

VSRX VIRTUAL FIREWALL DATASHEET

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 for service providers and enterprises. vSRX empowers security professionals to deploy and scale firewall protection in highly dynamic environments.

To download a trial version of the vSRX, including advanced security services such as IPS, AppSecure, and content security, visit https://www.juniper.net/us/en/products/security/srx-series/vsrx-virtual-firewall-datasheet.html.

Product Description

Data centers increasingly rely on server virtualization to deliver services faster and more efficiently than ever before. The virtualized data center, however, introduces new challenges that require additional security considerations beyond those needed to secure physical assets.

Virtual machines (VM) can be highly dynamic and elastic in a virtualized data center, with frequent additions, moves, and changes. These frequent changes complicate the ability to attach security policies to a VM instantiation and track security policies with VM movement to ensure continued regulatory compliance. In short, the dynamic and flexible nature of virtualization can easily lead to a loss of visibility and control.

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

Juniper addresses these challenges head-on by extending the capabilities of the award-winning Juniper Networks® SRX Series Firewalls to the virtual world with the vSRX Virtual Firewall. Juniper makes security easy by securing the cloud at every level: between applications, between instances, and across environments.

Powered by Juniper Networks Junos® operating system, the vSRX delivers a complete and integrated virtual security solution, including L4-L7 advanced security services, robust networking, and automated life cycle management capabilities for service providers and enterprises alike.

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

For service providers and organizations deploying service-oriented applications in software, the vSRX's portfolio of virtualized network and security services supports a variety of Network Functions Virtualization (NFV) use cases. The vSRX also supports Juniper Networks Contrail, OpenContrail, and other third-party solutions, and can be integrated with other next-generation cloud orchestration tools such as OpenStack, either directly or through rich APIs.

Table 1. vSRX Content Security Features and Benefits

Feature	Feature Description	Benefits
Antivirus	• Reputation-enhanced, cloud-based antivirus capabilities that detect and block spyware, adware, viruses, keyloggers, and other malware over POP3, HTTP, SMTP, and FTP protocols • Service provided either on-box or in the cloud	• Sophisticated protection from respected antivirus experts against malware attacks that can lead to costly data breaches and lost productivity
Web filtering	• Enhanced Web filtering, including extensive category options (90+ categories) and a real-time scorecard	• Protection against lost productivity and the impact of malicious URLs, as well as helping to maintain network bandwidth for essential business traffic
Content filtering	• Effective inbound and outbound content filtering based on MIME type, file extension, and protocol commands	• Protection against inadvertent or malicious file transmitting and malicious content on the network to minimize the risk of compromise or data leakage
Antispam	• Multilayered spam protection, up-to-date phishing URL detection, standards-based S/MIME, Open PGP and TLS encryption, MIME type, and extension blockers	• Protection against advanced persistent threats perpetrated through social networking attacks and the latest phishing scams with sophisticated e-mail filtering and content blockers

Architecture and Key Components

Advanced Security Services

Implementing nonintegrated, legacy systems built around traditional firewalls and individual standalone appliances and software is no longer adequate 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 continually changing threat landscape. Real-time updates ensure that the technologies, policies, and other security measures are always current.

The vSRX delivers a versatile and powerful set of advanced security services, including content security, intrusion detection and prevention (IDP/IPS), and application control and visibility services through Juniper Networks AppSecure.

Content Security

The vSRX includes comprehensive content security against malware, viruses, phishing attacks, intrusions, spam, and other threats with best-in-class antivirus, antispam, Web filtering, and content filtering features (see Table 1).

Intrusion Prevention System (IPS)

IPS for vSRX controls access to IT networks to protect systems from attack by inspecting data and taking actions such as blocking attacks as they are developing—and before they succeed—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 protect against a wide range of attacks and vulnerabilities (see Table 2).

EVPN-VXLAN

All Juniper SRX Series Firewalls support EVPN-VXLAN Type 5 configuration so that security is embedded automatically across the entire EVPN-VXLAN fabric. As a result, customers can extend their workloads and securely connect from on-premises to public clouds and on-premises to on-premises (Date Center Interconnectivity).

When policy enforcement points are embedded into the data center fabric, the network becomes truly threat aware and security controls are composable like the rest of the network. Natively speaking EVPN/VXLAN enables the vSRX to be fully fabric aware, which means the technical contexts defined by the network engineering team such as tenant, virtual routing and forwarding, VNIs, and others are shared with vSRX, so security teams understand how the network is setup and segmented. Changes made to the network are automatically propagated via standard protocols eliminating manual intervention. Complete fabric awareness enables security operators to respond to threats faster and minimize the blast radius.

By offering both routing and security in a single virtualized network function, businesses can leverage the simplified and extended EVPN-VXLAN fabric design to rollout security services faster and logically separate customers.

Table 2. vSRX IPS Features and Benefits

Feature	Feature Description	Benefits
Stateful signature inspection	Signatures are applied only to relevant portions of the network traffic determined by the appropriate protocol context.	Minimizes false positives and offers flexible signature development.
Protocol decodes	More than 65 protocol decodes are supported, along with more than 500 contexts to ensure proper protocol usage.	Improves signature accuracy through the precise context of protocols.
Signatures	There are more than 15,000 signatures for identifying anomalies, attacks, spyware, and applications.	Attacks are accurately identified and attempts to exploit known vulnerabilities are detected.

Feature	Feature Description	Benefits
Traffic normalization	Reassembly, normalization, and protocol decoding is provided.	System overcomes attempts to bypass other IPS detections by using obfuscation methods.
Fast signature creation	Protocol anomaly detection and same day coverage for newly found vulnerabilities is provided.	Protects networks against any new exploits.
Recommended policy	The Juniper Security Team identifies attack signatures as critical for the typical enterprise.	Installation and maintenance are simplified while ensuring the highest network security.
Active/active traffic monitoring	IPS monitoring includes active/active vSRX chassis clusters.	Support included for active/active IPS monitoring.
Packet capture	IPS policy supports packet capture logging per rule.	Users can conduct further analysis of surrounding traffic and determine additional steps to protect the target.

Table 3. AppSecure for vSRX Features and Benefits

Feature	Description	Benefit
AppTrack	Analyzes application data and classifies it based on risk level, zones, source, and destination addresses.	Tracks application usage to identify high-risk applications and analyze traffic patterns, improving network management and control.
AppFW	Creates application control policies to allow or deny traffic based on dynamic application or group names.	Enhances security policy creation and enforcement based on applications rather than traditional port and protocol analysis.
AppQoS	Meters and marks traffic based on the application security policies set by the administrator.	Prioritizes traffic and limits and shapes bandwidth based on application information and context to improve overall performance.

Application Visibility and Control with AppSecure

AppSecure is a next-generation application security suite for vSRX and SRX Series Firewalls that delivers threat visibility, protection, enforcement, and control.

Whether needing to understand how many users are accessing cloud-based applications like Facebook every day, or needing to know what applications are using the most bandwidth, AppSecure delivers powerful visibility and ongoing application tracking. With open signatures, unique application sets can be monitored, measured, and controlled to tie closely to the organization's business priorities.

Juniper Advanced Threat Prevention

Juniper Advanced Threat Prevention integrates with the vSRX to provide dynamic, automated protection against known malware and advanced zero-day threats, resulting in instantaneous responses (see Table 4).

Security policies determine if a session can originate in one zone and be forwarded to another zone. The vSRX receives packets and keeps track of every session, every application, and every user. As a VM moves within a virtualized or cloud environment, it will still send packets to the vSRX for processing, continuously communicating in a secure mode.

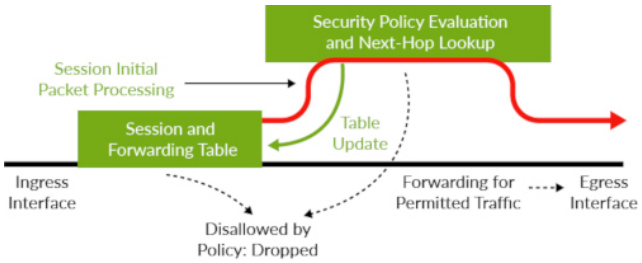


Figure 1: vSRX session-based forwarding algorithm

High Availability (HA)

The vSRX provides mission-critical reliability, supporting chassis clustering for active/active and active/passive modes. The HA functionality provides full stateful failover for any connections processed and for cluster members to span hypervisors. When configured in a cluster, vSRX VMs synchronize the connection/session state and flow information with IPsec security associations, Network Address Translation (NAT) traffic, address book information, configuration changes, and more. As a result, not only is the session preserved during failover, but security is also kept intact. In an unstable network, vSRX also mitigates link flapping.

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. Juniper Secure Connect is available for desktop and mobile devices including Windows, Mac OS, Android, and iOS. When combined with the SRX Series Firewalls, Secure Connect helps organizations achieve dynamic, flexible, and adaptable connectivity to any device anywhere, reducing risk by extending visibility and enforcement from users to cloud.

Table 4. Juniper ATP for vSRX Features and Benefits

Feature	Benefits
Deep inspection and analysis	Extracts compromised files and sends them to the cloud to rapidly identify known threats or deep-level file analysis that looks for particularly evasive malware.
Instant identification to block attacks	Instantly identifies and communicates detected malware to SRX Series firewalls to block attacks.
Web-based portal with rich reporting and analytics tools	Provides a web-based interface for performing management tasks such as configuration and product updates. It also offers a rich set of reporting and analytics tools that provide visibility into threats and compromised hosts.
Quarantine of systems and hosts	Analytics capability lets administrators and security staff analyze and correlate data, identifying compromised systems and feeding the information to SRX Series firewalls to quarantine those systems.
SecIntel	Dynamic threat intelligence feeds offered through SecIntel cascade threat information to SRX Series firewalls for immediate action.
AI-Predictive Threat Prevention	Keeps known and zero-day threats off the network at line rate for the entire attack lifecycle—not just for 24 hours—helping keep your network safe from initial and subsequent attacks.
Command and control (C&C) data	Provides C&C data to the SRX Series firewalls, preventing compromised internal systems from communicating with these devices.
E-mail analysis and remediation	Isolates and quarantines malicious malware, preventing e-mail from being used as an attack vector. Machine learning algorithms analyze e-mail traffic, detect malicious attachments, and block files at the firewall.
Threat intelligence	Uses powerful open APIs for seamless integration with third-party vendors, providing multiple threat intelligence feeds and reducing the attack surface.
Encrypted Traffic Insights	Restores visibility into traffic lost due to encryption without the heavy burden of full TLS/SSL decryption.
Adaptive Threat Profiling	Enables a quicker response time to combat the continuous onslaught of new threats. Organizations can use ATP Cloud's Adaptive Threat Profiling to automatically create security intelligence threat feeds based on who and what is currently attacking the network.

Table 5. vSRX Firewall Key Performance Metrics

Performance and Capacity[1]	VMware				KVM			
vCPUs	2	5	9	17	2	5	9	17
Memory	4 GB	8 GB	16 GB	32/64 GB	4 GB	8 GB	16 GB	32/64 GB
Firewall throughput, large packet (1514B)	15.7 Gbps	41 Gbps	73 Gbps	81 Gbps	17 Gbps	50 Gbps	79 Gbps	141 Gbps
Firewall throughput, IMIX	3.2 Gbps	11.1 Gbps	17 Gbps	27 Gbps	4.3 Gbps	12.5 Gbps	22 Gbps	40 Gbps
AES+GCM IPSec VPN throughput (1420B)	2.1 Gbps	3.8 Gbps	12 Gbps	13 Gbps	2.9 Gbps	6.3 Gbps	10.8 Gbps	14.9 Gbps
Application visibility and control[2]	3.7 Gbps	10.8 Gbps	21 Gbps	39 Gbps	2.4 Gbps	10.8 Gbps	20.7 Gbps	35.8 Gbps
IPS recommended signatures	3.6 Gbps	11 Gbps	18 Gbps	39 Gbps	2.2 Gbps	12.6 Gbps	20.8 Gbps	36.2 Gbps
TCP connections per second	55,000	166,250	351,250	537,660	69,000	239,380	360,000	612,660
Maximum concurrent sessions[3]	512,000	2M	4M	12/28M	512,000	2M	4M	12/28M
Number of remote access/SSL VPN (concurrent) users	500	500	500	500	500	500	500	500

[1] All performance numbers are "up to" and depend on the underlying hardware configuration (some server configurations may perform better). Performance, capacity and features listed are based on vSRX running Junos OS 20.4R1 release and are measured under ideal testing conditions. Actual results may vary based on Junos OS releases and by deployments

[2] Throughput numbers based on HTTP traffic with 44KB transaction size.

[3] Maximum concurrent sessions can be increased based on the memory allocation for the vSRX. For more information, visit https://www.juniper.net/documentation/en_US/vsrx/information-products/topic-collections/release-notes/19.2/topic-98044.html#jd0e119

Performance

Traditionally, customers must choose between scalability and performance. The vSRX solution is optimized to leverage multiple virtual CPUs to maximize packet processing and overall throughput in the virtual environment. Each vSRX VM also has multiple virtual network interface cards (vNICs), which can be connected to various virtual networks to simultaneously protect multiple network segments. The vSRX operates from within the virtual fabric, providing the best of both worlds—strong security with the performance needed to support a virtualized or cloud-based environment.

Leveraging the Software Receive Side Scaling implementation, the vSRX provides additional cores* beyond the minimum two vCPU, up to a maximum of 32 vCPUs, to the same instance without having to certify a new instance image. By using 17 vCPUs from a single socket, the vSRX can achieve up to 98 Gbps performance.

*Number of cores should be power of 2 + 1 (i.e. 2n + 1)

Table 6. vSRX System Requirements

Virtual CPU Cores	Memory (GB)	Supported NIC Types
2	4, 8, 16, 20, 32	VMXNET3, VIRTIO, 82599 SR-IOV, I40E SR-IOV
5	8, 16, 20, 32	VMXNET3, VIRTIO, 82599 SR-IOV, I40E SR-IOV
9	16, 32, 50, 64	I40E SR-IOV
17	32, 50, 64	I40E SR-IOV
32	64	I40E SR-IOV

Junos Space Security Director

Junos Space Security Director provides security policy management through an intuitive and centralized web-based interface that offers enforcement across emerging and traditional risk vectors. As an application on the Junos Space platform, Security Director provides extensive security scale, granular policy control, and policy breadth across the network. It helps administrators quickly manage all phases of security policy life cycle for stateful firewall, content security, IPS, AppFW, VPN, and NAT.

Unified Management

Leveraging the power of Junos Space Security Director, administrators can significantly improve policy configuration, management, and visibility into both physical and virtual assets from one common, centralized platform.

Key Features and Benefits

- Secures multitenant private and public cloud environments by delivering a complete firewall with stateful packet processing and application-layer gateway features in a virtual machine format
- Leverages the same, consistent, advanced security and networking features (IPsec VPN, NAT, QoS, and full routing capabilities) of the SRX Series Firewalls
- Defends against an increasingly sophisticated threat landscape by integrating robust content security, IPS, and application visibility and control capabilities for a comprehensive threat management framework
- Improves management flexibility with open RESTful APIs to support integration with third-party management and cloud orchestration tools
- Expands visibility into and control over firewall security policy configuration and management across virtual and non-virtual environments with Junos Space Security Director
- Supports SDN and NFV via integration with Contrail, OpenContrail, and other third-party solutions

Available for Nutanix

The vSRX is available for deployment on Nutanix enterprise cloud to provide advanced network and application security and secure IPsec VPN connectivity between Nutanix AVH on-premises resources. Using Junos Space Security Director, customers can maintain and manage consistent security policies on SRX Series Firewalls spread across campus, data center, and cloud. The vSRX has been certified Nutanix Ready; for more information, visit https://www.nutanix.com/partners/technology-alliances/juniper-networks.

Available on Amazon Web Services Marketplace

The vSRX is available on the Amazon Web Services (AWS) Marketplace to provide advanced network and application security and secure IPsec VPN connectivity to AWS VPCs, private clouds, and on-premises resources. With vSRX 3.0, you can take advantage of AWS auto scaling to dynamically increase capacity while maintaining steady, predictable performance at the lowest possible cost. Using Junos Space Security Director, customers can maintain and manage consistent security policies on SRX Series Firewalls spread across on-premises and AWS VPCs. Customers using the vSRX on AWS can either bring their vSRX license or pay via usage-based pricing (pay-as-you-go, hourly or annually).

Available on Microsoft Azure Marketplace

The vSRX is available on the Microsoft Azure Marketplace and on Microsoft Azure Government to provide secure IPsec VPN connectivity and advanced next-generation security to Azure virtual networks. Using Junos Space Security Director, customers can maintain and manage consistent security policies on SRX Series

next-generation firewalls deployed on-premises as well as in Azure virtual networks. The vSRX is available in Bring-Your-Own-License (BYOL) mode on the Microsoft Azure Marketplace and Microsoft Azure Government.

