



Deploying Services in a Virtualized Environment

BRKVIR-2011

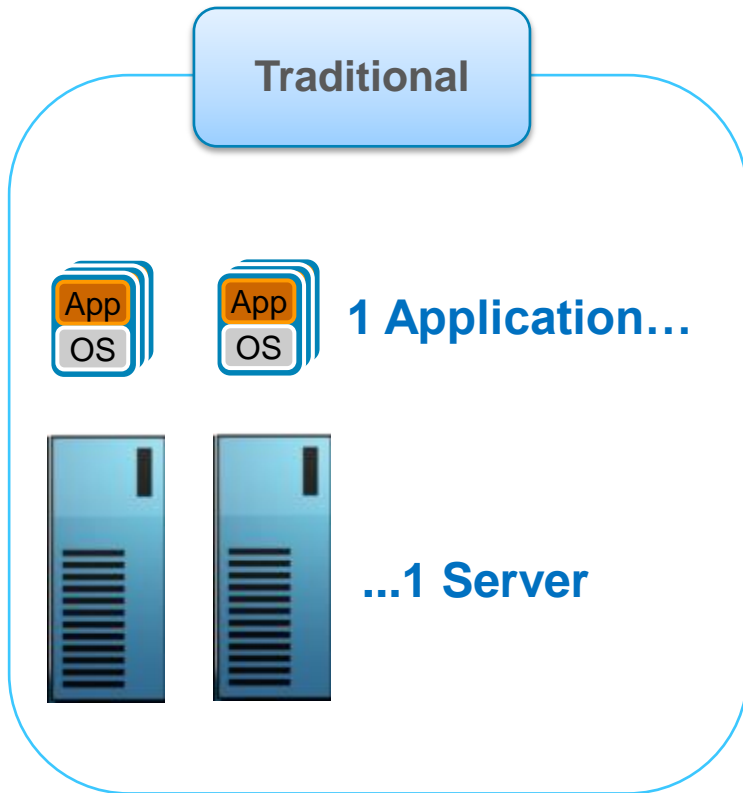


Agenda

- Overview
- Virtualization/Cloud Trends
- Requirements for Virtualized Services
- Nexus 1000V for Virtualized Services
- Virtualized Services
 - Virtual Security Gateway (VSG)
 - Virtual WAAS (vWAAS)

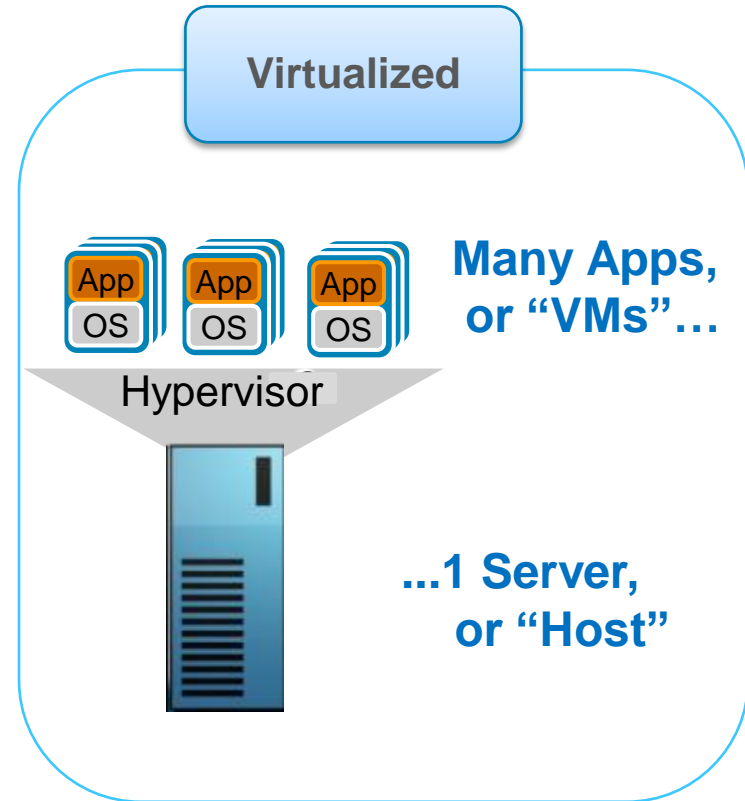
Present Day Virtualization

Virtualizing Consolidated Data Centers



Traditional Model:

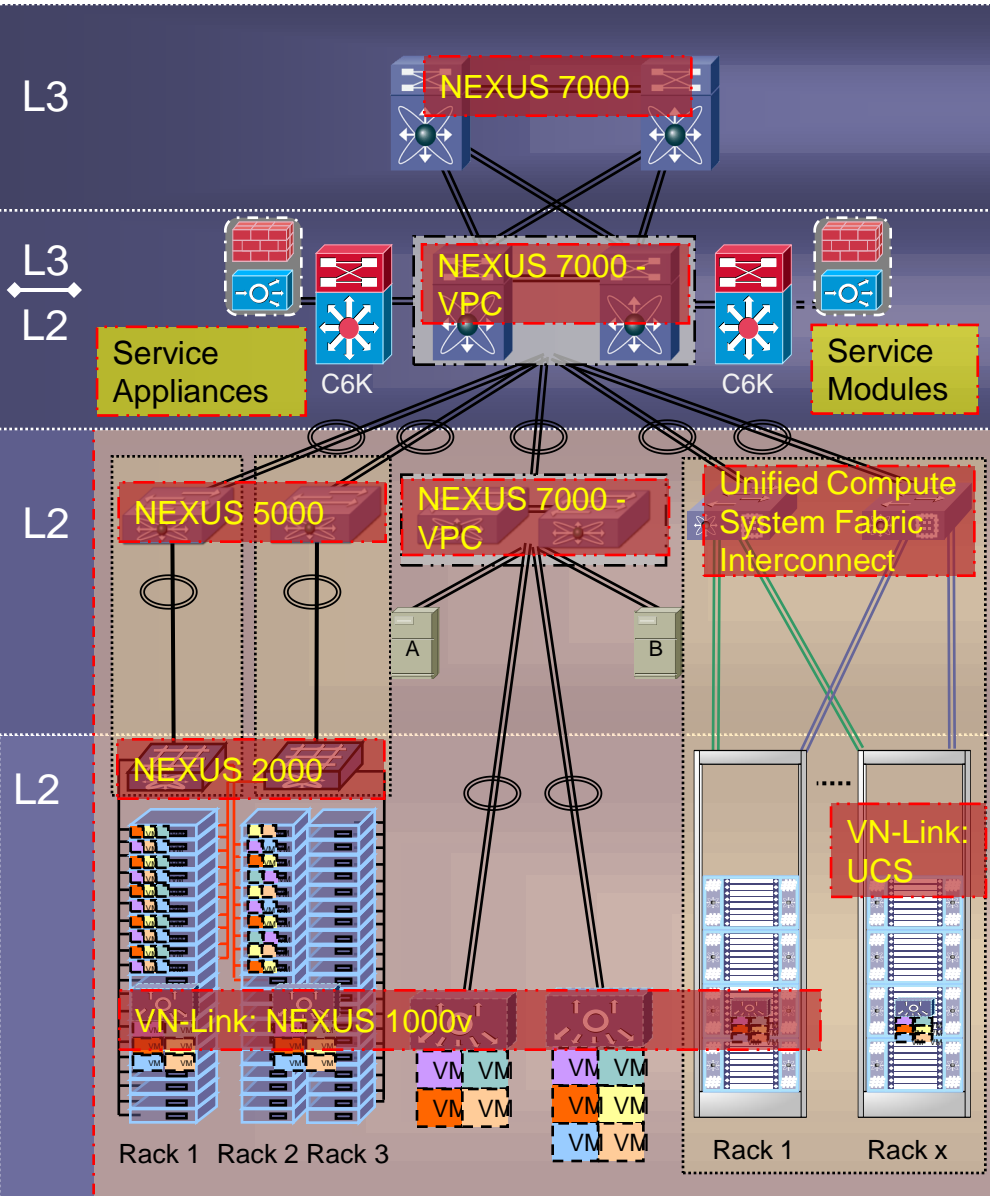
- Low CPU Utilization
- Heating/Cooling Challenges



Virtualized Model:

- Agile, Policy Driven, Multi-Tenant
- Forecasted to be 50% of all workloads in 2012
- Environment demands 10GbE and a new architectural framework

The Unified Data Center Architecture



Core: L3 boundary to the DC network. Functional point for route summarization, the injection of default routes and termination of segmented virtual transport networks

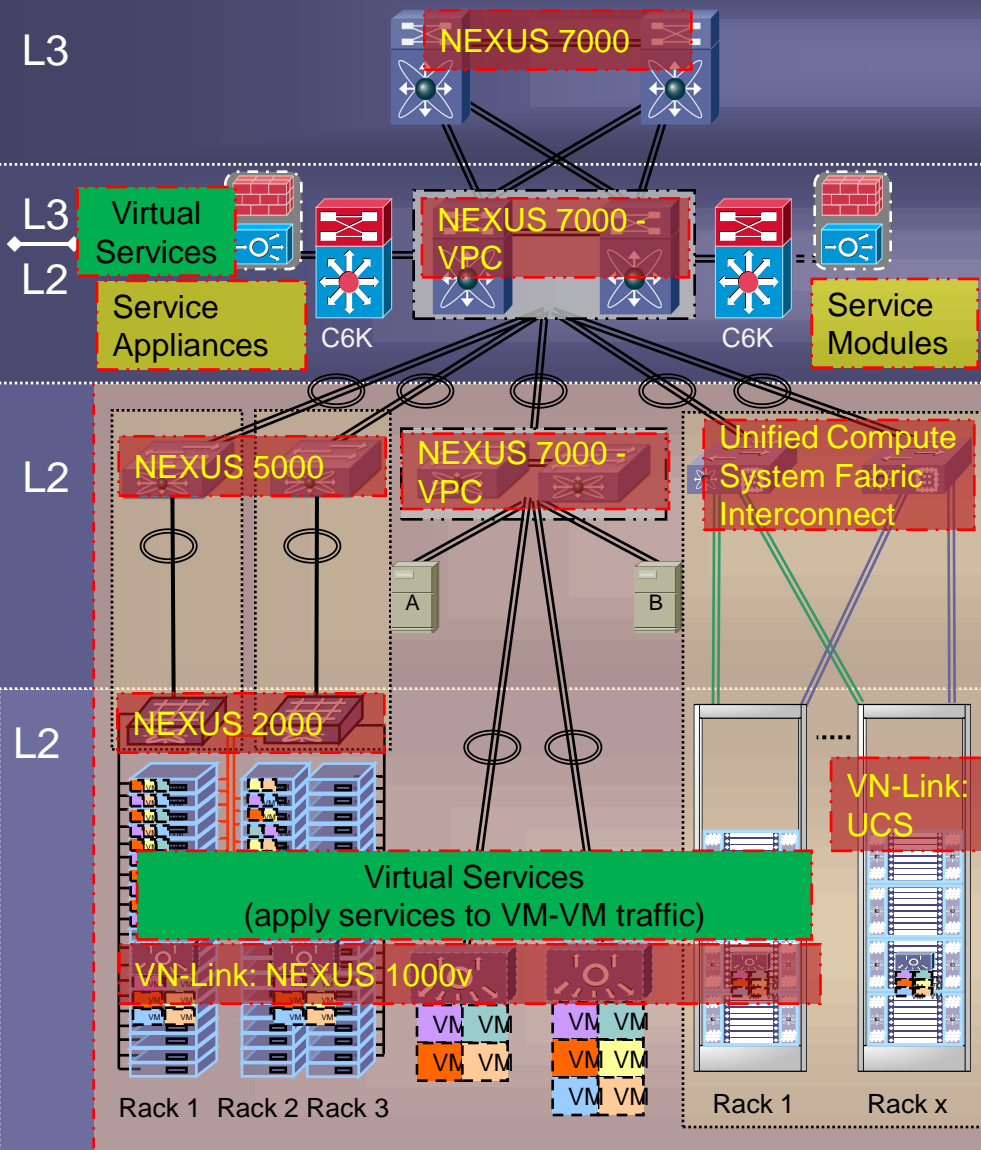
Aggregation: Typical L3/L2 boundary. DC aggregation point for uplink and DC services offering key features: VPC, VDC, 10GE density. Dedicated services are applied here

Access: Classic network layer providing non-blocking paths to servers & IP storage devices through VPC. It provides centralized config & mgmt and ease horizontal cabling demands related to 1G and 10GE server environments

Virtual Access: A virtual layer of network intelligence offering access layer-like controls to extend traditional visibility, flexibility and mgmt into virtual server environments. Virtual network switches bring access layer switching capabilities to virtual servers without burden of topology control plane protocols. Virtual Adapters provide granular control over virtual and physical server IO resources

The Unified Data Center Architecture

Deploying Virtual Services



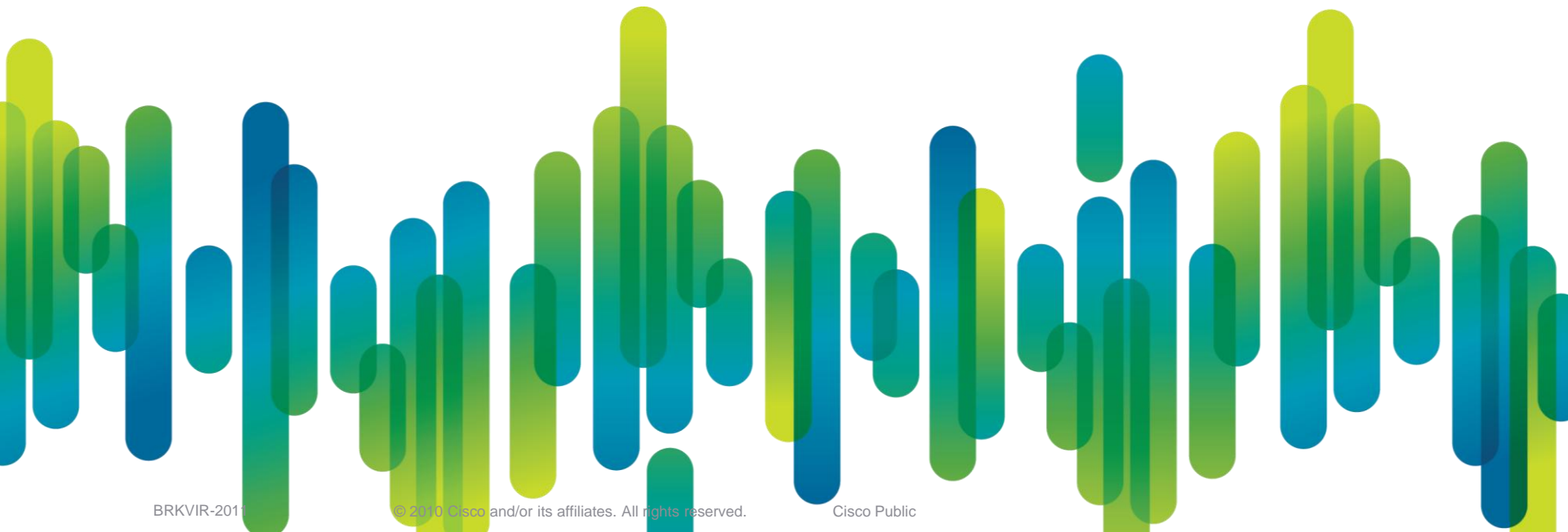
Aggregation: Service Layer

- Virtual Services deployed as an alternative to dedicated services

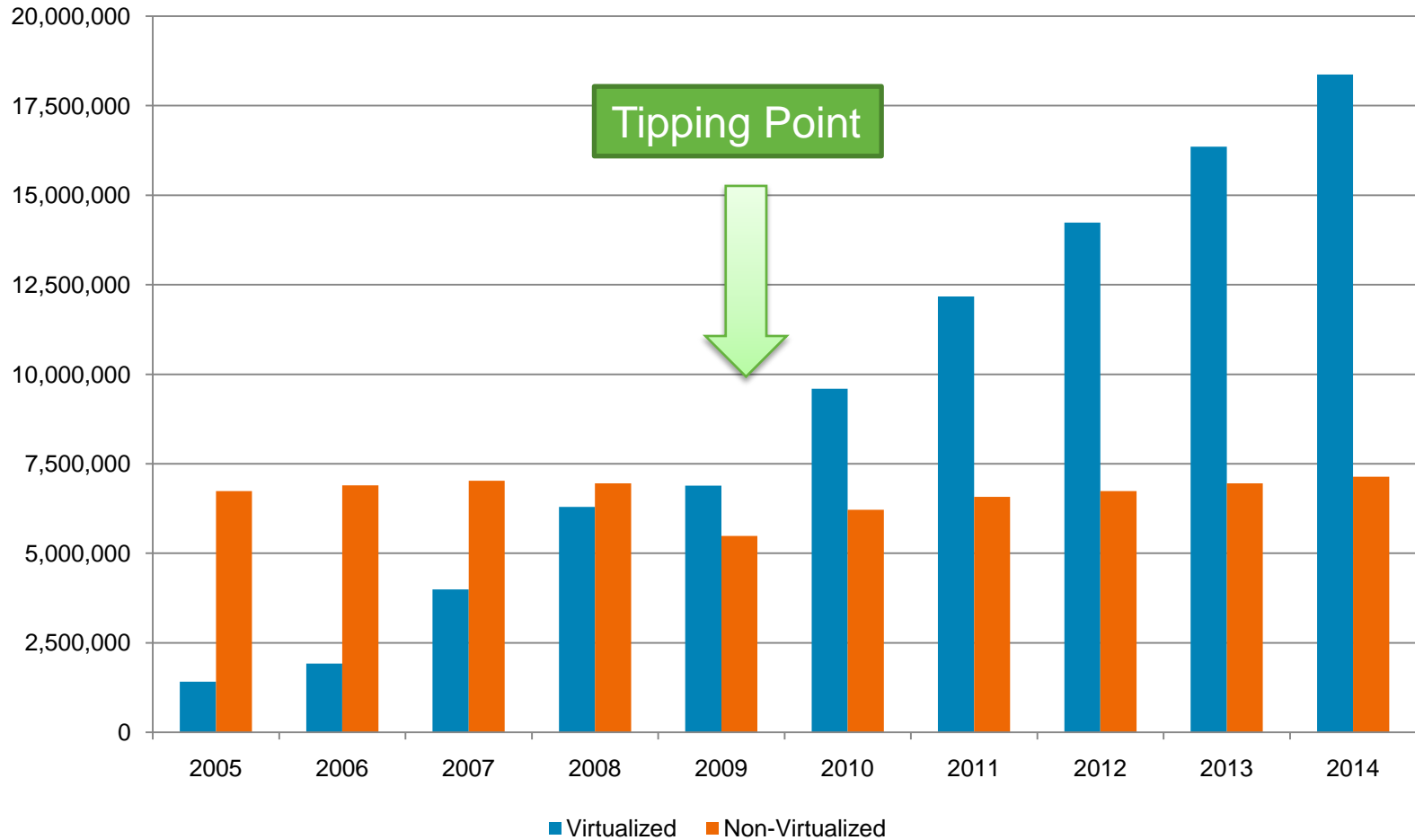
Virtual Access: Hypervisor-based Services

- Virtual Services applied to VM traffic
 - External-to-VM / VM-to-external
 - VM-to-VM
- Virtualization awareness
 - Dynamic policy-based provisioning
 - Support vMotion
 - Multi-tenant / Scale-out operation

Virtualization/Cloud Trends



More Servers are Virtualized



Source: IDC, Nov 2010

Benefits of Virtualization



Denton County: Before & After Virtualization

Physical
125 Physical Servers
325 tons of annual CO ₂ emissions
NO server clustering
Limited Network Capacity
Limited Data Protection

Virtual
9 Physical Virtualization Hosts
38 tons of annual CO ₂ emissions
HA for all servers
10 GB DCE Network (eventually)
Backups @ VM & File Levels DR foundation for all servers

Benefits of Virtualization



5-Year Savings for 96 Servers

	Unit Cost	Physical	Virtual	Savings
Servers (Existing)	\$10,000	\$1,200,000	\$136,170	\$1,063,830
New Servers (5/yr)	\$10,000	\$250,000	-	\$250,000
Power/Cooling Servers	\$75	\$432,000	\$27,000	\$405,000
Power/Cool New Servers	\$75	\$ 56,250	-	\$ 56,250
Maintenance	-	-	\$32,648	<\$32,648>
Windows Svr (74 Std)	\$ 789	\$ 125,183	-	\$125,183
Windows Svr (10 Ent)	\$ 2,559	\$ 54,850	\$75,000	<\$20,150>
SQL Svr (16 Std)	\$ 6,285	\$ 215,493	-	\$215,493
SQL Svr (0 Ent-8 CPU)	\$23,910	-	\$159,400	<\$159,400>
Total		\$2,360,633	\$430,218	\$1,930,415

Journey to 100% Virtualization

Recent Forbes Insights survey: 235 CIOs and IT executives:

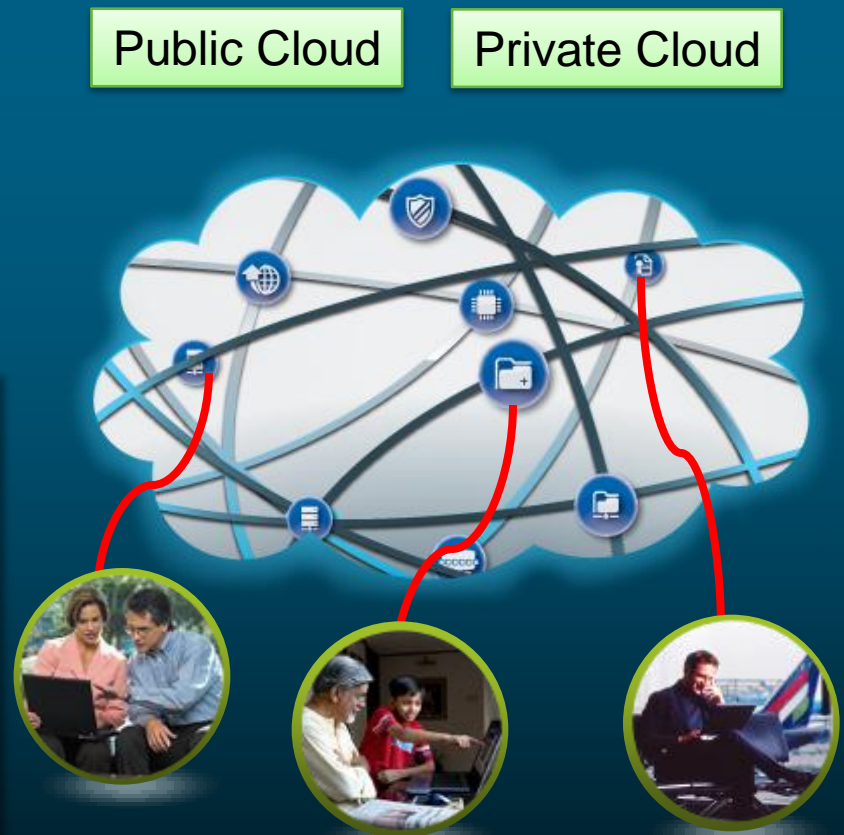
- ▶ **48%** have virtualized at least a quarter of their organization's servers in order to reduce infrastructure costs and deliver applications more rapidly
- ▶ **43%** of the survey respondents identified security as their top concern about adopting virtualization as the foundation for cloud computing

A Common Definition—Cloud Computing

IT Resources and Services that Are **Abstracted** from the Underlying Infrastructure and Provided “**On Demand**” and “**At Scale**” in a **Multitenant and Elastic** Environment

A Style of Computing Where Massively Scalable IT-Enabled Capabilities Are Delivered “As a Service” to Multiple External Customers Using Internet Technologies

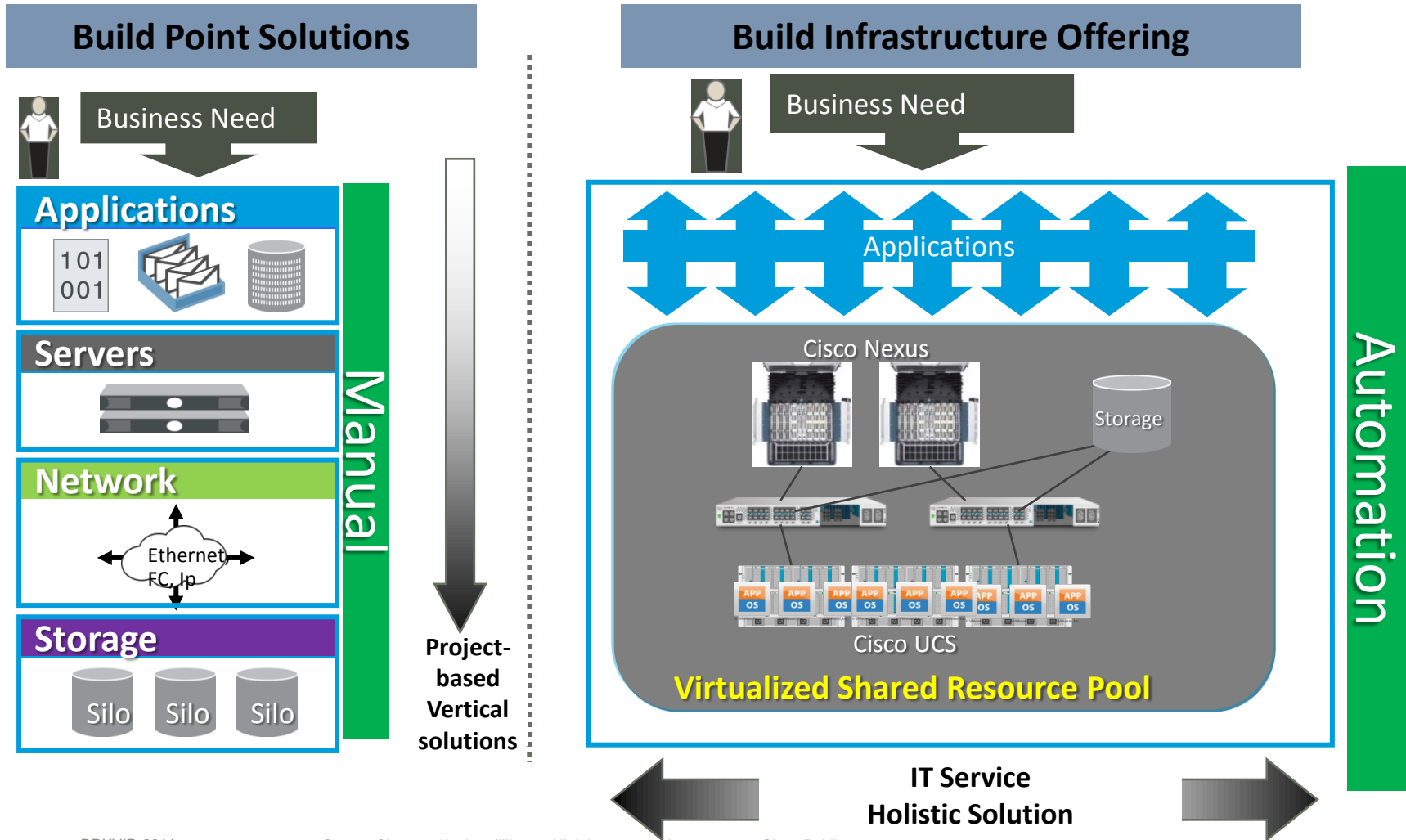
Source: Gartner “Defining and Describing an Emerging Phenomenon”
June 2008



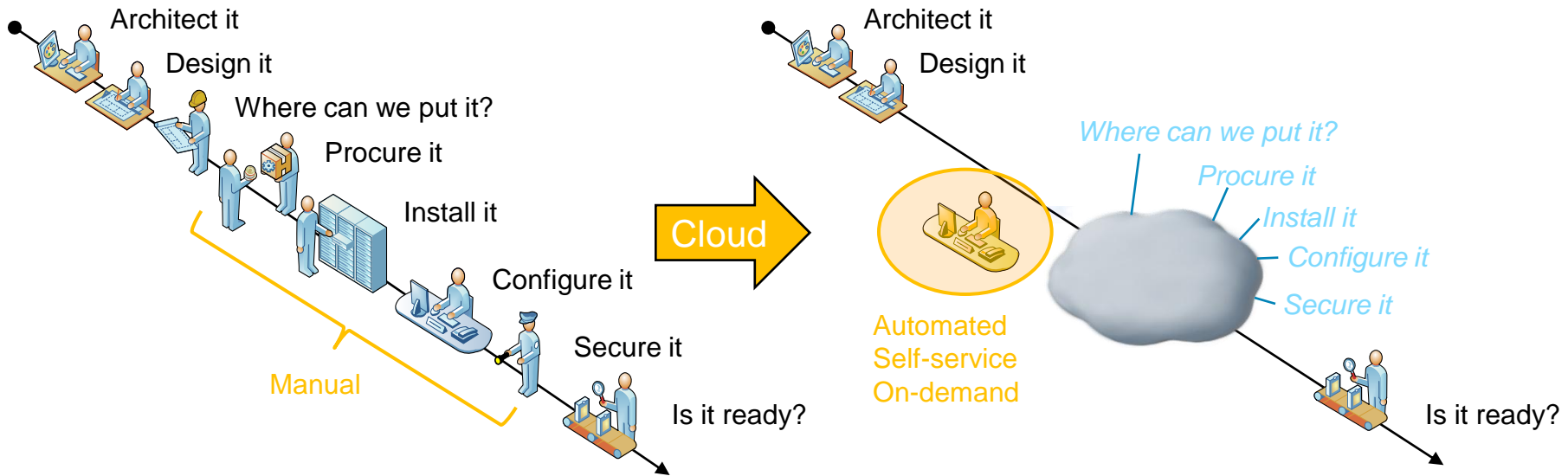
**Anywhere,
Anyone,
Any Service**

Enterprise Private Cloud Datacenter

IT as a Service Model



Delivering a (complex) service – faster (with full end-to-end automation)



Before

- Machine-oriented
- Manual provisioning
- Hard to control utilization

- High provisioning & ops cost
- Extended provisioning time
- Configuration risk

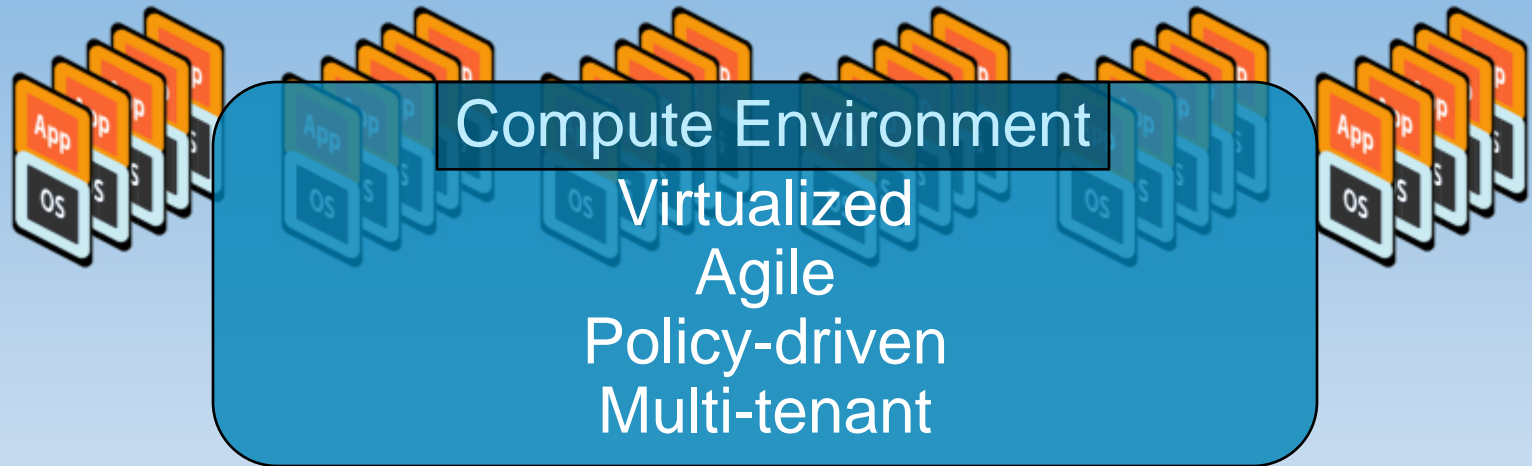
After

- Service-oriented
- Self-service; automated provisioning
- Elasticity (capacity-on-demand)

- Optimized provisioning & ops cost
- Rapid provisioning
- Increased Resiliency and Availability

Cisco's Virtual Networking Vision

Accelerate Data Center Virtualization



Virtual Network Link (VN-Link)

Extend networking to virtualized environments

- Hypervisor Switch (SW): **Nexus 1000V**
 - 802.1Q standards based, Feature rich
- External Switch (HW): **UCS 6100 + VIC**
(Pre-standard, IEEE 802.1Qbh)

Virtual Network Services

Extend network services to virtualized environments

- Virtual Security Gateway for Nexus 1000V
- Virtual WAAS
- NAM virtual service blade on Nexus 1010

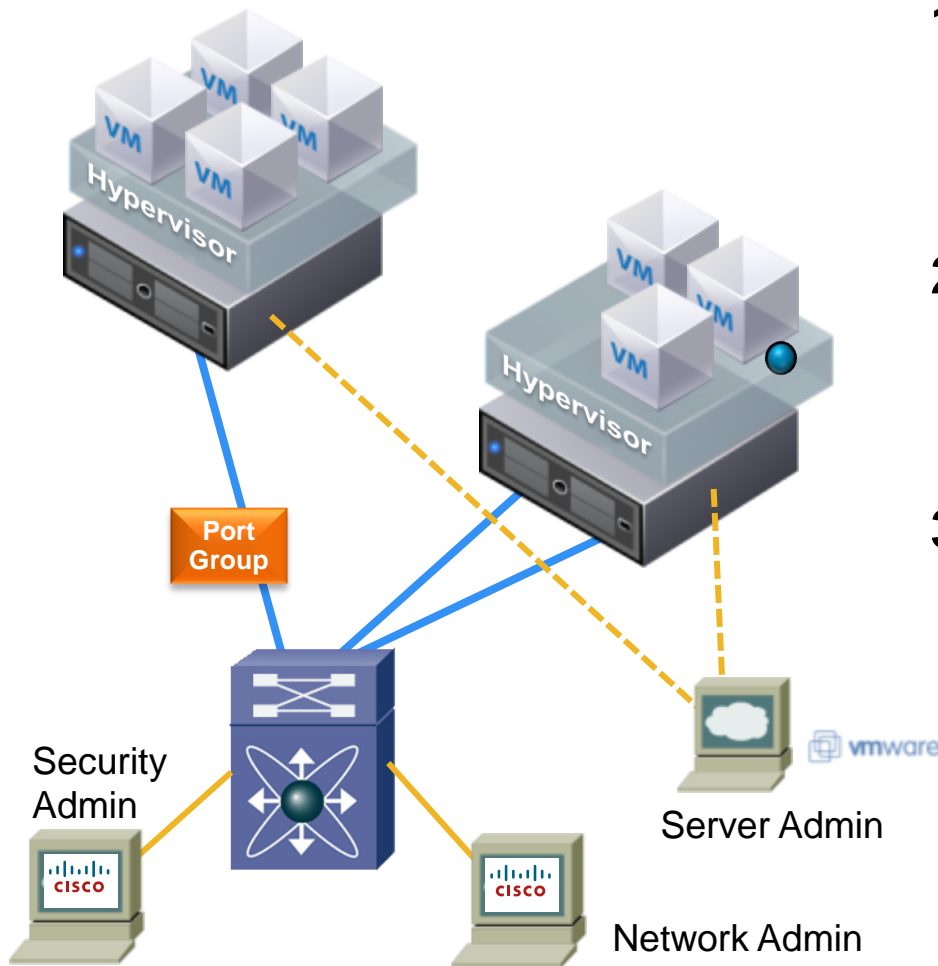
Virtual Network Management (UCSM, VNMC)

- Policy-driven, Programmatic, Multi-device, Multi-tenant

Virtual Networking

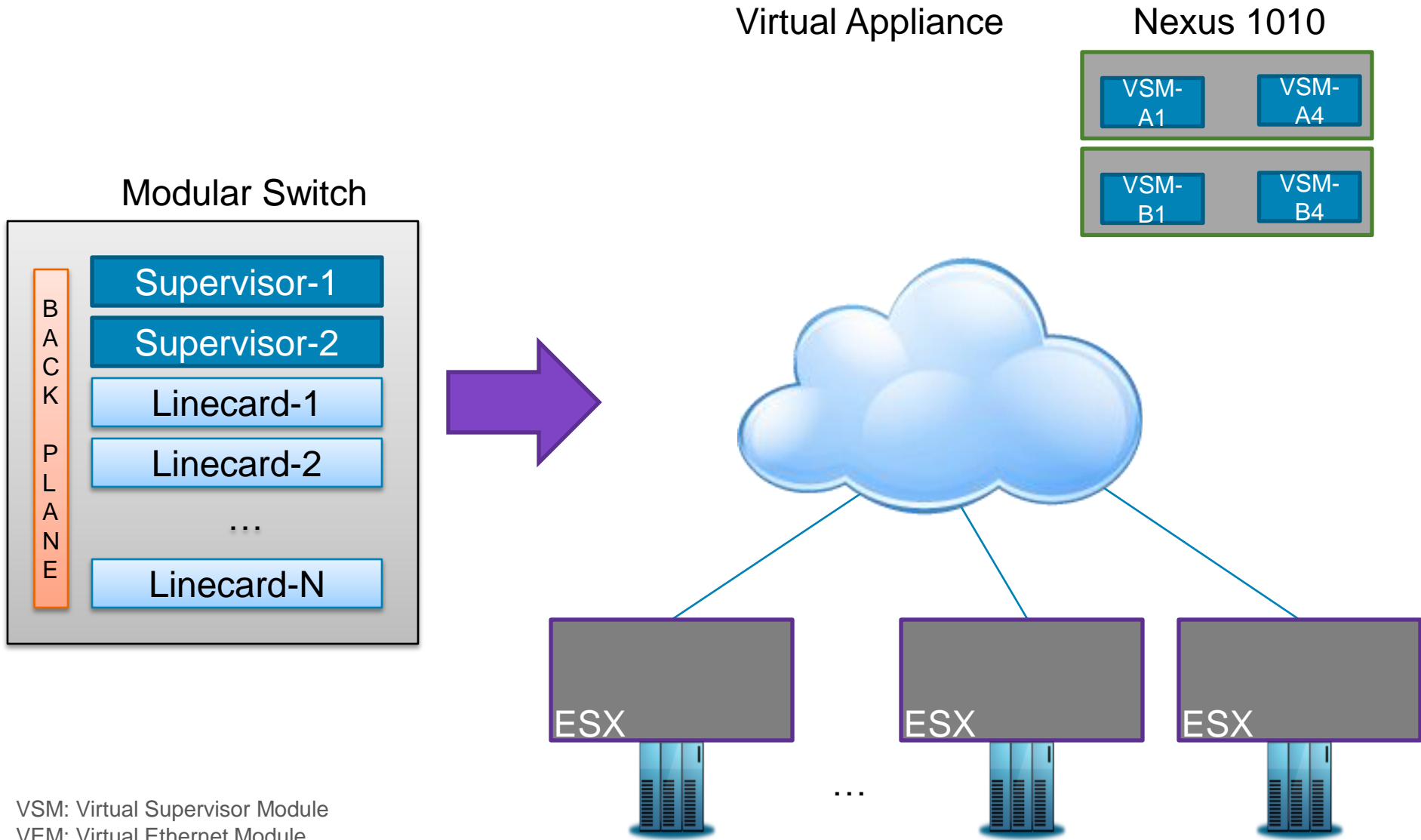
Architecting the Nexus 1000V

Server Virtualization 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 **segregation of duties** while ensuring **non-disruptive operations**

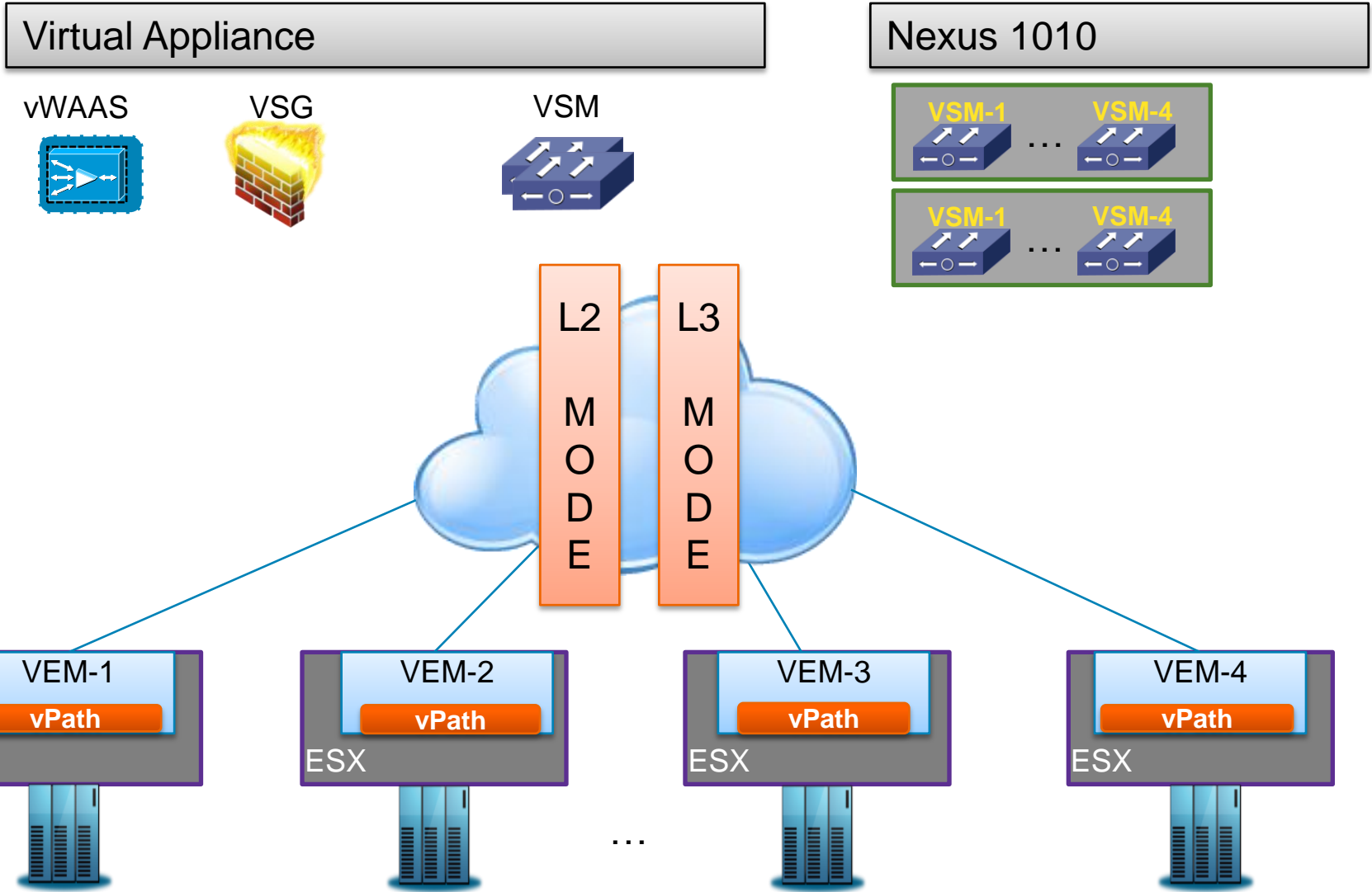
Nexus 1000V Architecture



VSM: Virtual Supervisor Module
VEM: Virtual Ethernet Module

Embedding Intelligence for Virtual Services

vPath – Virtual Service Datapath



vPath: Virtual Service Datapath

VSG: Virtual Security Gateway for 1000V

vWAAS: Virtual WAAS

Nexus 1010 – Virtual Service Appliance

Hosting platform for services

Virtual Appliances

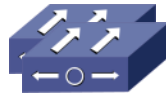
vWAAS



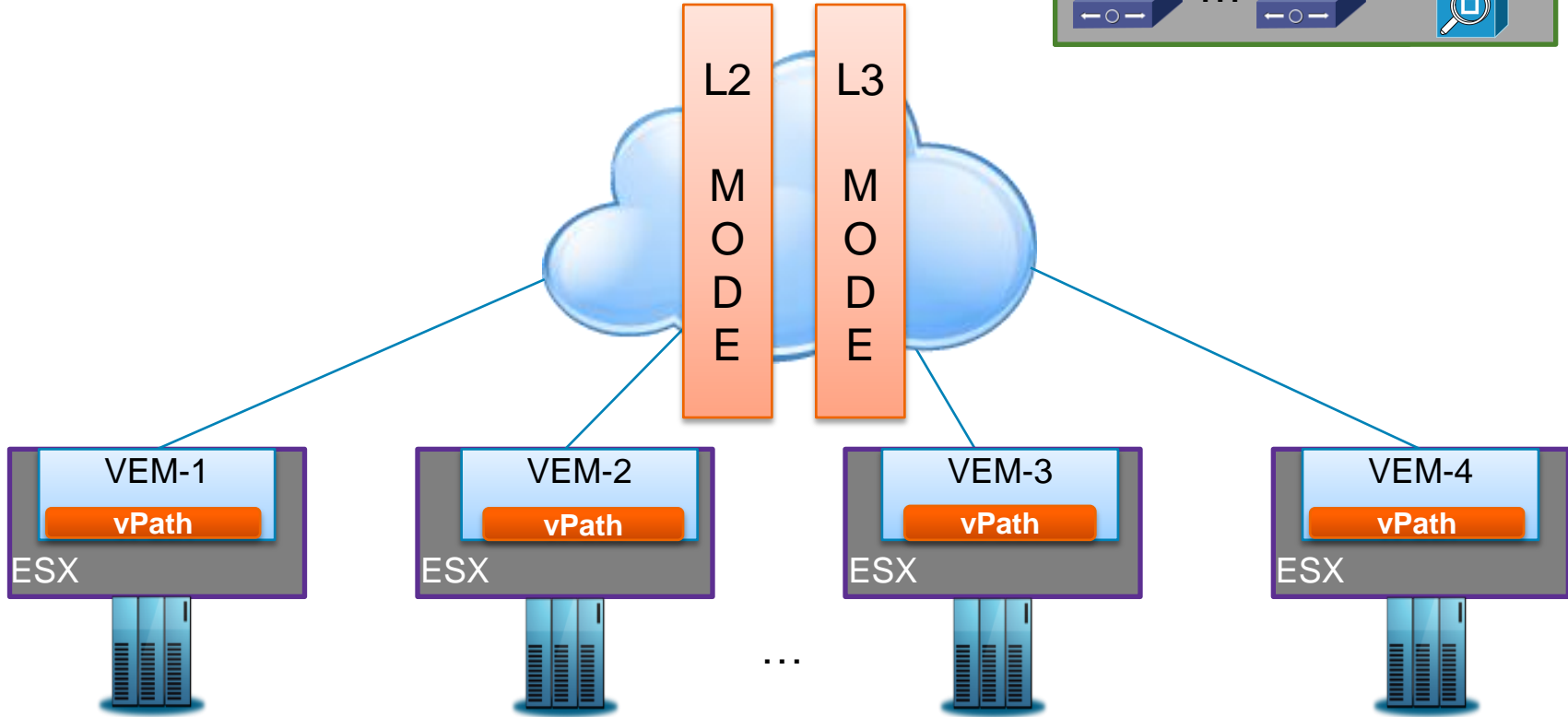
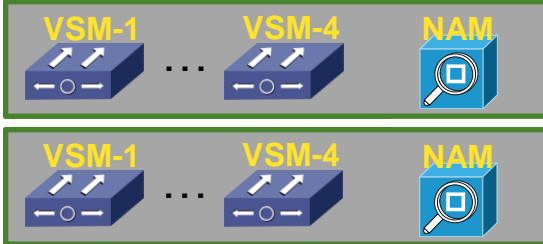
VSG



VSM



Nexus 1010



vPath: Virtual Service Datapath
VSG: Virtual Security Gateway for 1000V
vWAAS: Virtual WAAS

Cisco Nexus 1000V

Faster VM Deployment

Cisco VN-Link: Virtual Network Link

Policy-Based
VM Connectivity

Mobility of Network &
Security Properties

Non-Disruptive
Operational Model

Port Profiles

WEB Apps



HR



DB

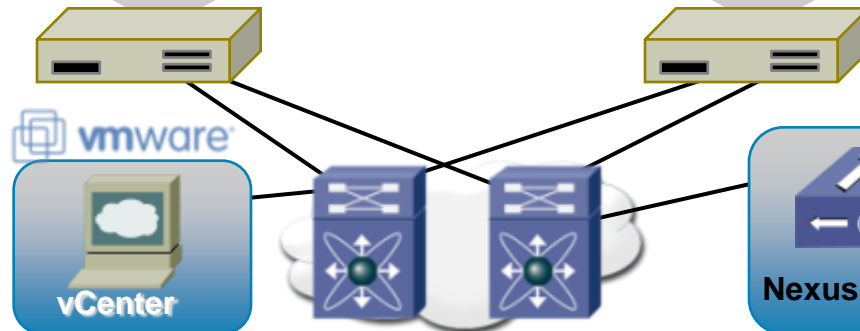
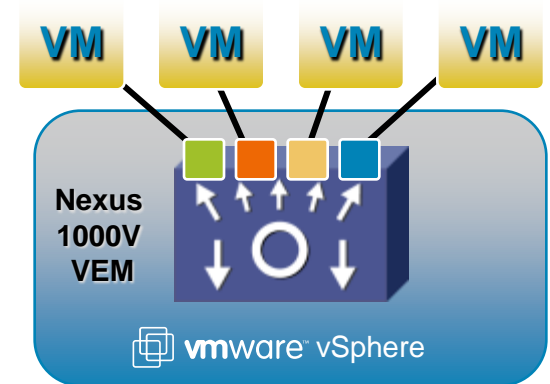
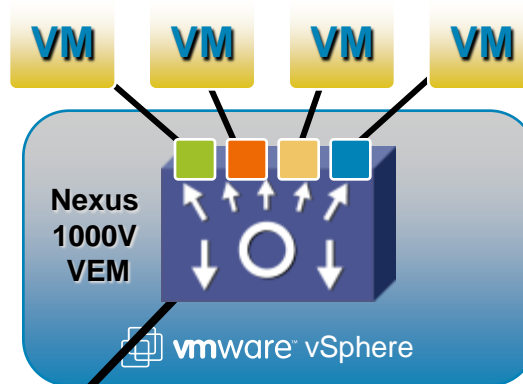


DMZ



VM Connection Policy

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



Cisco Nexus 1000V

Richer Network Services

Cisco VN-Link: Virtual Network Link

Policy-Based
VM Connectivity

Mobility of Network &
Security Properties

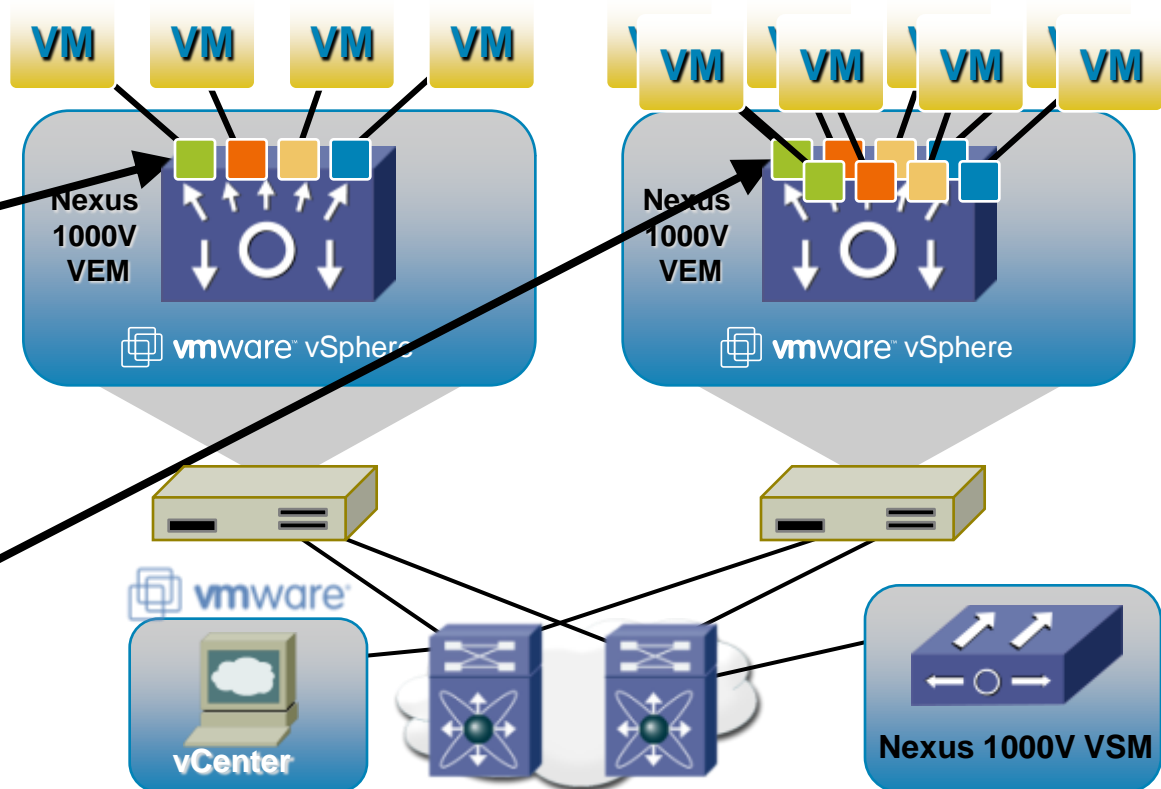
Non-Disruptive
Operational Model

VMs Need to Move

- VMotion
- DRS
- SW Upgrade/Patch
- Hardware Failure

Property Mobility

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



Cisco Nexus 1000V

Increased Operational Efficiency

Cisco VN-Link: Virtual Network Link

Policy-Based
VM Connectivity

Mobility of Network &
Security Properties

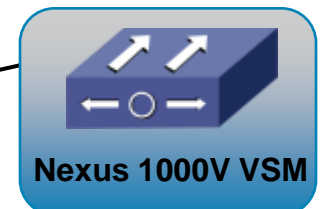
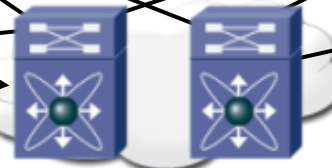
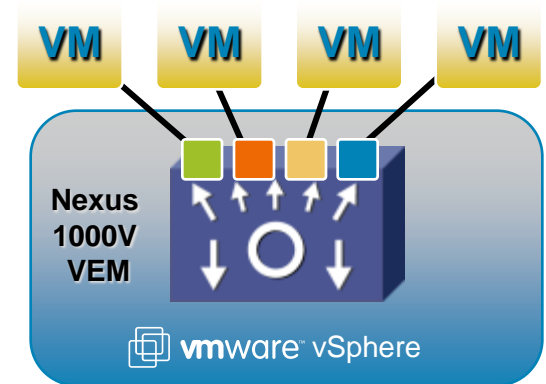
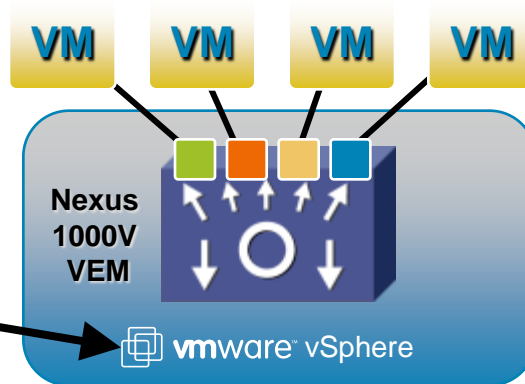
Non-Disruptive
Operational Model

VI Admin Benefits

- Maintains existing VM mgmt
- Reduces deployment time
- Improves scalability
- Reduces operational workload
- Enables VM-level visibility

Network Admin Benefits

- Unifies network mgmt and ops
- Improves operational security
- Enhances VM network features
- Ensures policy persistence
- Enables VM-level visibility



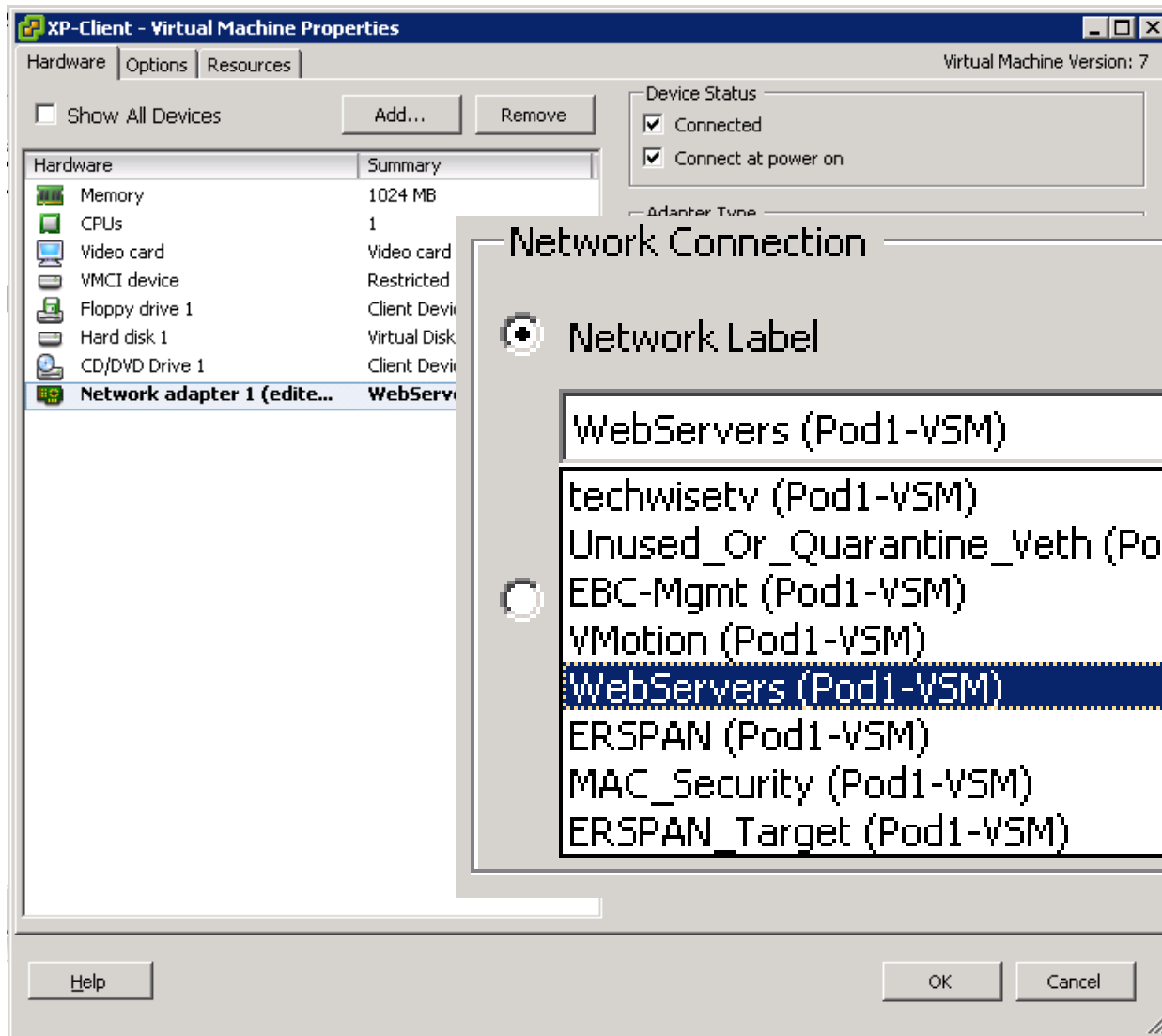
Port Profile: Network Admin View

```
n1000v# show port-profile name WebProfile
port-profile WebServers-PP
  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 Profile: Server Admin View



Advanced Features of the Nexus 1000V

Switching

- L2 Switching, 802.1Q Tagging, VLAN Segmentation, Rate Limiting (TX)
- IGMP Snooping, QoS Marking (COS & DSCP), Class-based WFQ

Security

- Policy Mobility, Private VLANs w/ local PVLAN Enforcement
- Access Control Lists (L2–4 w/ Redirect), Port Security
- Dynamic ARP inspection, IP Source Guard, DHCP Snooping

Network Services

- Virtual Services Datapath (vPath) support for traffic steering & fast-path off-load [leveraged by Virtual Security Gateway (VSG) and vWAAS]

Provisioning

- Automated vSwitch Config, Port Profiles, Virtual Center Integration
- Optimized NIC Teaming with Virtual Port Channel – Host Mode

Visibility

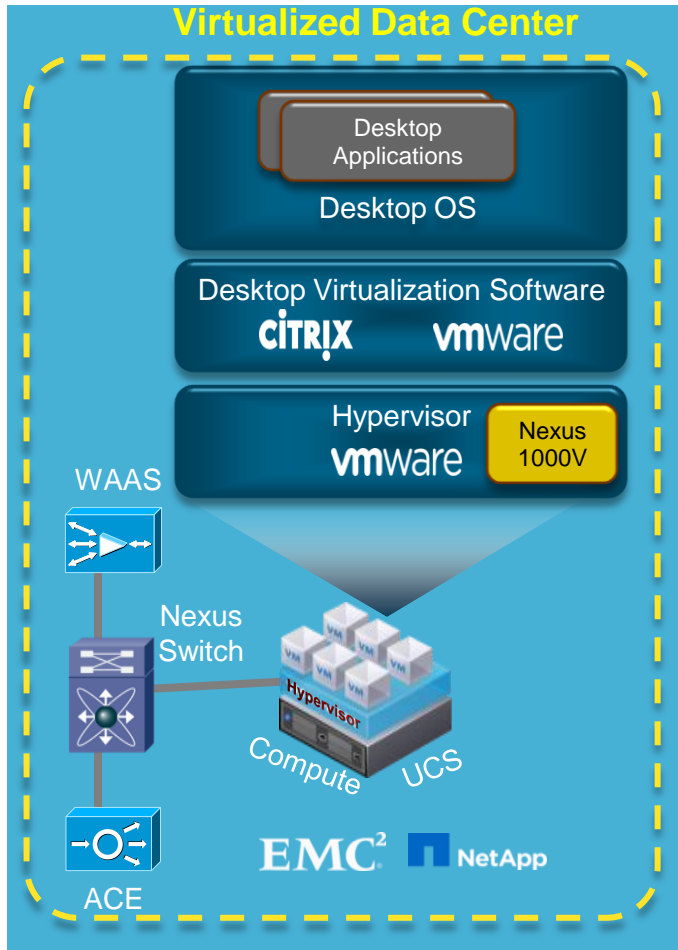
- VMotion Tracking, NetFlow v.9 w/ NDE, CDP v.2
- VM-Level Interface Statistics
- SPAN & ERSPAN (policy-based)

Management

- Virtual Center VM Provisioning, Cisco Network Provisioning, CiscoWorks
- Cisco CLI, Radius, TACACs, Syslog, SNMP (v.1, 2, 3)
- Hitless upgrade, SW Installer

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.

Securing Virtual Desktops (VDI)

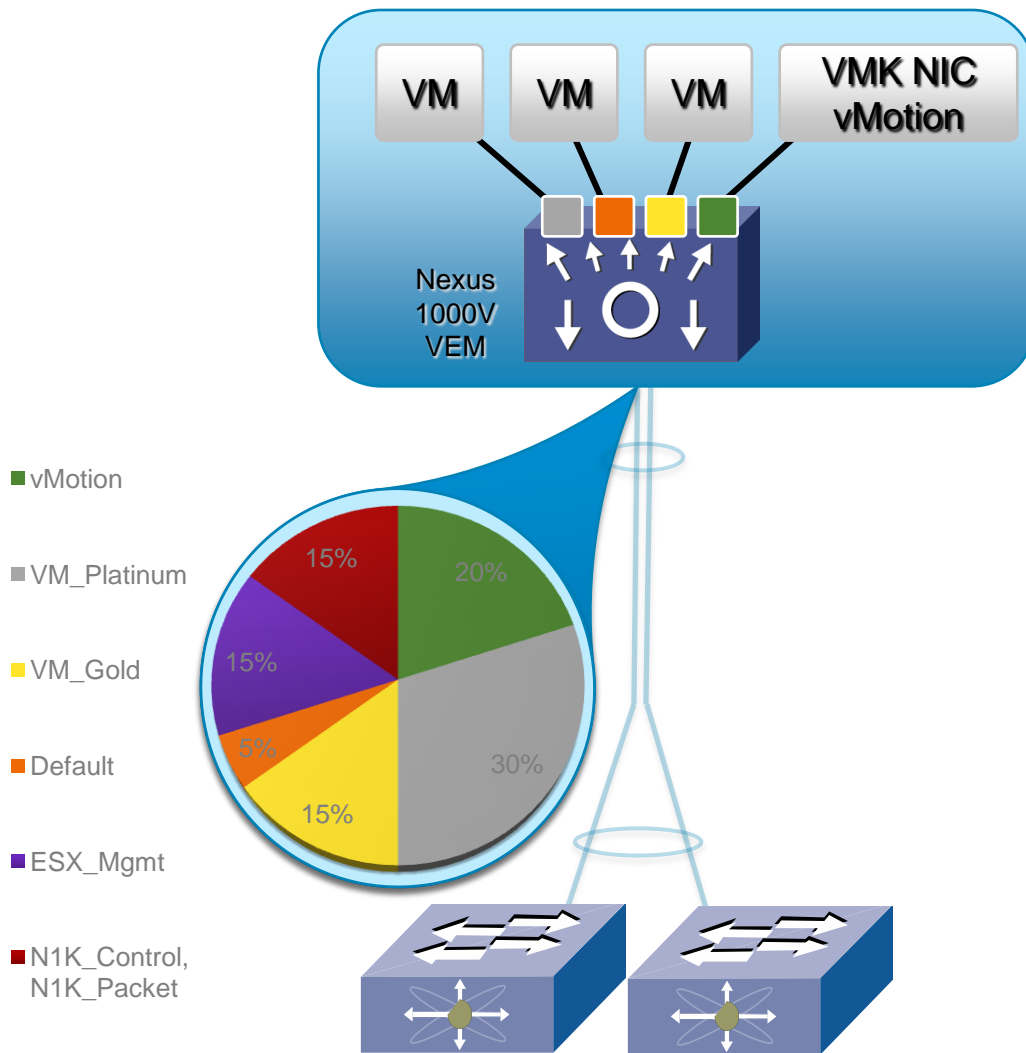


WAAS: Wide Area Application Service
ACE: Application Control Engine

1000V Security Features for VDI

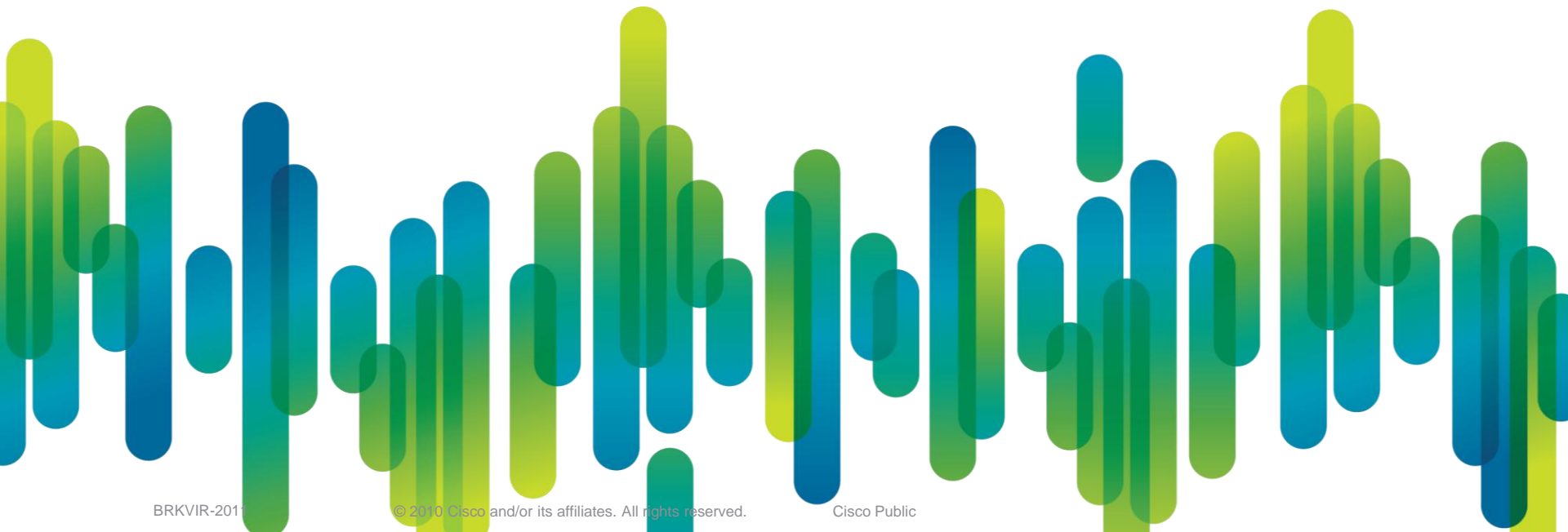
- Access Control List
- Port Security
- Private VLAN
- DHCP Snooping
- Dynamic ARP Inspection
- IP Source Guard

Quality of Service



- Provide bandwidth guarantee for up to 64 total queues on uplinks
- User defined Queues
- 8 Predefined traffic classes
 - For VMware and 1000V protocol traffic
- Queuing configured via modular QoS CLI (MQC)

Virtual Network Services



Data Center Business Advantage

New Architectural Framework: Cisco Data Center Business Advantage



Unified Fabric

- Nexus 1000V
- Nexus 5K/2K
- Nexus 7K



Unified Network Services

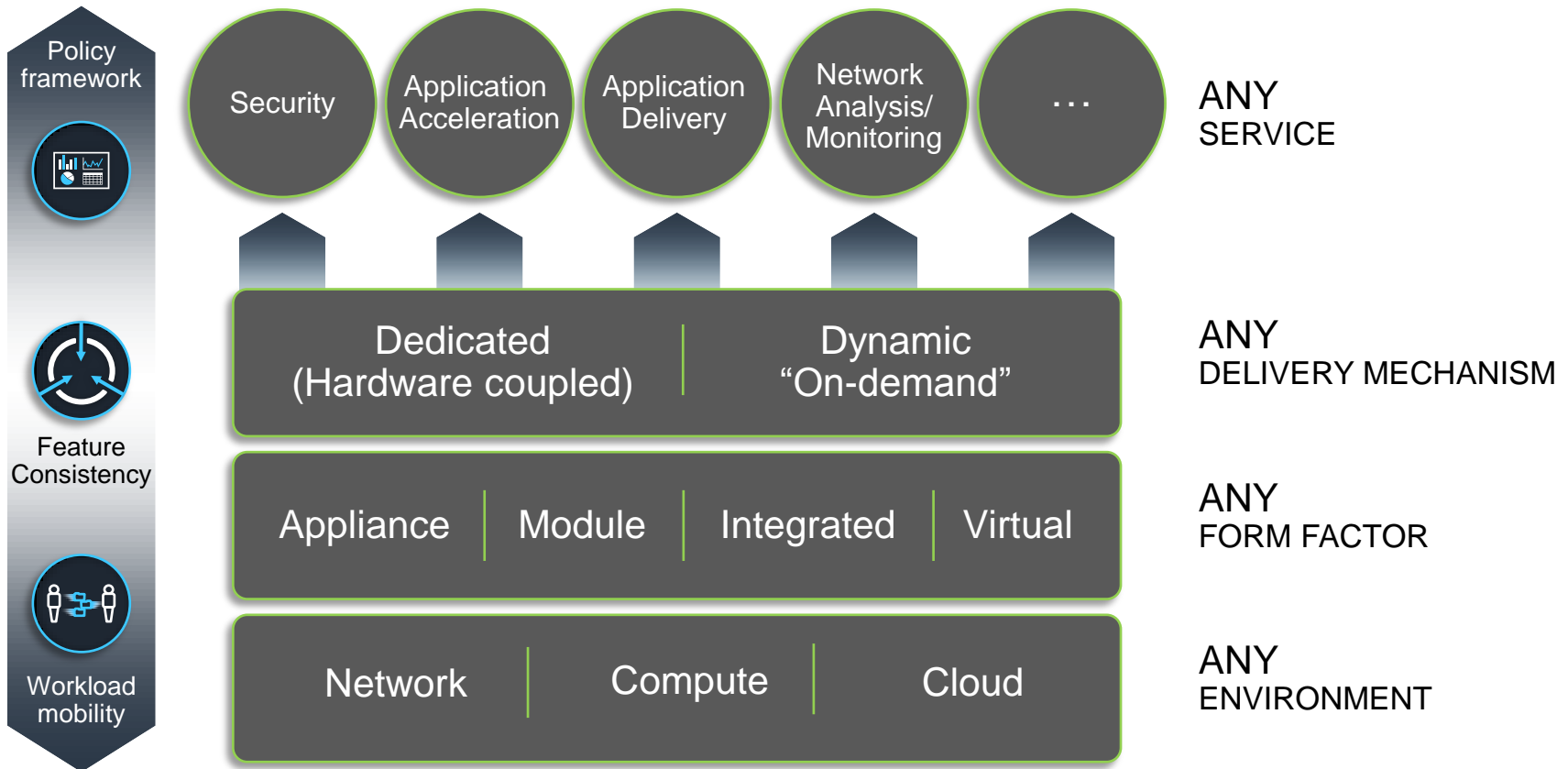
- **Virtual Security Gateway**
- **Virtual WAAS**



Unified Computing

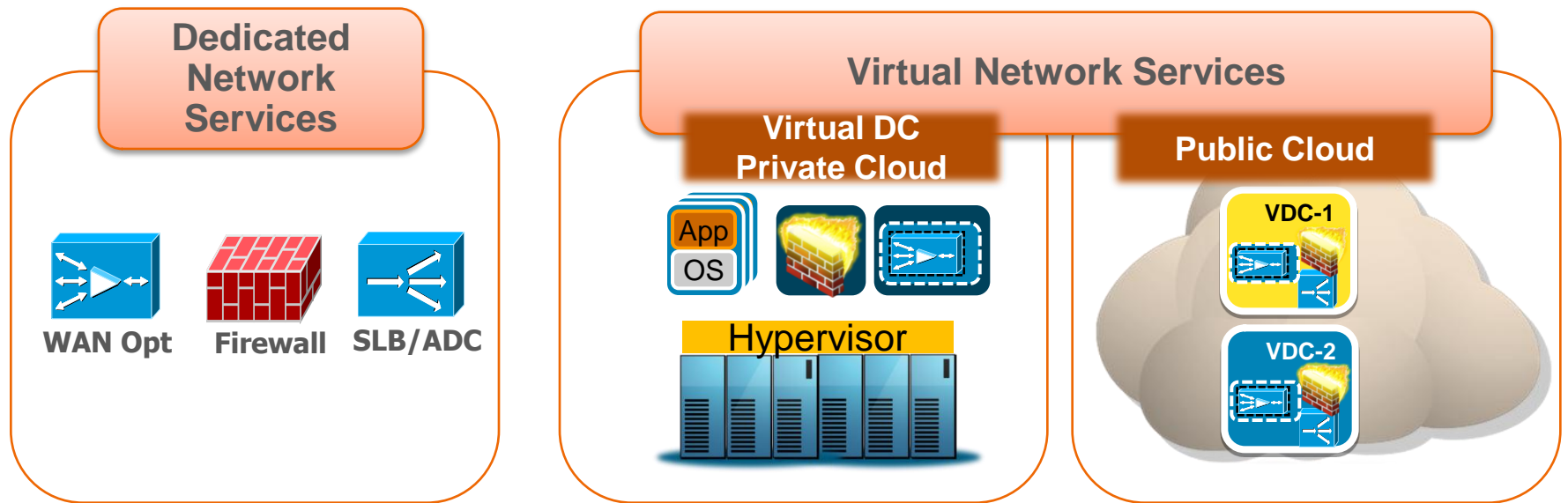
- Unified Compute System

Cisco Unified Network Services Vision



Flexibility and Choice For Any Deployment Model

Virtualization/Cloud driving new requirements for data center services



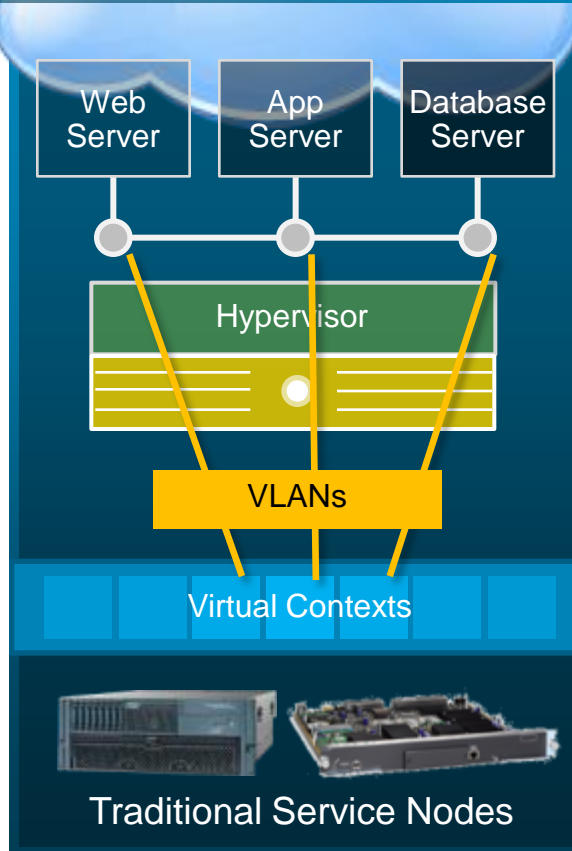
- Application-specific service nodes
- Form factors:
 - Appliance
 - Switch module
 - Router-integrated

- Virtual appliance form factor
- Elastic Instantiation/Provisioning
- Service transparent to VM mobility
- Support scale-out
- Large scale multi-tenant operation

Deployment options for Virtual Services

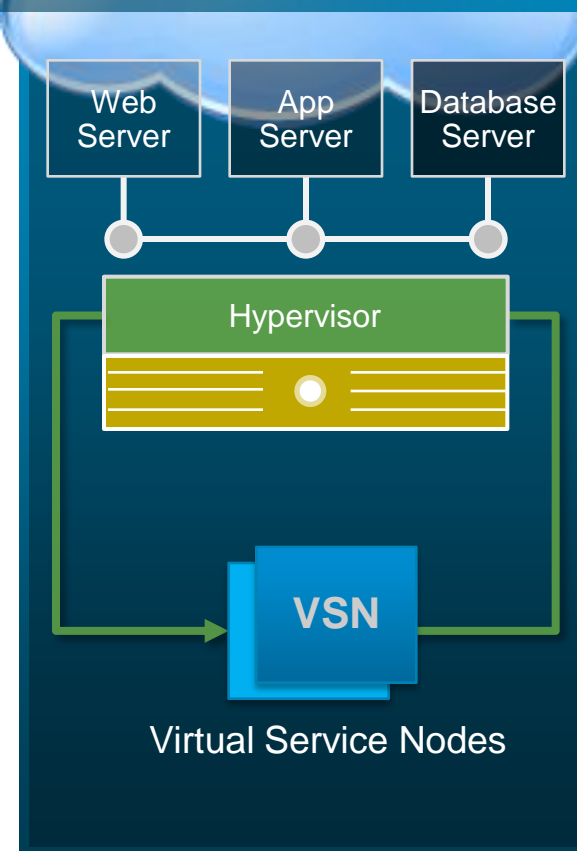
1

Redirect VM traffic via VLANs to external (dedicated) service node



2

Apply hypervisor-based Virtual Service Node (VSN)



UNS Products

Virtual Security Gateway (VSG)

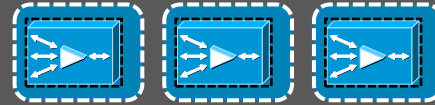
On Nexus 1000V



Virtual Network Management Center (VNMC)



Virtual WAAS



ESX ESXi Hypervisor
w/ Nexus 1000V

UCS /x86 Servers



vPath

Nexus 1000V

vPath: Fabric Intelligence for Virtual services

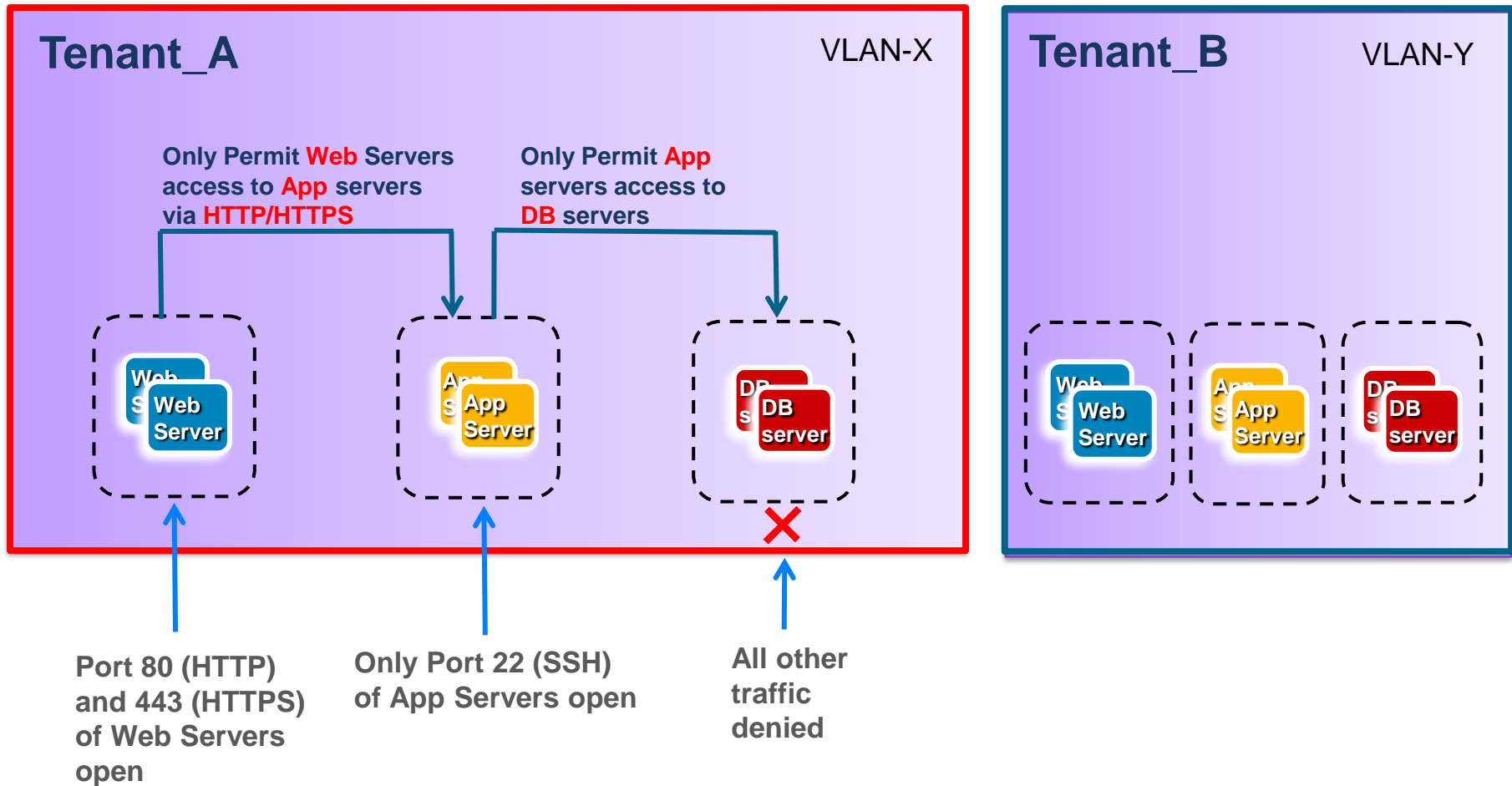
- Traffic interception/redirection, Fast-path off-load

Virtual Security Gateway (VSG)

Virtualization & Security

- Broad based DC virtualization & workloads moving to cloud
 - Lower cost, Agility, Scale-out
- Workloads of varied risk profiles share the same compute infrastructure
 - 3-tier applications, QA/Dev, HR, Finance
 - Unified Communications
 - Virtual Desktop
 - DMZ, Extranet, ...
- Increasing interest in Virtual Private Clouds
- How to:
 - Meet regulatory compliance, Audit needs
 - Ensure non-disruptive administration

Example Use Case: 3-tier Server Zones



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

Virtual Network Management Center (VNMC)



Non-Disruptive Operations

Security team manages security

Policy Based Administration

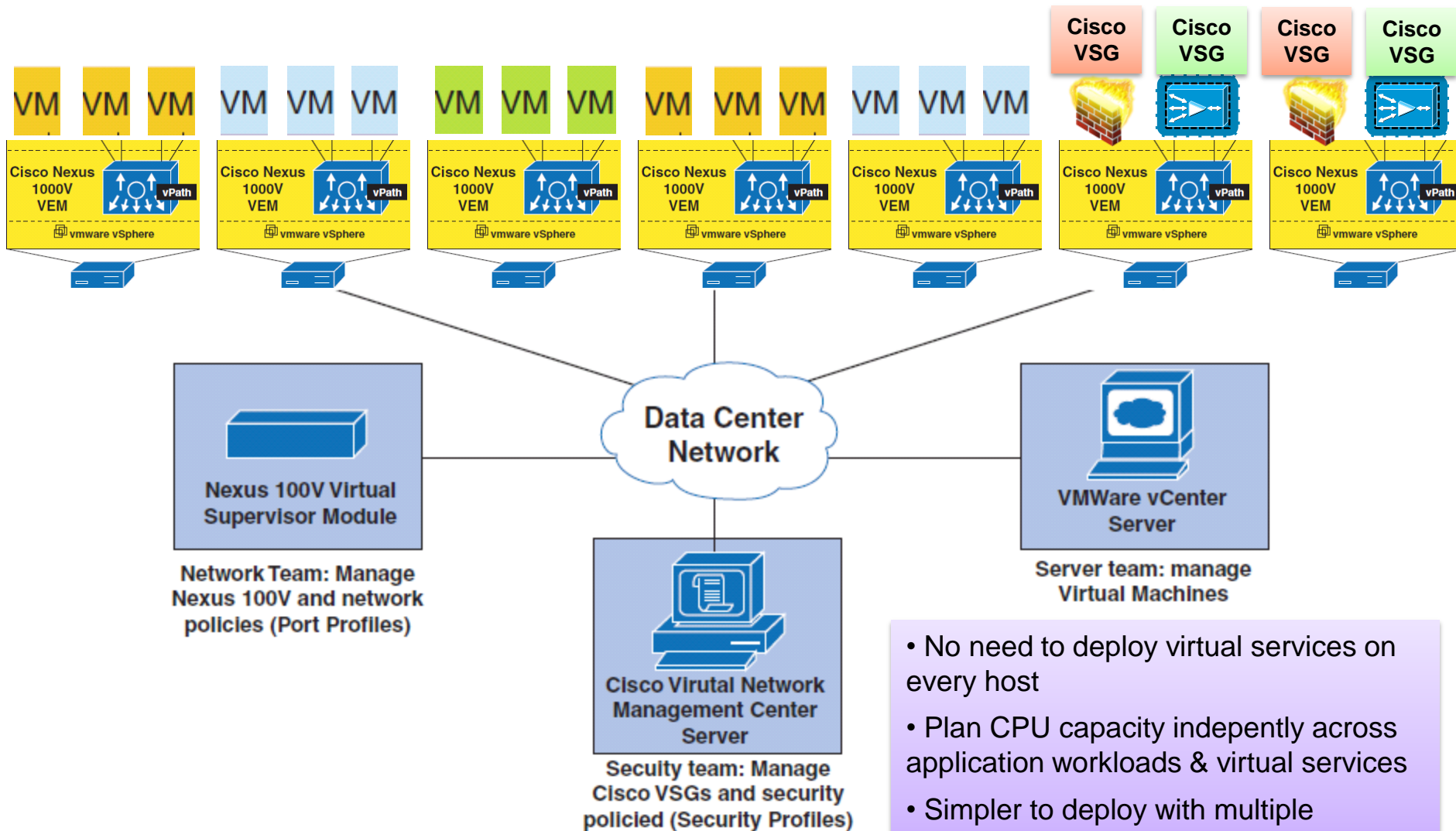
Central mgmt, scalable deployment, multi-tenancy

Designed for Automation

XML API, security profiles

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

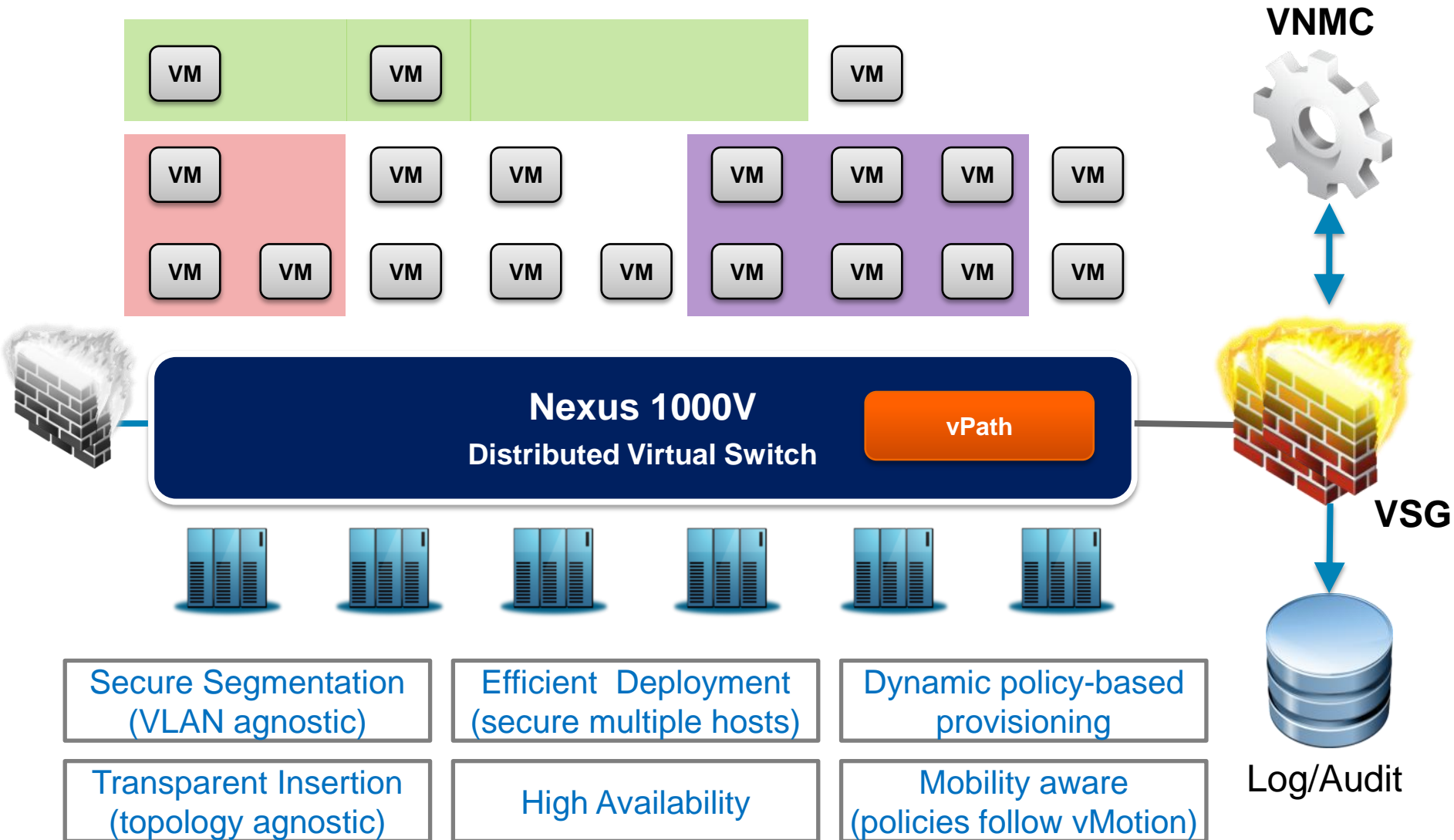
Decoupled Deployment across Applications & Virtual Services



- No need to deploy virtual services on every host
- Plan CPU capacity independently across application workloads & virtual services
- Simpler to deploy with multiple operations teams (server, network, security, etc.)

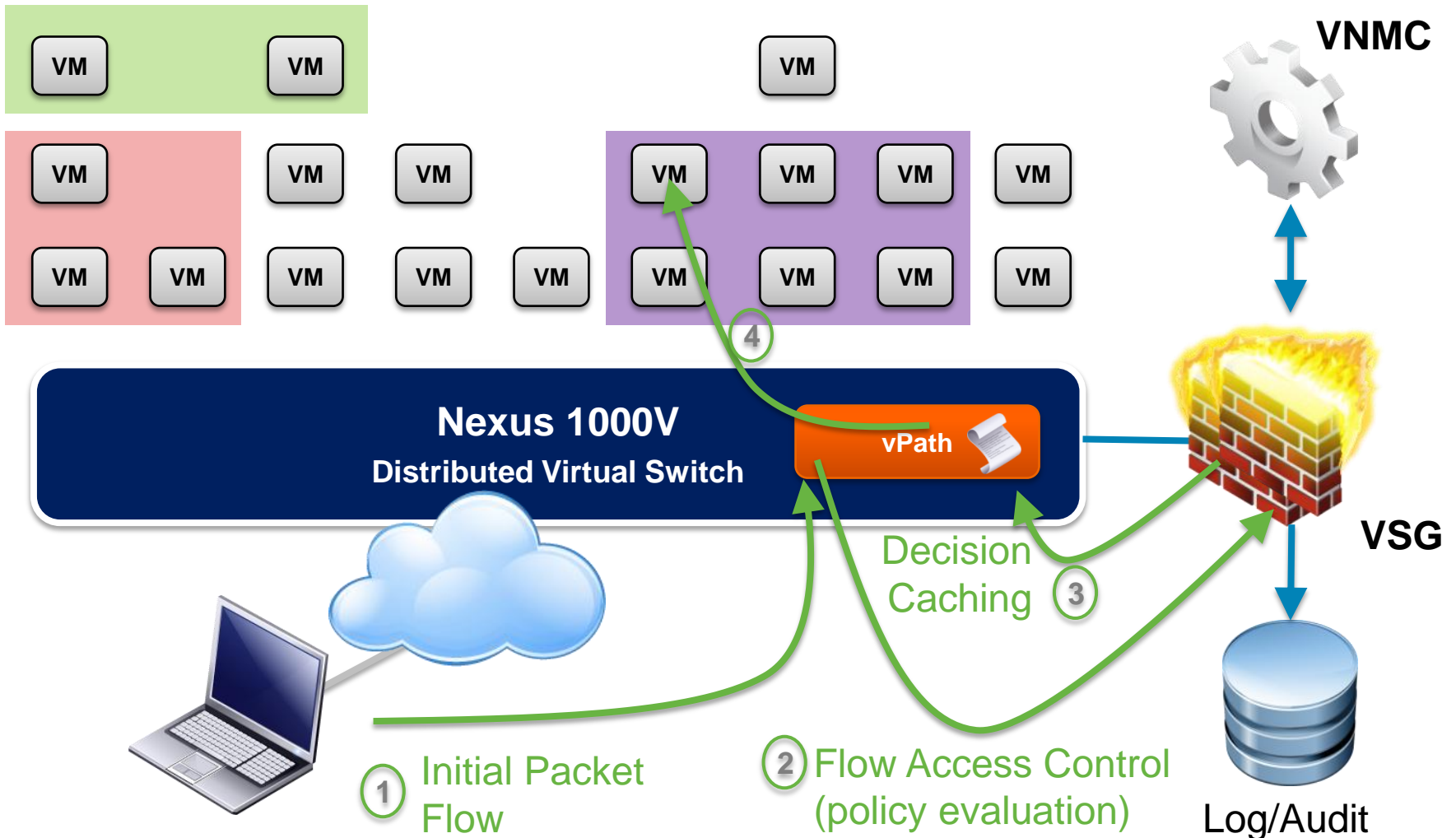
Virtual Security Gateway

Logical deployment like physical appliances



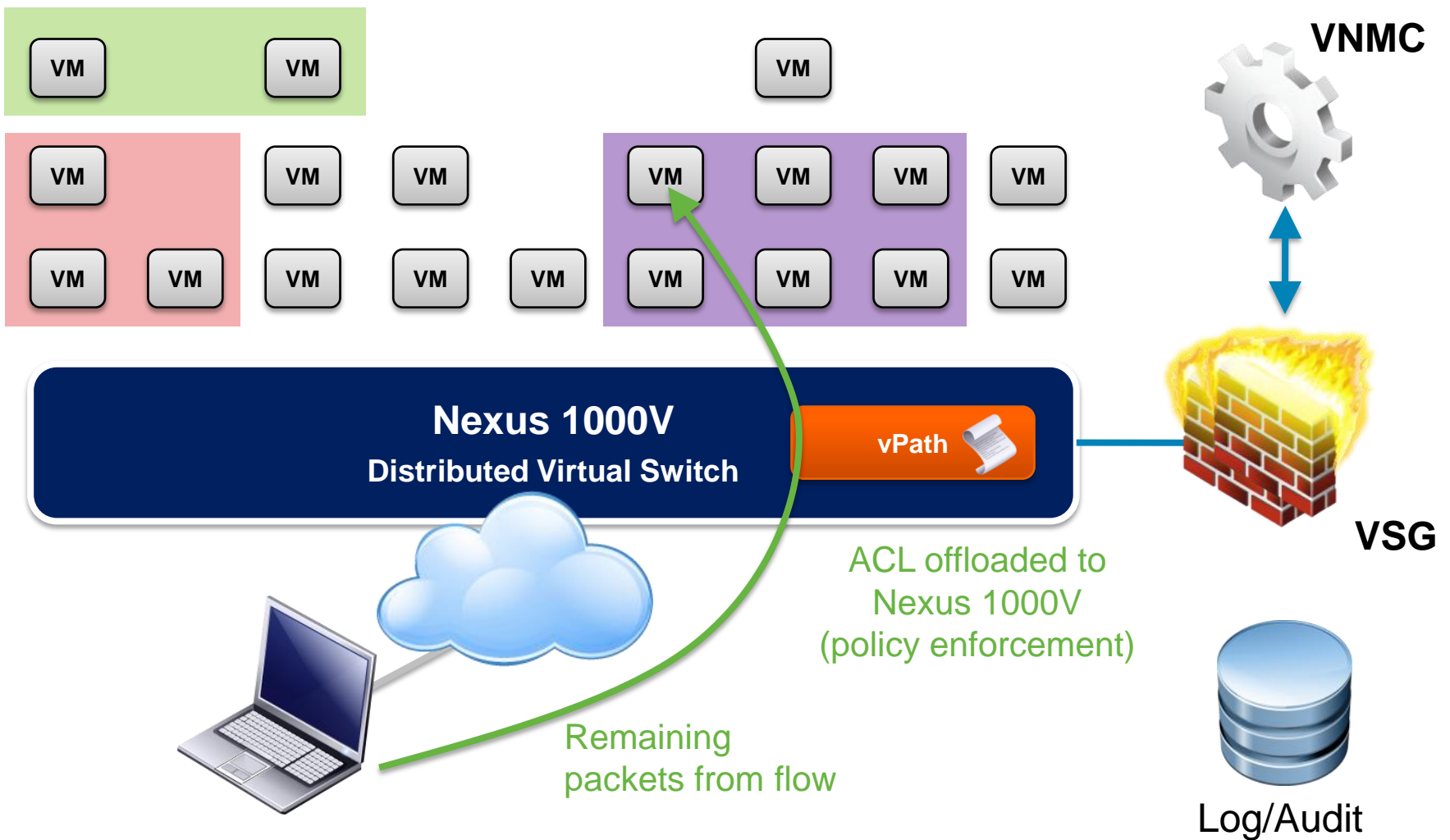
Virtual Security Gateway

Intelligent Traffic Steering with vPath

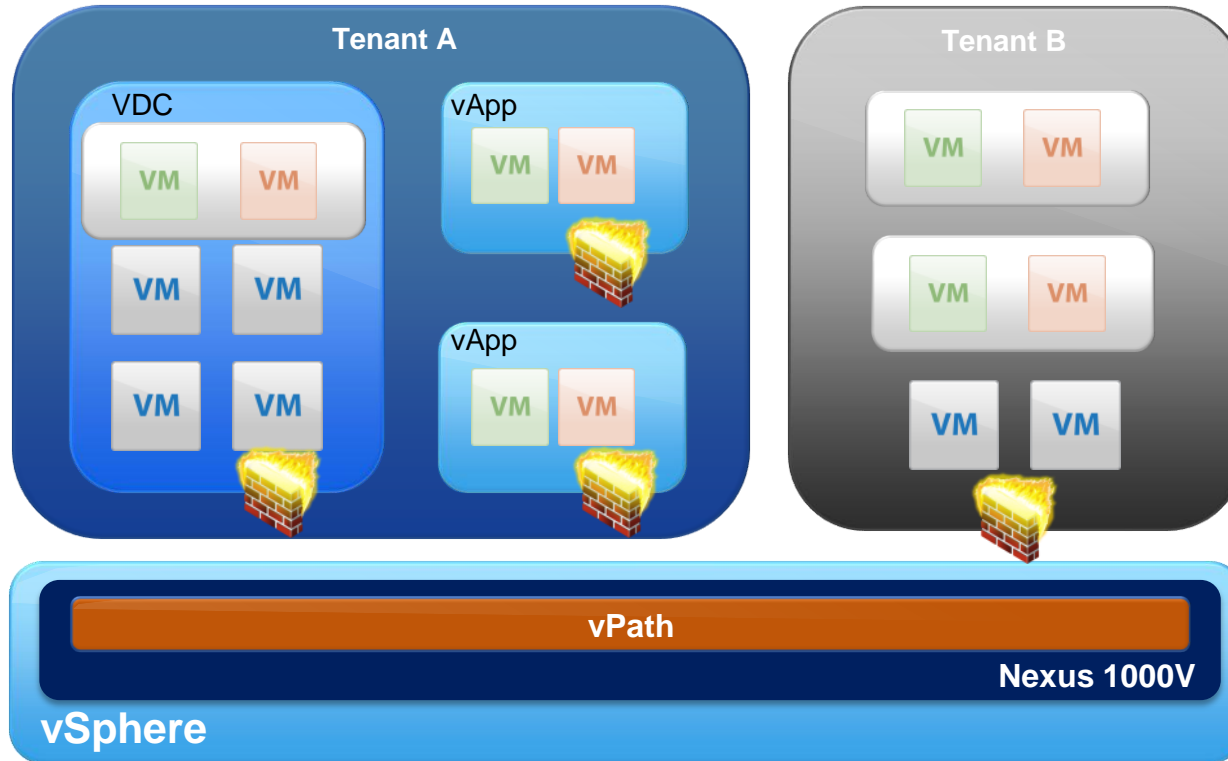


Virtual Security Gateway

Performance Acceleration with vPath



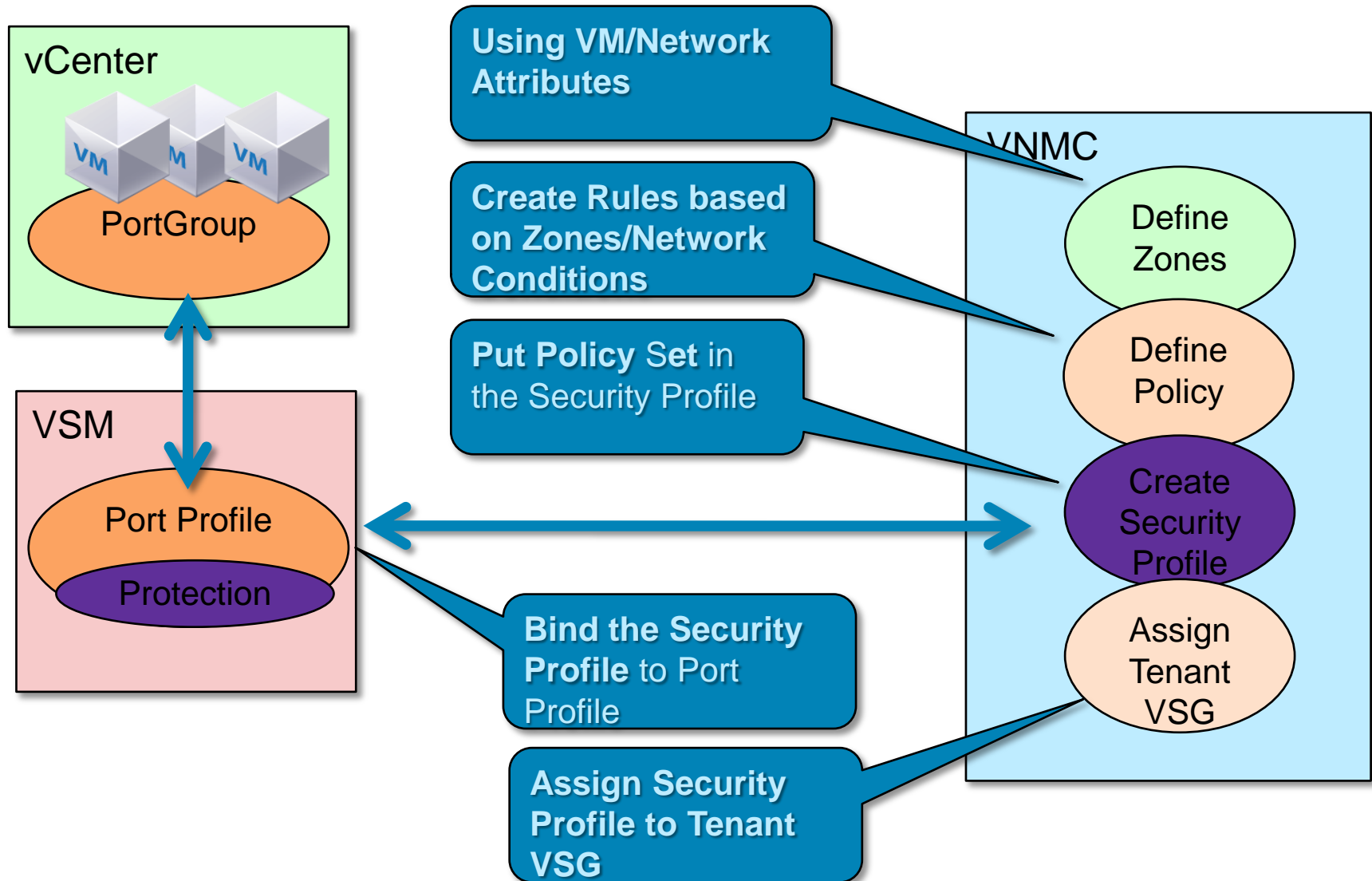
Apply Security at Multiple Levels



Specify zoning policy with the appropriate granularity

- Tenant
- VDC
- vApp

VSG Policy Provisioning Logical Flow



Define Condition for Rules

Add Add Destination Condition

Attribute Type: **Attribute Type**

Network
VM
Custom

Expression

Attribute Name: Operator: Attribute Value:

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

OK Cancel

Binding VSG Security Profile with 1000V Port-Profile

The screenshot displays the Cisco Virtual Network Management Center (VSM) interface and a terminal window. The VSM GUI shows the 'Security Profiles' configuration page for the 'Contrator' tenant. A table lists the security profiles, with 'SecureContractors' highlighted. The terminal window shows the configuration commands for the 'SecureContractors' profile, including the 'port-profile type vethernet' configuration and the 'vn-service' configuration that binds the profile to the 'SecureContractors' name.

Terminal Output:

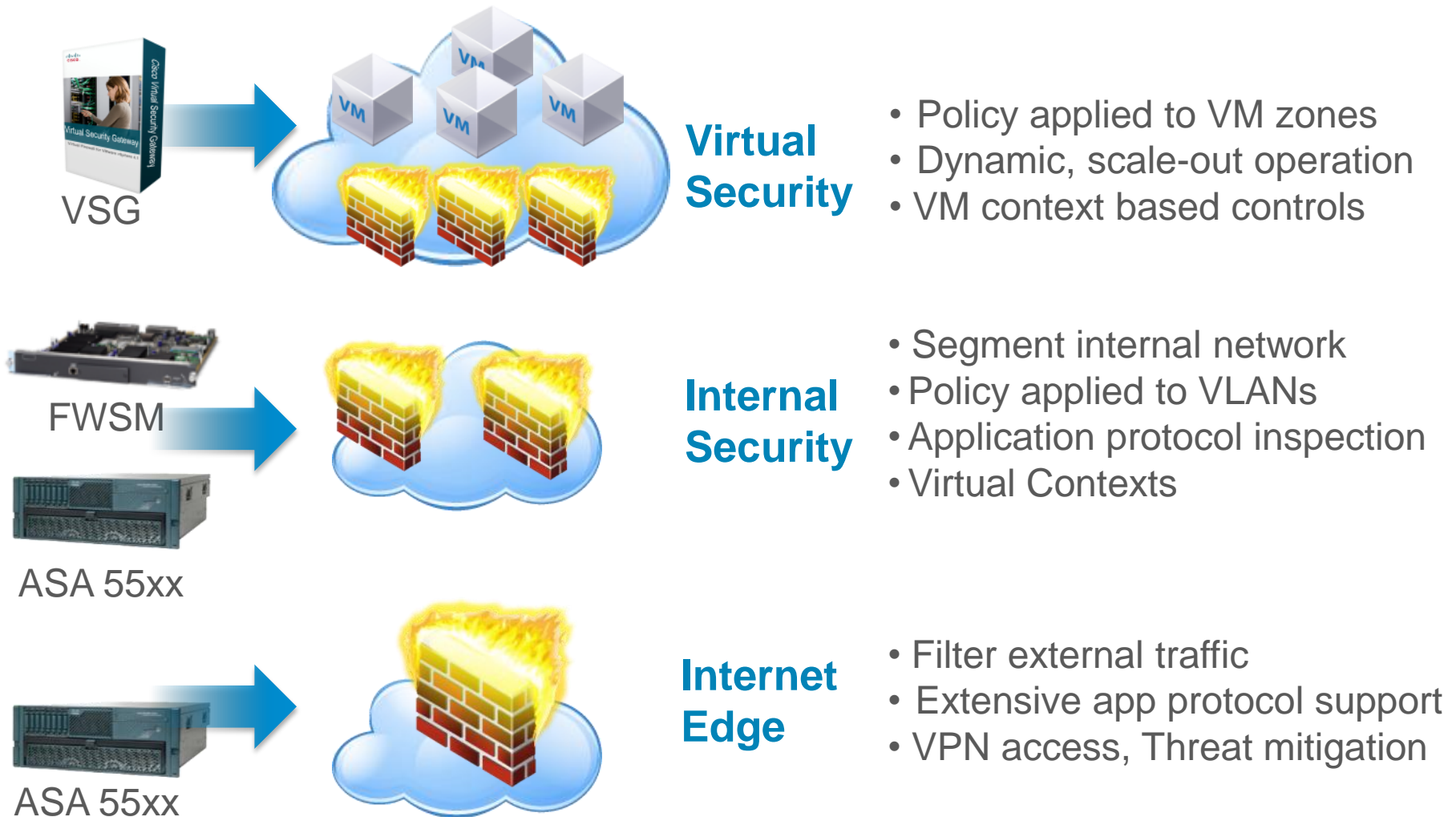
```
org root/Contrator
vn-service ip-address 192.168.173.42 vlan 20 security-profile SecureContractors
s
no shutdown
state enabled

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/Contrator
vn-service ip-address 192.168.173.42 vlan 20 security-profile SecureContractors
no shutdown
state enabled

N11#
```

Defense in Depth Security Model



Virtual Network Management Center (VNMC)

Simple yet powerful virtual security management

Virtual Network Management Center

Scalable

Multi Tenant

Different Customers, different needs

Stateless

Security Profiles

Simple, policy based security config

Expandable

XML API

3rd party integration ready

Partitionable

Integrated

Role Based Access Controls

Different users, different privileges

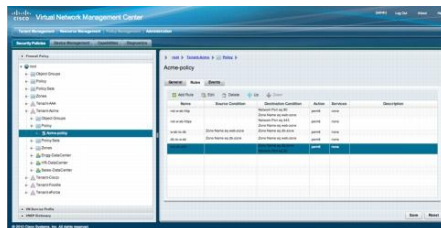
Automated

Nexus 1000V & vCenter

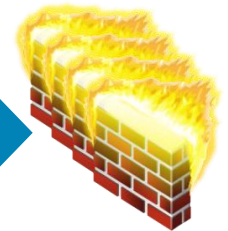
Port profiles refer to security profiles

Dynamic provisioning

One stop configuration of network & security

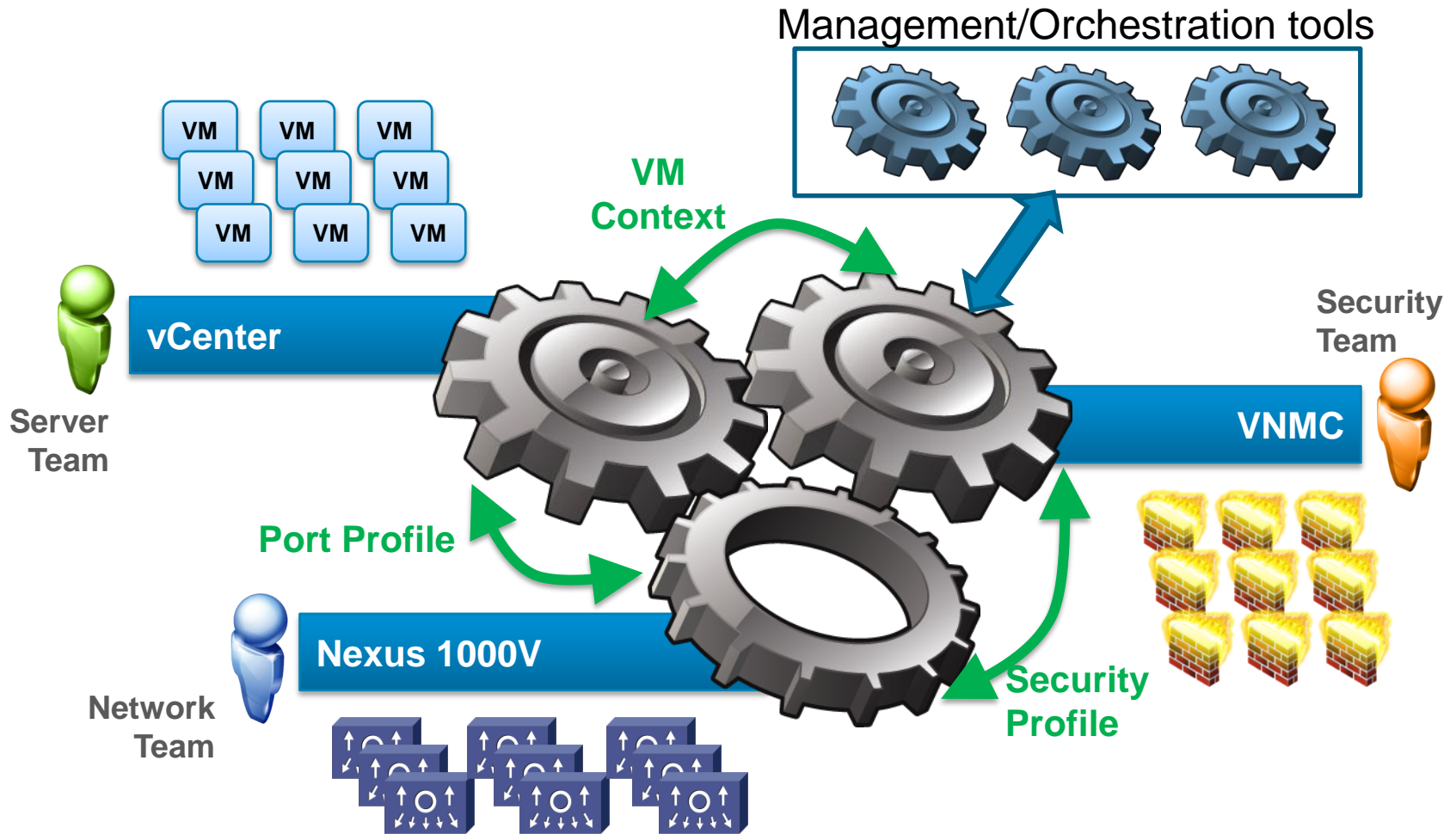


VNMC GUI



Virtual Security Gateway

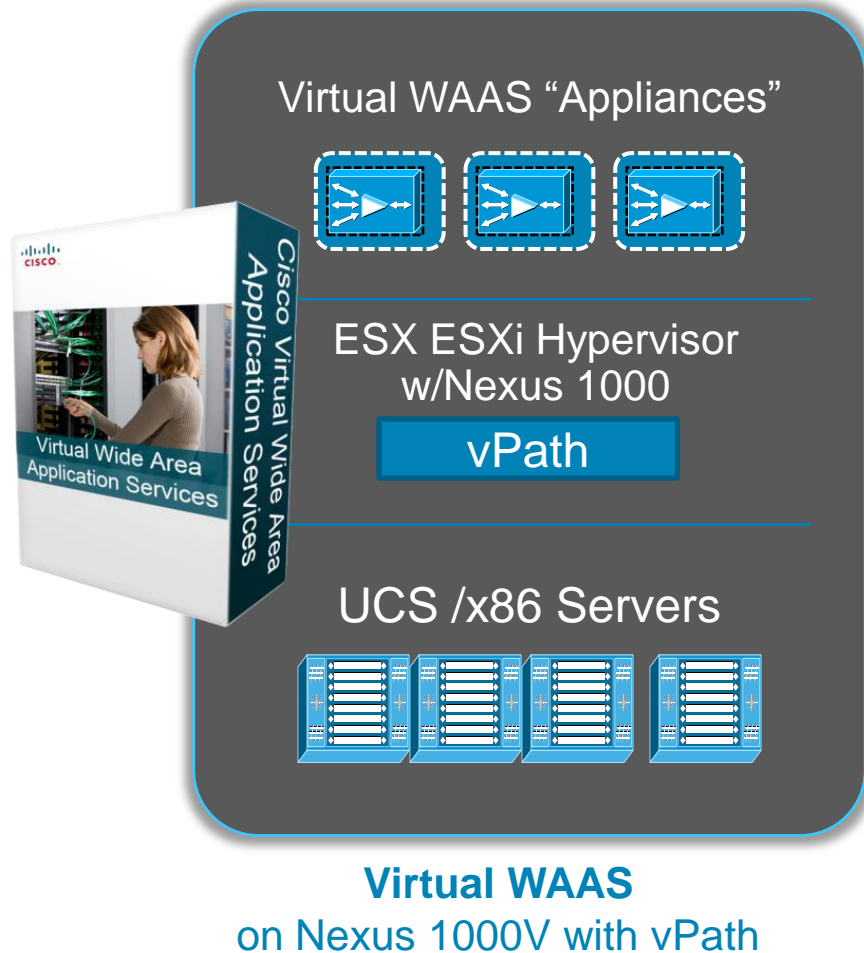
VNMC – Architected for Integrated & Automated Management



Virtual WAAS

Introducing: Cisco Virtual WAAS

Cloud-ready WAN Optimization



FEATURES

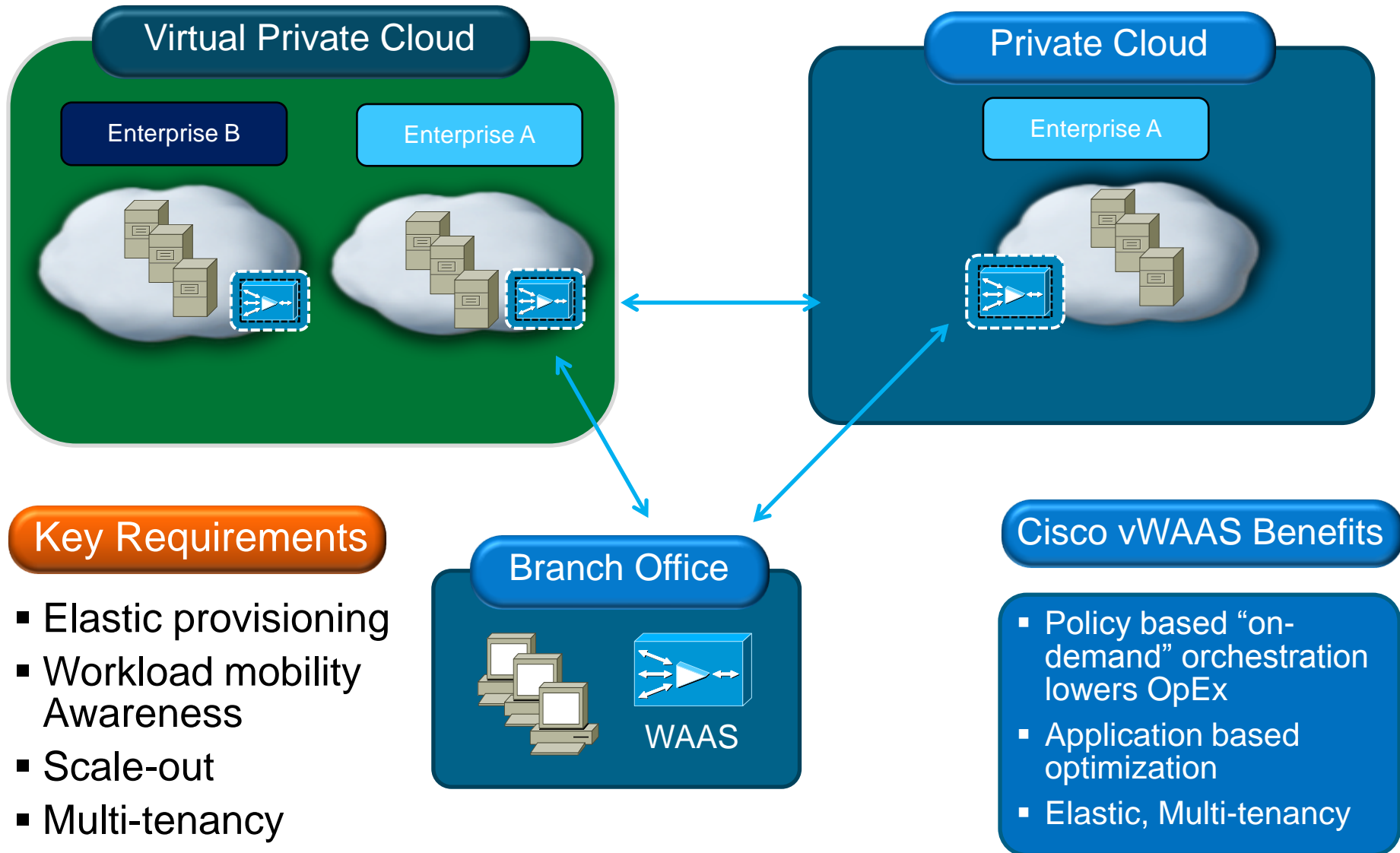
- Allows Agile, Elastic, & Multi Tenant Deployment
- Supports DRE Cache in SAN
- Policy-based Provisioning w/ Nexus 1000V
- Extends WAAS Solution Portfolio

BUSINESS BENEFITS

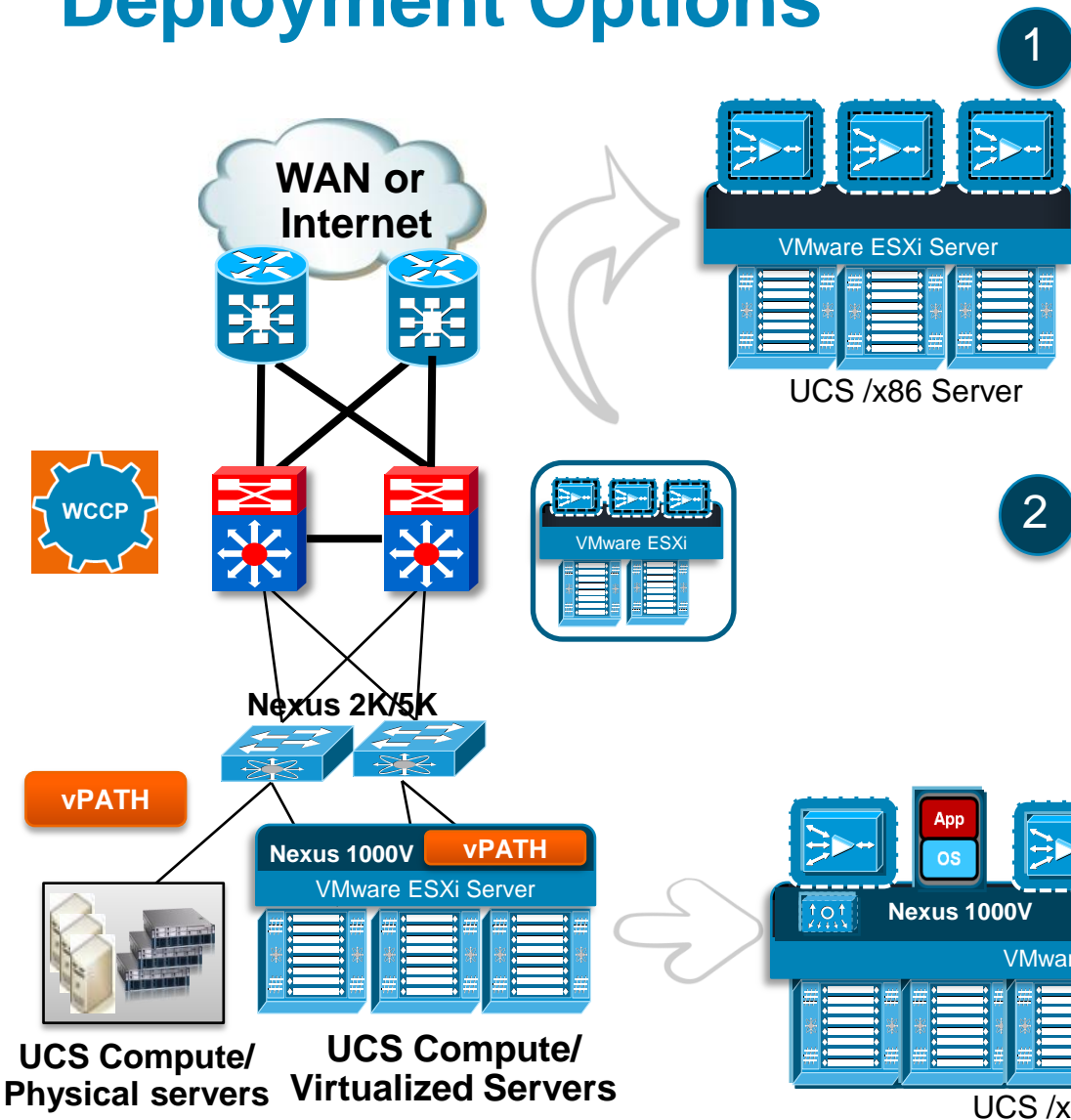
- Business Agility with on-demand orchestration
- Lower operational cost, reduced migration risk
- Fault-tolerance with VM mobility awareness

Cisco vWAAS Accelerates Cloud Deployment

Accelerate cloud-bursting, workload mobility, virtualized deployment



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

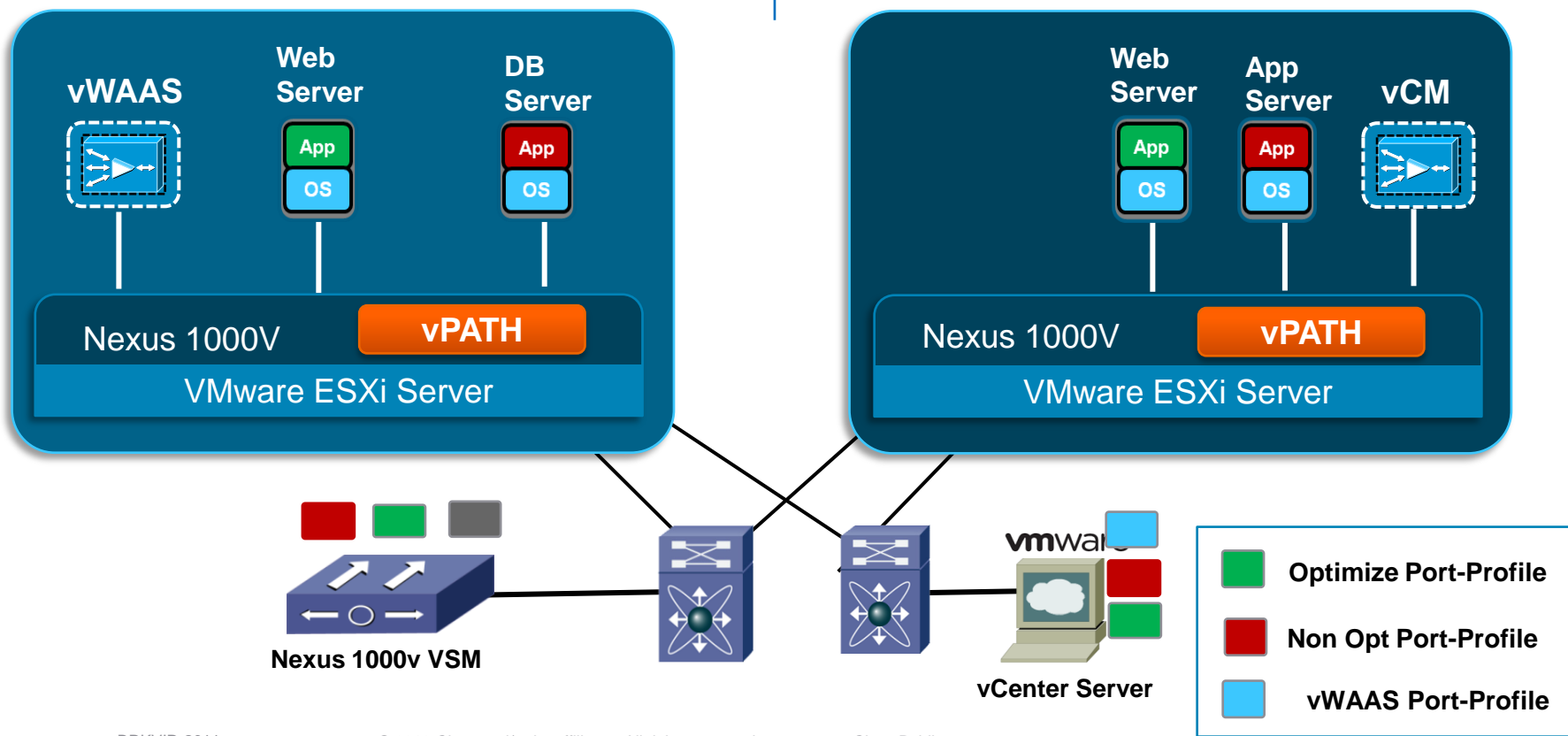
vWAAS – Policy Based configuration in N1000V

Feature

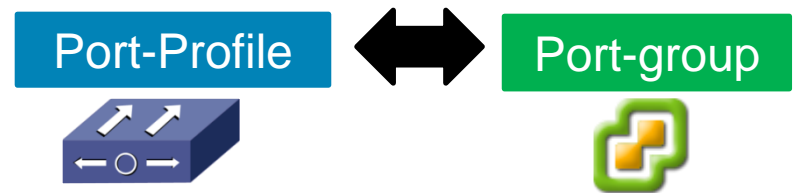
1. Optimization based on the port-profile policy configured in Nexus 1000V
2. Policy gets propagated to vCenter automatically

Benefit

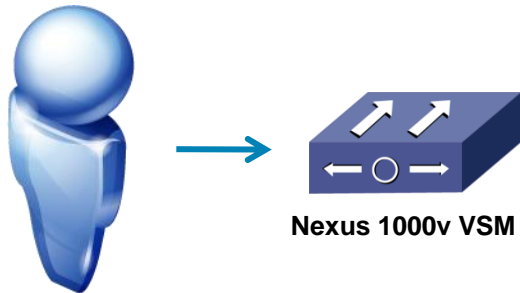
1. Provide on-demand service orchestration in the cloud without network disruption



vWAAS – Application based interception



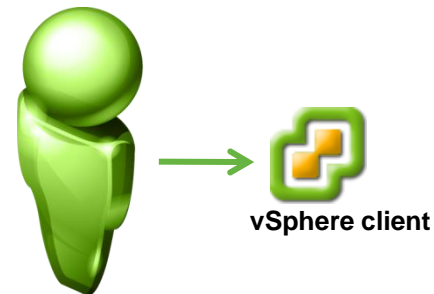
Network Admin view



```
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



Network adapter 1	VM-Data (N1Kv-VPC), ...
SCSI controller 0	LSI Logic SAS
Hard disk 1	Virtual Disk

Attach Opt-port-profile to server VMs

- VM-Data (N1Kv-VPC)
- n1kv-system-management (N1Kv-VPC)
- n1kv-system-packet (N1Kv-VPC)
- vWAAS-Network (N1Kv-VPC)
- iSCSI (N1Kv-VPC)
- VM-Data (N1Kv-VPC)
- Service-Console (N1Kv-VPC)
- Exchange-Server (N1Kv-VPC)
- Opt-Exchange-Server (N1Kv-VPC)

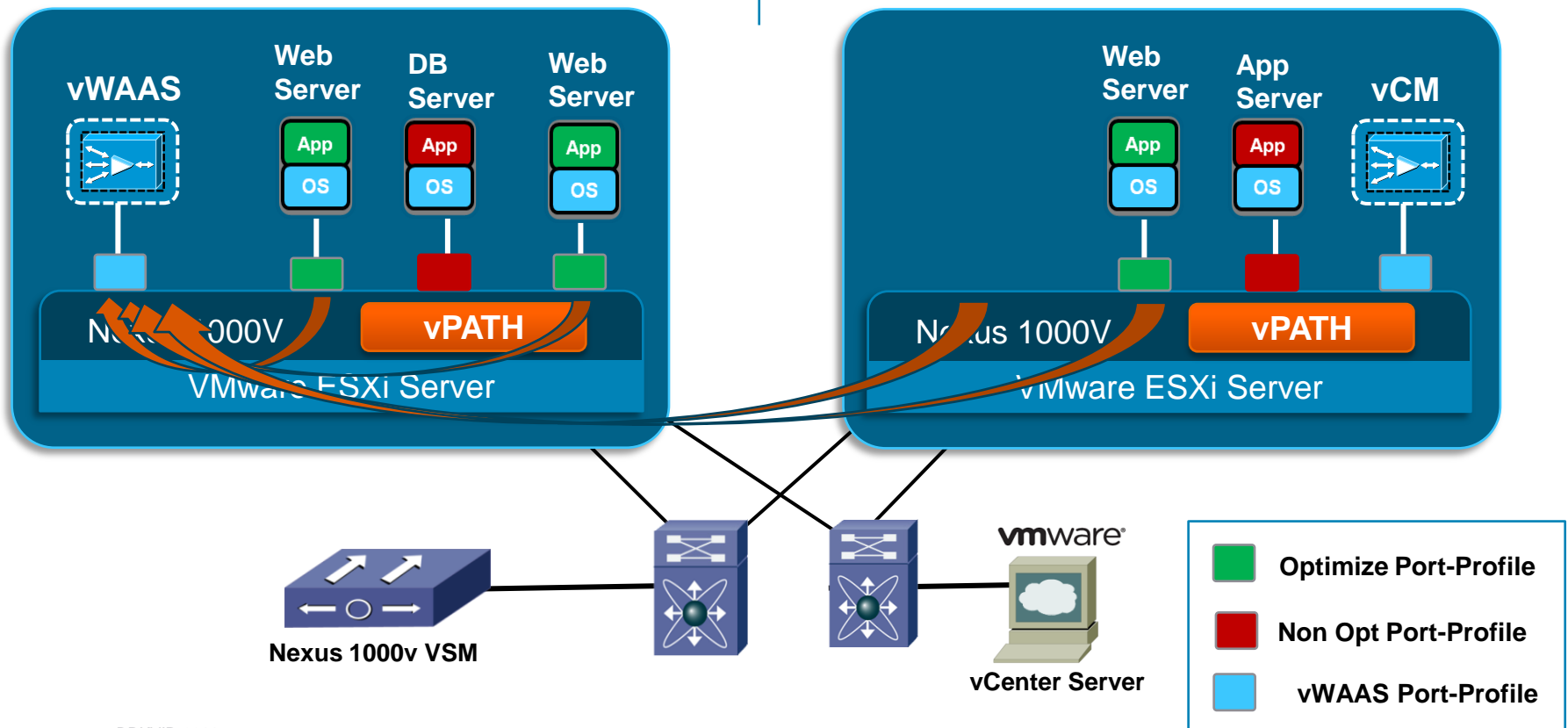
vWAAS – VM mobility awareness

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 optimization service if VM moves from one host to another.
2. Support VMware resources scheduling (DRS) and provides High availability



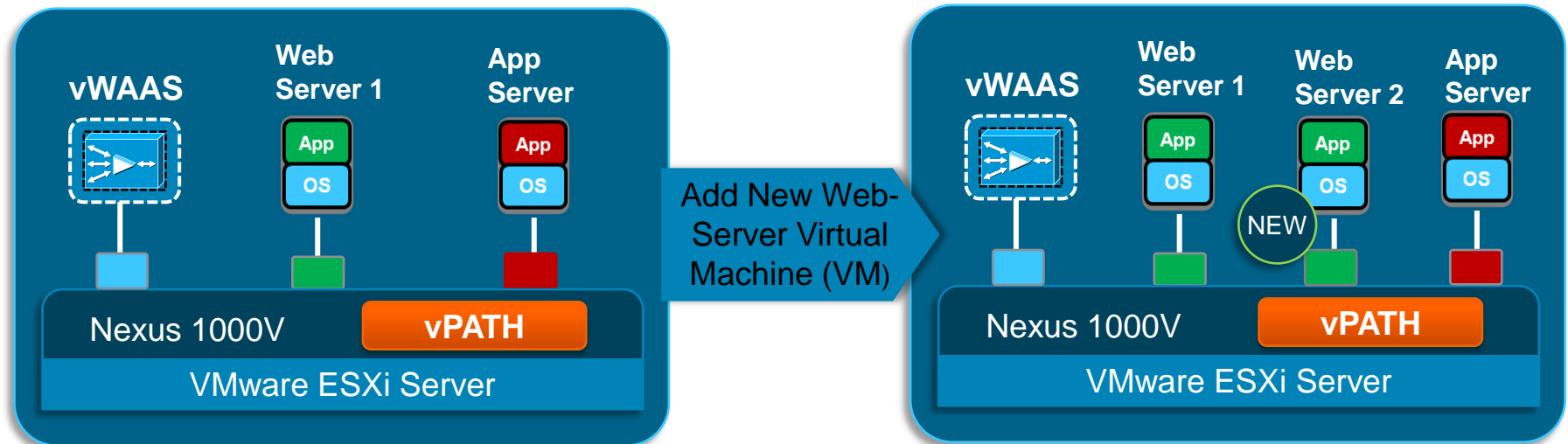
vWAAS – Architected for Elastic Workloads

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 optimization



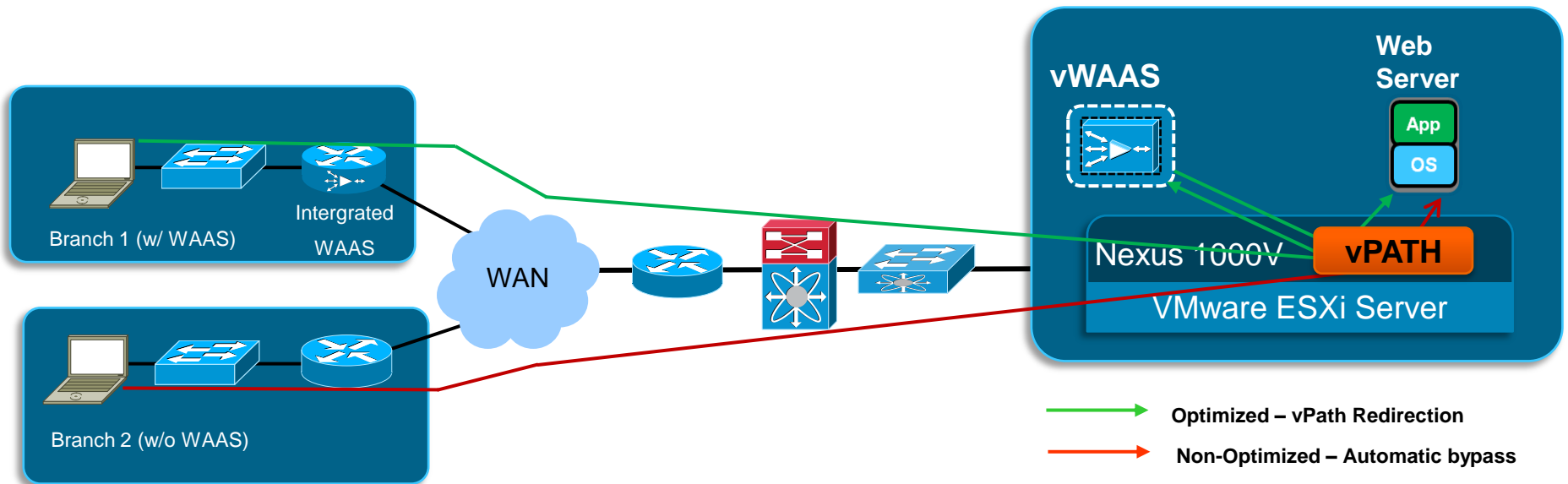
vWAAS – Optimized performance with vPath

Feature

1. vWAAS send “offload” to vPATH for non-interesting 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



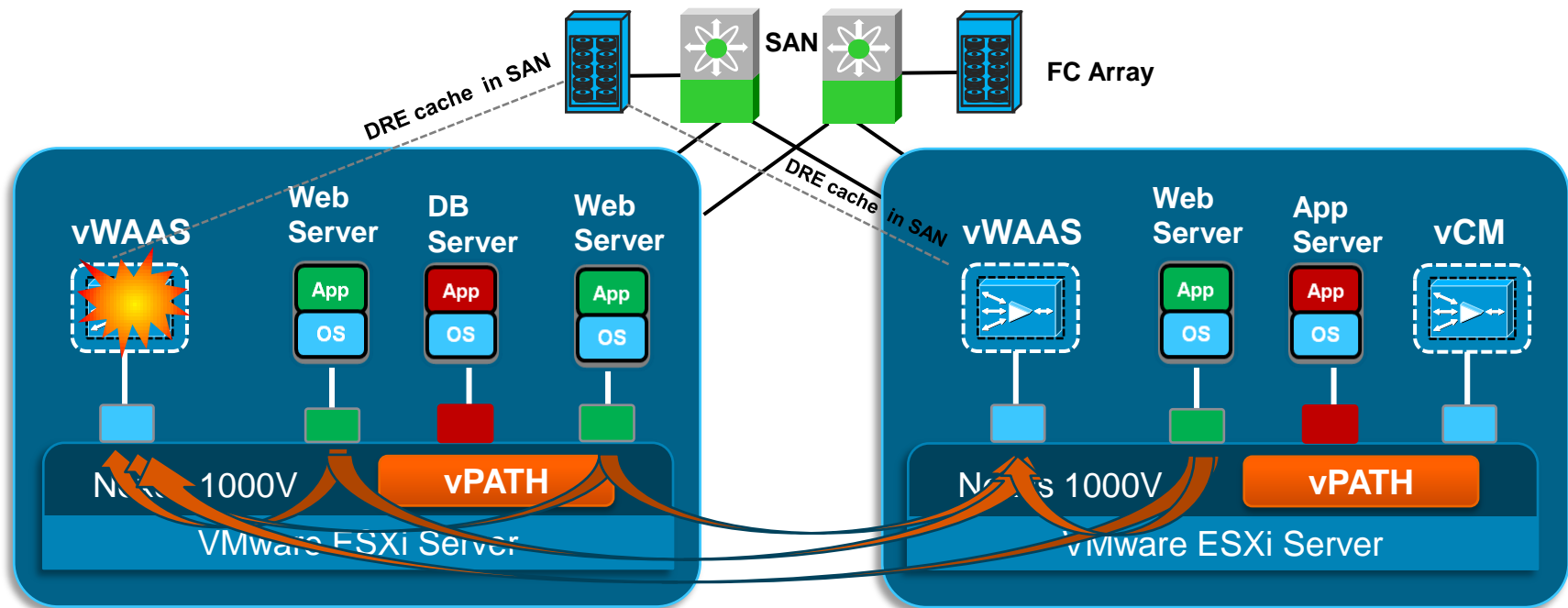
vWAAS – Fault tolerant persistent performance

Feature

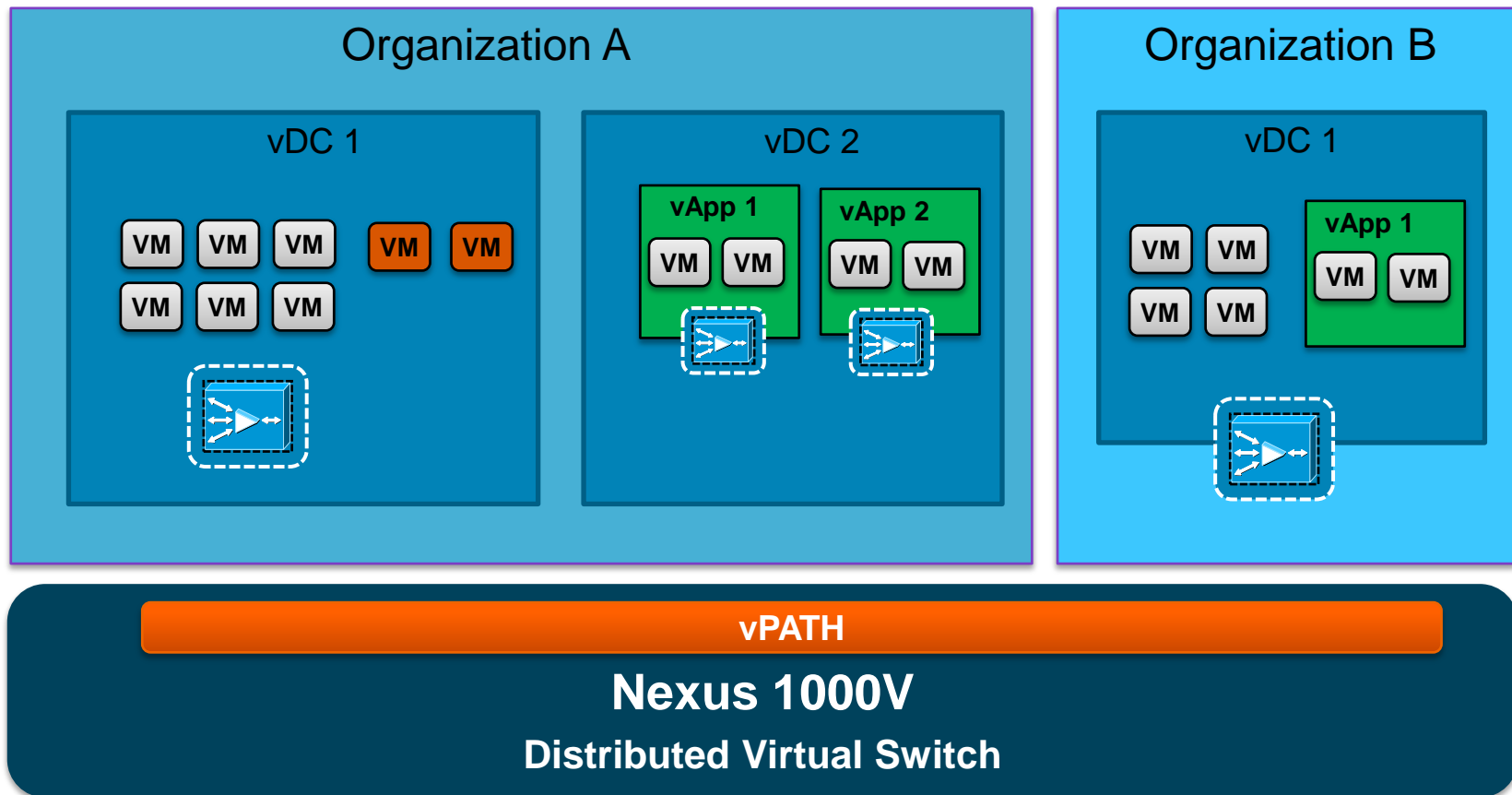
1. vWAAS DRE cache can be deployed in SAN
2. VMware HA creates new VM upon failure of vWAAS using same DRE cache storage.

Benefit

1. Ensures cache preservation and high persistent performance in the event of failure
2. Provide uninterrupted compression benefit of WAN optimization



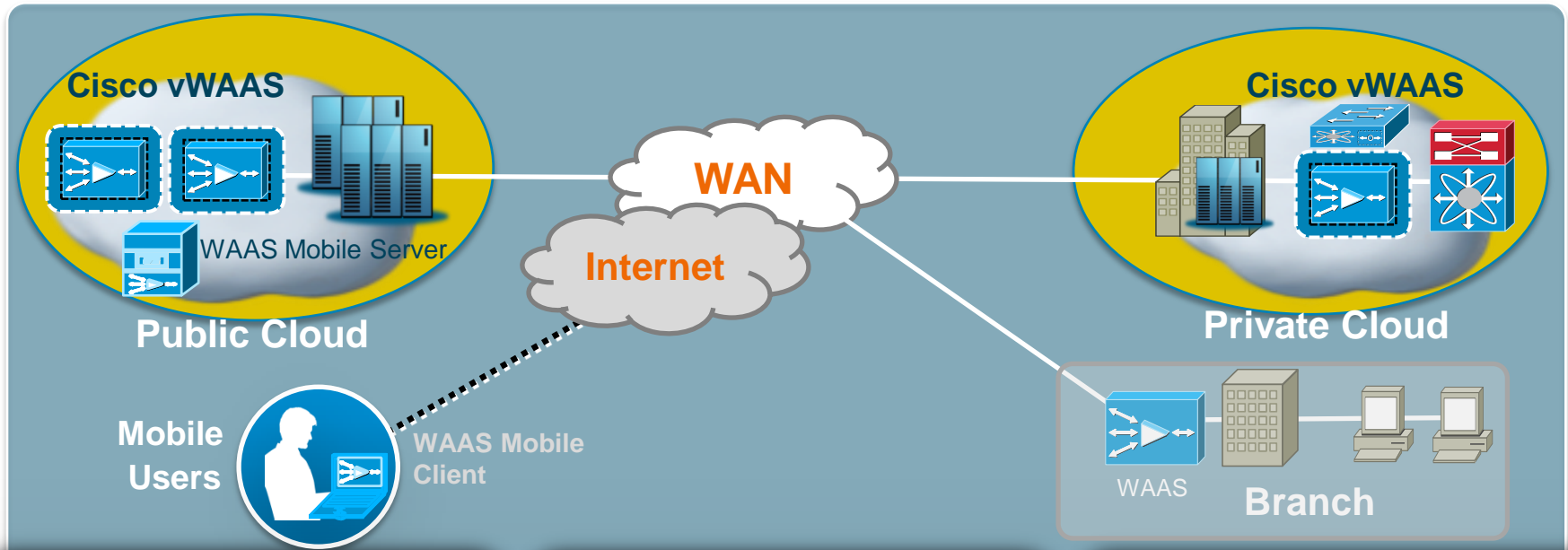
vWAAS – Multi-tenancy with flexible deployment



Cisco vWAAS can be deployed at:

- Organization level, vDC level, vApp level

Cisco vWAAS: Cloud Ready WAN Optimization



Key Requirements

- On demand deployment with elastic scalability
- Minimal network configuration
- VM mobility awareness
- Multi-tenant deployment

Benefits

- On-demand orchestration of WAN optimization
- Fault tolerance with VM mobility awareness
- Lower OPEX for Cloud Migration

Simplification

- Close Integration with Cisco Nexus 1000V
- Rapid creation of WAN Optimization Service
- Transparent deployment w/ WCCP

Concluding Remarks

- Virtual Services needs to be deployed with an architectural mind-set
 - Virtual Data Center, Private Cloud, Public Cloud
- Network intelligence for virtual services is critical for:
 - Simplified deployment
 - Optimized performance
 - Virtualization-aware operation
- Separation of duties and operational non-disruptiveness needs to be maintained

Cisco VSG and vWAAS with Nexus 1000V/vPath provide an excellent platform for building out virtual networking and virtual services infrastructure in data center and cloud computing environments



For Your
Reference

Other Related Sessions

At Cisco Live 2011

- BRKVIR-2931 End-to-End Data Center Virtualization.
- BRKVIR-2006 Deployment of VN-Link with the N1KV.
- BRKVIR-2008 UCS and Nexus1000V Virtualization for Cloud DC Services
- BRKSEC-2205: Security in the Data Center
- LABDCT-1901 Introduction to Nexus 1000V Hands-on Lab

Please complete your Session Survey

- We value your feedback - don't forget to complete your online session evaluations after each session. Complete 4 session evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Networkers 20th Anniversary t-shirt.
- All surveys can be found on our onsite portal and mobile website: www.ciscoliveeurope.com/connect/mobi/login.ww
- You can also access our mobile site and complete your evaluation from your mobile phone:
 1. Scan the Access Code
(See <http://tinyurl.com/qrmelist> for software, alternatively type in the access URL)
 2. Login
 3. Complete and Submit the evaluation





CISCO