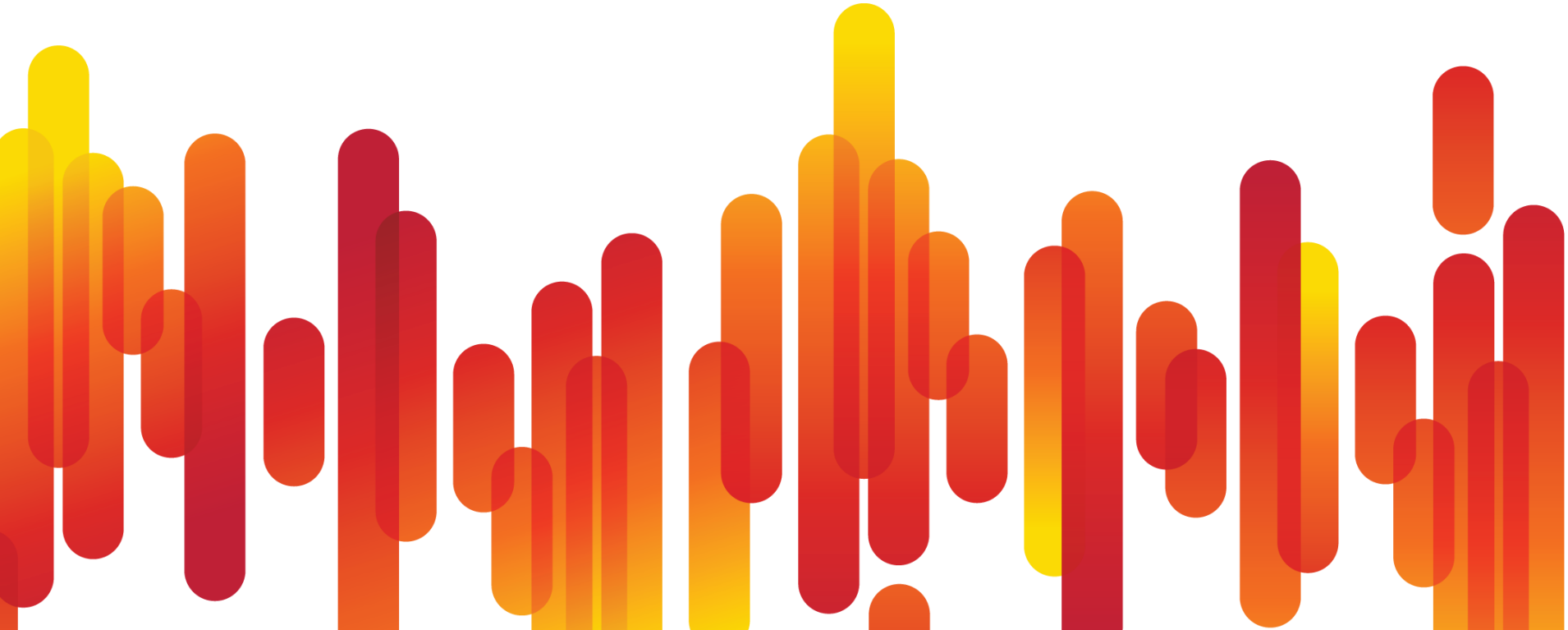
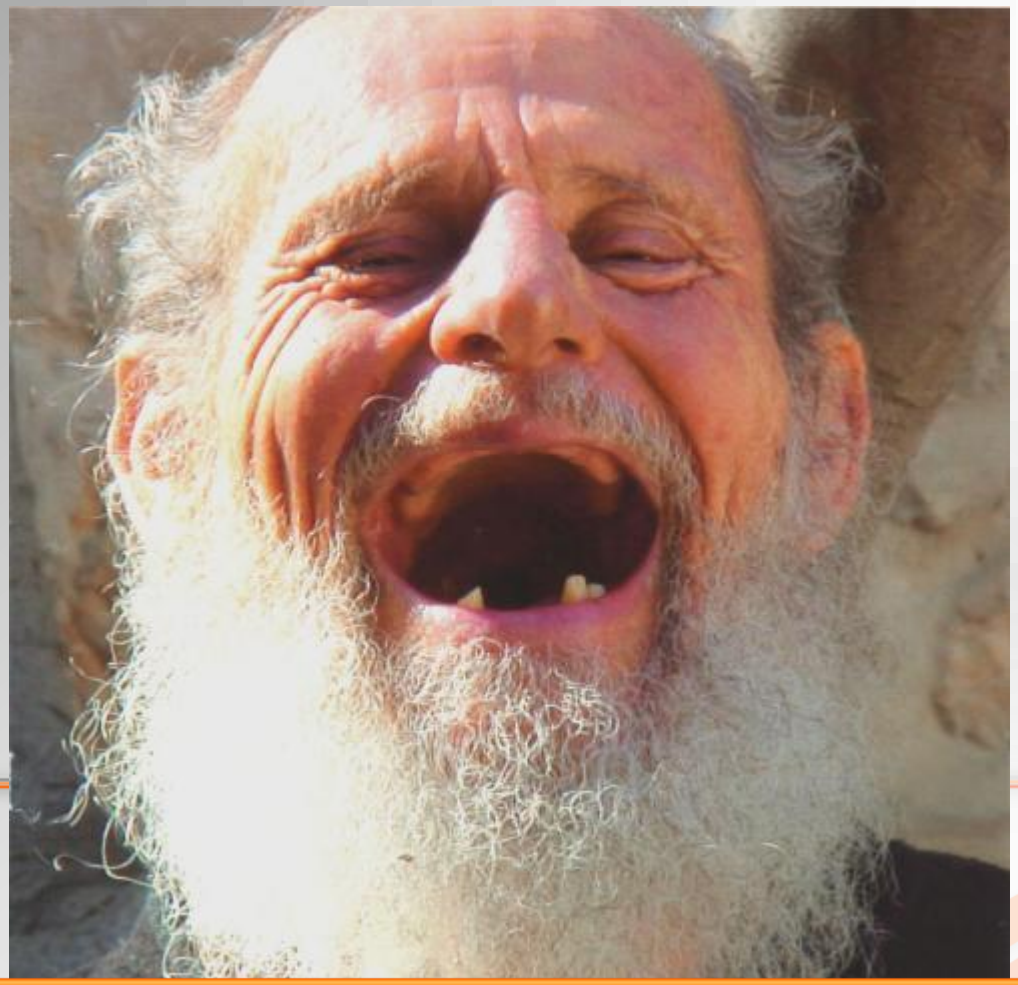
Cisco Networkers 2011

November 7, 2011 - Hong Kong

Cloud Security and Virtualized Data Center Security



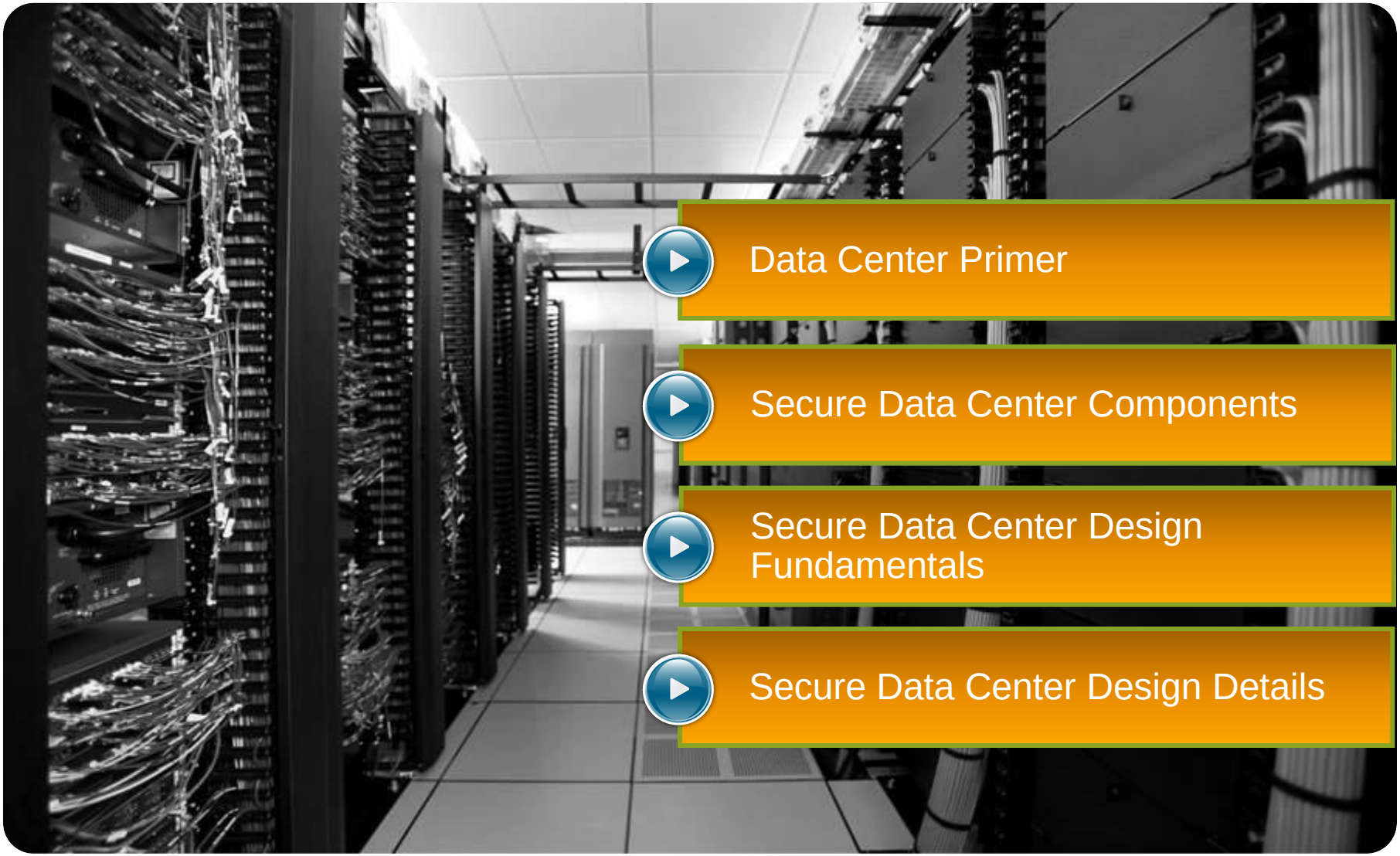


Data Center, Security, & Virtualization: It's so easy just ask this happy 35 year old Administrator

Takeaways

- Security must be included as part of the core design
- Integration with network and server virtualization technologies is key
- Need to understand the core data center fabric technologies and features: VDC, vPC, VRF, server virtualization, traffic flows
- The designs provide an architecture that is extremely flexible and secure.

Secure Data Center



Learn. Connect. Collaborate. together.

Data Center Primer: Terms and Technology

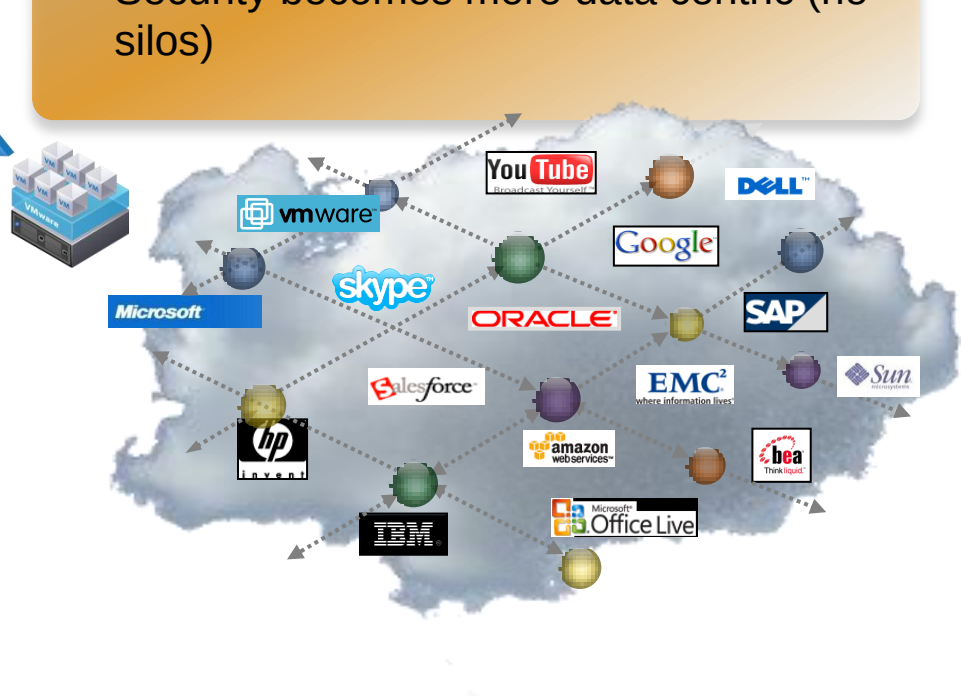
Virtualization in the Data Center

Legacy

- Accidental Architectures
- Applications deployed in fixed positions (ex. multi-tier deployment)
- Predictable traffic flows
- Security often deployed to each pod or silo

Emerging

- Data Center and Server Consolidation
- Server Virtualization
- “Any workload on any server”
- Unpredictable traffic flows as workloads migrate
- Security becomes more data centric (no silos)



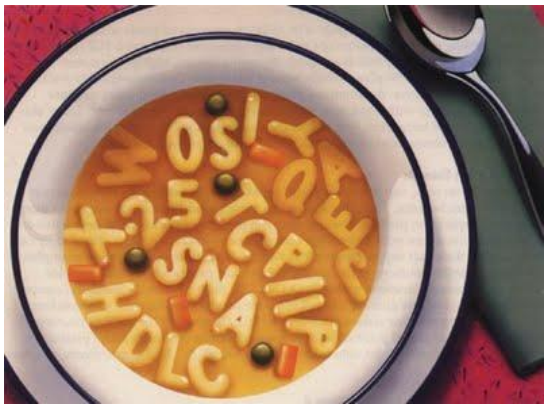
Journey to 100% Virtualization

Recent Forbes Insights survey: 235 CIOs and IT executives:

- **48%** have virtualized at least a quarter of their organization's servers in order to reduce infrastructure costs and deliver applications more rapidly
- **43%** of the survey respondents identified security as their top concern about adopting virtualization as the foundation for cloud computing

Ref: Session SE8195, VMWorld 2010

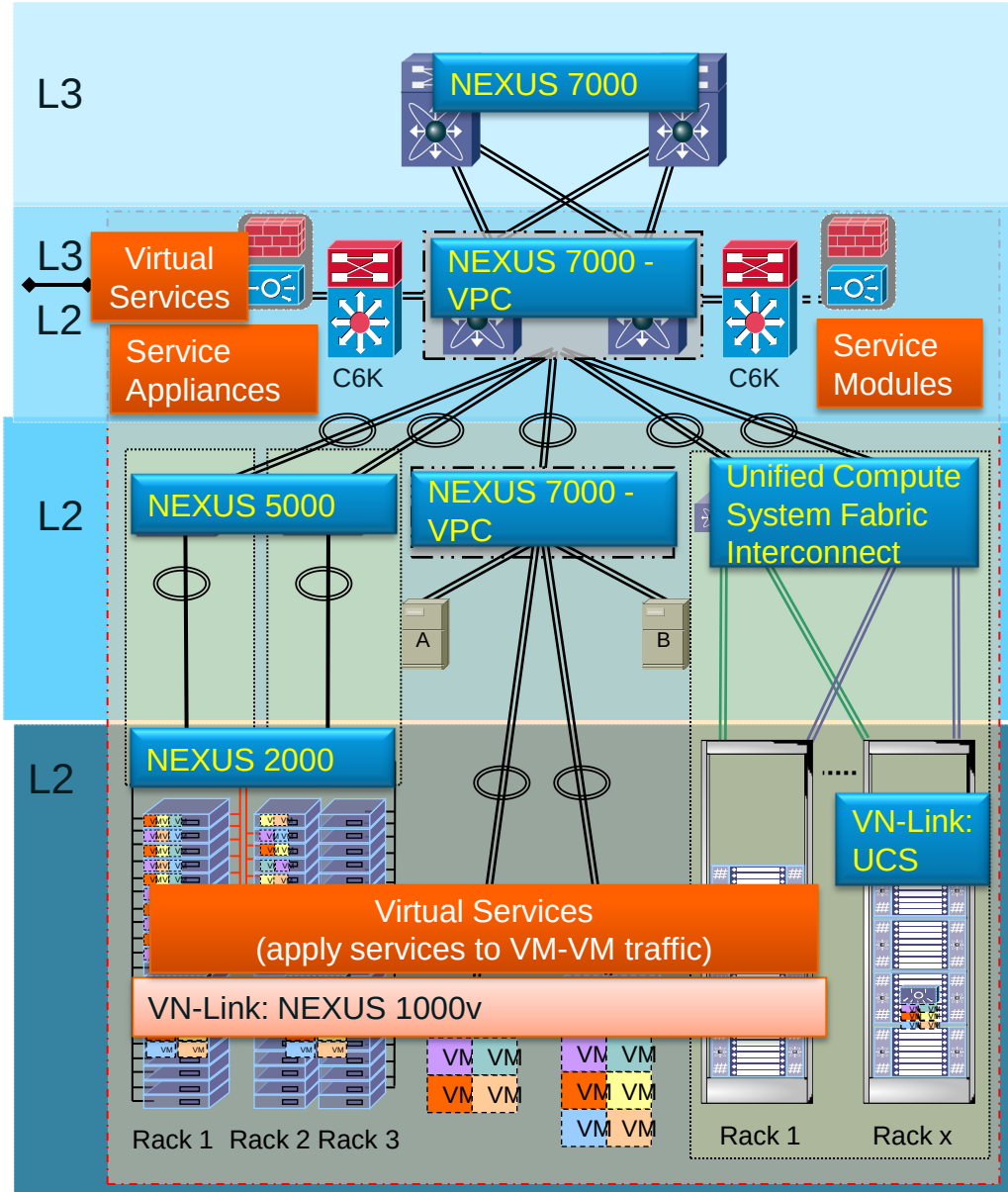
Cisco Datacenter Terms Primer



Know the lingo

- VDC – Virtual Device Context
- VPC – Virtual Port Channel
- VSS & MEC – Virtual Switching System & Multi-chassis Ether-channel
- VSL & Peer Link – Virtual Switch Link
- ECMP – Equal cost Multi-Path
- VSD – Virtual Service Domain
- VBS – Virtual Blade Switching
- VRF – Virtual Routing & Forwarding
- FabricPath

The Unified Data Center Architecture



Core: L3 boundary to the DC network. Functional point for route summarization, the injection of default routes and termination of segmented virtual transport networks

Aggregation: Typical L3/L2 boundary. DC aggregation point for uplink and DC services offering key features: VPC, VDC, 10GE density. Dedicated services are applied here

Access: Classic network layer providing non-blocking paths to servers & IP storage devices through VPC. It provides centralize config & mgmt and ease horizontal cabling demands related to 1G and 10GE server environments

Virtual Access: A virtual layer of network intelligence offering access layer-like controls to extend traditional visibility, flexibility and mgmt into virtual server environments. Virtual network switches bring access layer switching capabilities to virtual servers without burden of topology control plane protocols. Virtual Adapters provide granular control over virtual and physical server IO resources

Data Center Security Challenges

Security Layers Needed

- Denial of Service i.e. (Google, Twitter, Facebook)
- APT – Targeted Attacks / Nation State Attacks
- Data Protection for Privacy and Data Compliance
- Application Exploits (SQL Injection)
- Malware / Botnets
- Mobile Malicious Code
- *Virtualization*

What's The Cost of a Data Breach?

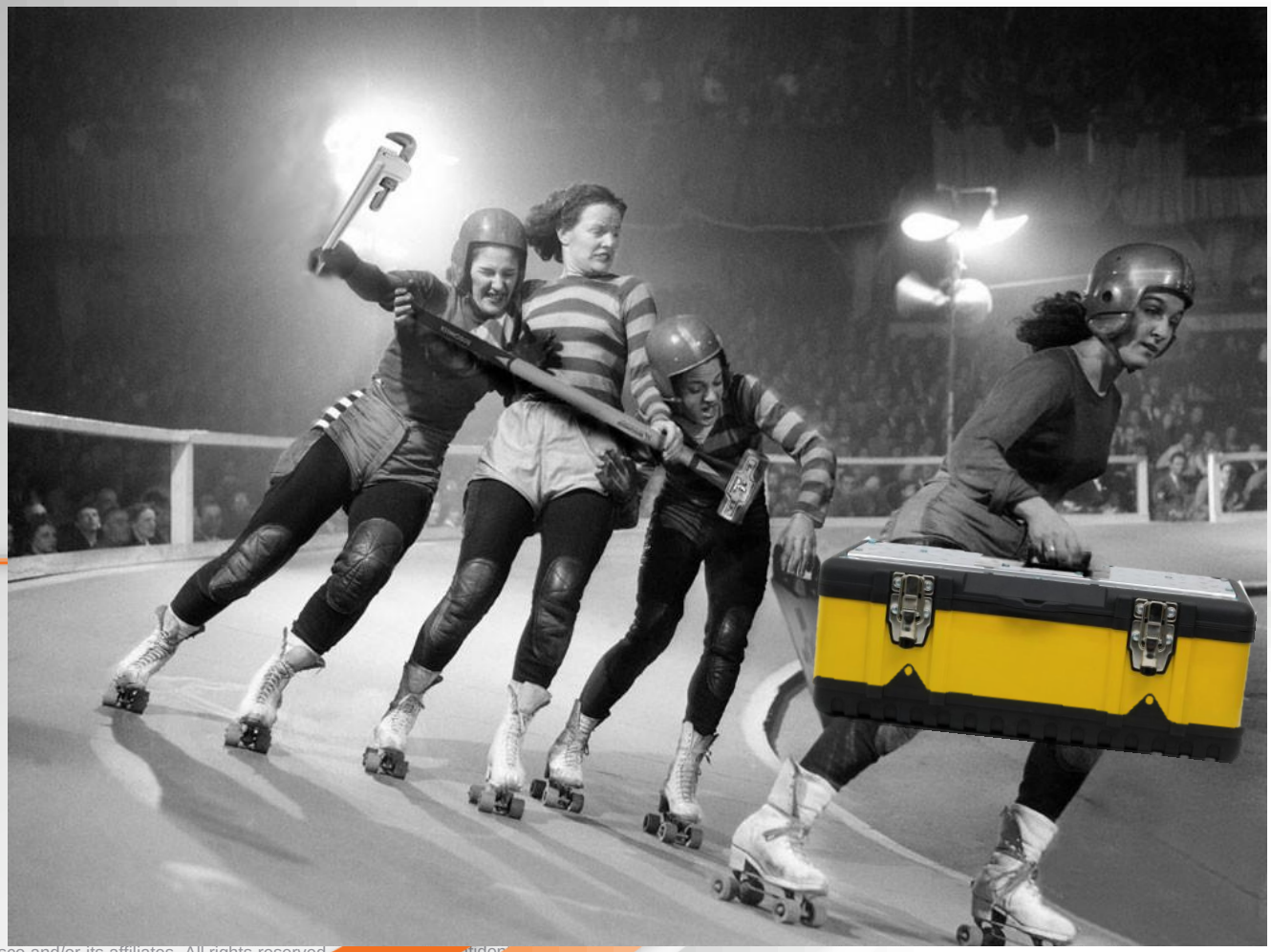
It will Cost you ☹

- Cost of a Data Breach
  - $204 per compromised customer record
  - Ponemon Institute's annual study
- The average total cost of a data breach
  - $6.65 million in 2008
  - $6.75 million in 2009

Source: http://www.networkworld.com/news/2010/012510-data-breach-costs.html

Learn. Connect. Collaborate. together.

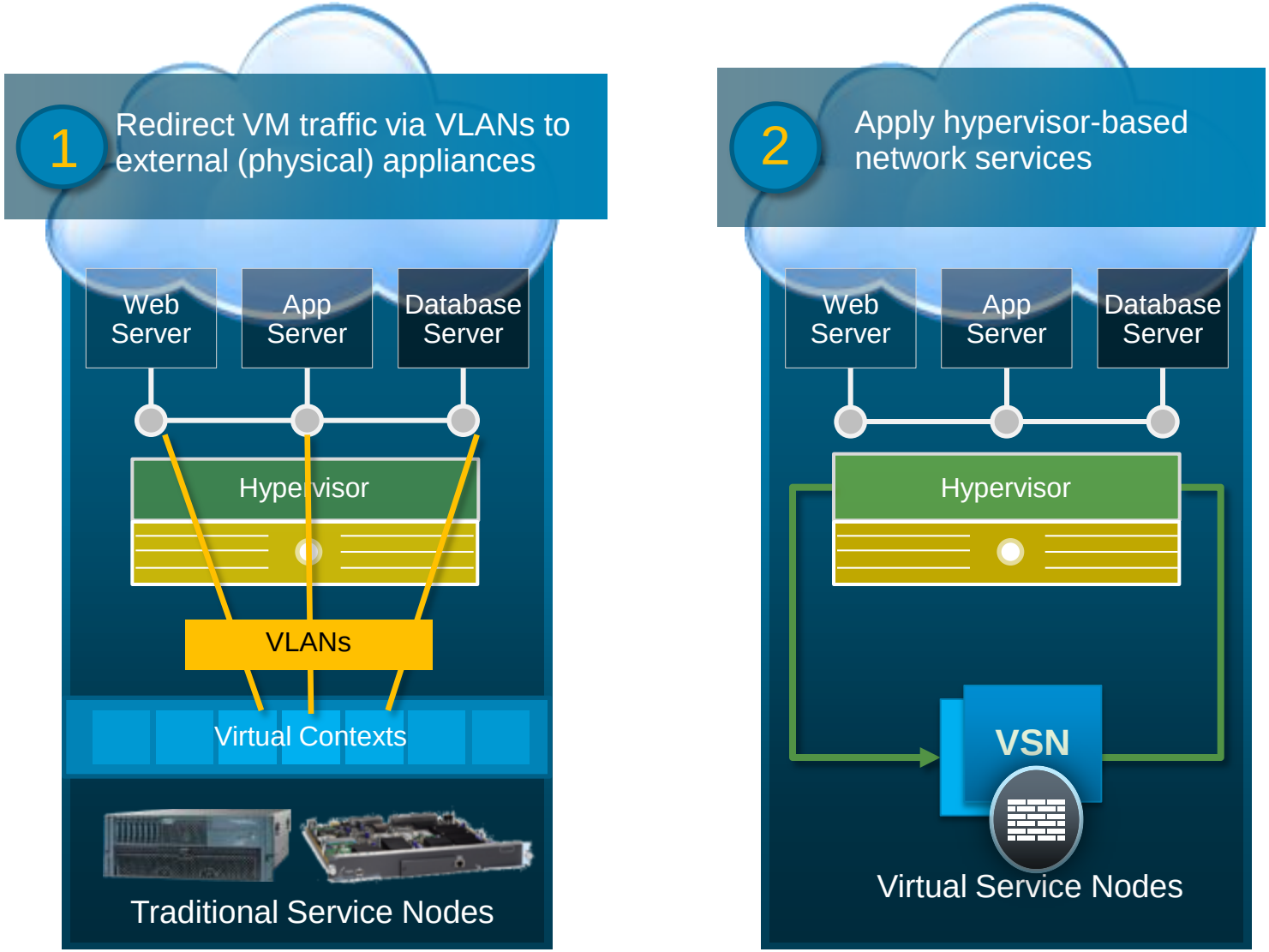
Data Center Security Components: What's in our toolbox



Virtualization is Driving Changes

- Broad based DC virtualization & workloads moving to cloud
  - Lower cost, Agility, Scale-out
- Workloads of varied risk profiles share the same compute infrastructure
  - 3-tier applications, QA/Dev, HR, Finance
  - Unified Communications
  - Virtual Desktop
  - DMZ, Intranet Extranet
- Increasing interest in Virtual Private Clouds
- How to:
  - Meet regulatory compliance, Audit needs
  - Ensure non-disruptive administration
  - Maintain policy and visibility

Physical and Virtual Network Security Deployment Options

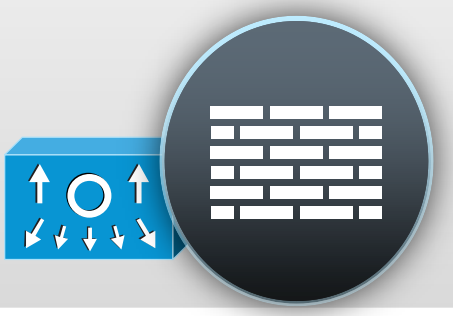


The Data Center Firewalls

5585

ASA Services Module

Virtual Security Gateway

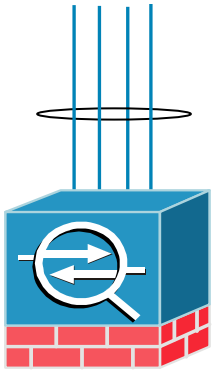


Data Center Firewall Design: ASA 5585 & 8.4(1)

- **Performance**
  - 10 Million connections + ~375Kcps delivers more capacity in a single system
  - Numbers are NOT inflated – Customers will be able to easily replicate
- **EtherChannel connectivity to support vPC / Multi-chassis EtherChannel in Nexus 7K**
  - No need for STP
  - Creates Secure Active/Active traffic flows in Nexus DC irrespective of HA type
- **Firewall & IPS Functionality for Nexus VDCs**
  - ASA/IPS protection can be implemented intra-VDC and/or inter-VDC
- **Up to 32 interfaces per Virtual Context (formerly 2)**
  - 4 Interfaces per bridge group 8 bridge groups per Virtual Context
- **Transparent FW (layer 2) versus Layer 3 Deployment**
  - Supports Virtualization without a Data Center redesign
- **Mixed mode support**
  - May blend Layer 2 and Layer 3 options within design framework(s)

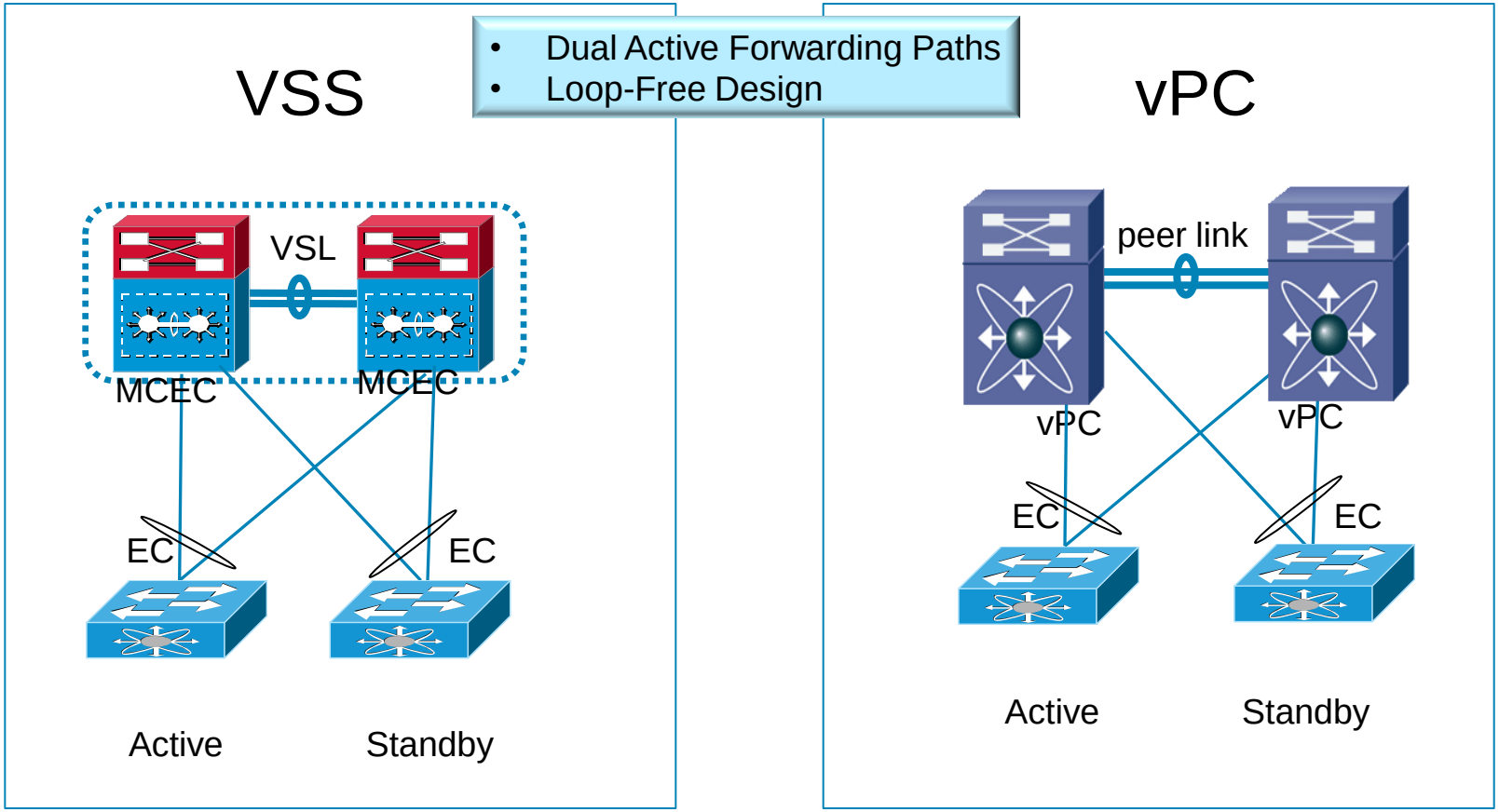
EtherChannel Supported in ASA 8.4(1)

- ASA supports Link Aggregation Control Protocol (LACP), an IEEE 802.3ad standard
- Each port-channel supports up to 8 active and 8 standby links
- Supported methods of aggregation: Active, Passive & On
- EtherChannel ports are treated just like physical and logical interfaces on ASA
- ASA can tie-in directly to vPC (Nexus 7000) or VSS (6500) enabled switch

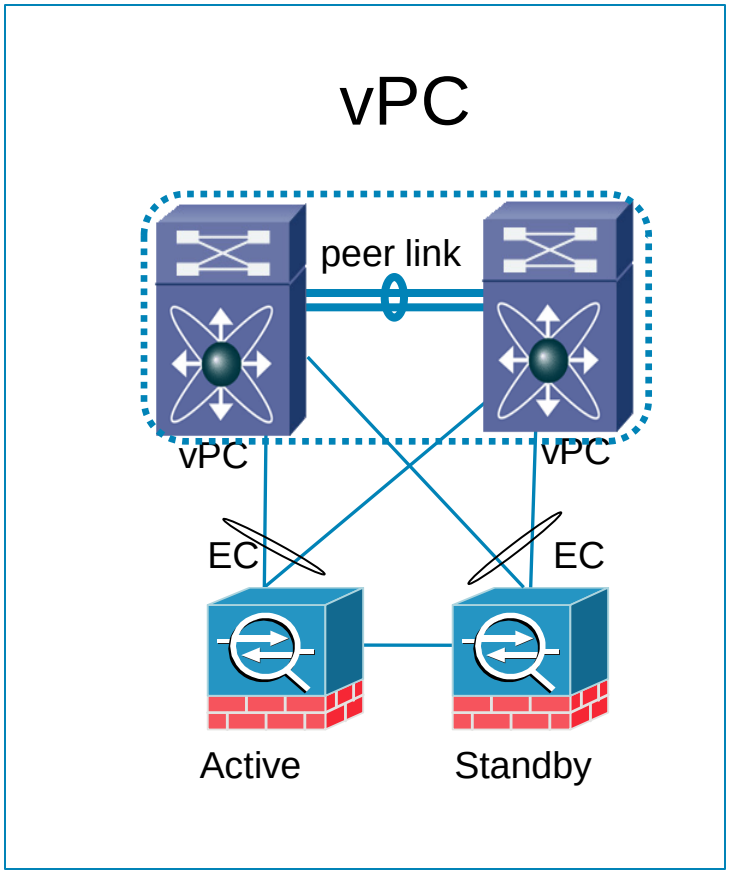


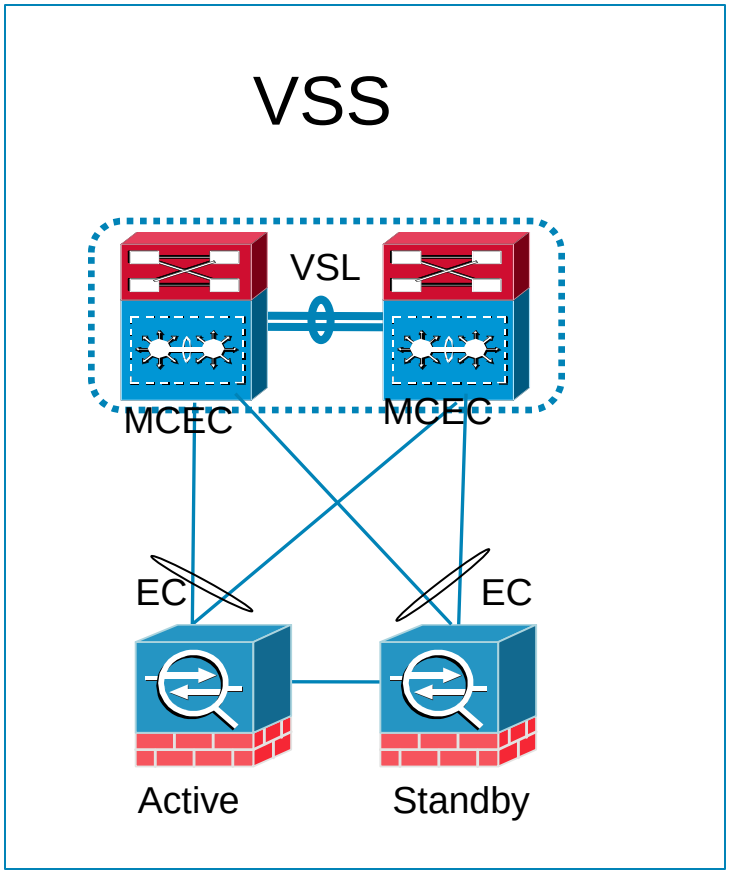
Catalyst 6500 VSS and Nexus 7000 vPC

- Dual Active Forwarding Paths
- Loop-Free Design



ASA Integration with vPC & VSS





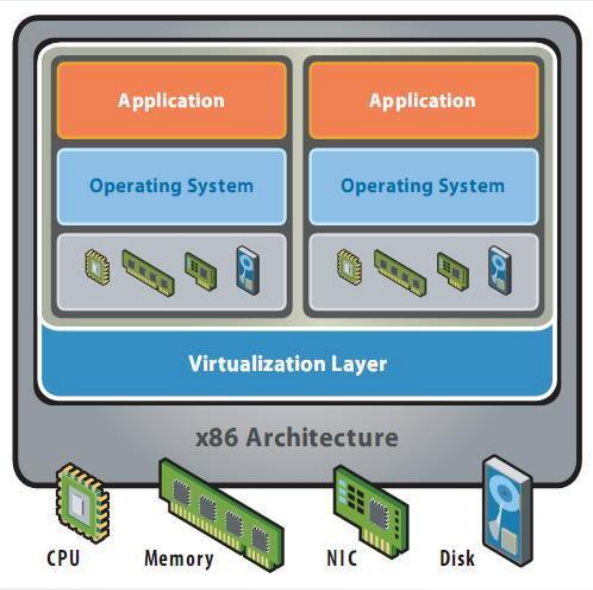
ASA 5585 Interface Options, Continued

10GB SFP+ Modules	1GB SFP Module
SFP-10G-SR SFP-10G-LR* SFP-10G-LRM*	SX LX*
Copper Twinax 1 meter Copper Twinax 3 meter* Copper Twinax 5 meter*	

