Datacenter Virtualization

Transforming Security for the Software Defined Datacenter

Alessio Agnello

Pre-Sales System Engineer

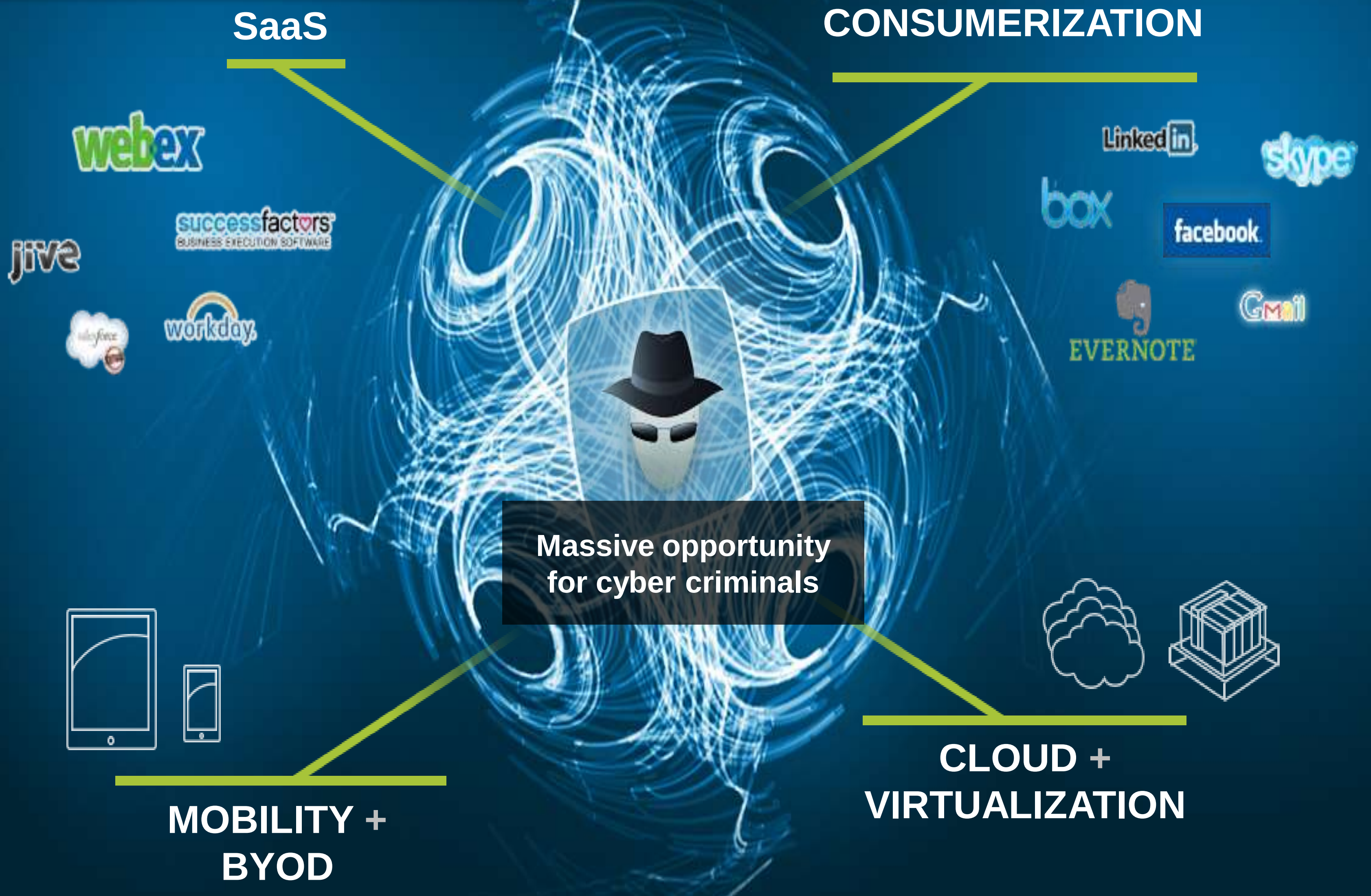
aagnello@paloaltonetworks.com

paloalto NETWORKS

the network security company™

What's changed?

THE EVOLUTION OF BUSINESS



SaaS

SOCIAL + CONSUMERIZATION

Massive opportunity for cyber criminals

MOBILITY + BYOD

CLOUD + VIRTUALIZATION

What’s changed?

THE EVOLUTION OF THE ATTACKER

THIS IS WHAT REALLY CHANGED!

Majority of adversaries are just doing their job….

- They have bosses, families, bills to pay.
- They want to get in, accomplish their task, and get out (un-detected).
- The goal isn’t making your life hard.

MALWARE UPDATES

24/7 support

SALES IN 18 MONTHS

$1.2B+/

This is WHAT CHANGED!

EXPLORING ACTOR MOTIVATIONS

…NOT MUTUALLY EXCLUSIVE

Cyber
Espionage

Cyber
Crime

Cyber
Hacktivism

Cyber
Warfare

Cyber
Terrorism

Cyber
Mischief

$$$

CYBERCRIME NOW

$1+ trillion industry

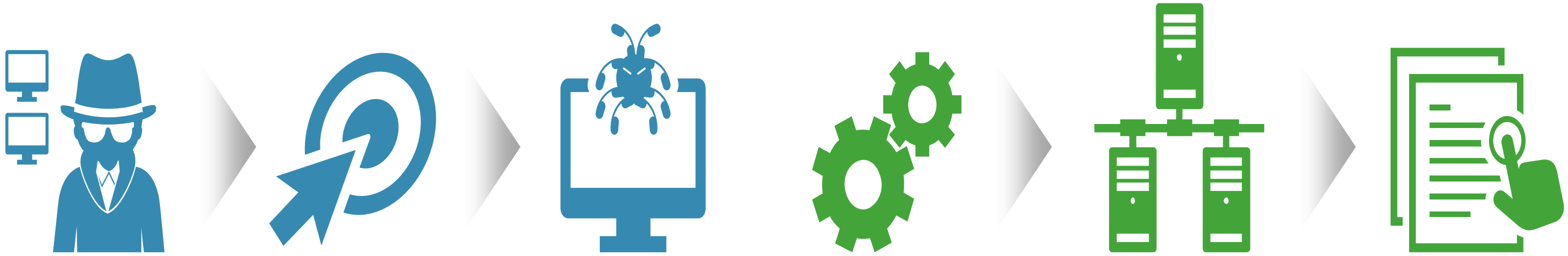
CYBER WARFARE

100+ nations

Advanced Persistent Threats

THE CYBER ATTACK LIFECYCLE

…YOU BETTER KNOW YOUR ENEMY



Reconnaissance

Weaponization and Delivery

Exploitation

Installation

Command-and-Control

Actions on the Objective

Unauthorized Access

Unauthorized Use

“ There is no predictable path for the *advanced adversary* ”

Advanced Persistent Threats

ATTACK TECHNIQUES / TOOLS

…MUST INCREASE THE COST FOR ADVERSARIES

Myth

- Highly customized and unique tools are used for every attack.
- Customized protocols, with unique encryption types are used for CnC.

Reality

- Off-the-shelf tools are the most common method of attack.
- HTTP is most common for custom backdoors.

Why Breaches still happen?

GOODs VS BADs

Port-based Firewall

Static IPS

0-Day Malware & Exploits

ID Credentials Hijacking

Why “Blacklisting-only” fails…

Evolution and Security Challenges in the Software Defined Data Center

paloalto NETWORKS

the network security company™

Evolution towards a software defined data center

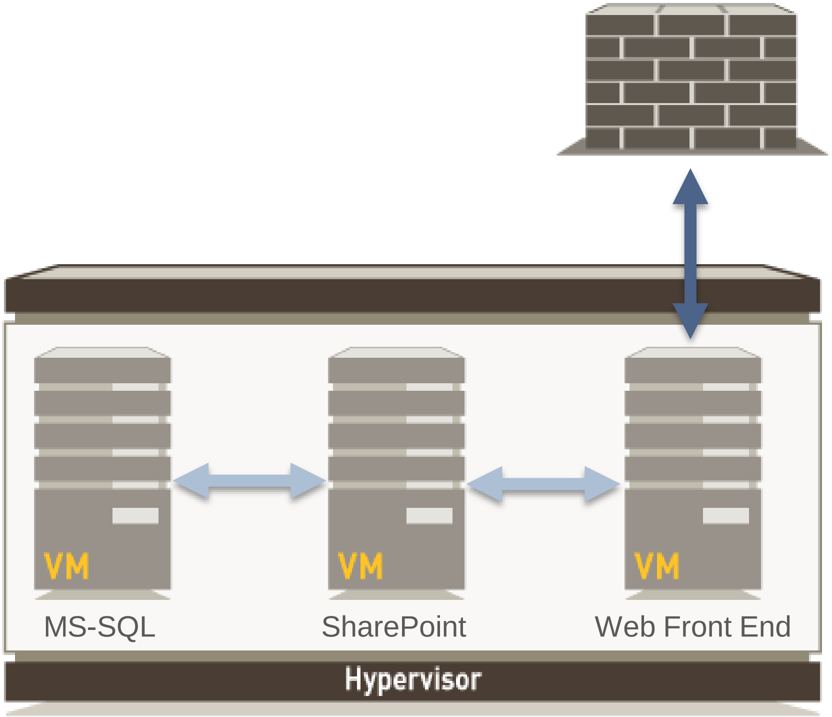
Server Virtualization

Software Defined Data Center

- A software defined data center is agile, flexible, elastic and simple
  - Fast workload provisioning – reduce from weeks to hours
  - Flexible workload placement
  - Simplified data center operations & economics
- **Security** is a critical component of the software defined data center

Security challenges

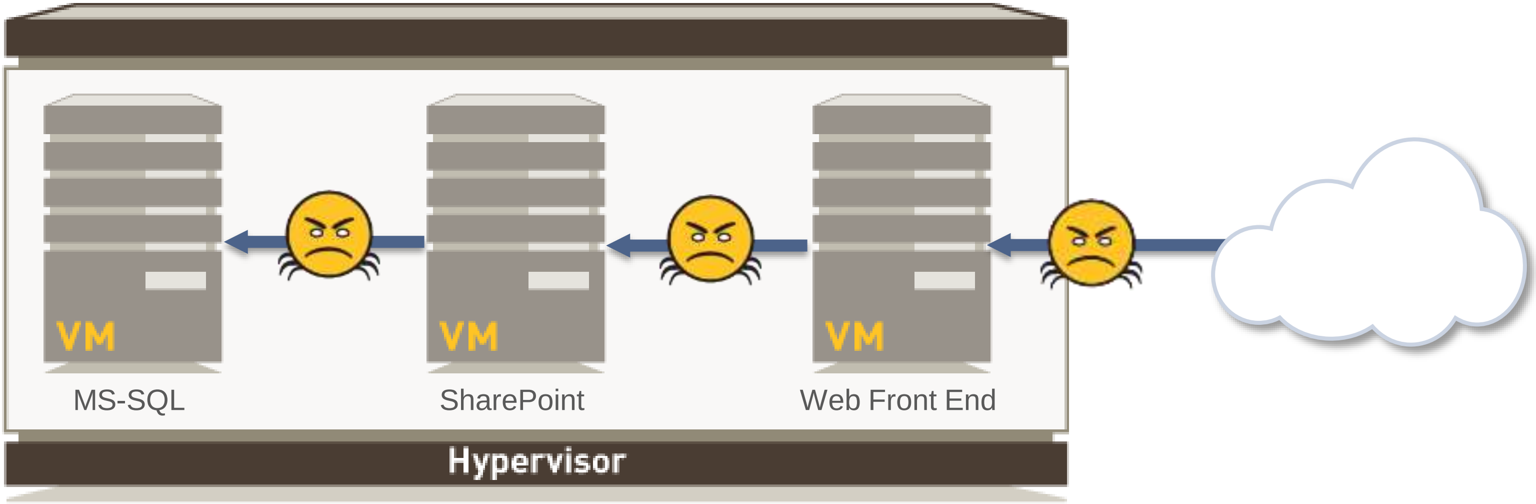
Physical firewalls may not see the East-West traffic



- Firewalls placement is designed around expectation of layer 3 segmentation
- Network configuration changes required to secure East-West traffic flows are manual, time-consuming and complex
- Ability to transparently insert security into the traffic flow is needed

Security challenges

Incomplete security features on existing virtual security solutions

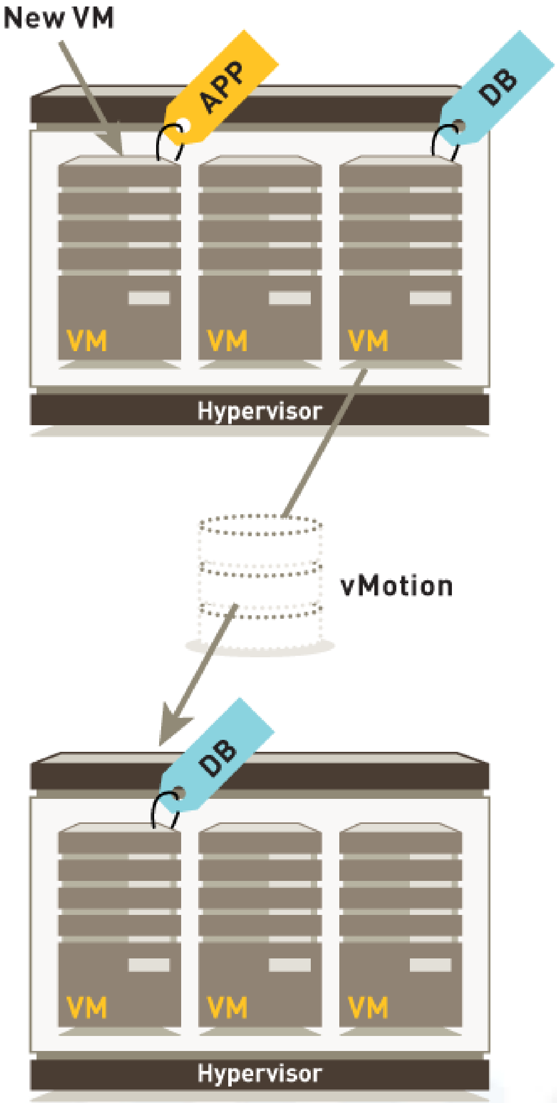


In the cloud, applications of different trust levels now run on a single server

- VM-VM traffic (East-West) needs to be inspected
- Port and protocol-based security is not sufficient
- Virtualized next-generation security is needed to:
  - Safely enable application traffic between VMs
  - Protect against against cyber attacks

