AN INTEGRATED SECURITY SOLUTION FOR THE VIRTUAL DATA CENTER AND CLOUD

Protecting Physical and Virtual Workloads

Table of Contents

Executive Summary

As momentum behind cloud computing continues to build at a rapid pace, IT leaders and stakeholders are sifting through vast amounts of information to best understand what advantages this new type of network holds for their environment. Their challenge is to adjust expectations for exaggeration and "hype" so that the true value and return on investment are understood. This means accounting for all dependencies in the cloud computing architecture, including the sourcing and provisioning of security.

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 organizations by maximizing compute resource utilization and reduction in power requirements.

It is estimated that, by 2015, cloud-based services will grow to become a $35.6 billion market[1] and that virtualization as a technology will be the near de facto architecture for clouds. The growth of cloud-based computing is outpacing even the most optimistic predictions based on its compelling value proposition of enabling:

- The rapid development and deployment of services
- Highly scalable compute power
- Adoption of the pay-for-use model of cloud services (i.e., lower CapEx)

Even with the undeniable cost and scalability benefits of virtualization and cloud computing, the evolution of the data center brings a new set of challenges to IT professionals. While the need for physical network security will continue to exist in data centers, organizations will continue to adopt cloud computing in phases, resulting in a mix of physical and virtualized data center workloads. This data center model will result in some workloads like those on physical servers being secured by physical firewalls, while others such as those running on virtual machines (VMs) will likely face security concerns because traditional security methods provide zero visibility into VM traffic.

Security, however, need not be an impediment to adopting cloud computing or taking advantage of the significant cost savings it promises. This paper outlines Juniper Networks' approach to providing pervasive and consistent protection for the entirety of the evolving data center.

Introduction—The Implications of Virtualized Workloads

Virtualization stands to bring enormous cost savings to organizations by significantly reducing the space and electrical power required to run data centers and clouds, and by streamlining the management of an ever growing number of servers. It is no wonder, then, that adoption of virtualization is proceeding at a very rapid rate, and being accelerated by tough economic times and cost cutting mandates. In fact, Gartner estimates that 50 percent of the world's workloads will be virtualized by 2012.[2]

Further, says Neil MacDonald, vice president and fellow at Gartner, "As organizations continue to virtualize their data centers and clouds, workloads of higher sensitivity will be virtualized and the workloads themselves will become more mobile, challenging traditional data center security architectures which rely solely on physical appliance-based enforcement."

With security and compliance concerns being top of mind in virtualization and cloud deployments, 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. Collapsing multiple servers into a single one comprised of several VMs significantly impacts all of the firewall, intrusion detection, and other physical network protections in use prior to the virtualization of workloads. Physical security measures literally become "blind" to traffic between VMs, since they are no longer in the data path (Figure 1). Consequently, they cannot enforce protections and maintain control.

