Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Methodology for Firewall Reviews for PCI Compliance

A senior executive of the organization must sign off on the PCI DSS attestation of compliance so has overall accountability for PCI compliance. By following the methodology described in this document, the organization can ensure ongoing firewall compliance to PCI DSS, protect the organization, lower the total cost of ownership and provide accountability to senior management.

Copyright SANS Institute
Author Retains Full Rights

AD

Methodology for Firewall Reviews for PCI Compliance

GIAC (GSNA) Gold Certification

Author: K. Warren, warrenkat@gmail.com
Advisor: Adam Kliarsky

Accepted: March 19th, 2013

Abstract
A senior executive of the organization must sign off on the PCI DSS attestation of compliance so has overall accountability for PCI compliance. By following the methodology described in this document, the organization can ensure ongoing firewall compliance to PCI DSS, protect the organization, lower the total cost of ownership and provide accountability to senior management.

© 2013 SANS Institute, Author retains full rights.

1. Introduction

The focus of the firewall review methodology described in this document is on ensuring ongoing compliance with PCI DSS rather than compliance at a point in time such as when the PCI assessor is coming. Although PCI requires that firewall configurations and rule sets are periodically reviewed, the firewall review methodology described in this document addresses a number of other PCI requirements as well.

The guiding principle of the firewall review methodology is to ensure "Actual" equals "Approved" where "Approved" includes all policies, documented standards and other directives from senior management.

The objectives of the firewall review methodology are as follows:

- Ensure that the firewall configuration and rule set meet business and PCI DSS v2.0 compliance requirements by verifying that actual configurations and traffic actually flowing through the firewalls matches approved configurations and traffic that is approved to flow through the firewalls,
- Identify change management process requirements to ensure ongoing compliance,
- Identify vulnerability management process requirements to reduce risks related to managing vulnerabilities in the infrastructure,
- Reduce effort required for future firewall reviews by developing repeatable processes and procedures (lower total cost of ownership),
- Provide a mechanism to demonstrate compliance to senior management.

Although this paper is focused on PCI DSS v2.0 compliance requirements related to firewalls, this methodology describes general security best practices and can be applied to ensure firewall compliance to other standards such as ISO 27001/2 and to business requirements.

© 2013 SANS Institute. Author retains full rights.

2. Terminology

For the purposes of this document, "infrastructure" refers to all devices, applications and network components as well as supporting policies and processes that are in scope for PCI.

3. Overview: Firewall Review Methodology

The purpose of the firewall review is to ensure that the firewall configuration and rule set meets the business and compliance requirements of the organization. In order to effectively review firewalls, the business and compliance requirements must be clearly identified.

For this reason, prior to reviewing the firewall configuration and rule set, it is critical to verify that the documentation describing the organization's business and compliance requirements is accurate, complete and current.

Table 1
Firewall Review Methodology Overview

Review Activity	Business and Compliance Requirements (Approved)	Actual
Configuration	Standard configuration for firewalls (secure baseline)	Configuration on the firewall
Rule Set	Network diagrams Documented information flows Approved services, protocols and ports list	Firewall rule set Hits on rules Traffic flowing though firewall

The initial firewall review is typically conducted in preparation for the first PCI assessment. As the business and compliance requirements may not be fully understood, the initial firewall review may include developing and refining the requirements and supporting documentation. For example the approved services, protocols and ports list may not exist as it may not be known what traffic should be allowed and what traffic is not required for valid business purposes.

The initial firewall review can be used to establish the process for subsequent firewall reviews. Section 4 describes the preparation activities for an initial firewall review. Preparation activities for the initial firewall review are summarized in Table 2 below.

© 2013 SANS Institute. Author retains full rights.

Table 2
Preparation for Initial Firewall Review

Activity	Section
Establish tracking mechanism for firewall reviews	4.1
Document information flows	4.2
Document approved services, protocols and ports list	4.3

The preparation activities for subsequent firewall reviews are described in section 5. Preparation for each firewall review includes the activities described in Table 3 below.

Table 3
Preparation for Each Firewall Review

Activity	Section
Assign review tasks	5.1
Verify mechanism to capture firewall rule usage	5.2
Collect required documentation	5.3

The activities of the firewall review are described in section 6. A summary of the firewall review activities is identified in Table 4 below.

Table 4
Firewall ReviewActivities

Step	Activity	Section
	Ensure business and compliance requirements are current, accurate and complete	
1	Review network diagram	6.1
2	Review information flows	6.2
3	Review approved services, protocols and ports list	6.3
	Assess firewall – Evaluate Actual Against Requirements	
4	Review Firewall configuration	6.4
5	Review FW rule set	6.5
	Remediate	
6	Implement remediation as required	6.6
	Ensure Audit Trail	
7	Prepare report on findings	6.7
8	Update firewall review audit trail	6.8

As compliance is not a point in time, the firewall methodology addresses ongoing firewall compliance. Key processes and procedures required for ongoing compliance are described in section 7. A summary section 7 is identified in Table 5 below.

Table 5

© 2013 SANS Institute. Author retains full rights.

Key Processes & Procedures for Ongoing Compliance

Activity	Section
Periodic firewall review	7.1
Change management process	7.2
Vulnerability management	7.3
Continual improvement	7.4

The PCI requirements applicable to the firewall review methodology are listed in Appendix B.

4. Preparation for Initial Firewall Review

4.1. Establish Tracking Mechanism

As firewall reviews must be conducted every six months (PCI requirement 1.1.6), it is beneficial to establish a mechanism that ensures consistency from review to review and that enables assessment and refinement of the process itself, that is, allows continual improvement. The mechanism must also ensure that an audit trail of each review is maintained. The PCI assessor not only looks for evidence that reviews are being conducted every six months but evidence of who conducted the reviews, what was reviewed and findings coming out of reviews.

The firewall review tracking requirements can be met by using two simple forms: a master firewall review tracking form and a firewall review results form.

The firewall review tracking form and the results form described in the next two subsections, along with the final report on findings, are designed to capture all information required for PCI as well as for continual improvement.

4.1.1. Master Firewall Review Tracking Form

The master firewall review tracking form is essentially a basic project management tracking spreadsheet. It identifies who is responsible for each review task, expected/actual completion date, the status of the activity and whether any deficiencies were found. The master firewall review tracking form accommodates different people conducting different portions of the review. If only one person is conducting all portions of the review then either

© 2013 SANS Institute. Author retains full rights.

insert that person's name in the "Assigned to" field for each task or, alternately, remove the "Assigned to" field and insert the person's name at the top of the form.

A sample master firewall review tracking form is illustrated in Figure 1 below.

Task	Assigned to	Completion Date	Status
Lead – Firewall Review			
Review/Update Network Diagram			
Review/Update Information Flow Diagrams			
Review/Update Approved List			
Review Firewall Configuration			
Review Firewall Rule Set			
Prepare Findings Report			
Lead – Remediate Deficiencies			
Final			
Prepare final report			
Present final report to senior management			
Update firewall review audit trail			

Figure 1. Sample Master Firewall Review Tracking Form

Figure 2 below illustrates an example of a completed firewall review tracking form. In this example, two firewalls were reviewed (the Internet facing firewall and the internal firewall).

Task	Assigned to	Completion Date	Status
Lead – Firewall Review	Philip Fry	Jan 31, 2013	Complete
Review/Update Network Diagram	Amy Wong	Dec 10, 2012	Complete
Review/Update Information Flow Diagrams	Amy Wong	Dec 17, 2012	Complete
Review/Update Approved List	Bender	Dec 1, 2012	Complete
Internet FW: Review Firewall Configuration	Leela	Dec 10, 2012	Complete
Internet FW: Review Firewall Rule Set	Leela	Dec 17, 2012	Complete
internal FW: Review Firewall Configuration	Professor Farnsworth	Dec 10, 2012	Complete
internal FW: Review Firewall Rule Set	Professor Farnsworth	Dec 17, 2012	Complete

© 2013 SANS Institute. Author retains full rights.

Task	Assigned to	Completion Date	Status
Prepare Findings Report	Philip Fry	Dec 20, 2012	Complete
Lead – Remediate Deficiencies	Philip Fry	Jan 15, 2013	Complete
Final			
Prepare executive summary	Philip Fry	Jan 31, 2013	Complete
Present final report to senior management	Philip Fry	Jan 31, 2013	Complete
Update firewall review audit trail	Philip Fry	Jan 31, 2013	Complete

Figure 2. Example - Completed Master Firewall Review Tracking Form

4.1.2. Firewall Review Results Form

A review form should be prepared for reviewers to capture review results. Each reviewer completes the firewall review results form for each review item. If a deficiency is found then the reviewer logs it on the form. If the remediation required to address the deficiency is known then it should also be recorded in the form. Some deficiencies may be remediated immediately but this is not required. For example when reviewing the network diagram a device is found to be missing. In this case it makes most sense to update the network diagram as soon as the omission is detected. Other remediation may require more effort so can be addressed later.

