Firewall Policy

Summary

Maintaining a safe and secure computing environment is one of CSU's information technology priorities. Historically, the risk of malicious packets entering university networks has been relatively high, and CSU is no exception. Assets at risk include data stored on servers, software and hardware, and access to the internet itself.

A perimeter firewall is the first line of protection for the campus network and an important measure in providing for the confidentiality, integrity, and availability of CSU's data and computing resources. One firewall design theory restricts access to unauthorized users while allowing access to authorized users located outside the firewall (users on the Internet).

The method for attaining this goal is a "deny everything, permit on exception" configuration approach. While this method does protect against many intrusions, it is not bulletproof. Therefore, the firewall architecture includes features that provide the forensic information needed to investigate violations.

Purpose

The CSU Firewall Policy governs how perimeter firewalls mitigate risks and losses associated with security threats to the University's network and information systems. The policy establishes procedures and responsibilities for CSU perimeter firewall administration, determines the technology standard used by the firewall hardware and software, and defines the filters applied to campus networks.

Policy

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

- Outbound - Allow ALL Internet traffic to hosts and services outside of the campus with the exception of known security vulnerabilities. This allows anyone connected to the CSU network to utilize all services on the Internet with the exception of known vulnerabilities.
- Inbound – Internet users can only access specific services that support the University mission

Procedures

Faculty, staff, and students may request access from the Internet to a service inside CSU's firewall. They must submit these requests via eQuest (faculty/staff) or the UITS Help Desk (students) and need to include a rationale for the request.

The Network Services Team and Information Security Officer 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 objectionable, the network administrator and requester can explore alternative solutions.

Turn around time for a request of common services (listed below) will be no more than two business days from the receipt of the request. Common services include:

- FTP
- Telnet/SSH
- SMTP
- HTTP/HTTPS

Turnaround time of a request for any other service will be no more than five business days. Investigation of associated risks requires this additional time.

Responsibilities

While responsibility for information systems security on a day-to-day basis is every user's responsibility, specific guidance and direction for information systems security is the responsibility of UITS. Accordingly, UITS is solely responsible for implementing and maintaining CSU's perimeter firewalls and all other activities related to this policy.

It is a violation of policy for anyone to attempt to bypass, penetrate, alter the configuration of, or otherwise affect the operation of any firewall or other network infrastructure device unless they are an authorized administrator of the device or are a member of UITS and in the execution of their duties.

Related USG Policy

3.4 (IT Handbook) Network Services & 5.13 (IT Handbook) Domain Name System

Last Update

3/14/2014

Responsible Authority

Chief Information Security Officer