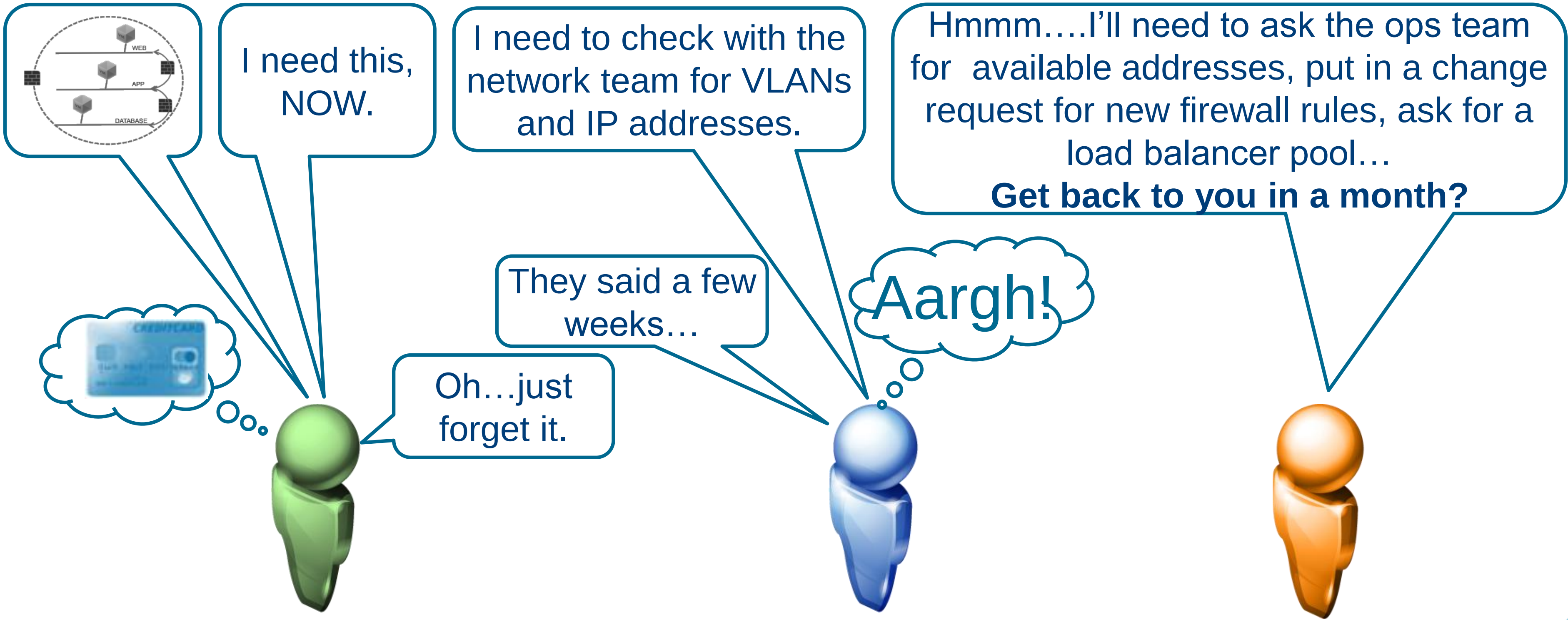
VMware NSX

Jan Tiri – jtiri@vmware.com

End Users Still Wait Weeks for Their Apps

Network and security challenges hamper cloud service provisioning.



I need this, NOW.

I need to check with the network team for VLANs and IP addresses.

Hmmm….I'll need to ask the ops team for available addresses, put in a change request for new firewall rules, ask for a load balancer pool…
Get back to you in a month?

They said a few weeks…

Aargh!

Oh…just forget it.

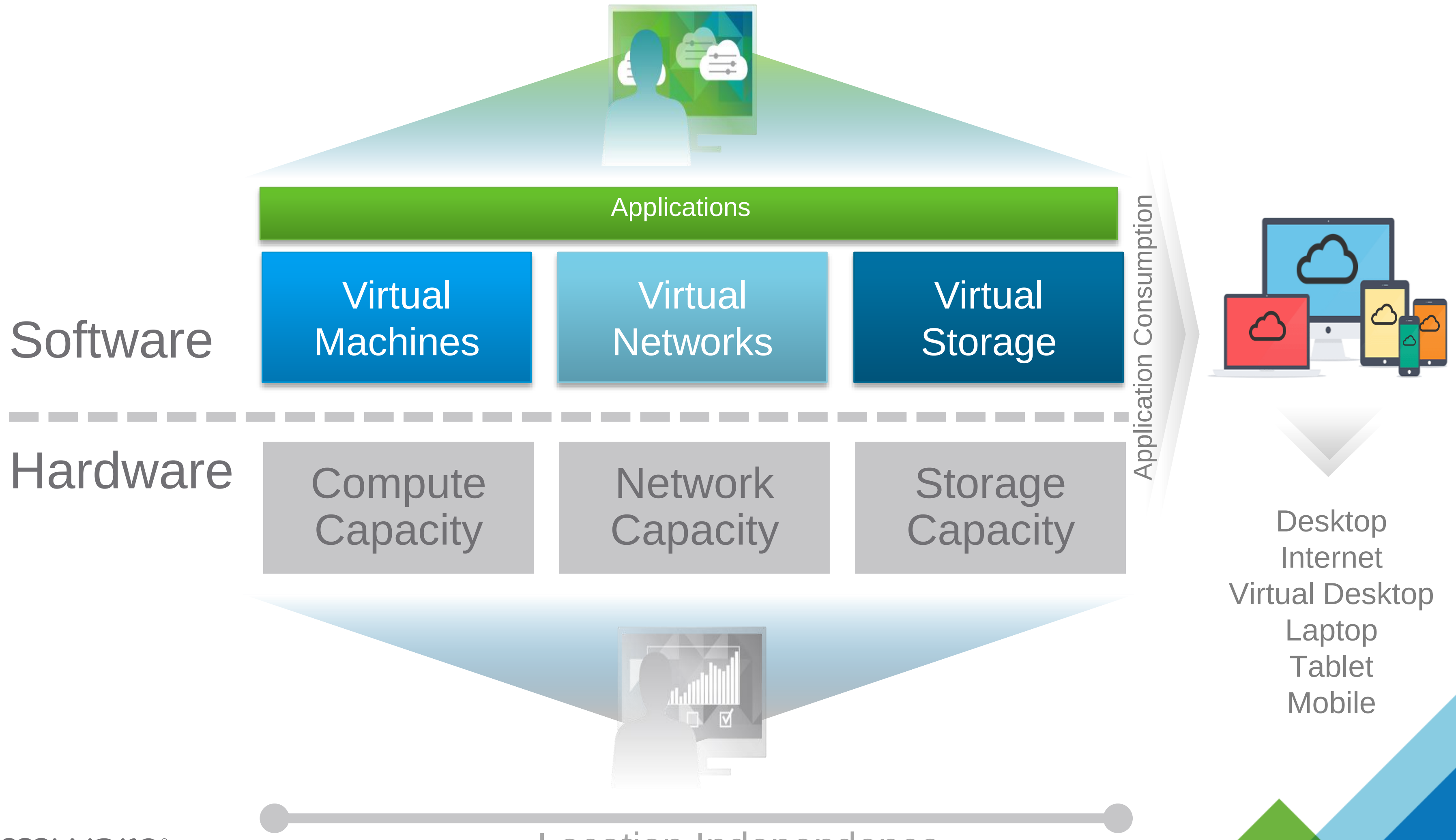
Business User

VI Admin / Cloud Operator

Network Architect

vmware®

The Software Defined Data Center (SDDC)



