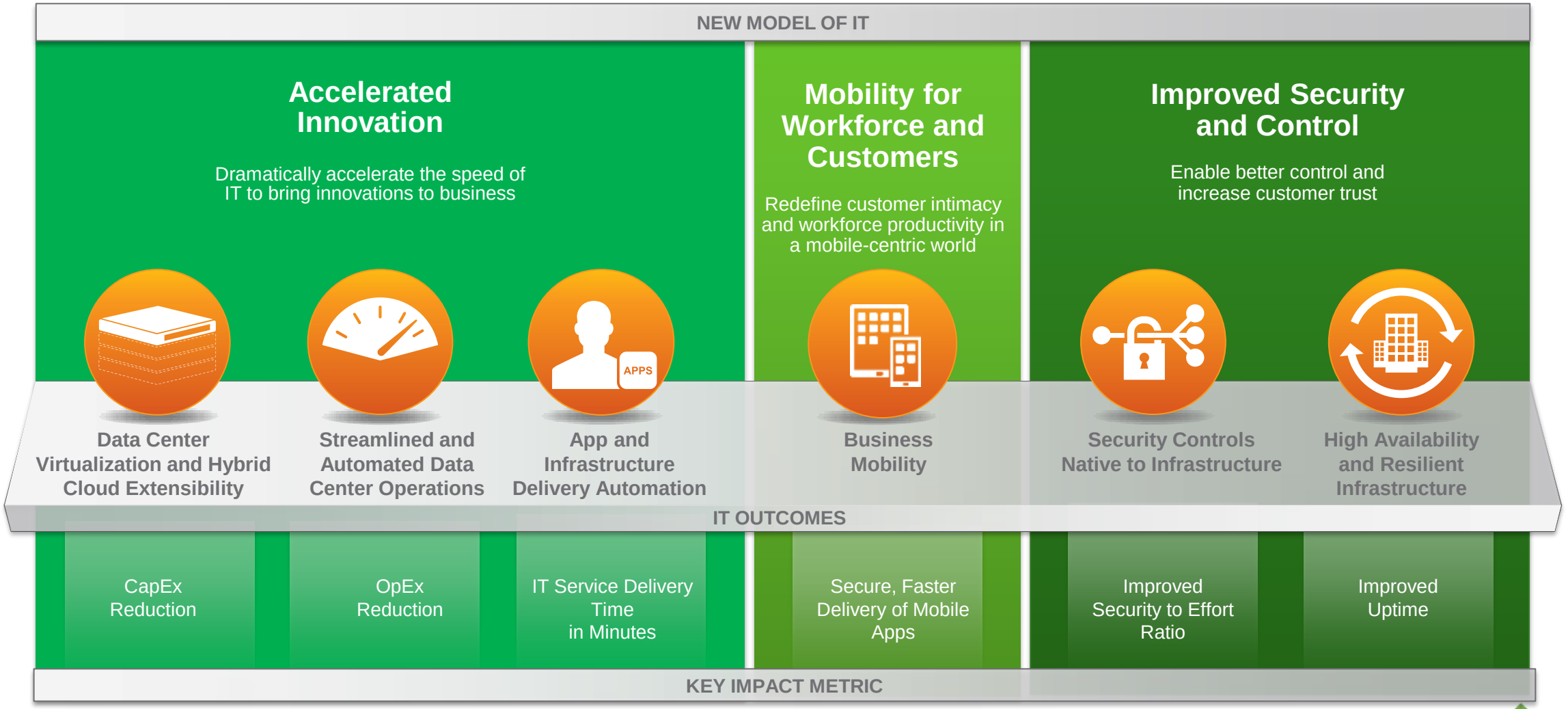
NSX - La piattaforma di sicurezza e virtualizzazione di rete

Luca Morelli
Sr. Systems Engineer @ VMware

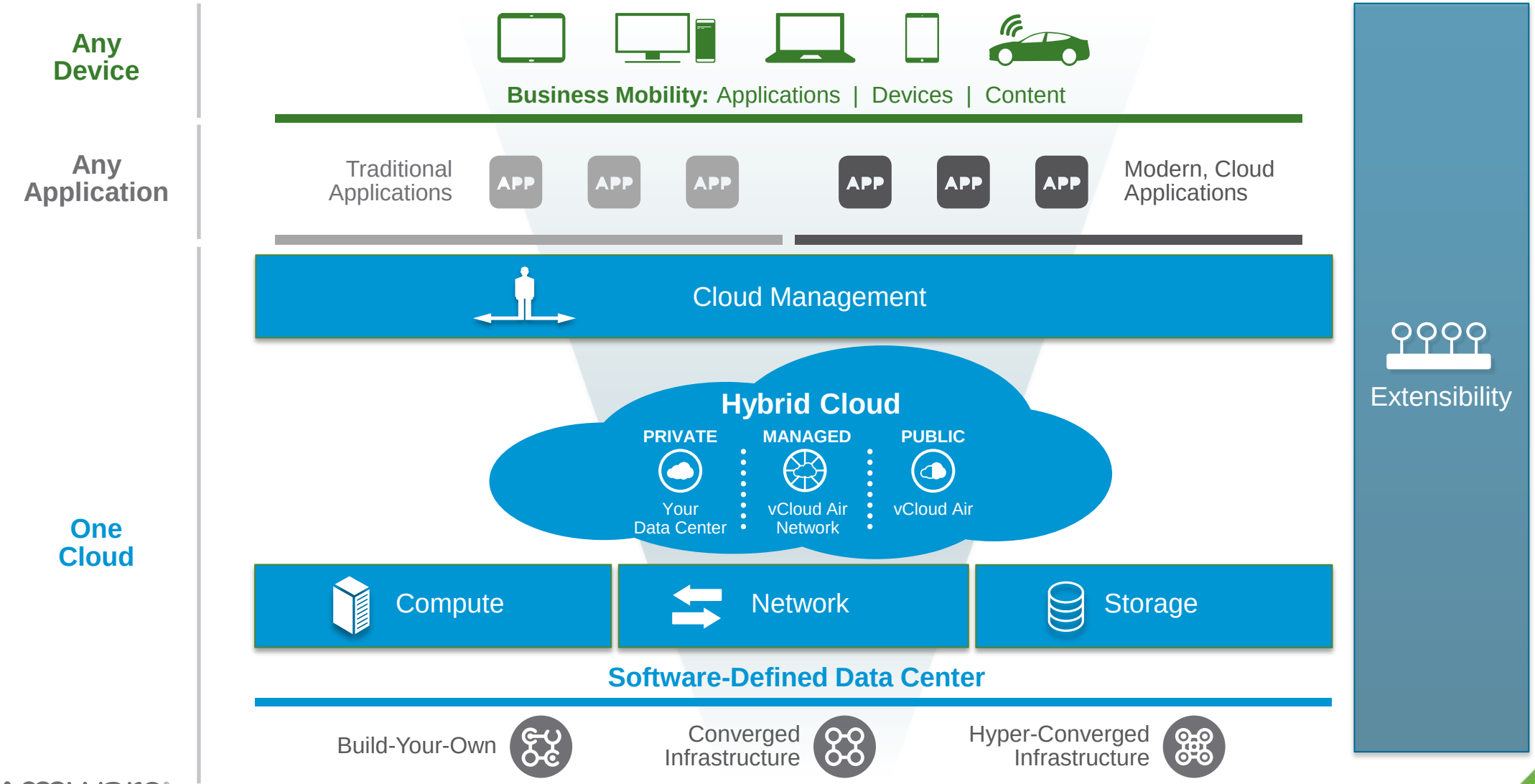
Agenda

1	La Visione di VMware nel Software Defined Data Center
2	Introduzione alla Virtualizzazione di Rete con NSX
3	Il Paradigma della Micro-Segmentazione
4	Principali Casi d’Uso

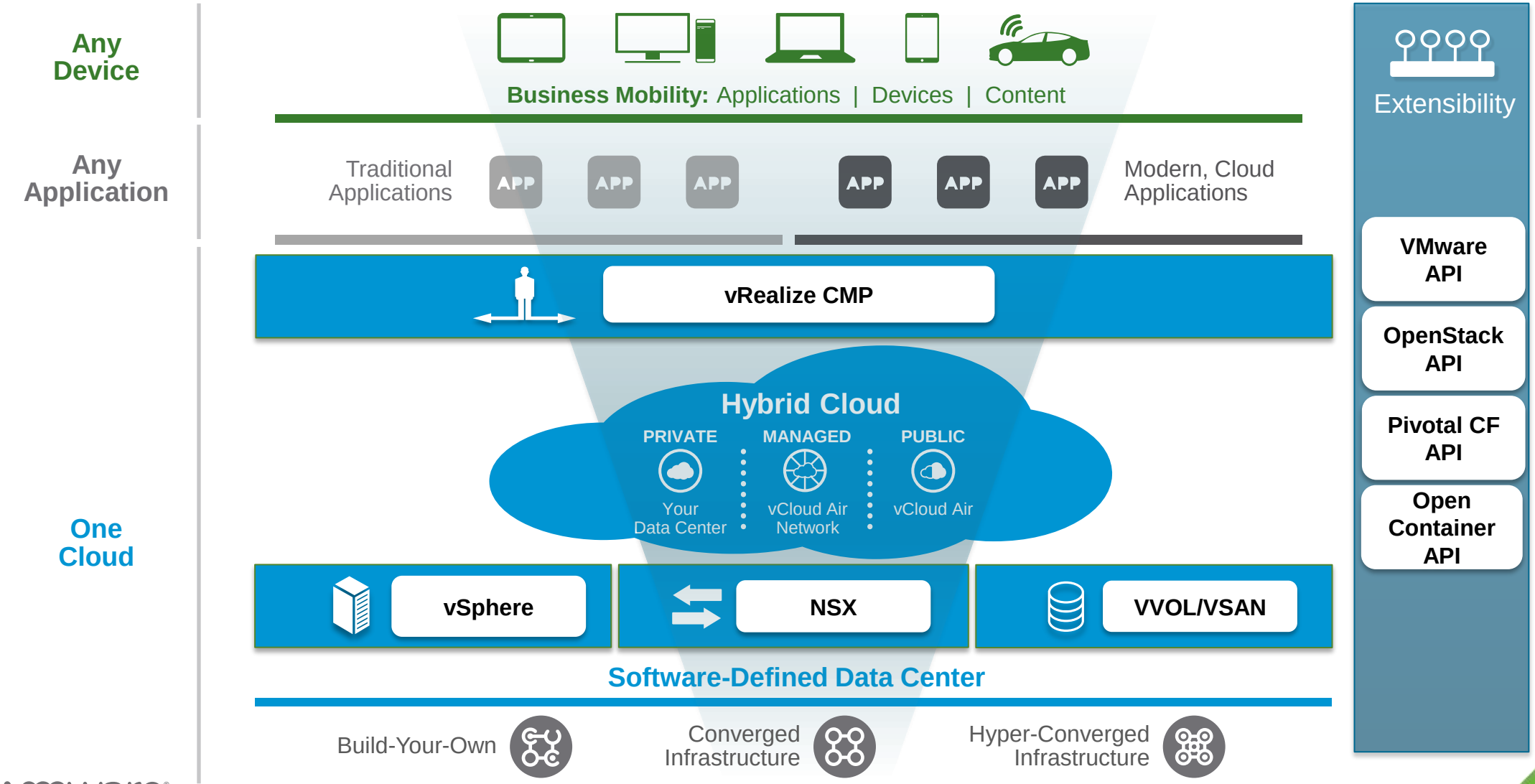
Outcomes Delivered by the New Model of IT



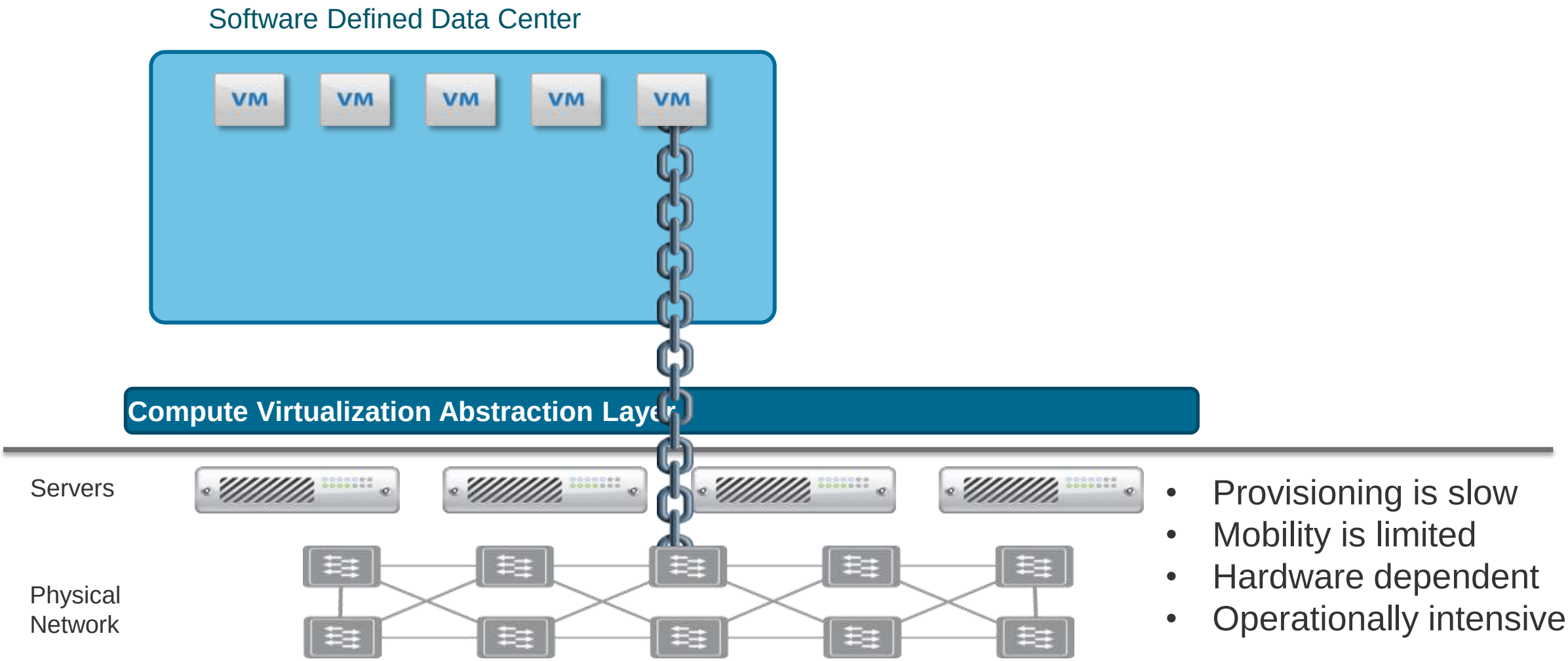
Software-Defined Data Center (SDDC): The Foundation of the New Model of IT



Software-Defined Data Center (SDDC): The Foundation of the New Model of IT



The Network Is a Barrier to Software Defined Data Center!!



- Provisioning is slow
- Mobility is limited
- Hardware dependent
- Operationally intensive

NSX - Distributed Services in the Hypervisor

Automated operational model of the SDDC

Applications

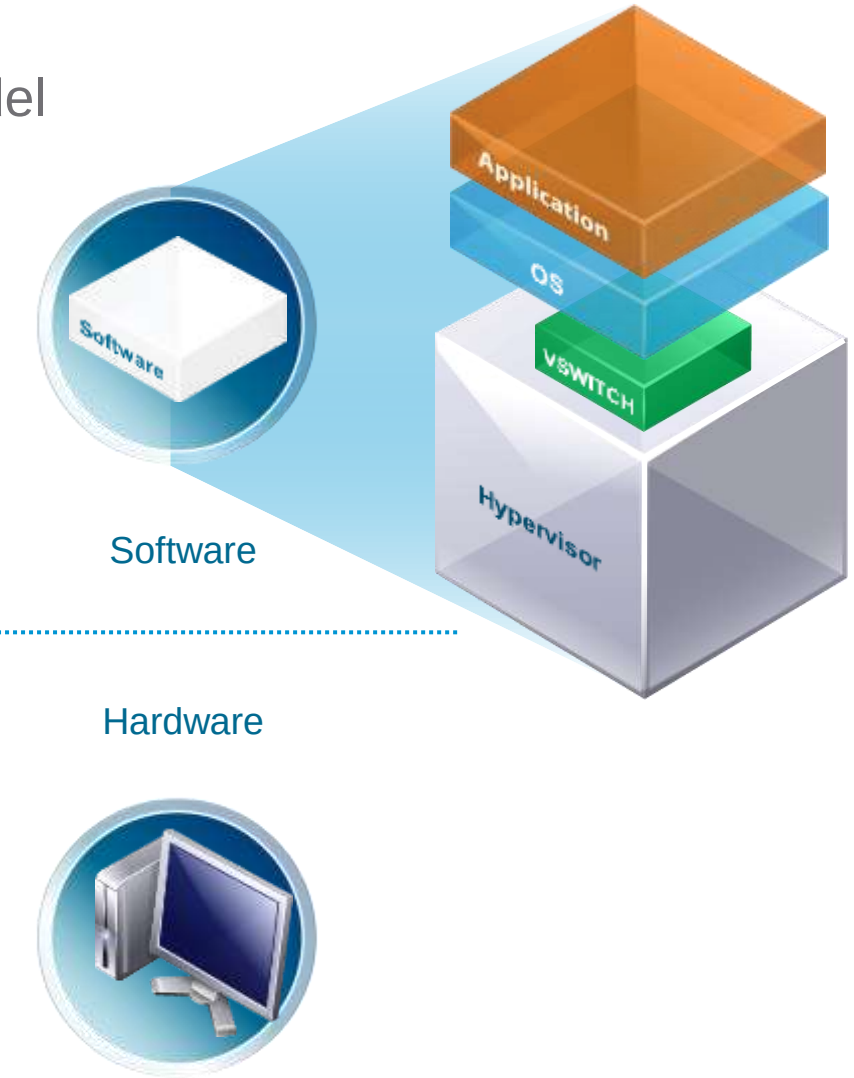
Virtual Machines	Virtual Networks	Virtual Storage

Data Center Virtualization

Compute Capacity	Network Capacity	Storage Capacity

Pooled compute, network and storage capacity; Vendor independent, best price/perf; Simplified config and mgt.

Location Independence

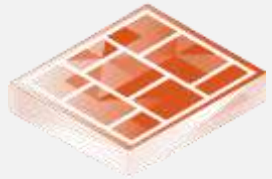


Network & Security Services Now in the Hypervisor

Load Balancing

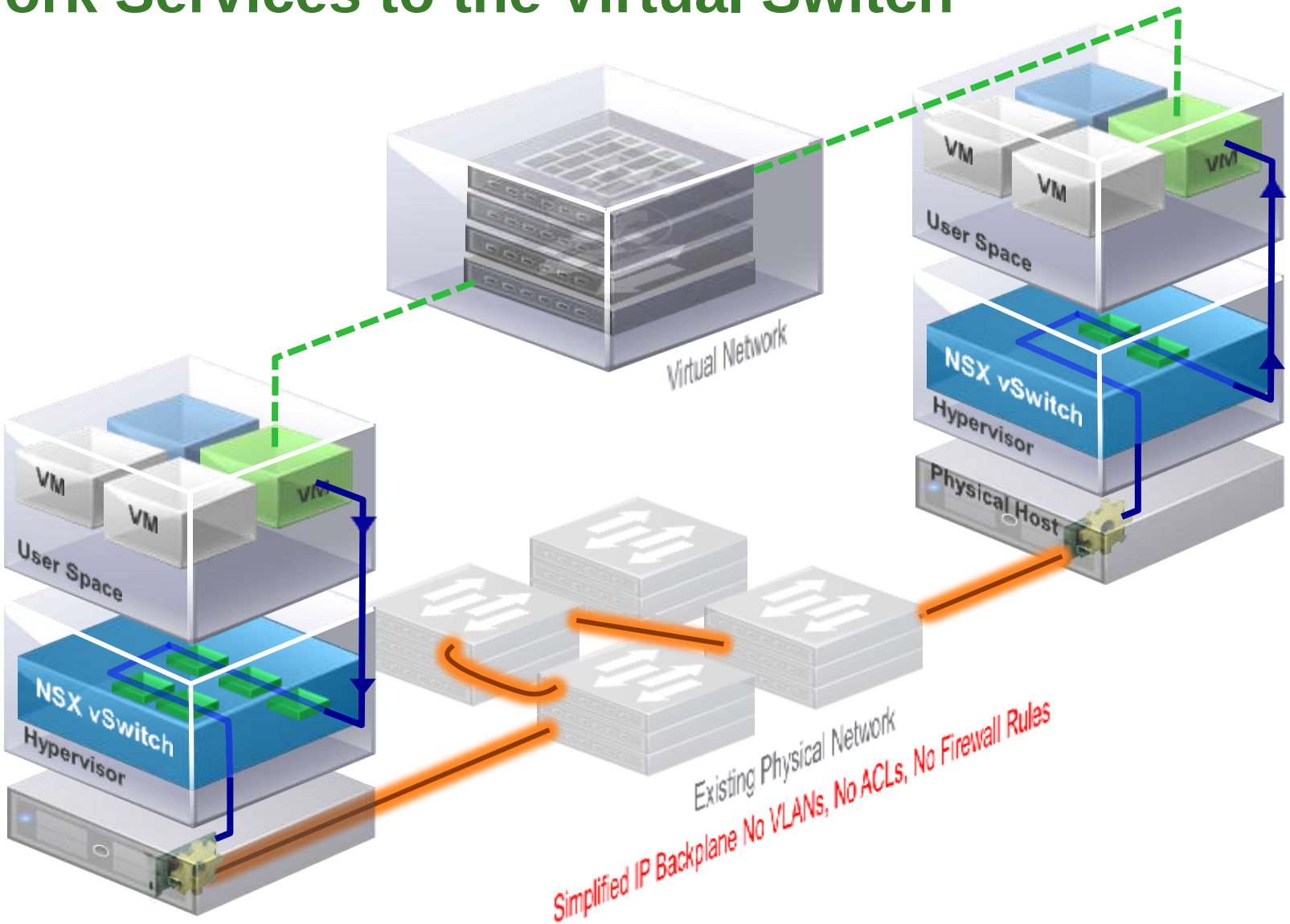
L3 Routing

L2 Switching



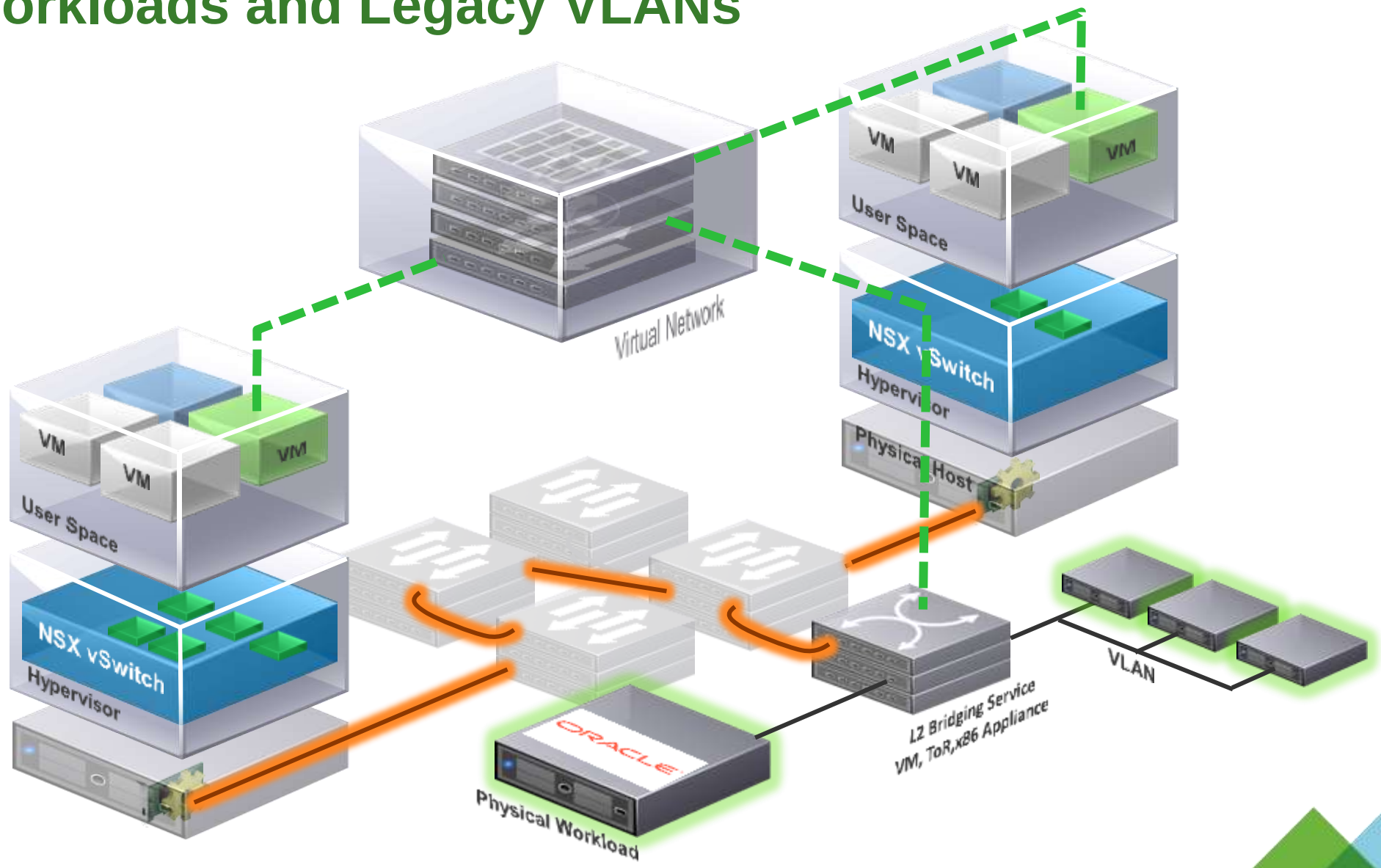
Firewalling/ACLs

Virtual Network Services to the Virtual Switch



vmware

Physical Workloads and Legacy VLANs

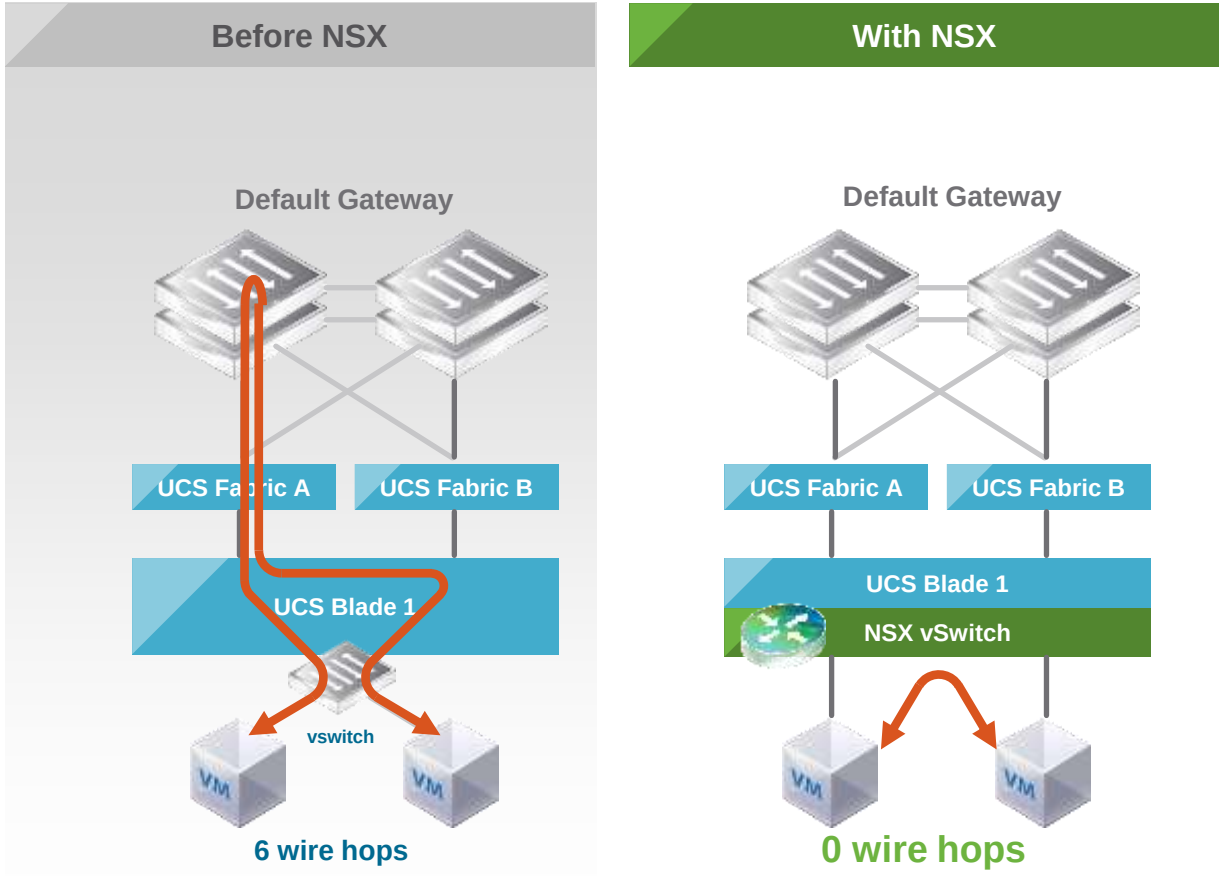


vmware

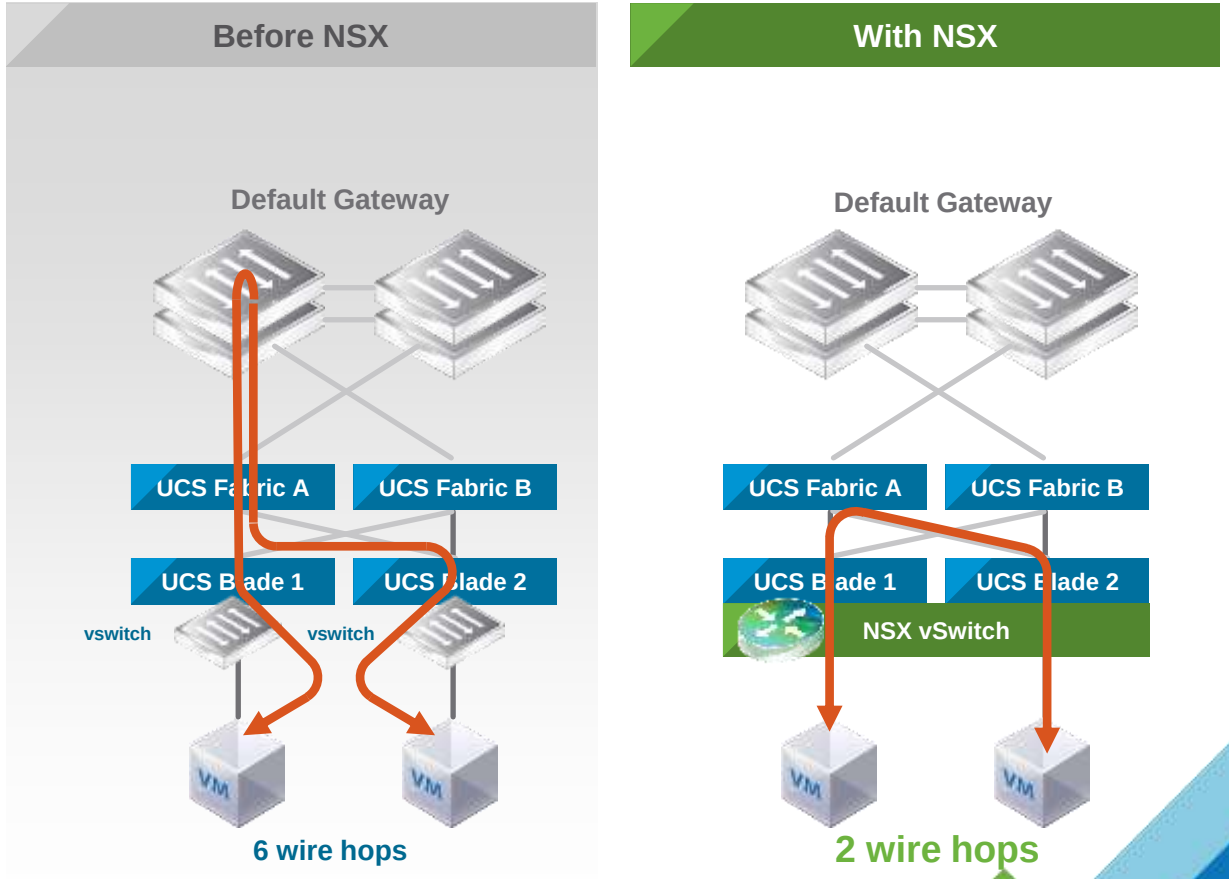
The 3 Advantages of Distributing Services

1. Routing - more efficient networking, fewer hops

East-West Routing / Same host



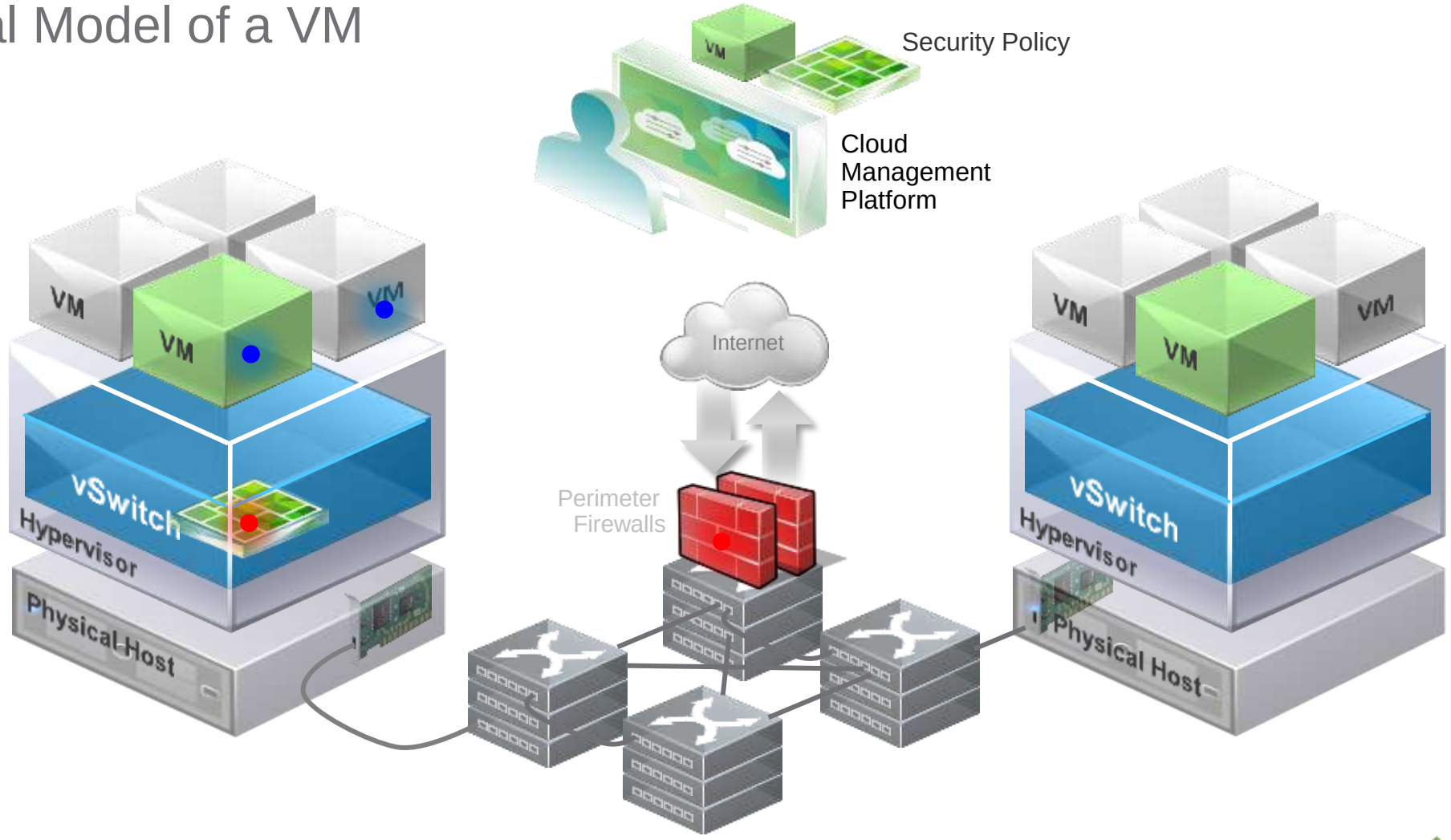
East-West Routing / Host to host



vmware

The 3 Advantages of Distributing Services

2. Operational Model of a VM



- Accurate firewall policies follow workloads as they move

The 3 Advantages of Distributing Services

3. Provisioning Automation with Scale-Out Performance

Platform-based automation

- Automated provisioning and workload adds/moves/changes

Hypervisor-based, in kernel distributed firewalling

- High throughput rates on a per hypervisor basis
- Every hypervisor adds additional east-west firewalling capacity

vmware

Gartner Magic Quadrant Data Center Networking 2015

"We believe VMware has **the largest installed base of any SDN solution** in the market today"

"VMware NSX can run **on top of any** appropriately provisioned **IP-based Ethernet network**"

"**VMware should be considered** for organizations looking to **increase networking agility or security** within highly virtualized data centers"

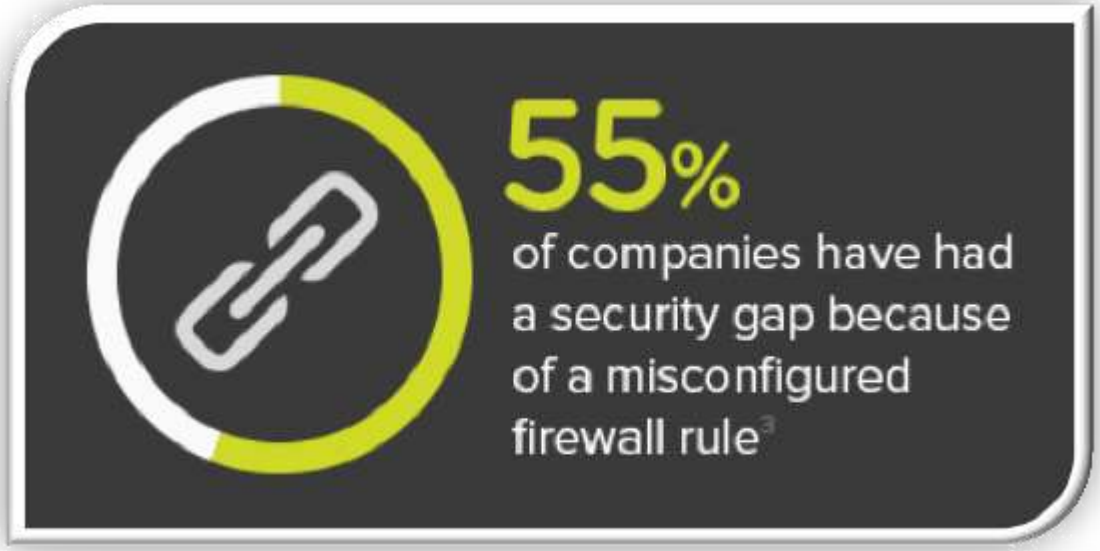
"NSX **microsegmentation is an innovative mechanism** to provide intra-data-center **security (east-west) in a cost-effective manner** compared with traditional appliance-based approaches."

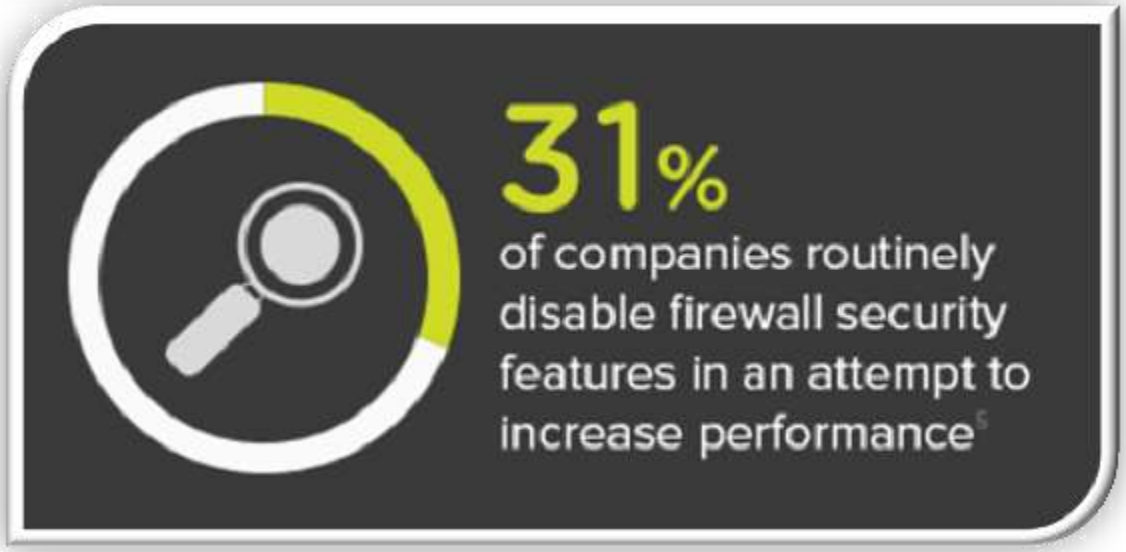
"Due to its pricing models, VMware's NSX allows organizations to incrementally **adopt SDN without requiring large upfront capital investments**."

