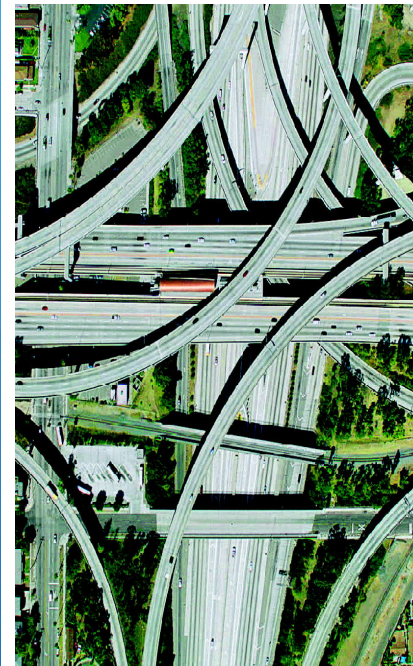


Virtuální firewall v ukázkách a příkladech

T-SEC3 / L2

Tomáš Michaeli – Cisco



Agenda

- VXLAN in Nexus 1000V 2.2
- VXLAN Gateway
- ASA 1000V and VSG demo

New in Nexus 1000V 2.2

"Evolve the virtual network"

In Beta!

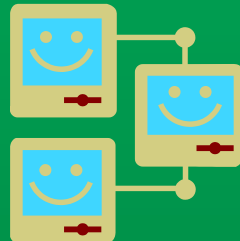
SCALE



Increased Scale

- 128 hosts
- 300 ports per host
- 4000+ ports per VSM

Evolution of VXLAN



VXLAN Unicast Mode

- No Multicast configuration
- No flood and learn
- Mac-address distribution

VXLAN Gateway



VXLAN to VLAN

- Seamless integration with Physical network
- Scale the Datacenter

Evolution of VXLAN

Unicast mode

- Simplifies VXLAN deployment
- Provides better performance
- Reduces network dependency
- Easier troubleshooting

No Flood and Learn

- Improved switching performance
- Reduced latency
- Lesser lookup cycles
- Increased security – Unknown broadcast suppressed

Mac-address Distribution

- Faster response time
- Efficient switching

VXLAN Gateway

What?

- A Layer 2 Gateway that extends the VXLAN Layer 2 domain to physical servers and services deployed on a VLAN

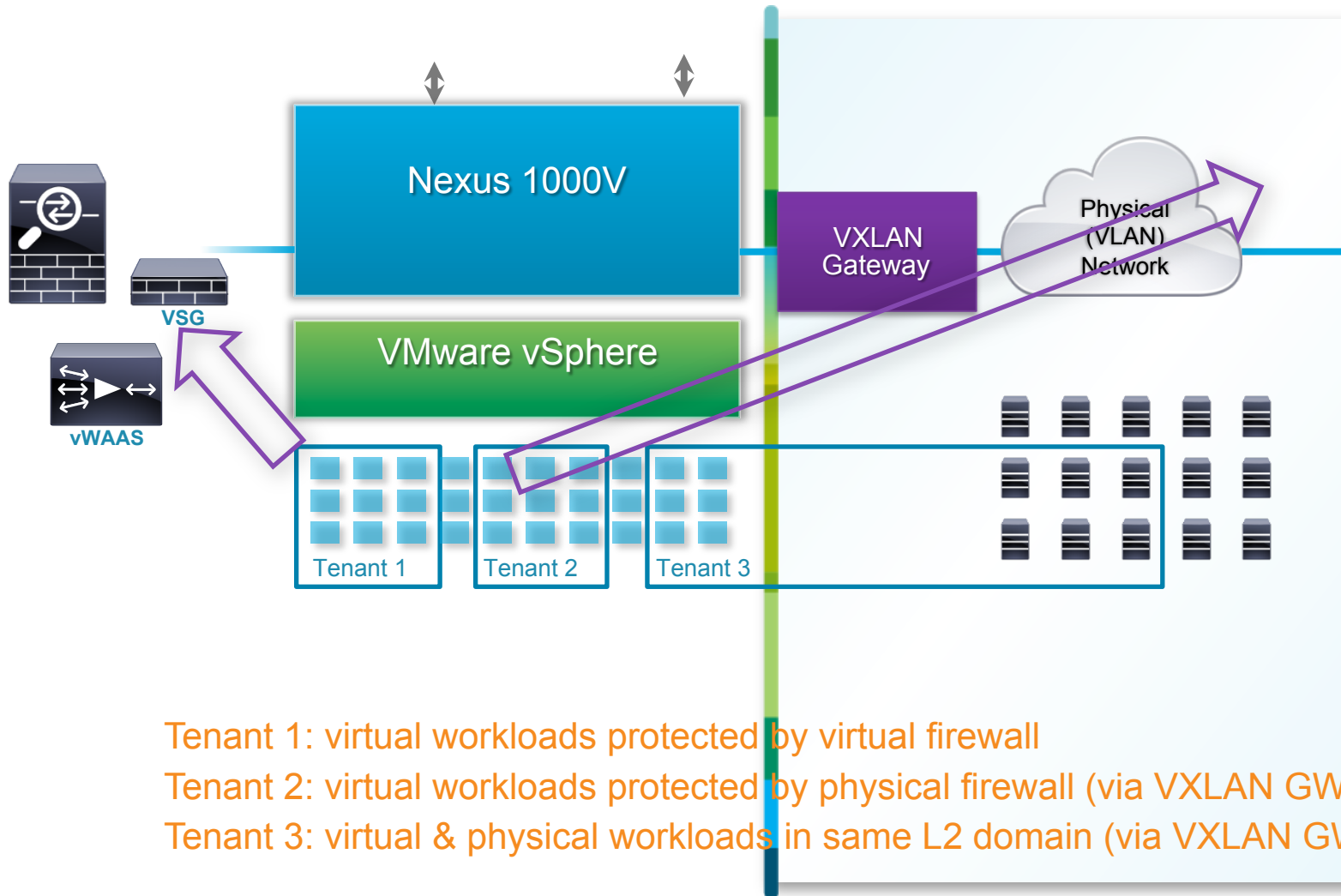
When?

- Created when a Layer 2 adjacency is required between VMs on a VXLAN and physical servers / services on a VLAN

How?

- The VXLAN gateway is managed as a VEM from the Nexus 1000V VSM
- VXLAN Gateway is a feature of the **Advanced Edition, no additional cost**
- Define a mapping between a VXLAN and VLAN on VSM

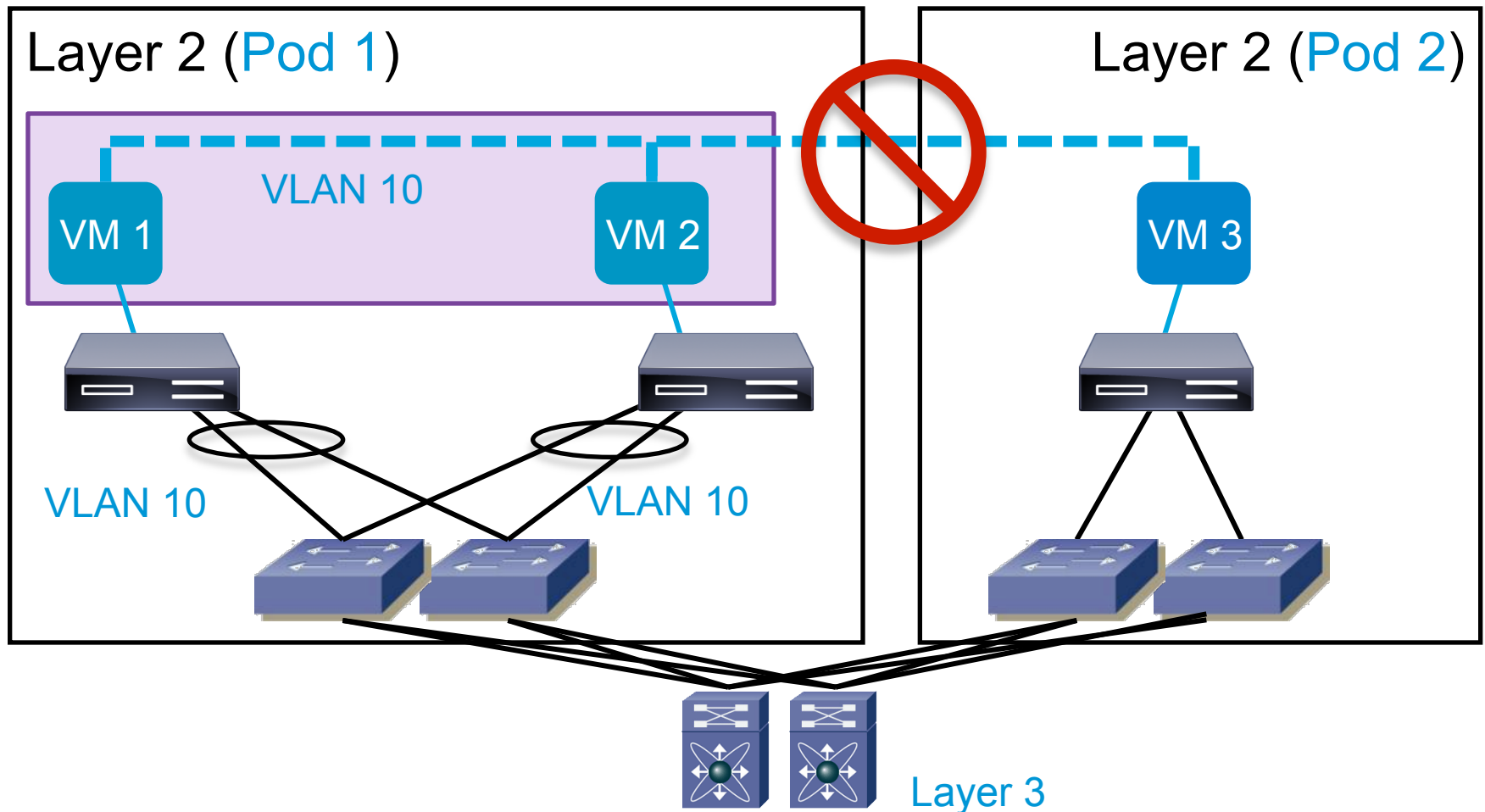
VXLAN Gateway



Deep dive

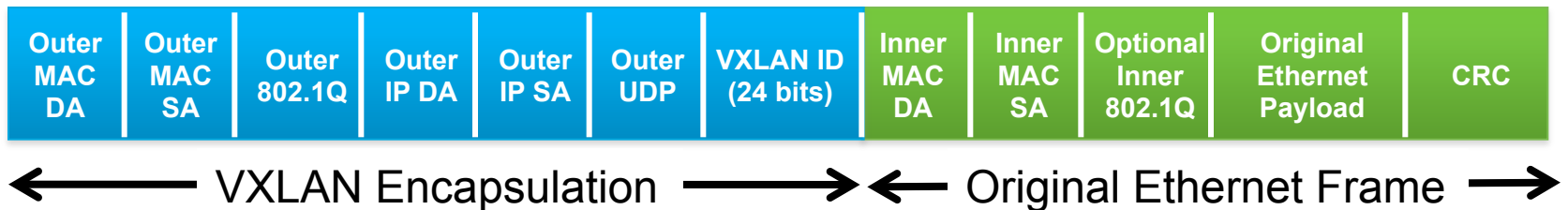


Existing Solution: Reachability of VMs Within VLAN

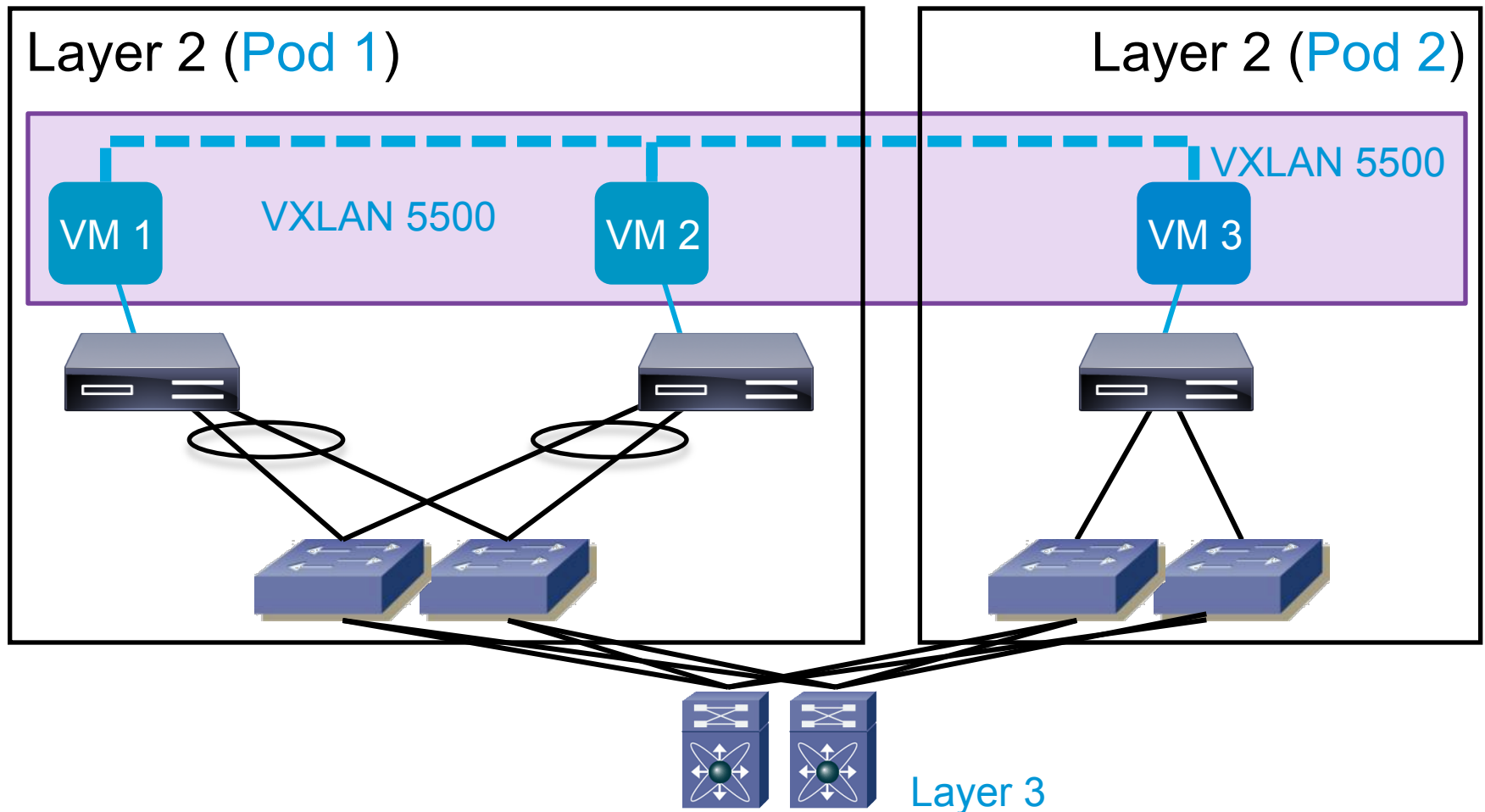


Virtual Extensible Local Area Network (VXLAN)

- Ethernet in IP overlay network
 - Entire L2 frame encapsulated in UDP
 - 50 bytes of overhead
- Include 24 bit VXLAN Identifier
 - 16 M logical networks
 - Mapped into local bridge domains
- VXLAN can cross Layer 3
- Tunnel between VEMs
 - VMs do NOT see VXLAN ID
- IP multicast used for L2 broadcast/multicast, unknown unicast
- Technology submitted to IETF for standardization
 - With VMware, Citrix, Red Hat and Others

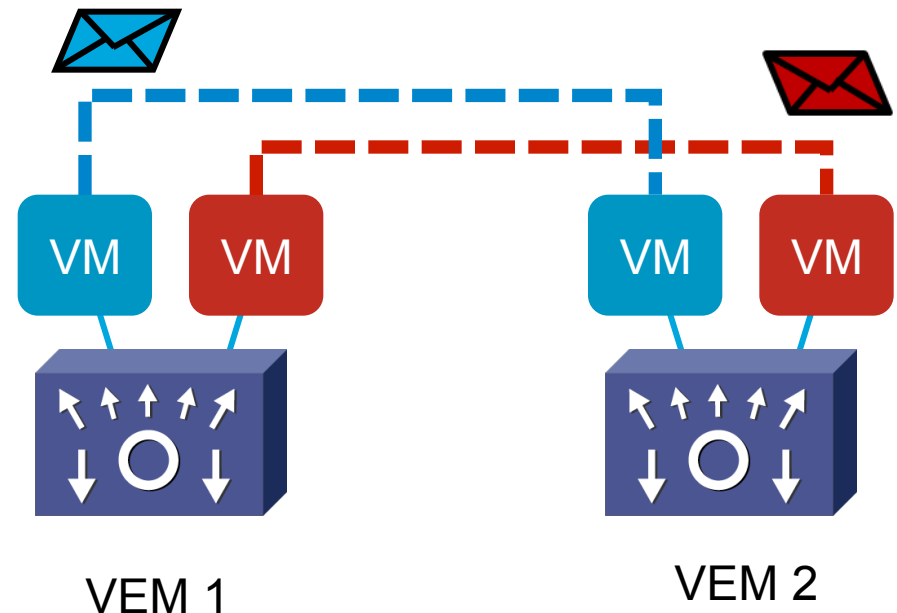


VXLAN: Reachability Across Subnet



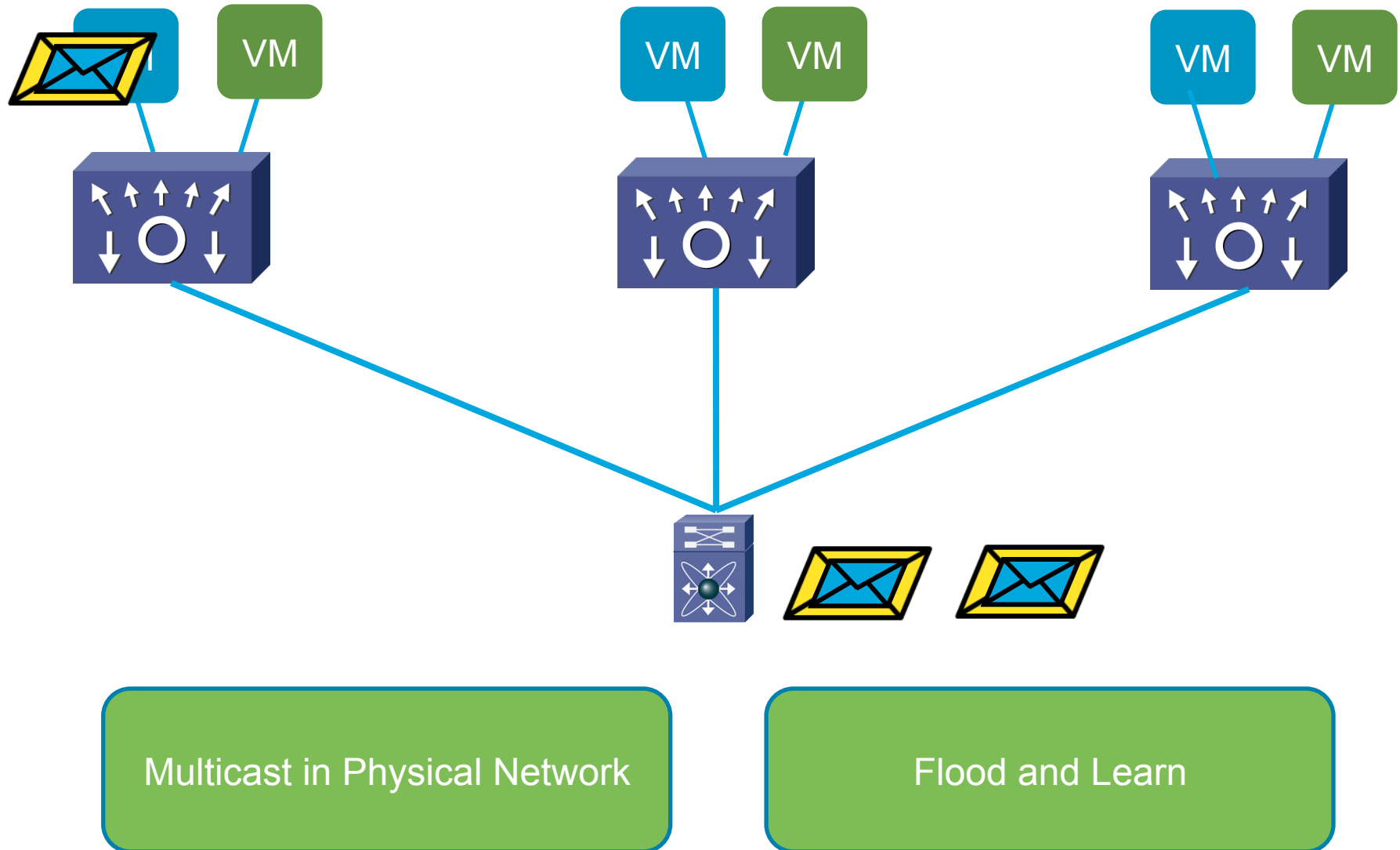
VXLAN Multicast Mode Forwarding

- Forwarding mechanisms similar to Layer 2 bridge: Flood & Learn
 - VEM learns VM's Source (MAC, Host VXLAN IP) tuple
- Broadcast, Multicast, and Unknown Unicast Traffic
 - VM broadcast & unknown unicast traffic are sent as multicast
- Unicast Traffic
 - Unicast packets are encapsulated and sent directly (not via multicast) to destination host VXLAN IP (Destination VEM)



VXLAN Multicast Mode - Challenges

Broadcast, Multicast and Unknown Unicast sent on Multicast group

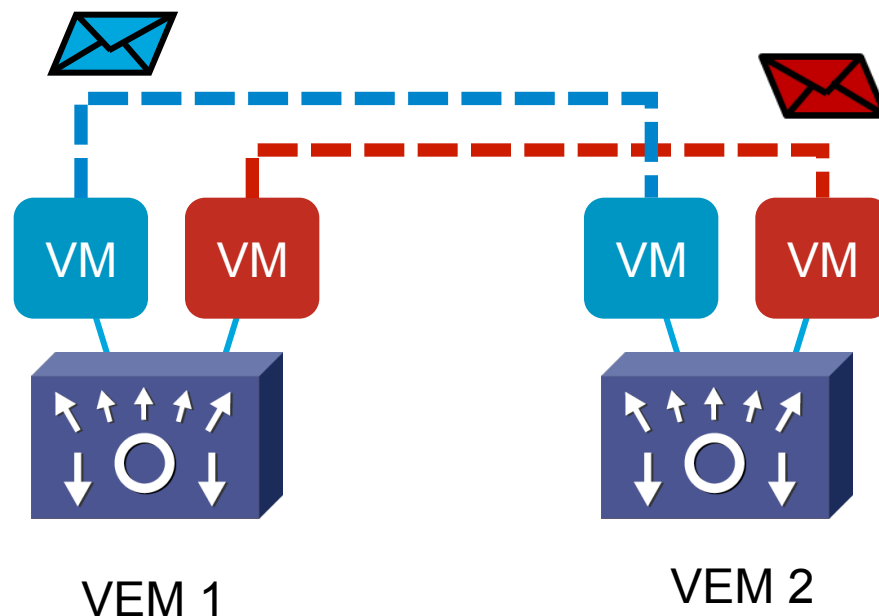


VXLAN Unicast Mode

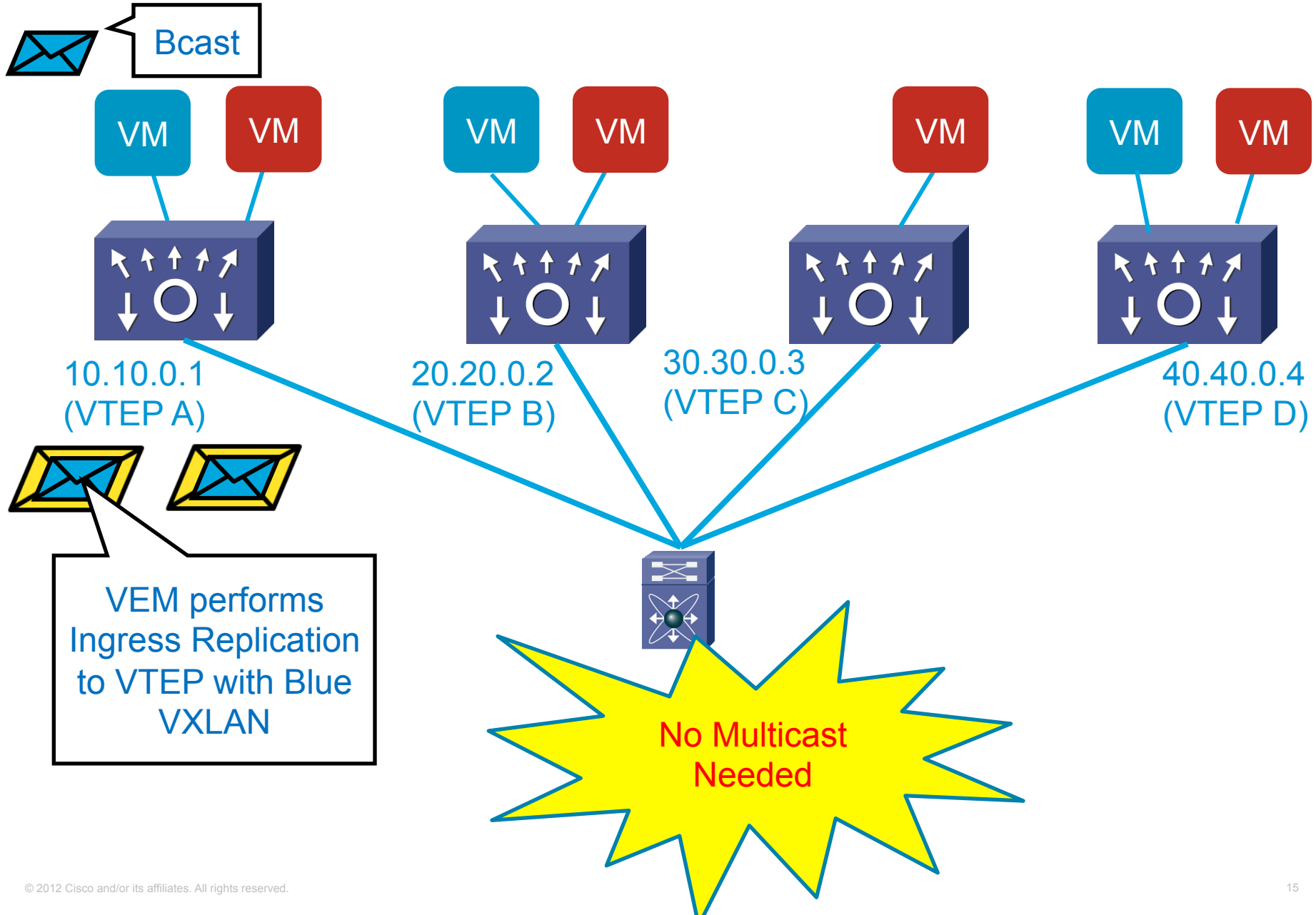


VXLAN Unicast Mode Forwarding

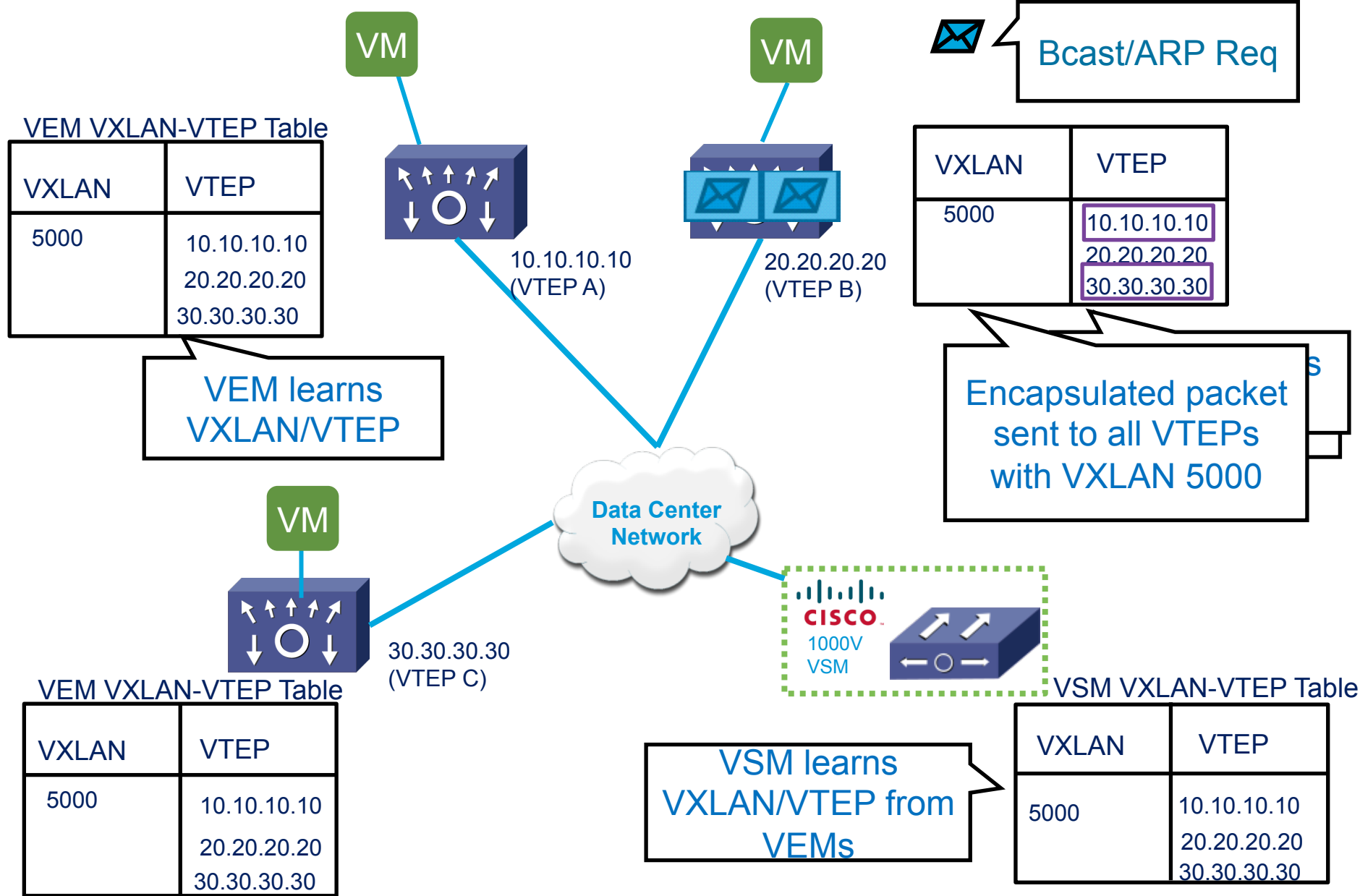
- **Evolutionary approach** - defines a Layer 2 domain without relying on IP Multicast.
- **Multicast Configuration Avoided** — VSM distributes (VXLAN, VTEP IP1, VTEP IP2,...VTEP IP n) list to all VEMs
- **Flooding Avoided** — using MAC Distribution. Each VEM knows all other VM MACs in a VXLAN segment.
- **Broadcast and Multicast**
VM broadcast and Multicast traffic is ingress replicated for each host having VMs in same VXLAN. Packet is encapsulated with destination IP set to host's VXLAN IP.
- **Unicast Traffic**
Unicast packets are encapsulated and sent directly (not via multicast) to destination host VXLAN IP (Destination VEM)



Broadcast and Multicast in VXLAN Unicast Mode



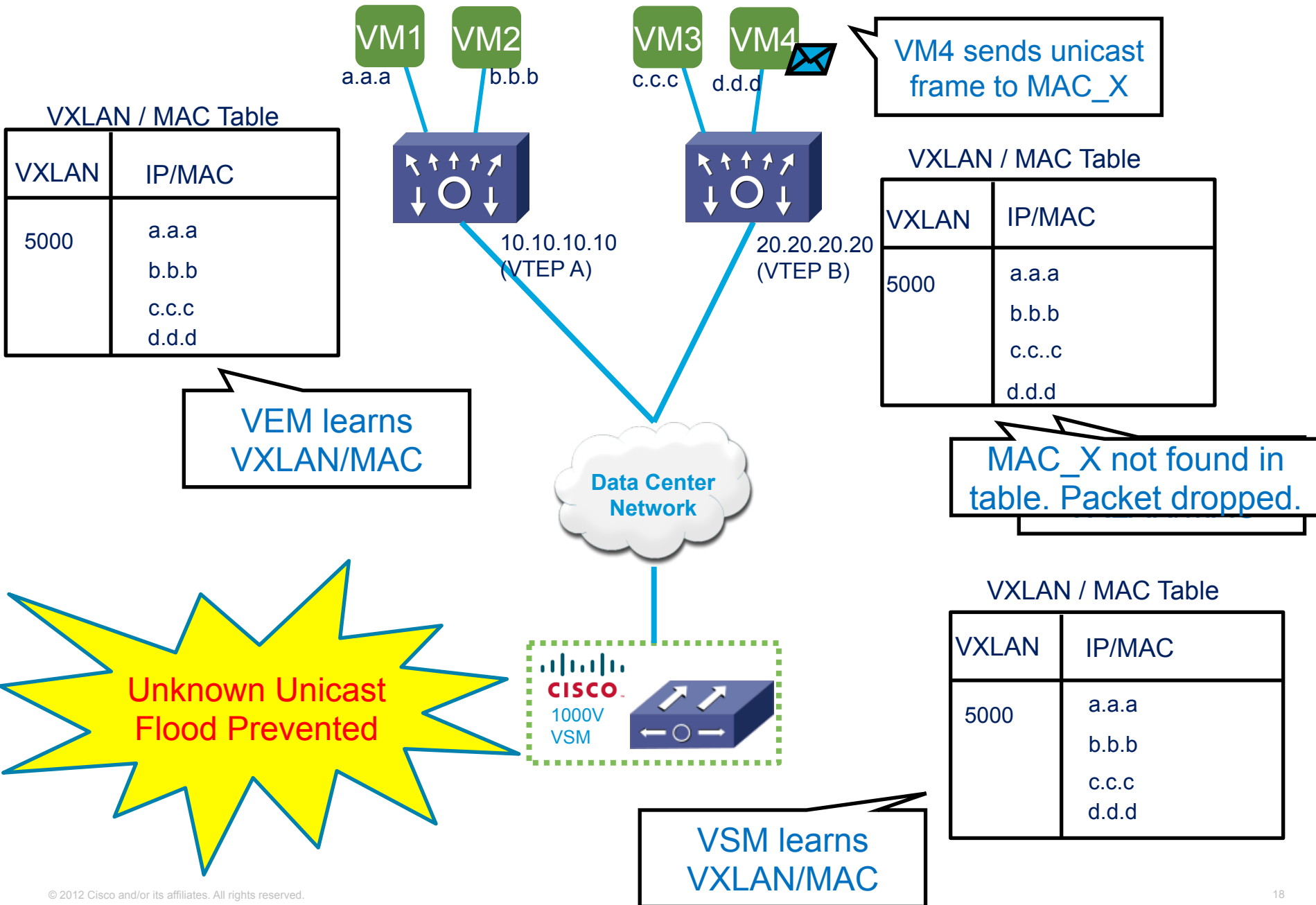
VXLAN Unicast Mode – Unknown/Bcast/ARP Forwarding



MAC Distribution – Forwarding Enhancement

- Enhancement that reduces "unknown unicast" Flooding.
- VEM learns all VM MAC addresses in a VXLAN from VSM.
- When VEM receives a MAC from VM in a VXLAN, if MAC is not found in the MAC table the frame is dropped.
- Security from Malicious VMs sending continuous stream of "Unknown Unicast" traffic.

MAC Distribution – Prevents Unknown Unicast Flood





For Your
Reference

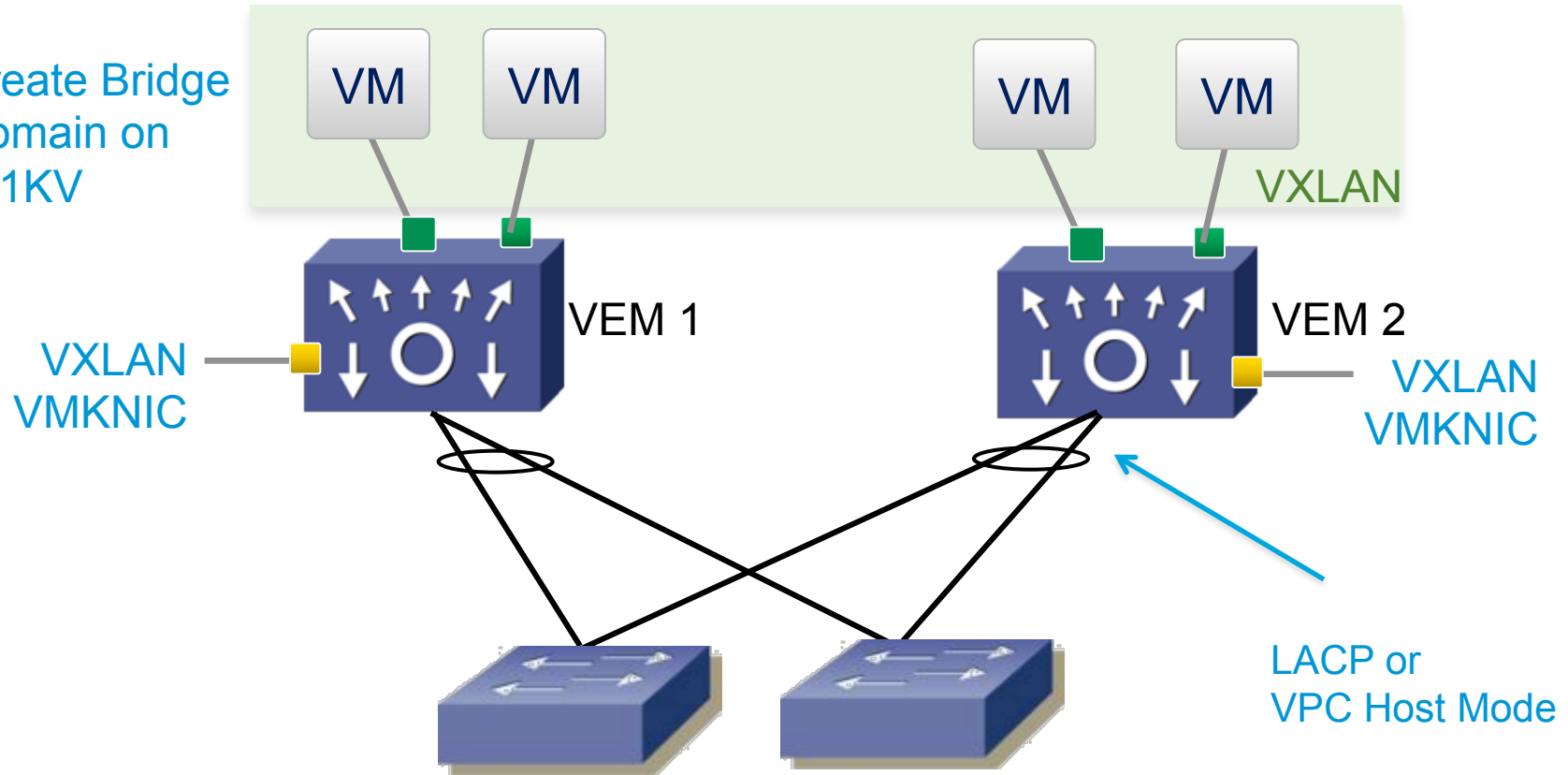
VXLAN Mode Packet	VXLAN Multicast Mode	VXLAN Unicast Mode	MAC Distribution (available when VXLAN is in Unicast mode)
Broadcast / Multicast	Multicast Encap	Replication + Unicast Encap	Replication + Unicast Encap
Unknown Unicast	Multicast Encap	Replication + Unicast Encap	Drop
Known Unicast	Unicast Encap	Unicast Encap	Unicast Encap
ARP	Multicast Encap	Replication + Unicast Encap	Replication + Unicast Encap

Configuring Nexus 1000V for VXLAN Unicast-Only Mode

- 1 Turn on VXLAN feature on N1KV
- 2 Configure global segment mode and mac distribution mode

- 3 Create Bridge Domain on N1KV

- 4



Configuring Nexus 1000V for VXLAN

1 N1KV(config)# feature segmentation

2 N1KV(config)# segment mode unicast-only

3 N1KV(config)# segment distribution mac

4 N1KV(config)# bridge-domain Segment5000
N1KV(config-bd)# segment id 5000
N1KV(config-bd)# segment mode unicast-only
N1KV(config-bd)# segment distribution mac

VXLAN Gateway



VXLAN Gateway

What?

- A Layer 2 Gateway that extends the VXLAN Segment / Layer 2 domain to physical servers and services deployed on a VLAN

When?

- Created when a Layer 2 adjacency is required between VMs on a VXLAN and physical servers / services on a VLAN

How?

- The VXLAN gateway is managed as a VEM from the Nexus 1000V VSM
- VXLAN Gateway is a feature of the **Advanced Edition, no additional cost**
- Defines a mapping between a VXLAN and VLAN on VSM

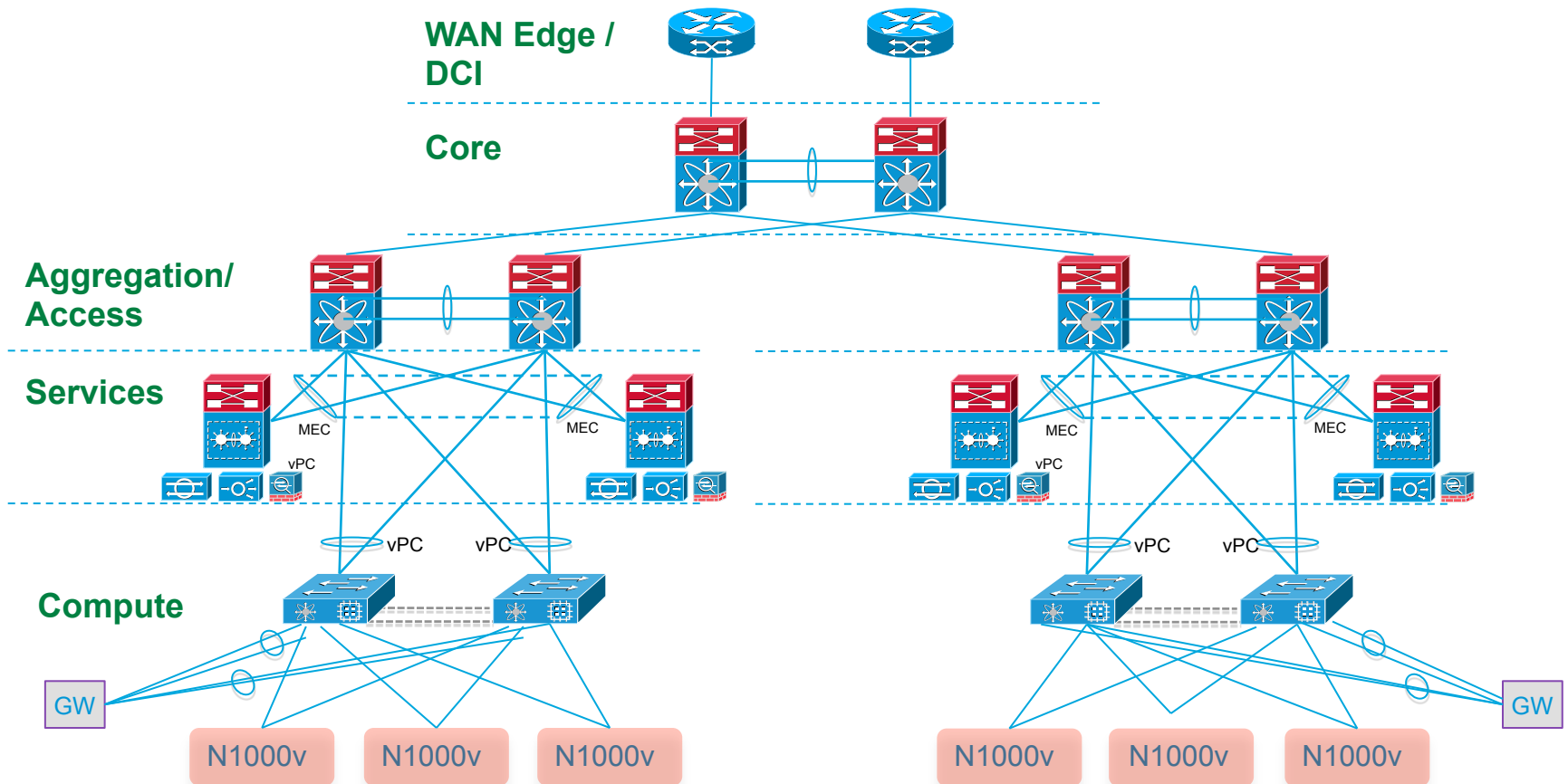
VXLAN Gateway Forwarding

- Defines a mapping between VXLAN and VLAN
- VTEP on the Overlay Network
 - Encapsulates packets received on VLAN with VXLAN encapsulation and forwards to VTEPs
 - Decapsulates packets received on VXLAN network and floods on VLAN
- Forwarding Publish Incapable VTEP

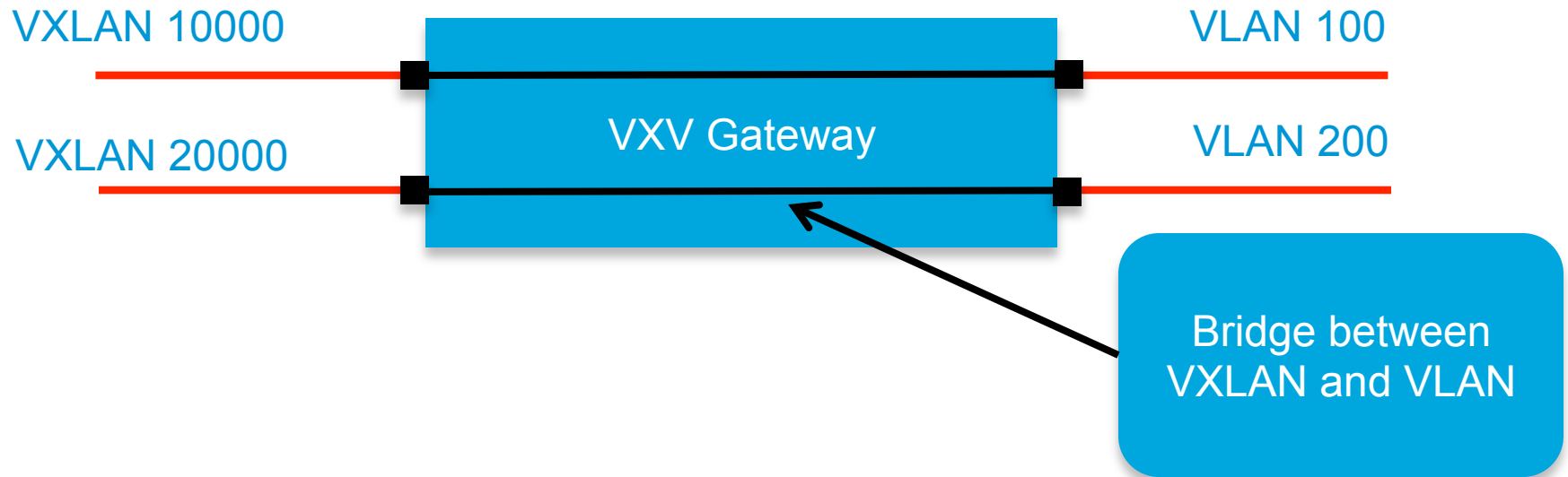
Unlike VTEPs on ESX hosts, Gateway cannot publish MAC addresses of physical hosts to VSM
- Supports both VXLAN Multicast and Unicast Mode

VXLAN Gateway can act as a VTEP in both VXLAN Multicast Mode and Unicast Mode.

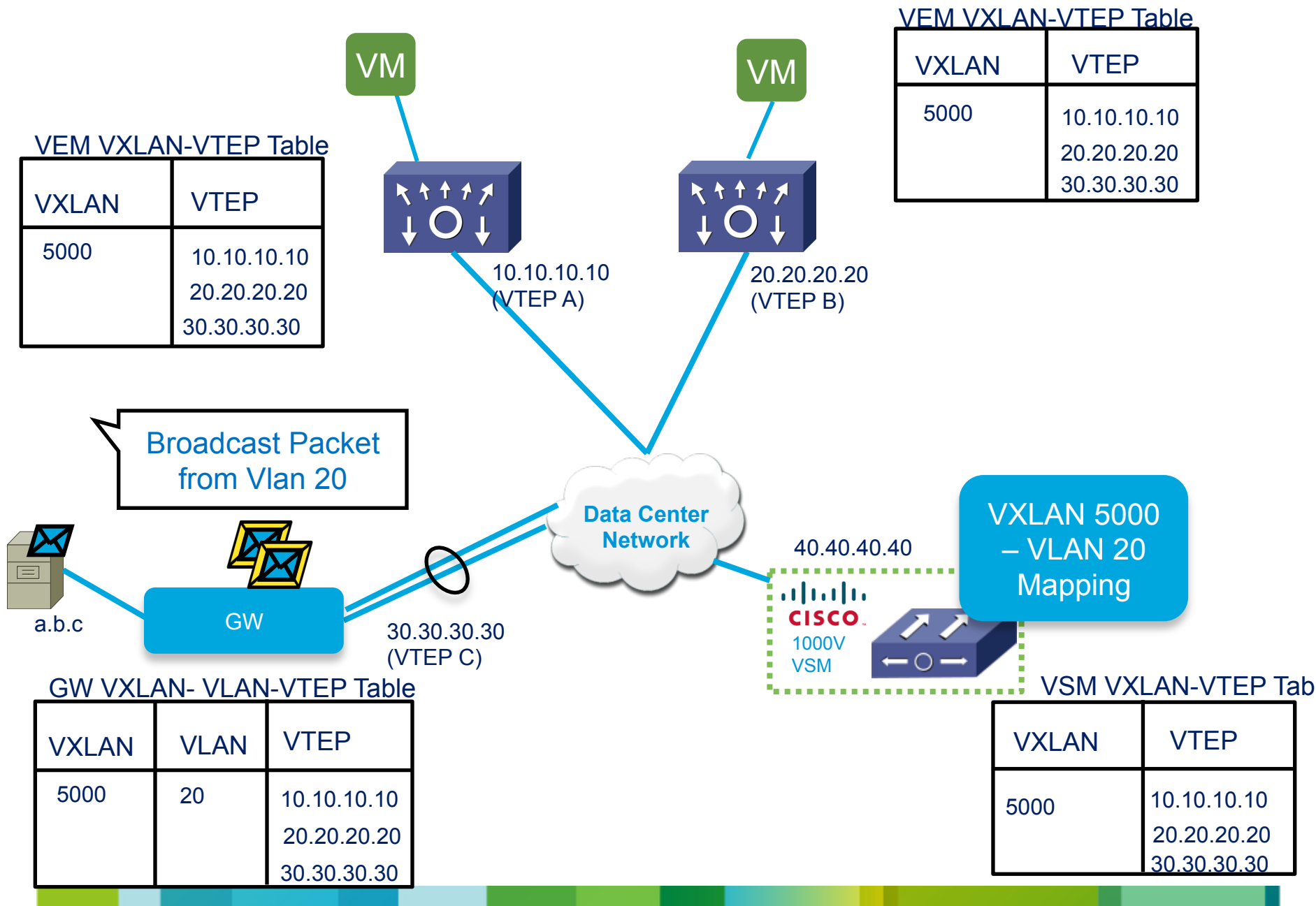
VXLAN Gateway Deployment



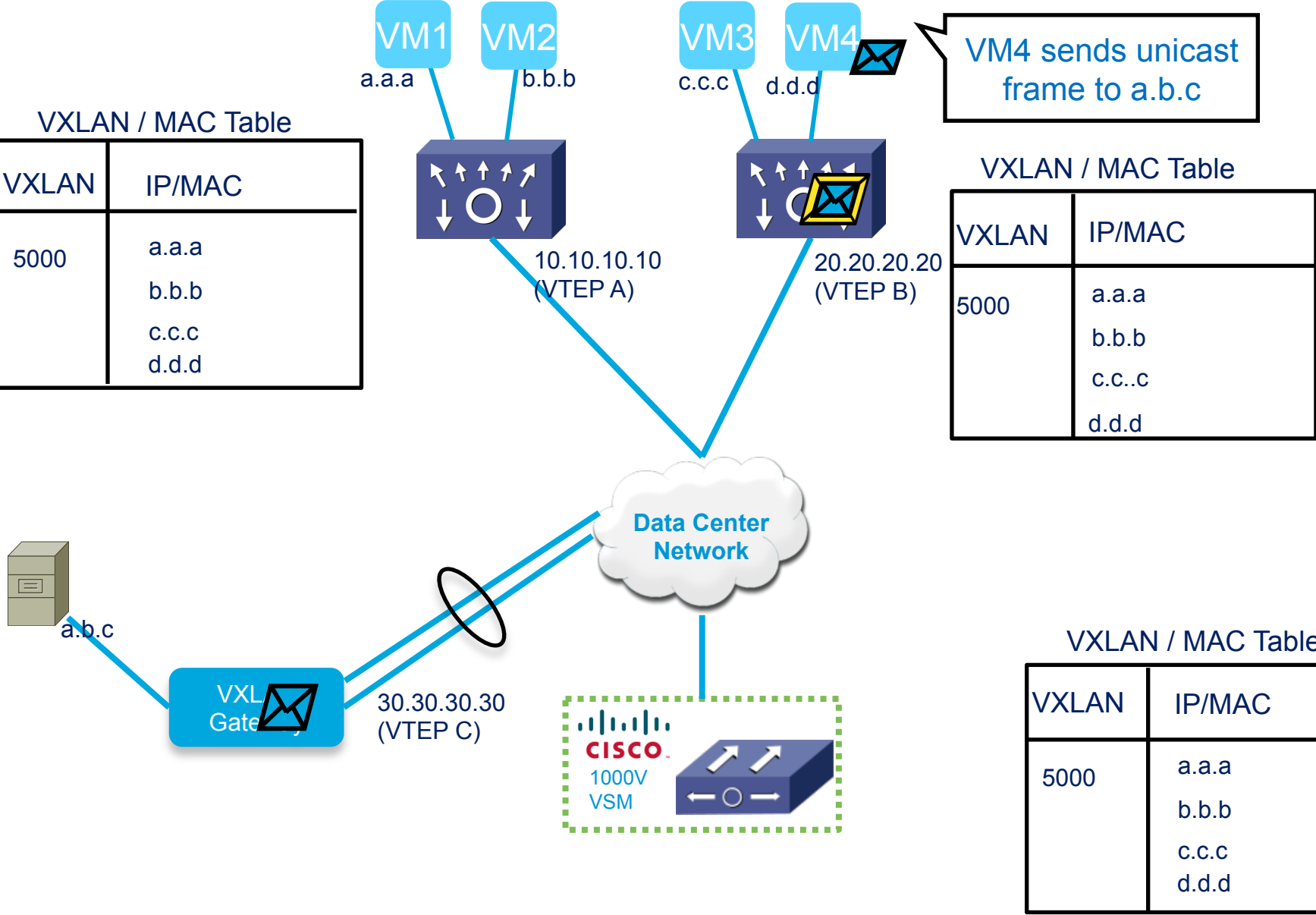
VXLAN Gateway – Logical View



Packet Flow – VLAN to VXLAN



Packet Flow – VXLAN to VLAN



VXLAN Gateway – Install/Config

1 Enable Feature vxlan-gateway

```
linux-vsm(config)#  
linux-vsm(config)# feature vxlan-gateway  
linux-vsm(config)#
```

2 Create Port Profiles on VSM for Gateway VTEP Port

```
linux-vsm(config)#  
linux-vsm(config)# port-profile type vethernet vxgw-veth  
linux-vsm(config-port-prof)# switchport access vlan 435  
linux-vsm(config-port-prof)# capability vxlan  
linux-vsm(config-port-prof)# switchport mode access  
linux-vsm(config-port-prof)# no shutdown  
linux-vsm(config-port-prof)# state enabled  
linux-vsm(config-port-prof)# exit  
linux-vsm(config)#
```

3 Create Port Profile on VSM for Gateway Data Uplink

```
linux-vsm(config)#  
linux-vsm(config)# port-profile type ethernet vxgw-pc  
linux-vsm(config-port-prof)# switchport mode trunk  
linux-vsm(config-port-prof)# switchport trunk allowed vlan 424,435  
linux-vsm(config-port-prof)# channel-group auto mode active  
linux-vsm(config-port-prof)# no shutdown  
linux-vsm(config-port-prof)# state enabled  
linux-vsm(config-port-prof)# exit  
linux-vsm(config)#
```

VXLAN Gateway – Install/Config

4

Configure VXLAN Gateway

```
cy1010(config-vsb-config)#  
cy1010(config-vsb-config)# enable  
Enter vsb image: [tonic.iso]  
Enter domain id[1-4095]: 921  
Management IP version [V4/V6]: [V4]  
Enter Management IP address: 172.23.180.189  
Enter Management subnet mask: 255.255.255.0  
IPv4 address of the default gateway: 172.23.180.1  
Enter HostName: VXLAN-GATEWAY  
Enter the password for 'admin': Sfish123  
VSM L3 Ctrl IPv4 address : 172.23.180.191  
VSM Primary MAC Address: 00:50:56:9c:22:cf  
Enter VSM uplink port-profile name: vxgw-pc  
Enter Encapsulation port-profile name: vxgw-veth  
Note: VSB installation is in progress, please use show virtual-service-blade comma  
llation status.  
cy1010(config-vsb-config)#
```

VXLAN-GY Mgmt IP

VSM Mgmt IP

Port Profiles for VSB

VXLAN Gateway – Install/Config

5

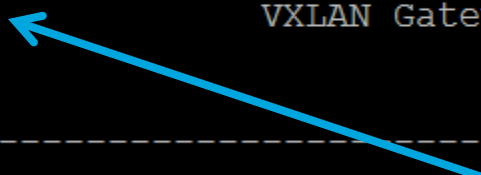
Gateway shows up as a Service Module

```
linux-vsm(config)# sh mod
```

Mod	Ports	Module-Type	Model	Status
1	0	Virtual Supervisor Module	Nexus1000V	active *
6	2080	Virtual Service Module	VXLAN Gateway	ok

Mod	Sw	Hw
1	4.2 (1) SV2 (2.0.189)	0.0
6	4.2 (1) SV2 (2.1)	Linux 2.6.27.10

VSB as a Service Module



6

Create VXLAN-VLAN mappings

```
linux-vsm(config)#
linux-vsm(config)# bridge-domain VXLANforWebServer
linux-vsm(config-bd)# segment id 900000
linux-vsm(config-bd)# segment mode unicast-only
linux-vsm(config-bd)# exit
linux-vsm(config)#
linux-vsm(config)# vlan 3000
linux-vsm(config-vlan)# name VlanForDBServer
linux-vsm(config-vlan)# exit
linux-vsm(config)#
linux-vsm(config)# port-profile type ethernet VXLANGatewayProfile
linux-vsm(config-port-prof)# service_instance 1
linux-vsm(config-port-prof-srv)# encapsulation dot1q 3000 bridge-domain VXLANforWebServer
linux-vsm(config-port-prof-srv)# exit
linux-vsm(config-port-prof)# exit
linux-vsm(config)#
```

VXLAN Gateway HA and Scale

- Two gateways can be configured in an active standby configuration
 - Active/standby have distinct management IP addresses
 - Active/standby share a “virtual” VTEP address
 - Active/standby synchronize configuration, MAC table and VTEP table.
 - Heartbeats are exchanged in the management network
-
- Each VSM can support 4 VXLAN Gateway modules

VXLAN Gateway use cases



VXLAN Gateway Use Cases

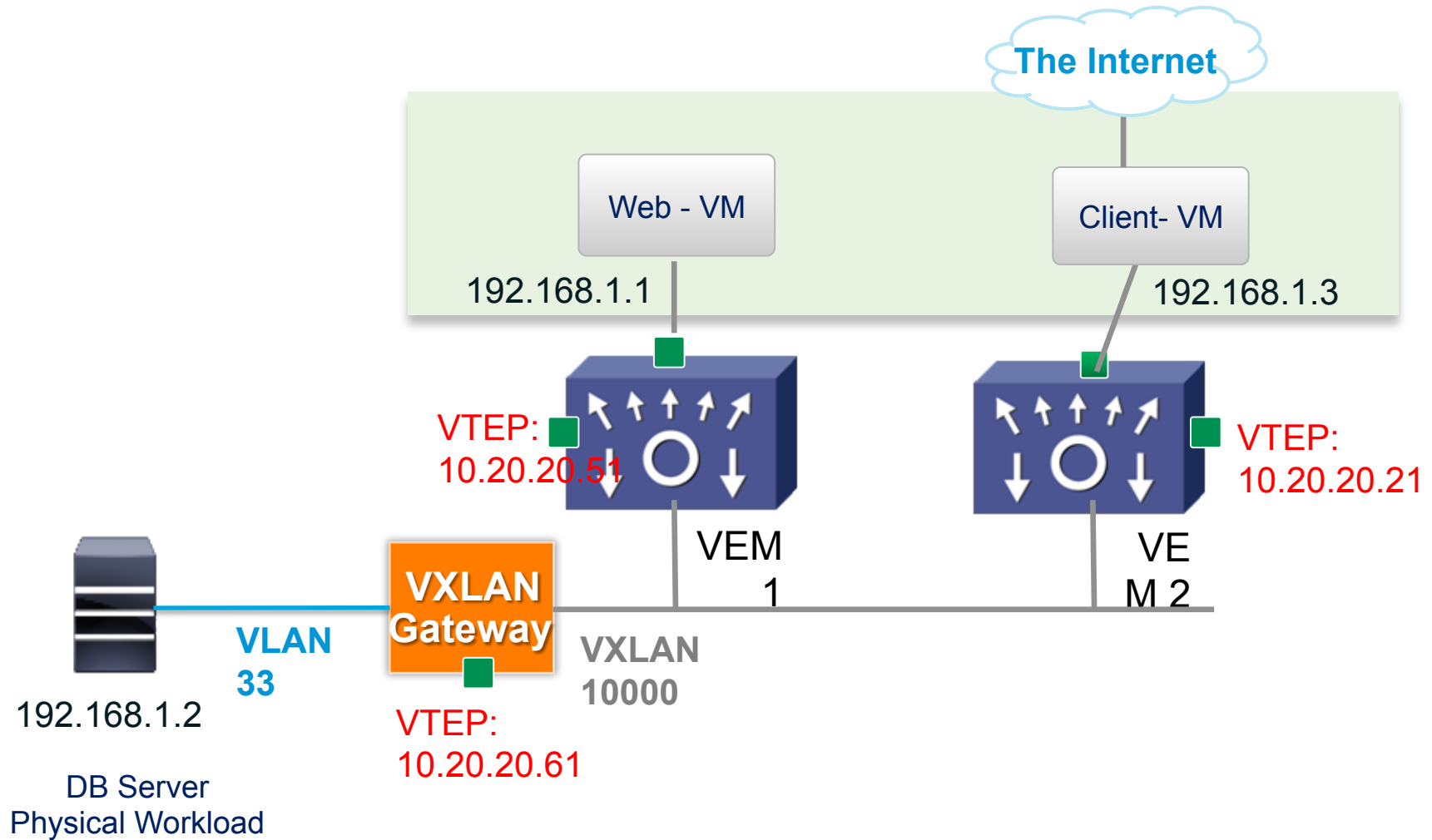
1

Virtualized WebServer VM communicating to Bare Metal DB Server

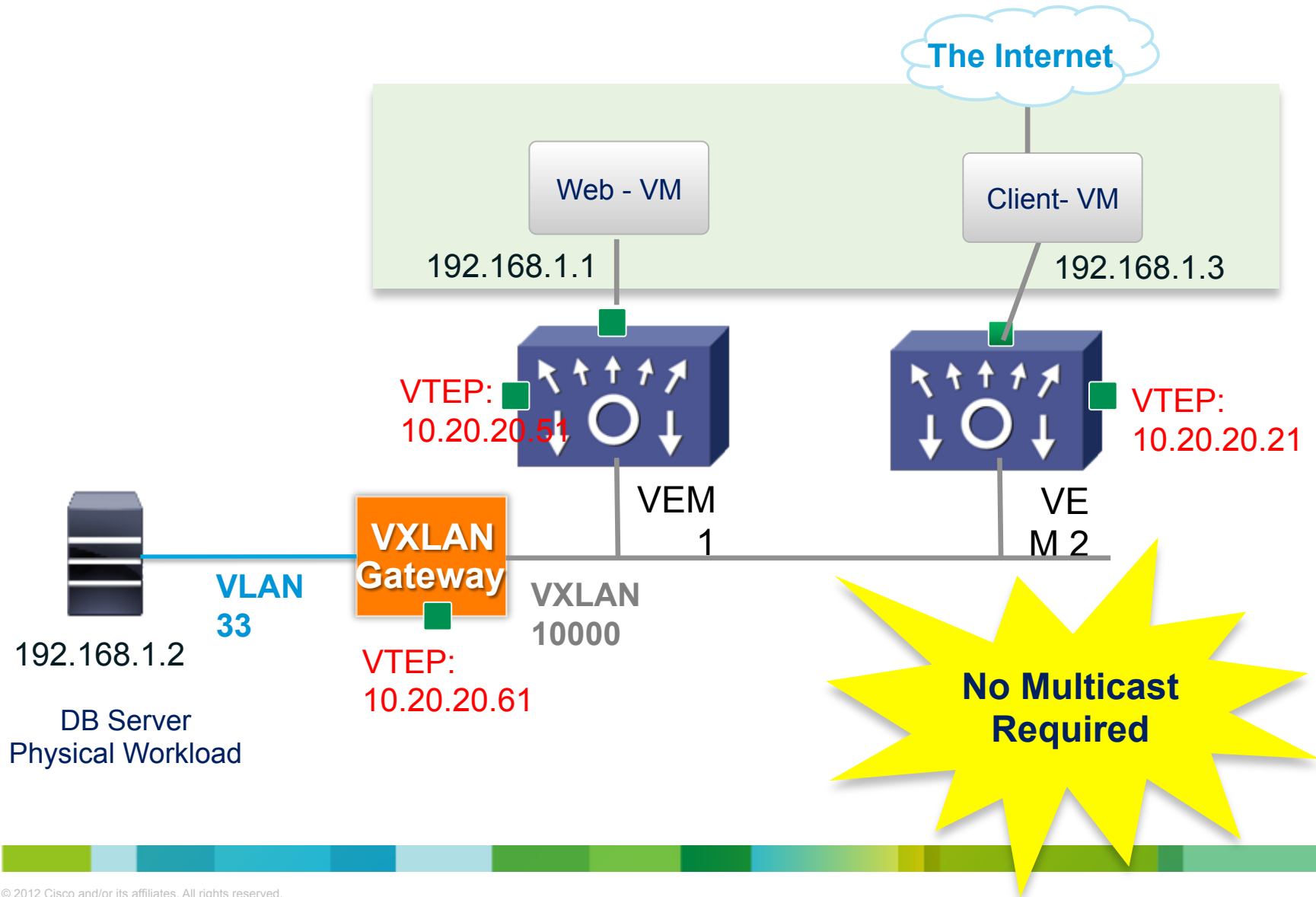
2

Data Center Services such as Firewall, WAN Accelerator deployed as Physical Boxes or Service Modules on Aggregation Switch

VXLAN-VLAN Gateway demo topology



VXLAN-VLAN Gateway demo topology

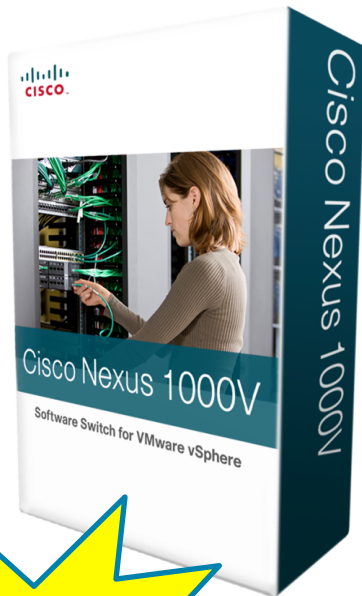


Deep dive summary

- VXLAN Unicast-Only Mode allows network administrators to deploy VXLAN without implementing Multicast in the Physical Network.
- Supports co-existence of both Multicast and Unicast Mode i.e. some VXLANs in multicast mode and some VXLANs in Unicast Mode.
- VXLAN Unicast-Only mode is a single VSM solution. VEMs can be in local or remote datacenter.
- MAC Distribution – helps prevent Unknown Unicast Flood.
- VXLAN Gateway allows the VXLAN layer 2 domain to be extended to physical servers and services.

Summary - New Features in version 2.2

“Evolve the virtual network”



In Beta!

- Improved Scale
 - 128 Hosts
 - 300 ports per host
 - 4000+ ports per VSM
- Evolution of VXLAN
 - **VXLAN Unicast Mode**
 - **Multicast-less mode**
 - **No flood and learn**
 - **Mac-distribution**
- VXLAN Gateway
 - **Available in Advanced Edition**
- Enhanced upgrade process

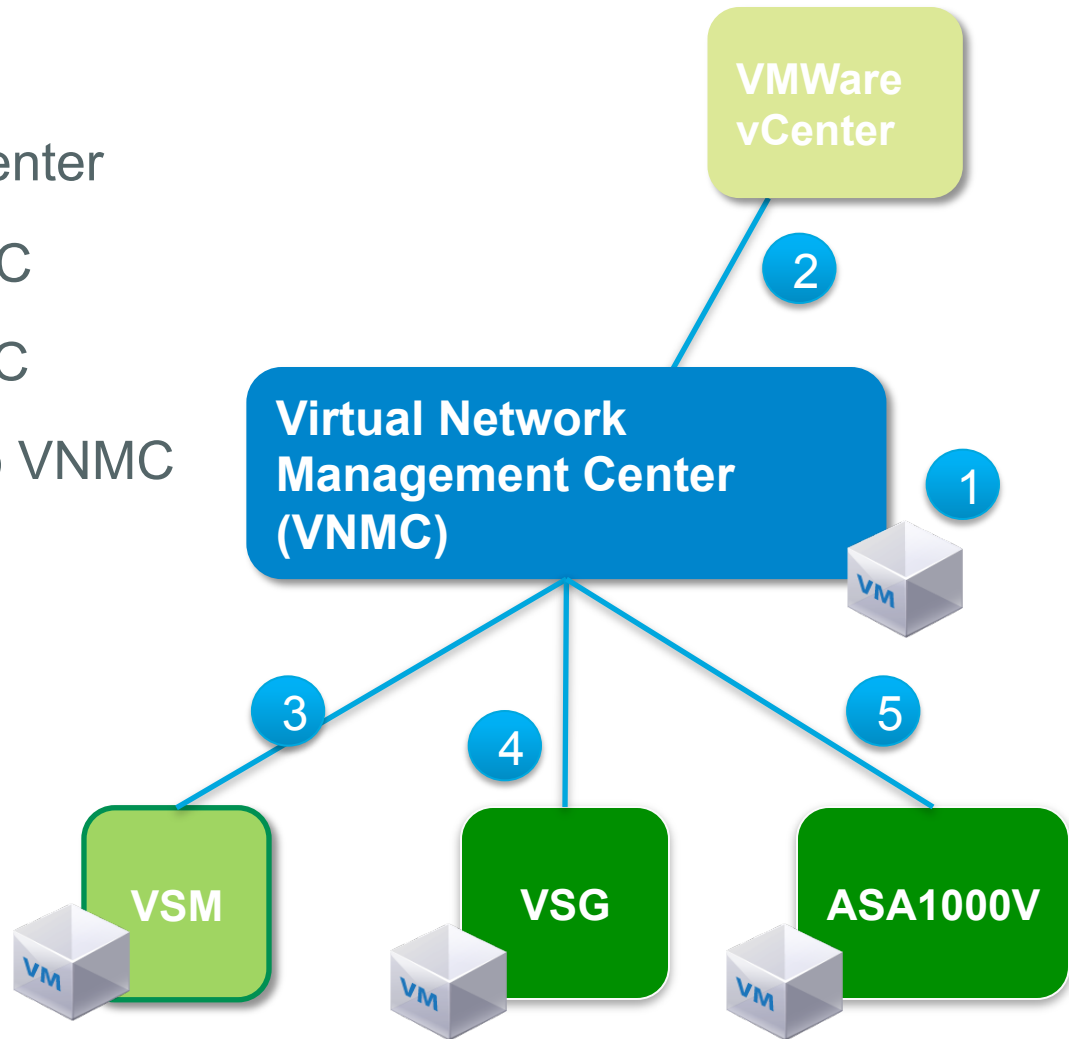
Available soon on CCO (Q2CY13)

VNMC Solution Deployment



Solution Deployment Steps

- 1) Install VNMC
- 2) Connect VNMC to vCenter
- 3) Connect VSM to VNMC
- 4) Connect VSG to VNMC
- 5) Connect ASA1000V to VNMC



Deployment Step 1: VNMC Installation

- Install VNMC as a Virtual Appliance in vCenter using OVA or ISO image
- Power on the VNMC virtual appliance after the OVA is deployed
- Access VNMC WebUI using: “*https://<Fully qualified VNMC hostname or IP Address>*”

Username – “admin”
Password – whatever set during installation

Deploy OVF Template

Ready to Complete
Are these the options you want to use?

[Source](#)
[OVF Template Details](#)
[End User License Agreement](#)
[Name and Location](#)
[Deployment Configuration](#)
[Datastore](#)
[Disk Format](#)
[Network Mapping](#)
[Properties](#)
Ready to Complete

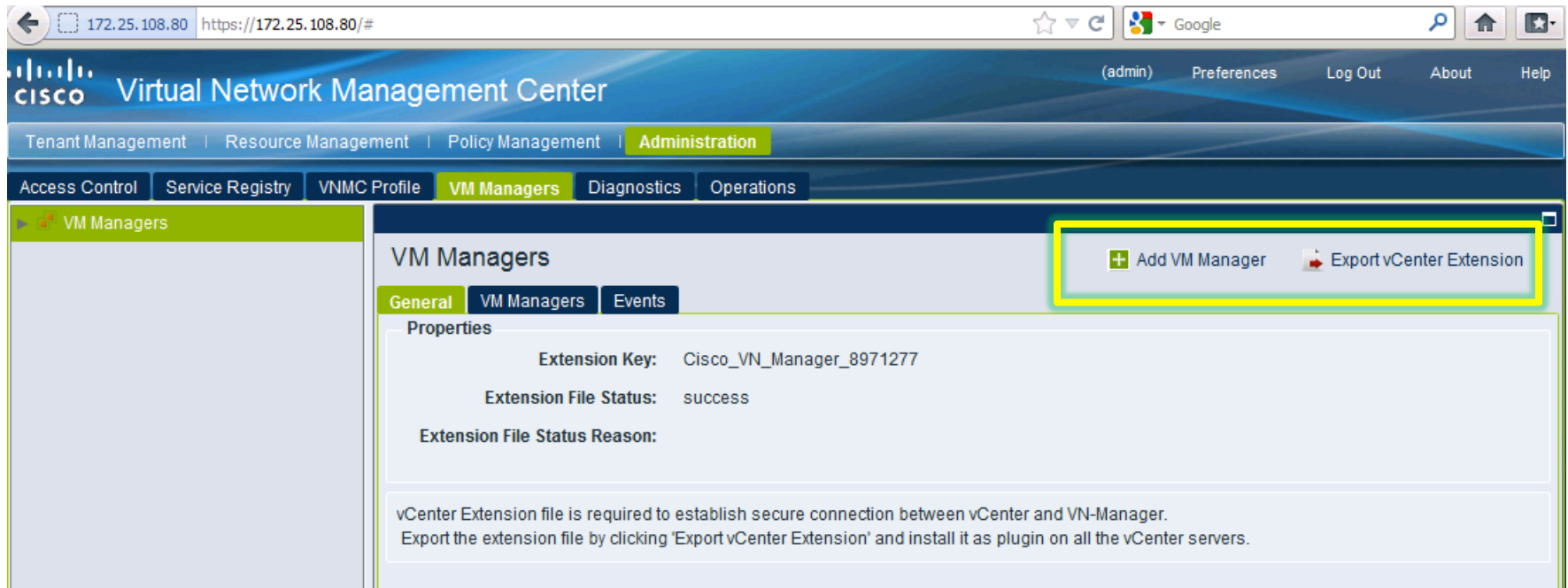
When you click Finish, the deployment task will be started.

Deployment settings:

OVF file:	C:\Downloads\vnmc-beta2-vsm62\vnmc.2.0.2.18.debug.ova
Download size:	999.4 MB
Size on disk:	4.1 GB
Name:	tme-vnmc20-trn-vnmc
Folder:	OverDrive
Deployment Configuration:	VNMC Installer
Host/Cluster:	Workstations
Resource Pool:	vnmc-training
Datastore:	OD-DE-3 (Nexsan 6)
Disk Format:	Thick Provisioning
Network Mapping:	"VM Network" to "cloudTME_203"
IP Allocation:	Fixed, IPv4
Property:	IPv4 = 172.25.108.80
Property:	Netmask = 255.255.255.224
Property:	IPv4Gateway = 172.25.108.65
Property:	Hostname = localhost
Property:	Domainname = localdomain
Property:	DNS = 0.0.0.0
Property:	Password = poPPee123
Property:	Secret = poPPee123
Property:	RestoreProto = scp
Property:	RestoreIP = 0.0.0.0
Property:	RestoreFile = ignore
Property:	RestoreUser = ignore
Property:	RestorePassword = ignore

Deployment Step 2: Connect VNMC to vCenter

Export vCenter Extension file



- Connection to the vCenter is certificate based (no password)
- Click on “Export vCenter Extension” and save extension to a file
- Using vCenter “Plug-ins → Manage Plug-ins” wizard create a new plug-in using the extension file
- Click on “Add VM Manager” to add a vCenter server to VNMC

Deployment Step 3: Connect VSM to VNMC

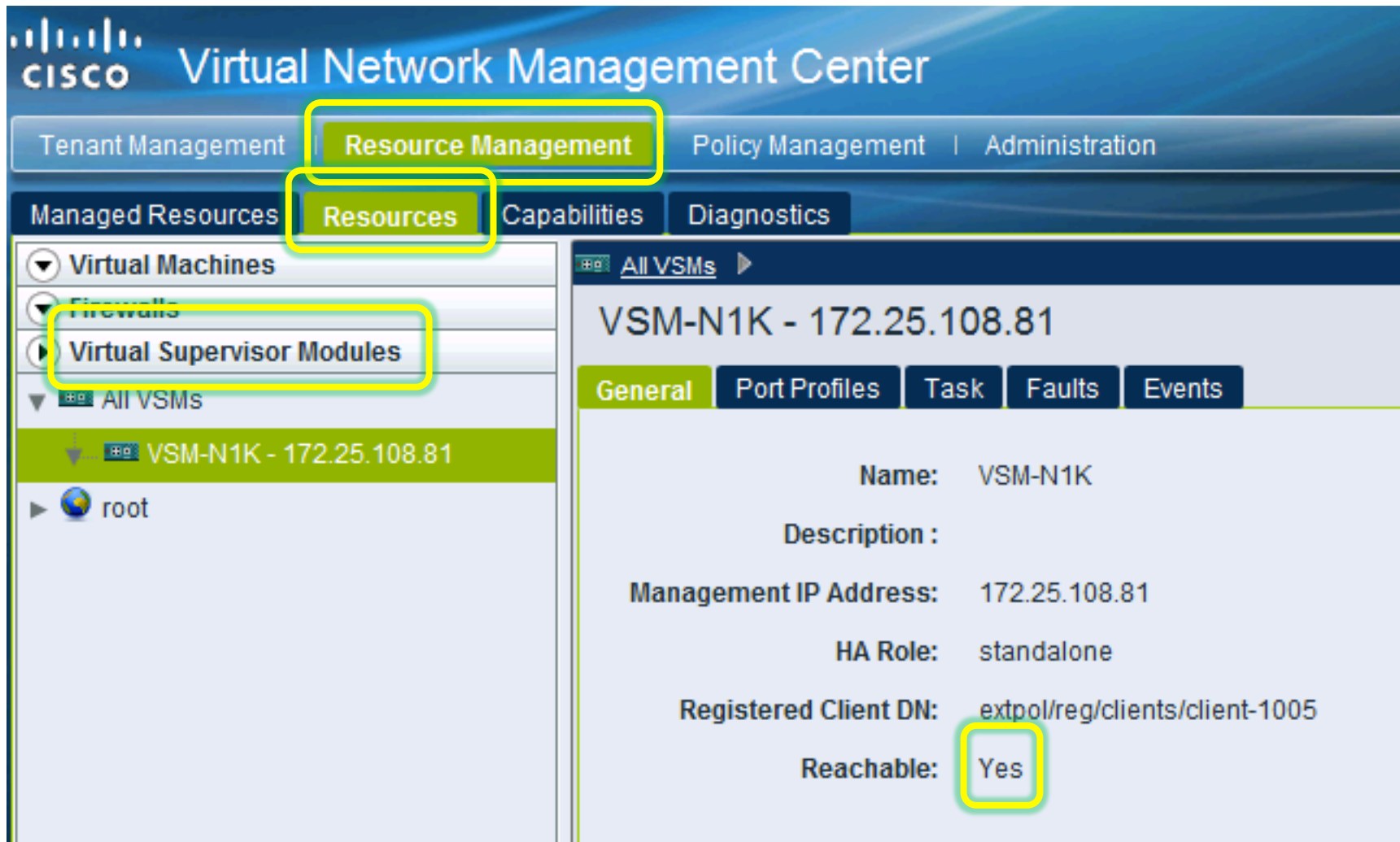
Setup Policy Agent in VSM

- Login to Nexus 1000V Virtual Supervisor Module (VSM)
- Configure vnm-policy-agent using VNMC IP address, shared secret and policy agent image

```
VSM-N1K(config)#  
VSM-N1K(config)#  
VSM-N1K(config)# vnm-policy-agent  
VSM-N1K(config-vnm-policy-agent)# registration-ip 172.25.108.80  
VSM-N1K(config-vnm-policy-agent)# shared-secret poPPee123  
VSM-N1K(config-vnm-policy-agent)# policy-agent-image vnmc-vsmpa.2.0.0.19.bin  
VSM-N1K(config-vnm-policy-agent)#  
VSM-N1K(config-vnm-policy-agent)#  
VSM-N1K(config-vnm-policy-agent)# show vnm-pa status  
VNM Policy-Agent status update in progress. Please retry later.  
VSM-N1K(config-vnm-policy-agent)# show vnm-pa status  
VNM Policy-Agent status is - Installed Successfully. Version 2.0(0.19)-vsm  
  
VSM-N1K(config-vnm-policy-agent)#
```

Deployment Step 3: Connect VSM to VNMC

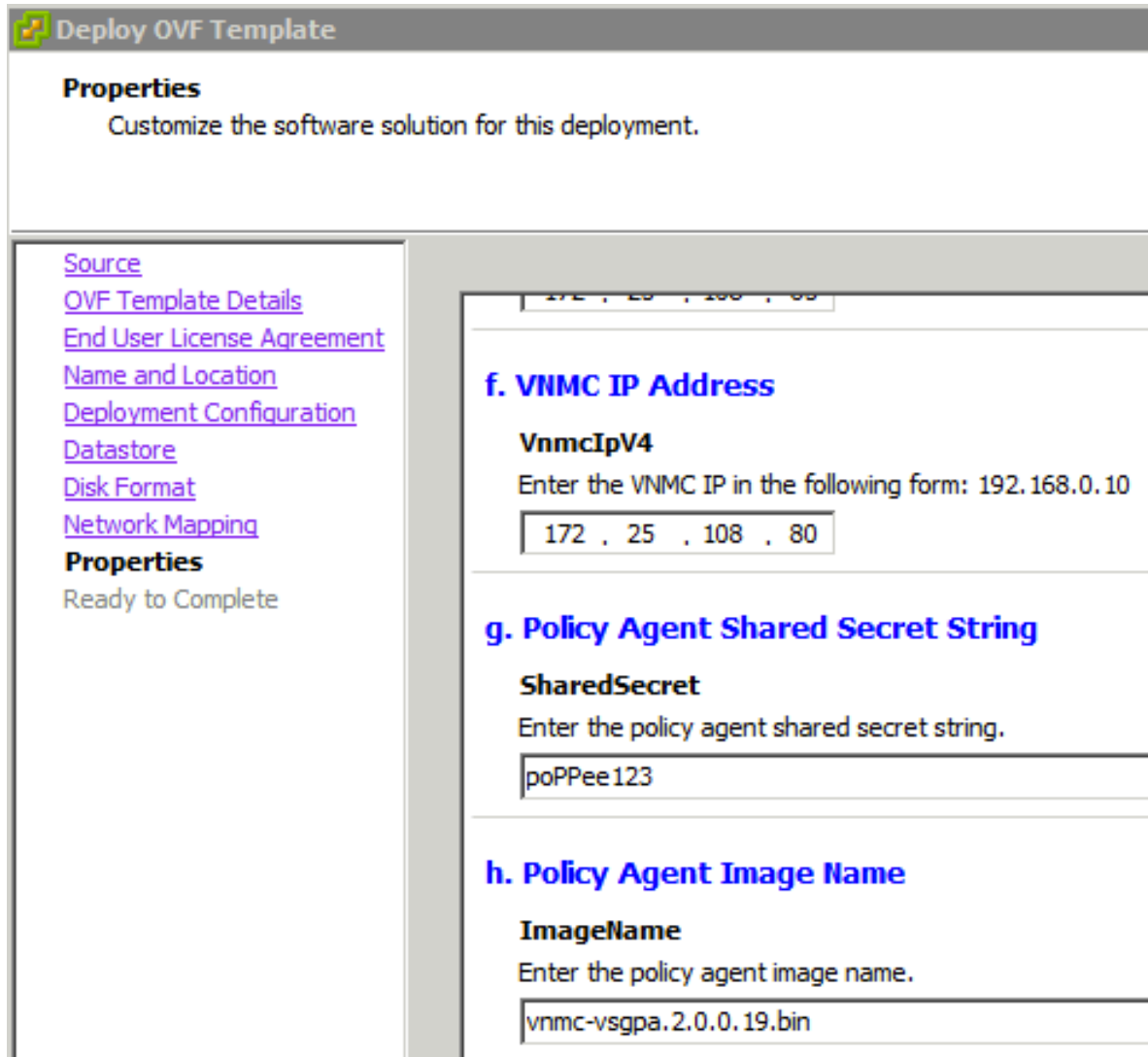
Verify VSM is connected and reachable from VNMC



The screenshot displays the Cisco Virtual Network Management Center (VNMC) interface. The top navigation bar includes 'Tenant Management', 'Resource Management' (highlighted with a yellow box), 'Policy Management', and 'Administration'. Below this, the 'Managed Resources' section contains 'Resources' (highlighted with a yellow box), 'Capabilities', and 'Diagnostics'. The left sidebar shows a tree view with 'Virtual Machines', 'Firewalls', and 'Virtual Supervisor Modules' (highlighted with a yellow box). Under 'Virtual Supervisor Modules', 'All VSMs' is expanded, showing 'VSM-N1K - 172.25.108.81' (highlighted with a yellow box) and a 'root' node. The main panel displays the configuration for 'VSM-N1K - 172.25.108.81'. The 'General' tab is selected, showing the following details:

- Name: VSM-N1K
- Description :
- Management IP Address: 172.25.108.81
- HA Role: standalone
- Registered Client DN: extpol/reg/clients/client-1005
- Reachable: Yes (highlighted with a yellow box)

Deployment Step 4: Connect VSG to VNMC



Deploy OVF Template

Properties
Customize the software solution for this deployment.

[Source](#)
[OVF Template Details](#)
[End User License Agreement](#)
[Name and Location](#)
[Deployment Configuration](#)
[Datastore](#)
[Disk Format](#)
[Network Mapping](#)
Properties
Ready to Complete

f. VNMC IP Address

VnmcIpV4
Enter the VNMC IP in the following form: 192.168.0.10

g. Policy Agent Shared Secret String

SharedSecret
Enter the policy agent shared secret string.

h. Policy Agent Image Name

ImageName
Enter the policy agent image name.

- As part of VSG OVA deployment specify the VNMC IP address, shared secret and policy agent information

Deployment Step 4: Connect VSG to VNMC (contd.)

- Once the VSG is powered ON, it will register with VNMC

The screenshot shows the Cisco Virtual Network Management Center (VNMC) web interface. The top navigation bar includes 'Tenant Management', 'Resource Management' (highlighted), 'Policy Management', and 'Administration'. Below this, the 'Managed Resources' section is active, showing 'Resources', 'Capabilities', and 'Diagnostics'. On the left sidebar, 'Virtual Machines' is expanded, and 'All VSGs' is highlighted. A yellow box highlights the entry 'VSG - 172.25.108.82'. The main content area displays a table titled 'All VSGs' with the following data:

Name	Management IP	HA Role	Association	Operational State	Reachable
VSG	172.25.108.82	standalone	none	unassociated	Yes

Yellow boxes highlight the 'Operational State' and 'Reachable' columns in the table.

VSG#

```
VSG# show runn | beg vnm-pol
vnm-policy-agent
  registration-ip 172.25.108.80
  shared-secret *****
  policy-agent-image bootflash:/vnmc-vsgpa.2.0.0.19.bin
  log-level
logging logfile messages 5 size 4194304
```

VSG# show vnm-pa status

VNM Policy-Agent status is - Installed Successfully. Version 2.0(0.19)-vsg

VSG# █

Deployment Step 5: Connect ASA 1000V to VNMC

- Login to ASA1000V
- Configure VNMC IP address and shared-secret

```
ciscoasa(config)#
ciscoasa(config)# vnmc policy-agent
ciscoasa(config-vnmc-policy-agent)# registration host 172.25.108.80
ciscoasa(config-vnmc-policy-agent)# shared-secret poPPeel23
Password:
sh: -stdin: not found
Password:
sh: -stdin: not found

Trustpoint CA certificate accepted.
route {
    from: 0.0.0.0/0 to: 0.0.0.0/0 via: 127.0.0.1 port = 1080
    proxyprotocol: socks_v5
}
ciscoasa(config-vnmc-policy-agent)#
```

Deployment Step 5: Connect ASA 1000V to VNMC (contd.)

- Verify ASA1000V registered with VNMC

The screenshot displays the Cisco Virtual Network Management Center (VNMC) interface. The top navigation bar includes the Cisco logo, the title "Virtual Network Management Center", and user links: "(admin)", "Preferences", "Log Out", and "About". Below this is a secondary navigation bar with tabs: "Tenant Management", "Resource Management" (highlighted), "Policy Management", and "Administration". A third bar shows "Managed Resources", "Resources" (highlighted), "Capabilities", and "Diagnostics".

The left sidebar contains a tree view with the following items:

- Virtual Machines
- Firewalls
 - All ASA 1000Vs (highlighted)
 - edgefirewall - 172.25.108.83
 - All VSGs

The main content area is titled "All ASA 1000Vs" and displays a table of records. The table has the following columns: Name, Management IP, HA Role, Association, Operational State, and Reachable. The "Operational State" and "Reachable" columns are highlighted with yellow boxes. The table shows one record for "edgefirewall" with a management IP of "172.25.108.83", an HA role of "standalone", and an association of "none".

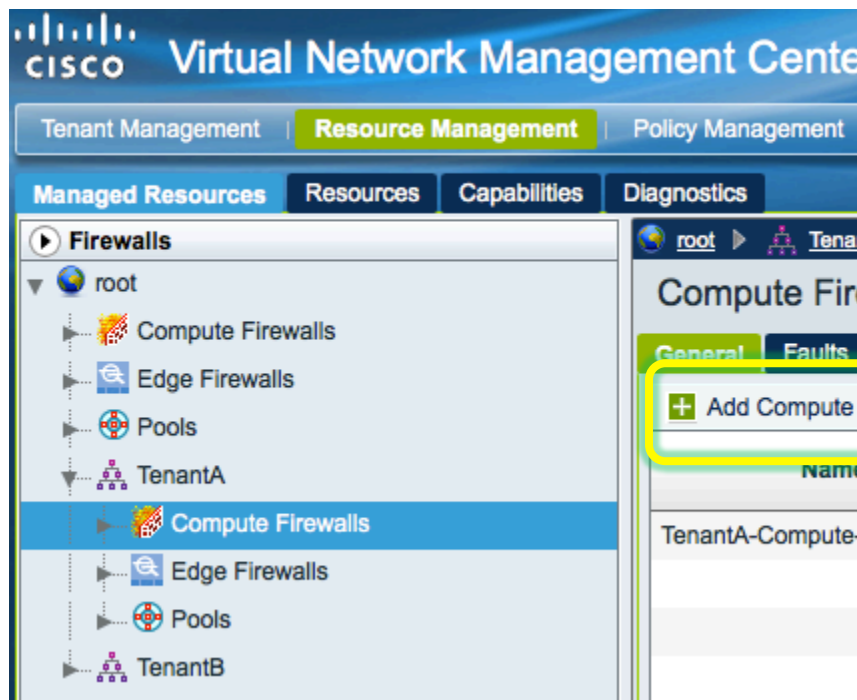
Name	Management IP	HA Role	Association	Operational State	Reachable
edgefirewall	172.25.108.83	standalone	none	unassociated	Yes

VSG (Compute Firewall) Use Case



Compute Firewall Creation

- Compute Firewall controls Inter-VM (East-West) traffic
- VLAN-agnostic policy based operation



Add Compute Firewall

org-root/org-TenantA

General

Name:

Description:

Firewall Settings

Device Profile: [Select](#)

Management Hostname:

Data IP Address:

Data IP Subnet:

Compute Firewalls

General **Faults**

[+ Add Compute Firewall](#)

Name	Device Profile	Config State
TenantA-Compute-FW	default	applied

Assign VSG to Compute Firewall

Virtual Network Management Center

(admin) Preferences Log Out About Help Feedback

Tenant Management **Resource Management** Policy Management Administration

Managed Resources Resources Capabilities Diagnostics

Firewalls

- root
 - Compute Firewalls
 - Edge Firewalls
 - Pools
 - TenantA
 - Compute Firewalls
 - TenantA-Compute-FW**
 - Edge Firewalls
 - Pools
 - TenantB

root > TenantA > Compute Firewalls

TenantA-Compute-FW Assign VSG Assign Pool Unassign VSG/Pool

General Compute Security Profiles Faults Events

Name: TenantA-Compute-FW

Description:

Pool Name: Not Assigned

States

Config State: applied

Association State: associated

In case of failure, check 'Faults' tab on this page or [Faults Associated with Firewall](#) or [View Configuration Faults](#)

Firewall Settings

Device Profile: default Select

Management Hostname: TenantA-Compute-FW

Data IP Address: 192 . 168 . 100 . 20

Data IP Subnet: 255 . 255 . 255 . 0

VSG Details

VSG Service ID: 1005

VSG Mgmt IP: 172.25.108.86

HA Role: standalone

Association: associated

Reachable: Yes

Compute Firewall Policy: Rule Construct

Rule

Source Condition

Destination Condition

Action

Condition

Attribute Type : Network

Expression

Attribute Name : IP Address

Operator : eq (Equals)

Attribute Value : 192 . 168 . 1 . 2

Attribute Type

Network

VM

User Defined

vZone

Action to Take:

drop

permit

reset

log

VM Attributes

VM Name

Guest OS full name

Zone Name

Parent App Name

Port Profile Name

Cluster Name

Hypervisor Name

VM DNS Name

Network Attributes

IP Address

Network Port

Operator

eq

neq

gt

lt

range

Not-in-range

Prefix

Operator

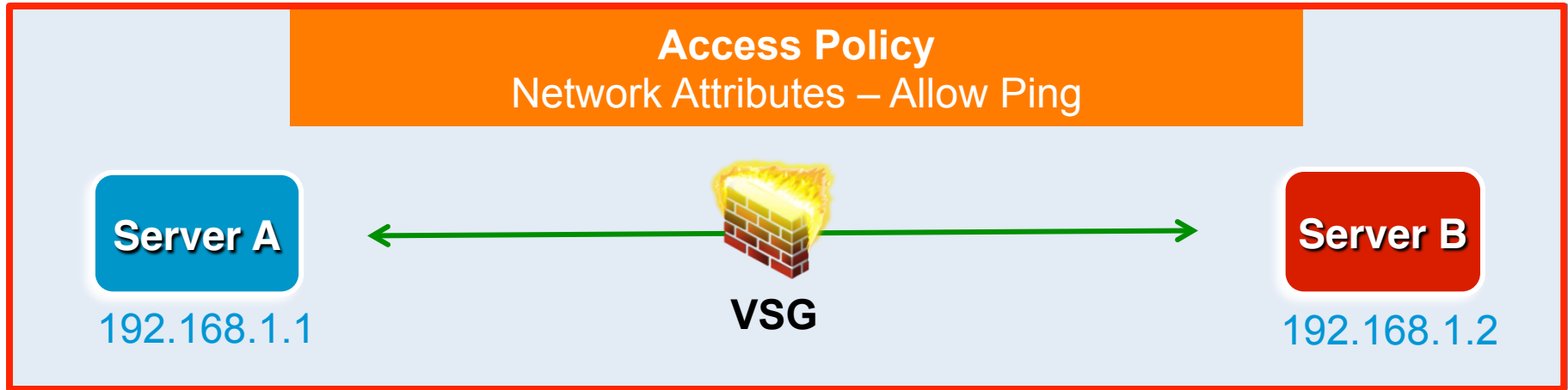
member

Not-member

Contains

Compute Firewall – Use Case 1a

Access Policy based on Network Attributes



Rule Table

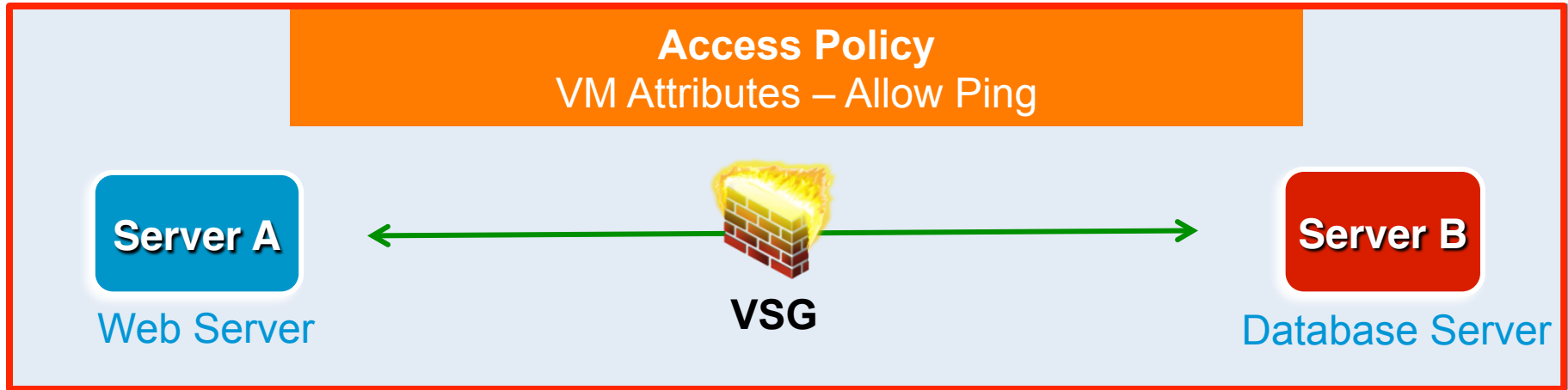
+ Add Rule | Edit | Delete | [Up Arrow] | [Down Arrow] | [Refresh Arrow]

Name	Source Condition	Destination Condition	Protocol	EtherType	Action
Allow_ICMP	IP Address eq 192.168.1.1	IP Address eq 192.168.1.2	eq ICMP	Any	Permit, Log

Source Condition Destination Condition Action

Compute Firewall – Use Case 1b

Access Policy based on VM Attributes



Rule Table

+ Add Rule | Edit | Delete | [Up Arrow] | [Down Arrow]

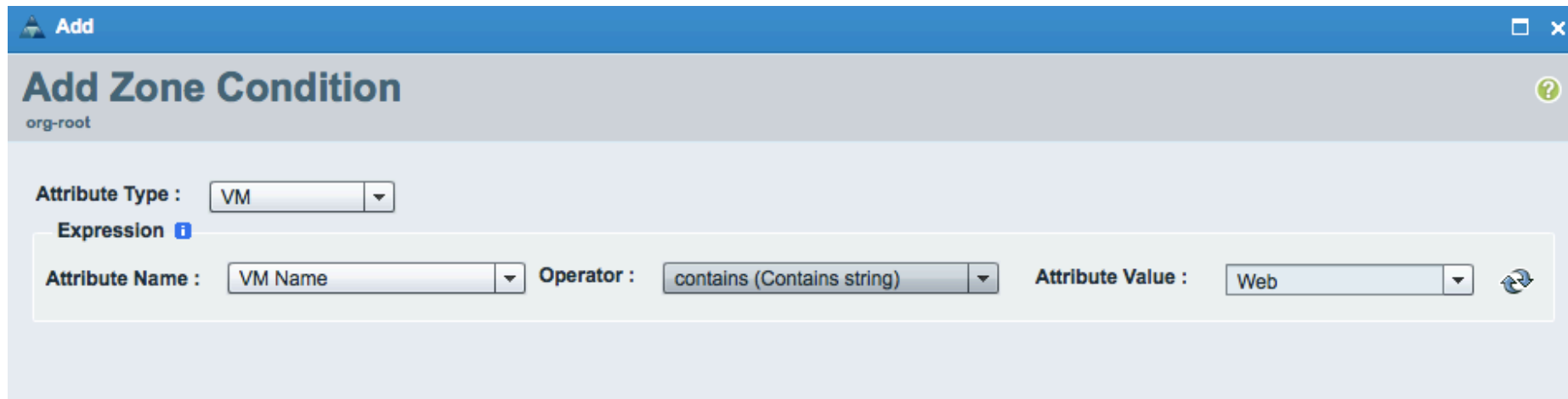
Name	Source Condition	Destination Condition	Protocol	EtherType	Action
Allow_ICMP	VM Name contains Web	VM Name contains Database	eq ICMP	Any	Permit, Log

Source Condition Destination Condition Action

Compute Firewall – Use Case 1c

Access Policy based on Zones

- Zones are defined by a condition leveraging the attributes e.g. Network, VM or User Defined Attributes

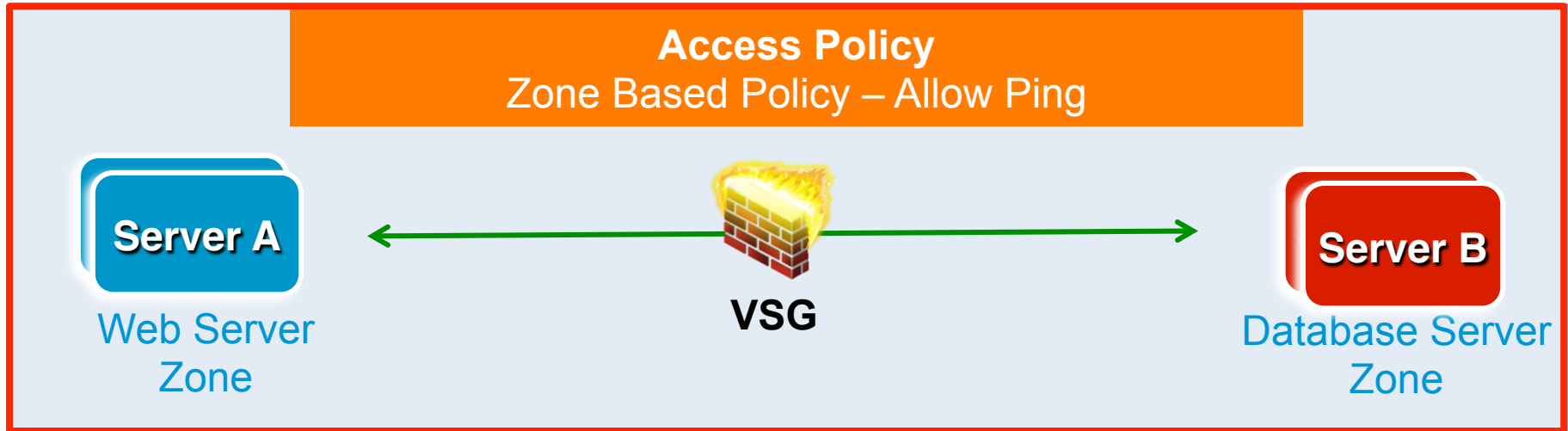


The screenshot shows a web-based interface for adding a zone condition. The window has a blue title bar with the text 'Add' and standard window controls. Below the title bar, the main heading is 'Add Zone Condition' with a sub-label 'org-root' and a help icon. The form contains the following fields:

- Attribute Type :** A dropdown menu with 'VM' selected.
- Expression :** A section containing three fields:
 - Attribute Name :** A dropdown menu with 'VM Name' selected.
 - Operator :** A dropdown menu with 'contains (Contains string)' selected.
 - Attribute Value :** A dropdown menu with 'Web' selected, followed by a refresh icon.

Compute Firewall – Use Case 1b

Access Policy based on Zones (contd.)



Rule Table

+ Add Rule | Edit | Delete | [Up Arrow] | [Down Arrow] | [Refresh] | [Export] | Records: 1

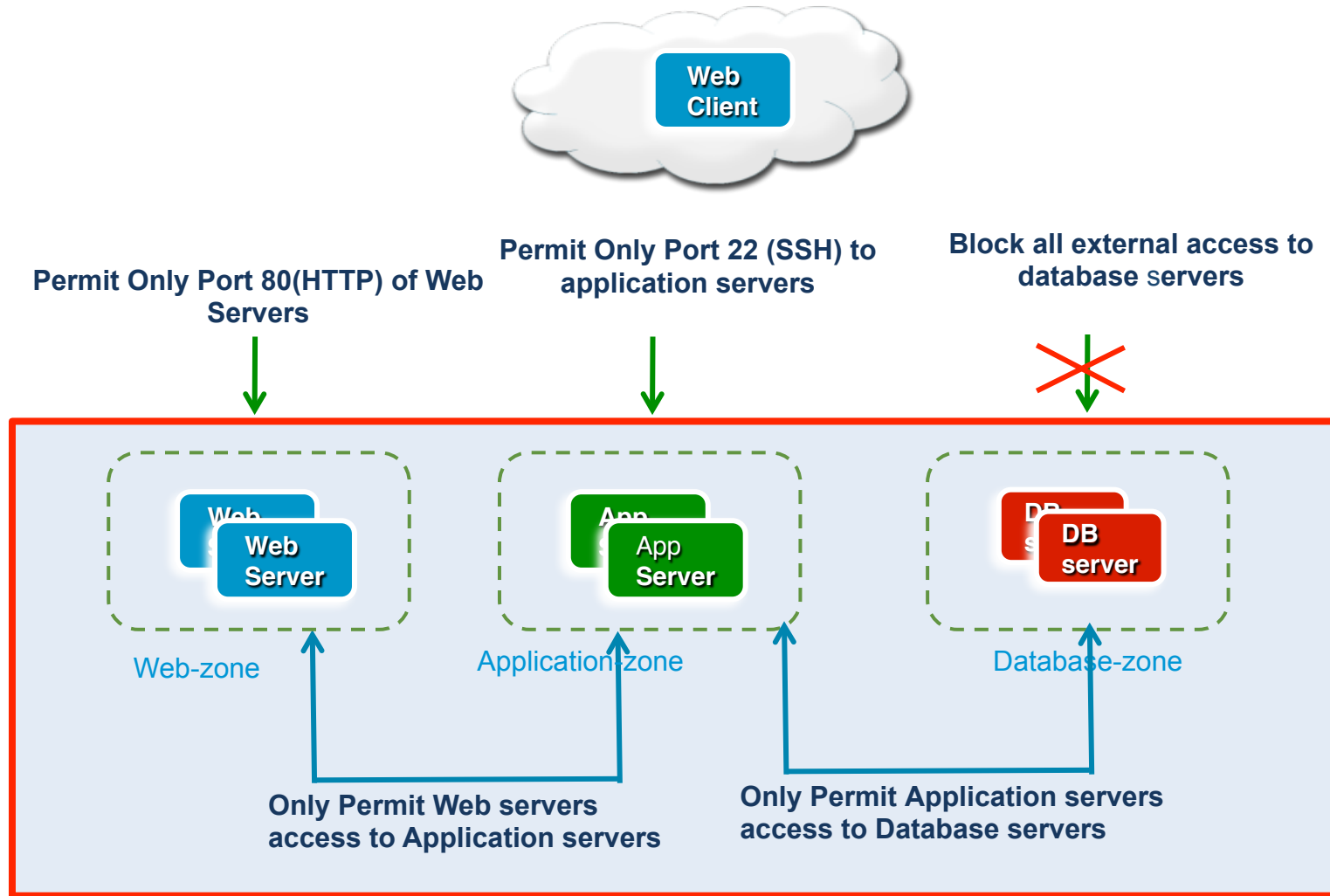
Name	Source Condition	Destination Condition	Protocol	EtherType	Action
Allow_ICMP	vZone Name eq WebZone	vZone Name eq DBZone	eq ICMP	Any	Permit, Log

Source Condition

Destination Condition

Action

Use Case 2: Content Hosting Policy



Policy – Content Hosting

Use Case 2: Policy Rules with Zones

- Leveraging Zones in Rule Conditions

Rule Table

 Add Rule |    

Name	Source Condition	Destination Condition	Protocol	EtherType	Action
Allow-Web	Any	Network Port eq 80 vZone Name eq WebZone	eq TCP	Any	Permit, Log
Allow-SSH	Any	Network Port eq 22 vZone Name eq AppZone	eq TCP	Any	Permit, Log
Allow-Web-To-App	vZone Name eq WebZone	vZone Name eq AppZone	Any	Any	Permit
Allow-App-To-Web	vZone Name eq AppZone	vZone Name eq WebZone	Any	Any	Permit
Allow-App-To-DB	vZone Name eq AppZone	vZone Name eq DBZone	Any	Any	Permit
Allow-DB-To-App	vZone Name eq DBZone	vZone Name eq AppZone	Any	Any	Permit
Deny-Rule	Any	Any	Any	Any	Drop, Log

Bind Compute Security Profile to a Port-Profile

- Define the service node using Nexus 1000V VSM

```
vservice node TenantA-vsg type vsg
  ip address 192.168.100.20
  adjacency l2 vlan 1203
  fail-mode close
```
- Define the Service Chain using Nexus 1000V VSM

```
vservice path security-chain
  node TenantA-vsg profile TenantA-Compute-Security-Profile order 1
```
- Enable the Service Chain on Port-Profile using Nexus 1000V VSM

```
port-profile type vethernet TenantA
  vmware port-group
  switchport mode access
  switchport access vlan 1203
  org root/TenantA
  vservice path security-chain ←
  no shutdown
  state enabled
```

ASA 1000V (Edge Firewall) Use Case



Edge Firewall – ASA 1000V

- Cisco ASA 1000V Edge Firewall complements Cisco VSG to provide multitenant edge security and default gateway functionality, and protects against network-based attacks.

TenantA-Edge-Firewall

Assign ASA 1000VAssign PoolUnassign

GeneralEdge Security ProfilesFaultsEvents

Pool Name: ⓘ Not Assigned

States

Config State: applied

Association State: associated

In case of failure, check 'Faults' tab on this page or [Faults Associated with Firewall](#) or [View Configuration Faults](#)

Firewall Settings

Device Profile: Device-Profile-2 Select

Edge Device Profile: TenantA-Edge-Device-Profile Select

Management Hostname: ⓘ TenantA-Edge-Firewall

ASA 1000V Details

Launch ASDM

Edge Firewall Service ID: 1008

Edge Firewall Mgmt IP: 172.25.108.87

HA Role: standalone

Association: associated

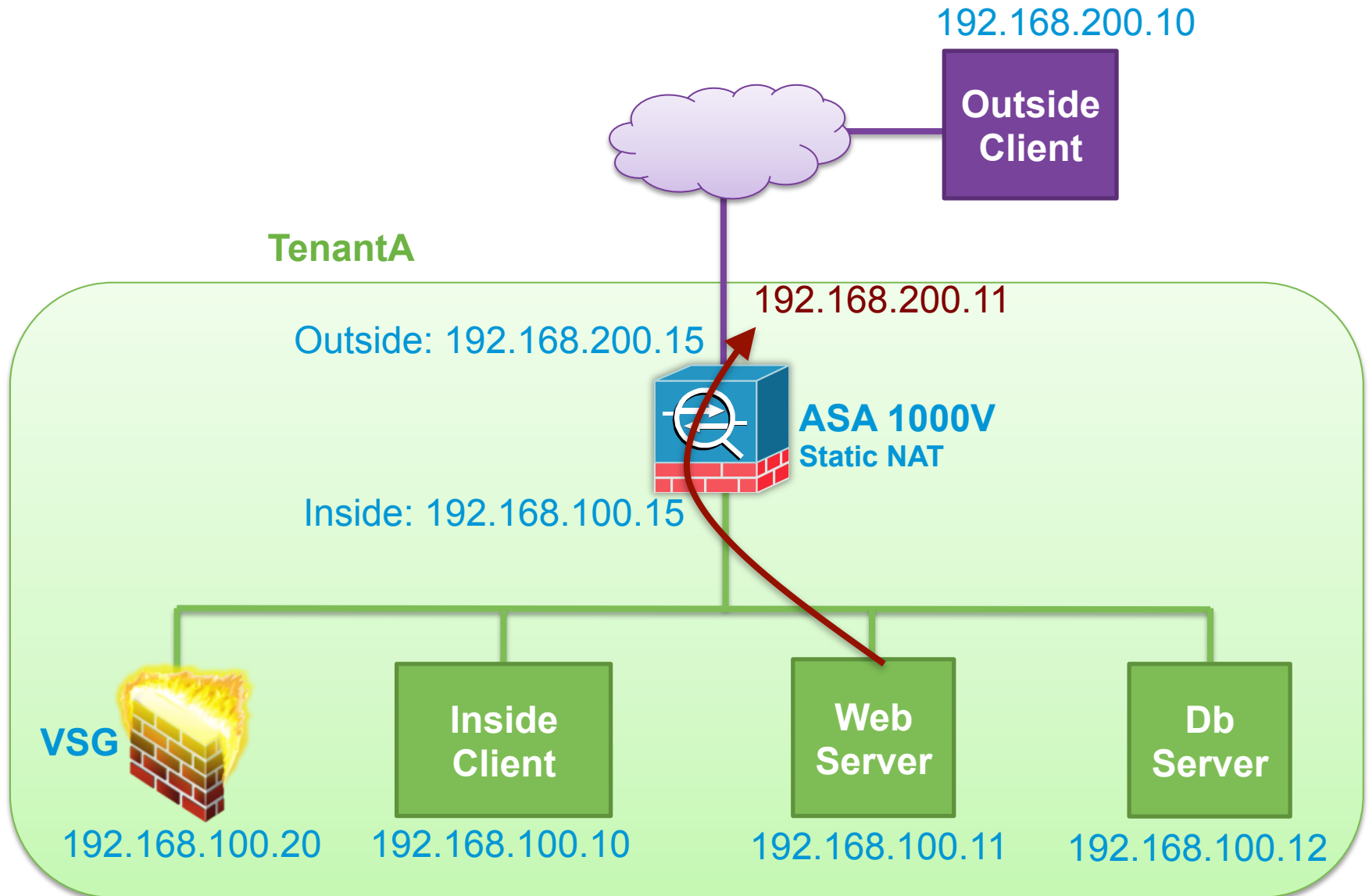
Reachable: Yes

Interfaces

+ Add Data Interface

Role	Name	Primary IP	Secondary IP	Network Mask	DHCP Enabled	Edge Security Profile	De
inside	inside	192.168.100.15	0.0.0.0	255.255.255.0	no		
outside	outside	192.168.200.15	0.0.0.0	255.255.255.0	no	TenantA-Outside-Intf	

Edge Firewall – Static NAT Use Case



Edge Security Profile – Static NAT

TenantA-Edge-Security-Profile

General Ingress Egress **NAT** VPN Advanced Events

Policy Set: + Add NAT Policy Set

Resolved NAT Policy Set: [org-root/natpset-default](#)

Add NAT Policy Set

org-root/org-TenantA

General

Name:

Description:

Admin State: ☐ disabled ☒ enabled

Policies: + Add NAT Policy Edit

Add NAT Policy

org-root/org-TenantA

General

Name:

Description:

Admin State: ☐ disabled ☒ enabled

Rule Table

+ Add Rule

Name	Source Condition
------	------------------

Edge Security Profile – Static NAT (2)

Add NAT Policy Rule

org-root/org-TenantA

General

Name:

Description:

Original Packet Match Conditions (Note: Configured Rule Conditions)

Source Match Conditions

Add Rule Condition Recd

Attribute Name	Operator	Attribute Value
----------------	----------	-----------------

Add Rule Condition

org-root/org-TenantA

Attribute Type : Network

Expression

Attribute Name : Operator : Attribute Value :

Edge Security Profile – Static NAT (3)

Name:

Description:

Original Packet Match Conditions (Note: Configured Rule Conditions will have A
Source Match Conditions ⓘ)

 Add Rule Condition Records: 1

Attribute Name	Operator	Attribute Value
IP Address	eq	192.168.100.11

If any port pool is set the protocol must be (use eq) TCP or UDP.

Protocol: ⓘ ☒ Any

*** Refer to NAT Action Table tooltip for validations. ***

NAT Action Table ⓘ

NAT Action: ⓘ

Translated Address:  Add Object Group

Resolved Source IP Pool:

Add Object Group

org-root/org-TenantA

General

Name:

Description:

Attribute Type :

Attribute Name :

Expression ⓘ

 Add Object Group Expression

Operator	Value
eq	192.168.200.11

Edge Security Profile – Static NAT (4)

Add NAT Policy Rule

org-root/org-TenantA

General

Name:

Description:

Original Packet Match Conditions (Note: Configured Rule Conditions will have AND semantics.) ⓘ

Source Match Conditions ⓘ

Destination Match

Records: 1

Attribute Name	Operator	Attribute Value
IP Address	eq	192.168.100.11

Protocol: ⓘ ☒ Any

Refer to NAT Action Table tooltip for validations.

NAT Action Table ⓘ

NAT Action: ⓘ Static ▼

Translated Address: ⓘ Add Object Group

Resolved Source IP Pool: [org-root/org-TenantA/objgrp-TenantA-NAT-Obj-Grp](#)

Edge Security Profile– Static NAT (5)

The screenshot displays the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes 'Tenant Management', 'Resource Management', 'Policy Management' (highlighted), and 'Administration'. Below this, a secondary bar shows 'Service Profiles', 'Service Policies', 'Device Configurations', 'Capabilities', and 'Diagnostics'. The left sidebar shows a hierarchical tree structure with 'TenantA' expanded, showing 'Compute Firewall', 'Compute Security Profiles' (containing 'TenantA-Compute-Security-Profile'), 'Edge Firewall', 'Edge Device Profiles' (containing 'TenantA-Edge-Device-Profile'), 'Edge Security Profiles' (containing 'TenantA-Edge-Security-Profile', which is highlighted), and 'TenantA-Outside-Intf'. The main content area shows the configuration for 'TenantA-Edge-Security-Profile' with tabs for 'General', 'Ingress', 'Egress', 'NAT' (highlighted), 'VPN', 'Advanced', and 'Events'. Under the 'NAT' tab, the 'Policy Set' is set to 'TenantA-NAT-PS' with a '+ Add NAT Policy Set' button. Below this, the 'Resolved NAT Policy Set' is shown as a link: 'org-root/org-TenantA/natpset-TenantA-NAT-PS'. The 'Resolved Policies' section includes a table with one rule: 'TenantA-NAT-Rule'.

Policy Set: + Add NAT Policy Set

Resolved NAT Policy Set: [org-root/org-TenantA/natpset-TenantA-NAT-PS](#) ↑

Resolved Policies ⓘ

+ (Un)assign Policy | | ↑ ↑ ↓ ↓

Name	Source Condition	Destination Condition	Protocol	Action
▼ TenantA-NAT-				
👉 TenantA-NAT-Rule	IP Address eq 192.168.100.11	Any	Any	Static

Bind Edge Security Profile to Port-Profile

- Define the service node in Nexus 1000V for ASA1000V

```
vservice node TenantA-asa type asa
  ip address 192.168.100.15
  adjacency l2 vlan 1203
  fail-mode open
```

- Define the Service Chain (Order is inside to outside)

```
vservice path security-chain
  node TenantA-vsg profile TenantA-Compute-Security-Profile order 1
  node TenantA-asa profile TenantA-Edge-Security-Profile order 2
```

- Enable the Service Chain on Port-Profile

```
port-profile type vethernet TenantA
  vmware port-group
  switchport mode access
  switchport access vlan 1203
  org root/TenantA
  vservice path security-chain
  no shutdown
  state enabled
```



Policy Enforcement Verification

■ Syslog Messages

Date	Time	Priority	Hostname	Message
07-31-2012	05:52:54	Local4.Info	172.25.108.87	%ASA-6-302014: Teardown TCP connection 314036493 for outside:192.168.200.10/4605 to sp0003:192.168.100.11/80 duration 0:00:15 bytes 1223 TCP FINs
07-31-2012	05:52:39	Local0.Info	172.25.108.86	: 2012 Jul 30 22:54:06 PDT: %POLICY_ENGINE-6-POLICY_LOOKUP_EVENT: policy=TenantA-ACL-PS@root/TenantA rule=TenantA-ACL-Policy/Permit-Web@root/TenantA action=Permit direction=egress src.net.ip-address=192.168.200.10 src.net.port=4605 dst.net.ip-address=192.168.100.11 dst.net.port=80 net.protocol=6 net.ethertype=800
07-31-2012	05:52:39	Local4.Info	172.25.108.87	%ASA-6-302013: Built inbound TCP connection 314036493 for outside:192.168.200.10/4605 (192.168.200.10/4605) to sp0003:192.168.100.11/80 (192.168.200.11/80)
07-31-2012	05:52:28	Local4.Info	172.25.108.87	%ASA-6-302014: Teardown TCP connection 314036492 for outside:192.168.200.10/4591 to sp0003:192.168.100.11/80 duration 0:00:15 bytes 1223 TCP FINs
07-31-2012	05:52:16	Local0.Info	172.25.108.86	: 2012 Jul 30 22:53:43 PDT: %POLICY_ENGINE-6-POLICY_LOOKUP_EVENT: policy=TenantA-ACL-PS@root/TenantA rule=TenantA-ACL-Policy/Deny-All@root/TenantA action=Drop direction=ingress src.net.ip-address=192.168.100.10 src.net.port=138 dst.net.ip-address=192.168.100.255 dst.net.port=138 net.protocol=17 net.ethertype=800
07-31-2012	05:52:12	Local0.Info	172.25.108.86	: 2012 Jul 30 22:53:40 PDT: %POLICY_ENGINE-6-POLICY_LOOKUP_EVENT: policy=TenantA-ACL-PS@root/TenantA rule=TenantA-ACL-Policy/Permit-Web@root/TenantA action=Permit direction=egress src.net.ip-address=192.168.200.10 src.net.port=4591 dst.net.ip-address=192.168.100.11 dst.net.port=80 net.protocol=6 net.ethertype=800
07-31-2012	05:52:12	Local4.Info	172.25.108.87	%ASA-6-302013: Built inbound TCP connection 314036492 for outside:192.168.200.10/4591 (192.168.200.10/4591) to sp0003:192.168.100.11/80 (192.168.200.11/80)

■ Verify NAT on ASA 1000V

```
TenantA-Edge-Firewall# show nat detail
Manual NAT Policies (Section 1)
1 (sp0003) to (any) source static NSONog:TenantA-NAT-Policy:TenantA-NAT-Rule@sp0
003 root:TenantA:TenantA-NAT-Obj-Grp
   translate_hits = 0, untranslate_hits = 0
   Source - Origin: 192.168.100.11/32, Translated: 192.168.200.11/32
TenantA-Edge-Firewall#
```

Cisco N1KV, VSG, ASA 1000V & VNMC

Version Compatibility

	N1KV 1.4	N1KV 1.4a	N1KV 1.4b	N1KV 1.5.1	N1KV 1.5.2
VSG 1.0	VNMC 1.0 VSM PA 1.0 VSG PA 1.0	VNMC 1.0 VSM PA 1.0 VSG PA 1.0			
VSG 1.2		VNMC 1.2 VSM PA 1.2 VSG PA 1.2	VNMC 1.3 VSM PA 1.2 VSG PA 1.2		
VSG 1.3		VNMC 1.3 VSM PA 1.2 VSG PA 1.3		VNMC 1.3 VSM PA 1.3 VSG PA 1.3	
VSG 1.3a		VNMC 1.3 VSM PA 1.2 VSG PA 1.3	VNMC 1.3 VSM PA 1.2 VSG PA 1.3	VNMC 1.3 VSM PA 1.3 VSG PA 1.3	VNMC 2.0 VSM PA 2.0 VSG PA 1.3
VSG 1.4		VNMC 2.0 VSM PA 1.2 VSG PA 2.0	VNMC 2.0 VSM PA 1.2 VSG PA 2.0	VNMC 2.0 VSM PA 1.3 VSG PA 2.0	VNMC 2.0 VSM PA 2.0 VSG PA 2.0

Cisco N1KV, VSG, ASA1000V & VNMC

Version Compatibility (contd.)

	N1KV 1.4	N1KV 1.4a	N1KV 1.4b	N1KV 1.5.1	N1KV 1.5.2
ASA 1000V 8.7.1					VNMC 2.0 VSM PA 2.0
Service chain (VSG 1.4 & ASA 1000V 8.7.1)					VNMC 2.0 VSM PA 2.0 VSG PA 2.0

Otázky a odpovědi

Zodpovíme též v “Ptali jste se” v sále LEO v 17:45 – 18:30

e-mail: connect-cz@cisco.com

Prosíme, ohodnotte
tuto přednášku.

Děkujeme za pozornost.

