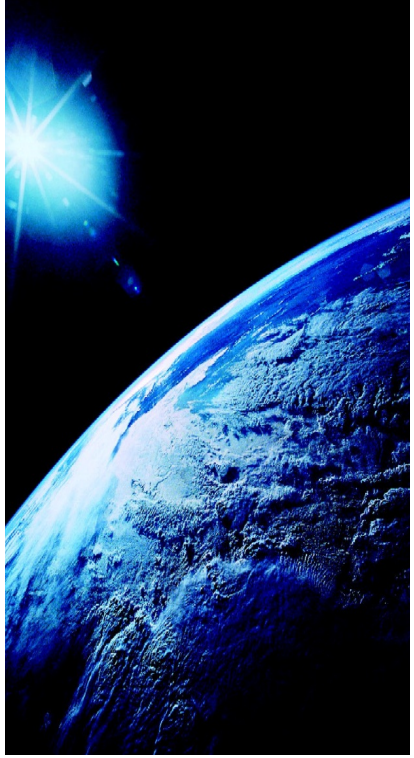
Cisco Connect

Praha, hotel Clarion
10. – 11. dubna 2013

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"

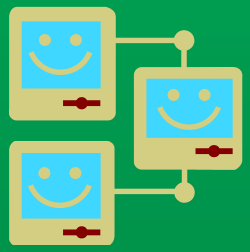
In Beta!

SCALE

Increased Scale

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

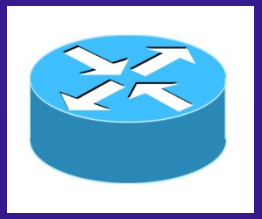
Evolution of VXLAN



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

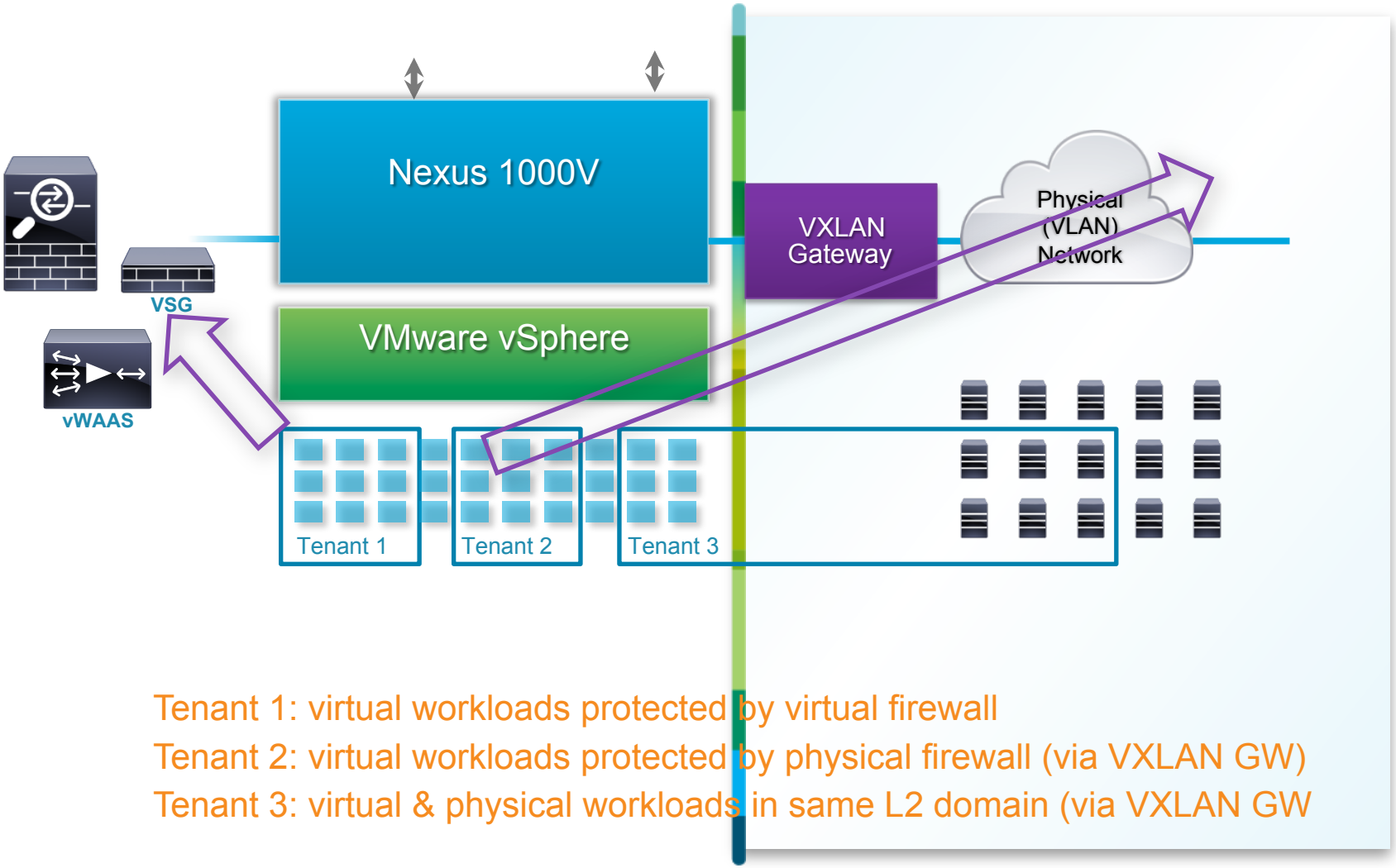
When?

- 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

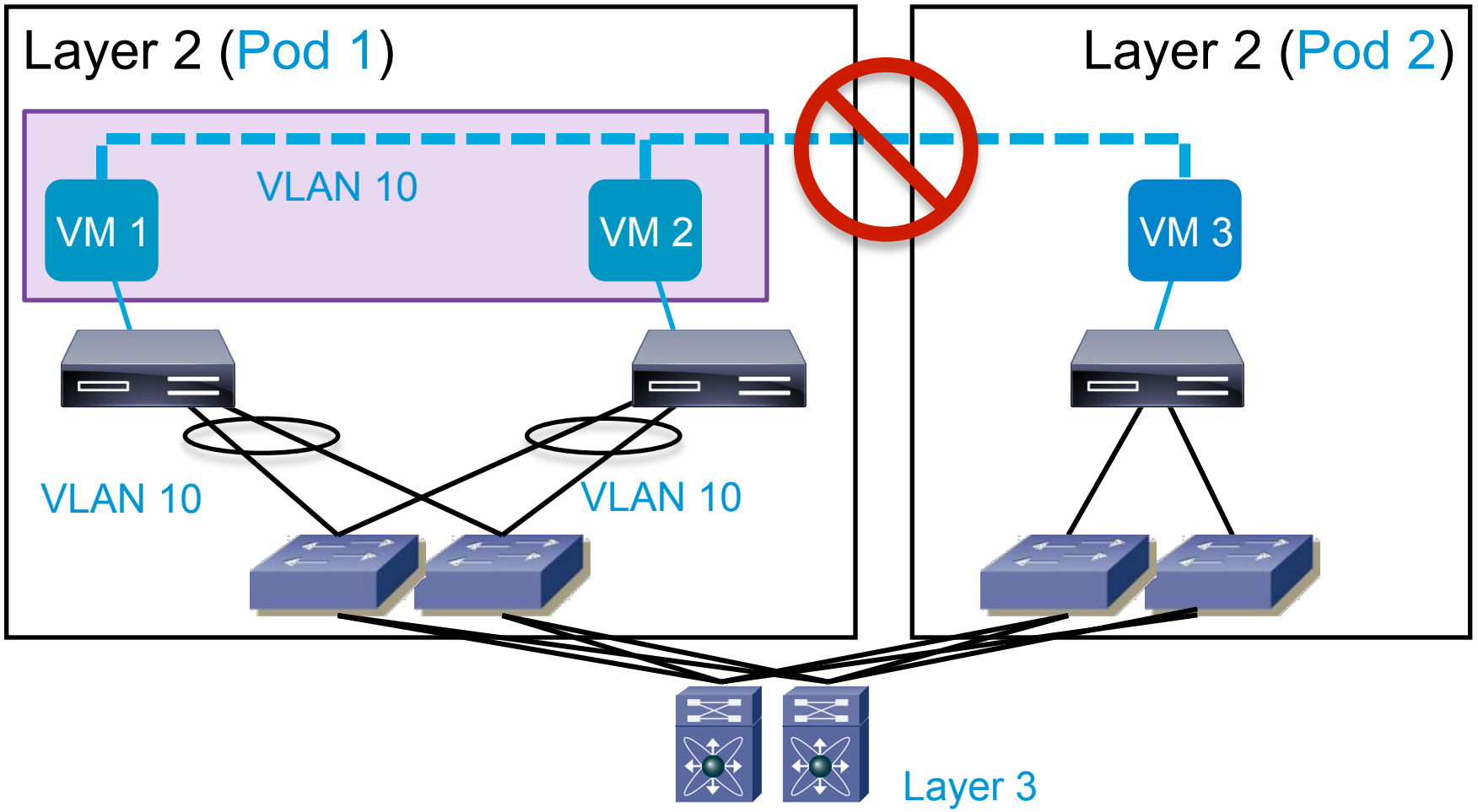
VXLAN Gateway



Tenant 1: virtual workloads protected by virtual firewall
Tenant 2: virtual workloads protected by physical firewall (via VXLAN GW)
Tenant 3: virtual & physical workloads in same L2 domain (via VXLAN GW

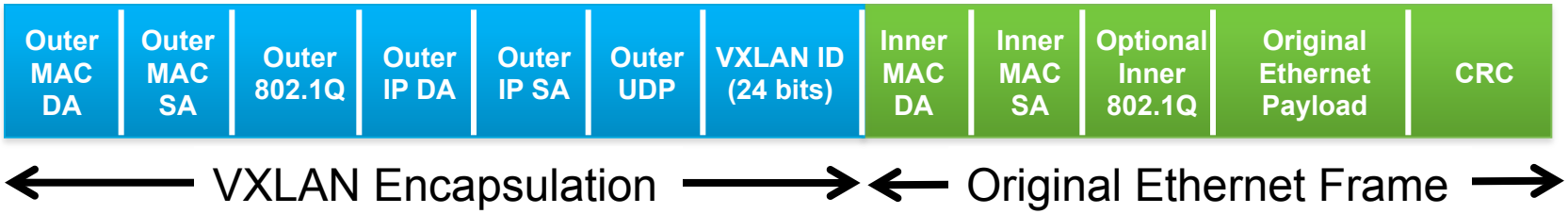
Deep dive

Existing Solution: Reachability of VMs Within VLAN

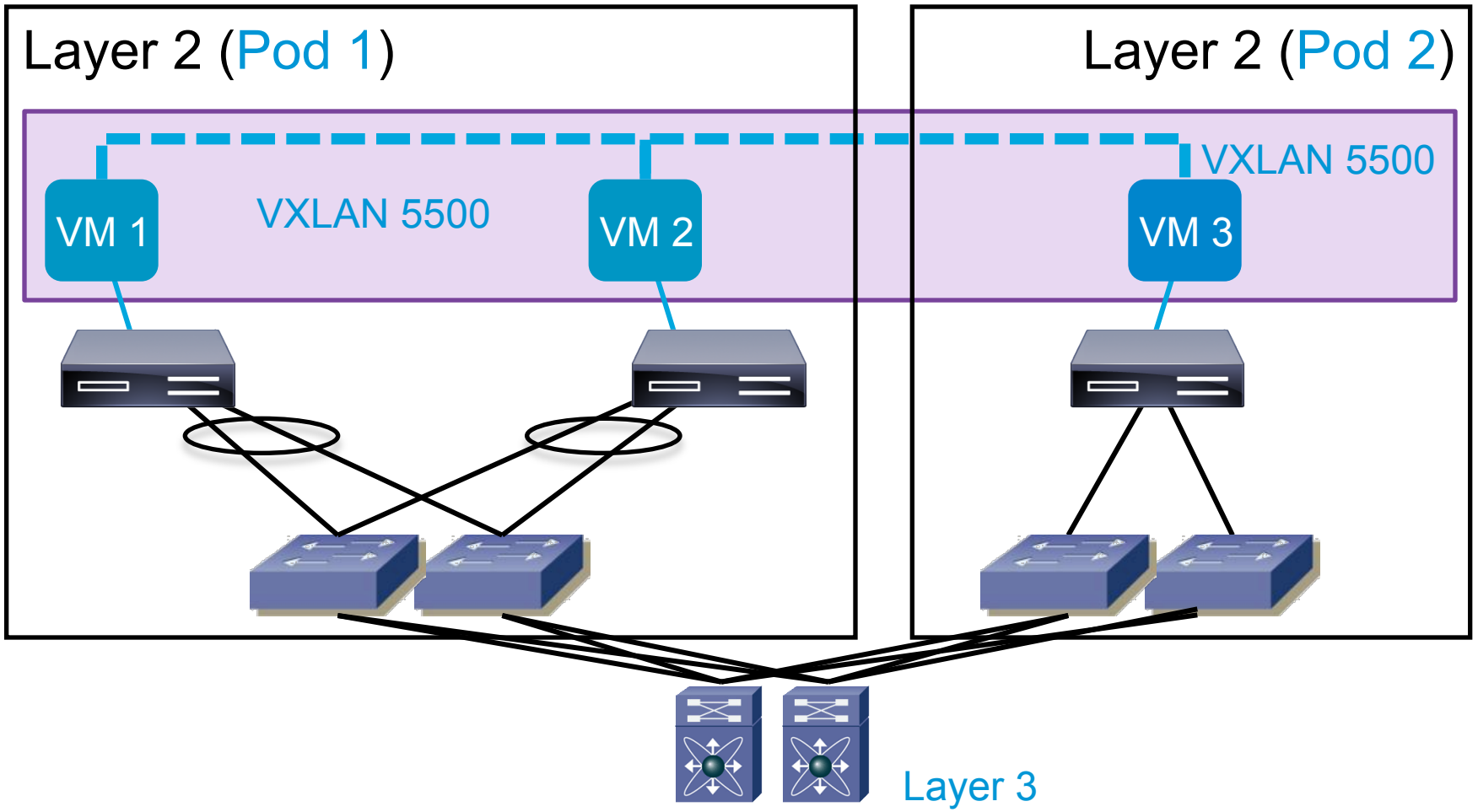


Virtual Extensible Local Area Network (VXLAN)

- 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

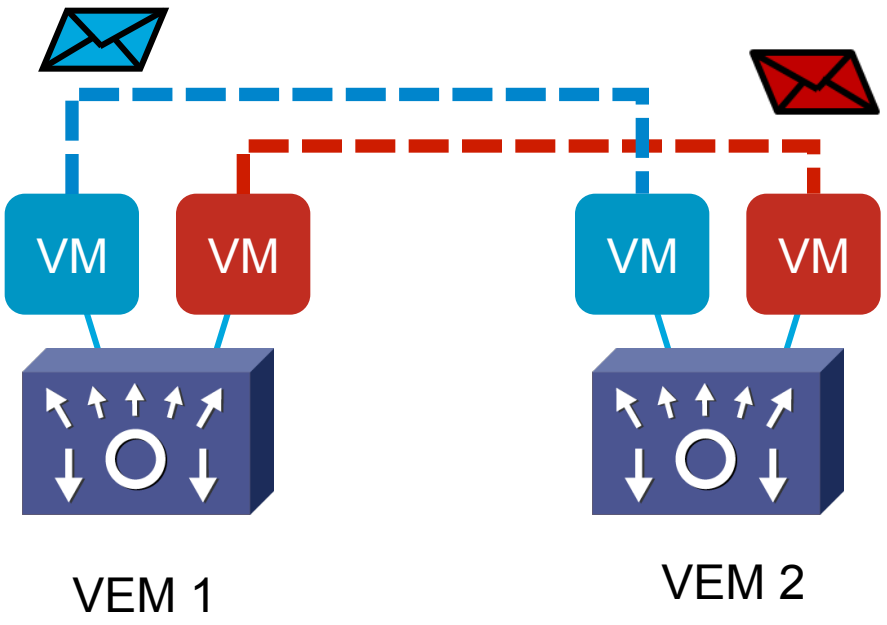
  VEM learns VM's Source (MAC, Host VXLAN IP) tuple

