How to Enable Client Fingerprinting

https://campus.barracuda.com/doc/89621168/

The Barracuda Web Application Firewall uses the client fingerprinting capability to increase security. The feature collects information about the browser attributes from all devices that the client uses during login. Client fingerprinting uses the collected information to identify suspicious clients (potential bots) and recognize web scraping attacks more quickly.

The Need for Client Fingerprinting

For a long time, incoming clients into applications were identified using IP addresses, which resulted in the following issues regarding accuracy:

- When clients are behind a NAT-ed network, blocking an IP address can block other valid users completely.
- The same client can jump IP addresses or use proxies to hide their actual location.

To more accurately identify clients, the Barracuda WAF uses various client fingerprinting techniques to identify a specific client down to the browser. This means that, when a client is identified with these techniques, it is at the browser level, and any blocks will affect only the specific client.

The Barracuda WAF uses a combination of Active and Passive Fingerprinting techniques along with a cloud-based advanced analysis layer (available with the Advanced Bot Protection subscription) to identify clients uniquely.

Techniques Used

The following are some of the techniques used by the Barracuda WAF to identify clients using fingerprinting:

- Active Client Fingerprinting based on characteristics of the client’s system.
- Active Request Analysis based on incoming traffic.
- Passive SSL Fingerprinting.
- Active Browser Analysis using an inserted JavaScript (Infisecure only in 10.0).

Enable Client Fingerprinting

1. Go to the **BOT MITIGATION > Bot Mitigation** page, **Bot Mitigation Policy** section, and click **Edit** next to the service**.**
    1. On the **Client Fingerprint** window, set **Enable Client Fingerprinting** to **Yes**.
2. Go to the **ADVANCED > System Configuration** page, **Advanced** section, and set **Enable Client Fingerprinting** to **Yes** under **Security Management**.

Viewing Client Fingerprints

After you enable client fingerprinting, the client fingerprints are displayed on the **BASIC > Web Firewall Logs** page and the **BASIC >Access Logs** page.