Lebanese American University

Information Security Regulations

Firewall Regulations

Last Updated: June 2017
Version 1.2

Overview

Firewalls are an essential component of LAU's network infrastructure. Firewalls are defined as security systems that control and restrict network connectivity and network services. Firewalls establish a control point where access controls may be enforced. Connectivity defines which computer systems are permitted to exchange information. A service is sometimes called an application, and it refers to the way for information to flow through a firewall. Examples of services include file transfer protocol (FTP) and web browsing (HTTP).

Purpose

The firewall regulations define the essential rules regarding the management and maintenance of firewalls at LAU and they apply to all firewalls owned, rented, leased, or otherwise controlled by LAU employees.

Scope

These firewall regulations apply on all firewalls on LAU networks, whether managed by LAU employees or by third parties.

Regulations

Internet Access

All Internet access from systems connected to the LAU networks must be routed through a firewall.

Firewall Change Control

Because firewalls support vital LAU information systems activities, they are considered to be critical systems. Firewall rules, defining permitted and denied services and connections, must be documented and reviewed at least twice a year by the IT Security Department. Major changes to LAU's internal networking environment, or any changes to the production business applications supported or any major information security incident must trigger an immediate review of or update if needed the firewall rules. The same documentation that is required for changes on production systems could also be used for firewall changes.

Firewall Configuration

All LAU firewalls connecting to the Internet must be configured so that every Internet service is disabled by default, with only those services enabled that have been requested through the Firewall Change Control.

Firewall Appliances

All firewalls used to protect the LAU internal network must run on separate dedicated appliances that serve no other purpose.

Internet Firewall Administrator Access

All LAU Internet-connected firewalls must have back channel access that will permit an authorized firewall administrator to establish a connection in the midst of a distributed denial of service attack.

Internet Server Firewalls

All University servers connected to the Internet must be protected by firewalls in a demilitarized zone.

Immediate Local Backup of Firewalls After Deployment

LAU firewalls must be fully backed-up immediately after deployment and regularly thereafter using a dedicated backup system or encrypting the backup files when using the centralized network backup system.

Remote Access to Firewalls

Remote management facilities for LAU firewalls must consistently employ session encryption and remote machine address restrictions.

Logs

All changes to firewall configuration parameters, enabled services and traffic logs must be logged. All suspicious activity that might be an indication of either unauthorized usage or an attempt to compromise security measures must also be logged. These logs must be stored for at least 12 months after the time they were recorded and must be reviewed periodically to ensure that the firewalls are operating in a secure manner.

External Connections

All in-bound Internet connections to LAU's networks must pass through a firewall.

Disclosure of Internal Network Information

The internal system addresses, configurations, products deployed, and related system design information for LAU networked systems must be restricted such that both systems and users outside LAU's internal network cannot access this information.

Posting Updates

LAU's firewalls must be running the latest stable release recommended and approved by the involved vender.

Monitoring Vulnerabilities

The firewall administrator must subscribe to the Computer Emergency Response Team advisories and other relevant sources providing current information about firewall vulnerabilities. Any vulnerability that appears to affect LAU networks and systems must be promptly brought to the attention of the IT Security department.