Configuring XML Firewall to Protect a Web Application

https://campus.barracuda.com/doc/4259973/

The "XML Firewall" feature is available only in the Barracuda Web Application Firewall 660 and above.

Configure the XML Firewall with the following steps:

1. Turn on the XML Firewall on **WEBSITES > XML Validations**, by setting **Enable XML Firewall** to *Yes.*
2. Import the Schema file(s) and WSDL file for the web service you want to protect.
3. Bind the Imported Schema file(s) and WSDL file to the website; select the validations you wish to enforce and enable validation checking for the website.
4. View or modify the Validation Settings for the XML features you choose to enforce.

Import the Schema file(s) and WSDL file for the Web Service

Import the Schema file(s), and then the WSDL file for your website on the **WEBSITES > XML Validations** page **Import Schema/WSDL** section using the following steps:

1. Select the **File Type** you want to import: **SCHEMA** or **WSDL**.
   Import all Schema files and WSDL references before importing the WSDL file.
2. Enter the **Name** you want to appear in the display list for this imported file. For example: Encoding.
3. Optionally, you can enter the **Namespace** you want to appear in the display list for this imported file. For example: http://schemas.xmlsoap.org/soap/encoding.
4. Click **Browse...**, locate the desired file and select it.
5. Click **Import** to upload the file. It will appear in the Imported Schema/WSDLs display with the provided **Name** and **Namespace**.

Repeat the import process for all Schemas and WSDL references before importing the WSDL file.

Bind the Imported Schema file(s) and WSDL file to the Website

To bind the schema(s) and WSDL to the website, do the following:

1. Click **Add** next to the desired website in the **WEBSITES > XML Validations, XML Protected URLs** list to bind the imported WSDL to the URL you want to protect. The Add Protected URL window appears. Do the following settings:

1. **Data Format** – You must choose *SOAP* if you want to enforce WS-I Validations or SOAP Validations. Otherwise, you may choose ***XML*** to intercept generic XML data.
2. **Enforce WSDL** – Select the WSDL you want to bind to the website.
3. **URLs** - Enter the URL pattern you want to protect using XML Firewall. **Note**: Selectively choose URLs requiring SOAP or XML validations to avoid introducing unnecessary latency in serving requests.
4. **Direction** – Select *Requests, Responses* or *Both* to be validated with the bound WSDL.
5. **Enforce XML Validations** – Set to *Yes* to enforce the settings configured on **WEBSITES > XML Protection > XML Validation Settings.**
6. **Enforce WS-I Validations** – Set to *Yes* to enforce the settings configured on **WEBSITES > XML Protection > WS-I Basic Profile Assertions**. **Note**: **Data Format** must be ***SOAP*** for this setting to apply.
7. **Enforce SOAP Validations** – Set to *Yes* to enforce the settings configured in **WEBSITES > XML Protection > SOAP Validations**. **Note**: **Data Format** must be *SOAP* for this setting to apply.
8. Set **Status** to *On* to enable XML firewall validations for this website. To disable all of your **Enforce ... Validations** settings for this website, set **Status** to *Off.*

2. Click **Add** to save your settings and bind them to the selected website.
3. Click **Edit** from **WEBSITES > XML Validations, XML Protected URLs** list by the desired website to change the enforcement parameters, the direction of enforcement, or to turn off XML firewall for this website by setting **Status** to *Off*.
4. Click **Delete** to remove the WSDL binding on the web service.

View or Modify the Validation Settings for the XML Firewall

Default settings for validations are provided for the XML Firewall. You can edit those settings on the **WEBSITES > XML Protection** page of the web interface.