Evaluation of Network Technologies

William Pascoe

CYB-220 Network Security

Jonathon Schumaker

December 11, 2025

Evaluation of Network Technologies

During recent times at our company there have been several incidents involving people trying to access parts of the company network that are only available to people in that department. As a result of these events, I will be discussing some security design principles that we will be employing and the technologies that will help us with these principles.

The security principle that I will be looking at is the principle of least privilege. The security design is meant to allow normal operations to continue uninhibited while also protecting against the threat of attack. This is accomplished by ensuring that all employees from the CEO to the bottom employees only have access to the minimum parts of the network that they need to accomplish their job and not be allowed access to anything else (Bocetta, 2019). By using access control lists to maintain proper role management we can ensure that internal threat actors are not breaching other departments and gaining access to sensitive information that isn't required for their job at the company.

Besides controlling access, we will employ 2 technologies to help protect and monitor our network. These technologies are Network Intrusion Protection System (NIPS) and a Host-Based Intrusion Detection System (HIDS). The NIP system is very good detecting issues across the network while the HID system is a more computer based localized protection for that particular device. Both of these systems are very effective to detect if there are intrusions into the network, to detect problems and alerts administrators to potential issues. In doing so, it plays a crucial role in minimizing the impact of cyber-attacks and fortifying network defenses (Kirvan, 2023). These systems do have a moderate to high cost associated with them for initial install and setup but with company preference to start with free and open sourced tools to start out with and purchasing higher grade tools over time we can limit our costs and control when we upgrade and the desired budget.

Implementing these systems will be a significant undertaking with our limited IT staff. We have a staff of five people including 2 recent graduates in the IT field. The network is approx. 150-200 workstations divided into 4 segments and each one, with the exception of IT, is independent. The IT department is the one department that is able to access all of the segments. With the company's utmost importance being able to identify anyone with malicious intent we will complete implementation of each system a zone at a time we should be able to get it done in a relative short amount of time.

References:

Bocetta, S. (2019, September 12). *Principle of Least Privilege: What, Why, and Best Practices*. Twilio. https://www.twilio.com/blog/principle-of-least-privilege-details-best-practices

Kirvan, P. (2023, July). *What is network intrusion protection system (NIPS)? - Definition from WhatIs.com*. WhatIs.com. https://www.techtarget.com/whatis/definition/network-intrusion-protection-system-NIPS

What is HIDS (Host-Based Intrusion Detection System)? | Sysdig. (2025). Sysdig.com. https://www.sysdig.com/learn-cloud-native/what-is-hids