Network Firewall Standard

Policy Title:
Network Firewall Standard

Responsible Executive(s):
Chief Information Security Officer

Responsible Office(s):
University Information Security Office

Contact(s):
If you have questions about this policy, please contact the University Information Security Office.

I. Policy Statement

These standards cover the configuration of Loyola University's network firewalls. In addition, please note that this policy covers all IoT devices. The purpose of this standard is 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.

II. Definitions

Not applicable.

III. Policy

Ownership and Responsibility

All equipment and applications within this scope will be administered by Network Services.

Network Security Zones

A set of clearly defined network zones, with different levels of security requirements, built to provide the proper secure levels of networking access to the University community.

- **Loyola DMZ:** a semi-restrictive network, or group of networks, whose purpose is to publish content for public and/or Internet consumption. This zone contains a mix of ITS and Academic resources.

- **Loyola Campus:** a semi-restrictive network, or group of networks, which contain the majority of Loyola's network traffic whose purpose is to provide internal and external connectivity to network and system resources as well as the Internet.
- **Management Network:** a restricted network that contains ITS network devices, such as network firewalls, routers, switches and managing servers, used in providing and controlling access to Loyola's network.
- **High Security DMZ:** a restricted access network, or group of networks, whose purpose is to publish high security content for public and/or Internet consumption. This zone will contain ITS resources that serve as an interface for the protected, mission critical systems. Only traffic that has previously been justified will be allowed to enter and leave this security zone.
- **High Security Internal:** a highly restricted network, or group of networks, whose purpose is to protect Loyola mission critical resources. This security zone will store, transmit or process Loyola Protected and Sensitive data (see Data Classification Policy). Only traffic that has previously been justified will be allowed to enter and leave this security zone.

Firewall Ruleset

Each network security zone shall have a different set of access restrictions applied to them, ranging from least restrictive to most restrictive. The ruleset for each network security zone is located in the ITS Network Firewall Supporting Documentation document.

All ports opened within either of the High Security DMZ, High Security Internal and the Management Network zone must have accompanied justification, documented within ITS Network Firewall Supporting Documentation, as well as an approved change management ticket.

Administrative Access

All administrative access to Loyola network firewalls will be governed by the following rules:

- All administrative users must authenticate using LDAP after connecting to LSA using Multi-Factor Authentication. A backup administrator account shall be used only for console access.
- All administrative access shall be encrypted, at a minimum, via the following method: AES 128 bit.
- All administrative access shall be restricted to networks and hosts as identified in the ITS Network Firewall Supporting Documentation document.

Each network firewall will present the following login banner when a user logs in to the device:

"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action in

accordance with the appropriate handbook and may be reported to law enforcement. There is no right to privacy on this device."

Logging

All network firewalls will be configured to use the syslog protocol for system log transport and abide by the audit and logging strategy based on the ITS Log Management Standard.

Addressing

No private address, as defined in RFC 1918, shall ever be routed to the Internet. Port Address Translation (PAT) or Network Address Translation (NAT) will be used to shield all internal addresses from being reveled externally.

Firewall Rule Set / Open Port Validation

To verify that there are no undocumented openings to the Internet, a bi-annually review of the firewall rule set will be performed by a joint team consisting of one member from each of the University Information Security Office and Network Infrastructure Services. This review will follow the PCI-DSS Firewall Rule Review Procedure.

Baseline Security Configuration

All vendor-supplied defaults must be changed. All unnecessary default accounts must be removed or disabled before installing a firewall on the network. This applies to ALL default passwords, including but not limited to those used by the operating system, software that provides security services, application and system accounts, Simple Network Management Protocol (SNMP) community strings, etc.

IV. Related Documents and Forms

Not applicable.

V. Roles and Responsibilities

Chief Information Security Officer	Enforcing the Network Firewall Standard at the University by setting the necessary requirements

VI. Related Policies

Please see below for additional related policies:

- ITS Log Management Standard
- Data Classification Policy
- PCI-DSS Firewall Rule Review Procedure

Approval Authority:	ITESC	**Approval Date:**	April 15th, 2016
Review Authority:	Jim Pardonek	**Review Date:**	July 31st, 2024
Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu