

Cisco Virtual Security Gateway

Joe Dillon

Product Manager, Server Access & Virtualization



Nexus 1000V Public Webinar Series

Date	Business Sessions
22-Mar	Nexus 1000V Family Overview and Update
5-Apr	Virtual Network Services (vPath, NAM, vWAAS)
19-Apr	Virtual Security Gateway Introduction
3-May	Journey to the Cloud w/ N1KV: vCloud Director & Long Distance vMotion
17-May	Secure VDI with Nexus1000V & VSG

Date	Technical Sessions
29-Mar	Nexus 1000V New Features and Installation Overview
12-Apr	Nexus1010 Installation & Upgrade
26-Apr	Virtual Security Gateway Installation and Basic Configuration
10-May	Nexus 1000V Advanced Configuration
24-May	Nexus 1000V Troubleshooting

Today's Agenda

- ***Vision***
- ***Virtual Switching***
 - Nexus 1000V*
 - Nexus 1010*
- ***Virtual Services and Security***
 - Virtual Security Gateway (VSG)*

Virtual Networking Vision

Accelerate Data Center Virtualization



Virtual Networking Vision

Accelerate Data Center Virtualization



Virtualized
Agile
Policy-Driven
Multitenant

Virtual Networking Vision

Accelerate Data Center Virtualization

Virtualized
Agile
Policy-Driven
Multitenant

Virtual Network Link (VN-Link)

Extend networking to virtualized environments:

- Hypervisor Switch (SW): **Nexus 1000V**—standard based, feature rich
- External switch (HW): **UCS 6100 + Cisco VIC** (pre-standard, IEEE 802.1Qbh)

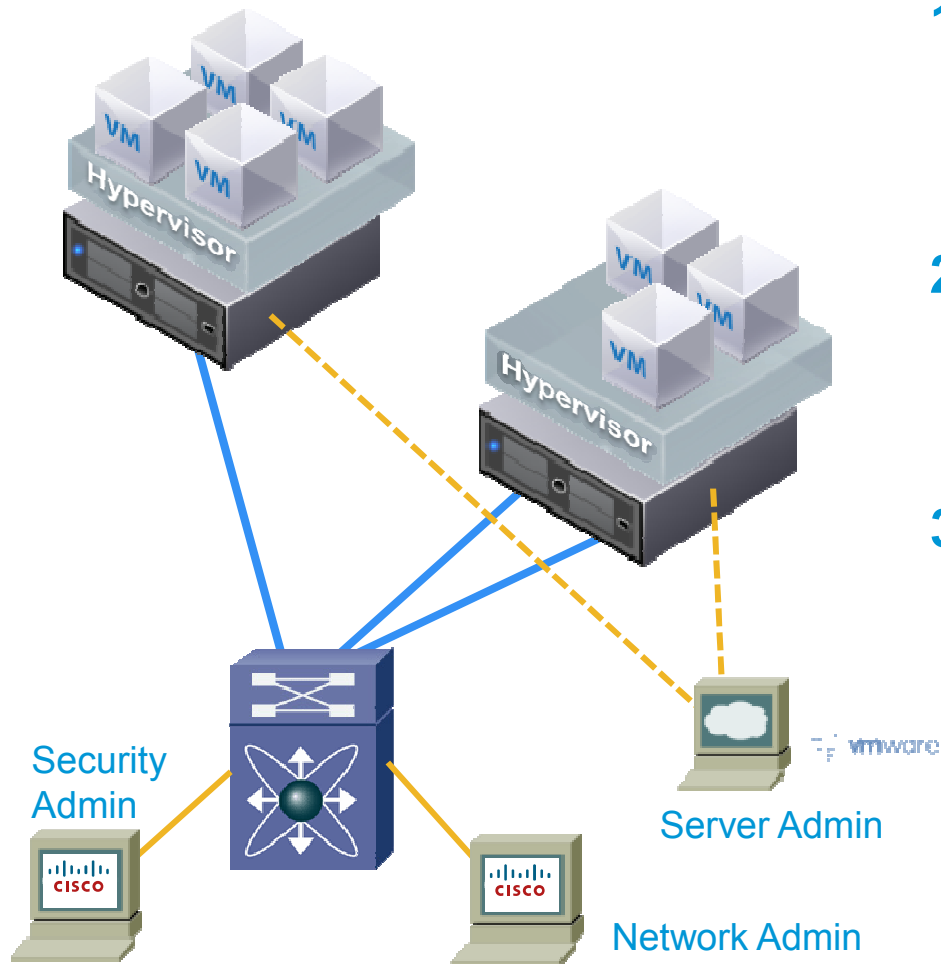
Virtual Network Services

Extend network services to virtualized environments

- **Virtual Service Node (VSN)** architecture
- Security service: **Virtual Security Gateway** for Nexus 1000V

Virtual Network Management (UCSM, VNMC)
Policy-Driven, Programmatic, Multi-Device, Multi-tenant