- GLC-T SFP should work but is not yet officially supported

* Minimum Software 8.2.5 or 8.4.1

Server Virtualization

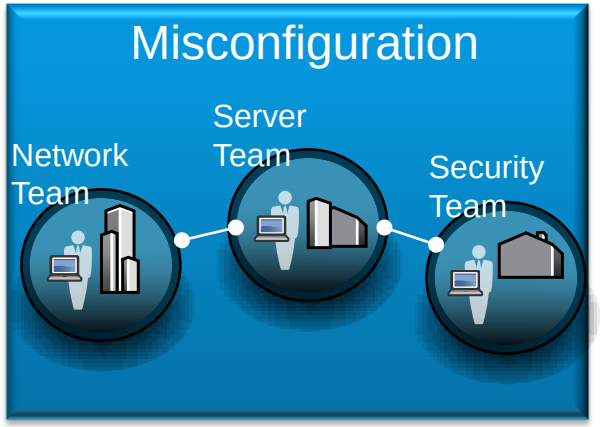


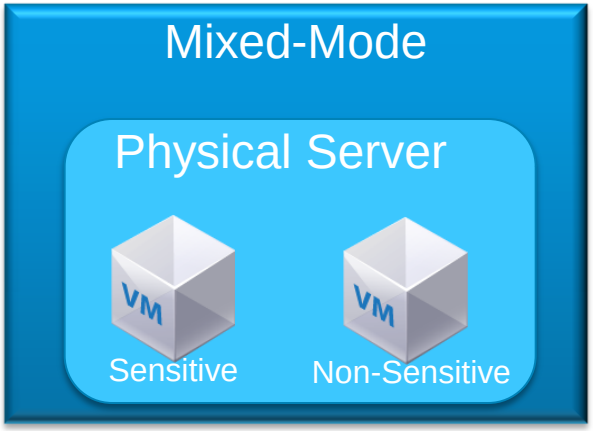
Security and Server Virtualization

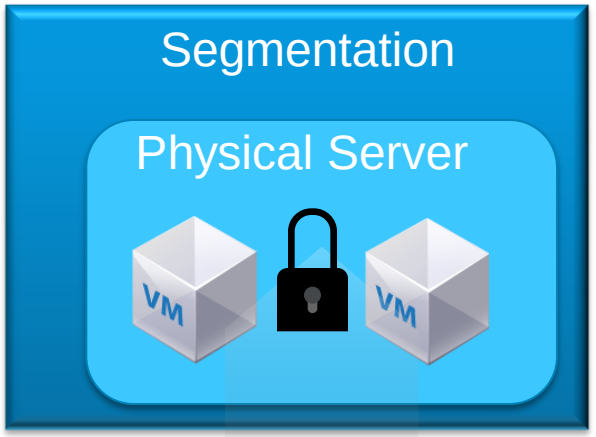
Virtualization a broad topic

Focus is areas were Cisco can add value

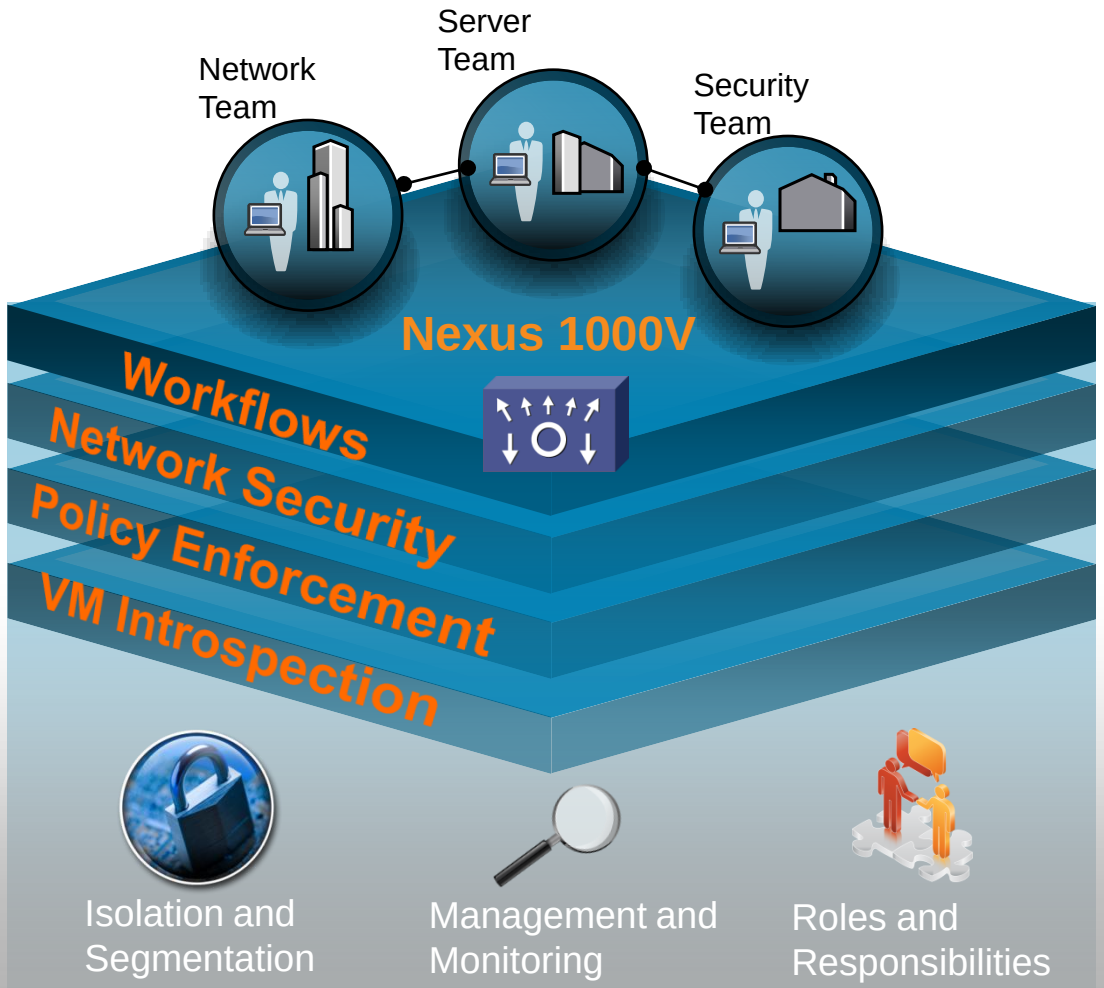
Virtualization Concerns







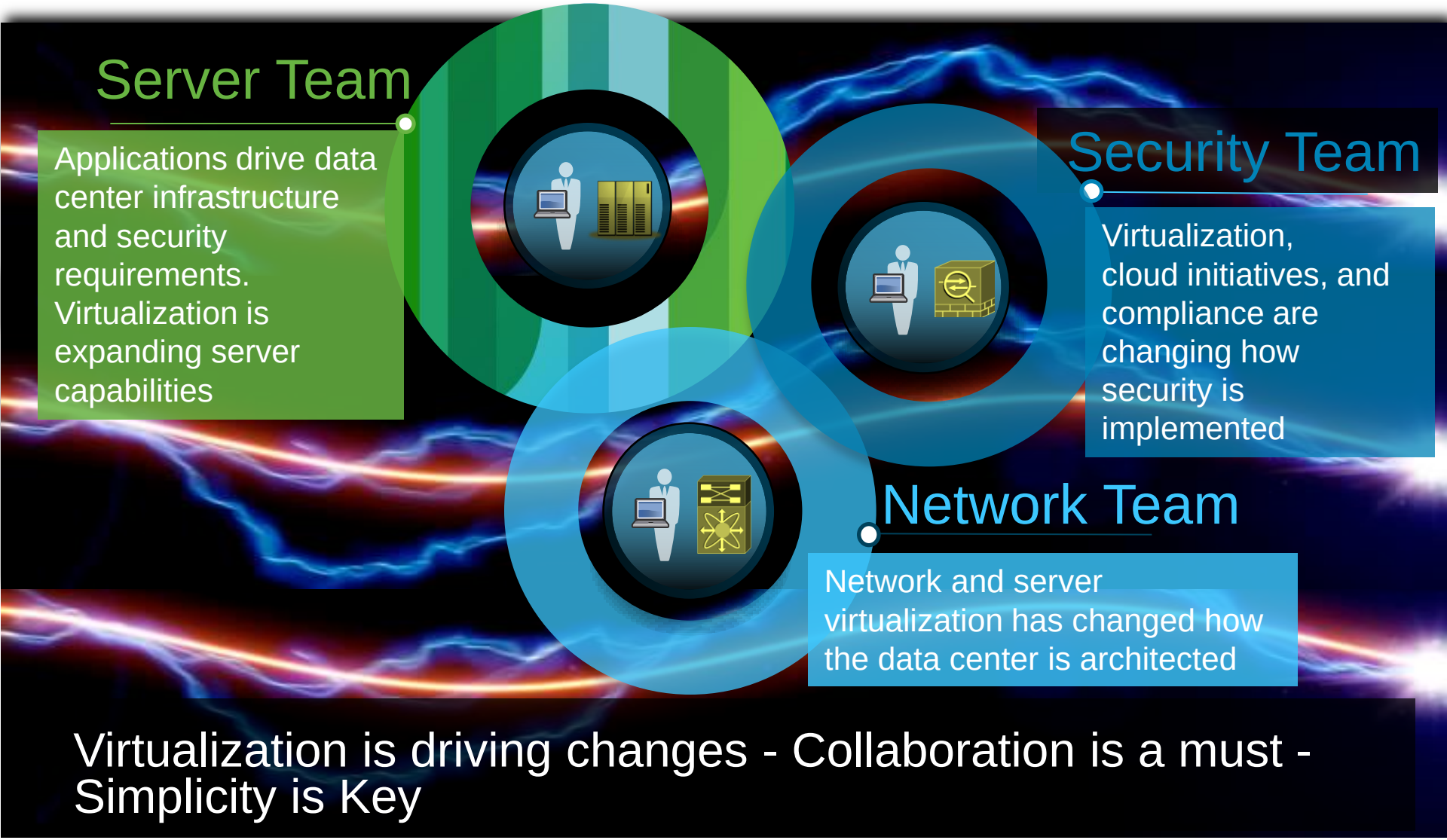
Managing Virtual Networking Policy



Nexus 1000V

- Non-disruptive operation model to maintain current workflows using Port Profiles
- Maintain network security policies with isolation and segmentation via VLANs, Private VLANs, Port-based Access Lists, Cisco Integrated Security Features
- Ensure visibility (VM Introspection) into virtual machine traffic flows using traditional network features such as ERSPAN and NetFlow

Data Center Politics (Don't cross the streams)

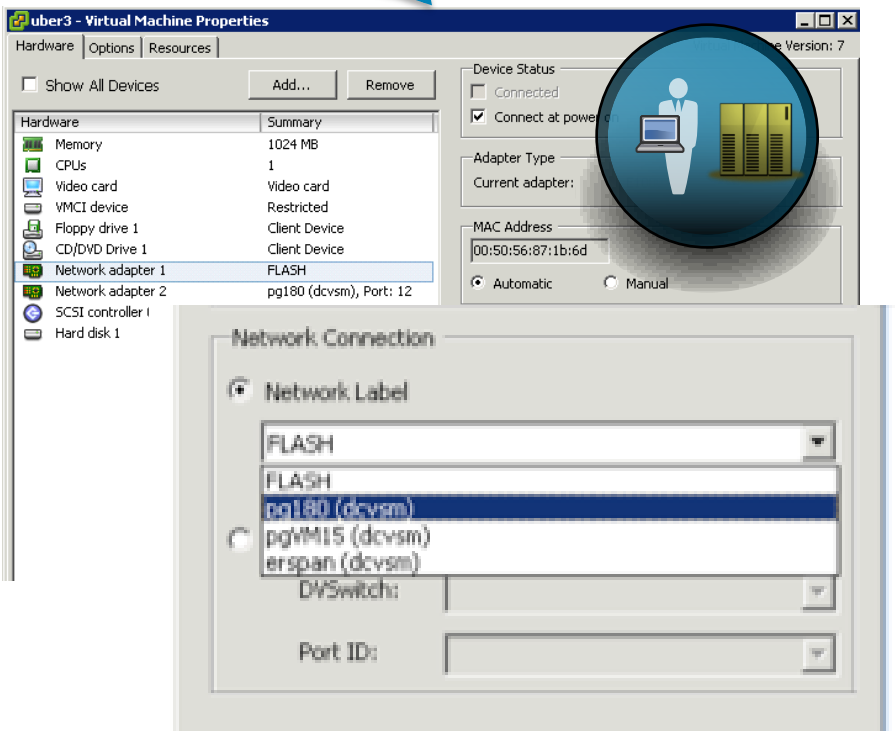


Port Profiles

Port Profile –> Port Group

vCenter API

```
port-profile vm180
  vmware port-group pg180
  switchport mode access
  switchport access vlan 180
  ip flow monitor ESE-flow input
  ip flow monitor ESE-flow output
  no shutdown
  state enabled

interface Vethernet9
  inherit port-profile vm180

interface Vethernet10
  inherit port-profile vm180
```



Cisco Virtual Security Gateway

Virtual Security Gateway (VSG)

Context aware Security	VM context aware rules
Zone based Controls	Establish zones of trust
Dynamic, Agile	Policies follow vMotion
Best-in-class Architecture	Efficient, Fast, Scale-out SW

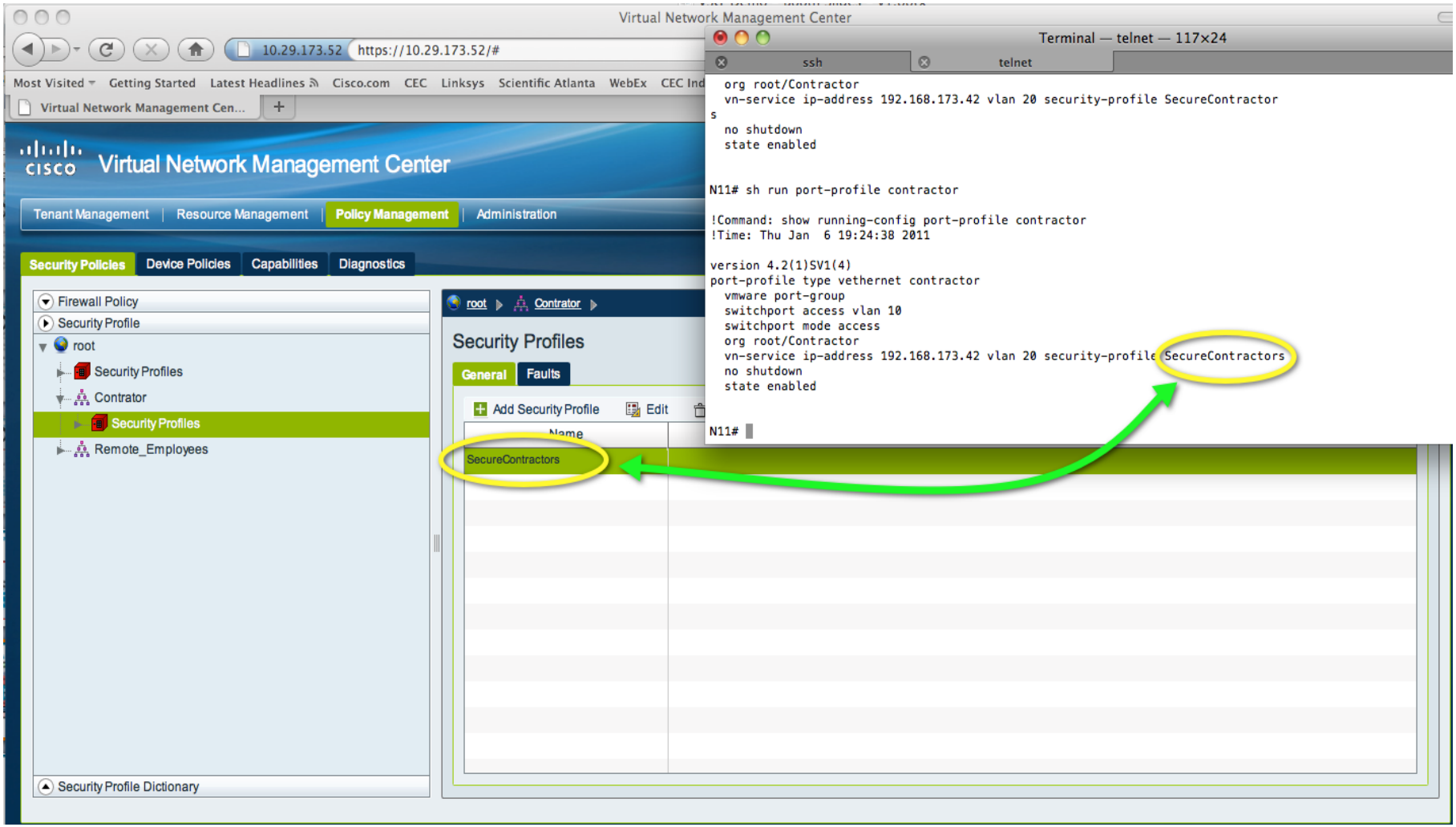
Virtual Network Management Center (VNMC)

Non-Disruptive Operations	Security team manages security
Policy Based Administration	Central mgmt, scalable deployment, multi-tenancy
Designed for Automation	XML API, security profiles

