Firewall Management Policy

Diné College Information Technology

Ihab Saleh

Revision History

Version Number	Revision Date
1.0	10/2/2024

Table of Contents

1. Purpose

The purpose of this Firewall Management Policy is to ensure a standardized approach to firewall configuration and management, maximizing protection and detection capabilities in support of the organization’s security requirements. Firewalls provide essential protection and detection when properly configured, managed, and monitored. This policy establishes guidelines to maintain effective firewall operations across the organization's environment.

2. Scope

This policy applies to all employees, contractors, third-party personnel, and any other individuals responsible for managing, configuring, or operating firewalls within the organization’s network infrastructure. It covers all firewall implementations, including those used for production, development, testing, and any other environments where the organization's data or systems are involved.

This policy also extends to the management of firewall hardware and software, ensuring that all devices and configurations are maintained according to lifecycle best practices. Additionally, it includes the monitoring and auditing of firewall activity, regardless of whether the firewall is hosted on-premises, in the cloud, or within hybrid environments.

3. Roles and Responsibilities

This section outlines the key responsibilities for individuals and teams involved in the management and configuration of firewalls, ensuring accountability and clear ownership for firewall-related tasks.

Chief Information Officer (CIO)

The CISO is responsible for the overall governance of the firewall management policy. This includes ensuring that all firewall configurations are in compliance with the organization's security standards and that any deviations are properly documented and approved. The CISO must also approve any changes to the policy and review firewall management reports regularly to ensure ongoing compliance.

Information Security Team

The Information Security Team is tasked with the day-to-day operations of firewall management. This includes configuring firewalls, conducting regular reviews of firewall rules, and ensuring that firewalls are properly maintained in accordance with EOL/EOS guidelines. The team must also handle the secure backup of firewall configurations and logs, as well as reviewing logs for any suspicious activity. The team collaborates with other departments to ensure that all firewall-related issues are promptly addressed and escalated as necessary.

System Administrators

System Administrators are responsible for implementing and managing firewall rules in accordance with organizational policies. They ensure that firewall rules are properly configured to meet operational requirements while adhering to the principle of least privilege. They are also responsible for reporting any configuration changes or issues to the Information Security Team.

Employees and Contractors

All employees and contractors who have access to the organization's firewall systems must comply with the firewall rules set forth by the Information Security Team. They are responsible for ensuring that their activities do not violate any established firewall policies and must report any suspicious activity or incidents to the appropriate personnel.

4. Firewall Configuration Standards

This section defines the standards for configuring and maintaining firewalls, ensuring they are properly managed throughout their lifecycle.

- Firewalls must be properly maintained from both hardware and software perspectives, including lifecycle planning for End of Life (EOL) and End of Support (EOS) systems.
- Firewall rulesets must be reviewed at least annually to identify shadow, redundant, or conflicting rules, and to ensure consistency across the organization's network.
- Firewall configurations and rulesets must be backed up regularly to alternate storage, ensuring multiple generations are retained. Access to these backups must be limited to authorized personnel.

5. Firewall Rules

This section outlines the guidelines for creating, managing, and enforcing firewall rules to ensure secure and controlled network traffic.

- Firewall rules must follow the principle of least privilege, denying all inbound traffic by default. Rules should be incrementally opened to allow only necessary traffic.
- Outbound traffic must be enumerated based on data stores, applications, or services, and overtly broad rules are prohibited unless explicitly approved by the CISO or their designee.
- Protocols and service names must follow assignments from the Internet Assigned Numbers Authority (IANA) unless a valid technical reason is documented.
- The use of ANY/ANY/ALL rules is strictly prohibited.

6. Firewall Logging

This section describes the requirements for logging firewall activity, ensuring logs are properly maintained and reviewed for security purposes.

- Firewalls must log configuration changes, service modifications, and suspicious activity. Logs must be stored outside the firewall and reviewed regularly (at least monthly).
- Firewall logs may be forwarded to the organization's Security Information and Event Management (SIEM) system for long-term retention and analysis.

7. Enforcement

Violations of this policy will result in disciplinary actions in accordance with organizational regulations, employment agreements, and applicable laws. Disciplinary measures may include, but are not limited to, mandatory re-training, formal warnings, suspension of access to information systems, or termination of employment or contract. In cases of severe or repeated violations, legal action may also be taken if the breach results in significant damage or liability to the organization.

Enforcement of this policy includes regular and ad-hoc audits to ensure compliance with firewall management standards. Audits will be conducted by the Information Security Team or an authorized third party to verify that firewall configurations, rulesets, and logging practices meet the requirements outlined in this policy. Any identified non-compliance will be documented and reported to the Information Security Team for prompt remediation. Failure to address non-compliance in a timely manner may result in escalated actions, including a formal review by senior management or external auditors.