COMPREHENSIVE SECURITY FOR TODAY'S DATA CENTER

Juniper's next-generation security solutions protect the physical and virtual network, Web applications, and access

Challenge

Firewalls, IPS, and even next-generation firewalls only address some of the risks to today's data centers. Amongst an Enterprise's critical assets, servers[1] , the source of its "crown jewels" aka. data, are targeted the most. Moreover, Enterprises are increasingly adopting virtualization. Unauthorized access is a significant risk.

Solution

Juniper uniquely addresses data center security for physical and virtual environments with next-generation services that include application visibility and control, DDoS and hacking prevention, and policy enforcement.

Benefits

- Superior security and performance for physical and virtual data center assets
- Innovative security and attacker intelligence sharing
- Granular policy enforcement for authenticated and authorized data center access

[1] Verizon Data Breach Investigation Report, 2013

Companies are struggling to keep pace with the increasing volume and sophistication of cyberattacks, particularly those aimed at gaining unauthorized access to high value Web applications and servers typically residing in data centers. According to a 2013 Ponemon Institute report commissioned by Juniper Networks, web-based (65 percent) and denial-of-service (DoS) attacks (60 percent) were cited as the most serious types of attacks experienced by companies. More telling, a majority (60 percent) of security professionals also indicated that current next-generation firewalls and IP reputation feeds only address part of the cybersecurity threat, leaving significant exposure to the most concerning attacks.

In addition, 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 is as integral a component as traditional firewalls are in today's networks.

To counter these threats, data centers need holistic critical asset protection, visibility, and policy enforcement for their physical and virtual environments.

The Challenge

The data center, composed of many parts, has a diverse set of security needs. Businesses need to secure the network, secure their high value Web applications, and secure access to corporate resources. For the network, cloud computing and virtualization offer 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 initially anticipated. 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 or maintain control.

With regards to Web applications, organizations still see a gap in security effectiveness, despite significant investment in security technology. The reason is simple. Traditional defenses rely on signatures and IP addresses. Signatures, used in products like antivirus and intrusion prevention systems (IPS), are effective at detecting known attacks at the time attacks are launched. They are not effective, however, at detecting new attacks or capable of detecting hackers who are still in the reconnaissance phase, probing for weaknesses to attack. IP reputation databases, meanwhile, rely on the notion that all bad actors can be identified by their IP addresses. However, blocking an IP address that represents the entirety of a company's employee base is disruptive to that business. To further complicate matters, consider how hackers can easily impersonate legitimate users, or simply change the IP address they are using by pointing to a different anonymous proxy.

Additionally, consider how new platforms, such as virtualization and cloud computing, do not even use IP addresses as identifying marks. In other words, bad actors have many easy ways to dissociate themselves from IP addresses. In addition, distributed denial of service (DDoS) attacks can bring down data center resources and disrupt businesses while both DDoS attacks and hacking threaten high value Web applications.

For securing access, data centers house the businesses' most important data. And thus, organizations require fine-grained control to ensure that only authorized and authenticated users gain access to these resources. In addition, most vendors have taken some proprietary freedoms in implementing their network access control solutions, making it much harder for businesses to quickly and simply deploy network access control (NAC) in a truly heterogeneous data center environment.

The Juniper Networks Security Solution Effectively Protects the Data Center

Juniper's next-generation security portfolio addresses the biggest security threats to data centers. For the network, the Juniper Networks® SRX Series Services Gateways with Firefly Host integration deliver the security necessary for today's data center with its mix of physical and virtualized workloads. Integrated with the SRX Series, the Firefly Host queries the SRX Series gateway for its zone, interface, network, and routing configuration. Firefly Host then uses that information with the Firefly Host management system to create VM Smart Groups so that users of Firefly Host can see VM to zone attachments, create additional inter-VM zone policies, and incorporate zone knowledge into compliance checks(for example, is a Client X VM connected to a Client Y zone?).

For applications, threats include disruption of availability and hacking/data breaches of Web applications. DDoS protection ensures that applications remain online and responsive to legitimate users. Intrusion deception accurately identifies hackers and enables flexible counterresponses both at the application layer and, through tight intelligence integration, at the network firewall. The Juniper security product line provides the most comprehensive data center protection regimen of its kind, complementing the protections of next-generation firewalls, reputation feeds, IPS, and Web application firewalls alone.

For access, Juniper Networks Unified Access Control (UAC)—comprised of the Junos® Pulse Access Control service running on MAG Series Junos Pulse Gateways—ensures that users are authorized to access the network and data center resources before being granted access, and that their devices adhere to a baseline of security policy throughout their network session. Organizations need the flexible UAC solution to protect their network and data center investments today and in the future. UAC supports phased deployments and can scale to cover an entire global enterprise. And Juniper Networks is the only vendor that can deliver comprehensive, standards-based, enterprise-wide NAC.

UAC is a uniquely extensible, open solution that delivers granular access control to the entire distributed enterprise, from remote users and branch offices to the data center, while reducing cost and complexity. UAC addresses myriad network challenges such as effective network segmentation or enclaves, insider threats, guest access, bring your own device (BYOD), and regulatory compliance to protect an organization's networks, mission-critical applications, and sensitive data.

These security solutions are available on dedicated hardware, hypervisors, and SDN-centric data centers. For an enterprise or service provider with physical, virtualized, or hybrid data centers and plans toward software-defined networking (SDN), there is no comparable alternative for data center protection breadth, detection accuracy, and SDN architecture support.

Solution Components

For unparalleled protection against data exfiltration, website outages, unauthorized access, and other serious data center threats, Juniper offers next-generation security products that include SRX Series Services Gateways, Firefly Host, WebApp Secure, Spotlight Secure attacker database, DDoS Secure, and Unified Access Control.

SRX Series Services Gateways are high-performance network security solutions that deliver security, routing, and networking capability. Specifically for security, the SRX Series offers next-generation firewall, application visibility and control, IPS, Unified Threat Management (UTM), as well as other security services. The SRX Series packs high port density, advanced security, and flexible connectivity into easily managed platforms. These versatile and cost-effective solutions support fast, secure, and highly available data center operations, with unmatched performance to deliver some of the industry's best price-performance ratios and lowest TCOs. The SRX Series is at the core of securing the network, and it is integrated with the other solutions to secure applications and secure access.

Firefly Host is a comprehensive virtualization security solution that includes a high-performance, hypervisor-based stateful firewall, integrated intrusion detection system (IDS), virtualization-specific antivirus protection, and unrivaled scalability for managing multitenant cloud security. Firefly Host brings forward powerful features that offer layers of defenses and automated security as well as compliance enforcement within virtual networks and clouds. The SRX Series and Firefly Host 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. Firefly Host 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.

WebApp Secure takes Web application protection to the next level, using the latest intrusion deception technology to definitively identify and mislead attackers while simultaneously profiling and fingerprinting them. Deployed in front of application servers behind the firewall, WebApp Secure is enhanced with the integration of security intelligence from other sources provided by Spotlight Secure. With this integrated intelligence, Juniper delivers threat mitigation with significantly better accuracy compared to IP-address-only approaches like current next-generation firewalls and reputation feeds, monitoring and identifying hackers as they move from target to target around the world. WebApp Secure is integrated with the SRX Series to extend the ability of the

SRX Series to block attackers that are identified at the security perimeter, and is particularly effective in blocking high volume automated hacking tools.

Spotlight Secure is a new cloud-based threat intelligence solution that will identify individual attackers at the device level (versus the IP address) and track them in a global database. The product creates a persistent fingerprint of attacker devices based on more than 200 unique attributes, delivering precision blocking identification of attackers without the false positives that could impact valid users. Once an attacker is identified and fingerprinted on a subscriber's network using WebApp Secure, the global attacker intelligence solution immediately shares the attacker profile with other subscribers, providing an advanced real-time security solution across multiple networks. When compared with currently available reputation feeds that rely on IP addresses, Spotlight Secure offers customers more reliable security intelligence about attackers and all but eliminates false positives.

DDoS Secure delivers fully automated DDoS protection for websites and Web applications. This solution uses a unique, behavior-based approach to DDoS mitigation that provides protection for high volume attacks, as well as advanced "low-and-slow" application attacks with minimal false positives. DDoS Secure can be deployed as a hardware appliance or as a virtual machine (VM) in private, public, or hybrid cloud environments.

Unified Access Control delivers comprehensive, standards-based, granular network and application access control for even the most diverse, complex environments, reducing cost and maximizing efficiencies. UAC offers best-in-class performance and scalability with centralized policy management, simplifying deployment, administration, and management. UAC combines user identity, device type and integrity, and user location information to create a unique, dynamic access control policy—per user and per session. UAC incorporates different levels of session-specific policy to create extremely granular access control that is easy to deploy, maintain, and dynamically modify. As the centralized policy decision point, UAC is integrated with the SRX Series, with the latter acting as the enforcement point to block unauthorized network access. UAC may be deployed as a dedicated appliance on the MAG Series gateways, or as a virtual appliance.

Summary—Comprehensive Security for Today's Data Center

Growing virtualization adoption leads to the need to secure both the physical and virtual infrastructure. And with a growing number of attacks from outside the company, protection for high value Web applications and defense against DDoS attacks are strict requirements. For further protection of data and digital assets, effective network segmentation and enclaves, along with authenticated and authorized access, are a must. Juniper addresses these challenges by offering superior security and performance for physical and virtual data center assets, innovative security and attacker intelligence sharing, and granular policy decisions and enforcement for authenticated and authorized data center access. Juniper delivers the comprehensive security portfolio that is needed to protect today's complex data center.

Next Steps

Please contact your Juniper Networks representative for more information about comprehensive security for today's data center or any of its solution components: SRX Series Services Gateways, Firefly Host, WebApp Secure, Spotlight Secure, DDoS Secure, and Unified Access Control.

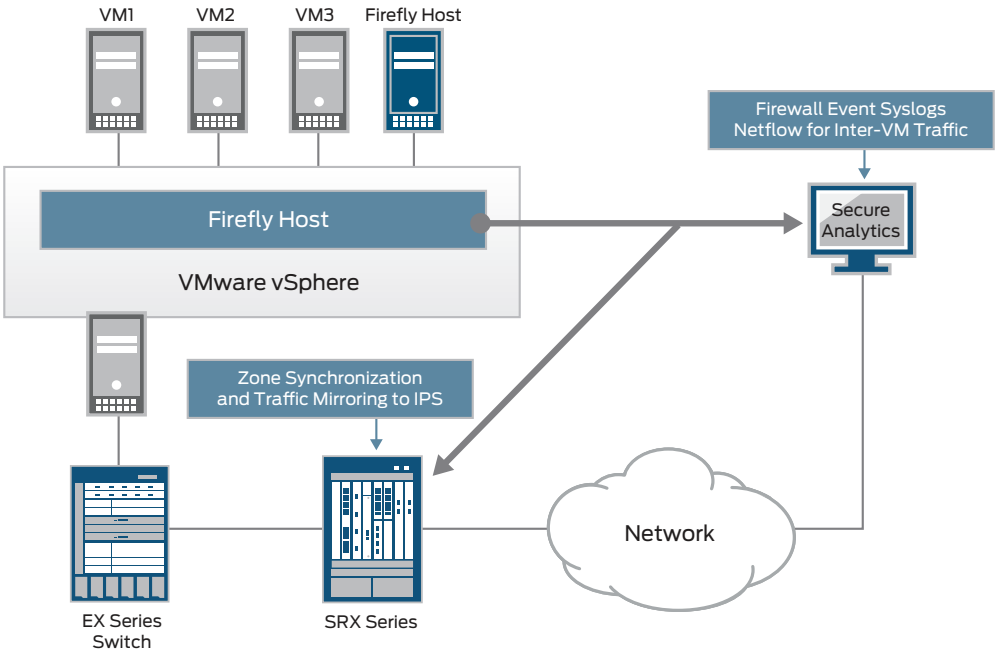

Figure 1: Integrated physical and virtual security delivers comprehensive network protection.

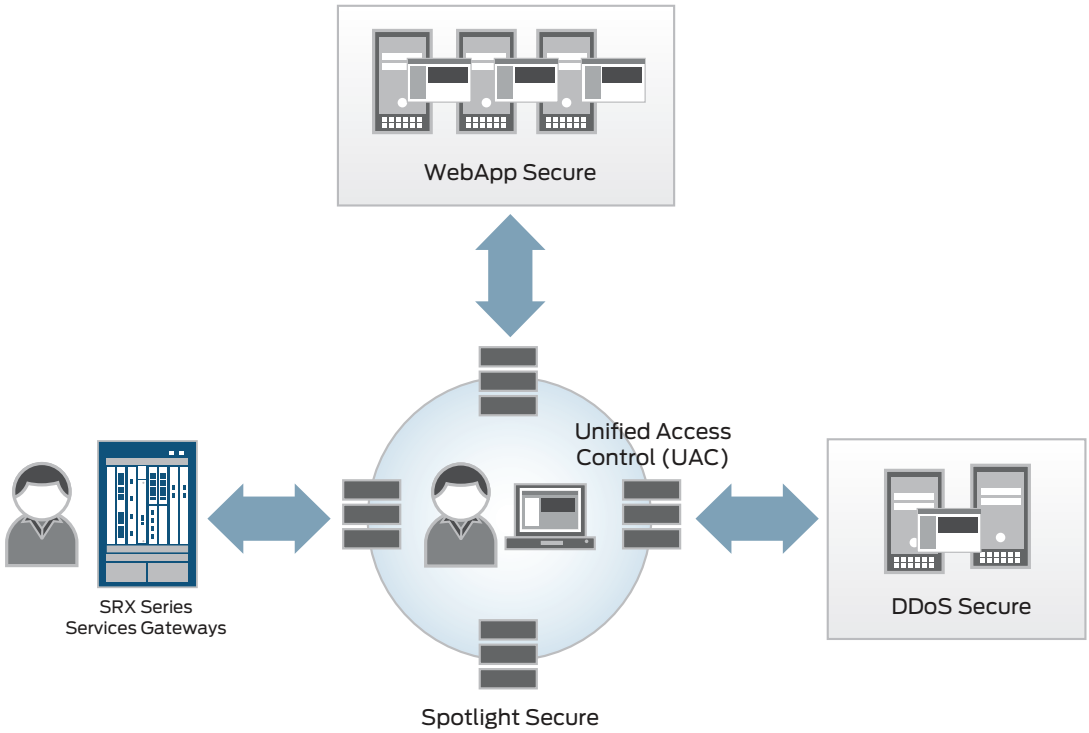

Figure 2: Spotlight Secure with WebApp Secure provides real-time global attacker intelligence sharing and UAC ensure authorized, authenticated access.

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.

3510489-002-EN June 2014