AUDIT REPORT
Firewall
Information Technology
June 2022

Internal Audit Department
City of Fort Smith, Arkansas
Tracey Shockley, CFE, CCA
Internal Audit Director

Our Mission

We deliver independent, transparent, and professional audits in order to safeguard and improve the public's investment in the City of Fort Smith. Our work is performed on behalf of everyone who cares about the City, including its residents, workers, and decision-makers.

BACKGROUND

What Is a Firewall?

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow block specific traffic based on a defined set of security rules.

Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the internet. A firewall can be hardware, software, or both.

There are multiple different types of firewalls. For instance, a proxy firewall is an early type of firewall device, a proxy firewall serves as the gateway from one network to another for a specific application. Proxy servers can provide additional functionality such as content cashing and security by preventing direct connections from outside the network.

Stateful inspection firewall is now thought of as a "traditional" firewall, a stateful inspection firewall allows or blocks traffic based on state, port, and protocol. It monitors all activity from the opening of a connection until it is closed. Filtering decisions are made based on both administrator-defined rules as well as context, which refers to using information from previous connections and packets belonging to the same connection.

Unified threat management (UTM) firewall is a device that typically combines, in a loosely coupled way, the functions of a stateful inspection firewall with intrusion prevention and antivirus. It may also include additional services and often cloud management. UTMs focus on simplicity and ease of use.

Next-generation firewall (NGFW) have evolved beyond simple packet filtering and stateful inspections. Most companies are deploying next-generation firewalls to track modern threats such as advanced malware and application-layer attacks.

Threat-focused NGFW are firewalls that include all the capabilities of a traditional NGFW and also provide advanced threat detection and remediation.

Lastly, Virtual firewall is typically deployed as a virtual appliance in a private cloud (VMware ESXi, Microsoft Hyper-V, KVM) or public cloud (AWS, Azure, Google, Oracle) to monitor and secure traffic across physical and virtual networks. A virtual firewall is often a key component in software-defined networks (SDN)

Elements of an Effective Policy and Procedure

A firewall policy dictates how firewalls should handle network traffic for specific IP addresses and address ranges, protocols, applications, and content types (e.g., active content) based on the organization's information security policies. Before a firewall policy is created, some form of risk analysis should be performed to develop a list of the types of traffic needed by the organization and categorize how they must be secured—including which types of traffic can traverse a firewall under what circumstances. This risk analysis should be based on an evaluation of threats;

vulnerabilities; countermeasures in place to mitigate vulnerabilities; and the impact if systems or data are compromised. Firewall policy should be documented in the system security plan and maintained and updated frequently as classes of new attacks or vulnerabilities arise, or as the organization's needs regarding network applications change. The policy should also include specific guidance on how to address changes to the ruleset.

Lastly, a Network Firewall is required in all instances where Sensitive Data is stored or processed; a Host Firewall is required in all instances where Sensitive Data is stored or processed and the operating environment supports the implementation. Both the Network and Host Firewalls afford protection to the same operating environment, and the redundancy of controls (two separate and distinct firewalls) provides additional security in the event of a compromise or failure.

Conclusion

The objective of our audit was to evaluate the City's Firewall process. The City Administrator and the Interim ITS Department Head did not assist in providing even minimal information necessary for progressing with this audit. Additionally, the Interim ITS Department Head would not respond to meeting request or emails from Internal Audit. IA could not locate a City Firewall policy.

The City and ITS should consider the following if it does not have it established in their plans:

- Firewall rules should be documented, tracking the rule's purpose, what services or applications it affects, affected users and devices, date when the rule was added, the rule's expiration date, if applicable, and who added the rule. A good firewall policy also has a formal change procedure to manage change requests.
- Firewall policies should be based on blocking all inbound and outbound traffic, with exceptions made for desired traffic.
- Policies should take into account the source and destination of the traffic in addition to the content.
- Many types of IPv4 traffic, such as that with invalid or private addresses, should be blocked by default.
- Organizations should have policies for handling incoming and outgoing IPv6 traffic.
- An organization should determine which applications may send traffic into or out of its network and make firewall policies to block traffic for other applications.