Chief Information Officer
Office of Information Technology
Centers for Medicare & Medicaid Services

CMS Operational Policy for
Firewall Administration

October 22, 2024

Document Number: CMS-CIO-POL-INF11-01

Record of Changes

Version	Date	Author/Owner	Description of Change
1.0	7/16/08		Created Policy
2.0	10/1/24	Wade Zarriello	Updated to include data center migration, updated standards, & accurate responsible components

Effective Date / Approval

This policy becomes effective on the date that CMS' Chief Information Officer (CIO) signs it and remains in effect until it is rescinded, modified or superseded by another policy.

Signature: GEORGE C. HOFFMANN -S Digitally signed by GEORGE C. HOFFMANN -S Date: 2024.10.25 07:12:59 -04'00'

George Hoffmann
Acting Chief Information Officer
Acting Director (Policy), Office of Information Technology

Policy Owner's Review Certification

This document must be reviewed in accordance with the established review schedule located on the CMS website.

Signature: Mark U. Oh -S Digitally signed by Mark U. Oh -S Date: 2024.10.17 16:06:50 -04'00'

Mark Oh
Infrastructure & User Services Group,
Office of Information Technology

TABLE OF CONTENTS

1. PURPOSE

This document establishes an operational policy for the administration (i.e., access, configuration, management, and monitoring) of firewalls at the Centers for Medicare & Medicaid Services (CMS).

2. BACKGROUND

CMS operates and maintains a complex computer networking infrastructure. Key components of CMS' networking infrastructure are firewalls, which are hardware or software devices that are configured to permit, deny, or proxy data through the network via different levels of trust.

The secure configuration of CMS' firewalls is necessary to enhance the overall security posture of CMS' layered security approach. This operational policy establishes parameters for the security of CMS' firewalls based on acceptable government and private industry standards for securing firewall devices.

The proper configuration of CMS' firewalls is necessary for overall security defense against unauthorized access and intrusions by preventing network attacks and penetration attempts. The review of firewall configuration, security, auditing logs, and firewall logs provides CMS with a means of:

- Ensuring that CMS' firewall configurations meet or exceed the security standards set forth by Federal guidelines; and
- Ensuring that an audit trail is in place for each change to a firewall's configuration.

3. SCOPE

This policy applies to all firewall devices controlled and operated by CMS or its designated IT Infrastructure Implementation Agent(s) or Contractor(s) for the CMS Hosting environments & associated infrastructure (i.e., CMS Hybrid Cloud Data Center's (HCDC's), CMS building locations, and other off-site facilities). Firewall devices controlled by contractors other than the CMS IT Infrastructure Implementation Agent(s), or Contractor(s) are not covered by this policy.

This policy does not supersede any other applicable law or higher-level agency directive, or existing labor management agreement in effect as of the effective date of this policy.

4. OPERATIONAL POLICY

4.A. Firewall Access

CMS firewall devices shall be accessible for configuration, management, and monitoring by only those individuals who are designated and authorized by CMS in accordance with established CMS Firewall Security Procedures.

4.B. Firewall Configuration

Firewalls shall be configured in accordance with CMS Firewall Security Procedures, and at a minimum shall address the following:

- All inbound traffic shall be denied unless explicitly allowed.
- All outbound traffic shall be denied unless explicitly allowed.
- Firewall devices shall be configured to prevent all known network attacks (e.g., Internet Protocol (IP) spoofing, TCP SYN, directed broadcast, Internet Control Message Protocol (ICMP) mapping, Simple Network Management Protocol (SNMP) mapping, Denial of Service (DoS), etc.).
- Firewall devices shall be secured behind locked doors within rooms that have air conditioning and air filtration. The secure room should have backup power supply and possible redundant connections to external networks.
- Firewall devices shall be connected to redundant power supply systems.
- All firewall management functions must use encryption along with user id and password. All passwords must be changed from default settings.
- Firewall operating system builds shall be based upon minimal feature sets. All unnecessary operating system features shall be removed from the build prior to firewall implementation. All appropriate operating system patches shall be applied before any installation of firewall components.
- The hardening configuration shall be tailored for the specific operating system undergoing hardening.
- Any unused physical network interfaces shall be disabled or removed from the server chassis.
- All firewalls shall have a fail over configuration & be designed as either Active/Active or Active/Standby in coordination with CMS.
- All firewalls shall be maintained at an N-1 software revision level.
- All firewalls shall be incorporated into a CMS monitoring and alerting engine and on boarded with the CMS Enterprise Operations Center (EOC).
- All firewalls shall be configured to use various logging facilities. The level and matter of logging shall include the following at a minimum:
    1) Critical warnings and error messages
    2) All login attempts
    3) All logon access

4) All configuration attempts
5) All configuration changes

4.C. Firewall Management & Monitoring

All Firewall log files shall be sent to a CMS approved Security Information and Event Management tool. Firewall configuration files shall be backed up on a weekly basis.

All firewall changes shall be performed in accordance with the standard CMS Change Management Protocol.

All firewall upgrades and patches shall follow the upgrade/patch process established for CMS firewalls.

All firewall configurations shall be reviewed, at a minimum, on a quarterly basis.

All firewall security policies shall be reviewed and updated annually. Ad hoc reviews may be necessitated by a security event, such as implementation of major enterprise computing environment modifications and any occurrence of a major information security incident.

5. ROLES AND RESPONSIBILITIES

The following entities have responsibilities related to the implementation of this operational policy:

5.A. Office of Information Technology (OIT)/Infrastructure & User Services Group (IUSG)/Division of Operations Management (DOM) Security Personnel

The OIT/IUSG/DOM Security Personnel are responsible for the following activities:

- Providing oversight and auditing of firewalls that are maintained by CMS IT Infrastructure Implementation Agent(s) or Contractor(s);
- Providing CMS standards, procedures, and guidelines for configuration, implementation, maintenance, technical support, management, and monitoring of firewalls in accordance with National Institute of Standards and Technology (NIST) and National Security Agency (NSA) guidelines; and
- Ensuring all firewall issues are addressed in an appropriate and timely manner.

5.B. CMS IT Infrastructure Implementation Agent(s) or Contractor(s)

The IT Infrastructure Implementation Agent(s) or Contractor(s) is responsible for the following activities:

- Providing implementation, maintenance, technical support, management, and monitoring of CMS' firewall devices;
- Assisting CMS in providing standards, procedures, and guidelines for configuration, implementation, maintenance, management, and monitoring of firewalls in accordance with NIST and NSA guidelines;
- Implementing changes (e.g., platform upgrades, device upgrades, and patches) to firewalls in a timely manner in accordance with CMS' change control procedures; and
- Reviewing and approving firewall audit logs, procedures, and policy changes.

6. APPLICABLE LAWS/GUIDANCE

The following laws and/or guidance are applicable to this operational policy:

- NIST SP 800-41, "Guidelines on Firewalls and Firewall Policy."
- NIST SP 800-61, "Computer Security Incident Handling Guide."
- Department of Health and Human Services (DHHS) Network and Telecommunications Security Policy.
- CMS Policy for Information Security (IS).
- CMS Policy for the Information Security Program.
- CMS Information Security (IS) Acceptable Risk Safeguards (ARS).

7. INFORMATION AND ASSISTANCE

Contact the Director of the Infrastructure & User Services Group (IUSG) within the Office of Information Technology (OIT) for further information regarding this operational policy.

8. ATTACHMENTS

The following documents augment this policy:

- CMS Firewall Security Procedures
- CMS Firewall Log Review Procedures

GLOSSARY

Denial of Service (DoS)

A DoS is a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic.

Directed Broadcast

Directed broadcast is a type of attack that allows the attacker to send ICMP datagrams to addresses of remote LANs broadcast addresses, using so-called directed broadcast addresses. These datagrams are then broadcasted via LANs by the connected router.

Firewall

A firewall is a hardware or software device that is configured to permit, deny, or proxy data through the network via different levels of trust.

Internet Control Message Protocol (ICMP) Mapping

ICMP mapping is a type of attack designed to use the ICMP to discover a network, the devices associated with it, and determine how they are physically connected together.

Internet Protocol (IP) Spoofing

IP spoofing is a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host.

Operating System Hardening

Operating system hardening is the process of eliminating basic vulnerabilities on the operating system by removing all non-essential tools, utilities, and other systems administration options from “out of the box” systems. Following a hardening process ensures that all appropriate security features are activated and configured correctly.

Simple Network Management Protocol (SNMP) Mapping

SNMP mapping is a type of attack designed to use the SNMP to discover a network, the devices associated with it, and determine how they are physically connected together.

TCP SYN

When a normal TCP connection starts, a destination host receives a SYN (synchronize/start) packet from a source host and sends back a SYN ACK (synchronize acknowledge). The destination host must then hear an ACK (acknowledge) of the SYN ACK before the connection is established. This is referred to as the "TCP three-way handshake." While waiting for the ACK to the SYN ACK, a connection queue of finite size on the destination host keeps track of connections waiting to be completed. This queue typically empties quickly since the ACK is expected to arrive a few milliseconds after the SYN ACK.

The TCP SYN attack exploits this design by having an attacking source host generate TCP SYN packets with random source addresses toward a victim host. The victim destination host sends a

SYN ACK back to the random source address and adds an entry to the connection queue. Since the SYN ACK is destined for an incorrect or non-existent host, the last part of the "three-way handshake" is never completed and the entry remains in the connection queue until a timer expires, typically for about one minute. By generating phony TCP SYN packets from random IP addresses at a rapid rate, it is possible to fill up the connection queue and deny TCP services (such as e-mail, file transfer, or WWW) to legitimate users.