Juniper Networks Cloud Security

Table of Contents

Executive Summary ... 3
Introduction—Cloud Computing Overview ... 3
- Private Cloud ... 4
- Public Cloud ... 4
- Hybrid Cloud ... 4

Evolution in Data Center Technologies Affecting Security for the Cloud ... 4
- Evolving Business Application Architectures ... 4
- Server Virtualization ... 4
- Reducing Operational Expenses ... 4
- Protecting Against Evolving Security Threats ... 5

The Business Imperative of the Public Cloud ... 5
- Performance ... 5
- Elasticity ... 5
- Fault Tolerance ... 6

Assessing the Cloud Security Requirements of Service Providers ... 6
- Visibility ... 6
- Compliance Enforcement ... 6
- Protection ... 6
- Multi-Tenancy Management and Isolation Enforcement ... 6
- Service-Level Agreements ... 7
- Juniper Networks' Cloud Security Architecture ... 7
- The Components of Juniper Networks' Cloud Security Architecture ... 7
  - SRX Series Services Gateways for Comprehensive Physical Security ... 7
  - Firefly Host to Protect Virtualized Environments ... 8
  - Secure Analytics for Centralized Logging and Monitoring ... 8
- The Juniper Networks Vision for Cloud Security ... 9

Juniper Cloud Security at Work ... 9
- Private Cloud Use Case ... 9
- Public Cloud Use Case ... 10

Conclusion ... 10
About Juniper Networks ... 10

List of Figures

Figure 1: Virtualization, cloud computing's de facto operating system, requires new security architecture. ... 3
Figure 2: Cloud computing market forecast (Source: Gartner). ... 5
Figure 3: Cloud computing requires integrated security. ... 7
Figure 4: Integrated physical and virtual security for comprehensive cloud protection. ... 8
Figure 5: Multi-tenancy management and isolation enforcement. ... 9

©2015, Juniper Networks, Inc.

Executive Summary

Cloud computing is creating a new world of benefits for users and providers alike, but is also creating new concerns around security and risk management that must be dealt with for cloud computing to reach its ultimate potential. In fact, when it comes to cloud computing, security has been a major inhibitor for businesses. This is why security needs to be consideration number one for any service provider planning to offer hosted cloud computing services.

To provide security in the cloud, it is necessary to address the most significant underlying technology of the cloud: virtualization of workloads and servers. Service providers want to employ the largest pool of shared resources possible for their offerings because the more they can host on their virtualized infrastructure, the more business they can take on. But key to maximizing the effectiveness of this virtualized capacity is security purpose-built for the environment. For applications leveraging a virtual server/virtual machine environment, adding hypervisor-based security to the architecture is the only way service providers can truly optimize for scale, while enabling the granular segmentation required to guarantee isolation of multi-tenant resources as well as consistently high performance.

While traditional security architectures (such as network-based firewalls and intrusion prevention system devices) are essential to the security of the physical network of the cloud, they provide no visibility into the traffic generated in the virtualized part of the network (i.e., traffic flowing between virtual machines housed on a host server). Understanding this, Juniper Networks has developed a security architecture that offers integrated solutions to protect both physical and virtualized workloads, provides visibility and protection for the entirety of the cloud computing environment, and makes secure multi-tenancy possible in the cloud computing world.

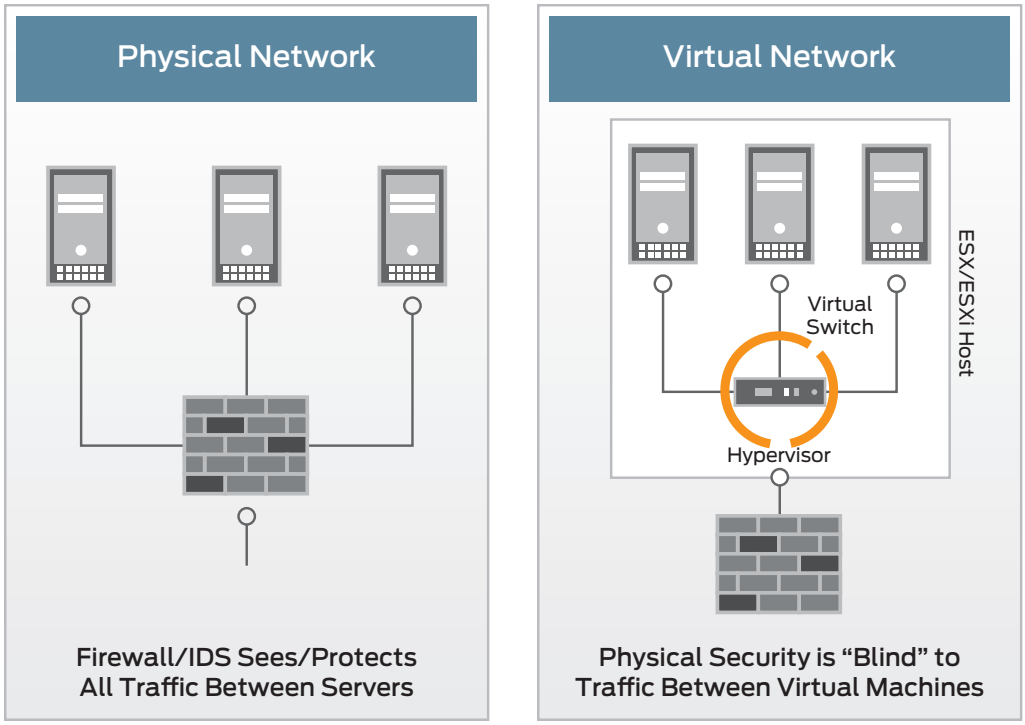

Figure 1: Virtualization, cloud computing's de facto operating system, requires new security architecture.

Introduction—Cloud Computing Overview

Cloud computing entails the pooling of resources like computing and storage together and making them available on demand as logical rather than physical groups (e.g., rather than identifying specific physical test-dev servers, think of defining test-dev workloads, where a workload would be run in a virtual machine residing in any one of a pool of host virtualization servers available to the service).

Though a cloud computing environment can be run as a private, public, or hybrid type of service, the ultimate goal of any cloud is to enable simple, yet dynamically and broadly scalable access to computing resources and IT services—with security and high performance as inherent parts of the "network."

©2015, Juniper Networks, Inc.

Private Cloud

A private cloud (internal) is a virtualized network or virtualized data center that exists within the boundaries of an organization and is typically managed by that organization and available for that organization's exclusive use. It supplies hosted services to a limited number of people or organizational and departmental groups, and offers many of the benefits of a public cloud computing environment such as being elastic and service based. In a private cloud-based service, however, data and processes are managed within the organization and, by extension, give implementing organizations and businesses greater control over that data than they may get by using a third-party hosted service.

Public Cloud

A public cloud (external) is one whose resources are available for use by the general public, whether individuals, corporations, or other types of organizations. One implementation of the public cloud is by service providers who offer compute, storage, and securely hosted resources to individual clients and businesses of all sizes via the Internet.

Generally, these services are divided into three categories: infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS). And each service has three distinct characteristics: (1) it is created on demand and priced by use (by time, amount of resource used, or a combination of those); (2) it is elastic (consumers can have as much or as little of a service as they want at any given time); and (3) the service is fully managed by the provider.

Hybrid Cloud

A hybrid cloud combines aspects of both private (internal) and public (external) cloud computing environments. In this model, users typically outsource non-business-critical information and processing to the public cloud, while keeping business-critical services and data within their control. With a hybrid cloud, some processes remain on-premise and some move to the cloud, an architectural choice requiring new and extended security processes that require multiple hybrid cloud administrators to collaborate in order to achieve comprehensive data protection.

Evolution in Data Center Technologies Affecting Security for the Cloud

Key market and technology trends inherently affect public and private cloud security requirements. Some of these are evolving business application architectures, virtualization of server resources, reducing operational expenses, and protecting against new and evolving security threats.

Evolving Business Application Architectures

Business applications enable transactions for internal employees, collaboration with outside partners and customers, and capabilities that improve the business' competitive advantage. In today's globally competitive world, applications must be available from everywhere and at all times.

Concurrently, a rich mix of application architectures must be supported in their own right. In many cases, these are blended into tiered designs with a range of resulting information flows. Some are strictly constrained to a narrow, necessary content mix, while others are more fluid and involve a varying mix of content and transaction types depending on business need. A key requirement of securing data center architectures is to protect the communications that are the lifeblood of enterprises and organizations *without impacting application performance and availability*.

Server Virtualization

Aligned with the trend toward more powerful servers, more open application designs, and the need to accomplish "more with less" is the adoption of virtualization within the data center, especially for servers. Server virtualization offers significant operational cost savings, but also introduces risks, because multiple logical hosts now run on a single physical server or "host." From a security standpoint, it becomes necessary to differentiate virtual server or virtual machine (VM) identities within the network and enable them to operate within their own logical domains. At the same time, the need to secure VMs in a manner consistent with the physical servers they replace is key. Security policies for controlling VM access must be applied as they are to physical workloads, while also allowing for VMs to be created, deleted, or moved without requiring complex security reconfiguration.

Reducing Operational Expenses

Changes in the global economy and the desire to achieve greater business value associated with IT investment are creating more pressure to control costs. Highly resilient and available data centers are expensive to implement, run, and manage on a day-to-day basis. In an effort to reduce these costs, organizations are turning to a public cloud model where service providers offer "pay per use" models.

©2015, Juniper Networks, Inc.

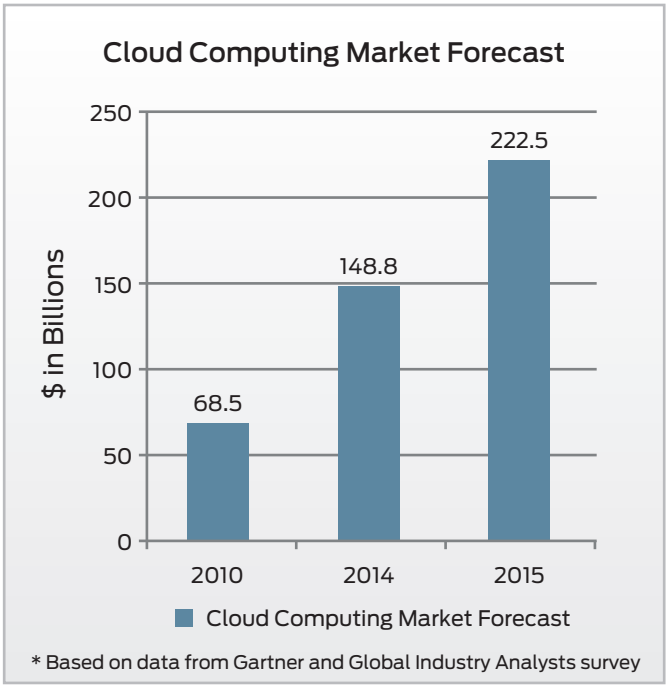

Figure 2: Cloud computing market forecast (Source: Gartner).

Protecting Against Evolving Security Threats

The emergence of new data center technologies and applications is giving cyber attackers a new footprint to exploit. Malware that is deeply embedded within applications or that leverages their pervasive use (e.g., social media, Web 2.0) is proliferating. Therefore, advanced security measures with high application awareness and appropriate mitigation are must-haves to protect the new network.

The Business Imperative of the Public Cloud

Cloud computing exemplifies a significant shift in application and data center architectures by enabling theoretically limitless scale, while reducing capital expenditures for hardware sourcing and maintenance. In fact, IDC predicts that cloud computing will reduce the cost of owning IT infrastructure by 54 percent as businesses either roll out their own private clouds, turn to cloud services, or, most likely, commit to some combination of the two. But the ultimate benefit to businesses and organizations is achieving new levels of agility, competitiveness, and efficiency for the long term. This is why removing the key barrier to cloud adoption—security—is an absolute imperative. Performance, elasticity, and fault tolerance are key to the blueprint of a highly efficient and scalable cloud—and security should enable and enhance each of these.

Performance

To an organization's customers, partners, and employees, business applications are the means to an end. They let users access information, make transactions, and, ultimately, perform their jobs. This means that applications must perform well, as they are essential to employee productivity, customer satisfaction, and an enterprise's bottom line. When it comes to securing them, the key is to avoid the "security tax" or, stated differently, not introduce latency into performance. To that end, it is necessary to tune security solutions to applications.

Elasticity

Elasticity is the ability to scale resources up and down as needed. In typical computer and network environments, planning for growth and change is a costly and time-consuming effort. A successful organization must be able to readily and cost-effectively scale business applications. Private and public clouds are being built on server virtualization precisely because this elasticity is delivered at a very low cost. With clouds, new workloads can be provisioned with a mouse click rather than taking days to weeks, while adding more compute or storage is almost as quick. Inherent in virtualization technology are features that maximize this elasticity so the implementation of security should not require that they be disabled.

©2015, Juniper Networks, Inc.

Fault Tolerance

Fault tolerance is a must in data centers and clouds and the same holds true for the technology that secures them. The application of access controls and advanced security features is an "always on" operation. Security technology must provide fault tolerance at the enforcement and management layers such that a failure at either point does not cause disruption to mission critical traffic.

Assessing the Cloud Security Requirements of Service Providers

To create services that deliver increased agility, flexibility, and cost efficiency for their customers, service providers need to guarantee effective security—currently the biggest inhibitor to the adoption of the public cloud. Generally, large cloud providers are making a much bigger investment (medium and long term) in virtualization and cloud computing than the average IT department and, therefore, have more to lose should something go wrong. This makes choosing the right security solution all the more important, as it will enable delivery of the best possible cloud computing service.

Elements of a successful solution for securing the public cloud should include capabilities for visibility, compliance, protection against threats, isolation of multiple tenants' assets, and management of service-level agreements (SLAs).

Visibility

Visibility into operation and results of service is essential to effective cloud computing offerings. An organization should have total visibility of users, resources, applications, operating systems, and services. Service providers must have and provide to their customers a complete view of all network traffic—in both the physical and virtualized realms. This includes assigning trust based on identity and authorization levels, and facilitating monitoring to look for malicious activities.

Compliance Enforcement

Most organizations and businesses today must comply with a variety of regulations and standards. In a cloud environment, compliance functionality should include continuous monitoring and enforcement of segregation of duties, business warranted access, and ideal/desired server and/or VM configuration based on custom whitelists (desired configurations) and blacklists (unwanted conditions). Cloud administrators must be able to see their aggregate compliance posture at a glance. Should a noncompliance alert be triggered, they should be able to drill down within servers/VMs to identify the exact condition that caused the alert.

Protection

Protection in the cloud requires layered defenses. Cloud providers must apply security policies and controls for both the physical and the virtualized portions of their environment to block unwanted users and flows and lessen the probability of attacks. They must be able to monitor and inspect packets for the presence of malware or malicious traffic and send alerts to cloud service managers, as well as subscribing customers, as appropriate, through the use of intrusion detection and prevention systems (IPS). Finally, they should have virtualization-specific antivirus protections in place that can deliver highly efficient on-demand and on-access scanning of VM disks and files with the capability to quarantine infected entities.

Multi-Tenancy Management and Isolation Enforcement

Multi-tenancy is the property of service providers' environments in which multiple systems, applications, and data from different logical entities (e.g., organizations, departments, users) are hosted on the same physical hardware. In the multi-tenant cloud, a service provider's computing resources are pooled to serve multiple customers using dynamically assigned resources based on demand. Generally, the customer has no control over or knowledge of the exact location of the provided resources. Because of this, it is important for providers to enforce isolation of customer-specific traffic, data, and resources, so one tenant cannot pose risks to others in terms of data loss, misuse, or privacy violation. By isolating areas of the virtualized network into security zones, service providers can control access between these areas, limit the scope of exploits, and consistently facilitate policy enforcement throughout the cloud—all while maximizing the capacity of their systems to hold the resources of tenants.

©2015, Juniper Networks, Inc.

