



Cisco Networkers 2011

November 7, 2011 - Hong Kong

Cloud Security and Virtualized Data Center Security



Learn. Connect.
Collaborate. *together.*

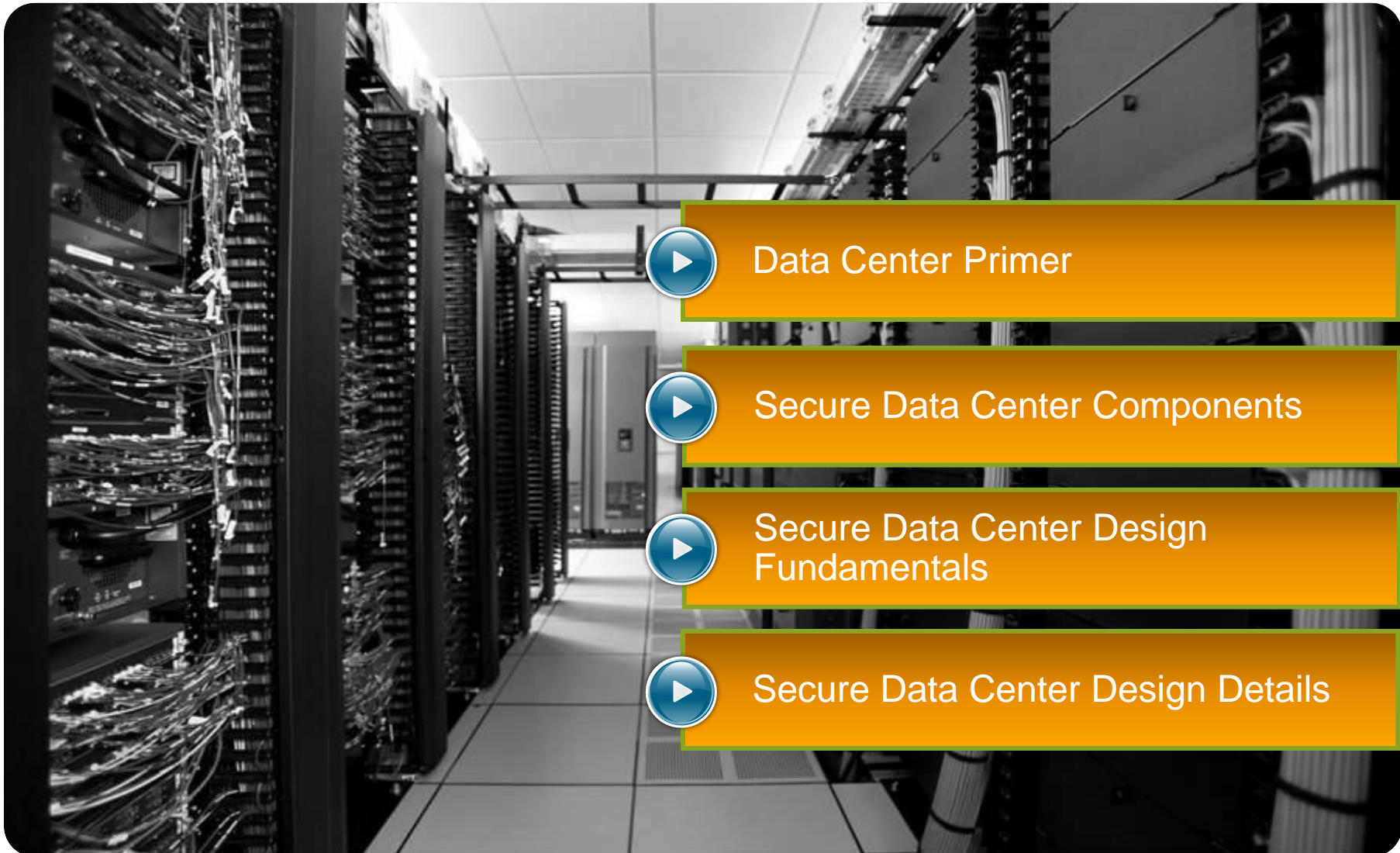


**Data Center, Security, & Virtualization: It's so easy
just ask this happy 35 year old Administrator**

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



Data Center Primer



Secure Data Center Components



Secure Data Center Design
Fundamentals



Secure Data Center Design Details

Data Center Primer: Terms and Technology



Virtualization in the Data Center

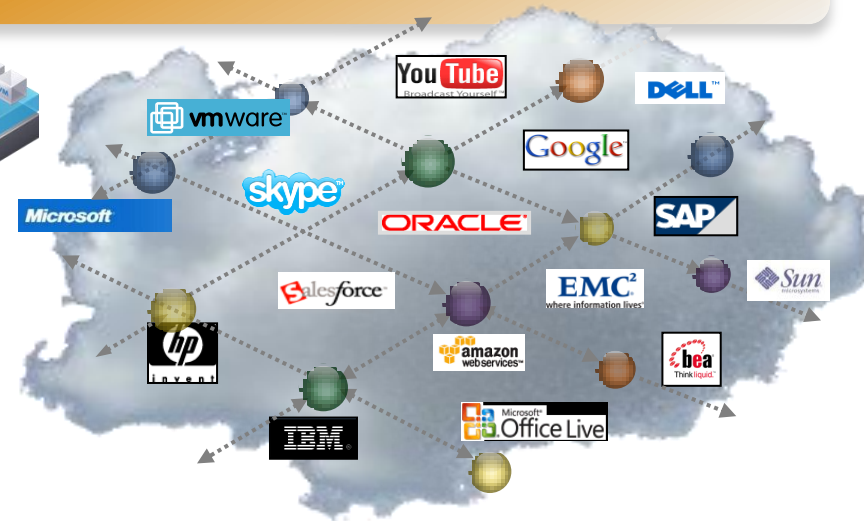
Legacy

- 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

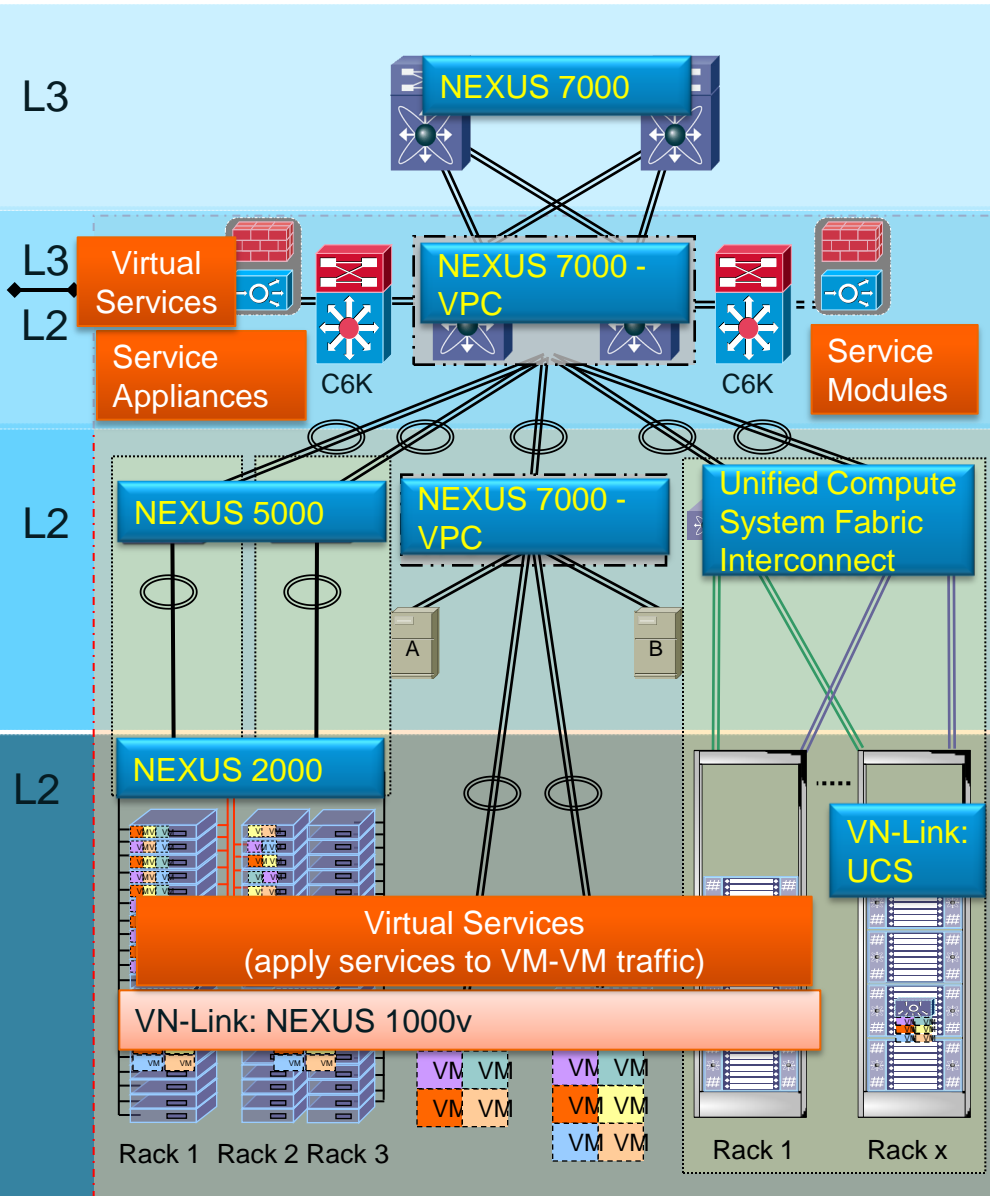
Cisco Datacenter Terms Primer

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 centralized 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

Learn. Connect.
Collaborate. *together.*

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



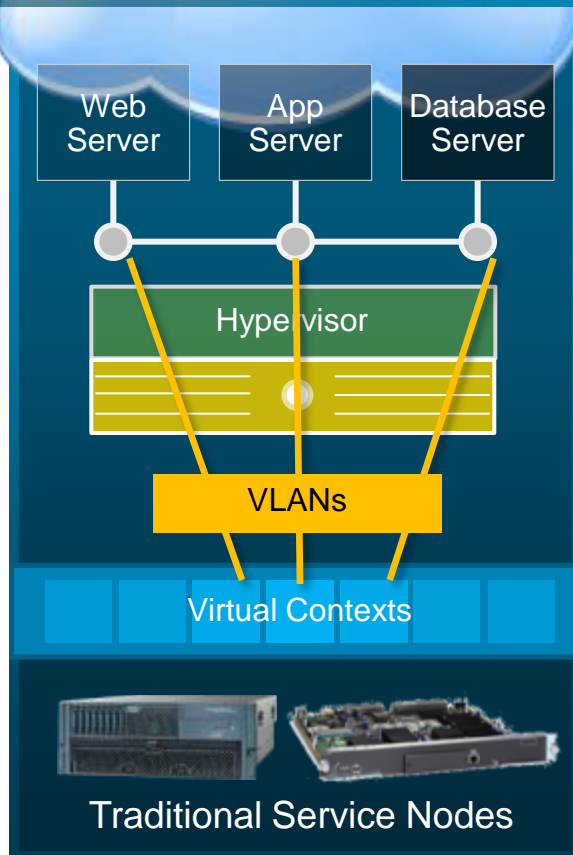
Virtualization is Driving Changes

- 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

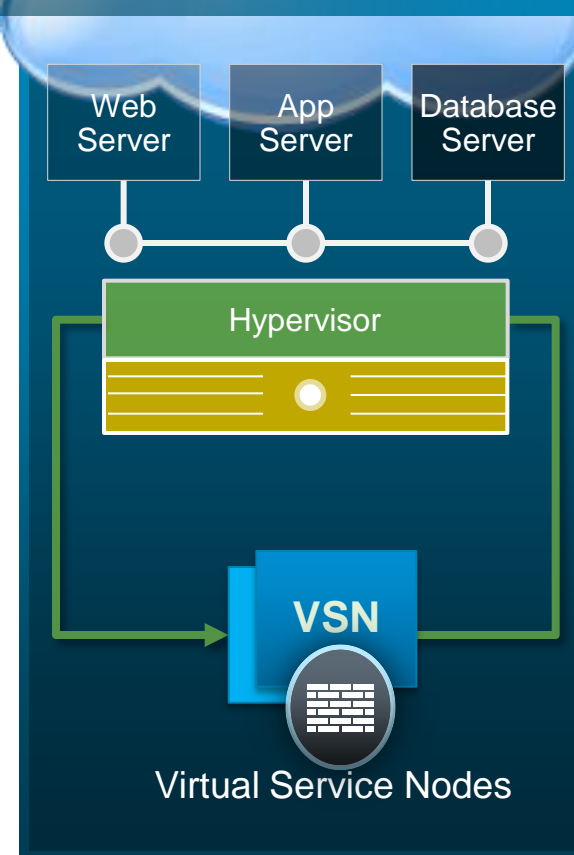
1

Redirect VM traffic via VLANs to external (physical) appliances



2

Apply hypervisor-based network services



The Data Center Firewalls

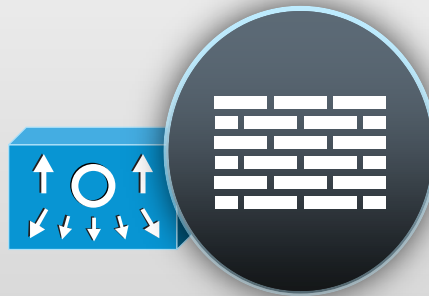
5585



ASA Services Module



Virtual Security Gateway

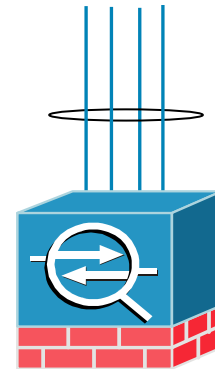


Data Center Firewall Design: ASA 5585 & 8.4(1)

