Hi Uvaraj,

This was a very fascinating post. You made a great point about how standard techniques of network filtering by firewalls do not adequately protect against the large surface assault that surrounds web applications.

When used as a reverse proxy, the WAF prevents clients from communicating directly with the backend system. Rather than that, they communicate only with the WAF. Typically, customers are unaware that this is taking place; to them, the process seems transparent.

The two fundamental WAF implementation models are negative security, in which the WAF is configured to prevent known vulnerabilities, attack signatures, and threat actors from accessing the web application based on pre-defined signatures, or positive security, in which the WAF is configured to allow only pre-approved traffic that meets specifically configured criteria. One of the most prevalent WAF configurations is a hybrid model, which incorporates both positive and negative security principles.

Probably the only two disadvantages of a WAF are that traffic latency will be decided by the WAF's performance and that WAFs may also be difficult to implement, where their effectiveness is dependent on the quality of the policies.

**References**

* Indusface (2019). What is WAF and How Does WAF Works? | Indusface Blog. Indusface. Available from: https://www.indusface.com/blog/how-web-application-firewall-works/ [Accessed 17 Apr. 2022].
* Reblaze (2022). How Does a WAF Work? - Reblaze. Reblaze. Available from: https://www.reblaze.com/wiki/waf/how-does-a-waf-work/ [Accessed 16 Apr. 2022].
* Avi Networks (n.d.). Web Application Firewall 101 - Learn All About WAFs. Avi Networks. Available from: https://avinetworks.com/what-is-a-web-application-firewall/ [Accessed 17 Apr. 2022].