- Broadcast, Multicast, and Unknown Unicast Traffic

  VM broadcast & unknown unicast traffic are sent as multicast

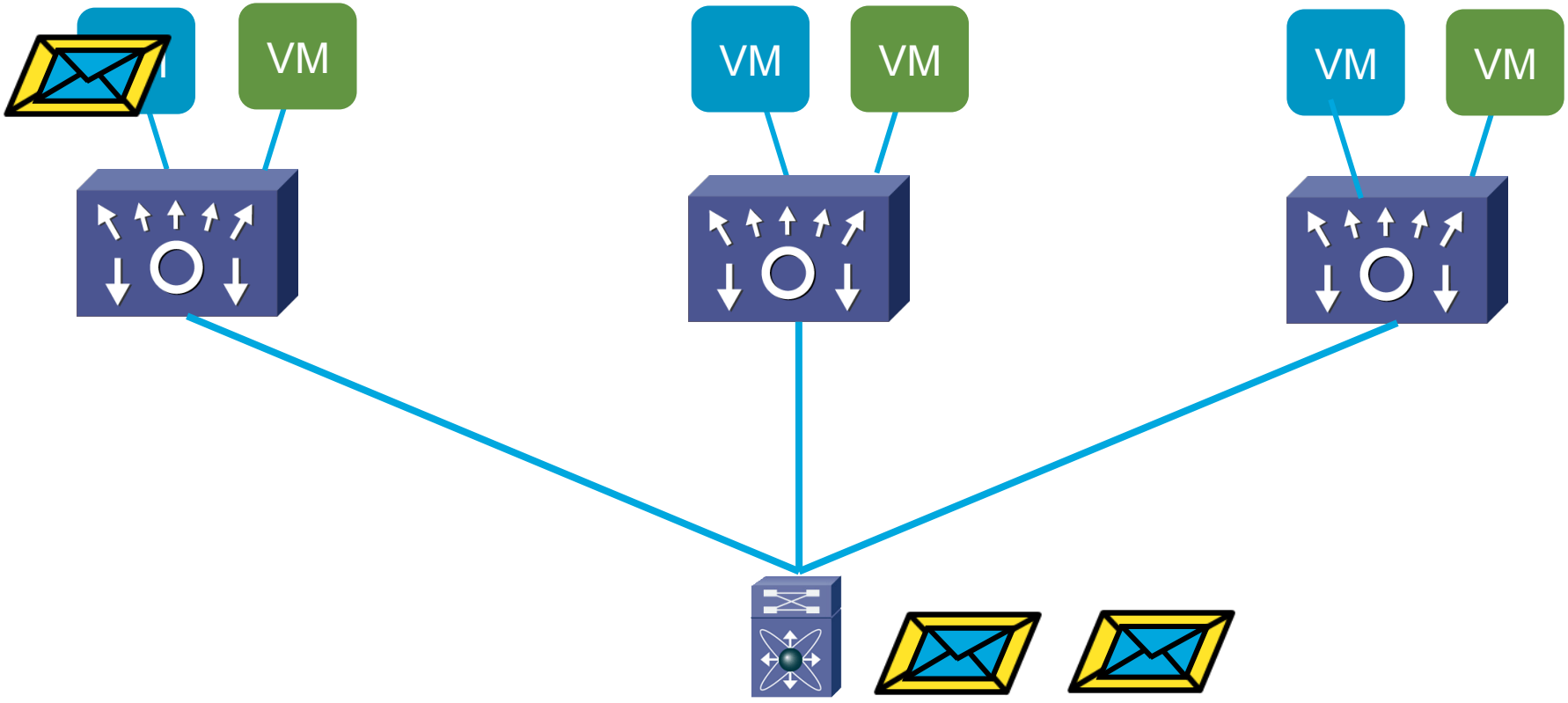
- Unicast Traffic

  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



Multicast in Physical Network

Flood and Learn

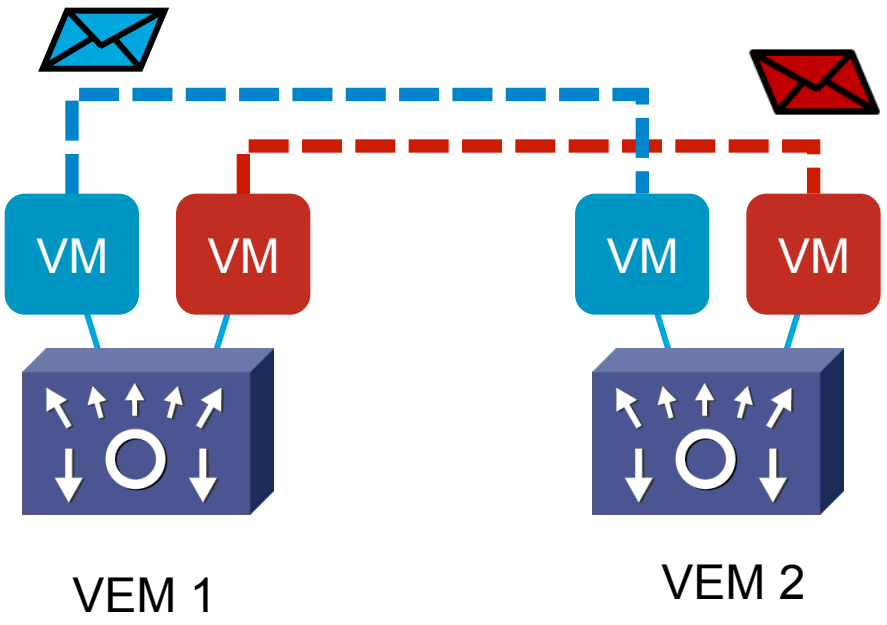
VXLAN Unicast Mode

VXLAN Unicast Mode Forwarding

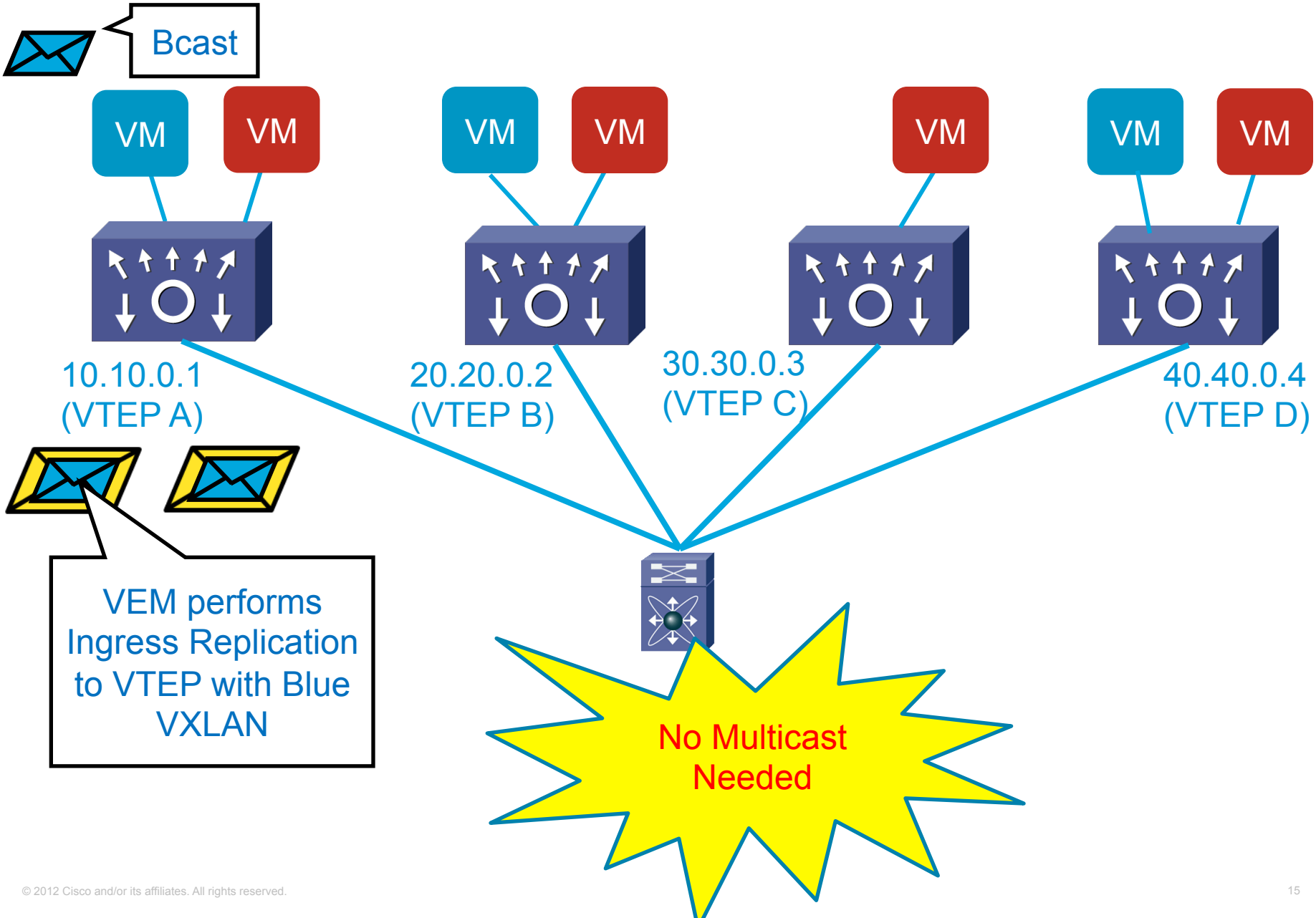
- Evolutionary approach - defines a Layer 2 domain without relying on IP Multicast.
- Multicast Configuration Avoided – VSM distributes (VXLAN, VTEP IP1, VTEP IP2,….VTEP IP n) list to all VEMs
- Flooding Avoided – using MAC Distribution. Each VEM knows all other VM MACs in a VXLAN segment.
- Broadcast 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

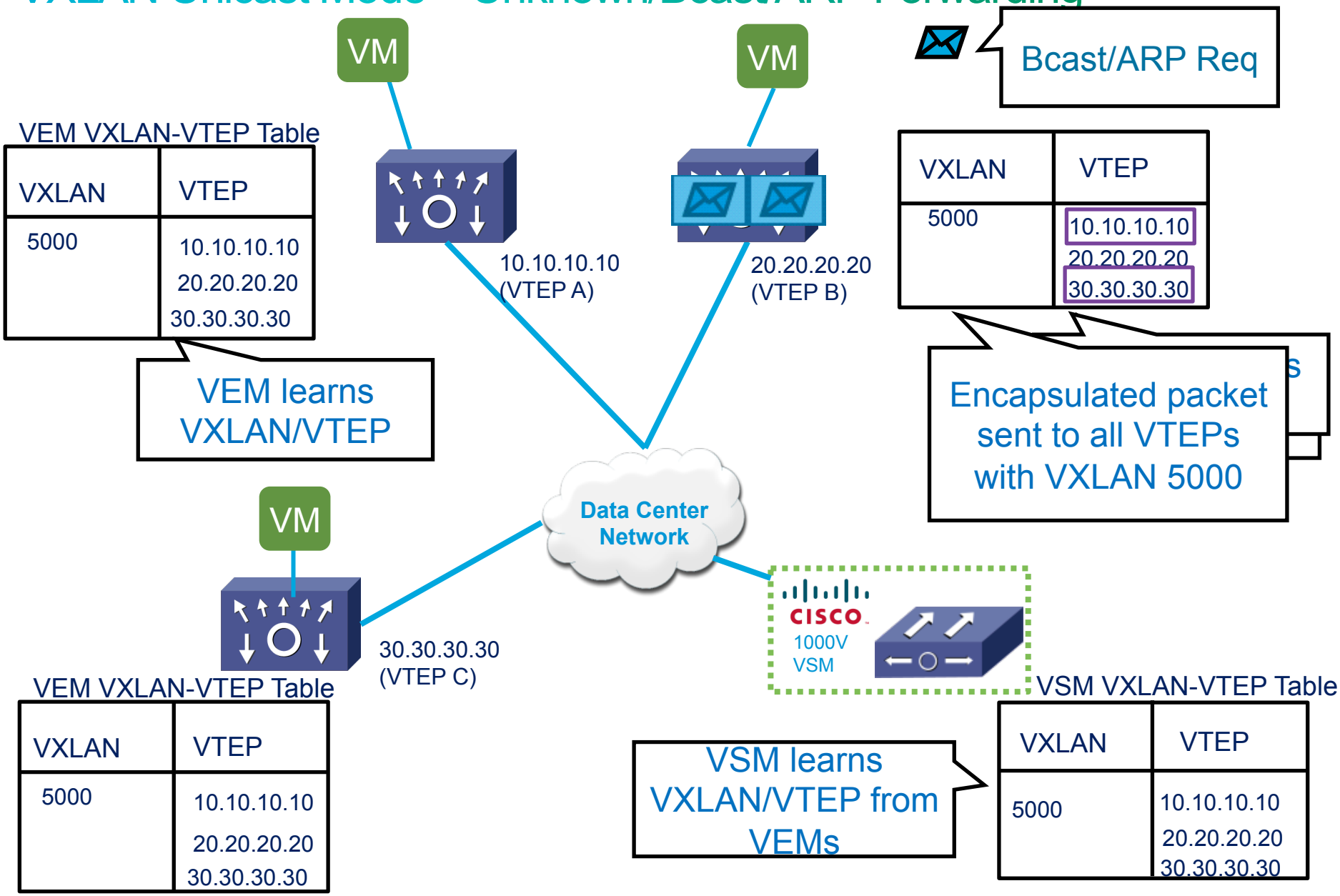
  Unicast packets are encapsulated and sent directly (not via multicast) to destination host VXLAN IP (Destination VEM)



Broadcast and Multicast in VXLAN Unicast Mode



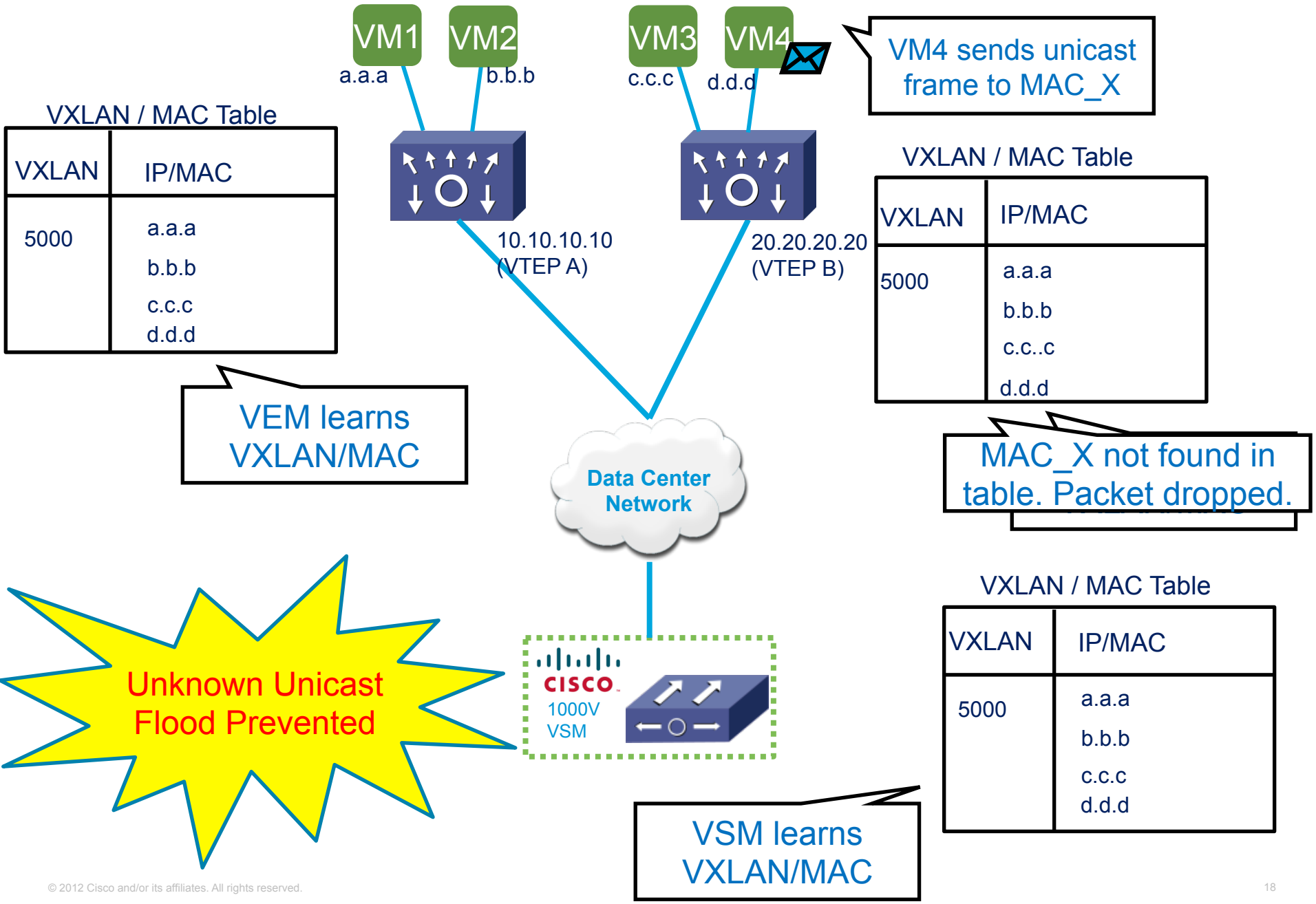
VXLAN Unicast Mode – Unknown/Bcast/ARP Forwarding



