Learn About Security Virtualization

This *Learn About* introduces the fundamentals of security virtualization and explains how a virtual security appliance can provide security and networking services in virtualized private or public cloud environments.

For those readers needing field knowledge, this *Learn About* also reviews the core functions of the vSRX Services Gateway, the Juniper Networks solution for security virtualization, and details how this virtual firewall solution is increasingly necessary to the network security of countless businesses and organizations.

Virtualizing Network Elements

Virtualization has become an important focus of the IT world because it fundamentally centralizes administrative tasks while improving scalability and workloads, which can lead to the consolidation of network infrastructure, lower OPEX, greater security, ease of management, and other benefits. That's why virtualization technologies are poised to change the landscape of the industry as they move to the cloud, further consolidating network infrastructures.

However, in most organizations, security technologies and practices have not yet adapted this fundamental change in IT infrastructure to the cloud. For example, many organizations do not realize that using their existing legacy security solutions to address the prevailing threat landscape in virtual environments can expose them to new types of attacks and data loss.

Introduction to Virtualization

Virtualization is the process of running multiple virtual instances of a device on a single physical hardware resource. A very basic virtualization system consists of a host operating system, a hypervisor, and a guest operating system as shown in Figure 1.

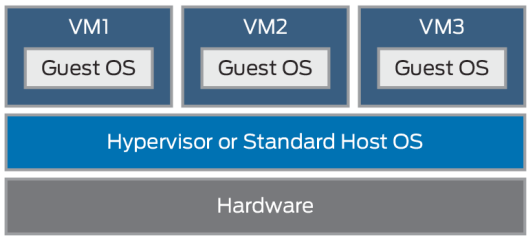


Figure 1 Virtualization Components

The host is the underlying hardware of the virtualization system that provides computing resources to support guests' virtual machines (VM). The host contains all the physical interface cards, CPUs, memory, and Ethernet management ports, and the host also contains the base operating system, applicable third-party software, and the hypervisor. All of this enables the host to contain one or more VMs (or partitions) and share physical resources with them.

A hypervisor, also called a virtual machine manager (VMM), is a program that allows multiple operating systems to share a single hardware host, with each operating system appearing to have all the host's resources all to itself. So the hypervisor handles resource and memory allocation of the host for all the VMs, ensuring they cannot disrupt each other. It also provides various interfaces for administration and monitoring tools.

There are two types of virtualization hypervisors:

- Bare-metal hypervisor (Type 1) runs on top of the hardware. This hypervisor does not require a server operating system and has direct access to the hardware. Some bare-metal hypervisors are embedded into the firmware suite of the computing platform.
- Hosted hypervisor (Type 2) is installed on top of the host operating system.

Here, the hypervisor controls access, shares underlying hardware resources, and partitions your physical server hardware into multiple VMs (guests).

A VM is an instance created by utilizing the physical hardware resources. VMs run on top of a host machine and share the same physical host resources as other VMs; they truly do act like a real computer with their operating system and devices (virtual hardware – CPUs, Memory, I/O). Each VM is completely separate and independent, and can run simultaneously on a single computer.

So you can begin to see the benefits of virtualization systems, where one hardware platform can support dozens of VMs, each doing a specific task, or number of tasks. Enterprises are adopting these virtualization systems to increase their overall efficiency by consolidating servers, streamlining operations, and reducing costs. Some businesses are consolidating whole data centers.

The benefits of virtualization are many: optimizing resources, simplifying management, delivering high availability, minimizing downtime, and much, much more. But it's important to note that the security of the virtualization system is based on the security of the host operating system. Any breach to the host operating system could potentially result in an attacker obtaining complete control over the virtualization system.

Security Challenges in Virtualization

While virtualization technology is cutting down administration and OPEX costs, it's also introducing new security challenges that physical security systems cannot adequately protect against:

- File sharing between hosts and guests is not secure.
- Isolation and communication between separated components such as guest OSs and applications, hypervisors, hardware, and virtualization management systems are sometimes weakened to allow for inter-OS communication or for performance reasons.
- In virtualization, multiple servers are consolidated onto one host, removing the physical separation between servers, and increasing the risk that a compromise may spread from one application to others on the same host.

Compromised virtualization layers and an attack on the host hypervisor can lead to a compromise of all hosted VMs as well as the shared physical resources delivered by that host. If the hypervisor is compromised, any attached VMs will also be compromised.

So when the hypervisor is attacked and is taken over, the attacker gains full control over all the data that's in the hypervisor environment. Similarly, VMs that are not isolated can have full access to host resources, so any compromise of the VM can lead to a compromise of the resources.

Virtualization adds new layers of infrastructure complexity, so much so that monitoring for unusual events and anomalies becomes more complex, which in turn makes it more difficult to identify security issues, such as advanced persistent threats.

There is also a lack of visibility into traffic between VMs that never touch the physical network; VM-to-VM traffic in virtualized environments complicates the ability to attach security policies to VM instances and track those security policies to ensure continued regulatory compliance.

The dynamic nature of virtualized environments also presents new challenges for intrusion prevention systems (IPS). Malware created to target both physical and virtual machines causes infection via the virtual network. Undetected and uncontained malware outbreaks or insider attacks in the virtual environment also pose problems. Other security threats include unauthorized access, denial of service, exploits, and so on.

Clearly, we want to keep virtualized systems for all the benefits they bring, but we need to deal with the security overhead they require. Traditional network security tools are just not adequate in virtual environments. Firewalls must rely on physical or network layer attributes to protect servers and applications that are particularly vulnerable to security breaks, and security products designed for individual physical servers and workstations can cause serious problems in virtualized environments.

Juniper Networks has addressed these security challenges by extending the capabilities of their award-winning SRX Series Services Gateways into the virtual world.

The Virtual Firewall: the vSRX Services Gateway

The vSRX Services Gateway is a stateful firewall that integrates with a hypervisor at the kernel and inspects and secures traffic at the virtual layer, between VMs on a single host, or between VMs on a virtual network. The vSRX allows network and security administrators to quickly and efficiently provision and scale firewall protection to meet the dynamic needs of virtualized and cloud environments. Figure 2 illustrates a typical Juniper Networks virtualization solution that includes the vSRX.

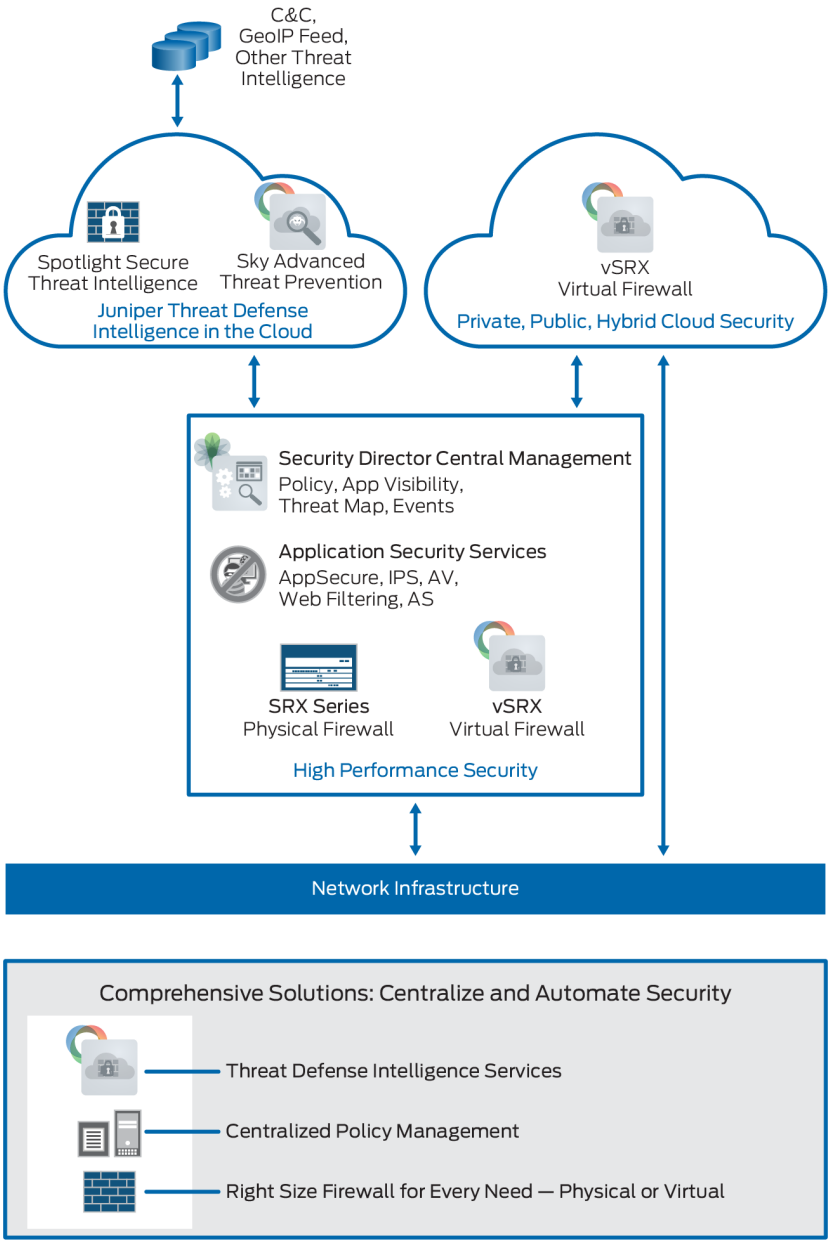


Figure 2 Juniper Networks Security Virtualization

The vSRX brings the Junos operating system to x86-based virtualization environments, enabling it to deliver a complete, integrated virtual security solution including network firewall, IPS, and VPN technologies. The vSRX also integrates a comprehensive set of next-generation firewall technologies: Layer 7 application control, availability, traffic flow optimization, web filtering, antivirus, anti-spam, and network access control enforcement.

You can see in Figure 2 that using both the SRX Series and vSRX platforms defends applications and protects data as it moves across the wide area between enterprise and cloud facilities, and between and within data center devices. The vSRX can be used in the same way as a physical appliance. For example, it can be used for segmentation of traffic in a cloud service model, or a dedicated edge device per user in a hosted service, or a virtual CPE for MPLS service, or simply as a more robust alternative to a host-based firewall.

The vSRX can act as barrier to secure perimeter access to a network. It provides dedicated security services and assured traffic isolation within the cloud, along with customizable firewall controls as an additional managed service. So the vSRX is ideally suited for organizations that are standardizing hardware platforms or deploying virtual environments.

Enterprises and service providers can leverage their virtualization investment to create a granular security perimeter, giving dedicated security resources within a cloud construct to both tenants and service subscribers. The vSRX also supports the Juniper Networks Contrail product, OpenContrail, a variety of Network Functions Virtualization (NFV) use cases, and third-party SDN solutions, and it can be integrated with next-generation cloud orchestration tools such as OpenStack, either directly or through APIs. (For a full list of vSRX features and benefits, see the *Resources and References* section at the end of this *Learn About*.)

To better understand security virtualization, let's walk through three use cases using the virtual firewall capabilities of the vSRX, placing the virtual firewall at the perimeter or edge in virtualized private- and public-cloud environments:

- Public Cloud Use Case (Cloud-Hosting Providers)
- Public Cloud Use Case (Managed Security Service Providers)
- Private Cloud Use Case

Public Cloud (Cloud-Hosting Providers)

In the public cloud, service providers can host large numbers of VMs—in some cases exceeding 50,000— for their tenant customers. And in a public cloud, all the segmented groups, or tenants, belong to different companies, so each one has its own usage patterns. Therefore, the public cloud service provider must accommodate ever-shifting workload sizes, that are also scalable and elastic.

With the vSRX such service providers can provide their customers with the security required, both inside their virtualized data centers and at the tenant virtual network edge. Important vSRX benefits are:

- Customer segmentation
- Edge security
- Control access to the VMs
- Granular control over physical and virtual assets

Figure 3 shows this public cloud use case solution topology. It includes the vSRX working with Junos Space products, Juniper Networks Secure Analytics virtual appliances, and VMware products that are deployed in the cloud infrastructure.

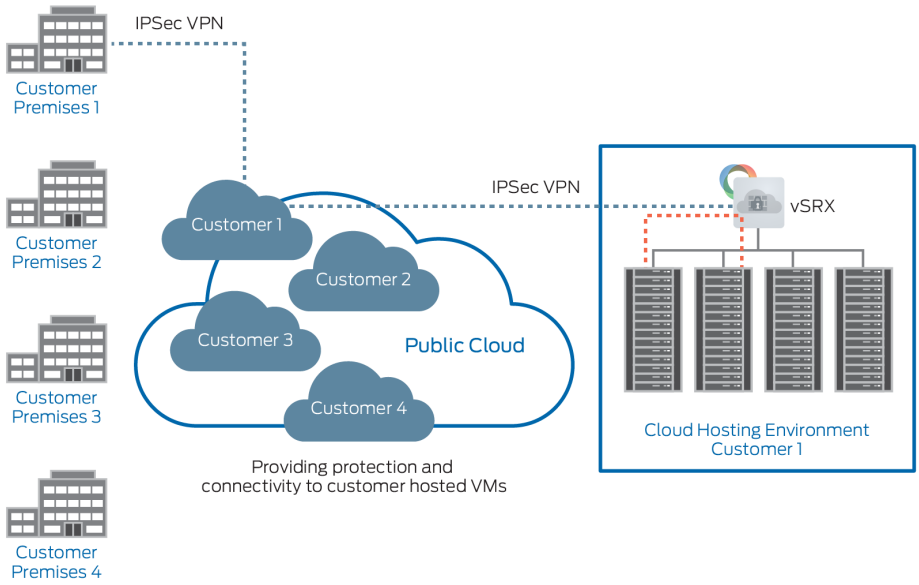


Figure 3 Public Cloud Use Case Topology (Cloud-Hosting Providers)

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. The vSRX offers rich routing, VPN, and Network Address Translation (NAT) features, and its simple provisioning allows service providers to easily connect tenants from the public cloud to their private cloud.

Finally, a variety of management interfaces for vSRX enables VMs to be securely initiated via the bootstrap settings and then managed via the CLI, J-Web, or Junos Space Virtual Director.

Public Cloud Use Case (Managed Security Service Providers)

Large telecom service providers and managed security services providers offer complete security services to their customers, including dedicated firewalls and IPsec VPNs. *Virtual* security services can be deployed in a number of ways in this general use case. For the vSRX, the service provider might typically consolidate services on virtual hardware at their site and then offer the virtual firewall as a fully managed service. The vSRX can offer:

- Customer segmentation
- Security
- Compliance
- Reduction of CAPEX and OPEX

Figure 4 illustrates the software and hardware products such an extensively managed security services data center might contain, using other, appropriate, Juniper Networks products.

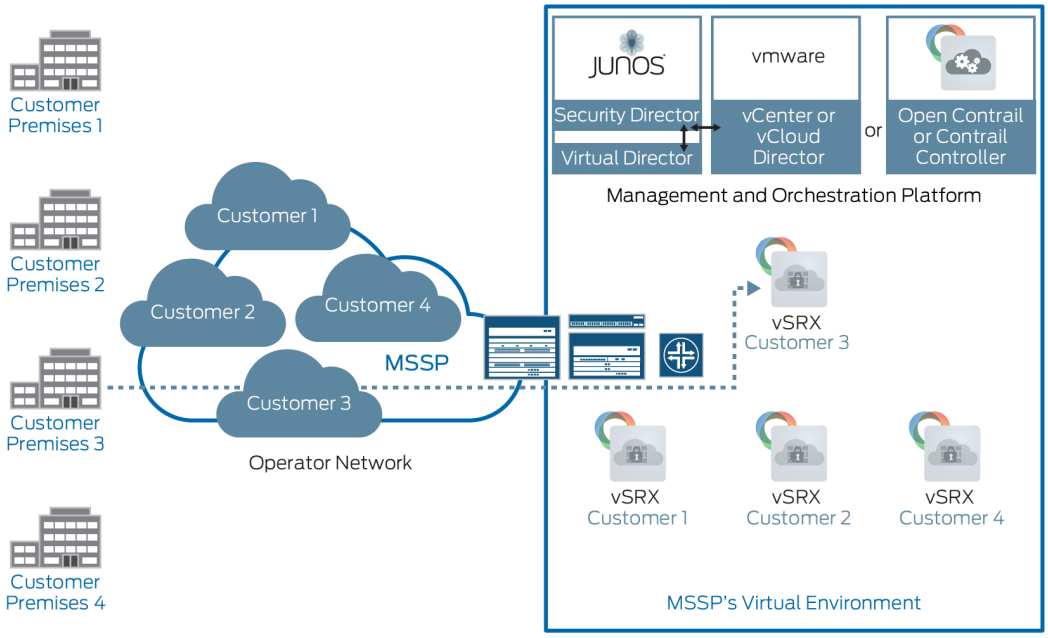


Figure 4 Public Cloud Use Case (Managed Security Service Providers)

Managed security services providers can use the vSRX to offer security services to customers with multiple remote locations. That's because a single vSRX instance can be used for many remote locations. For example, the service provider's customer might have many remote retail stores, coffee shops, or outlets. By using the vSRX instance that resides on the service provider's infrastructure, there's no need to have devices at every remote store branch or site. The security services provider hosts and manages the vSRX, which, with the combination of the vSRX VM management application and Junos Space Security Director, enables the service provider to manage all phases of the security-policy life cycle, for both physical and virtual assets, from a common, centralized platform. It's one of the ways that security virtualization is transforming networks.

Private Cloud Use Case

Private clouds are used exclusively for their owner's needs. They are common solutions for large enterprises, universities, and financial institutions.

Private clouds allow their owners to maximize resources by pooling and sharing them, but the use of virtualized, pooled resources in a private cloud can challenge privacy requirements unless security for the virtualized environment is implemented.

To keep data private, and protect it, the private cloud owner can segment their virtualized environments into groups, such as business units or corporate departments, and then use the vSRX to secure those groups differently based on internal or regulatory requirements. The vSRX can provide all the necessary virtual benefits:

- Securely communicate via routing, NAT, and VPNs
- Provide edge security
- Keep and provide functional separation
- Support compliance and regulatory needs

Figure 5 illustrates this private cloud use case topology, using security virtualization via the vSRX, Junos Space products, Juniper Networks JSA Series Secure Analytics Virtual Appliance, and the VMware products that are deployed in the cloud infrastructure.

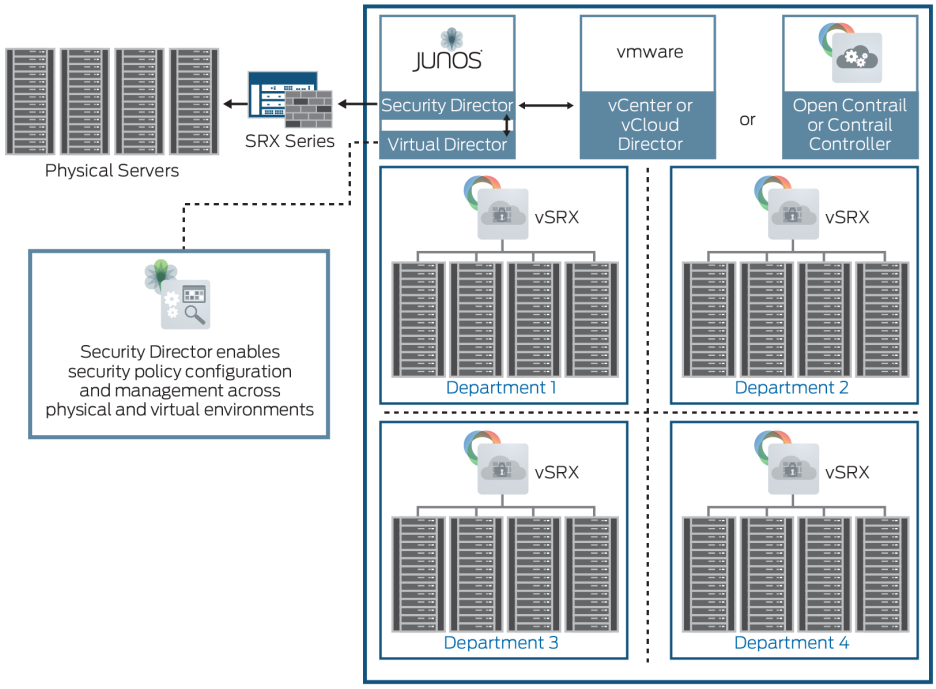


Figure 5 Private Cloud Use Case Topology

In Figure 5, a private cloud administrator can deploy multiple vSRX instances to secure the virtualized environment even at the VM level and the network edge of each segmented group. The vSRX provides customized security for the virtual environments, automation for operational ease and efficiency, and granular control over the physical and virtual assets. By combining Junos Space Security Director with Virtual Director, administrators can improve policy configuration, management, and visibility into both physical and virtual assets from one common, centralized platform.

Use Case Summary

The vSRX Services Gateway is designed to facilitate security deployment for virtualized environments. These three use cases are but a few examples of security virtualization in action, where administrators can now use product GUIs to provision and deploy security to protect VMs and their traffic.

Resources and References

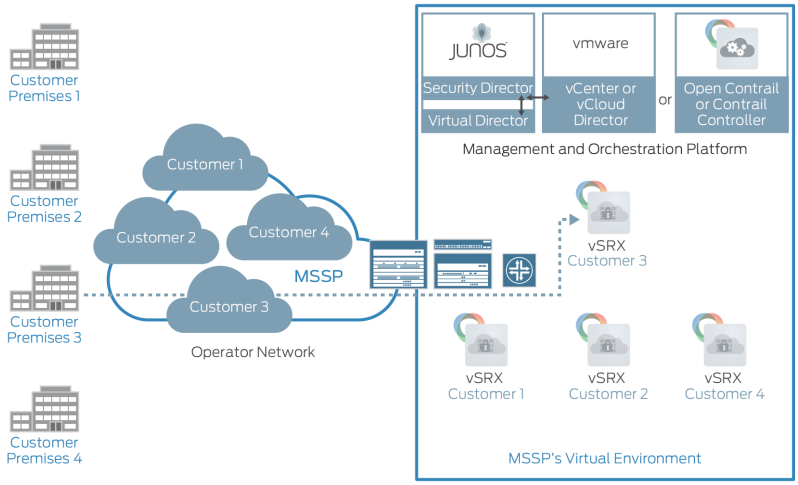
- The vSRX Data Sheet:
  http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000489-en.pdf
- The vSRX Product Page
  http://www.juniper.net/us/en/products-services/security/srx-series/vsrx/
- The Juniper Networks technical documentation includes everything you need to understand and configure all aspects of vSRX:
  http://www.juniper.net/techpubs/en_US/vsrx15.1x49-d40/information-products/pathway-pages/security-vsrx-15.1x49-d40-software-version-index.html
- A vSRX introduction video. This video provides an overview of the architecture and use cases for the solution:
  https://www.youtube.com/watch?v=UXeJf6QZN9Y
- The VMware page to know more about virtualization technology and its features:
  http://www.vmware.com/in/virtualization/overview
- Resources for virtualization basics:
  https://itechthoughts.wordpress.com/2009/11/10/virtualization-basics/

Learn About Security Virtualization

by Madhavi Katti

The dynamic and flexible nature of virtualization and cloud computing can easily lead to a loss of visibility and control, traits always taken for granted in administering physical networks. So it's important to adopt an approach that secures virtual assets without compromising performance, availability, and management control. Let's learn about securing virtual networks!

.



About the Author:
Madhavi Katti is an Information Development Engineer at Juniper Networks with over 10 years of experience in writing and developing documentation for networking and telecommunications.

Author's Acknowledgments:
Thanks to Patrick Ames, Nancy Koerbel, Julie Wider, Lisa Eldridge, and Karen Joice for their engagement in this project, and to project promoters Mindy Isham and Indira Upadhayaya

Version History: First Edition, April 2016 2 3 4 5 6 7 8 9

For more information go to the TechLibrary at: www.juniper.net/documentation