



PCI and VIRTUAL DATA CENTERS

W H I T E P A P E R

How to meet PCI DSS requirements and virtualize

Charlie Winckless

November, 2009

Table of Contents

1. Abstract	3
2. Executive Overview	4
3. Introduction	5
4. PCI Overview and Key Virtualization challenges	Error! Bookmark not defined.
4.1. PCI Overview	5
4.2. Virtualization Challenges.....	6
5. Security Principles	Error! Bookmark not defined.
5.1. Policy and Procedure.....	7
5.2. Defence in Depth	8
5.3. Segmentation	8
5.4. Least Privilege	10
5.5. Network intelligence.....	11
6. INX Reference Architecture	Error! Bookmark not defined.
6.1. Reference Architecture Diagram.....	Error! Bookmark not defined.
6.2. Reference Architecture Security Elements.....	Error! Bookmark not defined.
7. References	13

1. Abstract

This document provides mappings and justifications between INX's Reference Data Center architecture and the PCI DSS standard.

2. Executive Overview

With the broad reach of the PCI Data Security Standard and the increasing importance of virtualization as a business enabling technology it is crucial that organizations be prepared to address both. At the time of writing, the standard is at revision 1.2 and does not address virtualization directly. Indeed, some of the requirements appear difficult to meet within a virtualized data center.

This white paper shows how, by applying INX's reference architecture as the data center is virtualized, then PCI requirements and objectives can be met. The paper discusses the areas the standard and virtualization run into conflict, and how to address them with the correct combination of policy, technology, and architecture choices.

3. Introduction

3.1. PCI Overview

Like the need for virtualization, the Payment Card Industry Data Security Standard (PCI DSS) impacts a broad range of businesses. If a company processes, stores or transmits payment cardholder data then they must comply with the standard, regardless of their size or volume of transactions.

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized:

- **Build and Maintain a Secure Network**
 - *Requirement 1:* Install and maintain a firewall configuration to protect cardholder data
 - *Requirement 2:* Do not use vendor-supplied defaults for system passwords and other security parameters
- **Protect Cardholder Data**
 - *Requirement 3:* Protect stored cardholder data
 - *Requirement 4:* Encrypt transmission of cardholder data across open, public networks
- **Maintain a Vulnerability Management Program**
 - *Requirement 5:* Use and regularly update anti-virus software
 - *Requirement 6:* Develop and maintain secure systems and applications
- **Implement Strong Access Control Measures**
 - *Requirement 7:* Restrict access to cardholder data by business need-to-know
 - *Requirement 8:* Assign a unique ID to each person with computer access
 - *Requirement 9:* Restrict physical access to cardholder data
- **Regularly Monitor and Test Networks**
 - *Requirement 10:* Track and monitor all access to network resources and cardholder data
 - *Requirement 11:* Regularly test security systems and processes
- **Maintain an Information Security Policy**
 - *Requirement 12:* Maintain a policy that addresses information security

Also called out in the standard (though not an actual requirement) is segmenting the network. By reducing the number of areas where cardholder data is stored and managing the dataflow to and from these areas, the attack surface of the cardholder data is reduced. This reduction also allows reduction of the scope of the audit.

Currently, the standard is in revision 1.2 and there isn't any reference to virtualization, leading to all requirements being subject to the auditor's decision. Until this is addressed in the next revision (due out early next year), this white paper is designed to address best practices in the virtualized data center in line with the intent of the standard. We believe that virtualization and the standard are in no way incompatible and that appropriate data center architecture will allow organizations to meet and, in fact, exceed the requirements. We believe that, by following the tenets described and presenting them to the auditor, a virtual data center based in INX's Reference Architecture will be accepted as PCI DSS compliant.

INX is not, however, directly associated with the PCI Security Standards Council and cannot guarantee that these best practices will meet with the approval of all auditors.

3.2. Virtualization Challenges

Security in a virtualized environment changes a number of parameters from a traditional, physical machine based environment. Among these are:

- The hypervisor presents a new control plane attack
- Multiple 'machines' are now running on one physical platform
- 'Machines' can migrate between physical platforms and potentially geographies
- Interconnections between machines are present inside the physical platform, limiting both visibility and the ability to implement traditional controls
- Machines that are not running are potentially targets as much or more so than running machines

The PCI DSS covers a number of areas that intersect with these challenges. Of specific interest are the areas

- Network Segmentation
- Firewalls are required between the Internet and credit card data and the creation of DMZs to manage inbound access (1.1.3, 1.2, 1.3)
- Single function per server (2.2.1)
- Separating test and production environments (6.3.2)
- Access control for cardholder data (7)
- Use of IPS/IDS to monitor access to cardholder data (11.4)
- Direct threats to the hypervisor itself

3.3. The INX Reference Architecture

INX is in a unique position for developing virtual data center reference architecture. With expertise in all the key areas, including networking and network infrastructure, operating systems, storage, security, and in the underlying virtualization technologies, we can provide a holistic view of the required solution. Using this INX has developed a reference virtual data center architecture designed to include best practices across a range of critical areas.

4. Solutions

INX's Secure Virtual Data Center architecture addresses the PCI Data Security Standard via the use of a range of technologies, policies, and implementation standards. The PCI requirements listed in Section 3.2 can be mapped to a few basic security principles that can be extended into a virtual arena.

- Policy and Procedure
- Defense in depth
- Least Privilege
- Segmentation
- Network Intelligence

Above and beyond these areas, it is critical to use a secure and well-evaluated hypervisor platform, such as VMware's vSphere. The presentation of documentation on the security of the hypervisor can be used as a compensating control, especially as cascading threats are a significant issue in the virtualized environment without opening up a possible path to and through the underlying hypervisor.

4.1. Policy and Procedure

Many security implications for virtualization are policy and procedure based, especially around server sprawl, patching and patch management, administrative access and separation of duties, managing off-line images (both current machines and gold images for new deployments) and how new machines are deployed into networks. Additionally, much of the PCI DSS calls for clear documentation on policies and the reasons for those choices. For instance, firewall and router configurations must be documented¹, any 'insecure' access through the firewall must have business reasons², system components must have configuration standards that meet industry accepted hardening standards³, change control procedures must be in place⁴ and more.

Most of these are simply derivations of standard policies, but made more complicated by virtual machines. Some require additional enforcement hardware or systems, particularly for verification.

Deployment policies are particularly important, since they cover a multitude of security sins. These policies should address areas such as how 'gold images' are maintained (both in terms of ensuring that they are not tampered with and ensuring that they are reasonably up to date), what administrative steps are required to deploy a new virtual machine (to limit 'server sprawl' and to help maintain inventory) and the actual procedures for deploying a virtual machine (does a staging server in an isolated environment exist so that the machine can be deployed safely and securely).

¹ PCI DSS Requirement 1.1

² PCI DSS Requirement 1.1.5

³ PCI DSS Requirement 2.2

⁴ PCI DSS Requirement 6.4

Documenting how these challenges will be addressed will allow for far greater control and will feed into future policies, such as patch management.

Administrative access is another area where policy and enforcement mechanisms can be combined. Access to the hypervisor console should be restricted, authenticated, and audited, with log files written to an external system. Access to networking systems should be similarly controlled (though the use of the Nexus 1000v allows traditional network AAA methods to be used and enforced). The actual enforcement and techniques for ensuring this control is described later in this document, but it should be based upon a solid, documented foundation.

The remainder of the policies will be similar to those for traditional servers. What security software is mandated on what OS, how/when/why are systems to be patched and updated how will systems be decommissioned and similar all must be addressed. Virtualization does not provide any exceptions to traditional 'good security behaviors'.

4.2. Defense in Depth

The principle of defense in depth underlines all the other security elements being discussed here. With virtual machines capable of moving, it is critically important that security be in zones, with multiple perimeters. Additionally, these perimeters must be designed to cover virtual machines as they move from host to host (and, possibly, from data center to data center in an internal cloud).

INX's Reference Architecture provides multiple levels of control, designed to follow the machine as it moves, whether from a regular vMotion, DRS, DPM, or for business continuity reasons.

4.3. Segmentation

4.3.1. Functional Segmentation

The PCI standard requires one function per server⁵. INX recommends mapping this to one function per guest OS. When a DMZ server (or servers) are also involved, this can be mapped to a distinct blade on a UCS chassis to limit the impact.

This form of segmentation leads to each guest OS being a simpler environment and thus more easily managed and secured from a host perspective. By providing security at the host level, the threat of a cascading attack inside the virtual environment is reduced.

Further, it is important that appropriate resource limitations be configured for all servers and documented. This serves two purposes. First, the documentation provides the auditor with assurance that the chances of machines interfering with each other has been both considered and minimized. Secondly, the configuration and resource management enforces the decisions and allocations made for the machines and processes, ensuring the most efficient use of the hardware provisioned to support the line of business applications.

⁵ Requirement 2.2.1

As elsewhere, the goal is to ensure that the security elements of the design are non-intrusive and support doing business in the most efficient and effective manner possible, rather than the ‘traditional’ high impact designs.

4.3.2. Network Segmentation

INX’s reference architecture uses a combination of physical interfaces and the Nexus 1000v switch to enforce appropriate network segmentation. While this may seem controversial, the use of VLANs on the Catalyst switches as a security and segmentation device has been tested by @stake⁶ and the results show that this method provide more than sufficient segmentation. The following is excerpted from the report:

“In the interests of identifying and precisely defining security risks associated with VLANs implemented using the Cisco Catalyst family of products, @stake designed and executed a comprehensive test program. Through techniques devised to penetrate security weaknesses from a staging point within one VLAN, the @stake test suite attempted to send packets to a different VLAN and receive packets from a different VLAN. The results of @stake’s test sequences clearly demonstrate that VLANs on Cisco Catalyst switches, when configured according to best-practice guidelines, can be effectively deployed as security mechanisms.”

In our architecture, we follow these best practice methods for securing VLANs⁷ to ensure that this level of protection continues to be met.

The one area where the architecture deviates from this model is in recommending the use of a dedicated physical network for the management network. All the remaining networks are VLAN segregated on a second physical interface. These networks include:

- Dedicated Storage Network
- Dedicated vMotion Network
- Isolated networks for virtual machine zones.

Security in last category can be further enhanced by careful use of Private VLANs to isolate machines inside zones from each other as required.

The use of the Nexus 1000v allows further security measures to be applied to these VLANs, isolating traffic within the virtual machine and allowing it to be passed off to external security appliances if required. With the port profile of the Nexus switch following the virtual machine, this allows for vMotion moves to occur and the traffic to still be handled correctly in the presence of the appropriate external network elements.

⁶ http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/tech/stake_wp.pdf

⁷ http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/vlnwp_wp.htm

4.3.3. Firewalling

Separating machines into isolated networks is the first element of network segmentation. The second half, required by the standard, is to firewall these networks off from each other. The PCI standard requires the use of a stateful firewall⁸ such as an external ASA or VMware's vShield internal to the virtualized domain.

As discussed above in Section 4.1, much of the validating an environment against the PCI Standard revolves around evaluating documented policies and then ensuring that the controls in place. This is repeatedly emphasized in Section 1 of the standard, which calls for firewall configuration documents⁹ that cover change management and approval, network diagramming, management standards, business justifications of insecure protocols, and rule reviews. Once this documentation is generated, the firewall can be configured to enforce the business decisions reflected in it.

This documentation and the architecture it describes must also extend to showing how the network remains secure at all times. As above, virtualization presents some unusual challenges in this regard as Guest OS systems may physically migrate to different platforms. INX's reference architecture ensures that hosts remain secure both during this migration and after it is complete, with the security following the virtual host during its peregrinations around the physical hardware.

With vShield, this is functionality is innate; vShield security is tied to the virtual machine or group of virtual machines, not to network components. With an external firewall (such as the Cisco ASA5580), the reference architecture shows how VLANs are mapped to this device at layer 2 via the Nexus 1000v, ensuring that the security is maintained. The routed interfaces for the networks are present on the firewall platform, and this is duplicated across data centers as required to ensure that wherever the machine physically runs, the integrity of the security infrastructure remains intact.

The primary advantage of an external firewall is the ability to separate the duties of the firewall administrator and the virtual machine administrator. This is further addressed in Section 4.4.2 below.

4.4. Least Privilege

Many PCI requirements revolve around ensuring that access to the card holder data is limited to those with 'need to know'. Ensuring that users and admins have the required privilege to do their jobs and no more enforces this. In a virtual environment this includes access to stored images, to the hypervisor, and to administrative functions on the virtualized platform.

⁸ Requirement 1.3.6

⁹ Requirement 1.1

4.4.1. Default access

The first step in enforcing least privilege is to ensure that no default access methods remain. This is required by the standard¹⁰, so all default passwords, SNMP strings, and extraneous accounts on the networking and virtualization elements of the environment must be eliminated during the deployment.

4.4.2. Administrative Access

Restricting access to administration functions and ensuring that administrators can only perform the correct sub-set of functions is the first step to ensuring the security of the cardholder data. The implementation of the Nexus 1000v provides a first step in separating these duties, moving the configuration and mapping of network functions off the server administrator.

All vSphere (and Nexus 1000v) administrators should have their own, unique, user accounts¹¹. A global administrator account should be available, but not used except to recover systems and user accounts that are otherwise inaccessible. The rights of these user accounts must be documented, with only users who require access to VMs able to view or manipulate or view being given these rights.

Consideration should be given to provisioning strong authentication technologies for all users.

4.4.3. Hypervisor Access

Access to the hypervisor, whether it be direct access to the service console on an ESX system, the vCLI on an ESXi system, the web interface or from the vSphere Management Client should be restricted to a tightly controlled set of systems and networks.

This is achieved by only allowing management access to the virtual machine environment on one dedicated network, and (at a minimum) ensuring that a stateful firewall is placed between that network and any less secure network. This provides both the tight control and filtering required and provides a consolidated audit point for any attempted access.

4.5. Network intelligence

The final precept from which the architecture supports PCI is in the depth of network intelligence it presents above and beyond a bread and butter design. The incorporation of the Nexus 1000v and the use of VLAN segregation (along with intelligent choices of routing destinations) allows extensive visibility into traffic that would ordinarily be concealed.

¹⁰ Requirement 2.1

¹¹ Requirement 8.1

4.5.1. Netflow

The Nexus 1000v provides the capability for Netflow data export. This allows insight into traffic and protocols flowing inside the virtual switch, which can then be used for data analysis and anomaly detection.

This capability can be used to supplement the traditional intrusion detection or prevention type model. The Nexus's netflow capability allows insight into traffic at both the virtual adapter and physical adapter levels, significantly increasing the amount of data available for verification of the system security.

4.5.2. Intrusion Detection and Prevention

The standard calls out a requirement for up-to-date and maintained intrusion detection or prevention capabilities¹² to be deployed in networks containing cardholder data.

This can be provisioned in one of two ways. First, ERSPAN can be used to direct data to a passive IDS, merely monitoring the data. This method, while least intrusive, is also least efficient at protecting the network. It does, however, avoid issues with limiting throughput (at the expense of potentially lost attacks should the capacity of the IDS be overrun)

INX prefers to deploy an IPS solution, using an ether channel load balanced architecture. This model allows IPS devices to be stacked in a redundant configuration and to exceed 10Gb throughput.

4.5.3. Logging and Auditing

The final piece of network intelligence is the ability to see and prioritize events, as well as maintaining a trail so that data can be audited at a later date. The PCI standard requires logging to a 'difficult to alter' log host¹³, analysis of logs from security devices¹⁴ on a daily basis, and log retention for at least a year¹⁵.

At very least, the requirement for regular daily analysis predicates the installation of log analysis and correlation software, able to accept the input from the virtual machines, the security components, and critical applications running on the virtual machines.

¹² Requirement 11.4

¹³ Requirement 10.5.3

¹⁴ Requirement 10.6

¹⁵ Requirement 10.7

5. References

Reference	URL
PCI DSS	https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
Nexus 1000v overview	http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns224/ns892/ns894/at_a_glance_c45-492852.pdf
Cisco Nexus 1000V Command Reference, Release 4.0	http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0/command/reference/n1000v_cmd_ref.html
ERSpan information	www.cisco.com/web/strategy/docs/gov/turniton_erspan.pdf
vShield Overview	http://www.vmware.com/company/news/releases/vshield-security-vmworld.html
Cisco IPS4200 platforms	http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/brochure_c02-518424.pdf
Cisco SAFE – Layer 2 Security In depth	http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/sfb/lu_wp.pdf