Release Notes: Junos® OS Release 15.1X49-D50 for the SRX Series

Release 15.1X49-D50
12 July 2018
Revision 11

Contents

Introduction

Junos OS runs on the following Juniper Networks® hardware: ACX Series, EX Series, M Series, MX Series, PTX Series, QFabric, QFX Series, SRX Series, and T Series.

These release notes accompany Junos OS Release 15.1X49-D50 for the SRX Series. They describe new and changed features, known behavior, and known and resolved problems in the hardware and software.

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

NOTE: Junos OS Release 15.1X49-D50 supports SRX300, SRX320, SRX340, SRX345, SRX550 High Memory (SRX550M), SRX1500, vSRX, and SRX5400, SRX5600, and SRX5800 devices with host subsystems composed of either an SRX5K-RE-1800X4 (RE2) with an SRX5K-SCBE (SCB2), or an SRX5K-RE-1800X4 (RE2) with an SRX5K-SCB3 (SCB3).

For more details about SRX Series high-end hardware and software compatibility, please see https://kb.juniper.net/KB30446. If you have any questions concerning this notification, please contact the Juniper Networks Technical Assistance Center (JTAC).

New and Changed Features

This section describes the new features and enhancements to existing features in Junos OS Release 15.1X49-D50 for the SRX Series devices.

Release 15.1X49-D50 Hardware Features

Wireless WAN

- **CBA850 3G/4G/LTE Wireless WAN Bridge**-Starting with Junos Release 15.1X49-D50, the SRX300 line of services gateways and the SRX550HM Services Gateway support the CBA850 3G/4G/LTE wireless WAN bridge. The CBA850 can be deployed as a primary WAN or as a backup WAN to the primary wired network for the services gateways.

  [See CBA850 3G/4G/LTE Wireless WAN Bridge Overview.]

Release 15.1X49-D50 Software Features

Authentication and Access Control

- **Integrated ClearPass on SRX300, SRX320, SRX340, SRX345, SRX550 High Memory (HM), SRX1500, SRX5400, SRX5600, and SRX5800 devices, and vSRX**—Junos OS Release 15.1X49-D50 supports the integrated ClearPass authentication and enforcement feature. Integrated ClearPass authentication and enforcement enables SRX Series devices and Aruba ClearPass to collaborate in protecting your company's resources by enforcing security at the user identity level, not the IP address of a user's device. Not only can you configure security policies that apply to a user by username or group regardless of the device used, you can also configure a policy that specifies a group of users and a device type. Focusing security policies on user identity gives you exceptional control. Additionally, the SRX Series device provides ClearPass with threat and attack logs associated with users to inform your security enforcement at the ClearPass end. ClearPass can authenticate users across wired, wireless, and VPN infrastructures, and as the authentication source, post that information to the SRX Series device.

- **Individual user query on SRX300, SRX320, SRX340, SRX345, SRX550 High Memory (HM), SRX1500, SRX5400, SRX5600, and SRX5800 devices, and vSRX**—Junos OS Release 15.1X49-D50 supports the integrated ClearPass authentication and enforcement feature that includes the user query function. User query allows you to configure supported SRX Series devices to automatically query the Aruba ClearPass server for individual user authentication information when ClearPass does not post that information to it.

  [See Upgrading the VDSL PIC Firmware.Understanding the Integrated ClearPass Authentication and Enforcement User Query Function.]

- **Threat Detection and Notification to ClearPass on SRX300, SRX320, SRX340, SRX345, SRX550 High Memory (HM), SRX1500, SRX5400, SRX5600, and SRX5800 devices, and vSRX**—Junos OS Release 15.1X49-D50 supports the integrated ClearPass authentication and enforcement feature that includes the threat detection and notification function. This function allows the SRX Series device to filter detected events specifically for threats and attacks and send logs about them to the ClearPass Policy Manager.

  [See Understanding How the Integrated ClearPass Feature Detects Threats and Attacks and Notifies the CPPM.]

- **User and Role Enforcement on SRX300, SRX320, SRX340, SRX345, SRX550 High Memory (HM), SRX1500, SRX5400, SRX5600, and SRX5800 devices, and vSRX**—Junos OS Release 15.1X49-D50 supports the integrated ClearPass authentication and enforcement feature that includes the user role and enforcement function. For this feature, the SRX Series device relies on Aruba ClearPass as its authentication source. With the user authentication information provided by ClearPass, you can configure security policies and allow the SRX Series device to enforce them based on user identity (source identity) rather than relying on the IP address of a user's device. You can also use group, or role, identities in security policies.

  [See Understanding Enforcement of ClearPass User and Group Authentication on the SRX Series Devices.]

- **Web API and Message Dispatcher on the SRX300, SRX320, SRX340, SRX345, SRX550 High Memory (HM), SRX1500, SRX5400, SRX5600, and SRX5800 devices, and vSRX.**—Junos OS Release 15.1X49-D50 supports the integrated ClearPass authentication and enforcement feature which includes the Web API function. This function allows Aruba ClearPass to initiate a connection with the SRX Series device to provide it with user authentication and identity information.

  [See Understanding How ClearPass Initiates a Session and Communicates User Authentication Information to the SRX Series Device Using the Web API.]

- **Expanded error detection and management on the SRX5000 line of devices**—Starting with Junos OS Release 15.1X49-D50, this feature provides enhanced error detection and management for the Junos OS Routing Engine version 2 and microkernel. These enhancements prevent silent errors from degrading system performance and adversely affecting traffic. The feature is supported on IOC2, IOC3, and SPC2. For each error type, you can specify the actions to take when an error is detected and a specified threshold is reached.

  [See Error Handling Extensions.]

Chassis Cluster

- **In-Band Cluster Upgrade for SRX1500 devices** —Starting in Junos OS Release 15.1X49-D50, this feature is supported on SRX1500 Services Gateways.

  Devices in a chassis cluster can be upgraded with a minimal service disruption using in-band cluster upgrade (ICU). The chassis cluster ICU feature allows both devices in a cluster to be upgraded from supported Junos OS versions using a single command.

  You can enable this feature by executing the **request system software in-service-upgrade *image_name*** command on the primary node. This command upgrades the Junos OS and reboots both the secondary node and the primary node in turn.

  During the ICU process, traffic outage is minimal; however, cold synchronization is provided between the two nodes.

  [See Upgrading Devices in a Chassis Cluster Using ICU.]

Interfaces

- **G.993.5 Vectoring support for VDSL modules on SRX Series devices**— Starting with Junos OS Release 15.1X49-D50, firmware version, v2.16.0, is available for SRX-MP-1VDSL-R to support VDSL vectoring. Vectoring on VDSL reduces crosstalk and increases network bandwidth.

  [See Upgrading the VDSL PIC Firmware.]

Layer 2 Features

- **Support for enhanced Layer 2 transparent bridge mode and switching mode for the SRX1500 device** —Starting with Junos OS Release 15.1X49-D50, enhanced Layer 2 transparent bridge mode and switching mode features are supported on the SRX1500 device.

