Security Services Design in the Next-Generation Data Center

Ken Kaminski

Security Technical Solutions Architect – Northeast

CISSP, GCIA, GCFA, GAWN, GPEN

Cisco Systems

Agenda

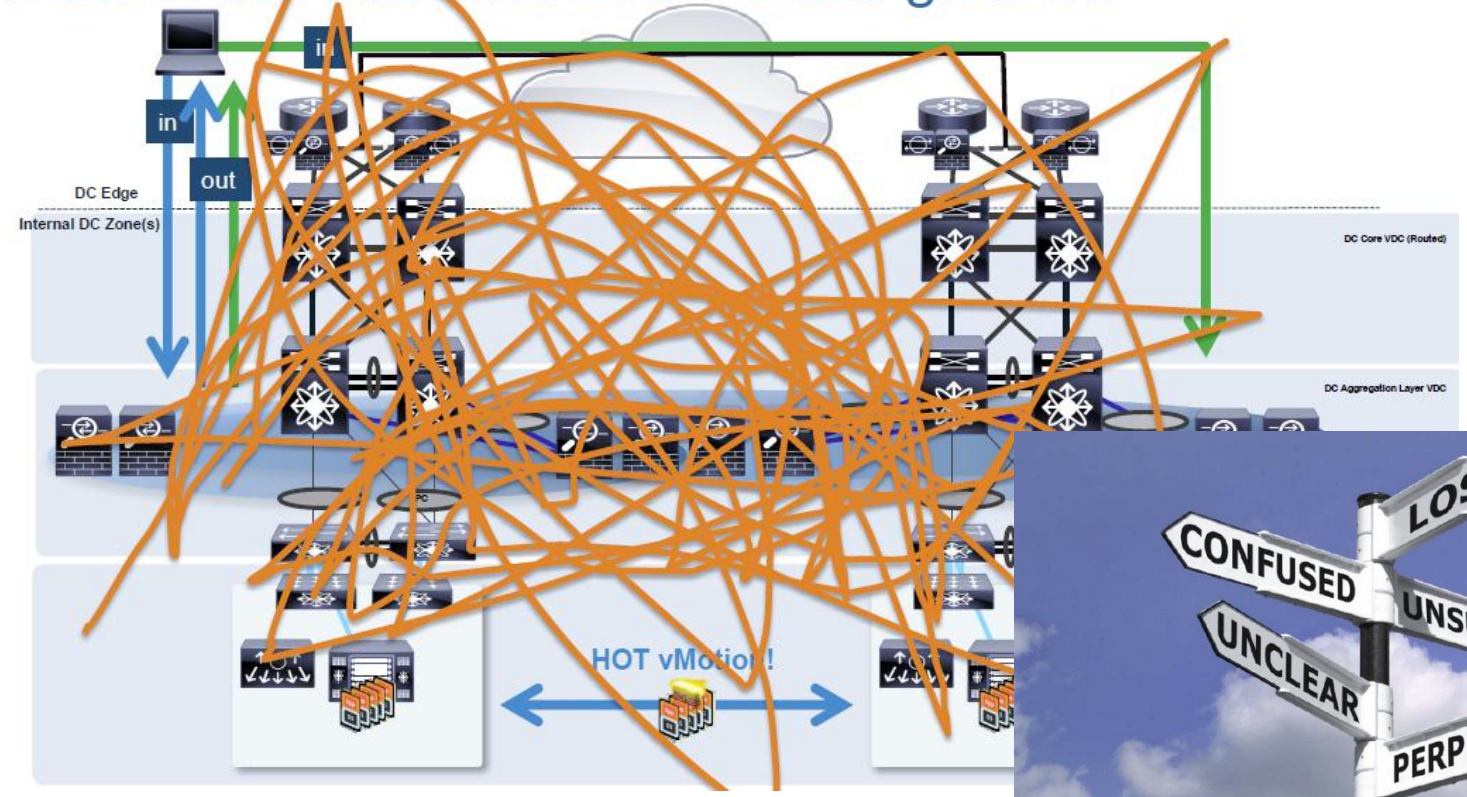
1. Data Center Design Concepts
2. Firewalls in the Data Center
3. Secure Virtual Containers
4. Visibility and Threat Defense

- This presentation is focused upon the Enterprise Data Center

Data Center Design Concepts

Secure Data Center Design

Data Center Interconnects – Entanglement



Some Loops are Fun ...

But Not All ... Sounds Familiar...?

“The whole network is down”

```
%IP-4-DUPADDR: Duplicate address 10.87.1.2 on Vlan100, sourced by 00d0.04e0.63fc
%IP-4-DUPADDR: Duplicate address 10.87.1.2 on Vlan100, sourced by 00d0.04e0.63fc
%IP-4-DUPADDR: Duplicate address 10.87.1.2 on Vlan100, sourced by 00d0.04e0.63fc
...
```

“I can’t access anything”

ll systems are unreachable

```
%C4K_EBM-4-HOSTFLAPPING: Host 00:02:A5:8A:8B:5E in vlan 60 is flapping between port Gi3/6 and port Po9
%C4K_EBM-4-HOSTFLAPPING: Host 00:02:A5:8A:8B:5E in vlan 60 is flapping between port Gi3/6 and port Po9
%C4K_EBM-4-HOSTFLAPPING: Host 00:02:A5:8A:8B:5E in vlan 60 is flapping between port Gi3/6 and port Po9
...
```

“Nothing seems to work”

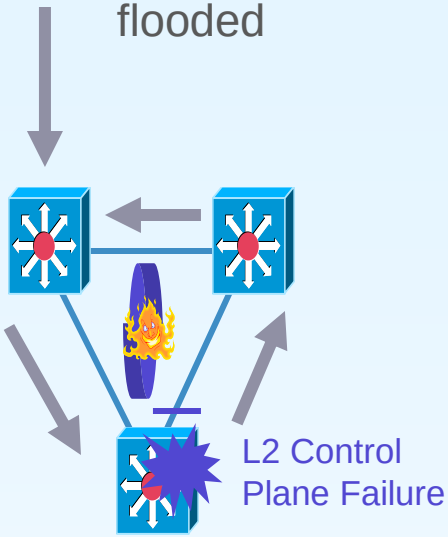
```
Number of topology changes 2433341 last change occurred 00:00:02 ago
```

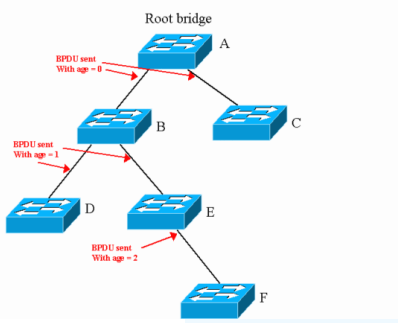
```
%PM-SP-4-LIMITS: Virtual port count for module 5 exceeded the recommended limit of 1800
%PM-SP-4-LIMITS: Virtual port count for switch exceeded the recommended limit of 13000
```

Many of us have suffered the consequences of a L2 loop

The Problem?

L2 Fails Open – i.e. Broadcast and Unknowns flooded

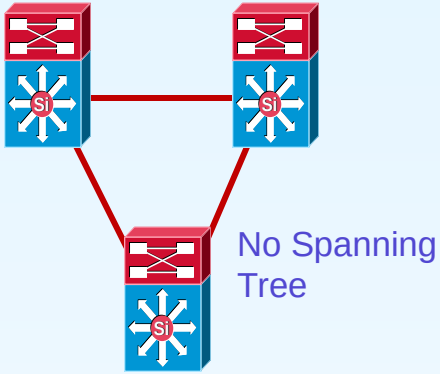




... a loop and a network down

One Solution...

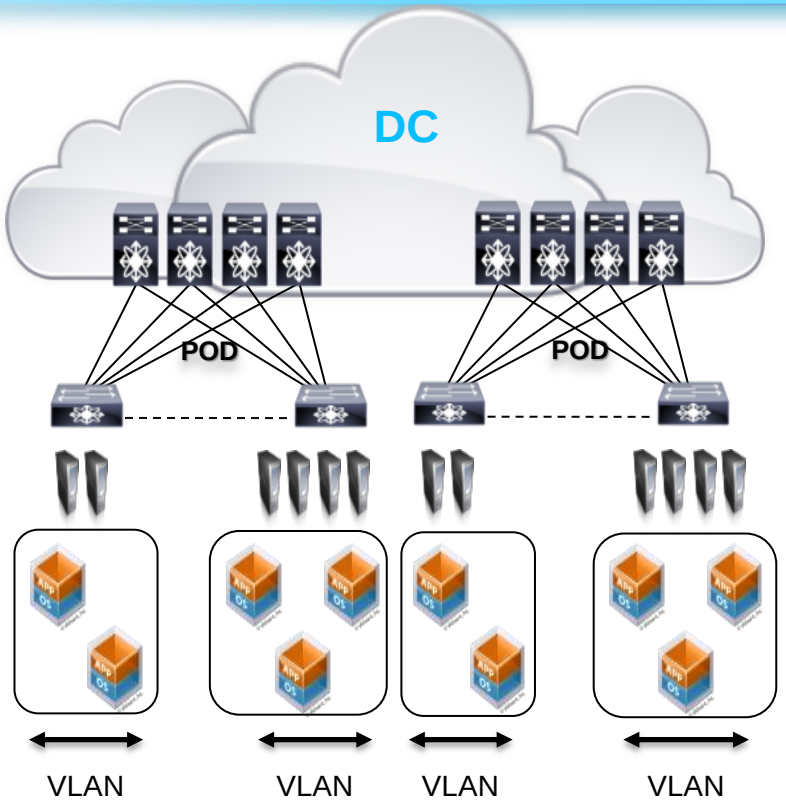
Layer 3 Routing



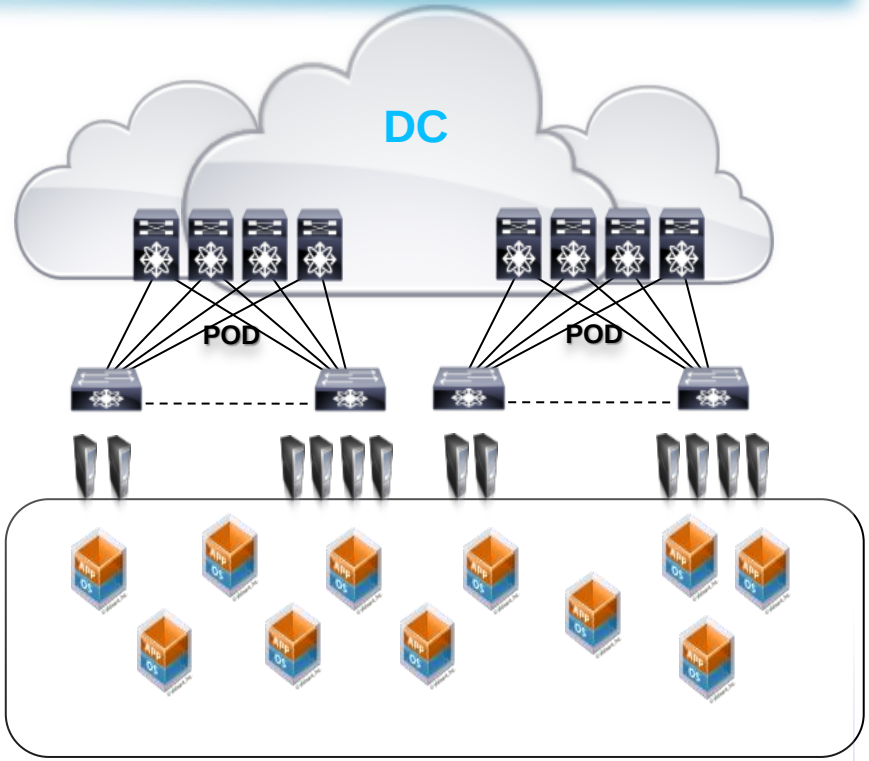
... But this is not a Solution in the Data Center