Security challenges

Static policies cannot keep pace with dynamic workload deployments



- Provisioning of applications can occur in minutes with frequent changes
- Security approvals and configurations may take weeks/months
- Dynamic security policies that understand VM context are needed

VM-Series for VMware NSX

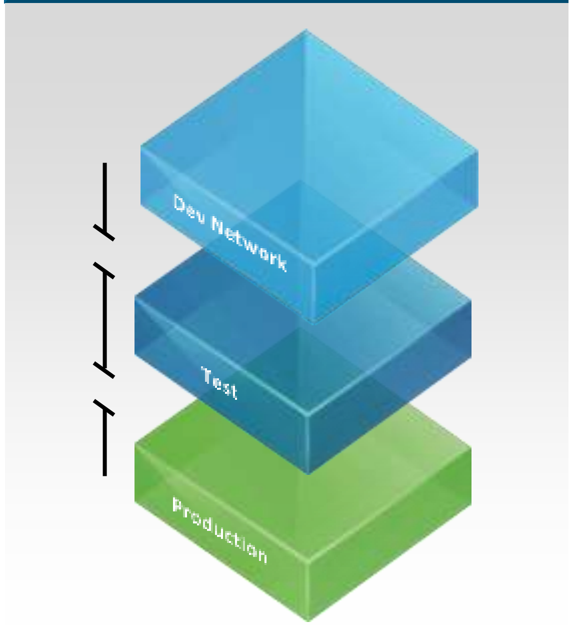
Solution Overview

paloalto NETWORKS

the network security company™

Data Center: Micro-segmentation in detail

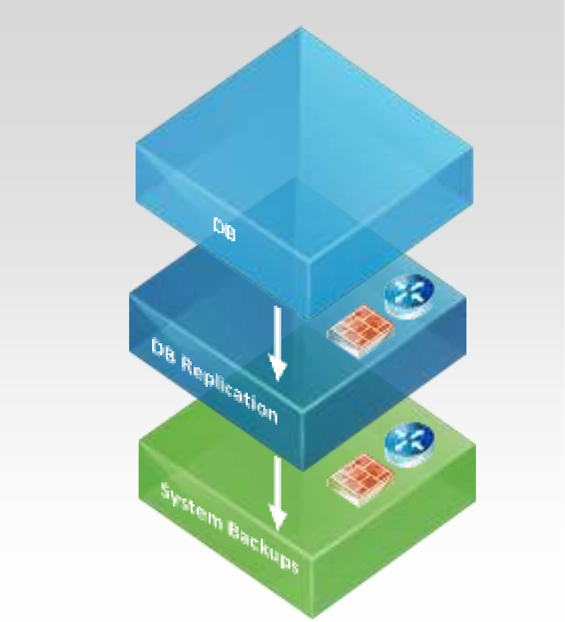
Isolation



No communication path between unrelated networks

- No cross-talk between networks
- Overlay technology assures networks are separated by default

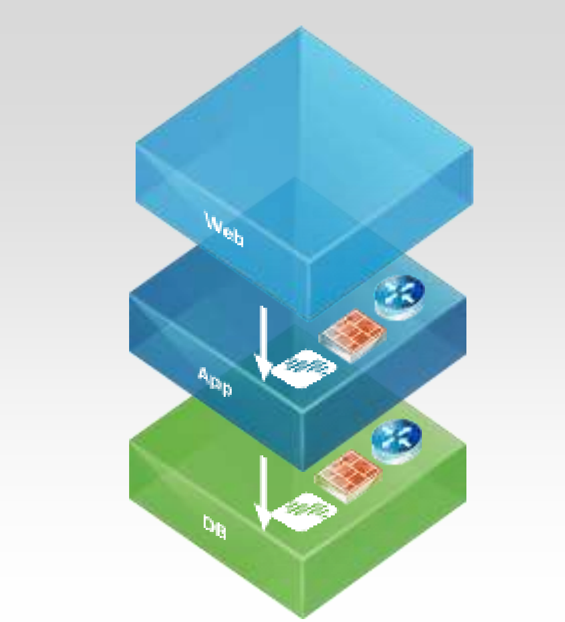
Segmentation



Controlled communication path within a single network

- Fine-grained enforcement of security
- Security policies based on logical groupings of VMs

Advanced services



Advanced services: addition of 3rd party security, as needed by policy

- Platform for including leading security solutions
- Dynamically add advanced security to adapt to changing security conditions

Joint solution components and benefits

VMware NSX

VM-Series

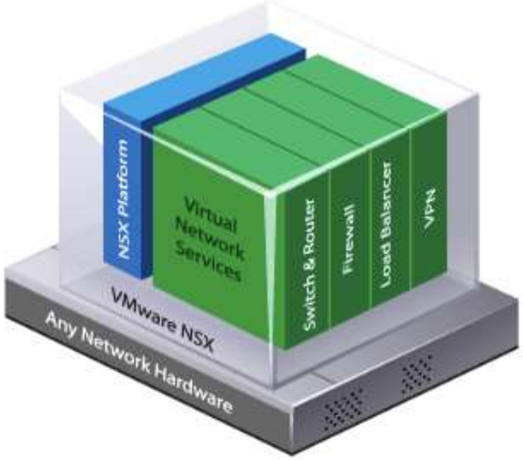
Panorama

Safe application enablement with deep protection against cyber attacks

- ○ Automated provisioning and configuration
- ○ Seamless service insertion
- ○ Dynamic security policy updates

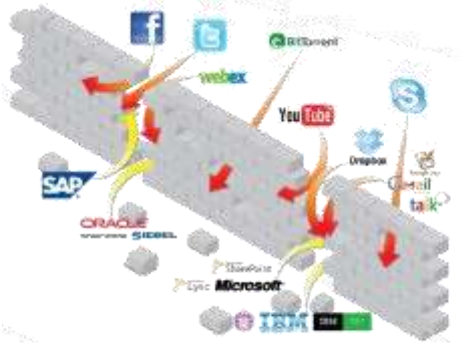
VMware Solution Requirements

- ESXi Hosts 5.0 or later
- vCenter 5.5
  - Central Management
  - Deployed as a OVA on a ESXi host
- NSX Manager 6.0.x
  - Networking and Security Platform
  - Deployed as a OVA on a ESXi host
- Integrates via the NetX API
- All management is done through the vSphere web client connected to vCenter
- Supports Standard and Distributed Switches from VMware

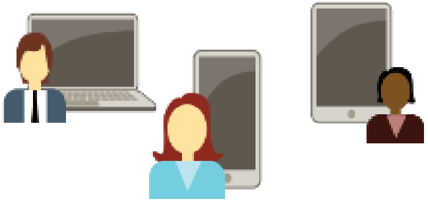


VM-Series: Next Generation Security Platform

- **Consistent Features** as hardware-based next-generation firewall
  - App-ID
  - User-ID
  - Content-ID
  - Wildfire



- Inspects and **Safely Enables Intra-Host Communications** (East-West traffic)



- **Tracks VM Creation and Movement** with Dynamic Address Group objects

- API integration with orchestration: **Automate Workflows**

- **Centrally Managed** through Panorama

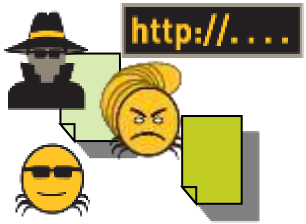
Next Generation Firewall Technologies
Visibility and Safe Enablement of All Traffic

Applications: Safe enablement in the data center begins with application classification by App-ID.

- Applications classified regardless of ports, protocols, evasive tactic, encryption
- Classify custom applications and unknowns in the data center

Users: Tying users and groups, regardless of location or devices, to applications with User-ID and GlobalProtect.

- Differentiate access based on user, device and endpoint profile



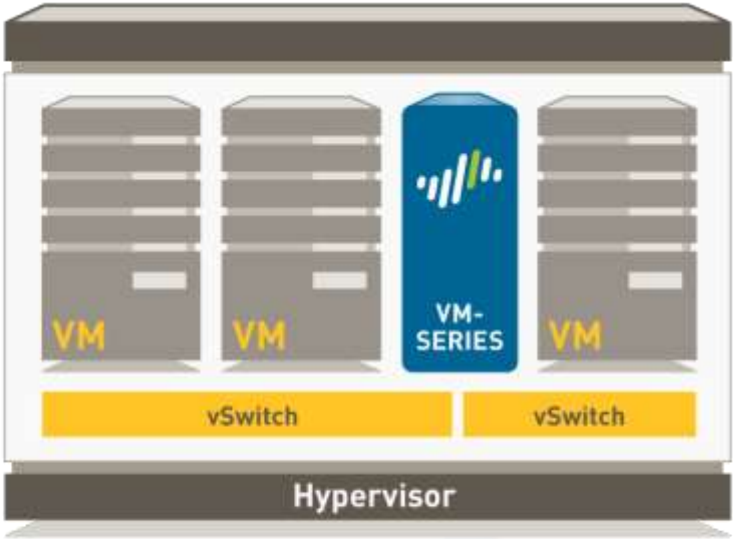
Content: Scanning content and protecting against all threats – both known and unknown;
with Content-ID and WildFire.

- Protect any type of traffic from targeted attacks

NGFW as a VM, versus as a Service

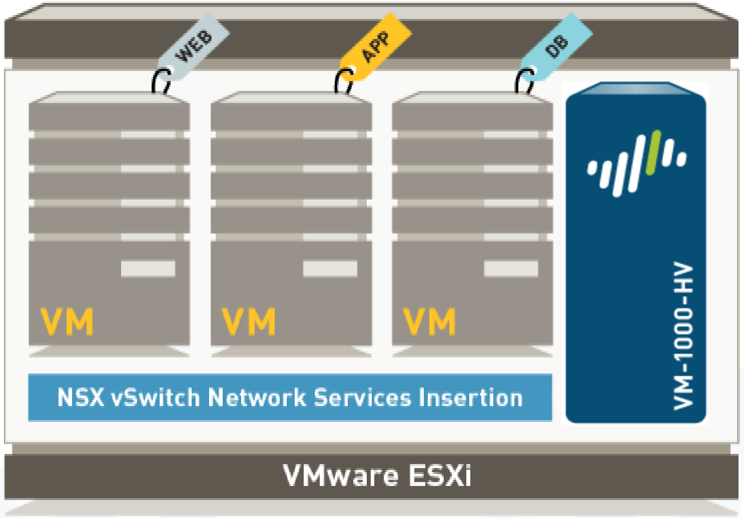
VM-Series as a Guest VM

- Virtual Networking configured to pass traffic through Firewall
- Requires vSwitch and Port Group Configuration
- Connects as L3, L2, V-wire, or Tap



VM-Series NSX Edition as a Service

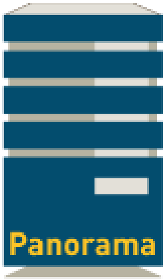
- NGFW is an NSX Service
- Resides below the vSwitch and above vNIC
- NSX steers traffic to and from VM before Networking



VM-Series Sizing

- **vCPUs**
  - 2 minimum expand to 4 or 8
  - One always allocated to the management plane
  - Additional vCPUs are for the data plane
- **vNICs**
  - Up to 10 for VMware ESXi (VMware Guest Limit)
  - 3 Fixed for VMware NSX
  - One always allocated for the management interface
  - For VMware the vNICs must be type VMXNET3
- **Virtual Disk Space**
  - Minimum of 40 GB virtual disk
  - A second optional virtual disk (up to 2 TB) may be added for VM-Series logging
- **Additional memory beyond 4GB is supported**
  - but all memory in excess of 4GB is only used by the management plane (VM-100, VM-200, VM-300)
  - VM-1000-HV requires 5 GB of memory minimum

Centralized Management and Policy Automation



Panorama

- Global, centralized management of your next-generation firewalls, regardless if they're physical or virtual platforms
- Centralized logging and reporting across all managed devices
- Deploy as VM or via M-100 appliance
- Scalability – Managing up to 1000 Next-Gen Firewalls
- Delegate administrative access and responsibilities
- Simplifies firewall deployment; decreasing deployment time and improved operational efficiency