[1]Source: Analysys Mason, 2010
[2]Source: Gartner, 2010

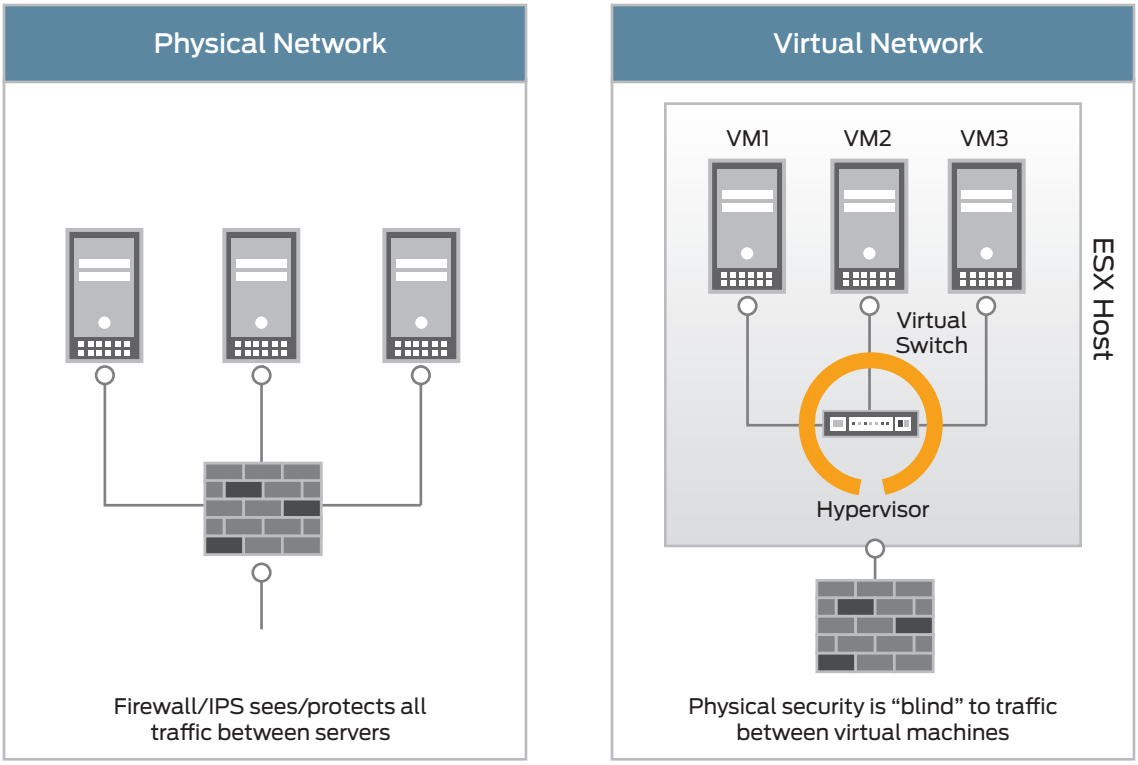

Figure 1: Security implications of virtualizing workloads

Making the virtualization security challenge even more acute is the highly dynamic nature of VMs. For instance, VMware, the leader in virtualization and cloud infrastructure, provides features like VMotion and Distributed Resource Scheduling (DRS), which allow for hardware and capacity pooling by enabling VMs to move from physical host to physical host as performance needs dictate. VM provisioning is also very quick and easy. IT operations personnel and department administrators can create new VMs using templates or cloning existing ones. So, while virtual environments can scale in a flash, the security policies that control access and suppress malware proliferation cannot—unless the process for doing so is equally automated and scalable. Consequently, the contents of VMs and the applications they host are at high risk from inappropriate access, malicious traffic, and weak (in some cases inherited) security posture. Looking at the implications of virtualized workloads on the evolving data center, it is becoming clear that organizations would greatly benefit from a solution that scales as part of the virtual environment.

An Integrated Security Solution for the Virtualized Data Center and Cloud

Today, we know that technologies to monitor and protect inter-VM traffic for virtualized workloads exist and are in broad use worldwide. We also know that firewalls in the data center will continue to provide valuable security for physical workloads. And with security and compliance concerns being top of mind for IT professionals, what organizations need is an integrated security solution that provides consistent application of security policy throughout the physical and virtualized network.

The Juniper Solution: SRX Series Services Gateways—Protecting Physical Workloads

Juniper Networks® SRX Series Services Gateways are high-performance security, routing, and network solutions for the enterprise and service provider. The SRX Series platform provides high port density, advanced security, and flexible connectivity in a single, easily managed platform that supports fast, secure, and highly available data center operations. The SRX Series is based on Juniper Networks Junos® operating system, the proven OS that delivers security and advanced protection services and is the foundation of the world's largest networks.

SRX Series Zones—Segmenting and Isolating Traffic Among Physical Workloads

A security zone is a collection of interfaces with similar security requirements that define a security boundary. Internal network interfaces may be assigned to a security zone named "trust," and external network interfaces may be assigned to a security zone named "untrust." Security policies, which are associated with zones, are then used to control transit traffic between security zones. A packet's incoming zone, as determined by the interface through which it arrived, and its outgoing zone, as determined by the forwarding lookup, together determine which policy is used for packets in a flow. The SRX Series, a zone-based firewall, offers great efficiencies in three key areas:

- Packet processing
- Security policy management
- Reporting

Packet Processing: If we think about how a "traditional" or non-zone-based firewall works, the firewall contains lists of policies and the policies are processed from top to bottom, in sequential order. Once the firewall obtains a match for the packet, the firewall then applies the policy. For a small policy base, this is a nonissue but as security policies grow, this introduces more and more latency to the packet. With a zone-based firewall, policies are separated based on the source and destination zones. Policies are still processed from top to bottom, but only a subset of the policy base is assessed.

As an example, let's take a look at a basic, non-zoned-based ("traditional") firewall installation with trust, untrust, and DMZ zones. For simplicity purposes, we will use 300 policies. With a traditional firewall, as each packet comes into an interface, it is potentially assessed against all 300 policies until it finds a match to the source, destination, and service, and then an action is taken on the packet. In contrast, with a zone-based firewall, policies are segregated based on zone structures—trust, untrust, and DMZ. In this example (Figure 2), we will assume that there is an even distribution of policies between all three interfaces. This means that there are six available flows, equating to 50 policies per possible flow.

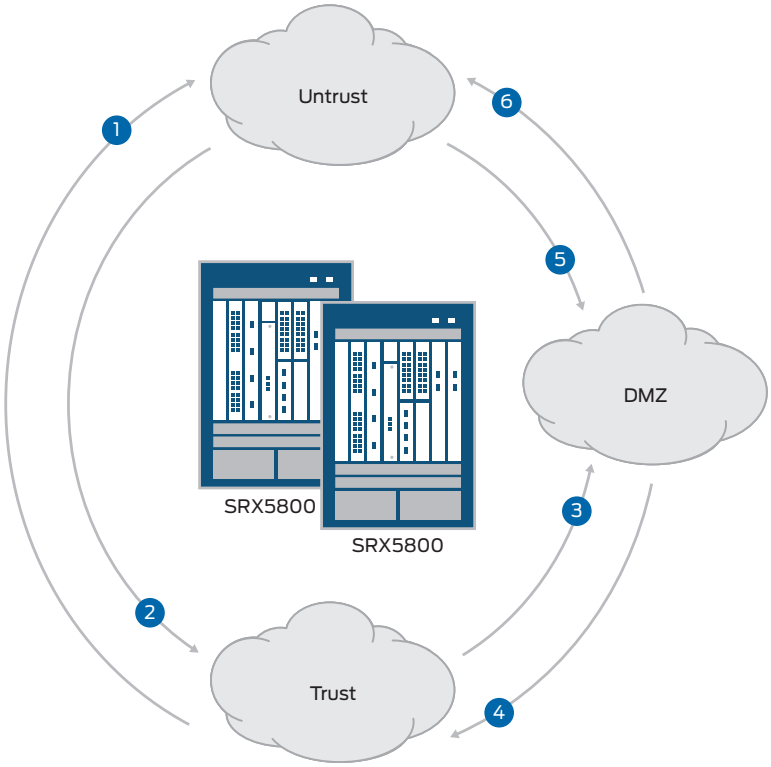

Figure 2: Packet processing

As a packet comes in, the firewall will convert the source and destination interfaces into zones. Furthermore, as the packet is assessed, it will only be assessed against 50 policies, compared to 300 policies in the non-zone-based firewall example. For smaller implementations, the impact is not as great, but as the number of policies increase, the impact grows.

Security Policy Management: When looking at a traditional firewall, the policy is written based on host-to-host information. With this limited information, it can be tough to tell much about the flow other than names and numbers (source, destination, service). Now, in contrast, we have added a new layer—zones—that introduce clarity to the flow. Not only will you see the names and numbers, but you will also see the expected flow of the packet. In the above example, (Figure 2), you can determine that the packet is expected to flow from the untrust zone to the DMZ, or the trust zone to the untrust zone. Being able to easily visualize this information greatly increases policy management. More importantly, by combining this visual aspect with the subset of policies available for a given flow, managing policies also becomes much easier.

Reporting: The visibility and availability of zone data greatly increases the reporting of information and, as a result, zones have become an invaluable tool for compliance reporting like Payment Card Industry Data Security Standard (PCI DSS), Health Industry Portability and Accountability Act (HIPPA), Sarbanes-Oxley Act (SOX), etc. For example, if the firewall receives an http request flowing from A to B, the administrator would first need to understand what A and B are in order to determine if the packet should be allowed to pass. However, if the administrator sees the same request flowing from the untrust zone to the finance zone, the administrator would not have to know what A and B are in order to make the determination that such a packet should not be allowed to flow in this direction, and at the same time could track down the policy that is allowing the packet to pass or write a policy to specifically deny the packet.

Firefly Host—Protecting Virtualized Workloads

TheFirefly Host* is technology based on a four-tiered architecture comprised of a hypervisor-based module, a security virtual machine, a management server, and a Web interface. The hypervisor-based module resides within the hypervisor of each virtual machine host and performs security functions, including packet inspection and security policy enforcement.

The security VM facilitates communication between the Firefly Host management server where security policy information and detail about VMs is stored, and the hypervisor module. The Firefly Host management server stays in constant communication with the VMware vCenter so that as changes to VMs occur, they are synchronized to the Firefly Host management server.

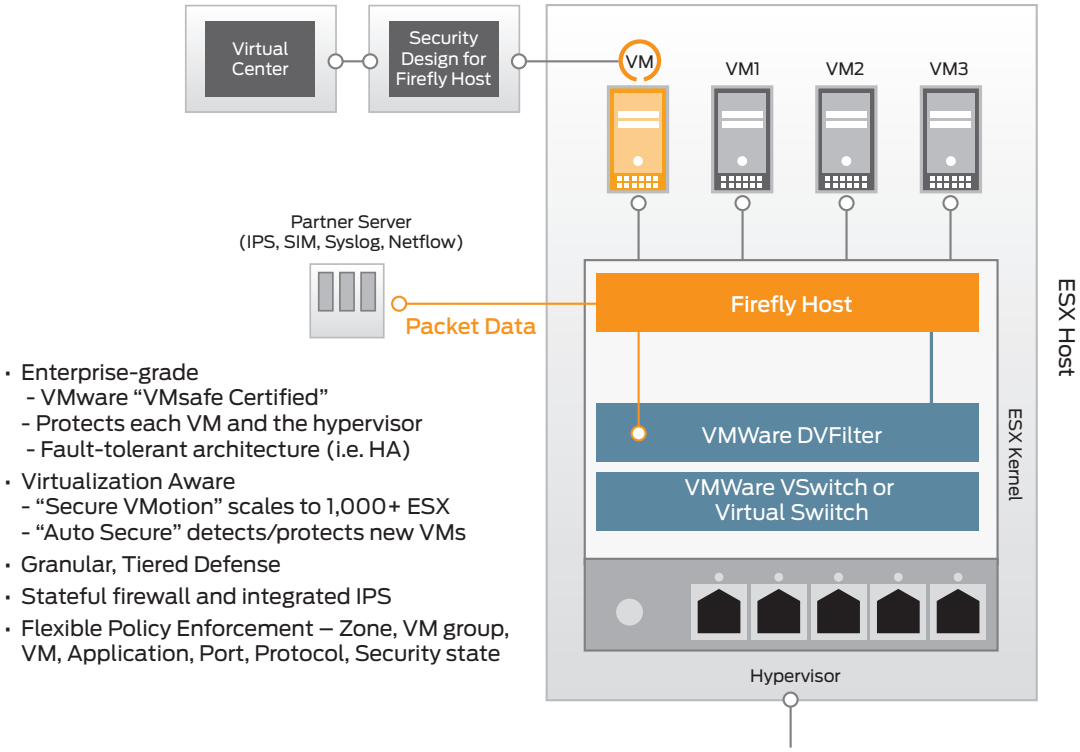

Figure 3: Firefly Host

*Formerly vGW Virtual Gateway

The web-based interface is the window to all Firefly Host functionality, with virtualization security policy editors that follow well established conventions for a highly intuitive user experience. Furthermore, Firefly Host provides features that automate security and compliance enforcement within virtual networks and clouds, while tightly integrating with existing Juniper security technologies that include intrusion prevent system (IPS), Juniper Networks STRM Series Security Threat Response Managers for logging and reporting, and Firefly Host security design for policy management

The SRX Series and Firefly Host—Integrated Zone Enforcement

Juniper understands that the keys to effective security are pervasiveness and consistency. To that end, the security that is applied in a collaborative way on physical and virtualized workloads are designed to ensure that security policies applied to workloads are consistent with their logical use, regardless of the platform on which they are deployed (Figure 4). To do this, Juniper has integrated the SRX Series zone concept with the Firefly Host VM enforcement engine such that the zone information is synchronized to and used by Firefly Host within the virtualized environment.

Here is a synopsis of how this works. The SRX Series delivers zone-based segregation at the data center perimeter, while Firefly Host integrates knowledge of SRX Series zones to ensure that zone integrity is enforced on the hypervisor using automated security features like Smart Groups and VM Introspection. The Smart Groups feature allows for the creation of a group of VMs that changes based on administratively defined criteria. VMs that suddenly have a configuration change that meets predefined criteria can be added to or removed from groups within seconds. For example, if a VM administrator associates the virtual network interface of a VM to the corporate production network, you can immediately apply a set of firewall rules to protect that system. Moreover, VM Introspection provides rich detail about the applications and services that are installed on a VM, as well as its configuration. It is possible, then, to construct security policies on the basis of VM Introspection parameters. An example of such a policy might be to not allow a new virtual machine to join a VM group or cluster unless it has a specific OS configuration and hot fix installed.

Thanks to this integrated approach, security administrators can confidently guarantee consistent security enforcement from the data center perimeter to the server VM. The role of zone synchronization between the SRX Series and Firefly Host provides an automated way to link the Firefly Host virtual security layer with the SRX Series physical device and network security. The SRX Series zone feature simplifies VM-to-zone mapping by importing zones configured on SRX Series Services Gateways into the virtual environment.

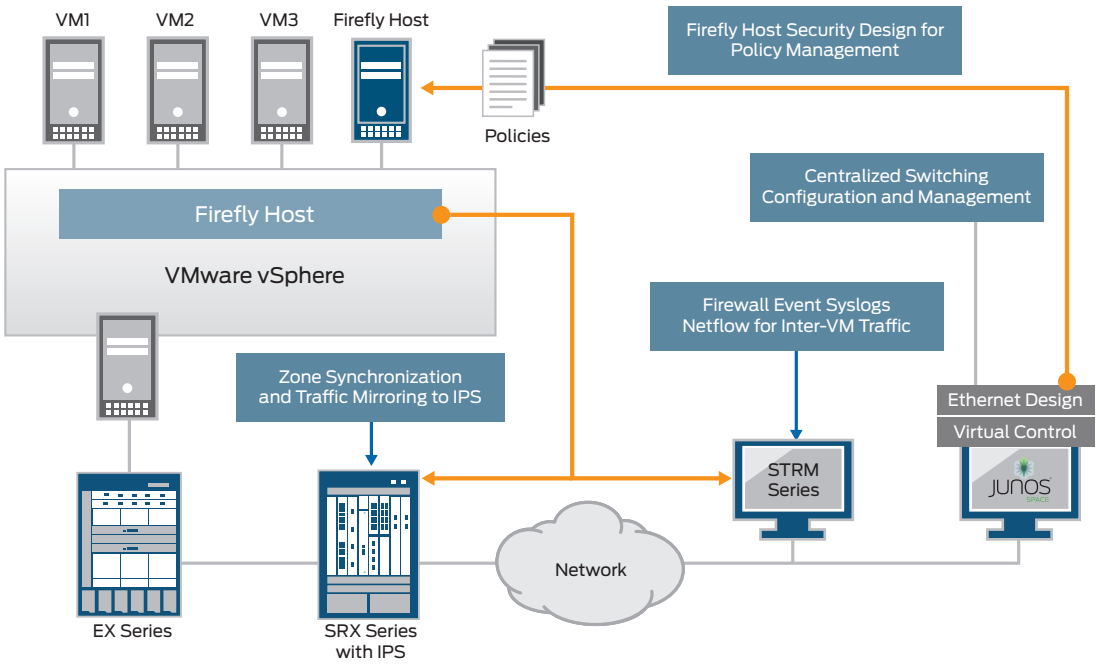

Figure 4: Integrated zone enforcement

Why SRX Series Zone Synchronization in the Virtualized Network?

The SRX Series zone synchronization feature provides an automated way to link the Firefly Host virtual security layer with SRX Series physical security. This means that traffic isolation policies flow through to the virtualization layer and are enforced there as well as for end-to-end security (e.g., from data center perimeter to the VM). By importing the zones defined within the SRX Series devices, VM-to-zone mapping is simplified. The zone assignments can be used to apply inter-VM zone policies as well as to integrate zones into compliance checking to ensure that VMs are only attached to authorized zones.

Zone synchronization between the SRX Series and Firefly Host is as easy as 1-2-3.

1. Firefly Host pulls zone definitions from the SRX Series device, mapping zones to the SRX Series interface and associated VLANs or network ranges for each zone. In the "Settings" module (Figure 5), select SRX Series zones in the Security Settings section. Select Add to create a new SRX Series instance. The configuration parameters are **Name, Host, and Port**.

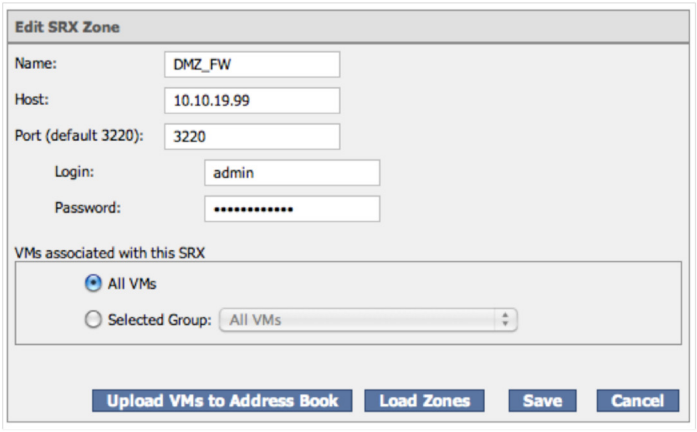

Figure 5: SRX Series configuration

Name: Name to represent this SRX Series gateway. Note that this name will be used within the VM zone labels, so a short descriptive name is best.

Host: Enter the SRX Series management IP address, where Firefly Host Security Design (i.e., Firefly Host management server) will connect to the SRX Series gateway.

Port: The TCP port used to connect the SRX Series via the Junoscript interface.

2. Firefly Host defines zones as a Policy Group based on the VLANs and networks associated with each zone. Once an SRX Series object has been saved, select Load Zones to initiate zone synchronization. You will be shown the list of all retrieved zones to select what you would like to import into Firefly Host as VM zone groupings. Within the Load Zones dialog, the zone synchronization can be configured to automatically poll the SRX Series for zone updates. The configuration parameters for scheduled updates are:

Update Frequency: How often to query the SRX Series for updates.

Relevant Interfaces: If only a subset of the SRX Series interfaces are protecting the virtual network, those interfaces should be selected here, so that only zones related to the virtual network are updated.

