



Cisco Virtual Security Gateway (VSG) Technical Overview

Syed Ghayur
Technical Marketing Engineer
SAVBU

Cisco Confidential



Nexus 1000V Public Webinar Series

Date	Business Sessions
22-Mar	Nexus 1000V Family Overview and Update
5-Apr	Virtual 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

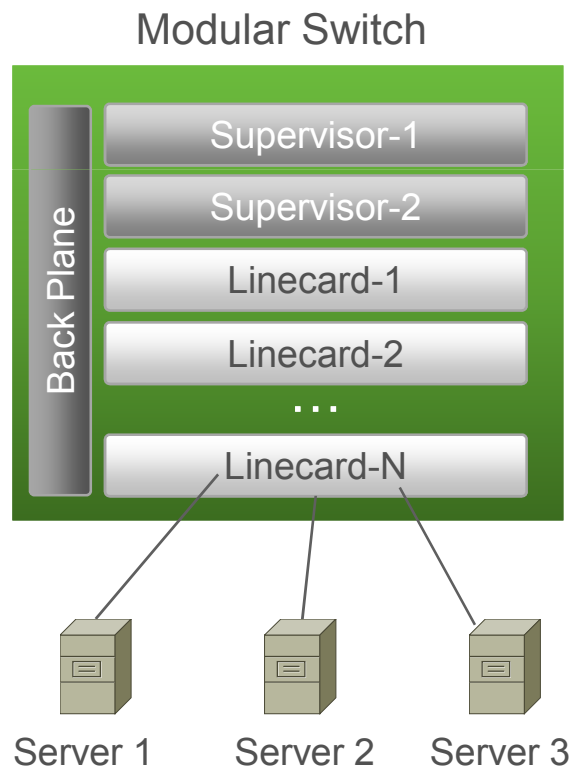
Date	Technical Sessions
29-Mar	Nexus 1000V New Features and Installation Overview
12-Apr	Nexus1010 Installation & Upgrade
26-Apr	Virtual Security Gateway Technical Overview
10-May	Nexus 1000V Advanced Configuration
24-May	Nexus 1000V Troubleshooting

Nexus 1000V Architecture Overview



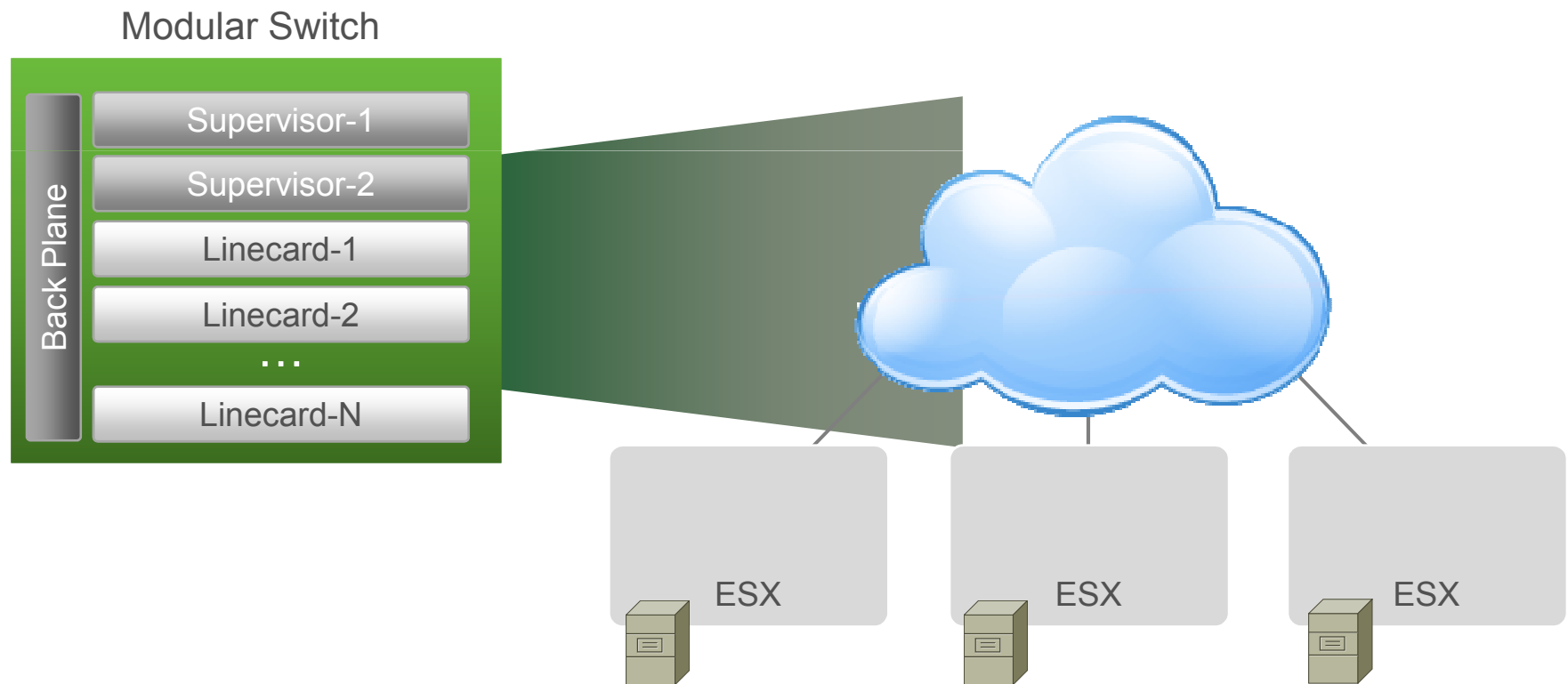
Nexus 1000V Architecture

Comparison to a Physical Switch



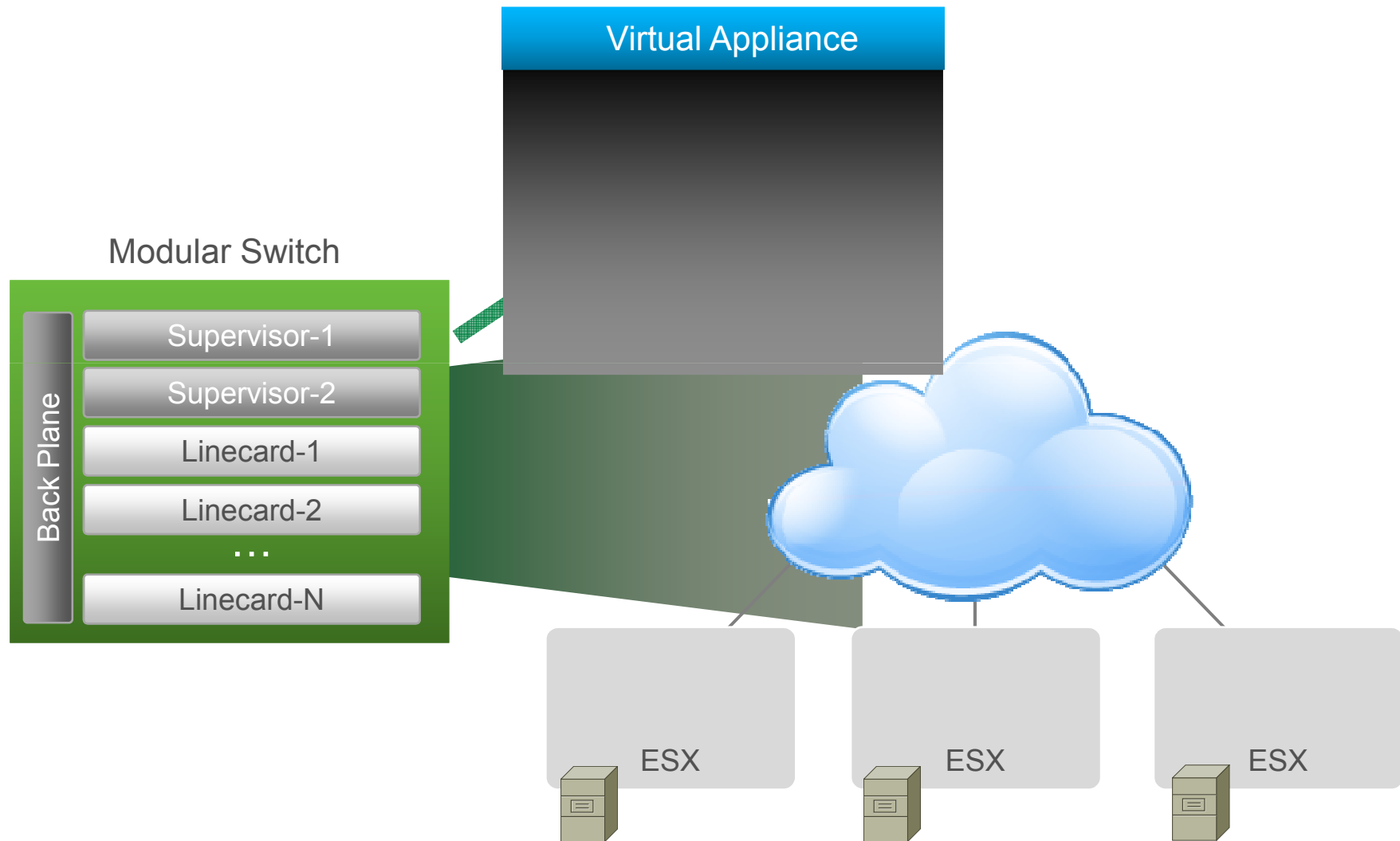
Nexus 1000V Architecture

Moving to a Virtual Environment



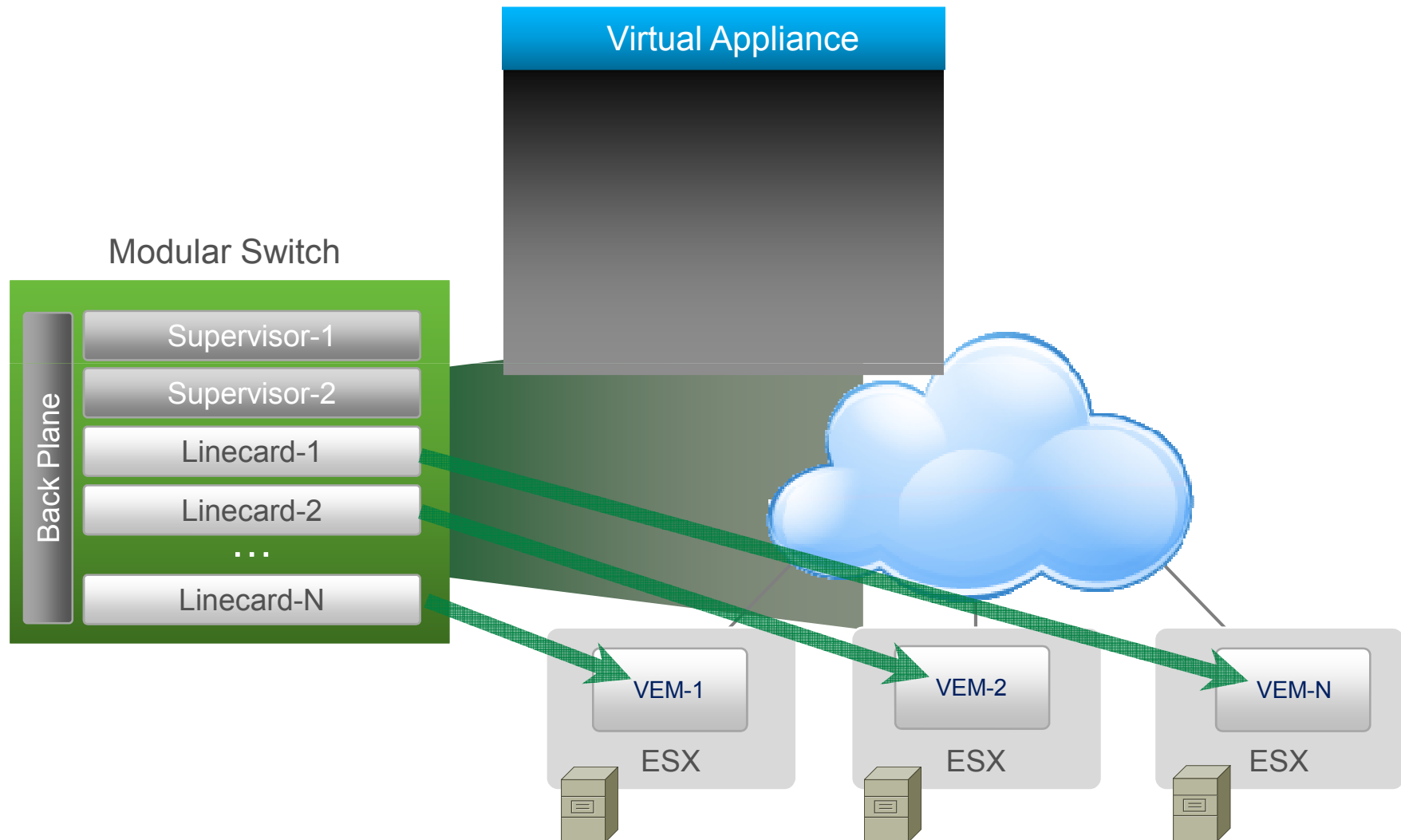
Nexus 1000V Architecture

Supervisors → Virtual Supervisor Modules (VSMs)



Nexus 1000V Architecture

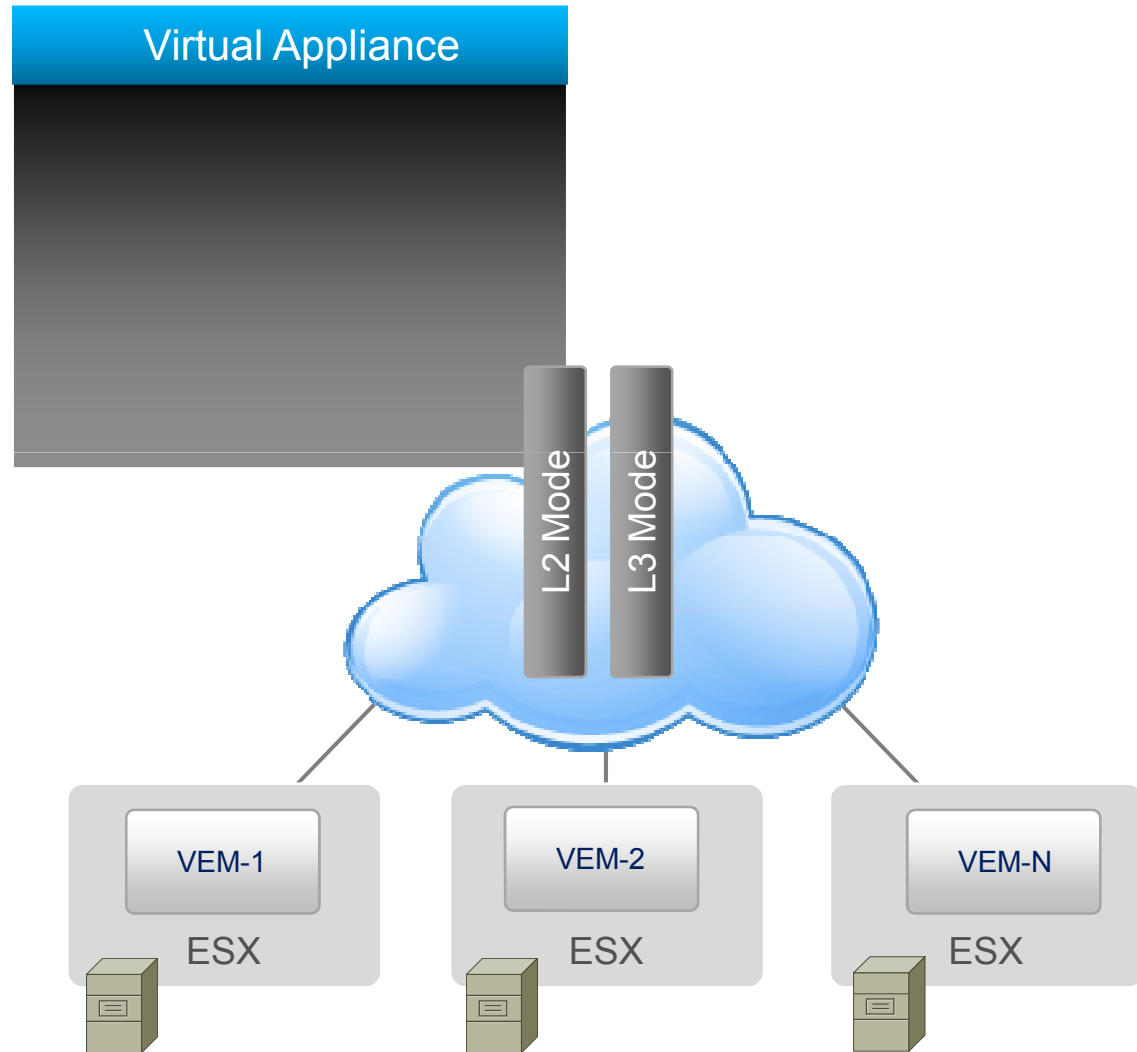
Linecards → Virtual Ethernet Modules (VEMs)



Nexus 1000V Architecture

VSM + VEMs = Nexus 1000V Virtual Chassis

- 64 VEMs per 1000V (connected by L2 or L3)
- 200+ vEth ports per VEM
- 2K vEths per 1000V
- Multiple 1000Vs can be created per vCenter



VSM: Virtual Supervisor Module
 VEM: Virtual Ethernet Module

Slide 8

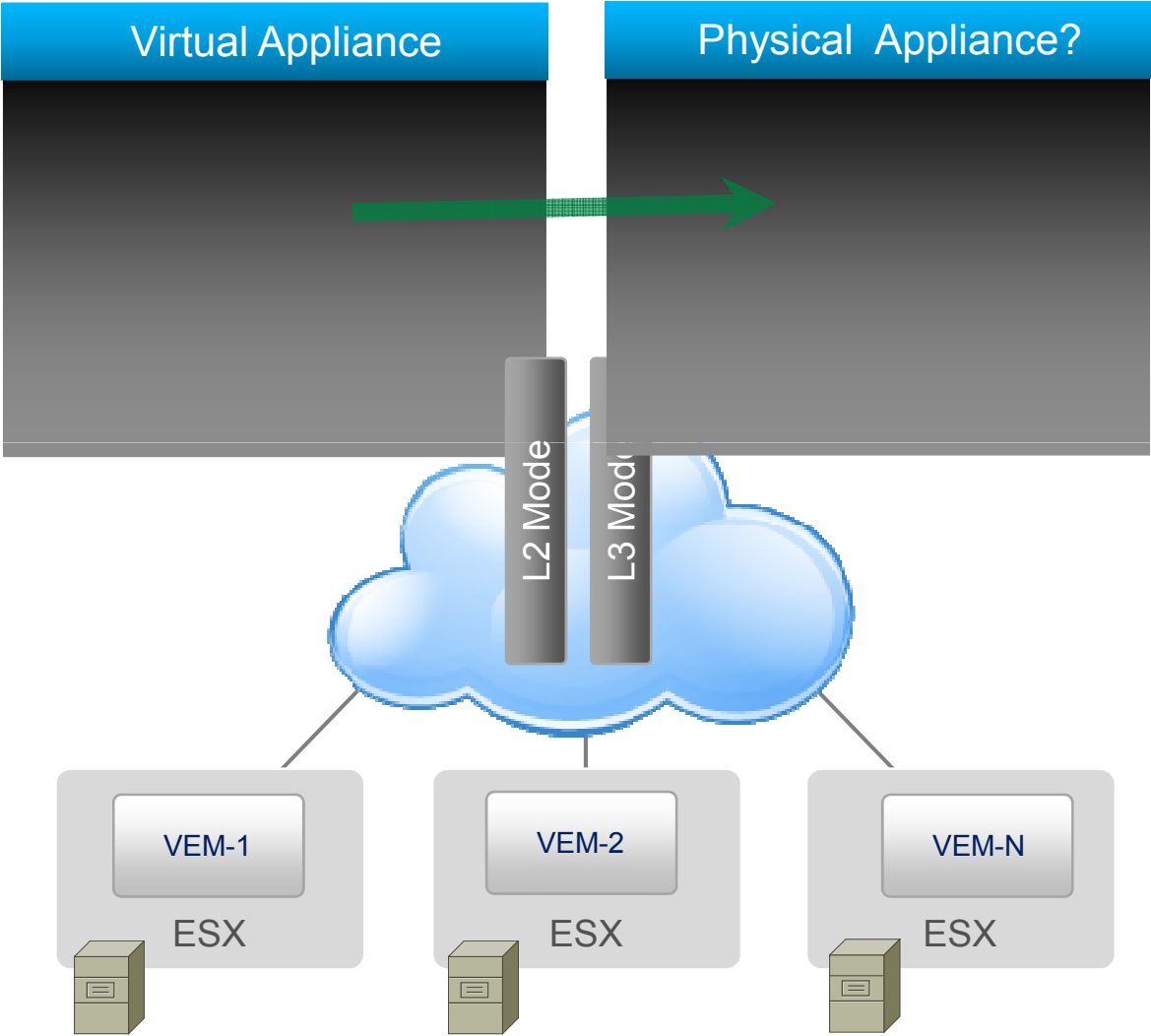
NM15 clean up this slide. It's N1K specific

make colors match better

Neal Mueller, 3/11/2011

Nexus 1000V Architecture

Customer Request: Host VSMs on a Physical Appliance



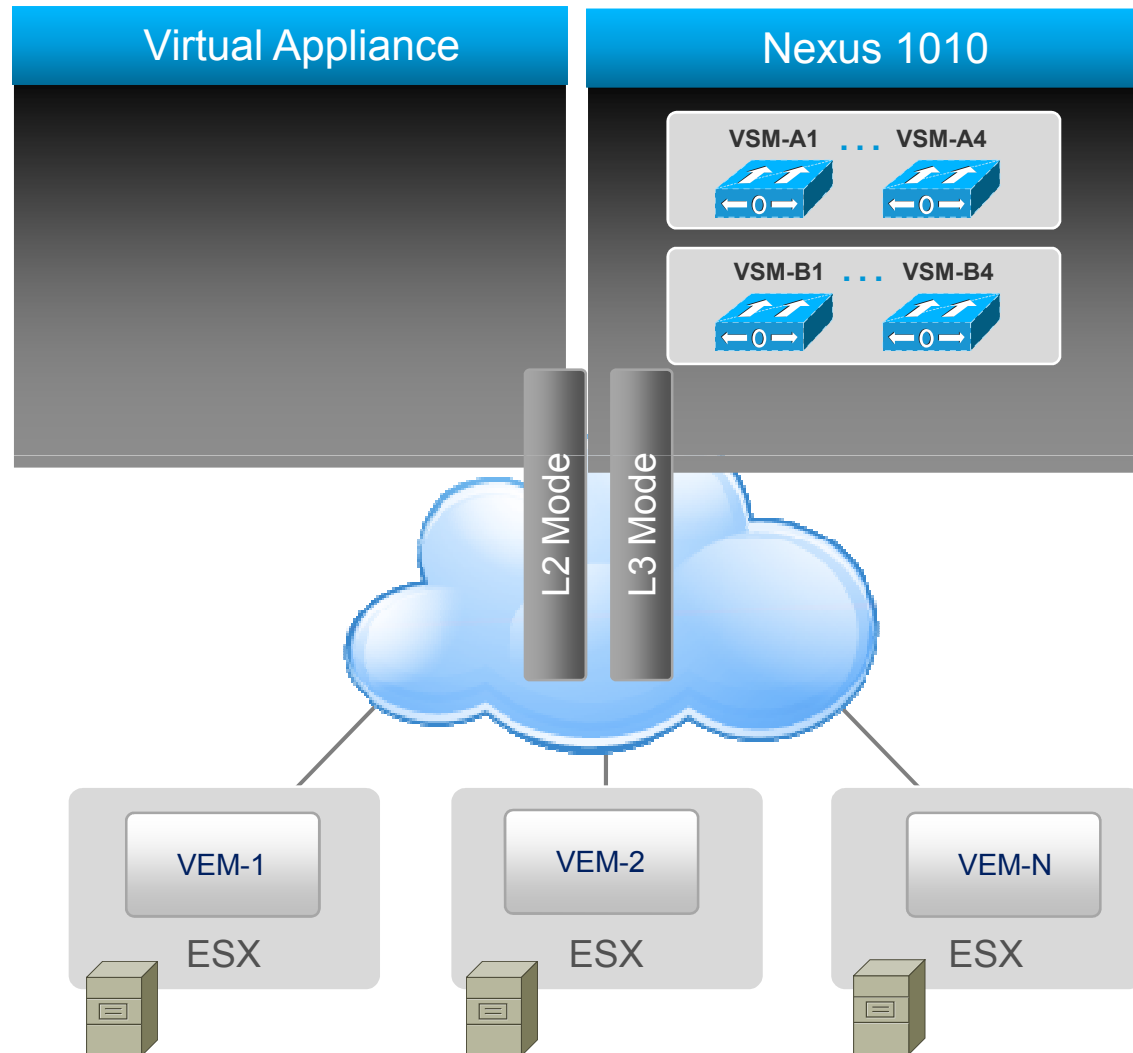
- 200+ vEth ports per VEM
- 64 VEMs per 1000V
- 2K vEths per 1000V
- Multiple 1000Vs can be created per vCenter

VSM: Virtual Supervisor Module
VEM: Virtual Ethernet Module

Nexus 1000V Architecture

VSMs hosted on a Physical Appliance: Nexus 1010

- Up to 4 VSMs per Nexus 1010
- Nexus 1010s deployed in redundant pair

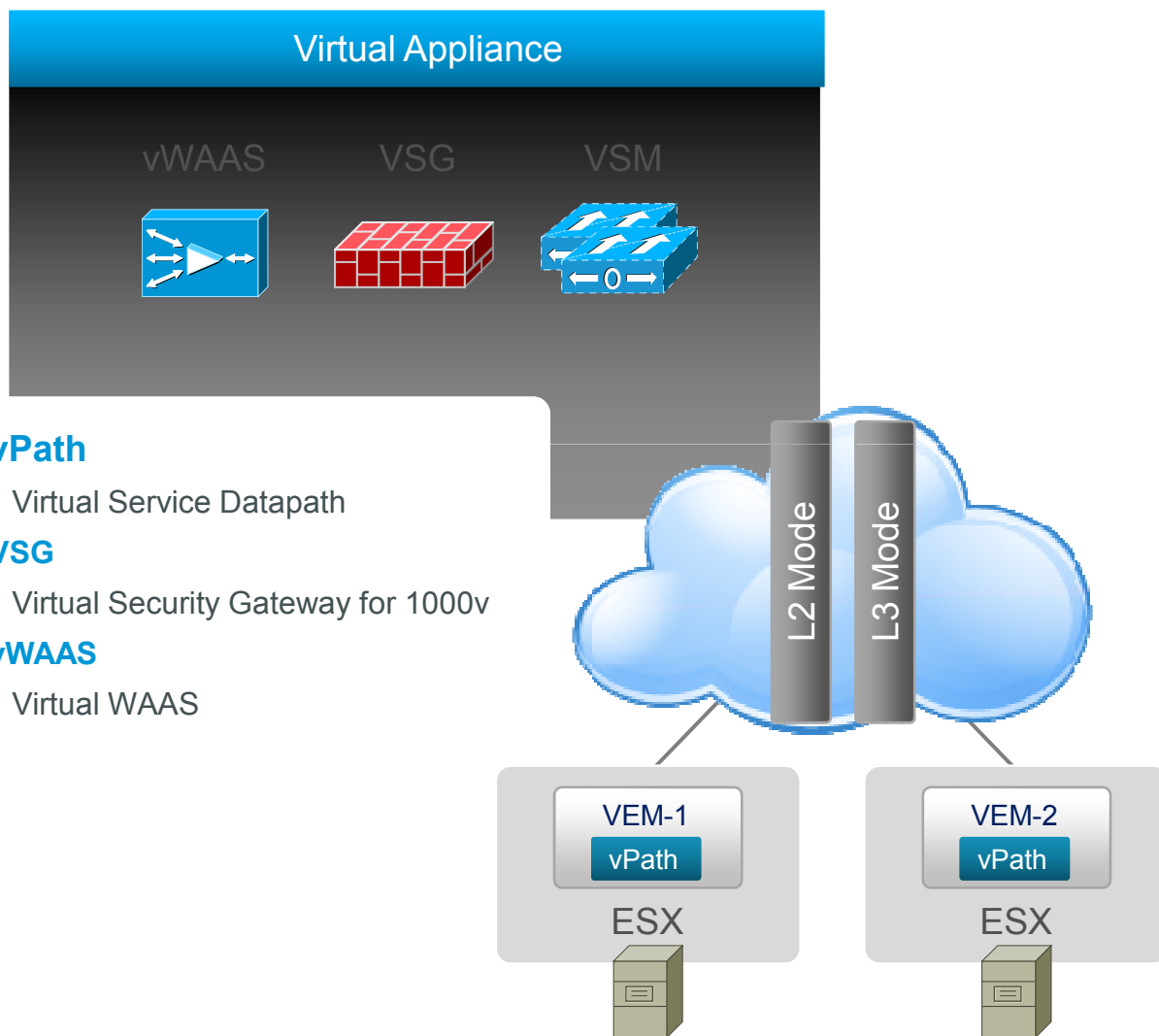


- 200+ vEth ports per VEM
- 64 VEMs per 1000V
- 2K vEths per 1000V
- Multiple 1000Vs can be created per vCenter

VSM: Virtual Supervisor Module
VEM: Virtual Ethernet Module

Embedding Intelligence for Virtual Services

vPath – Virtual Service Datapath



VSG and vWAAS available now

vPath

- Virtual Service Datapath

VSG

- Virtual Security Gateway for 1000v

vWAAS

- Virtual WAAS

vPath

- Traffic Steering
- Fast -Path Offload

• Nexus 1000V ver 1.4 & above

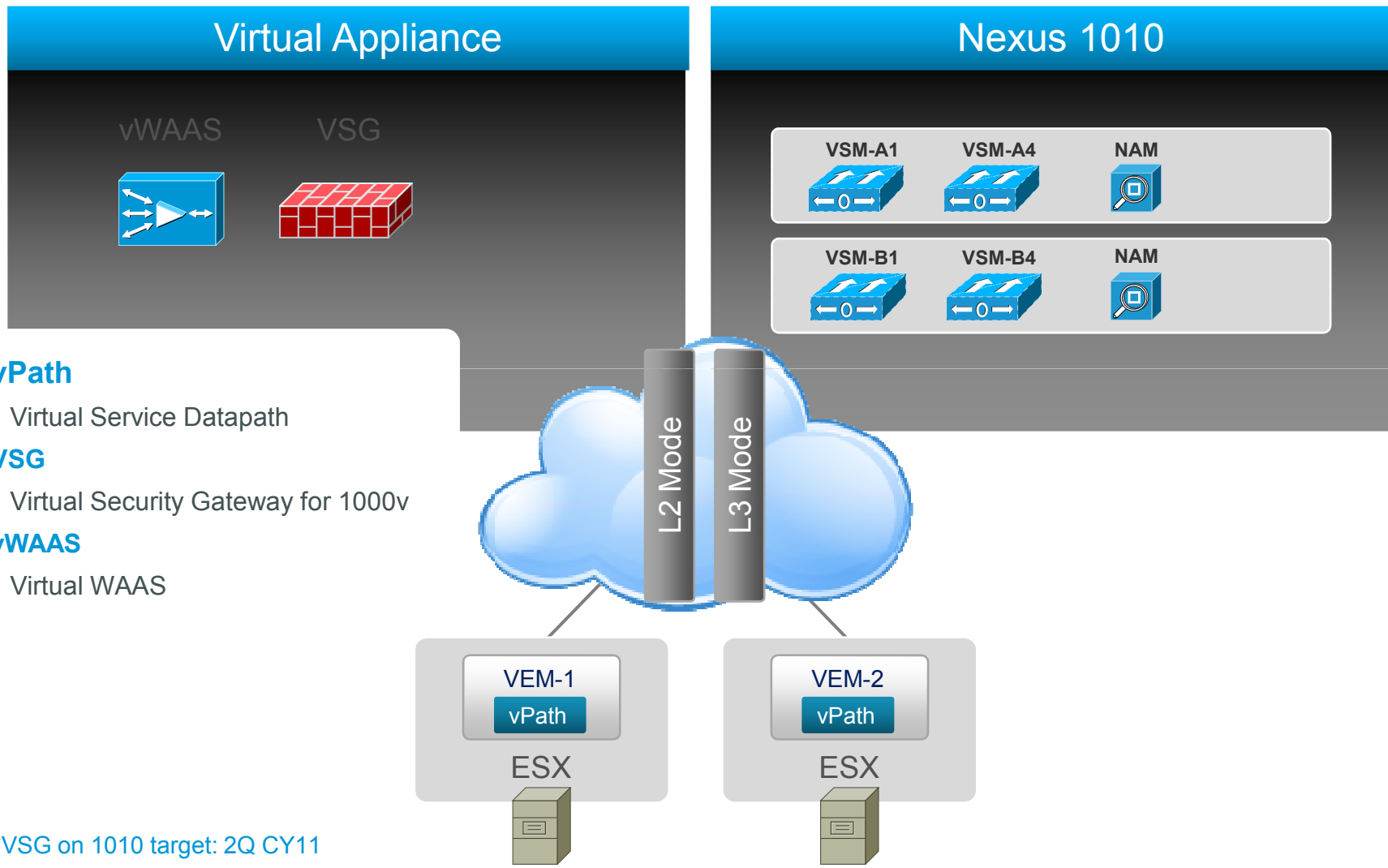
Slide 11

NM18 clean up this slide. It's N1K specific

make colors match better

Neal Mueller, 3/11/2011

Nexus 1010 – Hosting Platform for Services



vPath

- Virtual Service Datapath

VSG

- Virtual Security Gateway for 1000v

vWAAS

- Virtual WAAS

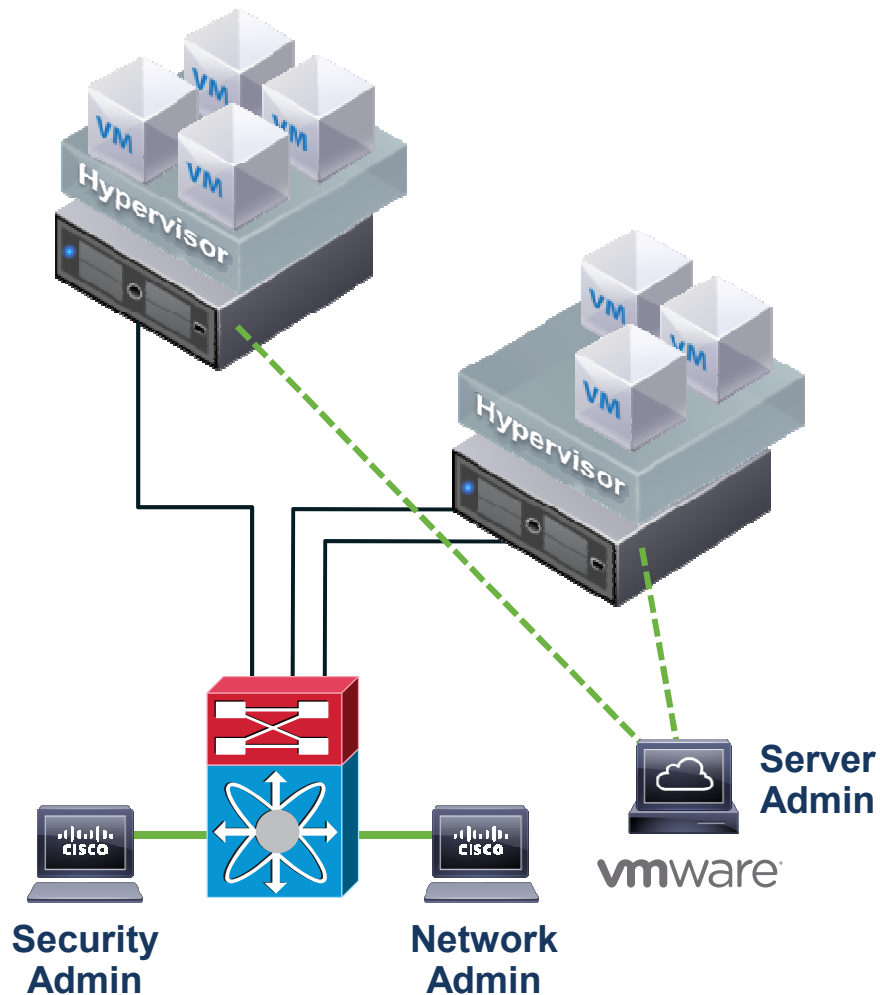
*VSG on 1010 target: 2Q CY11



Cisco Virtual Security Gateway (VSG)

Syed Ghayur - TME

Server Virtualization Issues

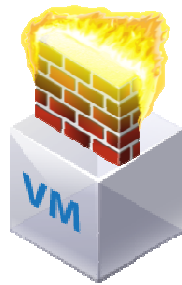


1. vMotion moves VMs across physical ports—the network **policy must follow vMotion**
2. Must view or apply network/security policy to **locally switched** traffic
3. Need to maintain **segregation of duties** while ensuring **non-disruptive operations**

Virtual Security Gateway

Virtual Firewall for Nexus 1000V

Virtual Security Gateway (VSG)



Context Aware Security

VM context aware rules

Zone-Based Control

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

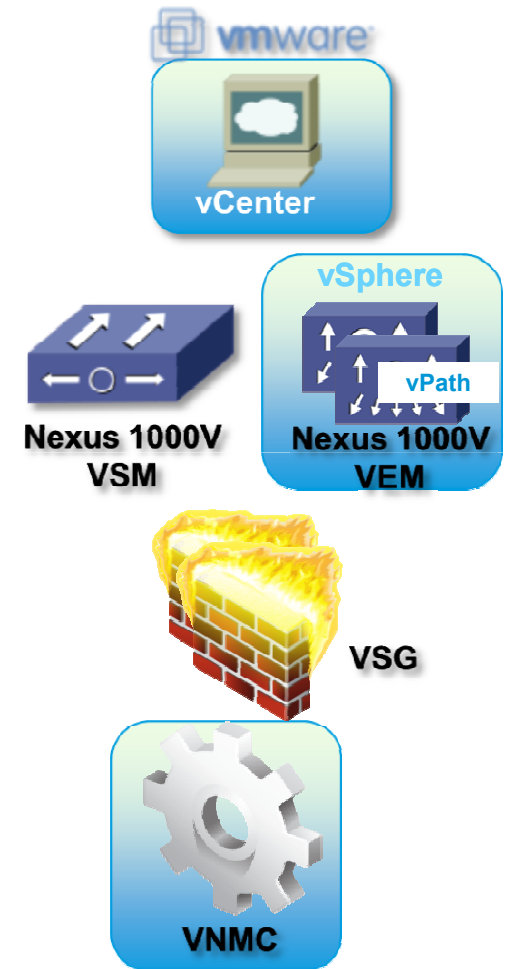
XML API, security profiles

VSG Deployment Requirements

- VMWare vSphere 4.0+ and Virtual Center
- Nexus 1000V Series switch (1.4 or later)
- One (or More) Active VSGs per tenant
- Virtual Network Management Center (VNMC)

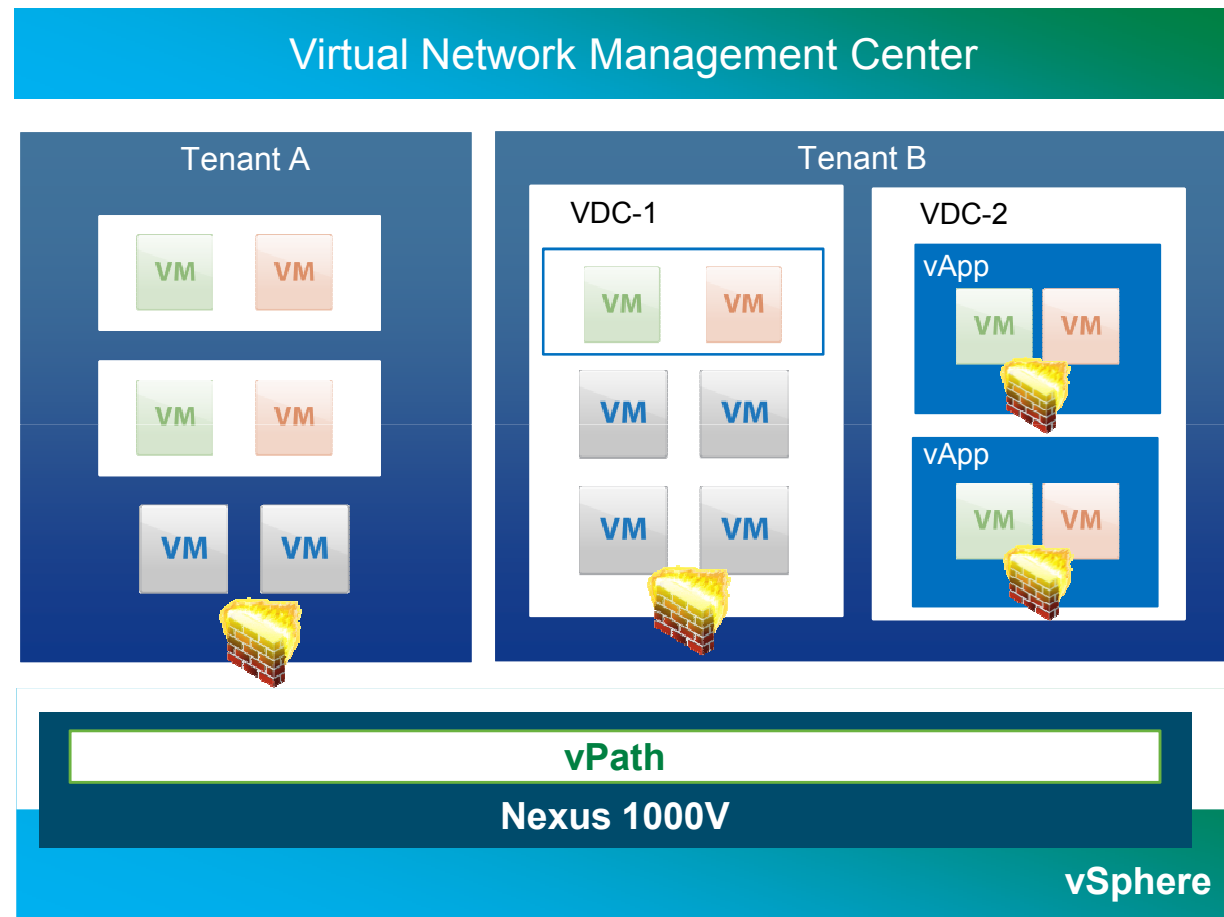
Note: Licensing is based on per protected CPU socket (same as Nexus 1000V)

VSG can protect subset of 1000V-licensed CPUs.



