COMPREHENSIVE SECURITY FOR TODAY'S DATA CENTER

Protecting Your Physical and Virtual Infrastructures with SRX Series Services Gateways and the vGW Virtual Gateway

Challenge

Data centers supporting private clouds need to secure both their physical and virtual infrastructures. Traditional methods of securing these zones typically require trade-offs such as negative performance impacts or reduced visibility into tenant VMs.

Solution

Juniper Networks SRX Series Services Gateways, integrated with the vGW Virtual Gateway, work in concert to provide consistent application of security policy throughout the physical network and within the virtualized network.

Benefits

- Guarantee integrity of zones on hypervisor
- Automate and verify that VM connectivity complies with zone policy
- Identify and mitigate VM policy violations
- Empower the SRX Series network with knowledge of VMs and their zone locations

Thanks to the exploding adoption of virtualization, a new type of data center is here. Architected for cloud computing, this new data center is a mix of physical servers and virtual workloads—and this means that it requires an even more pervasive range of security. As nearly every business and organization in the world implements some degree of cloud computing, virtualization security will be as integral a component as traditional firewalls are in today's networks. In fact, the virtualization security market is one of the fastest growing market segments of this decade, with various analysts putting the five-year opportunity in the hundreds of millions to billions of dollars.

Juniper not only understands the security requirements of the new data center, but its solutions are prepared to adequately address these needs. Combining the new Juniper Networks® vGW Virtual Gateway with the high-end Juniper Networks SRX Series Services Gateways, Juniper offers the most comprehensive security suite for all critical workloads—regardless of the platform on which they run.

The Challenge

At its simplest, the "cloud" is an Internet-based environment of computing resources comprised of servers, software, and applications within a data center that can be accessed by any individual or business with Internet connectivity. Cloud computing offers significant benefits to enterprises using clouds, as well as to enterprises offering cloud services. In a rush to implement virtualized networks and data centers, however, some organizations are struggling with how to reconcile competing priorities to virtualize their environments, while still ensuring that existing requirements for protection and visibility are maintained.

These challenges are much bigger than an initial glance might suggest. Collapsing multiple servers into a single one comprised of several virtual machines (VMs) literally eliminates all firewall, intrusion detection, and other protections in use prior to virtualization. Physical security measures literally become "blind" to traffic between VMs, since they are no longer in the data path. Consequently, they cannot enforce protections and maintain control. Further increasing the risks to virtualized traffic are the very features and functions that make virtualization highly desirable for optimal resource use.

Common approaches to security pose their own risks. VLAN segmentation, for example, extends the notion of LAN resource segmentation to include VMs, essentially requiring that VMs, which can naturally be grouped (e.g., by function or user base), be isolated from other VMs using virtual switches and routing (e.g., the HR VLAN contains HR-serving VMs). However, VLAN segmentation is not a permanent solution to securing virtual environments because of the networking complexities, performance degradation, and security limitations of the approach.

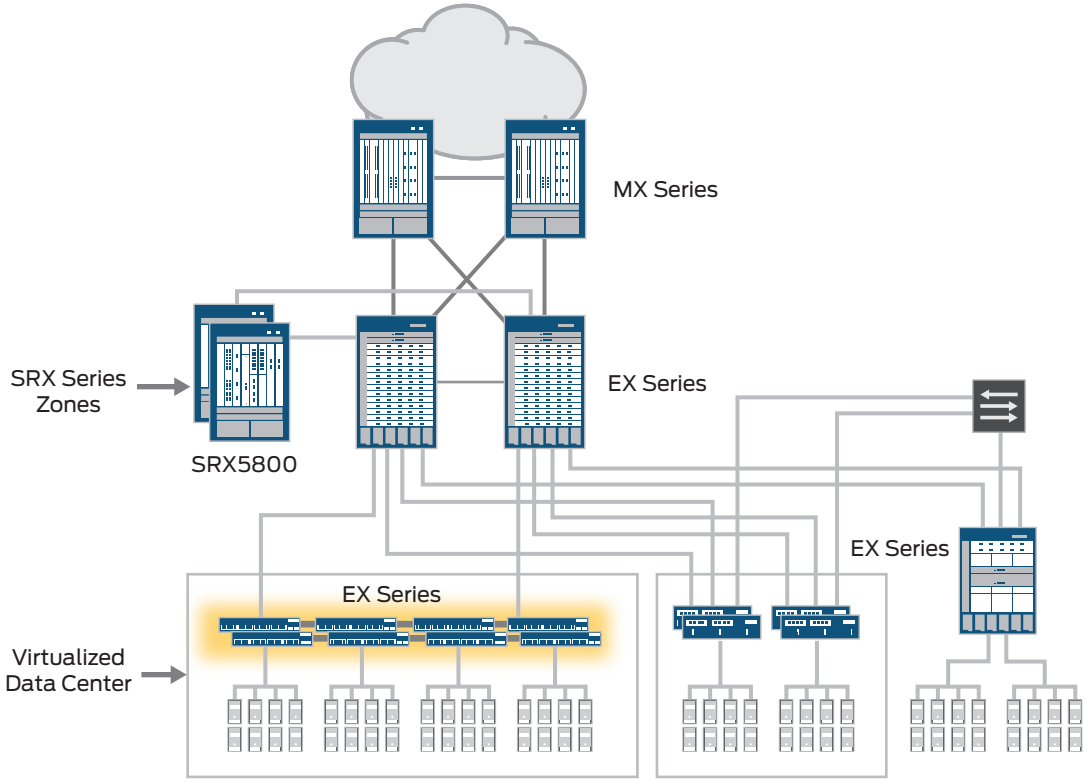

Figure 1. In today's data center, security is needed across the physical and virtual infrastructure.

Another alternative, software-based firewalls used as agents that run on each virtual machine, seems like a reasonable approach at first glance because it lets users buy a product with which they are familiar. But as VMs increase in number or "sprawl," so does the number of agents that must be managed, making this a costly solution. Security, too, is less than optimal with the agent-based mode, in that there is no protection for the hypervisor (i.e., the virtualization operating system). So attacks that strike by turning "off" VM-based services like the Conficker Worm can bypass agent-based protection.

Juniper Networks SRX Series and vGW Integrated Solution

The SRX Series with vGW Virtual Gateway integration delivers the security necessary for today's data center with its mix of physical and virtualized workloads. Integrated with the SRX Series, the vGW Virtual Gateway queries the SRX Series gateway for its zone, interface, network, and routing configuration. vGW then uses that information with the vGW management system (i.e., Security Design for vGW) to create VM Smart Groups so that users of vGW can see VM to zone attachments, create additional inter-VM zone policies, and incorporate zone knowledge into compliance checks (e.g., Is a Client X VM connected to a Client Y zone?).

Features and Benefits

The SRX Series and vGW together deliver best-in-class security to the data center, enabling security administrators to guarantee that consistent security is enforced from the perimeter to the server VM. The SRX Series delivers zone-based segregation at the data center perimeter. vGW integrates the knowledge collected in SRX Series zones to ensure that zone integrity is enforced on the hypervisor using automated security concepts like Smart Groups and VM Introspection. Together, these solutions deliver stateful firewall and optional malware detection for inter-zone and inter-VM traffic; compliance monitoring and enforcement of SRX Series zones within the virtualized environment; and automated quarantine of VMs that violate access, regulatory, or zone policies.

In terms of the benefits of zone synchronization between the SRX Series and vGW, implementers will have:

- Guaranteed integrity of zones on the hypervisor (i.e., virtualization operating system)
- Automation and verification that VM connectivity does not violate zone policy
- Enhancement of the SRX Series network with knowledge of VMs and their zone location

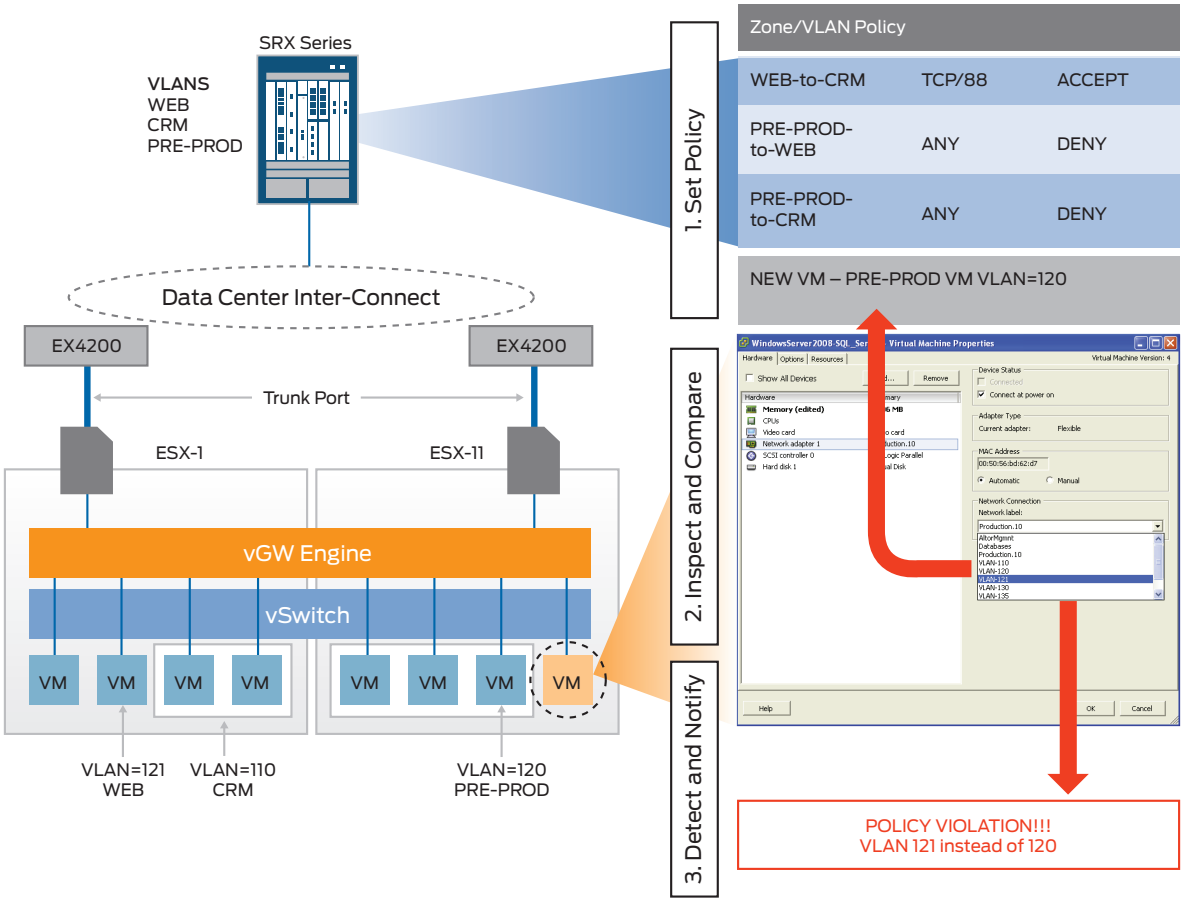

Figure 2. SRX Series gateways with vGW integration detect and resolve issues.

Moreover, thanks to the features and functionality of vGW, additional benefits include:

- **Visibility**—vGW has a complete view of all network traffic flowing between VMs, as well as a complete VM and VM group inventory, including virtual network settings. It also has deep knowledge of all VM states, including installed applications, operating systems, and patch levels, through VM Introspection.
- **Protection**—A VMsafe-certified, stateful firewall provides access control over all traffic via policies that define which ports, protocols, destination VMs, etc. should be blocked. Further, an integrated intrusion detection engine inspects packets for the presence of malware or malicious traffic and alerts as appropriate. Finally, virtualization-specific antivirus protections deliver highly efficient on-demand and on-access scanning of VM disks and files with quarantining of infected entities.
- **Compliance**—vGW enables enforcement of corporate and regulatory policies for the presence of required or banned applications via VM Introspection. Some practical applications of compliance enforcement, such as assurance of segregation of duties, ensure that VMs are assigned to the right trust zones inside the virtual environment. Pre-built compliance assessment is based on common industry best practices and leading regulatory standards. vGW can also enforce a VM "gold" image, ensuring that deviations from the desired VM configuration do not create a security risk.

Summary—Physical and Virtual Security in Concert

Virtualization's undeniable cost and scalability benefits are making it a near de facto choice for data centers and clouds. If virtualizing your servers isn't on your current project short list, it should be soon. While planning or augmenting your virtual environment, it is important to include the integration of monitoring and access control in the mix. Seeing your inter-VM traffic can help you troubleshoot and optimize your virtual network. It can also help you define and refine access controls so that all traffic is business appropriate and enabling.

While it is natural to think existing security tools might have these concerns covered, the fact is that many use legacy technologies as far as virtualization is concerned. And if threats by insiders seem somehow less likely, they are on the rise. For this reason, updates to regulations are underway.

However, you don't have to wait for a forced mandate to have the benefit of virtualization security. The technology to monitor and protect your inter-VM traffic exists and is in broad use worldwide. Your biggest challenge is in understanding the different offerings and choosing the one that best protects your security and virtualization investment.

Combining the vGW Virtual Gateway with the high-end SRX Series Services Gateways, Juniper offers the most comprehensive security suite for all critical workloads—a solution that provides consistent security policy throughout the physical network and within the virtualized network, delivering best-in-class security for the data center.

Next Steps

To learn more about securing the physical and virtual infrastructure within your data center, please 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.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

3510418-001-EN Aug 2011 Printed on recycled paper