Cisco Cloud Networking

Han Yang
Product Manager, Data Center Group

May, 2013

NDA Discussion

Physical | Virtual | Cloud Journey

PHYSICAL WORKLOAD

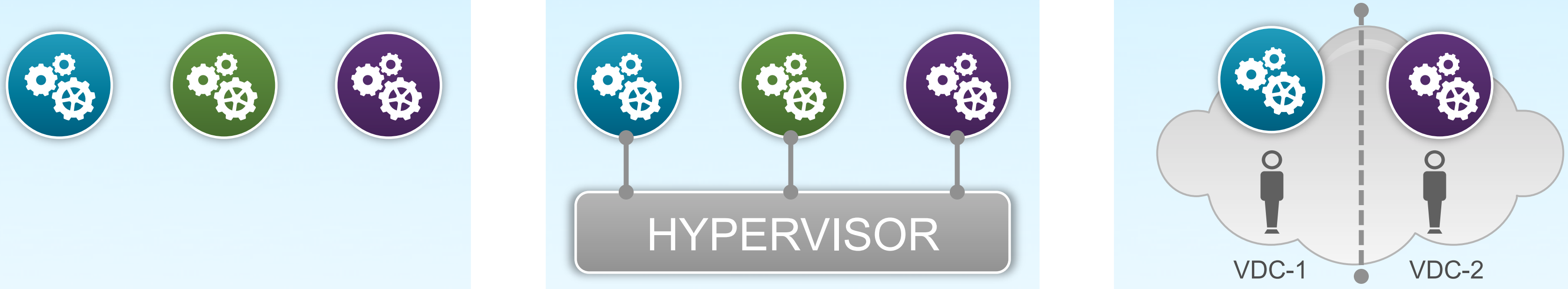
- One app per Server
- Static
- Manual provisioning

VIRTUAL WORKLOAD

- Many apps per Server
- Mobile
- Dynamic provisioning

CLOUD WORKLOAD

- Multi-tenant per Server
- Elastic
- Automated Scaling

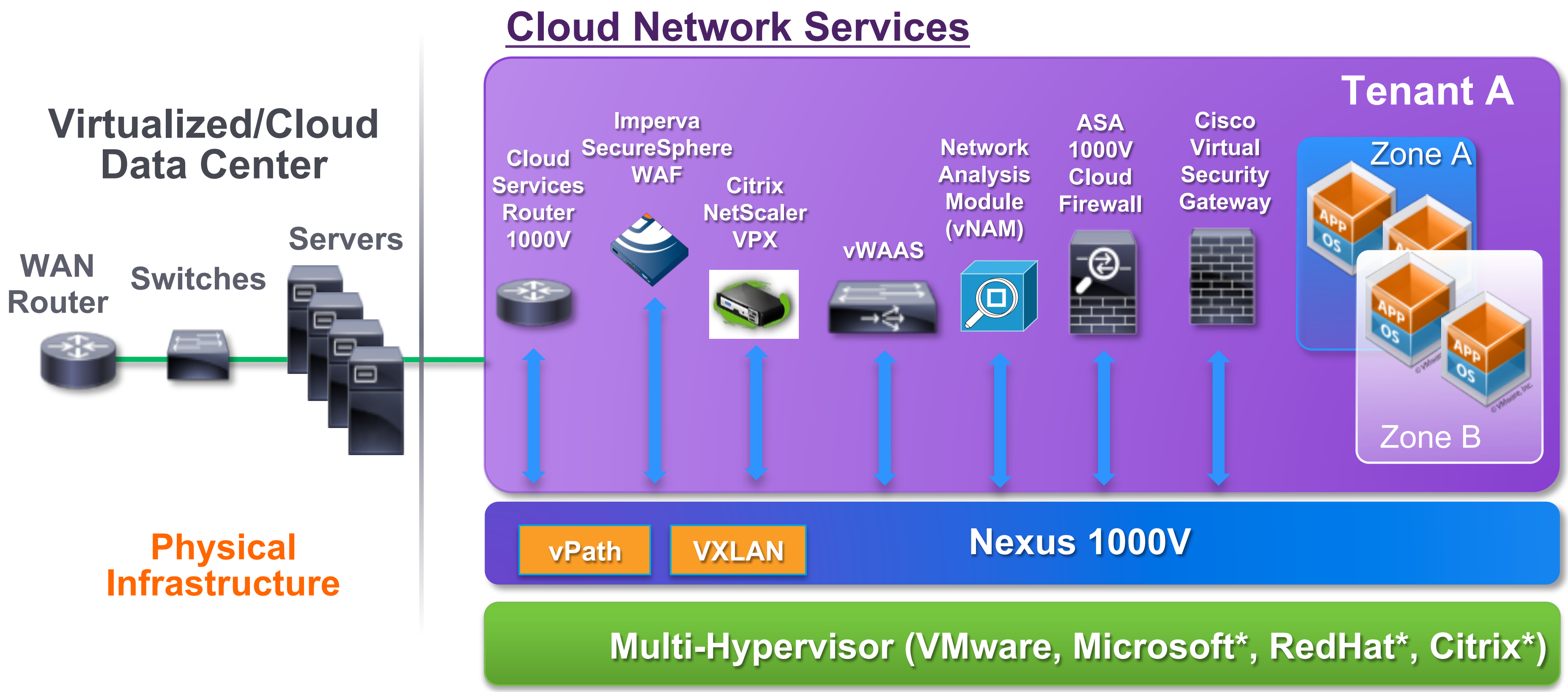


CONSISTENCY: Policy, Features, Security, Management, Separation of Duties

Switching	**Nexus 7K/5K/3K/2K**	**Nexus 1000V, VM-FEX**
Routing	**ASR, ISR**	**Cloud Services Router (CSR 1000V)**
Services	**WAAS, ASA, NAM**	**vWAAS, VSG, ASA 1000V, vNAM****
Compute	**UCS for Bare Metal**	**UCS for Virtualized Workloads**

** 1H 2013

Cisco Virtual Networking and Cloud Network Services



Virtualized/Cloud Data Center

WAN Router

Switches

Servers

Physical Infrastructure

Cloud Network Services

Tenant A

Cloud Services Router 1000V

Imperva SecureSphere WAF

Citrix NetScaler VPX

vWAAS

Network Analysis Module (vNAM)

ASA 1000V Cloud Firewall

Cisco Virtual Security Gateway

Zone A

Zone B

vPath

VXLAN

Nexus 1000V

Multi-Hypervisor (VMware, Microsoft*, RedHat*, Citrix*)

Nexus 1000V

- Distributed switch
- NX-OS consistency

7000+ Customers (on VMW)

VSG

- VM-level controls
- Zone-based FW

Shipping (on VMW)

ASA 1000V

- Edge firewall, VPN
- Protocol Inspection

Shipping (on VMW)

vWAAS

- WAN optimization
- Application traffic

Shipping (on VMW)

CSR 1000V (Cloud Router)

- WAN L3 gateway
- Routing and VPN

Shiping

Ecosystem Services

- Citrix NetScaler VPX virtual ADC
- Imperva Web App. Firewall

2013

Cisco-Citrix Alliance Webinar: - *Oct 22, 2012* (Webinar, PPT)
Imperva WAF update: *June 5th, 2012* (Email Annoucement, Imperva FAQ)

vNAM: Q2 CY13

Virtual Overlay Networks

Example: Virtual Overlay Networks and Services with Nexus 1000V

- **Scalable Multi-tenancy**

  Tens of thousands of virtual ports, L2 networks

  Hundreds of Servers

  Scalable segmentation: VXLAN

- **Common APIs**

  Incl. OpenStack Quantum API's for cloud automation/orchestration

- **Virtual Services**

  vPath for traffic steering / service chaining

  VSG, ASA 1000V (cloud-ready security), vWAAS (application acceleration)

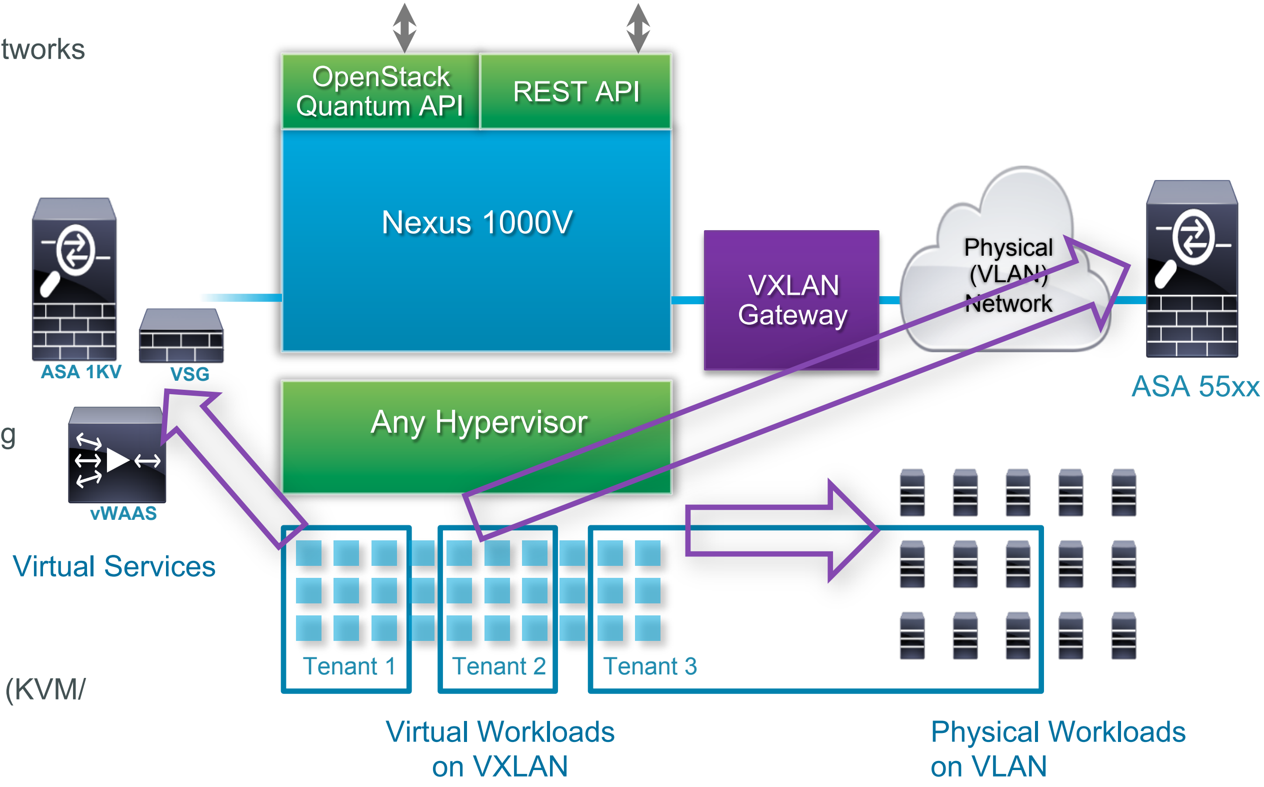
  CSR 1000V (cloud router)

- **Multi-hypervisor**

  ESX, Hyper-V, OpenSource Hypervisors (KVM/ Xen)

- **Hybrid Use Cases** (Physical and Virtual)

  VXLAN to VLAN GW

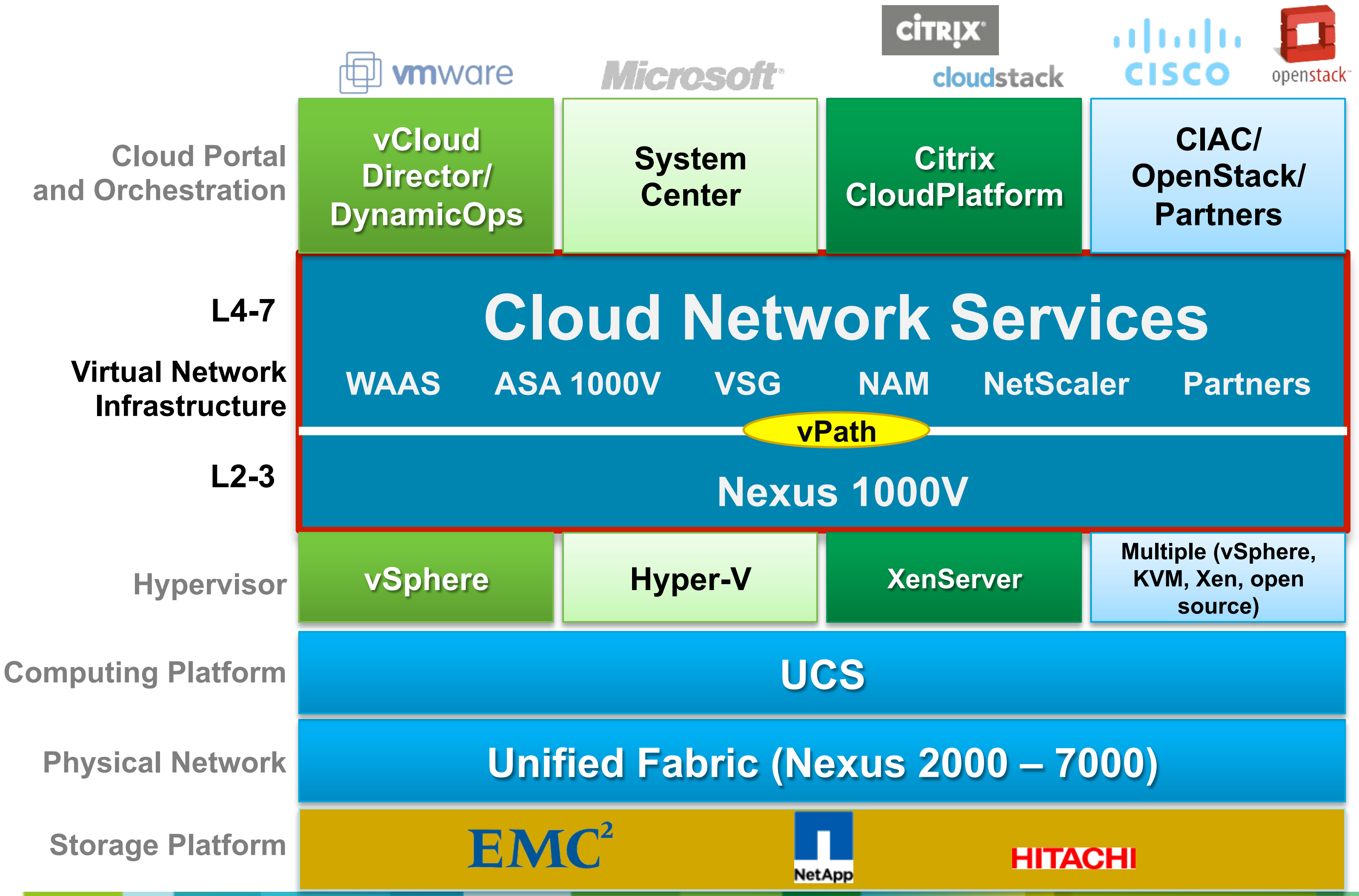


Tenant 1: virtual workloads protected by virtual firewall

Tenant 2: virtual workloads protected by physical firewall (via VXLAN GW)

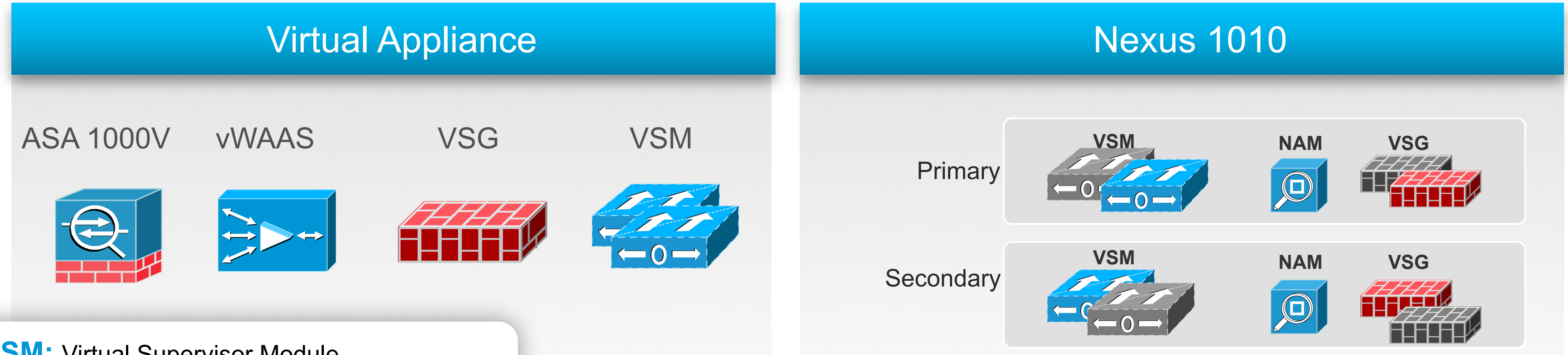
Tenant 3: virtual & physical workloads in same L2 domain (via VXLAN GW

Cloud Network Services



Cloud Portal and Orchestration	vCloud Director/ DynamicOps	System Center	Citrix CloudPlatform	CIAC/ OpenStack/ Partners
L4-7 Virtual Network Infrastructure	Cloud Network Services WAAS ASA 1000V VSG NAM NetScaler Partners vPath			
L2-3	Nexus 1000V			
Hypervisor	vSphere	Hyper-V	XenServer	Multiple (vSphere, KVM, Xen, open source)
Computing Platform	UCS			
Physical Network	Unified Fabric (Nexus 2000 – 7000)			
Storage Platform	EMC²	NetApp	HITACHI	

