

SE8378 - Compliance-Ready Virtual Infrastructure, Addressing PCI Security Standard for Virtualized Deployments

Charu Chaubal

Tom McAndrew



Compliance-Ready Virtual Infrastructure, Addressing PCI Security Standard for Virtualized Deployments

Agenda

- ✓ Overview of virtualization controls for compliance
- ✓ Foundations for virtual security
- ✓ Current limitations/questions with the current PCI-DSS and how they affect virtualization audits (for customers and QSA's)
- ✓ Example architectures being deployed to meet PCI requirements

Virtualization Controls for Security

Network Controls

Change Control and Configuration Management

Access Controls & Management

Vulnerability Management

Virtualization Controls for Security

Area	Change Control and Configuration Management
Issue	Incorrect configurations can lead to poor security posture or exposed interfaces
Solution	<ul style="list-style-type: none">• Use predefined, vetted configurations• Enforce auditable and repeatable procedures• Monitor and track all important system state changes.
Technologies	<ul style="list-style-type: none">• Host Profiles• Templates• vCenter Event-based Alarms• vCenter Orchestrator• Scripting

Virtualization Controls for Security

Area	Access Controls and Management
Issue	<ul style="list-style-type: none">• Individuals granted excess or inappropriate access can do harm, whether intentionally or accidentally• Insider threats in particular need to be guarded against
Solution	<ul style="list-style-type: none">• Integrate with central authentication service, e.g. Active Directory• Enforce principle of least privileges and strong separation of duties• Perform logging and auditing of sessions
Technologies	<ul style="list-style-type: none">• vCenter Roles, including portgroup and datastore privileges• vCenter event logging• ESX/ESXi logging

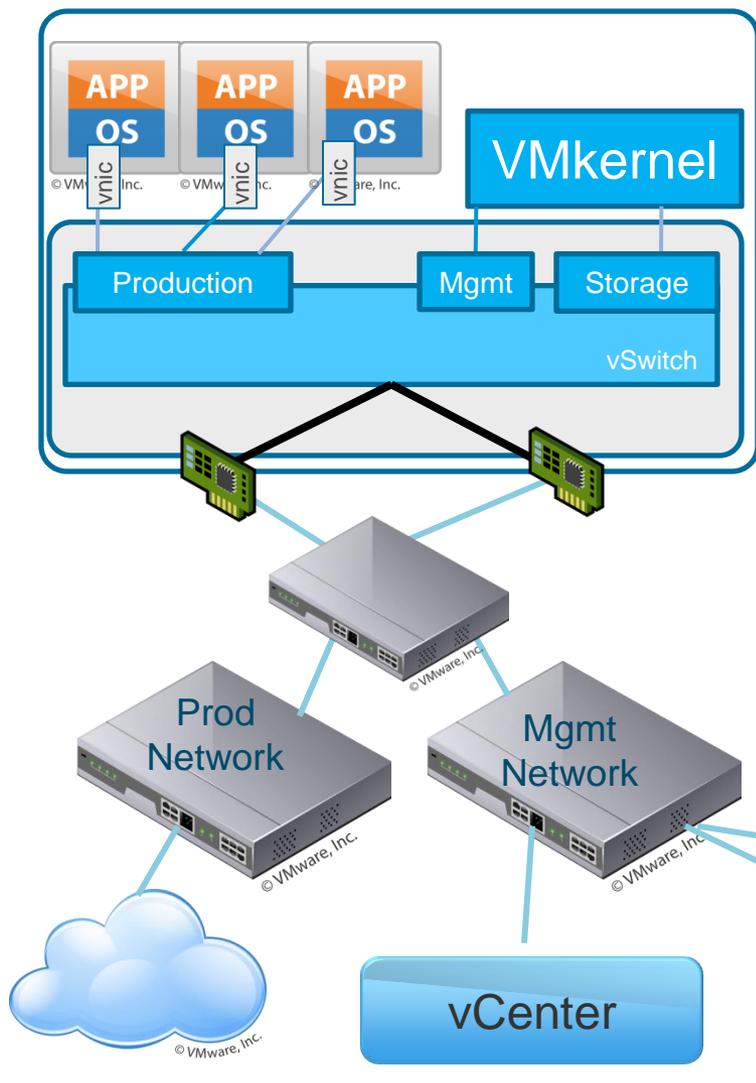
Virtualization Controls for Security

Area	Network and Interface Controls
Issue	Any interface into a system represents a point of attack and exposure of potential vulnerabilities
Solution	<ul style="list-style-type: none">• Restrict or disable unused or unnecessary interfaces• Architect for isolation of non-production networks
Technologies	<ul style="list-style-type: none">• vNetwork Distributed Switch• VLAN and PVLAN• vShield

Virtualization Controls for Security

Area	Vulnerability Management
Issue	Unpatched vulnerabilities can be used to bypass other security controls
Solution	<ul style="list-style-type: none">• Follow relevant security hardening guidelines• Include offline VMs in patch process• Stay up to date on hypervisor patching
Technologies	<ul style="list-style-type: none">• Update Manager

