coast mountain college

**RESOURCE INF-003**

# Firewall Guideline

## Purpose

This guideline governs how the firewalls will filter Internet traffic to mitigate the risks and losses associated with security threats to Coast Mountain College's (CMTN's) network and information systems.

## Overview

CMTN operates network firewalls between the Internet and its private internal network to create a secure operating environment for CMTN's computer and network resources. A firewall is just one element of a layered approach to network security.

## Definitions

**Firewall**: Any hardware and/or software designed to examine network traffic using statements (ruleset) to block unauthorized access while permitting authorized communications to or from a network or electronic equipment.

**Firewall Configuration**: The system setting affecting the operation of a firewall appliance.

**Firewall Ruleset**: A set of statements or instructions used by a firewall to filter network traffic.

**Host Firewall**: A firewall application that addresses a separate and distinct host, such as a personal computer.

**Internet Protocol (IP):** Primary network protocol used on the Internet.

**Network Firewall**: A firewall appliance attached to a network for the purpose of controlling traffic flows to and from single or multiple hosts or subnet(s).

**Network Topology**: The layout of connections (links, nodes, etc.) of a computer network.

**Simple Mail Transfer Protocol (SMTP):** An Internet standard for electronic mail (e-mail) transmission across IP networks.

**Virtual Private Network (VPN):** A network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with private, secure access to their organization's network.

## Scope

The firewall will (at minimum) perform the following security services:

- access control between the trusted internal network and untrusted external networks
- block unwanted traffic as determined by the firewall ruleset
- hide vulnerable internal systems from the Internet
- hide information, such as system names, network topologies, and internal user IDs, from the Internet
- log traffic to and from the internal network
- provide robust authentication
- provide virtual private network (VPN) connectivity.

## Details

All network firewalls, installed and implemented, must conform to the current standards as determined by CMTN's IT Department. Unauthorized or non-standard equipment is subject to immediate removal, confiscation, and/or termination of network connectivity without notice.

The approach adopted to define firewall rulesets is that all services will be denied by the firewall unless expressly permitted in this guideline.

- outbound – allows all Internet traffic to authorized groups.
- All traffic is authorized by Internet Protocol (IP) address and port.

The firewalls will provide:

- Packet filtering – selective passing or blocking of data packets as they pass through a network interface. The most often used criteria are source and destination address, source and destination port, and protocol.
- Application proxy – every packet is stopped at the proxy firewall and examined and compared to the rules configured into the firewall.
- Stateful Inspection – a firewall technology that monitors the state of active connections and uses this information to determine which network packets to allow through the firewall.

The firewalls will protect against:

- IP spoofing attacks – the creation of IP packets with a forged source IP address with the purpose of concealing the identity of the sender or impersonating another computing system
- denial-of-service (DoS) attacks - the goal is to flood the victim with overwhelming amounts of traffic and the attacker does not care about receiving responses to the attack packets
- any network information utility that would reveal information about the CMTN domain.

A change control process is required before any firewall rules are modified. Prior to implementation, the third-party vendor and CMTN network administrators are required to have the modifications approved by the Director of IT or the VP of IT. All related documentation is to be retained for three years.

All firewall implementations must adopt the position of "least privilege" and deny all inbound traffic by default. The ruleset should be opened incrementally to only allow permissible traffic.

Firewall rulesets and configurations require periodic review to ensure that they afford the required levels of protection:

CMTN must review all network firewall rulesets and configurations during the initial implementation process and periodically thereafter.

Firewall rulesets and configurations must be backed up frequently to alternate storage (not on the same device). Multiple generations must be captured and retained, to preserve the integrity of the data, should restoration be required.

Access to rulesets and configurations and backup media must be restricted to those responsible for administration and review.

## Responsibilities

The IT Department is responsible for implementing and maintaining CMTN firewalls, as well as for enforcing and updating this guideline. Logon access to the firewall will be restricted to a primary firewall administrator and designees as assigned. Password construction for the firewall will be consistent with the strong password creation practices outlined in INF-008G, *Password Choice and Protection Guideline*.

The specific guidance and direction for information systems security is the responsibility of IT. Accordingly, IT will manage the configuration of the CMTN firewalls.

CMTN has contracted with a third-party vendor to manage the external firewalls. This vendor will be responsible for:

- retention of the firewall rules
- patch management
- reviewing the firewall logs for:
    - system errors
    - blocked web sites
    - attacks
- sending alerts to the CMTN network administrators in the event of attacks or system errors
- backing up the firewalls.

## Related Policies, Guidelines, and Other Resources

- INF-008G, *Password Choice and Protection Guideline*