Cisco Expo 2012

Nasazení VDI/VXI z pohledu bezpečnosti a nástrojů pro spolupráci

ARCH2/L2

Tomáš Horák, tohorak@cisco.com
Systems Engineer, Data Center & Collaboration

Petr Wünsch, petr@netapp.com
Systems Engineer

Prosíme, ptejte se nás

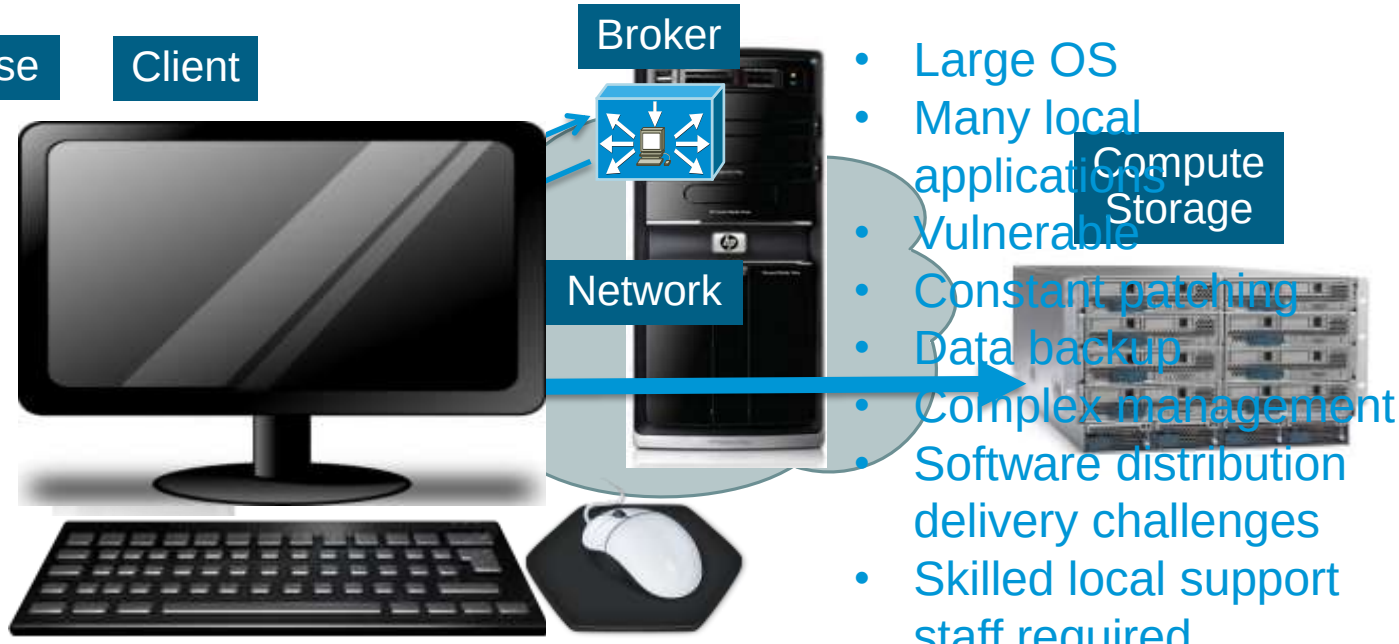
- Twitter www.twitter.com/CiscoCZ
- Talk2cisco www.talk2cisco.cz/dotazy
- SMS 721 994 600

Program

- Why Desktop Virtualization?
- Cisco VXI Vision
- VXI & Collaboration
- NetApp Storage for VDI
- VXI Security
- DC Security
- Conslusion

Why Desktop Virtualization?

Overview
The Network Is the Desktop



- Large OS
- Many local applications
- Vulnerable
- Constant patching
- Data backup
- Complex management
- Software distribution delivery challenges
- Skilled local support staff required

- Personal Computer is disaggregated
- Keyboard, Video, and Mouse stay with user
- Compute and storage move to the data center
- Network availability is required for all application access
- Network performance is critical to user experience

VDI Drivers for Decision Makers

Challenges of Traditional PC Environment

Purchase Drivers

Microsoft Windows 7 Migration

- Reduce migration costs
- Reduce application incompatibility
- Extend life of existing desktop software

Contractors and Employee-Owned IT

- Manage desktop image on employee-owned assets
- Provide separation between corporate and personal desktops

Business Continuity

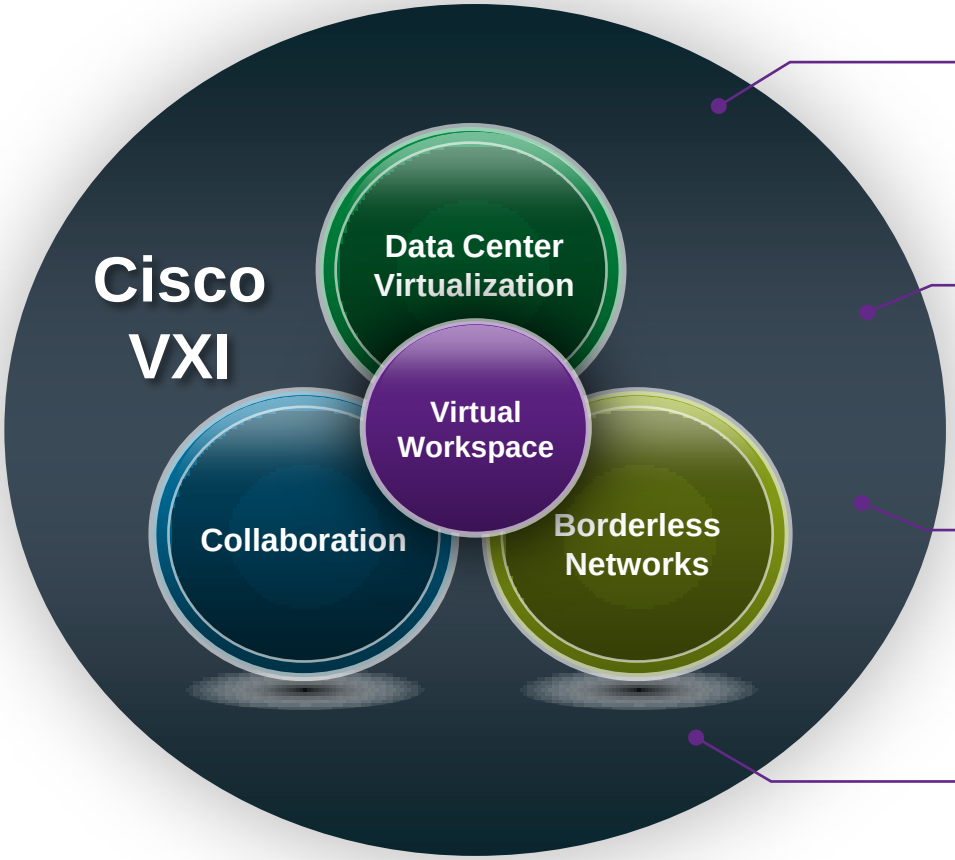
- Endpoint Independence
- Rapid Provisioning

Remote and Mobile Users

- Enable desktop access regardless of network connection type
- Extend security and control
- Centrally control sensitive data

Cisco VXI Vision

Cisco Virtualized eXperience Infrastructure



Media Rich Experience

Security

TCO / ROI

System Integration

Bringing Together Desktop Virtualization & Collaboration

- Data security & compliance
- Business continuity / agility
- Reduced TCO
- Standardized IT experience, customizable user experience

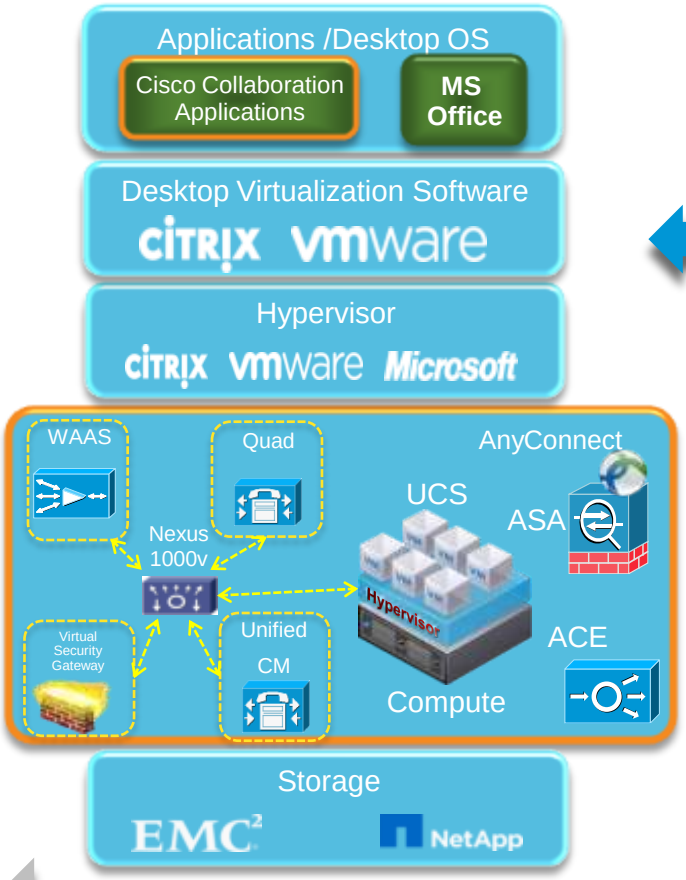
- Voice, Video, IM, Conference
- Presence
- Mobility
- Real time
- Range of devices

IT Standardization **High Quality Experience**

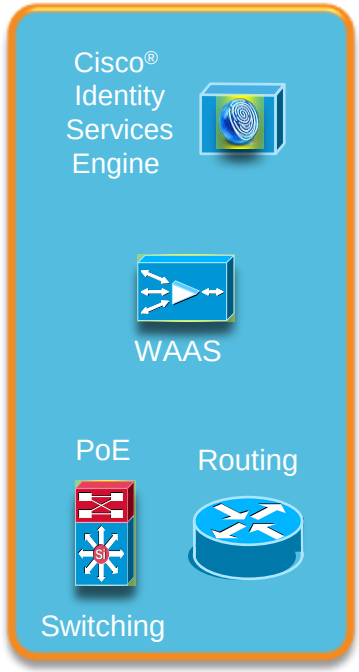
Cisco VXI Virtualized End-to-End System

= Cisco Products

Virtualized Data Center



Virtualization-Aware Borderless Network



End-to-End, Management and Optimization

atlantis COMPUTING · AppSense · Liquidware Labs · unidesk

Virtualized Collaborative Workspace

VXI 2.5 System

VXI & Collaboration

VXI Virtualized Collaborative Workplace

Today's Workspace

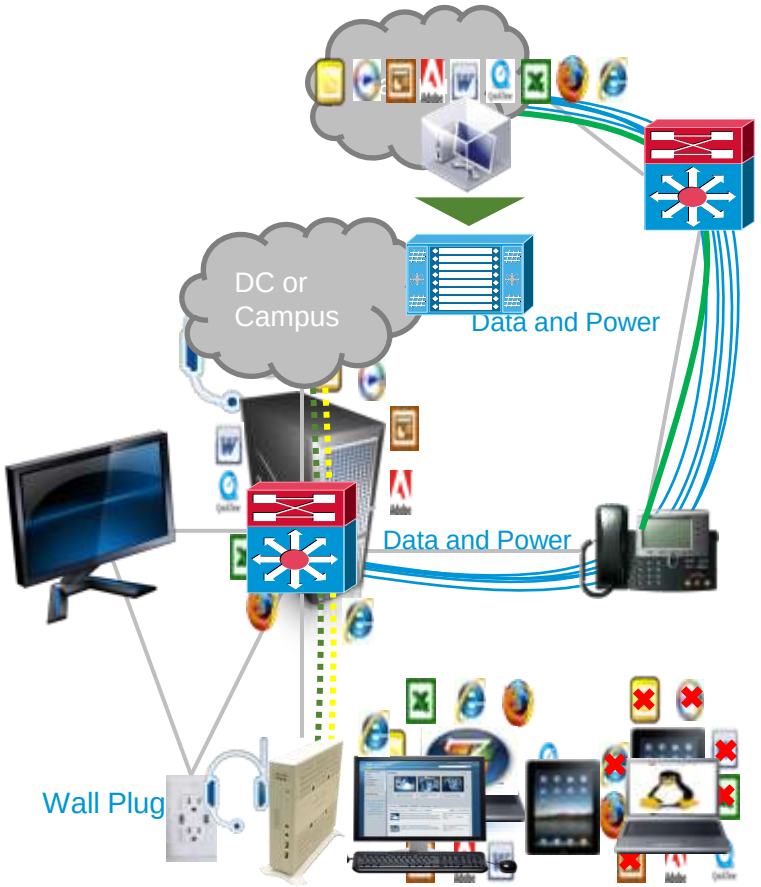
- Multiple devices for Desktop, Display, Collaboration
- Multiple wires for Data and Power
- Multiple Applications and versions on each desktop
- End-user tied to endpoint for work
- Multiple data flows to manage from each Workspace – Telephony, Video, HTTP, SMTP, IMAP, CIFS, Custom, etc.

