(Abdulhak, 2021) highlighted two security technologies which are network security and software security, stateful firewalls as a network security tool to protect networks against potential threats by inspecting packets alongside tracking connection state, authentication system as a software security technique to protect systems from unauthorized access.

Four peer responses to the initial post are as following: (Biljon, 2021) focused on the human factor roles such as changing default user and password which are in the devices such as switches, routers, firewalls, in addition, companies have to apply device best practice and ensuring that default user and password is changed before goes to real online, he suggested a checklist sheet is needed before choose the network design. Of course, I agree with Biljon about the importance of human factor roles in cyber security at all, the network is devices (HW), data, communication, and user, where according to (IBM, 2020) report 95% of cyber security breaches because of human errors.

(Callaghan, 2021) highlighted some advantages and limitations of stateful firewalls such as they are faster than proxy firewalls but less secure, for UDP they are worthless because they only track IP source and destination, furthermore, they are slower than packet filtering and vulnerable to attacks such as SYN-Flooding. As an advantage, they can work independently of the application, and regarding the network performance, they have little impact. I agree with Callaghan on many ideas except that the stateful firewall is vulnerable to SYN flood attacks because setting a limit to the number of half-open connections from a single computer will drop TCP packets from a specific computer if the limit is reached (Deep Security Help Center, 2020).

(Onyeemeosi, 2021) agree with the initial post about that the stateful firewall inspecting the content to identify threats, also monitoring the state of active connections. Moreover, added limitations such that it requires powerful hardware to perform fast filtering which makes it very expensive, alongside the configuration complexity and overload to network performance. An additional limitation with dealing with FTP protocol. Here I agree with Onyeemeosi regarding the added limitations, according to (Simic, 2020) it requires more resources which means more price and may slow down the performance. (Monir & Akhter, 2019) highlights that delay and overload with the dynamic control of stateful firewalls.

(Mundy, 2021) agree with the initial post about the weakness of stateful firewall, moreover, added some limitations such as being exploited through TCP/UDP traffics and no protection against attacks on the application layer. In addition, he suggested a web application firewall to protect web applications. I agree with Mundy, the stateful firewall situated at layers 3 and 4 of the Open Systems Interconnection (OSI) model (Fortinet, 2021) therefore, will not protect application-layer attacks.

In conclusion, as all security tools have advantages and limitations, the stateful firewall may succeed to protect the network against some attacks but not for all, to enhance the protection needs to apply more than one security solution.

References

Abdulhak, H. (2021) Collaborative Learning Discussion 2. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=275464 [Accessed 29 September 2021]

Biljon, E. (2021) Collaborative Learning Discussion 2. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=275464 [Accessed 28 September 2021]

Callaghan, J. (2021) Collaborative Learning Discussion 2. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=275464 [Accessed 29 September 2021]

Deep Security Help Center (2021) Define stateful firewall configurations. Available from: https://help.deepsecurity.trendmicro.com/10\_3/on-premise/Protection-Modules/ui-policies-rules-statefulconfigs.html [Accessed 29 September 2021]

IBM (2021) Cost of a Data Breach Report 2021. Available from: https://www.ibm.com/security/data-breach [Accessed 28 September 2021]

Monir, M. and Akhter, S. (2019) "Comparative Analysis of UDP Traffic With and Without SDN-Based Firewall", *2019 International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST)*. Dhaka, 10-12 Jan.IEEE. 85-90. Available from: http://doi: 10.1109/ICREST.2019.8644395 [Accessed 29 September 2021]

Mundy, A. (2021) Collaborative Learning Discussion 2. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=275464 [Accessed 29 September 2021]

Onyeemeosi, K. (2021) Collaborative Learning Discussion 2. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=275464 [Accessed 29 September 2021]

Simic, S. (2021) 8 Types of Firewalls: Guide For IT Security Pros. Available from: https://phoenixnap.com/blog/types-of-firewalls [Accessed 29 September 2021]