vSRX Services Gateway: Protecting the Hybrid Data Center

Extending Juniper Networks award-winning security products to virtualized, cloud-based, and hybrid IT environments

Challenge

Virtualization and cloud computing technologies are introducing new security vulnerabilities that physical legacy security systems cannot adequately protect against.

Solution

vSRX brings the power of Juniper's award-winning SRX Series Services Gateways to virtual, cloud, and hybrid IT environments. Delivering a complete virtual solution to enterprises and service providers, vSRX includes core firewall, robust networking, advanced security, and automated VM management.

Benefits

- Extends SRX Series capabilities to your virtualized and cloud environments, directly addressing the new security vulnerabilities introduced by those technologies
- Enables you to rapidly provision security infrastructure, wherever and whenever it's needed on your network
- Implements critical security controls within your virtual infrastructure, not just at the perimeter, eliminating blind spots

The last few years have seen a rapid move to virtualization and cloud technology. According to Gartner, organizations had virtualized 50 percent of their server workloads by mid-2014, a number that is expected to increase to 86 percent by 2016. And the global cloud market is maturing quickly. IDC predicts it will reach $118 billion this year and $200 billion by 2018, and it is small wonder that organizations are eagerly adopting these technologies, given their proven benefits. They can achieve tremendous reductions in capital expenses by eliminating extra hardware and excess data center space. They can also significantly reduce operational expenses due to lower power and cooling requirements, as well as simplified infrastructure maintenance that frees up IT staffs for more important duties.

The Challenges

In most cases, your physical data center will not disappear as these growth trends play out. Instead, it will evolve into a hybrid environment, incorporating a mixture of physical and virtual computing technologies—including both public and private clouds. You'll face even more challenging security risks within these hybrid environments than you have protecting your physical data center today. And you won't be alone with these challenges when making the shift to a hybrid data center architecture.

The problem is that today, many organizations still rely exclusively on physical security. As hackers and malware grow more sophisticated, the stopgap measure of trying to protect virtual assets with physical security mechanisms becomes increasingly ineffective, undermining your ability to fully leverage the new computing paradigms and achieve high ROI.

For example, when physical firewalls are used to address virtual traffic, this traffic must be routed out of the virtual environment, passed through the physical security infrastructure, and then redirected back into the virtual environment.

This kind of "hairpinning" adds complexity, increases instability, and decreases your ability to move workloads around.

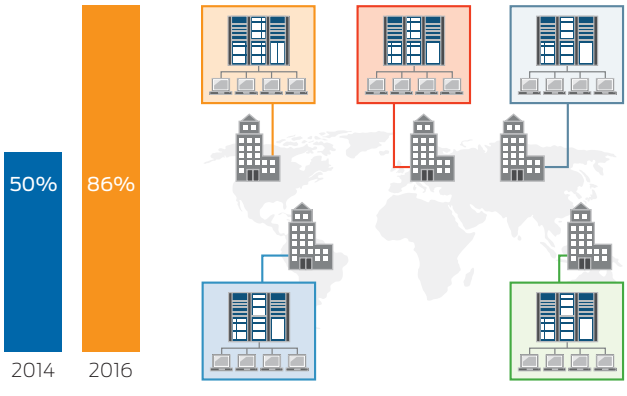

Figure 1. Global explosion in virtualization.

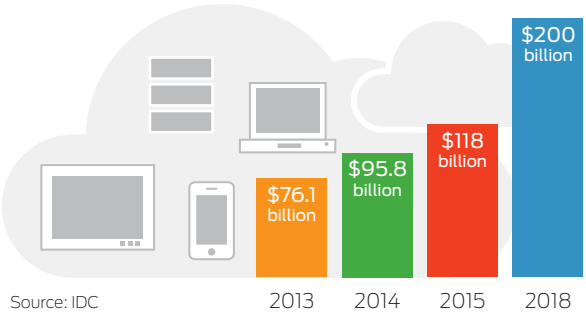

Figure 2. Cloud is quickly becoming a mainstream technology.

Security Risks Unique to Virtual Environments

The security risks that impact physical environments impact virtualized environments to the same—or an even greater—extent. In addition, security professionals must address new risks that are unique to virtualized environments, and which exist within each layer of the virtualization stack: the host, the hypervisor, and guest layers.

Recent high profile attacks have shown that cyberthreats exploit common applications to bypass controls; then, once inside your network, they move with little resistance while hiding in plain sight. An attack on or compromise of your virtualized environment is arguably even more serious than an incident in a physical environment. Your workloads and associated data—which can possess different trust levels—are centralized, with no security barriers in between to keep them segmented. So if your virtual environment is compromised, the attacker has access to everything. An additional challenge to securing your data center workloads is the fact that security policies and associated updates cannot keep pace with the speed of your workload (or VM) changes, resulting in a weakening of your overall security posture.

Figure 3. Global revenue forecast for virtual security appliances (Source: Infonetics).

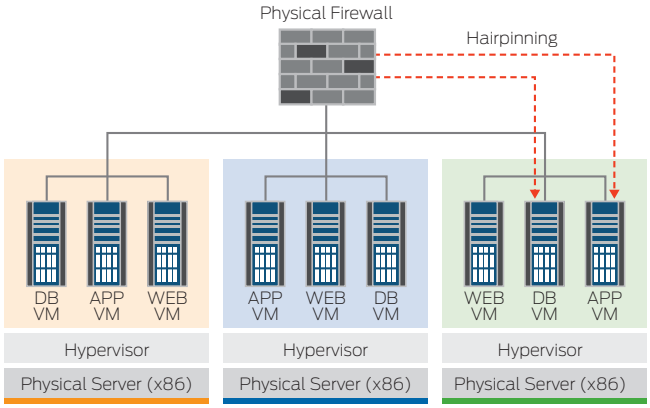

Figure 4. Virtualized servers + non virtualized security = hairpinning

Table 1. Security Risks Unique to Virtual Environments

Mixed-trust workloads	Sensitive data, previously restricted to trust domains, now coexists with other data, increasing the risk of data loss.
Self-service virtual provisioning	Security is left to nontraditional security staff.
Compromised virtualization layer	One compromised layer can immediately impact all hosted workloads.
Host hypervisor (the new attack target)	An attack on the host's hypervisor can potentially compromise all workloads delivered by that host.
Traditional network security tools in virtual environments	Network tools that rely on physical- or network-layer attributes to protect servers and applications are particularly vulnerable to security breaks.

What's needed to overcome these many challenges is a new kind of security—a virtual one that can scale as easily as the virtualized and cloud-based resources themselves. Such a solution needs to provide robust defense against a variety of sophisticated threats, yet still achieve desired performance, scalability, availability, and visibility.

Juniper Networks® vSRX Services Gateway (formerly Firefly Perimeter) is that new kind of virtual security solution.

The Juniper Networks vSRX Services Gateway Solution

vSRX Services Gateway is a virtual firewall that offers the rich functionality of Juniper's award-winning SRX Series Services Gateways in a virtual machine (VM) format.

Powered by Juniper Networks Junos® operating system, the vSRX virtual firewall delivers a complete, integrated virtual security solution that includes core firewall, robust networking, L4-L7 advanced security services, and automated VM life cycle management capabilities for organizations. The automated VM life cycle management 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 VM management application with the power of Junos Space Security Director, security administrators can quickly manage all phases of security policy life cycle for physical and virtual assets from a common, centralized platform. Moreover, the vSRX 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 third-party SDN solutions, and it can be integrated with next-generation cloud orchestration tools such as OpenStack, either directly or through rich APIs.

vSRX is a flexible solution designed to keep your VMs secure while addressing the operational challenges raised by virtualized and cloud environments. In many cases, organizations wish to replace physical with virtual appliances, and vSRX can deliver the more agile virtual infrastructure that service providers or cable operators need in their data centers.

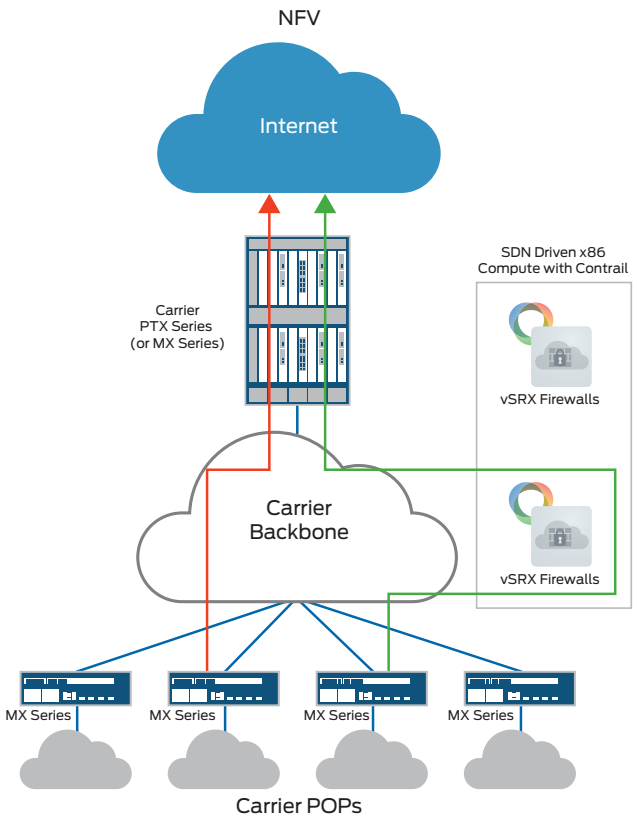

Figure 5. vSRX supports SDN and NFV solutions

Features and Benefits

The vSRX Services Gateway combines core firewall, robust networking, advanced security services, and automated management in a VM format. It provides virtualization defense that is unmatched by other solutions in terms of reliability, scalability, efficacy, and visibility. The vSRX:

- Extends proven SRX Series capabilities to a virtual platform
- Delivers robust connectivity and routing features based on the power of Junos OS
- Provides mission-critical reliability for business continuity
- Integrates virtualization-specific advanced security services for a comprehensive threat management framework
- Automates the VM life cycle, from provisioning to decommissioning
- Unifies security policy management across physical and virtual environments
- Supports a variety of SDN and NFV solutions

Solution Components

Nonintegrated legacy systems built around traditional firewalls and individual standalone point solutions can no longer protect against today's sophisticated attacks. The vSRX all-in-one virtual firewall provides core firewall, rich networking, and L4 to L7 advanced security services so that you can protect your virtual assets from the evolving threat landscape. Juniper's solution includes the following components:

Complete Firewall

- Includes stateful packet processing and an application-layer gateway for virtualized and cloud environments
- Supports active/passive and active/active high availability (HA) deployment options for VMware and KVM

Rich Connectivity and Routing Features

- Includes IPsec VPN, Network Address Translation (NAT), and advanced routing in a flexible VM format based on the proven Junos OS foundation

Advanced Security Features

- Provides virtualization-specific L4 to L7 advanced security services that incorporate unified threat management (UTM), intrusion prevention system (IPS), and AppSecure 2.0 services for a comprehensive threat management framework

Unified Threat Management

- Encompasses comprehensive content security with best-in-class antivirus, antispam, Web filtering, and content filtering features to protect against:
  - Malware attacks that can lead to data breaches and lost productivity
  - Advanced persistent threats perpetrated through social networks and the latest phishing scams
  - Malicious URLs that can significantly reduce the network bandwidth for business-essential traffic

Intrusion Prevention System

- Inspects attack data and takes an action such as blocking the intrusion as it develops or creating a series of rules in the firewall to help you:
  - Minimize false positives by offering flexible signature development
  - Improve accuracy of signatures through precise context of protocols
  - Accurately identify attacks
  - Overcome attempts to bypass other IPS detections using obfuscation methods
  - Simplify installation and maintenance while ensuring the highest network security
  - Perform active/active IPS monitoring

AppSecure 2.0 for vSRX

- Provides application visibility and control features that help protect virtualized and cloud environments from sophisticated application-based threats. vSRX supports AppSecure 2.0 capabilities such as AppTrack, AppFW, and AppQoS that, working together:
  - Track application usage to identify high-risk applications and analyze traffic patterns, improving network security
  - Enhance security policy creation and enforcement based on applications rather than traditional port and protocol management and analysis
  - Prioritize traffic as well as limiting and shaping bandwidth based on application information and context to improve overall performance

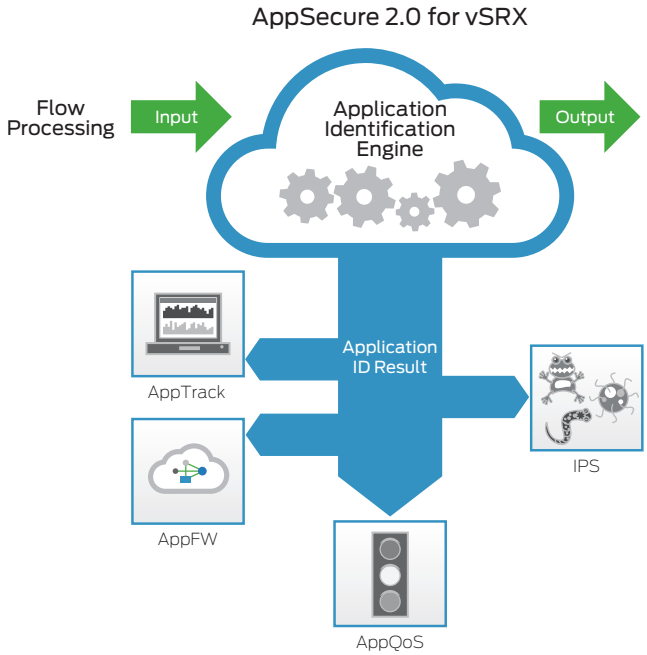

Figure 6. AppSecure 2.0 is tightly integrated with Juniper's IPS solution to further mitigate threats and protect against a wide range of attacks and vulnerabilities.

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 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 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.

Unified Management

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

Use Cases—Real-Life Applications for the vSRX Services Gateway

vSRX can be used in a broad range of virtualized or hybrid data centers. Here are some of the most common use cases for this flexible and integrated network security solution:

- **Private cloud**—vSRX is ideal for private cloud environments in which the cloud and the equipment it runs on are internal to an organization, such as a large enterprise, a university, or a financial institution. In private clouds, the administrators want to rapidly provide their employees or partners with VMs, and segment and secure them within groups such as departments and lines of business.

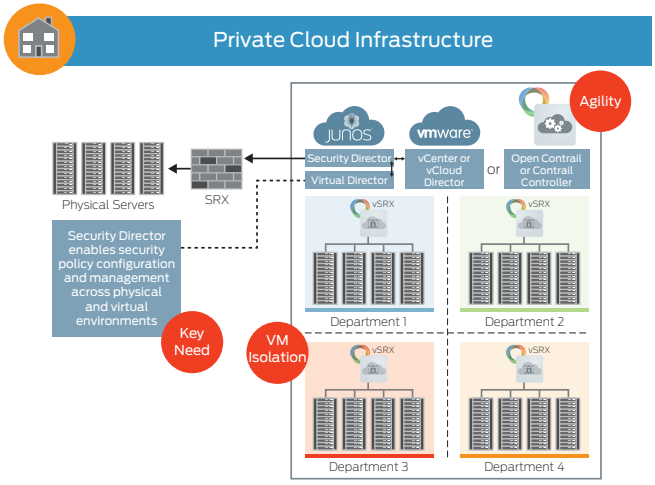

Figure 7. Private cloud use case

- **Public cloud (cloud-hosting providers)**—vSRX is also useful in public clouds in which the cloud hosting providers must deliver strong security for their tenant customers. Public cloud service providers can deploy vSRX to protect their customers by placing the virtual firewall in front of each customer's individual hosting environment, keeping the hosting environments separate from each other.

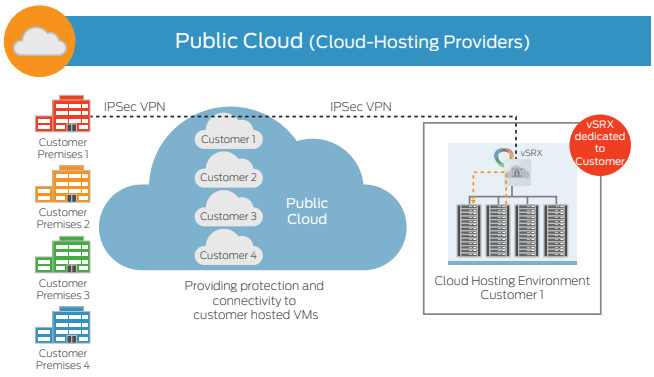

Figure 8. Public cloud (cloud-hosting providers) use case

- **Public cloud (managed security service providers)**—vSRX can provide the virtual protection required by managed security service providers (MSSPs) that deliver cloud services with tenant VMs and manage dedicated firewalls and secure VPNs. Unlike cloud hosting providers, MSSPs do not host their end customers' VMs, yet still want the ability to quickly create virtual firewalls and connectivity rather than procure physical equipment for each new request.

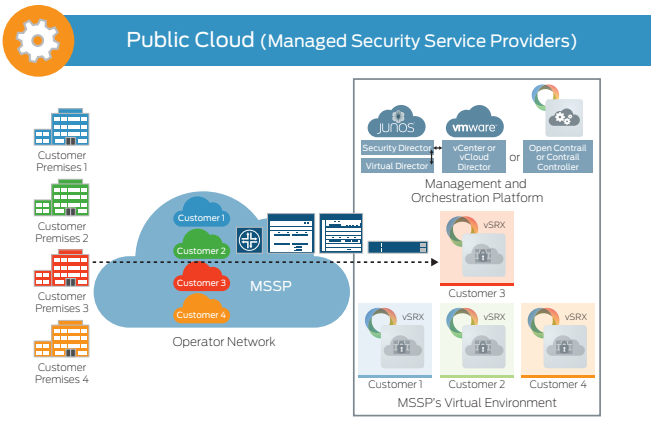

Figure 9. Public cloud (managed security service providers) use case

Summary—vSRX Protects the Data Center in an Increasingly Virtualized World

The vSRX virtual firewall offers the rich functionality of Juniper's award-winning SRX Series Service Gateways in a virtual machine (VM) format. Powered by Junos OS, the vSRX extends Juniper's best-in-class security products to virtualized cloud-based and hybrid IT environments.

vSRX gives organizations a complete, integrated virtual security solution that includes core firewall, robust networking, L4-L7 advanced security services, and automated VM life cycle management capabilities. It provides mission-critical reliability for business continuity and unifies security policy management across physical and virtual environments. vSRX can be used in a broad range of virtualized or hybrid data centers that include private cloud infrastructure, public cloud (cloud hosting providers), and public cloud (managed security service providers).

Next Steps

To learn more about how your organization can benefit from the vSRX Services Gateway, please visit www.juniper.net or contact your Juniper Networks 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

3510547-001-EN June 2015