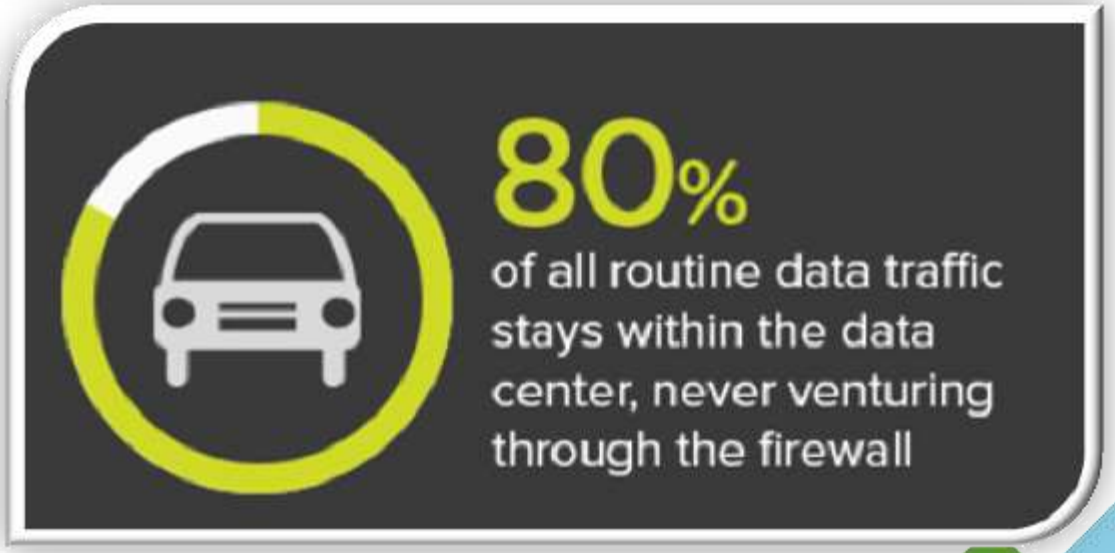
vmware

Gartner Data Center Networking Magic Quadrant, May 11, 2015

Organizations are Facing Multiple Issues with Security



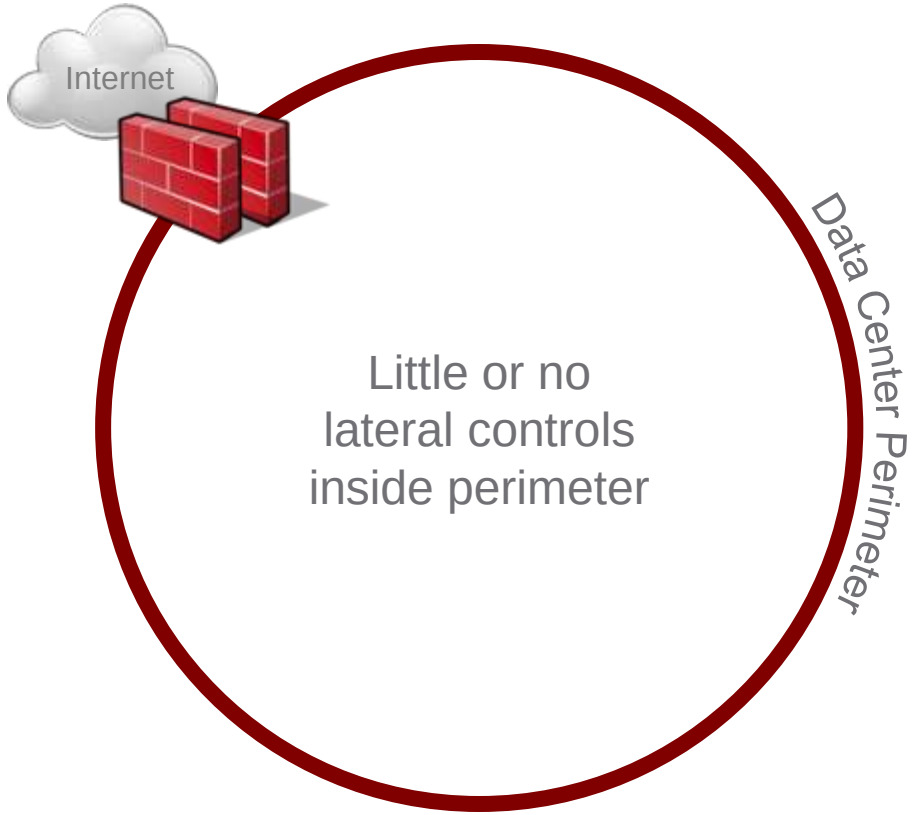




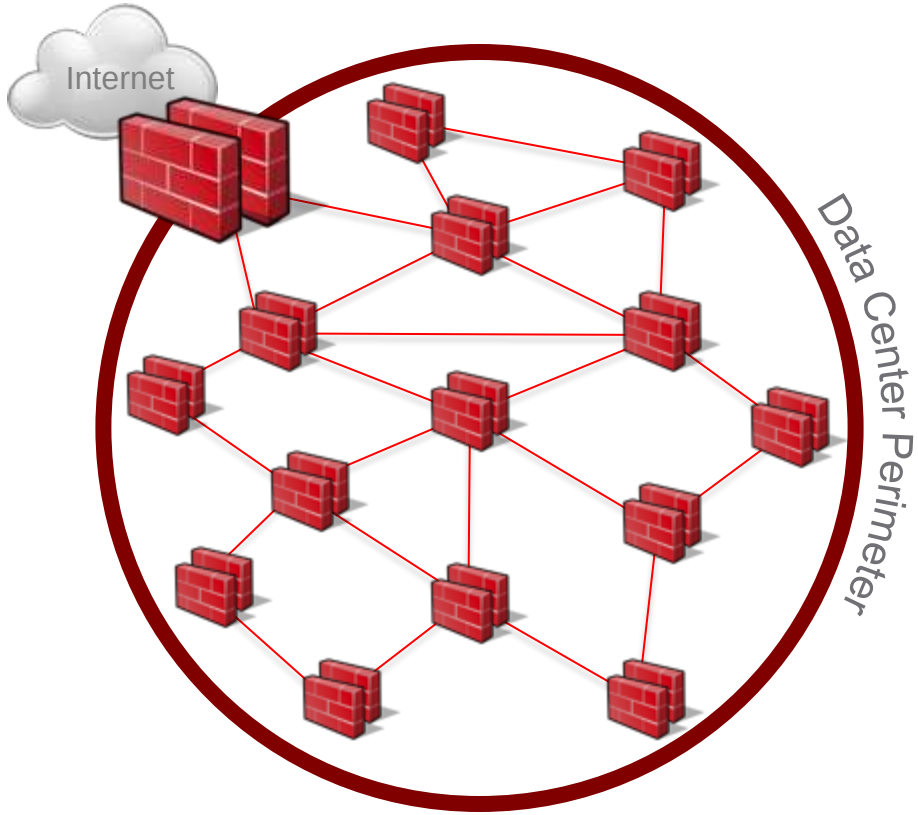
Source NSX Security Infographic: http://vmw.re/1AdyTEA

Problem: Data Center Network Security

Perimeter-centric network security has proven insufficient, and micro-segmentation is operationally infeasible



Insufficient



Operationally
Infeasible

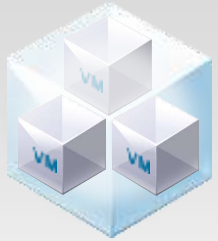
vmware

VMware NSX Micro-Segmentation

Zero-Trust security model that follows the VM

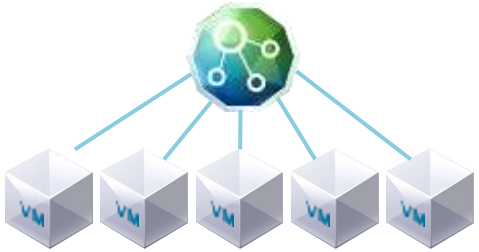
FORRESTER

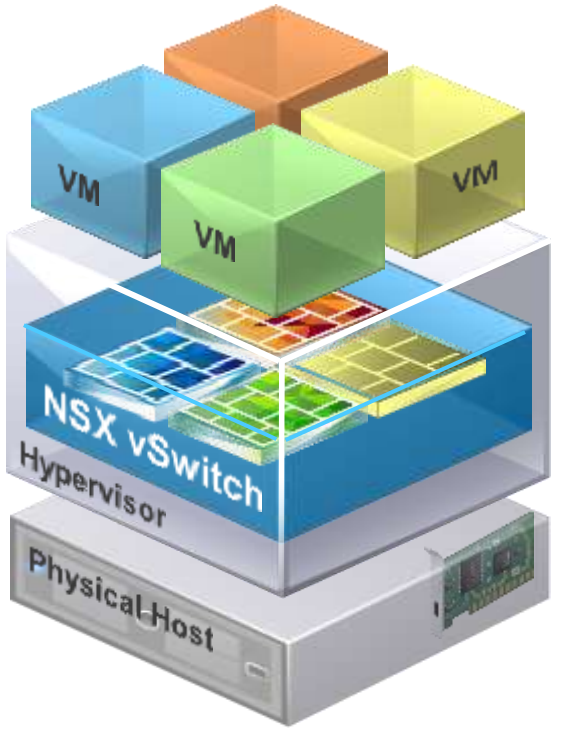
1 Isolation and segmentation



2 Unit-level trust / least privilege

3 Ubiquity and centralized control





Microsegmentation is now possible in dynamic, multi-tenant environments:

- High performance, **in kernel** distributed stateful firewall
- Security between VMs **on same IP Subnet**
- Integration with **best-of-breed security partners**

vmware

VMware NSX Ecosystem: http://www.vmware.com/products/nsx/resources
Developing a Framework to Improve Critical Infrastructure Cybersecurity: http://csrc.nist.gov/cyberframework/rfi_comments/040813_forrester_research.pdf

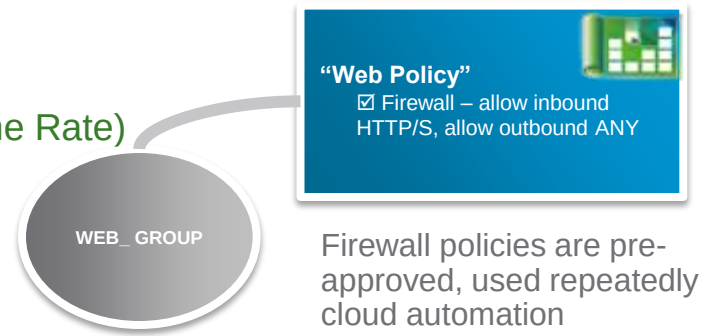
NSX Distributed Firewall is Optimized for SDDC

NSX Distributed Firewall

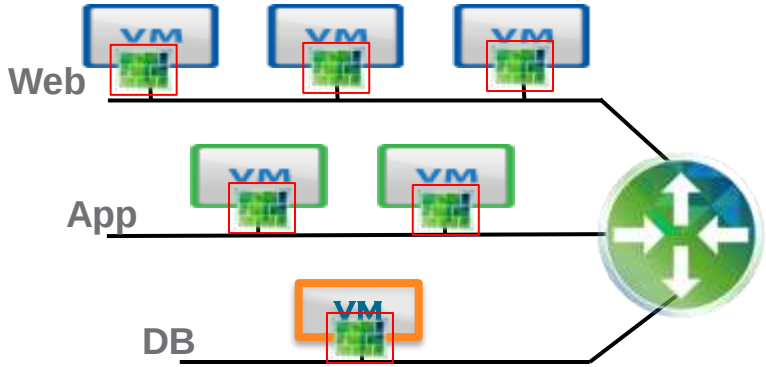
Src	Dst
ANY	Shared Service
Desktop	WEB_GROUP

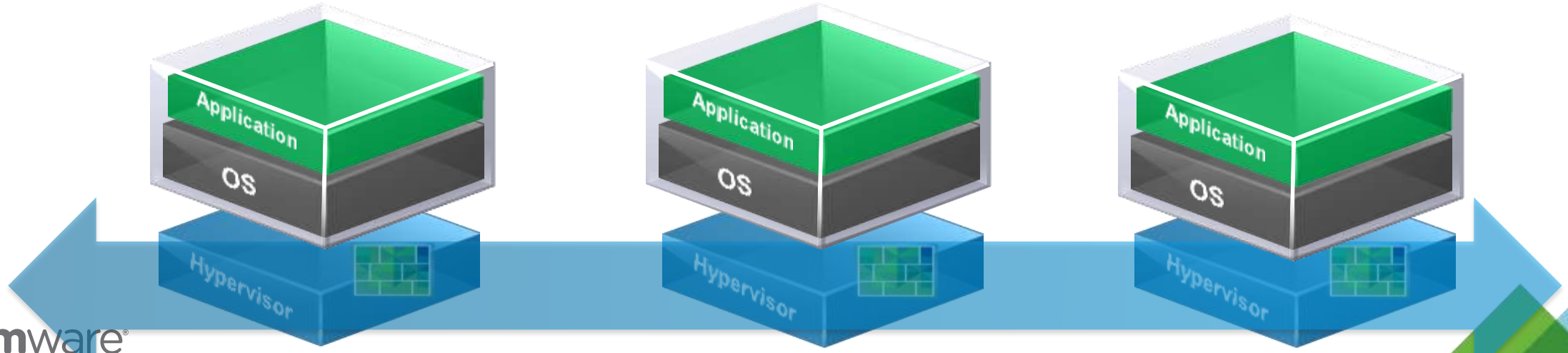
Rules based on logical containers

- Delivers Micro-Segmentation
- Efficient rule management
- Dynamic Policy (e.g: AV, DLP, Vulnerability Scan)
- No choke points with scale out performance (Near Line Rate)
- Enabled for cloud automation



