JUNOS 9.2 Software for SRX-series Services Gateway Release Notes

Release 9.2, R2
September 2008
Part Number: 530-025668-01
Revision R2

These release notes accompany Release 9.2 of JUNOS software for SRX-series services gateways. They briefly describe new software and hardware features and provide a summary of the current software and hardware limitations and known defects that exist in this release. You can also find these release notes on the Juniper Networks Technical Publications Web page located at http://www.juniper.net/techpubs/.

Contents

SRX-series Hardware Features

The SRX-series services gateway is a high-performance, highly scalable, carrier-class device. It features multiprocessor architecture optimized for JUNOS software.

By installing different combinations of I/O Cards (IOCs) and Services Processing Cards (SPCs), you can tailor both the number of Gigabit ports and the maximum security processing capacity to suit your network.

The following table compares the SRX 5600 and SRX 5800 services gateways:

	SRX 5600	SRX 5800
Maximum Throughput	60 Gigabits per second	120 Gigabits per second
Total Slots	8	14
Slots for SPCs and IOCs	6	12
Slots for Switch Control Boards (SCBs)	2	3
Chassis Height	8 RU (14”)	16 RU (28”)
Devices per Rack	6	3

Two types of I/O Cards (IOCs) interface cards are available, both of which consist of four Packet Forwarding Engines and enable a throughput of 10 Gbps:

- A 40-port Gigabit Ethernet IOC with SFP connectors (1000 Mbit copper and fiber only)
- A 4-port 10-Gigabit Ethernet IOC with XFP connectors

The SRX 5600 services gateway chassis provides redundancy and resiliency. The hardware system is fully redundant, including power supplies, fan trays, and Switch Control Boards.

JUNOS Software for SRX-series Features

Flow and Processing

- **Flow-based stateful processing**—In addition to packet processing, JUNOS software for SRX-series performs flow-based stateful processing. When a packet enters the device, the system applies any packet-based filter processing associated with the interface to the packet. Next, the system attempts to match the packet against an existing session based on a session's match criteria (source and destination addresses, source and destination ports, and protocol and session tokens derived from the zone and virtual router). If a packet matches an existing session, the system processes it according to the flow's session features, security policies, screens, and other features. If the packet does not match an existing session, the system establishes a new session for the packet based on routing,

policy, and other classification information. Before a packet leaves the device, the system applies filters and traffic shaping to it.

- **Distributed multithread flow** —The SRX-series services gateway is multicore, multichassis hardware with distributed computing engines. The network processing units (NPUs) on the I/O cards and multicore security processing units (SPUs) on the security processing cards comprise the data plane.

  Packets for any given flow usually traverse two NPUs and possibly more than one SPU (in the case of tunnels). Therefore, a distributed flow module is needed that can span multiple computing engines. Note that combo-mode, in which one SPU directs traffic to itself as well as other SPUs on the SPC, is not supported in this release. Instead, the SPU can only direct traffic to other SPUs.

  To configure flow options, use the flow statement at the set security hierarchy. For more information, see the *JUNOS Software Security Configuration Guide*.

Interfaces and Routing

- **Interfaces**—Interfaces act as a doorway through which traffic enters and exits a device. Several security-related configuration and runtime attributes are kept in an interface object. Different modules in the data path use these attributes. Many interfaces can share exactly the same security requirements; however, different interfaces can also have different security requirements for inbound and outbound (I/O) data packets.

  Security processing and inbound and outbound (I/O) data packets analysis are separated in JUNOS software and SRX-series service gateways. As a result, the line-card interface on the input/output card (IOC) and the security processors on the services processing card (SPC) are separated by a fabric. The security data plane is simultaneously performing multiprocessing (32-way MT per XLR SPU) and distributed processing (a maximum of 2 SPUs per SPC). For more information, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

- **Routing**— SRX-series services gateways support using the Border Gateway Protocol (BGP), the Open Shortest Path First (OSPF) Protocol, and the Routing Information Protocol (RIP) to deliver routing information across networks. To configure the services gateway to use these protocols, use the bgp, ospf, or rip statements (respectively) at the [protocols] hierarchy level. You can also configure the services gateway to use static routes. For more information, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

  SRX-series services gateways also support the following additional routing functionality:

  - **DHCP**— JUNOS software for SRX-series supports Dynamic Host Configuration Protocol (DHCP) client, relay, and server functions, enabling the services gateway to provide IP addresses and settings to hosts that are connected to the device's interfaces. When you configure the SRX-series device as a DHCP server, hosts can connect to the device's interface via subnet or through DHCP relay. To configure DHCP, use the dhcp statement at the [system services] hierarchy level.
  - **DNS**— JUNOS software for SRX-series incorporates Domain Name System (DNS) support, enabling the services gateway to reference locations by

domain name (such as www.juniper.net) in addition to using the routable IP address. To configure DNS, see the *JUNOS Software Administration Guide*.