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

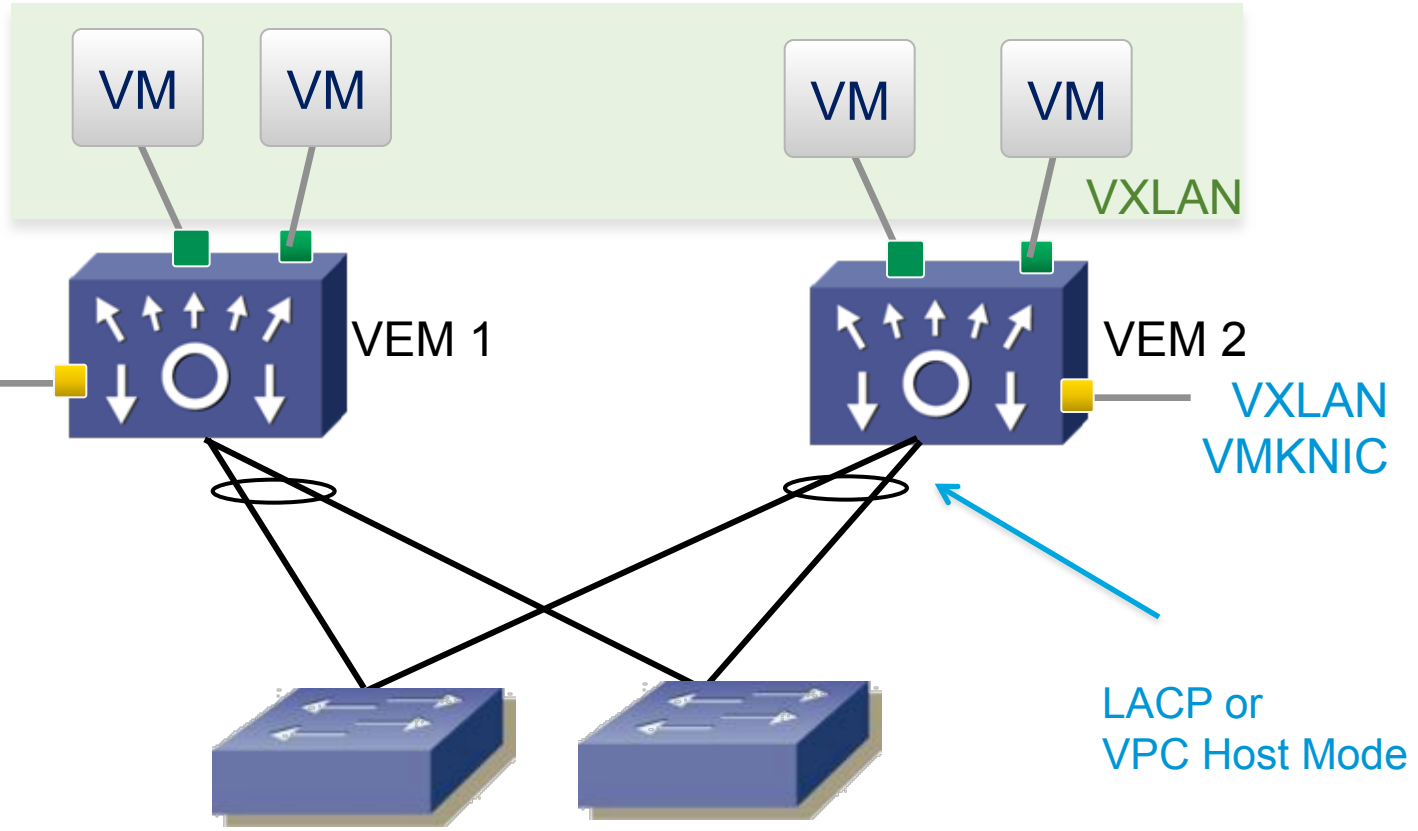


For Your Reference

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. VXLAN VMKNIC



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

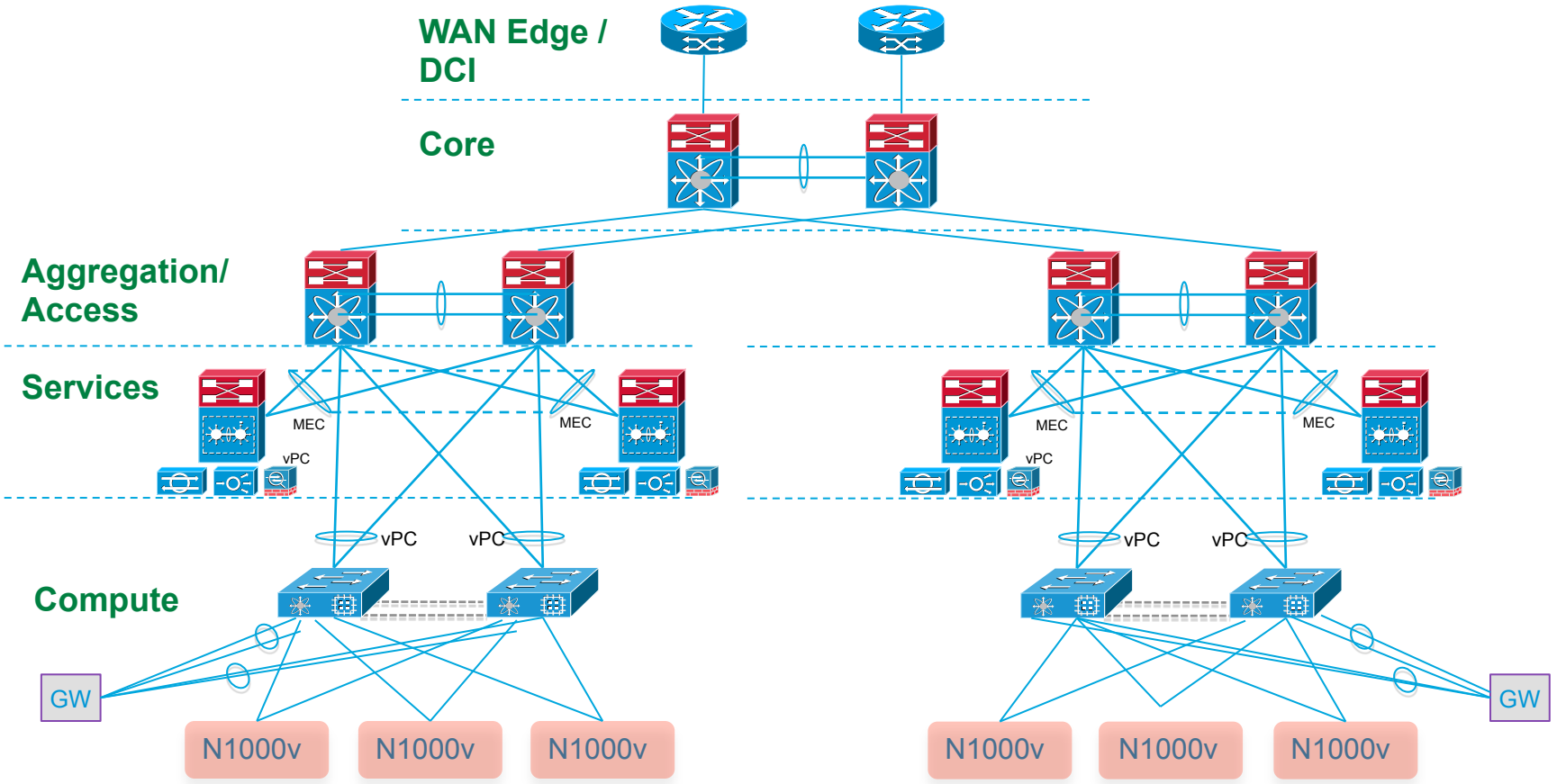
VXLAN Gateway Forwarding

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

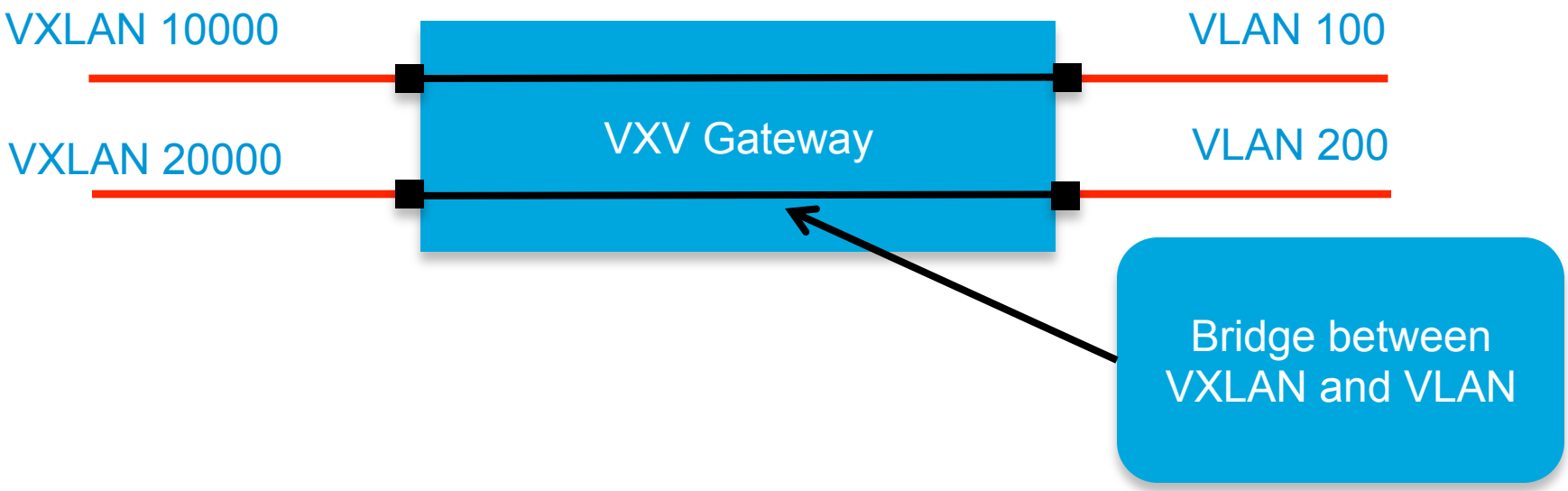
  Unlike VTEPs on ESX hosts, Gateway cannot publish MAC addresses of physical hosts to VSM
- Supports both VXLAN Multicast and Unicast Mode

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

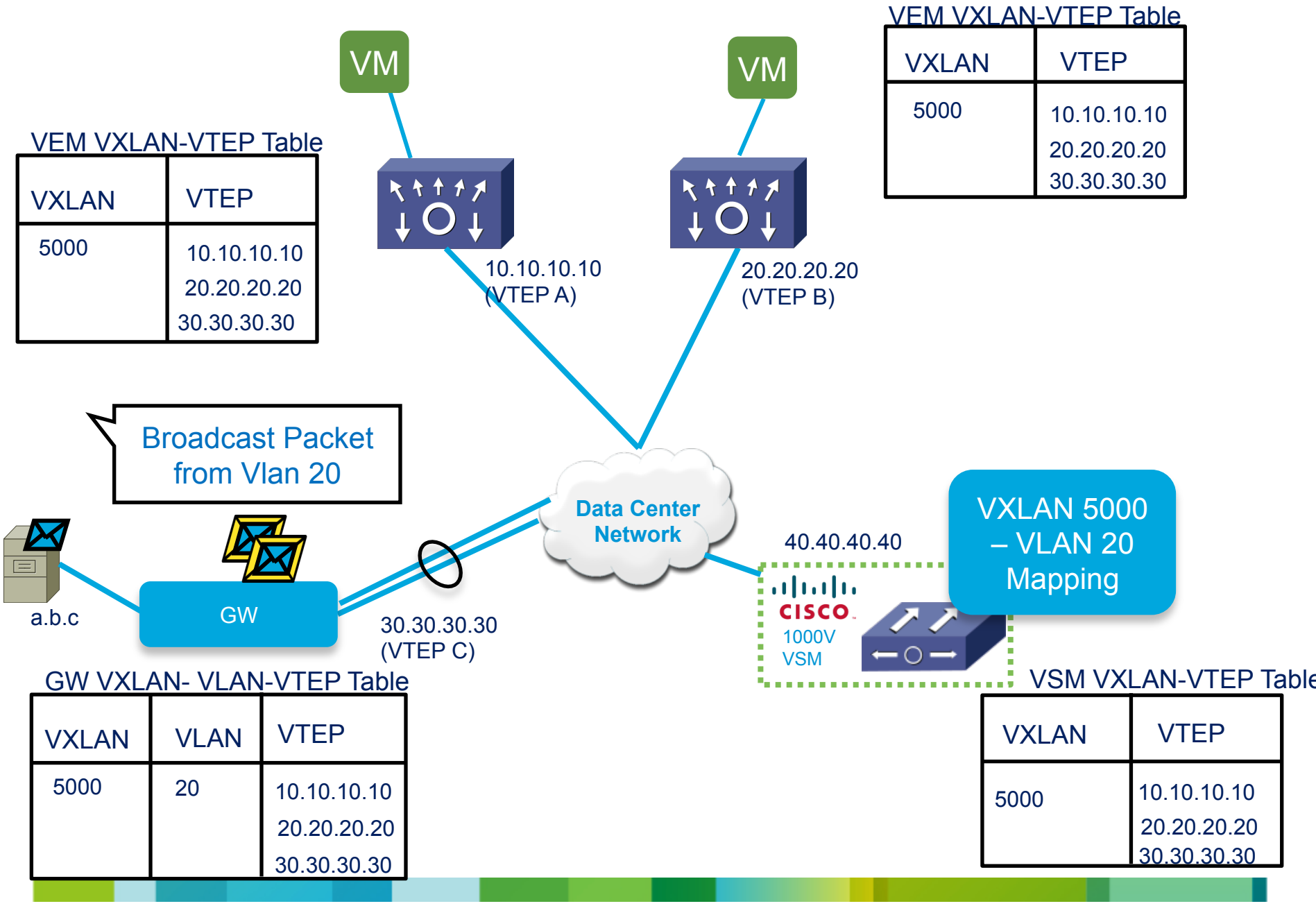
VXLAN Gateway Deployment



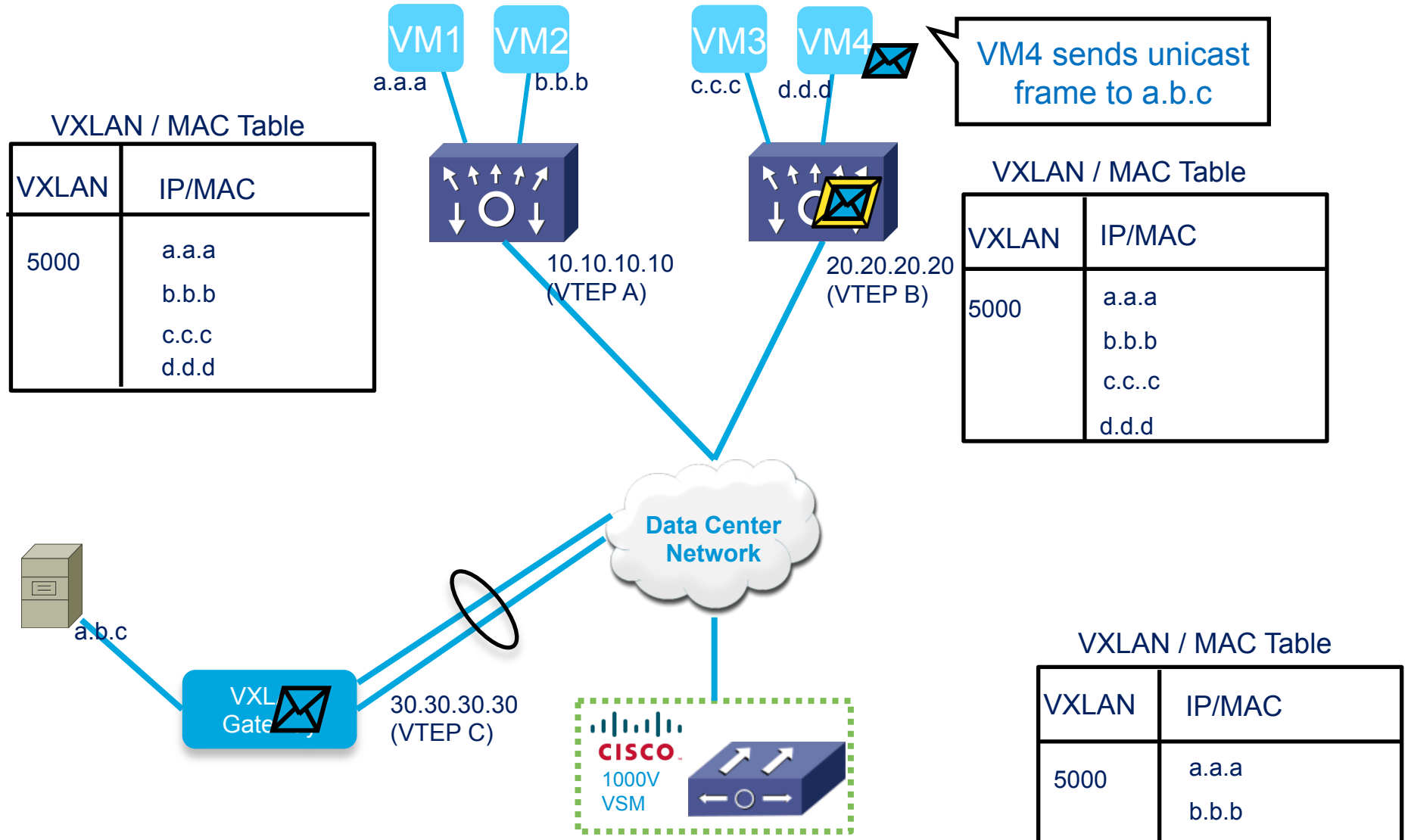
VXLAN Gateway – Logical View



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)#
```

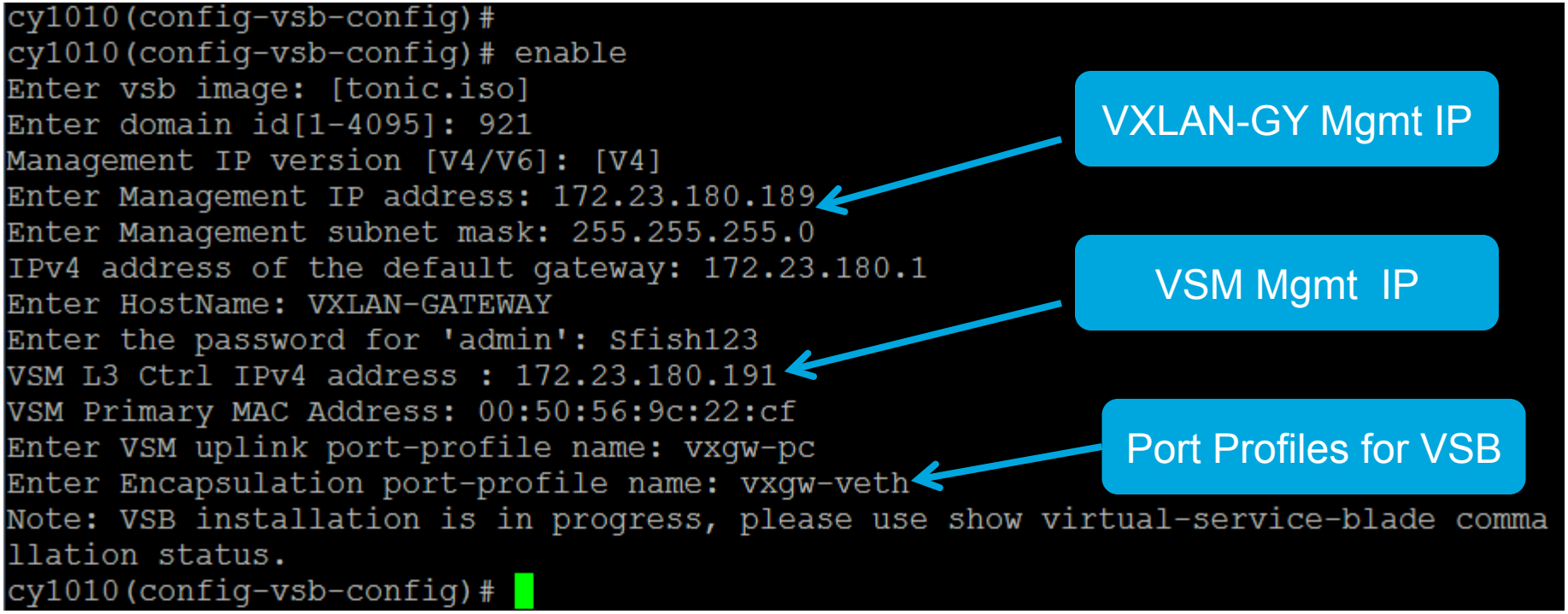
3. Create Port Profile on VSM for Gateway Data Uplink

```
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 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

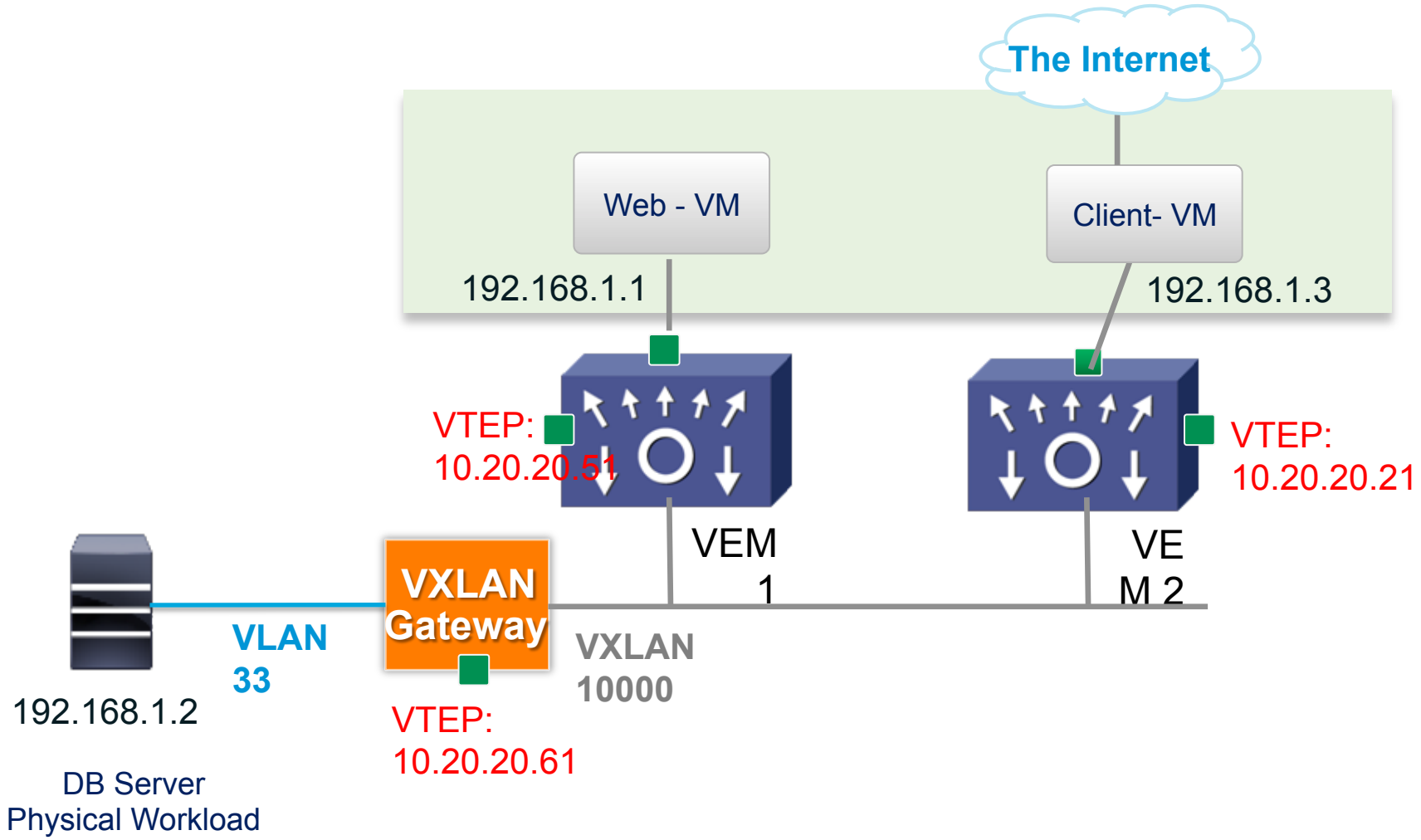
VXLAN Gateway use cases

VXLAN Gateway Use Cases

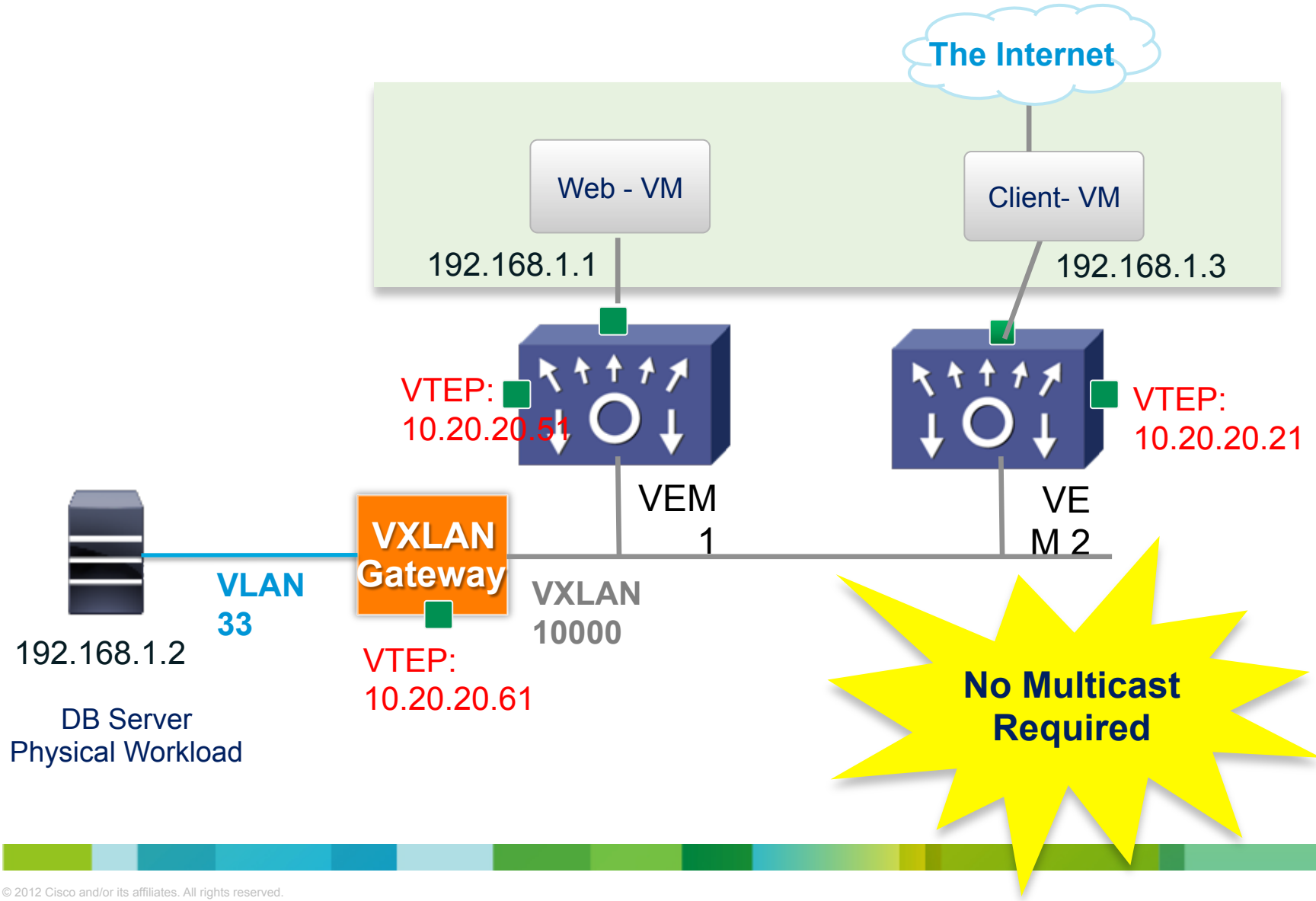
1. Virtualized WebServer VM communicating to Bare Metal DB Server

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

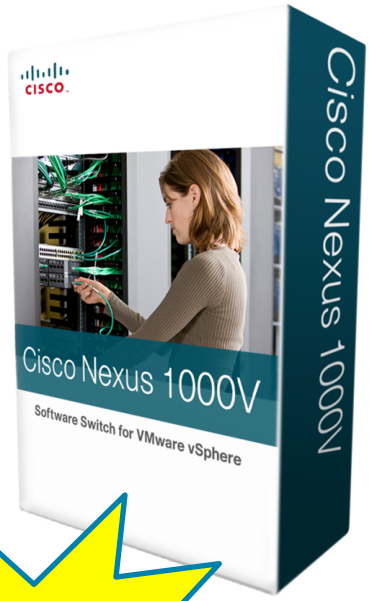


Deep dive summary

- 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!

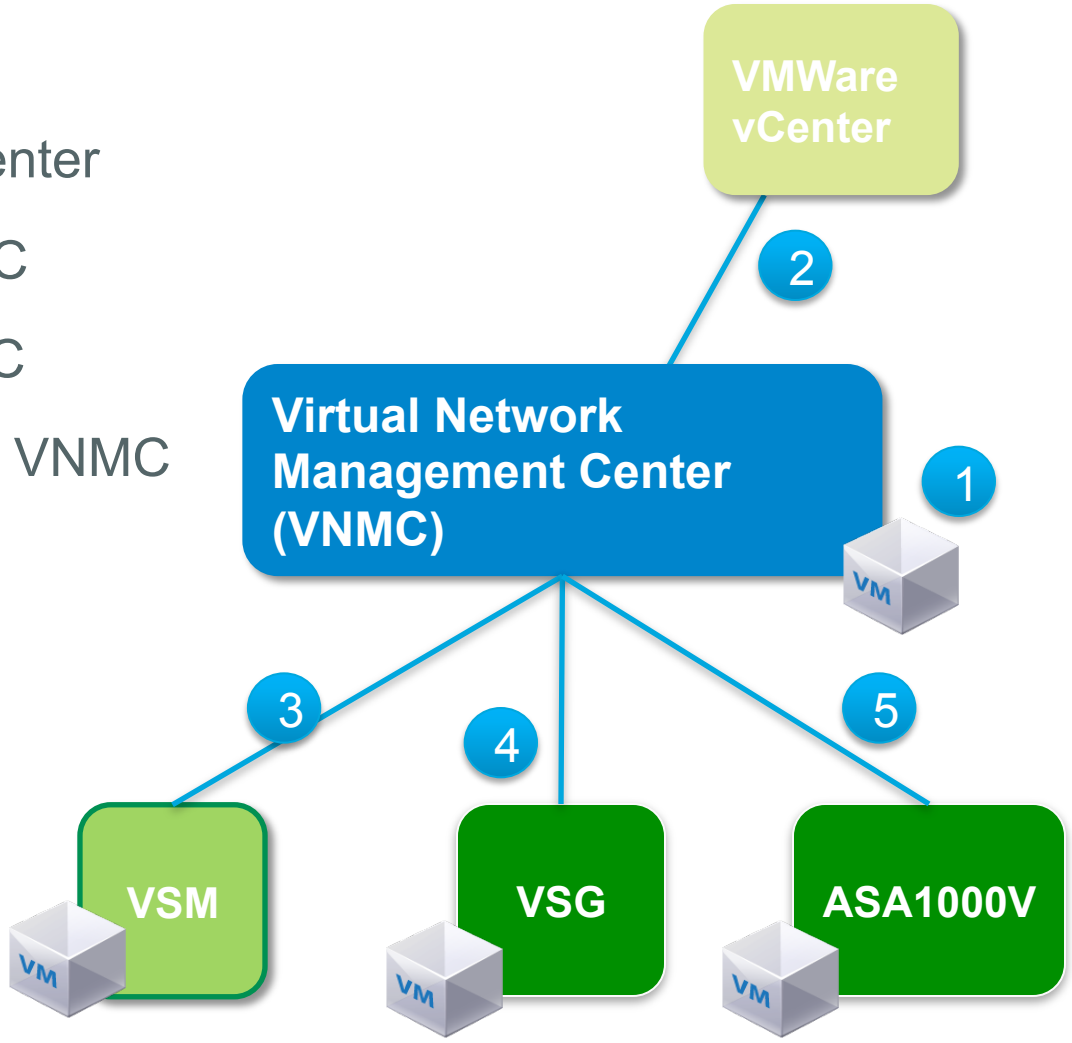
- Improved Scale
  - **128 Hosts**
  - **300 ports per host**
  - **4000+ ports per VSM**
- Evolution of VXLAN
  - **VXLAN Unicast Mode**
  - **Multicast-less mode**
  - **No flood and learn**
  - **Mac-distribution**
- VXLAN Gateway
  - **Available in Advanced Edition**
- Enhanced upgrade process

