Allow/Deny Rules for URLs

https://campus.barracuda.com/doc/20645731/

Strict allow/deny rules for a web application can be configured on the **WEBSITES > Allow/Deny** page. Allow/Deny rules allow you to customize access to the web application based on a set of matching criteria. An administrator can configure a rule to control access to certain portions of the web application as per the business requirement without changing any configuration on the web application itself.

A rule can be configured for a URL match, a Host header match and a set of optional extended match criteria (example: client IP address or the HTTP method). Once a match is found, the request will be processed as per the configured action. The rule action can be configured to either redirect the incoming request to another absolute URL, or to continue the processing of the request using the other security layers of the Barracuda Web Application Firewall, in addition to allowing or denying a request explicitly.

To configure a specific match, click **Add** or **Edit** next to the Service and use the **Extended Match** widget. For rule matching and subsequent evaluation, URL match and Host header matches are prioritized over extended matches. If more than one rule with the same URL match/Host header match is configured, they are evaluated based on the specified extended match sequence.

There are two ways of redirecting a request using the URL ACL:

- Set the **Action** parameter to **Temporary Redirect** or **Permanent Redirect**, and specify the **Redirect URL**.
- Set the **Action** parameter to **Deny and Log**, set the **Deny Response** to **Temporary Redirect** or **Permanent Redirect** and specify the **Redirect URL**.

The first case is not considered an attack, therefore:

- It is logged at a lesser severity.
- Passive mode has no effect on it.

The second case is a suspected attack, therefore:

- It is logged at a higher severity.
- Passive mode is applied so that the request is not denied.

To create a URL ACL rule:

1. Go to the **WEBSITES > Allow/Deny Rules** page.
2. In the **URL : Allow/Deny Rules** section, identify the Service to which you want to add the URL

ACL rule.
3. Click **Add** next to the Service. The **Create ACL** window appears.
4. Specify appropriate values for the given fields and click **Save**.

For more information, click **Help** in the web interface.

Related Articles:

Allow/Deny Rules for Headers