- **NTP**— JUNOS software for SRX-series incorporates Network Time Protocol (NTP) support, enabling the services gateway to synchronize time and coordinate time distribution in a large, diverse network. To configure NTP, use the ntp statement at the [system] hierarchy level.

For more information, see the *JUNOS Software Administration Guide*.

NOTE: Release 9.2 of JUNOS software for the SRX-series services gateway does not support packet-based protocols such as MPLS, Connectionless Network Service (CLNS), and IP version 6 (IPV6).

- **IPv4**—JUNOS software for SRX-series supports processing IPv4 (IP version 4) traffic through an interface. The IPv4 protocol family supports 32-bit addresses and subnets. To enable the IPv4 protocol for an interface, specify inet for the interface family. For example, use edit interfaces ge-0/0/3 unit 0 family inet address 10.10.10.10/24.
- **Class of Service (CoS)** —The JUNOS software for SRX-series Class of Service (CoS) feature provides a set of mechanisms that you can use to provide differentiated services when best-effort traffic delivery is insufficient. When a network experiences congestion and delay, some packets must be dropped. JUNOS software for SRX-series CoS allows you to classify and then divide traffic into classes and offer various levels of throughput and packet loss when congestion occurs. This allows packet loss to happen according to rules that you configure. Note that CoS policing is not available in this release.

  You can use an SRX-series services gateway to control traffic rate by applying classifiers and shapers. To configure CoS components, use the component you want to configure at the [edit class-of-service] hierarchy level of the configuration. For more information, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

Chassis Clustering

- **Support for chassis clustering**—You can connect the chassis of two SRX 5600 services gateways or two SRX 5800 services gateways to provide stateful failover of JUNOS processes and services. Interchassis clustering removes the single point of failure in the network by allowing the services gateway to be configured in a redundant cluster, with one device acting as the primary and the other as a backup. If the primary fails, the backup takes over traffic processing. Clustered services gateways synchronize configuration, kernel, and Packet Forwarding Engine session states across the cluster to facilitate high availability of interfaces and services. JUNOS software for SRX-series includes the following chassis cluster features:

- Resilient system architecture includes a single control plane for the entire cluster to manage multiple Packet Forwarding Engines.
- Configuration and dynamic runtime states are synchronized between the services gateways within a cluster.
- Graceful restart of the routing protocols enables the services gateway to minimize traffic disruption during a failover.
- Physical interfaces are grouped and monitored to trigger failover to the backup services gateway if the failure parameters cross a configured threshold.

For more information, see the *JUNOS Software Security Configuration Guide*.

NOTE: In this release of JUNOS software for SRX-series, synchronization of IDP-specific runtime data does not occur across the cluster. As a result, IDP processing is not continued for sessions that fail over. (IDP processing resumes for sessions created after failover.)

NOTE: When configuring chassis clusters, you are automatically in configure private mode. As a result, you must commit changes from the top of the hierarchy. For information about the configure private mode, see the *JUNOS CLI User Guide*.

NOTE: In SRX-series services gateways, the offline, online, and restart commands are supported only on IOCs and are not supported on SPCs.

Security

- **Security zones**—Security zones are the building blocks for policies; they are logical entities to which one or more interfaces are bound. Security zones provide a means of distinguishing groups of hosts (user systems and other hosts, such as servers) and their resources from one another in order to apply different security measures to them. From the perspective of security policies, traffic enters into one security zone (to-zone) and goes out on another (from-zone). To configure security zones, use the zones statement at the [security zones] hierarchy level. For more information, see the *JUNOS Software Security Configuration Guide*.
- **Security policies**—Security policies can be configured to control traffic flow from one zone to another by defining a certain action on the kinds of traffic that is allowed from specified sources to specified destinations at scheduled times. When packets match a policy, the policy instructs the flow to apply different rules for features. To configure a policy, use the screen statement at the [set security policies] hierarchy level.
- **Firewall screens**—JUNOS software for SRX-series provides various detection methods and defense mechanisms to combat the following security breaches at all stages of their execution:

- SYN, UDP, and ICMP flood attacks
- Network DoS attacks
- Operating system-specific DoS attacks

To configure screen options, use the screen statement at the [set security screen] hierarchy level.

