Risk Scoring

https://campus.barracuda.com/doc/90442900/

Risk scores are a core part of the Advanced Bot Protection capabilities of the Barracuda Web Application Firewall. There are two types of risk scores that can be computed and then used to detect malicious requests or clients.

- Request Risk Score
- Client Risk Score

Request Risk Score

Every incoming request is evaluated by the Barracuda WAF on multiple parameters. As multiple aspects of requests are evaluated, each deviation from the expected structure and behavior contributes to risk score for that specific request.

Each deviation detected by the Barracuda WAF is associated with an attack ID**.** The risk metric associated with each attack ID provides the weights used to compute the Request Risk Score.

A request identified with one deviation shows the same risk score, whereas a request identified with two or more deviations shows the weighted sum of all the risk scores in the Access log. In Web Firewall logs, for service in “Passive” mode, multiple logs are generated for the same request (i.e., the same ID), so the risk scores are shown in individual logs, adding themselves with every identified attack.

Client Risk Score

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 client as a good bot / bad bot and a good user / attacker.

Some of the characteristics utilized to compute the score for a client are as follows:

- Request risk scores for the requests in a session
- Attacks on the applications in the given session
- Statistical anomalies in the client session
- Suspicious client fingerprints, devices, and so on

- Previous anomalous behavior exhibited by clients

Configuring Risk Scores

The **Risk Scores** page displays the risk levels that can be assigned to an action policy. Risk levels can be updated for an individual action policy or can be updated for multiple action policies using the **Bulk Edit** option. The **Security Policies > Risk Scores** tab displays the scores associated with each risk level.

Risk Scores and Risk Levels

Below are the standard risk scores defined and cannot be modified by users:

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

Users can modify the risk levels for each action policy. Risk scores are used across various features, such as Tarpit and Advanced Bot Protection, to identify risky clients and perform specific response actions.
To configure risk scores for an attack ID, move the slider to the desired risk level. The bar next to the slider shows the risk levels with different colors.
To configure risk scores in bulk, select all the attack IDs for which you want to configure the scores and then click **Bulk Edit**. Select the **Risk Score** check box, move the slider to the corresponding risk level, and then click **Save**.

The corresponding values configured for the Request Risk Score and Client Risk Score are displayed on the **Access Logs/Web Firewall Logs > Details** page. The Request Risk Score and Client Risk Score fields are also displayed when a CSV is generated. To view these fields while exporting logs on an external Syslog server or FTP server, configure %rrs for Request Risk Score and %crs for Client Risk Score in the **Export Logs > Custom Log Format** page.