VM-SERIES FOR NSX IMPLEMENTATION AND TRAFFIC STEERING GUIDELINES

VMware® and Palo Alto Networks® have partnered on a solution that leverages NSX® to enable the VM-Series to be transparently inserted into software-defined data center (SDDC) environments, enabling organizations to protect their virtualized applications and data with next-generation firewalls and advanced threat prevention. The integrated solution includes the VM-Series for NSX, Panorama™ network security management and VMware NSX.

This paper provides some design considerations and recommendations for customers who are deploying the VMware NSX and Palo Alto Networks VM-Series integrated solution. It also outlines how the NSX Distributed Firewall (DFW) is used to steer business-critical traffic to the VM-Series firewall for more granular analysis and inspection, thereby protecting the applications and data within your SDDC from advanced cyberattacks.

Table of Contents

The Need for East-West Traffic Protection

In order to better understand the need to secure traffic flowing from VM to VM in an east-west manner, it is important to establish an architectural framework. Figure 1 displays a typical virtualized data center (private cloud) design.

The compute cluster is the building block for hosting the application infrastructure and provides the necessary resources in terms of compute, storage, networking and security. Compute clusters can be interconnected using L2 or L3 technologies, such as VLAN, VXLAN or IP, providing a domain extension for workload capacity. Innovations in the virtualization space allow VMs to move freely in this private cloud while preserving compute, network, storage, and security characteristics and postures.

In a private cloud, there are two different types of traffic, each of which is secured in a different manner:

- **North-south:** refers to data packets that move in and out of the virtualized environment from the host network or a corresponding traditional data center. North-south traffic is secured by one or more physical form factor, perimeter edge firewalls. The edge firewall is usually a high throughput appliance working in high availability active/passive (or active/active) mode to increase resiliency. It controls all the traffic reaching into the data center and authorizes only allowed and "clean" packets to flow into the virtualized environment.
- **East-west:** refers to data packets moving between virtual workloads entirely within the private cloud. East-west traffic is protected by a local, virtualized firewall instantiated on each hypervisor. East-west firewalls are inserted transparently into the application infrastructure and do not necessitate a redesign of the logical topology.

Corporate Data at Risk

Data centers are typically centralized repositories of an organization's most critical asset: the data that drives the business, which can include customer information, such as credit card numbers or patient medical records. That data is a target for cybercriminals, as evidenced by the number of high-profile data breaches. Historically, organizations implemented security to protect traffic flowing north-south, which is insufficient in protecting east-west traffic within a private cloud from advanced cyberattacks.

To improve their security posture relative to their corporate data, organizations have acknowledged that protecting against threats across the entire network, both north-south and east-west has become a security best practice.

One common practice in a private cloud is to isolate VMs into different tiers. Isolation provides clear delineation of application functions and allows security teams to easily implement security policies. With NSX, isolation is

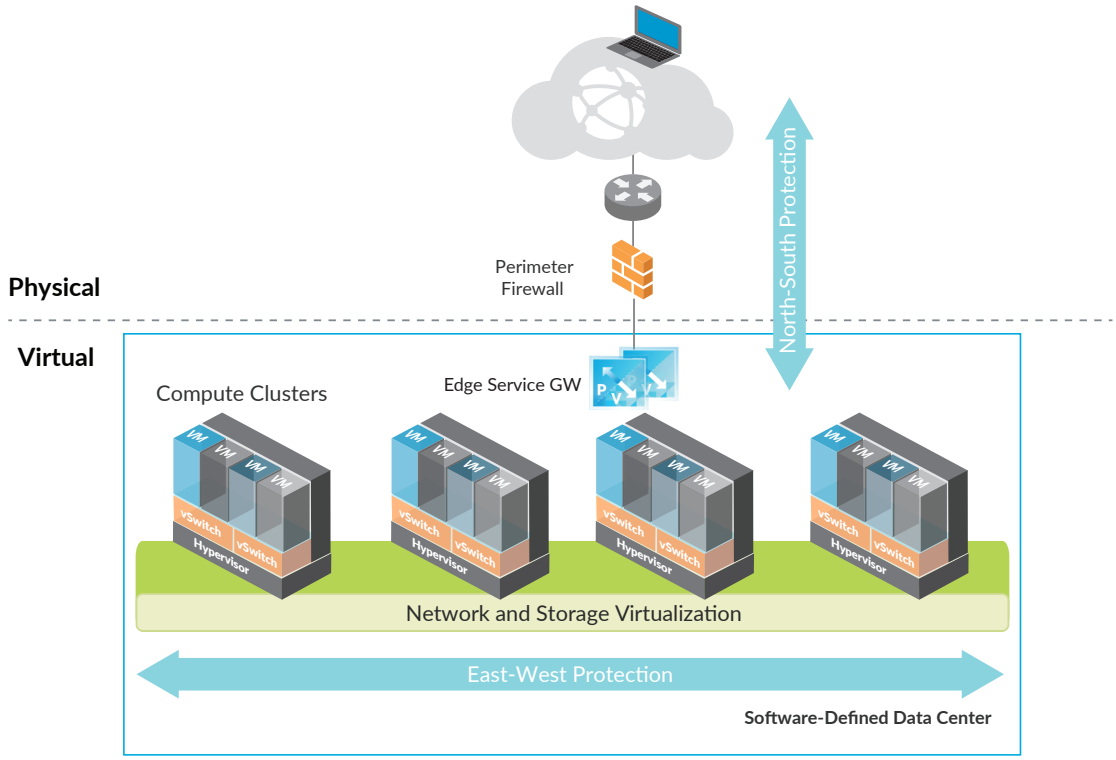

Figure 1: A typical virtualized data center (private cloud) design

configured using logical software constructs (e.g., Security Groups) and performed at the virtual network interface of each VM. Figure 2 displays a simple three-tier application that is comprised of a WEB-VM as the front end, an APP-VM as the application, and Figure 2 displays a simple three-tier application that is comprised of a WEB-VM as the front end, an APP-VM as the application, and a DB-VM providing database services.

An attacker has multiple options to steal data from the DB-VM. The first option is to initiate an SQL injection attack by sending HTTP requests containing normalized SQL commands that target an application vulnerability. The second option is to compromise the WEB-VM (using vulnerability exploits), and then move laterally to the APP-VM, initiating a brute force attack to retrieve the SQL admin password.

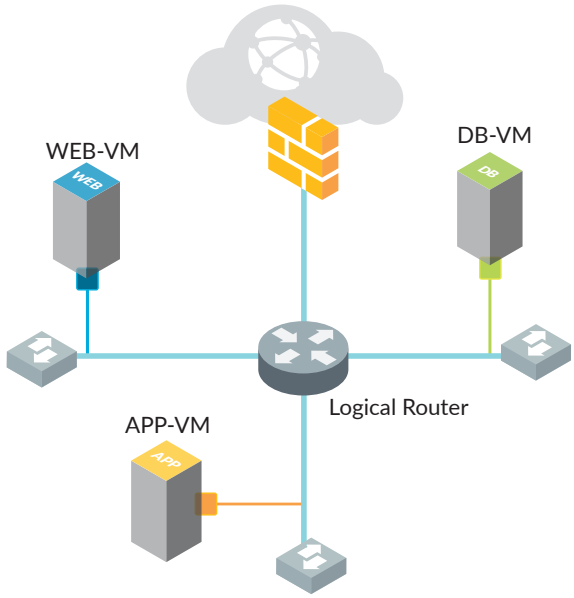

Figure 2: Three-tier application hosted in a virtual data center

Once the DB-VM is compromised, the attacker can hide sensitive data extraction in plain sight using techniques like DNS tunneling, or by moving data across the network with NetBIOS and then off the network via FTP. In fact, using applications commonly found on nearly every network, the options are virtually unlimited for attackers to steal critical data in this environment. Infiltration into the environment and exfiltration of critical data can be completely transparent and undetected by the operations team because the data (carried over legitimate protocols like HTTP, SQL and DNS) are used for day-to-day business activities.

Virtual data center security best practices dictate a combination of north-south and east-west protection. East-west protection provides the following benefits:

- Authorizes only allowed applications to flow inside the data center, between VMs.
- Reduces lateral threat movement when a front-end workload has been compromised (attacker successfully breaches the front-end server using a misconfigured application or unpatched exploit).
- Stops known and unknown threats that are sourced internally within the data center.
- Protects against data theft by leveraging data/file filtering capability and blocking anti-spyware communications to the external world.

An added benefit of using virtual firewalls for east-west protection is the unprecedented traffic and threat visibility that the virtualized security device can now provide due to the greater context available. Once traffic logs and threat logs are turned on, VM-to-VM communications and malicious attacks become visible. This virtual data center awareness allows security teams to optimize policies and enforce advanced threat protection (e.g., IPS, anti-malware, anti-spyware, file blocking, data filtering, DoS protection) where needed.

Hidden Lynx: Highlighting the Need for East-West Protection

In many of the recent breaches, attackers moved laterally across either a physical or virtualized network to accomplish their goals. In an attack documented by Symantec™ in 2013, the APT group Hidden Lynx was able to gain access to a software supplier's virtualized environment and move laterally from VM to VM. The attackers first gained access to the network using an SQL injection attack, as shown in Figure 3.

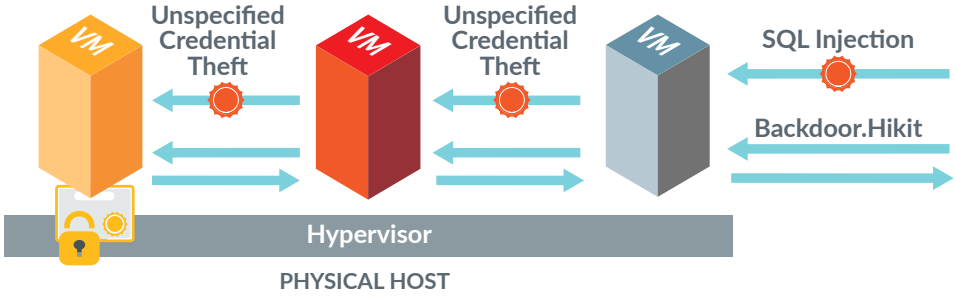

Figure 3: Hidden Lynx attack propagation in a virtual data center

Once on the network, the attackers had installed Backdoor.Hikit, a Trojan that provides extremely stealthy remote access to compromised systems. The attackers then stole the credentials for the virtual machine that contained the digital code-signing certificates. The attackers used this code-signing infrastructure to sign thirty-two malicious files that were found within organizations in the United States Defense Industrial Base Sector. The signing of these files is significant, since the process of digital signing implies trust and, therefore, simplifies the attackers' goal of compromising the network.

This case study highlights the level of sophistication attackers have achieved, and it clearly demonstrates the need to protect east-west traffic. Using the VM-Series Next-Generation Firewall, in this example, could have controlled the application traffic, forcing it (and only it) over a standard set of ports, and it could have prevented the SQL injection attack, as well as the lateral movement (by detecting and blocking credential theft attempts) and malware download.

VM-Series and NSX Joint Solution

Overview

VMware and Palo Alto Networks have partnered on a solution that leverages NSX to enable the VM-Series to be transparently inserted into software-defined data center (SDDC) environments, enabling organizations to protect their virtualized applications and data with next-generation firewalls and advanced threat prevention. The integrated solution is comprised of three components:

- **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 the integration of next-generation security services. NSX native, kernel-based distributed firewall (DFW), 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 is the Palo Alto Networks 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. Identifying and controlling your data center traffic reduces the scope of attacks by:
  - Validating data center applications are in use on standard ports.
  - Blocking rogue or non-compliant applications.
  - Preventing known and unknown threats from moving laterally.
  - Systematically managing unknown traffic.
- **Palo Alto Networks Panorama:** Panorama is a centralized 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.

Figure 4 highlights how the integrated solution works. Panorama registers the VM-Series firewall as an available service with NSX Manager. This allows the VM-Series to be provisioned on all hosts through NSX Manager/vCenter interaction while removing the requirement of manually configuring IP addresses within Panorama, further automating the provisioning and management process.

Once a VM is deployed, its associated VM-Series firewall will subsequently register with Panorama, and obtain the required licenses and associated security policies. In NSX Manager, virtual machines are grouped into logical containers, called NSX Security Groups, based on desired considerations (e.g., function like a tier of an application). As servers are added, they can dynamically join groups based on specified criteria, including name, security tag and operating system.

Once a security group has been defined in NSX Manager, a Dynamic Address Group is created in Panorama and mapped to the parallel group. This process is key to automating the flow of workload changes made in the NSX environment into the Panorama system. This connection and ongoing communications eliminate the manual intervention required to update all firewalls with these policy-related changes.

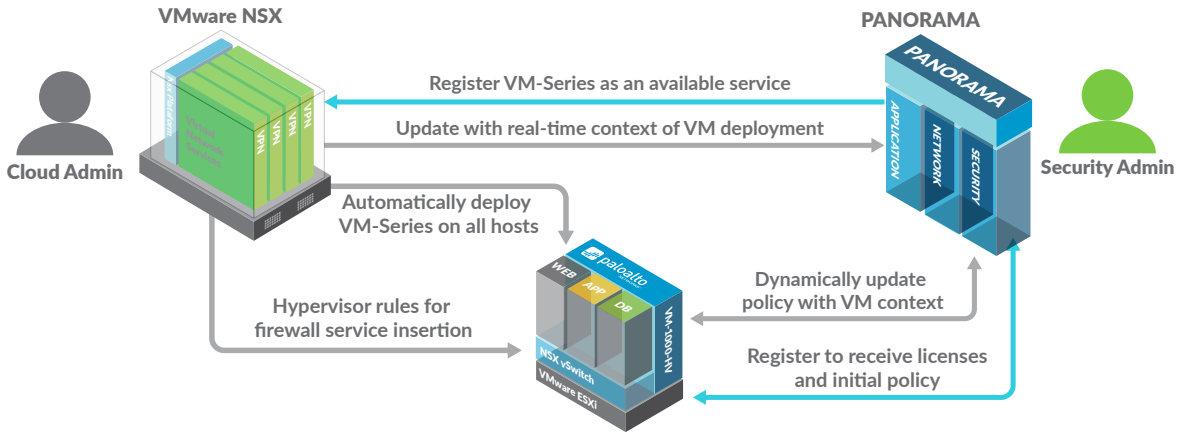

Figure 4: Interactions between NSX Manager, Panorama and the VM-Series

Solution Benefits

The benefits of using the integrated solution can be broken down into the three areas of deployment, security and operations.

Deployment Benefits

- Off-the-shelf integration between NSX, the VM-Series and Panorama eliminates the need for any additional installation components, thereby simplifying deployment.
- Automates the deployment of the VM-Series on VMware ESXi™ hosts in the cluster, ensuring no system downtime or traffic disruption.
- The VM-Series deployment lifecycle (provisioning and removal) is fully managed by VMware NSX, thereby reducing administrative efforts and ensuring security keeps pace with the business.
- Panorama fully manages the VM-Series licensing process, eliminating the need to perform any additional administrative operations every time a new VM-Series is instantiated.
- VM-Series insertion is network topology agnostic, eliminating the administrative effort associated with virtual networking reconfiguration in order to redirect traffic to the VM-Series for inspection.
- VMware NSX allows application and cloud administrators to selectively redirect application traffic for advanced L4–L7 inspection by the VM-Series, resulting in an improved security posture.

Advanced Security Benefits

- Unprecedented protection of applications and data from known and unknown threats by leveraging advanced security features, which includes application-level control, vulnerability protection, anti-spy- ware, anti-malware, file and data filtering, and DoS protection.
- Security policies are deployed as the VM is connected to the network, reducing the chance for attackers to exploit any transitory states.
- Policy consistency across the entire virtual infrastructure guarantees the same (improved) security posture for each VM irrespective of location.
- Real-time exchange of VM addition/deletion/changes context between NSX and Panorama enables security policies to be dynamically updated, ensuring security keeps pace with the business.
- Unlocks VM workload mobility across hosts in the cluster while preserving security posture and maintaining active flow sessions.

Operational Benefits

- Security policies can be predefined by security administrators (even before VM workloads are created), thereby streamlining secure workload deployment.
- Single pane of glass to manage all VM-Series operations (e.g., security policies, configuration, traffic and threat monitoring, signature updates, firmware code upgrade) using Panorama centralized management.

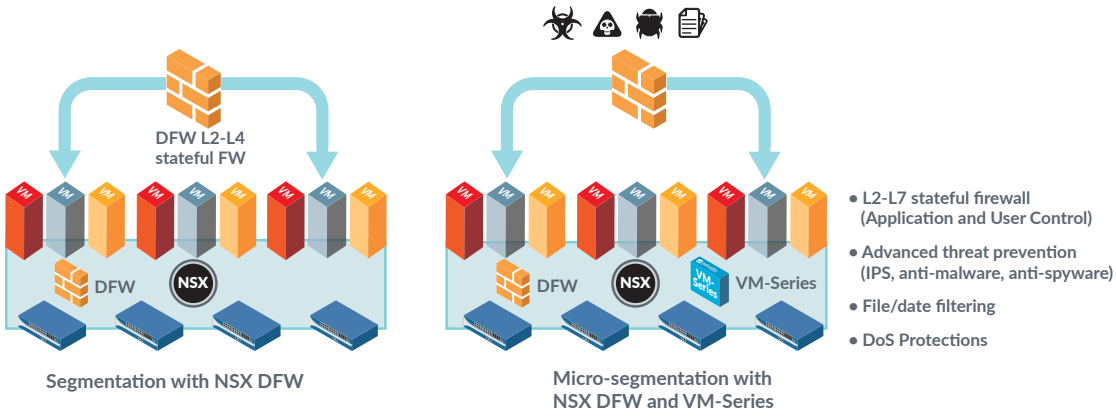

Figure 5: Augmenting micro-segmentation security capabilities using VM-Series virtualized next-generation firewalls

- Eliminates the time gap between security policy update and workload provisioning by fully automating security deployment, including VM-Series deployment, NSX traffic redirection rules, and VM-Series security policy delivery and update.

VM-Series and Distributed Firewall Complementary Security Services

Attackers have become increasingly sophisticated, using common applications to bypass traditional port/IP-based controls, and then moving with little resistance across the network, using applications commonly found on your network to steal their targeted payload. To help you prevent these sophisticated attacks, the VM-Series complements the distributed firewall (DFW) port-based filtering with full-stack (Layer 4–7) traffic classification and inspection in the NSX environment, allowing customers to control which applications talk with each other while blocking both known and unknown threats, as shown in Figure 5.

The following sections will highlight important characteristics to take into account when using the DFW and VM-Series to provide advanced security functions for virtual data center workloads.

Design Considerations for East-West Protection

As discussed previously, the VMware NSX DFW and Palo Alto Networks VM-Series are both designed to protect east-west traffic. DFW provides in-kernel, stateful, port-based inspection while the VM-Series provides next-generation firewall and advanced threat prevention capabilities (e.g., application control, IPS, antivirus, anti-malware, data/file filtering, DoS protection).

Using the three-tier application example defined earlier, VMs are partitioned across WEB, APP and DB tiers. Each tier can be instantiated by either a logical switch (VXLAN) or a DVS port-group (VLAN).

This L2 broadcast domain is connected to a DLR (Distributed Logical Router) to enable inter-tier communication (e.g., IP address on the DLR logical interface becomes the default GW for guest VM). In this scenario, DFW can be used to protect intra-tier traffic and, if needed, to protect storage and backup traffic. The VM-Series would then be used to protect inter-tier traffic. Figure 6 shows the division of roles between the DFW and the VM-Series.

Based on the recommendations above, traffic between WEB servers is protected by DFW (same behavior for traffic between the APP servers and for traffic between DB servers). The DFW security control based on L2/L3 services and L2/L3 addresses is sufficient to prevent any lateral move or attack from hackers by limiting access – and not by using other threat prevention elements. For instance, an L2 rule can control ARP protocol, while an L3 rule can control communication on a specific TCP/UDP port.

Traffic from WEB server to APP server (as well as traffic from APP server to DB server) is protected by the VM-Series. Inter-tier traffic essentially contains critical data that must be deeply analyzed (up to Layer 7) to prevent any threat or malware propagation across the different systems. The VM-Series also reduces the attack surface by safely enabling communications only between those application tiers as defined by policy.

Referring to the attack case study, using the VM-Series for inter-tier protection would have effectively blocked the attack at any stage: first, by detecting and stopping SQL injection; second, by preventing the attacker from moving laterally using the credential theft technique; and third, by blocking any malware download that opens a back door to the system.

