Firewall Policy

Created by Webster, James D on Jun 04, 2015

Purpose

The purpose of this policy is to explain how the Information Technology Center at UMES ensures the security and reliable performance of the campus network through the use of a perimeter firewall.

Introduction

We at the Information Technology Center recognize that constant attempts are made around the world to gain unauthorized access to private and sensitive information stored on computers. This constant barrage of reconnaissance and attacks on vulnerable systems puts all internet connected devices at risk. In order to protect University assets, the IT department has implemented a perimeter firewall as the first in a series of security layers.

A firewall, by definition, allows or disallows network access based on a defined policy. The UMES firewall policy must serve the purpose of protecting university assets from being compromised while at the same time ensuring access to necessary services. The academic mission of the university must not be compromised. Therefore, the following policy has been implemented.

Policy

Outbound Traffic

All outbound traffic to hosts and services will be allowed with the following exceptions:

1. Any website or service deemed to be malicious or harmful to the operation of the UMES network or its academic mission.
2. Traffic originating from networked computing equipment designated for a specific use where internet access is not necessary (i.e., HVAC control or time clocks)
3. Web traffic originating from designated controlled areas such as a computer lab designated for a specific purpose.
4. Any traffic that jeopardizes the integrity of the UMES network.
5. Any traffic that jeopardizes the integrity of systems outside of the UMES network.

Inbound Traffic

All traffic from external hosts to internal hosts (including the firewall itself) will be blocked with the following exceptions:

1. Public services to specific servers that are necessary for the operation of the university (i.e., campus website).

2. Connections from a designated outside source to a specific host that are necessary to the academic mission of UMES. Such connections must be requested and will be reviewed for approval by the firewall administrator. (see Exception Requests)
3. VPN connections that have been reviewed and approved by the firewall administrator.

Exception Requests

Faculty and staff may request that access to the internal network be granted to an internal host for legitimate university business. Such requests will be made by a supervisor or department head. Requests must be submitted using the appropriate request form. The form must be filled out in full.

The firewall administrator will review the risks involved with the request. If the risks are acceptable the request will be granted. If the risks are questionable or even unacceptable the firewall administrator will explore alternatives and present them to the requestor. If the alternative is acceptable, it will be implemented. If no alternative can be found the request will be denied and the requestor will receive an explanation of said denial. All firewall rules will be reviewed quarterly to ensure there are no outdated rules that may compromise the security of the network. Requestors will be contacted via email and asked if they still require the exception. If the exception is no longer necessary, it will be removed from the firewall. If the requestor does not respond within a reasonable amount of time the exception will be removed and a new request shall be submitted if necessary. The IT department reserves the right to immediately remove any exception that jeopardizes campus assets.

Violations

Any attempt to bypass or breach the firewall is a direct violation of firewall policy and will result in the immediate denial of network connectivity. Changes in firewall configuration shall only be made by authorized administrators in the Information Technology department.