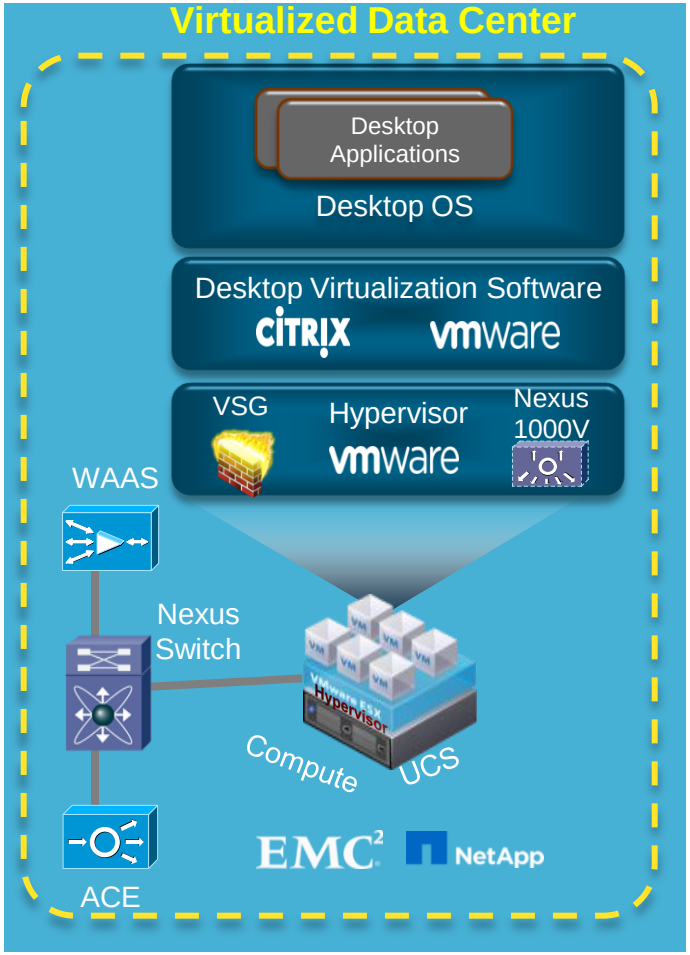
Virtual Security Gateway

- Context based rule engine, where ACLs can be expressed using any combination of network (5-tuple), **custom** and **VM attributes**. It's extensible so other types of context/attributes can be added in future
- No need to deploy on every physical server (this is due to 1000V vPath intelligence)
- Hence can be deployed on a dedicated server, or hosted on a Nexus 1010 appliance
- Performance optimization via enforcement off-load to 1000V vPath
- High availability

Security Profile to Port Profile



Securing Virtual Desktops (VDI)



Security Features for VDI

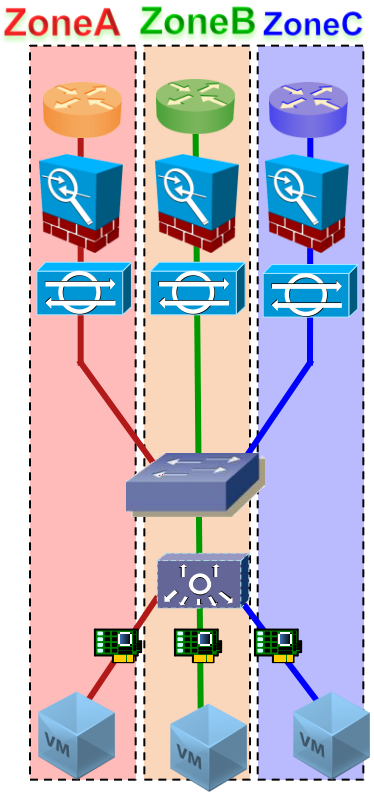
- ASA
- Virtual Security Gateway
- Nexus 1000V
  - Access Control List
  - Port Security
  - Private VLAN
  - DHCP Snooping
  - Dynamic ARP Inspection
  - IP Source Guard
- 802.1x & TrustSec

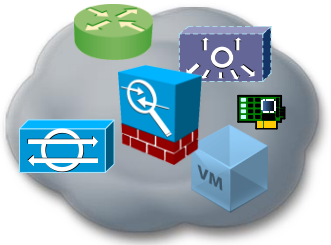
Cisco solution = VXI: Virtualization Experience Infrastructure:

Design Fundamentals

Secure Data Center

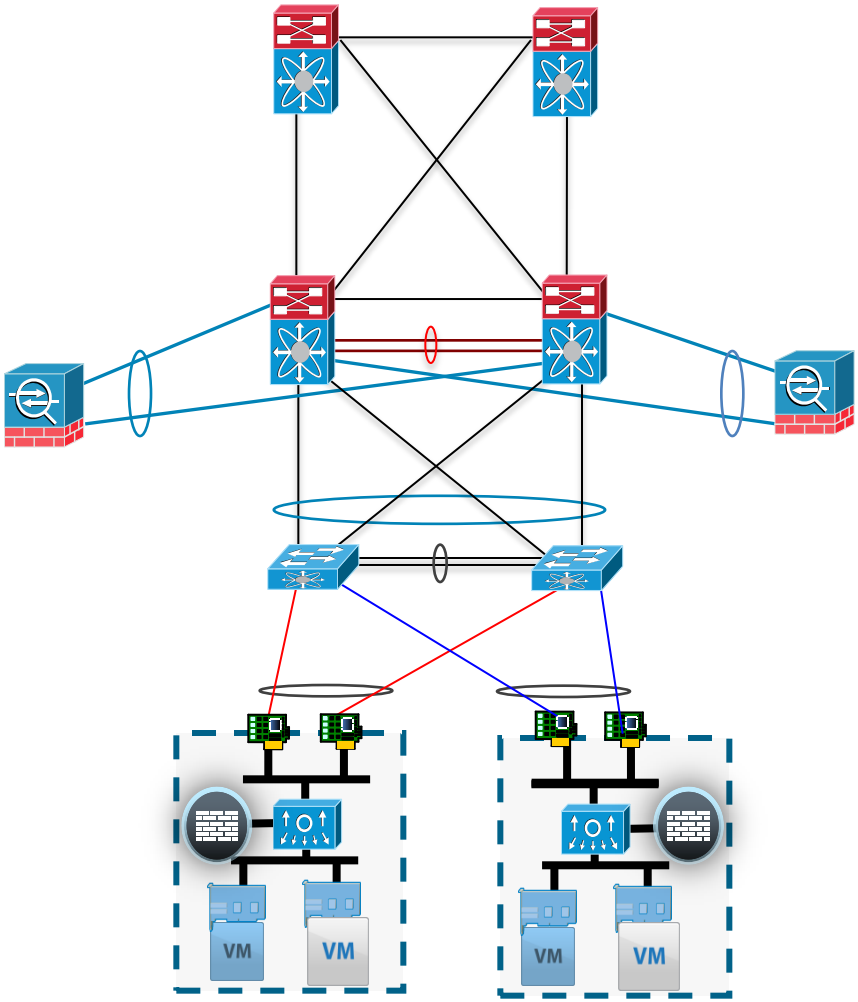
- Network security can be mapped and applied to both the physical and virtual DC networks
- Zones can be used to provide data centric security policy enforcement
- Steer VM traffic to Firewall Context
- Segment pools of blade resources per Zone
- Segment Network traffic w/in the Zone
  - System Traffic
  - VM Traffic
  - Management Traffic
- Lockdown elements w/in a Zone
- Unique policies and traffic decisions can be applied to each zone creating very flexible designs
- Foundation for secure private cloud





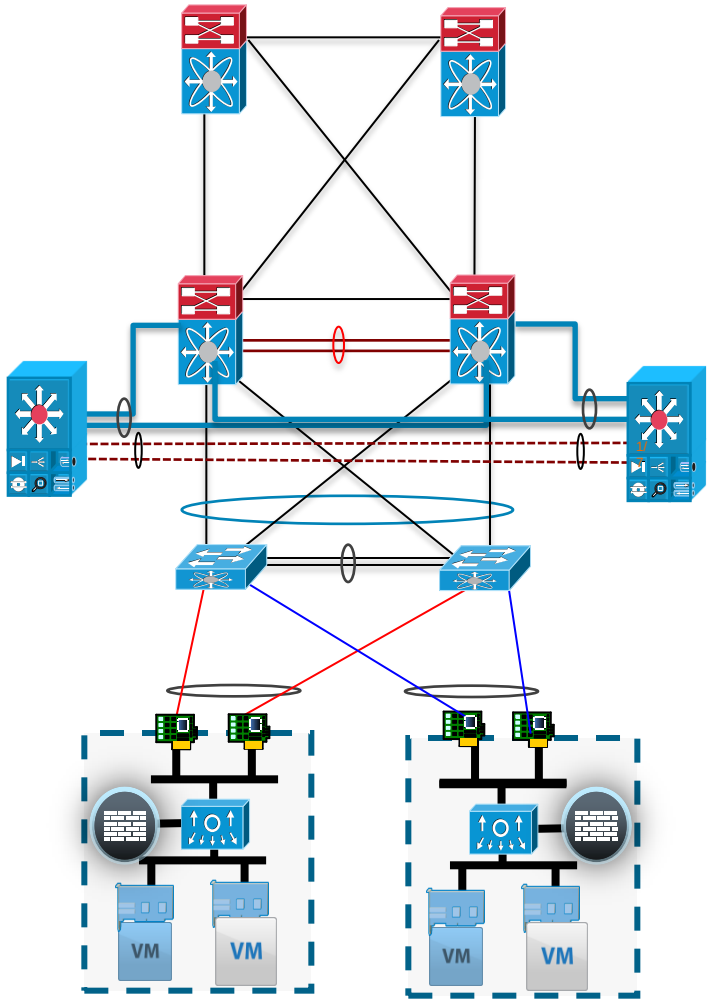
Traditional Model

- Services are Aggregated at the Distribution Layer
- Single or Multi-Tenant zone based segmentation
- Virtual Context create security zones from the DC edge to the Virtual Machine
- VRF->Firewall->VLAN->Virtual Switch->Virtual Firewall->vNIC->VM
- EtherChannel and vPC provide loop-free Layer 2 environment
- Visibility and control for vm-to-vm flows



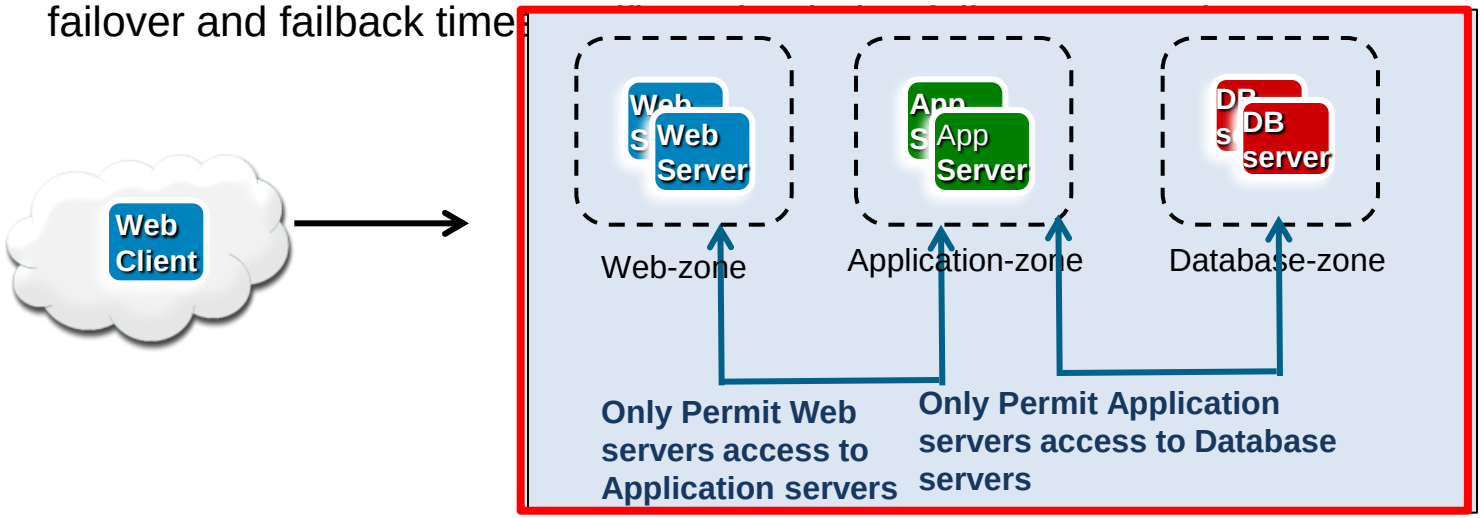
Secure Service Pod Model

- Services Pod centralizes security services
- Traffic forwarded via service-specific VLANs
- Modules (Cat 6500) and appliances supported
- Highly scalable module design
- Single or Multi-Tenant zone based segmentation
- Security zones from the DC edge to the Virtual Machine



Understand Network and Application Flows

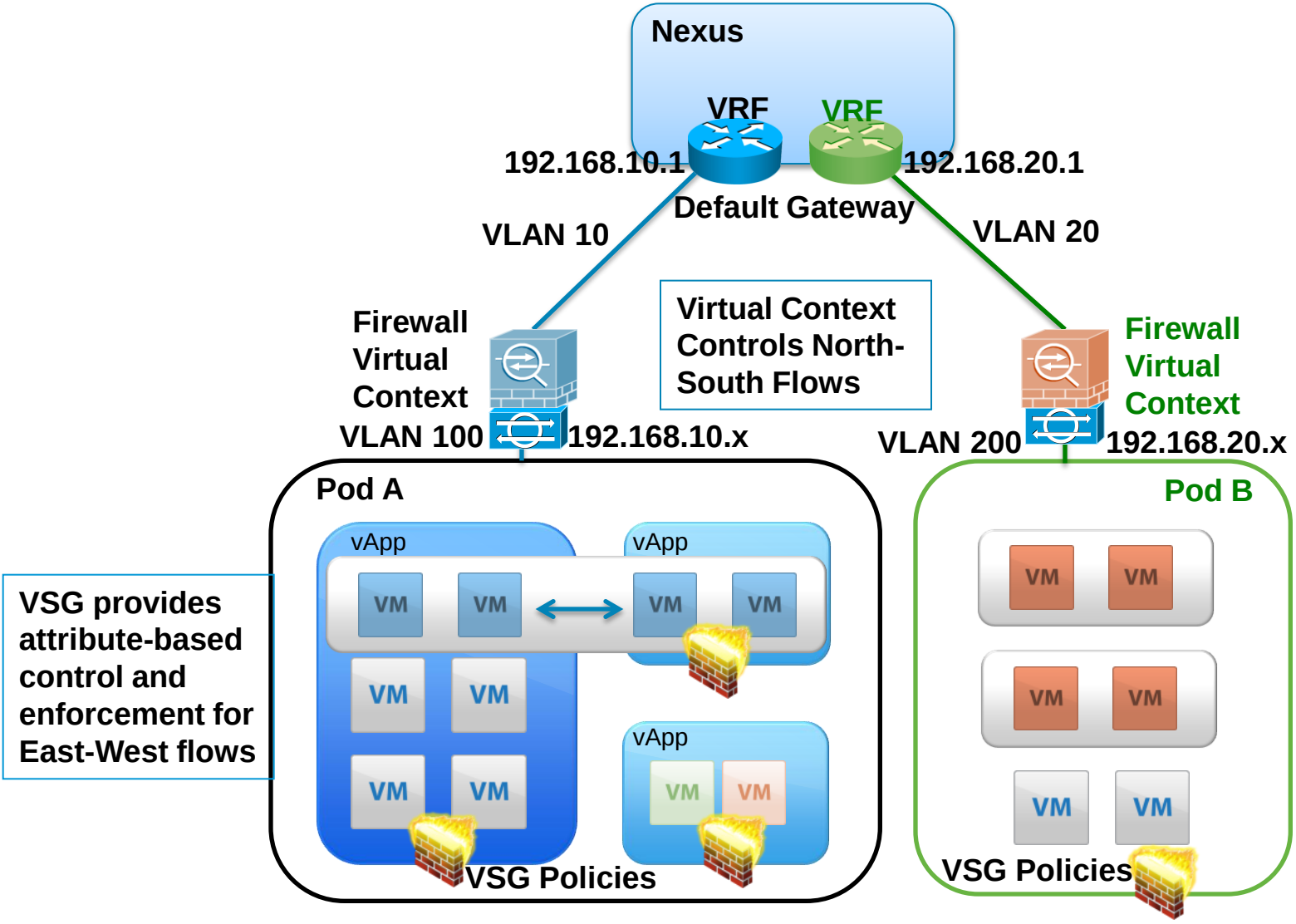
- Understand how the applications are deployed and accessed both internally and externally
- Understand the North-South, East-West flow patterns
- Remember careful attention should be given to where the server's default gateway resides
- Adjacency of services to servers is important. Adding services to existing flow patterns minimizes packet gymnastics!
- Again, design with the maximum amount of high availability: know your failover and failback time



Important

- Careful attention should be given to where the server's default gateway resides
- Can be disruptive to introduce changes to where the gateway resides. Non-greenfield designs require flexibility for deploying new services. Ex. From switch to service appliance
- Service introduction ie. Firewall, Web security, load balancing, can all have an impact on data center traffic flows
- Design with the maximum amount of high availability: know your failover and failback times, traffic paths during failover scenarios
- Multicast support considerations for L2 vs L3 services

