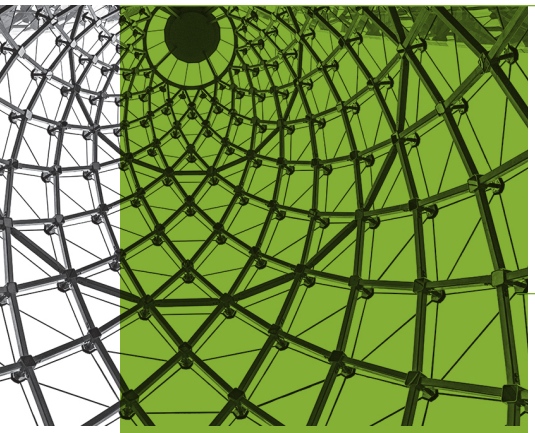

vSRX VIRTUAL FIREWALL FOR GOOGLE CLOUD PLATFORM

Product Overview

The vSRX Virtual Firewall delivers a complete cloud-native virtual firewall for Google Cloud Platform, including advanced security, secure SD-WAN, robust networking, and automated virtual machine life-cycle management for service providers and enterprises. To activate a trial version of the vSRX for Google Cloud Platform, please visit the GCP marketplace.

Product Description

As workloads move to the public cloud, they introduce challenges around securing the data and communication between workloads running in the cloud and other locations.

Network and security professionals must perform a delicate balancing act, delivering the benefits of cloud technologies without undermining the organization's security. This challenge can only be met by a solution that keeps pace with evolving threats while matching the agility and scalability of cloud environments—without sacrificing reliability, visibility, and control.

Juniper Networks addresses these challenges head-on by extending the capabilities of the award-winning Juniper Networks® SRX Series Services Gateways as a cloud-native virtual firewall for Google Cloud Platform (GCP), empowering security professionals to deploy and scale firewall protection for workloads running within GCP. The Juniper Networks vSRX Virtual Firewall offers unparalleled next-generation firewall (NGFW) security that includes intrusion prevention system (IPS), malware protection, app control, and on-demand threat detection. The vSRX also supports secure communications with SD-WAN, GCP virtual networks, and SD-LAN for secure segmentation between workloads.

The vSRX for GCP automated provisioning capabilities allow network and security administrators to quickly and efficiently provision and scale firewall protection to meet the dynamic needs of cloud environments. By combining the vSRX with the power of Junos Space® Security Director or Contrail® Service Orchestration, administrators can significantly improve policy configuration, management, and visibility into both physical and virtual assets from a common, centralized platform.

Juniper is committed to helping customers realize the value of their existing investments and has committed to interoperability for all of its SRX Series firewalls. In addition to Security Director and Contrail Service Orchestration, the vSRX supports OpenContrail and other third-party management solutions. The vSRX can also integrate with other next-generation cloud orchestration tools such as OpenStack, either directly or through rich APIs.

In addition to public cloud and traditional virtualization use cases, the vSRX allows service providers and enterprises to deploy a secure SD-WAN fabric with edge defenses. The secure SD-WAN fabric is adaptable to any site's individual needs while also providing the flexibility to defend virtualized and service-oriented applications wherever they exist throughout the network.

Security Director can manage up to 25,000 SRX Series firewalls—whether physical, virtual, or containerized—from a single management instance. This tool allows organizations to manage, automate, and orchestrate network security, virtualization, and interconnectivity, from endpoint to edge and every cloud in between, from a single platform.

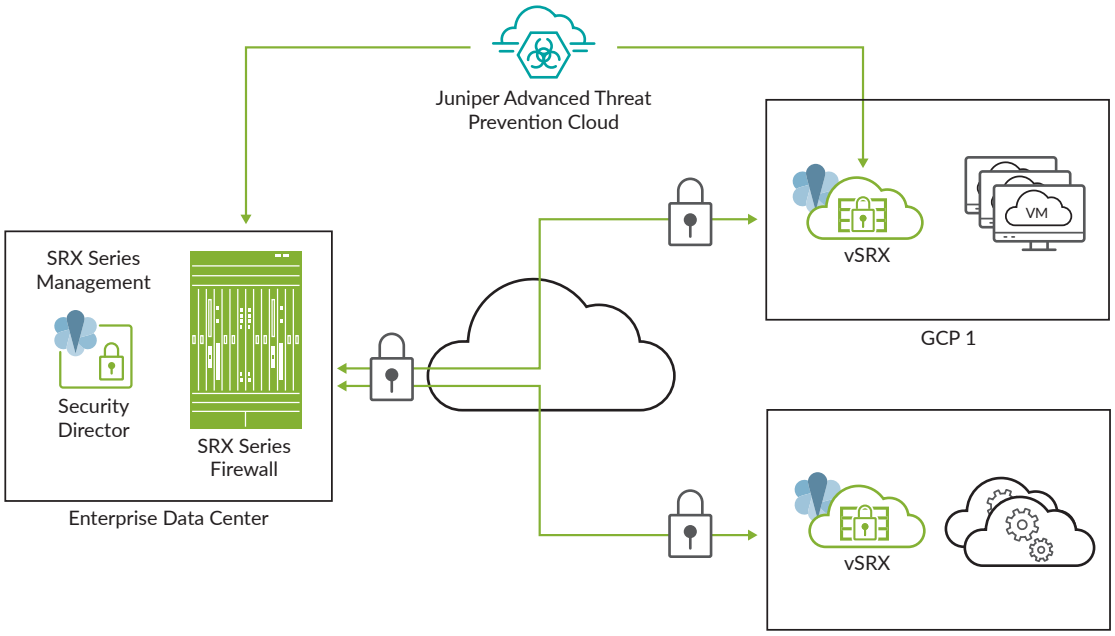

Figure 1: vSRX to secure workloads in GCP

Architecture and Key Components

Secure Connectivity

The vSRX on GCP can secure communications between workloads running in different virtual networks and/or an on-premises data center. The vSRX VPN capability allows for secure connectivity between virtual network peering in the same GCP region, and global virtual network peering across GCP regions. The VPN capability enables the vSRX to offer secure connectivity between GCP virtual networks without sending data flows over the Internet, which minimizes cost, latency, and availability concerns.

The vSRX Virtual Firewall can also use multiple connectivity options to connect sites securely. Whether virtual or physical to the enterprise WAN fabric, extending secure connectivity to other data centers (such as collocation of third-party cloud deployments) may need to communicate with the cloud workloads.

Secure SD-WAN

To access applications hosted in the Google Cloud, branch offices traditionally leverage connections through corporate campus locations to access GCP applications. In this situation, secure SD-WAN can be deployed at the branch and use vSRX on GCP to activate a more optimized solution for connectivity that goes directly to GCP, bypassing the need to access cloud applications through the campus network.

A vSRX deployed in GCP can act as an SD-WAN spoke or hub, supporting secure access between campus and branch locations and GCP directly as part of a larger SD-WAN deployment. It can also act as the SD-WAN hub, where it provides secure access to cloud resources hosted in GCP, becoming the central point for regionally based Internet breakouts. This central point allows the vSRX on GCP to secure workloads and provide secure SD-WAN connectivity that adapts to changing business needs.

Workload Protection

Firewalls protect workloads, but not all firewalls are created equal. With the vSRX on GCP, customers can ensure policies are consistently deployed across their entire network, whether those workloads operate on premises, in the public cloud, or at the edge. Customers already using SRX Series firewalls in their networks can easily extend those policies to any vSRX Virtual Firewall operating in the public cloud or elsewhere.

The vSRX supports the creation and deployment of firewall policies using metadata tags, facilitating security automation and reducing the number of rules required during initial implementation or ongoing maintenance. This metadata gives security administrators greater visibility by providing a full network view based on the metadata tags, meaning they are no longer limited to IP address-based rule management and filtering.

In addition to policy enforcement, the vSRX provides advanced security services, including IPS, antivirus, and anti-malware, to identify and block advanced threats targeting workloads hosted in the GCP cloud.

Workload Segmentation

The vSRX can secure communication and ensure workload segmentation on GCP by enforcing policies regarding which communications should be allowed between workload segments. The vSRX facilitates granular network segmentation

and control by applying security policies at the virtualized workload level. From a security perspective, the more granular the level at which the threat is blocked, the more effective the containment of the threat's propagation.

Features and Benefits

Advanced Security Services

Implementing nonintegrated legacy systems built around traditional firewalls and individual standalone appliances and software is no longer enough to protect against today's sophisticated attacks.

Juniper's advanced security suite enables users to deploy multiple technologies to meet the unique and evolving needs of modern organizations and the constantly changing threat landscape. Real-time updates ensure that technologies, policies, and other security measures are always current.

The vSRX for GCP delivers a versatile and powerful set of advanced security services, including IPS, malware protection, app control, and content security.

Intrusion Prevention System

IPS for vSRX for GCP controls access to IT networks, protecting systems by inspecting data and taking actions such as blocking attacks as they develop or creating a series of rules in the firewall. IPS tightly integrates Juniper's application security features with the network infrastructure to further mitigate threats and defend against a wide range of attacks and vulnerabilities.

Juniper Advanced Threat Prevention

Juniper® Advanced Threat Prevention integrates with the vSRX for GCP to provide dynamic, automated protection against known malware and advanced zero-day threats, resulting in nearly instantaneous responses.

Application Visibility and Control with AppSecure

Juniper Networks AppSecure is a next-generation application security suite, delivering threat visibility, protection, enforcement, and control. This optional feature provides powerful visibility and ongoing application tracking. With open signatures, unique application sets can be monitored, measured, and controlled to closely align with the organization's business priorities.

Content Security

The vSRX for GCP includes comprehensive content security against malware, viruses, phishing attacks, spam, and other threats with best-in-class antivirus, antispam, Web filtering, and content filtering features.

Juniper Secure Connect

Juniper Secure Connect is a highly flexible SSL VPN application that provides secure access to corporate and cloud resources for employees working away from protected resources. This SSL VPN app is available for the most common operating systems. It offers adaptable connectivity to any device anywhere, reducing risk by extending visibility and enforcement from users to the cloud.

Table 1. vSRX Features and Benefits for GCP

Feature	Feature Description	Benefit
Scalable hardware support	Allows you to start with 2 CPU cores and 7.5 GB of memory and scale up to 16 cores and 60 GB memory	Provides a flexible and scalable hardware footprint to support your needs now and in the future, as traffic grows
Flexible licensing	Supports both pay-as-you-go (PAYG) and bring-your-own-license (BYOL) options	Provides flexible license and purchase options to secure workloads in GCP and connectivity between your data center and GCP

Specifications

Table 2. vSRX on GCP Instance Types

GCP Instance Type	vCPUs in Instance Type	Memory in Instance Type (GB)
N1-standard-2	2	7.5
N1-standard-4	4	15
N1-standard-8	8	30
N1-standard-16	16	60

For a full list of GCP instance types supported, please visit www.juniper.net/documentation/en_US/vsrx/topics/topic-map/security-vsrx-google-system-requirements.html.

Ordering Information

For more information about Juniper Networks vSRX Virtual Firewall BYOL for GCP, please visit www.juniper.net/us/en/products-services/security/srx-series/vsrx or contact your Juniper Networks sales representative.

To activate a trial version of the vSRX for GCP, visit the GCP Marketplace at https://console.cloud.google.com/marketplace/details/juniper-marketplace/vsrx-next-generation-firewall?q=vsrx&id=de0a15a3-968e-4bed-8eca-e892b06e8701.

Product	Description
vSRX Virtual Firewall	• Core firewall featuring IPsec VPN, Network Address Translation (NAT), cost of service, and rich routing services • AppSecure featuring AppID, AppFW, AppQoS, and AppTrack • Content security services that include IPS
vSRX Virtual Firewall with Anti-Virus Protection	• Core firewall features, IPsec VPN, NAT, cost of service, and rich routing services • AppSecure featuring AppID, AppFW, AppQoS, and AppTrack • Content security services including IPS, anti-virus, anti-spam, web, and content filtering

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700