CEDAR

Firewall Change Management Policy

Version 1

Esteban Miranda
6-9-2024

Contents

1. Overview and Policy Summary

This document establishes procedures for managing changes to CEDAR's firewall configurations, ensuring security, compliance, and operational efficiency.

2. Purpose

This policy details a process for reviewing, approving, executing, managing, and documenting firewall change requests to maintain confidentiality, integrity, and availability.

3. Scope

This policy applies to all CEDAR employees and anyone who works with CEDAR's firewalls and is involved in the change management process.

4. Policy

The following are the policy requirements regarding all of CEDAR'S firewalls.

4.1 Firewall Configuration

Each firewall should have a firewall configuration created and documented. The IT department should report any firewall hardware, software, and physical operating environment changes and the firewall change management policy. The firewall configuration documentation should have backups, with multiple copies saved in a secured location.

4.2 Firewall Change Requests

Firewall changes should be submitted for approval by the Chief Information Security Officer (CISO) and the IT Security team. If approved, a scheduled date for their implementation will be issued promptly.

4.3 Emergency Firewall Changes

Emergency firewall rules should be submitted directly to the Chief Information Security Officer and highlighted as needing immediate attention.

4.4 Authorization

The upper management of IT is responsible for identifying authorized employees to submit firewall rules.

4.5 Firewall Reviews and Updates

Firewall rules should be reviewed quarterly and updated accordingly in the documentation of the firewall rule configurations.

4.6 Deny Traffic by Default

All firewalls should be configured to deny all traffic by default and all traffic that has not been approved.

4.7 Block ICMP

Inbound Internet Control Message Protocol will be blocked at the perimeter.

4.8 Authentication

Firewalls will authenticate users with IPsec or Virtual Private Networks (VPN).

4.9 Detail Description

Each rule documented should have a detailed description.

4.10 Inactivity

The firewall policy should include an inactivity network feature. By default, the firewall disconnects inactive sessions after 60 seconds of inactivity.

4.11 Logging and Audits

All firewalls should have management logging and auditing. The log events will be forwarded to the Security Incident Event Management (SIEM) system. All firewalls must also use an authentication mechanism that allows users to access information through secure channels.

4.12 Top Teir Hardware

CEDAR should use top-of-the-line firewalls to protect confidentiality, integrity, and availability.

4.13 ICSA

All firewalls should meet the latest International Computer Security Association (ICSA) lab's certification.

4.15 Training

Frequent training should be provided for all employees on the firewall policy and procedures.

4.16 Incident Response

Procedures should be implemented to respond to detected incidents through the firewall logs and audits. Steps for mitigating and reporting should be included.

4.17 Testing

All firewalls should undergo testing before being implemented to avoid vulnerabilities and disruptions. After implementation, testing should be conducted to verify proper performance. All testing procedures should be documented.

4.18 Documentation Approval

Documentation should be provided on the review and approval of firewall changes, including roles and responsibilities.

4.19 Backups

To ensure business continuity, the firewalls should be backed up daily, and recovery procedures should be implemented.

5. Enforcement and Penalties

Any authorized firewall users who violate this policy will face disciplinary actions by the appropriate department. Violators may be subject to criminal prosecution, civil liability, or both of any unlawful use of access.

6. Revision History

Version	Date	Updates Made By	Update Details
1.0	6/9/2024	Esteban Miranda	Policy Creation

7. Approval History

Version	Date	Approved By
1.0	6/9/2024	Chief Information Security Officer

8. Review History

Date	Reviewed By
6/9/2024	Chief Information Security Officer

9. Firewall Change Management Cycle

Phase	Actions
Change Request is issued	▪ The request will be made by authorized individuals in the IT department.
Investigate the details and impact of the change	▪ The network administrator or firewall administrator will investigate which firewall will need configuration and will support the request. ▪ Implementation details will be documented.
Assess the potential risk	▪ Each request will be investigated to assess its risk and compliance regarding business continuity, integrity, and availability. ▪ The IT security team will be involved, and other necessary departments may also be involved.
Approval	▪ The request will be either approved, denied, or improved by the CISO and IT security team.
Configure the change	▪ Changes will be implemented as Access Control Lists (ACL), Network Address Translation (NAT), Virtual Private Network (VPN), and anything necessary.
Resolve and authenticate	▪ Firewall changes are recorded. ▪ Firewall changes will be compared with approved requests. ▪ Verify and identify that firewall changes are identical with requests. ▪ Change requests will be resolved and closed.

10. Firewall Change Request Form

Requester's Name	Requester's Phone	Requester's Email	Request Type: Initial or Additional or Delete	Date of Request

Description of Request

Firewall Rule Request

	Source Address and Subnet Mask	Destination Address and Subnet Mask	Source Protocol and Port Number	Destination Protocol and Port Number	Deny or Permit	Add or Remove or Modify	Description
1							
2							
3							
4							
5							
6							
7							

Signature:

x _____