Policy Title: Firewall

Policy Type: Technology **New/revised:** Revised

Old Policy #: Firewall

Approval level: ☐ Board of Trustees
☒ President
☐ Vice President
☐ Other (specify here)

Purpose: East Tennessee State University operates Perimeter Firewalls or gateways between the Internet and the university network to establish a secure environment for the university's computing and network resources. The University's Perimeter Firewalls are key components of the University's Network Security Architecture. The University Perimeter Firewall Policy governs how the Perimeter Firewalls will filter Internet traffic to mitigate the risks and losses associated with security threats to the University's network and information systems.

Policy:

Among a university's information technology priorities is the maintenance of a safe and secure computing environment. Historically, the risk of malicious packets making it into the university network has been relatively high. The assets at risk from targeted attacks against the network include data/information, software, and hardware. Services, including access to the Internet and access to central servers, are also at risk. Often, the data that is stored on such servers are the true targets of attackers.

Firewalls are purpose-built computers that examine network traffic. Firewalls determine where the traffic came from, where it's going, and determine the type of traffic. Based on this information firewalls decide to either allow traffic onto the network, or to block the traffic. Decisions to either allow or block traffic is governed by a set of rules configured inside the firewall. These rules are maintained by the firewall administrators and operate as follows.

When outside traffic arrives at the firewall, the firewall inspects the traffic and searches for a rule that tells it how to treat the traffic. If it finds a rule telling it to let the traffic pass, it allows the traffic inside. If no such rule is found, the traffic is blocked and may not enter. There must be a rule, for example, to allow someone on the Internet to view the University's web site. Such a rule is currently configured on the Perimeter Firewalls. If it were to be removed, the University's web site would be inaccessible to anyone not connected to the inside (ETSU) network.

Care must be taken when configuring the firewall rules. While we do want to allow traffic to the University's web server, we don't necessarily want that same traffic to be allowed to any other computer on the ETSU network. Allowing traffic to pass too freely increases risk to the University. This risk may be manifested by malware, denial-of-service attacks, client-side exploits, and various other vulnerabilities.

The University's Perimeter Firewalls help mitigate the risk of intrusion from outside entities. Exemptions may be granted under certain circumstances to allow outside traffic to access services located inside the ETSU network. While this method does protect against many intrusions, it is not invincible. When a violation is suspected, the firewall architecture has logging capabilities to provide forensic information.

Responsibilities

Information Technology Services (ITS) is responsible for implementing and maintaining the University's Perimeter Firewalls. Therefore, ITS is also responsible for activities relating to this policy. Accordingly, ITS will manage the configuration of the University's Perimeter Firewalls.

Policy for Perimeter Firewalls

The Perimeter Firewall permits the following for outbound and inbound Internet traffic:

- Outbound -- Allow ALL Internet traffic to hosts and services outside of the University.
- Inbound -- Allow Internet traffic from outside the University that supports the mission of the University after approval of a firewall exemption request

Operational Procedures

Faculty and staff may request access from the Internet for service inside ETSU for a new or existing server by requesting a firewall exemption. These requests can be made by submitting a Network Security Request Form. The request must include:

- A written rationale for the exemption request.
- The server hostname.
- The server IP address.
- The TCP or UDP ports required.
- The effective date & expiration date.

ITS 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 original requestor and alternative solutions will be explored. ITS reserves the right to review and remove firewall exemptions that exceed acceptable risk.

Policy Dispute

The Chief Information Officer and Senior Vice Provost for Information Technology Services, is charged with the responsibility to periodically review the policy and propose changes as needed.

Notes:

Approved: Information Technology Governance Council
Reviewed: February 2017
Active since: March 2010

3/24/2017 – approved by the Board of Trustees.