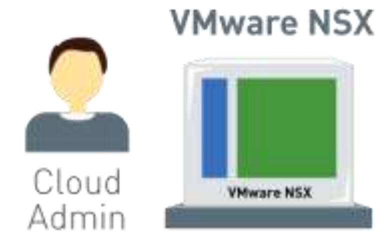
VM-Series for VMware NSX

How it works

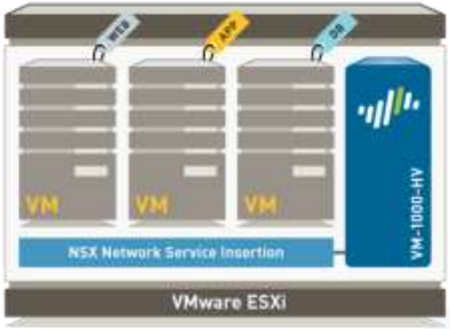
paloalto NETWORKS

the network security company™

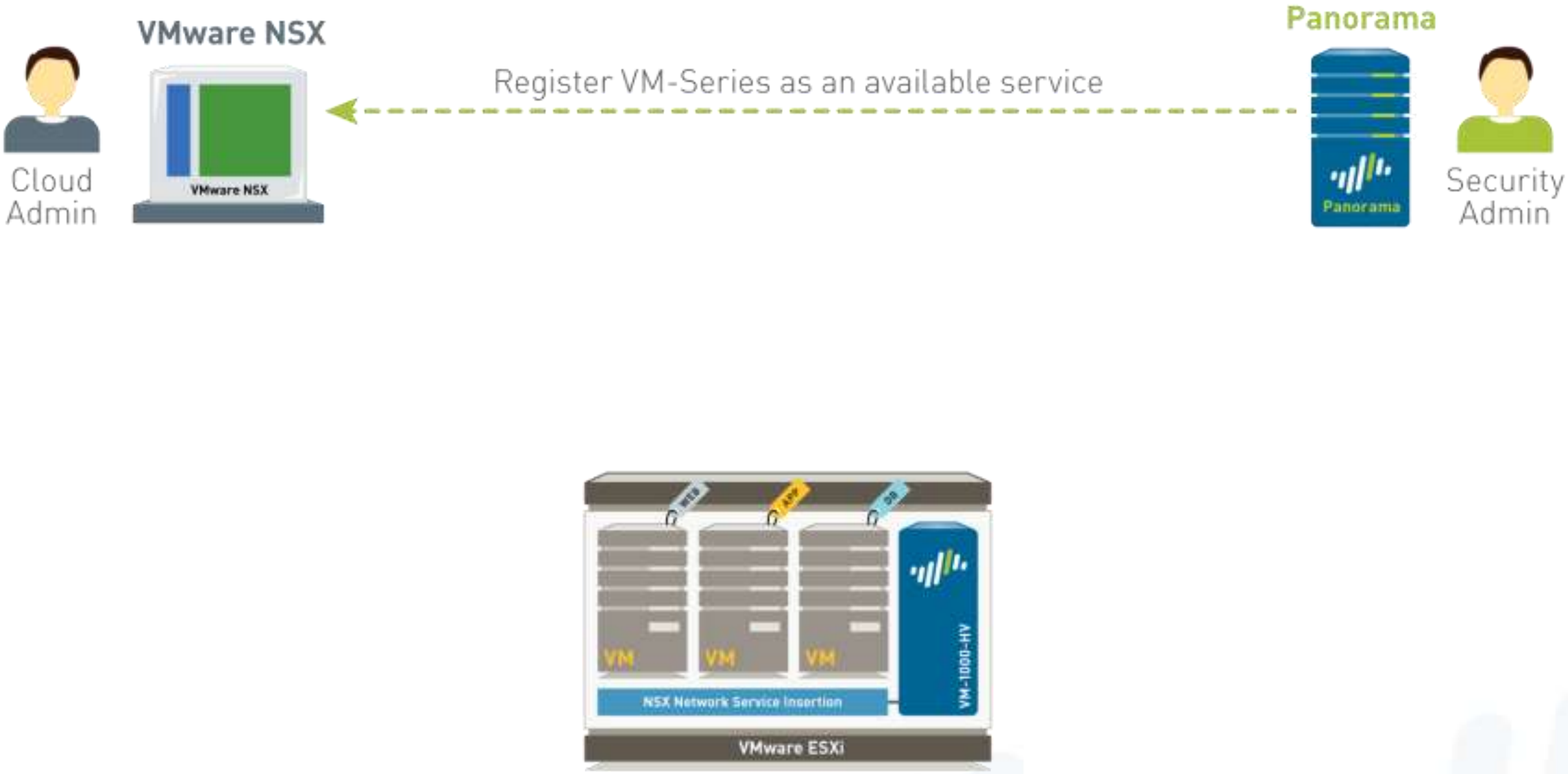
How it works: The joint solution components



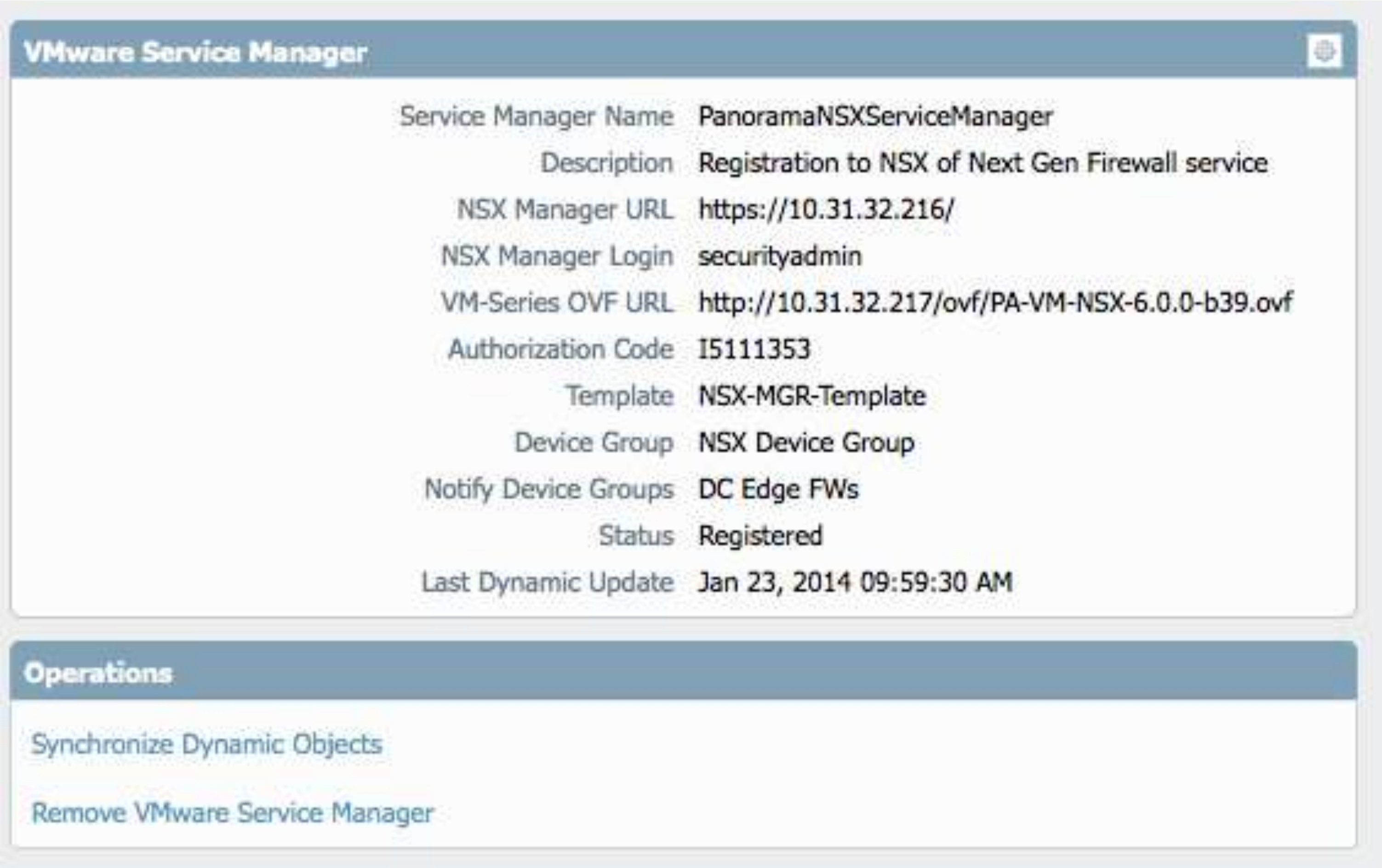
Panorama
Panorama
Security Admin



How it works: Registration



How it works: Panorama



VMware Service Manager

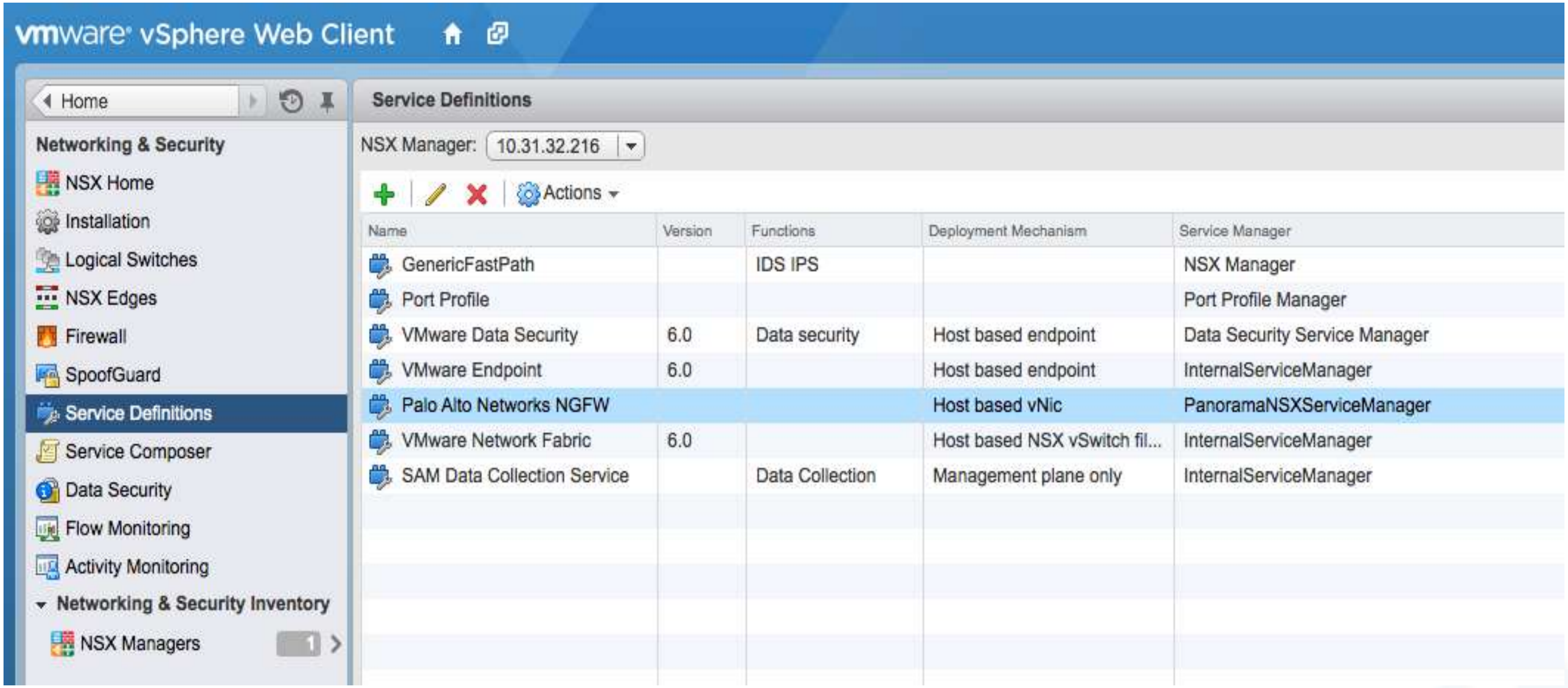
Service Manager Name	PanoramaNSXServiceManager
Description	Registration to NSX of Next Gen Firewall service
NSX Manager URL	https://10.31.32.216/
NSX Manager Login	securityadmin
VM-Series OVF URL	http://10.31.32.217/ovf/PA-VM-NSX-6.0.0-b39.ovf
Authorization Code	I5111353
Template	NSX-MGR-Template
Device Group	NSX Device Group
Notify Device Groups	DC Edge FWs
Status	Registered
Last Dynamic Update	Jan 23, 2014 09:59:30 AM

