Thank you, Haseeb, for the informative post. The benefits of stateful firewalls, as suggested, can offer more than packet inspection. The inspection process is far more secure than the basic packet filtering and can be quicker than proxy firewalls making it a helpful method. Also, it can be used at the transport level and below as well as the application level if considering an FTP session protocol. Despite these benefits, we see limitations as they are less secure than proxy firewalls due to the level of content filtering. Also, it is worth noting that for protocols such as UDP, stateful firewalls can only track the source and destination IP addresses and ports. The state occurs challenge at the transport layer; therefore, only a DNS response from an external source previously seen from a DNS query from an internal source could help permit a pass (Scarfone & Hoffman, 2009). Further limitations are that it can be slower than packet filtering and vulnerable to attacks such as SYN-Flooding (Hao, 2019), which could cause other attacks such as Distributed Denial of Service (DDoS). Despite this, stateful firewalls provide an effective security measure as they can be application independent, implemented transparently and have little impact on network performance (Porter & Gough, 2007).

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

Porter, T. & Gough, M. 2007. Chapter 8 - Logically Segregate Network Traffic. *In:* PORTER, T. & GOUGH, M. (eds.) *How to Cheat at VoIP Security.* Burlington: Syngress.

Scarfone, K. & Hoffman, P. 2009. Guidelines on Firewalls and Firewall Policy. *In:* TECHNOLOGY, N. I. O. S. A. (ed.).