Foundations of Virtual Security: Secure Deployment

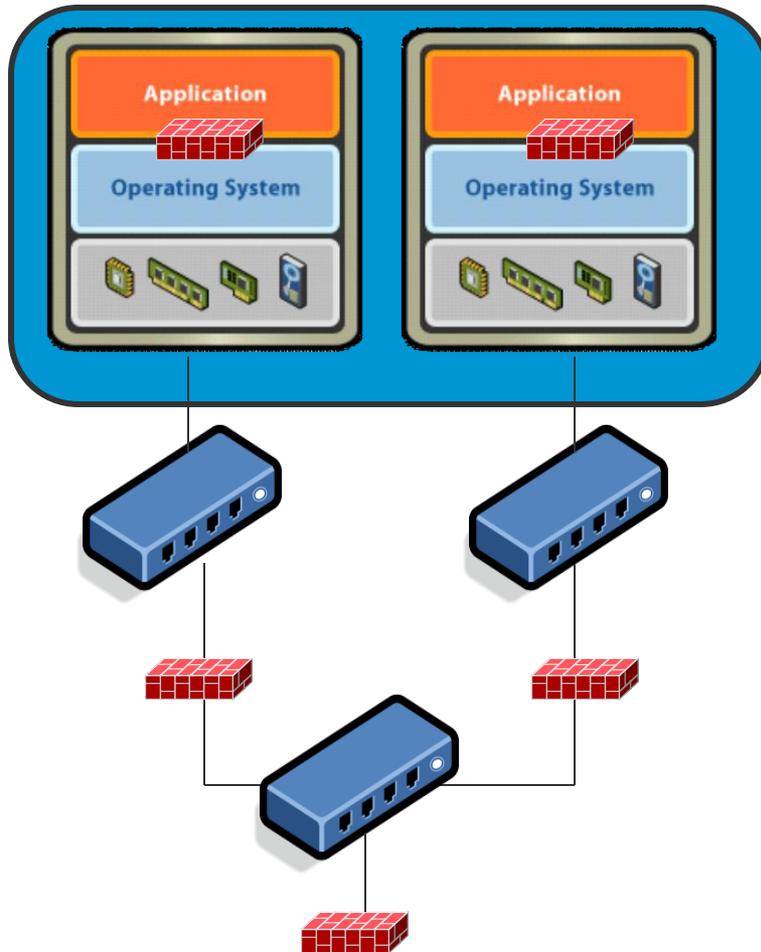


VMware Security Hardening Guides

- Being provided for major platform products
 - vSphere 4.0
 - VMware Cloud Director (in progress)
 - View (in progress)
- Important for architecture and deployment related controls

vSphere 4.0 Security Hardening Guide
<http://www.vmware.com/resources/techresources/10109>

Foundations of Virtual Security: Securing Virtual Machines



Provide Same Protection as for Physical Servers

Host

- Anti-Virus
- Patch Management

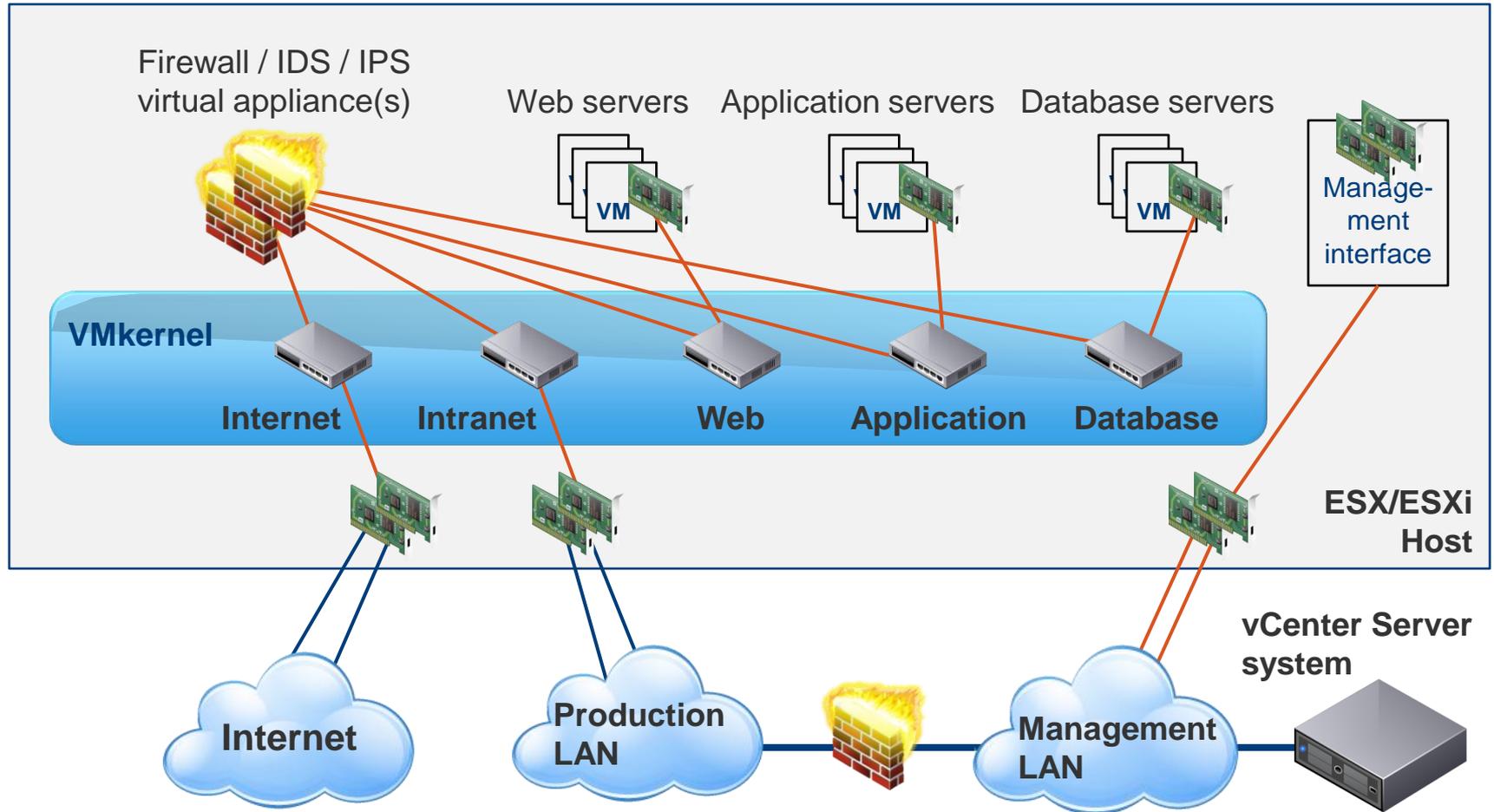
Network

- Intrusion Detection/Prevention (IDS/IPS)

Edge

- Firewalls

Foundations of Virtual Security: Virtual Trust Zones



Compliance vs. Security



Compliance

Conforming to a set of rules or standards. This is generally confirmed by an assessor providing an opinion based on observation, inquiry, and inspection.

Security

Implementing Technical, Physical, and Administrative controls to provide confidentiality, integrity, availability, accountability and assurance.

Why is PCI so hard for virtualization?

Technology changes faster than any standard (including the PCI DSS)

PCI applies to all systems “in scope”

Segmentation defines scope

The DSS is vendor agnostic

Most whitepapers are written for security, not compliance

If network segmentation is in place and will be used to reduce the scope of the PCI DSS assessment, the assessor must verify that the segmentation is adequate to reduce the scope of the assessment.

- PCI DSS p. 6

What is “in-scope”

All systems that **Store, Process, or Transmit** cardholder data, and all system components that are in or connected to the cardholder data environment (CDE).

What’s unique in a virtual environment?

Storage

Data that used to reside only in memory could be written to disk (encryption keys, PAN)

The integrity of data can now be altered in several locations (i.e. a log server that is stored as VM on the ESX host)

SAN – Can VM’s be altered in storage? How will you know?

Transmission

Data that used to physically reside in one location could now be transmitted logically across the network (i.e. VMotion, pulling images from a SAN, storage)

Authentication controls (how can you ensure that authentication systems cannot be by-passed)

What “system components” could be used to sniff sensitive data?