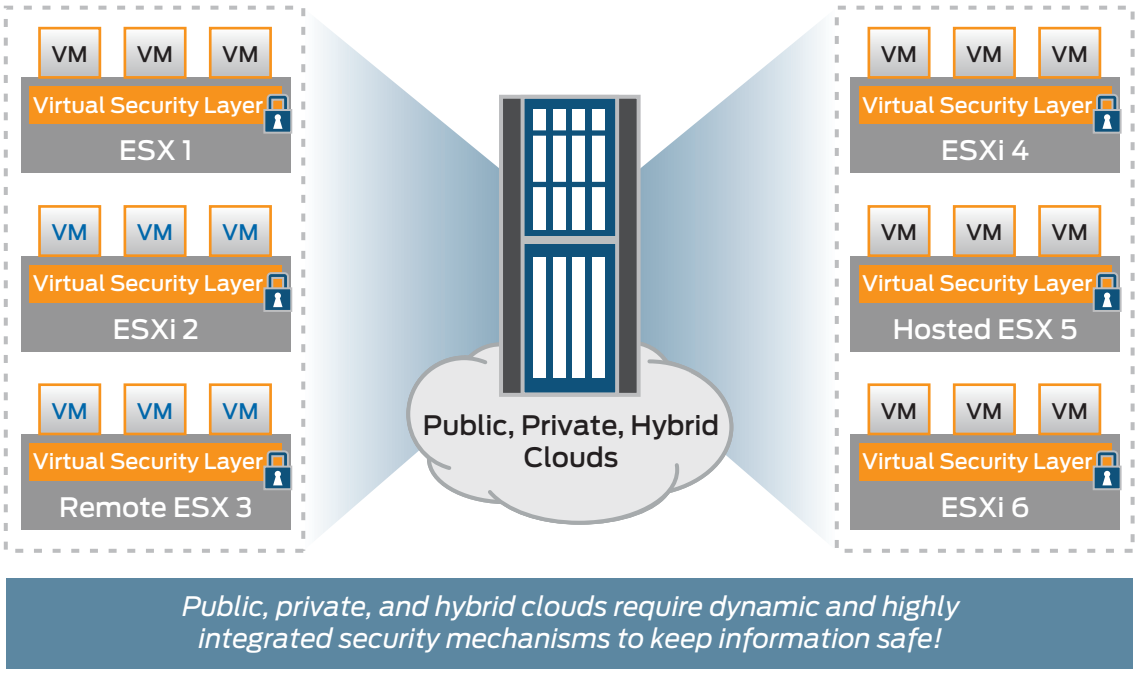

Figure 3: Cloud computing requires integrated security.

Service-Level Agreements

The advantages of the public cloud include reduced cost of ownership, no capital investment, scalability, self-service, location independence, and rapid deployment. But to get organizations to move to this model, service providers need to create trust—and this comes with transparency. The cloud should be viewed as an extension of an internal IT infrastructure, and organizations need not lose all control over risk mitigation. Service providers can instill that confidence with customers by putting proper SLAs into effect. Customers must be able to see that cloud service providers are complying with mutually agreed upon security standards and practices. Therefore, an SLA must clearly articulate expectations regarding the handling, use, storage, and availability of data, as well as requirements for business continuity and disaster recovery. If an SLA includes intrusion detection, for example, there should be details about the frequency of alerts and level of monitoring. Having a security infrastructure that can provide the controls and create the reports necessary to support SLAs is key.

In the cloud, both physical and virtualized infrastructures must be secured. In order to maintain the visibility and protection that is required, service providers should seek out security solutions that work in concert to provide consistent application of security policy throughout the physical network and within the virtualized network. Only with this type of integration can they guarantee to their customers that security is truly pervasive and enforceable from the perimeter to the VM.

Juniper Networks' Cloud Security Architecture

Juniper Networks not only understands the requirements of the new data center and cloud, but it also understands and delivers on the security requirements of both. By leveraging a combination of products, technologies, services, and design expertise, Juniper enables the most efficient, scalable, cost-effective, and secure cloud computing environment possible.

The Components of Juniper Networks' Cloud Security Architecture

Juniper's broad portfolio of security products enables the pervasive, integrated, end-to-end cloud security that enterprises and service providers alike require. Juniper emphasizes strong isolation, integrity, and resiliency in order to provide visibility, control, and automation across the entire cloud computing infrastructure.

SRX Series Services Gateways for Comprehensive Physical Security

Juniper Networks® SRX Series Services Gateways offer high-performance security, routing, and network solutions for enterprises and service providers. These gateways combine routing, switching, application services, and user- and application-aware security within a modular, expandable chassis to deliver unprecedented performance and flexibility, while reducing management overhead.

SRX Series Services Gateways serve as the cornerstone of consolidated security within the data center, providing effective network segmentation, securing flows, delivering IPsec VPN encryption services, and offering IPS protection, Network Address Translation (NAT), and application-specific malware detection and protections. By consolidating

switching, routing, and security in a single device, managers can economically deliver new applications, secure connectivity, and deliver quality end user experiences. With its highly modular architecture, the SRX Series supports new services without sacrificing performance. It offers flexible deployment options that allow service providers to host and secure customer servers and workloads or secure them at the customer premise. Regardless of their placement on the network, these solutions provide fast and highly scalable segmentation of customer resources.

Firefly Host to Protect Virtualized Environments

Juniper Networks Firefly Host[1] is a comprehensive, hypervisor-based, virtualization security solution for the cloud that provides full visibility and granular access control over all traffic flowing through VMs. Firefly Host enforces a granular virtualized security policy consistent and integrated with physical server security, including SRX Series Services Gateways and Juniper Networks Secure Analytics[2]. With Juniper's solution, security policies are extended from the data center perimeter to the hypervisor and down to the individual VM such that the application of access control is both continuous and comprehensive across physical and virtualized workloads.

Specifically, in the case of SRX Series integration, Firefly Host is able to retrieve security policy and interface information from the SRX Series, and then replicate the access policies that are in effect within the physical network so that they are also applied within the virtualized environment. For instance, an SRX Series policy that prevents human resources (HR) servers from connecting to the Internet will also be enforced within the cloud computing realms so that HR VMs cannot connect to the Internet either. Firefly Host innovation also adds layered defenses that are highly virtualization aware, enabling real-time detection of VM changes and movement, and the automatic invocation of security policies when those changes impact VM security and compliance posture in a negative way.

By shrink wrapping each customer VM or group of VMs in a distinct security policy, Firefly Host is able to provide strict isolation of cloud tenant resources, ensuring that access to VMs is strictly "business warranted." Further, detailed logging and reporting of all access events and traffic enables service providers to furnish customers with proof that supports their SLAs. Integration with Secure Analytics further augments this reporting with access events occurring on the physical network segments where customer servers reside or are hosted. Delivering this level of documentation in support of SLAs distinguishes service provider cloud offerings with security and operational transparency.

Secure Analytics for Centralized Logging and Monitoring

Secure Analytics combines network performance and security management into a single solution for enterprise and service provider customers, in addition to integrated log, threat, and compliance management for both Juniper and non-Juniper products. Secure Analytics delivers a complete network visibility and access picture, making troubleshooting and cloud security optimization easier and faster. Service providers can extend Secure Analytics reports to their customers as part of a reporting service or SLA, in order to provide further peace of mind and as appropriate proof of regulatory compliance for operation of the cloud computing environment.

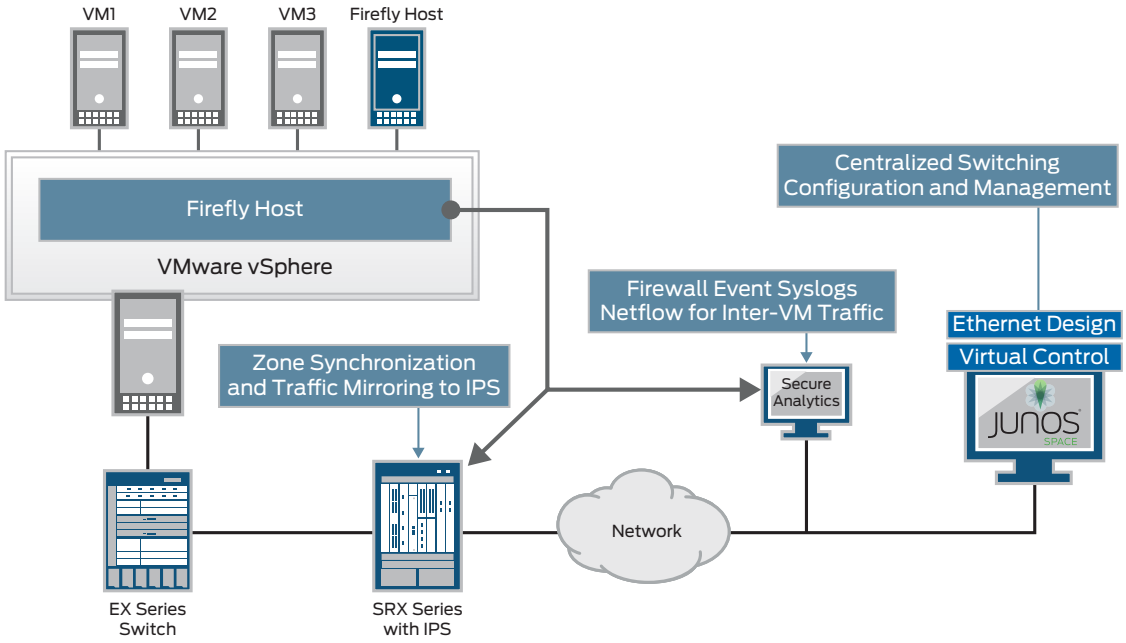

Figure 4: Integrated physical and virtual security for comprehensive cloud protection.

[1] Formerly vGW Virtual Gateway

[2] Formerly STRM Series Security Threat Response Managers

The Juniper Networks Vision for Cloud Security

Juniper Networks' vision for cloud security is driven by achieving complete integration and pervasive protection of resources and information. Our end goal is to enable organizations to implement cloud computing at a pace and with an approach compatible with their business objectives. We understand that enterprises and service providers must secure traffic flows between physical elements, as well as virtual ones. For this reason, we have developed a comprehensive solution that spans both.

Juniper delivers a rich set of protections that not only meets today's cloud security and performance requirements, but scales to address future on-demand growth. Services such as application-aware denial of service (DoS), stateful firewall, antivirus, and intrusion detection and prevention systems are consolidated and can be enforced on the physical network or within the virtualized environment, providing the flexibility required to dynamically assign resources to services.

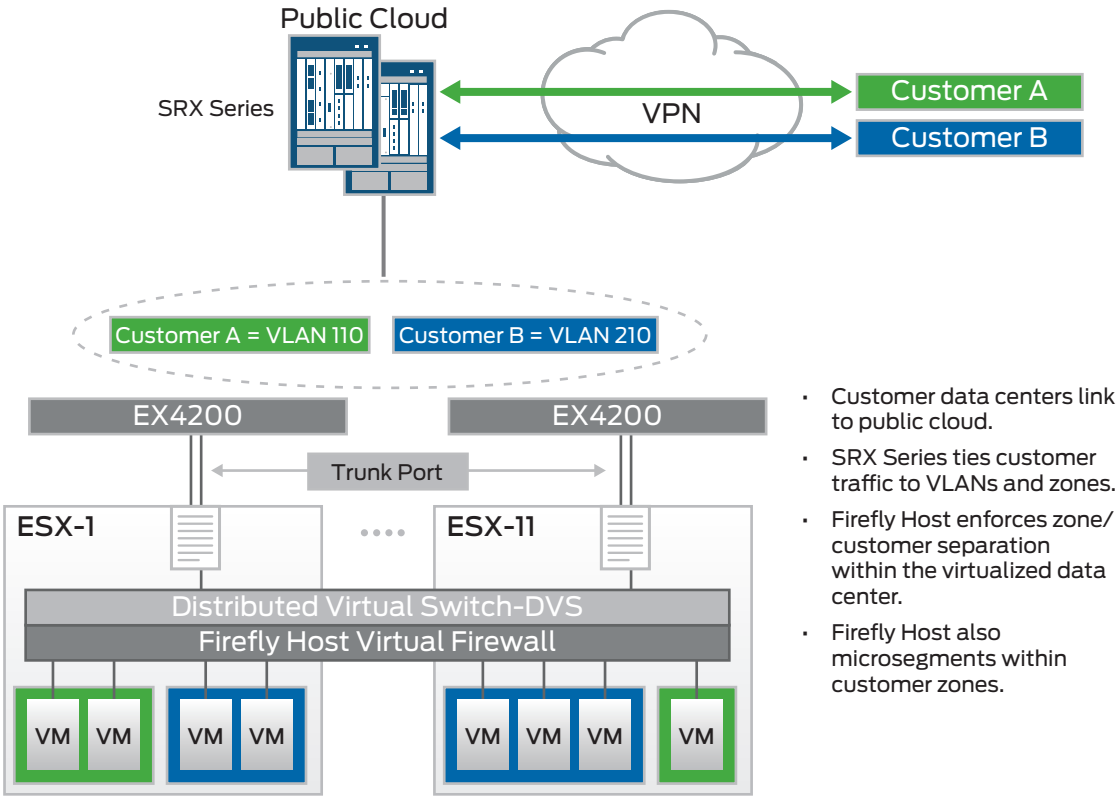

Figure 5: Multi-tenancy management and isolation enforcement.

Juniper Cloud Security at Work

Juniper solutions secure all types of clouds (i.e., private, public, and hybrid). Outlined below are two real-world deployments.

Private Cloud Use Case

Recently, data center architects at a healthcare agency decided to virtualize their entire data center and build a private cloud in an effort to improve application availability, IT agility, and operational efficiency, as well as contain costs. Knowing they wanted to re-engineer the security environment and processes by simplifying firewall design, layers, and policies in combination with improved management and reporting, the agency turned to Juniper Networks.

With Juniper Networks Firefly Host, agency security stakeholders were able to eliminate the DMZ so that network segregation into physically segmented trust zones would no longer be required. By using security policy rules within Firefly Host instead of VLANs to segregate traffic within the private cloud, the agency implemented a vastly simpler way to manage the network that is not only more secure, but easier to configure and exponentially easier to monitor and troubleshoot. Additionally, the introduction of Secure Analytics into the environment provides this health agency with a comprehensive suite of tools for monitoring all security, networking, and server infrastructure. This holistic approach empowers the agency's network and security operations teams to efficiently manage the business operations of their networks from a single console. As a result, the amount of resources required to produce timely, meaningful, and accurate information has significantly decreased.

©2015, Juniper Networks, Inc.

Public Cloud Use Case

An IaaS provider also chose to implement the Firefly Host to meet must-have requirements for cloud security: ease of installation, ease of security policy configuration, logging and reporting comprehensiveness, and availability of layered defenses like integrated antivirus and intrusion detection. With Firefly Host in place, the cloud service provider delivers guaranteed VM isolation for customers and the reports to prove access control enforcement. Customers of this particular provider can choose from a menu of integrated security options, which are enabled by Firefly Host to provide additional security and facilitate VM maintenance and compliant operation. With the Firefly Host cloud software development kit (SDK), the provider can even automate the provisioning of security for new VMs. Customers simply select to purchase additional VMs at the service provider portal and Firefly Host takes care of the rest—in a manner that is completely transparent to the cloud tenants. What customers learn from the reports they receive is that their VMs are properly configured for compliance and will only be accessed in accordance with predefined policies.

Conclusion

As enterprises seek to meet today's business demands to reduce costs, offer more services, and support a growing amount of data, they will increasingly consider moving to the cloud. Whether public, private, or a hybrid, the cloud offers too many benefits to be ignored. What becomes extremely important, however, is choosing a cloud strategy that does not introduce more risks than benefits. This is why an end-to-end cloud security solution such as Juniper offers can be highly advantageous.

Juniper Networks not only understands the requirements of the new data center and cloud, but it also understands and delivers on the security requirements of both. By leveraging a combination of products, technologies, services, and design expertise, Juniper enables the most efficient, scalable, cost-effective, and ***secure*** cloud computing environment in the industry.

Juniper Networks has developed a security architecture that leverages the combined power of SRX Series Services Gateways, the Firefly Host, and Secure Analytics. This integrated solution protects both physical and virtualized workloads, provides visibility and protection for the entirety of the cloud computing environment, and makes secure multi-tenancy possible in the cloud computing world.

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

Copyright 2015 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos and QFabric are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

2000465-003-EN Sept 2015