Operations

Synchronize Dynamic Objects

Remove VMware Service Manager

How it works: VMware NSX Manager

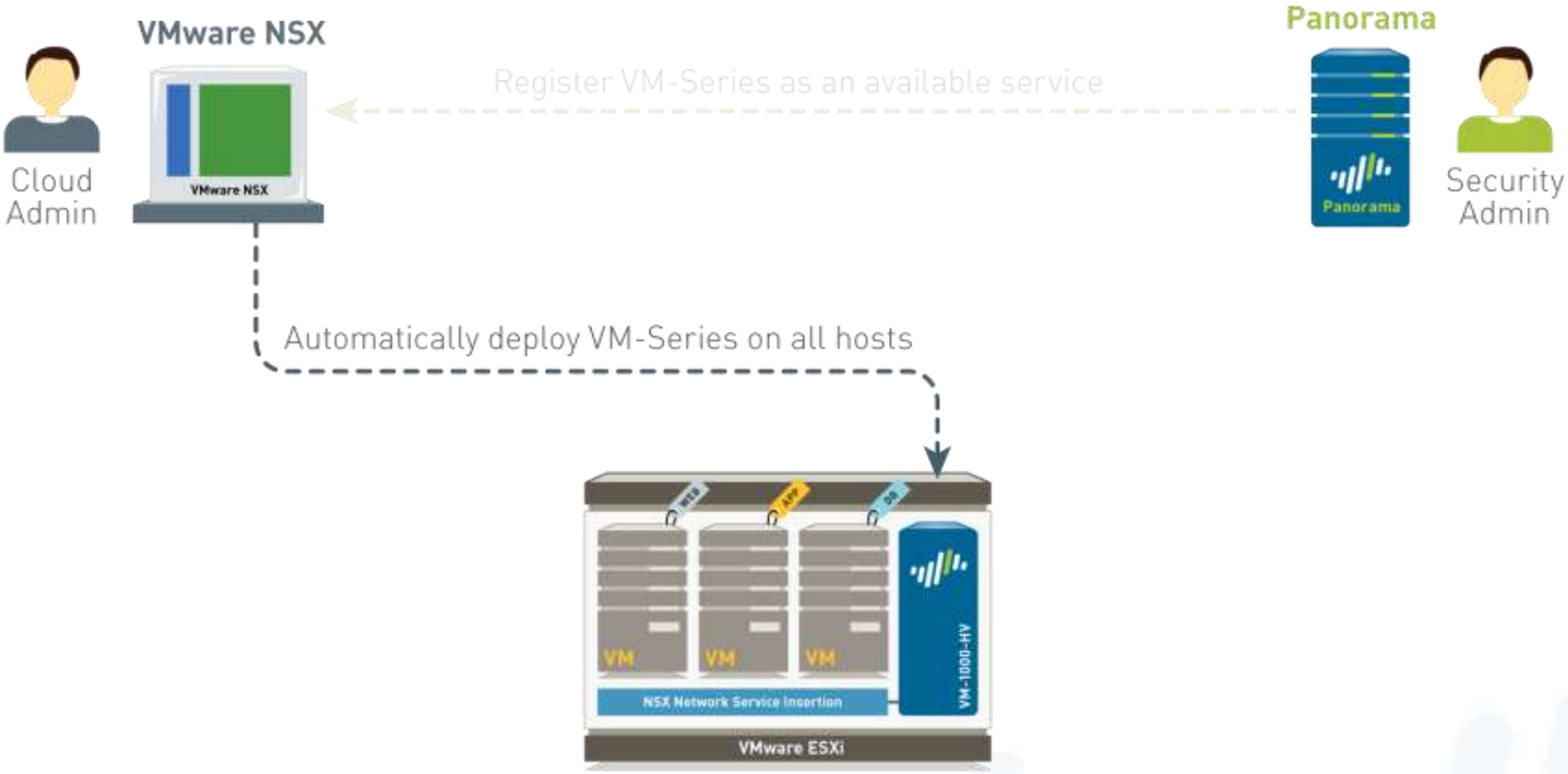


Service Definitions

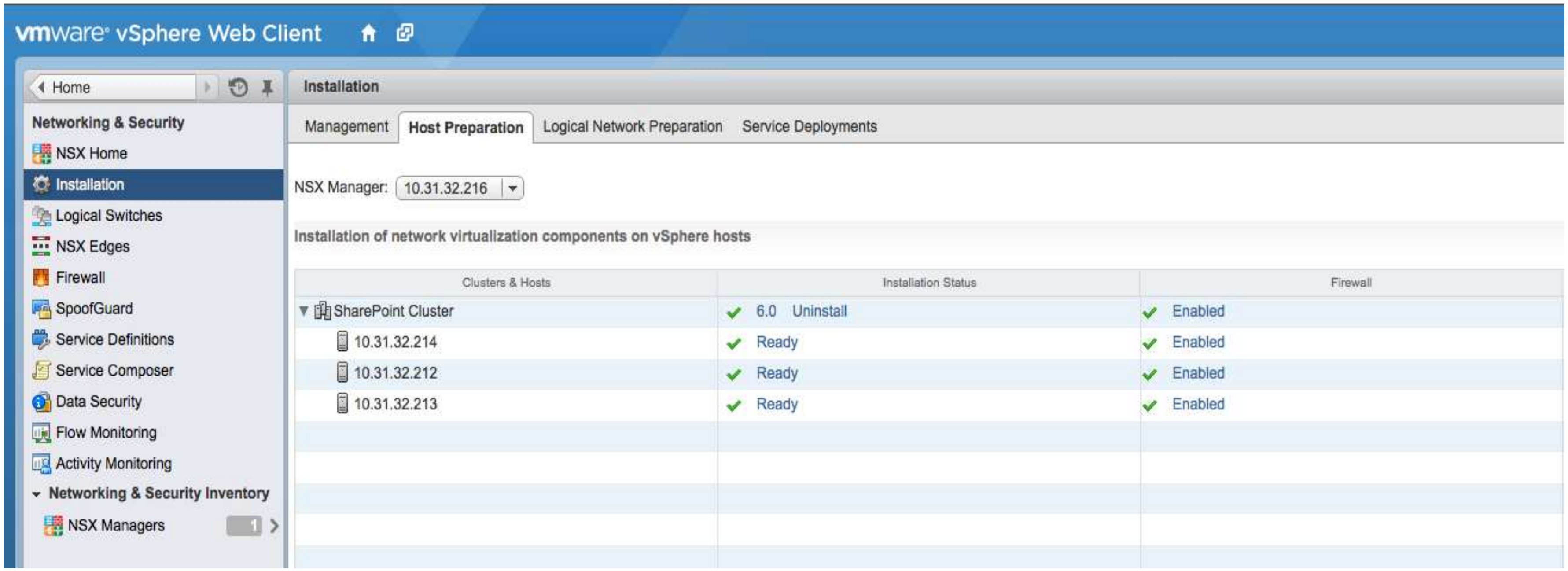
NSX Manager: 10.31.32.216

Name	Version	Functions	Deployment Mechanism	Service Manager
GenericFastPath		IDS IPS		NSX Manager
Port Profile				Port Profile Manager
VMware Data Security	6.0	Data security	Host based endpoint	Data Security Service Manager
VMware Endpoint	6.0		Host based endpoint	InternalServiceManager
Palo Alto Networks NGFW			Host based vNic	PanoramaNSXServiceManager
VMware Network Fabric	6.0		Host based NSX vSwitch fil...	InternalServiceManager
SAM Data Collection Service		Data Collection	Management plane only	InternalServiceManager

How it works: Deployment


VMware NSX
Cloud Admin
VMware NSX
Register VM-Series as an available service
Panorama
Panorama
Security Admin
Automatically deploy VM-Series on all hosts
WEB
APP
DB
VM
VM
VM
NSX Network Service Insertion
VM-1000-HV
VMware ESXi

How it works: NSX Manager

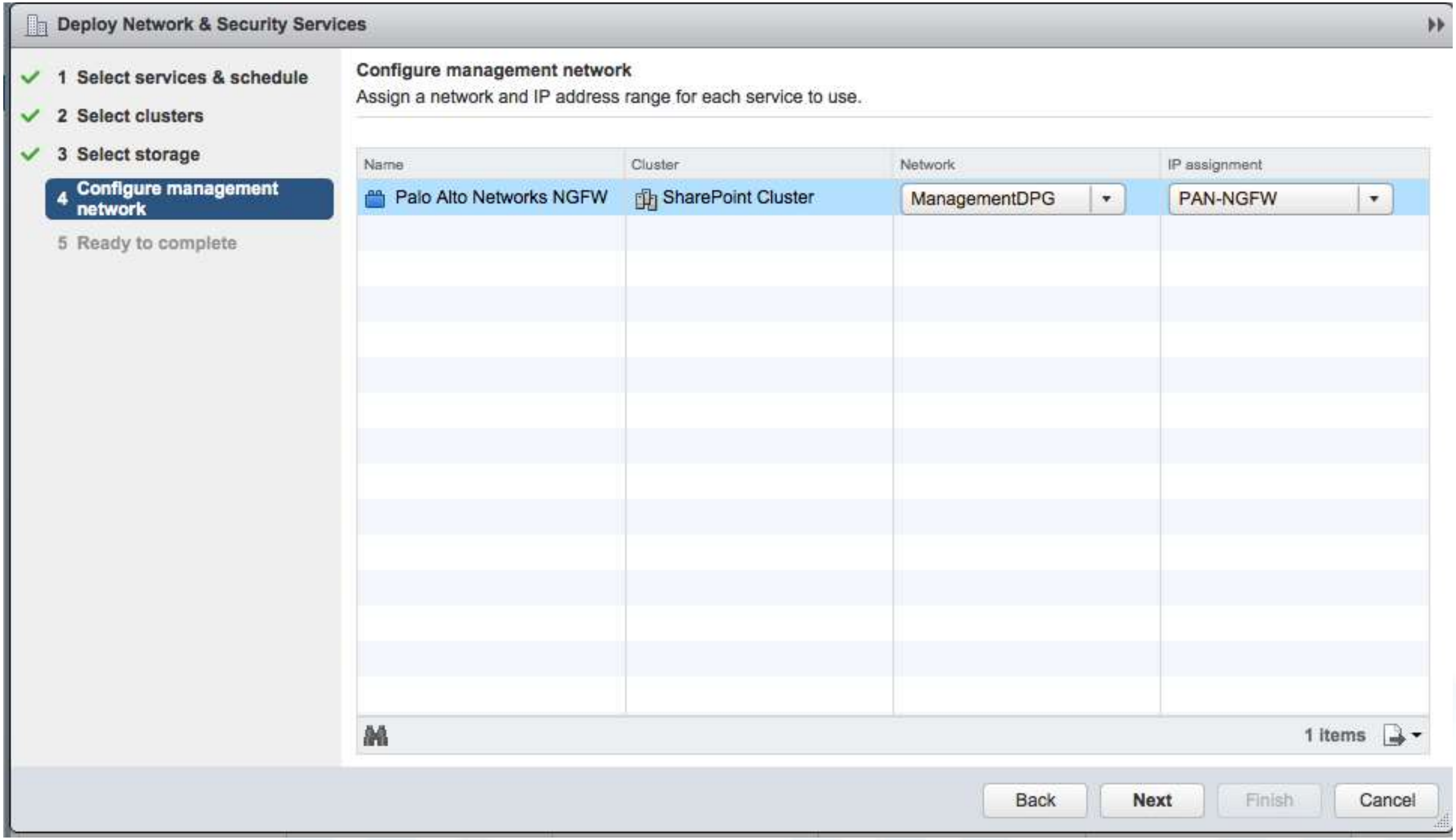


NSX Manager: 10.31.32.216

Installation of network virtualization components on vSphere hosts

Clusters & Hosts	Installation Status	Firewall
▼ SharePoint Cluster	✓ 6.0 Uninstall	✓ Enabled
10.31.32.214	✓ Ready	✓ Enabled
10.31.32.212	✓ Ready	✓ Enabled
10.31.32.213	✓ Ready	✓ Enabled

How it works: NSX Manager



Deploy Network & Security Services

✓ 1 Select services & schedule
✓ 2 Select clusters
✓ 3 Select storage
4 Configure management network
5 Ready to complete

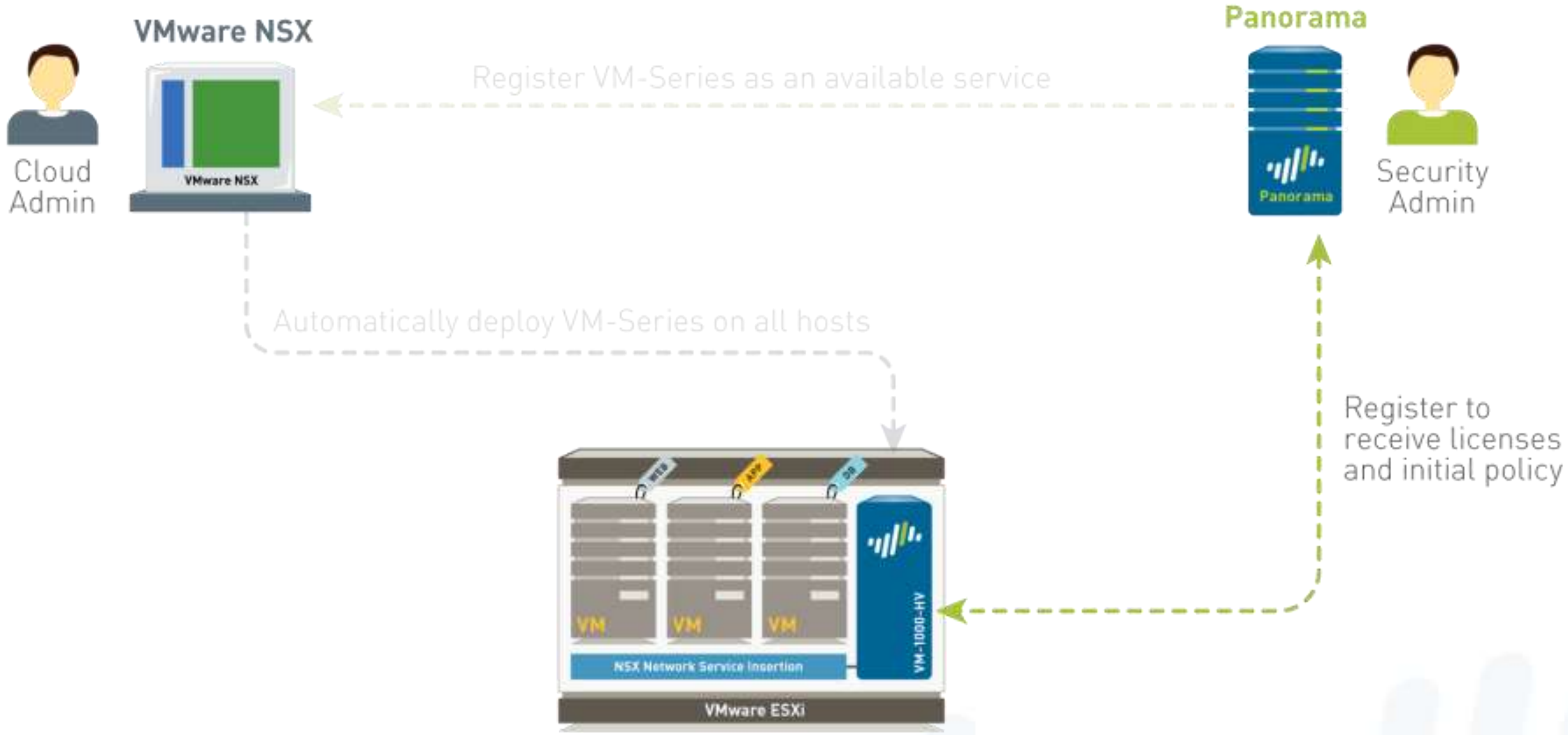
Configure management network

Assign a network and IP address range for each service to use.

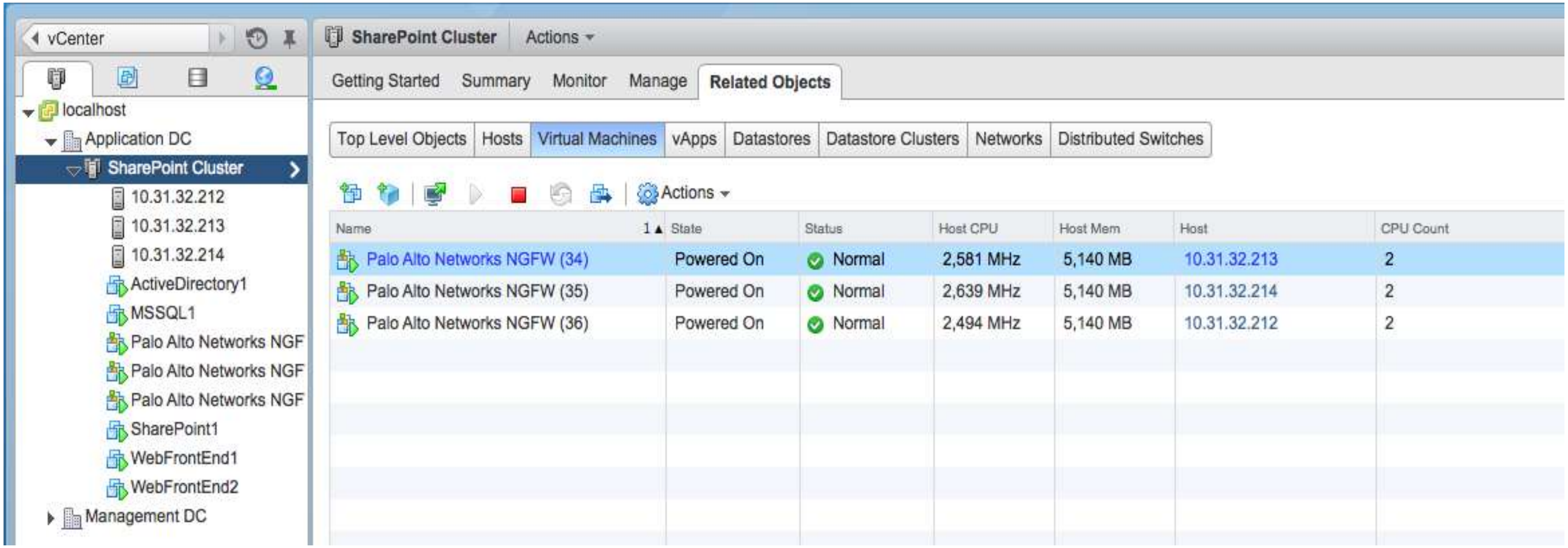
Name	Cluster	Network	IP assignment
Palo Alto Networks NGFW	SharePoint Cluster	ManagementDPG	PAN-NGFW

1 items

How it works: Licensing and Configuration

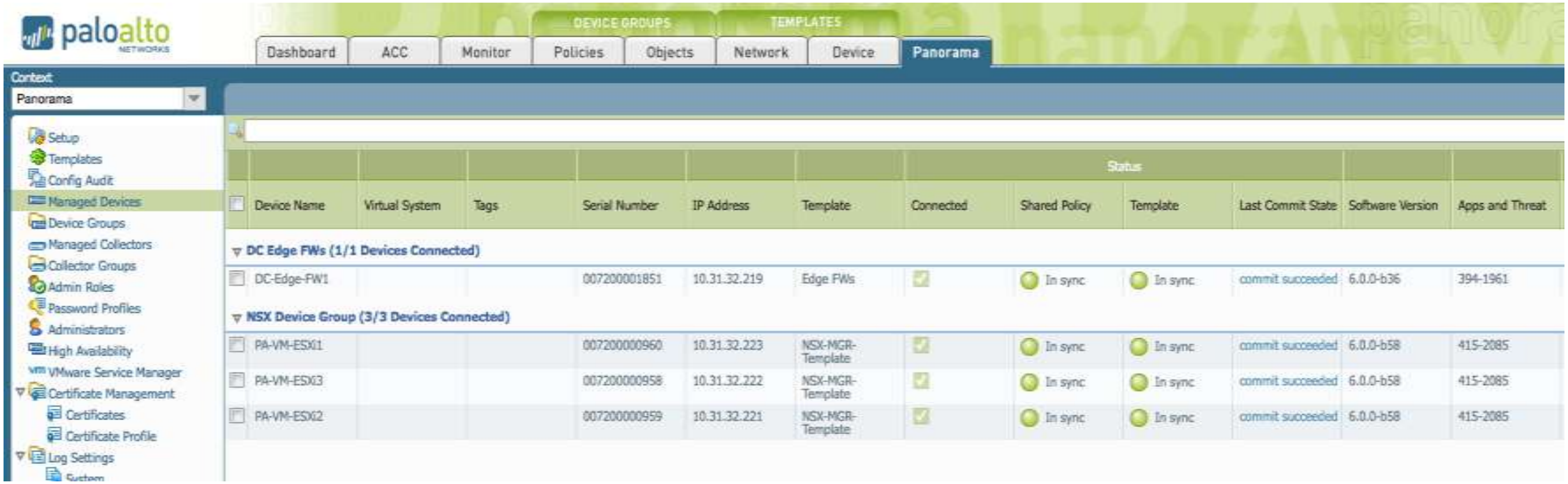

VMware NSX
Cloud Admin
VMware NSX
Register VM-Series as an available service
Panorama
Panorama
Security Admin
Automatically deploy VM-Series on all hosts
Register to receive licenses and initial policy
WEB
APP
DB
VM
VM
VM
VM-1000-HV
NSX Network Service Insertion
VMware ESXi

How it works: VMware vCenter



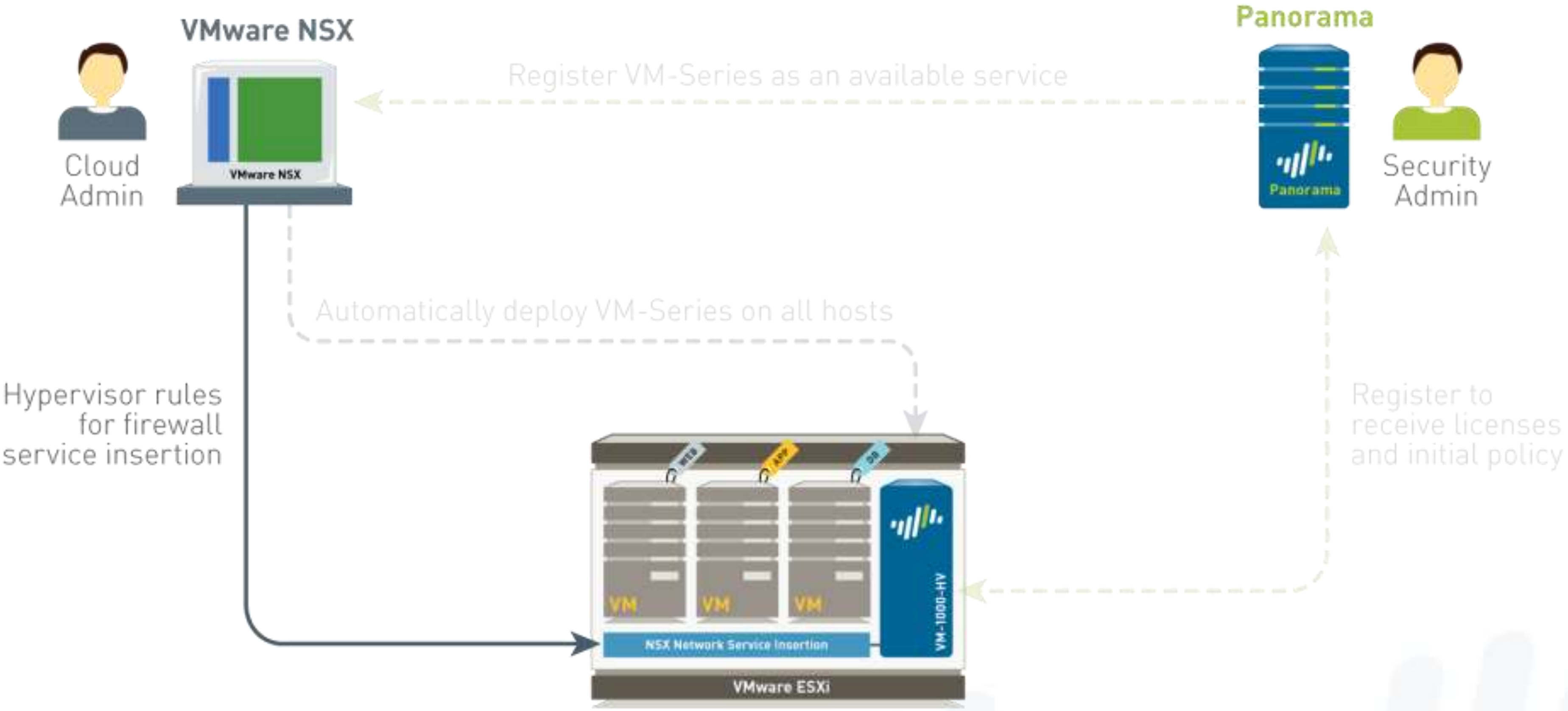
Name	State	Status	Host CPU	Host Mem	Host	CPU Count
Palo Alto Networks NGFW (34)	Powered On	✓ Normal	2,581 MHz	5,140 MB	10.31.32.213	2
Palo Alto Networks NGFW (35)	Powered On	✓ Normal	2,639 MHz	5,140 MB	10.31.32.214	2
Palo Alto Networks NGFW (36)	Powered On	✓ Normal	2,494 MHz	5,140 MB	10.31.32.212	2

How it works: Panorama

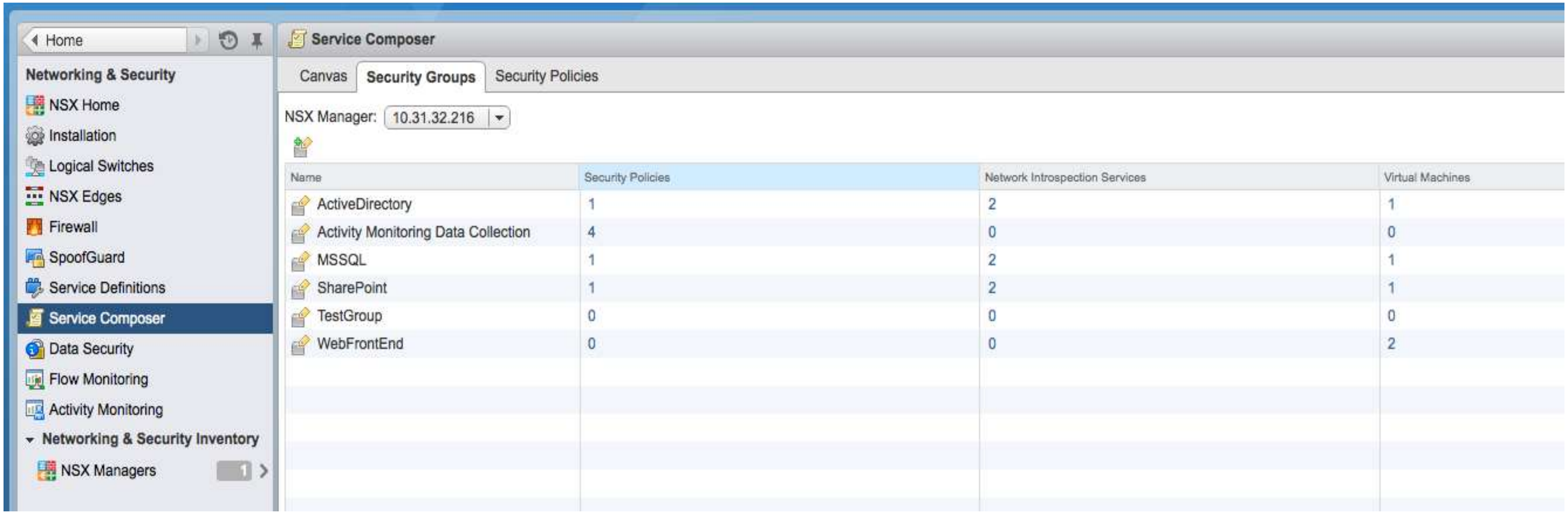


							Status					
□	Device Name	Virtual System	Tags	Serial Number	IP Address	Template	Connected	Shared Policy	Template	Last Commit State	Software Version	Apps and Threat
▽ DC Edge FWs (1/1 Devices Connected)												
□	DC-Edge-FW1			007200001851	10.31.32.219	Edge FWs	☑	● In sync	● In sync	commit succeeded	6.0.0-b36	394-1961
▽ NSX Device Group (3/3 Devices Connected)												
□	PA-VM-ESXi1			007200000960	10.31.32.223	NSX-MGR-Template	☑	● In sync	● In sync	commit succeeded	6.0.0-b58	415-2085
□	PA-VM-ESXi3			007200000958	10.31.32.222	NSX-MGR-Template	☑	● In sync	● In sync	commit succeeded	6.0.0-b58	415-2085
□	PA-VM-ESXi2			007200000959	10.31.32.221	NSX-MGR-Template	☑	● In sync	● In sync	commit succeeded	6.0.0-b58	415-2085

