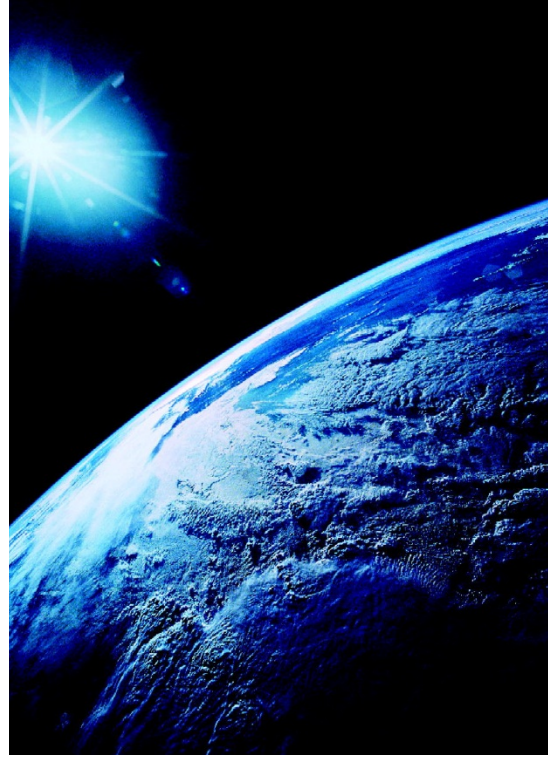
Cisco Connect

Praha, hotel Clarion
10. – 11. dubna 2013

Bezpečnost ve virtualizovaném DC

SEC4 / L2

Tomáš Michaeli - Cisco
Speaker -



© 2013 Cisco and/or its affiliates. All rights reserved.

DC Market

- Almost 65% of all datacenter workloads are virtualized
- Computing model has changed
- IT Service model has changed
- IT organizations expected to change

Cisco

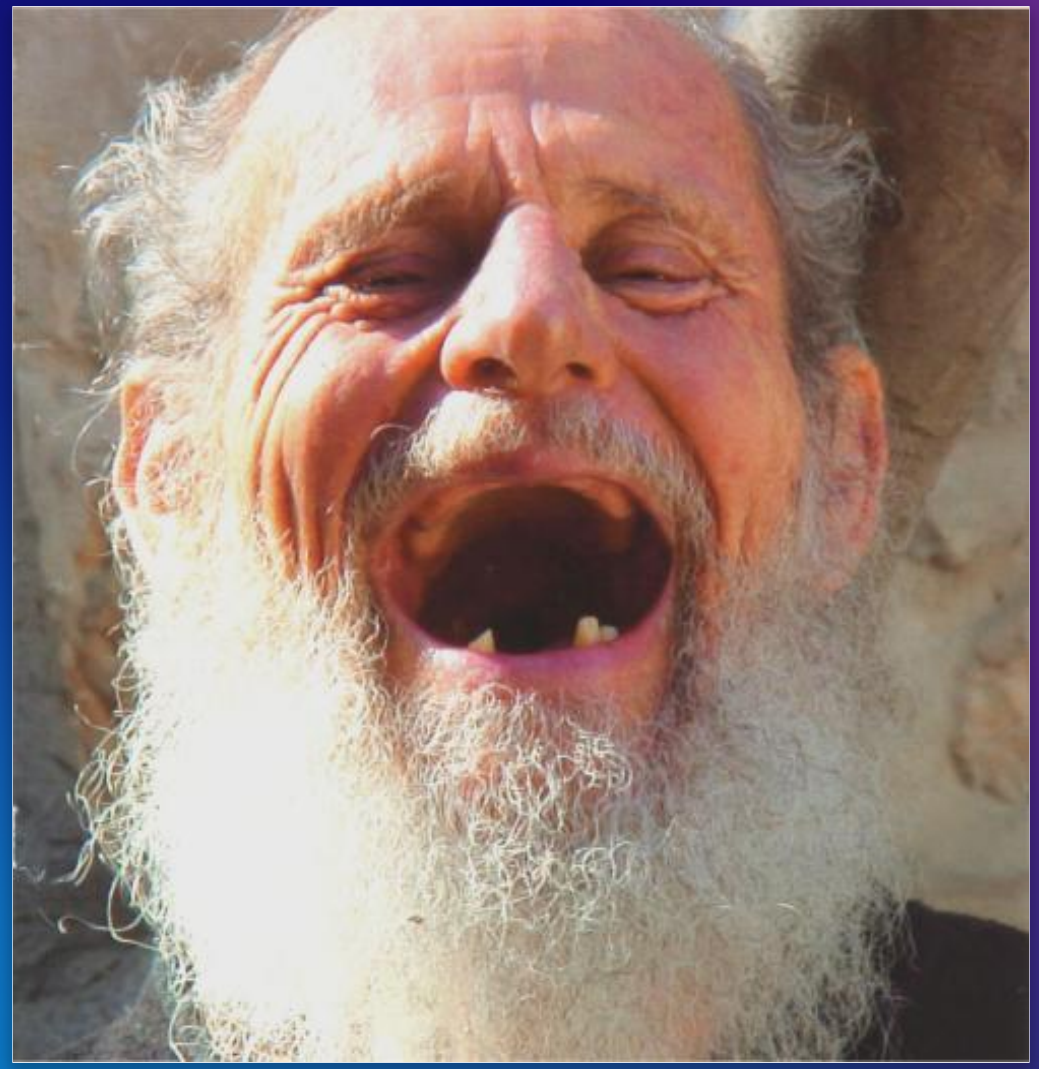
- Company extending direction from purely HW based appliance to SW based virtual service node
- Easy service integration in virtual environment
- Cloud, automation
- SDN arena

VMware, Microsoft, Citrix, RedHat, Oracle

- VMware announced NXS
- Windows 2012 released
- Hypervisor market transforms to cloud market
- Competitors in one space, friends in other
- Cisco now partnering with Citrix

Data Center, Services, & Virtualization: It's so easy!

Just ask this 35 year old Administrator.

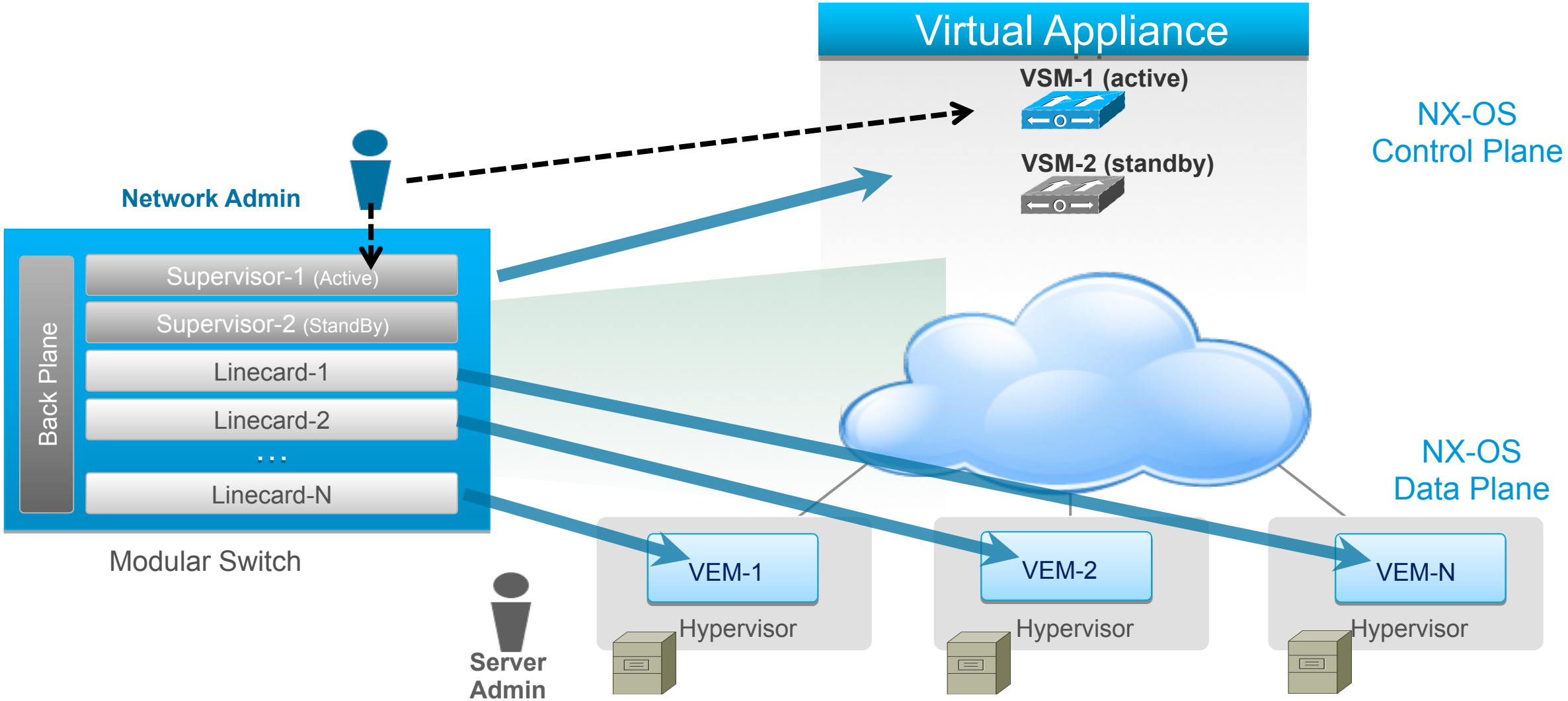


© 2011 Cisco and/or its affiliates. All rights reserved.

Agenda

- Architecture for virtualized services
- Understanding vPath
- Virtual Security Gateway overview
- Virtual ASA 1000V role in overall architecture
- Virtual Network Management Center overview
- VXLAN extend your cloud
- Summary
- Resources

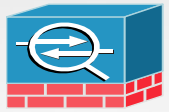
Network team manages virtual & physical networks



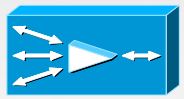
Virtual Services Portfolio

Virtual Appliance

ASA



vWAAS



VSG

CRS

VSM: Virtual Supervisor Module

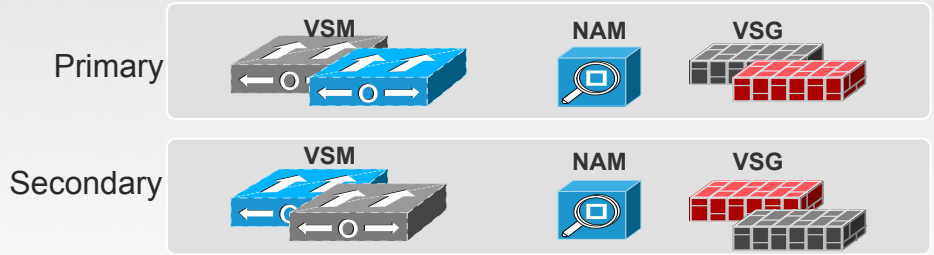
VSG: Virtual Security Gateway

CRS 1000V: Virtual Router

vWAAS: Virtual WAAS

ASA 1000V: Tenant-edge security

Nexus 1010 / 1010X



Virtual Blades

Virtual Supervisor Module (VSM)

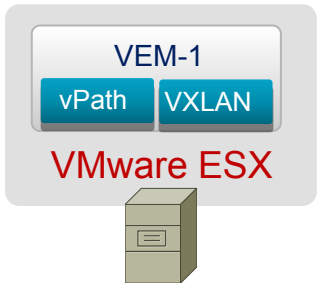
Network Analysis Module (NAM)

Virtual Security Gateway (VSG)

Data Center Network Manager (DCNM)

vPath

- Virtual service data-path



VXLAN

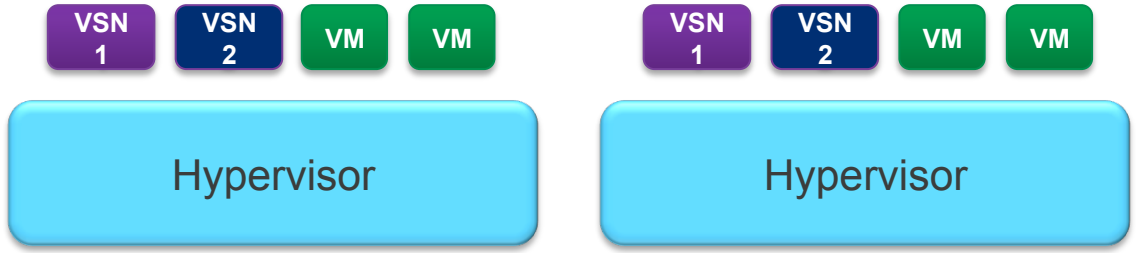
- Scalable Segmentation

Virtual Services Node

Stand-alone VSN

Can be deployed with any virtual switch

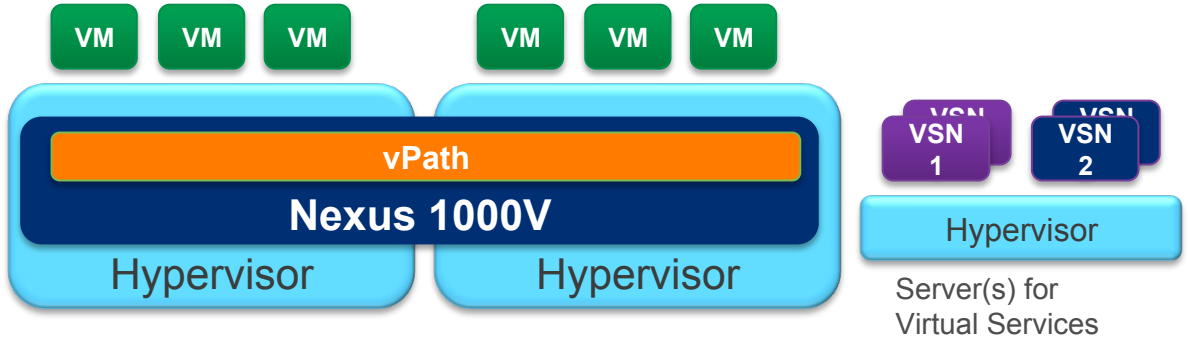
Example: vWAAS



N1KV vPath integrated VSN

Integrates with N1KV port profile and virtual service datapath (vPath)

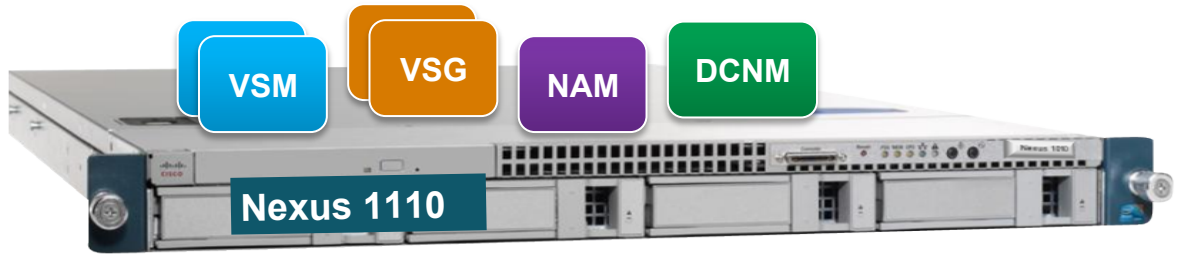
Example: vWAAS, VSG, ASA 1000V



VSN hosted on Nexus 1110 appliance

VSN can be stand-alone or vPath integrated

Example: VSG, NAM



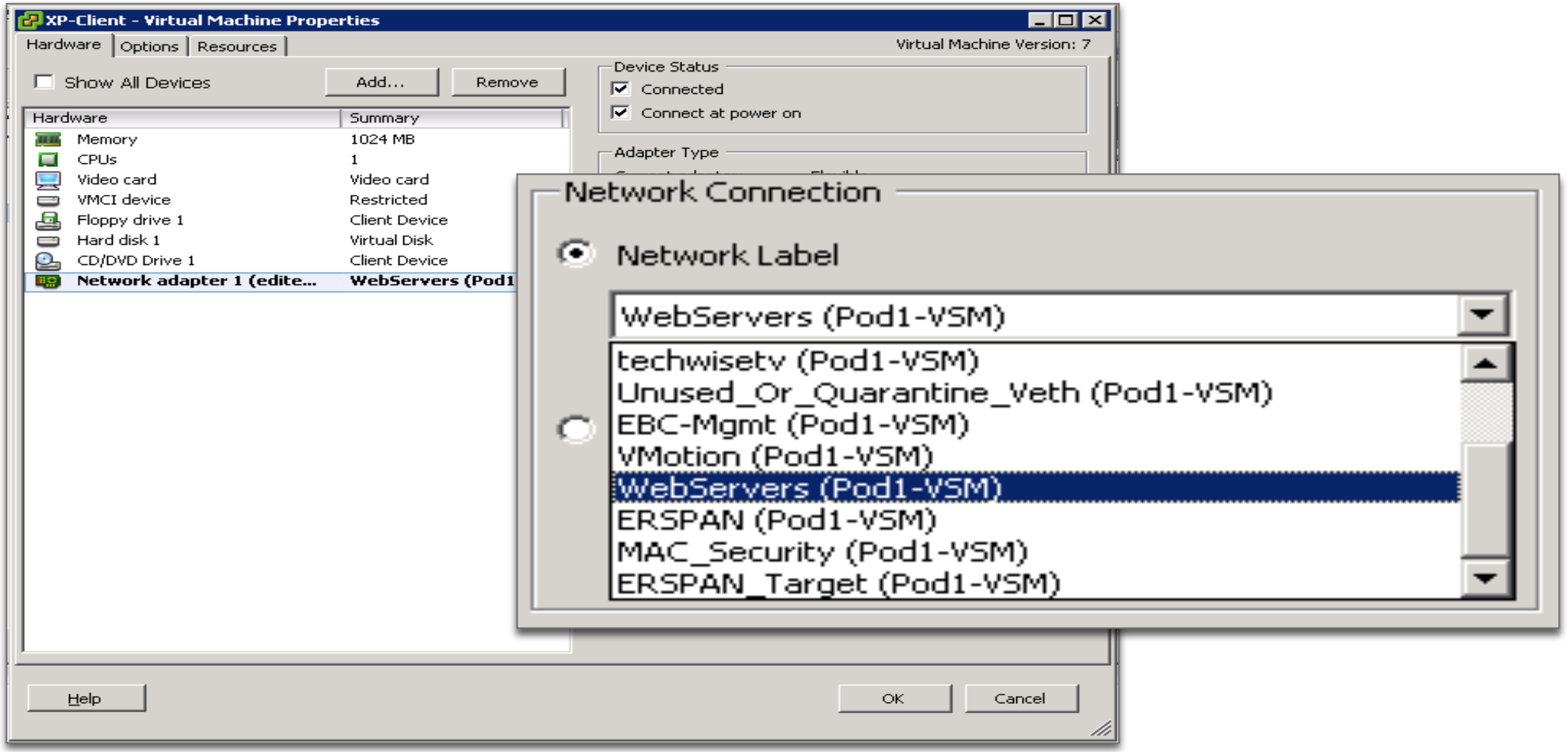
Network Admin - Port Profile Configuration

```
n1000v# show port-profile name WebServers
port-profile WebServers
  description:
  status: enabled
  capability uplink: no
  system vlans:
  port-group: WebServers
  config attributes:
    switchport mode access
    switchport access vlan 110
    no shutdown
  evaluated config attributes:
    switchport mode access
    switchport access vlan 110
    no shutdown
  assigned interfaces:
    Veth10
```

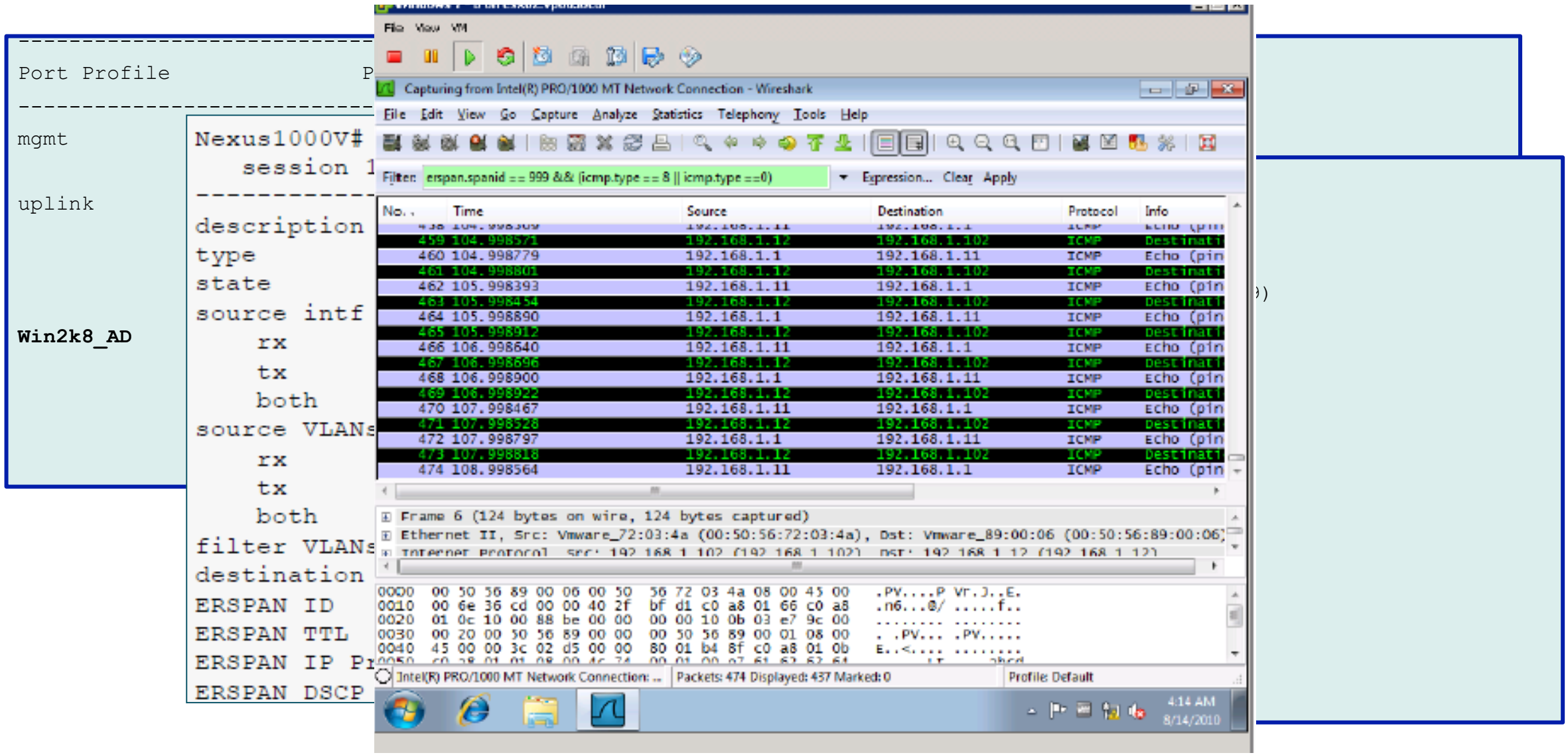
Support Commands Include:

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

Server Admin – Server configuration

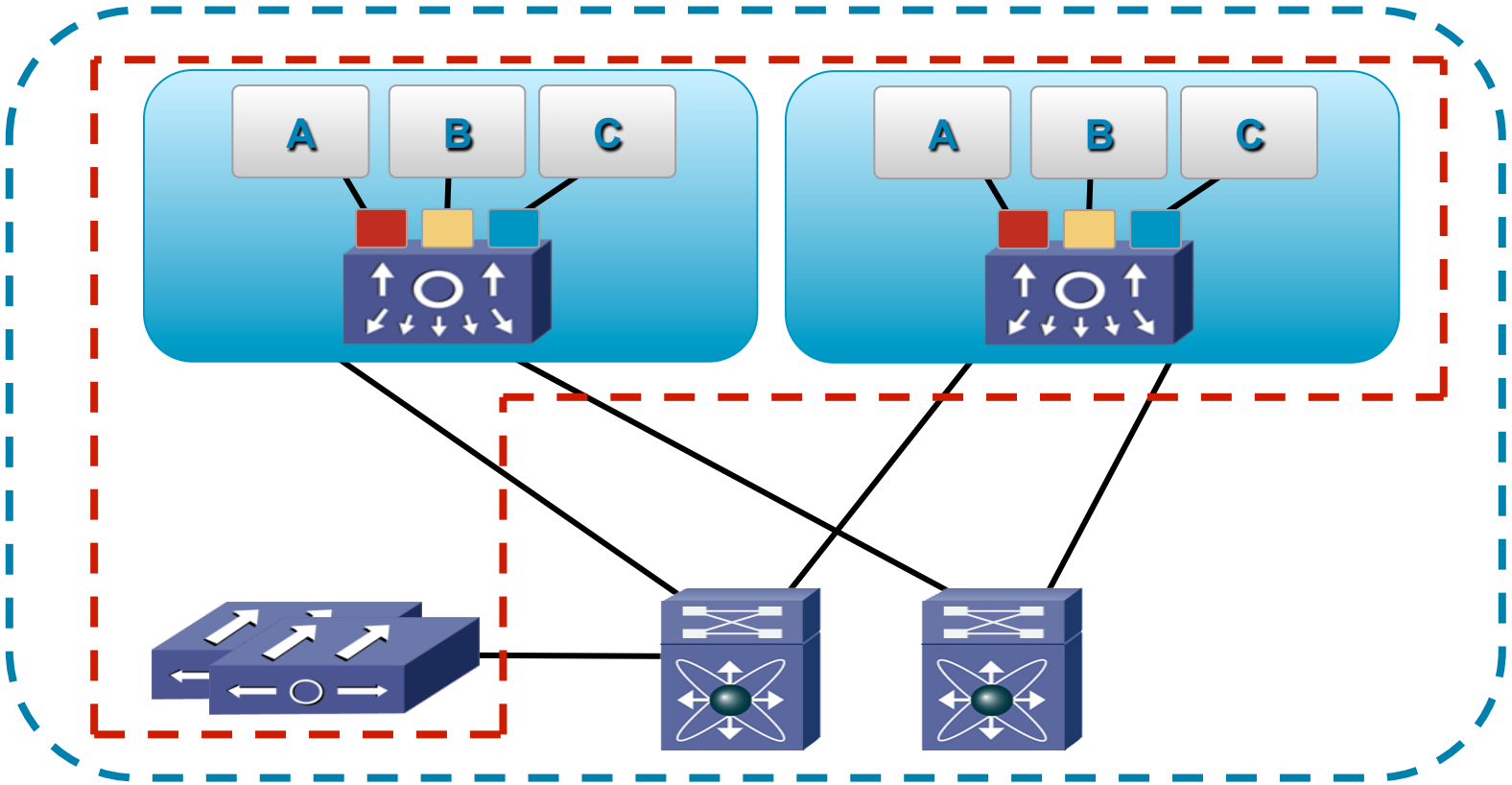


Traffic monitoring for security or t-shooting purposes



Private VLAN for basic segmentation

Two ways to do Private VLAN



Promiscuous Trunk

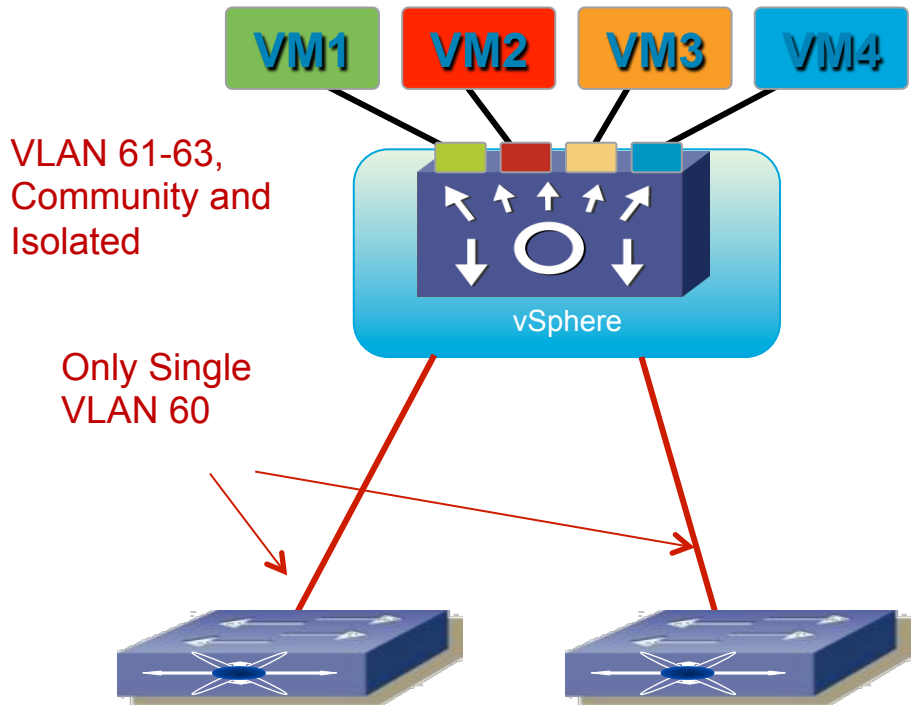
The Nexus 1000V do the mapping from secondary vlan to primary vlan

Trunk

The Nexus 1000V rely on the upstream switch to do the mapping from secondary to primary vlan

VMs isolation with PVLAN or MAC ACL

- VM's are Isolated or Community
- All VM's talk to Promiscuous devices
- Only Primary VLAN needed outside
- MAC filter default-gateway



With PVLAN

```
port-profile type ethernet UPLINK
  vmware port-group
  switchport mode private-vlan trunk promiscuous
  switchport private-vlan mapping trunk 60 61-63
  switchport private-vlan trunk allowed vlan 2-5, 60-63
  channel-group auto mode on mac-pinning
  no shutdown
  system vlan 2-5
  state enabled
```

With MAC ACL

```
port-profile type vethernet access6
  mac port access-group JustExternalHost in

mac access-list JustExternalHost
  10 permit any 0022.1991.7e08 0000.0000.0000
  20 deny any any
```

