Are there any configuration changes needed when behind the WAF?

Ricardo Dias - 2020-04-30 - Comments (0) - FGX WAF

Once you have configured the WAF it's more than likely that the IP address being logged on your web server will be from one of our WAF IP addresses' rather than the real user's.

This is because the WAF will pass on and/or include the real user's IP address via the variable HTTP_X_FORWARDED_FOR and our WAF IP address' will be stored in the REMOTE_ADDR variable.

This means that your log files (if set up correctly) are most probably recording the real user's IP address by using the REMOTE_ADDR variable (which would be our WAF's IP address). In order to continue recording the real user's IP in the log files you will need to configure the server to use HTTP_X_FORWARDED_FOR when capturing the request for the logs. This can typically be done within the configuration file (nginx.conf, httpd.conf, depending on your server).

Nginx logging configuration to write both WAF and real user IP address

log_format WAFformat '$remote_addr ' '$HTTP_X_FORWARDED_FOR - $remote_user [$time_local]' '"$request" $status $body_bytes_sent ' '"$http_referer" "$http_user_agent"';

access_log **[path to log files]** WAFformat;

The above format is an example of how to configure the log files for an NGINX server set up.

1. We simply add into the current configuration the variable $HTTP_X_FORWARDED_FOR so that the log file also captures the real user IP along with the WAF IP.
2. We then specify the name of the log file (access_log) and then the path where we want to store this log file and then the name of the format we provided in step 1 (WAFformat)

Apache logging configuration to include the real user's IP address when behind the WAF

The example below logs the X-forwarded-For for request coming in through the WAF, and the remote IP for

"direct" requests (without passing through the WAF). Providing the best of both in order to allow requests to be logged regardless of if they pass through the WAF or not.

LogFormat "%h %l %m %u %t \"%r\" %>s %b %D \"%{Referer}i\" \"%{User-Agent}i\"" withoutWAF

LogFormat "%{X-Forwarded-For}i %l %m %u %t \"%r\" %>s %b %D \"%{Referer}i\" \"%{User-Agent}i\"" withWAF

SetEnvIf X-Forwarded-For "^.*\..*\..*\..*" forwarded

CustomLog **[path to log file]** withoutWAF env=!forwarded

CustomLog **[path to log file]** withWAF env=forwarded

1. Define a log format called " withoutWAF ", which is basically the default format, but you need to name it later
2. Define a log format called " withWAF ", which is like withoutWAF, only it logs X-Forwarded-For in place of the remote IP
3. Set the environment variable "forwarded" to TRUE if X-Forwarded-For exists
4. Log using default format if the variable "forwarded" is not set
5. Log using withWAF format if the variable “forwarded” is set

It is also worth noting that if you are using the real user's IP address for anything within your site (geo ip, shipping, etc) that you will need to amend the code in order to look for HTTP_X_FORWARDED_FOR as this is where the real user's IP address will be stored when requests are passed on by the WAF.

Tags
FGX-Web
WAF