Initial Post

Network security keeps evolving as new technologies emerge. A common method used to protect networks is a packet filtering firewall. Packet filtering firewalls implement policies based on IP addresses, ports or protocols (Rountree, 2011). These firewalls are considered to be inexpensive and can operate at high speeds since their processing logic is simple. Hardware devices such as routers and switches still make use of packet filtering firewalls due to its high speed networking requirement (Melanson, 2014). In contrast packet filtering firewalls do not store any state information i.e. ports will need to be open statically for traffic to pass through (Andress, 2014). Packet filtering firewalls operate at level 3 of the OSI (Open Systems Interconnection) model rendering it ineffective against layer 7 (HTTP/S) attacks; since they cannot inspect the payload of a packet and can be easily spoofed (fake IP addresses inserted into packets) by an attacker (Rountree, 2011).

One method of protecting against HTTP/S attacks is through the implementation of a Web Application Firewall (WAF) which aims at protecting applications accessible from the internet. WAF’s run at layer 7 of the OSI model and are able to filter, monitor and block malicious HTTP/S traffic destined to web applications (F5 Inc, 2021). Internet facing applications require protection against SQL (Structured Query Language) injection achieved by injecting SQL code into a database, XSS (Cross-Site Scripting) attacks achieved by injecting malicious code into a web browser, cooking poisoning which occurs by hijacking a user’s session, amongst others (F5 Inc, 2021). However the draw backs of WAF’s includes cost as these can be relatively expensive and performance as WAF’s need to inspect each and every packet thereby slowing down a network. Babiker et al. (2018) further argue that WAF’s produce high false negatives and high false positives as well as their inability to detect unknown attacks.

In conclusion network security forms an important role within an organizations security plan. Selecting an appropriate firewall starts by understanding the architecture and the network that needs to be protected.

List of References

Andress, J. (2014) *The Basics of Information Security, Understanding the Fundamentals of InfoSec in Theory and Practice*. 2nd ed. Massachusetts: Syngress Publishing. Available from: https://doi.org/10.1016/C2013-0-18642-4 [Accessed 16 September 2021]

Babiker, M., Karaarslan, E., Hoscan, Y. (2018) ‘Web application attack detection and forensics: A survey’, *6th international symposium on digital forensic and security (ISDFS).* Turkey, 22-25 March 2018. USA: IEEE. Available from: http://acikerisim.mu.edu.tr/xmlui/bitstream/handle/20.500.12809/1677/Karaarslan.pdf?sequence=1&isAllowed=y [Accessed 15 September 2015]

F5 Inc. (2021) What is a Web Application Firewall. Available from: https://www.f5.com/services/resources/glossary/web-application-firewall [Accessed 16 September 2021]

Melanson, T J. (2014) Firewall Evolution from Packet Filter to Next Generation. Available from: https://www.juniper.net/documentation/en\_US/learn-about/LA\_FIrewallEvolution.pdf [Accessed 17 September 2021]

Rountree, D. (2011) *Security for Microsoft Windows System Administrators*, *Introduction to Key Information Security Concepts*. Massachusetts: Syngress Publishing. Available from: https://doi.org/10.1016/B978-1-59749-594-3.00003-X [Accessed 16 September 2021]