Generating JSON Policy and Key Profiles by Importing the OpenAPI Specification File

https://campus.barracuda.com/doc/91130328/

The Barracuda Web Application Firewall supports API Discovery for APIs that are built with the OpenAPI specification. You can import a new OpenAPI specification file or associate an existing specification file to a service. The OpenAPI schema in JSON/YAML for specification versions 2.0, 3.0, and 3.0.1 are supported for API Discovery.

The OpenAPI specification is a widely adopted standard for documenting APIs. They are easy to understand and enable users to secure their endpoints with ease while using the Barracuda Web Application Firewall. The OpenAPI Schema is represented through YAML or JSON files that are easy to read.

If the APIs are defined in an OpenAPI Specification file, you can easily import them to Barracuda Web Application Firewall.

Perform the following steps:

1. Go to the **WEBSITES > JSON Security** page.
2. In the **API Discovery** section, click **Import API Spec**. The **API Discovery Wizard** appears.
3. On the **API Discovery Wizard** window:
    1. **Service** - Select the service to which you want to associate the API specification file.
    2. **API Specs to be Used** - The specification file to be used for the selected service. Select **Import New Spec File** to import a new specification file. Select **Associate Existing Spec File** to choose a specification file from the existing API files. Swagger, Open API, and Google API files are supported.
    3. **API Spec Name** - Specify a name for the API specification file that is being uploaded.
    4. **API Specs to be Used** - This field is enabled only when the **Associate existing Spec file** option is selected. It lists all existing specification files that can be associated with a service.
    5. Click **Next**.
4. On the next **API Discovery Wizard** window:
    1. **Host/Domain Name** – Displays the domain name or IP address of the host that serves the API.
    2. **Base URL** – Displays the base URL to which the endpoint path is appended.
    3. **API Endpoints to Configure** – Displays the endpoint paths, REST method, Parameters and Rate Limit that are appended to the base URL. By default, all endpoint paths are selected. You can clear the check box next to the endpoint path if required. Use the down arrow button to modify the brute force values for endpoints.
    4. Click **Next**.
5. On the next **API Discovery Wizard** window:
    1. **JSON Profile** - When set to **Active**, the WAF enforces checks on the requests using this

JSON Profile. By default, the JSON Profile mode is set to **Active**. Click **Show Advanced Settings** and modify the values as required.

2. **URL Profile** - When set to **Active**, the requests are allowed or blocked by validating against this URL profile. By default, the URL Profile mode is set to **Active**. Click **Show Advanced Settings** and modify the values as required.
3. **Header ACLs** - When set to **Active**, the WAF blocks the request if an anomaly or intrusion is observed. By default, the URL Profile mode is set to **Active**. Click **Show Advanced Settings** and modify the values as required.
4. **Application DDoS Prevention** - When set to **On**, Slow Client Attack validation is enabled for the service.
5. Click **Next**.

6. On the next **API Discovery Wizard** window:
   1. **Configure Authentication and Authorization** - Select the authentication policy that needs to be associated with the service.
   2. Select the **Create Authorization Policies Based on the Spec File** check box.
      This option is available ONLY if there is a pre-configured OpenAPI authentication service on the Barracuda WAF. To add an OpenAPI authentication service, go to the **ACCESS CONTROL > Authentication Services** page.
   3. Click **Preview** to view the configuration.
   4. Click **Apply** to apply the schema through RESTful API.