Network Firewall Standard

Objective

In accordance with the Information Security and Acceptable Use Policy, all systems owned or managed by the University of Texas at Dallas must be adequately protected to ensure confidentiality, integrity, availability, and accountability of such systems. Firewalls may be used to establish a perimeter between the University network and the public Internet, or within the University to maintain segmentation between networks.

Physical Location

Network perimeter firewalls should be installed on dedicated hardware in locked rooms that meet the applicable minimum standards defined in the Standard for Server Rooms. Use of workstation-class hardware to deliver the services of a network perimeter firewall is not recommended.

Support Requirements

All firewalls must have a valid support contract or, in the case of open-source software, be commercially or community supported.

Patching

Security patches for all firewalls must be installed in a timely manner, depending on the likelihood and impact of vulnerability exploitation.

Rules

Network firewalls must be configured to deny all traffic by default, with specific rules permitting the minimum traffic required for University operations. Global allow rules should not be enabled because they provide unnecessarily broad access. Rules are generally processed in order from the top downward, thus “deny all” rules should be placed below the explicit allows.

Rules must be appropriately documented with business justifications and reference to change control ticket number, where applicable.

Rulesets must be reviewed at least annually to ensure efficiency and ongoing justification for each rule.

Logging

Activity must be logged and retained for a minimum of 90 days to facilitate troubleshooting and investigations. The following types of activities must be logged:

- Successful and unsuccessful login attempts
- Any firewall modification operation

- Rejected connection attempts; logging of allowed connections is recommended when feasible
- Number of hits for each rule should be logged, to assist in the identification of rules that may not be needed or are redundant with other rules

Logs should also be sent to a centralized logging server to reduce storage requirements on local systems and reduce feasibility of log tampering.

Incident Management

System owners are required to report any suspicious activity to the Information Security Office for investigation.

Backup / Recovery

Backup and recovery procedures must be established to ensure that firewalls can be rebuilt in the event of a disruptive event. Further, configuration backups should be captured before significant configuration changes to ensure a method of failing back after an unexpected disruption. Backup media should be encrypted if transported or stored outside of a UTD facility.

Exemptions

In the event that compliance with this standard cannot be met, please contact infosecurity@utdallas.edu to submit an exemption request which will be approved or denied by the CISO. Denied exemption requests may be appealed to the UTD President for final decision.