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

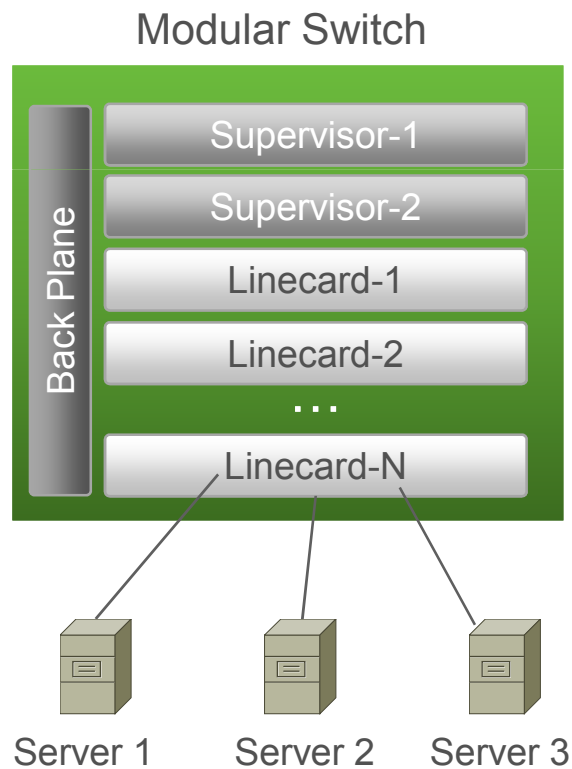


Nexus 1000V

NDA Presentation

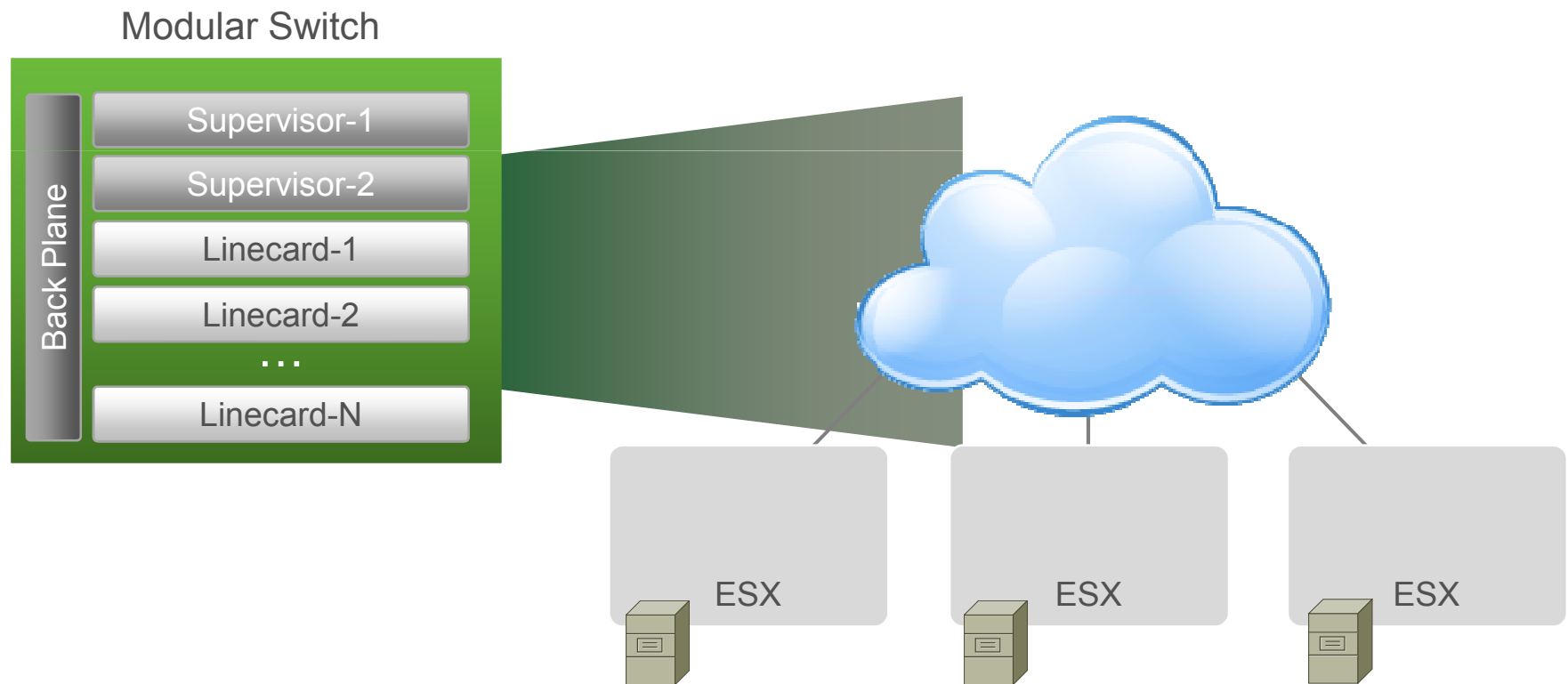
Nexus 1000V Architecture

Comparison to a Physical Switch



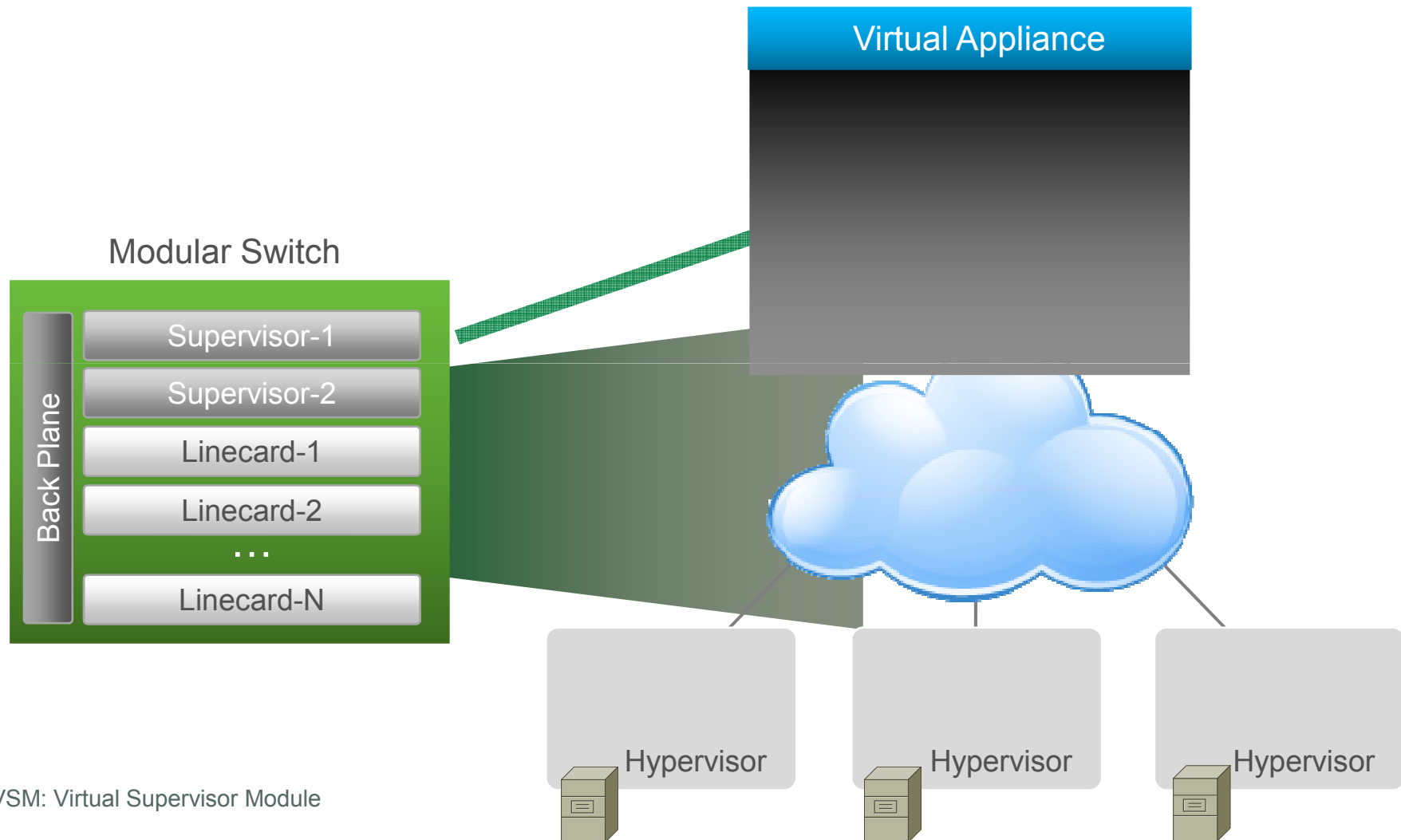
Nexus 1000V Architecture

Moving to a Virtual Environment



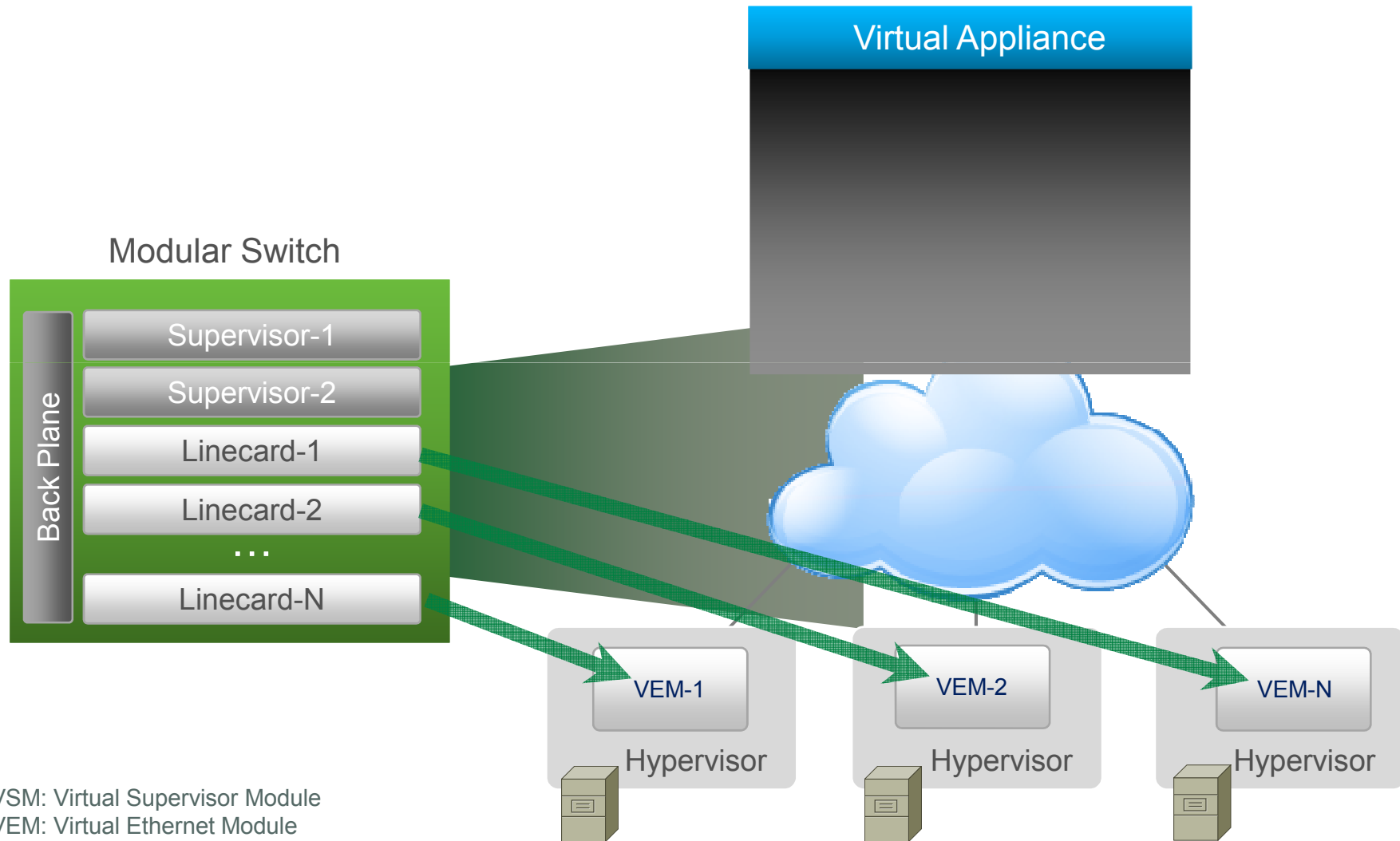
Nexus 1000 Architecture

Supervisors → Virtual Supervisor Modules (VSMs)



Nexus 1000 Architecture

Linecards → Virtual Ethernet Modules (VEMs)

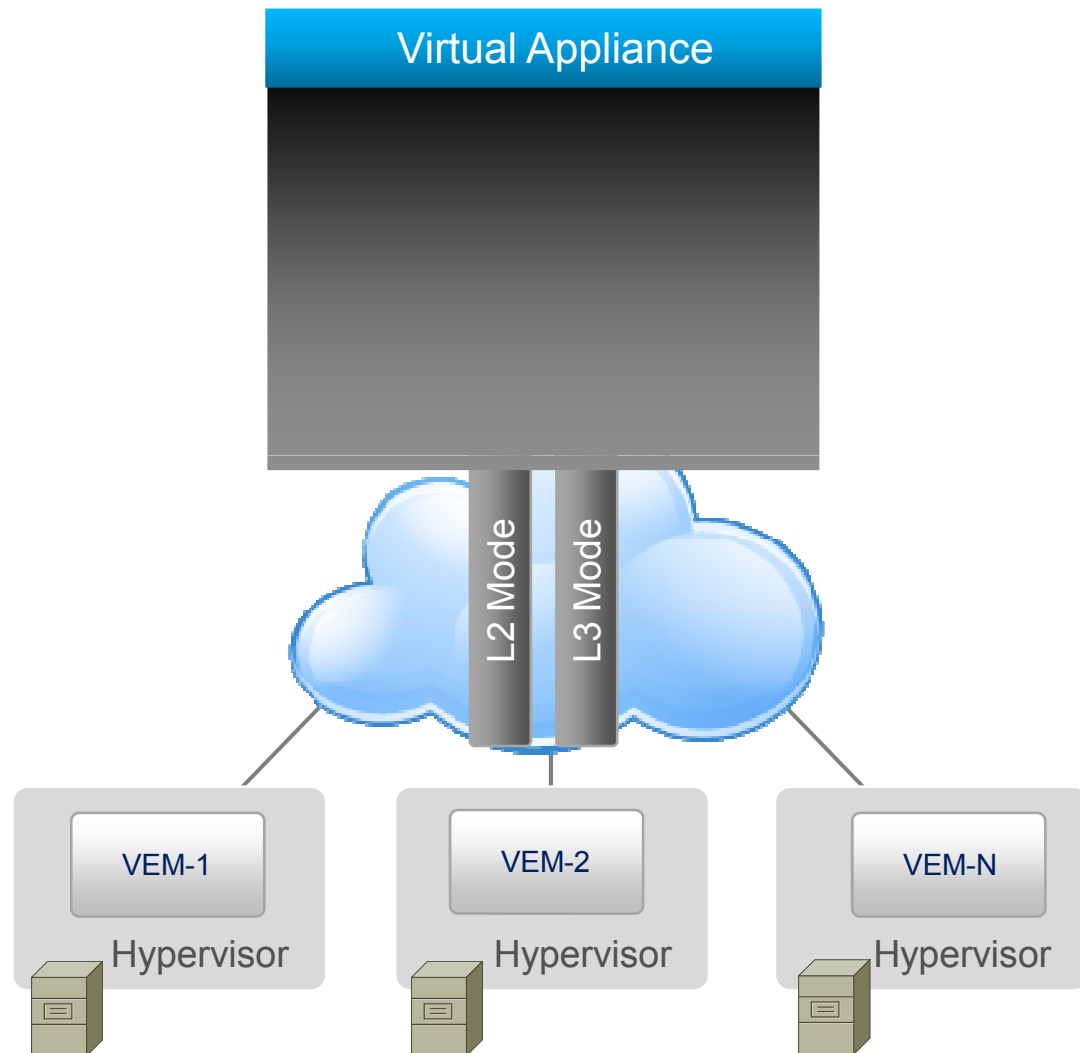


VSM: Virtual Supervisor Module
VEM: Virtual Ethernet Module

Nexus 1000 Architecture

VSM + VEMs = Nexus 1000 Virtual Chassis

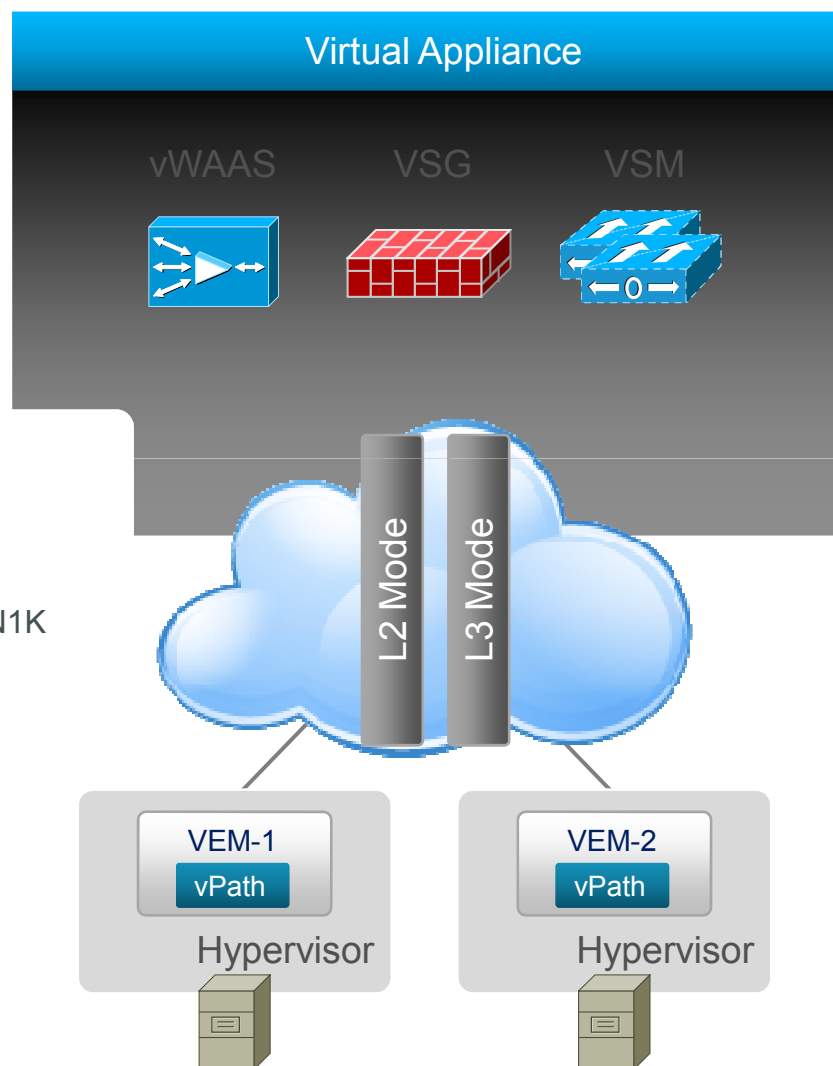
- 200+ vEth ports per VEM
- 2K vEths per N1K
- 64 VEMs per N1K (connected by L2 or L3)
- Multiple N1Ks can be created (under single hypervisor management center)



