Configuring Action Policy for Attack Groups

https://campus.barracuda.com/doc/4259924/

Go to **SECURITY POLICIES > Action Policy** to configure for each security policy what action to take when a violation occurs. Discrete Action Policies can be configured for the following attack groups:

- **advanced-policy-violations**
- **application-profile-violations**
- **param-profile-violations**
- **protocol-violations**
- **request-policy-violations**
- **response-violations**
- **url-profile-violations**
- **header-violations**

To edit the action taken when a particular attack is detected, locate the respective **Attack Action Name** in the list and click **Edit** (in the **Options** column) next to it.

You can choose from the response to a request deemed an attack by this security policy:

- **Protect and Log**: Blocks any request containing the specified attack and logs the attack.
- **Protect and no Log**: Blocks any request containing the specified attack without logging the attack.
- **Allow and Log**: Logs the violation.
- **None**: Ignores the violation.

For a description about the attack actions under each attack group, see Attacks Description - Action Policy .

Configuring Request Denials

If you choose an action policy that protects (denying attacks, whether logging or not), you must configure the Deny Response and Follow Up Actions for attacks.

Set **Deny Response** to one of the following options:

- *Close Connection*: Closes the connection to the sending client.
- *Temporary Redirect*: Redirects the request with the 302 status code to the URL specified in the parameter Redirect URL.
- *Permanent Redirect*: Redirects the request with the 301 status code to the URL specified in the parameter Redirect URL.

Redirect URL: Specifies the URL where the request is redirected if the deny response is set to *Temporary Redirect or Permanent Redirect*.
Redirect URL should be specified when the status code in HTTP status is one of 3xx redirect response codes.

Redirect URL should be specified in one of the following formats:

- **http://domain/url**
- **https://domain/url**
- **/url**

Where "url" and "domain" can be any ASCII strings. URL can be empty.

Examples: **http://secure.xyz.com/error.html** , **https://secure.xyz.com/logerror.cgi** , or **/error.html**

- **Send Response:** Sends the response indicated in **Response Page**.
  Response Page: Specify the response page to be sent to the client.

Configure a **Follow Up Action** taken when a request is denied by choosing from the following:

- *None*: Ignores the violation.
- *Block Client* IP: Blocks the sending client for the time specified in **Follow Up Action Time**.
- *Challenge with CAPTCHA:* Denies the response, and any subsequent requests from the same client IP address will be tracked for the next 900 seconds and will be challenged with a CAPTCHA image. The client will not be allowed to access any further resource until the CAPTCHA is answered. This is to thwart any reconnaissance efforts from the automated clients that are found to be suspicious due to such attack activity. The number of attempts for solving such a CAPTCHA challenge is five (5), and the number of re-fetches of the CAPTCHA image allowed is 128. Such tracked client IP addresses will have to answer the CAPTCHA if they are idle for more than 300 seconds. Note that the **Follow Up Action Time** has no relevance to this option.

Follow Up Action Time: Specifies the time in seconds to block the sending client if **Follow Up Action** is set to *Block Client IP*.

- **Range**: 1 to 600000
- **Units**: Seconds

Click **Help** on the **SECURITY POLICIES > Action Policy** page for more information about configuring action policy.