Summary Post:

Both the Web Application Firewall (WAF) and the Firewall are critical components of any IT design, and I went into great length about them in the first blog piece I discussed about them. In the long run, no single technology will be able to totally replace another.

As Yash Roongta points out, the WAF requires substantial configuration and testing in order to be effective. I agree with him that this is an important consideration. The effectiveness of the WAF deployment is directly proportional to the quality of the policy that has been developed.

I agree that its Next Generation Firewalls (NGFW) may drop genuine traffic because of the high threshold, as Amit Pahuja , Gokul Kurunthasalam points out in his addition to the discussion about the Next Generation Firewall. I also agree that its Next Generation Firewalls (NGFW) may drop genuine traffic because of the high threshold (NGFW). Tuning the policy as a routine task required the use of manual labor.

In application development and maintenance, bug fixing is a never-ending process. Bugs are vulnerabilities in an application. The majority of organizations become aware of a vulnerability only after an attack occurs. Even more pitiful is the fact that they lack any quick repairs or patches. Attackers always target the unpatched system and gain control of other systems. One good use case is from the Equifax. The first Equifax hack was due to an Apache struts flaw. In March 2017, Apache patched. Unpatched systems at Equifax for months. This allowed attackers to launch a multi-layered attack. It was hidden until Equifax detected irregularities. (Annon, 2019)

This is where WAF's ability to temporarily repair itself comes in handy. Attack patterns are analyzed by machine learning to stop malicious requests. When a web application is formally patched, it is virtually patched for known vulnerabilities and the WAF profile is updated.

To conclude, it is critical to adhere to the security guideline at all times and to constantly review the policies and procedures to ensure they meet the demands of the organization. A specific Security technology or a solution is not a one-size-fits-all problem.

1. Anon., (2019) Benefits of using Web Application Firewall. Available from: https://www.inspirisys.com/blog-details/Benefits_of_using_Web_Application_Firewall/32 [Accessed 8 Apr 2022]