VM-SERIES FOR VMWARE NSX

VMware® and Palo Alto Networks® have partnered on a solution that leverages NSX® to enable the VM-Series to be transparently inserted into SDDC environments, allowing you to protect your applications and data with the Next-Generation Firewall and advanced threat prevention.

A strategic partnership for Palo Alto Networks, the integration of our Next-Generation Security Platform with VMware NSX, automates next-generation firewall services for the software-defined data center (SDDC).

Highlights

- Accelerate the deployment of business-critical applications by provisioning security services and new virtual workloads simultaneously.
- Dynamically scale next-generation security in lockstep with workload build-out by simply adding hypervisors.
- Isolate and safely enable virtualized applications of different trust levels through micro-segmentation and secure multi-tenancy support.
- Address security and compliance mandates with protection against known and unknown threats including exploits, viruses, spyware, malware and advanced persistent threats (APTs).
- Simplify automation of security workflows across your software-defined data center (SDDC).
- Enforce policy consistency across north-south and east-west data center traffic through Panorama.

SDDC architectures virtualize compute, storage and networking infrastructure to enable you to simplify operations, speed time to provision network and security services, and fundamentally improve your data center security. VMware NSX is a network virtualization platform that delivers the operational model of a VM for the network and reproduces all networking services in software. NSX extensibility, native security capability, including kernel-based distributed firewalling, and security operations automation allow server-to-server traffic inside the data center to be automatically steered to the VM-Series for granular inspection based on applications, content and users. Together, the integrated solution delivers the dynamic insertion, chaining, distribution and orchestration of advanced security services for SDDC environments.

Existing network security solutions are optimized for perimeter-based defense, but server-to-server traffic, which represents 80 percent of overall data center traffic, is not inspected by security controls.

The joint solution leverages VMware NSX to fully automate the provisioning and deployment of Palo Alto Networks VM-Series Next-Generation Firewall, allowing customers to protect their applications and data from today's advanced cyberattacks. The components of the solution include:

- **VMware NSX:** NSX, the leading network and security virtualization platform 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. NSX applies security controls at the hypervisor layer for optimal context and isolation, inherently provides security isolation, enables micro-segmentation based on logical boundaries, and allows for workload-level isolation and segmentation. Policies are enforced at the virtual interface and follow the workload unconstrained by physical topology. The NSX distributed service framework and service insertion platform enable integration of next-generation

security services. The NSX native, kernel-based distributed firewall, used for L2–L4 filtering, steers traffic transparently to the VM-Series for advanced inspection.

- **Palo Alto Networks VM-Series for NSX:** The VM-Series virtualized Next-Generation Firewall brings secure application enablement and threat prevention to the virtualized and cloud environments. At the core of the VM-Series platform is the Next-Generation Firewall, which determines the three critical elements of your security policy: The application identity regardless of port, the content malicious or otherwise, and the user identity – all in a single pass. Unlike traditional security solutions, the VM-Series offers the same set of security features as our physical form factor firewalls, and is managed using the same management platform, ensuring a consistent set of policies is maintained in the data center.
- **Palo Alto Networks Panorama:** Panorama™ network security management platform that provides the ability to manage a distributed network of virtualized and physical firewalls from a single 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.

The integrated solution allows you to leverage NSX to automate the provisioning of next-generation security services. Additional integration points between NSX and the VM-Series can automate policy updates to help eliminate the time lag that may occur between new virtualized application deployments, or changes, and the associated security policy updates. As shown in Figure 1, the 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. The VM-Series is deployed by NSX manager, keeping security in lockstep with the fluid virtual compute layer. Panorama communicates with the NSX Manager to register the VM-Series as a security service. NSX Manager then deploys the VM-Series on every VMware ESXi™ server in an automated manner, thereby ensuring security is deployed as the environment scales. Each VM-Series deployed then communicates directly with Panorama to receive associated security policies.
- Next-generation security protection for virtualized applications and data. Each ESXi server that needs security receives a VM-Series Next-Generation Firewall, which will allow you to deploy security policies to identify, control, and safely enable data center 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).
- Seamless traffic steering to next-generation security: Traffic is steered by the NSX Distributed Firewall, a stateful, in-kernel firewall to the VM-Series via NSX APIs without needing to manually make configuration changes to virtual networking elements.
- Dynamic security policies based on application, content and user. VM-Series security policies can be defined based on applications, content and users through the use of security groups. As virtualized applications are instantiated, they are placed in security groups in NSX manager, which are recognized by Panorama and the VM-Series. Security groups then become the basis of the security policies that are deployed to each VM-Series.
- Multiple security policy sets within the SDDC environment. VM-Series for NSX can be configured to support dedicated security policy sets per cluster. A separate service profile gets assigned to each tenant leading to duplicate IP address support, isolation of network traffic, security policy and logs per tenant. Secure multi-tenancy can be implemented across shared and dedicated virtual compute infrastructure.

