**Summary Post**

**Introduction**

This post will consider my peers' feedback, summarising our collaborative discussion and enhancing my initial post on the technologies used to combat Denial of Service (DoS) attacks.

**What is a DoS attack?**

My initial post discussed availability as a core tenet of information security (Cawthra, 2020) and briefly covered the differences between a DoS attack and a DDoS attack. To expand on Louis's suggestion, the traditional concept of a denial-of-service attack is sending a large number of requests to a network, meaning it cannot respond to requests from legitimate users (Chapple, 2024). As Edward rightfully noted, DDoS attacks are evolving. For example, advanced attacks can be disguised as low-rate traffic by initiating the TCP handshake but not completing it (Vedula, 2021). Motivations for such attacks vary, from political ideologies to financial benefits (Mohammed Salim, 2019).

**Firewalls**

I mentioned how firewalls are one method to combat DoS-style attacks and how next-generation firewalls can use threat signatures to identify them (Google, 2024). I also explored how the arrival of cloud technology has made it more challenging to define a network boundary (Anderson, 2020). This has led to the "Zero Trust Approach," where all traffic is considered untrusted. The peer responses suggested providing examples to strengthen this point. Microsoft has forgone firewalls and uses Azure conditional access policies; Google’s BeyondCorp model emphasises using access proxies (Haddon, 2021).

**Content Delivery Network**

Another technology to combat a DoS threat is a content delivery network (CDN). CDNs are a group of geographically distributed servers that web applications use to achieve high availability. As Louis rightfully pointed out, this is achieved by caching the resource and reducing the strain on what is known as the “origin server” (Cloudflare, ND). In my initial post, I noted how CDNs aren’t entirely secure. Problems have arisen with a lack of secure backend configuration and the potential for MitM (man in the middle) attacks (Shobhiri, 2023). This can be avoided through careful and proper configuration, which aligns with Deivid’s view on “the human factor” and the necessity of training and educating developers.

**Conclusion**

This post summarises our discussion and enhances my initial post. Firewalls and CDNs are technologies that mitigate DoS attacks and ensure high availability. Proper thought must be given to their placement and configuration to ensure their most effective use.

**References**

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].

Chapple, M. (2024) *CC Certified in Cybersecurity Study Guide.* Newark: John Wiley & Sons, Inc. Available from: <https://learning.oreilly.com/library/view/cc-certified-in/9781394213832/?sso_link=yes&sso_link_from=university-of-essex> [Accessed 19 June 2024].

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

Haddon, D. (2021) Zero trust networks, the concepts, the strategies and the reality. *Strategy, Leadership and AI in the Cyber Ecosystem*. DOI:10.1016/B978-0-12-821442-9.0000001-X

Mohammed Salim, M., Rathore, S., & Hyuk Park, J. (2019) Distributed denial of service attacks and its defenses in IoT: a survey. *The Journal of Supercomputing* 2020(76):5320-5363. DOI: <https://doi.org/10.1007/s11227-019-02945-z>

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**](https://dl.acm.org/doi/pdf/10.1145/3499428)

Vedula, V. et al. (2021) On the Detection of Low-Rate Denial of Service Attacks at Transport and Application Layers. *Electronics* 2021(10):2105. DOI: [**https://doi.org/10.3390/electronics10172105**](https://doi.org/10.3390/electronics10172105)