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

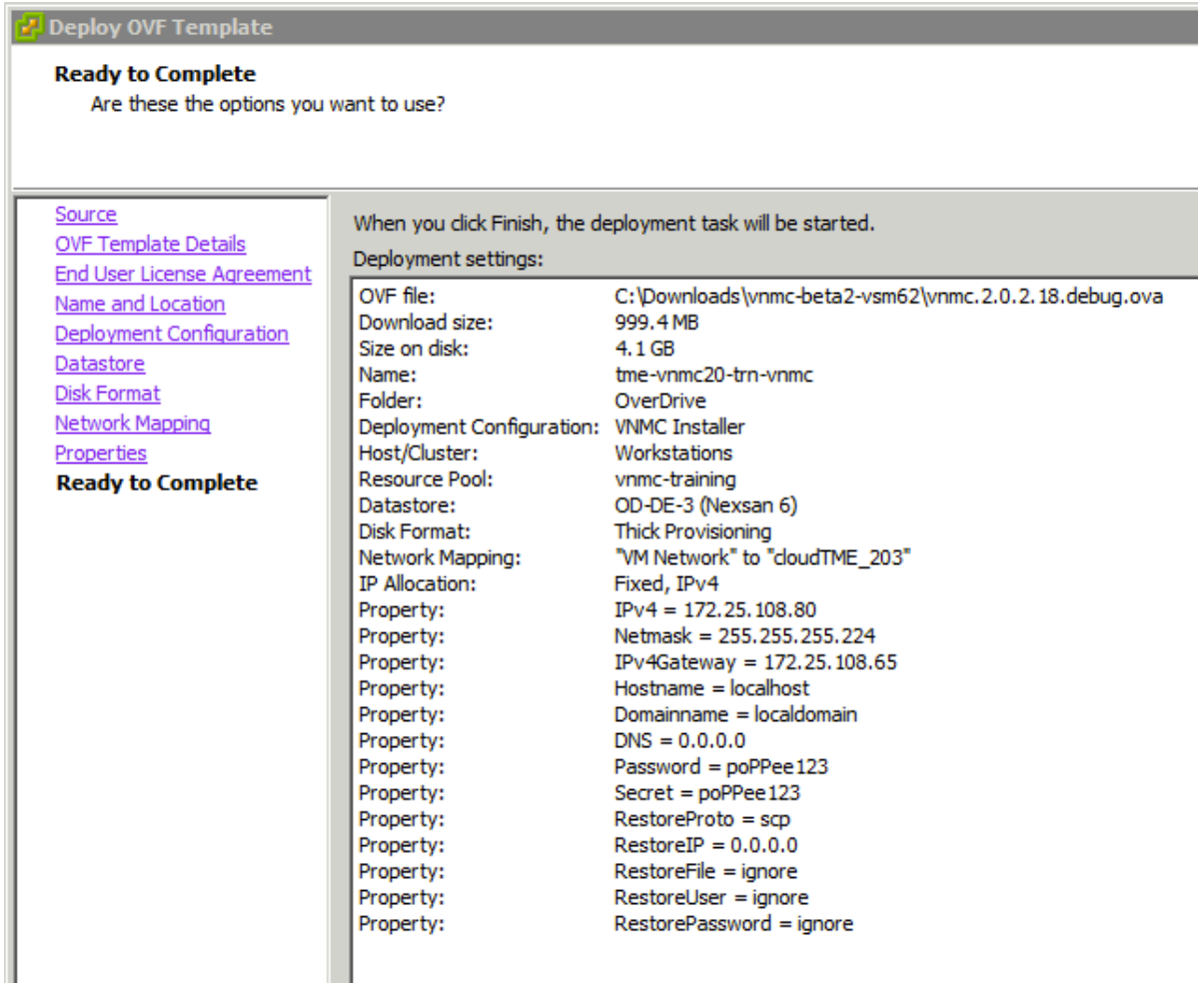


Deployment Step 1: VNMC Installation

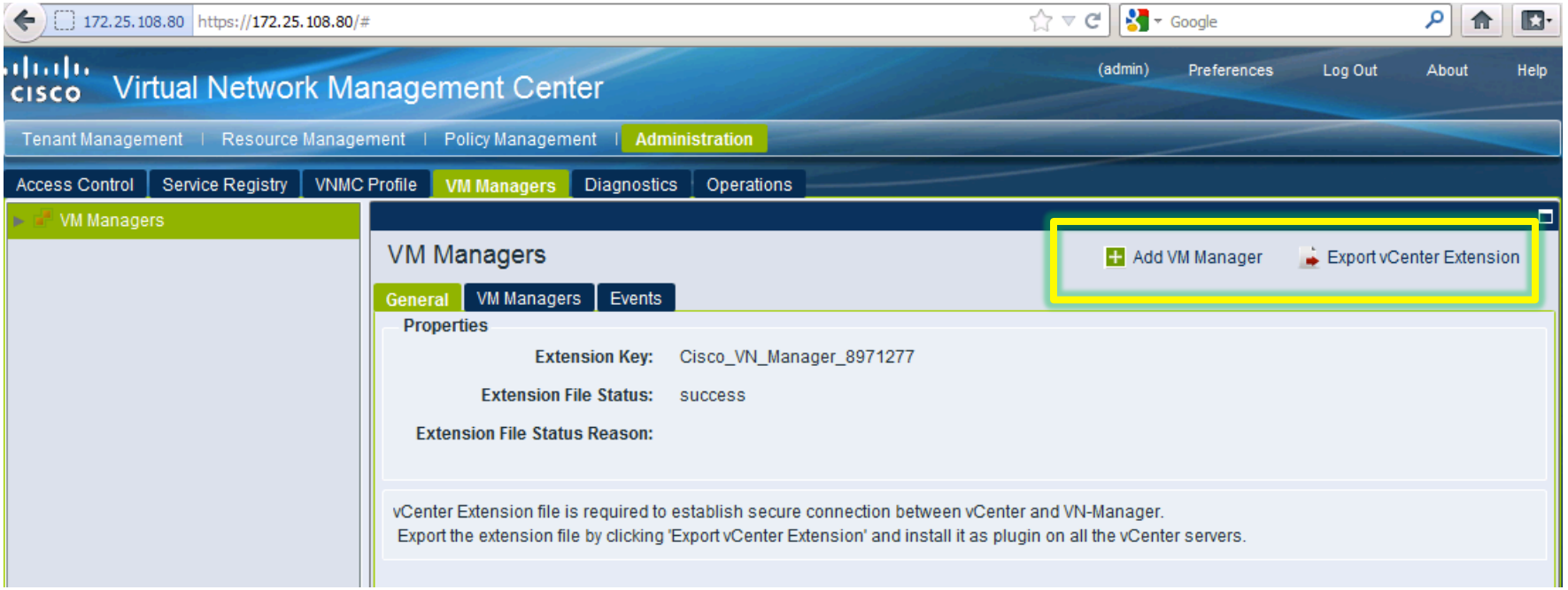
- Install VNMC as a Virtual Appliance in vCenter using OVA or ISO image
- Power on the VNMC virtual appliance after the OVA is deployed
- Access VNMC WebUI using: *"https://<Fully qualified VNMC hostname or IP Address"*

  Username – "admin"

  Password – whatever set during installation



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

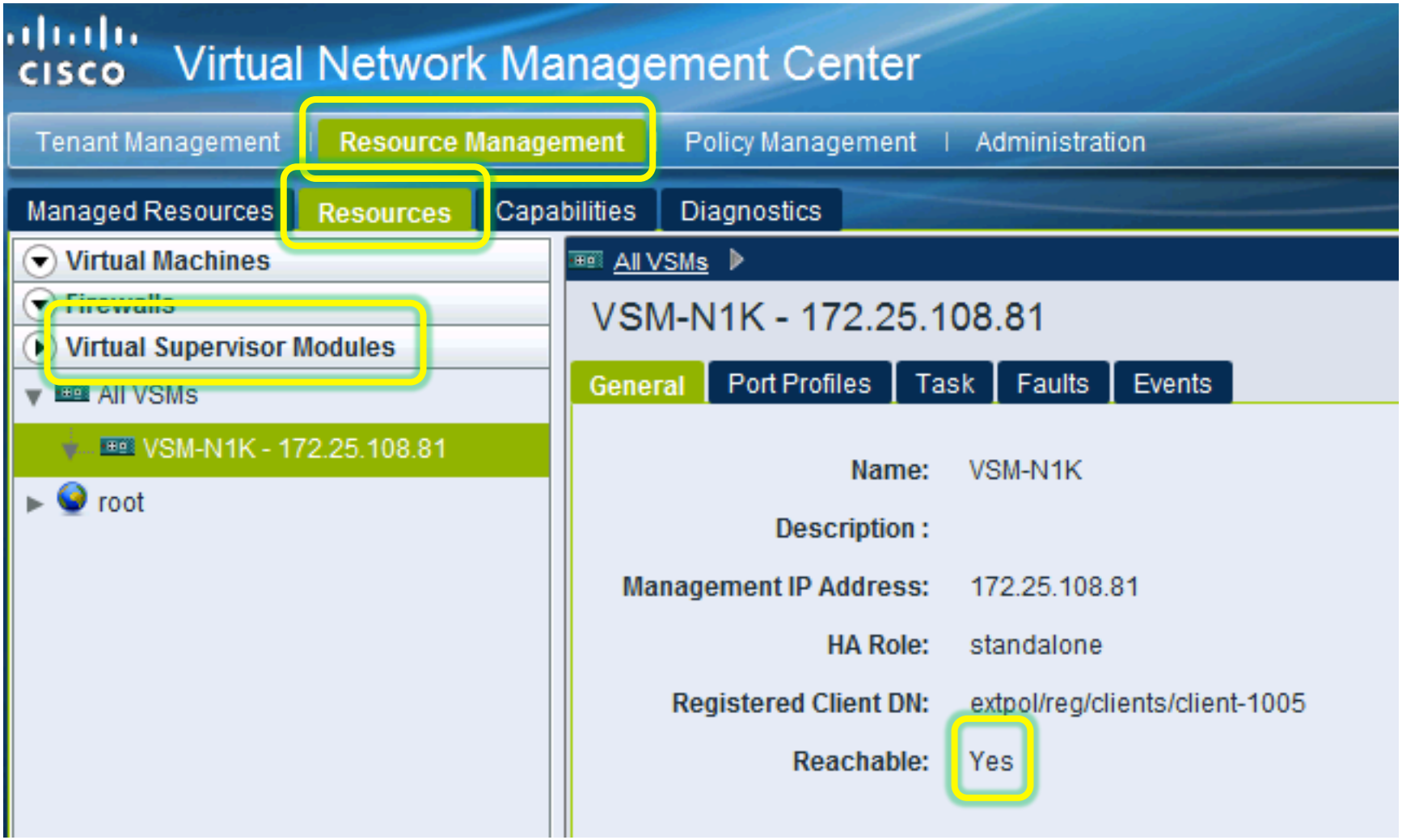
Deployment Step 3: Connect VSM to VNMC
Setup Policy Agent in VSM

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

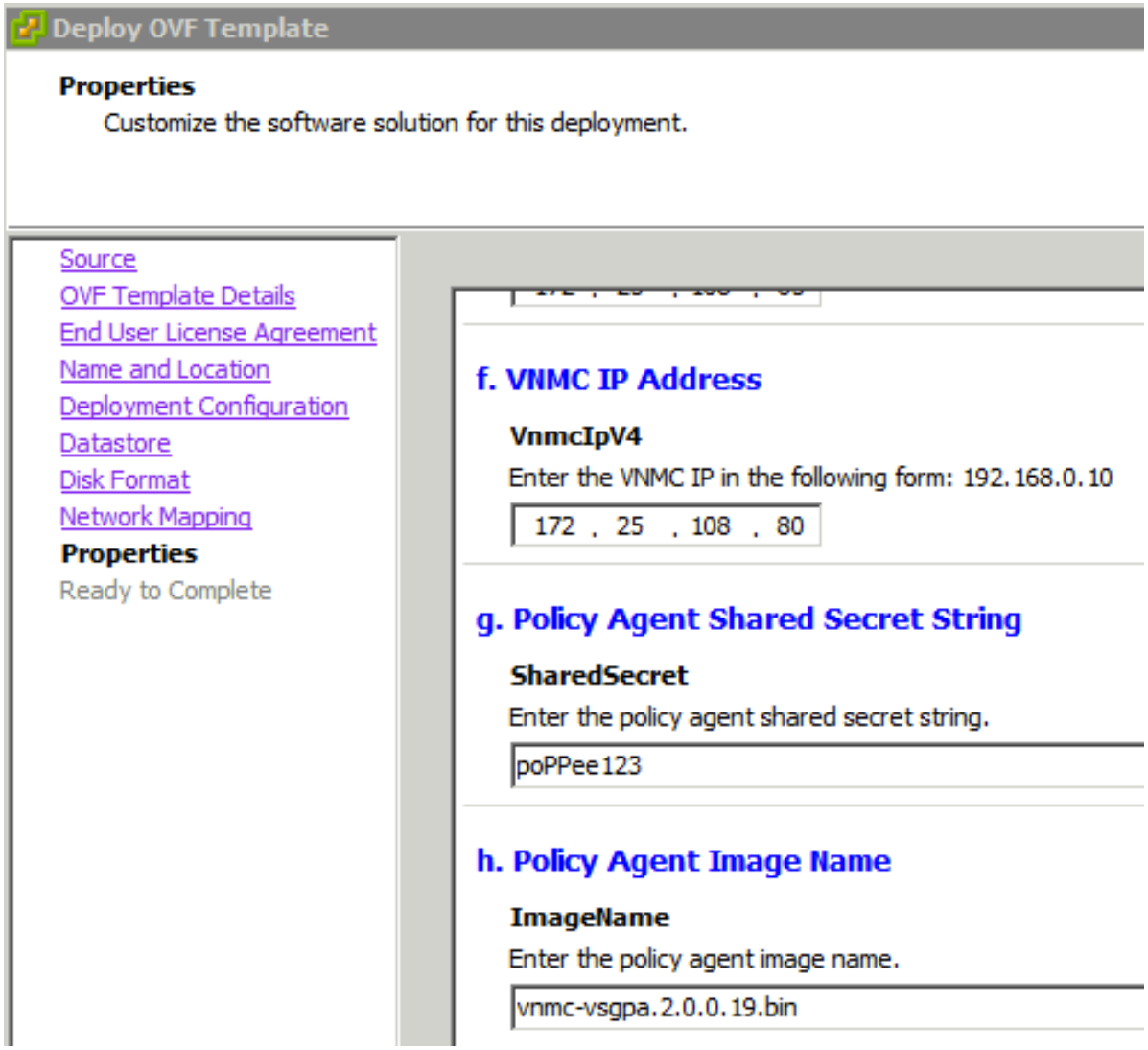
```
VSM-N1K(config)#
VSM-N1K(config)#
VSM-N1K(config)# vnm-policy-agent
VSM-N1K(config-vnm-policy-agent)# registration-ip 172.25.108.80
VSM-N1K(config-vnm-policy-agent)# shared-secret poPPee123
VSM-N1K(config-vnm-policy-agent)# policy-agent-image vnmc-vsmpa.2.0.0.19.bin
VSM-N1K(config-vnm-policy-agent)#
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



Deployment Step 4: Connect VSG to VNMC



- 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


