Configuring AzureAD for Open ID Connect on the Barracuda Web Application Firewall

https://campus.barracuda.com/doc/92767250/

Azure Active Directory (AD) is the identity provider responsible for authenticating users accessing web applications hosted on the Microsoft Azure cloud. Azure AD manages user identities along with applications. You should configure the Open ID Connect endpoints in Azure AD for web applications requiring protection from the Barracuda Web Application Firewall.

Perform the Following Steps to Configure Azure AD on the Barracuda Web Application Firewall

Step 1 - Create an HTTPS Service on the Barracuda Web Application Firewall.

For more information on how to create a HTTPS service, see Creating an HTTPS Service

Step 2 - Generate Azure AD Identity Provider Metadata URL

1. Log into the Microsoft Azure Portal.
2. In the left pane, select **Azure Active Directory** > **App registrations > New registration**.
3. Specify the name for the application.
4. Specify the redirect URI to redirect the user back to the application. Retain the other settings to default.
5. Click **Register**.
6. Click **Endpoints** and copy the **OpenID Connect METADATA DOCUMENT** link.
   The **Identity Provider Metadata URL** to be configured on the Barracuda Web Application Firewall in the **ACCESS CONTROL > Authentication Services** > **New Authentication Service** > **OpenID Connect** page is https://login.microsoftonline.com/<tenant_id>/v2.0/. well-known/openid-configuration.

Step 3 - Configuring the Azure AD OpenID Connect Provider on the Barracuda Web Application Firewall

1. Navigate to **ACCESS CONTROL > Authentication Services** and click the **OpenID Connect** tab.
2. In the **Realm Name** box, specify a name to identify the OpenID Connect.
3. In the **Open ID Connect Alias** box, specify the OpenID Connect alias name to identify the OpenID Connect provider on the Barracuda Web Application Firewall. *Example: AzureAD*
4. Choose **Discovery URL** as the mode to identify the provider's endpoint configuration. The end point URLs are automatically filled from the metadata URL.
5. Specify the metadata URL of the Azure AD OpenID Connect.
   Example: https://login.microsoftonline.com/4c2cee7c-97ca-4f42-88ea-6acf44978369/v2.0/.well-

known/openid-configuration

6. Click **Retrieve** to display the end point URLs in the fields by default (except for client/clientsec).
7. Configure the client ID and client secret that you noted down while performing the Azure AD configuration. Also, ensure that the Scope field has the openid displayed.
8. Click **Add**. AzureAD OpenID Connect authentication service is displayed in the **Existing Authentication Service** section.

Step 4 - Configure the Authentication Policy for the Service

1. Go to the **ACCESS CONTROL > Authentication Policies** page.
2. In the **Authentication Policies** section, for the service to which you want to enable authentication, click the drop-down list and select **Edit Authentication** from the **Options** column.
3. In the **Edit Authentication Policies** window, configure the following:
    1. Set Status to ***On*** .
    2. From the **Authentication Service** drop-down list, select the authentication service realm.
    3. Enter the redirect URL. Ensure that you use the same redirect URL that was configured on the Microsoft Azure Portal.
4. The login page is selected by default in the **Access Control Pages** section.
5. (optional) In the **OpenID Connect Claim Configuration** section, specify the claim name and local ID received from the identity provider that needs to be sent to the application server.
6. Click **Save**.

Step 5 - Configure the Authorization Policy for the Service

1. Go to the **ACCESS CONTROL > Authentication Policies** page.
2. In the **Authentication Policies** section, click on **Add Authorization** next to the service to which you want to enable authorization.
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. For example *"/*"*
    4. **Host Match** – Enter the host name to be matched against the host in the request. For example, *openid.selahcloud.in*
4. Click **Save**.