PCI DSS 3.1 Requirement 1 - Compliance Calendar Controls

Version 1.0
July 20th 2015

PCI DSS Requirements	Testing Procedure	Daily Ctrl	Weekly Ctrl	Monthly Ctrl	Quarter Ctrl.	Biannual Ctrl.	Annual Ctrl	Each Change
1.1 Establish and implement firewall and router configuration standards that include the following	**1.1** Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows:						A	
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	**1.1.1.a** Examine documented procedures to verify there is a formal process for testing and approval of all: - Network connections and - Changes to firewall and router configurations						A	
	1.1.1.b For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved and tested						A	
	1.1.1.c Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested.						A	
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	**1.1.2.a** Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to cardholder data, including any wireless networks.					B		
	1.1.2.b Interview responsible personnel to verify that the diagram is kept current.					B		
1.1.3 Current diagram that shows all cardholder data flows across systems and networks	**1.1.3** Examine data-flow diagram and interview personnel to verify the diagram: . Shows all cardholder data flows across systems and networks. . Is kept current and updated as needed upon changes to the environment.					B		
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	**1.1.4.a** Examine the firewall configuration standards and verify that they include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone.							C
	1.1.4.b Verify that the current network diagram is consistent with the firewall configuration standards.							C
	1.1.4.c Observe network configurations to verify that a firewall is in place at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone, per the documented configuration standards and network diagrams.							C
1.1.5 Description of groups, roles, and responsibilities for management of network components	**1.1.5.a** Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for management of network components.					B		
	1.1.5.b Interview personnel responsible for management of network components to confirm that roles and responsibilities are assigned as documented.					B		
1.1.6 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. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2.	**1.1.6.a** Verify that firewall and router configuration standards include a documented list of all services, protocols and ports, including business justification for each—for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols.					B		
	1.1.6.b Identify insecure services, protocols, and ports allowed; and verify that security features are documented for each service.					B		
	1.1.6.c Examine firewall and router configurations to verify that the documented security features are implemented for each insecure service, protocol, and port.					B		
1.1.7 Requirement to review firewall and router rule sets at least every six months	**1.1.7**.a Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months.					B		
	1.1.7.b Examine documentation relating to rule set reviews and interview responsible personnel to verify that the rule sets are reviewed at least every six months.					B		

Legend: *A: Annual Control, B: Biannual Control, C: Each Major Change, D: Daily Control, M: Monthly Control,Q: Quarter Control, W: Weekly Control*

1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	**1.2** Examine firewall and router configurations and perform the following to verify that connections are restricted between untrusted networks a							C
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	**1.2.1.a** Examine firewall and router configuration standards to verify that they identify inbound and outbound traffic necessary for the cardholder data environment.							C
	1.2.1.b Examine firewall and router configurations to verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment.							C
	1.2.1.c Examine firewall and router configurations to 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.							C
1.2.2 Secure and synchronize router configuration files.	**1.2.2.a** Examine router configuration files to verify they are secured from unauthorized access.							C
	1.2.2.b Examine router configurations to verify they are synchronized—for example, the running (or active) configuration matches the start-up configuration (used when machines are booted).							C
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	**1.2.3.a** Examine firewall and router configurations to verify that there are perimeter firewalls installed between all wireless networks and the cardholder data environment.						A	
	1.2.3.b Verify that the firewalls deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.						A	
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	**1.3.1** Examine firewall and router configurations to verify that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.						A	
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	**1.3.2** Examine firewall and router configurations to verify that inbound Internet traffic is limited to IP addresses within the DMZ.						A	
1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.	**1.3.3** Examine firewall and router configurations to verify direct connections inbound or outbound are not allowed for traffic between the Internet and the cardholder data environment.						A	
1.3.4 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)	**1.3.4** Examine firewall and router configurations to verify that anti-spoofing measures are implemented, for example internal addresses cannot pass from the Internet into the DMZ.						A	
1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	**1.3.5** Examine firewall and router configurations to verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized.						A	
1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only “established” connections are allowed into the network.)	**1.3.6** Examine firewall and router configurations to verify that the firewall performs stateful inspection (dynamic packet filtering). (Only established connections should be allowed in, and only if they are associated with a previously established session.)						A	
1.3.7 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	**1.3.7** Examine firewall and router configurations to verify that system components that store cardholder data are on an internal network zone, segregated from the DMZ and other untrusted networks.						A	
1.3.8 Do not disclose private IP addresses and routing information to unauthorized parties.	**1.3.8.a** Examine firewall and router configurations to verify that methods are in place to prevent the disclosure of private IP addresses and						A	
	1.3.8.b Interview personnel and examine documentation to verify that any disclosure of private IP addresses and routing information to external entities is authorized.						A	
1.4 Install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network. Firewall configurations include: - Specific configuration settings are defined for personal firewall software. - Personal firewall software is actively running. - Personal firewall software is not alterable by users of mobile and/or employee-owned devices.	**1.4.a** Examine policies and configuration standards to verify: - Personal firewall software is required for all mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network. - Specific configuration settings are defined for personal firewall software. - Personal firewall software is configured to actively run. - Personal firewall software is configured to not be alterable by users of mobile and/or employee-owned devices.				Q			

Legend: *A: Annual Control, B: Biannual Control, C: Each Major Change, D: Daily Control,*
M: Monthly Control,Q: Quarter Control, W: Weekly Control

	1.4.b Inspect a sample of mobile and/or employee-owned devices to verify that: - Personal firewall software is installed and configured per the organization's specific configuration settings. - Personal firewall software is actively running. - Personal firewall software is not alterable by users of mobile and/or employee-owned devices.				Q			
1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.	**1.5** Examine documentation and interview personnel to verify that security policies and operational procedures for managing firewalls are: - Documented, - In use, and - Known to all affected parties.					B		

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

Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network.

A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Other system components may provide firewall functionality, as long as they meet the minimum requirements for firewalls as defined in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1.

About the Author:

Marc Frederic Gomez ITIL certified, is referent PCI DSS for a French Bank. Marc-Frederic has more twenty years of Information Technology in a variety of fields included International heavy manufacturing, large finance organizations, Open Source companies, Hosting Companies, and IT Companies.

PCI DSS is a very exiting project and compliance program. Marc Frederic enjoy to share with you tips and solutions about this. Don't hesitate to follow Marc-frederic on the web sites http://blog.marcfredericgomez.com (EN) or http://blog.marcfredericgomez.fr (FR)

When not engaged in PCI DSS Audit or compliance he enjoys sport with his family.