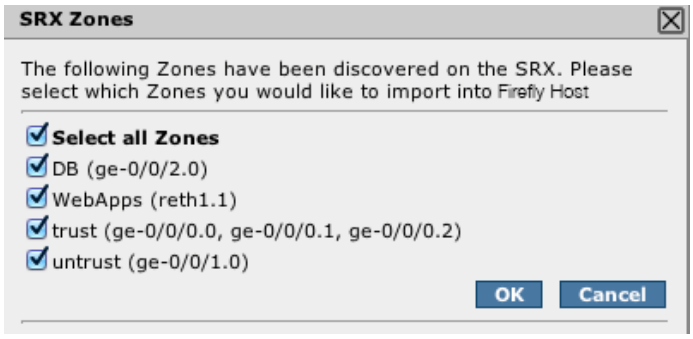

Figure 6: Zone selection

3. Firefly Host Policy Groups dynamically associate each VM to its zone, which can be used for inter-VM policy enforcement and zone compliance validations. The SRX Series zones are created in Firefly Host as VM Policy Groups. Using zone information from SRX Series devices, a Policy Group is created based on the following parameters:

   VLANs: VLANs associated with the SRX Series interface.

   IP Ranges: Subnet defined on the SRX Series interface, as well as routes defined within a zone.

   VM Scope: If the zone sync configuration includes a "VMs associated" selection, the chosen group will be included in the Policy Group.

   The Firefly Host zones synchronization feature also allows VM records to be populated within the address book for the zone to which the VM belongs. This allows the VM-to-zone mapping validation to also be performed from the context of SRX Series management.

   When a VM record is added to the SRX Series, it is created with the name of the VM as defined in vCenter. To make it clear that these are auto-generated VM records, a string is prepended to the name of the VM in its address book entry. By default, this string is "VM-", but this can be modified within the synchronization dialog.

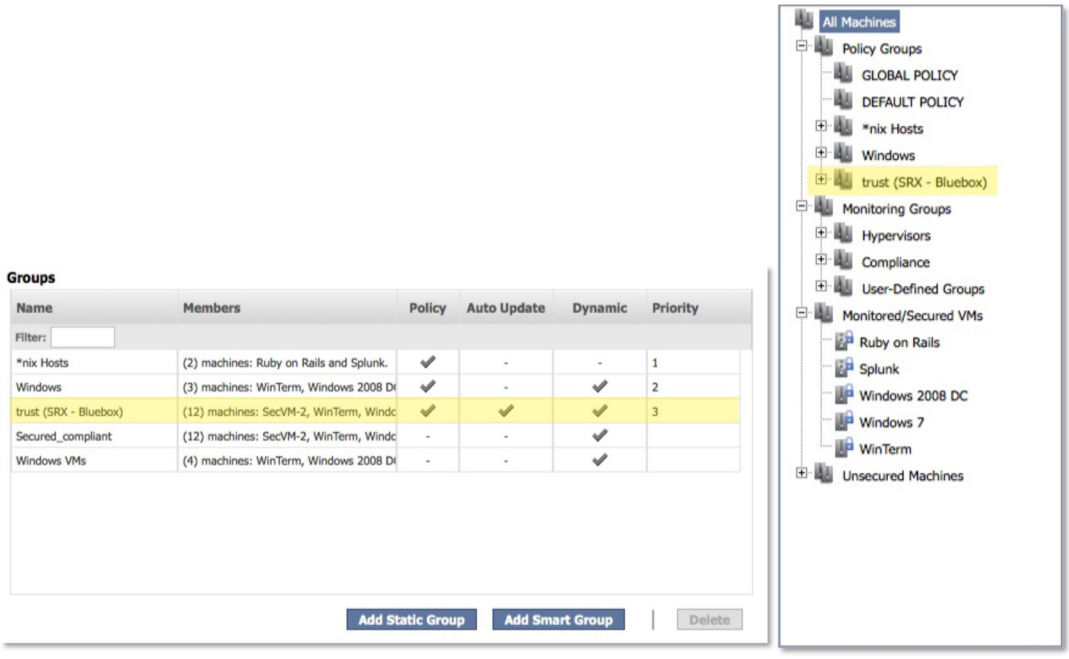

Figure 7: Policy groups

Benefits of zone synchronization between the SRX Series and Firefly Host provide guaranteed zone integrity on the hypervisor (i.e., virtualization operating system), automation and verification that a VM policy violation has not occurred, and visibility for the SRX Series gateways.

Use Cases: Multi-Tenancy and Regulatory Compliance

SRX Series/Firefly Host Integration for Multi-Tenancy Management and Isolation Enforcement

Multi-tenancy, or many tenants sharing resources, is fundamental to cloud computing. Cloud service providers are able to build network infrastructures and data centers that are computationally very efficient, highly scalable, and easily incremented to serve the many customers that share them. Key to ensuring that cloud service providers can meet their security service-level agreements (SLAs) for their customers is the proper isolation of customer resources and virtualized workloads (e.g., Coca-Cola VMs are kept separate from Pepsi VMs). Tenants or customers of public cloud and VM hosting services need written proof that communication and access to their hosted VMs is limited to the appropriate entities and not accessible by other customers of the same public cloud.

Juniper's security suite of SRX Series and Firefly Host accomplishes this by isolating customer traffic flows to the right physical network segments or zones, and by wrapping customer VMs within those zones in a customer-specific security policy that limits access to only that which is business appropriate for that tenant. In the public cloud diagram depicted in Figure 8, customer A traffic flows through the data center edge router to the SRX Series device where customer A zone policy is enforced, limiting traffic for customer A to VLAN 110. The Firefly Host, for its part, will identify the green VMs belonging to zone/customer A and ensure that those VMs are never assigned in error to VLAN 210. Also, any customer A to customer B communication will be blocked by both SRX Series and Firefly Host zone policies.

The benefit to the service provider is maximum use of virtualization infrastructure (note that both hosts have the maximum number of VMs resident), while customer resource isolation is enforced at the logical layer (e.g., customer A VMs will be isolated from customer B, even if they reside on the same host.).

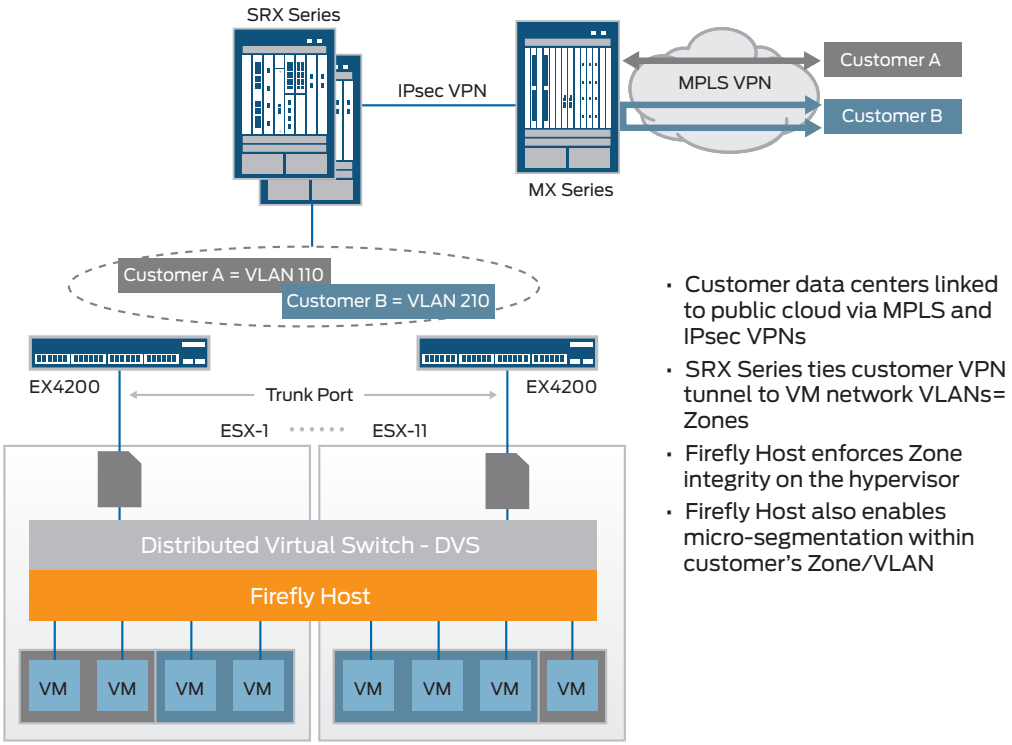

Figure 8: Multi-tenancy management and isolation enforcement

SRX Series/Firefly Host Integration for Policy Compliance Enforcement

Private clouds are defined as those cloud computing environments that are entirely owned by, controlled by, and provide service to a single organization. The business or government agency cloud may serve many departments or sub-organizational segments and, in that way, is similar to the public cloud service provider. This means that VM and VM group isolation by department or function is key both for security policy compliance, as well as to ensure that risky data behaviors from one department don't put the VMs of another department at risk as well. Imagine, as examples, the university that has an engineering department doing computer virus research sharing a cloud with the medical school that has VMs with patient data; or the business with customer relationship management (CRM) VMs sharing a host with Web servers.

These mixed-mode deployments are typical because businesses want to compress as many VMs onto a host for cost savings. Security best practice, however, requires that the VMs be isolated from one another such that connectivity from an infected Web server to a customer database is not possible. Consider the diagram below (Figure 9) to understand how this is enforced. Zone policies on the SRX Series will ensure that physical servers in zone preproduction will not be able to connect to Web servers and vice versa. All bidirectional traffic flows between those zones will be "denied" by the SRX Series gateway. In the case where the physical servers in those zones actually contain VMs, Firefly Host will step in and enforce the same policy. So VMs belonging to zone preproduction will not communicate with Web VMs. Should an administrator accidentally assign a new preproduction VM to the wrong zone (VLAN)—an action which is all too likely and common given the scale of these networks—Firefly Host will quarantine that VM and alert the administrator of the policy violation.