```
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 poPPee123
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)#
```

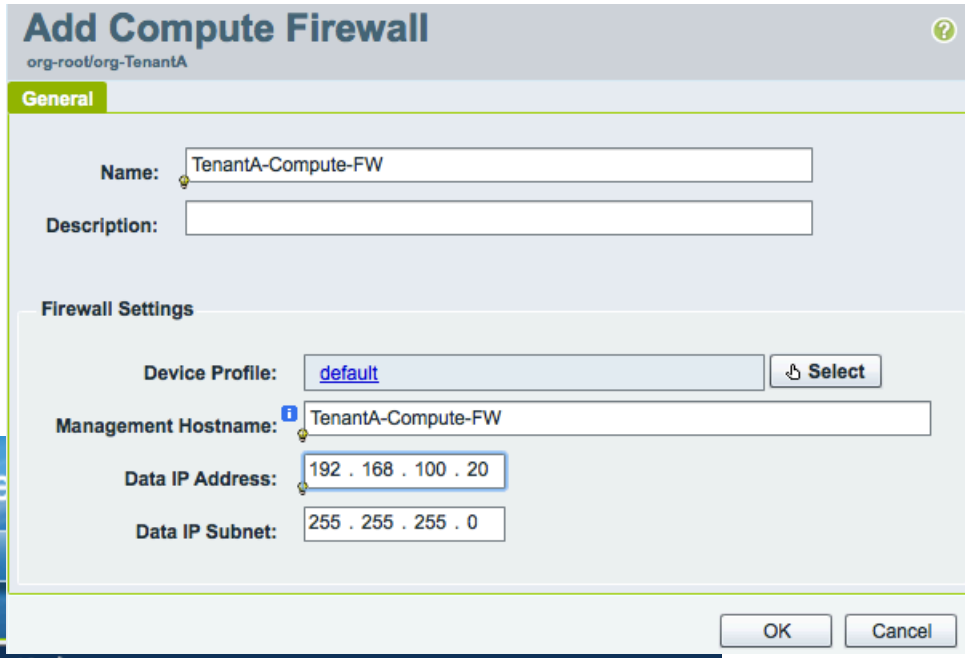
Deployment Step 5: Connect ASA 1000V to VNMC (contd.)

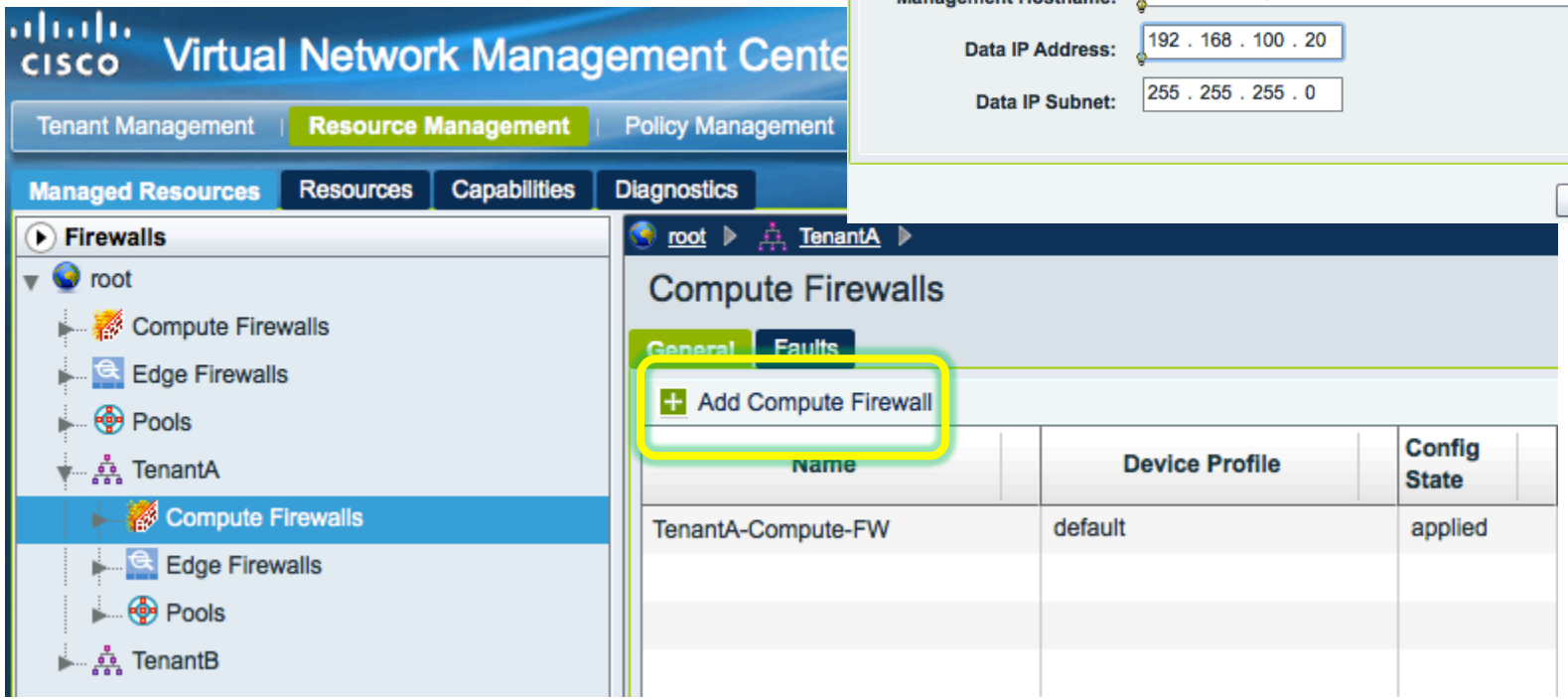
- Verify ASA1000V registered with VNMC

VSG (Compute Firewall) Use Case

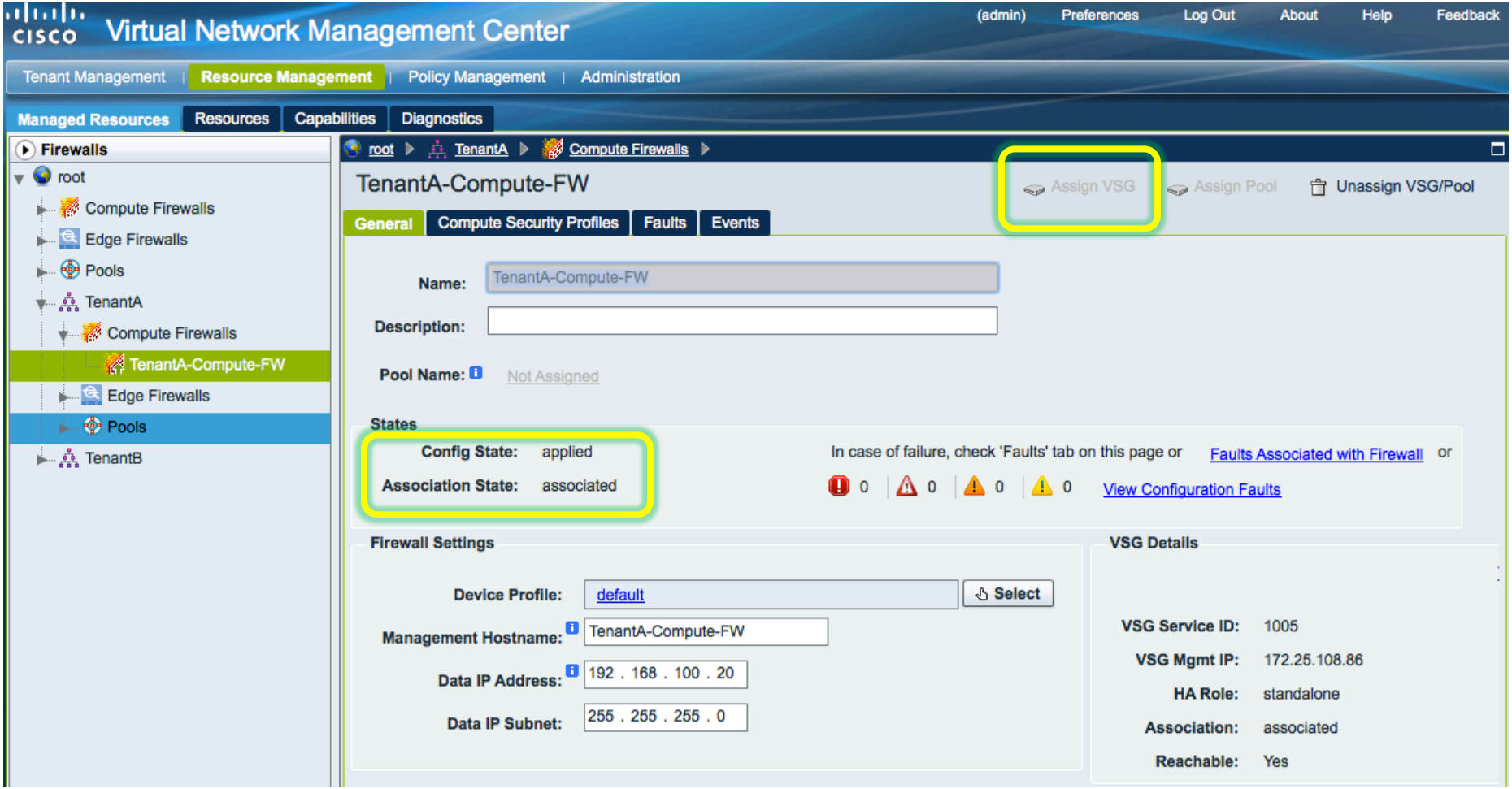
Compute Firewall Creation

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

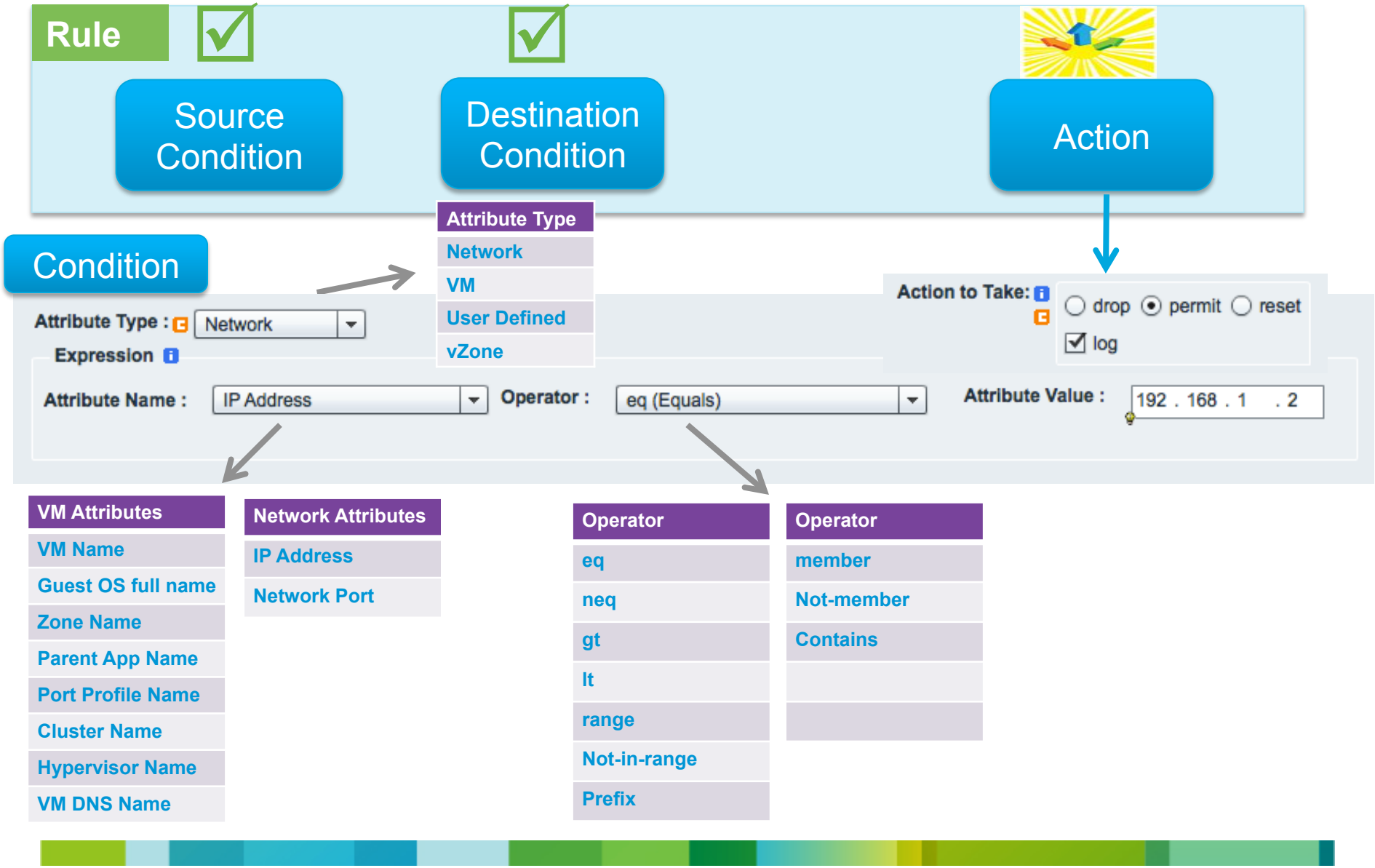




Assign VSG to Compute Firewall

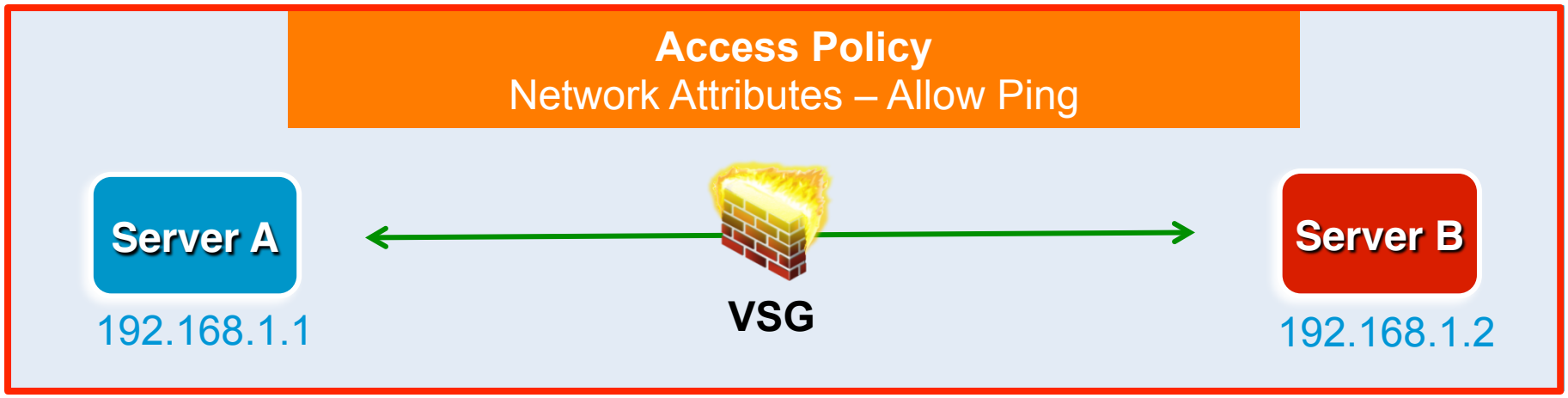


Compute Firewall Policy: Rule Construct



Compute Firewall – Use Case 1a

Access Policy based on Network Attributes



Rule Table

Add Rule | Edit | Delete

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

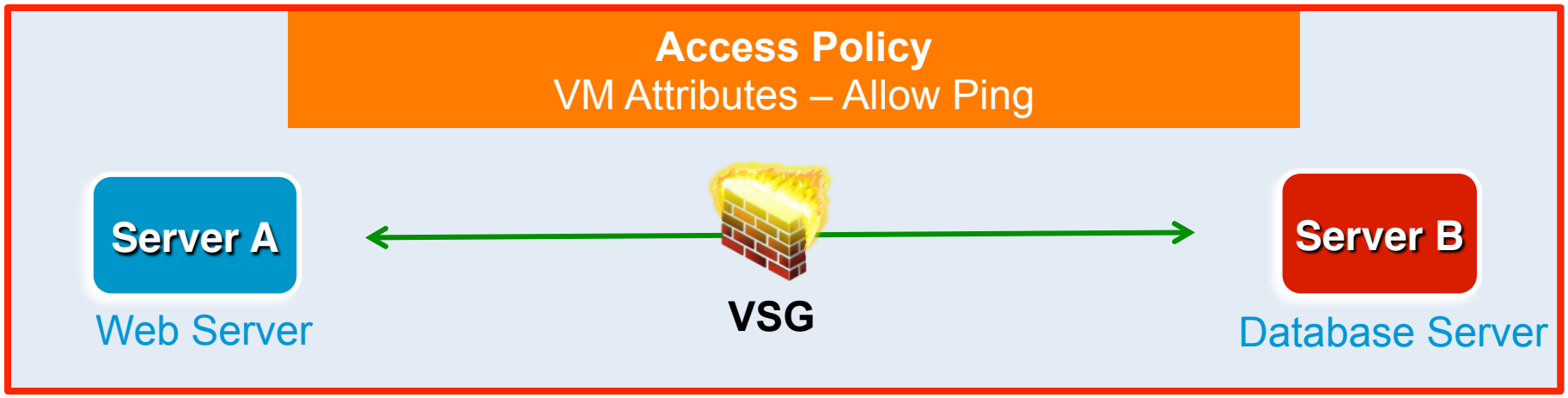
Source Condition

Destination Condition

Action

Compute Firewall – Use Case 1b

Access Policy based on VM Attributes



Rule Table

Add Rule | Edit | Delete

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

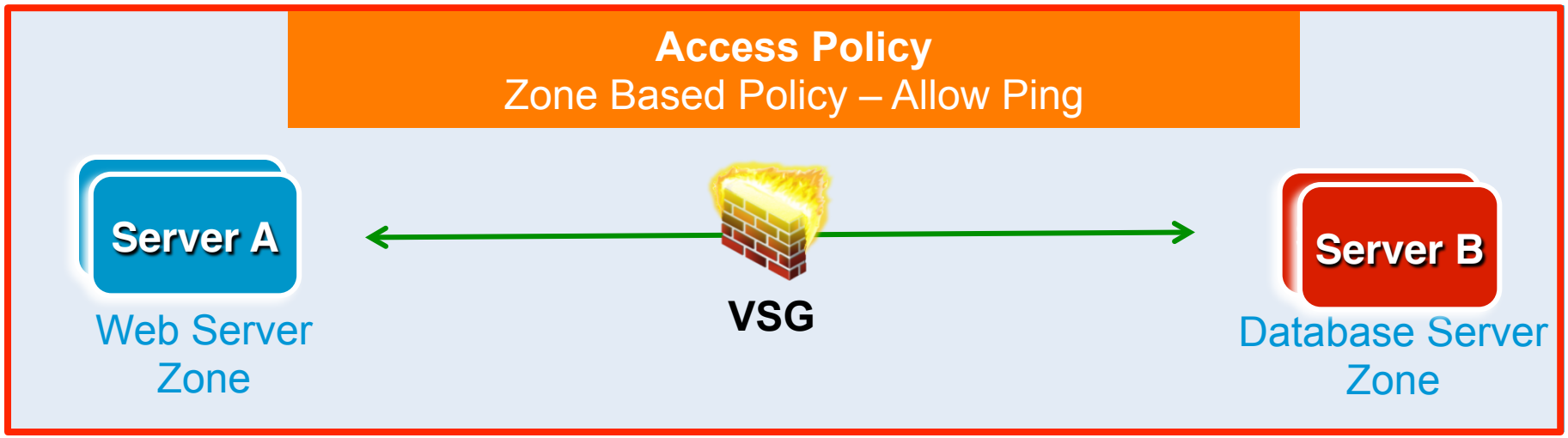
Action

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

Compute Firewall – Use Case 1b

Access Policy based on Zones (contd.)



Rule Table

Add Rule | Edit | Delete | Records: 1

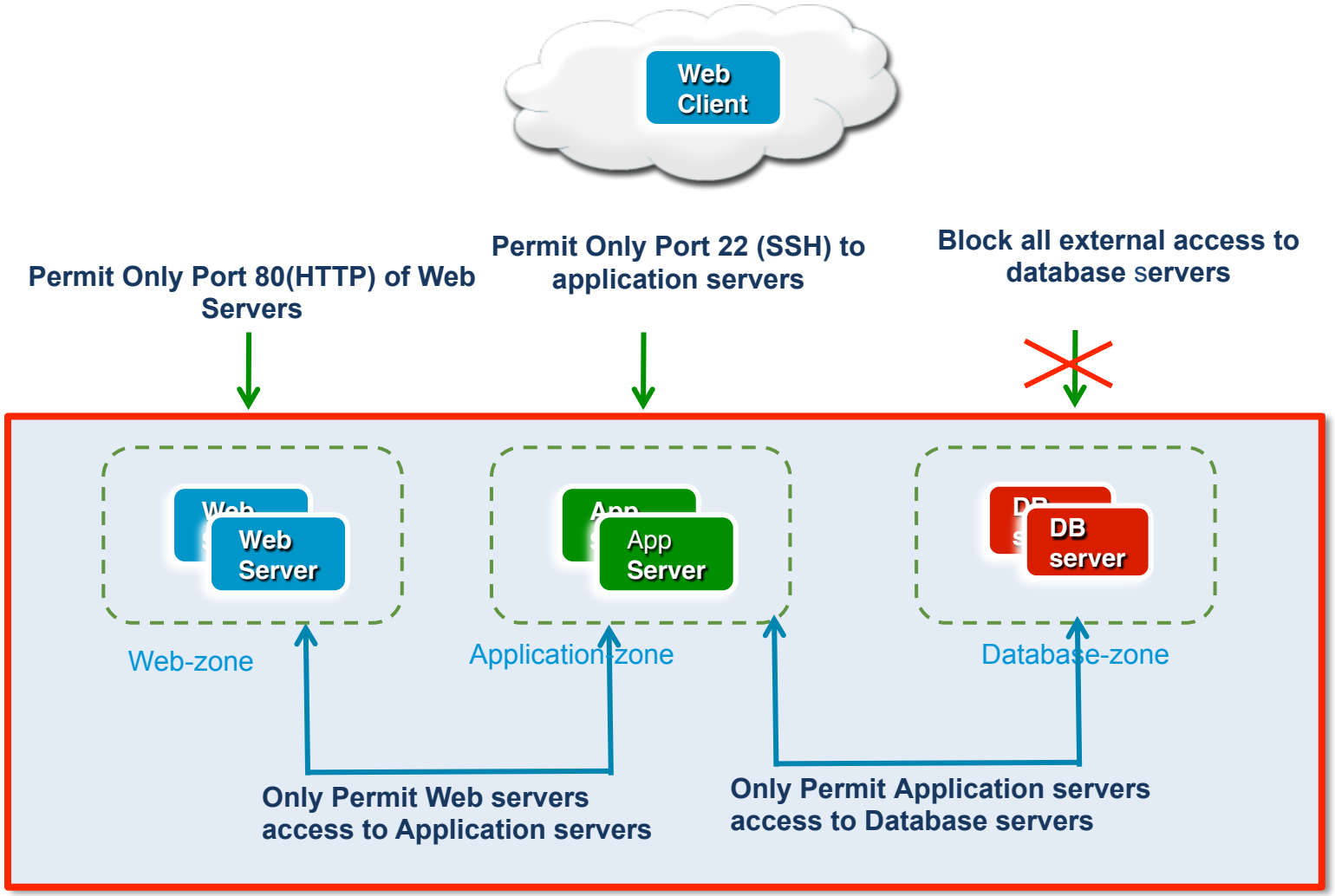
Name	Source Condition	Destination Condition	Protocol	EtherType	Action
Allow_ICMP	vZone Name eq WebZone	vZone Name eq DBZone	eq ICMP	Any	Permit, Log

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
```