What is important here is that all found deficiencies are identified even if remediated immediately. This enables assessment of the efficiency of and compliance with organizational processes and procedures. For example an out of date network diagram could be a result of a gap in the change management process or of non-compliance with the process.

On completion of the review item, the reviewer submits the completed form to the firewall review lead. The firewall review lead is responsible for consolidating the results into the firewall review findings report.

If multiple firewalls are reviewed, use a separate form for each firewall.

Tip: Use the initial firewall review as an opportunity to document review procedures. Subsequent firewall reviews are opportunities to review and refine the procedures.

A sample review results form is illustrated in Figure 3 below.

Firewall Review Results Form

© 2013 SANS Institute, Author retains full rights.

Item(s) Reviewed	☐ Network Diagram ☐ Information Flow Diagrams ☐ Approved Services, Protocols and Ports List ☐ Firewall Configuration ☐ Firewall Rule Set
Reviewer	
Review Start Date	
Review End Date	
Effort (hours)	
Firewall Hostname/IP (if reviewing firewall configuration or rule set)	

Documents Reviewed

<include document version>

Describe tools, data and methodology used to conduct review

<If documented procedure was followed then identify the document describing the procedure.>

	Deficiency Found	**Remediation**	**Status** (completed/outstanding)
1			
2			
3			
4			

Figure 3. Master Firewall Review Results Form

© 2013 SANS Institute. Author retains full rights.

4.2. Document Information Flows

4.2.1. Information Flows and Firewall Reviews

Although documentation of information flows is not specifically required for PCI compliance, it facilitates compliance and provides many other benefits to the organization. Information flows can be documented in matrices and/or diagrams. Capturing information flows in diagrams or matrices provide a logical/pictorial view of traffic flows in the infrastructure. Documented information flows provide an effective aid in identifying potential security risks in the infrastructure and in identifying what services, protocols and ports are allowed through firewalls.

A key component of the firewall review is verification of actual traffic flows and services/protocol/ports flowing through the firewall against the approved services, protocols and ports list. The first time the organization conducts a firewall review, actual traffic flowing through the firewall is mostly likely not well understood and the approved services, protocols and ports list, if it does exist, probably does not identify all services, protocols and ports required for the business. Traffic sniffing may be required to determine actual traffic. Port scans through the firewall are also in order to identify services which are not currently being used but are allowed through the firewall.

Documented information flows facilitate creation of the approved services, protocols and ports list and provide valuable input to the initial firewall review. They are also useful for validating the approved services, protocols and ports list in future firewall reviews.

© 2015 SANS Institute, Author retains full rights.

4.2.2. Other Benefits

A logical/pictorial understanding of traffic flows in the infrastructure is an effective aid in planning for new services, changes in the infrastructure, equipment replacement/augmentation and decommissioning of devices and applications. They also facilitate troubleshooting activities as they illustrate the flow of traffic in the infrastructure, enabling support personnel to quickly drill down to the root cause of troubles. For example if traffic is not getting from point A to point B, documented information flows illustrate what components the traffic flows through between point A and point B. Lastly, documented

information flows enable new personnel to get up to speed quickly on what is going on in the infrastructure.

4.3. Prepare/Update Approved Services, Protocols and Ports List (Approved List)

4.3.1. Approved List & Firewall Reviews

PCI DSS requirement 1.1.5 states that the organization must ensure that all services, protocols and ports which are allowed through the firewall have a legitimate business purpose for PCI compliance. As senior management has overall accountability for compliance, they must sign off on the approved list of services, protocols and ports (hence "approved"). The Approved List is effectively a directive from senior management as to what traffic is to be allowed through the firewall.

Technical staff is responsible for obtaining senior management approval prior to introducing new services, protocols or ports into the infrastructure. Approval is obtained by updating the Approved List and submitting to senior management for approval. In this way the "rules" can be determined in a central place and then fanned out to existing devices and configuration standards reducing the risk that unnecessary services, protocols or ports are active.

Note that although the Approved List may not be specifically identified in other security standards, it is a critical component. The Approved List identifies acceptable risks related to services, protocols and ports in use and what traffic is allowed to flow where. As such, the Approved List enables senior management to understand the infrastructure security posture and is effectively the benchmark that firewall rule sets can be measured against.

4.3.2. Collecting Data for the Approved List

If the Approved List does not already exist, the data collected in the documented information flows can be used to create the initial approved list of approved services, protocols and ports. The initial firewall review will flag anything not initially identified in the Approved List.

© 2013 SANS Institute, Author retains full rights.

4.3.3. Use of Unencrypted Services, Protocols and Ports

PCI DSS requires that if an unencrypted service/protocol/port is required then compensating controls must be implemented. The PCI assessor will require that all compensating controls are well documented and meet PCI requirements. Compensating controls are tricky – even if the PCI Qualified Security Assessor (QSA) performing the PCI assessment may initially accept the compensating control, the acquiring bank has the final say.

See appendix B and C of the *PCI DSS Requirements and Security Assessment Procedures Version 2.0* (https://www.pcisecuritystandards.org/) for guidance on compensating controls.

4.3.4. Approved List Signoff

Senior management is responsible for ensuring that all services, protocols and ports identified in the Approved List can be justified for business purposes. Senior management is also responsible for ensuring that unencrypted services, protocols and ports are not used where possible.

If there is a business requirement for an unencrypted service/protocol/port then senior management is responsible for ensuring that appropriate compensating controls are identified, documented and are correctly implemented.

© 2013 SANS Institute. Author retains full rights.

5. Prepare for All Firewall Reviews

5.1. Assign Review Tasks

Use the master firewall review tracking form to record who is assigned to each task and to track status. Depending on the size and organizational structure of the organization, the firewall review lead may also be responsible for some or all of the review tasks. Regardless, the firewall review lead has overall responsibility for all review activities.

5.2. Verify Mechanism to Capture Firewall Rule Usage

Ensure that either all firewall rules have logging enabled, including "deny" rules, and that logs are being forwarded to a centralized log server. If logging was not enabled on all rules then postpone the firewall rule set review until sufficient log data has been collected once logging has been enabled.

PCI DSS does not specifically require logging of connections on firewalls (note that there is a specific requirement for audit logging – PCI requirement 10.2)). However logging of both connections and denies is recommended as this information is invaluable for both firewall rule set reviews and for troubleshooting issues in the infrastructure.

Monitoring "hit" counts on rules provides information on rule usage but is lacking the detail needed to drill down into what specific traffic is hitting a particular rule especially when a rule allows multiple protocols and IPs. This level of detail is particularly useful when trying to eliminate the use of "any" in rules (which should be avoided where possible for PCI compliance).

5.3. Collect Required Documentation

The following documents are required for the review. If a firewall review has not been conducted before then some of this documentation may be missing. The firewall review methodology will ensure that any missing documents will be created as part of the initial firewall review.

The required documents are listed in Table 6 below.

Table 6
Documents Required for the Firewall Review

Document
Approved Services, Protocols and Ports List (Approved List)
Network Diagram
Information Flow Diagrams/Matrices
Firewall standard configuration (secure baseline)

© 2013 SANS Institute, Author retains full rights.

6. Firewall Review

The firewall review consists of 8 steps are identified in Table 7 below.

Table 7
Firewall Review Steps

Step	Activity
1	Review Network Diagram
2	Review Information Flows
3	Review Approved Services, Protocols and Ports List
4	Review Firewall Configuration
5	Review Firewall Rule Set
6	Implement Remediation as Required
7	Prepare Report on Findings
8	Update Firewall Review Audit Trail

Record all deficiencies found along with the associated remediation status (remediation implemented, outstanding).Where possible implement remediation as you go. For all remediation implemented, appropriate verification testing is required. For example if the firewall configuration identifies unneeded services running then, after the services have been disabled, post change testing such as a port scan is required (PCI requirement 1.1.1 and 11.3).

6.1. Step 1: Review Network Diagram

Perform a device scan to discover all devices in the infrastructure. Use the device scan results to verify that the network diagram is current and complete. If devices are found that are not in the network diagram or there are devices in the network diagram that were not found by the scan then review change tickets to determine whether there is an approved change ticket supporting the change. Make sure that each component in the network diagram is properly labeled with its hostname and IP address(es).

An example of found deficiencies and associated remediation tasks is illustrated in Figure 4 below.

© 2013 SANS Institute, Author retains full rights.

Deficiency	Remediation	Status
New device found in infrastructure with no supporting approved change ticket	Remove device from infrastructure.	Done
	Review change management procedures . Ensure mechanisms in place to prevent this (e.g. all unused switch/router ports disabled until approved change ticket to enable).	Outstanding
Device no longer in infrastructure with no supporting approved change ticket	Submit change ticket for decommissioning of device (e.g. disable monitoring).	Done
	Update network diagram.	Done
New device has supporting change ticket but network diagram not updated	Review change management process/procedures and address any gaps. If no gaps in process then address non-compliance with change management processes/procedures.	Outstanding
	Update network diagram.	Done
Device removed with supporting change ticket but network diagram not updated	Review change management process/procedures and address any gaps. If no gaps in process then address non-compliance with change management processes/procedures.	Outstanding
	Update network diagram.	Done

Figure 4. Example illustrating found deficiencies in the network diagram, identified remediation activities and the status of the remediation.

© 2013 SANS Institute, Author retains full rights.

6.2. Step 2: Review Information Flow Diagrams

Verify that information flows have been captured for all components identified in the network diagram. Note that if deficiencies are identified in the network diagram review then it is highly likely that similar deficiencies will exist in the information flow diagrams.

6.3. Step 3: Firewall Configuration Review

For any deficiencies identified during the configuration review, record the deficiency and remediation status (e.g. remediation implemented or outstanding).

6.3.1. Verify the Standard Configuration

PCI requirement 2.2 requires that configuration standards be documented for all components in the infrastructure including firewalls and that the configuration standards are in alignment with industry-accepted hardening standards. It also states that configuration standards must address security hardening requirements to address all known security vulnerabilities. Requirement 2.2 specifically references several industry-accepted system hardening standards sources - the *Center for Internet Security (CIS) (www.cisecurity.org)*, the *International Organization for Standardization (ISO) (www.iso.org),* the *SysAdmin Audit Network Security* Institute (SANS) (www.sans.org) and the *National Institute of Standards Technology (NIST (www.nist.gov)*.

Configuration standards specify the minimum configuration to be applied to all new systems in the infrastructure. In addition, when the configuration standards are updated then the updated configuration standard must be applied to all applicable systems in the infrastructure.

Table 8 below lists minimum configuration items, as specifically identified in PCI DSS to be included in the standard firewall configuration.

Table 8
Standard Firewall Configuration – Minimum Requirements

Category	Standard Firewall Configuration	Comments
Version and Patch Level	Identify the current version and patch level.	When a new patch or version is identified, the configuration standard must be updated. Ensure that all critical patches have been applied to the firewall. PCI requirement 6.1 states that critical patches must be applied within one month of release by vendor.
Active Services	List all services, protocols and ports to be disabled.	Often the default configuration on firewalls has services such as TELNET, web services and finger enabled by default. Services, protocols and ports allowed on the firewall may be more restrictive that what is allowed on other systems. PCI requirements 2.2.2, 2.3 and 8.4
Disclosure of Private IP Addresses	Identify configuration of mechanisms to prevent disclosure of private IP addresses and routing information.	Appropriate mechanisms include one or more of the following - Network Address Translation (NAT), proxy servers, route advertising of private networks and/or use of the RFC 1918 address space for internal addressing. PCI requirement 1.3.8
Stateful Inspection	Specify requirement for use of stateful inspection	PCI requirement 1.3.6
Network Architecture	Specify requirement for a firewall at each Internet connection between any	PCI requirement 1.1.3

© 2013 SANS Institute, Author retains full rights.

Category	Standard Firewall Configuration	Comments
	demilitarized zone and the internal network zone	
Access Controls	Identify all vendor-supplied user accounts and specify what the defaults should be changed to (e.g. change username, password). Specify SNMP community strings to be used, SNMP servers allowed to connect, disable SNMP SET (i.e. SNMP set to read-only). Identify all necessary accounts to be removed or disabled.	Accounts with "admin" in the name should be changed where possible. Identify the configuration for integration with centralized access control (e.g. TACACS, RADIUS). PCI requirements 2.1, 7.1.1, 7.1.2 and 8.1
Time Synchronization	Identify central time synchronization servers.	All components in the infrastructure should synchronize to the same central time source. PCI requirement 10.4
Audit Trails	Identify logging configuration – log all access attempts. Specify configuration for forwarding of log data to a centralized log server.	May want to also log all connections through the firewall – if so the configuration should be documented in the standard configuration. PCI requirement 10.2
Other	Identify any other available security configuration such as IP spoofing prevention, DoS detection, blocking malicious/malformed DNS packets	Security best practice – features and mechanisms available are dependent on firewall make, model and IOS

6.3.2. Evaluate the Actual Firewall Configuration

Compare the actual firewall configuration with the documented standard configuration. Log any configuration items identified in the standard configuration which have not been implemented on the firewall as deficiencies. Run port scans against each interface on the firewall to identify any unneeded or insecure services running on the firewall. Pay particular attention to services, protocols and ports running on internet facing interfaces. Some protocols such as ICMP ping may be acceptable on internal firewall interfaces but not on any internet facing interfaces.

Although PCI requires that penetration testing is conducted on a yearly basis (PCI requirement 11.3), as part of the firewall configuration review it is beneficial to run specific penetration tests to investigate the behavior of the firewall when traffic such as malformed packets and unexpected packets is presented to the firewall (e.g. ACK with no connection attempt in progress).

Inspect firewall log data on the centralized log server and verify the presence of audit log data. Verify that the firewall logs all changes to the time configuration. Attempt to login to the firewall using vendor-supplied accounts/passwords (vendor-supplied accounts should be listed in the standard configuration) to verify that passwords have been changed from the

© 2013 SANS Institute, Author retains full rights.

default. Vulnerability scanners are useful here as they are able to report on vendor-supplied accounts with default passwords.

Review access controls in place for accessing firewalls and user accounts which are able to login to the firewalls and verify that access is based on the principle of least privilege and that assignment of privileges to individual is based on job classification and function (default "deny-all" as per PCI requirement 7.2.3). Check for the existence and use of generic user accounts. PCI requirement 8.1 requires that unique usernames, which are specifically assigned to an individual, are used to access all components in the infrastructure.

6.4. Step 4: Firewall Rule Set Review

6.4.1. Traffic Analysis

Firewall rule set reviews require a listing of the rule set from the firewall, rule usage statistics for each rule and data on both traffic allowed through the firewall and denied by the firewall. The Approved List is also required for the rule set review. Review the use of "any" in the source, destination or port in "allow rules". For each "allow" rule, drill down into actual traffic and determine what is talking to what on what port. Only traffic identified in the Approved list is allowed to pass through the firewall. This applies to not only inbound traffic but outbound traffic as well. Egress filtering is often overlooked but is required (PCI requirement 1.2.1).

Identify any traffic using unapproved ports that is being allowed through the firewall. For each detected instance, record the source and destination IP addresses. Inspect all traffic hitting the "deny" rules. Denied traffic may be an indication of unapproved services, protocols and ports in use in the infrastructure. Pay particular attention to denied traffic between the DMZ and the internal network and outbound to the Internet inbound. For all denied traffic originating from within the infrastructure, record the source IP and port(s) used.

Identify any "allow" rules which do not have comments. Each rule should have a comment indicating the business requirement. Where possible, the change ticket number associated with implementation and/or last modification of the rule should be included in the comments.

© 2013 SANS Institute, Author retains full rights.

Rules which are never hit and rules which "shadow" or partially "shadow" other rules should be assessed. "Shadow" rules are rules which grant the same or similar access to other rules. Rules which are never hit indicate the presence of more permissive rules prior to the unused rules and/or that the rules are not required and can be removed.

Pay particular attention to all instances where more permissive rules are hit before more restrictive rules.

Finally, verify that there is a "deny all" rule at the end of the rule set.

6.4.2. Performance Analysis

Tuning the firewall rule set is not required for PCI. However, as the firewall rule set review requires examining traffic patterns through the firewall in detail, by default the data required to tune the firewall is collected.

Review the hit counts on each firewall rule and identify those rules which are most frequently hit. As firewalls apply the rules to traffic in sequential order, for optimal performance the firewall rule set should be organized so that the most used rules should be higher up in the policy.

6.4.3. Prepare Updated Firewall Rule Set

Based on the findings from the rule set review and the performance analysis, prepare an updated rule set to be applied to the firewall (see Appendix A for tips on firewall rules). The updated rule set should address all deficiencies identified in the rule set review as well as any performance improvements that were identified in the performance analysis.

If a firewall review has not been conducted before, the Approved List most likely will have deficiencies. The biggest challenge when doing the firewall rule set review for the first time is that what traffic is required for the business is often not fully understood at the outset of the review. Be prepared to go through several iterations of the firewall rule set review to bring the Approved List and the firewall rule set into alignment.

© 2013 SANS Institute, Author retains full rights.

6.5. Step 5: Consolidate Findings

All reviewers submit their completed firewall review results forms to the firewall review lead. The firewall review lead is responsible for consolidating all identified deficiencies, remediation actions and the status of each remediation action from each results report into a consolidated list.

Figure 5 below illustrates an example consolidated list.

