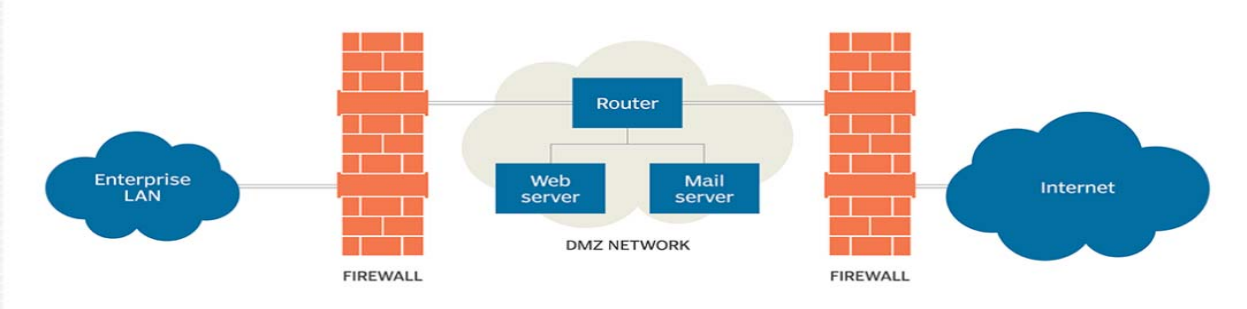
Arizona State University
Office of University Audits
Firewall-Perimeter Security
October 2, 2019

Summary:

The Firewall-Perimeter Security audit was included in the Arizona State University (ASU) FY 2019 audit plan approved by the Arizona Board of Regents (ABOR) Audit Committee and ASU senior leadership. The audit focused on the design and effectiveness of security controls related to enterprise managed firewall and network perimeter devices. This audit is in support of ASU's mission of preserving the availability, confidentiality, and integrity of its information resources.

Background:

A firewall is a network security system that monitors and controls incoming and outgoing traffic based on predetermined security rules. They act as a first line of defense in network security by acting as a barrier between internal networks and external networks, such as the internet as well as to further segment and restrict internal networks. There are various types of firewalls that address the different types of traffic and provide varying levels of protection; however, multiple layers of firewalls are generally utilized to increase overall security posture.



ASU uses a multilayer security approach that relies heavily on protection from border security devices such as border firewalls as well as internal firewalls. The University Technology Office (UTO) is responsible for oversight and management of all enterprise firewalls, including border firewalls and internal firewalls. Management of border firewall devices is outsourced to vendor/partners, while internal firewalls are managed by UTO.

Audit Objective: The objective of this engagement was to assess the design and effectiveness of controls related to border and departmental firewalls including the following areas:

- Ensure firewalls have logical access appropriately restricted
- Confirm firewalls are compliant with the ASU Password Standard
- Confirm changes to the firewalls, including applying patches, follow the ASU Change Management Standard
- Ensure firewalls are scanned and remediated based on the ASU Vulnerability Management Standard

- Ensure firewall rulesets are configured appropriately
- Identify opportunities for improvement

Scope: The scope of the audit focused on enterprise managed firewalls including both perimeter firewalls as well as departmental firewalls. The period considered in this review was January 2018 – June 2019. This audit utilized a commercial auditing tool to assess the appropriateness of firewall rules.

Vulnerability management was included in the scope of this review; however, could not be fully assessed due to the department or third party not actively scanning the devices or management consoles for performance and availability reasons. Other manual processes have been implemented such as receiving notifications directly from the vendor; however, these are not formally documented. Testing identified 19 unique potential vulnerabilities (2 critical, 5 high, and 12 medium) spanning four firewalls. These were confirmed as false positives by the firewall owner with the exception of three high-risk vulnerabilities related to one firewall. The firewall owner confirmed that the affected firewall is scheduled for replacement within the next three months.

Methodology: Our audit consisted of tests of procedures necessary to provide a reasonable basis for expressing our opinion. Specifically, audit work consisted of interviews with the firewall owners, observation of work processes, review of documented policies and procedures, and substantive tests for a sample of 26 firewalls including the following areas:

- Validating logical access through the following procedures:
    - Validating unique user IDs are utilized through review of access listing
    - Performing a high-level access review based on job title and department
    - Ensuring privileged access is appropriately restricted
    - Ensuring access is restricted to affiliated individuals
- Reviewing configuration to ensure password complexity requirements are met in addition to confirming passwords are encrypted at rest.
- Reviewing configuration to ensure idle lock requirements have been met.
- Validating firewall changes follow the defined Enterprise System Change Management Standard by reviewing a sample of 64 change records spanning border and department firewalls.
- Confirming firewalls are updated with vendor provided patches based on the defined Patch Management Standard by reviewing a sample of nine changes related to patches.

- Confirming logging has been implemented to capture appropriate detail related to firewall changes and that logs are retained for a minimum of one year through observation of log detail and tracing changes identified through the change management process to the enterprise-level log management system.
- Assessing the appropriateness of firewall rulesets and potential vulnerabilities utilizing the NIPPER auditing tool for 22 of the firewalls selected. The tool was not compatible with four of the firewalls selected for testing. In these instances, rulesets were not assessed.

Conclusion: UTO has implemented effective controls to ensure border network traffic is appropriately restricted; however, existing processes do not ensure that department firewall rules are adequately maintained to ensure rules are relevant and still necessary. Specifically, three high-risk configuration errors were identified on 16 department firewalls. Additionally, department firewalls do not have adequate documentation to support why some rules have been implemented. Firewalls can have hundreds of rules established that can go back multiple years resulting in a lack of continuity of resources managing the change process. Without an effective firewall rule management process, rules may not be properly managed resulting in potential increased network vulnerability or performance issues. This is further compounded by informal change management processes.

In addition, issues were noted in several security control areas. Logical access was not appropriately restricted in addition to a shared administrator account being utilized on one of the border firewalls. It was also noted that the border firewalls did not require multi-factor authentication as required by the Privileged Accounts Standard to minimize the risk of privileged accounts being compromised. Testing also identified that border and departmental firewalls did not meet required password complexity rules or session lockout best practices. During the course of the audit, issues related to logical access, password complexity, session lockout configuration, and multi-factor authentication were remediated.

Change management and logging processes have been implemented; however, require further improvement. Generally, border firewalls follow the defined change management process with the exception of completing the planning aspect of the change record, which is important to ensure there is consideration of necessary steps if the change does not go as planned. Testing also indicated that informal processes are generally followed for department firewalls, which do not follow the Enterprise Change Management Standard. It was also noted that existing system logging practices do not ensure detailed logging of border firewall changes are captured in addition to logs not being retained for the required retention period.

The control standards University Audit considered during this audit and the status of the related control environment are provided in the following table.

General Control Standard (The bulleted items are internal control objectives that apply to the general control standards, and will differ for each audit.)	**Control Environment**	**Finding No.**	**Page No.**
Reliability and Integrity of Financial and Operational Information	Not Applicable	N/A	N/A
Effectiveness and Efficiency of Operations			
• Firewall rules are configured to appropriately restrict network traffic.	Opportunity for Improvement	1	6
• Logical access to firewalls is appropriately restricted.	Opportunity for Improvement	N/A	N/A
• Password requirements and complexity configuration meet the defined Information Security Policy.	Opportunity for Improvement	N/A	N/A
• Idle session / screen lock is configured to meet ASU's best practice.	Opportunity for Improvement	N/A	N/A
• Encryption is implemented to meet the defined Privileged Accounts Standard.	Reasonable to Strong Controls in Place.	N/A	N/A
• Multi-Factor authentication is required to access border firewalls.	Opportunity for Improvement	N/A	N/A
• Change Management is implemented to meet the defined Enterprise System Change Management Standard.	Opportunity for Improvement	2	7
• Patch Management is implemented to meet the defined Patch Management Standard.	Reasonable to Strong Controls in Place.	N/A	N/A
• Logging has been implemented to capture appropriate level of detail to identify changes to firewall configuration.	Opportunity for Improvement	3	8
Safeguarding of Assets	Not Applicable	N/A	N/A
Compliance with Laws and Regulations	Not Applicable	N/A	N/A

We appreciate the assistance of UTO during the audit.

Lisa Grace, Executive Director, University Audit and Advisory Services
David Jones, SR IT Auditor, University Audit and Advisory Services

Audit Results, Recommendations, and Responses

1. Processes have not been implemented to periodically review and assess department firewalls resulting in some department firewalls not being configured to appropriately restrict network traffic.

Condition: Configuration errors were noted in department firewalls in addition to some department firewall rulesets not having adequate documentation related to established rules to justify why the rule was implemented or if it is still necessary.

Criteria: Firewall rulesets should be formally documented to ensure all rules are appropriate and still required. Firewalls can have hundreds of rules established that can go back multiple years resulting in a lack of continuity of resources managing the change process. Without an effective change management and rule management process, rules may not be properly managed resulting in increased network vulnerability.

Cause: Formalized review processes have not been implemented to assess and review firewall rulesets to ensure they are relevant and still required.

Effect: Three high-risk firewall rule configuration errors were noted through the NIPPER audit tool relating to 16 of the department firewalls tested. Configuration errors noted included: access to administrative services, clear text protocol, and packets from any source to network destination and a port range. Lower risk configuration errors that were identified as part of the assessment were not verified as part of this review; however, were provided to the department to further review and action if necessary. In addition, as part of our review, it was noted that the department firewall documentation contain out of date rule comments which indicate the rules may no longer be necessary, and rules with no comments, therefore having no documented purpose for the rule.

Recommendation: UTO should formalize documentation of firewall rules including performing a full review of existing rules to ensure they are still necessary and relevant. In addition, it is recommended that periodic reviews of firewalls be performed to ensure rules are appropriately configured to appropriately restrict network traffic.

