Zihaad, thanks for your great post with a lot of reference data. As mentioned, the security technology Web Application Firewall (WAF) which can protect layer 7 attack. Besides the cost and performance, there are a few conditions and limitations on WAF that need to be aware of.

WAF service can prevent malicious traffic, however, it could not be possible to protect all attacks in layer 7. In several conditions, a SQL Injection attack can effectively circumvent the WAF. The blind-SQL Injection by replacing keywords can successfully bypass the WAF regular expression (Dhiraj, 2019). Moreover, the Regular expression Denial of Service (ReDoS) can attack WAF by injecting an “Evil Regex” (Adar, 2020). To enhance the WAF, some of the cloud services like AWS, Azure combined WAF with Content Delivery Network (CDN) solution (Azure, 2020). CDN is reliable and having redundancy, which can provide more endpoints for protection and fast delivery for different geolocation users. Moreover, it can filter out the abnormal volume traffic to clean traffic before the process to WAF.

Nevertheless, even the website is protected by CDN and WAF, the service could be still denied by hackers. In 2015, Malaysia Airlines (MAS) official website had been redirected to another site (Trend Micro, 2015). MAS confirms that its Domain Name System (DNS) has been compromised where users are redirected. The DNS is the front-end network defined, spoofing and defacement can impact the whole design. Network protection is combined end-to-end with different layers, organizations should consider the threat based on each part.

References:

Dhiraj, M. (2019) SQL Injection Bypassing WAF. *OWASP*. Available from: https://owasp.org/www-community/attacks/SQL\_Injection\_Bypassing\_WAF [Accessed 25 September 2021].

Adar, W. (2020) Regular expression Denial of Service – ReDoS. *OWASP*. Available from: https://owasp.org/www-community/attacks/Regular\_expression\_Denial\_of\_Service\_-\_ReDoS [Accessed 25 September 2021].

Azure (Aug 31, 2020) Azure Web Application Firewall on Azure Content Delivery Network from Microsoft. *Microsoft*. Available from: https://docs.microsoft.com/en-us/azure/web-application-firewall/cdn/cdn-overview [Accessed 25 September 2021].

Trend Micro (January 26, 2015) Hacked or Spoofed: Digging into the Malaysia Airlines Website Incident. *Cyber Attacks*. Available from: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/hacked-or-spoofed-digging-into-the-malaysia-airlines-website-compromise [Accessed 25 September 2021].

https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=275575

Zihaad Khan