Applications

Software

Virtual Machines

Virtual Networks

Virtual Storage

Hardware

Compute Capacity

Network Capacity

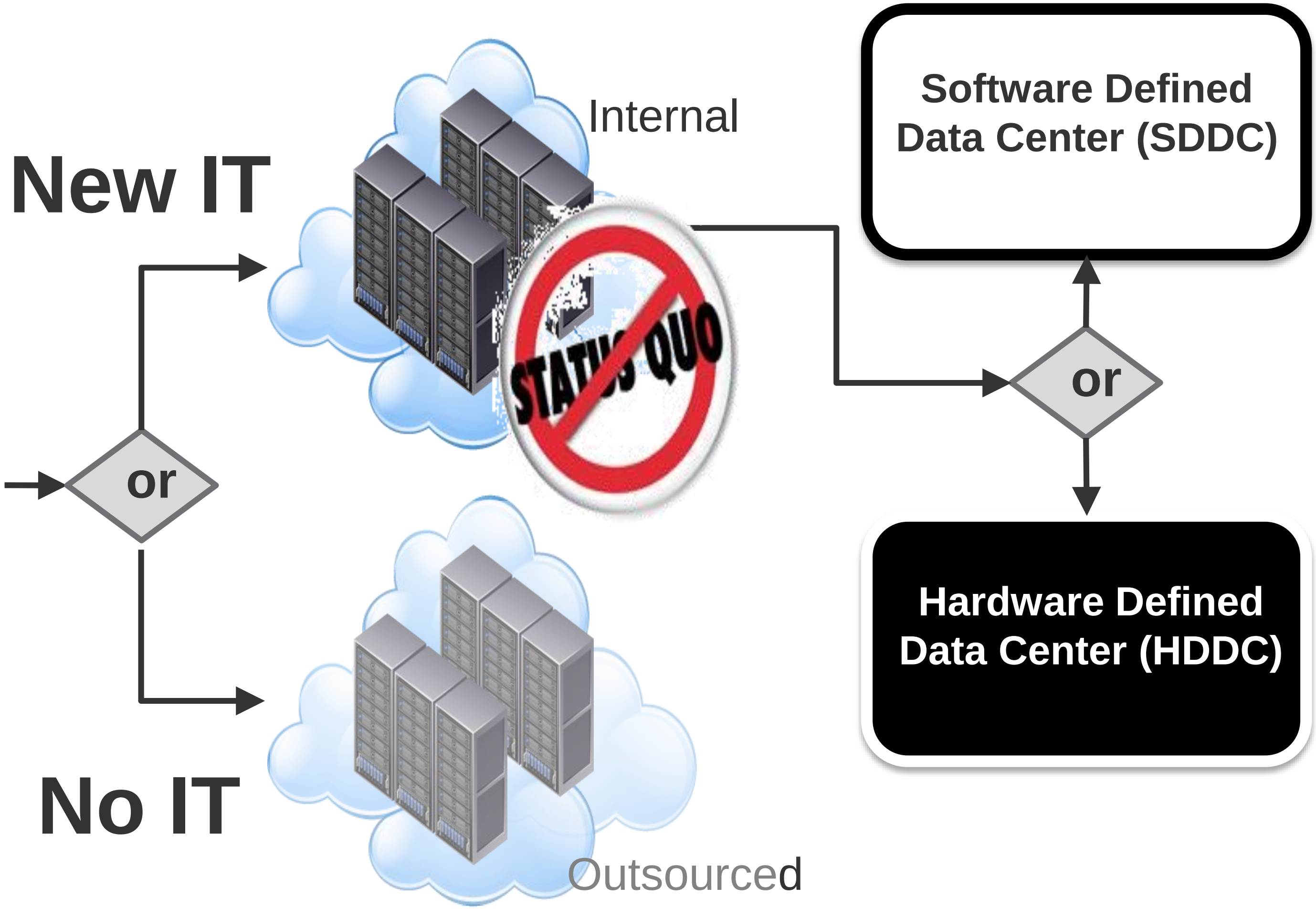
Storage Capacity

Application Consumption

Desktop
Internet
Virtual Desktop
Laptop
Tablet
Mobile

Location Independence

Enterprise business leaders want their IT to be like Amazon



New IT

Internal

or

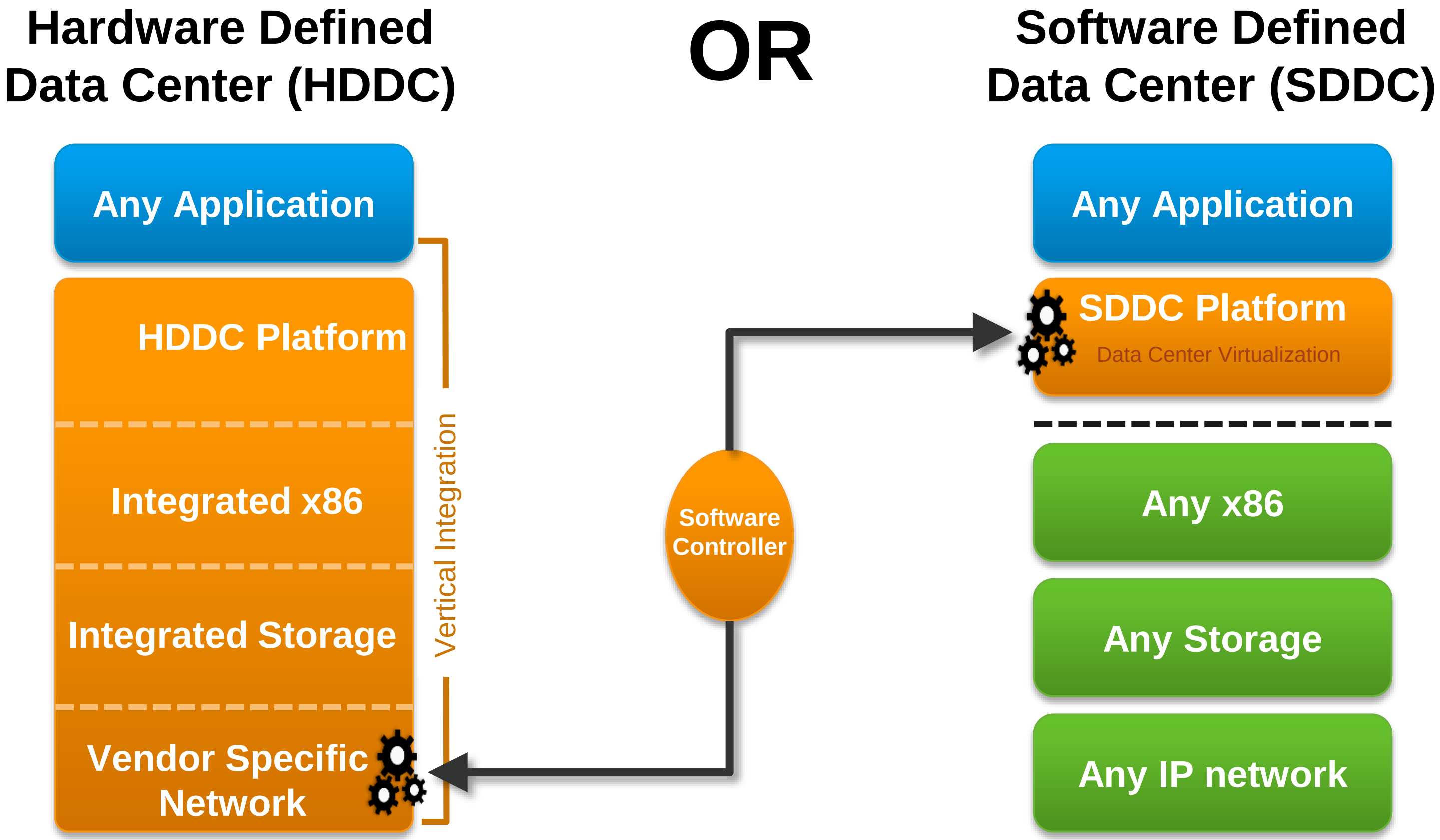
Software Defined Data Center (SDDC)

or

Hardware Defined Data Center (HDDC)

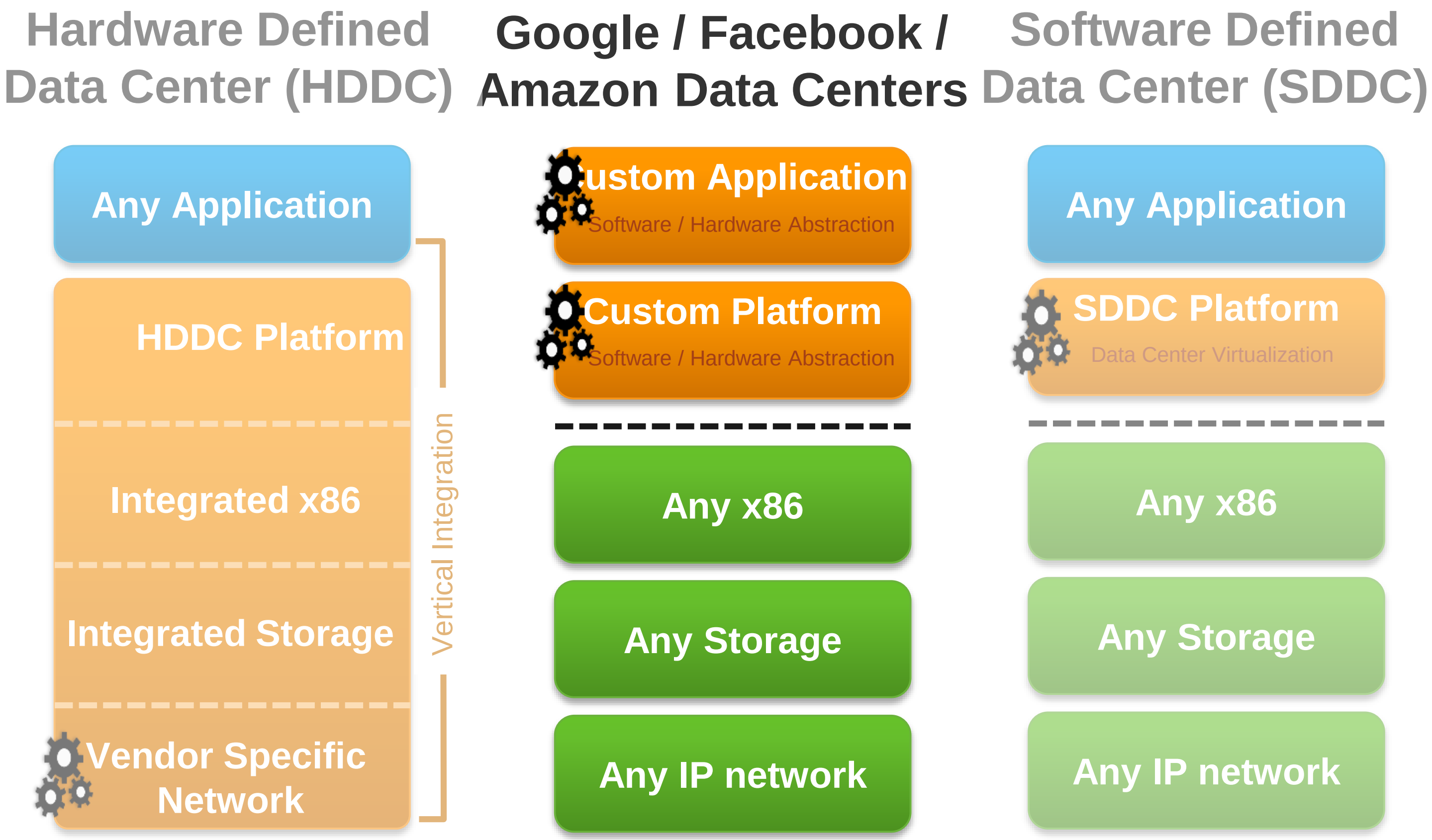
No IT

Outsourced



Hardware Defined
Data Center (HDDC)
OR
Software Defined
Data Center (SDDC)
Any Application
HDDC Platform
Integrated x86
Integrated Storage
Vendor Specific Network
Vertical Integration
Software Controller
Any Application
SDDC Platform
Data Center Virtualization
Any x86
Any Storage
Any IP network

The anatomy of the modern data center



Hardware Defined Data Center (HDDC)

Any Application

HDDC Platform

Integrated x86

Integrated Storage

Vendor Specific Network

Vertical Integration

Google / Facebook / Amazon Data Centers

Custom Application

Software / Hardware Abstraction

Custom Platform

Software / Hardware Abstraction

Any x86

Any Storage

Any IP network

Software Defined Data Center (SDDC)

Any Application

SDDC Platform

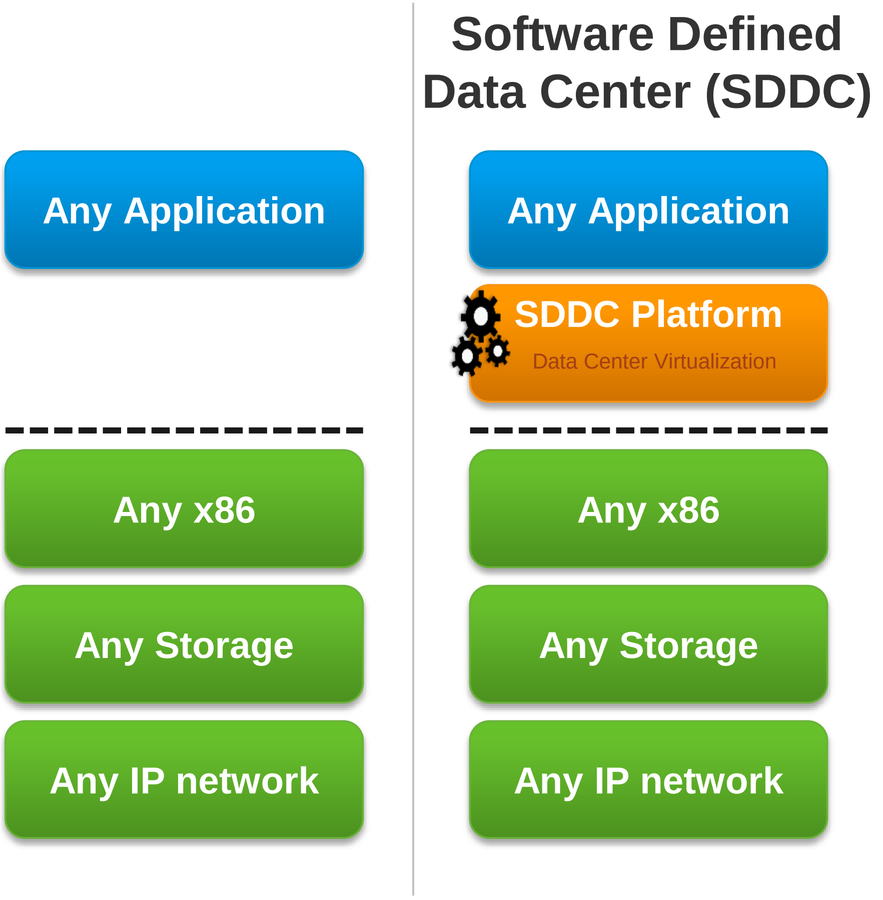
Data Center Virtualization

Any x86

Any Storage

Any IP network

The Power of SDDC – Intra Data Center



Software Defined Data Center (SDDC)

Any Application

Any x86

Any Storage

Any IP network

Any Application

SDDC Platform

Data Center Virtualization

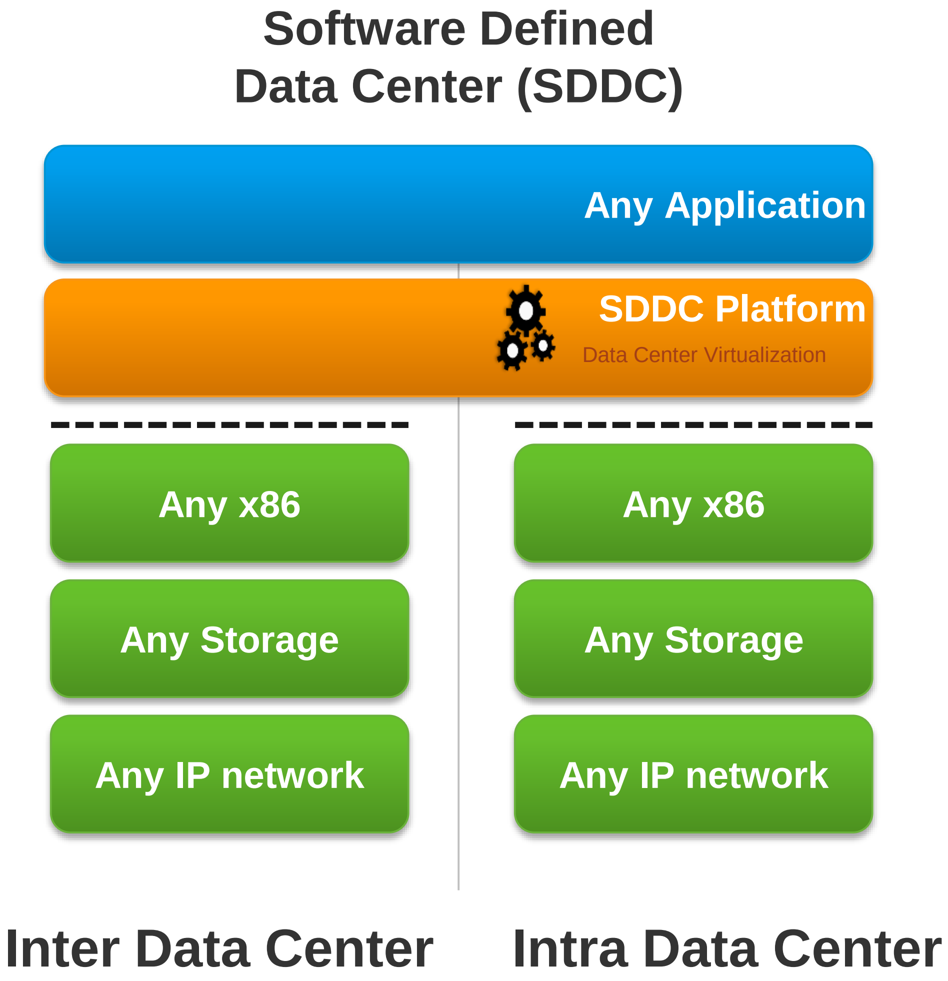
Any x86

Any Storage

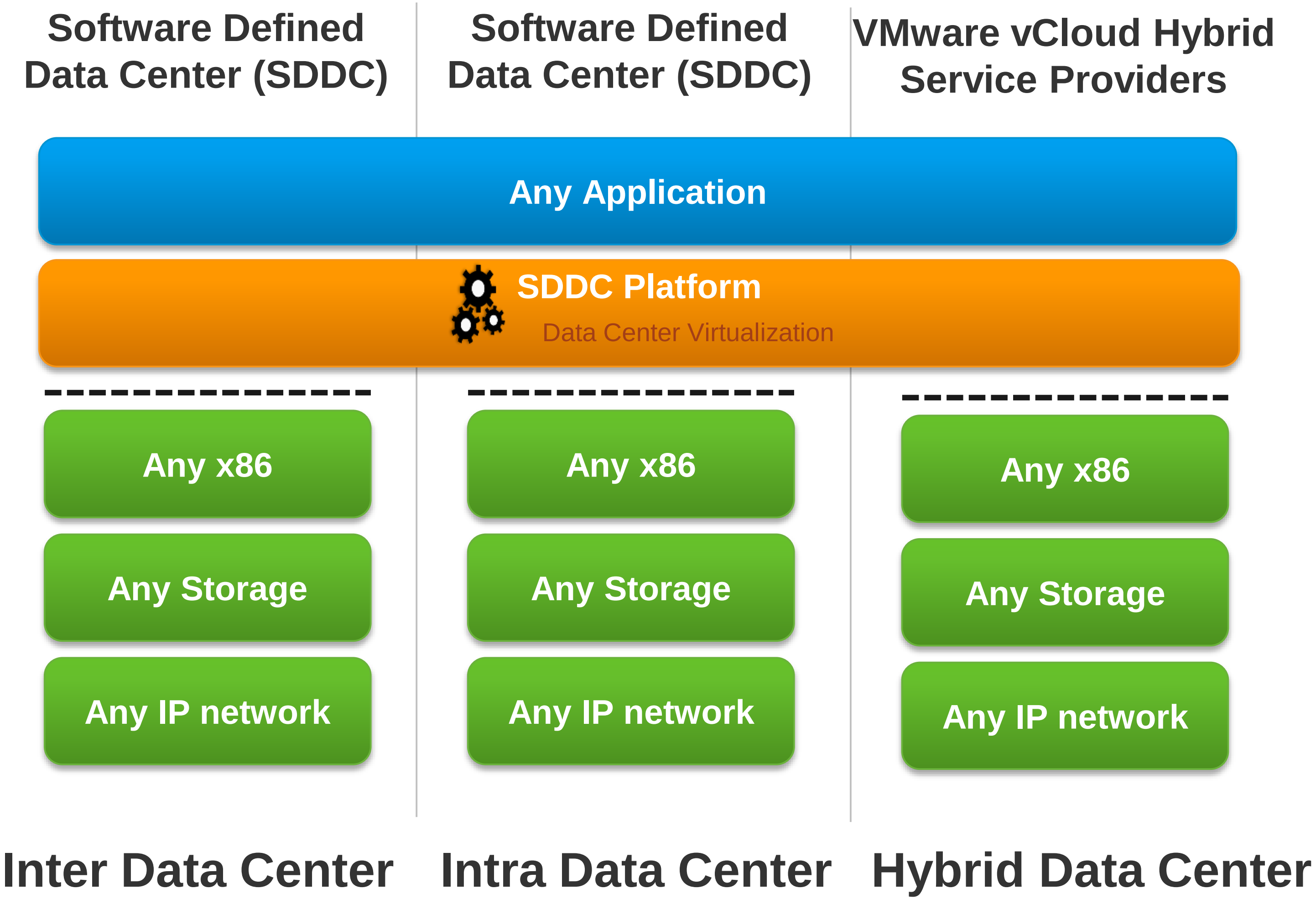
Any IP network

Intra Data Center

The Power of SDDC – Inter Data Center



The Power of SDDC – Hybrid Data Center



Software Defined Data Center (SDDC)

Software Defined Data Center (SDDC)

VMware vCloud Hybrid Service Providers

Any Application

SDDC Platform

Data Center Virtualization

Any x86

Any Storage

Any IP network

Any x86

Any Storage

Any IP network

Any x86

Any Storage

Any IP network

Inter Data Center

Intra Data Center

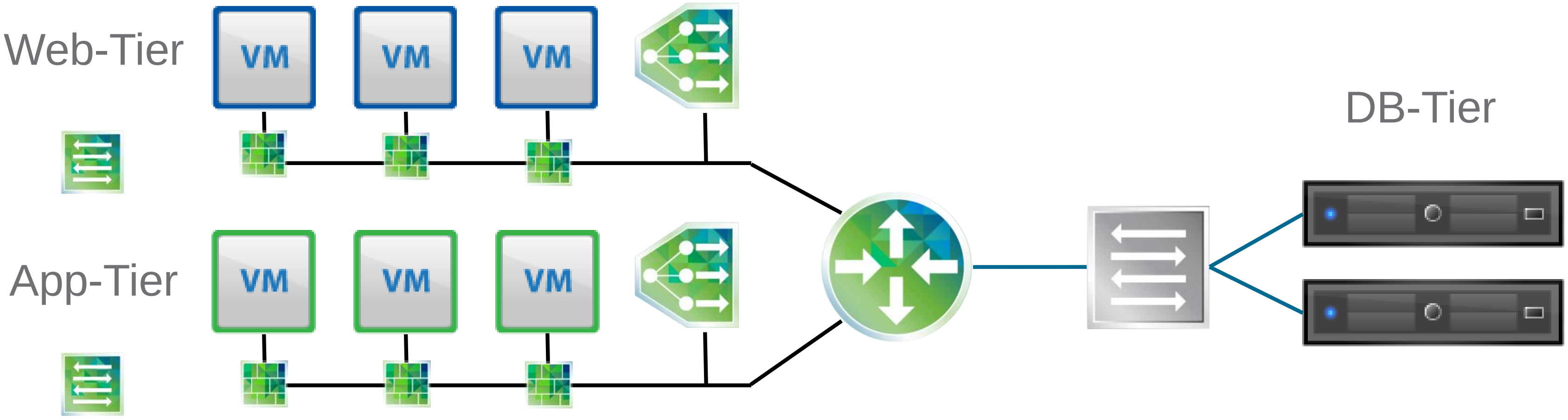
Hybrid Data Center

Provides

A Faithful Reproduction of Network & Security Services in Software

- Switching
- Routing
- Firewalling
- Load Balancing
- VPN
- Connectivity to Physical

