Violation Responses - Policy Options

https://campus.barracuda.com/doc/96024545/

You can specify specific actions for Barracuda WAF-as-a-Service to take when it detects certain violations in requests to your application. For example, you might want to challenge a suspicious client with CAPTCHA or completely block a likely bad client.

For background information on risk scores, client fingerprinting, and tarpits, refer to Violation Responses - Response Policies.

Specifying Risk Score Thresholds and Responses

Notes:

- This information is visible only if you subscribe to Advanced Bot Protection.
- If the **Enable Risk Score Thresholds** is set to **Off**, switch it to **On** to set the thresholds and associated actions.
  In the **Off** position, the system still calculates risk scores for each client (visible in the Logs), but the actions you specify for Suspicious and Bad clients are not applied.

To specify responses to violations:

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 **Policy Options**. If it is not present, click **Add Components** and add it.
3. In the **Risk Score Thresholds** section, use the sliders to specify values above which you consider a client to your application to be either **Suspicious** or **Bad**, causing Barracuda WAF-as-a-Service to take specific actions. Scores range from 0 (no risk) to 100 (maximum risk).
   By default, the risk score for a Suspicious client is 60 and above. The risk score for a Bad Client is 80 and above.
4. Review the default actions specified for the Suspicious Client and for the Bad Client. To edit the action taken, click the three dots in the More column and select **Edit Response**.
   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.

Activating Client Fingerprinting

Client fingerprinting can be in passive or active mode. Active mode is more accurate, but only works if clients are running a standard browser.

- **Passive Mode** – Barracuda WAF-as-a-Service calculates the fingerprint for a client by observing only its traffic patterns.
- **Active Mode** – In addition to observing traffic patterns for a client, Barracuda WAF-as-a-Service uses a JavaScript fingerprint challenge to create the fingerprint that is logged in the Access Logs.

To set client fingerprinting mode to active:

1. In the **Client Fingerprinting** section, set the **Client fingerprinting mode** to **Active**. Setting the mode to active displays the default action to take when the fingerprint challenges are exceeded.
2. Optionally change the configuration for **Fingerprint Challenges Exceeded**. Click the three dots in the **More** column and select **Edit Response**.
3. Edit the response policy as described in the Risk Score Thresholds section above.
4. Click **Save**.

Specifying Client Fingerprints to Exempt

You can specify client fingerprints that you want to be exempt from the Risk Score Threshold actions configured at the top of this page.

> If you exempt client fingerprints, no actions will be taken against clients with those fingerprints.

To specify a client fingerprint. find the fingerprint you want to exempt in the Access Logs. For details on Access Logs, refer to Access, Firewall, and Event Logs.

1. In WAF-as-a-Service, select an application.
2. In the left navigation, select **Logs**.
3. Select the **Access Logs** tab.
4. Locate the appropriate log entry and click the plus icon to expand it. In the **Bot Protection** section, copy the **Client Fingerprint** value.
5. Return to the **Violation Responses - Policy Options** page.
6. In the **Risk Score Exempt Client Fingerprints** section, paste the copied value into the **Client Fingerprints** field. Then click the plus button to add the client fingerprint.
7. Repeat the process to exempt additional client fingerprints.