VXI Virtual Workspace Vision

- Single endpoint minimum wiring and data flows
- Integrated Virtual Desktop and Collaboration
- Secure Workspace flexibility and mobility

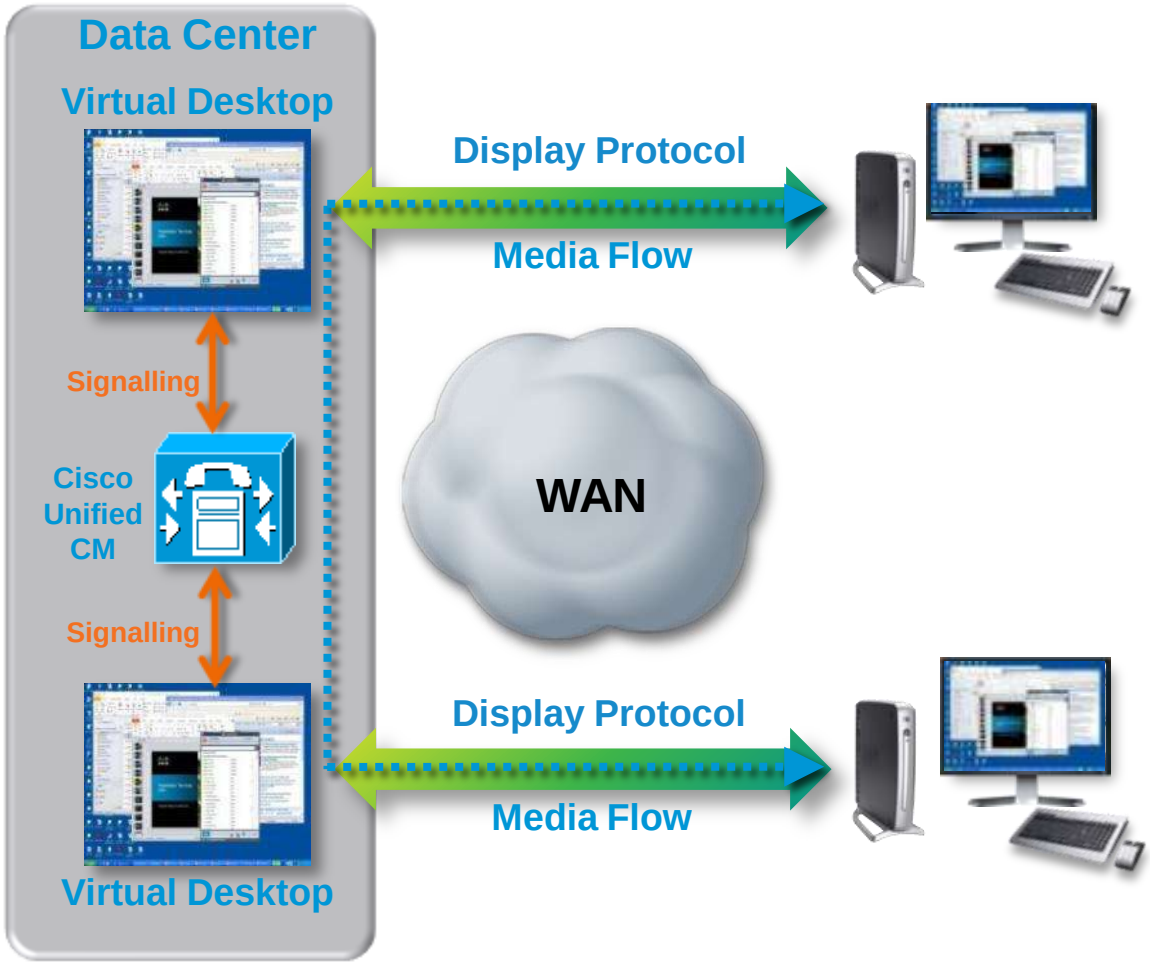
What is Needed

- Cisco VXC endpoints
- Network access capable of providing power and Data to the workspace
- Desktop Virtualization System that integrates business class collaboration capabilities and Virtualization aware network



Voice, Video, Virtual Desktop Challenge

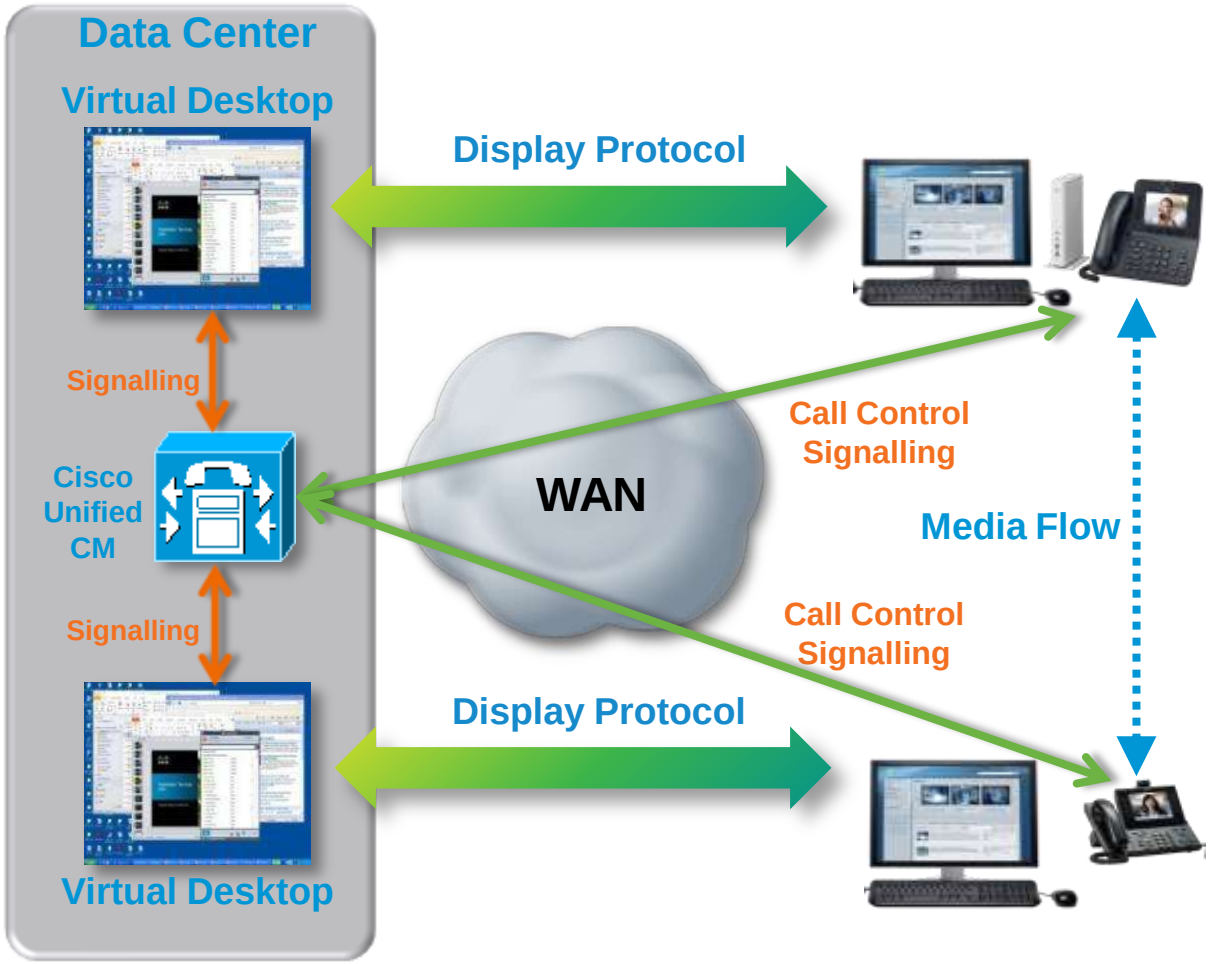
Hairpin Effect



- Voice/Video embedded in the display protocol
- Media flow goes all the way back to data center and back
- Heavy processing on virtual desktop in data center
- Bandwidth explosion
- Latency and jitter
- Display protocol and possible endpoint become unstable

Voice, Video, Virtual Desktop Zero Clients

Cisco Unified Communications using desk phone control



- UC media “voice/video” (RTP) flows outside the display protocol
- Signaling of Cisco UC Client back to Unified CM remains inside the display protocol
- QoS can be used on media
- Path is optimized
- Location Awareness and 911, Codec selection, CAC, SRST, Reference, Time Zone, Dial-Plan

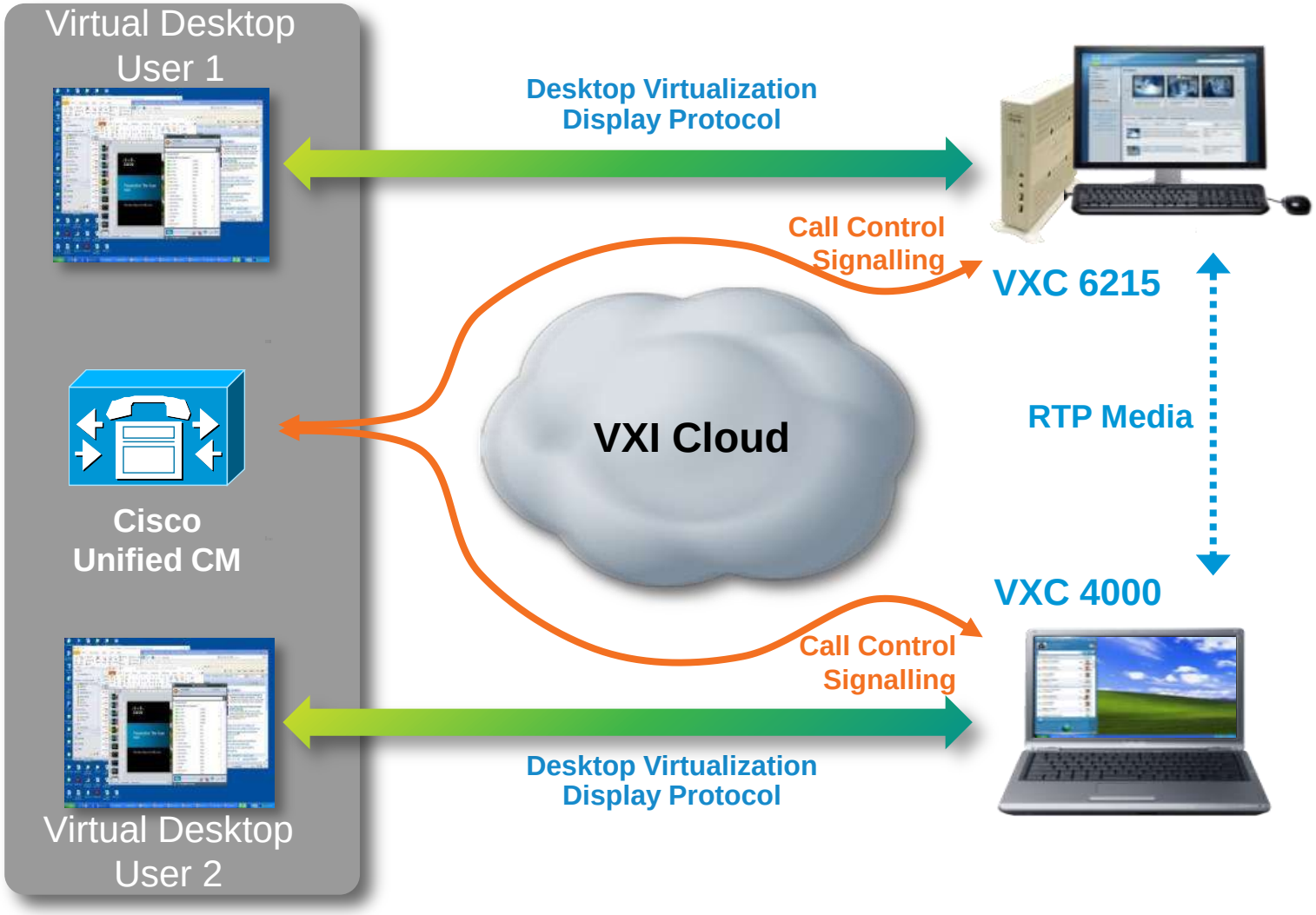
Collaboration
Citrix XenDesktop and RDP

	Phone Integrated	Stand Alone
Model	VXC-2112	VXC-2212
Software	ICA 11.x, RDP 6.x (No View 4 support)	
I/O	4 x USB 2.0 1 x DVI-D 1 x VGA (1920x1200) 1 x Analog Audio	4 x USB 2.0 1 x DVI-D 1 x VGA (1920x1200) 1 x RJ45, 1 x Analog Audio
Network	89XX/99XX Phone Phone Ethernet (No WiFi)	Ethernet (No WiFi)
Power Over Ethernet	802.3AT supports Phone with No Camera All other configurations require a Power Brick	1 Display – 802.3AF Optional Power Brick

Collaboration
VMware View PCoIP

	Phone Integrated	Stand Alone
Model	VXC-2111	VXC-2211
I/O	4 x USB1.1 2 x DVI-I (1920x1200) 1 x Analog Audio	4 x USB1.1 2 x DVI-I (1920x1200) 1 x RJ45, 1 x Analog Audio
Network	89XX/99XX Phone Phone Ethernet (No WiFi)	Ethernet (No WiFi)
Power Over Ethernet	802.3AT supports Phone with No Camera All other configurations require a Power Cube	1 Display – 802.3AF 2 Displays – 802.3AT Optional Power Cube

Convergence of VDI, Video, and Voice



Cisco VXC 6215

- A thin client that unifies voice, video, and virtual desktop in one device
- Supports high quality, scalable voice and video, delivering optimal user experience
- Introduces unique voice and video processing capabilities that efficiently use network and data center CPU resources, eliminating the hairpin effect
- Linux based platform supports VDI deployment only with HDX/ICA, PCoIP, & RDP

Cisco VXC 4000

- Enables UC voice only capabilities for repurposed windows PCs for virtual desktops
- Introduces unique voice processing capabilities that efficiently use network and data center CPU resources, eliminating the hairpin effect
- Supports Citrix XenDesktop and VMware View
- Based on Cisco IP Communicator
- OS support: Windows XP, Windows 7

Cisco CIUS

Enterprise tablet that combines voice, video, collaboration, and VDI

Supports external Bluetooth/USB mouse & keyboard when docked

Supports external display in "mirror mode"

Supports Citrix Receiver, VMware View Client and Wyse PocketCloud

VXC Feature Comparison

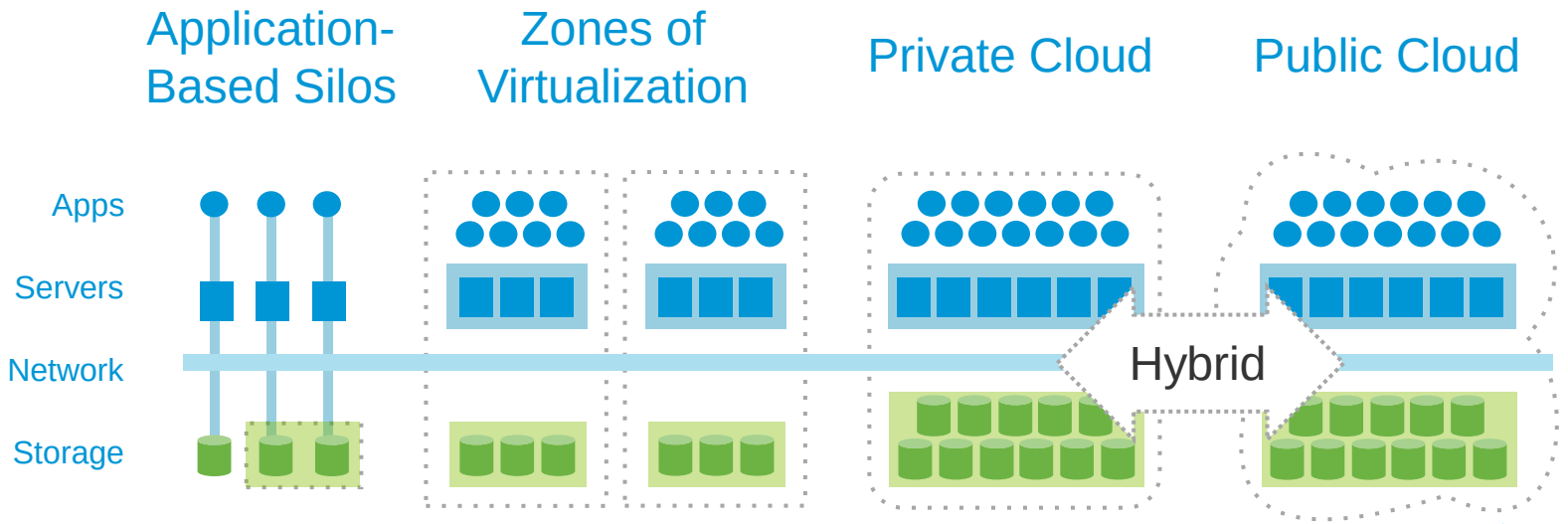




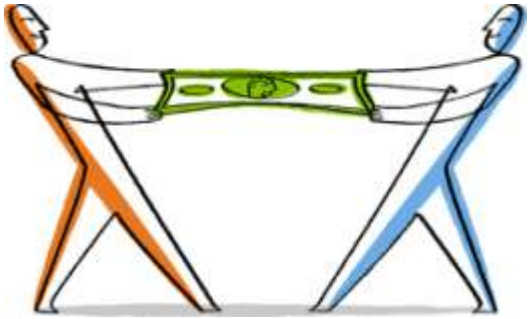
	VXC 2100 Series	VXC 2200 Series	VXC 4000*	VXC 6215*	Cisco Cius
Form Factor	"Backpack" Integrated	"Tower" Standalone	PC Software	"Tower" Standalone	Enterprise Tablet
Availability	Shipping	Shipping	Shipping	Shipping	Shipping
Platform	Zero Client	Zero Client	Win7, XP	Linux	Android (x86)
HVD Protocol Support	2111 – PCoIP 2112 – HDX,RDP	2211 – PCoIP 2212 – HDX,RDP	Citrix XenDesktop, VMware View	Citrix XenDesktop, VMware View, RDP	Citrix XenDesktop, VMware View
UC Protocol Support (add on)	N/A	N/A	Software Appliance	HDX, RDP PCoIP	N/A
UC Client Support*	CUPC, Connect	CUPC, Connect	CUPC, CUCILync	CUPC, CUCILync	Native
Voice	IP Phone 8961, 9951, 9971	N/A, can be used with IP Phone	Yes	Yes	Yes
Video	IP Phone 9971, 9951	N/A, can be used with IP Video Phone	No	Yes	Yes
Monitor Support	Single or Dual, 1920x1200	Single or Dual, 1920x1200	Varies based on underlying HW	Single:2560x1600 Dual:1920x1200	Single Mirror, 1024x600 (on the roadmap for dual monitor support)
PoE	PoE	PoE	N/A	No	PoE
Encoding & Decoding	Via IP Phone	Via IP Phone	Audio only. Video on the roadmap.	Standard Video HD Capable*	HD Capable (720p)

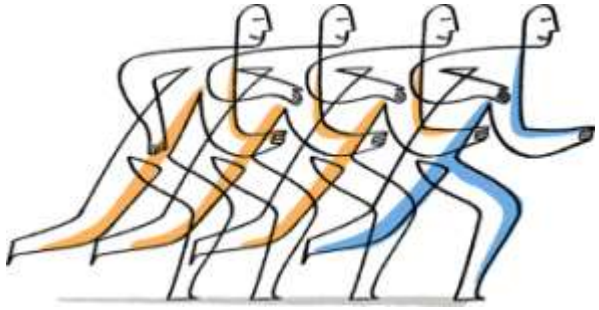
VDI & NetApp Storage

Transitioning from Virtualization to ITaaS



Workloads moving increasingly to virtualized cloud infrastructure





Software Efficiencies

RAID 6 Protection (RAID-DP®)

Protects against double disk failure with no performance penalty.

Thin Provisioning (FlexVol®)

Create flexible volumes that appear to be a certain size but are really a much smaller pool.

Thin Replication (SnapVault® and SnapMirror®)

Make data copies for disaster recovery and backup using a minimal amount of space.

Snapshot™ Copies

Point-in-time copies that write only changed blocks. No performance penalty.

Virtual Copies (FlexClone®)

Near-zero space, instant “virtual” copies. Only subsequent changes in cloned dataset get stored.

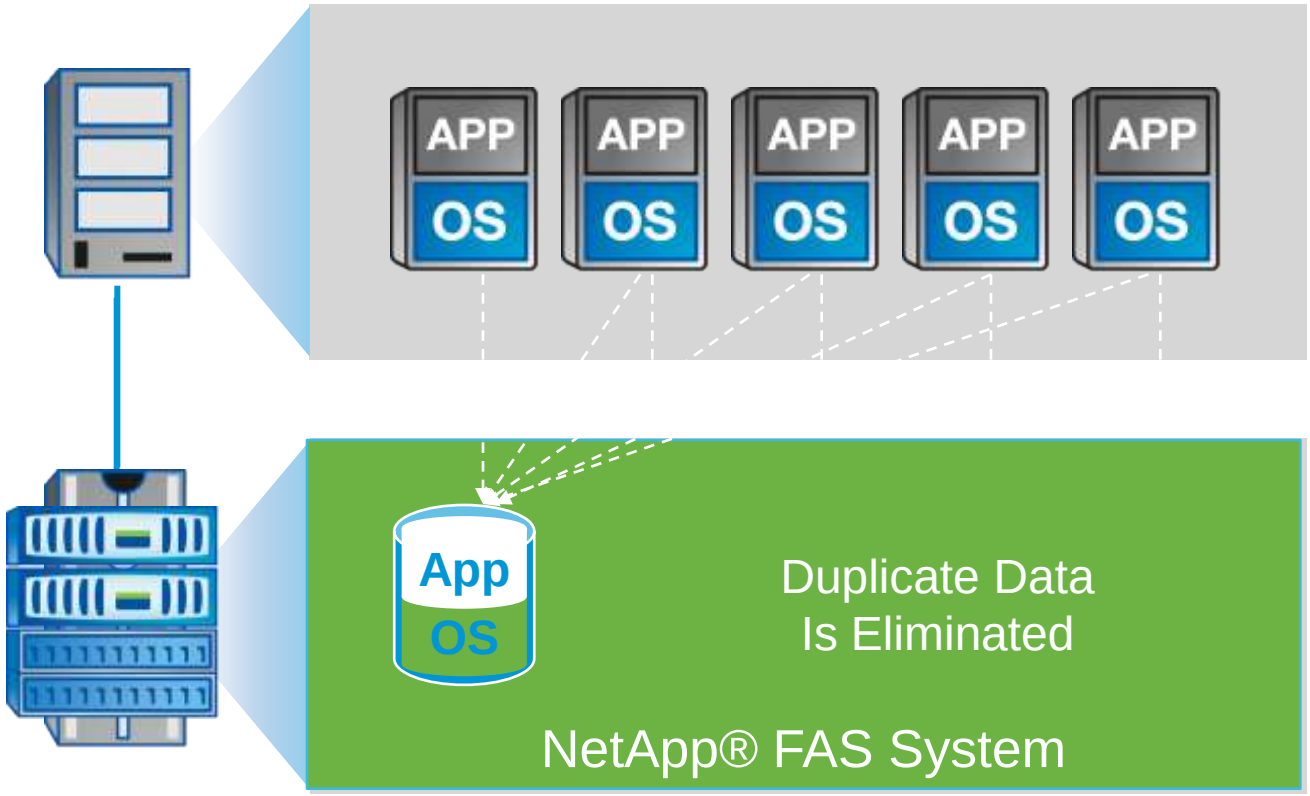
Deduplication

Removes data redundancies in primary and secondary storage.

Data Compression

Removes redundant data patterns in primary and secondary storage.

Deduplication: Essential for Virtualization

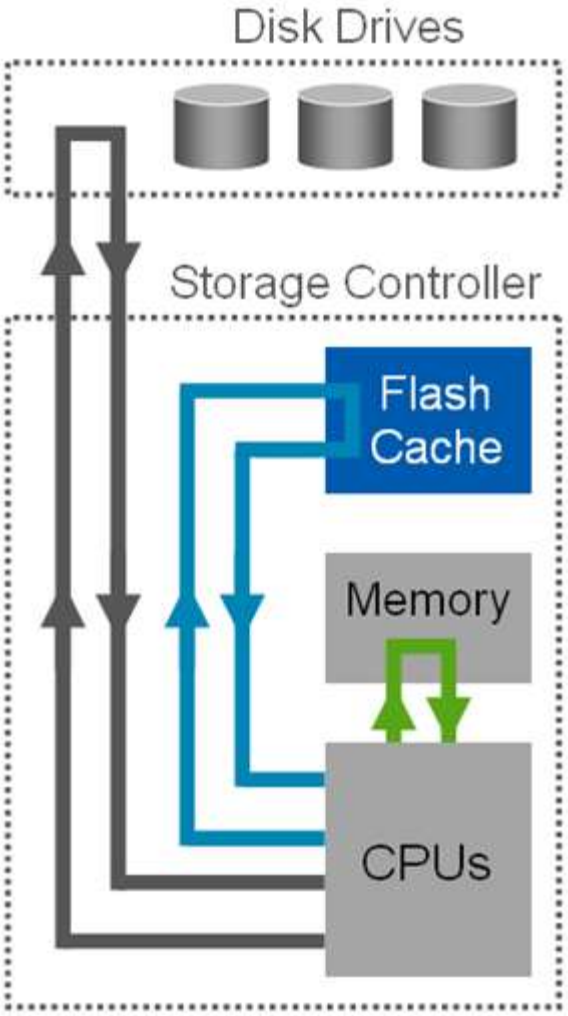


Savings extend to all copies of the data

Including backup, DR, test clones, and archival copies

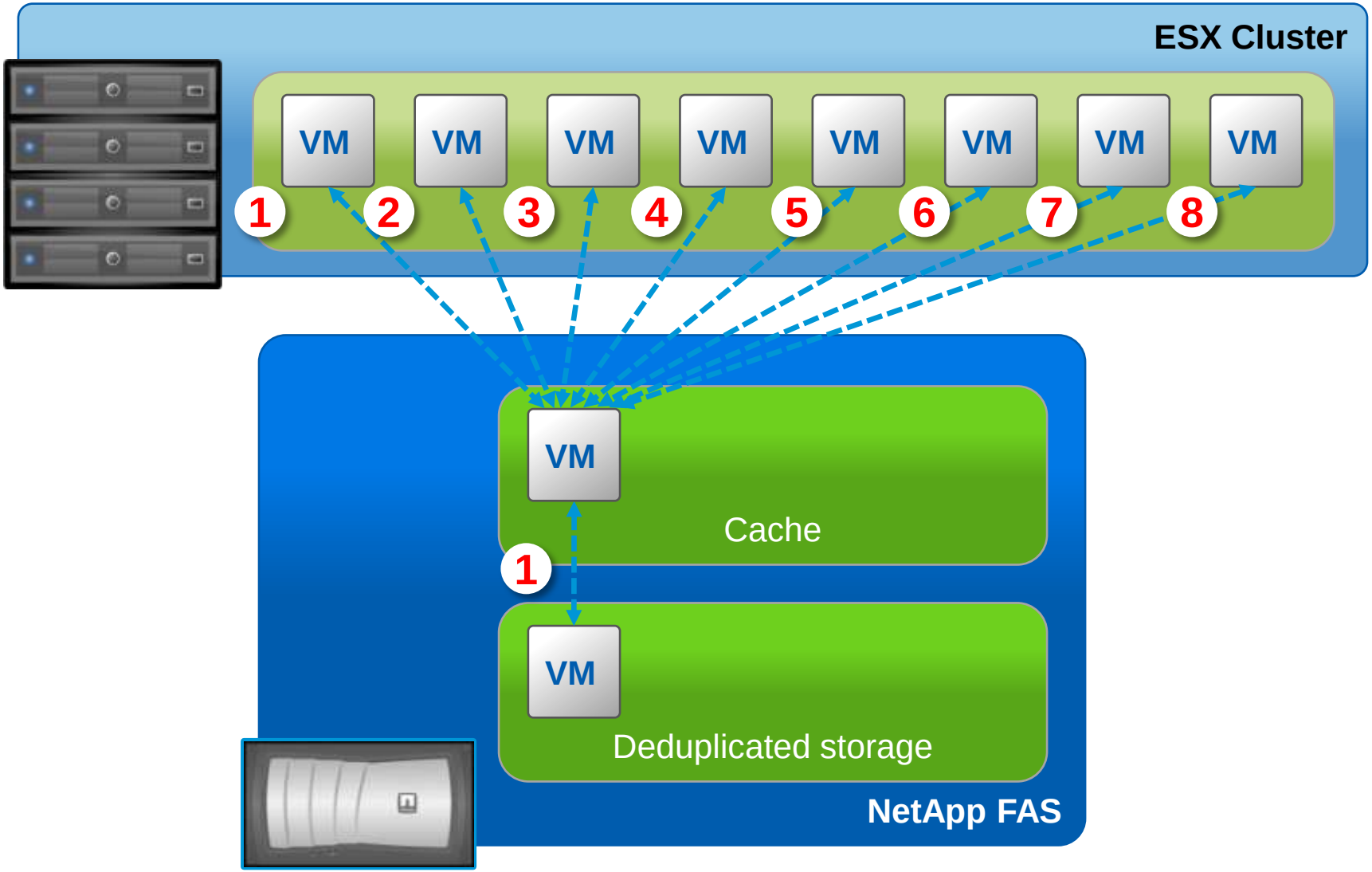
NetApp FlashCache Performance with Extreme Efficiency

- Flash Cache improves average **latency** for random reads
- Increase **I/O throughput** of disk-bound storage systems without adding more disk drives
- Reduce **costs** by using fewer, larger disk drives
- **Effective** for file services, databases, messaging, and virtual infrastructure
- **Predict** your results before buying for an existing storage system



Synergy of Flash Cache and Deduplication

Reducing the Duration of Boot Storms in a Virtual Infrastructure



Flexible Storage
A Single, Unified Platform

Single, Unified Storage Platform

Low-to-High Scalability

Multiple Networks

Multiple Protocols

- SAN
- NAS
- iSCSI

Multiple Disks

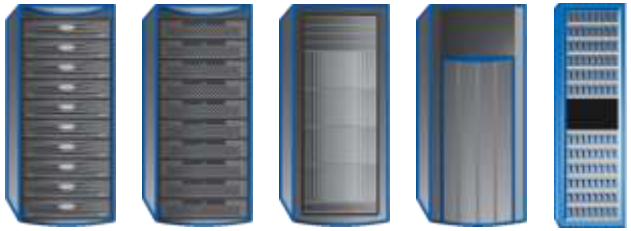
- FC
- SATA
- SSD

Unified Management

- Same tools and processes: learn once, run everywhere
- Integrated management
- Integrated data protection

Storage Virtualization

Multivendor Virtualization



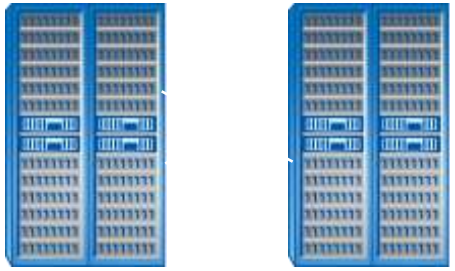
Unified Flash

Flash Cache

SSD

FlexCache®

Unified Scaleout

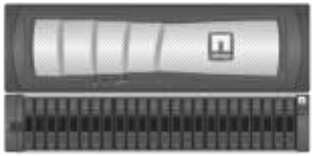


Introducing FlexPod

Cisco® UCS B-Series Blade Servers and UCS Manager

Cisco Nexus® Family Switches

NetApp® FAS 10GE and FCoE



Shared infrastructure for wide range of environments and applications

Benefits

- Low-risk standardized shared infrastructure supporting a wide range of environments
- Highest possible data center efficiency
- IT flexibility, providing business agility: scale out or up, but manage resource pools

Features

- Complete data center in a single rack
- Performance-matched stack
- Step-by-step deployment guides
- Multiple classes of computing and storage supported in a single FlexPod
- Centralized management: NetApp OnCommand and Cisco® UCS Manager

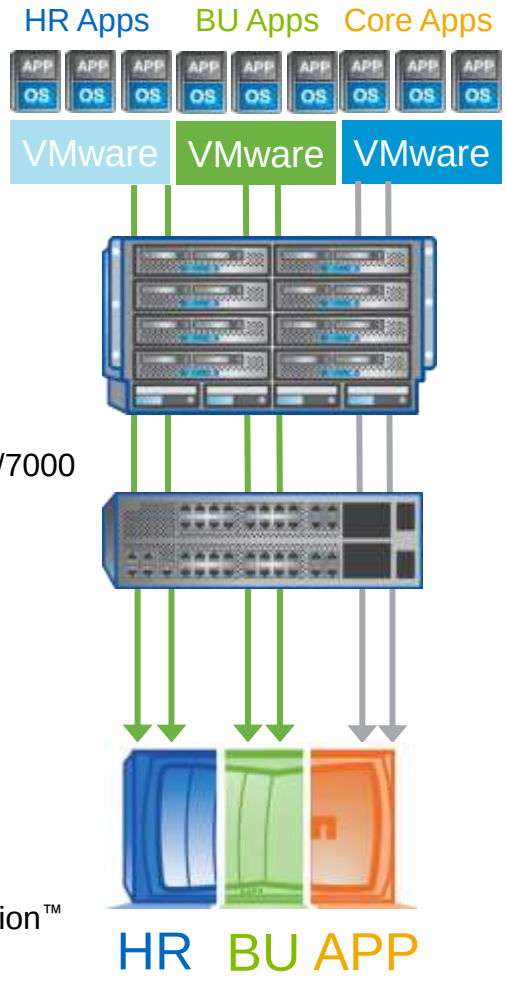
Secure Multi-Tenancy

The industry's only end-to-end secure multi-tenancy solution

vmware
- vSphere™
- vShield Zones
- vCenter™

CISCO
- Nexus 1000V
- Nexus 2000/5000/7000
- UCS
- 10GbE

NetApp™
- MultiStore®
- NetApp Data Motion™
- NFS/iSCSI



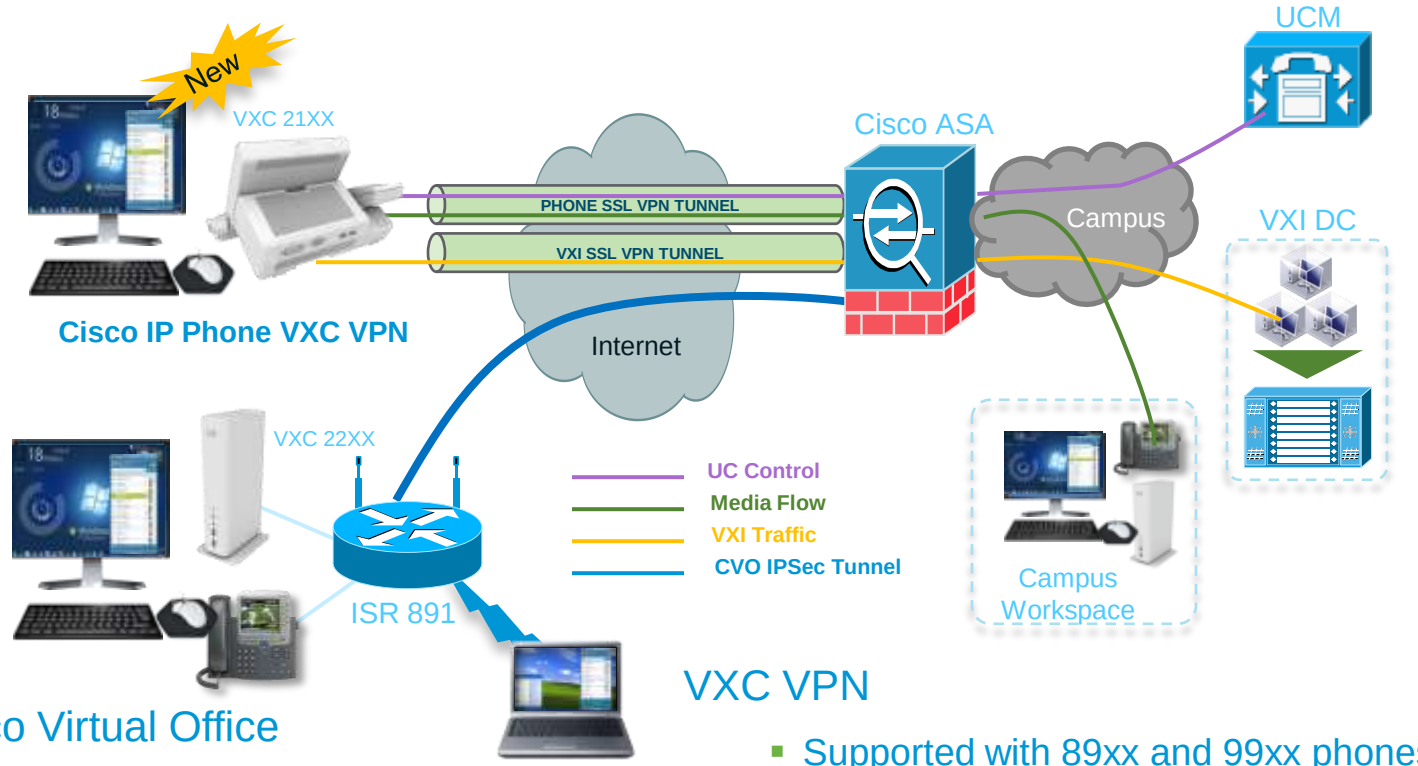
- Securely isolate shared compute, network, and storage resources
- Consistent QoS at each layer
- Manage each resource pool independently as a dynamic asset
- Reduce risk and cost while boosting IT agility
- A Cisco Validated Design
- Security audited by ICSA Labs
- PCI compliant

Cisco VXI Security

Need for Security in VDI

- Enterprises expect security policy compliance. Compliance is typically achieved by using technologies such as 802 1.x based machine and user authentication, IPSec/SSL VPNs, Smartcards, 2 factor authentication, certificate based authentication
- Moving to desktop virtualization creates an access layer in the data center that needs to be secured similar to the Campus access
- To enable BYOD in highly flexible hybrid deployments, device profiling, access restrictions and versatile remote access solutions are required
- Antivirus solutions for VDI environment are required without impacting TCO

Secure access for Teleworkers and Small branches



- Cisco Virtual Office
  - VXI ACLs to allow only Display traffic
  - VXC 2112, 2212, 4000, 6215 supported using 802.1x, MAB and Auth Proxy
  - WiFi support for mobile endpoints

VXC VPN

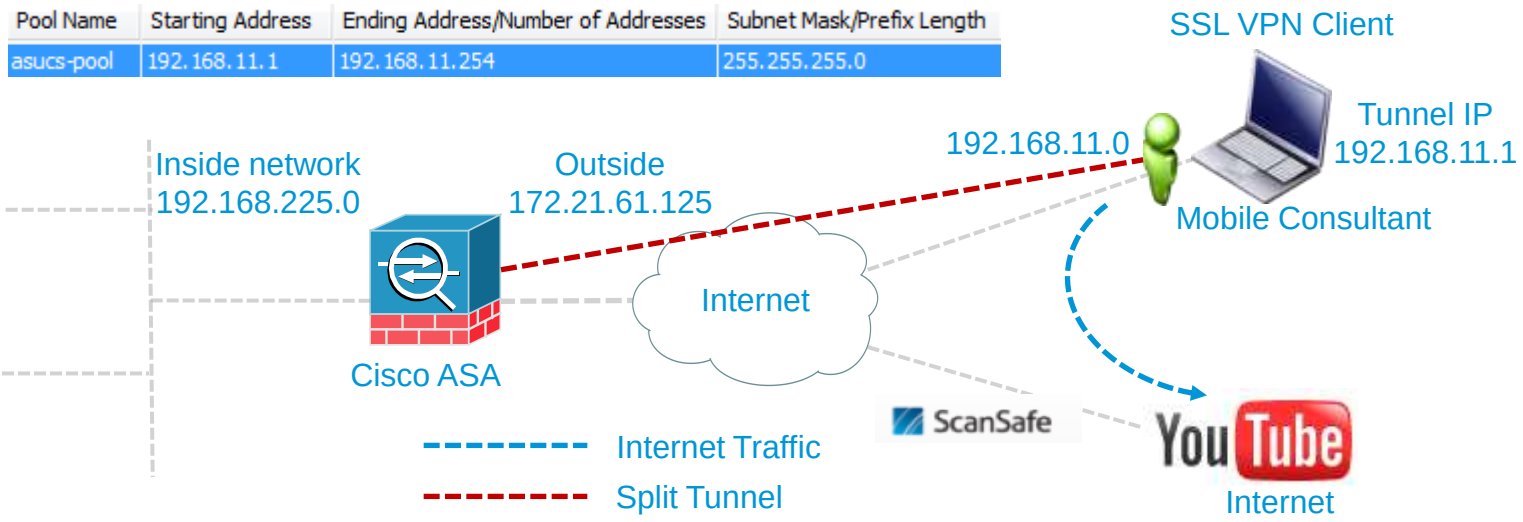
- Supported with 89xx and 99xx phones with Phone load 9.2.3 and CUCM 9.0
- Requires ASA to terminate two tunnels
- Two SSL VPN licenses consumed on the ASA
- Unified communication traffic prioritized over VXI traffic
- Computer port on the phone protected by VXI ACL and MAC address authentication

Secure Remote Connectivity with AnyConnect 3.0

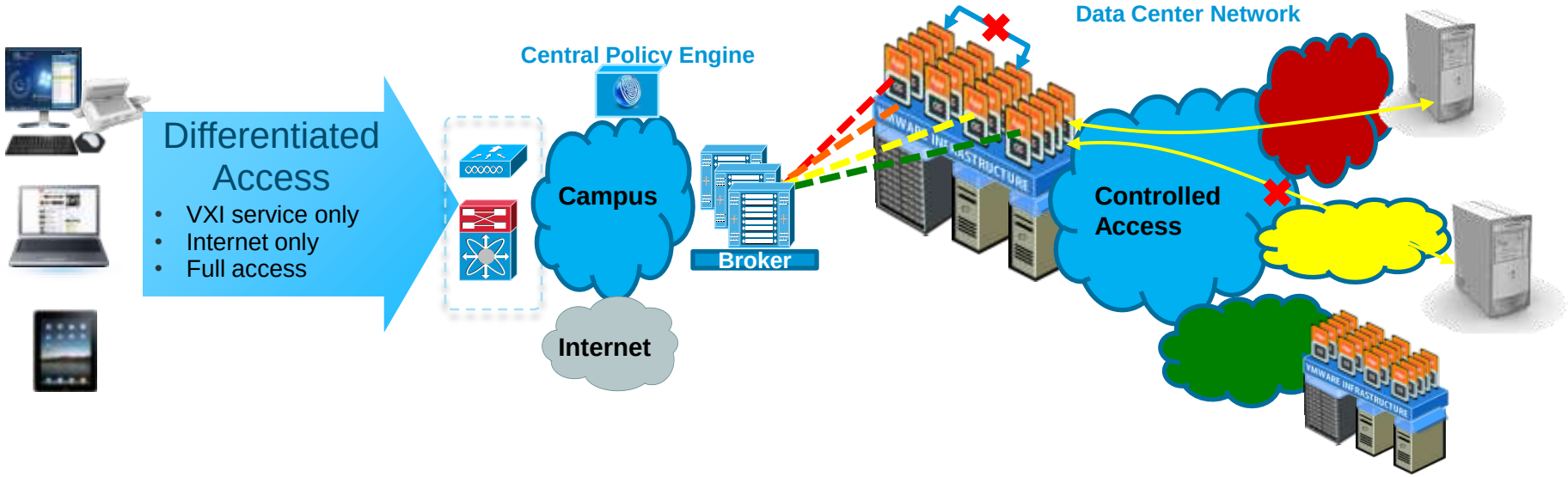
- Anyconnect has the largest footprint of supported devices
  - Thick endpoints: Windows, Mac and Linux
  - Apple iOS 4 - Including iPhone
  - Cisco VXC endpoints not supported today
  - iPad and CIUS support Anyconnect 2.5 only
- Always On or On-Demand VPN
- Auto Re-Connect (Persistence)
- Built-In Digital Cert Support
- Support for VDI Applications/ Receiver Support

Secure Remote Access with VXI

- AnyConnect on Mobile Client allows secure remote connections to corporate network and Virtual Desktops
- Split tunneling and ScanSafe allow secure remote access to Internet from local browser on the endpoint or from within Virtual Desktop
- Web traffic is inspected by WSA at HQ or in the ScanSafe Cloud
- VXI traffic is forwarded to the DataCenter
- Remote HVD access using Cisco VPN technology allows access to both VXI and non-VXI applications while still using a single, and in most cases existing, infrastructure.

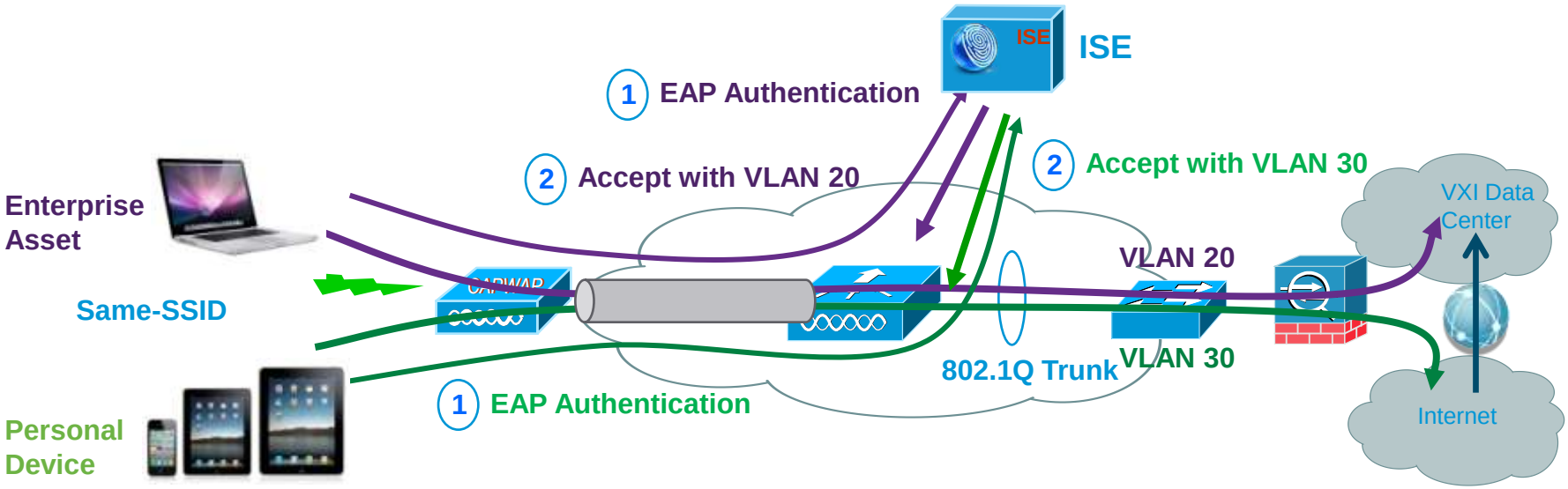


End-End Access control in VXI



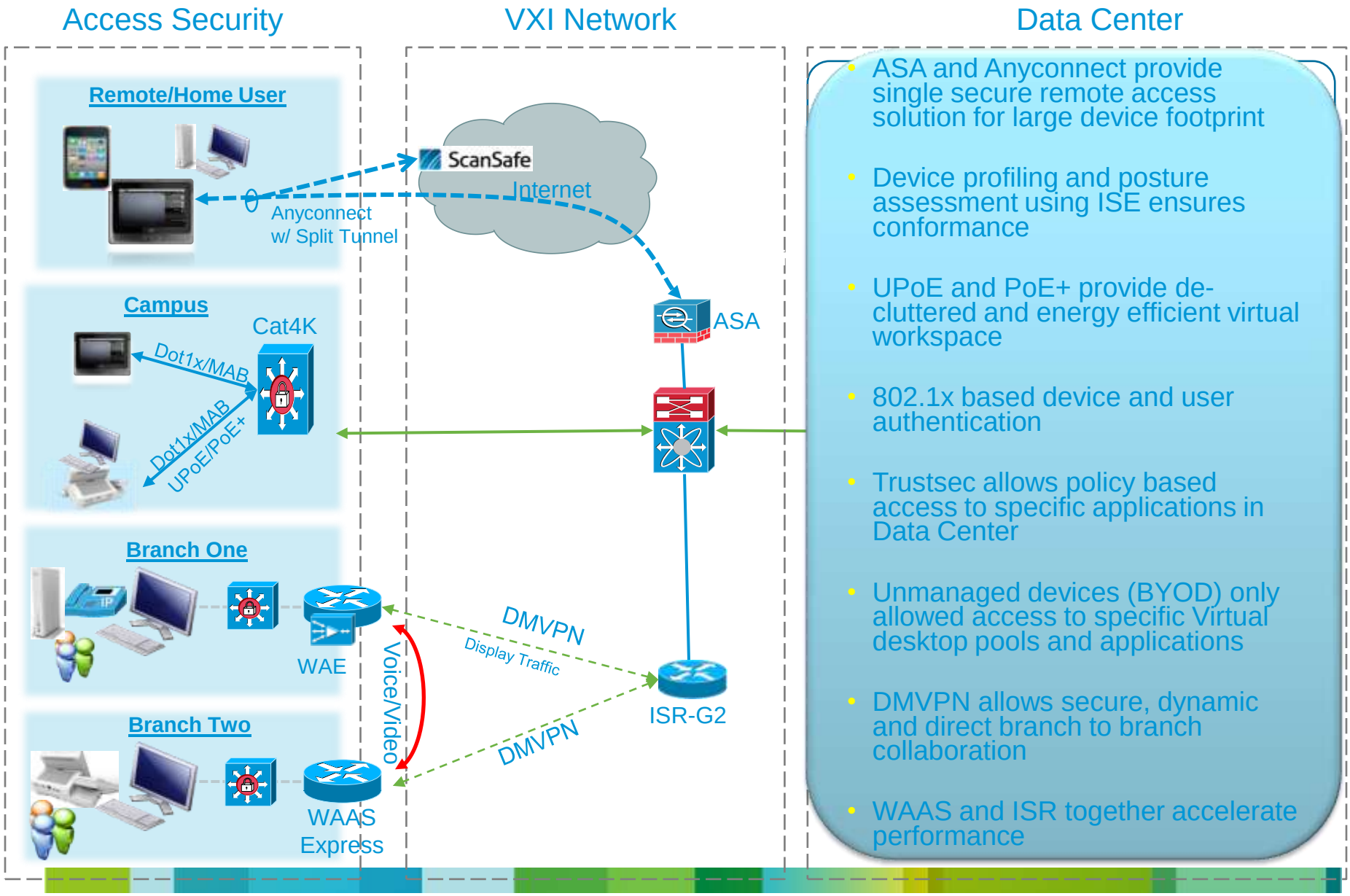
- Policy Based Device/User Network Access
  - Enable differentiated network access to Device/User type
  - Utilize existing network access control infrastructure
  - Allow controlled access only to VXI infrastructure for Employee owned assets, Temporary workers etc.
- Policy Based DC resource access **from** HVD
  - Common VDI infrastructure for different user groups for cost and flexibility reasons
  - Controlled access to sensitive resources in Data Center
  - Using Security Group Access
    - Goal: Extend existing SGA based access control to VDI (SMB)
  - Using Virtual Switch and Virtual Firewall
    - Goal: Provide access level security closest to HVD (including east-west traffic Control)
    - Open to separate policy management using virtual firewalls

Policy based VXI access using ISE

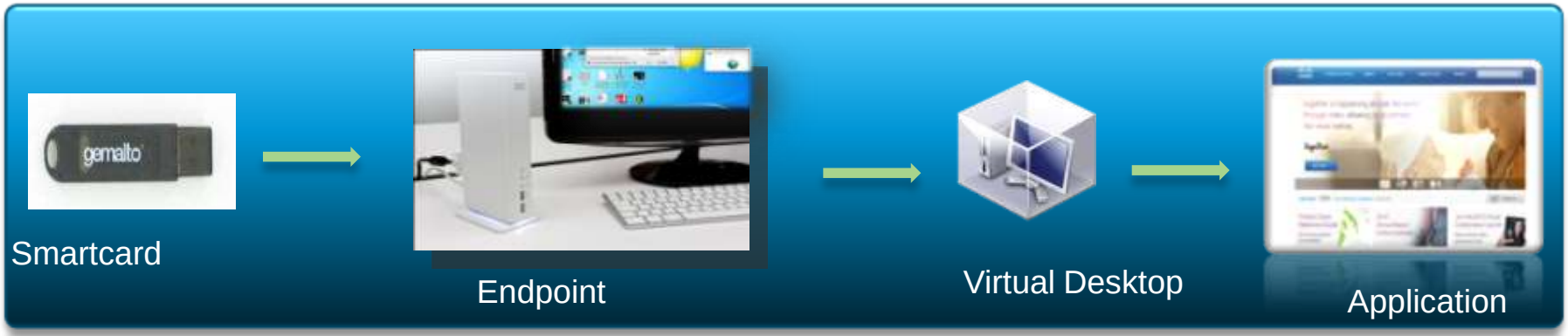


- Data Containment in personal devices using ISE
- Device Profiling
- Simplified, Scalable Access Policy
- Corporate device with AD credential and certificate (EAP-TLS), is corporate access to the network
- Bring Your Own Devices (BYOD) will be given only limited access

VXI Security deployment scenarios



Smartcards support on VXC



- Smartcard Support on VXC 2000 series for user authentication in Citrix XenDesktop 5.0/5.5 or VMware View 4.6/5.0 environments
- Multiple deployment models such as Campus, Branch, Home User supported
- Multiple industries globally (Healthcare, Financial, Federal, Defense etc.) mandate Smart Cards
- USB based smartcards validated with certificates on VXC 21xx and 22xx

Smart Card	Smart Card Reader	Validated DV Environment
Gemalto Smart Card .NET V2+	Omnikey Cardman 5321	XenDesktop 5.0
Gemalto Smart Card .NET V2+	Gemalto PC Link Reader - PC USB TR	VMware View 4.6/5.0 and XenDesktop 5.0
ActivClient Common Access Cards (CAC)	SCM SCR331	VMware View 4.6 /5.0

Under Test

- Locally connected smart cards available in HVD using USB redirection or if endpoint supports drivers
- Smart Card Solution Components
  - Smart Card Middleware (Mini Driver) and USB Reader Driver on each Hosted Virtual Desktop
  - Smart Card Authentication enabled in HVD and Broker
  - Certificate Authority
  - Root certificate on all devices (Broker, Endpoint, Active directory and HVD)
  - Certificate with pin installed on Smart Card

Anti-Virus in VXI

Virus scan is an essential component of Virtual desktop environments

VXI offers choices from an ecosystem of validated AV solutions optimized for Desktop Virtualization

Traditional AV software, even when optimized, impact HVD densities and hence the TCO

Workload Profile	AV Scan Policy	HVD Density
KW only	N/A	110/110
KW with MoveAV 1.5	Default	90/90

18% impact on HVD Density

XenDesktop 5/ ESXi 4.1 , Win 7 32b/1.5G/20G
Optimizations done based on Citrix/VMware recommendations

Workload Profile	AV Scan Policy	HVD Density
KW only	N/A	110/110
KW with MoveAV 1.5	Default	90/90

18% impact on HVD Density

View 4.5/ ESXi 4.1 , Win 7 32b/1.5G/20G
Optimizations done based on Citrix/VMware recommendations

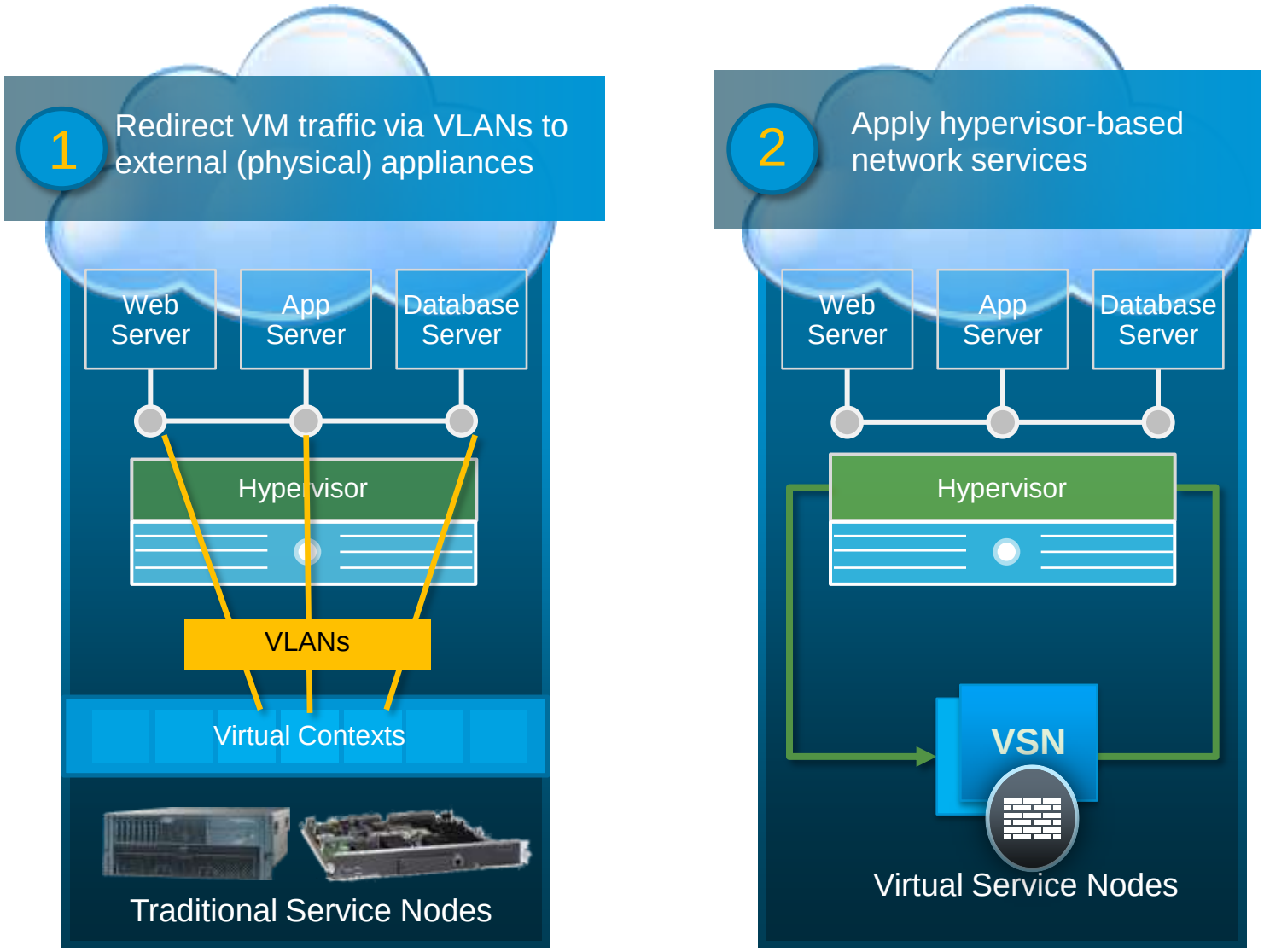
Trend Micro Anti-Virus solution has been added to VXI Phase 2.5 along with McAfee MOVE-AV 1.5

Storage IOPS requirements and Login/Boot/AV Storms should be considered in the design apart from HVD density impact

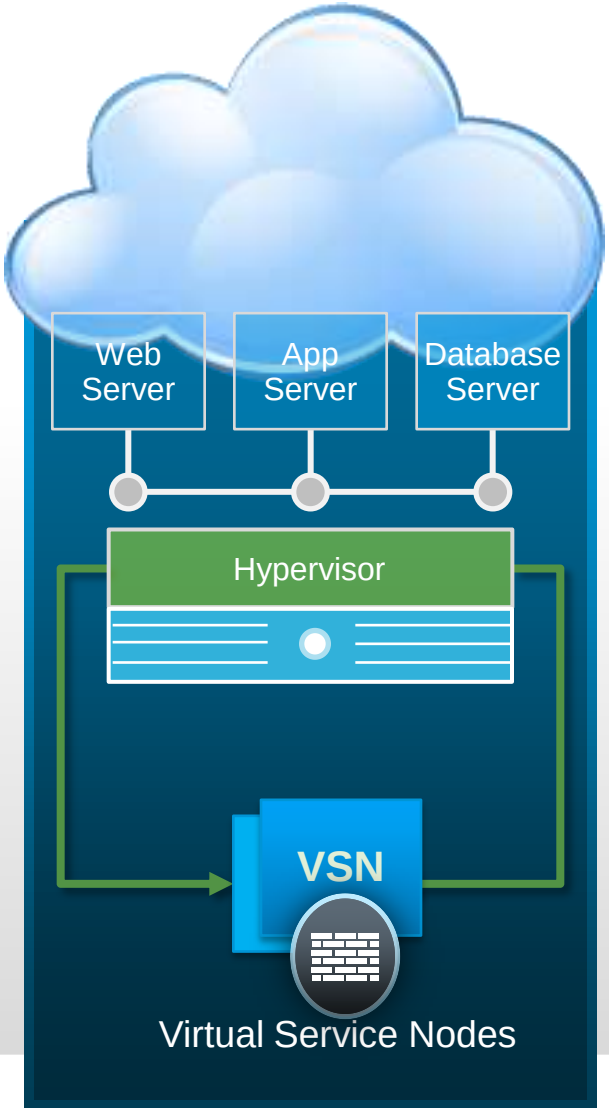
Licensing and Support directly from AV vendor

DC Security

Physical and Virtual Service Nodes



Virtualization & Virtual Service Nodes



Nexus 1000V

Virtual Security Gateway

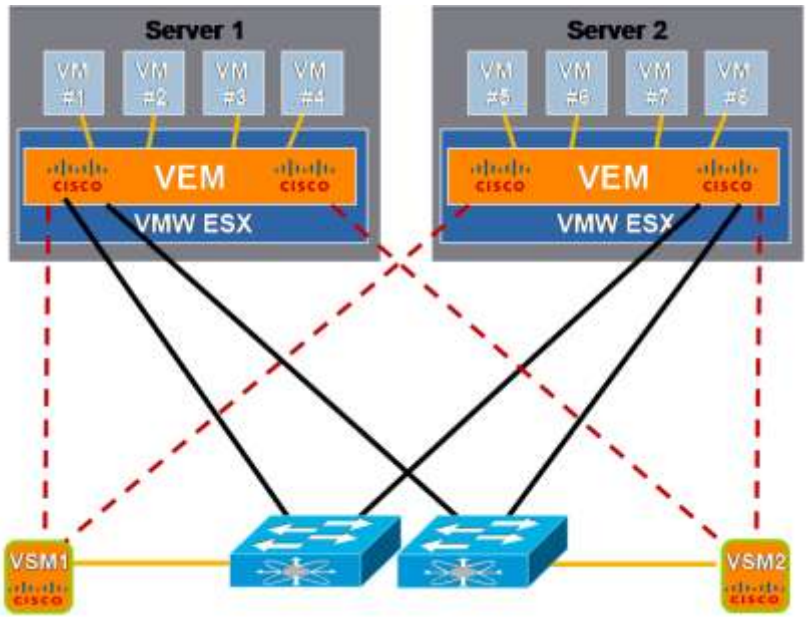
Zone based intra-tenant segmentation of VMs

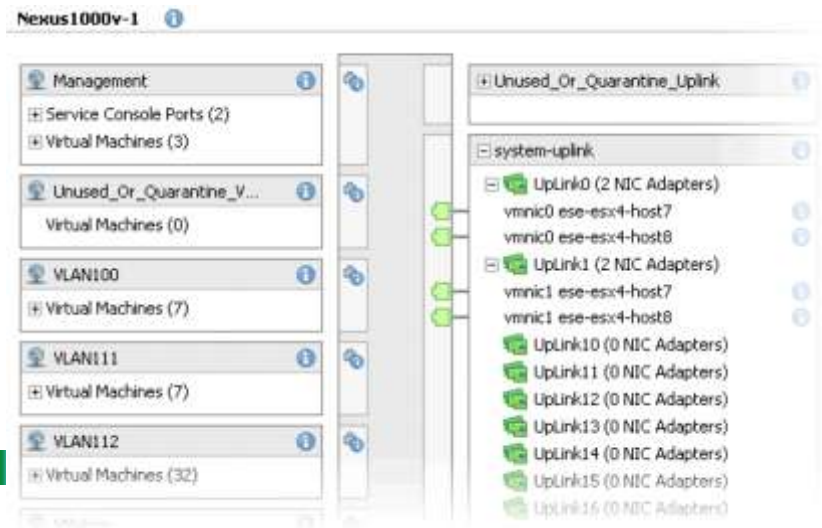
ASA 1000V

Ingress/Egress multi-tenant edge deployment

Nexus 1000v per VM Network Services

- Client LAN Features
  - DHCP Snooping
  - Dynamic ARP Inspection
  - IP Source Guard
- Virtual Ethernet Module (VEM)
  - Networking capabilities at the hypervisor level
  - L2 switching, CDP, Netflow, ACLs, QoS, SNMP, SPAN, etc
  - Local Switching
  - Port Profile to simplify Network Policy
- Virtual Supervisor Module (VSM)
  - Mgmt, monitoring and config of VEM instances
  - Sees each VEM as a virtual chassis module
  - Configuration done through port-profiles
  - Tight integration with Virtual Center
  - Runs on dedicated appliance or virtual machine
- Virtual Chassis Concept
  - Redundant Supervisors (VSMs)
  - Currently up to 128 VEM instances (128 ESX hosts)
  - Presents a network view of the virtual access layer

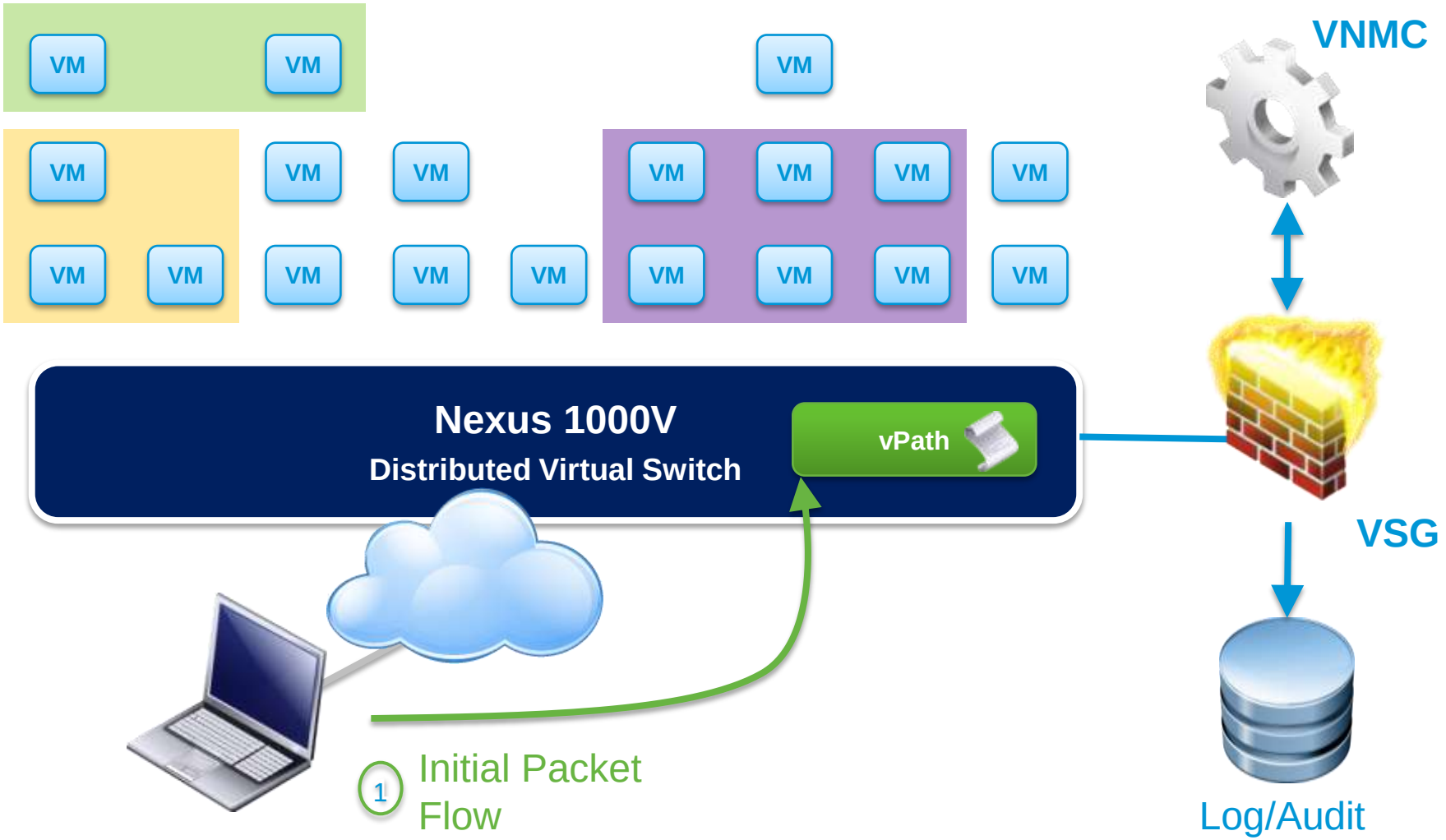




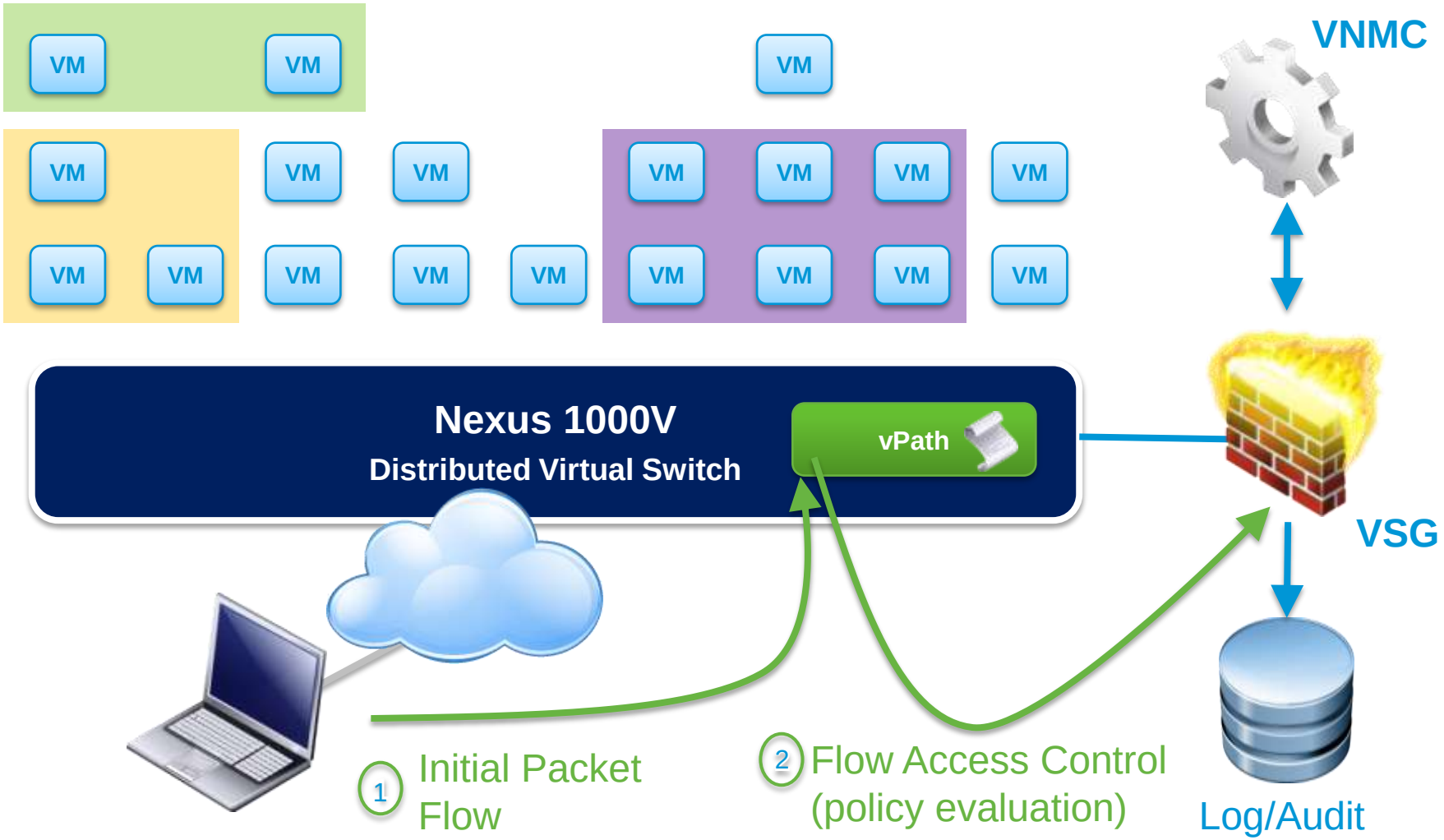
vPath— The intelligent virtual network

- vPath is intelligence build into Virtual Ethernet Module (VEM) of Nexus 1000V (1.4 and above)
- vPath has two main functions:
  - Intelligent Traffic Steering
  - Offload processing via Fastpath from Virtual Service Nodes to VEM
- Dynamic Security Policy Provisioning (via security profile)
- Leveraging vPath enhances the service performance by moving the processing to Hypervisor

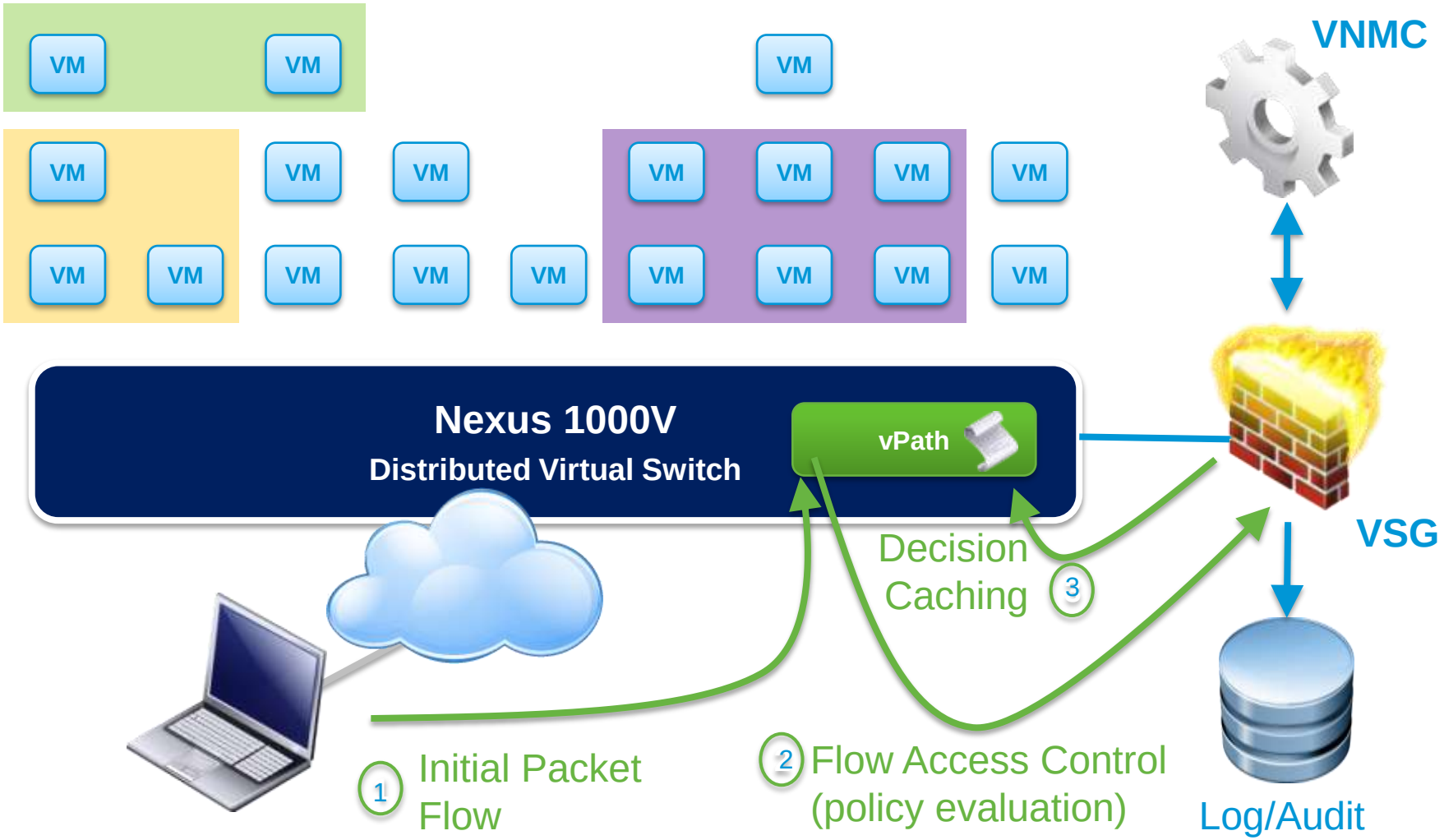
Virtual Security Gateway
Intelligent Traffic Steering with vPath



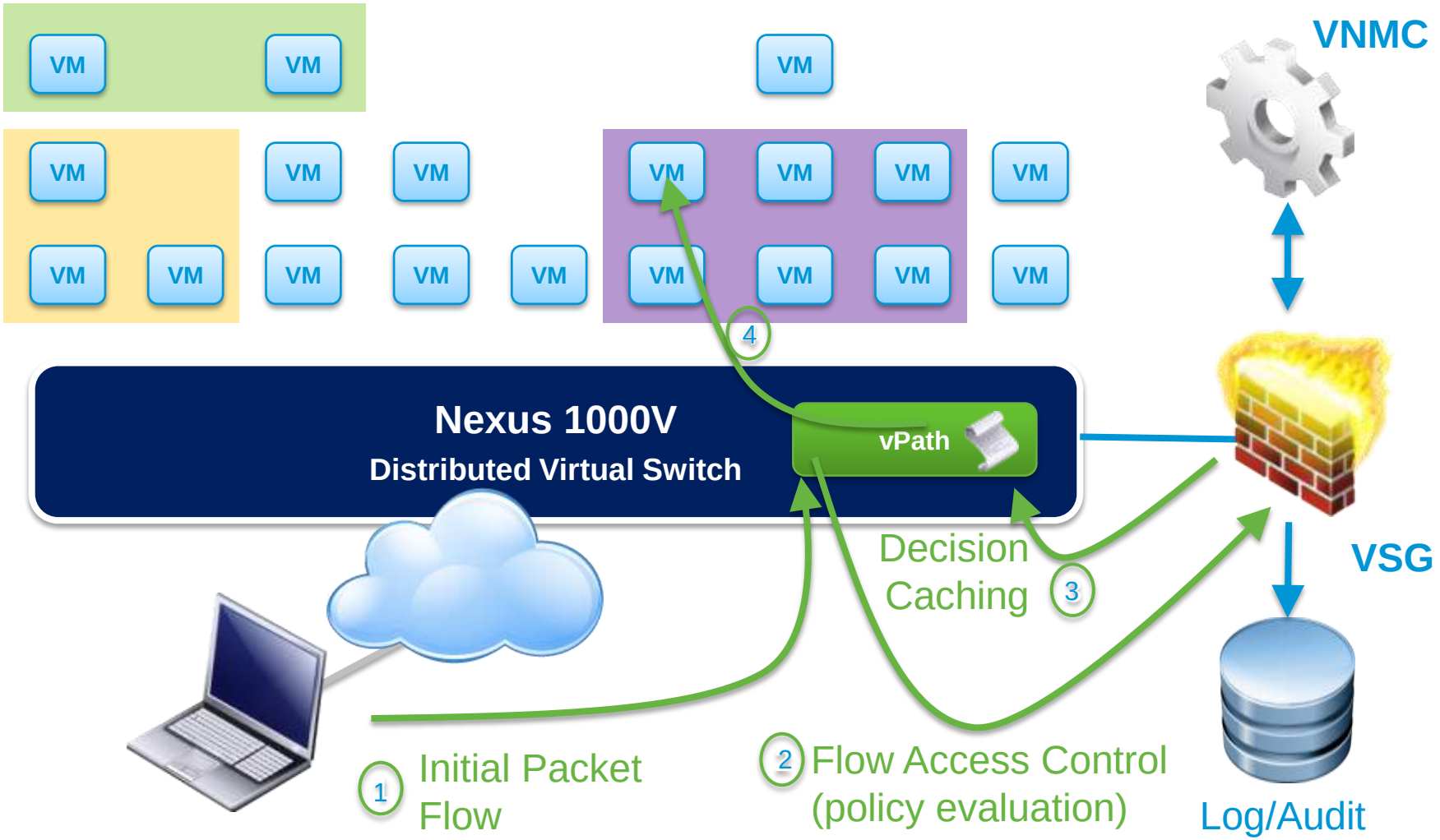
Virtual Security Gateway
Intelligent Traffic Steering with vPath



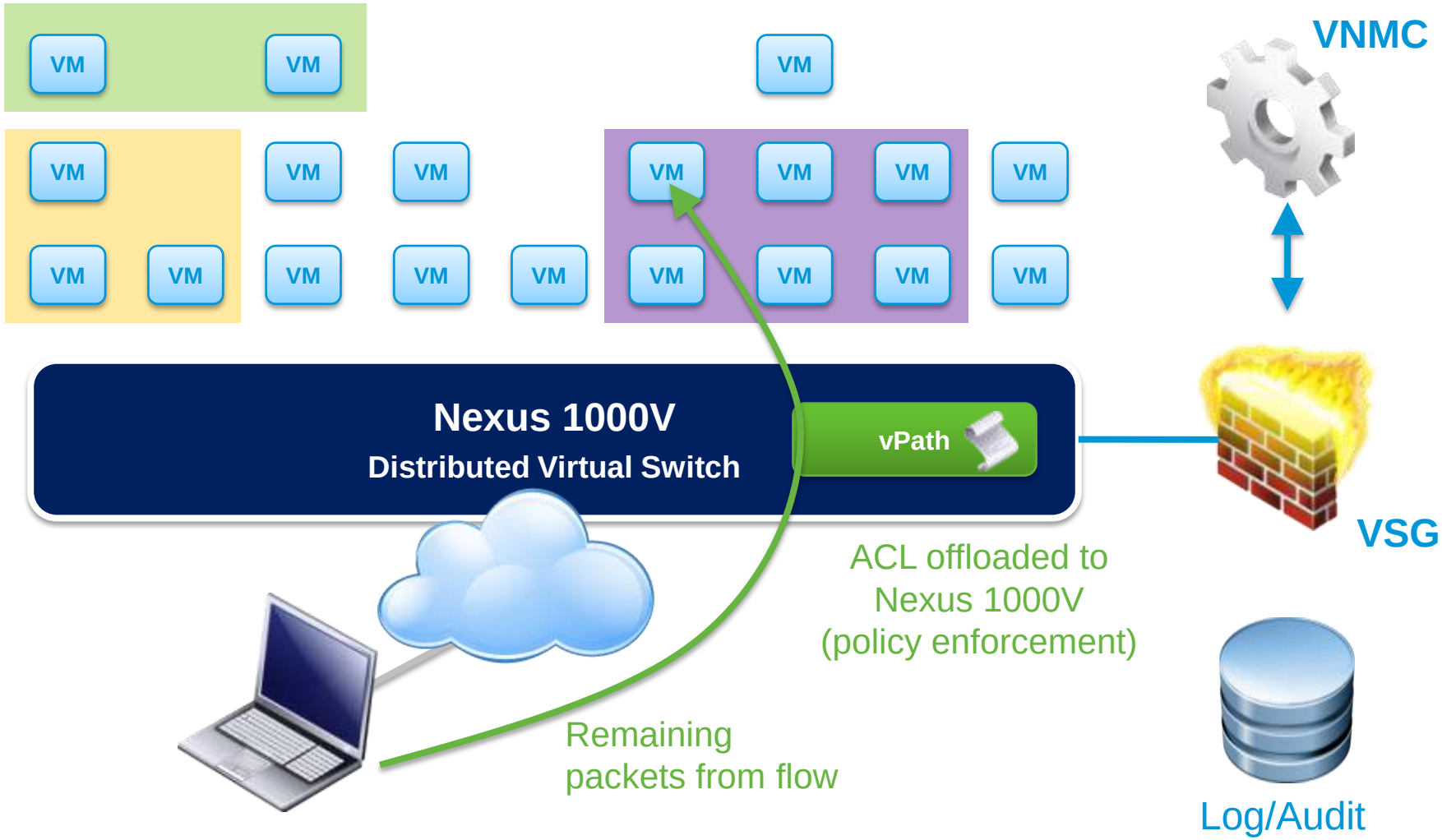
Virtual Security Gateway
Intelligent Traffic Steering with vPath



Virtual Security Gateway
Intelligent Traffic Steering with vPath



Virtual Security Gateway
Performance Acceleration with vPath



Cisco Virtual Security Gateway

Virtual Security Gateway (VSG)

Context aware Security	VM context aware rules
Zone based Controls	Establish zones of trust
Dynamic, Agile	Policies follow vMotion
Best-in-class Architecture	Efficient, Fast, Scale-out SW

Virtual Network Management Center (VNMC)

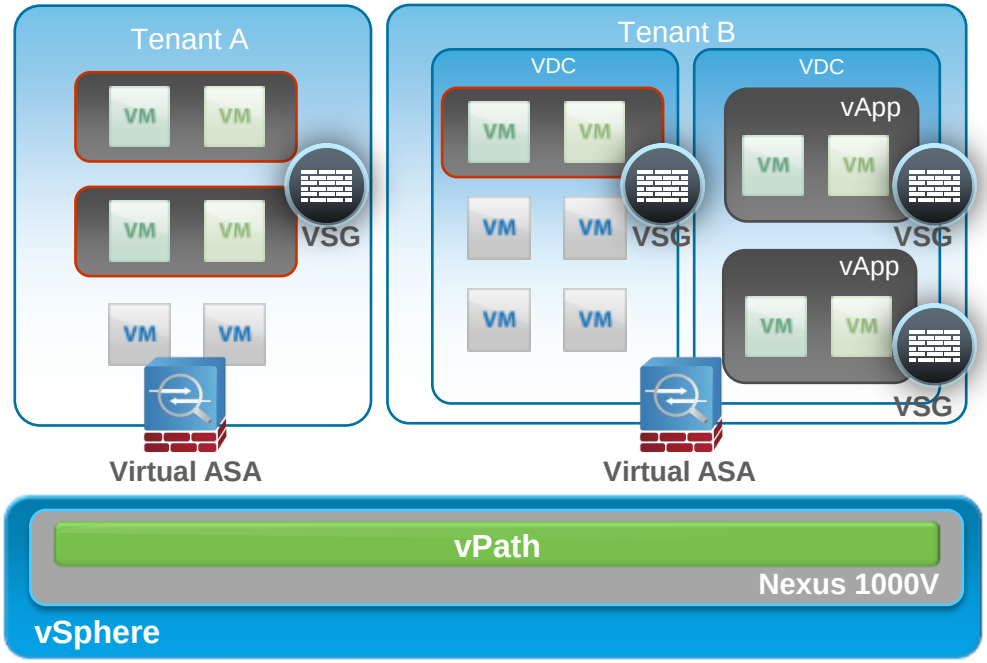
Non-Disruptive Operations	Security team manages security
Policy Based Administration	Central mgmt, scalable deployment, multi-tenancy
Designed for Automation	XML API, security profiles

Virtual Security Gateway

- Context based rule engine, where ACLs can be expressed using any combination of network (5-tuple), **custom** and **VM attributes**. It's extensible so other types of context/attributes can be added in future
- No need to deploy on every physical server (this is due to 1000V vPath intelligence)
- Hence can be deployed on a dedicated server, or hosted on a Nexus 1010 appliance
- Performance optimization via enforcement off-load to 1000V vPath
- High availability

ASA 1000v

- Runs same OS as ASA appliance and blade
- Maintains ASA Stateful Inspection Engines
- IPSEC site-to-site VPN
- Collaborative Security Model
  - VSG for intra-tenant secure zones
  - Virtual ASA for tenant edge controls
- Integration with Nexus 1000V & vPath



Conclusion

Conclusion

- Cisco VXI Virtualized End-to-End System
- User Experience
- NetApp Storage Partner
- Secure Access
- Secure Data Center

Odkazy

- VXI Page

  http://www.cisco.com/go/vxi

- VXC Clients

  http://www.cisco.com/go/vxc

- VXI Design Zone

  http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns1100/landing_vxi.html

Otázky a odpovědi

- Twitter www.twitter.com/CiscoCZ
- Talk2Cisco www.talk2cisco.cz/dotazy
- SMS 721 994 600

- Zveme Vás na **Ptali jste se…** v sále **LEO**
  1.den 17:45 – 18:30
  2.den 16:30 – 17:00

Prosíme, ohodnoťte tuto přednášku.