

Security and Virtualization in the Data Center

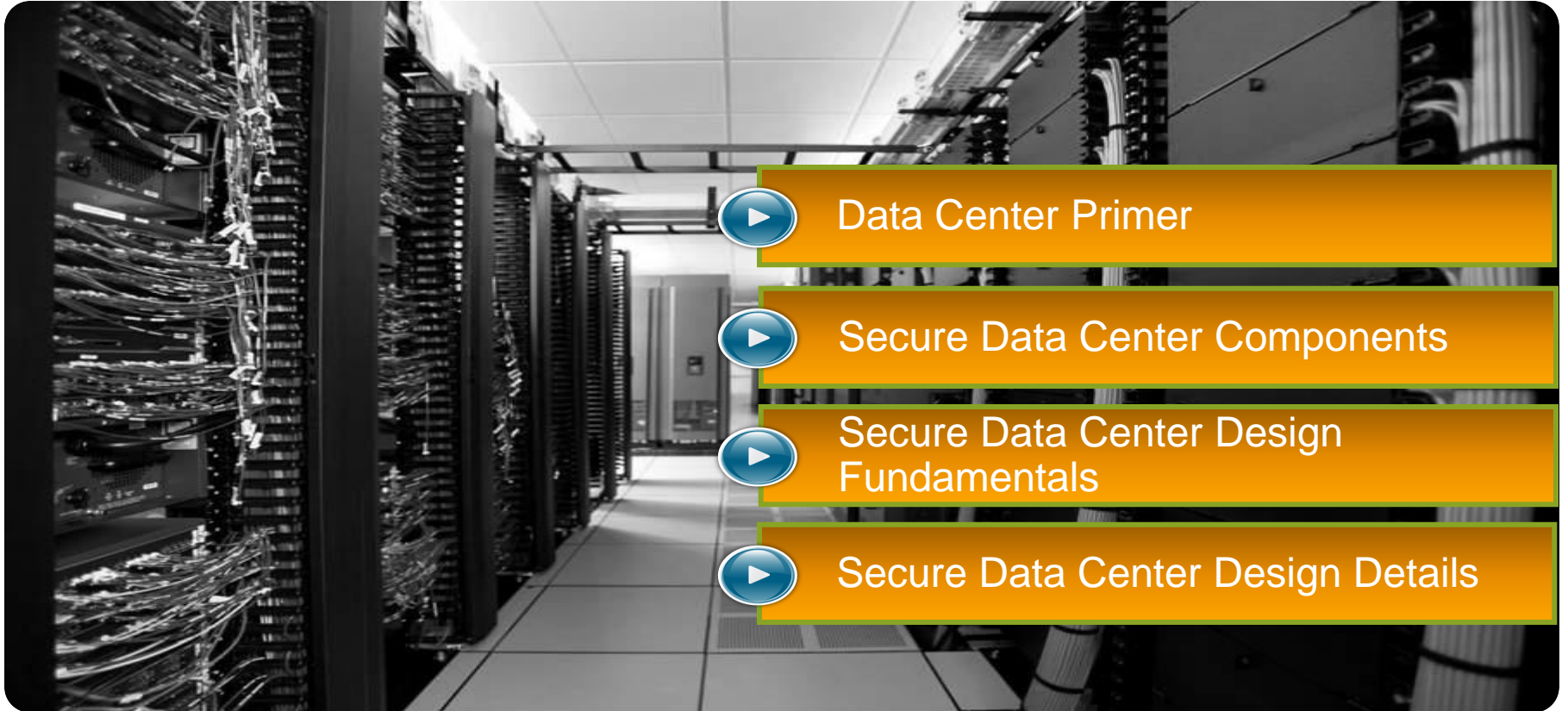
Speaker information

- Contact information:
 - David Anderson
 - Solutions Architect
 - Borderless Security team – US
 - E-mail:
- Focus areas:
 - Data Center Security
 - Virtualization
 - Secure Mobility
 - Security Design
 - Compliance (PCI, Federal)

Takeaways

- To effectively integrate security must understand the core data center fabric technologies and features: VDC, vPC, VRF, server virtualization, traffic flows
- Security as part of the core design
- Designs to enforce microsegmentation in the data center
- Enforce separation of duties in virtualized and cloud environments
- Security to enforce continuous compliance

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

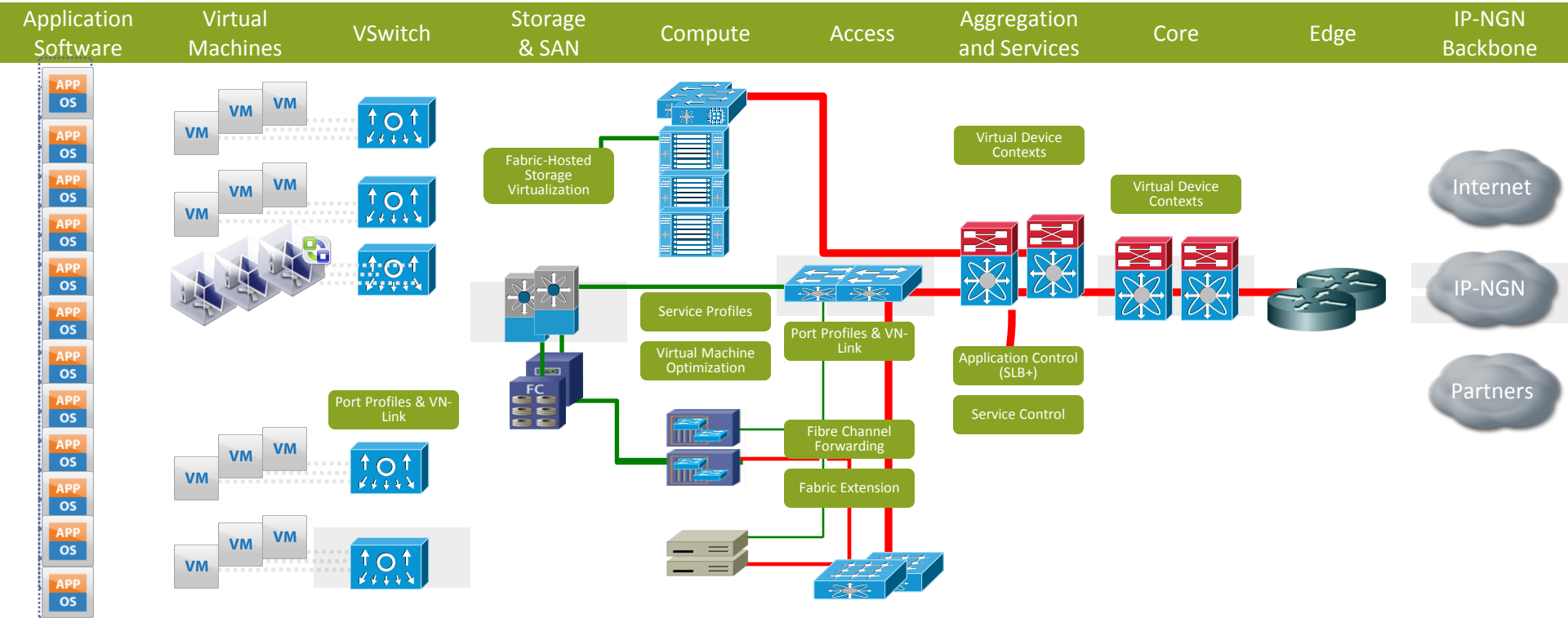
Cisco Datacenter Terms Primer

Know the lingo

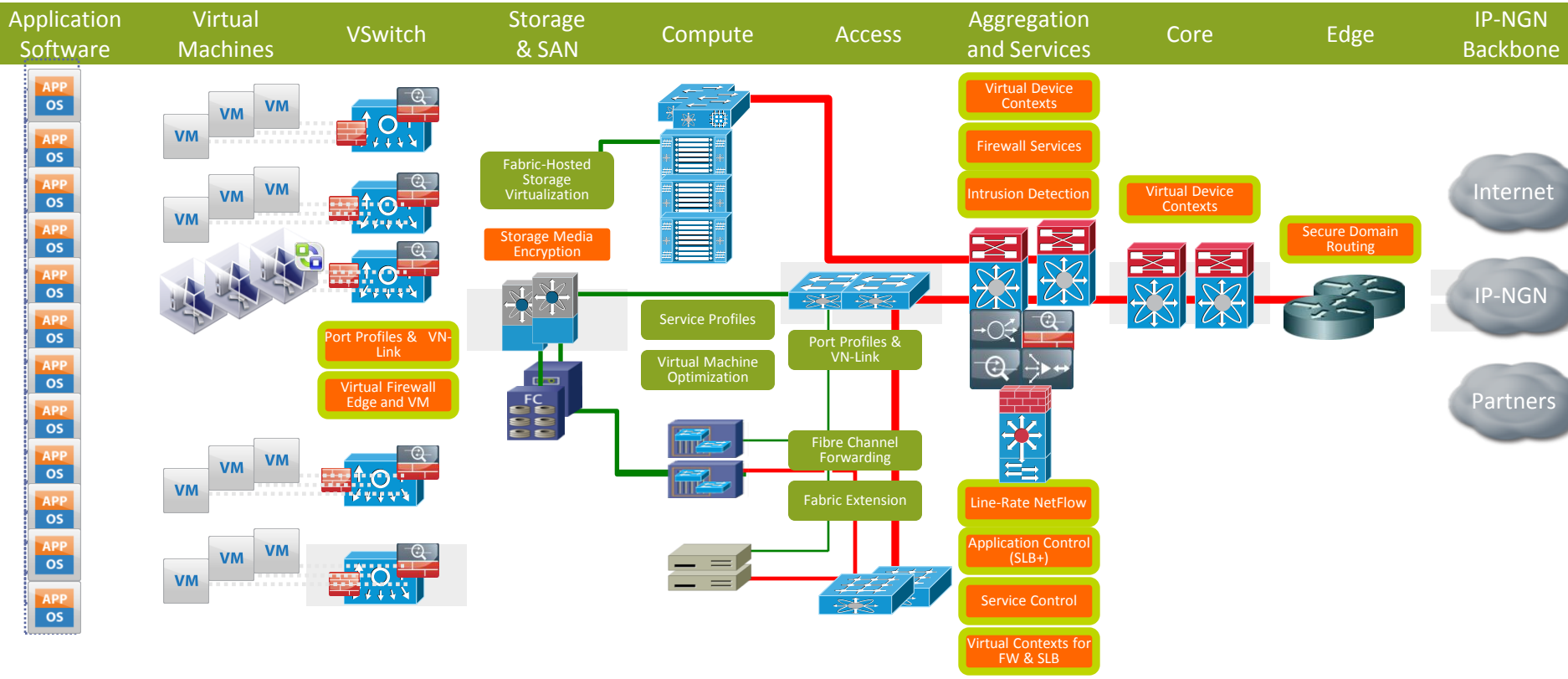
- **VDC** – Virtual Device Context
- **VPC** – Virtual Port Channel
- **VSS & MEC** – Virtual Switching System & Multi-chassis Ether-channel
- **VSL & Peer Link** – Virtual Switch Link
- **ECMP** – Equal cost Multi-Path
- **VSD** – Virtual Service Domain
- **VBS** – Virtual Blade Switching
- **VRF**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



Data Center Architecture



Secure Data Center Architecture



Data Center Security Challenges



Security Threats & Considerations

- 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 Concerns*

Secure the Platform

Network security best practices

- Network device hardening
- Defense in Depth
- AAA
- NetFlow
- Separation of duties and least privileges

Virtualization specifics

- Follow hypervisor hardening recommendations
- Access Controls (production vs. management)
- Secure and harden Guest OS
- Segmentation

Add Security Services

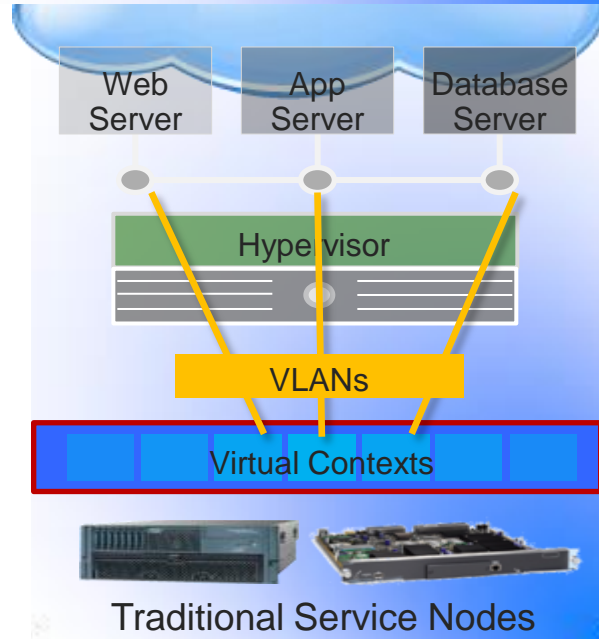
- VRF, VLAN, Access control Lists
- Stateful Network Firewalls
- Intrusion Detection and Prevention
- Web firewalls
- Load Balancers
- SSL Offloading
- Virtual security appliances
- Management and Visibility tools

Data Center Security Components: What's in our toolbox

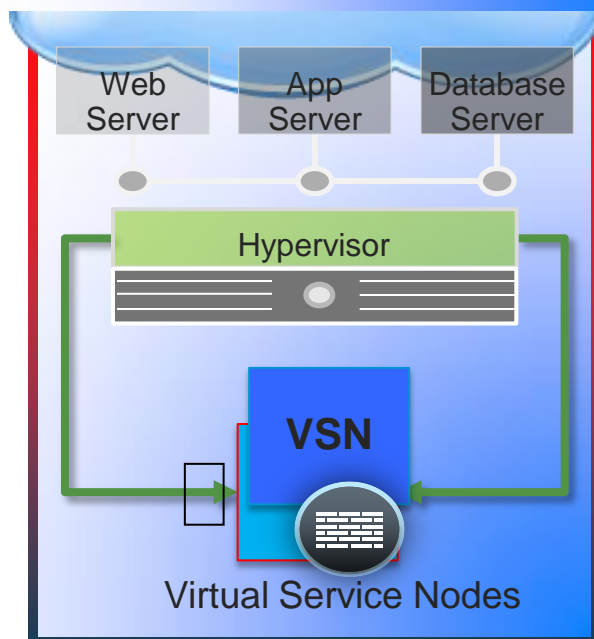


Physical and Virtual Service Nodes

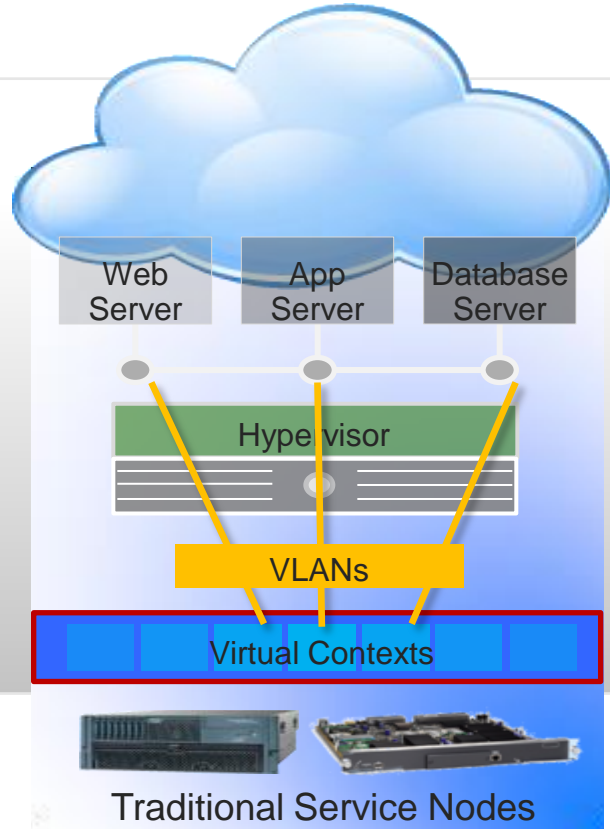
1 Redirect VM traffic via VLANs to external (physical) appliances



2 Apply hypervisor-based network services



Physical Firewalls



ASA Services Module



ASA 5585 Appliance



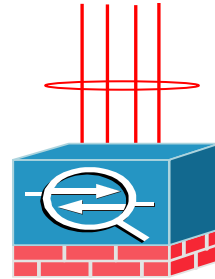
Features in ASA Firewalls

EtherChannel

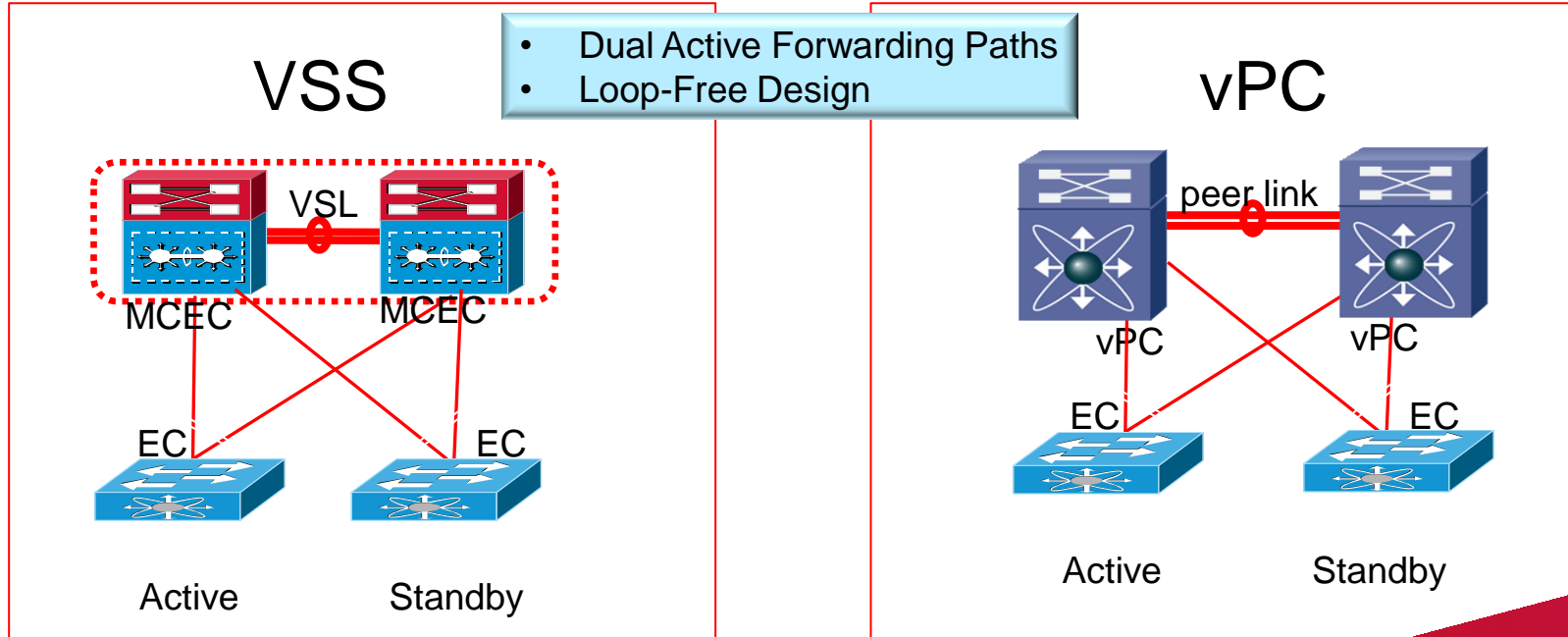
- ASA supports Link Aggregation Control Protocol (LACP), an IEEE 802.3ad standard
- Each port-channel supports up to 8 active and 8 standby links
- Supported methods of aggregation: Active, Passive & On
- EtherChannel ports are treated just like physical and logical interfaces on ASA
- ASA can tie-in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

Up to 32 interfaces per Virtual Context (formerly 2)

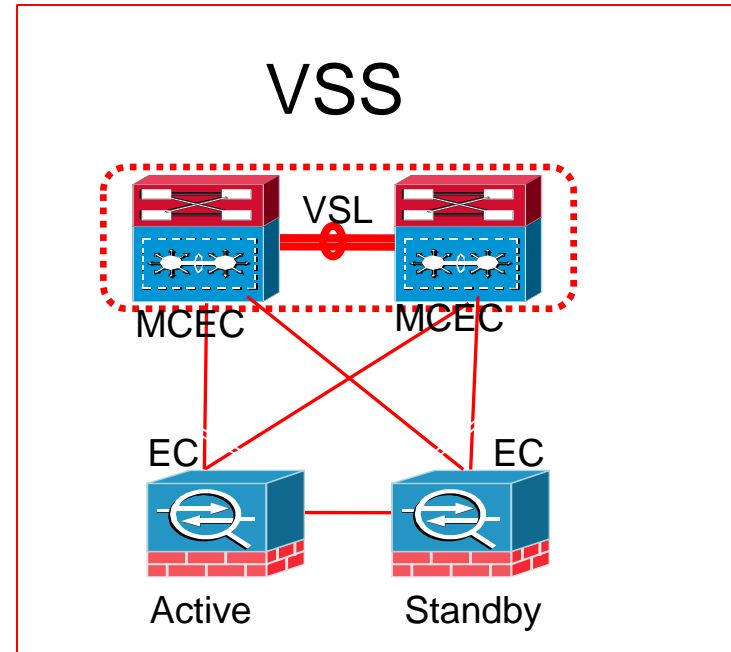
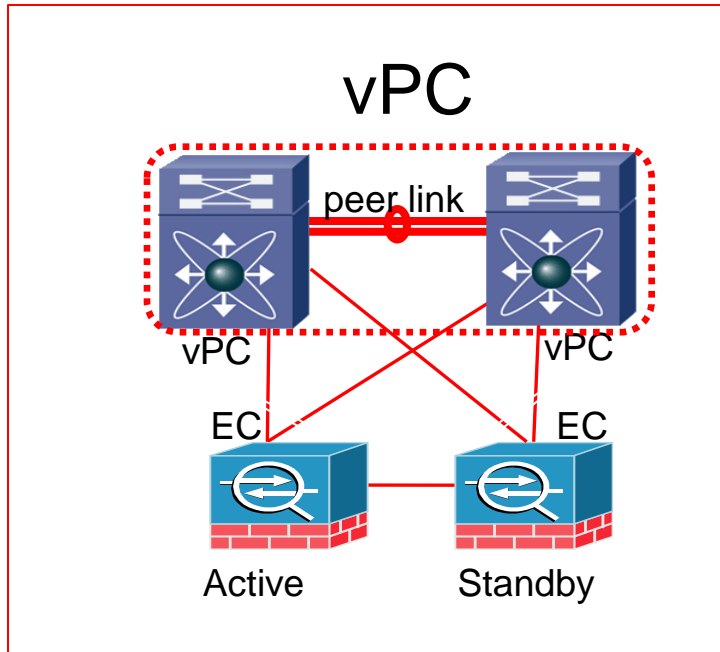
- - 4 Interfaces per bridge group 8 bridge groups per Virtual Context



Catalyst 6500 VSS and Nexus 7000 vPC



ASA Integration with vPC & VSS



Virtualization Concerns



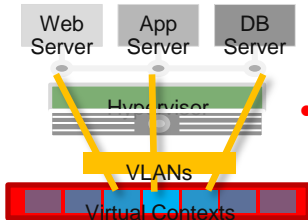
- Policy Enforcement
 - Applied at physical server—not the individual VM
 - Impossible to enforce policy for VMs in motion



- Operations and Management
 - Lack of VM visibility, accountability, and consistency
 - Difficult management model and inability to effectively troubleshoot

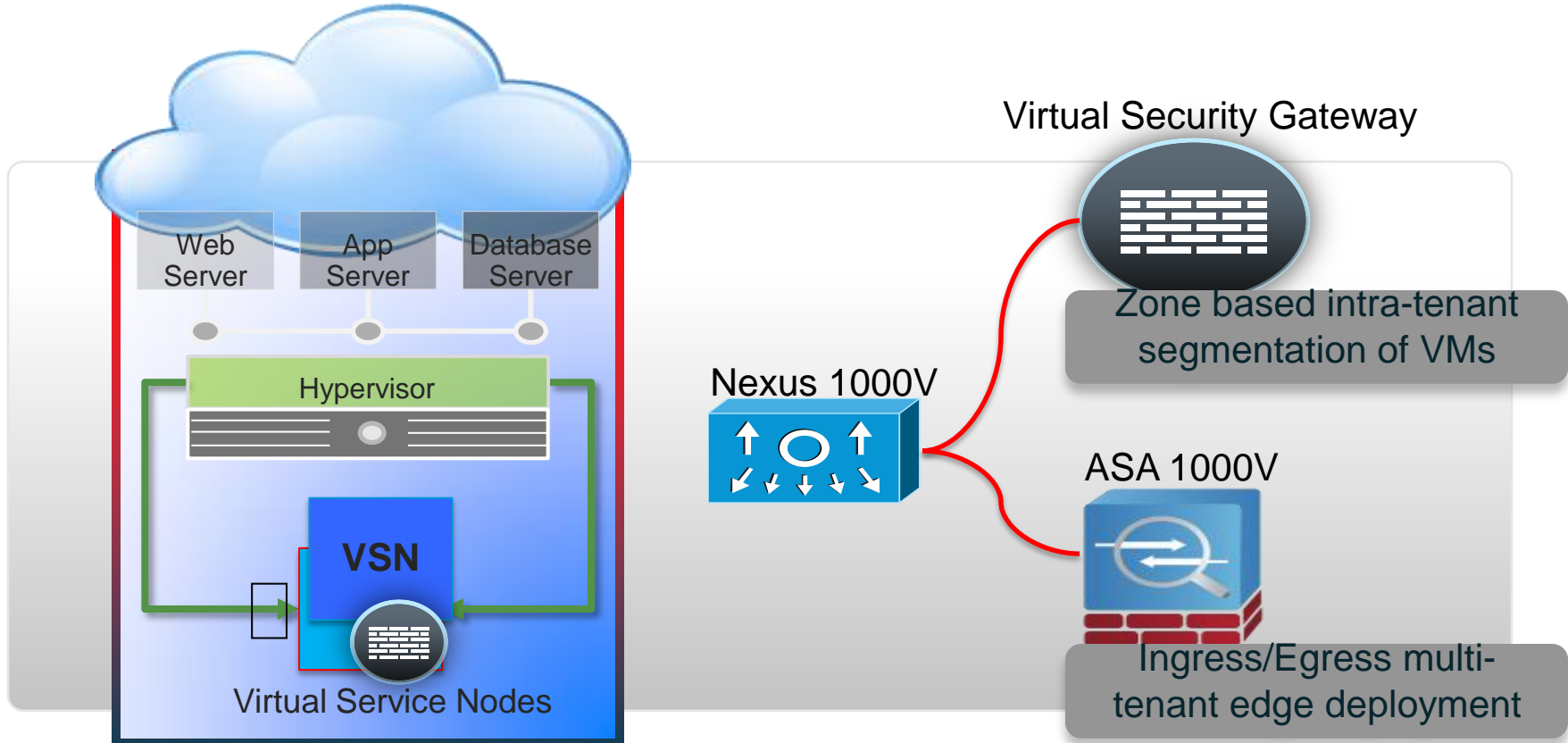


- Roles and Responsibilities
 - Muddled ownership as server admin must configure virtual network
 - Organizational redundancy creates compliance challenges



- Machine Segmentation
 - Server and application isolation on same physical server
 - No separation between compliant and non-compliant systems...

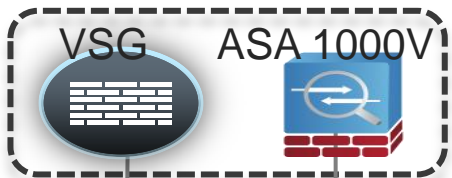
Virtualization & Virtual Service Nodes



Cisco's Virtual Security Architecture

Orchestration / Cloud Portals

Virtual Network Management Center



Extending existing **operational workflows** to virtualized environments

Extending **network services** to virtualized environments

Extending **networking** to virtualized environments

Nexus 1000V

vPath

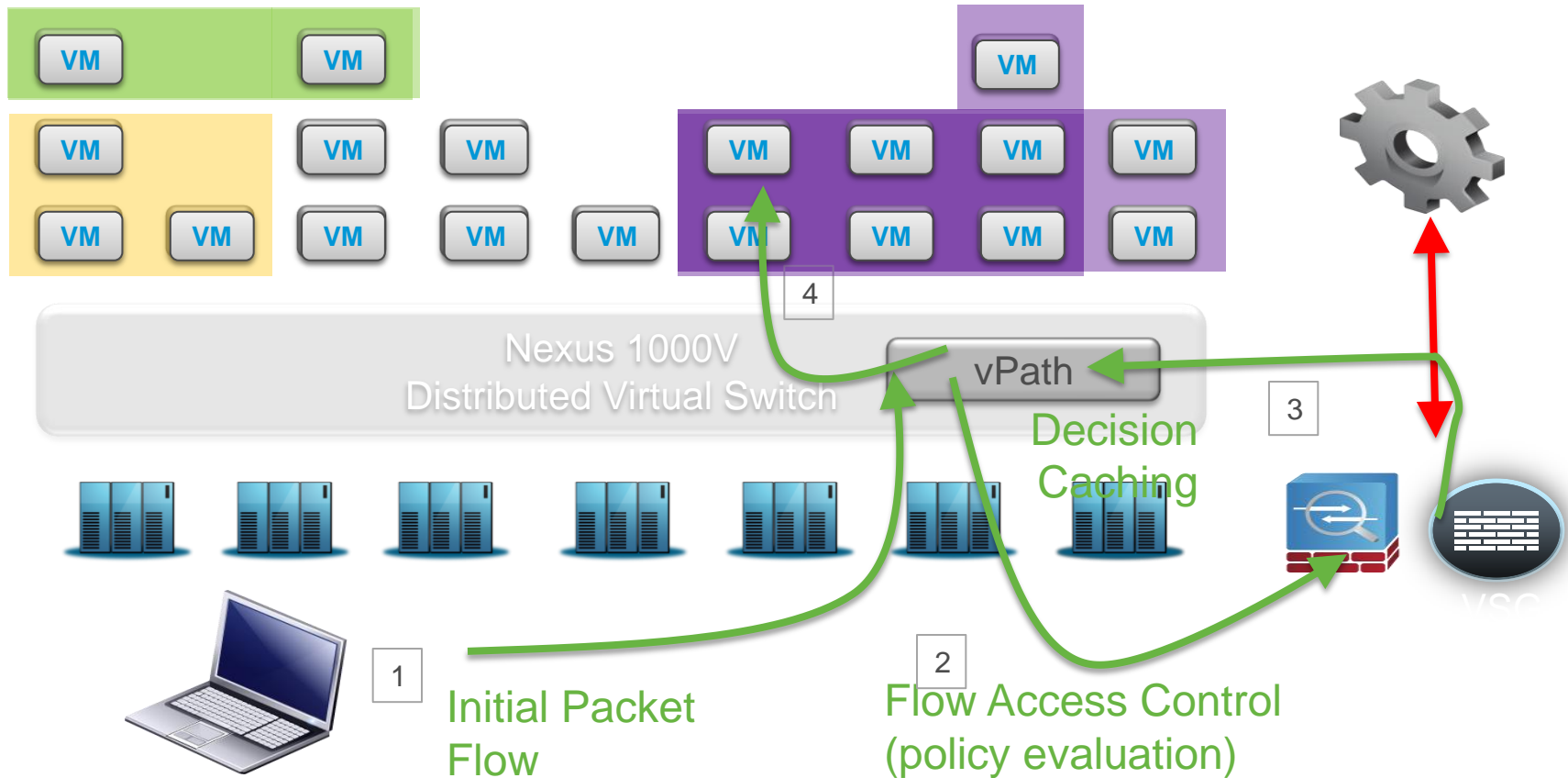


vPath— The intelligent virtual network

- vPath is intelligence build into Virtual Ethernet Module (**VEM**) of Nexus 1000V (1.4 and above)
- vPath has two main functions:
 - a. **Intelligent Traffic Steering**
 - b. **Offload processing via Fastpath from virtual Service Nodes to VEM**
- Dynamic Security Policy Provisioning (via security profile)
- Leveraging vPath enhances the service performance by moving the processing to Hypervisor

vPath
Nexus 1000V-VEM

vPath: Fast Path Switching for Virtualization



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)

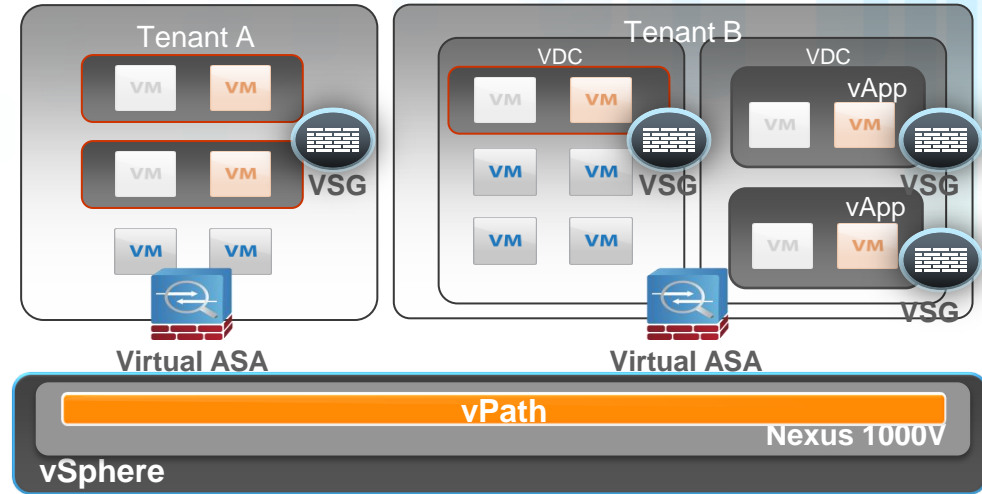
Hence can be deployed on a dedicated server, or hosted on a Nexus 1010 appliance

Performance optimization via enforcement off-load to 1000V vPath

High availability

ASA 1000v

- Runs same OS as ASA appliance and blade
- Maintains ASA Stateful Inspection Engines
- IPSEC site-to-site VPN
- Collaborative Security Model
 - VSG for intra-tenant secure zones
 - Virtual ASA for tenant edge controls
- Integration with Nexus 1000V & vPath



Nexus 1000V 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

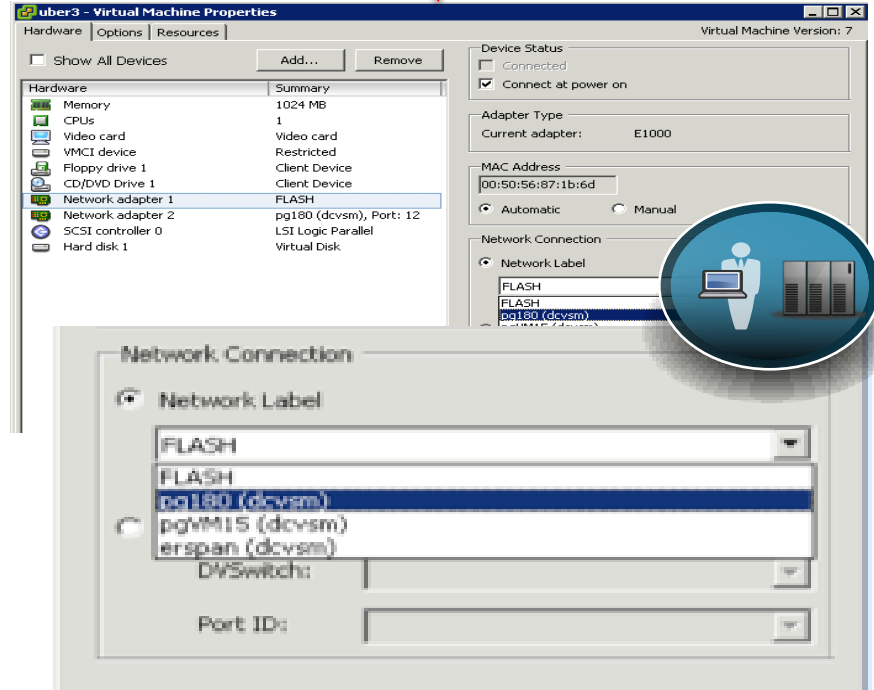
state enabled

interface Vethernet9

inherit port-profile vm180

interface Vethernet10

inherit port-profile vm180



Support Commands Include:

- ✓ Port management
- ✓ Port-channel
- ✓ VLAN
- ✓ ACL
- ✓ PVLAN
- ✓ Netflow
- ✓ Port Security
- ✓ QoS

Security Policy to Port Profile

The screenshot displays the Cisco Virtual Network Management Center (VNM) interface. On the left, the navigation pane shows the hierarchy: Firewall Policy > Security Profile > root > Contrator > Security Profiles. The 'Security Profiles' folder is expanded, and the 'SecureContractors' profile is selected. The main pane shows the 'General' tab for this profile, with a table containing one entry:

Name
SecureContractors

On the right, a terminal window shows the configuration commands for the 'Contractor' vethernet:

```
org root/Contractor
vn-service ip-address 192.168.173.42 vlan 20 security-profile SecureContractor
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#
```

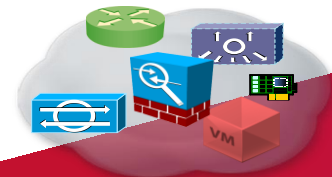
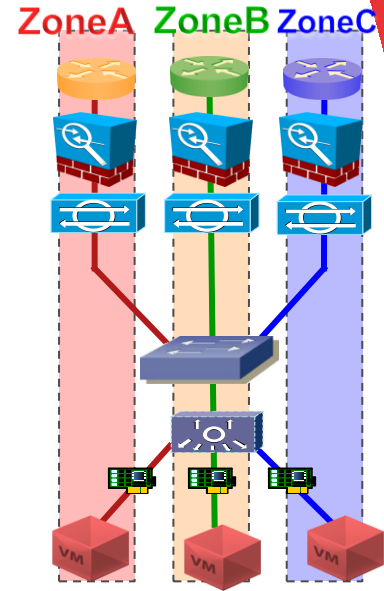
Two yellow circles highlight the 'SecureContractors' profile name in the VNM interface and the 'SecureContractors' text in the terminal output. A green arrow points from the terminal output back to the VNM interface, indicating the mapping between the CLI configuration and the GUI representation.

Design Fundamentals



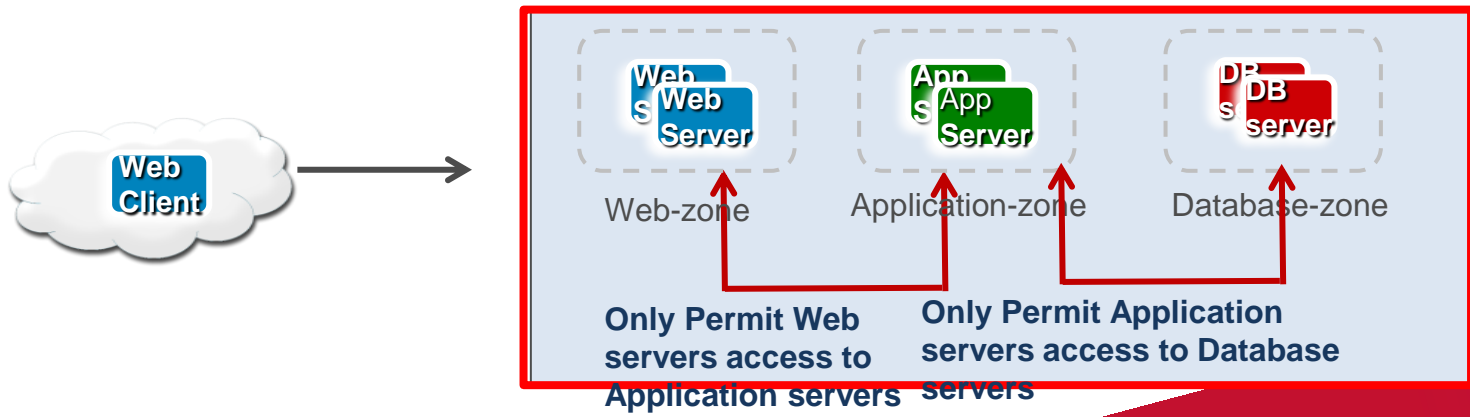
Secure Data Center

- 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



Understand Network and Application Flows

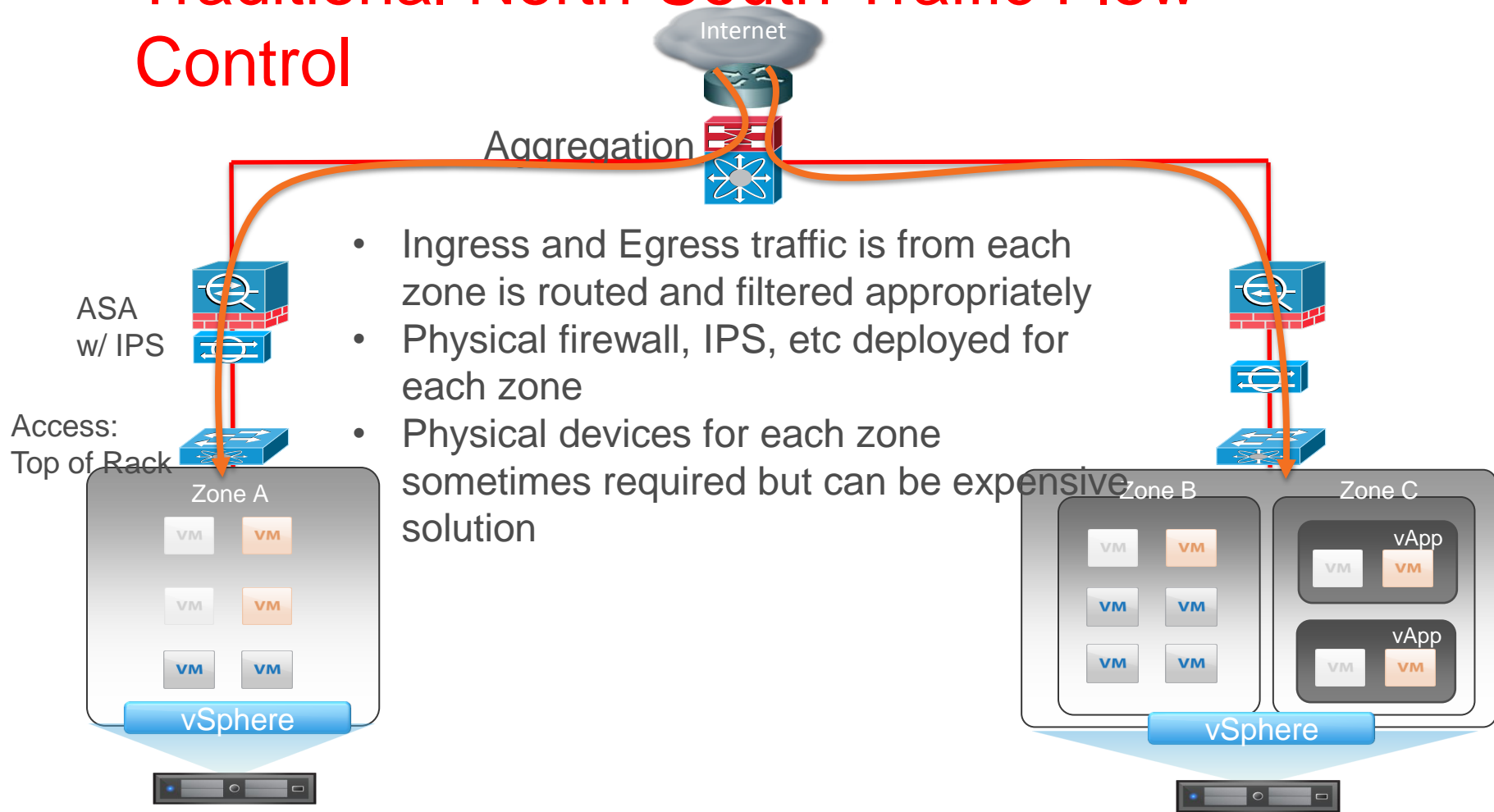
- Understand how the applications are deployed and accessed both internally and externally
- Understand the North-South, East-West flow patterns
- Adjacency of services to servers is important. Adding services to existing flow patterns minimizes packet gymnastics!
- Again, design with the maximum amount of high availability: know your failover and fallback times, traffic paths during failover scenarios



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

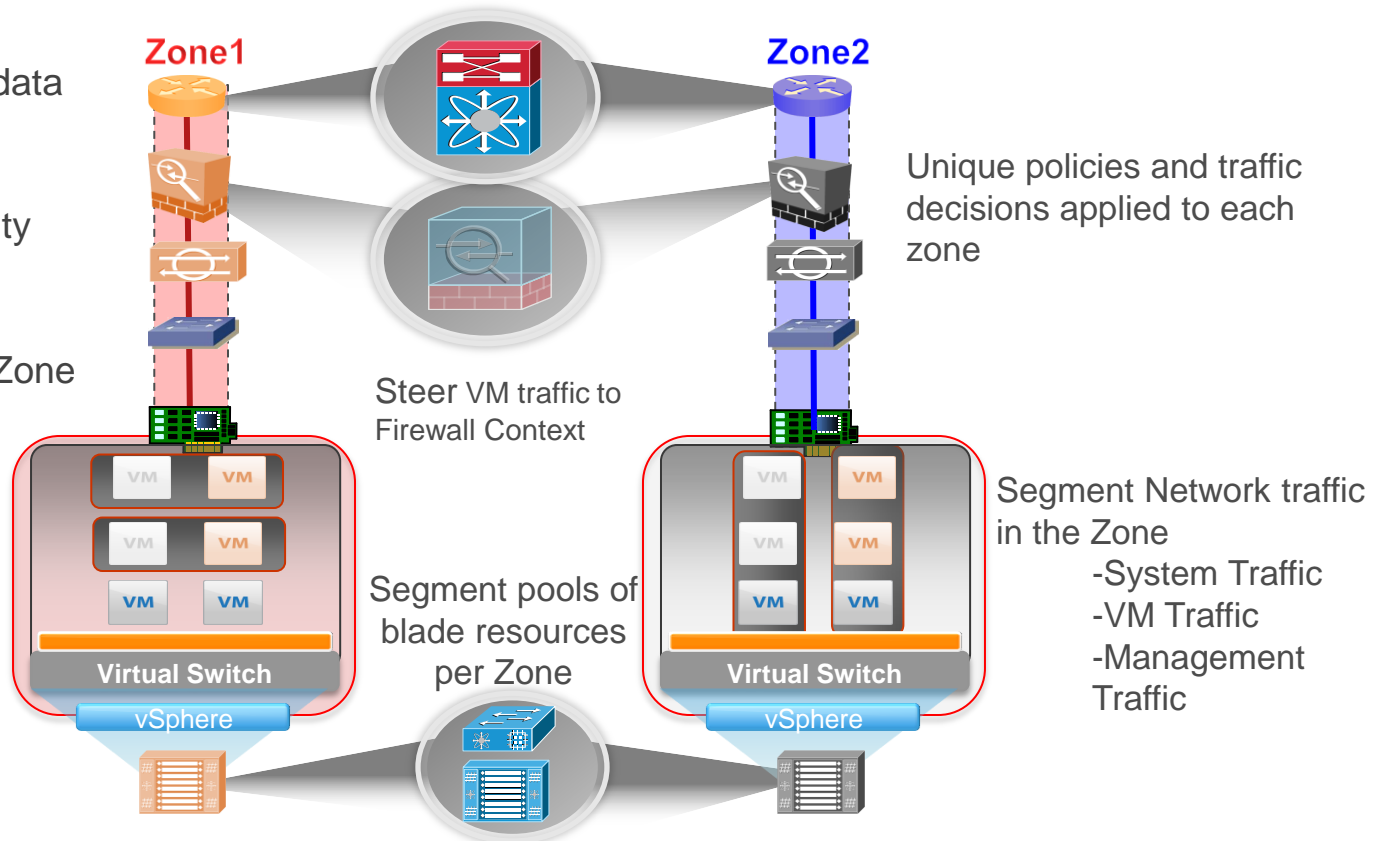
Traditional North-South Traffic Flow Control



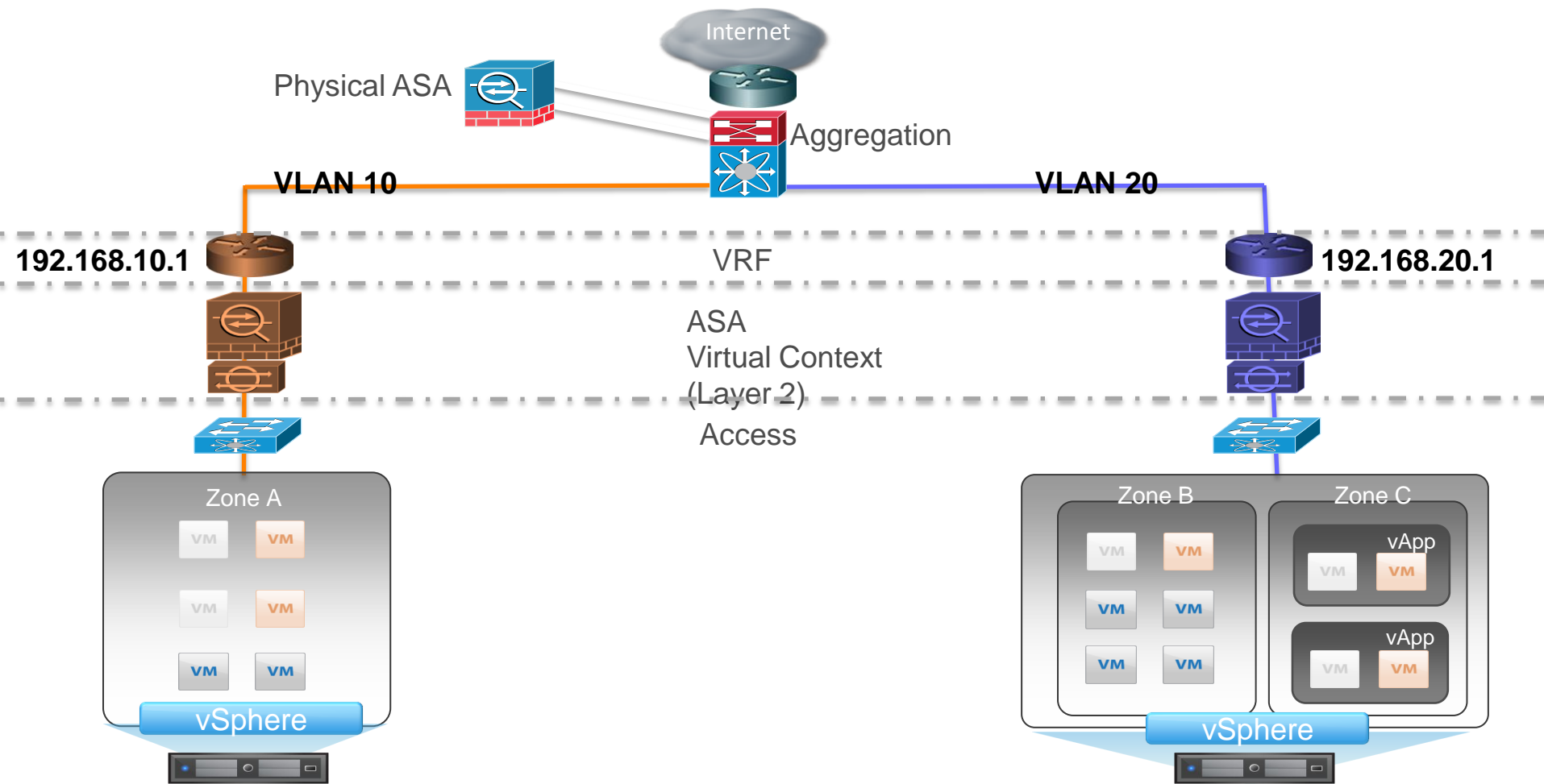
Network Virtualization and Zones

Acme Co. - Control Traffic and Apply Policy per Zone

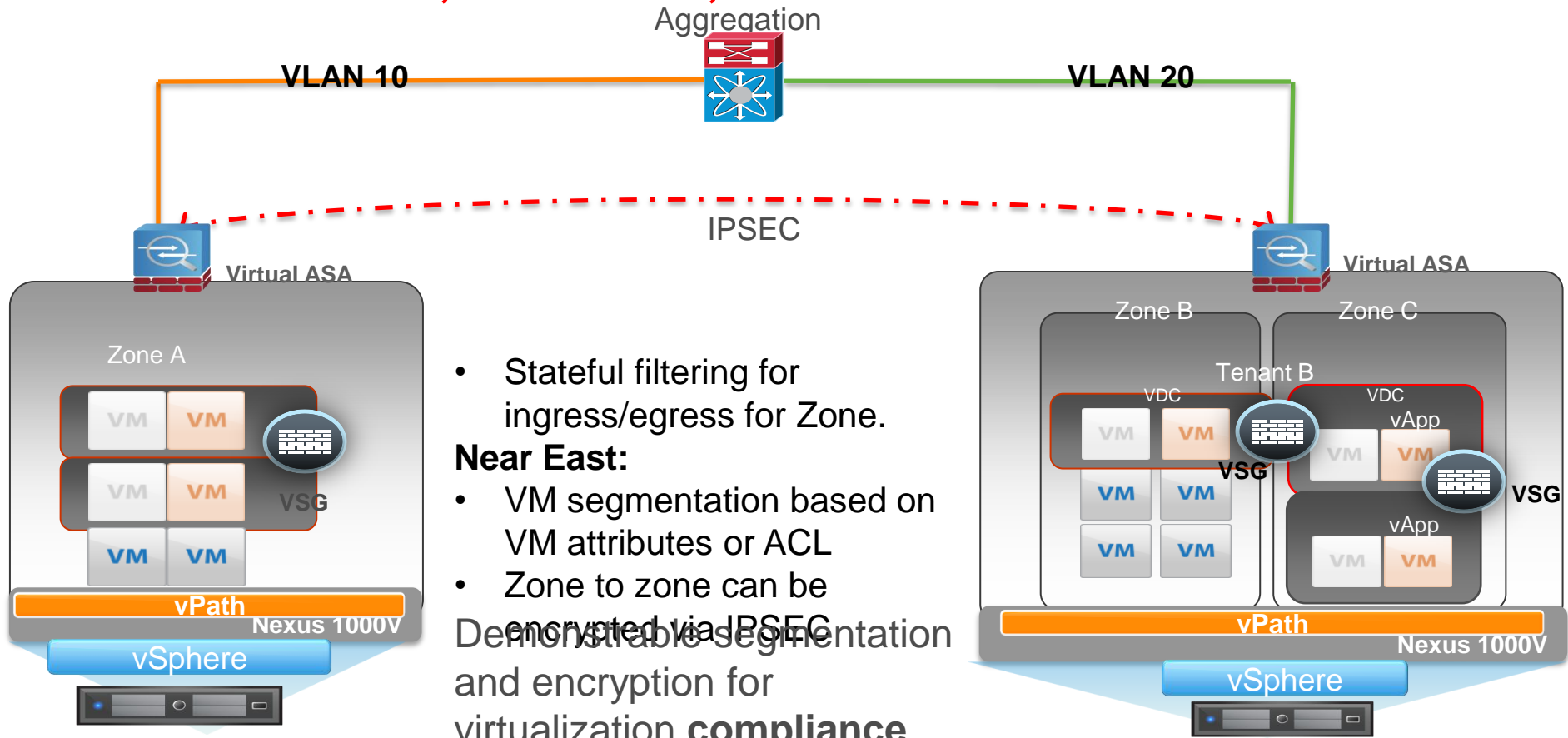
- Zones used to provide data centric security policy enforcement
- Physical network security mapped per zone
 - VRF, Virtual Context
- Lockdown elements in Zone



North-South Traffic with Network Virtualization

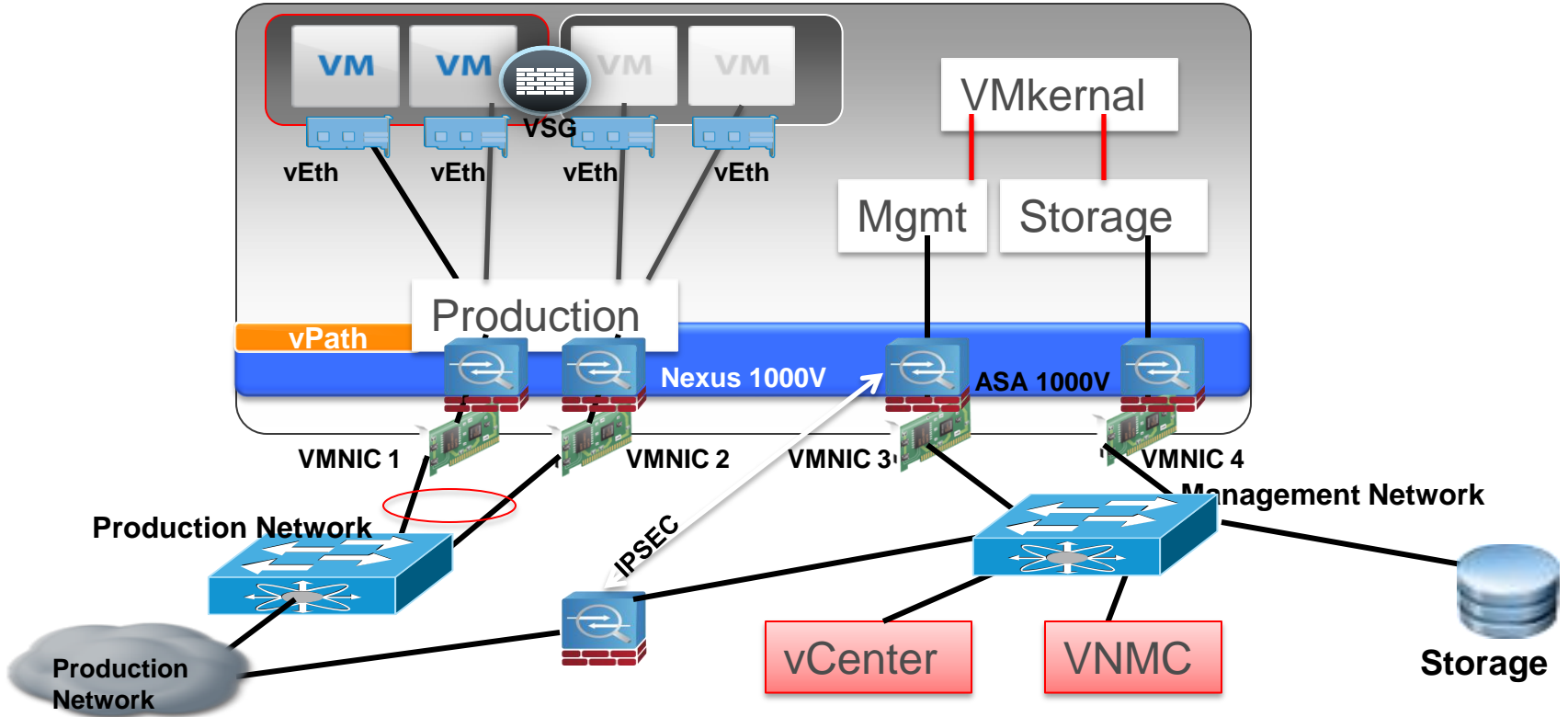


Microsegmentation: Per Zone, Per VM, Per vNIC

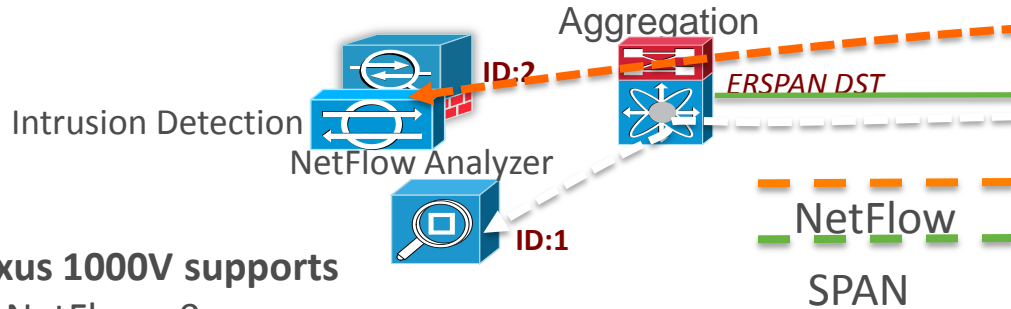


- Stateful filtering for ingress/egress for Zone.
- Near East:**
- VM segmentation based on VM attributes or ACL
 - Zone to zone can be encrypted via IPSEC
- Demonstrable segmentation and encryption for virtualization **compliance**

Segmentation of Production and Non-Production Traffic



Visibility: Monitor VM to VM Traffic

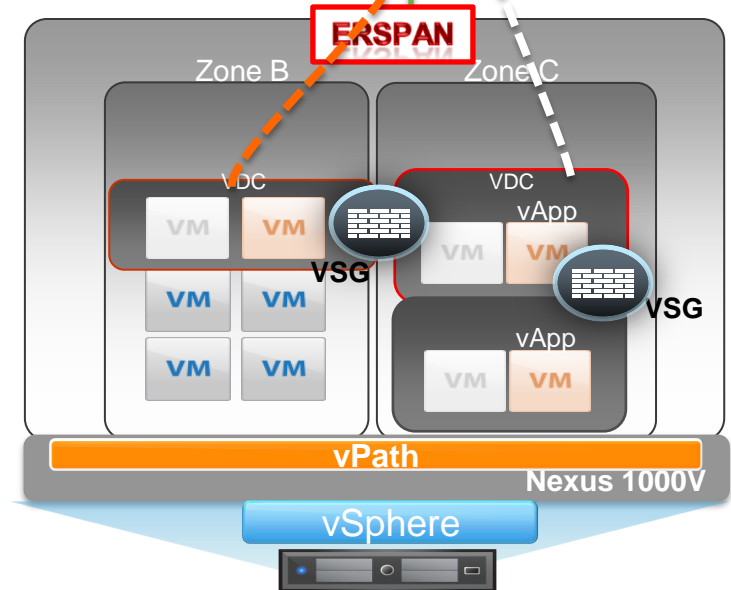


Nexus 1000V supports

- NetFlow v9
- ERSPAN/SPAN
- Permit protocol type header "0x88BE" for ERSPAN GRE
- ERSPAN does **not** support fragmentation
- 1000V requires Netflow source interface Defaults to Mgmt0

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

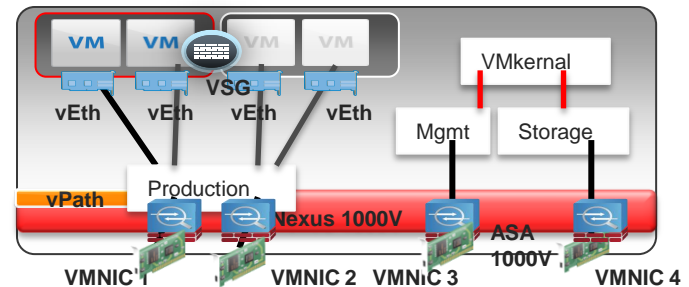


Virtualization & Compliance: PCI DSS 2.0

- PCI security requirements apply to all 'system components.'
- System components are defined as:
 - Any network component, server, or application that is included in or connected to the cardholder data environment.
 - Virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors.
- The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data.
- Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment.

Guidance

- All virtual components in scope
- All virtual communications and data flows must be identified and documented
- Virtualized environment must maintain proper segmentation
- Must meet intent of all 12 PCI requirements



Design Details

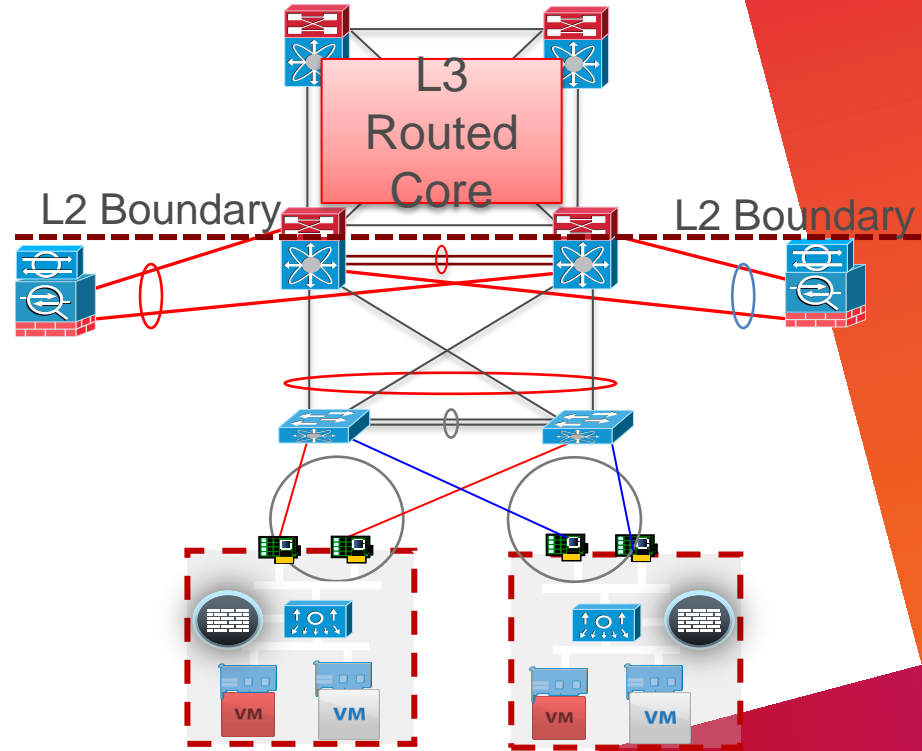


Secure Data Center Reference Architecture

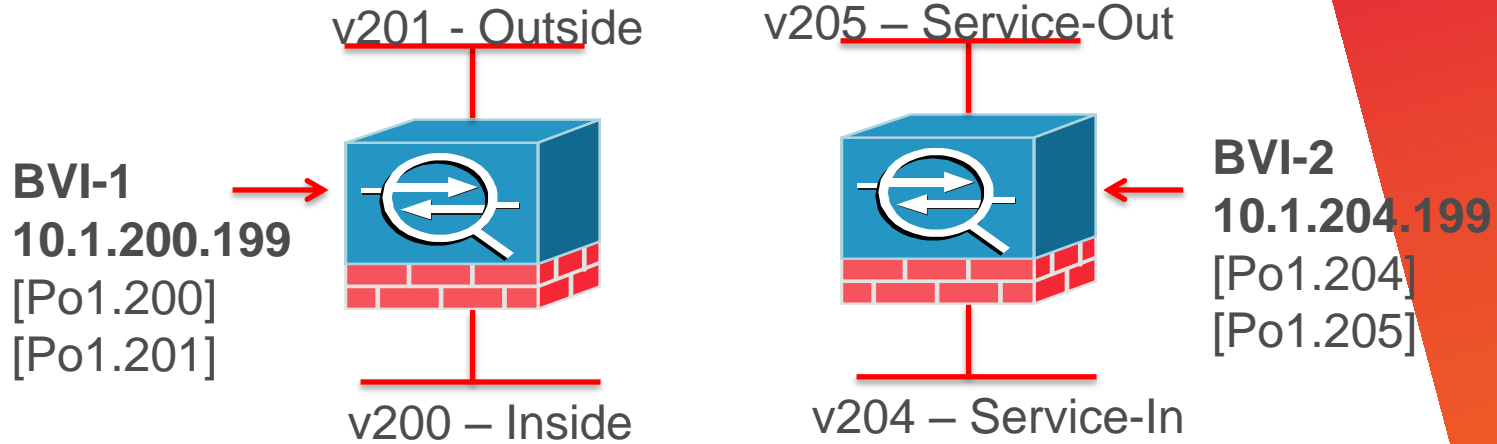
- 2x Nexus 7010s with VDCs (Core and Aggregation) (NX-OS 5.1(3))
- 2x Nexus 5Ks for top of rack
- 2x ASA 5585-60 with IPS
- 2x 6500-E with ASA-SMs
- 2x Virtual Security Gateway (VSG) in HA mode
- 2x Nexus 1000V with redundant VSMS
- Identity Services Engine (ISE) for 802.1x user AAA
- Standard VMWare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

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



ASA Details



channel-group 1 mode passive



vPC9



channel-group 1 mode active



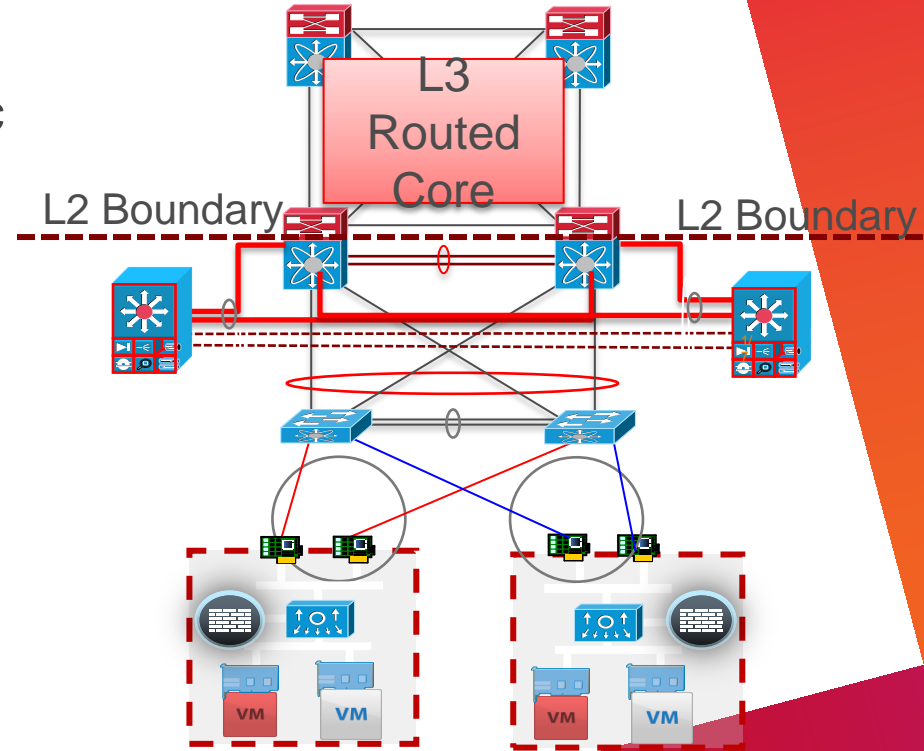
vPC10



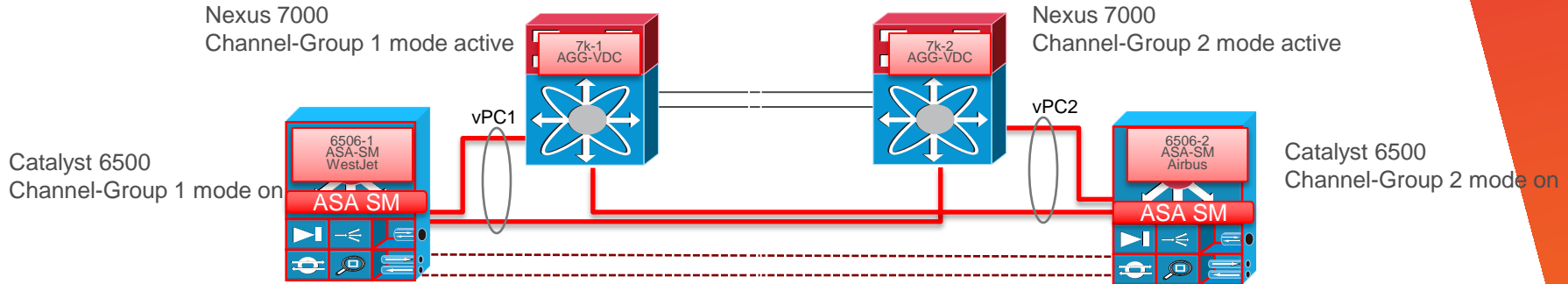
Port Channel Load-Balancing Configuration:
System: src-dst ip

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



Nexus 7000 & Cat 6500 Channel Group Modes

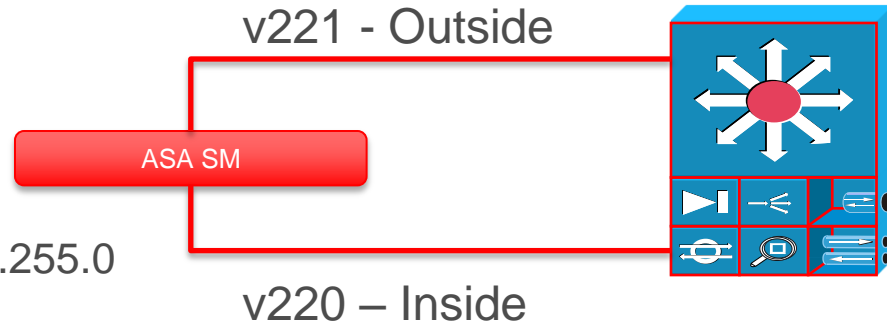


ASA SM Layer 2 and 3

interface BVI2

description bvi for 221 and 220

ip address 10.1.221.199 255.255.255.0

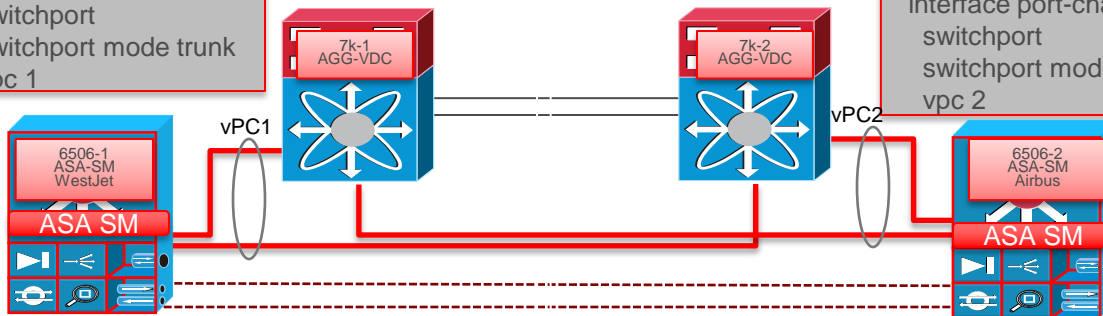


ASA SM Details

```
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
```

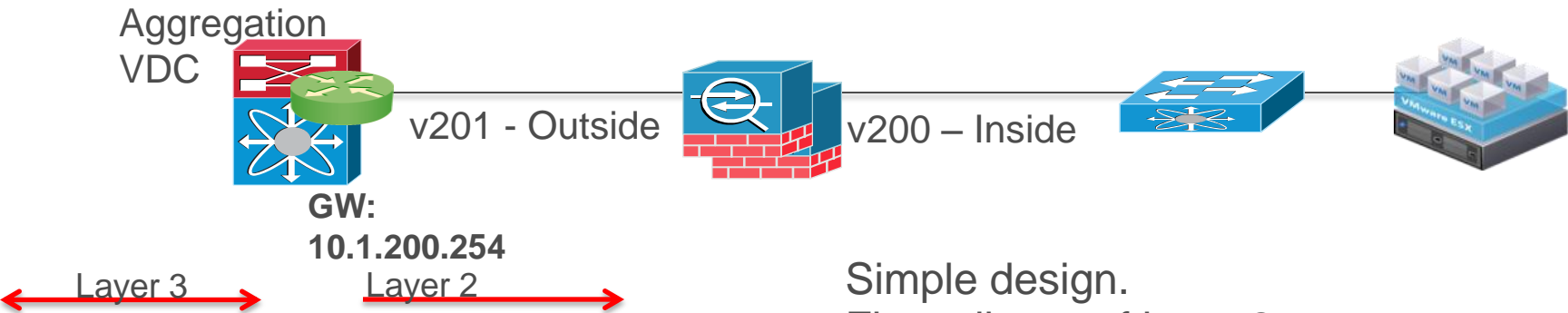
```
BVI2
ip address
10.1.221.199
interface Vlan220
  nameif inside
  bridge-group 2
  security-level 100
!
interface Vlan221
  nameif outside
  bridge-group 2
  security-level 0
```



```
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 Gateway Outside of Firewall: Design #1

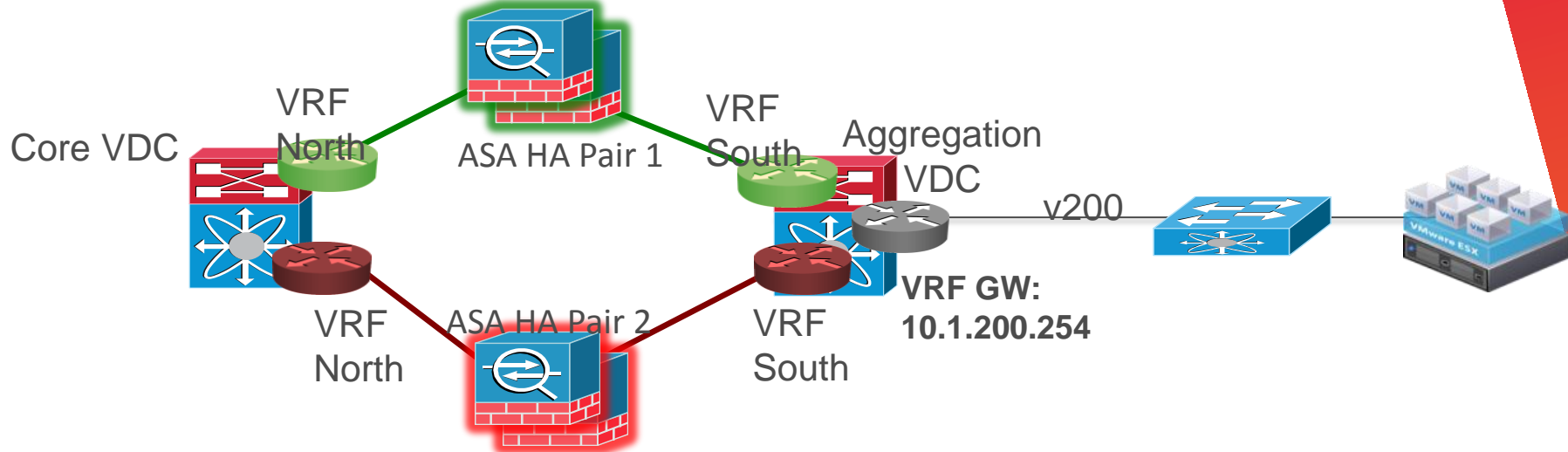
ASA HA pair in transparent mode with SVI on Aggregation VDC. Server gateway on outside of firewall



Simple design.
Firewall part of layer 2
failure domain.

ASA in the Data Center: Design #2

Firewall Between Inter-VDC Traffic

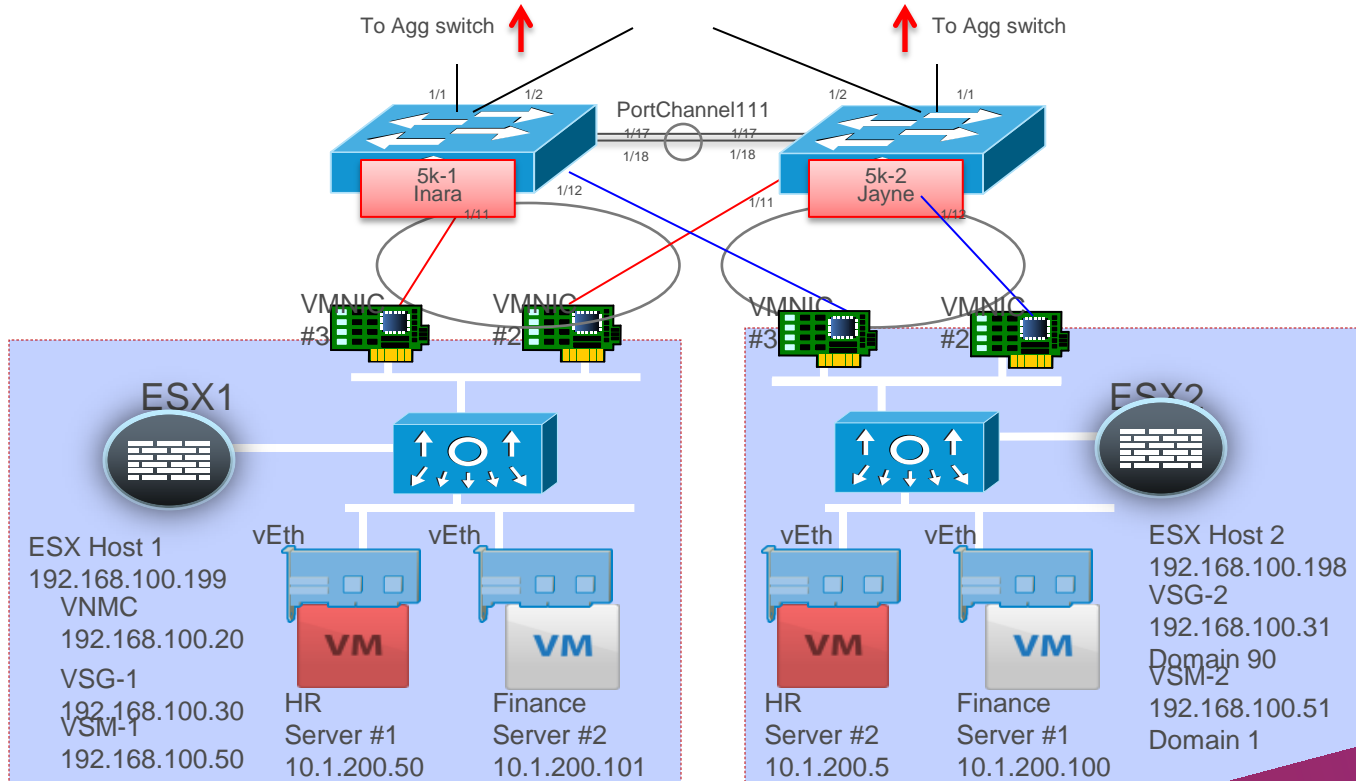


- Transparent (L2) firewall services are “sandwiched” between Nexus VDCs
- Allows for other services (IPS, LB, etc) to be layered in as needed
- ASAs can be virtualized to for 1x1 mapping to VRFs
- Useful for topologies that require a FW between aggregation and core
- Downside is that most/all traffic destined for Core traverses FW; possible bottleneck, etc

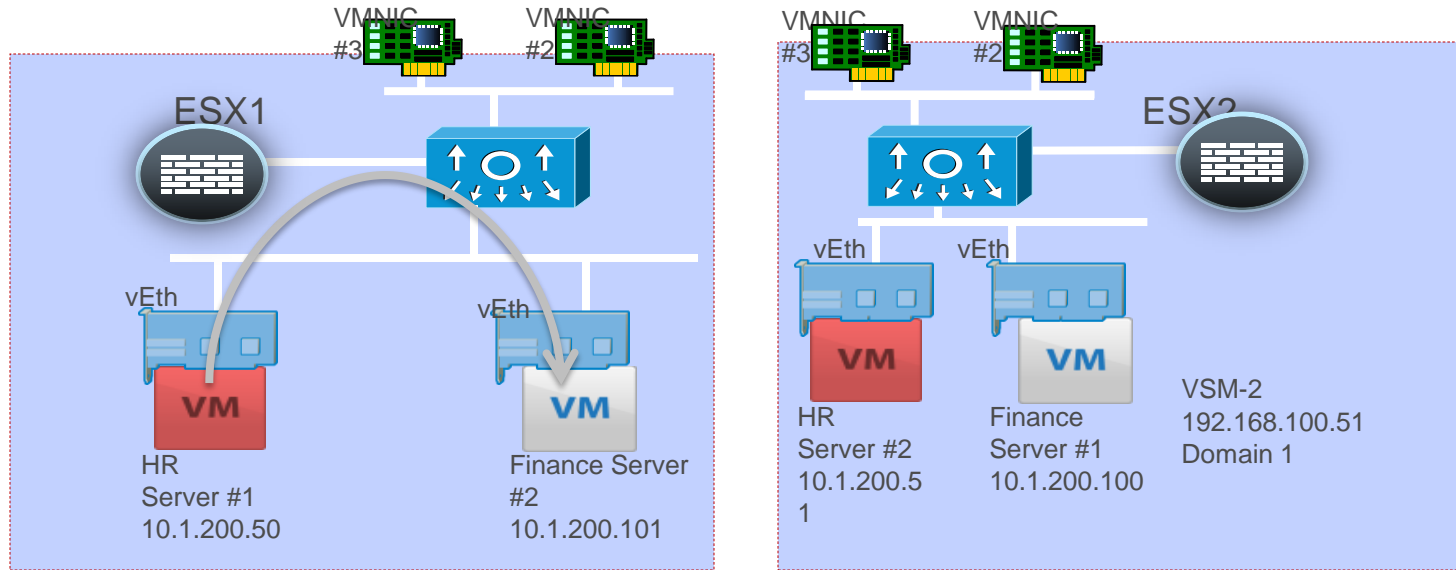
Design Details and Benefits

- Zone based differentiation, building blocks with VLANs and VRFs
 - ✓ Inter-VM firewalling via VSG/ASA 1000V
 - ✓ Intra-zone firewalling via both VSG/ASA 1000V and ASA/ASA-SM
 - ✓ Inter-zone firewalling via ASA 1000V, ASA, or ASA-SM

Server Access and VM Network Details



Deny HR to Finance



Policy Hierarchy

The screenshot displays the Cisco Virtual Network Management Center interface. The top navigation bar includes the Cisco logo, the title "Virtual Network Management Center", and user information: "(admin)", "Log Out", "About", and "Help". Below this is a secondary navigation bar with tabs for "Tenant Management", "Resource Management", "Policy Management" (which is highlighted), and "Administration".

The main content area is divided into two sections. On the left is a "Firewall Policy" tree view showing a hierarchy starting from "root". Under "root", there are "Object Groups", "Policies", "Policy Sets", and "Zones". The "Zones" folder is expanded, showing "CPOC" and "HR" (which is highlighted in green). Under "CPOC", there are "Object Groups", "Policies" (including "Deny_Interzone_traffic"), "Policy Sets" (including "Deny_Interzone_PolicySet"), and "Zones" (including "Finance" and "HR").

On the right is a configuration window for the "HR" zone. The breadcrumb path is "root > CPOC > Zones > HR". The window has 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.

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', and 'Administration'. The 'Policy Management' section is active, showing 'Security Policies', 'Device Policies', 'Capabilities', and 'Diagnostics'. The left sidebar shows a tree view of the network configuration, with 'Deny_Interzone_traffic' selected under 'Policies'. The main content area shows the configuration for 'Deny_Interzone_traffic', with the 'Deny_HR_to_Finance' rule highlighted. An 'Edit Rule' dialog box is open, showing the configuration for 'Deny_HR_to_Finance'. The 'General' tab is selected, and the 'Action to take' section is highlighted with an orange box and an arrow pointing to the 'drop' radio button. The 'log' checkbox is checked. The 'Protocol' and 'Ether Type' sections both have 'Any' selected. The 'Events' tab is also visible, showing a table of actions.

Edit Rule
Edit (Deny_HR_to_Finance)

General | Source and Destination Condition | Events

Name: Deny_HR_to_Finance
Description:
Action to take: drop permit
 log
Protocol: Any
Ether Type: Any

Action
Permit
Permit
Drop, Log
Drop, Log
Permit

OK Cancel

Save Reset

© 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

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 On Field discovery

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

Other interesting fields (20)

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

Results per page 10

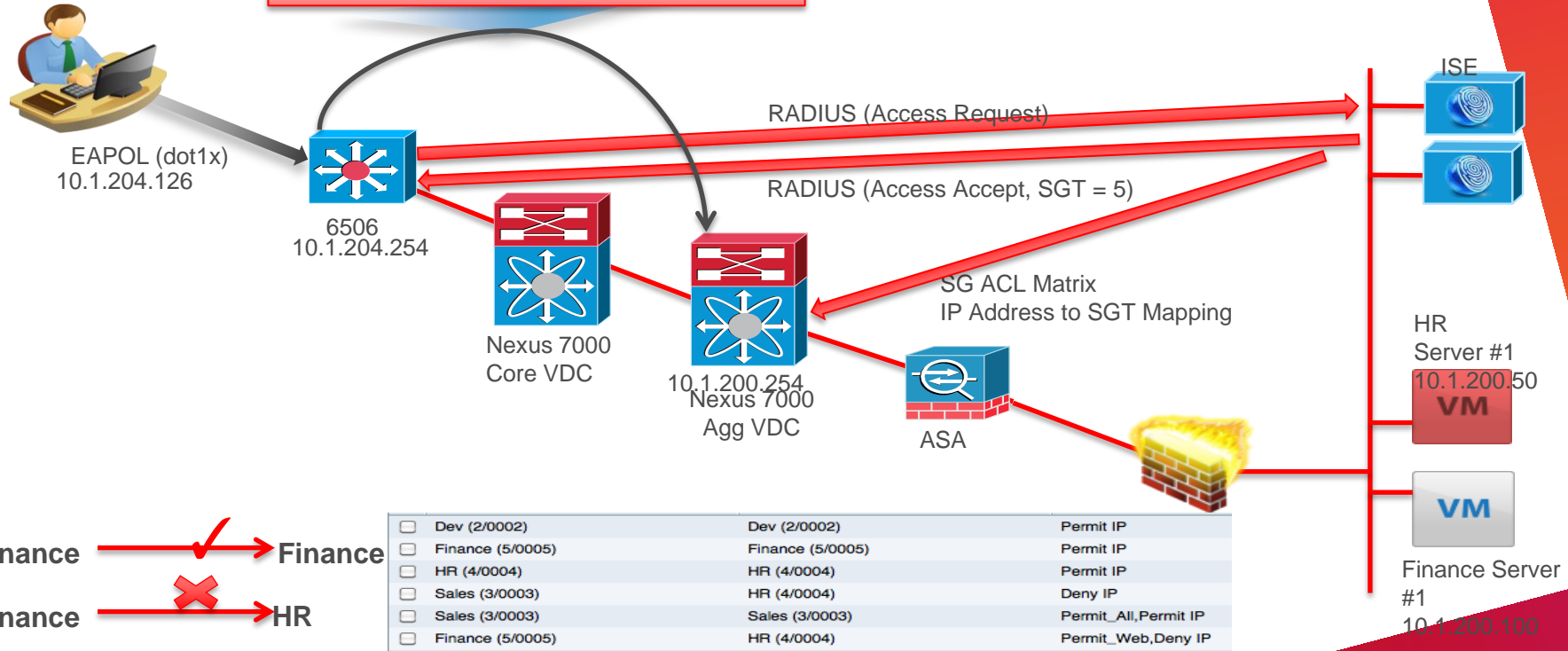
1 5/24/11 2:55:40.000 PM May 24 14:55:40 192.168.100.35 : 2011 May 24 11:41:01 PDT: %POLICY_ENGINE-6-POLICY_LOOKUP_EVENT: policy=Deny_Interzone_PolicySet@root/CPOC rule=Deny_Interzone_traffic/Deny_Finance_to_HR@root/CPOC action=Drop direction=ingress src.net.ip-address=10.1.200.100 src.net.port=49159 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



Adding Identity and Access Control Services : ISE and TrustSec

ISE Traffic Flow

SXP IP Address 10.1.204.126 = SGT 5



<input type="checkbox"/> Dev (2/0002)	Dev (2/0002)	Permit IP
<input type="checkbox"/> Finance (5/0005)	Finance (5/0005)	Permit IP
<input type="checkbox"/> HR (4/0004)	HR (4/0004)	Permit IP
<input type="checkbox"/> Sales (3/0003)	HR (4/0004)	Deny IP
<input type="checkbox"/> Sales (3/0003)	Sales (3/0003)	Permit_All,Permit IP
<input type="checkbox"/> Finance (5/0005)	HR (4/0004)	Permit_Web,Deny IP

ISE Configuration Highlights

Results

Authentication

Authorization

Profiling

Posture

Client Provisioning

Security Group Access

Security Group ACLs

- Permit_All
- Permit_Web

Security Groups

- Dev
- Finance
- HR
- Sales
- Unknown

Security Group Mappings

- Finance (10.1.200.100)
- Finance (10.1.200.101)
- HR (10.1.200.50)
- HR (10.1.200.51)
- Sales (10.1.200.53)

Network Devices

Edit Add Duplicate Import Export Delete Filter

	Name	IP/Mask	Location	Type
<input type="checkbox"/>	Airbus	10.1.204.149/32	All Locations	Cat6K
<input type="checkbox"/>	champs1	10.1.204.252/32	All Locations	N7K
<input type="checkbox"/>	champs2	10.1.204.253/32	All Locations	N7K

Security Group Details

Name **Finance**
Description **Finance Organization**
SGT(Dec/Hex) **5 / 0005**

OK

Security Group Details

Name **Dev**
Description **Development Organization**
SGT(Dec/Hex) **2 / 0002**

OK

Security Group Details

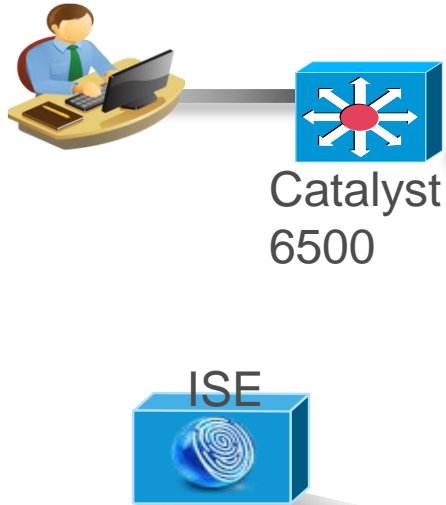
Name **Sales**
Description **Sales Organization**
SGT(Dec/Hex) **3 / 0003**

OK



ISE

ISE Authentication



```
6506-2-airbus#sho authen sess int g3/1
Interface: GigabitEthernet3/1
MAC Address: 0027.0e15.578e
IP Address: 10.1.204.126
User-Name: finance1
Status: Authz Success
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: N/A
SGT: 0005-0
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 0A01CC95000000D0EDFC178
Acct Session ID: 0x0000001E
Handle: 0xC500000D
```

Apr 28,11 03:31:03.651 PM   finance1 00:27:0E:15:57:8E 1

```
Runnable methods list:
Method State
mab Failed over
dot1x Authc Success
```

AnyConnect Authenticated Client Details



The screenshot displays the Cisco AnyConnect Secure Mobility Client interface. The main window is titled "Cisco AnyConnect Secure Mobility Client" and shows the "Network Access Manager (NAM)" configuration page. The interface is divided into two main sections: "Connection Information" and "Security Information".

Connection Information:

- Status: Connected (Authenticated)
- Name: Finance
- Local MAC Address: 00:27:0e:15:57:8e
- Remote MAC Address:
- IP Address: 10.1.204.126
- Speed (Mbps): 1000.0
- FIPS Mode: Disabled
- Media: Wired
- Adapter: Intel(R) 82578DC Gigabit Network Connection

Security Information:

- Configuration: 802.1X
- Encryption: None
- EAP Method: eapFast(eapMschapv2)
- Server:
- Credential Type: Username/Password

Bytes:

- Sent: 920688
- Received: 10258160

Frames:

- Sent: 14126
- Received: 139884

On the right side of the interface, there is a "Host Name:" field with the value "NILE12". Below it, the "IP Address:" is "10.1.204.150", "Network Speed:" is "1 Gb/s", and "PortID:" is "GigabitEthernet3/1". Other fields include "SwitchName:" "6506-2-airbus", "Image:" "FEB 8, 2011", "OS Version:" "Windows XP", and "Service Pack:" "Service Pack 3".

The bottom of the screenshot shows the Windows taskbar with the Start button, several application icons, and the system tray showing the time as 3:30 PM. A small "Cisco Systems" logo is visible in the bottom right corner of the interface.

Driving Simplicity: Data Center Design – Resources from Cisco



Validated Design Guides

Design Zone

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.

Cisco Validated Designs for the DC

- CVD > SAFE

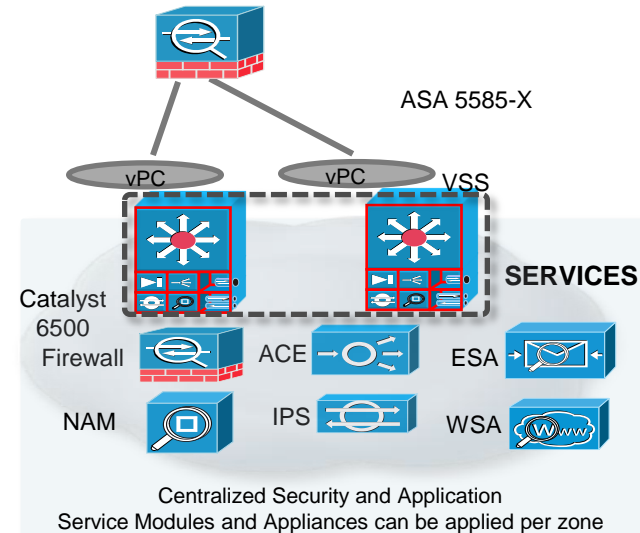
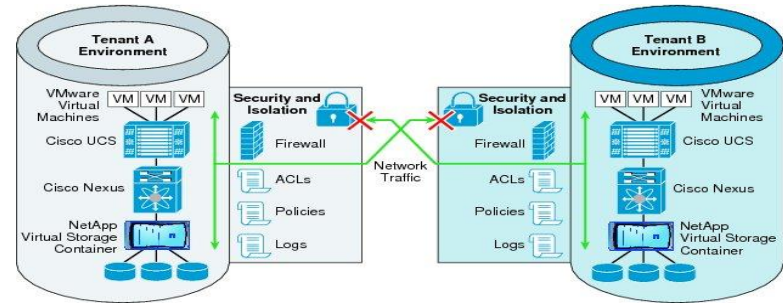
- http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg.pdf

- CVD >Virtualized Multi-Tenant Data Center (VMDC)

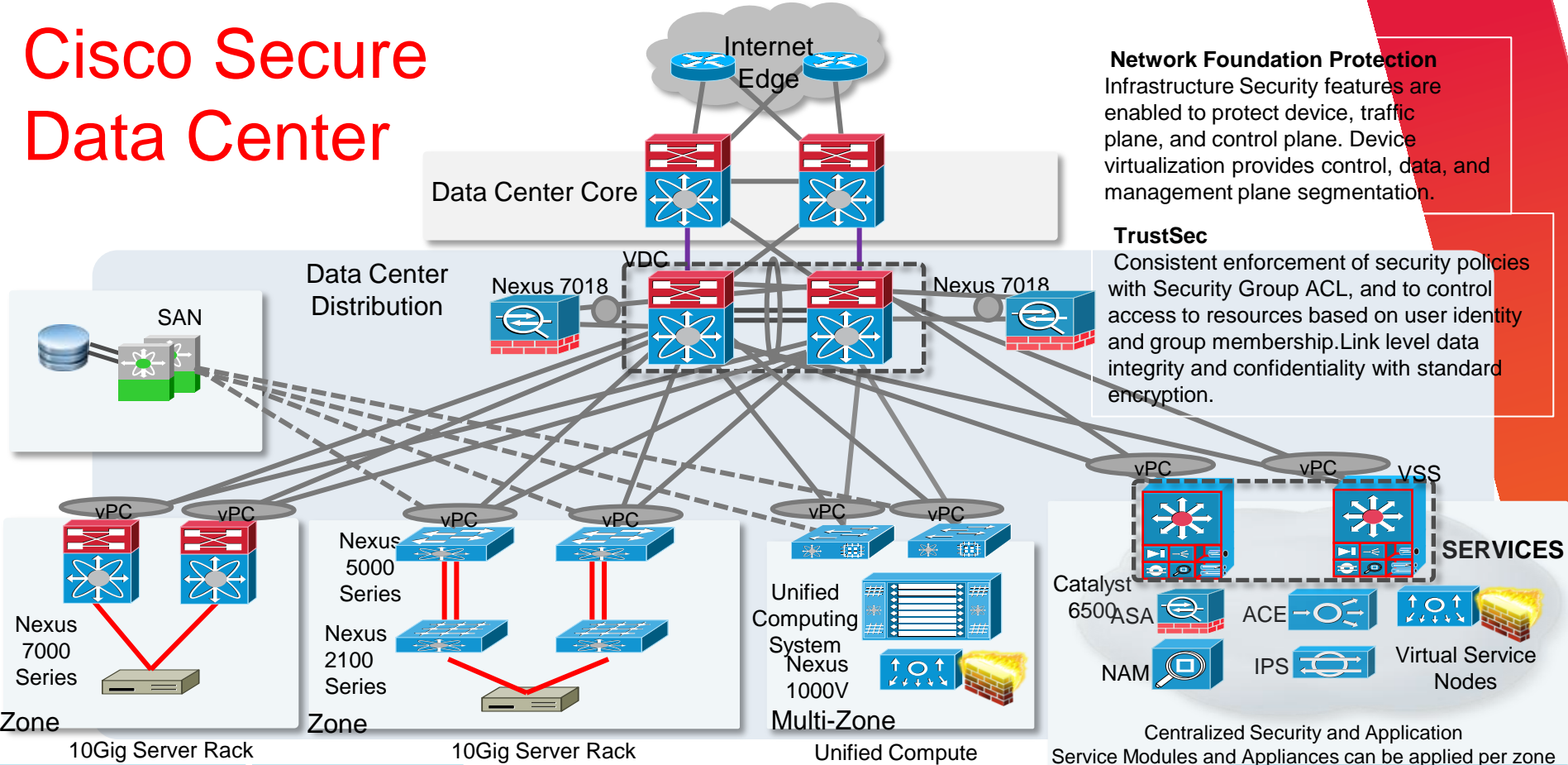
- http://www.cisco.com/en/US/partner/docs/solutions/Enterprise/Data_Center/VMDC/1.1/design.html

- CVD > Secure Multi Tenant CVD

- http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns743/ns1050/landing_dcVDDC.html



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

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

Q&A



We value your feedback.

Please be sure to complete the Evaluation Form for this session.



Access today's presentations at cisco.com/ca/plus



Follow [@CiscoCanada](https://twitter.com/CiscoCanada) and join the [#CiscoPlusCA](https://twitter.com/CiscoCanada) conversation