

Firewall and Router Policy

Approved By: \\S\ James Palmer CSC Loss Prevention Director December 31, 2011 Date	PCI Policy # 1600 Version # 1.1 Effective Date: 12/31/2011 Revision Date: 12/31/2014
---	--

1.0 Purpose:

The purpose is to describe required minimum firewall and router configurations to protect all Coast Guard Morale, Well-Being and Recreation Program (MWR) systems from unauthorized access from the Internet.

2.0 Compliance:

PCI DSS Requirement 1

3.0 Scope:

This policy applies to all firewall and routers connected to MWR PROGRAM'S network.

4.0 Policy:

Procedures for managing firewalls will be documented, implemented and known to all affected parties.

Network Diagram

A current network diagram will be maintained which displays all connections to cardholder data, including wireless networks. Diagram must show credit card databases segregated from the DMZ. The network diagram must show the flow of cardholder data.

Physical Security

Only members of the Administrators to Network Devices (Form 1604) or their designee may install, uninstall, move, perform maintenance upon, or change the physical configuration of a firewall or router.

Any additions to the administrators group will require the Change Control Form 'Add Administrators to Network Devices' (Form 1601) to be completed and approved by the MWR Director/Officer.

Only the Administrators to Network Devices or their designee may make physical connections to a network device including direct access ports, console ports, etc.

In the event a firewall or router suffers physical damage or there is evidence of tampering, it will be fully evaluated by hardware diagnostics and the physical configuration checked with existing documentation.

Configuration Requirements

Only members of the Administrators to Network Devices or their designee may do the following:

- Log in directly to a network device's console port or other direct access port
- Assume administrative privileges on a network device
- Log in to the network device remotely

Any configuration changes will be approved and implemented in accordance with the MWR PROGRAM Change Management Policy, found in Policy 1500 – System Application Development and Maintenance Policy. The Network Device Implementation Checklist and Approval Form, (Form 1605), must be completed for all implemented network devices.

Network device password policies shall be the same as the MWR PROGRAM password policies.

Network devices shall limit administrative access to MWR PROGRAM networks that are firewalled from any untrusted source.

A demilitarized zone (DMZ) will be used to filter and screen all traffic and to prohibit direct routes for inbound and outbound Internet traffic.

Firewall and/or router configurations will restrict outbound traffic from payment card applications to IP addresses within the DMZ.

IP masquerading will be used to prevent internal addresses from being translated and revealed on the Internet such as port address translation (PAT) or network address translation (NAT).

Firewalls are to be placed at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.

Firewalls will restrict inbound Internet traffic to internal protocol (IP) addresses within the DMZ.

Firewalls will not allow internal addresses to pass from the Internet into the DMZ.

Firewalls will perform stateful inspection.

Anti-spoofing measures will be implemented to detect and block forged source IP addresses from entering the network.

Perimeter firewalls will be installed between any wireless networks and the cardholder data environment to permit only authorized traffic. These firewalls will be configured to deny any traffic from the wireless environment or from controlling any traffic.

Personal firewall software will be installed on any mobile and employee-owned computers with direct connectivity to the Internet which are used to access MWR PROGRAM's network. The personal firewall software will be configured so that it is unalterable by the user.

No local user accounts will be configured on the router except one emergency account. Routers will use TACACS+ for all user authentication and only members of the Administrators to Network Devices will have administrative access to these devices.

The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.

Routers must deny all inbound and outbound traffic not specifically allowed.

Router access rules are to be added as business needs arise.

Router configuration files (Form 1606) will be secure from unauthorized access and synchronized.

Each router will have the following statement in clear view:

ATTENTION!!!
You have accessed a Coast Guard Morale, Well-Being and Recreation restricted device. The actual or attempted unauthorized access, use or modification of this system is strictly prohibited. Unauthorized users are subject to disciplinary proceedings and/or criminal and civil penalties under state, federal or other applicable domestic and foreign laws. The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity we may provide the evidence of such activity to law enforcement.

A documented list of services and ports that are necessary for business will be identified on the Firewall Application Traffic Ruleset (Form 1602) and Ruleset for Boundary Router (Form 1603). Documentation will include justification for protocols besides hypertext transfer protocol (HTTP) and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN). Justification includes business reason for use of protocol and security features implemented.

Monitoring

All firewalls and router rulesets will be reviewed on a quarterly basis.

The List of Approved Network Device Administrators (Form 1604) will be reviewed on a quarterly basis.

5.0 Responsibility:

The MWR Director/Officer is responsible for leading compliance activities that bring THE COAST GUARD – MWR into compliance with the PCI Data

Security Standards and other applicable regulations and maintaining the documentation of the quarterly reviews.

6.0 Form(s):

Form 1601 – Change Control Form to Add Administrators to Network Devices

Form 1602 – Firewall Application Traffic Ruleset

Form 1603 – Ruleset for Boundary Router

Form 1604 – List of Approved Network Device Administrators

Form 1605 – Network Device Implementation Checklist and Approval

Form 1606 – Router Template/Checklists

7.0 Definition(s):

Definitions for technical terms can be found in Appendix A of your MWR PCI Compliance Workbook.

8.0 Policy History:

Initial effective date: 7/01/1999

First revision date: 12/31/2011

- *Revisions for PCI DSS Version 2.0*

Second revision date: 12/31/2014

- *Revisions for PCI DSS Version 3.0*