Junos OS Release 18.2R1 for cSRX Release Notes

Release 18.2R1
28 June 2018
Revision 1

Contents

Introduction

This release note accompanies Junos OS Release 18.2R1 for the cSRX Container Firewall, a containerized version of the SRX Series Services Gateway. It describes the new features, known behavior, and known and resolved problems in the software.

New and Changed Features

This section describes new features as well as enhancements to existing features starting in Junos OS Release 18.2R1 for cSRX support.

New Features in Junos OS Release 18.2R1 for cSRX

Security Policies

- **Support for unified policies (SRX Series, cSRX)**—Starting in Junos OS Release 18.2R1, unified policies are now supported on all SRX Series devices, allowing granular control and enforcement of dynamic Layer 7 applications within the traditional security policy.

  Unified policies are the security policies, where you can use dynamic applications as match conditions along with existing 5-tuple or 6-tuple matching conditions (with user firewall) to detect application changes over time, and allow you to enforce a set of rules for the transit traffic.

  Unified policies allow you to use dynamic application as one of the policy match criteria rule in each application. Application identification (AppID) is applied on the traffic, and the application is identified after several packets are checked.

  Before identifying the final application, the policy cannot be matched precisely. A potential policy list is made available, and the traffic is permitted using the potential policy from the list.

  After the application is identified, the final policy is applied to the session. Policy actions such as permit, deny, reject, or redirect is applied on the traffic as per the policy rules.

The following features support unified policies:

- **Application Identification (AppID)**—Unified policy leverages the application identity information from the Application Identification (AppID). AppID provides the information such as dynamic application classification, default protocol and port of an application. For any application included in the dependent list of another application, AppID provides this information.

  [See Application Identification Support for Unified Policies.]

- **Application firewall (AppFW)**—Unified policy configuration handles AppFW functionality and simplifies the task of configuring firewall policy to permit or block application traffic from the network.

  If you configure a unified policy with a dynamic application as one of the matching conditions, then the configuration eliminates the additional steps involved in AppFW configuration—that is, configuring a security policy to invoke the application firewall service.

  Starting in Junos OS Release 18.2R1, the Application Firewall (AppFW) functionality is deprecated— rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.

  The **[edit security application-firewall]** hierarchy and all configuration options under this hierarchy are deprecated.

- **Application Quality of Service (AppQoS)**—AppQoS functionality is supported when the device is configured with unified policies. You can configure a default AppQoS rule set to manage unified policy conflicts, if multiple security policies match the traffic.

- **ICAP service redirect**—Internet Content Adaptation Protocol (ICAP) service redirect functionality is supported when the device is configured with unified policies.

- **IDP**—Starting with Junos OS Release 18.2R1, with unified policies support, when a security rule has IDP enabled, the name of the actual IDP policy is replaced. This is to simplify IDP policy usage and to provide flexibility to have multiple policies active at the same time.

  All IDP matches will now be handled within the unified policies. As a part of session interest check IDP will enabled if IDP policy is present in any of the matched rules.

  IDP policy is activated in security policies, by permitting the IDP policy within the application services using the **set security policies from-zone zone-name to-zone zone-name policy policy-name then permit application-services idp-policy idp-policy-name** command.

  Since IDP policy name is directly use in the security policy rule, the **[edit security idp active-policy policy-name]** statement is deprecated.

- **SSL proxy**—SSL proxy functionality is supported when the device is configured with unified policies. You can configure a default SSL proxy profile to manage unified policy conflicts, if multiple security policies match the traffic.

- **UTM**—A new dynamic-application policy match condition is added to SRX Series devices, allowing an administrator to more effectively control the behavior of Layer

7 applications. To accommodate Layer 7 application-based policies in UTM, the **[edit security utm default-configuration]** command is introduced. If any parameter in a specific UTM feature profile configuration is not configured, then the corresponding parameter from the UTM default configuration is applied.

Additionally, during the initial policy lookup phase which occurs prior to a dynamic application being identified, if there are multiple policies present in the potential policy list which contains different UTM profiles, the SRX Series device applies the default UTM profile until a more explicit match has occurred.

[See Unified threat management (UTM) support within Unified Policy.]

cSRX Architecture Illustration

cSRX Architecture

Figure 1 on page 4 is a high-level illustration of the cSRX architecture and Figure 2 on page 5 is a high-level illustration of a cSRX compute node in a Contrail Networking cloud environment.

For details about the cSRX architecture, see the *Overview* topic in cSRX Deployment Guide for Bare-Metal Linux Server and cSRX Deployment Guide for Contrail.

Figure 1: cSRX Architecture

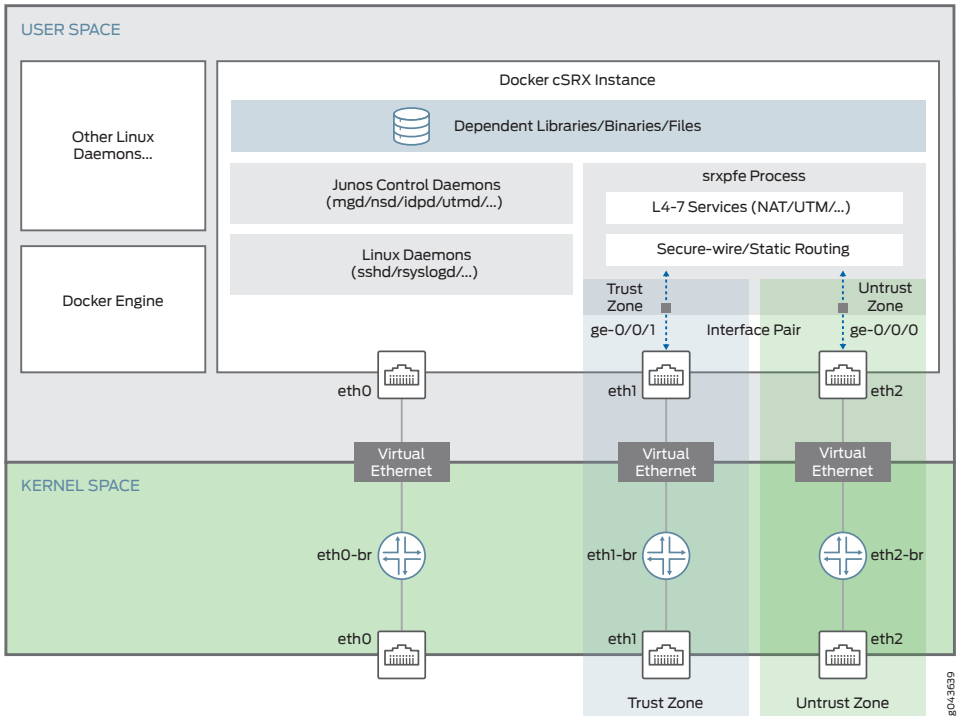
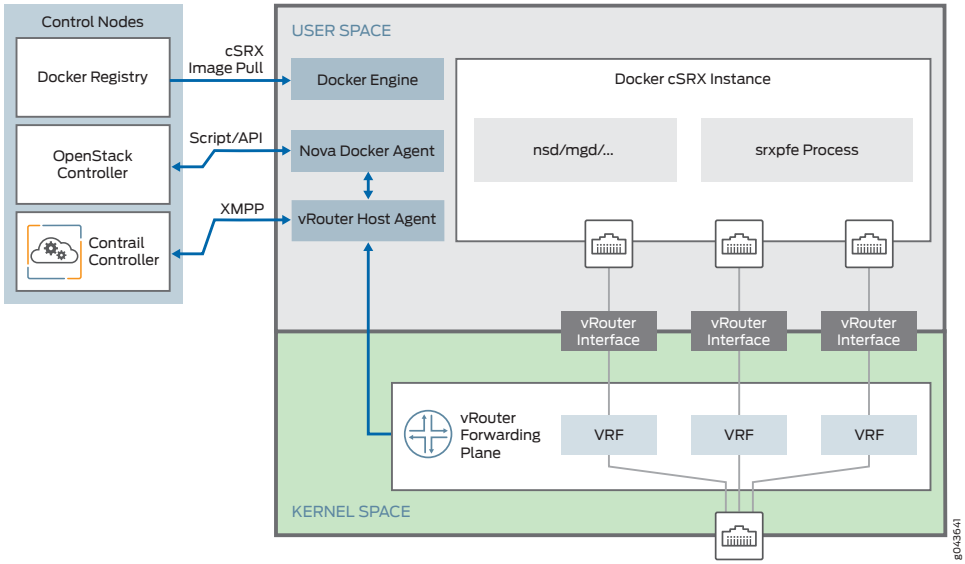


Figure 2: cSRX Architecture in Contrail



Supported Features

The cSRX Container Firewall inherits many of the branch SRX Series Junos OS features. This topic outlines the SRX series features supported by cSRX along with the features that are not applicable in a containerized environment.

SRX Series Features Supported on cSRX

Table 1 on page 5 provides a high-level summary of the feature categories supported on cSRX and any feature considerations.

To determine the Junos OS features supported on cSRX, 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. See Feature Explorer.

Table 1: SRX Series Features Supported on cSRX

Feature	Considerations
Application Firewall (AppFW)	Application Firewall Overview
Application Identification (AppID)	Understanding Application Identification Techniques
Application Tracking (AppTrack)	Understanding AppTrack
Basic firewall policy	Understanding Security Basics
Brute force attack mitigation	

Table 1: SRX Series Features Supported on cSRX (continued)

Feature	Considerations
Central management	CLI only. No J-Web support.
DDoS protection	DoS Attack Overview
DoS protection	DoS Attack Overview
Interfaces	Two revenue network interfaces (eth1, and eth2). Network Interfaces
Intrusion Detection and Prevention (IDP)	For SRX Series IPS configuration details, see: Understanding Intrusion Detection and Prevention for SRX Series
IPv4 and IPv6	Understanding IPv4 Addressing Understanding IPv6 Address Space
Jumbo frames	Understanding Jumbo Frames Support for Ethernet Interfaces
Malformed packet protection	
Network Address Translation (NAT)	For SRX Series NAT configuration details, see: Introduction to NAT
Routing	Basic Layer 3 forwarding with VLANs. Layer 2 through 3 forwarding functions: secure-wire forwarding or static routing forwarding
SYN cookie protection	Understanding SYN Cookie Protection
User Firewall	For SRX Series user firewall configuration details, see: Overview of Integrated User Firewall
Unified Threat Management (UTM)	For SRX Series UTM configuration details, see: Unified Threat Management Overview For SRX Series UTM antispam configuration details, see: Antispam Filtering Overview
Zones and zone-based IP spoofing	Understanding IP Spoofing

SRX Series Features Not Supported on cSRX

Table 2 on page 7 lists SRX Series features that are not applicable in a containerized environment, that are not currently supported, or that have qualified support on cSRX.

Table 2: SRX Series Features Not Supported on cSRX

	SRX Series Feature
Application Layer Gateways	
	Avaya H.323
Authentication with IC Series Devices	
	Layer 2 enforcement in UAC deployments NOTE: UAC-IDP and UAC-UTM also are not supported.
Class of Service	
	High-priority queue on SPC
	Tunnels
Data Plane Security Log Messages (Stream Mode)	
	TLS protocol
Diagnostics Tools	
	Flow monitoring cflowd version 9
	Ping Ethernet (CFM)
	Traceroute Ethernet (CFM)
DNS Proxy	
	Dynamic DNS
Ethernet Link Aggregation	
	LACP in standalone or chassis cluster mode
	Layer 3 LAG on routed ports
	Static LAG in standalone or chassis cluster mode
Ethernet Link Fault Management	
	Physical interface (encapsulations)
	ethernet-ccc **ethernet-tcc**

Table 2: SRX Series Features Not Supported on cSRX (continued)

