PCI Compliant Private Cloud Reference Architecture

Hemma Prafullchandra, CTO, HyTrust, Inc.
PCI DSS and Virtualization

*What’s the fuss?*

- Payment Card Industry Data Security Standard (PCI DSS) v1.2 does not mention virtualization.

- A virtualization Special Interest Group (SIG) was formed in February 2009 which has been working diligently on guidance on how to implement the DSS requirements in a virtualized environment and for Qualified Security Assessors (QSAs) to perform an audit.

- Good news: the upcoming release in October (PCI DSS 2.0) will address virtualization (summary of proposed changes released).

- However, virtualization technology is still evolving - cannot provide sufficient guidance for “mixed-mode” in a vendor neutral manner!
Challenges to Enabling PCI Compliant Cloud

*Existing tools & processes are inadequate for virtualized environments*

- PCI DSS definitions assume physical servers, physical switches, physical firewalls, physical load balancers,
  ...  

- One primary function per “server” – what is a “server’?  
  Hypervisor/host, virtual machine, virtual appliance, virtualized infrastructure

- Scope reduction through network segmentation – what network?  
  Lack visibility and control of virtual networks

- What is “mixed-mode” and how can it be made PCI DSS compliant?  
  Cloud implies consolidation of different workloads on a single physical system – what if these workloads were both Cardholder Data Environment (CDE) VMs and non-CDE VMs – what is in-scope and how can you demonstrate adequate protection, and isolation to reduce scope?
Current Early Guidance

**MUST be Vendor Neutral**

- “System components” definition is changed to allow virtual system components: servers and infrastructure components (management, security, network switches)

- One primary function applies mainly to CDE-VMs

- Hypervisor *always* in scope – all requirements must be met
  
  Selection matters – look for 3rd party certification, introspection APIs, …

- Virtual switch is in-scope if providing services to CDE-VMs or on host in-scope; upstream physical switches pulled into scope

- Must segment (virtual) networks to reduce scope
Enabling PCI Compliant Private Cloud

Qualified architecture – need Nexus 1000V and HyTrust Appliance

- Cisco, HyTrust, Savvis and Coalfire are collaborating to jointly provide detailed guidance on PCI DSS compliance private reference architecture.

- Selected virtualization-aware technologies:
  - VMware vSphere ESXi 4.0 or later and vCenter server
  - Cisco Nexus 1000V distributed virtual switch
  - HyTrust Appliance
  - Cisco Virtual Security Gateway

- Plan to release in September/October
Cisco Nexus 1000V Architecture

Virtual Supervisor Module (VSM)
- Virtual or Physical appliance running Cisco NXOS (supports HA)
- Performs management, monitoring, & configuration
- Tight integration with VMware vCenter

Virtual Ethernet Module (VEM)
- Enables advanced networking capability on the hypervisor
- Provides each VM with dedicated "switch port"
- Collection of VEMs = 1 vNetwork Distributed Switch

Cisco Nexus 1000V Installation
- ESX & ESXi
- VUM & Manual Installation
- VEM is installed/upgraded like an ESX patch

Nexus 1000V VSM
### Cisco Nexus 1000V Advantages

#### Capabilities Mapped to PCI DSS Requirements

<table>
<thead>
<tr>
<th>PCI DSS 1: Do not use vendor specified defaults for system passwords and other security parameters</th>
<th>Private VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI DSS 3: Protect stored cardholder data</td>
<td>ACL, Private VLAN, and anti-spoofing features to protect against man-in-the-middle attacks and maintain separation on the virtual infrastructure.</td>
</tr>
<tr>
<td>PCI DSS 6: Develop and maintain secure systems and applications</td>
<td>With the N1KV datacenter teams manage their virtual network with the same security policies and workflow that they use to manage their physical network. This reduces recertification guesswork and rework.</td>
</tr>
<tr>
<td>PCI DSS 7: Restrict access to cardholder data by business need-to-know</td>
<td>ACL, AAA, Private VLANs</td>
</tr>
<tr>
<td>PCI DSS 10: Track and monitor all access to network resources and cardholder data</td>
<td>Without N1KV port statistics are reset each time a VM migrates from server to server using vMotion. With N1KV port statistics are persistent, creating a clear audit trail. Auditing tools such as Netflow &amp; ERSPAN are also available and are persistent during vMotion.</td>
</tr>
<tr>
<td>PCI DSS 11: Regularly test security systems and processes</td>
<td>With N1KV test procedures are the same for the physical virtual networks, reducing audit complexity &amp; hours.</td>
</tr>
<tr>
<td>PCI DSS 12: Maintain a policy that addresses information security</td>
<td>With N1KV port profiles &amp; security profiles are maintained centrally and migrate with each VM during vMotion; and clear separation of duty can be enforced between the server admin and network admin.</td>
</tr>
</tbody>
</table>
HyTrust Appliance

Policy-based control and visibility for vSphere and Nexus 1000V

- **Unified Access Control**: centralized management, consistent separation of duties, management of privileged accounts for vSphere and Nexus 1000V

- **Audit-Quality Logging**: granular, user-specific, compliance-ready logs for vSphere and Nexus 1000V

- **Virtual Infrastructure Policy Management**: configurable enforcement, infrastructure segregation, better organization & greater visibility for vSphere and Nexus 1000V

- **Hypervisor Hardening**: consistent, scalable assessment and remediation
## HyTrust Appliance Advantages

**Capabilities Mapped to PCI DSS Requirements**

<table>
<thead>
<tr>
<th>PCI DSS 2: Do not use vendor specified defaults for system passwords and other security parameters</th>
<th>Root Password Vault (privileged account management); Hypervisor Hardening (checks/remediates default values)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI DSS 6: Develop and maintain secure systems and applications</td>
<td>Hypervisor Hardening; Root Password Vault; and Unified Access Control to secure the host</td>
</tr>
<tr>
<td>PCI DSS 7: Restrict access to cardholder data by business need-to-know</td>
<td>Unified Access Control (hypervisor-level management); Policy Management (enforce VM affinity to host/network)</td>
</tr>
<tr>
<td>PCI DSS 8: Assign a unique ID to each person with computer access</td>
<td>Unified Access Control and AD/LDAP bridging</td>
</tr>
<tr>
<td>PCI DSS 10: Track and monitor all access to network resources and cardholder data</td>
<td>Audit-Quality Logging (every attempted hypervisor-level management request logged for both allowed and denied)</td>
</tr>
<tr>
<td>PCI DSS 11: Regularly test security systems and processes</td>
<td>Hypervisor Hardening (scheduled assessments; daily centralized log review)</td>
</tr>
<tr>
<td>PCI DSS 12: Maintain a policy that addresses information security</td>
<td>Unified Access Control and Policy Management (separation of duties; VI segregation; central control; distributed deployment)</td>
</tr>
</tbody>
</table>
Next Steps

**Cisco & HyTrust: Ensuring PCI Compliant Clouds**

- See Cisco Nexus 1000V at Cisco booth (#801)
- See HyTrust Appliance at HyTrust booth (#236)
- Look for PCI Compliant Cloud Reference Architecture whitepaper from Cisco/Savvis/HyTrust/Coalfire in the next month
- Email hemma@hytrust.com
- Look for PCI DSS 2.0 in October, Virtualization Information Supplement later this year.
Q & A