How it works: Traffic Re-direction Rules


VMware NSX
Panorama
Register VM-Series as an available service
Cloud Admin
VMware NSX
Panorama
Security Admin
Automatically deploy VM-Series on all hosts
Hypervisor rules for firewall service insertion
Register to receive licenses and initial policy
WEB
APP
DB
VM
VM
VM
VM-1000-HV
NSX Network Service Insertion
VMware ESXi

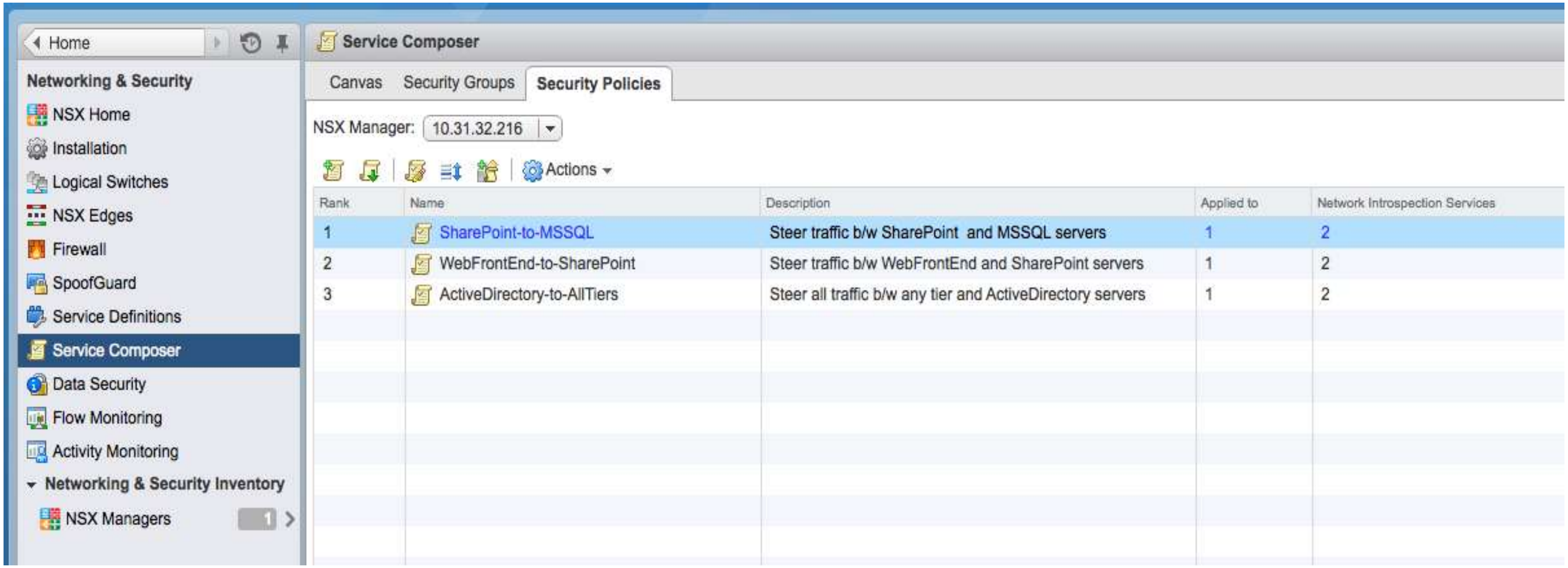
How it works: NSX Mgr.: Service Composer: Containers



NSX Manager: 10.31.32.216

Name	Security Policies	Network Introspection Services	Virtual Machines
ActiveDirectory	1	2	1
Activity Monitoring Data Collection	4	0	0
MSSQL	1	2	1
SharePoint	1	2	1
TestGroup	0	0	0
WebFrontEnd	0	0	2

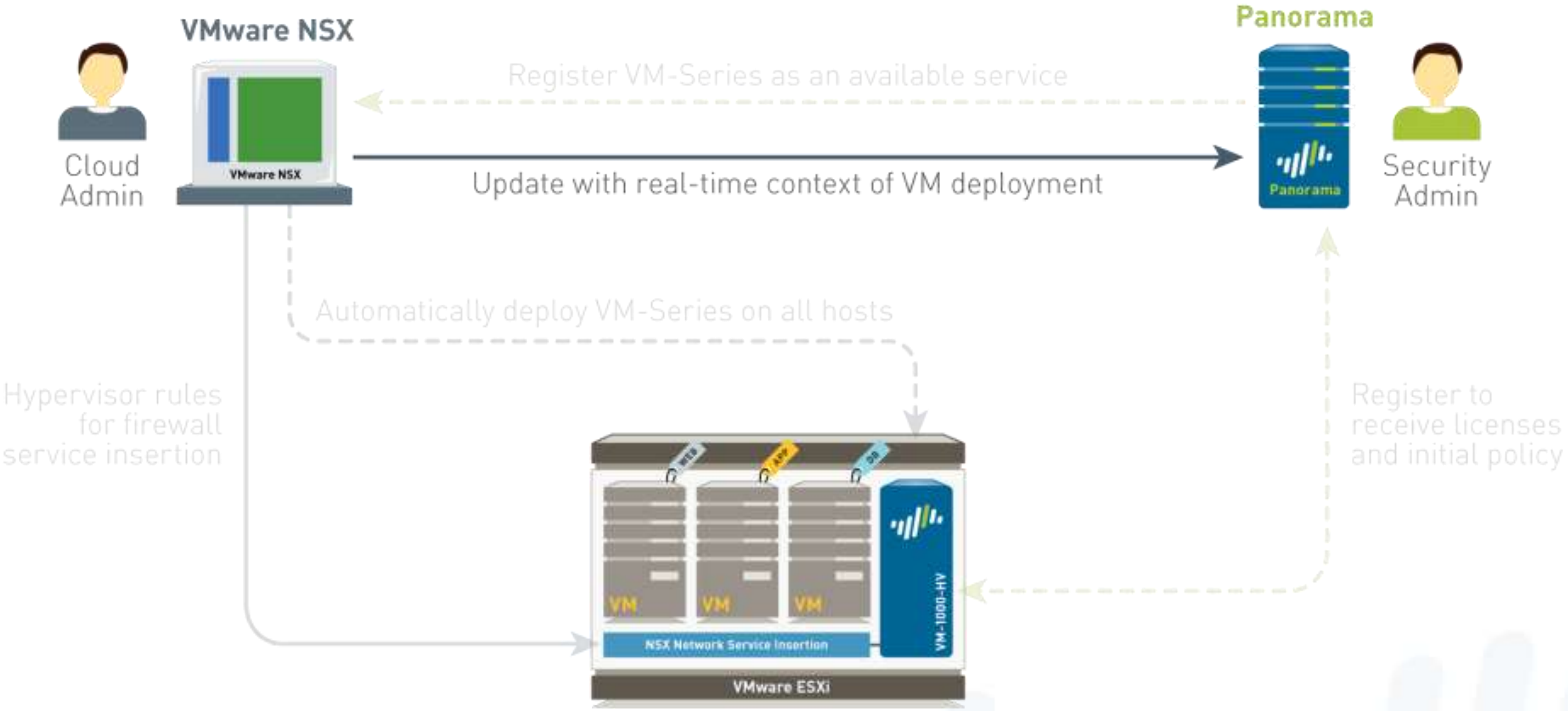
How it works: NSX Mgr.: Service Composer: Rules



NSX Manager: 10.31.32.216

Rank	Name	Description	Applied to	Network Introspection Services
1	SharePoint-to-MSSQL	Steer traffic b/w SharePoint and MSSQL servers	1	2
2	WebFrontEnd-to-SharePoint	Steer traffic b/w WebFrontEnd and SharePoint servers	1	2
3	ActiveDirectory-to-AllTiers	Steer all traffic b/w any tier and ActiveDirectory servers	1	2

How it works: Real-time updates



VMware NSX

Panorama

Cloud Admin

Security Admin

Register VM-Series as an available service

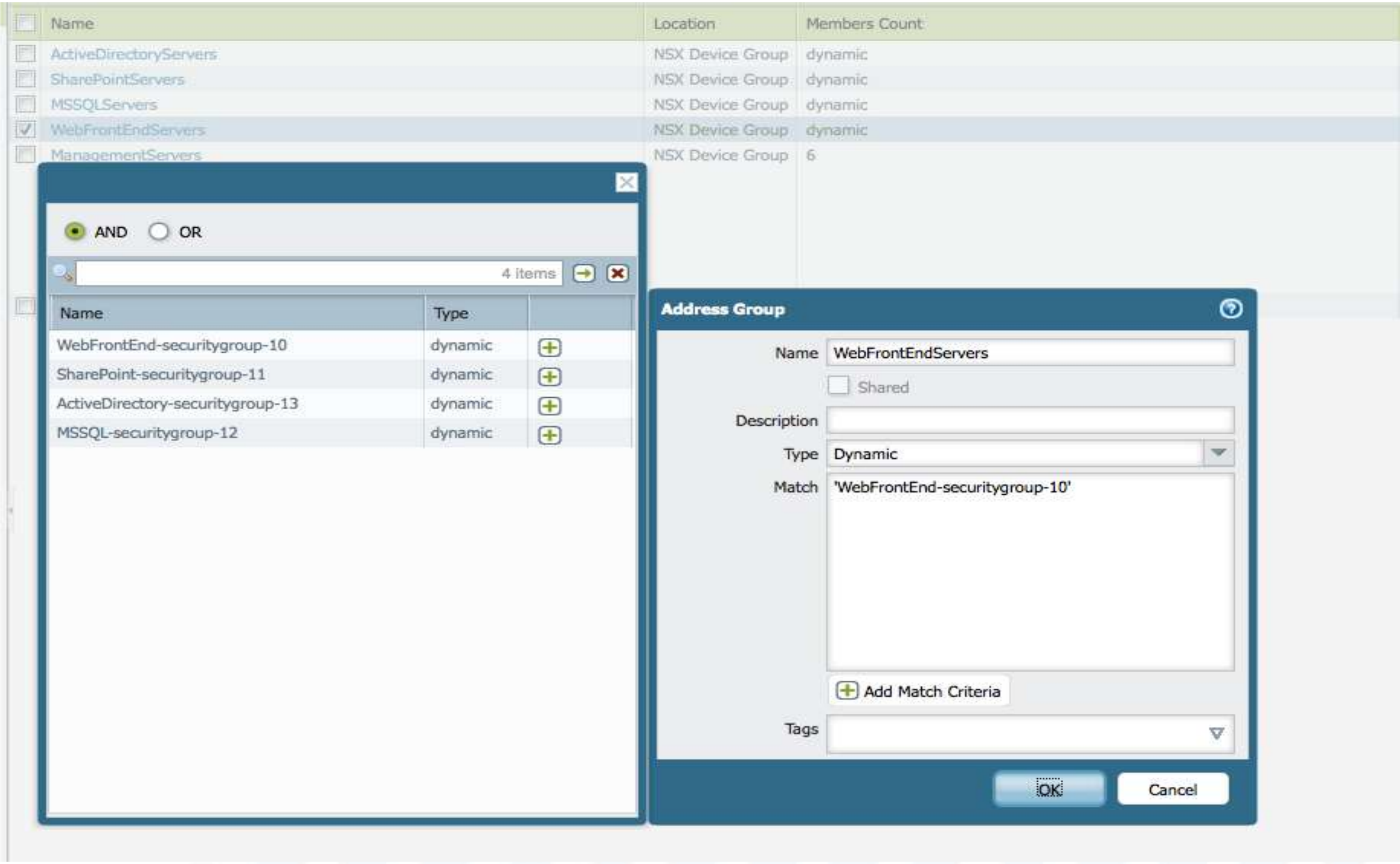
Update with real-time context of VM deployment

Automatically deploy VM-Series on all hosts

Hypervisor rules for firewall service insertion

Register to receive licenses and initial policy

How it works: Panorama: Dynamic Address Groups



□	Name	Location	Members Count
□	ActiveDirectoryServers	NSX Device Group	dynamic
□	SharePointServers	NSX Device Group	dynamic
□	MSSQLServers	NSX Device Group	dynamic
☑	WebFrontEndServers	NSX Device Group	dynamic
□	ManagementServers	NSX Device Group	6

● AND ○ OR

4 items

Name	Type	
WebFrontEnd-securitygroup-10	dynamic	⊞
SharePoint-securitygroup-11	dynamic	⊞
ActiveDirectory-securitygroup-13	dynamic	⊞
MSSQL-securitygroup-12	dynamic	⊞

Address Group

Name: WebFrontEndServers

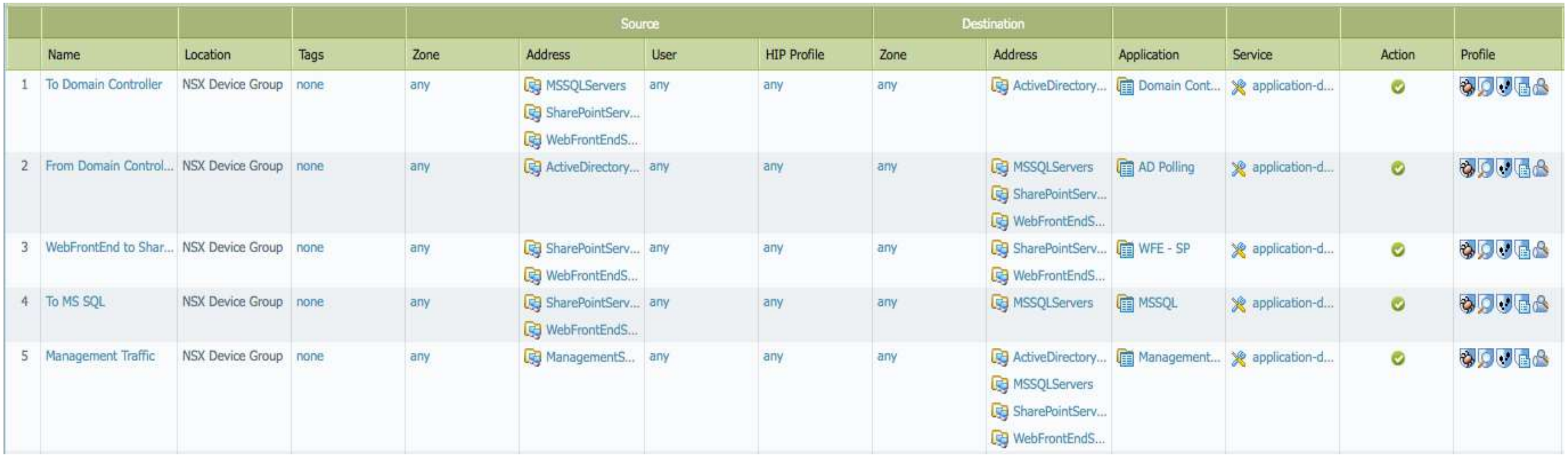
□ Shared

Description:

Type: Dynamic

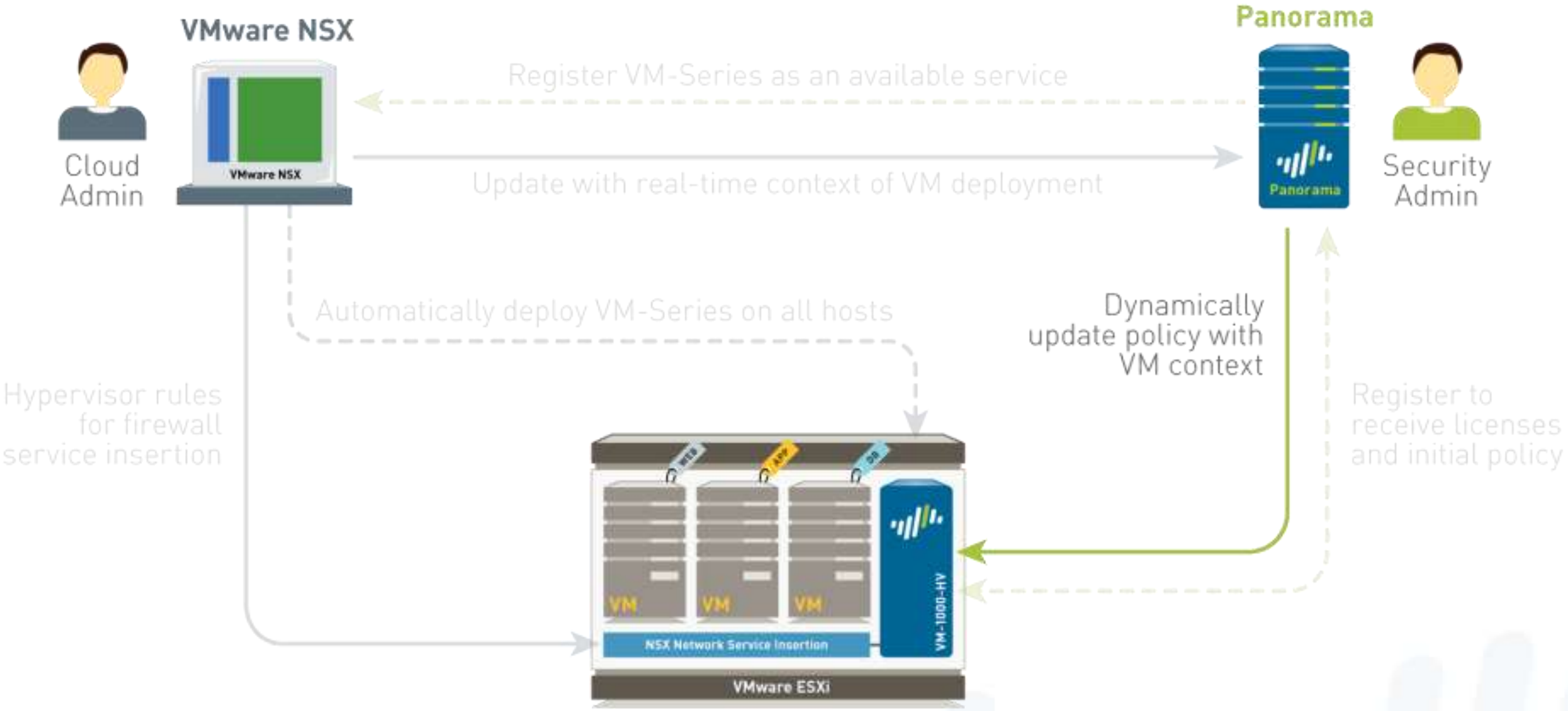
Match: 'WebFrontEnd-securitygroup-10'

How it works: Panorama: Security Policies



				Source				Destination					
	Name	Location	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile
1	To Domain Controller	NSX Device Group	none	any	MSSQLServers SharePointServ... WebFrontEndS...	any	any	any	ActiveDirectory...	Domain Cont...	application-d...	✓	
2	From Domain Control...	NSX Device Group	none	any	ActiveDirectory...	any	any	any	MSSQLServers SharePointServ... WebFrontEndS...	AD Polling	application-d...	✓	
3	WebFrontEnd to Shar...	NSX Device Group	none	any	SharePointServ... WebFrontEndS...	any	any	any	SharePointServ... WebFrontEndS...	WFE - SP	application-d...	✓	
4	To MS SQL	NSX Device Group	none	any	SharePointServ... WebFrontEndS...	any	any	any	MSSQLServers	MSSQL	application-d...	✓	
5	Management Traffic	NSX Device Group	none	any	ManagementS...	any	any	any	ActiveDirectory... MSSQLServers SharePointServ... WebFrontEndS...	Management...	application-d...	✓	

How it works: Dynamic Addr. Groups: Address Updates



Register VM-Series as an available service

Update with real-time context of VM deployment

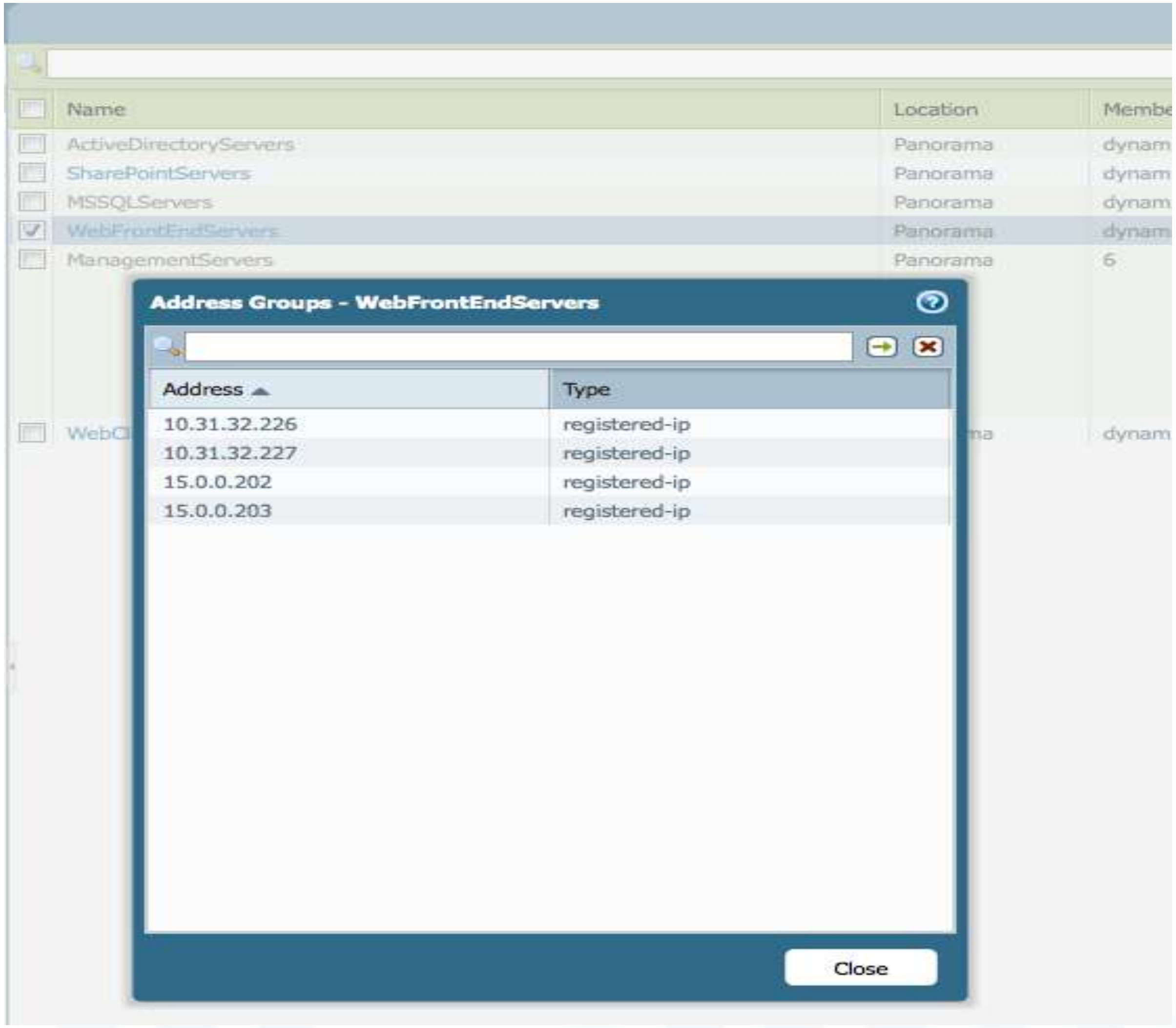
Automatically deploy VM-Series on all hosts

Dynamically update policy with VM context

Hypervisor rules for firewall service insertion

Register to receive licenses and initial policy

How it works: VM-Series: Dynamic Address Groups



☐	Name	Location	Membe
☐	ActiveDirectoryServers	Panorama	dynam
☐	SharePointServers	Panorama	dynam
☐	MSSQLServers	Panorama	dynam
☑	WebFrontEndServers	Panorama	dynam
☐	ManagementServers	Panorama	6
☐	WebCl	na	dynam

Address Groups - WebFrontEndServers

Address ▲	Type
10.31.32.226	registered-ip
10.31.32.227	registered-ip
15.0.0.202	registered-ip
15.0.0.203	registered-ip

Dynamic Address Groups

VMware vCenter or ESXi

Name	IP	Guest OS	Container
web-sjc-01	10.1.1.2	Ubuntu 12.04	Web
sp-sjc-04	10.1.5.4	Win 2008 R2	SharePoint
web-sjc-02	10.1.1.3	Ubuntu 12.04	Web
exch-mia-03	10.4.2.2	Win 2008 R2	Exchange
exch-dfw-03	10.4.2.3	Win 2008 R2	Exchange
sp-mia-07	10.1.5.8	Win 2008 R2	SharePoint
db-mia-01	10.5.1.5	Ubuntu 12.04	MySQL
db-dfw-02	10.5.1.2	Ubuntu 12.04	MySQL
db-mia-05	10.5.1.9	Ubuntu 12.04	MySQL

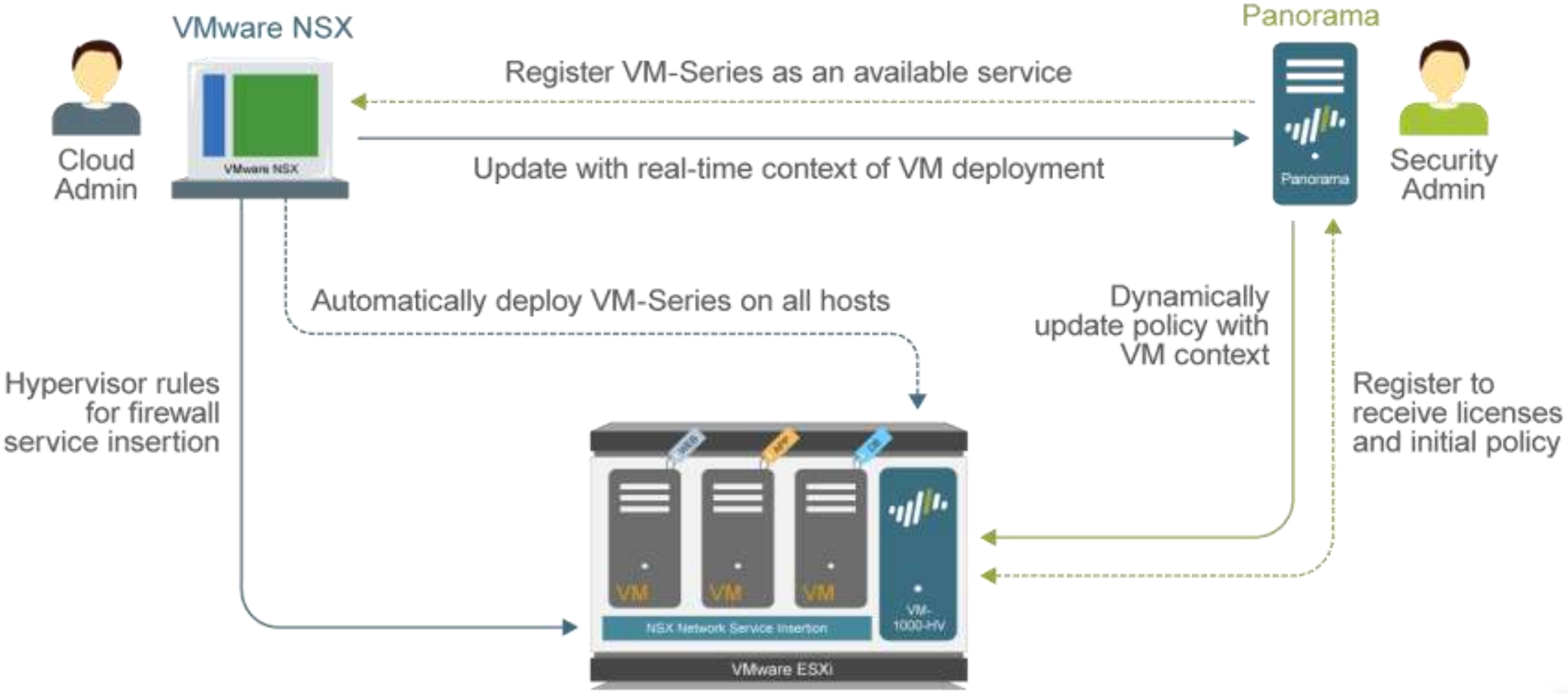
PAN-OS Dynamic Address Groups

Name	Tags	Addresses
SharePoint Servers	SharePoint Win 2008 R2 “sp”	10.1.5.4 10.1.5.8
MySQL Servers	MySQL Ubuntu 12.04 “db”	10.5.1.5 10.5.1.2 10.5.1.9
Miami DC	“mia”	10.4.2.2 10.1.5.8 10.5.1.5
San Jose Linux Web Servers	“sjc” “web” Ubuntu 12.04	10.1.1.2 10.1.1.3

