

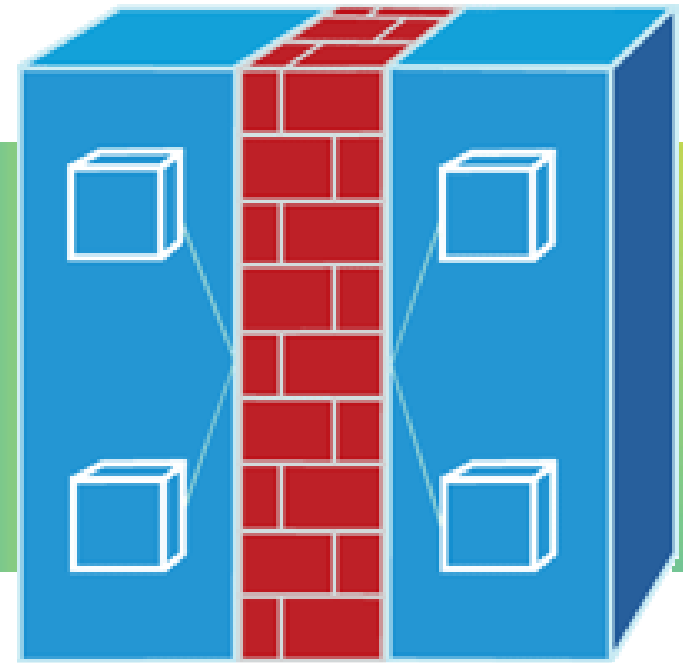


# Virtual Security Gateway (VSG) v1.3 Technical Deep Dive

Soumen Chatterjee, VSG Product Manager  
Server Access Virtualization Technology Group (SAVTG)

Yogesh Shetty, Technical Marketing Engineer (TME)  
Server Access Virtualization Technology Group (SAVTG)

Gunnar Anderson, Nexus 1000V Product Manager [HOST]  
Server Access Virtualization Technology Group (SAVTG)



# Public Webcasts Series, Spring 2012

Date	Technical Track Topics	Webinar
2/14/12	Virtual Security Gateway (VSG) v1.3 Technical Deep Dive	<a href="#">Register</a>
2/22/12	Nexus 1000V v1.5 Technical Deep Dive	<a href="#">Register</a>
2/29/12	Nexus 1010-X v1.4 Technical Deep Dive	<a href="#">Register</a>
3/7/12	vWAAS and Nexus 1000V Technical Deep Dive	<a href="#">Register</a>
3/14/12	FlexPod & Nexus 1000V/1010	<a href="#">Register</a>
3/21/12	QoS for multimedia traffic in the Virtualized DC (w/ Nexus 1000V)	<a href="#">Register</a>
3/28/12	Vblock & Nexus 1000V / VSG / vWAAS	<a href="#">Register</a>
4/4/12	vCloud Director, Nexus 1000V, and VXLAN Technical Deep Dive	<a href="#">Register</a>
4/11/12	Cisco's CloudLab Deep Dive: Hands-on labs for N1KV, VSG & VXLAN	<a href="#">Register</a>

Webinar Link: [www.cisco.com/go/1000vcommunity](http://www.cisco.com/go/1000vcommunity)

# 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

# Agenda



Virtual Security Gateway (VSG) Overview

VSG Packet Flow

VSG Policy Model

Use Case Example

Policy Configuration

1.3 Feature Update

Summary

# Introducing Virtual Security Gateway

## *Stateful virtual FW for Nexus 1000V*

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 vPath intelligence)

Virtual Network Management Center (VNMC)



Non-Disruptive Operations

Security team manages security

Policy Based Administration

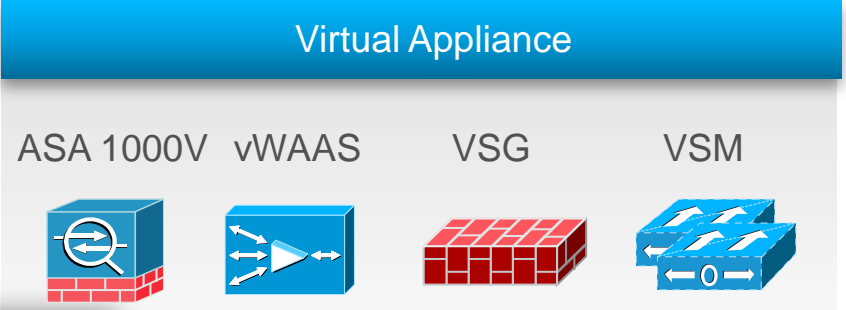
Central mgmt, scalable deployment, multi-tenancy

Designed for Automation

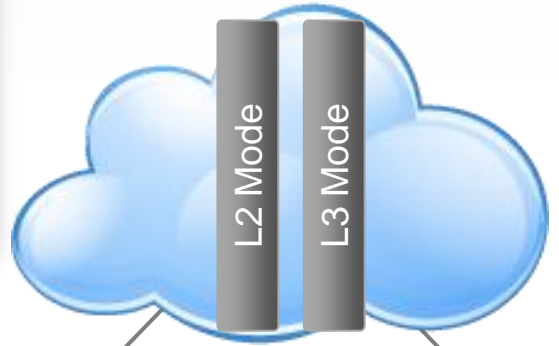
XML API, security profiles

# Embedding Intelligence for Virtual Services

## vPath – Virtual Service Datapath



- VSG**
  - Virtual Security Gateway for N1K
- vWAAS**
  - Virtual WAAS
- ASA 1000V**
  - Virtual ASA



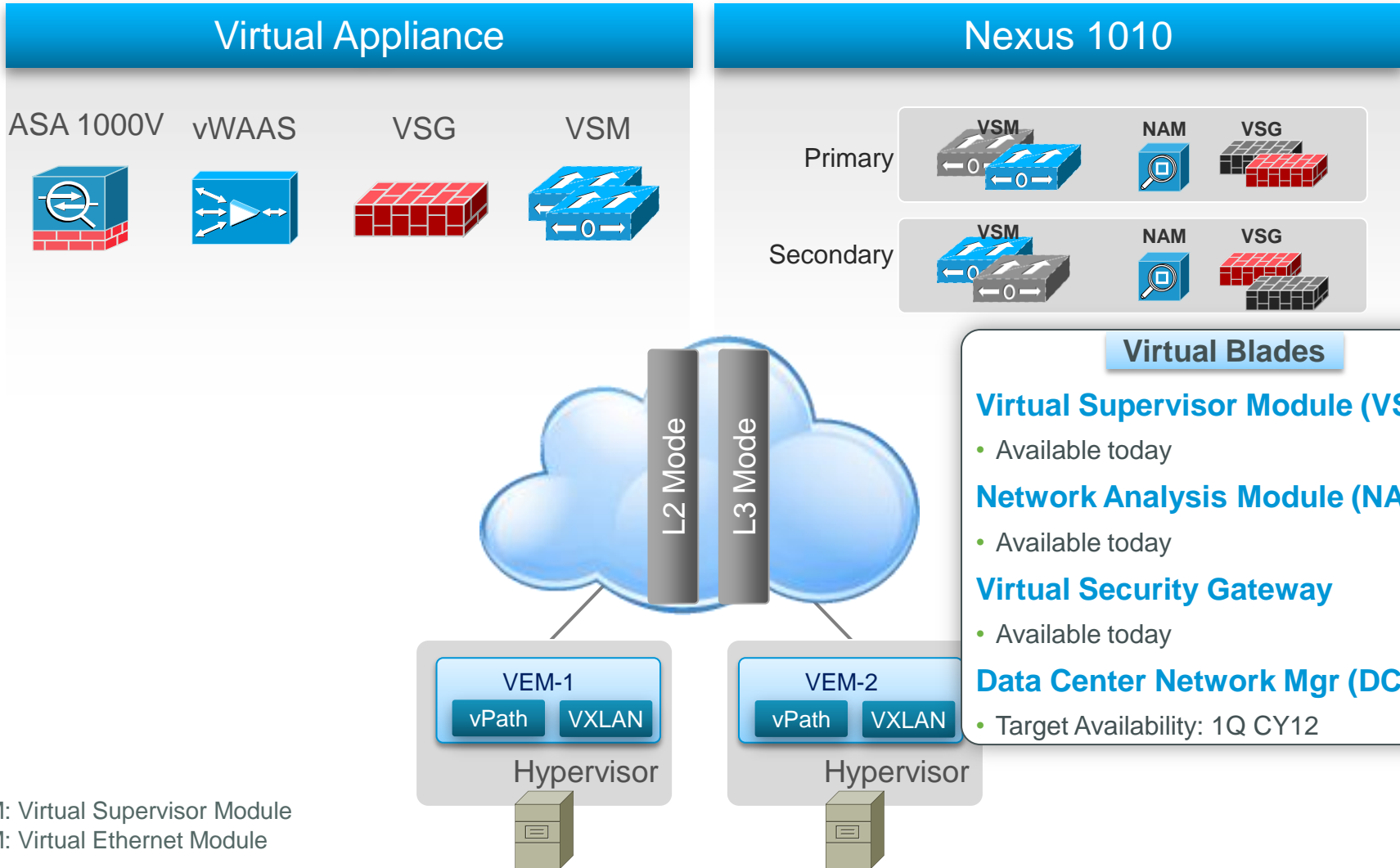
### vPath

Virtual Service Datapath

- Service Binding (Traffic Steering)
- Fast-Path Offload
- VXLAN aware



# Nexus 1010 – Hosting Platform for Services



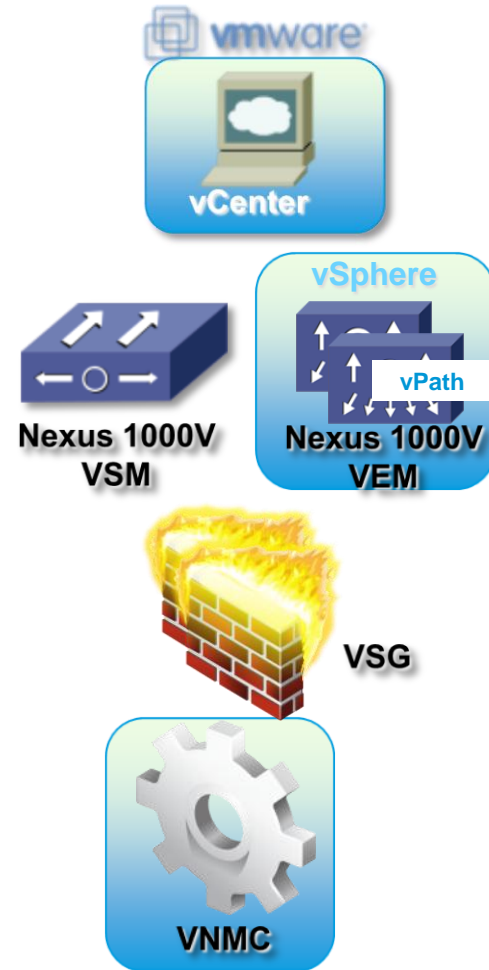
VSM: Virtual Supervisor Module  
VEM: Virtual Ethernet Module

# 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)

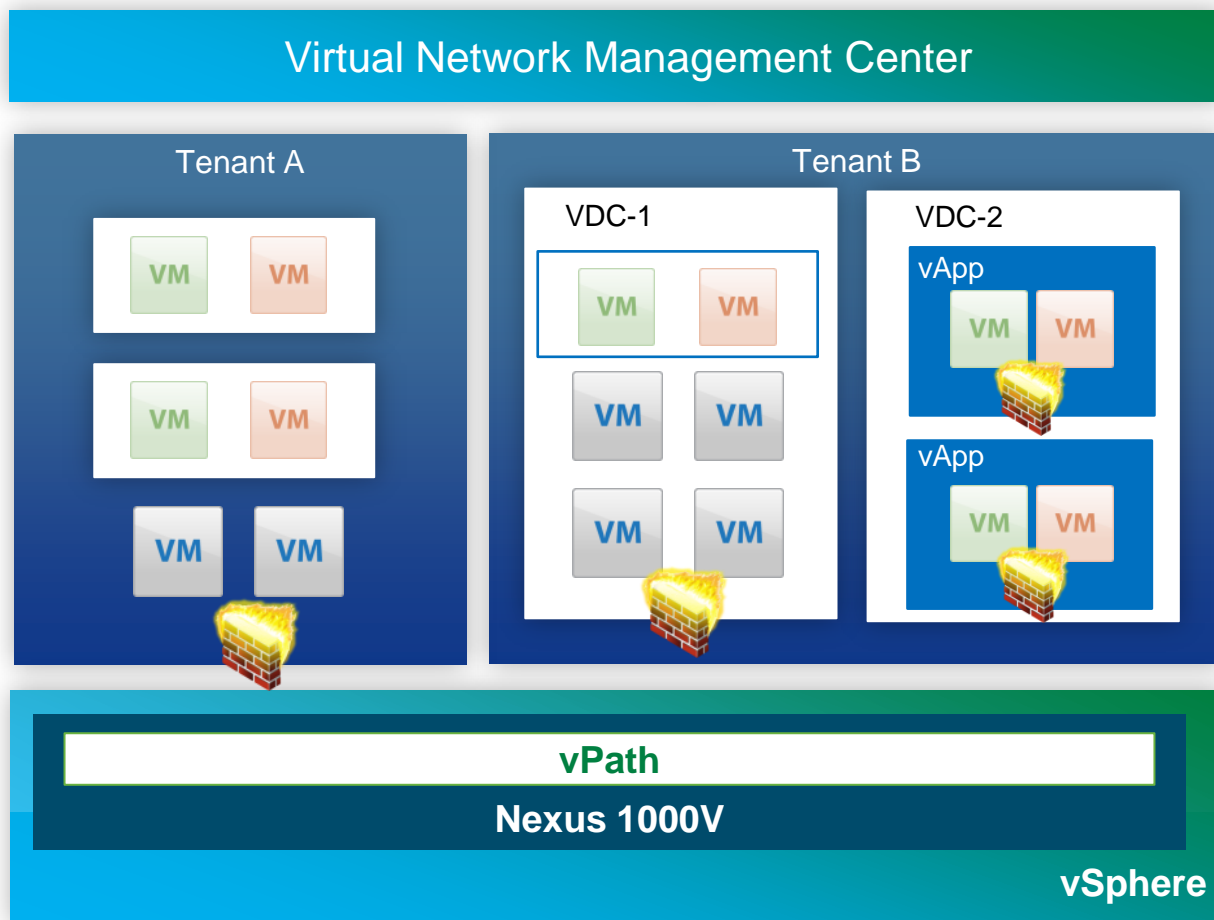
VSG can protect subset of 1000V-licensed CPUs.