- **Firewall user authentication** Firewall user authentication enables you to restrict and permit access to protected resources behind a firewall based on a user's source IP address and other credentials. You may use pass-through authentication or Web authentication to control access to the protected resources. With pass-through authentication, a user from one zone tries to access resources from another zone over an FTP, Telnet, or HTTP connection. With Web authentication, a user tries to connect to an IP address on the device over an HTTP connection. With both methods, the device forwards the user's credentials to the server of your choice (local, RADIUS, LDAP, or RSA SecurID) to authenticate the user and control subsequent access requests.

  To configure pass-through authentication, use the following statements:

  set security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit firewall-authentication pass-through

  To configure Web authentication, use the following statements:

  set security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit firewall-authentication web-authentication

  For more information, see the *JUNOS Software Security Configuration Guide*.

- **Network Address Translation**— Network Address Translation (NAT) is a method by which IP addresses in a packet are mapped from one group to another and, optionally, port numbers in the packet are translated into different port numbers. NAT is described in RFC 1631 to solve IP (version 4) address depletion problems. On an SRX-series services gateway, JUNOS software decouples NAT configuration from policy configuration. NAT has its own rules to regulate traffic on the SRX-series services gateway.

  To configure NAT, use the nat statement at the [set security] hierarchy level. For more information, see the *JUNOS Software Security Configuration Guide*.

NOTE: Release 9.2 of JUNOS software for the SRX-series services gateway does not support Static NAT.

IDP

- **IDP Policies**—Intrusion Detection and Prevention (IDP) policy enables you to selectively enforce various attack detection and prevention techniques on network traffic passing through an IDP-enabled device. It allows you to define policy rules to match a section of traffic based on a zone, network, and application, and then take active or passive preventive actions on that traffic.

  A policy is made up of *rulebases*, and each rulebase contains a set of *rules*. You define rule parameters, such as traffic match conditions, action, and logging requirements and then add the rules to rulebases. You can create new IDP policies from scratch or start with a predefined template provided by Juniper Networks. Juniper Networks also provides custom application objects and attack objects that you can configure as match conditions in policies.

  To configure an IDP policy, use the idp-policy statement at the [edit security idp] hierarchy level. For more information, see the *JUNOS Software Security Configuration Guide*.

- **IDP Signature Database**—Signature database is one of the major components of IDP. It contains definitions of different objects—such as attack objects, application signatures objects, and service objects—that are used in defining IDP policy rules. As a response to new vulnerabilities, Juniper Networks periodically provides a file containing attack database updates on the Juniper Web site.

  To protect your network from new threats, you can download signature database updates manually or configure your device to download them automatically at a specified interval. For more information, see the *JUNOS Software Security Configuration Guide*.

- **IDP Application Identification**—Juniper Networks provides predefined application signatures that detect TCP and UDP applications running on non standard ports. Identifying these applications allows IDP to apply appropriate attack objects to applications running on non standard ports. It also improves performance by narrowing the scope of attack signatures for applications without decoders.

  Application signatures are available as part of the security package provided by Juniper Networks. You download predefined application signatures along with the security package updates. Application identification is enabled by default and is automatically turned on when you configure the default application in the IDP policy. For more information, see the *JUNOS Software Security Configuration Guide*.

- **Protocol Detector Engine**—The IDP protocol detector engine contains Application Layer protocol decoders or services. You can download the protocol detector updates along with the signature database updates.

  IDP supports 52 protocol decoders or services. Protocol decoders scan protocol headers and message body to identify individual fields in the protocols to determine if data conforms to the RFC. You configure protocol decoders in IDP policy rules to specify the protocol that an attack uses to access your network. For more information, see the *JUNOS Software Security Configuration Guide*

- **IDP Logging**—The basic JUNOS system logging continues to function after IDP is enabled. An IDP-enabled device supports basic JUNOS system logging and continues to record events that occur because of routine operations, such as a

user login into the configuration database. It records failure and error conditions, such as failure to access a configuration file. In addition to the regular system log messages, IDP generates event logs for attacks. To manage attack log volume and message size, IDP supports log suppression.

Enabling log suppression ensures that minimal numbers of logs are generated for the same event or attack that occurs multiple times. To configure log suppression, use the suppression statement at the [edit security idp sensor-configuration log] hierarchy level. For more information, see the *JUNOS Software Security Configuration Guide*.

- **IDP DiffServ Marking**—Configuring Differentiated Services Code Point (DSCP) values in IDP policies provides a method of associating class-of-service (CoS) values—thus different levels of reliability—for different types of traffic on the network. DSCP is an integer value encoded in the 6-bit field defined in IP packet headers. It is used to enforce CoS distinctions. CoS allows you to override the default packet-forwarding behavior and assign service levels to specific traffic flows.

  You can configure DSCP value as an action in an IDP policy rule. Based on the DSCP value, behavior aggregate classifiers set the forwarding class and loss priority for the traffic determining the forwarding treatment the traffic receives. For more information, see the *JUNOS Software Security Configuration Guide*.

- **IDP J-Web Support**—You can configure IDP policies and request security package updates by using Quick Configuration pages in the J-Web user interface. You can also display IDP status and memory usage in the J-Web monitoring pages. For more information, see the *JUNOS Software Security Configuration Guide* and the *JUNOS Software Administration Guide*.

J-Web

J-Web User Interface—A graphical user interface enables you to configure, monitor, troubleshoot, and manage the SRX-series devices through an Internet browser. The J-Web interface includes Quick Configuration pages to perform basic configuration of the devices and monitoring tools to view system health, routes, and statistics. The J-Web interface provides diagnostic tools (such as ping and traceroute) and file utilities to manage configuration files, licenses, and temporary files on the device. The J-Web interface also includes a chassis viewer, which provides a graphical, dynamic view of the SRX-series of devices. For more information, see the *J-Web Interface User Guide*.

Management and Administration

NOTE: NSM-Aragorn (2008.1) supports Viking via forward support.

- **Chassis management**—JUNOS software for SRX-series provides the ability to monitor and manage select chassis components. This includes monitoring chassis clusters, component temperature and cooling systems, chassis firmware, and chassis location. The CLI also provides commands for bringing most chassis components online and offline.

  To bring chassis components online and offline, use the chassis statement at the [request] hierarchy level. For more information, see the *JUNOS Software Security Configuration Guide*.

- **Packet tracing infrastructure**—The JUNOS software for SRX-series trace function provides a tool for applications to write security and security flow debugging information to a file. The information that appears in this file is based on configured criteria. This criteria includes source port, destination port, protocol, interface, and string matching. Use this information to analyze security application issues. The trace function operates in a distributed manner, with each thread writing to its own trace buffer. These trace buffers are then collected at one point, sorted, and written to trace files. Trace messages are delivered using the InterProcess Communications (IPC) protocol.

  To configure traceoptions, use the traceoptions statement at the [set security] hierarchy level. For more information, see the *JUNOS Software Security Configuration Guide*.

- **SPU monitoring** —The JUNOS software for SRX-series provides a new JUNOS software-based security device that uses multiple processors to process traffic. SPU monitoring allows for:

  - CPU utilization per SPU in percentage
  - Memory utilization per SPU in percentage

  These metrics provide information that can be used to prevent unexpected outages and look for trends for capacity planning. To monitor the Flexible PIC Concentrator (FPC) card by using the SPU unit's CPU and memory utilization, use the show security monitoring fpc statement. For more information, see the *JUNOS Software Security Configuration Guide*.

- **System logging**— JUNOS software for SRX-series generates separate system log messages (also called syslog messages) to record events that occur on the system's data and control planes.

  The data plane logs primarily include a list of security events that the system has handled directly inside the data plane. Because the system has already handled these events, it does not send them on to the Routing Engine. Instead, the system streams the logs directly to external log servers, bypassing the Routing Engine. To view the data plane logs, use the log statement at the [security] hierarchy level.

  The control plane logs, on the other hand, include a list of actionable events. The system sends this list of control plane events on to the eventd process on the Routing Engine, which then handles the events using JUNOS event policies and/or by generating system log messages. You can choose to send control plane logs to a file, user terminal, routing platform console, or remote machine.

