

PCI within the IU Enterprise

Cheryl L. Shifflett, AAP, CTP
Associate Director
Treasury Operations

Daniel “Tony” Brazzell, Security+, GCUX
Lead Network Systems Engineer
University Information Technology
Services



INDIANA UNIVERSITY



IU Merchant Landscape

- Centrally Managed by Treasury Operations
- Over 200 merchant locations
- Centralized systems
 - Dial-up terminals
 - IPAS-PF (PayPal PayFlow Pro)
- Outsourced systems
 - NBS QuikPay
 - NBS Commerce Manager
 - Volusion Shopping Cart



IU Merchant Landscape

- Specialty locations with exceptions
 - Hotel
 - Ticketmaster
 - Dining
 - Parking
- 3rd parties doing business in IU space
 - Barnes & Noble
 - FLIK/Compass
 - Sodexo



IU Enterprise Environment

- 8 Campuses
- 10 Gig connection to the Internet2 backbone
- Multiple commercial Internet circuits
- 248 Buildings
- 3,148 Wireless Access Points
- 775 Switches
- 8 Class B subnets
- Multiple Firewalls



PCI Obstacles

- Specialty systems managed by departments
 - Several areas involved in PCI compliance initiative
 - Location of servers and systems
- # of locations to monitor
- Containing “surprises”
- Cost of firewalls, File Integrity Monitoring, logging solution
- Multiple solutions vs. Centralized solution



PCI Solutions

- Buy in from departments
 - Mandate from Board of Trustees
- RFP for QSA
 - Gap Analysis
 - Self Assessment Questionnaire Tracking
- RFP for ASV
- RFP for File Integrity Monitoring Solution
 - Cost sharing among departments
 - Solution includes Remote Logging, Deep Packet Inspection and Virtual Patching



Network segregation

- PCI-DSS Network
- Project management
- Host registration for cutover (moving a host to the new network)
- Pre cutover firewall requests
- Scheduling a cutover date
- Where to place firewalls
- Merchant separation – Host Based Firewalls



Host based firewalls

- Required for merchant segregation
- Host based firewalls must be stateful (SPI)
- Windows XP firewall not capable of limiting egress traffic
- Linux based systems with IPTABLES are using a stateful firewall and are capable of limiting egress traffic
- What about Deep Packet Inspection ? (6.6)



2 Factor Authentication Challenges

- What about vendors?
- Where is the PCI-DSS Network Border (Req 8.3)?
- What VPN solution should we use ?
- Can you push the two factor authentication requirement for vendors back to the vendor ?
 - Example - Ticketmaster



Firewall & Deep Packet Inspection

- Application layer firewall
- Virtual patching
- Centralized rule management



File Integrity Monitoring

- Requirement 11.5:
Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.
- What did we do ?
 - Research, RFP and Vendor Demos
 - Selected Third Brigade's Deep Security Manager
 - Open Source Products



Log Analysis

- Requirement 10.5.5:
Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).



Log Analysis - Continued

- Requirement 10.6:
Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).

Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6



New Merchant Agreements

- PCI DSS language and responsibilities
- Technical & System requirements
 - Static IP Addresses
 - Anti-virus
 - Host based firewall
 - FIMS – File Integrity Monitoring Software
 - System and Audit logs
 - Monthly Scans



