Violation Responses - Response Policies

https://campus.barracuda.com/doc/96765688/

When clients make requests to your application, Barracuda WAF-as-a-Service detects violations and takes actions that correspond to the severity of the violation. For details on the various actions, refer to Violation Responses - Policy Options.

You can leave the default actions as is, or customize them to suit the specific needs of your organization.

Understanding Risk Scores

Metadata from each request and response are sent to the cloud-based Barracuda Application Intelligence Network. This information is analyzed for each session, and the risk of the client is computed based on the traffic and client's behavioral characteristics.

This score is used to identify the riskiness of a specific client - whether the client is good, suspicious, or bad.

Some of the characteristics used to compute the score for a client are:

- Attacks on the applications in the given session
- Statistical anomalies in the client session
- Suspicious client fingerprints, devices, etc. Fingerprints include information about the browser attributes from all the devices that the client uses during login.
- Previous anomalous behavior exhibited by the client

Risk Levels

These risk scores are used as standards and cannot be modified:

- 100 - Critical
- 80 - High
- 60 - Elevated
- 40 - Medium
- 20 - Low

Understanding Client Fingerprinting

In the process of client fingerprinting, Barracuda WAF-as-a-Service collects information about the browser attributes from all the devices that the client uses during login. This collected information helps Barracuda WAF-as-a-service identify suspicious clients (potential bots) and recognize web scraping attacks more quickly. Clients are often identified solely by their IP address. But depending on IP addresses is not always accurate, based on these examples:

- Blocking a client IP address that is behind a NATed network can also block other, valid users.
- The same client can jump IP addresses or use proxies to hide their actual location.

With client fingerprinting, Barracuda WAF-as-a-Service can identify a specific client down to the browser, so other, valid clients are not affected.

Data used to identify clients using fingerprinting include:

- characteristics of the client’s system
- request analysis based on incoming traffic
- SSL information

Understanding Tarpits

As the name implies, within a *tarpit*, everything moves very slowly. When a client repeatedly attempts to access your application, Barracuda WAF-as-a-Service can intentionally delay those incoming requests with a tarpit. This slow processing often makes bad clients give up, rather than keep trying, protecting your application. On the Policy Options page, you can specify a limit for the number of requests that a single client can make. After that number is reached, the client is put into a tarpit. Their requests are put in a backlog and are only processed after active requests are served and then only after the time delay interval between requests that you specify. The client remains in the tarpit for the amount of time you specify and is then released.

Editing Response Policies

To edit a response policy:

1. On the Barracuda WAF-as-a-Service dashboard, click the link for the desired application.
2. In the left navigation, select **Violation Responses**, then **Response Policies**. If it is not present, click **Add Components** and add it.
3. Locate the violation that you want to edit. Note that there are over 200 violations, so you might want to use the Search function or view all pages of violations.
4. In the **More** column, click the three dots and select **Edit Response**.
5. Edit some or all of the values, then click **Save**.

Specify a new **Risk Level**.

Specify an action to take:

- **Close Connection** – Closes the connection and does not allow the request to be processed.
- **Send Response Page** – Display a specific page that you specify below.
- **Send Redirect** – Redirect the client to another page. Specify the redirect type and URL in the next fields.
- **Allow Request** – Not recommended. This bypasses all Barracuda WAF-as-a-Service rules and is extremely risky.
- **No Action** – Not recommended. Barracuda WAF-as-a-Service will continue to process other rules that might block the request, but will take no action for this specific violation, which could be a risk.

Specify whether to log the violation request in the Firewall Logs. Logging the request gives you a record of the violation.

Specify a follow-up action to take if an action is specified above. Follow-up actions include:

- **None** – Take no action
- **Block Client IP** – Block the IP address of the client, so it cannot contact your application. Specify the duration of time to block the client IP, in seconds, in the next field.
- **Challenge with CAPTCHA** – Require the client to prove it is a human by providing a CAPTCHA challenge.
- **Block Client Fingerprint** – Block the fingerprint of this client, so it cannot contact your application. Specify the duration of time to block the client IP, in seconds, in the next field.
- **Tarpit Client** – Intentionally delay incoming requests coming from suspicious or bad clients. For more information, refer to the Understanding Tarpits section below.
  - **Backlog Requests Limit** – The maximum number of requests from a client that is in the tarpit to be put in the Tarpit Backlog queue. These requests are processed only after active, valid requests are served.
  - **Time Between Tarpit Requests** – The interval, in seconds, to wait before serving each queued request from the client in the tarpit.
  - **Time Before Tarpit Expires** – The time, in seconds, after which the client is released from the tarpit.