Understanding Monitor and Block Modes

https://campus.barracuda.com/doc/77401089/

Barracuda WAF-as-a-Service has two modes: Monitor mode and Block mode. The difference lies in what Barracuda Networks' Cloud Scrubbing Centers do with traffic that is detected as malicious.

- In **Monitor Mode**, Barracuda WAF-as-a-Service detects malicious traffic, but forwards it on unmodified to your application server.*Your application server is still vulnerable to attacks.*The malicious traffic is logged and you can view it on the Firewall Logs page, described in Access, Firewall, and Event Logs.
- In **Block Mode**, Barracuda WAF-as-a-Service detects malicious traffic and blocks it. Your application server does not receive this traffic and is safe from attacks.

Important

Malicious traffic is only blocked from reaching your application server when Barracuda WAF-as-a-Service is in Block mode.

When to use Monitor Mode

When setting up Barracuda WAF-as-a-Service on an application, you might want to first ensure that it is configured properly. Specifically, ensure that it is not erroneously detecting legitimate traffic as malicious. This is known as a *false positive*. False positives can cause users to be blocked when attempting to legitimately use your application.

You can put your application in Monitor mode to see how Barracuda WAF-as-a-Service detects malicious traffic on your application. By inspecting the Firewall Logs page, you can see what traffic is being detected as malicious, and if any of it is legitimate traffic, modify your configuration to exclude that traffic from detection. For more information, see Access, Firewall, and Event Logs.

When to use Block Mode

After you have finished setting up and configuring Barracuda WAF-as-a-Service on an application, *always* put it in Block mode to secure the application. Barracuda WAF-as-a-Service only blocks malicious traffic in Block mode, keeping your application server safe.