  Use the **set protocols l2-learning global-mode (transparent-bridge | switching)** command to switch between the Layer 2 transparent bridge mode and switching mode. After switching the mode, you must reboot the device for the configuration to take effect.

  The Layer 2 protocol supported in switching mode is LACP.

  NOTE:
  - LACP is not supported in transparent bridge mode.

  You can now configure Layer 2 mode on redundant Ethernet interfaces. Use the following commands to define a redundant Ethernet interface:

  - **set interfaces *interface-name* ether-options redundant-parent *reth-interface-name***
  - **set interfaces *reth-interface-name* redundant-ether-options redundancy-group *number***

[See Ethernet Switching and Layer 2 Transparent Mode Overview.]

Sky Advanced Threat Prevention

- **Support for SRX5400, SRX5600, and SRX5800 devices**—Junos OS Release 15.1X49-D50 and later releases support Sky Advanced Threat Prevention running on SRX5400, SRX5600 and SRX5800 devices, in addition to existing support for SRX1500 devices.

  [See the Sky Advanced Threat Prevention Supported Platforms Guide.]

User Access and Authentication

- **Harden Shared Secrets in Junos**—Starting with Junos OS Release 15.X49-D50, new CLI commands are introduced to configure a system master password and request to decrypt an encrypted secret, allowing for hardening of shared secrets, such as pre-shared keys and RADIUS passwords.

  Having a master password allows devices to encrypt passwords in such a way that only devices running Junos OS that have knowledge of the master password can decrypt the encrypted passwords. The following new CLI commands are available:

  · **request system decrypt password**

  · **set system master-password**

  [See Hardening Shared Secrets in Junos OS.]

VPNs

- **Policy-based VPNs supported on SRX300, SRX320, SRX340, SRX345, SRX1500 devices, and vSRX instances**–Starting in Release 15.1X49-D50, policy-based VPNs are supported on SRX300, SRX320, SRX340, SRX345, SRX1500 devices, and vSRX instances, in addition to SRX5400, SRX5600, and SRX5800 devices.

  [See Understanding Policy-Based IPsec VPNs.]

Related Documentation

- Known Behavior on page 17
- Known Issues on page 21
- Resolved Issues on page 26
- Migration, Upgrade, and Downgrade Instructions on page 30

Changes in Behavior and Syntax

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands from Junos OS Release 15.1X49-D50.

Application Identification

- When you upgrade or downgrade an application signature package, an error message is displayed if there is any mismatch of application IDs (unique ID number of an application signature) between the protocol bundles and the applications associated with the IDs. This scenario occurs when AppFW and AppQoS rules are configured. An example message follows:

  ```
  Please resolve following references and try it again [edit class-of-service
  application-traffic-control rule-sets RS8 rule 1 match application junos:CCPROXY]
  ```

  As a workaround, disable AppFW and AppQoS rules before upgrading or downgrading an application signature package. You can reenable AppFW and AppQoS rules once the upgrade or downgrade procedure is complete.

Application Layer Gateway

- In Junos OS Release 15.1X49-D40 and earlier, on all SRX Series devices, the DNS ALG only recorded and forwarded the DNS packets for which the packet length exceeded the threshold value (range from 512 through 8192).

  Starting in Junos OS Release 15.1X49-D50, the DNS ALG can be configured to drop the oversized DNS packets if the length exceeds the threshold value. To enable this, you need to configure the new CLI command **set security alg dns oversize-message-drop**. If the command **set security alg dns oversize-message-drop** is not configured, the DNS ALG will only record and forward the oversized DNS packets.

AppSecure

- On SRX Series devices, the following CLI statements are deprecated—rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration:

  edit services ssl termination profile *profile-name* protocol-version ssl3

  edit services ssl initiation profile *profile-name* protocol-version ssl3

- On SRX300, SRX320, SRX340, and SRX345 devices, AppSecure is part of Juniper Networks Secure Edge software or IPS subscription license. A separate license key is not required on your device to download and install the AppID signature database updates, or to use other AppSecure features such as AppFW, AppQoS, and AppTrack.

Authentication, Authorization and Accounting (AAA)

- On SRX340 and SRX345 devices, the factory-default configuration has a generic HTTP configuration. To use **ge** and **fxp0** ports as management ports, you must use the **set system services web-management http** command. The Web management HTTP and HTTPS interfaces are changed to fxp0.0 and from **ge-0/0/1.0** through **ge-0/0/7.0**.

Chassis Cluster

- When an SRX Series device is operating in chassis cluster mode and encounters any IA-chip access issue in an SPC or an I/O Card (IOC), a minor FPC alarm will be activated to trigger redundancy group failover.
- Starting in Junos OS Release 15.1X49-D20, for all SRX Series devices, reth interface supports proxy ARP.

Installation and Upgrade

- Factory-default configuration—Starting with Junos OS Release 15.1X49-D50, configuring autoinstallation using USB and Layer 2 Ethernet switching is not supported on the same interface for SRX300, SRX320, SRX340, SRX345, SRX550HM, and SRX1500 devices and vSRX instances. The **system autoinstallation interfaces <interface names>** command and the **set interface <interface names> unit 0 family ethernet-switching** command cannot be configured on the same interface.

  In Junos OS Release 15.1X49-D40 and earlier, configuring autoinstallation using USB and Layer Ethernet switching was supported on the same interface. However, the command caused the interface-control (dcd) process to exit, resulting in improper installation of the interface-related configurations.

- Starting in Junos OS Release 15.1X49-D50, the **request system scripts add** *package-name* **no-copy | unlink** command is updated to include the following options for installing AI Script install packages on SRX Series devices in a chassis cluster:

  - **master**- Install AI script packages on the primary node.
  - **backup**- Install AI script packages on the secondary node.

  This enhancement eliminates the need for separate AI script installations on the primary node and the secondary node.

Interfaces and Routing

- In Junos OS Release 15.1X49-D40 and earlier, on all SRX Series devices, GARP packets were sent out only for one IP address per IFL during RG1+ failover.

  Starting with Junos OS Release 15.1X49-D50, the IP address count per IFL during RG1+ failover has been enhanced to support up to eight IP addresses when sending GARP packets.

- **GRE keepalive time feature for SRX Series devices**—Starting in Junos OS Release 15.1X49-D30, the GRE keepalive time feature is supported on the GRE tunnel interface. You can configure the keepalives on a GRE tunnel interface using the **keepalive-time**

and **hold-time** commands at the [**edit protocols oam gre-tunnel interface interface-name**] hierarchy level.

Intrusion Detection and Prevention (IDP)

- On all SRX Series devices, the following new CLI options are introduced:
  - The **checksum-validate** option has been added to the following hierarchies:

    [**edit security idp custom-attack ipv4_cust attack-type signature protocol ipv4**]

    [**edit security idp custom-attack tcp_cust attack-type signature protocol tcp**]

    [**edit security idp custom-attack udp_cust attack-type signature protocol udp**]

    [**edit security idp custom-attack icmp_cust attack-type signature protocol icmp**]

    [**edit security idp custom-attack icmpv6_cust attack-type signature protocol icmpv6**]

    To configure this option, use the following commands:

    set security idp custom-attack ipv4_cust attack-type signature protocol ipv4 checksum-validate

    set security idp custom-attack tcp_cust attack-type signature protocol tcp checksum-validate

    set security idp custom-attack udp_cust attack-type signature protocol udp checksum-validate

    set security idp custom-attack icmp_cust attack-type signature protocol icmp checksum-validate

    set security idp custom-attack icmpv6_cust attack-type signature protocol icmpv6 checksum-validate

  - The new **checksum-validate** option allows you to specify a particular checksum to match. The following example shows a command to validate the user-specified checksum of match equal value 0x20:

    ```
    set security idp custom-attack ipv4_cust attack-type signature protocol ipv4
     checksum-validate match equal value 0x20
    ```

  - The **routing-header** option and the **destination-option** option have been added to the [**edit security idp custom-attack ipv6_cust attack-type signature protocol ipv6 extension-header**] hierarchy. The **routing-header** option inspects the **routing-header** type field and reports a custom attack if a match with the specified value is found. The **destination-option** option inspects the header option type of **home-address** and **option-type** field in the extension header and reports a custom attack if a match is found.

    To configure these options, use the following commands:

    set security idp custom-attack ipv6_cust attack-type signature protocol ipv6 extension-header routing-header

    set security idp custom-attack ipv6_cust attack-type signature protocol ipv6 extension-header destination-option

NOTE: For extension header of subtype routing-header, all type of inspections are supported as per RFC.

For extension header of subtype destination-option, the home-address and the option-type field type of inspections are supported.

- On all SRX Series devices, the following new CLI commands are introduced:
  - The new **ihl** option at the [**edit security idp custom-attack ipv4_custom attack-type signature protocol ipv4**] hierarchy level is used to inspect the length of the IPv4 header. To configure the **ihl** option, use the following command:

    ```
    set security idp custom-attack ipv4_custom attack-type signature protocol
    ipv4 ihl
    ```

  - The new **reserved** option at the [**edit security idp custom-attack tcp_custom attack-type signature protocol tcp**] hierarchy level is used to inspect the three reserved bits in the TCP header. To configure the **reserved** option, use the following command:

    ```
    set security idp custom-attack tcp_custom attack-type signature protocol tcp
     reserved
    ```

- On SRX Series devices, starting for Junos OS Release 15.1X49-D50, a new CLI option **drop-on-syn-in-window** is introduced for controlling the IDP behavior when SYN is seen in the TCP window. To enable this option use the **set security idp sensor-configuration re-assembler drop-on-syn-in-window** command.

  When the **sensor-configuration** option is:

  - Disabled (Not set (default))—Drops the packet and ignore current session.
  - Enabled (Set)—Drops the packet after IDS processing is complete.

Layer 2 Features

- Starting in Junos OS Release 15.1X49-D50, the factory-default configuration of the SRX300, SRX320, SRX340, and SRX345 devices is switching mode. When these devices are loaded or reset with the factory-default configuration, they start up in switching mode.
- **Enhanced Layer 2 CLI**—Starting with Junos OS Release 15.1X49-D10, enhanced Layer 2 CLI configurations are supported on SRX5400, SRX5600, and SRX5800 devices. Legacy Layer 2 transparent mode configuration statements and operational commands are not supported. If you enter legacy configurations in the CLI, the system displays an error and fails to commit the configurations.

  For example, the following configurations are no longer supported:

  - **set bridge-domain**
  - **set interfaces ge-1/0/0 unit 0 family bridge**
  - **set vlans vlan-1 routing-interface**

Use the SRX L2 Conversion Tool to convert Layer 2 CLI configurations to enhanced Layer 2 CLI configurations.

The SRX L2 Conversion Tool is available at https://www.juniper.net/support/downloads/?p=srx5400#sw .

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

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

MPLS

- Starting in Junos OS Release 15.1X49-D50, the **vrf-table-label** statement allows mapping of the inner label to a specific Virtual Routing and Forwarding (VRF). This mapping allows examination of the encapsulated IP header at an egress VPN router. For SRX Series devices, the **vrf-table-label** statement is currently supported only on physical interfaces. As a workaround, deactivate **vrf-table-label** or use physical interfaces.

Multicast

- Starting with Junos OS Release 15.1X49-D40, for all SRX Series devices, configuration of patterns in standard PCRE format is supported in the custom attacks.

NAT

- In Junos OS Release 15.1X49-D45 and earlier, on SRX Series devices and in vSRX instances, the system log messages in IDP attack logs contained only IPv4-based NAT address fields.

  Starting in Junos OS Release 15.1X49-D50, the system log messages in IDP attack logs contain both IPv4-based and IPv6-based NAT address fields.

- Source NAT pool port configuration options—Starting with Junos OS Release 15.1X49-D40, the **port-overloading-factor** option and the **port-range** option at the [edit security nat source pool *source-pool-name* port] hierarchy level can be configured together. Prior to Release 15.1X49-D40, the options would overwrite each other.

  [See port (Security Source NAT).]

Network Time Protocol

- Starting in Junos OS Release 15.1X49-D10, on all SRX Series devices, when the NTP client or server is enabled in the [**edit system ntp**] hierarchy, the REQ_MON_GETLIST and REQ_MON_GETLIST_1 control messages supported by the monlist feature within the NTP client or server might allow remote attackers, causing a denial of service. To identify the attack, apply a firewall filter and configure the router's loopback address to allow only trusted addresses and networks.

Public Key Infrastructure

- The **request security pki local-certificate enroll** command now includes the **cmpv2** and **scep** keywords for CMPv2 and SCEP certificate enrollment. Each keyword has configurable options. In previous releases, SCEP enrollment parameters were entered after the **enroll** keyword. Starting with this release, SCEP enrollment parameters should be entered after the **scep** keyword. In a future release, SCEP enrollment parameters after the **enroll** keyword will be deprecated.

  The **auto-re-enrollment** configuration statement at the [**edit security pki**] hierarchy level now includes the **cmpv2** and **scep** keywords for automatic reenrollment of local certificates using CMPv2 or SCEP. Each keyword has configurable options. In previous releases, SCEP enrollment parameters were entered after the **set security pki auto-re-enrollment certificate-id** *certificate-id-name* statement. Starting with this release, SCEP reenrollment parameters should be entered after the **scep** keyword. In a future release, SCEP enrollment parameters after the **set security pki auto-re-enrollment certificate-id** *certificate-id-name* statement will be deprecated.

Screen

- In Junos OS releases earlier than Junos OS Release 15.1X49-D20, the firewall generates a log for every packet that exceeds the source-ip-based or destination-ip-based threshold and triggers the source or destination session limit. This can lead to a flood of logs if a large number of packets is received every second after the threshold has been reached. For example, if the source or destination session limit has been reached and 100 additional packets arrive in the next second, 100 log messages are sent to the system log server.

  Starting in Junos OS Release 15.1X49-D20, the firewall generates only one log message every second irrespective of the number of packets that trigger the source or destination session limit.

  This behavior also applies to flood protection screens with TCP-Synflood-src-based, TCP-Synflood-dst-based, and UDP flood protection.

System Logs

- In Junos OS Release 15.1X49-D30 and earlier, the severity parameter for RT_SRC_NAT_PBA messages was “debug”.

  Starting in Junos OS Release 15.1X49-D40, the severity parameter has changed. The RT_SRC_NAT_PBA messages are now fixed with severity as “info”.

  The following example shows RT_SRC_NAT_PBA messages before Junos OS Release 15.1X49-D40:

  16:32:43.760393 In IP (tos 0x0, ttl 254, id 16957, offset 0, flags [none], proto: UDP (17), length: 218) 192.0.2.4.syslog > 192.0.2.2.syslog: SYSLOG, length: 190 Facility user (1), Severity debug (7)

  Feb 5 16:32:49 RT_NAT: RT_SRC_NAT_PBA_ALLOC: Subscriber 192.0.2.2 used/maximum [1/32] blocks, allocates port block [27200-27263] from 198.51.100.3 in source pool src-nat-pool-1 lsys_id: 0\012

  The following example shows RT_SRC_NAT_PBA messages in Junos OS Release 15.1X49-D40, indicating the change in the severity parameter:

  16:32:43.760393 In IP (tos 0x0, ttl 254, id 16957, offset 0, flags [none], proto: UDP (17), length: 218) 192.0.2.4.syslog > 192.0.2.2.syslog: SYSLOG, length: 190 Facility user (1), Severity info (6)

  Feb 5 16:32:49 RT_NAT: RT_SRC_NAT_PBA_ALLOC: Subscriber 192.0.2.2 used/maximum [1/32] blocks, allocates port block [27200-27263] from 198.51.100.3 in source pool src-nat-pool-1 lsys_id: 0\012

System Management

- During a load override, to enhance the memory for the commit script, you must load the configuration by applying the following commands before the commit step:
  set system scripts commit max-datasize 800000000
  set system scripts op max-datasize 800000000
- On all SRX Series devices in transparent mode, packet flooding is enabled by default. If you have manually disabled packet flooding with the **set security flow ethernet-switching no-packet-flooding** command, then multicast packets such as OSPFv3 hello packets are dropped.

Unified Threat Management (UTM)

- In Junos OS Release 15.1X49-D45 and earlier, the structured log of Web filtering has inappropriate field names.

  Starting in Junos OS Release 15.1X49-D50, the structured log fields have changed. The corresponding fields in the UTM Web filter logs WEBFILTER_URL_BLOCKED, WEBFILTER_URL_REDIRECTED, and WEBFILTER_URL_PERMITTED are now fixed with the appropriate structured log fields.

  The following example shows WEBFILTER_URL_BLOCKED messages before Junos OS Release 15.1X49-D50:

  <12>1 2016-02-18T01:32:50.391Z utm-srx550-b RT_UTM - WEBFILTER_URL_BLOCKED [junos@2636.1.1.1.2.86 source-address="192.0.2.3" source-port="58071"

destination-address="198.51.100.2" destination-port="80" name="cat1" error-message="BY_BLACK_LIST" profile-name="uf1" object-name="www.example.com" pathname="/" username="N/A" roles="N/A"] WebFilter: ACTION="URL Blocked "192.0.2.3(58071)->198.51.100.2(80) CATEGORY="cat1" REASON="BY_BLACK_LIST" PROFILE="uf1" URL=www.example.com OBJ=/ username N/A roles N/A

The following example shows WEBFILTER_URL_BLOCKED messages in Junos OS Release 15.1X49-D50, indicating the change in structured log fields:

<12>1 2016-02-18T01:32:50.391Z utm-srx550-b RT_UTM - WEBFILTER_URL_BLOCKED [junos@2636.1.1.1.2.86 source-address="192.0.2.3" source-port="58071" destination-address="198.51.100.2" destination-port="80" category="cat1" reason="BY_BLACK_LIST" profile="uf1" url="www.example.com" obj="/" username="N/A" roles="N/A"] WebFilter: ACTION="URL Blocked" 192.0.2.3(58071)->198.51.100.2(80) CATEGORY="cat1" REASON="BY_BLACK_LIST" PROFILE="uf1" URL=www.example.com OBJ=/ username N/A roles N/A

The structured log field changes in the UTM Web filter logs WEBFILTER_URL_BLOCKED, WEBFILTER_URL_REDIRECTED, and WEBFILTER_URL_PERMITTED are as follows:

- name -> category
- error-message -> reason
- profile-name -> profile
- object-name -> url
- pathname -> obj

User Interface and Configuration

- You can configure only one rewrite rule for one logical interface. When you configure multiple rewrite rules for one logical interface, an error message is displayed and the commit fails.

VPNs

- Starting with Junos OS Release 15.1X49-D40, the **hmac-sha-256-96** option is deprecated at the [**edit security ipsec proposal** *proposal-name* **authentication-algorithm**] and [**edit security ipsec vpn** *vpn-name* **manual authentication algorithm**] hierarchy levels.
- Dynamic VPN is not supported in Junos OS 15.1X49 releases. Dynamic VPN is supported only in Junos OS Releases 12.3X48 and earlier on SRX100, SRX210, SRX220, SRX240, SRX550, and SRX650 devices.

Zones and Interfaces

- System services configuration option—Starting with Junos OS Release 15.1X49-D40, the **system-services** option at the **[edit security zones security-zone *zone-name* host-inbound-traffic]** hierarchy level and the **system-services** option at the **[edit security zones security-zone *zone-name* interfaces *interface-name* host-inbound-traffic]** hierarchy level no longer support the configuration of the Session Initiation protocol (SIP) system service.

  [See system-services (Security Zones Interfaces) and system-services (Security Zones Host Inbound Traffic).]

Related Documentation

- New and Changed Features on page 5
- Known Behavior on page 17
- Known Issues on page 21
- Resolved Issues on page 26
- Migration, Upgrade, and Downgrade Instructions on page 30

Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 15.1X49-D50.

AppSecure

- On SRX Series devices, when you change the timeout value for the application system cache entries using the command **set services application-identification application-system-cache-timeout**, the cache entries need to be cleared to avoid inconsistency in timeout values of existing entries.

Attack Detection and Prevention (ADP)

- On all high-end SRX Series devices, the first path signature screen is performed first, followed by the fast path bad-inner-header screen.
- On all SRX Series devices, when a packet allow or drop session is established, the bad-inner-header screen is performed on every packet, because this screen is a fast path screen.

CLI

- On SRX5000 line devices, the following CLI statement is deprecated—rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration:

  set chassis fpc <*fpc-slot*> services offload

  The following new CLI statement replaces the deprecated CLI statement:

  set chassis fpc <*fpc-slot*> np-cache

Flow-based and Packet-based Processing

- On SRX Series devices, the default mode for processing traffic is flow mode. To configure an SRX Series device as a border router, you must change the mode from flow-based processing to packet-based processing. Use the **set security forwarding-options family mpls mode packet-based** statement to configure the SRX device to packet mode. You must reboot the device for the configuration to take effect.

General Packet Radio Service (GPRS)

- On SRX5000 line devices, when you use the GTP inspection feature, during an ISSU from Junos OS Release 15.1X49-D10, 15.1X49-D20, or 15.1X49-D30 to Junos OS Release 15.1X49-D40 or later, GTPv0 tunnels will not be synchronized to the upgraded node.

  For GTPv1 and GTPv2, the tunnels will be synchronized, but the timeout gets restarted.

  Beginning with Junos OS Release 15.1X49-D40, ISSU is fully supported with the GTP inspection feature enabled.

Integrated User Firewall

- For integrated user firewall in Junos OS 151.X49-D50 you cannot use the Primary Group, whether by its default name of Domain Users or any other name (if you happened to have changed it), in integrated user firewall configurations.

  When a new user is created in Active Directory, the user is added to the global security group Primary Group which is by default called Domain Users. The Primary Group is less specific than other groups created in Active Directory because all users belong to it. Consequently it can become very large.

IP Monitoring

- On SRX5400, SRX5600, and SRX5800 devices, IP monitoring does not support MIC online/offline status.

Layer 2 Features

- **Layer 2 Bridging and Transparent Mode**— On all SRX Series devices, bridging and transparent mode are not supported on Mini-Physical Interface Modules (Mini-PIMs).

- In Junos OS Release 15.1X49-D40, the following features are not supported on SRX Series devices and vSRX instances:
  - Layer 2 transparent mode policer
  - Three-color policer

Network Address Translation (NAT)

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

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

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

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

Platform and Infrastructure

- On all high-end SRX Series devices, when you enable a global services offloading policy utilizing IOC2 line-cards, the connections per second (CPS) rate might be reduced. It is recommended to utilize IOC3 line-cards to maximize the CPS rate, or alternatively, lower the session count to ensure that the IOC2 is capable of scaling. As a workaround, identify the sessions that must be offloaded and only enable services offloading on those sessions.

Software Installation and Upgrade

- On SRX5000 Series devices, In-Service Software Upgrade (ISSU) is not supported for upgrading from earlier Junos OS releases to Junos OS Release 15.1X49. ISSU is supported for upgrading to successive Junos OS Release 15.1X49 releases and to major Junos OS releases.

  NOTE: **SRX300 Series devices, SRX550HM, and SRX1500 devices do not support ISSU.**

USB autoinstallation

- On SRX300 Series Services Gateways on which the USB autoinstallation feature is enabled (the default configuration), removal of a USB storage device immediately after insertion is not supported.

  After you insert a USB storage device, Junos OS scans the device to check whether it contains the USB autoinstallation file. This process might take up to 50 seconds to complete depending on the quality of the USB storage device and the number and size of the files in the device. Removing the USB storage device while this process is running might cause the services gateway to reboot, the USB port to stop working, and data loss on the USB. We recommend that after inserting a USB storage device, you wait for at least 60 seconds before removing it.

  By issuing the **set system autoinstallation usb disable** command (which disables the USB autoinstallation feature) before you insert the USB device, you can reduce the waiting interval between insertion and removal of a USB storage device from 60 seconds to 20 seconds.

VPN

- On a high-end SRX Series device, VPN monitoring of an externally connected device (such as a PC) is not supported. The destination IP address for VPN monitoring must be a local interface on the high-end SRX Series device.
- On SRX Series devices, configuring RIP demand circuits over P2MP VPN interfaces is not supported.

Related Documentation

- New and Changed Features on page 5
- Changes in Behavior and Syntax on page 8
- Known Issues on page 21
- Resolved Issues on page 26
- Migration, Upgrade, and Downgrade Instructions on page 30

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 15.1X49-D50.

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

Application Layer Gateway

- On branch SRX devices with Media Gateway Control Protocol (MGCP) Application Layer Gateway (ALG) enabled, the flowd process might crash while processing the MGCP traffic and generating the related traffic (security policy) logs. PR871354

NOTE: **Note: This issue occurs only on Junos OS Release 11.1 and previous releases.**

Chassis Clustering

- On high-end SRX Series devices in a chassis cluster, after reboot if the secondary node (RG1) claim cold synchronize (CS) completes first, this might result in bidirectional RTO synchronization or incorrect direction for RTO synchronization. PR1138502
- On high-end SRX Series devices, when large configuration with 32 logical systems and more than 10,000 NAT rules is load override by one without logical system and NAT, the NSD might core on the backup node occasionally. The chassis cluster can be set up normally after the crash. PR1183342
- The master password cannot be configured in chassis cluster mode. PR1184613
- On chassis cluster devices with master password configured and 8 secrets, ISSU can fail with validation errors. PR1186202

Command-Line Interface (CLI)

- On SRX Series devices running Junos OS Release 15.1X49-D50, the **master-password** parameter such as **iteration-count** and **pseudorandom-function** configuration cannot take effect after the configuration is committed. The user has to configure the **master-password** plain-text-password again to make the parameter changing take effect. PR1179095

- On devices running Junos OS Release 15.1X49-D50, a higher master-password iteration count (such as 1000) with large scale shared secret configuration (10000 and more) might impact the configuration commit time even though the configuration change is minor and has nothing to do with the shared secret. PR1181000

Dynamic Host Configuration Protocol (DHCP)

- On SRX Series devices configured as a DHCP server (using the jdhcpd process), when the DHCP server gets a new request from a client and applies an IP address from the authentication process (authd), the jdhcpd process communicates with authd twice as expected (once for the DHCP discovery message and once for the DHCP request message). If the authentication fails in the first message, the authd process will indefinitely wait for the second authentication request. However, the jdhcpd process never sends the second request, because the process detects that the first authentication did not occur. This causes memory leak on the authd process, and the memory might get exhausted, generating a core file and preventing DHCP server service. High CPU usage on the Routing Engine might also be observed. PR1042818
- On SRX1500 devices, after you commit the DHCPv6 configuration, the DHCPv6 relay might not work, because the reply packet is dropped. PR1142727

