Protection and Limitations of Current Network Defense Technologies

Truc L. Huynh, Computer Science

Purdue University Fort Wayne

**Protection and Limitations of Current Network Defense Technologies**

Modern network defense technologies such as network access control (NAC) systems, firewalls, virtual LANs, and IDS/IPSs… have their strengths and weaknesses.

According to (1), Network Access Control (NAC) allows networks to require users to authenticate the network. It can also use the software on systems to access those systems’ security and compliance data. If the user is validated properly, the user can then be placed into the proper network segment based on his or her user’s right. While NAC has been around for a while it shows age and possible evolving threat landscaping: limited granular control & segmentation capabilities; no support for wired users or IoT or OT (limited access for these devices); no continuous verification after initial authorization (only verified at the point of authentication) … (2)

Network firewalls use a set of rules about “which traffic may travel to them based on the network address, ports, protocols, or details of the traffic sent”. The list of rules is known as the rulesets, and the firewall administrator managed their firewall rulesets carefully to ensure that only allow, trusted traffic is passed through (1). Although firewalls are a commonly used tool to secure networks, there are some drawbacks: IP-based policies are hard to manage; Firewall policies are statically configured and cumbersome to manage and update and often based on traditional networking constructs; access is based on location; challenging to create policies for on-prem and remote users… (2)

The intrusions Detection and Prevention systems are a combination of Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs). IDSs detect the network’s attacks based on the network’s signatures or their behaviors. IPSs is the act of putting the IDSs in between the attackers and their victims and allowing the victim’s system to detect and prevent the attacks.

A Virtual Private Network (VPN) uses software and network protocols to build a private channel through other networks. VPNs are often, but not always, encrypted, allowing a separate, secure network path through otherwise public or untrusted networks. VPNs are also used to connect remote networks to third-party infrastructure such as the Internet. VPN setup between two side can allow those side to appear to be directly connected, although they're not actually both connected to the same physical network. This can cause security flaws such as attackers can gain VPN credentials from unpatched VPN devices (1).

References

Chapple, M., & Seidl, D. (2023). Chapter 12: Computer Network Defense. In *Cyberwarfare: Information Operations in a Connected World* (Second, pp. 9–20). essay, Jones & Bartlett Learning. (1)

Pithawala, B., (2021) Overcoming the Limitations of VPN, NAC, and Firewalls with ZTA. Retrieved from [Overcoming the Limitations of VPN, NAC, and Firewalls with ZTA (elisity.com)](https://blog.elisity.com/zta-vs-vpn-nac-firewalls#:~:text=NAC%20provides%20binary%20network%20access%20%28either%20%22on%22%20or,NAC%2C%20there%20is%20no%20continuous%20verification%20of%20authorization.)