**Introduction**

Availability is a core tenet of information security (Cawthra, 2020). As such it is important for a network to achieve high uptime, and withstand denial of service (DoS) attacks. This post will briefly discuss DoS and two technologies one can employ to mitigate this threat.

**What is a DoS attack?**

A DoS attack is used by a hostile actor to consume the resources of a network, rendering it unavailable. A distributed denial of service (DDoS) is similar, however will use more than one host, known as a botnet, in order to achieve it’s aim (Grigutyte, 2023).

**Firewalls**

One technology used to mitigate the effects of these attacks is a firewall (Ahmed, 2022). Firewalls sit at the edge of the “trusted” network and filter traffic using a predefined set of rules. Next generation firewalls are able to use threat signatures to identify attacks like DoS (Google, 2024). However, the arrival of cloud technology is making it harder to define a network boundary and companies such as Google are opting for more modern defensive technologies to firewalls (Anderson, 2020). Commercially available networks can also be seen as expensive (Ambhore, 2020).

**Content Delivery Network**

Another technology to combat a DoS threat is a content delivery network (CDN). CDNs are a group of geographically distributed servers used by web applications to achieve high availability. This is done by caching the resource and will help reduce the strain on a single server (Cloudflare, ND). It’s important to note that CDNs aren’t completely secure. Problems have arisen with a lack of secure backend configuration and the potential for MitM (man in the middle) attacks (Shobhiri, 2023).

**Conclusion**

This post briefly discussed DoS and DDoS attacks. Two technologies to mitigate or avoid these attacks are firewalls and CDNs. Proper consideration must be taken in order to deploy these technologies effectively, ensuring their placement and configurations are correct.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**References**

Ahmed, D. & HamaAmin, R. (2022) Multi-layered firewall to mitigate the impact of Distributed Denial of Service on a network. *Passer journal of basic and applied sciences.* Available from: <https://passer.garmian.edu.krd/article_160803_447dff3e7973a3e0660bf576c7cd8250.pdf> [Accessed 07 June 2024].

Ambhore, P. & Wankhade, A. (2020) ‘Firewall for Intranet Security’, *International Conference on Mobile Computing and Sustainable Informatics*. Lalitpur, Nepal, 23 – 24 January. Springer*.* 653-659.

Anderson, R. (2020) *Security engineering: A guide to building dependable distributed systems.* Indianapolis, Indiana: John Wiley & Sons, Inc. DOI: 10.1002/9781119644682

Cawthra, J. (2020) Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events. Available from: <https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html> [Accessed 28 May 2024].

Cloudflare (ND) What is a CDN? Available from: <https://www.cloudflare.com/en-gb/learning/ddos/how-to-prevent-ddos-attacks/> [Accessed 07 June 2024].

Google (2024) Threat Signatures Overview. Available from: <https://cloud.google.com/firewall/docs/about-threats#:~:text=If%20any%20configured%20threat%20signature,profile%20on%20the%20matched%20packets>. [Accessed 29 May 2024].

Grigutyte (2023) DoS vs DDoS: A comparison and differences in the attacks. Available from: <https://nordvpn.com/blog/dos-vs-ddos/> [Accessed 07 June 2024].

Shobhiri, B. et al. (2023) CDNs’ Dark Side: Security Problems in CDN-to-Origin Connections. *Digital Threats: Research and Practice* 4(1):3. DOI <https://dl.acm.org/doi/pdf/10.1145/3499428>