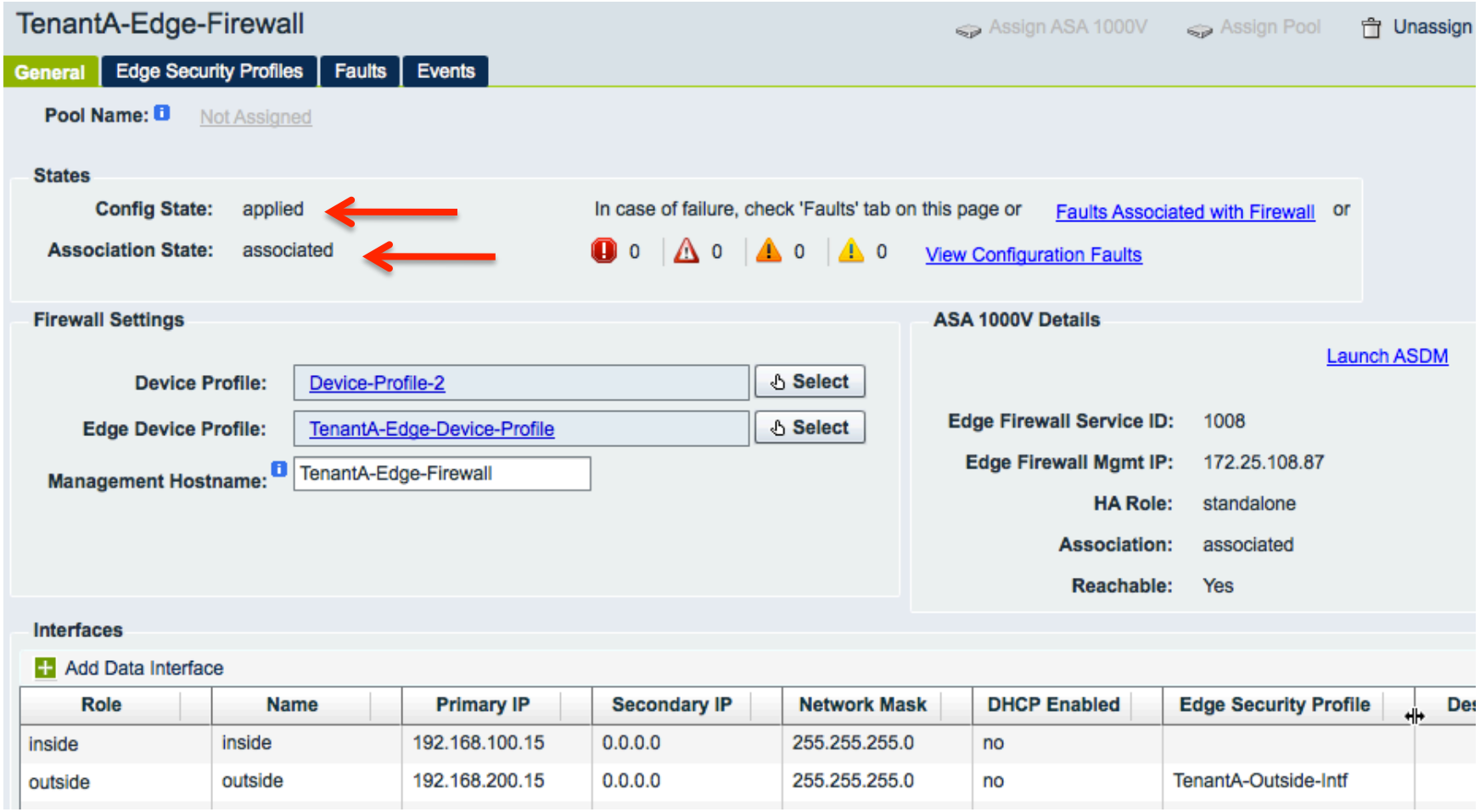
- Enable the Service Chain on Port-Profile using Nexus 1000V VSM

```
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
```

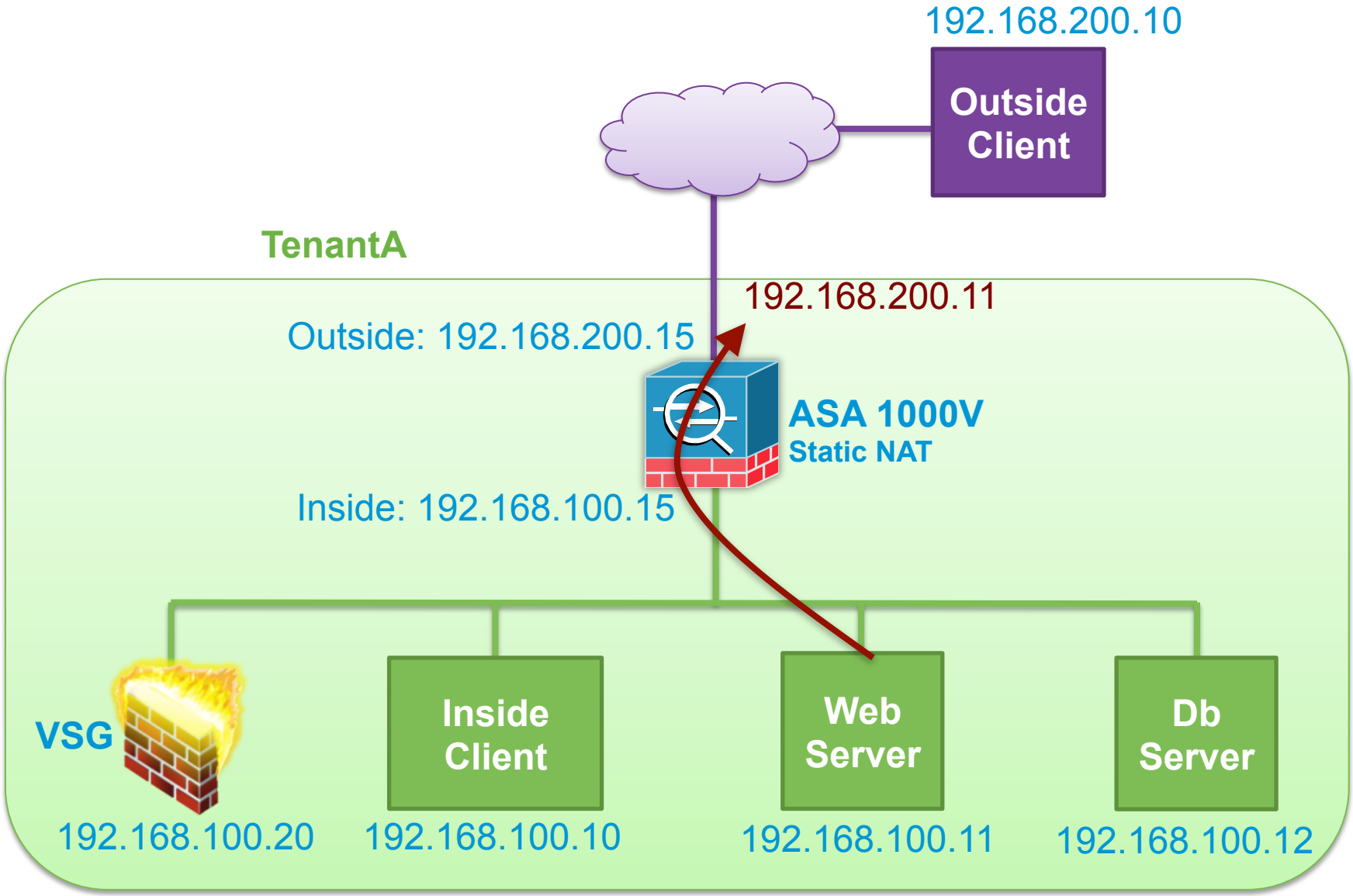
ASA 1000V (Edge Firewall) Use Case

Edge Firewall – ASA 1000V

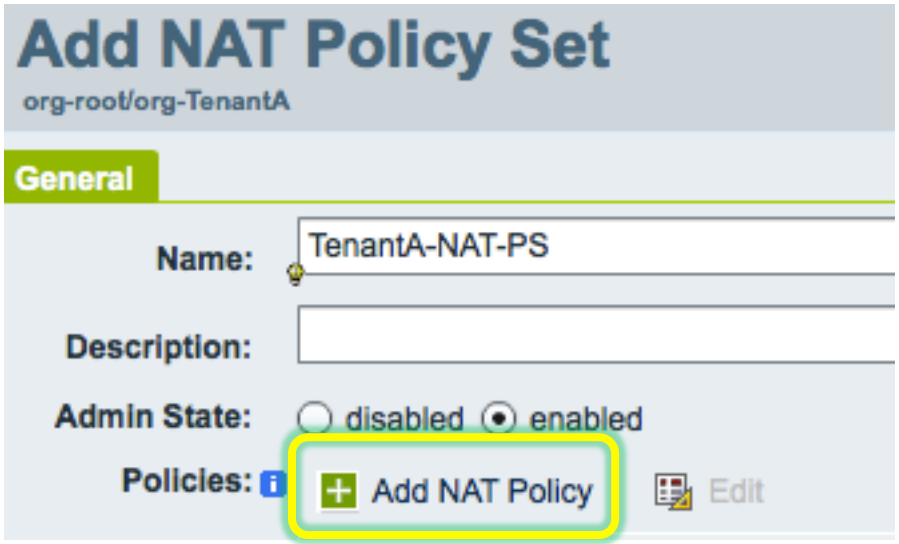
- Cisco ASA 1000V Edge Firewall complements Cisco VSG to provide multitenant edge security and default gateway functionality, and protects against network-based attacks.

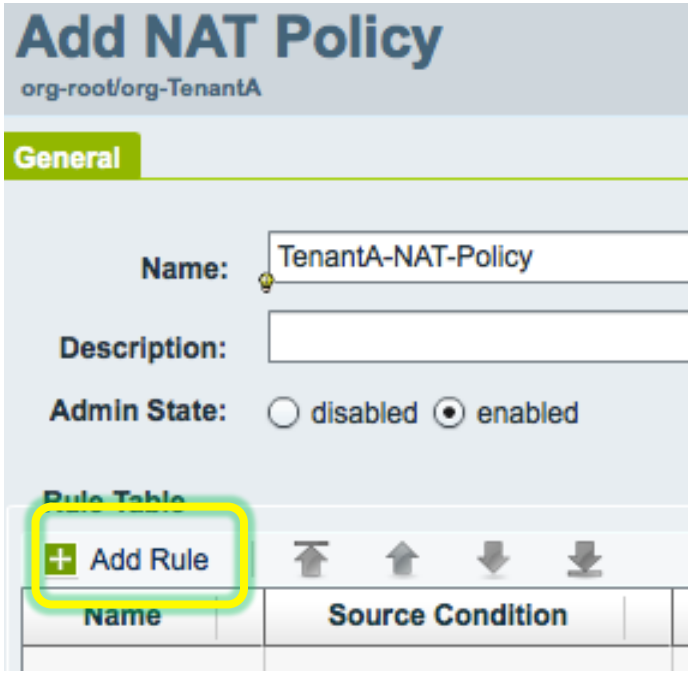


Edge Firewall – Static NAT Use Case

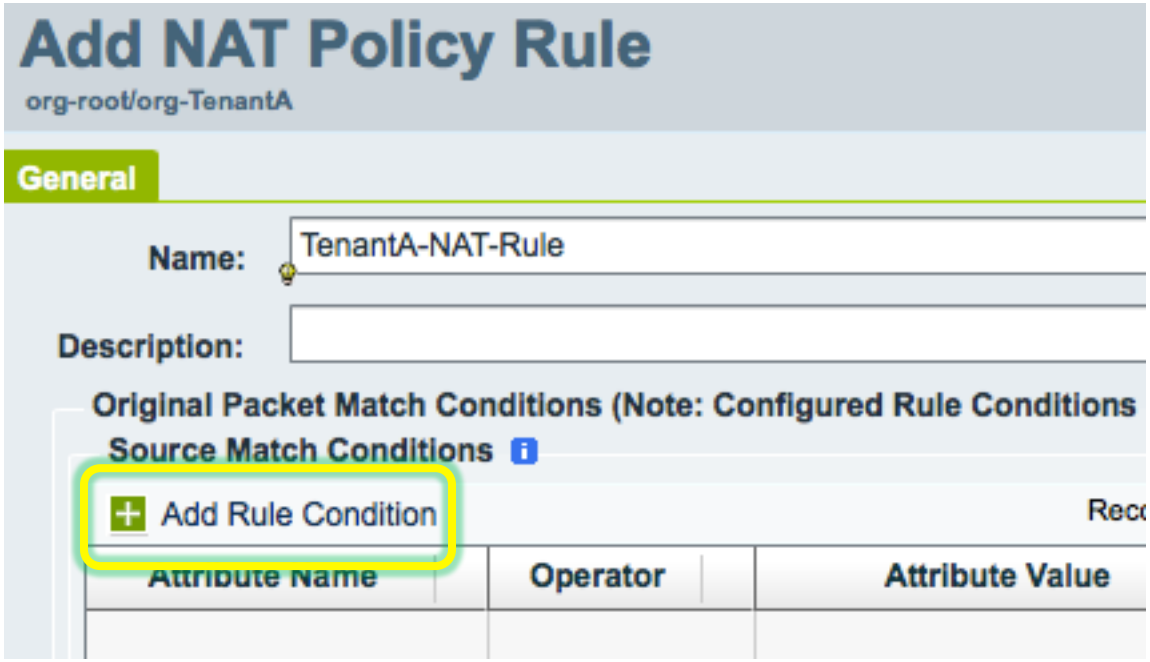


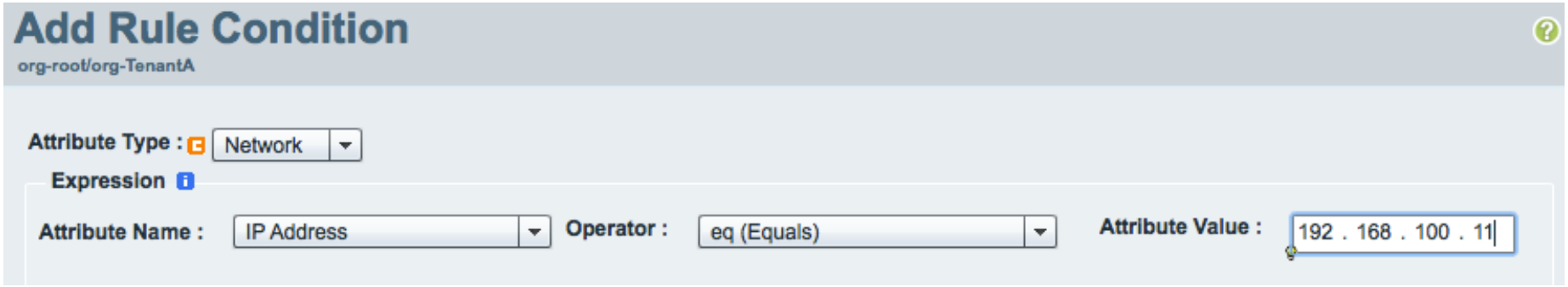
Edge Security Profile – Static NAT



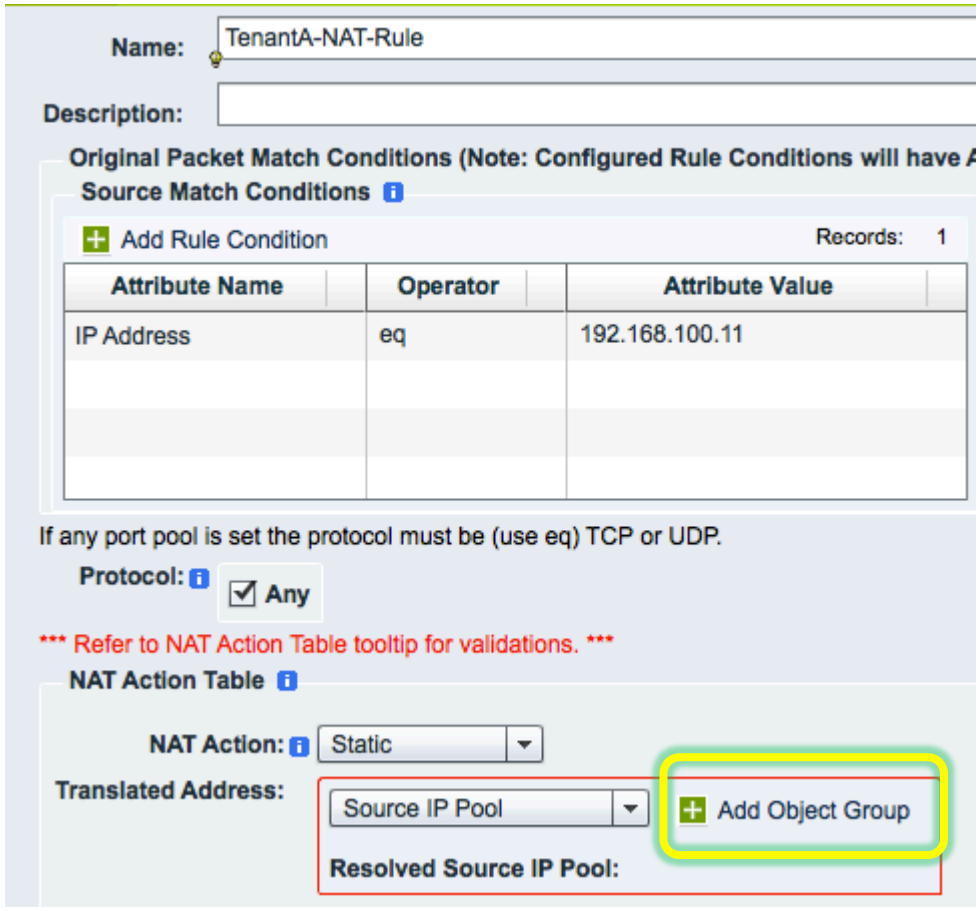


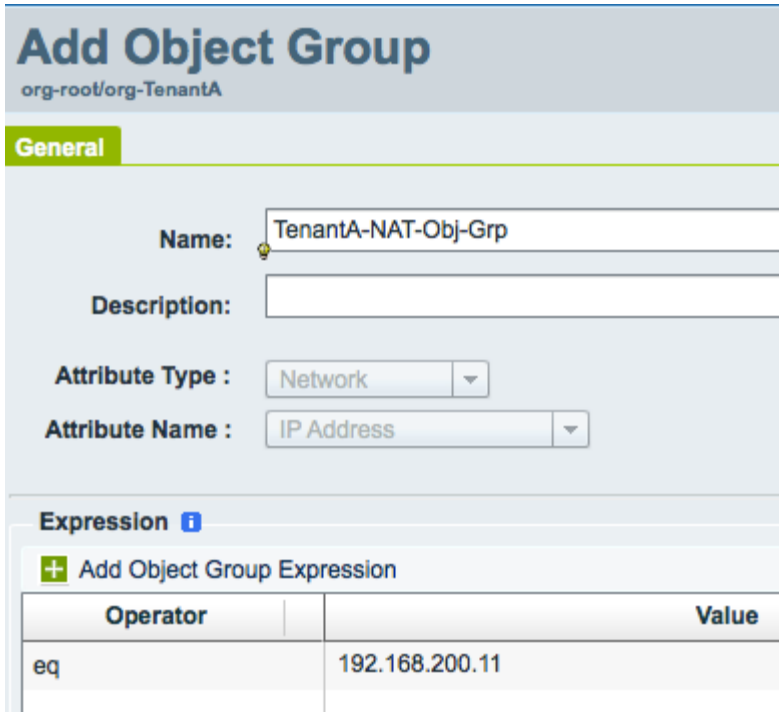
Edge Security Profile – Static NAT (2)



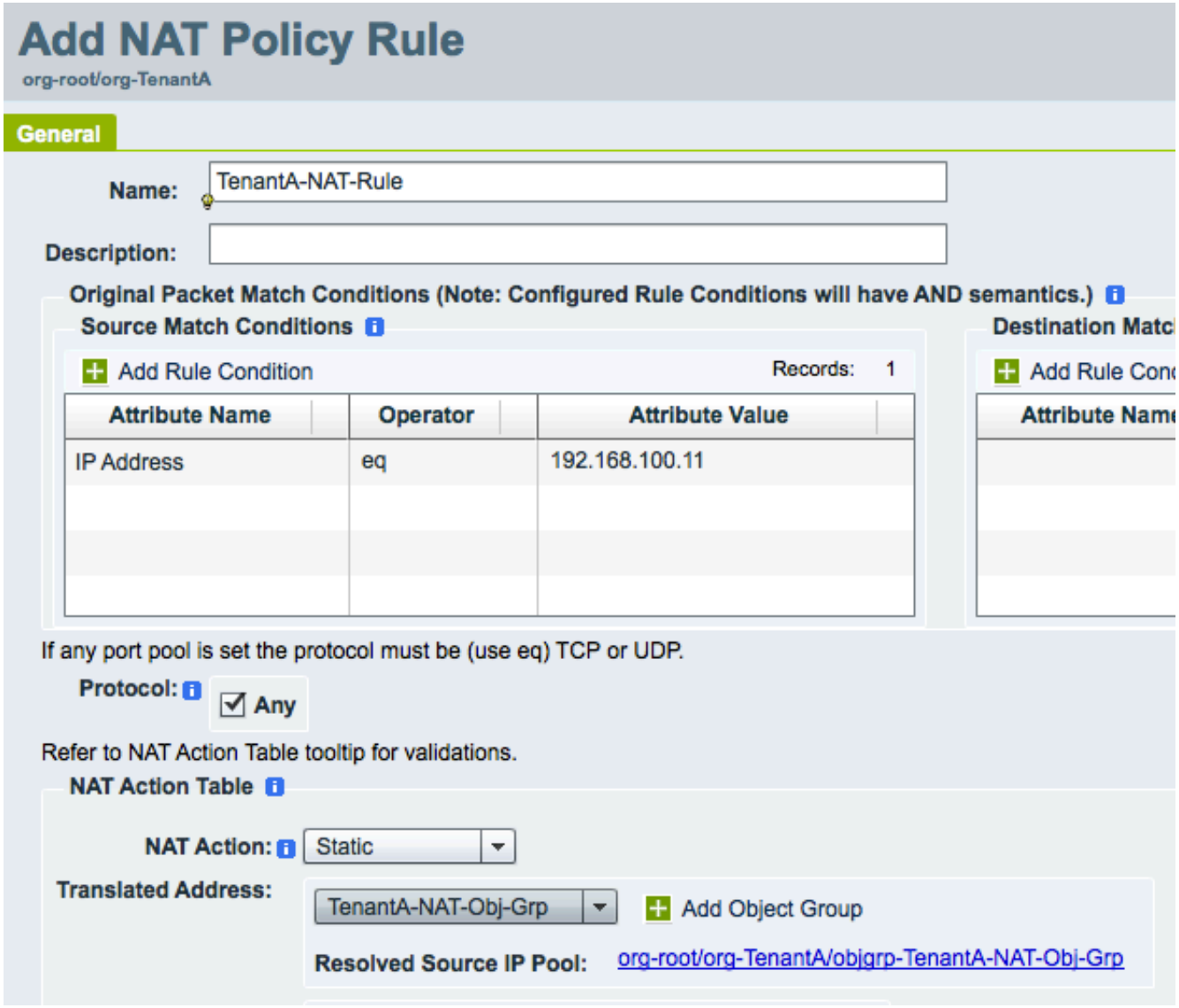


Edge Security Profile – Static NAT (3)

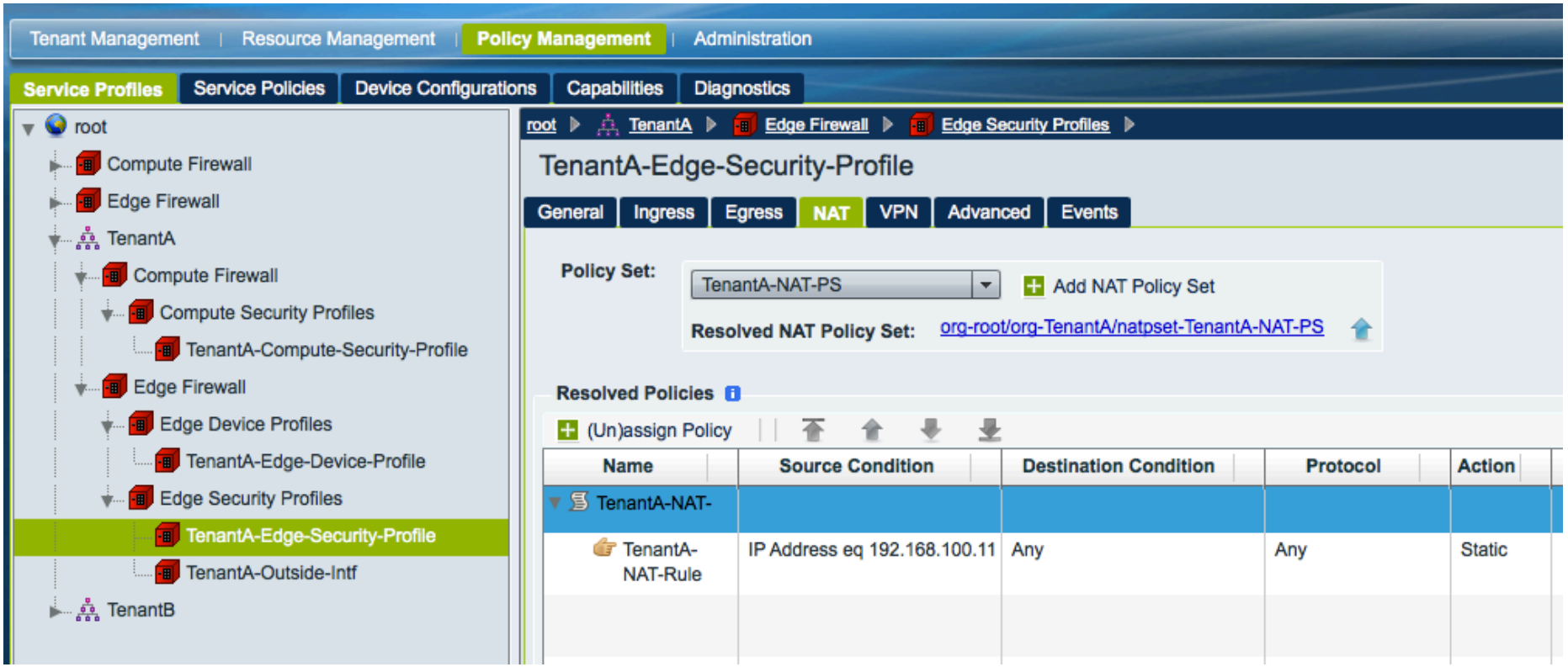




Edge Security Profile – Static NAT (4)



Edge Security Profile– Static NAT (5)



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 VSMPA 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, ohodnoťte tuto přednášku.

Děkujeme za pozornost.