



# Next Generation Security with VMware® NSX and Palo Alto Networks® VM-Series

TECHNICAL WHITE PAPER

## Summary of Contents

Introduction .....	3
Intended Audience and purpose of document. ....	3
Solution Overview. ....	3
VMware NSX Network Virtualization Platform Overview. ....	3
Palo Alto Networks Next Generation Firewall Overview .....	5
NSX Architecture Components .....	6
VMware NSX Architecture. ....	6
Data Plane. ....	6
Control Plane .....	6
Management Plane. ....	6
Consumption Platform .....	6
Functional Services of NSX for vSphere. ....	6
NSX Distributed Firewalling .....	7
Network Isolation. ....	7
Network segmentation. ....	7
Palo Alto Networks Solution Components .....	8
How VMware NSX and Palo Alto Networks Integrate .....	9
Advanced Security Service Insertion, Chaining and Steering .....	9
Panorama service registration and VM-Series deployment. ....	9
Service Composer/Security Groups and Dynamic Address Group .....	10
Traffic Steering .....	12
VMware NSX and Palo Alto Networks Use Cases .....	13
Use-Case 1: VXLAN Segmentation With Advanced Protection Across Tiers .....	13
Use-Case 2: Micro-Segmentation of a Multi-Tiered Application with Malware Protection .....	16
Use-Case 3: Enterprise Multi Zones Security (PCI, Production and Development Zones) .....	18
Use-Case 4: Scale In / Scale Out for Elastic Applications .....	19
Traffic Visibility and Operational Efficiency .....	21
Solution Benefits .....	23
Conclusion .....	24
References .....	24

## Introduction

This document is targeted at virtualization, security, and network architects interested in deploying Cloud and Software Defined Data Center (SDDC) architectures based on VMware® network virtualization solutions with Palo Alto Networks® next-generation firewalls and services.

VMware pioneered the Software Defined Data Center (SDDC) to transform data center economics and to increase business agility. The SDDC is rooted in virtualization and is defined by three pillars server virtualization, storage virtualization and network virtualization. Although server virtualization has enabled organizations to speed application deployment and reduce data center costs, applications also need fast provisioning of networking and security services including support for mixed trust level workloads to optimize infrastructure resources without compromising security.

VMware and Palo Alto Networks have collaborated on an integrated solution to enable companies to realize the full potential of the Software Defined Data Center while providing protection against potential vulnerabilities. The joint solution addresses current challenges faced by data centers including:

- Lack of visibility into East-West (VM-to-VM) traffic
- Manual, process-intensive networking configurations to deploy security within the virtualized environment
- Security not keeping pace with speed of server provisioning
- Incomplete or irrelevant feature sets within virtualized network security platforms

VMware NSX network virtualization platform provides the network virtualization pillar of the SDDC. Using the VMware NSX platform's extensible service insertion and service chaining capabilities, the virtualized next-generation firewall from Palo Alto Networks is automatically and transparently deployed on every ESXi server. Context is shared between VMware NSX and Palo Alto Networks centralized management platform, enabling security teams to dynamically apply security policies to virtualized application creation and changes. This is accomplished while maintaining the separation of duty between security and virtualization/cloud IT administrators.

The integrated solution provides several benefits:

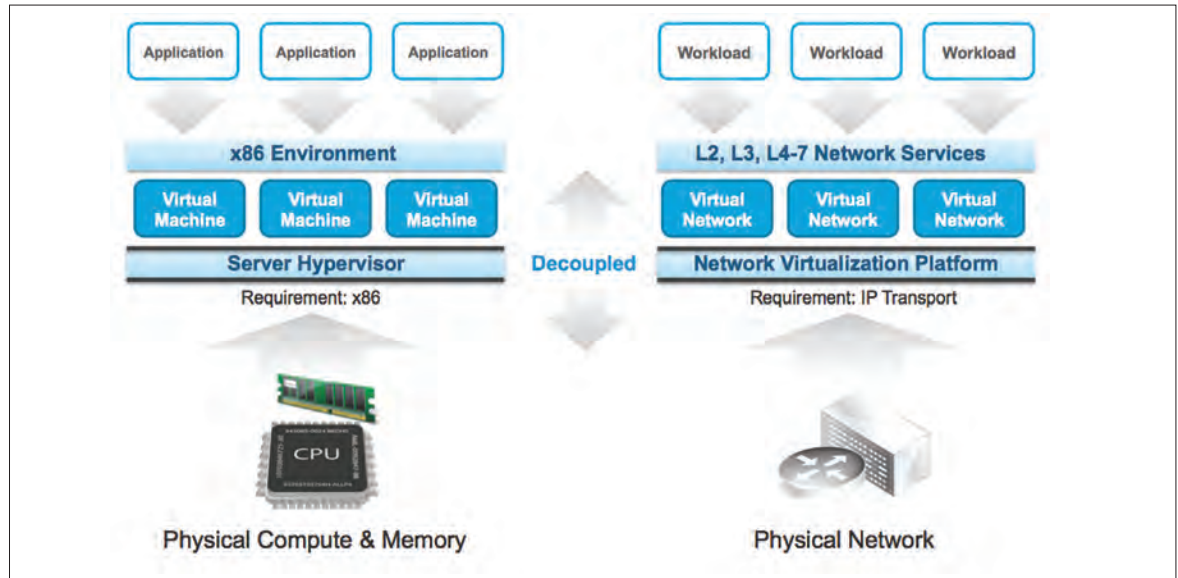
- **Better security** – enterprises can automate the delivery of Palo Alto Networks next-generation security features including visibility, safe application enablement and protection against known and unknown threats to protect their virtual and cloud environments. Dynamic network security policies stay in sync with virtual application changes
- **Operational flexibility** – next-generation security capabilities are deployed in an automated, transparent manner without manual, operational complexities
- **Accelerated deployments of business-critical applications** – enterprises can provision security services faster and utilize capacity of cloud infrastructures—more efficiently to deploy, move and scale their applications without worrying about security

## VMware NSX Network Virtualization Overview

VMware's vision of the SDDC leverages virtualization technologies to drive economic benefits including greater business responsiveness and improved cost efficiencies in the data center.

NSX is the functional equivalent of a “network hypervisor” and reproduces the complete set of L2-L7 services, (e.g., switching, routing, access control, firewalling, QoS, and load balancing) in software. As a result, these services can be programmatically assembled in any arbitrary combination—to produce unique, isolated virtual networks in a matter of seconds. In much the same way that server virtualization programmatically creates, snapshots, deletes and restores software-based virtual machines (VMs), NSX creates, snapshots, deletes, and restores software-based virtual networks. Just as VMs are independent of the underlying x86 platform and allow IT to treat physical hosts as a pool of compute capacity, virtual networks are independent of the underlying IP network hardware and allow IT to treat the physical network as a pool of transport capacity that can be consumed and repurposed on demand. Unlike legacy architectures, virtual networks can be provisioned, changed, stored, deleted and restored programmatically without reconfiguring the underlying physical hardware or topology.

By delivering a completely new operational model for networking, NSX transforms networking economics allowing data center managers to achieve orders of magnitude better agility and economics, and a vastly simplified operational model for the underlying physical network. With the ability to be deployed on any IP network, including both existing traditional networking models and next generation fabric architectures from any vendor, NSX is a completely non-disruptive solution. In fact, with NSX, the physical network infrastructure you already have is all you need to deploy a Software Defined Data Center.



**Figure 1:** Compute and Network Virtualization Parallels

Figure 1 draws an analogy between compute and network virtualization. With server virtualization, a software abstraction layer (server hypervisor) reproduces the familiar attributes of an x86 physical server (e.g., CPU, RAM, Disk, NIC) in software, allowing them to be programmatically assembled in any arbitrary combination to produce a unique virtual machine (VM) in a matter of seconds.

NSX includes firewalling capability to provide inherent isolation, security and network segmentation. Because each virtual network operates in its own address space, it is by default isolated from other virtual networks and the underlying physical networks. This approach effectively delivers the principle of least privilege, without requiring physical subnets, VLANs, ACLs or firewall rules. Traditional firewalling solutions suffer from performance choke points and increased network capacity costs due to the need for hair-pinning and multiple hops to route traffic through essential network services. Increased East-West traffic in a data center exacerbates this problem. NSX has been architected for performance at scale and avoids the security and service blind spots that result when data center operators deploy risky routing schemes to avoid hair-pinning.

NSX is natively extensible to provide third party best-of-breed solutions. Its distributed services framework and service insertion capability allows ecosystem partners to integrate advanced services at multiple points in the logical service chain. A powerful traffic steering capability allows any combination of network and security services to be chained together in the order defined by application policies, for every application workload. NSX distributes partner services to every hypervisor, making the partner service available locally to virtual machines at runtime.

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.

## Palo Alto Networks Next-Generation Firewall Overview

Fundamental shifts in application usage, user behavior, and network infrastructure have resulted in an evolved threat landscape that has exposed weaknesses in traditional port-based firewall protection. Users are accessing an increasing number of applications with a wide range of device types, often to get their job done, yet with little regard to the business or security risks. Meanwhile, data center expansion, network segmentation, virtualization and mobility initiatives are forcing organizations to re-think how to enable access to applications and data, yet protect the network from a new, more sophisticated class of advanced threats that are adept at evading traditional security mechanisms.

Historically organizations were left with two basic choices: either block everything in the interest of network security or enable everything in the interest of business. These choices left little room for compromise. Palo Alto Networks pioneered the next-generation firewall to enable organizations to accomplish both objectives—safely enable applications while protecting against both known and unknown threats.

