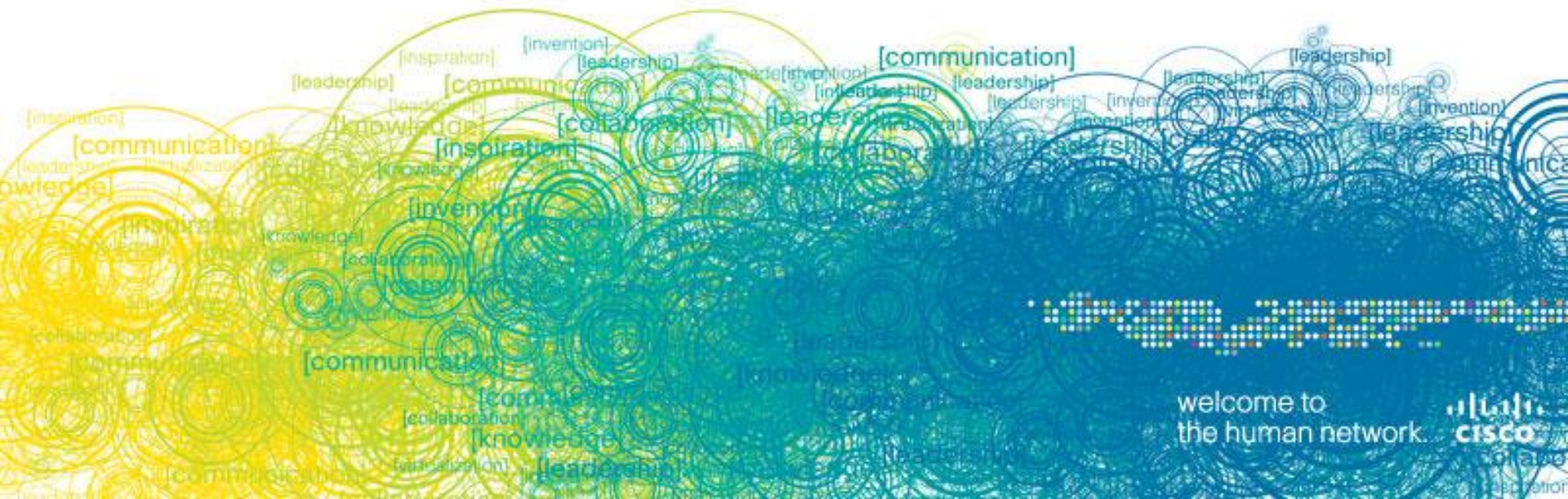


Security and Virtualization in the Data Center



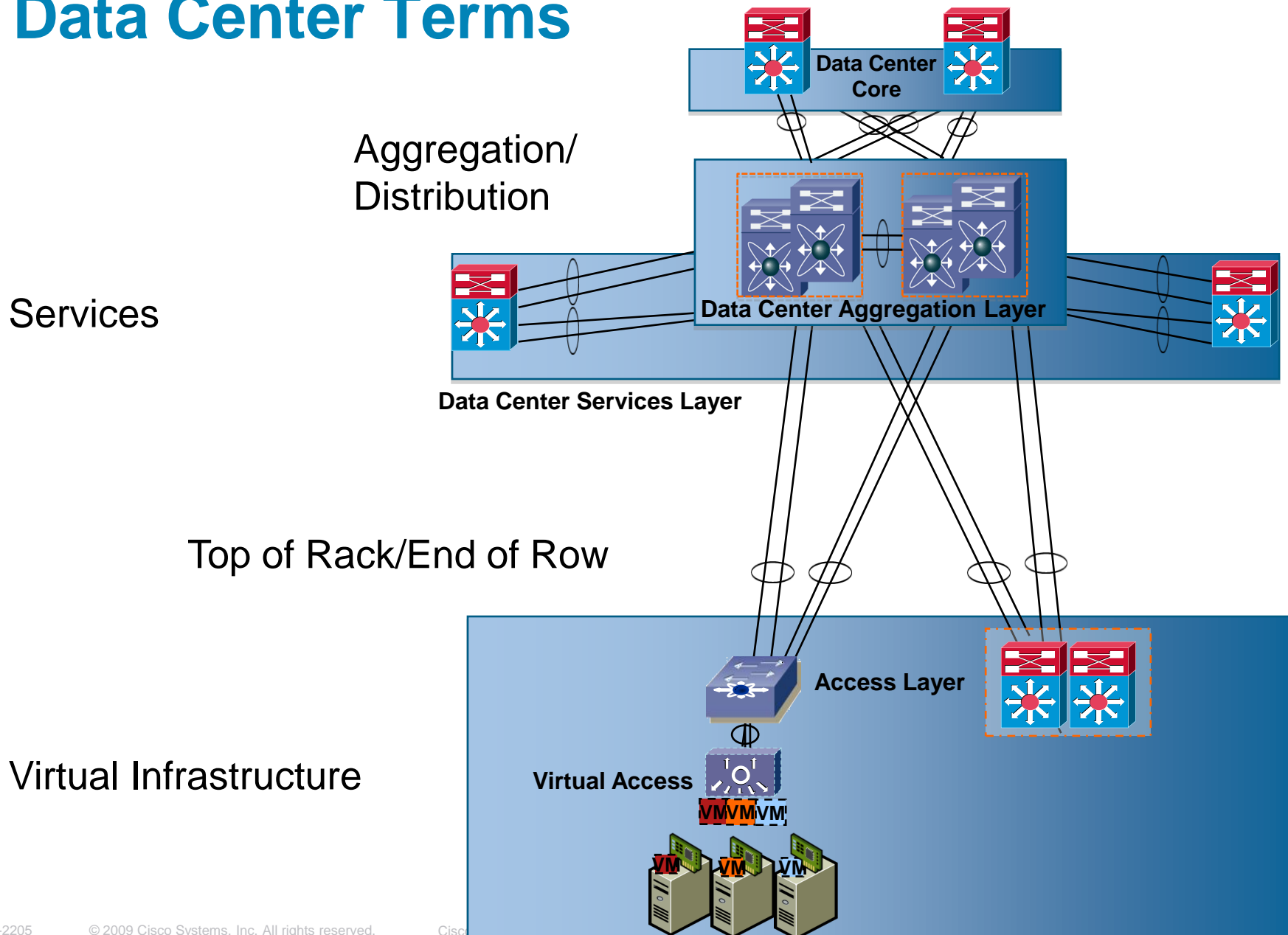
What We'll Cover

- Areas of Interest
- Security for Data Center Layers
- Device Virtualization & Security Services
- Security Considerations for Server Virtualization

Where Are We Now?

- Securing virtualized environments is a big concern
- We are still early in virtualization adoption
- Two forms of virtualization we are discussing. Both apply to the Data Center
 - Server virtualization
 - Device virtualization
- Security requirements shouldn't change with virtualization

Data Center Terms



Data Center Security Challenges

- Virtualization
- Applications
- Data Loss
- Compliance
- Availability

Addressing the Challenges

Stateful Packet Filtering

Initial filter for all DC ingress and egress traffic. Virtual Context allow correlation to Nexus VDC.



Stateful Packet Filtering

Additional Firewall Services for Server Farm specific protection



Server Load Balancing

Server Load Balancing masks servers and applications



Application Firewall

Application Firewall mitigates XSS, HTTP, SQL, XML based attacks

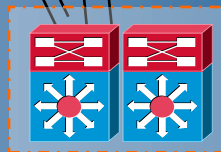
Enhanced Layer 2 Security

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

Virtual Access



Access Layer



Layer 2 Flow Monitoring

NetFlow, ERSPAN, SPAN

Endpoint security

Host intrusion prevention protect server against zero day attacks



Data Center Core

Data Center Aggregation Layer

Data Center Services Layer

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

Network Intrusion Prevention

IPS/IDS: provides traffic analysis and forensics

Flow Based Traffic Analysis

Network Analysis for traffic monitoring and data analysis

XML based Application Control

XML Gateway to protect and optimize Web-based services

Security Management

- Visibility
- Even Correlation
- Forensics
- Anomaly Detection
- Compliance

CS-MARS



CSM



BRKSEC-2205

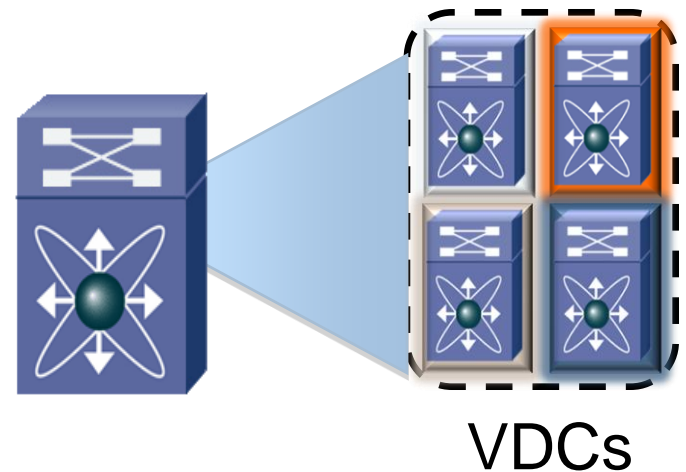
© 2009 Cisco

Data Center: Aggregation

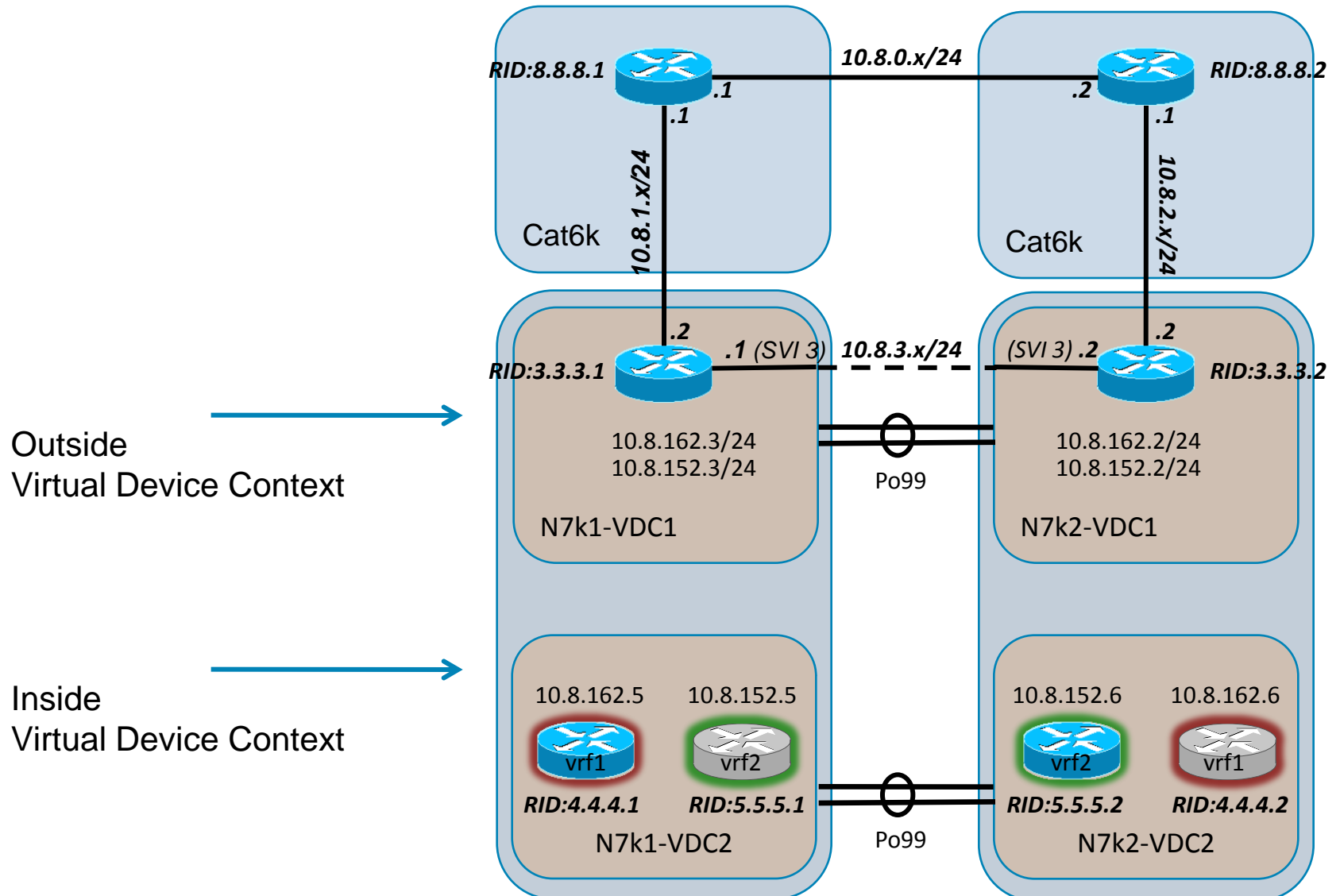


Device Virtualization: Nexus 7000 Virtual Device Contexts

- Up to 4 separate virtual switches from a single physical chassis with common supervisor module(s)
- Separate control plane instances and management/CLI for each virtual switch
- Interfaces only belong to one of the active VDCs in the chassis, external connectivity required to pass traffic between VDCs of the same switch

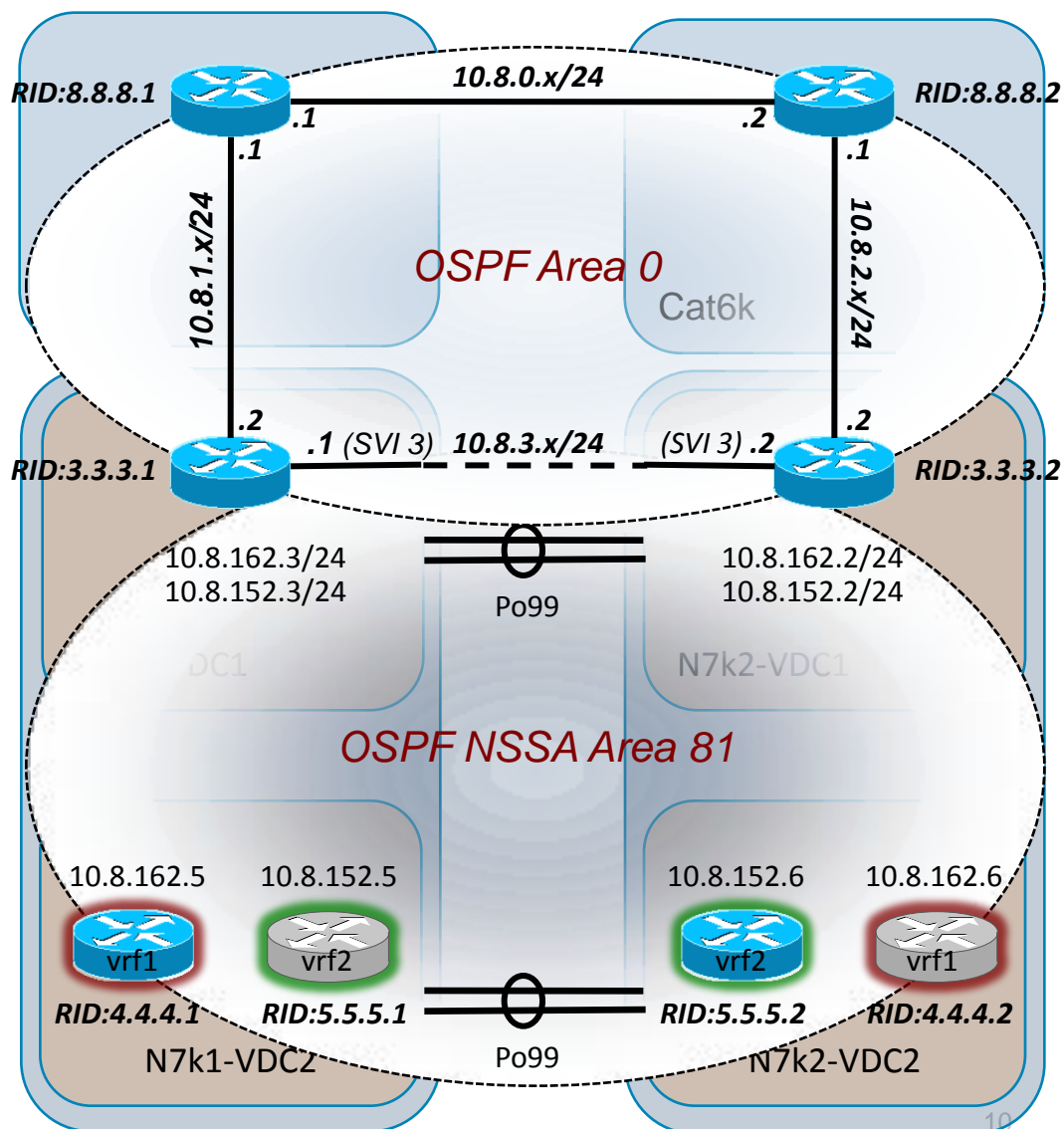


Aggregation Layer with VDCs



Control and Segmentation

- Control Routing Propagation
- Example: inject only default route to internal VDC
- Traffic between VDCs must be routed or bridged via external
- Access controlled to inside and outside contexts



Aggregation Security Features

- CoPP

Protect the supervisor from DoS attacks preventing outages. Prevent Layer 2 broadcast storms and irrelevant traffic redirections to CPU

- Broadcast Suppression

Protects the data center against broadcast storms at the port level that pose risks to bandwidth availability

- Packet Sanity Checks

Forwarding engine performs extensive checks on IPv4 and IPv6 packet headers to protect the network from illegal packets.

- LinkSec

Wire-rate link-layer cryptography is provided at all ports. Packets are encrypted on egress and decrypted on ingress so they are clear inside the device.

Additional Nexus 7000 Tidbits

- Virtualization support

AAA configuration and operation are local to the VDC.

AAA authentication methods for the console login only apply to the default VDC.

AAA accounting log is on per VDC basis

- Role Based Access

Four default roles

Network-admin

Permission to create/delete/assign resources to VDC.

Can create other roles and users.

Network-operator

Permission to run show command across all VDCs.

VDC-admin

Permission to manage a VDC, create other VDC roles and users for that VDC.

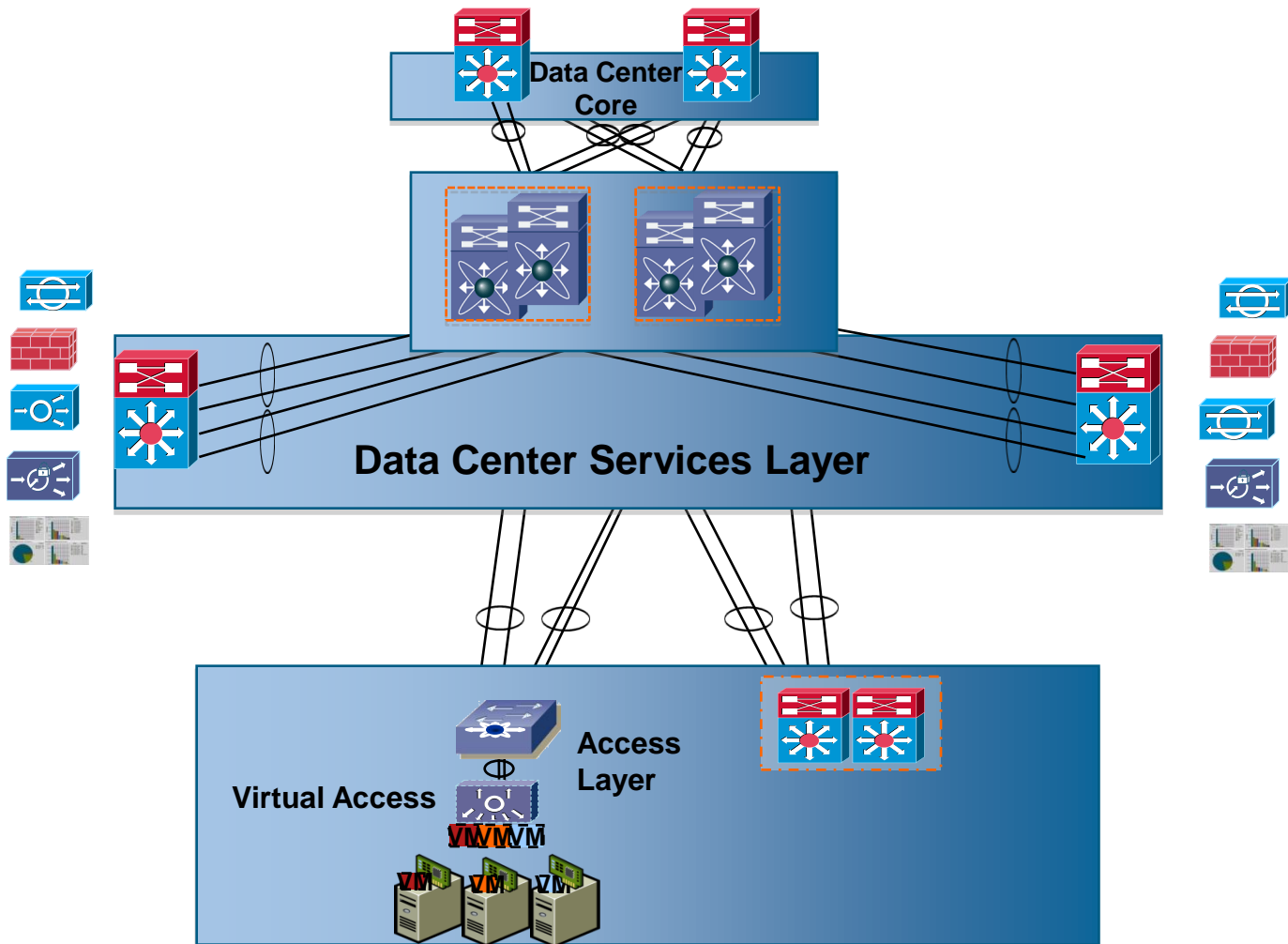
VDC-operator

Local to a VDC and has show command privilege

Data Center: Security Services (and Others)



Security Services



Security Service Integration

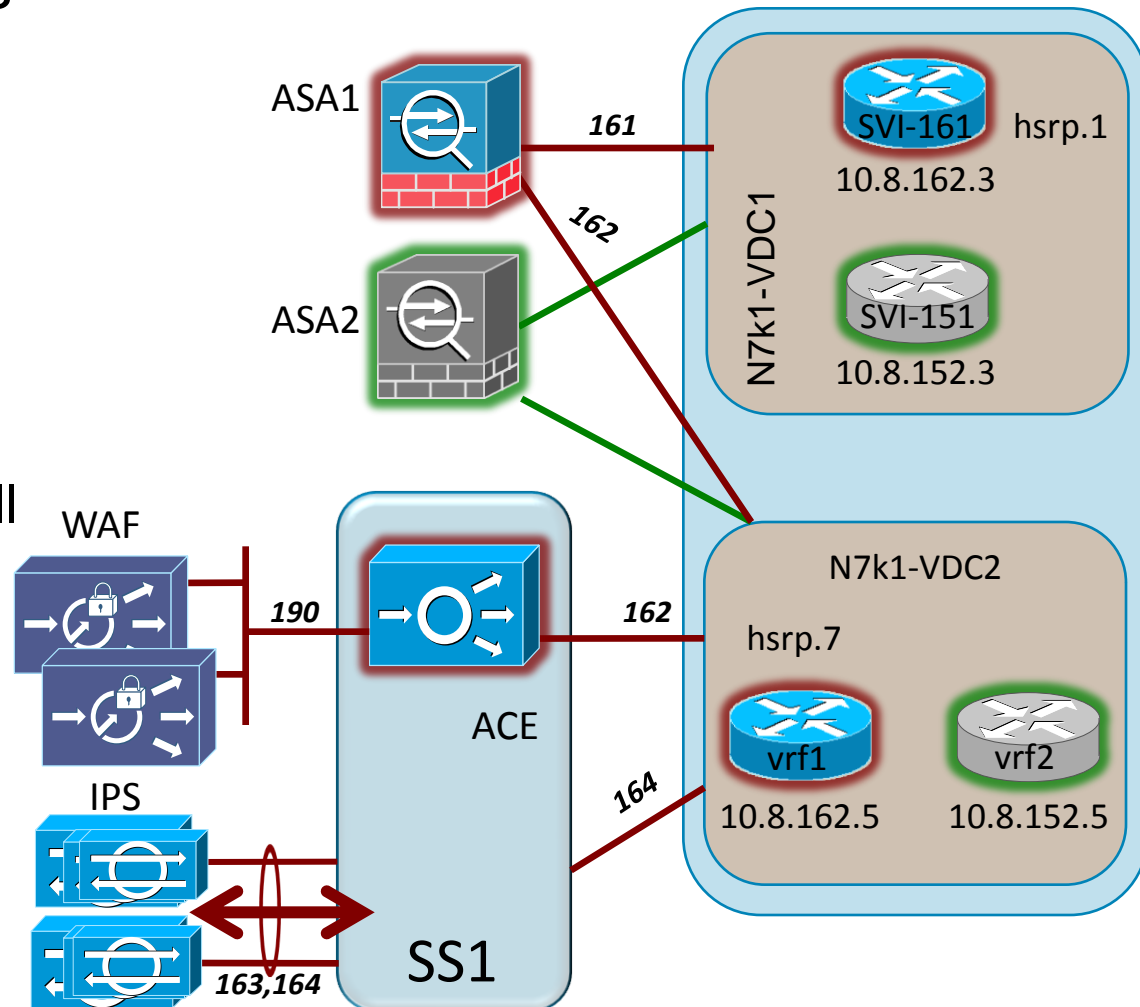
- Deploy security services and appliances as transparently as possible.
 - Maintain predictable traffic flows to ensure availability
 - Need to think about scalability of current infrastructure when planning designs.
- Create Security Zones based on Trust
- Minimal impact to allowed functions while maintaining
 - Enforcement, Isolation, Visibility
- Business model, compliance, applications, can all drive policy
- One model does not fit all but there are some design guidelines we can provide



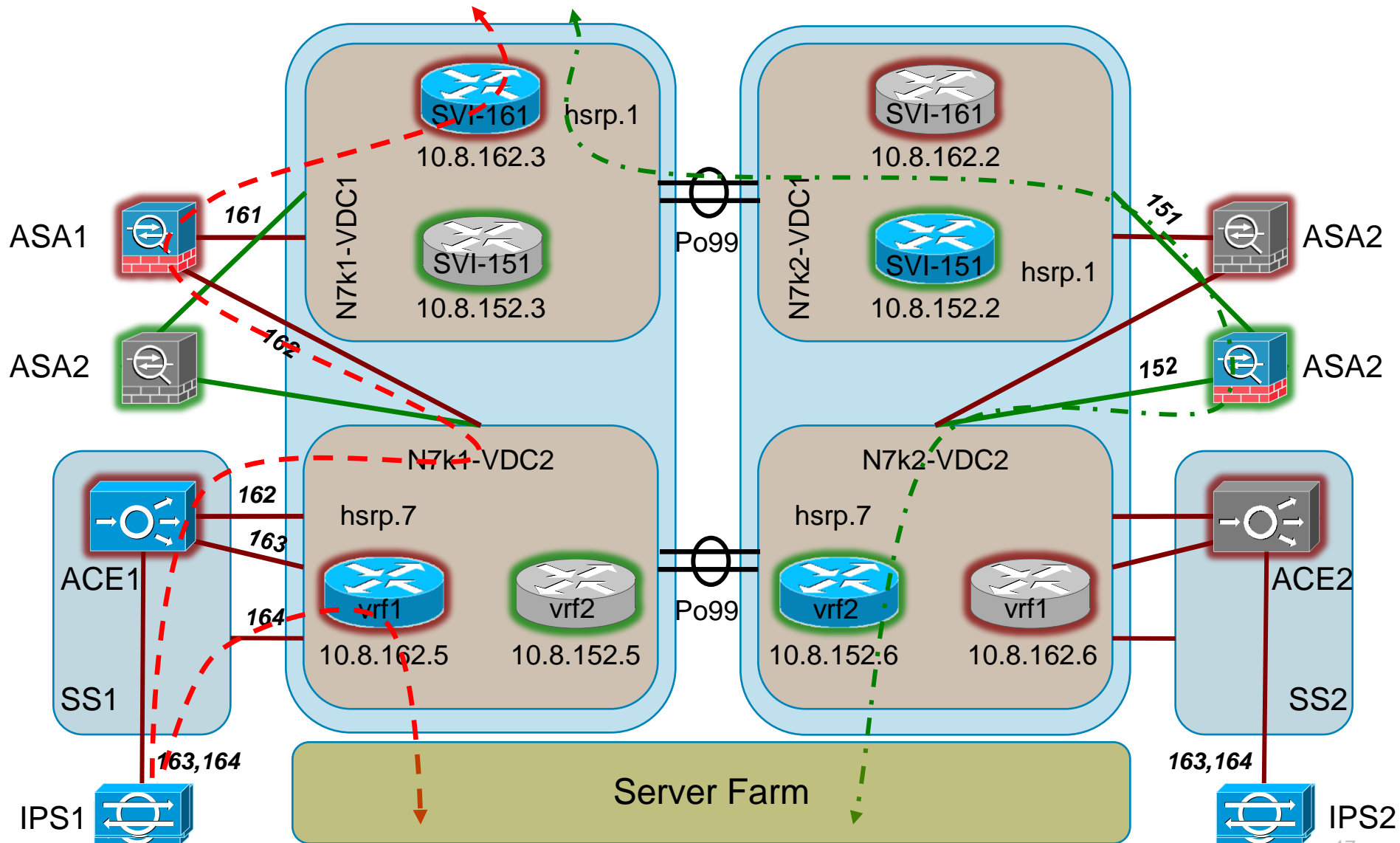
Security Services

Transparent Services Are “Sandwiched” between Nexus VDCs

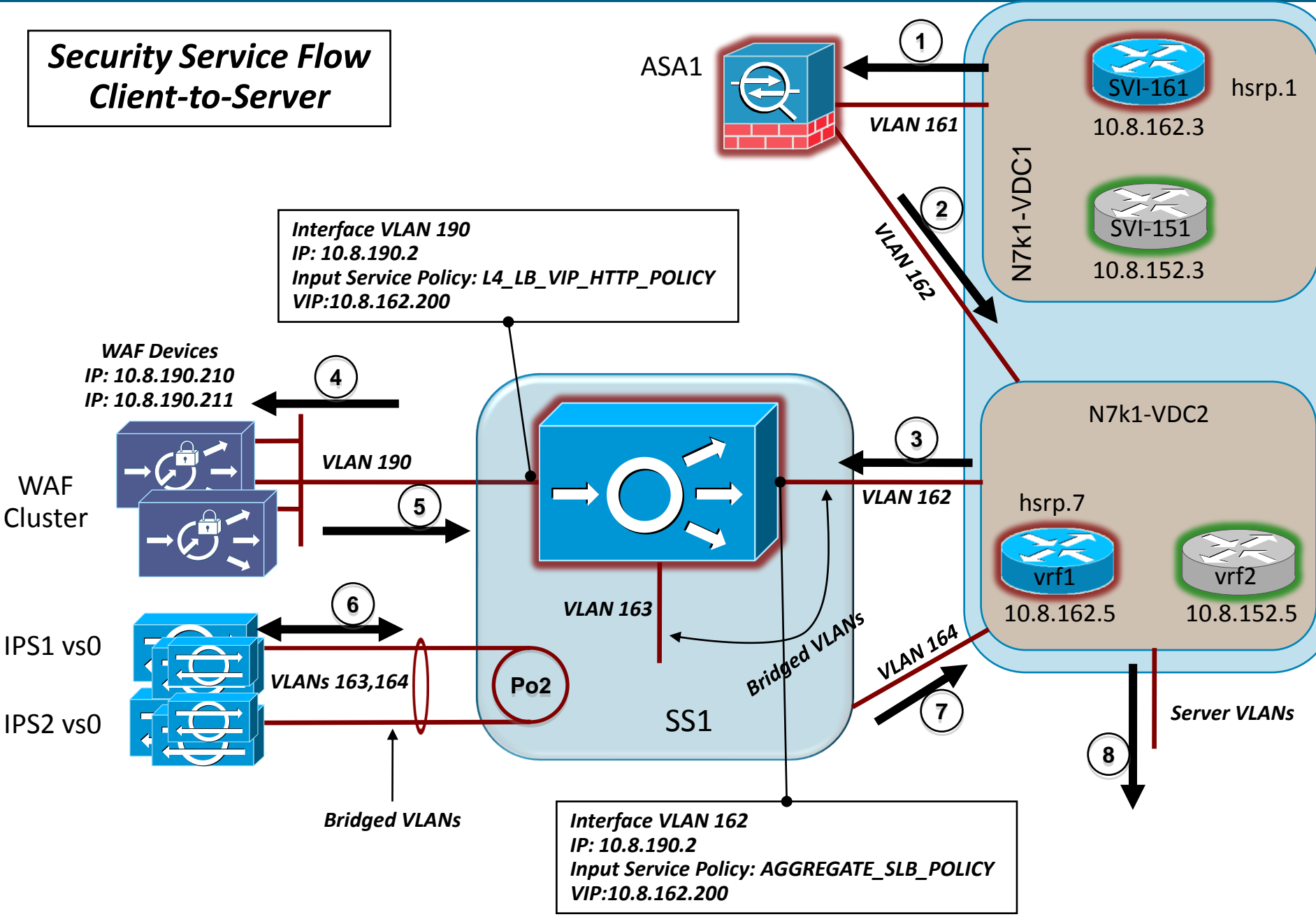
- ASA Stateful Firewall
 - Virtual Contexts
 - Transparent mode
- ACE LB
 - Transparent mode
- Web Application Firewall
 - Firewall farm
- Network IPS/IDS
 - Inline or promiscuous



Traffic Flows



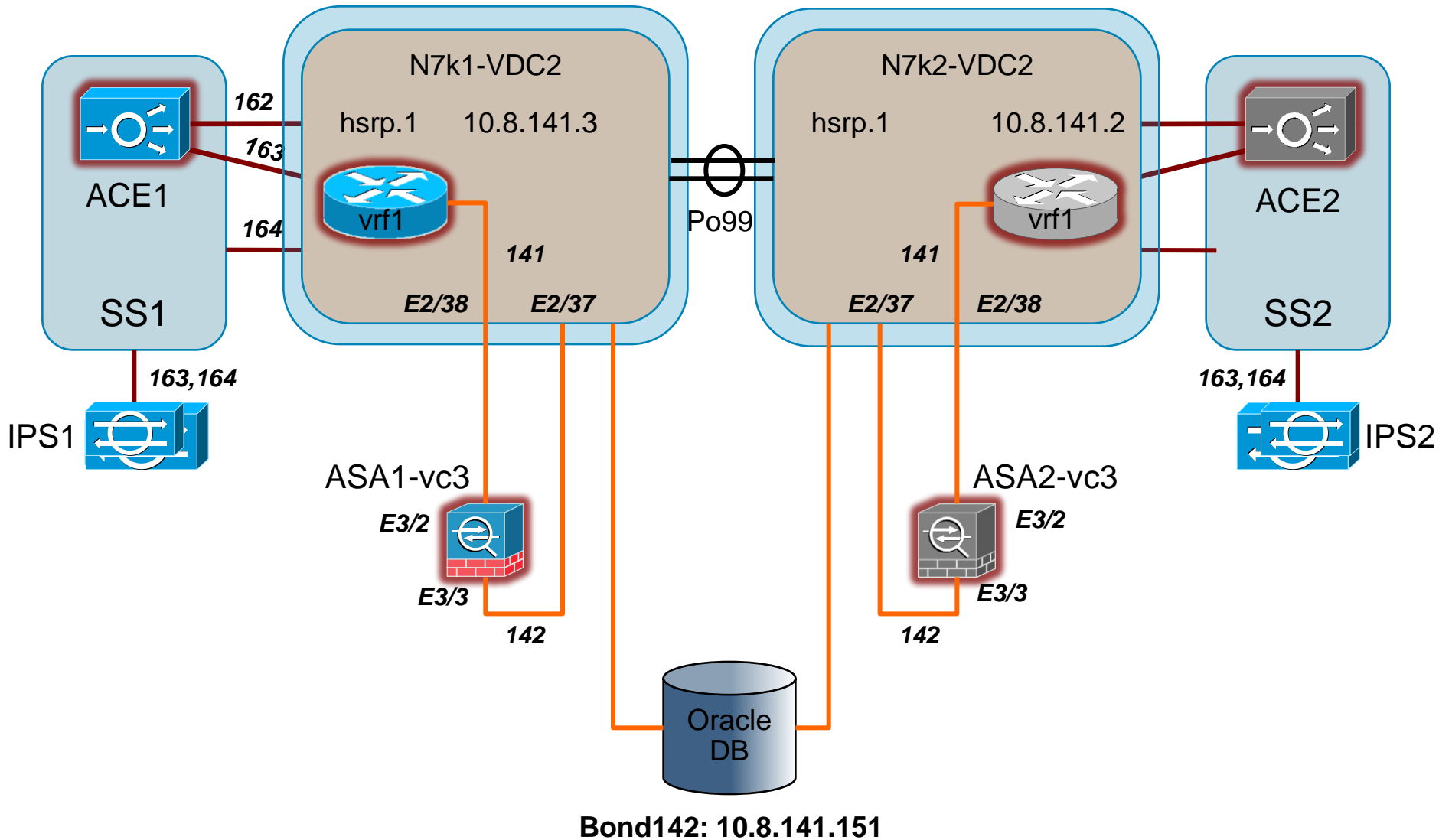
Security Service Flow Client-to-Server



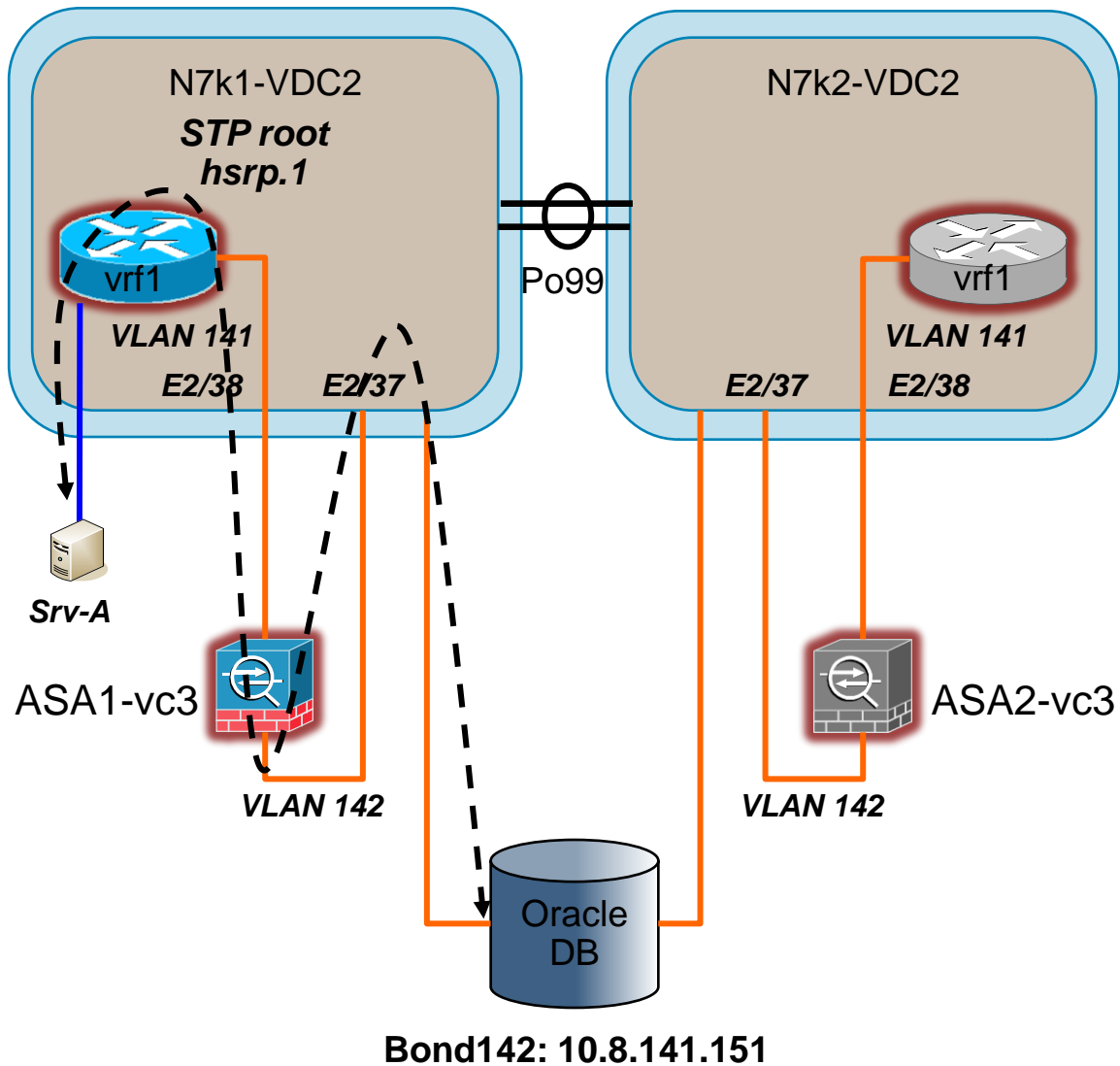
Examples



Virtual Context on ASA for ORACLE DB Protection



Example of Server to Database access through virtual firewall context.



Using ACE and WAF to Maintain Real Client IP Address as Source in Server Logs

The image shows two screenshots of the Cisco ACE Web Application Firewall Manager interface. The top screenshot shows the 'Profiles' page, and the bottom screenshot shows the 'HTTP Header Processing' configuration page for the 'myClientInsert' profile.

Top Screenshot: Profiles

Subpolicy: **Shared**

Manager Dashboard

Policy

- HTTP Ports & Hostnames
- Destination HTTP Servers
- Virtual Web Applications
 - Profiles** >>
 - Rules & Signatures
- Policy Management
 - Subpolicies

Profiles

New Profile...

Profile	Description
myClientInsert	This policy inserts the originating IP address
Pass-through Profile [Built-In]	The default profile designed to pass through all traffic.
PCI Compliance [Built-In]	A Profile with all inspection rules enabled.

Bottom Screenshot: Profiles > myClientInsert > HTTP Header Processing

Subpolicy: **Shared**

Manager Dashboard

Policy

- HTTP Ports & Hostnames
- Destination HTTP Servers
- Virtual Web Applications
 - Profiles** >>
 - Rules & Signatures
- Policy Management
 - Subpolicies

Resources

- Public/Private Keypairs
- Trusted Certificate Authorities
- Remote Server Certificates

Reports & Tools

- Web App Firewall Incidents
- Event Log
- Performance Monitor

Profiles > myClientInsert > HTTP Header Processing

HTTP headers will be passed through unless otherwise specified below.

REQUEST HEADERS

- Insert "X-Forwarded-For" header with client's IP address
- Insert Client SSL Certificate DN in header named if the header does not a
- Rewrite "Host" header with destination server hostname

Custom Header Processing

RESPONSE HEADERS

- Replace "Server" header value with

Custom Header Processing

Server Logging

- Session persistence maybe maintained via HTTP header insertion
- ACE LB and Web Application Firewall support this functionality

Virtual Web Applications > [www](#) > Crack Me

Crack Me



Virtual URL: http://*:81/ (prefix)

Destination: http://10.8.162.200

Firewall Profile: [myClientInsert](#)

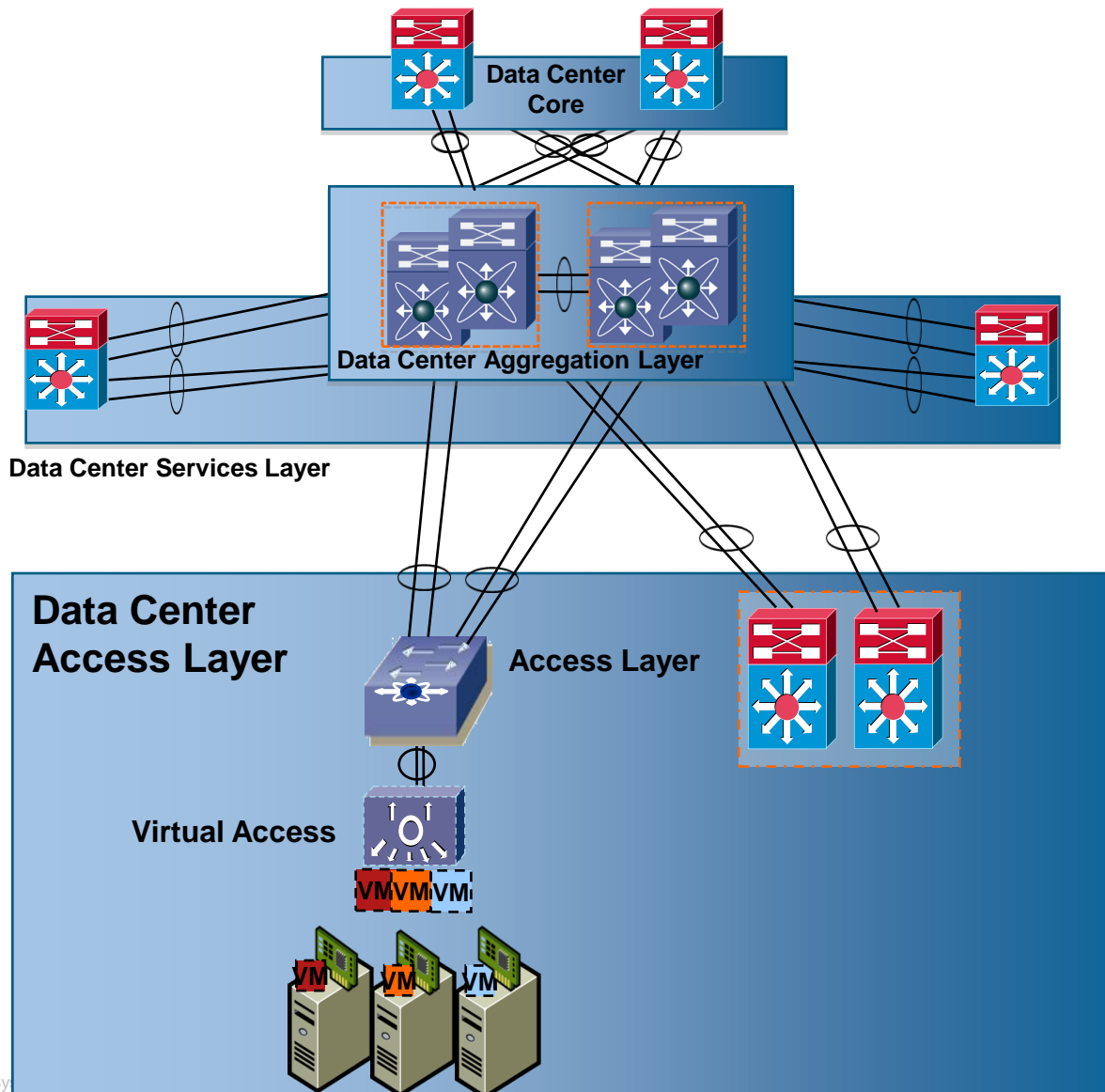
Firewall Modifiers - no modifiers configured

```
Stream Content
GET /kelev/view/home.php HTTP/1.1
Connection: keep-alive
ACEForwarded: 10.7.54.34
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/xaml+xml,
application/vnd.ms-xpsdocument, application/x-ms-xbap, application/x-ms-application,
application/x-shockwave-flash, */*
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.2; EmbeddedWB 14.52 from:
http://www.bsalsa.com/ EmbeddedWB 14.52; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.30; .NET CLR 3.0.04506.648)
Host: 10.8.162.200
Cookie: wafcookie=R2632847463; bankcookie=R2070880508
X-Forwarded-For: 10.7.54.34
```

Access Layer



Data Center Access



Security Considerations

- In many cases server tiers/clusters are separated by VLANs
- Servers are often Layer 2 adjacent
- Must allow for mobility
 - DR
 - Maintenance
- Security is key in maintaining availability of servers and applications connected here.

Make Use of Switch Security Features

- Anti-spoofing features

 - Dynamic ARP Inspection, IP Source Guard, DHCP Snooping

- STP protection (BPDU Guard)

- QoS

- Broadcast Packet Suppression

- PVLANs

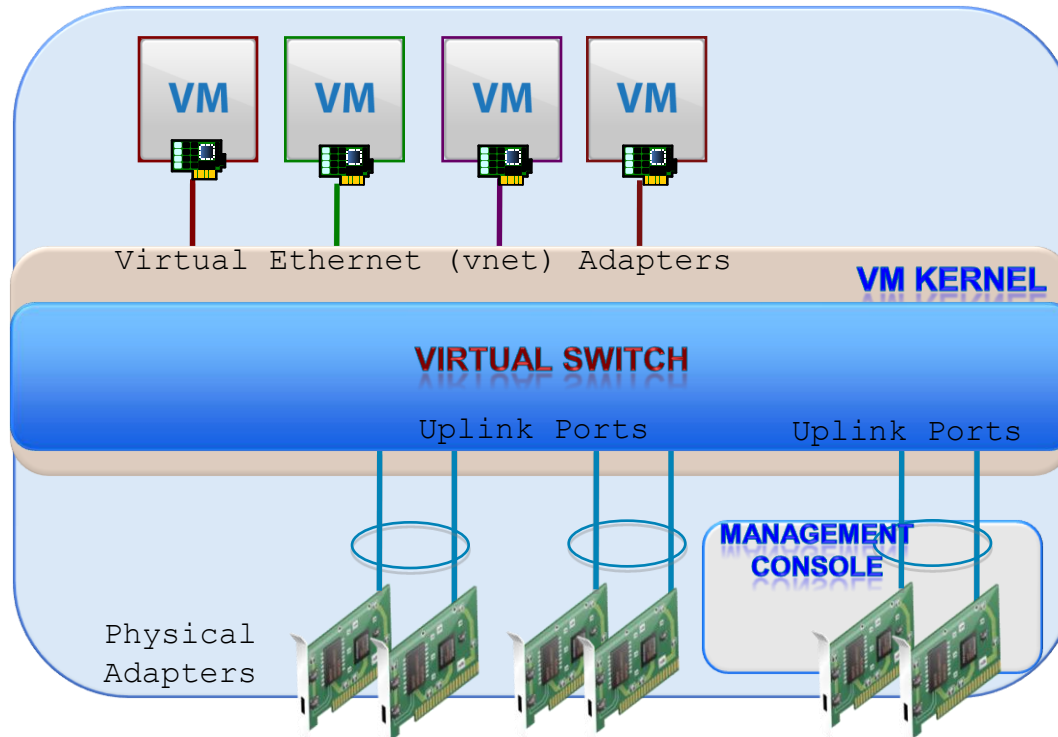
- Access Lists

- SPAN, ERSPAN, NetFlow

Virtual Access and Security



Server Virtualization



Benefits of Virtualization

- Power savings
- Consolidation of resources
- Server portability
- Application failover

Server Virtualization

- Hypervisors: Type 1 or Type 2

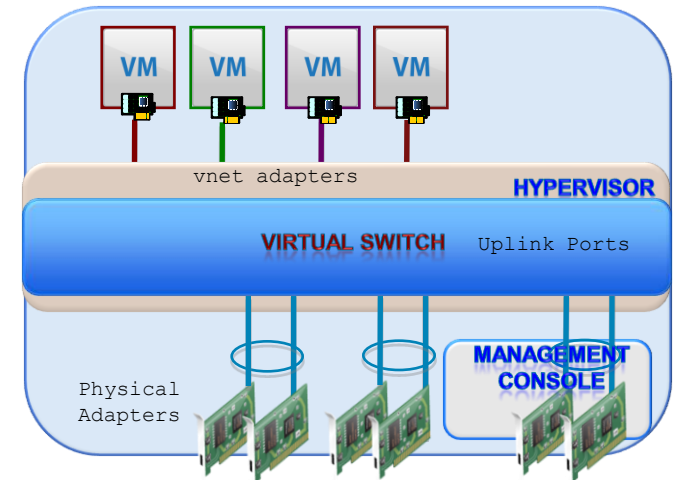
Type 1 hypervisors as shown below are built into a pre-hardened host. There is no distinct boundary between the host operating system and the hypervisor.

Type 2 hypervisors as shown below are installed as separate software on top of the existing host operating system

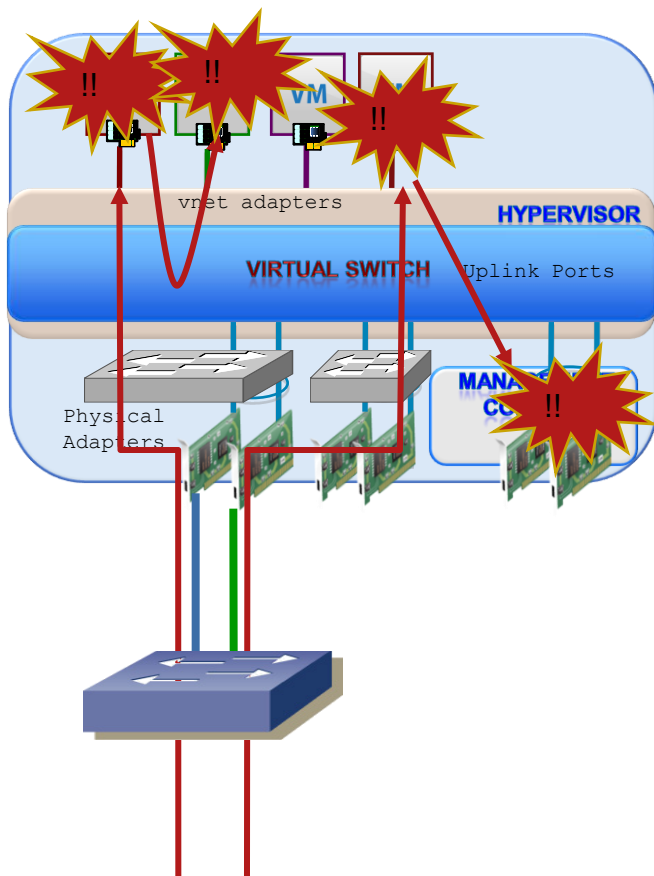
- Primary role of the host OS or hypervisor is to work with the VMM to coordinate access to the physical host system's hardware resources (CPU, Device Drivers, etc)
- Theoretically the hypervisor should have fewer security vulnerabilities because it runs minimal services and contains only essential code BUT maintaining security updates is still important!

Server Virtualization Security Concerns

- **Secure Hypervisor**
 - Mitigate risk towards the hypervisor
 - an attacker gaining unauthorized access to the hypervisor and taking control of the physical server and related virtual servers
- **Rogue VMs**
 - Has a guest operating system been compromised?
 - Virtual Server Mobility
- **Inter-VM traffic visibility and security**
 - Traffic between two virtual machines can flow across the bus inside the hosting physical server and not be required to be switched on an external network where traditional tools can be used
 - VMware “virtual switch” lacks security features available in Cisco switching platforms
- **Shared File system between VMs**
 - VMFS and VMotion
 - Consolidated SANs or NAS attached storage

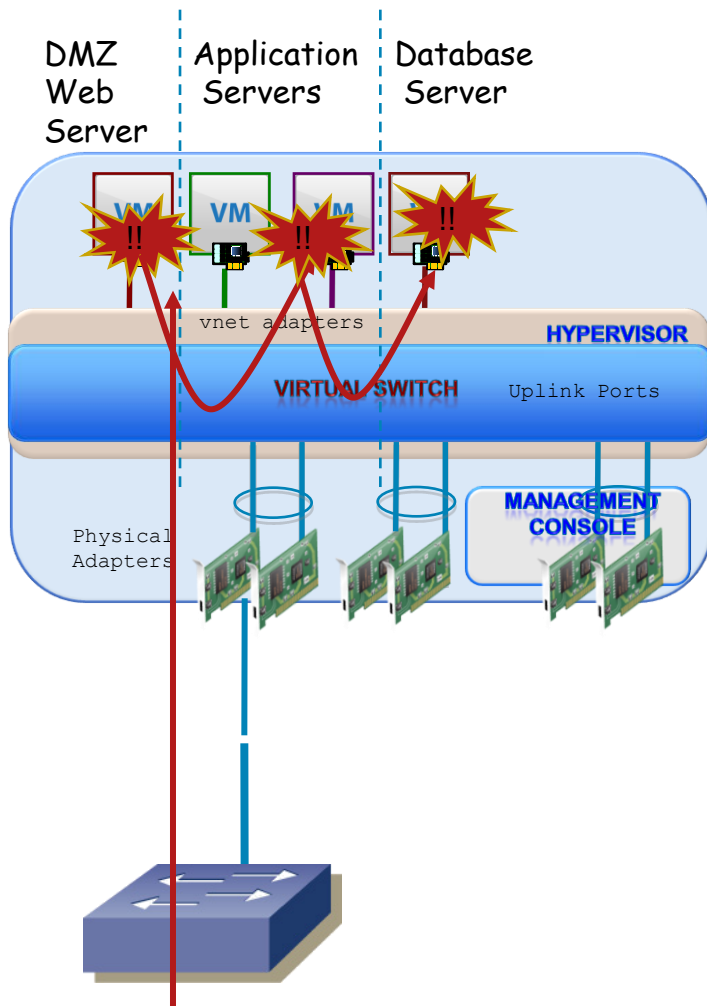


Securing the Hypervisor...



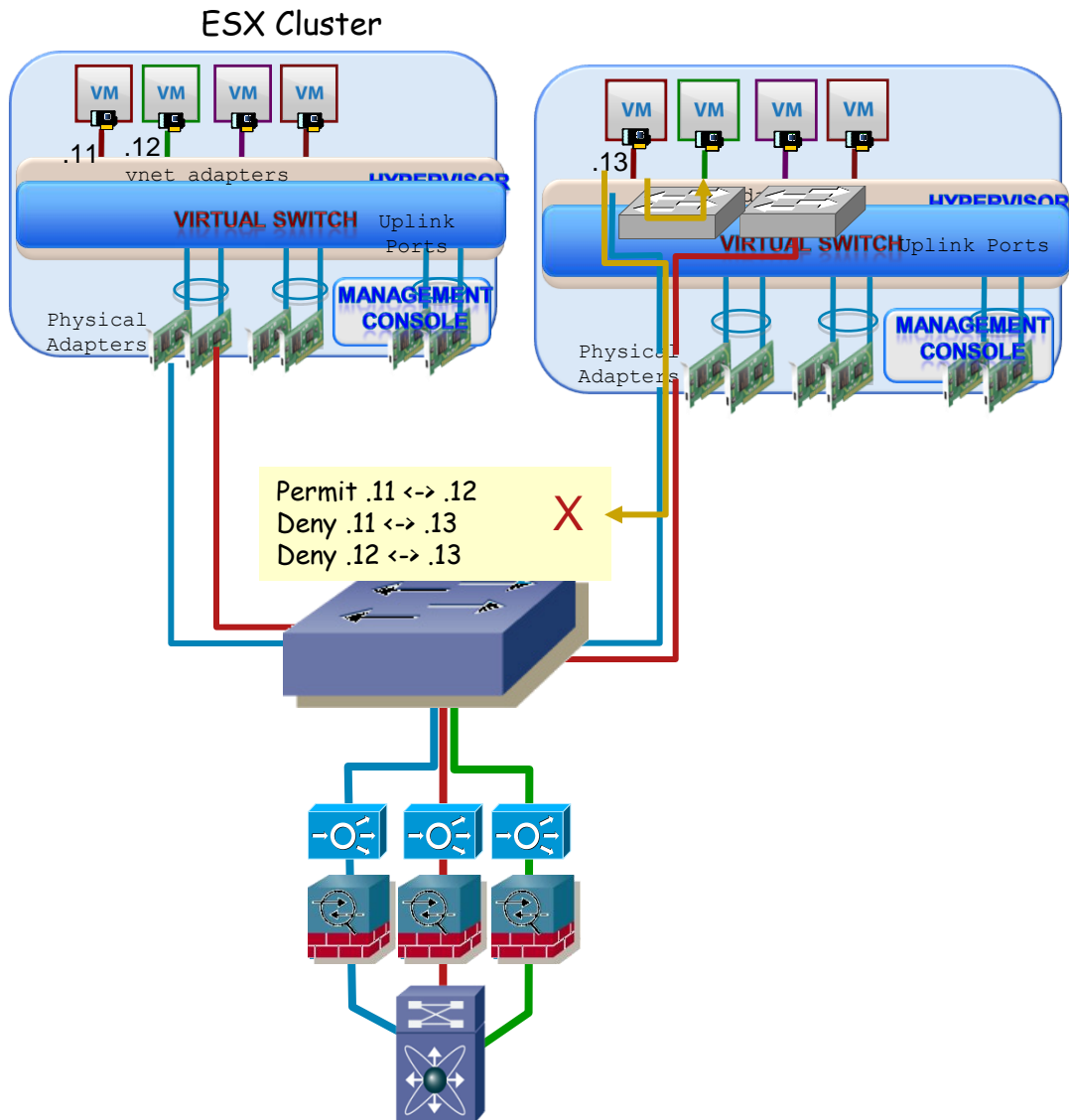
- **Hypervisor** has access to all resources
 - Manages all system resources
 - Manages LAN & SAN access
- **vSwitch** lacks “standard” network functions
 - No visibility into VM-to-VM traffic on a port group
 - No visibility into VM-to-Hypervisor calls

Virtual Machine LAN Security



- Be aware of **security affinities**
Would you place all your applications on the same VLAN?
- Challenging **troubleshooting & monitoring** environment
- **Recommendation**: Do not consolidate servers with unlike security affinities onto a single VLAN

Virtual Machine VMotion Security



- VMotion enables **workload mobility & Disaster Recovery**
- Increases **server utilization efficiency** by balancing workloads between servers
- VMs can move between ESX cluster members with the **same configuration**
 - Port-groups, VLANs, etc
- Inconsistent security policies enforcement and visibility
 - Policies applied at the server port or VLAN cannot be consistently applied
- Vmotion traffic sent in clear text. Take precautions for isolating

Virtual Machine Exploits

- Several Theoretical Exploits
 - Gain Control of the Hypervisor
 - Exploiting vMotion
- Reconnaissance: Virtual Machine Detection
 - VME artifacts
 - Malware that detects virtual machines
 - Tools: (The Red Pill, Scoopy & Doo, VMDetect, etc)
 - Virtual machine-based root kits

Theoretical attacks are interesting but lets focus on the simple things that cover 99% of the issues. Most people don't even have the simple items covered!

Lets worry about this before we worry about theoretical Hypervisor attacks.



Things to Ponder...

- Traditional Security Problems Unchanged
- Security Policies still need to be enforced
- Virtualization introduces some new flavors
 - Hypervisor is a new layer of privileged software
 - Potential loss of separation of duties
 - Limited visibility into inter-VM traffic
- So What's the Secret Ingredient?



There Is NO Secret Ingredient!



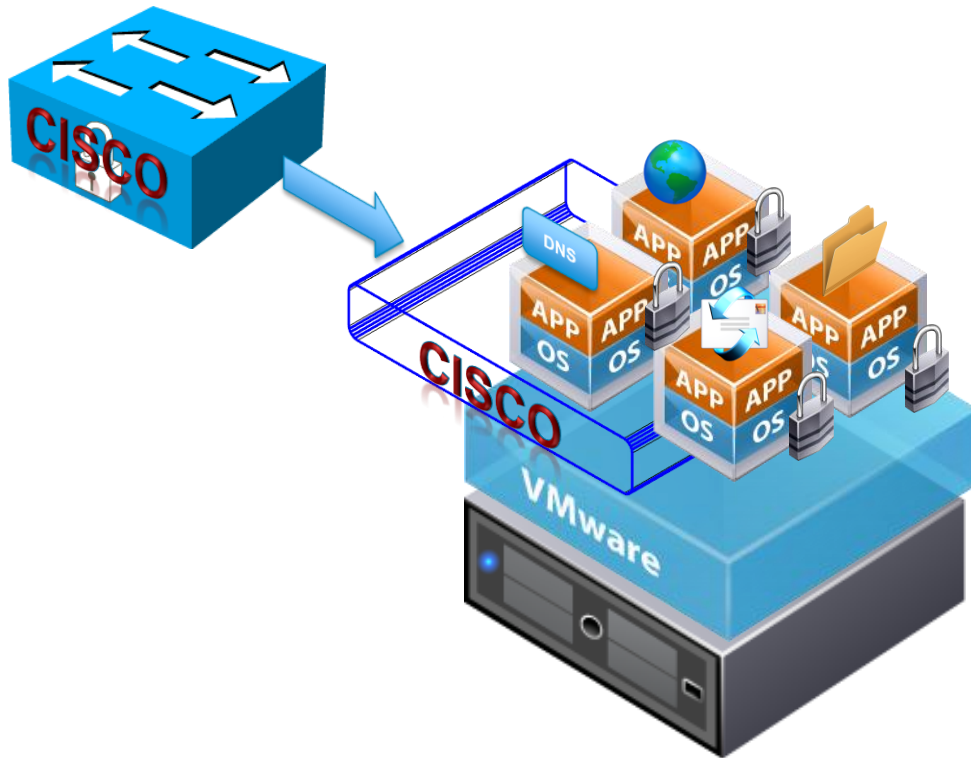
Security best practices still apply!

If you would not do it on a non-virtualized server, you probably should not do it on a virtualized server.

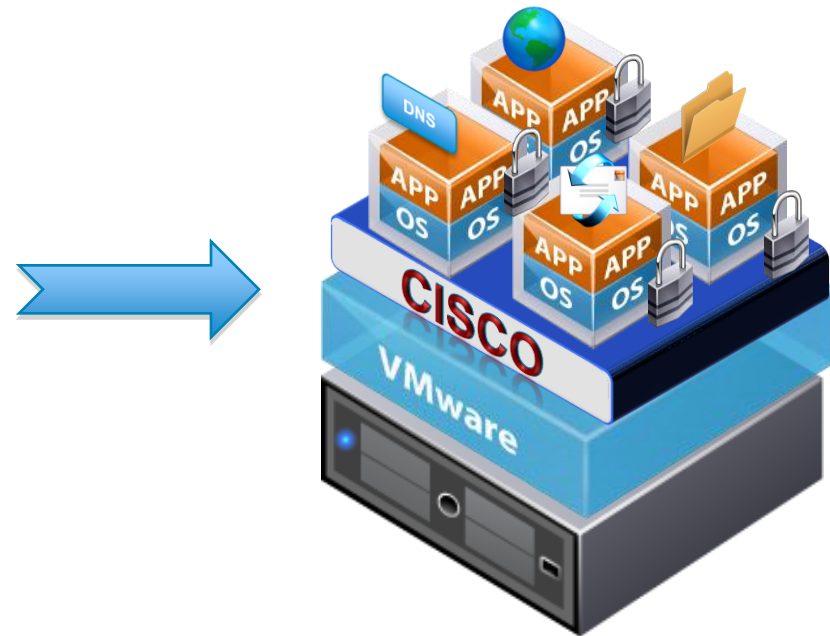
But we can address the virtualization concerns...

Merging Physical to Virtual Infrastructure

Physical Access Switch



Integrated Nexus 1000V Virtual Switch

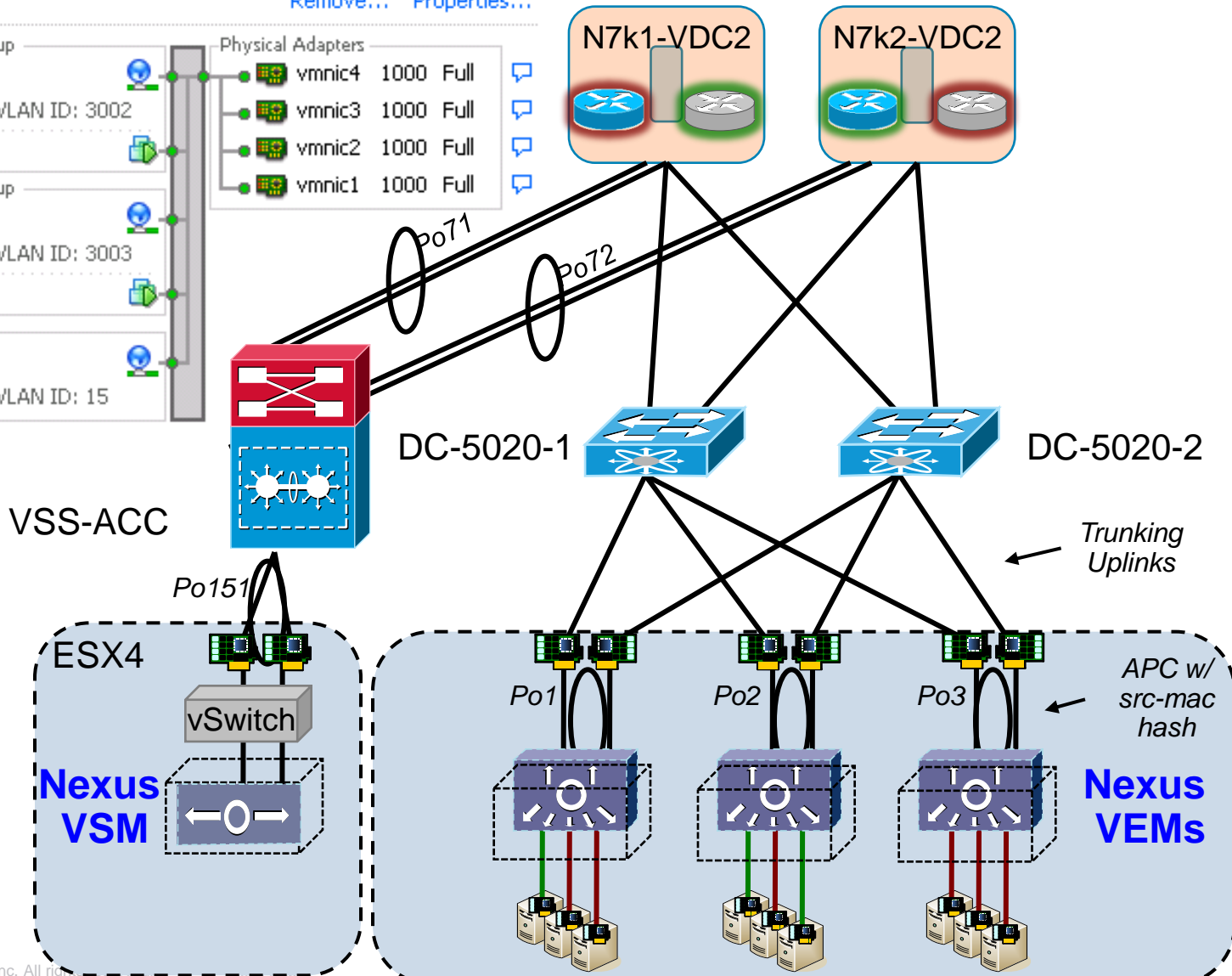


Virtual Access Fabric: Nexus 1000V

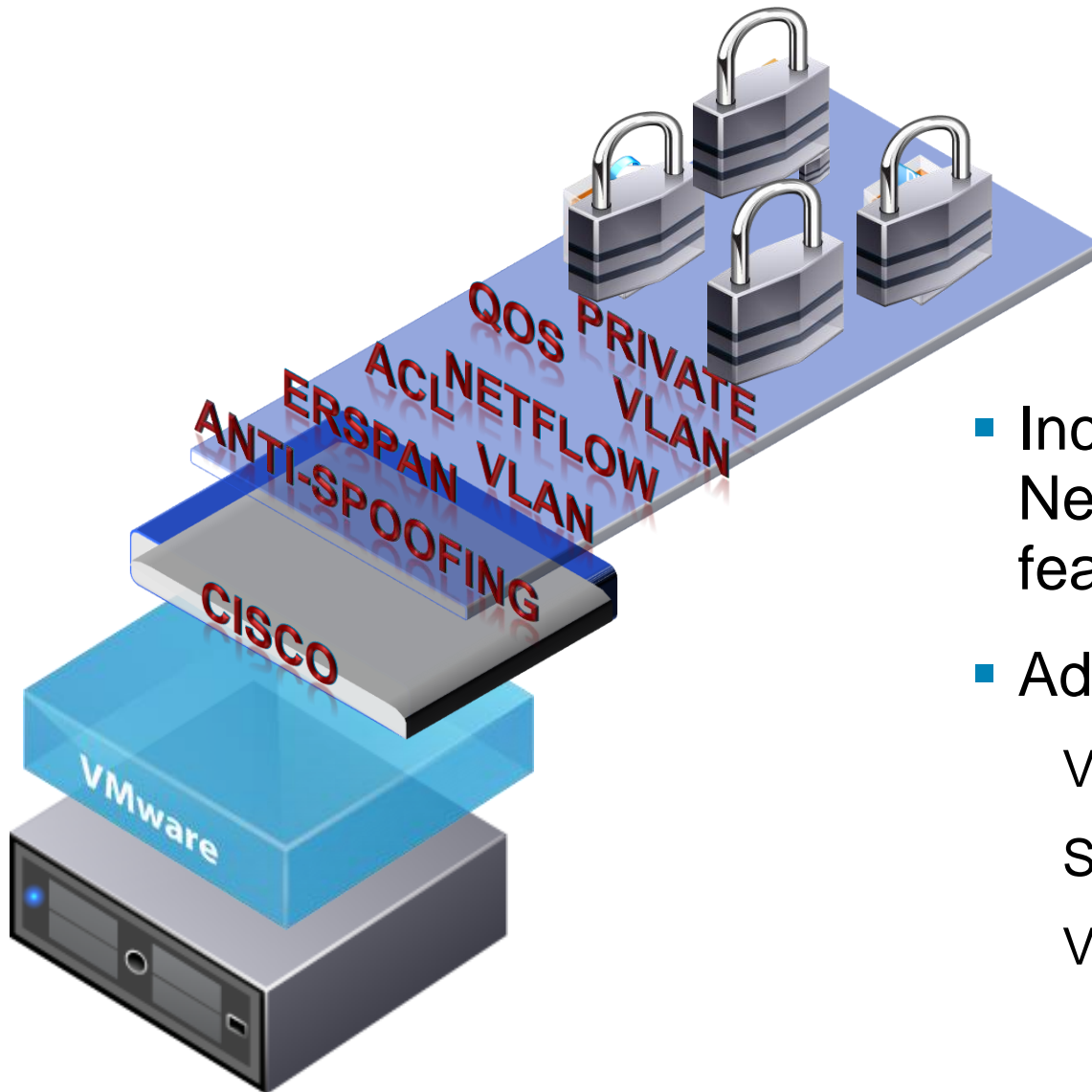
Virtual Switch: vSwitch0

Remove... Properties...

Virtual Machine Port Group		Physical Adapters	
vmcontrol	1 virtual machine(s) VLAN ID: 3002	vmnic4	1000 Full
VSM		vmnic3	1000 Full
Virtual Machine Port Group		vmnic2	1000 Full
vempacket	1 virtual machine(s) VLAN ID: 3003	vmnic1	1000 Full
VSM			
VMkernel Port			
VMkernel	vmk0 : 10.8.15.153 VLAN ID: 15		



Nexus 1000V Key Features

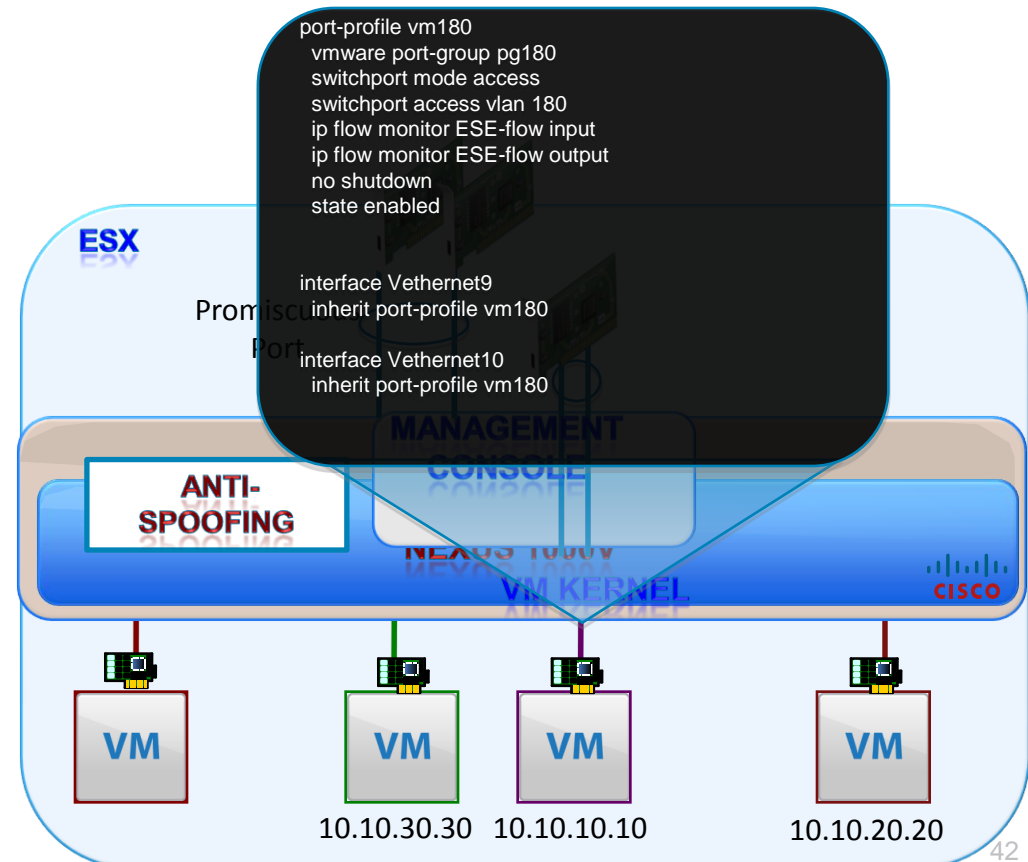


- Includes Key Cisco Network and Security features
- Addressing Issues for:
 - VM Isolation
 - Separation of Duties
 - VM Visibility

Separation of Duties: Network and Server Teams

Port Profiles

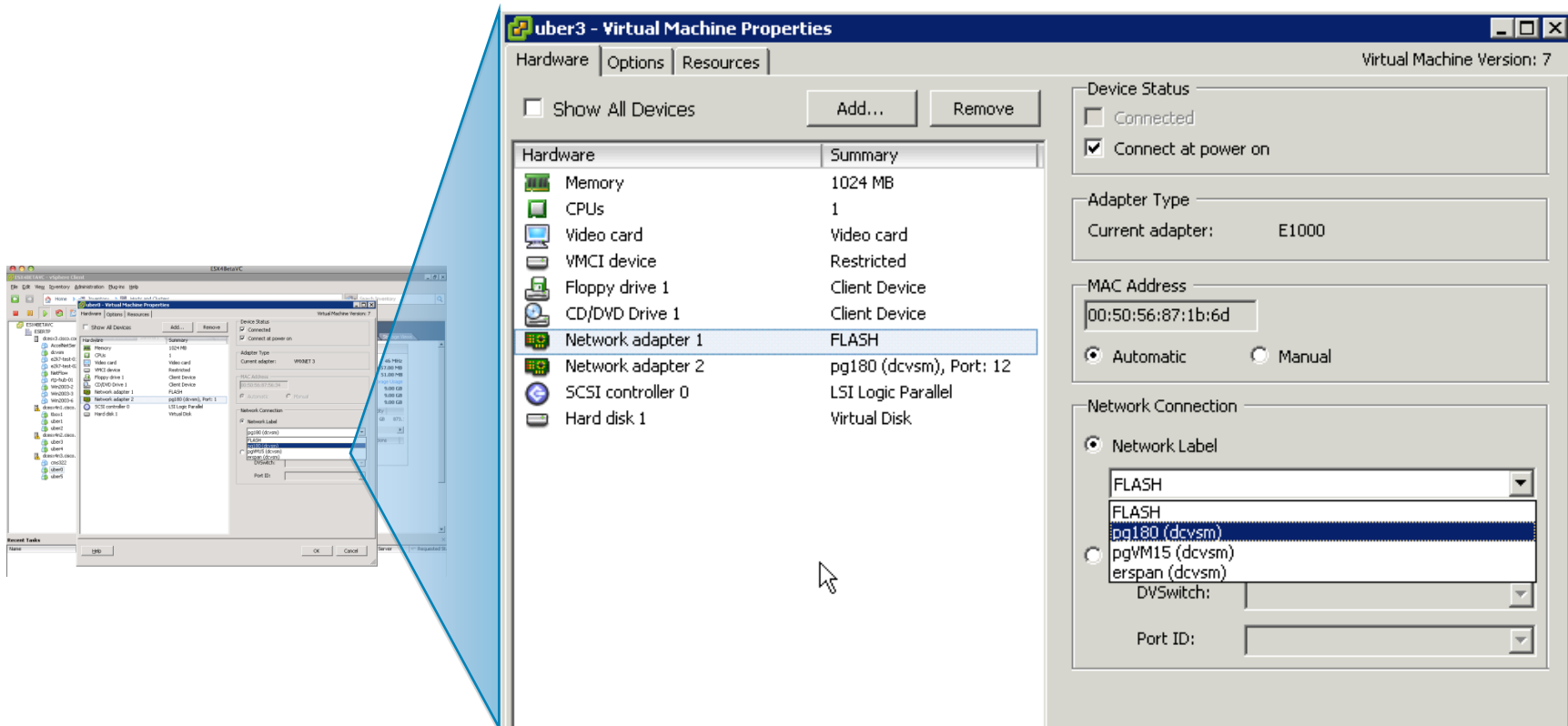
- A network feature macro
- Example: Features are configured under a port profile once and can be inherited by access ports
- Familiar IOS look and feel for network teams to configure virtual infrastructure



Separation of Duties: Network and Server Teams

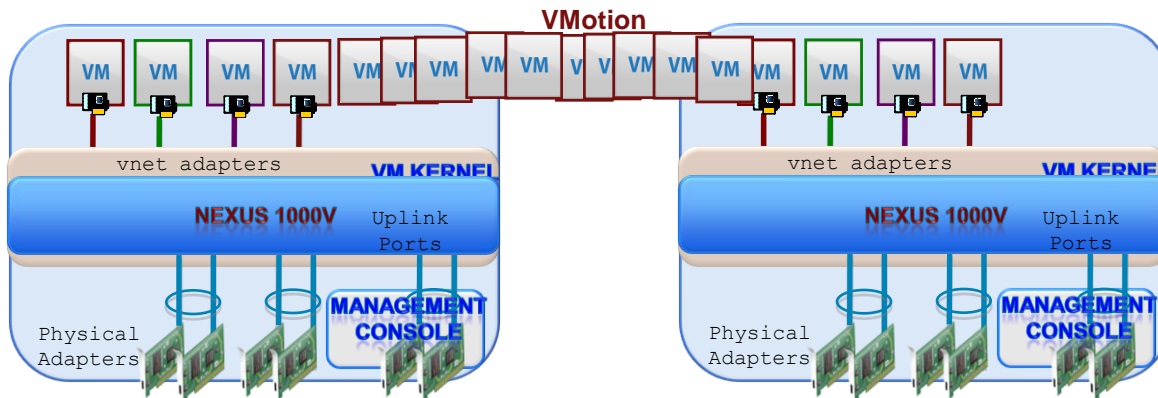
1. Nexus 1000V automatically enables port groups in Virtual Center via API
2. Server Admin uses Virtual Center to assign vnic policy from available port groups
3. Nexus 1000V automatically enables VM connectivity at VM power-on

Workflow remains unchanged



VMotion

1. Virtual Center kicks off a VMotion (manual/DRS) & notifies Nexus 1000V
2. During VM replication, Nexus 1000V copies VM port state to new host
3. Once VMotion completes, port on new ESX host is brought up & VM's MAC address is announced to the network

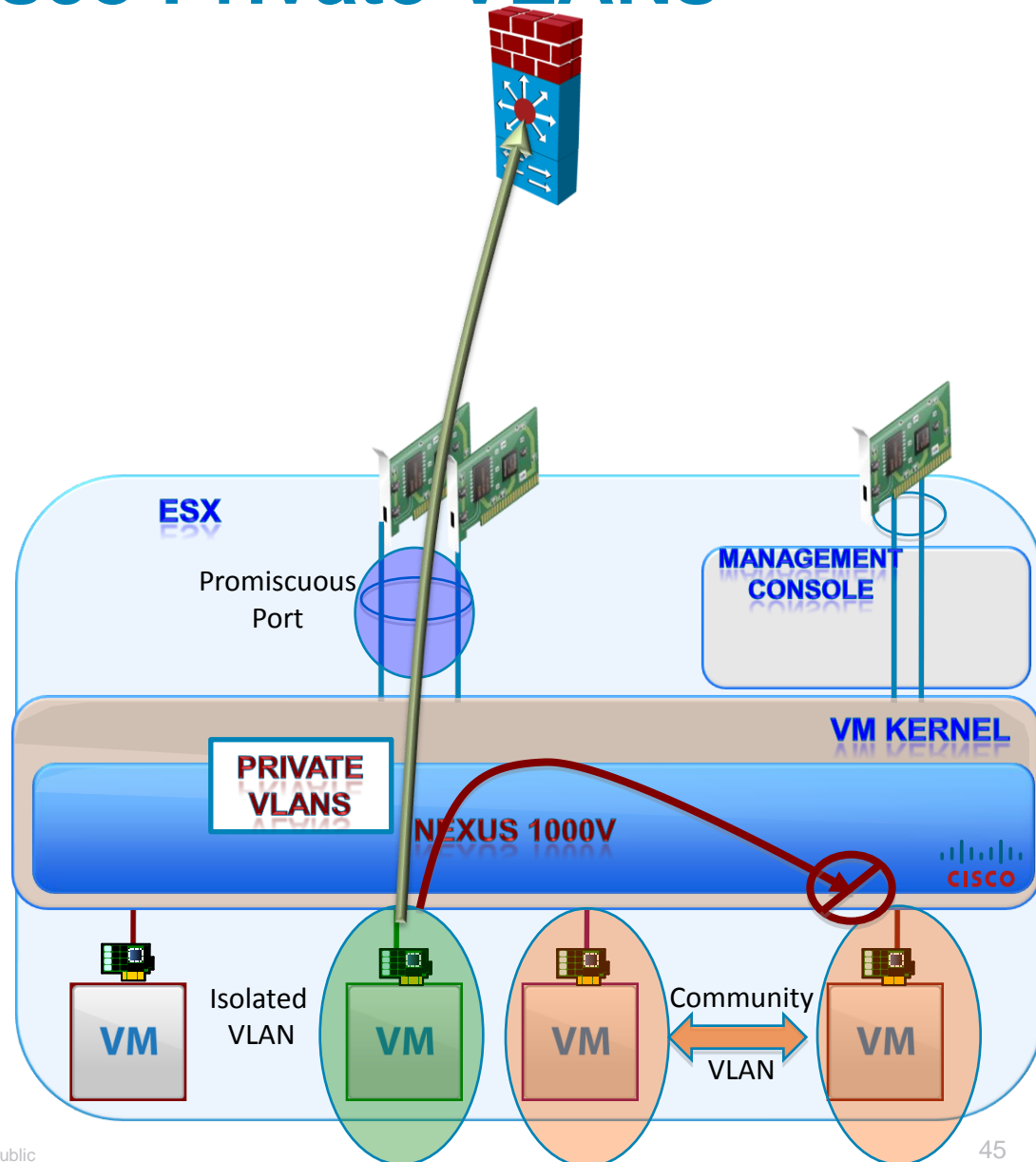


Mobile Properties Include:

- Port policy
- Interface state and counters
- Flow statistics
- Remote port mirror session

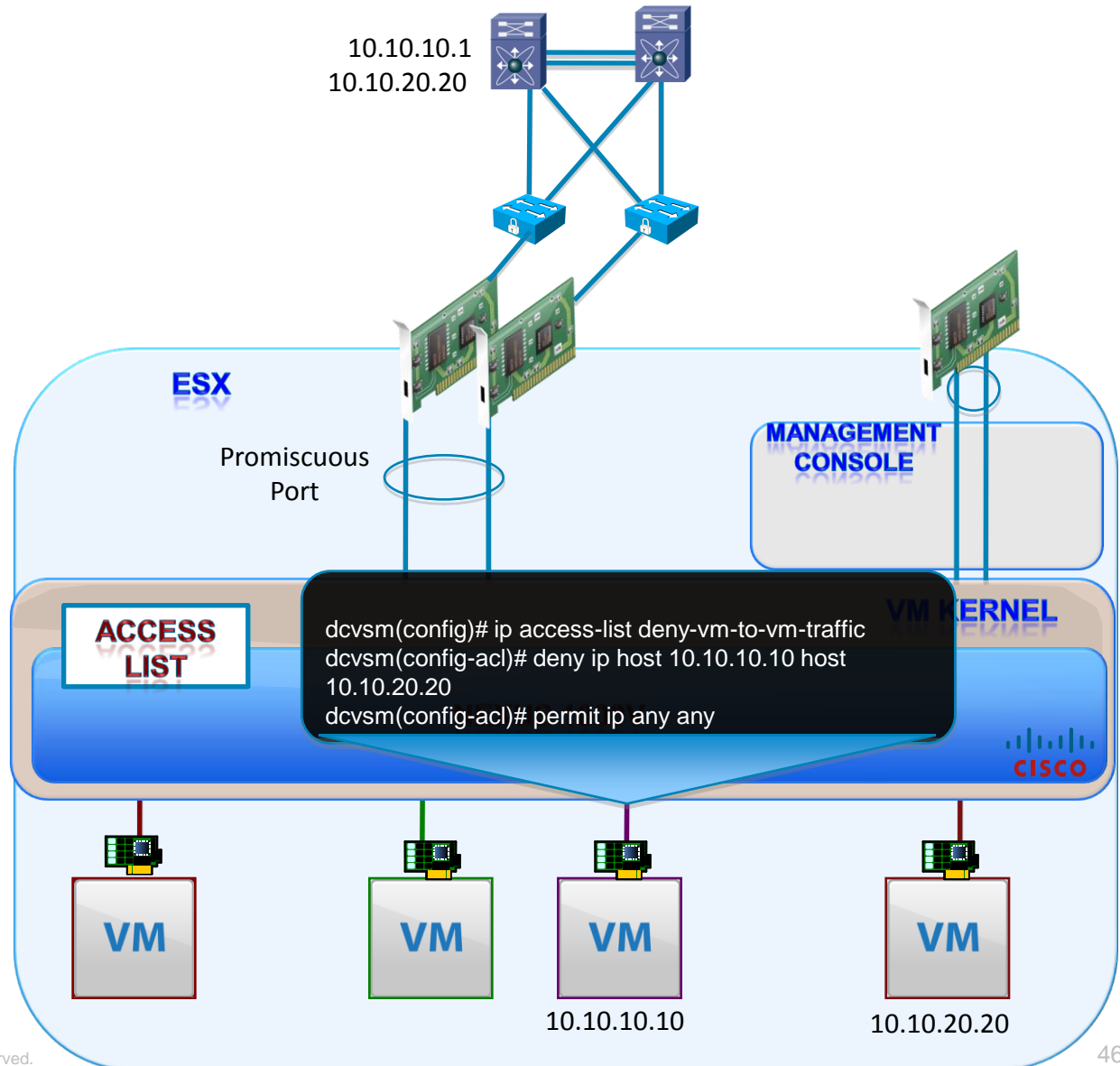
VM Isolation: Cisco Private VLANs

- Private VLANs provide layer 2 isolation for hosts in the same subnet
- Traditional Cisco PVLANS are supported: Isolated & Community ports
- Physical Infrastructure is PVLAN aware. You can carry PVLAN to physical devices ie: FWASM



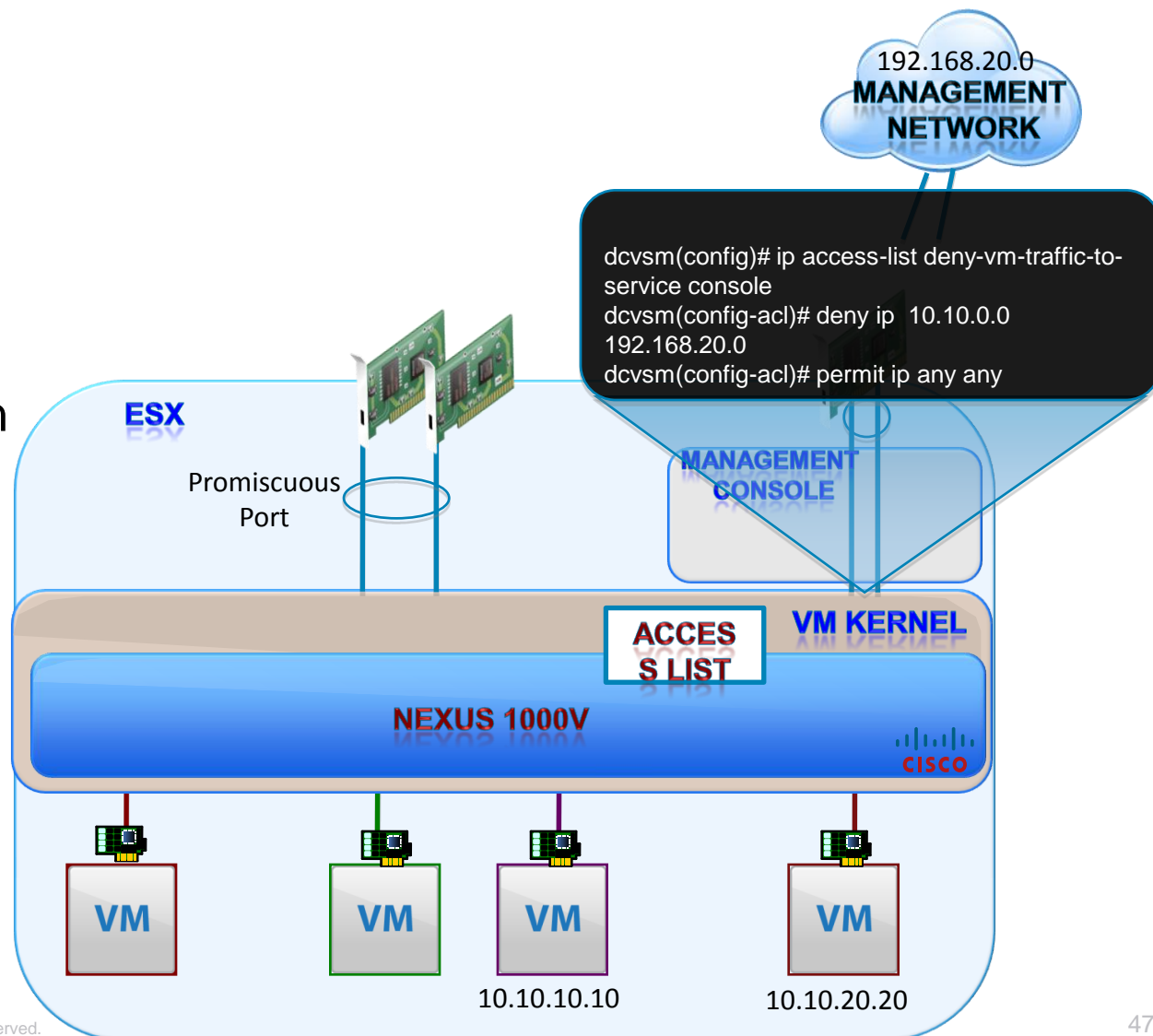
VM Isolation and Traffic Control

- Port ACLs
- Limit VM to VM traffic flows
- Enforce the way you enforce between physical servers today
- Use in conjunction with VLANs, PVLANS



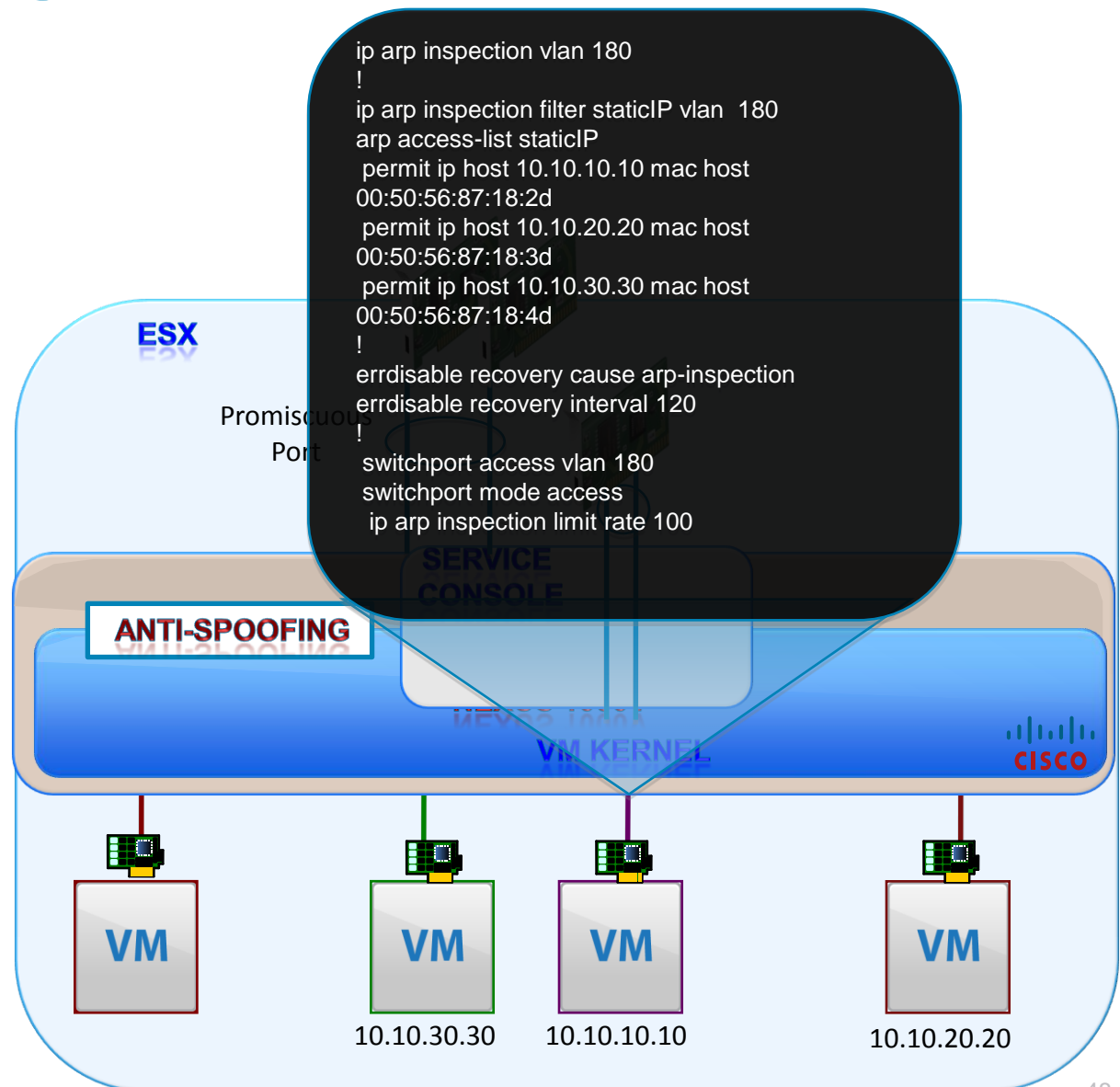
Isolating Production and Management Traffic

- Isolate management traffic from production
- Enforce physical separation and virtual separation



Anti-Spoofing

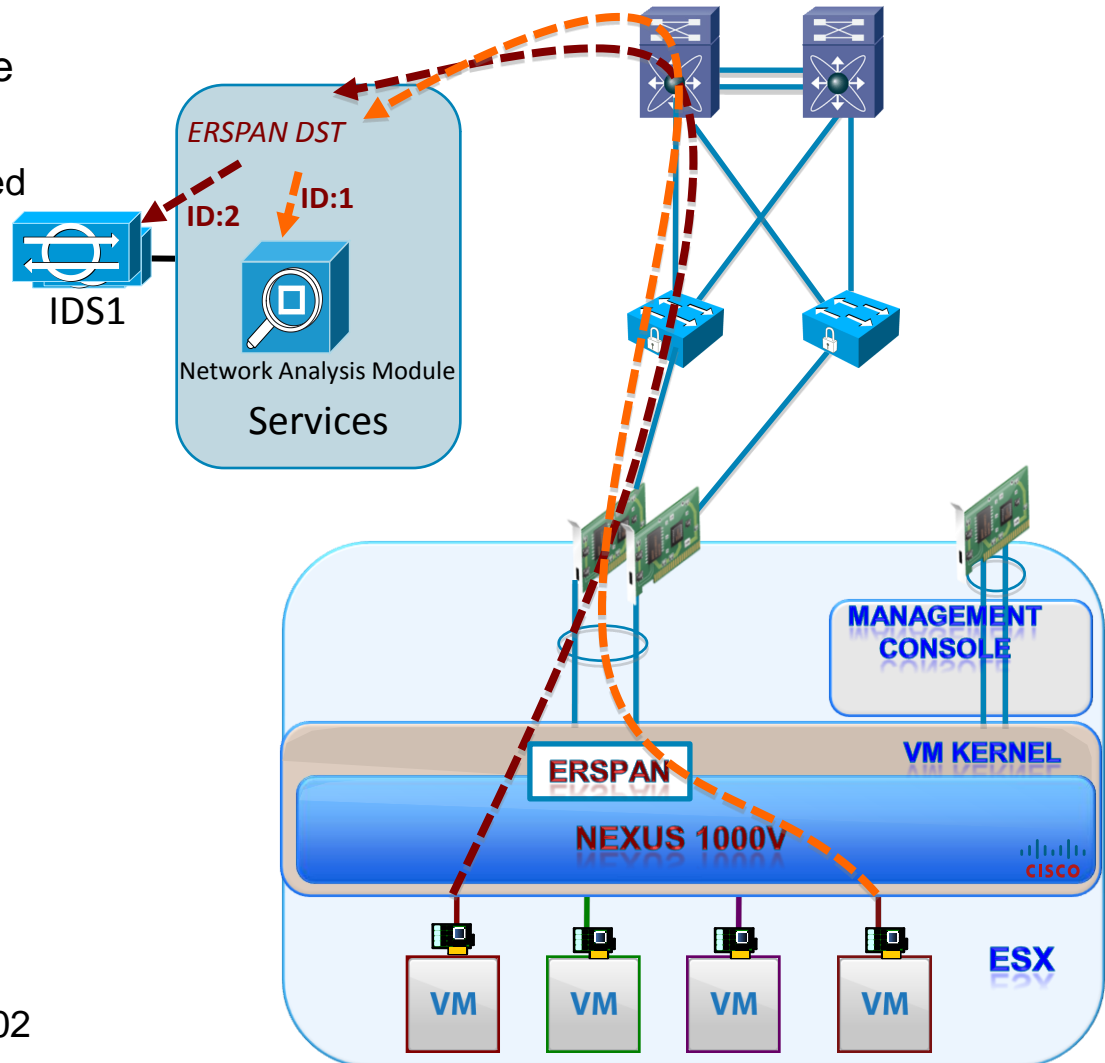
- Protection against man-in-the middle attacks
- Dynamic ARP Inspection, DHCP Snooping, IP Source Guard



VM to VM Visibility

ERSPAN

- ERSPAN source requires use of ERSPAN destination
 - Only one IP address associated with the ERSPAN source/destination per switch
- ERSPAN ID provides segmentation
- Permit protocol type header "0x88BE" for ERSPAN GRE
- ERSPAN frame considerations:
 - ERSPAN does **not** support fragmentation
 - Appends 50 Byte header to frame
 - Default 1500 MTU allows for 1468 byte frames
 - Max frame size supported 9,202 bytes



ERSPAN

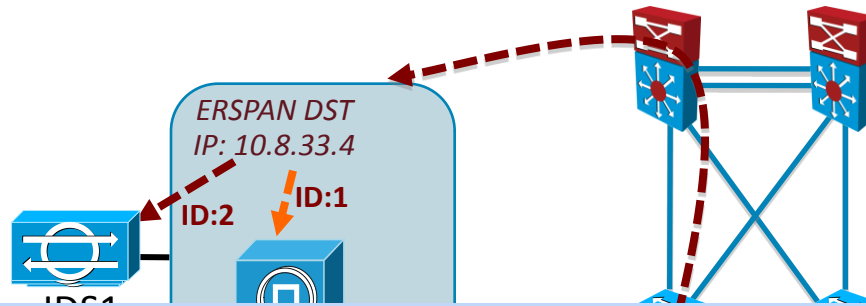
Nexus 1000 Configuration

dcvsm ⓘ

The screenshot displays a configuration interface for a Nexus 1000v switch. It is divided into three main sections:

- erspan**:
 - VMkernel Ports (4)**: A list of four VMkernel ports, each with an IP address and an information icon: vmk1 : 10.8.3.100, vmk1 : 10.8.3.101, vmk1 : 10.8.3.102, and vmk1 : 10.8.3.103. A mouse cursor is pointing at the first entry.
 - pg180**: A port group containing 8 Virtual Machines.
 - pgVM15**: A port group containing 4 VMkernel Ports and 0 Virtual Machines.
- SystemUplinks**: A list of 16 uplink ports, each with a count of NIC Adapters:
 - UpLink0 (4 NIC Adapters)
 - UpLink1 (4 NIC Adapters)
 - UpLink10 (0 NIC Adapters)
 - UpLink11 (0 NIC Adapters)
 - UpLink12 (0 NIC Adapters)
 - UpLink13 (0 NIC Adapters)
 - UpLink14 (0 NIC Adapters)
 - UpLink15 (0 NIC Adapters)
 - UpLink2 (1 NIC Adapter)
 - UpLink3 (1 NIC Adapter)
 - UpLink4 (0 NIC Adapters)
 - UpLink5 (0 NIC Adapters)
 - UpLink6 (0 NIC Adapters)
 - UpLink7 (0 NIC Adapters)
 - UpLink8 (0 NIC Adapters)
 - UpLink9 (0 NIC Adapters)

Example: Using ERSPAN to IDS for VM to VM Traffic



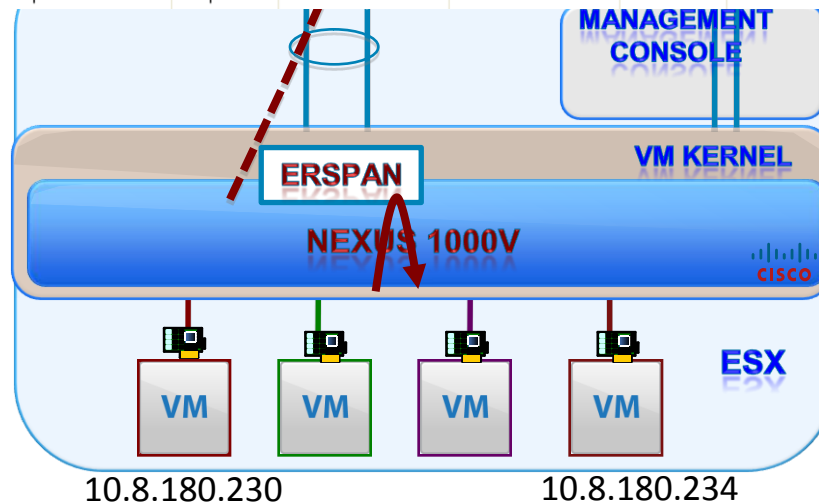
Event Monitoring > Event Monitoring > My Views

View Settings

Video

Pause Event Show All Details Filter Edit Signature Create Rule Stop Attacker Tools Other

Severity	Date	Time	Device	Sig. Name	Sig. ID	Attacker IP	Victim IP	Actions T...	Victim Port	Threat Ra...	Risk Rating	Virtual
medium	03/02/2009	12:05:05	dca-ips1	Malformed HTTP Request	5769/1	10.8.180.230	10.8.180.234		80	61	61	vs1



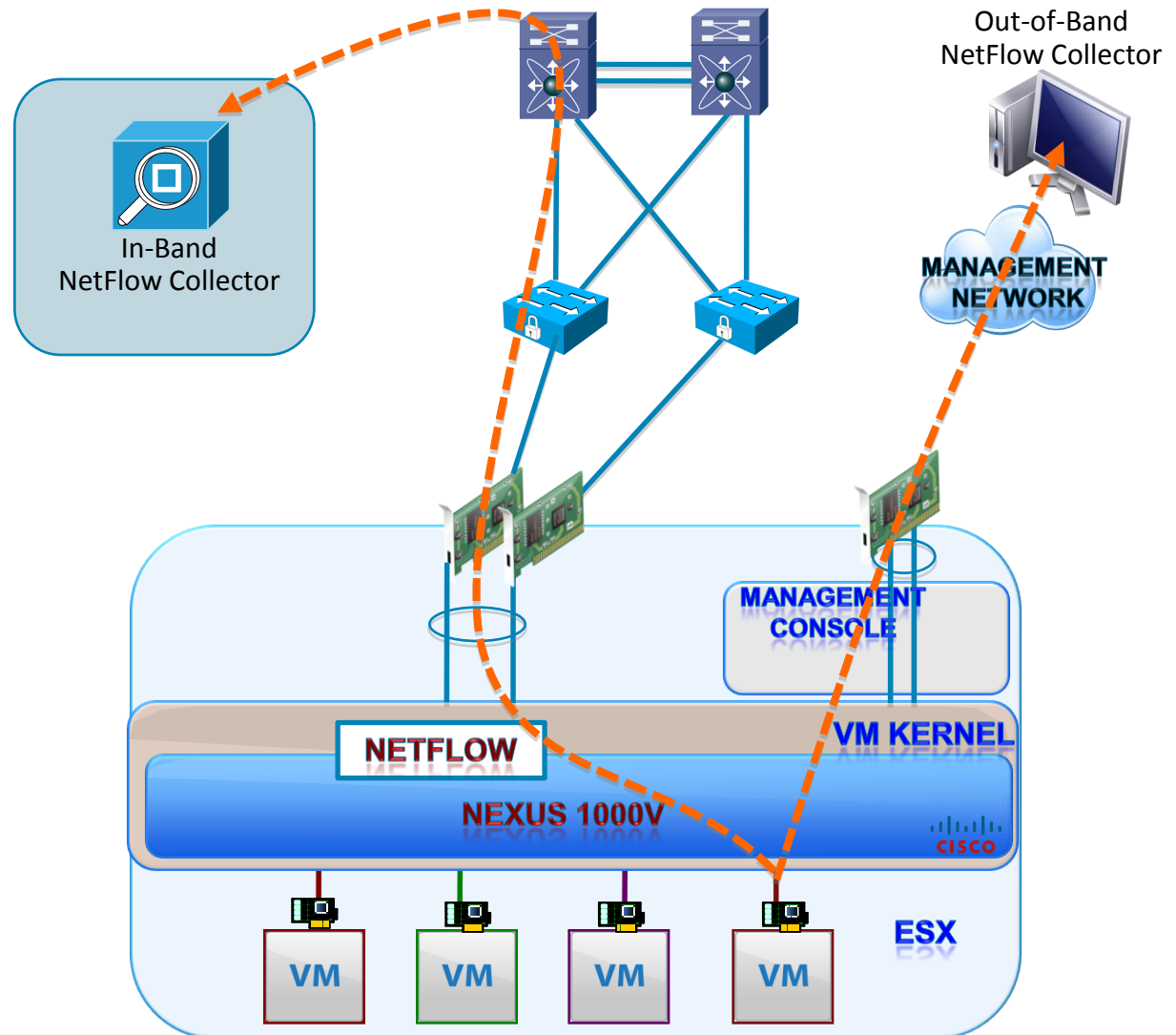
VM to VM Visibility

NetFlow

- N1k requires Netflow source interface

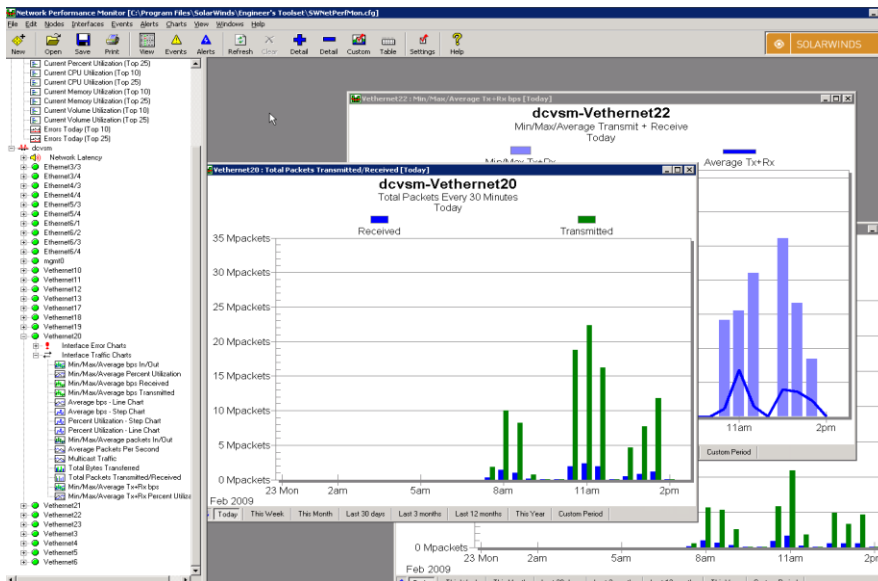
Defaults to Mgmt0

Support v9 format

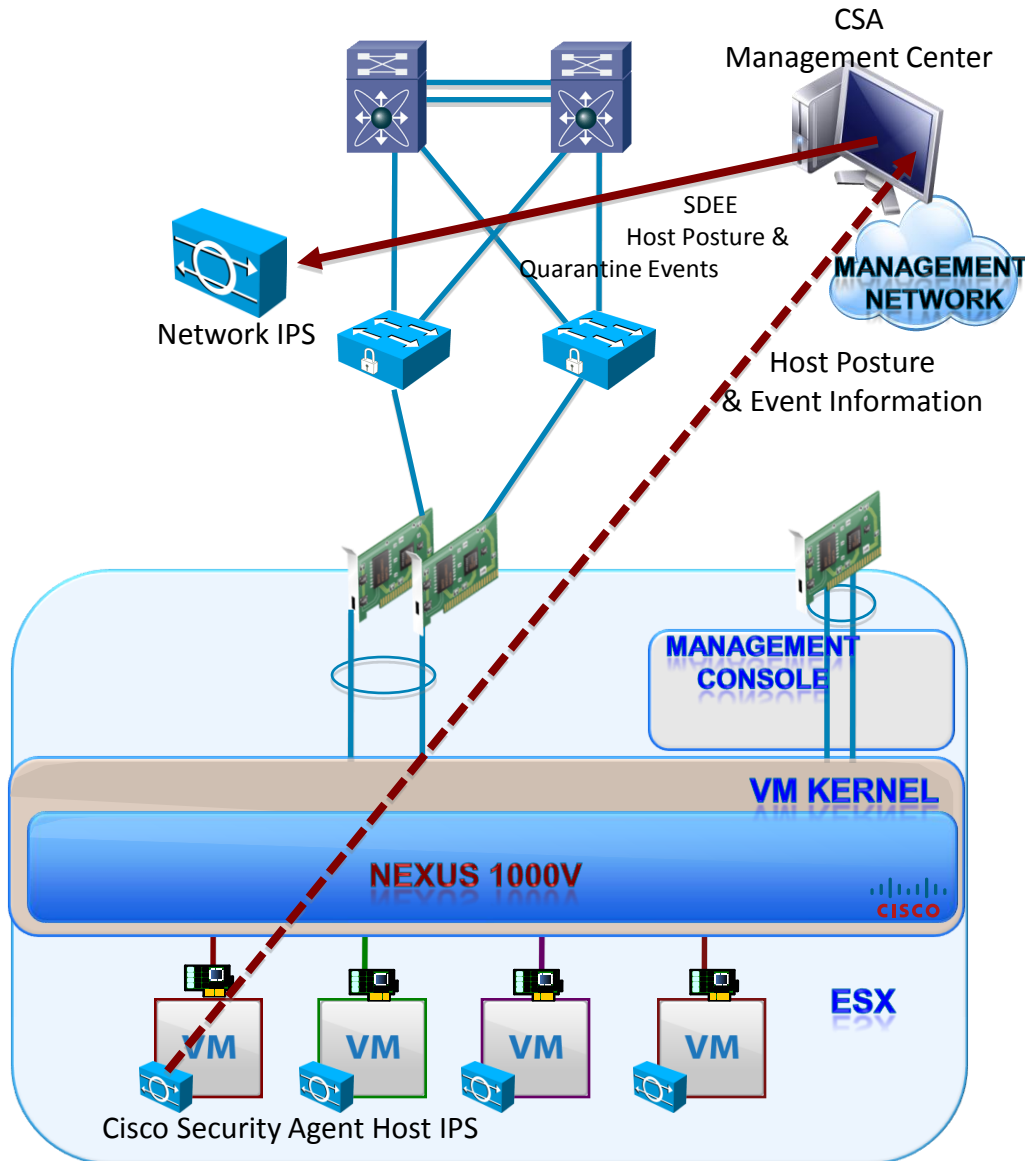


NetFlow

- Maximum of one flow monitor per interface per direction is permitted
- Maximum of two flow exporters per monitor are permitted
- Port profiles afford easy deployment



VM Guest OS Protection



Host IPS and Integration with Network IPS

- A host is quarantined manually by a Cisco Security Agent MC administrator or rule-generated by global correlation
- Quarantine events include
 - the reason for the quarantine
 - the protocol associated with a rule violation (TCP, UDP, or ICMP), an indicator on whether a rule-based violation was associated with an established TCP connection or a UDP session
 - the IP address of the host to be quarantined.



Protect the Endpoint

Remember...

- Security best practices still apply
- Limit Data Flow to other servers and resources
- Do not use non-persistent disks
- Harden the Host OS, Hypervisor, & Guest OS
- Use AV, maintain patches and updates
- Consider using a HIPS solution



Takeaways

- Device Virtualization

 - Scale use of network and security components

 - Flexible integration options

 - Can get complicated...plan accordingly

- Server Virtualization

 - Secure virtual machine environment

 - Use features to maintain visibility

 - Ensure Separation of Duties is maintained

 - Don't do what you wouldn't do on a physical machine

Additional Resources

■ Data Center Design Zone

<http://www.cisco.com/go/designzone>

The screenshot shows a web browser window displaying the Cisco Design Zone for Data Centers. The page title is "Design Zone for Data Centers - Cisco Systems". The URL in the address bar is "http://www.cisco.com/en/US/netso1/ns743/networking_solutions_program_home.html". The page features the Cisco logo and a navigation menu with categories like Solutions, Products & Services, Ordering, Support, Training & Events, Partner Central, and My Cisco. A search bar is located in the top right corner. The main content area is titled "Design Zone for Data Centers Introduction" and includes a list of bullet points, a paragraph about DCAP, and a link to a PDF document. A sidebar on the left lists various design zones, and a right sidebar contains featured content and related links.

Worldwide [change] | Log In | Register | About Cisco

Search Go

Solutions | Products & Services | Ordering | Support | Training & Events | Partner Central | My Cisco

HOME
SOLUTIONS
ENTERPRISE
PROGRAMS FOR ENTERPRISE
DESIGN ZONE
Cisco Validated Design Program
Design Zone for Branch
Design Zone for Campus
Design Zone for Data Centers
Design Zone for Financial Services
Design Zone for Government
Design Zone for Healthcare
Design Zone for Interoperability Systems
Design Zone for Manufacturing
Design Zone for Mobility
Design Zone for Retail
Design Zone for Security
Design Zone for Unified Communications

Design Zone for Data Centers

Introduction

By using Cisco Data Center Assurance Program (DCAP) best practices, IT professionals can:

- Build a data center-class network
- Accelerate project deployments with lower risk
- Facilitate new technology adoption and upgrades
- Help ensure that IT staff is equipped with the right skills and expertise for their dynamic environment

Designed, tested, and validated by Cisco engineering teams, and based on customer input and requirements, DCAP is consistent with the quality standards defined by the [Cisco Validated Designs \(CVD\)](#) program that provides design guidance across Cisco network architectures.

For a concise overview of the Data Center Assurance Program, read the [Cisco Data Center Assurance Program Design Best Practices: At-a-Glance](#) (PDF - 220 KB)

Use this newly updated interactive tool to gain access to the most recent DCAP design best practices. **Now!** > [Launch Interactive Tool](#)

Cisco Validated Design Guides

Cisco Validated Designs consist of systems and solutions that are developed, tested, and documented to facilitate faster, more reliable, and more predictable deployments. Cisco Validated Designs are documented in three formats: Design Guides, System Assurance Guides, and Application Deployment Guides.

[Storage Networking](#)
Consolidating, virtualizing, and managing information resources across Fibre Channel, iSCSI, and Ginabit

Featured Content

Interactive Data Center Assurance Program
Access all DCAP 4.0 design information through an interactive graphical interface.
> [Go Now](#)

Data Center Assurance Program At-a-Glance
System assurance testing supports your data center networking deployments, learn how.
> [Read More](#) (PDF - 160 KB)

Data Center Assurance Program for Applications
Discover how Cisco is optimizing applications throughout the network.
> [Learn More](#)

Related Links

- [Cisco Data Center Networking Solutions](#)
- [Cisco Data Center Network Services Offerings](#)

See the new Cisco Nexus 5000 Series Switches in operation
> [View Webcast](#)

