Datacenter Virtualization

Transforming Security for the Software Defined Datacenter

Domenico Stranieri

Pre-Sales System Engineer

dstranieri@paloaltonetworks.com

paloalto NETWORKS

the network security company™

Agenda

- Zero Trust Network – The State of Modern Malware
- Evolution and Security Challenges in the Software Defined Data Center
- VM-Series for VMware NSX
  - Solution Overview
  - How it works
- Open Discussion - Q & A
- Conclusions

What's changed?

THE EVOLUTION OF BUSINESS

SaaS

SOCIAL + CONSUMERIZATION

Massive opportunity for cyber criminals

MOBILITY + BYOD

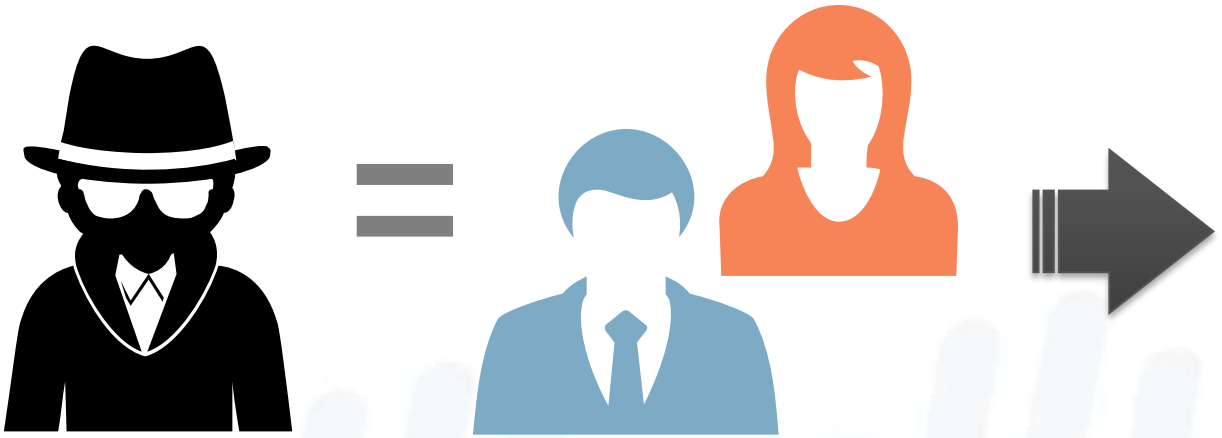
CLOUD + VIRTUALIZATION

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+/

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…

paloalto NETWORKS

Must improve the Security Posture….

Zero Trust Network

“ The path to reducing the Trust Zone

following the path of the attacker “

paloalto NETWORKS

the network security company™

What About Zero Trust Network?

FORRESTER

The Zero Trust Model Of Information Security

The Zero Trust architecture approach, first proposed by **Forrester Research (2009)**, is intended to address this by promoting "**never trust, always verify**" as its guiding principle.

With Zero Trust there is **no default trust for any entity** — including users, devices, applications, and packets — regardless of what it is and its location on or relative to the corporate network.

By establishing Zero Trust boundaries that effectively compartmentalize different segments of the network, you can **protect critical intellectual property** from unauthorized applications or users, **reduce the exposure of vulnerable systems**, and **prevent the lateral movement of malware** throughout your network

paloalto NETWORKS

Zero Trust Network

Zero Trust Concepts

Access control is on a “need-to-know” basis and is strictly enforced.

All resources are accessed in a secure manner regardless of location.

Verify and never trust.

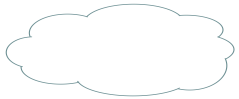
Inspect and log all traffic.

The network is designed from the inside out.

Zero Trust Network

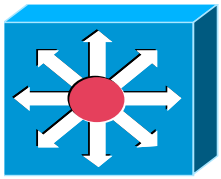
To secure a Multi-Layer Infrastructure is a hard job

Traditional Hierarchal Network

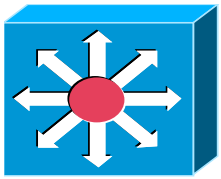


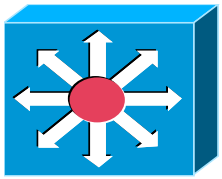
Edge

Core



Distribution



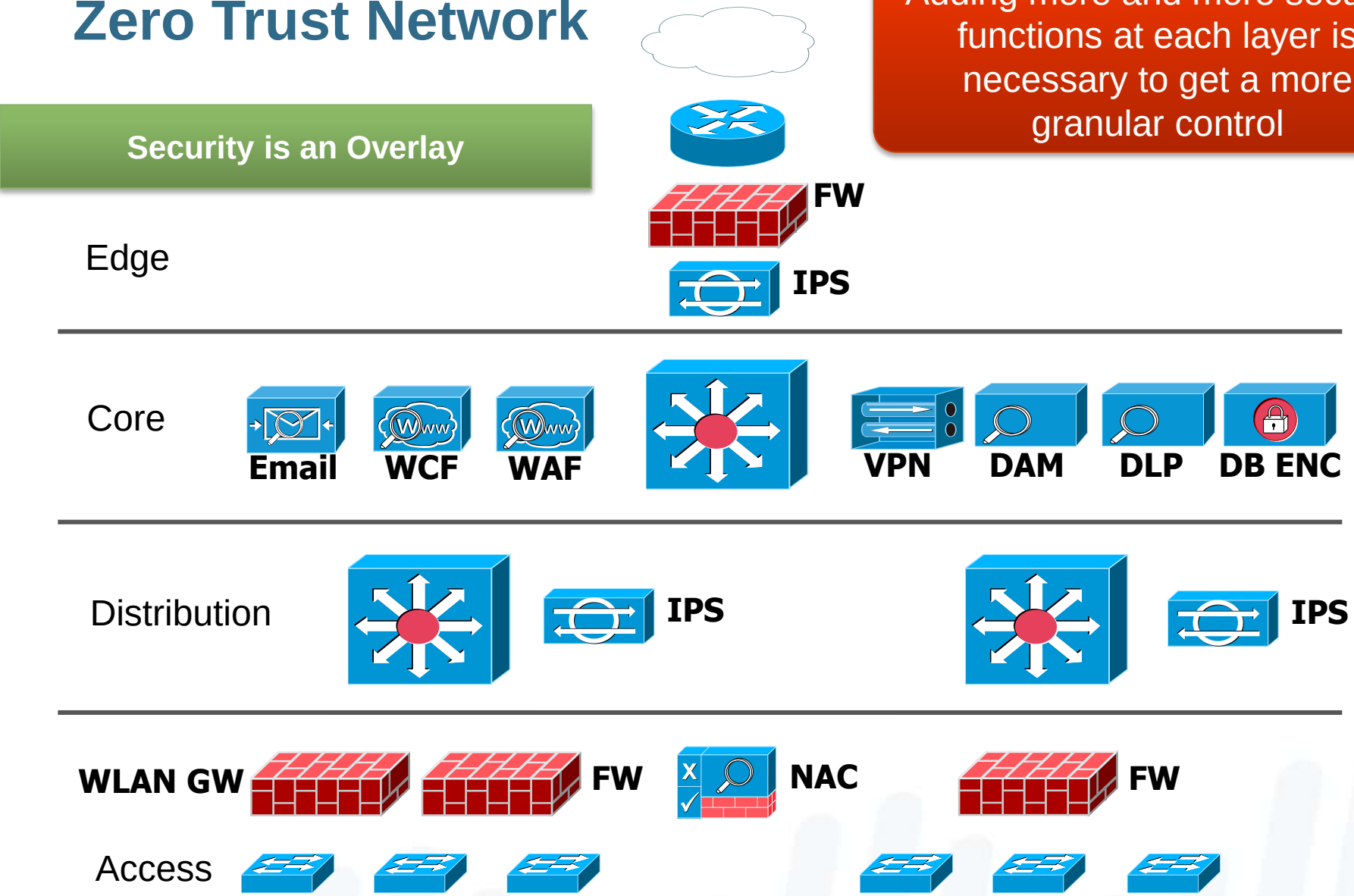


Access

Zero Trust Network

Adding more and more security functions at each layer is necessary to get a more granular control

Security is an Overlay

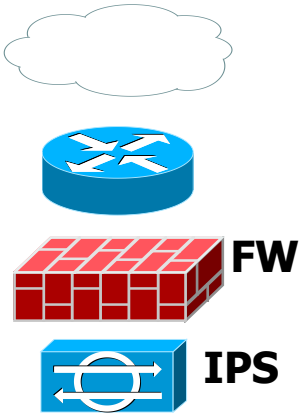


Zero Trust Network

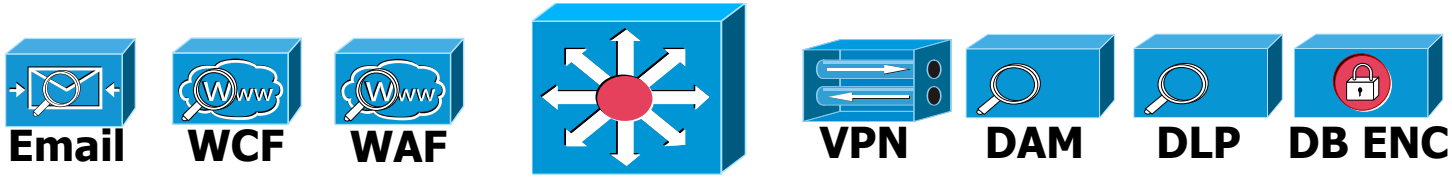
Deconstructing the Network

Having many security functions provided by different components from different Vendors is not really scalable / agile, not easy to manage, and does not provide a natively integrated security platform

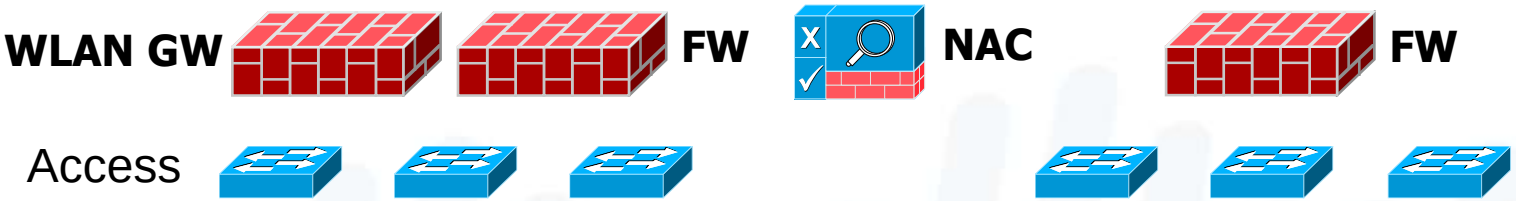
Edge



Core



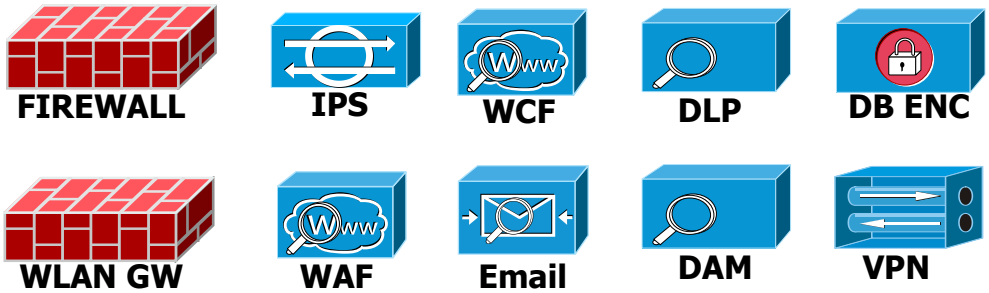
Distribution

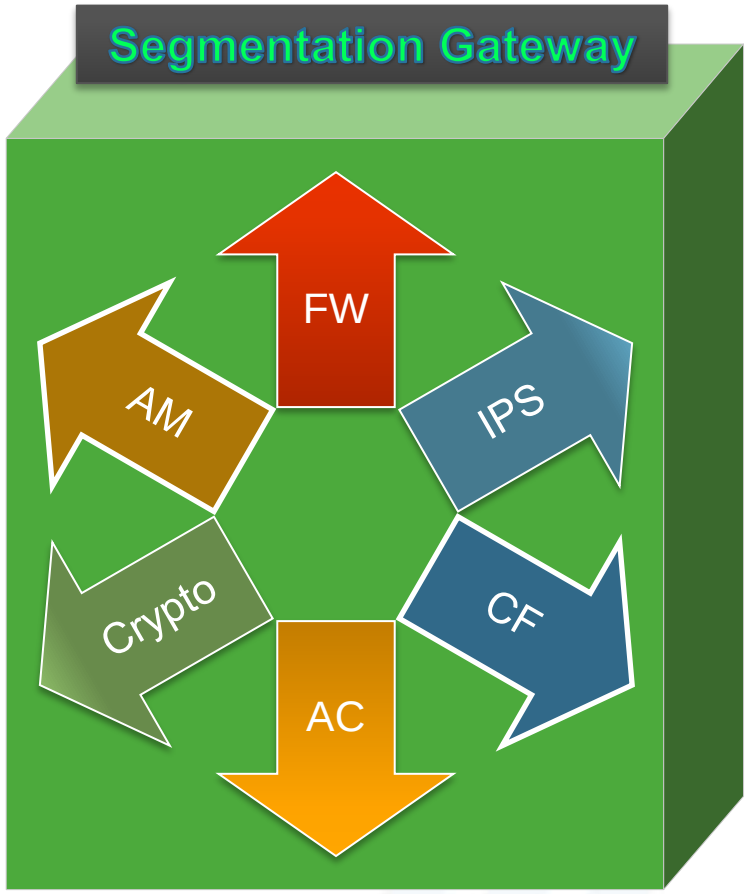


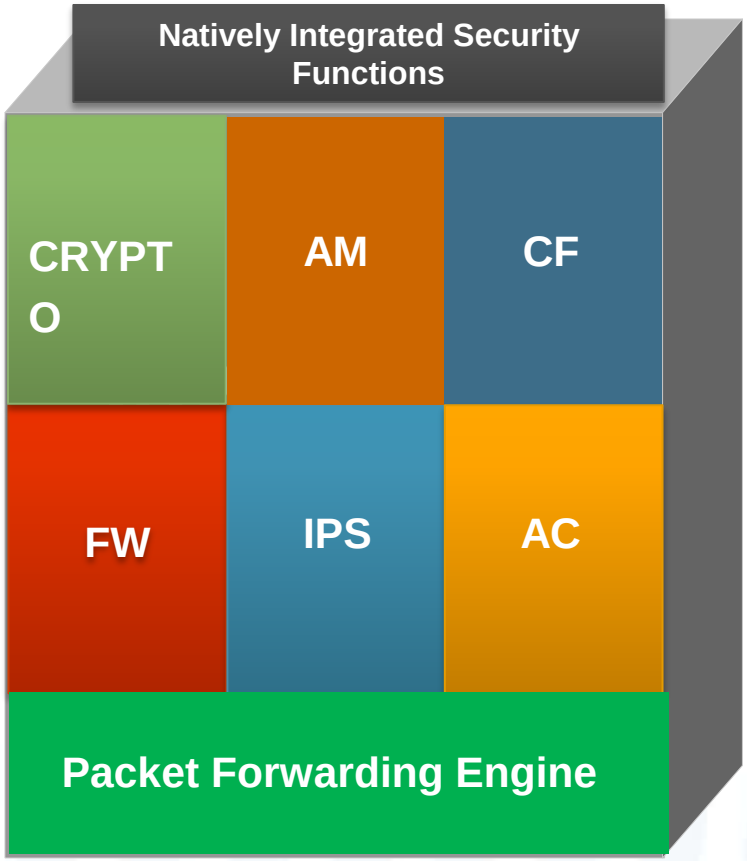
Access

Zero Trust Network

Re-building the Secure Network



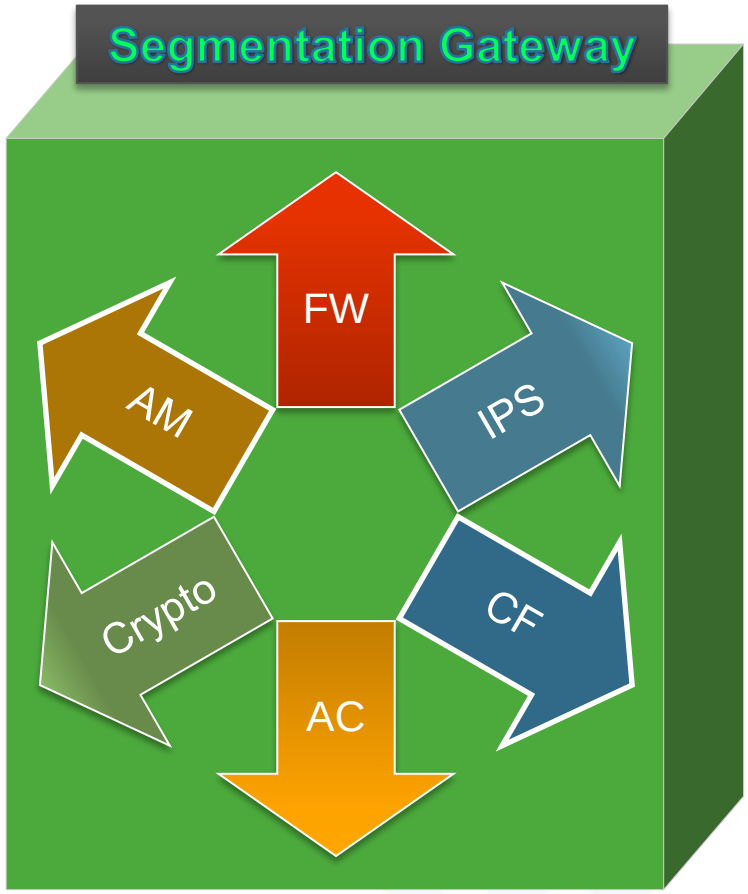




paloalto NETWORKS

Zero Trust Network

Re-building the Secure Network



Next Generation Firewall

Very High Performance
Multiple 10GE Interfaces
Application Awareness
Content Awareness
User Awareness
Known Threats Detection
Unknown Threats Prevention
URL-Filtering
VPN / Access Management
Security Events Logging
Security Events Correlation

paloalto NETWORKS

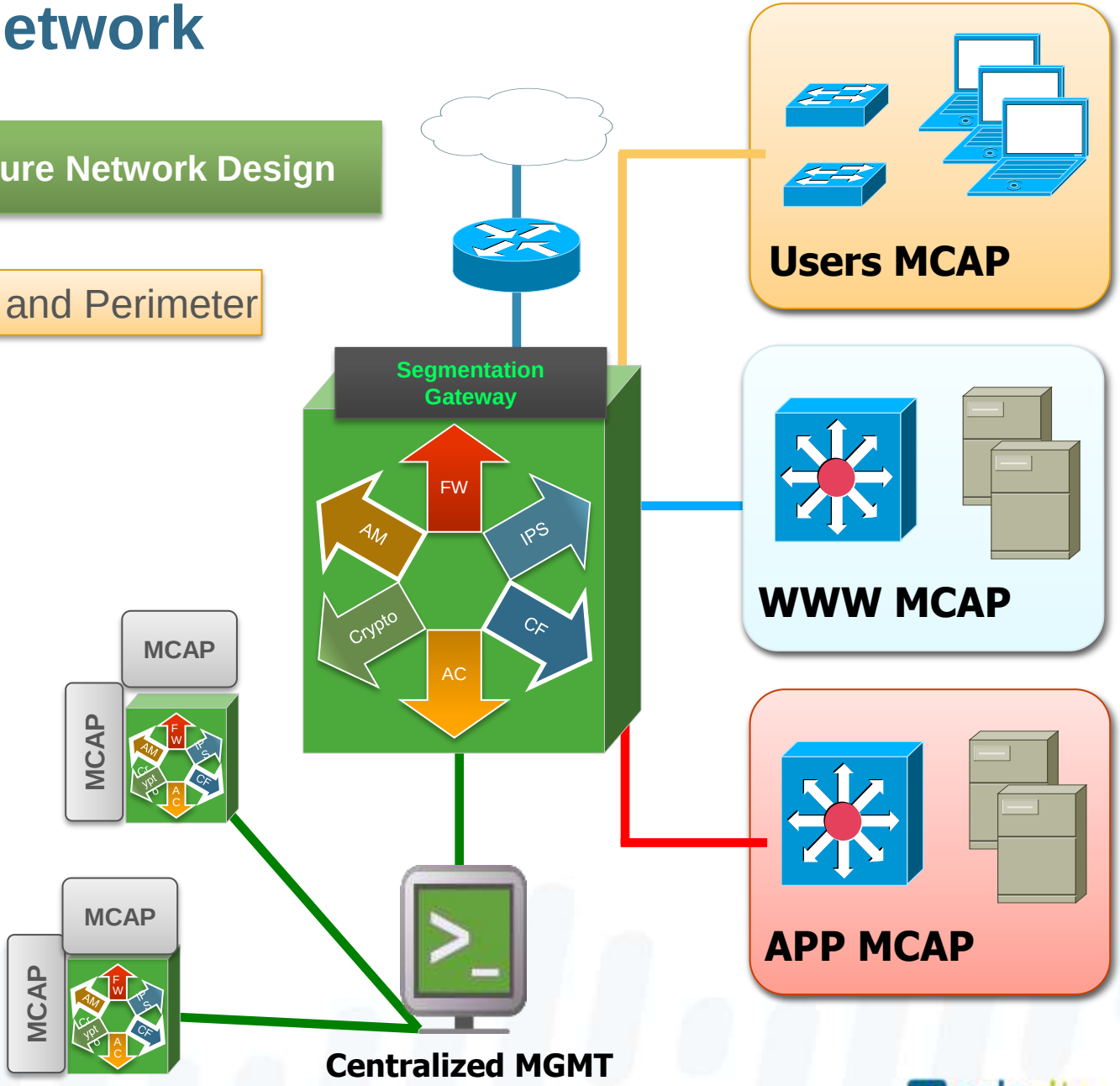
Zero Trust Network

Zero Trust Drives Future Network Design

MCAP – Micro Core and Perimeter

MCAP resources have similar functionality and share global policy attributes

MCAPs are centrally managed to create a unified switching fabric



Evolution and Security Challenges in the Software Defined Data Center

paloalto NETWORKS

the network security company™

Evolution towards a software defined data center

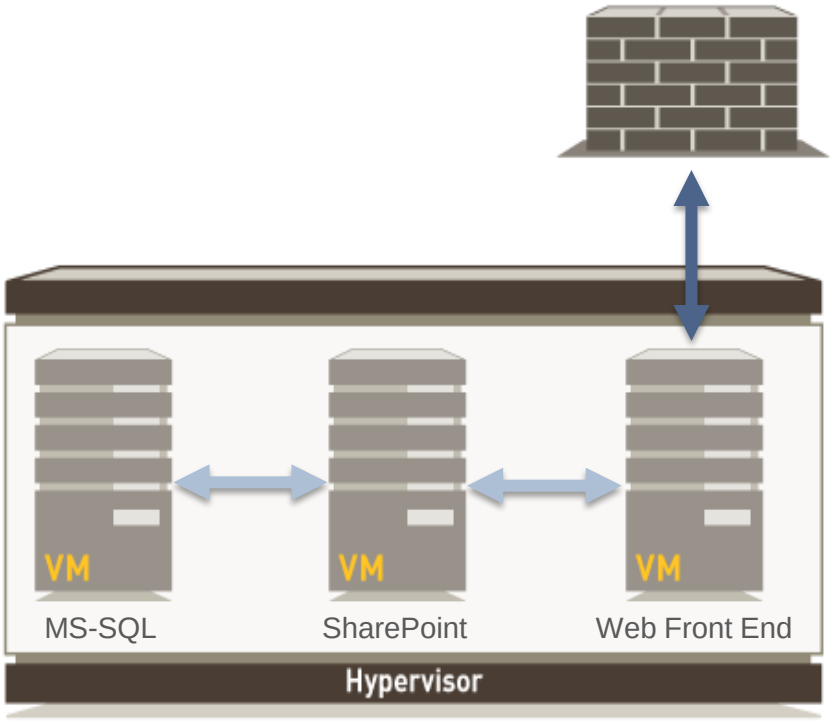
Server Virtualization

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

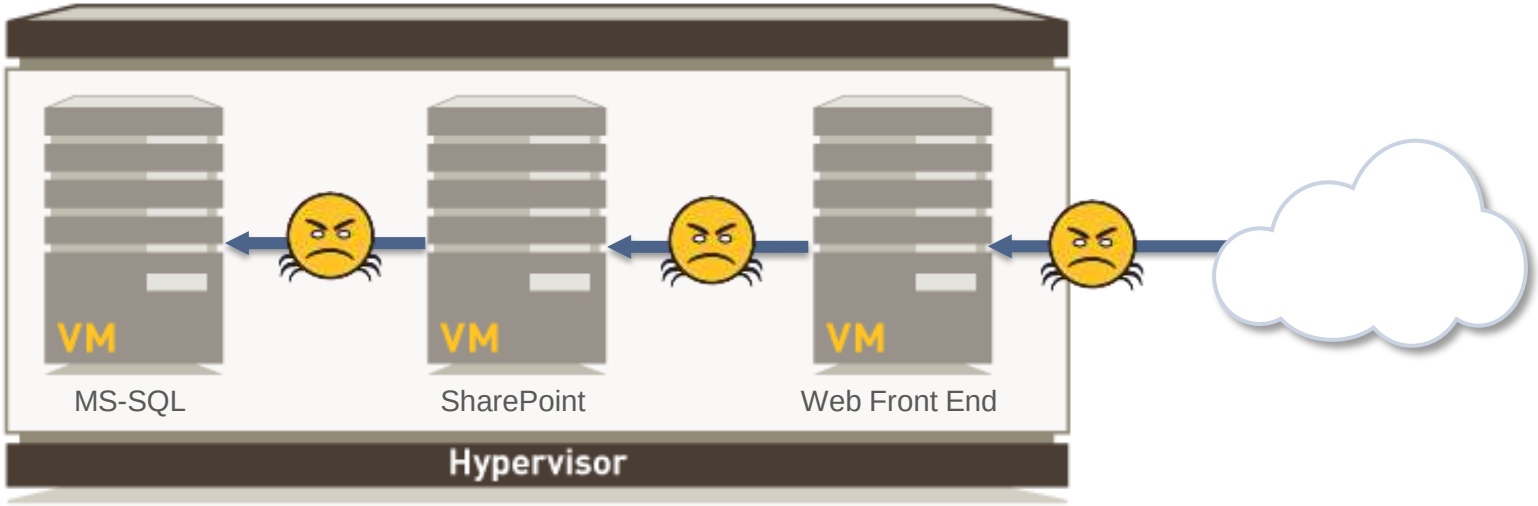
Physical firewalls may not see the East-West traffic



- 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

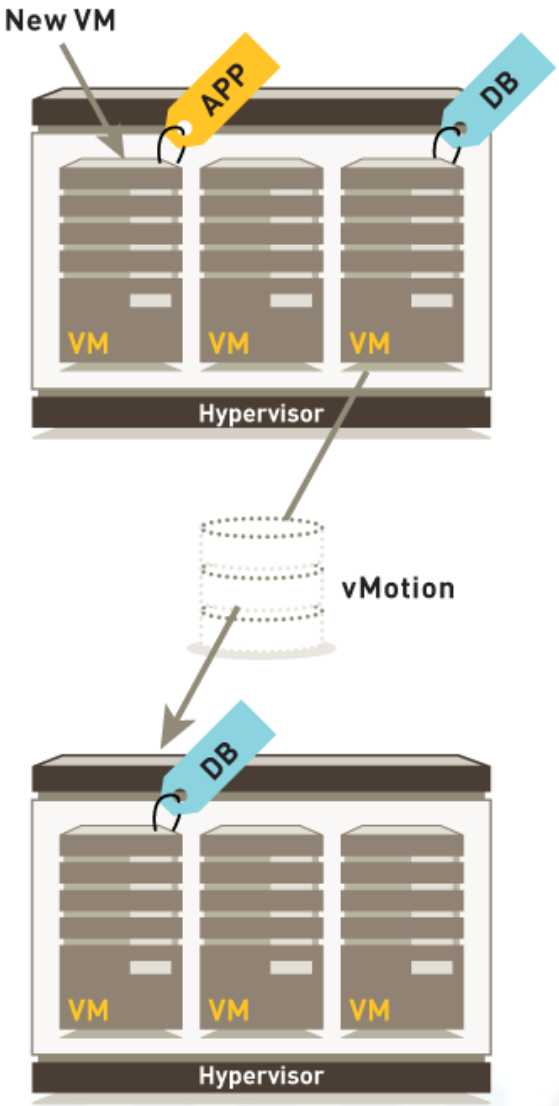


In the cloud, applications of different trust levels now run on a single server

- 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

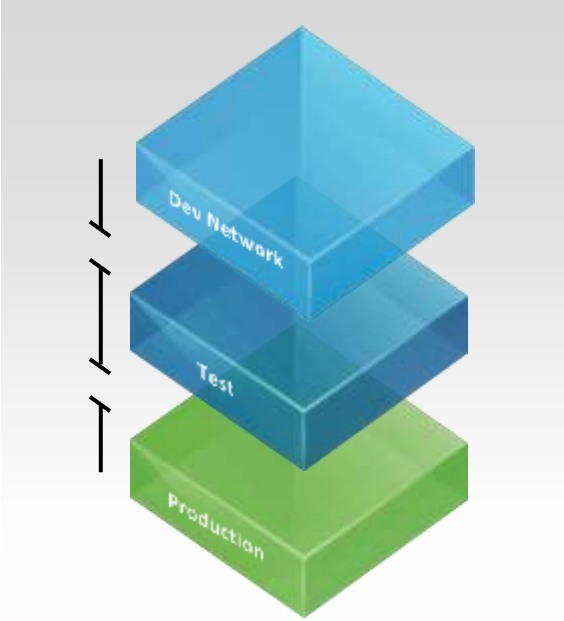
VM-Series for VMware NSX

Solution Overview

the network security company™

Data Center: Micro-segmentation in detail

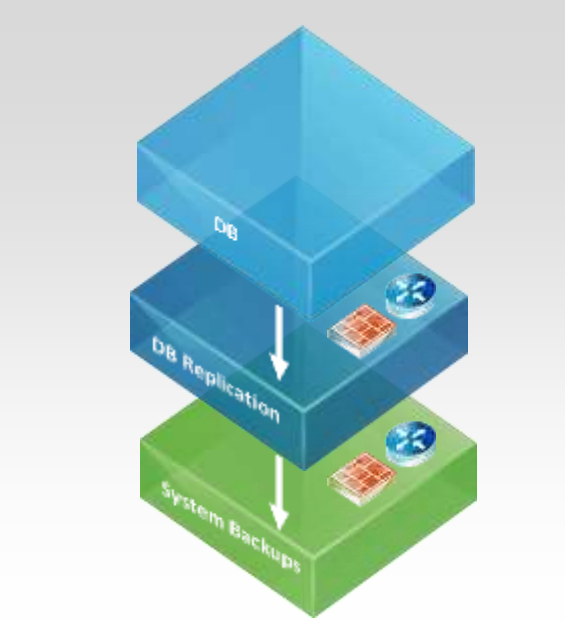
Isolation



No communication path between unrelated networks

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

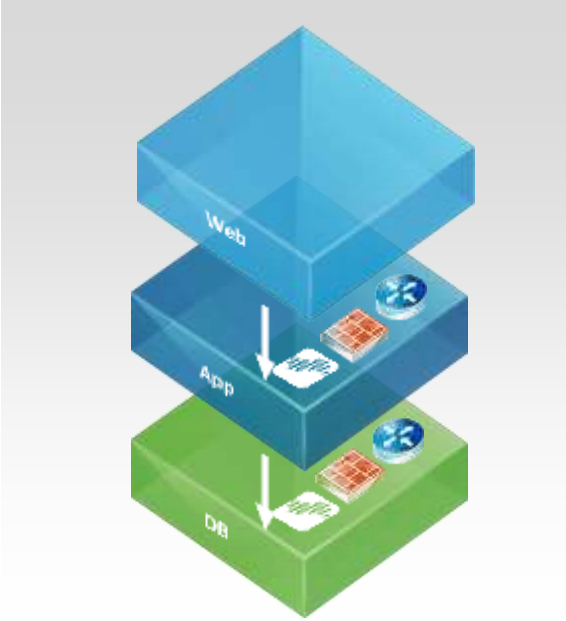
Segmentation



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

paloalto NETWORKS

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

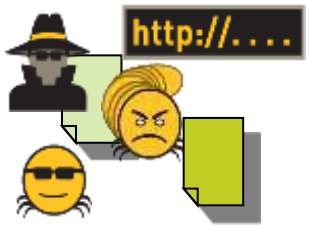
Next Generation Firewall Technologies
Visibility and Safe Enablement of All Traffic

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.

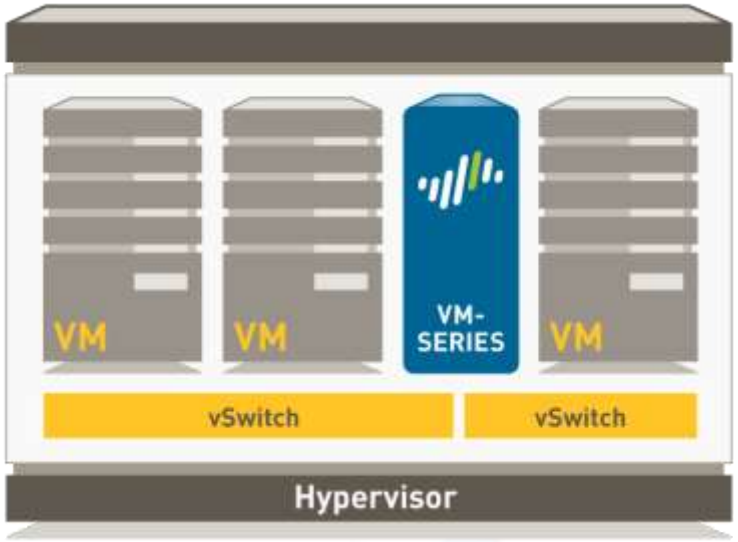
- Protect any type of traffic from targeted attacks

paloalto NETWORKS

NGFW as a VM, versus as a Service

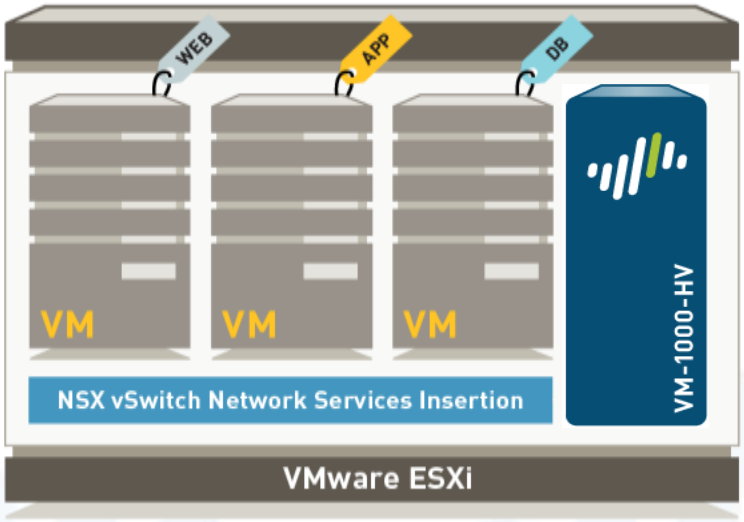
VM-Series as a Guest VM

- 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



Centralized Management and Policy Automation

Panorama

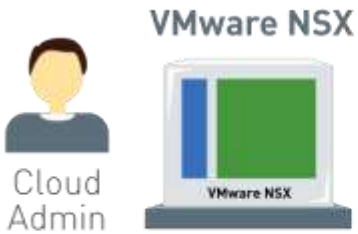
- Global, centralized management of your next-generation firewalls, regardless if they're physical or virtual platforms
- Centralized logging and reporting across all managed devices
- Deploy as VM or via M-100 appliance
- Scalability – Managing up to 1000 Next-Gen Firewalls
- Delegate administrative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

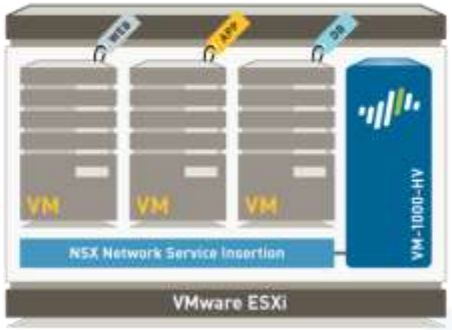
VM-Series for VMware NSX

How it works

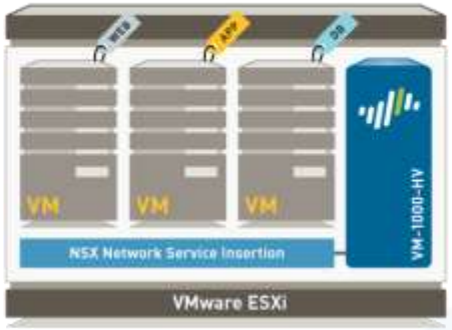
the network security company™

How it works: The joint solution components





How it works: Registration



How it works: Panorama

VMware Service Manager

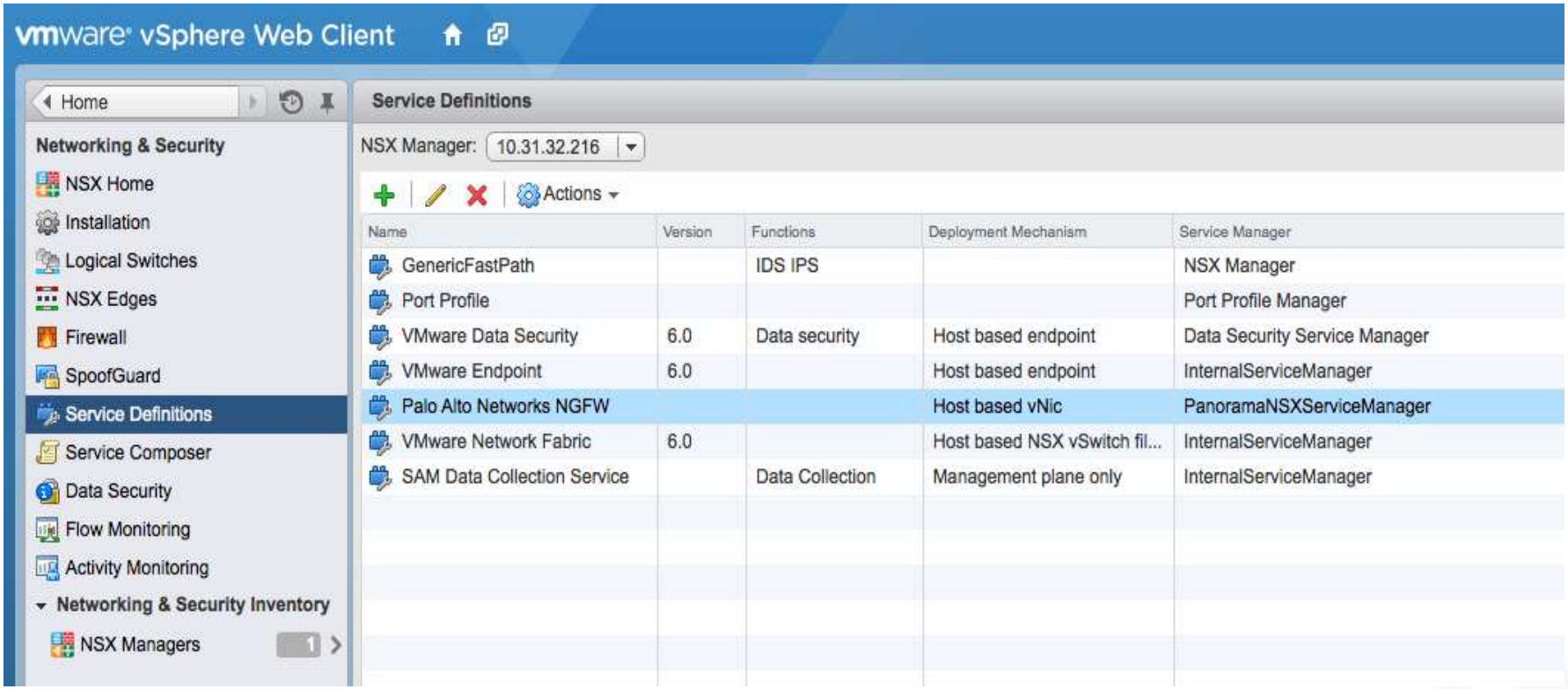
Service Manager Name	PanoramaNSXServiceManager
Description	Registration to NSX of Next Gen Firewall service
NSX Manager URL	https://10.31.32.216/
NSX Manager Login	securityadmin
VM-Series OVF URL	http://10.31.32.217/ovf/PA-VM-NSX-6.0.0-b39.ovf
Authorization Code	I5111353
Template	NSX-MGR-Template
Device 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