Category	Deficiencies	Remediation Actions	Status
Approved List	Ports 18190 and 18205 (Checkpoint SmartCenter) in use but missing in Approved List	• Update Approved List and obtain sign-off.	Completed
Approved List	Requirement for FTP to obtain AV updates from vendor	• Determine required compensating controls. • Document and implement compensating controls.	Outstanding
Actual Configuration - Firewall	Small services such as TELNET, finger active on firewall – secure baseline includes directives to disable these services	• Review change management processes to ensure secure baselines are applied prior to deployment in the infrastructure and that when the secure baseline is updated the updated configuration is applied to the firewall.	Outstanding
Firewall Rule Set	No restrictions on outbound traffic	• Apply updated rule set to firewall to restrict outbound traffic as per Approved List	Completed
Network Diagram	Network diagram missing recently deployed system	• Update network diagram to reflect current infrastructure. • Review change management processes to ensure network diagram is updated when changes are implemented.	Completed
Secure Baseline Configurations – other systems	Windows 2008 servers attempting to communicate with remote devices via services identified to be disabled in the Windows 2008 secure baseline (traffic was denied by the firewall)	• Update secure baseline configurations to disable unapproved services//protocols/ports. • Apply updated secure baseline configuration to all applicable systems.	Outstanding

Figure 5. Example consolidated list of found deficiencies, identified remediation actions and the status of the remediation actions.

© 2013 SANS Institute. Author retains full rights.

6.6. Step 6: Remediate Deficiencies

6.6.1. No Remediation Required

If no remediation required then go to step 7.

6.6.2. Prepare Remediation Plan

The firewall review lead is responsible for preparing the remediation plan and overseeing the remediation tasks. Use the consolidated list to build the remediation plan. Assign an "owner" and determine target completion dates for each task.

An example remediation plan is illustrated in Figure 6 below.

Task	Owner	Target Completion Date	Actual Completion Date	Status
Apply updated firewall rule set	Leela	Jan 10, 2013	Jan 11, 2013	Done
Update Approved List	Bender	Jan 10, 2013	Jan 8, 2013	Done
Update secure baseline configuration – Windows XP	Malcolm Reynolds	Jan 3, 2013	Jan 10, 2013	Done
Apply updated secure baseline configuration – Windows 2008	Malcolm Reynolds	Jan 18, 2013	Jan 18, 2013	Done
Update information flow diagrams	Hermes Conrad	Jan 31, 2013		Open
Apply updated firewall rule set	Leela	Jan 31, 2013		Open

Figure 6. Example remediation plan showing the owner of each task, expected and actual completion dates and the current status.

© 2013 SANS Institute. Author retains full rights.

6.6.3. Implement Remediation

Implement all remediation identified in the report on findings. Task owners are responsible for the preparation of change implementation plans, submission of change tickets, change implementation, verification, updating of documentation and obtaining sign-off on documentation, where applicable.

Task owners are also responsible for notifying the firewall review lead when the task has been completed. The firewall review lead is responsible for updating the status of each task in the remediation plan.

6.7. Step 6: Present Final Report to Senior Management

6.7.1. Prepare Final Report

The final report should include the date the final report was prepared, the author of the report, whom the report is to be submitted to, the final outcome of the firewall review (compliant/not compliant), an executive summary, the completed firewall review forms, the completed tracking form, the consolidated list of findings and the remediation plan (including the status of all remediation activities).

Including trending data in the report is useful for demonstrating continual improvement. Useful metrics include the effort required to complete the firewall review and the number of deficiencies found. As this data has already been collected, little effort is required to pull the trending data together. By presenting the metrics for previous reviews along with the latest review, the organization can determine whether the firewall process and/or other processes are becoming more efficient over time. The effort required to complete firewall reviews should decrease over time as the procedures are refined and personnel gain proficiency. The number of deficiencies found not going down over time is an indication of ongoing non-compliance.

With the exception of the executive summary, all of the information to be included in the final report has already been collected and just needs to be pulled together.

A sample template for the final report is illustrated in Figure 7 below.

© 2013 SANS Institute, Author retains full rights.

Firewall Review <hostname(s)> Final Report
Date of Final Report
Prepared by:
Submitted to:

Status: Compliant/not compliant

Executive Summary
Objectives are:
- Demonstrate that actual = approved
- Awareness to senior management of problematic areas (e.g. denied traffic indicating deficiencies in secure baseline configurations on other systems in the infrastructure, gaps in change management processes/procedures)

Trending Data

Appendix A: Completed review forms
Appendix B: Completed tracking form
Appendix C: Consolidated list of findings
Appendix D: Remediation Plan

Figure 7. Sample final report template.

6.7.2. Present Final Report to Senior Management

The firewall review lead submits the final report to senior management. In addition, senior management may choose to hold a meeting where the firewall review lead presents the report. In this case, a few t slides highlighting key points from the executive summary are in order. Include the trending data to demonstrate efficiency gains in the firewall review process. A low effort to execute the firewall review and a low number of deficiencies found indicates both ongoing compliance and the efficiency of the firewall review process.

© 2013 SANS Institute, Au

6.8. Step 8: Update Firewall Review Audit Trail

The organization must provide proof to the PCI assessor that firewall reviews are conducted at minimum every six months and will want to see all supporting documentation. As the final report contains all the information required to satisfy PCI requirements, it is sufficient to simply store the final report from each firewall review in a secure location. Due to the sensitivity of the information contained in the final report, access to the reports should be restricted.

7. Maintaining Firewall Rule Set Compliance

7.1. Periodic Firewall Review

Firewall reviews must be conducted, at minimum, every six months (PCI requirement 1.1.6). In order to demonstrate compliance, an audit trail must be maintained (see section 6.8). Keep all firewall review reports in a secure location and make sure they can be accessed when required (e.g. when the PCI assessor comes).

The first time a firewall review is conducted, the review is effectively a discovery phase to determine what is actually going on in the infrastructure. With the knowledge gained from the first firewall review and effective change management processes and procedures (see section 7.2) going forward, subsequent rule set reviews should require significantly less effort as the gap between what is approved and actual traffic allowed through the firewall is minimized.

7.2. Change Management Process

A change management process that ensures that appropriate testing is conducted to verify that changes do not introduce unacceptable risks into the infrastructure and that documentation is kept current as changes are introduced into the infrastructure is not only a PCI requirement itself but is critical to ensuring ongoing compliance.

Security testing procedures should be identified for different change scenarios, such as when introducing significant changes into the infrastructure, changing firewall rules, upgrading major software versions and changing standard configurations.

The PCI assessor will want to see evidence of an effective change management process (approvals, appropriate documentation updated, verification testing, etc.). For example, incorporating updating of the network diagram in the change management process ensures that the network diagram is kept current at all times and reduces effort required preparing for audits and firewall reviews.

Checklists identifying all activities which must be completed when devices/applications are introduced into or removed from the infrastructure ensure that

© 2013 SANS Institute, Author retains full rights

activities are not missed. As such, checklists help to reduce risks related to changes and the risk of falling out of compliance.

7.2.1. New Device or Application Checklist

The change approver should verify that all items in the checklist are addressed in the implementation plan prior to granting approval to proceed. The change is considered complete only when all of the items in the checklist have been addressed.

A sample new device/application checklist is shown in Figure 8 below.

#	Item
1	Network diagram updated?
2	Secure baseline applied to device?
3	Asset/configuration inventory (CMDB) updated? IP address list, serial #, support contract info, business owner, custodian/support team, etc
4	Appropriate logging enabled, logs forwarded to central log management server?
5	Has it been determined what other devices or applications the new device/application will talk to and on what ports?
6	If unencrypted services, protocols or ports required have the compensating controls been identified, approved by senior management and implemented?
7	FW rule change required?
8	If FW rule change required then has the Approved list been updated and signed off?
9	Monitoring of new device and/or application in place?
10	Regular backup of device and/or application in place?
11	Procedures for restore from backup documented and tested?
12	Procedures for regular patching, application of signature updates (where appropriate) documented and tested?
13	Procedures for other maintenance activities, as required documented and tested?
14	Functional testing conducted as required?
15	Security testing conducted as required? VA scan, port scan, penetration test against new device/application and against firewall (if firewall changes implemented)

Figure 8. Sample New Device/Application Checklist.

© 2013 SANS Institute, Author retains full rights.

7.2.2. Decommissioned Device/Application Checklist

Change approval should depend on all items in the checklist being addressed in the decommissioning plan. The change is considered complete only when all of the items in the checklist have been addressed.

A sample decommissioned device/application checklist is illustrated in Figure 9 below.

