Firewall Policy

Document Number: ITS-0011

Date Published(sys): 7/8/2021

General Description

Purpose:

The purpose of this document is to establish an understanding of the function that a firewall plays in the overall security of Trinity University's network.

Policy Content

1 Summary

The Trinity University department of Information Technology Services (ITS) manages a perimeter firewall with a backup firewall between its Internet connection and the Trinity University campus network to establish a secure environment for the campus network and computer resources. This firewall filters Internet traffic to mitigate the risks and potential losses associated with security threats to the campus network and information systems.

Firewall configuration rules and permissible services rules have been reached after an extended evaluation of cost and benefits. These rules must not be changed unless the permission of both the Information Security Administrator and the Director and Chief Information Technology Officer has first been obtained. Request to change the Trinity University firewall rules must be submitted in writing or electronically including a rationale for the request. Firewall changes will be implemented by a Senior Level Systems Administrator. All changes to firewall configuration parameters, enabled services, and permitted connectivity must be logged. These logs must be reviewed periodically to ensure that the firewalls are operating in a secure manner.

The authorized Senior Level Systems Administrator 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.

All Trinity University firewalls must be located in locked rooms accessible only to those who must have

physical access to such firewalls to perform the tasks assigned by management. The placement of firewalls in the open area within a general purpose data processing center is prohibited, although placement within separately locked rooms or areas which themselves are within a general data processing center is acceptable.

② Configuration

The firewall will be configured to deny any service unless it is expressly permitted.

- If there are no rules defined for a University network address, then traffic to or from that address must be denied.
- Access to the University network must be blocked during the start-up procedure of the firewall.

The firewall Operating System will be configured for maximum security.

- The underlying operating systems of firewall hosts must be configured for maximum security including the disabling of any unused services.

The firewall product suite must reside on dedicated hardware.

- Applications that could interfere with, and thus compromise, the security and effectiveness of the firewall products must not be allowed to run on the host machine.

The initial build and configuration of the firewall must be fully documented.

- This provides a baseline description of the firewall system to which all subsequent changes can be applied. This permits tracking of all changes to ensure a consistent and known state is maintained.

Security must not be compromised by the failure of any firewall component.

- If any component of the firewall fails, the default response will be to immediately prevent any further access, both "outbound" as well as "inbound."
- A firewall component is any piece of hardware or software that is an integral part of the firewall system. A hardware failure occurs when equipment malfunctions or is switched off. A software failure can occur for many reasons e.g. bad maintenance of the rules database on the firewall or software which is incorrectly installed or upgraded.
- IP forwarding at the operating system level must be disabled until the firewall software is operational and IP filtering policies active.

Request a Firewall

Revision Management

Revision History Log:

Revision #:	Date:	Recorded By:
v1.0	8/14/2019 3:00 PM	Courtney Cunningham

Vice President Approval:

Enter Vice President(s) that are responsible for approving this document

Name:	Title:
Gary Logan	Vice President for Finance & Administration