vSRX Services Gateway

Product Overview

vSRX Services Gateway (formerly known as Firefly Perimeter) 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.

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 over and above those required to secure physical assets.

In the virtualized data center, virtual machines (VM) can be highly dynamic, with frequent additions, moves, and changes. This can complicate the ability to attach security policies to 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 that is taken for granted in a physical world.

Network and security professionals must perform a delicate balancing act, delivering the benefits of virtualization and cloud technologies without undermining the security of the organization. This challenge can only be met by a new breed of 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 Services Gateways to the virtual world with the vSRX Services Gateway. 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, enabled through Junos Space Virtual Director, 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's provisioning application 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 common, 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.

Your ideas. Connected.™

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 constantly changing threat landscape. Real-time updates ensure that the technologies, policies, and other security measures are always current.

The vSRX delivers a versatile, powerful virtualization-specific set of advanced security services, including unified threat management (UTM), intrusion detection and prevention (IDP), and application control and visibility services through AppSecure 2.0.

Unified Threat Management (UTM)

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.

Table 1: vSRX UTM 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 in cooperation with Sophos Labs, a leader in anti-malware technology	• 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 delivered in partnership with Websense, the leading Web security provider	• Protection against lost productivity and the impact of malicious URLs, as well as helping to maintain network bandwidth for business essential 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 provided in cooperation with Sophos Labs	• Protection against advanced persistent threats perpetrated through social networking attacks and the latest phishing scams with sophisticated e-mail filtering and content blockers

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.

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 usage of protocols.	Accuracy of signatures is improved through precise context of protocols.
Signatures	There are more than 8,500 signatures for identifying anomalies, attacks, spyware, and applications.	Attacks are accurately identified and attempts to exploit known vulnerabilities are detected.
Traffic normalization	Reassembly, normalization, and protocol decoding are provided.	System overcomes attempts to bypass other IPS detections by using obfuscation methods.
Zero-day protection	Protocol anomaly detection and same day coverage for newly found vulnerabilities are provided.	Networks are already protected against any new exploits.
Recommended policy	Attack signatures are identified by Juniper's Security Team as critical for the typical enterprise to protect against.	Installation and maintenance are simplified while ensuring the highest network security.
Active/Active traffic monitoring	IPS monitoring includes active/active vSRX chassis clusters.	Support for active/active IPS monitoring is included.
Packet capture	IIPS policy supports packet capture logging per rule.	Users can conduct further analysis of surrounding traffic and determine further steps to protect target.

Application Visibility and Control with AppSecure 2.0

AppSecure 2.0 is a next-generation application security suite for vSRX and SRX Series Services Gateways 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.

Table 3: AppSecure 2.0 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 name 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 as well as limits and shapes bandwidth based on application information and context to improve overall performance.

Simple Configuration

The vSRX uses two basic features—zones and policies. The default configuration contains, at a minimum, a "trust" and an "untrust" zone. The trust zone is used for configuration and attaching the internal network to vSRX. The untrust zone is commonly used for untrusted networks. To streamline installation and make configuration simpler, a default policy is in place that allows traffic originating from the trust zone to flow to the untrust zone, but blocks traffic originating in the untrust zone from flowing to the trust zone. A traditional router forwards all traffic without regard for a firewall (session awareness) or policy (origination and destination of a session). Furthermore, because of the virtual nature of vSRX, customers can leverage snapshots, cloning, and related technologies to streamline maintenance and operational tasks.

In order to optimize the throughput and latency of the combined router and firewall, Junos OS implements session-based forwarding, an innovation that combines the session state information of a traditional firewall and the next-hop forwarding of a classic router into a single operation. With Junos OS, a session that is permitted by the forwarding policy is added to the forwarding table along with a pointer to the next-hop route.

This efficient algorithm improves throughput and lowers latency for session traffic when compared with a classic router that performs multiple table lookups to verify session information and then find a next-hop route. Subsequent packets for the established session require a single table lookup in the session and forwarding table, and are forwarded to the egress interface.

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.

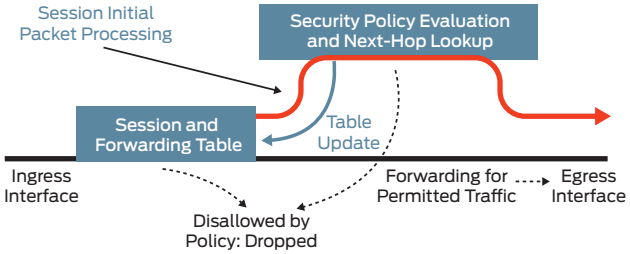

Figure 1: vSRX session-based forwarding algorithm

High Availability (HA)

The vSRX provides mission-critical reliability, supporting chassis clustering for both active/active as well as active/passive modes. The HA functionality provides full stateful failover for any connections being processed as well as for cluster members to span hypervisors. When vSRX VMs are configured in a cluster, the VM synchronizes connection/session state and flow information, 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.

Performance

Traditionally, customers have been required to make a trade-off 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. Operating from within the virtual fabric, the vSRX provides the best of both worlds—strong security with the performance needed to support a virtualized or cloud-based environment.

Table 4: vSRX Services Gateway Key Performance Metrics

Performance*	VMware	KVM
Firewall (UDP 1514 byte puts)	4.35 Gbps	2.6 Gbps
Firewall (IMIX)	1.05 Gbps	620 Mbps
Firewall ramp rate (TCP)	22,000 cycles/second	22,000 cycles/second
Firewall latency (512 byte UDP)	107 ms	87 ms
Firewall IPv6 (UDP 512 byte packets)	1.46 Gbps	829 Mbps
NAT (UDP 1514 byte packets)	4.3 Gbps	2.45 Gbps
NAT (IMIX)	1.05 Gbps	630 Mbps
NAT ramp rate (TCP)	19,000 cycles/second	19,000 cycles/second
IPsec (3DES+SHA1, 1420 byte)	290 Mbps	238 Mbps
IPsec (3DES+SHA1, IMIX)	146 Mbps	88 Mbps
IPsec (3DES+SHA1, 64 byte)	29 Mbps	21 Mbps
Internet Key Exchange (IKE) rate (3DES+SHA1, v1 or v2)	Up to 2,000 tunnels / 71 tunnels per second	Up to 2,000 tunnels / 48 tunnels per second
EWF (44 KB file)	251 Mbps	4 Mbps
SAV (Allscan 44 KB file)	279 Mbps	385 Mbps
IDP HTTP Throughput** (Response Content – 44KB File)	911 Mbps	8 Mbps
IDP HTTP CPS** (Response Content – 64 bytes)	6,300 cycles/second	6,000 cycles/second
IDP Session Scaling**	32,000	32,000
AppSecure HTTP Throughput IPv4**	760 Mbps	290 Mbps
AppSecure HTTP CPS IPv4**	5,600	3,100

* Reference platform for VMware performance: Dell PowerEdge R910, ESXI 5.1.0, 40 Core, 2.393 Ghz CPUs (02/2015). Reference platform for KVM performance: KVM-Ubuntu-14.04. Loss tolerance: 0.01%. All performance numbers are "up to" and will depend on underlying hardware configuration (some server configurations may perform better).

** IDP and AppSecure performance is based on data center use case (client-to-server protection) with the recommended IDP policy template. AppSecure performance results are based on tests with AppFW, AppTrac, AppQos and IDP all enabled.

Junos Space Virtual Director

As a full life cycle management application for vSRX, Junos Space Virtual Director enables organizations to automate provisioning and resource allocation of vSRX Services Gateway VMs. The application runs on top of Juniper's well-established Junos Space Network Management Platform and supports the design, deployment, monitoring, grouping, and reporting of vSRX VM instances. Network and security administrators will benefit from rapid service rollouts and error-free deployments by using the Virtual Director's predefined configuration templates, automation tools, workflow-based tasks, and intuitive GUI. Virtual Director's open set of RESTful APIs provides a single interface to all third-party orchestration tools and custom applications for end-to-end configuration and management.

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, UTM, IPS, AppFW, VPN, and NAT.

Unified Management

By combining the power of Junos Space Security Director with the Junos Space Virtual 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 Services Gateways
- Defends against an increasingly sophisticated threat landscape by integrating powerful UTM, IPS, and application visibility and control capabilities for a comprehensive threat management framework
- Simplifies administrative functions with Junos Space Virtual Director, an intelligent, automated life cycle management application at no additional cost
- 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

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services that are 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 www.juniper.net/us/en/products-services.

Specifications

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

Table 5: vSRX Services Gateway 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 (generic routing encapsulation, IP-IP) • IPsec, Data Encryption Standard (DES) (56-bit), triple Data Encryption Standard (3DES) (168-bit), Advanced Encryption Standard (AES) (128-bit+) encryption • Message Digest 5 (MD5), SHA-1, SHA-128, SHA-256 authentication • 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 confirm for changes • Auto-record for diagnostics • Software upgrades • J-Web • CLI	• Supports VMware vSphere 5.0. 5.1, 5.5, KVM CentOS 63, Ubuntu 14.04 and Contrail

Ordering Information

For more information about Juniper Networks vSRX Services Gateway, please go to www.juniper.net or contact the nearest Juniper Networks sales representative.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.

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
Fax: +1.408.745.2100
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
Fax: +31.0.207.125.701

1000489-004-EN Feb 2015