When IPsec VPN Internet Key Exchange (IKE) traffic passed through the device, memory leaks were observed and the VPN connection could not be established. [PR857013]
- Automatic enrollment of PKI certificates did not work as expected. [PR860923]
- When an IPsec tunnel was established from a routing instance, the enable VPN session affinity (SA) feature caused VPN traffic drop in the anchor Services Processing Unit (SPU). If the clear-text session was located in a SPU that is different from the anchor SPU, the routing instance ID was lost when the packet was forwarded from the central point to the anchor SPU in the first path processing, and caused the routing lookup to occur in the wrong routing table (inet.0 table). [PR866220]

Related Documentation

- New and Changed Features in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 89
- Known Behavior in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 116
- Documentation Updates for Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 148

Documentation Updates for Junos OS Release 12.1X45 for High-End SRX Series Services Gateways

This section lists the errata and changes in Junos OS Release 12.1X45 documentation.

Documentation Updates for the Junos OS Software Documentation

This section lists improvements and outstanding issues with the software documentation.

Security Policy Applications Feature Guide for Security Devices

- On the Overview tab, under IP-Related Predefined Policy Applications, in the topic entitled “Understanding IP-Related Predefined Policy Applications,” the Port column for both TCP-ANY and UDP-ANY should indicate 0-65535. The lead-in sentence should read, “Each entry includes the port and a description of the application.” TCP-ANY means any application that is using TCP, so there is no default port for it. The same is true for UDP-ANY.

- In the topic entitled “Understanding Miscellaneous Predefined Policy Applications,” table “Predefined Miscellaneous Applications” is incomplete. Under the RADIUS row, add a new row:

Table 15: Predefined Miscellaneous Applications

Application	Port	Description
RADIUS Accounting	1813	Enables the collecting of statistical data about users logging in to or out from a LAN and sending the data to a RADIUS Accounting server.

In table “Predefined Miscellaneous Applications” replace the IPsec-NAT row with the following:

Table 16: Predefined Miscellaneous Applications

Application	Port	Description
IKE	500	Internet Key Exchange is the protocol that sets up a security association in the IPsec protocol suite.
IKE-NAT	4500	Helps to perform Layer 3 NAT for S2C IKE traffic.

Table 17: Predefined Miscellaneous Applications

Application	Port	Description
VoIP	389	Internet Locator Service (ILS)
	522	User Location Service (ULS)
	1503	T.120 Data sharing
	1719	H.225 RAS message
	1720	Q.931 Call Setup
	1731	Audio Call Control
	5060	SIP protocol

Certificates and Public Key Infrastructure Feature Guide for Security Devices

- In "Example: Using SCEP to Automatically Renew a Local Certificate," the overview states that you can configure when the device is to send out the certificate renewal request as the number of days and minutes before the certificate's expiration date. This is incorrect. The trigger for the device to send out a certificate renewal request is a specified percentage of the certificate's lifetime that remains before the certificate expires. For example, if the renewal request is to be sent when the certificate's remaining lifetime is 10%, then configure 10 for the reenrollment trigger.

Junos OS for SRX Series Documentation

The Junos OS for SRX Series technical documentation set has been expanded, restructured, and retitled in this release to make it more comprehensive, easy-to-use, and intuitive. Highlights:

- (New) The Complete Software Guide consolidates all of the release-specific content that applies to Junos OS for SRX Series devices (except release notes) into a three volume set of PDFs that you can download and view offline. The first volume contains getting started and administration information; the second contains feature information; the third contains developer information. You can find the PDFs in the Downloads box on the right side of the *Junos OS for SRX Series Services Gateways, Release 12.1X45* index page.
- (New) The *Getting Started Guide for Branch SRX Series* describes how to get up and running with branch SRX Series devices.
- (Expanded) The *Junos OS Monitoring and Troubleshooting Library for Security Devices* contains significantly more content to help network and security managers keep their SRX Series devices running smoothly in their production environments.
- (Expanded) The *Junos OS for SRX Series Services Gateways, Release 12.1X45* index page has been expanded to serve as a "one stop shop" for all of your Junos OS for SRX Series technical documentation needs.

For more information about technical documentation improvements in this release, see Getting the Content You Need. To see a detailed mapping of how 12.1X44 Junos OS for SRX Series content maps to the new 12.1X45 guides, see Where's My Content Now? Junos OS Release 12.1X45.

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.

Network Address Translation (NAT)

The command **show security nat source persistent-nat-table** under **Network Address Translation > Administration > Source NAT Operational Commands** has the following errors:

- The command is missing the **summary** option:**summary**—Display persistent NAT bindings summary.
- The command contains incomplete sample output —The corrected sample output is as follows:

show security nat source persistent–nat–table internal-ip internal-port

```
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
```

show security nat source persistent–nat–table all

```
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
```

show security nat source persistent-nat-table summary

```
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
```

Various Guides

- Some Junos OS 12.1X45 user, reference, and configuration guides and topics still include references to discontinued guides such as the *Feature Support Reference for SRX Series and J Series Devices* and the *Junos OS CLI Reference*. Please disregard those erroneous references. For more information about documentation changes implemented in 12.1X45 and which guides have been discontinued or moved, please see Where's My Content Now? Junos OS Release 12.1X45.

Related Documentation

- New and Changed Features in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 89
- Known Behavior in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 116
- Known Issues in Junos OS Release 12.1X45-D15 for High-End SRX Series Services Gateways on page 133
- Resolved Issues in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 136

Migration, Upgrade, and Downgrade Instructions for Junos OS Release 12.1X45 for High-End SRX Series Services Gateways

This section includes the following topics:

- Upgrading and Downgrading among Junos OS Releases on page 152
- Upgrading an AppSecure Device on page 154
- Upgrade and Downgrade Scripts for Address Book Configuration on page 154
- Upgrade Policy for Junos OS Extended End-Of-Life Releases on page 157
- Hardware Requirements for Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 157

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 or later, 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 156).

- About Upgrade and Downgrade Scripts on page 155
- Running Upgrade and Downgrade Scripts on page 156

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.

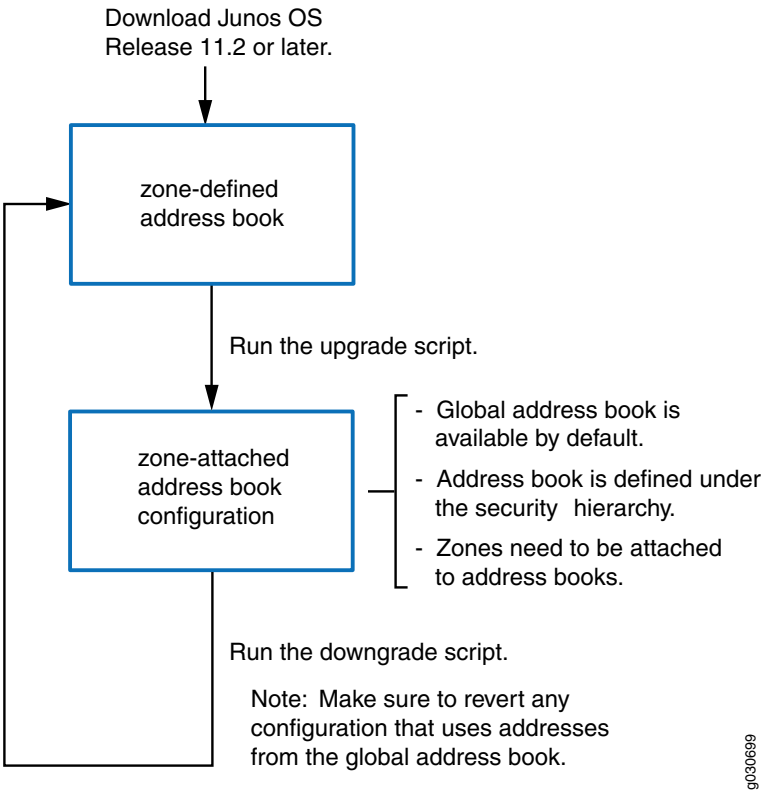
  After upgrading to the zone-attached address book configuration:

  - 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 2: 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 12.1X45 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 and Changed Features in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 89
- Documentation Updates for Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 148
- Changes in Behavior and Syntax in Junos OS Release 12.1X45 for High-End SRX Series Services Gateways on page 105

Junos OS Release Notes for LN Series Routers

Powered by Junos OS, Juniper Networks LN Series Routers provide high-performance network routing, next generation firewall, and unified threat management capabilities in a single platform. The LN Series includes the LN1000 and LN2600 devices.

- New and Changed Features in Junos OS Release 12.1X45-D15 for LN Series Routers on page 158
- Known Behavior in Junos OS Release 12.1X45 for LN Series Routers on page 159

New and Changed Features in Junos OS Release 12.1X45-D15 for LN Series Routers

The following feature has been added to Junos OS Release 12.1X45-D15.

- Hardware Features on page 158

Hardware Features

LN2600 Rugged Security Router

- **LN2600 Rugged Security Router**—This release introduces the Juniper Networks LN2600 Rugged Security Router to the LN Series Routers. The LN2600 provides the advanced routing and security technology required to secure remote locations, including perimeter security, content security, application visibility, tracking and policy enforcement, role-based access control, and network-wide threat visibility and control. The LN2600 uses Junos OS software for stateful firewalls, intrusion detection and prevention, and IPsec encryption to protect remote locations from unauthorized access, and to protect mission critical control applications from remote locations to a centralized control center. It meets the requirements of ingress protection rating IP64 for dust-proof and splash-proof environments. The conduction cooled, fanless LN2600 design can operate in extreme temperature ranges. Dual boot root partitions and a Non-Volatile Memory Read-Only (NVMRO) option enable reliable operations and protection against modifications or loss in remote locations. The LN2600 router can be installed as a rack-mountable or wall-mountable chassis. The LN2600 Rugged Security Router can be used effectively in energy and utility companies, mission critical infrastructure companies, public sector safety organizations, and military and defense establishments.

Related Documentation

- Known Behavior in Junos OS Release 12.1X45 for LN Series Routers on page 159

Known Behavior in Junos OS Release 12.1X45 for LN Series Routers

LN Series

- The LN1000-V and LN2600 do not turn off the laser on optical SFPs when the interface is disabled.
- You can install a new Junos OS version using the software.tgz file on a USB storage device or the system flash memory by using the CLI. You can also boot from a Junos OS image on a USB storage device if the image was created using the **request system snapshot** command.

Related Documentation

- New and Changed Features in Junos OS Release 12.1X45-D15 for LN Series Routers on page 158

Product Compatibility

- Hardware Compatibility on page 160

Hardware Compatibility

To obtain information about the components that are supported on the device, and special compatibility guidelines with the release, see the SRX Series Hardware Guide.

To determine the features supported on SRX Series devices in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at:

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

Third-Party Components

This product includes third-party components. To obtain a complete list of third-party components, see Copyright and Trademark Information.

Finding More Information

For the latest, most complete information about known and resolved issues with the Junos OS, see the Juniper Networks Problem Report Search application at:

http://prsearch.juniper.net.

Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos OS feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at:

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

Juniper Networks Content Explorer is a Web-based application that helps you explore Juniper Networks technical documentation by product, task, and software release, and download documentation in PDF format. Find Content Explorer at:

http://www.juniper.net/techpubs/content-applications/content-explorer/.

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

21 October 2013—Revision 4, Junos OS 12.1X45-D15 – High End SRX Series, Branch SRX Series, J Series, and LN Series.