Creating Sophisticated Application Topologies

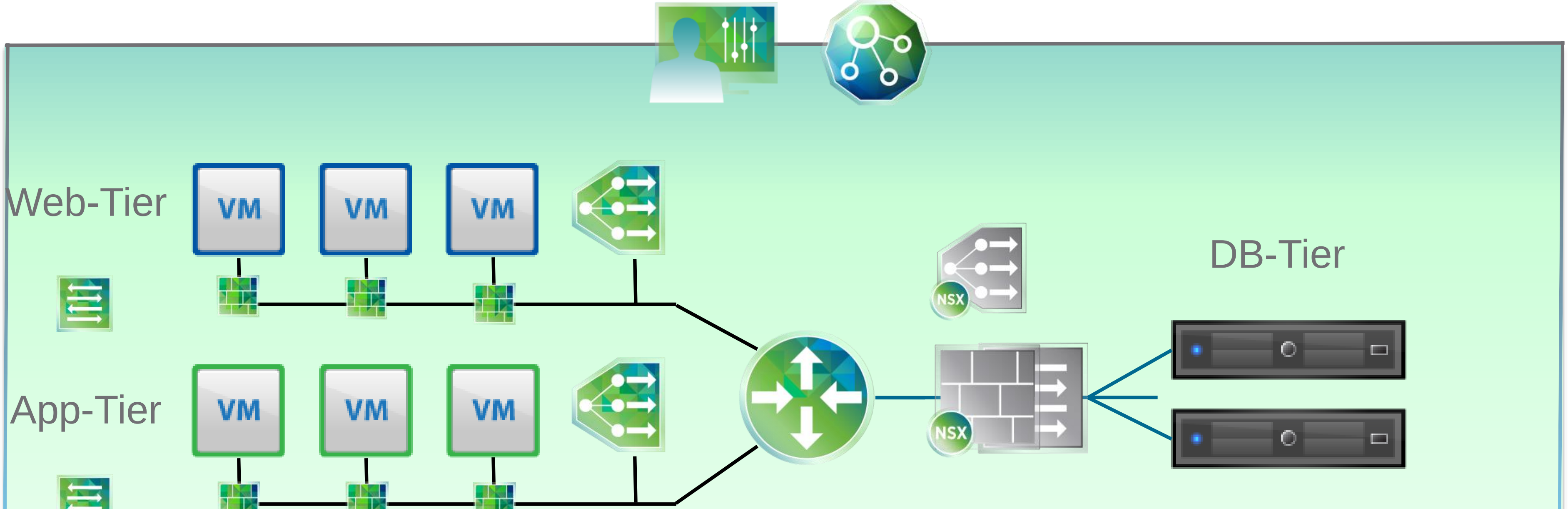


VMs Connect to Virtual Networks

Security Enforcement at vnic level

Virtual Networks Connect to Physical Workloads

Creating Sophisticated Application Topologies



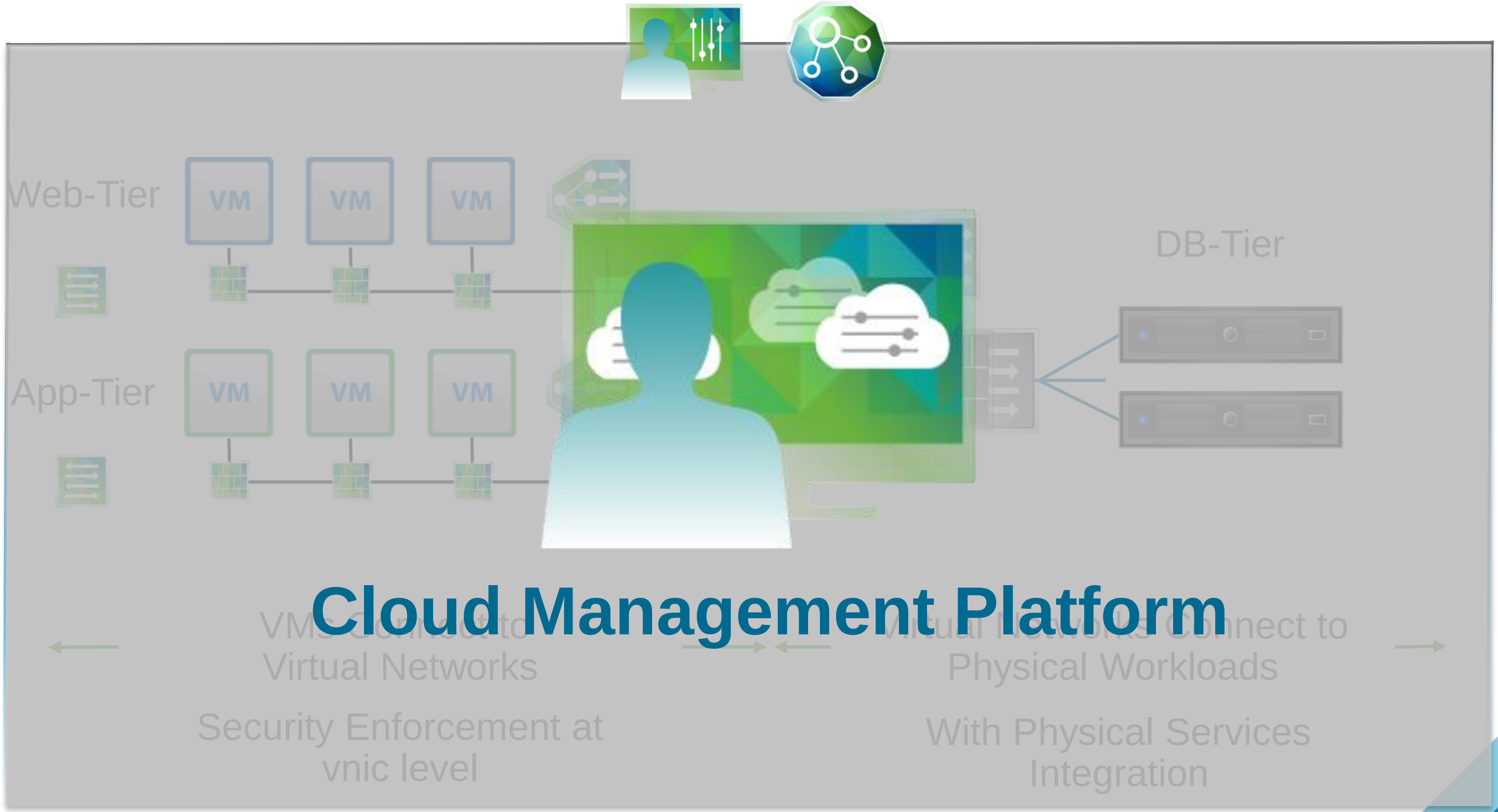
VMs Connect to Virtual Networks

Security Enforcement at vnic level

Virtual Networks Connect to Physical Workloads

With Physical Services Integration

On-Demand Application Deployment



Cloud Management Platform

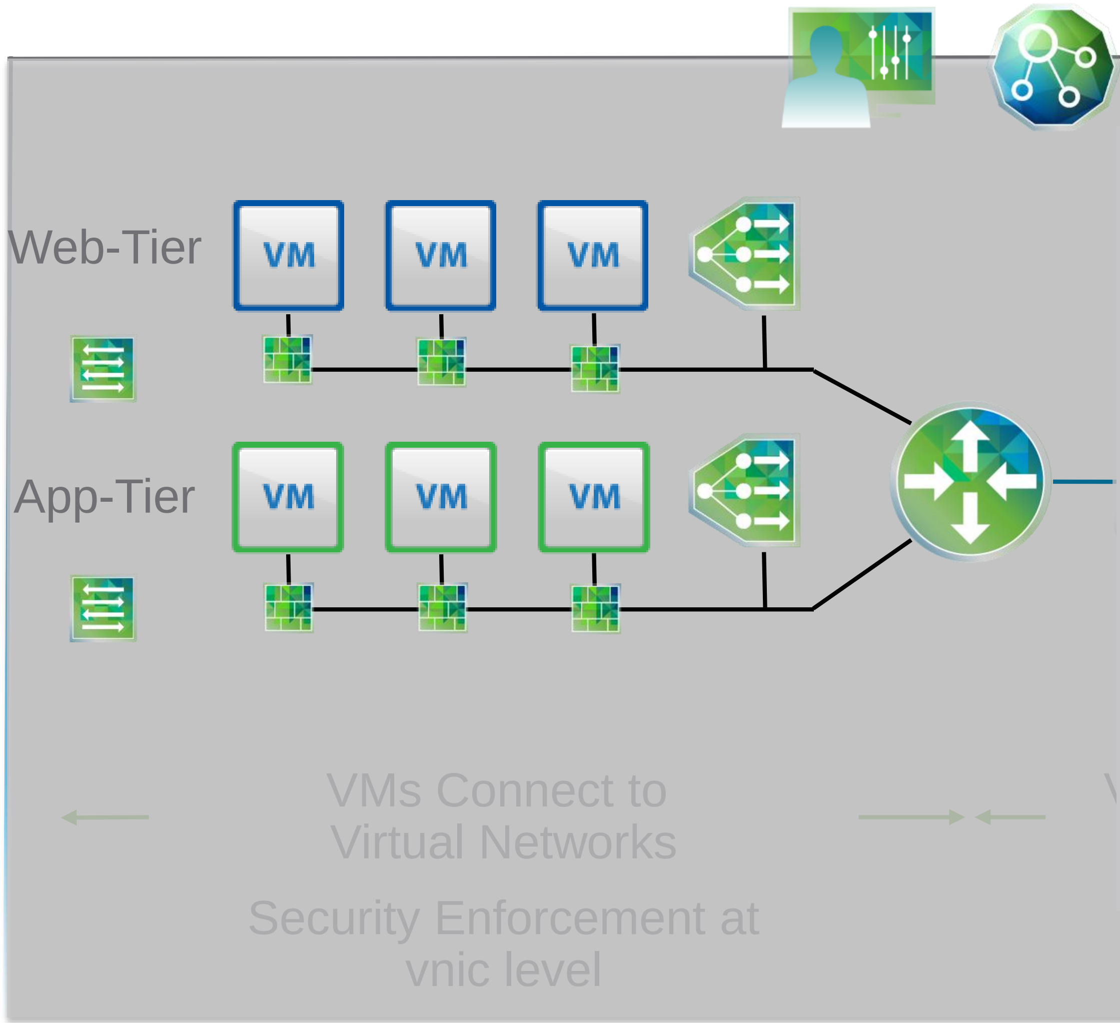
VMs Connect to Virtual Networks

Security Enforcement at vnic level

Virtual Networks Connect to Physical Workloads

With Physical Services Integration

Agenda



NSX Components

Switching

Routing

Security

Services

Putting it all Together

With Physical Services
Integration

Agenda

1 NSX Components

2 Switching

3 Routing

4 Security

5 Services

6 Putting it all Together

NSX Components

Logical Network

Cloud Consumption

- Self Service Portal
- vCloud Automation Center, OpenStack, Custom CMS

Management Plane

NSX Manager

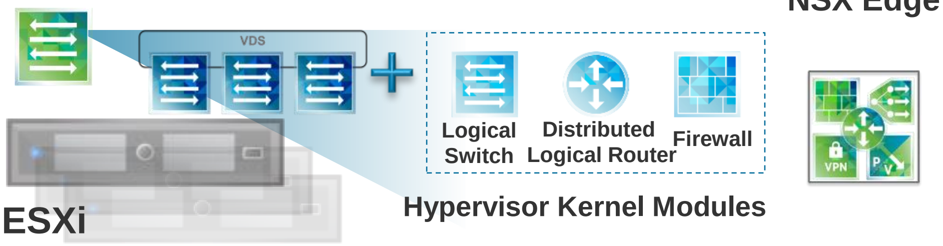
- Single configuration portal
- REST API entry-point

Control Plane

NSX Controller

- Manages Logical networks
- Control-Plane Protocol
- Separation of Control and Data Plane

Data Plane



Distributed Services

ESXi

Logical Switch

Distributed Logical Router

Firewall

Hypervisor Kernel Modules

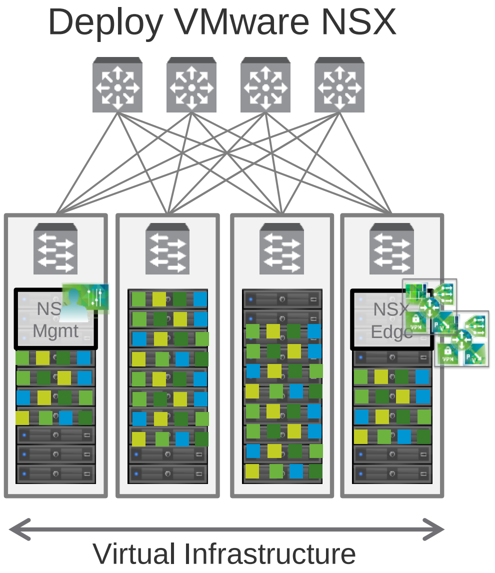
NSX Edge

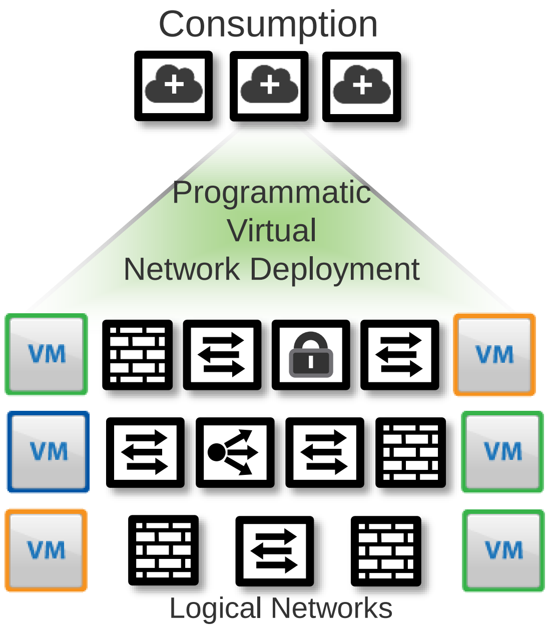
- High – Performance Data Plane
- Scale-out Distributed Forwarding Model

Physical Network

vmware®

Deploying VMware NSX





One Time

Component Deployment

1 **Deploy NSX Manager**

2 **Deploy NSX Controller Cluster**

Preparation

1 Host Preparation

2 Logical Network Preparation

Recurring

Logical Network/Security Services

1 Deploy Logical Switches per tier

2 Deploy Distributed Logical Router or connect to existing

3 Create Bridged Network

Agenda

1 NSX Components

2 Switching

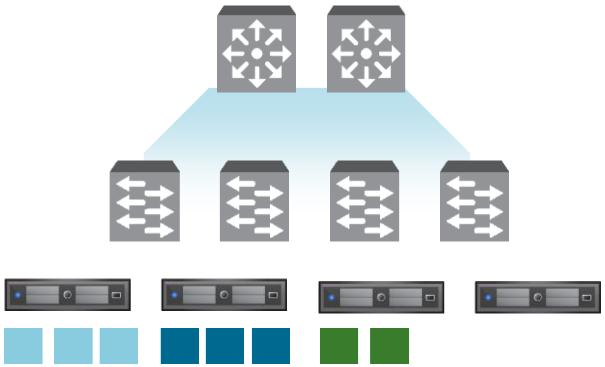
3 Routing

4 Security

5 Services

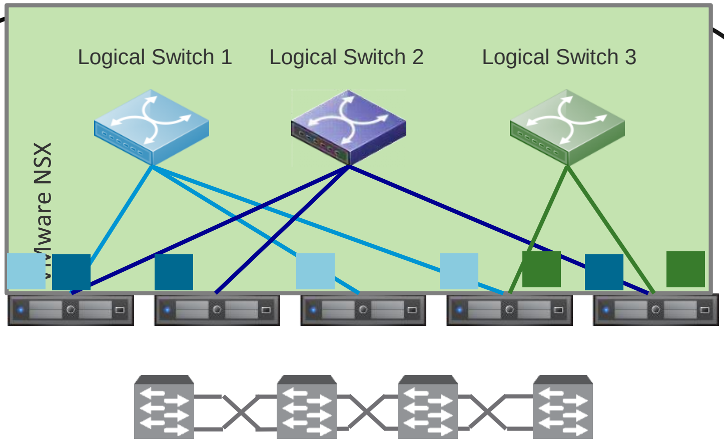
6 Putting it all Together

NSX Logical Switching



Challenges

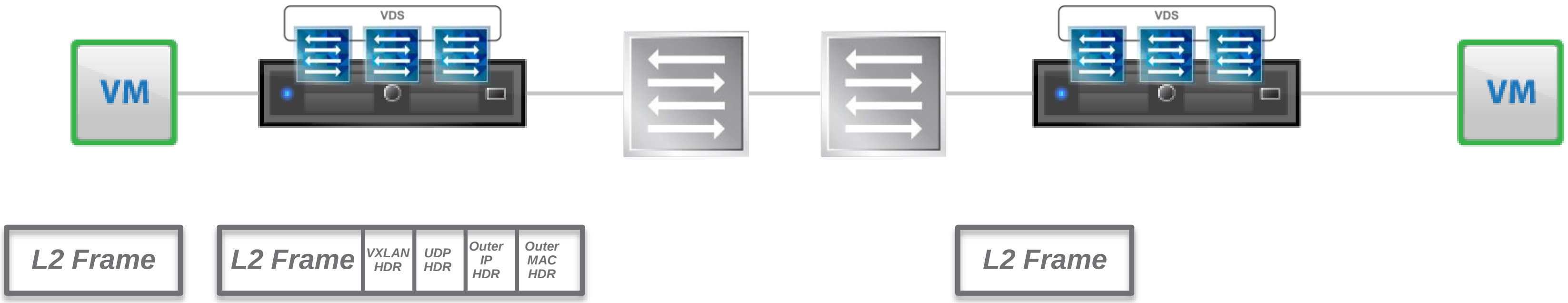
- Per Application/Multi-tenant segmentation
- VM Mobility requires L2 everywhere
- Large L2 Physical Network Sprawl – STP Issues
- HW Memory (MAC, FIB) Table Limits



Benefits

- Scalable Multi-tenancy across data center
- Enabling L2 over L3 Infrastructure
- Overlay Based with VXLAN, STT, GRE, etc,
- Logical Switches span across Physical Hosts and Network Switches

De-mystifying Overlay Networks



1

VM Sends a
standard L2 Frame

2

Source Hypervisor
(VTEP)
Adds VXLAN, UDP &
IP Headers

3

Physical Network
forwards frame as
standard IP frame

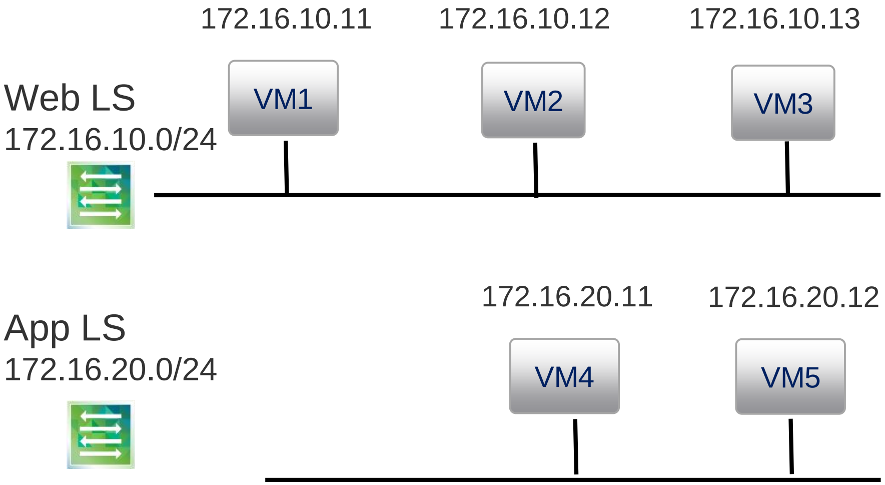
4

Destination
Hypevisor (VTEP)
de-encapsulates
headers

5

Original L2 Frame
delivered to VM

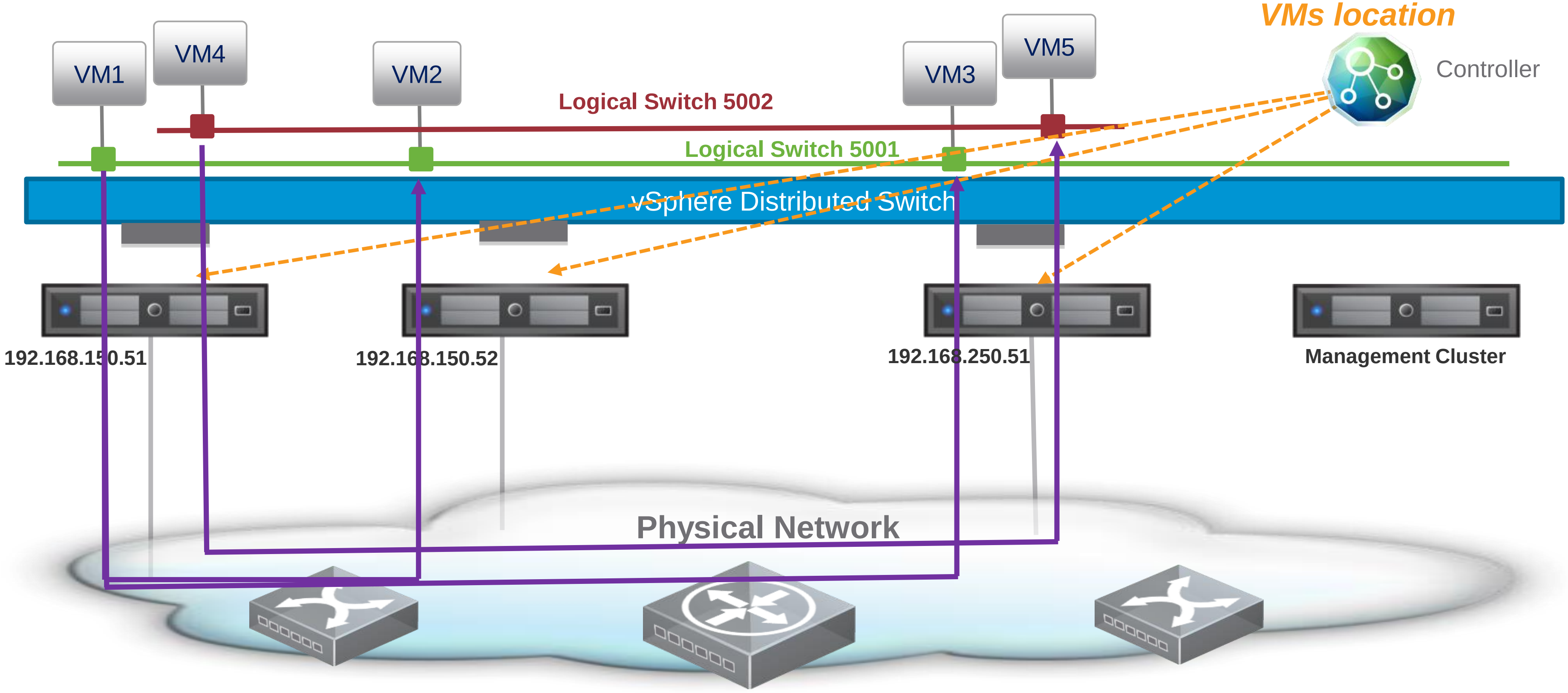
Logical View: Logical Switches



Physical View: Logical Switches

172.16.20.11 ➔ 172.16.20.12

Pushing remote VMs location



192.168.150.51 ➔ 192.168.250.52

[172.16.10.11 ➔ 172.16.10.12]

- - - ➔ L2 Control Plane Programming

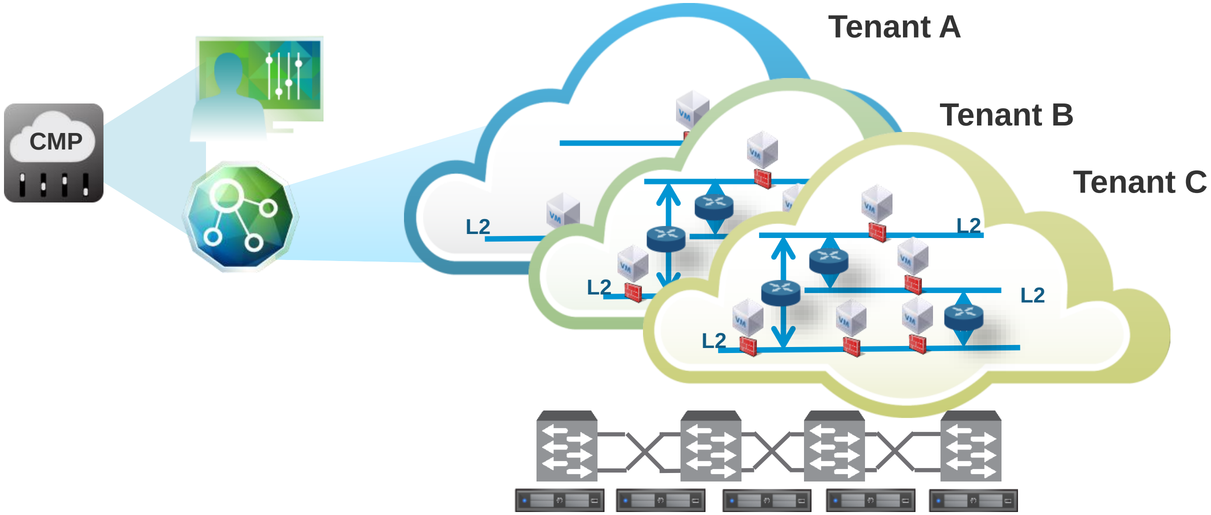
——➔ Data Plane

vmware®

Agenda

1. NSX Components
2. Switching
3. Routing
4. Security
5. Services
6. Putting it all Together

NSX Layer 3 Routing: Distributed, Feature-Rich



Challenges

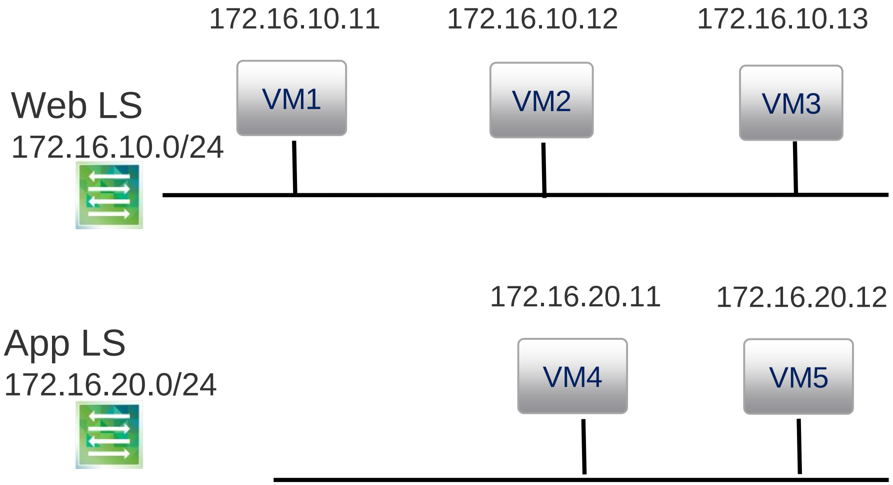
- Physical Infrastructure Scale Challenges – Routing Scale
- VM Mobility is a challenge
- Multi-Tenant Routing Complexity
- Traffic hair-pins

Benefits

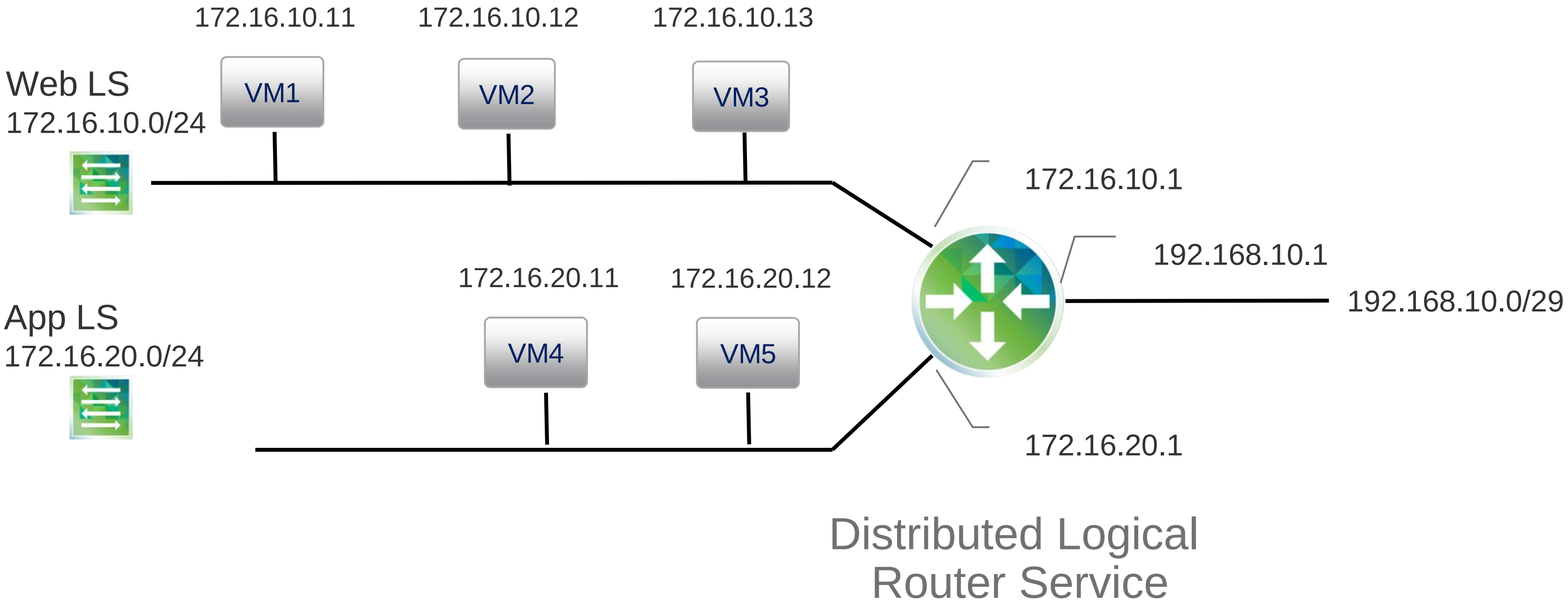
- Distributed Routing in Hypervisor
- Dynamic, API based Configuration
- Full featured – OSPF, BGP, IS-IS
- Logical Router per Tenant
- Routing Peering with Physical Switch

SCALABLE ROUTING – Simplifying Multi-tenancy

Logical View: VMs in a Single Logical Switch



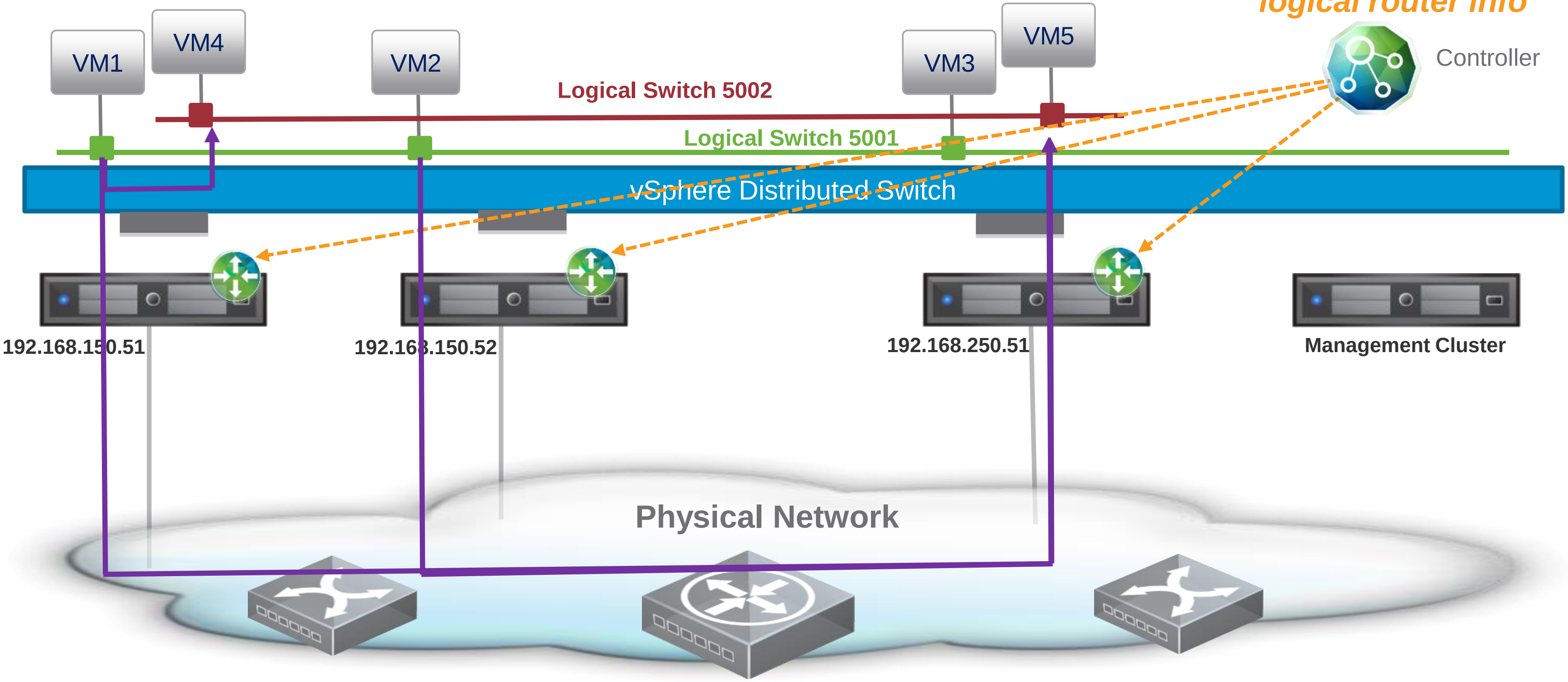
Logical View: Distributed Routing



Physical View: Distributed Routing

172.16.10.12 → 172.16.20.12

Pushing distributed logical router info



N/A

192.168.150.51 → 192.168.250.51

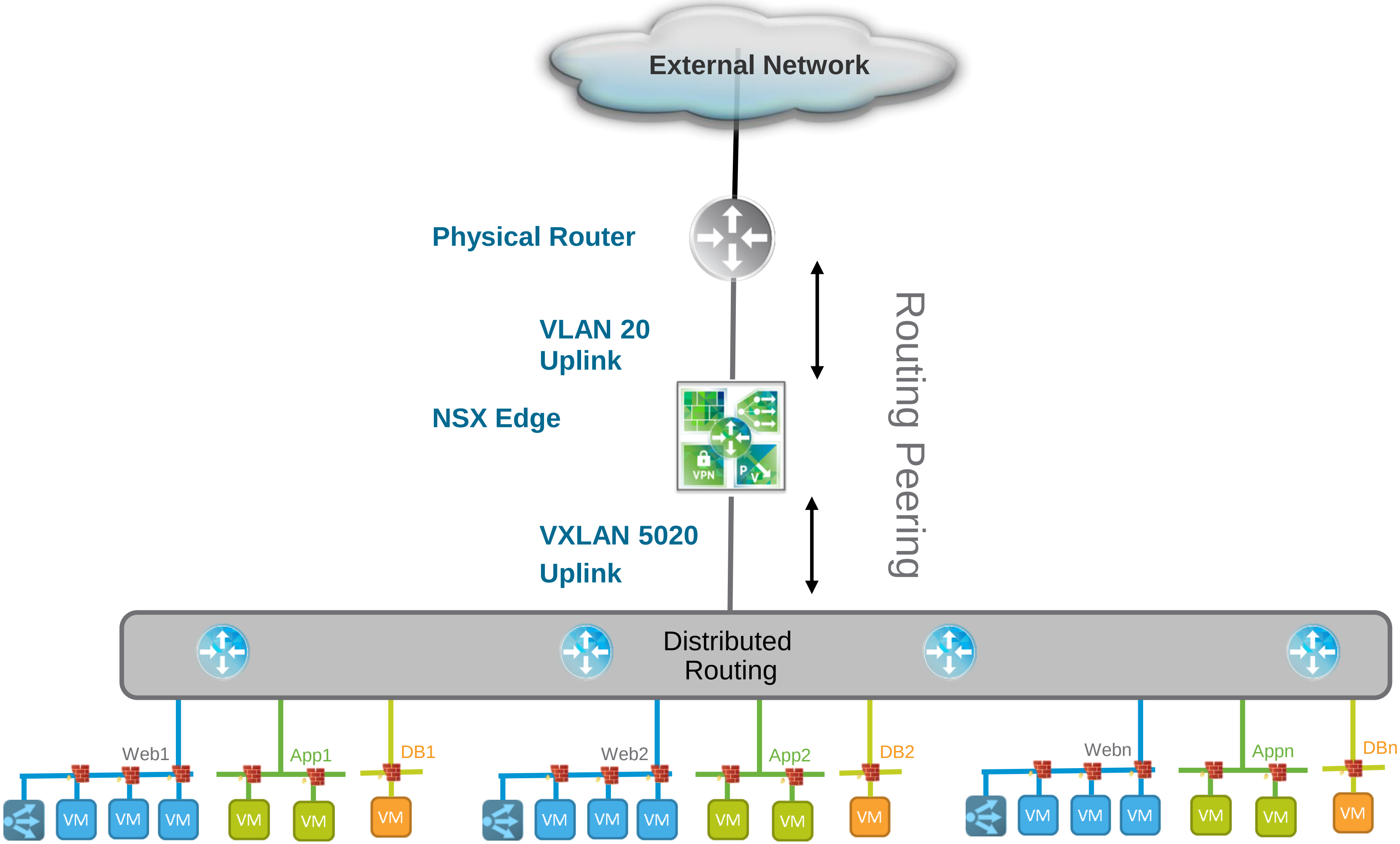
[*172.16.10.11 → 172.16.20.12*]

- - - → L3 Control Plane Programming

——→ Data Plane

vmware®

Example: Enterprise Routing Topology



External Network

Physical Router

VLAN 20
Uplink

NSX Edge

VXLAN 5020
Uplink

Routing Peering

Distributed
Routing

Agenda

1 NSX Components

2 Switching

3 Routing

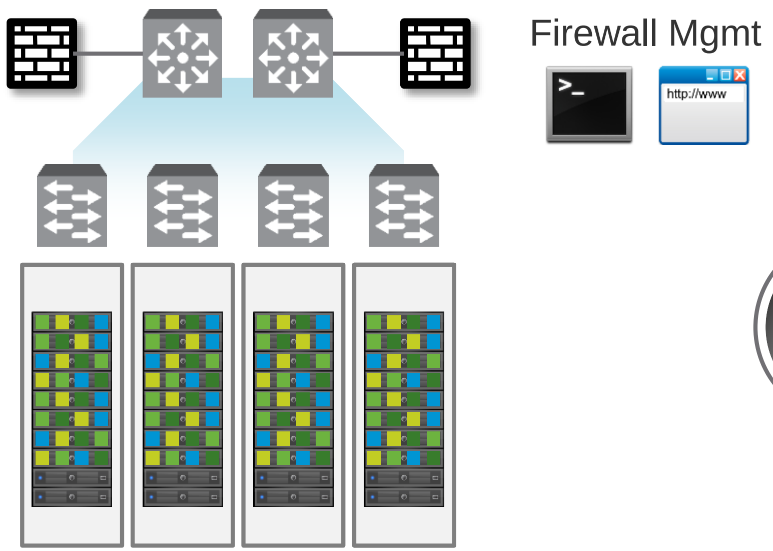
4 Security

5 Services

6 Putting it all Together

NSX Distributed Firewalling

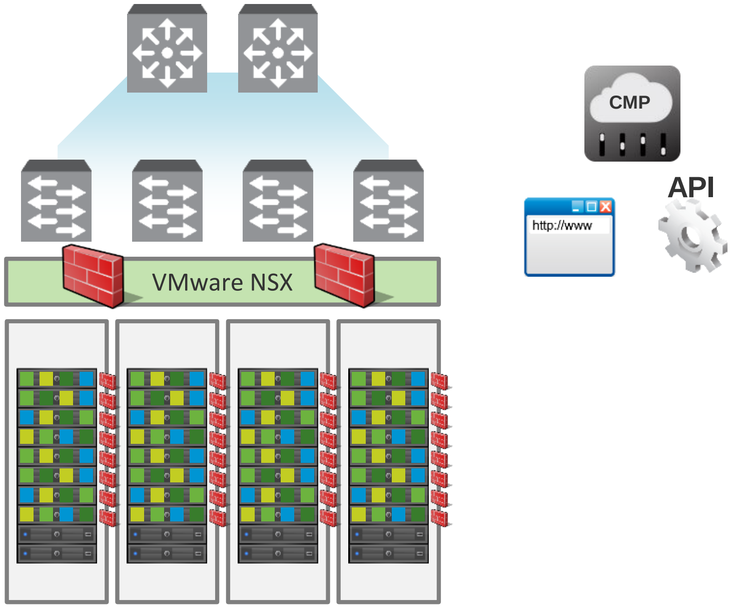
PHYSICAL SECURITY MODEL



Challenges

- Centralized Firewall Model
- Static Configuration
- IP Address based Rules
- 40 Gbps per Appliance
- Lack of visibility with encapsulated traffic

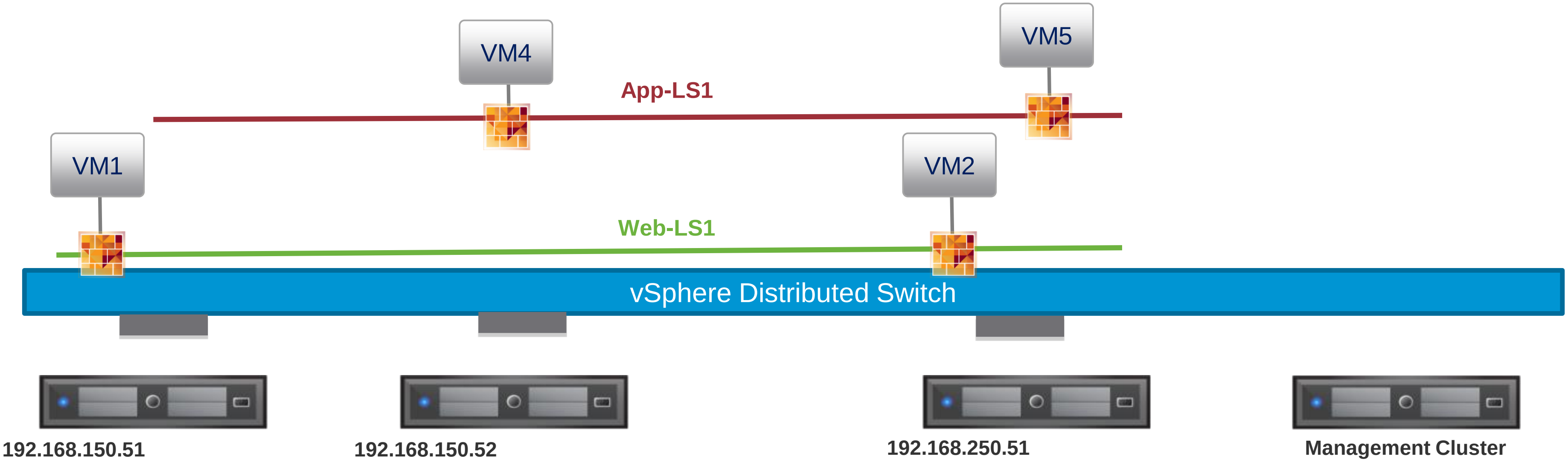
DISTRIBUTED FIREWALLING



Benefits

- Distributed at Hypervisor Level
- Dynamic, API based Configuration
- VM Name, VC Objects, Identity-based Rules
- Line Rate ~20 Gbps per host
- Full Visibility to encapsulated traffic

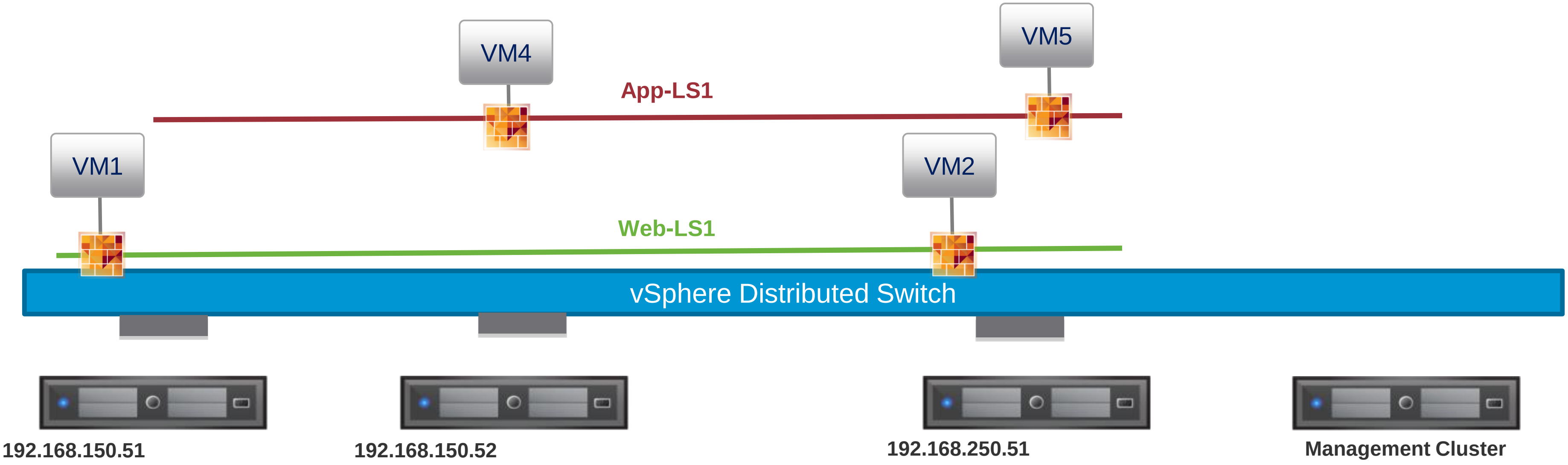
Distributed Firewall Features

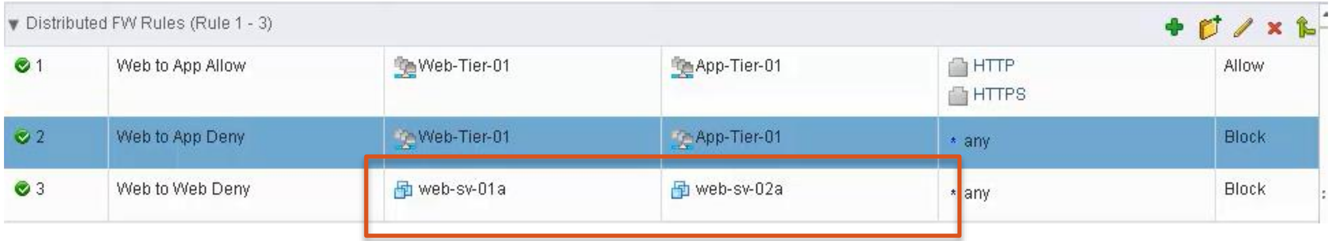


Capabilities

- Firewall rules are enforced at VNIC Level
- Policy independent of location (L2 or L3 adjacency)
- State persistent across vMotion
- Enforcement based on VM attributes like Tags, VM Names, Logical Switch, etc

Distributed Firewall Rules



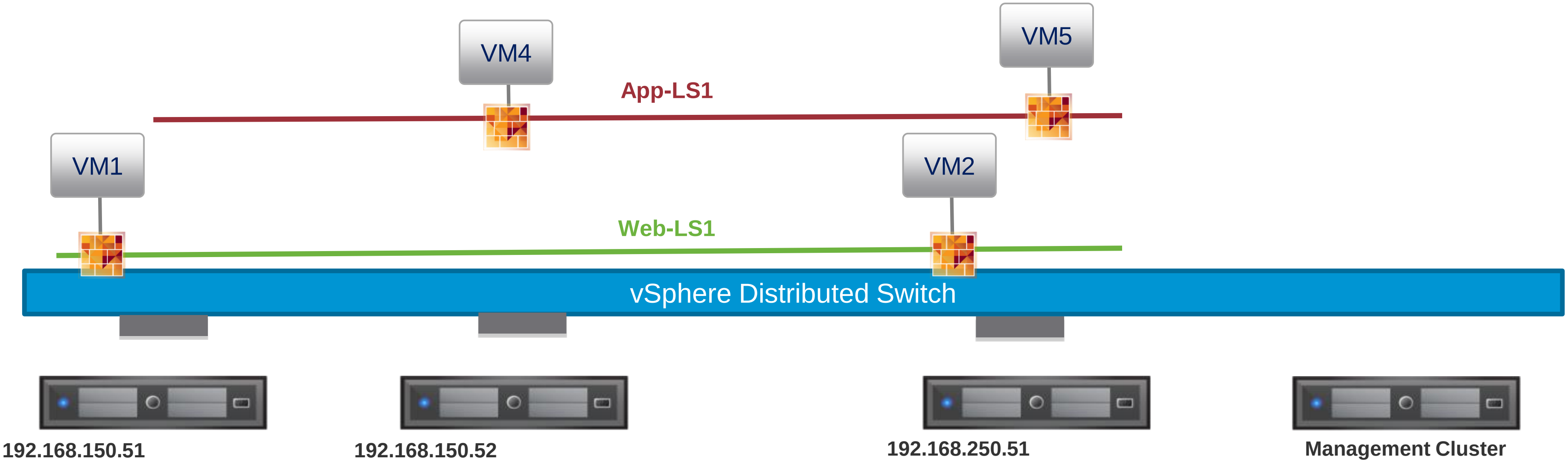


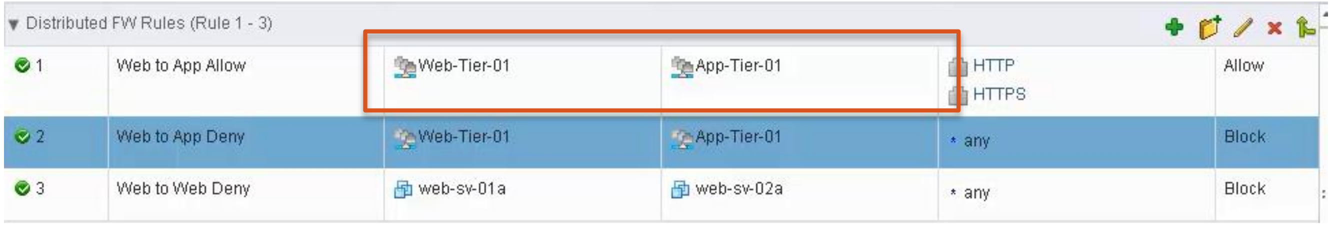
▾ Distributed FW Rules (Rule 1 - 3)

✓ 1	Web to App Allow	Web-Tier-01	App-Tier-01	HTTP HTTPS	Allow
✓ 2	Web to App Deny	Web-Tier-01	App-Tier-01	* any	Block
✓ 3	Web to Web Deny	web-sv-01a	web-sv-02a	* any	Block

Rules Based on VM Names

Distributed Firewall Rules

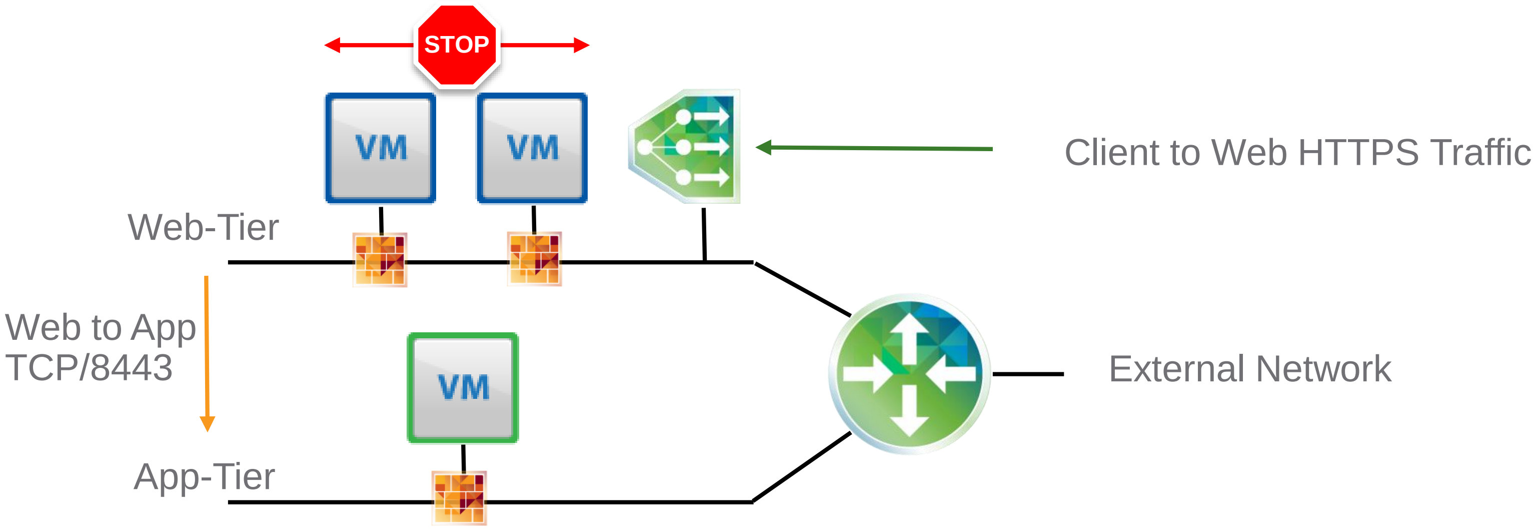



▾ Distributed FW Rules (Rule 1 - 3)

✓ 1	Web to App Allow	Web-Tier-01	App-Tier-01	HTTP HTTPS	Allow
✓ 2	Web to App Deny	Web-Tier-01	App-Tier-01	* any	Block
✓ 3	Web to Web Deny	web-sv-01a	web-sv-02a	* any	Block

Rules Based on Logical Switches

Example Building a Web DMZ

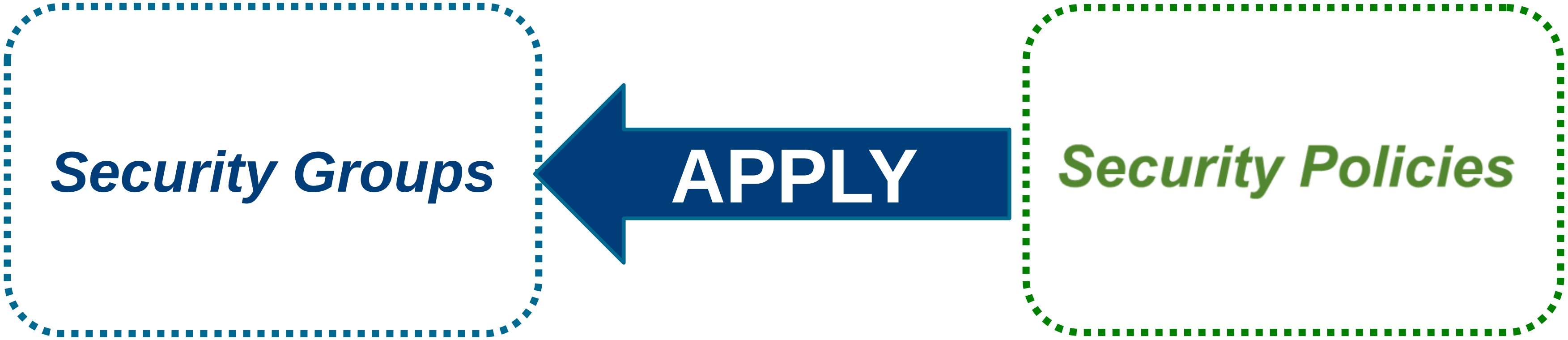


Source	Destination	Service	Policy
Web-VM1	Web-VM2		Block
Any	Web-Tier LS	HTTPS	Allow
Any	Web-Tier LS		Block
Web-Tier LS	App-Tier LS	TCP 8443	Allow
Any	App-Tier LS		Block

Define security policies based on service profiles already defined by the security team. Apply these policies to one or more security groups where your workloads are members.

WHAT you want to protect

HOW you want to protect it



Security Groups

APPLY

Security Policies

Members (VM, vNIC…) and **Context** (user identity, security posture)

Services (Firewall, antivirus…) and **Profiles (**labels representing specific policies)

Security Group

Containers – Grouping of VMs, IPs, and more…to define WHAT you want to protect.

