Configuring Action Policy

https://campus.barracuda.com/doc/4259856/

Action policy is a collection of settings that decide what action to be taken when a violation occurs. It consists of a set of attack groups and associated attack actions with it. The following attack groups are available:

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

The attack action specifies the action to be taken for a particular type of web attack. The attack action can be modified by clicking **Edit** next to it. For description about the attack actions under each attack group, see Attacks Description - Action Policy.

Steps to Edit an Attack Action Policy

1. Go to the **SECURITY POLICIES > Global ACLs** page.
2. Select the policy from the **Policy Name** drop-down list.
3. In the **Action Policy** section, identify the attack action and click **Edit** next to it. The **Edit Attack Action** window appears. Specify values for the following:
    1. **Action** – Select the action to be enforced when this attack is encountered.
        1. **Protect and Log** – Blocks any request with the specified attack with a log message.
        2. **Protect and no Log** – Blocks any request with the specified attack with no log message.
        3. **Allow and Log** – Logs the request error.
        4. **None** – Allows the request by ignoring the violation.
    2. **Deny Response** – Select the response to be sent to the client if the request is denied. A deny response is used when **Action** is set to *Protect and Log* or *Protect and no Log*.
        1. **Close Connection** – Closes the connection to the client sending the invalid request.
        2. **Send Response** – Sends the specified response page for the denied request.
        3. **Temporary Redirect** – Redirects the request with the 302 status code to the URL specified in the **Redirect URL** field below.
        4. **Permanent Redirect** – Redirects the request with the 301 status code to the URL specified in the **Redirect URL** field below.
    3. **Redirect URL** – Enter the URL to be used to redirect the request if the deny response is set to **Redirect**. The Redirect URL should be specified when the status-code in HTTP Status is one of 3xx redirect response codes.

        The parameter "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
/error.html

4. **Response Page** – Select the response page to be sent to the client, if the parameter **Deny Response** is set to *Send Response*.
5. **Follow Up Action** – Select the follow up action to be taken if the request is denied.
   - **None** – Allows the request by ignoring the violation.
   - **Block Client-IP** – Determines whether you need to block any subsequent request from the same client for the time specified in **Follow Up Action Time**. Subsequent requests will be blocked for a specific service or for all services based on the configuration made in the Advanced Settings page.
   - **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 which 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.

1. **Follow Up Action Time** – Specify the time in seconds to block the client IP, if **Follow Up Action** is set to *Block Client IP*.
   - **Range**: 1 to 600000
   - **Units**: Seconds

4. Click **Save**.