Cisco live!

What You Make Possible

TOMORROW
starts here.

CISCO

Deploying Services in a Virtualised Environment

BRKVIR-2011

TOMORROW starts here.

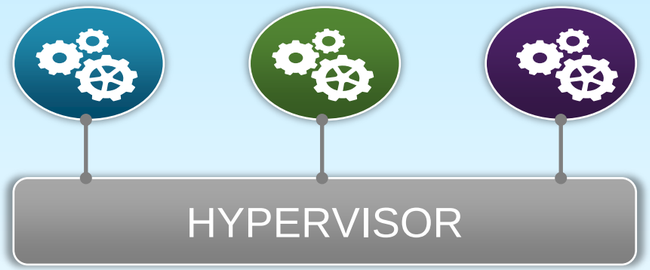
Agenda

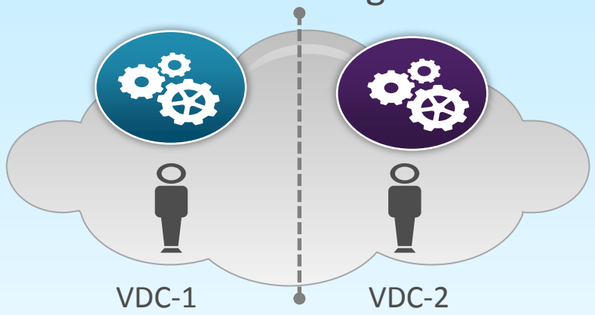
- Virtualisation/Cloud Trends
- Requirements for Virtualised Services
- Virtual Networking & Services – architecture
  - Nexus 1000V for Virtualised Services
- Implementing Virtualised Services
  - Virtual Security Gateway (VSG)
  - ASA 1000V
  - Virtual WAAS (vWAAS)
  - Network Analysis Module (NAM)
  - 3rd Party Services on vPath
  - Virtual Services for VM Mobility
  - Virtual Services on VXLAN
- Reference Solutions, Resources & Wrap-Up

Cisco's Approach

Physical → Virtual → Cloud Journey

PHYSICAL WORKLOAD	VIRTUAL WORKLOAD	CLOUD WORKLOAD
• One app per Server • Static • Manual provisioning	• Many apps per Server • Mobile • Dynamic provisioning	• Multi-tenant per Server • Elastic • Automated Scaling



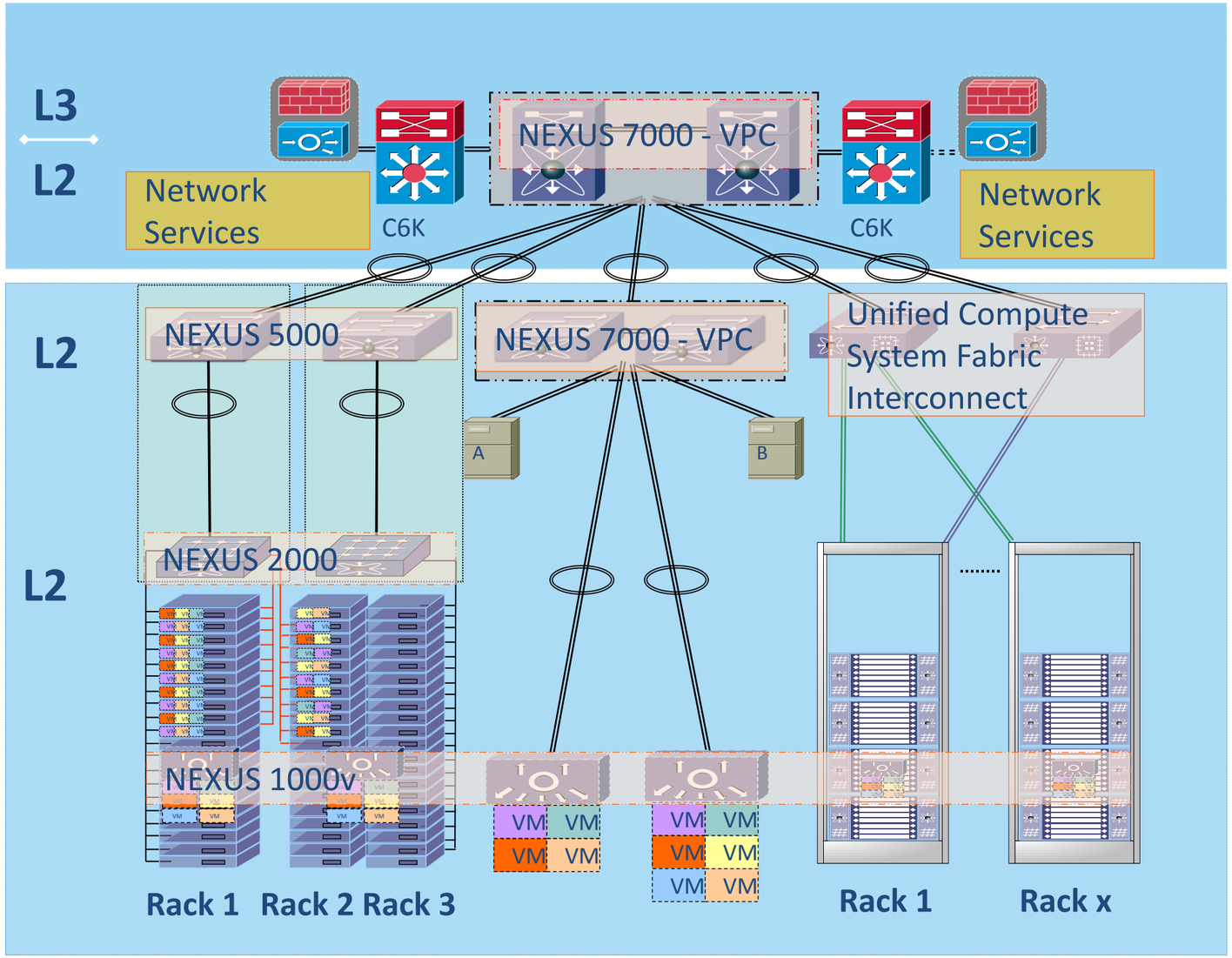


CONSISTENCY: Policy, Features, Security, Management

Nexus 7K/5K/3K/2K	Nexus 1000V, VM-FEX
WAAS, ASA, NAM, ACE →	Virtual WAAS, VSG*, ASA 1000V, 3rd Party Appliance

* Virtual only

Virtual Services in a Data Centre POD



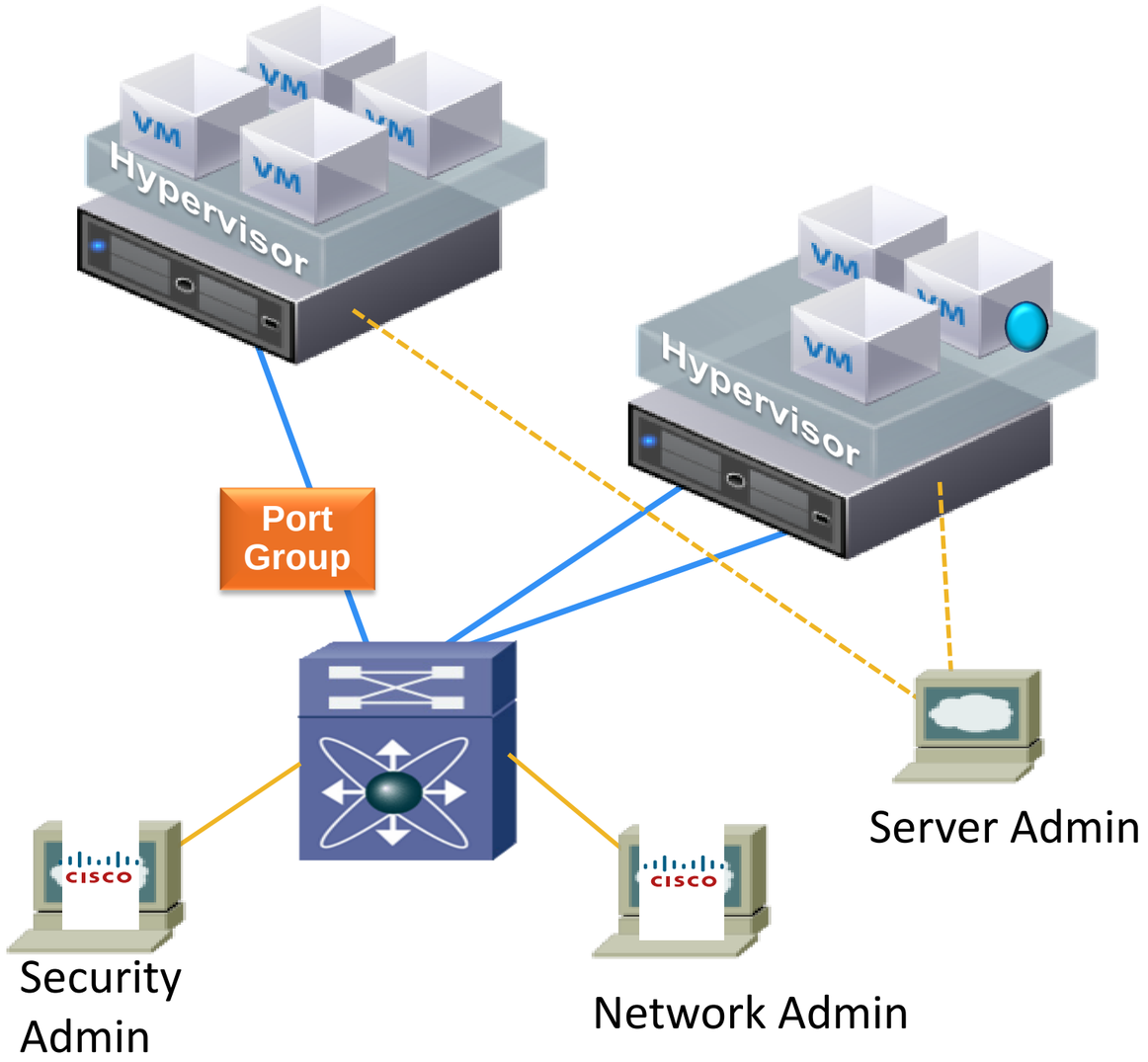
Aggregation
- Typical L3/L2 boundary.
- Physical network services

Unified Access
- Non-blocking paths to servers & IP storage devices

Virtual Access
- Virtual switches
- Virtual services with horizontal scaling

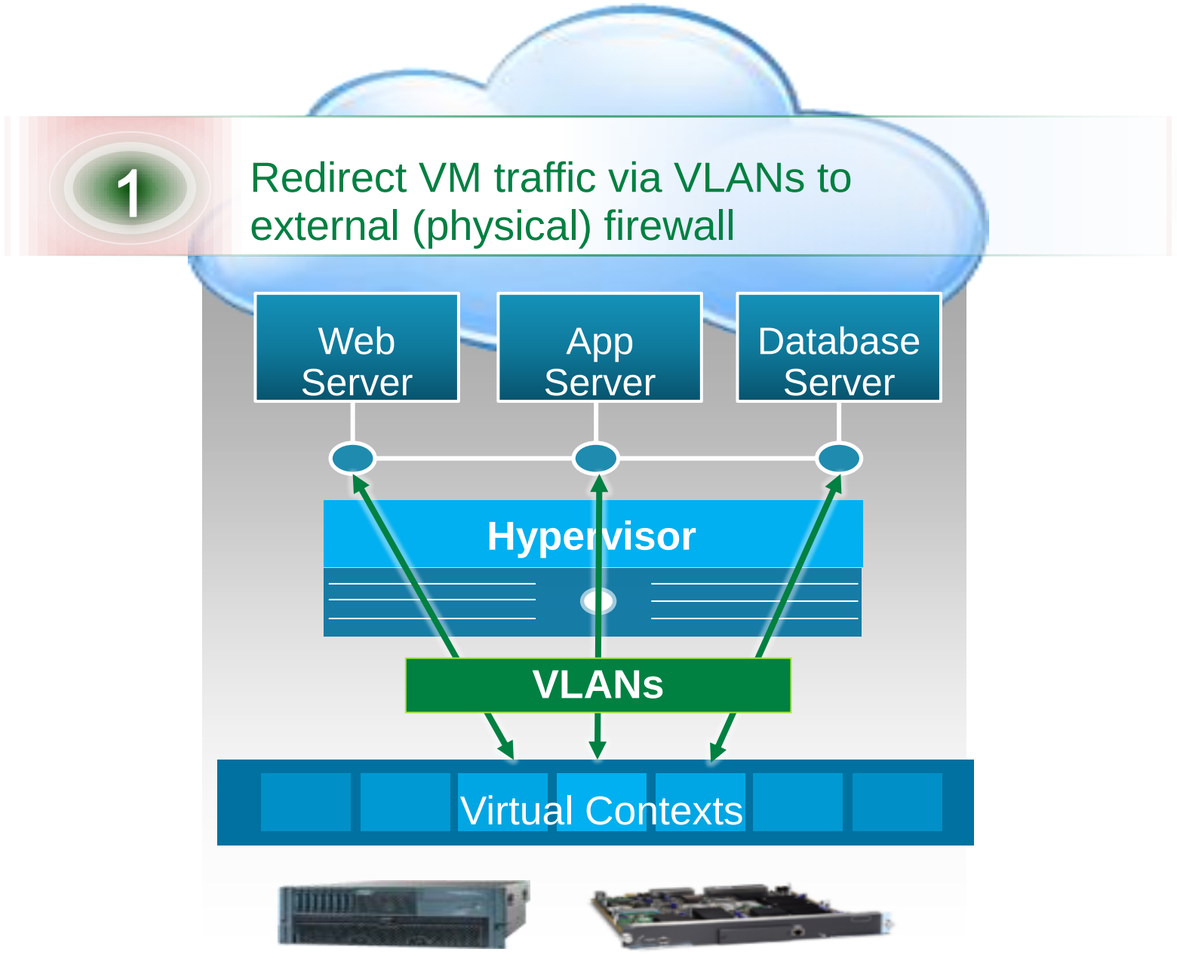
Virtual Services' Requirements

Server Virtualisation Issues

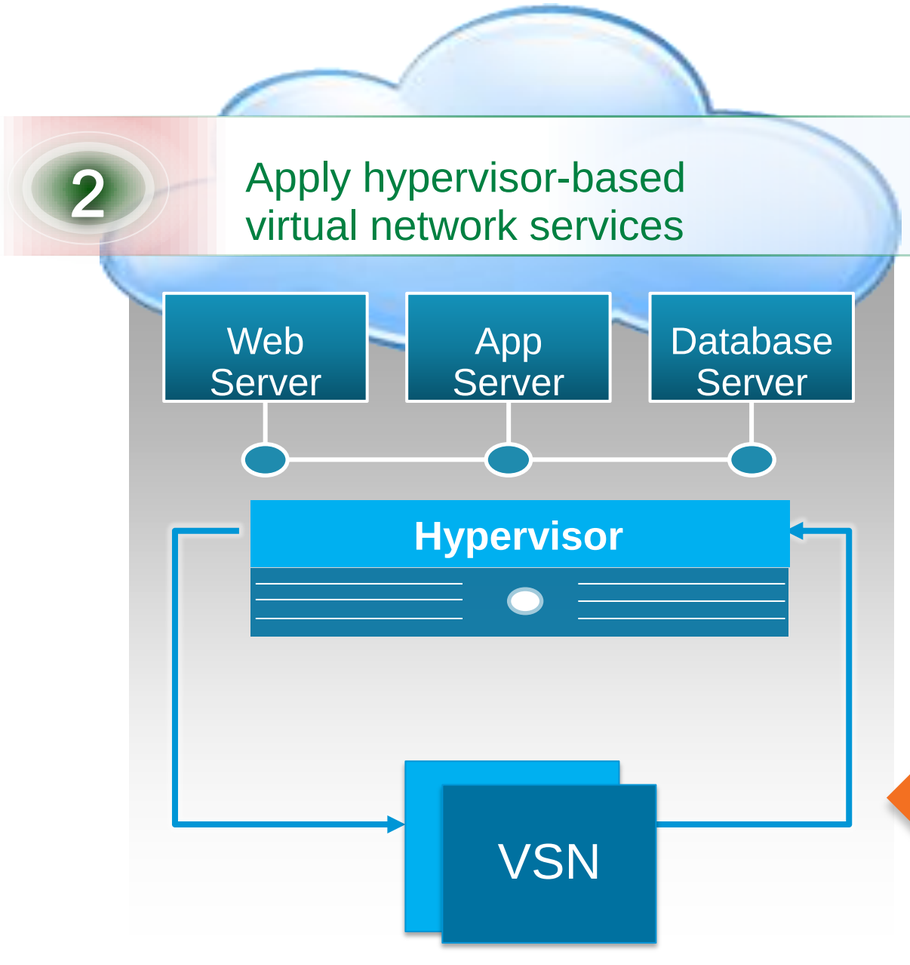


1. vMotion moves VMs across physical ports—the network policy must follow vMotion
2. Must view or apply network/security policy to locally switched traffic
3. Need to maintain separation of duties while ensuring non-disruptive operations

Network Services Options for Virtualised/Cloud DC



Dedicated Service Nodes

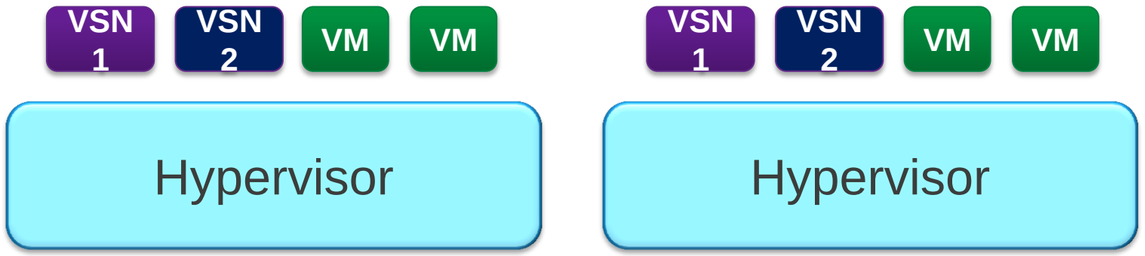


Virtual Service Nodes

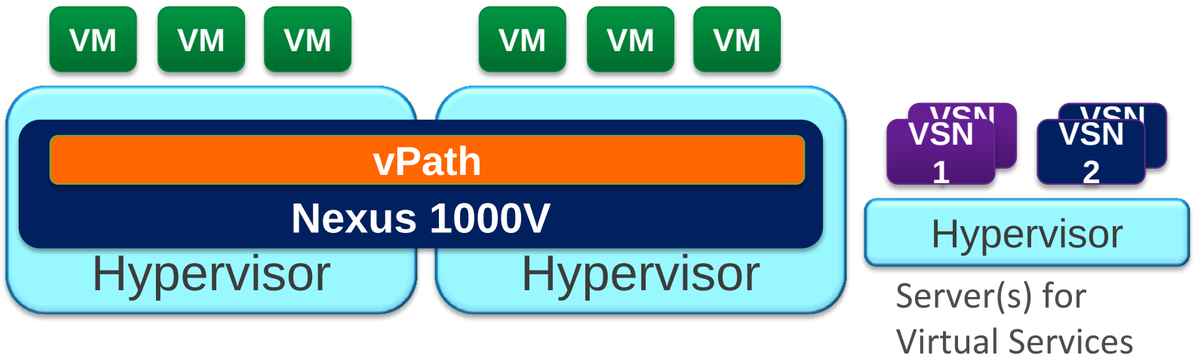
This Session

Virtual Services Options

- Stand-alone VSN
  - Can be deployed with any virtual switch
  - Example: vWAAS



- N1KV vPath integrated VSN
  - Integrates with N1KV port profile and virtual service datapath (vPath)
  - Example: vWAAS, VSG, ASA 1000V



VSN: Virtual Service Node

Virtual Services – Architectural Approach

Requirement	Solution
Virtualisation Awareness • Dynamic policy-based provisioning • Support VM mobility (e.g. vMotion)	• Virtual (SW) form-factor • Integration with VM mgmt tools (e.g. vCenter, SC-VMM in future) • Policies bound to vNIC/VM • Integration with N1KV (vPath*)
Multi-tenant / Scale-out deployment	• Virtual service: multi-instance deployment • Management: Multi-tenant • N1KV vPath: Multi-tenant
Separation of Duties • Non-disruptive to server team	• Profile-based provisioning for services • Integration with N1KV port profile • Optional hosting on Nexus 1010 HW appliance
• Efficient deployment • Performance optimisation	Integration with N1KV vPath
Broad mobility diameter • DC-wide, DC-to-DC, DC-to-Cloud	• DC-wide: VXLAN** • DC-to-DC: OTV**

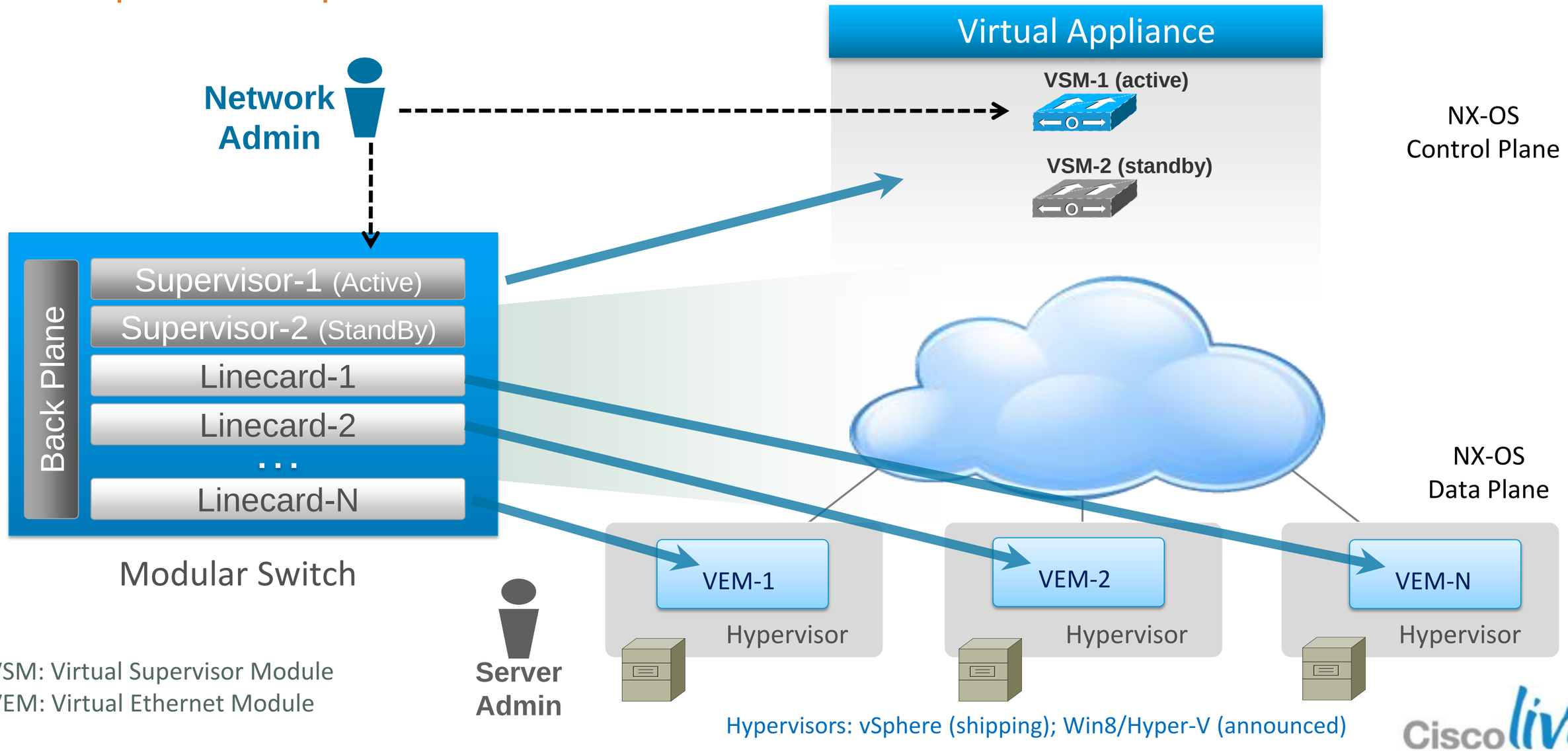
*vPath: Virtual Service Datapath
**VXLAN: Virtual Extensible LAN
**OTV: Overlay Transport Virtualisation

Virtual Networking

Architecture for Virtual Services

Nexus 1000V Architecture

Respects DC Operational Model for P→V



VSM: Virtual Supervisor Module
VEM: Virtual Ethernet Module

Embedding Intelligence in Virtual Network

vPath: Virtual Services Data Path

VSG

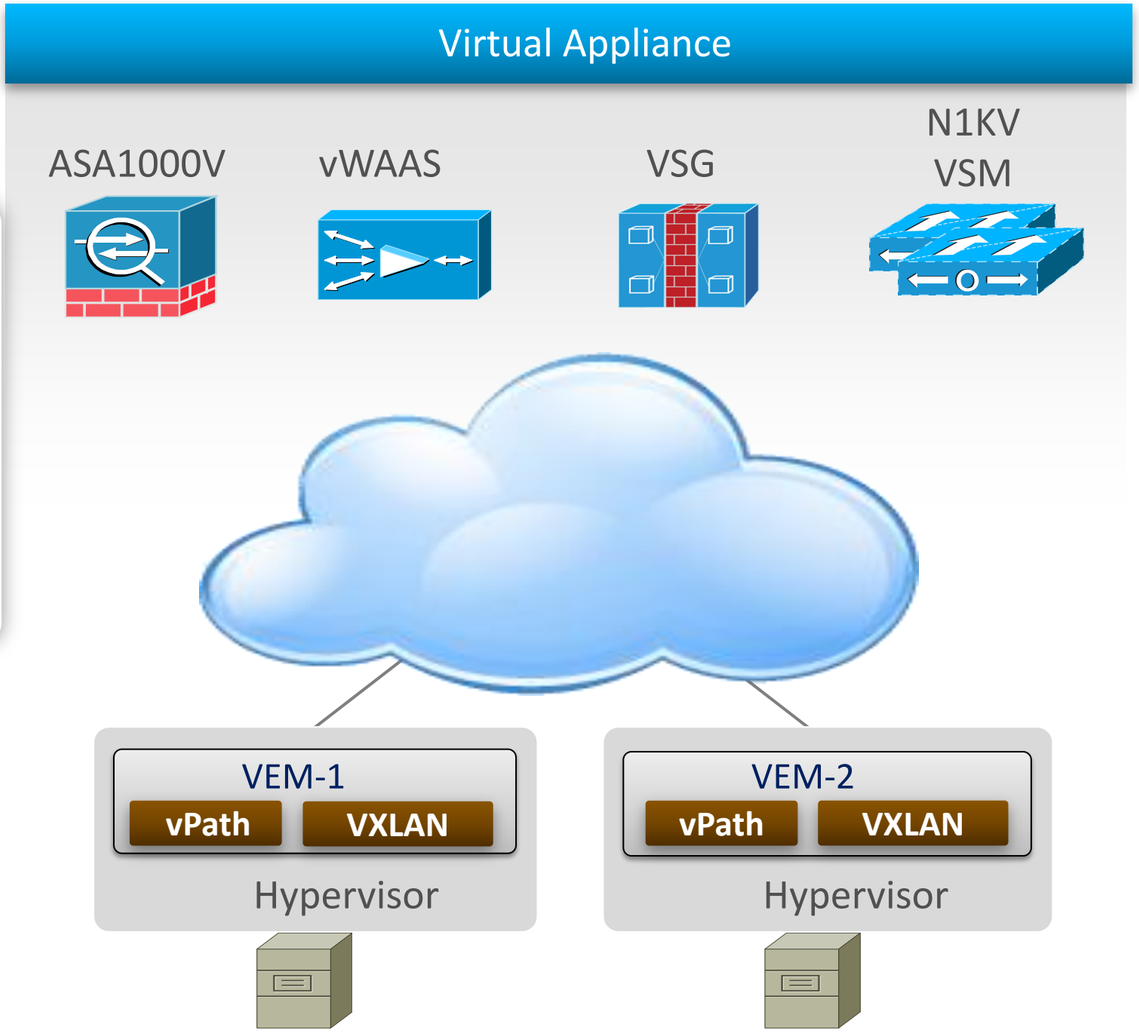
- Virtual Security Gateway

vWAAS

- Virtual WAAS

ASA 1000V

- Virtual ASA (announced)



vPath
Virtual Service Datapath

- **Service Binding**
- **Fast-Path Offload**
- **VXLAN aware***

VXLAN*
Virtual Extensible LAN

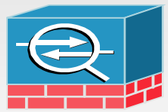
- **LAN segment over L3 (Mac-over-UDP)**
- **16M LAN segments**
- **Submitted to IETF with VMware, Citrix, RedHat, …**

Nexus 1010 / 1010-X

Hosting Platform for Virtual Services

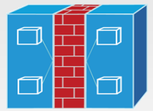
Virtual Appliance

ASA 1000V

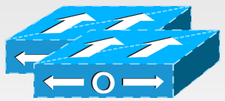


vWAAS

VSG



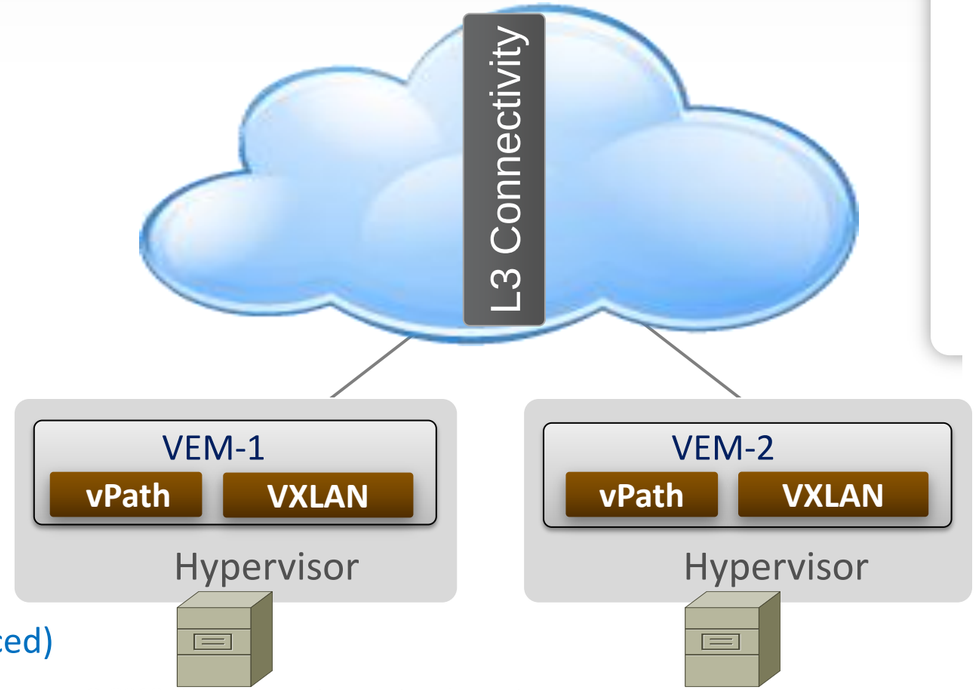
VSM



Nexus 1110 / 1110-X

Primary

Secondary



Nexus 1010 / 1010-X

NX-OS based physical (server) appliance

Access to VM mgmt tools NOT required

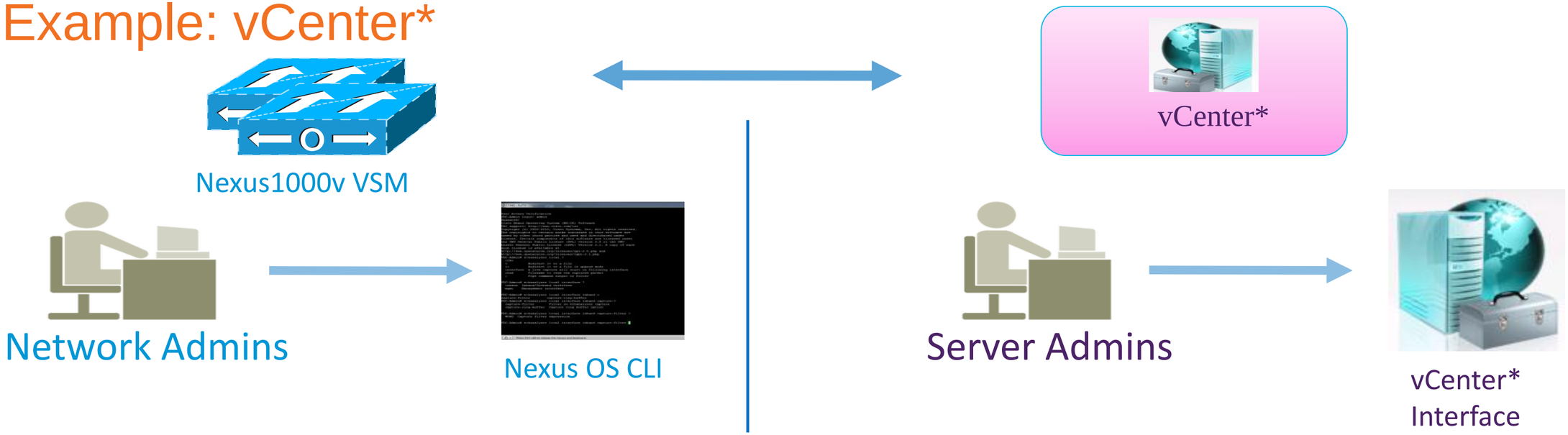
Network team deploys & manages it

Up to 10 virtual blades on Nexus 1010-X

Hypervisors:
vSphere (shipping); Win8/Hyper-V (announced)

Operational Segregation

Example: vCenter*



- Create or Update port-profiles

- Install hypervisor on hosts with N1KV VEM
- Create VM and assign Port profiles to VM

No hand-off required between Server and Network Admins for Virtualised environment

*SCVMM for Win8/Hyper-V

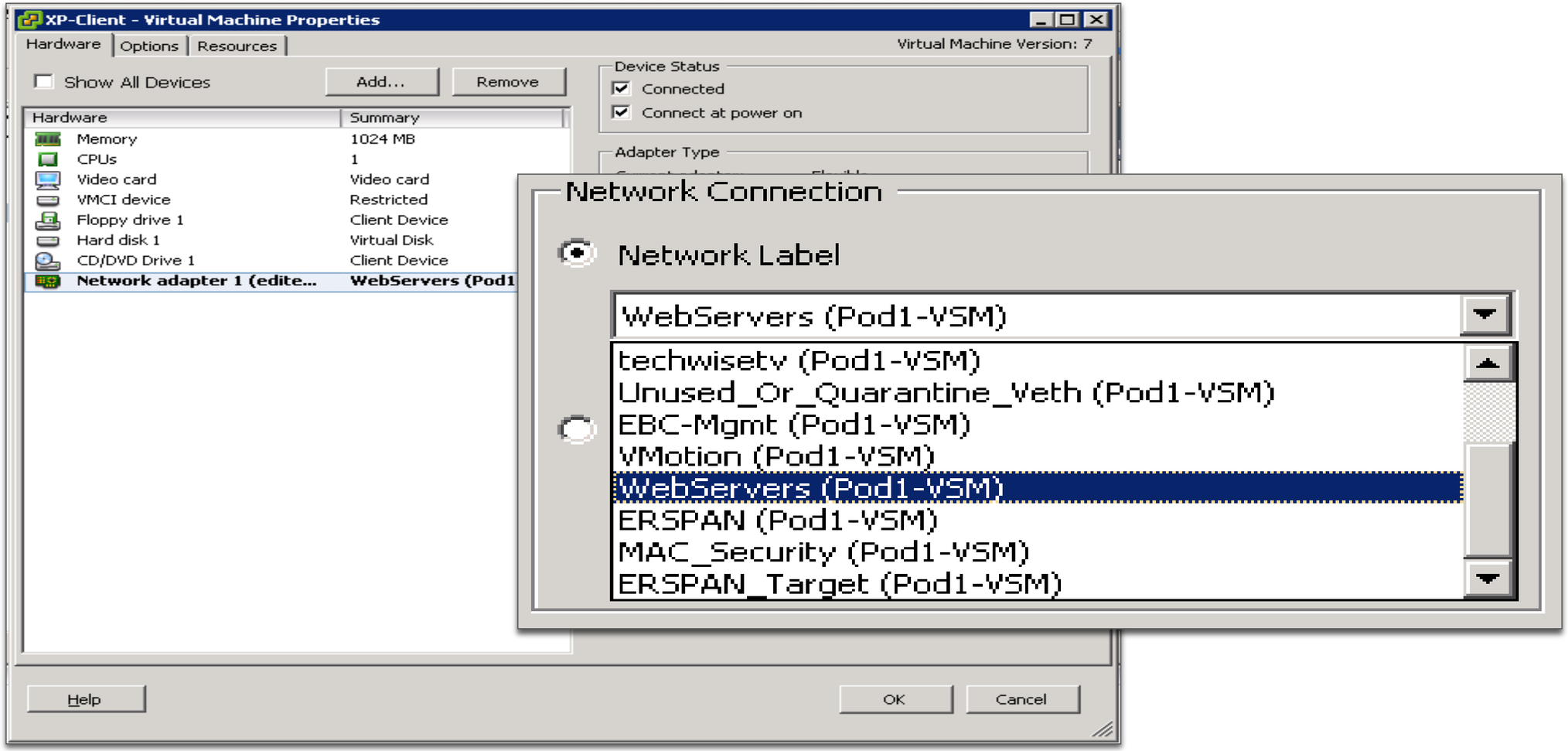
Port Profile Configuration

```
n1000v# show port-profile name WebProfile
port-profile WebServers
  description:
  status: enabled
  capability uplink: no
  system vlans:
  port-group: WebServers
  config attributes:
    switchport mode access
    switchport access vlan 110
    no shutdown
  evaluated config attributes:
    switchport mode access
    switchport access vlan 110
    no shutdown
  assigned interfaces:
    Veth10
```

Support Commands Include:

- ✓ Port management
- ✓ VLAN
- ✓ PVLAN
- ✓ Port-Channel
- ✓ ACL
- ✓ Netflow
- ✓ Port security
- ✓ QoS

Port Groups: VI Admin View



Cisco Nexus 1000V

Faster VM Deployment

Cisco Virtual Machine Networking

Policy-Based VM Connectivity

Port Profile

Defined Policies

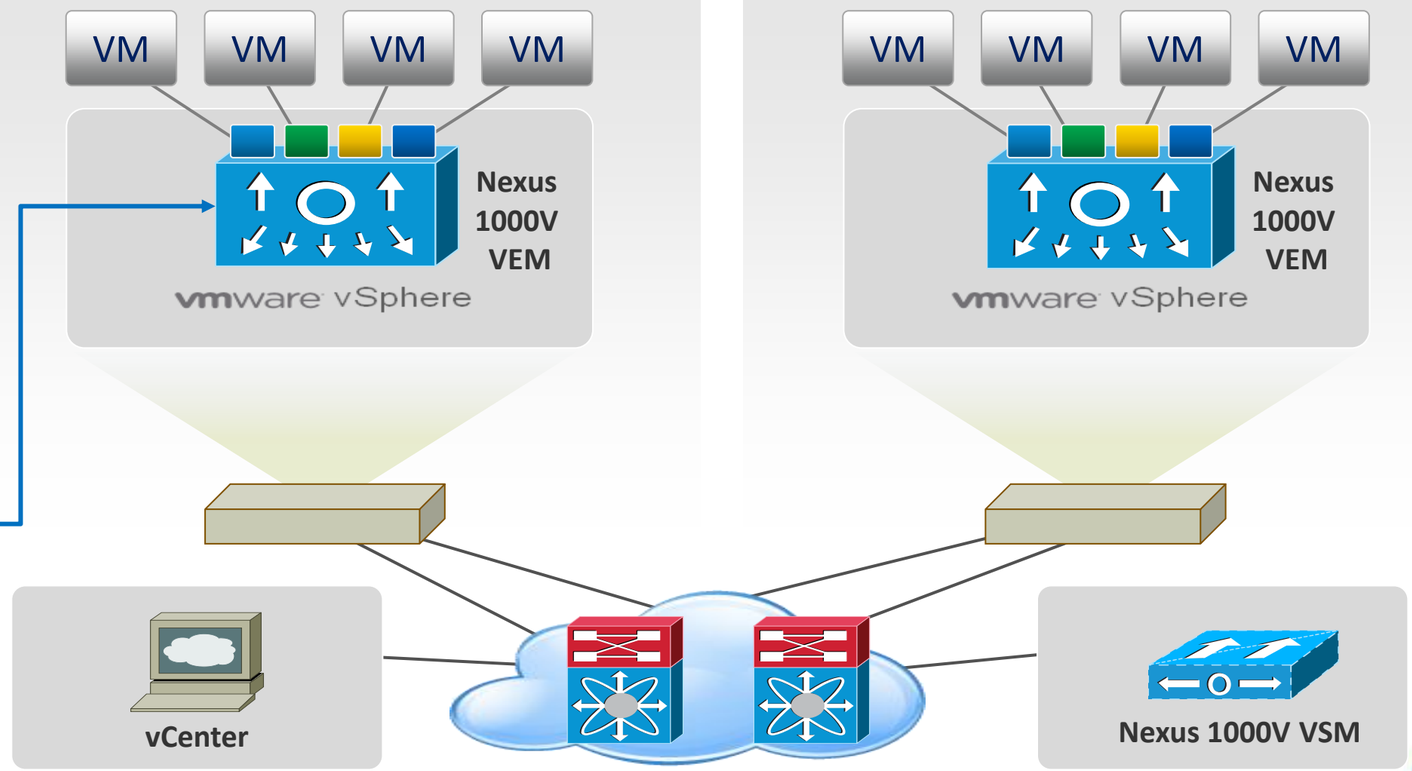
- WEB Apps
- HR
- DB
- DMZ

VM Connection Policy

- Defined in the network
- Applied in Virtual Centre
- Linked to VM UUID

Mobility of Network and Security Properties

Non-Disruptive Operational Model



Cisco Nexus 1000V

Richer Network Services

Cisco Virtual Machine Networking

Policy-Based VM Connectivity

Mobility of Network and Security Properties

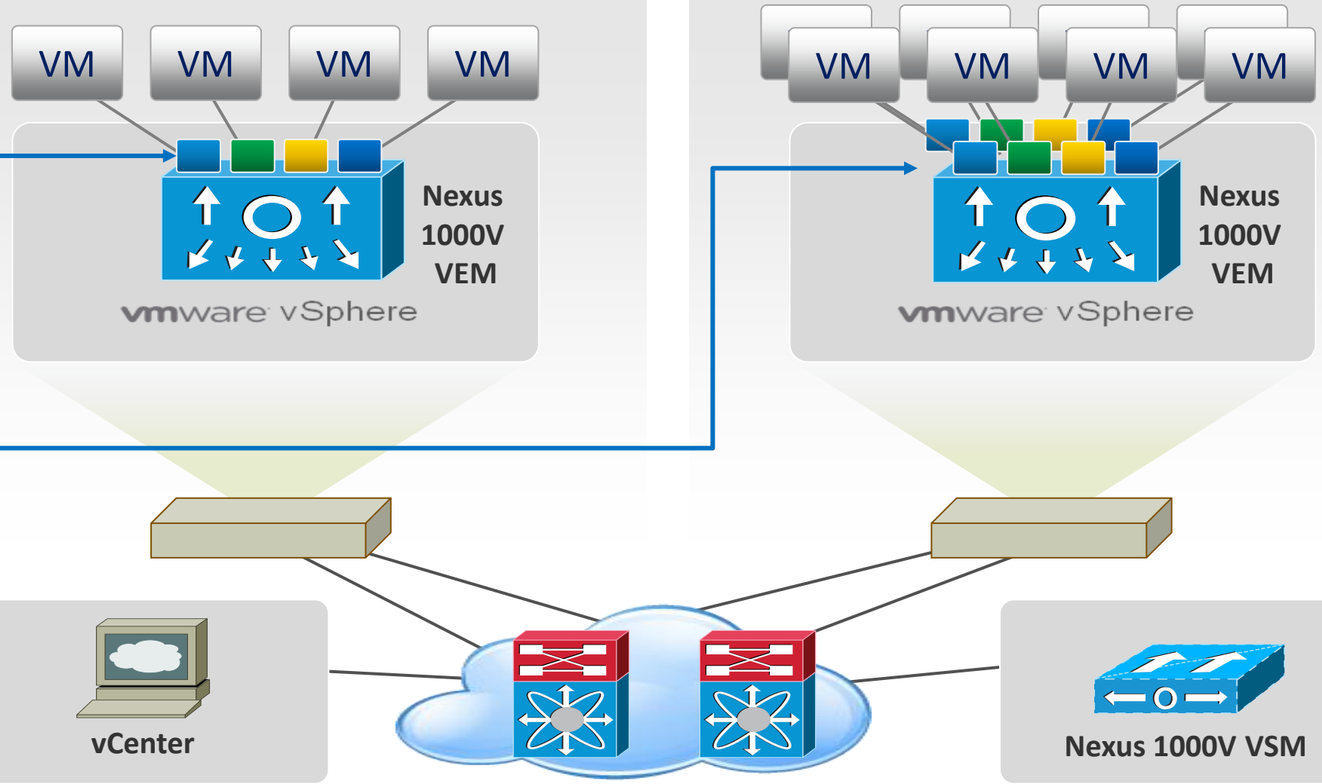
Non-Disruptive Operational Model

VMs Need to Move

- VMotion
- DRS
- SW upgrade/patch
- Hardware failure

N1KV Property Mobility

- VMotion for the network
- Ensures VM security
- Maintains connection state



Advanced Features of the Nexus 1000V

Switching	VLAN/VXLAN, IGMP Snooping, QoS Marking (COS & DSCP), Class-based WFQ
Security	Policy Mobility, Private VLANS, Access Control Lists , Port Security, Dynamic ARP inspection, IP Source Guard, DHCP Snooping
Network Services	vPath technology to support services e.g. VSG, vWAAS
Provisioning	Automated vSwitch Config, Port Profiles, Virtual Centre Integration
Visibility	vMotion, NetFlow v.9 w/ NDE, CDP v.2, VM-Level Interface Statistics, SPAN & ERSPAN (policy-based)
Management	Cisco CLI, Radius, TACACs, Syslog, SNMP (v.1, 2, 3

IPv6 Support: As a Layer-2 switch, Nexus 1000V supports forwarding of IPv6 packets as well as Layer-2 features such as PVLAN and Port Security. Also, management interface can be assigned an IPv6 address.

Nexus 1000V Interoperability with VMware

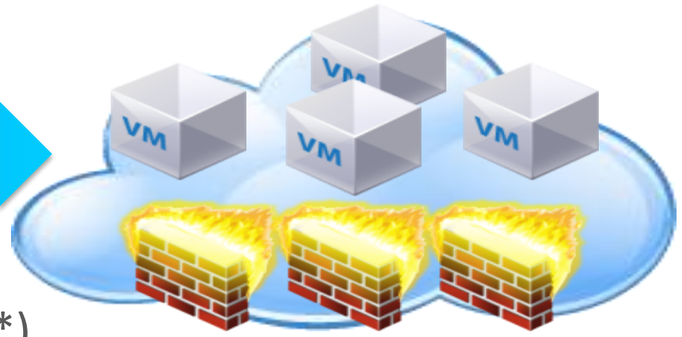
VMware Product	Nexus 1000V support
vSphere 4	☑
vSphere 5 (with stateless ESX)	☑ (Release 1.4a & above)
VMware View 5	☑
VMware vCloud Director • Port-group backed pools	☑
VMware vCloud Director 5.1 • Port-group backed pools • VLAN-backed pools • Network-isolation backed pools (via VXLAN)	☑ (Release 2.1)

Implementing Virtual Network Services

- Virtual Security Gateway (VSG)
- ASA 1000V
- Virtual WAAS (vWAAS)
- NAM on Nexus 1110
- 3rd Party Services

Defence in Depth Security Model

VSG
(and ASA 1000V*)



Virtual Security

- Policy applied to VM zones
- Dynamic, scale-out operation
- VM context based controls

ASA-SM

ASA 55xx

Internal Security

- Segment internal network
- Policy applied to VLANs
- Application protocol inspection
- Virtual Contexts

ASA 55xx

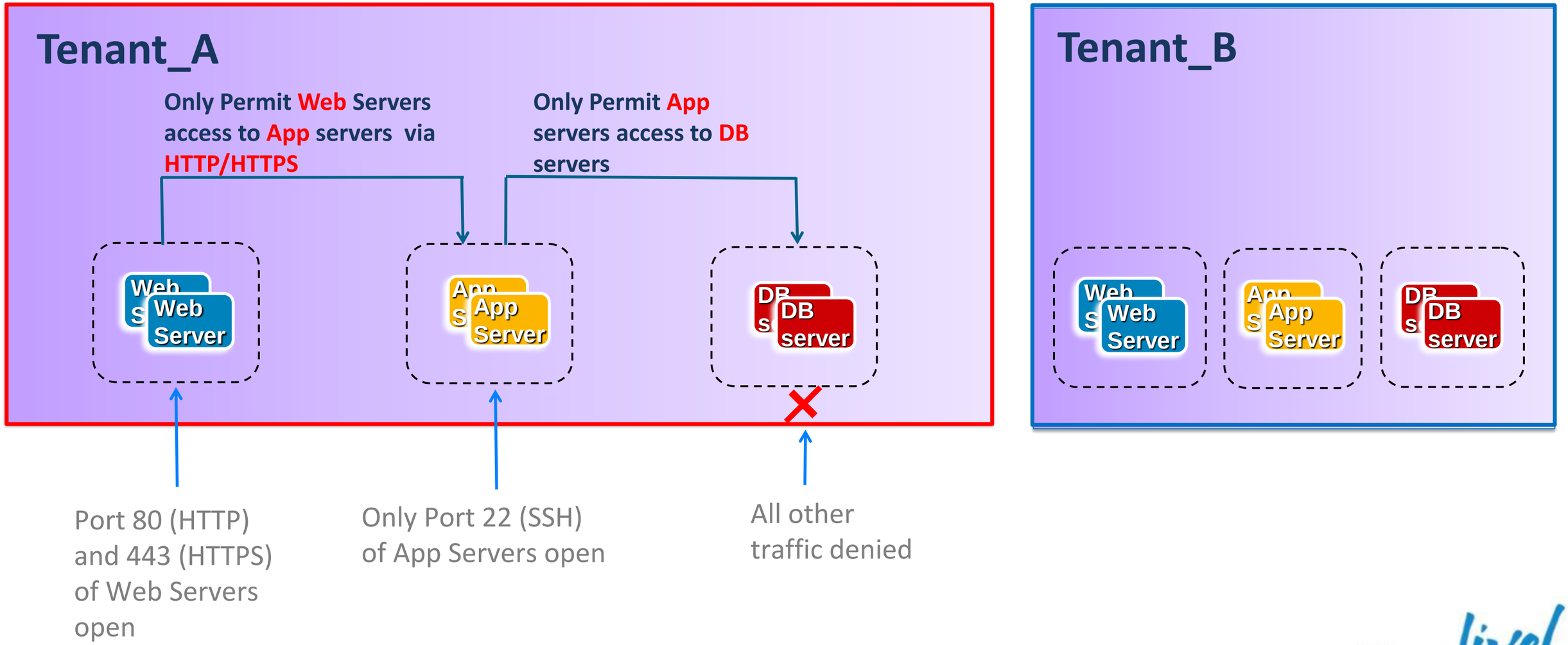
Internet Edge

- Filter external traffic
- Extensive app protocol support
- VPN access, Threat mitigation

*Announced

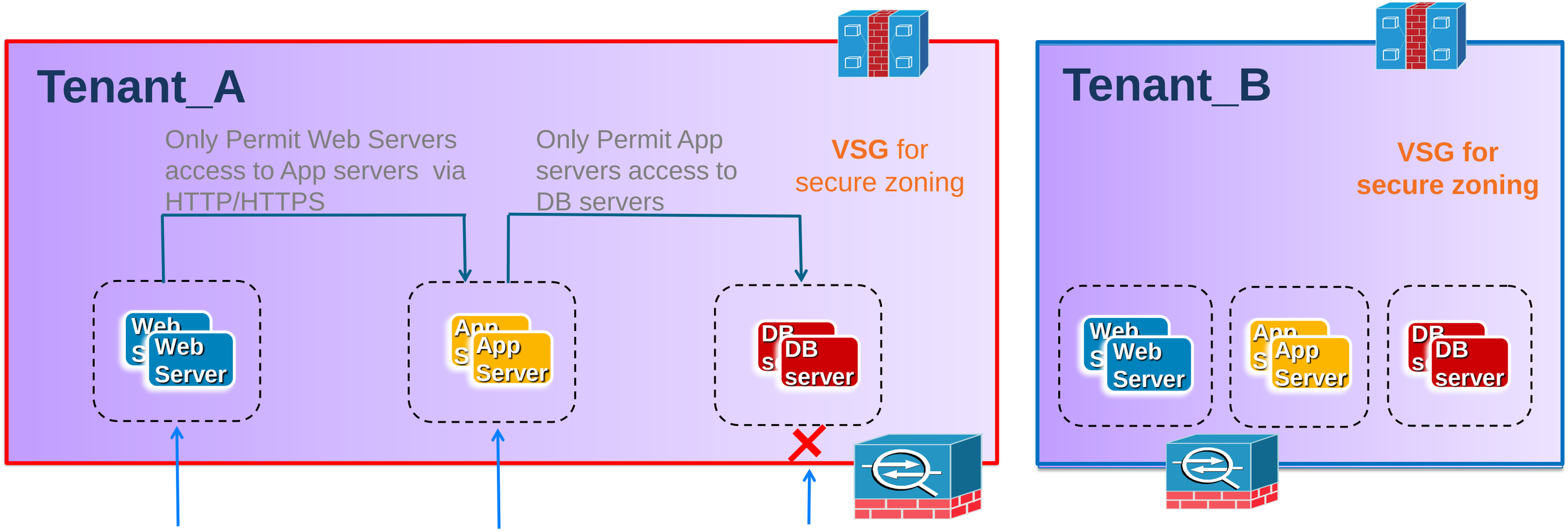
Use Case – Secure Multi-tenancy

Secure zoning of 3-Tier Application Workload



Use Case – Secure Multi-tenancy

Secure zoning of 3-Tier Application Workload



Port 80 (HTTP) and 443 (HTTPS) of Web Servers open

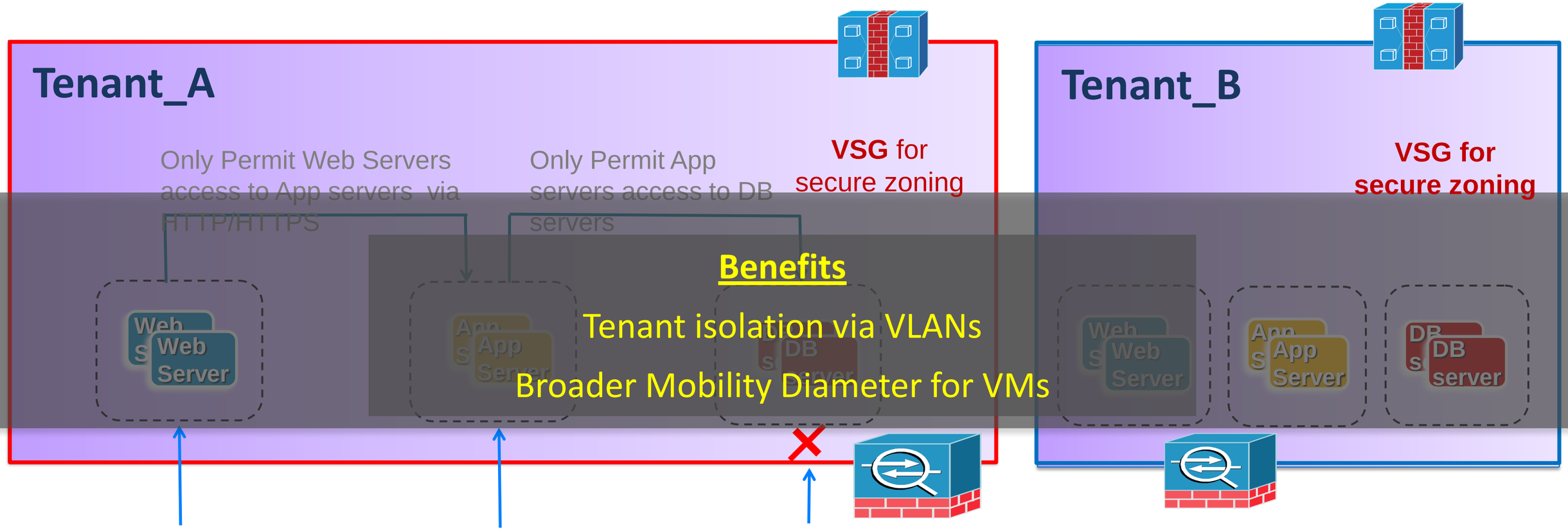
Only Port 22 (SSH) of App Servers open

All other traffic denied

ASA Firewall for Inter-tenant Edge Control (VLAN based)

Use Case – Secure Multi-tenancy

Secure zoning of 3-Tier Application Workload



Benefits

Tenant isolation via VLANs

Broader Mobility Diameter for VMs

Port 80 (HTTP) and 443 (HTTPS) of Web Servers open

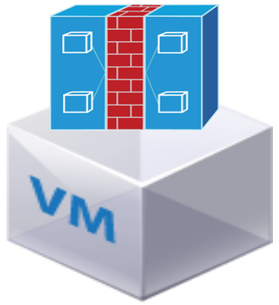
Only Port 22 (SSH) of App Servers open

All other traffic denied

ASA Firewall for Inter-tenant Edge Control (VLAN based)

Introducing 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 (with Nexus 1000V vPath)

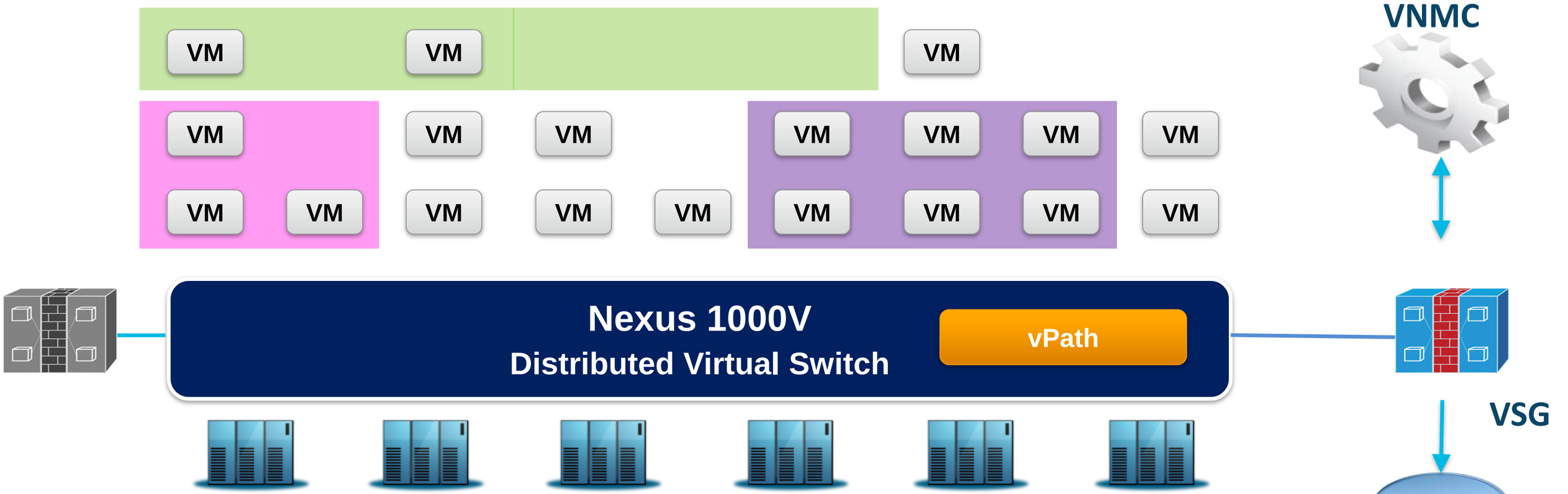
Virtual Network Management Centre (VNMC)

Non-Disruptive Operations	Security team manages security
Policy Based Administration	Central mgmt, scalable deployment, multi-tenancy
Designed for Automation	XML API, security profiles

IPv6 Support: VSG/VNMC support IPv4 packets in Phase 1. Security rules based on Ethertype can be deployed to permit or deny IPv6 packets.

Virtual Security Gateway

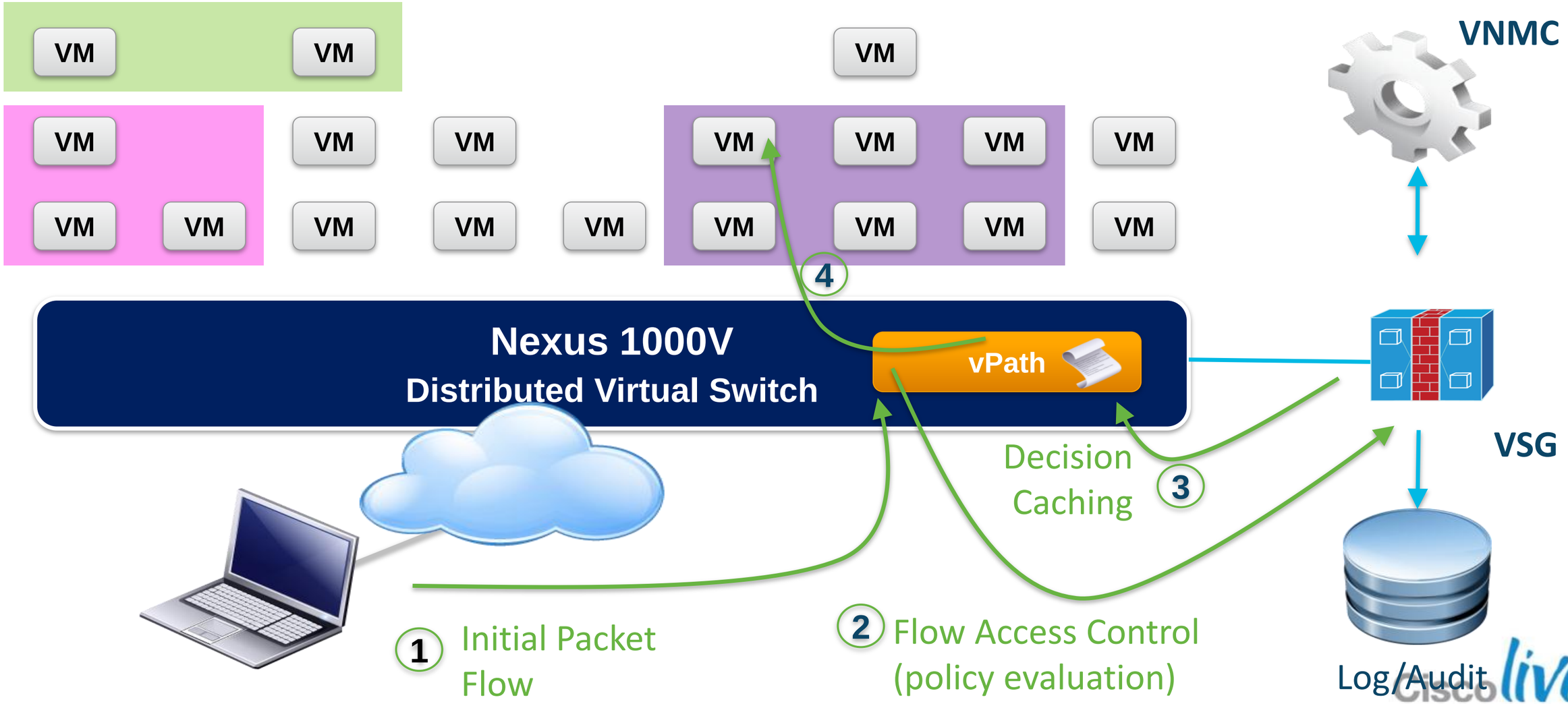
Logical deployment like physical appliances



Secure Segmentation (VLAN agnostic)	Efficient Deployment (secure multiple hosts)	Dynamic policy-based provisioning
Transparent Insertion (topology agnostic)	High Availability	Mobility aware (policies follow vMotion)

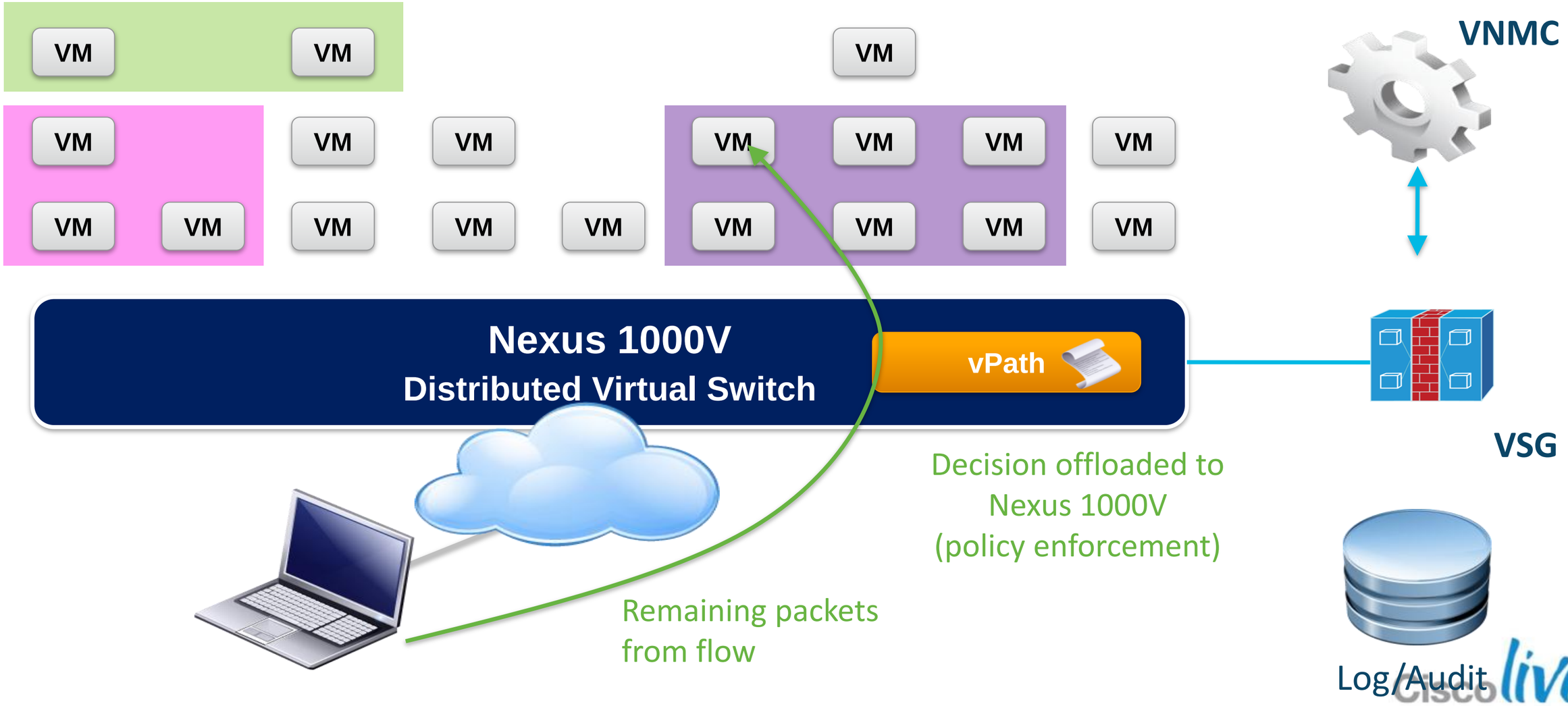
Virtual Security Gateway

Intelligent Traffic Steering with vPath

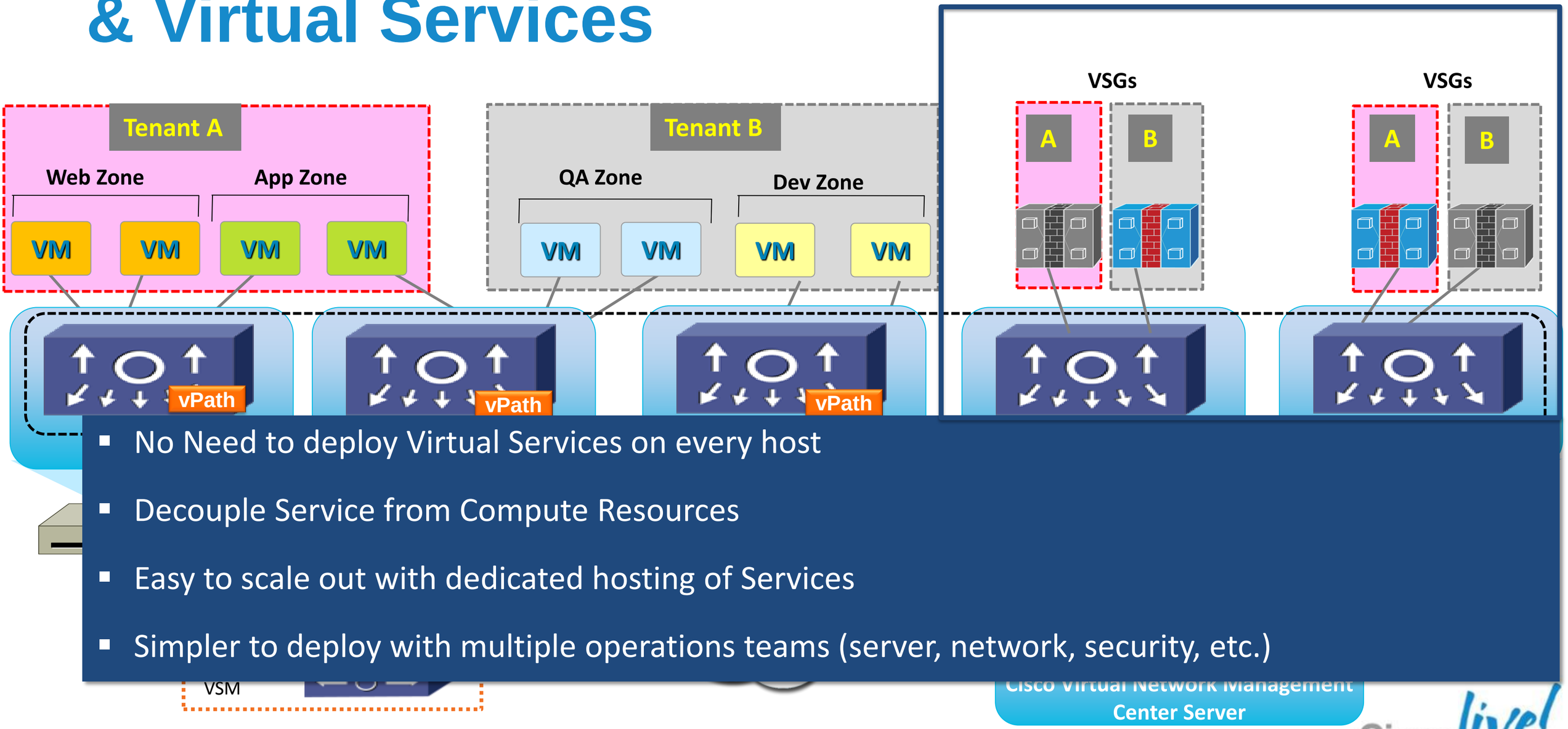


Virtual Security Gateway

Performance Acceleration with vPath



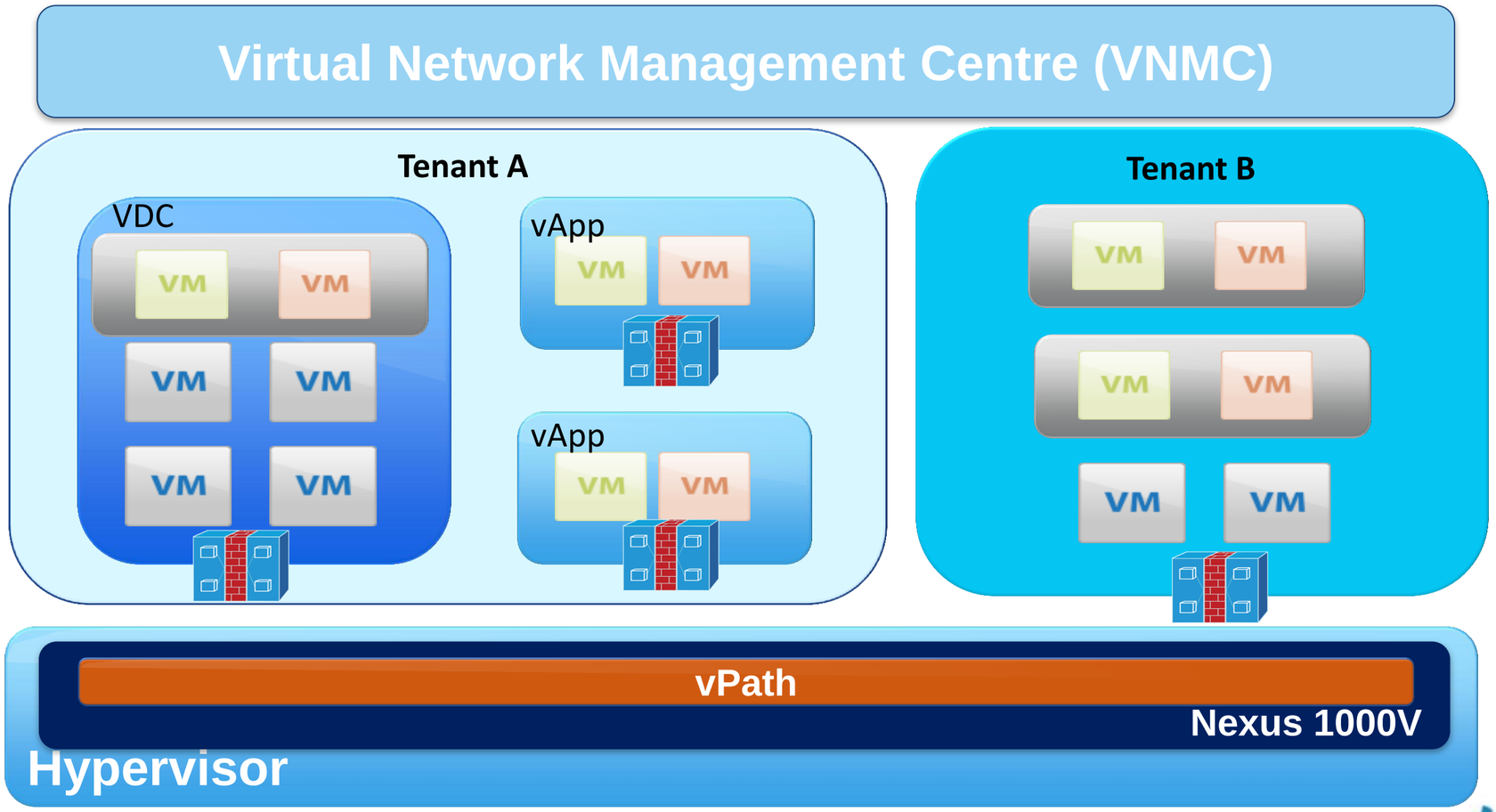
Decoupled Deployment Across Applications & Virtual Services



- No Need to deploy Virtual Services on every host
- Decouple Service from Compute Resources
- Easy to scale out with dedicated hosting of Services
- Simpler to deploy with multiple operations teams (server, network, security, etc.)

Apply Security at Multiple Levels
Enables multi-tenant scale-out deployment

- Deployment granularity depending on use case
  - Tenant, VDC, vApp
- Multi-instance deployment provides horizontal scale-out



VSG Policy: Rule (ACE) Construct

Rule

- Source Condition
- Destination Condition
- Action

Condition

Attribute Type : Network

Expression

Attribute Name : IP Address

Operator : eq

Attribute Value : 192 . 168 . 1 . 2

drop permit reset

log

Attribute Type
Network
VM
User Defined
vZone

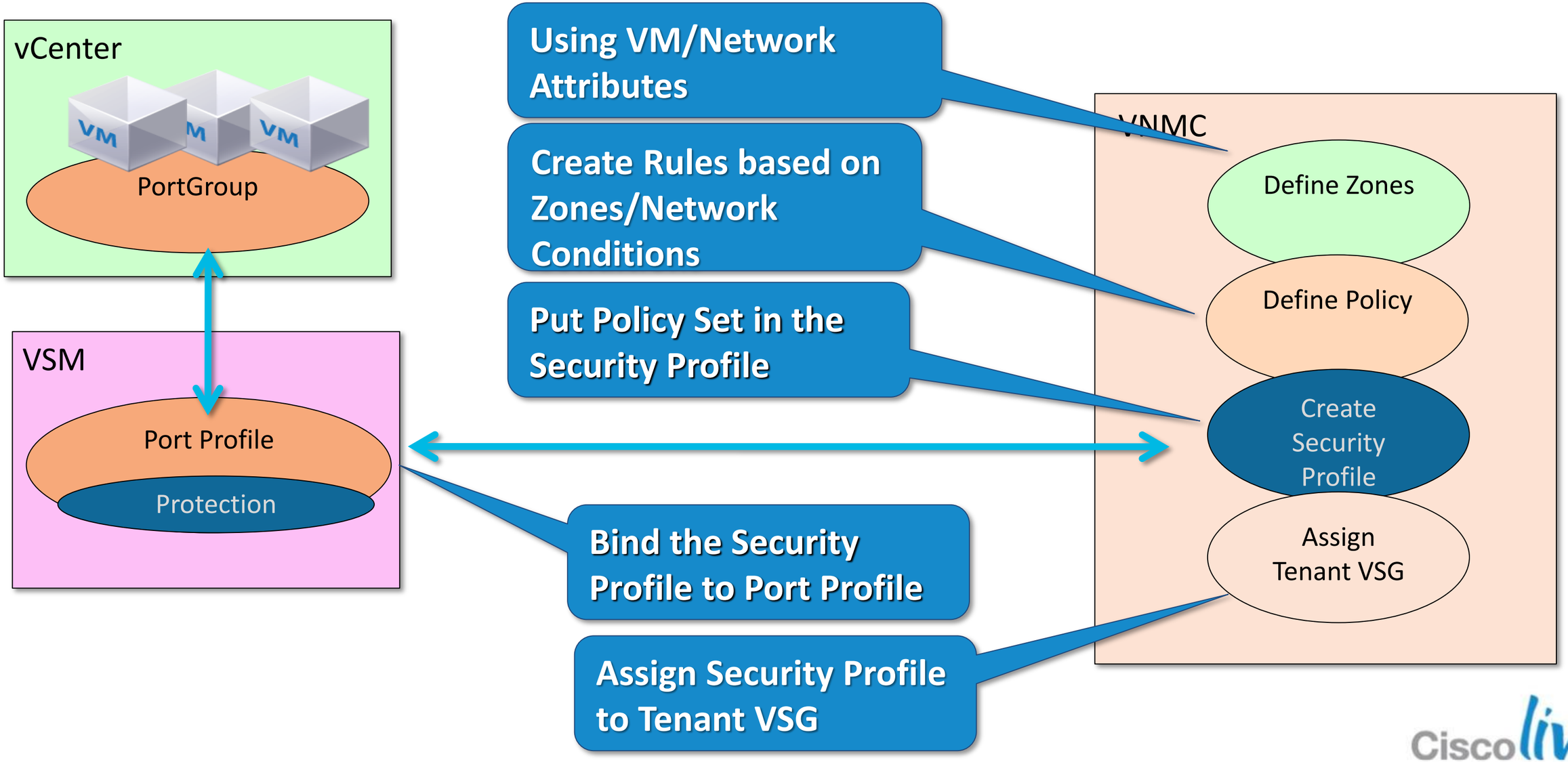
VM Attributes
Instance Name
Guest OS full name
Zone Name
Parent App Name
Port Profile Name
Cluster Name
Hypervisor Name