Cisco Nexus 1000 Portfolio



VSM: Virtual Supervisor Module

VEM: Virtual Ethernet Module

vPath: Virtual Service Data-path

VXLAN: Scalable Segmentation

VSG: Virtual Security Gateway

vWAAS: Virtual WAAS

ASA 1000V: Tenant-edge security

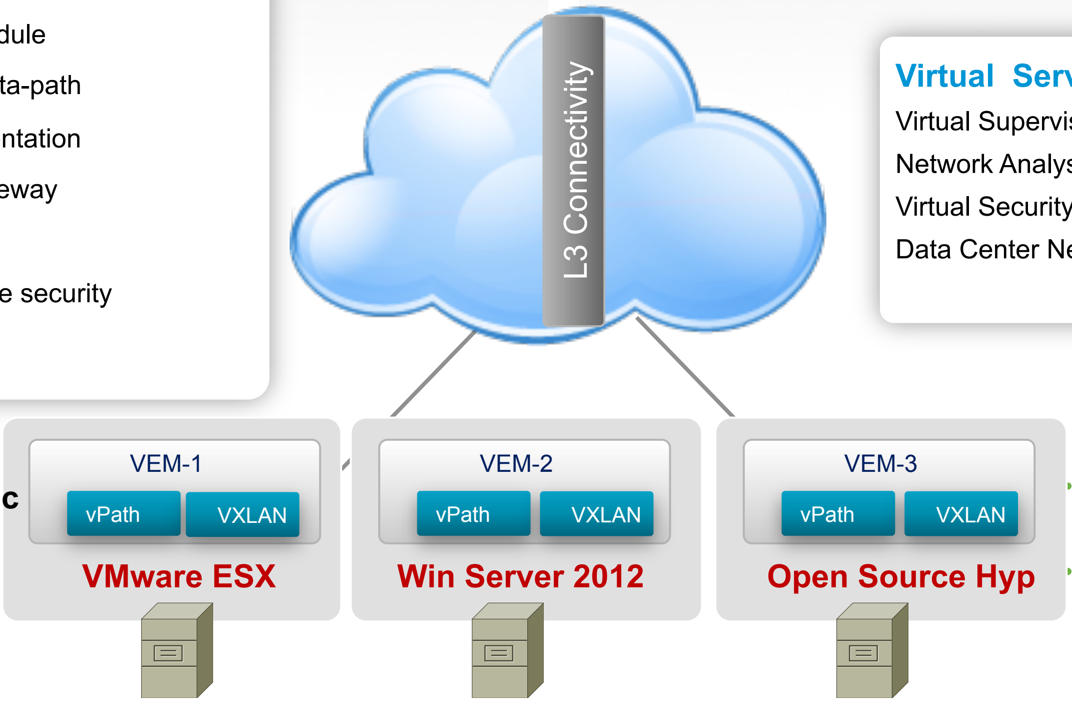
Virtual Service Blades

Virtual Supervisor Module (VSM)

Network Analysis Module (NAM)

Virtual Security Gateway (VSG)

Data Center Network Manager (DCNM)



vPath

- Service Binding (Traffic Steering)
- Fast-Path Offload
- Service Chaining

VXLAN

- 16M address space for LAN segments
- Network Virtualization (Mac-over-UDP)

New Nexus 1000V Freemium Go-To-Market Model

No-Cost Version

Nexus 1000V **Essential** Edition

The world's most advanced virtual switch

- Full Layer-2 Feature Set
- Security, QoS Policies
- VXLAN virtual overlays
- Full monitoring and management capabilities
- vPath enabled Virtual Services

$695 per CPU MSRP

Nexus 1000V **Advanced** Edition

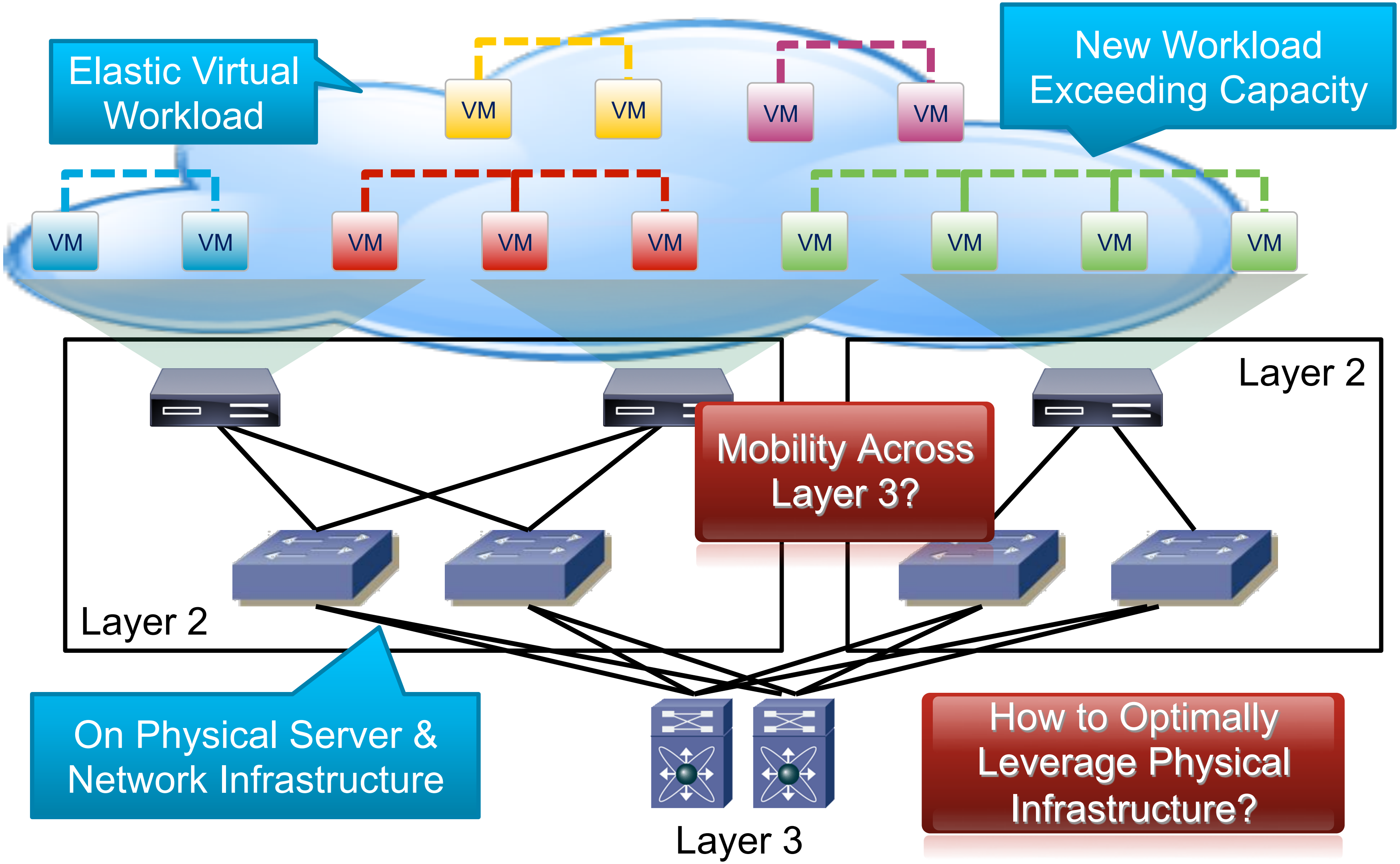
Adds Cisco value-add features for DC and Cloud

- All Feature of Essential Edition
- VSG firewall bundled (previously sold separately)
- Support for Cisco TrustSec SGA policies
- Platform for other Cisco DC Extensions in the Future

Freemium Pricing Model Offers Flexibility for Customers to Deploy Cisco Virtual Data Center

Virtual Extensible Local Area Network (VXLAN)

Virtual Workload on Physical Data Center



Elastic Virtual Workload

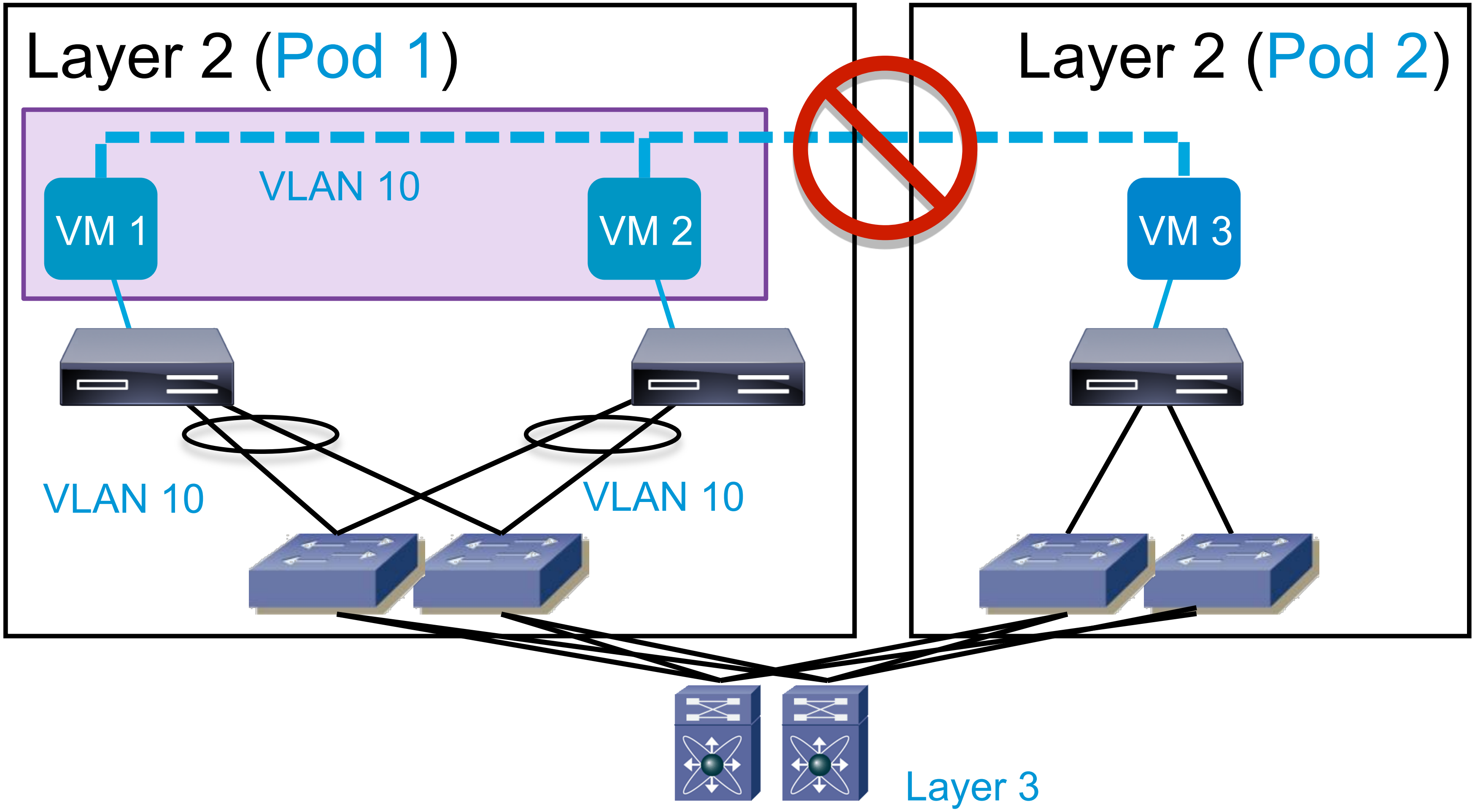
New Workload Exceeding Capacity

Mobility Across Layer 3?

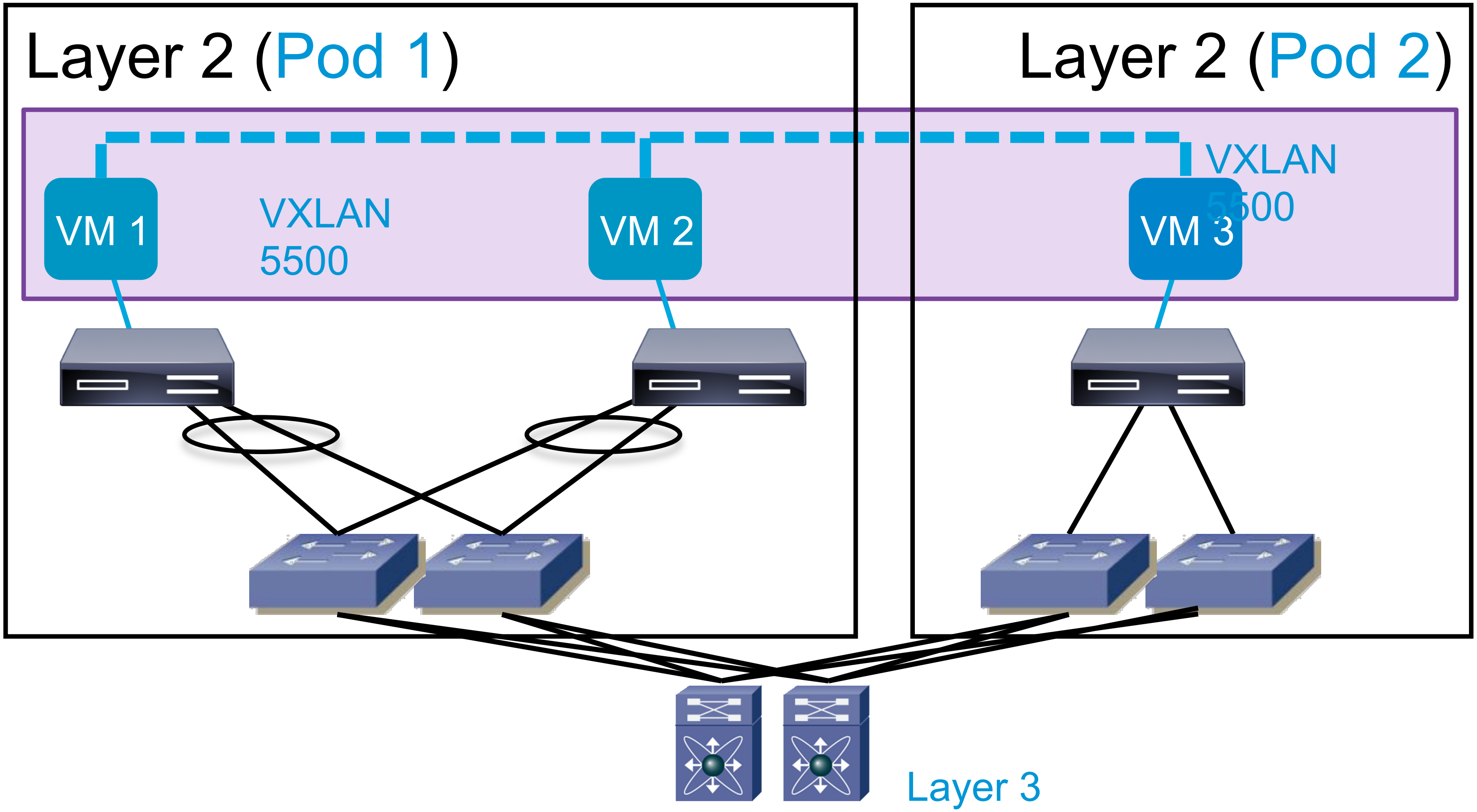
On Physical Server & Network Infrastructure

How to Optimally Leverage Physical Infrastructure?

Existing Solution: Reachability of VMs Within VLAN



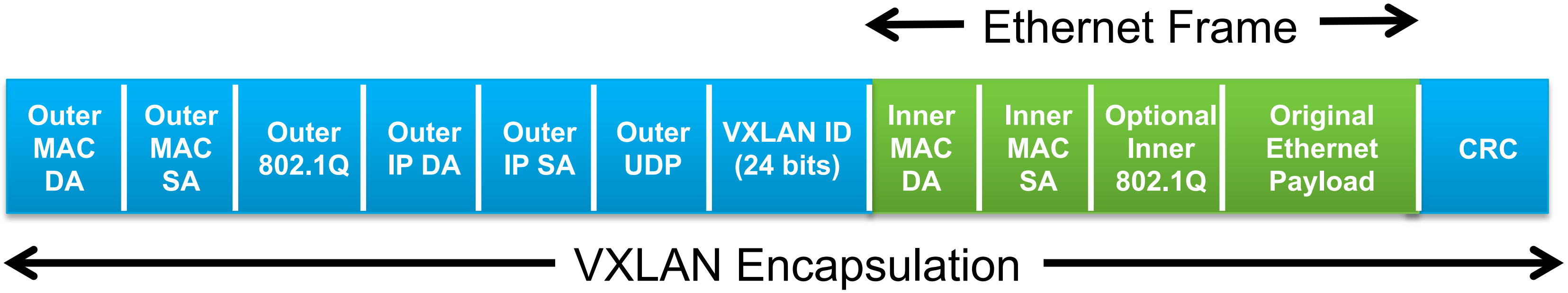
VXLAN: Reachability Across Layer 3



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 VMware, Citrix, Red Hat, and Others

