Junos OS Release 20.2R1 for cSRX Release Notes

Release 20.1R1
30 June 2020
Revision 1

Contents

Introduction

These release notes accompany Junos OS Release 20.2R1 for the cSRX Container Firewall, a containerized version of the SRX Series Services Gateway. They describe the new features, known limitations, and known and resolved problems in the software.

The cSRX Container Firewall is a containerized version of the SRX Series Services Gateway with a low memory footprint. cSRX provides advanced security services, including, Content security, AppSecure, and Unified Threat Management (UTM) in a container form factor.

By using a Docker container in a Linux server, the cSRX can substantially reduce overhead because each container shares the Linux host's OS kernel. Regardless of how many containers a Linux server hosts, only one OS instance is in use. Also, because of the containers' lightweight quality, a server can host many more container instances than it can virtual machines (VMs), yielding tremendous improvements in utilization. With its small footprint and Docker as a container management system, the cSRX Container Firewall enables agile, high-density security service deployment.

What's New

IN THIS SECTION

This section describes new features as well as enhancements to existing features starting in Junos OS Release 20.2R1 for cSRX support.

Licensing

- **Juniper Agile Licensing support for cSRX**—Starting in cSRX 20.2R1, Juniper Agile Licensing supports the cSRX Container Firewall, a containerized version of the SRX Series Services Gateway.

  Juniper Agile Licensing provides simplified and centralized license administration and deployment. Using Juniper Agile Licensing, you can install and manage licenses for hardware and software features.

  You require new license keys to use the licenses for cSRX Container Firewall features. Contact Customer Care for exchanging license keys earlier than cSRX 20.2R1.

  [See Flex Software Subscription Model Support, Juniper Agile Licensing Guide, and Managing cSRX Licenses]

Security

- **Contrail network support (cSRX)**—Starting in Junos OS Release 20.2R1, we have integrated cSRX Container Firewall into a Contrail network as a distributed host-based firewall service on a Docker container. Using this deployment, you can obtain agile, elastic, and cost-saving security services.

  The new virtual solution provides the following capabilities:

  - Layer 7 security protection (antivirus, application firewall, IPS, application identification, URL filtering, user firewall, UTM content and Web filtering only)
  - Automated service provisioning and orchestration
  - Distributed and multitenant traffic securing
  - Centralized management with Junos Space Security Director, including dynamic policy and address update, remote log collections, and security events monitoring
  - Scalable security services with small footprints

  [See cSRX as Contrail Host-based Firewall User Guide.]

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 supported in a containerized environment.

SRX Series Features Supported on cSRX

Table 1 on page 4 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	-
Central management	CLI and Security Director only. No J-Web support.
DDoS protection	DoS Attack Overview
DoS protection	DoS Attack Overview
Interfaces	Upto 15 revenue interfaces 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	-

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

Feature	Considerations
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 5 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.

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

	SRX Series Feature
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**
	extended-vlan-ccc **extended-vlan-tcc**
	Interface family

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

	SRX Series Feature
	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
IPSec and VPNs	Not supported
IPv6 Support	
	DS-Lite concentrator (also known as AFTR)
	DS-Lite initiator (also known as B4)

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

	SRX Series Feature
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
	Juniper Sky ATP
	SNMP
	Spotlight Secure integration
	USB modem
	Wireless LAN
MPLS	

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

	SRX Series Feature
	CCC and TCC
	Layer 2 VPNs for Ethernet connections
Network Address Translation	
	Maximize persistent NAT bindings
Packet Capture	
	Packet capture
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

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

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

What's Changed

Learn about what changed in Junos OS main releases for cSRX.

This section lists the changes in behavior of Junos OS features and changes from Junos OS Release 20.2R1 for the cSRX.

Application System Cache for Application Services (SRX Series and 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, 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 might 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 releases 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 Limitations

There are no known system maximums, or limitations in hardware and software in Junos OS Release 20.2R1 for cSRX.

Open Issues

There are no open issues in Junos OS Release 20.2R1 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.

Resolved Issues

There are no resolved issues in Junos OS Release 20.2R1 for cSRX.

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

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 Requirements for Deploying cSRX Container on Contrail vRouter topic in the cSRX as Contrail Host-Based Firewall User Guide.

Accessing the cSRX Image

The cSRX image is now available from the support download site, similar to other Junos OS Platform images starting in Junos OS Release 20.2R1.

- For a cSRX on bare-metal Linux server deployment, see the Loading the cSRX Image topic in the cSRX Deployment Guide for Bare-Metal Linux Server.

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/

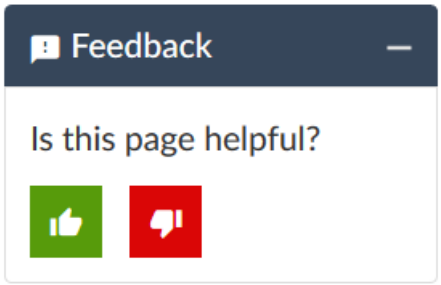
Juniper Networks Content Explorer is a Web-based application that helps you explore Juniper Networks technical documentation by product, task, and software release, and download documentation in PDF format. Find Content Explorer at

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 system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:



  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide 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

30 June 2020—Revision 1— Junos OS 20.2R1 – cSRX.