	SRX Series Feature
	extended-vlan-ccc **extended-vlan-tcc**
	Interface family
	ccc, **tcc**
	ethernet-switching
Flow-Based and Packet-Based Processing	
	End-to-end packet debugging
	Network processor bundling
	Services offloading
Interfaces	
	Aggregated Ethernet interface
	IEEE 802.1X dynamic VLAN assignment
	IEEE 802.1X MAC bypass
	IEEE 802.1X port-based authentication control with multisupplicant support
	Interleaving using MLFR
	PoE
	PPP interface
	PPPoE-based radio-to-router protocol
	PPPoE interface
	Promiscuous mode on interfaces
IP Security and VPNs	
	Acadia - Clientless VPN
	DVPN
	Hardware IPsec (bulk crypto) Cavium/RMI
	IPsec tunnel termination in routing instances

Table 2: SRX Series Features Not Supported on cSRX (continued)

	SRX Series Feature
	Multicast for AutoVPN
	Suite B implementation for IPsec VPN
IPv6 Support	
	DS-Lite concentrator (also known as AFTR)
	DS-Lite initiator (also known as B4)
Log File Formats for System (Control Plane) Logs	
	Binary format (binary)
	WELF
Miscellaneous	
	AppQoS
	Chassis cluster
	GPRS
	Hardware acceleration
	High availability
	J-Web
	Logical systems
	MPLS
	Outbound SSH
	Remote instance access
	RESTCONF
	Sky ATP
	SNMP
	Spotlight Secure integration
	USB modem
	Wireless LAN

Table 2: SRX Series Features Not Supported on cSRX (continued)

	SRX Series Feature
MPLS	
	CCC and TCC
	Layer 2 VPNs for Ethernet connections
Network Address Translation	
	Maximize persistent NAT bindings
Packet Capture	
	Packet capture NOTE: Only supported on physical interfaces and tunnel interfaces, such as *gr*, *ip*, and *st0*. Packet capture is not supported on a redundant Ethernet interface (*reth*).
Routing	
	BGP extensions for IPv6
	BGP Flowspec
	BGP route reflector
	Bidirectional Forwarding Detection (BFD) for BGP
	CRTP
Switching	
	Layer 3 Q-in-Q VLAN tagging
Transparent Mode	
	UTM
Unified Threat Management	
	Express AV
	Kaspersky AV
Upgrading and Rebooting	
	Autorecovery
	Boot instance configuration
	Boot instance recovery

Table 2: SRX Series Features Not Supported on cSRX (continued)

	SRX Series Feature
	Dual-root partitioning
	OS rollback
User Interfaces	
	NSM
	SRC application
	Junos Space Virtual Director

Changes in Behavior and Syntax

This section lists the changes in behavior of Junos OS features and changes from Junos OS Release 18.2R1 for the cSRX. For the most complete and latest information about changes in command behavior and syntax applicable to all SRX Series platforms in Junos OS Release 18.2R1, see Changes in Behavior and Syntax for SRX.

Application System Cache for Application Services (SRX Series, cSRX Instances)

Starting with Junos OS 18.2R1, the default behavior of the ASC has changed as follows:

- Security services such as security policies, application firewall (AppFW), Juniper Sky ATP, IDP, and UTM do not use the ASC by default.
- Miscellaneous services such as APBR and AppTrack use the ASC for application identification by default.

NOTE: The change in the default behavior of the ASC affects the legacy Application Firewall (AppFW) functionality. With the ASC disabled by default for the security services starting in Junos OS Release 18.2 onwards, the AppFW will not use the entries present in the ASC.

You can revert to the ASC behavior as in Junos OS releases prior to 18.2 by using the **set services application-identification application-system-cache security-services** command.

CAUTION: The SRX Series device may become susceptible to application evasion techniques if the ASC is enabled for security services. We recommend that you enable the ASC only when the performance of the device in its default configuration (disabled for security services) is not sufficient for your specific use case.

Use the following commands to enable or disable the ASC:

- Enable the ASC for security services:

  user@host# set services application-identification application-system-cache security-services

- Disable the ASC for miscellaneous services:

  user@host# set services application-identification application-system-cache no-miscellaneous-services

- Disable the enabled ASC for security services:

  user@host# delete services application-identification application-system-cache security-services

- Enable the disabled ASC for miscellaneous services:

  user@host# delete services application-identification application-system-cache no-miscellaneous-services

You can use the **show services application-identification application-system-cache** command to verify the status of the ASC.

The following sample output provides the status of the ASC:

```
user@host>show services application-identification application-system-cache
Application System Cache Configurations:
  application-cache: on
```

```
  Cache lookup for security-services: off
  Cache lookup for miscellaneous-services: on
cache-entry-timeout: 3600 seconds
```

For Junos OS Release prior to 18.2R1, application caching is turned on by default. You can manually turn this caching off using the CLI.

```
user@host# set services application-identification no-application-system-cache
```

Known Behavior

This section contains the known behaviors and limitations in Junos OS Release 18.2R1 for cSRX.

cSRX in Contrail

- Web console does not support a cSRX container in the OpenStack Dashboard. This is an expected limitation since cSRX is a container deployed in the OpenStack environment and is not a Virtual Machine (VM) deployed in a hypervisor. PR1308835
- The Docker node may run out of space due to a terminated container's cache not being properly cleaned, which will result in a failure to deploy the cSRX container. If you perform a cleanup of the Docker cache the Docker node returns to normal operation. PR1315154

Known Issues

This section lists the known issues in Junos OS Release 18.2R1 for cSRX.

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

cSRX in Contrail

- When configuring cSRX in Contrail, there is a limitation with the use of an Openstack user date file and XML tag names. For, example, if you use an Openstack user date file that includes **<size><small | middle | large></size>** in the file, the cSRX flavor will remain at the small default setting. You must pass configuration settings by using Openstack metadata and the available cSRX environment variables. You can, however, use an Openstack user date file to pass a Junos configuration in <conf></conf/> and <boot_script></script> for cSRX boot-time configuration, but excluding the cSRX-specific XML tags. PR1310158

  Workaround: To change a configuration setting for the cSRX container, pass the configuration setting by including the **–meta** option in the **nova boot** command. See the cSRX Deployment Guide for Contrail for details.

- When configuring cSRX in a Contrail service chain, the service chain does not support traffic forwarding in secure-wire mode. PR1323762

Workaround: The cSRX uses routing as the default environment variable for traffic forwarding mode. Do not change the traffic forwarding mode of the cSRX container to secure-wire mode. See the cSRX Deployment Guide for Contrail for details.

Resolved Issues

This section lists the issues that have been fixed in the Junos OS Release 18.2R1.

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

cSRX in Contrail

- In certain cases, you might find that you are unable to properly configure the cSRX container when operating under the following conditions: PR1326218
  - Poll mode–After running the cSRX container for a long duration (hours or days), and operating under a stress of over 1 to 3 GB of UDP traffic and around 520K UDP sessions, the cSRX cannot be properly configured (for example, attempting to configure a new IPv6 address on ge-0/0/0 or ge-0/0/1).

    Workaround: Launch a new cSRX container if you encounter this behavior.
  - Interrupt mode–After running the cSRX container for a long duration (hours or days), and operating under a stress of 200 packets per second (pps) TCP traffic and 300 to 500 TCP sessions, the cSRX does not allow new configurations or may stop forwarding traffic.

    Workaround: Reduce the load on the cSRX container while sending stress traffic for long durations. If this does not resolve the issue, launch a new cSRX container.
- You cannot configure pre-defined IDP policies from policy templates for a cSRX instance. The issue occurs because the **set system scripts commit file templates.xsl** command to load the pre-defined policy templates in cSRX is not available.PR1338101

System Requirements by Environment

The topics below provide detailed system requirement specifications for each supported environment for a cSRX deployment.

- For a bare-metal Linux server deployment, see the *Host Requirements* topic in the cSRX Deployment Guide for Bare-Metal Linux Server.
- For a Contrail deployment, see the *Platform and Server Requirements* topic in the cSRX Deployment Guide for Contrail.

Finding More Information

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

https://prsearch.juniper.net

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

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 provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at https://www.juniper.net/documentation/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at https://www.juniper.net/documentation/feedback/.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software 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 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://prsearch.juniper.net/
- 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, see https://www.juniper.net/support/requesting-support.html.

Revision History

28 June 2018 —Revision 1— Junos OS 18.2R1 – cSRX.