Evaluation of Network Protection Technologies

Andree Salvo
Southern New Hampshire University
CYB 220-10030
7-2 Project
Instructor: Wesley Buchan

Employing a Fundamental Security Design Principle

For this project, I will apply the security design principle of defense in depth, also known as layering. This security principle is a "strategy that uses multiple security products and practices to safeguard an organization's network, web properties, and resources" (Cloudflare, n.d.). For this scenario, basic access alone isn't enough, as individuals in the Acquisitions department continue to attempt to connect to the HR network segment. To handle this situation, a layered approach includes both detection and prevention. With tools like IDS and IPS, we can keep an eye on any unauthorized attempts, block threats in real time, and monitor overall network activity. This gives us more control and awareness across the different network segments of our system. If one layer does fail or misses something, another layer is there to catch it. Using defense in depth is especially important for a financial institution like ours, where protecting sensitive data is a top priority. This also gives us flexibility, and we can start with lower-impact tools like network-based IDS for visibility and add more prevention-focused tools. This approach works well with our limited IT team and preference for open-source solutions. Defense in depth helps reduce risks, detect threats, and limit damage before it spreads through the network.

Recommended network protection approach

Looking at the Evaluation Criteria, I recommend using Network Intrusion Detection System (NIDS) and Network Intrusion Prevention System (NIPS). Using both these approaches provides real-time monitoring and active blocking. For example, "NIPS is installed with strategic points to monitor all network traffic and scans for threats." (Palo Alto Networks, n.d.). While NIDS is a "solution that analyzes traffic and tries to find unusual activities, like scanning, intrusion attempts, lateral movements, exfiltration, backdoors, command and control, etc." (TEHTRIS,

n.d.) Using both balances the effectiveness, cost, and technical side, which supports our organization's goals. However, both systems can generate alerts, but also require tuning. This is manageable over time. With a small IT staff and some newer employees, we can start with open-source tools, like Snort or Suricata. Both these tools can be used to protect our network with both detection and prevention. They also help control costs and limit deployment complexity. In conclusion, combining NIPS and NIDS, we create a layered defense known as "Defense in Depth." This will detect threats, prevent attacks, and support long-term security for the network.

Recommend resources

For the scenario that was given to us, I recommend implementing three of the resources. Firstly, with organizational assets, we can start with open-source tools like Snort, Suricata, or Wazuh. Applying these 3 open-source tools will stay within the organizational budget and have a strong detection and prevention system. Workforce allocation: At least two IT professionals should handle the workforce allocation for tuning and monitoring the networks. While the new trainees get a better understanding from two of the IT professionals on learning alert response and threat analysis when using IDS and IPS. Policies and procedures are also essential. Applying an Incident Response Plan will also help when documenting alerts. According to CISA.gov, "An Incident Response Plan is a written document, formally approved by the senior leadership team, that helps your organization before, during, and after a confirmed or suspected security incident. Your IRP will clarify roles and responsibilities and will guide key activities." (Cybersecurity and Infrastructure Security Agency, n.d). Additionally, on the hardware side, A server can be dedicated to run these open-source IDS and IPS tools. This setup can allow

monitoring of network traffic to occur efficiently and without interfering with normal operations, while giving full control over how these tools are configured and being maintained.

Adversarial mindset

When using an adversarial mindset, we must prepare for possible threats that people might try to access restricted areas of the network without permission. In conclusion, by adding tools, training staff, and enforcing strong policies, we can build a network capable of detecting and stopping attacks before they cause further harm.

References

Cloudflare. (n.d.). *What is defense in depth?* Cloudflare Learning Center. Retrieved June 17, 2025, from https://www.cloudflare.com/learning/security/glossary/what-is-defense-in-depth/

Palo Alto Networks. (n.d.). *What is an intrusion prevention system (IPS)?* In *Cyberpedia*. Retrieved from Palo Alto Networks website: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips paloaltonetworks.com

TEHTRIS. (n.d.). *NIDS (Network Intrusion Detection System)*. Retrieved from https://tehtris.com/en/glossary/nids-network-intrusion-detection-system/

Cybersecurity and Infrastructure Security Agency. (n.d). *Incident response plan (IRP) basics* (Pub. No. IRP-Basics). U.S. Department of Homeland Security. Retrieved from https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf