Juniper Networks | Engineering Simplicity

cSRX Container Firewall as Contrail Host-Based Firewall User Guide

Published
2023-06-19

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

cSRX Container Firewall as Contrail Host-Based Firewall User Guide
Copyright © 2023 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide

Use this guide to install the containerized security gateway application on Contrail vRouter.

1

CHAPTER

Introduction

Understanding cSRX Container Firewall on Contrail Host-Based Firewall

IN THIS SECTION

Containerized SRX (cSRX Container Firewall) is a virtual security solution, which is integrated into a Contrail networking as distributed host-based firewall (HBF) service. cSRX Container Firewall is built based on Docker container to deliver agile, elastic, and cost-saving security services. The cSRX Container Firewall Container Firewall is a containerized version of the SRX Series Services Gateway with a low-memory footprint. cSRX Container Firewall provides advanced security services, including content security, AppSecure, and Content Security in a container.

cSRX Container Firewall Overview

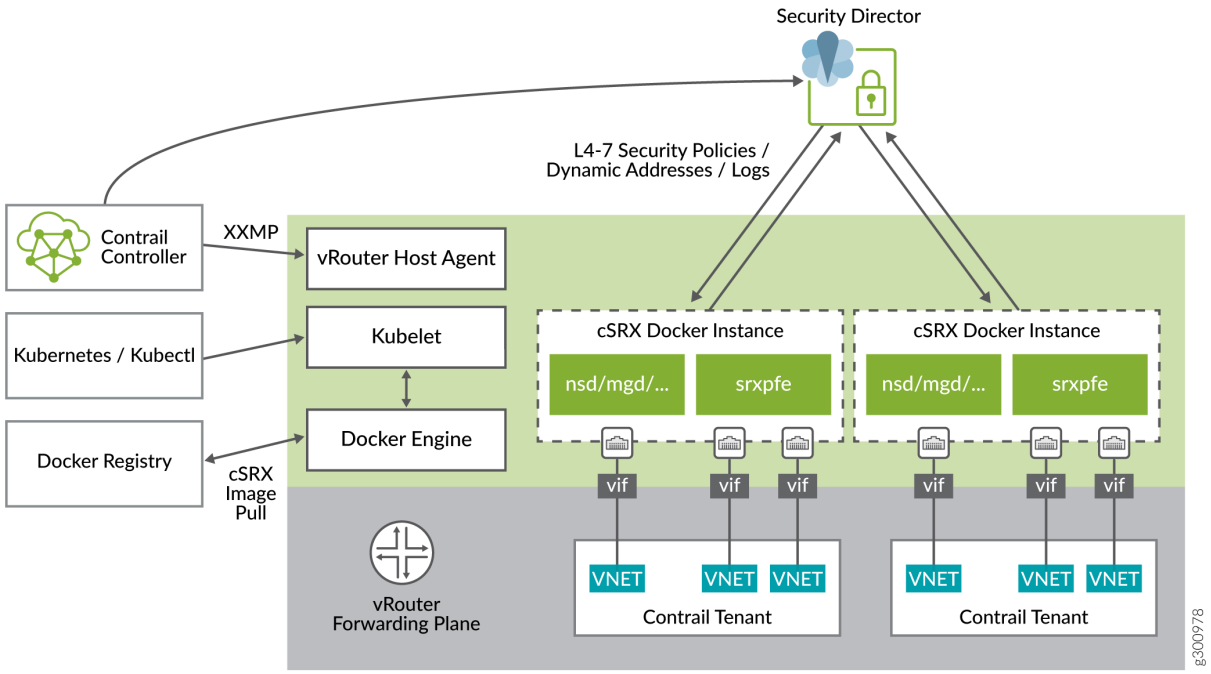
The cSRX Container Firewall Container Firewall deploys as a single container on a Docker Engine compute node running in a Contrail cluster. It runs on a Linux bare-metal server as the hosting platform for the Docker container environment. The cSRX Container Firewall container packages all the dependent processes (or daemons) and libraries to support the different Linux host distribution methods (Ubuntu, Red Hat Enterprise Linux, or CentOS).

When the cSRX Container Firewall container runs, there are several processes (or daemons) inside the Docker container that launch automatically when cSRX Container Firewall becomes active. Some daemons support Linux features, providing the same service as if they are running on a Linux host (for example, sshd, rsyslogd, and monit). Other daemons are compiled and ported from Junos OS to perform configuration and control jobs for security service (for example, MGD, NSD, Content Security, IDP, and AppID). srxpfe is the data plane daemon that receives and sends packets from the revenue ports of a cSRX Container Firewall container. cSRX Container Firewall uses srxpfe for Layer 2 through 3 forwarding functions as well as for Layer 4 through 7 network security services.

The distributed software security solution is built on top of Contrail Networking using Contrail Controller and Contrail vRouter to prevent threats in a customer's multi-cloud environment.

When cSRX Container Firewall acts as distributed firewall service on Contrail, Kubernetes is used to orchestrate cSRX Container Firewall instances on compute nodes. The Kubernetes API server can respond to Contrail Controller after HBF policies are configured on the Contrail user interface. A cSRX Container Firewall image is pulled from the Docker registry to compute nodes after the instances are provisioned.

Figure 1: cSRX Container Firewall on Contrail Host-Based Firewall



Contrail Security includes an integrated virtual router (vRouter) that acts as a distributed element on every host where cSRX Container Firewall application is created. The vRouter enforces security at Layers 4–7 by monitoring traffic flows and redirecting suspicious traffic to next-generation firewalls.

After provisioning the cSRX Container Firewall instances:

- Three VIFs connect the cSRX Container Firewall instance to vRouter.
  - The Management interface is connected to the management virtual network.
  - Two secure data interfaces are connected to the left and right virtual networks, receiving packets steered from vRouter and sending packets to vRouter after security check.

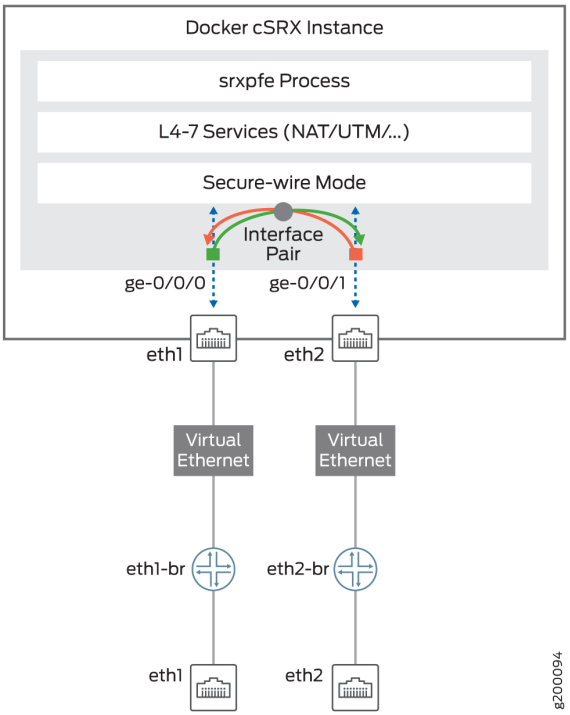
- Security Director updates L7 security policies and dynamic addresses to cSRX Container Firewall instances.
- cSRX Container Firewall instances send security logs to Security Director.
- Each tenant that needs HBF service will start a private cSRX Container Firewall instance on the compute node.

With Contrail Security, you can define policies and automatically distribute them across all deployments. You can also monitor and troubleshoot traffic flows inside each cSRX Container Firewall instance and across cSRX Container Firewall instances.

In Contrail HBF, the cSRX Container Firewall Container Firewall is supported only in secure-wire mode and enables advanced security at the network edge in a multitenant virtualized environment. cSRX Container Firewall provides Layer 4 through 7 advanced security features such as firewall, IPS, and AppSecure. The cSRX Container Firewall container also provides an additional interface to manage cSRX Container Firewall. When cSRX Container Firewall is operating in Layer 2 mode, incoming Layer 2 frames from one interface go through Layer 4 through 7 processing based on the configured cSRX Container Firewall services. cSRX Container Firewall then sends the frames out of the other interface. The cSRX Container Firewall container either allows the frames to pass through unaltered or drops the frames, based on the configured security policies.

Figure 2 on page 5 illustrates the cSRX Container Firewall operating in secure-wire mode.

Figure 2: cSRX Container Firewall in Secure-Wire Mode

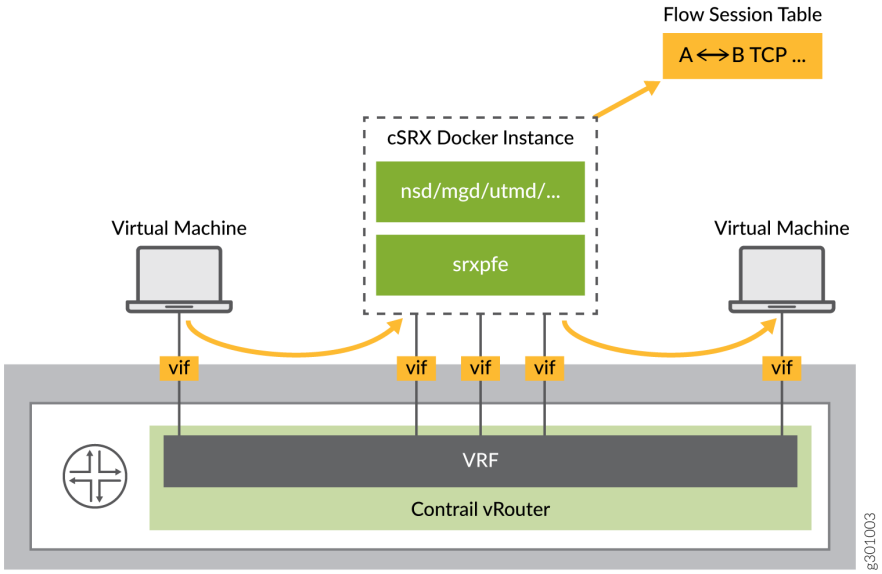


cSRX Container Firewall Deployment Modes

Secure Traffic Inside Compute Node

When cSRX Container Firewall is securing traffic inside a compute node, vRouter will steer all traffic to cSRX Container Firewall which match HBF filter. Flow sessions are created for the traffic sent from vRouter to cSRX Container Firewall. After L7 security check in cSRX Container Firewall, traffic is sent back to vRouter and forwarded to the destination as shown in Figure 3 on page 6.

Figure 3: Secure Traffic Inside Compute Node

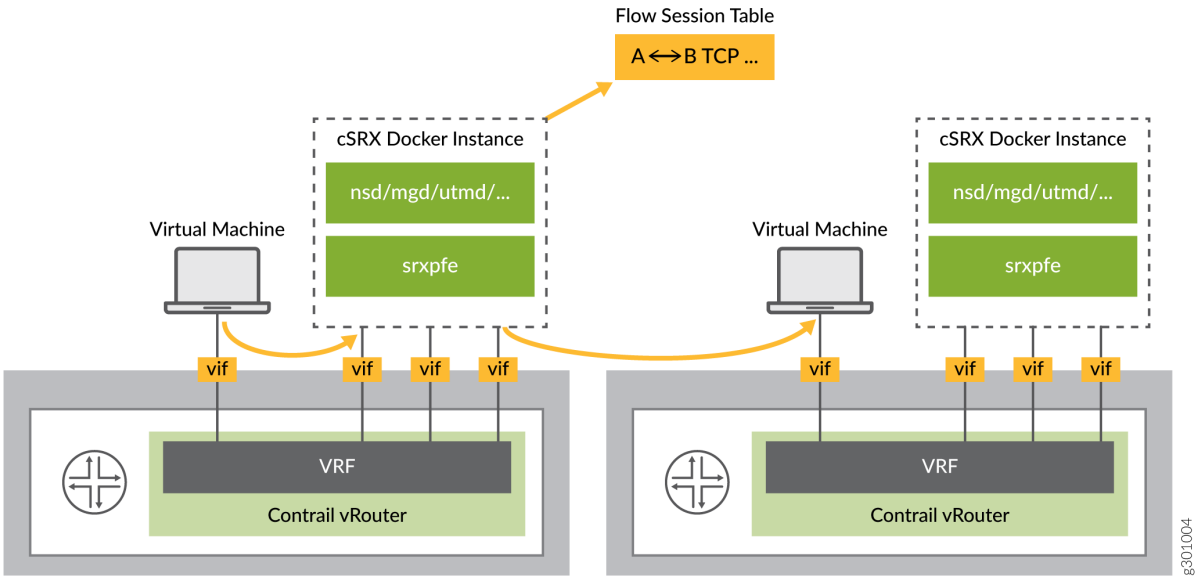


- cSRX Container Firewall works in bump-in-the-wire mode with two data interfaces connected to vRouter
- vRouter filter traffic to cSRX Container Firewall VIF which needs L4-7 security check
- After L4-7 security check, traffic is sent back to vRouter

Secure Traffic Cross Compute Nodes

cSRX Container Firewall works the same as when it is securing the traffic inside the compute node. The difference is, vRouter needs to guarantee that traffic is steered to same cSRX Container Firewall instance when traffic is crossing different compute nodes, so cSRX Container Firewall flow sessions are created and matched in same cSRX Container Firewall instance on both directions.

Figure 4: Secure Traffic Cross Compute Nodes

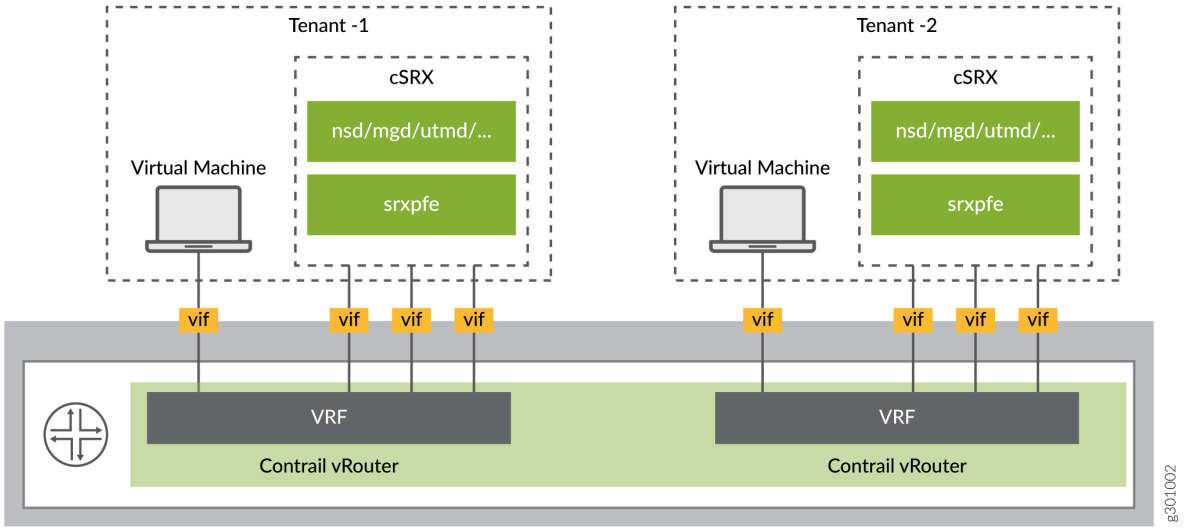


Multitenant Support

For supporting multitenancy, there is separate cSRX Container Firewall instance started for each tenant on same compute node.

Figure 5 on page 8 shows the multitenancy support.

Figure 5: Multitenancy Support



Licensing

The cSRX Container Firewall Container Firewall software features require a license to activate the feature. To understand more about cSRX Container Firewall Container Firewall licenses, see cSRX Flex Software Subscription Model.

cSRX Container Firewall Benefits and Uses

The cSRX Container Firewall Container Firewall enables you to quickly introduce new firewall services, deliver customized services to customers, and scale security services based on dynamic needs. The cSRX Container Firewall container differs from VMs in several important ways. It runs with no guest OS overhead, has a notably smaller footprint, and is easier to migrate or download. The cSRX Container Firewall container uses less memory, and its spin-up time measures in subseconds—all leading to higher density at a lower cost. The boot time is reduced from several minutes with a VM-based environment to less than a few seconds for the cSRX Container Firewall container. cSRX Container Firewall is ideal for public, private, and hybrid cloud environments.

The virtual solution provides the following capabilities:

- Layer 7 security services such as firewall, intrusion prevention system (IPS), and AppSecure

- Automated service provisioning and orchestration
- Distributed and multitenant traffic securing
- Centralized management with Junos Space Security Director, including dynamic policy/address update, remote log collections, and security events monitoring
- Scalable security services with small footprints

You can deploy the cSRX Container Firewall Container Firewall in the following scenario:

- Contrail microsegmentation–Within a Contrail environment running mixed workloads of VMs and containers, cSRX Container Firewall can provide security for Layer 4 through 7 traffic, managed by Security Director.

Junos OS Features Supported in cSRX Container Firewall for Contrail HBF

cSRX Container Firewall provides Layer 4 through 7 secure services for a Contrail HBF in a containerized environment.Table 1 on page 9 provides a high-level summary of the security features supported on cSRX Container Firewall.

To determine the Junos OS features supported on cSRX Container Firewall, 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: Security Features Supported on cSRX Container Firewall HBF

Security Features	Considerations
Application Tracking (AppTrack)	Understanding AppTrack
Application Firewall (AppFW)	Application Firewall Overview
Application Identification (AppID)	Understanding Application Identification Techniques
Basic Firewall Policy	Understanding Security Basics

Table 1: Security Features Supported on cSRX Container Firewall HBF *(Continued)*

Security Features	Considerations
Brute force attack mitigation	
DoS/DDoS protection	DoS Attack Overview DoS Attack Overview
Intrusion Prevention System (IPS)	For SRX Series IPS configuration details, see: Understanding Intrusion Detection and Prevention for SRX Series
IPv4	Understanding IPv4 Addressing
Interfaces	Supports two revenue (ge) interfaces. Out-of-band management Interface (eth0 In-band interfaces (ge-0/0/0 to ge-0/0/1)
Jumbo Frames	Understanding Jumbo Frames Support for Ethernet Interfaces
SYN cookie protection	Understanding SYN Cookie Protection
Malformed packet protection	
Routing	Supports secure-wire mode forwarding only.

Table 1: Security Features Supported on cSRX Container Firewall HBF *(Continued)*

Security Features	Considerations
Content Security	Includes support for all Content Security functionality on the cSRX Container Firewall platform, such as: • Antispam • Sophos Antivirus • Web filtering • Content filtering For SRX Series Content Security configuration details, see: Unified Threat Management Overview For SRX Series Content Security antispam configuration details, see: Antispam Filtering Overview
User Firewall	Includes support for all user firewall functionality on the cSRX Container Firewall platform, such as: • Policy enforcement with matching source identity criteria • Logging with source identity information • Integrated user firewall with active directory • Local authentication For SRX Series user firewall configuration details, see: Overview of Integrated User Firewall
Zones and Zone based IP spoofing	Understanding IP Spoofing

2

CHAPTER

Integrating cSRX Container Firewall into a Contrail Networking

Requirements for Deploying cSRX Container Firewall Container on Contrail vRouter

IN THIS SECTION

This topic discusses the requirements for integrating cSRX Container Firewall into Contrail cluster.

Contrail Requirements

Table 2 on page 13 lists the supported platforms and server requirements.

Table 2: Supported Platforms and Server Requirements

Component	Specification	Release
Contrail Networking		2005
Ubuntu		14.04 and newer
CentOS		6.5 and newer
Redhat		7.0 and newer
vCPU	2 CPU cores	
Memory	8 GB	

Table 2: Supported Platforms and Server Requirements *(Continued)*

Component	Specification	Release
Disk space	40 GB	
Network Interfaces	2 Revenue Interfaces	

cSRX Container Firewall Container Interfaces

Table 3 on page 14 lists the cSRX Container Firewall container interfaces.

Table 3: cSRX Container Firewall Container Interfaces

Interfaces	Purpose	Created By
eth0	Management Interface	Orchestrator
eth1	ge-0/0/0	Orchestrator
eth2	ge-0/0/1	Orchestrator
lo	Loopback	Docker Engine

cSRX Container Firewall Basic Configuration Settings

The cSRX Container Firewall container requires the following basic configuration settings:

- Interfaces must be bound to security zones.
- Policies must be configured between zones to permit or deny traffic.

cSRX Container Firewall Virtual Security Solution on Contrail vRouter

IN THIS SECTION

Before you deploy the cSRX Container Firewall Container Firewall as an advanced security service in the Contrail Networking cloud environment, ensure that you:

- Review "Requirements for Deploying cSRX Container Firewall Container on Contrail vRouter" on page 13 for deploying a cSRX Container Firewall container in a compute node.

Deploying a cSRX Container Firewall POD with Kubernetes

Kubernetes is enhanced to support multiple interfaces all supported by a single Contrail Container Network Interface (CNI) (Network Provider). The cSRX Container Firewall container can be orchestrated on compute nodes and attached to multiple virtual networks. For a single cSRX Container Firewall container, those virtual networks are either attached for management purposes or used to collect traffic from vRouter. A cSRX Container Firewall POD can be deployed with a YAML template in Kubernetes.

To deploy a cSRX Container Firewall POD, see Host-Based Firewalls on a compute node.

3

CHAPTER

Managing cSRX Container Firewall

Debugging and Managing cSRX Container Firewall

IN THIS SECTION

Stop a cSRX Container Firewall POD

By default, cSRX Container Firewall will not mount any external volumes from compute node. When a new cSRX Container Firewall instance is started, it will synchronize configuration from Security Director. Any syslog and security logs will be posted to Security Director as well. So cSRX Container Firewall POD can be stopped and destroyed directly by Contrail Service Orchestration (CSO).

To stop the cSRX Container Firewall POD:

- Run the Docker command to stop cSRX Container Firewall.

  # **kubectl delete -f <csrx-yaml-file>**

  After the cSRX Container Firewall POD is stopped and destroyed, compute and storage resources of this cSRX Container Firewall POD are released.

kubectl delete -f <csrx-yaml-file>

Verify Network Name

To verify the network name:

Run the following command to check the network name:

kubectl get network-attachment-definitions -n

Verify Logs

To view and verify logs:

1. Run the following command to access the path for log details:

   # **cat /var/log/contrail/**

2. Run the following command to view the logs:

   # **kubectl describe pods -n**