Firewall Updates Policy at UMSL

The firewall is an essential component of the overall security of the UMSL computer network. Improper configuration or mismanagement of this device can severely degrade the effectiveness of the security program while at the same time making the network susceptible to malicious attacks or completely unavailable to the internet.

Audience

UMSL Network and Security Administrators with access to update the firewall, and any individual who may be requesting changes to it.

Definition

The campus firewall is our main security device that separates the UMSL network from the rest of the world. It is also used to separate certain internal networks from one another.

Policy Statement

The intent of this policy is to provide guidance and structure for the day to day administration of the UMSL firewall as it relates to the network security and administration teams. It is designed to provide instructions on authorizations, implementation and any signoffs needed for firewall changes.

Procedures and Guidelines

It is important that strict guidelines be established and followed so that only necessary and effective changes are made to the firewall.

Requesting information related to the firewall rule-base.

- Information regarding specific rules or configurations will be disclosed only by specific members of our IT Security team on a strict need to know basis.

Requesting a change to the firewall rule-base.

- Individuals requiring a change to the firewall rule-base must submit a request using the firewall rule request form located at http://www.umsl.edu/technology/security

Prioritization of Firewall Change Requests

There are 2 main priority categories, they are routine and emergency.

- Routine firewall changes are usually made weekly when needed. They are typically made during off business hours. These changes include the updating, adding or deleting of firewall rules. These rules are to be approved by our IT Security Administrator. They are usually made within 5 to 7 days of their request and approval.

- Emergency firewall changes are made as soon as possible. These can be made at anytime during the day. These changes include hardware repairs due to failure, rules that are blocking or will allow access to critical services that are needed for business with no workaround, or any updates needed to bring back up a down network.

Emergency changes can be made without the approval of the IT Security Administrator or the Network Manager if the need arises. Typically these changes will be approved by the IT Security Administrator or the Network Manager.

Reviewing the Firewall Change Request

- Most firewall rule changes can be approved by the IT Security Administrator. However, rules that may have a heavy impact on the entire campus or any network with compliance issues, such as HIPPA or PCI, will need to be approved by the CSIRT Team.
- When a request is accepted or rejected, the requester will be notified by email by the IT Security Team.

Firewall Rule-Base Change Implementation

- Once a rule change has been accepted, a message is sent to the requestor letting them know when the change will take place. At that scheduled time the rule is updated by a member of the IT Security Team or Networking Team. The rule is also commented in the firewall with the purpose of the rule, the date it was added or changed, and the initials of the admin who put it in place. The requestor is then contacted and asked to test the rule.
- For rules that affect larger numbers or systems, the IT Security Team will notify the Technology Support Center and the CSIRT team.

Completing Firewall Change Requests

- Once the firewall rule change has been completed. The firewall rule request form is then filed in the file cabinet in the IT Security Administrator’s office.

Periodic Reviews

- The firewall rules will be reviewed on a yearly basis to ensure validity.
- It is the responsibility of the rule requestor to notify the IT Security Team when a rule is no longer valid and needs to be removed and updated.
- All rules and configurations will also be audited by the IT Security Team.

Original Issue Date

March 2008

Revision Date