Management Response: UTO agrees with the audit recommendation and will complete a full review of existing department firewall rules and implement a periodic review cycle by September 30, 2020.

2. UTO has implemented some processes governing change management; however, further improvement is necessary to ensure compliance with the defined Enterprise Change Management Standard.

Condition: UTO has generally implemented the standard Enterprise Change Management Process for border firewall changes, including patching; however, further enhancement is required to ensure the planning portion of the change record is consistently completed. In addition, less formal processes are followed for departmental firewalls.

Criteria: ASU's Enterprise System Change Management Process establishes a requirement for a formal change management process. It provides a framework that:

- Identifies the flow of activities, roles and responsibilities, and inputs and outputs of the ASU change process.
- Minimizes the impact of change-related incidents upon quality of service and consequently improves the day-to-day operations of the University.
- Establishes a formal process of recording, assessing, authorizing, scheduling and effectively communicating changes to ASU's technology systems.
- Provides a framework for managing IT baseline configurations and changes for all UTO-operated and managed devices.
- Ensures all changes have been properly assessed for their potential impacts to the ASU IT environment and a risk-based approval process is applied prior to implementation.
- Establishes processes for initiating, tracking and approving change requests.
- Clarifies specific roles, responsibilities and timelines related to change management.

Cause: UTO has implemented change management processes; however, do not follow them consistently to ensure all changes follow the defined standard.

Effect: Testing indicated that existing processes around change management are generally being followed; however, these processes are omitting key aspects of the change management process including planning, assessing, authorizing, scheduling, and communicating changes.

- 20 of 64 (31%) of firewall change requests did not adequately capture all necessary fields including planning, completion and closing. Of these, six were related to patches, which was also in violation of the Patch Management standard.

- The Security Operations Center utilizes blanket change requests for routine changes. These do not capture proper Change Advisory Board (CAB) approvals, nor have adequate planning details to ensure adequate implementation, testing

and rollback strategies. In some instances, it was noted that details regarding the specific change are also not captured in the task level detail as indicated by their process.

- Department firewall changes often utilize an informal process with reliance on email and internal distribution lists rather than the defined ServiceNow process.

Recommendation: UTO should further enhance their change management practices to ensure compliance with the Enterprise System Change Management Standard for ASU firewalls.

Management Response: UTO agrees with the audit recommendation. We have recently transitioned to a new ServiceNow module to enhance tracking and governance change management. Planning documentation will be required for all Enterprise managed firewalls including both perimeter firewalls as well as department firewalls by January 1, 2020.

3. Some system logging has been implemented; however, improvement is needed to meet the defined System Audit Requirements and Enterprise Change Management Standard as it relates to border firewalls.

Condition: Firewall audit logs are generally loaded to the enterprise-level log management system; however, the border firewall audit logs are not at a level of detail that captures the configuration changes made nor are they maintained for a minimum of one year as required. For one firewall, it was noted that the audit logs are not loaded to the enterprise-level log management system and is only maintained locally for seven days.

Criteria: ASU's Enterprise System Change Management Standard stipulates that a rule tracking mechanism be used that provides for change logging in order to capture all modifications to enterprise firewalls. In addition, ASU's System Audit Requirements Standard stipulates that logs must be retained per applicable ASU data retention policies, which state for a period of no less than one year.

Cause: The border firewall audit logs have not been configured to capture the level of detail required. In addition, the enterprise-level log management system has not be configured to retain the firewall audit logs for the required record retention period.

Effect: ASU does not capture adequate detail in the audit logs to ensure they can be utilized to identify and track changes made to firewall rules. This is further compounded by the inconsistent change management processes noted related to firewalls.

Recommendation: UTO should configure the firewall audit logs to capture the level of detail required by the Enterprise Change Management Standard. In addition, retention should be extended to one year. If space or performance is of concern due to the size of the logs, and approved exception should be obtained from the CISO due the criticality of the border firewalls to the overall security posture of the university.

Management Response: UTO agrees with the audit recommendation. UTO will implement audit logs to capture the level of detail required by the Enterprise Change Management Standard. In addition, UTO will confirm and receive necessary approvals to support the appropriate storage duration. Logging will be fully implemented by January 1, 2020.

Distribution:

Arizona Board of Regents Audit Committee
Michael M. Crow, President
Morgan R. Olsen, Executive Vice President, Treasurer and Chief Financial Officer
Lev Gonick, Chief Information Officer
Tina Thorstenson, Deputy Chief Information Officer and Chief Information Security Officer
Jess Evans, Chief Operating & Digital Transformation Officer
Timothy Summers, Executive Director Cloud & Advanced Network Engineering Services
Tom Castellano, Lead Architect & Senior Director of Cybersecurity
Shawn Bryan, Cloud Migration Advisor
Carolee Deuel, Director of Policy and Compliance
Internal Audit Review Board