How to Enable WebSocket Security

https://campus.barracuda.com/doc/95262402/

WebSocket Security inspects and secures WebSocket connections and data being transferred through those connections by enforcing protocol checks and various other security validations.

A default WebSocket profile is created for every service with the status OFF. When the WebSocket profile status is enabled, a request rewrite rule to remove sec-web socket-extensions is automatically added under **WEBSITES > Website Translations > HTTP Request Rewrite**. The name of the rule is "remove-sec-Web Socket-extensions-header".

Currently, data payload checks such as inspecting data for injection attacks can only be applied to data being transferred in JSON format.

For Binary payload, only protocol level checks (like verifying the WebSocket frame headers) are performed. For JSON payload, you MUST configure a matching JSON profile under **WEBSITES > JSON Security**. Also, enable **Enforce JSON Checks** under **WEBSITES > Web Socket Security > Add/Edit Web Socket Security Policy > Message Security** for the corresponding WebSocket profile.

> Any configuration changes made to the WebSocket profile is applicable ONLY to the new connections, and NOT to the existing connections.

Enable WebSocket Security for a Service

Perform the following steps:

1. Go to the **BASIC > Services** page, **Services** section.
2. Identify the service to which you want to enable WebSocket security, and click **Edit** next to the service.
3. On the **Service** window, scroll down to the **Advanced Configuration** section, and set **Enable WebSocket** to **Yes**.

   > If you want the Barracuda Web Application Firewall to behave like a WebSocket proxy ONLY and do not want to process the WebSocket frames, then skip the configuration steps below.
4. Create a WebSocket Profile. Refer to the **Steps to Add a WebSocket Profile** section.
5. Create a JSON Profile ONLY if **Message Format** is JSON and **Enforce JSON Checks** is set to **Yes** under **WEBSITES > Web Socket Security > Add/Edit WebSocket Security Policy >**

Message Security.

When a service is created, a default WebSocket profile is created for that service. You can add multiple WebSocket profiles for the service on the **WEBSITES > Web Socket Security** page. To modify an existing WebSocket policy, select **Edit** from the drop-down list under **Options** and fine-tune the settings as required.

Add a WebSocket Profile

Perform the following steps:

1. Go to the **WEBSITES > Web Socket Security** page.
2. In the **Web Socket Policy** section, click **Add** next to the service.
3. On the **Add Web Socket Security Policy** window, specify values for the following fields:

- **Web Socket Security Policy**
  - **Policy Name** - Enter a name for the WebSocket profile.
  - **Status** - Set to **On** to enforce checks on requests using this WebSocket profile.
  - **Mode** - Set the mode for the WebSocket profile.
    - **Active** - If the request violates the WebSocket profile settings, the request will be blocked if the Mode of the service on the **BASIC > Services** page is also set to **Active**. If the **Mode** of the service is set to **Passive** and the request violates the WebSocket profile settings, the request can pass through but logs the request errors on the **BASIC > Web Firewall Logs** page.
    - **Passive** - The requests are validated against the WebSocket profile settings and allows to pass through but logs the request errors on the **BASIC > Web Firewall Logs** page.
  - **Host** - 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 host is required to authenticate before accessing this page.
  - **URL** - This is used to specify the matching criterion for the URL field in the **Request Header**. The URL should start with a "/" and can have only one " * " anywhere in the URL. A value of /* means that the profile applies for all URLs in that domain. Example: /*
  - **Extended Match Sequence** - 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 and responses. Use '*' to denote "any request", that is, do not apply the Extended Match condition.
  - **Extended Match** - Enter a number to indicate the order in which the URL is to be matched to the URL in the request and response. The URL should start with a "/" and can have at most one " * " anywhere in the URL.
- **Protocol Security**.

- **Frame Size** - The maximum size allowed for the WebSocket frame.
- **Max Frame per Fragmented Message** - The maximum number of frames that a message can be fragmented into.
- **Payload Types** - The message format the user wants the Barracuda Web Application Firewall to process.
  - **TEXT** - Allows only TEXT payload to process over a WebSocket connection. On receiving a BINARY frame, the Barracuda Web Application Firewall terminates the WebSocket connection.
  - **BINARY** - Allows only BINARY payload to process over a WebSocket connection. On receiving a TEXT frame, the Barracuda Web Application Firewall terminates the WebSocket connection.
  - **BOTH** - Allows both TEXT and BINARY payload to process.

- **Message Security**:
  - **Enable Message Security** - Specify whether to enable the Barracuda Web Application Firewall to process the WebSocket frames.
    - **Yes** - The Barracuda Web Application Firewall processes ONLY TEXT payload.
    - **No** - ONLY WebSocket headers are processed by the Barracuda Web Application Firewall and NOT payload.
  - **Message Format** - Select the type of text payload transferred over WebSocket connection. It can be either **Plain Text** or **JSON** or any other format.
    - **JSON** - JSON security checks are applied on the WebSocket payload. Any attack in the payload can be detected through JSON security policies. Ensure that you provide the correct request method in **WEBSITES > JSON Security > Edit JSON Profile**.
      - **Enforce JSON Checks** - Set to **Yes** ONLY when the payload is JSON and JSON security policies need to be applied on the payload. Set to **No** when payload is either **Plain text** or **Binary**.
    - **Plain Text** - The payload is not a formatted data but plain text.
  - **Allowed Origin URI** - Specify the allowed origin URI. The URI must be specified in the following format:

    (scheme) "://" (hostname) [":" (port)]

    Currently the Allowed Origin URI feature does not support wildcards.