Network security would benefit from technology such as Intrusion Prevention Systems (IPS). IPS supports mitigating threats placed upon the network, notwithstanding monitoring traffic and making critical decisions whether to drop packets, block/reset connections, and raise alarms for malicious activity detection to an administrator (Abdulhak, 2021). This can be crucial against a Distributed Denial of Service (DDoS) attack, severely limiting a company's and end-users operations, as in the NZ stock exchange case (Casey, 2020). Despite the valuable technology, IPS are costly to implement and can cause a cumbersome workload for administrators due to false positive and false negative alerts. Additionally, threat actors can evade detection with robust techniques (Kılıç et al., 2019). Abdulhak (2021) also highlighted that such systems could reduce network performance due to deep packet inspection. Next-Generation Firewalls can utilise IPS effectively by incorporating its technology (Balakrishnan, 2021) which can offer a well rounded technological solution.

Packet filtering firewalls have importance as a starting point in network security which aims to protect and determine the protection of the network behind the firewall (Geiger, 2021). The benefit of the technology is that it is low development cost and almost transparent, suggesting users are alerted it is in operation when a packet is rejected through malicious activity detection. In some cases, attackers may access services on firewall servers due to their stateless approach with information not recorded from previous sessions and limited detection alerts (Wool, 2006). This technology offers little evaluative scrutiny of traffic with fewer processing times. The payload is not inspected; the risk is elevated as decisions are not made based on the packet's content, and harmful traffic could pass through the firewall. Still, it provides high-speed performance whilst rules can be implemented centrally to provide an explicit and straightforward method. (Romanofski, 2002).

Abdulhak, H. 2021. *Peer Response* [Online]. University of Essex Online. Available: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=275374 [Accessed 1 October 2021].

Balakrishnan, J. 2021. *Peer Response* [Online]. University of Essex Online. Available: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=275374 [Accessed 1 October 2021].

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].

Geiger, M. 2021. *Peer Response* [Online]. University of Essex Online. Available: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=275374 [Accessed 1 October 2021].

Kılıç, H., Katal, N. S. & Selçuk, A. A. Evasion Techniques Efficiency Over The IPS/IDS Technology. 2019 4th International Conference on Computer Science and Engineering (UBMK), 11-15 Sept. 2019 2019. 542-547.

Romanofski, E. 2002. *A Comparison of Packet Filtering Vs Application Level Firewall Technology* [Online]. Available: https://www.giac.org/paper/gsec/693/comparison-packet-filtering-vs-application-level-firewall-technology/101569 [Accessed 26 September 2021].

Wool, A. 2006. Packet filtering and stateful firewalls. *Handbook of Information Security,* 3**,** 526-536.