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.
   This is 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. Example: https://login.microsoftonline.com/<tenant_id>/v2.0/. well-known/openid-configuration

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

1. In the **Real Name** box, specify a name to identify the Open ID Connect provider on the Barracuda Web Application Firewall. *Example: AzureAD*
2. Choose **Discovery URL** as the mode to identify the provider's endpoint configuration.
3. Specify the metadata URL of the Azure AD Open ID Connect. Example: https://dev-9wh7d1r1.auth0.com/.well-known/openid-configuration
4. Click **Retrieve** to display all other details by default.

5. Configure the client ID and client secret that you had noted down while performing the Azure AD configuration and then click **Add**. AzureAD Open ID 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, click on **Edit Authentication** next to the service to which you want to enable authentication.
3. In the **Edit Authentication Policies** window, configure the following:
    1. Set Status to ***On***.
    2. Select the AzureAD authentication service created from the **Authentication Service** drop-down list.
    3. Verify the Redirect URL.
4. The login page is selected by default in the **Access Control Pages** section.
5. 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**.

Step 5 - Verify by Logging into the Microsoft Application.

Figures

1. AzureAD1.png
2. image2020-5-26 15:27:59.png
3. AzureAD2.png