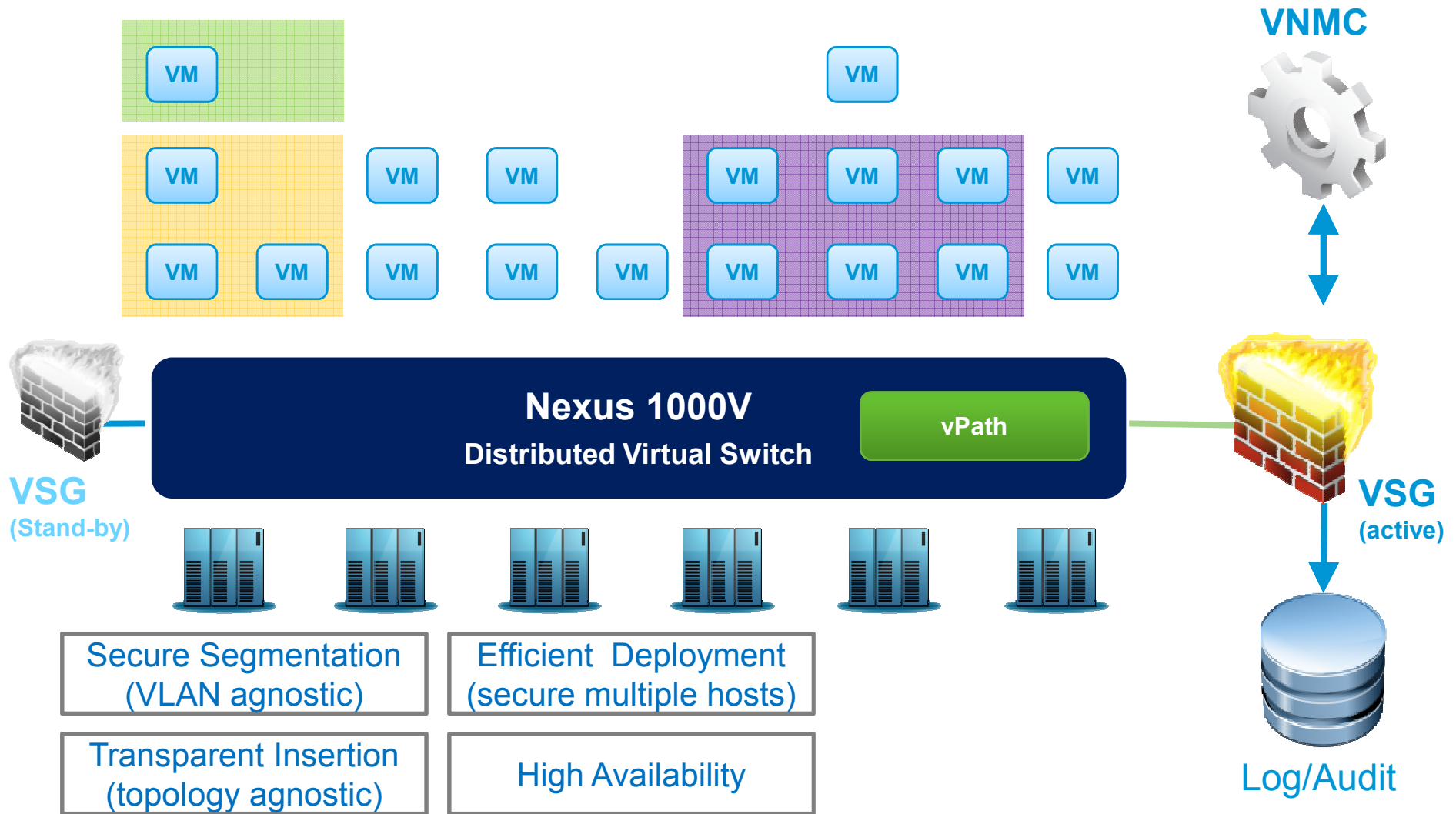
Multi-Tenant Deployment

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



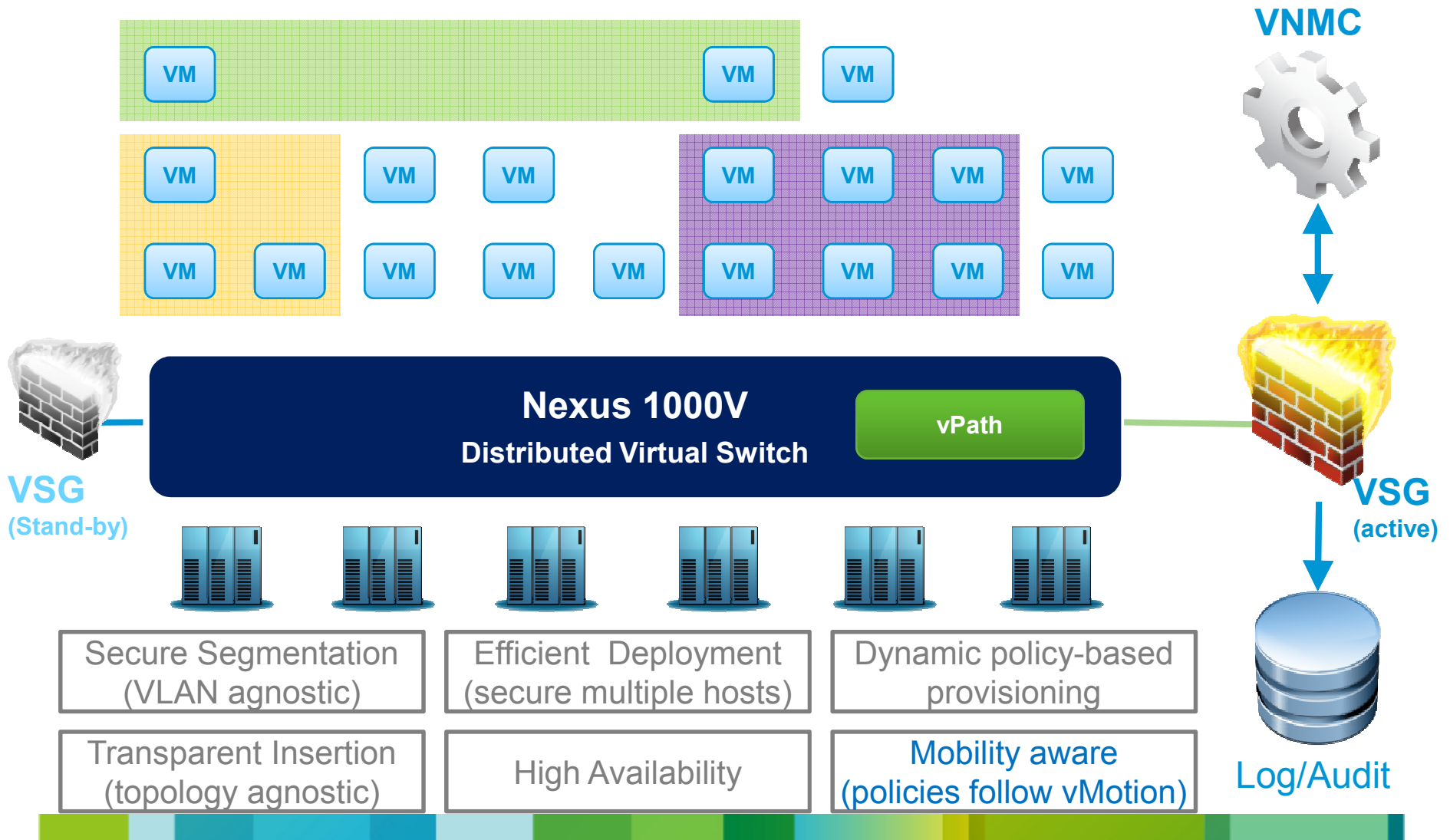
Virtual Security Gateway for Nexus 1000V

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



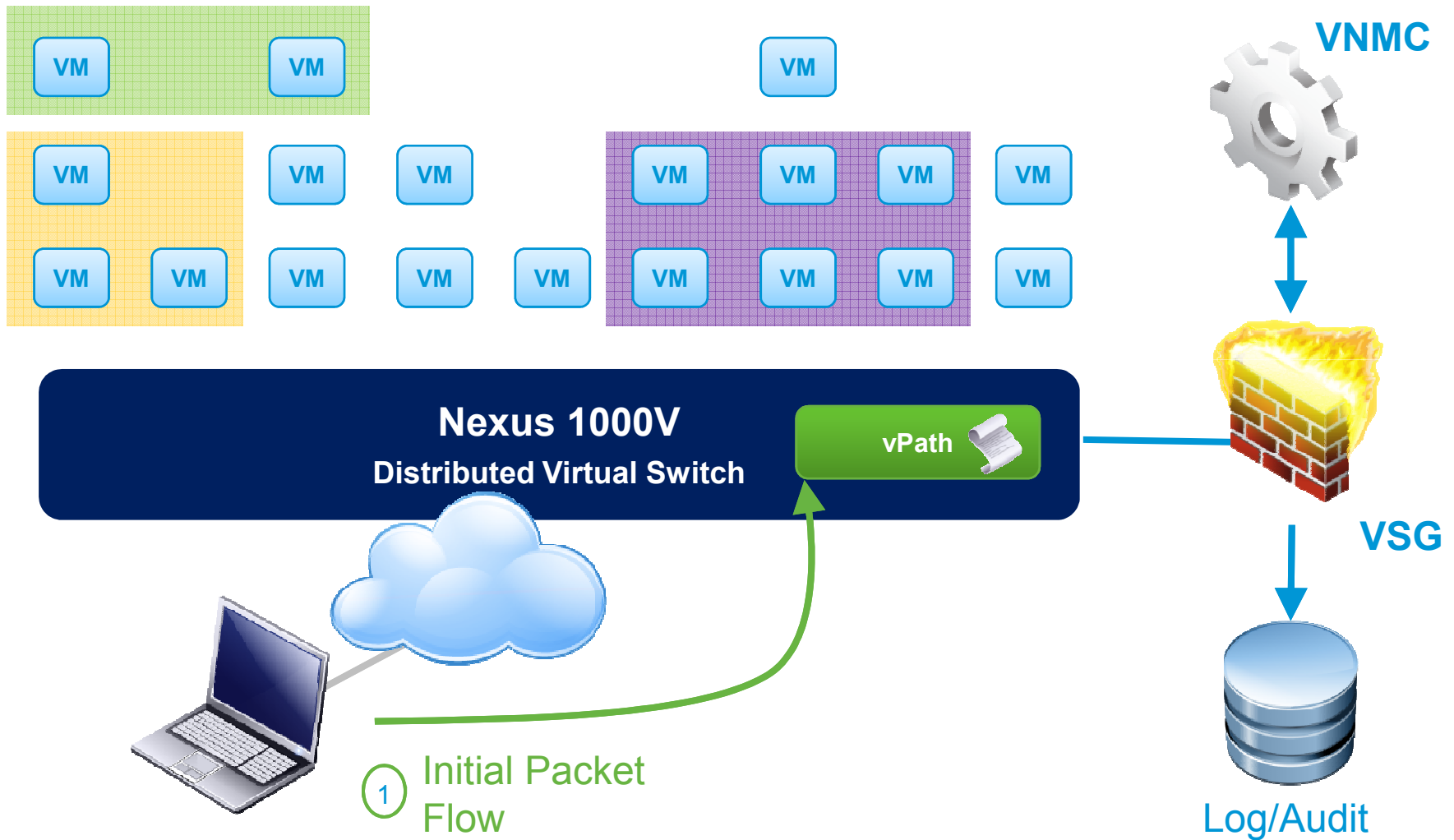
Virtual Security Gateway for Nexus 1000V

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



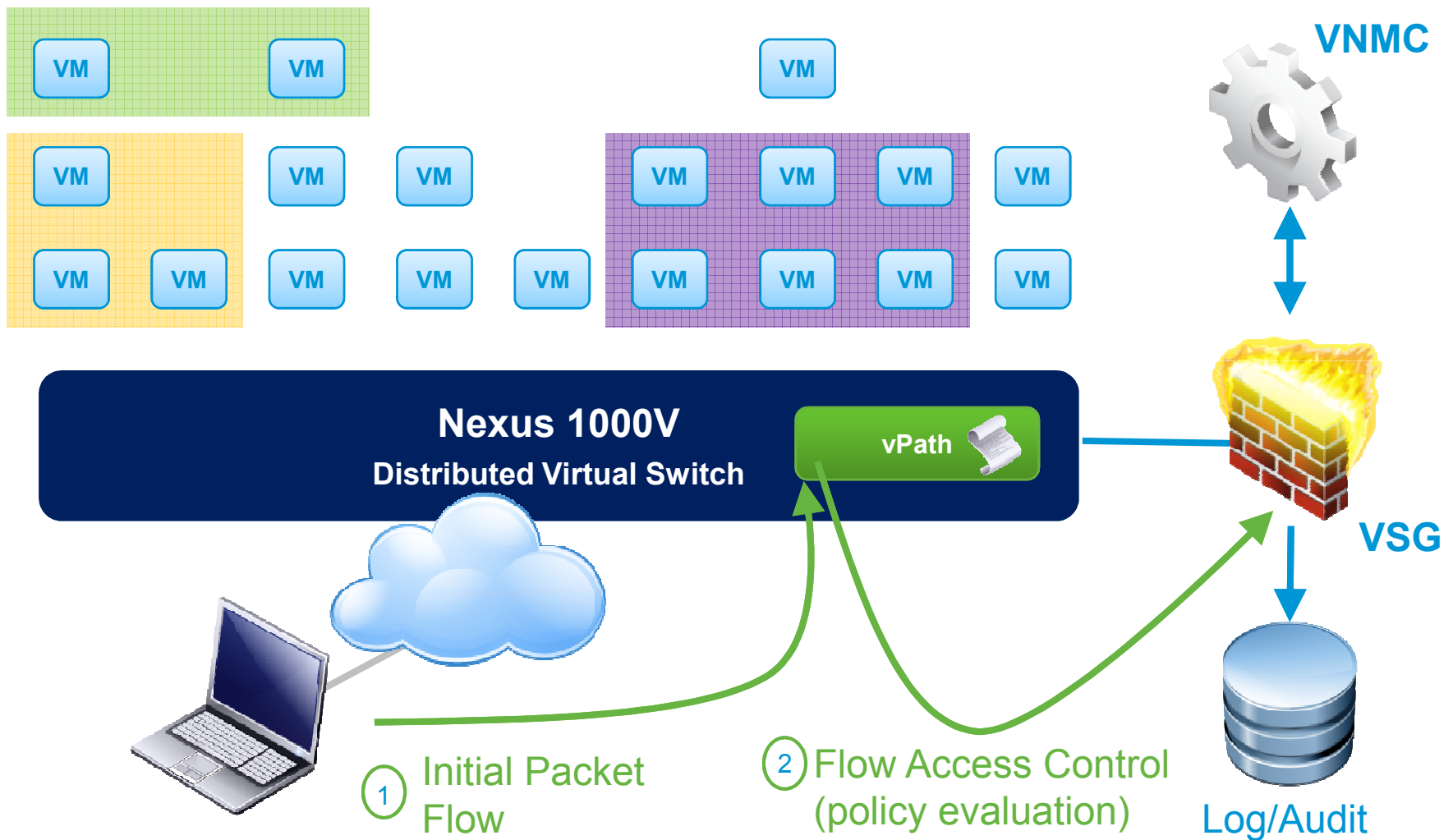
Virtual Security Gateway

Intelligent Traffic Steering with vPath



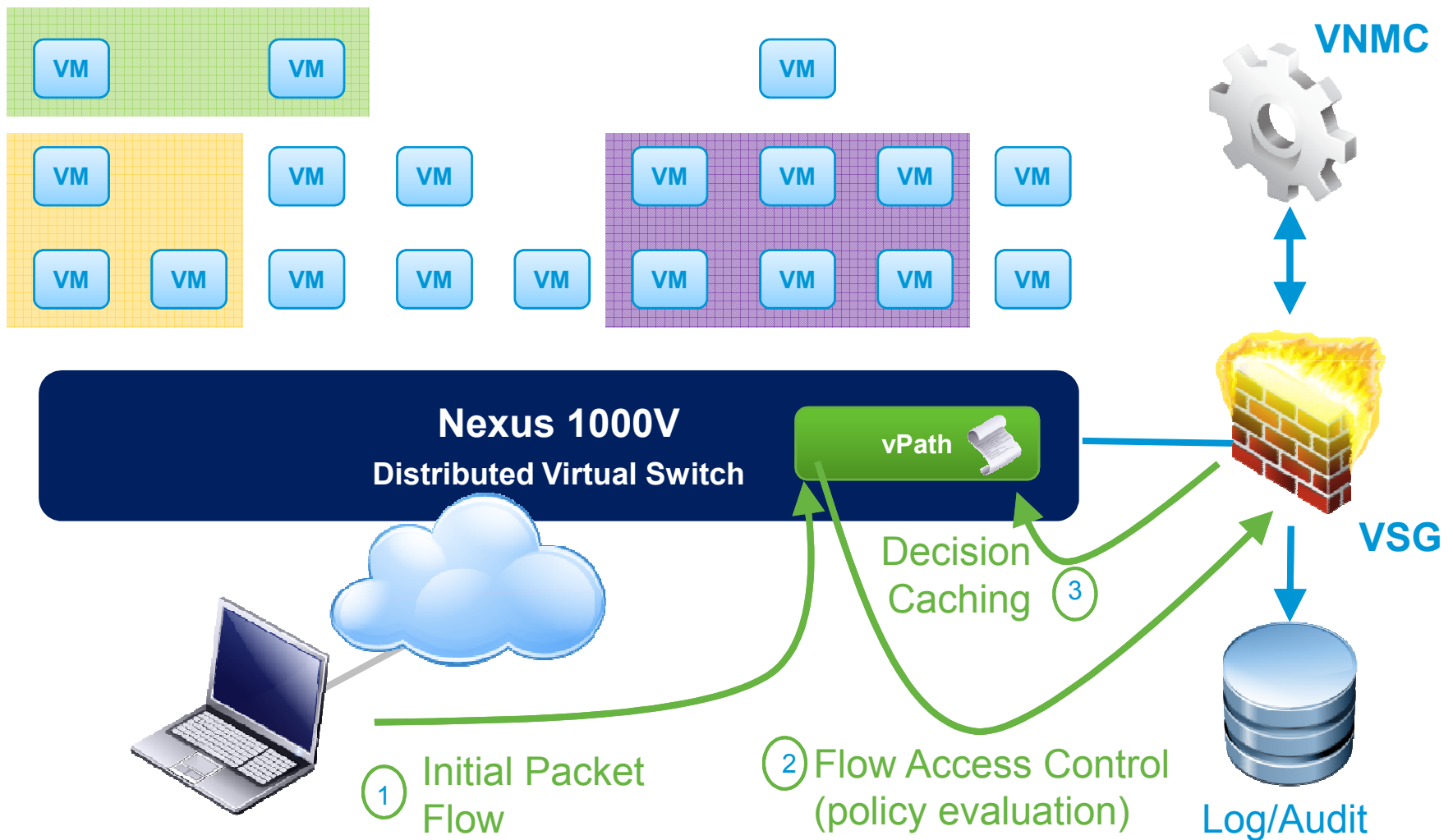
Virtual Security Gateway

Intelligent Traffic Steering with vPath



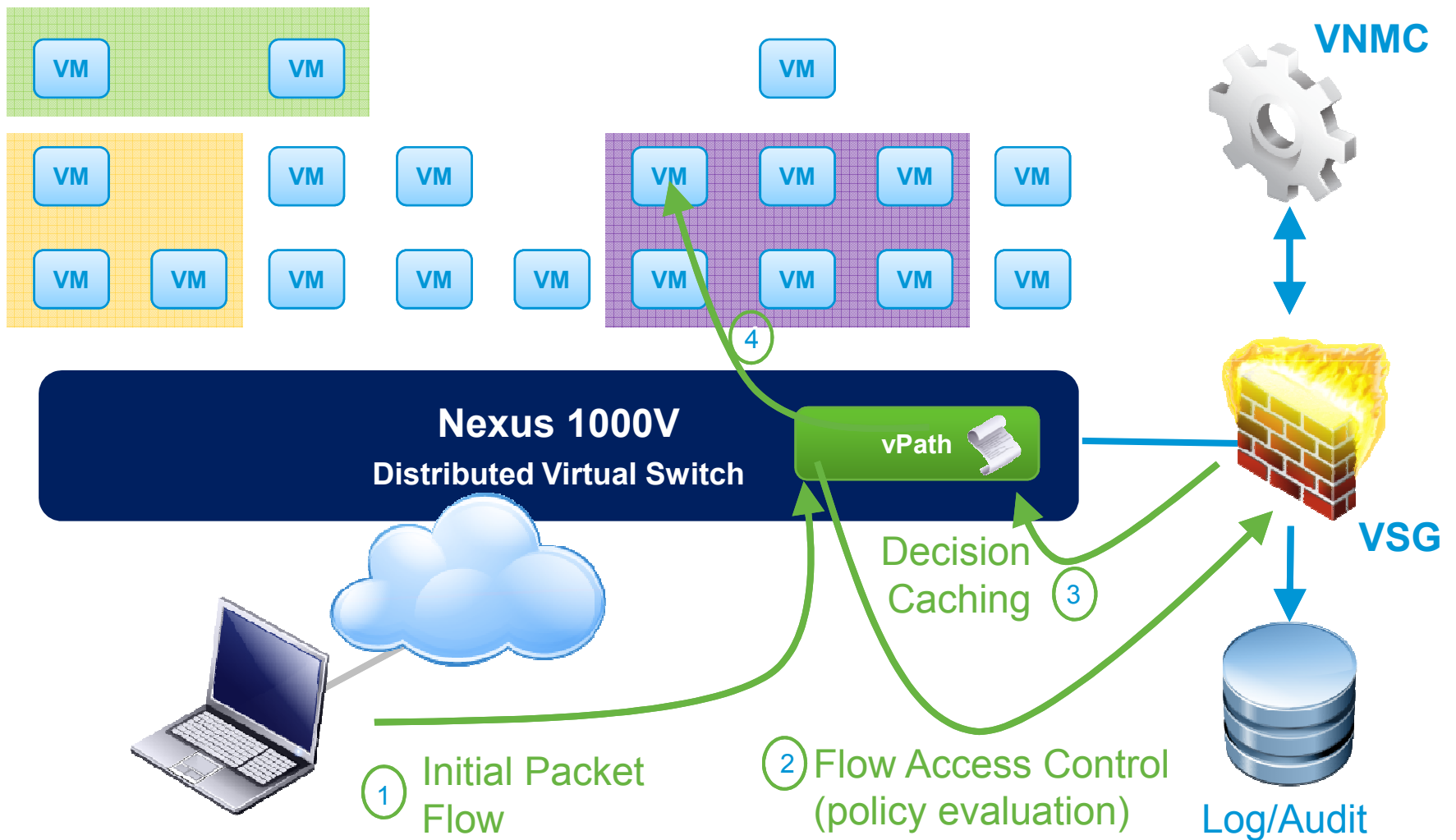
Virtual Security Gateway

Intelligent Traffic Steering with vPath



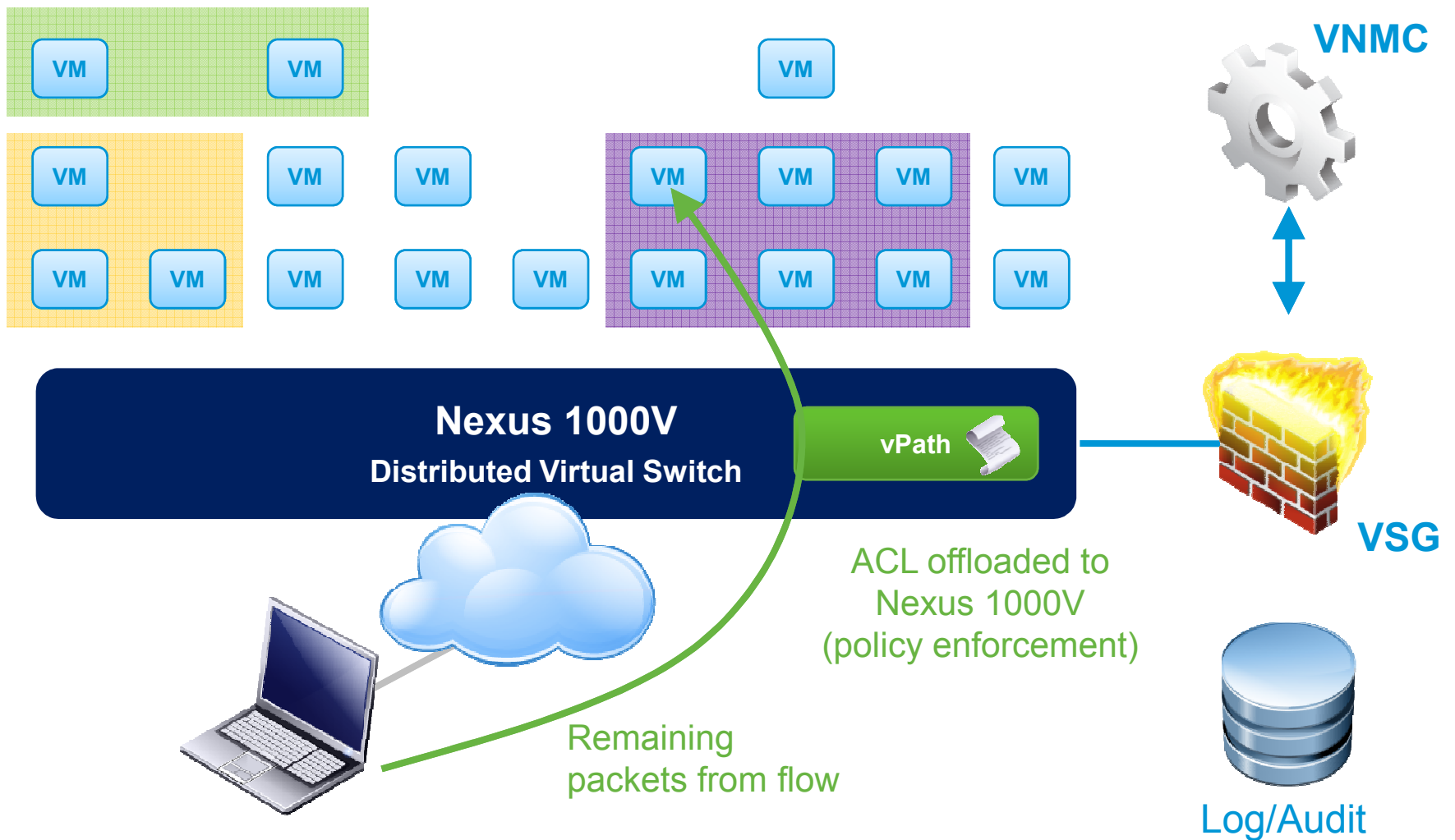
Virtual Security Gateway

Intelligent Traffic Steering with vPath



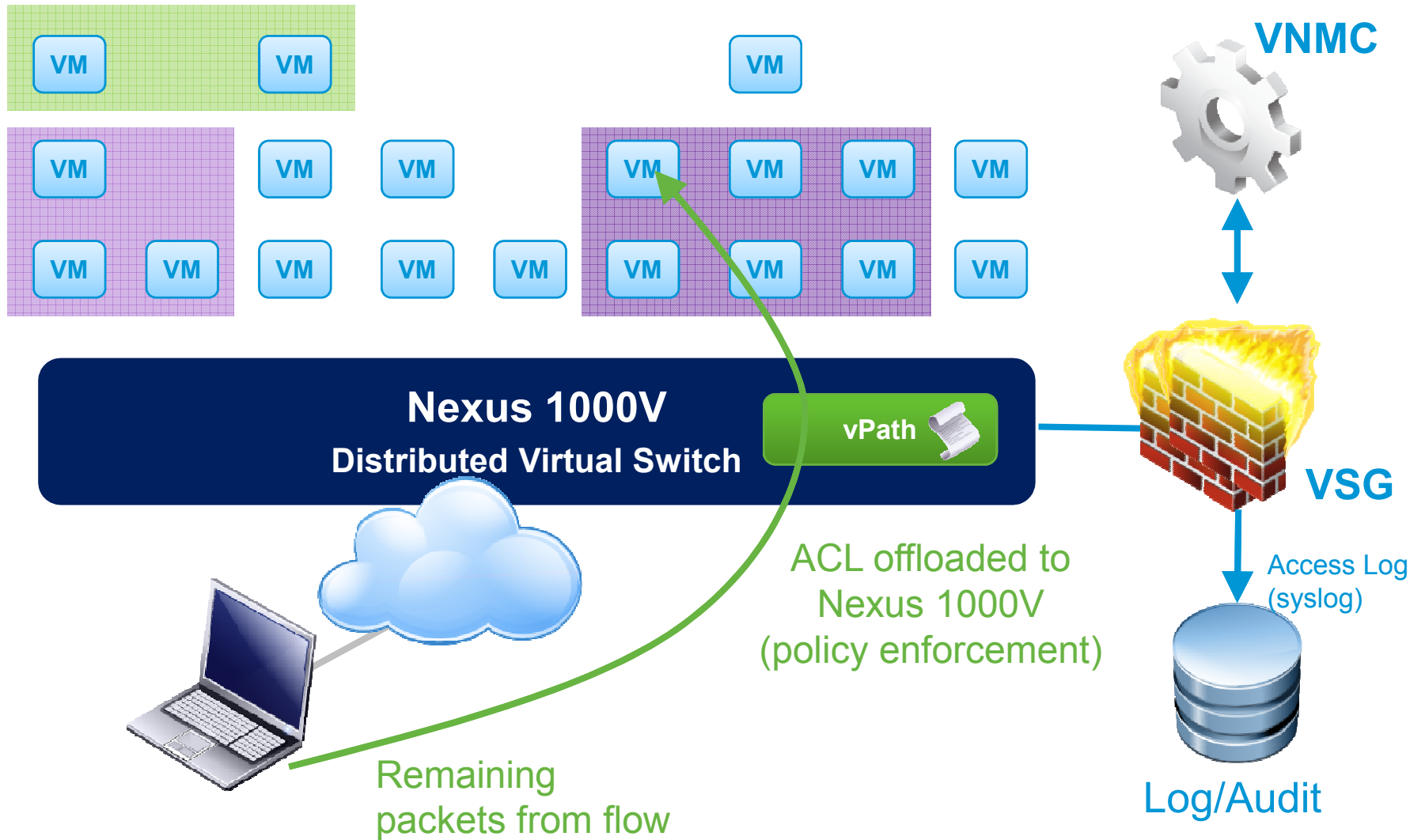
Virtual Security Gateway

Performance Acceleration with vPath



Virtual Security Gateway

Performance Acceleration with vPath

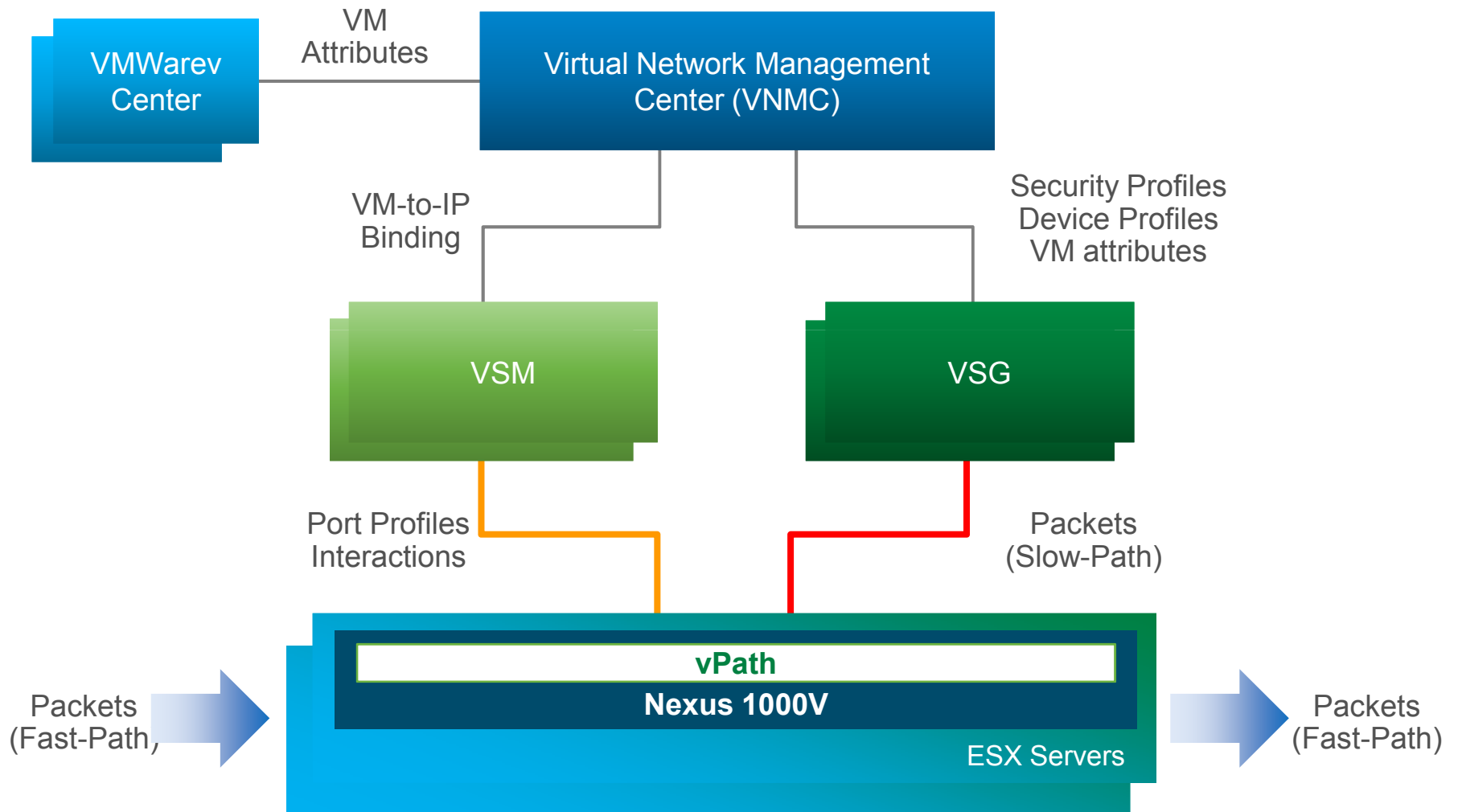


vPath—Summary

- vPath is intelligence build into Virtual Ethernet Module (**VEM**) of N1KV (1.4 and above)
- vPath has two main functions:
 - a. Intelligent Traffic Steering to VSG
 - b. Offload the processing from VSG to VEM
- Dynamic Security Policy Provisioning (via security profile)
- vPath is Multi-tenant Aware
- Leveraging vPath enhances the service performance by moving the processing to Hypervisor



VSG System Architecture

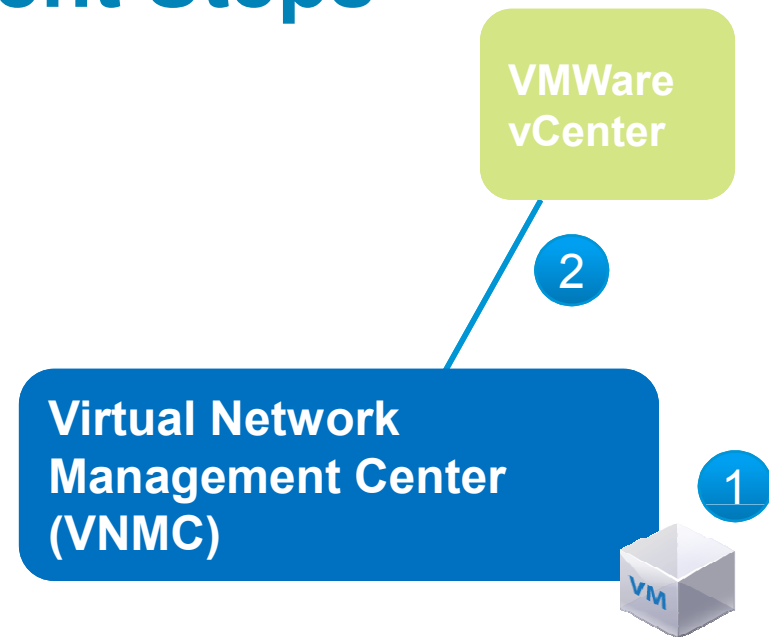


VSG Installation Steps



VSG/VNMC Deployment Steps

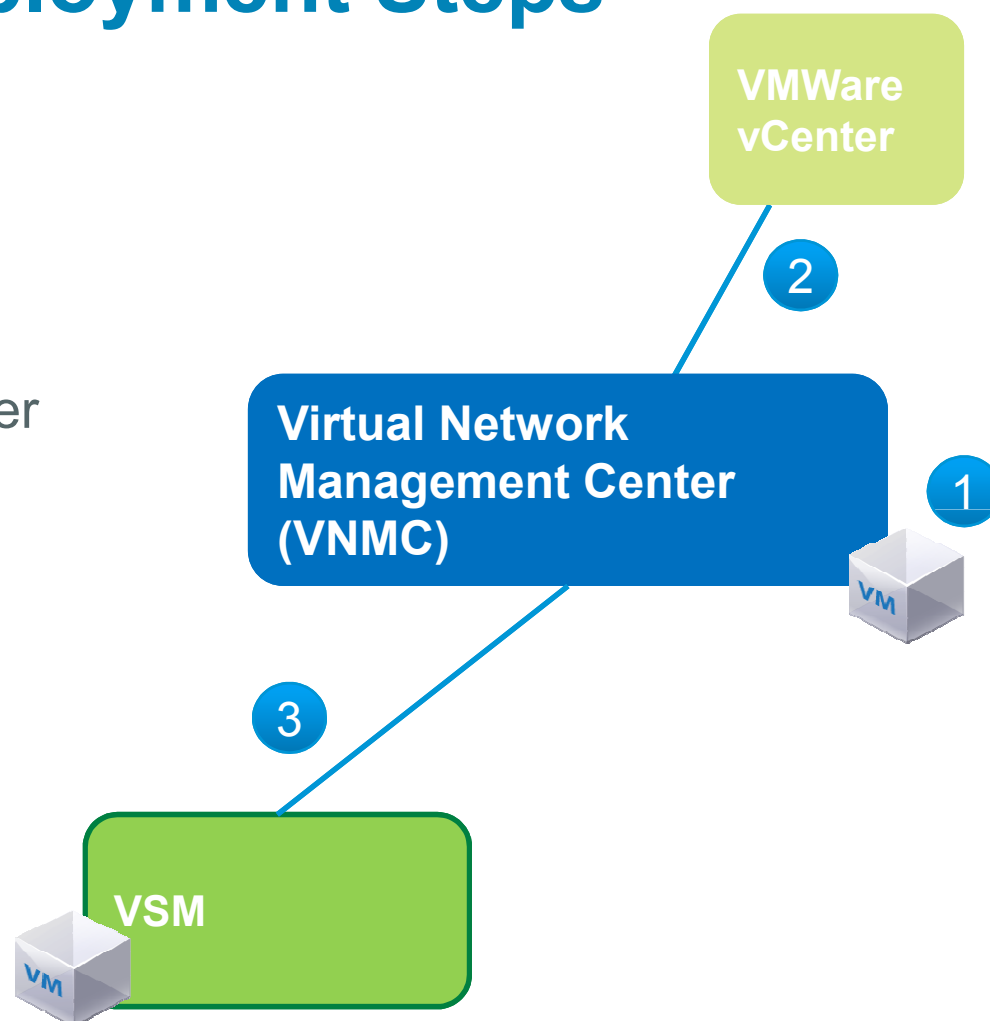
- 1) Install VNMC
- 2) Register VNMC to vCenter



Note: vCenter, vSphere and Nexus 1000V (VSM & VEMs) are assumed to be already installed;
VSM can be a VM or on Nexus 1010

VSG/VNMC Deployment Steps

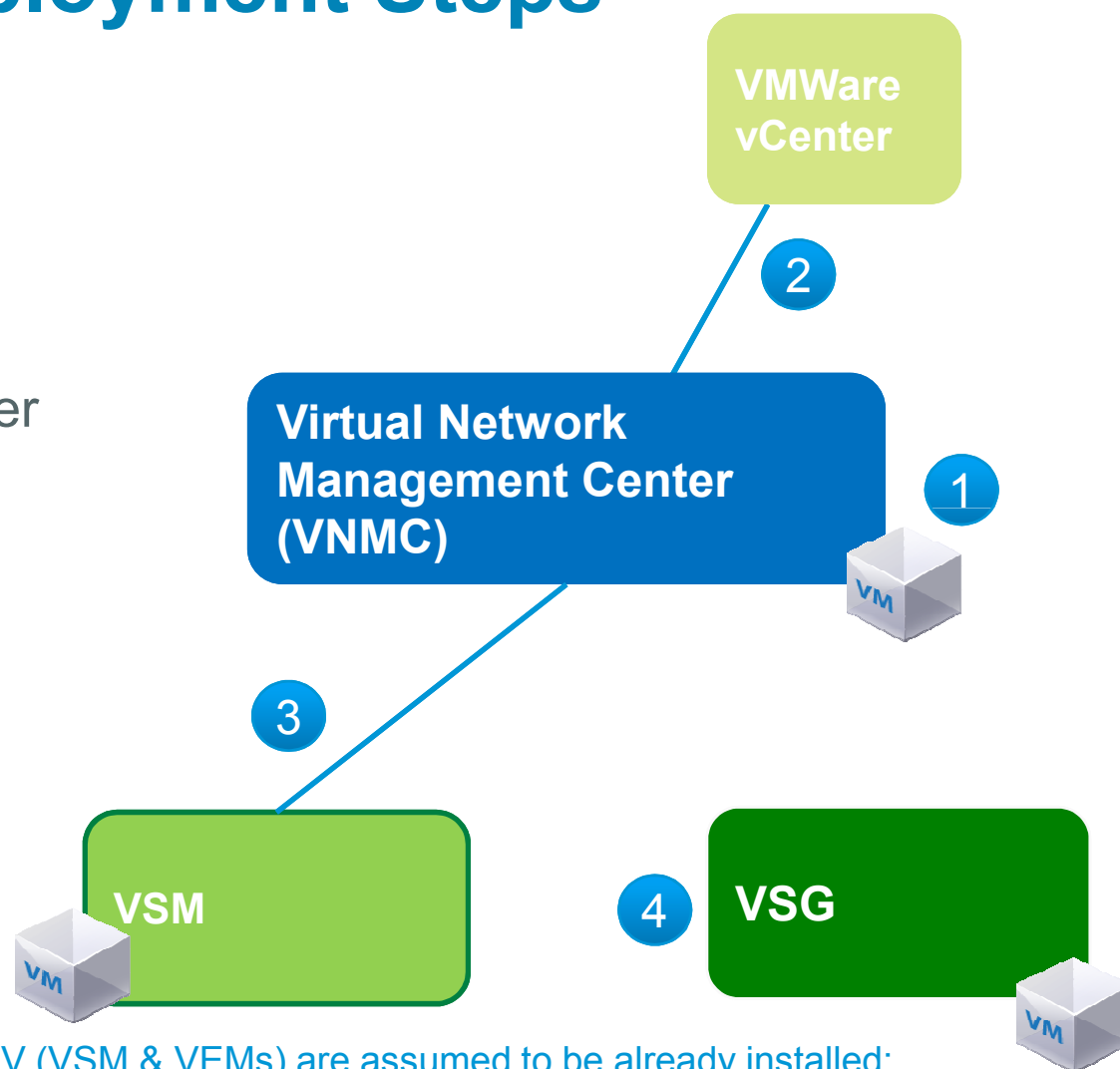
- 1) Install VNMC
- 2) Register VNMC to vCenter
- 3) Register VSM to VNMC



Note: vCenter, vSphere and Nexus 1000V (VSM & VEMs) are assumed to be already installed;
VSM can be a VM or on Nexus 1010

VSG/VNMC Deployment Steps

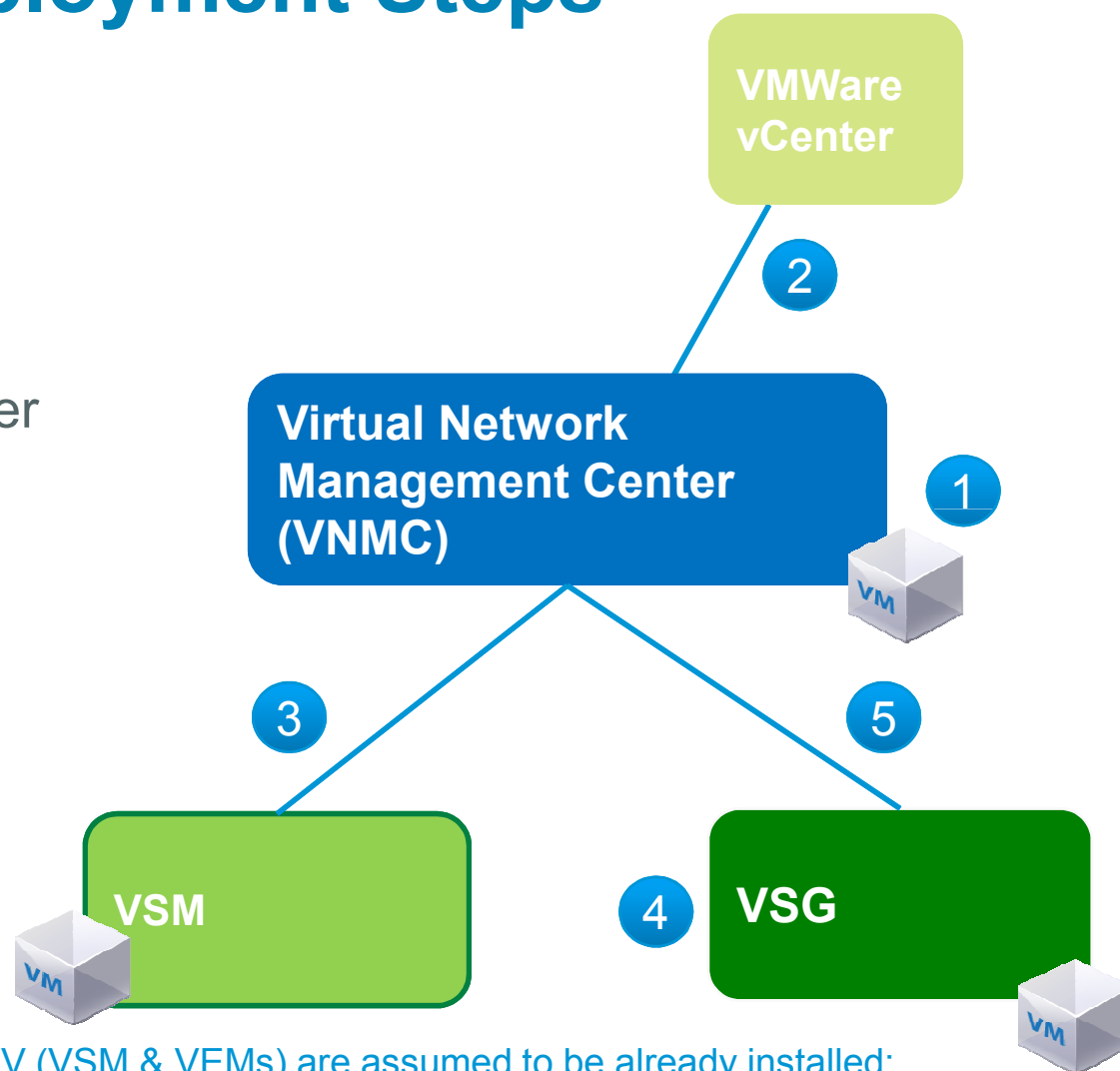
- 1) Install VNMC
- 2) Register VNMC to vCenter
- 3) Register VSM to VNMC
- 4) Install VSG



Note: vCenter, vSphere and Nexus 1000V (VSM & VEMs) are assumed to be already installed;
VSM can be a VM or on Nexus 1010

VSG/VNMC Deployment Steps

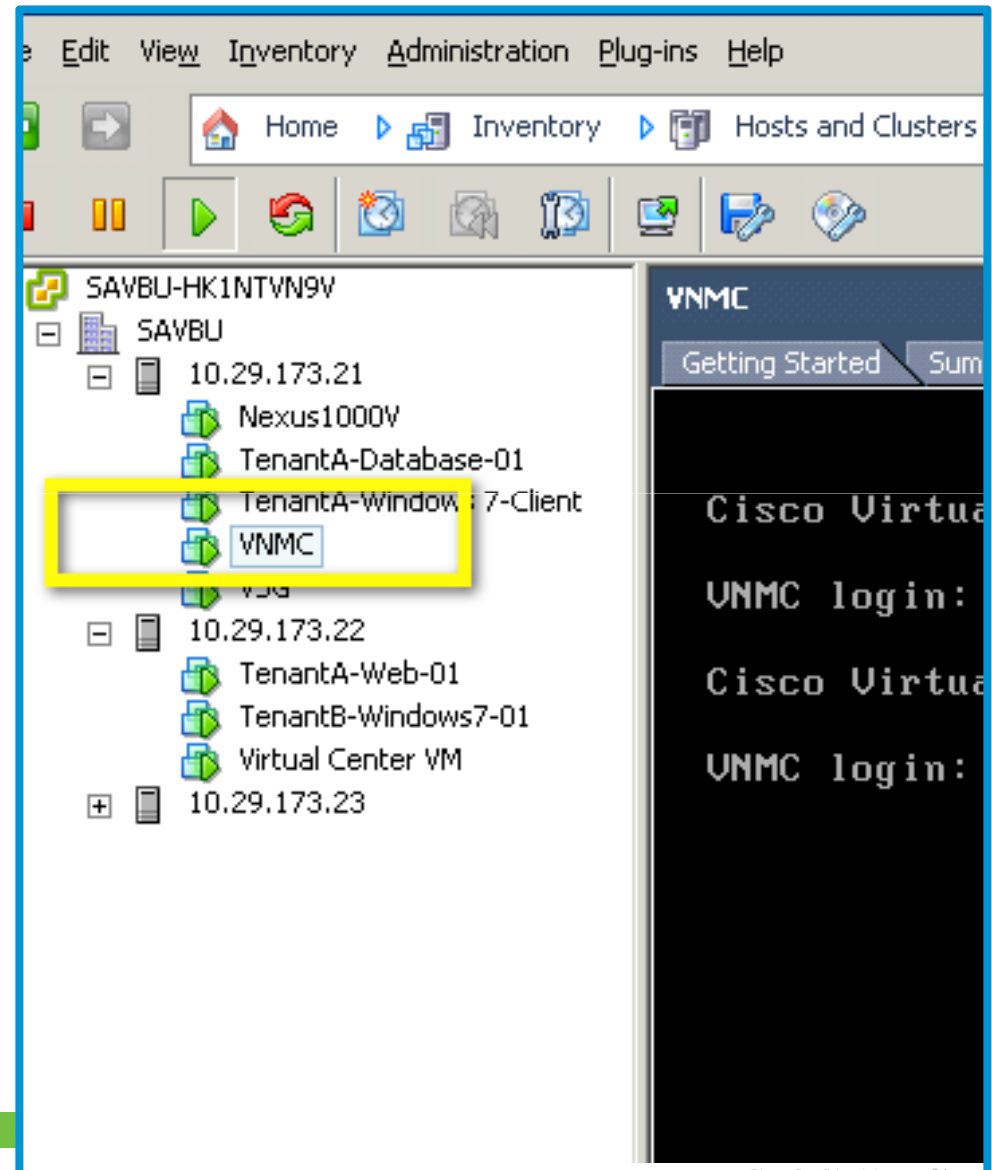
- 1) Install VNMC
- 2) Register VNMC to vCenter
- 3) Register VSM to VNMC
- 4) Install VSG
- 5) Register VSG to VNMC



Note: vCenter, vSphere and Nexus 1000V (VSM & VEMs) are assumed to be already installed;
VSM can be a VM or on Nexus 1010

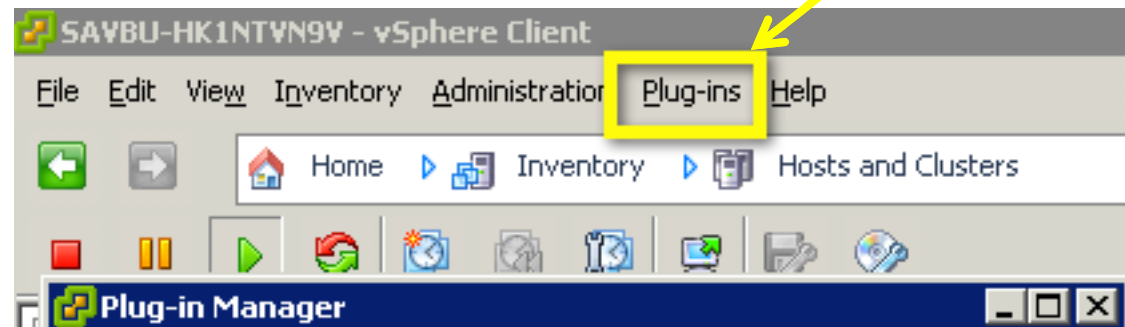
Deployment Step 1: Install VNMC

- Install VNMC as a Virtual Appliance in vCenter
- Installed as OVA or ISO image



Deployment Step 2: Register VNMC

- Register the VNMC to vCenter
- vCenter Extension File installed via vCenter Plug-in
- Similar to VSM integration with vCenter



Deployment Step 3: Register VSM

- Register VSM to VNMC via Policy Agent
- VNMC gets the VM to IP Mapping from VSM

Registration Steps

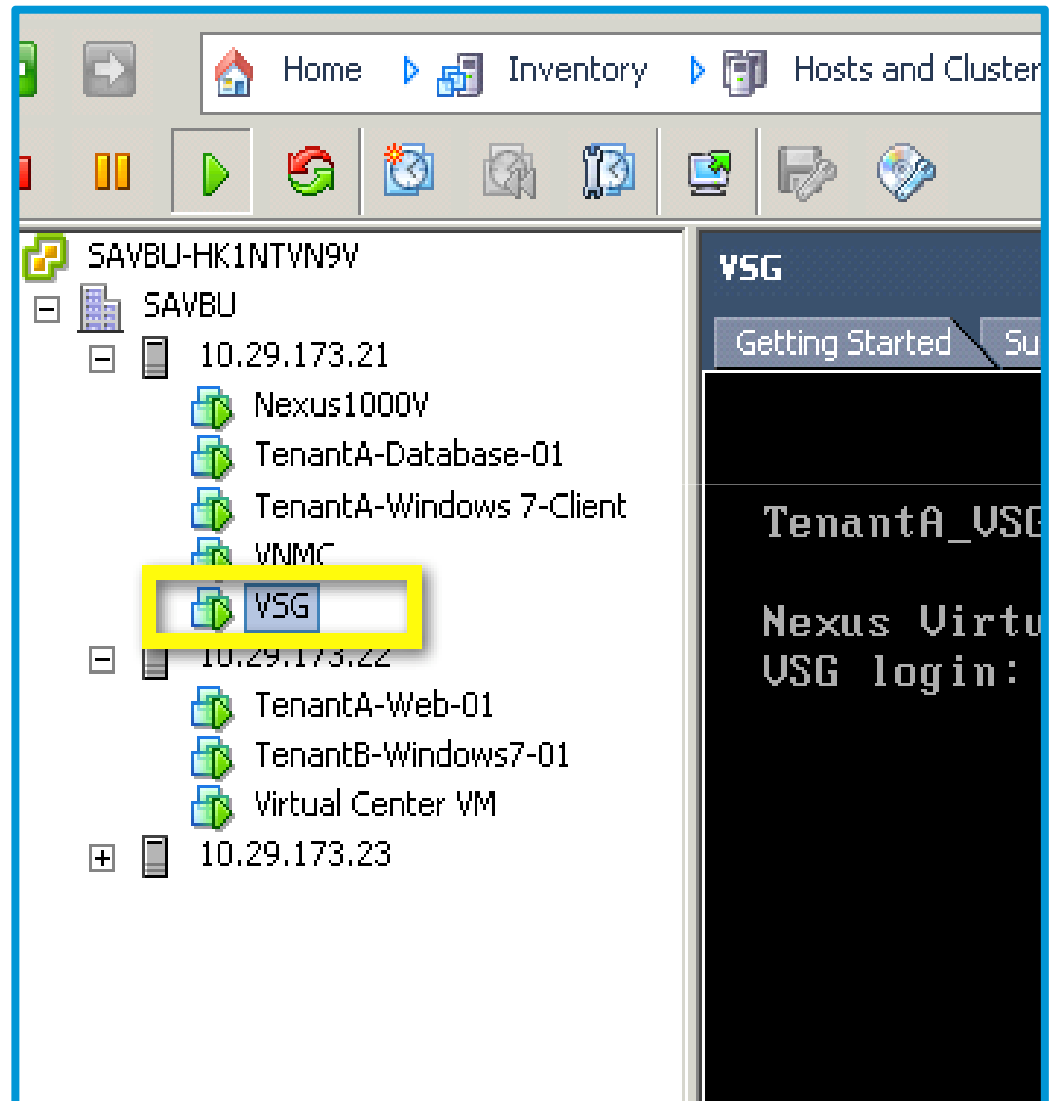
```
vnm-policy-agent
registration-ip 10.29.173.52
shared-secret *****
policy-agent-image bootflash:/vnmc-vsmpa.1.0.1f.bin
log-level
```

```
VSM-Nexus1000V# sh vnm-pa status
VNM Policy-Agent status is - Installed Successfully.
Version 1.0(1f)-vsm
```

Registration Status

Deployment Step 4: Install VSG

- Install VSG as a Virtual Appliance in vCenter
- Installed as OVA or ISO image



Deployment Step 5: Register VSG

- Register VSG to VNMC via Policy Agent
- Security and Device Policies are published to VSG once it is registered to VNMC

Registration Steps

```
vnm-policy-agent
registration-ip 10.29.173.52
shared-secret *****
policy-agent-image bootflash:/vnmc-vsgpa.1.0.1f.bin
log level
logging server 10.29.173.53 6 facility local0
```

```
TenantA_VSG# sh vnm-pa status
VNM Policy-Agent status is - Installed Successfully.
Version 1.0(1f)-vsg
```

Registration Status

NOTE: Registration is done as part of installing VSG via OVA Template

VSG High Availability (HA)



VSG Solution – High Availability

Component	High Availability	Behavior
VSG	Active Standby	Standby VSG takes over within 6-10 seconds
VNMC	VMware High Availability	Hardware Failures backup
VSM	Active Standby	Standby VSM takes over within 6-10 seconds

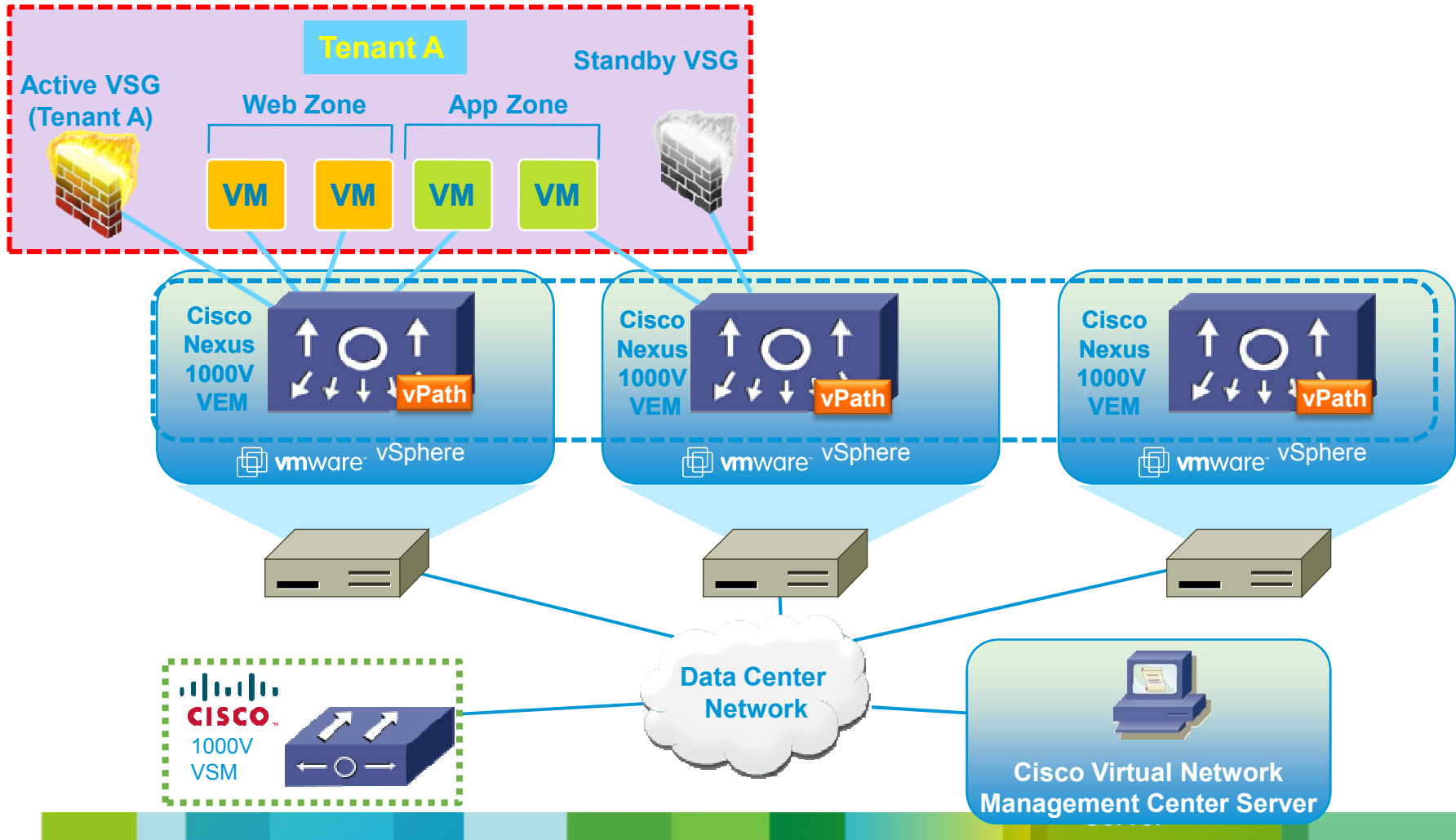
Performance/Scale

Feature	VSG	VNMC
Zones	32	4096
Access control Rules	1024	8192
Max attributes per rule	16	16
Max concurrent connections	128K in vPath 256K in VSG	N/A
Max New Connections/Sec	4K	N/A
Max VSGs	N/A	128
Max VSMs	N/A	3
Max VCs	N/A	2
Max tenants	1	128
Max VMs	300	800 – 1000 (1600 vnics)
Host scalability	12 VEMs	N/A
Max Security Profiles	256	2048

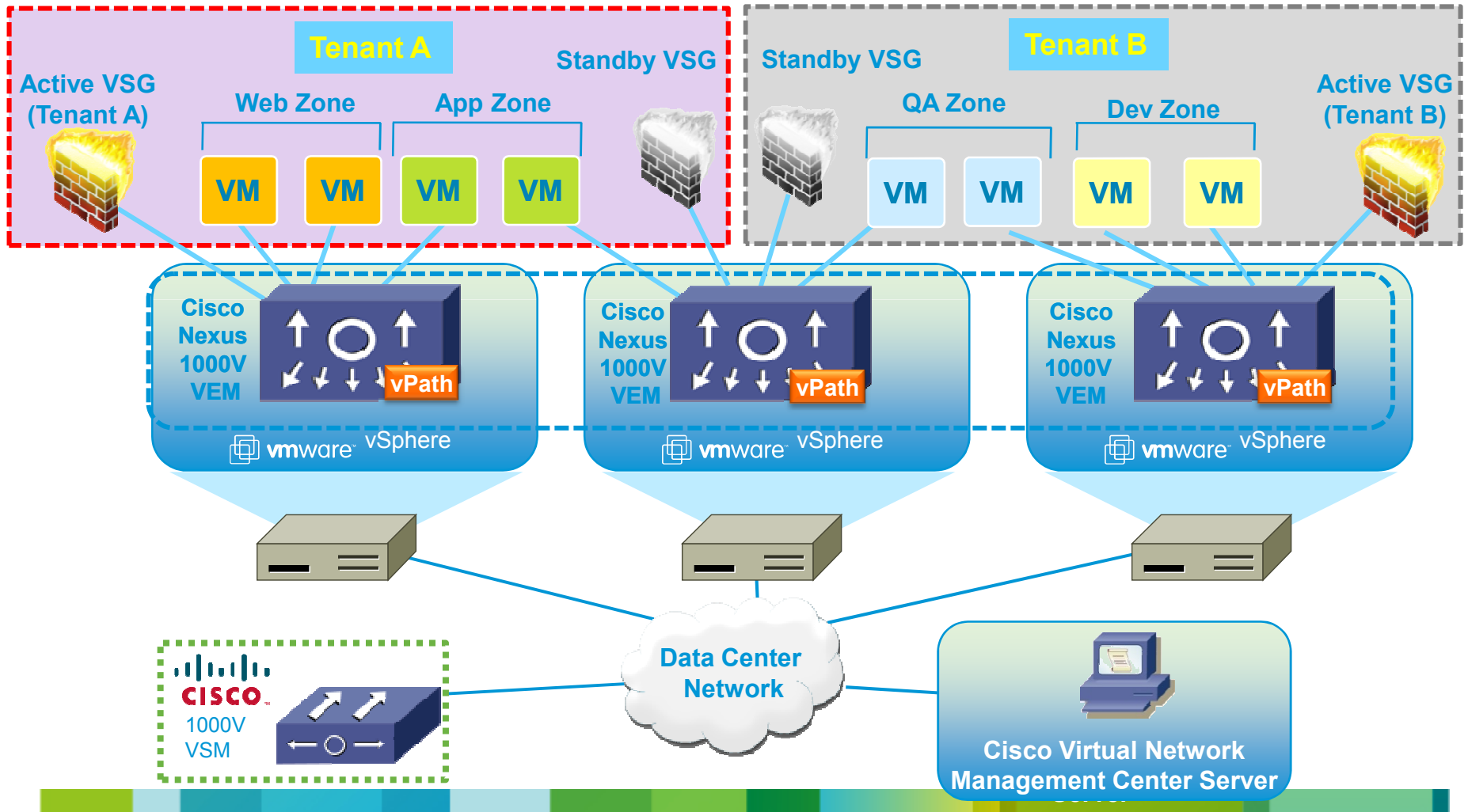
VSG Deployment Scenario



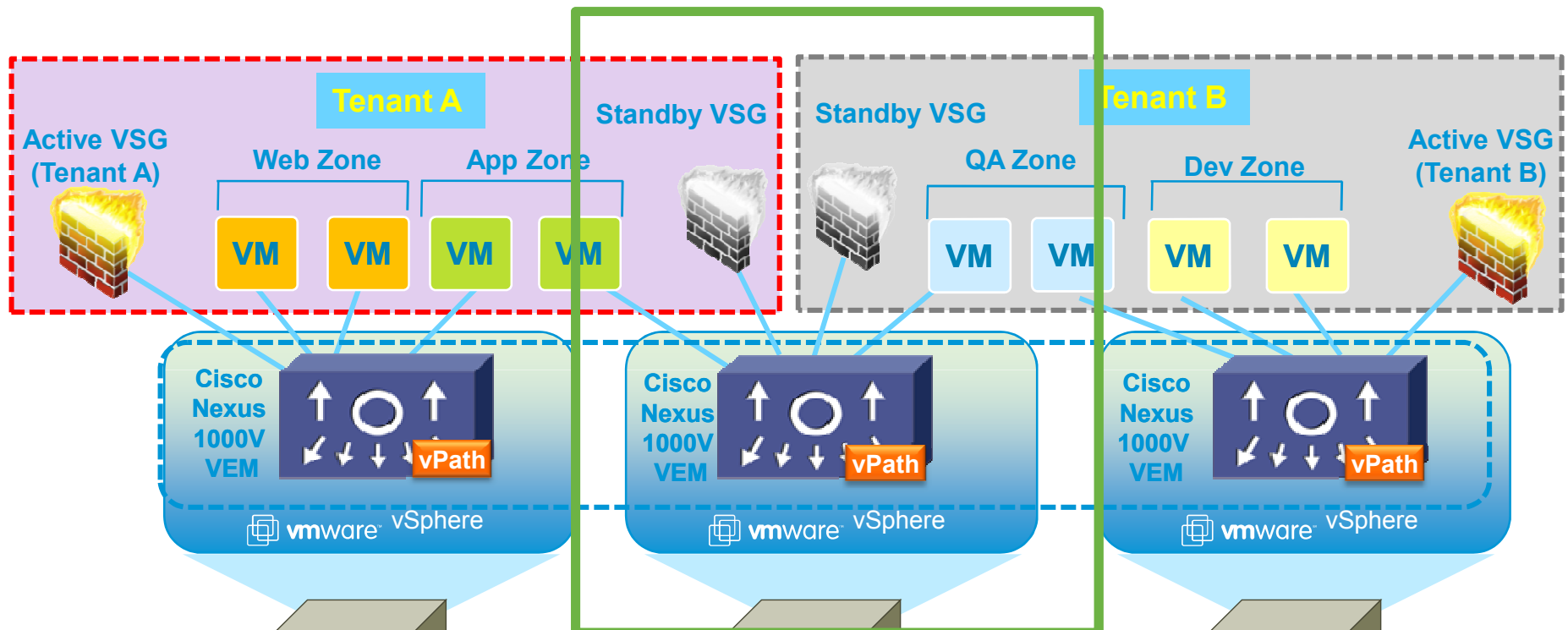
Deployment in Multitenant Environment



Deployment in Multitenant Environment

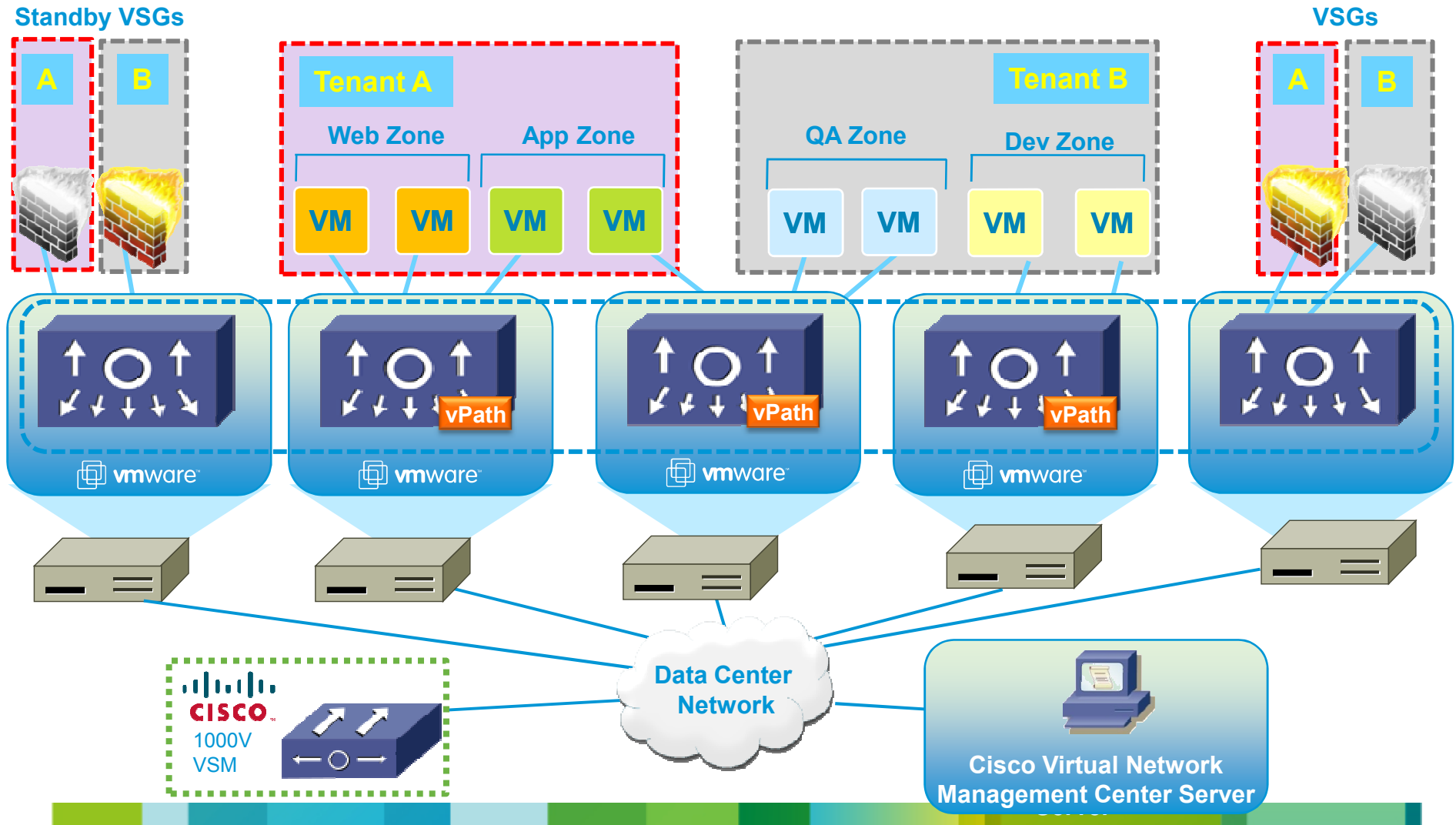


Deployment in Multitenant Environment

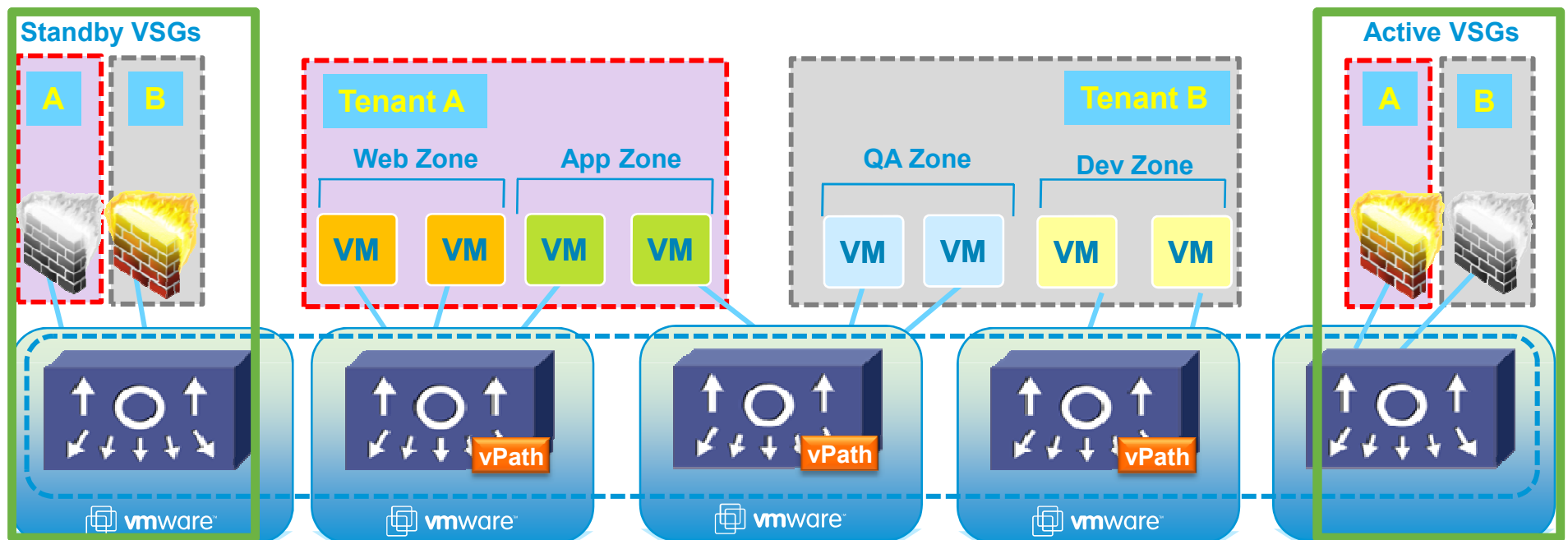


- Security Policies Enforced on Shared Compute Environment
- vPath Multitenant Aware
- Active Stand by VSGs on different Physical Host

Deployment VSGs on Dedicated Host



Deployment VSGs on Dedicated Host



- Dedicated Servers to host VSG Appliances
- Decouple Service from Compute Resources
- Easy to scale out with dedicated hosting of Service

Cisco Virtual Network
Management Center Server

VSG Security Policy Model

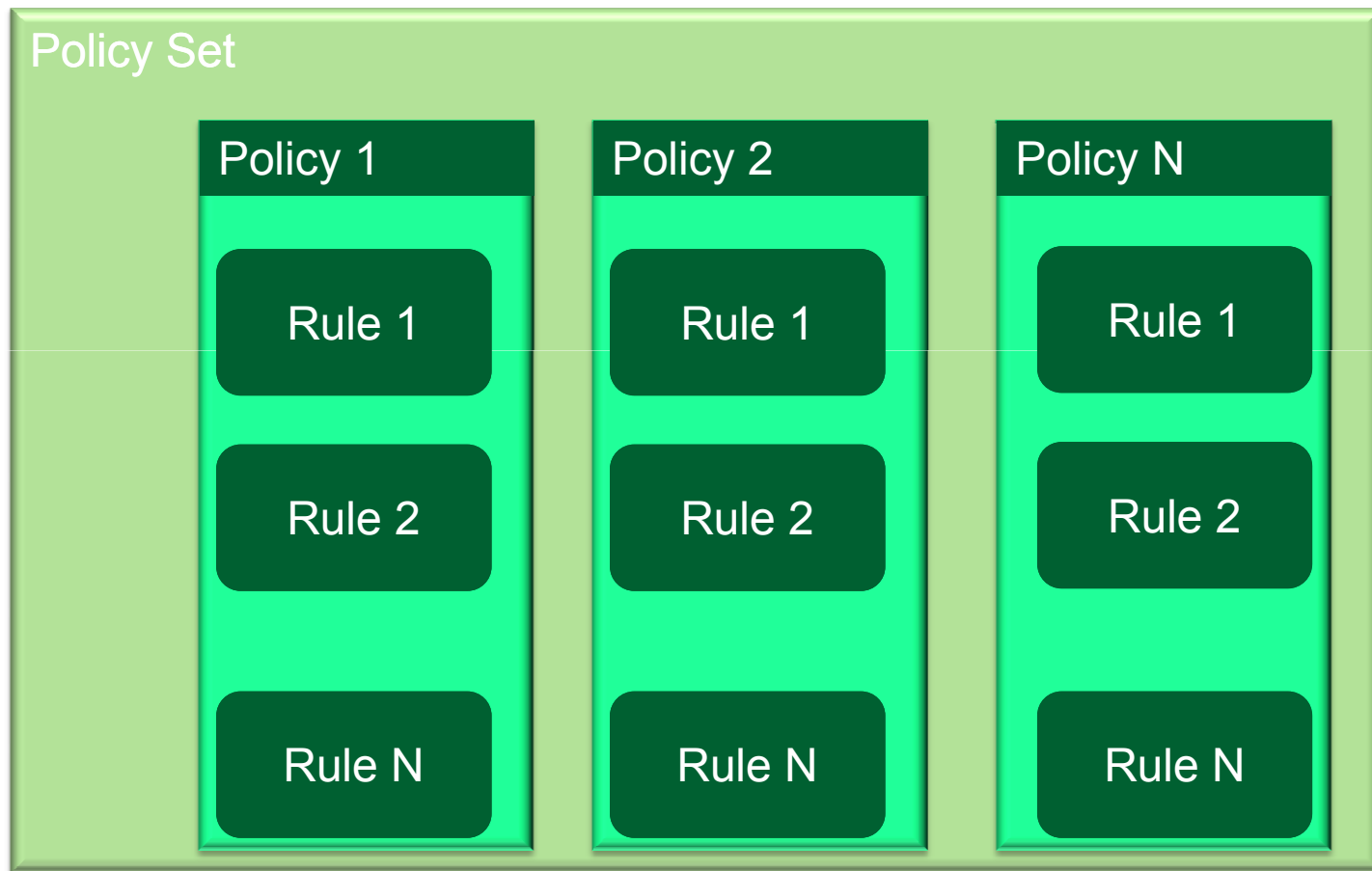


Security Policy Building Block



Rule is analogous to an ACE; Policy is analogous to an ACL

Security Policy Building Block



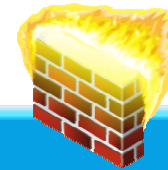
Rule is analogous to an ACE; Policy is analogous to an ACL

Security Policy Building Block



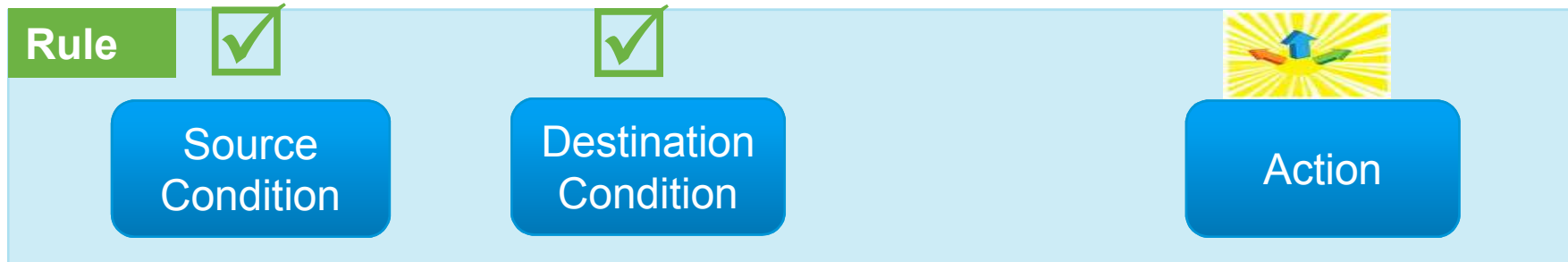
Rule is analogous to an ACE; Policy is analogous to an ACL

Security Policy Building Block

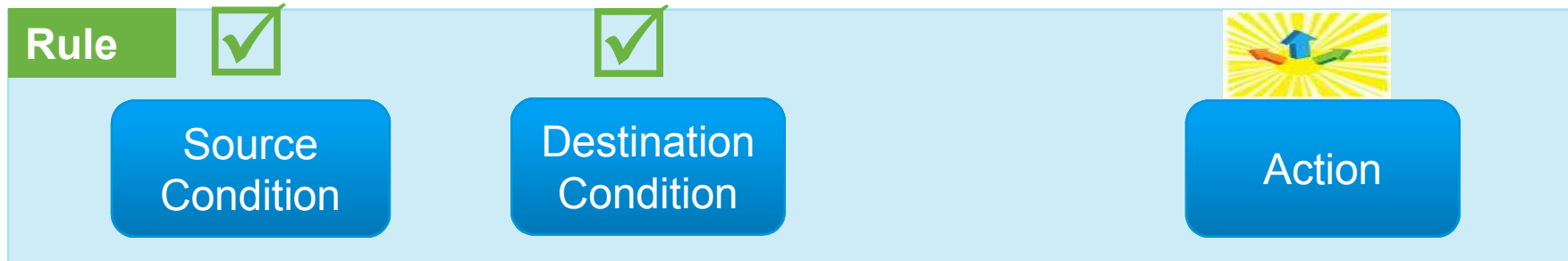


Rule is analogous to an ACE; Policy is analogous to an ACL

VSG Policy: Rule (ACE) Construct

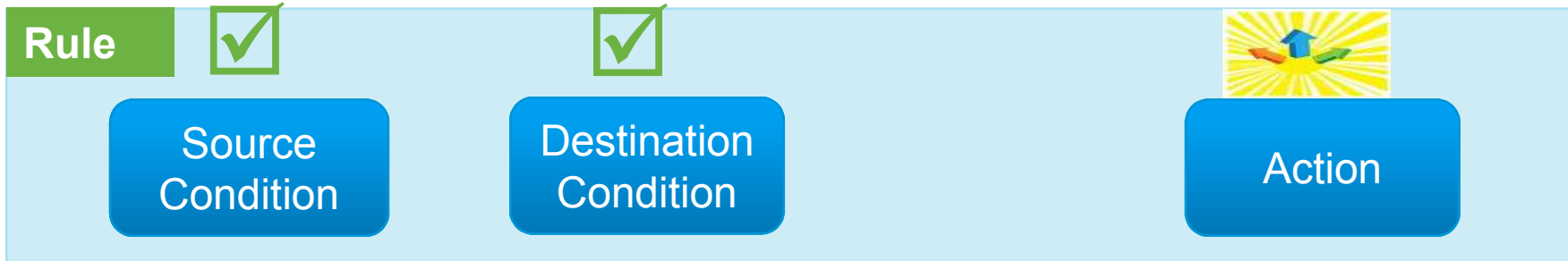


VSG Policy: Rule (ACE) Construct



The screenshot shows the 'Condition' configuration interface. A blue button labeled 'Condition' is at the top left. Below it, the 'Attribute Type' is set to 'Network' in a dropdown menu. An arrow points from this dropdown to a list of options: 'Network', 'VM', and 'Custom'. The 'Expression' section contains three fields: 'Attribute Name' is 'IP Address', 'Operator' is 'eq', and 'Attribute Value' is '192 . 168 . 1 . 2'.

VSG Policy: Rule (ACE) Construct



Condition

Attribute Type:

Expression

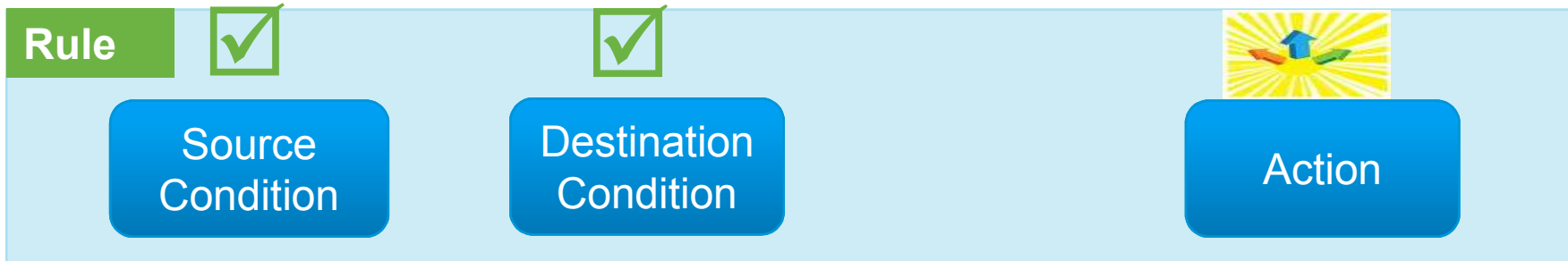
Attribute Name: Operator: Attribute Value:

- Attribute Type**
- Network
 - VM
 - Custom

- 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

VSG Policy: Rule (ACE) Construct



Condition

Attribute Type : ▼

Expression

Attribute Name : ▼ Operator : ▼ Attribute Value :

Attribute Type
Network
VM
Custom

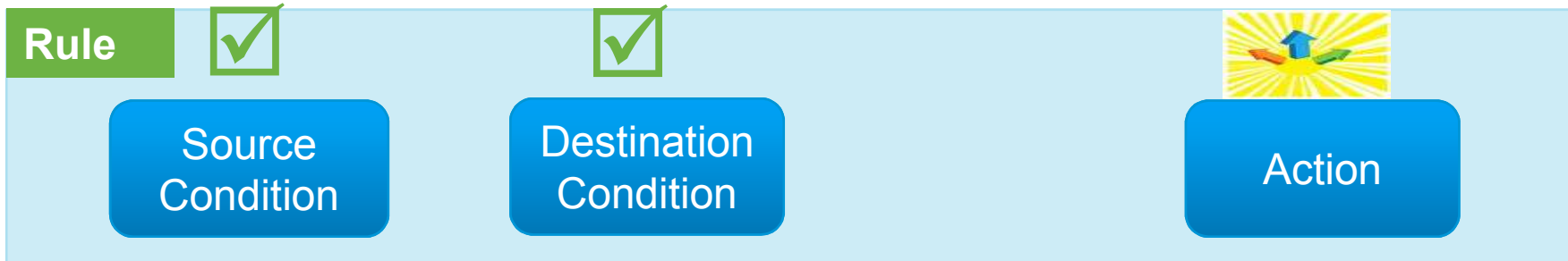
VM Attributes
Instance Name
Guest OS full name
Zone Name
Parent App Name
Port Profile Name
Cluster Name
Hypervisor Name

Network Attributes
IP Address
Network Port

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

Operator
member
Not-member
Contains

VSG Policy: Rule (ACE) Construct



The screenshot shows the configuration interface for a 'Condition'. The 'Attribute Type' is set to 'Network'. The 'Expression' section includes 'Attribute Name' (IP Address), 'Operator' (eq), and 'Attribute value' (192.168.1.2). The 'Action to take' section has 'drop' selected, 'permit' selected, and 'log' checked.

