Advanced Micro-Segmentation Services with VMware NSX and Palo Alto Networks®

Technology Segment: Virtualization and Cloud

The Palo Alto Networks Technology Partner Program includes a select group of partners that deliver solutions or products that interoperate with the next-generation firewall.

HIGHLIGHTS

The VMware NSX and Palo Alto Networks integrated solution unlocks the full potential of the software defined datacenter, allowing IT organizations to:

- Automate delivery of next-generation security services
- Accelerate deployment of business critical applications through transparent security enforcement
- Optimize operational efficiency via simplified security policies with virtual, cloud and business context
- Reduce errors in security configuration through context sharing between virtualization and security environments
- Facilitate dynamic service chaining and service orchestration
- Support micro-segmentation initiatives to easily isolate and safely enable virtualized applications of different trust levels in the datacenter
- Create consistent policies across North/South and East/West datacenter traffic
- Address simplified security and compliance mandates with protection against known and unknown threats including exploits, viruses, spyware, malware and advanced persistent threats (APTs).

SOLUTION OVERVIEW

While organizations have gained operational flexibility and lowered datacenter costs by deploying virtualization solutions, the true promise of a secure, agile, extensible, and flexible private cloud continues to be elusive. One of the key barriers is the ability to deploy security services at the same pace as virtual machine deployments without compromising the level of protection needed. VMware and Palo Alto Networks have partnered to address these challenges.

VMware NSX is a network virtualization platform that delivers the operational model of a VM for the network. Using the NSX platform extensible service insertion and chaining capabilities, Palo Alto Networks builds on VMware's native kernel-based firewall capabilities to add next-generation security services. The deployment of next-generation security from Palo Alto Networks is automated; context is shared between virtualization and security elements, and rich security policies based on applications, users, content, and virtual machine "containers" can be defined.

Security Barriers in the Software Defined Datacenter

Existing network security solutions, whether physical or virtualized, exhibit limited security features or are too complex to deploy in a dynamic, agile cloud environment. In order to fully realize the benefits of the software defined datacenter, security requirements need to be addressed in an automated, integrated manner, without trading off features or performance. Challenges include:

- Lack of visibility into East-West traffic
- Security not keeping pace with the rate of change in virtual environments
- Manual, process-intensive networking configurations to deploy security within the virtualized environment
- Performance degradation in virtual environments
- Misaligned cloud admin and security admin workflows
- Incomplete protection against threats to the datacenter

paloalto networks

vmware

VMware NSX and Palo Alto Networks Next-Generation Security

The joint solution featuring VMware NSX and the Palo Alto Networks enterprise security platform was designed to solve these datacenter security challenges. The components of the solution include:

- **VMware NSX:** NSX is the leading network and security virtualization platform that delivers the operational model of a VM for the network. NSX is a full-service, programmable platform that provides logical network abstraction of the physical network and reproduces the entire network model in software allowing diverse network topologies to be created and provisioned in seconds. The NSX distributed service framework and service insertion platform and APIs enable integration of next-generation security services. This is facilitated by the native, kernel based VMware NSX Firewall that provides basic firewall capabilities and steers traffic seamlessly and transparently to the Palo Alto Networks next-generation security platform for inspection.
- **Palo Alto Networks VM-Series for NSX:** The VM-Series is the Palo Alto Networks enterprise security platform in virtualized form factor, designed to address security challenges in virtualized and cloud environments. At the core of this platform is the next-generation firewall, which offers the ability to identify, control, and safely enable applications while inspecting all content for all threats all the time. Palo Alto Networks uses multiple threat prevention disciplines, including IPS and anti-malware, along with URL filtering and file and content blocking, to control known threats, and uses automated sandbox analysis of suspicious files to reveal unknown malware and APTs (advanced persistent threats). Unlike traditional security solutions, the VM-Series offers the same set of security features as the next-generation physical firewalls, and is managed using the same management platform, ensuring a consistent set of policies is maintained in the datacenter.
- **Palo Alto Networks Panorama:** Panorama is the Palo Alto Networks centralized management platform, providing the ability to manage a distributed network of virtualized and physical firewalls from a centralized location. Capabilities include the ability to view all firewall traffic, manage all aspects of device configuration, push global policies; and generate reports on traffic patterns or security incidents.

As shown in Figure 1, the tightly integrated solution delivers the following capabilities:

- **Independence from networking topology.** Security policies are applied regardless of where a VM connects at a point in time. This works with any network overlay, and with traditional VLAN networking.
- **Automated deployment and provisioning** of next-generation security in lock step with the fluid virtual compute layer. Panorama communicates with the NSX Manager to register as a security management platform, providing information about the VM-Series. NSX Manager then automates the deployment of next-generation security services on every VMware ESXi server. Each VM-Series deployed then communicates directly with Panorama for automated licensing and provisioning.
- **Seamless traffic steering to next-generation security:** Within the VMware virtualized server environment, application traffic is steered to the VM-Series via NSX APIs without needing to manually make configuration changes to virtual networking elements.
- **Dynamic security policies based on application, user, content and virtual machine "container":** Palo Alto Networks next-generation security policies can be defined based on applications, users, content and virtual machine (VM) "containers". As virtualized applications are instantiated and placed in logical "containers", the notion of "containers" can be extended to VM-Series security policies via the Palo Alto Networks dynamic address group feature.

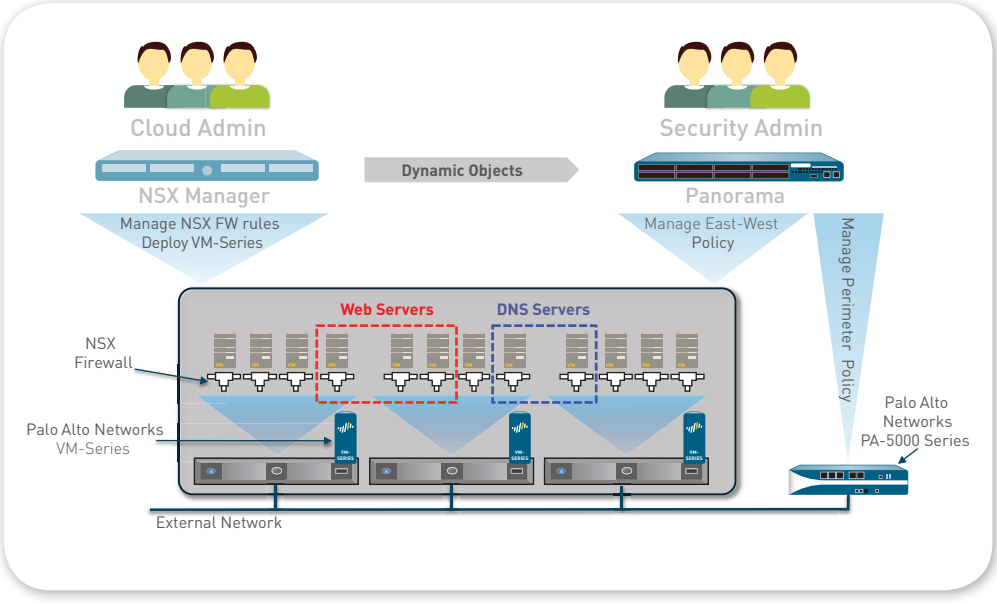

Figure 1: VMware NSX and Palo Alto Networks Next-Generation Security Platform

Full context sharing between the VMware and Palo Alto Networks management platforms ensures that dynamic address groups is updated with the latest information representing the VM container instead of having to manually track hundreds or thousands of IP addresses. This makes it incredibly easy to apply security to virtualized applications no matter when they are created or moved across the network.

- **Next-generation security protection for virtualized applications and data:** Because the VM-Series supports the PAN-OS™ operating system, comprehensive next-generation security features can be deployed to identify, control, and safely enable data enter applications while inspecting all content for all threats. Safe application enablement means you can build firewall policies that are based on application/application feature, users and groups, and content, as opposed to port, protocol and IP address, transforming your traditional allow or deny firewall policy into business-friendly elements. Threat protection capabilities address the whole attack lifecycle, featuring protection against exploits, viruses, spyware, malware and targeted unknown threats such as advanced persistent threats (APTs).
- **Scales linearly with the number of hypervisors:** The IT administrator no longer needs to guess how much network security capacity is needed. Any time a new hypervisor is added, next-generation security capacity is automatically added.

Summary

The VMware NSX and Palo Alto Networks integrated solution extend the basic firewall services delivered by the NSX virtualization platform. The joint solution provides an integrated datacenter solution that allows IT organizations to unlock all the benefits of the software defined datacenter, from optimized capacity utilization and operational efficiencies to greater flexibility and agility without compromising security. IT administrators can now automate the delivery of leading next-generation security services from Palo Alto Networks in lock step with the fluid virtual compute layer, to provide comprehensive visibility and safe enablement of all datacenter traffic including intra-server virtual machine communications.

About Palo Alto Networks

Palo Alto Networks is the leading next-generation network security company. Its innovative platform allows enterprises, service providers, and government entities to secure their networks by safely enabling the increasingly complex and rapidly growing number of applications running on their networks and by providing prevention against cyberthreats. The core of Palo Alto Networks is its enterprise security platform which delivers application, user, and content visibility and control integrated within the firewall through its proprietary hardware and software architecture. Palo Alto Networks products and services can address a broad range of network security requirements, from the datacenter to the network perimeter, as well as the distributed enterprise, which includes branch offices and a growing number of mobile devices. Palo Alto Networks products are used by more than 17,000 customers in over 120 countries. For more information, visit **www.paloaltonetworks.com**.

paloalto networks
the enterprise security company™

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com