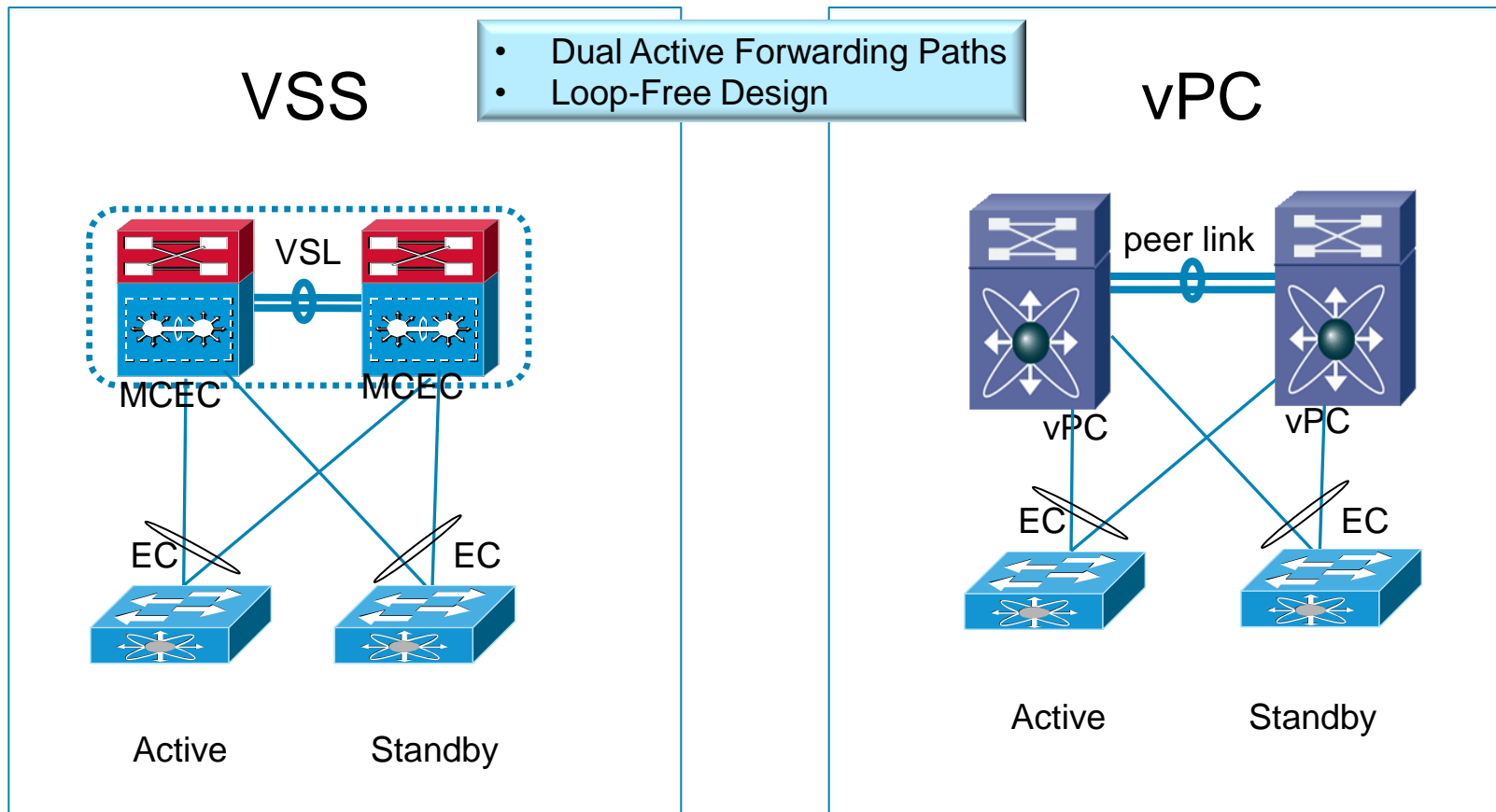
- **Performance**
 - 10 Million connections + ~375Kcps delivers more capacity in a single system
 - Numbers are NOT inflated – Customers will be able to easily replicate
- **EtherChannel connectivity to support vPC / Multi-chassis EtherChannel in Nexus 7K**
 - No need for STP
 - Creates Secure Active/Active 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)

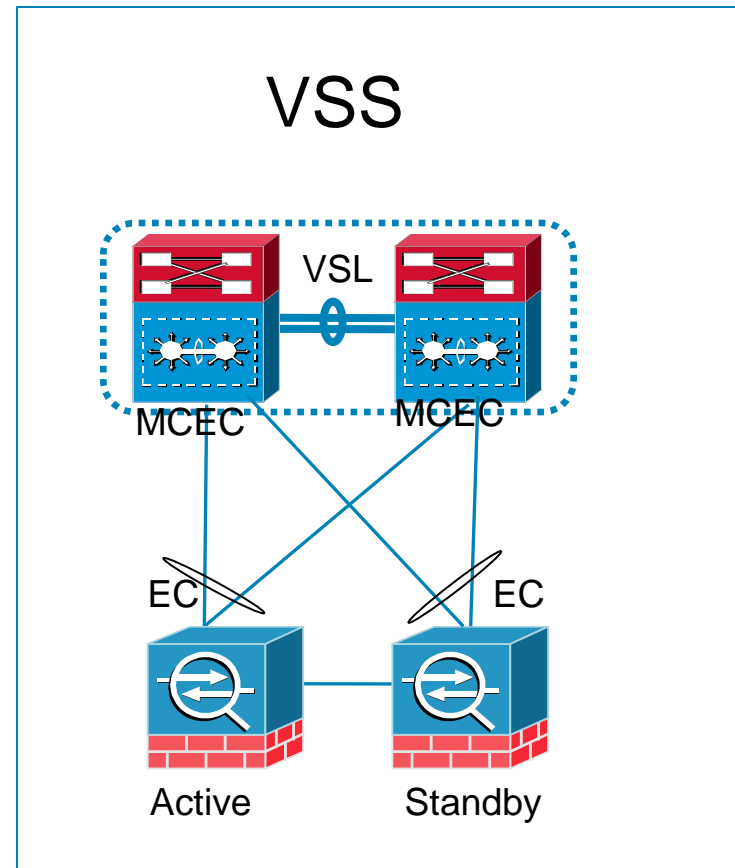
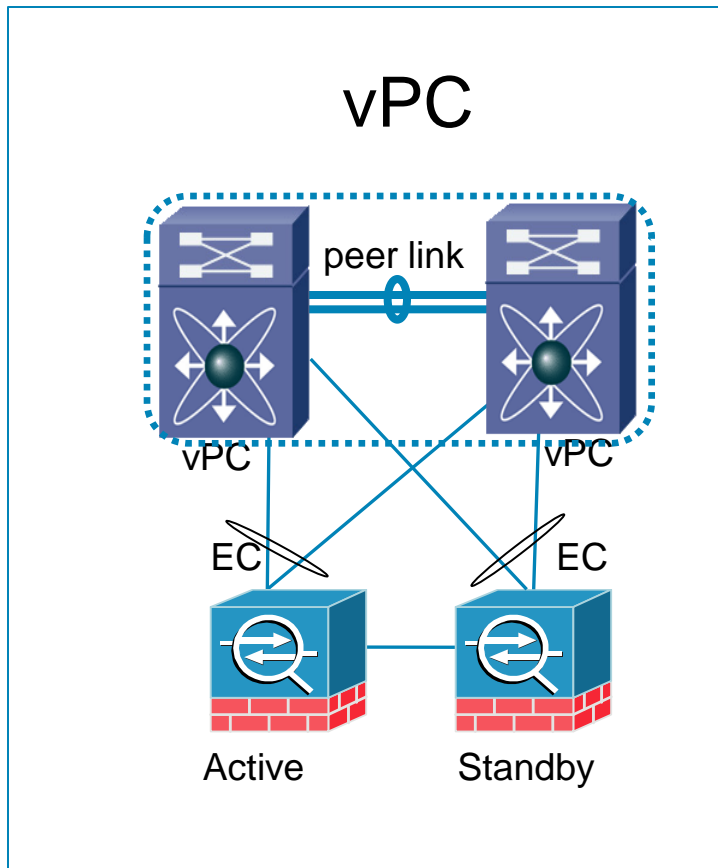
- ASA supports Link Aggregation Control Protocol (LACP), an IEEE 802.3ad standard
- Each port-channel supports up to 8 active and 8 standby links
- Supported methods of aggregation: Active, Passive & On
- EtherChannel ports are treated just like physical and logical interfaces on ASA
- ASA can tie-in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




Catalyst 6500 VSS and Nexus 7000 vPC



ASA Integration with vPC & VSS



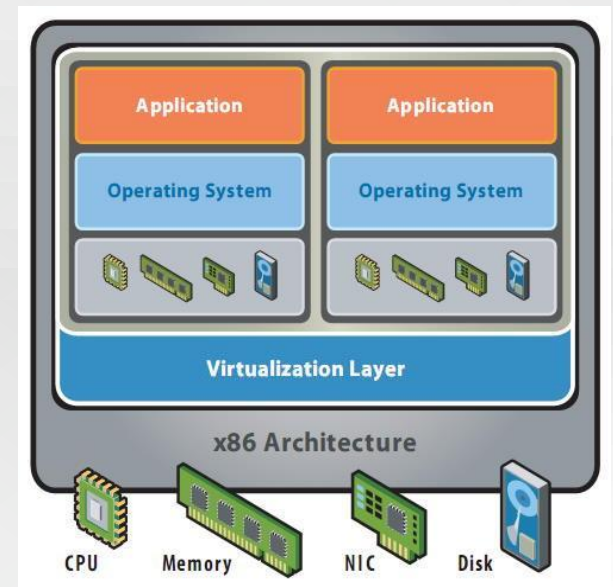
ASA 5585 Interface Options, Continued

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*	

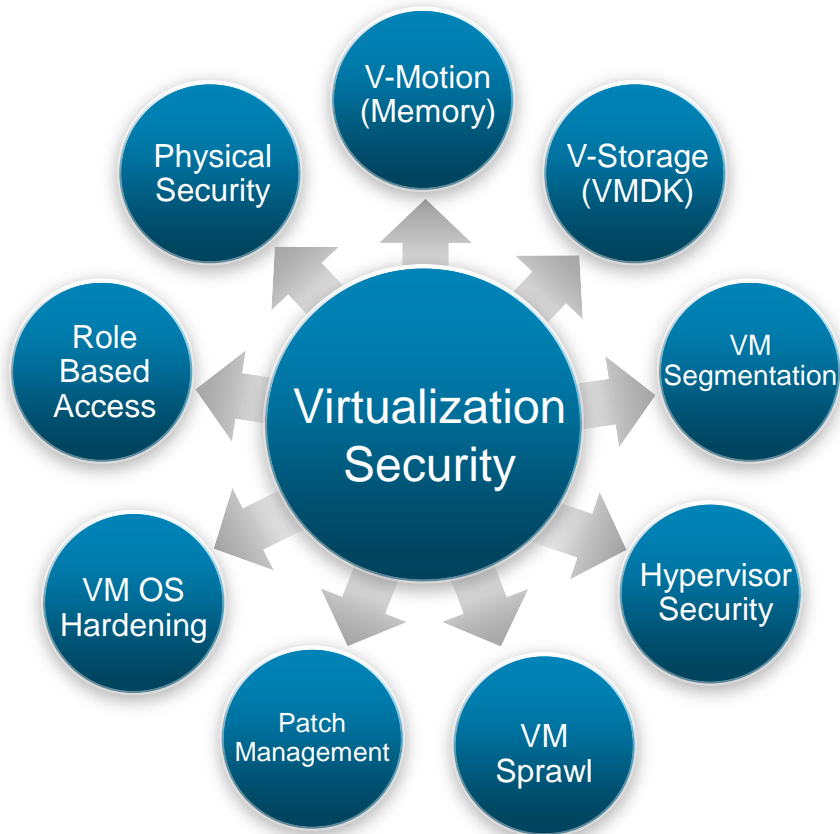
- GLC-T SFP should work but is not yet officially supported

* Minimum Software 8.2.5 or 8.4.1

Server Virtualization



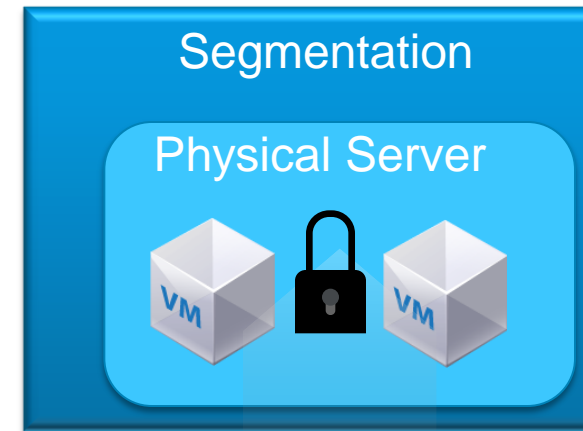
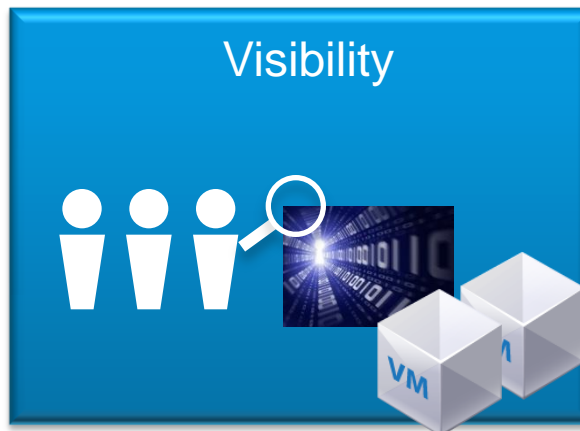
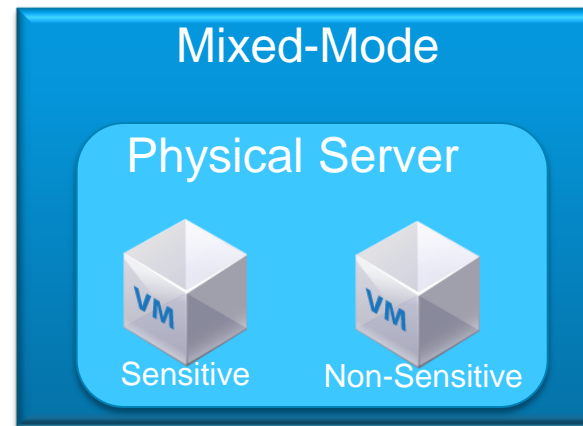
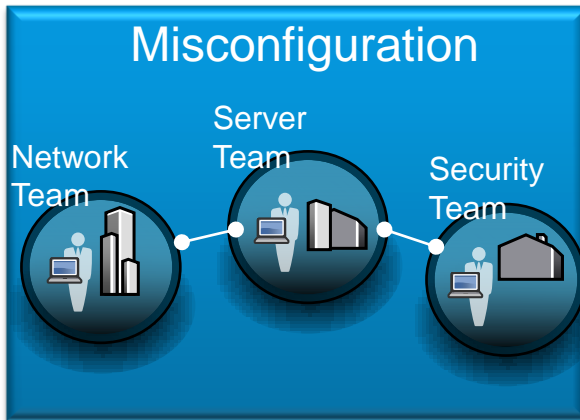
Security and Server Virtualization



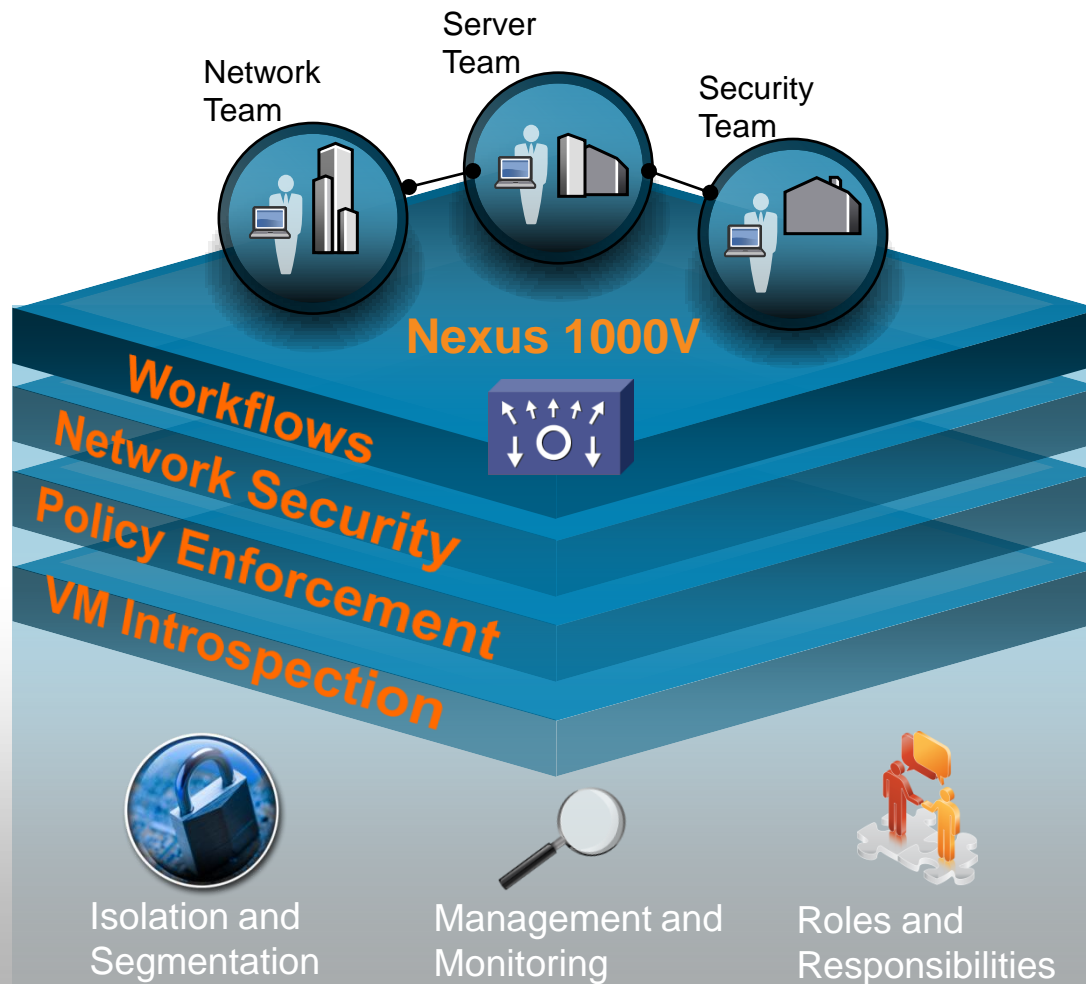
Virtualization a broad topic

Focus is areas where 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)

Server Team

Applications drive data center infrastructure and security requirements. Virtualization is expanding server capabilities



Security Team

Virtualization, cloud initiatives, and compliance are changing how security is implemented



Network Team

Network and server virtualization has changed how the data center is architected



Virtualization is driving changes - Collaboration is a must -
Simplicity is Key

Port Profiles

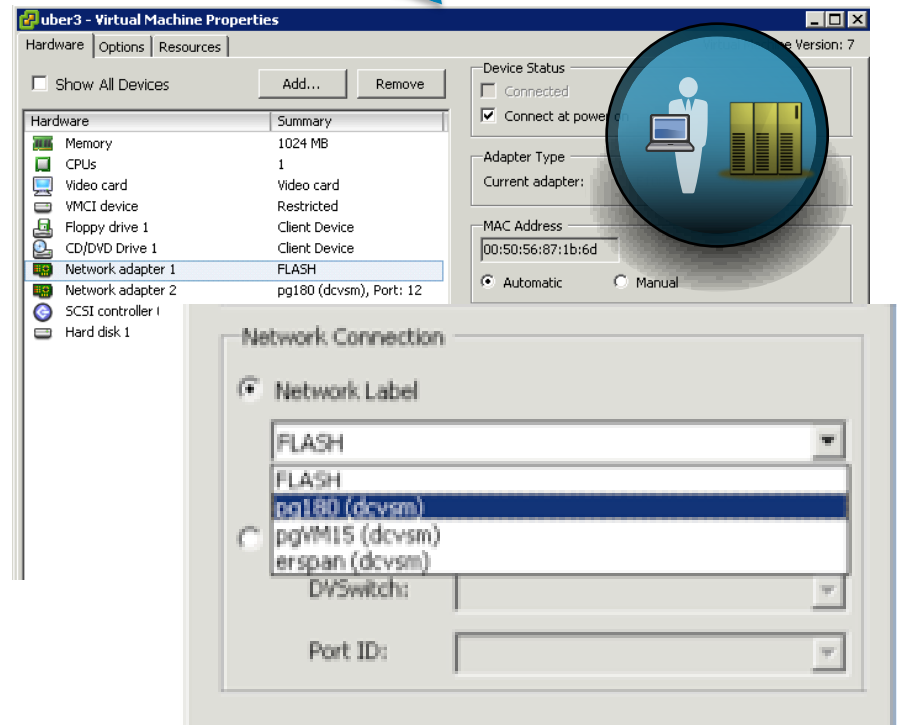
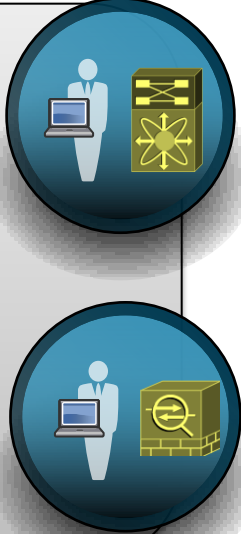
Port Profile → Port Group

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



uber3 - Virtual Machine Properties

Hardware | Options | Resources

Show All Devices Add... Remove

Hardware	Summary
Memory	1024 MB
CPUs	1
Video card	Video card
VMCI device	Restricted
Floppy drive 1	Client Device
CD/DVD Drive 1	Client Device
Network adapter 1	FLASH
Network adapter 2	pg180 (dcvsm), Port: 12
SCSI controller 1	
Hard disk 1	

Device Status
 Connected
 Connect at power

Adapter Type
Current adapter:

MAC Address
00:50:56:87:1b:6d
 Automatic Manual

Network Connection

Network Label

FLASH

FLASH

pg180 (dcvsm)

pg1M15 (dcvsm)

erspan (dcvsm)

DYSwitch: [Dropdown]

Port ID: [Dropdown]

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

The screenshot displays the Cisco Virtual Network Management Center (VMNC) interface. On the left, a navigation tree shows the hierarchy: Firewall Policy > Security Profile > root > Security Profiles > Contractor > Security Profiles. The 'SecureContractors' profile is highlighted in green. The main panel shows the 'Security Profiles' configuration page with the 'General' tab selected. A table lists the profile 'SecureContractors' with a yellow circle around its name. A green arrow points from this profile to a terminal window on the right.

The terminal window shows the following configuration commands:

```
org root/Contractor
vn-service ip-address 192.168.173.42 vlan 20 security-profile SecureContractor
s
no shutdown
state enabled

N11# sh run port-profile contractor

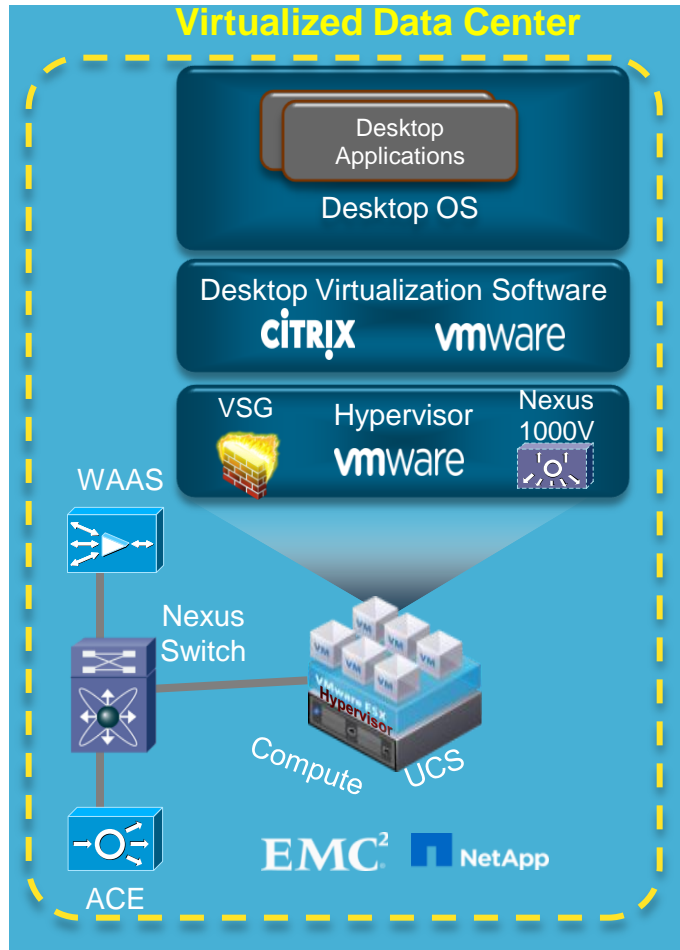
!Command: show running-config port-profile contractor
!Time: Thu Jan 6 19:24:38 2011

version 4.2(1)SV1(4)
port-profile type vethernet contractor
vmware port-group
switchport access vlan 10
switchport mode access
org root/Contractor
vn-service ip-address 192.168.173.42 vlan 20 security-profile SecureContractors
no shutdown
state enabled

N11#
```

The terminal output shows the configuration for the 'contractor' port-profile, which is linked to the 'SecureContractors' security profile. A yellow circle highlights 'SecureContractors' in the terminal output, and a green arrow points from the 'SecureContractors' entry in the VMNC table to this circle.

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

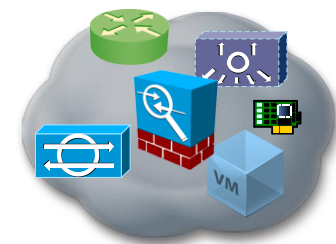
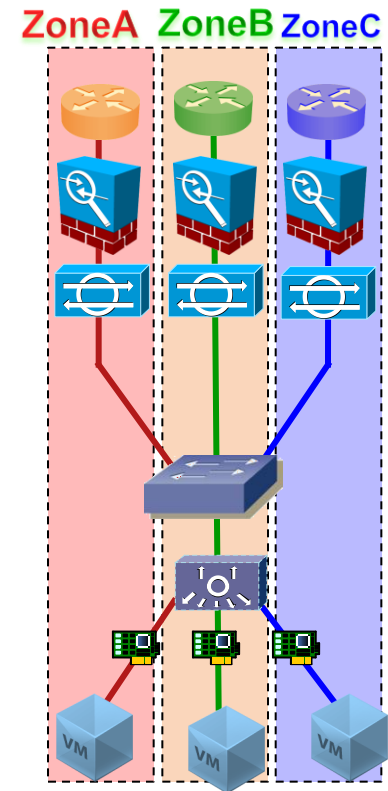
Cisco solution = VXi: Virtualization Experience Infrastructure:

Design Fundamentals



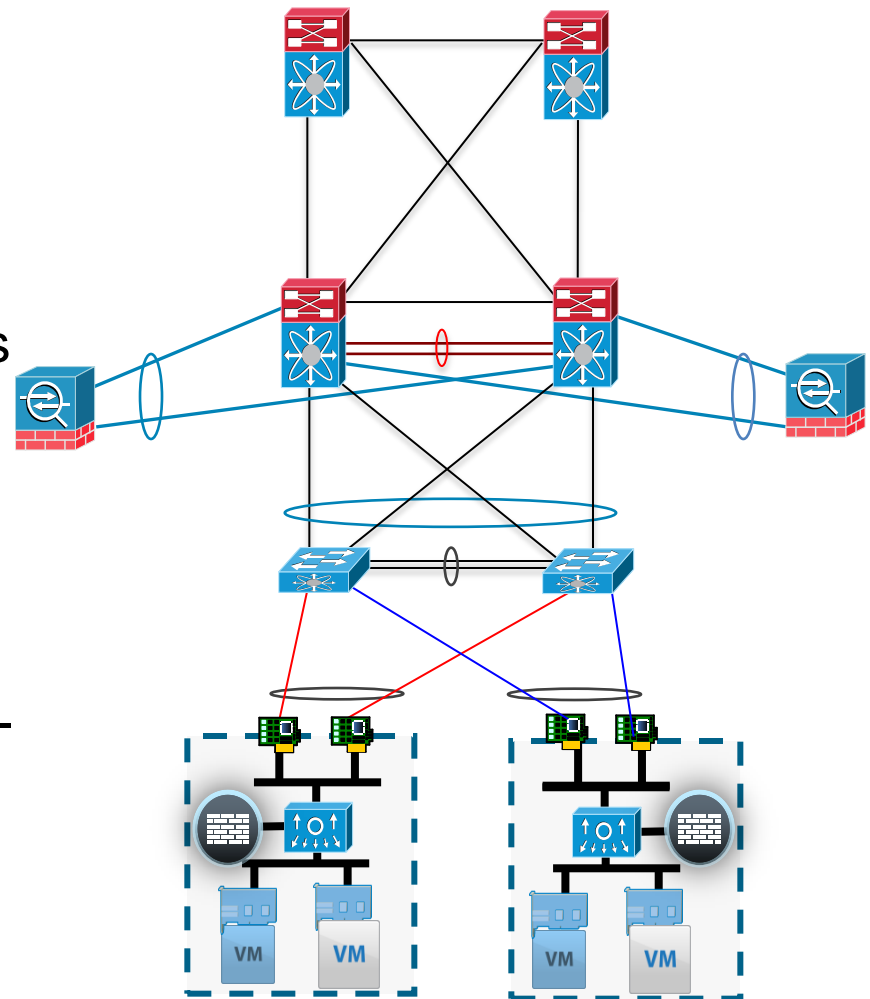
Secure Data Center

- 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



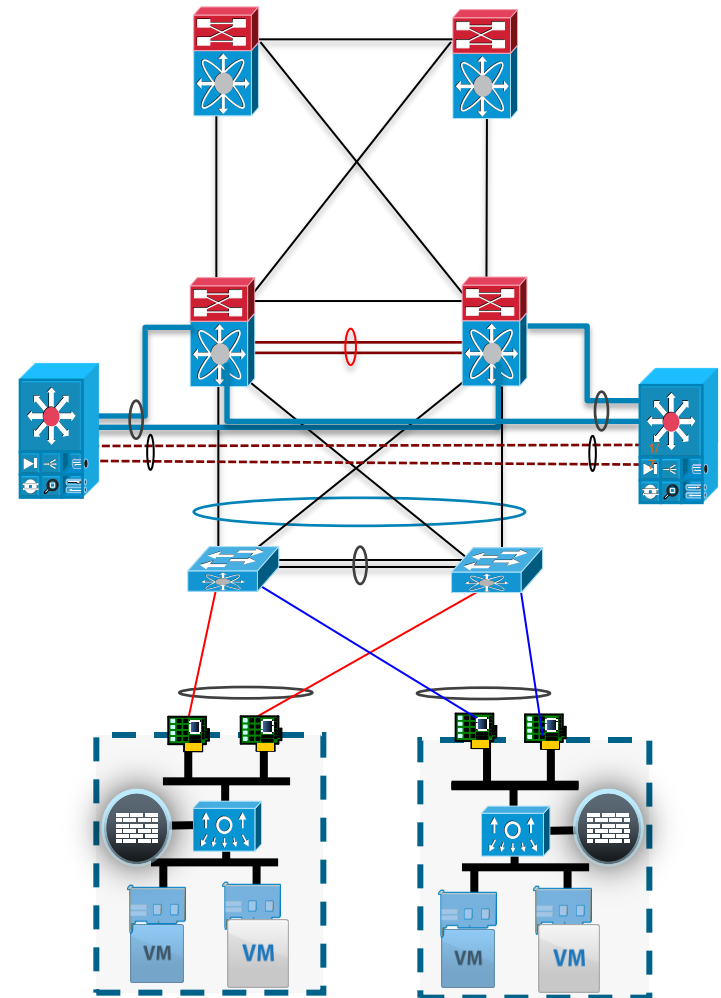
Traditional Model

- 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



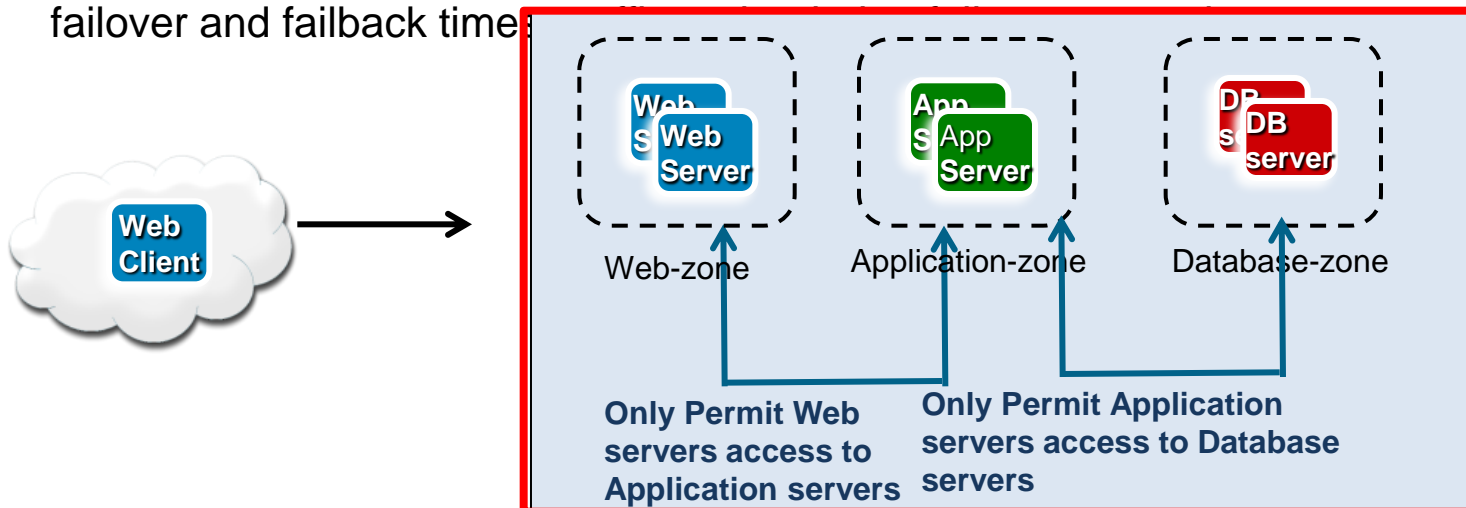
Secure Service Pod Model

- 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

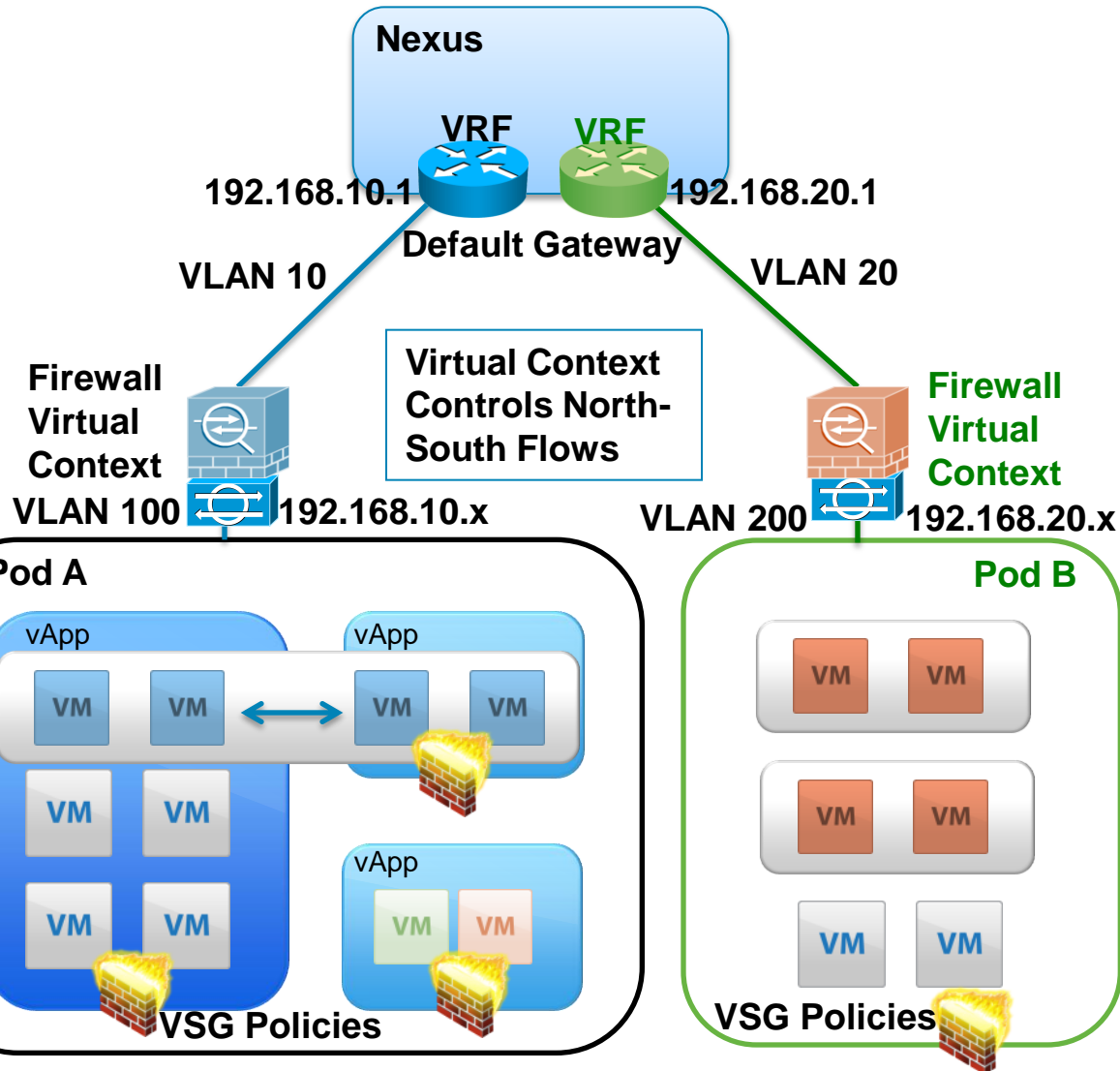
- Understand how the applications are deployed and accessed both internally and externally
- Understand the North-South, East-West flow patterns
- Remember careful attention should be given to where the server's default gateway resides
- Adjacency of services to servers is important. Adding services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



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



VSG provides attribute-based control and enforcement for East-West flows

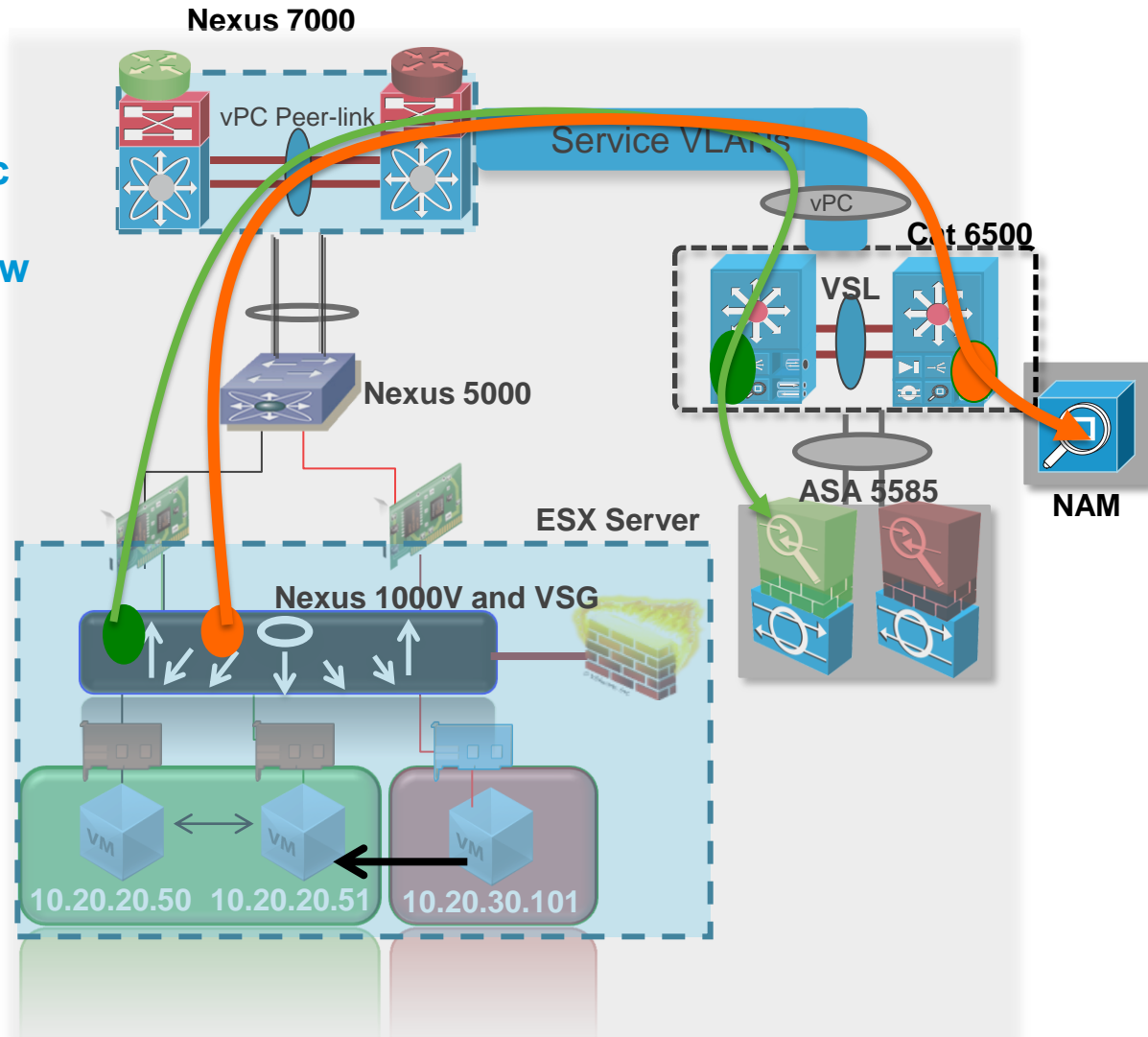
Monitoring Virtual Machine Flows

The Nexus 1000V & ERSPAN

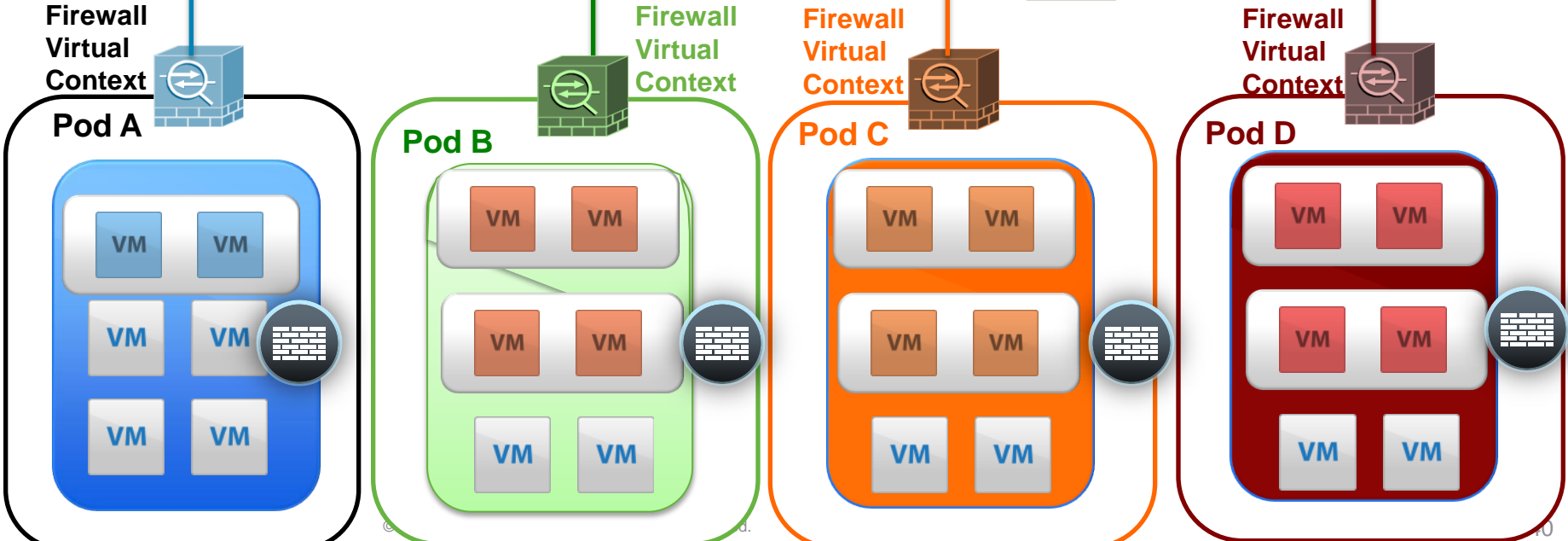
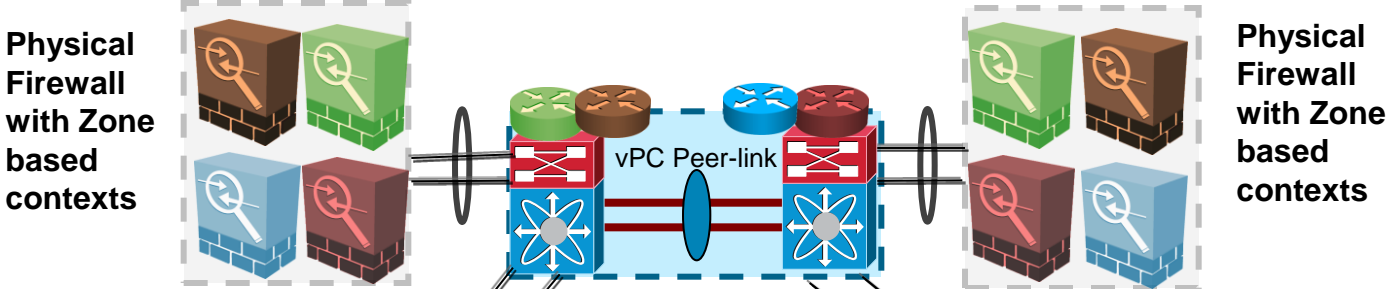
- Visibility of vm-to-vm traffic
- Use existing IDS/IPS
- Use NAM to analyze NetFlow

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



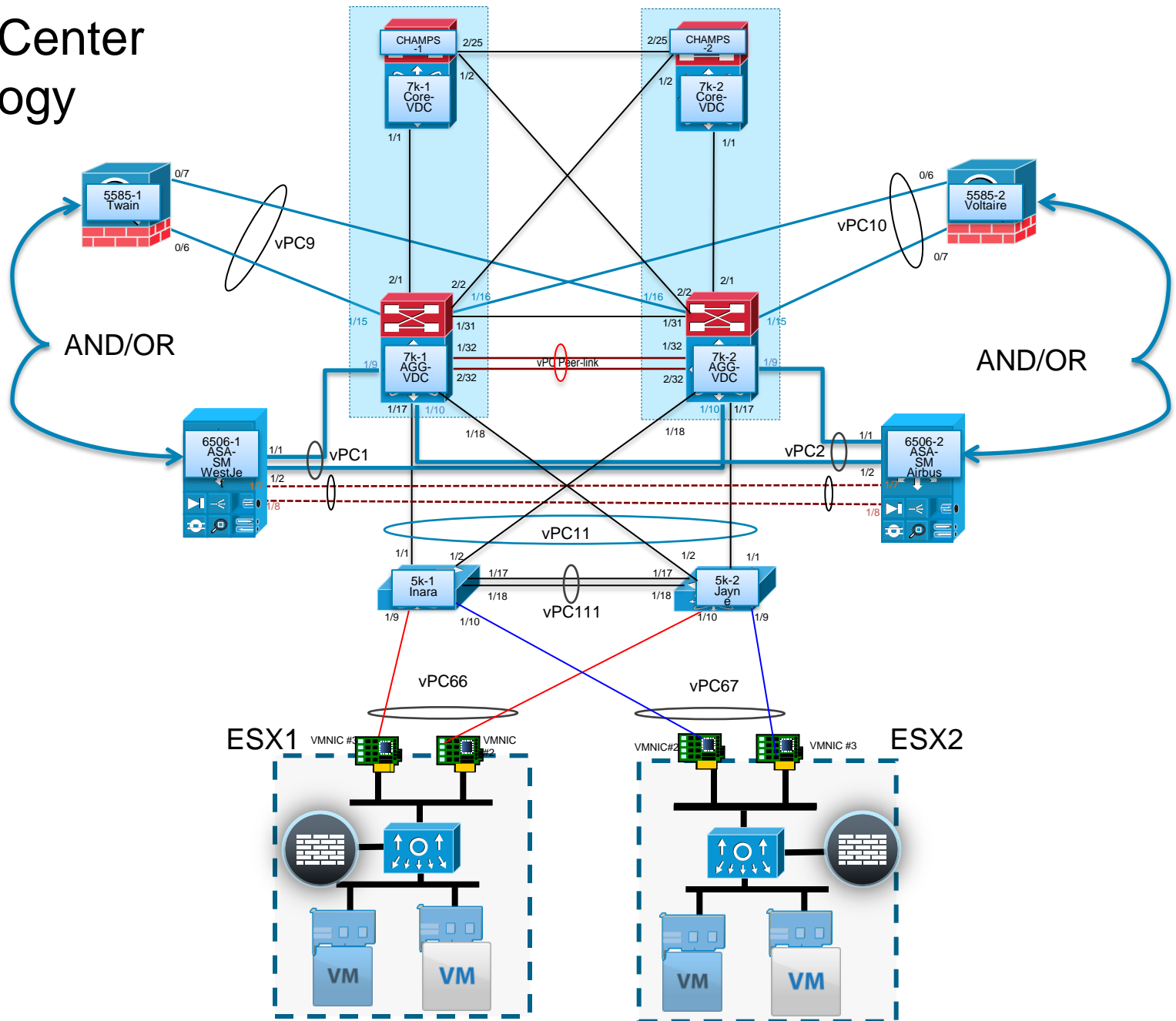
Design Details



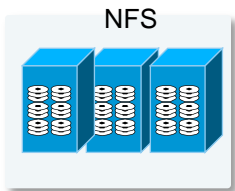
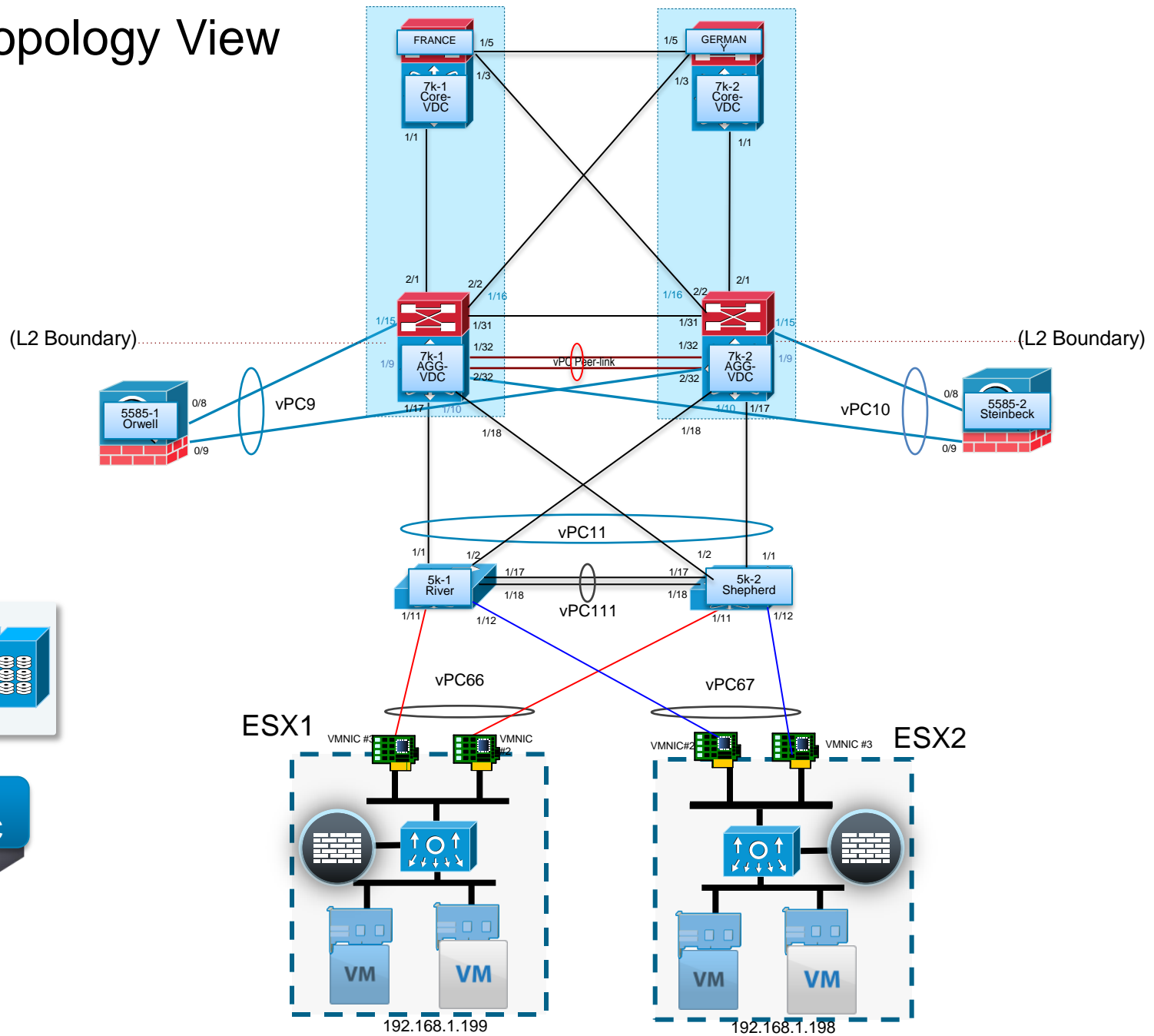
Secure Data Center Test Architecture

- 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



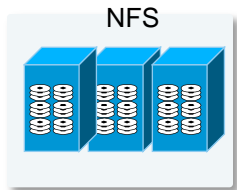
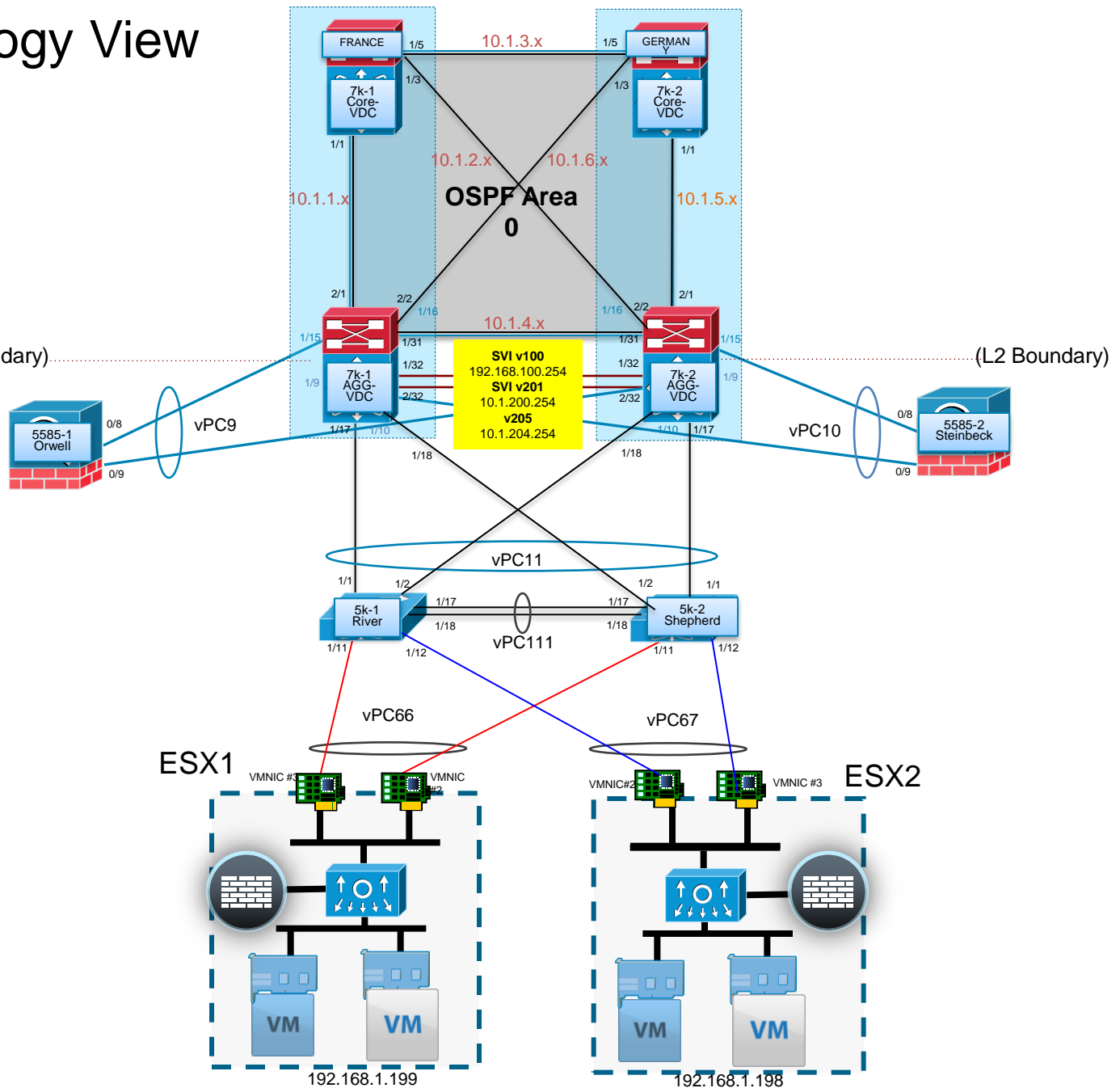
L3 Topology View

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

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

(L2 Boundary)

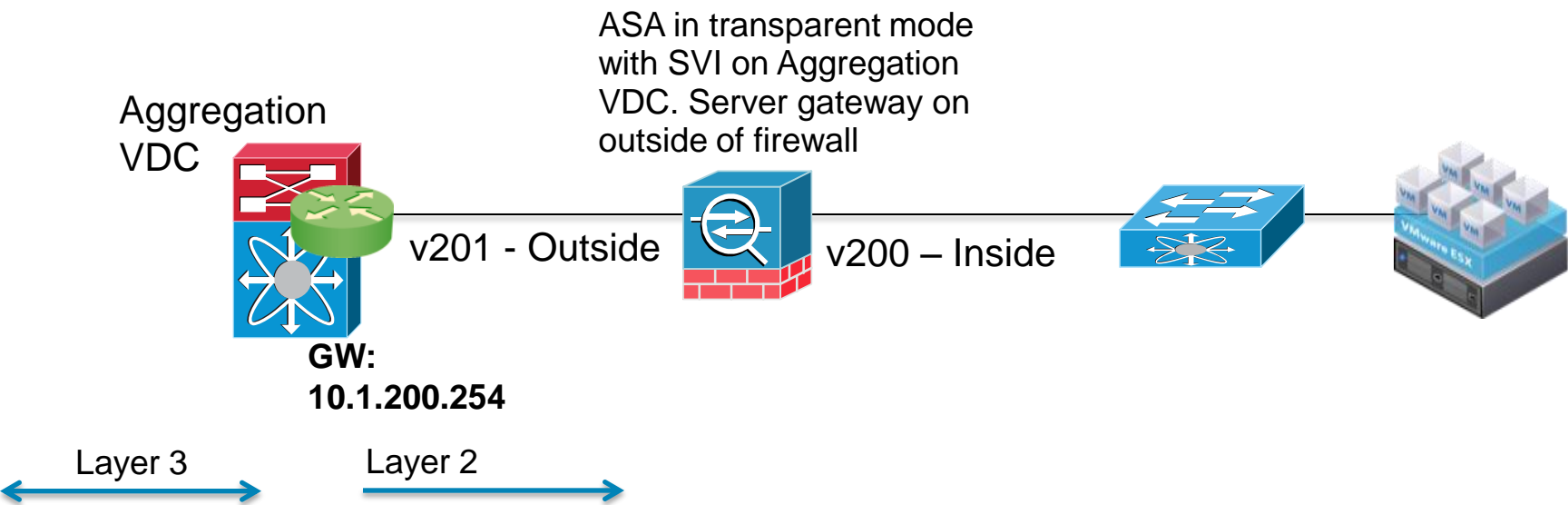
(L2 Boundary)



Design Details and Benefits

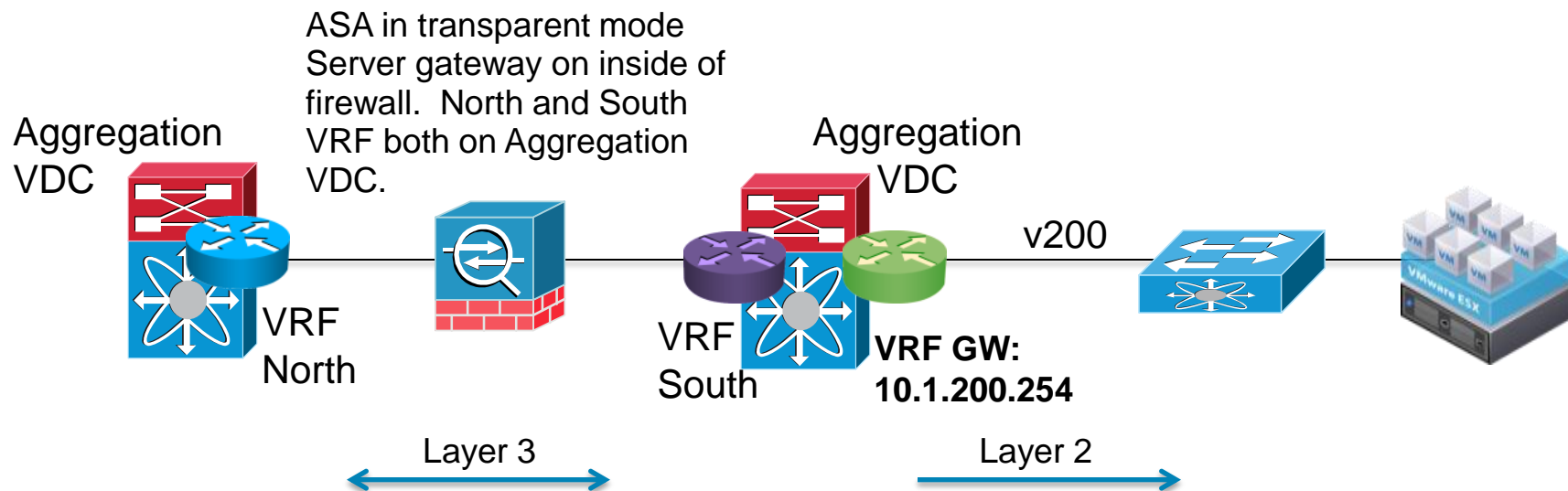
- Virtual Device Contexts (VDC) used to create virtual core and aggregation layer
- vPC used to create loop-free design
- Each ASA firewall is connected to aggregation switch over a dedicated vPC domain
- Each firewall is deployed in transparent mode. Offers easiest integration with existing addressing 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

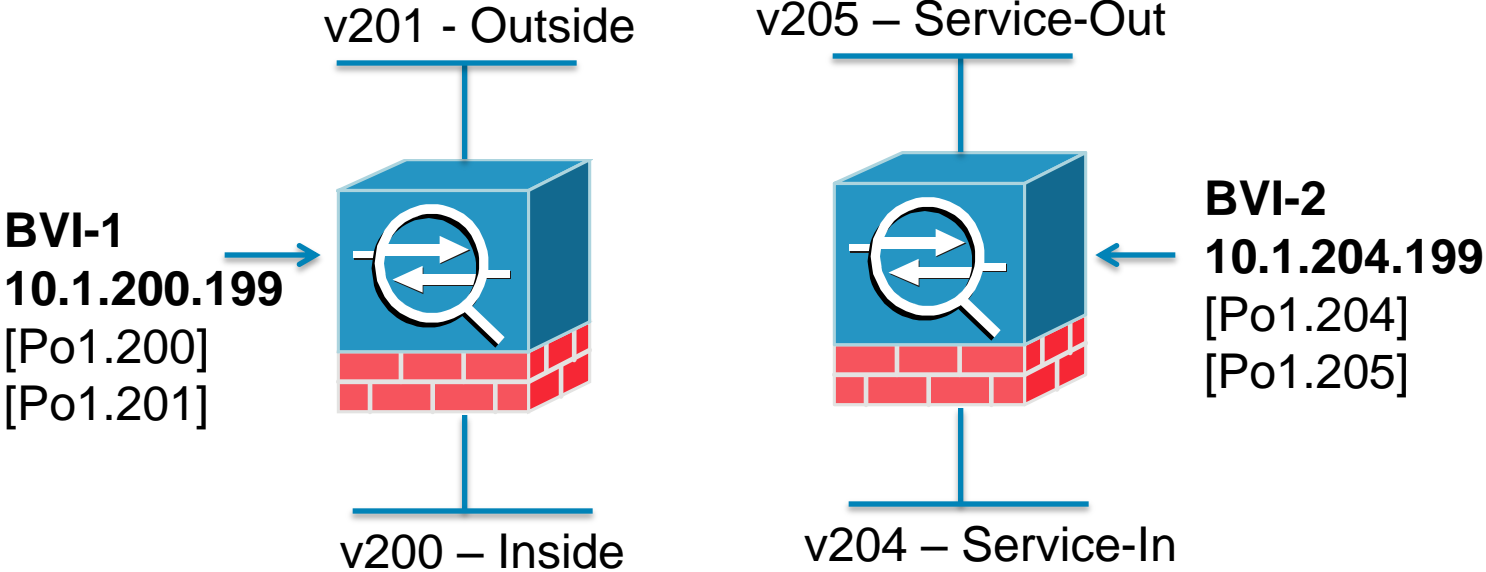


A little more complex design. Gateway on inside of firewall means smaller failure domain.

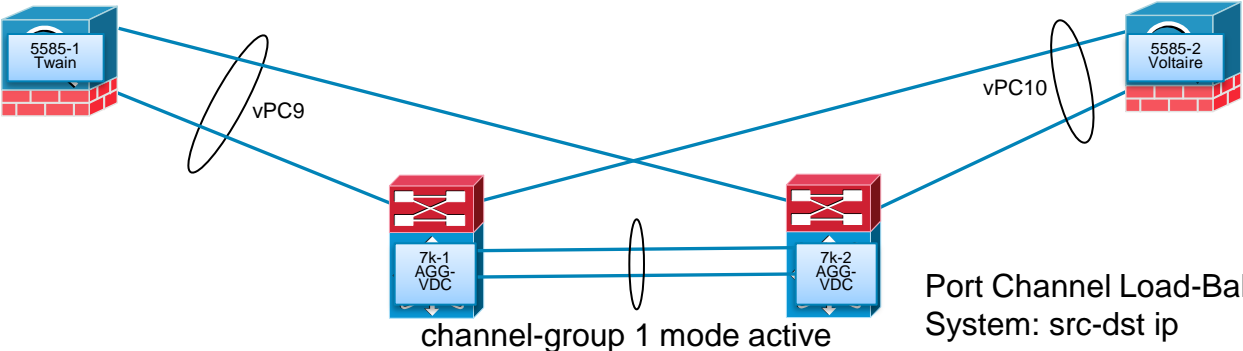
Design Details and Benefits

- 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



channel-group 1 mode passive



Port Channel Load-Balancing Configuration:
System: src-dst ip

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

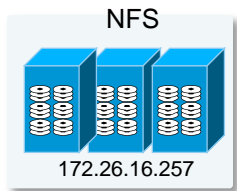
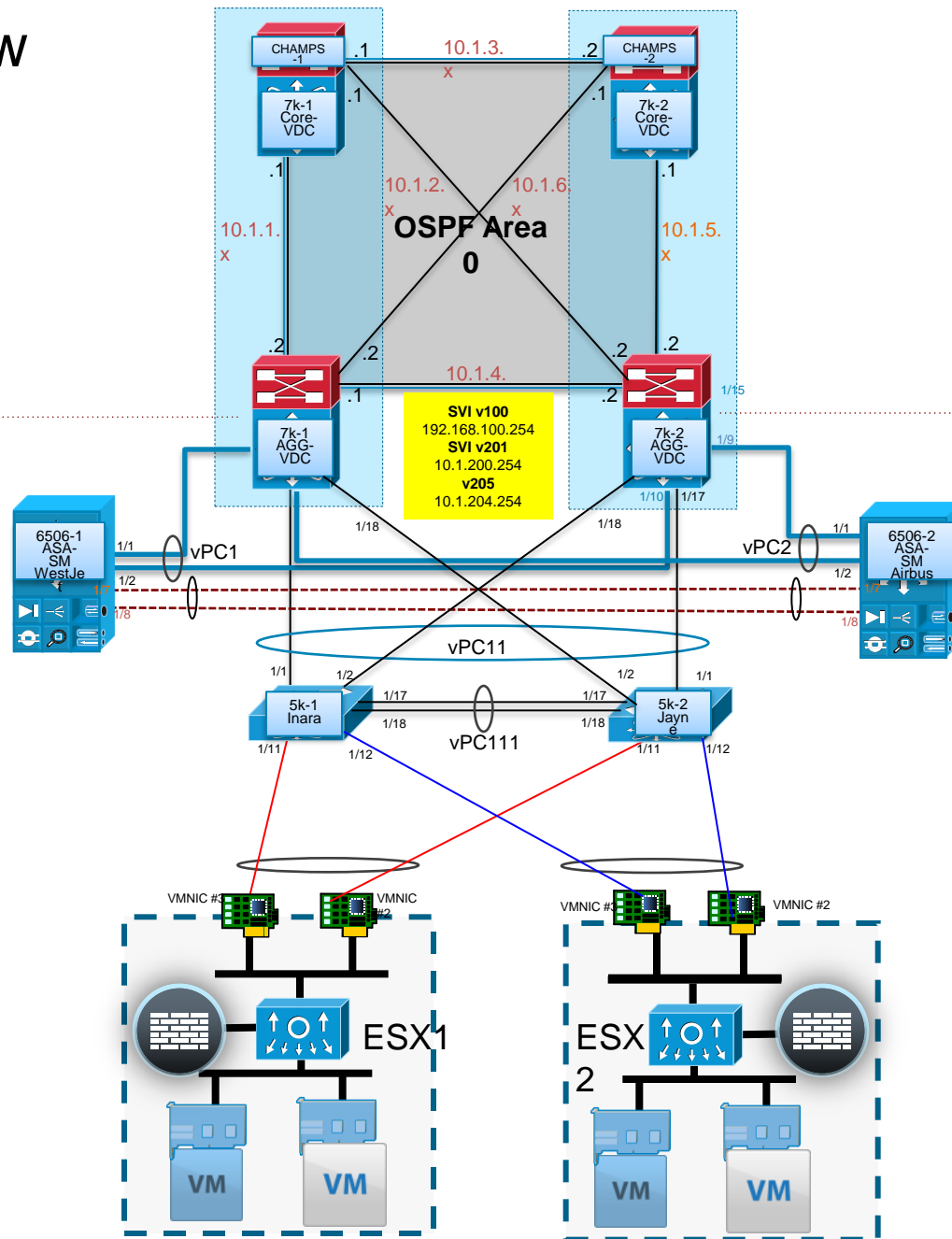
```
champs1-agg-vdc# sh int | i b414.89e1.a043
Hardware: 10000 Ethernet, address: b414.89e1.a043 (bia f866.f23e.0f86)
Hardware: 10000 Ethernet, address: b414.89e1.a043 (bia f866.f23e.0f87)
Hardware: 10000 Ethernet, address: b414.89e1.a043 (bia f866.f23e.0f88)
Hardware is EtherSVI, address is b414.89e1.a043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

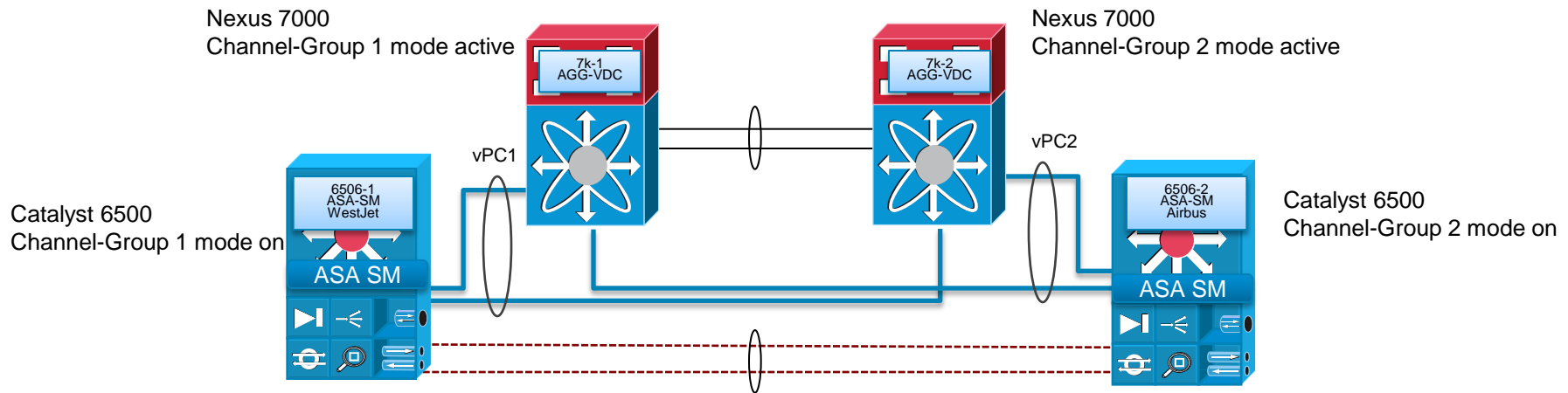
```
champs1-agg-vdc(config)# int vlan 100
champs1-agg-vdc(config-if)# mac-address b414.89e1.1111
champs1-agg-vdc(config-if)# int vlan 201
champs1-agg-vdc(config-if)# mac-address b414.89e1.2111
champs1-agg-vdc(config-if)# int vlan 205
champs1-agg-vdc(config-if)# mac-address b414.89e1.3111
```

Topology View with ASA SM

(L2 Boundary) (L2 Boundary)



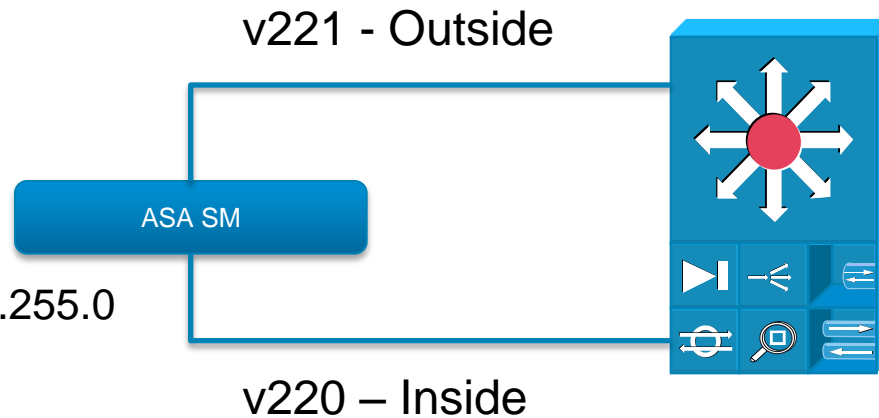
Nexus 7000 & Cat 6500 Channel Group Modes



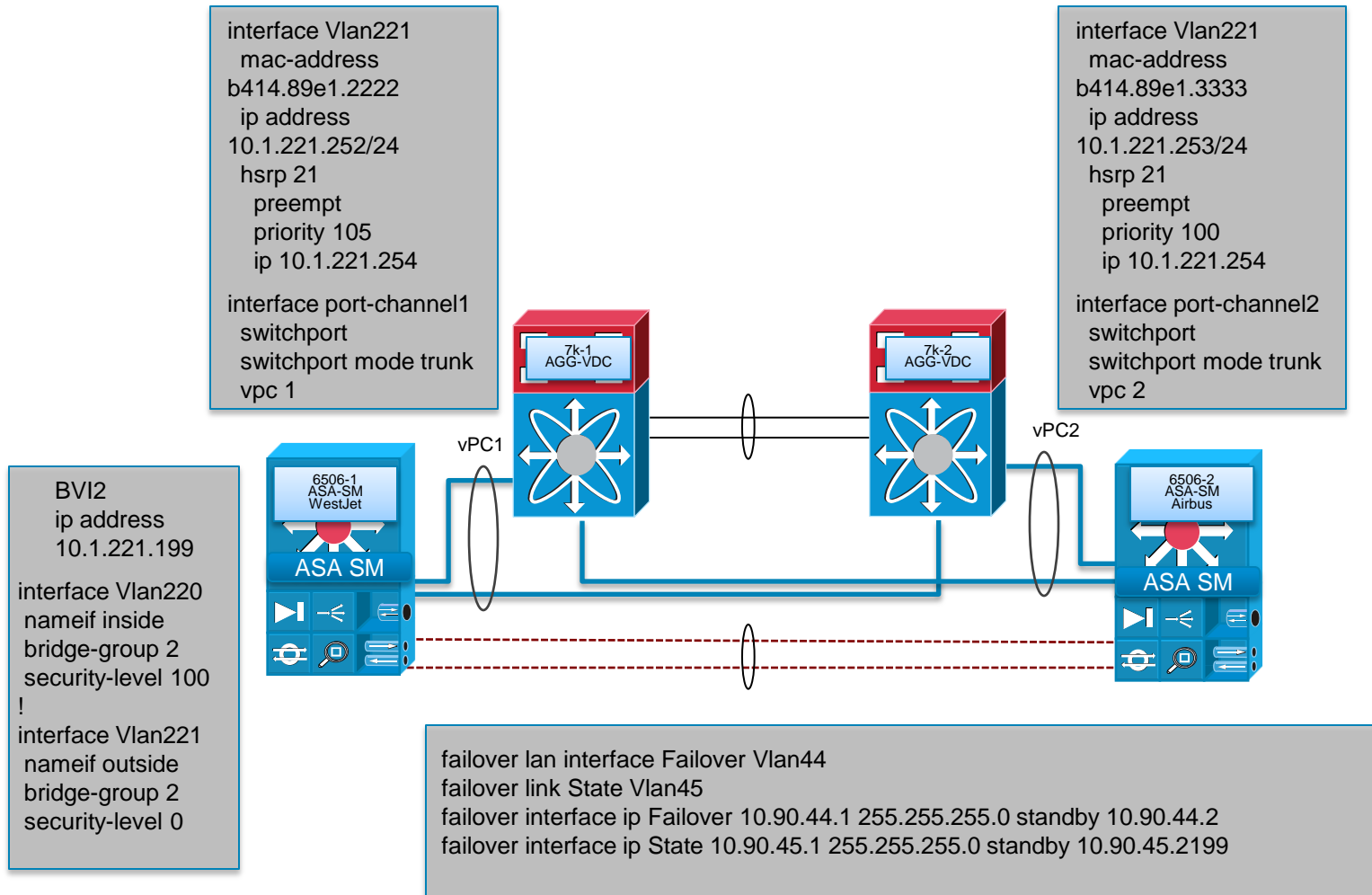
ASA SM Layer 2 and 3

interface BVI2

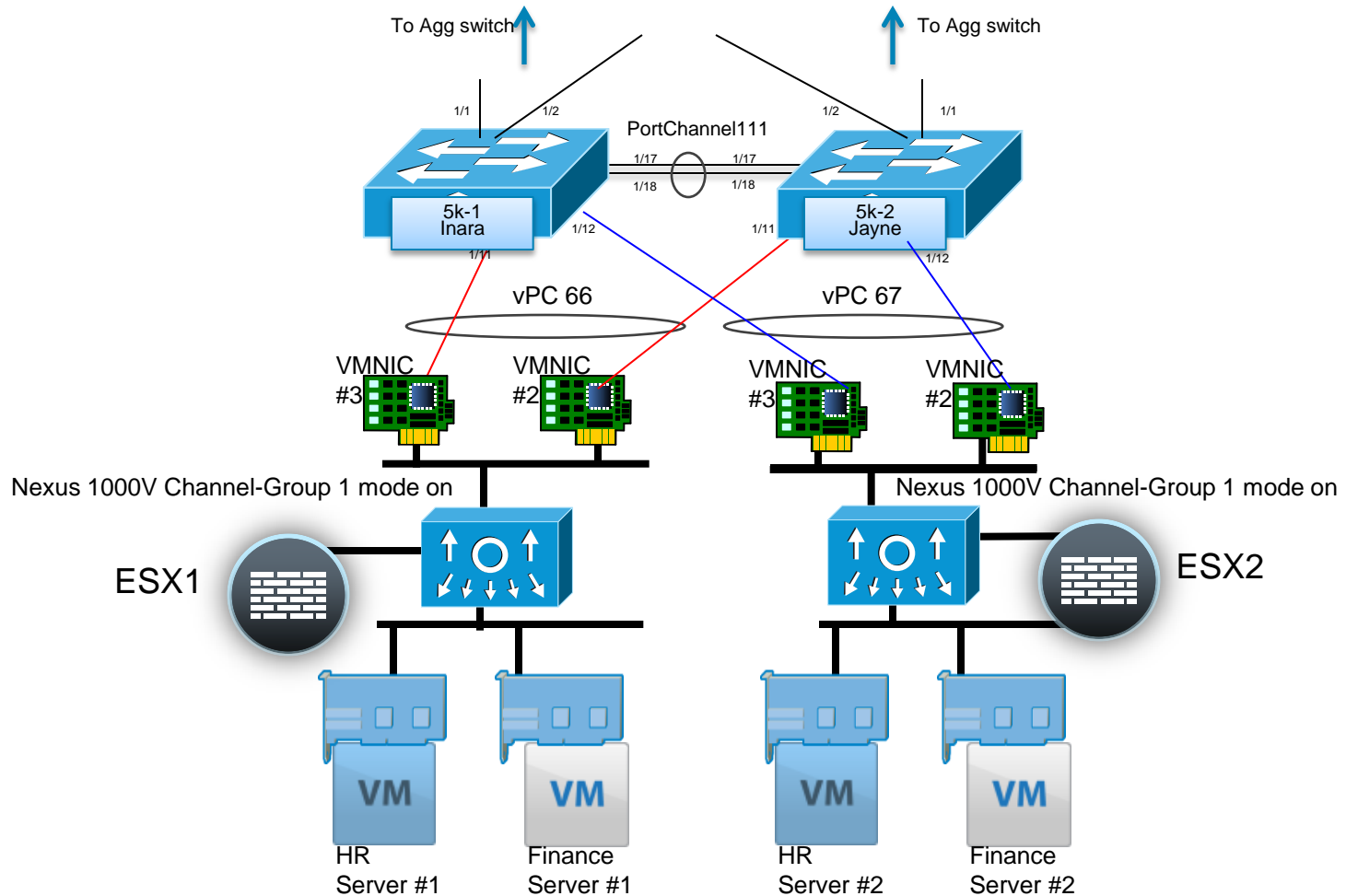
```
description bvi for 221 and 220  
ip address 10.1.221.199 255.255.255.0
```



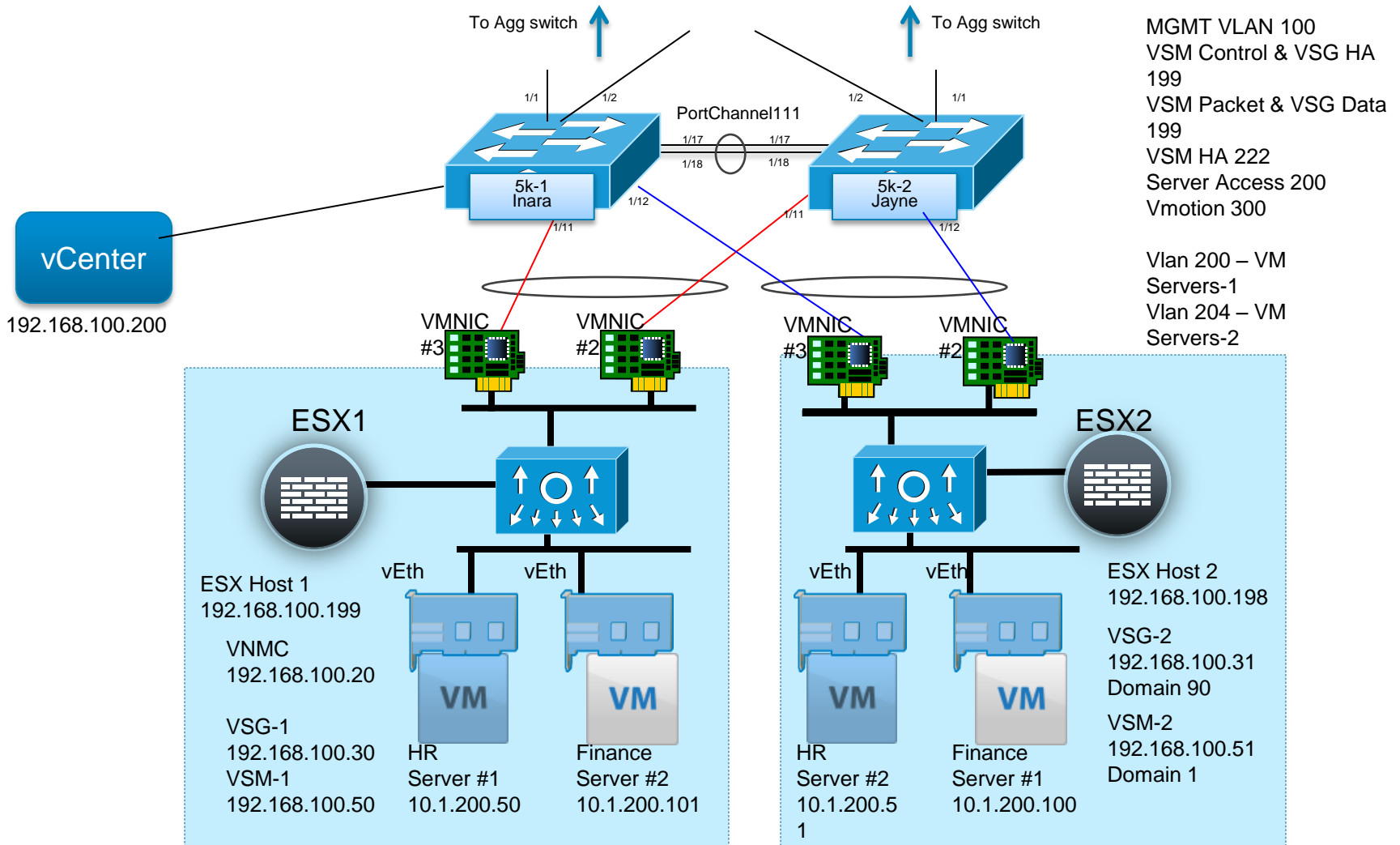
ASA SM Details



Server Access and VM Environment



Server Access and VM Network Details



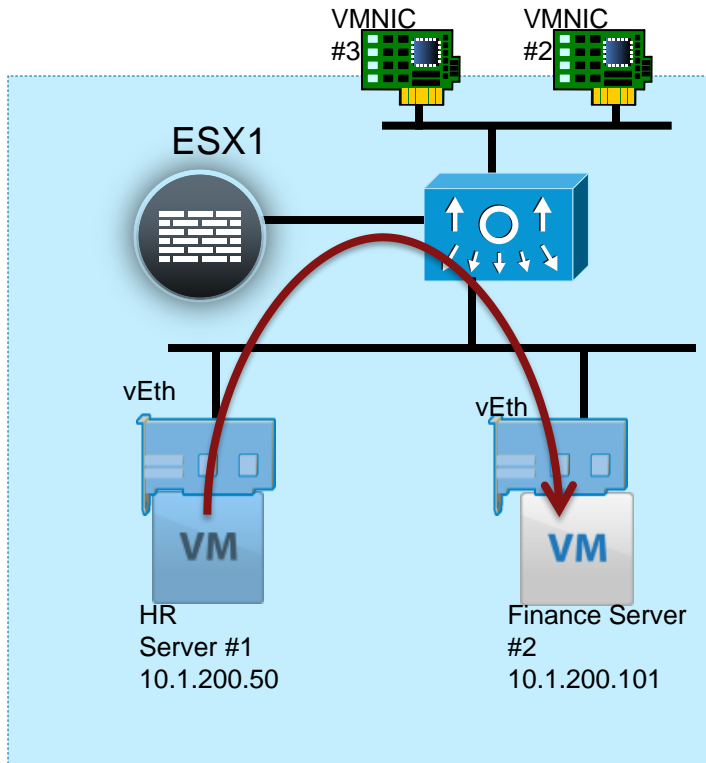
Deny HR to Finance

ESX Host 1
192.168.100.199

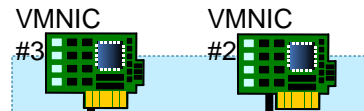
VNMC
192.168.100.20

VSG-1
192.168.100.30

VSM-1
192.168.100.50

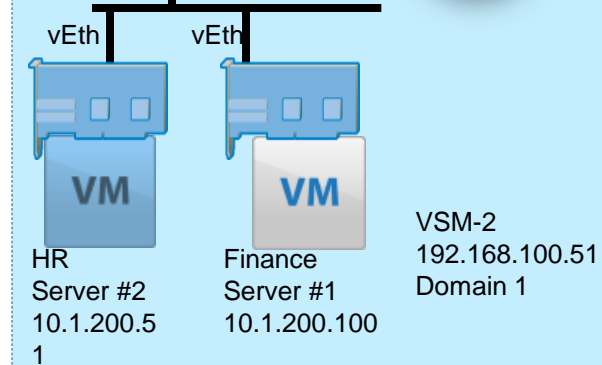


ESX Host 2
192.168.100.198



ESX2

VSG-2
192.168.100.31
Domain 90



Policy Heirarchy

The screenshot displays the Cisco Virtual Network Management Center interface. At the top, the Cisco logo and "Virtual Network Management Center" are visible, along with user information: "(admin) Log Out About Help". The main navigation bar includes "Tenant Management", "Resource Management", "Policy Management" (highlighted), and "Administration". Below this, a sub-menu shows "Security Policies" (highlighted), "Device Policies", "Capabilities", and "Diagnostics".

The left pane shows a tree view of the "Firewall Policy" hierarchy. The tree is expanded to show the "CPOC" folder, which contains "Object Groups", "Policies", "Policy Sets", "Zones", and "CPOC". Under "CPOC", there are sub-folders for "Object Groups", "Policies", "Policy Sets", "Zones", and "CPOC". The "Zones" folder is expanded, showing "Finance" and "HR" (highlighted).

The right pane shows the configuration for the "HR" zone. The breadcrumb path is "root > CPOC > Zones > HR". The configuration is divided into three tabs: "General" (selected), "Conditions", and "Events". The "General" tab contains two text input fields: "Name" with the value "HR" and "Description" with the value "HR Zone". At the bottom right of the configuration area are "Save" and "Reset" buttons.

At the bottom left of the interface, there are two expandable sections: "Security Profile" and "Security Profile Dictionary".

© 2010 Cisco Systems, Inc. All rights reserved.

VNMC: Deny Interzone Policy

Virtual Network Management Center

(admin) Log Out About Help

Tenant Management | Resource Management | **Policy Management** | Administration

Security Policies | Device Policies | Capabilities | Diagnostics

Firewall Policy

- root
 - Object Groups
 - Policies**
 - Policy Sets
 - Zones
 - CPOC
 - Object Groups
 - Policies**
 - Deny_Interzone_traffic**
 - Policy Sets
 - Zones
 - Finance
 - HR

Security Profile

Security Profile Dictionary

root > CPOC > Policies > Deny_Interzone_traffic

Deny_Interzone_traffic

General | **Rules** | Events

+ Add Rule ↑ Up ↓ Down

Name	Source Condition	Destination Condition	Protocol	Ethertype	Action
Permit_Finance	Zone Name eq Finance	Zone Name eq Finance	Any	Any	Permit
Permit_HR	Zone Name eq HR	Zone Name eq HR	Any	Any	Permit
Deny_HR_to_Fi	Zone Name eq HR	Zone Name eq Finance	Any	Any	Drop, Log
Deny_Finance_	Zone Name eq Finance	Zone Name eq HR	Any	Any	Drop, Log
Permit_All	Any	Any	Any	Any	Permit

Save Reset

© 2010 Cisco Systems, Inc. All rights reserved.

VNMC Policy: Deny HR to Finance Requests

The screenshot displays the Cisco Virtual Network Management Center (VNMC) interface. The main navigation bar includes "Tenant Management", "Resource Management", "Policy Management" (highlighted), and "Administration". The left sidebar shows a tree view of the configuration hierarchy, with "Deny_Interzone_traffic" selected under "CPOC".

The central window is titled "Deny_Interzone_traffic" and shows the "Edit Rule" dialog for "Deny_HR_to_Finance". The dialog has three tabs: "General", "Source and Destination Condition", and "Events". The "General" tab is active, showing the following configuration:

- Name: Deny_HR_to_Finance
- Description: (empty)
- Action to take: drop permit
- log:
- Protocol: Any
- Ether Type: Any

An orange box highlights the "Action to take" section, and an orange arrow points to the "drop" radio button. To the right of the dialog, a table shows the "Action" column with the following entries:

Action
Permit
Permit
Drop, Log
Drop, Log
Permit

At the bottom of the dialog are "OK" and "Cancel" buttons. At the bottom of the main window are "Save" and "Reset" buttons.

© 2010 Cisco Systems, Inc. All rights reserved.

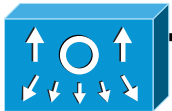
Policy Summary on VSG

```
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

The screenshot displays the vSphere Client interface. On the left, the inventory tree shows a host named '192.168.100.199' with several virtual machines, including 'HR-Server'. The main console window shows the 'HR-Server' console, which is running Windows Server 2008 R2 Standard. A yellow notification bar at the top of the console states: 'Number of active connections has changed. There are now 3 active connections to this console'. Below this, the console displays a 'Remote Desktop Connection' dialog box. The dialog box is titled 'Remote Desktop Connection' and shows the following fields: 'Computer:' with the value '10.1.200.101', and 'User name:' with the value 'None specified'. Below these fields, it says 'You will be asked for credentials when you connect.' and has 'Options', 'Connect', and 'Help' buttons. A second, smaller dialog box is overlaid on top of the first, titled 'Remote Desktop Connection' with a red 'X' icon. It contains the following text: 'Remote Desktop can't connect to the remote computer for one of these reasons: 1) Remote access to the server is not enabled 2) The remote computer is turned off 3) The remote computer is not available on the network. Make sure the remote computer is turned on and connected to the network, and that remote access is enabled.'

Syslog from VSG

splunk Search Logged in as admin | App | Manager | Alerts | Jobs | Logout

Summary Search Status Views Searches & Reports Help | About

Search | Actions

host="192.168.100.35" All time >

2,939 matching events Create alert Add to dashboard Save search Build report

Timeline: zoom in zoom out select all Scale: linear log 1 bar = 1 hour

250 12:00 PM Tue May 24 2011 12:00 AM Wed May 25 12:00 PM Thu May 26 250

31 fields | [Pick fields](#) Field discovery On Results per page 10

Selected fields (3)
host (1)
source (1)
sourcetype (1)

Other interesting fields (20)

1 event at 2 PM on Tuesday, May 24, 2011 Options...

```
1 5/24/11 2:55:40.000 PM May 24 14:55:40 192.168.100.35 : 2011 May 24 11:41:01 PDT: %POLICY_ENGINE-6-POLICY_LOOKUP_EVENT: policy=Deny_Interzone_PolicySet@root/CPOC rule=Deny_Interzone_traffic/Deny_Finance_to_HR@root/CPOC action=Drop direction=ingress src.net.ip-address=10.1.200.100 src.net.port=49159 dst.net.ip-address=10.1.200.50 dst.net.port=3389 net.protocol=6 net.ethertype=800 dst.zone.name=HR@root/CPOC src.zone.name=Finance@root/CPOC host=192.168.100.35 VSG | sourcetype=syslog | source=udp:514
```



Learn. Connect.
Collaborate. *together.*

Driving Simplicity: Data Center Design – Resources from Cisco

Validated Design Guides

A Cisco Competitive Differentiator

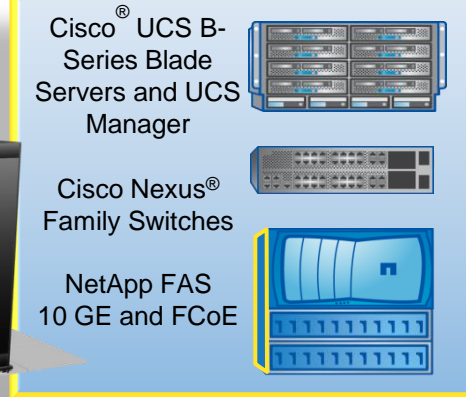
- Cisco Validated Designs are recommended, validated, end-to-end designs for next-generation networks.
- The validated designs are **tested** and fully **documented** to help ensure **faster**, more **reliable**, and more **predictable** customer deployments.
- 3 types of guides
 - Design Guides – comprehensive 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

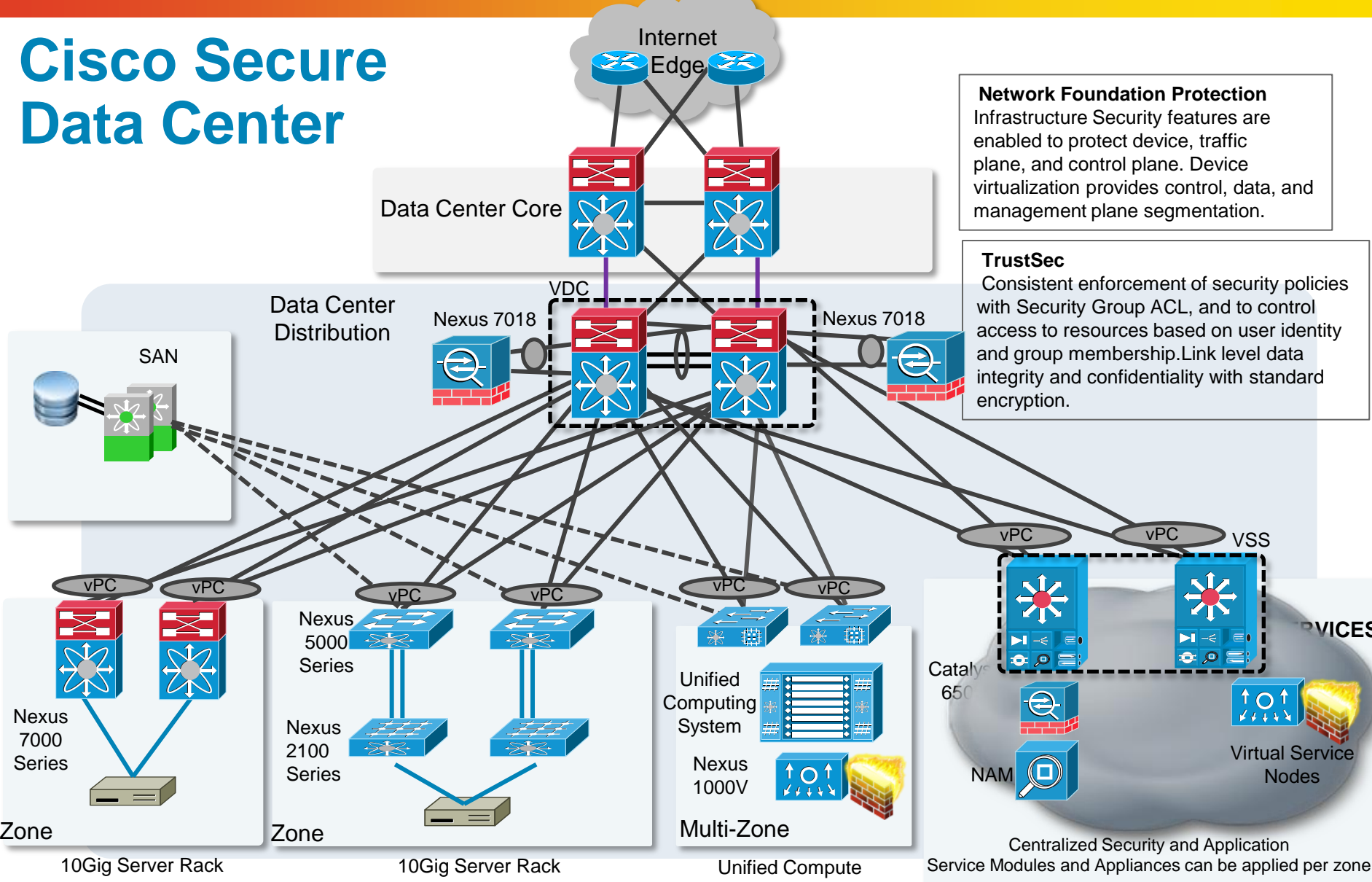


FlexPod



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.

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