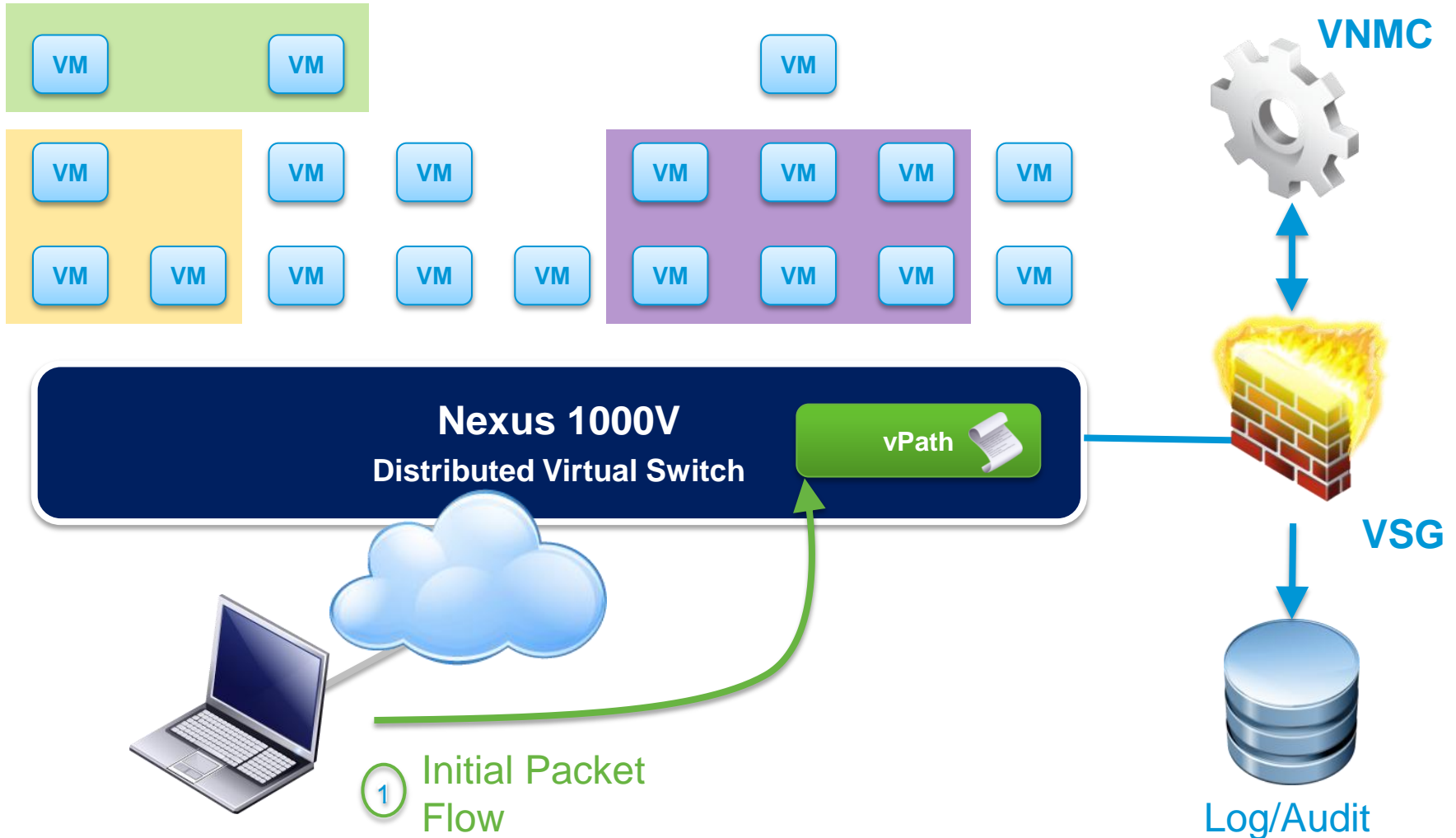
# Multi-Tenant Deployment

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



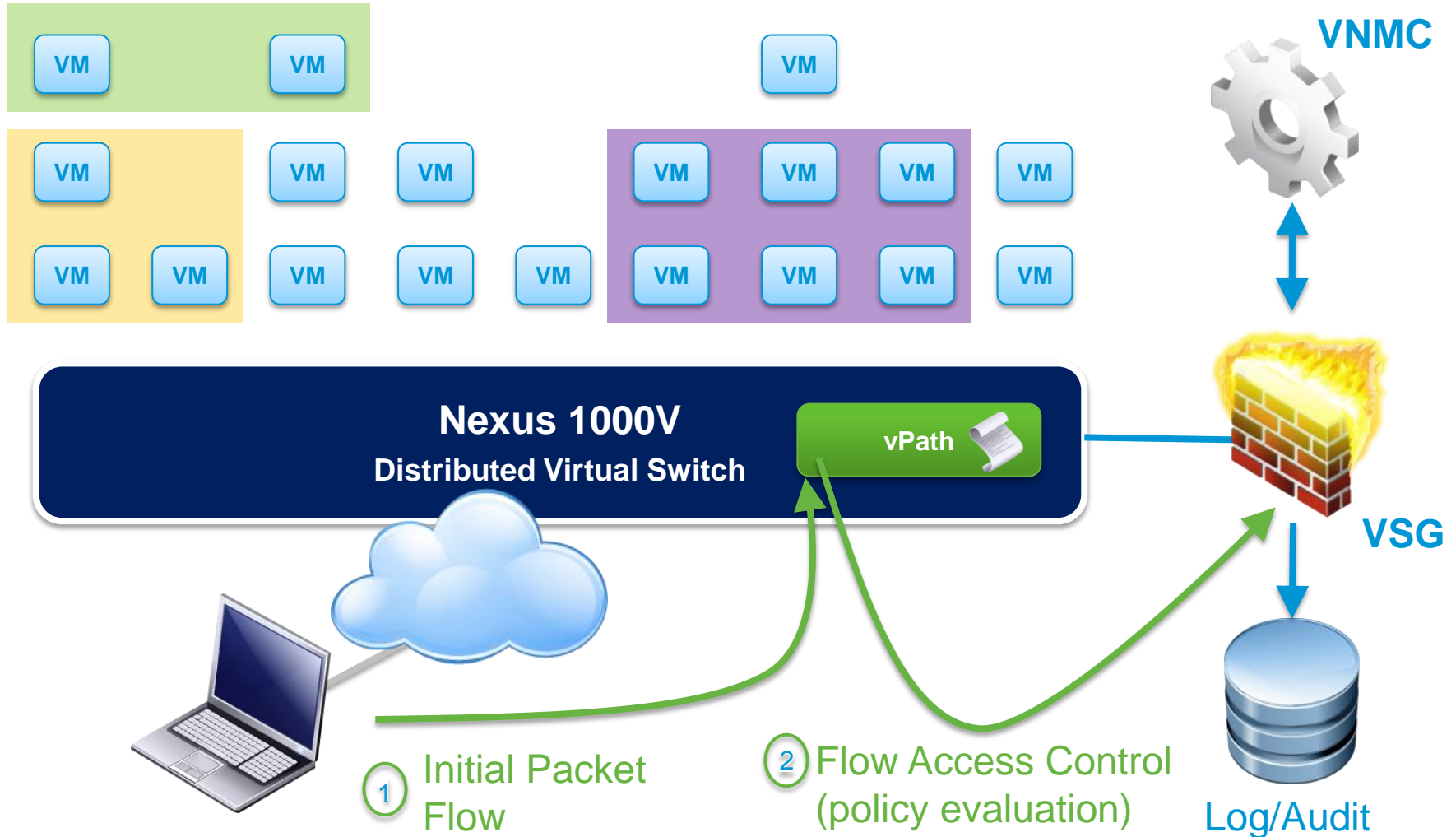
# Virtual Security Gateway

## Intelligent Traffic Steering with vPath



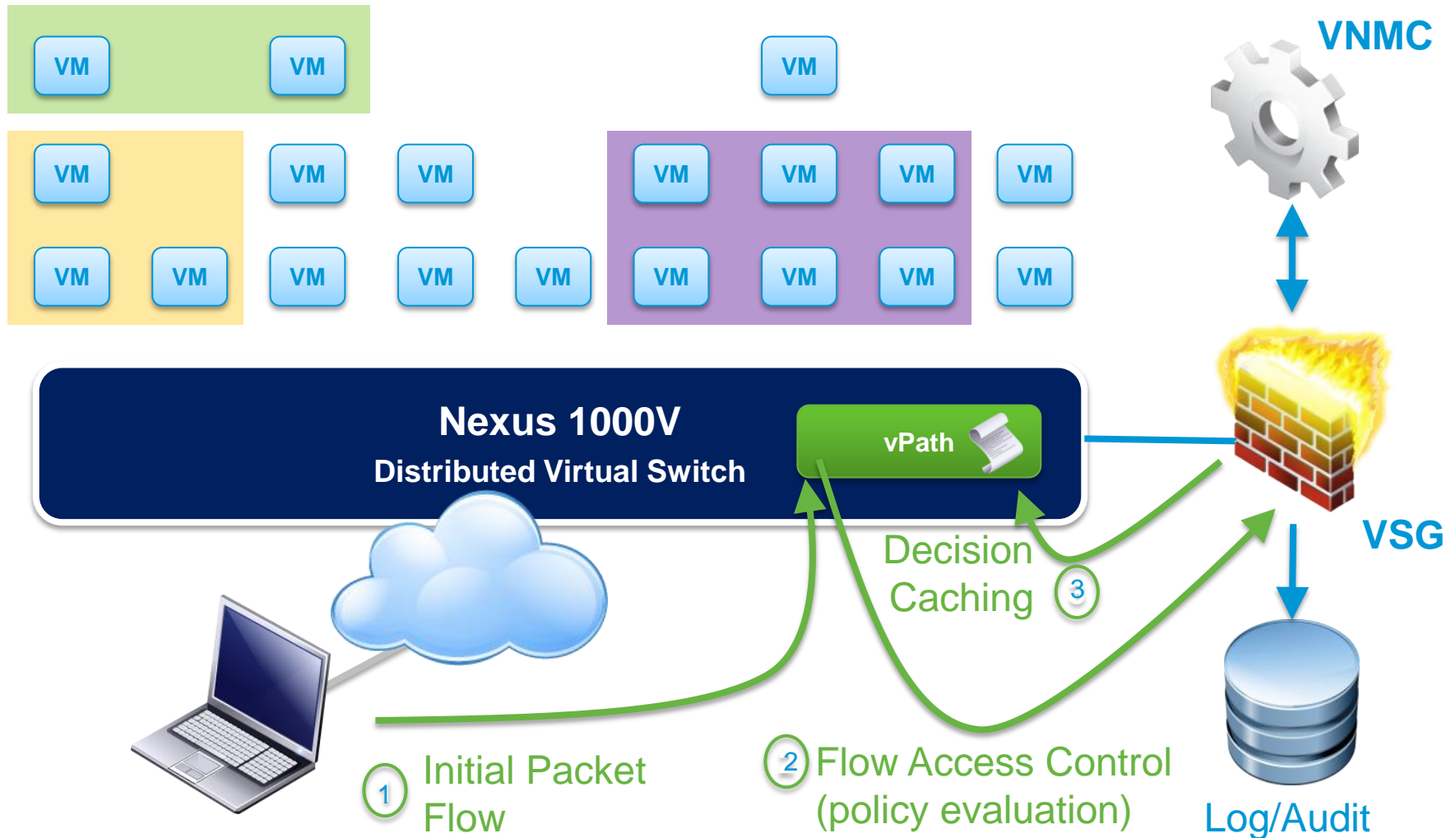
# Virtual Security Gateway

## Intelligent Traffic Steering with vPath



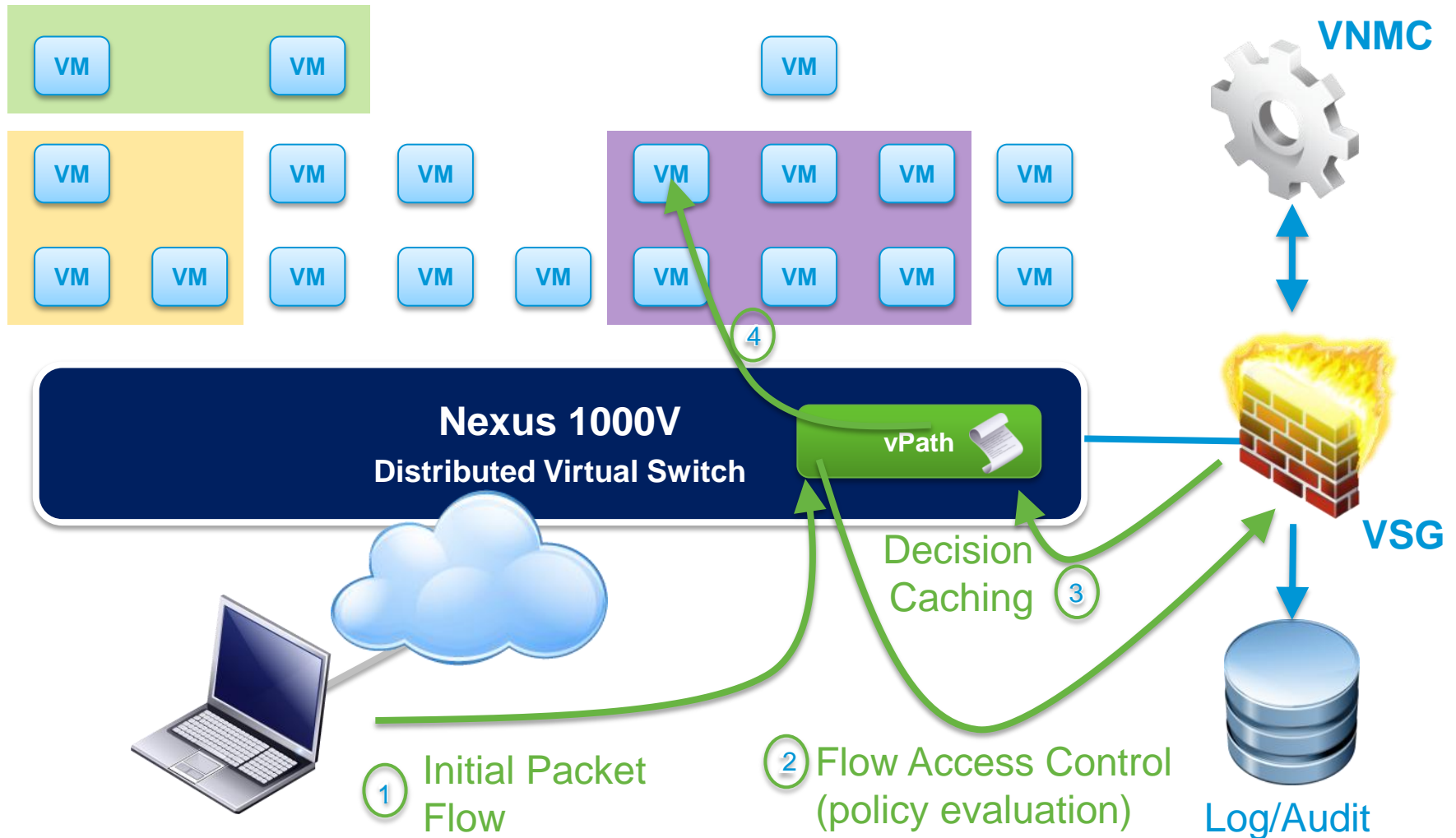
# Virtual Security Gateway

## Intelligent Traffic Steering with vPath



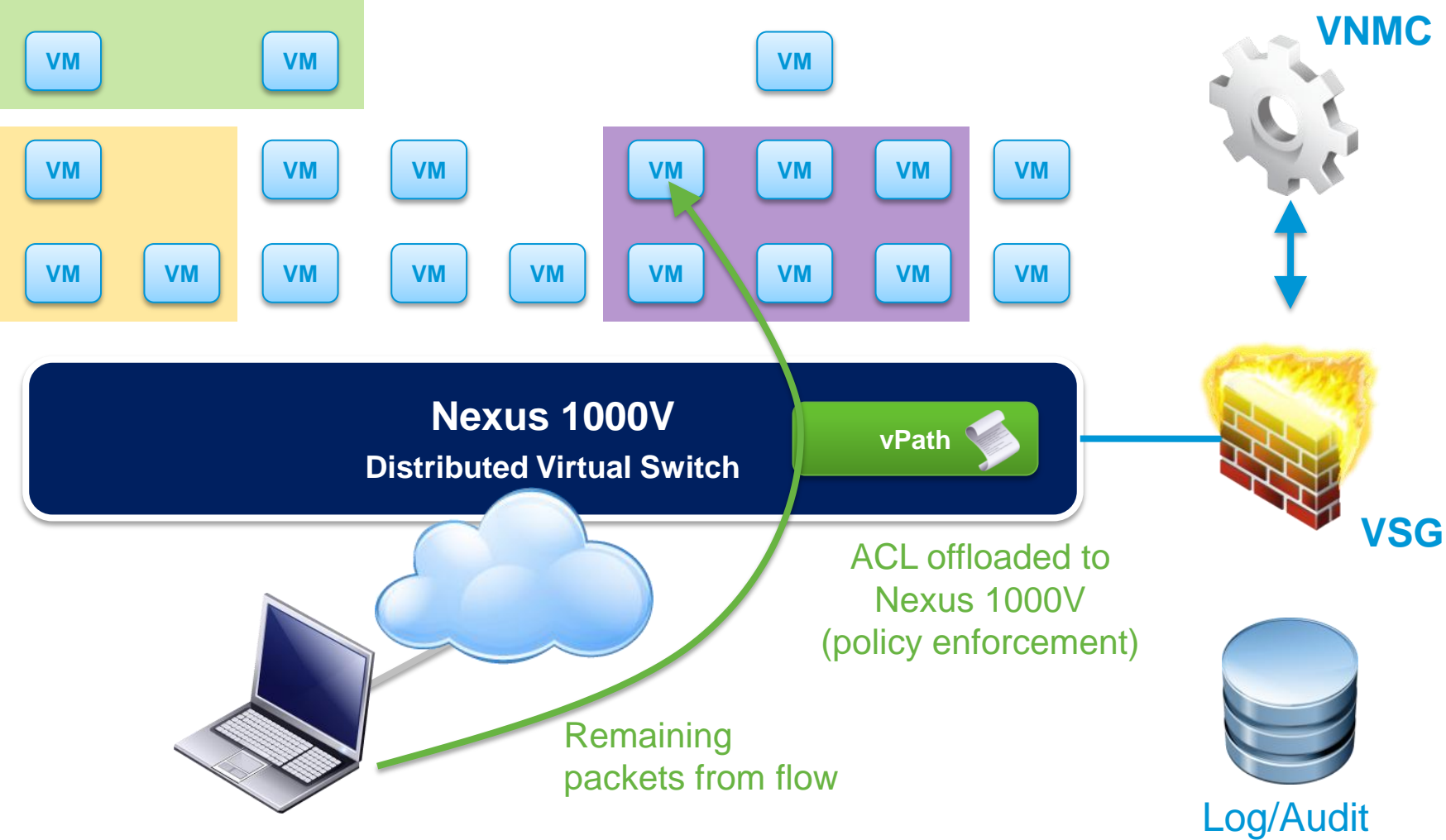
# Virtual Security Gateway

## Intelligent Traffic Steering with vPath



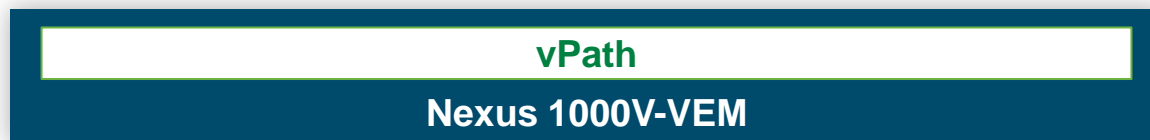
# Virtual Security Gateway

## Performance Acceleration with vPath

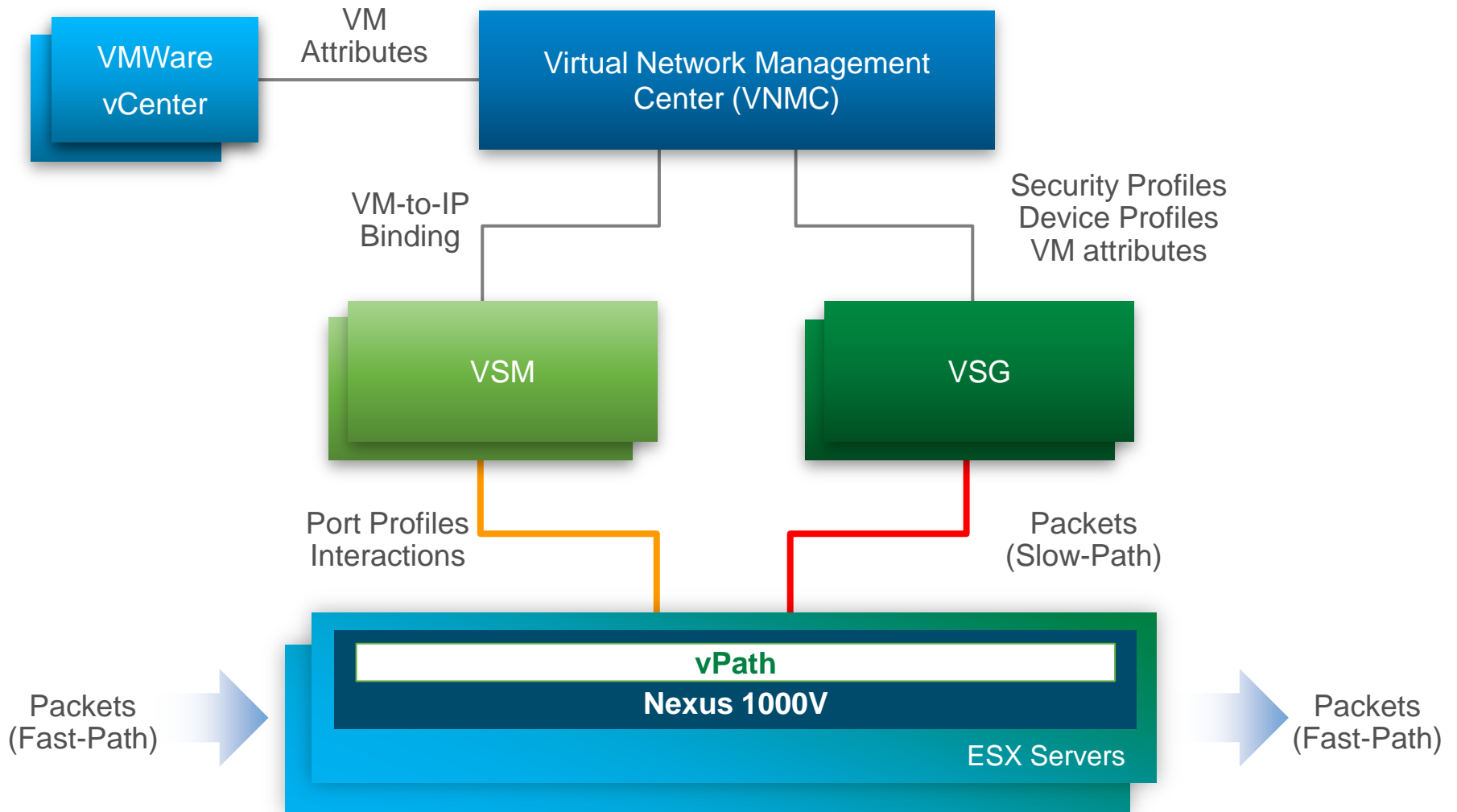


# vPath—Summary

- vPath intelligence is built 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



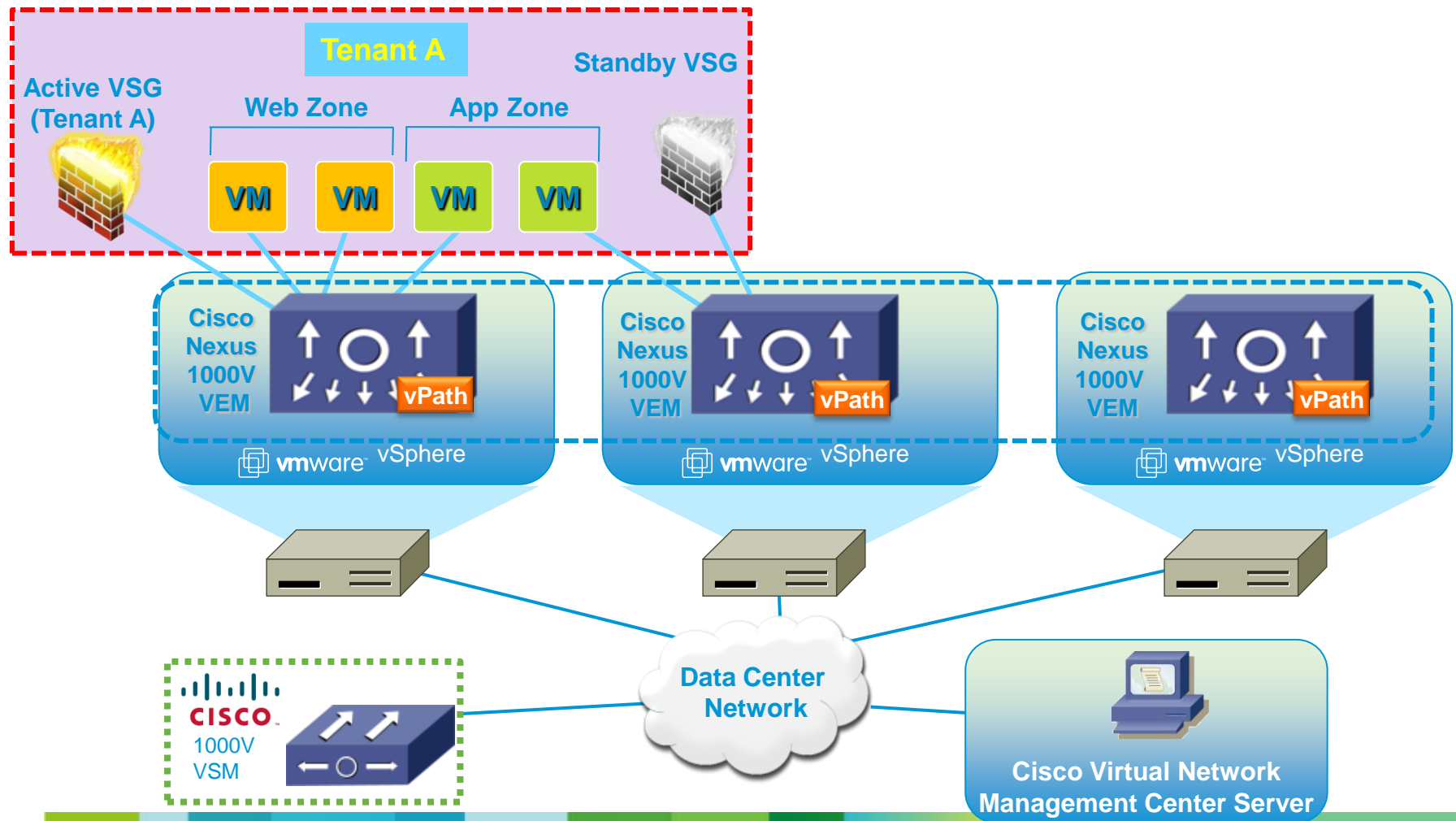
# VSG System Architecture



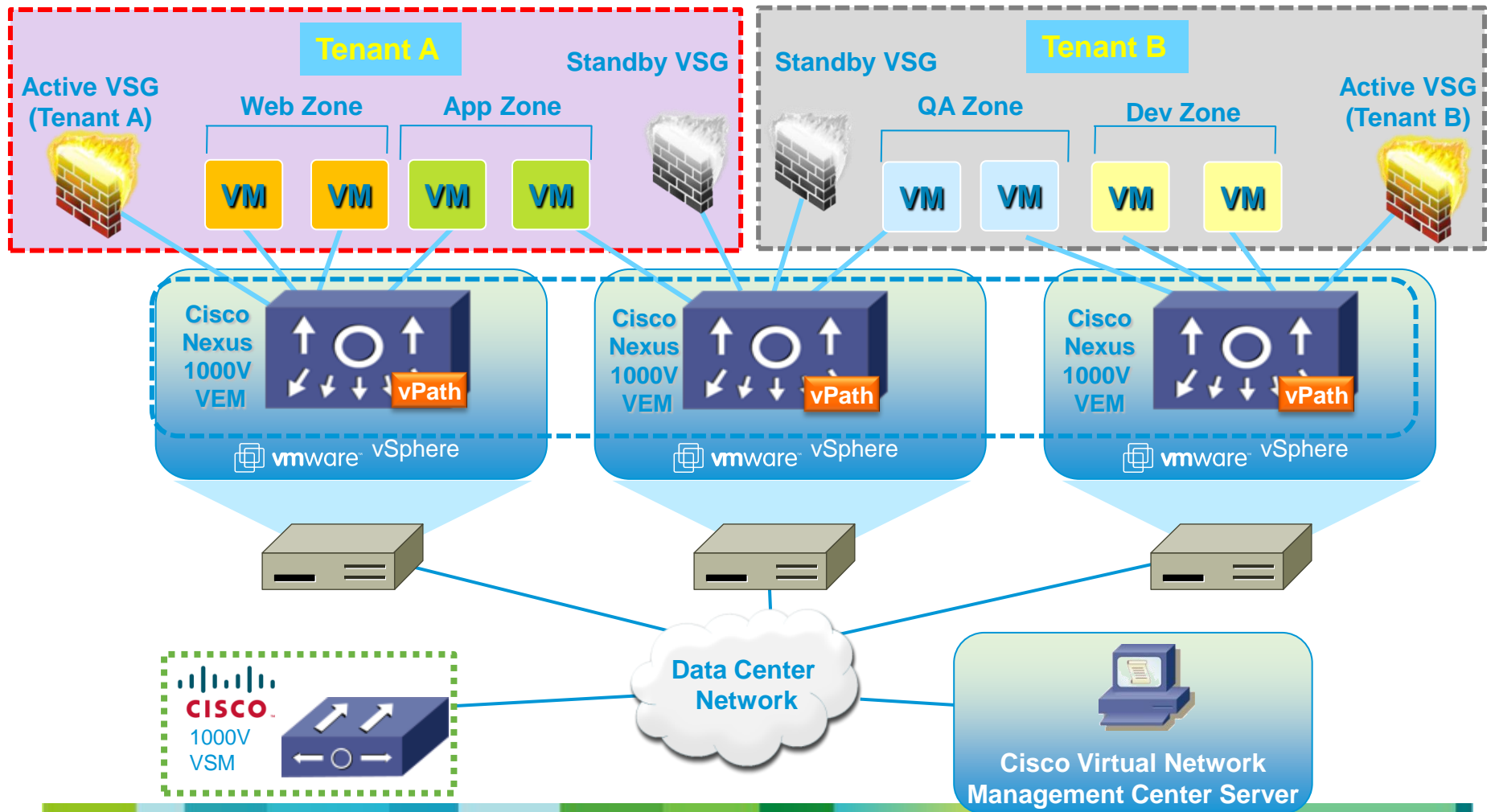


# VSG Deployment Scenario

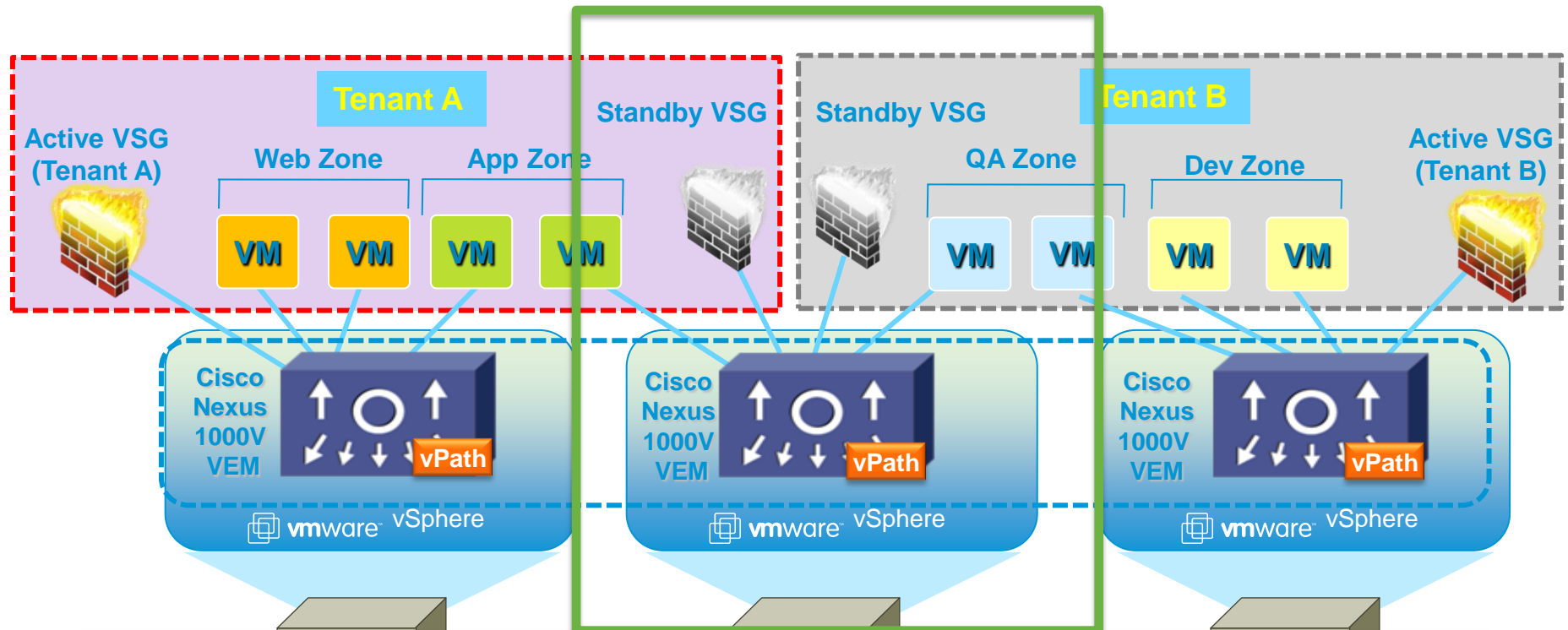
# Deployment in Multitenant Environment



# Deployment in Multitenant Environment

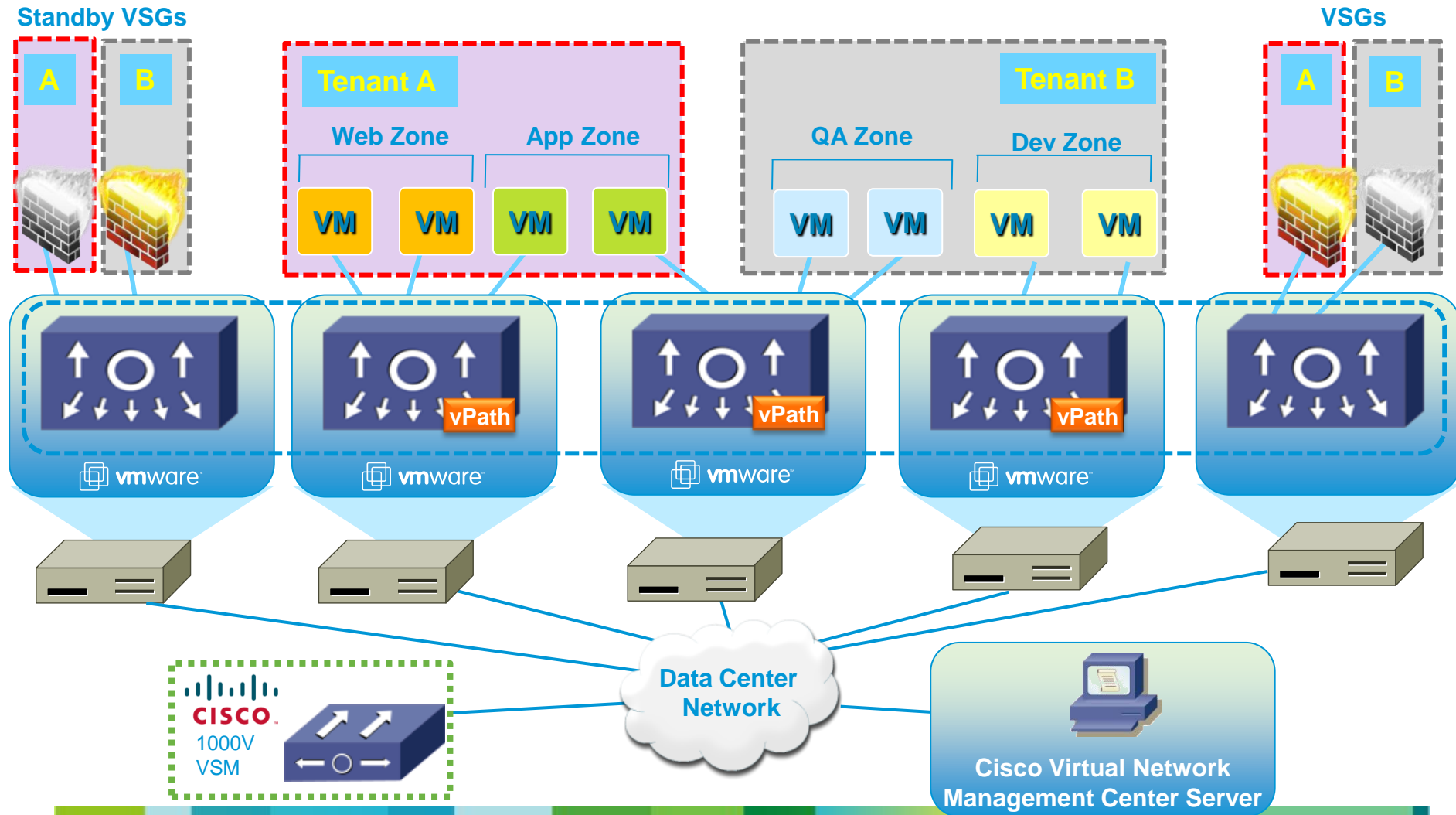


# Deployment in Multitenant Environment

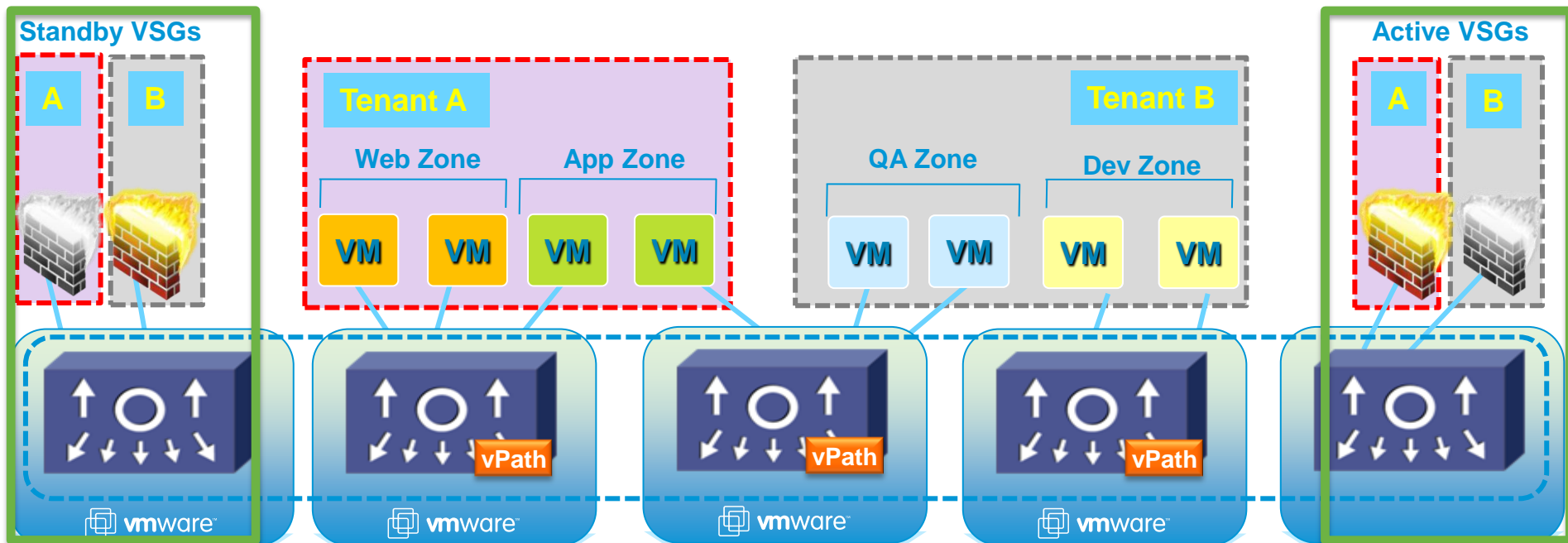


- Security Policies Enforced on Shared Compute Environment
- vPath Multitenant Aware
- Active Stand by VSGs on different Physical Host

# 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

# VSG Security Policy Model

# Security Policy Building Block

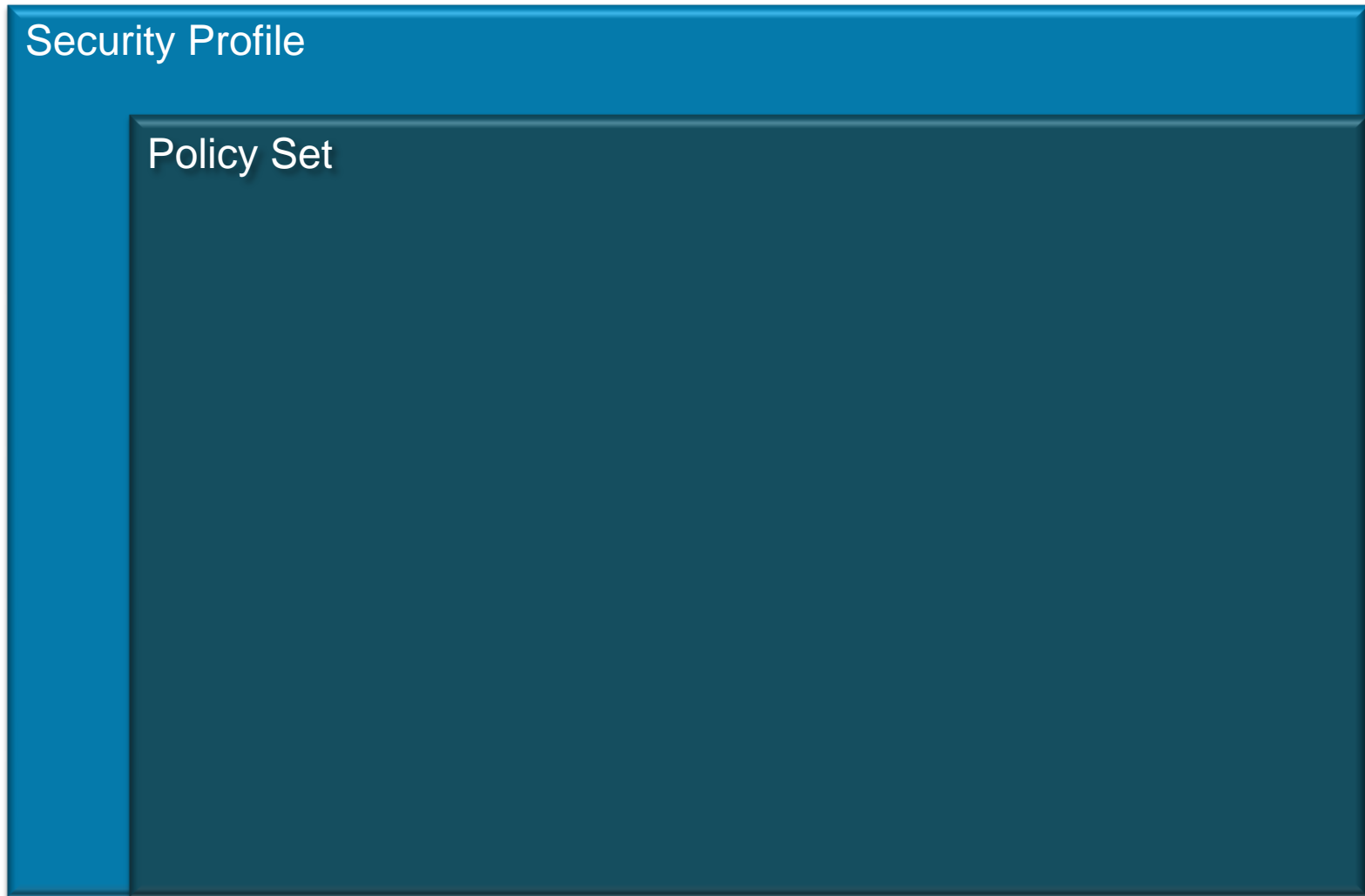
Security Profile

A large blue rectangular box with a thin black border, representing a Security Profile. The text "Security Profile" is written in white in the top-left corner of the box.

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

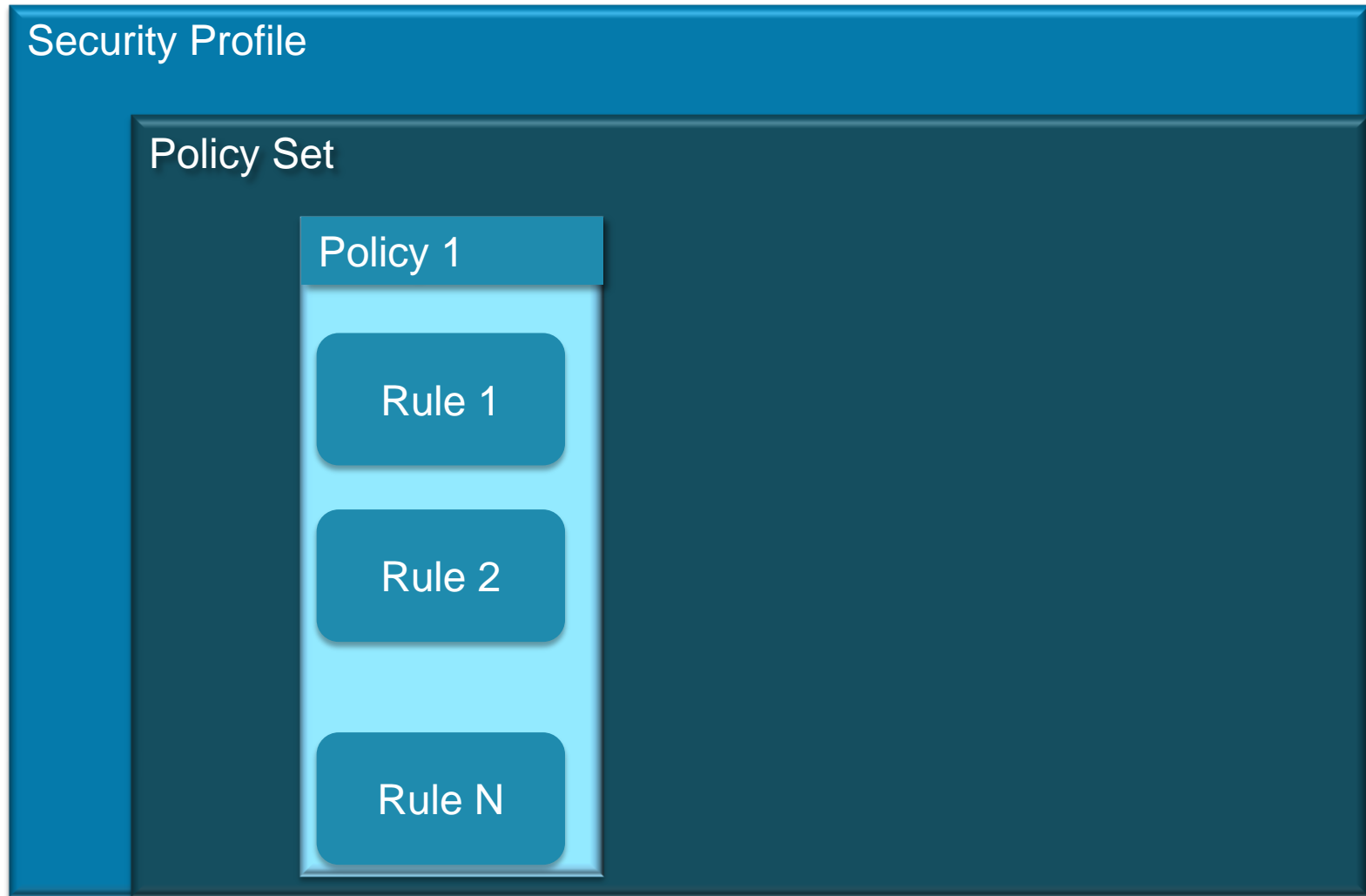


# Security Policy Building Block



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



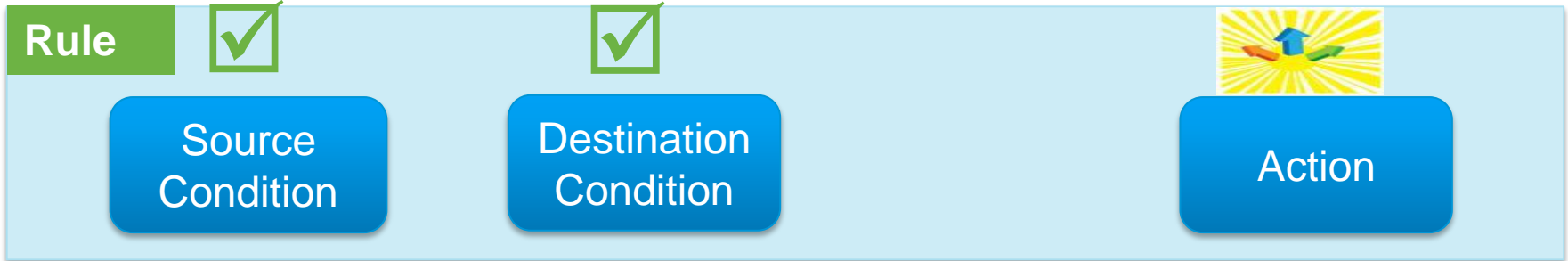
Rule is analogous to an ACE; Policy is analogous to an ACL

# Security Policy Building Block

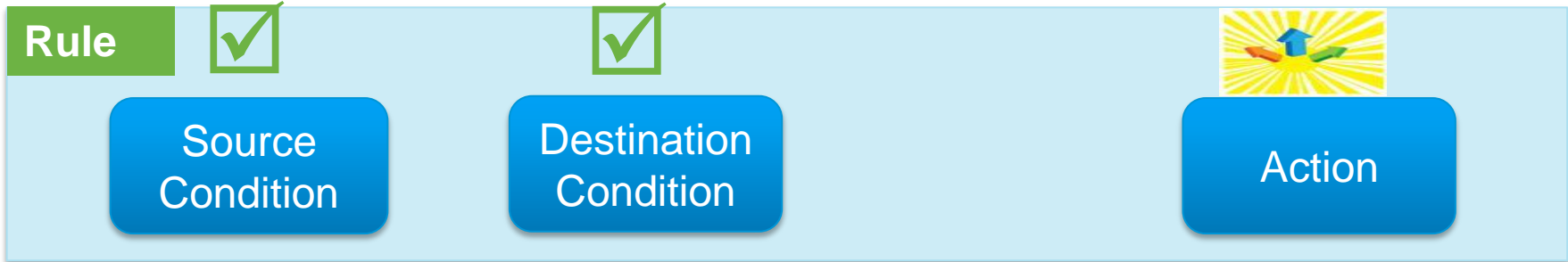


Rule is analogous to an ACE; Policy is analogous to an ACL

# VSG Policy: Rule (ACE) Construct



# VSG Policy: Rule (ACE) Construct



## Condition

Attribute Type :

Network ▼

Attribute Type

Network

VM

User Defined

vZone

Expression

Attribute Name :

IP Address

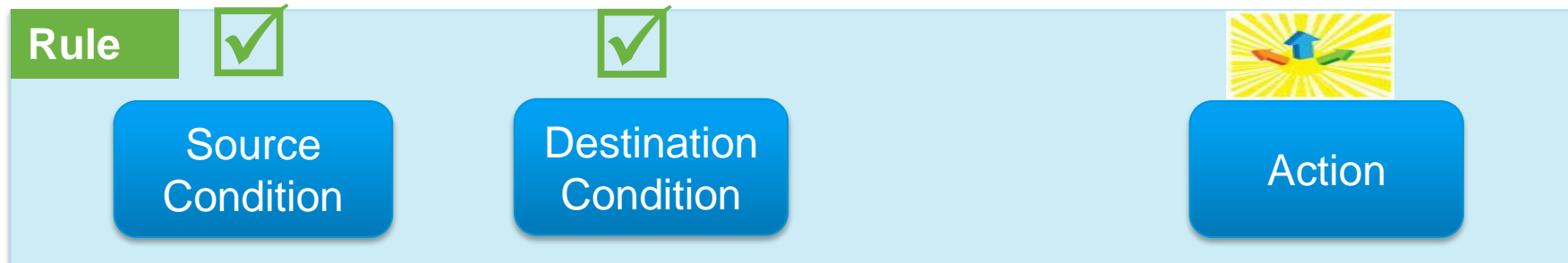
Operator :

eq ▼

Attribute Value :

192 . 168 . 1 . 2

# VSG Policy: Rule (ACE) Construct



## Condition

Attribute Type :

Network

Attribute Type

Network

VM

User Defined

vZone

Expression

Attribute Name :

IP Address

Operator :

eq

Attribute Value :

192 . 168 . 1 . 2

VM Attributes

VM Name

Guest OS full name

Resource Pool

Parent App Name

Port Profile Name

Cluster Name

VM DNS Name

Hypervisor Name

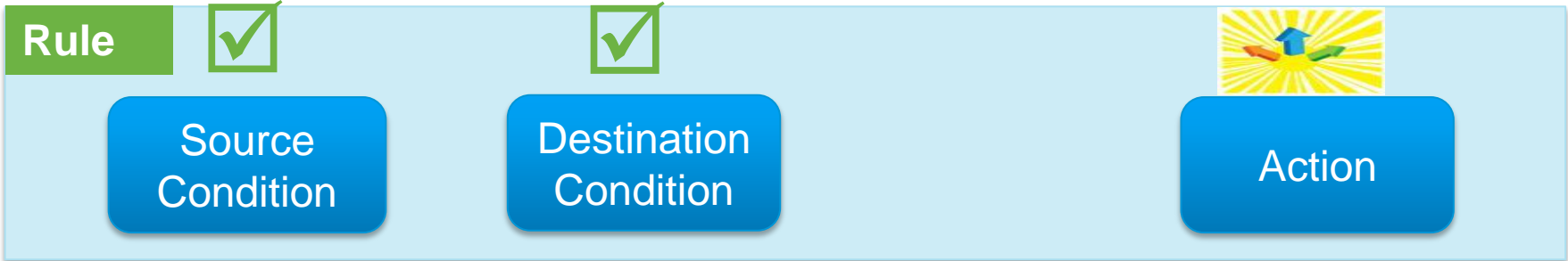
Network Attributes

IP Address

Network Port

New

# VSG Policy: Rule (ACE) Construct



## Condition

Attribute Type :

Network

### Attribute Type

- Network
- VM
- User Defined
- vZone

### Expression

Attribute Name :

IP Address

Operator :

eq

Attribute Value :

192 . 168 . 1 . 2

### VM Attributes

- VM Name
- Guest OS full name
- Resource Pool
- Parent App Name
- Port Profile Name
- Cluster Name
- VM DNS Name
- Hypervisor Name

### Network Attributes

- IP Address
- Network Port

### Operator

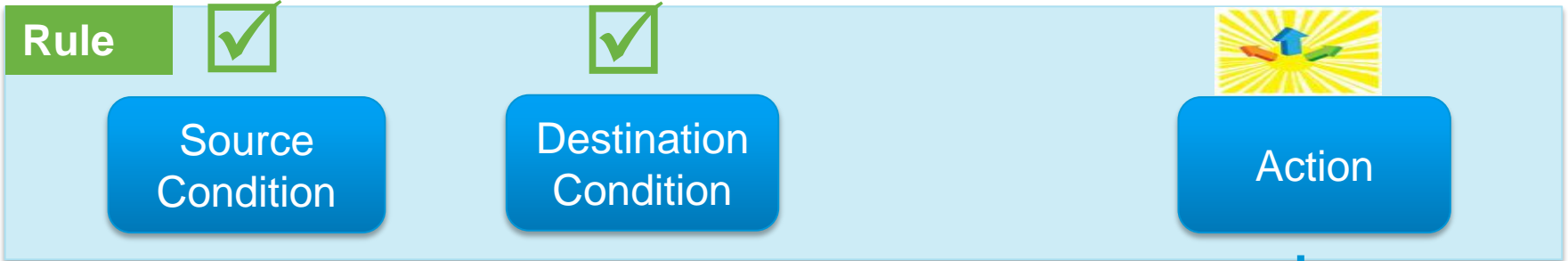
- eq
- neq
- gt
- lt
- range
- Not-in-range
- Prefix

### Operator

- member
- Not-member
- Contains



# VSG Policy: Rule (ACE) Construct



The screenshot shows the configuration interface for a Condition. The **Condition** header is highlighted in blue. The **Attribute Type** is set to **Network**. The **Expression** section shows the **Attribute Name** as **IP Address**, the **Operator** as **eq**, and the **Attribute Value** as **192 . 168 . 1 . 2**. The **Action** section shows radio buttons for **drop** (selected), **permit**, and **reset**, and a checkbox for **log**. A purple starburst labeled **New** is positioned near the Action section.

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

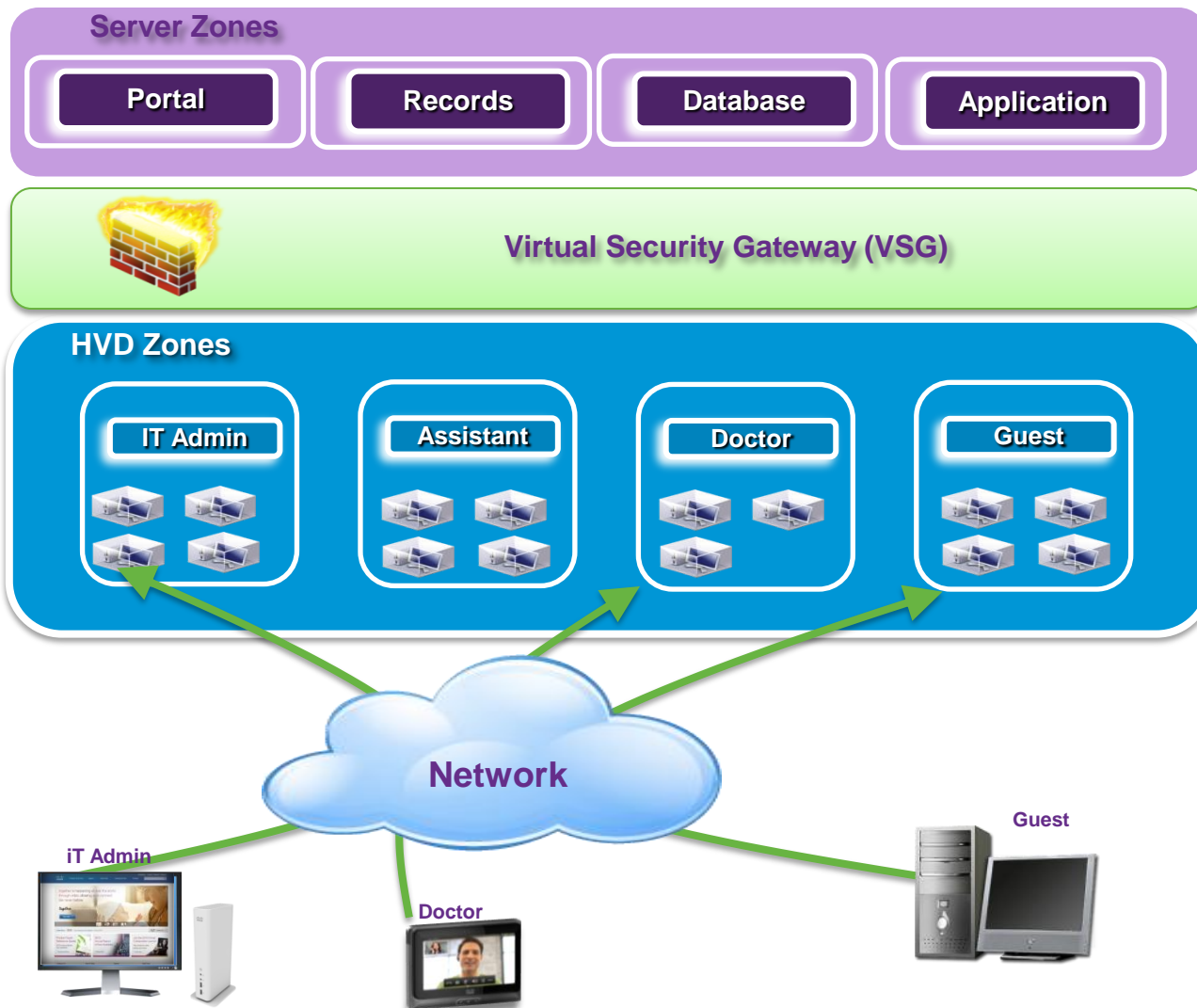
Network Attributes
IP Address
Network Port

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

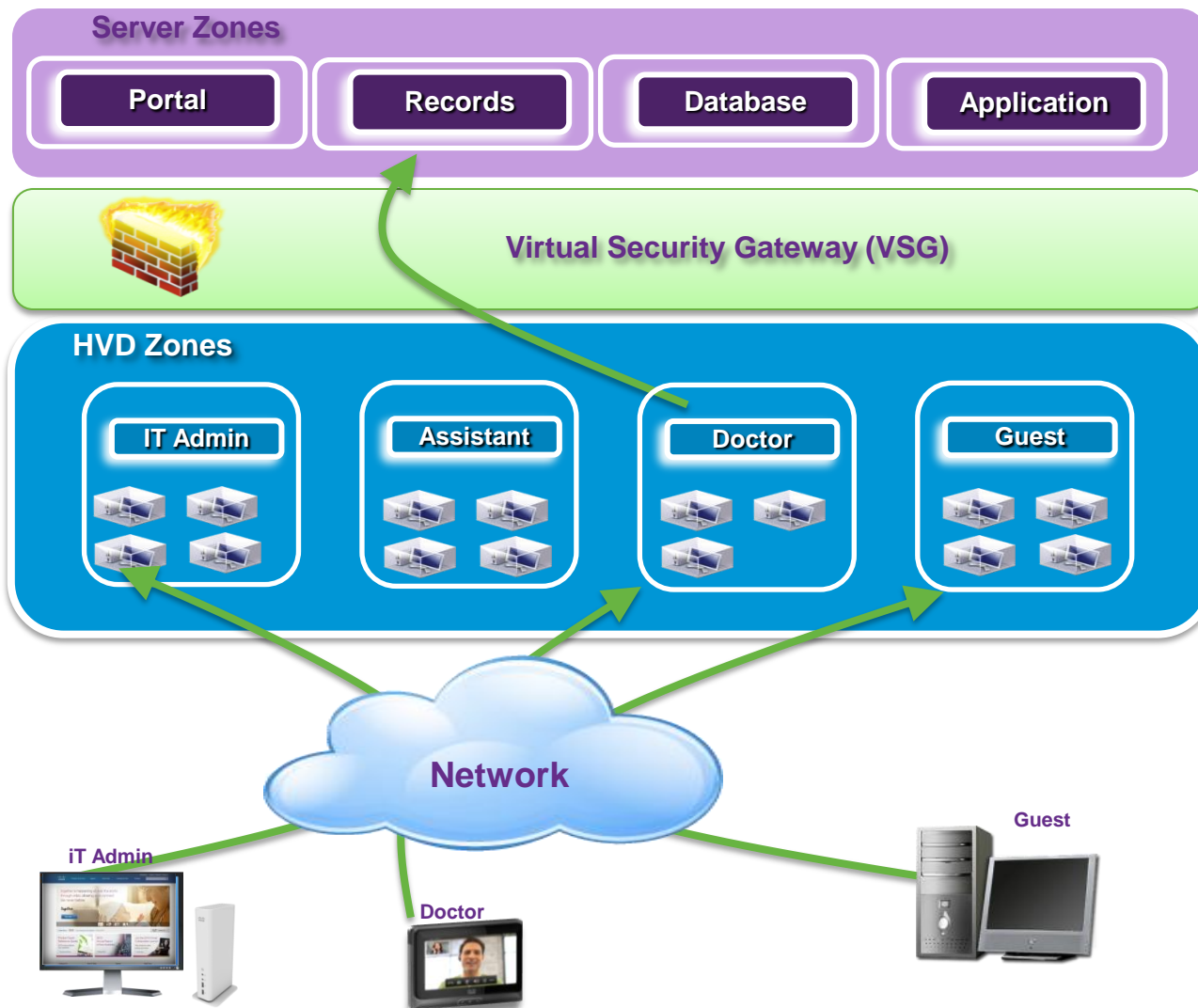
Operator
member
Not-member
Contains

# VSG: Use Cases

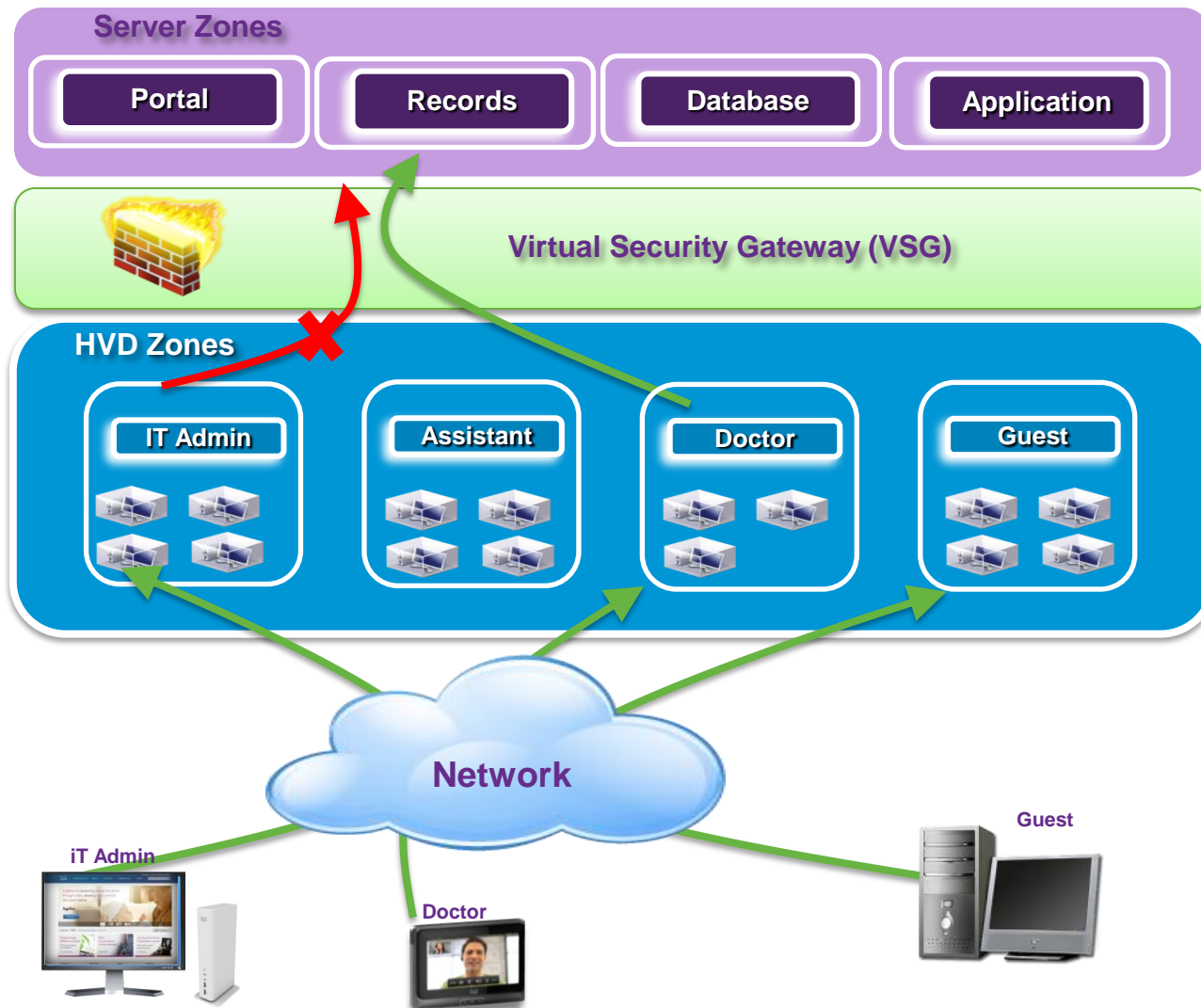
# VSG Deployment for VDI



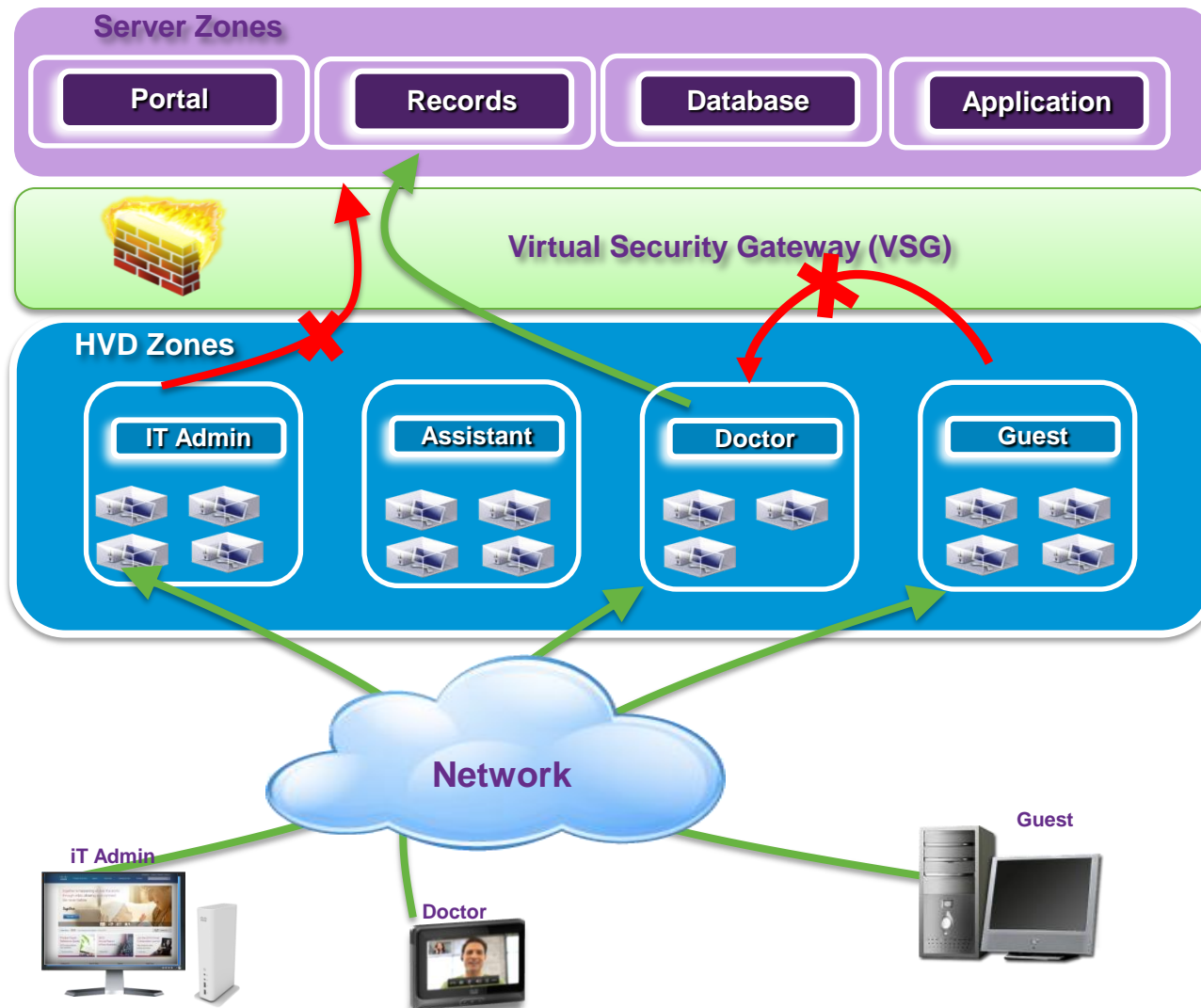
# VSG Deployment for VDI



# VSG Deployment for VDI

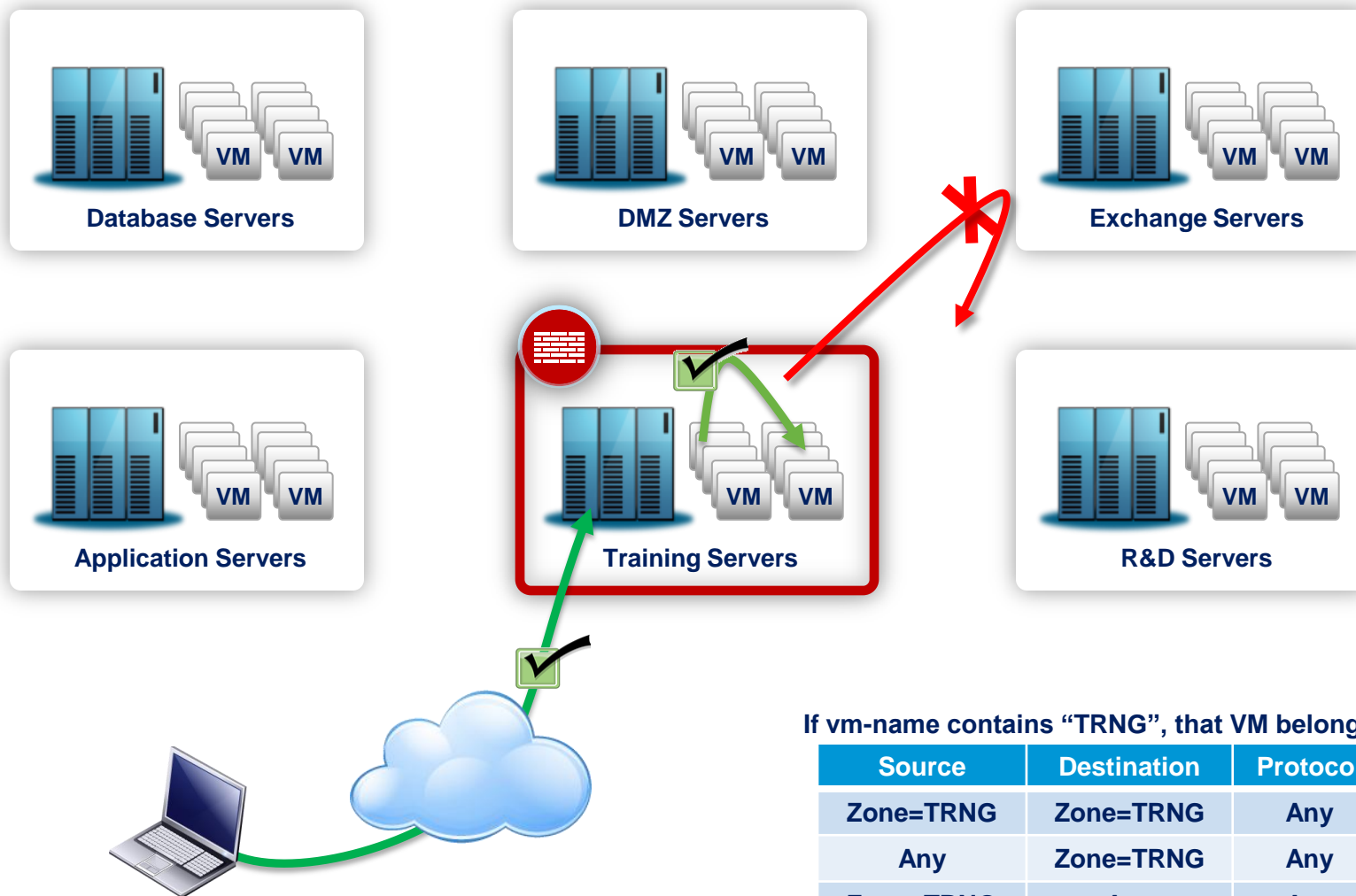


# VSG Deployment for VDI



# VSG Deployment at CareCore National

## Logical zoning, vMotion support & scalable solution



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

# VSG Deployment in a 3-tier DC

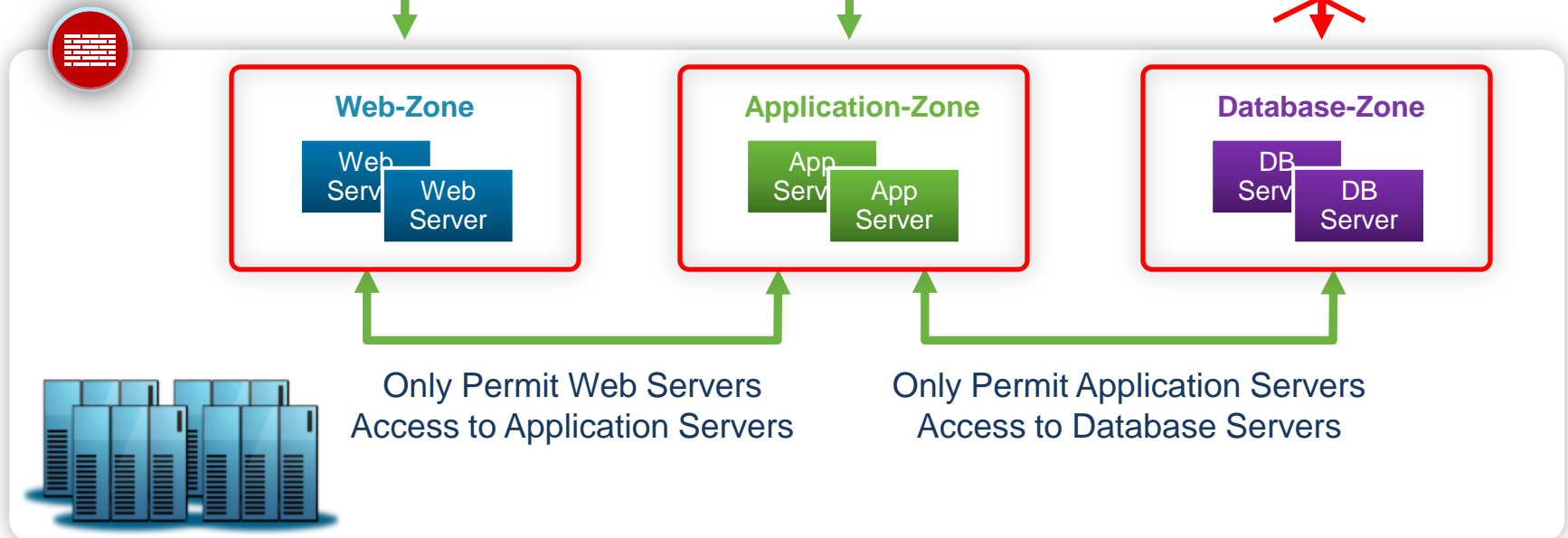
## Securing Web, Apps & DB servers



Permit Only Port 80(HTTP)  
of Web Servers

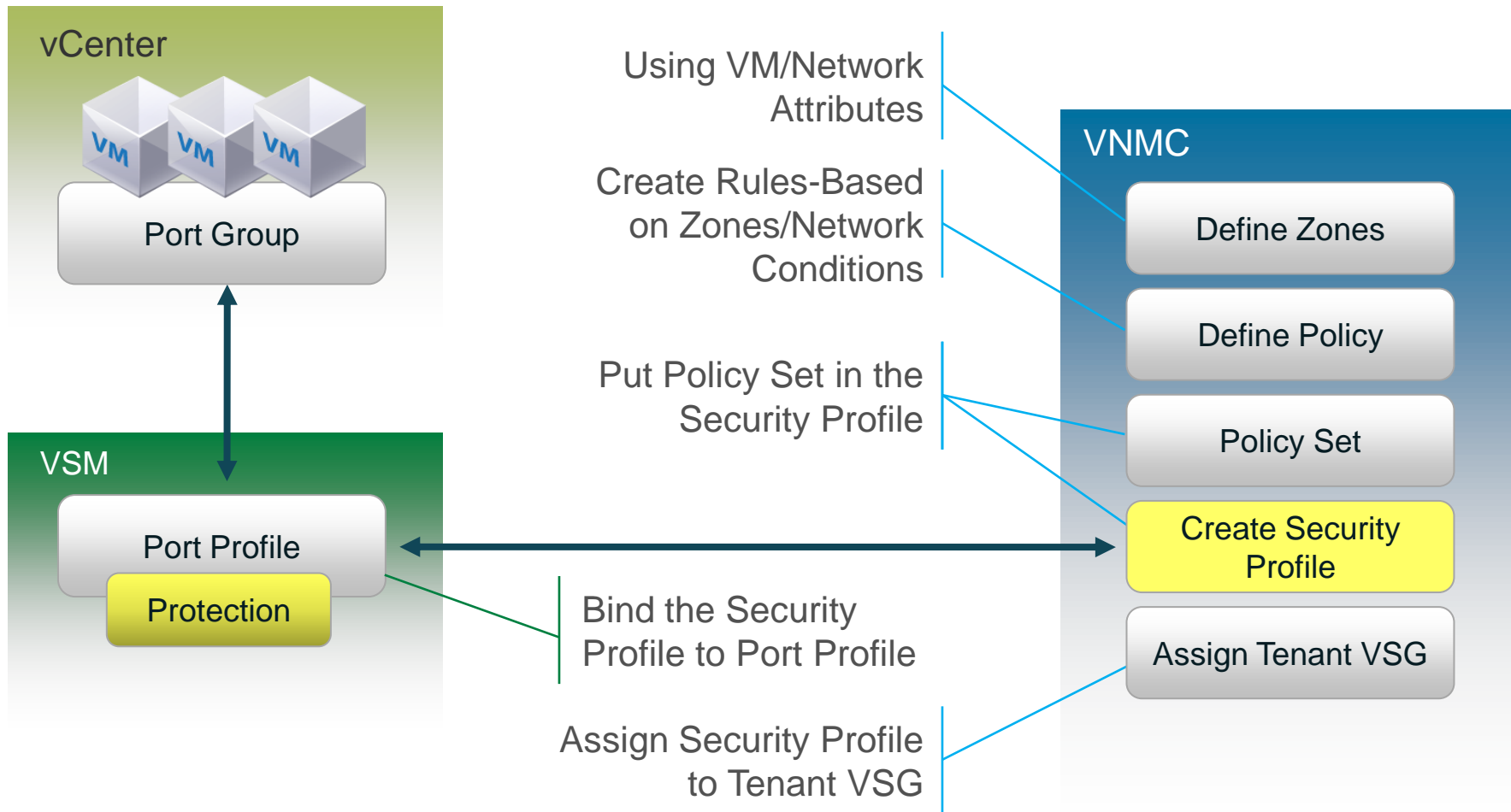
Permit Only Port 22 (SSH)  
to Application Servers

Block All External Access  
to Database Servers





# 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 left sidebar shows a tree view with 'TenantA' expanded, and 'vZones' selected at the bottom. The main content area shows the 'vZones' configuration page for 'TenantA' in 'Advanced' mode. A table with a yellow border highlights the 'Name' column, containing the entries 'AppZone', 'DBZone', and 'WebZone'. The interface includes tabs for 'Security Policies', 'Device Configurations', 'Capabilities', and 'Diagnostics' at the top, and 'General' and 'Faults' for the current configuration page.

# 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. At the top, there are navigation tabs: 'Tenant Management', 'Resource Management', 'Policy Management' (highlighted), and 'Administration'. Below this, there are sub-tabs: 'Security Policies', 'Device Policies', 'Capabilities', and 'Diagnostics'. The main content area shows a tree view on the left with 'Firewall Policy' expanded to 'root'. A dialog box titled 'Edit (WebZone)' is open, showing the 'Conditions' tab. The table below has the following data:

Attribute Name	Operator	Attribute Value
Instance Name	contains	Web

# 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 Security Policy Management interface. The top navigation bar includes tabs for Security Policies, Device Configurations, Capabilities, and Diagnostics. The left sidebar shows a tree view of the configuration hierarchy, with the 'Policies' folder under 'TenantA' selected. The main content area shows the 'Policies' configuration page for 'TenantA', with the 'General' tab active. A yellow box highlights the '+ Add Policy' button and the 'Name' input field, which contains the text 'Content\_Policy'.

# 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 a Content Policy. 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, including WebTraffic, DB-SSH, DBZone-WebZ, WebZone-DBZ, and Deny\_All\_Zone.

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. On the left, a navigation tree shows the hierarchy: Security Profiles > Advanced > Demo > TenantA > Security Profiles > Advanced. The main content area is titled 'Edit (Content\_PolicySet)' and is divided into two tabs: 'General' (selected) and 'Events'. The 'General' tab contains the following fields and controls:

- Name:** Content\_PolicySet
- Description:** Policy Set for Content Hosting Policies for Tenant A
- Policies:** A section with an information icon, a '+ Add Policy' button, and an 'Edit' button.
- Available :** A list containing the item 'default'.
- Assigned :** A section with four arrow icons (up, up, down, down) and a list containing the item 'Content\_Policy', which is highlighted with a yellow box.

A yellow arrow points from the 'Content\_PolicySet' entry in the 'Policy Sets' table above to the 'Content\_Policy' entry in the 'Assigned' list below.

# 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 configuration interface for a Security Profile. On the left, a tree view shows the hierarchy: TenantA > Security Profiles > Secure\_TenantA (highlighted). The right pane shows the configuration form for 'Secure\_TenantA'. The 'Name' field is 'Secure\_TenantA'. The 'Policy set' dropdown menu is set to 'Content\_PolicySet' and is highlighted with a yellow box. Below this, the 'Resolved Policy Set' is shown as 'org-root/org-T'. At the bottom, a 'Resolved Policies' section contains a table with one entry: 'Content\_Policy'.

Name	Source Condition
Content_Policy	

Policies can also be Authored from Security Profile



# 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 management console interface. On the left, a tree view under 'Virtual Security Gateways' shows a hierarchy: root > TenantA > VSG-TenantA. The 'VSG-TenantA' node is highlighted. On the right, the 'VSG-TenantA' configuration page is shown with tabs for 'General', 'Firewall Details', 'VSG Details', 'Faults', and 'Events'. The 'VSG Details' tab is active, and a yellow box highlights the following configuration details:

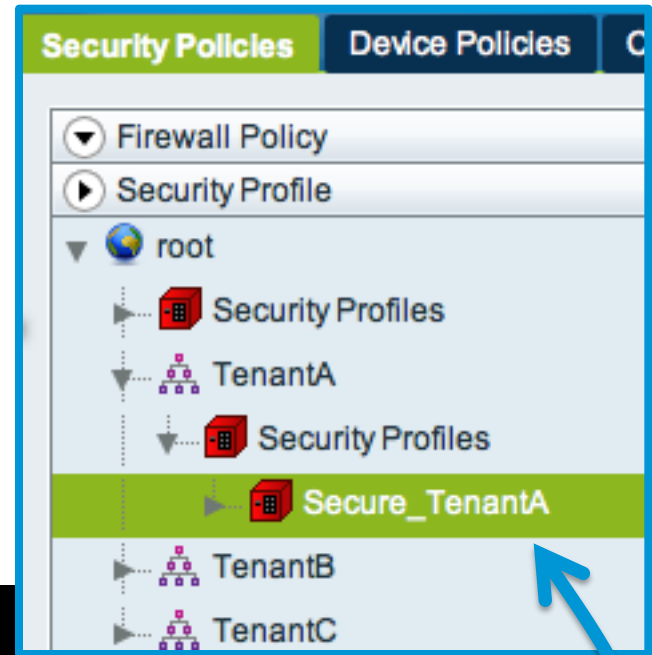
VSG Service ID:	1005
VSG Mgmt IP:	10.29.173.42
HA Role:	standalone
Association:	associated

# 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 selected, and the 'Network adapter 1' is highlighted in the hardware list. The right-hand pane shows the configuration for this network adapter, including 'Device Status', 'Adapter Type', 'MAC Address', and 'Network Connection'. The 'Network Connection' dropdown is highlighted with a yellow box, showing 'TenantA (VSM-Nexus1000V)' selected. Below it, the 'Port' is set to '356'. The 'Specify standalone port (Advanced)' options are also visible.

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

Virtual Machine Version: 7

Device Status

- Connected
- Connect at power on

Adapter Type

Current adapter: Flexible

MAC Address

00:50:56:94:33:d1

Automatic  Manual

Network Connection

TenantA (VSM-Nexus1000V)

Port: 356

Specify standalone port (Advanced):

DVS: [ ]

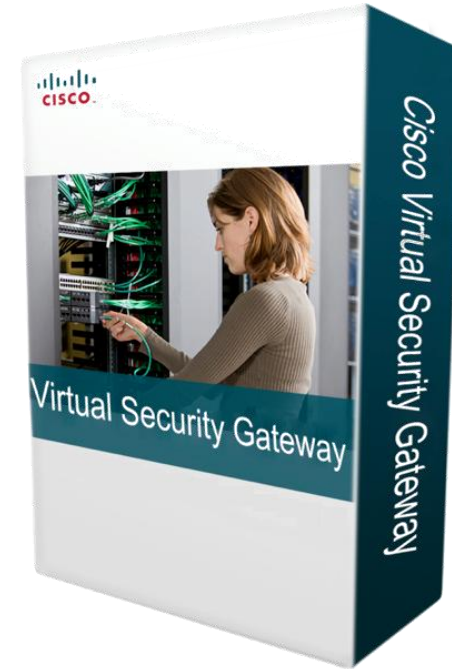
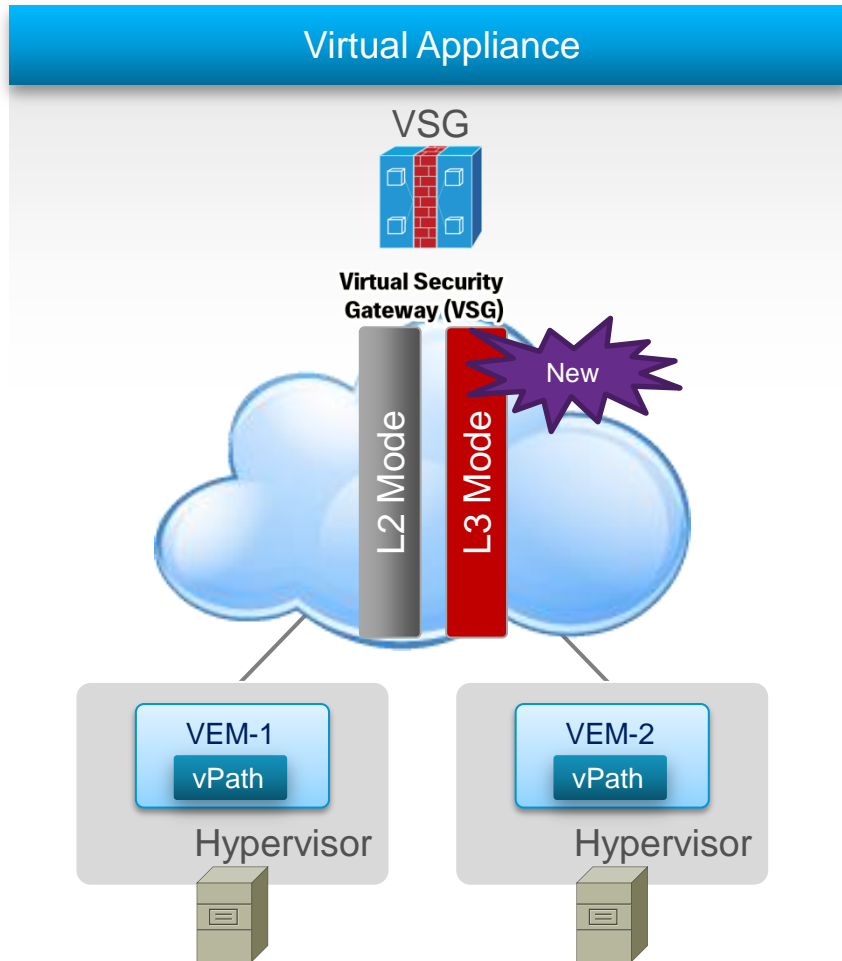
Port ID: [ ]



# Virtual Security Gateway (VSG) v1.3 Release

# VSG1.3: Flexible deployment options

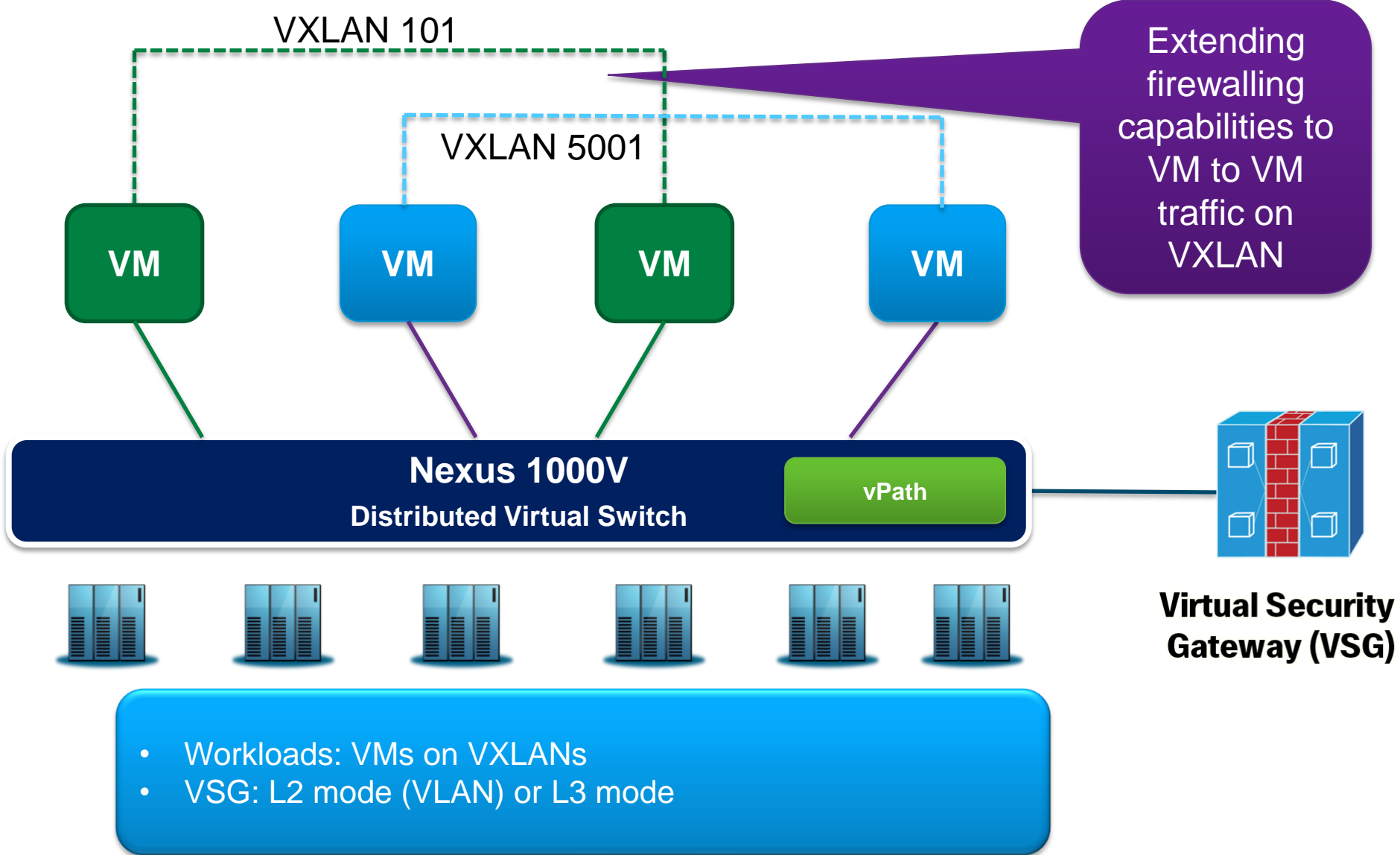
## *vSphere 5.0 support and Layer 2 & Layer 3 deployment options*



VMware Product	VSG & VNMCM support
vSphere 4	<input checked="" type="checkbox"/>
vSphere 5	<input checked="" type="checkbox"/> <span style="color: purple;">New</span>

# VSG 1.3: Securing VMs on VXLANs

*Enabling zone firewalling capabilities to VMs on VXLAN*



# VSG 1.3: vSphere 5.0 support

- Hitless upgrade with HA mode
  - Standby VSG is upgraded first, and then after a switchover previously active VSG is upgraded