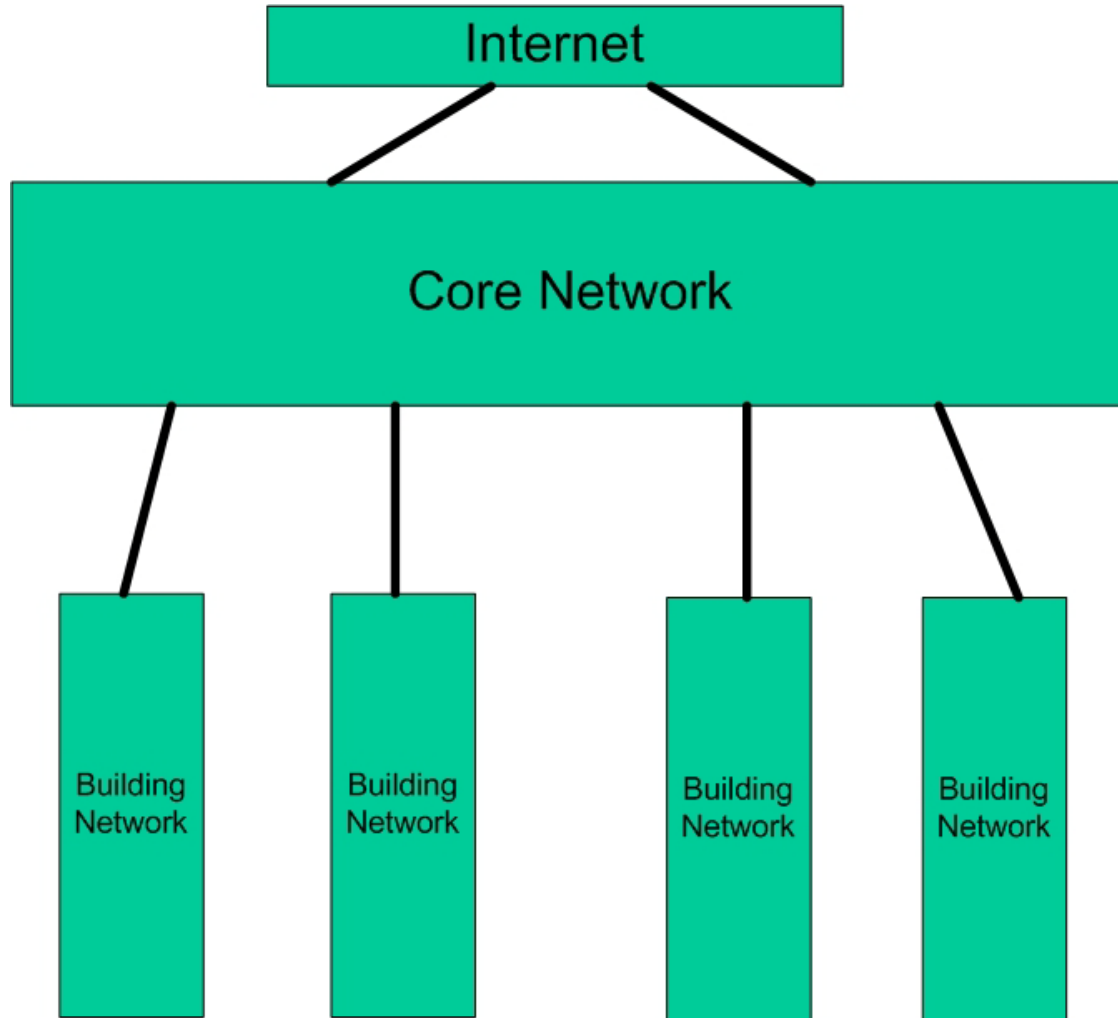
Internal Training

- SANS “Secure Coding for PCI-DSS Compliance”
- Two day mini sessions covering a variety of technical topics
 - IU Certificate Authority
 - Firewalls
 - Antivirus
 - File Integrity Monitoring
 - Remote logging
 - Network Infrastructure for PCI-DSS
 - Web Application Firewall’s
- PCI Workshop with outside expert
- Revenue Processing Training
- Quarterly Newsletter



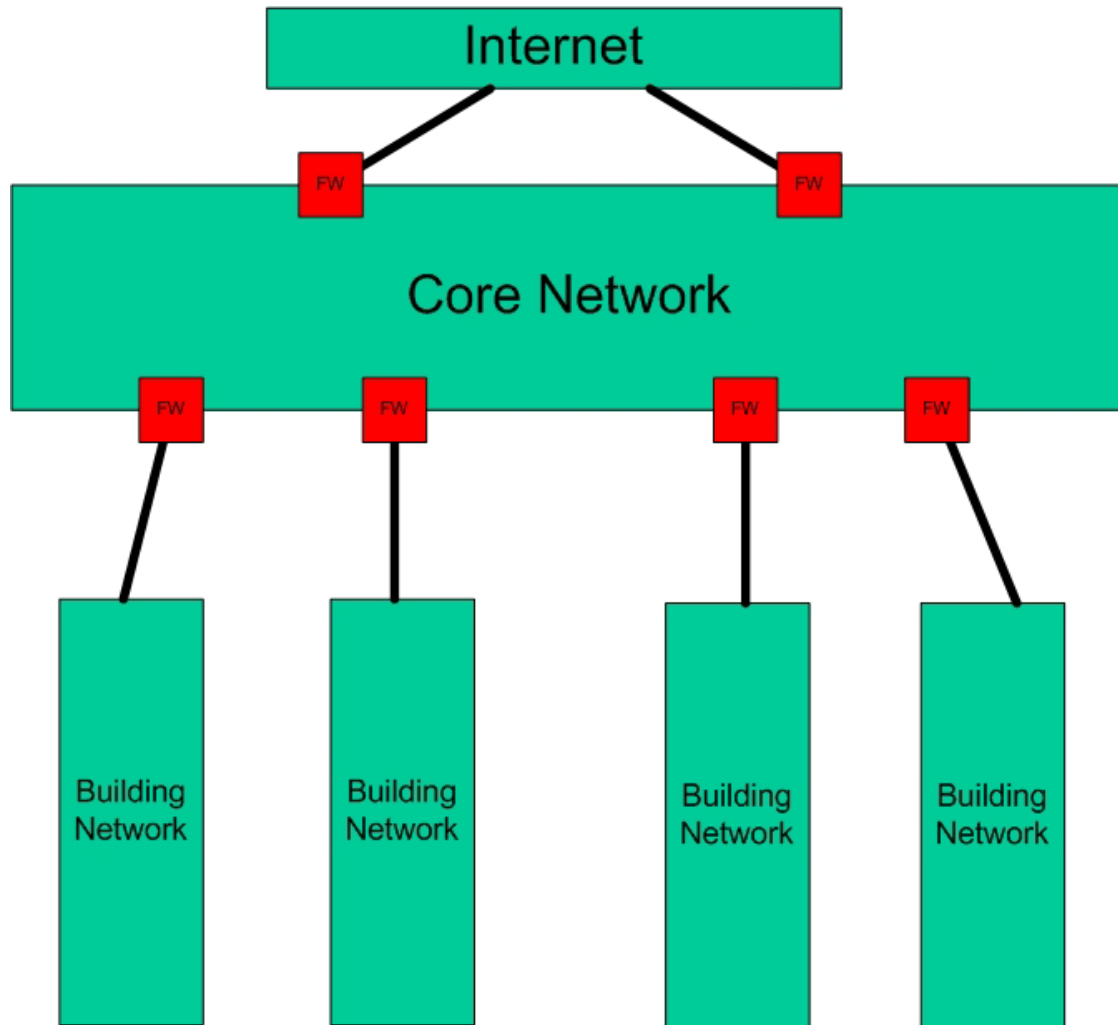
INDIANA UNIVERSITY

IU Network Core



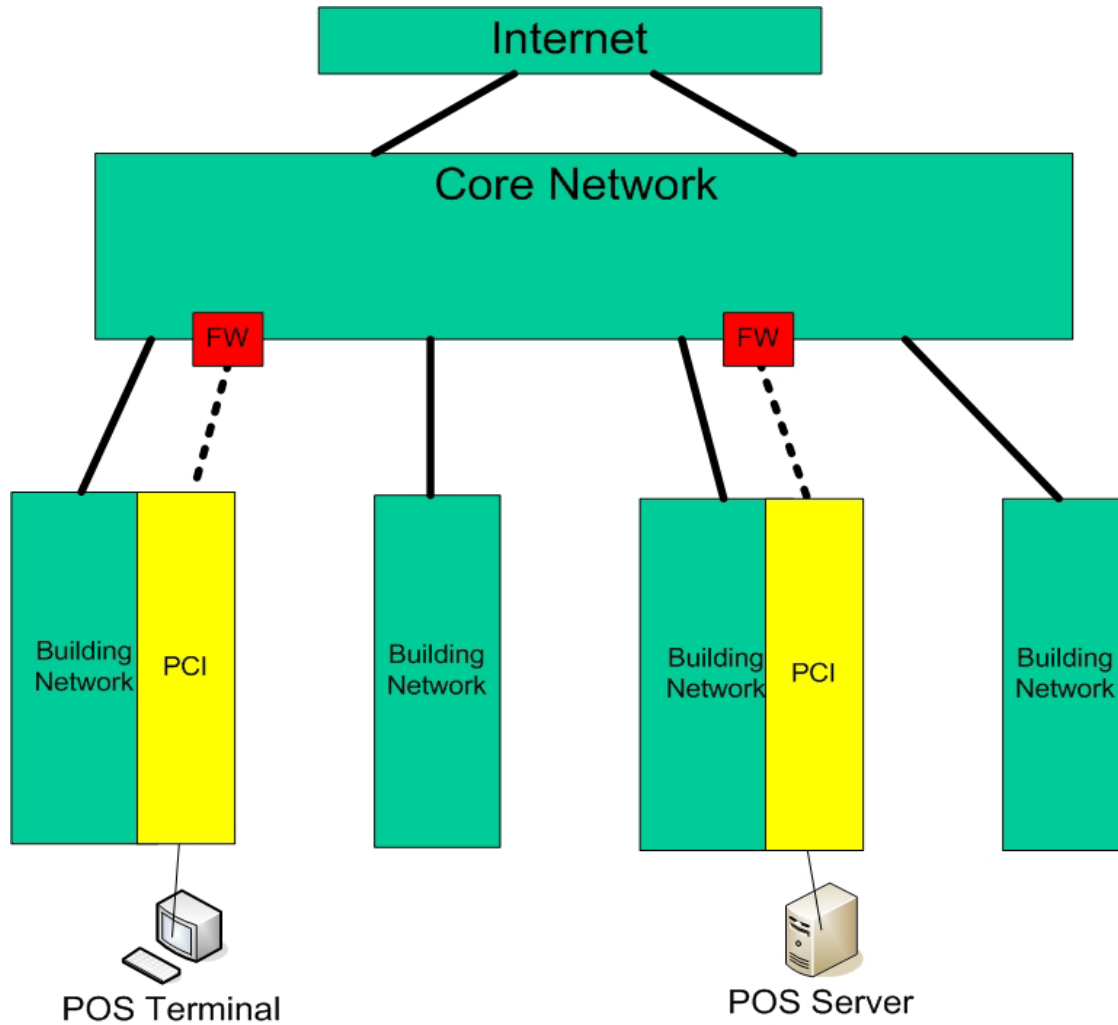


Design Options



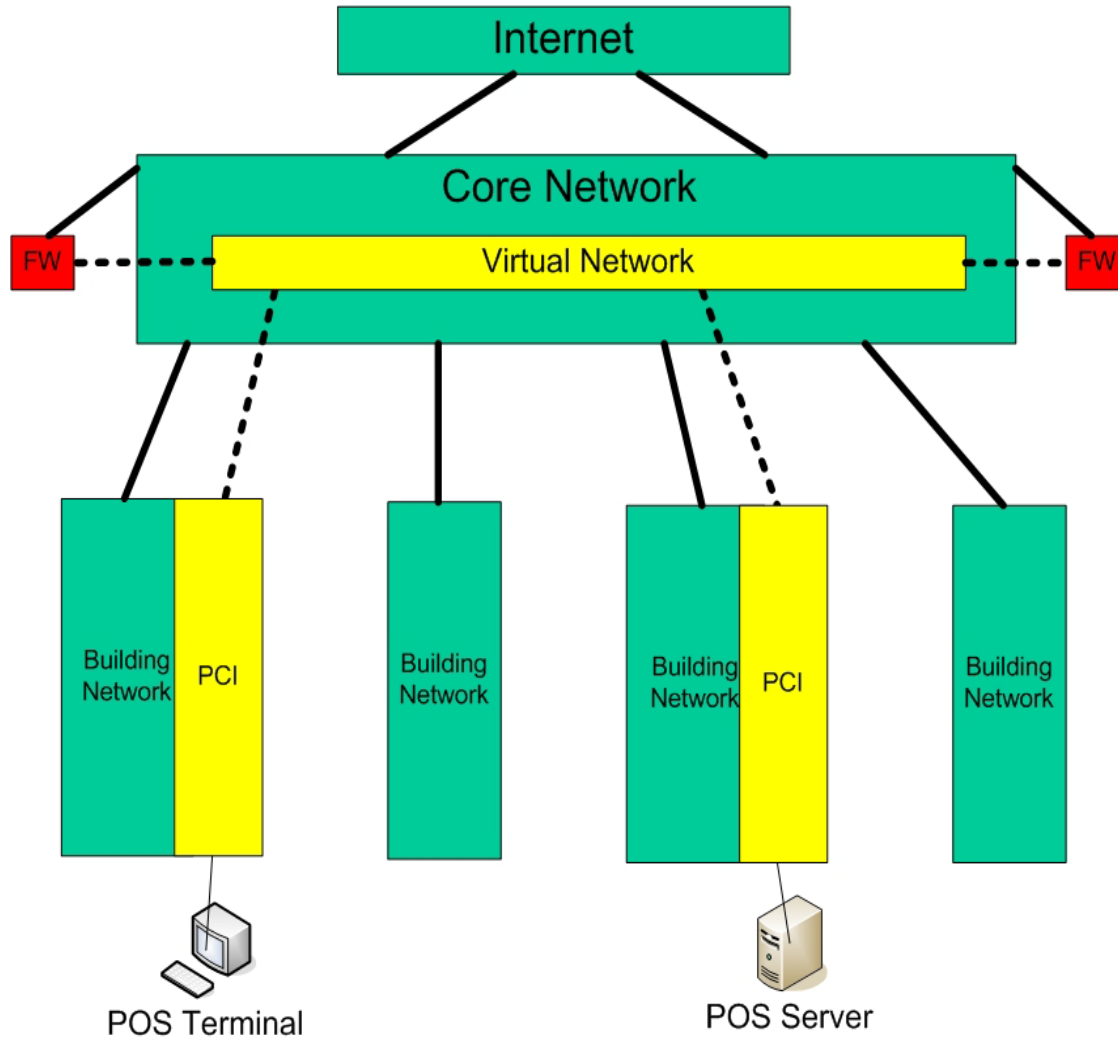


Design Options





Design Implemented





Summary

- Req 1 – Implement a stateful hardware firewall with ingress and egress filtering at the PCI-DSS Network Border. Implement host based firewall on hosts with ingress and egress filtering.
- Req 2 – Implement a configuration management system.
- Req 3 – Use database encryption and ask your outsourced vendors to use database encryption.
- Req 4 – Configure PCI-DSS systems to use encrypted transport protocols. Verify configuration with network analyzers.
- Req 5 – Use a managed AV solution with email notifications for systems with alerts.



Summary - Continued

- Req 6 – Use a Web Application Firewall such as Mod_Security or equivalent .
- Req 7 & 9 – Use the “Principle of Least Privilege” when granting access.
- Req 8 – Do not allow the use of shared or group accounts.
- Req 10 - Use an automated log parsing application.
- Req 11 – Try to group all of your merchants into a limited number of maskable IP address ranges.
- Req 12 – Develop baseline policies that your departments can use as a template.



INDIANA UNIVERSITY

Questions ?



INDIANA UNIVERSITY

References

- Cheryl Shifflett – cshiffl@indiana.edu
- Tony Brazzell – dbrazzel@indiana.edu
- Treasury Operations web site:
<http://www.indiana.edu/~iutreas>