Build and Maintain a Secure Network

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

Firewalls are computer devices that control computer traffic allowed into and out of a company's network, as well as traffic into more sensitive areas within a company's internal 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 the Internet, whether entering the system as e-commerce, employees' Internet-based access through desktop browsers, or employees' e-mail access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

1.1 Establish firewall configuration standards that include the following:

- **1.1.1** A formal process for approving and testing all external network connections and changes to the firewall configuration
- **1.1.2** A current network diagram with all connections to cardholder data, including any wireless networks
- **1.1.3** Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone
- **1.1.4** Description of groups, roles, and responsibilities for logical management of network components
- **1.1.5** Documented list of services and ports necessary for business
- **1.1.6** Justification and documentation for any available protocols besides hypertext transfer protocol (HTTP), and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN)
- **1.1.7** Justification and documentation for any risky protocols allowed (for example, file transfer protocol (FTP), which includes reason for use of protocol and security features implemented
- **1.1.8** Quarterly review of firewall and router rule sets
- **1.1.9** Configuration standards for routers.

1.2 Build a firewall configuration that denies all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment.

1.3 Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. This firewall configuration should include the following:

- **1.3.1** Restricting inbound Internet traffic to Internet protocol (IP) addresses within the DMZ (ingress filters)
- **1.3.2** Not allowing internal addresses to pass from the Internet into the DMZ
- **1.3.3** Implementing stateful inspection, also known as dynamic packet filtering (that is, only "established" connections are allowed into the network)
- **1.3.4** Placing the database in an internal network zone, segregated from the DMZ
- **1.3.5** Restricting inbound and outbound traffic to that which is necessary for the cardholder data environment
- **1.3.6** Securing and synchronizing router configuration files. For example, running configuration files (for normal functioning of the routers), and start-up configuration files (when machines are re-booted) should have the same secure configuration

1.3.7 Denying all other inbound and outbound traffic not specifically allowed

1.3.8 Installing perimeter firewalls between any wireless networks and the cardholder data environment, and configuring these firewalls to deny any traffic from the wireless environment or from controlling any traffic (if such traffic is necessary for business purposes)

1.3.9 Installing personal firewall software on any mobile and 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 Prohibit direct public access between external networks and any system component that stores cardholder data (for example, databases, logs, trace files).

1.4.1 Implement a DMZ to filter and screen all traffic and to prohibit direct routes for inbound and outbound Internet traffic

1.4.2 Restrict outbound traffic from payment card applications to IP addresses within the DMZ.

1.5 Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet. Use technologies that implement RFC 1918 address space, such as port address translation (PAT) or network address translation (NAT).