Network Attributes
IP Address
Network Port

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

Operator
member
Not-member
Contains

VSG Policy Provisioning Logical Flow

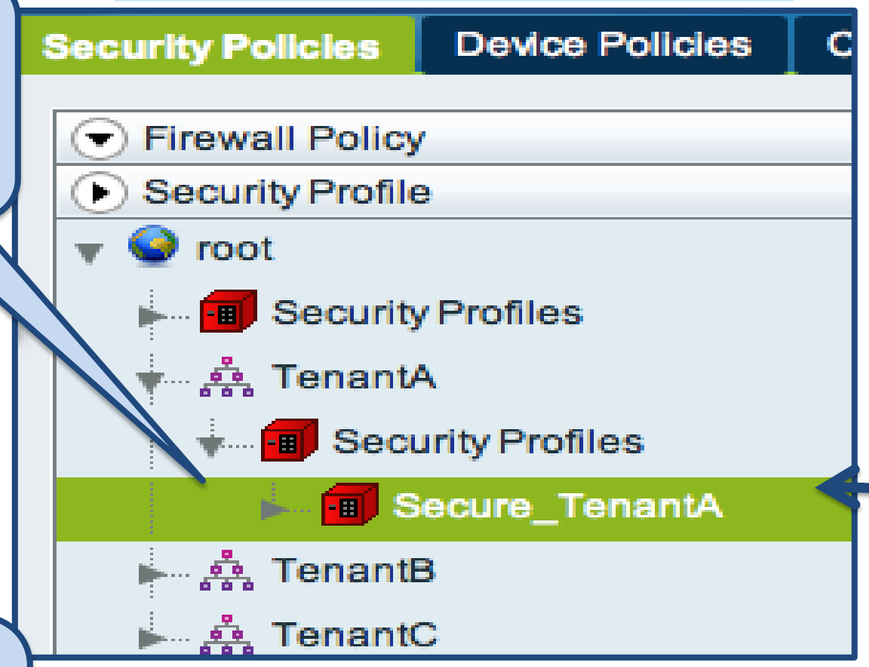


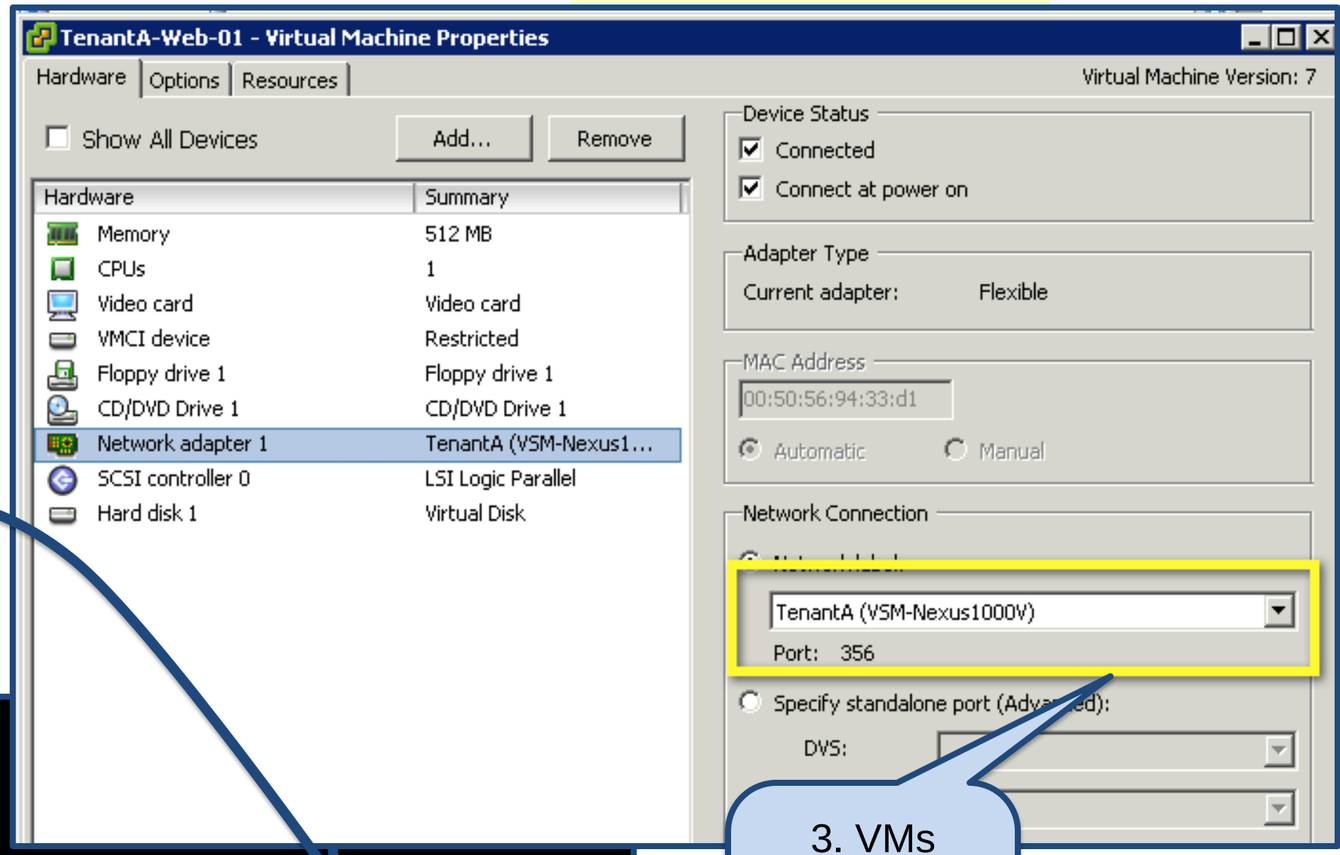
Port Profile to Security Profile Binding

VNMC – Tenant Policy Management

vCenter – VM Properties

1. Create Security Profile for Tenant A in VNMC





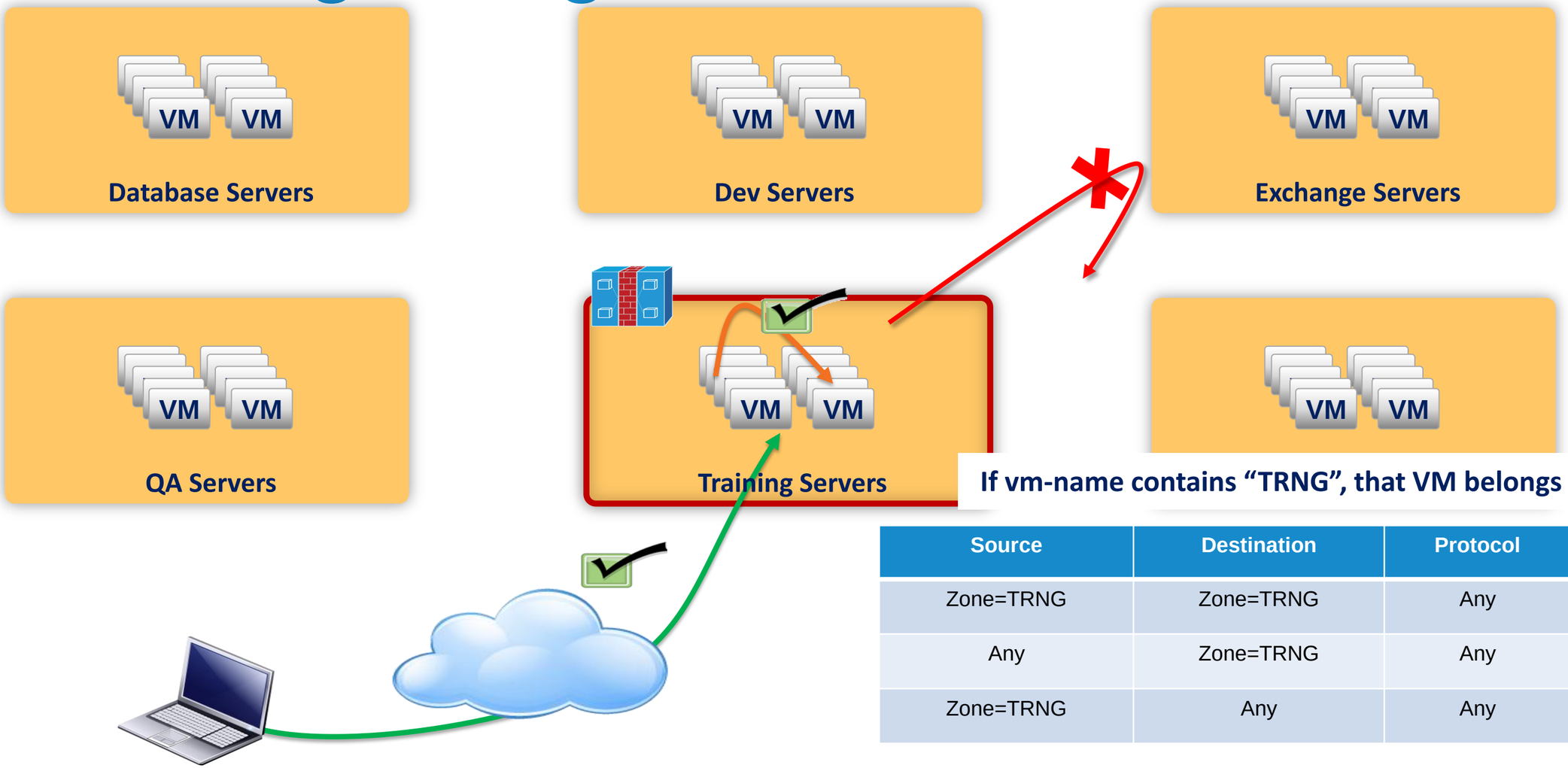
2. Bind the Security Profile with the Port-Profile for Tenant A

```
port-profile type vethernet TenantA
  vmware port-group
  switchport access vlan 10
  switchport mode access
  org root/TenantA
  vn-service ip-address 192.168.173.42 vlan 20 security-profile Secure_TenantA
  state enabled
```

Nexus 1000V

3. VMs connect to the Network with Firewall enabled

Use Case 1: Carecore National Secure Zoning Using VM Attribute

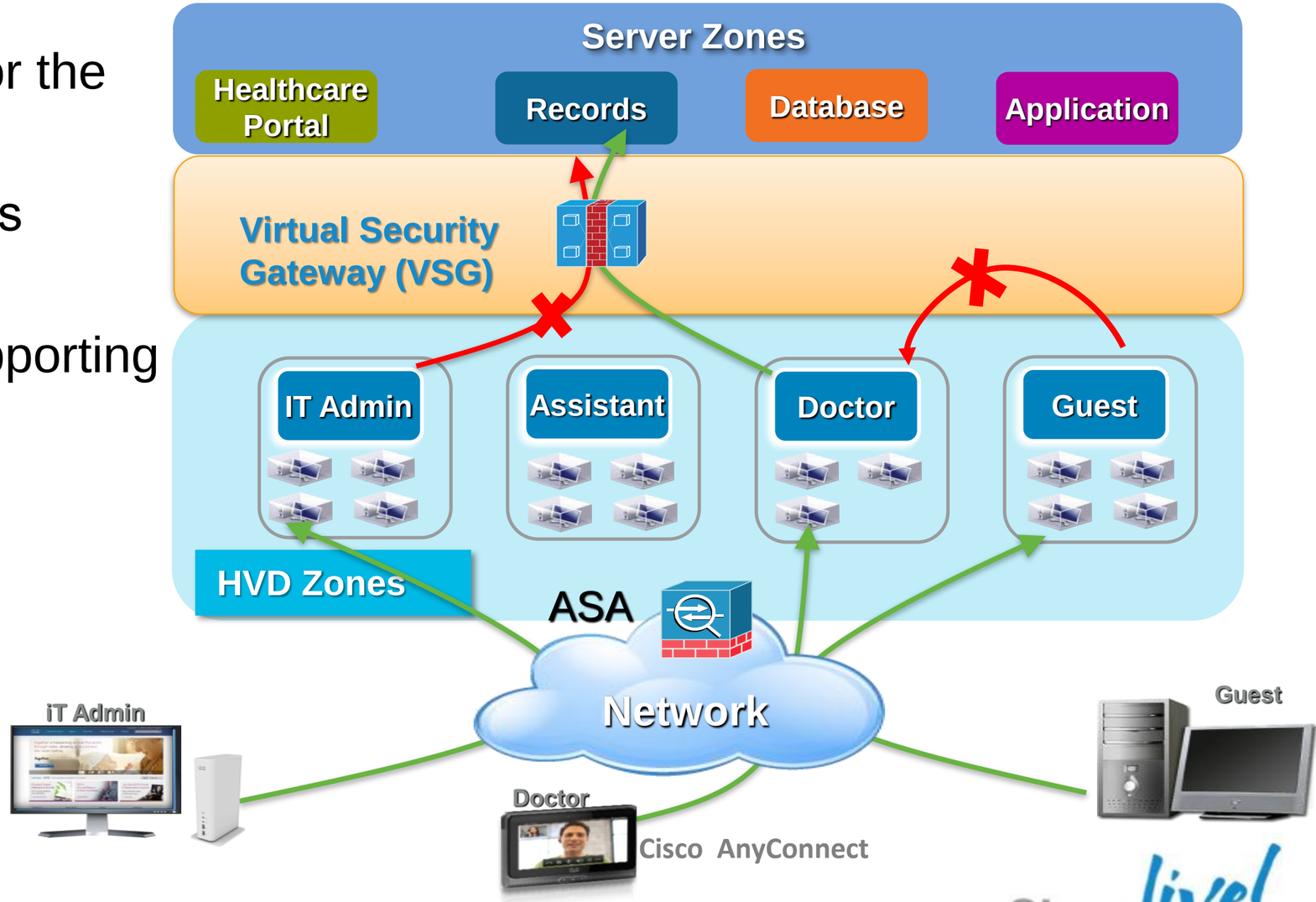


If vm-name contains "TRNG", that VM belongs to TRNG zone

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

Use Case 2
Securing VDI with Cisco VSG

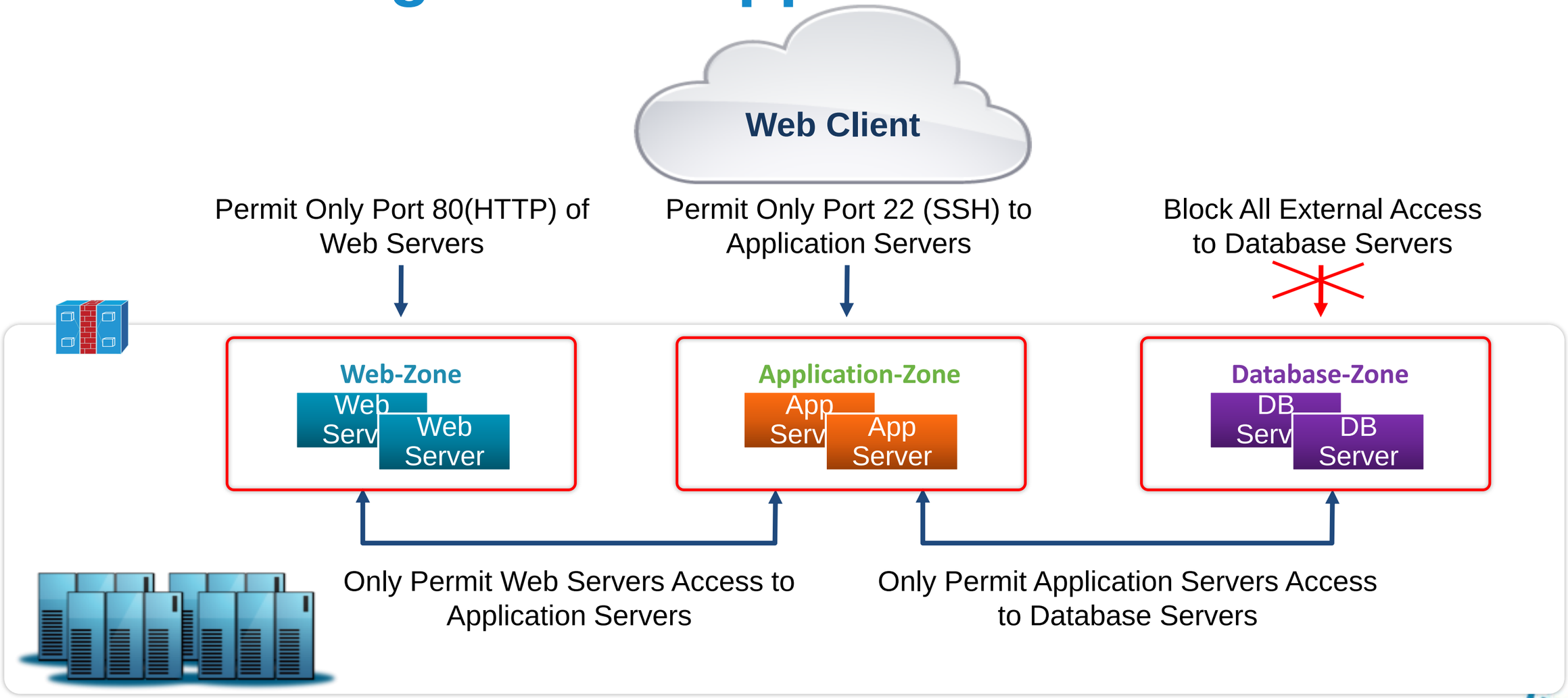
- Persistent virtual workspace for the doctor
- Flexible workspace for Doctor's assistant
- Maintain compliance while supporting IT consumerisation



Leverage VM context (eg VM-name) to create VSG security policies

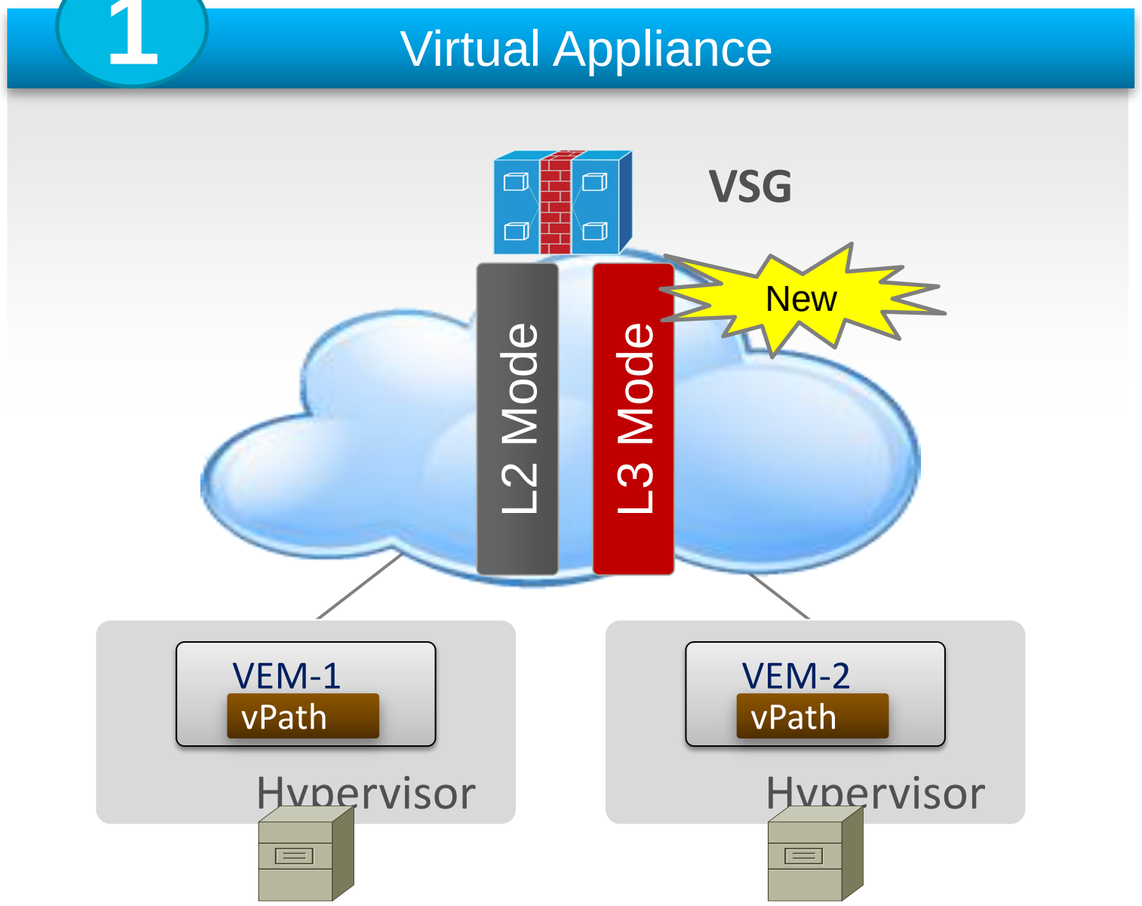
Reference Architecture:
- 1000V and VSG in VXI Reference Architecture

Use Case 3
Securing a 3-tier Application Infrastructure



VSG Release 1.3: What's New?

1



2

VMware Product	VSG & VNMC support
vSphere 4	R
vSphere 5 New	R

3 Protect VMs on VXLAN (see details in the "VM Mobility" section)

ASA 1000V

Cloud Firewall

Cisco Virtual Security Products

Virtual Security Gateway

Zone based intra-tenant segmentation of VMs

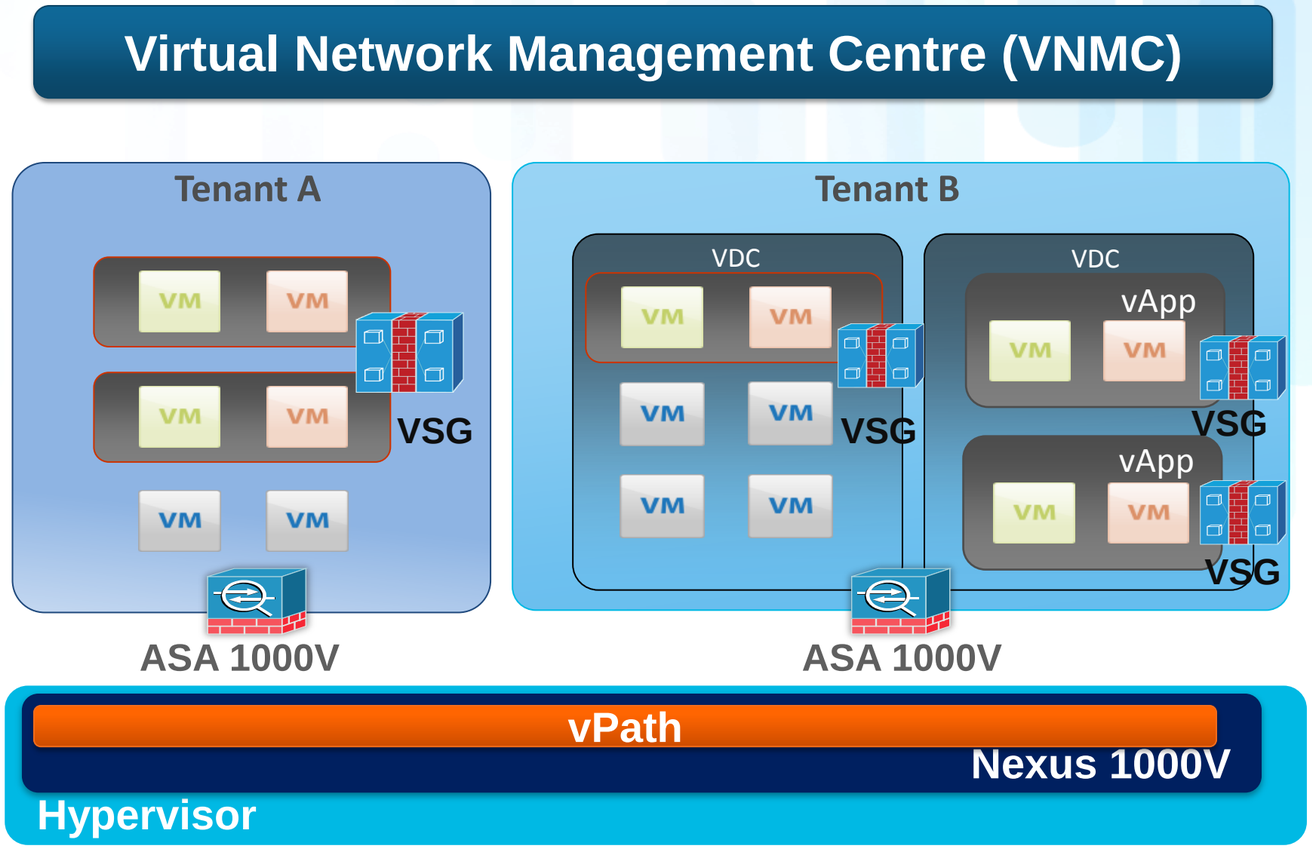
ASA 1000V

External / multi-tenant edge deployment

Securing Multi-tenant Cloud

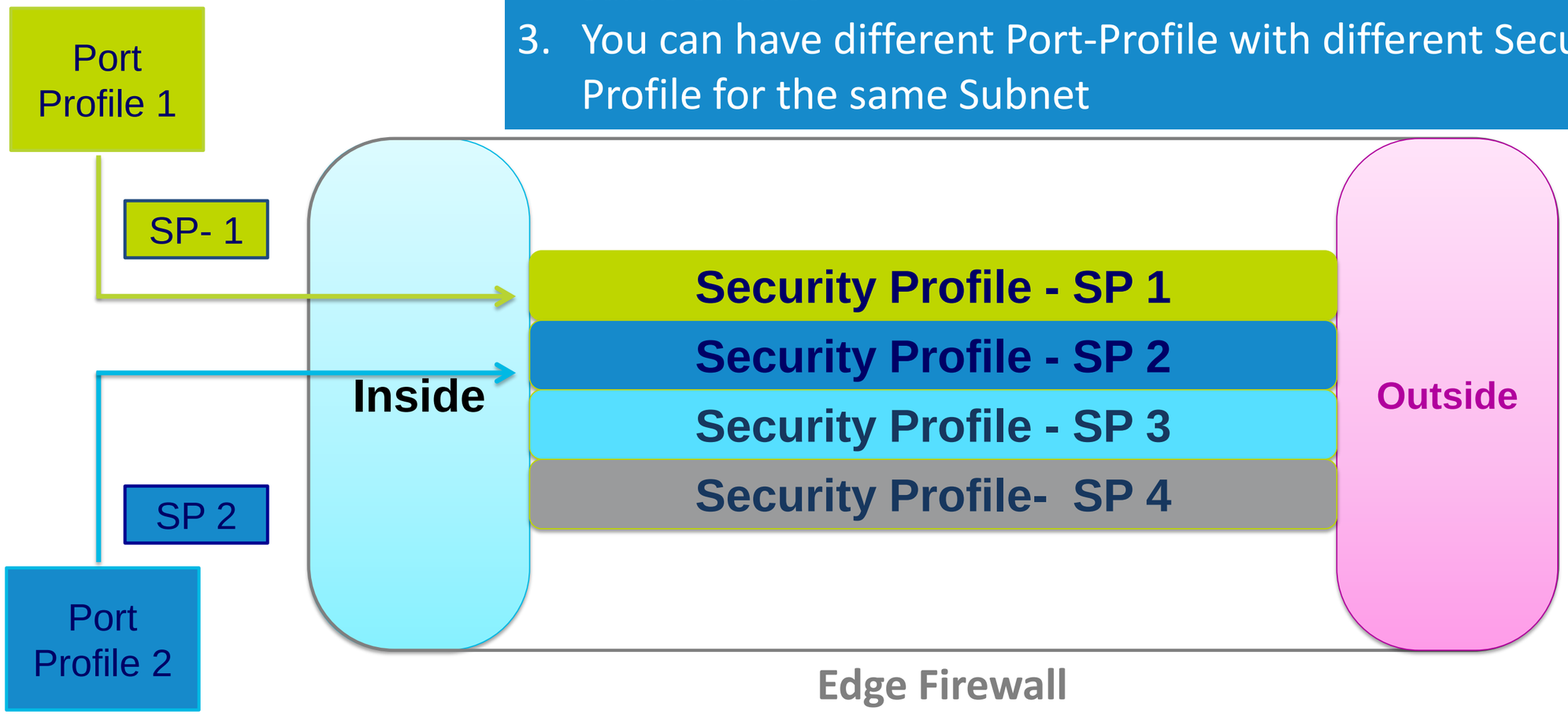
With Virtual ASA and VSG

- Proven Cisco Security…Virtualised
  - Physical – virtual consistency
- Collaborative Security Model
  - VSG for intra-tenant secure zones
  - Virtual ASA for tenant edge controls
  - Context-based controls
- Seamless Integration
  - With Nexus 1000V & vPath
- Scales with Cloud Demand
  - Multi-instance deployment for horizontal scale-out deployment

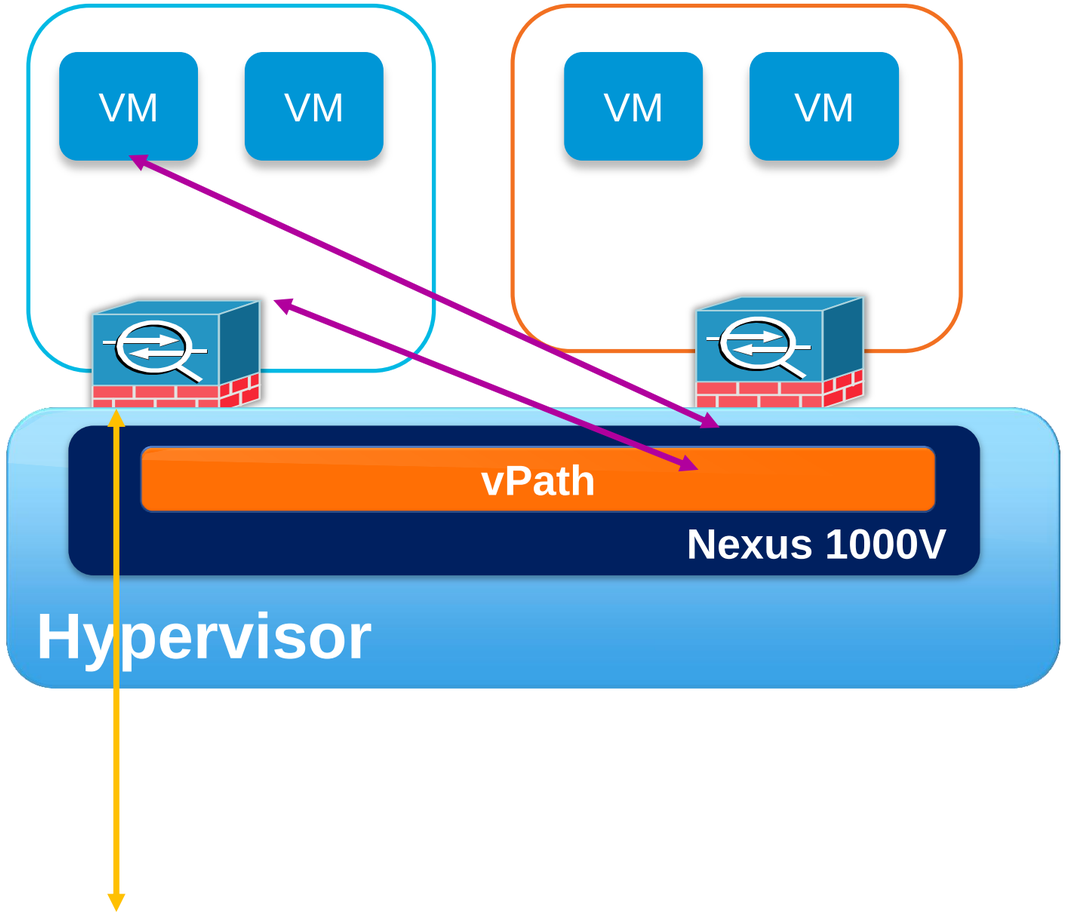


Policies Enforcement with the ASA 1000V

1. Security Policy is attached to the Port-Profile
2. No vPath encapsulation for VM to VM communication in the same subnet
3. You can have different Port-Profile with different Security Profile for the same Subnet



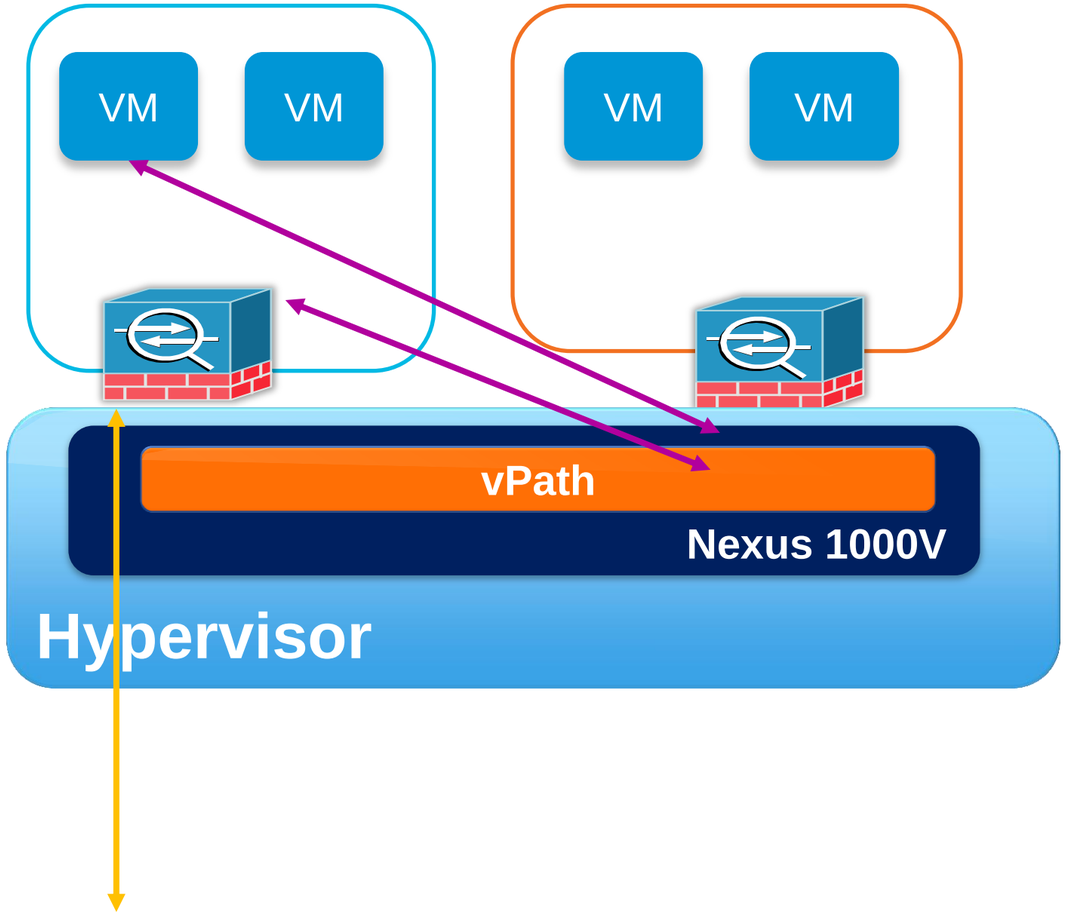
Integration with vPath: Outbound Access



1. Nexus 1000V [vPath] receives packet to be sent to the outside, looks up the security profile binding, and **attaches vPath tag.**
2. This tag contains the service profile ID for the source VM
3. ASA 1000V **creates forward and reverse flows** for the packet and **applies policy** corresponding to the security profile specified in the packet
4. **ASA 1000V 'routes' the packet** to the outside without a tag
5. Reply packet comes from the outside without any vPath tag
6. ASA 1000V **looks up the flow table, adds a vPath tag** with the Service profile ID cached in flow table
7. vPath receives the packet, removes the tag and forwards it to the VM

For Your Reference

vPath as Data Plane: Inbound Access



1. Packet from the outside hits ASA 1000V, which **performs NAT translation** to get the internal VM IP address.
2. ASA 1000V **consults the VM IP address to service profile binding database** received from VNMC,
3. ASA 1000V **creates forward and reverse flows** for this packet, **adds a vPath tag** with Service profile ID, and forwards packet to the destination VM
4. The VM responds with a packet which reaches vPath
5. vPath **adds vPath tag** (same as previous) and forwards to ASA
6. ASA 1000V receives the packet, **matches it to the flow created previously,** applied NAT and **forwards it to the outside** without the vPath tag

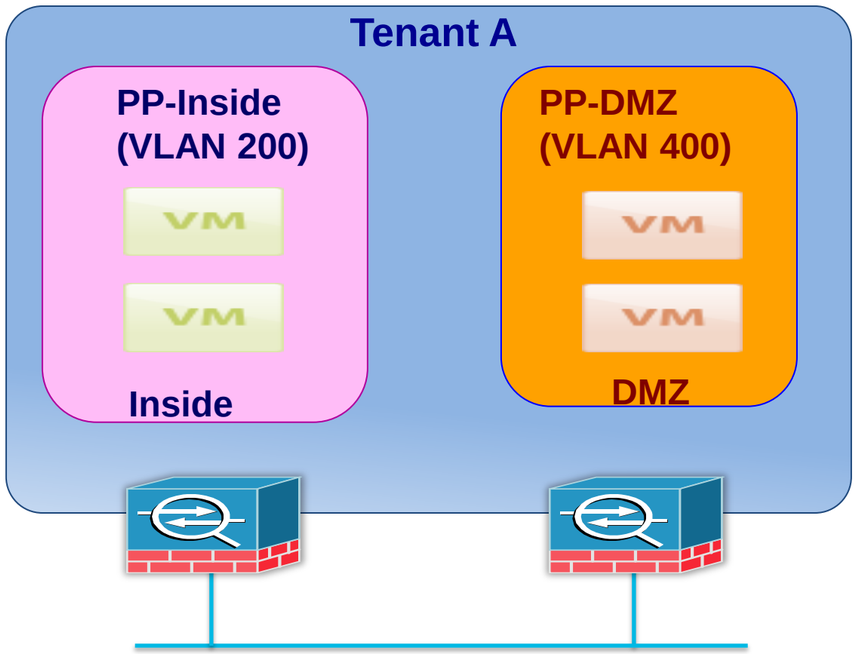
For Your Reference

DMZ Use Cases

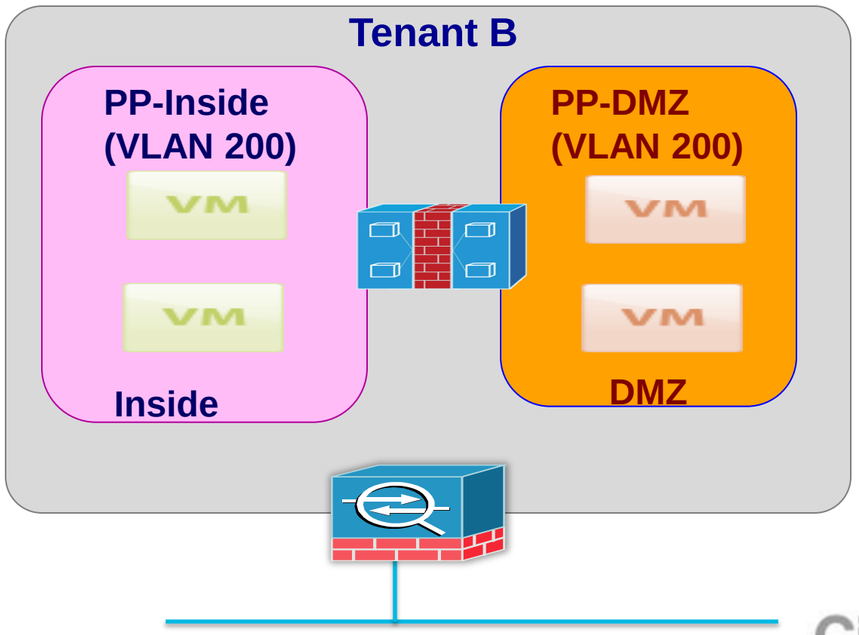
ASA 1000V DMZ Use Case

- Two ASA 1000V Approach
- Two Edge Firewalls one for inside subnet and other for DMZ subnet
- No enforcement within Inside and DMZ VLAN

- ASA 1000V and VSG Approach
- Inside Security Profile and DMZ Security Profile addressing the security requirements for both Zones
- Shared VLAN for both DMZ and Inside



PP- Port-Profile
SP- Security Profile



ASA 1000V 1.0: Features and Capabilities

- NAT
- IPSec VPN (Site-to-Site)
- Default Gateway
- DHCP
- Static Routing
- Stateful Protocol
- IP Audit

Role based separation

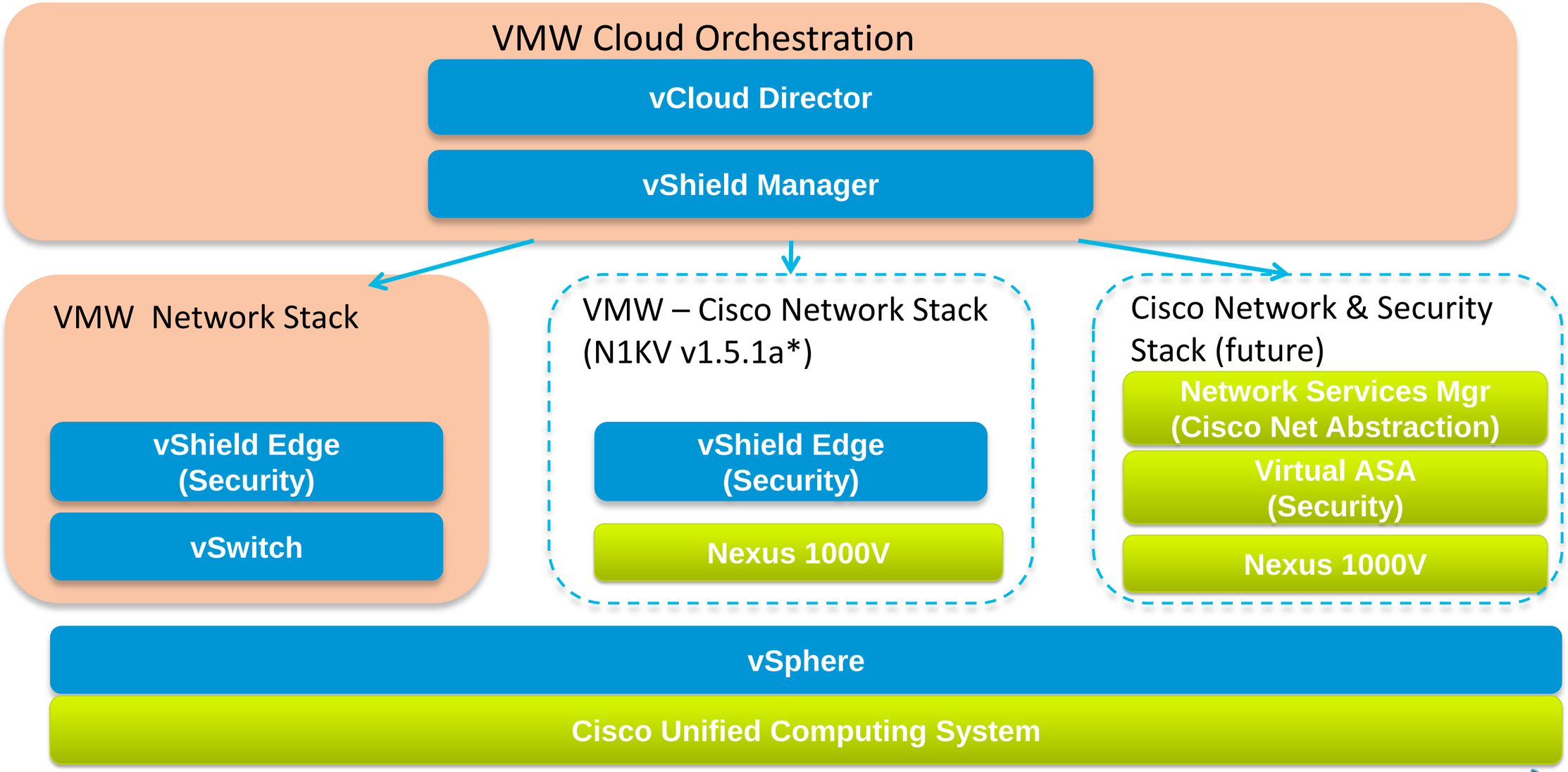
Consistent ASA feature set

Intelligent traffic steering via vPath

Strategic Partnership with VMWare

Not just an ASA – Part of a solution which benefits from vPath

vCD Technology Integration Roadmap

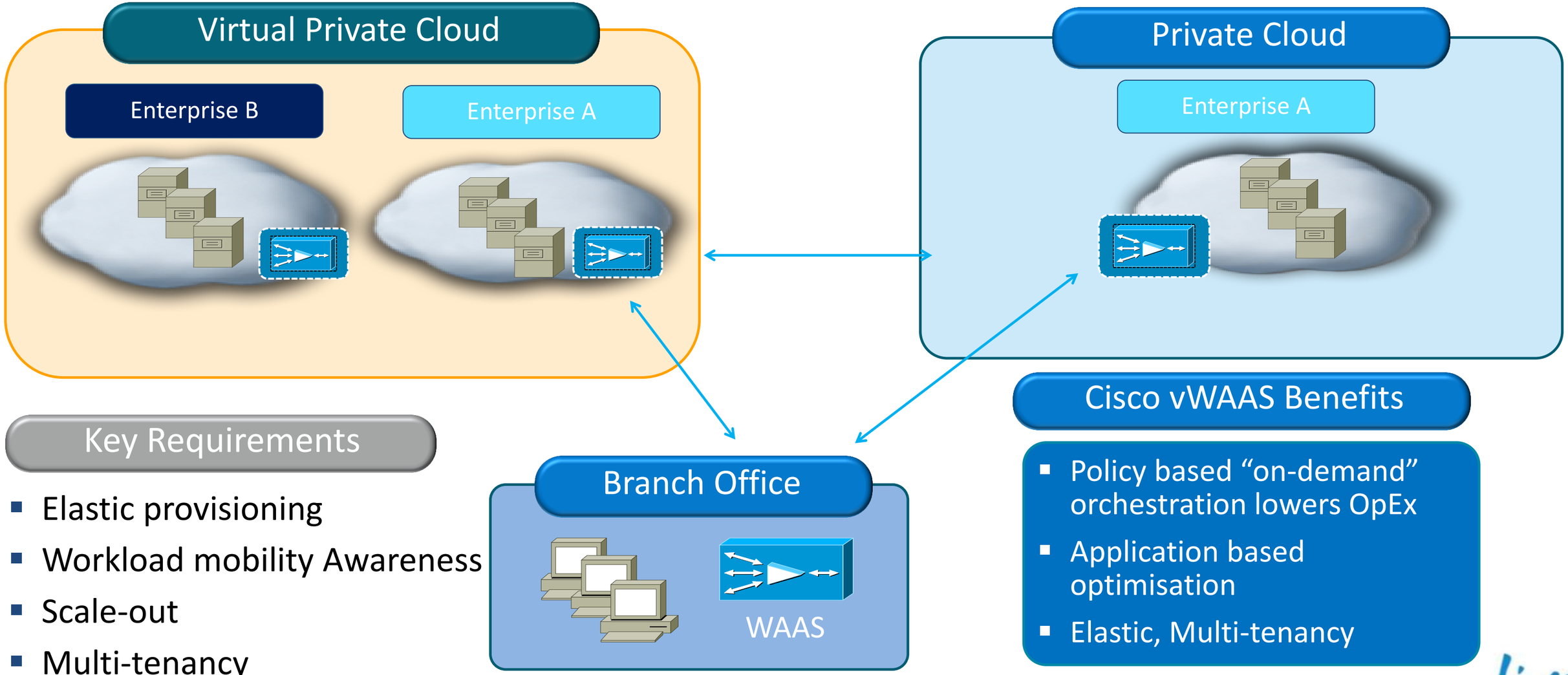


Continue future innovations across virtual/hypervisor and physical security

Virtual WAAS

Cisco vWAAS Accelerates Cloud Deployment

Accelerate cloud-bursting, workload mobility, virtualised deployment



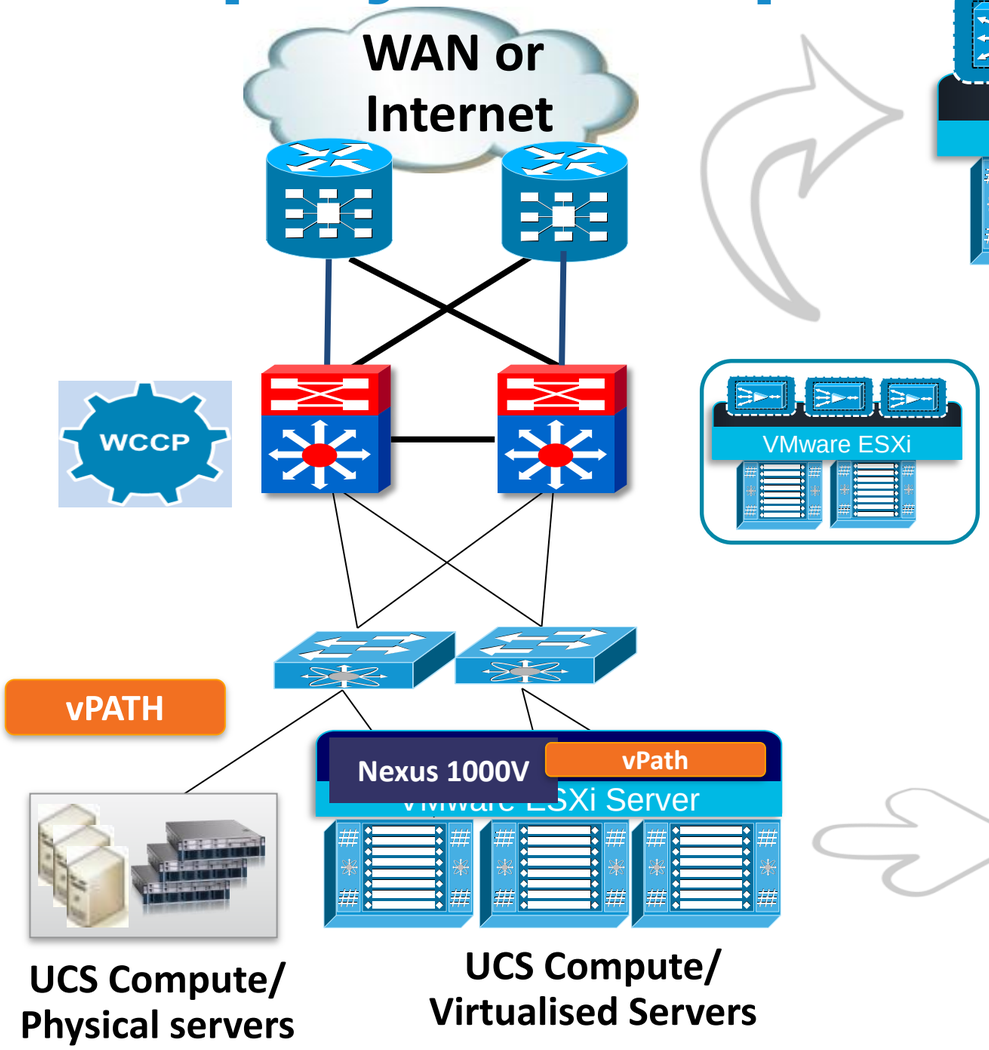
Key Requirements

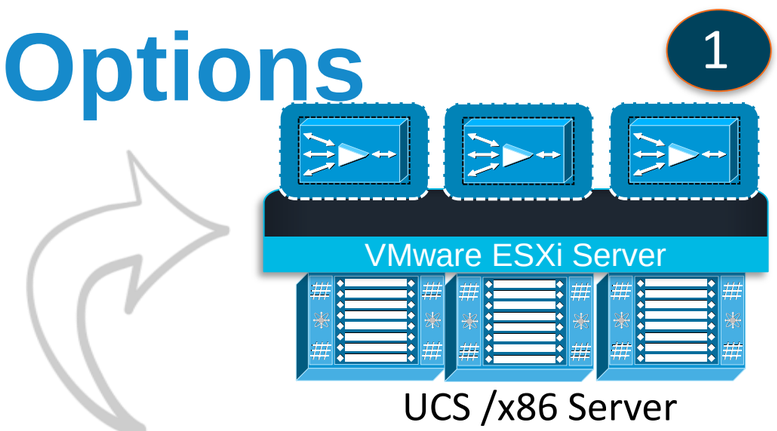
- Elastic provisioning
- Workload mobility Awareness
- Scale-out
- Multi-tenancy

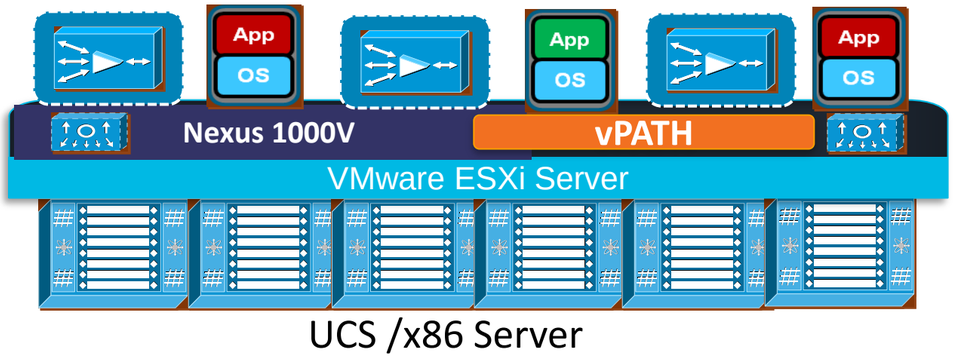
Cisco vWAAS Benefits

- Policy based "on-demand" orchestration lowers OpEx
- Application based optimisation
- Elastic, Multi-tenancy

Cisco vWAAS Provides Flexible Cloud Deployment Options







1

Private Cloud

- Traditional WAN Edge Deployment at Branch and DC
- Gradual migration from Physical to Virtual
- Multi-tenancy support

2

Private Cloud, Virtual Private Cloud, & Public Cloud

- Re-direction using vPath @VM level
- Elastic provisioning
- Multi-tenancy support

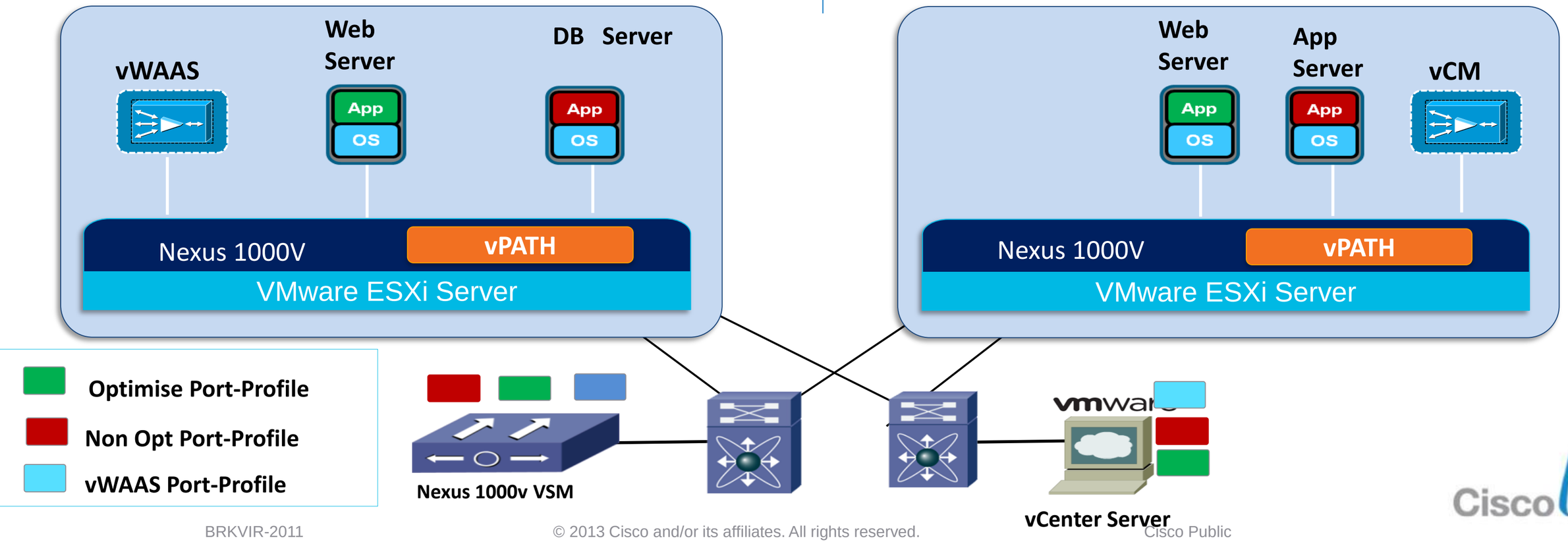
vWAAS – Policy Based configuration in N1000V

Feature

1. Optimisation based on the port-profile policy configured in Nexus 1000V
2. Policy gets propagated to vCenter automatically

Benefit

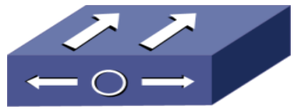
1. Provide on-demand service orchestration in the cloud without network disruption



vWAAS – Application Based Interception

Port-Profile ⟷ Port-group

Network Admin view



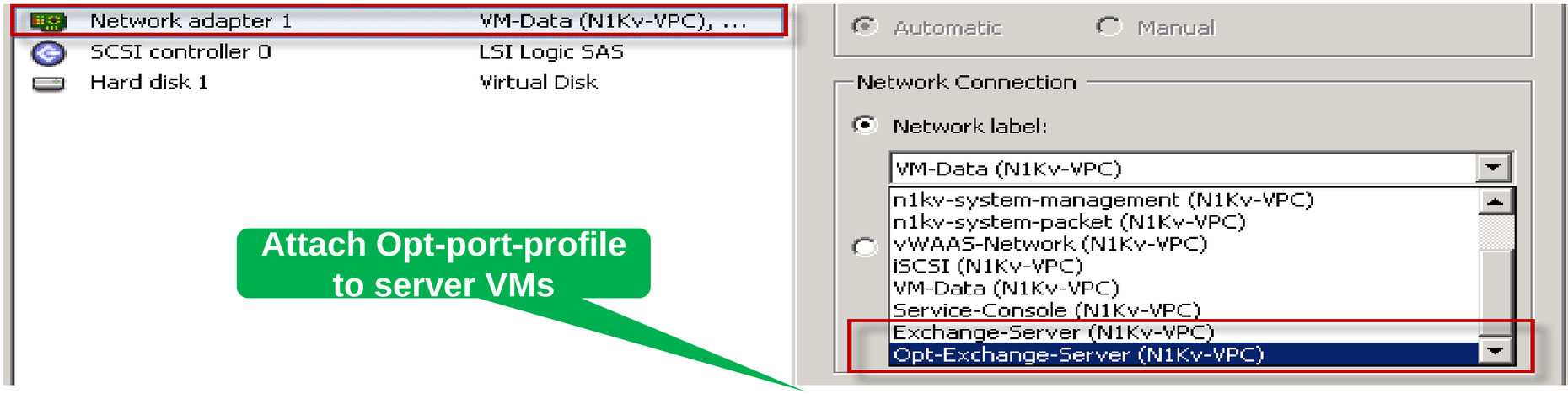
Nexus 1000v VSM

```
port-profile type vethernet Opt-Exchange-Server
  vmware port-group
  switchport mode access
  switchport access vlan 3185
  vn-service ip-address 2.8.2.90 vlan 3002 mgmt-ip-address 2.8.2.90 fail open
  no shutdown
  state enabled
```

vPATH interception

Server Admin view

vSphere client



Attach Opt-port-profile to server VMs

vWAAS – VM Mobility Awareness

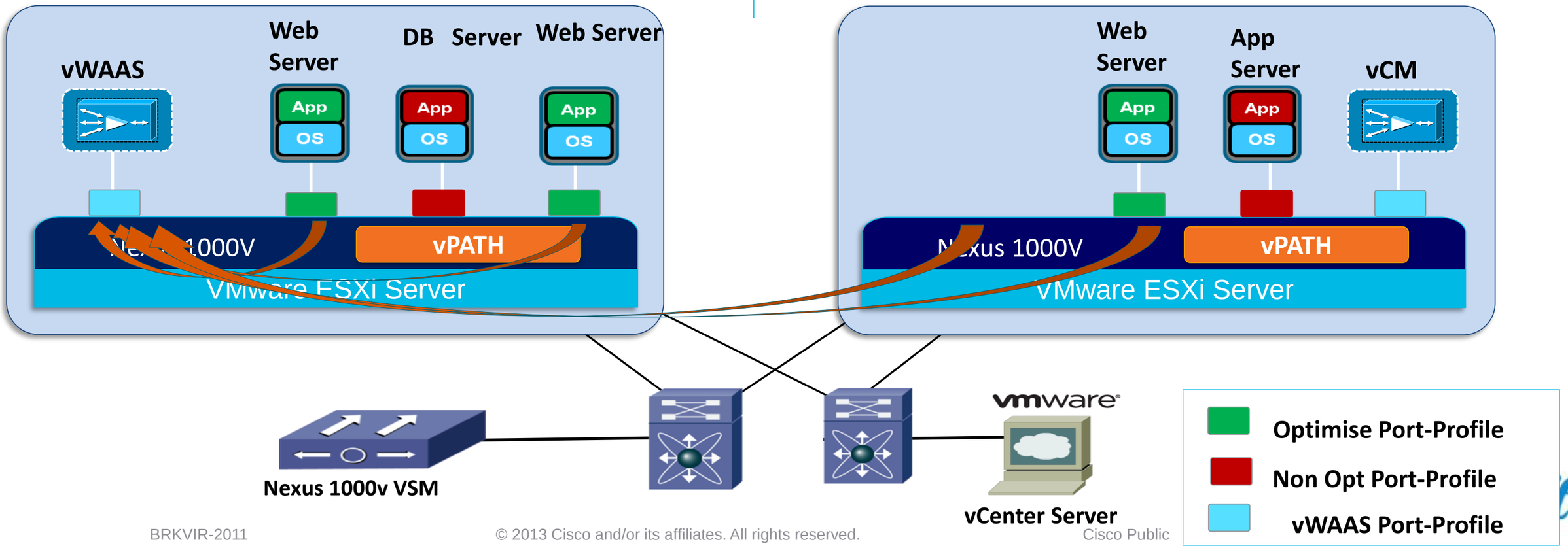
Feature

1. vPATH aware of movement of VM from one host to another.

2. Traffic interception continue to work as-is without any disruption or changes required.

Benefit

1. No disruption in WAN optimisation service if VM moves from one host to another.
2. Support VMware resources scheduling (DRS) and provides High availability



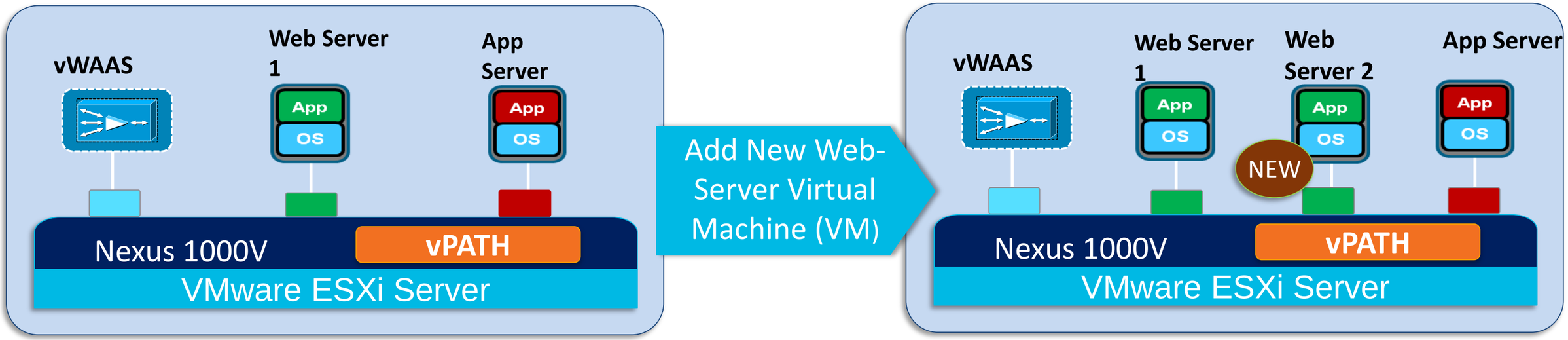
vWAAS – Architected for Elastic Workloads

Feature

1. Automatic application of vWAAS service when a new 'Web Server' VM gets provisioned
2. vWAAS services associated with 'Web server' VMs using Nexus 1000V policies.

Benefit

1. Elastic vWAAS deployment
2. Scale-out Virtual Web Server farm by provisioning additional VMs while applying WAN optimisation



vWAAS – Optimised Performance with vPath

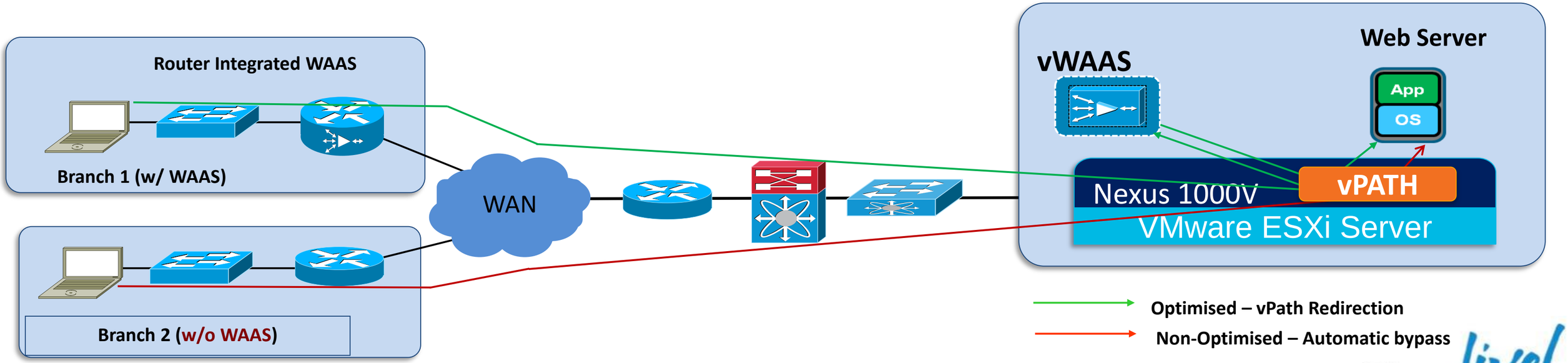
Feature

1. vWAAS send “offload” to vPATH for non-intresting traffic (inter-server traffic or no-peer traffic)

2. vPATH provide automatic bypass of these traffic

Benefit

1. High scale with automatic application or port-profile based traffic filtering

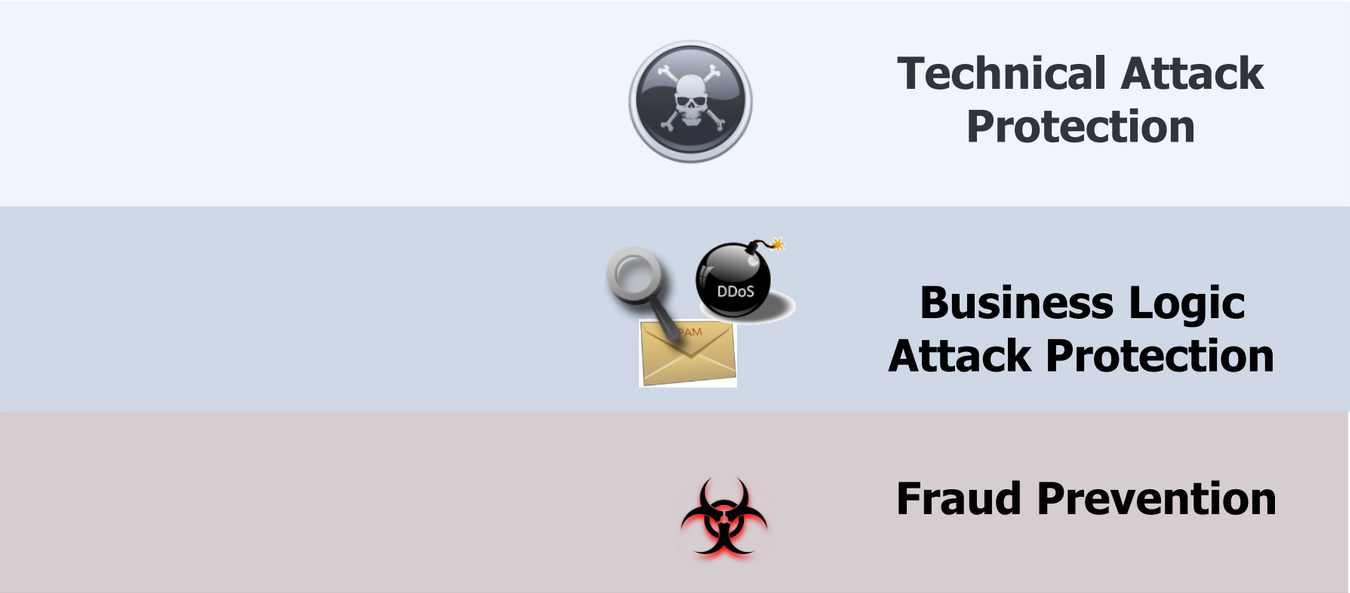


3rd Party Service on vPath

Imperva Web Application Firewall (WAF)

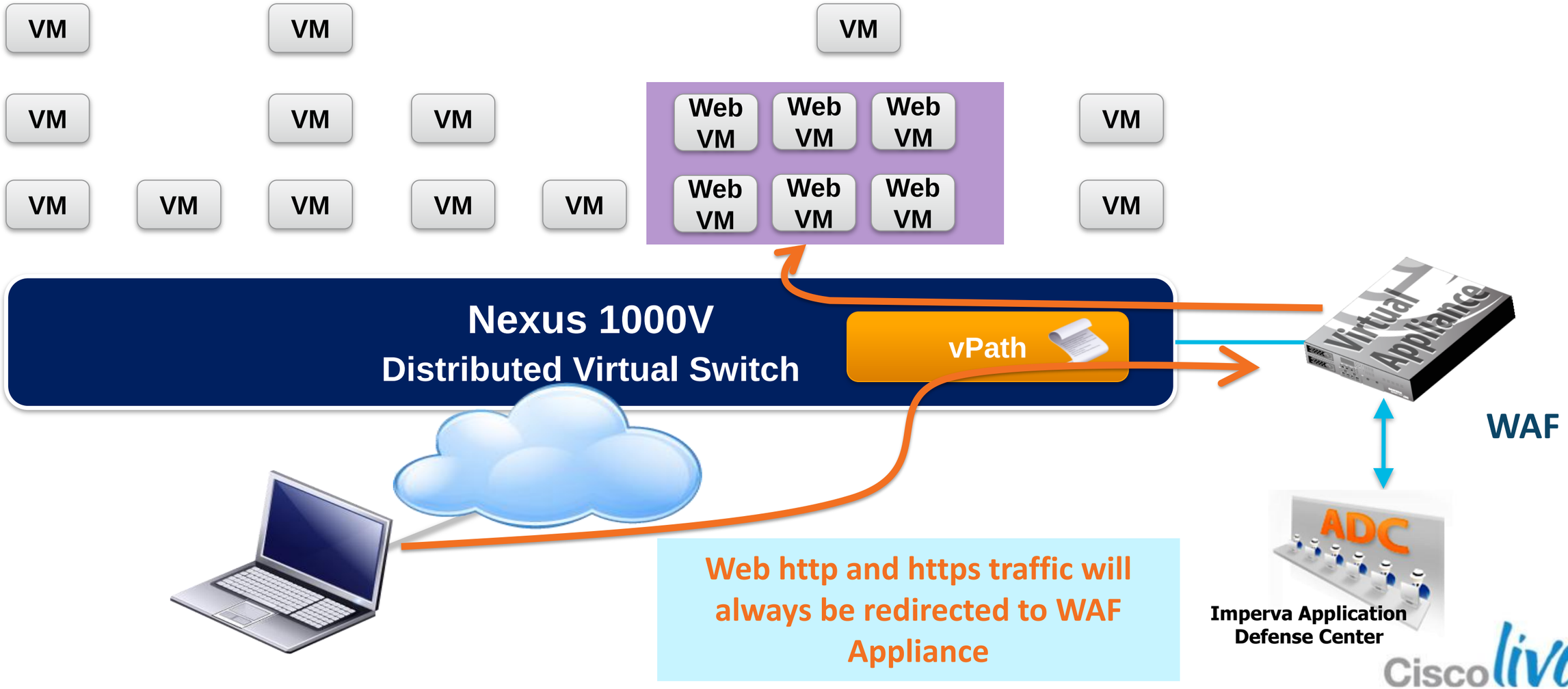
3rd Party Service leveraging vPath for Policy based Service Insertion

- **Imperva SecureSphere WAF** protects from Web-borne threats like SQL injection or fraud that can lead to a costly Website breach.
- Available as a virtual appliance and integrates with the Cisco Nexus 1000V Series vPath Architecture



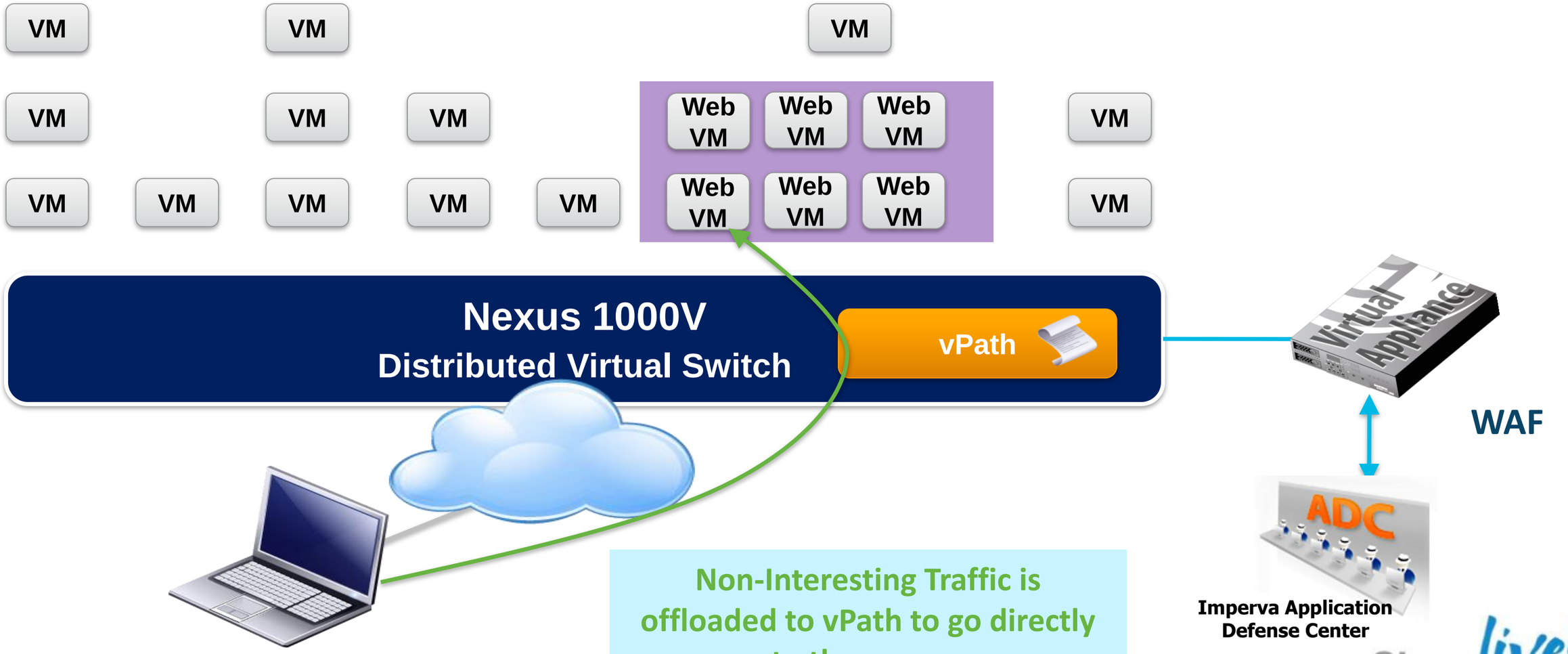
Virtual Security Gateway

Performance Acceleration with vPath



Virtual Security Gateway

Performance Acceleration with vPath

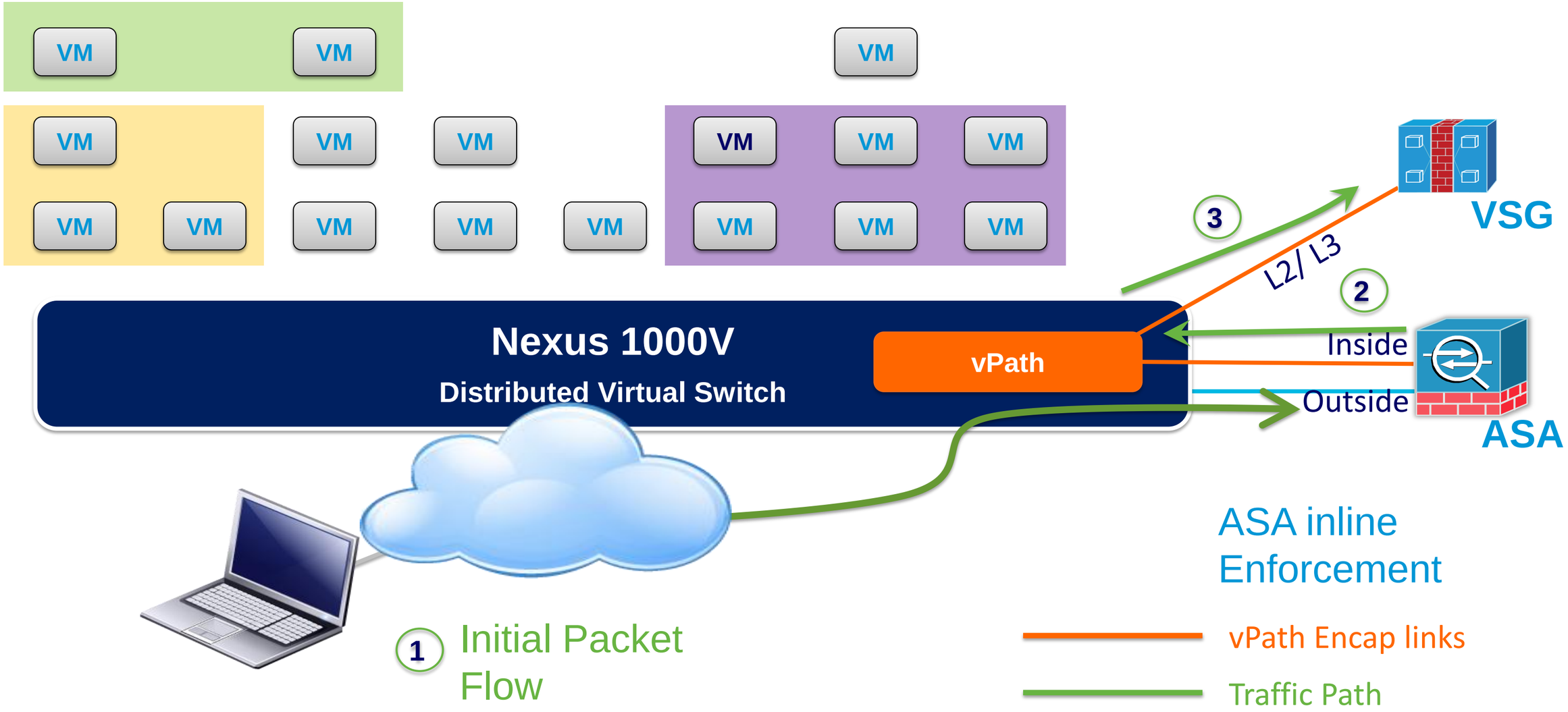


Non-Interesting Traffic is offloaded to vPath to go directly to the servers

vPath 2.0 Service Chaining

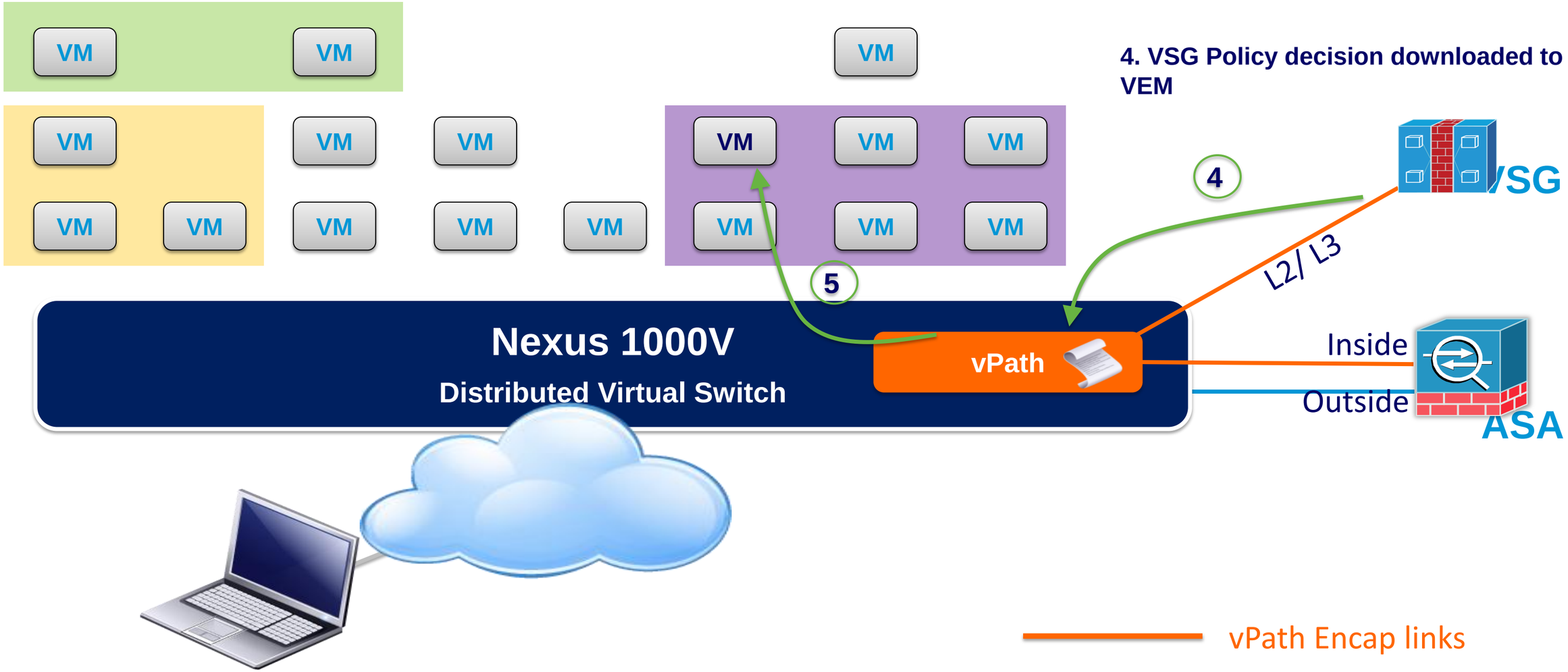
VSG and ASA Service Chainig Example 1:

Outside Client trying to access a VM protected by both VSG and ASA



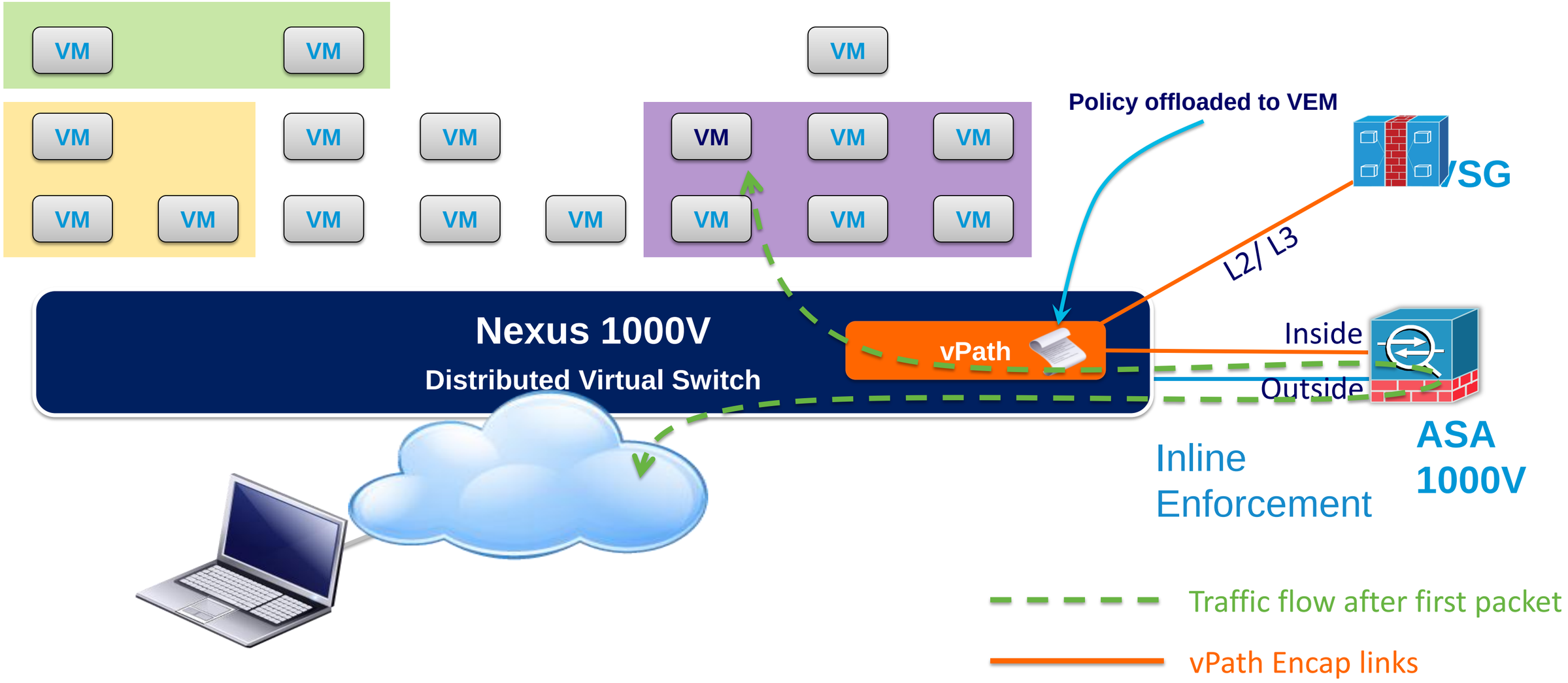
VSG and ASA Service Chaining Example 1:

Outside Client trying to access a VM protected by both VSG and ASA



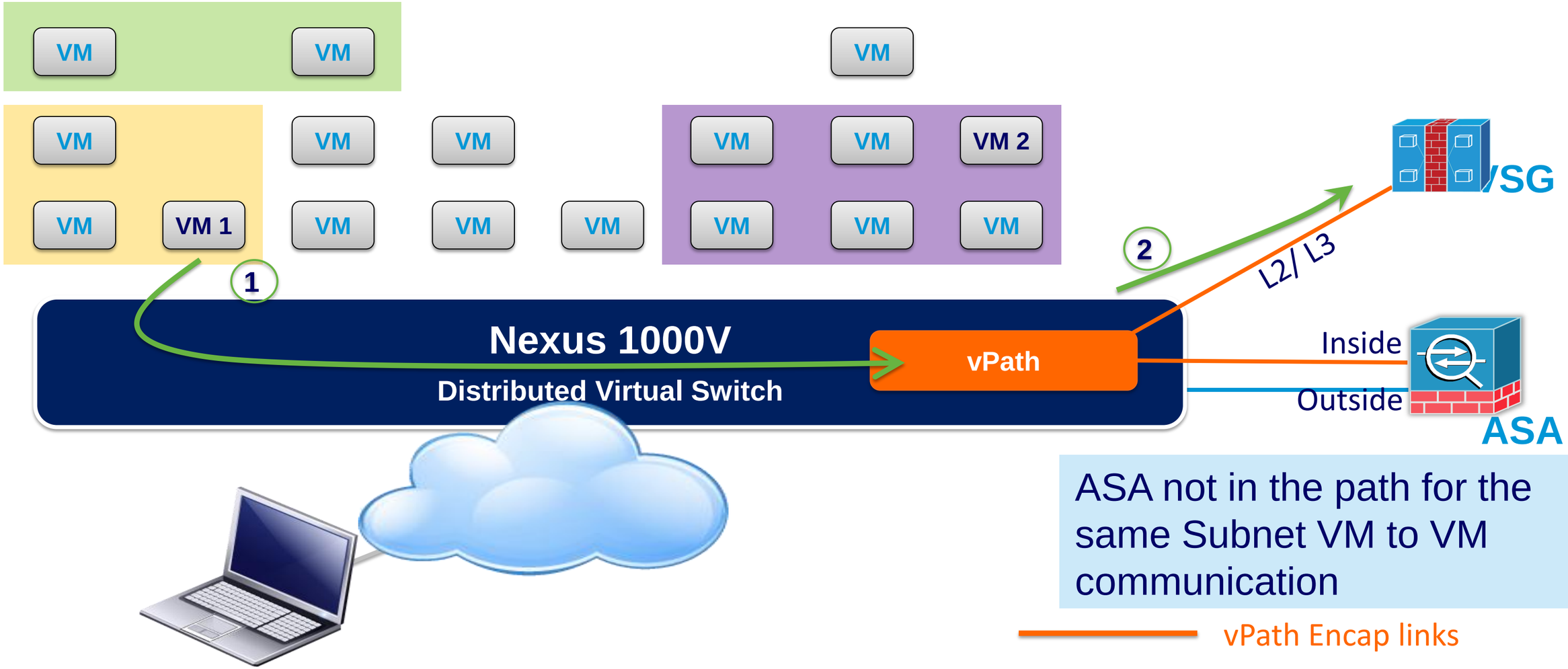
VSG and ASA Service Chaining Example 1:

Outside Client trying to access a VM protected by both VSG and ASA



VSG and ASA Service Chaining Example 2:

VM1 to VM2 communication on the same subnet

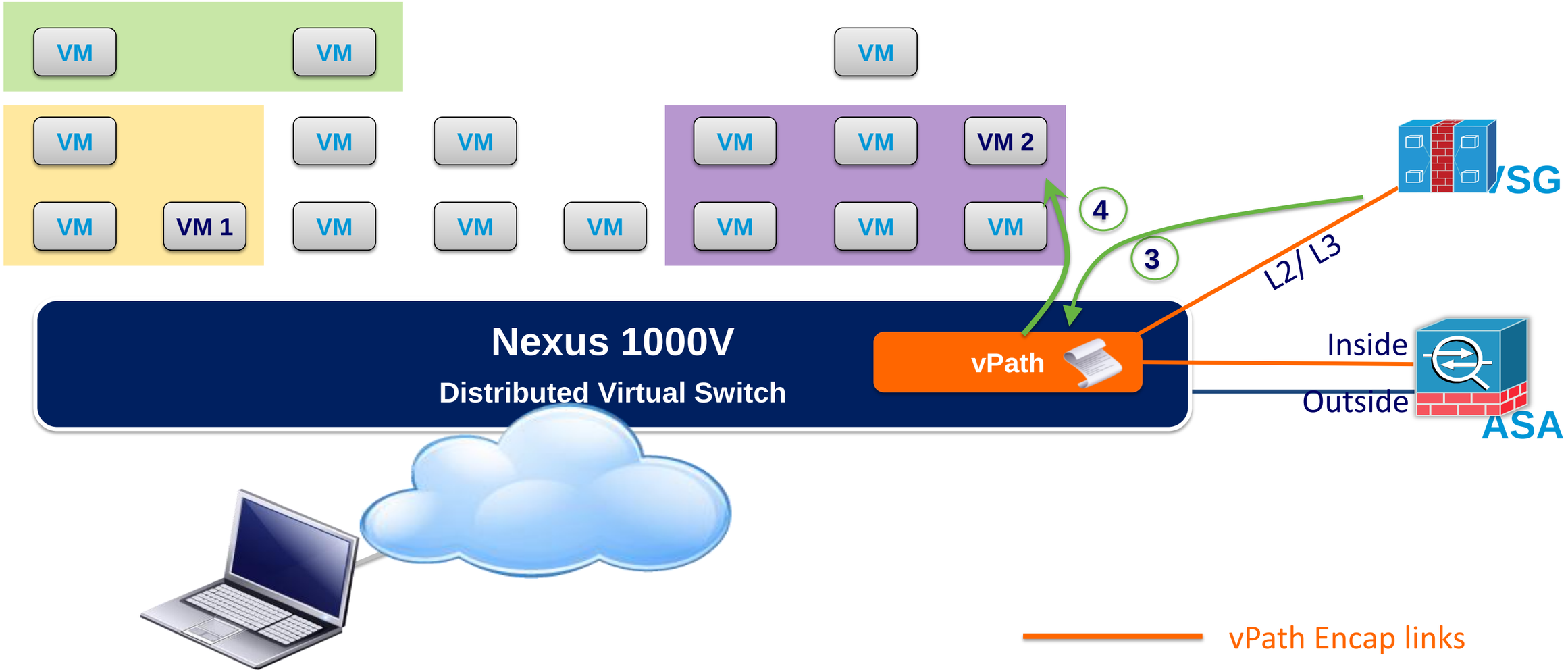


ASA not in the path for the same Subnet VM to VM communication

vPath Encap links

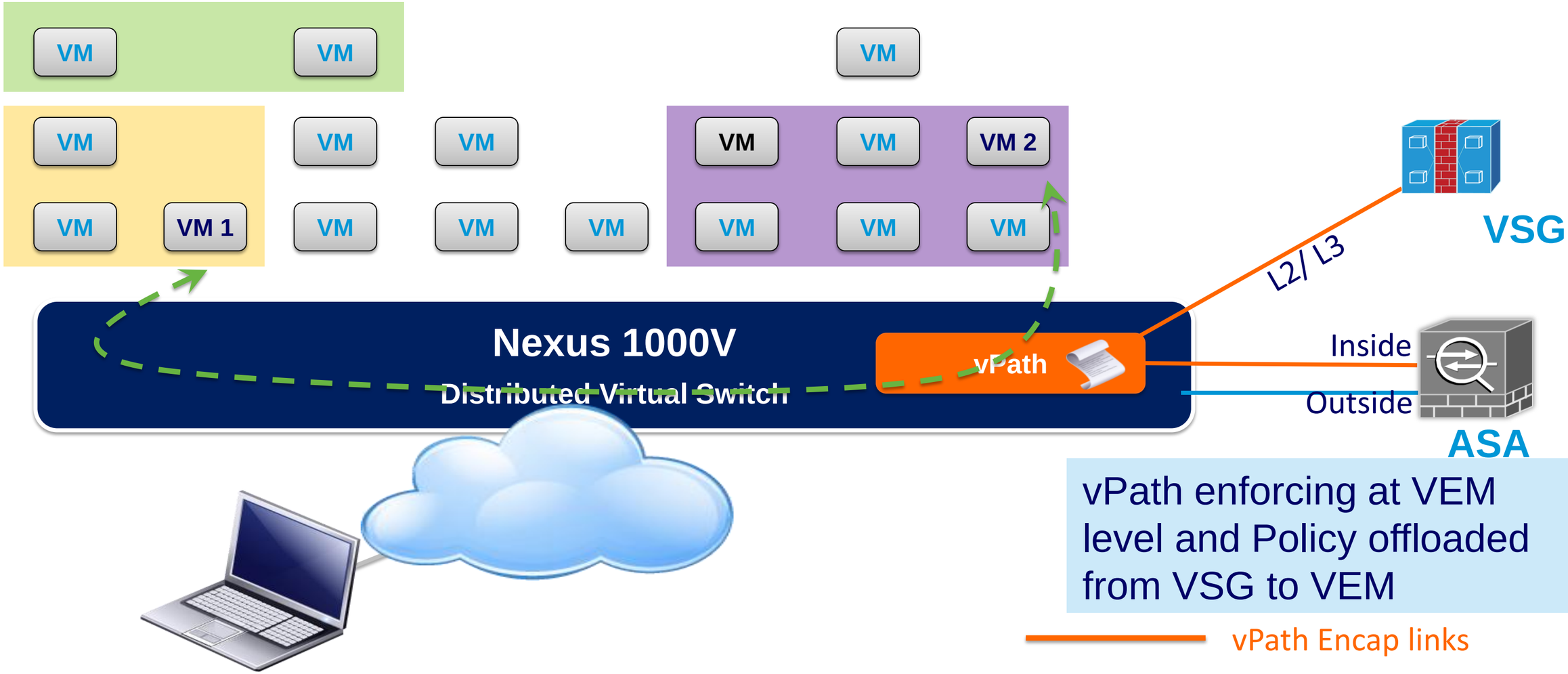
VSG and ASA Service Chaining Example 2:

VM1 to VM2 communication on the same subnet



VSG and ASA Service Chaining Example 2:

VM to VM communication on the same subnet



vPath enforcing at VEM level and Policy offloaded from VSG to VEM

vPath Encap links

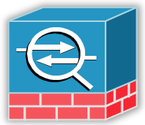
Service Channing Example

Chain VSG and ASA 1000V for a tenant

- vservice node ASA1 type asa

  ip address 172.31.2.11

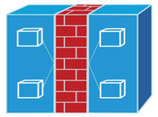
  adjacency l2 vlan 3770



- vservice node VSG1 type vsg

  ip address 10.10.11.202

  adjacency l3



Defining the Service Node on Nexus 1000V

- vservice path chain-VSG-ASA

  node VSG1 profile sp-web order 10

  node ASA1 profile sp-edge order 20

Chain the Service Nodes
Order is inside to outside

- port-profile type vethernet Tenant-1

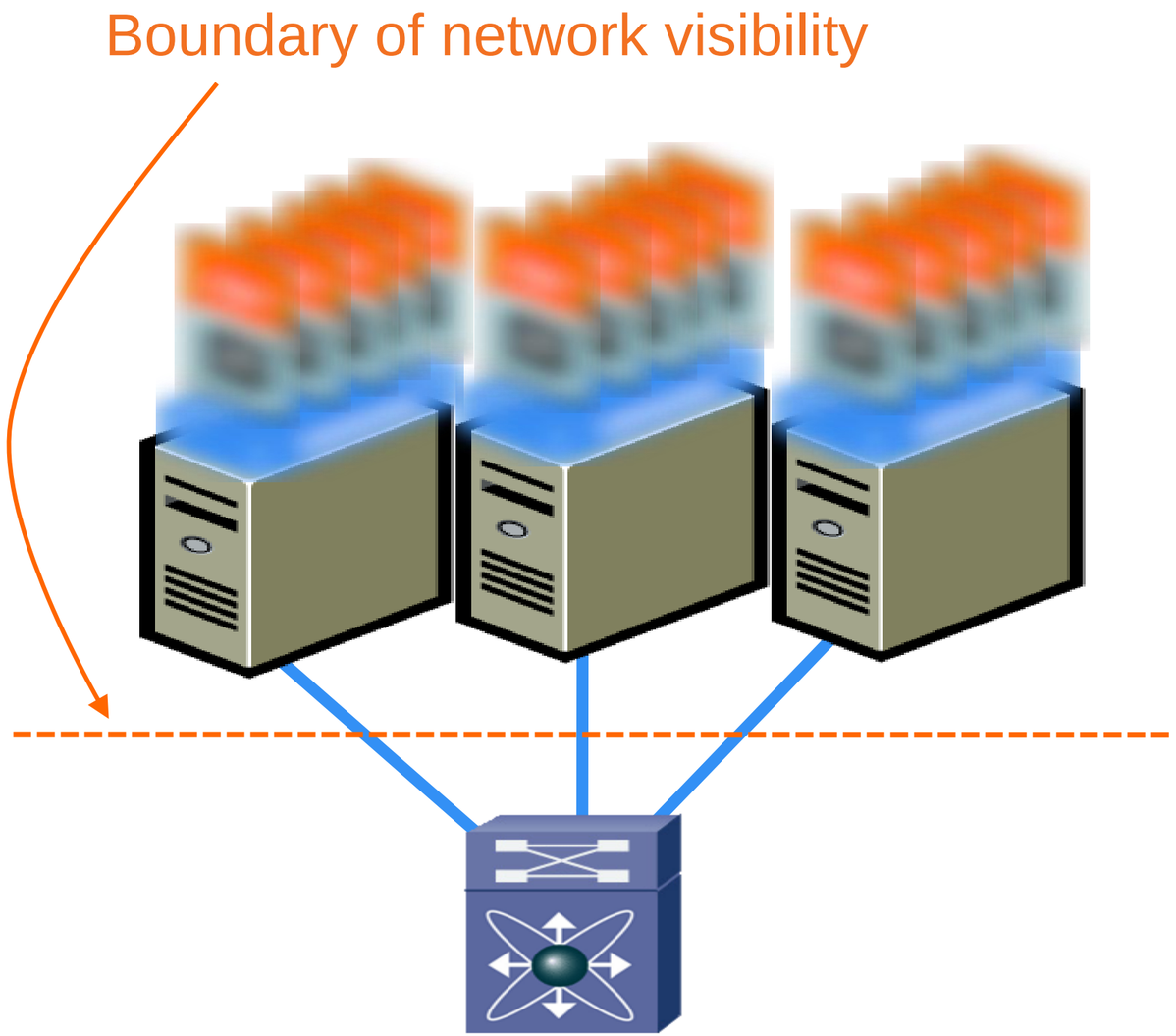
  org root/Tenant-1

  vservice path chain-VSG-ASA

Enable the Service Chain
Per Port-Profile

Cisco Prime NAM for Nexus 1010

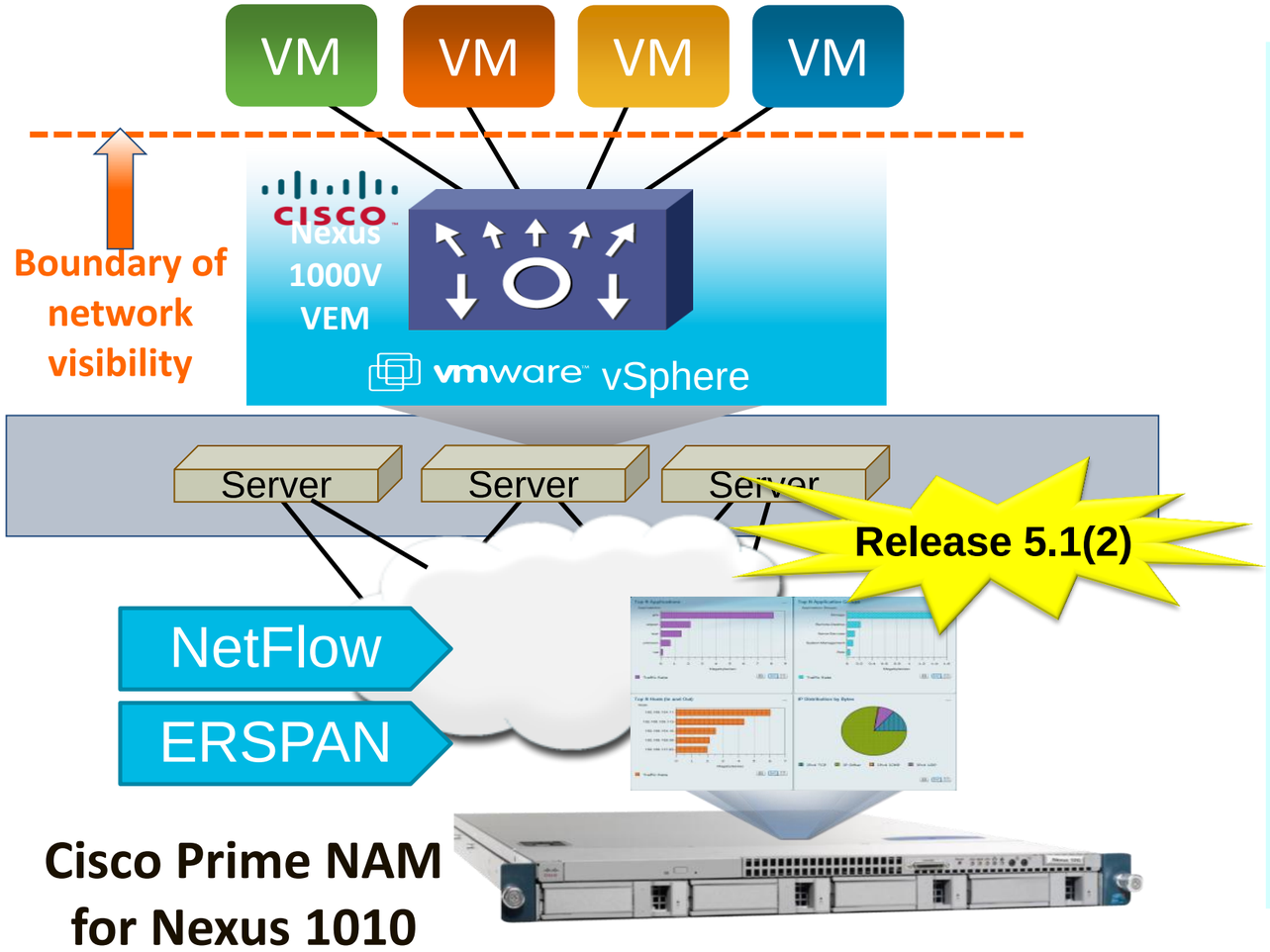
The Challenge: Server Virtualisation Creates a Demand for VM-level Visibility



- Lack of visibility into network behaviour at the VM level
- Lack of visibility into cross-VM interactions
- Need for operational consistency and continuity across physical and virtual network

Cisco Prime NAM for Nexus 1110

Extends Visibility into Virtual Machine (VM) Network



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

Enable NAM as a Network Service on N1KV

- **Netflow Configuration**

```
flow exporter exporter1
  destination 172.23.180.38
  transport udp 3000
  source mgmt0
  dscp 63
  version 9
…..
```

- **ERSPAN Configuration**

```
monitor session 1 type erspan-source
  source vlan 16,173 both
  destination ip 172.23.180.38
  erspan-id 100
  mtu 1500
  header-type 3
```

For Your Reference

NAM Receiver for Netflow and ERSPAN Traffic

Virtual Services & VM Mobility

- DC wide
- DC to DC

DC-wide VM Mobility – Multiple Options

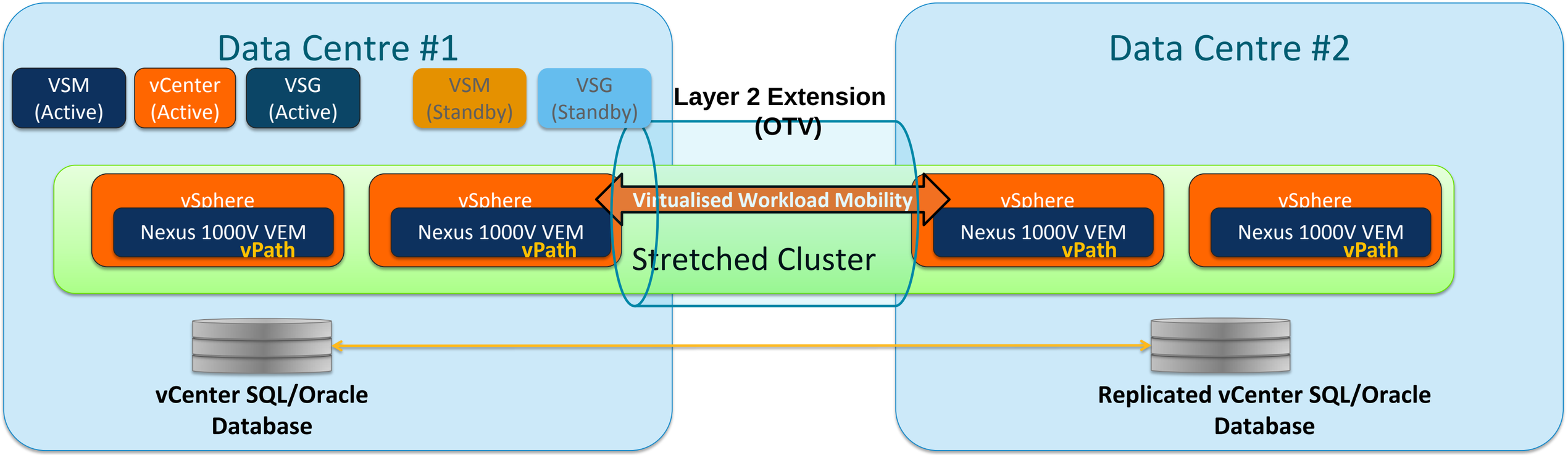
- Bigger UCS domain → broader mobility within UCS domain
- FabricPath/Trill → DC-wide VM mobility with N7K/N5K
- Nexus 1000V & VXLAN w/ OTV

This Session

VM Mobility across DCs

Maintain network & security policies during vMotion

Nexus 1000V VSM Pair & VSG Pair
(or VSG/VSG hosted on Nexus 1010s)



Migrate virtual workloads seamlessly across Data Centres
Maintain transparency to network & security policies (via N1KV & VSG)

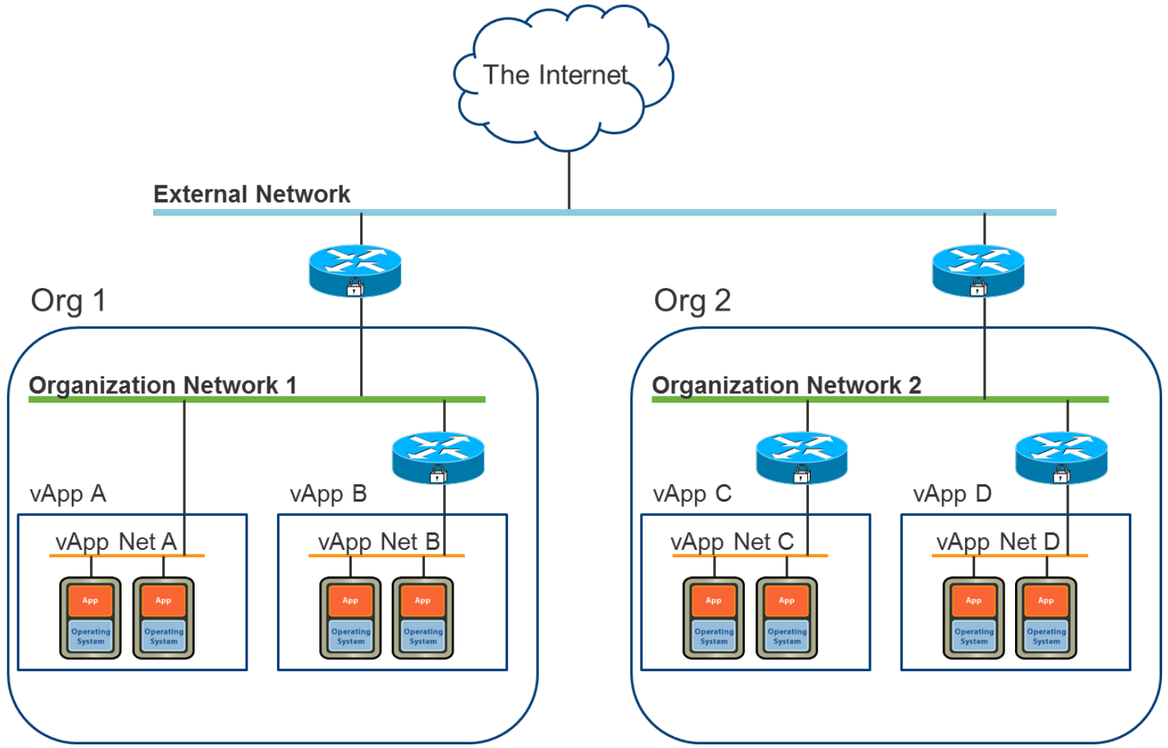
Deploying Services on VXLAN

Why VXLANs?

Pain points in scaling cloud networking

- Use of server virtualisation and cloud computing is stressing the network infrastructure in several ways:
  - Server Virtualisation increases demands on switch MAC address tables
  - Multi-tenancy and vApps driving the need for more than 4K VLANs
  - Static VLAN trunk provisioning doesn’t work well for Cloud Computing and VM mobility
  - Limited reach of VLANs using STP constrains use of compute resources

Multi-Tenancy and vApps Drive the Need for Many L2 Segments

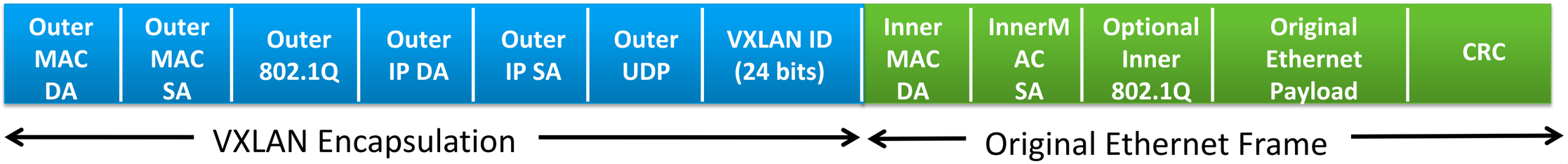


- Both MAC and IP addresses could overlap between two tenants, or even within the same tenant in different vApps.
  - Each overlapping address space needs a separate segment
- VLANs use 12 bit IDs = 4K
- VXLANs use 24 bit IDs = 16M

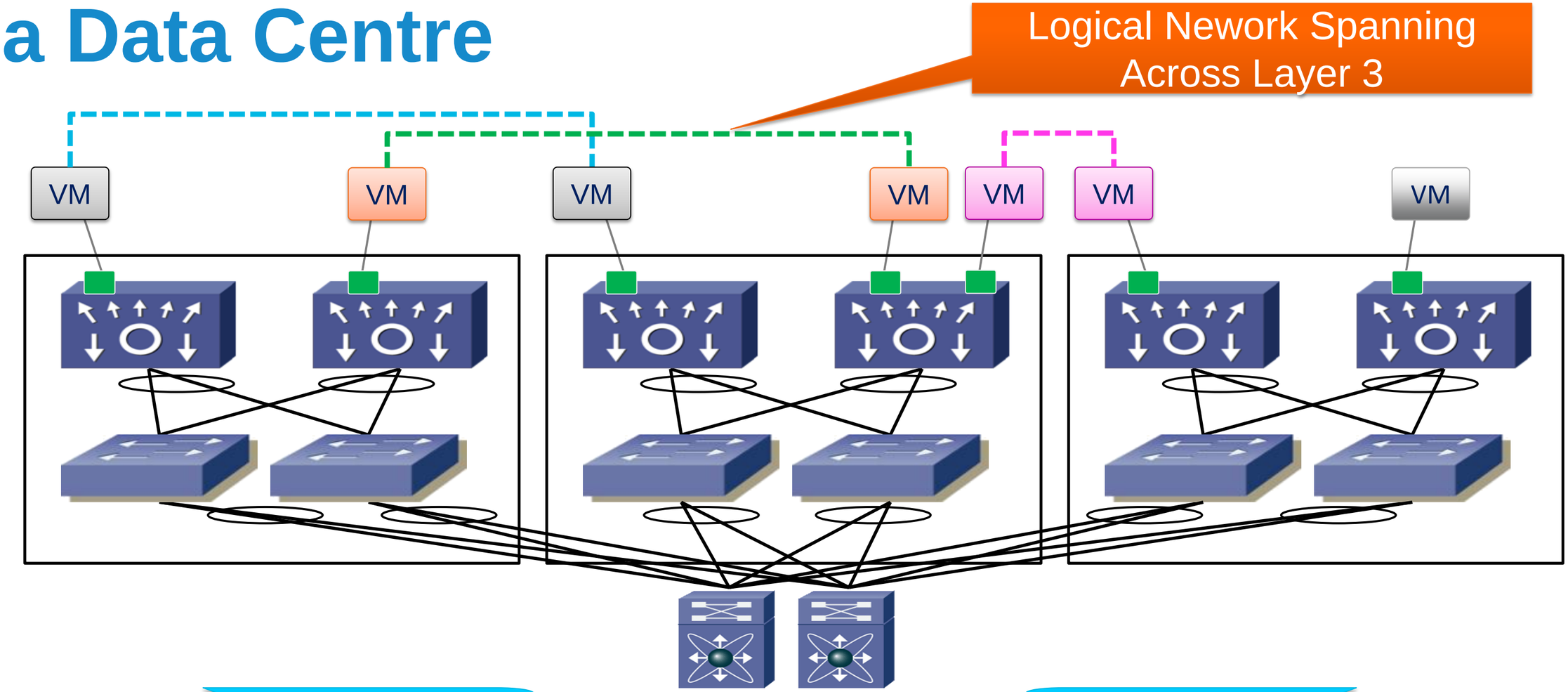
Virtual Extensible Local Area Network (VXLAN)

Supported in Nexus 1000V Release 1.5

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



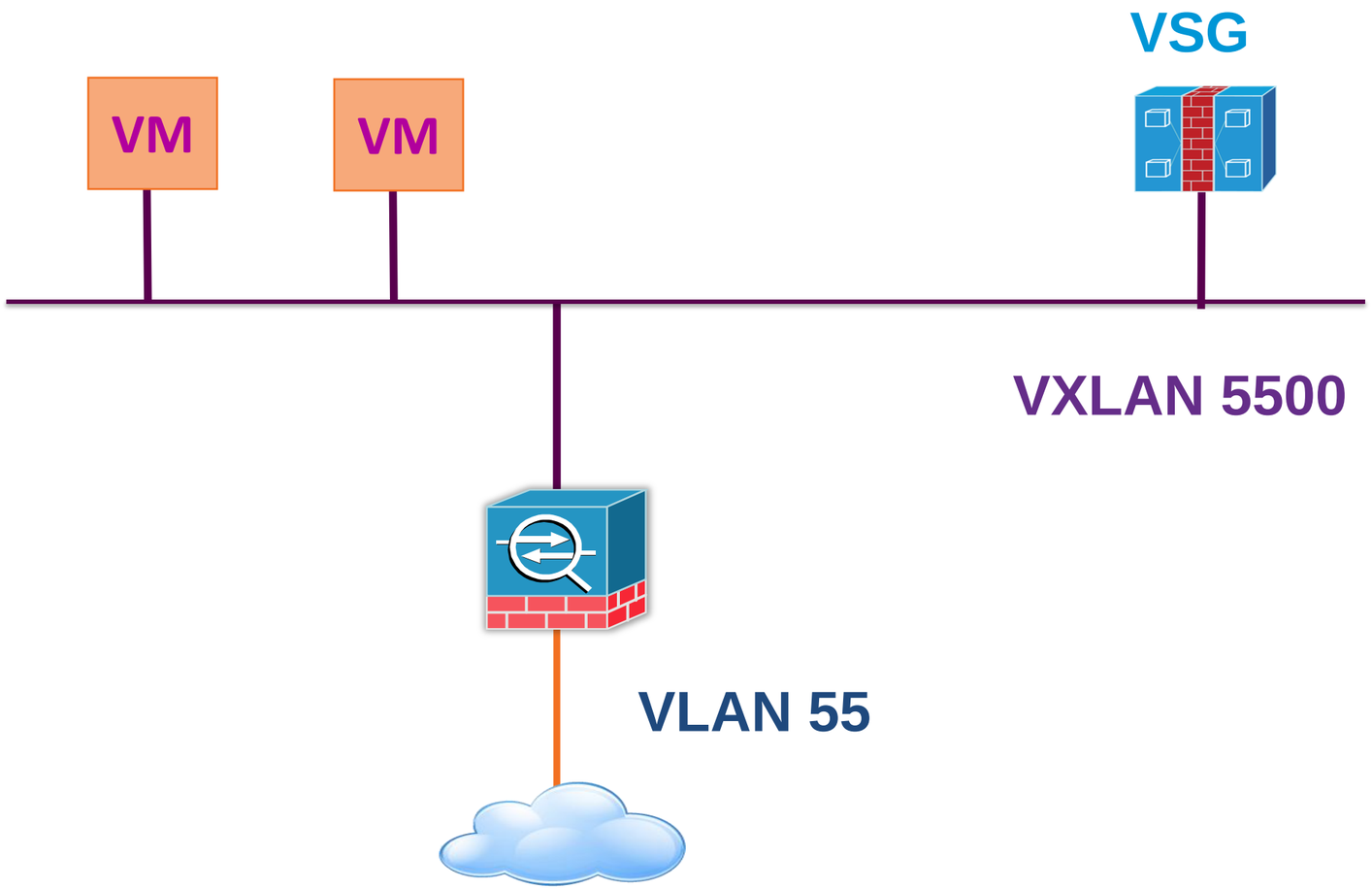
Scalable Pod Deployment with VXLAN within a Data Centre



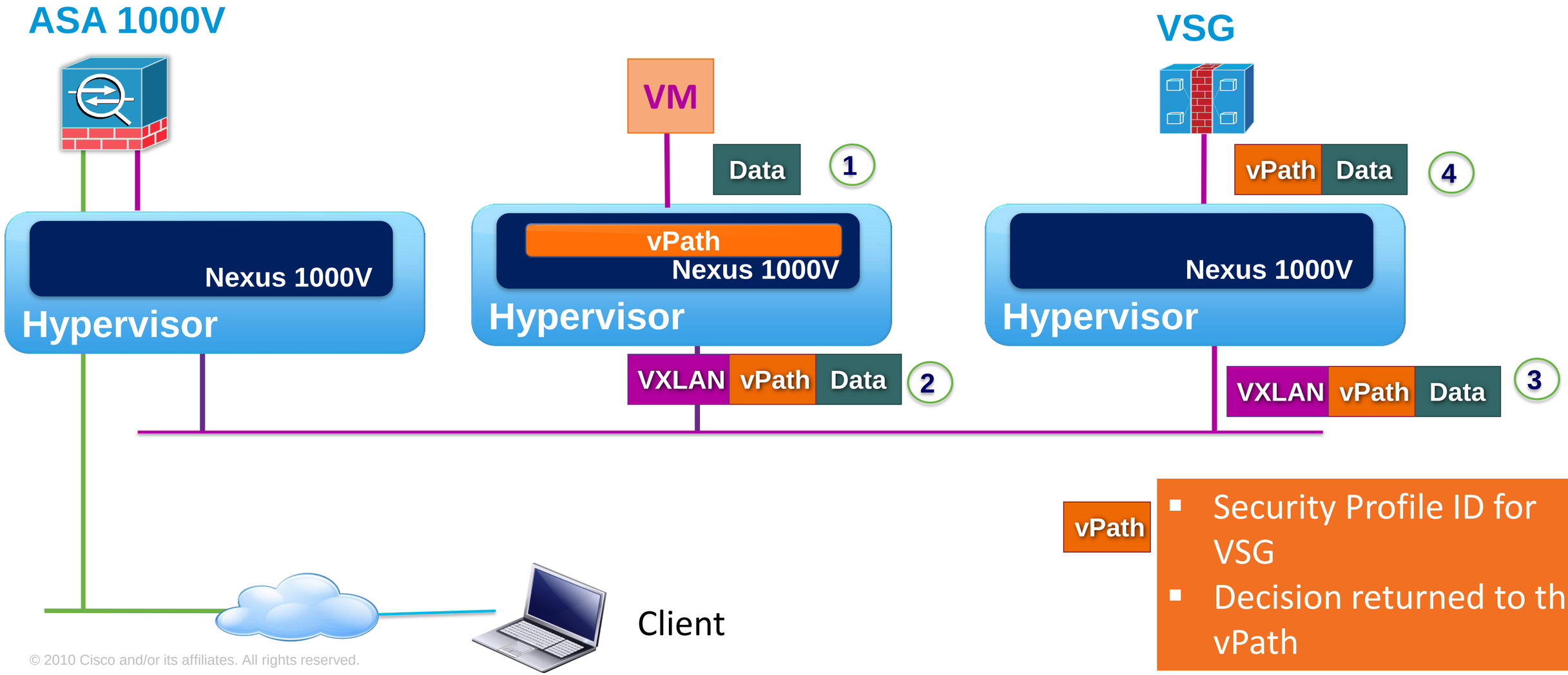
Add More Pods to Scale

Logical Topology with VSG and ASA 1000V

VSG and workload and inside interface of ASA 1000V on the same L2 segment (VXLAN 5500)



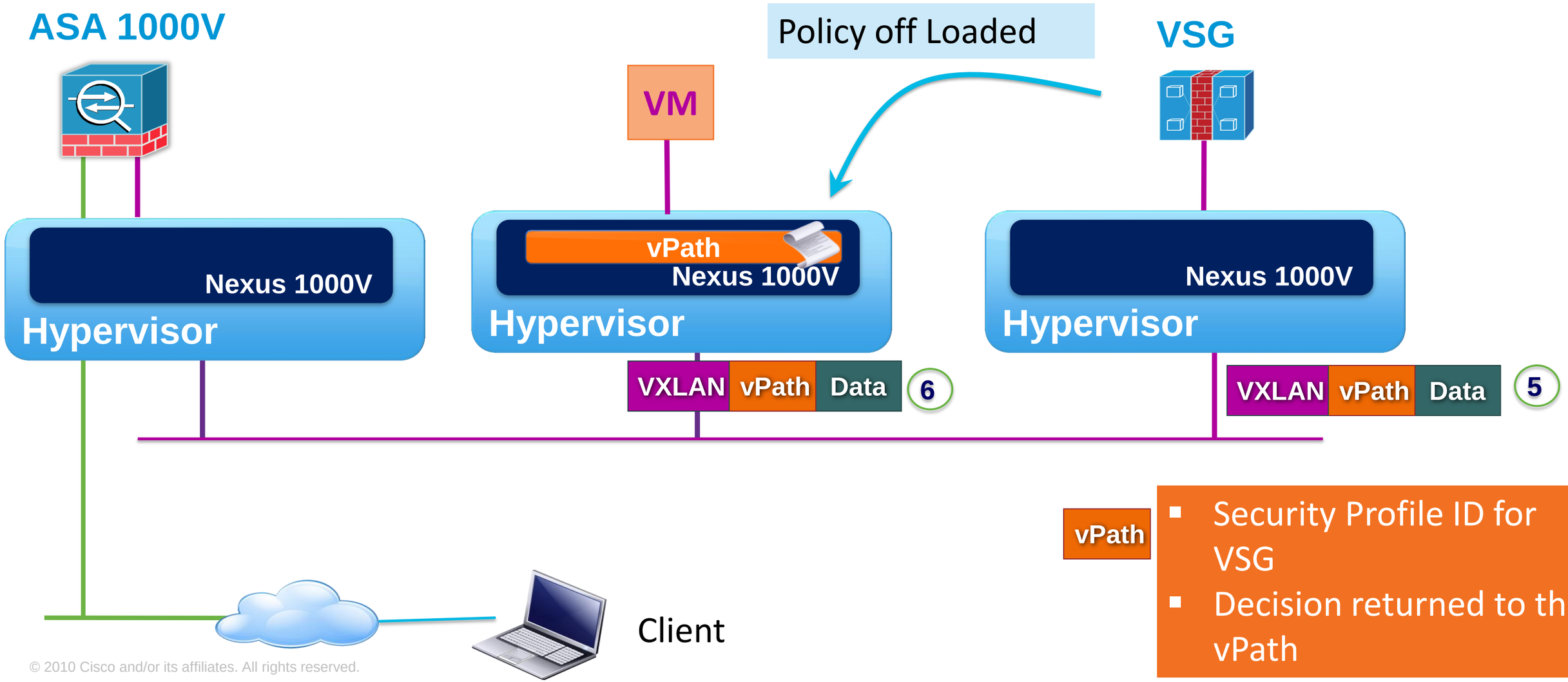
ASA 1000V and VSG Service Chaining on VXLAN



vPath

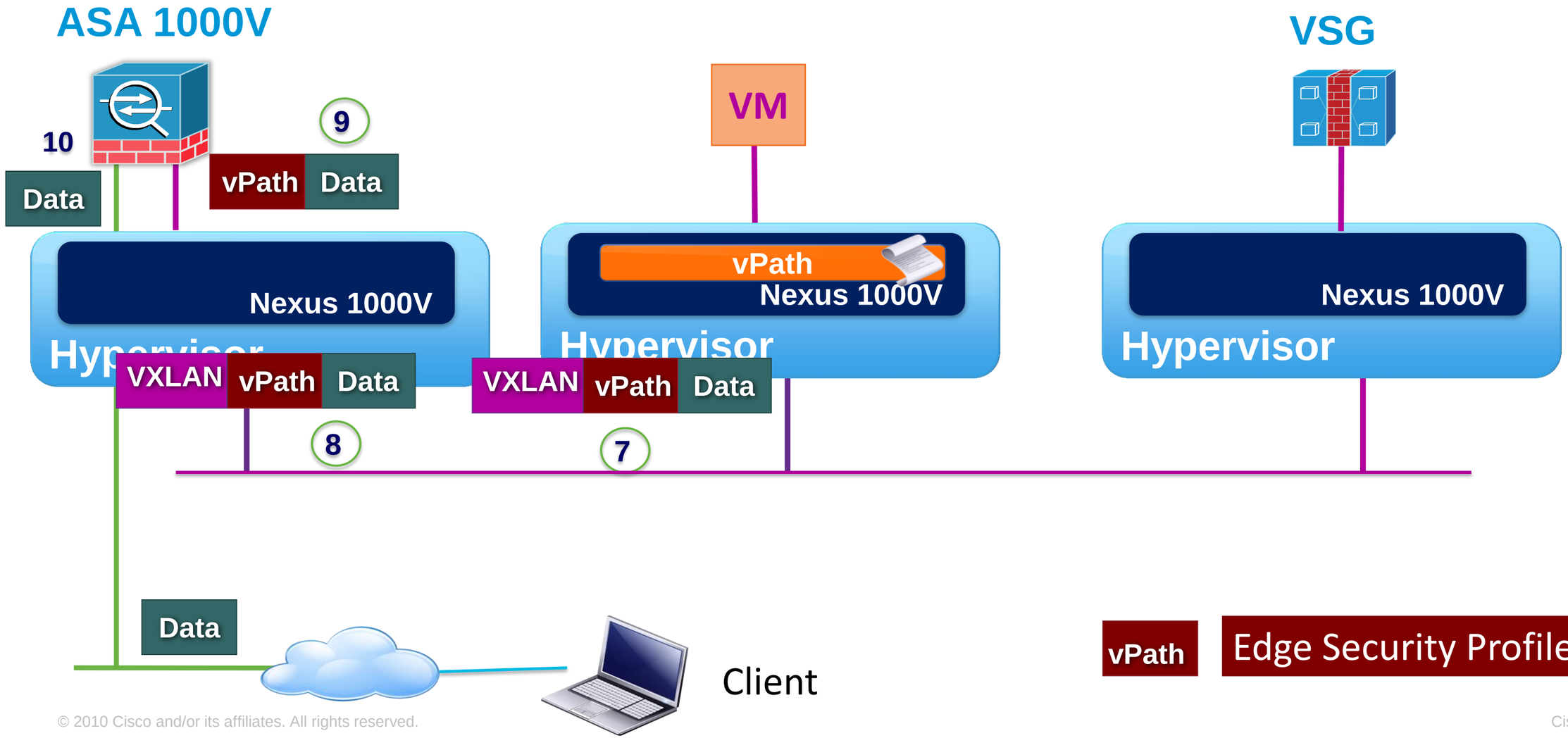
- Security Profile ID for VSG
- Decision returned to the vPath

ASA 1000V and VSG Service Chaining on VXLAN



- Security Profile ID for VSG
- Decision returned to the vPath

ASA 1000V and VSG Service Chaining on VXLAN



vPath Edge Security Profile ID for ASA

Configuration Example

Applying Service on both VLAN and VXLAN backed Port-Profiles

For Your Reference

```
vlan 10

! Port-Profile VLAN Backed
port-profile type vethernet TenantA
switchport access vlan 10

org root/abc
vn-service ip-address 10.10.10.137 vlan 20 security-profile secure-abc
no shutdown
state enabled
```

```
bridge-domain vxlan_5005
  segment id 5005
  group 225.1.1.5

! Port-Profile VXLAN Backed
port-profile type vethernet TenantA
switchport access bridge-domain vxlan_5005
org root/abc
vn-service ip-address 10.10.10.137 vlan 20 security-profile secure-abc
no shutdown
state enabled
```

Bridge Domain

Summary

- Nexus 1000V vPath makes the Virtual Service Possible
- VSG and ASA 1000V are different firewalls but they compliment each other
- Services can be enabled on a per tenant basis
- vPath is designed to scale out for Multi-tenant Environment
- Services can be deployed on VXLANs as well as VLANs

Related Sessions

For Your Reference

Other N1KV Related Session which you may be interested to attend

- BRKVIR-2011 Deploying Services in a Virtualised Environment
- BRKVIR-2014 Architecting Scalable Clouds using VXLAN and Nexus 1000V
- BRKVIR-2017 The Nexus 1000V on Microsoft Hyper-V: Expanding the Virtual Edge
- BRKVIR-3013 Deploying and Troubleshooting the Nexus 1000v virtual switch

Wrap-Up

- Solutions
- Webcasts
- Resources
- CloudLab (on-line remote lab)
- Related Sessions & Cisco Live hands-on labs
- Session Evaluation

Reference Solutions

Solution	Nexus 1000V	Nexus 1010	Virtual Security Gateway	Virtual WAAS	NAM (N1010)
Vblock	✓		✓	✓	
FlexPOD	✓	✓			
Virtual Desktop	✓	Implicit Support	✓	✓*	Implicit Support
Virtual Multi-tenant DC (VMDC)	✓	Implicit support	✓		Implicit support
DC-to-DC vMotion	✓	Implicit support	✓	✓	Implicit support
PCI 2.0	✓	Implicit support	✓		Implicit support
Hosted Collaboration	✓	Implicit support			Implicit support

*Based on default Citrix configuration

Reference Solutions

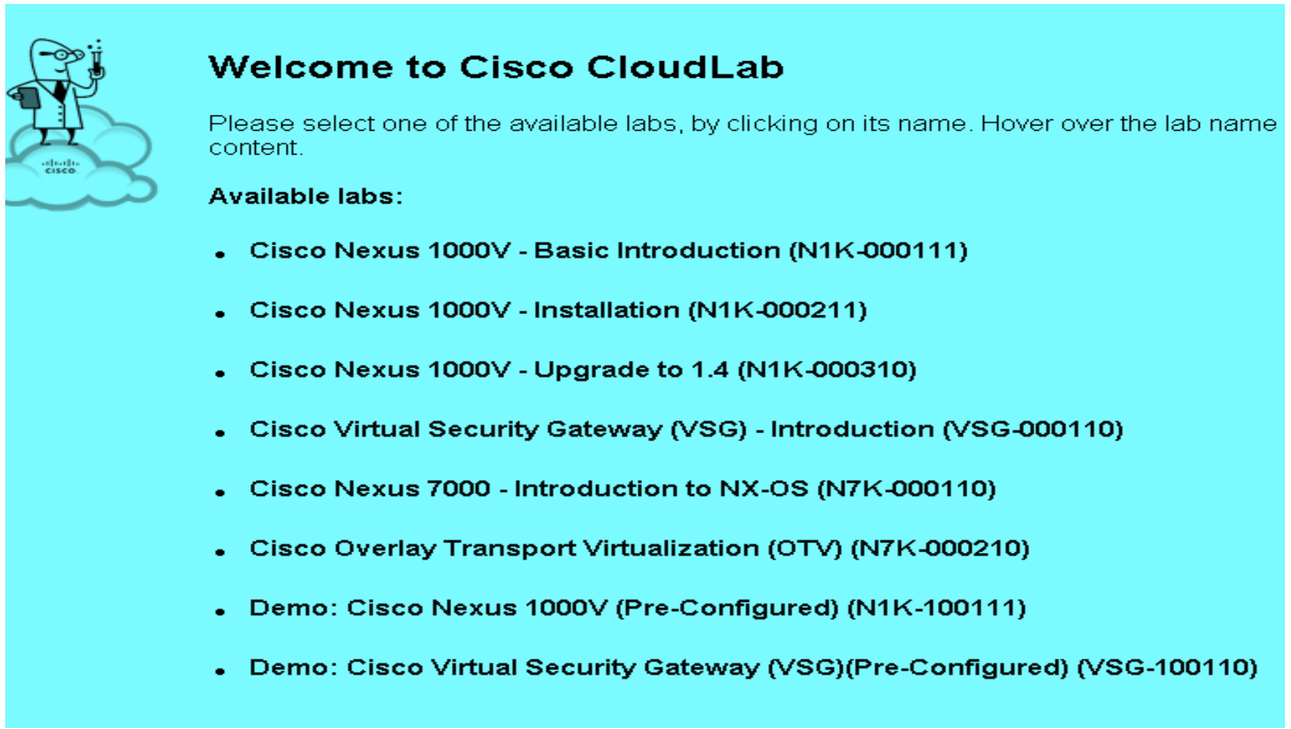
For Your Reference

- Vblock with Nexus 1000V; Vblock with VSG and vWAAS
- FlexPOD with Nexus 1000V and Nexus 1010
- Virtual Multi-tenant Data Centre with Nexus 1000V and VSG
- Virtual Desktop
  - 1000V and VMware View
  - 1000V and Citrix XenDesktop
  - 1000V and VSG in VXI Reference Architecture
- Virtual Workload Mobility (aka Long-distance vMotion)
  - Cisco, VMware and EMC (with 1000V and VSG)
  - Cisco, VMware and NetApp (with 1000V and VSG)
- PCI 2.0 with Nexus 1000V and VSG

Cisco Cloud Lab Hands On Training & Demos

For Your Reference

- Hands on labs available for Nexus 1000V and VSG in Cloud Lab https://cloudlab.cisco.com
- Open to all Cisco employees
- Customers/Partners require sponsorship from account team for access via CCO LoginID



Resources

For Your Reference

- CCO Links
  - 1000V: www.cisco.com/go/1000v
  - 1010: www.cisco.com/go/1010
  - VSG: www.cisco.com/go/vsg
  - VNMC: www.cisco.com/go/vnmc
  - vWAAS: www.cisco.com/go/waas
- Deployment Guides
  - Nexus 1000V Deployment Guide
  - Nexus 1000V on UCS – Best Practices
  - Nexus 1010 Deployment Guide
  - VSG Deployment Guide
- White papers:
  - Nexus 1000V and vCloud Director
  - N1K on UCS Best Practices
  - Nexus 1000V QoS White paper (draft)
  - VSG and vCloud Director (draft)
  - vWAAS Technical Overview
  - vWAAS for Cloud-ready WAN Optimization
- Nexus 1000V Community

Additional Links

For Your Reference

- N1K Download and 60-day Eval: www.cisco.com/go/1000vdownload
- N1K Product Page: www.cisco.com/go/1000v
- N1K Community: www.cisco.com/go/1000vcommunity
- N1K Twitter www.twitter.com/official_1000V
- N1K Webinars: www.tinyurl.com/1000v-webinar
- N1K Case Studies: www.tinyurl.com/n1k-casestudy
- N1K Whitepapers www.tinyurl.com/n1k-whitepaper
- N1K Deployment Guide: www.tinyurl.com/N1k-Deploy-Guide
- VXI Reference Implementation: www.tinyurl.com/vxiconfigguide
- N1K on UCS Best Practices: www.tinyurl.com/N1k-On-UCS-Deploy-Guide

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm

Cisco live! 365

Don't forget to activate your Cisco Live 365 account for access to all session material, communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.
www.ciscoliveaustralia.com/portal/login.ww