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

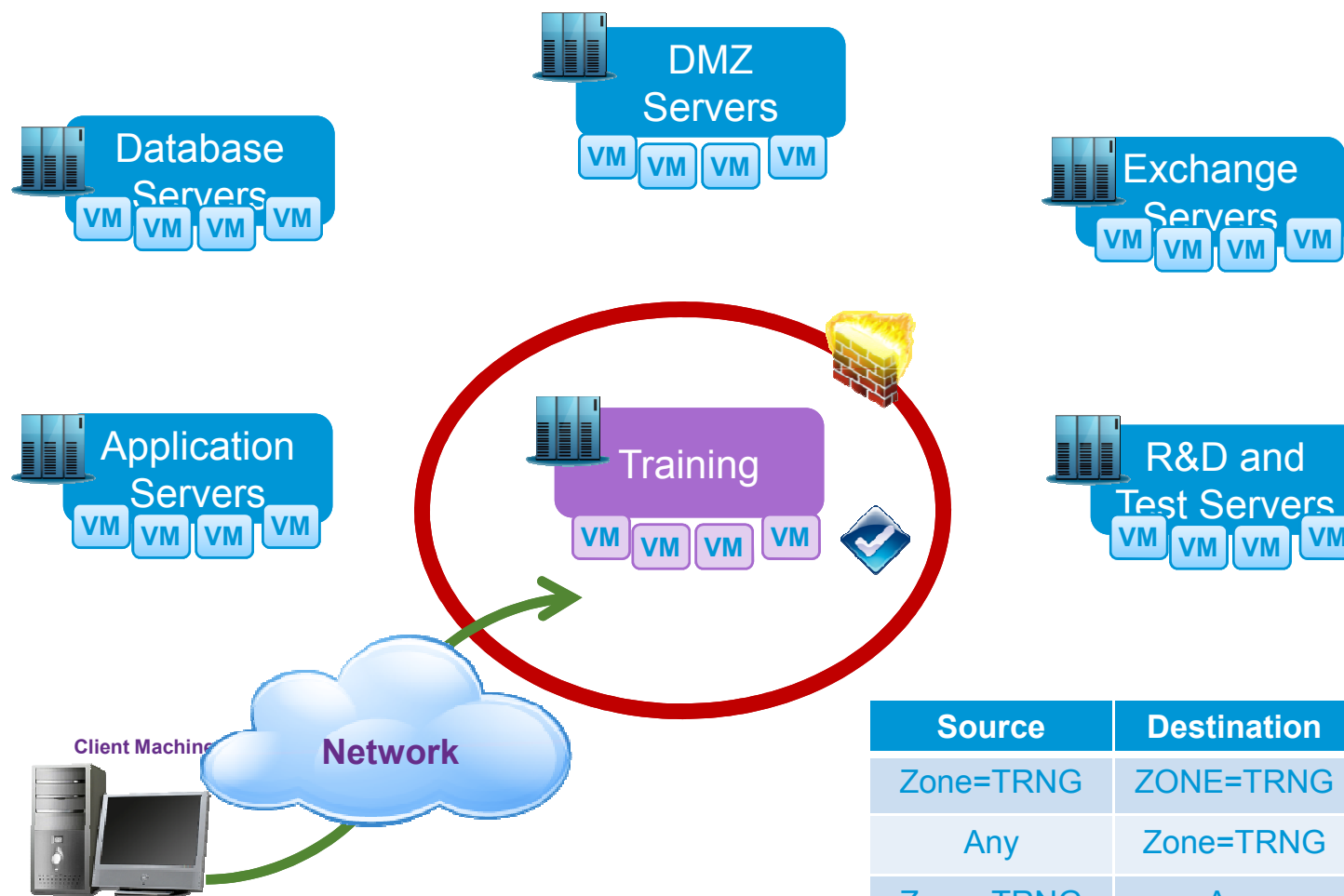
Operator
member
Not-member
Contains

rights reserved.

VSG: Use Cases

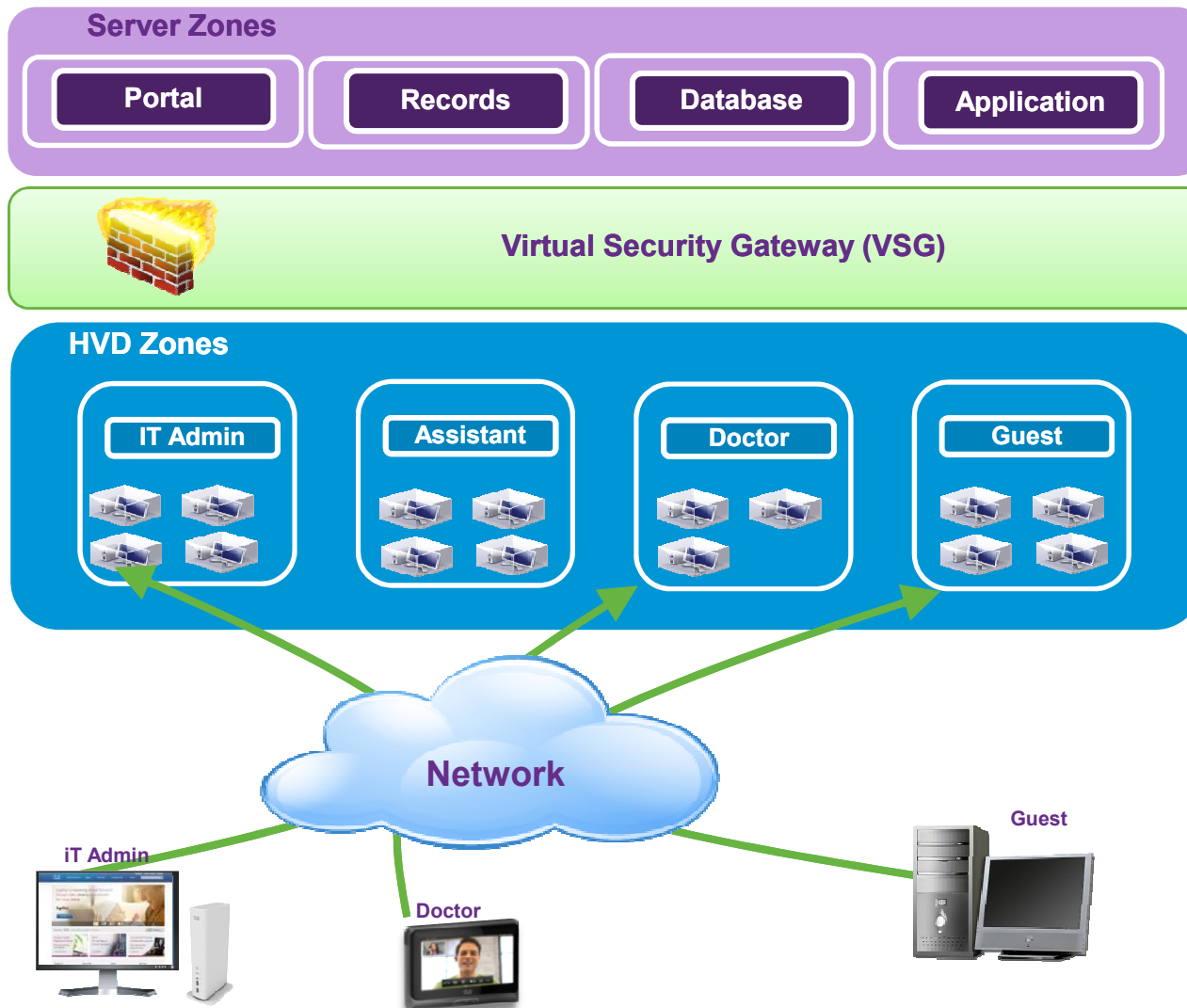
VSG Deployment at CareCore National

Logical zoning, vMotion support & scalable solution

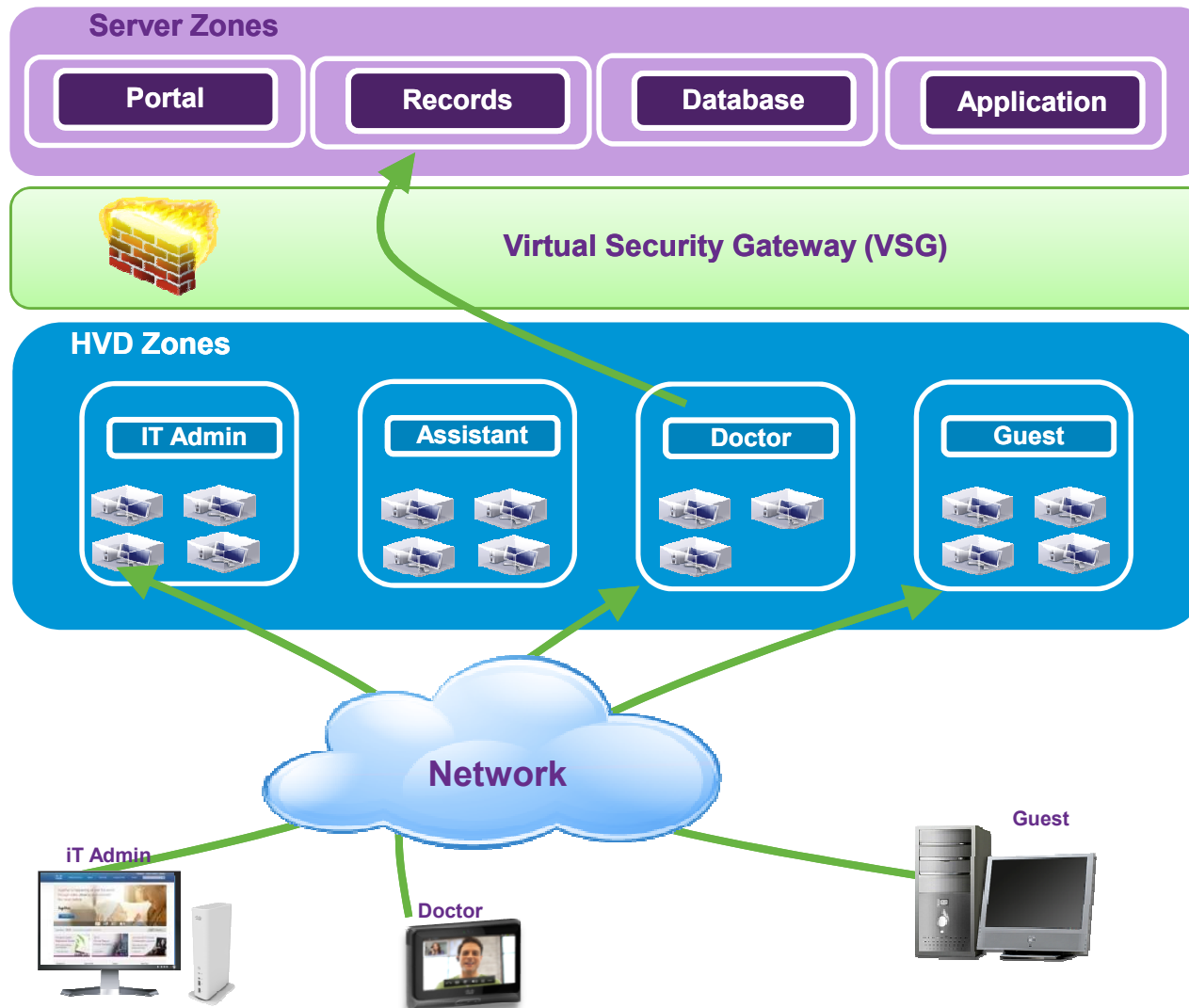


Source	Destination	Protocol	Action
Zone=TRNG	ZONE=TRNG	Any	Permit
Any	Zone=TRNG	Any	Permit
Zone=TRNG	Any	Any	Drop

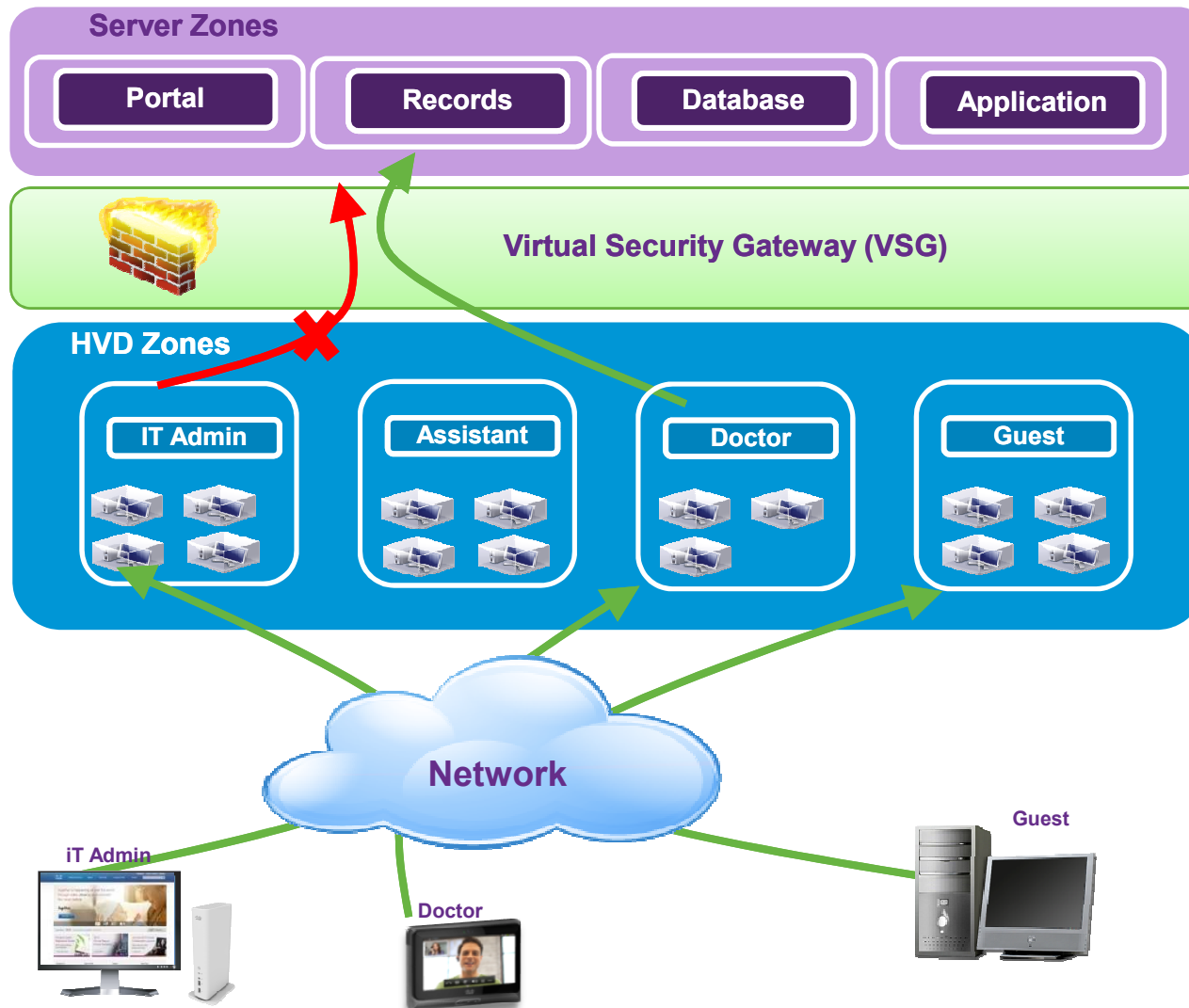
VSG Deployment for VDI



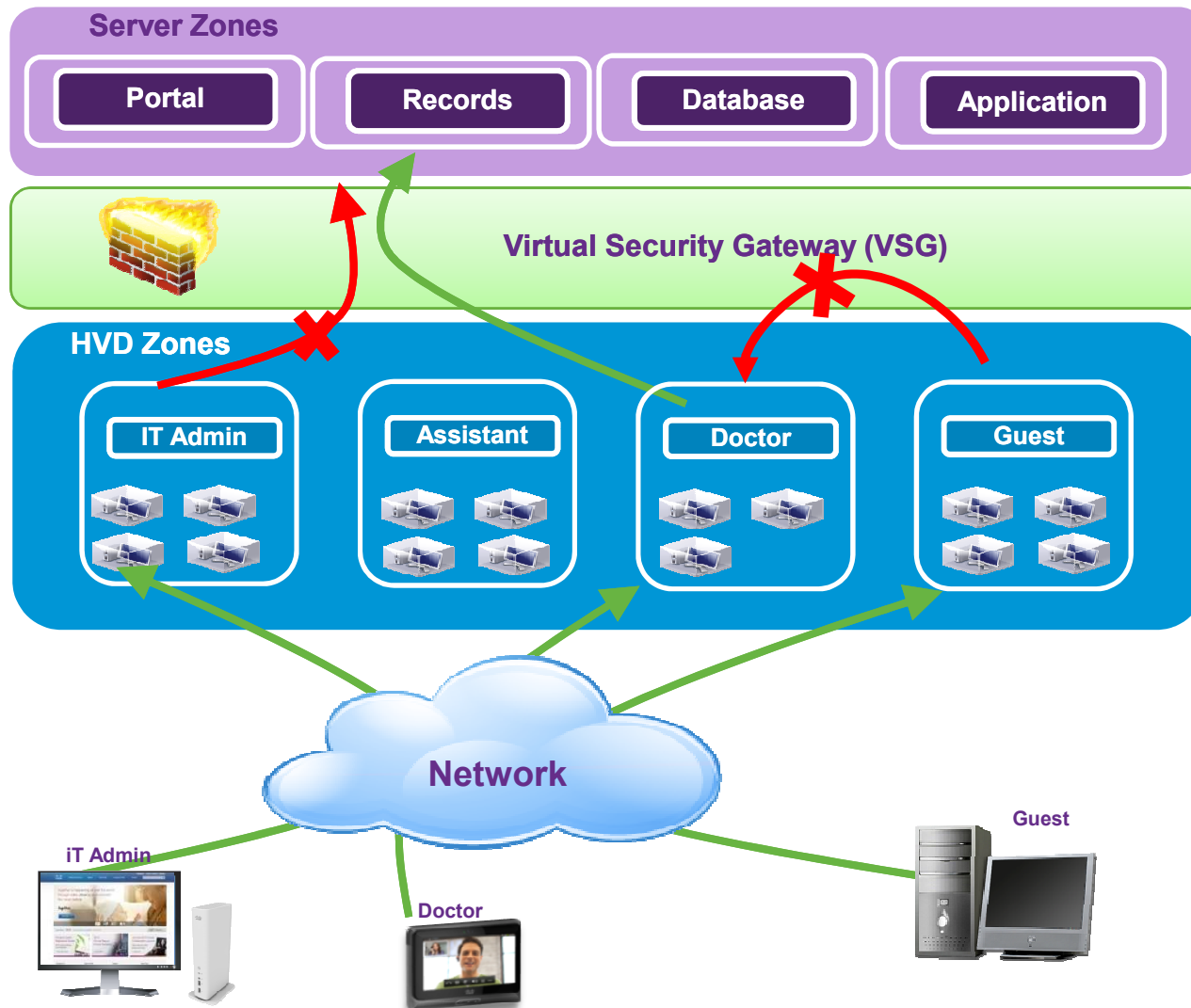
VSG Deployment for VDI



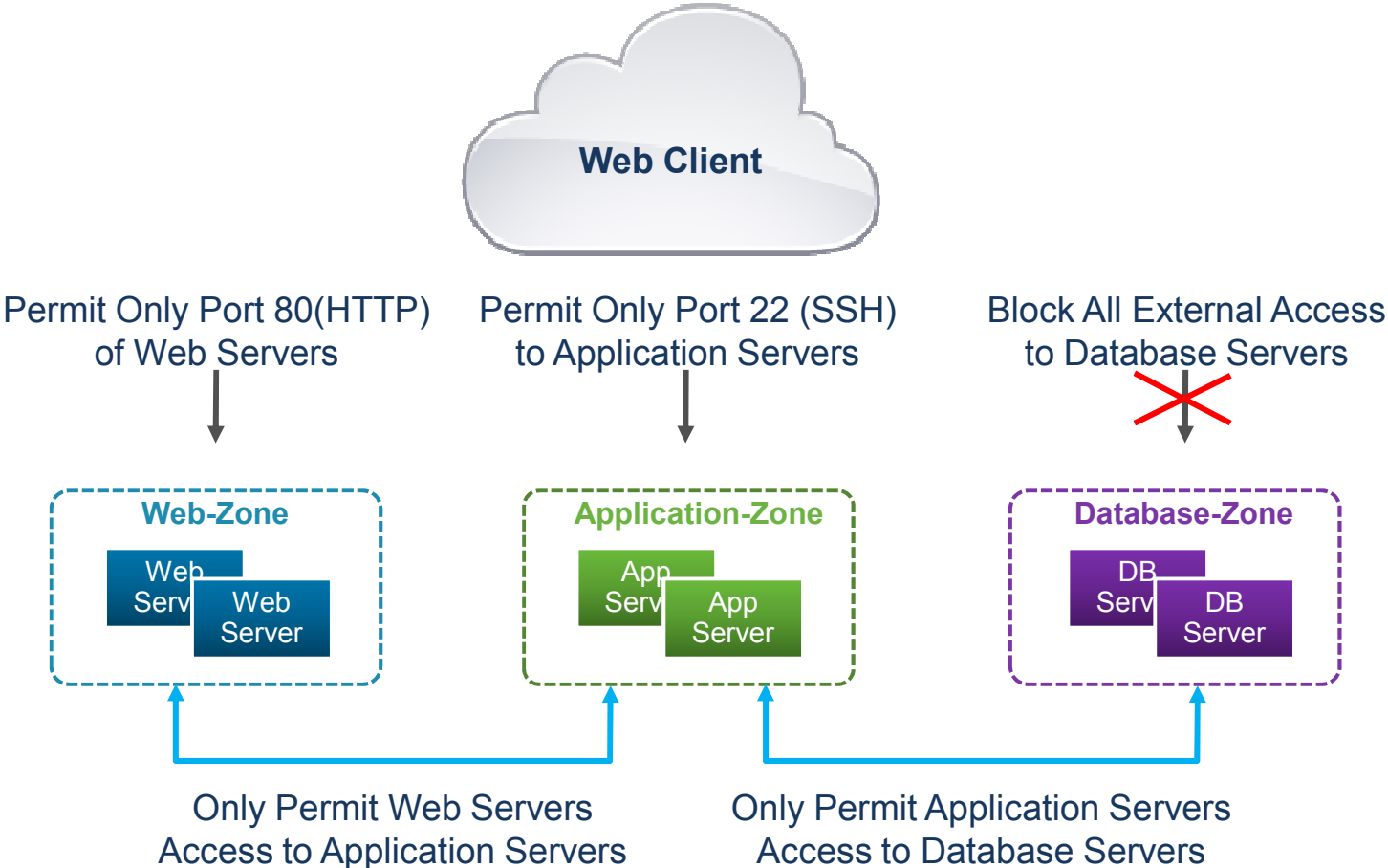
VSG Deployment for VDI



VSG Deployment for VDI

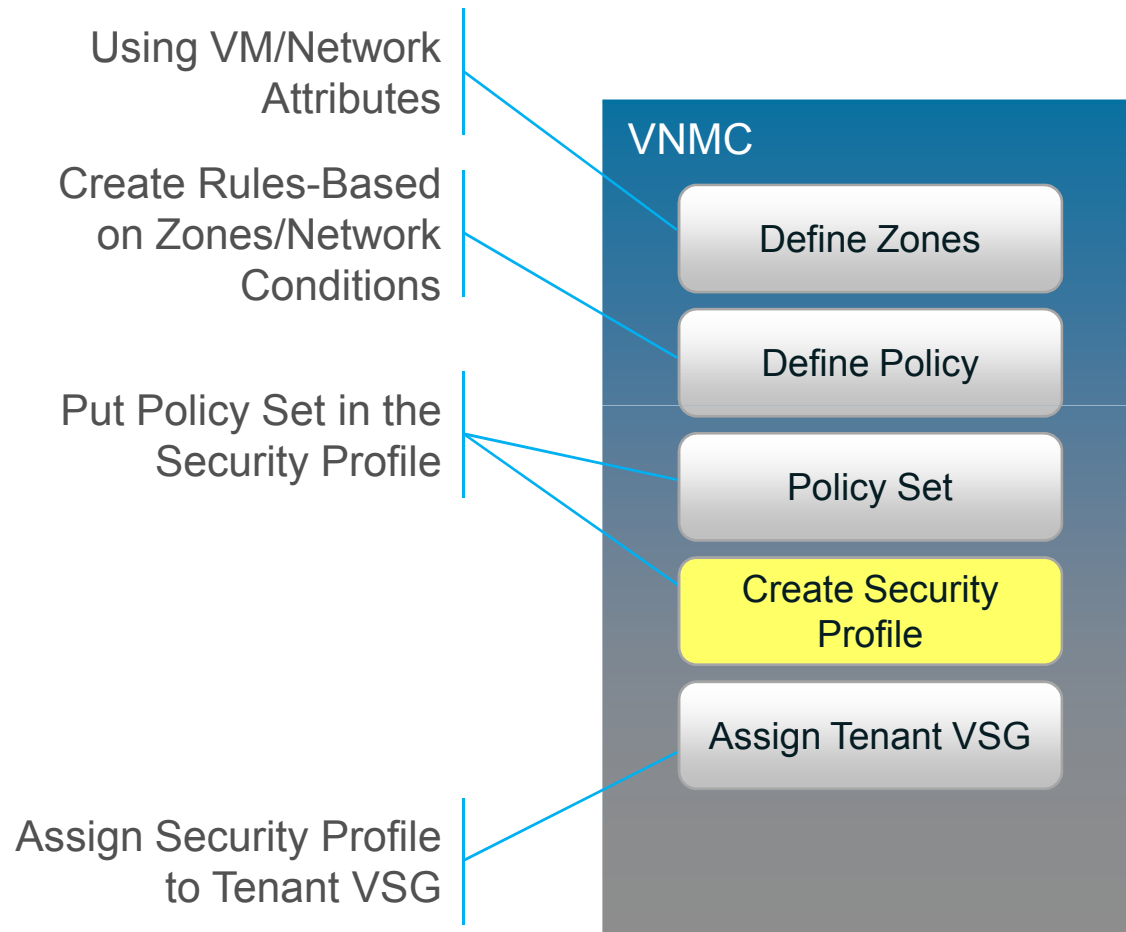


Example: 3-Tier Server Zones

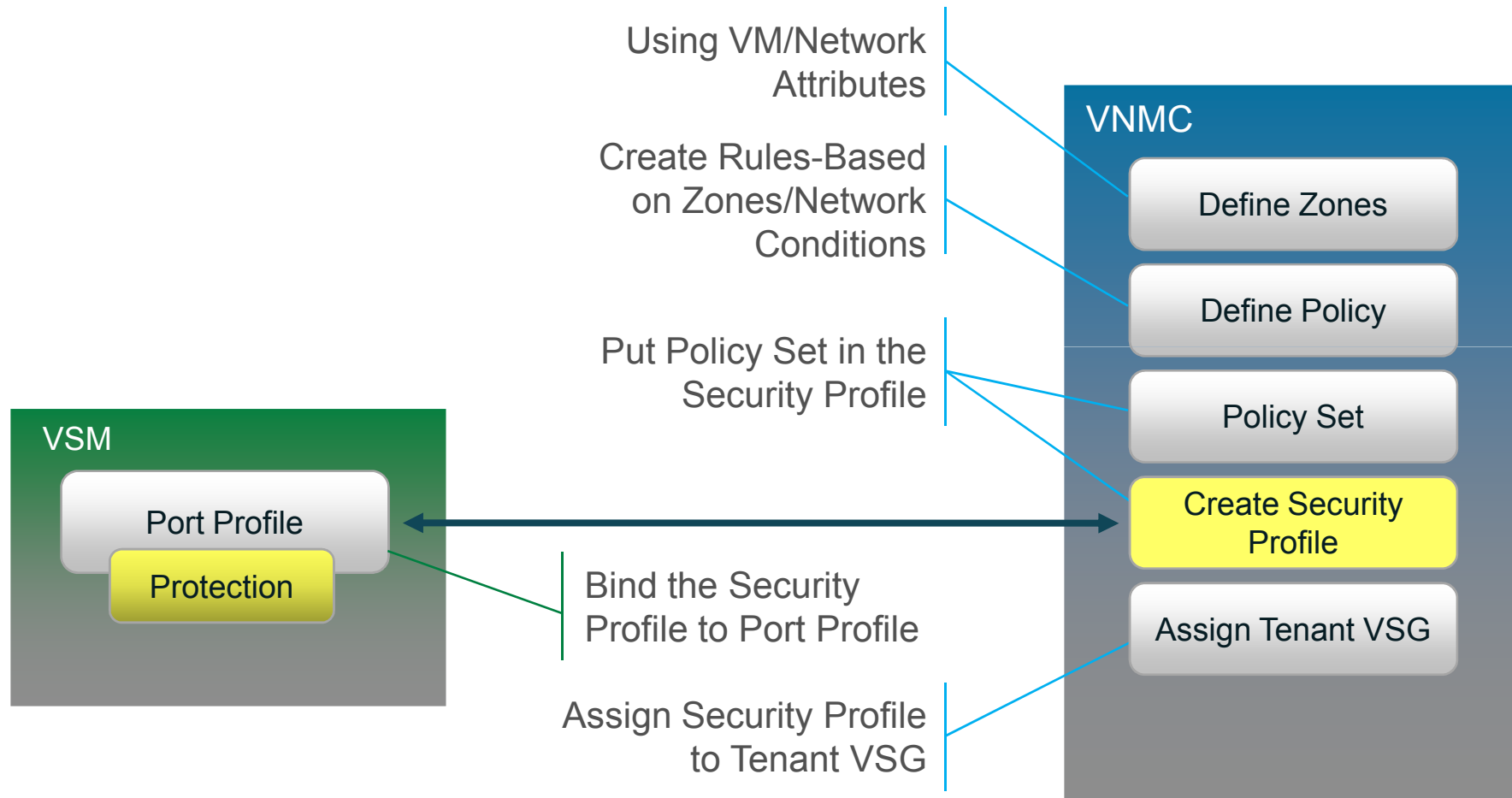


Policy—Content Hosting

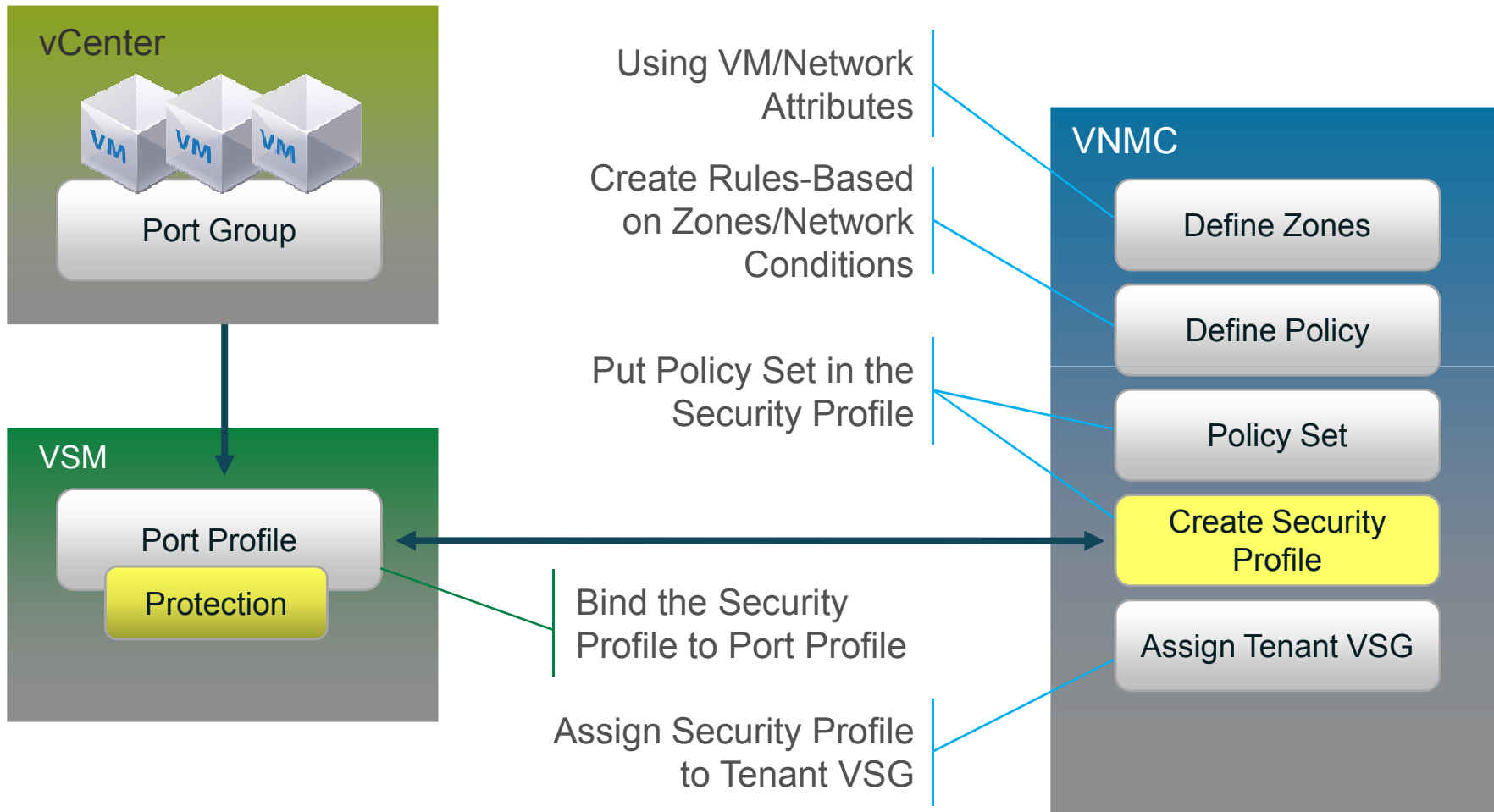
VSG Policy Provisioning Logical Flow



VSG Policy Provisioning Logical Flow



VSG Policy Provisioning Logical Flow



Security Policy Flow – Define Zones

Policy Management > Firewall Policy > Tenant > Zones

- 1 Zones
- 2 Policies
- 3 Rules
- 4 Conditions
- 5 Policy Set
- 6 Security-Profile
- 7 Assign VSG
- 8 Profile-Binding

The screenshot displays the Cisco Security Policy Management interface. The top navigation bar includes tabs for 'Security Policies', 'Device Policies', 'Capabilities', and 'Diagnostics'. The main content area is titled 'Firewall Policy' and shows a tree view of the configuration hierarchy. The 'Zones' folder under 'TenantA' is selected and highlighted in green. The right-hand pane shows the 'Zones' configuration page for 'TenantA', with the 'General' tab active. A yellow box highlights the 'Add Zone' button and the table of existing zones.

Name
AppZone
DBZone
WebZone

Security Policy Flow – Define Zones

Policy Management > Firewall Policy > Tenant > Zones

- 1 Zones
- 2 Policies
- 3 Rules
- 4 Conditions
- 5 Policy Set
- 6 Security-Profile
- 7 Assign VSG
- 8 Profile-Binding

Tenant Management | Resource Management | **Policy Management** | Administration

Security Policies | Device Policies | Capabilities | Diagnostics

Firewall Policy

root

root | Niners

Zones

Edit (WebZone)

General | **Conditions** | Events

+ Add

Attribute Name	Operator	Attribute Value
Instance Name	contains	Web

Raiders

Security Policy Flow – Define Policy

Policy Management > Firewall Policy > Tenant > Policies

- 1 Zones
- 2 Policies
- 3 Rules
- 4 Conditions
- 5 Policy Set
- 6 Security-Profile
- 7 Assign VSG
- 8 Profile-Binding

The screenshot displays the Cisco Policy Management web interface. At the top, there are navigation tabs: 'Tenant Management', 'Resource Management', 'Policy Management' (which is highlighted), and 'Administration'. Below these are sub-tabs for 'Security Policies', 'Device Policies', 'Capabilities', and 'Diagnostics'. The main content area shows a tree view under 'Firewall Policy' with 'root' expanded to show 'TenantA' and its 'Policies' sub-item, which is highlighted in green. The right-hand pane shows the configuration for 'Content_Policy' under the 'Policies' section, with 'General' and 'Faults' tabs. A yellow box highlights the 'Content_Policy' text in the right-hand pane.

Security Policy Flow – Rules Within Policy

Edit the Policy to create Rule(s) where source and destination conditions are specified based on

- 1 Zones
- 2 Policies
- 3 Rules
- 4 Conditions
- 5 Policy Set
- 6 Security-Profile
- 7 Assign VSG
- 8 Profile-Binding

The screenshot shows the 'Edit Policy' interface for 'ContentPolicy'. The 'Rules' tab is selected, displaying a table of rules. The table has columns for Name, Source Condition, Destination Condition, Protocol, Ethertype, and Action. There are five rules listed:

Name	Source Condition	Destination Condition	Protocol	Ethertype	Action
WebTraffic	Any	Network Port eq 80 Zone Name eq WebZone	Any	Any	Permit, Log
DB-SSH	Any	Network Port eq 22 Zone Name eq DBZone	Any	Any	Permit, Log
DBZone-WebZ	Zone Name eq DBZone	Zone Name eq WebZone	Any	Any	Permit, Log
WebZone-DBZ	Zone Name eq WebZone	Zone Name eq DBZone	Any	Any	Permit, Log
Deny_All_Zone	Any	Zone Name member All_Zones	Any	Any	Drop, Log

Security Policy Flow- Conditions Within Rules

Edit the Policy to create Rule(s) where source and destination conditions are specified

- 1 Zones
- 2 Policies
- 3 Rules
- 4 Conditions
- 5 Policy Set
- 6 Security-Profile
- 7 Assign VSG
- 8 Profile-Binding

Edit (web-rule)

General **Source and Destination Condition** Events

Source Conditions

+ Add

Attribute Name	Operator	Attribute Value

Destination Conditions

+ Add

Attribute Name	Operator	Attribute Value
Zone Name	eq	webzone
Network Port	eq	80

No Condition means "Any" traffic

Security Policy Flow- Assign Policies to Policy Set

One OR More Policies are assigned to the Policy Set

- 1 Zones
- 2 Policies
- 3 Rules
- 4 Conditions
- 5 Policy Set
- 6 Security-Profile
- 7 Assign VSG
- 8 Profile-Binding

The screenshot displays the Cisco Security Manager interface. The main window shows a tree view under 'Firewall Policy' with 'Policy Sets' selected. A modal dialog titled 'Edit Policy Set' is open, showing the 'Policies' tab for 'Content_PolicySet'. The 'Assign Policy' button is highlighted, and the 'Content_Policy' policy is listed in the table below.

Policy Name
Content_Policy

Security Profile

Create Security Profile at the tenant level

Select from the available Policy Sets from the drop down menu

- 1 Zones
- 2 Policies
- 3 Rules
- 4 Conditions
- 5 Policy Set
- 6 Security-Profile
- 7 Assign VSG
- 8 Profile-Binding

The screenshot displays the Cisco Security Manager interface. The top navigation bar includes tabs for 'Security Policies', 'Device Policies', 'Capabilities', and 'Diagnostics'. The breadcrumb trail shows the path: root > TenantA > Security Profiles. The main content area is divided into a left-hand tree view and a right-hand configuration panel. In the tree view, the 'Secure_TenantA' profile is highlighted with a yellow box. The configuration panel on the right shows the 'General' tab for 'Secure_TenantA'. It includes a 'Name' field with the value 'Secure_TenantA', a 'Description' field, and a 'Policy Set' dropdown menu currently set to 'Content_PolicySe'.

Assign VSG to the Tenant

Assign VSG at a tenant level under Resource Management > Managed Resources > Virtual Security Gateways > Tenant (tree level) > VSG Details

- 1 Zones
- 2 Policies
- 3 Rules
- 4 Conditions
- 5 Policy Set
- 6 Security-Profile
- 7 Assign VSG
- 8 Profile-Binding

The screenshot displays the Cisco VSG configuration interface. The left sidebar shows a tree view under 'Virtual Security Gateways' with 'VSG-TenantA' selected. The main content area shows the configuration for 'VSG-TenantA' with tabs for 'General', 'Firewall Details', 'VSG Details', 'Faults', and 'Events'. The 'VSG Details' tab is active, showing the following configuration:

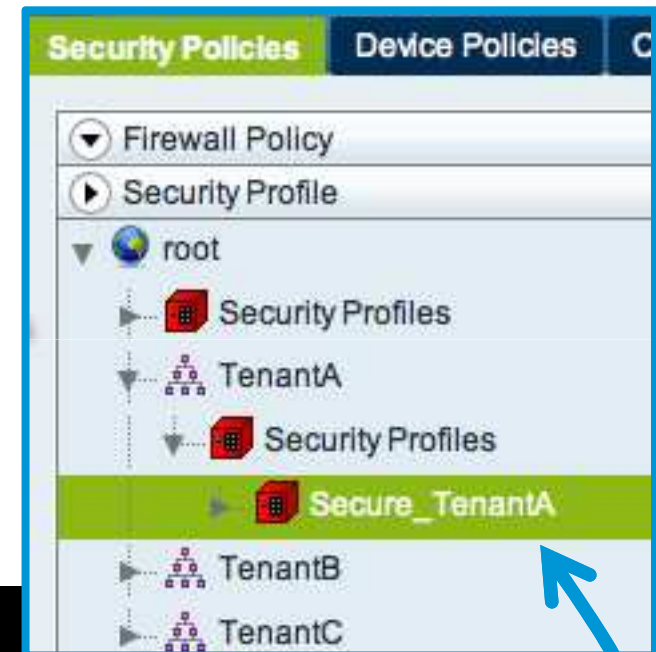
VSG Service ID:	1005
VSG Mgmt IP:	10.29.173.42
HA Role:	standalone
Association:	associated

Port Profile to Security Profile Binding

- In VSM, Associate Port Profile to the Tenant and bind the Security Profile

- 1 Zones
- 2 Policies
- 3 Rules
- 4 Conditions
- 5 Policy Set
- 6 Security-Profile
- 7 Assign VSG
- 8 Profile-Binding

```
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
```



vCenter: VM attach to a PortGroup (PortProfile)

- 1 Zones
- 2 Policies
- 3 Rules
- 4 Conditions
- 5 Policy Set
- 6 Security-Profile
- 7 Assign VSG
- 8 Profile-Binding
- 9 VM Port-Group Mapping

The screenshot shows the 'Virtual Machine Properties' dialog for 'TenantA-Web-01'. The 'Hardware' tab is active, and the 'Network adapter 1' is selected in the hardware list. The right-hand pane shows the configuration for this network adapter. The 'Device Status' section has 'Connected' and 'Connect at power on' checked. The 'Adapter Type' is 'Flexible'. The 'MAC Address' is '00:50:56:94:33:d1' with 'Automatic' selected. In the 'Network Connection' section, the 'Network' dropdown is highlighted with a yellow box and set to 'TenantA (VSM-Nexus1000V)'. The 'Port' is set to '356'. The 'Specify standalone port (Advanced)' section is currently unselected.

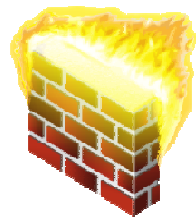
Hardware	Summary
Memory	512 MB
CPUs	1
Video card	Video card
VMCI device	Restricted
Floppy drive 1	Floppy drive 1
CD/DVD Drive 1	CD/DVD Drive 1
Network adapter 1	TenantA (VSM-Nexus1000V)
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk

Key Takeaways

- Cisco N1KV (vPAth) is leveraged by VSG for deployment
- VSG is NOT required to installed on every physical host
- VSG provides a High Availability solution to protect multiple ESX hosts
- Supports a Multitenant Environment
- Non-Disruptive Administration Model - Security team manages Security Polices



VNMC



VSG



For More Information

See the following Resources

- [Nexus 1000V Configuration, Installation and Upgrade Guides](#)
- [Nexus 1000V Deployment Guide Version 3.0](#)
- [QoS Queuing for Nexus 1000V Whitepaper](#)
- [Nexus 1000V Integration with vCloud Director Technical Whitepaper](#)
- [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 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 Installation & Upgrade Overview
12-Apr	Nexus1010 Installation & Upgrade
26-Apr	Virtual Security Gateway Technical 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.