To generate control plane logs, use the syslog statement at the [system] hierarchy level. For more information, see the *JUNOS Software Administration Guide*.

NOTE: In SRX-series devices, data plane logs and control plane logs have to be configured separately.

Known Limitations

IDP

- This release of JUNOS software for SRX-series only supports the following IDP policies:
  - Recommended IDP policy template
  - DNS_server IDP policy template
  - Custom IDP policy with critical attack group
- The default URL for signature download is not accessible to external customers in this release. To download IDP signatures, you must configure the following URL through the CLI: https://services.netscreen.com

Outstanding Issues

Chassis

- LEDs on the Routing Engine and PICs are not shown as green when they are up and online on chassis view in a SRX-series device. [PR/297693]

Chassis Cluster

- On SRX 5600 and SRX 5800 devices, local interfaces are not supported in chassis cluster mode. [PR/296168]
- Chassis SNMP objects are not reporting correctly when the device is operating in JSRP cluster mode with JUNOS software. [PR/304082]
- Platforms supporting chassis cluster do not support vlan-ids greater than 1023 on reth interfaces. [PR/314636]

Class of Service

- On SRX 5600 devices, class-of-service based-forwarding (CBF) is not working. [PR/304830]
- On SRX 5600 and SRX 5800 devices, when the traffic profile attached to the physical interface is added or removed, the class-of-service (CoS) configuration is bypassed. As a workaround, deactivate and activate the CoS configuration. [PR/306309]

Firewall

- When you issue the firewall authentication command with 5000 users connected to the device, about 200-300 requests stay in the pending state. As a workaround, start a new session after closing the existing session. [PR/293206]
- When the show firewall log output command is issued, the time logged by the firewall will be ahead of the current system time. [PR/296348]

Flow

- In a SRX-series device, when traffic matches a deny policy, sessions will not be created successfully. However, sessions are still consumed, and the "Unicast-sessions" and "Sessions-in-use" fields shown by the show security flow session summary command will reflect this. [PR/284299]
- You are unable to run the show security flow session command on the secondary node in the following instances:
  - When you restart an SRX-series device
  - When the device crashes due to kernel replication process (kysncd)

  As a work around, restart the chassis-control of the device. [PR/290053]
- On an SRX-series device, the show security flow session command currently does not display aggregate session information. Instead, it displays sessions on a per-SPU basis.. [PR/264439]
- Configuring the flow filter with the all flag might result in traces that are not related to the configured filter. As a workaround, use flow trace flag basic with the command set security flow traceoptions flag. [PR/304083]

Hardware

- On SRX 5600 and SRX 5800 devices, the HA LED on the SPC does not light. [PR/303899]

IDP

- On SRX 5600 and SRX 5800 devices, IDP does not respond to security package requests after you create the policy with all the predefined attack groups. As a workaround, delete all the policies and retry. [PR/279147]
- On SRX 5600 and SRX 5800 devices, the custom attack detection fails in backward FTP flow. [PR/287912]
- On SRX 5600 and SRX 5800 devices, the large policy load fails on the second successive attempt with policy aging enabled. [PR/289362]
- When the firewall and IDP policy both enable diffServ marking with a different DSCP value for the same traffic, the firewall DSCP value takes precedence and the traffic is marked using the firewall DSCP value. [PR/297437]
- When you push a large IDP policy under insufficient memory, the policy fails to get through due to heavy traffic. [PR/300411]
- On SRX 5600 and SRX 5800 devices, when a new signature pack is downloaded and installed in the absence of a policy on the dataplane, the new detector is not installed on both the Routing Engine and the dataplane. [PR/303561]
- Loading a new IDP policy fails as the memory on the device is insufficient and the last policy pushed to the device is restored. As a result, logs are generated incorrectly for the failed policy loads. [PR/304388]
- On SRX 5600 and SRX 5800 devices, the output of show security idp status output is not accurate for chassis cluster. [PR/310777]
- When there are 8 or 9 policies already in the data plane, a policy cannot load because of insufficient heap memory. [PR/388190]

