Overview

Among a university's information technology priorities is the maintenance of a safe and secure computing environment. Historically, the risk of malicious packets entering university networks has been relatively high. Assets at risk include information resources, software and hardware, and services, including access to the Internet and access to central servers. Often, data stored on servers are the true targets of attack. While protecting the network from attack, the UTHSC perimeter firewall(s) must also allow access to protected resources from authorized users located outside the firewall. An increasing number of users work at home or while traveling. Research collaborators may also need to enter the UTHSC network from remote hosts. While firewalls do protect against many intrusions, they are not bullet proof. When a violation is suspected, the firewall architecture has logging capabilities to provide forensic information.

Purpose

The UTHSC operates perimeter firewalls or gateways between the Internet and the University network to establish a more secure environment for the University's computer and network resources. The University's perimeter firewalls are key components of the University's network security architecture. The University Firewall Policy governs how perimeter firewalls will filter internet traffic to mitigate risks and losses associated with security threats to the University's network and information systems.

Scope

This Policy, although focusing on perimeter firewalls, applies to all firewalls on the UTHSC network. While responsibility for day-to-day security of users' computing devices falls primarily on individuals (i.e. students, faculty, staff, etc.), specific guidance and direction for campus wide information systems security is the responsibility of the UTHSC Security Team. The Security Team is responsible for implementing and maintaining the University network's perimeter firewalls as well as other perimeter control devices such as intrusion detection systems (IDS), switches, routers, and firewalls placed in segmentation points of the campus network. The Security Team is, therefore, responsible for activities relating to this policy.

Definitions

Intrusion detection:	A process that enhances the identification of threats
UTHSC device:	A device with computing capability that is connected to the UTHSC network
External device:	A device with computing capability that is NOT connected to the UTHSC network
Outbound traffic:	Traffic from a UTHSC device to an external device
Inbound traffic:	Traffic from an external device to a UTHSC device
Connection initiation:	The act of a device sending a network connection request to another device
Outbound initiation:	A connection request from a UTHSC device to an external device
Inbound initiation:	A connection request from an external device to a UTHSC device

Open Zone or DMZ: A network segment with a less restricted set of internet access rules than the corporate production network. Also called DMZ

Internet facing: The condition of a (UTHSC) device that will accept inbound connection requests from devices on the internet

Segmentation level: The network behind a major network branching point

Policy

1. ALL firewalls on the University network including personal firewalls shall be registered, documented and accessible to UTHSC Security Team staff.

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

Perimeter Firewall Configuration

3. The perimeter firewall permits all traffic to and from UTHSC devices which have initiated a connection with an external device with two exceptions:

   a. Traffic known to be problematic or malicious will be blocked at the network boundary.

   b. Traffic from internal servers providing only services for University use will be blocked at the network boundary to prevent University confidential and mission critical information from being transmitted to the internet.

4. The perimeter firewall will permit internet traffic from outside the University that supports the mission of the Institution as defined by the UTHSC Security Director. The UTHSC Security Director is defined by the University and can be an individual or group making these decisions. There are three methods or configurations that are applicable to inbound traffic:

   a. Secure inbound VPN traffic from the internet to UTHSC is allowed.

      A Virtual Private Network (VPN) connection to UTHSC allows a private client connection to the UTHSC network. It emulates a workstation internally connected to the campus network. VPN connections are useful for connections from home or when traveling. VPN clients must have approved antivirus software with current virus definitions. (**REFERENCE Remote Access Addendum).**

   b. Inbound connections from external devices to UTHSC servers located in the network Open Zone or DMZ are allowed.

      Server devices can be physically or virtually located in the Open Zone to accept connections from the external devices. The benefit of this is an increased security of the University network.

c. Inbound connections from external devices to UTHSC internal devices are the least secure and the most problematic configurations that the University can use for inbound initiated connections. As a result, permission is needed for the security variance it causes. Written requests for security variances to accommodate specific business needs and mission-critical functions will be considered on an individual basis.

==========

The UTHSC Multi-Layer-Approach to Network Security [i.e. Defense-In-Depth] (Summary)

Tier 1 - Internet perimeter connection for the UTHSC

- Consists of a perimeter firewall, Intrusion Detection (IDS) and VPN concentrator;
- For detecting and stopping significant numbers of security breaches and intrusions;
- Configure IDS to monitor incoming threats (scans/probes) to the UTHSC Network;
- Encryption between clients located anywhere in the world and to the university;

Tier 2 - Segmentation layer

- Consists of routers, IDS's, and firewalls (as needed) at the segmentation level;
- For internal units and University infrastructure servers;
- IDS helps identify and flag harm to internal university machines or external computers, in real time;

Tier 3 - Desktop machine, File Servers or UTHSC customer

- The responsibility of the end user and departmental administrators;
- Personal firewall, where appropriate, and approved anti-virus software with current descriptions to protect the individual machine **(Reference Anti-virus Addendum)**;
- Responsibilities include: **(Reference General Computing Device addendum)** installing updates and patches on a regular basis, **(Reference Patch Update Addendum)**,
  performing regular backups to prevent data loss, and **(Reference Backup Addendum)**, using strong passwords and changing them periodically. **(Reference Password Addendum)**

==========

Enforcement

Reference **Enforcement** in Acceptable Use Document

Additional Information

Any inquiries relating to this Firewall Policy should be directed to the Security Director.