#	Item
1	Network diagram updated?
2	Information flow documentation updated?
3	Asset/configuration inventory (CMDB) updated? Mark device/application as decommissioned
4	Centralized log mgmt. system updated to no longer collect log data from decommissioned device and/or application? Disable log collection for decommissioned device and/or application (don't want log mgmt. system to alert on no log data from decommissioned device)
5	If services, protocols or ports used by the decommissioned devices or applications are no longer required then has the Approved list been updated and signed off?
6	If services, protocols or ports no longer required, have the applicable updated secure baseline configurations been updated (disable unrequired services, protocols and ports)?
7	Has the updated secure baseline configuration been applied to all applicable systems?
8	FW rule change required? Remove rule entries related to any services, protocols or ports which are no longer required
9	Device/application removed from regular backups?
10	Security testing conducted as required? VA scan, device scan, port scan

Figure 9. Sample decommissioned device/application checklist.

© 2013 SANS Institute. Author retains full rights.

7.3. Vulnerability Management

The organization must ensure that processes/procedures are in place to track vulnerabilities related to firewalls. Vendor and industry advisories should be monitored regularly and procedures should be in place to ensure patches and/or workaround are implemented promptly.

The vulnerability management process should include updating of the standard configuration for the firewall with all identified patches/remediation and the updated configuration must be applied to all applicable firewalls. PCI requirement 6.1 states that critical patches are applied within one month of release by vendor.

7.4. Continual Improvement

As firewall reviews must be conducted at least every six months, it is beneficial to review the firewall review process itself. The objectives of reviewing the firewall review process are to fine tune the process and identify mechanisms to reduce the effort required to complete firewall reviews.

When reviewing the firewall review process, identify what is working well as well as problematic areas. For problematic areas identify recommendations for improvement.

Areas for improvement could include reducing effort required to complete reviews or addressing non-compliance with or gaps in organizational processes (e.g. change management, maintenance of standard configurations, vulnerability and patch management).

If it is determined that firewall configuration and rule set reviews require significant effort then procurement of commercial tools to analyze firewall rule sets or for reviewing configurations (e.g. CIS benchmark tools) could be justified by the organization.

A review of the process should include investigation of recurring issues indicating such as network diagrams not current or unapproved services, protocols or ports in use which may indicate gaps in processes or non-compliance with processes. For all identified recurring issues, the root cause should be addressed.

© 2013 SANS Institute, Author retains full rights.

8. Conclusion

For PCI compliance, the key objectives with respect to firewalls is to ensure that "Approved" equals "Actual" (where "Approved" includes all applicable policies, documented standards and other directives from senior management). The methodology laid out in this document enables organizations to get to and maintain compliance across a number of PCI requirements while reducing ongoing effort. It also provides to senior management a measurable assurance of firewall compliance. Keeping the infrastructure as close to "actual = approved" as possible at all times lowers the cost of ongoing compliance. Periodic firewall reviews along with good change and vulnerability management enables the organization to keep firewalls in compliance at all times.

The initial firewall review will require significant effort but subsequent firewall reviews will require less effort as the business and compliance requirements are well understood and the procedures are established. A continual improvement methodology will help to further reduce the effort and number of instances of deficiencies indicating non-compliance over time.

© 2013 SANS Institute, Author retains full rights.

9. References

Chuvakin, Dr. Anton A. & Williams, Branden R.. *PCI Compliance Understand and Implement Effective PCI Data Security Standard Compliance*, Second Edition. Syngress (2010).

PCI Security Standards Council. *Payment Card Industry (PCI) Data Security Standard – Navigating PCI DSS – Understanding the Intent of the Requirements version 2.0*. PCI Security Standards Council (October 2010). https://www.pcisecuritystandards.org/

PCI Security Standards Council. *Payment Card Industry (PCI) Data Security Standard – Requirements and Security Assessment Procedures Version 2.0*. PCI Security Standards Council (October 2010). https://www.pcisecuritystandards.org/

Williams, Branden. *Data Flows Made Easy*. (March 2008). Retrieved January 26, 2013 from https://www.brandenwilliams.com/brwpubs/DataFlowsMadeEasy.pdf

© 2013 SANS Institute, Author retains full rights.

10. Appendix A: Firewall Rule Set Tips

10.1. Leverage Groups in Rule Sets

The firewall rule set should ensure only approved traffic is allowed through firewalls while at the same time maintaining a balance between tight rules and not impeding business. If rules are too tight then firewall rule sets have to be changed frequently, if too loose then actual may not equal approved (resulting in increased security risks in the infrastructure).

To minimize negative impact on the infrastructure while cleaning up the rule set, insert more restrictive rules before the rules that you want to replace. Leave the original rules in place. Then conduct the firewall rule set review again and pay particular attention to all traffic hitting the original rule. Verify whether the traffic hitting the original rule is required. If so then update the new rules (and the Approved List) to include the required traffic prior to removing the original rules.

Avoid, where possible, the use of "Permit any" in source, destination and services allowed through firewalls.

Define IP ranges or groups of devices. Some rules may apply to all devices in a network zone so define a device group with the IP subnet instead of individual devices. When new devices are added to the network zone then the firewall rule set does not need to be changed. Services groups are useful for identifying services which are related to a particular function.

Rules related to devices and services, protocols and ports which handle/transmit credit card data should be very tight. Identify specific devices rather than IP range – use device groups and service groups.

<u>Example</u>

Organization XYZ's network is configured as shown in Figure 10 below. There are two firewalls, the Internet facing FW and the internal firewall. The internal firewall has three interfaces: untrust, trust and mgmt.

© 2013 SANS Institute, Author retains full rights.

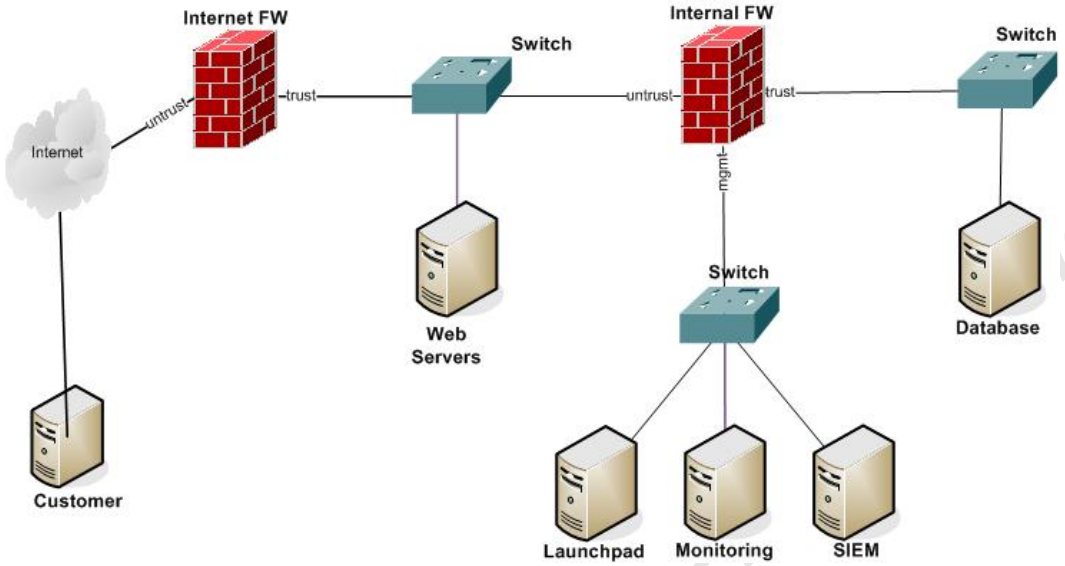

Figure 10. Organization XYZ - network diagram.

Internal Firewall Rule Set

Device Groups

Internal = 10.10.10.0/24
DMZ = 10.105.85.0/24
Management-devices =
172.50.10.1 # SNMP monitoring VIP
172.50.10.2 # SNMP monitoring Active
172.50.10.3 # SNMP monitoring Standby
172.50.10.30 # centralized syslog server (SIEM)
172.50.10.100 # launch pad active
172.50.10.101 # launch pad standby

Web-servers =
10.5.2.1
10.5.2.2
10.5.2.3

DB-servers =
10.6.56.1
10.6.56.2

Service Groups

management-services =
snmp get (161 udp)
snmp trap (162 udp)
ping (8 icmp)
ssh (22 tcp)
https (443 tcp)

web–DB =
Microsoft SQL (1433 tcp)

Rule Set

MGMT interface to Trust interface
Permit "Management-devices" to "Internal" service "management-services"

© 2013 SANS Institute. Author retains full rights.

Deny any to any service any

Untrust interface to MGMT interface
Permit "DMZ" to "Management-devices" service "management-services"
Deny any to any service any

Untrust to Trust
Permit "web servers" to "DB servers" service "web–DB"
Deny any to any service any

When you add a new device in the internal network or in the DMZ, you just have to add the device IP to the appropriate group to enable monitoring and log collection.