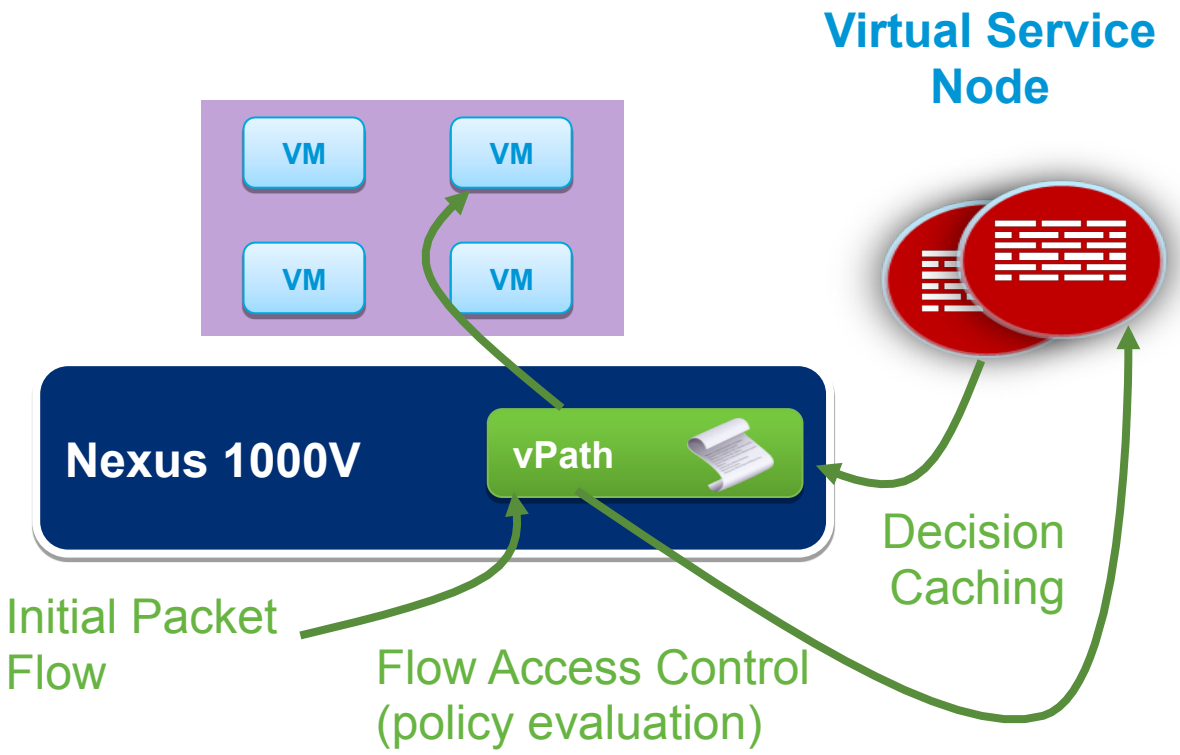
Understanding vPath and VXLAN

© 2011 Cisco and/or its affiliates. All rights reserved.

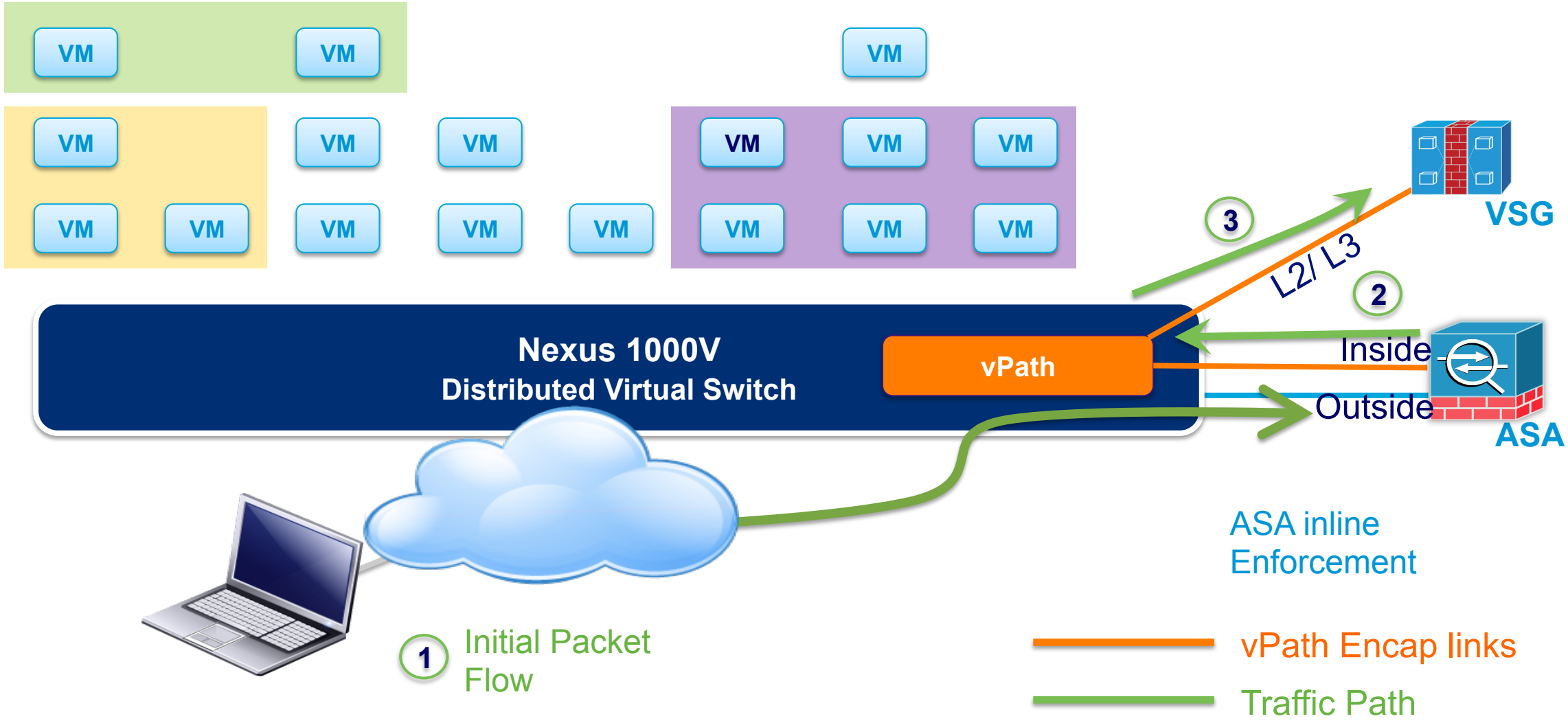
Virtualized Network Services – vPath

vPath 2.0 is now a part of N1kV

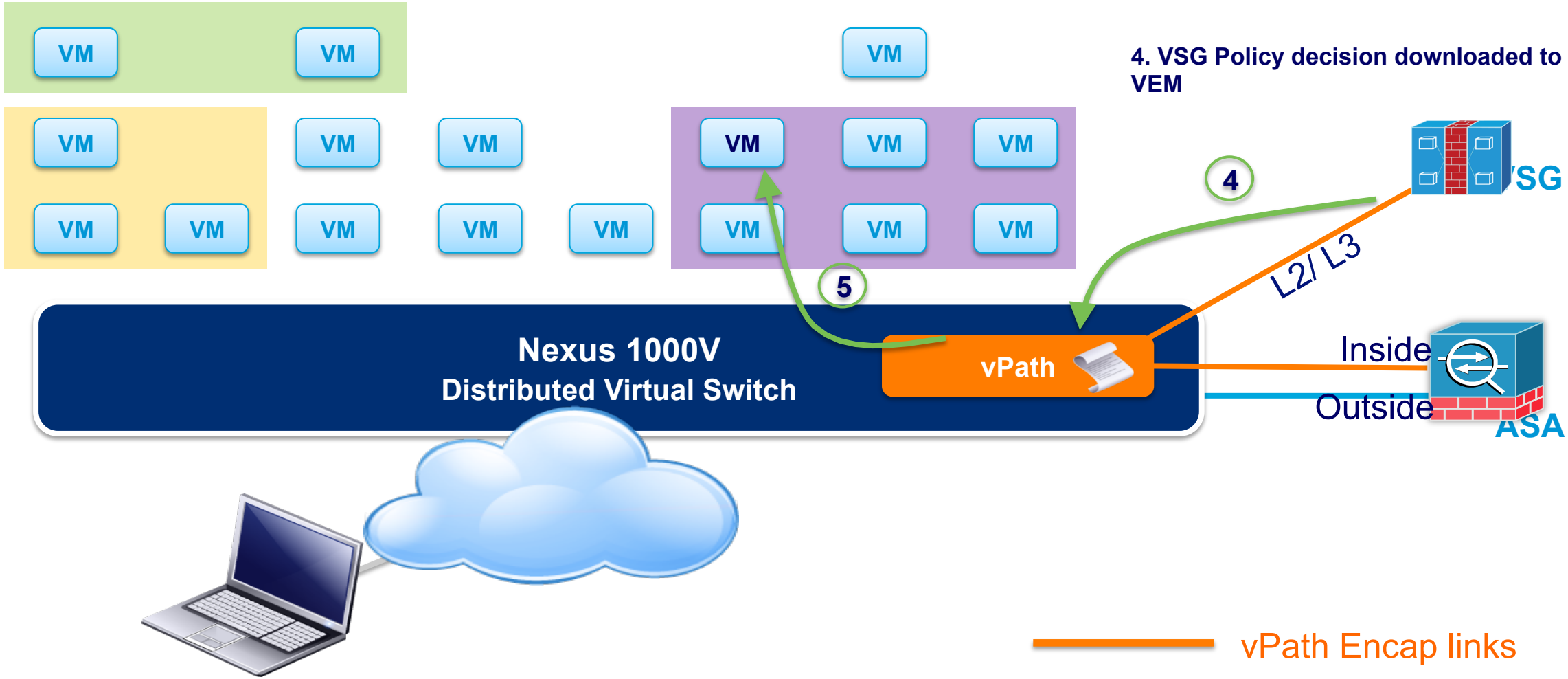
- Designed for virtualized network services
- VEM must be able to reach the L3 VSN
- Fast-Path Offload
- VSN on VXLAN
- Service chaining
- Proxy ARP required for L3
- Encapsulation Uplink MTU +96B



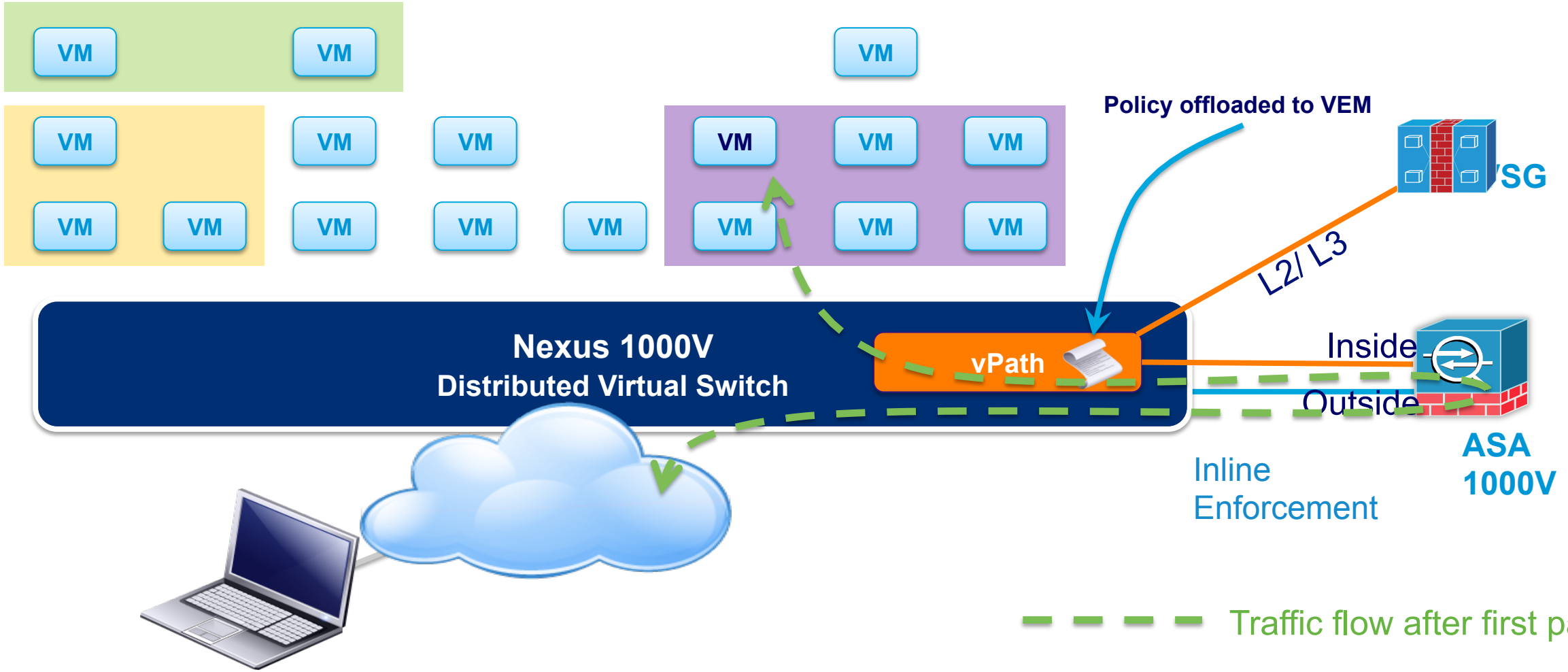
vPath service chain I. – Outside client to VM



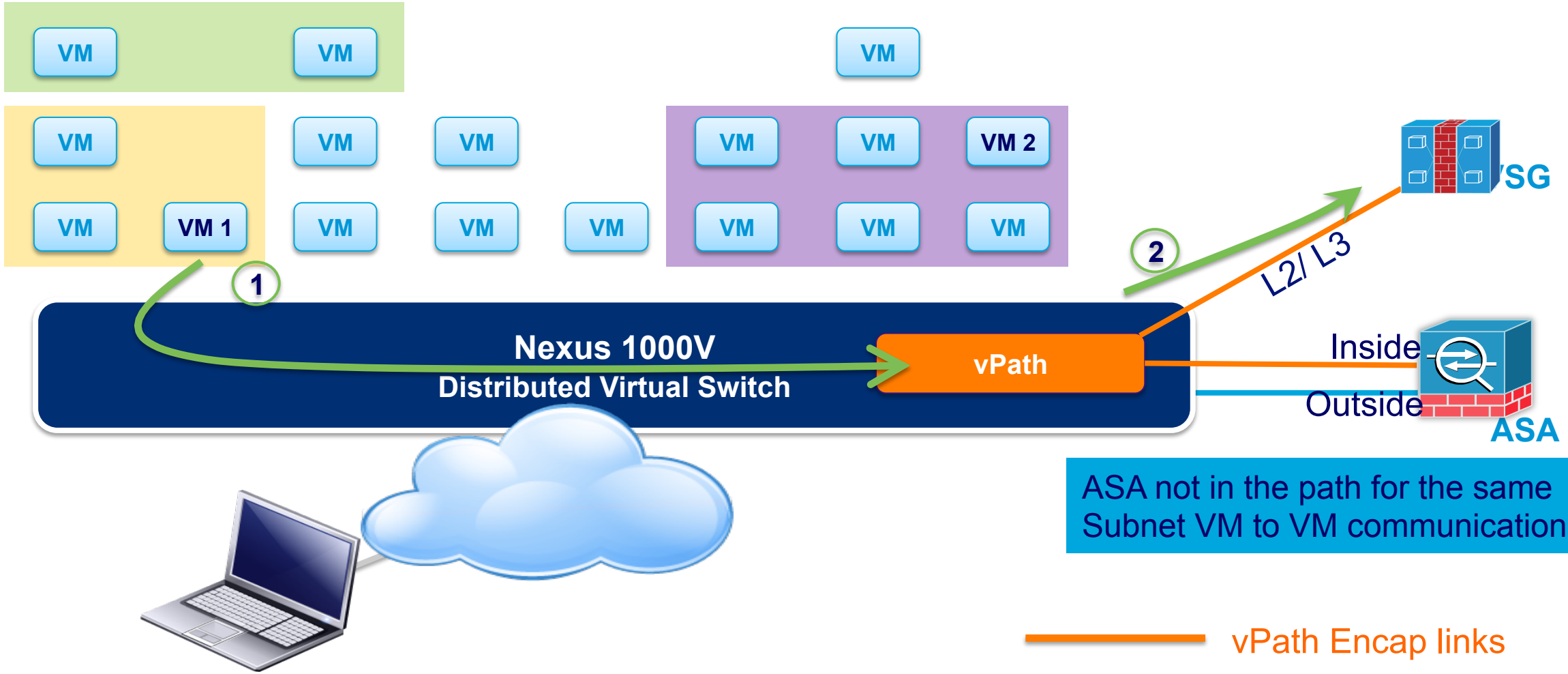
vPath service chain II. – Outside client to VM



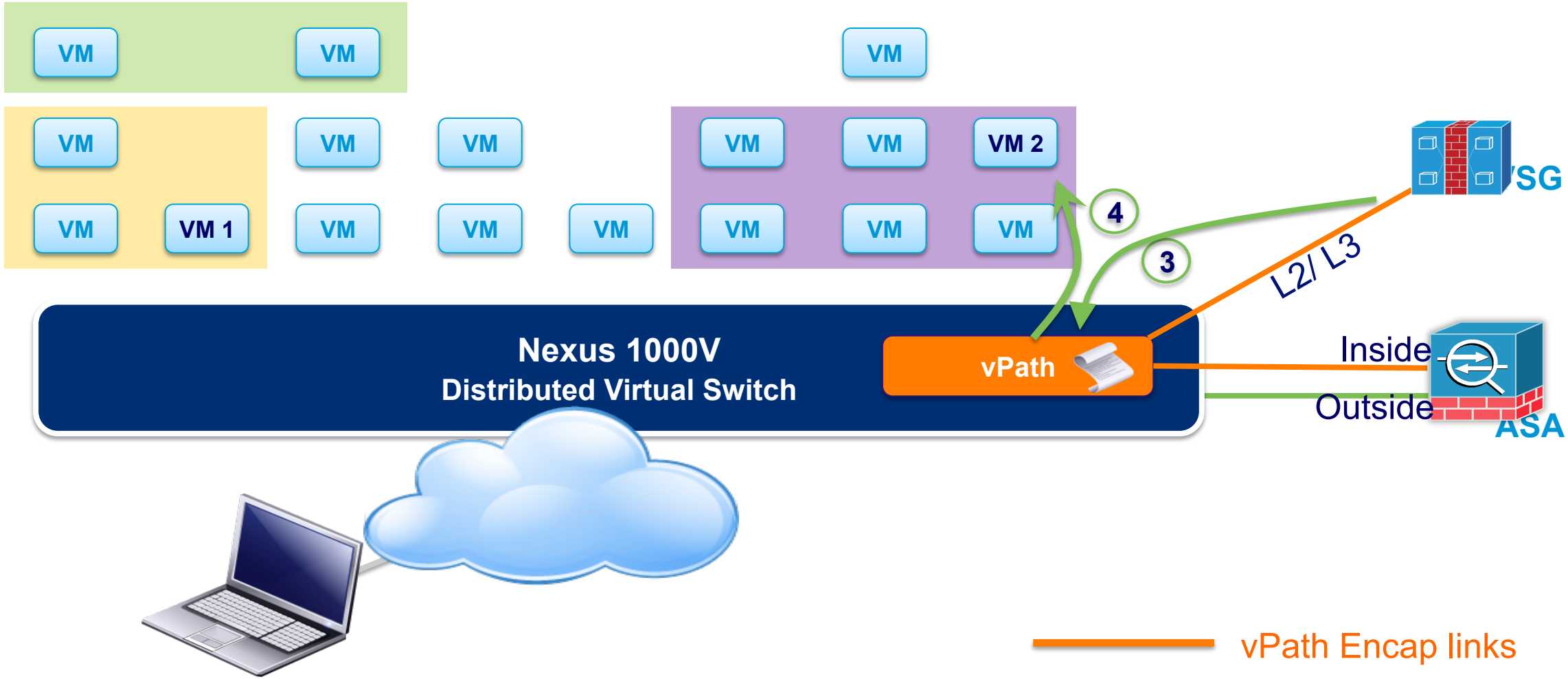
vPath service chain III. – Outside client to VM



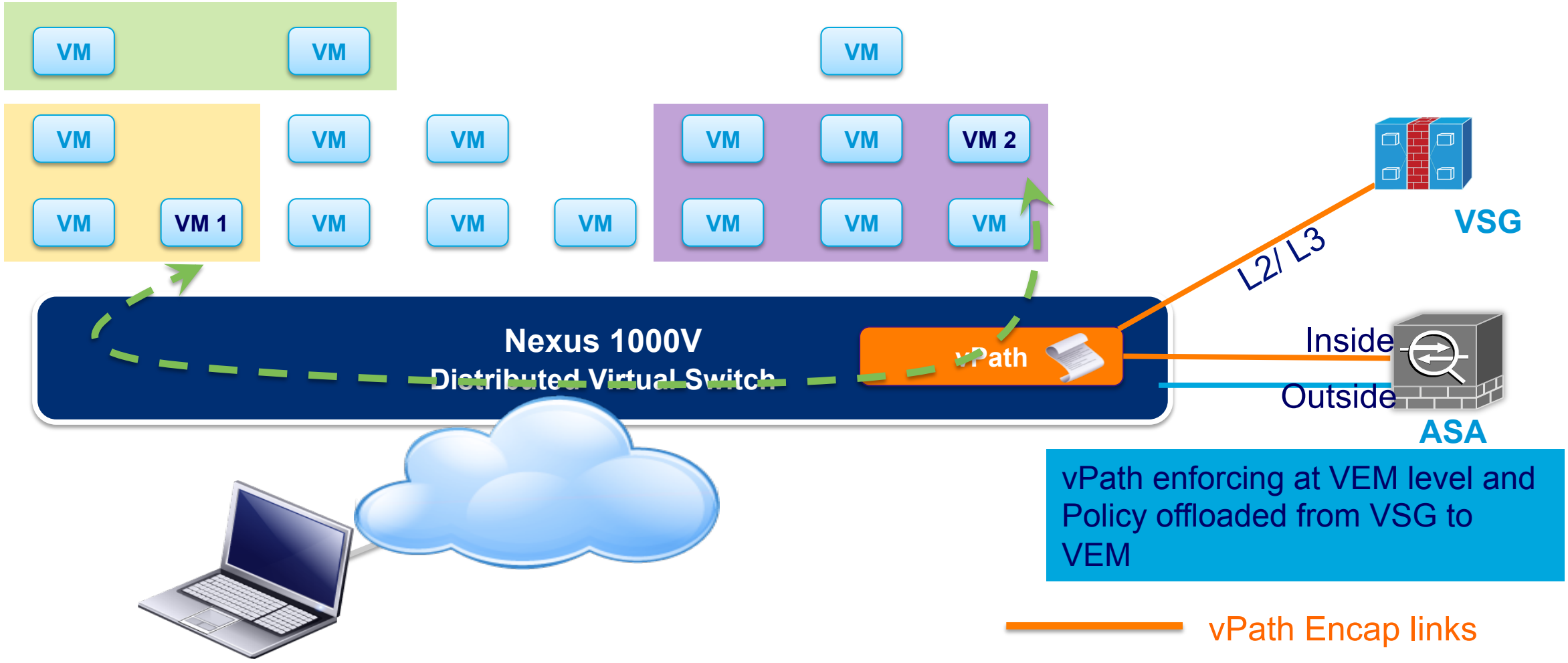
vPath service chain I. – VM1 to VM2 inside VLAN



vPath service chain II. – VM1 to VM2 inside VLAN

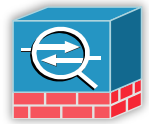


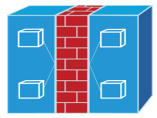
vPath service chain III. – VM1 to VM2 inside VLAN



Example of VSG and ASA 1000V chain for tenant

- vservice node ASA1 type asa
  - ip address 172.31.2.11
  - adjacency l2 vlan 3770
- vservice node VSG1 type vsg
  - ip address 10.10.11.202
  - adjacency l3
- vservice path chain-VSG-ASA
  - node VSG1 profile sp-web order 10
  - node ASA1 profile sp-edge order 20
- port-profile type vethernet Tenant-1
  - org root/Tenant-1
  - vservice path chain-VSG-ASA





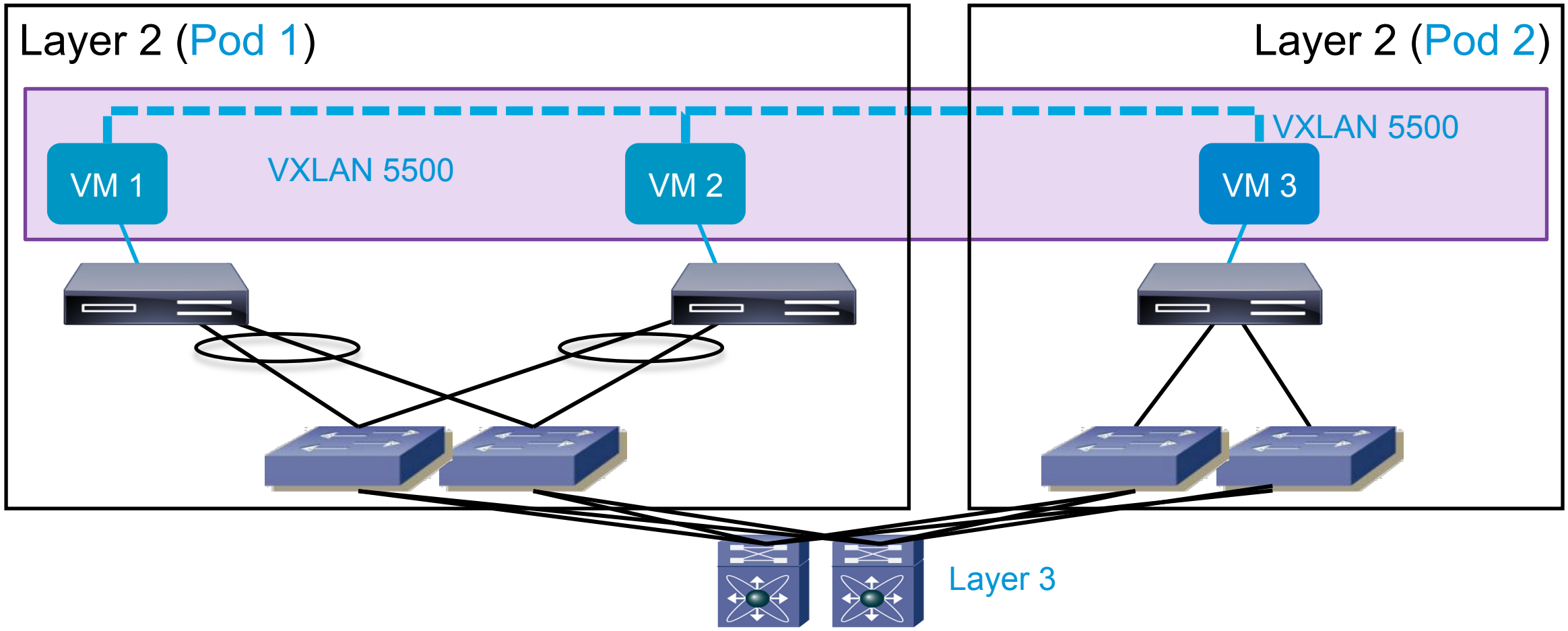
Defining the Service Node on Nexus 1000V

Chain the Service Nodes Order is inside to outside

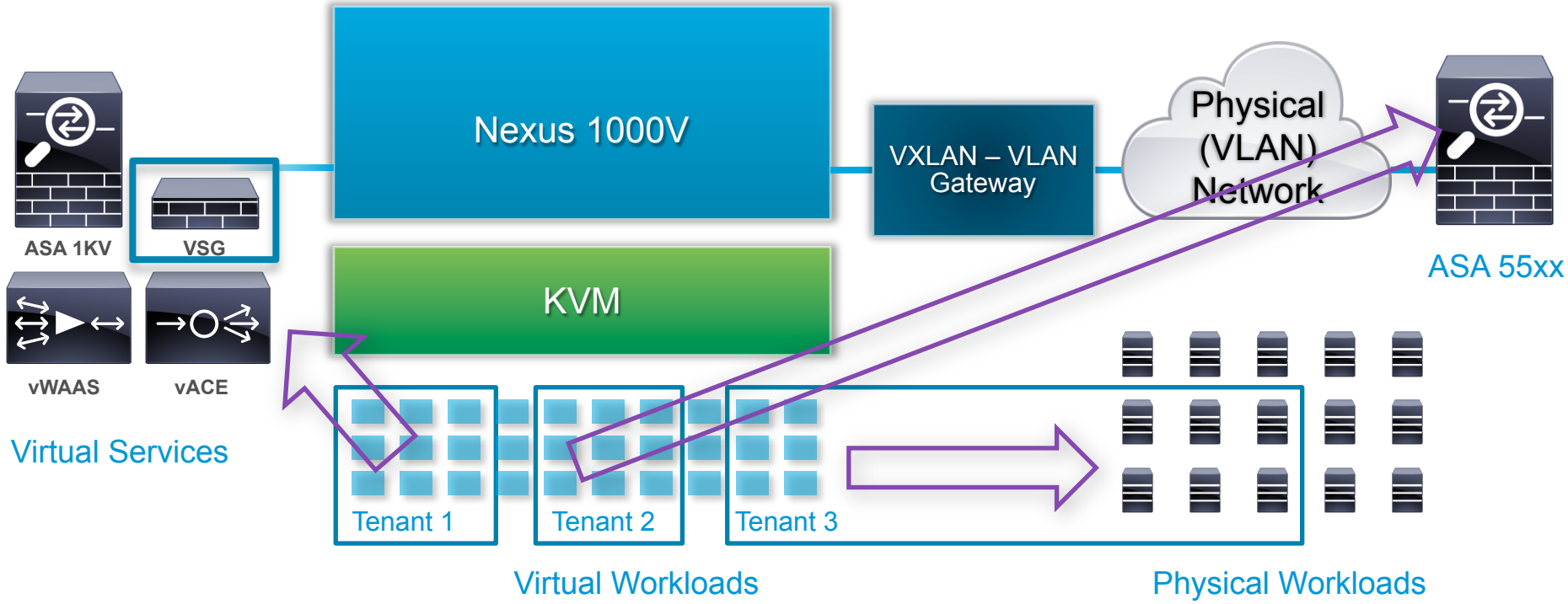
Enable the Service Chain Per Port-Profile

VXLAN: Reachability Across Subnet

- VM connectivity across L3 networks POD-to-POD, DC-to-DC
- VLAN indexes eXtenssion from 4k to 16M, IETF Standard Body



VXLAN Gateway

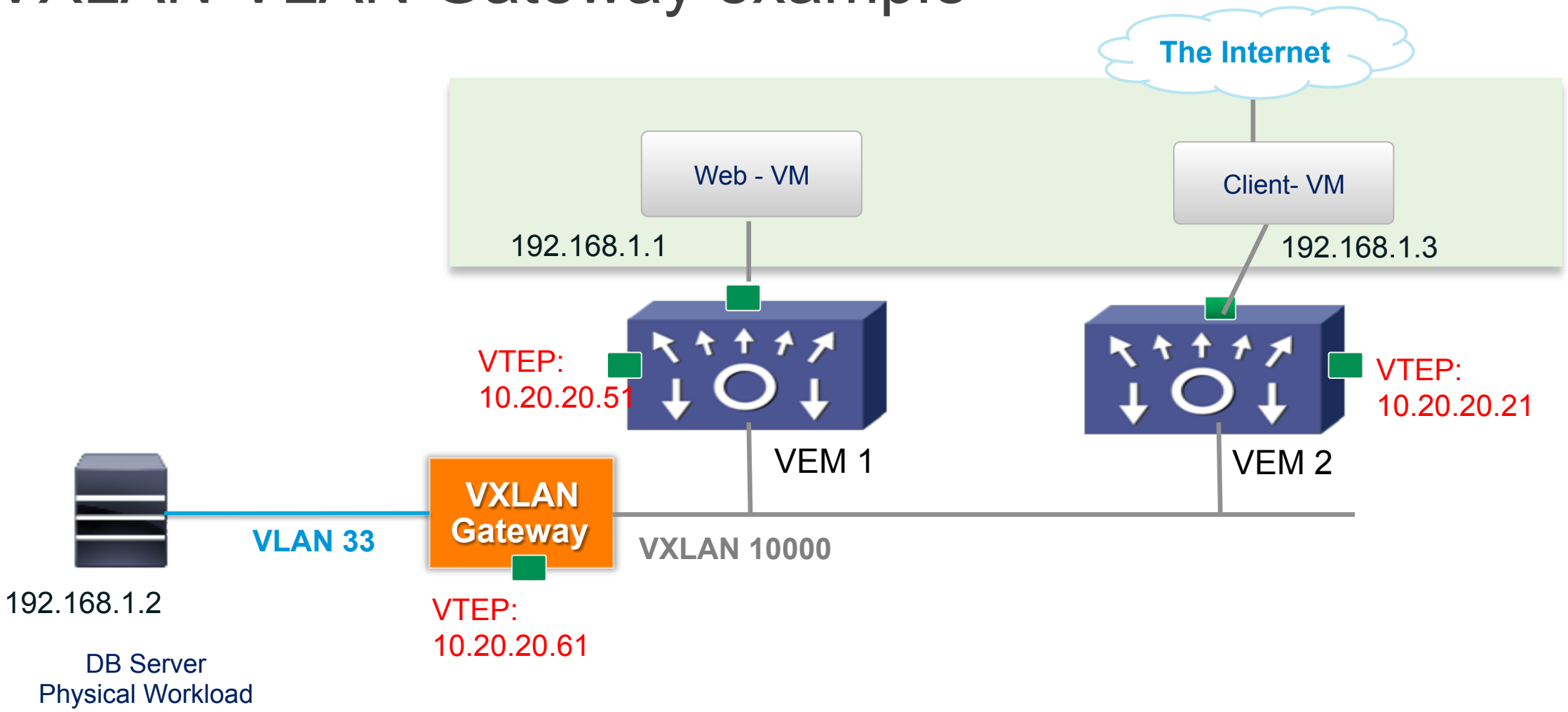


Tenant 1: virtual workloads protected by virtual firewall

Tenant 2: virtual workloads protected by physical firewall (via VXLAN GW)

Tenant 3: virtual & physical workloads in same L2 domain (via VXLAN GW)

VXLAN-VLAN Gateway example



Virtual Security Gateway overview

© 2011 Cisco and/or its affiliates. All rights reserved.

Virtual Security Gateway – Virtual Firewall for N1K

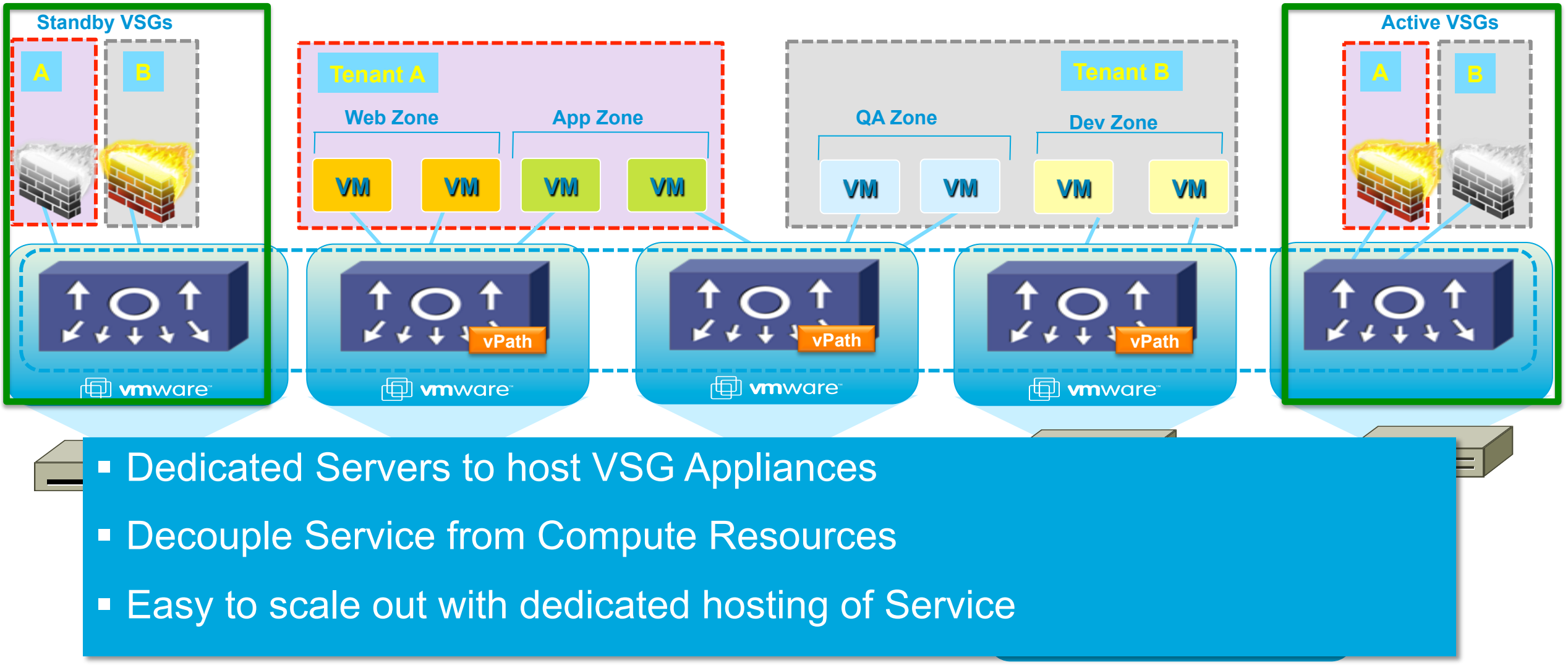
Virtual Security Gateway (VSG)

Context Aware Security	VM context aware rules
Zone-Based Control	Establish zones of trust
Dynamic, Agile	Policies follow vMotion
Best-in-Class Architecture	Efficient, fast, scale-out

Virtual Network Management Center (VNMC)

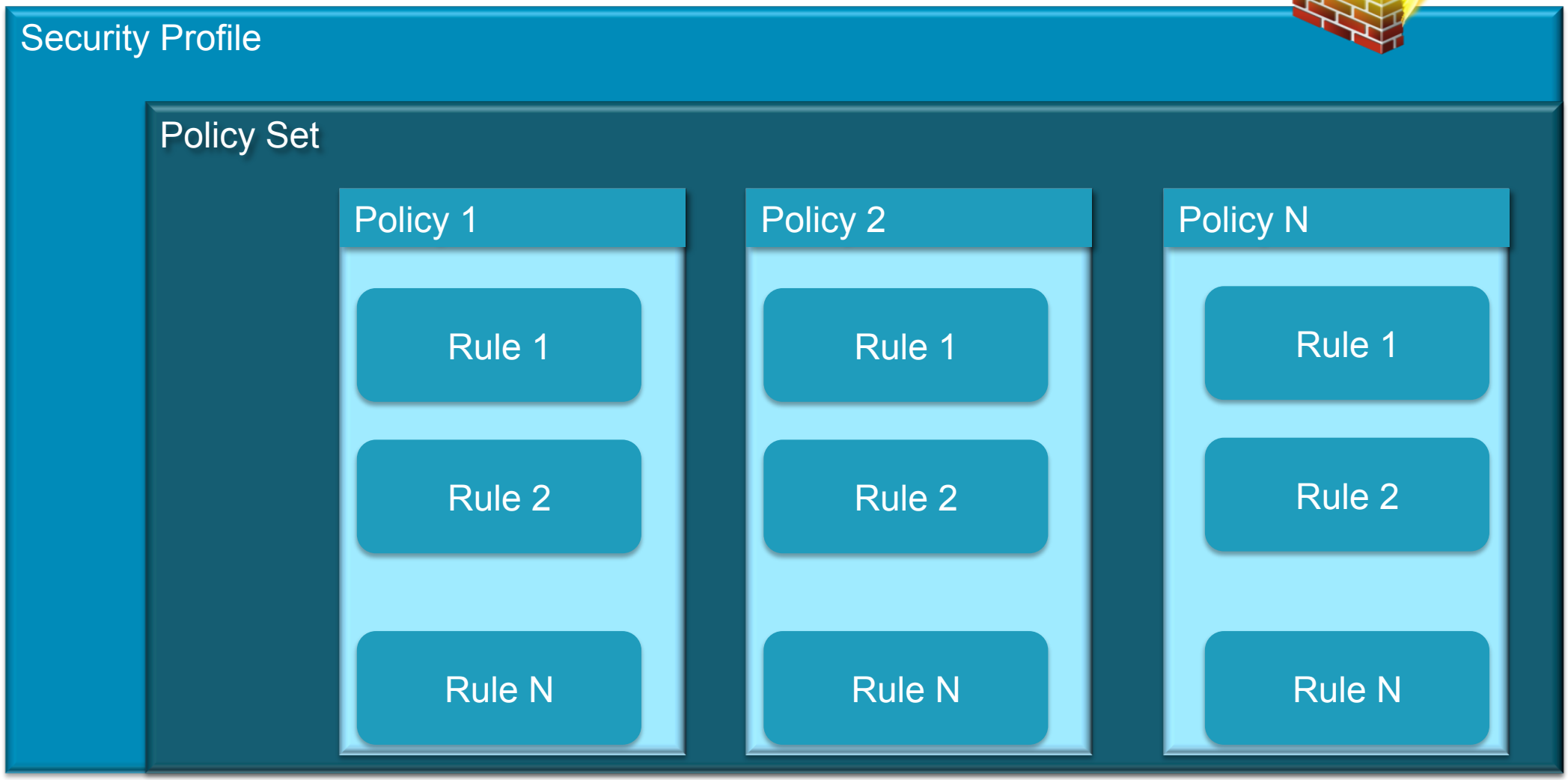
Non-Disruptive Operations	Security team manages security
Policy Based Administration	Central mgmt, scalable deployment, multi-tenancy
Designed for Automation	XML API, security profiles

Deployment VSGs on Dedicated Host



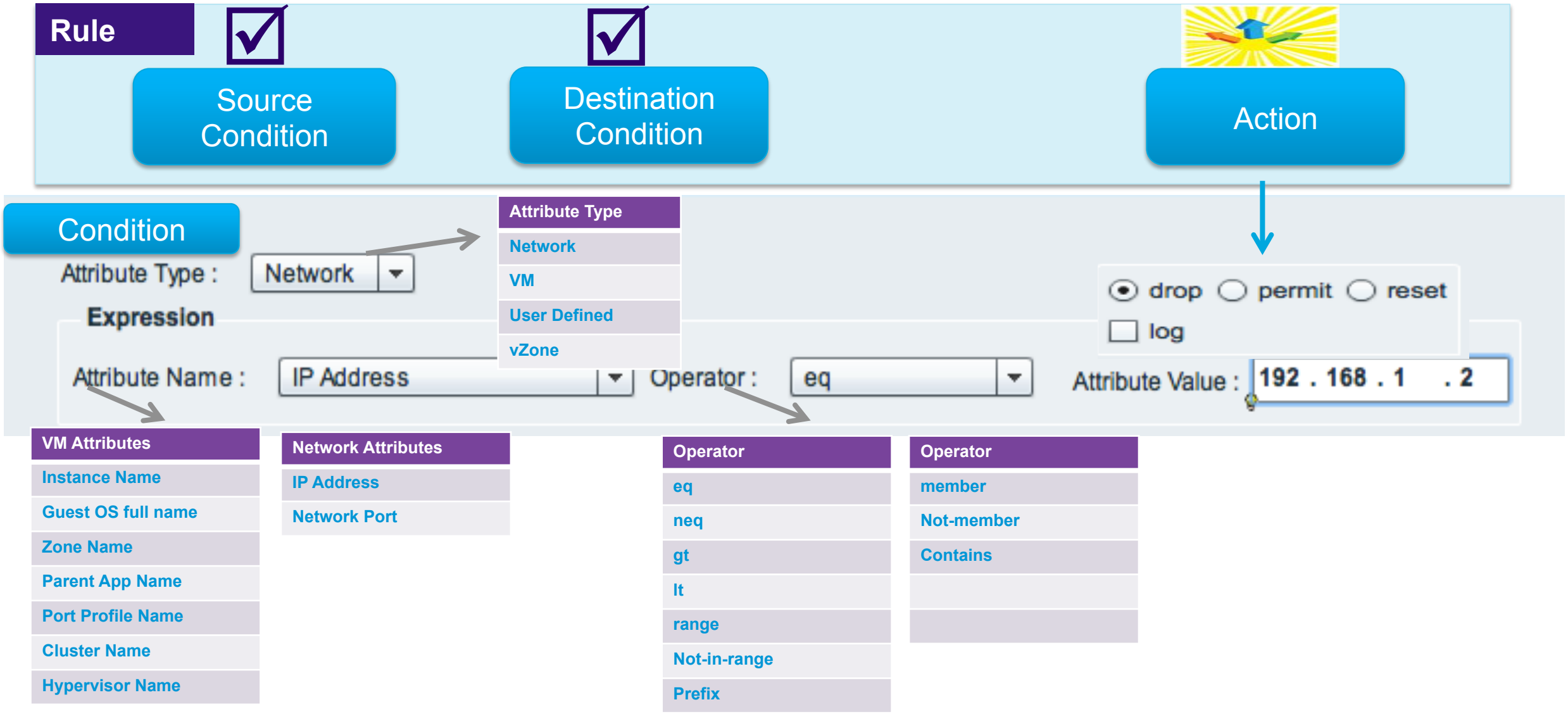
- Dedicated Servers to host VSG Appliances
- Decouple Service from Compute Resources
- Easy to scale out with dedicated hosting of Service