Available on Google Cloud Platform Marketplace

The vSRX is available on the Google Cloud Platform Marketplace and Google Cloud Government, providing secure IPsec VPN connectivity and advanced next-generation and content security features to Google virtual networks. Juniper offers Bring-Your-Own-License (BYOL) as well as Pay-as-You-Go (PAYG) licensing options on the Google Cloud Platform and Google Cloud Government.

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit https://www.juniper.net/us/en/products.html.

Specifications

The following table highlights high-level specifications. Please see the product documentation for a complete list.

Table 7. vSRX Virtual Firewall Specifications

Protocols	IP Address Management	Security	SLA, Measurement, and Monitoring	Hypervisors
• IPv4, IPv6, MPLS, ISO Connectionless Network Service (CLNS) • Static routes • RIPv2 +v1 • OSPF/OSPFv3 • BGP • IS-IS • Multicast (Internet Group Management Protocol, PIM, Session Description Protocol) • MPLS • VPLS	• Static • Dynamic Host Configuration Protocol (DHCP) • Internal DHCP server, DHCP relay • Address Translation • Source NAT with Port Address Translation (PAT) • Static NAT • Destination NAT with PAT • Persistent NAT, NAT64 • Encapsulations • Ethernet • 802.1Q VLAN support	• Firewall • Firewall, zones, screens, policies • Stateful firewall, stateless filters • Network attack detection • Screens denial of service (DoS) and distributed DoS (DDoS) protection (anomaly-based) • Replay attack prevention; anti-replay • Unified access control (UAC) • TCP reassembly for fragmented packet protection • Brute force attack mitigation • SYN cookie protection • Zone-based IP spoofing • Malformed packet protection • VPN • Tunnels: Site-to-Site, Hub and Spoke, Dynamic Endpoint, AutoVPN, ADVPN, Group VPN (IPv4/IPv6/Dual Stack) • Internet Key Exchange (IKE): IKEv1/IKEv2 • Configuration Payload • IKE Authentication Algorithms: MD5, SHA1, SHA-256, SHA-384 • IKE Encryption Algorithms: Prime, DES-CBC, 3DES-CBC, AEC-CBC, AES-GCM, SuiteB • Authentication: Pre-shared key and public key infrastructure (PKI X.509) • IPsec (Internet Protocol Security): Authentication Header (AH)/Encapsulating Security Payload (ESP) protocol • Perfect forward secrecy • IPsec Authentication Algorithms: hmac-md5, hmac-sha-196, hmac-sha-256 • IPsec Encryption Algorithms: rime, DES-CBC, 3DES-CBC, AEC-CBC, AES-GCM, SuiteB • Monitoring: Standard-based Dead peer detection (DPD), VPN monitoring • VPNs (GRE, IP-in-IP, MPLS) • Microsoft Azure dedicated Hardware Security Module (HSM) • IPv6	• Real-time performance monitoring (RPM) • Sessions, packets, and bandwidth usage • IP monitoring • Logging • System logging • Traceroute • Extensive control and data plane structured and unstructured system log administration • Junos Space Security Director support • Juniper Networks Secure Analytics • Juniper Networks Advanced Insight Solutions support • External administrator database (RADIUS, LDAP, SecureID) • Auto-configuration • Configuration rollback • Rescue configuration with button • Commit confirms for changes • Auto-record for diagnostics • Software upgrades • J-Web • CLI	• VMware ESXi 5.5, 6.0, 6.5, 7.0 KVM/QEMU*: - CentOS 7 - Ubuntu 16.04, 16.10, 18.04 - RHEL 7.7 - Oracle Linux 7.3 • Hyper-V 2012, 2012R2, 2016 • Nutanix AHV: - AOS: 5.15 LTS

*Hypervisor support is regularly updated. To find the complete list of all hypervisor versions supported, please view the vSRX on KVM page.

ICSA Labs Firewall Certification

Juniper Networks vSRX Virtual Firewall has satisfied the complete set of ICSA Labs Firewall security testing requirements in both the baseline and corporate criteria documents and has been awarded the ICSA Labs Firewall Certification.

Ordering Information

For more information about Juniper Networks vSRX Virtual Firewall, please visit https://www.juniper.net/us/en/products/security/srx-series/vsrx-virtual-firewall.html or contact the nearest Juniper Networks sales representative. For a free vSRX trial, visit https://www.juniper.net/us/en/dm/download-next-gen-vsrx-firewall-trial.html.

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

Driven by Experience

Copyright 2023 Juniper Networks, Inc. All rights reserved. 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.