Client-Side Protection

https://campus.barracuda.com/doc/95259558/

A supply chain attack is a type of cyber attack that can damage an organization, individual departments, or an entire industry by targeting and attacking less-secure or the weakest elements of a supply chain.

Client Side Protection can be enabled for individual pages or for a group of pages that use the same set of resources. The administrator must first add a Client Side Protection rule for a service and then configure Content Security Policy (CSP) or Sub-Resource Integrity (SRI) policies based on the requirements.

- To add an SRI, select the page for which you want to add an SRI. Then, from the **Actions** column, click the drop-down list and select **Add SRI**. You can also choose to **Edit/Delete** from the drop-down to update or delete an SRI.

Add Rule

Perform the following steps to add a rule:

1. Go to **WEBSITES > Client Side Protection**.
2. On the **Client Side Protection** section and from the **Actions** column, click the **Add Rule** link for the service that needs a rule to be created.
3. In the **Content Security Policy** window, specify the values for the following fields:
   - **Rule Name** - Specify a name for the CSP/SRI rule.
   - **Status** - Specify the status of the CSP/SRI rule. Set to **On** to add content-security-policy header in the response if CSP has been configured, or add integrity token in the response if SRI policy has been defined under the rule.
   - **URL Match** - Specify the URL to be matched to the URL in the request. The URL should start with a "/" and can have at most one " * " anywhere in the URL. A value of /* means that the profile applies for all URLs in that domain. Example: /*/index.html/public/index.html
   - **Host Match** - Enter a host name to be matched against the host in the request. This can be either a specific host match or a wildcard host match with a single * anywhere in the host name. For example, *.example.com. Any request matching this rule should have to go through the Page Integrity validation before accessing the page.
   - **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 more

information on how to write an extended match expression, see Extended Match Syntax Help.

  - **Extended Match Sequence** - Enter a number to indicate the order in which the URL is to be matched to the URL in the request. The URL should start with a "/" and can have at most one " * " anywhere in the URL.

For viewing the CSP violations generated by clients, see Client-Side Protection Dashboard.

The CSP Dashboard requires the Advanced Bot Protection License to be enabled.