# I have completed the WAF setup, does this mean I am protected now?

rdavis@foregenix.com - 2017-11-02 - Comments (0) - FGX WAF

**I have completed the WAF setup, does this mean I am protected now?**

Short answer: not completely. There are certain post installation steps that you must carry out in order to secure your web application.

The first and most important thing to note is that the WAF will block almost no traffic under its default configuration. Low layer attacks such as a SYN flood are of course blocked, and so are certain very obviously malformed requests where the probability for a false positive is zero. With regards to HTTP(S) traffic however, the WAF is operating on so-called “Alert” mode. If a request is inspected and found to contain malicious payload it will still be allowed and an alert will be raised.

This is by design, to prevent serious malfunctioning of your site in the (relatively quite rare) case that legitimate requests result in false positives. We generally recommend that you leave the WAF under that mode for at least a couple of hours, and quickly review any alerts that have been generated. If in doubt about false positives, please ask Support.

So the first thing to do after the short “test” period in the alert mode ist o visit the WAF configuration and switch the mode to “Protect Against Threats” so that it begins blocking malicious attacks. If you have purchased a managed service this will be done by us.

Second, you need to lock down your server so that it accepts HTTP and HTTPS traffic only from the WAF and other trusted sources (such as your developer’s IP or payment systems). The way to lock down your server generally depends on its configuration and the policies of your hosting provider. For example you could implement blocking at the operating system firewall level, or at the web server level with .htaccess. Your hosting provider and/or system administrator will recommend the appropriate method. Regardless of the exact way, it is important that you lock down your server. Otherwise anybody who knows or can guess your server’s IP can simply access it directly, completely bypassing the WAF.

Finally, if you have a trusted static IP from which you perform administrative tasks (for example your office’s IP), it is recommended (but not mandatory) to do the following:

- Go to the WAF Configuration UI, section “Advanced Settings”.
- Add your application’s administrative URL(s) (for example: /admin/) to the list of blacklisted URL(s)
- Add your trusted IP(s) to the “Whitelisted IP Addresses” section.

Tags
PROTECT
STATIC IP
WAF
Whitelist