Segmentation

Defining system boundaries can be more difficult, with virtual firewalls, virtual switches, VLANs, and High Availability switches.

Mixed mode environments, multi-tenancy.

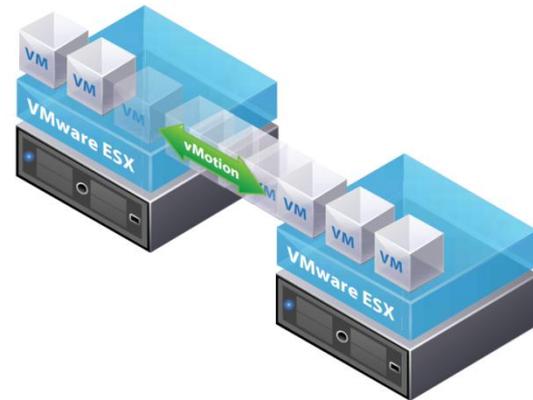
Can all system components in the virtual environment meet ALL PCI controls?

Aren't firewalls required for segmentation?

QSA's have historically relied on stateful firewalls for network segmentation.

PCI allows for "other technology" as an acceptable use of segmentation.

How do firewalls impact the flow of data unique to a virtual environment (VMotion, Pulling Images from a SAN, taking "dirty" snapshots)



Network segmentation can be achieved through internal network firewalls, routers with strong access control lists or other technology that restricts access to a particular segment of a network. - PCI DSS p. 6

What about one function per server?

PCI applies to all system components that are “in scope”

Segmentation defines scope

What is “adequate” segmentation

At a high level, adequate network segmentation isolates systems that store, process, or transmit cardholder data from those that do not. However, the adequacy of a specific implementation of network segmentation is highly variable and dependent upon such things as a given network's configuration, the technologies deployed, and other controls that may be implemented. - PCI DSS p. 6

“ Documenting cardholder data flows via a dataflow diagram helps fully understand all cardholder data flows and ensures that any network segmentation is effective at isolating the cardholder data environment.” – p.6

A Data Flow Diagram Is NOT just a logical network Diagram!

Focus on business (not technical) processes.

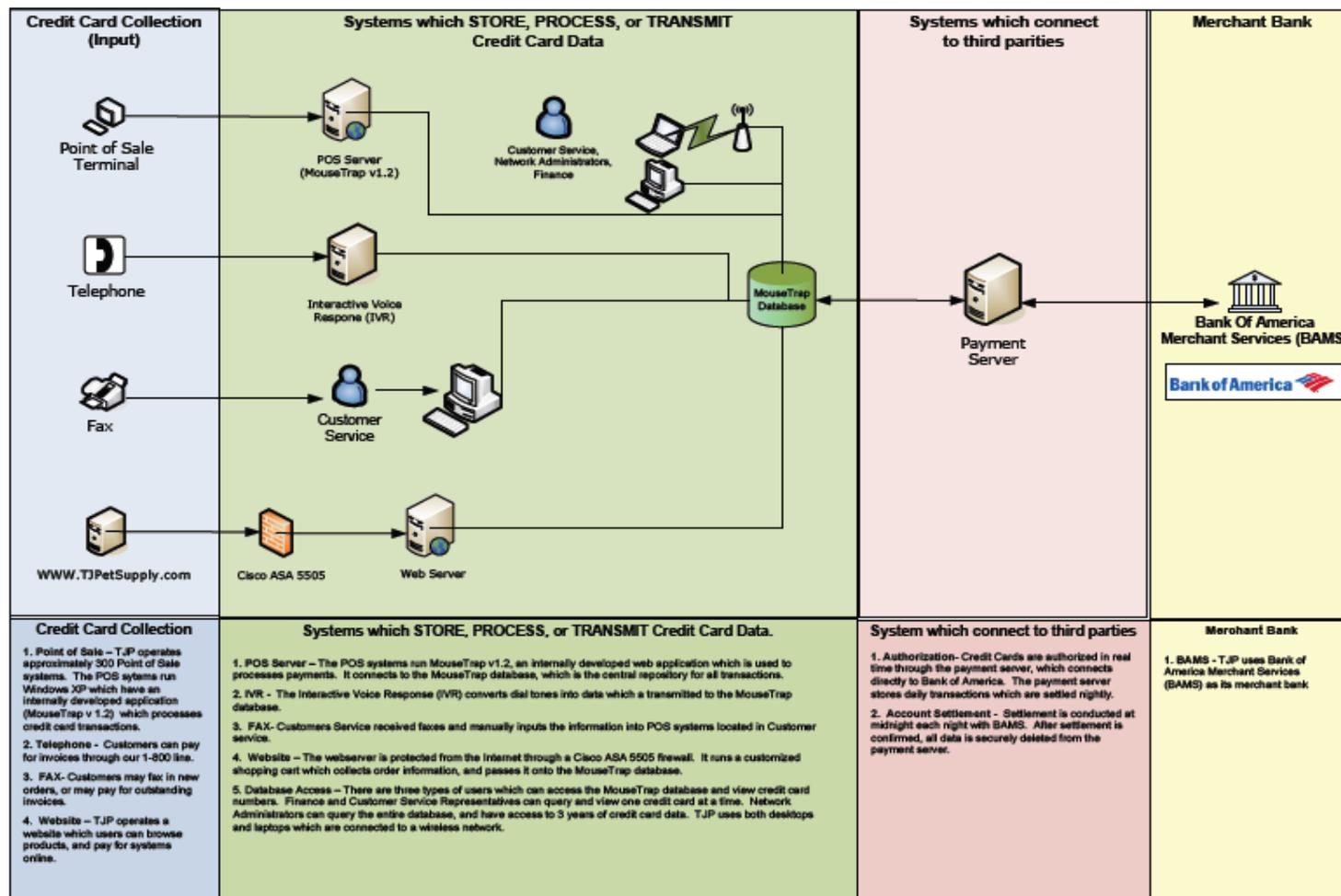
Assessors should begin by reviewing the system boundaries for:

- 1. Input** Where does data originate?
- 2. Process** How does it get used?
- 3. Output** Where does it go?

Sample Cardholder Data Flow – No Virtualization

Cardholder Data Environment (CDE) Tom and Jerry's Pet Supply (TJP)

March 7, 2009
Version 1.0



Why are virtual environment so much harder to document?

1. System boundaries are not as clear as their non-virtual counterparts.
2. Even the simplest network is rather complicated.
3. More components, more complexity, more areas for risk.
4. Digital forensic risks are more complicated.
5. More systems are required for logging and monitoring.
6. More access control systems.
7. Memory can be written to disk.
8. Many applications and O/S were not designed for Virtualization
9. VM Escape?
10. Mixed Mode environments.

