



PCI Compliance Audit Using Athena FirePac

“Build and Maintain a Secure network” is the first of six PCI DSS control objectives, and perhaps the hardest to audit, because it involves auditing large rule-bases in the boundary firewalls of the enterprise network. It is estimated that each firewall rule-base needs, on the average, 15 person days to audit. With 15, 50 or even 200 firewalls in an enterprise, it is easy to see the time and expense involved to gain a sufficient understanding of the exposures inherent in these devices.

Athena FirePac’s technological innovation, firewall *policy computation*, is a new approach to the problem of analyzing a firewall rule-base. Firewalls are increasingly configured so companies can do more with less. While this allows for more value to be extracted from existing IT investments, analysis also becomes complicated. The combined effect of VPN’s, complex objects, natted sources and complex rulesets make it difficult to identify policy risks. FirePAC makes the behavior of the firewall explicit, eliminating the guesswork (or need for specialized technical skill), to achieve consistent and accurate audit results.

FirePac runs off-line, so you are not running or doing anything that could potentially harm the network. The analysis is presented in easy to understand formatted reports that include summary and policy detail.

- It eliminates manual analysis of rule-bases.
- It eliminates the need for log analysis
- It reduces the need for extensive pen testing in gauging application vulnerabilities.
- There is no connection to a firewall necessary- thus no permissions, passwords, etc., required, and no injection of packets into the network.

FirePac has proven to reduce over 75% of the manual effort required to perform a thorough firewall audit. Even the most complex firewalls, with hundreds or even thousands of rules, take no more than hours to complete. The cost for a perpetual FirePAC license pays for itself in a single day.

To complete your PCI compliance audit using FirePac, use our 11-page guide to address the control items related to firewalls. Here is a summary of what FirePac covers:

PCI Requirement or Control item	FirePac support
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	

1.2 Establish firewall and router configuration standards that include the following:	
1.1.1. <u>A formal process for approving and testing all network connections and changes to the firewall and router configurations</u>	√
1.1.2. <u>A current network diagram with all connections to cardholder data, including any wireless networks</u>	√
1.1.3. Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	X
1.1.4. Description of groups, roles, and responsibilities for logical management of network components	X
1.1.5. <u>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.</u>	
1.1.5.a. Verify that firewall and router configuration standards include a documented list of services, protocols and ports necessary for business—for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols.	√
1.1.5.b Identify insecure services, protocols, and ports allowed; and verify they are necessary and that security features are documented and implemented by examining firewall and router configuration standards and settings for each service. An example of an insecure service, protocol, or port is FTP, which passes user credentials in clear-text.	√
1.1.6. <u>Requirement to review firewall and router rule sets at least every six months</u>	
1.1.6.a Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months.	√
1.1.6.b Obtain and examine documentation to verify that the rule sets are reviewed at least every six months.	√
1.2 Build a firewall configuration that restricts connections between un-trusted networks and any system components in the cardholder data environment.	
1.2.1. <u>Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.</u>	

1.2.1.a	Verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment, and that the restrictions are documented.	√
1.2.1.b	Verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit “deny all” or an implicit deny after allow statement.	√
1.2.2.	Secure and synchronize router configuration files.	
1.2.3.	<u>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.</u>	√
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	
1.3.1	<u>Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.</u>	√
1.3.2	<u>Limit inbound Internet traffic to IP addresses within the DMZ.</u>	√
1.3.3	<u>Do not allow any direct routes inbound or outbound for traffic between the Internet and the cardholder data environment.</u>	√
1.3.4	<u>Do not allow internal addresses to pass from the Internet into the DMZ.</u>	√
1.3.5	<u>Restrict outbound traffic from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ.</u>	√
1.3.6	Implement stateful inspection, also known as dynamic packet filtering. (That is, only “established” connections are allowed into the network.)	X
1.3.7	<u>Place the database in an internal network zone, segregated from the DMZ.</u>	√
1.3.8	<u>Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet, using RFC 1918 address space. Use network address translation (NAT) technologies—for example, port address translation (PAT).</u>	√
1.4	Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access	

the organization's network.	
1.4.b <i>Verify that mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), and which are used to access the organization's network, have personal firewall software installed and active.</i>	X
1.4.b <i>Verify that the personal firewall software is configured by the organization to specific standards and is not alterable by mobile computer users.</i>	X
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	
2.1 Always change vendor-supplied defaults before installing a system on the network --for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	
2.1.1 <i>For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.</i>	X
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.	
2.2.a <i>Examine the organization's system configuration standards for all types of system components and verify the system configuration standards are consistent with industry accepted hardening standards—for example, SysAdmin Audit Network Security (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).</i>	X
2.2.b <i>Verify that system configuration standards include each item below (at 2.2.1 – 2.2.4).</i>	X
2.2.c <i>Verify that system configuration standards are applied when new systems are configured.</i>	X
2.2.1 <u>Implement only one primary function per server.</u>	√

2.2.2	<u>Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the device's specified function).</u>	√
2.2.3	Configure system security parameters to prevent misuse.	
	2.2.3.a Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for system components.	X
	2.2.3.b Verify that common security parameter settings are included in the system configuration standards.	X
	2.2.3.c For a sample of system components, verify that common security parameters are set appropriately	X
2.2.4	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	X
2.3	<u>Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.</u>	√
2.4	Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.	X

Guide to Using AthenaFirePac in a PCI Compliance Audit

The Payment Card Industry (PCI) Data Security Standard (DSS), version 1.1, consists of 6 “control objectives” and 12 requirements. The objectives and requirements are:

1. Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

2. Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

3. Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

4. Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

5. Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

6. Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

In this technical brief we will discuss how FirePac can be used to satisfy PCI requirements in Control Objectives 1,2 and 11.

1 Collect data on the network for a PCI compliance audit

Start the audit by getting to know the customer's network at a very high level. Key information that is needed:

1. The access points to the network:
 - a. Border firewalls
 - b. Border routers
 - c. Wireless access points
 - d. Third party access points
2. Data storage in the network:
 - a. Is sensitive/credit card data stored in the network
 - b. Is there sensitive archival data
 - c. Is third party storage used for credit card data
3. Data access policies:
 - a. Access/login policies

2 Use FirePac reports generated on each firewall to flesh out the network

Run FirePac on each of the firewalls in the network and generate the following reports:

FirePAC Policy Analysis Summary Report

FirePAC Policy Analysis Detail Report

FirePAC Policy Analysis with Rule Trails Report

FirePAC Policy Comparison Report

View the **Firewall Connectivity** section of the **Policy Analysis Summary Analysis** report, and observe subnets identified as belonging to three zones – DMZ, External, and Internal. The reachable network segments for each zone are listed. This means that there are rules in the firewall configuration that allow packets to these network segments.

Besides manual specification, Firepac makes a best guess of which firewall interfaces correspond to which zone, using the following rules:

- For Cisco PIX firewalls, interfaces are marked internal or external interfaces based on security level. The remainder are marked DMZ.
- For Checkpoint firewalls, some interfaces are marked in the configuration.
- For Juniper Netscreen, zone references are used to map interfaces.

These mappings can be modified, so you may want to re-run the report if you need to alter an interface's zone identification.

Views the list of point-to-point Ipsec VPN's in the **Ipsec VPN Tunnels** section. These are the VPN's that allow traffic to remote sites through the firewall. Identify the remote sites and ascertain their current business purpose.

At this point having mapped all internal, DMZ, and remote networks accessible from all the firewalls, the next step is to associate key applications with some of the network segments. These could be application and database servers or those that offer network services such as mail, dns/dhcp, and AAA services.

Use the **Policies Passing Through Firewall** section of the report to look at the services available at a specific internal or DMZ interface. Use this information to validate the overall information on the network that has been gathered. The validation checks that can be made are:

- Zone assigned to a network segment is consistent across all firewalls in the network.
e.g. A network segment reachable from an interface assigned the zone DMZ, should be reachable, if ever, only from DMZ interfaces on other firewalls.
- Services available through an interface are compatible with application servers on networks reachable through the interface.
- VPN tunnels listed in the IPSEC VPN tunnels tables support services consistent with business need.

Inconsistencies may arise due to incorrect data that has been gathered or may point to a problem in the network that can amount to a potential security exposure.

We can now go ahead and generate the **Firewall policy detail** report for each firewall. This provides a breakdown of the **Policies Passing through a Firewall** table (from the summary report) listing individual sources and destinations that were not included in the summary.

We need to understand what each entry in this report portends and how it applies to PCI compliance. Each entry in the **Policies for <firewall name> as Pass-through** section of the report displays a policy that the firewall does **not** block. Thus, *the policy's existence is due to a perceived business need (that has or must have been documented) or is an exposure that indicates non-compliance.*

3 Applying the data generated to PCI requirements.

PCI control objective: Build and maintain a secure network

The first of the two requirements,

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

has several sub-sections with individual control items. We will describe how FirePac can be used to check individual control items for compliance.

CO 1.1 Establish firewall and router configuration standards that include the following:

CO 1.1.1 A formal process for approving and testing all external network connections and changes to the firewall and router configurations

A corporate change management policy should be in place for compliance, but AthenaFirepac provides the crucial testing step at the end of the process, using its **Policy Comparison Report** feature. This feature can take a “before” and “after” set of configurations and highlight the new services allowed, and existing services denied, as a result of changes in the configuration. The report, generated whenever a change is made, creates a documented change history.

CO 1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks

- a. *Verify that a current network diagram (for example, one that shows cardholder data flows over the network) exists and that it documents all connections to cardholder data, including any wireless network.*

Our AthenaVerify product can create a topology of the entire network that can satisfy this requirement. A layer-3 network diagram can be approximated, at least in its Public access policies, using FirePac on all the firewalls in the network.

- b. *Verify that the diagram is kept current.*

The network diagram created in our AthenaVerify product can be kept current.

- CO 1.1.3 *Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone*

This has to be checked manually.

- CO 1.1.4 *Description of groups, roles, and responsibilities for logical management of network components*

This has to be checked manually

- CO 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.*

- a. *Verify that firewall and router configuration standards include a documented list of services, protocols and ports necessary for business—for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols.*

- b. *Identify insecure services, protocols, and ports allowed; and verify they are necessary and that security features are documented and implemented by examining firewall and router configuration standards and settings for each service. An example of an insecure service, protocol, or port is FTP, which passes user credentials in clear-text.*

Use the *Policies Passing Through Firewall* table from the *FirePac Policy Summary report* to list all the services corresponding to exit interfaces that are INTERNAL or DMZ. Choose the exit interface to be DMZ or Internal for services entering the network. Similarly choose DMZ or Public interfaces for services allowed from the network. The Firewall Connectivity table provides a list of interfaces and the zones to which they are assigned.

The IPSec VPN Tunnels section of the report lists all the VPN's tunnels that are allowed through this firewall.

To identify insecure protocols and associated ports, use the *Firewall Policy Detail for <firewall_name> report*, which lists the exit interface, source and destination addresses, and service (protocol/port number).

For each service other than HTTP, SSL, SSH, and IPSEC, use the Policy Detail report to identify the internal and external sub-nets that use the protocol. Some, such as ICMP services, can be justified based on corporate policy. Others, such as IPSEC, need to be justified based on a particular feature that they enable, and this may be restricted to a subnet. Document the need for these services based on the business application that uses the service, identifiable through the service and subnet addresses.

CO 1.1.6 *Requirements to review firewall and router rule sets at least every six months.*

a. Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months

b. Obtain and examine documentation to verify that rule sets are reviewed at least every six months

The four reports generated by FirePac:

FirePAC Reports

FirePAC Policy Summary Report

FirePAC Policy Detail Report

FirePAC Policy Analysis with Rule Trails Report

FirePAC Policy Comparison Report

constitute a formal set of documents for review of a firewall or router rule sets, every six months.

CO 1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.

- CO 1.2.1 *Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.*
- a. *Verify that inbound traffic is limited to that which is necessary for the cardholder data environment, and that restrictions are documented.*
 - b. *Verify that all other inbound and outbound traffic is specifically denied, for example, by using an explicit “deny all” or implicit deny after allow statements.*

Collect the list of external source and destination addresses from the *Firewall Connectivity* section of the *Firewall Summary* report, and classify them into **trusted** and **untrusted** sources.

Generate a *Firewall Policy Detail* report for each **untrusted** host first as source, and then as destination. Based on the protocols that connect them to internal or DMZ networks, find a business reason for the existence of each policy in the report.

The *Findings* section of the *Firewall Summary* report identifies whether all other inbound or outbound traffic is denied by the use of an explicit or implicit “deny all” statement.

- CO 1.2.2 *Secure and synchronize router configuration files.*
This has to be performed manually

- CO 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.*

Analyze the perimeter firewall between the wireless network and the cardholder data environment using FirePac. Use the *Firewall Summary* report to identify whether any traffic is allowed to the cardholder data environment. If so, use the *FirePAC Policy Detail* report to identify all the services, if any, between the wireless network and the cardholder environment.

Use the *FirePac Policy Analysis with Rule Trails* report to identify the firewall rules associated with the allow policy. Modify the rules, and rerun FirePac on the modified configuration. Use the *FirePAC Policy Comparison Report* to compare the before and after policies between the wireless and cardholder data environment.

- CO 1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

- CO 1.3.1 *Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.*

Identify the interfaces in the firewall that that allow traffic to the cardholder data networks, and DMZ networks, using the *Firewall Connectivity* table of the *Firewall Summary* report. Use *Policies for <firewall-name> as pass-through* table in the *Firewall Policy Detail* report to identify all services destined for the cardholder environment networks. Ensure that these services are necessary, and that they originate in an interface connected to an interface identified as being in the DMZ zone.

- CO 1.3.2 *Limit inbound Internet traffic to IP addresses within the DMZ.*

This is essentially a check on whether the firewall configuration allows any traffic into the network from the public networks, other than to the DMZ.

The *Policies Passing Through Firewall* table in the *FirePac Summary* report provides information on all traffic between the Internet and the DMZ and Internal networks. Ensure that the policy between the Internet and the Internal networks is that everything is denied.

- CO 1.3.3 *Do not allow any direct routes inbound or outbound for traffic between the Internet and the cardholder environment*

The *Policies for <firewall-name> as pass-through* table in the *Firewall Detail Analysis* report provides information on all inbound/outbound traffic from/to the Internet that passes through the firewall. Identify if any of those policies has as a cardholder data network as source or destination.

- CO 1.3.4 *Do not allow internal addresses to pass from the Internet into the DMZ*

This is essentially a check on whether the firewall configuration has an anti-spoofing rule. The *Findings* section of the *Firewall Summary* report will report on anti-spoofing in the firewall.

- CO 1.3.5 *Restrict outbound traffic from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ*

This requires specific source and destination information that can be found by generating a *Firewall Policy Detail* report with the cardholder data environment as destination, and later as source. For each such policy in the report, verify that there is a business need. For those policies, that cannot be justified, generate a *Firewall Policy Analysis with Rule Trails* report that specifies configuration rules* that need to be modified.

*The actual rules (for Checkpoint, it is a vendor view) in the configuration are specified at the back of the report.

CO 1.3.6 *Securing and synchronizing router configuration files*
This needs to be performed manually.

CO 1.3.7 *Implement stateful inspection, also known as dynamic packet filtering. (That is, only “established” connections are allowed into the network)*

Most firewalls, including Cisco PIX, ASA, Juniper Netscreen, Nokia IPSO, and Checkpoint NGX are stateful.

CO 1.3.8 *Implement IP address masquerading to prevent internal addresses from being translated and revealed on the Internet using RFC 198 address space. Use network translation technologies (NAT)—for example, port address translation (PAT).*

The FirePAC Policy Analysis Summary Report provides a list of internal network segments that are accessible from the outside and the DMZ. Routable addresses may be identified in this list. If the list is small, then the *Firewall Policy Analysis with Rule Trails* report can be generated for these few addresses, and the rule trails individually examined for natting. This quickly becomes tedious for a larger number of routable addresses.

CO 1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization’s network.

a. *Verify that mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), and which are used to access the organizations network, have personal firewall software installed and active.*

This needs to be performed manually

- b. *Verify that the personal firewall software is configured by the organization to specific standards and is not alterable by mobile computer users.*

This needs to be performed manually.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

CO 2.1 Always change vendor-supplied defaults before installing a system on the network (for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts).

- CO 2.1.1 *For wireless environments, change wireless vendor defaults, including but not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings. Disable SSID broadcasts. Enable WiFi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable.*

This needs to be performed manually.

CO 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 as defined, for example, by SysAdmin Audit Network Security Network (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).

- CO 2.2.1 *Implement only one primary function per server (for example, web servers, database servers, and DNS should be implemented on separate servers).*

Using the *Firewall Policy Detail* report, identify whether these services have a common source network segment. Servers on the same network segment should be considered to be at the same security level, and cannot be considered separate.

- CO 2.2.2 *Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function)*

The *Firewall Summary* report under the *Findings* section presents a risk analysis based on an analysis of the configuration rules of the firewall. [//www.cisco.com/warp/public/146/news_cisco/ekits/vulnerability_report.pdf](http://www.cisco.com/warp/public/146/news_cisco/ekits/vulnerability_report.pdf) lists a set of insecure protocols that include RPC, SMTP, finger, TFTP, HTTP, HTTPS, DNS, FTP, NFS, SNMP, and X Window.

Use the *Details* hyperlink in the *Firewall Summary* report to identify the firewall configuration rules involved in allowing insecure services. This rule needs to be modified or eliminated. Re-run the report after the rule is modified to ascertain that the insecure or unnecessary service is disabled.

Similarly, unnecessary protocols may be identified in the *Policies passing through the Firewall* table of the *Firewall Summary* report. If any are found, the *Firewall Policy Detail with Rule Trails* is run report to identify the firewall configuration rules involved in allowing insecure services. This rule needs to be modified or eliminated. Re-run the *Firewall Summary* report after the rule is modified to ascertain that the insecure or unnecessary service is disabled.

CO 2.2.3 *Configure system security parameters to prevent misuse*

This needs to be performed manually.

CO 2.2.4 *Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

This needs to be performed manually.

CO 2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.

The *Firewall Policy Summary* report under the table *Policies to the Firewall* provides a list of services to the Firewall, which includes the list of management services and administrative access. Ensure that these services are encrypted.

CO 2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A.

This needs to be performed manually.

Source: [//www.pcisecuritystandards.org/pdfs/navigating_pci_dss_v1-2.pdf](http://www.pcisecuritystandards.org/pdfs/navigating_pci_dss_v1-2.pdf)