Client Evaluation

https://campus.barracuda.com/doc/98225915/

Client Evaluation enables you to configure the Captcha policy for validating the clients accessing your application. When **Client Evaluation** is enabled, the user is challenged to solve the Captcha to access the application. Captcha challenges are enforced to ensure that the user accessing the application is really a human and not a malicious bot.

The Barracuda WAF-as-a-Service provides the following CAPTCHA methods to evaluate incoming clients:

- CAPTCHA
- reCAPTCHAv2
- reCAPTCHAv3
- hCAPTCHA

CAPTCHA

A challenge is enforced on the client when they are tagged as suspicious. The client is forced to answer a CAPTCHA challenge before accessing the URL space. The suspicious client IP addresses will be tracked for a defined time of 900 seconds.

reCAPTCHAv2

A challenge enforced on the client for protecting a website from spam or any other types of automated abuse like BOTS etc. The Barracuda WAF-as-a-Service uses Google reCAPTCHA, which is an advancement over the classical version of CAPTCHA for protecting websites from spams. reCAPTCHA uses an advanced risk analysis engine and adaptive CAPTCHAs to keep automated software from engaging in abusive activities on a client's site. It also allows all valid clients to pass through with ease.

The administrator should generate a unique key pair (a site key and a site secret) specific to the website at the following link: Sign up for an API key pair. The key pair consists of a site key and a secret key. The site key is used to invoke the reCAPTCHA service for the website, and the secret key authorizes communication between the client and the website. The secret key must be kept safe for security purposes.

- **Domains** – Specify the domain to be challenged with the selected CAPTCHA method

- **Site Key** – Specify the reCAPTCHA site key for the selected domain
- **Site Secret** – Specify the reCAPTCHA secret for the selected domain

reCAPTCHAv3

An invisible CAPTCHA that returns a score for the request without interpreting with the user. This means that the user has no action to perform during validation. The invisible reCaptcha automatically analyzes and appears only when it realizes the existence of any type of automated abuses like BOTS etc. When a challenge is enforced on the client, it returns a score for the request. The score is based on interactions with your website and enables you to take appropriate action.

hCAPTCHA

A challenge enforced on the client for protecting a website from spam or any other types of automated abuse like BOTS, etc. hCaptcha is an advancement over the classical version of CAPTCHA for protecting websites from spam and is an alternative to reCAPTCHA. It uses an advanced risk analysis engine and adaptive CAPTCHAs to keep automated software from engaging in abusive activities on a client's site. The captchas are clearer and challenging to humans. It also allows all valid clients to pass through with ease.

hCaptcha is designed to perform without relying on historic data or the personal information of users. hCaptcha' s advanced machine learning capabilities automatically adapt to new threats and offers a suite of advanced features to protect your organization against the most sophisticated threat actors from advanced persistent threat mitigation to private learning.

The administrator should generate a unique key pair (a site key and a site secret) specific to the website at the following link: Sign up for an API key pair. The key pair consists of a site key and a secret key. The site key is used to invoke the hCaptcha service for the website and the secret key authorizes communication between the client and the website. The secret key must be kept safe for security purposes.

- **Domains** - Specify the domain to be challenged with the selected CAPTCHA method.
- **Site Key** - Specify the hCaptcha site key for the selected domain.
- **Site Secret** - Specify the hCaptcha secret for the selected domain.

Steps to Configure the CAPTCHA Policy

1. On the WAF-as-a-Service web interface, go to the **APPLICATIONS** page and click on the application to which you want to enable Client Evaluation.

2. On your application page, click **DDoS** in the left panel and then click **Client Evaluation**.
3. On the **Client Evaluation** page, do the following:
    1. **Client Evaluation** - Set to **ON** to enable client evaluation.
    2. **Captcha Method** - Select the method that needs to be presented to incoming clients for validation.
    3. **Enforce CAPTCHA** – Select which type of clients you want to challenge with the Captcha code:
        1. **Suspicious Clients Only** - CAPTCHA is enforced to clients that exhibit suspicious behavior. The criteria for suspicion, at this point, is failure to answer/solve the client evaluation challenge.
        2. **All Clients** - CAPTCHA is enforced to all clients accessing the application.
    4. **Max CAPTCHA Attempts** – Specify the number of attempts a client can make to solve a CAPTCHA challenge. If the attempts exceed the configured limit, the client is added to the block list.
    5. **Max Unanswered CAPTCHA** - Specify the number of attempts a client can make in fetching the CAPTCHA image without answering it. This limitation is enforced to ensure the possibility of an attacker creating a DoS attack on the service by rendering CAPTCHA images without submitting the CAPTCHA response, is mitigated. The client IP address which exceeds this limit, will be added to the block list.
    6. **Expiration Time** – Specify the number of seconds a client can access the application after solving the CAPTCHA challenge, before being challenged again.
    7. Click **Save**.