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](http://www.twitter.com/CiscoCZ)
- **Talk2cisco**  [www.talk2cisco.cz/dotazy](http://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
• Conclusion
Why Desktop Virtualization?
Overview
The Network Is the Desktop

- 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

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

Challenges of Traditional PC Environment

- Lost Agility & Productivity
- High TCO and Lifecycle Costs
- Heavy Administration
- Data Security Compliance
- User End point and Application Demands

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

Cisco VXI

Data Center Virtualization
Virtual Workspace
Collaboration
Borderless Networks

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
Cisco VXI Virtualized End-to-End System

Virtualized Data Center
- Applications/Desktop OS
  - Cisco Collaboration Applications
  - MS Office
- Desktop Virtualization Software
  - Citrix
  - VMware
- Hypervisor
  - Citrix
  - VMware

Virtualization-Aware Borderless Network
- Cisco® Identity Services Engine
- WAAS
- AnyConnect
- PoE
- Routing
- Switching

Virtualized Collaborative Workspace
- Cisco Virtualization Experience Clients
  - AnyConnect
  - Cisco VXC 6215 Thin Client
  - Cisco VXC 4000 PC Client
  - Cisco VXC 22xx & 21xx Zero Client
- Cius Business Tablet

End-to-End, Management and Optimization

VXI 2.5 System

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

<table>
<thead>
<tr>
<th></th>
<th>Phone Integrated</th>
<th>Stand Alone</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Model</strong></td>
<td>VXC-2112</td>
<td>VXC-2212</td>
</tr>
<tr>
<td><strong>Software</strong></td>
<td>ICA 11.x, RDP 6.x (No View 4 support)</td>
<td></td>
</tr>
<tr>
<td><strong>I/O</strong></td>
<td>4 x USB 2.0</td>
<td>4 x USB 2.0</td>
</tr>
<tr>
<td></td>
<td>1 x DVI-D</td>
<td>1 x DVI-D</td>
</tr>
<tr>
<td></td>
<td>1 x VGA (1920x1200)</td>
<td>1 x VGA (1920x1200)</td>
</tr>
<tr>
<td></td>
<td>1 x Analog Audio</td>
<td>1 x RJ45, 1 x Analog Audio</td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td>89XX/99XX Phone</td>
<td>Ethernet</td>
</tr>
<tr>
<td></td>
<td>Phone Ethernet (No WiFi)</td>
<td>(No WiFi)</td>
</tr>
<tr>
<td><strong>Power Over Ethernet</strong></td>
<td>802.3AT supports Phone with No Camera</td>
<td>1 Display – 802.3AF Optional Power Brick</td>
</tr>
<tr>
<td></td>
<td>All other configurations require a Power Brick</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Phone Integrated</td>
<td>Stand Alone</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Model</td>
<td>VXC-2111</td>
<td>VXC-2211</td>
</tr>
<tr>
<td>I/O</td>
<td>4 x USB1.1</td>
<td>4 x USB1.1</td>
</tr>
<tr>
<td></td>
<td>2 x DVI-I (1920x1200)</td>
<td>2 x DVI-I (1920x1200)</td>
</tr>
<tr>
<td></td>
<td>1 x Analog Audio</td>
<td>1 x RJ45, 1 x Analog Audio</td>
</tr>
<tr>
<td>Network</td>
<td>89XX/99XX Phone Phone Ethernet (No WiFi)</td>
<td>Ethernet (No WiFi)</td>
</tr>
<tr>
<td>Power Over Ethernet</td>
<td>802.3AT supports Phone with No Camera</td>
<td>1 Display – 802.3AF</td>
</tr>
<tr>
<td></td>
<td>All other configurations require a Power Cube</td>
<td>2 Displays – 802.3AT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Optional Power Cube</td>
</tr>
</tbody>
</table>
Convergence of VDI, Video, and Voice

Virtual Desktop
User 1

Desktop Virtualization Display Protocol

Virtual Desktop
User 2

Desktop Virtualization Display Protocol

Cisco Unified CM

Call Control Signalling

VXI Cloud

Call Control Signalling

VXC 6215

RTP Media

VXC 4000
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
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

<table>
<thead>
<tr>
<th>VXC 2100 Series</th>
<th>VXC 2200 Series</th>
<th>VXC 4000*</th>
<th>VXC 6215*</th>
<th>Cisco Cius</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Form Factor</strong></td>
<td>“Backpack” Integrated</td>
<td>“Tower” Standalone</td>
<td>PC Software</td>
<td>“Tower” Standalone</td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td>Shipping</td>
<td>Shipping</td>
<td>Shipping</td>
<td>Shipping</td>
</tr>
<tr>
<td><strong>Platform</strong></td>
<td>Zero Client</td>
<td>Zero Client</td>
<td>Win7, XP</td>
<td>Linux</td>
</tr>
<tr>
<td><strong>UC Protocol Support (add on)</strong></td>
<td>N/A</td>
<td>N/A</td>
<td>Software Appliance</td>
<td>HDX, RDP PCoIP</td>
</tr>
<tr>
<td><strong>UC Client Support</strong></td>
<td>CUPC, Connect</td>
<td>CUPC, Connect</td>
<td>CUPC, CUCILync</td>
<td>CUPC, CUCILync</td>
</tr>
<tr>
<td><strong>Voice</strong></td>
<td>IP Phone 8961, 9951, 9971</td>
<td>N/A, can be used with IP Phone</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Video</strong></td>
<td>IP Phone 9971, 9951</td>
<td>N/A, can be used with IP Video Phone</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Monitor Support</strong></td>
<td>Single or Dual, 1920x1200</td>
<td>Single or Dual, 1920x1200</td>
<td>Varies based on underlying HW</td>
<td>Single:2560x1600 Dual:1920x1200</td>
</tr>
<tr>
<td><strong>PoE</strong></td>
<td>PoE</td>
<td>PoE</td>
<td>N/A</td>
<td>No</td>
</tr>
<tr>
<td><strong>Encoding &amp; Decoding</strong></td>
<td>Via IP Phone</td>
<td>Via IP Phone</td>
<td>Audio only. Video on the roadmap.</td>
<td>Standard Video HD Capable*</td>
</tr>
</tbody>
</table>
VDI & NetApp Storage
Transitioning from Virtualization to ITaaS

Application-Based Silos

Zones of Virtualization

Private Cloud

Public Cloud

Apps

Servers

Network

Storage

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
Multiple Disks
SAN
FC
NAS
SATA
iSCSI
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

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

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
Secure Multi-Tenancy
The industry’s only end-to-end secure multi-tenancy solution

- 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
  - VXI 2112, 2212, 4000, 6215 supported using 802.1x, MAB and Auth Proxy
  - WiFi support for mobile endpoints

- VXI 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.

![Diagram showing network connections and traffic flow]

<table>
<thead>
<tr>
<th>Pool Name</th>
<th>Starting Address</th>
<th>Ending Address/Number of Addresses</th>
<th>Subnet Mask/Prefix Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>asucs-pool</td>
<td>192.168.11.1</td>
<td>192.168.11.254</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

SSL VPN Client
Tunnel IP 192.168.11.1
Mobile Consultant

Inside network 192.168.225.0
Outside 172.21.61.125
192.168.11.0
Internet

Internet Traffic
Split Tunnel

Cisco ASA
ScanSafe
YouTube
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
• 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

**Access Security**
- Remote/Home User
  - Anyconnect w/ Split Tunnel

**VXI Network**
- Internet
  - ASA

**Data Center**
- ASA and Anyconnect provide single secure remote access solution for large device footprint
- Device profiling and posture assessment using ISE ensures conformance
- UPoE and PoE+ provide de-cluttered and energy efficient virtual workspace
- 802.1x based device and user authentication
- Trustsec allows policy based access to specific applications in Data Center
- Unmanaged devices (BYOD) only allowed access to specific Virtual desktop pools and applications
- DMVPN allows secure, dynamic and direct branch to branch collaboration
- WAAS and ISR together accelerate performance
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 |

- 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.

<table>
<thead>
<tr>
<th>Workload Profile</th>
<th>AV Scan Policy</th>
<th>HVD Density</th>
</tr>
</thead>
<tbody>
<tr>
<td>KW only</td>
<td>N/A</td>
<td>110/110</td>
</tr>
<tr>
<td>KW with MoveAV 1.5</td>
<td>Default</td>
<td>90/90</td>
</tr>
</tbody>
</table>

**18% impact on HVD Density**

XenDesktop 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

1. Redirect VM traffic via VLANs to external (physical) appliances
   - Web Server
   - App Server
   - Database Server
   - Virtual Contexts
   - VLANs
   - Hypervisor

2. Apply hypervisor-based network services
   - Web Server
   - App Server
   - Database Server
   - Hypervisor
   - Virtual Service Nodes
   - VSN
Virtualization & Virtual Service Nodes

- Web Server
- App Server
- Database Server

Virtual Service Nodes

VSN

Virtual Security Gateway

Nexus 1000V

ASA 1000V

Zone based intra-tenant segmentation of VMs

Ingress/Egress multi-tenant edge deployment

Zone based intra-tenant segmentation of VMs

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 built 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

Nexus 1000V
Distributed Virtual Switch

VNMC
VSG
Log/Audit

Initial Packet Flow
Virtual Security Gateway
Intelligent Traffic Steering with vPath

Nexus 1000V
Distributed Virtual Switch

1. Initial Packet Flow
2. Flow Access Control (policy evaluation)

VNMC
VSG
Log/Audit

Cisco Expo
© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public
Virtual Security Gateway
Intelligent Traffic Steering with vPath

Nexus 1000V
Distributed Virtual Switch

1. Initial Packet Flow
2. Flow Access Control (policy evaluation)
3. Decision Caching
Virtual Security Gateway
Intelligent Traffic Steering with vPath

Nexus 1000V
Distributed Virtual Switch

1. Initial Packet Flow
2. Flow Access Control (policy evaluation)
3. Decision Caching
4. vPath
Virtual Security Gateway

Performance Acceleration with vPath

Nexus 1000V
Distributed Virtual Switch

ACL offloaded to Nexus 1000V (policy enforcement)

Remaining packets from flow

Log/Audit

VSG

VNMC
Cisco Virtual Security Gateway

Virtual Security Gateway (VSG)

- Context aware Security
- Zone based Controls
- Dynamic, Agile
- Best-in-class Architecture

- VM context aware rules
- Establish zones of trust
- Policies follow vMotion
- Efficient, Fast, Scale-out SW

Virtual Network Management Center (VNMC)

- Non-Disruptive Operations
- Policy Based Administration
- Designed for Automation

- Security team manages security
- Central mgmt, scalable deployment, multi-tenancy
- XML API, security profiles

Security team manages security
Efficient, Fast, Scale-out SW
Central mgmt, scalable deployment, multi-tenancy
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
Otázky a odpovědi

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

- Zveřejňuji Vás na **Ptali jste se…** v sále LEO
  1.den 17:45 – 18:30
  2.den 16:30 – 17:00
Prosíme, ohodnoťte tuto přednášku.