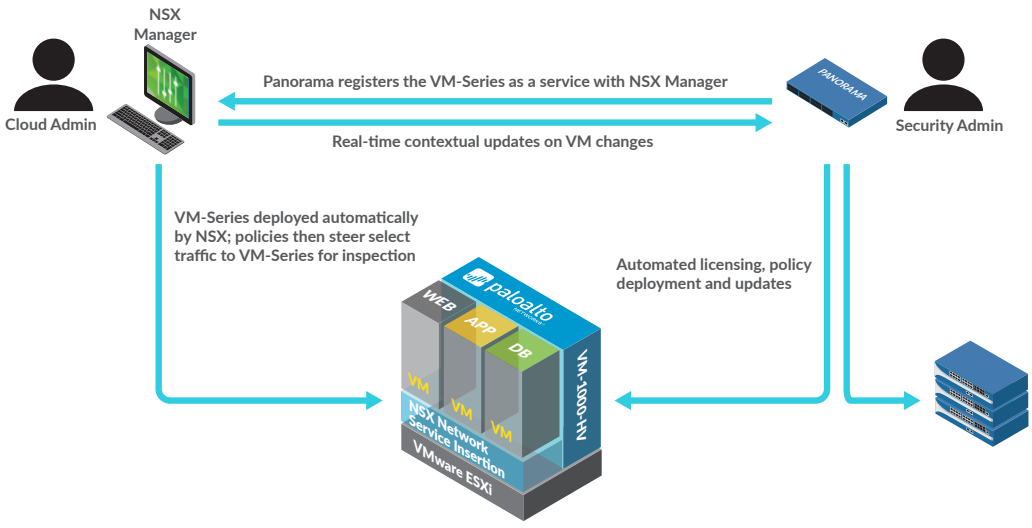

Figure 1: VMware NSX and Palo Alto Networks VM-Series integrated solution

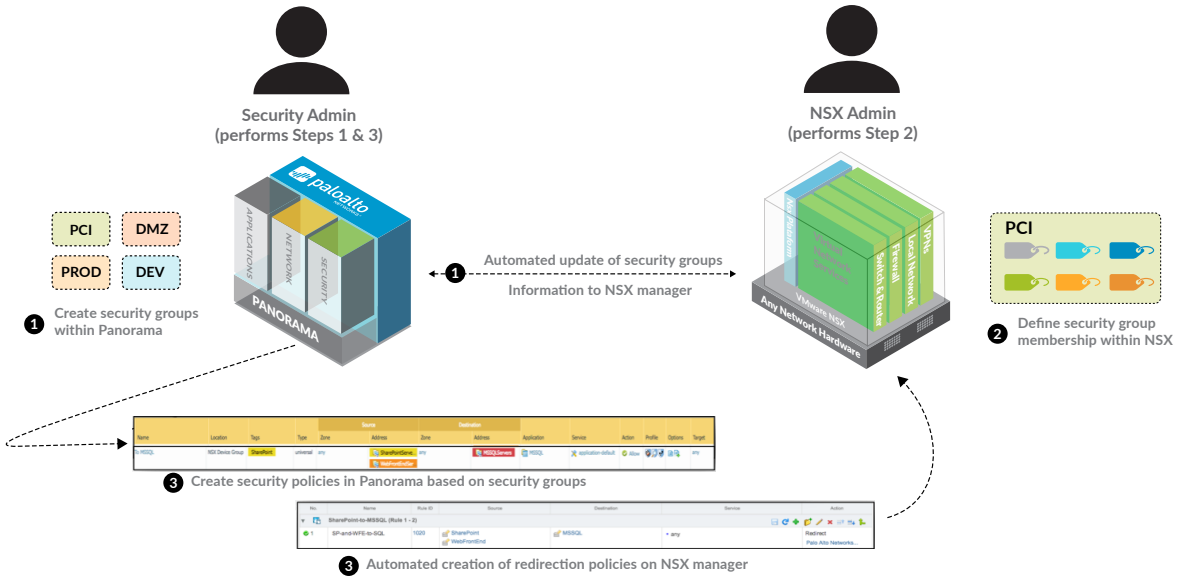

Figure 2: Automated security policy creation within Panorama

- **Simplified security automation workflows with Panorama:** Panorama can manage the entire security workflow in the NSX deployment. As shown in figure 2, creation of NSX security groups and traffic steering rules within NSX manager is automated and streamlined during security policy creation within Panorama. Panorama also ensures security configurations are in sync with NSX manager for consistent security posture.

As virtual workloads within the security groups change, context sharing between NSX manager and Panorama occurs, triggering a dynamic policy update. The use of security groups combined with the dynamic context sharing ensures security is deployed for virtualized applications, no matter when they are created or moved across the network.

Performance and Capacities Summary

The Security performance table listed below is tested under controlled lab conditions with PAN-OS® 8.0. In virtualized and cloud environments, many factors such as type of CPU, hypervisor version, numbers of cores assigned and network I/O options can impact your performance. We recommend additional testing within your environment to ensure your performance and capacity requirements are met.

Model	VM-100/ VM-200 (2 Cores)	VM-300/ VM-1000-HV (4 Cores)	VM-500 (8 Cores)
Firewall throughput (App-ID enabled)	1 Gbps	1.5 Gbps	3 Gbps
Threat prevention throughput	500 Mbps	1 Gbps	3 Gbps
IPsec VPN throughput*	In process	In process	In process
New sessions per second *	In process	In process	In process
Max sessions	250,000	800,000	2,000,000

*IPsec VPN throughput and new sessions per second data will be published upon completion of the test suite

The performance and capacities results were tested under following conditions:

- Firewall and IPsec VPN throughput are measured with App-ID and User-ID features enabled.
- Threat prevention throughput is measured with App-ID, User-ID, IPS, antivirus and anti-spyware featured enabled.
- Throughput is measured with 64Kb HTTP transactions.
- Connections per second is measured with 4Kb HTTP transactions.

VM-Series for VMware NSX Specifications and Requirements

The table below lists all supported specifications and resource requirements on VM-Series for VMware NSX.

VIRTUALIZATION SPECIFICATIONS	
Hypervisor version supported	VMware vSphere 5.5, 6.0 VMware NSX Manager 6.0, 6.1, 6.2
I/O options supported	VMware paravirtual drivers (vmxnet3, e1000)

SYSTEM REQUIREMENTS	VM-100/ VM-200 (2 Cores)	VM-300/ VM-1000-HV (4 Cores)	VM-500 (8 Cores)
CPU cores configurations	2	2,4	2,4 and 8
Memory (minimum)	6.5GB	9GB	16GB
Disk drive capacity (min/max)	60GB/ 2TB	60GB/ 2TB	60GB/ 2TB

Summary

The integration between VMware NSX and the Palo Alto Networks VM-Series fully automates the deployment of the Next-Generation Firewall and advanced Threat prevention services for SDDC environments.

About Palo Alto Networks

Palo Alto Networks is leading a new era in cybersecurity by protecting thousands of enterprise, government, and service provider networks from cyberthreats. Unlike fragmented legacy products, our security platform safely enables business operations and delivers protection based on what matters most in today's dynamic computing environments: applications, users and content. Find out more at www.paloaltonetworks.com.

About VMware

VMware is a global leader in cloud infrastructure and business mobility. Built on VMware's industry-leading virtualization technology, our solutions deliver a brave new model of IT that is fluid, instant and more secure. Customers can innovate faster by rapidly developing, automatically delivering and more safely consuming any application. With 2014 revenues of $6 billion, VMware has more than 500,000 customers and 75,000 partners. The company is headquartered in Silicon Valley with offices throughout the world and can be found online at www.vmware.com.

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

vm-series-for-vmware-nsx-ds-020617