You brought up some good points about packet filtering firewalls and web application firewalls (WAF). A firewall is the first line of defence for networks regardless of the business size for network security. The variation in firewalls usually depends on the size of the business and its security goals. For smaller companies, a packet filtering firewall can be used. Packet filtering still allows packet filtering based on a static set of rules (Cuppens et al, 2012). It also is fast and therefore has fewer bottlenecking issues. As you mentioned, a packet filtering firewall lacks features and came to be spoofed. It could be argued that packet filtering firewalls are no longer good enough for modern business. Even for a smaller company that traditionally may use a packet filtering firewall, the other options, such as a stateful firewall, would render them obsolete.

You also brought up another type of firewall in a web application firewall (WAF). Web application firewalls protect the application layer against threats like SQL injections (Razzaq, 2013). As you noted, they aren’t foolproof and have problems with cost, performance, and detection rates (Khan, 2021). Although WAF’s have some prominent weaknesses, they are still a beneficial application. Web application attacks are prevalent, and forgoing a device because of some weaknesses would be unwise. As pointed out in a 2018 [IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)](https://ieeexplore.ieee.org/xpl/conhome/8376143/proceeding) report, no tool is full proof (Clincy & Shahriar, 2018). Implementing secure programming and network configurations would be beneficial when combined with a WAF. Ultimately, a WAF is an essential security device that needs to be appropriately incorporated to make up for its weaknesses.

References:

Clincy, V., Shahriar, H. (2018) ‘Web Application Firewall: Network Security Models and Configuration’, [*2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*](https://ieeexplore.ieee.org/xpl/conhome/8376143/proceeding)*.* Tokyo, Japan, 23-27 July 2018. Japan: IEEE.

Cuppens, F., Cuppens-Boulahiai, N., Garcia-Alfaro, J., Moataz, T., Rimasson, X. (2012) *Handling Stateful Firewall Anomalies.* Available from: <https://cs.brown.edu/~tmoataz/publications/sec.pdf>. [Accessed 24 September 2021].

 Razzaq, A., Hur, A., Shahbaz, S., Masood, M., Ahmad, H.(2013) ‘Critical analysis on web application firewall solutions’, *2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS)*, Mexico City, Mexico, 6-8 March 2013. Mexico: IEEE.