vSRX VIRTUAL FIREWALL FOR AZURE

Product Overview

The vSRX Virtual Firewall delivers a complete cloud-native virtual firewall for Microsoft Azure, 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 Azure, please visit the Azure marketplace.

Product Description

As workloads move to the public cloud, they introduce 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 virtual firewall for Microsoft Azure, empowering security professionals to deploy and scale firewall protection for workloads running within Azure. 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 communications security with secure SD-WAN, Azure virtual networks, and SD-LAN for secure segmentation between workloads.

The vSRX for Azure 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 invested in interoperability for all of its SRX Series firewalls. In addition to Security Director and Contrail Service Orchestration, the vSRX also supports OpenContrail® as well as 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 Azure 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 Azure region and global virtual network peering across Azure regions. This allows the vSRX to offer secure connectivity between Azure virtual networks without having to send data flows over the Internet, which minimizes cost, latency, and availability concerns.

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 (such as collocation of third-party cloud deployments) that may need to securely communicate with the cloud workloads.

Secure SD-WAN

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

A vSRX deployed in Azure can act as an SD-WAN spoke or hub, offering secure access between campus and branch locations and Azure 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 Azure, becoming the central point for regionally based Internet breakouts. This allows vSRX on Azure 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 Azure, 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 Virtual Firewall 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 Azure cloud.

Workload Segmentation

To secure communication and ensure workload segmentation on Azure, 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.

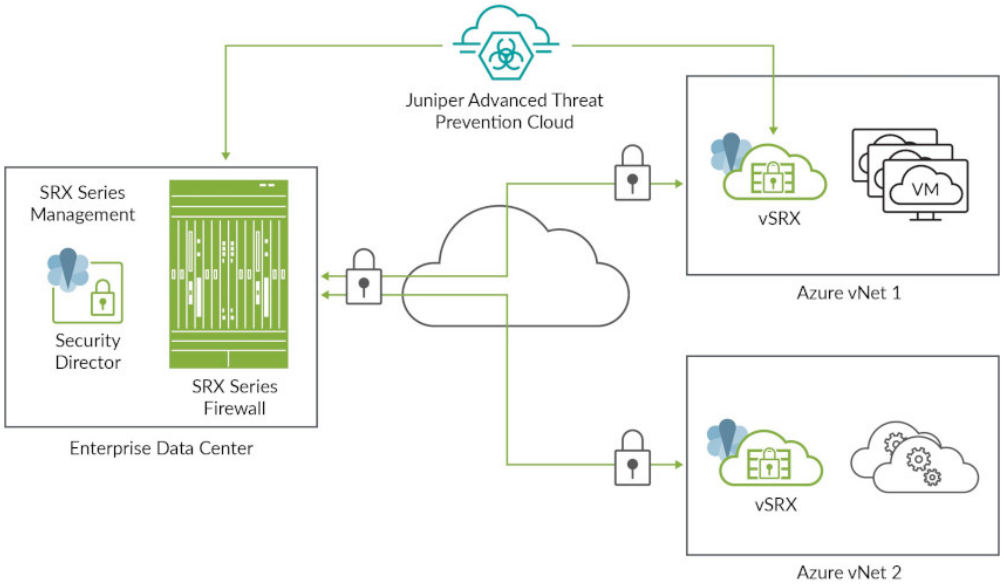

Figure 1. vSRX to secure workloads in Azure

Features and Benefits

Table 1. vSRX Features and Benefits for Azure

Feature	Feature Description	Benefit
Scalable hardware support	Allows you to start with 4 CPU cores and 14 GB of memory and scale up to 16 cores and 56 GB memory	Provides a flexible and scalable hardware footprint to support your needs now and into the future as traffic grows
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 Azure tags
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 Azure and connectivity between your data center and Azure
Azure Load Balancer	Provides traffic distribution or load balancing to a pool of vSRX virtual firewalls deployed in Azure	Increases the capacity and performance of vSRX firewalls deployed in Azure
Microsoft Azure Key Vault hardware security module (HSM)	• Allows the vSRX to use SHA256-bit encryption to hash the current configuration file • Encrypts the device primary password used to encrypt data at rest on the vSRX • Ensures that key pairs are generated and stored In the Azure Key Vault. The private key is no longer stored on the vSRX, only the public key is stored and encrypted on the vSRX	Reduces risk and improves security by securely encrypting the data at rest on the vSRX running in Azure

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 Azure 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 Azure 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.

Juniper Advanced Threat Prevention

Juniper Advanced Threat Prevention integrates with the vSRX for Azure 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 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 Azure 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 which 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 and offers adaptable connectivity to any device anywhere, reducing risk by extending visibility and enforcement from users to the cloud.

Specifications

Table 2. vSRX on Azure Instance Types

Azure instance type	Standard_DS3_v2	Standard_DS4_v2	Standard_DS5_v2
vCPU cores	4	8	16
Memory	14 GB	28 GB	56 GB

For a full list of Azure instance types supported, please visit https://www.juniper.net/documentation/en_US/vsrx/topics/reference/general/security-vsrx-azure-system-requirements.html.

Ordering Information

For more information about Juniper Networks vSRX Virtual Firewall Bring-Your-Own-License (BYOL) for Azure, 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 Azure, visit the Azure Marketplace at https://azuremarketplace.microsoft.com/en-us/marketplace/apps/juniper-networks.vsrx-next-generation-firewall-payg?tab=PlansAndPrice.

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

Table 3. Ordering information for PAYG on the Azure Marketplace

Product	Description
vSRX Next-Generation Firewall	• Core firewall featuring IPsec VPN, Network Address Translation (NAT), cost of service (CoS), and rich routing services • AppSecure featuring AppID, AppFW, AppQoS, and AppTrack • Content security services that include IPS

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