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 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 deviation 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:

- 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

Risk Scores are configured in the **Security Policies > Action Policy** page.

1. Click **Edit** next to the attack ID for which you want to configure the risk score.
2. In the **Risk Score** field, enter the risk score value. Note that only integer values in the range 0-100 is permitted.

The corresponding values configured for 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**.