Firewall policies are pre-approved, used repeatedly by cloud automation



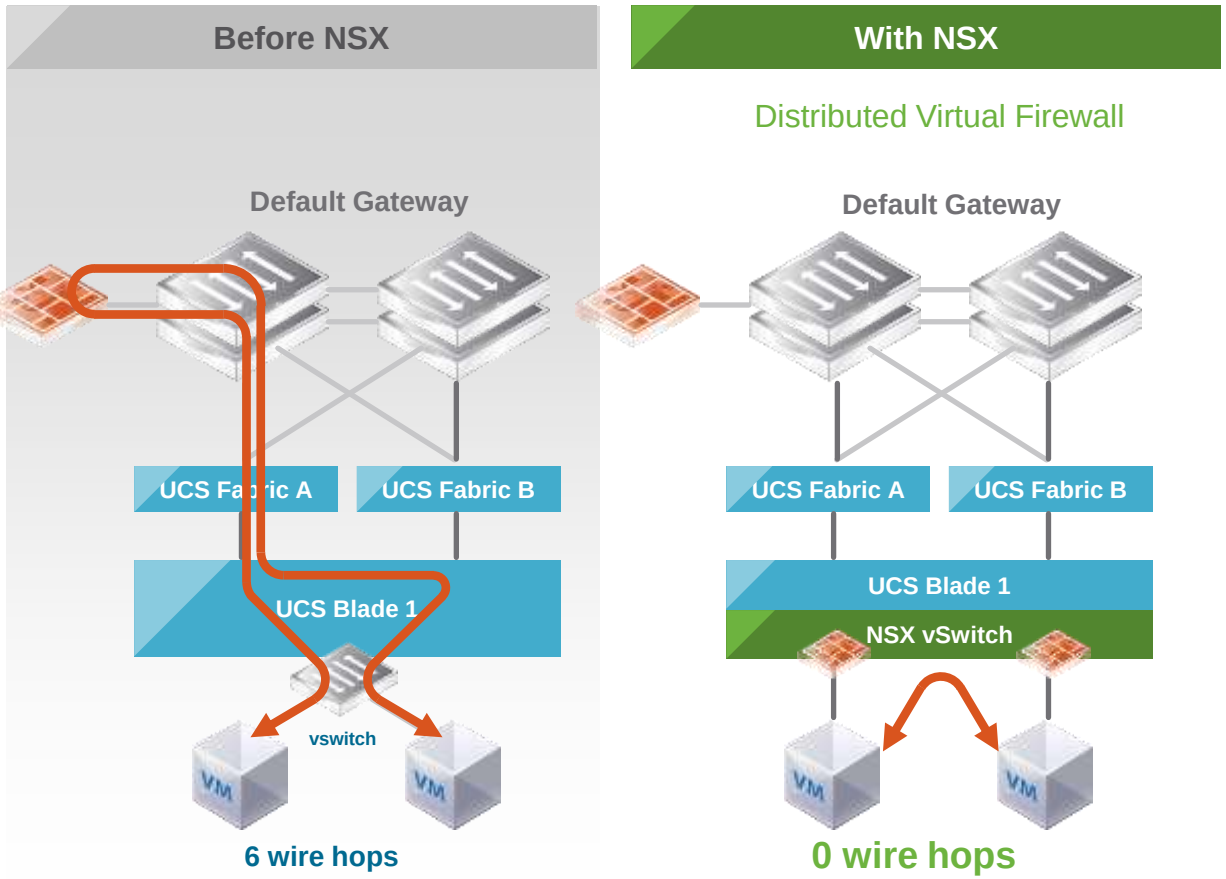


Platform for Distributed Services

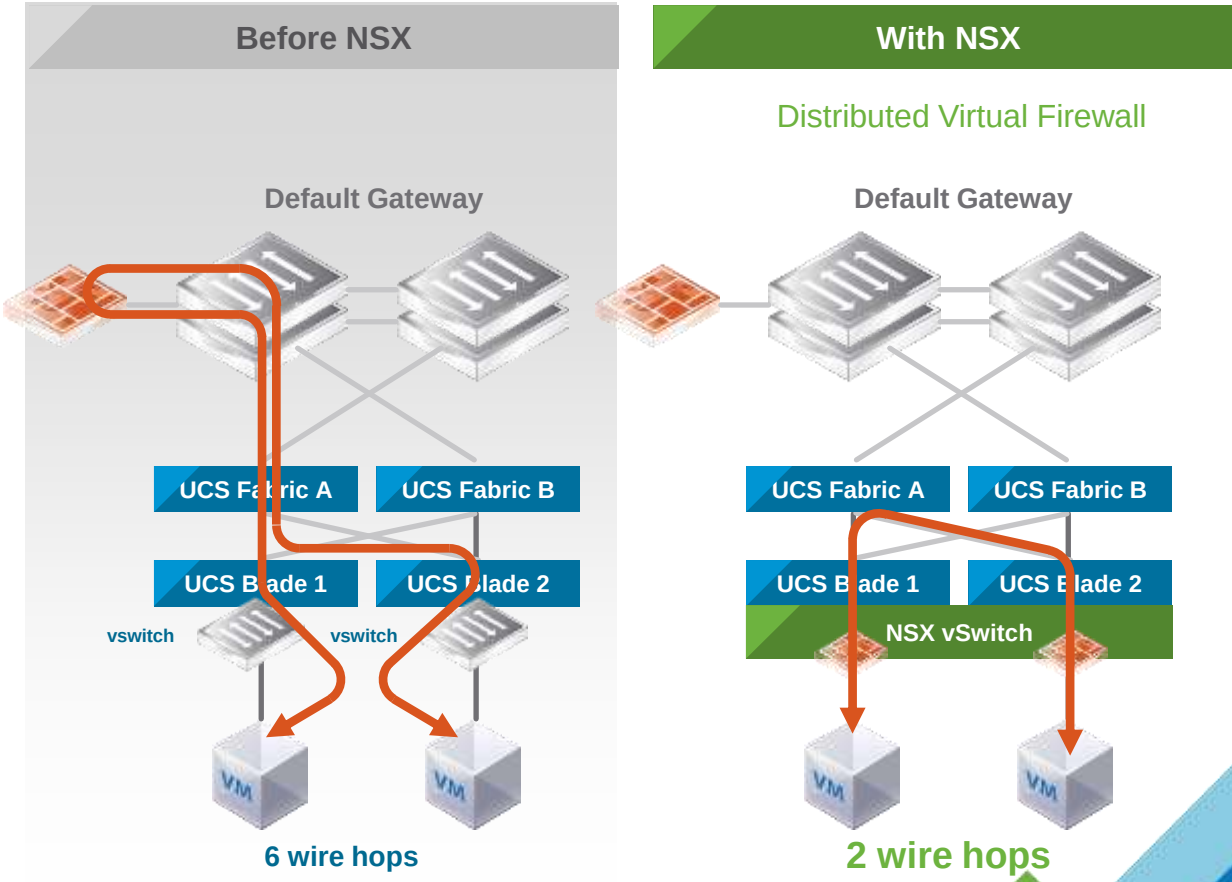
The 3 Advantages of Distributing Services

Firewalling – much simpler operations

East-West Firewalling / Same host



East-West Firewalling / Host to host



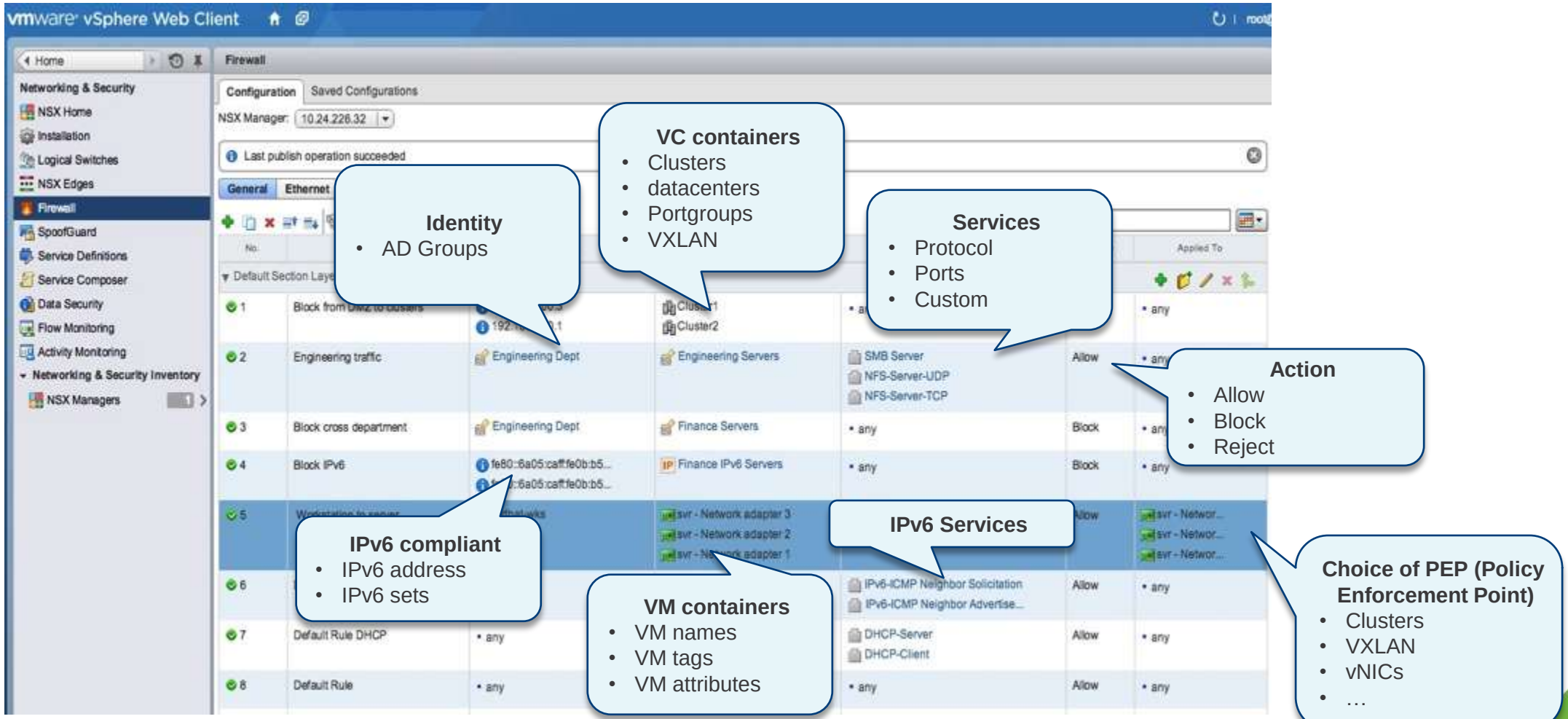
vmware

NSX DFW Policy Objects

- Policy rules construct:

Rule ID	Rule Name	Source	Destination	Service	Action	Applied To

- Rich dynamic container based rules apart from just IP addresses:

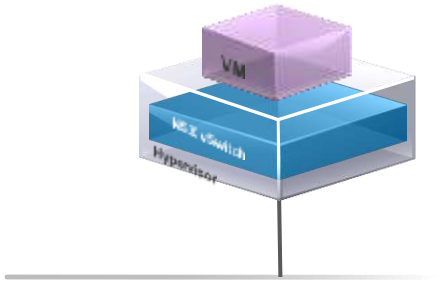


Configure Policies with Security Groups

1 Select elements to uniquely identify application workloads

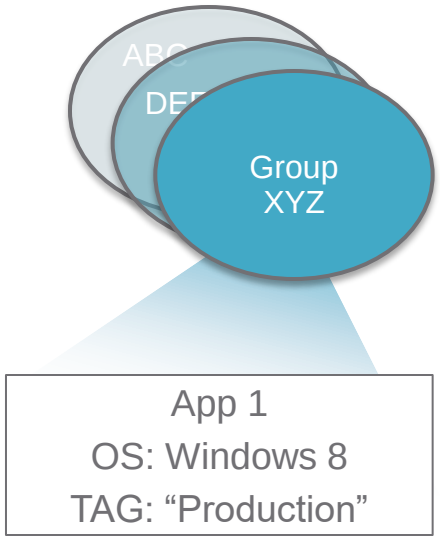
2 Use attributes to create Security Groups

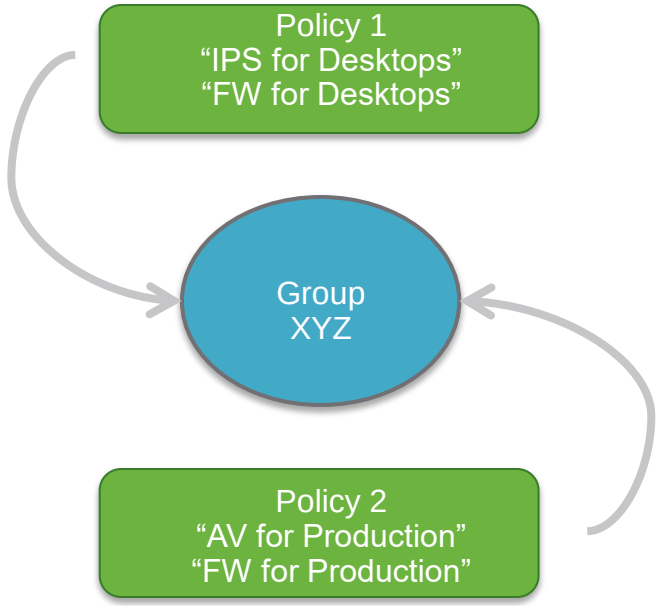
3 Apply policies to security groups



Element type

Static	Dynamic
Data center	VM name
Virtual net	OS type
Virtual machine	User ID
vNIC	Security tag



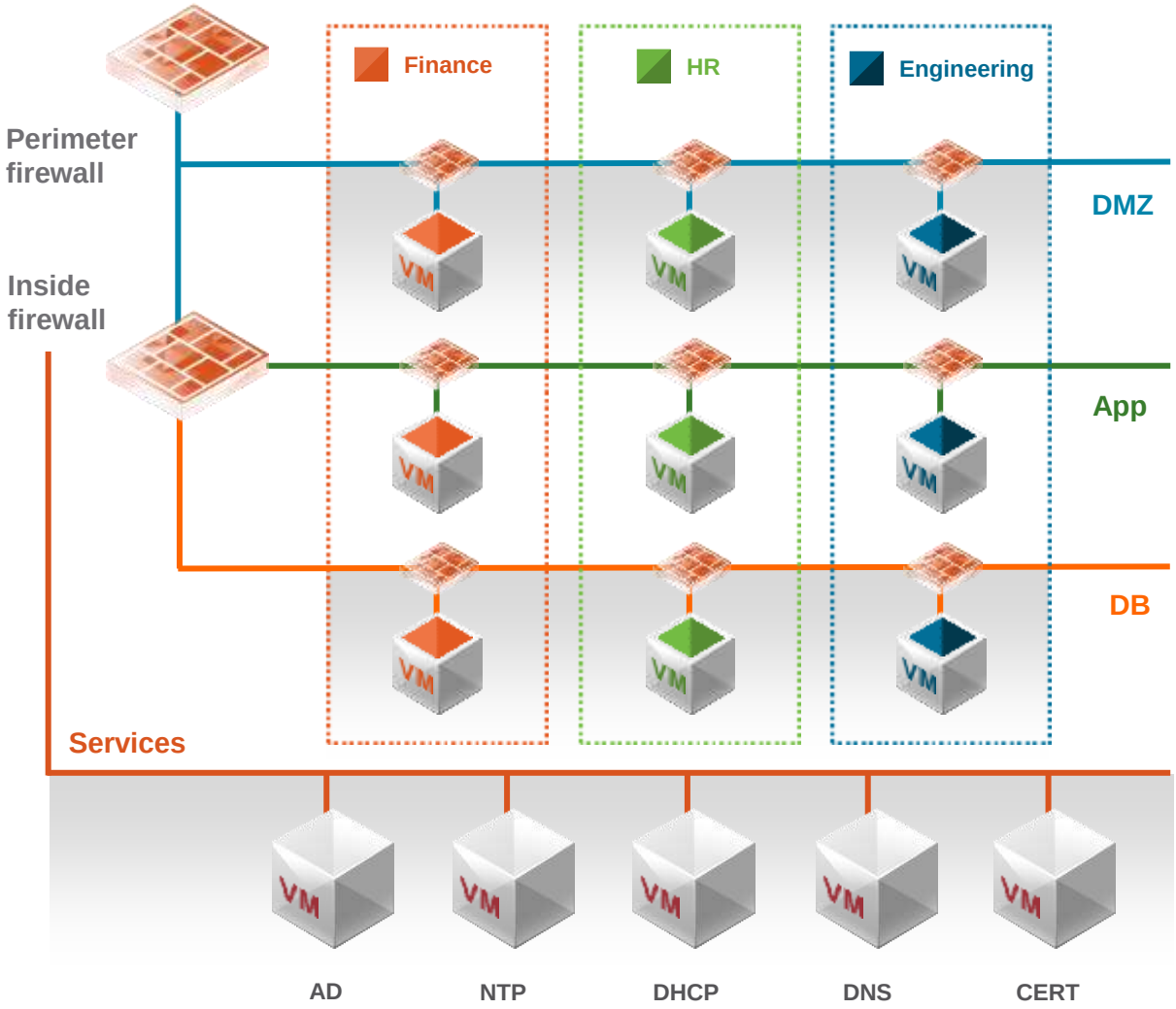


Use security groups to abstract policy from application workloads.

- Enforce policy based on logical constructs
- Policy follows VM, not IP
- Reduce configuration errors
- Reduce rule sprawl and complexity

vmware

Micro-segmentation simplifies network security

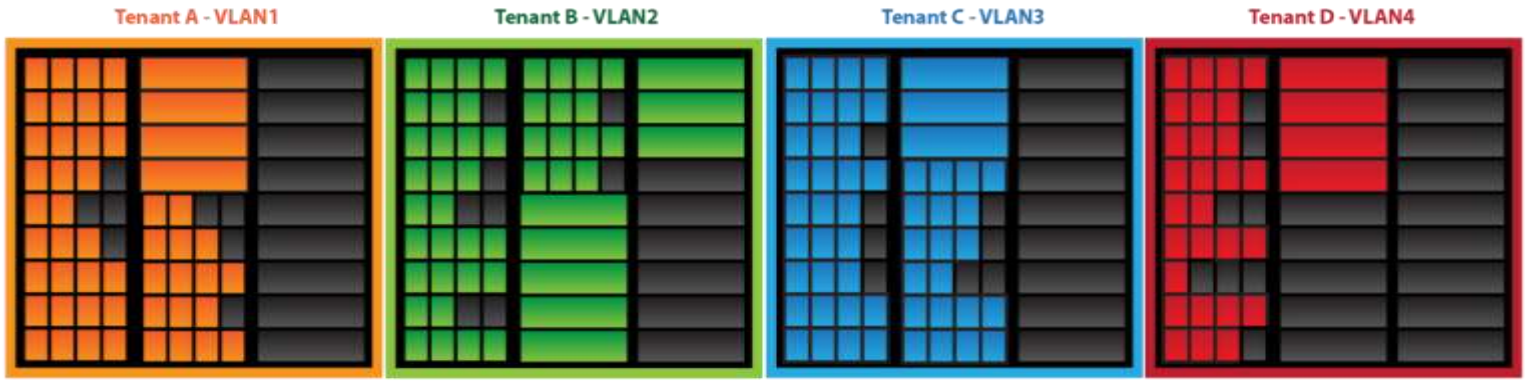


- Each VM can now be its own perimeter
- Policies align with logical groups
- Prevents threats from spreading

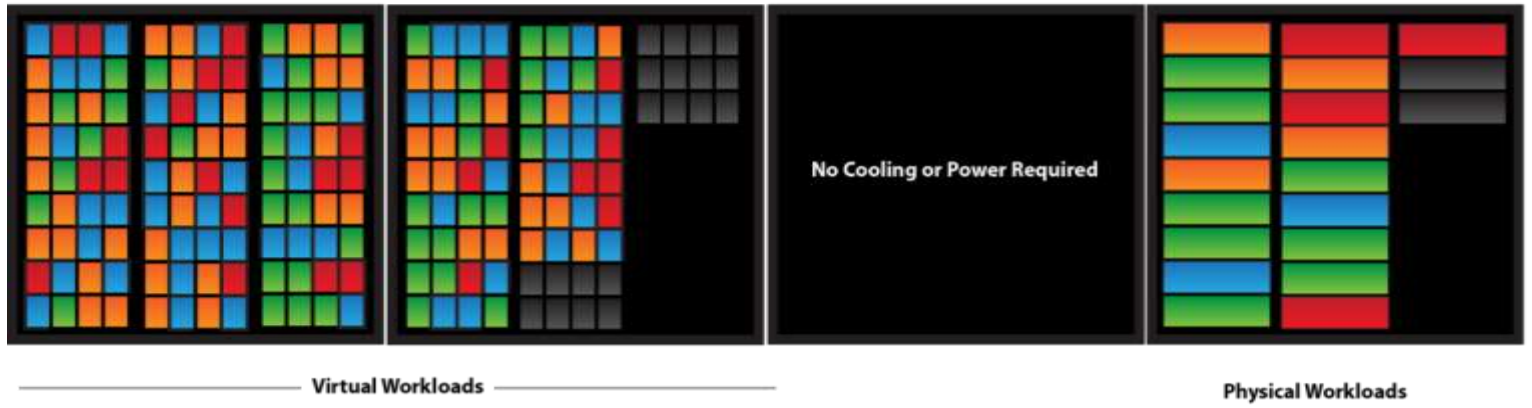
vmware

Improved Server Utilization – less overprovisioning of servers

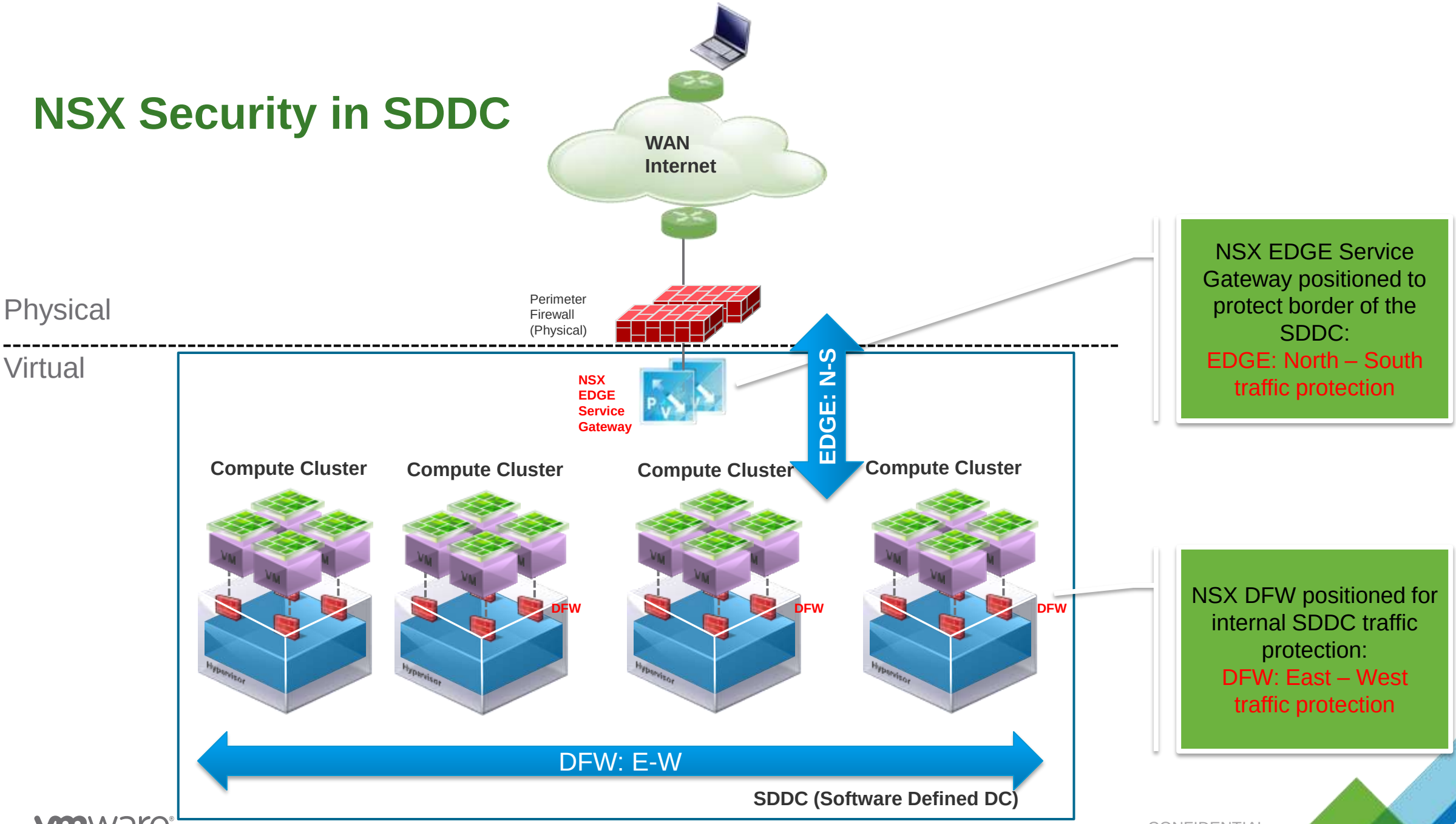
Without Network Virtualization 60% Asset Utilization



With Network Virtualization 90% Asset Utilization



NSX Security in SDDC

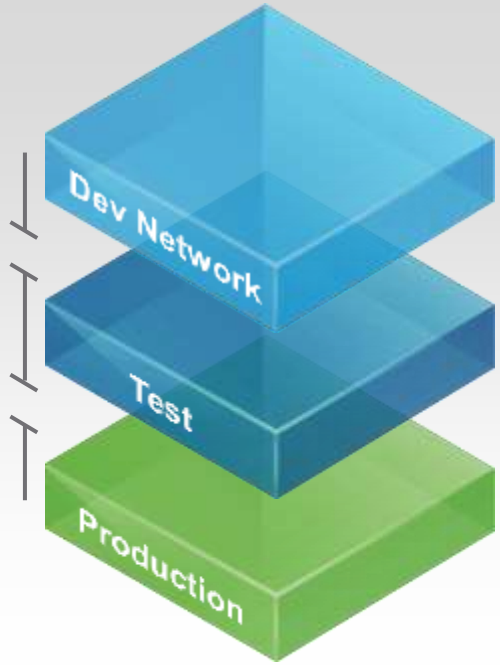


NSX EDGE Service Gateway positioned to protect border of the SDDC:
EDGE: North – South traffic protection

NSX DFW positioned for internal SDDC traffic protection:
DFW: East – West traffic protection

Micro-segmentation in detail

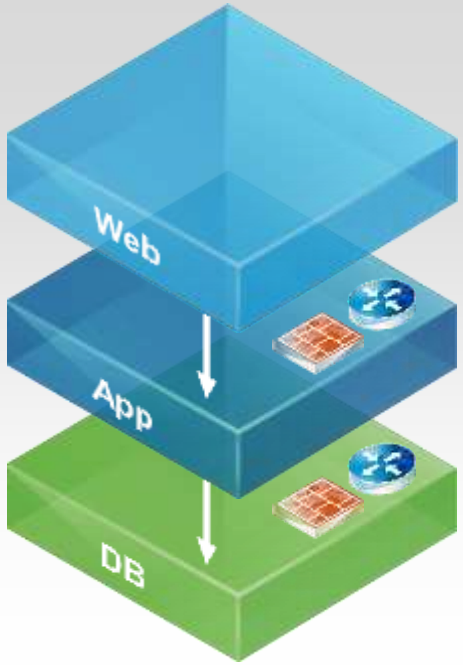
Isolation



No communication path between unrelated networks

- No cross-talk between networks
- Overlay technology assures networks are separated by default

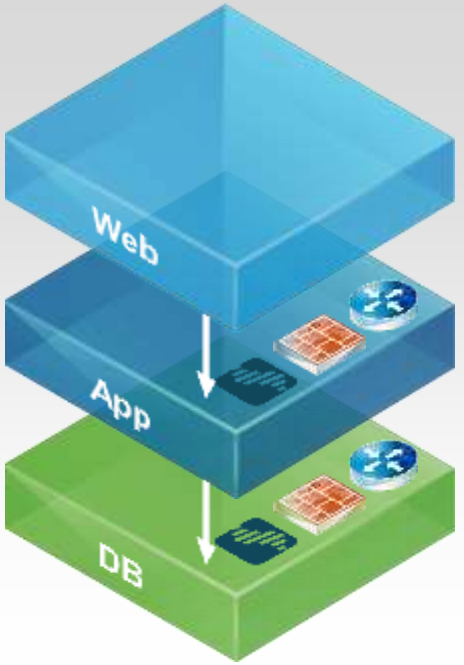
Segmentation



Controlled communication path within a single network

- Fine-grained enforcement of security
- Security policies based on logical groupings of VMs

Advanced services



Advanced services: addition of 3rd party security, as needed by policy

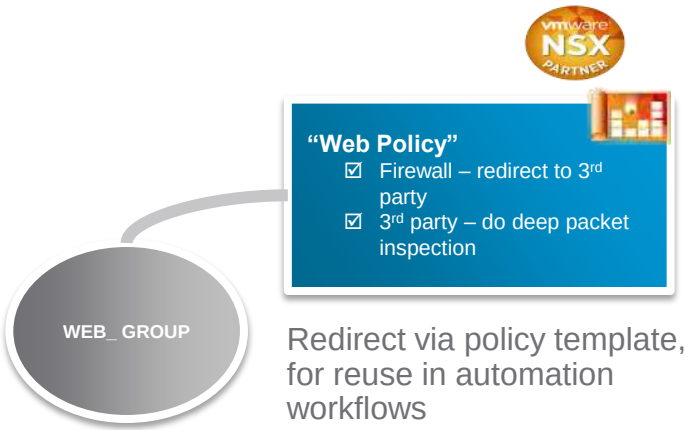
- Platform for including leading security solutions
- Dynamic addition of advanced security to adapt to changing security conditions

vmware

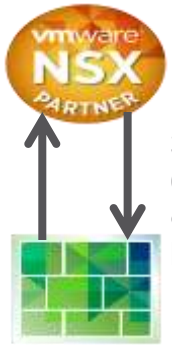
Third-Party Firewall, Network Security Options for NSX Integration

Src	Dst	Action
ANY	Shared Service	Allow
Desktop	WEB_GROUP	Redirect to 3rd party

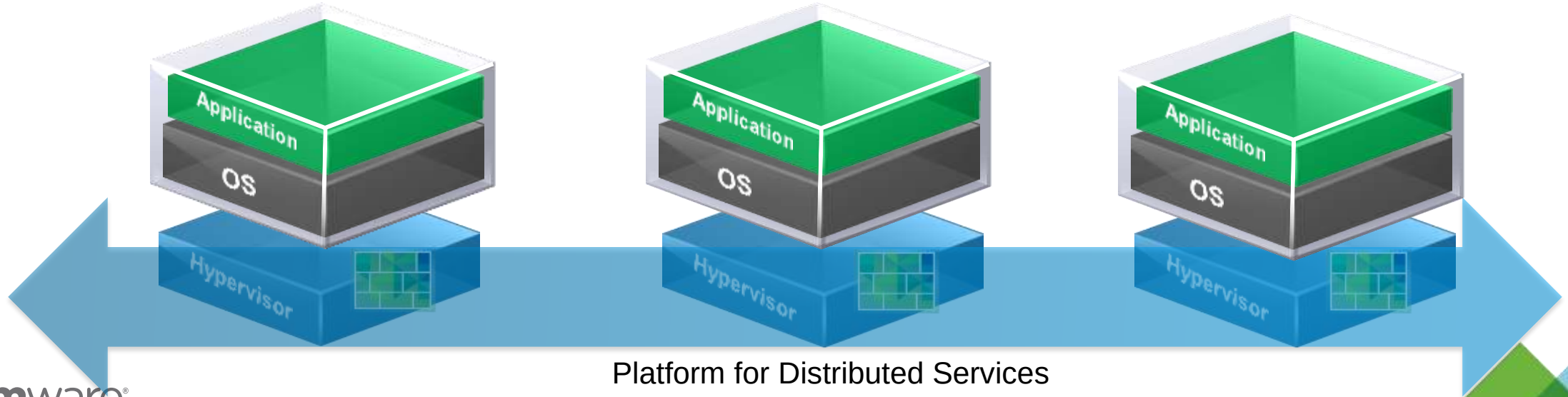
Redirect via global rule to 3rd party



Redirect via policy template, for reuse in automation workflows

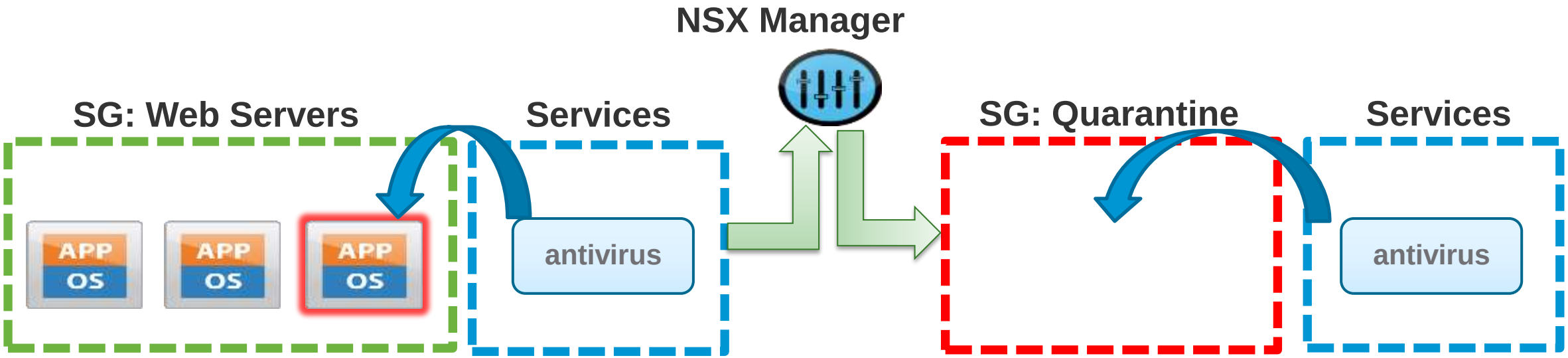


3rd party can program NSX distributed firewall directly – and set/get context to inform policy



Example : Orchestrating Security Between Multiple Services (Vulnerability Scan)

1. Web Server VM running IIS is deployed, **unknowingly** having a vulnerability
2. Vulnerability Scan is initiated on web server (3rd party AV product)
3. VM is tagged in NSX Manager with the CVE and CVSS Score
4. NSX Manager associates the VM with the Quarantine (F/W Deny)
5. [Externally] Admin applies patches, 3rd party AV product re-scans VMs, clears tag
6. NSX Manager removes the VM from Quarantine ; VM returns to it's normal duties



vmware

NSX Partners and Service Categories

NSX Partner Extensions

Physical-to-Virtual Services

ARISTA

BROCADE

cumulus networks

DELL

hp

JUNIPER NETWORKS

IBM

lenovo

Operations and Visibility

EMC² smarts

NETSCOUT.

riverbed

ixia
Deliver On

Gigamon

Fishtech

solarwinds

SUSE

VENERA
SPIRIT OF INNOVATION

Security

paloalto NETWORKS

intel Security

Symantec.

tufin

TREND MICRO

Check Point

RAPID7

Xceedium

catbird

HYTRUST

FireEye

SkyBox

algosec

Application Delivery Services

f5

radware

CITRIX

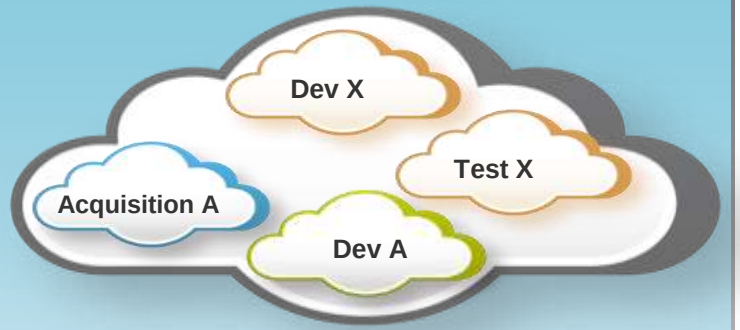
A10 Networks

vmware

http://www.vmware.com/products/nsx/resources.html

VMware NSX –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

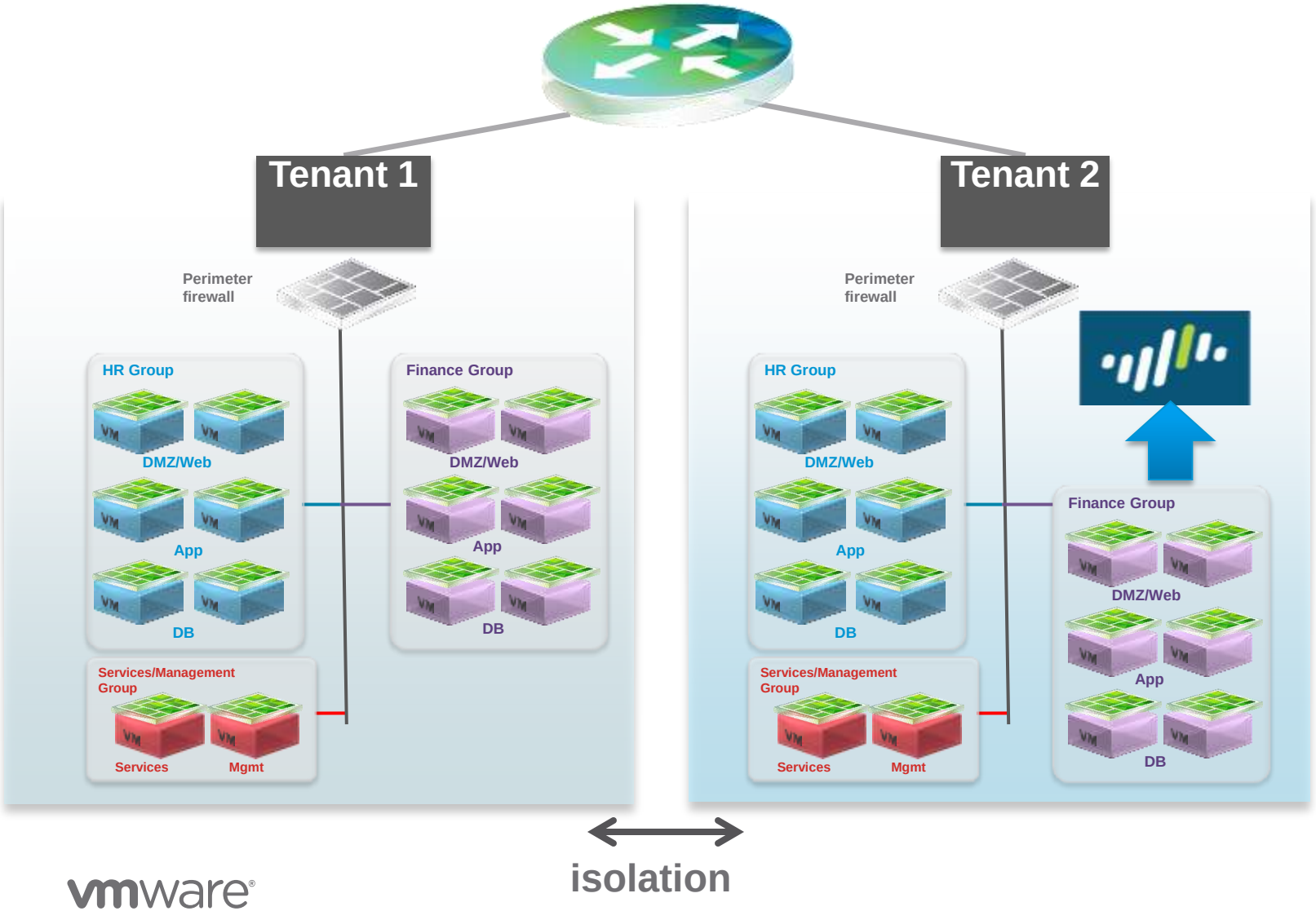
XaaS Clouds
Vertical Clouds

Key Capabilities

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

vmware

Use Case : Multi-tenancy with Segmentation and Advanced Services

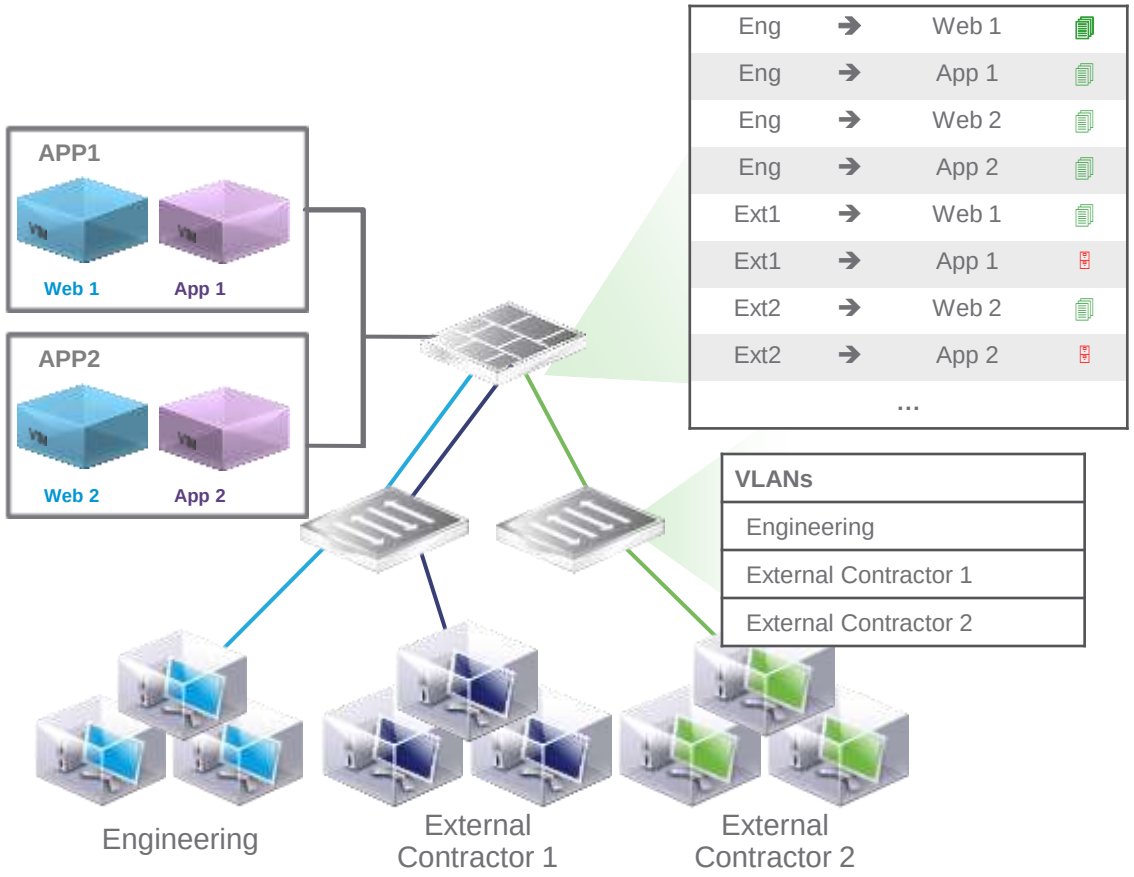


No traffic between networks

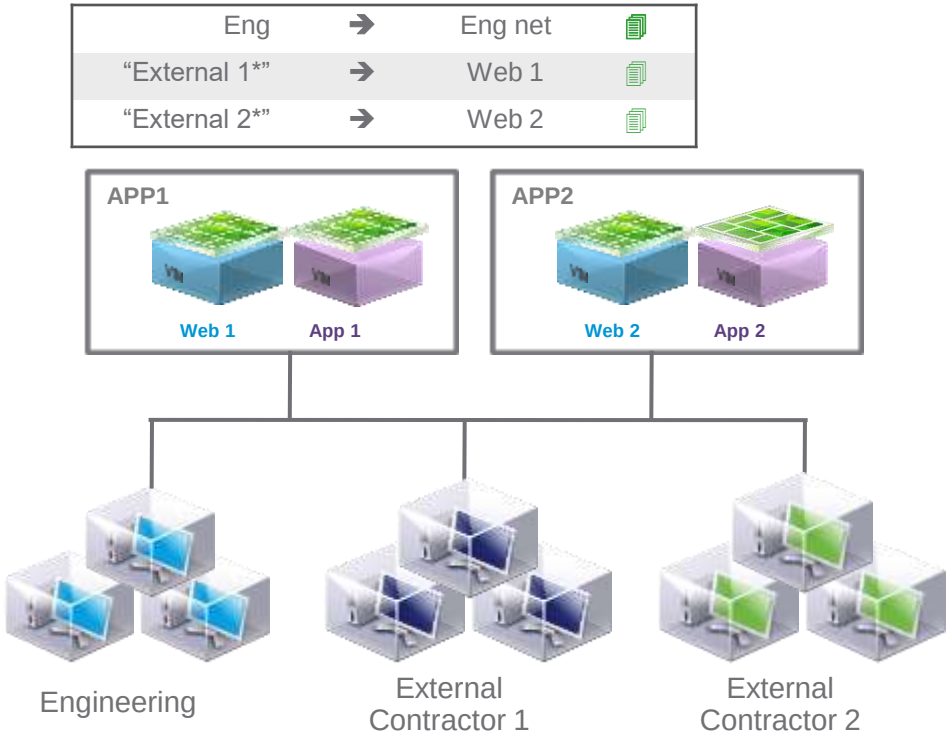
- Completely separate unrelated networks
- Add advanced services based on virtual network, network segment, or Security Group

Use Case: Networking and Security for VDI

Traditional Data Center



NSX Data Center

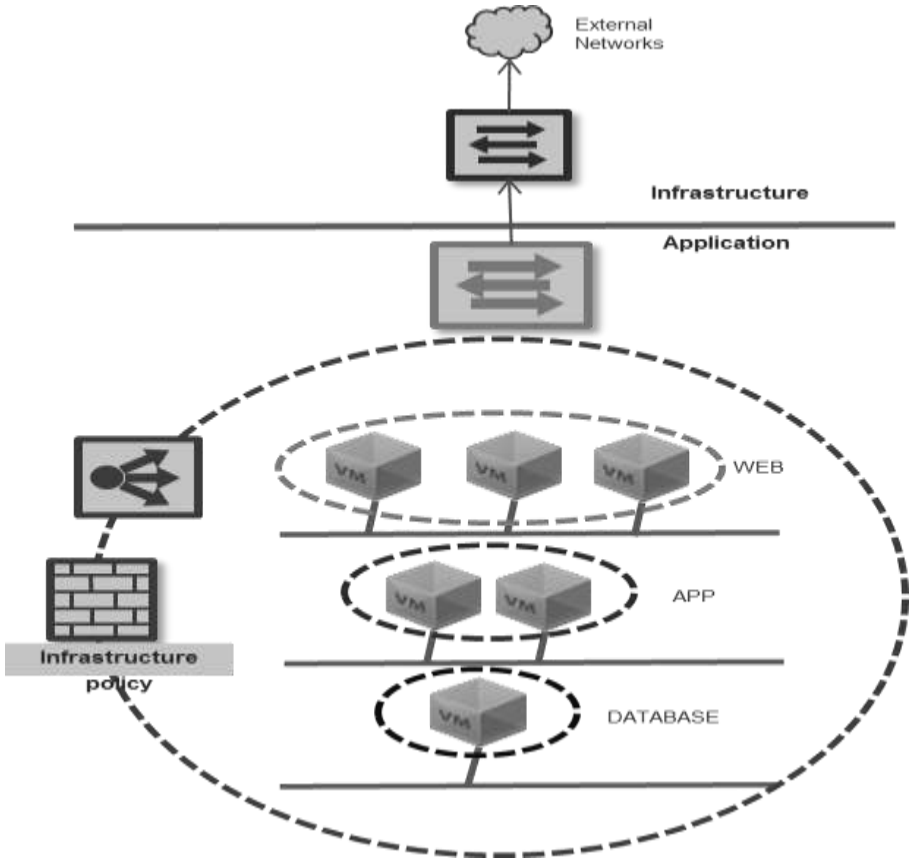


Simplify VDI deployments

- Eliminate complex policy sets and topologies for different VDI users
- Align policies to logical grouping
- Decouple network topology from VDI security

Use Case: Infrastructure Management with vRealize Automation

Dynamically Provision and Decommission NSX Logical Services



New Features

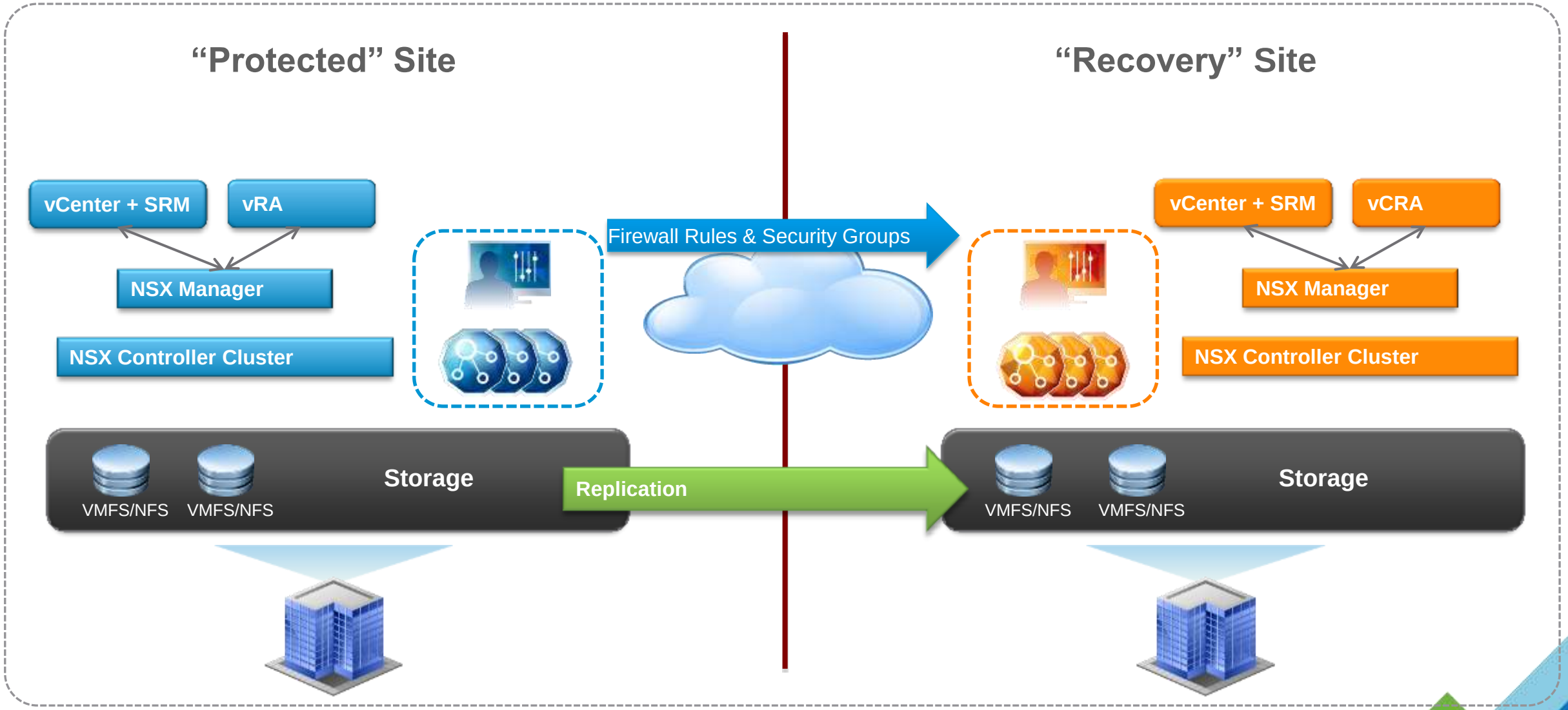
- **Simplified Multi-Tier App Deployment**
- **Improved Connectivity**
  - Deployment of logical switches and networks
- **Enhanced Security**
  - Intelligent placement of workloads in security groups protected by firewalls
- **Increased Availability**
  - Via deployment of NSX distributed firewalls and load balancers

Benefits

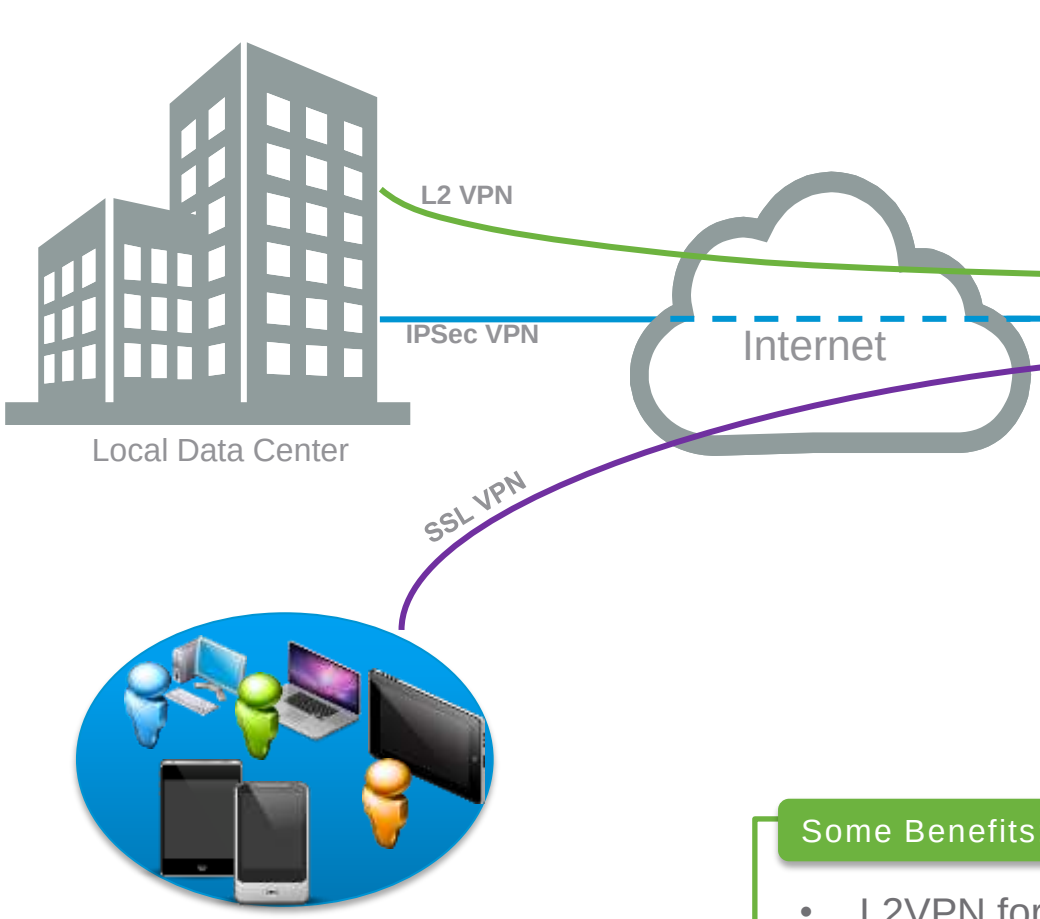
- Deliver **secure**, **scalable**, **performing** application-specific infrastructure on-demand

vmware

Use Case: Disaster Recovery Scenarios with NSX+SRM



Use Case: A True Hybrid Cloud powered by VMware NSX



Some Benefits:

- Today with **vCloud AIR**
- Tomorrow with **Amazon AWS, Azure, Google and other Public Cloud Providers**

Some Benefits:

- L2VPN for **DC Extension**
- Granular Network Security with **Trust Groups**
- **Bi-directional workload migration** using **vSphere web client**

NSX Customer and Business Momentum

1200+

NSX Customers

250+

Production Deployments
(adding 25-50 per QTR)

100+

Organizations have spent over US$1M on NSX

vmware

Stats as of end of Q4 2015

VMware NSX Value Prop

VMware NSX Transforms the Operational Model of the Network

Innovative Speed & Business Velocity

Reduce network provisioning time from days to seconds

Network provisioning time reduced from 7 days to
30 sec.

Cost Savings

Operational automation

Simplified IP hardware

Reduce operational costs by 80%
Increase compute asset utilization to 90%, reduce hardware costs by 40-50%

Choice

Any hypervisor
Any CMP
with Partners

Any Hypervisor: vSphere, KVM, Xen, HyperV (future)
Any Network Hardware
Any CMP: vRealize, OpenStack
Partner Ecosystem.

vmware

What's Next…

Play

VMware NSX Hands-on Labs
labs.hol.vmware.com

Learn

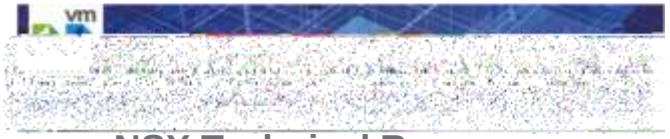
Explore, Engage, Evolve
virtualizeyournetwork.com

Network Virtualization Blog
blogs.vmware.com/networkvirtualization

NSX Product Page
vmware.com/go/nsx

NSX Training & Certification
www.vmware.com/go/NVtraining

Deploy



NSX Technical Resources
Reference Designs
vmware.com/products/nsx/resources

VMware NSX YouTube Channel
youtube.com/user/vmwarensx

VMware NSX Community
communities.vmware.com/community/vmtn/nsx

vmware

Q&A


Thank you.
vmware