



OIT 62.005: Firewall Administration

Responsible Executive: Chief Information Officer (CIO)
Responsible Office: Office of Information Technology
Related Policy: NSU 60.201: Acceptable Use of Technological Resources
Approved-On Date: November 23, 2004
Effective Date: November 23, 2004
Revision Date: December 17, 2009

Policy Statement

Norfolk State University (NSU) operates perimeter firewalls or gateways between the Internet and the campus networks to establish a security environment for the University's technological resources. NSU's perimeter firewalls are key components of the institution's Network Security Architecture. The perimeter firewall policy governs how the perimeter firewalls will filter Internet traffic to mitigate the risks and possible losses associated with security threats to the networks and information systems.

Purpose

This policy establishes procedures for NSU perimeter firewall administration, determines the technology standard used by the firewall hardware and software, assigns firewall administration responsibilities and defines the filters applied to campus networks.

Responsibilities

The Office of Information Technology (OIT) is responsible for implementing and maintaining the institution's networks perimeter firewalls and is also responsible for activities relating to this policy. While responsibility for information systems security on a day-to-day basis is everyone's responsibility, specific guidance and direction for information systems security is the responsibility of OIT. Accordingly, the OIT Security Team composed of the Information Security Officer and other OIT specialists as may be needed will manage the configuration of the University's perimeter firewalls.

Policy for Perimeter Firewalls

The perimeter firewall permits the following outbound and inbound Internet traffic:

- Outbound - All Internet traffic to hosts and services outside of NSU metropolitan area network with the exception of traffic defined in Table 1.
- Inbound - Allow Internet traffic that supports the mission of the institution, Table 1 is pertinent.
- Outbound/Inbound – All internet traffic detected as malicious by the firewall's intrusion prevention system (IPS) and/or all traffic violating NSU policies is dropped.

Reason for filtering ports:

- Protecting NSU Internet Users - Certain ports are filtered to protect NSU networks and users. The perimeter firewall protects against certain common worms and from dangerous services on NSU computers that could allow intruders access.
- Protecting our outbound bandwidth - If NSU Internet users overuse their outbound bandwidth by running high-traffic servers or by becoming infected with a worm or virus, it can degrade the service of other NSU systems.
- Protecting the rest of the Internet - Some filters prevent personnel who are associated with the University from both knowingly or unknowingly attacking other computers on the Internet. In addition to being in NSU's interests for protecting our bandwidth, it is the institutions' responsibility to prevent abuse of its network.

Firewall Standards

NSU is committed to operate application aware Next Generation Layer 7 firewalls supporting state-full inspection.

Logs

Firewall logs will be sent to the designated syslog server where they will be archived and retained for a period of time commensurate to available space on the logs server and for a minimum of 30 days. Automatic programs to detect intrusion and anomalies will parse firewall logs and send scheduled reports.

Configuration

The Information Security Officer will examine firewall configuration and ruleset periodically and not less than annually.

Logical Security

Logical access to the firewall and account management shall be controlled by the University central authentication system.

Physical Security

Firewalls must be located in locked and electronically monitored rooms accessible only by those who must have physical access to such firewalls and/or the equipment therein. Firewalls shall not be placed in publicly accessible rooms or rooms lacking proper access control.

Backups

Firewall configuration will be backed up every time a change is made to the configuration. In addition

Upgrades and Patches

Firewall upgrades and patches will be applied in accordance to Change Management processes when released by the software vendor.

Operational Procedures

- Faculty, staff, and students may request that access be granted from the Internet to services inside NSU for a new or existing server or service. These requests will be submitted to the Information Security Officer and must include detailed justification to support the request. Requests will be submitted using the Firewall Access Request Form that is available online at <http://www.nsu.edu/forms/>
- The OIT Security Team will evaluate the risk of opening the firewall to accommodate requests. Where the risk is acceptable, granting of requests will be dependent on network infrastructure limitations and the availability of required resources to implement the request. If the risk associated with a given request is deemed objectionable, then an explanation of the associated risks will be provided to the requestor and alternative solutions will be explored.
- If during the implementation of an approved request it is determined that the request does not provide the functionality to meet the requestor's business need, then the OIT Security Team may, on a short-term basis, provide open access through the firewall. Afterward, the team will work with the requestor to determine exactly what ports are needed to meet the requestor's needs.
- Certain mission-critical functions require outside vendors and other entities to have secure, limited access to campus information systems achieved by way of the Internet. Such access must be approved and then coordinated through the OIT Security Team by submitting written request signed by an appropriate University representative. Requests will be submitted using the Firewall Access Request Form that is available online at <http://www.nsu.edu/forms/>

TABLE 1
Filtered network ports

Port	Transport	Protocol	Direction	Reason for Filtering
25	TCP	SMTP	Both*	SMTP Relays
80	TCP	HTTP/S	Inbound*	Web servers, worms
135-139	UDP, TCP	NetBIOS	Both	Worms, Network Neighborhood
445	TCP	MS-DS/ NetBIOS	Both	Worms, Network Neighborhood
1900	UDP	MS-DS/ NetBIOS	Both	Worms, Network Neighborhood

*SMTP is only permitted to/from NSU-provided or authorized SMTP servers

*HTTP/S is only permitted inbound to NSU-provided or authorized HTTP servers