North-South & East-West Data Center Flows



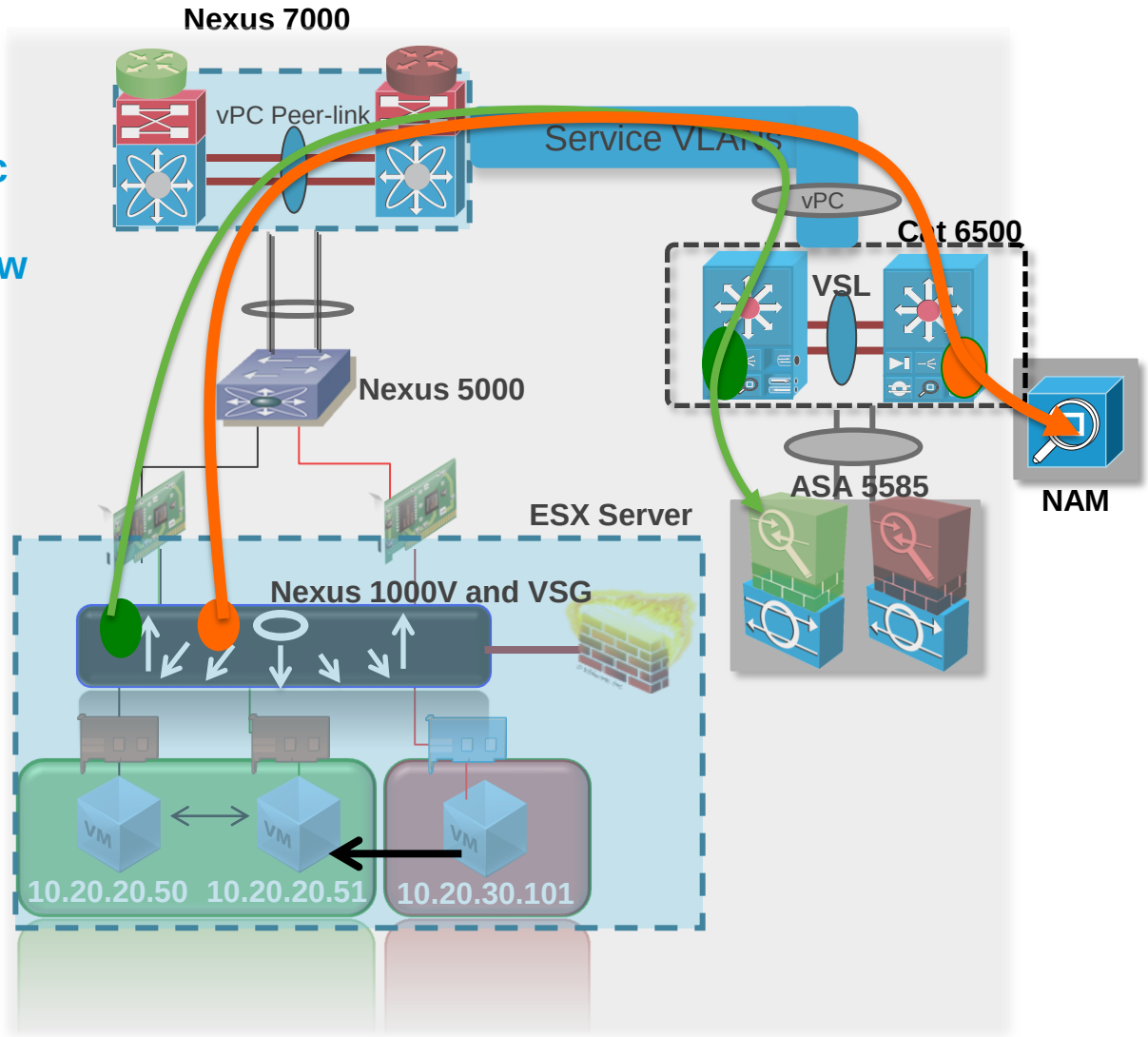
Monitoring Virtual Machine Flows

The Nexus 1000V & ERSPAN

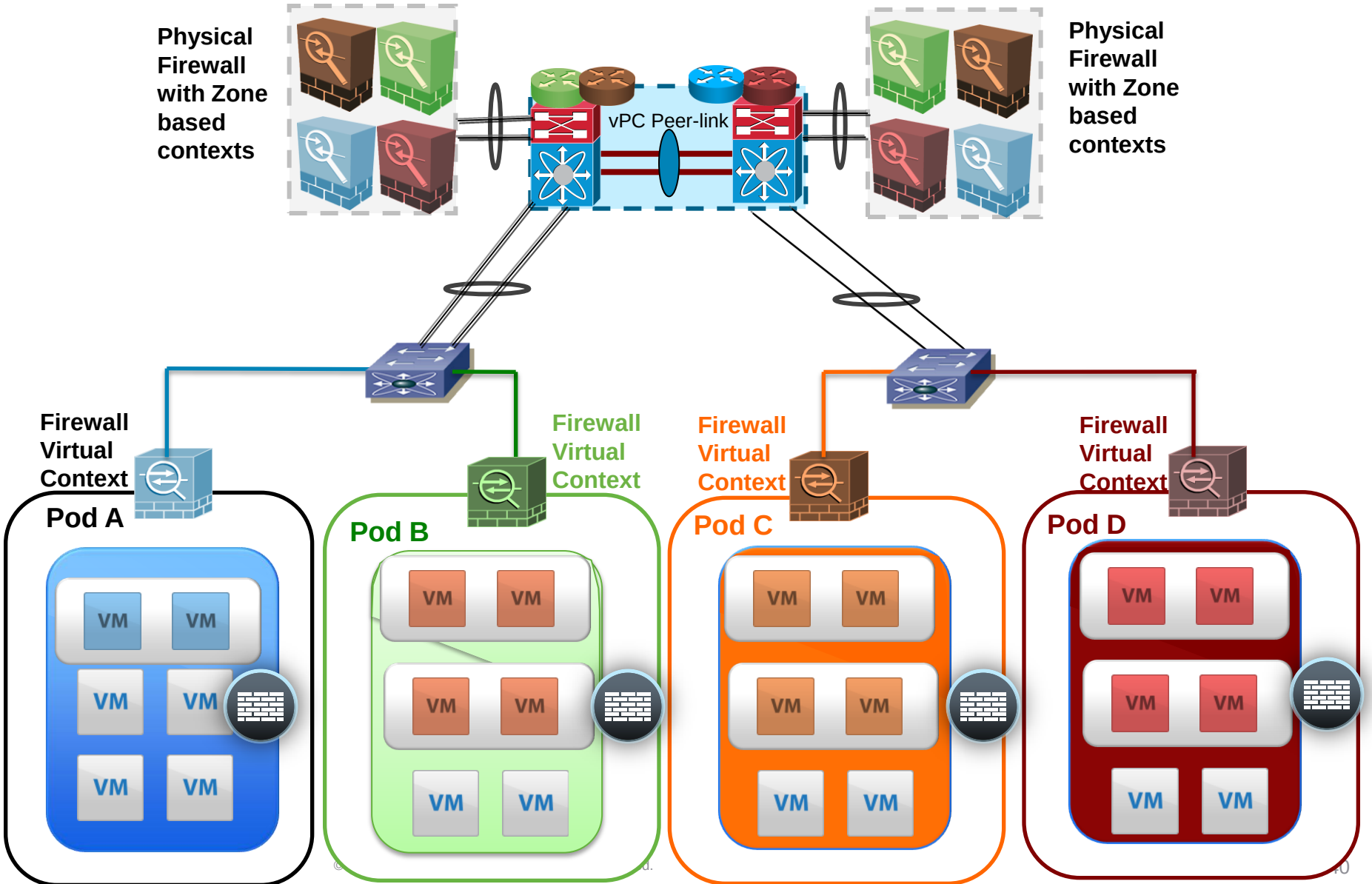
- Visibility of vm-to-vm traffic
- Use existing IDS/IPS
- Use NAM to analyze NetFlow

```
monitor session 1 type erspan-source
 description N1k ERSPAN – session 1
monitor session 3 type erspan-destination
 description N1k ERSPAN to NAM
```

```
monitor session 2 type erspan-source
description N1k ERSPAN –session 2
monitor session 4 type erspan-destination
 description N1k ERSPAN to IDS1
```



Scalable Model

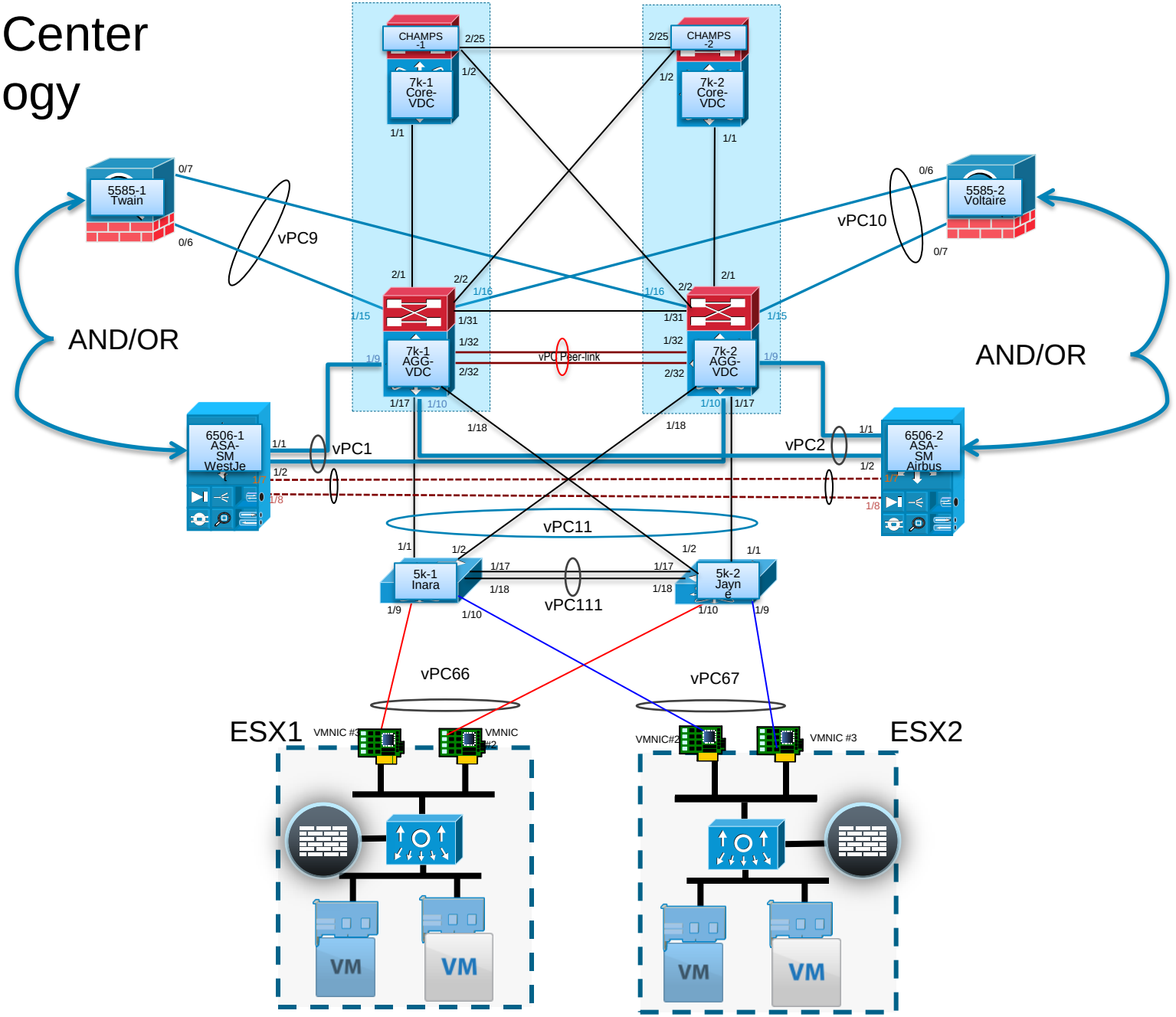


Design Details

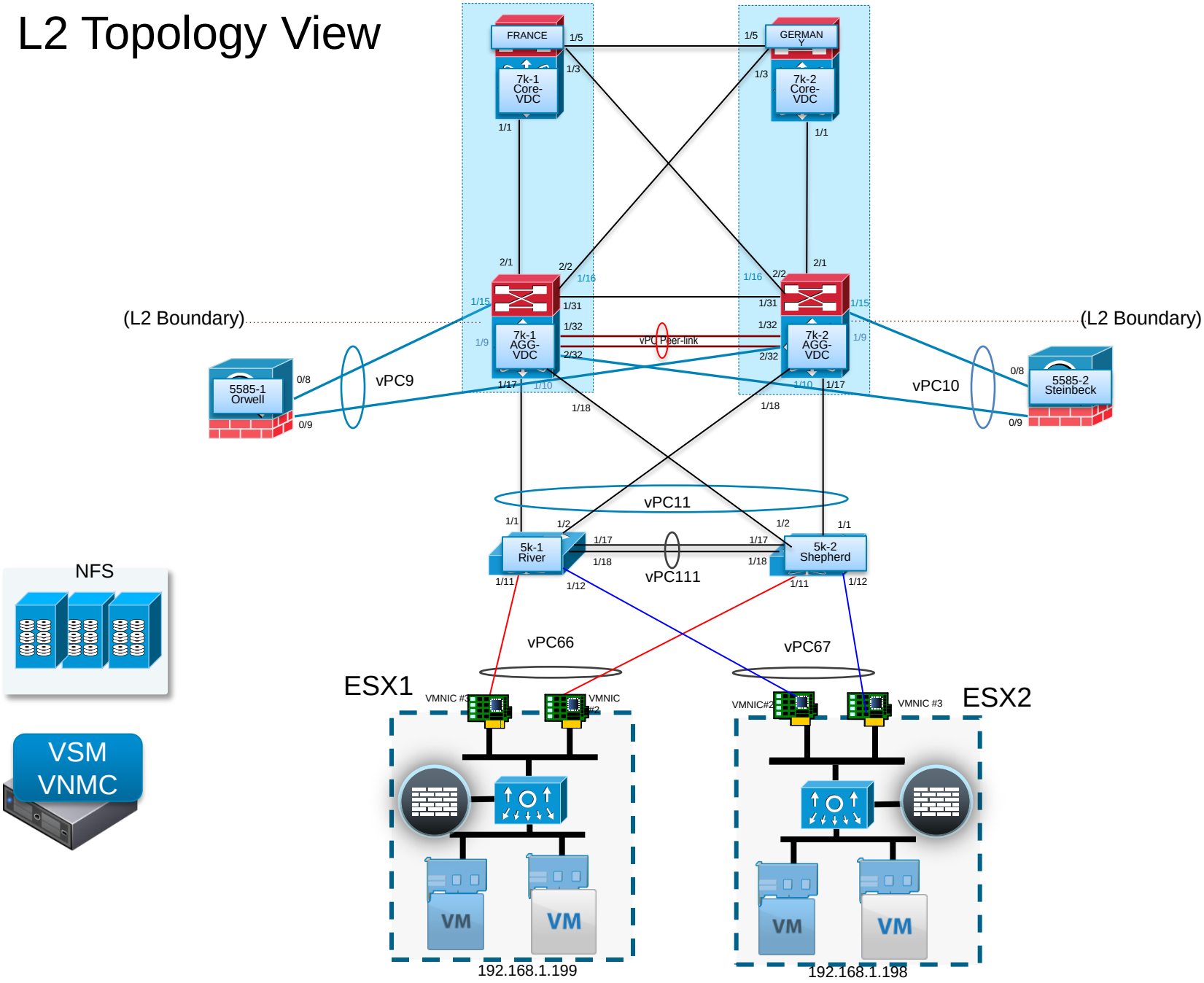
Secure Data Center Test Architecture

- 2x Nexus 7010s with VDCs (Core and Aggregation) (NX-OS 5.1(3))
- 2x Nexus 5Ks for top of rack
- 2x ASA 5585-60 with IPS
- 2x 6500-E with ASA-SMs
- 2x Virtual Security Gateway (VSG) in HA mode
- 2x Nexus 1000V with redundant VSMs
- Identity Services Engine (ISE) for 802.1x user AAA
- Standard VMWare ESXi Infrastructure with multiple service domains (Active Directory, DNS, VDI, etc)

Data Center Topology



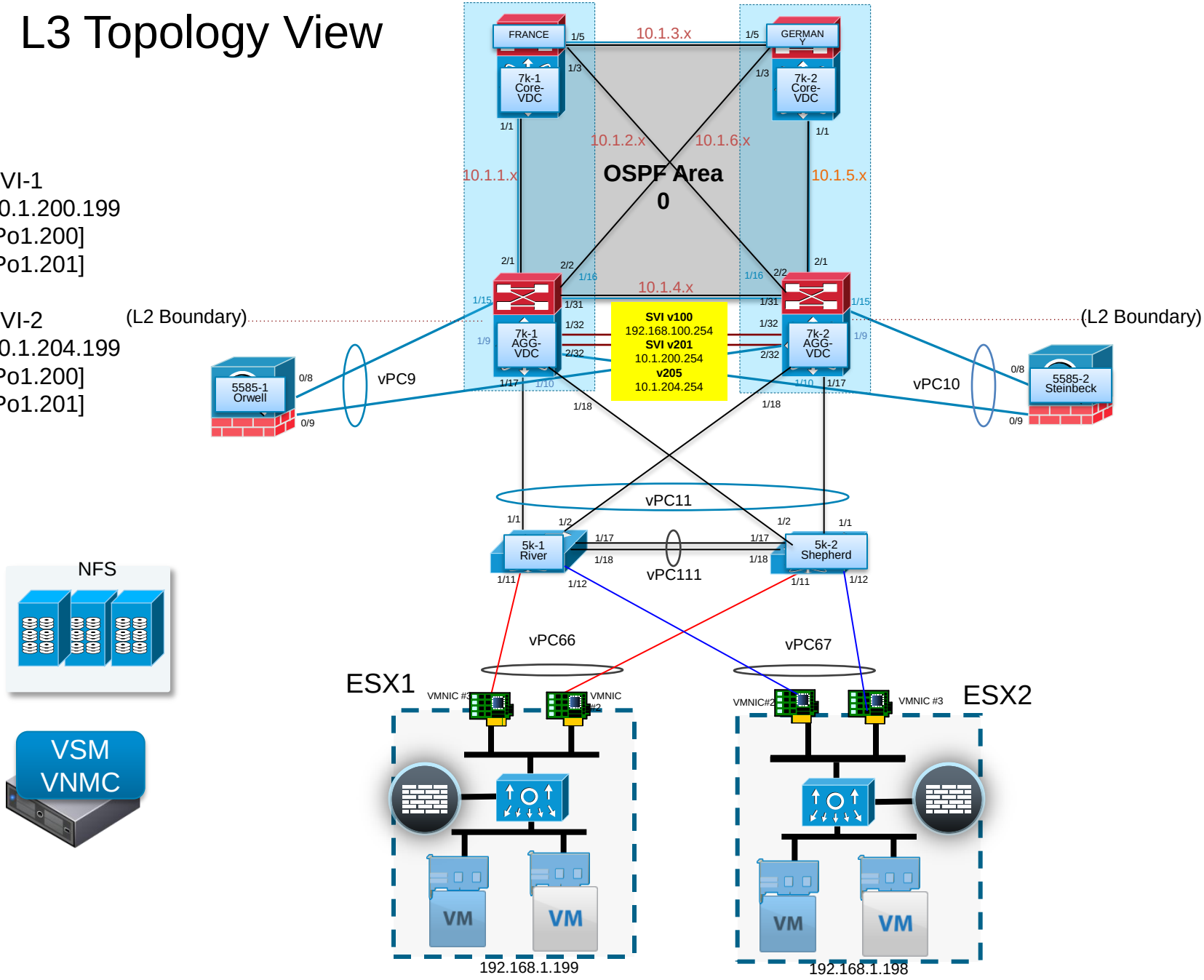
L2 Topology View



L3 Topology View

BVI-1
10.1.200.199
[Po1.200]
[Po1.201]

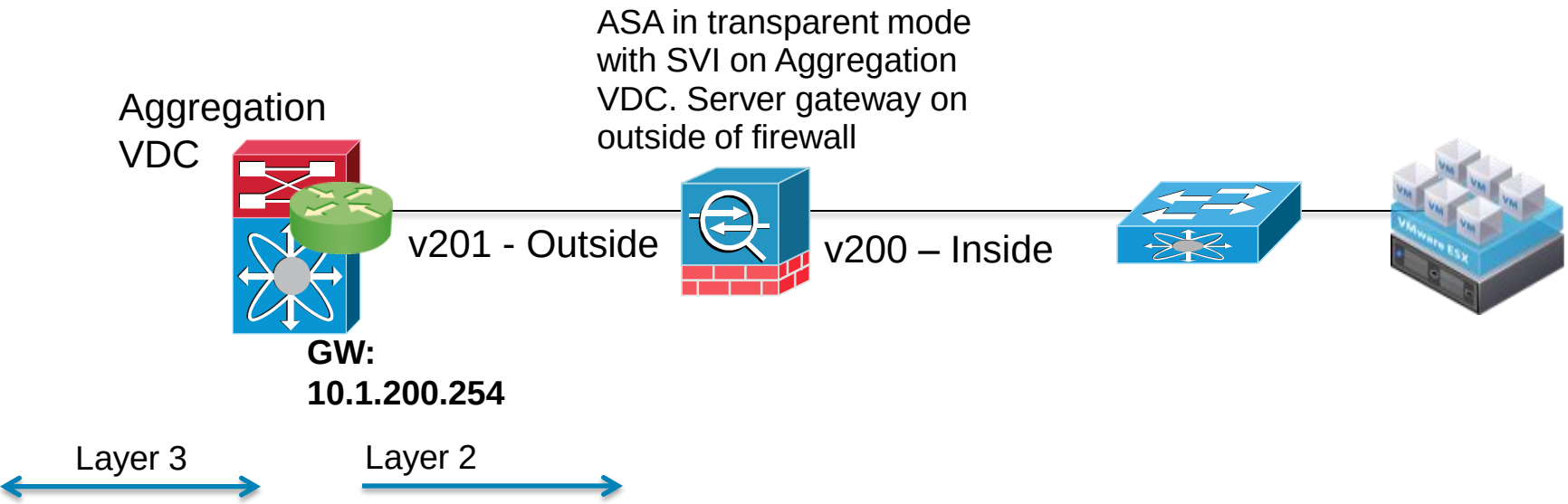
BVI-2
10.1.204.199
[Po1.200]
[Po1.201]



Design Details and Benefits

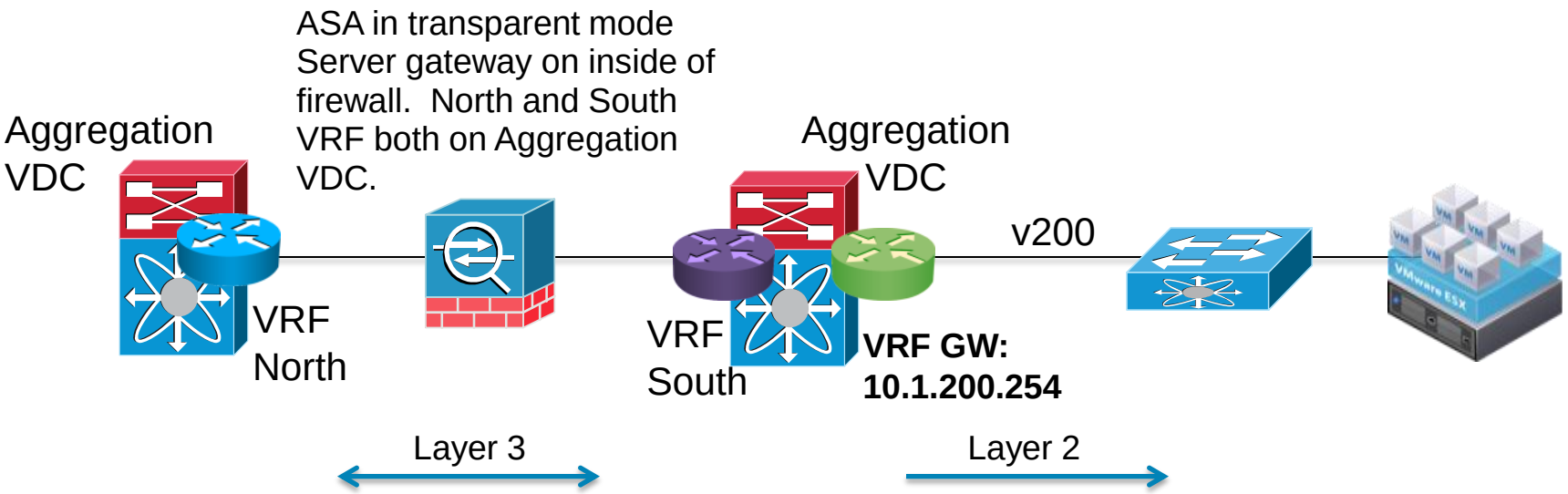
- Virtual Device Contexts (VDC) used to create virtual core and aggregation layer
- vPC used to create loop-free design
- Each ASA firewall is connected to aggregation switch over a dedicated vPC domain
- Each firewall is deployed in transparent mode. Offers easiest integration with existing addressing and flows and additional services (load balancing, etc).
- SVI on each aggregation switch provides default gateway for servers
- Server Gateway location is important – Design dependent – NEXT SLIDE

Server Gateway Outside of Firewall: Design #1



Simple design. Firewall part of layer 2 failure domain.

Server Gateway VRF Sandwich Design #2

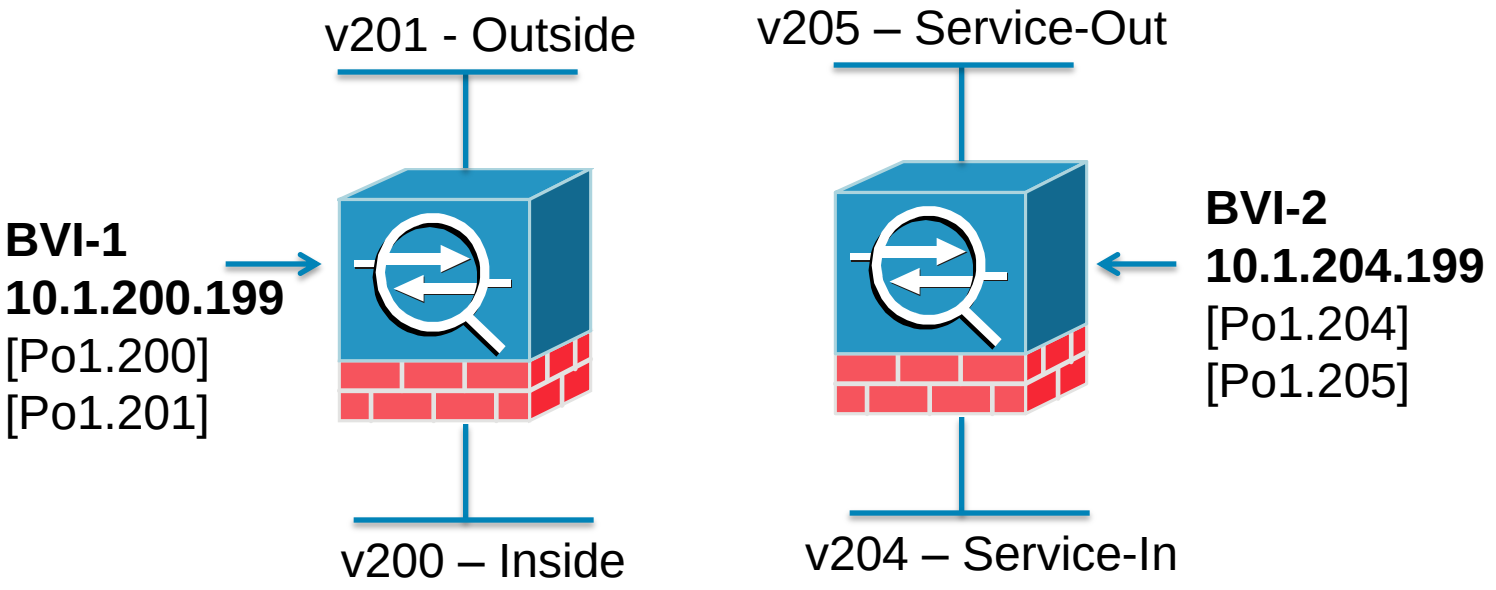


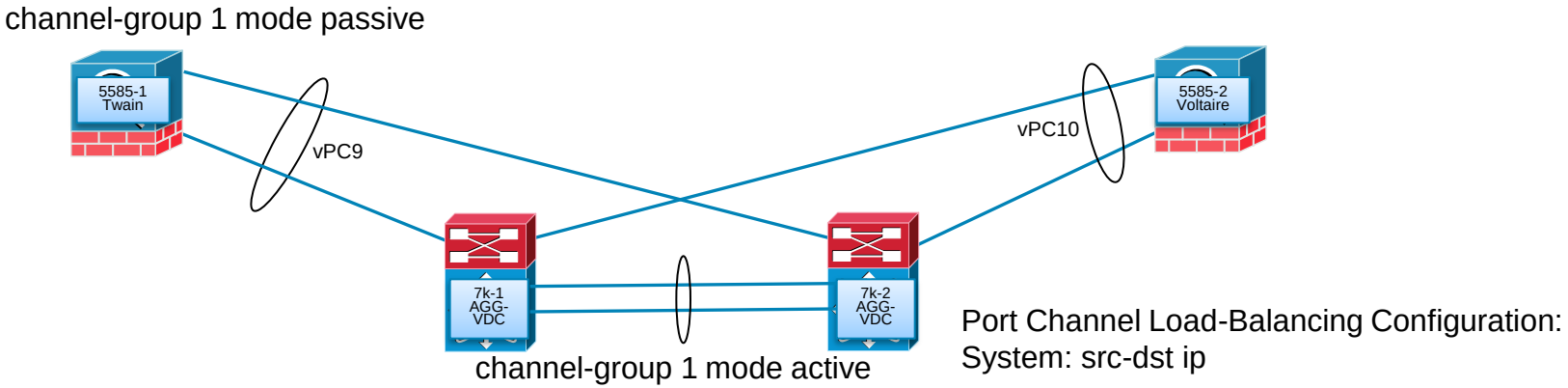
A little more complex design. Gateway on inside of firewall means smaller failure domain.

Design Details and Benefits

- Zone based differentiation, building blocks with VLANs and VRFs
  - ✓Intra-VM firewalling via VSG
  - ✓Intra-zone firewalling via both VSG and ASA/ASA-SM
  - ✓Inter-zone firewalling via ASA or ASA-SM
- Layered security with VRF segmentation via routing
- Identity based access and segmentation via 802.1x + SGTs (TrustSec) + ISE

ASA Details





ASA Multiple Bridge Groups and Duplicate MAC Addresses on Switch

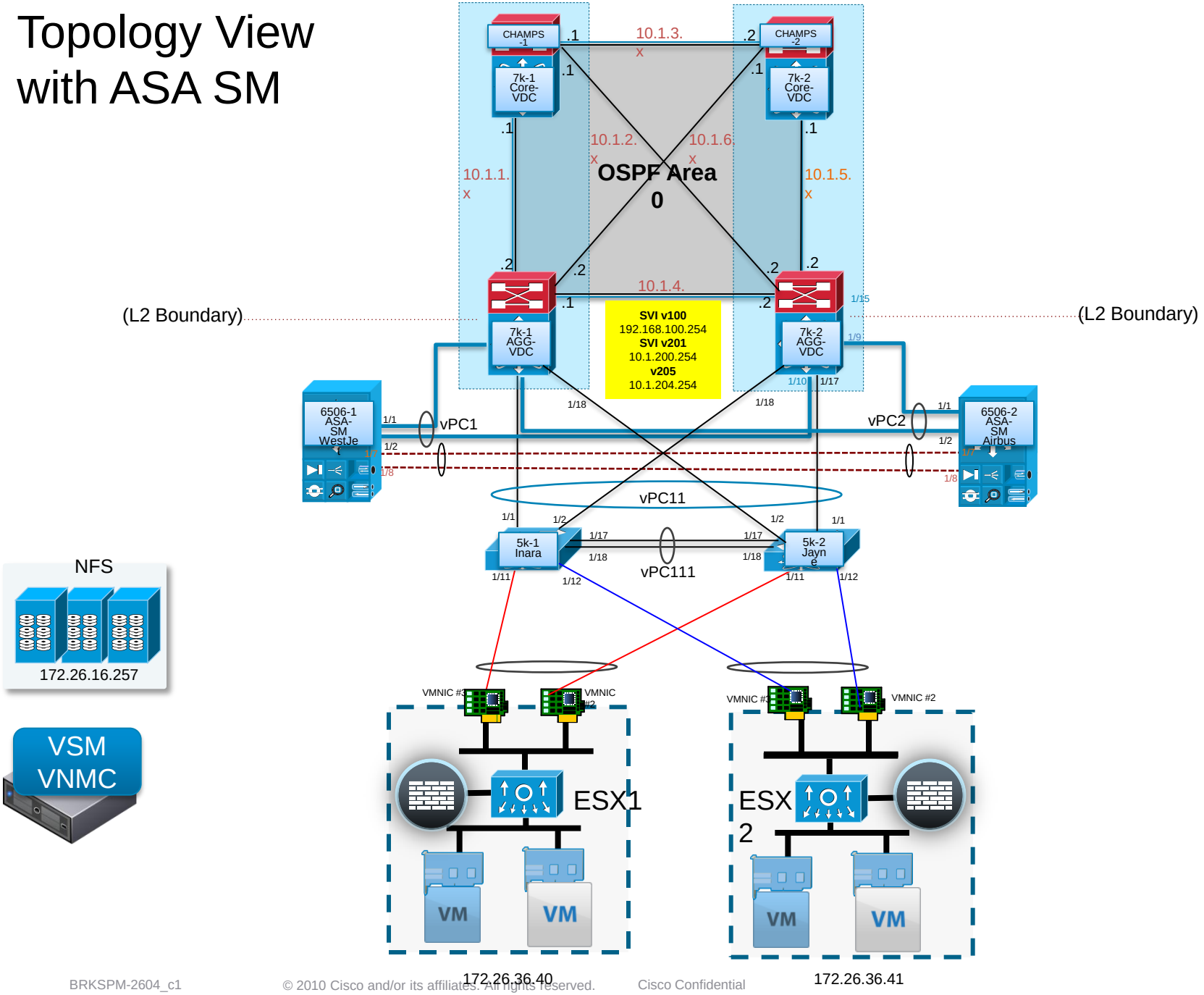
- When using multiple bridge groups within ASA 8.4+ be aware all L3 (SVI) interfaces on Catalyst 6500 and Nexus 7000 use the same MAC address by default

```
champs1-agg-vdc# sh int | i b414.89e1.a043
  Hardware: 10000 Ethernet, address: b414.89e1.a043 (bia f866.f23e.0f86)
  Hardware: 10000 Ethernet, address: b414.89e1.a043 (bia f866.f23e.0f87)
  Hardware: 10000 Ethernet, address: b414.89e1.a043 (bia f866.f23e.0f88)
  Hardware is EtherSVI, address is  b414.89e1.a043
  Hardware is EtherSVI, address is  b414.89e1.a043
  Hardware is EtherSVI, address is  b414.89e1.a043
```

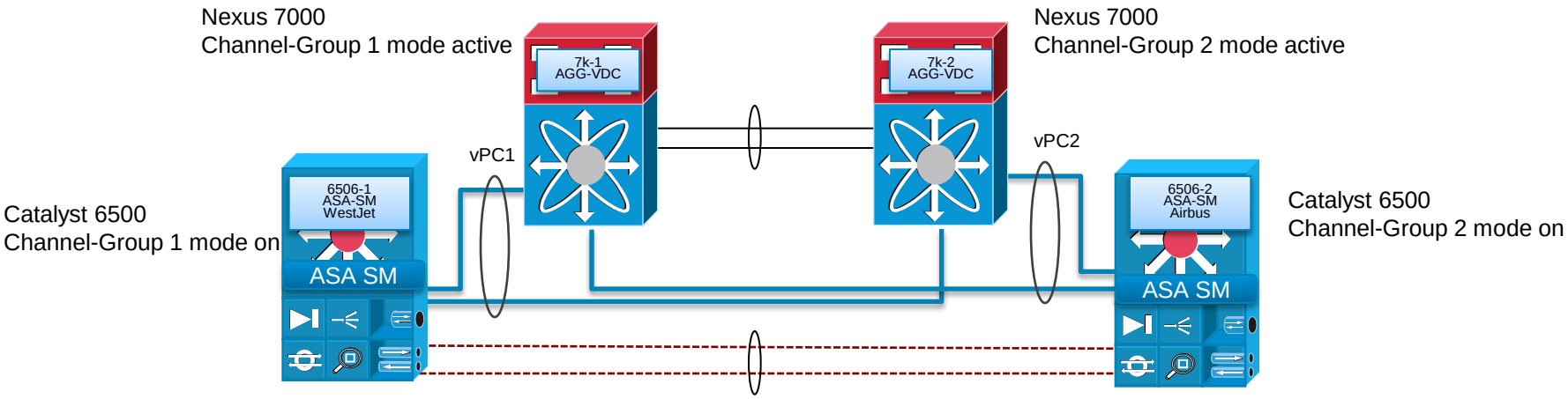
- Same MAC address seen on multiple bridge groups is seen as possible threat and the ASA drops the packet
- Easy fix is to create a unique MAC for each L3 interface

```
champs1-agg-vdc(config)# int vlan 100
champs1-agg-vdc(config-if)# mac-address b414.89e1.1111
champs1-agg-vdc(config-if)# int vlan 201
champs1-agg-vdc(config-if)# mac-address b414.89e1.2111
champs1-agg-vdc(config-if)# int vlan 205
champs1-agg-vdc(config-if)# mac-address b414.89e1.3111
```

Topology View with ASA SM

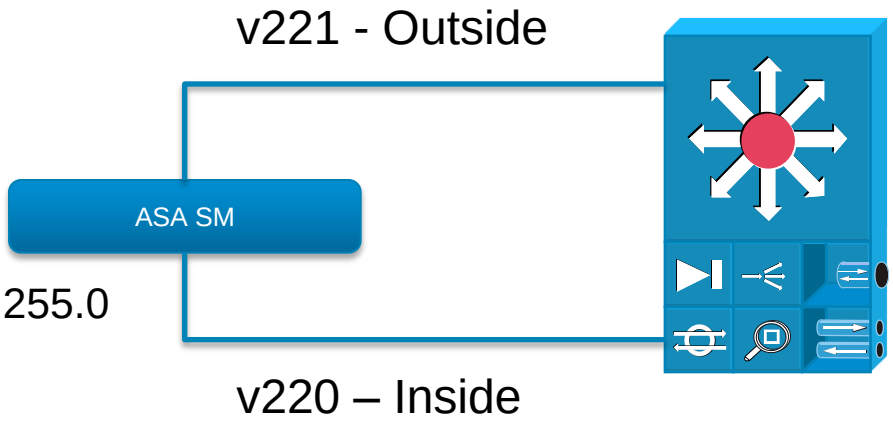


Nexus 7000 & Cat 6500 Channel Group Modes



ASA SM Layer 2 and 3

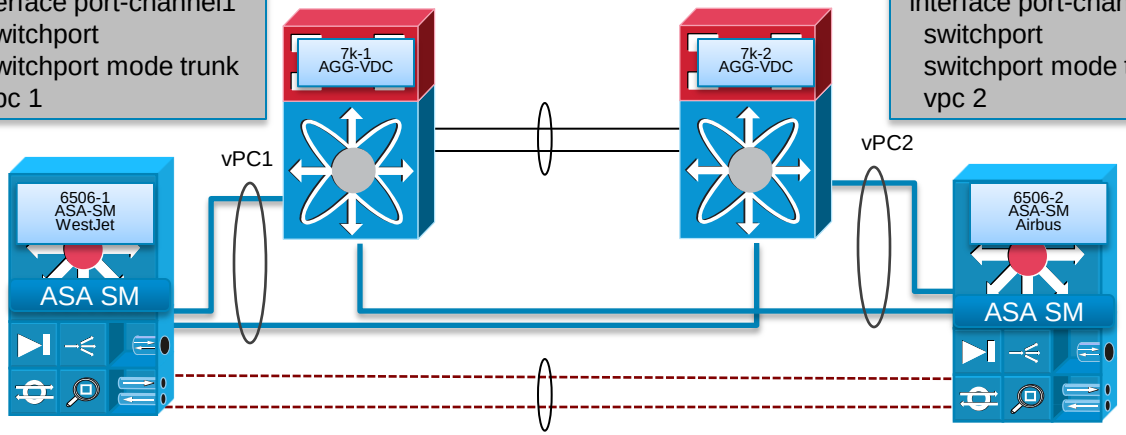
interface BVI2
 description bvi for 221 and 220
 ip address 10.1.221.199 255.255.255.0



ASA SM Details

```
interface Vlan221
  mac-address
b414.89e1.2222
  ip address
10.1.221.252/24
  hsrp 21
    preempt
    priority 105
    ip 10.1.221.254

interface port-channel1
  switchport
  switchport mode trunk
  vpc 1
```