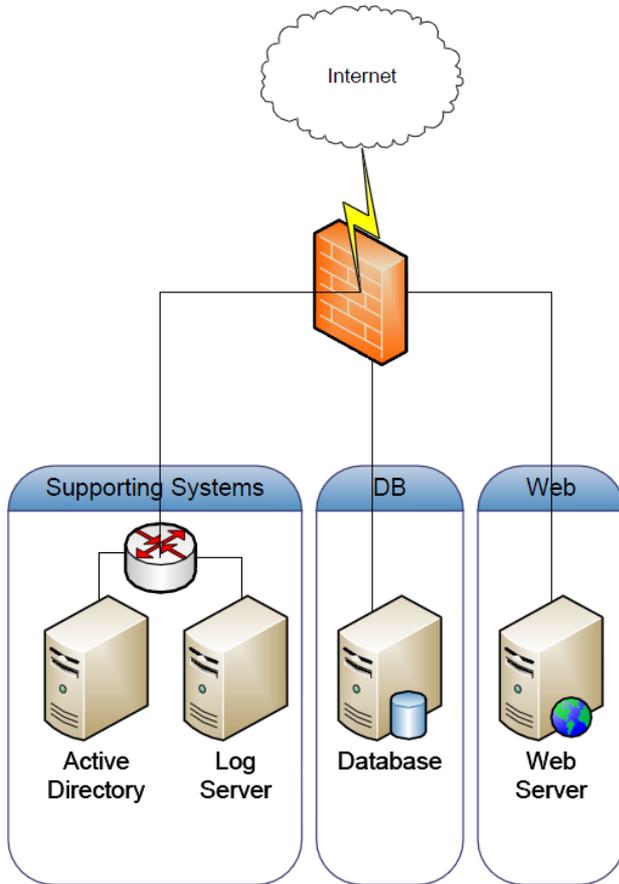
What compliance benefits are there for virtual environments?

1. Repeatable security
2. Scalable controls
3. Risk aggregation/concentration
4. Improve security without impacting operations
5. Stronger/quicker configuration management
6. More money can be spent on security controls
7. Quickly provision and release with minimal management
8. Faster recovery after an attack
9. Ability to quickly capture and isolate compromised VM's.

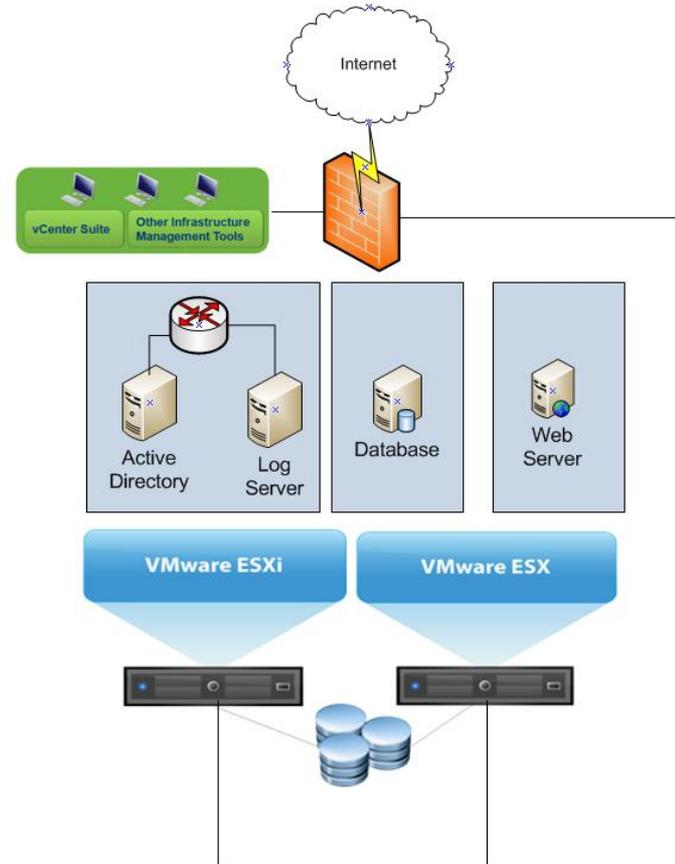
System boundaries are not as clear as their non-virtual counterparts

Basic Web Server and Database

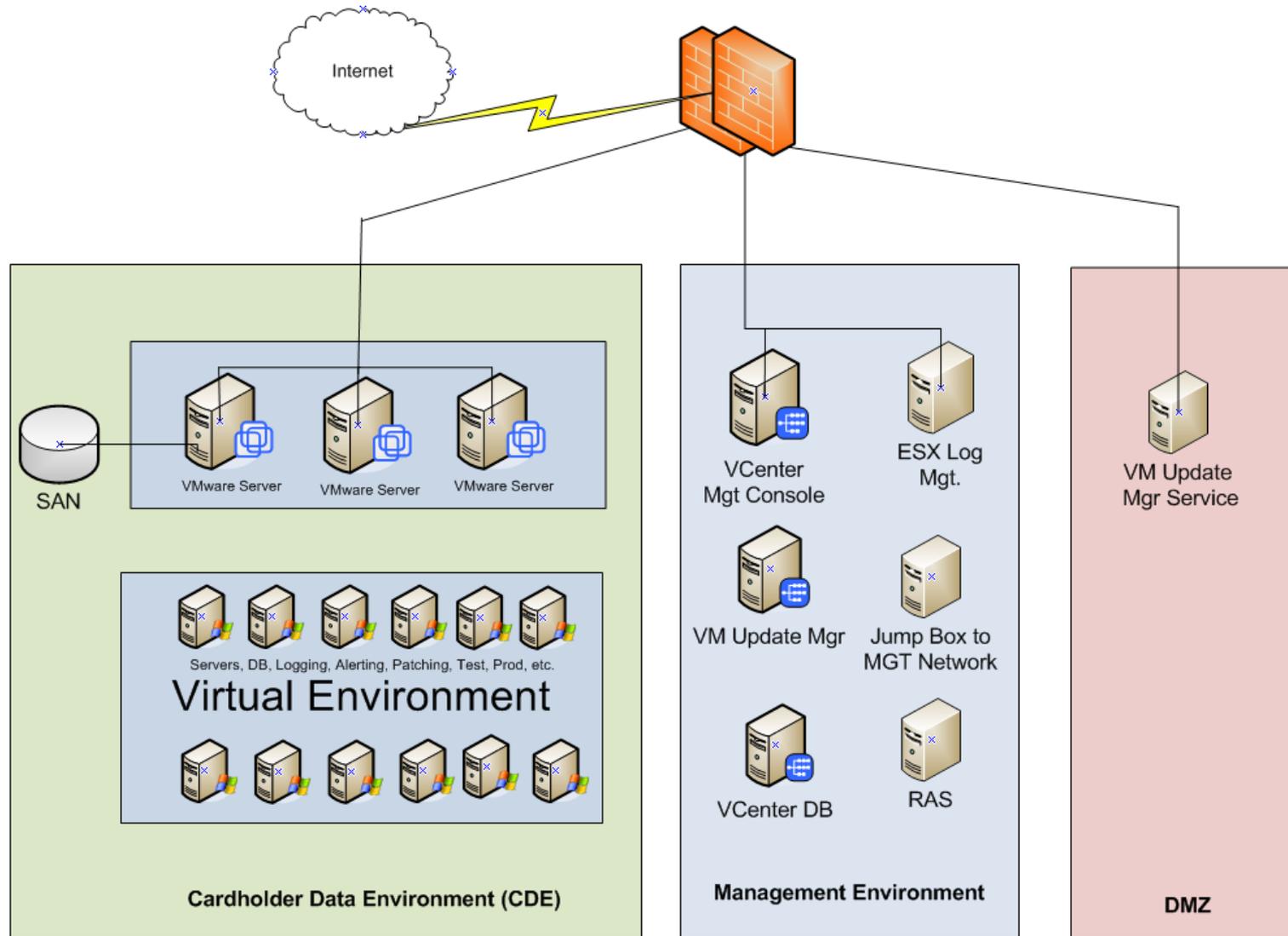
Standard Environment



Virtual Environment



Sample Virtualized CDE



Problems with Compensating Controls for Multi-Tenancy

PCI DSS does not define what should be in a compensating Control worksheet in a virtual environment.

Are compensating controls required for virtual environments?

If so, what do they look like?

 PCI Security Standards Council

Compensating Controls Worksheet – Completed Example

Use this worksheet to define compensating controls for any requirement noted as "in place" via compensating controls.

Requirement Number: 8.1—Are all users identified with a unique user name before allowing them to access system components or cardholder data?

	Information Required	Explanation
1. Constraints	List constraints precluding compliance with the original requirement.	Company XYZ employs stand-alone Unix Servers without LDAP. As such, they each require a "root" login. It is not possible for Company XYZ to manage the "root" login nor is it feasible to log all "root" activity by each user.
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	The objective of requiring unique logins is twofold. First, it is not considered acceptable from a security perspective to share login credentials. Secondly, having shared logins makes it impossible to state definitively that a person is responsible for a particular action.
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	Additional risk is introduced to the access control system by not ensuring all users have a unique ID and are able to be tracked.
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	Company XYZ is going to require all users to log into the servers from their desktops using the "SU" command. "SU" allows a user to access the "root" account and perform actions under the "root" account but is able to be logged in the "SU-log" directory. In this way, each user's actions can be tracked through the "SU" account.
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	Company XYZ demonstrates to assessor that the "SU" command being executed and that those individuals utilizing the command are logged to identify that the individual is performing actions under root privileges.
6. Maintenance	Define process and controls in place to maintain compensating controls.	Company XYZ documents processes and procedures to ensure "SU" configurations are not changed, altered, or removed to allow individual users to execute root commands without being individually tracked or logged.

PCI DSS Requirements and Security Assessment Procedures, v1.2.1
Appendix C: Compensating Controls Worksheet

July 2009
Page 44

Virtualization Risks by Requirement – Executive Summary

Requirement	Unique Risks to Virtual Environments	How you can address them
<p>Executive Summary</p>	<p>Defining the CDE is particularly challenging in a virtual environment. Every physical and virtual “system component” should be carefully documented.</p> <p>Will this address multi-tenancy environment or use “mixed-mode” virtualization?</p> <p>If “other technology” is used to segment systems (such as ACL’s on virtual components) they should be described in detail. The organization should also describe exactly how it isolated, how it was tested, and how auditor can test that segmentation is in place and will remain in place over time.</p> <p>There should be three separate network diagrams available for the assessor.</p> <ol style="list-style-type: none"> 1. A data flow diagram of the Cardholder Data Environment (CDE) 2. A logical diagram of physical components. 3. A logical diagram of virtual components. 	<p>Document every “system component.” Do your research and be proactive with identify risks and security concerns with your specific approach and implementation. Don’t expect your assessor to do the work, work collaboratively!</p> <p>If your network is simple, do not use multi-tenancy or mixed mode. They add another layer of risk and complexity which makes for more documentation and more risks.</p> <p>This is one of the biggest mistakes of new users. Most virtual environment rely on additional technology other than stateful firewalls. (Such as memory segmentation, ACL’s, virtual switches, core routers, virtual firewalls, storage, and SDLC processes). Address how hardware and software provide segmentation, and how it can and will be tested.</p> <p>Do not provide just a layer 3 diagram! Prepare a Cardholder Data Flow describing authorization, settlement, chargebacks, etc. (PCI 1.2.1a requirement). Also include the “virtual” view of the network.</p>

Virtualization Risks by Requirement – Requirement 1

Requirement	Unique Risks to Virtual Environments	How you can address them
<p>1. Install and maintain a firewall configuration to protect cardholder data.</p>	<p>Most virtual and private cloud environments rely additional technology beyond a standard stateful firewall to establish separate security zones. Virtual NICs', Virtual Switches, Virtual Firewalls, and any other physical components which use software or hardware to create segmentation should be documented and included in section 1, as they are used to establish and maintain segmentation and protect cardholder data from access.</p>	<p>Do not simply address physical firewalls in section 1. This requirement is about setting up appropriate segmentation and documenting the standards in place.</p> <p>Establish and document clear logical and physical zones.</p> <p>Within the hypervisor traffic from CDE-VM to Non-CDE-VM traffic should not be allowed.</p> <p>Document mapping of Virtual NICs to Physical NICs, and use of Container Groups/Port Groups in any distributed virtual switches.</p> <p>Document how technology and policies can be used to enforce network zoning through label-based policy so administrators cannot accidentally/intentionally connect VMs to incorrect portgroups and virtual networks.</p> <p>If virtual firewalls are used (vShield) document permissions, zoning, and access controls.</p> <p>Document how the SAN segments and protects Data Storage (Port Groups)</p>

Virtualization Risks by Requirement – Requirement 2

Requirement	Unique Risks to Virtual Environments	How you can address them
2. Do not use vendor-supplied defaults for system passwords and other security parameters.	<p>The provisioning systems for creating new virtual components must include a way of ensuring that new components are hardened and remove any default settings.</p>	<p>Consider using third party add-ons protecting the hypervisor root account and logging.</p> <p>Use a jump boxes and RAS servers so there is a central point of monitoring and logging all administrator access to the hypervisor.</p> <p>Use hardening guidelines such as CIS or VMware as templates for the virtual infrastructure.</p> <p>Hardening should be monitored to ensure that systems do not “soften” over time.</p> <p>Implement scanning and configuration tools to automatically check for hardening</p> <p>Use VMware host profiles to “templatize” host configurations/host profiles.</p> <p>Discuss use existing or virtualization-aware solutions for guest OS and vCenter.</p> <p>Each CDE-VM should serve only one primary function.</p> <p>Memory reservations should be set to 100% to prevent a memory swar file from being created on the storage device.</p> <p>Set “sched.mem.pshare.enable” to “false” for PCI VM’s.</p>

Virtualization Risks by Requirement – Requirement 3

Requirement	Unique Risks to Virtual Environments	How you can address them
<p>3. Protect stored cardholder data.</p>	<p>Memory that was previously only stored as volatile memory may now be written to disk as stored (i.e. taking snapshots of systems).</p> <p>How are memory resources and other shared resources protected from access? (How do you know that there are no remnants of stored data?)</p>	<p>Apply data retention and disposal policy to CDE-VMs, snap-shots, and any other components which have the possibility of storing CHD, encryption keys, passwords, etc.</p> <p>Document storage configuration and SAN implementation.</p> <p>Document any encryption process, encryption keys, & encryption key management used to protects stored CHD?</p> <p>Fully isolate the Vmotion network to ensure that as hosts are moved from one physic server to another, memory and other sensitive running data cannot be sniffed or logged.</p> <p>Do not used shared VM Folders</p>

Virtualization Risks by Requirement – Requirement 4

Requirement	Unique Risks to Virtual Environments	How you can address them
4. Encrypt transmission of cardholder data across open, public networks.	Is any part of the virtual environment considered a “public” network? How are risks to satellite communications, cellular networks, etc. address if the environment covers a large WAN.	Document how transmission protocols encrypt data (i.e. VPN, IPSEC, SSL, private lines, etc.) between any two end-points (virtual or physical) which are considered public or untrusted in the CDE.

Virtualization Risks by Requirement – Requirement 5

Requirement	Unique Risks to Virtual Environments	How you can address them
5. Use and regularly update anti-virus software or programs.	<p>What components do have anti-virus and how do they report status and ensure that newly provisioned systems have AV installed?</p> <p>If a component will not have AV, what is the justification that it is not “a system that is commonly affected by viruses?”</p>	<p>CDE-VMs should run existing A/V solution or virtualization-aware A/V solution.</p> <p>If using VMSafe enabled A/V, ensure that it is monitoring all system components it is current, and that it cannot be disabled or altered.</p>

Virtualization Risks by Requirement – Requirement 6

Requirement	Unique Risks to Virtual Environments	How you can address them
6. Develop and maintain secure systems and applications.	<p><i>This is one of the most critical sections in the virtual/cloud environment.</i> The process for creating, implementing, and maintaining the virtual cloud environment is different than a physical environment. Building images, backing up data, building Disaster Recover and Business Continuity introduce unique risks. How is VM Sprawl addressed?</p>	<p>Document the process for provisioning, maintaining, and retiring virtual and physical components.</p> <p>Document the process for updating and testing patches and updates.</p> <p>Document how Update Manager is used and maintained to manage components.</p> <p>Don't forget to include the patch management process for all the virtual hosts (i.e. WSUS).</p>

Virtualization Risks by Requirement – Requirement 7

Requirement	Unique Risks to Virtual Environments	How you can address them
7. Restrict access to cardholder data by business need-to-know.	Access controls are more complicated. In addition to hosts, there are now applications, virtual components, and storage of these components (i.e. what protects their access while they are waiting to be provisioned). Organizations should carefully document all the access controls in place, and ensure that there are separate access controls for different “security zones.”	Document all the types of different Role Based Access Controls (RBAC) used for access to physical hosts, virtual hosts, physical infrastructure, virtual infrastructure, logging systems, IDS/IPS, multi-factor authentication, and console access. Ensure that physical hosts do not rely on virtual RBAC systems that they host.

Virtualization Risks by Requirement – Requirement 8

Requirement	Unique Risks to Virtual Environments	How you can address them
8. Assign a unique ID to each person with computer access.	No major differences unless system components do not allow unique ID's or do not allow disabling standards accounts.	Ensure that every action in the virtual environment can be traced back to a specific individual (non-repudiation).

Virtualization Risks by Requirement – Requirement 9

Requirement	Unique Risks to Virtual Environments	How you can address them
9. Restrict physical access to cardholder data.	Risks are greater since physical access to the hypervisor could lead to logical access to every component.	Ensure that you are considering physical protection in your D/R site. Physical access to a single server or SAN can result in logical access to hundreds of servers!

Virtualization Risks by Requirement – Requirement 10

Requirement	Unique Risks to Virtual Environments	How you can address them
10. Track and monitor all access to network resources and cardholder data.	<p>Some virtual components do not have the robust logging requirements of their physical counterparts. Many systems are designed for troubleshooting and not to create detailed event and system logs which provide sufficient detail to meet PCI logging requirements.</p> <p>PCI requires logs to be stored in a central location that is independent of the systems being logged.</p>	<p>Establish unified and centralized log management solutions which cannot be altered or disabled by access to the hypervisor.</p> <p>ESX logs should not be stored on a virtual host on the ESX server, as compromising the ESX server could compromise the logs. Be prepared to demonstrate that the logs are forensically sound.</p>

Virtualization Risks by Requirement – Requirement 11

Requirement	Unique Risks to Virtual Environments	How you can address them
11. Regularly test security systems and processes.	<p>How are scans conducted on virtual components?</p> <p>How do organizations know that the scans that were run matched the inventory of all systems that were actually running at the time?</p> <p>Are new virtual components scanned before going live?</p>	<p>Document your process of conducting:</p> <ol style="list-style-type: none">1. External scans (from an Approved Scan Vendor)2. Internal scans3. Penetration tests <p>Document your process for ensuring that you are scanning all system components (how do you know that all virtual devices that are running where scanned?)</p> <p>There should be a process for linking system components to patch management process to vulnerability scans (vulnerabilities are merely symptoms of problems in configuration and patch management)</p>

Virtualization Risks by Requirement – Requirement 12

Requirement	Unique Risks to Virtual Environments	How you can address them
12. Maintain a policy that addresses information security for employees and contractors.	All policies should be updated to include the unique risks of a cloud environment, including forensics, employee background checks, vendor agreements, etc.	Document, Document, Document. Work collaboratively with your assessor before the assessment. Collaborate with vendors and service providers.

Where to Learn More



Home > Technology > Technology and Architecture > Security > Overview

Secure Your Virtual Infrastructure

All virtualization platforms are not the same. As you move to adopt virtual infrastructure solutions to reduce costs and improve IT operations, make sure you understand the security implications of virtualization technology and the platform you choose. VMware offers the most robust and secure virtualization platform available. Let us help you:

- Separate fact from fiction when it comes to virtualization and IT security
- Understand the most significant ways in which virtualization affects security
- Find resources as well as the latest news on virtualization security

Overview

Hosted vs. Bare

There are two common ways to run an application or "guest" on a computer: hosted and bare metal. Each has its own set of issues and the implications for security and compliance.



VMware Compliance Center

Easily achieve regulatory compliance within a virtualized environment. Our overview of the issues involved with virtualization and compliance, a comprehensive listing of partner virtualization compliance solutions, references such as white papers and recorded webcasts, and real-life examples of customers who have successfully passed compliance audits in their VMware environments will help you understand how best to achieve compliance. In addition to the PCI DSS (Data Security Standard), these resources should prove valuable for those of you looking to satisfy other regulations, such as Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), and others.

Overview

Partner Solutions

Resources

As regulatory compliance expands, more and more of your virtual environment will become subject to security and compliance standards, such as PCI DSS, HIPAA and SOX (GLBA). With the proper tools, achieving and demonstrating compliance on VMware Infrastructure is not only possible, but can often become easier than a non-virtual environment.

Security

- Hardening Best Practices
- Implementation Guidelines

<http://vmware.com/go/security>

Compliance

- Partner Solutions
- Advice and Recommendation

<http://vmware.com/go/compliance>

Operations

- Peer-contributed Content

<http://viops.vmware.com>

Thank You! Comments or Questions?

Charu Chaubal

charu@vmware.com

Tom McAndrew

Tom.McAndrew@coalfiresystems.com

Top Virtualization Compliance Issues



Issue	Significance
Segregation of Systems	Strong isolation guarantees are required for consolidating mutually untrusted VMs
Segmentation of Networks	
Monitoring	Virtualization represents a new layer on which traditional controls need to be applied

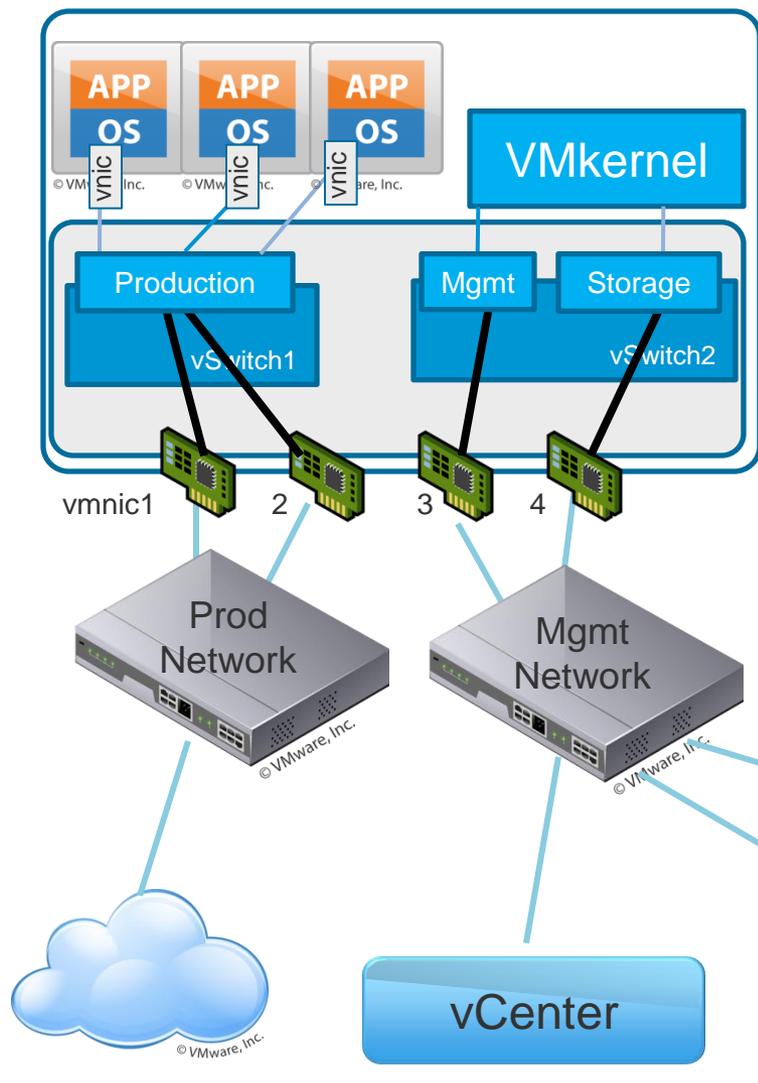
The Auditor's View

For a given virtual deployment

- Demonstrate that the required segregation exists between sensitive data and other data
- Show how this isolation is maintained beyond just a point in time
- Show how any breaks or attempted breaks in this isolation are made known



Isolation in the Architecture



Segment out all non-production networks

- Use VLAN tagging, or
- Use separate vSwitch (see diagram)

Strictly control access to management network, e.g.

- RDP to jump box, or
- VPN through firewall

VMware Infrastructure 3 Security Hardening Guide
<http://www.vmware.com/resources/techresources/726>

vSphere 4: Segmentation of Production Networks

PVLAN (Private VLAN)

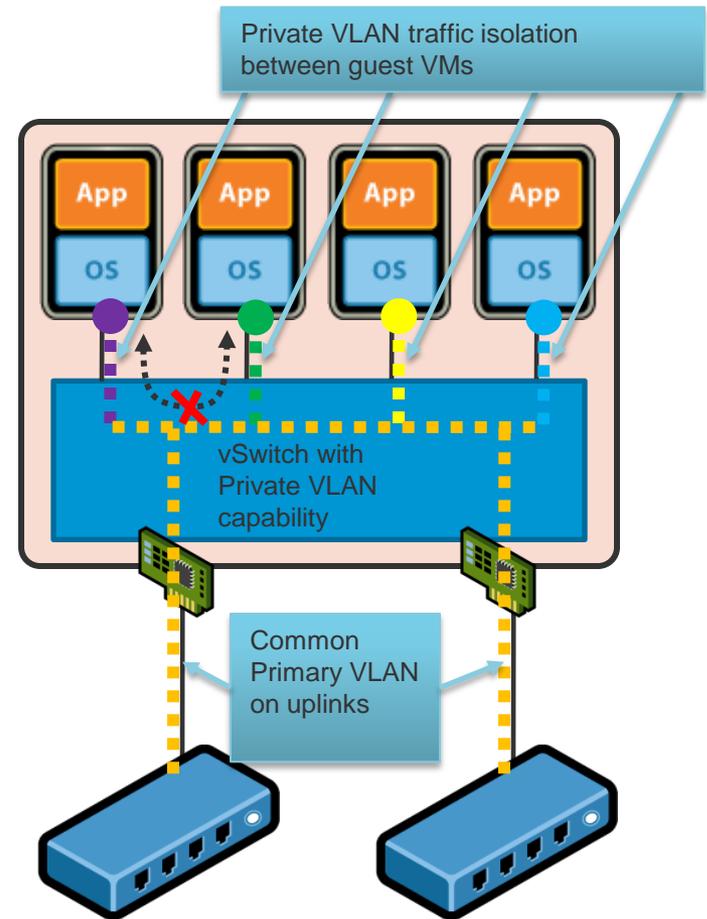
- Enables Layer-2 isolation between VMs on the same switch, even though they are on the same subnet
- Traffic from one VM forwarded out through uplink, without being seen by other VMs
- Communication between VMs on PVLANS can still occur at Layer-3

Benefits

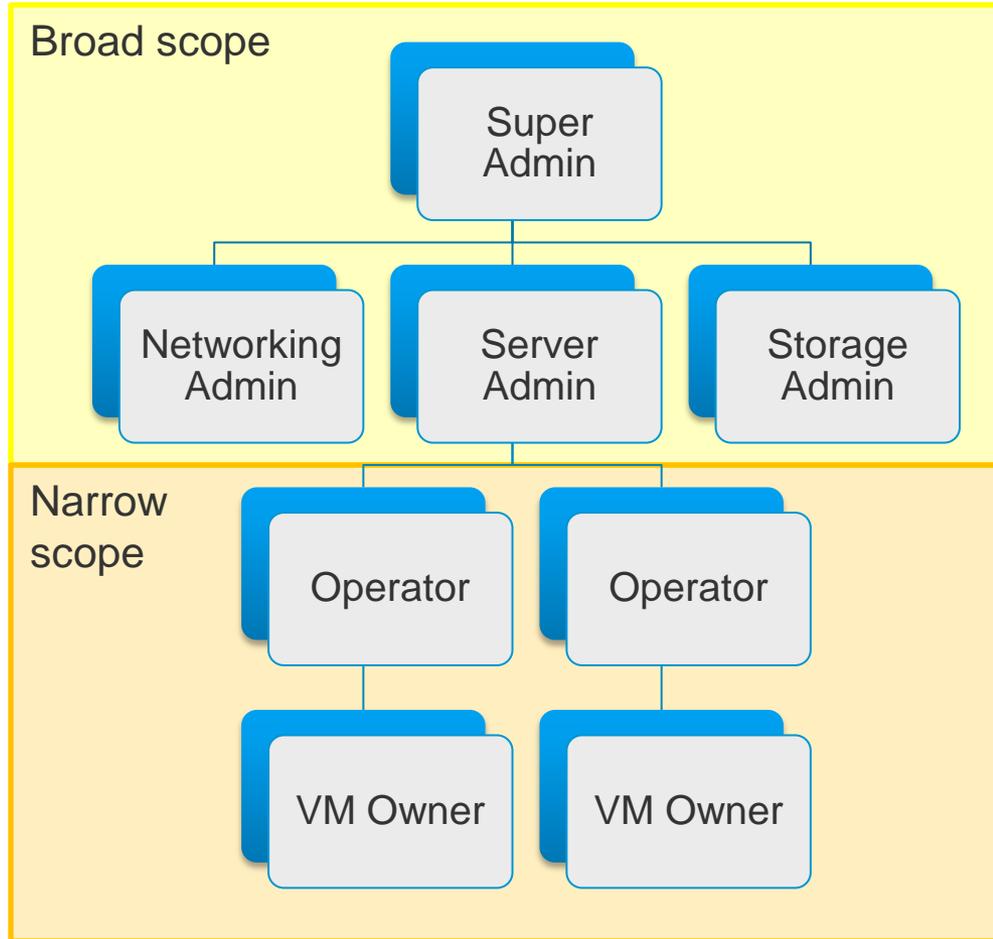
- Scale VMs on same subnet but selectively restrict inter-VM communication
- Avoids scaling issues from assigning one VLAN and IP subnet per VM

Implementation

- Available when using Distributed Switch



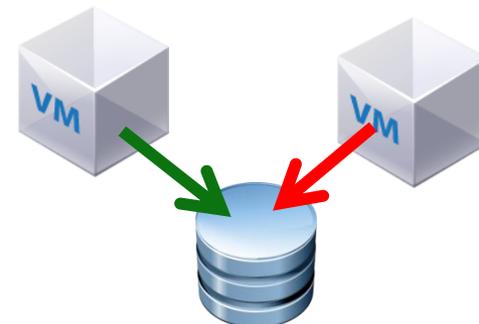
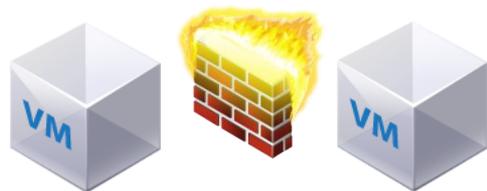
Separation of Duties with vSphere



Security Advantages of Virtualization

- Allows Automation of Many Manual Error Prone Processes
- Cleaner and Easier Disaster Recovery/Business Continuity
- Better Forensics Capabilities
- Faster Recovery After an Attack
- Patching is Safer and More Effective
- Better Control Over Desktop Resources
- More Cost Effective Security Devices
- App Virtualization Allows de-privileging of end users
- Better Lifecycle Controls
- Security Through VM Introspection

Isolation by Design



CPU & Memory

- VMs have limited access to CPU
- Memory isolation enforced by Hardware TLB
- Memory pages zeroed out before being used by a VM

Virtual Network

- No code exists to link virtual switches
- Virtual switches immune to learning and bridging attacks

Virtual Storage

- Virtual Machines only see virtual SCSI devices, not actual storage
- Exclusive virtual machine access to virtual disks enforced by VMFS using SCSI file locks

Confidential - INTERNAL ONLY

Security Design of the VMware Infrastructure 3 Architecture

<http://www.vmware.com/resources/techresources/727>