CHRISTOPHER NEWPORT
UNIVERSITY

Network Firewall Standard

VERSION 1.4

January 2024

Department: Information Security

Proprietary Statement

Review and Revision History

Date	Version	Description of Change (Affected Sections)	Author
April 2019	1.0	Initial Plan	Wendy Murray
August 2020	1.1	Annual Review	Wendy L. Corrice
August 2021	1.2	Annual Review	Wendy L. Corrice
June 2023	1.3	Annual Review	Wendy L. Wilde
January 2024	1.4	Change – Moved procedure items into “Standards Statement” and modified statements, added Appendix-A, and updated References	Matthew Dillion

TABLE OF CONTENTS

Network Firewall Standard

Introduction:

In accordance with the Christopher Newport University Acceptable Use Policy, all systems owned or managed by the University must be adequately protected to ensure confidentiality, integrity, availability and accountability of such systems. Firewalls may be used to establish a perimeter between the University internal network and external networks (i.e. Internet, Internet2, E-LITE, etc.) or within the University to maintain segmentation between internal networks.

Purpose:

To establish a uniform set of standards for implementing and maintaining established network firewall baseline configurations including, but not limited to: defining intrusion prevention, web filtering, network security zones, and security policies, specifying the application and port of traffic which will be allowed or denied access to those zones. Also, to maintain the stability of the network and increase visibility and the security for identified resources.

Scope:

These standards cover the configuration of the Christopher Newport University network firewall appliances and network virtual firewalls.

Standards Statement:

Ownership, Responsibility and Access

All equipment and applications within this scope must have a valid support contract and will be administered by the ITS Infrastructure team. Physical access to equipment shall be limited, and equipment located in a secure environment.

Administrative Access

Administrative users shall: access the firewall from authorized hosts located no internal subnets only, or, authorized VPN software. Accounts used for firewall administration must authenticate via Active Directory Federation Services; a “backup” local administrator account shall be used for access when AD Federation services are unavailable or when required to perform “privileged” tasks associated only with the local administrative account.

The organization-defined system use notification banner below will be presented on the firewall login page before granting access to the system.

“This system is the property of the Commonwealth of VA. Only persons authorized shall be allowed access to this system. Those permitted access shall use this system ONLY for purposes for which they have been authorized. ALL access and usage on this system is logged. ANY unauthorized access, use, or abuse of this system or the information contained therein shall be reported to appropriate authorities for investigation and prosecution to the fullest extent of the law.”

Firewall Hardening and Best Practices

All unnecessary vendor-supplied defaults must be changed to Christopher Newport-specific configurations and Software/Firmware updates are required to be installed in a timely manner, depending on the likelihood and impact of vulnerability exploitation.

Firewall security and privacy configuration settings must be implemented based on: vendor best practices, industry best practices, and University business needs; the monitoring and deviation of settings will be accomplished using a vulnerability verification tool (Appendix A).

Changes to security and privacy firewall configuration settings will be documented through Change Management and saved as part of the baseline configuration.

Firewall Baseline Configurations

Firewall Baseline configurations include connectivity, operational, and communications aspects of the system. Baseline configurations are saved “offline” in a designated space and subsequent updates are documented and tracked through version control. Changes to the baseline configuration must be initiated through Change Management and supporting documentation updated (Appendix A).

An annual review of firewall configuration files will be completed to verify the continued validity of the firewall security policy rules and configurations as compared with the baseline and that no unauthorized changes have occurred. The annual review will be initiated through Change Management and supporting documentation updated.

Change Management

Configuration changes made to University network firewalls are completed in accordance with the “*Firewall Change Management Standard*”. Modification of firewall settings are carefully evaluated based on: business justification, applicable rules and requirements, the protective value of the institutional assets involved, and the impact to network access and performance.

Incident Reporting:

System Administrators are required to report any suspicious activity to the Information Security Officer for Investigation.

Security Updates

Security patches for firewalls must be installed in a timely manner, depending on the likelihood and impact of vulnerability exploitation. Refer to the "*Vulnerability Scanning & Management Procedures*" for specifics.

Logging of Administrative Access

ITS will retain audit records consistent with the "*Security Logging and Monitoring Standard*" to provide support for after-the-fact investigations of security incidents and to meet regulatory and agency information retention requirements.

The following types of activities must be logged: successful/unsuccessful administrative login attempts, any firewall modification operation, rejected administrative connection attempts.

Backup and Recovery

Vendor provided backup and recovery procedures will be referenced to ensure the firewalls can be rebuilt in the event of a disruptive event. Further, configuration backups and log exports should be captured before significant changes, to ensure a copy of the configuration exists for reverting changes after an unexpected disruption.

Firewall Deployment:

External Network Segmentation (i.e. Internet, Internet2, E-LITE, etc.)

The University network must be protected from malicious Internet traffic. Information Technology Services (ITS) will restrict traffic at the connection points between the University and external networks. Restrictions will be based on: current guidance from authoritative sources, such as block lists supplied by multiple vendors and validated with Palo Alto Networks threat intelligence data, from historical knowledge of common avenues of attack, and University operational requirements.

Network architecture decisions are made after careful evaluation of: business rules and requirements, the protective value of the institutional assets involved, and network performance. Actions are taken in the best interest of the overall security and performance of the network.

Internal Network Segmentation (i.e. Production, Dev, R&D, Auxiliary, etc.)

The University network employs methods to manage and improve security through logical and physical segmentation of networks, systems, and users.

Controls are applied to the network based on system security, timing, operational impact, and funding limitations.

Access to network resources is authorized on a necessity basis only after a valid business reason is determined and approved.

Logging of Security Policies and System Events

ITS will retain audit records consistent with the "*Security Logging and Monitoring Standard*" to provide support for after-the-fact investigations of security incidents and to meet regulatory and agency information retention requirements.

The following types of activities must be logged: hits for each security policy rule, Threat Prevention profile, Antivirus profile, Anti-Spyware profile, URL Filtering profile, VPN authentication/establishment, and system events.

Procedures:

- Firewall Hardening and Implementing Best Practices
    - Reference CIS Benchmark published steps
    - Reference vendor supplied documentation
    - Modify settings based on University business needs

- Baseline Configuration Change procedure
    - Reference Change Management procedure

- Perform annual review of firewall configuration files

- Firewall Account Management Procedures - Link

- Firewall Change Management Procedures - Link

- Configuration Backup and Restoration - Link

- Vulnerability Scanning & Management Procedures - Link

Exceptions:

Exceptions to this standard will be handled on a case by case basis and approval of the Information Security Officer.

References:

ITS Managed Network Infrastructure Standard

Security Monitoring and Logging Standard

VITA ITRM Information Security Standard (SEC530)

Vulnerability Assessment & Management Standard

Appendix A:

- Vulnerability verification tool: Nessus
- Supporting documentation location: Confluence

Review:

Next Review Date: June 2024