PCI Network - Network Security Procedure

Office: Information Technology
Procedure Contact: IT Infrastructure Manager
Related Policy or Policies: PCI Network - User Accounts, PCI Network - Device Security

Revision History

Revision Number:	Change:	Date:
1.2	Formatting modification and expansion of Section B	**June 2017**
1.1	Post-QSA Update	**May 2017**
1.0	Initial Version	**November 2016**

A. Purpose

Networks within the scope of PCI compliance must be secured to prevent unauthorized access to cardholder data. This procedure outlines the steps that must be taken to properly secure a network of devices that contain or have access to cardholder data.

B. Definitions

"PCI" stands for "Payment Card Industry".

"DSS" stands for "Data Security Standards".

“User” shall refer to a single person with access to devices and/or network resources.

A “network” is a system of electronic devices interconnected by telecommunication equipment or cables used to transmit or receive information. The bounds of a “network” may be defined by the ability of traffic to pass unimpeded between devices, similar to a broadcast domain, or a specific range of IP addresses, around which connectivity restrictions are based.

A "PCI network" refers to any network as defined above, intended to enable credit card processing.

A “device” is a unit of physical microprocessor equipment, that either resides on a PCI network, or has direct access to the data/traffic on the PCI network.

"CDE" stands for "Cardholder Data Environment". The CDE is the the networks and devices involved in processing credit card transactions.

A “firewall” may be a device as defined above, or a software application, with the capability and intended purpose of filtering traffic in and/or out of a network.

Accessing a device “remotely” refers to any non-console access, or any console access that does not require physical presence at the device.

“CVSS” stands for Common Vulnerability Scoring System. The CVSS is a common set of base metrics used to evaluate how much risk a vulnerability poses to network security.

C. Network Description

The network where payment data is processed uses an RFC1918 IP Address space unique in the SOU environment. This network is isolated from other networks using a hardware machine firewall, and additionally isolated from the outside world by a hardware firewall device at the SOU network border.

No wireless connectivity is allowed within PCI networks. Devices capable of wireless communication must have their wireless radios disabled before being connected to a PCI network, and checked on a quarterly basis to ensure they remain disabled.

D. Network Firewall

1. A firewall shall be in place to restrict traffic in and out of the network.
2. The underlying hardware running the firewall shall be physically distinct from hardware used to run applications or services (including other firewalls) for non-PCI purposes.
3. All outbound traffic must be filtered to ensure only traffic critical to the operation, maintenance, and monitoring of the network is allowed out.
4. All inbound traffic must be filtered such that the only network activity allowed inbound, is a response to a permitted outbound request. Network traffic originating from outside the PCI network must not be allowed to pass through the firewall.
5. Authentication relying on strong cryptography must be implemented and required for any and all remote access to the firewall. Remote access to the firewall shall not be permitted from outside the bounds of the SOU network.
6. All non-console access to the firewall shall be protected by multi-factor authentication.
7. The firewall must conform to all of the requirements listed in the document PCI Network - Device Hardening, unless otherwise stated here.

E. Network Scanning

Internal and external scans of all PCI networks shall be performed on a quarterly basis. Internal and external scans must meet the following criteria:

1. The scans must be performed by a PCI Security Standards Council Approved Scanning Vendor.
2. For external scans, no vulnerabilities exist that are scored 4.0 or higher by the CVSS.
3. For internal scans, a passing result is obtained or all "high-risk” vulnerabilities as defined in PCI-DSS Requirement 6.1 are resolved.
4. Any vulnerabilities exposed by the internal or external scans will be remediated within 30 days.
5. A follow-up re-scan will performed after to ensure successful remediation.
6. Additional scans will be performed following any major changes to the CDE that are not completed within 30 days of an existing scheduled scan.

F. Penetration Testing

Penetration testing must be performed by a qualified outside vendor on an annual basis. The penetration testing must meet the following standards:

1. Performed at least annually and after any changes to segmentation controls/methods.
2. Covers all segmentation controls/methods in use.
3. Verifies that segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.