vSRX VIRTUAL FIREWALL FOR AMAZON WEB SERVICES

Product Overview

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

Product Description

Workloads are continuing to move to the public cloud, introducing challenges around not only how to secure the data, but also around securing 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 security of the organization. This challenge can only be met by a security 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 vSRX Virtual Firewall for Amazon Web Services (AWS), empowering security professionals to deploy and scale firewall protection for workloads deployed within AWS. This 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 communications security with secure software-defined WAN (SD-WAN), transit virtual private cloud (VPC), and software-defined LAN (SD-LAN) for secure segmentation between workloads.

The vSRX for AWS 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 is committed to interoperability across all SRX Series firewalls. In addition to Security Director and Contrail Service Orchestration, the vSRX supports OpenContrail®, as well other third-party management solutions. The vSRX can also be integrated 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 that are 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 allows organizations to use a single platform to manage, automate, and orchestrate network security, virtualization, and interconnectivity, from endpoint to edge and every cloud in between.

Architecture and Key Components

Secure Connectivity

The vSRX on AWS can secure communications between workloads running in different virtual private clouds (VPCs), and/or an on-premises data center.

The vSRX Virtual Firewall can make use of multiple connectivity options to securely connect sites—whether virtual or physical—to the enterprise WAN fabric. Secure connectivity can be extended to include other data centers that may host or need to securely communicate with the cloud workloads.

On-premises or colocated data centers using AWS Direct Connect operate in a similar manner to inter-region connectivity within AWS, while data centers not using Direct Connect can be connected over the Internet using a VPN.

Secure SD-WAN

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

A vSRX deployed in AWS can act as an SD-WAN spoke or hub, offering secure access between campus and branch locations and AWS 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 AWS, becoming the central point for regionally based Internet breakout. This allows vSRX on AWS to not only secure workloads, but also provide secure SD-WAN connectivity that fits changing business needs.

Workload Protection

Firewalls protect workloads, but not all firewalls are created equal. With vSRX on AWS, 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 vSRX operating in the public cloud or elsewhere.

vSRX supports the creation and deployment of firewall policies using metadata tags, which facilitates security automation and reduces 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 AWS cloud.

Workload Segmentation

To secure communication and ensure workload segmentation on AWS, the vSRX can be deployed to enforce 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 level at which a threat can be blocked, the more effective it will be containing the threat's propagation.

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 the technologies, policies, and other security measures are always current.

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

Intrusion Prevention System

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

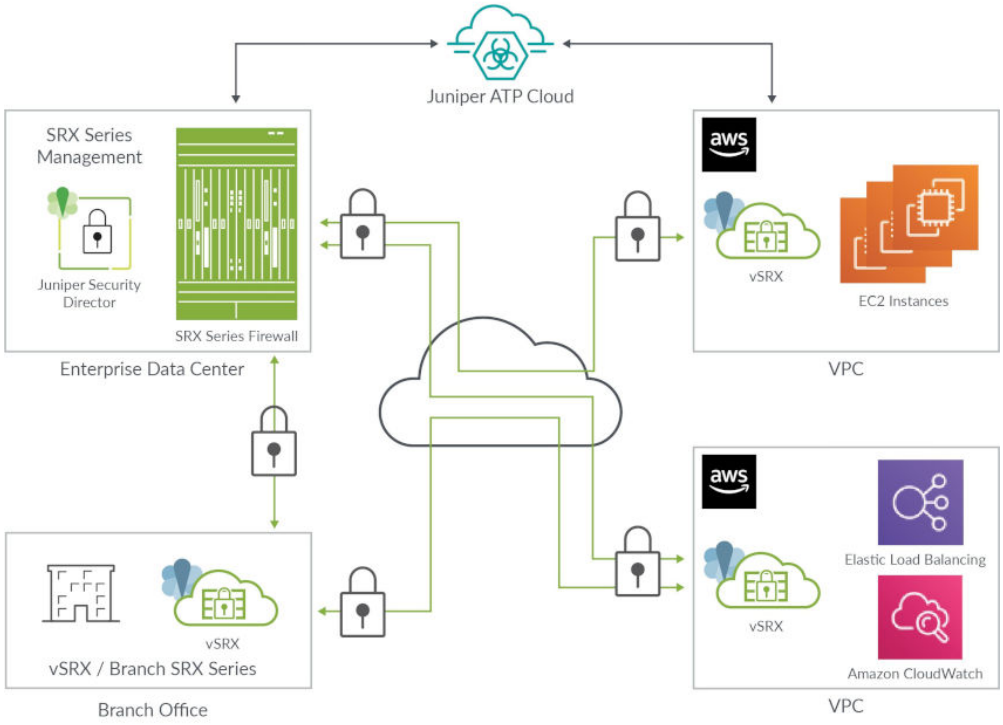

Figure 1: vSRX to secure cloud workloads in AWS

Features and Benefits

Table 1. vSRX Features and Benefits for AWS

Feature	Feature Description	Benefit
Scalable hardware support	Lets you start with 2 CPU cores and 4 GB of memory and scale up to 36 cores and 93 GB memory	Provides flexible and scalable hardware footprint to support your traffic needs now and into the future
Metadata-based firewall policies	Allows administrators to leverage the power of Dynamic Address Group functionality on the vSRX to create object metadata-based user-intent firewall policies	Simplifies policy creation as well as maintenance workflows by allowing firewall policies to be enabled or disabled based on metadata such as AWS tags
Auto-scaling	Supports vSRX deployments that require dynamic spin-up security resources when workloads increase	Increases scale and security performance without the need to manually spin up additional vSRX instances
Elastic load balancing	Increases Internet-facing traffic capacity using application load balancing	Allows the vSRX to be deployed where greater capacity is required to keep up with traffic demands
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 AWS and connectivity between your data center and AWS

Juniper Advanced Threat Prevention

Juniper Advanced Threat Prevention integrates with the vSRX for AWS 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 for vSRX on AWS, delivering threat visibility, protection, enforcement, and control. This optional feature delivers 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 AWS 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.

Specifications

Table 2. vSRX on AWS Key Performance Metrics

Performance and Capacity[1]	vSRX on AWS			
AWS instance type	c4-xLarge	c5-Large	c5n-2xLarge	c5n-9xLarge
vCPU cores	4	2	8	36
Memory	7 GB	3 GB	20 GB	93 GB
Firewall throughput, large packet (UDP)	1.2 Gbps	10 Gbps	25.5 Gbps	51.5 Gbps
IPsec VPN throughput (AES-GCM256 TCP)	630 Mbps	2 Gbps	5.9 Gbps	15.5 Gbps
Maximum concurrent sessions[2]	2 million	512,000	4 million	24 million

1. All performance numbers are measured under ideal test conditions using open source tools. Juniper recommends that customers test the performance in their public cloud deployment to meet their specific security performance requirement.

2. The maximum concurrent sessions supported is dependent on the memory assigned to the vSRX. Refer to the vSRX datasheet for more information https://www.juniper.net/us/en/products-services/security/srx-series/datasheets/1000489.page.

To see a full list of AWS instance types supported, go to https://www.juniper.net/documentation/product/us/en/vsrx.

Ordering Information

For more information about Juniper Networks vSRX Virtual Firewall BYOL license for AWS, 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 AWS, visit the AWS marketplace.

Customers who wish to purchase directly through the AWS Marketplace have two options to deploy vSRX pay-as-you-go (PAYG), either as one-hour or one-year subscriptions.

Table 3. Ordering Information for PAYG on the AWS Marketplace

vSRX PAYG Offerings	vSRX PAYG Features
vSRX next-generation firewall	• Core firewall features, IPsec VPN, Network Address Translation (NAT), class of service (CoS), and rich routing services • AppSecure features that include AppID, AppFW, AppQoS, and AppTrack • Content security services that include IPS
vSRX next-generation firewall with antivirus protection	• Core firewall features, IPsec VPN, NAT, CoS, and rich routing services • AppSecure features that include AppID, AppFW, AppQoS, and AppTrack • Content security services that include IPS, antivirus, anti-spam, Web and content filtering

About Juniper Networks

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability and equality.

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: +31.207.125.700

Juniper Networks | Driven by Experience™