Configuring Global ACLs

https://campus.barracuda.com/doc/4259851/

Global ACLs (URL ACLs) are strict allow/deny rules shareable among multiple services configured on the Barracuda Web Application Firewall. They are associated with configured Security Policies. The default global ACLs configured in the SECURITY POLICIES page are:

- access-control-login-url - The ACL is displayed when AAA is enabled on the service and is used to process the Login requests.
- apache_range_header_vulnerability - The ACL is used to block the requests that try to misuse the apache range header vulnerability.
- backups-prefix-copy - The ACL is used to block the requests trying to access backup files on the application.
- backups-prefix-hash - The ACL is used to block the requests trying to access backup files on the application.
- backups-suffix-bak - The ACL is used to block the requests trying to access backup files on the application.
- backups-suffix-old - The ACL is used to block the requests trying to access backup files on the application.
- backups-suffix-sav - The ACL is used to block the requests trying to access backup files on the application.
- favicon.ico - The ACL is used to allow access to favicon.ico file of the application.
- phpinfo - The ACL is used to deny access to phpinfo.php file on the application to avoid disclosing the sensitive php settings of the application.
- robots.txt - The ACL is used to make robots.txt file accessible to all without exception.
- translate-f-vulnerability - The ACL is used to block any attempts the client makes to misuse Translate:f vulnerability that exposes IIS files source.

Steps to Configure Global ACLs

1. Go to the **SECURITY POLICIES > Global ACLs** page.
2. Select the policy from the **Policy Name** drop-down list.
3. In the **Create Global ACL** section, specify values for the following:
    1. **URL ACL Name** – Enter a name for the URL ACL.
    2. **URL Match** – Enter a URL to be matched against the URL in the request. The URL should start with a "/" and can have at most one " * " anywhere in the URL. Examples: /Bank/Forms/*, /images/*.
    3. **Extended Match** – Define an expression that consists of a combination of HTTP headers and/or query string parameters. This expression is used to match against special attributes in the HTTP headers or query string parameters in the requests. Use '*' to denote "any request", that is, do not apply the Extended Match condition. For information on how to write extended match expression, see Extended Match Syntax Help.
    4. **Extended Match Sequence** – Enter a number to indicate the order in which the extended match rule must be evaluated in the requests.
        - **Range**:1 to 1000

- **Default**: 1

5. **Action** – Select the action from the drop-down list to be taken on the request matching this URL.
    1. *Process* – Processes any request matching this ACL.
    2. *Allow* – Allows the request by disabling all security checks on an incoming request that matches the ACL. It also disables Data Theft on such responses.
    3. *Deny and Log* – Denies any request matching this ACL and also logs the event. The request is not subjected to any security policies. This is an unconditional Deny. When a request is denied, the Barracuda Web Application Firewall sends a cryptic error response.
    4. *Deny with no Log* – Same as Deny, but the event is not logged.
    5. *Temporary Redirect* – Redirects the denied request with the 302 status code to the URL specified in the **Redirect URL** field.
    6. *Permanent Redirect* – Redirects the denied request with the 301 status code to the URL specified in the **Redirect URL** field.
6. **Redirect URL** – Specify a URL to which a user should be redirected if **Action** is set to *Redirect.*
7. **Follow Up Action** - Select the required follow-up action to be taken whenever the request is denied.
    - *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.
    - ***Block Client Fingerprint*** - Blocks all requests from the client fingerprint to the service for the time specified in **Follow Up Action Time**.
    - ***Tarpit Client*** - Puts the clients into Tarpit whose risk scores have crossed the suspicious value for the time specified in **Tarpit Inactivity Timeout**.
        - ***Backlog Requests Limit*** - The total number of requests that are held in a backlog to be served from a tarpitted client.
          Values: 0 to 100
          Recommended: 50
        - ***Tarpit Inactivity Timeout*** - The idle timeout time in seconds, after which the client will be removed from the tarpit.
          Values: 300 to 36000 secs
          Recommended: 300 secs

1. **Follow Up Action Time** - Specify the time (sec) to block the client IP if **Follow Up Action** is set to **Block Client-IP**. The time can range between 1 to 600000 seconds.

4. Click **Add**.