Configuring DDoS Policy

https://campus.barracuda.com/doc/19693870/

The DDOS policy allows administrators to validate incoming users by challenging them with **CAPTCHA**s to find out if a client is a regular browser, a BOT, or a crawler. Administrators can configure the DDOS policy to issue CAPTCHAs to all clients who access a URL space, or to issue CAPTCHAs only to clients with suspicious profiles.

The DDOS policy provides a way to evaluate a client and determine if it is suspicious or not. When **Evaluate Clients** is set to *On*, the Barracuda Web Application Firewall embeds JavaScript challenges in responses that are going out. The client is tagged as suspicious if more than a configured number of requests do not come back with the JavaScript challenge answer, indicating the requests are coming from an automated source, such as a bot or a crawler that cannot execute JavaScripts.

The client tagged as suspicious is forced to answer a CAPTCHA challenge before accessing the URL space. Suspicious client IP addresses are tracked and challenged with a CAPTCHA image for a period of time. The client is not allowed to access any further resource until the CAPTCHA is answered. This thwarts reconnaissance efforts from suspicious clients.

Clients that answer the CAPTCHA can access the URL space. If a validated client remains idle for more than the configured **Expiry Time** seconds, it is challenged with CAPTCHA to access the resource again. This re-issuance of CAPTCHA after an **Expiry Time** ensures that a public IP validated as a good client source once does not remain permanently in good standing, but is detected as a non-browser if it gets compromised.

To configure a DDoS policy, click **Add** next to the Service in the **DDoS Policy** section.

Configuration of DDoS Policy

The following settings allow the Barracuda Web Application Firewall to enforce the DDoS policy for a service:

Host Match

The host name, compared to the host in the request. This can be either a specific host match or a wildcard host match with a single “*“. For example, *.example.com; any request matching this host is required to authenticate before accessing this page.

URL Match

The URL compared to the URL in the request. The URL should start with a "/" and can have at most

one " * " anywhere in the URL. For example, /netbanking.html; any request matching this URL is required to authenticate before accessing this page. A value of “/*” means that the access control rule (ACL) applies for all URLs in that domain.

Extended Match

Define an expression that consists of a combination of HTTP headers and/or query string parameters. This expression is compared to special attributes in the HTTP headers or query string parameters in the requests.

Extended Match Sequence

This number indicates the order in which the extended match rule must be evaluated in the requests.

Evaluate Clients

When set to *On*, the Barracuda Web Application Firewall inserts JavaScript in the responses that are sent to the client. Note that the JavaScript mechanism will work only if at least one URL accessed within the specified **URL Match** space is an HTML file. If the URL space does not result in at least one request for an HTML URI, the Barracuda Web Application Firewall continues to add to the failed count and eventually issues CAPTCHA instances to all client IP addresses. In other words, the response to at least one request within the URL space should have a content type of text/HTML for the mechanism to work effectively and encourage clients to use regular web browsers.

Enforce CAPTCHA

Select the enforce CAPTCHA option.

- **Do Not Enforce** – Clients are allowed to pass through with the usual security validation.
- **Suspicious Clients Only** – CAPTCHA is enforced for clients that exhibit suspicious behavior.
- **All Clients** – CAPTCHA is enforced for all clients accessing this Service.

Detect Mouse Event

If **Detect Mouse Event** is set to **Yes** and **Enforce CAPTCHA** is set to **Suspicious clients** only, the JavaScript gets executed only when the "Mousemove" event is detected in the client's browser. The JavaScript gets executed and returns with a value for the cookie. "Mousemove" is a Mouse Event.

Max CAPTCHA Attempts

The number of attempts a client can make before failing to solve the CAPTCHA.

Max Unanswered CAPTCHA

This limits the number of CAPTCHA instances that can be issued to a given client IP address,

preventing an attacker from executing a DoS attack on the service by rendering CAPTCHA images without submitting the CAPTCHA response.

Expiry Time

The number of seconds a client IP can be idle before being challenged for CAPTCHA again.

Steps to Configure DDoS Policy for a Service

1. Go to the **BOT MITIGATION > Application DDoS Mitigation > DDoS Policy** section.
2. Identify the service to which you want to enable the DDoS policy.
3. Click **Add** next to that service. The **Add DDoS Policy** window appears.
4. Specify values for the given parameters and click **Save**.

For more information, click the **Help** icon on the web interface.