Unique to the Palo Alto Networks enterprise security platform is the use of a positive control model that allows security IT administrators to enable specific applications or functions and block all else (implicitly or explicitly). The safe application enablement and positive control model uses the following approach:

- **Classify all traffic, across all ports, all the time** – Today, applications and the associated content can easily bypass a port-based firewall using a variety of techniques. The Palo Alto Networks enterprise security platform addresses the traffic classification visibility limitations that plague port-based security by natively applying multiple classification mechanisms to the traffic stream as soon as the platform sees it, to determine the identity of the applications traversing your network and if they are carrying any threats or malware. All traffic is classified regardless of port, encryption (SSL or SSH) or evasive techniques employed. Unidentified applications, typically a small percentage of traffic, yet high in potential risk, are automatically categorized for systematic management.
- **Reduce the threat footprint, prevent known threats** – Once the traffic is fully classified, organizations can protect their network from a range of cyber attacks by allowing only the applications required for the business and inspecting the content for exploits, malware, dangerous files or content. Intrusion Prevention System (IPS) capabilities block network and application-layer vulnerability exploits, buffer overflows, DoS attacks, and port scans. Antivirus/ Anti-spyware protection blocks millions of malware variants, including those hidden within compressed files or web traffic (compressed HTTP/HTTPS) as well as known PDF viruses. For traffic that may be encrypted with SSL, policy-based decryption can be selectively applied and traffic inspected for threats, regardless of port. Threat prevention capabilities goes beyond simply blocking malicious content to include the control of specific file types by policy, as well as inspecting traffic for specific content to prevent data loss
- **Prevent unknown threats** – Custom or otherwise unknown threats, such as custom or polymorphic malware, are increasingly used in modern cyberattacks. Unknown threats is analyzed and identified via WildFire technology by executing unknown files and directly observing their malicious behavior in a sandbox environment. If new malware is discovered, a signature for the infecting file and related malware traffic is automatically generated and delivered in as little as 30 minutes. All major file types are supported by WildFire including: PE files; Microsoft Office .doc, .xls, and .ppt; Portable Document Format (PDF); Java Applet (jar and class); and Android Application Package (APK).

Unlike traditional blade or UTM architectures that notoriously introduce performance penalties for each feature that is enabled due to repeatedly processing traffic for each blade or feature. Palo Alto Networks designed a unique approach that performs all networking, policy lookup, application identification and code, and signature matching for any and all threats and content once. This means that performance remains steady even as additional threat prevention features are enabled.

# NSX Architecture Components

## VMware NSX Virtual Components

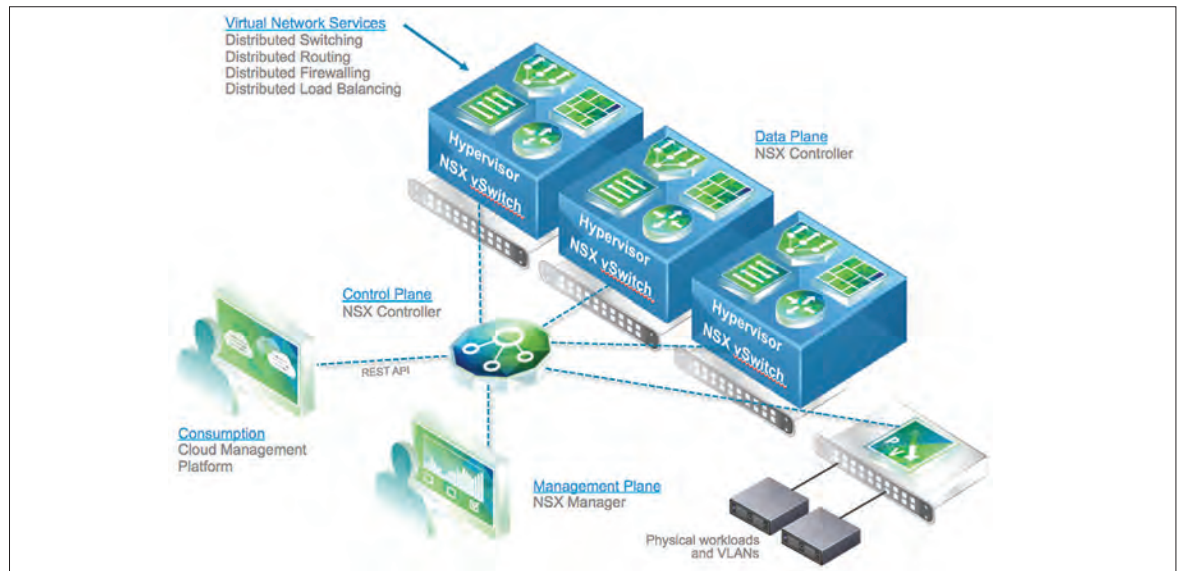


Figure 2: VMware Network Virtualization Solution Components

## Consumption Platform

Typically end-users tie in network virtualization to their cloud management platform for deploying applications. NSX provides a rich set of integration points into virtually any CMP via the REST API. In a vSphere environment NSX is integrated with the vSphere Web UI itself providing out of the box experience for deployment and consumption of the services.

## Management Platform

The NSX management plane is built by the NSX manager. The NSX manager provides the single point of configuration and exposes REST API entry-points

## Control Plane

The NSX control plane enables multicast-free VXLAN, control plane programming of distributed logical router. The control plane is managed centrally through the NSX controller. The controller is highly resilient and failure-tolerant, and runs independent of data path which runs under VDS.

## Data Plane

The NSX data plane consists of the NSX vSphere Distributed Switch (VDS) with add-on components such as distributed routing, distributed firewall and VXLAN bridging support. These services run as kernel modules (VIBs) providing scalable and line rate performance. The NSX vSwitch (VDS) abstracts the physical network and provides access-level switching in the hypervisor. Key functions which are central to network virtualization and enable decoupling of logical networks from the underlying physical components include:

- o VXLAN protocol-based support for overlay networks and centralized network configuration. Overlay networking enables extension of a layer 2 (L2) segment anywhere in the fabric without physical network design constraints
- o Distributed L3 Routing – Optimizes the forwarding of logical network segments (East-West) traffic while maintaining isolation between tenants.

- o Distributed Firewall – Security enforcement is done at the kernel and vNIC level itself. This enables firewall rule enforcement in a highly scalable manner without creating bottlenecks onto physical appliances. The firewall is distributed in kernel allowing minimal CPU overhead and line rate performance.
- o Traditional network features – such as Port Mirroring, NetFlow/IPFIX, Configuration Backup and Restore, Network Health Check, QoS, and LACP.
- o Logical Load-balancing – Support for L4-L7 load balancing

## NSX Distributed Firewalling

The VMware NSX platform includes distributed kernel-enabled firewalling with line-rate performance, virtualization and identity aware with activity monitoring, among other network security features native to network virtualization.

### Network Isolation

Isolation is the foundation of most network security, whether for compliance, containment or simply keeping development, test and production environments from interacting. Traditionally VRF (virtual route forwarding), access control lists (ACLs), physically separated stacks (network & compute) and physical firewall rules/contexts have been used to establish and enforce isolation; in network virtualization, virtual networks are isolated from any other virtual network and from the underlying physical network by default, delivering the security principle of least privilege. Virtual networks are created in isolation and remain isolated unless specifically connected together. No physical subnets, no VLANs, no ACLs, no firewall rules are required to enable this isolation.

Any isolated virtual network can be made up of workloads distributed anywhere in the data center. Workloads in the same virtual network can reside on the same or separate hypervisors. Additionally, workloads in several multiple isolated virtual networks can reside on the same hypervisor. Case in point, isolation between virtual networks allows for overlapping IP addresses, making it possible to have isolated development, test and production virtual networks, each with different application versions, but with the same IP addresses, all operating at the same time, all on the same underlying physical infrastructure.

Virtual networks are also isolated from the underlying physical infrastructure. Because traffic between hypervisors is encapsulated, physical network devices operate in a completely different address space than the workloads connected to the virtual networks. For example, a virtual network could support IPv6 application workloads on top of an IPv4 physical network. This isolation protects the underlying physical infrastructure from any possible attack initiated by workloads in any virtual network, independent from any VLANs, ACLs, or firewall rules that would traditionally be required.

### Network segmentation

Network isolation is between discrete entities. Network segmentation applies to homogeneous entities, e.g. protection within a group or three-tier application. Traditionally, network segmentation is a function of a physical firewall or router, designed to allow or deny traffic between network segments or tiers. For example, segmenting traffic between a web tier, application tier and database tier. Traditional processes for defining and configuring segmentation are time consuming and highly prone to human error, resulting in many security breaches. Implementation requires deep and specific expertise in device configuration syntax, network addressing, application ports and protocols.

Network segmentation, like isolation, is a core capability of VMware NSX network virtualization. A virtual network can support a multi-tier network environment, meaning multiple L2 segments with L3 segmentation or micro-segmentation on a single L2 segment using distributed firewall rules. In a virtual network, network services (L2, L3, ACL, Firewall, QoS, etc.) that are provisioned with a workload are programmatically created and distributed to the hypervisor vSwitch. Network services, including L3 segmentation and firewalling, are enforced at the virtual interface.

Isolation and segmentation requires identifying application flows and enforcing security policies, which can be created programmatically or using a template-based process. Integrating the virtual isolation and segmentation



with physical firewall functions and workflow has been the Achilles' heel of securing virtual data centers. This integration with Palo Alto Networks physical and virtual next-generation firewall services with the NSX native security capabilities allows cloud administration a powerful method to manage the risk associated with integration between physical and virtual domain.

## Palo Alto Networks Solution Components

The Palo Alto Networks VM-Series and NSX integrated solution includes Panorama and the VM-Series next-generation firewall. The following are key elements of the solution:

- **VM-Series Firewall** — The VM-Series firewall is a next-generation firewall in virtual form factor that extends safe application enablement to virtualized and cloud environments using the same PAN-OS feature set available in hardware firewalls. This means when applied to a virtualized and cloud environment, Palo Alto Networks can determine the exact identity of the applications traffic traversing from VM to VM using App-ID technology. Coordinated threat protection can then be applied to the allowed traffic, blocking known malware sites, preventing vulnerability exploits, viruses, spyware and malicious DNS queries using Content-ID technology. Custom or otherwise unknown malware found in the applications on the network is analyzed and identified by executing the files and directly observing their malicious behavior in a sandbox environment via WildFire. If new malware is discovered, a signature for the infecting file and related malware traffic is automatically generated in as little as 30 minutes.
- **Dynamic Address Groups** — In a virtualized and cloud environment where virtual machines often change functions and can move from server to server, building security policies based on static IP addresses alone can have limited value. The Dynamic Address Groups feature in PAN-OS 6.0 allows you to create policies using tags as an identifier for virtual machines instead of a static object definition. Multiple tags representing virtual machine attributes such as IP address and operating system can be resolved within a Dynamic Address Group, allowing you to dynamically apply policies to virtual machines as they are created or travel across the network.
- **Panorama Centralized management** — Security appliances in a virtual and cloud environment should be managed in the same consistent manner as physical security appliances. Panorama enables you to centrally manage the process of configuring devices, deploying security policies, performing forensic analysis, and generating reports across your entire network of next-generation firewalls. Panorama automatically registers the Palo Alto Networks VM-Series as a service to NSX. Once the service is registered, it can be deployed to one or more clusters. Each host on the cluster will automatically have a VM-Series firewall deployed, licensed, registered, and configured.

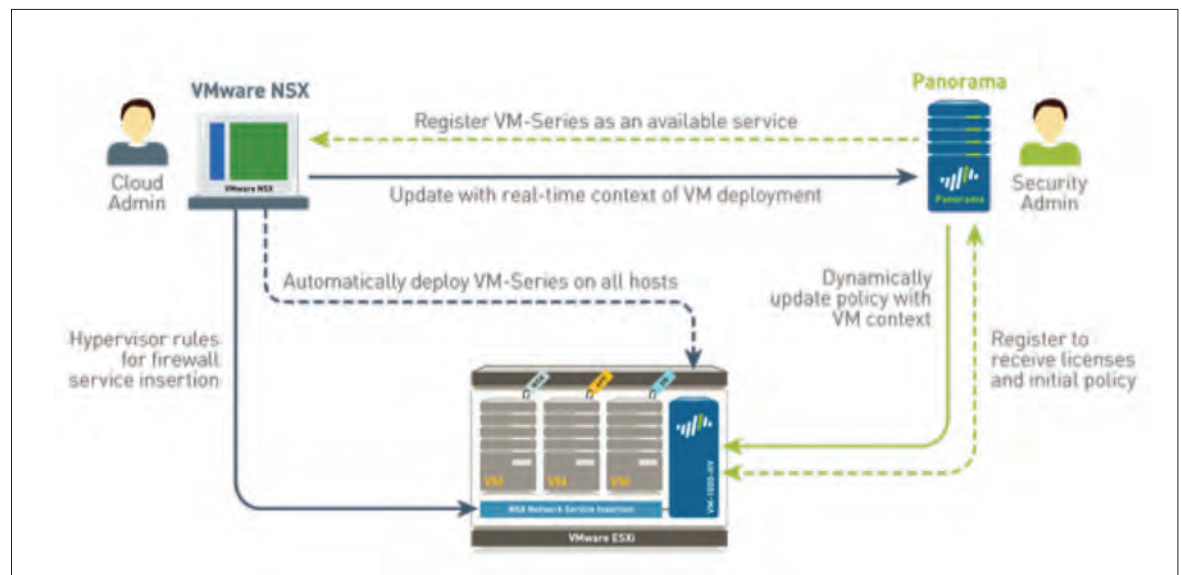


Figure 3: Palo Alto Networks Solution Components



## How the Integrated VMware NSX and Palo Alto Networks VM-Series Solution Works

### Advanced Security Service Insertion, Chaining and Steering

VMware NSX network virtualization platform provides L2-L4 stateful firewalling features to deliver segmentation within virtual networks. Environments that require advanced, application-level network security capabilities can leverage VMware NSX to distribute, enable and enforce advanced network security services in a virtualized network context. NSX distributes network services into the VM vNIC to form a logical pipeline of services applied to virtual network traffic. The Palo Alto Networks VM-Series firewall integrates directly into this logical pipeline, enabling visibility and safe enablement of VM traffic, along with safe enablement of applications and complete threat protection.

Another powerful benefit of the integrated NSX and Palo Alto Networks solution is the ability to build policies that leverage NSX service insertion, chaining and steering to drive service execution in the logical services pipeline, based on the result of other services, making it possible to coordinate otherwise completely unrelated network security services from multiple vendors.

#### Version requirements

VMware NSX and Palo Alto Networks integration work with the following versions:

- PAN-OS 6.0 (Panorama and VM-Series)
- ESXi 5.1 or 5.5
- vCenter 5.5
- NSX Manager 6.0

### Panorama Service Registration and VM-Series Deployment

The first step in deploying the integrated solution is to define NSX manager information (IP/Hostname and credentials) under Panorama so that the Palo Alto Networks VM-Series firewall can be registered as an advanced NSX service. This registration process provides the necessary data to deploy PAN-OS as a service. The registration also allows NSX to update Panorama with dynamic changes to the SDDC.

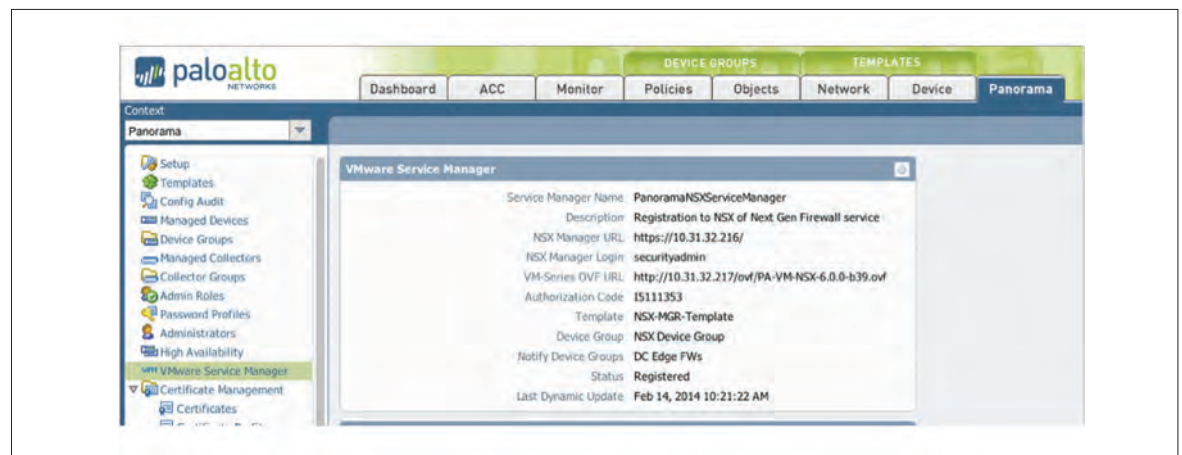


Figure 4: Panorama Registration with NSX

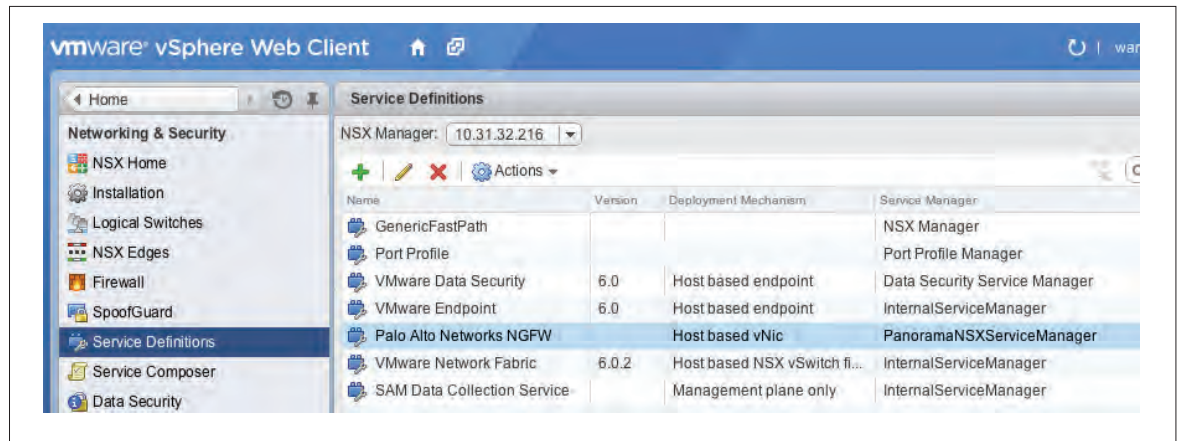


Figure 5: New Service Definition Available in NSX

The second step is to deploy the Palo Alto Networks NGFW service on each host of the cluster. Once the deployment process for a cluster is started, NSX will automatically load the defined VM-Series OVF on each host, boot the VM-Series virtual firewall, and provide the new firewall with addressing and Panorama information. Then Panorama will license each firewall and push the shared policies and configuration elements. If a cluster grows and a new host is added, these steps will automatically take place and the new host will be ready to enforce the security policy.

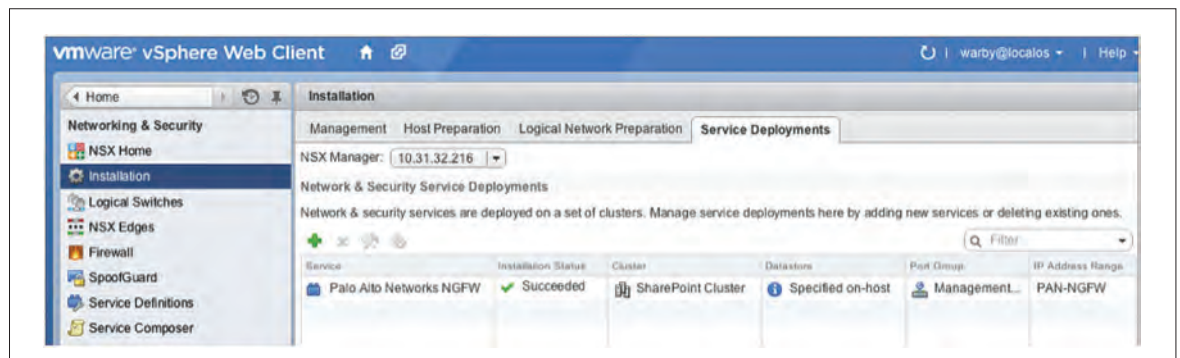


Figure 6: Palo Alto Networks NGFW Successfully Deployed

Palo Alto Networks VM-Series is instantiated with only one vNIC used for management purposes. This Interface enables communication with Panorama server to retrieve policy rule configuration and exchange real-time information such as traffic logs and policy updates.

When these two steps have been completed, the Palo Alto Networks firewall Service is ready for consumption.

## Service Composer/Security Groups and Dynamic Address Groups

The integrated NSX/Palo Alto Networks solution leverages VMware's Service Composer to create logical groups of the assets to be protected including VM, vNIC, clusters and users.

NSX and Panorama do a dynamic exchange of the protected policy objects:

When a Security Group is created under NSX, the information is transmitted to Panorama. The security administrator can then link the NSX Security Groups with Panorama Dynamic Address Groups. Then, the PAN-OS security policies are created referencing these Dynamic Address Groups.

Any virtual machine added or removed inside a Security Group is immediately reflected within Dynamic Address Group. The security policy is in effect without the need to change the configuration on the firewalls or Panorama.

