Configuring SAML on the Barracuda Web Application Firewall

https://campus.barracuda.com/doc/46896075/

Before proceeding with the SAML configuration on the Barracuda Web Application Firewall, download the metadata file from the IdP server. For more information on configuring the IdP server, see Configuring Identity Provider (IdP) for SAML Authentication.

Perform the steps below to configure SAML on the Barracuda Web Application Firewall.

Step 1 - Upload a Certificate on the Barracuda Web Application Firewall

For testing purposes, self-signed certificates (either uploaded or generated on the Barracuda Web Application Firewall) can be used for signing and encrypting SAML IdP requests and responses. In case of production environment, upload a CA-signed certificate on the Barracuda Web Application Firewall to be used for signing the requests sent to the IdP server, and decrypting the response received from the IdP server. The certificate can be uploaded on the **BASIC > Certificates** page, in the **Upload Certificates** section.

The uploaded certificate can be associated with the service for SAML authentication on the **ACCESS CONTROL > Authentication Policies** page, in the **Authentication Policies** section. Refer to Step 4 - Enable Authentication and Configure SAML Service Provider.

Step 2 - Create an HTTPS Service on the Barracuda Web Application Firewall

1. Go to the **BASIC > Services** page.
2. In the **Add New Service** section, specify values for the following:
   - **Service Name** - Enter a name for the service.
   - **Type** - Select **HTTPS**.
   - **Version** - Select the Internet protocol version (IPv4 or IPv6) for the service.
   - **Virtual IP Address** - Enter the virtual IP address that will be used for accessing this service.
   - **Port** - Enter the port number on which your web server responds.
   - **Version** - Select the Internet protocol version (IPv4 or IPv6) for the server that hosts the service.
   - **Real Servers** - Enter the IP address of the server that hosts the service. This is the backend server that is protected by the Barracuda Web Application Firewall.
   - **Service Groups** - Select the group under which the service should be added.
   - **Certificate** - Select the certificate you uploaded/generated in Step 1 - Upload a Certificate on the Barracuda Web Application Firewall .

- Click **Add**.

Step 3 - Configure a SAML IdP Authentication Service

The Identity Provider server should be configured as the authentication service on the **ACCESS CONTROL > Authentication Services** page, in the **SAML Identity Provider** tab. The Barracuda Web Application Firewall uses this information to communicate with the Identity Provider server to authenticate a user.

1. Go to the **ACCESS CONTROL > Authentication Services** page, select the **SAML Identity Provider** tab, and specify values for the following:
   - **Realm Name** – Enter a name to identify the SAML authentication service on the Barracuda Web Application Firewall.
   - **Identity Provider Name** - Enter a name to identify the Identity Provider on the Barracuda Web Application Firewall.
   - **Identity Provider Metadata Type** - Select **URL** or **File Upload** to associate the metadata file.
     - **Metadata URL** - Enter the URL to download the IdP metadata file. **Example**: https://login.windows.net/xxxxx/federationmetadata/2007-06/federationmetadata.xml
     - **Metadata File Upload** - Click the **Browse** button to select the Identity Provider metadata file. Use this option if you have already downloaded the metadata file.
2. Click **Add**.
3. SAML authentication service with the specified values gets created under **Existing Authentication Service.** The **Type** for the SAML authentication service will be displayed as "SAMLSP".

Step 4 - Enable Authentication and Configure SAML Service Provider

1. Go to the **ACCESS CONTROL > Authentication Policies** page.
2. In the **Authentication Policies** section, click on **Edit Authentication** next to the service to which you want to enable authentication.
3. In the **Edit Authentication Policies** window:
   1. Configure the following in the **Edit Authentication Policy** section:
      1. Set Status to *On*.
      2. Select the SAML authentication service created in Step 3 - Configure a SAML IdP Authentication Service from the **Authentication Service** drop-down list.
   2. Configure the following in the **SAML Service Provider Configuration** section:
      - **Organization Name** – Enter your organization name. This name will be used when the Barracuda Web Application Firewall sends SAML requests to the IdP.
      - **Organization URL** – Enter the URL of the organization. Example:

https://serviceprovider.com
- **Organization Display Name** – Enter a name to be displayed to the users accessing this service.
- **SP Entity ID** – Enter either the fully qualified domain name through which the service can be accessed *or* the SAML entity ID if you have any for the application. Example: https://waf.example.com/.
- Choose the signing certificate.