PAN-OS Security Policy

Source	Destination	Action
SharePoint Servers	San Jose Linux Web Servers	✓
MySQL Servers	Miami DC	⊘

How it works: The Complete Picture



VMware NSX

Panorama

Cloud Admin

Security Admin

Register VM-Series as an available service

Update with real-time context of VM deployment

Automatically deploy VM-Series on all hosts

Hypervisor rules for firewall service insertion

Dynamically update policy with VM context

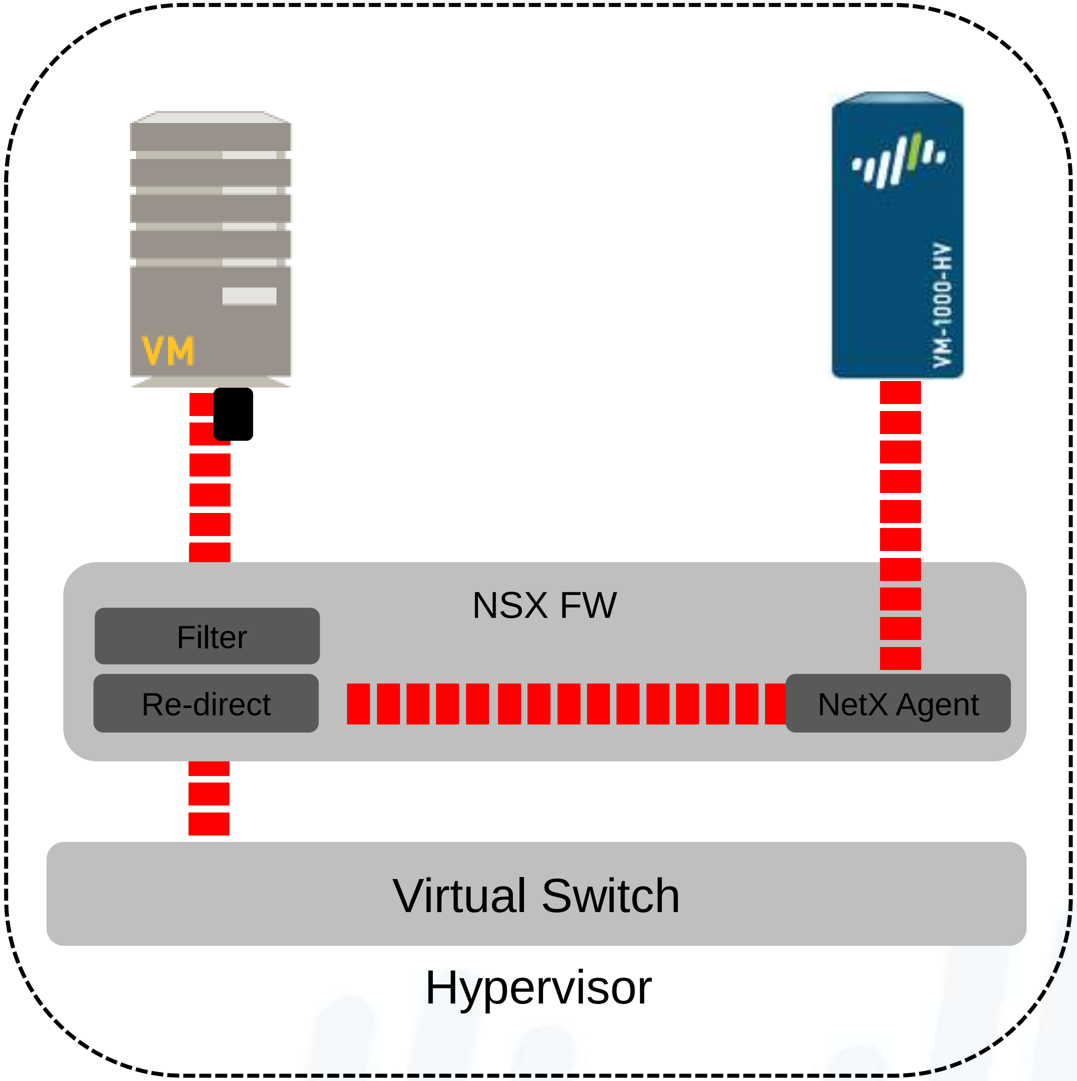
Register to receive licenses and initial policy

VM Monitoring – ESXi & vCenter Dynamic Tags

VM Monitoring Tags			
Tag Name	Format	Tag Name	Format
UUID for VM instance	uuid.<uuid sring>	**VLAN ID**	vlanId.<VLAN ID>
VM Instance Name	vmname.<name string>	**VM Info Source**	vm-info-source.<name string>
Gurest OS	guestos.<guset OS name>	**Datacenter Object Name**	datacenter.<datacenter object name>
VM State	state.<vm power state>	**Resource Pool Name**	resource-pool.<ResourcePool object name>
Annotation	annotation.<annotation string>	**Cluster Object Name**	cluster.<cluster object name>
VM Version	version.<version string>	**Hostname**	hostname.<host name>
Virtual Switch Name	vswitch.<virtual switch name>	**Host IP Address**	host-ip.<host IP address>
Port Group Name	portgroup.<network name>		

Note: all tags generated by VM monitor are normalized before sending to XMLAPI layer. Special characters which are invalid inside a tag on PAN-OS will be removed. Those special characters include single-quota, double-quota, CR, LF, "(", and ")". Also, multiple spaces will be replaced by single space.

How it works: Packet Flow



NSX Firewall installs a dvFilter on Guest VM vNIC

VM-Series firewall is deployed and connected to NSX Firewall

Rules to re-direct traffic VM-Series are configured in NSX

Packet emerging from Guest VM is redirected to VM-Series

VM-Series inspects packet and applies Security Policy

Packet is forwarded to the virtual switch

How it works: VM-Series - Interface Configuration

- Default vWire between Ethernet1/1 and Ethernet1/2
- Both Ethernet1/1 and Ethernet1/2 are in the same Zone
- Outbound traffic from Guest VMs is received on Ethernet1/1 and its forwarded out of Ethernet1/2
- Inbound traffic to Guest VMs is received on Ethernet1/2 and its forwarded out of Ethernet1/1
- An explicit deny policy to ensure default deny behavior is preserved

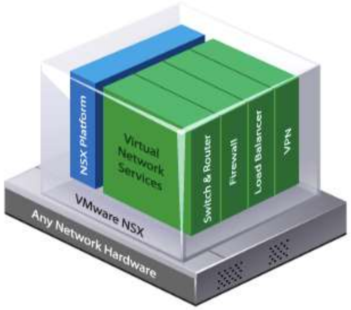
Meeting the needs of both Infrastructure and Security

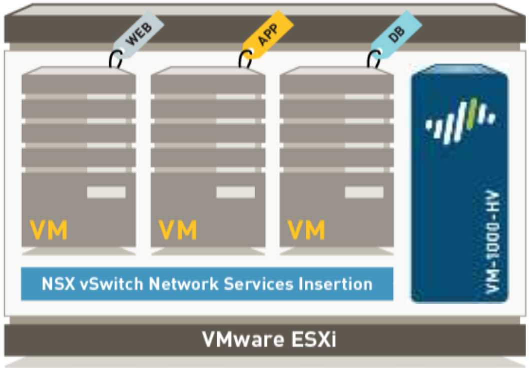
Cloud

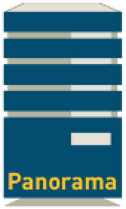
- **Accelerate app deployments** and unlock cloud agility
- **Meet expectations** of security in new operating model

Security

- **Increase visibility** and protection against cyber attacks
- **Maintain** consistent security controls for all DC traffic







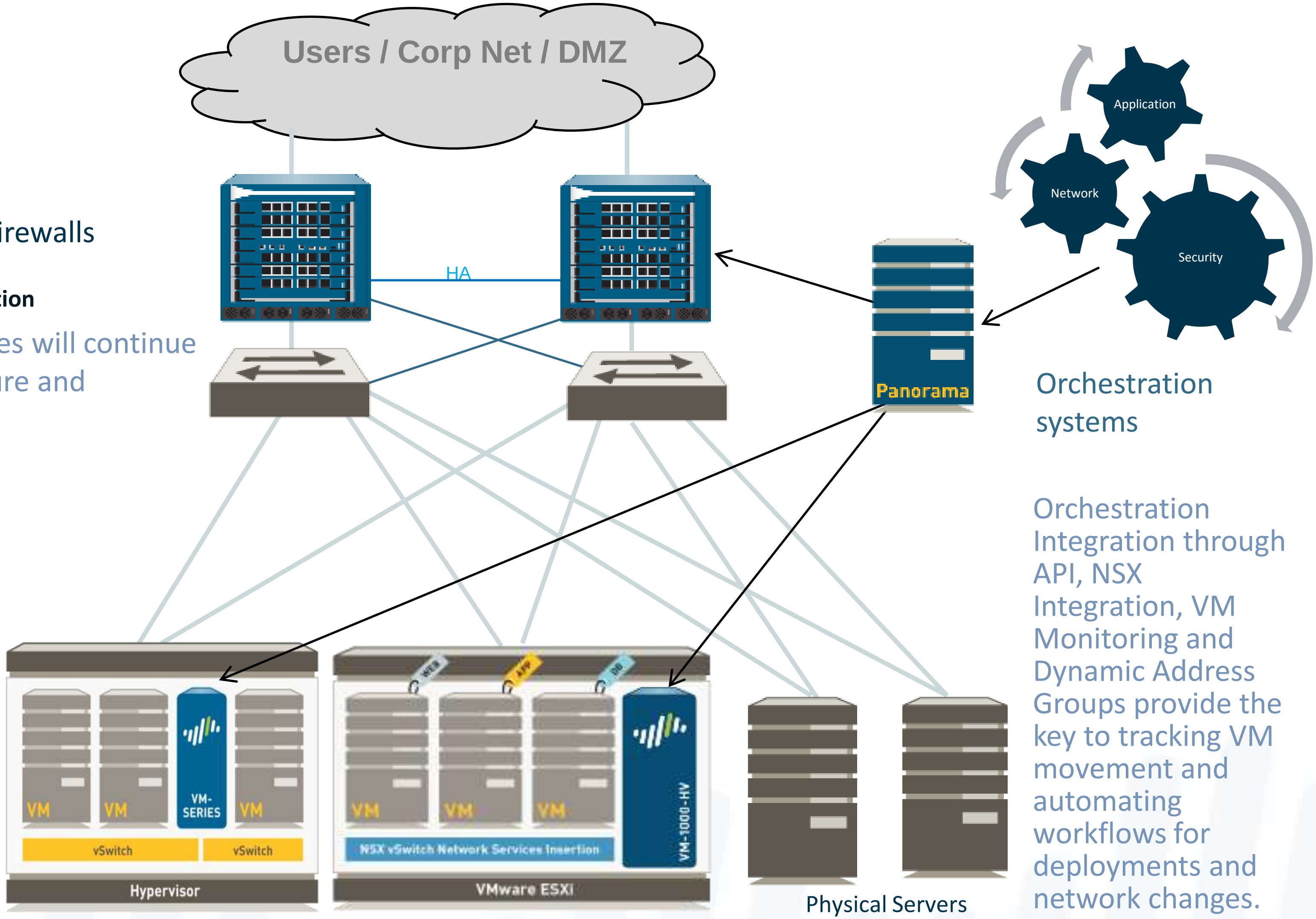
Conclusions

Wrap-up

paloalto NETWORKS

the network security company™

Zero Trust for the Software Defined Data Center



Physical Firewalls

Inter-host Segmentation

Physical security devices will continue to be deployed to secure and segment data centers.

Orchestration systems

Virtualized Firewalls

Intra-host Segmentation

VM-Series provides the ability to safely enable east-west communication

Orchestration Integration through API, NSX Integration, VM Monitoring and Dynamic Address Groups provide the key to tracking VM movement and automating workflows for deployments and network changes.

Physical Servers

Virtualized servers

Ultimate Test Drive Workshop on NSX

- Join us for this hands-on workshop where you'll get experience test-driving the integrated solution.
- You will learn how to:
  - Steer traffic from VMware NSX network virtualization platform to Palo Alto Networks for application of advanced services
  - Create dynamic address groups on the Palo Alto Networks next-generation firewall based on the context from VMware NSX
  - Gain application visibility through the use of VMware NSX traffic steering and Palo Alto Networks App-ID
  - Protect VM to VM communications against advanced threats

paloalto NETWORKS

the network security company™

Alessio Agnello

Pre-Sales System Engineer

aagnello@paloaltonetworks.com