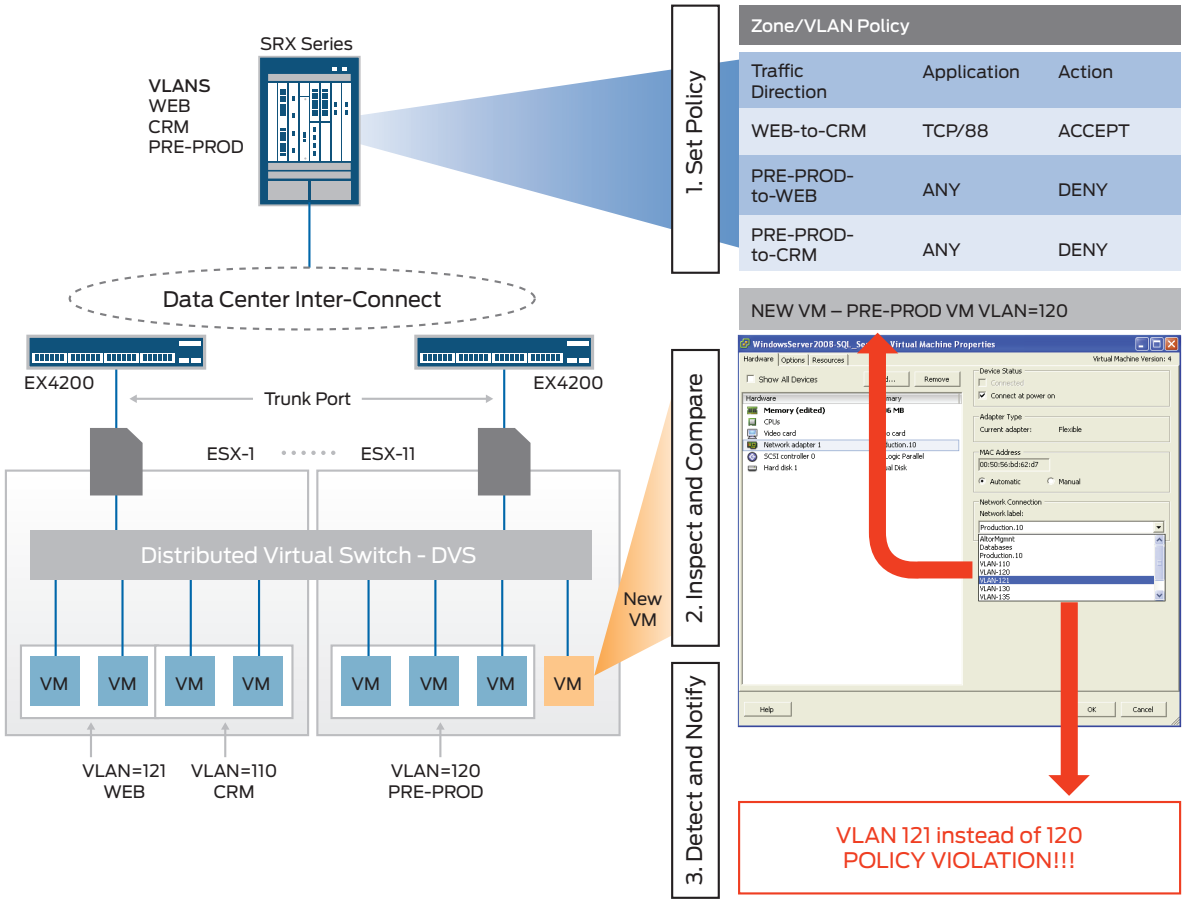

Figure 9: Policy compliance enforcement

Conclusion

Cloud computing and virtualization are two major catalysts in the evolving data center design. Though both present compelling cost saving opportunities for customers, there are still significant security concerns that stand to diminish their overall value proposition. Organizations that act early to implement an integrated best-of-breed security—such as Juniper offers with SRX Series and Firefly Host will be best positioned to scale their cloud both in terms of secure cloud infrastructure and in-house cloud security expertise. Since cloud computing and virtualization adoption are usually implemented in phases, the typical data center will, for the foreseeable future, be a mix of physical and virtualized workloads. Therefore, a security framework that is independent of the underlying workload platform is key to ensuring protections for all workloads throughout the migration to and implementation of virtualization and cloud computing. With the right security solution, organizations will be able to derive the most value from their virtualization and cloud computing infrastructure without sacrificing security breadth and effectiveness.

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 +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

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

2000431-002-EN Nov 2013 Printed on recycled paper