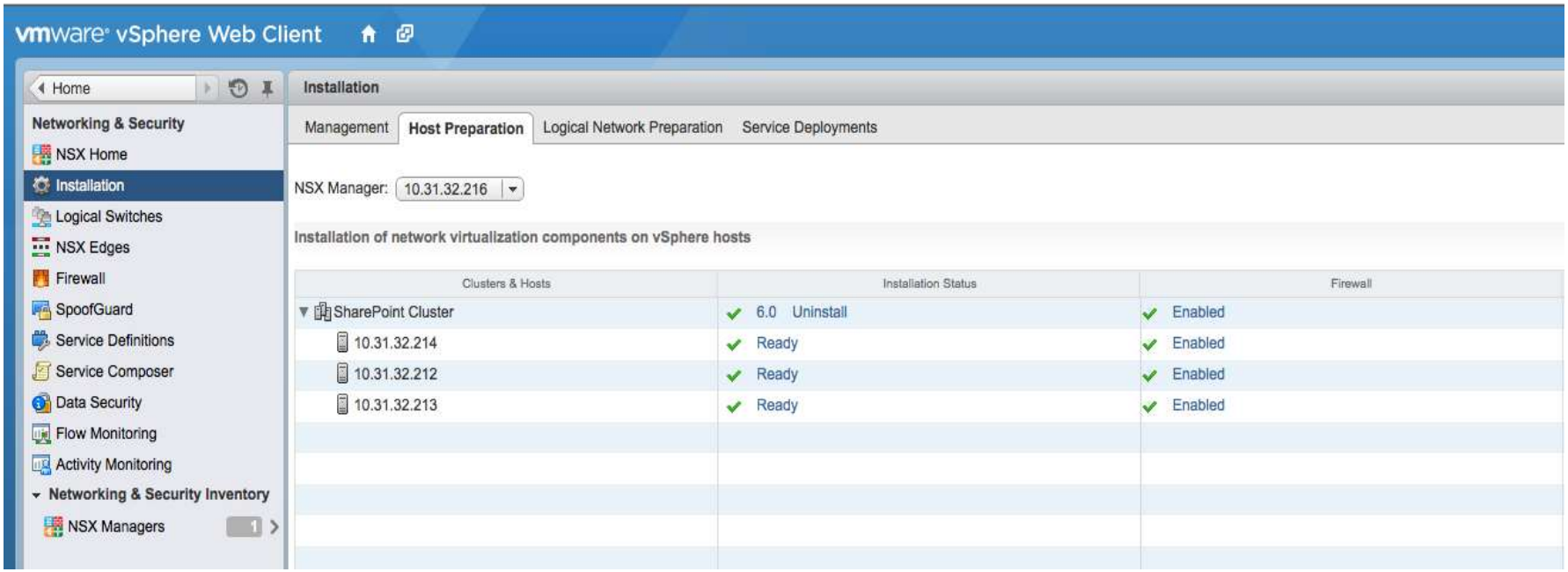
Remove VMware Service Manager

How it works: VMware NSX Manager

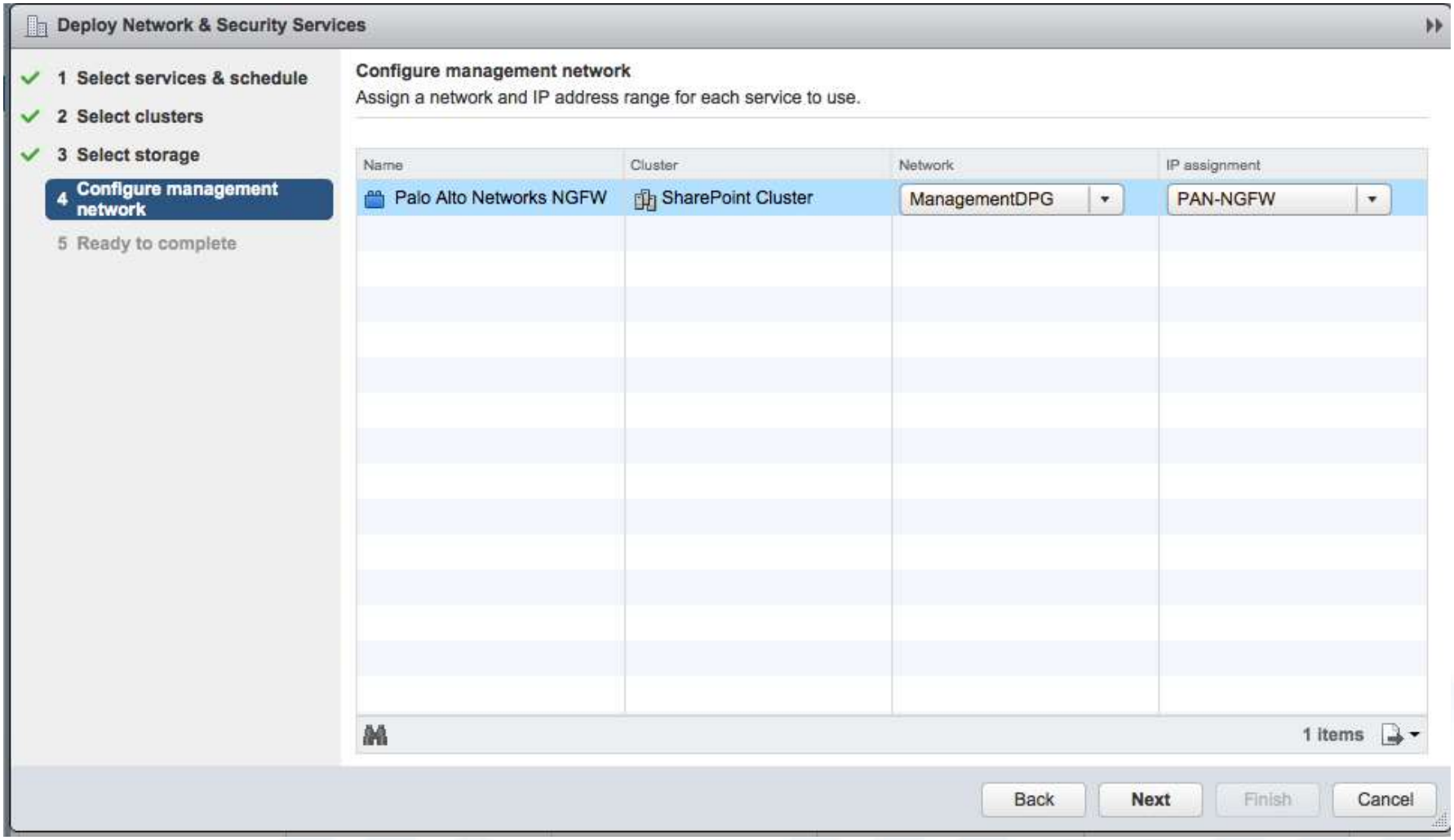


How it works: Deployment

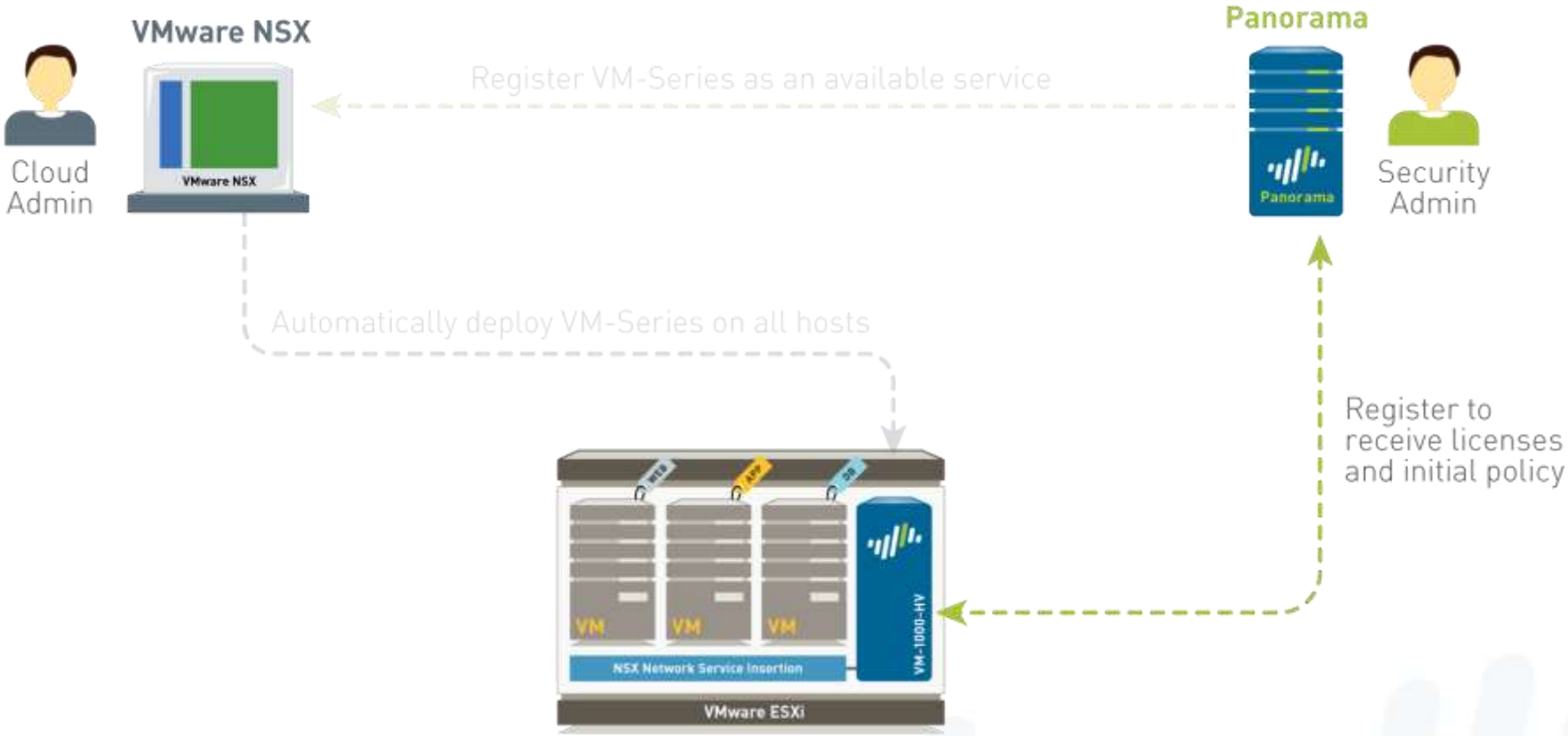
How it works: NSX Manager



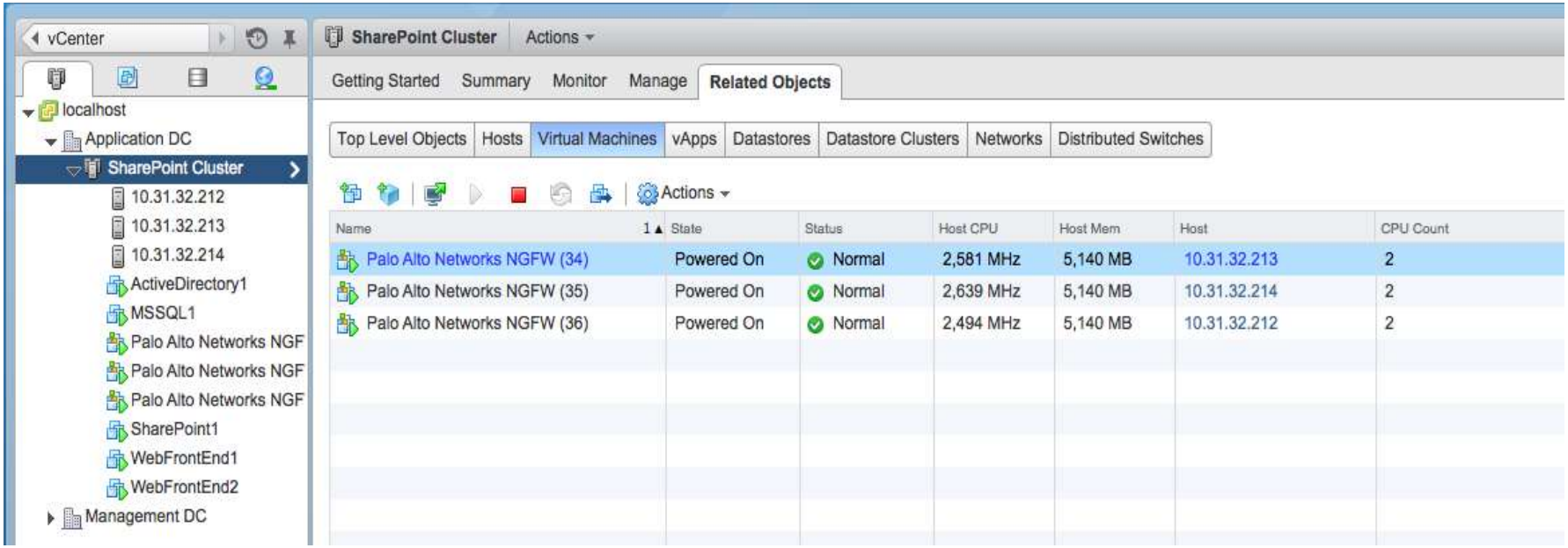
How it works: NSX Manager



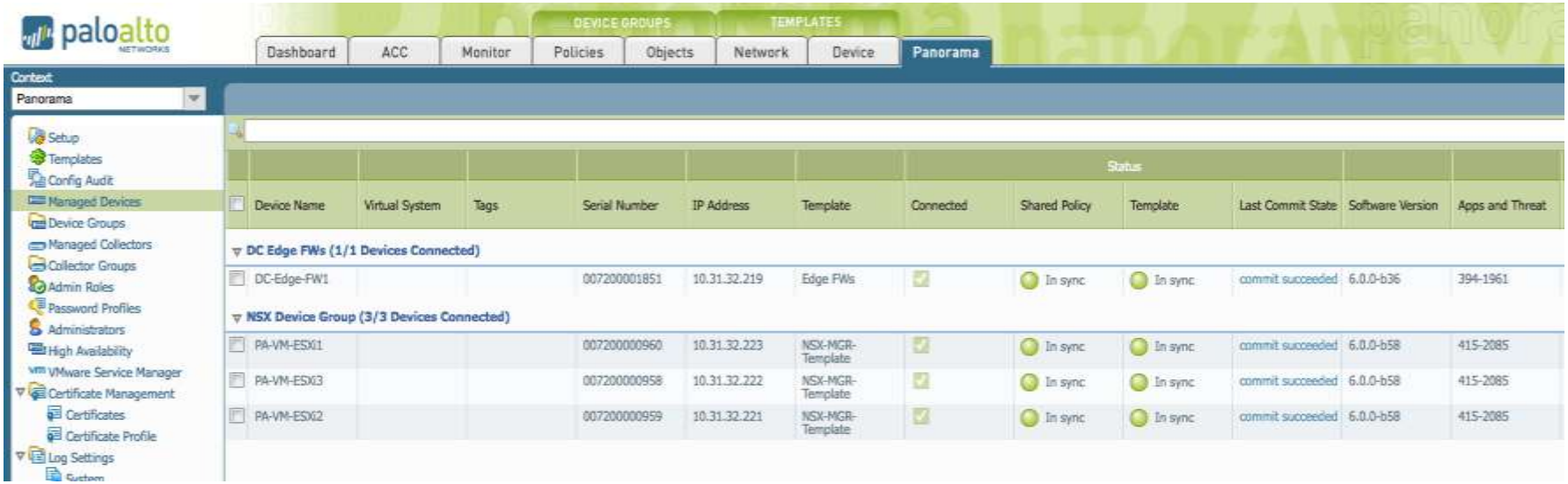
How it works: Licensing and Configuration



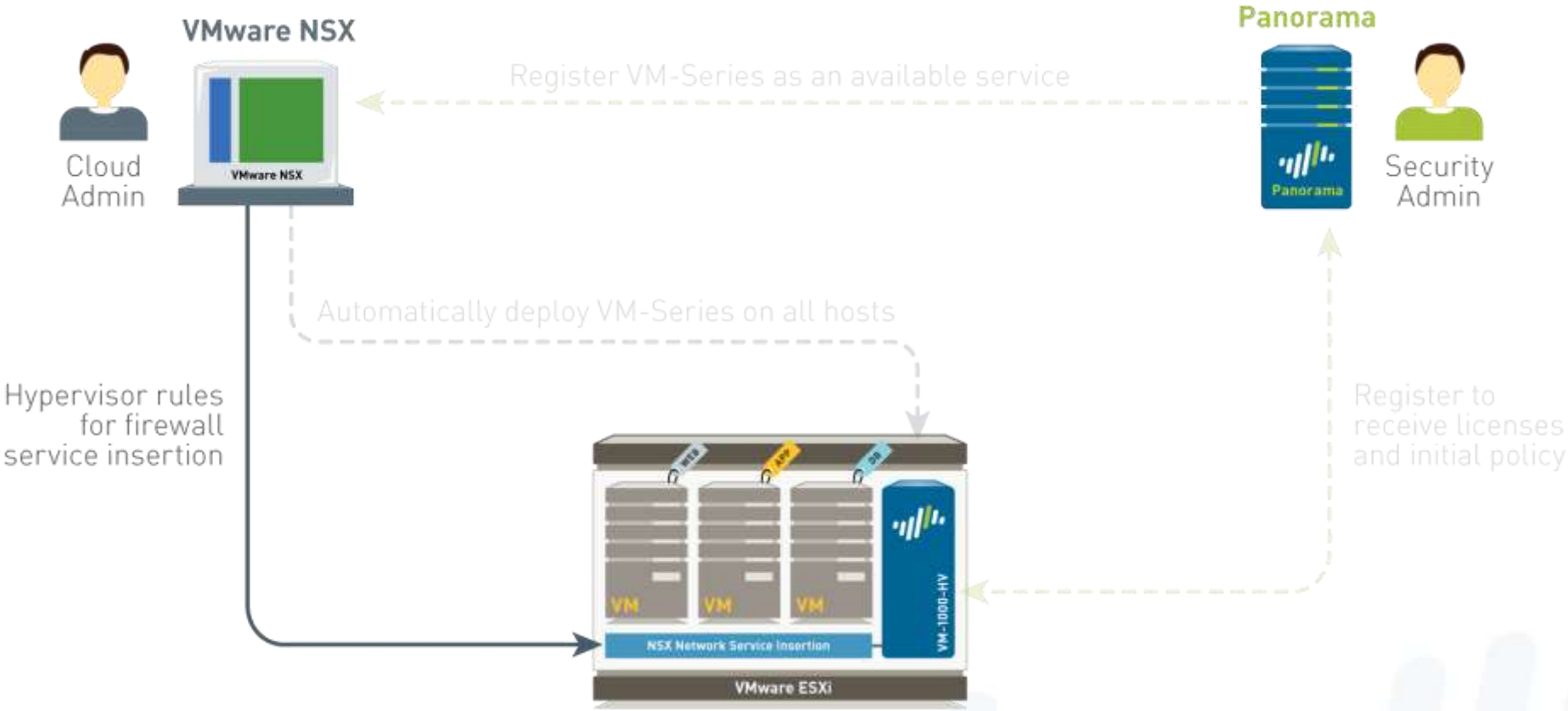
How it works: VMware vCenter



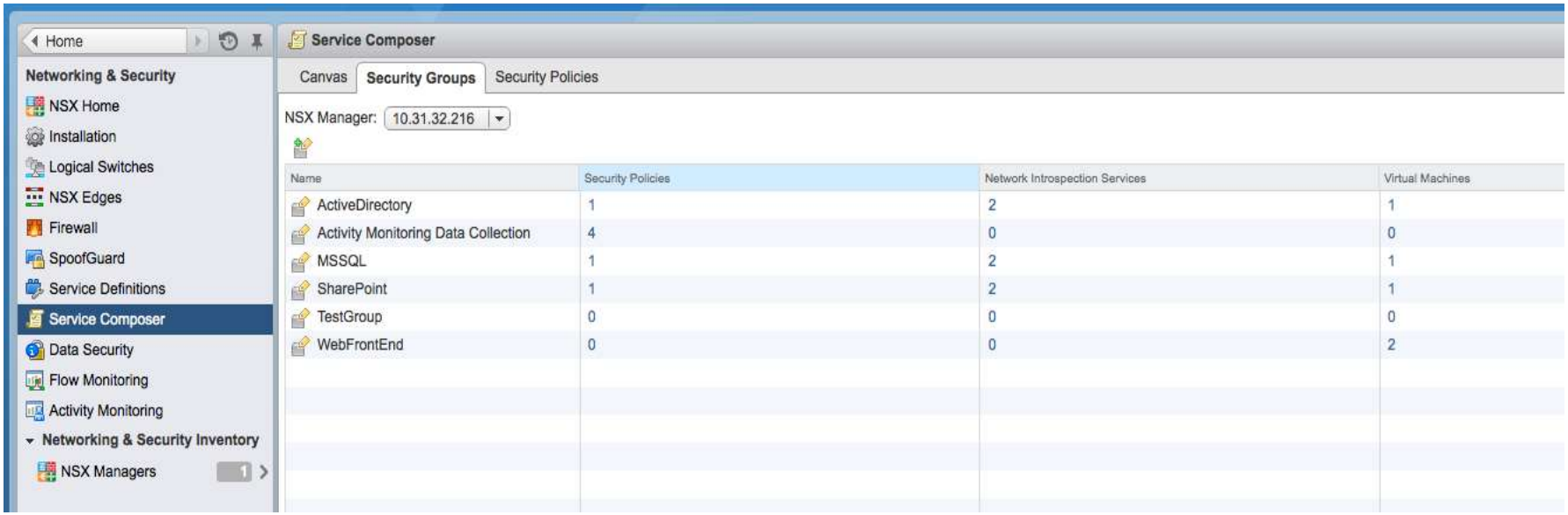
How it works: Panorama



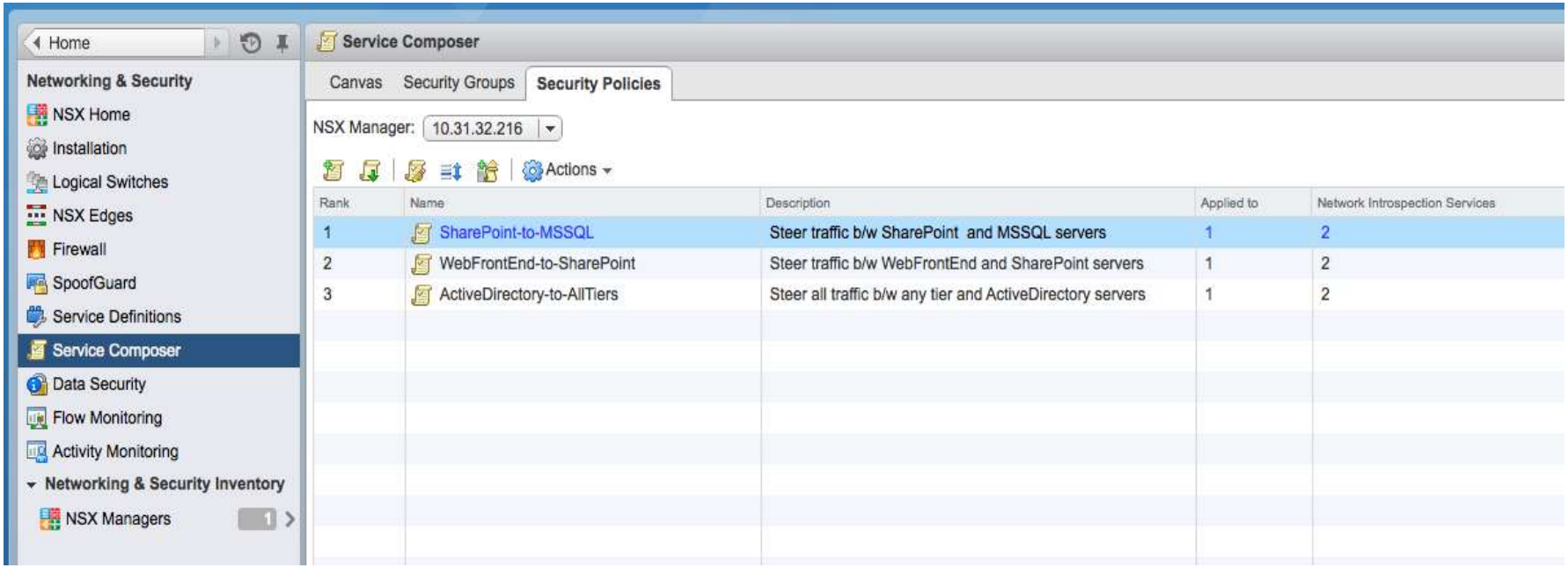
How it works: Traffic Re-direction Rules



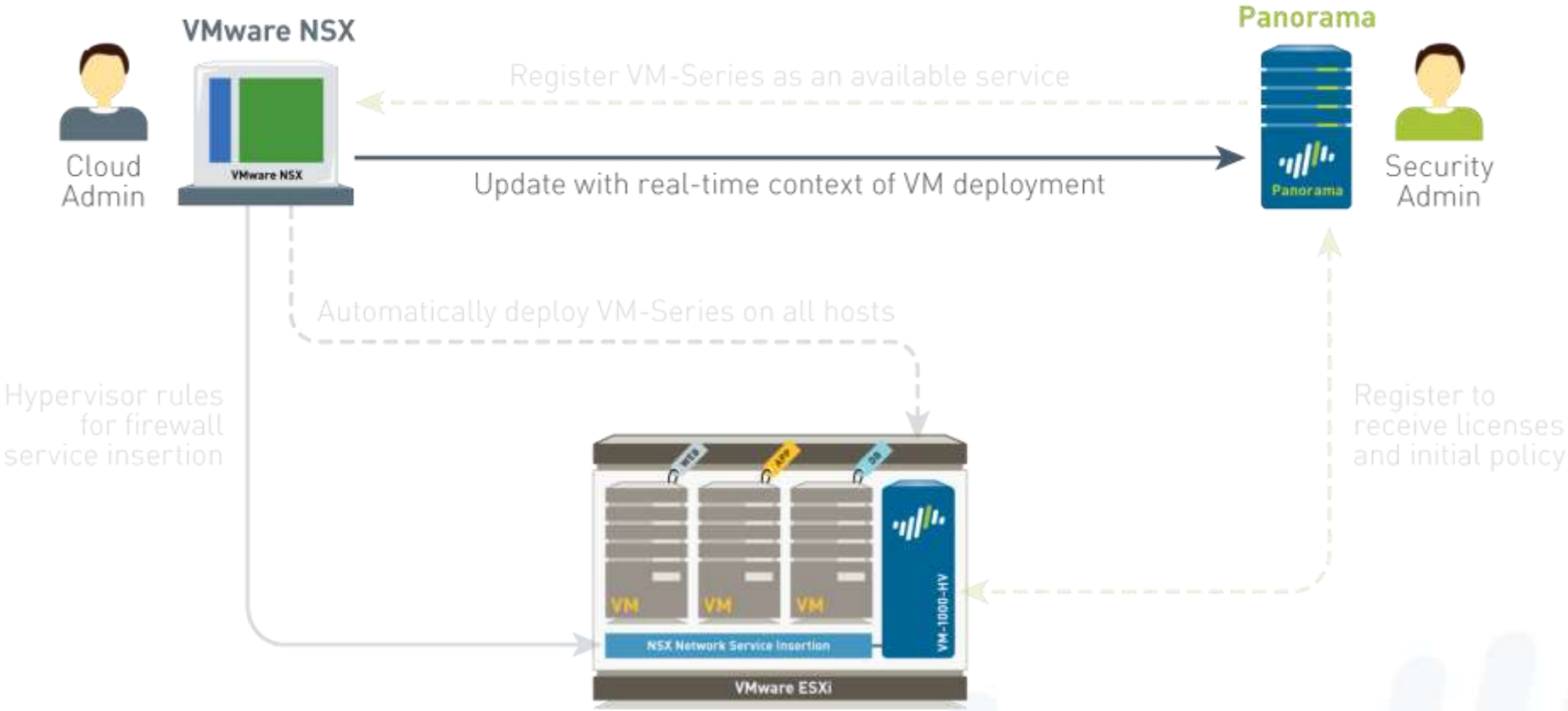
How it works: NSX Mgr.: Service Composer: Containers



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



How it works: Real-time updates



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'

Add Match Criteria

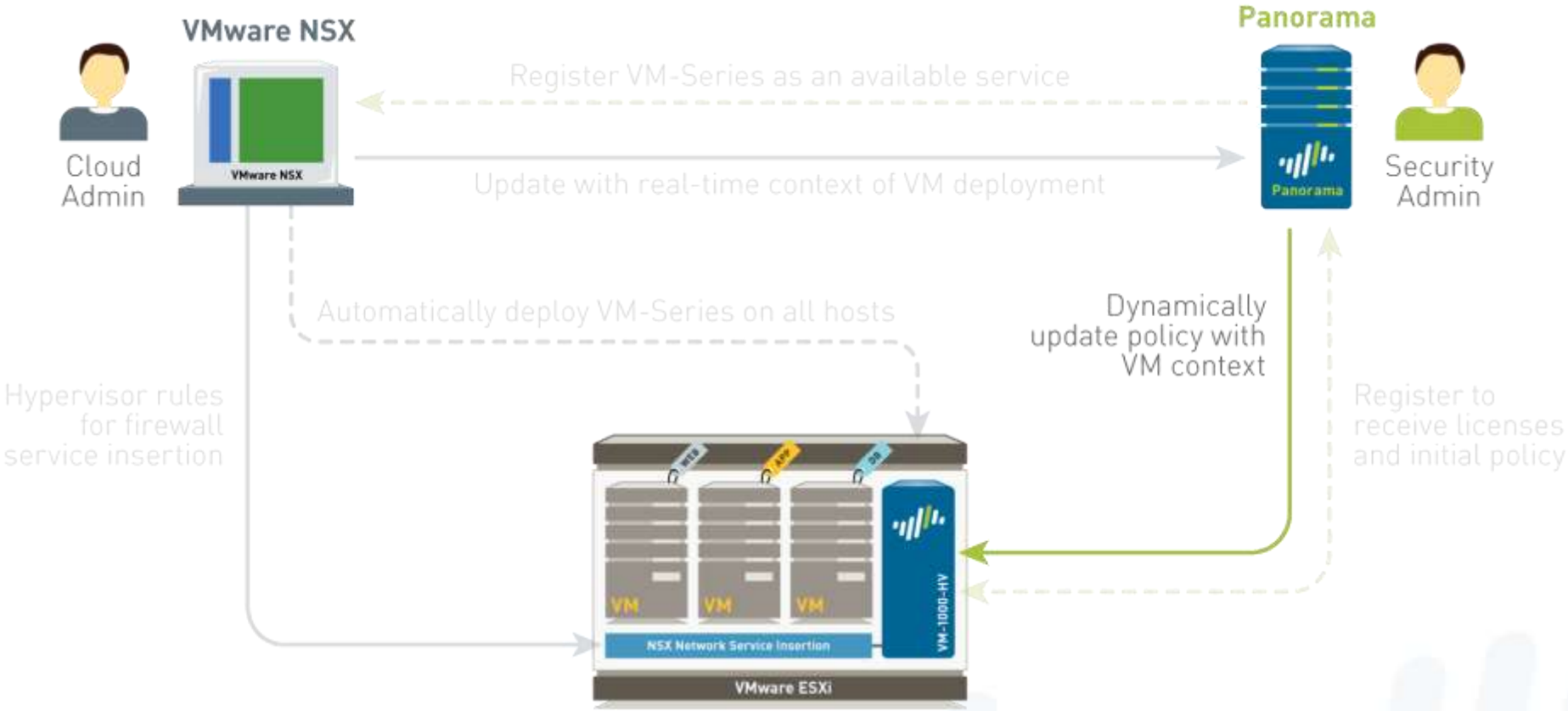
Tags:

OK Cancel

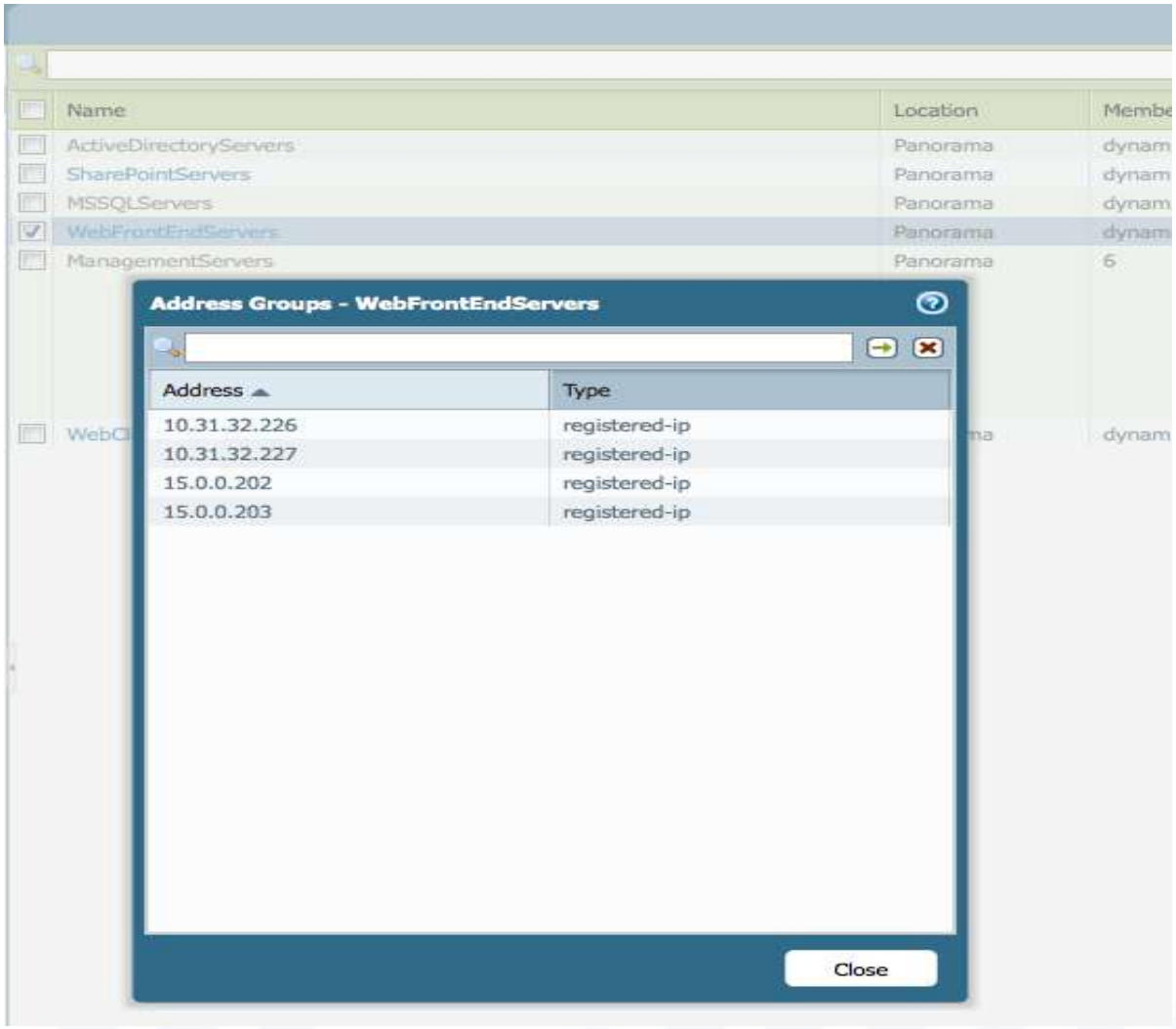
How it works: Panorama: Security Policies

				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



How it works: VM-Series: Dynamic Address Groups



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

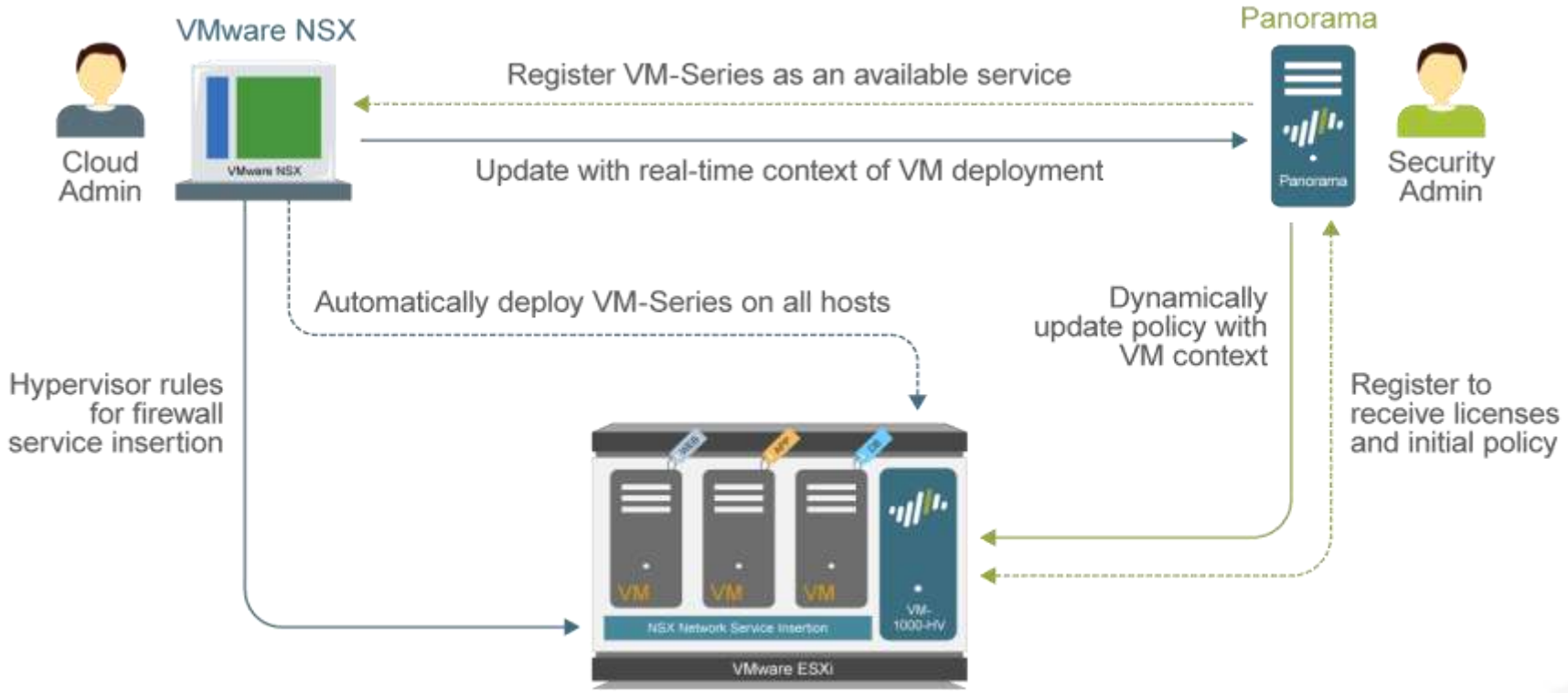
PAN-OS Dynamic Address Groups

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

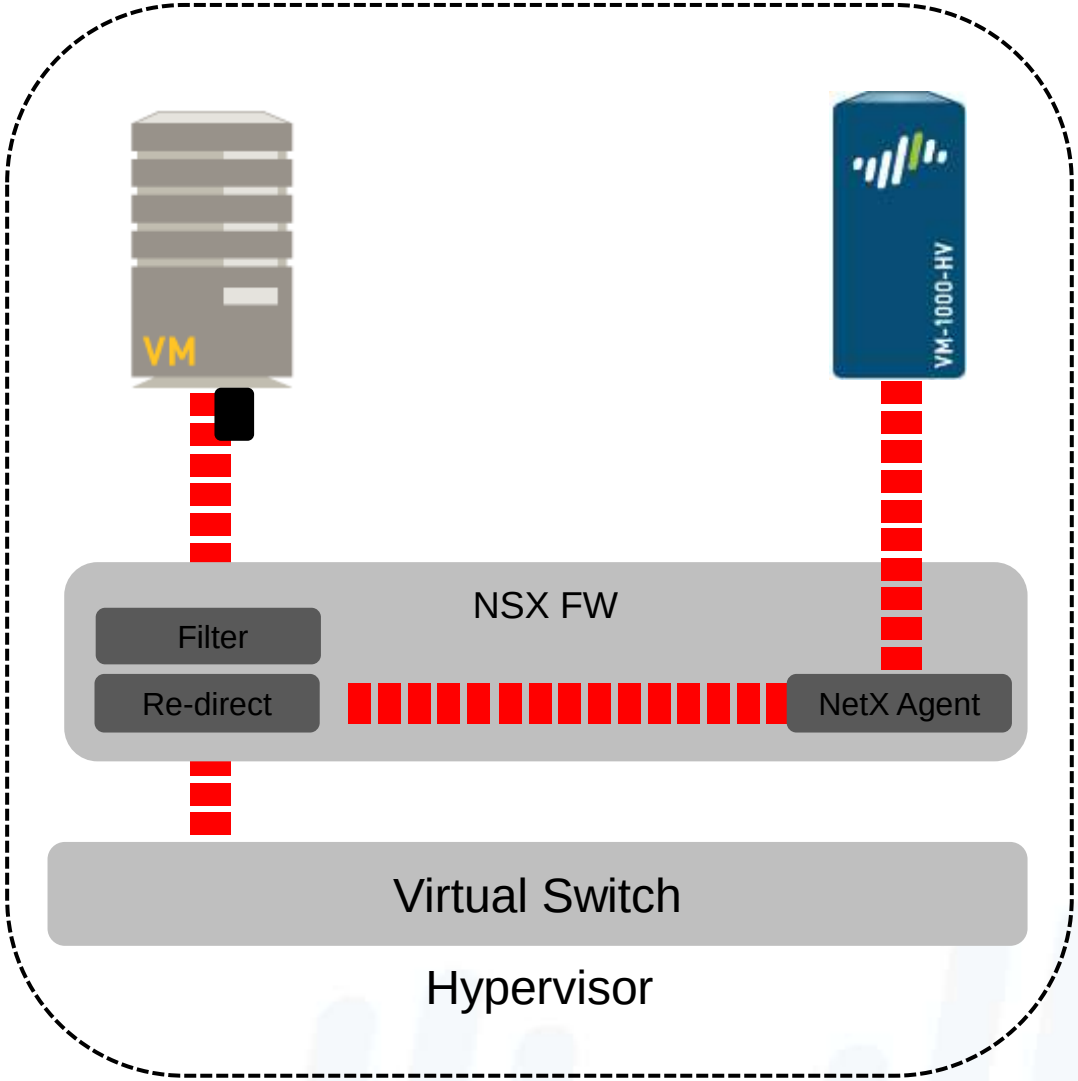


VM Monitoring – ESXi & vCenter Dynamic Tags

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

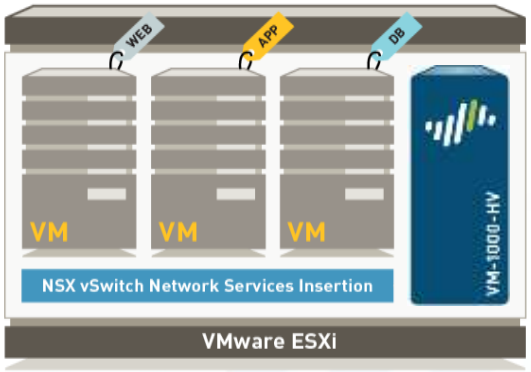
Meeting the needs of both Infrastructure and Security

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



Open Discussion

Questions & Answers

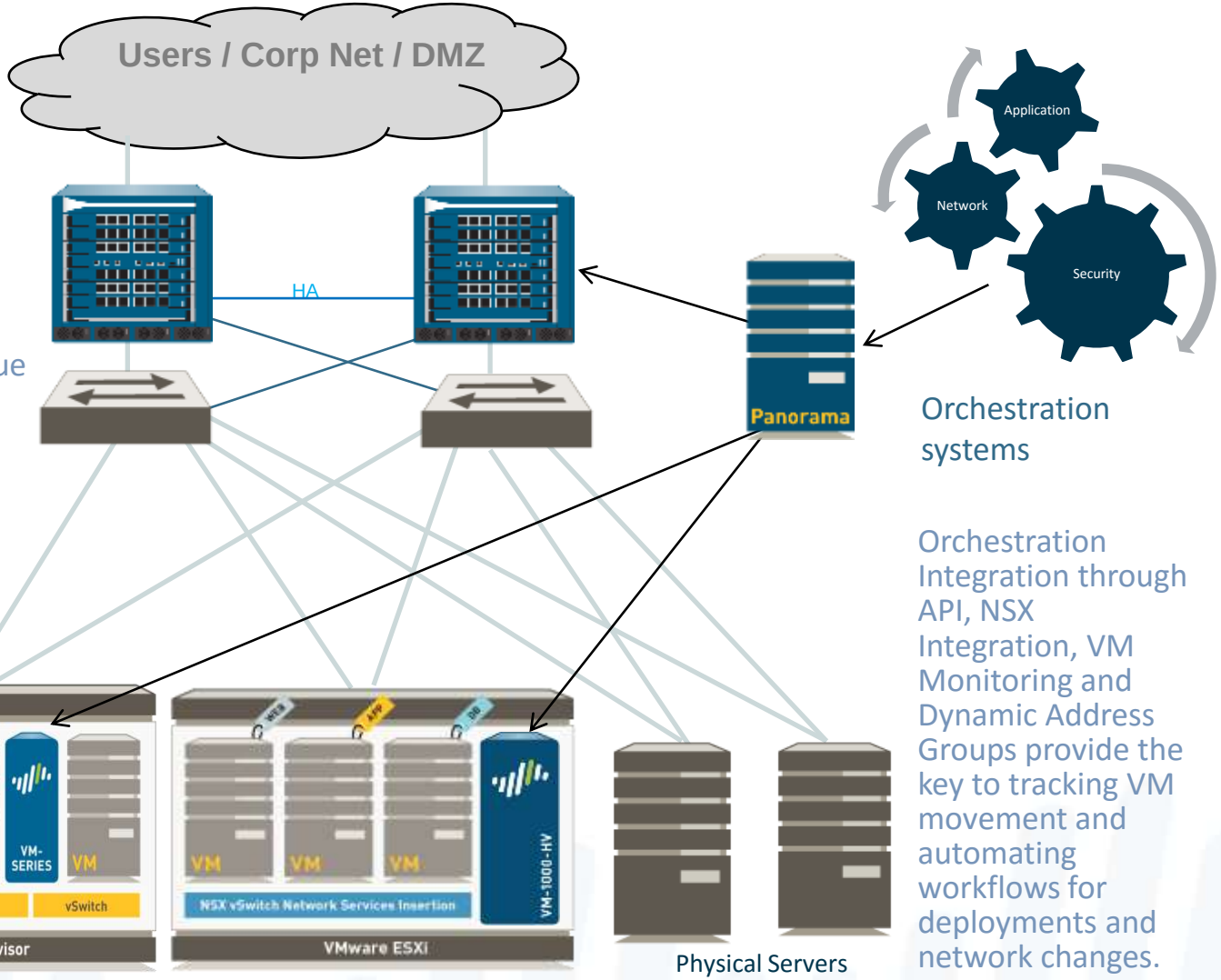
paloalto NETWORKS

the network security company™

Conclusions

Wrap-up

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

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.

Virtualized Firewalls

Intra-host Segmentation

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

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 virtualisation 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™

Domenico Stranieri

Pre-Sales System Engineer

dstranieri@paloaltonetworks.com