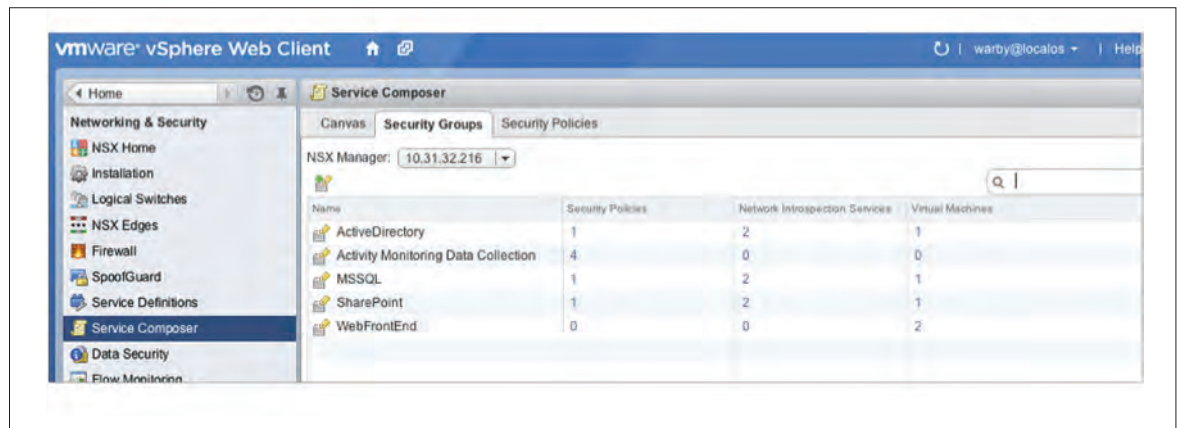


Figure 7: Defining Security Groups in NSX

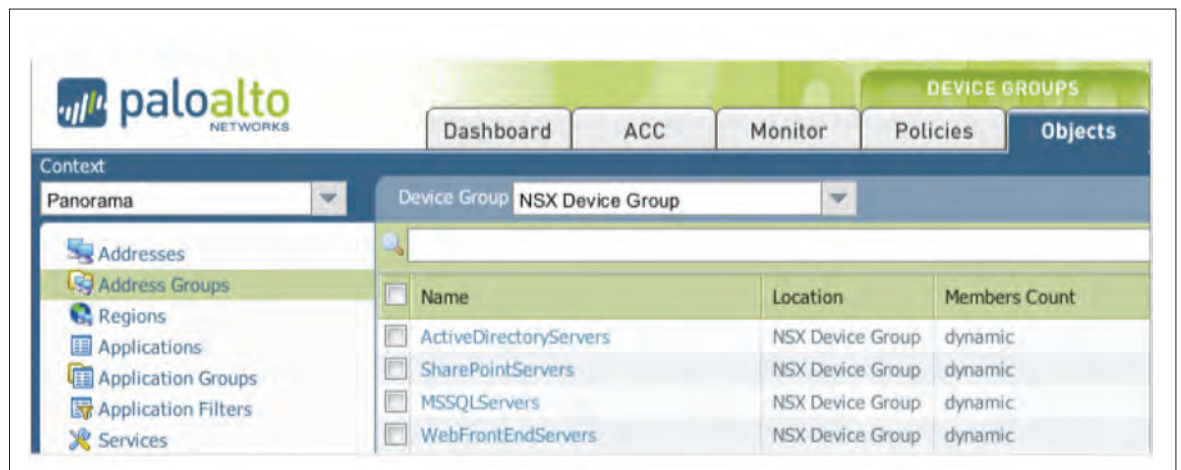


Figure 8: Creating Dynamic Address Groups in Panorama

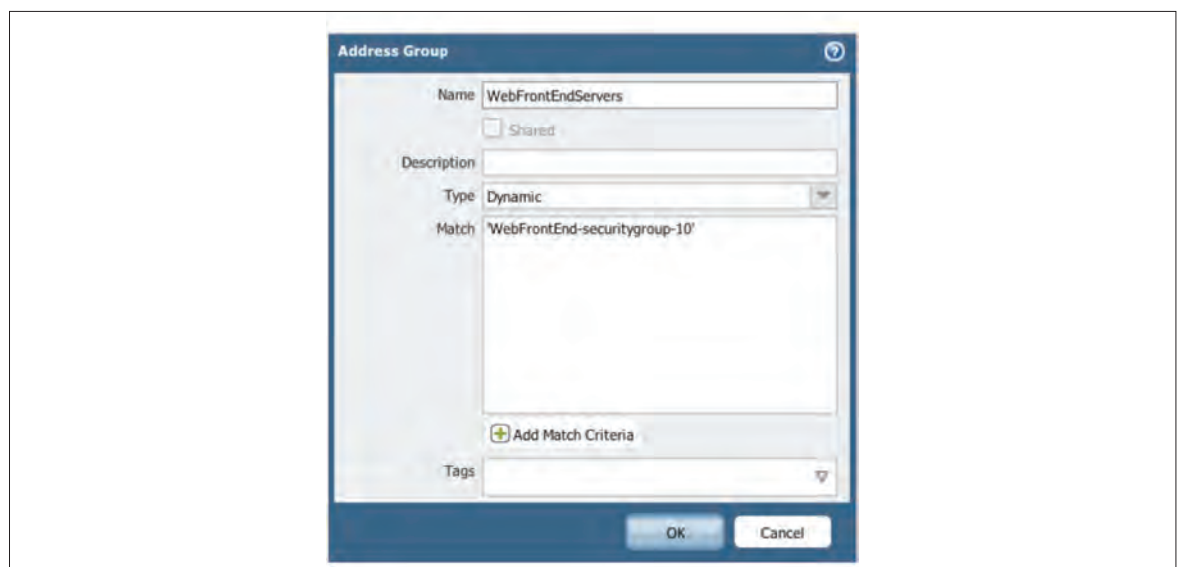
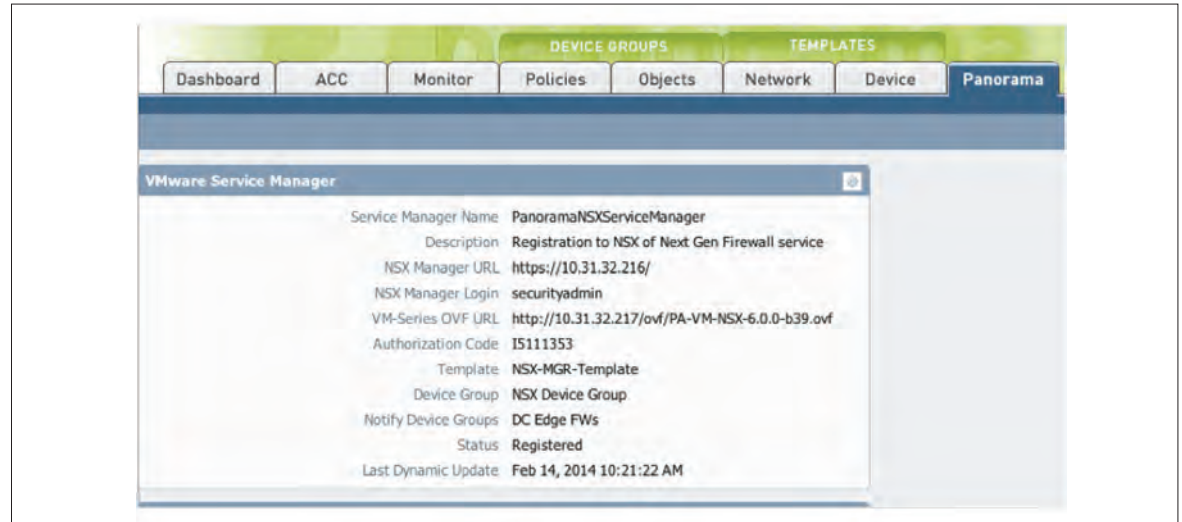


Figure 9: Mapping Dynamic Address Groups to NSX Security Groups Automatically

In addition, updates to NSX security groups can be forwarded to other Palo Alto Networks firewalls using the Notify Device Groups feature in PAN-OS. This is specified during the registration process in Panorama.



A physical data center perimeter firewall may also have Dynamic Address Groups. These Dynamic Address Groups can also be linked to the NSX security groups using the Notify Device Groups feature in Panorama. This enables the physical firewall to also dynamically enforce security policy for traffic entering the data center. As virtual machines join and leave the NSX security groups, the perimeter firewall will dynamically learn about those addresses just as the VM-Series firewalls do.

## Traffic Steering

Traffic steering from a guest VM to a Palo Alto Networks VM-Series firewall is performed internally at the hypervisor level using shared memory space. The NSX administrator specifies which DVS port-group or logical switch (VXLAN) needs to be served by the Palo Alto Networks VM-Series firewall.

Using Service Composer/Security Policy, the security team can granularly define traffic flows that will be redirected to the Palo Alto Networks VM-Series firewall for inspection and enforcement. Traffic allowed by the VM-Series Firewall is then returned to the NSX virtual switch for delivery to the final destination (guest VM or physical device).

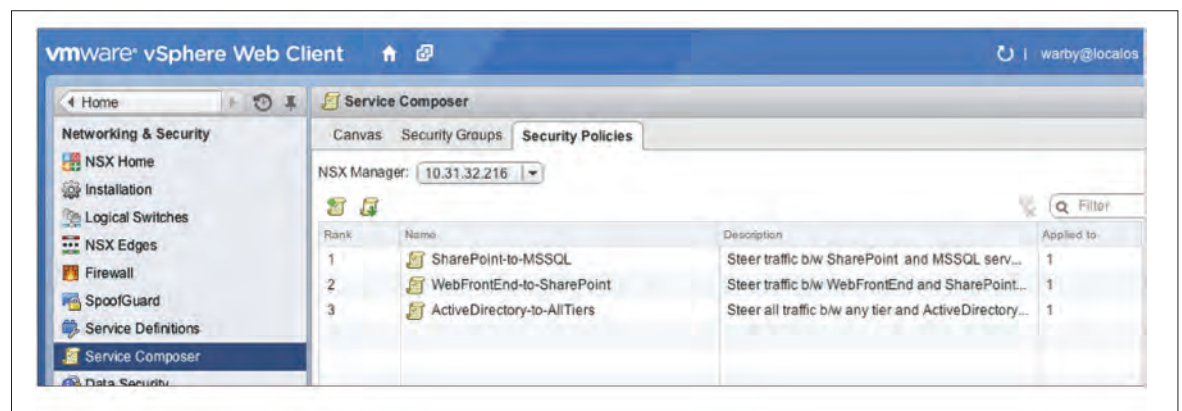
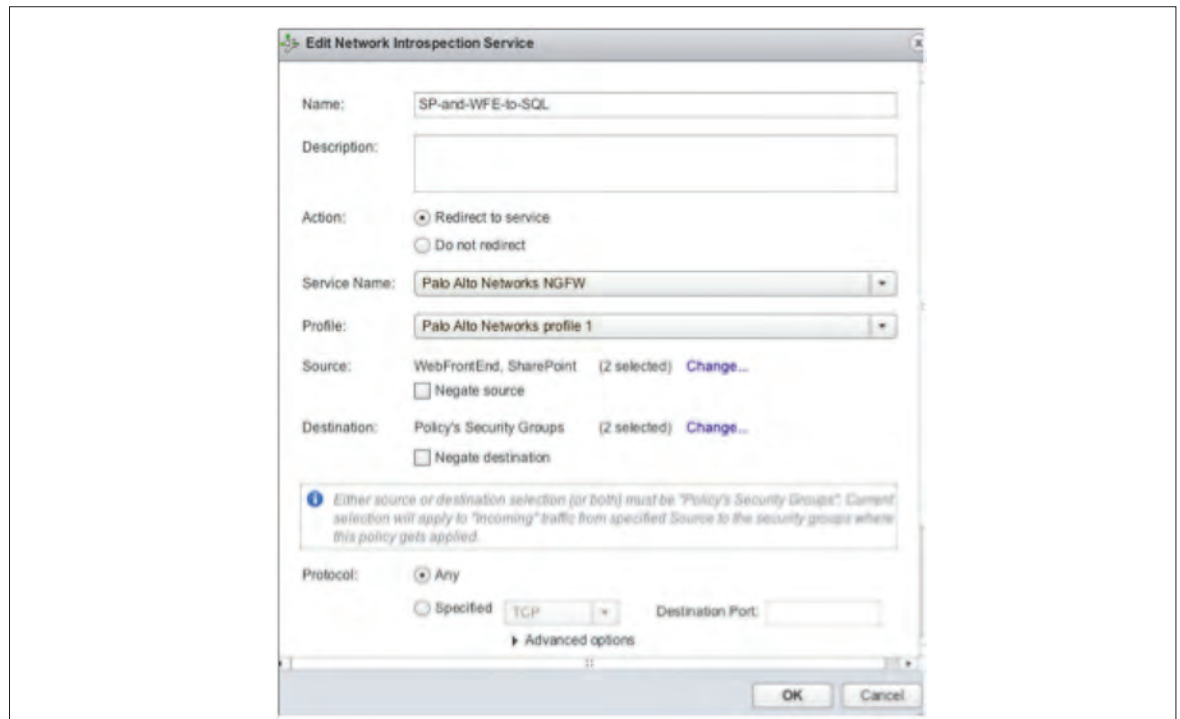


Figure 10: Sample Security Policies in NSX





**Figure 11:** Defining Traffic Steering Rules

Traffic redirection (defined within Network Introspection Service window) can be defined in the following ways:

- From Security Group (SG-1 for instance) to Security Group (SG-2 for instance)
- From ANY to Security Group (SG-1 for instance)
- From Security Group (SG-1 for instance) to ANY

ANY means any source or destination IP address respectively.

## VMare NSX and Palo Alto Networks VM-Series Integration Use Cases

### Use Case 1: VXLAN Segmentation With Advanced Protection Across Tiers

In this scenario, guest VMs are segregated using a traditional model of segmentation based on L2 domain separation:

VMs are connected to dedicated VXLAN logical switches depending on their role.

For instance, in a 3-tier application model, all web server VMs are connected to WEB logical switch (VXLAN-id 5000), application logic VMs to APP logical switch (VXLAN-id 5001) and database VMs to DB logical switch (VXLAN-id 5002).

Guest VMs can be instantiated in any ESXi host as long as VXLAN reachability is extended to these hosts (in other words clusters belong to same transport zone).

The following diagram shows a physical view of this example topology. In this topology compute cluster 1 and cluster 2 belong to the same transport zone meaning any logical switch (VXLAN-id 5000 to 5002) can be expanded to any host. Even if WEB-VM-1 and WEB-VM-2 are created on different hosts, they are connected to the same L2 domain. To enable communication between WEB, APP and DB tiers, the logical routing function of NSX is leveraged so that a single Logical Router (LR) instance connects all three logical switches.

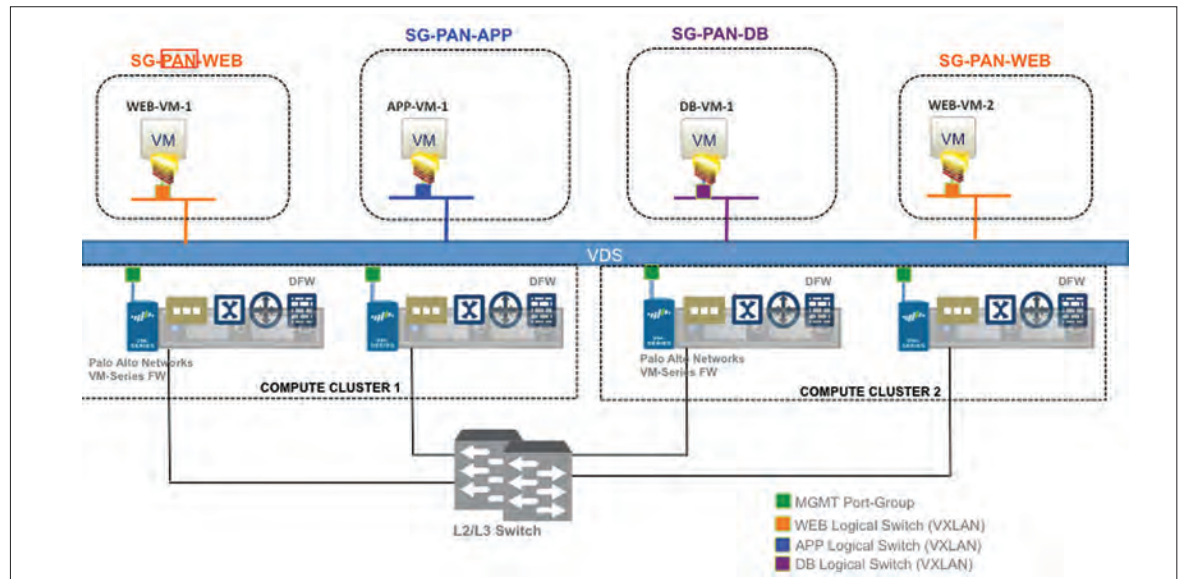


Figure 12: Physical View of Use Case 1 Topology

Notice that all ESXi hosts in this topology have been prepared (all NSX kernel modules successfully installed) so that the Distributed Firewall (DFW) module can run and operate. DFW is a NSX key element for traffic redirection to the Palo Alto Networks VM-Series firewall.

In terms of traffic steering, the following configurations will be applied:

- Traffic from INTERNET tier to WEB tier is redirected by the guest VM and processed by the VM-Series firewall.
- Traffic from WEB tier to APP tier is redirected by the guest VM and processed by the VM-Series firewall.
- Traffic from APP tier to DB tier is redirected by the guest VM and processed by the VM-Series firewall.

This list is not exhaustive and depends only on customer traffic engineering.

Once traffic reaches the Palo Alto Networks VM-Series firewall, security policies defined on Panorama will dictate the enforcement action for the identified application.

The following figure shows a logical view of traffic redirection and processing for this use case:

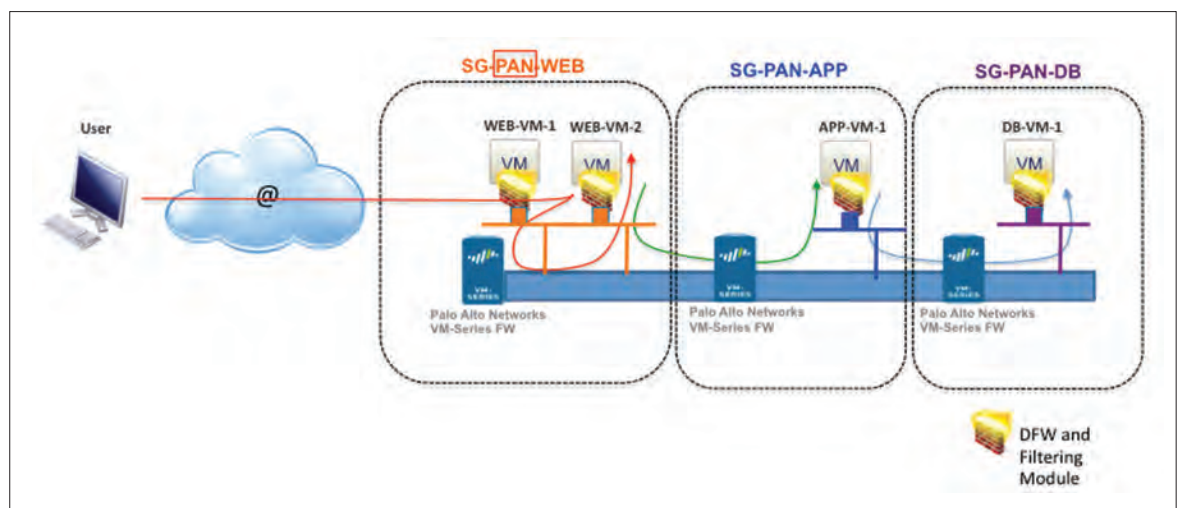


Figure 13: Logical View of Traffic Flows for Use Case 1

To implement this use case scenario, we first need to create the following Service Composer/Security Groups (SGs):

Security Group Name	Inclusion
<b>SG-PAN-WEB</b>	WEB logical switch (VXLAN-id 5000)
<b>SG-PAN-APP</b>	APP logical switch (VXLAN-id 5001)
<b>SG-PAN-DB</b>	DB logical switch (VXLAN-id 5002)

A Security Group is a very dynamic construct by nature. As defined in the above table, any VM (existing or new) connected to the WEB logical switch will automatically be part of SG-PAN-WEB. The same behavior applies for VMs connected to the APP logical switch or the DB logical switch.

Secondly, we need to configure the following Service Composer/Security Policy (SP):

Security Policy Name	Network Introspection Policy	SP Applied to	Comments
<b>SP-PAN-INTERNET-to-WEB</b>	Source: any Destination: Policy's Security Group Protocol: any Action: redirect to PAN NGFW	SG-PAN-WEB	Any traffic from INTERNET tier to WEB tier is redirected to VM-Series firewall
<b>SG-PAN-WEB-to-APP</b>	Source: SG-PAN-WEB Destination: Policy's Security Group Protocol: any Action: redirect to PAN NGFW	SG-PAN-APP	Any traffic from WEB tier to APP tier is redirected to VM-Series firewall
<b>SG-PAN-APP-to-DB</b>	Source: SG-PAN-APP Destination: Policy's Security Group Protocol: any Action: redirect to PAN NGFW	SG-PAN-DB	

Note that Security Policy allows for a more granular configuration in regard to traffic redirection:

Instead of redirecting all traffic, it is possible to define particular traffic to redirect using the TCP/UDP destination port (and optionally source port). As an example, if only HTTPS traffic needs to be redirected to the Palo Alto Networks VM-Series firewall, then use destination TCP port 443.

