CHRISTOPHER NEWPORT
UNIVERSITY

Network Firewall Standard

VERSION 1.4

June 2023

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

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 network and the public Internet, or within the University to maintain segmentation between the networks.

Purpose:

To establish a uniform set of standards for implementing and maintaining established network firewall policies. Including, but not limited to, defining network security zones within the University's network and the type and nature of traffic which will be allowed or denied access to those zones. Also, to maintain the stability of the network and increase the security for identified resources.

Scope:

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

Standards Statement:

1. **Protecting the Network from the Internet**

The University network must be protected from malicious Internet traffic. Information Technology Services (ITS) will minimally restrict traffic at the connection points between the University and the Internet. Restrictions will be based on current guidance from authoritative sources, such as the SANS/FBI Top 20 Internet threats list, and from historical knowledge of common avenues of attack.

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

1. **Network Segregation**

The University network employs methods to manage and improve security through logical and physical segregation. Groups of users and information systems are segregated on the network.

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

Access to network resources is segmented into user and system domains and access is authorized on a necessity basis only after a valid business reason is determined and approved. Security controls are placed on many shared access segments to mitigate the spread of malicious traffic.

1. **Cabling Security**

ITS is responsible for the installation or coordination of network cabling at Christopher Newport University. All communication cabling activities are required to meet code for the locality involved. ITS uses industry standards according to a quality of service criteria. Cabling is best viewed as a component of the building infrastructure. Its design and management must be considered in context with the long term requirements of the campus.

Users are prohibited from altering or otherwise extending the campus network. All network connectivity is coordinated through ITS. Only authorized personnel have access to campus wiring closets.

1. **Service Agreements**

In-house or third-party network service agreements must include detailed requirements for security compliance, service levels, and management requirements. Users are required to follow the Acceptable Use of Computing Resources Policy when using the University's network and other technology resources.

Procedures:

- **Ownership and Responsibility:**

All equipment and applications within this scope will be administered by the ITS Infrastructure team.

1. **Physical Location:**
    1. Network perimeter firewalls should be installed on dedicated hardware in secure areas.
2. **Support Requirements:**
    1. All firewalls must have a valid support contract.
3. **Baseline Security Configuration:**
    1. All vendor-supplied defaults must be changed to Christopher Newport-specific configurations.
    2. All unnecessary default accounts must be removed or disabled before installing a firewall on the network.
    3. Any security updates to Baseline configuration must be documented through Change Management and supporting documentation updated.

4. Perform annual review of firewall configuration files to ensure the continued validity of the firewall rules and configurations as compared with the baseline to ensure no unauthorized changes have occurred.
    1. Log "firewall base configuration" review at Firewall Baseline Configuration

4. **Patching:**
    1. 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.
5. **Rules:**
    1. Network firewalls must be configured to deny all ingress traffic by default, with specific rules permitting the minimum traffic required for University operations. Global allow rules should not be enabled as they provide unnecessarily broad access. Rules are generally processed in order from the top downward, thus, “deny all” rules should be placed below the explicit allows.
    2. Rules must be documented with business justifications and reference to Change Control number where applicable.

- **Administrative Access:**
    1. All administrative access to University Firewalls will be governed by Firewall Account Management Procedures.
    2. All administrative users must authenticate via Active Directory Federation Services. A backup administrator account shall be used for console access.
    3. All administrative access must originate from internal subnet only, or, authorized VPN access.
    4. All administrative access shall be restricted to internal networks and authorized hosts.
    5. Additional control is subnet VLAN limitations to internal subnet access only.
    6. Each network firewall will present the following login banner when a user logins to the device:

“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 reportedto appropriate authorities for investigation and prosecution to the fullest extent of the law.”

- **Logging:**
    1. 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:

1. Successful and unsuccessful administrative login attempts
2. Any firewall modification operation
3. Rejected connection attempts
4. Number of hits for each rule should be logged to assist in the identification of rules that may not be needed or are redundant with other rules

- **Incident Management:**
    1. System Administrators are required to report any suspicious activity to the Information Security Officer for Investigation.

- **Backup and Recovery**
    1. Backup and recovery procedures must be established 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 method of failing back after an unexpected disruption.
    2. Major version upgrades require the creation of a Change Management Request.

Exceptions:

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

References:

VITA ITRM Information Security Standard (SEC501)

ITS Managed Network Infrastructure Standard

Review:

Next Review Date: June 2024