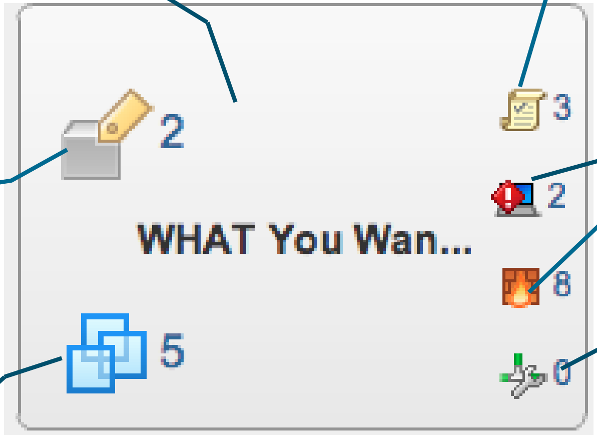
e.g. "Financial Applications", "Desktop Users", "Quarantine Zone"

Policies – collection of service profiles - assigned to this container…to define HOW you want to protect this container

e.g. "PCI Compliance" or "Quarantine Policy'

Nested containers – other groupings within the container

e.g. "Quarantine Zone" is a sub group within "My Data Center"



Service profiles for *deployed* services, assigned to these policies

Services supported today:

- Distributed Virtual Firewall
- Anti-virus
- Vulnerability Management
- Network IPS
- Data Security (DLP scan)
- User Activity Monitoring
- File Integrity Monitoring

VMs (workloads) that belong to this container.

e.g. "Apache-Web-VM", "Exchange Server-VM"

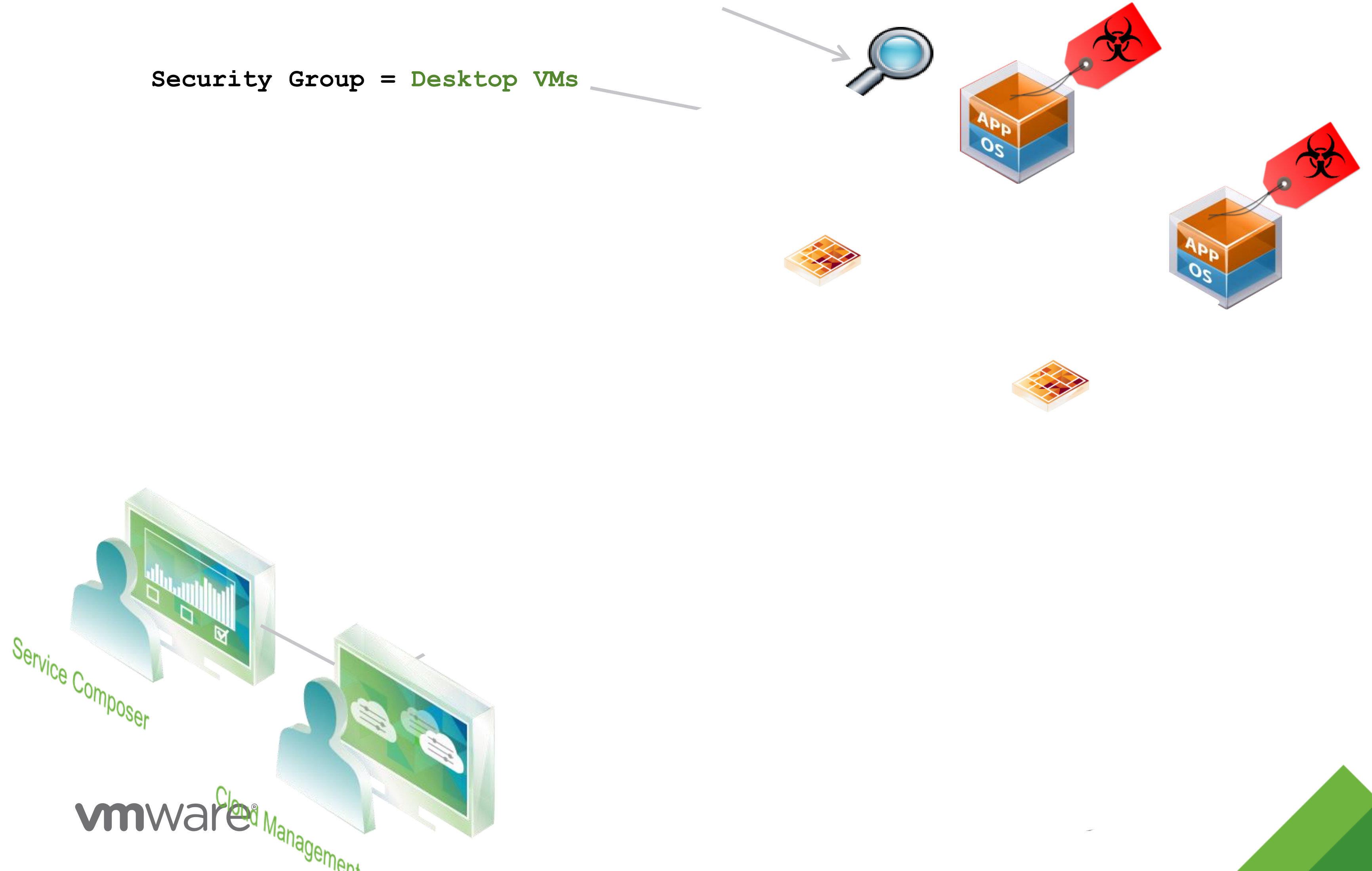
vmware®

Automated Security with Service Composer

Quarantine Vulnerable Systems until Remediated

Security Group = Quarantine Zone
Members = {Tag = ‘ANTI_VIRUS.VirusFound’, L2 Isolated Network}

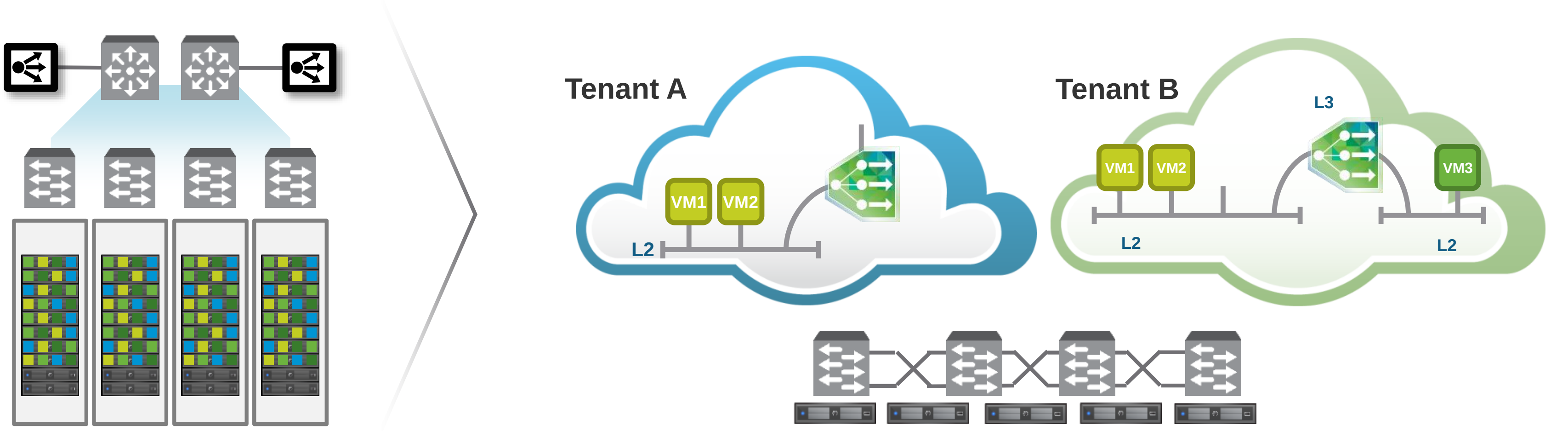
Security Group = Desktop VMs



Agenda

1	NSX Components
2	Switching
3	Routing
4	Security
5	Services
6	Putting it all Together

VMware NSX Load Balancing



Challenges

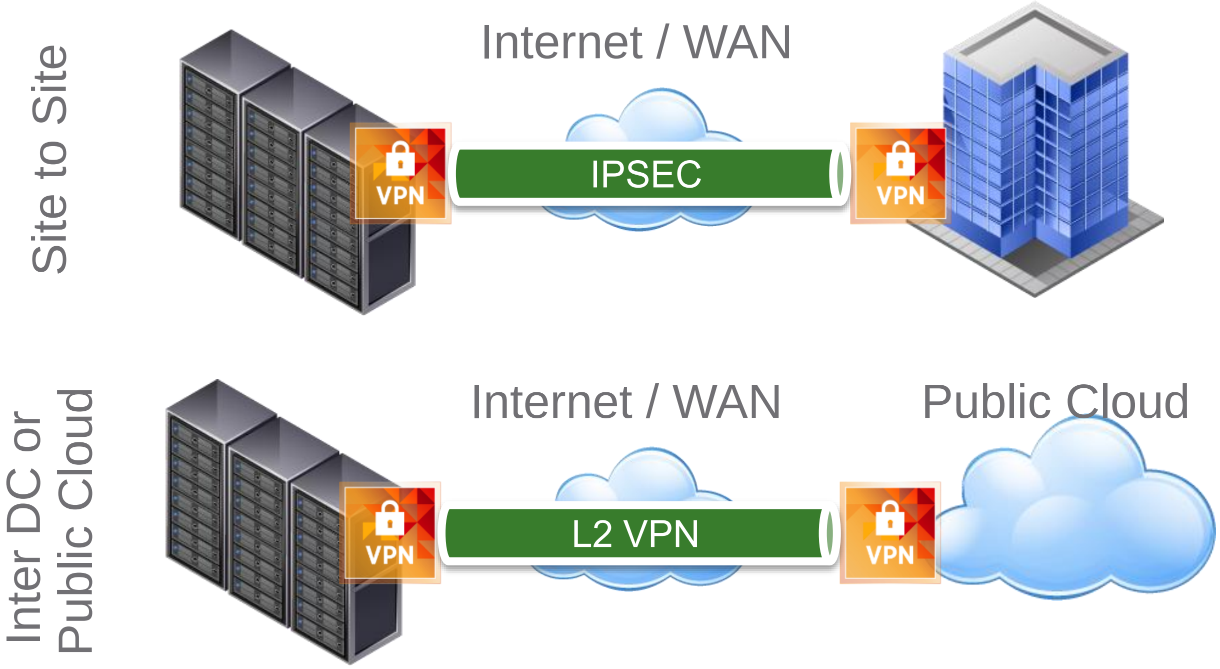
- Application Mobility
- Multi-tenancy
- Configuration complexity – manual deployment model

Benefits

- On-demand load balancer service
- Simplified deployment model for applications – one-arm or inline
- Layer 7, SSL, …

LOAD BALANCER – Per Tenant Application Availability Model

NSX Logical VPN Services



- VPN Services are delivered as a service via Edge
- Interoperable with IPSec Clients
- Hardware Offload for Performance
- Ability to extend L2 across sites for active-active DC

Agenda

1 NSX Components

2 Switching

3 Routing

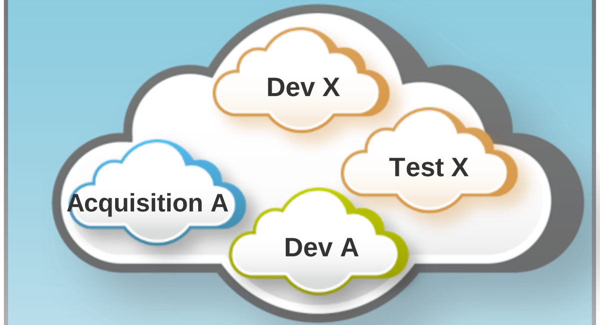
4 Security

5 Services

6 Putting it all Together

VMware NSX – Deployment Use Cases

Self-Service IT



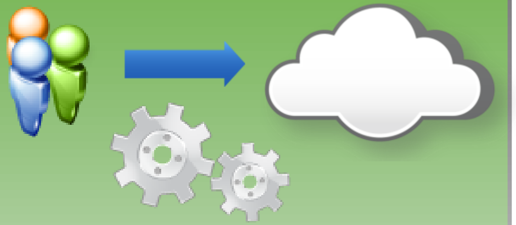
Examples

DevOps Cloud
On-boarding M&A

Key Capabilities

Application specific networking
Flexible IP Address Mgmt
Simplified consumption

Data Center Automation



Examples

Micro-segmentation of App
Simplifying Compute Silos
DMZ Deployments

Key Capabilities

Programmatic Consumption
Full featured stack
Visibility and ops

Public Clouds

Examples

XaaS Clouds
Vertical Clouds

Key Capabilities

Multi-tenant Deployment
Programmatic L2, L3, Security
Overlapping IP Addressing
Any Hypervisor, Any CMP

Your cloud service automation solution CAN spin up and tear down logical networks and services on-demand, with configurable options and with optimal value.

Got my machines. Now I’m in business. Thanks!

Business User

I saved a lot of time, too. Now I can work on other stuff.

VI Admin / Cloud Operator

I’ve got visibility and control over virtual network infrastructure. No complaints here.

Network Architect

What's Next ..

Play

VMware NSX
Hands-on Labs

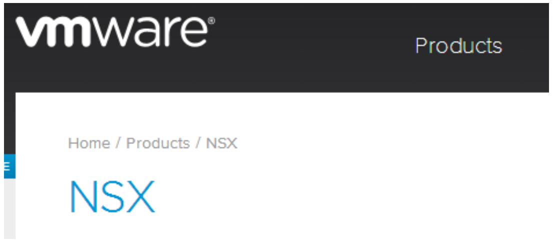
labs.hol.vmware.com

Learn

vmware | BLOGS

Home > Blogs > The Network Virtualization Blog

The Network Virtualization Blog



vmware Products

Home / Products / NSX

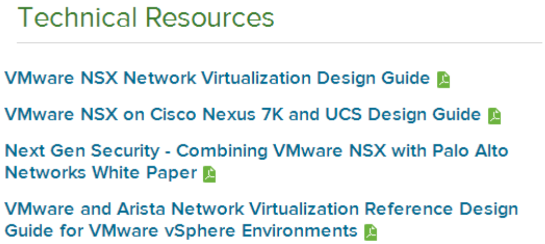
NSX

Network Virtualization Blog
blogs.vmware.com/networkvirtualization

NSX Landing Page
www.vmware.com/go/nsx

Whitepapers

Deploy



Technical Resources

- VMware NSX Network Virtualization Design Guide
- VMware NSX on Cisco Nexus 7K and UCS Design Guide
- Next Gen Security - Combining VMware NSX with Palo Alto Networks White Paper
- VMware and Arista Network Virtualization Reference Design Guide for VMware vSphere Environments

NSX Technical Resources
www.vmware.com/products/nsx/resources.html

Reference Designs

Thank You

vmware®