After completing the NSX configuration, the next step is to define Dynamic Address Group (DAG) on Panorama.

A 1:1 mapping exists between a DAG and a Security Group:

Dynamic Address Group	Security Group Name
<b>DAG-PAN-WEB</b>	SG-PAN-WEB
<b>DAG -PAN-APP</b>	SG-PAN-APP
<b>DAG -PAN-DB</b>	SG-PAN-DB



The final step is to define security policy rules on Panorama. At this level, the security administrator can define which applications are authorized or forbidden from the Internet and between the different tiers of the application.

For instance, in this use case HTTP and HTTPS are allowed at the WEB tier for traffic coming from the Internet. Message Bus applications are permitted at the APP tier and the SQL protocol is authorized at the DB tier. All other applications are by default denied.

Table below shows an example of policy rules defined on Panorama:

Source	Destination	Application	Action
Any	DAG-PAN-WEB	HTTP, HTTPS	Permit
DAG-PAN-WEB	DAG-PAN-APP	RabbitMQ	Permit
DAG-PAN-APP	DAG-PAN-DB	SQL	Permit

## Use Case 2: Micro-Segmentation of a Multi-Tiered Application with Malware Protection

In this next use case, we do not rely on traditional network constructs for segmentation (i.e guest VMs segregated per L2 domain based on their role). Using the integrated NSX and Palo Alto Networks solution, the segmentation is now independent of the network topology and the NSX Security Groups with Panorama Dynamic Address Group Objects are leveraged for segmentation and security enforcement.

For example, a customer with an application that has a web front-end tier, an application tier, and a database tier no longer needs to create three network segments. All of these tiers and VMs can exist on one flat virtual network. NSX Security Groups, which define the micro-segmentation, aligns VMs with the tiers of the application.

Steering rules can then be created in NSX Service Composer/Security Policy that redirect traffic between any of the tiers to the Palo Alto Networks VM-Series firewalls. Using Panorama Dynamic Address Groups, VM-Series security policy based on the same tiers is enforced. In this way, we can ensure for example that only SQL traffic is allowed between the application and database tier.

Figure below shows a physical view of the topology for use case 2:

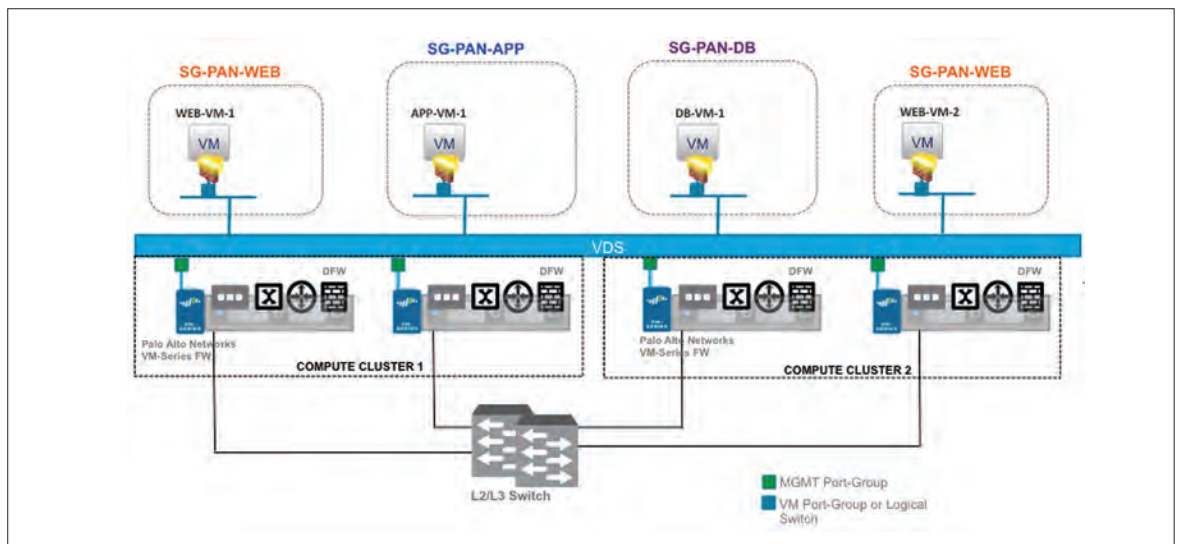
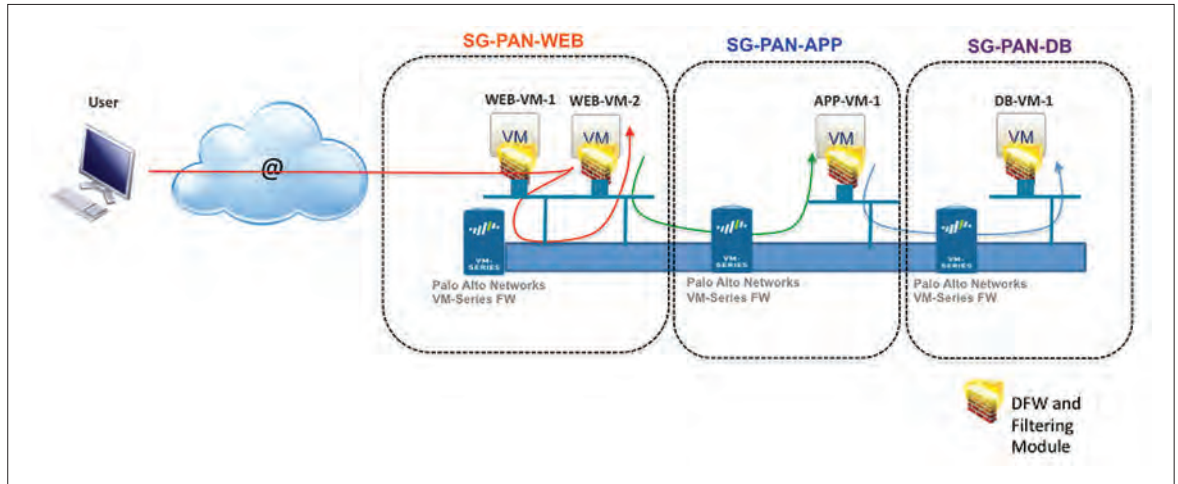


Figure 14: Physical View of Use Case 2 Topology

When inspecting traffic between these tiers, the VM-Series firewall will perform deep level packet inspection first to ensure that the application is valid and contains no threats. The VM-Series will prevent threats like viruses, botnet traffic, malware etc. from flowing between the tiers. This gives visibility and protection in the SDDC East/West traffic that isn't available on the perimeter firewall.

By leveraging the dynamic signature updates from Panorama, we can guarantee the solution is always protected with the latest threat and application databases.

The following figure shows a logical view of traffic redirection and processing for this use case:



**Figure 15:** Logical View of Traffic Flows for Use Case 2

The only difference in terms of configuration between this use case and the previous one (VXLAN segmentation) is the way Service Composer/Security Groups needs to be configured:

Security Group Name	Inclusion
SG-PAN-WEB	WEB-VM-1, WEB-VM-2
SG-PAN-APP	APP-VM-1
SG-PAN-DB	DB-VM-1

Instead of using logical switches for the inclusion field, we need to explicitly select appropriate guest VM.

Note: If using standardized guest VM naming convention, Security Group dynamic inclusion feature can be used. For instance, if all WEB VMs start with "WEB" (APP VM name start with "APP" and DB VM name start with "DB"), we can use the following Security Group definition:

Security Group Name	Inclusion (Dynamic)
SG-PAN-WEB	VM name contains "WEB"
SG-PAN-APP	VM name contains "APP"
SG-PAN-DB	VM name contains "DB"

In this case when a new WEB, APP or DB VM is instantiated using the predefined naming convention, the new VM will automatically be integrated into the corresponding Security Group, which will trigger an update to the associated Panorama Dynamic Address Group.

### Use Case 3: Enterprise Multi-Zone Security (PCI, Production and Development Zones)

In this scenario, a Software Defined Data Center (SDDC) is created with three internal zones:

- **Dev Zone:** used for developers to create, test and validate new types of enterprise applications.
- **Prod Zone:** used for all applications running under production are located in this part of the SDDC.
- **PCI Zone:** Used for VMs that require access to customer personal information and payment card identification (compliance driven environment).

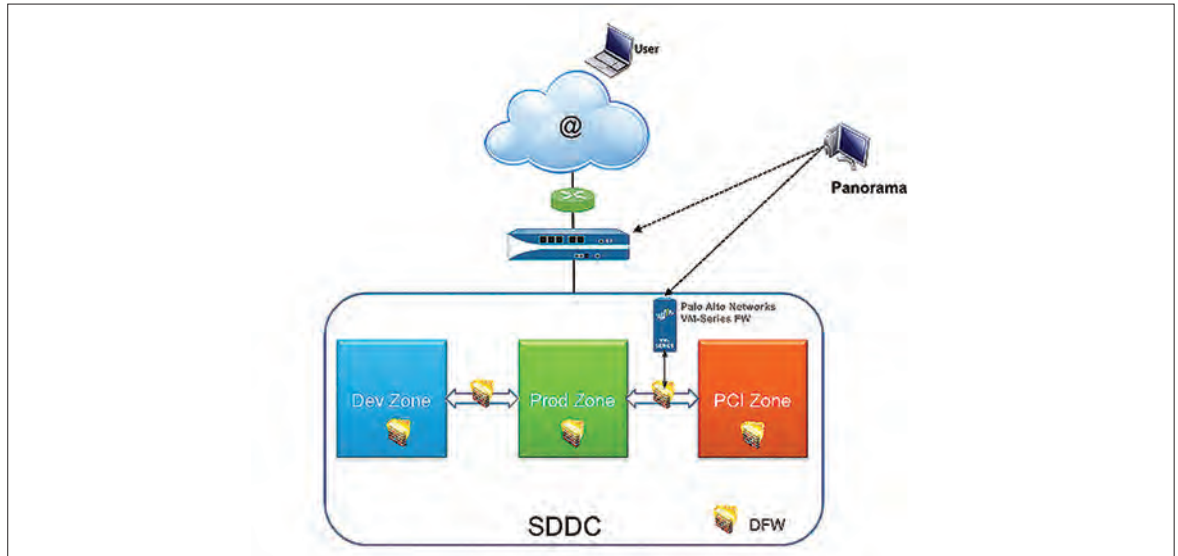


Figure 16: Multi-Zone SDDC

Traffic from Dev Zone to Prod Zone is protected by DFW. Traffic from Prod Zone to PCI Zone is redirected and enforced by the Palo Alto Networks VM-Series firewall leveraging advanced security features of PAN-OS such as IPS and malware prevention.

Palo Alto Networks provides critical functionality when dealing with PCI standard compliance. Please refer to the link in the reference section to learn more about it.

To implement this use case, we need to create the following three Security Groups:

Security Group Name	Inclusion
SG-DEV-ZONE	All logical switches used in Dev Zone (or all virtual switches port-group)
SG-PROD-ZONE	All logical switches used in Prod Zone (or all virtual switches port-group)
SG-PCI-ZONE	All logical switches used in PCI Zone (or all virtual switches port-group)

To redirect traffic between Prod Zone and PCI Zone to PAN VM-Series FW, following Security Policy can be used:

Security Policy Name	Network Introspection Policy	SP Applied to
SP-PAN-DEV-to-PROD-ZONE	Source: Policy's Security Group Destination: SG-PROD-ZONE Protocol: any Action: do not redirect	SG-DEV-ZONE
SP-PAN-PROD-to-PCI-ZONE	Source: Policy's Security Group Destination: SG-PCI-ZONE Protocol: any Action: redirect to PAN NGFW	SG-PROD-ZONE

Panorama Dynamic Address Groups are 1:1 mapped with Security Groups:

Dynamic Address Group	Security Group Name
DAG-PAN-PROD-ZONE	SG-PROD-ZONE
DAG-PAN-PCI-ZONE	SG-PCI-ZONE

Finally on Panorama, define policy rules for applications/protocols permitted or denied between Prod Zone and PCI Zone:

Source	Destination	Application	Action
DAG-PAN-PROD-ZONE	DAG-PAN-PCI-ZONE SQL, HTTPS, LDAP		Permit

## Use Case 4: Scale In / Scale Out for Elastic Applications

One major characteristic of Cloud technology is the ability to dynamically adapt to user workload: during high activity periods, an application should be able to scale out rapidly and automatically in order to absorb all end user traffic. In the same way, once activity goes back to a normal state or even to a lower state, the application should be able to scale down dynamically to save energy and resources. A common name given to this type of application is “elastic application”.

For example, let's take a 3-tier type of application with WEB, APP and DB tiers.

In case of high activity, the WEB and APP tiers should be agile enough to expand quickly without any human intervention. Once VMs are instantiated on these tiers, consistent security policy should be enforced and as such, overall systems always guarantee a high degree of protection even in case of dynamic workload creation / intrinsic application growth.

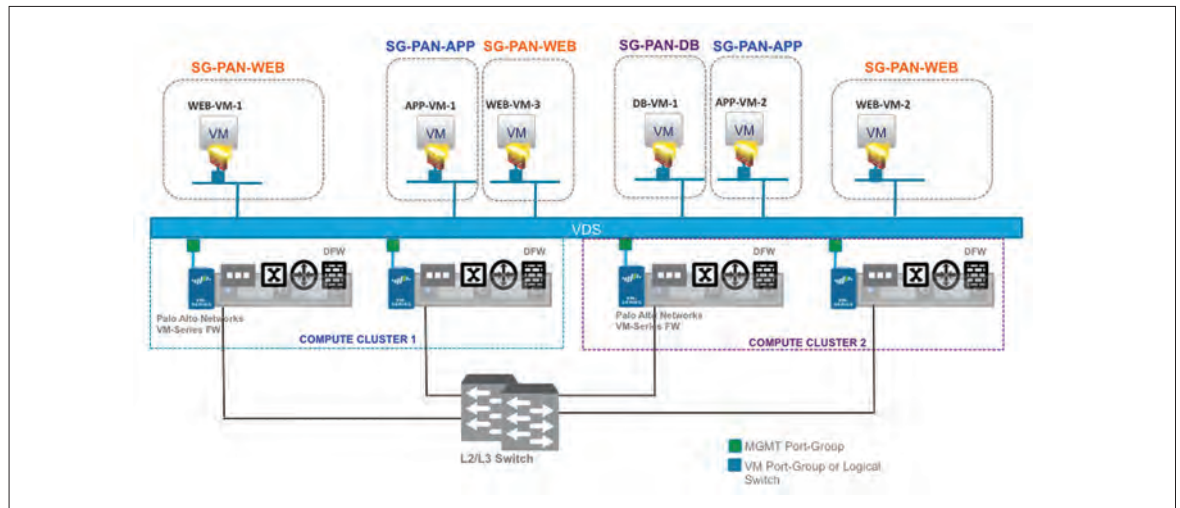
Starting with use case 2 (or use case 1 – same concepts apply here), let's consider a scale out situation:

application must be expanded in order to support high demand at a point of time. This is practically translated by adding additional WEB VMs and APP VMs.

As depicted in the diagram below (showing physical view of the topology), WEB-VM-3 and APP-VM-2 have been added dynamically on WEB tier and APP tier respectively.

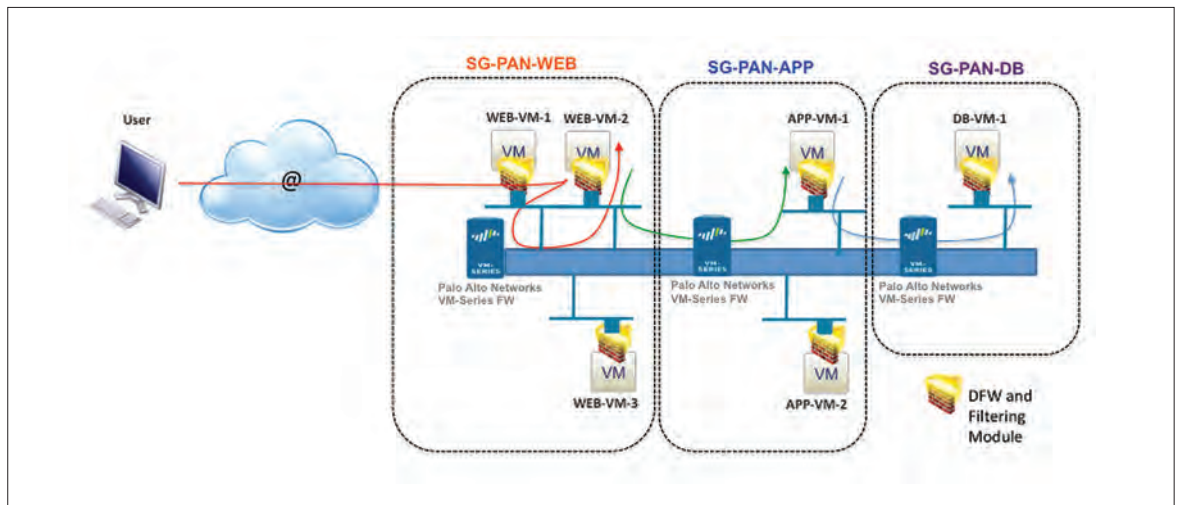
Notice that WEB-VM-3 has been added to ESXi host 2 (which is different from host 1 where WEB-VM-1 reside and host 4 where WEB-VM-2 reside). There is no requirement at all that VM belonging to same tier should reside on same ESXi host.

Existing policy rules defined on Panorama will be enforced for the 2 new VMs.



**Figure 17:** Physical View of Use Case 4 Topology

The following figure shows a logical view of traffic redirection and processing for this use case:



**Figure 18:** Logical View of Traffic Flows for Use Case 4

Upon completing the boot process, WEB-VM-3 and APP-VM-2 will register to vCenter and NSX via VMware tools.

WEB-VM-3 will be automatically added to SG-PAN-WEB and APP-VM-2 will be automatically added to SG-PAN-APP (using dynamic inclusion based on naming convention).

All traffic redirection enforced for the Security Groups will be applied to the new VMs.

And because there is a dynamic relationship between a Security Group on NSX and a Dynamic Address Group on Panorama, IP addresses of the two new VMs will be automatically transmitted from NSX to Panorama, which in turn updates all the VM-Series firewalls in the cluster.

As shown above, there is absolutely no human intervention in case of scale out situation: the application still grows organically and both NSX and the Palo Alto Networks systems will be able to apply traffic redirection and traffic protection adequately for the newly created VMs. PAN-OS security policy is applied to WEB-VM-3 and APP-VM-2 in a seamless and automatic way.



In case of scale down scenario (WEB-VM-3 and APP-VM-2 removed because of lower activity), both NSX and Palo Alto Networks systems behave the same way: the two new VMs will be automatically removed from their respective Security Groups and the associated Dynamic Address Groups will be immediately updated with this information. Again, no human intervention is required!

## Traffic Visibility and Operational Efficiency

Using PAN-OS next-generation firewall features such as App-ID and threat prevention, applications can be safely enabled. Below is a sample PAN-OS security policy rule showing precisely which applications are allowed between the application servers and the database servers.

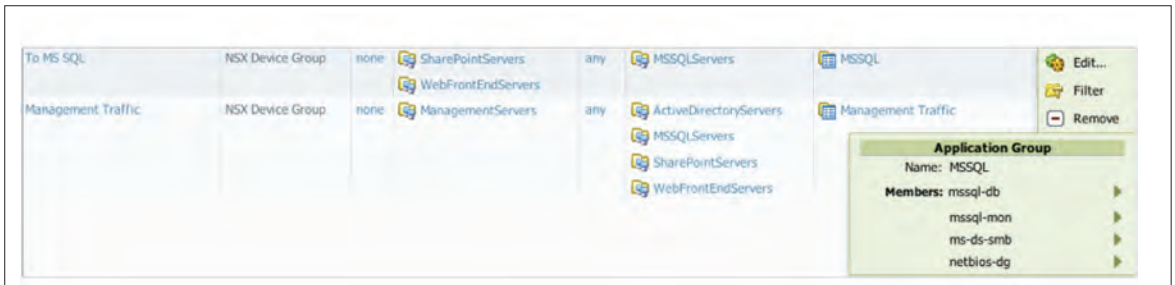


Figure 19: Creating Security Policy in Panorama

Only the required applications are enabled and packets are inspected to ensure they are truly the correct applications and not a nefarious application using a standard port.