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 N1K

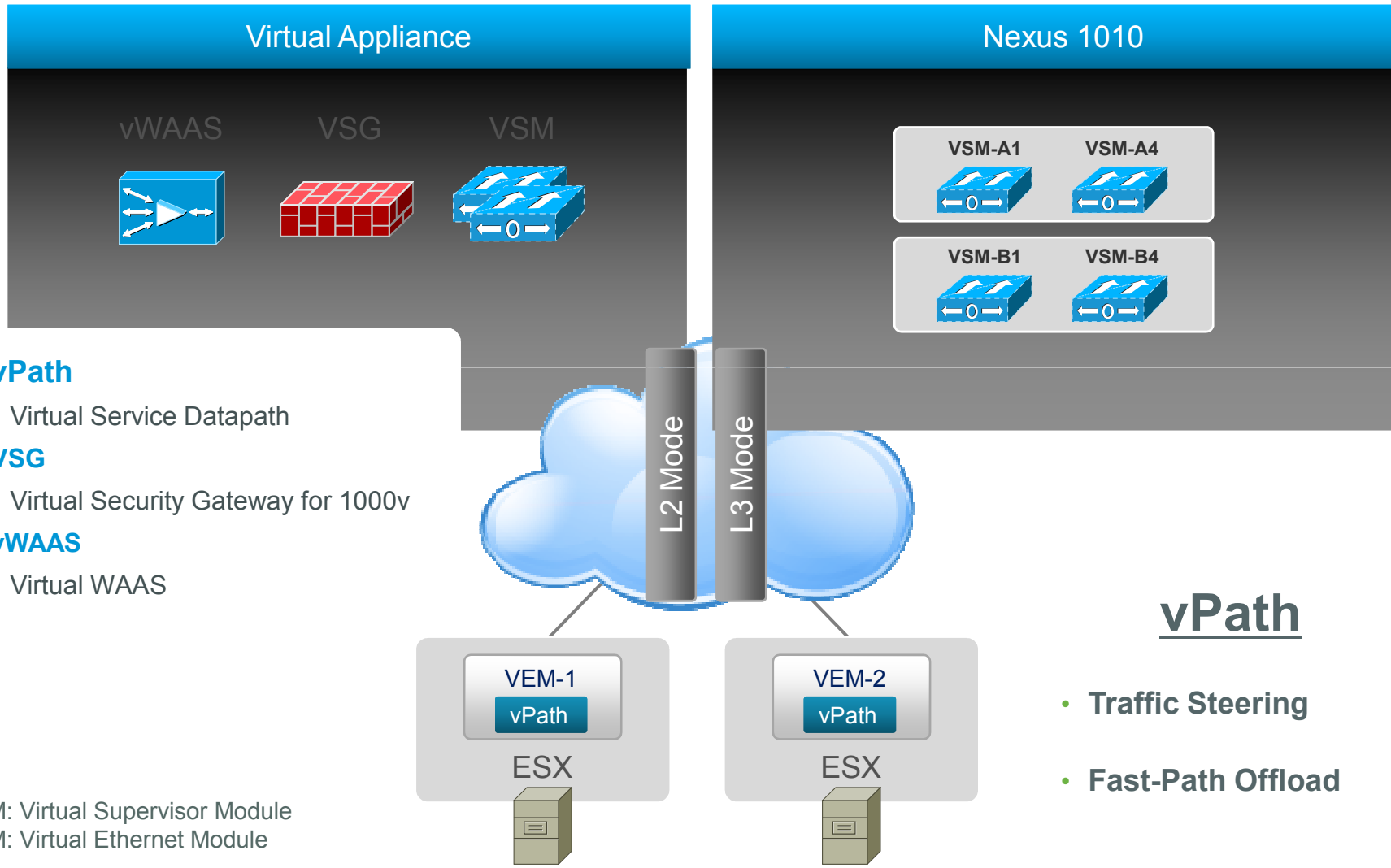
vWAAS

- Virtual WAAS

vPath

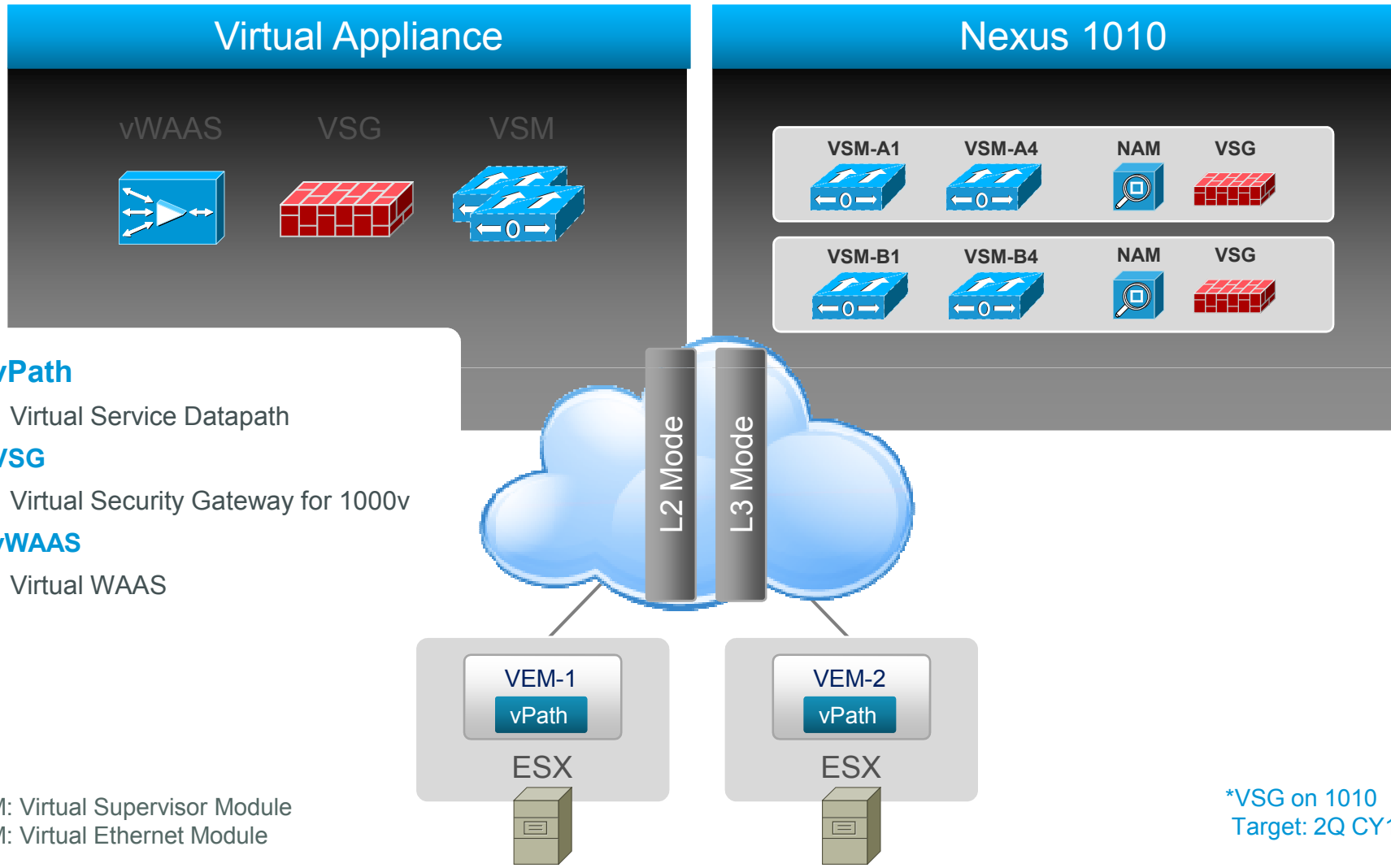
- Traffic Steering
- Fast-Path Offload

Nexus 1010 – Hosting Platform for VSM



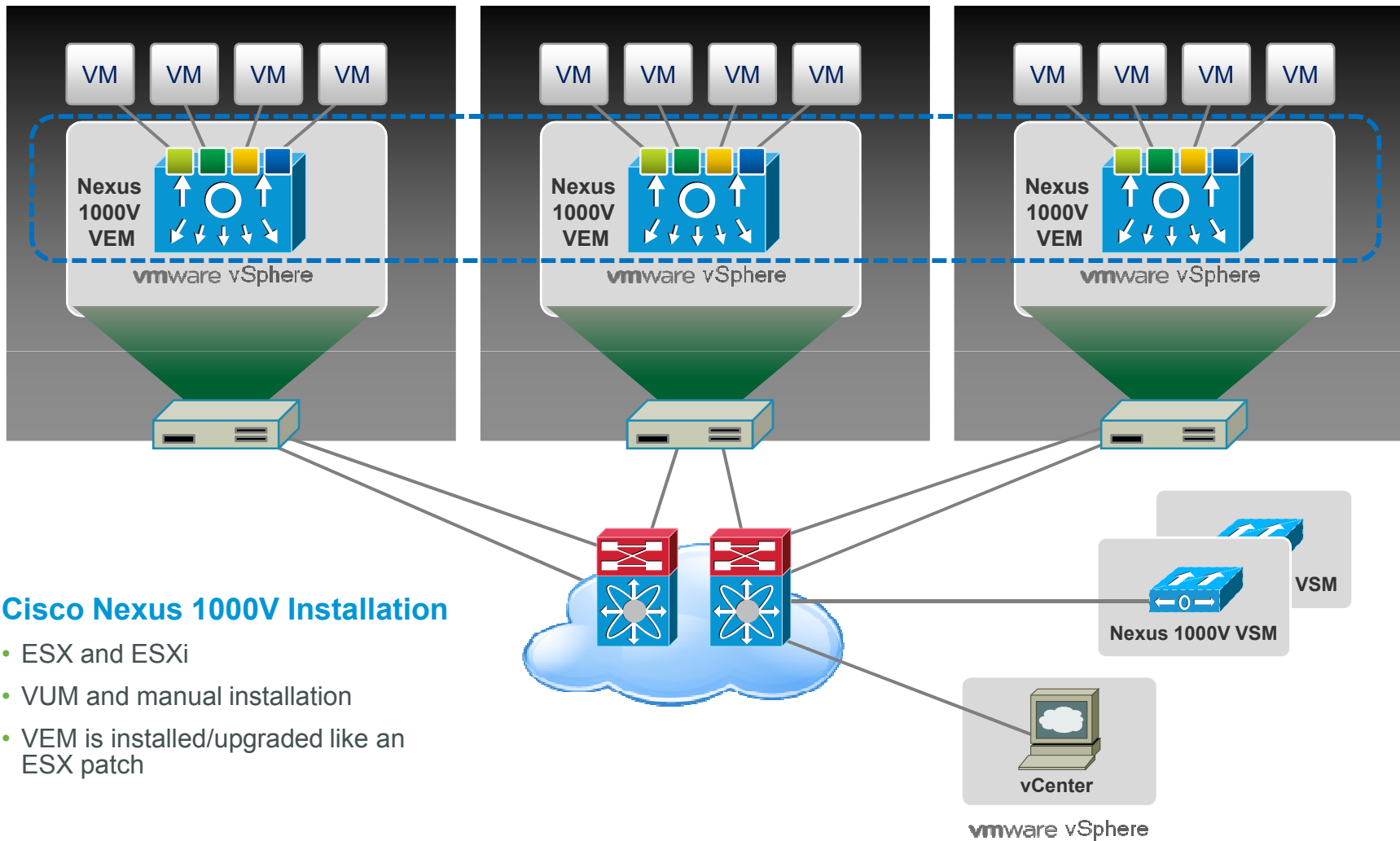
VSM: Virtual Supervisor Module
 VEM: Virtual Ethernet Module

Nexus 1010 – Hosting Platform for Services





Cisco Nexus 1000V Architecture



Cisco Nexus 1000V Installation

- ESX and ESXi
- VUM and manual installation
- VEM is installed/upgraded like an ESX patch





Cisco Nexus 1000V

Faster VM Deployment

Cisco VN-Link: Virtual Network Link

Policy-Based VM Connectivity

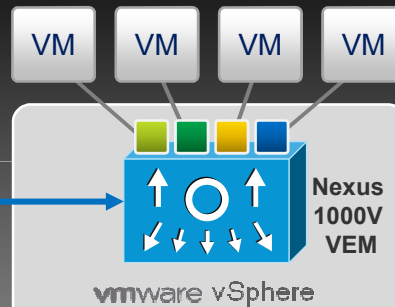
Defined Policies

WEB Apps	
HR	
DB	
DMZ	

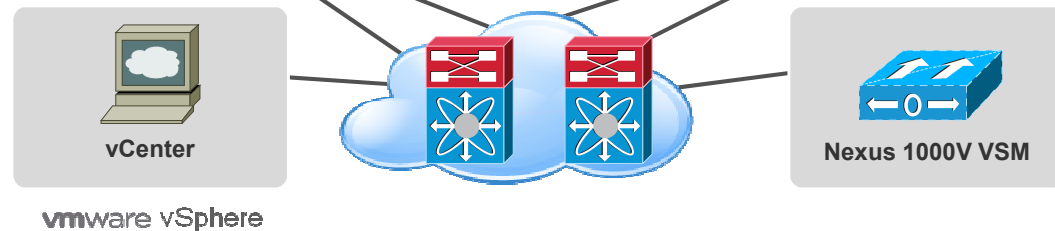
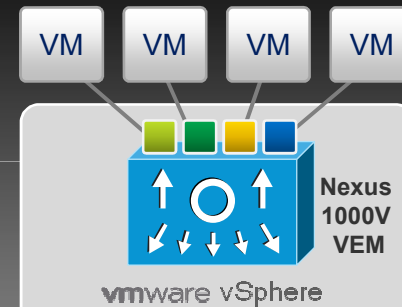
VM Connection Policy

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

Mobility of Network and Security Properties



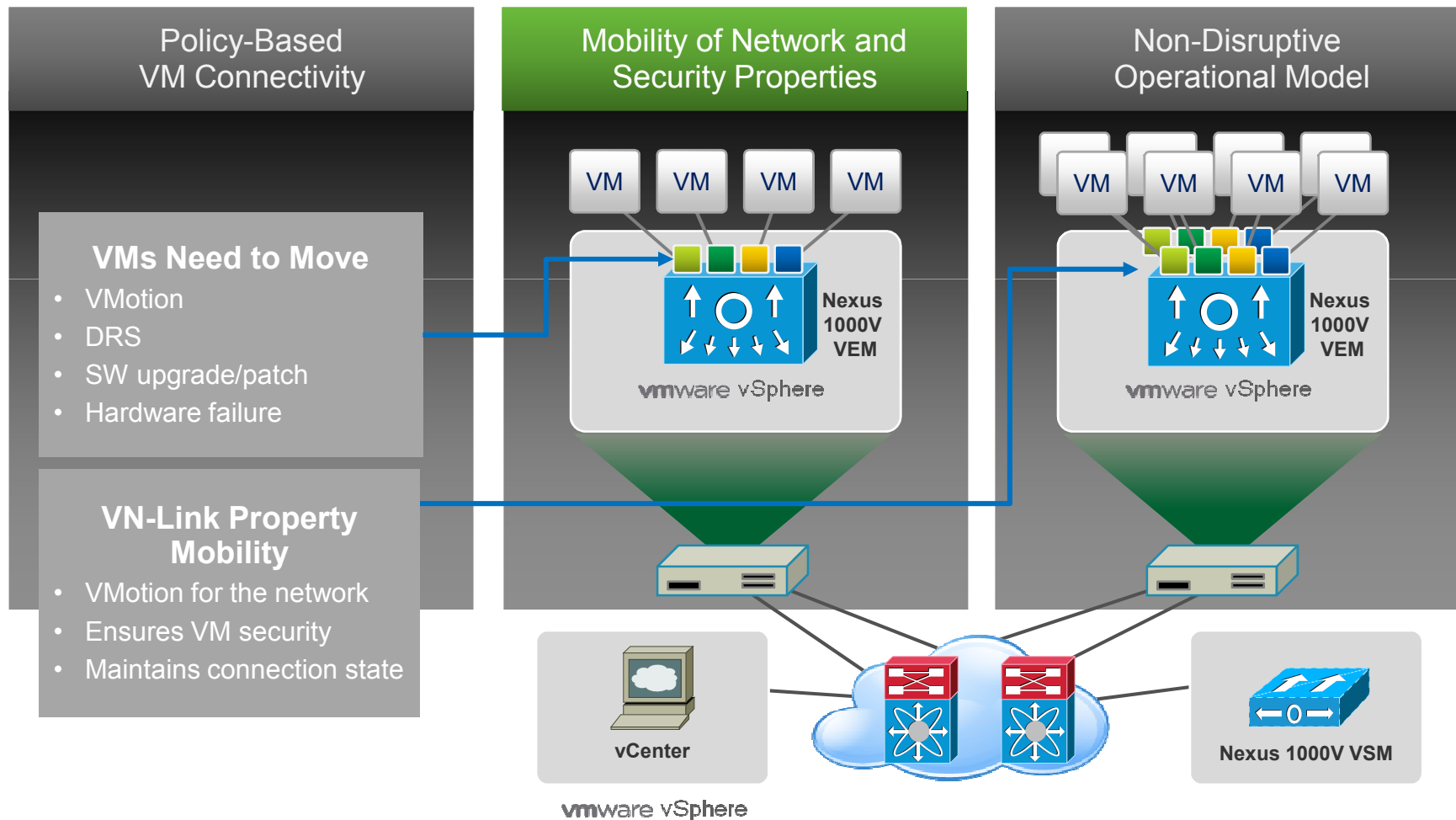
Non-Disruptive Operational Model



Cisco Nexus 1000V

Richer Network Services

Cisco VN-Link: Virtual Network Link



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

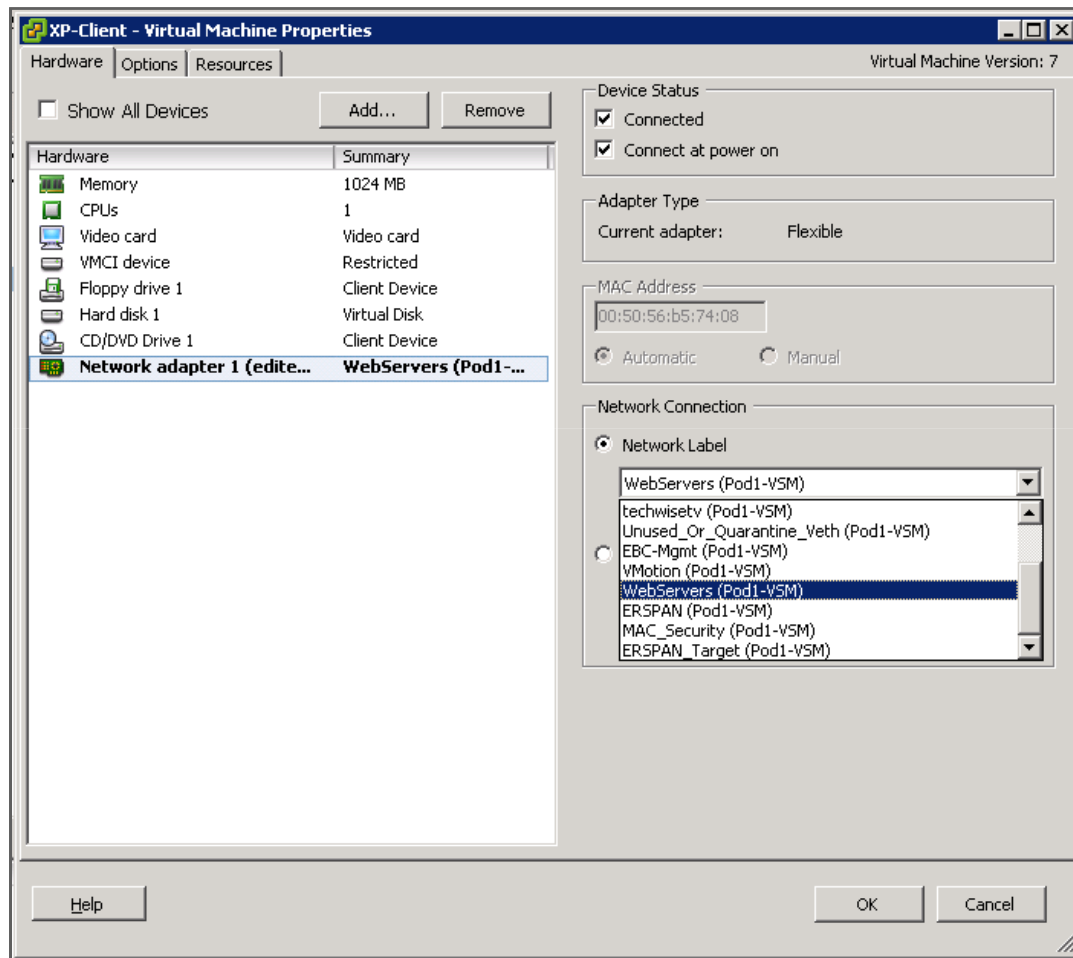
Port Profile Configuration

```
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
```

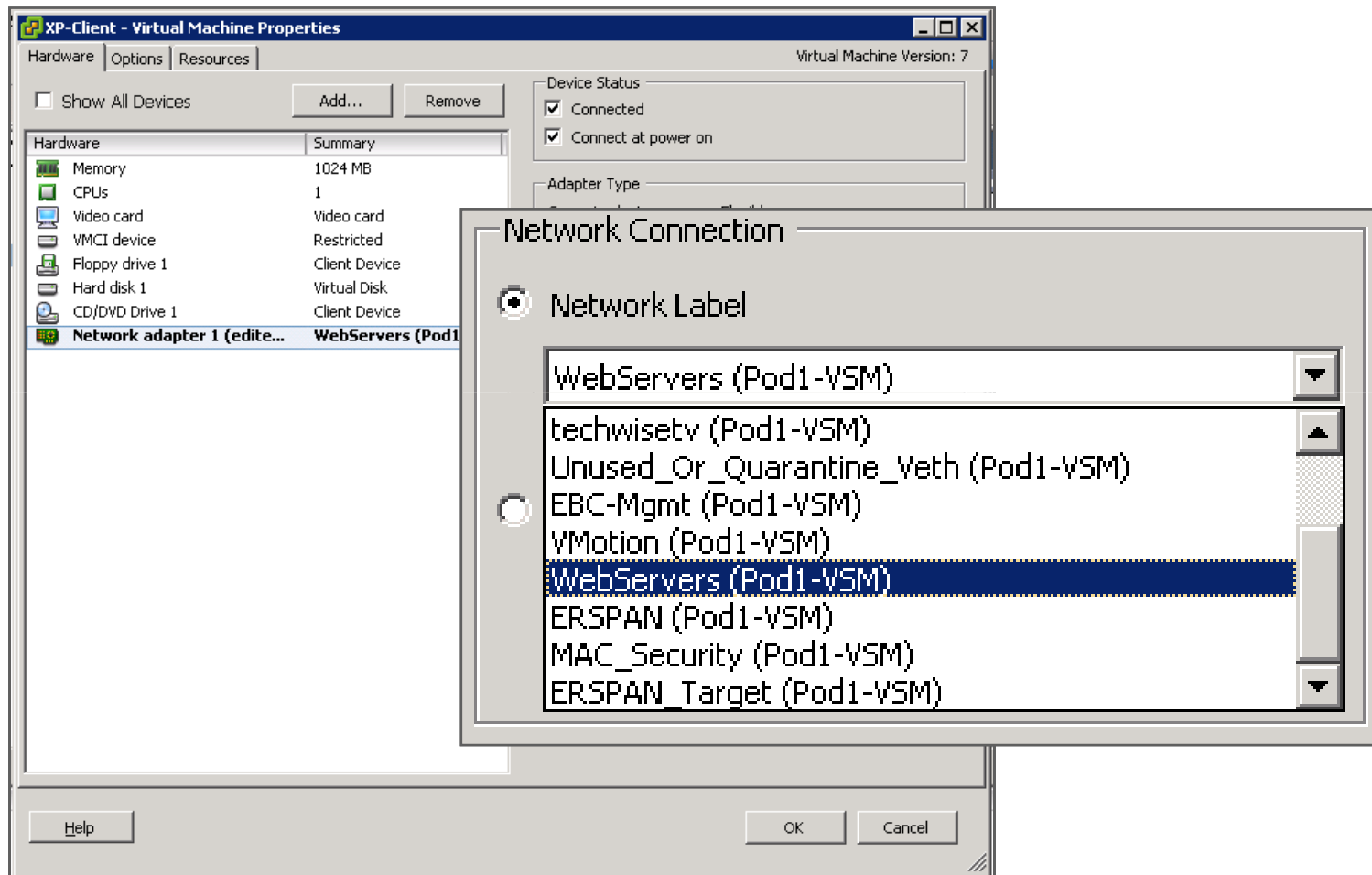
Support Commands Include:

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

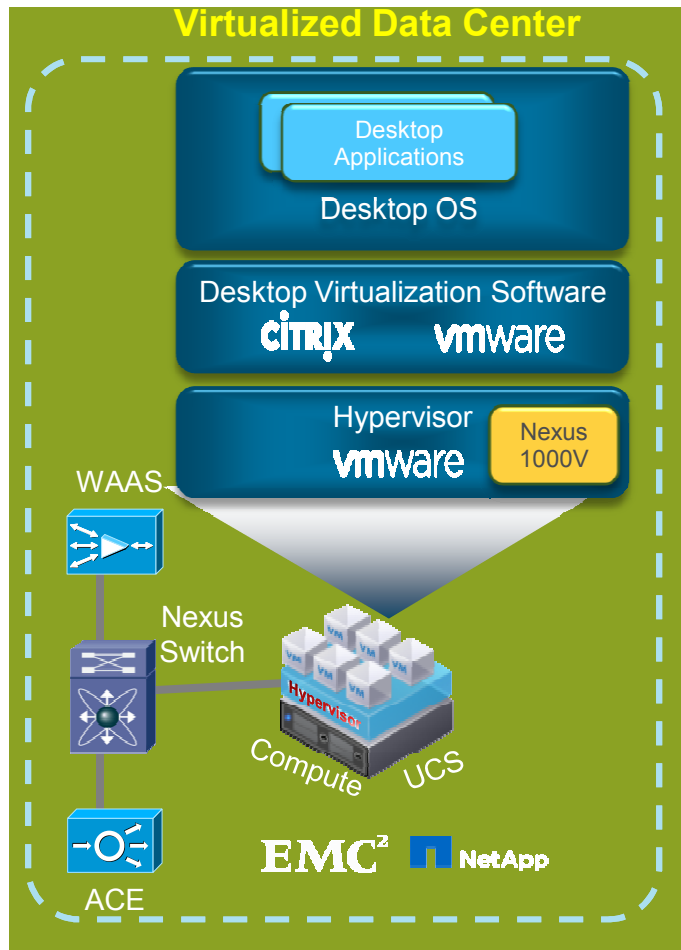
Port Groups: VI Admin View



Port Groups: VI Admin View



Securing Virtual Desktops (VDI)



WAAS: Wide Area Application Service
ACE: Application Control Engine

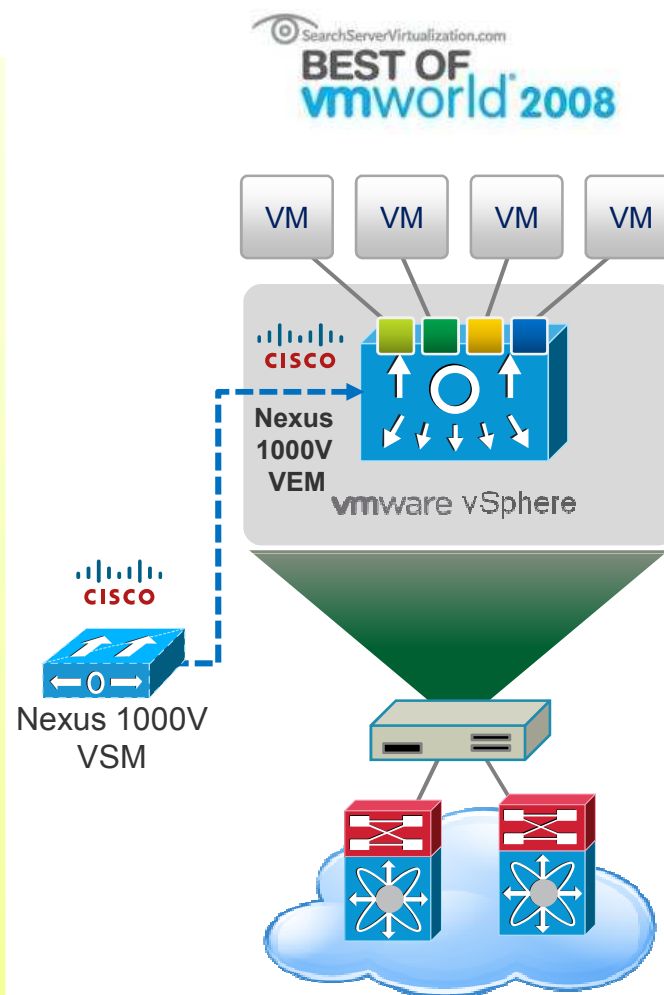
1000V Security Features for VDI

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

Cisco Nexus 1000V

Software-Based NX-OS switch

- Market Momentum
 - Introduced in 2009; now shipping Release 1.4
 - 3000+ customers world-wide
 - Over 1.5M virtual ports licensed
- Built on Cisco NX-OS
 - IEEE 802.1Q standards based
 - Network team manages virtual and physical networks
 - Feature and operational consistency
 - Advanced switching features
 - vPath intelligence for virtual network services
- Maximum compatibility
 - Interoperates with any upstream .1Q Ethernet switch
 - Deployable on all servers running VMware vSphere 4.x
 - Supports VMware HW Compatibility List (HCL)
 - Interoperates with VMware vCloud Director



Policy-Based
VM Connectivity

Mobility of Network and
Security Properties

Non-Disruptive
Operational Model

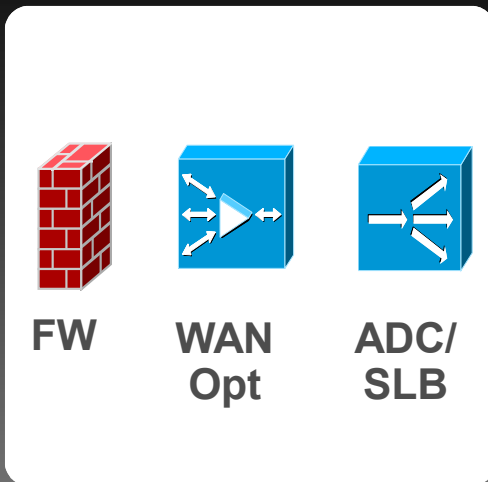


Virtual Security Gateway (VSG)



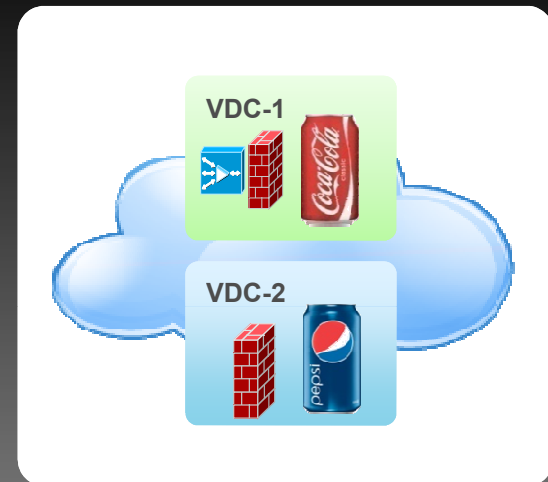
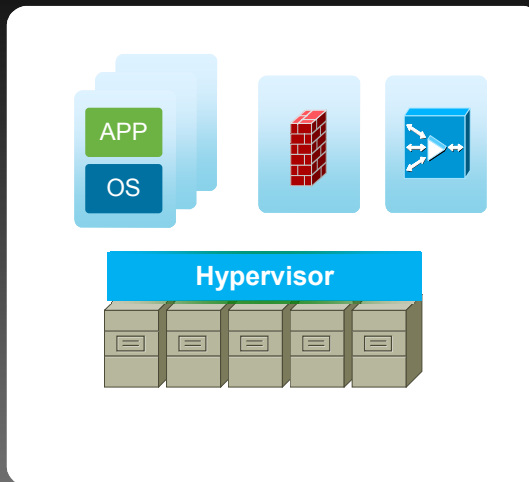
Virtualization and Cloud Driving New Requirements in Data Center

Traditional Data Center



- Application-specific services
- Form factors:
 - Appliance
 - Switch module

Virtual/Cloud Data Center



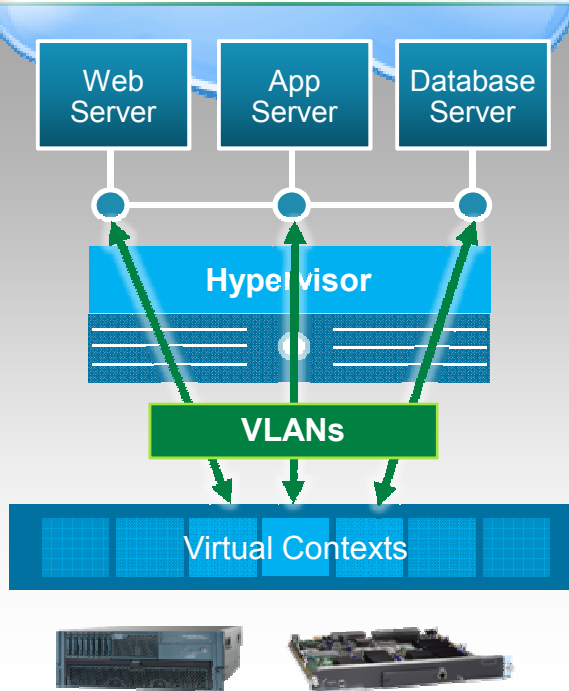
Virtual Service Node (VSN)

- Virtual appliance form factor
- Dynamic instantiation/provisioning
- Service transparent to VM mobility
- Support scale-out
- Large scale multitenant operation

Deployment Considerations in Virtualized/Cloud DC

1

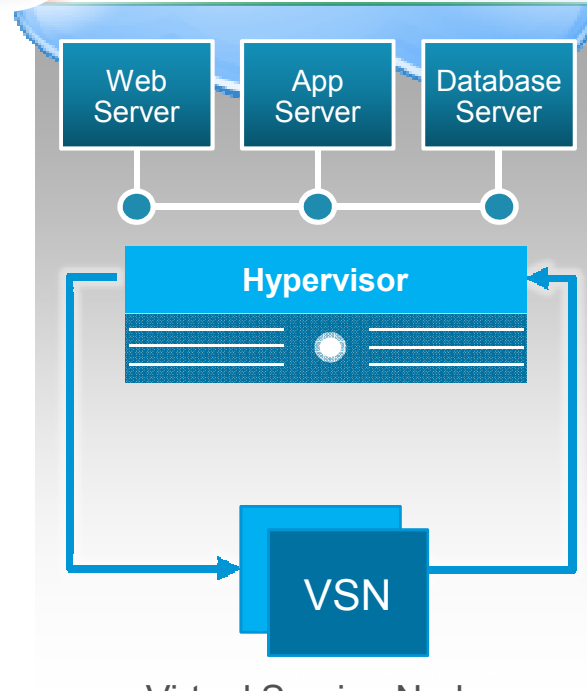
Redirect VM traffic via VLANs to external (physical) firewall



Traditional Service Nodes

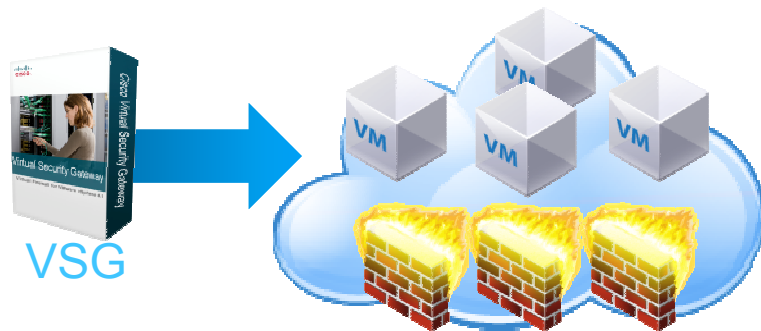
2

Apply hypervisor-based virtual network services



Virtual Service Nodes

Defense in Depth Security Model

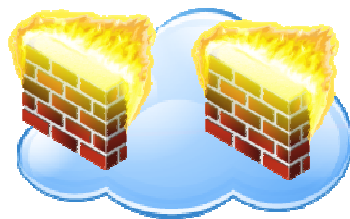


Virtual Security

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



FWSM

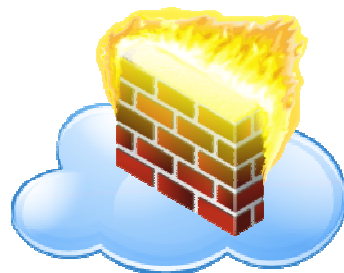


Internal Security

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



ASA 55xx



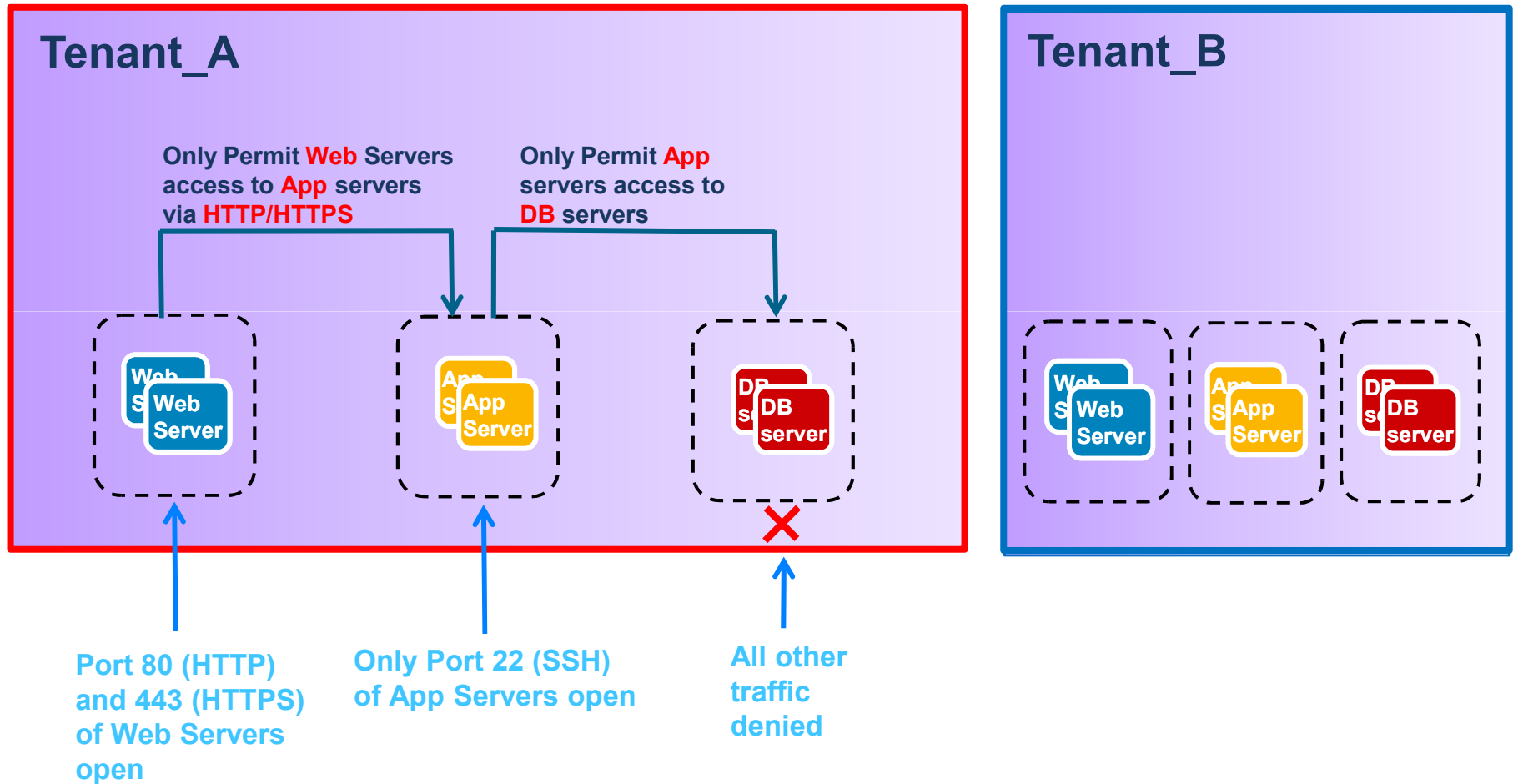
Internet Edge

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

ASA 55xx

Use Case – Secure Segmentation

3-Tier Application Workload



Cisco Virtual Security Gateway

Optimized for Multi-tenant Cloud Environments

Features

- Secure segmentation with **zone-based FW**
- **VM-level granularity** with context-aware rules
- Virtual Network Management Center:
Centralized **policy-based management**

Business Benefits

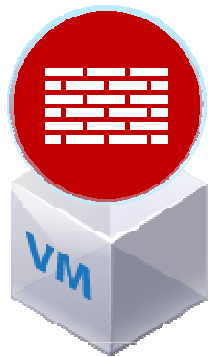
- Operational simplicity
- Deployment flexibility
- Performance optimization
- Consistent security policy compliance and auditing



Virtual Security Gateway on
Nexus 1000V with vPath

Virtual Security Gateway Components

Virtual Security Gateway (VSG)



Security

VM context aware rules

Controls

Establish zones of trust

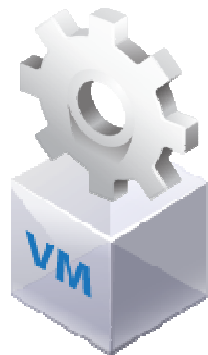
Dynamic, Agile

Policies follow vMotion

Architecture

Efficient, Fast, Scale-out SW

Virtual Network Management Center (VNMC)



Virtual Security Gateway Components

Virtual Security Gateway (VSG)



Security

VM context aware rules

Controls

Establish zones of trust

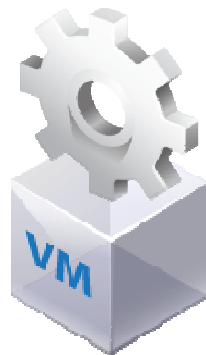
Dynamic, Agile

Policies follow vMotion

Architecture

Efficient, Fast, Scale-out SW

Virtual Network Management Center (VNMC)



Operations

Security team manages security

Administration

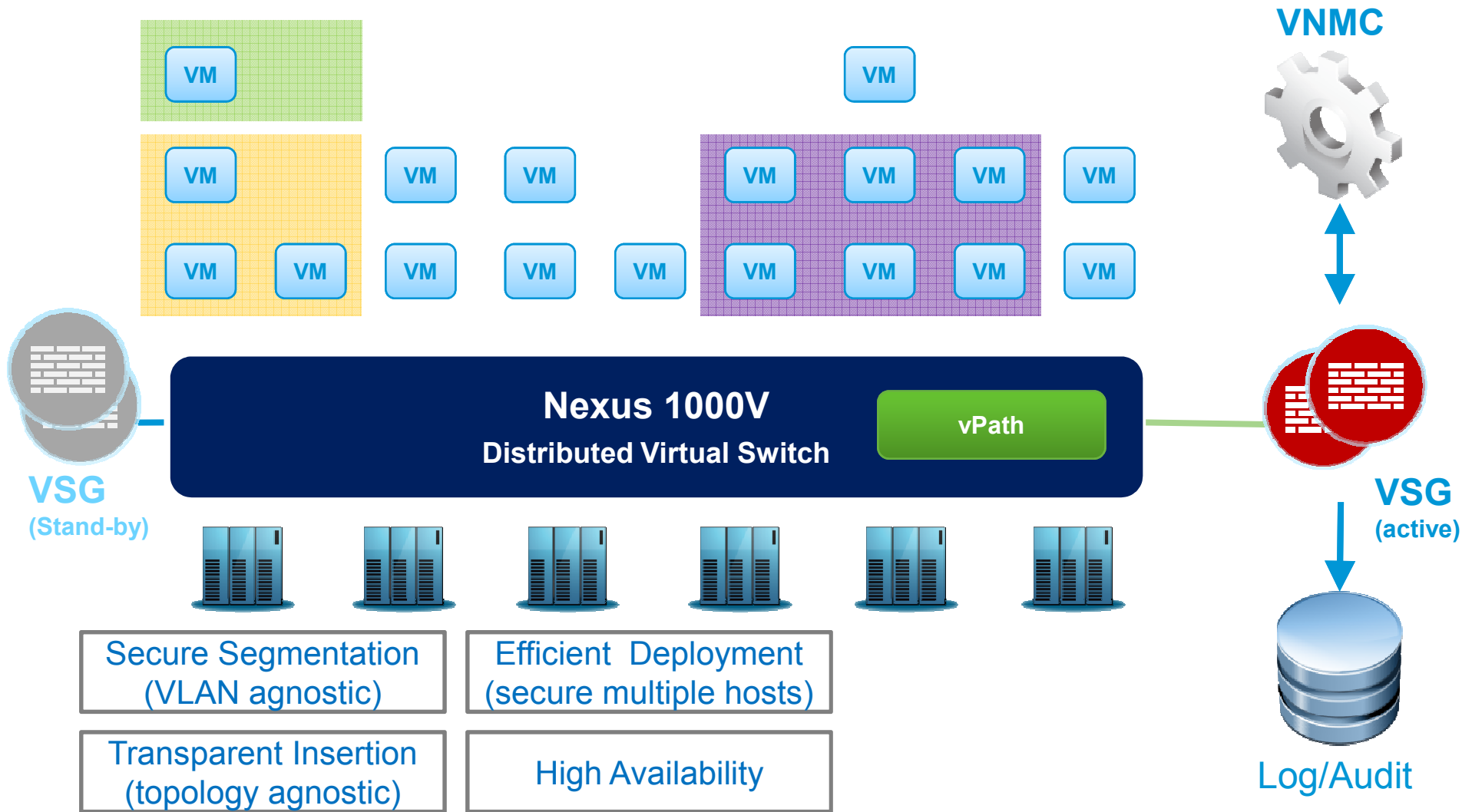
Central mgmt, scalable deployment, multi-tenancy

Automation

XML API, security profiles

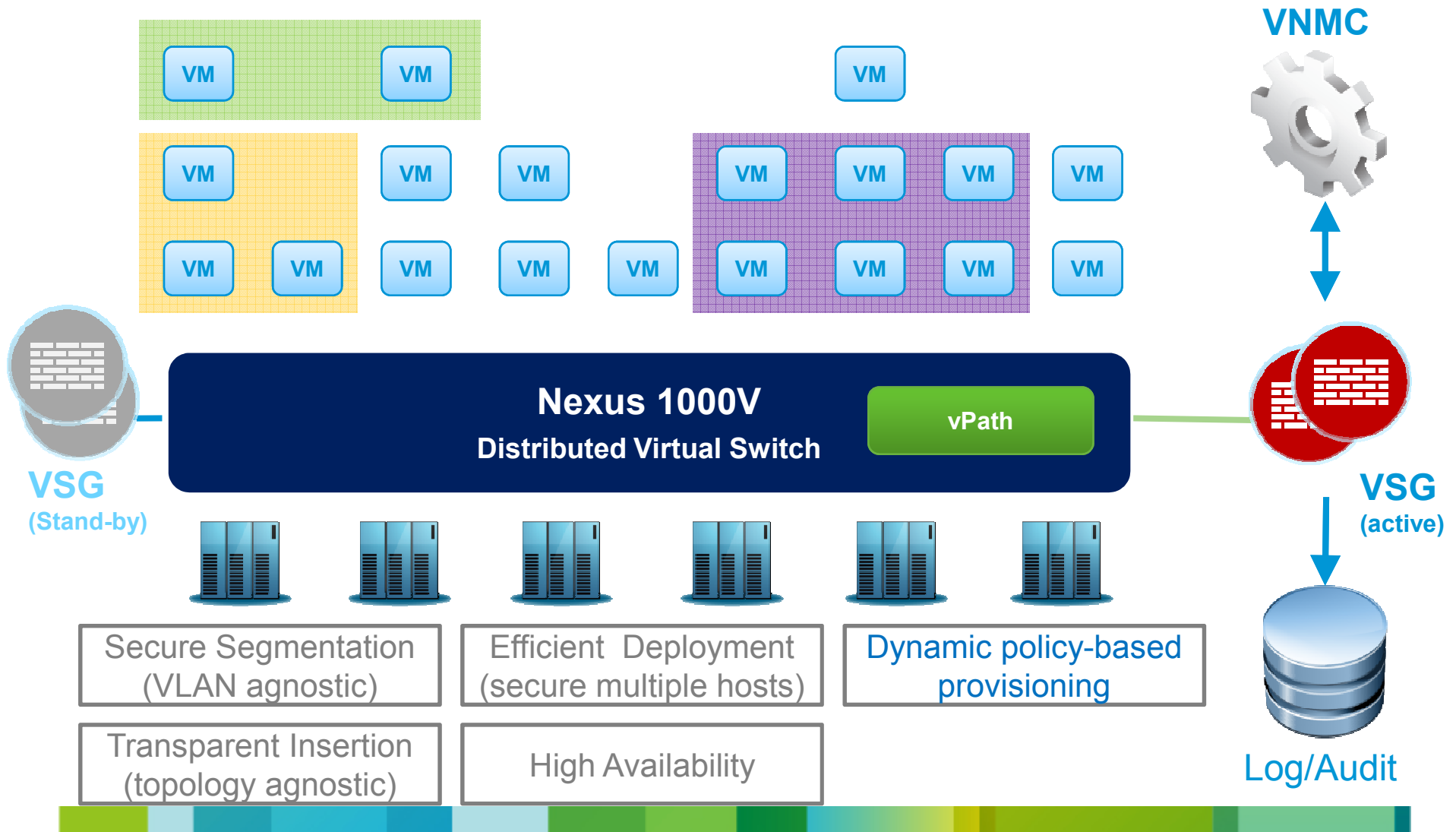
Virtual Security Gateway for Nexus 1000V

