I'm working on my website but after a while I'm blocked by the WAF - Why?

Dario Susman - 2021-08-19 - Comments (0) - FGX WAF

The reputation mechanism is an extension to normal payload filtering, designed to address the problem of automated attacks. Initially, the reputation score of an IP is zero and the WAF inspects the payload of every request, as well as the response. If the payload matches a rule, the reputation score of the IP is increased. If the reputation score exceeds a threshold, the IP is banned for at least 15 minutes. Banning means requests from that IP are denied without any inspection of the payload. In addition, those requests continue to contribute to the bad reputation score, with every attempt renewing the ban for another 15 minutes.

Examples of behavior that will trigger a reputation-based ban:

- Repeated authentication failures (requests with a 401 response). In that case, about 5 authentication failures within the same 15 minutes (seen by the same WAF node) will result in a ban. This mechanism aims to counter Brute Force (password guessing) attacks.

- Repeated triggers of "normal" payload inspection rules, for example sending a request that matches a known SQL injection pattern. In that case it takes about 50 triggers within 15 minutes, but the ban lasts for at least 2 hours. This mechanism aims to counter attacks based on vulnerability scanning.

- Repeated requests for certain URLs that have been observed in DoS attacks, where the attacker is trying to spam, overload or otherwise deplete resources of the target server. For example /customer/account/createPost is used a lot in Magento. In that case it takes about 20 requests within the same 30 minutes and the ban lasts about 55 minutes.

- Requests matching known spam content, of which it takes just 3 to ban an IP.

The figures are approximate because different rules contribute differently to the reputation score, and the reputation score has both deprecation rate and expiration period. Also, each WAF node maintains its own reputation lists so the actual point that a full ban is triggered has a probabilistic element (of course a persistent attack will result in the source being banned by all active WAF nodes very quickly) But they are pretty much what you should expect.

The problem is administrative activity is very similar to such malicious activity (except for the last category) since they both try to do roughly the same privileged stuff on the server. In fact, we always recommend that the administrative section of the site is blacklisted, meaning any attempt to access it from a non-whitelisted IP will by definition be treated as an attack and eventually result in a ban. Even in the first case, it is conceivable that an administrator will forget the password but try a few times, thus triggering a ban. And because the reputation-based ban takes precedence over any other rule (including the ones for whitelisting), once an IP has been banned it is impossible to clear its reputation unless a Foregenix administrator takes action directly on the WAF nodes (or the ban expires).

For those reasons, it is very important that IPs engaging in administrative activity are whitelisted in advance, to prevent them from being wrongfully banned.