Configuring Cloaking

https://campus.barracuda.com/doc/4259864/

Cloaking prevents hackers from obtaining information that could be used to launch a successful subsequent attack. HTTP headers and return codes are masked before sending a response to a client. The response headers are filtered based on the headers defined in the Headers to **Filter** field.

Cloaking features include:

- Removing banner headers such as "Server" etc from responses.
- Blocking client error (status code 4xx) and server error (status code 5xx) responses.

Steps To Configure Cloaking

1. Go to the **SECURITY POLICIES > Cloaking** page.
2. Select the policy from the **Policy Name** drop-down list for which you want to modify cloaking settings.
3. In the **Cloaking** section, specify values for the following fields:
    1. **Suppress Return Code** – When set to *Yes*, the Barracuda Web Application Firewall blocks an HTTP Status code in the response header and inserts a default of custom response page in case of any error responses from the server. Two types of response error codes are suppressed:
        1. **4xx (client):** These are 400-series error codes. These codes are intended for instances when a client seems to have erred when attempting to access a Web page.

            The codes 401 and 407 are not suppressed since these are for authentication and the clients need to see them to return the authentication credentials. **Example**: 404: Page not found.

            .
        2. **5xx (server):** These are 500-series error codes. These codes are intended to indicate that a server is aware that it has a problem or that it is incapable of performing a request. Example: 500: Internal Error.
            - **Values**: Yes, No
            - **Recommended**: Yes
    2. **Filter Response Header** – Set to *Yes* to remove HTTP headers in the response before relaying to the client. The HTTP headers are filtered based on the headers defined in the **Headers to Filter** field below.
        - **Values**: Yes, No
        - **Recommended**: Yes
    1. **Headers to Filter** – Define the HTTP headers to be removed from the response before serving it to the client.

        If "set-cookie" header is added to **Headers to Filter** and **Cookie Security** is enabled, then set-cookie header is not filtered from the response.
4. Click **Save**.

When **Suppress Return Code** is set to *Yes*, the Barracuda Web Application Firewall inserts a default or custom response page in case of any error responses from the server. Typically, the Barracuda Web Application Firewall uses the default response page for error responses from the server. You can define custom response page on the **ADVANCED > Libraries > Response Pages** section using **Add Response Page**. The default response page can be replaced with the custom response page on:

- **SECURITY POLICIES > Action Policy**
- **SECURITY POLICIES > Global ACLs > Existing Global ACLs**
- **WEBSITES > Allow/Deny > URL : Allow/Deny Rules**