PAN-OS also inspects the traffic for threats including vulnerabilities, viruses, and other malware. Below is a sample of the security policy rule for safely enabling database traffic.

Service Composer Canvas view provides a quick view of all Security Groups defined on NSX as well as characteristics per Security Group:

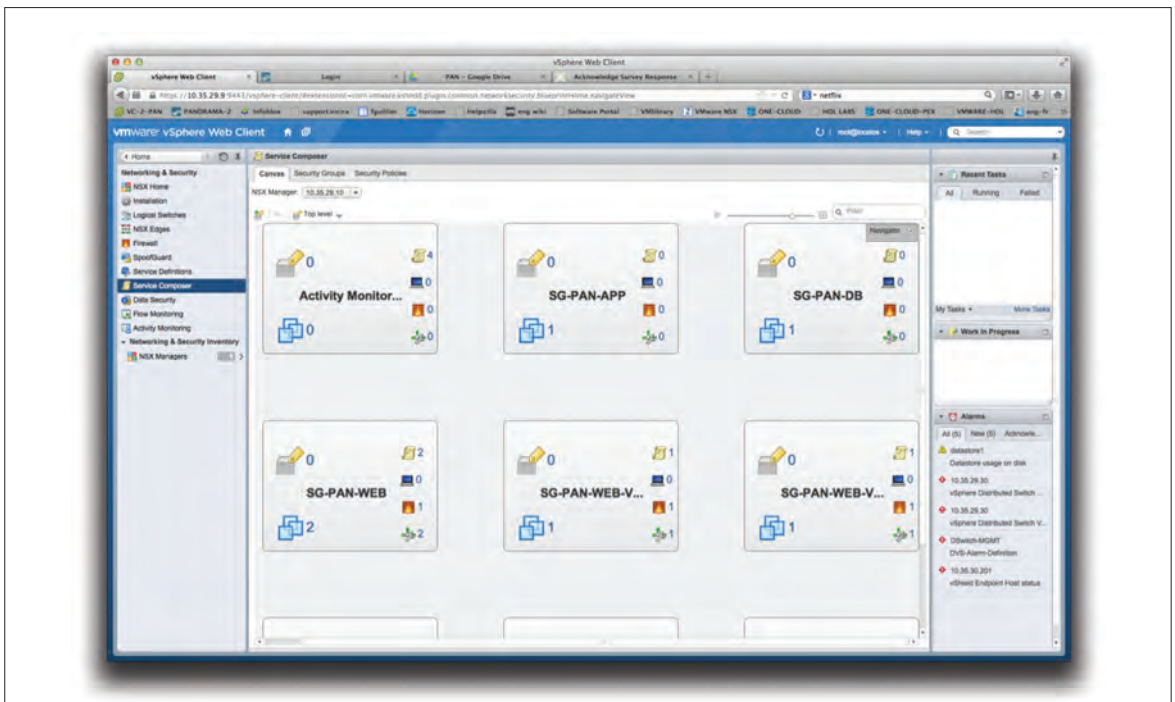


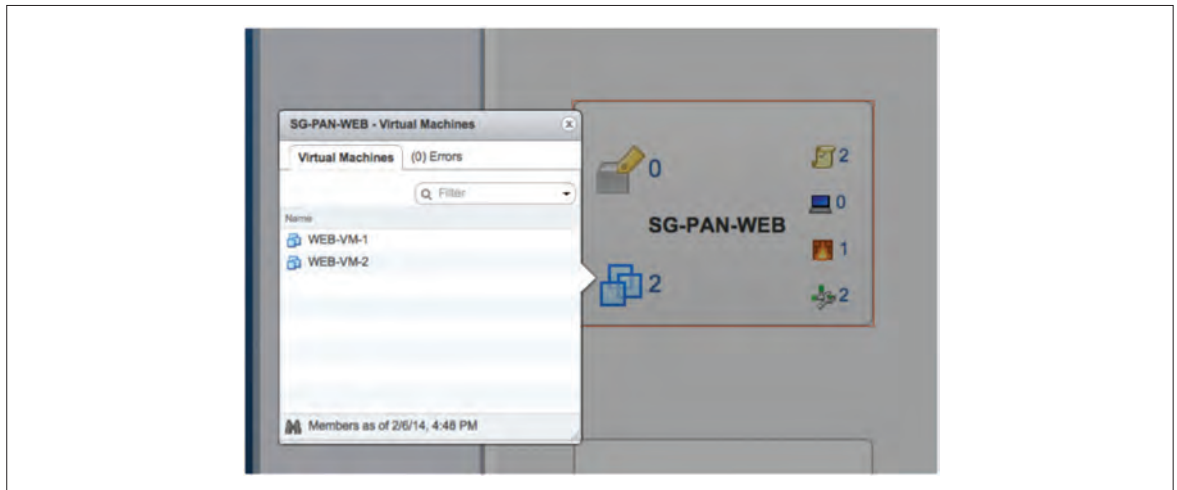
Figure 20: Service Composer Canvas View

Let's take for example SG-PAN-WEB:

Number 2 at bottom left represents number of VMs included in this Security Group. Number 2 at upper right represents the number of Security Policies attached to this SG.

Number 1 indicates the number of NSX firewall rules created for this SG. And finally number 2 at bottom right indicates the number of traffic redirection rules instantiated for this SG.

Clicking on any of these numbers displays details:



**Figure 21:** Guest VMs within a Security Group

The ESXi host provides a CLI to check traffic redirection configuration at the VM layer and some statistics associated with it.

First connect to the ESXi host using SSH (assuming access service is enabled on the host itself) and then type the following commands:

```
~ # summarize-dvfilter
<snip>
world 42825 vmm0:WEB-VM-1 vcUuid:'50 22 14 cd de a5 08 a6-fe c1 ce e2 94 ce 44 24'
port 50331656 WEB-VM-1.eth0
vNic slot 2
  name: nic-42825-eth0-vmware-sfw.2
  agentName: vmware-sfw
  state: IOChain Attached
  vmState: Detached
  failurePolicy: failClosed
  slowPathID: none
  filter source: Dynamic Filter Creation
vNic slot 4
  name: nic-42825-eth0-serviceinstance-1.4
  agentName: serviceinstance-1
  state: IOChain Attached
  vmState: Attached
  failurePolicy: failOpen
  slowPathID: 1
  filter source: Dynamic Filter Creation
<snip>
```



**~ # vsioctl getrules -f nic-42825-eth0-serviceinstance-1.4**

```
ruleset 1441 {
  # Filter rules
  rule 4952 at 2 out protocol any from addrset ip-securitygroup-35 to addrset ip-securitygroup-36 punt with log;
  rule 4956 at 3 out protocol any from addrset ip-securitygroup-36 to addrset ip-securitygroup-35 punt with log;
  rule 4960 at 4 in protocol any from any to addrset ip-securitygroup-16 punt with log;
}
```

**~ # vsioctl getaddrsets -f nic-42825-eth0-serviceinstance-1.4**

```
addrset ip-securitygroup-16 {
  ip 10.35.34.70,
  ip 10.35.34.89,
  ip fe80::54bd:5144:2bde:f58c,
  ip fe80::a450:d96f:26c0:b5fe,
}
addrset ip-securitygroup-35 {
  ip 10.35.34.70,
  ip fe80::a450:d96f:26c0:b5fe,
}
addrset ip-securitygroup-36 {
  ip 10.35.34.89,
  ip fe80::54bd:5144:2bde:f58c,
}
```

**~ # vsioctl getrules -f nic-42825-eth0-serviceinstance-1.4 -s**

```
rule 4952: 215247 evals, in 0 out 0 pkts, in 0 out 0 bytes
rule 4956: 101550 evals, in 0 out 0 pkts, in 0 out 0 bytes
rule 4960: 215247 evals, in 96891 out 497 pkts, in 12185212 out 905016 bytes
```

## Solution Benefits

The VMware NSX and Palo Alto Networks VM-Series integration provides the following benefits:

- **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:** Next-generation security is 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 firewall. The NSX Manager then automates the deployment of next-generation security services on every VMware ESXi server. Each VM-Series firewall 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 ESXi kernel module without the need 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 firewall 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” called security groups, which are mapped to dynamic address groups on Panorama, which the VM-Series uses to enforce security policies. Full context sharing between the VMware and Palo Alto Networks management platforms ensures that dynamic address groups are 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 firewall supports the PAN-OS operating system, comprehensive next-generation security features can be deployed 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).
- **Linear scaling with the number of hypervisors:** The IT administrator no longer needs to guess how much network security capacity is needed. Anytime a new hypervisor is added, next-generation security capacity is automatically added.

## Conclusion

The VMware network virtualization solution addresses current challenges with physical network infrastructure and brings flexibility, agility and scale through VXLAN-based logical networks. Along with the ability to create on-demand logical networks using VXLAN, the vCloud Networking and Security Edge gateway helps users deploy various logical network services such as firewall, DHCP, NAT and load balancing on these networks.

The VMware NSX and Palo Alto Networks integrated solution extends the basic firewall services delivered by the NSX virtualization platform. The joint solution provides an integrated data center solution that allows IT organizations to unlock all the benefits of the software defined data center, from greater flexibility and agility to optimized capacity utilization and operational efficiencies, 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 data center traffic including intra-server virtual machine communications.

## References

- [1] *What's New in VMware vSphere 5.5*  
<http://www.vmware.com/files/pdf/vsphere/VMware-vSphere-Platform-Whats-New.pdf>
- [2] *vSphere 5.5 Configuration Maximums*  
<http://www.vmware.com/pdf/vsphere5/r55/vsphere-55-configuration-maximums.pdf>
- [3] *What's new in PAN-OS 6.0*  
<https://paloaltonetworks.com/products/newinpan-os.html>
- [4] *VM-Series Introduction*  
[https://www.paloaltonetworks.com/content/dam/paloaltonetworks-com/en\\_US/assets/pdf/datasheets/vm-series/vm-series.pdf](https://www.paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/datasheets/vm-series/vm-series.pdf)
- [5] *How To Dramatically Reduce the Cost and Complexity of PCI Compliance*  
[http://media.paloaltonetworks.com/documents/Reducing\\_PCI\\_Compliance.pdf](http://media.paloaltonetworks.com/documents/Reducing_PCI_Compliance.pdf)
- [6] *vSphere 5.5 Hardening Guide*  
<http://www.vmware.com/security/hardening-guides.html>



**VMware, Inc.** 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 [www.vmware.com](http://www.vmware.com)

Copyright © 2014 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: