

Next Generation Firewall (NGFW)



Seamless and secure connectivity

Key benefits

- Scalable hardware support provides flexible and scalable hardware footprint to support your traffic needs now and into the future.
- Metadata-based firewall policies simplifies creation as well as maintenance workflows by allowing firewall policies to be enabled or disabled based on metadata such as AWS tag.
- Auto-scaling increases scale and security performance without the need to manually spin up additional vSRX instances.
- Elastic load balancing allows the vSRX to be deployed where greater capacity is required to keep up with traffic demands.
- Flexible licensing provides flexible license and purchase options to secure workloads in AWS and connectivity between your data center and AWS.

Product overview

The vSRX Virtual Firewall delivers a complete virtual firewall solution, including advanced security, robust networking, and automated virtual machine life cycle management capabilities. vSRX empowers security professionals to deploy and scale firewall protection in highly dynamic environments.

Juniper Networks simplifies the complexities of migrating to the cloud with solutions and services to transform your network.

Combined with the agility of AWS, the vSRX Next Generation Virtual Firewall delivers secure connectivity with advanced automation, enabling you to achieve your business goals.

Create a secure internet gateway using the high-performing vSRX. With advanced cloud-grade routing capabilities, you can stay ahead of threats and protect your workloads while providing enhanced connectivity using IPsec and full mesh VPN termination services all in one, easy to use, platform.

Product features

Juniper Advanced Threat Prevention

- Provides dynamic, automated protection against known malware and advanced zero-day threats, resulting in nearly instantaneous responses.

Intrusion Prevention System (IPS)

- IPS tightly integrates Juniper's applications security features with the network infrastructure to further mitigate issues and defend against a wide range of incidents and vulnerabilities.

Content Security

- Includes comprehensive content security against malware, viruses, phishing, bugs, spam, and other issues with first-rate antivirus, antispam, web filtering, and content filtering features.

Workload Protection & Segmentation

- Ensures policies are consistently deployed across their entire network, wherever the workloads operate
- Facilitates granular network segmentation and control by applying security policies at the virtualized workload level.

How it works

Juniper Networks extends 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 outstanding 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 (SDWAN), transit virtual private cloud (VPC), and software-defined LAN (SD-LAN) for secure segmentation between workloads.

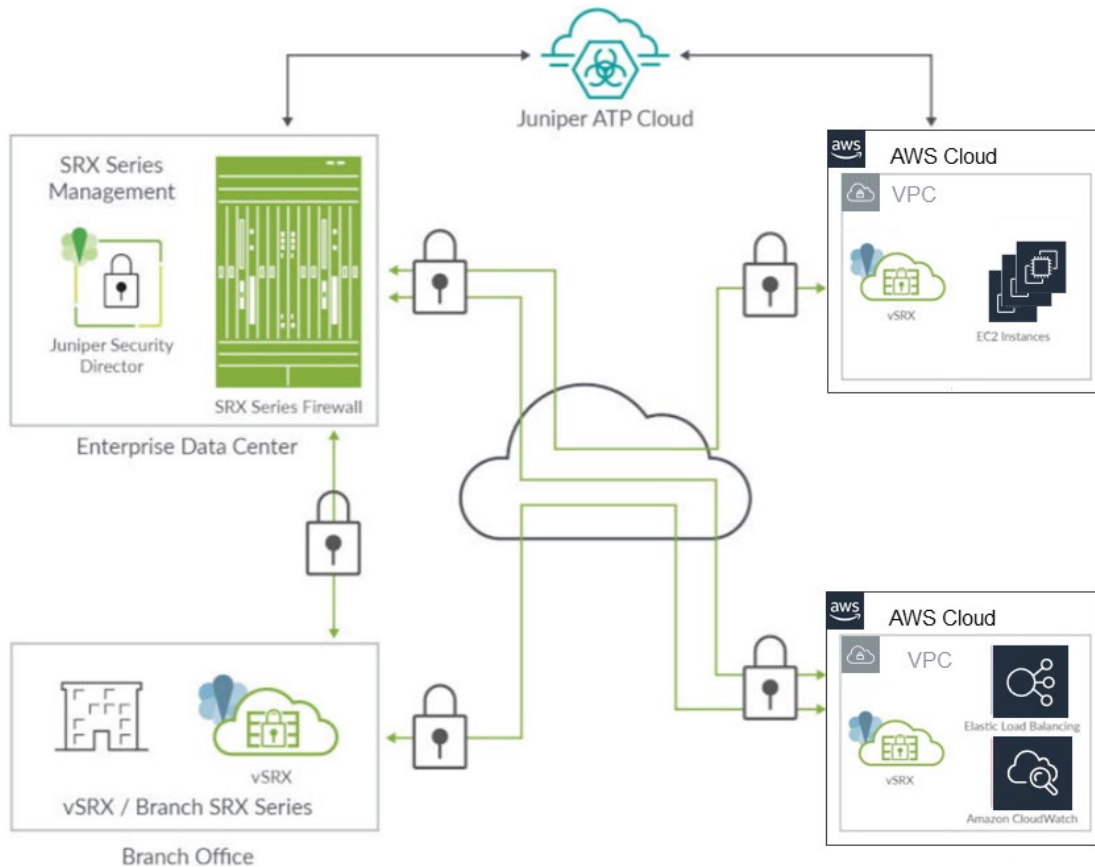


Figure 1: vSRX to secure cloud workloads in AWS

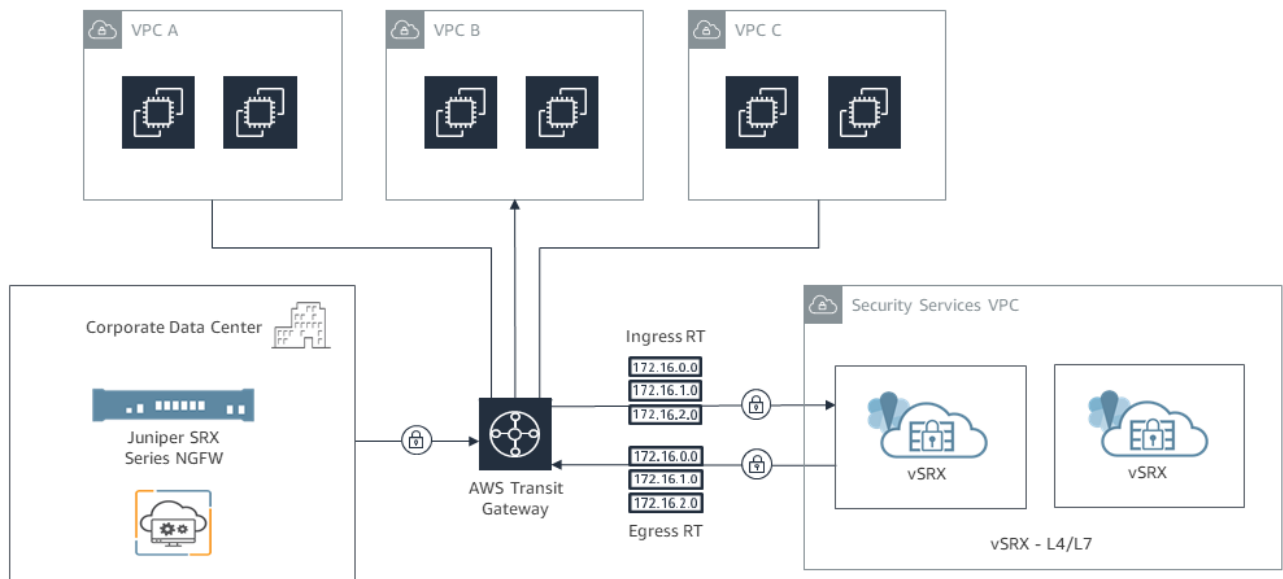


Figure 2: Hybrid cloud security

Differentiators

- Supports software-defined networking (SDN) and network functions virtualization (NFV) through integration with Contrail, OpenContrail, and third-party SDN solution.
- Scales up to 100 Gbps for ultra-high-performance protection across public and private cloud.
- Automate management and orchestration via powerful, versatile application programming interface (APIs) in Junos OS.
- Simple, flexible, and scalable licensing models to match different business requirements, including pay-as-you-go (PAYG) and bring-your-own-license (BYOL) for public clouds.

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>