Interfaces

- Jumbo frames are not supported. [PR/271507]
- You cannot apply shaper, scheduler and output-control-profile to the reth interface on an SRX-series device. [PR/298102]
- Configuring an SRX-series device with set system process jsrp-service disable only on a primary node of the cluster causes the cluster to go into bad state. [PR/292411]
- Readback error messages are seen in the system log on commit. [PR/306046]
- Fragmentation does not work on packets originating from the device when the interface is part of a virtual-router routing instance. [PR/306836]

J-Web

- On SRX 5600 and SRX 5800 devices, there are no options for loading and activating the policy template through J-Web. [PR/291317]
- On SRX 5600 and SRX 5800 devices, the J-Web policy rule configuration page should list the available predefined attacks and groups, so that the user can select the attacks and groups and configure the rules. [PR/295283]
- When you plot a graph for an interface in the J-Web, the I/O bytes of the interface does not get refreshed. The I/O bytes in interface summary panel gets refreshed only when the graph is stopped or closed. [PR/304278]
- On SRX-series devices, the "Data Refresh Failed" message is seen on the **Monitor > Interface** page. [PR/309197]
- When the J-Web session is terminated from the CLI, error and warning messages related to J-Web appear in the log. [PR/311181]

Routing Engine

- The SRX 5600 and SRX 5800 services gateways only support a single Routing Engine installed in the Switch Control Board (SCB) in slot 0. The device will not start if a Routing Engine is installed in an SCB in slot 1. [PR/303914]

System

- The show security monitoring Flexible PIC Concentrator (FPC) shows previous data when a card is replaced. [PR/285551]
- The new custom detector installation does not get loaded to the data plane. Hence, the Packet Forwarding Engine displays the old detector version. As a workaround, reboot the device. [PR/291205]
- The device will crash if you use set system processes chassis-control disable for 4-5 minutes and then enable it. Do not use this command in chassis cluster mode. [PR/296022]
- On SRX-series devices, you can reboot the media disk from the CLI but not from the J-Web interface. [PR/300270]
- After configuring session idle timeout less than the dashboard refresh interval, you are able to navigate to other J-web pages even after the session is timed out. [PR/302054]
- On SRX-series devices, the default J-Web session timeout is not working. [PR/311160]

Errata

This section lists outstanding issues with the documentation.

ALGs

- The *JUNOS Software Security Configuration Guide* and *JUNOS Software CLI Reference* incorrectly state that MGCP ALGs are supported on SRX-series services gateways. This functionality will be supported in a future release of the product.

Authentication

- The *JUNOS Software Administration Guide* incorrectly states that local authentication is not supported on SRX-series services gateways. This error has been corrected in subsequent revisions.

Chassis Cluster

- The *JUNOS Software Security Configuration Guide* states that although services routers or services gateways connected in a chassis cluster must be the same kind, they can contain different Physical Interface Modules (PIMs). This is true for J-series chassis clusters, but not for SRX-series chassis clusters. For SRX-series chassis clusters, the SPCs must be identical and in identical slots on the two boxes, but the IOCs need not be in identical slots.

Flow

- The *JUNOS Software CLI Reference* states that the following aggressive aging statements are supported on SRX-series devices when in fact they are not:
  - [edit security flow aging early-ageout]
  - [edit security flow aging high-watermark]
  - [edit security flow aging low-watermark]

  [*JUNOS Software CLI Reference*]

IDP

- The *JUNOS Software Security Configuration Guide* incorrectly states that the Dynamic Attack Groups field described in the "Adding an IPS Rulebase Quick Configuration Page Summary" and the "Adding an Exempt Rulebase Quick Configuration Page Summary" sections are supported in the JUNOS software with enhanced services Release 9.2. [*JUNOS Software Security Configuration Guide*]
- The commands listed under the "Monitoring IDP" section of *JUNOS Software Administration Guide* are incorrect. The correct commands are:
  - show security idp status
  - show security idp memory

  [*JUNOS Software Administration Guide*]
- The *JUNOS Software CLI Reference* incorrectly states that the following IDP output fields are in use:

  show security idp counters application-identification
  - AI-disabled sessions due to Aux/Dynamic/Encap/Mgmt flows
  - AI-disabled sessions due to no AI signatures

show security idp counters flow

- ICMP-error packets
- Session construction failed
- Not a new session
- Invalid index at ageout
- Busy packets
- BAD-UDP-Checksum packets
- Gate matches
- Session aged-out
- Sessions in use while ageout

show security idp counters ips

- IDS cache hits
- IDS cache misses
- No Peer MAc

show security idp counters log

- Logs waiting for post-window packets
- Logs ready to be sent
- Logs in suppression list
- Logs ready to be sent high watermark
- Log receive buffer full
- Packet log too big
- Reads per second
- Logs in read buffer high watermark
- Packets lost
- Packet copied
- Packets held
- IP Action Messages
- IP Action Drops
- IP Action Exits