Internet Firewall Rule Set

Device Groups
DMZ = 10.105.85.0/24
web-servers =
10.5.2.1
10.5.2.2
10.5.2.3

Service Groups
web-services =
https (443 tcp)

Rule Set
Untrust to Trust
Permit any to "web-servers" service "web-services"
Deny any to any service any

Trust to Untrust
Deny any to any service any

When a new web server is added to the pool then only the device group "web-servers" needs to be modified – add 10.5.2.4 to the list.

© 2013 SANS Institute. Author retains full rights.

10.2. Avoid "any" in Rule Sets

It is important to avoid the use of "any" where possible in source, destination and services in firewall rules. Instead of "any" in source or destination, especially for internal networks, identify the specific IP addresses or, at minimum, the subnet range. This applies equally to both inbound and outbound traffic. The rule of thumb is anything not specifically allowed as per the Approved List is not permitted.

10.3. Use Iterative Approach to Modifying Rule Sets

To minimize negative impact on the business when tightening up rule sets, an iterative approach as described below is recommended.

Original rule: *Permit "management-devices" to "Internal" service any*

New rule: *Permit "Management-devices" to "Internal" service "management-services"*

For the first iteration, insert the new rule before the original rule in the access control list but do not remove the original rule. Monitor any traffic hitting the original rule and determine if there is a valid business requirement for that traffic. If so, then either modify the new rule or create another rule to specifically allow that traffic. If adding a new rule then make sure that the new rule is positioned before the original rule in the access control list. Again, monitor any traffic hitting the original rule.

Once it has been determined that either no traffic is hitting the original rule or the traffic that is hitting the original rule is unauthorized then remove the original rule from the rule set.

© 2013 SANS Institute. Author retains full rights.

11. Appendix B: Applicable PCI DSS Requirements

Excerpted from *Payment Card Industry (PCI) Data Security Standard –Navigating PCI DSS – Understanding the Intent of the Requirements version 2.0 9* (www.pcisecuritystandards.org/)

Review Activity	Section	PCI DSS Requirements	PCI DSS Guidance
Approved Services, Protocols and Ports List	**4.3**	**1.1.5** Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	Compromises often happen due to unused or insecure service and ports, since these often have known vulnerabilities—and many organizations are vulnerable to these types of compromises because they do not patch security vulnerabilities for services, protocols, and ports they don't use (even though the vulnerabilities are still present). Each organization should clearly decide which services, protocols, and ports are necessary for their business, document them for their records, and ensure that all other services, protocols, and ports and disabled or removed. Also, organizations should consider blocking all traffic and only re-opening those ports once a need has been determined and documented. Additionally, there are many services, protocols, or ports that a business may need (or have enabled by default) that are commonly used by malicious individuals to compromise a network. If these insecure services, protocols, or ports are necessary for business, the risk posed by use of these protocols should be clearly understood and accepted by the organization, the use of the protocol should be justified, and the security features that allow these protocols to be used securely should be documented and implemented. If these insecure services, protocols, or ports are not necessary for business, they should be disabled or removed.
Approved Services, Protocols and Ports List	**4.3**	**4.1** Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.	Sensitive information must be encrypted during transmission over public networks, because it is easy and common for a malicious individual to intercept and/or divert data while in transit. For example, Secure Sockets Layer (SSL) encrypts web pages and the data entered into them. When using SSL secured websites, ensure "https" is part of the URL. Note that some protocol implementations (such as SSL version 2.0 and SSH version 1.0) have documented vulnerabilities, such as buffer overflows, that an attacker can use to gain control of the affected system. Whichever security protocol is used, ensure it is configured to use only secure configurations and versions to prevent an insecure connection being used.
Network Diagram	**6.1**	**1.1.2** Current network diagram with all connections to cardholder data, including any wireless networks.	Network diagrams enable the organization to identify the location of all its network devices. Additionally, the network diagram can be used to map the data flow of cardholder data across the network and between individual devices in

© 2013 SANS Institute, Author retains full rights.

Review Activity	Section	PCI DSS Requirements	PCI DSS Guidance
			order to fully understand the scope of the cardholder data environment. Without current network and data flow diagrams, devices with cardholder data may be overlooked and may unknowingly be left out of the layered security controls implemented for PCI DSS and thus vulnerable to compromise. Network and data flow diagrams should include virtual system components and document Intra-host data flows.
Network Diagram **Standard Firewall Configuration -** ***Network Architecture***	**6.1** **6.3**	**1.1.3** Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.	Using a firewall on every connection coming into (and out of) the network allows the organization to monitor and control access in and out, and to minimize the chances of a malicious individual's obtaining access to the internal network.
Standard Firewall Configuration	**7.2**	**1.1** Establish firewall and router configuration standards that include the following:	Firewalls and routers are key components of the architecture that controls entry to and exit from the network. These devices are software or hardware devices that block unwanted access and manage authorized access into and out of the network. Without policies and procedures in place to document how staff should configure firewalls and routers, a business could easily lose its first line of defense in data-protection. The policies and procedures will help to ensure that the organization's first line of defense in the protection of its data remains strong. Virtual environments where data flows do not transit a physical network should be assessed to ensure appropriate network segmentation is achieved.
Standard Firewall Configuration	**6.3**	**2.2** Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: § Center for Internet Security (CIS) § International Organization for Standardization (ISO) § SysAdmin Audit Network Security (SANS) Institute § National Institute of Standards Technology (NIST)	There are known weaknesses with many operating systems, databases, and enterprise applications, and there are also known ways to configure these systems to fix security vulnerabilities. To help those that are not security experts, security organizations have established system-hardening recommendations, which advise how to correct these weaknesses. If systems are left with these weaknesses—for example, weak file settings or default services and protocols (for services or protocols that are often not needed)—an attacker will be able to use multiple, known exploits to attack vulnerable services and protocols, and thereby gain access to your organization's network. Source websites where you can learn more about industry best practices that can help you implement configuration standards include, but are not limited to: www.nist.gov, www.sans.org, www.cisecurity.org, www.iso.org. System configuration standards must also be kept up to date to ensure that newly identified weaknesses are corrected prior to a system being installed on the network.
Standard Firewall Configuration ***Version and Patch Level***	**6.3**	**6.1** Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches	There are a considerable amount of attacks using widely published exploits, often"0 day" (published within the hour) against otherwise secured systems. Without implementing the most recent patches on critical systems as soon as

© 2013 SANS Institute, Author retains full rights.

Review Activity	Section	PCI DSS Requirements	PCI DSS Guidance
Vulnerability Management	**7.3**	within one month of release. ***Note:*** *An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*	possible, a malicious individual can use these exploits to attack and disable the network. Consider prioritizing changes such that critical security patches on critical or at-risk systems can be installed within 30 days, and other less-risky changes are installed within 2-3 months.
Standard Firewall Configuration - ***Access Controls***	**6.3**	**2.1** Always change vendor-supplied defaults before installing a system on the network—including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	Malicious individuals (external and internal to a company) often use vendor default settings, account names, and passwords to compromise systems. These settings are well known in hacker communities and leave your system highly vulnerable to attack.
Standard Firewall Configuration - ***Access Controls***	**6.3**	**7.1** Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following: **7.1.1** Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities	The more people who have access to cardholder data, the more risk there is that a user's account will be used maliciously. Limiting access to those with a strong business reason for the access helps your organization prevent mishandling of cardholder data through inexperience or malice. When access rights are granted only to the least amount of data and privileges needed to perform a job, this is a called "least privilege" and "need to know," and when privileges are assigned to individuals based on job classification and function, this is called "role-based access control" or RBAC. Role based access control enforcement is not limited to an application layer or any specific authorization solution. For example, technology including but not limited to directory services such as Active Directory or LDAP, Access Control Lists (ACLs), and TACACS are viable solutions as long as they are appropriately configured to enforce the principles of least privilege and need to know. Organizations should create a clear policy and processes for data access control based on need to know and using role-based access control, to define how and to whom access is granted, including appropriate management authorization processes.
Standard Firewall Configuration - ***Access Controls***	**6.3**	**7.1.2** Assignment of privileges is based on individual personnel's job classification and function	Without a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data. Use of an automated access control system or mechanism is essential to manage multiple users. This system should be established in accordance with your organization's access control policy and processes (including "need to know" and "role-based access control"), should manage access to all system components, and should have a default "deny-all" setting to ensure no one is granted access until and unless a rule is established specifically granting such access.

© 2013 SANS Institute. Author retains full rights.