Content-based, Virtualization-aware, Multi-tenant, Workload Segmentation for Data Centers and Clouds



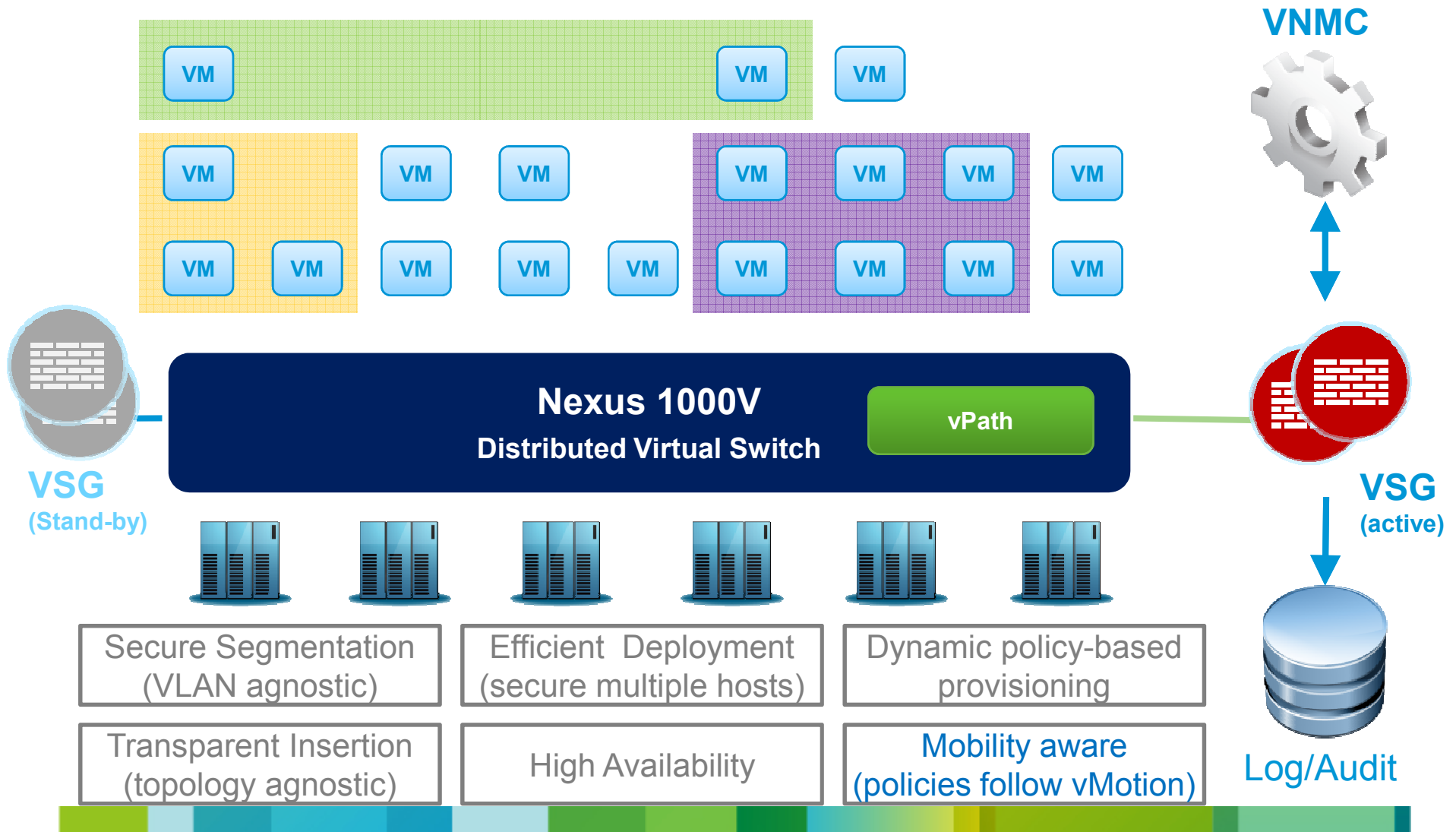
Virtual Security Gateway for Nexus 1000V

Content-based, Virtualization-aware, Multi-tenant, Workload Segmentation for Data Centers and Clouds



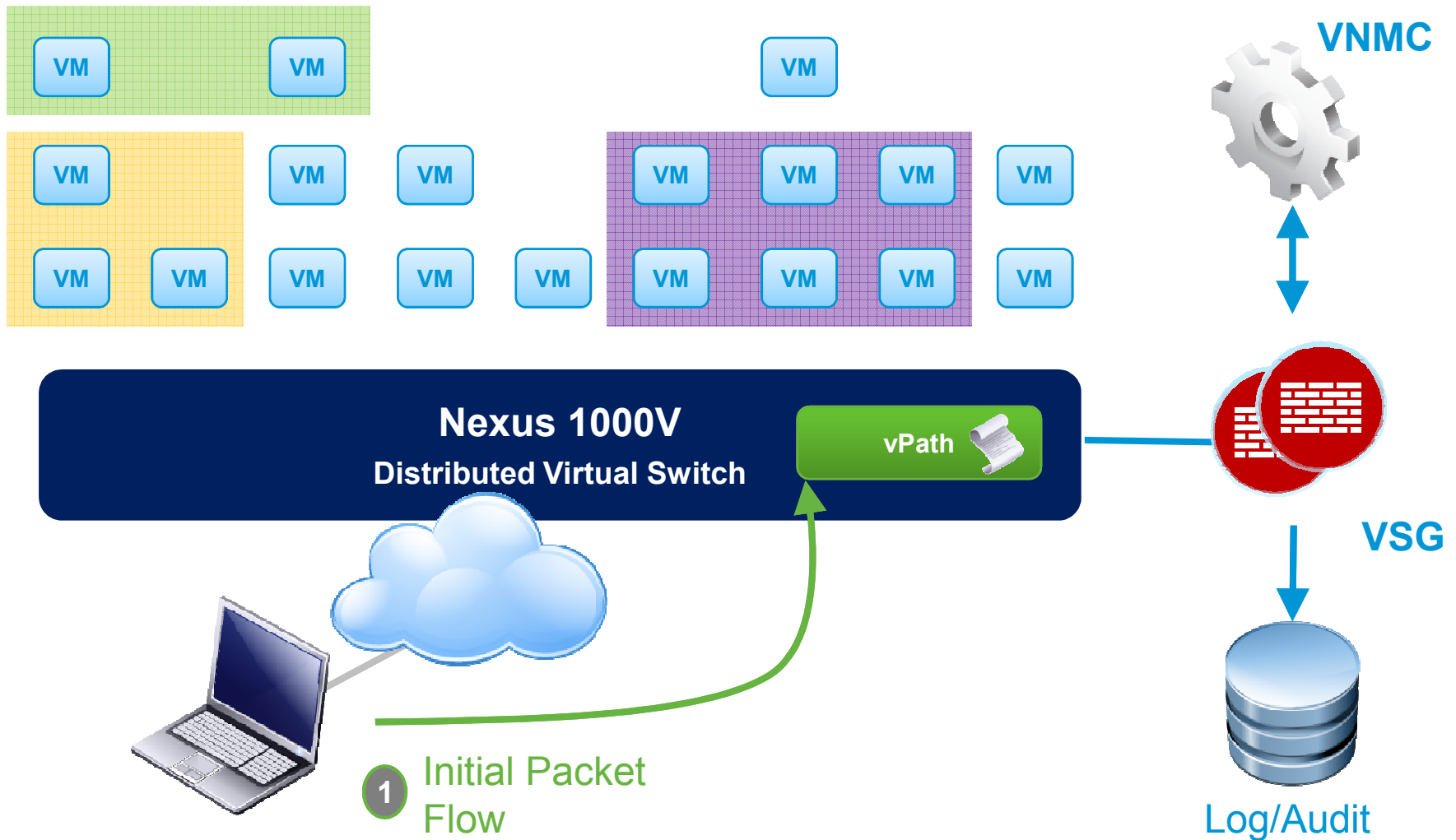
Virtual Security Gateway for Nexus 1000V

Content-based, Virtualization-aware, Multi-tenant, Workload Segmentation for Data Centers and Clouds



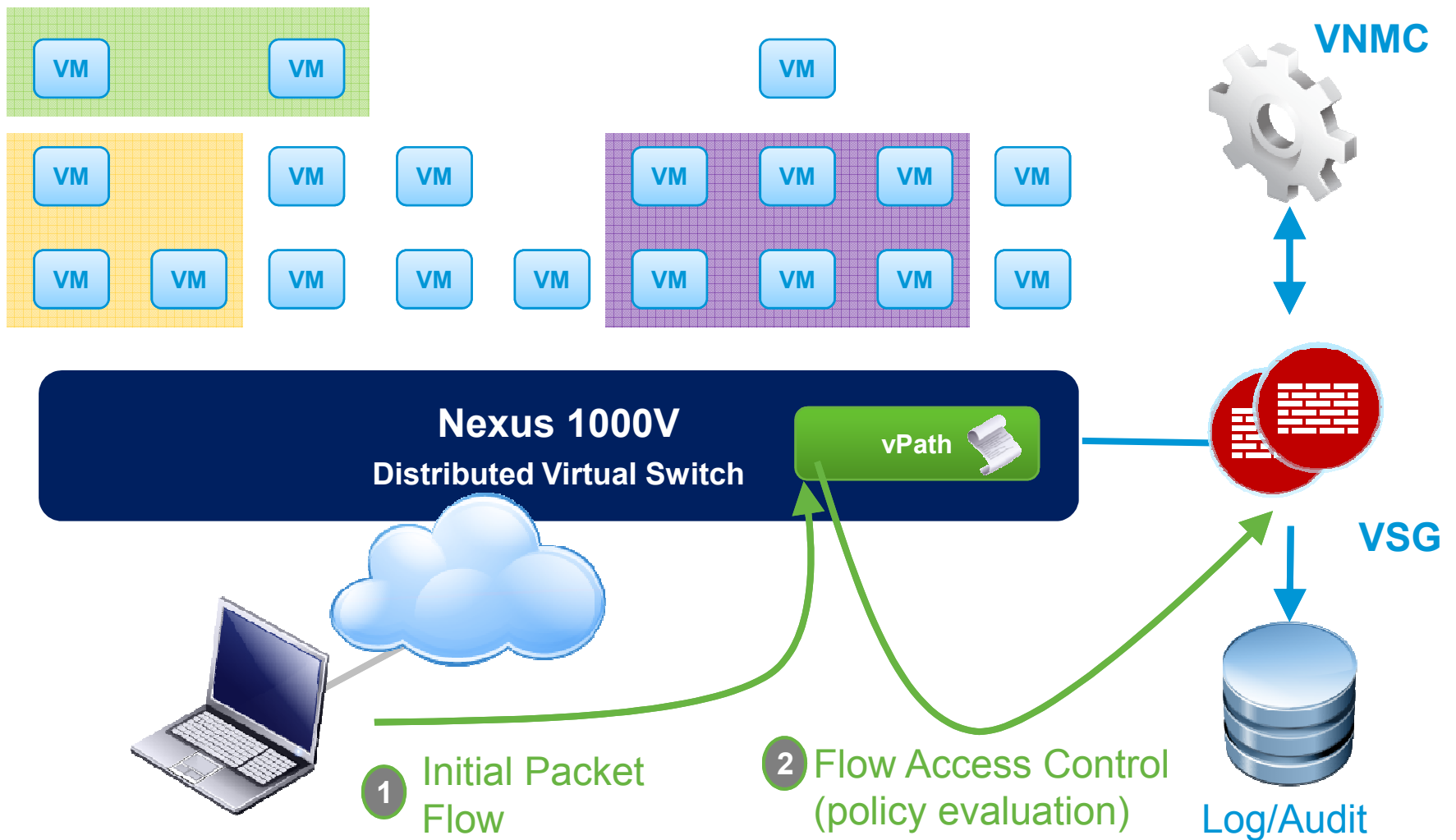
Virtual Security Gateway

Intelligent Traffic Steering with vPath



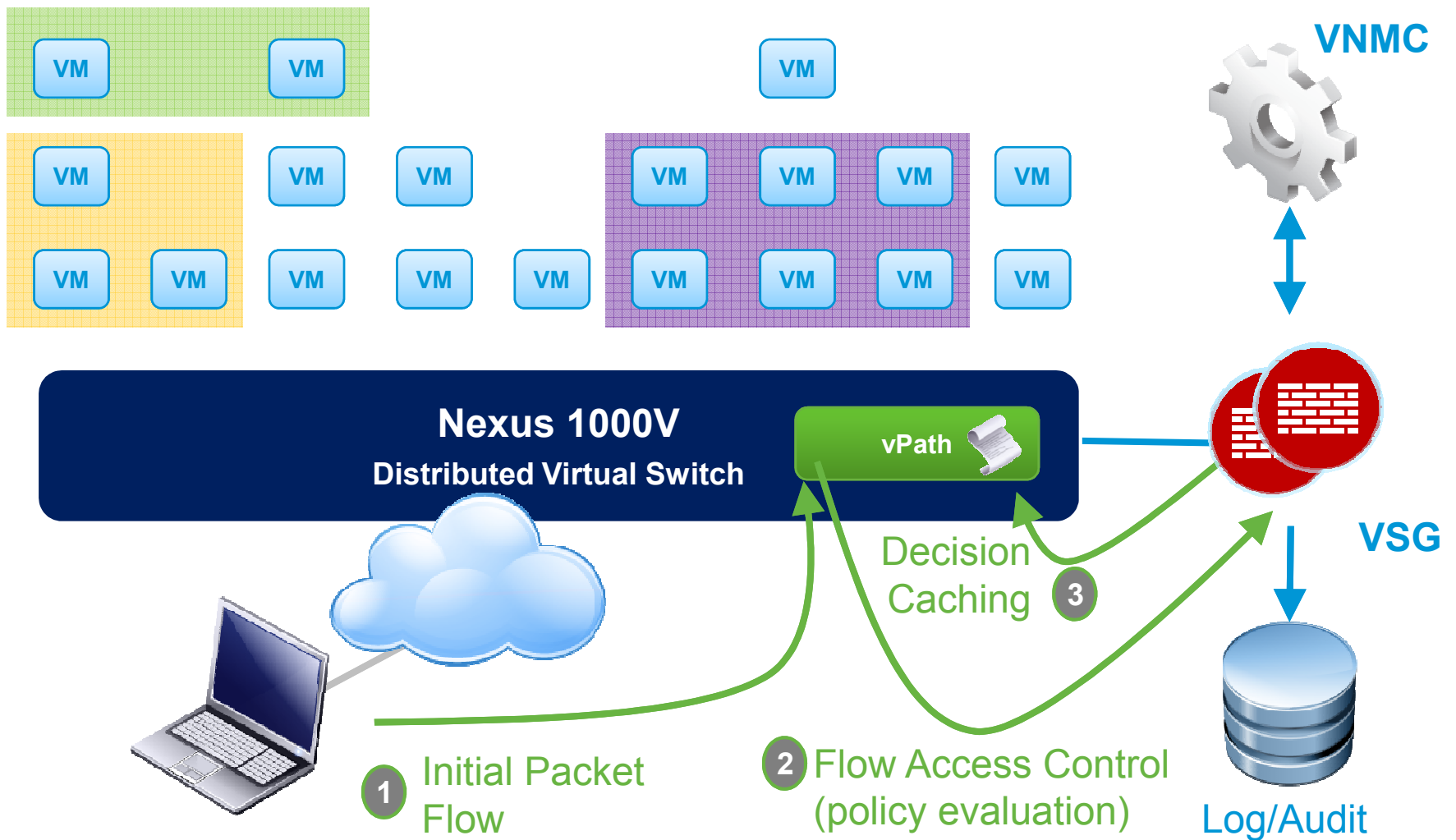
Virtual Security Gateway

Intelligent Traffic Steering with vPath



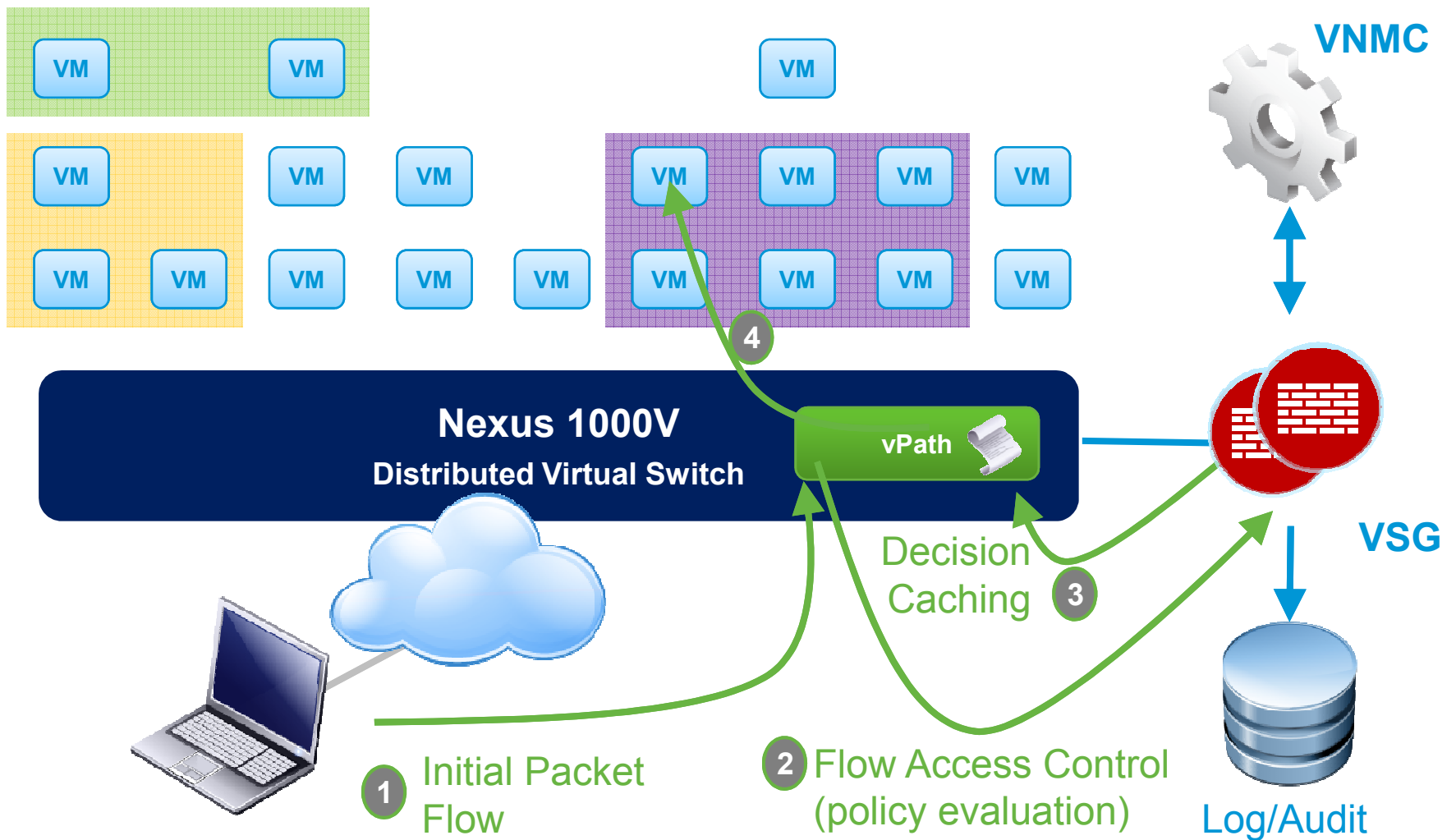
Virtual Security Gateway

Intelligent Traffic Steering with vPath



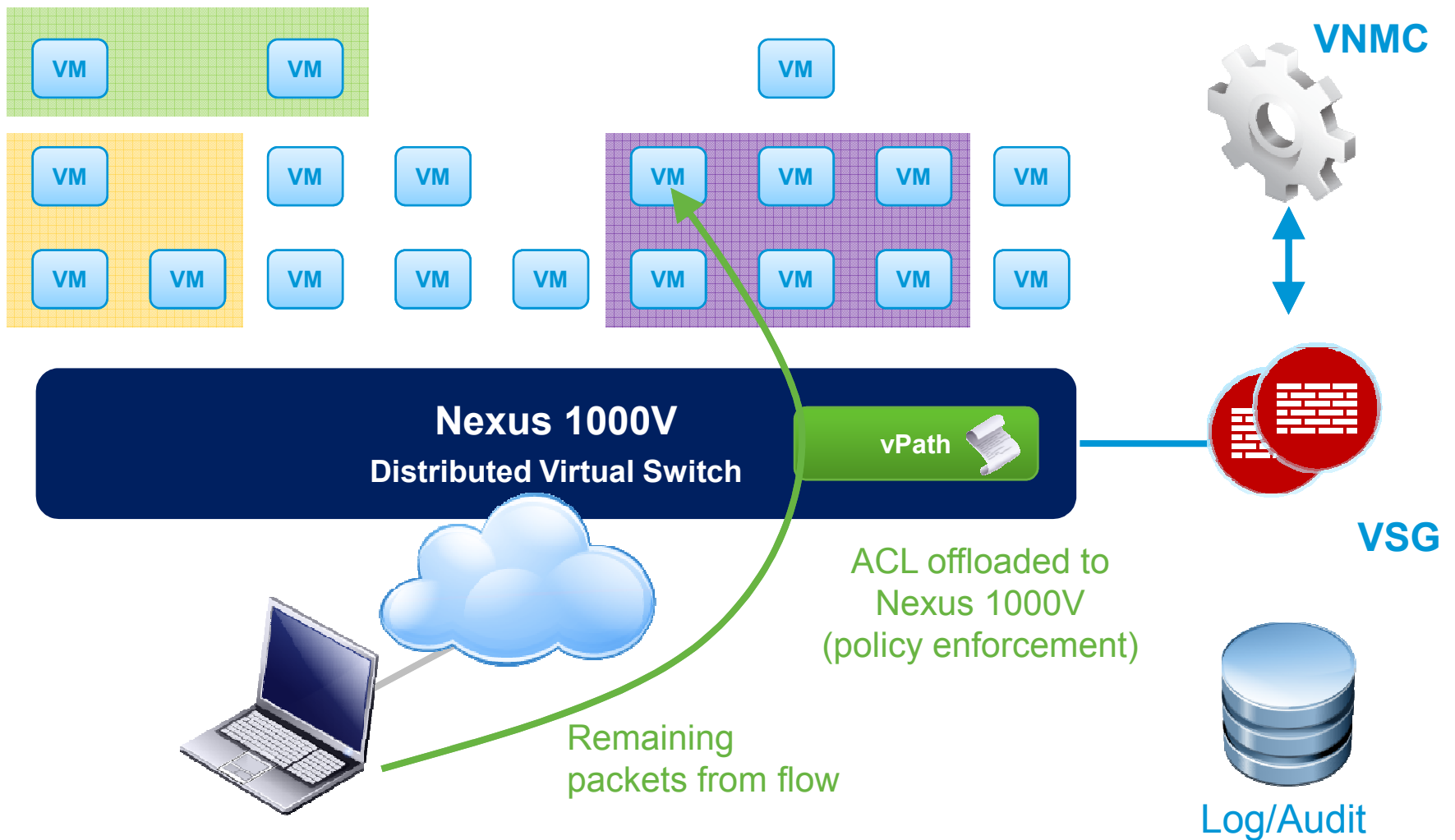
Virtual Security Gateway

Intelligent Traffic Steering with vPath

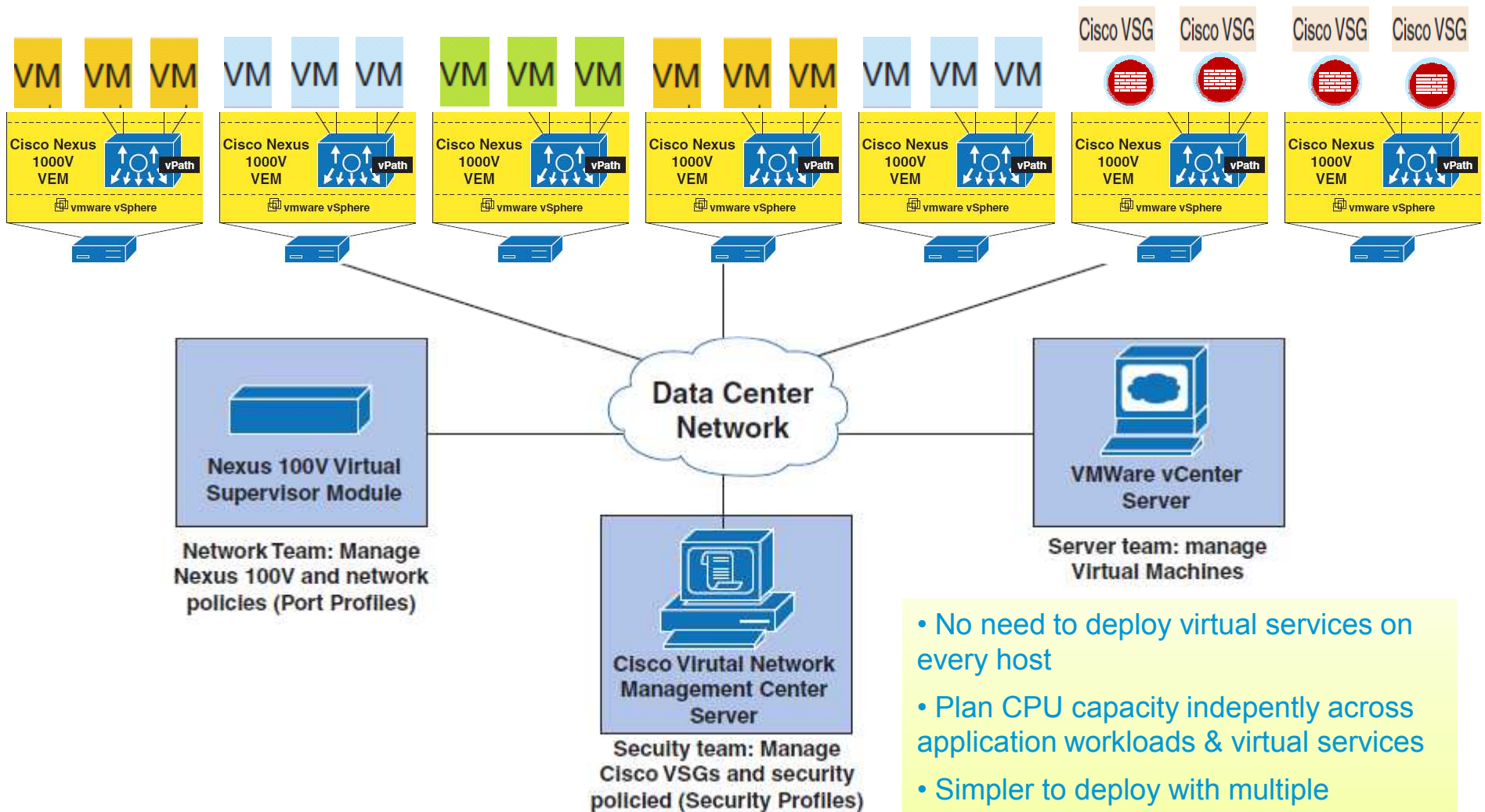


Virtual Security Gateway

Performance Acceleration with vPath

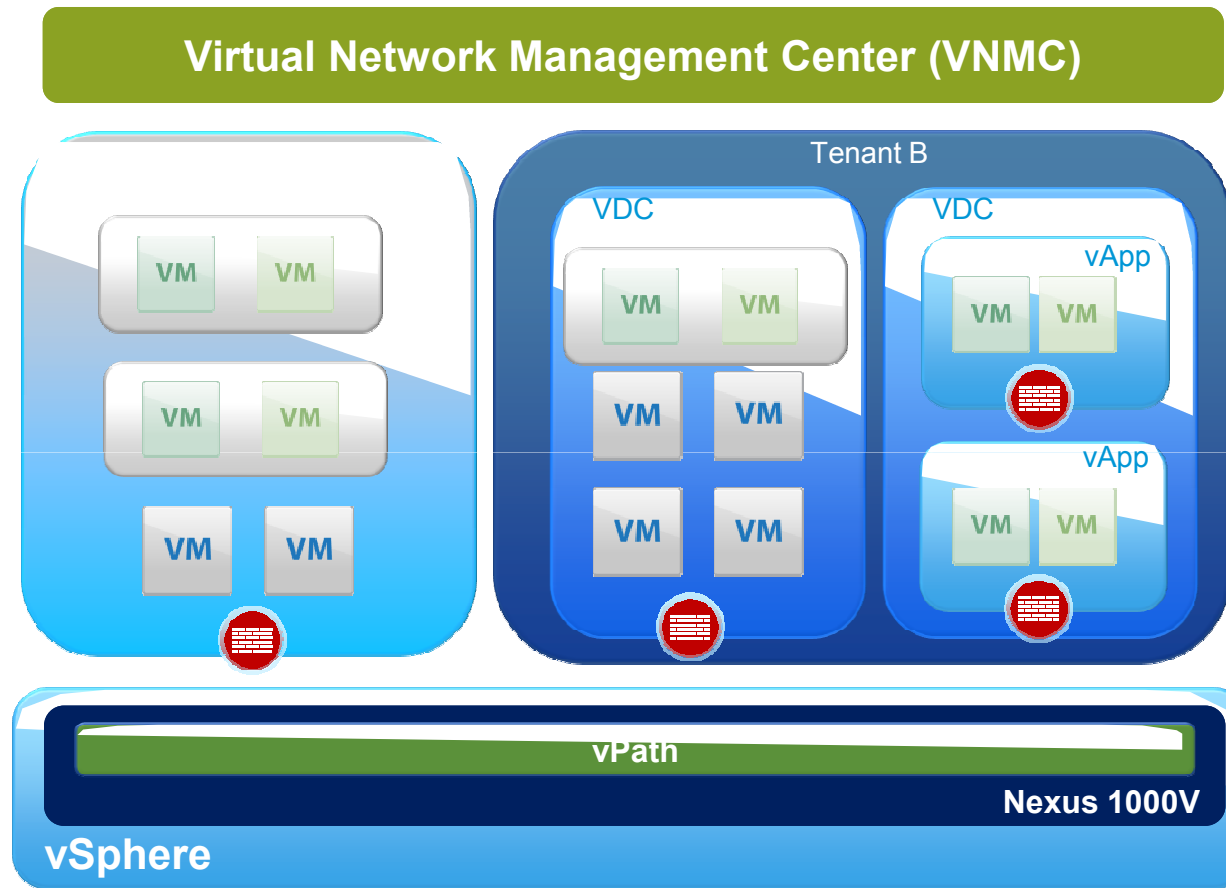


Decoupled Deployment across Applications & Virtual Services



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

Apply Security at Multiple Levels



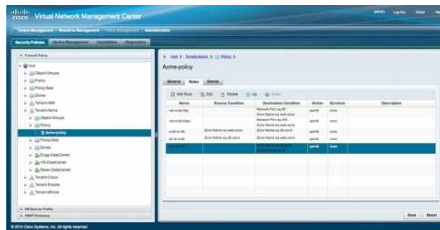
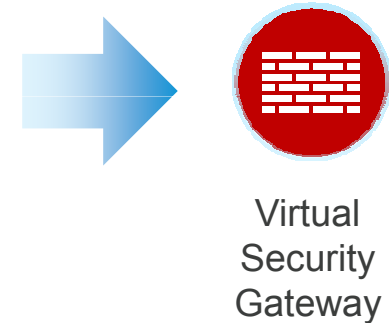
Specify zoning policy with the appropriate granularity

- Tenant, VDC, vApp

Virtual Network Management Center (VNMC)

Simple yet powerful VM security management

- Scalable — **Multi Tenant**
Different Customers, different needs
- Stateless — **Security Profiles**
Simple, policy based security config
- Expandable — **XML API**
3rd party integration ready
- Partitionable — **Role Based Access Controls**
Different users, different privileges
- Integrated — **Nexus 1000V & vCenter**
Port profiles refer to security profiles
- Automated — **Dynamic provisioning**
One stop configuration of network & security

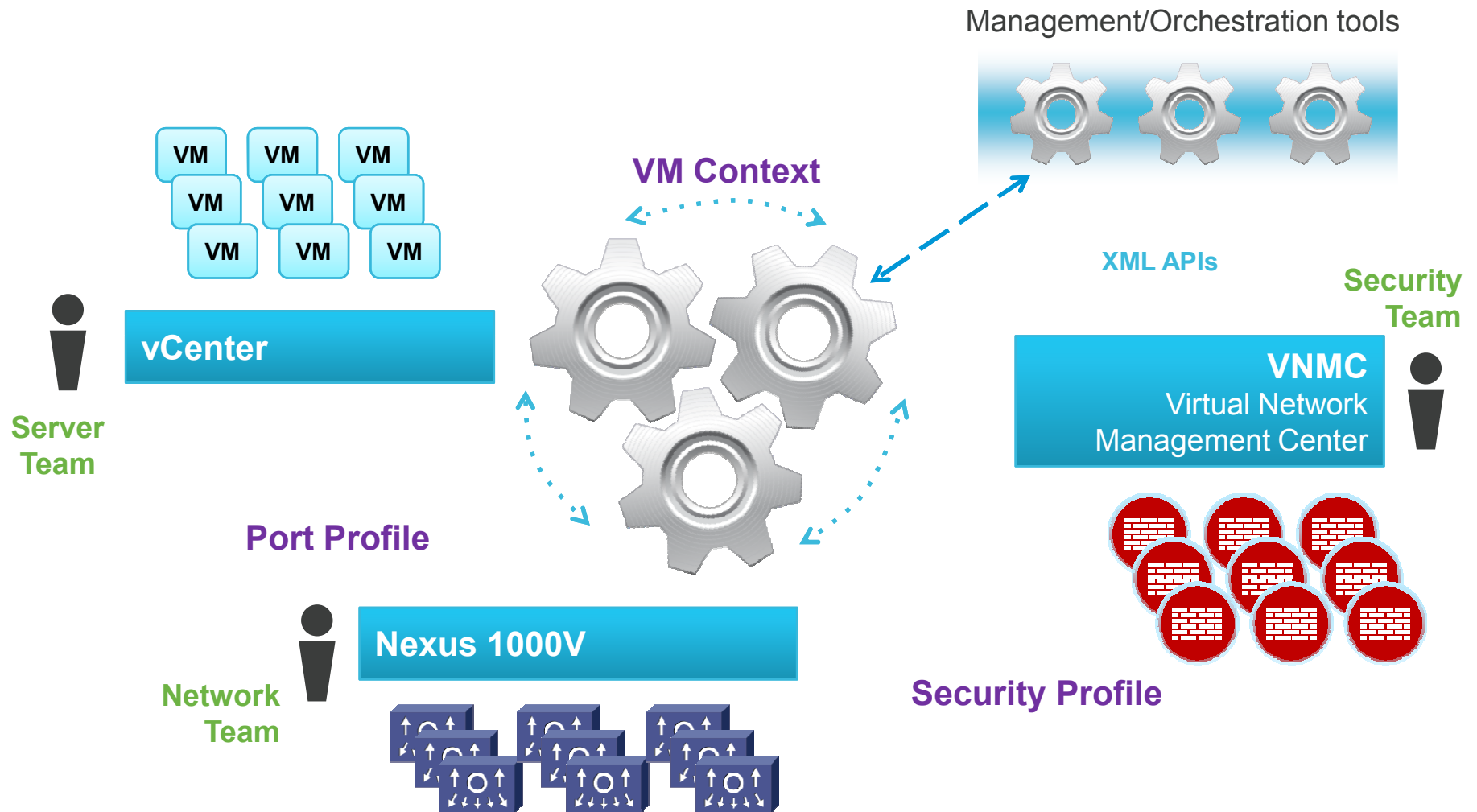


VNMC GUI

Virtual Network Management Center

Virtual Network Management Center (VNMC)

Seamless Policy-Based Management



VM Context-based Rule Engine

Add

Add Destination Condition

Attribute Type :

Expression

Attribute Name : Operator : Attribute Value :

*Obtained from vCenter

VM Context-based Rule Engine

Add Destination Condition

Attribute Type :

Expression

Attribute Name : Operator : Attribute Value :

Attribute Type options: Network, VM, Custom

Buttons: OK, Cancel

*Obtained from vCenter

VM Context-based Rule Engine

Add Destination Condition

Attribute Type :

Expression

Attribute Name : Operator : Attribute Value :

Attribute Type
Network
VM
Custom

VM Attributes
Instance (VM) Name*
Guest OS full name*
vApp Name*
Cluster Name*
Hypervisor Name*
Zone Name
Port Profile Name

Network Attributes
IP Address
Network Port

OK Cancel

*Obtained from vCenter

VM Context-based Rule Engine

Add Destination Condition

Attribute Type :

Expression

Attribute Name : Operator : Attribute Value :

Attribute Type
Network
VM
Custom

VM Attributes
Instance (VM) Name*
Guest OS full name*
vApp Name*
Cluster Name*
Hypervisor Name*
Zone Name
Port Profile Name

Network Attributes
IP Address
Network Port

Operator
EQ (equal to)
NEQ (not equal to)
GT (greater than)
LT (less than)
Range
Not-in-range
Prefix

Operator
Member
Not-member
Contains

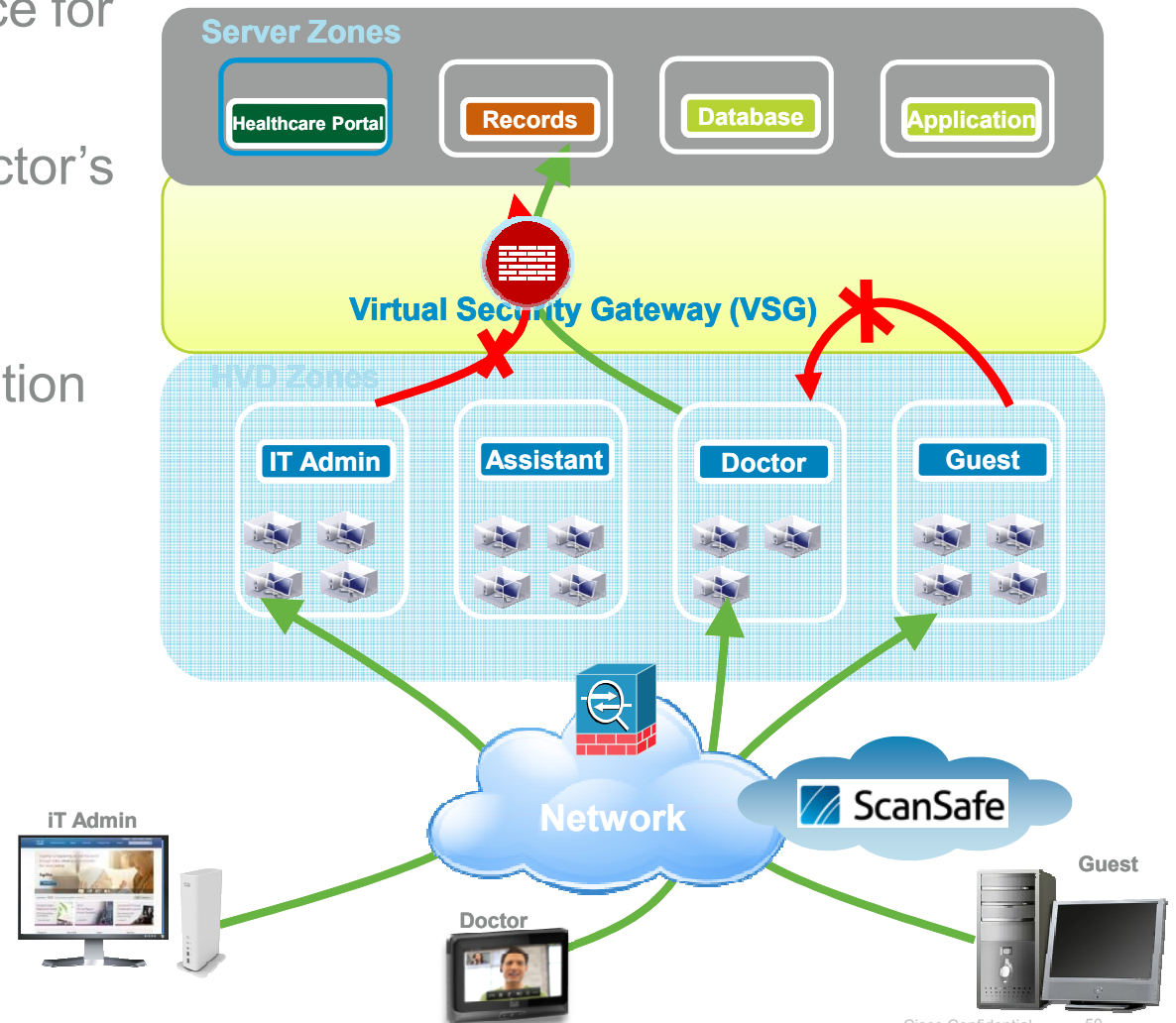
OK Cancel

*Obtained from vCenter

VSG Use Case

Securing Virtual Desktops

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



CareCore National – VSG Usecase

Customer Challenge

- Secure traffic between different VM zones in a shared work-load environment
- Multi-tenant aware solution
- Maintain administrative responsibility with Security teams providing security policies

Cisco Solution

- Secure zones created using VM attributes (not VLANs)
- Cisco VSG installed to protect VMs across multiple physical servers
- Deployed in HA pair

Results & Impact

- Training Apps – isolated from other apps
- Enable secure zoning without VLAN configurations & VLAN proliferation



“Cisco’s Virtual Security Gateway not only met our virtual security needs, but with its VM-aware rule engine, allowed us to re-think the way we write security policies.”

Bill Moore, CTO



VSG Deployment at CareCore National

Logical zoning, vMotion support & scalable solution



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

VSG Deployment at CareCore National

Before & After Cisco Virtual Security Gateway

Before VSG

Controls: applied within training application (via config)

New VM: must be added manually to these config. files. Dependency on application admin.

Network: Prefer not to use VLANs for segmentation due to changes on switches

Intrusiveness: highly manual, prone to errors

After VSG Deployment

- Controls applied outside the apps
- No need to change appl configs
- Training ALWAYS matches PROD rev

- New VMs are automatically firewalled
- No dependency on application admin.
- Lower admin cost at faster deploy

- VLAN agnostic FW controls
- More effective DR
- VPLEX compatible

- Security profiles & VM-name based policies
- Simpler and faster
- Reduces 'himan error' conditions



Additional Information

Additional Information

- 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

- My Cisco Community

<https://www.myciscocommunity.com/community/products/nexus1000v>

- Deployment Guides

[Nexus 1000V Deployment Guide](#)

[Nexus 1000V on UCS – Best Practices](#)

[Nexus 1010 Deployment Guide](#)

[VSG Deployment Guide](#)



Sign up at: <http://tinyurl.com/1000v-webinar>

Date	Business Sessions
22-Mar	Nexus 1000V Family Overview and Update
5-Apr	Virtual Network Services (vPath, vWAAS, NAM)
19-Apr	Virtual Security Gateway Introduction
3-May	Journey to the Cloud w/ N1KV: vCloud Director & Long Distance vMotion
17-May	Secure VDI with Nexus1000V & VSG

Date	Technical Sessions
29-Mar	Nexus 1000V New Features and Installation Overview
12-Apr	Nexus1010 Installation & Upgrade
26-Apr	Virtual Security Gateway Installation and Basic Configuration Overview
10-May	Nexus 1000V Advanced Configuration
24-May	Nexus 1000V Troubleshooting

Web Sites

www.cisco.com/go/1000v

www.cisco.com/go/nexus1010

www.cisco.com/go/vsg

www.cisco.com/go/vnmc

www.cisco.com/go/1000vcommunity
(Preso and Q&A posted here)

Thank you.