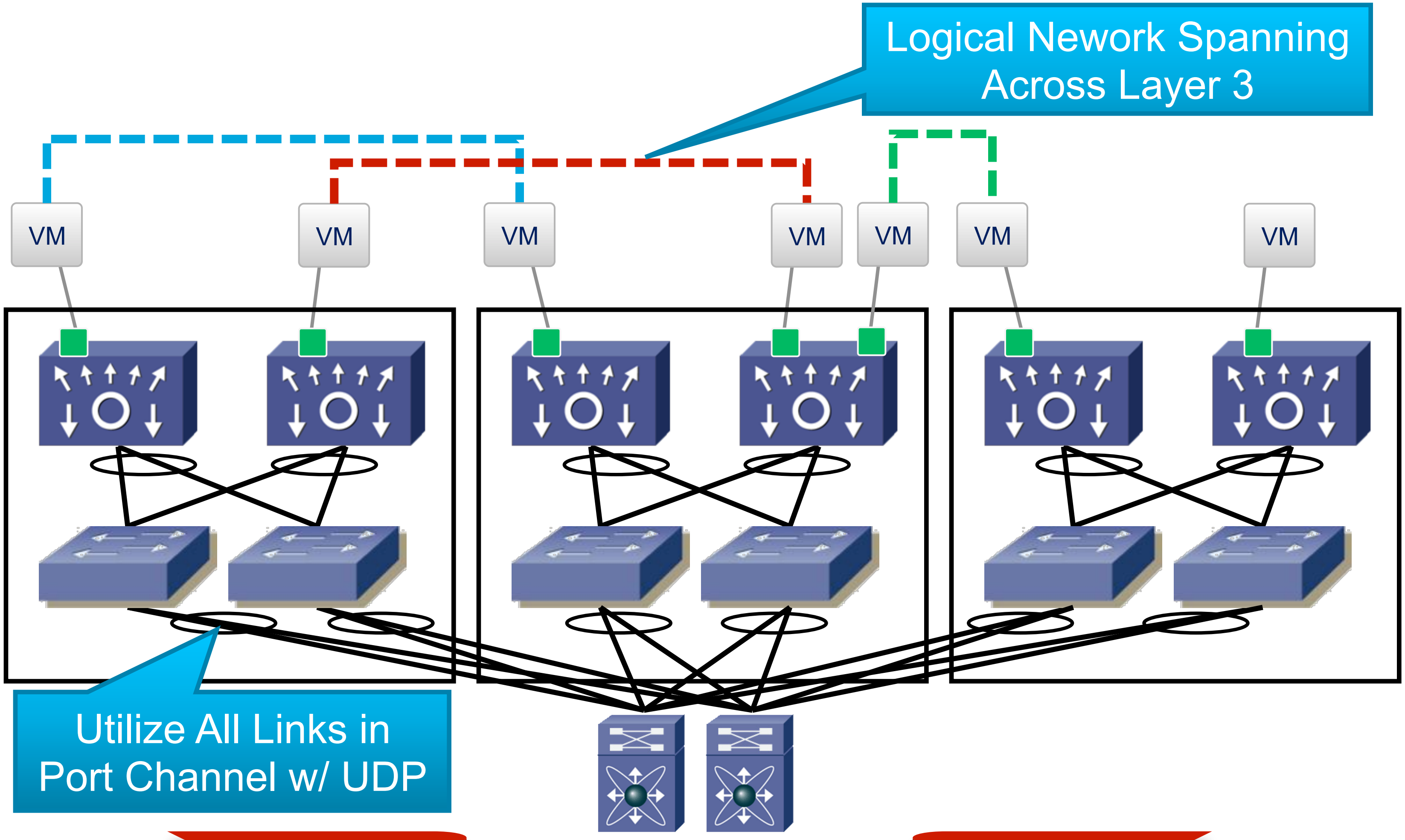


Ethernet Frame

Outer MAC DA | Outer MAC SA | Outer 802.1Q | Outer IP DA | Outer IP SA | Outer UDP | VXLAN ID (24 bits) | Inner MAC DA | Inner MAC SA | Optional Inner 802.1Q | Original Ethernet Payload | CRC

VXLAN Encapsulation

Scalable Pod Deployment with VXLAN within a Data Center

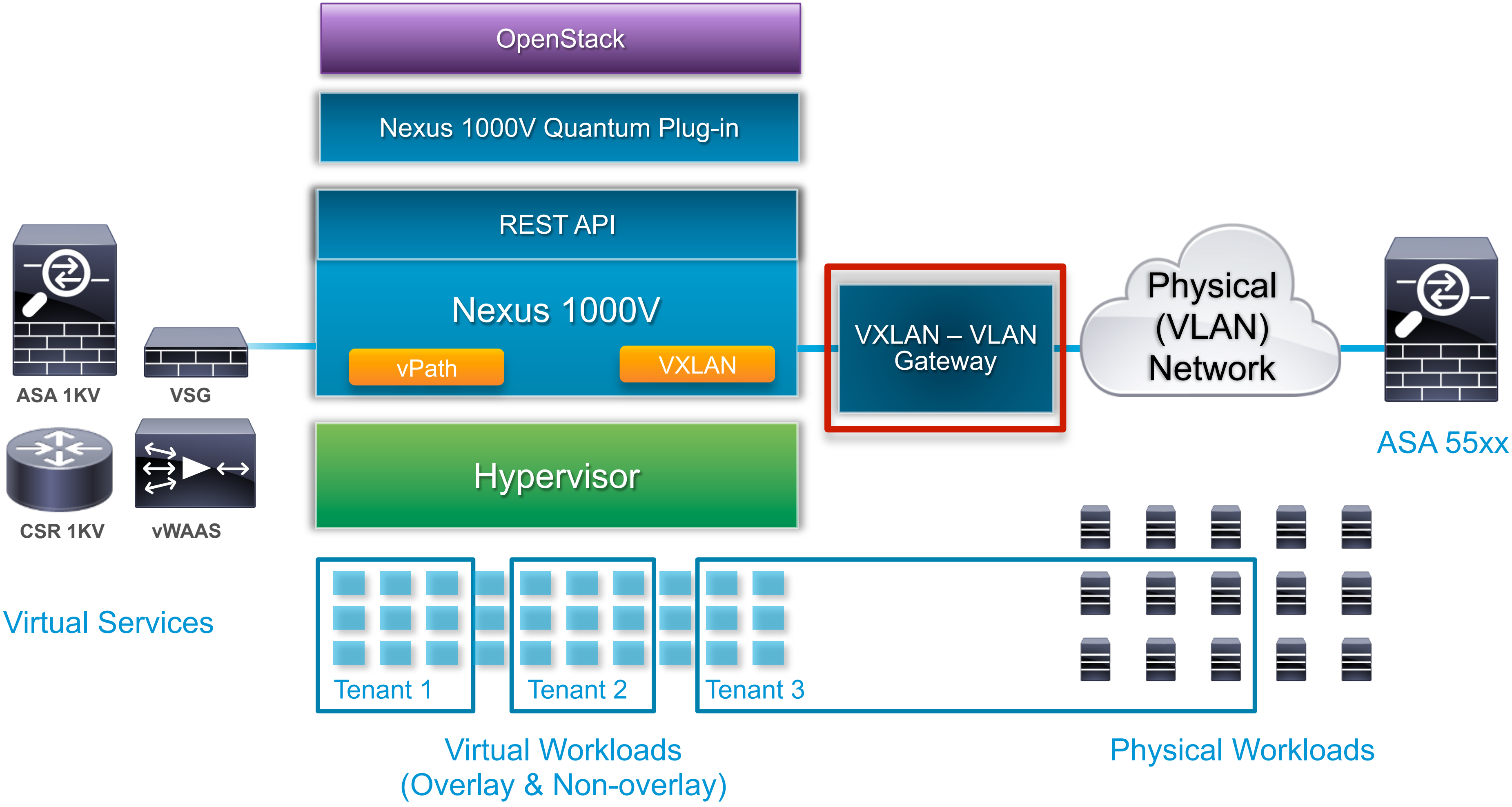


Logical Nework Spanning Across Layer 3
VM
VM
VM
VM
VM
VM
VM
Utilize All Links in Port Channel w/ UDP

Add More Pods to Scale

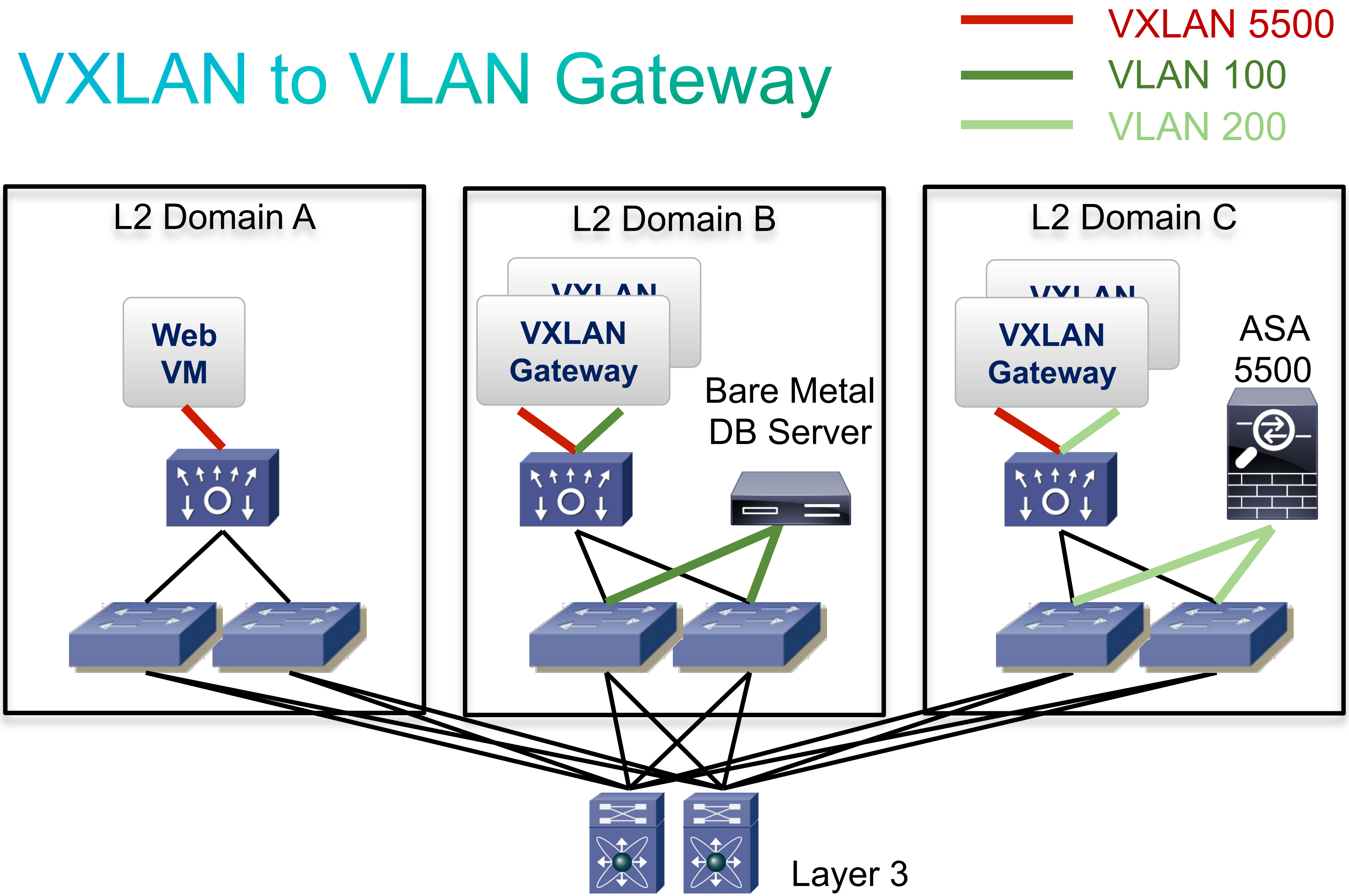
Seamless Interactions Across Virtual & Physical

Tenant Definition can include Physical Services & Physical Workloads



* VXLAN GW & OpenStack Quantum support announced

VXLAN to VLAN Gateway



Increasing Scale

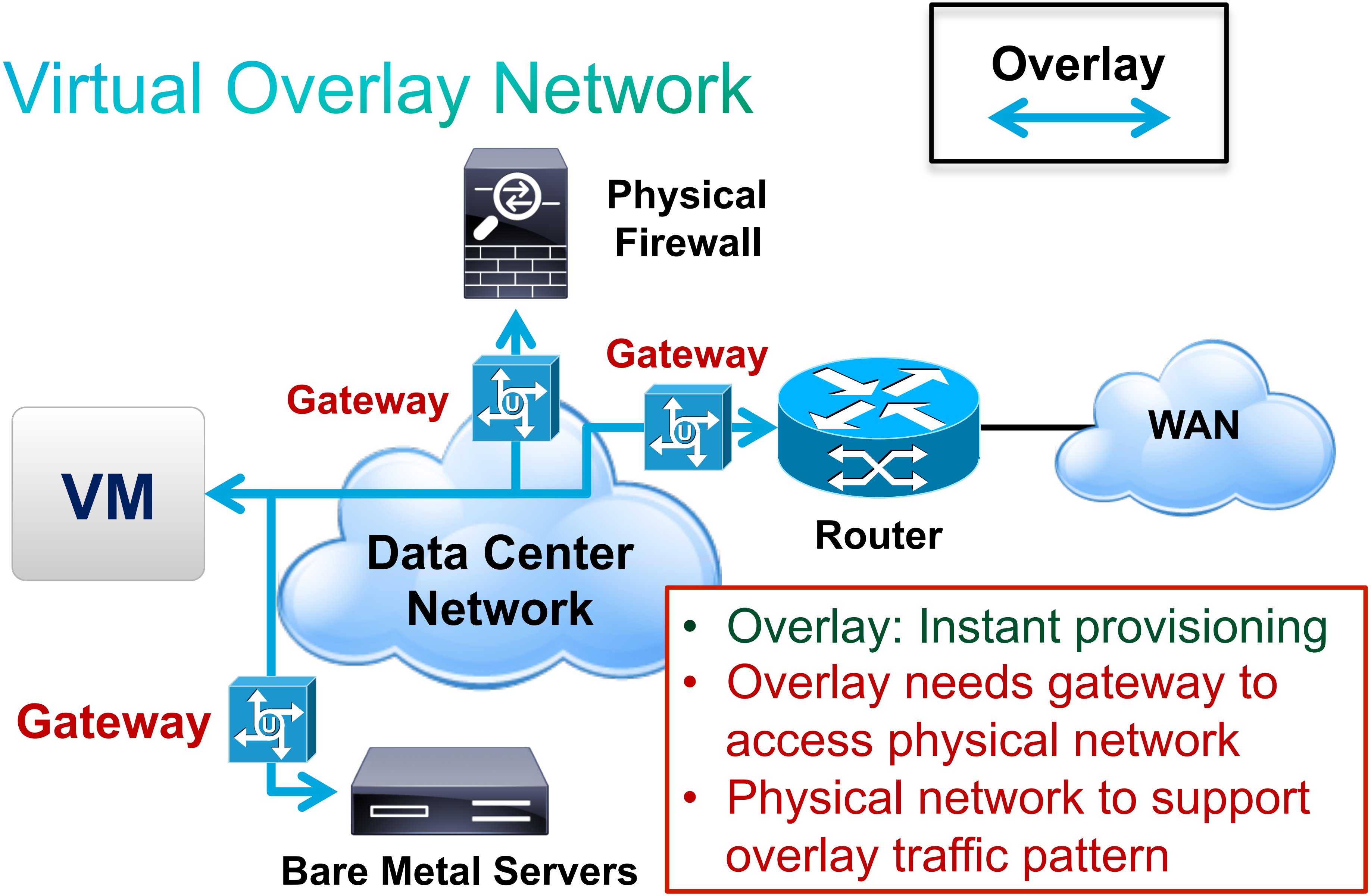
Rearchitected for Resiliency & Scale

- Migrating workload from VSM to VEM
- Loosely Coupled between VSM and VEM
- vMotion even when VSM is disconnected from VEM

Target Scale

- Veths/VSM: 16-32k
- VEMs/VSM: 256-512
- Veths/VEM: 300+
- Active VLANs: 4,096
- Active VXLANs: 16,384

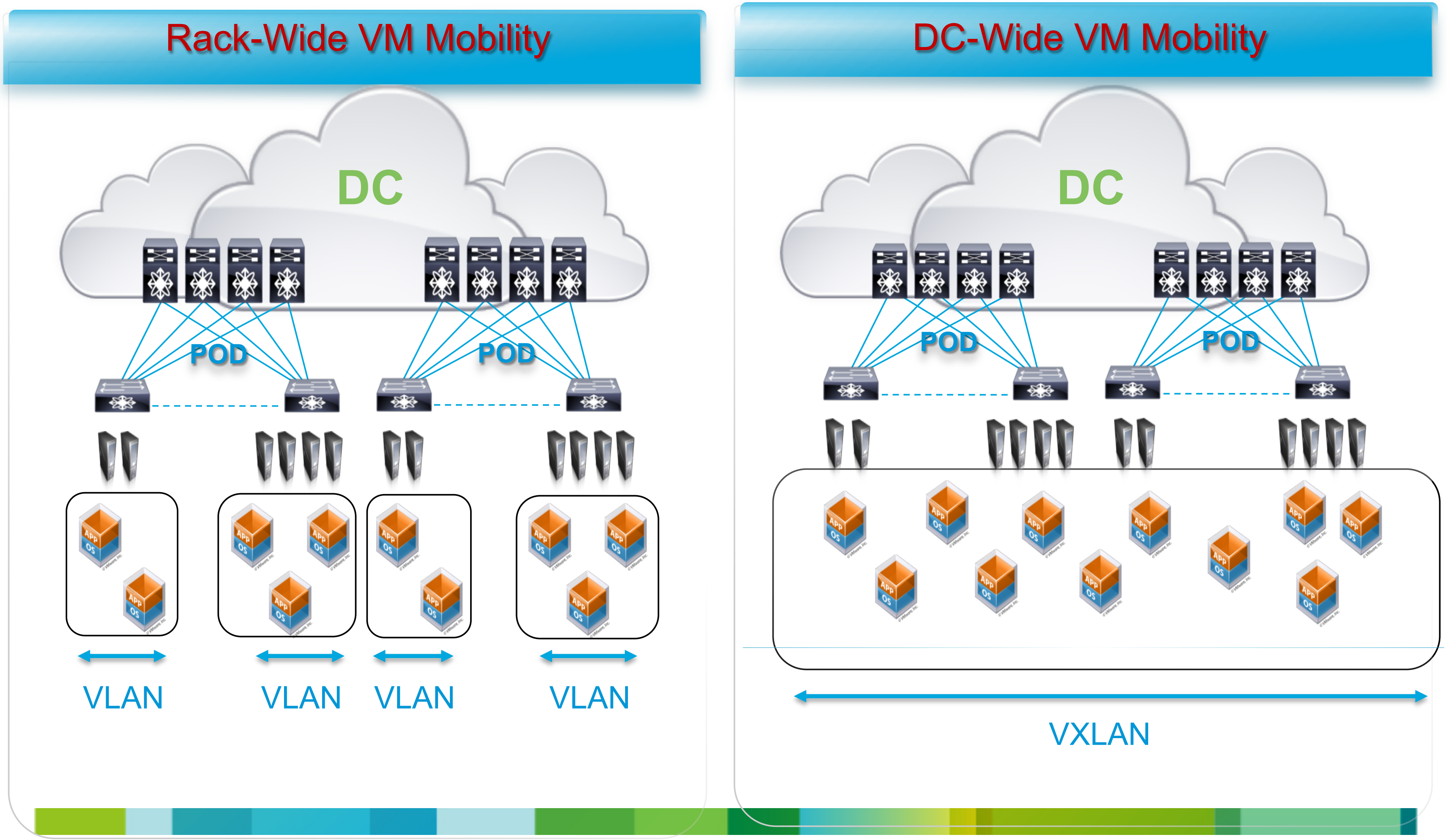
Virtual Overlay Network



- Overlay: Instant provisioning
- Overlay needs gateway to access physical network
- Physical network to support overlay traffic pattern

