What is the Web Application Firewall?

rdavis@foregenix.com - 2018-09-12 - Comments (0) - FGX WAF

Web Application Firewall (WAF)

FGX-Web Protect WAF is a Layer 7 (Application Layer) firewall. Essentially it is a reverse HTTP proxy that controls input, output and/or access from or to an application or service. It operates by monitoring and potentially blocking the input, output or system service calls that do not meet the configured policies of the firewall.

More specifically, when a browser requests a page for a site that is behind the WAF, the HTTP request is passed to the WAF first. This is achieved by having the original site's domain name resolving to the WAF IP, instead of the original site's IP. This DNS change is essentially the only thing that is required for traffic to go through the WAF first. For full protection, the target site should also ensure that it only accepts incoming traffic from the WAF IPs.

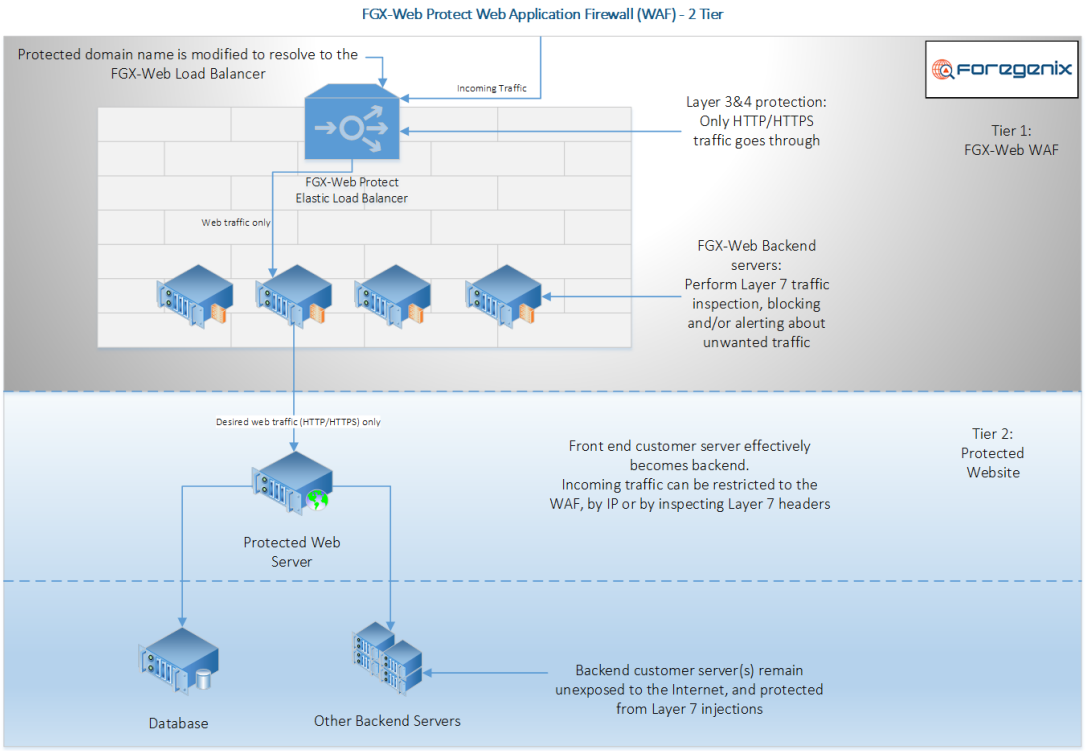
After request headers and body are inspected, there are three possible outcomes:

- The request is forwarded to the target site (legitimate traffic).
- The request is forward to the target site, but an alert is generated ("warning" mode).
- The request is blocked (undesirable traffic).

The actual rules determining what is desirable, what should be ignored, what should be blocked etc. are configurable through the FGX-Web Web UI. For example a site running ASP would activate the rules that block requests matching known ASP vulnerabilities, but add an exception for a trusted source IP that is used for system administration, to just warn in that case.

It should be noted that FGX-Web Protect offers full Layer 3&4 protection. Non-Web traffic cannot get through the WAF to the customers site, as its entry point only allows packets for the HTTP and HTTPS ports, and then completely blocking anything else.

2 Tier Diagram



Tags

FGX WAF

WAF