  It is recommended to select **Encryption Certificate** to avoid SAML vulnerability [CVE-2018-0486].

3. Specify values for other parameters as required.
4. Click **Save**.

Step 5 - Configure the Authorization Policy for the Service

1. Go to the **ACCESS CONTROL > Authentication Policies** page.
2. In the **Authentication Polices** section, click **Add Authorization** next to the service to which you want to configure the authorization policy. The **Add Authorization Policy** window opens.
3. In the **Add Authorization Policy** section, configure the following:
   1. **Policy Name** – Enter a name for the policy.
   2. Set **Status** to *On*.
   3. **URL Match** – Enter the URL that needs to be matched in the request. Any request matching the configured “URL” and “Host” is subjected to SAML authentication. For example, if the web server URL is https://www.abc.com/sports/Tennis/group1, https://www.abc.com/sports/Football/group1, etc., then the **URL Match** can be one of the following: "/sports/Tennis/group1” OR “/sports/Tennis/*" OR “/sports/*” OR “/*”.
   4. **Host Match** – Enter the host name to be matched against the host in the request. For example, if the web server URL is "https://www.abc.com", then the **Host Match** should be "www.abc.com".

      - Ensure that you enter the host name with which the service can be accessed.
      - The wildcard host match with a single * anywhere in the host name is not supported.

      If there is a real requirement for the “*” (star wildcard) character to be used in Host Match, you can do so in the following ways with the help of URL ACLs.
      1. Create a new URL ACL for the service, from **WEBSITES > Allow/Deny/Redirect** rules by mentioning all domains that should be allowed in the Extended match field.
      2. Set the action as **Deny and Log**. The domain separator operation should be “doesn’t contain”.
      3. Configure Allowed Domains from **WEBSITES > Website Profiles** that will make sure to validate requests/responses only for those domains against the URL and Parameter Profiles.
   5. **Enable Signing on AuthRequest** - When set to **Yes**, the "AuthnRequest" sent by the Barracuda Web Application Firewall to IdP is signed using the IdP's certificate taken from the IdP metadata.

6. **AuthnContextClassRef** - Enter the type of authentication to be used by the IdP. The following are the known authentication methods that are supported by the IdP that can be configured for **AuthnContextClassRef**.
   - urn:oasis:names:tc:SAML:2.0:ac_classes:TLSClient
   - urn:oasis:names:tc:SAML:2.0:ac_classes:PasswordProtectedTransport
   - urn:oasis:names:tc:SAML:2.0:ac_classes:X509
   - urn:oasis:names:tc:SAML:2.0:ac_classes:Kerberos
   - urn:oasis:names:tc:SAML:2.0:ac_classes:Password
   - urn:federation:authentication:windows
7. **Access Rules (Optional)** – Select the check box or check boxes next to the rules that need to be applied in the authorization policy. To create access rules, follow the steps mentioned in **Configuring Access Rules for SAML Attributes** in the Advanced Configuration for SAML Authentication article.
8. Specify values for other parameters as required and click **Save**.

Step 6 - Generate Service Provider (SP) Metadata

After you have configured the Barracuda Web Application Firewall, you must generate the metadata file of the SAML service provider (i.e., the Barracuda Web Application Firewall), and export the metadata file to the Identity Provider (IdP).

To Generate the metadata file of the SAML Service Provider (SP):

1. Go to the **ACCESS CONTROL > Authentication Policies** page.
2. In the **Authentication Policies** section, click **Generate** next to the service under **Metadata**.
3. Save the Service Provider (SP) metadata XML file to your local machine. **Example**: sp_metadata_app.xml, where “sp_metadata” indicates the Service Provider metadata file configured for the service “app”.

- If you modify an authorization/authentication policy associated with the service that was uploaded earlier to the Identity Provider, you must generate the Service Provider metadata file again and upload it to the Identity Provider. Follow the same procedure if you add another authorization policy to the service. Typically, SAML endpoints are created on a per-application basis and any change made in the authentication/authorization policy associated with the application may cause the application to not work properly. For this reason, you need to regenerate the metadata file and upload it to the Identity Provider.
- Some Identity Providers may not provide a metadata upload option. In such cases, SAML endpoints can be configured manually on Identity Provider. See Advanced Configuration for SAML Authentication.

Next Step

[Configuring Identity Provider (IdP) for SAML Authentication]