VLAN Ubiquity Intra Data Center

Rack-Wide VM Mobility

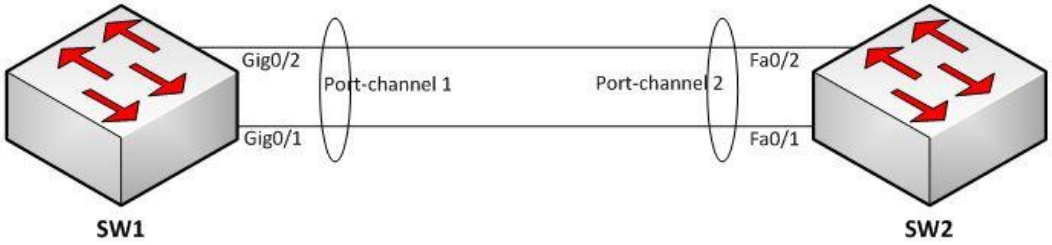


DC-Wide VM Mobility

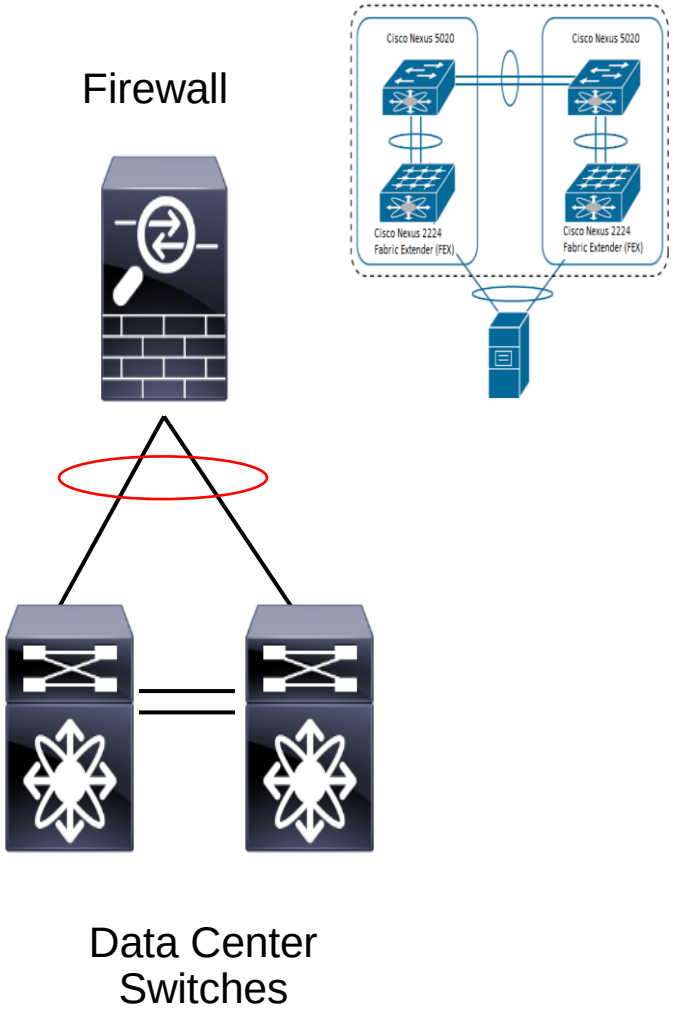


- Network protocols enable broader VM Mobility
- Implementable on Virtual and Physical
- Examples: VPC, FabricPath/TRILL, VXLAN

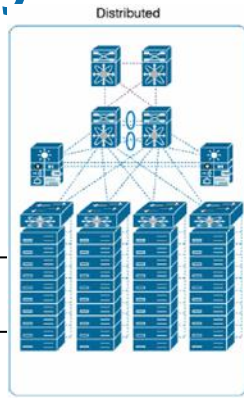
Key Concept: Virtual Port Channel (VPC) and Multichassis Etherchannel (MEC)



- Virtual Port Channels (vPC) are port channels where both links are actively forwarding traffic
- Typically deployed in the Data Center
- VPC was created to solve two inherent network problems: Spanning-tree recalculation times and unused capacity in redundant L2 uplinks (due to STP blocks)
- No additional config required on Firewall
- Multi-vendor – Multichassis Etherchannel (MEC)



Classic Data Center Design – Multilayer Distributed Model



Aggregation Layer

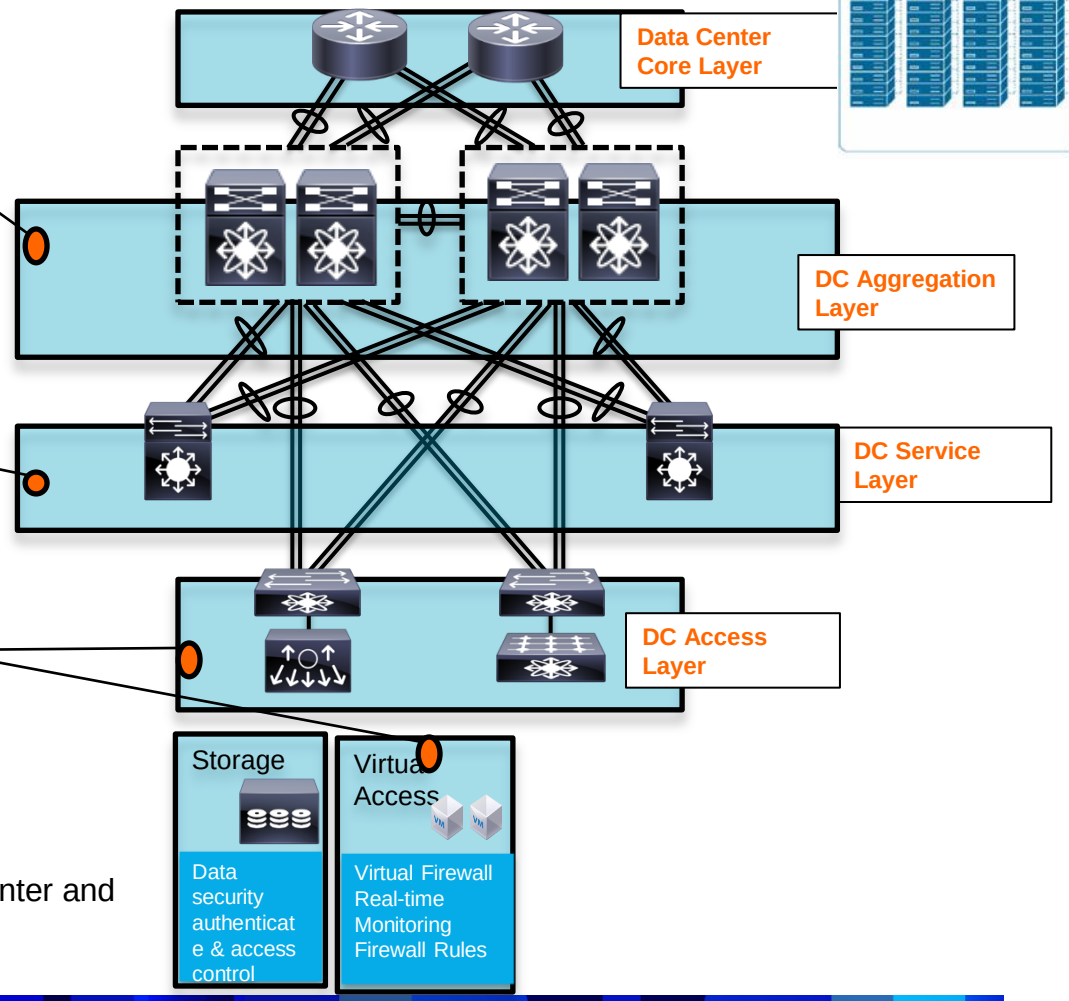
Centralized point for ingress and egress data center flows
Can be demarcation point for L2 and L3
Services can be scaled as data center grows

Services Layer

Additional services location for server farm specific protection
Offloads port utilization from Aggregation Layer

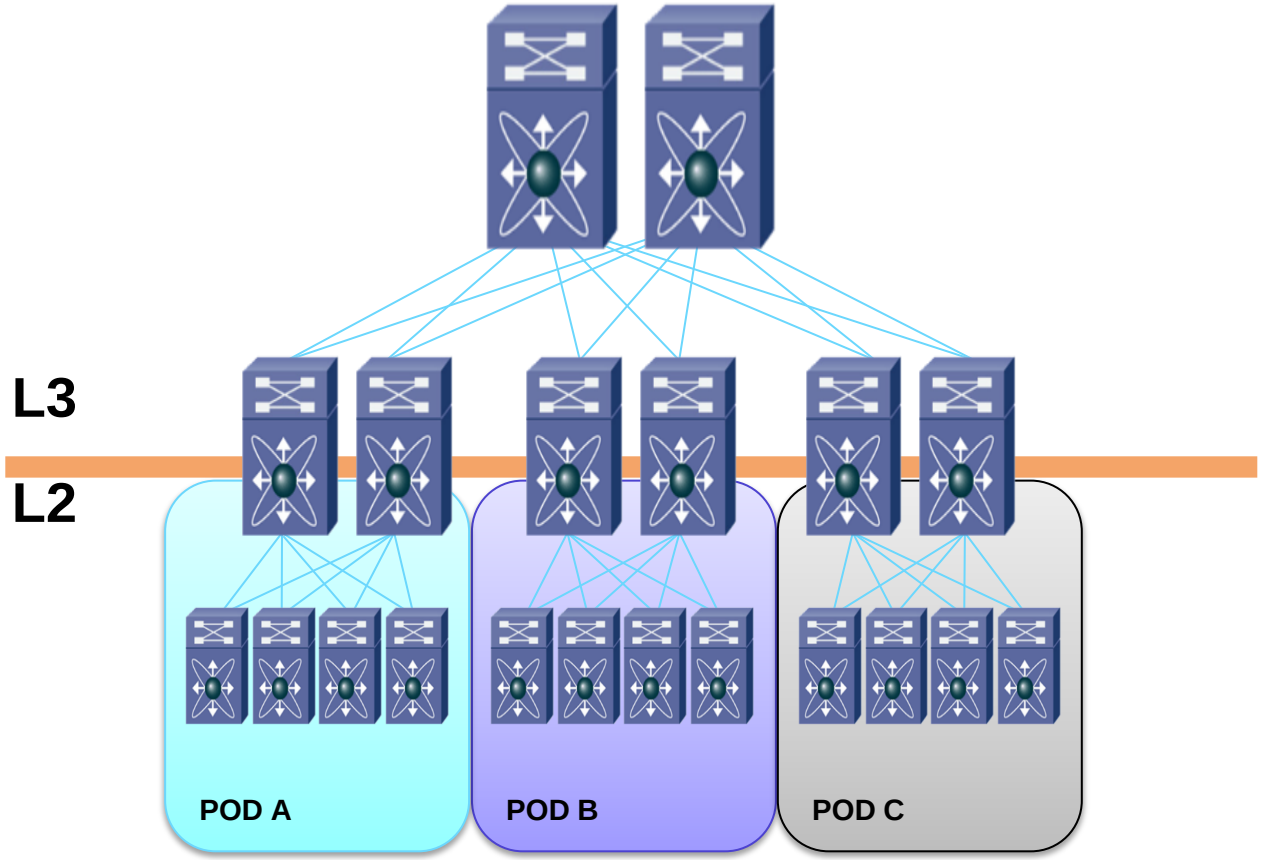
Virtual Network & Access

Physical and virtual form factor for server connectivity
Top of rack provides port density for server connections



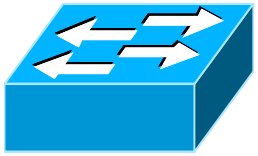
*Note: This diagram is focused only on internal data center and does not include the data center edge, extranet, DMZ.

Classic Multilayer Data Center Design



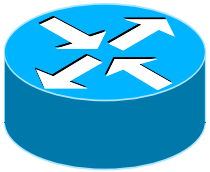
Layer 2 benefits limited to a POD

Key Concept: FabricPath-TRILL



Switching

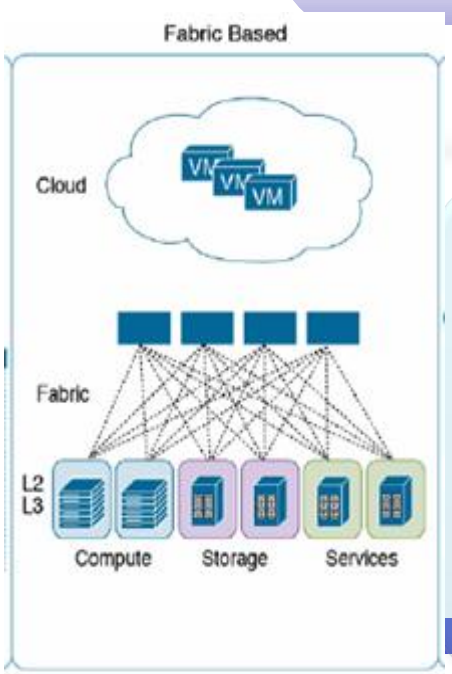
- **Easy Configuration**
- **Plug-and-Play**
- **Flexible Provisioning**

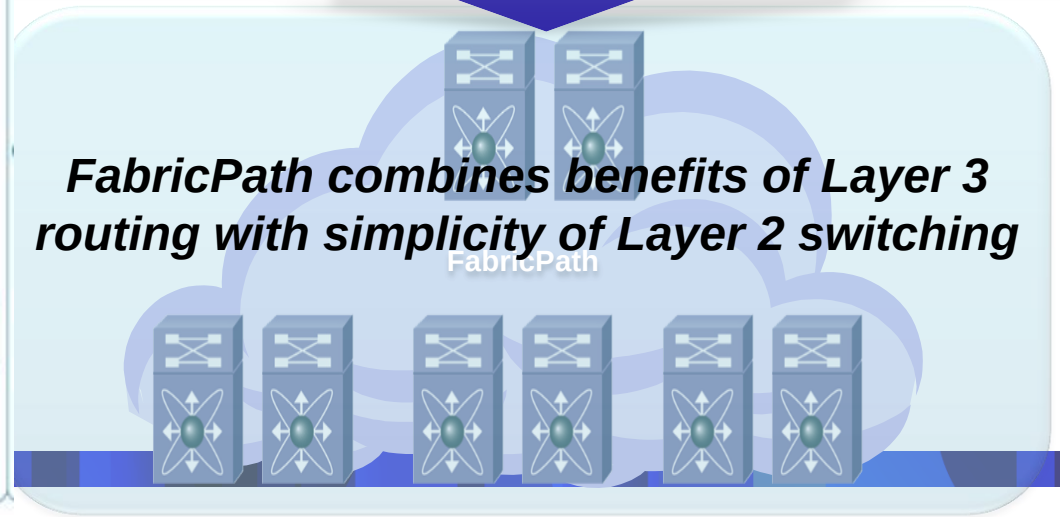


Routing

- **Multipathing (ECMP)**
- **Fast Convergence**
- **Stable and Scalable**

FabricPath





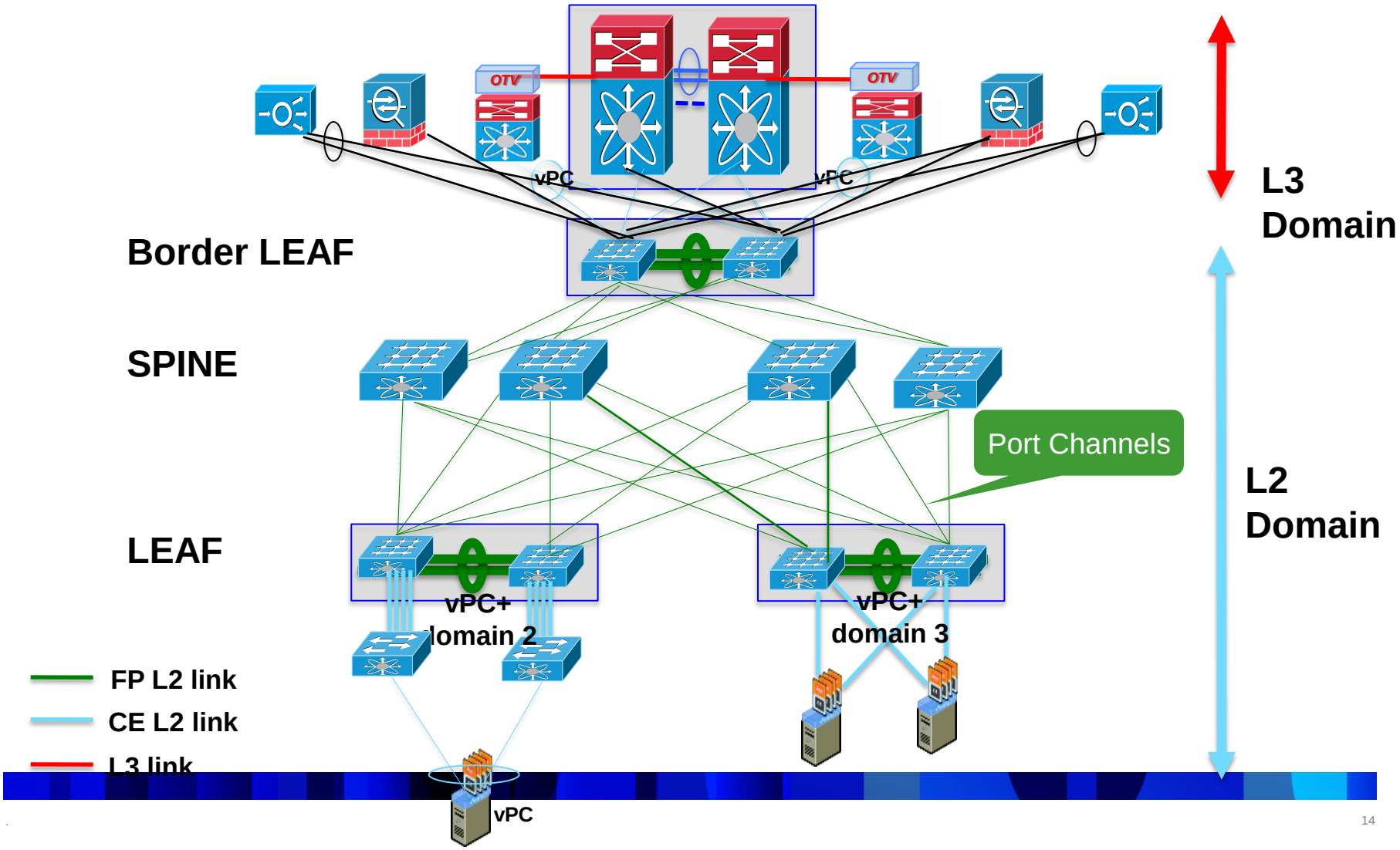
FabricPath combines benefits of Layer 3 routing with simplicity of Layer 2 switching

Key Concept: Fabric Path
Enhancing L2 with L3

FabricPath

Data Plane Innovation	Control Plane Innovation
▪ Routing Ethernet frame, not bridging ▪ MAC in MAC Encapsulation (uses Switch-ids) ▪ Built-in loop-mitigation Time-to-Live (TTL) RPF Check	▪ Plug-n-Play Layer 2 IS-IS ▪ Support unicast and multicast ▪ Fast, efficient, and scalable ▪ Equal Cost Multipathing (ECMP) ▪ VLAN and Multicast Pruning

Fabric Path Based Data Center



Transparent Interconnection of Lots of Links (TRILL)

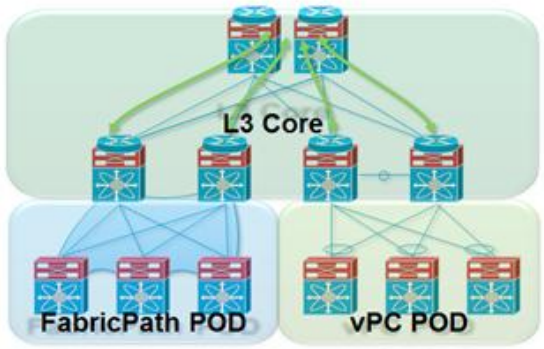
- TRILL is an IETF standard for Layer 2 multipathing
- IETF Proposed Standard that “suggests applying modern network-layer routing protocols at the link layer”
- –RFC 5556, RFC 6325, etc
- Driven by multiple vendors, including Cisco
- FabricPath capable hardware is also TRILL capable
- Cisco provides TRILL as a special mode for FabricPath with a software upgrade

I E T F

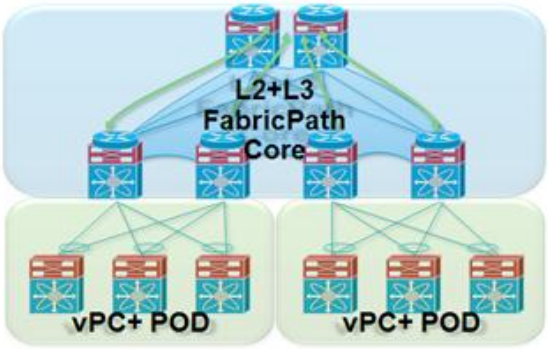
http://datatracker.ietf.org/wg/trill/

Key Concept: Fabric Path

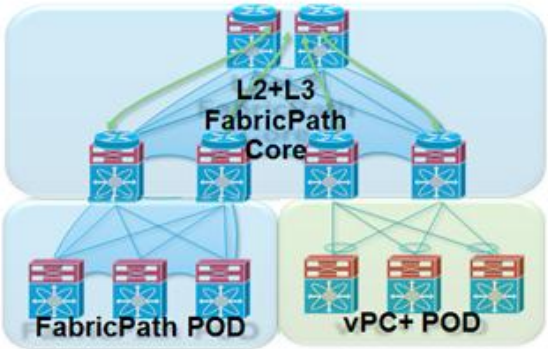
Some Additional FabricPath Options



Option 1 – FabricPath POD(s) with traditional L3 Core



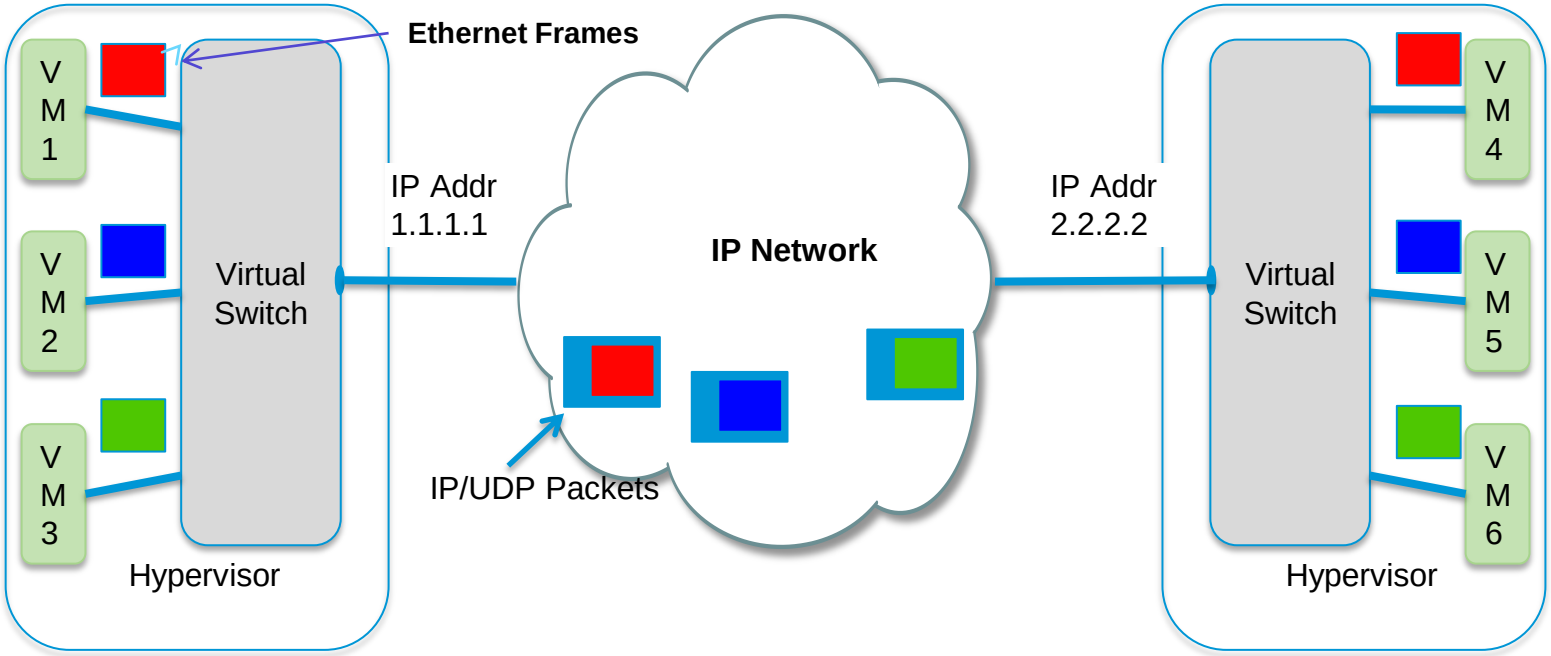
Option 2 – FabricPath Core with traditional Aggregation POD(s)



Option 3 – FabricPath Core with Combination of FabricPath POD and Traditional Aggregation POD

Key Concept: Virtual Overlay Technology

- Virtualized Servers: no hardware switches and routers
- **Requirement in Large Multitenant Data Centers**
- Servers perform data encapsulation and forwarding
- SW based virtual switches instantiate customer topologies



Virtual Overlay Encapsulations and Forwarding

- Ethernet Frames are **encapsulated** into an IP frame format
- **New control logic** for learning and mapping VM identity (MAC address) to Host identity (IP address)

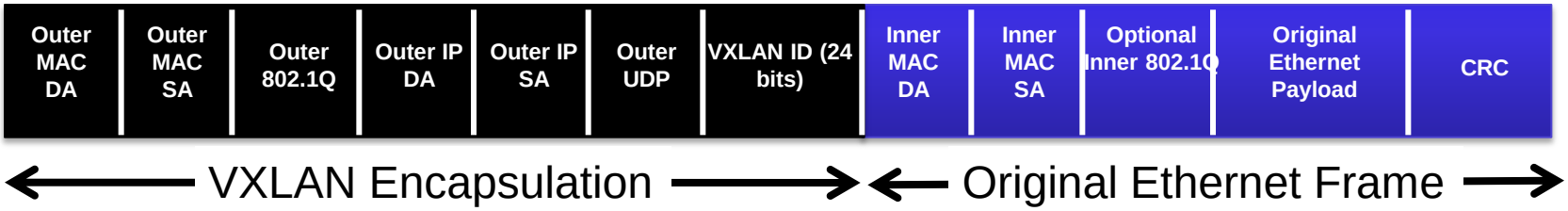
- **Three Hypervisor based Overlays**
  - VXLAN Virtual Extensible Local Area Network
  - NVGRE, Network Virtualization Generic Router Encapsulation
  - STT Stateless Transport Tunneling

- **Network Based Overlays**
  - VXLAN and NVGRE

Virtual Extensible Local Area Network (VXLAN)

- Ethernet in IP overlay network
  - Entire L2 frame encapsulated in UDP
  - 50 bytes of overhead
- Include 24 bit VXLAN Identifier
  - 16 M logical networks
  - Mapped into local bridge domains
- VXLAN can cross Layer 3

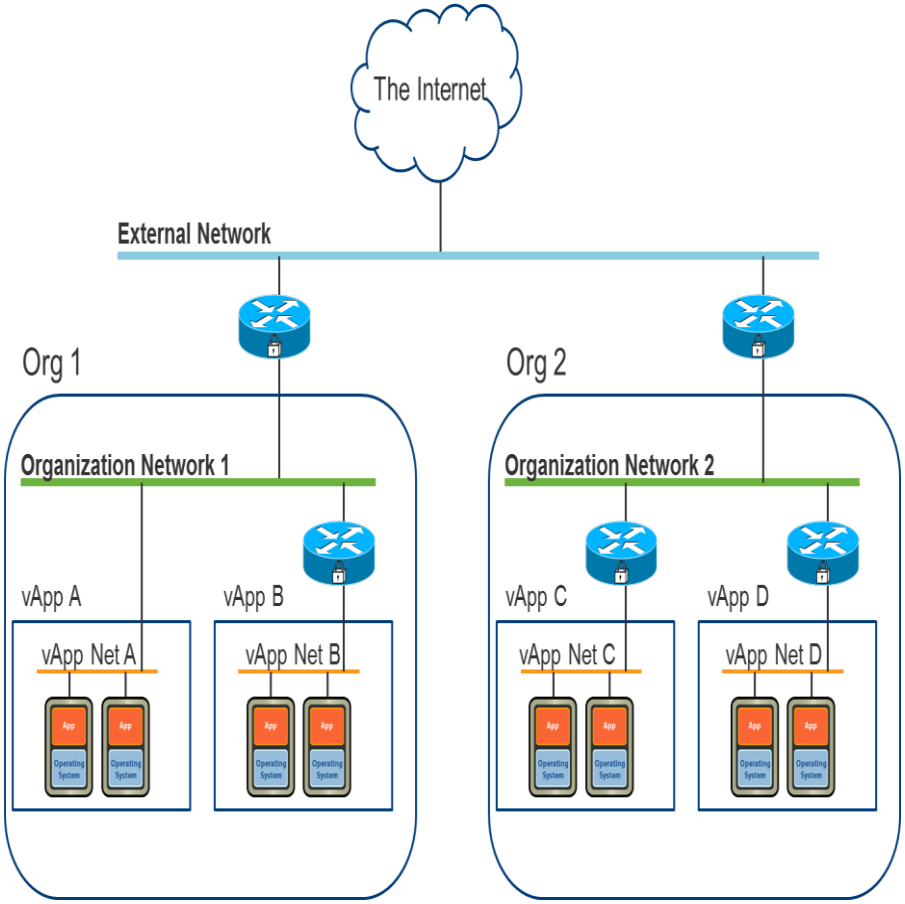
- Tunnel between VEMs
  - VMs do NOT see VXLAN ID
- IP multicast used for L2 broadcast/multicast, unknown unicast
- Technology submitted to IETF for standardization
  - With Cisco, Arista, VMware, Citrix, Red Hat and Others



Multi-Tenancy and vApps Drive Layer2 Segments

- Both MAC and IP addresses could overlap between two tenants, or even within the same tenant in different vApps.
  - Each overlapping address space needs
  - a separate segment

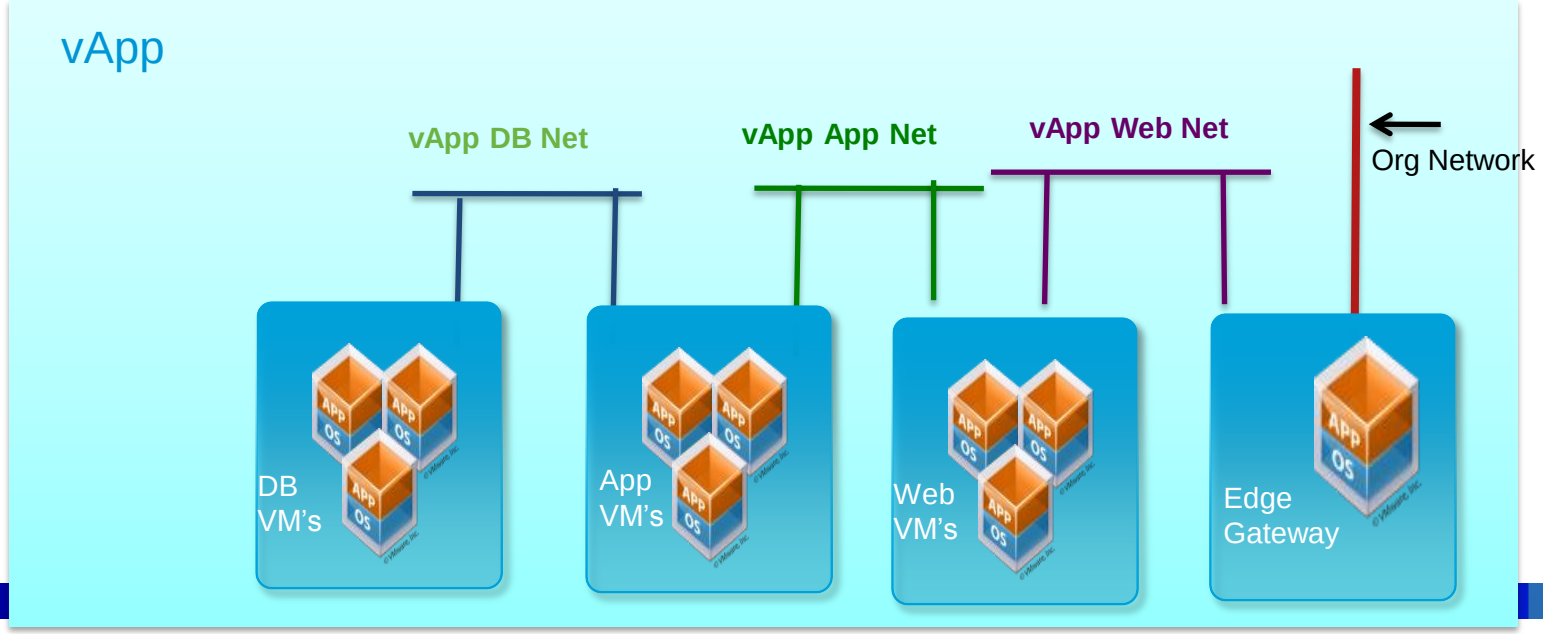
- VLANs uses 12 bit IDs = 4K
- VXLANs use 24 bit IDs = 16M
- NVGRE uses 24 bit IDs = 16M



20

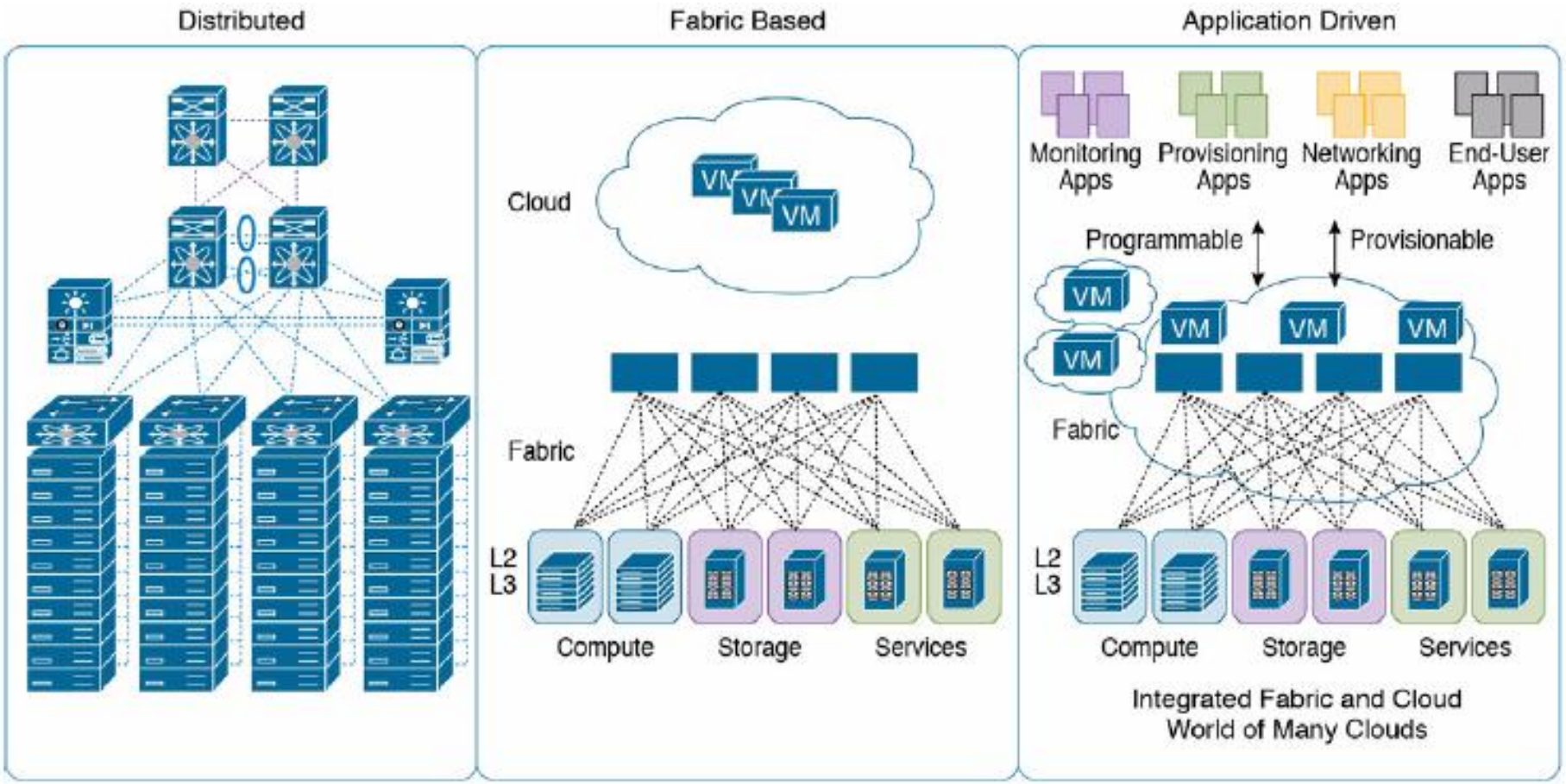
What is a vApp?

- A Cloud Provider using vCloud Director offers catalogs of vApps to their Users
- When cloned, new vApps retain the same MAC and IP addresses
- Duplicate MACs within different vApps requires L2 isolation
- Duplicate IP addresses requires L2/L3 isolation (NAT of externally facing IP addresses)
- Usage of vApps causes an explosion in the need for isolated L2 segments



21

Evolution of Data Center Fabric Architectures



- Manual Provisioning
- Limited scaling
- Rack-wide VM mobility

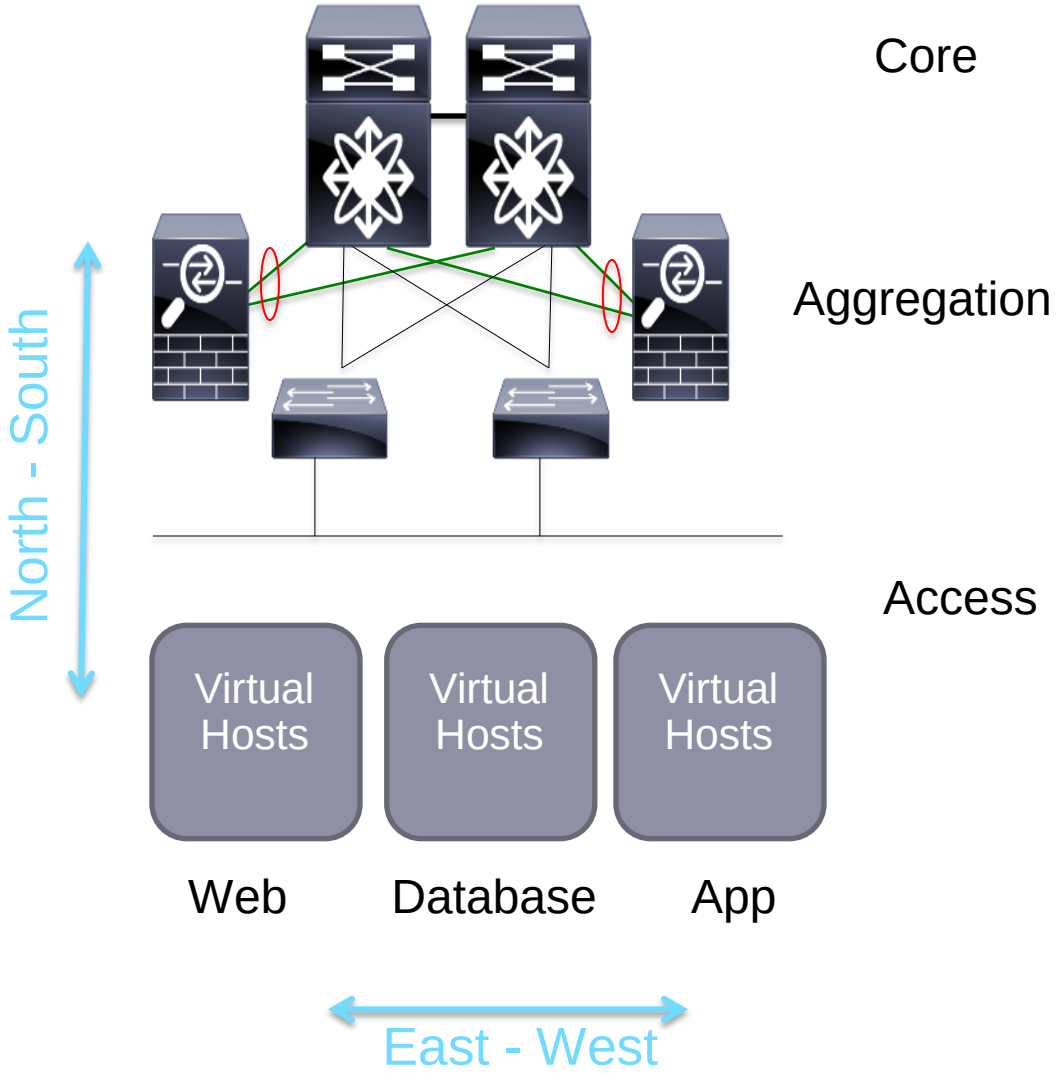
- Policy-based Provisioning
- Scale Physical and Virtual/Cloud
- DC-wide/Cross-DC VM mobility

- Service-centric Provisioning
- Flexible – Anywhere, Anytime
- Cross-cloud VM mobility

347902

What are North-South and East-West Flows?

- North-South (N-S) flows are typically flows to and from Access layer to Aggregation Layer and Core
- East-West (E-W) flows typically stay either within a zone or between zones and often server to server traffic



Problem statement: Evolving Network Requirements ….

- Changing Traffic Flow Requirements: (Cisco's Global Cloud Index): Dominant volume of traffic in the DC traverses in an "East-West" direction (76%), "North-South" traffic (17%), inter-DC traffic (7%)- gradually growing. In campus networks, traffic is primarily (90+%) "North-South" traffic.
- Physical to Virtual Resources - number of hosts huge increase
- Insertion of services {load-balancing, firewalling, IPS/IDS, WAAS, tenant routing}

24

Where do Services go in the Data Center?

- Insertion of services fundamentally drives the logical design (both L2 and L3) within the Data Center: Firewall, Application Firewalls, Application Delivery Controllers, IDS/IPS, Client Routing
- Classic MultiLayer Distributed Data Center Design
  - Services Layer – large scale appliances
  - Virtualized Services as VMs – East-West
- Fabric Based Data Center Design
  - Separate Border Leaf – large scale appliances
  - Virtualized Services as VMs – East-West

Firewalls in the Data Center

Firewall Segmentation

Physical

North-south traffic: Inspecting all traffic into and out of the data center

- Data center edge security appliance inspects all traffic into the data center
- High speed with all services, best with full Intrusion Prevention System (IPS), through a single choke point
- Separates what is outside the network from what is inside (such as north-south traffic)

Virtual / Multitenant

Virtual Edge Firewall

Virtual Firewall – VM Attributes

East-west traffic: Creating secure trust zones between applications and tenants within the data center

Virtual Regular Firewall controls edges

- Separates tenants in large scale multitenant environments – inter-VLAN

Virtual Firewall – VM Attributes

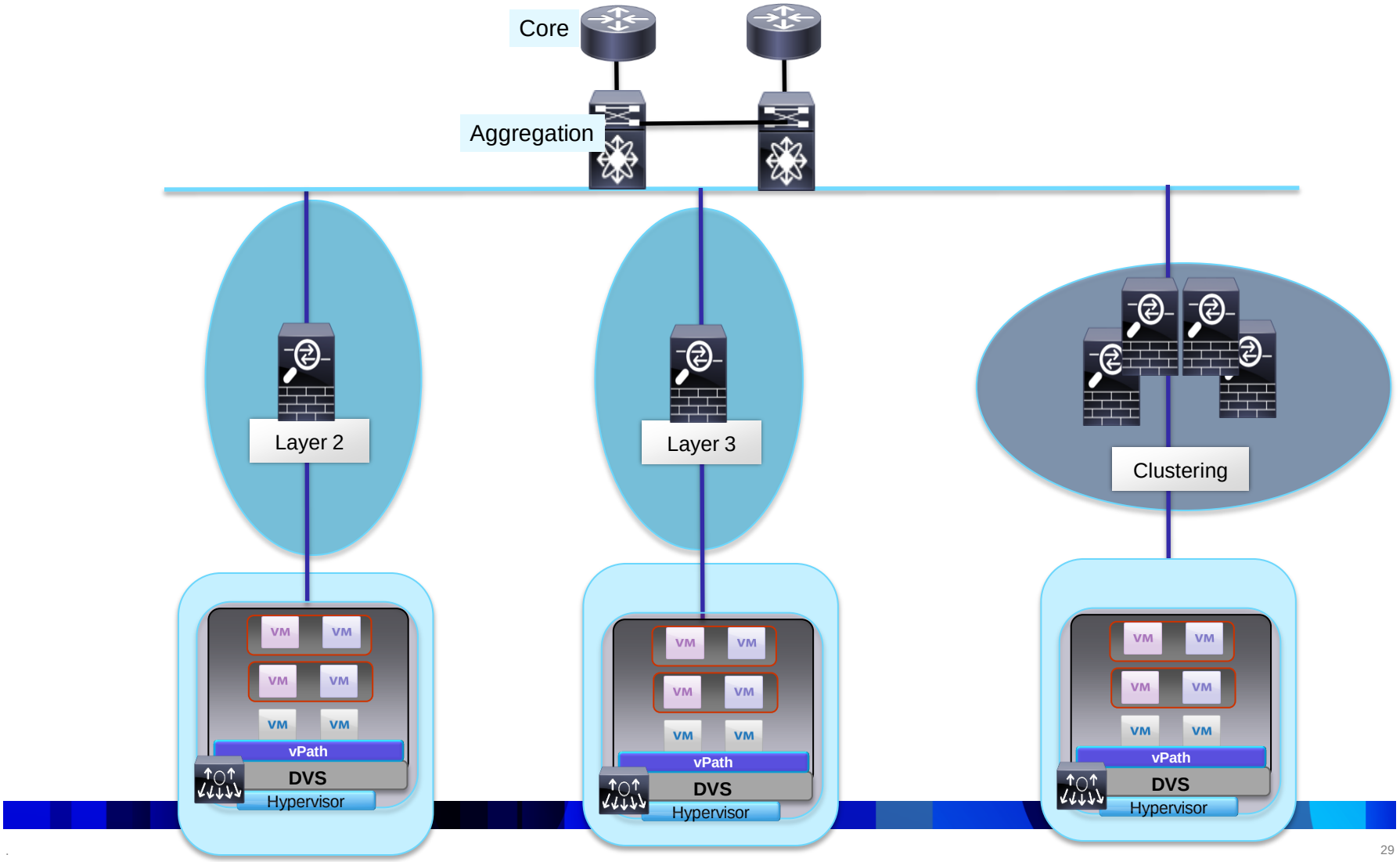
- Separates applications or virtual machines within a single tenant or POD, examples: Cisco VSG, VMWare Vshield: intra-VLAN

Virtualized Firewalls and Virtual Firewalls

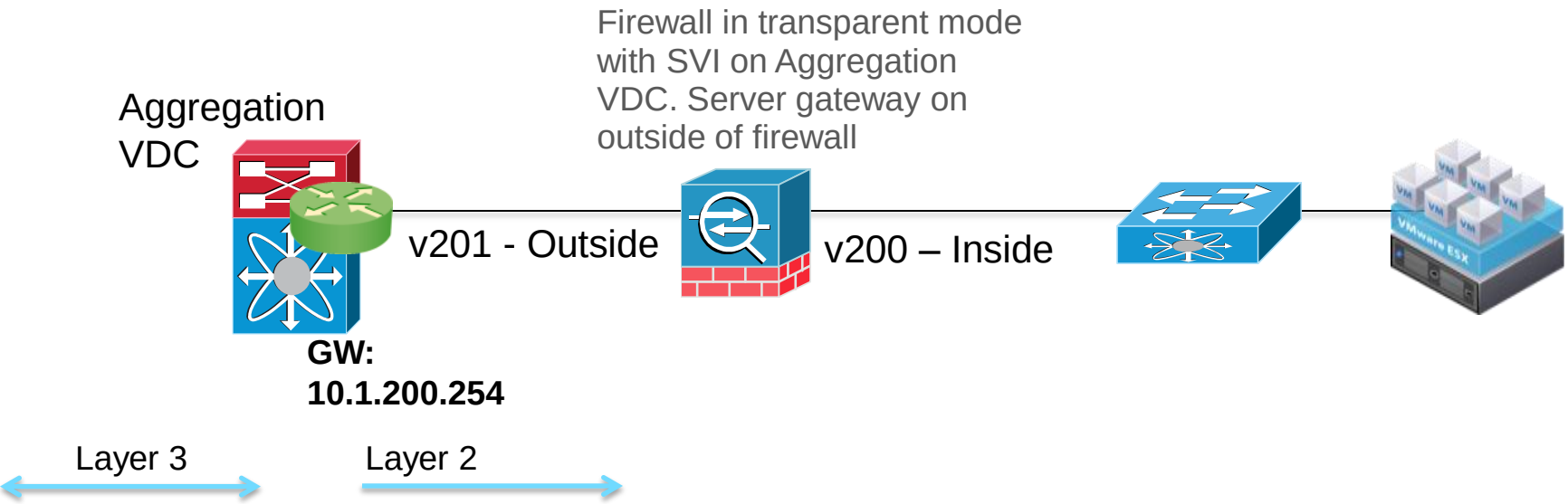
- Two types: multi-context mode and virtual firewalls
- Multi-context mode was originally designed for SMT (Secure Multi Tenant) deployments
- Virtual firewalls are software-only firewalls optimized to work in a hypervisor
- Examples: Cisco Virtual Security Gateway (VSG),ASA1000V,ASAv. VMWare Vshield. Other vendors also have offerings.
- Virtual Firewalls are often tied to the vendor's distributed virtual switch (DVS)
- Virtual firewalls can be deployed rapidly with typical orchestration tools, etc. but there is an added layer of operational complexity
- Virtual firewalls are heavily dependent on available RAM and CPU on the host server

Firewall Deployment

Methods of Operation



Server Gateway Outside of Firewall: Layer 2 Firewalls Explained



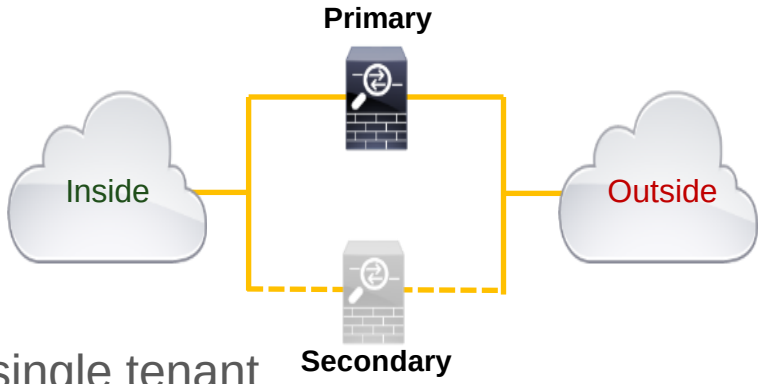
Simple design. Firewall part of layer 2 failure domain.

Transparent Layer 2 Mode

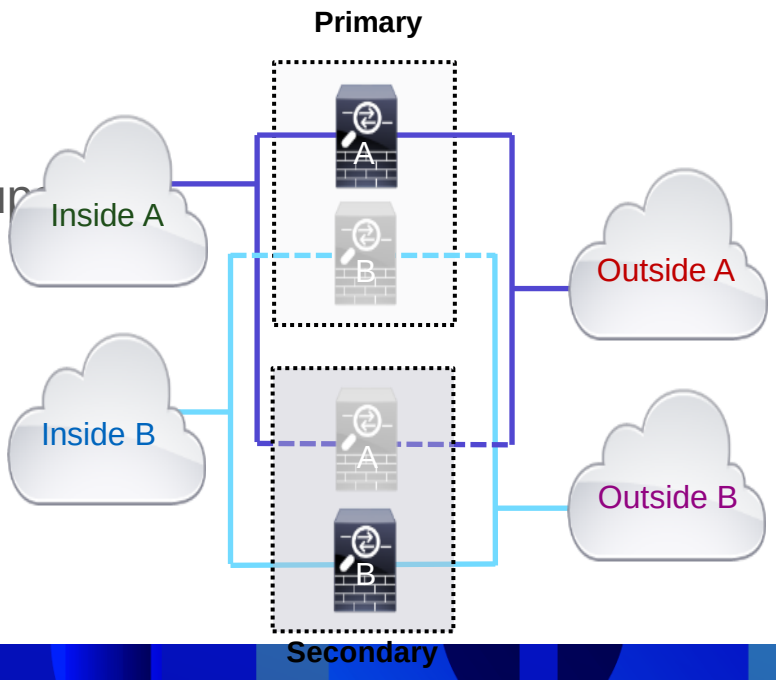
- Firewall functions like a bridge (“bump in the wire”) at L2, only ARP packets pass without an explicit ACL
- Still can use traditional ACLs on the firewall
- **Different VLANs** on inside and outside interfaces but the **same subnet**
- In addition to Extended ACLs, use an EtherType ACL to restrict or allow L2 protocols
- Routing protocols can establish adjacencies through the firewall
- Protocols such as HSRP, VRRP, GLBP can cross the firewall
- Multicast streams can traverse the firewall
- Non-IP traffic can be allowed (IPX, MPLS, BPDUs)
- Deploy where IP address schemes can not be modified

Firewall Failover Types

- Active/Standby Failover
  - Single- or multiple-context mode
  - Device-level switchover on failure
  - One unit is always “idling”
  - Ideal plain and simple design for single tenant



- Active/Active Failover
  - **Requires** multiple-context mode
  - Switchover based on context group
  - Both units are passing traffic
  - Design caveats exist



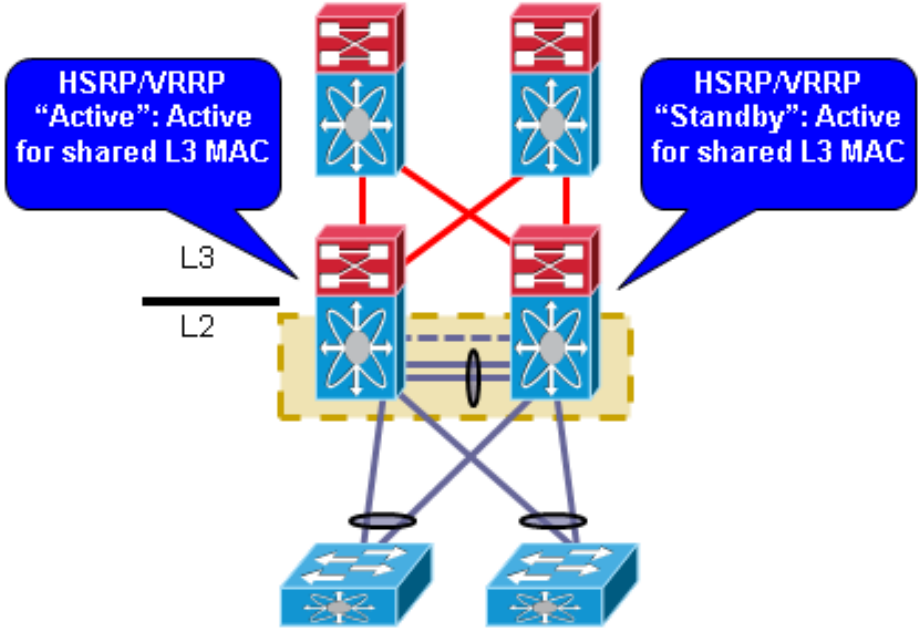
Firewall Clustering

- Clustering was introduced to solve the problem of redundancy with scalability
- Allows for N+1 redundancy with a backup firewall for every active flow
- A Firewall cluster is treated by the network as one logical firewall
- Configuration is synchronized among cluster members
- Three reasons to consider Clustering:
  1. **Redundancy** – no single point of failure, actively using all cluster members
  2. **Scalability** – cluster can grow as requirements increase over time
  3. **Asymmetric flow handling** – the cluster maintains symmetry for all conns

33

Layer 2 or Layer 3 Firewalls?

- Layer 2 better design. You do not want the firewall to be the Default Gateway for the physical and virtual servers. You want that on the high capacity Layer 3 Data Center Switches for redundancy and resiliency reasons. **HSRP, VRRP and GLBP** in vPC environment operate in Active/Active mode and **Anycast HSRP** operates in 4-way active mode in FabricPath environment
- You can overlay Layer 2 firewalls into the DC without having to adjust the ip addressing and routing.



Secure Virtual Containers

The most significant transformation affecting enterprise data centers today is the adoption of server virtualization technology -- **rolling out virtualized servers will require enterprises to invest in new security** solutions in the data center

Drivers are a mix of specific security issues (**preventing new and inter-VM threats**) and configuration/management issues (maintaining server configs, **improving server performance**)

68% of Infonetics' survey respondents name **protecting virtualized servers** an important driver

86% already have a spot in their IT budget for security solutions for their virtualized server environments

82% believe that virtualization fundamentally changes security architecture, but…

…58% deploy security in their virtualized environments using a reliable (but expensive and difficult to manage) solution: installing discreet security applications on each virtual machine

*Infonetics : **Security for Virtualized Infrastructure: North American Enterprise Survey***

Security for Virtualized Servers

Distributed Virtual Switch Port Profiles

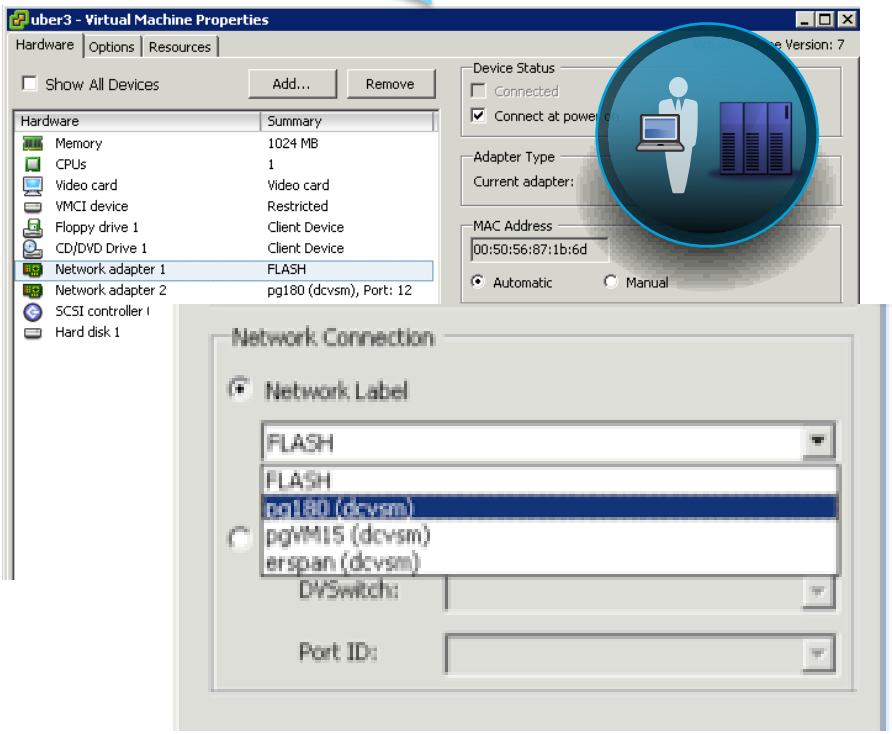
Port Profile –> Port Group

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
```



Distributed Virtual Switch supports:

- ✓ ACLs
- ✓ Quality of Service (QoS)
- ✓ PVLANs
- ✓ Port channels
- ✓ SPAN ports

DVS Service Path Chaining Function

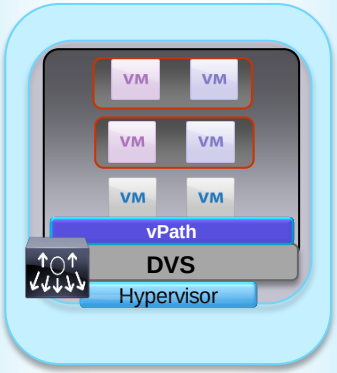
- The vendor DVS must provide service path chaining or the chaining of various services together inside the virtual environment: Server Load Balancers, Virtual Firewalls, Virtual Edge Firewalls, Virtual Web Application Firewalls, Network Sniffers. These are called Virtual Service Nodes
- This is all inside the virtual environment within and between Hypervisors
- Examples: Cisco Vpath, Cisco ACI, and VMWare NSX

Security Services for Virtualization

Virtual Firewall

Intra-Tenant Security

- Secures traffic between virtual machines within a tenant
- Layer 2 and 3 firewall to secure east-to-west traffic
- ACLs using network attributes and virtual machine attributes



Virtual Edge Firewall

Tenant-Edge Security

- Secures the tenant edge
- Default gateway; Layer 3 firewall to secure north-to-south traffic
- Edge firewall capabilities including network attribute-based ACLs, site-to-site VPN, NAT, DHCP, inspections, and IP audit

Virtual Firewall Attributes

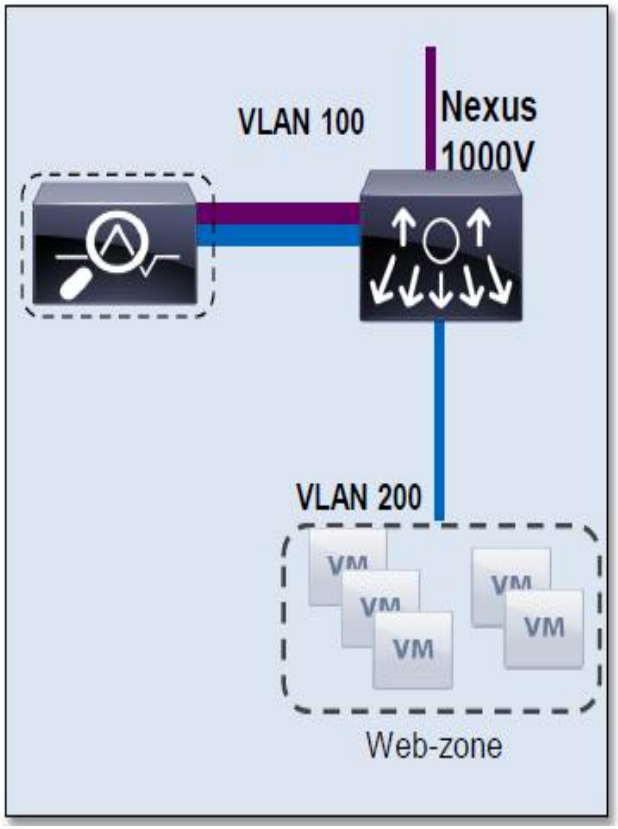
vCenter Example VM Attributes

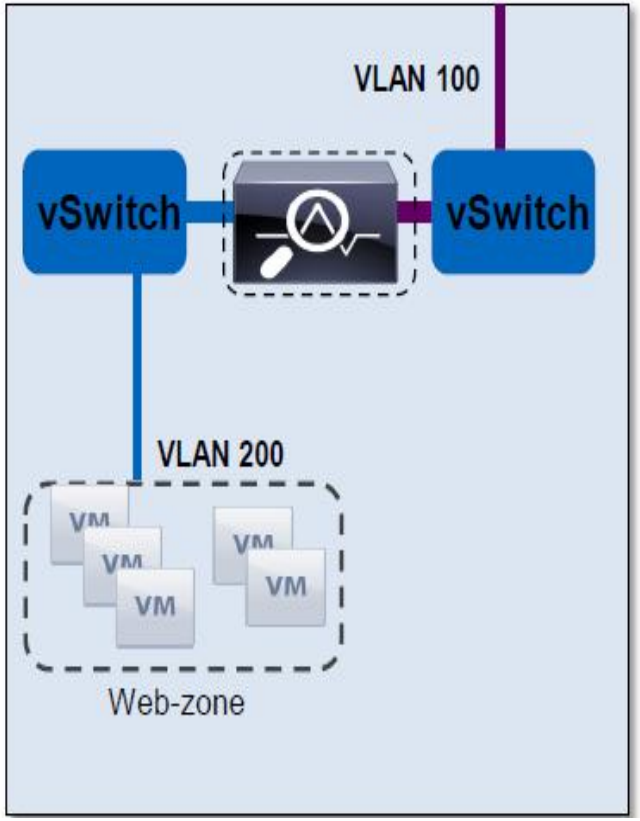
Name	Meaning	Source
vm.name	Name of this VM	vCenter
vm.host-name	Name of this ESX-host	vCenter
vm.os-fullname	Name of guest OS	vCenter
vm.vapp-name	Name of the associated vApp	vCenter
vm.cluster-name	Name of the cluster	vCenter
vm.portprofile-name	Name of the port-profile	Port-profile

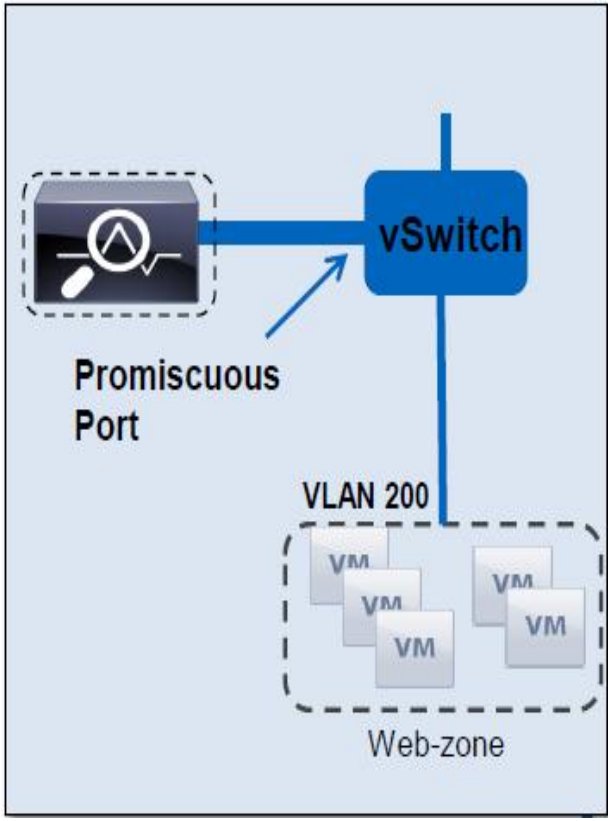
VM attribute information collected is used for enforcing security policy

vIPS

Virtual Switch Inline and Passive Deployment Options

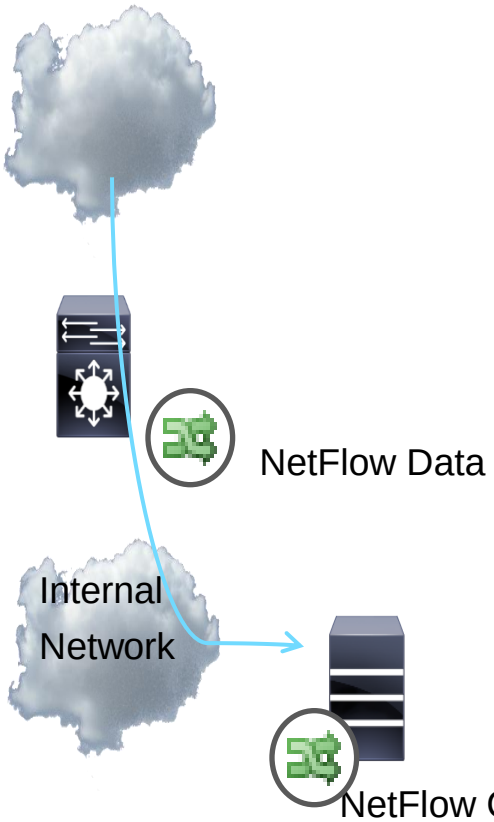






Visibility and Threat Defense

NetFlow in a Nutshell



Usage →	• Packet count • Byte count	• Source IP address • Destination IP address	← From/To
Time →	• Start sysUpTime • End sysUpTime	• Source TCP/UDP port • Destination TCP/UDP port	← Application
Port utilization →	• Input ifIndex • Output ifIndex	• Next hop address • Source AS number • Dest. AS number • Source prefix mask • Dest. prefix mask	← Routing and peering
QoS →	• Type of Service • TCP flags • Protocol		

NetFlow Security Use Cases

- **Detecting Sophisticated and Persistent Threats.** Malware that makes it past perimeter security can remain in the enterprise waiting to strike as lurking threats. These may be zero day threats.
- **Identifying BotNet Command & Control Activity.** BotNets are implanted in the enterprise to execute commands from their Bot herders to send SPAM, Denial of Service attacks, or other malicious acts.
- **Uncovering Network Reconnaissance.** Some attacks will probe the network looking for attack vectors to be utilised by custom-crafted cyber threats.
- **Finding Internally Spread Malware.** Network interior malware proliferation can occur across hosts for the purpose gathering security reconnaissance data, data exfiltration or network backdoors
- **Revealing Data Loss.** Code can be hidden in the enterprise to export of sensitive information back to the attacker. This Data Leakage may occur rapidly or over time.

NetFlow for Security

Can be used to answer the questions:

- Who's talking to whom?
- What is happening on the network?
- Where is the data going?
- Did someone access the payroll server?

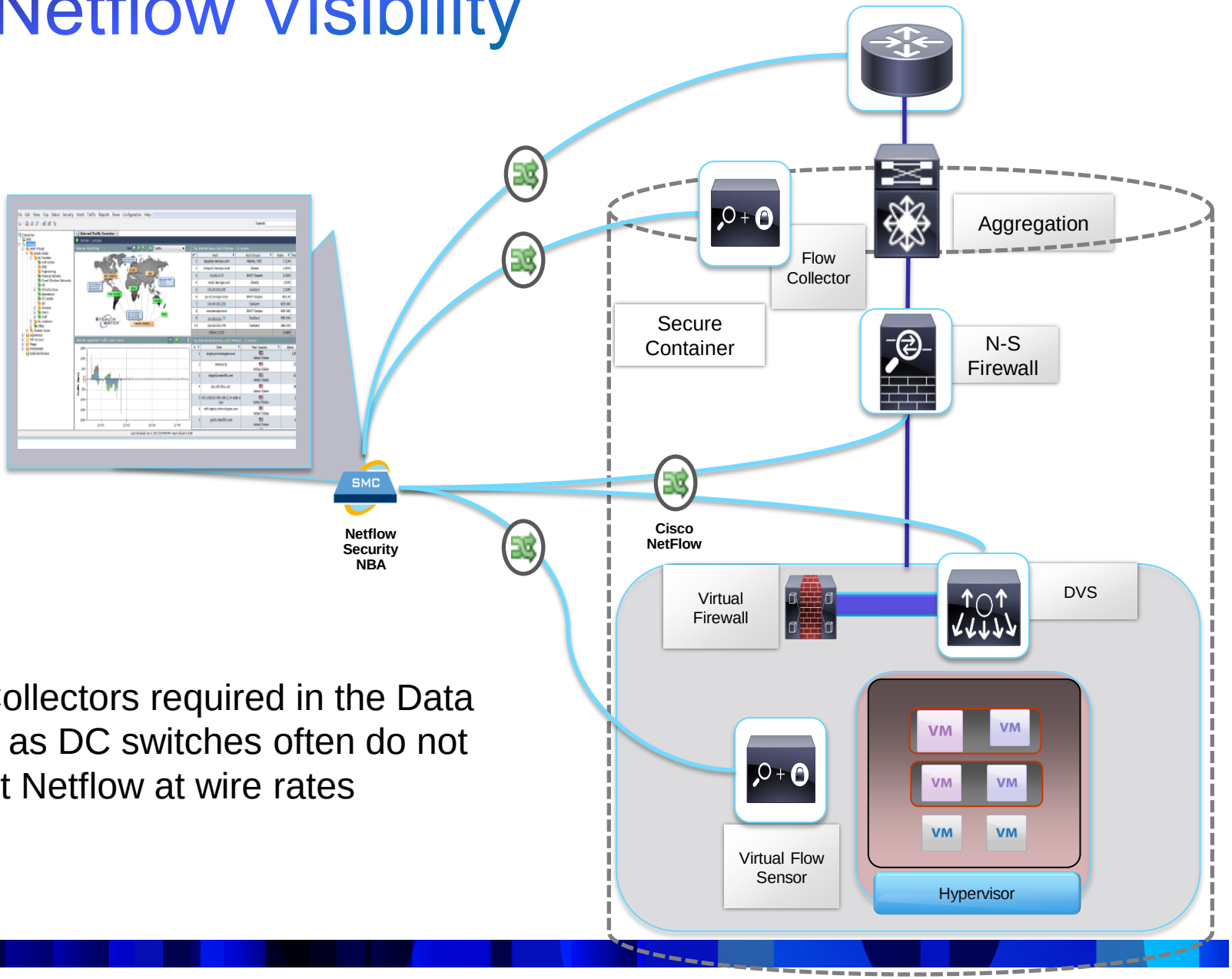
NetFlow requirements for security

- Full Flow capabilities – Unsampled Line Rate
- Aggressive export
- Requires extra fields (new aggregation)

Example: Detecting Data Loss

- Data is often exfiltrated over stealthy channels
  - Hidden inside normal communication payloads
    - Payload padding
  - Encrypted over standard ports
    - TCP port 80, TCP port 443, etc.
  - Standard applications and protocols (ex. SFTP, HTTP, HTTPS)
- Detection requires deep visibility into user and device behaviour
    - Historical data transfers – to establish patterns of communication
    - Applications – is their behaviour “normal”?
    - Time of day – why is Bob transferring data at 2:00 am?
    - Countries – do we really do business with North Korea?

Netflow Visibility



Flow Collectors required in the Data Center as DC switches often do not support Netflow at wire rates