Flow-based and Packet-based Processing

- On SRX5600, SRX5800 with SRX5K-SPC-4-15-320 card installed, after being in operation for 49 days, a CPU timer rollover on NG-SPC card will occur. When CPU rollover occurs, CPU scheduling of keepalives from NG-SPC to Routing Engine (RE) might fail. This will result in RE triggering reset of all FPCs on local node via chassisd due to loss of keepalives. PR980650
- On high-end SRX Series devices, when a device forwards traffic, a flowd core file is generated. This is a generic issue and does not impact any feature. PR1027306
- On SRX Series devices, default trusted-ca list (Trusted_CAs.pem) is not bundled with Junos. PR1044944
- On SRX550 with 2G memory devices, traffic processed by the serialization process is dropped when the maximum limit of serialization sessions (32,000) is exceeded. As a result, advanced services such as IDP, ALG, GTP, SCTP, and AppSecure are impacted. The limitation of max serialization sessions should be enlarged to 64000. PR1061524
- On branch SRX Series devices, the maximum-sessions value is not displayed correctly. PR1094721
- On high-end SRX Series devices, in central point architecture, syslog is sent out per second per SPU. Hence, the number of SPUs define the number of syslog per second. PR1126885
- On SRX1500 devices, the log buffer size is expanded to 30,000 in event mode. When the log buffer size was 1000, the Packet Forwarding Engine generated logs burst when there were more than 30 entries and more logs were dropped. PR1133757
- On branch SRX Series devices, traffic does not pass with the maximum number of interface logicals (IFLs) 8 queues. PR1138997

- On SRX Series devices in chassis cluster, if you want to use J-Web to configure and commit some of the configurations, you must ensure that all other user sessions are logged out including any CLI sessions. Otherwise, the configurations might fail. PR1140019
- On SRX1500 devices, the security intelligence block-drop action for C and C policy for custom_url_data feed does not work. PR1141745
- On SRX1500 devices, when CPU goes very high (95%+), there is possibility that the connection between AAMW daemon and PKID daemon can be broken. In this case, the AAMW daemon will keep being in Initializing state until that connection is established. PR1142380
- On SRX1500 devices, after the user changes the revocation configuration of a CA profile, the change cannot be populated to the SSL-I's revocation check. It is recommended to change SSL-I configuration to enable or disable CRL checking instead of ca-profile configuration. PR1143462
- On SRX1500 devices in a chassis cluster with Sky Advanced Threat Prevention (ATP) solution deployed, if you disable and then reenable CRL checking of certificate validity, the system does not reenable CRL checking. PR1144280
- On high-end SRX Series devices, if revocation-check is enabled in a CA-profile that does not have CRL information present, then Packet Forwarding Engine (PFE) might stop working. PR1144836
- On SRX340 and SRX345 devices, half-duplex mode is not supported because BCM53426 does not support half-duplex mode. BCM5342X SoC Port configurations, BCM53426 does not have QSGMII interface. Only the QSGMII port supports half-duplex mode. PR1149904

Infrastructure

- On SRX Series devices with health monitor configured for Routing Engine, the system health management process (syshmd) might crash due to a memory corruption in some rare conditions, such as in the scenario that concurrent conflicting manipulation of the file system occurs. PR1069868
- When you plug out and re-plug the modem at CBA750B/CBA850, leading to CBA750B/CBA850 MIB tree change. This might cause the SRX Series device to not get the modem information from the expected MIB node. In such scenarios, the device will display the following modem information: **Connection status: Down** and all counters are set to zero by default. This is a status show problem and data link might still work. To fix this problem, just reboot the CBA750B/CBA850. CBA750B/CBA850 will rebuild the MIB tree and SRX Series device can get the information correctly. PR1187675

Installation and Upgrade

- On SRX340 and SRX345 devices, u-boot version 3.0 does not always detect eUSB at boot up on some devices. When this issue occurs, the device cannot boot the Junos image because the device cannot detect eUSB storage on the board. This issue only occurs when booting the device. As a workaround for this, please power cycle the device. PR1181340

Interfaces

- On SRX1500 devices, when 1G SFP-T is used on the 1G SFP ports (ge-0/0/12 to ge-0/0/15), it does not come up at 100M speed PR1133384
- On SRX series devices, the **show arp** command will show all the ARP entries learned from all interfaces. When layer 2 global mode is switching, the ARP entries learned from IRB interface can only show one specific VLAN member port instead of the actual VLAN port learned the ARP entries. PR1180949
- On branch SRX Series devices, interface statistics are not supported on the IRB interface. PR1182205
- On branch SRX Series devices, the dhcpd server cannot allocate the IP address to the client with the unicast flag set (typically it is on Apple Mac machine) on the IRB interface. PR1187235

Layer 2 Ethernet Services

- On branch SRX Series devices, the current L2NG MAC aging is using software to age out bulk learned MAC addresses. We cannot age specific MAC address learned at specific time immediately after the configured age. Theoretically, the MAC address might be aged out close to 2 times the configured age out time. PR1179089

Platform and Infrastructure

- On high-end SRX devices in a chassis cluster with dual control links, if the first control link (em0) goes down, the master Routing Engine does not send the IP traffic to the remote node. This means that if, for example, redundancy group 0 (control plane) is primary on one node and redundancy group 1 (data plane) is primary on another node, any IP traffic originated on the Routing Engine will not be passed out. PR1051535
- On high-end SRX Series devices, if global SOF policy (all session service-offload) is enabled, the connections per second (CPS) will be impacted due to IOC2 limitation. It is recommended to use IOC3 card if many sessions need to be SOF or lower the SOF session amount to make sure IOC2 is capable of handling it. PR1121262
- On high-end SRX Series devices, if system service rest API is added to the configuration, though commit can be completed, all the configuration change in this commit will not be able to take effect. This is caused due to the rest-api daemon failing to come up as the interface IP is not available during bootup. The configuration is not read on the Routing Engine side. PR1123304

- On SRX Series devices, File Descriptor (FD) might leak on the httpd-gk process when system fails to connect to the mgd process management socket. PR1127512
- On branch SRX Series devices, on addition or deletion of VLANs, the DHCP address will not be acquired by the client and fails from the JDHCP server. PR1139495

Routing Policy and Firewall Filters

- On high-end SRX Series devices, if there are two routing instances of instance type default and virtual router, when you change the instance type of one routing instance from default to virtual router after the routing policy is configured, the route is missing from the second routing instance. PR969944
- On SRX5800 devices in a chassis cluster, the flowd process would crash after a reboot with IPv6 security policies configured. PR1089272

System Logs

- On SRX Series devices, many **help syslog**messages are missing in Junos OS Release 12.1X44 and later releases. PR1159910

Unified Threat Management (UTM)

- On SRX Series devices, when the size of an attachment is larger than 20 MB, the SMTP antivirus scanning of UTM fails to transfer the attached file. PR838503
- On high-end SRX Series devices, under high CPS and UTM SAV interested traffic, SRX might ramp up to 99% CPU usage due to central lock of object cache memory allocation. There is no clear boundary since allocation race condition is varying. Basically, reducing traffic CPS could lower high CPU usage. PR967739
- On branch SRX Series devices (especially SRX550HM) with Sophos Antivirus (SAV) configured, some files whose sizes are larger than the max-content-size might not go into fallback. Instead, some protocols do not predeclare the content size. PR1005086

VPNs

- On SRX Series devices, if IPsec VPN tunnel is established using IKEv2, few drops might be observed during CHILD_SA rekey with the reason "bad SPI", when the SRX is the responder for this rekey. PR1129903
- On branch SRX Series devices with chassis cluster enabled, when the RG0 failover occurs, the pp0 interface will flap if the IPsec VPN tunnel is established using a pp0 interface as the external interface. Due to a timing issue, the pp0 interface flapping might cause the VPN tunnel session and IPsec Security Association (SA) installed in the data-plane to be deleted but the IKE/IPsec SA installed in the Routing Engine will remain causing the VPN traffic outage. PR1143955

Related Documentation

- New and Changed Features on page 5
- Changes in Behavior and Syntax on page 8

Resolved Issues

This section lists the issues fixed in hardware and software in Junos OS Release 15.1X49-D50.

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

Resolved Issues

Application Identification

- On SRX devices, when the application system cache has entries for the application identification, the overall throughput reduces for the related sessions. Clearing the ASC will immediately increase the throughput. In certain cases, IDP does not ignore the session once all signatures concerned to that session are exhausted. This issue is fixed in Junos OS Release 12.1X46, 12.1X47, 12.3x48, and 151.X49 by correcting the logic to make IDP to ignore the session in such cases. PR1155234
- On SRX Series devices with AppID and ASC (application-system-cache) enabled, running the **show services application-identification application-system-cache** command, or its RPC equivalent **get-appid-application-system-cache**, may raise the PFE (SPU) CPU up to 100% utilization. PR1169694

Application Layer Gateways (ALGs)

- On SRX Series devices, the mapping of the Microsoft Remote Procedure Call (MS RPC) universally unique identifier (UUID) to the object identifier (OID) does not associate the security zone information. MS RPC data traffic matching a specific UUID might not be searched for the correct security policy. As a result, MS-RPC data traffic might be dropped. PR1142841
- On branch SRX Series devices with H.323 ALG enabled, in a rare condition, if a gatekeeper sends a RAS gatekeeper confirm (GCF) packet which contains an extension with authentication mode header, H.323 ALG will drop the GCF packet. As a result, the register of H.323 client to gatekeeper will fail. PR1165433

Chassis Clustering

- On SRX5400, SRX5600, and SRX5800 devices in a chassis cluster with IOC II installed, when you simultaneously reboot both the nodes, the secondary node might come up in the ineligible state. After all line cards of the primary node are online, the fabric recovery procedure changes the secondary node from ineligible to the normal secondary state. PR1104249
- On high-end SRX Series devices in a chassis cluster, the GARP is not sent with a static MAC address when chassis cluster failure occurs. PR1115596
- On high-end SRX Series devices in a chassis cluster with the user firewall feature enabled, when you reboot both the nodes simultaneously, user firewall authentication entries are lost on specific SPUs. PR1140283
- On high-end SRX Series devices, when two GTP-U packets have the same address and different TEID and if these two packets are assigned to same SPU to process, the flow session for the secondary packet cannot be setup. PR1182920

Flow-based and Packet-based Processing

- On high-end SRX Series devices, the wrong IP information **Unknown IP version: 0** is displayed in some load-balancing thread (LBT) and packet-ordering thread (POT) logs that are triggered by fragmentation. PR1032647
- On high-end SRX Series devices, for some designed traffic, session limit SPU entries from the same source IP address do not distribute among all SPUs evenly. Some central point session limit entries might leak, which might lead to an inaccurate session limit. PR1161277
- On high-end SRX Series devices, when security intelligence is implemented, the global data shared memory might leak when you update the Command and Control (C) feed. PR1163463
- On SRX Series devices, there should not be an [enter] option after the authentication-source in the authentication table delete command. If you press enter then the command will not be successful. PR1168289
- On branch SRX Series devices PKI (re) enrollment stops in case of manual enrollment. If the CA is configured to approve certificate requests manually, CA responds back with PENDING for SCEP enrollment request until, the administrator accepts the request. After receiving the PENDING response, PKId needs to resend enrollment request at configured retry-interval time. Retry was not happening because of this bug and enrollment was failing. This behavior was observed only when SNMP walk was performed on certificates while enrollment was also in progress. PR1173598
- On high-end SRX Series devices, if the fireware runs for very long time, some counters might round back and show huge numbers because we add the number in mixture of int32_t and u_int64_t. This would not cause any functional outage, only affect the showing number for debug. PR1175469

Interfaces

- On SRX550HM devices, some LLC frames might get dropped if they are received on a VPLS-enabled interface. PR1160561
- On SRX300 and SRX320 devices, LACP is not supported. PR1165015
- On SRX300, SRX320, SRX340, and SRX345 devices, when you change the interface mode from 10m/no-auto-10m/no-auto to 100m/no-auto-100m/no-auto, interfaces might go down on both the sides. PR1165942
- On branch SRX Series devices, the IRB interface cannot be used as an external interface with IPsec VPN. PR1166714
- On branch SRX Series devices, input-traffic-control-profile, output-traffic-control-profile, scheduler-map, and shaping-rate can be configured on the IRB logical interface, to support QOS for the IRB interface. However, rewrite-rules are not supported on the IRB interface. PR1170472

Intrusion Detection and Prevention (IDP)

- On all SRX Series devices, when Sky Advanced Threat Protection inline blocking and IDP are configured together in the same security policy, Sky Advanced Threat Protection inline blocking is not supported, but files are still submitted to the cloud for scanning. In this scenario IDP functionality is not affected, and IDP functions normally. PR 1144843

Layer 2 Features

- On branch SRX Series devices in a chassis cluster, Layer 2 switching mode configurations do not work. PR1161372
- On branch SRX Series devices in a chassis cluster, enhanced Layer 2 does not fully support VPLS. When the logical interface is up or down, some message handlers related to Layer 2 might be triggered, which attempt to process VPLS-related route changes. As VPLS is not fully supported in Layer 2, this might cause an assertion failure. PR1167439

Network Address Translation (NAT)

- On SRX Series devices, when a routing instances name is configured with 32 characters or more for a virtual router, the interface that is configured with NAT proxy-arp in that virtual router does not respond to any ARP request. PR1164600
- On high-end SRX Series devices, when NAT with port-block allocation (PBA) is configured, the CPU is utilized at the optimum level and it affects the protocols such as LACP. This issue might cause temporary network instability. PR1172347

Platform and Infrastructure

- On SRX series devices, if OSPF over GRE tunnel is deployed with bandwidth configured in GRE interface and with RPM or IP monitoring configured, the OSPF cost calculation will be incorrect. PR1130370

VPNs

- On SRX devices, packet loss might be observed over IPsec tunnels after reconfiguring the IPsec peer facing interface. PR1162133
- On SRX Series devices, VPN monitoring feature is not working correctly in Junos OS Release 15.1X49-D40. Hence, it is better to avoid using it. PR1163751

Related Documentation

- New and Changed Features on page 5
- Changes in Behavior and Syntax on page 8
- Known Behavior on page 17
- Known Issues on page 21
- Migration, Upgrade, and Downgrade Instructions on page 30

Documentation Updates

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

Various Guides

Content from the Feature Guide for Junos OS Release 15.1X49-D50 is available in the feature-specific Guides at the Junos OS for SRX Series page.

Related Documentation

- New and Changed Features on page 5
- Changes in Behavior and Syntax on page 8
- Known Behavior on page 17
- Known Issues on page 21
- Resolved Issues on page 26
- Migration, Upgrade, and Downgrade Instructions on page 30

Migration, Upgrade, and Downgrade Instructions

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

Upgrade for Layer 2 Configuration

Starting with Junos OS Release 15.1X49-D10 and later, only enhanced Layer 2 CLI configurations are supported. If your device was configured earlier for Layer 2 transparent mode, then you must convert the legacy configurations to Layer 2 next-generation CLI configurations.

For details on how to migrate from Junos OS Release 12.3X48-D10 and earlier releases to Junos OS Release 15.1X49-D10 and later releases, refer to the Knowledge Base article at https://kb.juniper.net/InfoCenter/index?page=content&id=KB30445.

Upgrade and Downgrade Scripts for Address Book Configuration

Beginning with Junos OS Release 12.1, you can configure address books under the **[security]** hierarchy and attach security zones to them (zone-attached configuration). In Junos OS Release 11.1 and earlier, address books were defined under the **[security zones]** hierarchy (zone-defined configuration).

You can either define all address books under the **[security]** hierarchy in a zone-attached configuration format or under the **[security zones]** hierarchy in a zone-defined configuration format; the CLI displays an error and fails to commit the configuration if you configure both configuration formats on one system.

Juniper Networks provides Junos operation scripts that allow you to work in either of the address book configuration formats (see Figure 1 on page 32).

About Upgrade and Downgrade Scripts

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

- **Use the default address book configuration**—You can configure address books using the zone-defined configuration format, which is available by default. For information on how to configure zone-defined address books, see the Junos OS Release 11.1 documentation.

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

  After upgrading to the zone-attached address book configuration:

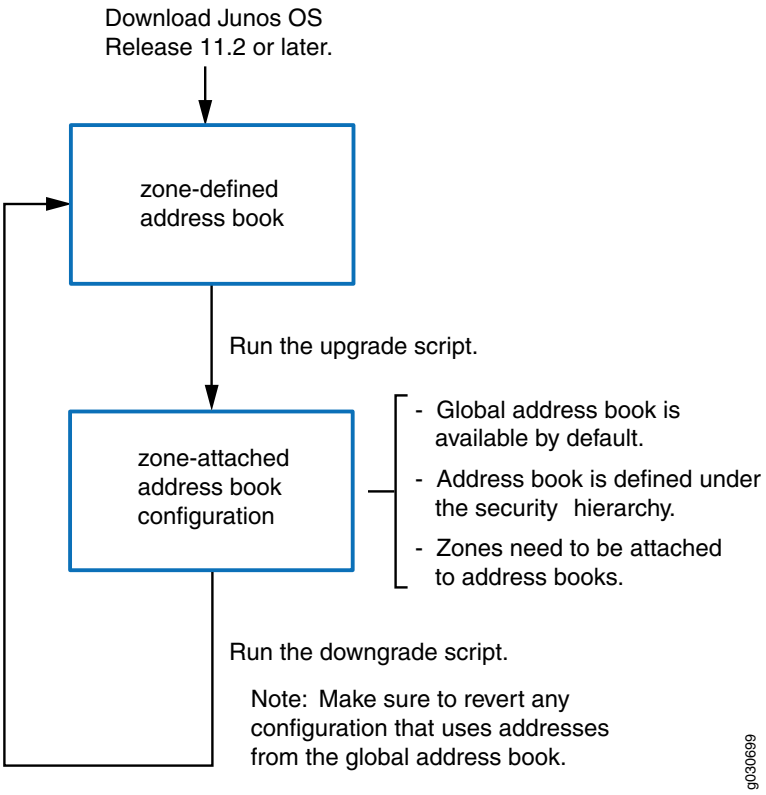
  - You cannot configure address books using the zone-defined address book configuration format; the CLI displays an error and fails to commit.
  - You cannot configure address books using the J-Web interface.

  For information on how to configure zone-attached address books, see the Junos OS Release 12.1 documentation.

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

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

Figure 1: Upgrade and Downgrade Scripts for Address Books



Running Upgrade and Downgrade Scripts

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

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

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

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

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 12.1X44, 12.1X46, and 12.3X48 are EEOL releases. You can upgrade from Junos OS Release 12.1X44 to Release 12.1X46 or even from Junos OS Release 12.1X44 to Release 12.3X48. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind.

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

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

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

Related Documentation

- New and Changed Features on page 5
- Changes in Behavior and Syntax on page 8
- Known Behavior on page 17
- Known Issues on page 21
- Resolved Issues on page 26

Product Compatibility

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

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

Hardware Compatibility

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

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

platform for your network. Find Feature Explorer at https://pathfinder.juniper.net/feature-explorer/.

Transceiver Compatibility for SRX Series Devices

We strongly recommend that only transceivers provided by Juniper Networks be used on SRX Series interface modules. Different transceiver types (long-range, short-range, copper, and others) can be used together on multiport SFP interface modules as long as they are provided by Juniper Networks. We cannot guarantee that the interface module will operate correctly if third-party transceivers are used.

Please contact Juniper Networks for the correct transceiver part number for your device.

Finding More Information

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

For regulatory compliance information about Common Criteria, FIPS, Homologation, RoHS2, and USGv6 for Juniper Networks products, see the Juniper Networks Compliance Advisor.

Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos OS feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at https://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 https://www.juniper.net/documentation/content-applications/content-explorer/.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post sales technical support, you can access our tools and resources online or open a case with JTAC.

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://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: https://www.juniper.net/customers/support/
- Search for known bugs: https://www.juniper.net/kb/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: https://www.juniper.net/cm/

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

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at https://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 https://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/documentation/feedback/.

Revision History

12, July 2018—Revision 11— Junos OS 15.1X49-D50 – SRX Series.

28, April 2017—Revision 10— Junos OS 15.1X49-D50 – SRX Series.

24, November 2016—Revision 9— Junos OS 15.1X49-D50 – SRX Series.

15, November 2016—Revision 8— Junos OS 15.1X49-D50 – SRX Series.

27, September 2016—Revision 7— Junos OS 15.1X49-D50 – SRX Series.

16, August 2016—Revision 6— Junos OS 15.1X49-D50 – SRX Series.

10, August 2016—Revision 5— Junos OS 15.1X49-D50 – SRX Series.

20, July 2016—Revision 4— Junos OS 15.1X49-D50 – SRX Series.

23, June 2016—Revision 3— Junos OS 15.1X49-D50 – SRX Series.

13, June 2016—Revision 2— Junos OS 15.1X49-D50 – SRX Series.

01, June 2016—Revision 1— Junos OS 15.1X49-D50 – SRX Series.