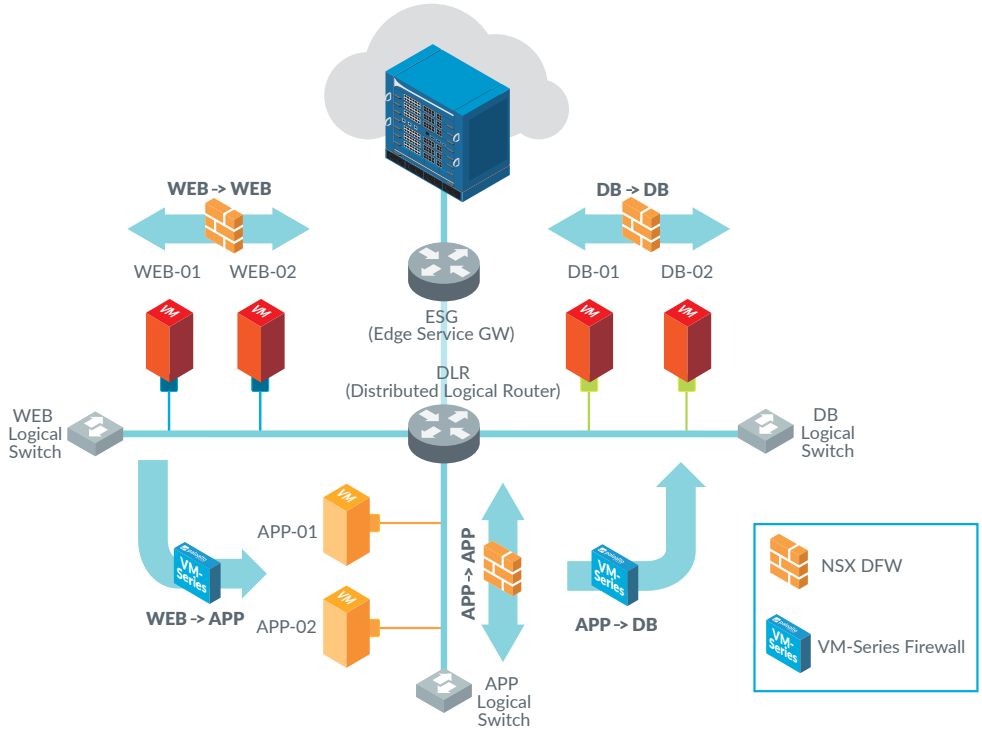

Figure 6: Complementary use of DFW for intra-tier and the VM-Series for inter-tier traffic protection

Up to now, isolation has been achieved using a logical network construct: each tier is instantiated by a specific VXLAN or VLAN entity. In fact, NSX provides the capability to define multiple tiers, even if VMs are located on the same L2 broadcast domain. This is achieved by using the NSX Security Groups construct. A security group is a logical entity that groups different objects (any vCenter object in reality – except folders) into the same container structure. The advantage of having all VMs located on a unique L2 domain is a reduction in L3 subnet addresses – and a simplification in the routing entity (no need to route between the tiers now) – while preserving the exact same security posture. In this flat topology, design considerations to properly implement both the DFW and VM-Series still apply, as shown in Figure 7.

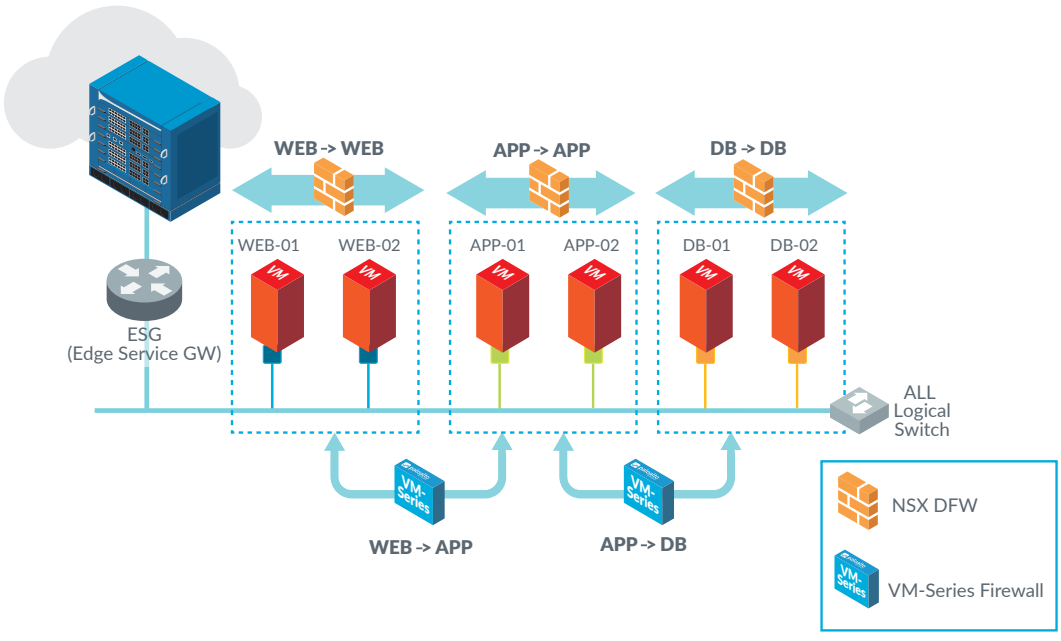

Figure 7: Complementary use of DFW and VM-Series for intra-tier and inter-tier traffic protection

As mentioned earlier in the document, the VM-Series sits off the data path and does not expose any external data ports. This simplifies virtual network topology design, as no change is required when inserting security services for VM-to-VM communications. In order to leverage the VM-Series, workload traffic must be redirected to the virtual appliance. The NSX DFW provides a very granular way to specify traffic that must be redirected to the VM-Series.

Traffic redirection rules are based on source/destination/service attributes (source and destination field can use any vCenter objects like VM name, Cluster, Resource Pool, Security Groups; service field can use any TCP/UDP ports). As a consequence, it is very easy to define traffic redirection policies based on a particular source VM to destination VM. In the same way, it is as easy (as before) to specify that traffic from a group of WEB-VM to a group of APP-VM needs to be redirected to the VM-Series.

To give a practical view of the required configuration for this joint solution integration, security policies and traffic redirection policies defined on NSX Manager and Panorama may look like the table above (example only).

Using the VM-Series, Threat Prevention capabilities are actionable per policy rule, using Security Profiles definition. Any of the following threat prevention features can be enabled per policy rule: IPS, antivirus, anti-malware, data/file filtering, DoS protection. This provides customers with significant flexibility and granularity in terms of security levels that can be applied per business application deployment and/or per VM-to-VM communications.

Deployment Example

When a security administrator initiates a new service deployment on NSX, NSX Manager will automatically deploy a VM-Series firewall instance per ESXi host in the cluster. Once the deployment is done, Panorama will provision the VM-Series firewall with predefined policy rules written by the security administrator ahead of time. Note that VMware service registration (defined under Panorama) must have been previously configured in order for the service deployment to be successful.

Anytime a new ESXi host is added to the cluster, NSX Manager will systematically trigger a deployment of a VM-Series instance on this host (followed by properly provisioning the virtual firewall). When the ESXi host is removed from the cluster, the VM-Series instance is then automatically deleted by NSX Manager. The same mechanism applies when a cluster exits the NSX domain ("un-prep" process). The automation of the VM-Series provisioning is one of the key benefits of the joint solution integration – it allows security to be deployed in lockstep with new workloads, as shown in Figure 8.

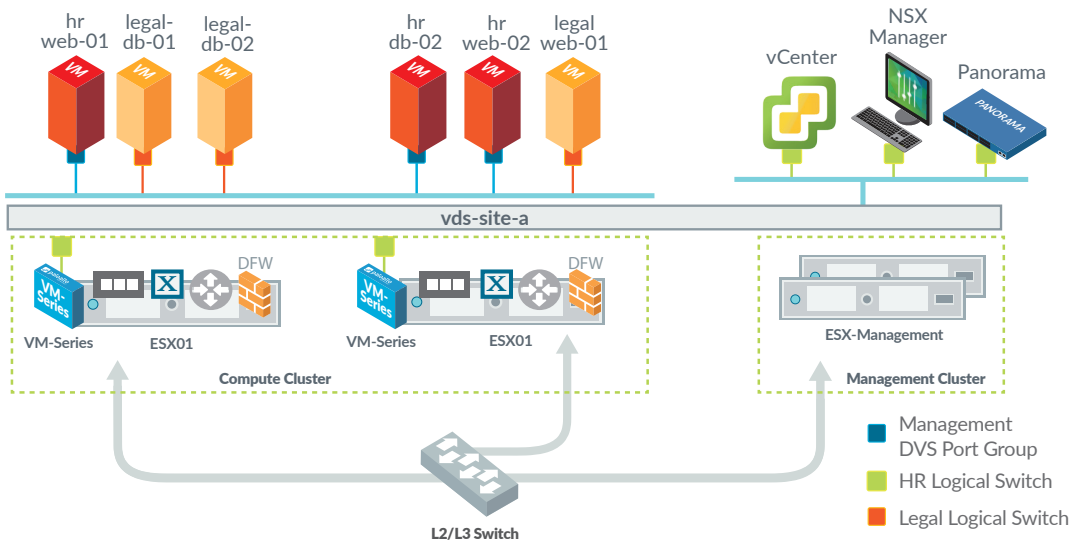

Figure 8: VM-Series deployment with NSX

In the current release of NSX, service deployment follows this unique rule: a single VM-Series per ESXi host (this is true for any service VM deployed by NSX), and this instance of the firewall is always in active mode. It inspects traffic initiated by the guest VM (or destined to the guest VM) on the same host, based on traffic redirection rules set by the security admin on NSX.

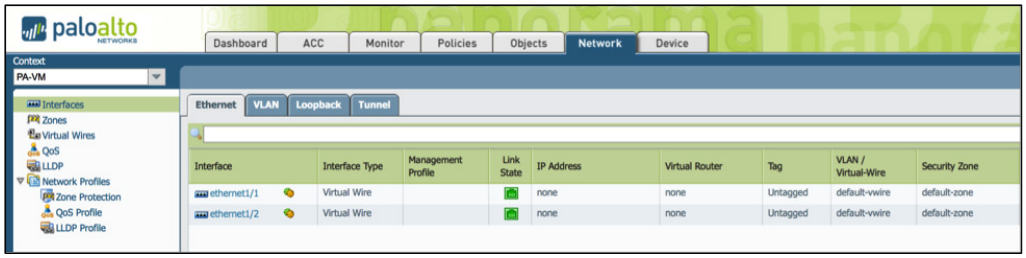

Figure 9: VM-Series uses two internal ports in virtual wire mode to process traffic from NSX

The VM-Series is connected to the back end system (for traffic processing) by the NetX API. As shown in Figure 9, internally, two data ports (i.e., ethernet1/1 and ethernet1/2) are configured in virtual wire mode to receive and transmit packets from guest VMs. Those interfaces are not visible from the vCenter UI (VM-Series summary page), and they use the NetX data plane API to communicate with the hypervisor. Traffic redirection to the VM-Series occurs through an internal construct using hypervisor-based memory sharing space (VMCI).

Figure 10 shows traffic redirection to the VM-Series using NetX data plane API. Note that traffic originated from a guest VM is steered to the VM-Series before reaching the virtual switch. The real benefit is the opportunity to protect the traffic at the earliest stage (closest to the source), before packets even reach the logical network wire.

The VM-Series exposes only one visible vNIC to vCenter: the management interface. This interface is used for management purposes only. The IP address assigned to this vNIC (and defined during the service deployment phase) must be reachable by Panorama. The VM-Series will use this interface to retrieve license information from Panorama. Panorama will communicate to the VM-Series through this interface for provisioning and signature/firmware updates.

DFW-to-VM-Series Traffic Steering Considerations

The virtual data center is at the heart of enterprise business, as it hosts strategic data for daily operations. There are many data flows traversing the data center, and they fall into four categories:

- North-south traffic flowing into and out of the data center.
- East-west traffic flowing from VM-to-VM, including inter-tier and intra-tier traffic.
- Storage and backup traffic, including network storage access from hypervisors (e.g., NFS, iSCSI, FCOE) and data backup for archive.
- Management traffic required for administration and maintenance tasks on servers (and other devices in the data center), typically a very small amount of traffic, but critical as it allows for remote management.

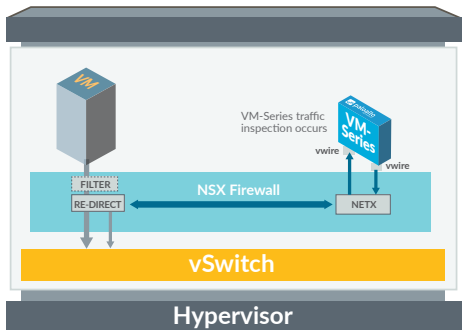

Figure 10: Traffic redirection to VM-Series using NetX data plane API

The VM-Series firewall supports up to 4 Gbps of firewall throughput (App-ID™ application identification technology enabled) per ESXi host and, as such, a common question that arises is how best to quantify the traffic to be inspected, in order to accurately size virtual data center appliances and correctly engineer traffic redirection to the VM-Series for Layer 7 analysis and inspection.

It is important to note that the 4 Gbps throughput number is per ESXi host, and aggregated throughput scales linearly with the total number of ESXi hosts in the cluster.

For instance, if the cluster contains up to 16 ESXi hosts (maximum of 32 hosts with vSphere version 6.0); then the total firewall throughput is 64 Gbps (up to 128 Gbps in the case of vSphere 6.0).

This linear increase provides flexibility in terms of server design and implementation: if an ESXi host redirects up to 4 Gbps of data traffic to its local VM-Series, it is very easy to deploy additional hosts in the cluster and evacuate VMs to offload traffic to the newly deployed VM-Series. For this task, VMware vMotion is fully supported with the joint solution integration, meaning no traffic disruption or downtime during the VM evacuation phase.

To address the 4 Gbps capacity question, Palo Alto Networks used NetFlow to analyze a customer's virtual data center traffic for approximately one month. The environment analyzed had the following characteristics:

- Medium-sized company with 1,500 employees

- 400 virtual machines
  - Linux® and Windows®
  - Lync, SAP, DNS, DHCP, AD
- 22 physical ESXi hosts
  - Each with redundant 10 Gbps physical connections
  - 10 Gbps internet connection

Based on these characteristics, the maximum theoretical network connectivity is 440 Gbps. This is obtained by taking all ESXi (22) multiplied by the number of NICs per host (2) multiplied by NIC bandwidth capacity (10 Gbps).

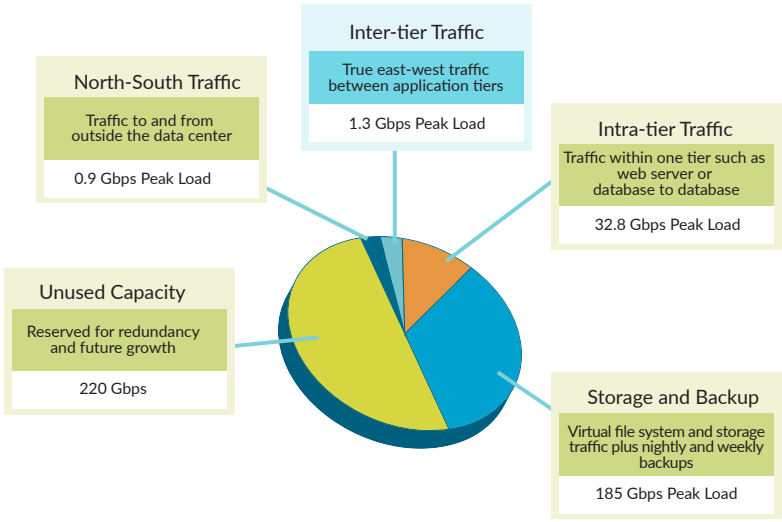

Figure 11: Peak traffic flow analysis by category

As displayed by the light blue box in Figure 11, the key outcome of the traffic analysis showed that the total inter-tier traffic that would be inspected by the VM-Series was 1.3 Gbps. Additional analysis showed the following traffic breakdown:

- Unused capacity represents 50 percent of maximum theoretical network connectivity, or 220 Gbps. This unused capacity is reserved for redundancy and future growth.
- Storage and backup represent the largest traffic amount in the virtual data center with 185 Gbps peak load. This traffic accounts for virtual file system and storage traffic, plus nightly and weekly backups.
- North-south traffic (traffic to and from outside the data center) was measured with a 0.9 Gbps peak load.
- East-west traffic has a total of 34.1 Gbps peak load and is broken down as follows:
  - 32.8 Gbps peak load for intra-tier traffic (traffic within same tier)
  - 1.3 Gbps peak load for inter-tier traffic (traffic between tiers)

The VM-Series is designed for classification and inspection of inter-tier traffic, which is a subset of the total traffic traversing the virtual environment. Figure 12 divides the inter-tier traffic by the number of total ESXi hosts, resulting in a firewall utilization per host of 60 Mbps: 1300 Mbps/22 hosts = 60 Mbps per host.

Based on the traffic analysis and the elasticity of the solution, the 4 Gbps of VM-Series firewall throughput is more than enough to support current and future NSX and Palo Alto Networks joint solution deployments.

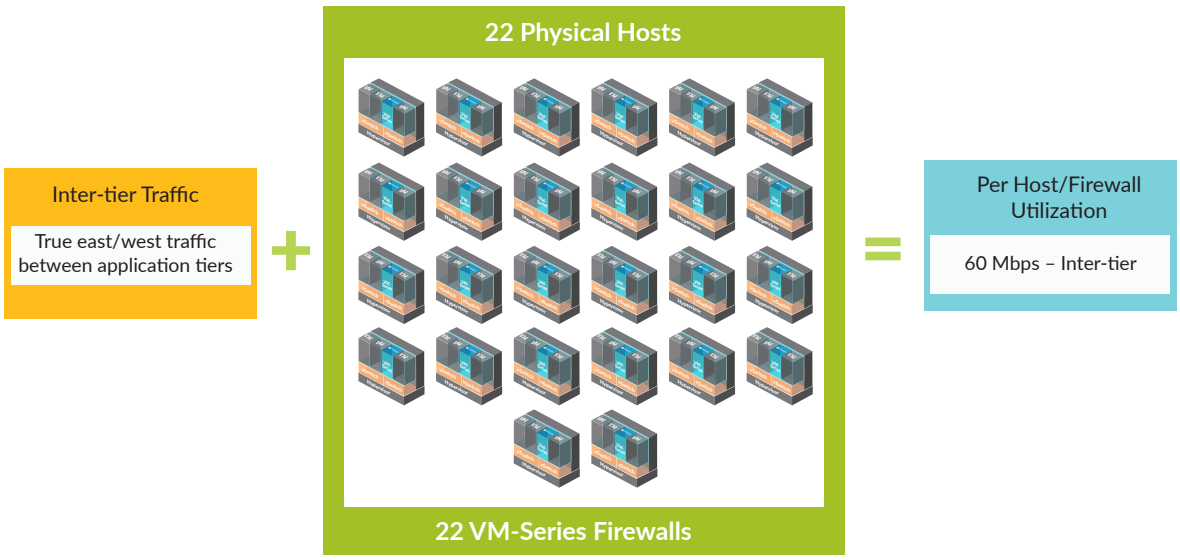

Figure 12: Inter-tier traffic per host

Conclusion

VMware and Palo Alto Networks have developed an integrated solution that fulfills the requirements of modern security in a virtual data center environment. The joint solution leverages multiple aspects: automation for VM-Series deployment via NSX; data exchange between NSX Manager and Panorama to dynamically drive security policy updates based on workload activity (creation/deletion of VM and associated IP addresses); and traffic redirection via the DFW to steer VM-to-VM traffic to the VM-Series for classification and inspection. Together, the NSX DFW and the VM-Series are fully complementary, working together to protect traffic in the virtual data center through a combination of micro-segmentation and malware prevention. Ideally, the DFW is used for intra-tier traffic protection, and the VM-Series is used for inter-tier traffic – a subset of overall traffic.

Useful resources:

- To deploy the joint solution integration, please refer to the following installation guide: https://www.paloaltonetworks.com/documentation/70/virtualization/virtualization.html
- Next-Generation Security with VMware NSX and Palo Alto Networks VM-Series technical white paper: https://www.paloaltonetworks.com/resources/whitepapers/vm-series-integration-technical-whitepaper.html
- Next-Generation Data Center Security Implementation Guidelines: https://www.paloaltonetworks.com/resources/whitepapers/next-generation-datacenter-security-implementation-guidelines.html
- Securing the Virtualized Data Center with Next-Generation Firewalls: https://www.paloaltonetworks.com/resources/whitepapers/securing-your-virtualized-data-center-with-next-generation-firewalls.html

Appendix: Prerequisites and Additional Resources

The VMware NSX with Palo Alto Networks VM-Series joint solution has been available since NSX version 6.0 and PAN-OS®/Panorama version 6.0. The table below lists all required components and minimum software versions.

Component	Minimum Software Version
NSX Manager	6.0
vSphere	5.5
Panorama	6.0
VM-Series (PAN-OS)	6.0

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