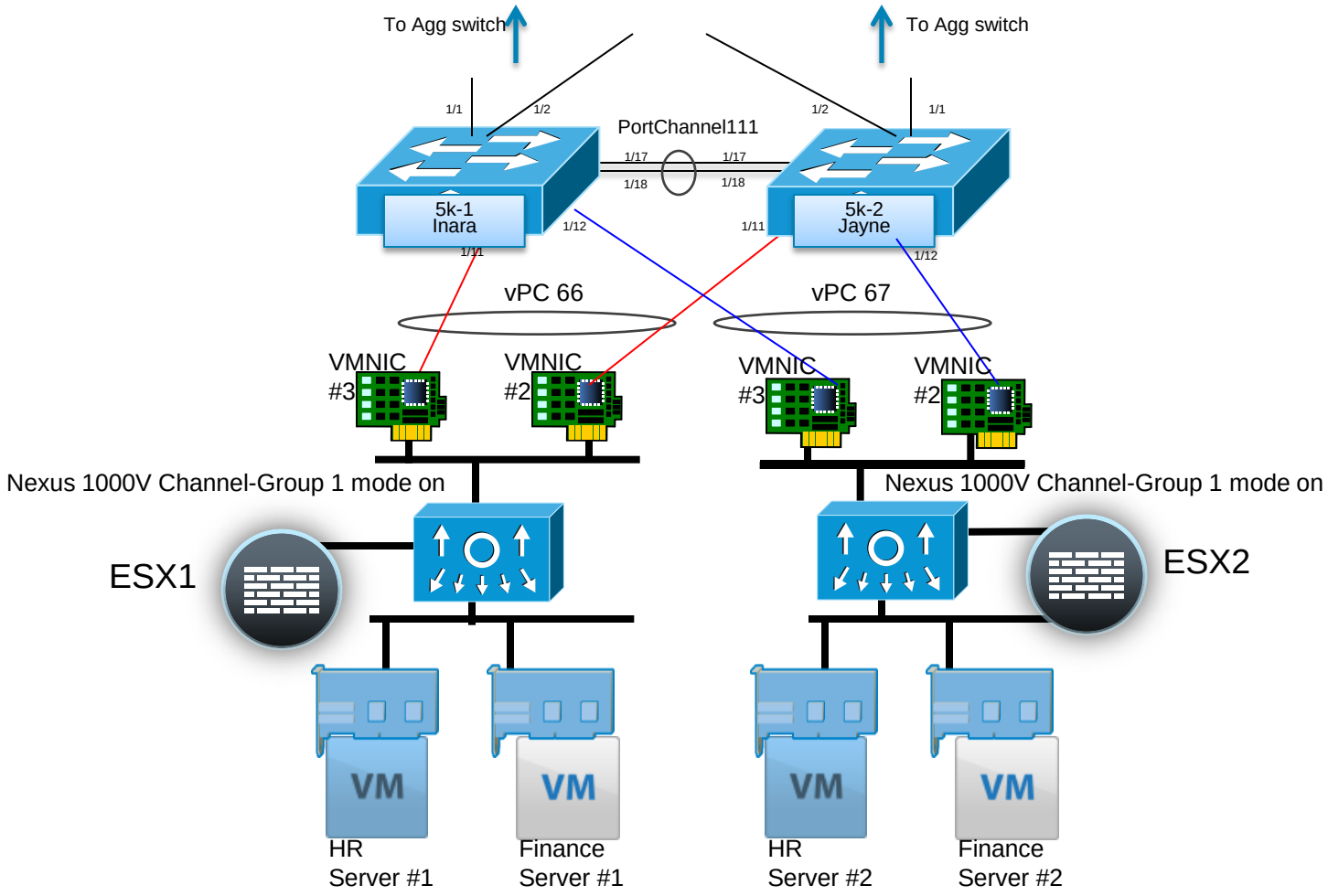
```
interface Vlan221
  mac-address
b414.89e1.3333
  ip address
10.1.221.253/24
  hsrp 21
    preempt
    priority 100
    ip 10.1.221.254

interface port-channel2
  switchport
  switchport mode trunk
  vpc 2
```



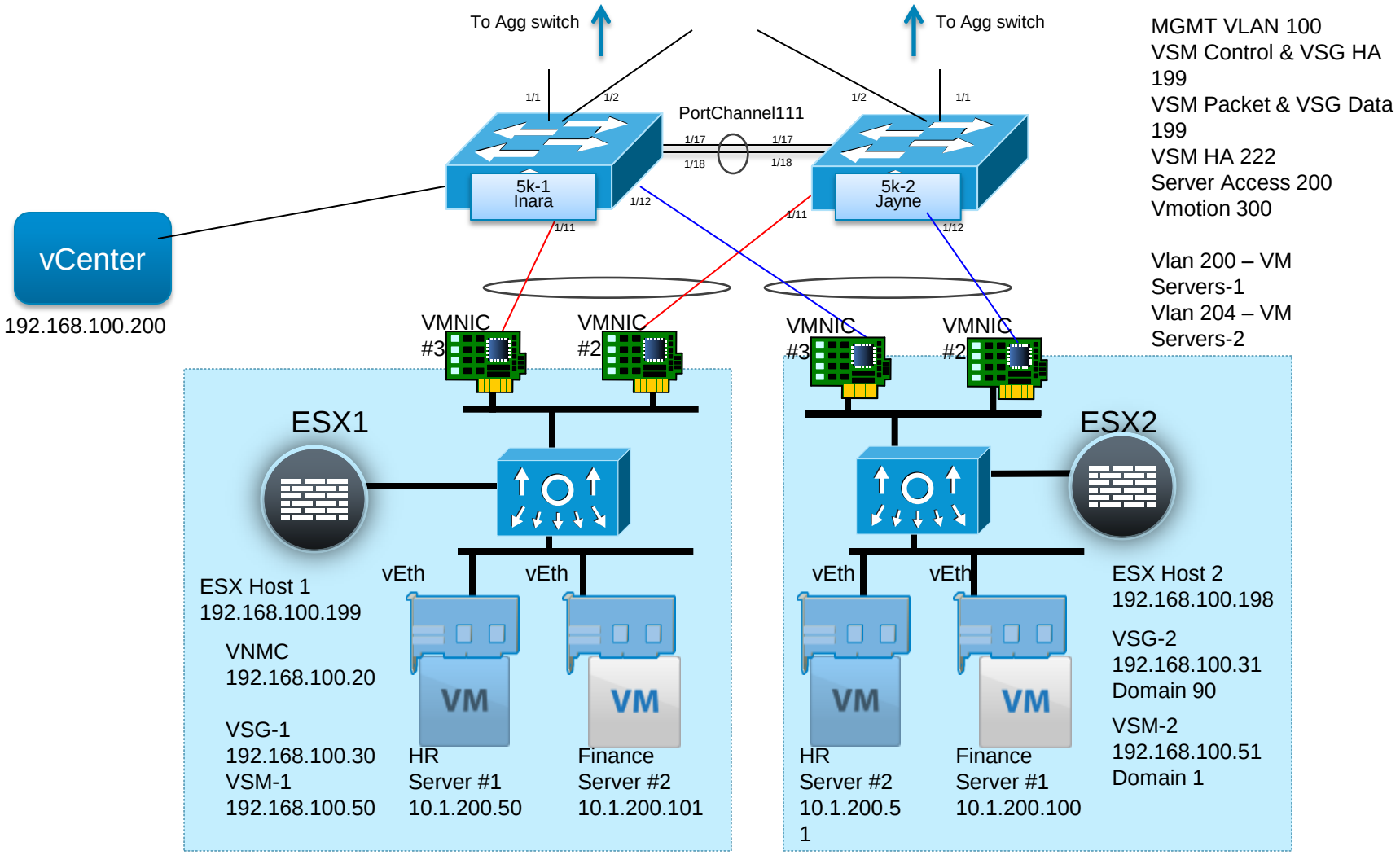

```
     BVI2
     ip address
     10.1.221.199

interface Vlan220
 nameif inside
 bridge-group 2
 security-level 100
!
interface Vlan221
 nameif outside
 bridge-group 2
 security-level 0
```

```
failover lan interface Failover Vlan44
failover link State Vlan45
failover interface ip Failover 10.90.44.1 255.255.255.0 standby 10.90.44.2
failover interface ip State 10.90.45.1 255.255.255.0 standby 10.90.45.2199
```

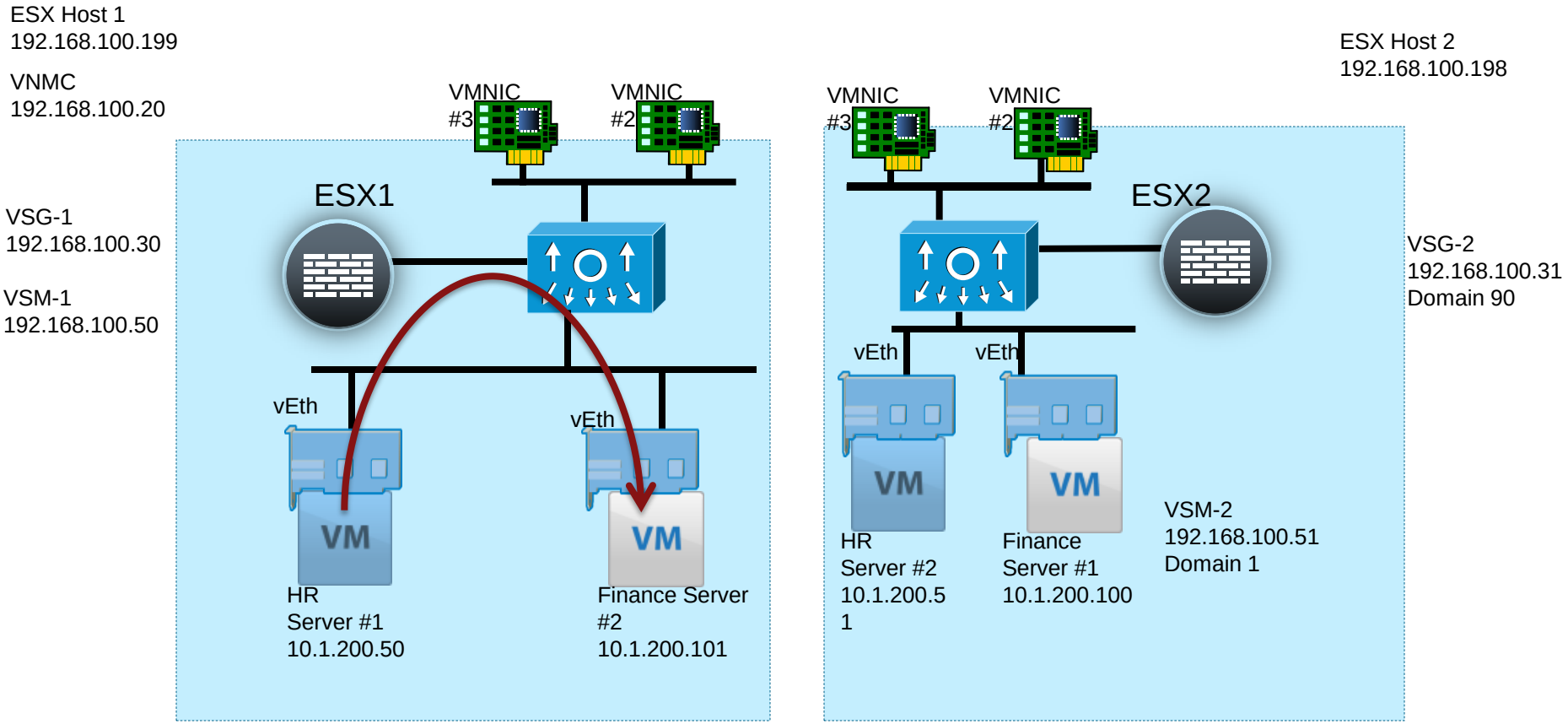
Server Access and VM Environment



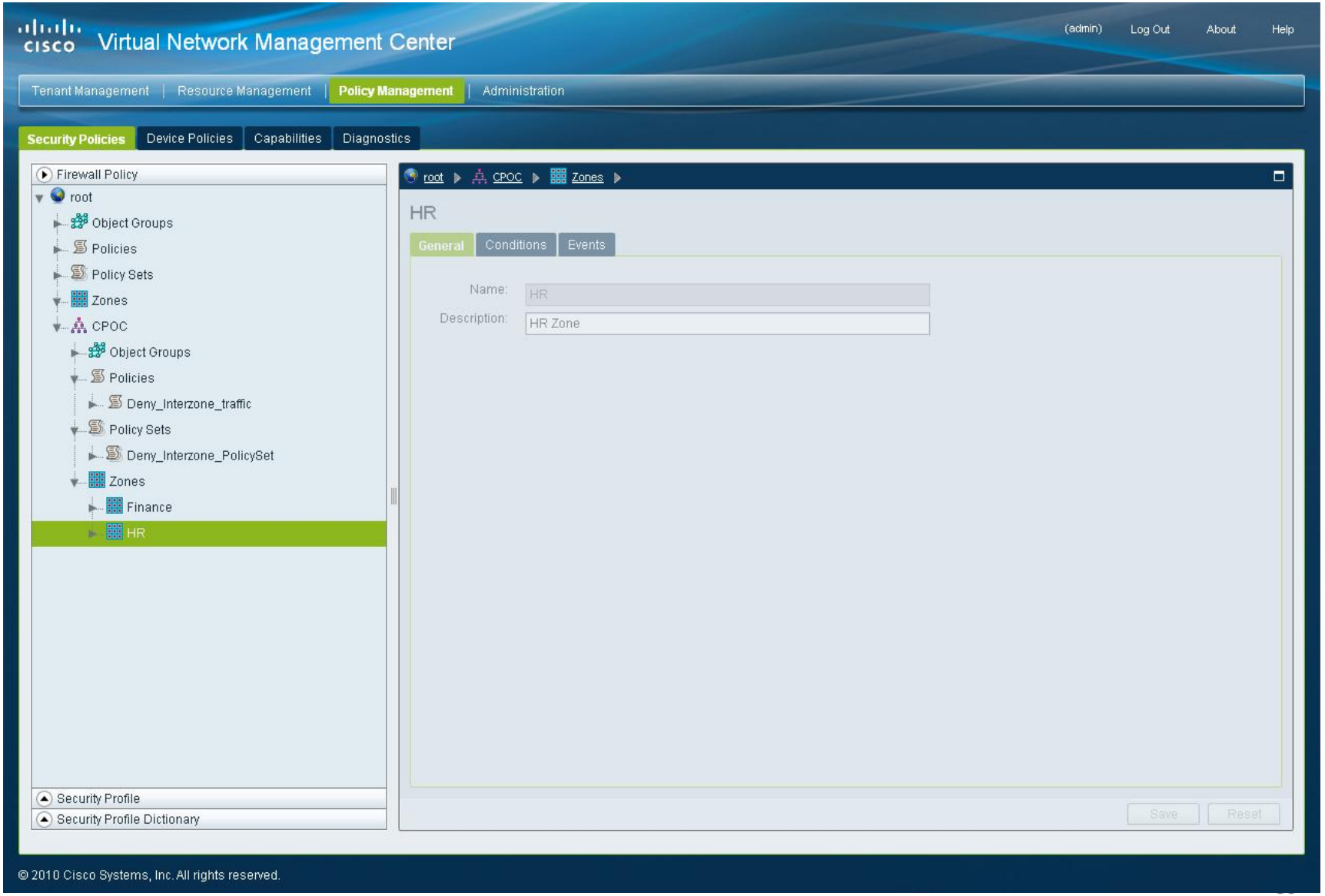
Server Access and VM Network Details



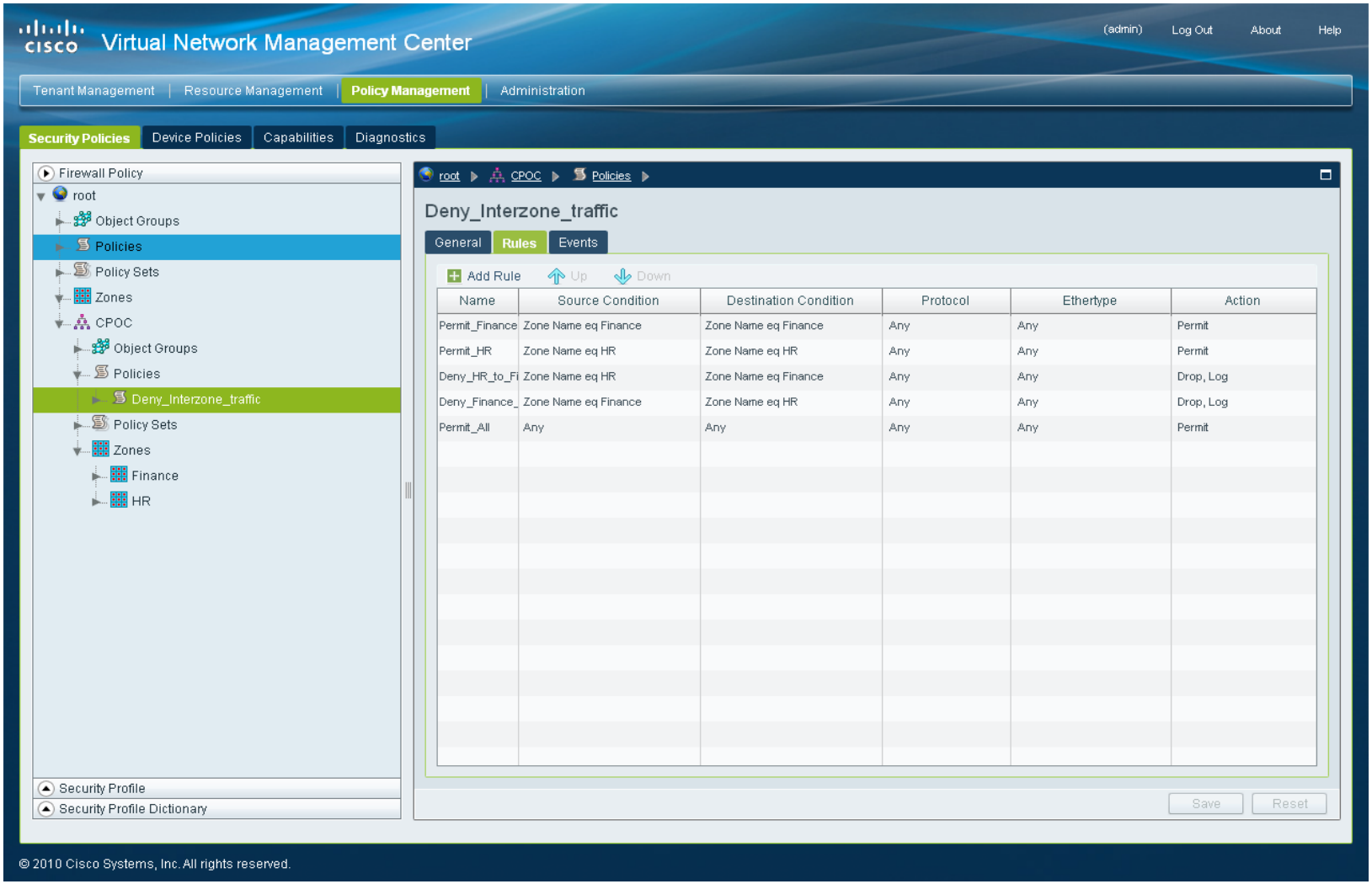
Deny HR to Finance



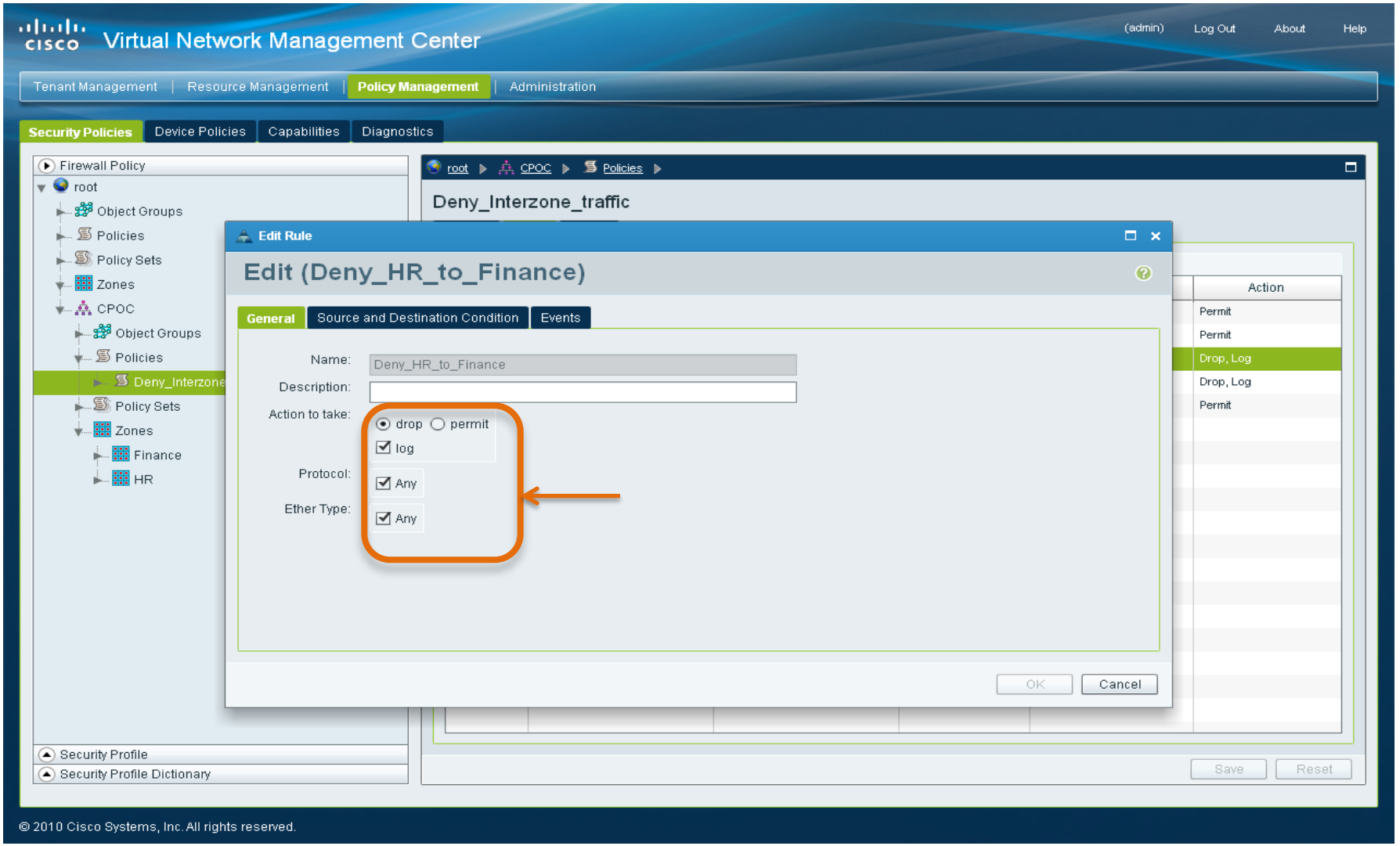
Policy Heirarchy



VNMC: Deny Interzone Policy

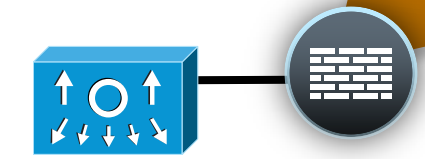


VNMC Policy: Deny HR to Finance Requests



Policy Summary on VSG

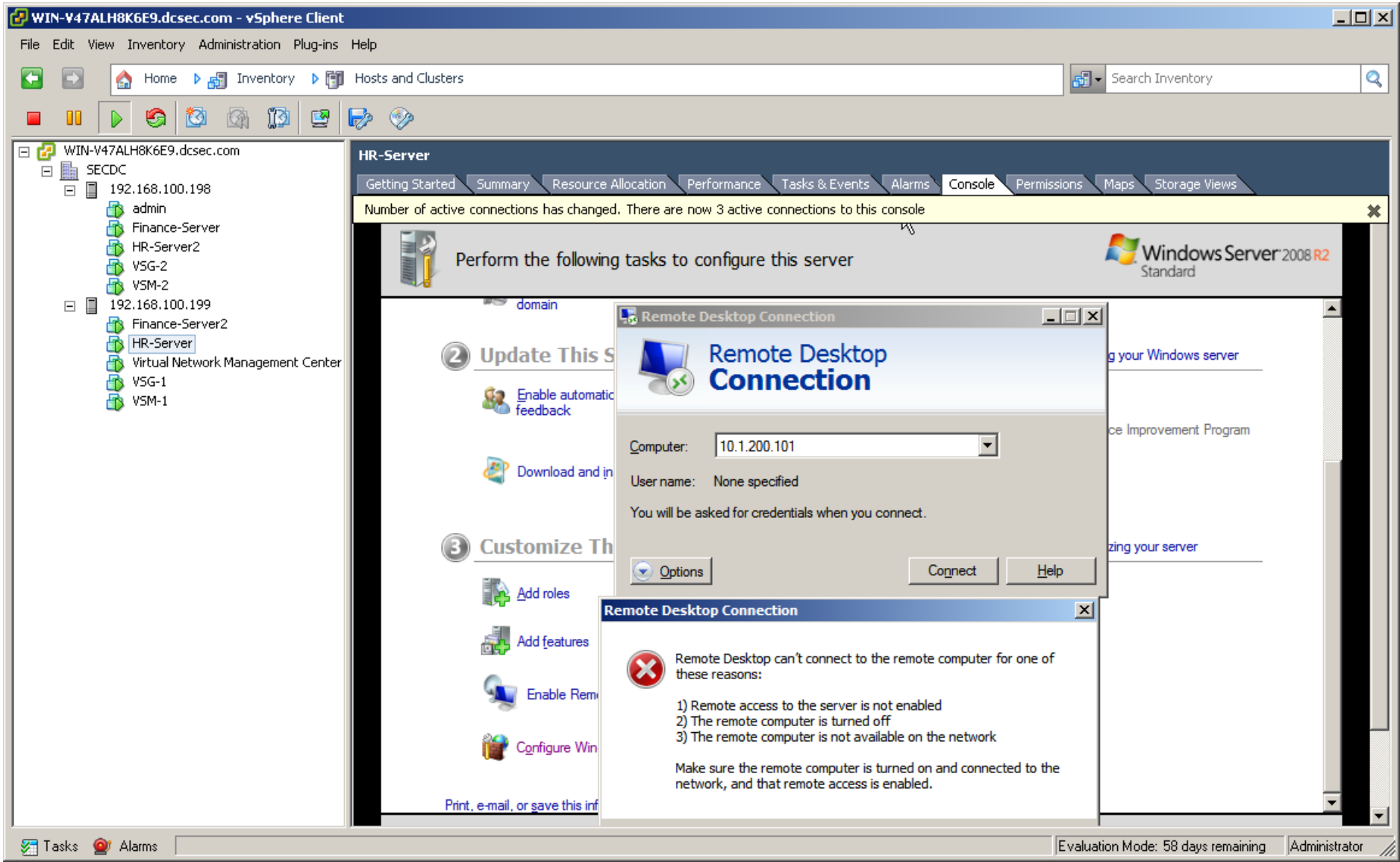
```
firewall# show running-config policy

policy default@root
  rule default/default-rule@root order 2
policy Deny_Interzone_PolicySet@root/CPOC
  rule Deny_Interzone_traffic/Permit_Finance@root/CPOC order 26
  rule Deny_Interzone_traffic/Permit_HR@root/CPOC order 51
  rule Deny_Interzone_traffic/Deny_HR_to_Finance@root/CPOC order 101
  rule Deny_Interzone_traffic/Deny_Finance_to_HR@root/CPOC order 201
  rule Deny_Interzone_traffic/Permit_All@root/CPOC order 301

firewall# show policy-engine stats

Policy Match Stats:

default@root                          :          0
  default/default-rule@root           :          0 (Drop)
  NOT_APPLICABLE                      :          0 (Drop)

Deny_Interzone_PolicySet@root/CPOC                          :       7703
  Deny_Interzone_traffic/Permit_Finance@root/CPOC           :         11 (Permit)
  Deny_Interzone_traffic/Permit_HR@root/CPOC                :          2 (Permit)
  Deny_Interzone_traffic/Deny_HR_to_Finance@root/CPOC       :          1 (Log, Drop)
  Deny_Interzone_traffic/Deny_Finance_to_HR@root/CPOC       :          2 (Log, Drop)
  Deny_Interzone_traffic/Permit_All@root/CPOC               :       7687 (Permit)
  NOT_APPLICABLE                                            :          0 (Drop)
```



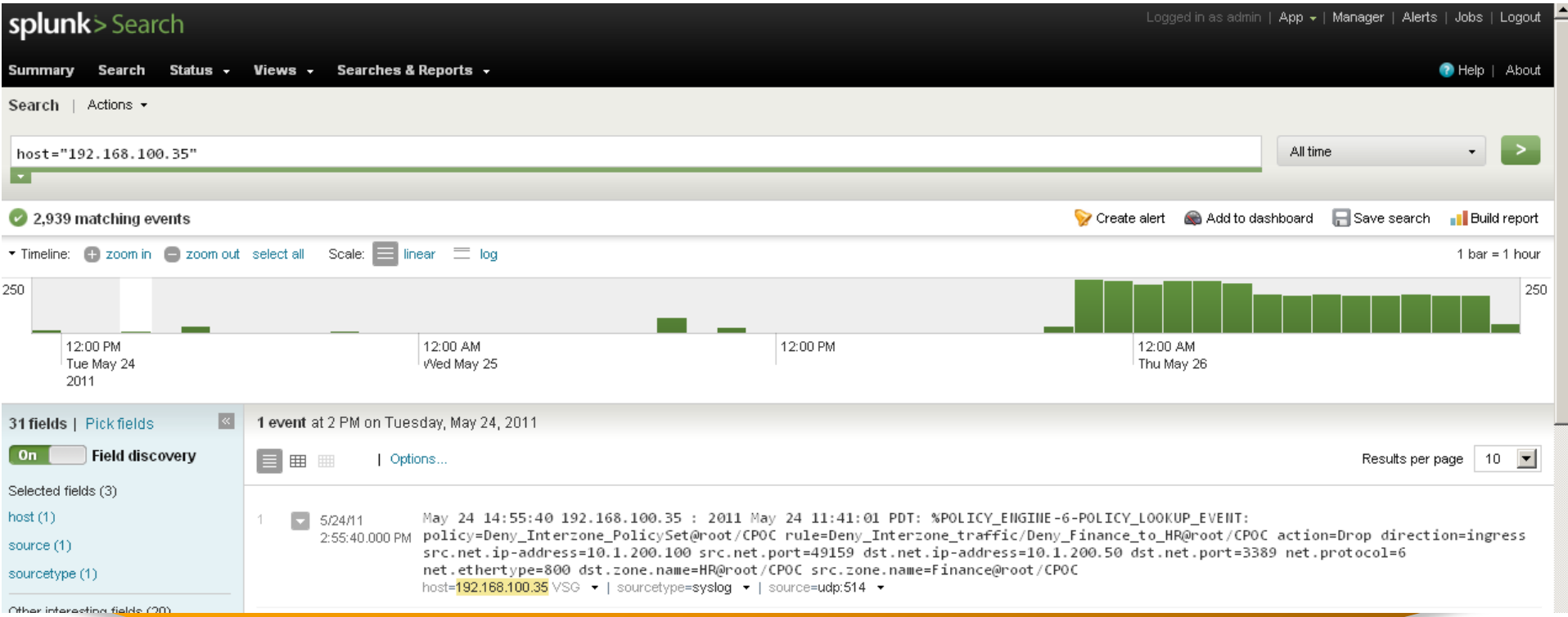
Nexus 1000V

VSG

Denied Connection Attempt from HR to Finance



Syslog from VSG



Learn. Connect. Collaborate. together.

Driving Simplicity: Data Center Design – Resources from Cisco

Validated Design Guides

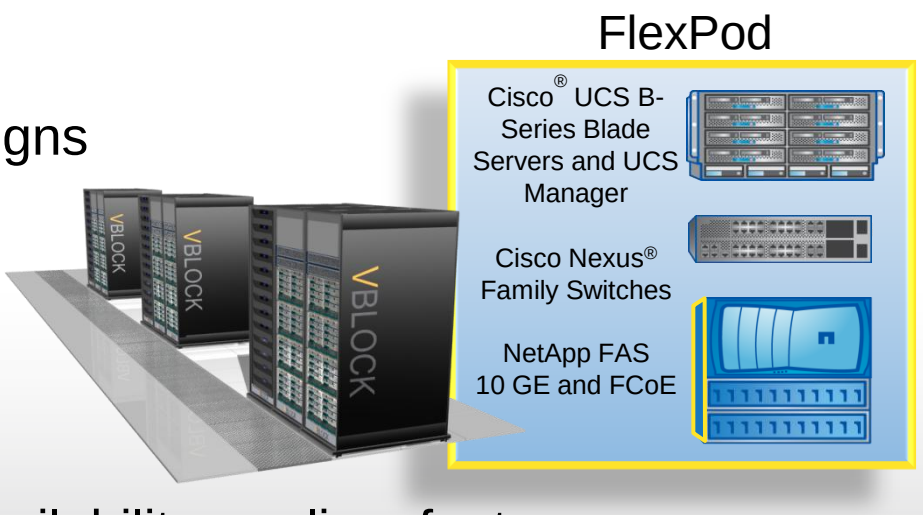
A Cisco Competitive Differentiator

Design Zone

- Cisco Validated Designs are recommended, validated, end-to-end designs for next-generation networks.
- The validated designs are tested and fully documented to help ensure faster, more reliable, and more predictable customer deployments.
- 3 types of guides
  - •Design Guides – comprehensive design/implementation
  - •Application Deployment Guides - Third-party applications
  - •System Assurance Guides - intensive, ongoing system assurance test programs targeted at major network architectures or technologies.

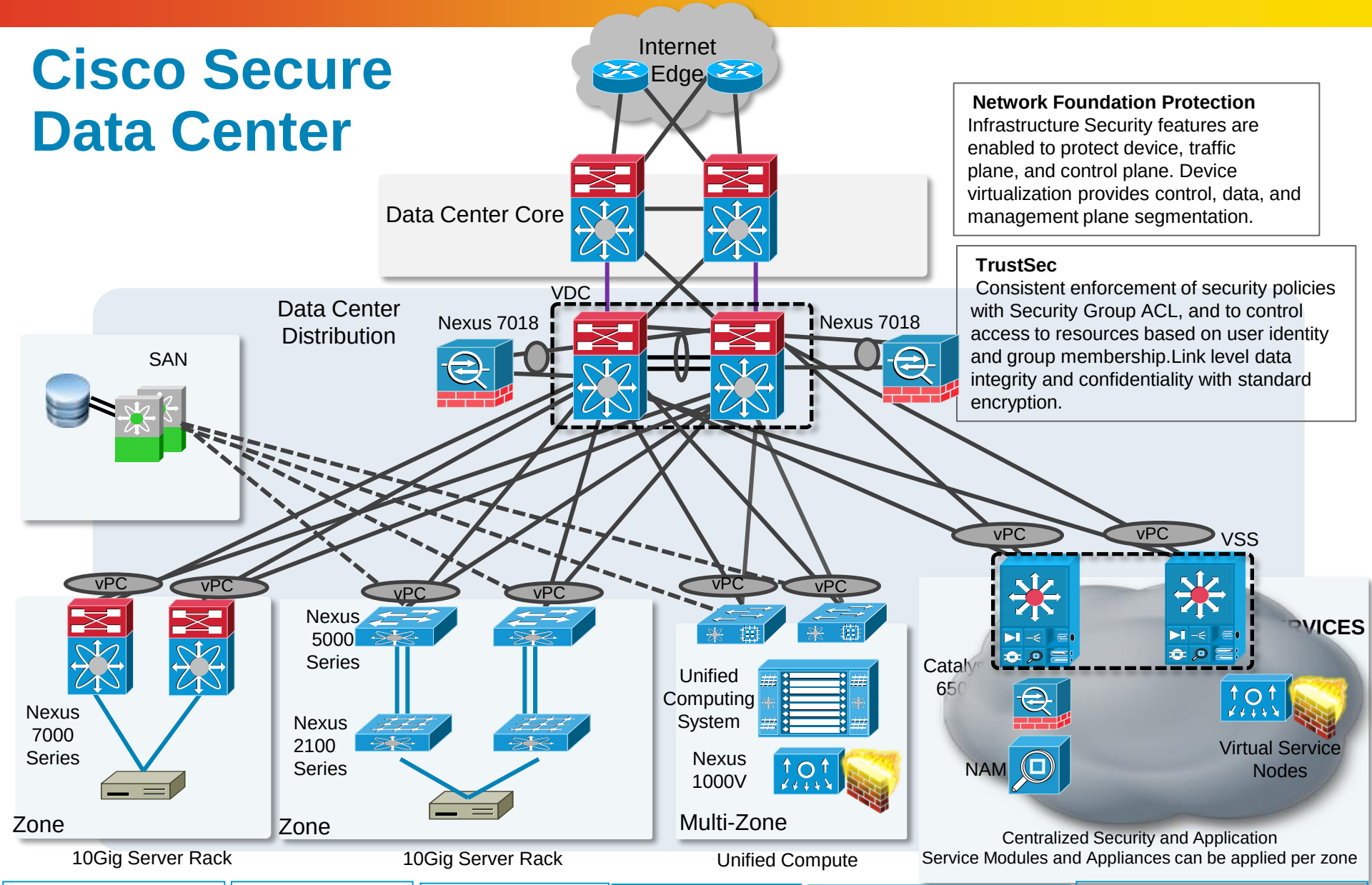
Data Center Validated Designs

- Partnership: VMWare, EMC, NetApp, BMC, Citrix, WYSE, Microsoft, and more.
- Vblock, FlexPod
- Enterprise and Service Provider designs
- Secure Multi-Tenant designs
- Cloud Computing & Automation
- Virtualized infrastructure integration
- Architecture recommendations for availability, scaling, feature integration, application and security services



WWW.CISCO.COM/GO/DESIGNZONE

Cisco Secure Data Center



Network Foundation Protection
Infrastructure Security features are enabled to protect device, traffic plane, and control plane. Device virtualization provides control, data, and management plane segmentation.

TrustSec
Consistent enforcement of security policies with Security Group ACL, and to control access to resources based on user identity and group membership.Link level data integrity and confidentiality with standard encryption.

Centralized Security and Application Service Modules and Appliances can be applied per zone

Stateful Packet Filtering
Additional Application Firewall Services for Server Farm zone specific protection

Network Intrusion Prevention
IPS/IDS: provides traffic analysis and forensics

Server Load Balancing
Masks servers and applications and provides scaling

Web and Email Security
Security and filtering for Web and Email applications

Access Edge Security
ACL, Dynamic ARP Inspection, DHCP Snooping, IP Source Guard, Port Security, Private VLANs, QoS

Flow Based Traffic Analysis
NAM virtual blade. Traffic analysis and reporting, Application performance monitoring. VM-level interface statistics

Complete Your Session Evaluation

- Please give us your feedback!!

  Complete the evaluation form you were given when you entered the room
- This is session 4.3

Don’t forget to complete the overall event evaluation form included in your registration kit

YOUR FEEDBACK IS VERY IMPORTANT FOR US!!! THANKS