- Upgrade procedure

Stage 1: Upgrading Cisco VNMC

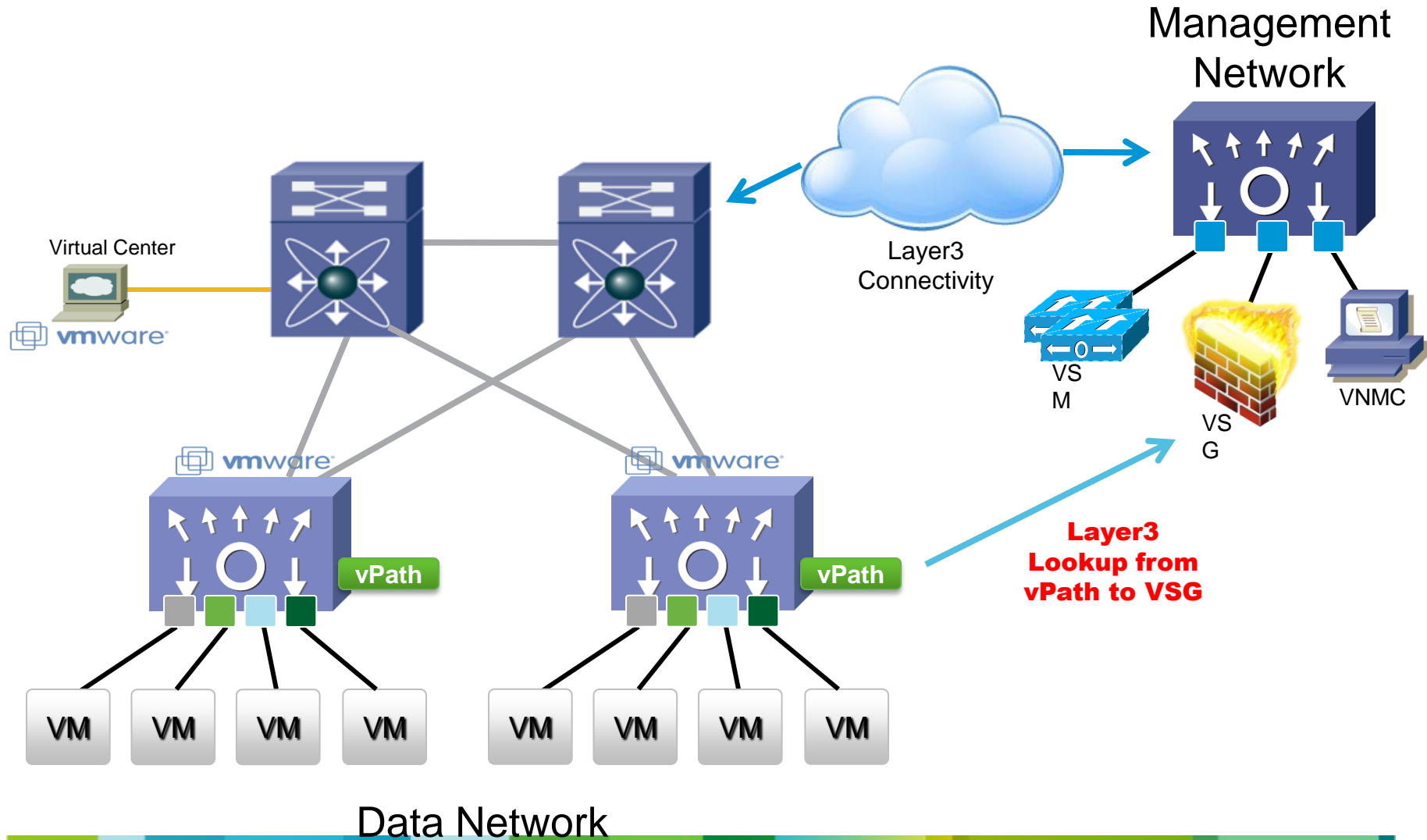
Stage 2: Upgrading a Cisco VSG Pair

Stage 3: Upgrading the Cisco VSM Pair and the VEM

- Supported versions

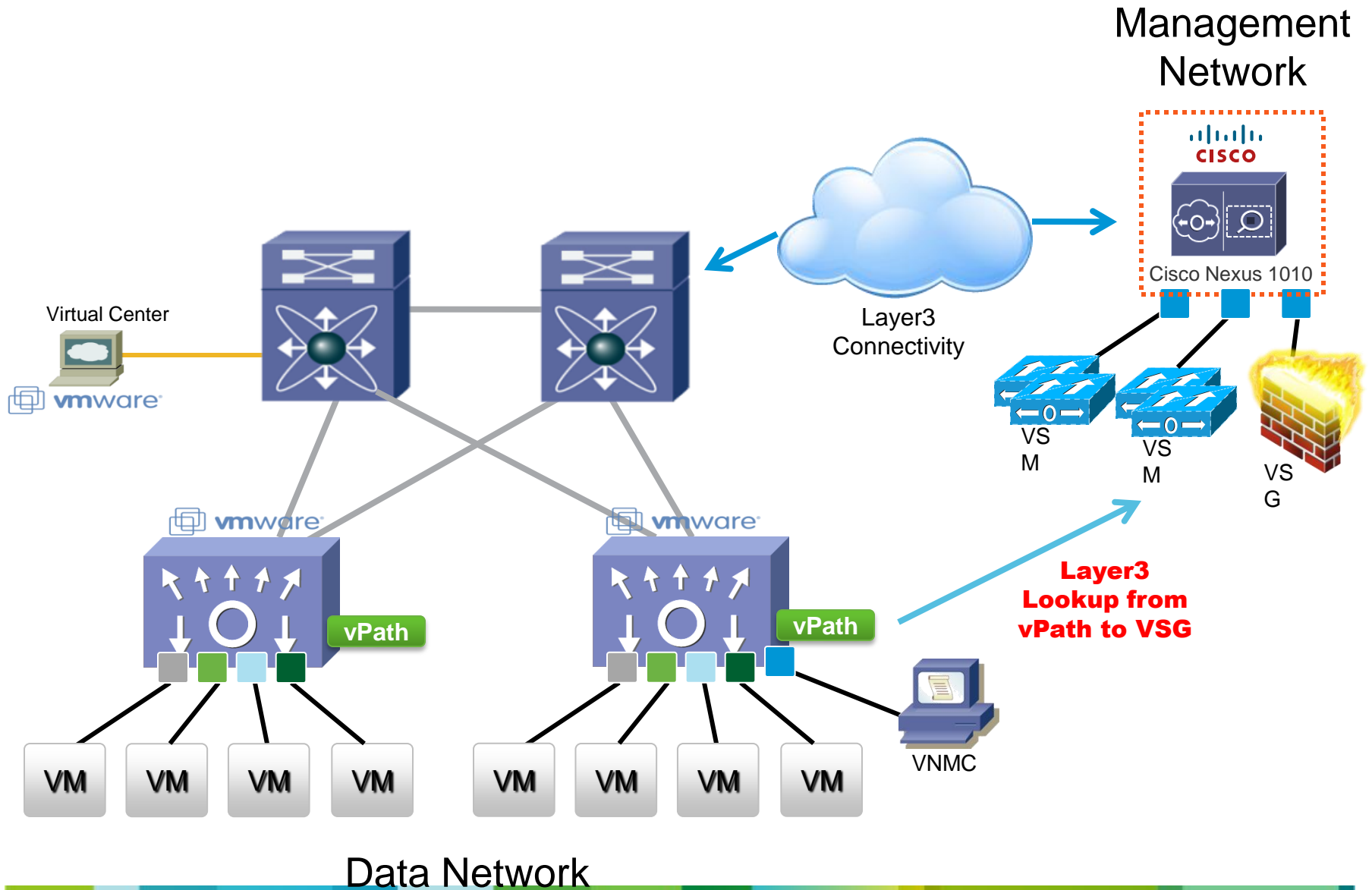
	N1KV Version	VSG Version
vSphere 5.0 Support	4.2(1)SV1(4a) Or 4.2(1)SV1(5.1)	4.2(1) VSG1(3.1)

# VSG 1.3: Layer 3 deployment





# VSG 1.3: Layer 3 deployment with N1010



# VSG 1.3: L3 Support Prerequisite

- Proxy ARP is needed on the upstream router.
- VEM sends ARP request for VSG IP address then uses the response as destination MAC.
- VSG assumes return path goes through the same router and flips the MAC header.

# VSG 1.3: L3 Interfaces

- Each VEM needs to have vmknics with I3-vn-service capability
- Up to four I3-vn-service vmknics are supported.
- Egress vmknics are selected based on source MAC hash.
- All vmknics need to be able to reach the VSG.
- If vPC-HM is configured to connect to multiple upstream switches, MAC-pinning will try to distribute the vmknics among each subgroup in the port channel evenly.
- Repin happens whenever one vmknics' state or configuration is changed.

# VSG 1.3: Health Probe

- For L2 mode, sticky ARP (ARP request every 6 seconds) is used to determine health of VSG.
- VSG is brought down after 3 tries.
- For L3 mode, sticky ARP is not used.
- vPath PING PDU is sent every 6 seconds to determine health of VSG.
- VSG is also brought down after 3 tries.
- ARP lookup is done before sending to VSG. Will be cached as regular ARP entry (20-min timeout).
- Whenever VSG data IP changes, its GARP should update the router proxy ARP information.

# Configuration and Troubleshooting



# L3 Interface Configuration

```
vsm-stargate (config-port-prof) #
```

```
capability l3-vn-service
```

- The same VSG can operate in L2 and L3 mode at the same time.
- When redirecting traffic to L3 mode VSG, the access vlan configured under the l3-vn-service vmknic will be used.
- Same vmknic can be shared by different capabilities, e.g. vxlan and l3control, except for iscsi-multipath.
- In addition to even distribution of vmknics with the same capability, MAC-pinning tries to distribute total number of vmknics that have capability evenly.

# Configuration Verification

```
vsm-stargate# module vem 3 execute vemcmd show port
```

LTL	VSM Port	Admin	Link	State	PC-LTL	SGID	Vem Port	Type
17	Eth3/1	UP	UP	F/B*	305	0	vmnic0	
18	Eth3/2	UP	UP	F/B*	305	1	vmnic1	
22	Eth3/6	UP	UP	F/B*	305	5	vmnic5	
49	Veth7	UP	UP	FWD	0		US193-3.eth1	
50	Veth9	UP	UP	FWD	0	0	vmk0	VXLAN
51	Veth1	UP	UP	FWD	0		US193-1.eth1	
52	Veth10	UP	UP	FWD	0	1	vmk1	L3VNSER
305	Po1	UP	UP	F/B*	0			

\*F/B: Port is BLOCKED on some of the vlans.

```
vsm-stargate# module vem 3 execute vemcmd show pinning
```

LTL	IfIndex	PC_LTL	VSM_SGID	Eff_SGID	iSCSI_LTL*	Name
10	0	305	32	5	0	
12	0	305	32	1	0	
50	1c000080	305	32	0	0	vmk0
52	1c000090	305	32	1	0	vmk1

iSCSI\_LTL\* : iSCSI pinning overrides VPC-HM pinning

# Sample Configuration

vmknic port profile seen in the last verification output

```
port-profile type vethernet 13vns
  vmware port-group
  switchport mode access
  switchport access vlan 64
  capability 13-vn-service
  no shutdown
  state enabled
```

```
port-profile type vethernet vxlan
  vmware port-group
  switchport mode access
  switchport access vlan 64
  capability vxlan
  no shutdown
  state enabled
```



# vPath | VSN Configuration

```
vsm-stargate (config-port-prof) #
```

```
vn-service ip-address <ipv4> vlan <vlan#> [{security-  
profile <profile-name> | fail {open | close}}]
```

```
vn-service ip-address <ipv4> l3-mode [{security-profile  
<profile-name> | fail {open | close}}]
```

- The same VSG can operate in L2 and L3 mode at the same time.
- When redirecting traffic to L3 mode VSG, the access vlan configured under the l3-vn-service vmknic will be used.

# Configuration Verification

```
vsm-stargate# show vsn brief
VSM-BKP# show vsn brief
  VLAN          IP-ADDR          MAC-ADDR  FAIL-MODE  STATE  MODULE
  -            192.168.129.2    -         Close     Up     3
  64           192.168.134.1  00:50:56:bb:00:2c  Open     Up     4

vsm-stargate# show vsn detail
#VSN VLAN: 64, IP-ADDR: 192.168.129.2
  MODULE      VSN-MAC-ADDR  FAIL-MODE  VSN-STATE
  3           -             Close     Up
#VSN VLAN: 64, IP-ADDR: 192.168.134.1
  MODULE      VSN-MAC-ADDR  FAIL-MODE  VSN-STATE
  4  00:50:56:bb:00:2c  Open     Up

#VSN Ports, Port-Profile and Security-Profile Association:
#VSN VLAN: -, IP-ADDR: 192.168.129.2
  Port-Profile: vsg129-2, Security-Profile: default
  Module  Vethernet
  3  2
#VSN VLAN: 64, IP-ADDR: 192.168.134.1
  Port-Profile: vsg134, Security-Profile: default
  Module  Vethernet
  4  7
```

# Sample Configuration

Two VSGs as seen in the last verification output

```
port-profile type vethernet vsg129-2
  vmware port-group
  switchport mode access
  switchport access vlan 63
  vn-service ip-address 192.168.129.2 13-mode security-profile sp1
  no shutdown
  state enabled

port-profile type vethernet vsg134
  vmware port-group
  switchport mode access
  switchport access vlan 63
  vn-service ip-address 192.168.134.1 vlan 64 fail open security-profile sp1
  no shutdown
  state enabled
```

# Troubleshooting CLI on VSM

```
vsm-stargate#
```

```
show vsn {brief | detail}
```

- Displays all the VSNs and their state

```
vsm-stargate#
```

```
show vsn statistics [{ip addr [module mod#]} | {module  
mod#} | {vlan vlan#}]
```

- Displays the VSN statistics
- IP, module & vlan are just filtering keywords

# Troubleshooting CLI on VSM

```
vsm-stargate#
```

```
show vsn port vethernet
```

- Displays details of the ports where vns is configured

```
vsm-stargate#
```

```
clear vsn statistics [{module mod#} | {vlan vlan#}]
```

- Clears the statistics on the specified module
  - Or those configured on the specified vlan

# Troubleshooting CLI on VEM

```
[root@smkumar-esx-2 /]#
```

```
vemcmd show vsn config
```

- Displays configuration of all VSNs available on the host

```
VNS Enabled | VNS Licenses Available 1
VSN#  VLAN          IP          STATIC-MAC          LEARNED-MAC  LTLs
  1     0    192.168.129.2  00:00:00:00:00:00  00:00:00:00:00:00    0
```

```
[root@smkumar-esx-2 /]#
```

```
vemcmd show vsn binding
```

- Displays port to VSN bindings

```
[root@smkumar-esx-2 /]# vemcmd show vsn binding
VNS Enabled | VNS Licenses Available 1
LTL  VSN  VLAN          IP          STATIC-MAC          LEARNED-MAC
  49   1    0    192.168.129.2  00:00:00:00:00:00  00:00:00:00:00:00
  51   1    0    192.168.129.2  00:00:00:00:00:00  00:00:00:00:00:00
```

# Troubleshooting CLI on VEM

```
[root@smkumar-esx-2 /]#
```

```
vemcmd show arp all
```

- Displays the ARP table on VEM

```
[root@smkumar-esx-2 /]#
```

```
vemlog show debug | grep sdp
```

- To obtain the available vPath debug options

```
[root@smkumar-esx-2 /]# vemlog show debug | grep sdp
```

<b>sfsdp</b>	ENWID P ( 95)	ENWIDTP (127)
sfsdpapi	ENWID P ( 95)	ENWIDTP (127)
<b>sfsdpfm</b>	ENWID P ( 95)	ENWIDTP (127)
sfsdpfsm	ENWID P ( 95)	ENWI ( 15)
sfsdputils	ENWID P ( 95)	ENWI ( 15)
<b>sfsdptun</b>	ENWID P ( 95)	ENWIDTP (127)
<b>sfsdpl3</b>	ENWID P ( 95)	ENWIDTP (127)

# Troubleshooting: Traffic fails

- Indication:
- Policies are configured on VSG to permit a certain type of traffic but it does not reach the destination – complete failure
  
- Problem:
- VSG is down
  
- Recommended Action:
- Do “show vsn brief” or “show vsn details” to check your VSG state.
- Make sure vmknic is configured and is attached to the correct port profile.
- Check VSG MAC is resolved by upstream router proxy ARP:  
vemcmd show arp all
- Make sure VSG is attached to the correct VLAN/port profile



# Troubleshooting: Traffic fails intermittently

- Indication:
  - Policies are configured on VSG to permit a certain type of traffic but sometimes traffic does not reach the destination
- Problem:
  - MTU is exceeded after vPath encapsulation
- Recommended Action:
  - “show vsn statistics vpath” should show drops because of MTU exceeded.
  - “vemlog show all” shows encapsulation failure because of MTU exceeded.
  - Make sure uplink MTU is adjusted with vPath encapsulation
  - Make sure upstream routers also have the correct MTU values

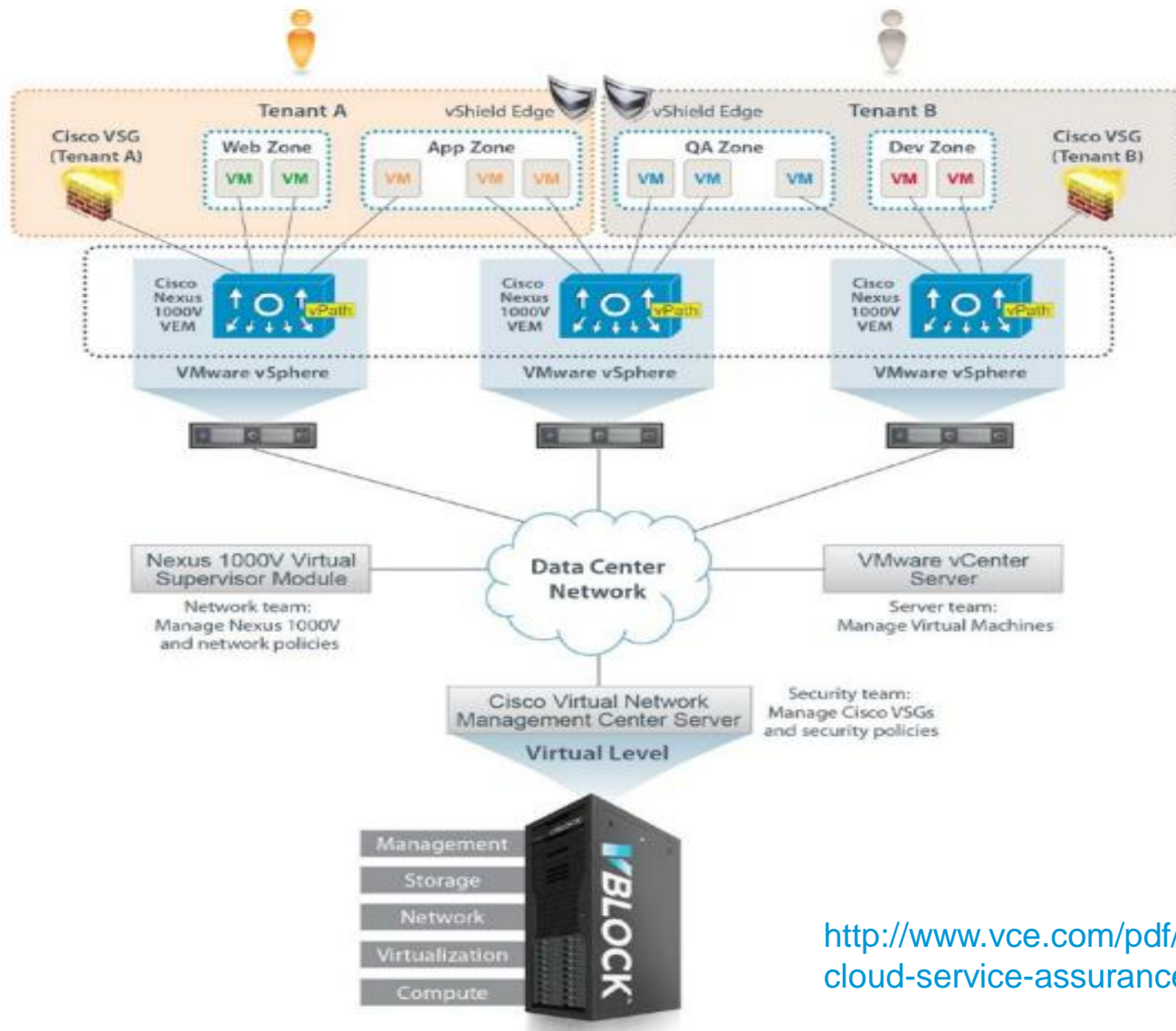
# Reference Solutions



# Reference Solutions

Solution	Nexus 1000V	Nexus 1010	Virtual Security Gateway
vBlock	✓		✓
Virtual Desktop	✓	Implicit Support	✓
Virtual Multi-tenant DC (VMDC)	✓	Implicit support	✓
Long-distance vMotion	✓	Implicit support	✓
PCI 2.0	✓	Implicit support	✓
Hosted Collaboration	✓	Implicit support	In progress

# Multi-tenant Deployment with Cisco VSG on Vblock Infrastructure Platform



<http://www.vce.com/pdf/solutions/vce-cloud-service-assurance.pdf>

# VMDC Security Control Framework

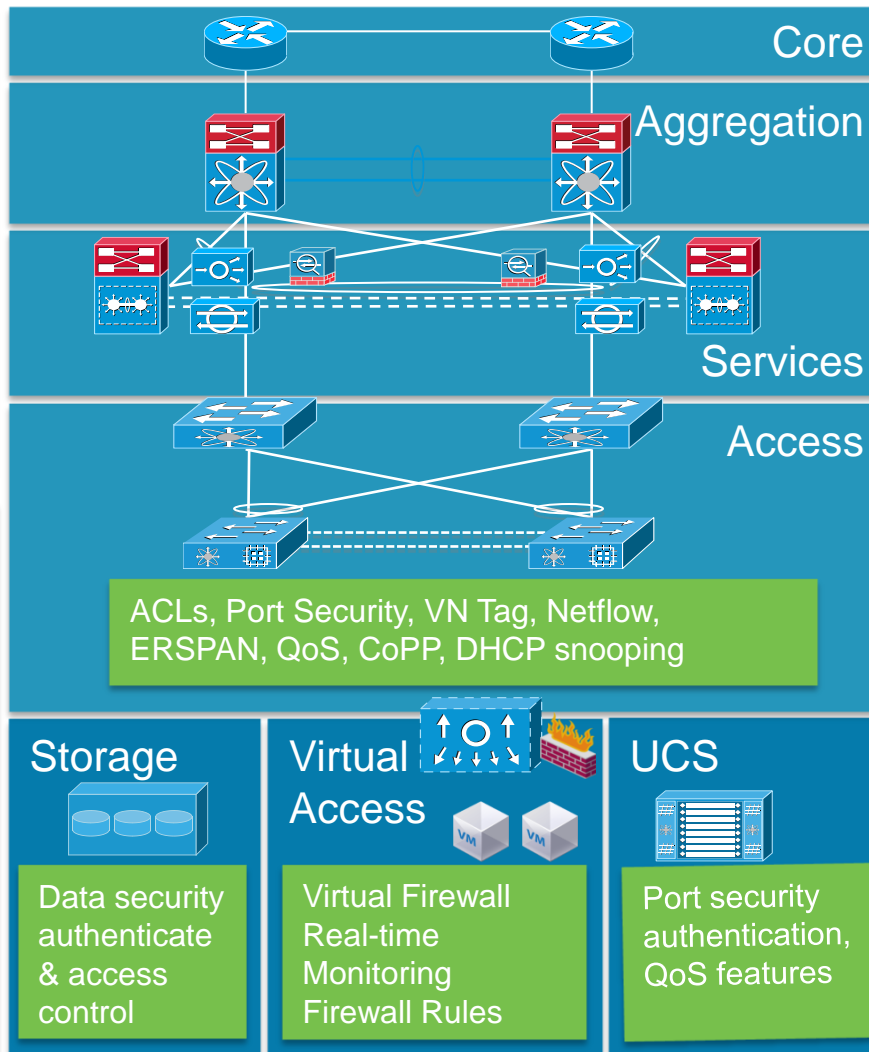
## The Sum Is Greater Than the Parts

### Security Management

- Visibility
- Event correlation, syslog, centralized authentication
- Forensics
- Anomaly detection
- Compliance

### Services

- Initial filter for DC ingress and egress traffic. Virtual Context used to split policies for server-to-server filtering
- Additional firewall services for server farm specific protection



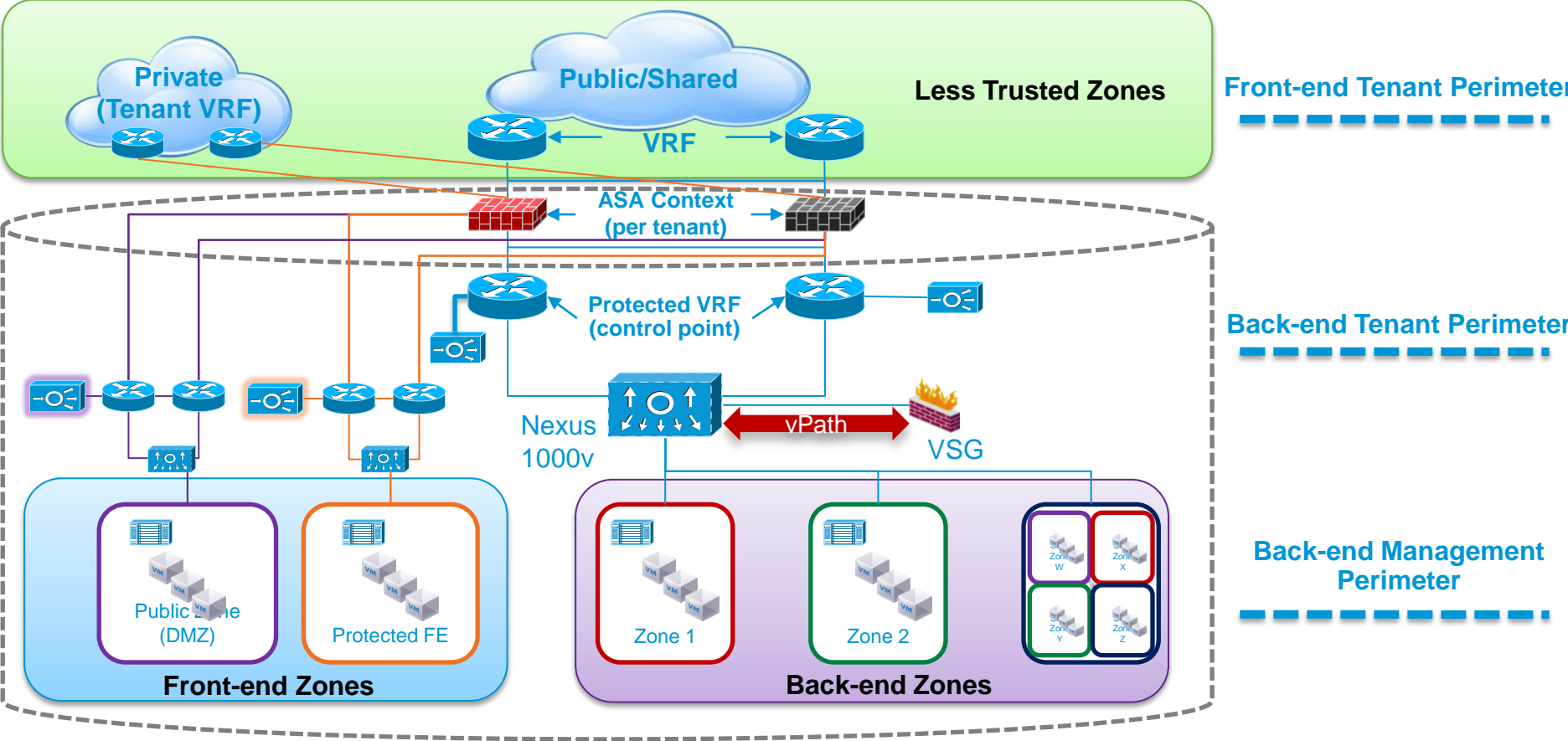
### Infrastructure Security

- Infrastructure Security features are enabled to protect device, traffic plane and control plane
- 802.1ae and vPC provides internal/external separation

### Services

- IPS/IDS provide traffic analysis and forensics
- Network Analysis provide traffic monitoring and data analysis
- Server load balancing masks servers and applications

# Tiered Security in VMDC 2.2



# What's coming?



# Cisco's Virtual Security Portfolio

Virtual Security Gateway

Zone based segmentation of VMs

ASA 1000V

External / multi-tenant edge deployment

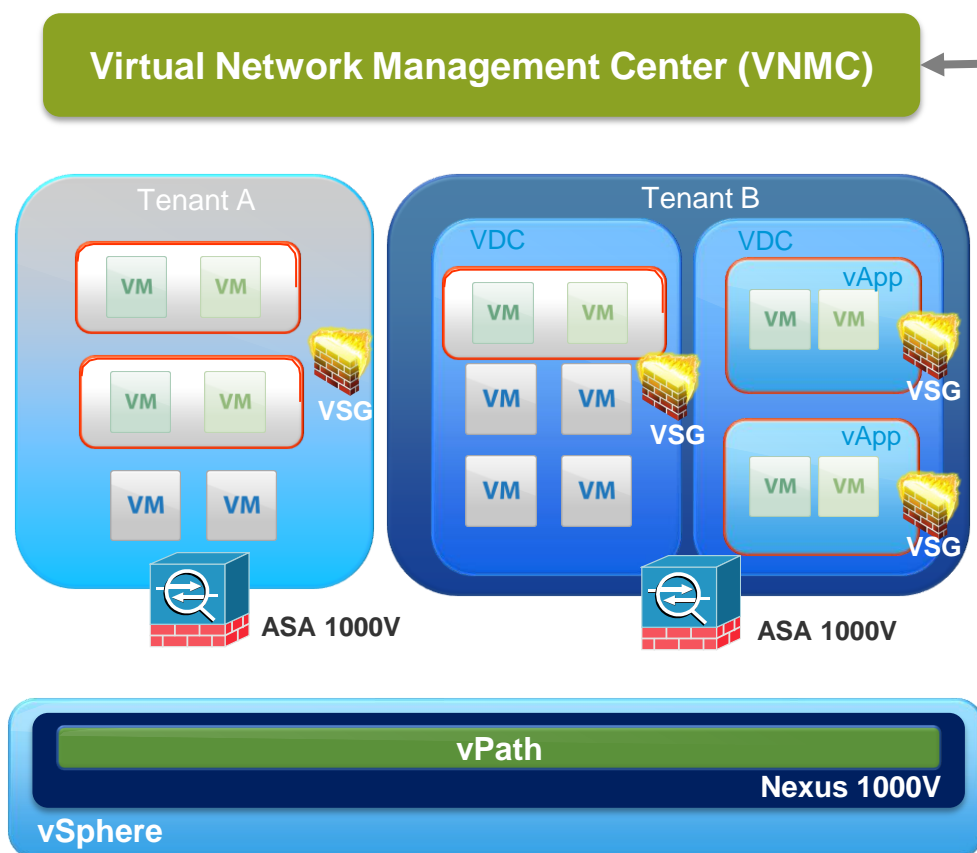
Hypervisor

Nexus 1000V

VNMC



# Cisco's Virtual Security Portfolio



VMware  
vCenter

- Virtual ASA provides consistent ASA feature set to secure the tenant edge

- VSG complements Virtual ASA to secure intra-tenant VM-to-VM traffic

- Solution provides:

- ✓ Increase flexibility and operational efficiency via vPath (Nexus1000V)

- ✓ Dynamic, context-aware, multi-tenant management via VNMC

# Why VSG?

- Efficient Deployment – no need to place on every server
- Granular enforcement – based on VM attributes
- Fast – with vPath cut-through processing
- Separation of duties – respected
- CPU capacity planning – decoupled operation between application workloads and FW instances
  - Optional hosting on Nexus 1010
- High availability – supported
- Server operations (add new servers, remove/upgrade servers) – seamless (FW is not in the way)
- Virtualization (eg vMotion) aware
- Integral component of multiple virtualization-centric CVDs (VMDC, VXI, DC-2-DC vMotion, PCI)

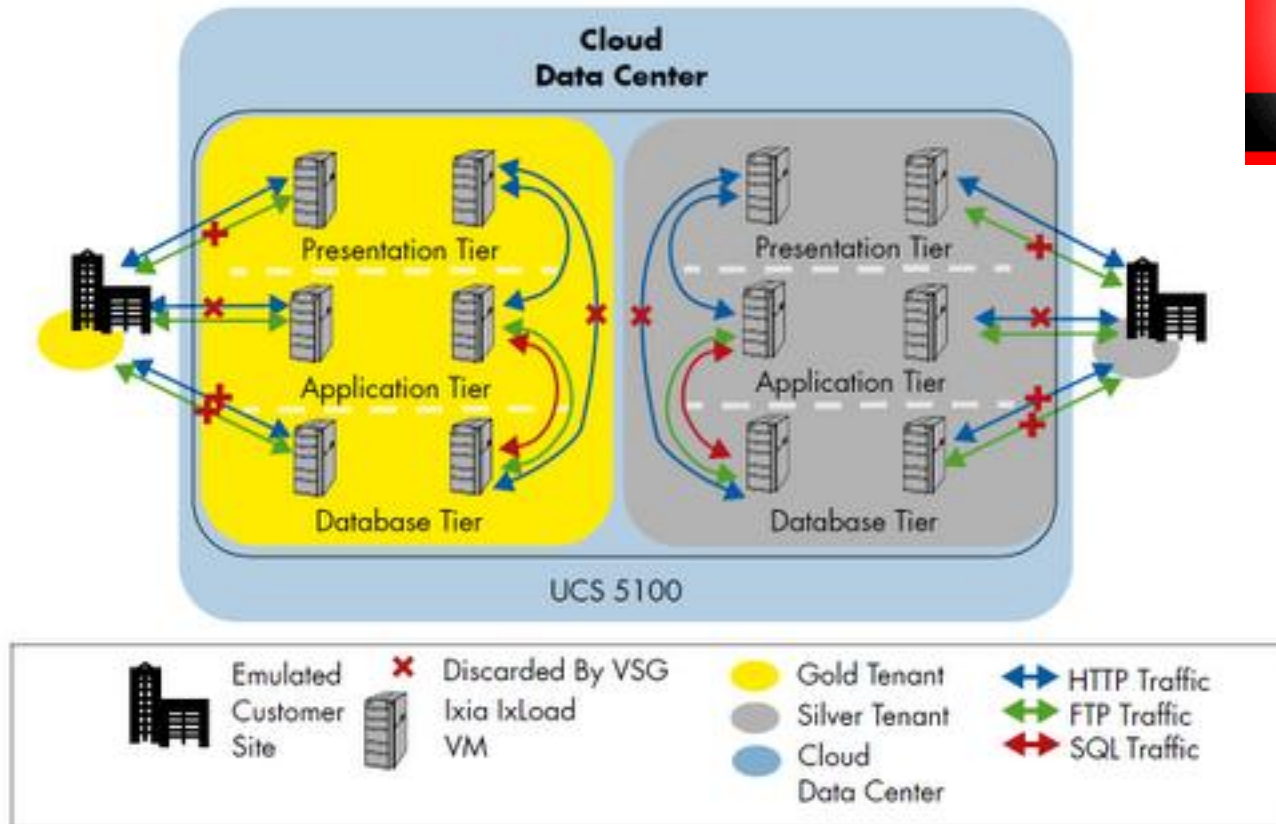
# Why ASA1000V?

- Physical and virtual consistency (operational behavior, features and policies)
- Mature ASA code base
- Layer-3 FW features
- Rich protocol support for stateful inspection
- vPath integrated
- High Availability - supported
- Separation of duties – respected
- Virtualization (eg vMotion) aware

# VSG testing analysis by LIGHTREADING



### Virtual Security Gateway Test Setup



[http://www.lightreading.com/document.asp?doc\\_id=216844](http://www.lightreading.com/document.asp?doc_id=216844)

# Resources





# Reference Solutions

- [Vblock with Nexus 1000V](#)
- [Vblock with VSG and vWAAS](#)
- [FlexPOD with Nexus 1000V and Nexus 1010](#)
- [Virtual Multi-tenant Data Center 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](#)

# Public Webcasts – Fall 2011



For Your  
Reference

Date	Technical Track Topics	Webinar	Preso
7/27	Long Distance vMotion with Nexus 1000V and VSG	<a href="#">Play</a>	<a href="#">PDF</a>
8/10	PCI Reference Architecture with Nexus 1000V and Virtual Security Gateway	<a href="#">Play</a>	<a href="#">PDF</a>
10/05	Nexus 1000V, VXLAN, and vCloud Director	<a href="#">Play</a>	<a href="#">PDF</a>
10/12	Virtualized Multi-Tenant Data Center (VMDC)	<a href="#">Play</a>	<a href="#">PDF</a>
10/19	Nexus 1010 v1.3 - What's New?	<a href="#">Play</a>	<a href="#">PDF</a>
10/26	Virtualized Workload Mobility - Latest Design Guidance	<a href="#">Play</a>	<a href="#">PDF</a>
11/02	UCS and Nexus 1000V - Best Practices	<a href="#">Play</a>	<a href="#">PDF</a>
11/09	Virtual Security Gateway (VSG) v1.2 - what's new? v1.3 - what's coming?	<a href="#">Play</a>	<a href="#">PDF</a>

Webinar Link: [www.cisco.com/go/1000vcommunity](http://www.cisco.com/go/1000vcommunity)

# Public Webcasts – Spring 2011



For Your Reference

Date	Business Track Topics	Webinar	Preso	Q&A
3/22	Nexus 1000V/1010 Overview and Update	<a href="#">Play</a>	<a href="#">PDF</a>	<a href="#">PDF</a>
4/05	Virtual Network Services: Virtual Service Datapath (vPath), Network Analysis Module (NAM), Virtual Application Acceleration (vWAAS)	<a href="#">Play</a>	<a href="#">PDF</a>	<a href="#">PDF</a>
4/19	Virtual Security Gateway (VSG) Overview  (Installation Videos: <a href="#">Link</a> )	<a href="#">Play</a>	<a href="#">PDF</a>	<a href="#">PDF</a>
5/03	Journey to the Cloud w/ N1KV: vCloud Director & Long Distance vMotion	<a href="#">Play</a>	<a href="#">PDF</a>	<a href="#">PDF</a>
5/17	Secure Virtual Desktop with Nexus 1000V & VSG	<a href="#">Play</a>	<a href="#">PDF</a>	<a href="#">PDF</a>

Date	Technical Track Topics	Webinar	Preso	Q&A
3/29	Nexus 1000V v1.4 Features & Install Overview  (Installation Screencasts <a href="#">Link</a> )	<a href="#">Play</a>	<a href="#">PDF</a>	<a href="#">PDF</a>
4/12	Nexus 1010 Overview & Best Practices	<a href="#">Play</a>	<a href="#">PDF</a>	<a href="#">PDF</a>
4/26	Virtual Security Gateway (VSG) Technical Overview	<a href="#">Play</a>	<a href="#">PDF</a>	<a href="#">PDF</a>
5/10	Nexus 1000V Key Features Overview	<a href="#">Play</a>	<a href="#">PDF</a>	<a href="#">PDF</a>
5/24	Nexus 1000V Troubleshooting	<a href="#">Play</a>	<a href="#">PDF</a>	<a href="#">PDF</a>

BrightTalk Link: <http://mediazone.brighttalk.com/event/Cisco/0e4ceef65a-4907-intro>

# Resources



- CCO Links
  - 1000V: [www.cisco.com/go/1000v](http://www.cisco.com/go/1000v)
  - 1010: [www.cisco.com/go/1010](http://www.cisco.com/go/1010)
  - VSG: [www.cisco.com/go/vsg](http://www.cisco.com/go/vsg)
  - VNMC: [www.cisco.com/go/vnmc](http://www.cisco.com/go/vnmc)
  - vWAAS: [www.cisco.com/go/waas](http://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](#)





For Your  
Reference

# Additional Links

- N1K Download and 60-day Eval: [www.cisco.com/go/1000vdownload](http://www.cisco.com/go/1000vdownload)
- N1K Product Page: [www.cisco.com/go/1000v](http://www.cisco.com/go/1000v)
- N1K Community: [www.cisco.com/go/1000vcommunity](http://www.cisco.com/go/1000vcommunity)
- N1K Twitter [www.twitter.com/official\\_1000V](http://www.twitter.com/official_1000V)
- N1K Webinars: [www.tinyurl.com/1000v-webinar](http://www.tinyurl.com/1000v-webinar)
- N1K Case Studies: [www.tinyurl.com/n1k-casestudy](http://www.tinyurl.com/n1k-casestudy)
- N1K Whitepapers [www.tinyurl.com/n1k-whitepaper](http://www.tinyurl.com/n1k-whitepaper)
- N1K Deployment Guide: [www.tinyurl.com/N1k-Deploy-Guide](http://www.tinyurl.com/N1k-Deploy-Guide)
- VXI Reference Implementation: [www.tinyurl.com/vxiconfigguide](http://www.tinyurl.com/vxiconfigguide)
- N1K on UCS Best Practices: [www.tinyurl.com/N1k-On-UCS-Deploy-Guide](http://www.tinyurl.com/N1k-On-UCS-Deploy-Guide)

# Cisco Cloud Lab

## Hands On Training & Demos



- 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
- Extended duration lab licenses for 1000V and VSG are available upon request



### Welcome to Cisco CloudLab

Please select one of the available labs, by clicking on its name. Hover over the lab name content.

#### Available labs:

- Cisco Nexus 1000V - Basic Introduction (N1K-000111)
- Cisco Nexus 1000V - Installation (N1K-000211)
- Cisco Nexus 1000V - Upgrade to 1.4 (N1K-000310)
- Cisco Virtual Security Gateway (VSG) - Introduction (VSG-000110)
- Cisco Nexus 7000 - Introduction to NX-OS (N7K-000110)
- Cisco Overlay Transport Virtualization (OTV) (N7K-000210)
- Demo: Cisco Nexus 1000V (Pre-Configured) (N1K-100111)
- Demo: Cisco Virtual Security Gateway (VSG)(Pre-Configured) (VSG-100110)

**Just added: VXLAN Basic Introduction**

Thank you.