Security Policy Building Block

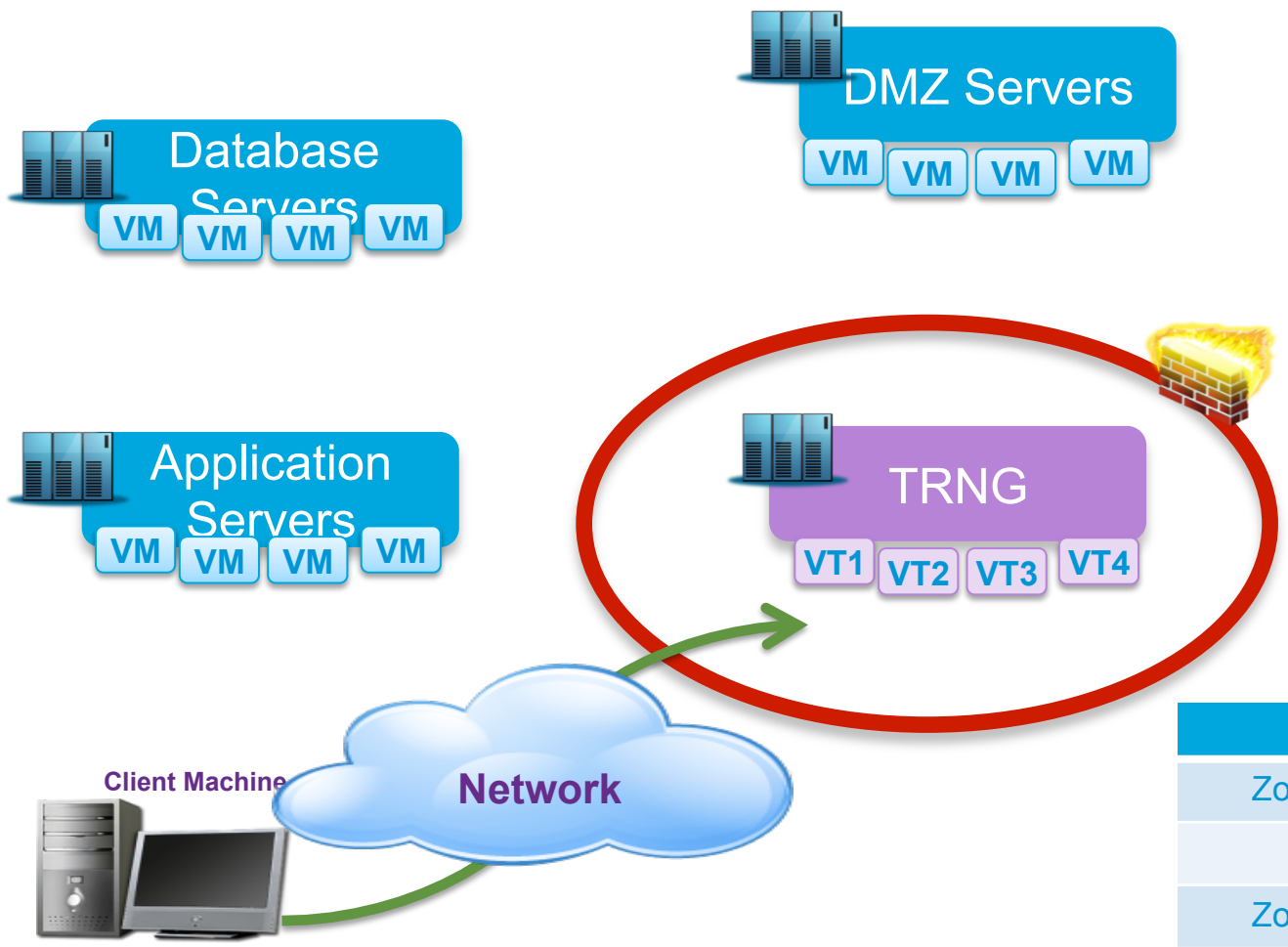


Rule is analogous to an MCL; Policy is analogous to an ACL

VSG Policy – Rule Construct



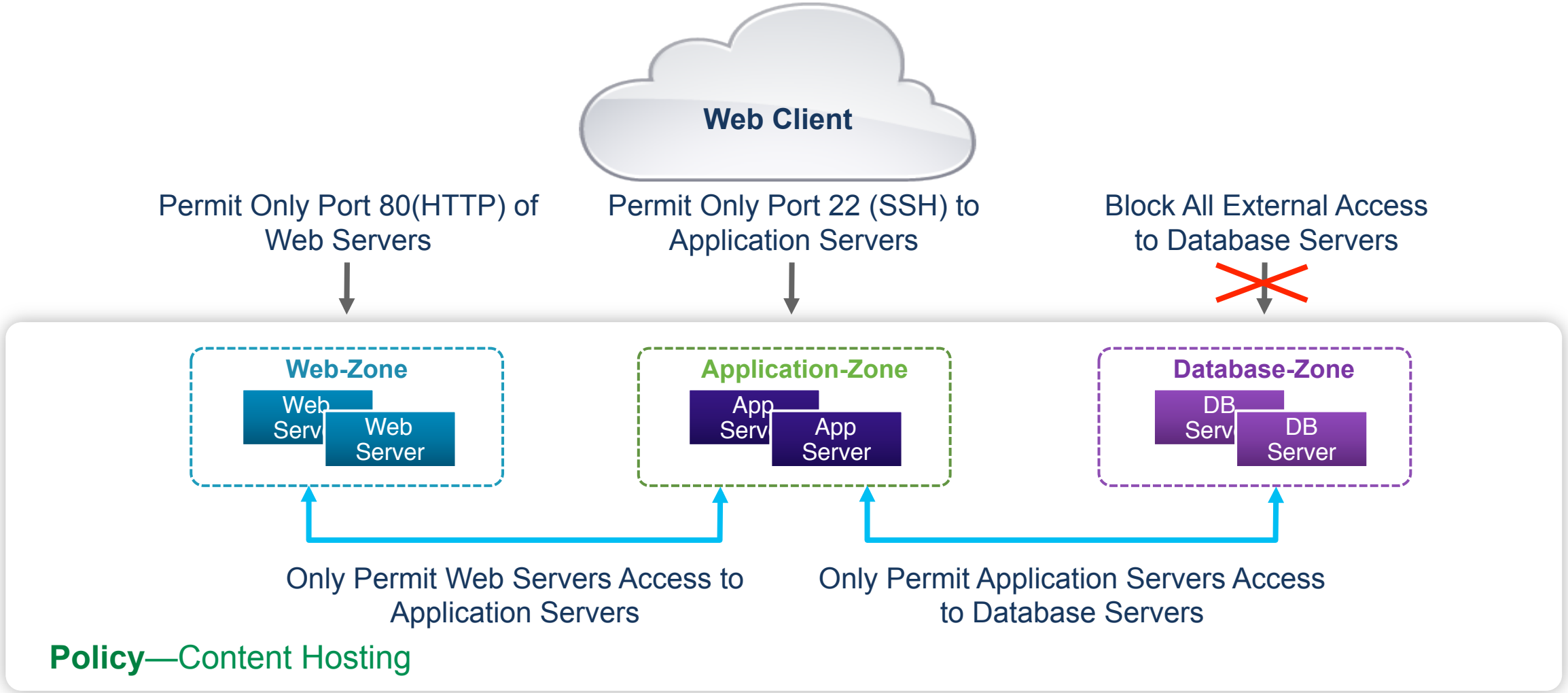
VSG Policy – Zone based policy



Zone	Attribute	Operator	Value
TRNG	VM Name	Contains String	VT1-4

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

Use Case – Tier Server Zones



Policy—Content Hosting

Use Case – Policy Rules with Zones

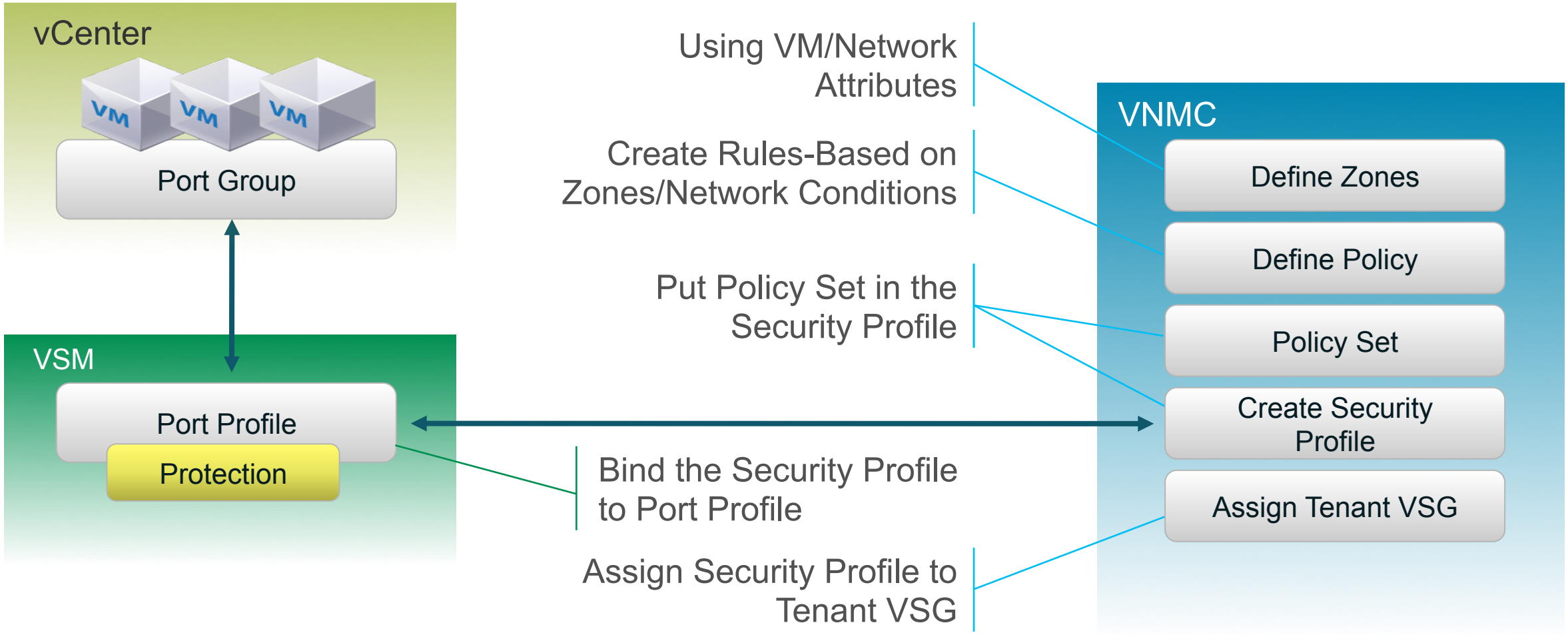
Leveraging Zones in Rule Conditions

Rule Table

Add Rule

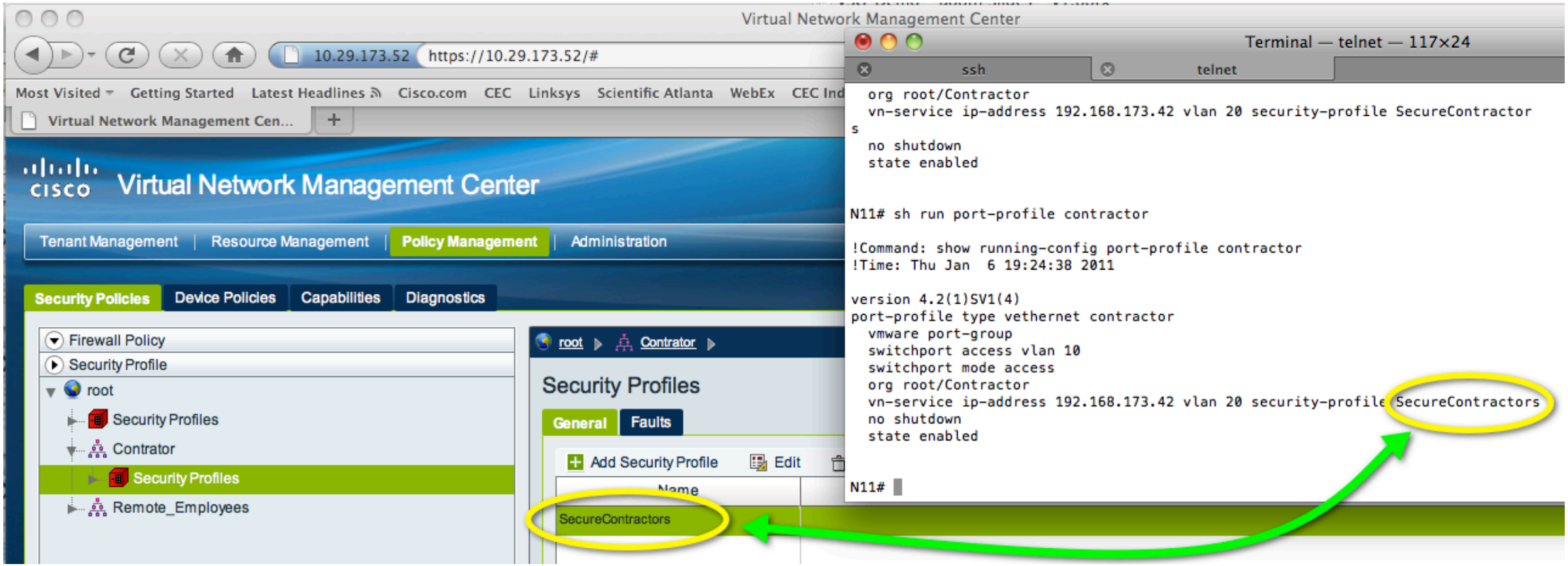
Name	Source Condition	Destination Condition	Protocol	EtherType	Action
Allow-Web	Any	Network Port eq 80 vZone Name eq WebZone	eq TCP	Any	Permit, Log
Allow-SSH	Any	Network Port eq 22 vZone Name eq AppZone	eq TCP	Any	Permit, Log
Allow-Web-To-App	vZone Name eq WebZone	vZone Name eq AppZone	Any	Any	Permit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

VSG Policy Provisioning Logical Flow



Binding VSG Security Profile with N1kV Port-Profile

Security-Profile "SecureContractors is attached to Port-Profile "contractor"

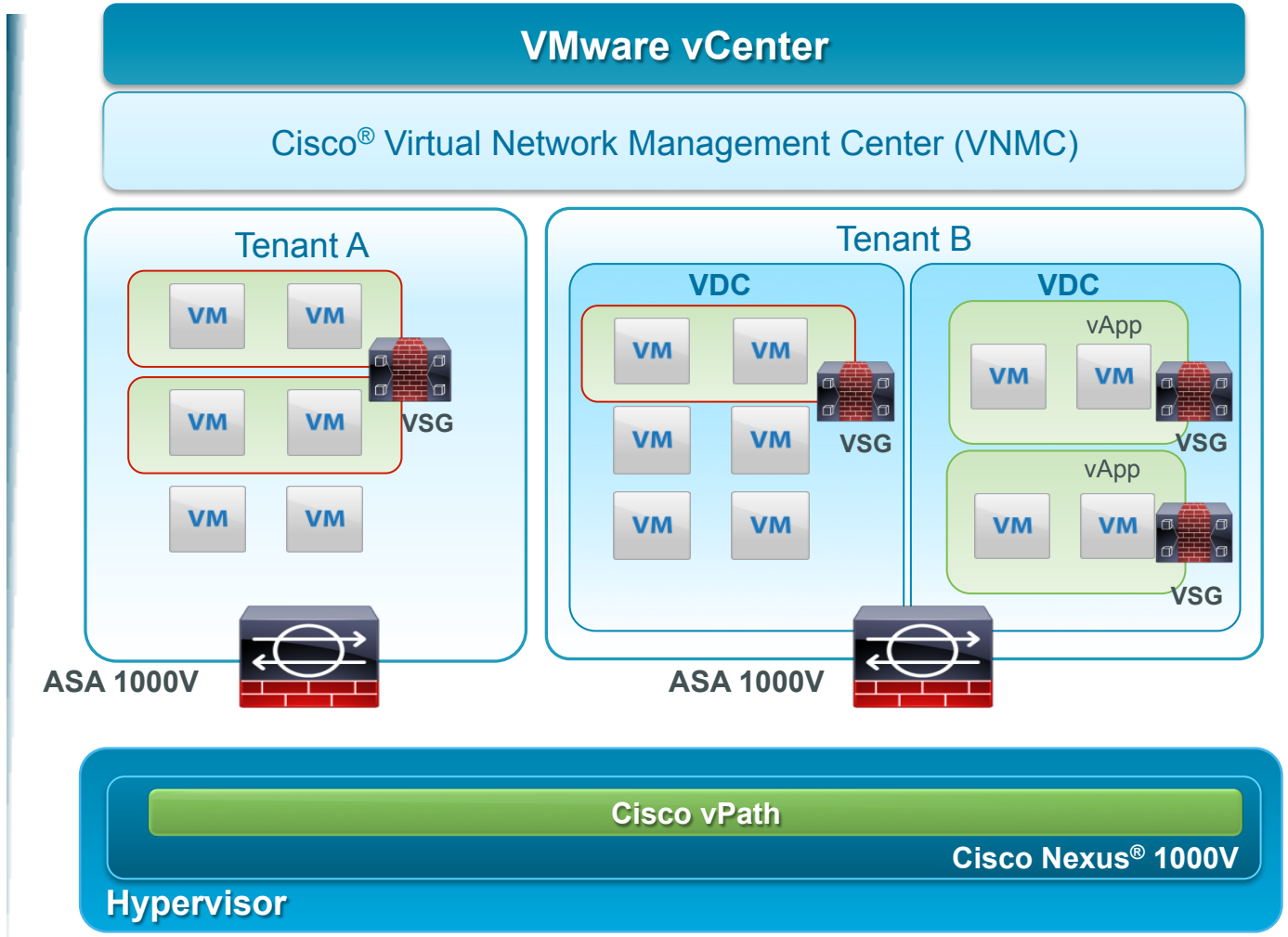


Virtual ASA 1000V role in overall architecture

© 2011 Cisco and/or its affiliates. All rights reserved.

Securing the tenant edge with Cisco ASA 1000V

- Proven Cisco security – physical and virtual consistency
- Collaborative security model
  - Cisco VSG for intra-tenant secure zones
  - Cisco ASA 1000V for tenant edge controls
- Transparent integration
  - Nexus 1000V Switch and vPath
- Scale flexibility to meet cloud demand
  - Multi-instance deployment for scale-out deployment across the data center

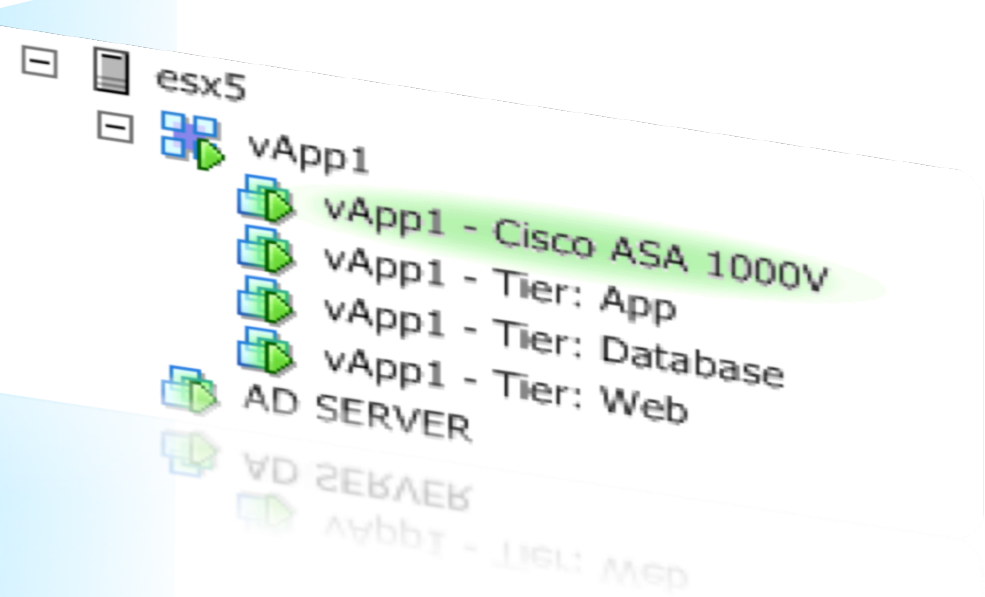


Virtual Form Factor Benefits

Efficient deployment as an ASA virtual machine

Deployed as you currently deploy or duplicate virtual machines and vApps

When the vApp or Tenant moves, the ASA 1000V can move with it



Example from Vmware vCenter where Cisco ASA 1000V is part of the vApp it protects

Cisco ASA 1000V Solution Features and Capabilities

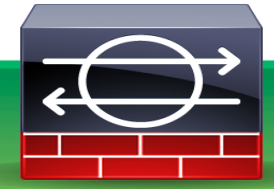
- Built using Cisco® ASA infrastructure
- Interoperability with Cisco VSG through service chaining
- VXLAN gateway
- Multi-tenant management Through Cisco VNMC

- IPsec VPN (site to site)
- NAT
- DHCP
- Default gateway
- Static routing
- Stateful inspection
- IP audit

Cisco ASA 1000V Performance Guidance

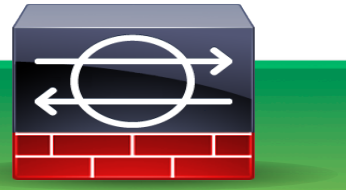
Performance depends on the resources available for the Cisco ASA 1000V instance

You can scale Cisco ASA 1000V by deploying additional instances



	Per Instance of Cisco® ASA 1000V
Maximum connections	**200,000**
Connections per second	**10,000**
VPN throughput	**200 Mbps**
Maximum VPN tunnels	**750**

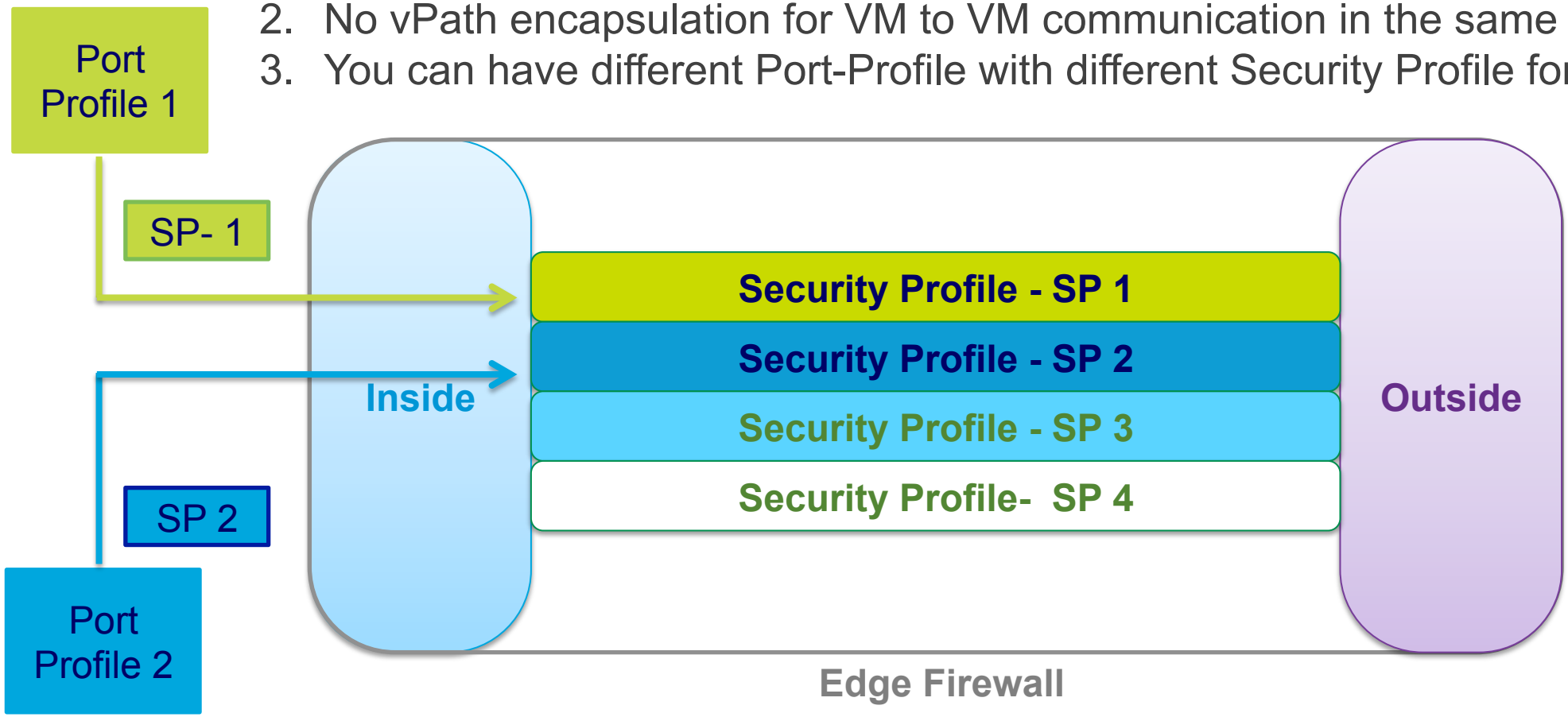
Cisco ASA 1000V Scalability



	Per Instance of Cisco® ASA 1000V
Policy rules per instance	4000
Minimum instances per tenant	1
Virtual machines secured per instance	512
Edge profiles per instance	32
Policies per policy set	256

Policies Enforcement with the ASA 1000V

1. Security Policy is attached to the Port-Profile
2. No vPath encapsulation for VM to VM communication in the same subnet
3. You can have different Port-Profile with different Security Profile for the same subnet



ASA 1000V DMZ use case

Two ASA 1000V Approach

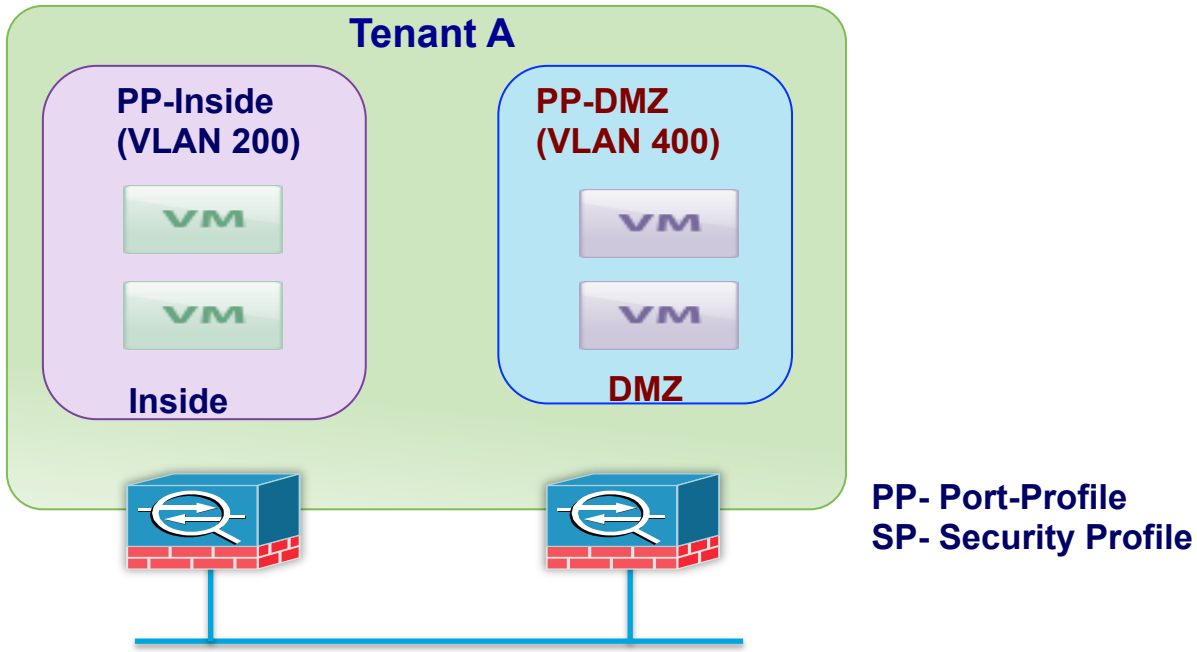
Two Edge Firewalls one for inside subnet and other for DMZ subnet

No enforcement within Inside and DMZ VLAN

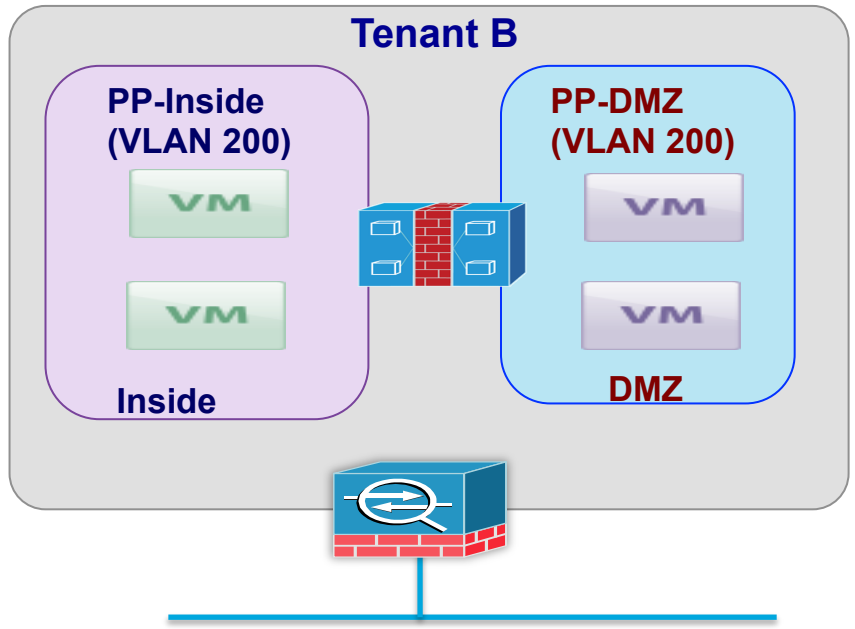
ASA 1000V and VSG Approach

Inside Security Profile and DMZ Security Profile addressing the security requirements for both Zones

Shared VLAN for both DMZ and Inside



PP- Port-Profile
SP- Security Profile



VNMC Overview

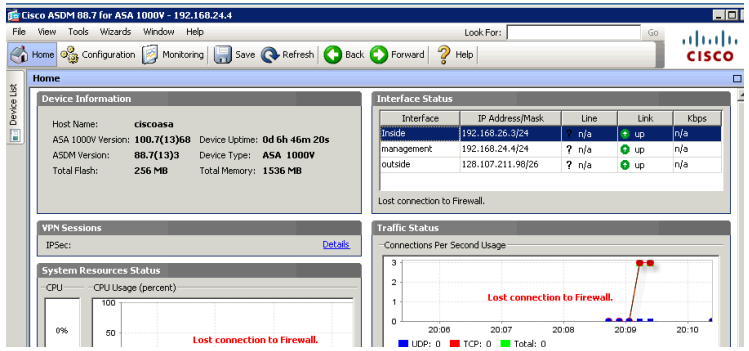
© 2011 Cisco and/or its affiliates. All rights reserved.

