Form Spam Protection

https://campus.barracuda.com/doc/91985659/

The Barracuda Web Application Firewall provides protection against fake/automated form submissions.

The Barracuda Web Application Firewall looks into the real-time traffic passing through and learns all the static forms and their parameters. Based on the type of values it has viewed for each of these parameters, it tries to associate a parameter class for them. In addition, the Barracuda Web Application Firewall also creates/suggests a Form Spam rule to ensure that any further submissions on the form conform to a matching rule. Using the learned data, it internally calculates the minimum form fill time required for a normal user to submit the form and make it a part of Form Spam rule.

The Barracuda Web Application Firewall Form Spam protection also provides an option to add honeypots dynamically into the form to stop bots from automating form submissions. Honeypots are fields added in forms that are not visible to the normal user. It is not possible for the user to alter these values. However, any changes made to these fields are used to differentiate between a normal user and an automated bot.

Learning a Form

The following configuration elements help the Barracuda Web Application Firewall to determine when to create a Form Spam rule.

1. Navigate to **BOT MITIGATION > Bot Spam Mitigation > Form Spam > Form Learning – Advanced settings**.
2. From the **Looking Criteria** drop-down list, select the criteria to stop Form Learning automatically.
3. Specify the number of number of submits to stop Form Learning automatically.
4. In the **Minimum Fill Time Calculation box,** specify the algorithm used by the Form Learning module to calculate the minimum form fill time for a form.
5. Click **OK**.

Editing Form Spam

Configure the following values:

1. Navigate to **BOT MITIGATION > Bot Spam Mitigation > Form Spam,** click the **Options** drop-down list, and then select **Edit**.

2. Set the **Form Spam Status** to **On** to enable form spam protection for the service.
3. Set the **Insert Honeypot Field to Yes** to insert the honeypot field in the forms. When this value is set to *Yes*, the Barracuda WAF inserts a dynamic form field that will not be visible to the normal user. These fields are called honeypot fields and any change to these values are used to differentiate between normal user and automated bots.
4. Set **Auto Configure Status** to **Yes** for the Web Application Firewall to learn the forms along with their parameters, and automatically configure the appropriate rules.

Adding a Form

Using this section, you can add a form.

1. Navigate to **BOT MITIGATION > Bot Spam Mitigation > Form Spam,** click the **Options** drop-down list, and then select **Add Form**.
2. Specify the following fields for the forms to be protected:
    - **Service Name**: Name of the service for which the form is to be added.
    - **Form Name:** Name for the form.
    - **Status**: Set to **On** to subject the form to go through form spam-related checks.
    - **Mode**: Set the mode for the URL profile.
        - **Learning** - Learns the web application and creates URL profiles and parameter profiles. Note that this is available only in models 660 and above.
        - **Passive** - Validates the requests against the URL profile and allows them to pass through but logs the request errors. Note: The Passive mode setting does not affect the parameter profiles under that URL profile.
        - **Active** - Allows or blocks the requests by validating against the URL profile.
    - **Action URL**: Action URL for the form that needs to be protected against form spam. An Action URL is a URL that is called when the form is submitted.
    - **Minimum Form Fill Time**: The minimum time required by normal clients to fill the form.
    - **Form Parameters**: The parameters of the form to be protected and its associated classes to be added in the Form Spam rule. You can click **+** and define custom parameters and associate them to the classes provided under the **Parameter Class** drop-down list.
3. Click **OK**.

Modifying a Form

Use this section to modify certain parameters of an existing form.

1. Select the form that needs to be modified, click the drop-down list, and then select **Edit**.
2. Provide new values for the following fields that can be edited and then click **Save**.

Viewing the Learned Forms

In this section, you can view forms that are automatically learned by Form Spam Learning along with their Action URLs, Fill Time Range, Total Number of Submits, Parameters and their associated classes.

These settings are used to create the Form Spam Rules only when the **Auto Configure Status** is set to **Yes** for a service on the **Edit Form Spam** page.