- NWaits
- Kpacket too big

show security idp counters packet

- Dropped Sessions
- GRE decapsulations
- PPP decapsulations
- GTP decapsulations
- GTP Flows
- TCP decompression uncompressed IP
- TCP decompression compressed IP
- Deferred send Packets
- Ip-in-ip packets
- TTL errors
- Routing Loops
- STP Drops
- No route packets
- Flood Ip
- Invalid Ethernet headers

show security idp counters tcp-reassembler

- Bad TCP checksums
- Copied packets

[*JUNOS Software CLI Reference*]

Interfaces

- The *JUNOS Software CLI Reference* incorrectly states request wan-acceleration-pim login fpc slot instead of request wan-acceleration login fpc slot.[*JUNOS Software CLI Reference*]

Screens

- The following guides contain incorrect screen configuration instructions:
  - *JUNOS Software Security Configuration Guide*, "Attack Detection and Prevention" chapter
  - *JUNOS Software with Enhanced Services Design and Implementation Guide*, "Implementing Firewall Deployments for Branch Offices" chapter

Examples throughout both of these guides describe how to configure screen options using the [set security screen *screen-name*] CLI statements. Instead, you should use the [set security screen ids-option *screen-name*] CLI statements. All screen configuration options are located in the [set security screen ids-option *screen-name*] level of the configuration hierarchy.

List of Technical Publications

The following sections list hardware and software guides and release notes for SRX-series services gateways running JUNOS software.

All documents are available at http://www.juniper.net/techpubs/.

Hardware Guides

- *SRX 5600 Services Gateway Hardware Guide*—Describes hardware components, installation, basic configuration, and basic troubleshooting procedures for the SRX 5600 services gateway. This guide explains how to prepare a site, unpack and install the device, replace device hardware, establish basic connectivity, and perform routine maintenance.
- *SRX 5800 Services Gateway Hardware Guide*—Describes hardware components, installation, basic configuration, and basic troubleshooting procedures for the SRX 5800 services gateway. This guide explains how to prepare a site, unpack and install the device, replace device hardware, establish basic connectivity, and perform routine maintenance.

Software Guides

- *JUNOS Software Interfaces and Routing Configuration Guide*—Explains how to configure SRX-series and J-series interfaces for basic IP routing with standard routing protocols, ISDN service, firewall filters (access control lists), and class-of-service (CoS) traffic classification.
- *JUNOS Software Security Configuration Guide*—Explains how to configure and manage SRX-series and J-series security services such as stateful firewall policies, IPsec VPNs, firewall screens, Network Address Translation (NAT), Public Key Cryptography, chassis clusters, Application Layer Gateways (ALGs), and Intrusion Detection and Prevention (IDP).
- *JUNOS Software Administration Guide*—Shows how to monitor SRX-series and J-series devices and routing operations, firewall and security services, system alarms and events, and network performance. This guide also shows how to administer user authentication and access, upgrade software, and diagnose common problems.
- *JUNOS Software CLI Reference*—Provides the complete configuration hierarchy available on SRX-series and J-series devices. This guide also describes the configuration statements and operational mode commands unique to these devices.
- *JUNOS Network Management Configuration Guide*—Describes enterprise-specific MIBs for JUNOS software. The information in this guide is applicable to M-series, T-series, EX-series, SRX-series, and J-series devices.
- *JUNOS System Log Messages Reference*—Describes how to access and interpret system log messages generated by JUNOS software modules and provides a reference page for each message. The information in this guide is applicable to M-series, T-series, EX-series, SRX-series, and J-series devices.

Release Notes

- *JUNOS Software for SRX-series Services Gateways Release Notes*—Summarizes new features and known problems for SRX-series services gateways and the JUNOS software running on those devices. The release notes also contain corrections and updates to the manuals and software upgrade and downgrade instructions.

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

September 2008—Revision 2, Release 9.2R2 of JUNOS software.