ADSM

Can configure both virtual and physical ASA from ASDM

Provides real-time logs, statistics on VPN connections

No VM attributes based policy configuration



VNMC

Can manage both VSG and ASA 1000V

Multitenant deployment

Policies can be pre-configured for future deployment

Stateless model

VM attribute based policy for ASA 1000V

Virtual Network Management Center

Simple yet powerful network virtual services management

Scalable
Stateless
Expandable
Partitionable
Integrated
Automated

Multi Tenant
Different Customers, different needs

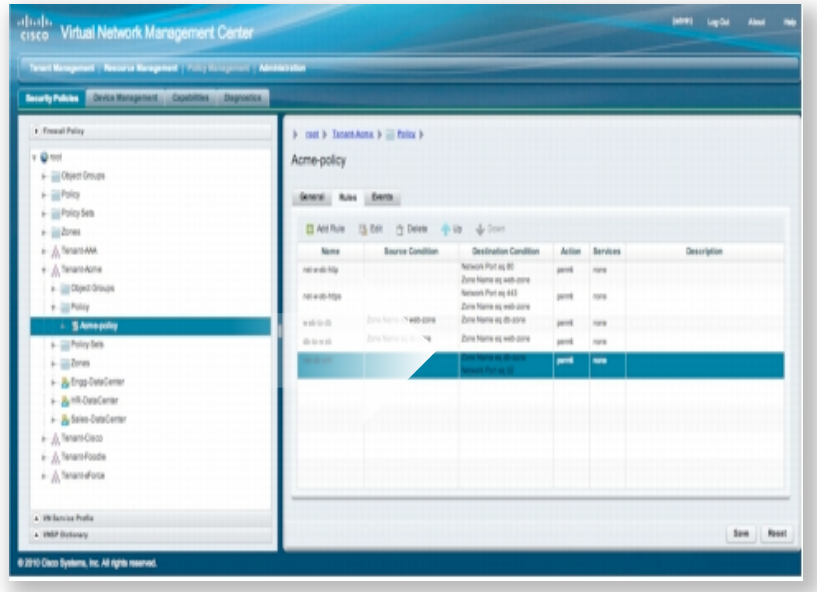
Security Profiles
Simple, policy based security configuration

XML API
3rd party integration ready

Role Based Access Controls
Different users, different privileges

Nexus 1000V & vCenter
Port profiles refer to security profiles

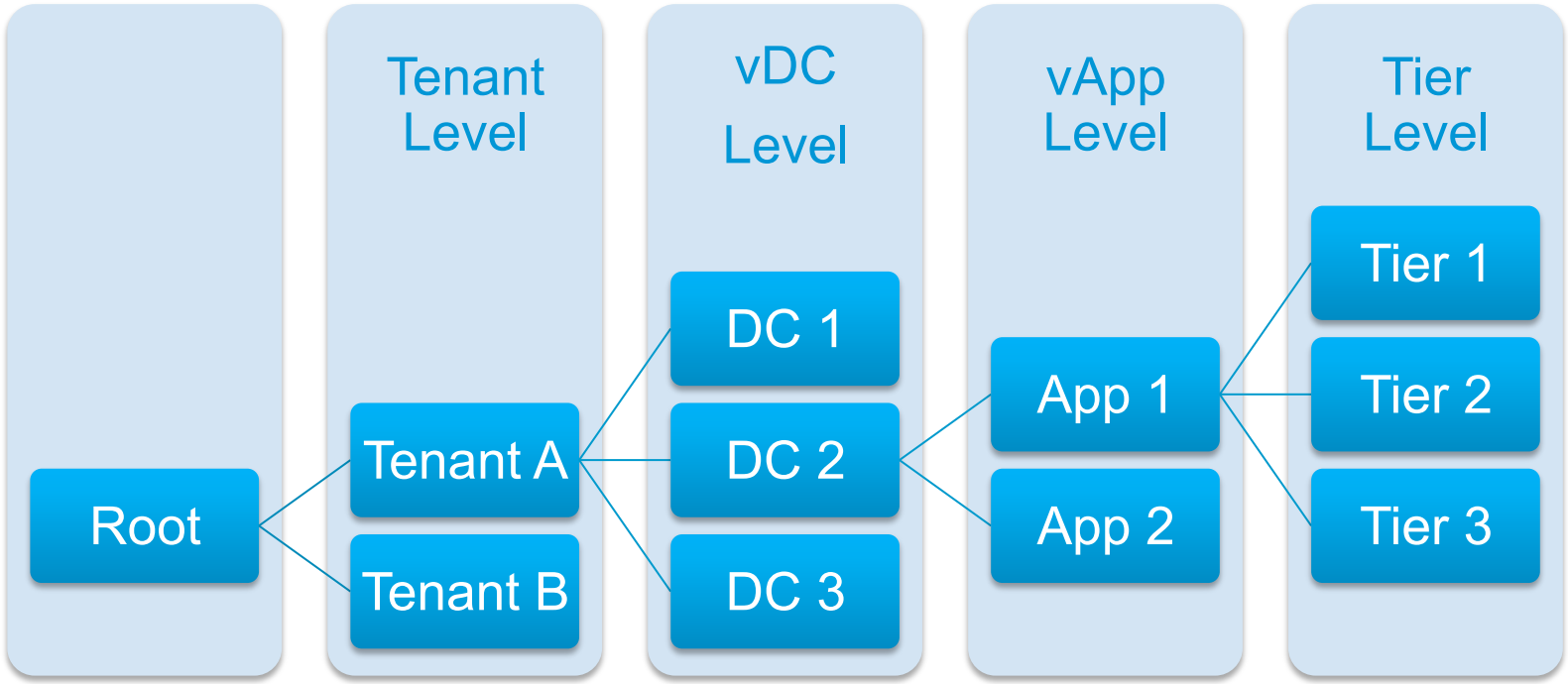
Dynamic provisioning
One stop configuration of network & security



VNMC GUI

Multitenant Org Structure

- Single Tenant can have up to 3 sub-levels of orgs
- Each sub-Level can have multiple orgs
- Overlapping Network Addresses across Tenants are supported

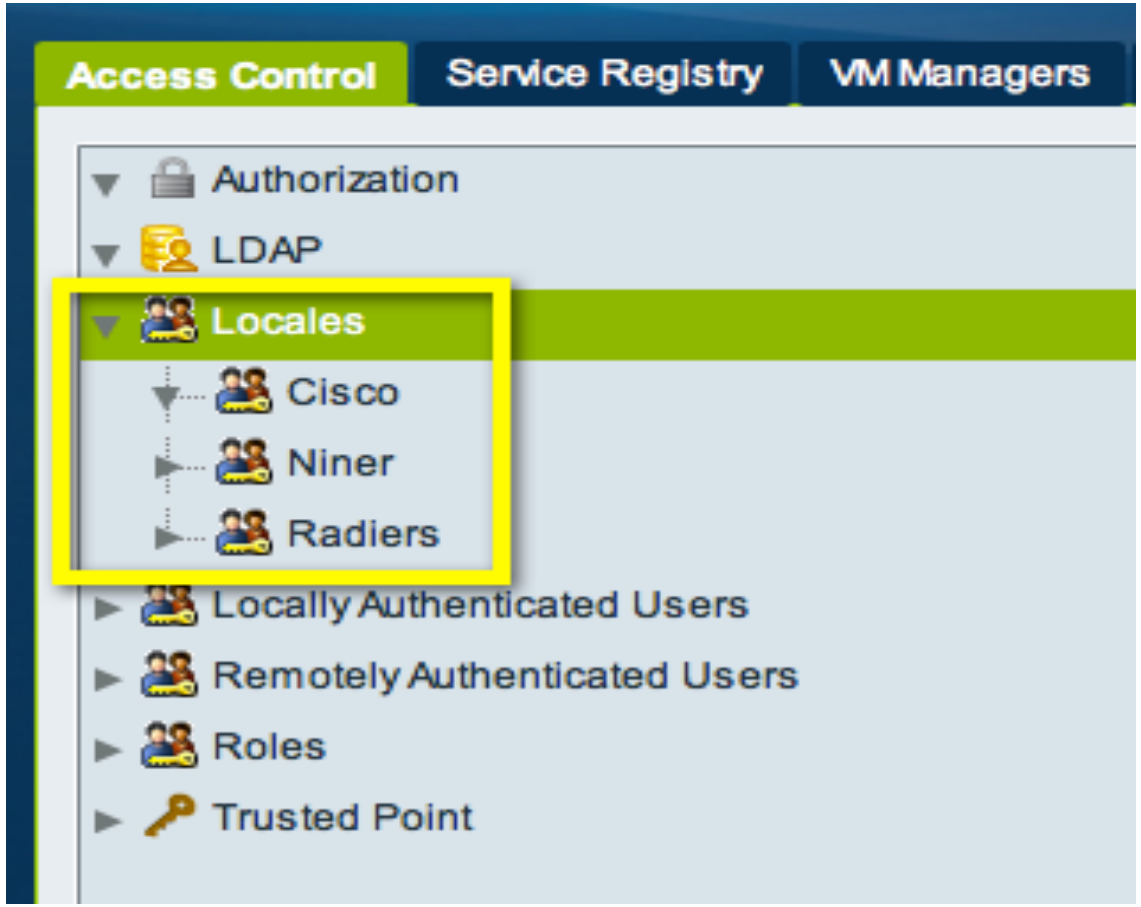


Administrative Roles

Tenant Level RBAC Access for Security Admin

1. VNMC Admin Roles

2. Tenant Level Access



VNMC Systems Requirements

VMware ESXi 4.1 +

vRAM: 3 GB

vHDD: 25 GB

vCPU: 1

Flash Player plug-in: version 11.2

Firewall ports requiring access

80 (HTTP/TCP), 443 (HTTPS), 843 (TCP

VSG System Requirements

VMWare ESXi 4.0

Nexus 1000V 1.4+

Virtual Network Management Center (VNMC)

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

ASA 1000V System Requirements

VMware ESXi 4.1 +

vRAM: 1.5 GB

vHDD: 1.5 GB

vCPU: 1 vCPU - 1 Ghz

vNIC: 4

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

Resume

Shift in Virtual Network Services strategy

VXLAN extends L2 boundaries and extend VLAN IDs for vCD

vPath traffic interception without topology change

Nexus 1000V is foundation for virtual services

Virtual Security Gateway zone based firewall between VMs

Virtual ASA is edge firewall for traffic entering/leaving tenants

Virtual WAAS easy traffic optimization in virtual environment

Upcoming Public Webcasts, Spring 2012

Spring 2013 Webinars			
4/10	Cloud Security with ASA 1000V and Virtual Security Gateway v2.1 (VSG)	Register	
4/17	Secure Hybrid Cloud solution with Nexus 1000V InterCloud & VNMC InterCloud	Register	
4/24	Nexus 1100 for Cloud Network Services: New Services & Ecosystem	Register	
5/1	Cloud Networking Services: vNAM and vWAAS	Register	
5/8	Virtualized Multiservice Data Center (VMDC) solution with Cloud Networking Services	Register	
5/15	Nexus 1000V for KVM (with OpenStack and VXLAN)	Register	

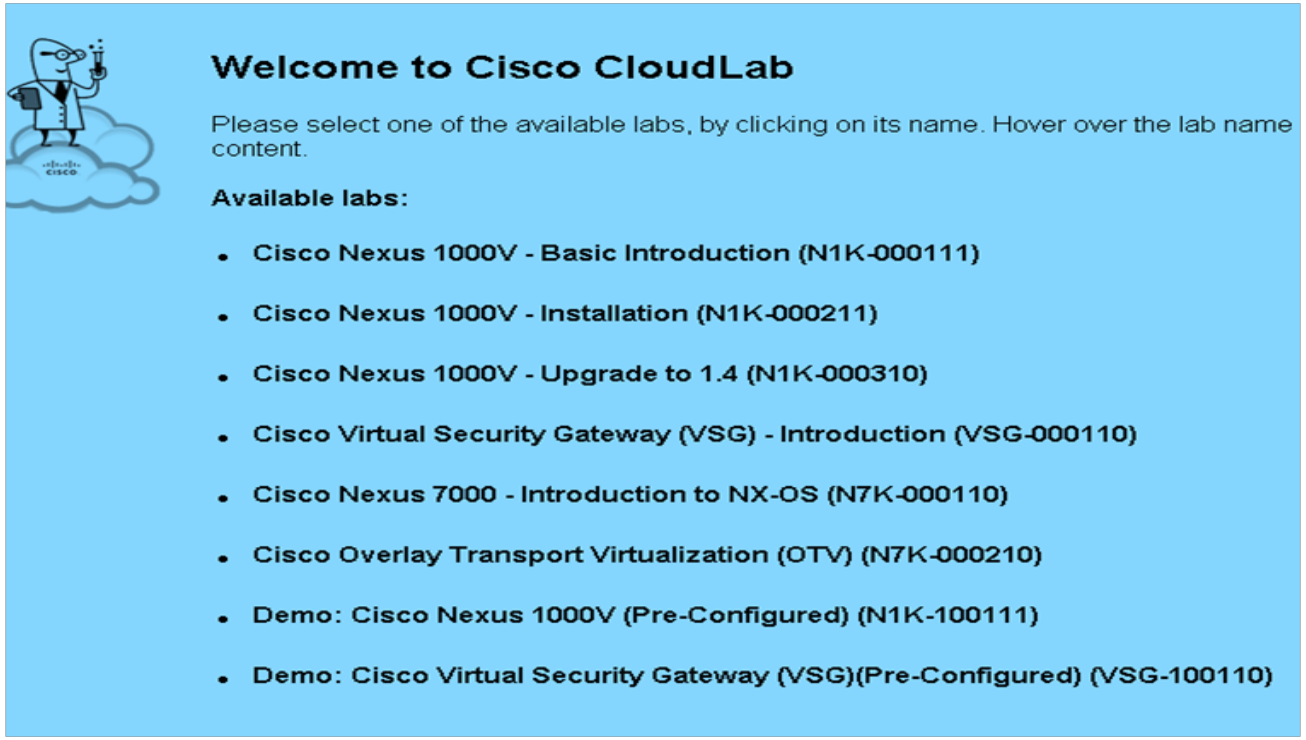
Webinar Link: www.cisco.com/go/1000vcommunity

Hands on for virtual networking specialists

- Hands-on labs available for Cisco® ASA 1000V, Cisco VSG, and Cisco Nexus® 1000V in Cisco 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



Otázky a odpovědi

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

e-mail: connect-cz@cisco.com

© 2013 Cisco and/or its affiliates. All rights reserved.

Prosíme, ohodnoťte tuto přednášku.

© 2013 Cisco and/or its affiliates. All rights reserved.

Děkujeme za pozornost.

© 2013 Cisco and/or its affiliates. All rights reserved.