Great post Kingsley, very informative. Stateful firewalls can be beneficial as a first layer of protection, as you have suggested and how Zihaad mentioned they could log behaviour for deeper analysis. The stateful inspection will only allow incoming packets to be part of an established connection (Garlick, 2009). This inspection process makes the process far faster than proxy firewalls and there is flexibility in the layer of security it can operate, such as the transport or application headers (Conran, 2014). Stateful firewalls can have an important part to play; Garlick (2009) suggests that some companies have riskily switched off stateful inspection firewalls due to dropped packets that can occur if returning traffic takes an alternative route from its outbound route. Any switch off would pose a significant risk that can render the firewall useless. An additional benefit is that the rule base is far shorter than basic packet filtering, which would need two rules for the same flow of packets. Ultimately there is less administrative work in writing and managing rules and also less chance for errors.

A disadvantage to this method is the risk posed on busy networks. The cache table grows dynamically, and if this overflows, the firewall will remove cache entries which can cause connections to drop. Attackers can utilise this to cause a Denial of Service attack (Wool, 2006). Additionally, if the time out period is set too short, that can cause a cache entry to be removed, and therefore timeout parameters must be reasonable.

Conran, M. 2014. *STATEFUL FIREWALL – TRAFFIC FLOW AND DEFAULT INSPECTION* [Online]. Available: https://network-insight.net/2014/12/stateful-firewall-traffic-flow-and-default-inspection/ [Accessed 26 September 2021].

Garlick, N. 2009. The hidden benefits of optimising your firewall. *Network Security,* 2009**,** 6-9.

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