Broaden Mobility Domain with VXLAN

Unprecedented Infrastructure Flexibility



Rack-Wide VM Mobility

DC-Wide VM Mobility

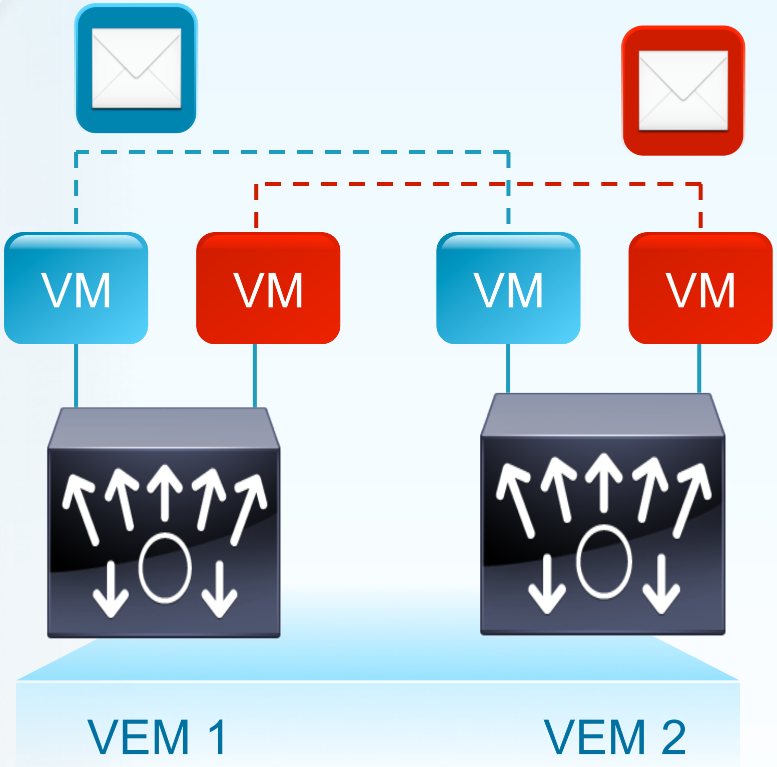
Enhanced VXLAN

Enhanced VXLAN - Forwarding Basics

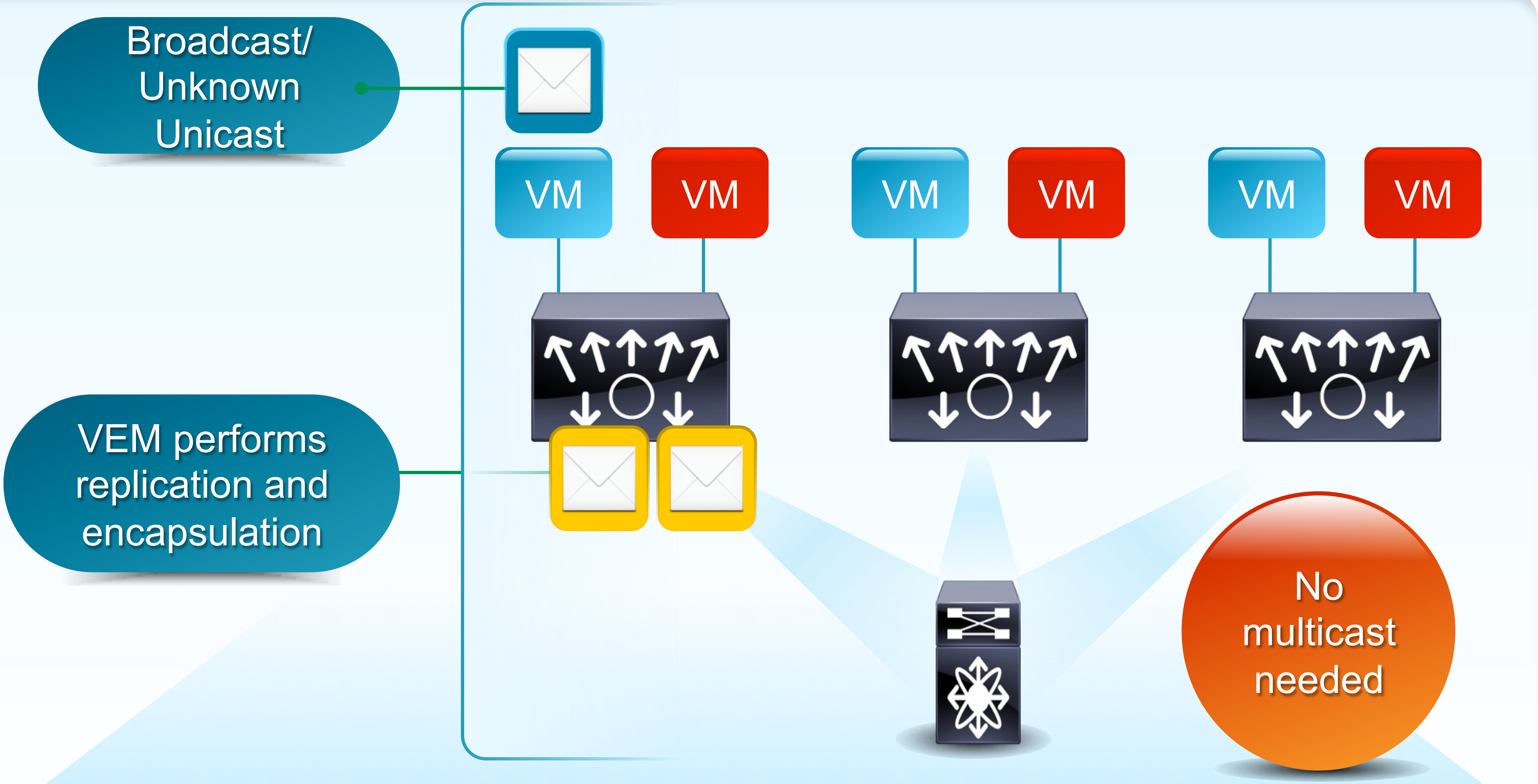
- Forwarding mechanisms similar to Layer 2 bridge: Flood and learn
  - VEM learns VM's source (MAC, host) tuple

- Broadcast, multicast, and unknown unicast traffic
  - VM broadcast, multicast, and unknown unicast traffic is replicated for each host having VMs in same VXLAN. Packet is encapsulated with destination IP set to the host's VXLAN IP.

- Unicast User
  - Unicast packets are encapsulated and sent directly (not through multicast) to destination host VXLAN IP (destination VEM)



Broadcast and Unknown Unicast in Enhanced VXLAN

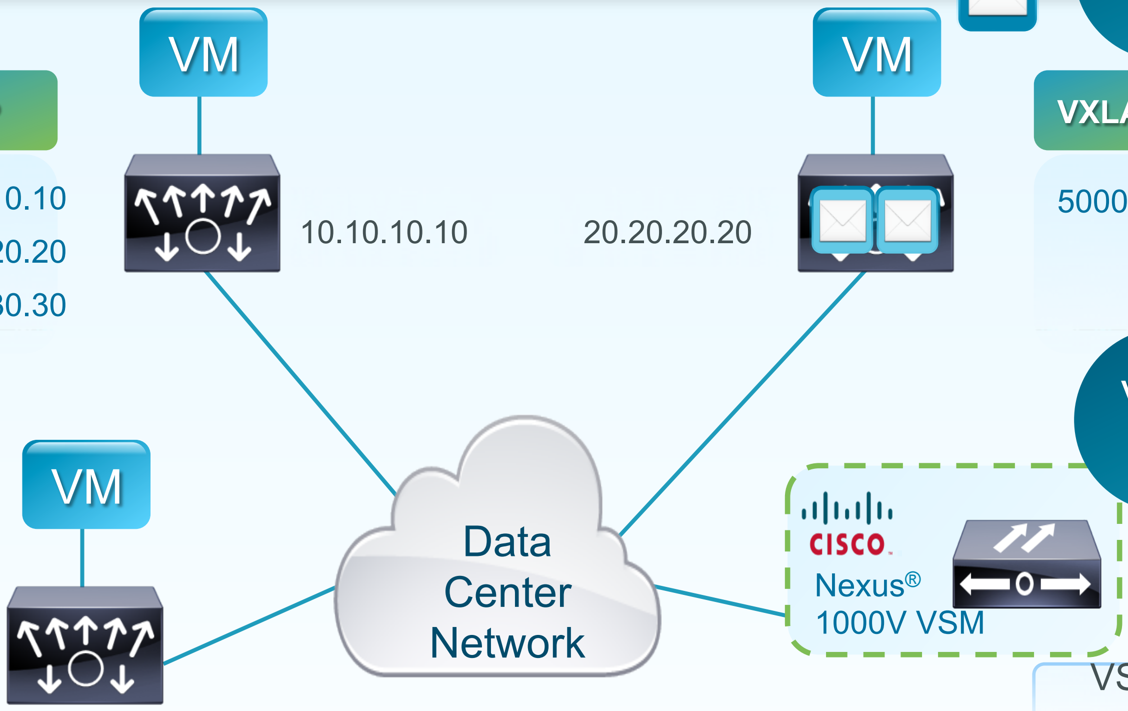


Broadcast/ Unknown Unicast

VEM performs replication and encapsulation

No multicast needed

Enhanced VXLAN -- Broadcast, Multicast, Unknown Unicast



Broadcast/ARP Requirement

VEM VTEP Table

VXLAN	VTEP
5000	10.10.10.10 20.20.20.20 30.30.30.30

VEM learns VXLAN/VTEP

VXLAN	VTEP
5000	10.10.10.10 20.20.20.20 30.30.30.30

VSM distributes VXLAN/VTEP

Encapsulated packet sent to all VTEPs with VXLAN 5000

VEM VTEP Table

VXLAN	VTEP
5000	10.10.10.10 20.20.20.20 30.30.30.30

VSM learns VXLAN/VTEP from VEMs

VSM VTEP Table

VXLAN	VTEP
5000	10.10.10.10 20.20.20.20 30.30.30.30

Enhanced VXLAN – Forwarding Enhancements

MAC Distribution

Security enhancement that prevents malicious VMs from causing ”unknown unicast” broadcast storms

VEM learns all (VXLAN, MAC)
from VSM

When VEM receives a MAC from VM in a VXLAN, if MAC is not found in the MAC table the frame is dropped.

Local ARP Termination

VEM terminates ARP locally for VMs in VXLAN reducing ARP broadcast traffic

VSM aggregates and distributes (VXLAN, IP, MAC) entries to VEMs

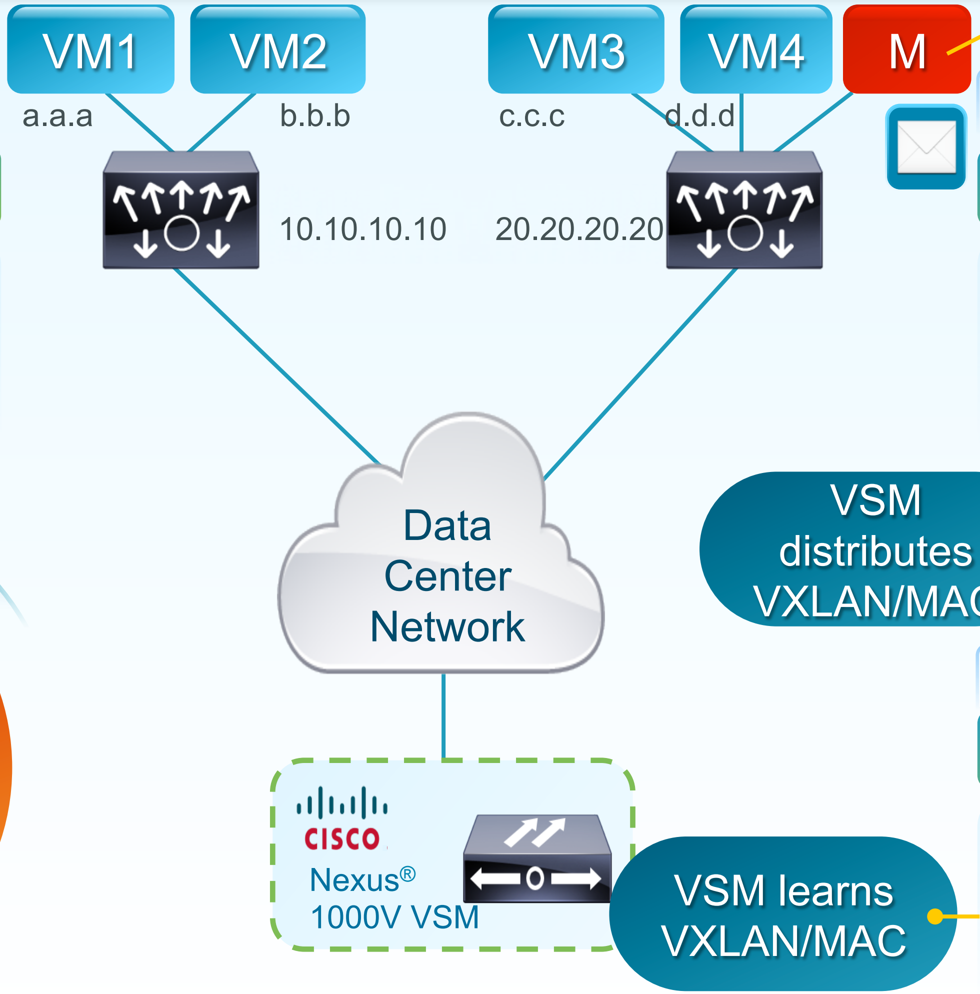
When VEM receives an ARP request, VEM looks up the MAC/ IPDB for MAC address of host

VEM replies to ARP request with MAC address of the destination VM

VXLAN MAC Distribution – Prevents Unknown Unicast Flood

VEM IP / MAC Table

VXLAN	IP/MAC
5000	a.a.a
	b.b.b
	c.c.c
	d.d.d



Malicious VM Send unicast to MAC_X

VEM IP / MAC Table

VXLAN	IP/MAC
5000	a.a.a
	b.b.b
	c.c.c
	d.d.d

VSM distributes VXLAN/MAC

MAC_X not found in table. Packet dropped.

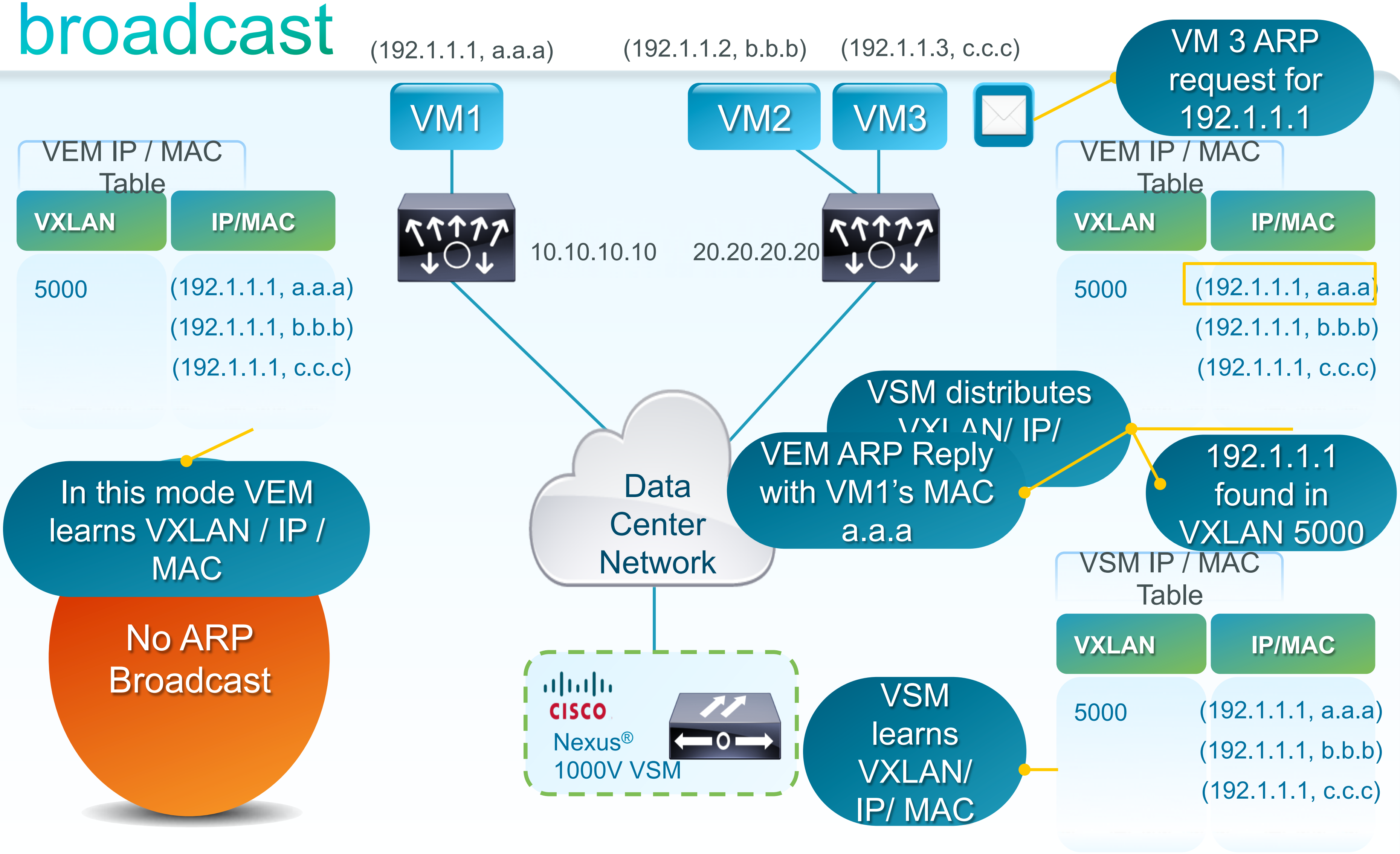
VSM IP / MAC Table

VXLAN	IP/MAC
5000	a.a.a
	b.b.b
	c.c.c
	d.d.d

VSM learns VXLAN/MAC

Unknown Unicast Flood Prevented

VXLAN ARP Termination – Reduces ARP broadcast



VM 3 ARP request for 192.1.1.1

VEM IP / MAC Table

VXLAN	IP/MAC
5000	(192.1.1.1, a.a.a)
	(192.1.1.1, b.b.b)
	(192.1.1.1, c.c.c)

In this mode VEM learns VXLAN / IP / MAC

No ARP Broadcast

VEM IP / MAC Table

VXLAN	IP/MAC
5000	(192.1.1.1, a.a.a)
	(192.1.1.1, b.b.b)
	(192.1.1.1, c.c.c)

VSM distributes VXLAN/ IP/

VEM ARP Reply with VM1's MAC a.a.a

192.1.1.1 found in VXLAN 5000

VSM IP / MAC Table

VXLAN	IP/MAC
5000	(192.1.1.1, a.a.a)
	(192.1.1.1, b.b.b)
	(192.1.1.1, c.c.c)

VSM learns VXLAN/ IP/ MAC

Enhanced VXLAN

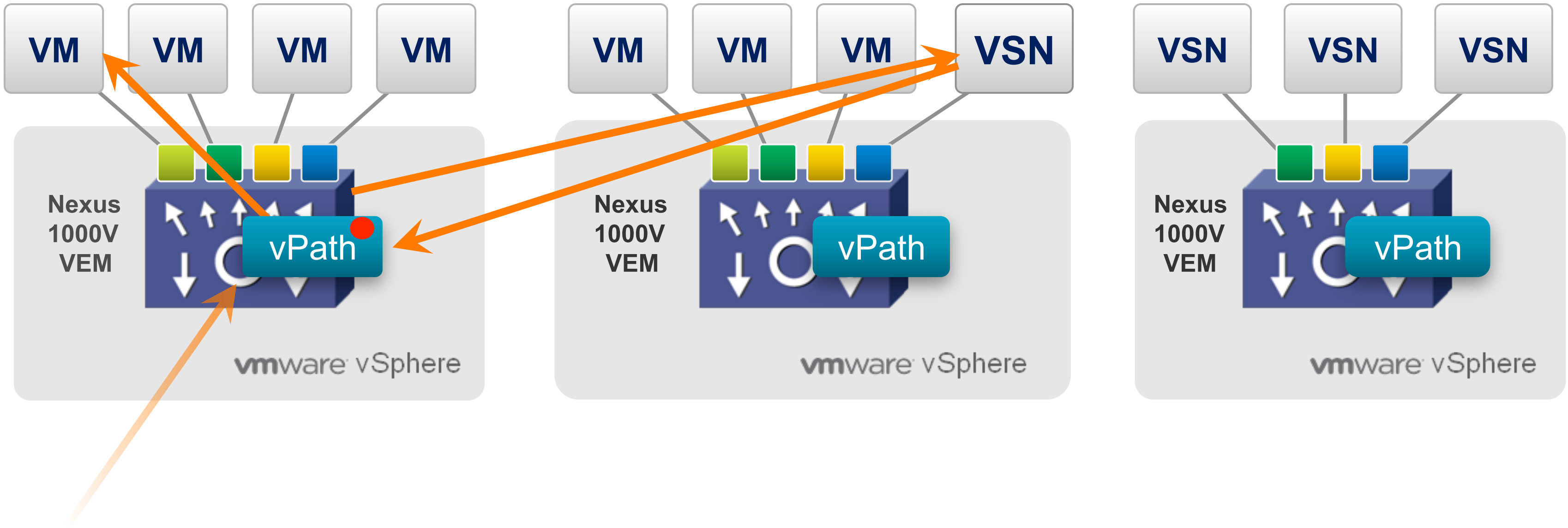
VXLAN Mode Packet	VXLAN (multicast mode)	Enhanced VXLAN (unicast mode)	Enhanced VXLAN MAC Distribution	Enhanced VXLAN ARP Termination
Broadcast / Multicast	Multicast Encapsulation	Replication plus Unicast Encap	Replication plus Unicast Encap	Replication plus Unicast Encap
Unknown Unicast	Multicast Encapsulation	Replication plus Unicast Encap	Drop	Drop
Known Unicast	Unicast Encapsulation	Unicast Encap	Unicast Encap	Unicast Encap
ARP	Multicast Encapsulation	Replication plus Unicast Encap	Replication plus Unicast Encap	VEM ARP Reply

your reference

Virtualized Network Services

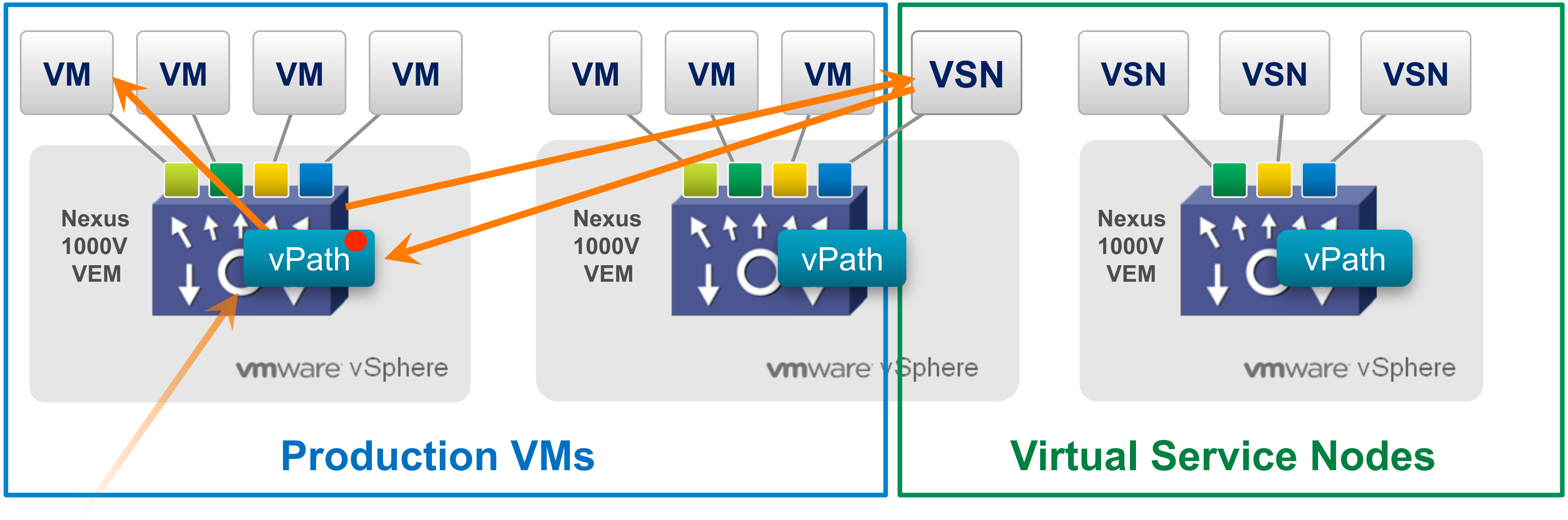
Cisco vPath: Intelligent Traffic Steering

Virtual Service Nodes (VSN)



- New flow is classified for VSN re-direction
- Initial packet(s) re-directed to VSN
- VSN installs a flow entry into vPath

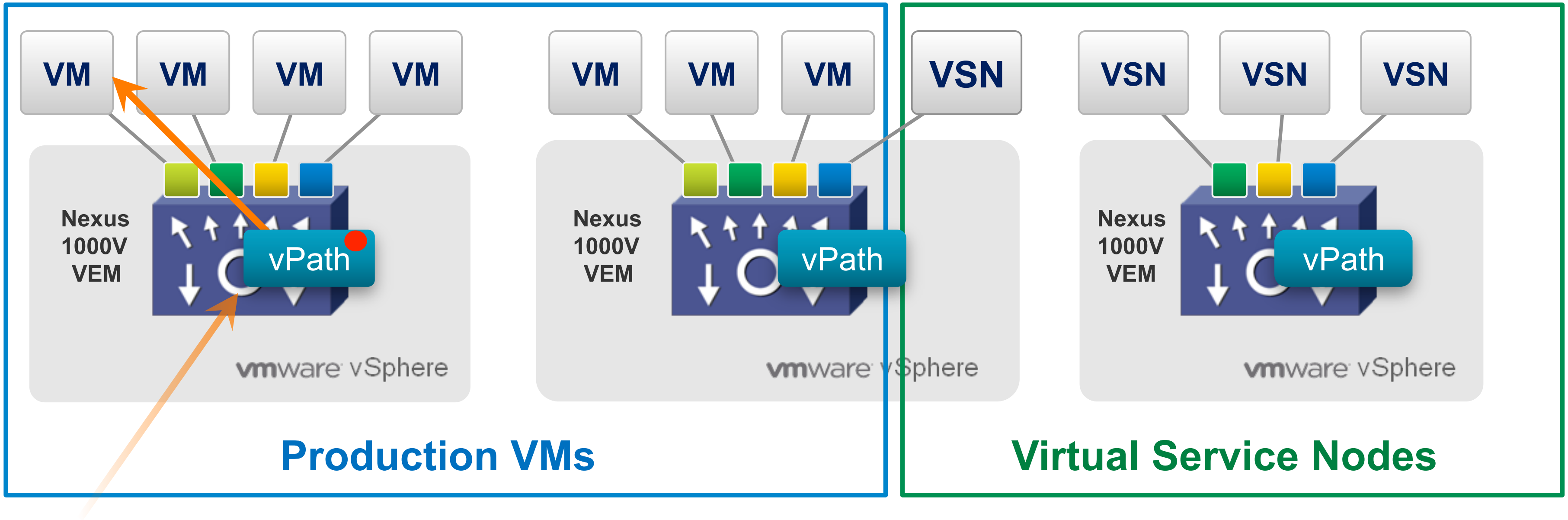
Cisco vPath: Flexible Deployment



- Service VMs placed with or separated from production VMs
- VSN can provide network service to multiple vSphere servers

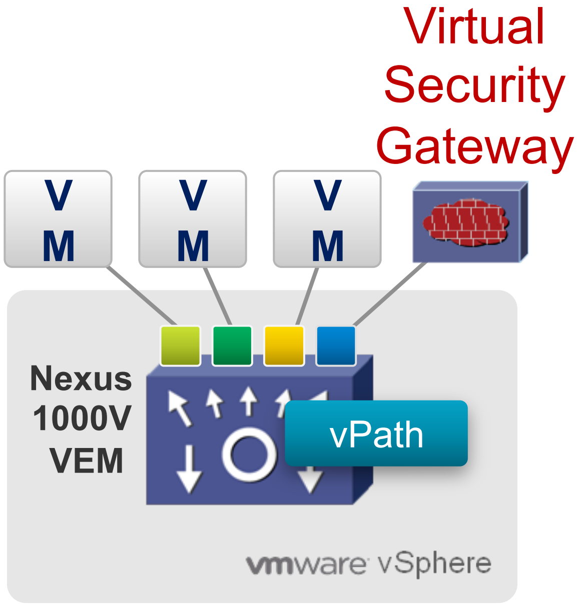
Cisco vPath: Performance Acceleration

Scalable Acceleration in Virtual Ethernet Module



- Network service policy for subsequent packets in the flow are enforced in VEM
- Reduces traffic steering
- VEMs are part of the network service: Scalable Acceleration in hypervisor kernel

Cisco Virtual Security Gateway



- First Virtual Service Node leveraging vPath
- Trusted segmentation

  Zone-based control and monitoring

- Dynamic operation

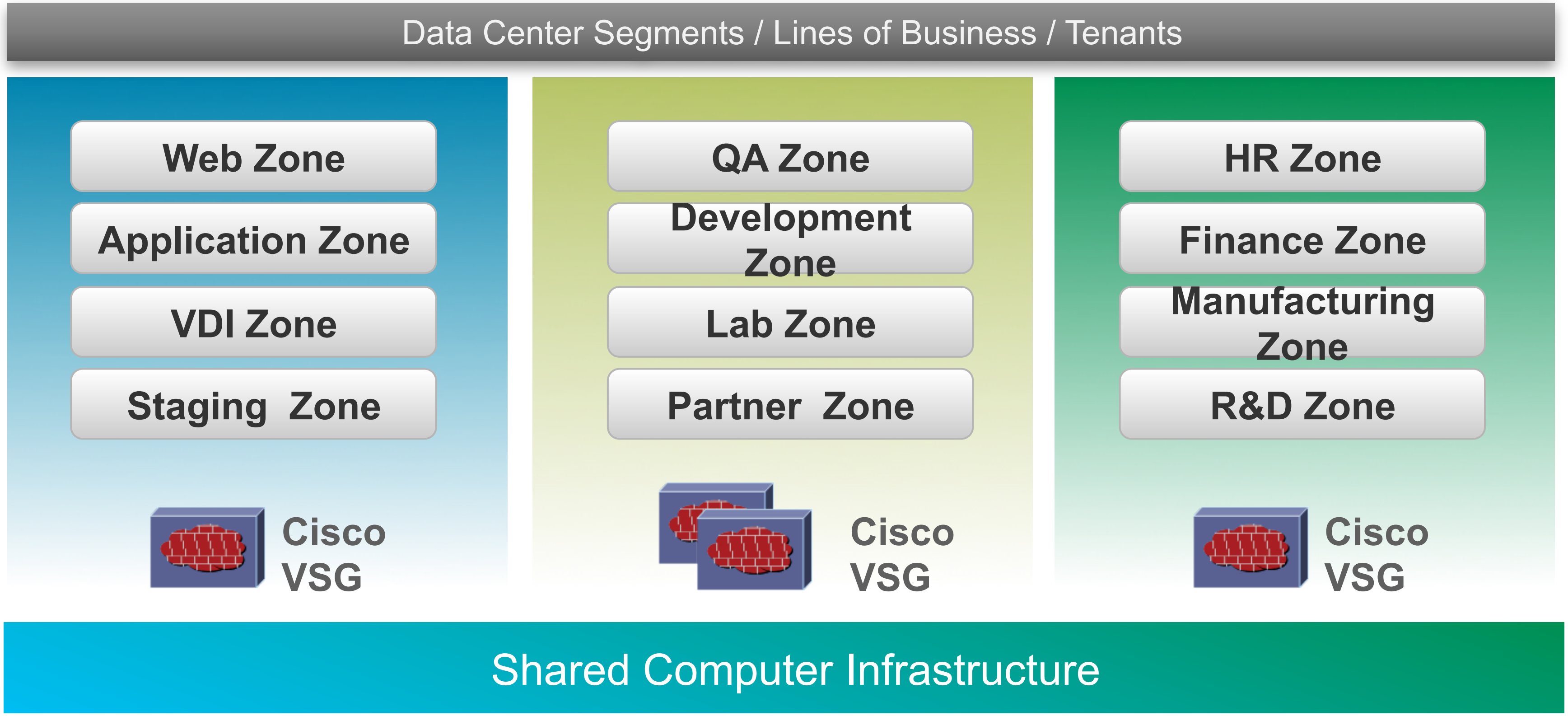
  On-demand provisioning

  Security policy follows vMotioned VM

- Non-disruptive administration for

  Virtualization, Security, and Network Teams

Virtual Security Gateway Use Case



Data Center Segments / Lines of Business / Tenants

Web Zone

Application Zone

VDI Zone

Staging Zone

Cisco VSG

QA Zone

Development Zone

Lab Zone

Partner Zone

Cisco VSG

HR Zone

Finance Zone

Manufacturing Zone

R&D Zone

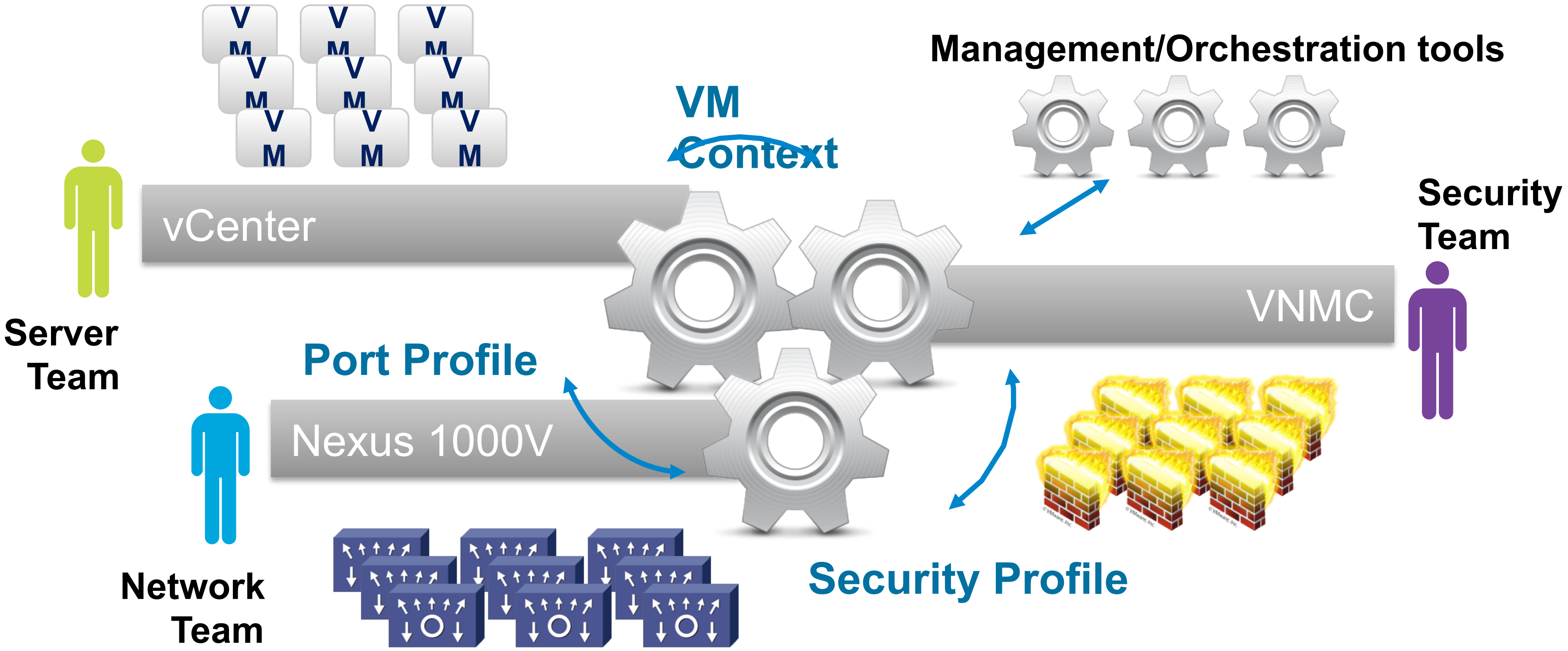
Cisco VSG

Shared Computer Infrastructure

- Zone-based access control
- Granular, context based security policies (supports VM, custom and network attributes)
- Multi-tenancy support

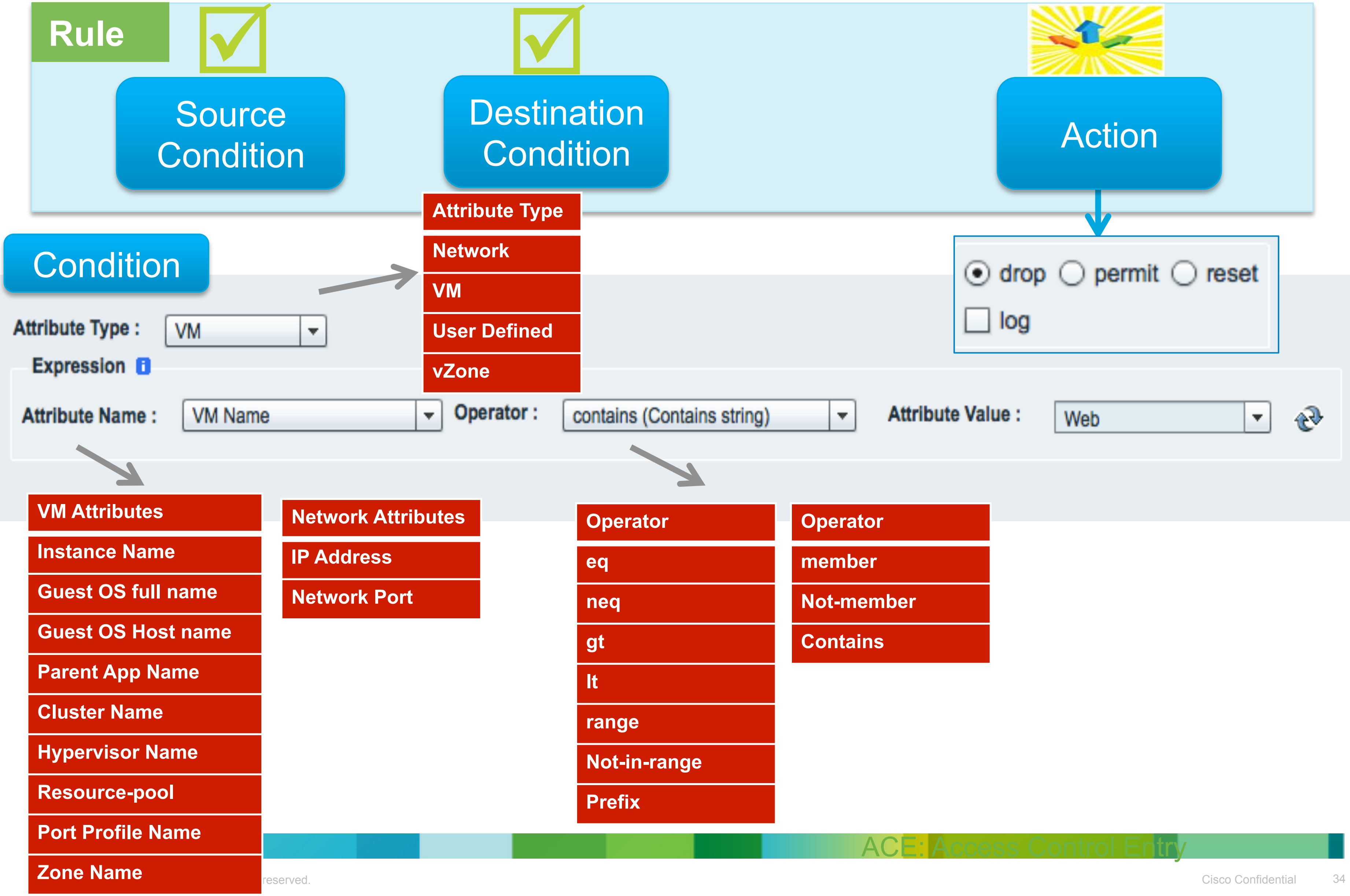
Virtual Network Management Center

Seamless Policy-Based VSG Management



- Centralized mgmt of VSG & security profiles
- Security team manages security
- Architected for multi-tenancy, RBAC
- XML API for automated provisioning

VSG Policy: Context-based Rule Engine



Rule

Source Condition

Destination Condition

Action

Attribute Type
- Network
- VM
- User Defined
- vZone

● drop ○ permit ○ reset

□ log

Condition

Attribute Type : VM

Expression

Attribute Name : VM Name

Operator : contains (Contains string)

Attribute Value : Web

VM Attributes
- Instance Name
- Guest OS full name
- Guest OS Host name
- Parent App Name
- Cluster Name
- Hypervisor Name
- Resource-pool
- Port Profile Name
- Zone Name

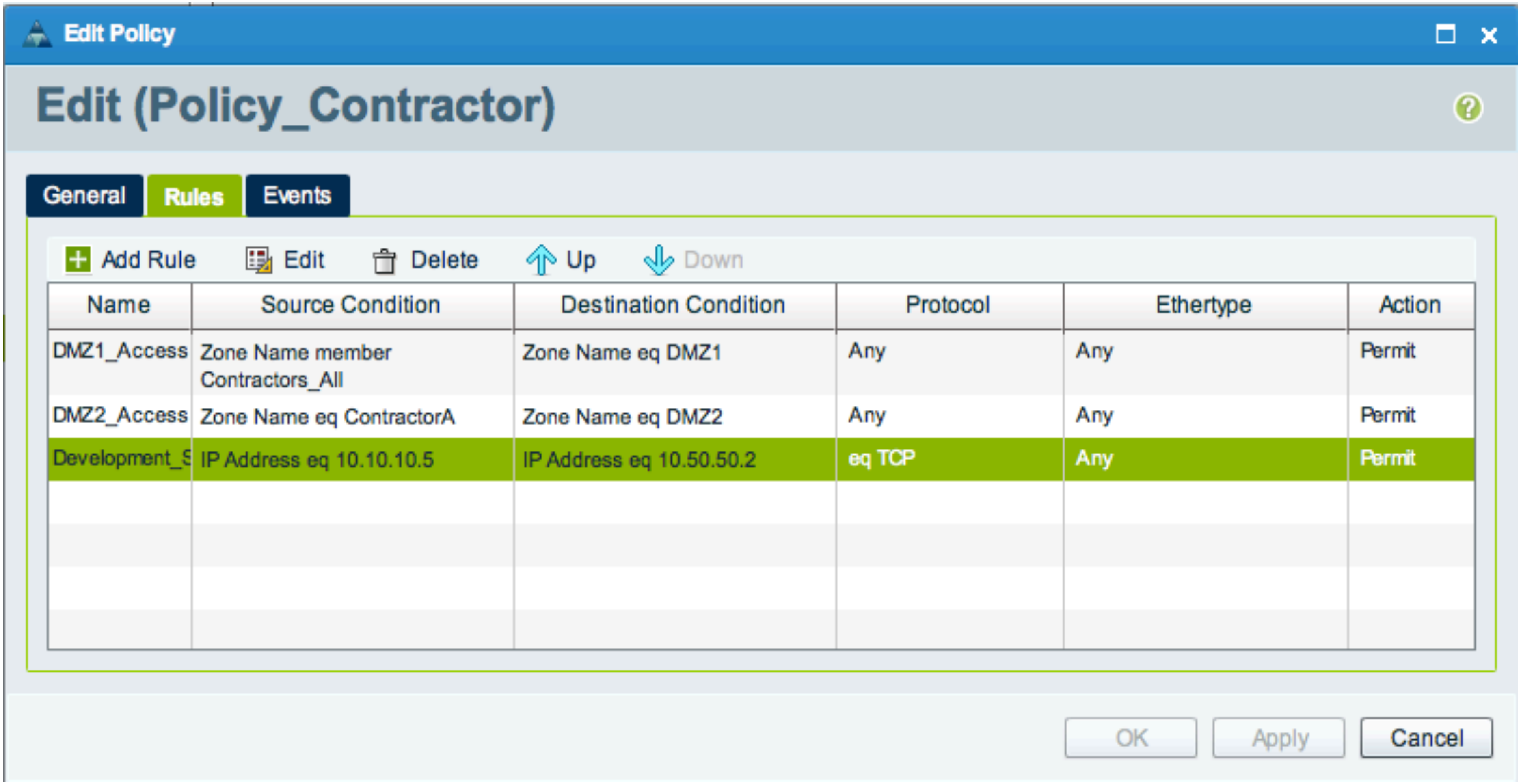
Network Attributes
- IP Address
- Network Port

Operator
- eq
- neq
- gt
- lt
- range
- Not-in-range
- Prefix

Operator
- member
- Not-member
- Contains

ACE: Access Control Entry

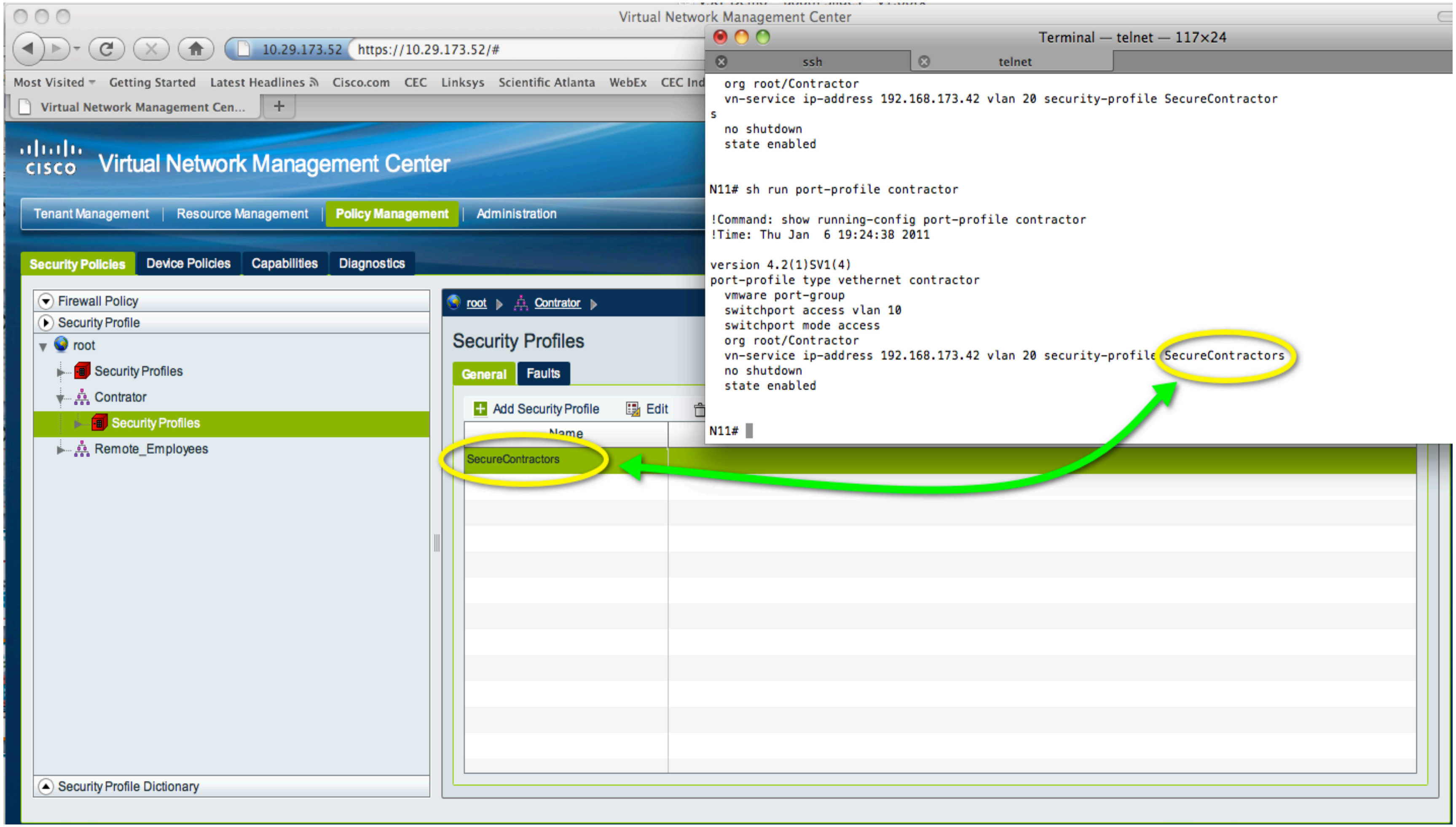
Defining Rules: Summary



Edit (Policy_Contractor)

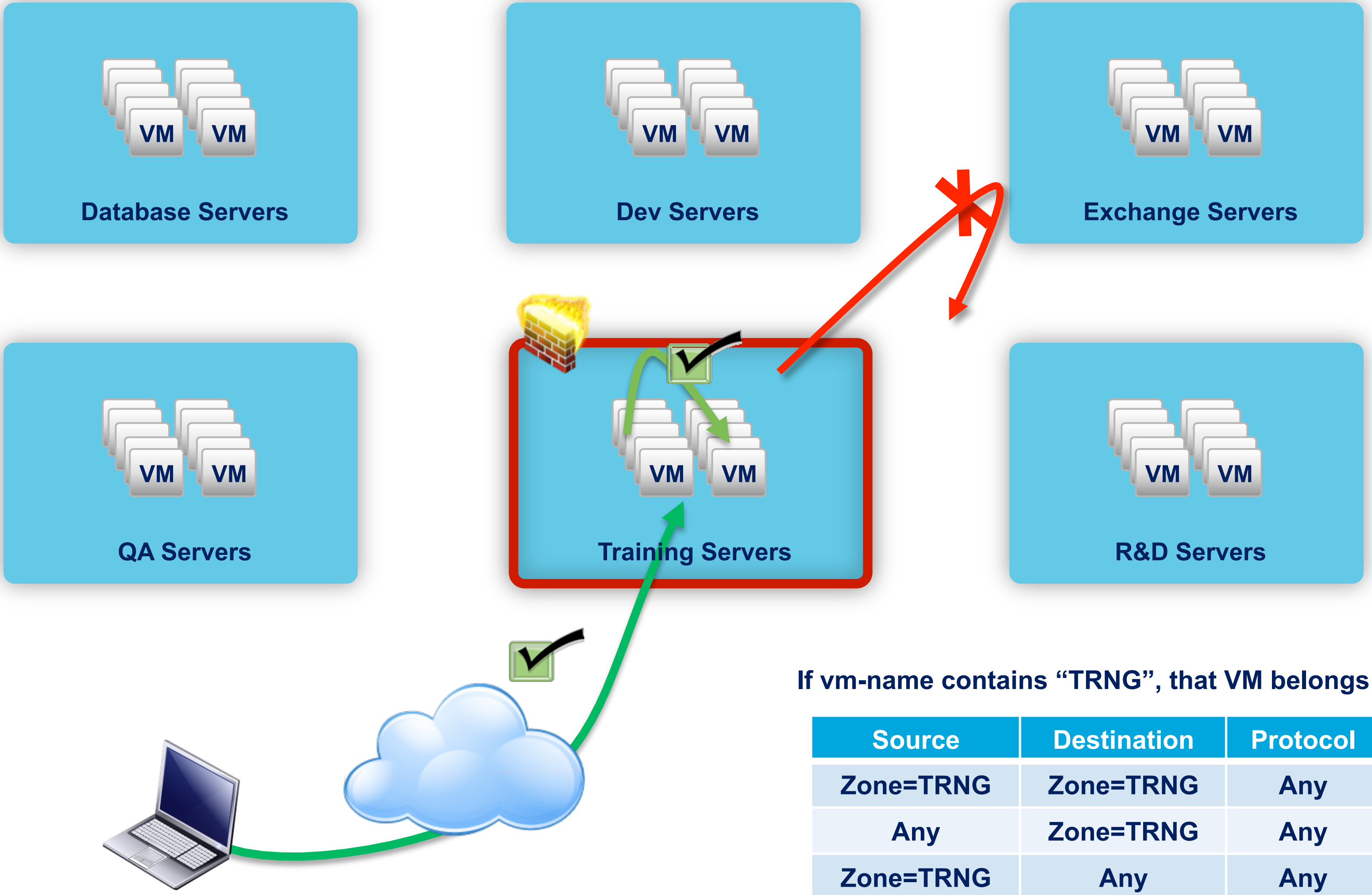
Name	Source Condition	Destination Condition	Protocol	Ethertype	Action
DMZ1_Access	Zone Name member Contractors_All	Zone Name eq DMZ1	Any	Any	Permit
DMZ2_Access	Zone Name eq ContractorA	Zone Name eq DMZ2	Any	Any	Permit
Development_S	IP Address eq 10.10.10.5	IP Address eq 10.50.50.2	eq TCP	Any	Permit

Binding VSG Security Profile with 1000V Port-Profile



```
  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# 
```

Carecore National Secure zoning using VM attribute



If vm-name contains “TRNG”, that VM belongs to TRNG zone

Source	Destination	Protocol	Action
Zone=TRNG	Zone=TRNG	Any	Permit
Any	Zone=TRNG	Any	Permit
Zone=TRNG	Any	Any	Drop

Cisco’s Virtual Security Portfolio

Virtual Security Gateway

Zone-based segmentation within a tenant

ASA 1000V

Tenant edge security

Hypervisor

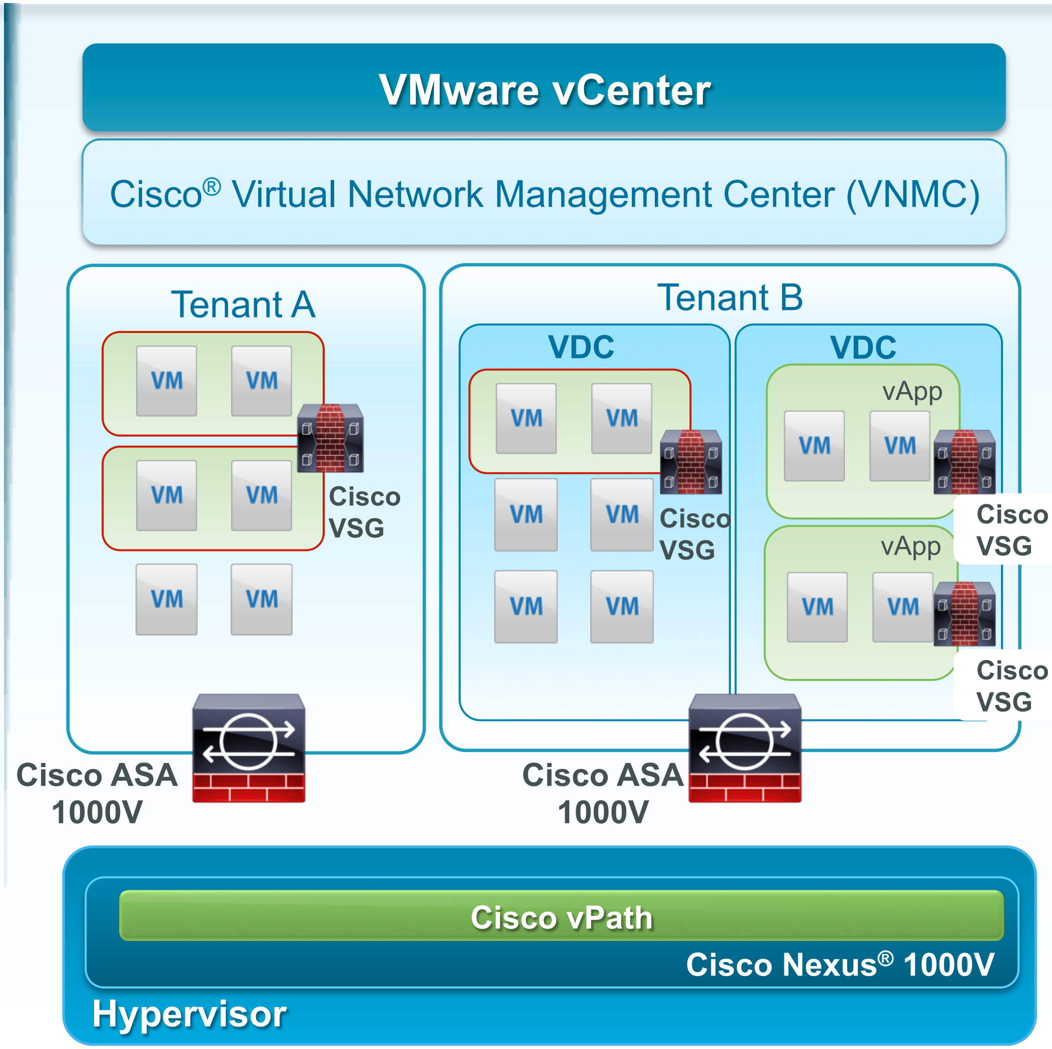
Nexus 1000V

VNMC

ASA 1000V – Release 8.7.1

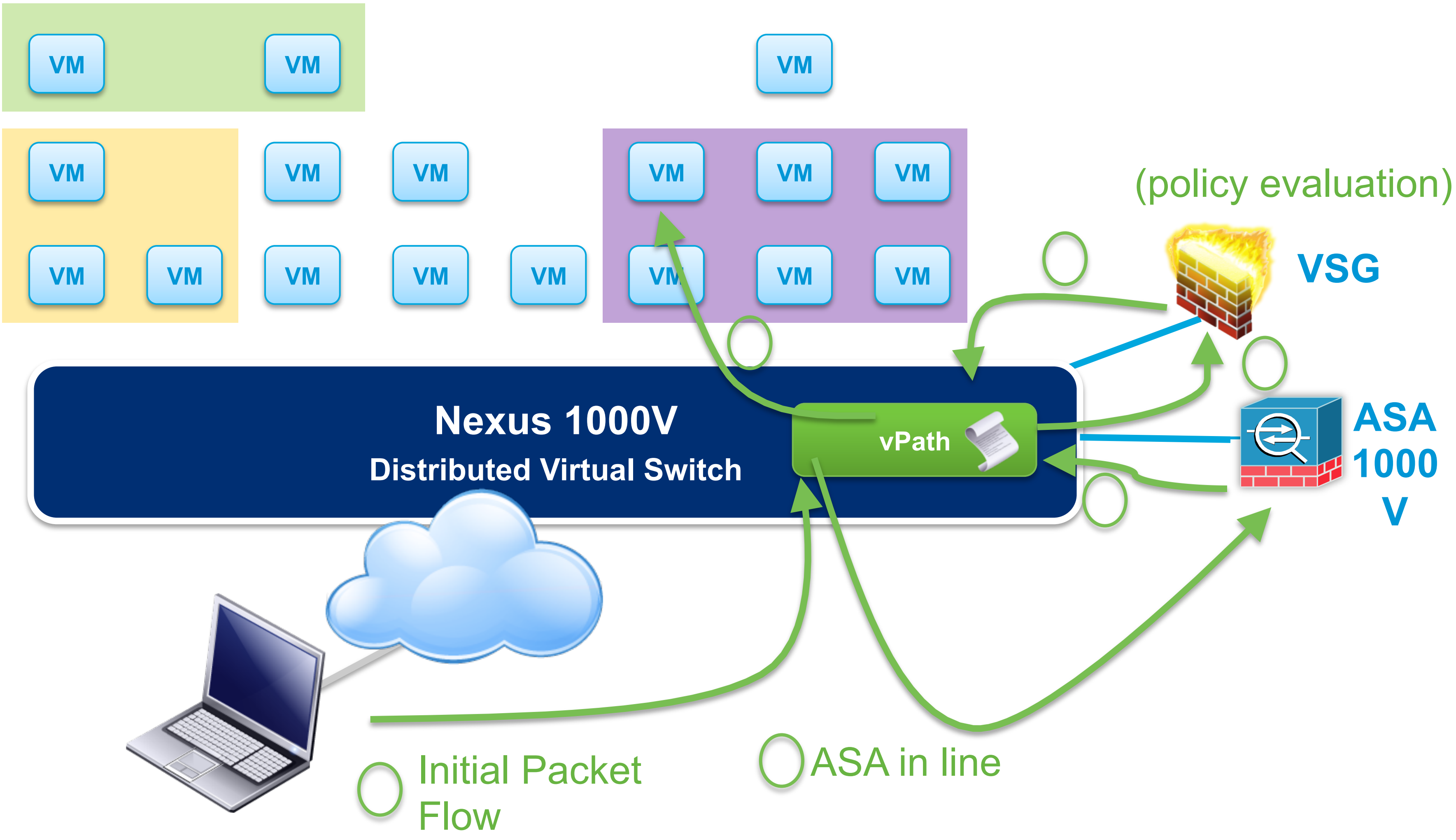
Securing the Tenant Edge with Cisco ASA 1000V

- Proven Cisco® security: virtualized physical and virtual consistency
- Collaborative security model
  - Cisco Virtual Secure Gateway (VSG) for intra-tenant secure zones
  - Cisco ASA 1000V for tenant edge controls
- Transparent integration
  - With Cisco Nexus® 1000V Switch and Cisco vPath
- Scale flexibility to meet cloud demand
  - Multi-instance deployment for scale-out deployment across the data center



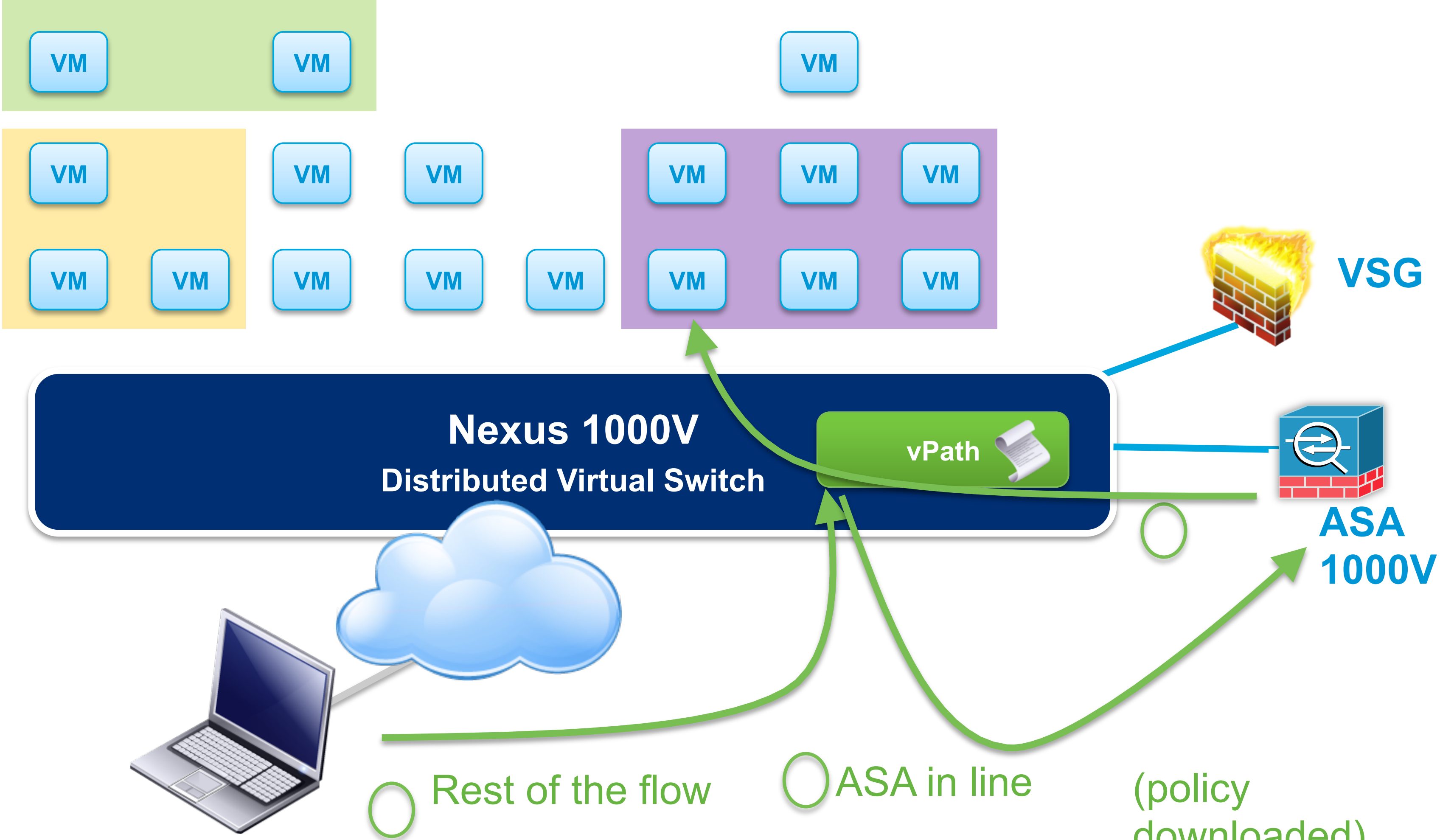
Nexus 1000V with vPath 2.0 Service Chaining

VSG & ASA 1000V



Nexus 1000V with vPath 2.0 Service Chaining

VSG & ASA 1000V

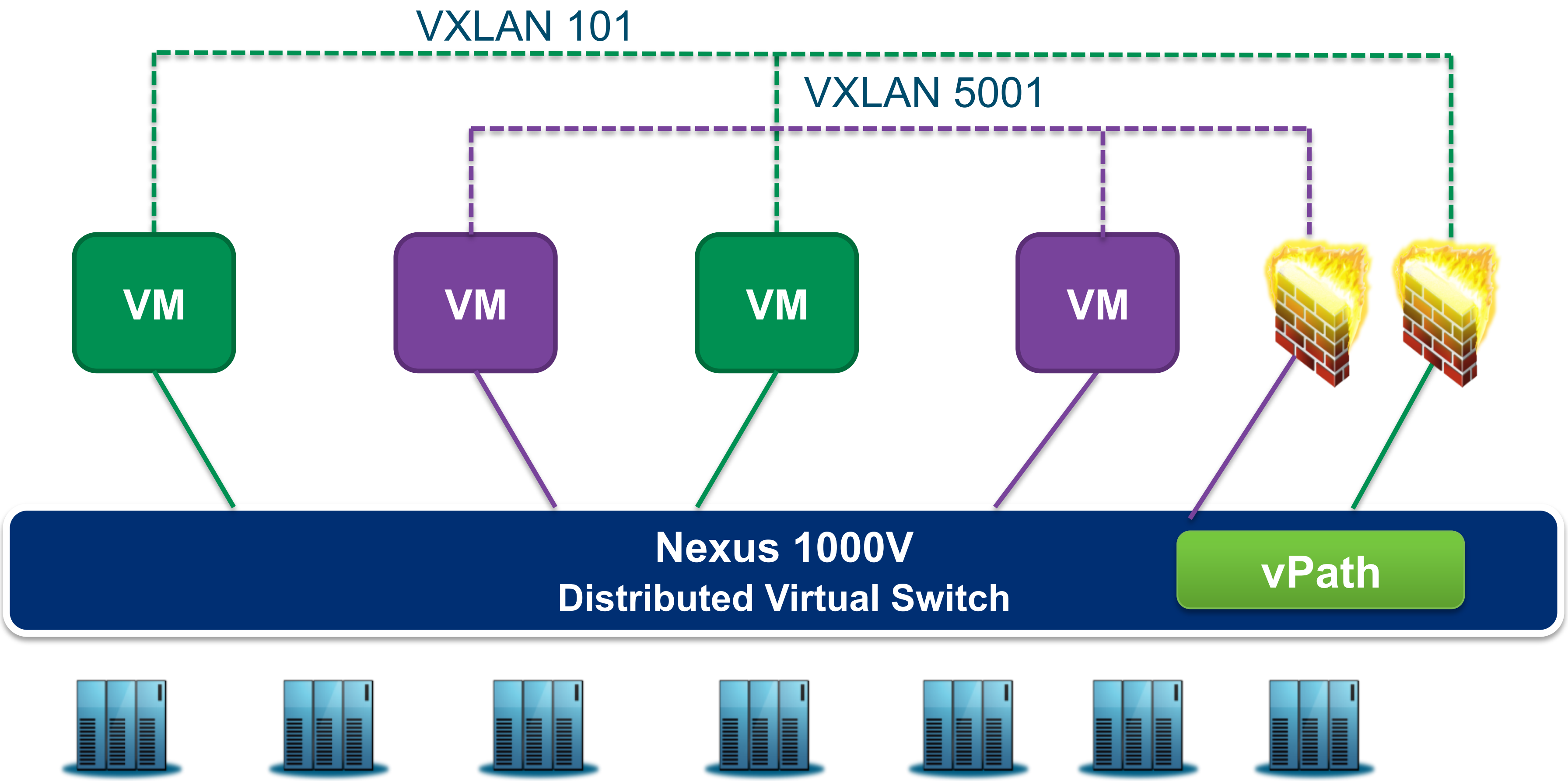


○ Rest of the flow

○ ASA in line

○ (policy downloaded)

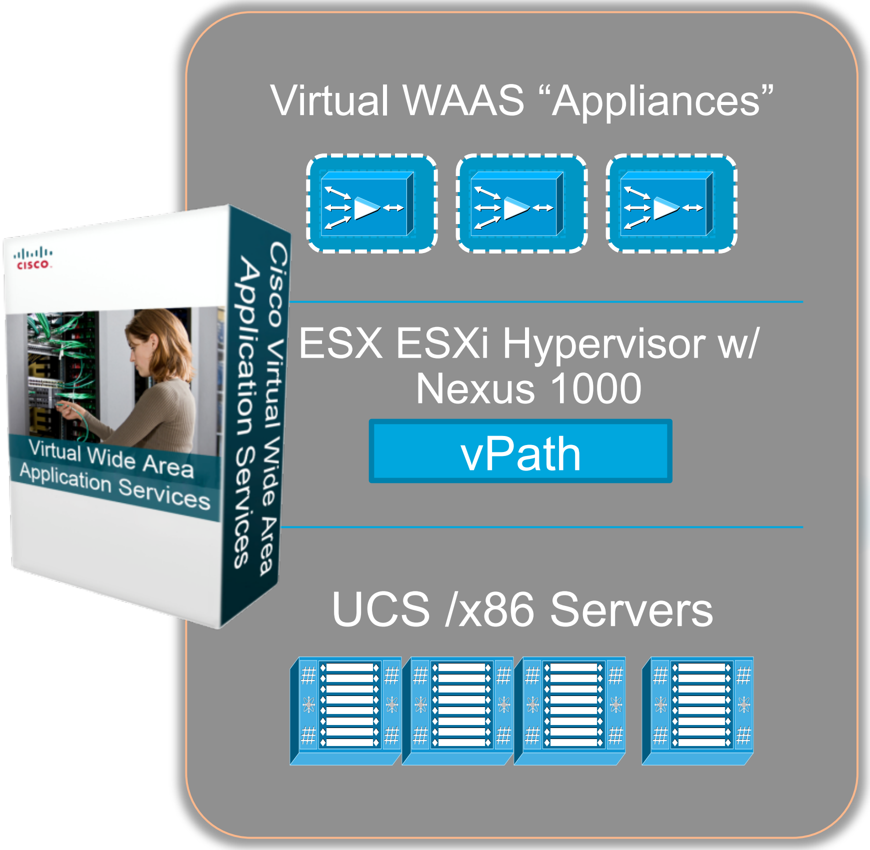
Nexus 1000V vPath2.0: VSNs on VXLANs



- Deployment- VMs and Virtual Service Nodes, ASA 1000V, VSG, vWAAS etc, on VXLANs
- Same VSG can protect VMs on multiple VXLANs with overlapping IP addresses

Shipping

Cisco Virtual WAAS
Cloud-ready WAN Optimization


Virtual WAAS “Appliances”
ESX ESXi Hypervisor w/ Nexus 1000
vPath
UCS /x86 Servers
cisco
Cisco Virtual Wide Area Application Services
Virtual Wide Area Application Services

Virtual WAAS
Stand-alone or with N1KV/vPath

FEATURES

- Allows Agile, Elastic, & Multi Tenant Deployment
- Supports DRE Cache in SAN
- Policy-based Provisioning w/ Nexus 1000V
- Extends WAAS Solution Portfolio

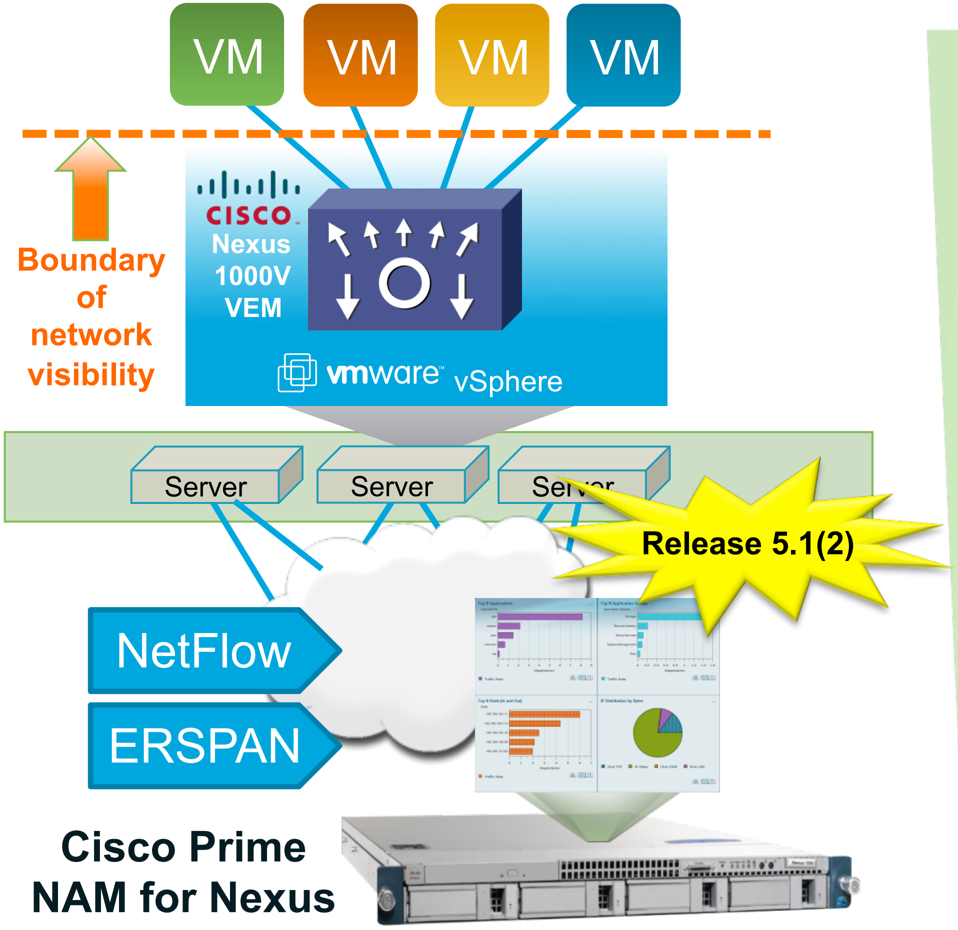
BUSINESS BENEFITS

- Business Agility with on-demand orchestration
- Lower operational cost, reduced migration risk
- Fault-tolerance with VM mobility awareness

Shipping

Cisco Prime NAM for Nexus 1010

Extends Visibility into Virtual Machine (VM) Network

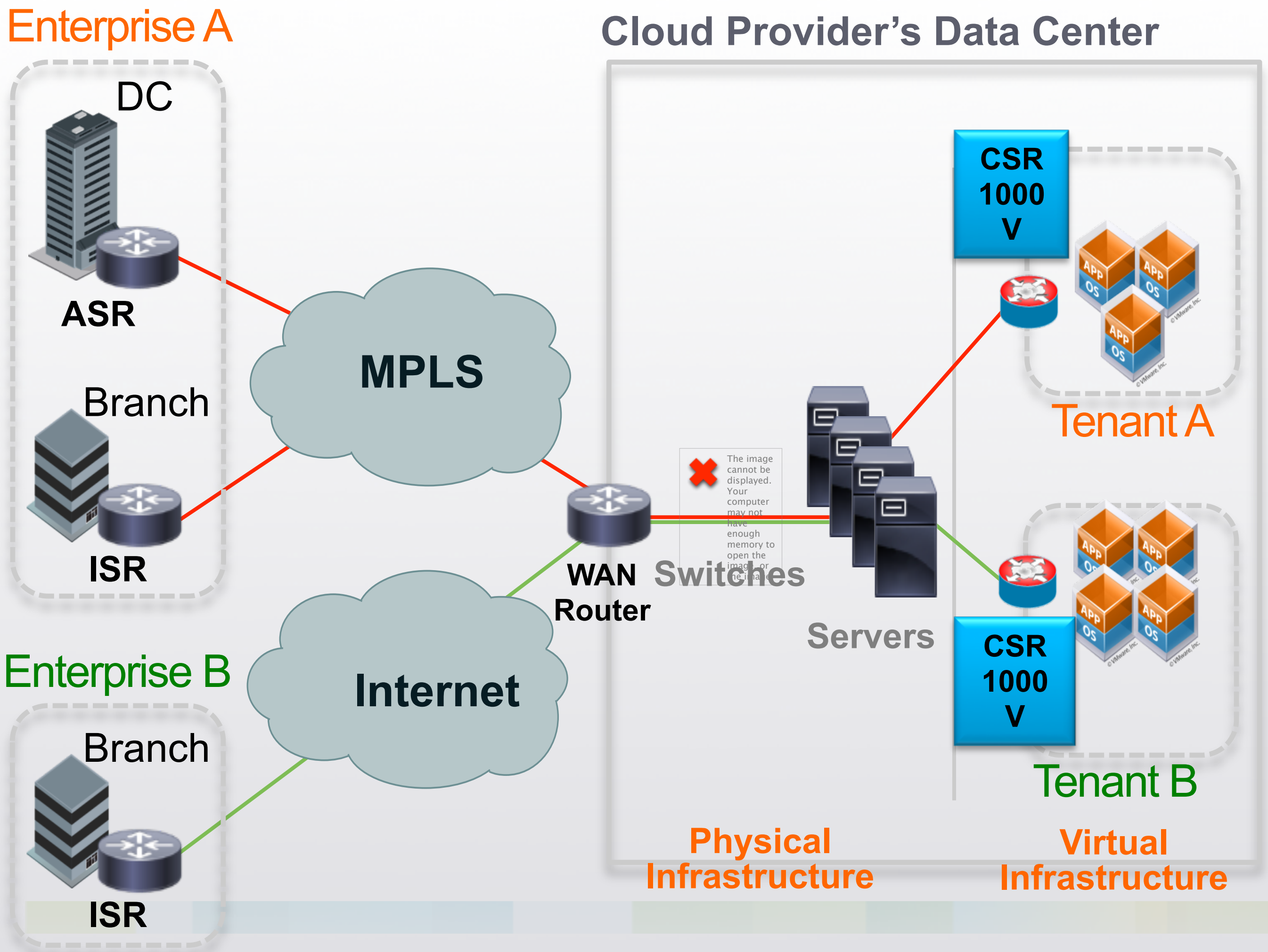


Cisco Prime NAM for Nexus 1010

- Profile VM Network Traffic
- Analyze Application Reponses Time
- Examine Virtual Interface Statistics
- Assess impact on network behavior due to changes such as VM migration, port profile update, etc.
- Watch VMs while they migrate with VMotion

CSR 1000V: Single-Tenant WAN Gateway in Shared Multi-tenant Clouds

Can be deployed by Enterprises or Cloud Providers



Enterprise Use Cases

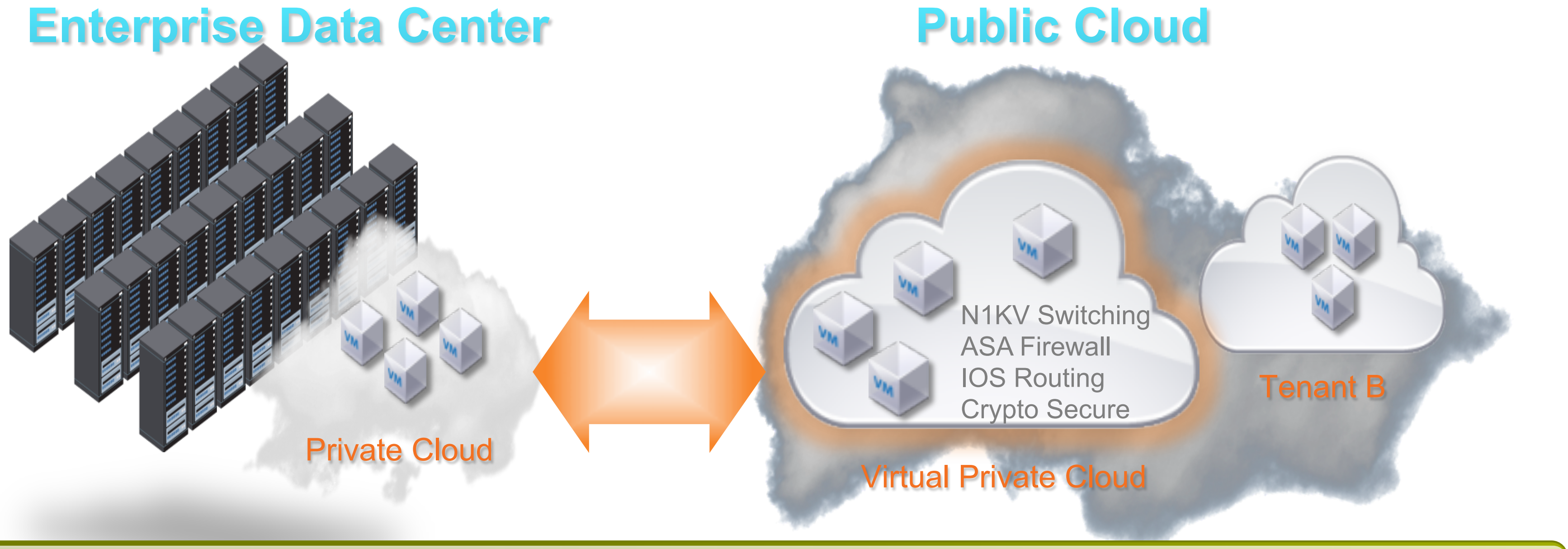
- Secure VPN Gateway
- L3 Extension

Cloud Provider Use Cases

- Secure VPN Gateway
- MPLS Extension

Nexus 1000V InterCloud Secure Hybrid Cloud

Cisco’s Vision for Hybrid Cloud



Secure Hybrid Cloud = Securely Connect Enterprise Private Cloud and Provider Public Cloud

Use Cases

- Bursting
- Disaster recovery/avoidance
- Upgrade/migration

Workloads

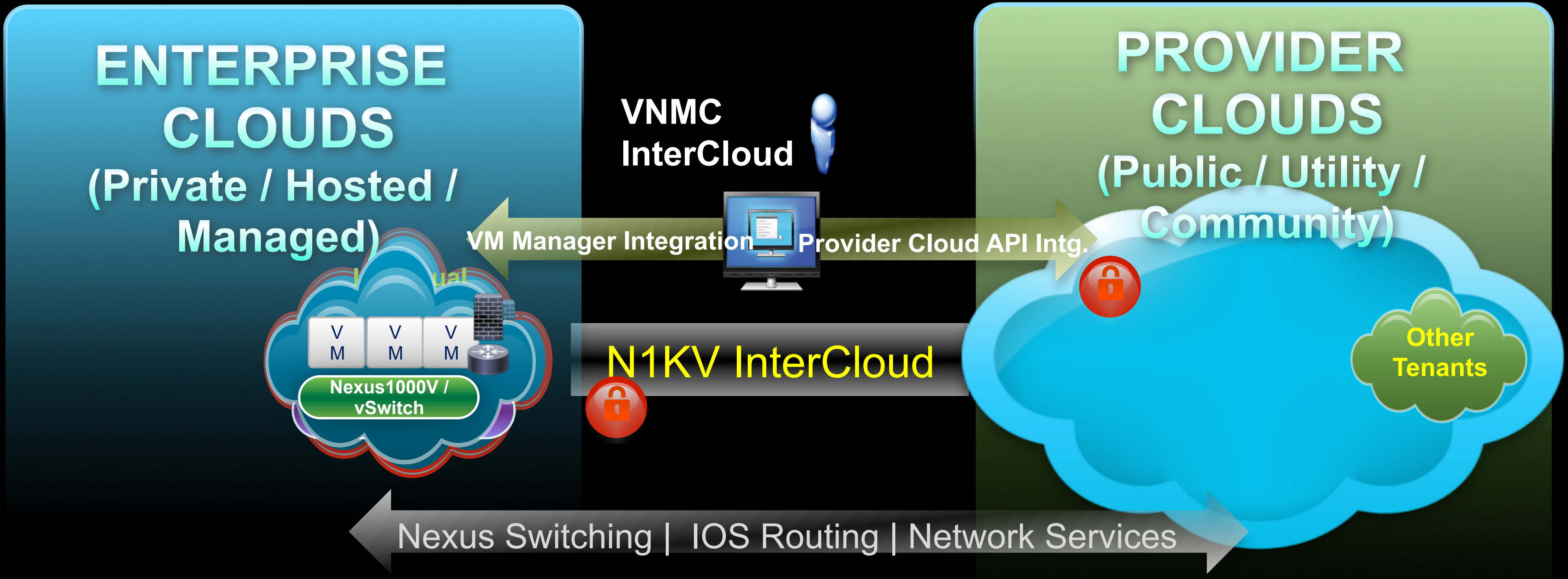
- Dev/QA
- Intern/Partner VDI
- Training Apps
- Initially low-value workloads

Requirements

- Network consistency
- Security consistency
- Policy consistency

Nexus1000V InterCloud (Project Kumo):

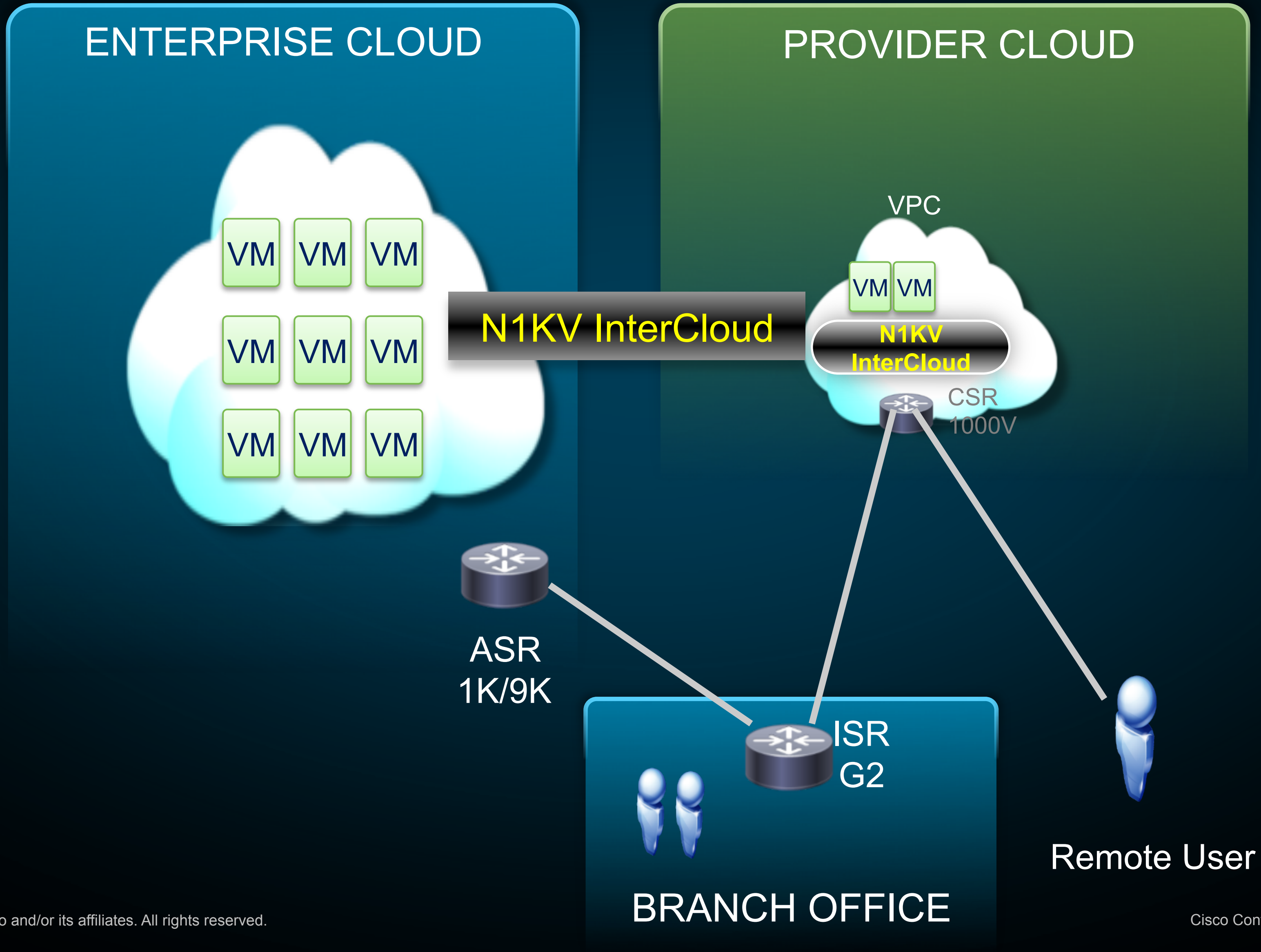
Securely Extend Enterprise Environment into Provider Cloud



Secure	Enterprise-Grade Crypto and Firewalling within & across clouds
Simple	Transparent Application Migration; Centralized Management
Flexible	Choice of Provider Clouds and Hypervisors

N1KV InterCloud Vision

Direct Access to VPC Workloads from Branch/ Remote Offices



Summary

- Nexus 1000V is the foundation for full portfolio of virtualized network machine networking
  - Nexus 1000V, CSR 1000V, Full portfolio of virtualized network services
- Enhanced VXLAN to ease and scale virtual overlay
- vPath supporting variety of virtualized network services
  - ASA 1000V, Virtual Security Gateway, NAM, vWAAS, Imperva WAF, Citrix VPX

Thank you.