Session Tracking

https://campus.barracuda.com/doc/4259862/

A session refers to all requests a single client makes to a server. A session is specific to the user, and for each user a new session is created to track all requests from that user. Every user has a unique session identified by a unique session identifier. Session Tracking enables the Barracuda Web Application Firewall to limit the number of sessions originating from a particular client IP address in a given interval of time. Limiting the session generation rate by client IP address helps prevent session-based Denial of Service (DoS) attacks.

Configure Session Tracking

1. Go to the **BOT MITIGATION > Bot Mitigation** page, **Session Tracking** section.
2. Click **Edit** next to the session identifier for which you want to configure session tracking.
3. Specify the desired session protection fields:
    1. **New Session Count** – Maximum number of new sessions allowed per IP address. Range: 1 - 65535; default: 10.
    2. **Interval** – The time in seconds for which the number of sessions cannot exceed the **New Session Count** setting. Range: 1 - 6000 seconds; default: 60.
    3. **Status** – Set to *On* to enable session tracking.
    4. **Session Identifiers** – The token type used to recognize sessions. Choose from the list, or see **Configuration of Session Identifiers** to add a session identifier.
    5. **Exception Clients** – List clients that are exempted from this protection. IP address ranges should be separated by a "-" (hyphen). Multiple ranges or IP addresses can be separated with a "," (comma). The list should not contain overlapping IP address ranges.
4. Click **Save** .

Configure Session Identifiers

Configuring session identifiers allows the Barracuda Web Application Firewall to recognize session information in requests and responses. To create a new session identifier, perform the following steps:

1. Go to **BOT MITIGATION > Libraries > Session Identifiers**.
2. Locate the desired identifier and click **Edit**, or to add a new identifier, click **Add Session Identifiers**.
3. Enter or modify the session **Identifier Name**. This name will appear in the list of session identifiers from which you choose when you configure **Session Tracking**.
4. Enter or modify the following session token parameters: **Token Name**, **Token Type**, **Start Delimiter**, **End Delimiter**. For example, “JSESSIONID=12345;” would be configured with session **Token Name**: JSESSIONID, **Token Type**: Parameter**, Start Delimiter**: = and **End**

Delimiter: ; to allow Barracuda Web Application Firewall to successfully extract the Session ID **12345**.

5. Newly added or edited session identifiers appear in the Session Identifiers list on the **Edit Session Tracking** page when you select the **Edit** option on the **BOT MITIGATION > Bot Mitigation > Session Tracking** section.