Intrusion Prevention Systems (IPS) are useful for preventing threats to network security (Palo Alto Networks, 2021). IPS mitigates threats such as Distributed Denial of Service attacks (DDoS) by preventing the delivery of packets based on the content. SYN flooding is a method that can cause such disruption to service, attaining 37.6% of attack traffic in 2018 (Hao, 2019). A threat actor acting as a client sends an SYN (synchronised) TCP connection request to the server. In this case, the client either never receives the SYN-ACK or send the ACK (Douligeris and Mitrokotsa, 2004). With open ports, the threat actor floods the server with more SYN packets, disrupting the service for users potentially shutting down the server, as seen in the New Zealand Stock Exchange case (Casey, 2020).

Limitations of the IPS technology are that they can be expensive to setup and result in many false positive and false negative alerts which can increase the workload of the network administrator. IPS really should be placed on near the edge of the network between the router and firewall to effectively deal with DDoS attacks (Lerace et al., 2005).

The second security technology to discuss is a firewall, namely packet filtering. Packet filtering is inexpensive, efficient and can block mischief traffic that can arrive on specific port numbers.

However, maintaining a list of undesirable IP addresses is difficult to manage. Anderson (2008) suggests that packets are stateless, and they are examined with no consideration of the firewall they have previously gone through. The process to configure the packet filtering can sometimes be difficult due to rule settings (Firkhan Ali Bin Hamid, 2011). Source addresses can be spoofed and threat actors could send packets within the protected network (Kamara et al., 2003) such as vulnerability CVE-1999-0528 (National Vulnerability Database, 1999).

Casey, T. 2020. *NZ Stock Exchange hit by major DDoS* [Online]. Available: **https://ia.acs.org.au/article/2020/nz-stock-exchange-hit-by-major-ddos.html** [Accessed 15 September 2021].

Douligeris, C. & Mitrokotsa, A. 2004. DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks,* 44**,** 643-666.

Firkhan Ali Bin Hamid, A. A study of technology in firewall system. 2011 IEEE Symposium on Business, Engineering and Industrial Applications (ISBEIA), 25-28 Sept. 2011 2011. 232-236.

Hao, M. 2019. *2018 DDoS Attack Landscape-4* [Online]. Available: **https://nsfocusglobal.com/2018-ddos-attack-landscape-4/** [Accessed 15 September 2021].

Kamara, S., Fahmy, S., Schultz, E., Kerschbaum, F. & Frantzen, M. 2003. Analysis of vulnerabilities in Internet firewalls. *Computers & Security,* 22**,** 214-232.

Lerace, N., Urrutia, C. & Bassett, R. 2005. Intrusion prevention systems. *Ubiquity,* 2005**,** 2.

National Vulnerability Database. 1999. *CVE-1999-0528* [Online]. Available: **https://nvd.nist.gov/vuln/detail/CVE-1999-0528** [Accessed 16 September 2021].

Palo Alto Networks. 2021. *What is an Intrusion Prevention System?* [Online]. Available: **https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips** [Accessed 15 September 2021].