Review Activity	Section	PCI DSS Requirements	PCI DSS Guidance
Standard Firewall Configuration - ***Access Controls***	**6.3**	**8.1** Assign all users a unique username before allowing them to access system components or cardholder data.	By ensuring each user is uniquely identified—instead of using one ID for several employees—an organization can maintain individual responsibility for actions and an effective audit trail per employee. This will help speed issue resolution and containment when misuse or malicious intent occurs.
Standard Firewall Configuration - ***Active Services***	**6.3**	**2.2.2** Enable only necessary and secure services, protocols, daemons, etc. as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure.	As stated in Requirement 1.1.5, there are many protocols that a business may need (or have enabled by default) that are commonly used by malicious individuals to compromise a network. To ensure that only the necessary services and protocols are enabled and that all insecure services and protocols are adequately secured before new servers are deployed, this requirement should be part of your organization's configuration standards and related processes.
Standard Firewall Configuration - ***Active Services***	**6.3**	**2.3** Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	If remote administration is not done with secure authentication and encrypted communications, sensitive administrative or operational level information (like administrator's passwords) can be revealed to an eavesdropper. A malicious individual could use this information to access the network, become administrator, and steal data.
Standard Firewall Configuration - ***Active Services***	**6.3**	**8.4** Render all passwords unreadable during transmission and storage on all system components using strong cryptography.	Many network devices and applications transmit the user ID and unencrypted password across the network and/or also store the passwords without encryption. A malicious individual can easily intercept the unencrypted or readable user ID and password during transmission using a "sniffer," or directly access the user IDs and unencrypted passwords in files where they are stored, and use this stolen data to gain unauthorized access. During transmission, the user credentials can be encrypted or the tunnel can be encrypted.
Standard Firewall Configuration - ***Audit Trails***	**6.3**	**10.2** Implement automated audit trails for all system components to reconstruct the following events: **10.2.2** All actions taken by any individual with root or administrative privileges **10.2.3** Access to all audit trails **10.2.4** Invalid logical access attempts **10.2 5** Use of identification and authentication mechanisms **10.2.6** Initialization of the audit logs	Generating audit trails of suspect activities alerts the system administrator, sends data to other monitoring mechanisms (like intrusion detection systems), and provides a history trail for post-incident follow-up. Logging of the following events enables an organization to identify and trace potentially malicious activities. Accounts with increased privileges, such as the "administrator" or "root" account, have the potential to greatly impact the security or operational functionality of a system. Without a log of the activities performed, an organization is unable to trace any issues resulting from an administrative mistake or misuse of privilege back to the specific action and individual. Malicious users often attempt to alter audit logs to hide their actions, and a record of access allows an organization to trace any inconsistencies or potential tampering of the logs to an individual account. Malicious individuals will often perform multiple access attempts on targeted systems. Multiple invalid login attempts may be an

© 2013 SANS Institute, Author retains full rights.

Review Activity	Section	PCI DSS Requirements	PCI DSS Guidance
			indication of an unauthorized user's attempts to "brute force" or guess a password. Without knowing who was logged on at the time of an incident, it is impossible to identify the accounts which may be used. Additionally, malicious users may attempt to manipulate the authentication controls with the intent of bypassing them or impersonating a valid account. Activities including, but not limited to, escalation of privilege or changes to access permissions may indicate unauthorized use of a system's authentication mechanisms. Turning the audit logs off prior to performing illicit activities is a common goal for malicious users wishing to avoid detection. Initialization of audit logs could indicate that the log function was disabled by a user to hide their actions.
Standard Firewall Configuration - ***Disclosure of Private IP Addresses***	**6.3**	**1.3.8** Do not disclose private IP addresses and routing information to unauthorized parties Note: Methods to obscure IP addressing may include, but are not limited to: § Network Address Translation (NAT) § Placing servers containing cardholder data behind proxy servers/firewalls or content caches, § Removal or filtering of route advertisements for private networks that employ registered addressing, § Internal use of RFC1918 address space instead of registered addresses.	Restricting the broadcast of IP addresses is essential to prevent a hacker "learning" the IP addresses of the internal network, and using that information to access the network. Effective means to meet the intent of this requirement may vary depending on the specific networking technology being used in your environment. For example, the controls used to meet this requirement may be different for IPv4 networks than for IPv6 networks. One technique to prevent IP address information from being discovered on an IPv4 network is to implement Network Address translation (NAT). NAT, which is typically managed by the firewall, allows an organization to have internal addresses that are visible only inside the network and external address that are visible externally. If a firewall does not "hide" or mask the IP addresses of the internal network, a malicious individual could discover internal IP addresses and attempt to access the network with a spoofed IP address. For IPv4 networks, the RFC1918 address space is reserved for internal addressing, and should not be routable on the Internet. As such, it is preferred for IP addressing of internal networks. However, organizations may have reasons to utilize non-RFC1918 address space on the internal network. In these circumstances, prevention of route advertisement or other techniques should be used to prevent internal address space being broadcast on the Internet or disclosed to unauthorized parties.
Standard Firewall Configuration - ***Stateful Inspection***	**6.3**	**1.3.6** Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)	A firewall that performs stateful packet inspection keeps "state" (or the status) for each connection to the firewall. By keeping "state," the firewall knows whether what appears to be a response to a previous connection is truly a response (since it "remembers" the previous connection) or is a malicious individual or software trying to spoof or trick the firewall into allowing the connection.

© 2013 SANS Institute, Author retains full rights.

Review Activity	Section	PCI DSS Requirements	PCI DSS Guidance
Standard Firewall Configuration - *Time Synchronization*	**6.3**	**10.4** Using time synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. **10.4.1** Critical systems have the correct and consistent time. **10.4.2** Time data is protected. **10.4.3** Time settings are received from industry-accepted time sources	Time synchronization technology is used to synchronize clocks on multiple systems. When properly deployed, this technology can synchronize clocks on large numbers of systems to within a fraction of a second of each other. Some problems that can occur when clocks are not properly synchronized include but are not limited to, making it difficult if not impossible to compare log files from different systems and establish an exact sequence of event (crucial for forensic analysis in the event of a breach), and preventing cryptographic protocols such as SSH that rely on absolute time from functioning properly. For post-incident forensics teams, the accuracy and consistency of time across all systems and the time of each activity is critical in determining how the systems were compromised. In order to ensure consistent time, ideally there should be only a few internal (central) time servers within an entity. These servers receive UTC (Coordinated Universal Time) data directly from reliable, known external time servers, via special radio, GPS satellites, or other external network source, and peer with each other to ensure they keep accurate time. Other systems then receive the time from these servers. If a malicious individual has entered the network, they will often attempt to change the time stamps of their actions within the audit logs to prevent detection of their activity. A malicious individual may also try to directly change the clock on a system component to hide their presence – for example, by changing the system clock to an earlier time. For these reasons, it is important that time is accurate on all systems and that time data is protected against unauthorized access and changes. Time data includes the parameters and methods used to set each system's clock. More information on NTP can be found at www.ntp.org, including information about time, time standards, and servers.
Firewall Rule Sets	**6.4**	**1.2** Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	It is essential to install network protection, namely a system component with (at a minimum) stateful inspection firewall capability, between the internal, trusted network and any other untrusted network that is external and/or out of the entity's ability to control or manage. Failure to implement this measure correctly means that the entity will be vulnerable to unauthorized access by malicious individuals or software. If firewall functionality is installed but does not have rules that control or limit certain traffic, malicious individuals may still be able to exploit vulnerable protocols and ports to attack your network.
Firewall Rule Sets	**6.4**	**1.2.1** Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.	This requirement is intended to prevent malicious individuals from accessing the organization's network via unauthorized IP

© 2013 SANS Institute, Author retains full rights.

Review Activity	Section	PCI DSS Requirements	PCI DSS Guidance
			addresses or from using services, protocols, or ports in an unauthorized manner (for example, to send data they've obtained from within your network out to an untrusted server. All firewalls should include a rule that denies all inbound and outbound traffic not specifically needed. This will prevent inadvertent holes that would allow other, unintended and potentially harmful traffic in or out.
Firewall Rule Sets	**6.4**	**1.2.3** Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	The known (or unknown) implementation and exploitation of wireless technology within a network is a common path for malicious individuals to gain access to the network and cardholder data. If a wireless device or network is installed without a company's knowledge, a malicious individual could easily and "invisibly" enter the network. If firewalls do not restrict access from wireless networks into the payment card environment, malicious individuals that gain unauthorized access to the wireless network can easily connect to the payment card environment and compromise account information. Firewalls must be installed between all wireless networks and the CDE, regardless of the purpose of the environment to which the wireless network is connected. This may include, but is not limited to, corporate networks, retail stores, warehouse environments, etc.
Firewall Rule Sets	**6.4**	**1.3** Prohibit direct public access between the Internet and any system component in the cardholder data environment.	A firewall's intent is to manage and control all connections between public systems and internal systems (especially those that store, process or transmit cardholder data). If direct access is allowed between public systems and the CDE, the protections offered by the firewall are bypassed, and system components storing cardholder data may be exposed to compromise.
Firewall Rule Sets	**6.4**	**1.3.1** Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	The DMZ is that part of the network that manages connections between the Internet (or other untrusted networks), and internal services that an organization needs to have available to the public (like a web server). It is the first line of defense in isolating and separating traffic that needs to communicate with the internal network from traffic that does not. This functionality is intended to prevent malicious individuals from accessing the organization's network via unauthorized IP addresses or from using services, protocols, or ports in an unauthorized manner.
Firewall Rule Sets	**6.4**	**1.3.2** Limit inbound Internet traffic to IP addresses within the DMZ.	Termination of IP connections at the DMZ provides opportunity for inspection and restriction of source/destination, and/or inspection / blocking of content, thus preventing unfiltered access between untrusted and trusted environments.
Firewall Rule Sets	**6.4**	**1.3.3** Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.	Termination of IP connections both inbound and outbound provides opportunity for inspection and restriction of source/destination, and/or inspection / blocking of content, thus preventing

© 2013 SANS Institute, Author retains full rights.

Review Activity	Section	PCI DSS Requirements	PCI DSS Guidance
			unfiltered access between untrusted and trusted environments. This helps prevent, for example, malicious individuals from sending data they've obtained from within your network out to an external untrusted server in an untrusted network.
Firewall Rule Sets	**6.4**	**1.3.4** Do not allow internal addresses to pass from the Internet into the DMZ.	Normally a packet contains the IP address of the computer that originally sent it. This allows other computers in the network to know where it came from. In certain cases, this sending IP address will be spoofed by malicious individuals. For example, malicious individuals send a packet with a spoofed address, so that (unless your firewall prohibits it) the packet will be able to come into your network from the Internet, looking like it is internal, and therefore legitimate, traffic. Once the malicious individual is inside your network, they can begin to compromise your systems. Ingress filtering is a technique you can use on your firewall to filter packets coming into your network to, among other things, ensure packets are not "spoofed" to look like they are coming from your own internal network. For more information on packet filtering, consider obtaining information on a corollary technique called "egress filtering."
Firewall Rule Sets	**6.4**	**1.3.5** Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	All traffic outbound from inside the cardholder data environment should be evaluated to ensure that outbound traffic follows established, authorized rules. Connections should be inspected to restrict traffic to only authorized communications (for example by restricting source/destination addresses/ports, and/or blocking of content). Where environments have no inbound connectivity allowed, outbound connections may be achieved via architectures or system components that interrupt and inspect the IP connectivity.
Periodic Firewall Reviews	**7.1**	**1.1.6** Requirement to review firewall and router rule sets at least every six months.	This review gives the organization an opportunity at least every six months to clean up any unneeded, outdated, or incorrect rules, and ensure that all rule sets allow only authorized services and ports that match business justifications. It is advisable to undertake these reviews on a more frequent basis, such as monthly, to ensure that the rule sets are current and match the needs of the business without opening security holes and running unnecessary risks.
Change Management	**7.2**	**1.1.1** A formal process for approving and testing all network connections and changes to the firewall and router configurations	A policy and process for approving and testing all connections and changes to the firewalls and routers will help prevent security problems caused by misconfiguration of the network, router, or firewall. Data flows between virtual machines should be included in policy and process.
Change Management	**7.2**	**11.2.3** Perform internal and external scans after any significant change.	Scanning an environment after any significant changes are made ensures that changes were

© 2013 SANS Institute, Author retains full rights.

Review Activity	Section	PCI DSS Requirements	PCI DSS Guidance
		Note: *Scans conducted after changes may be performed by int*ernal staff.	completed appropriately such that the security of the environment was not compromised as a result of the change. It may not be necessary to scan the entire environment after a change. However, all system components affected by the change will need to be scanned.
Change Management **Vulnerability Management**	**7.2** **7.3**	**11.3** Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following: **11.3.1** Network-layer penetration tests **11.3.2** Application-layer penetration tests	The intent of a penetration test is to simulate a real world attack situation with a goal of identifying how far an attacker would be able to penetrate into an environment. This allows an entity to gain a better understanding of their potential exposure and develop a strategy to defend against attacks. A penetration test differs from a vulnerability scan, as a penetration test is an active process which may include exploiting identified vulnerabilities. Often, performing a vulnerability scan is one of the first steps a penetration tester will perform in order to comprise a strategy of attack, although it is not the only step. Even if a vulnerability scan does not detect any known vulnerabilities, the penetration tester will often gain enough knowledge about the system to identify possible security gaps. Penetration testing is generally a highly manual process. While some automated tools may be used, the tester must utilize their knowledge of systems to penetrate into an environment. Often the tester will chain several types of exploits together with a goal of breaking through layers of defenses. For example, if the tester finds a means to gain access to an application server, they will then use the compromised server as a point to stage a new attack based on the resources the server has access to. In this way a tester is able to simulate the methods performed by an attacker in order to identify any areas of potential weakness in the environment that need to be addressed.
Vulnerability Management	**7.3**	**11.2** Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). **11.2.1** Perform quarterly internal vulnerability scans.	**11.2** Verify that internal and external vulnerability scans are performed as follows: **11.2.1.a** Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period. **11.2.1.b** Review the scan reports and verify that the scan process includes rescans until passing results are obtained, or all ―High‖ vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved. **11.2.1.c** Validate that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).
Vulnerability Management	**7.3**	**11.2.2** Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC).	**11.2.2.a** Review output from the four most recent quarters of external vulnerability scans and verify that four quarterly scans occurred in the most recent 12-month period. **11.2.2.b** Review the results of each quarterly scan to ensure that they satisfy the ASV Program Guide requirements (for example, no

© 2015 SANS Institute, Author retains full rights

Review Activity	Section	PCI DSS Requirements	PCI DSS Guidance
			vulnerabilities rated higher than a 4.0 by the CVSS and no automatic failures). **11.2.2.c** Review the scan reports to verify that the scans were completed by an Approved Scanning Vendor (ASV), approved by the PCI SSC.

© 2013 SANS Institute. Author retains full rights

Last Updated: October 21st, 2016

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS San Diego 2016	San Diego, CAUS	Oct 23, 2016 - Oct 28, 2016	Live Event
SANS FOR508 Hamburg in German	Hamburg, DE	Oct 24, 2016 - Oct 29, 2016	Live Event
SOS SANS October Singapore 2016	Singapore, SG	Oct 24, 2016 - Nov 06, 2016	Live Event
SANS Munich Autumn 2016	Munich, DE	Oct 24, 2016 - Oct 29, 2016	Live Event
Pen Test HackFest Summit & Training	Crystal City, VAUS	Nov 02, 2016 - Nov 09, 2016	Live Event
SANS Sydney 2016	Sydney, AU	Nov 03, 2016 - Nov 19, 2016	Live Event
SANS Gulf Region 2016	Dubai, AE	Nov 05, 2016 - Nov 17, 2016	Live Event
SANS Miami 2016	Miami, FLUS	Nov 07, 2016 - Nov 12, 2016	Live Event
DEV534: Secure DevOps	Nashville, TNUS	Nov 07, 2016 - Nov 08, 2016	Live Event
European Security Awareness Summit	London, GB	Nov 09, 2016 - Nov 11, 2016	Live Event
DEV531: Defending Mobile Apps	Nashville, TNUS	Nov 09, 2016 - Nov 10, 2016	Live Event
SANS London 2016	London, GB	Nov 12, 2016 - Nov 21, 2016	Live Event
Healthcare CyberSecurity Summit & Training	Houston, TXUS	Nov 14, 2016 - Nov 21, 2016	Live Event
SANS San Francisco 2016	San Francisco, CAUS	Nov 27, 2016 - Dec 02, 2016	Live Event
SANS Hyderabad 2016	Hyderabad, IN	Nov 28, 2016 - Dec 10, 2016	Live Event
MGT517 - Managing Security Ops	Washington, DCUS	Nov 28, 2016 - Dec 02, 2016	Live Event
ICS410 @ Delhi	New Delhi, IN	Dec 05, 2016 - Dec 09, 2016	Live Event
SANS Cologne	Cologne, DE	Dec 05, 2016 - Dec 10, 2016	Live Event
SEC560 @ SANS Seoul 2016	Seoul, KR	Dec 05, 2016 - Dec 10, 2016	Live Event
SANS Dublin	Dublin, IE	Dec 05, 2016 - Dec 10, 2016	Live Event
SANS Cyber Defense Initiative 2016	Washington, DCUS	Dec 10, 2016 - Dec 17, 2016	Live Event
SANS Frankfurt 2016	Frankfurt, DE	Dec 12, 2016 - Dec 17, 2016	Live Event
SANS Amsterdam 2016	Amsterdam, NL	Dec 12, 2016 - Dec 17, 2016	Live Event
SANS Security East 2017	New Orleans, LAUS	Jan 09, 2017 - Jan 14, 2017	Live Event
SANS Brussels Winter 2017	Brussels, BE	Jan 16, 2017 - Jan 21, 2017	Live Event
Cloud Security Summit	San Francisco, CAUS	Jan 17, 2017 - Jan 19, 2017	Live Event
SANS Tysons Corner 2016	OnlineVAUS	Oct 22, 2016 - Oct 29, 2016	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced