Configuring OKTA for Open ID Connect on Barracuda Web Application Firewall

https://campus.barracuda.com/doc/92767218/

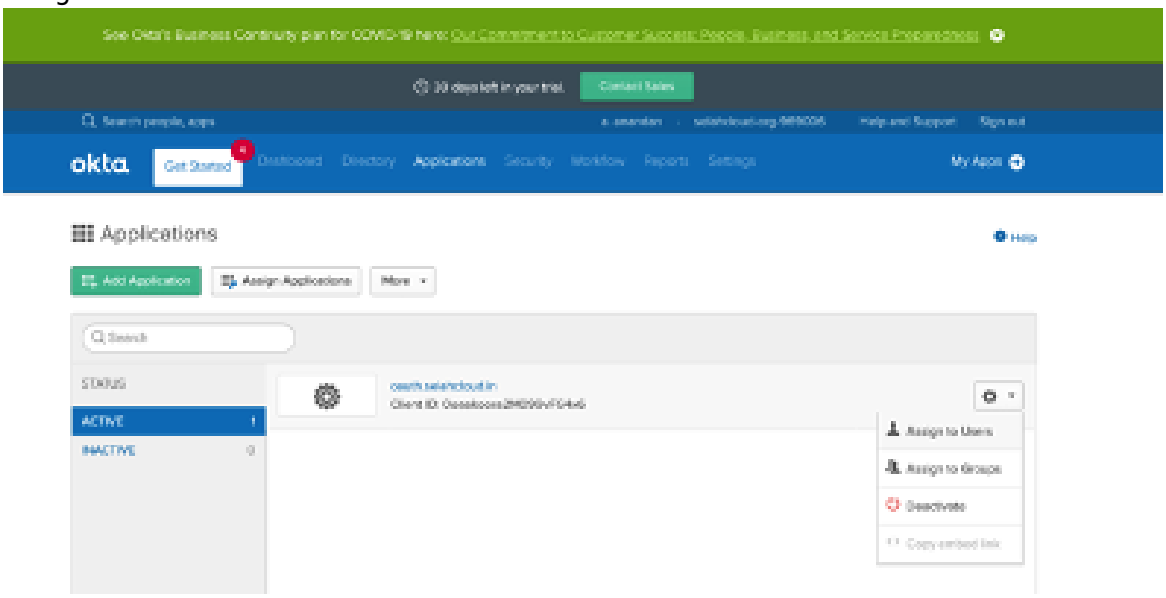
This section walks you through the steps on how to integrate the Barracuda WAF Access Control module with OpenID Connect-based authentication. The Barracuda Web Application Firewall allows customers to authenticate users in a simplified way using OpenID Connect. The URLs are personalized and can be referred here.

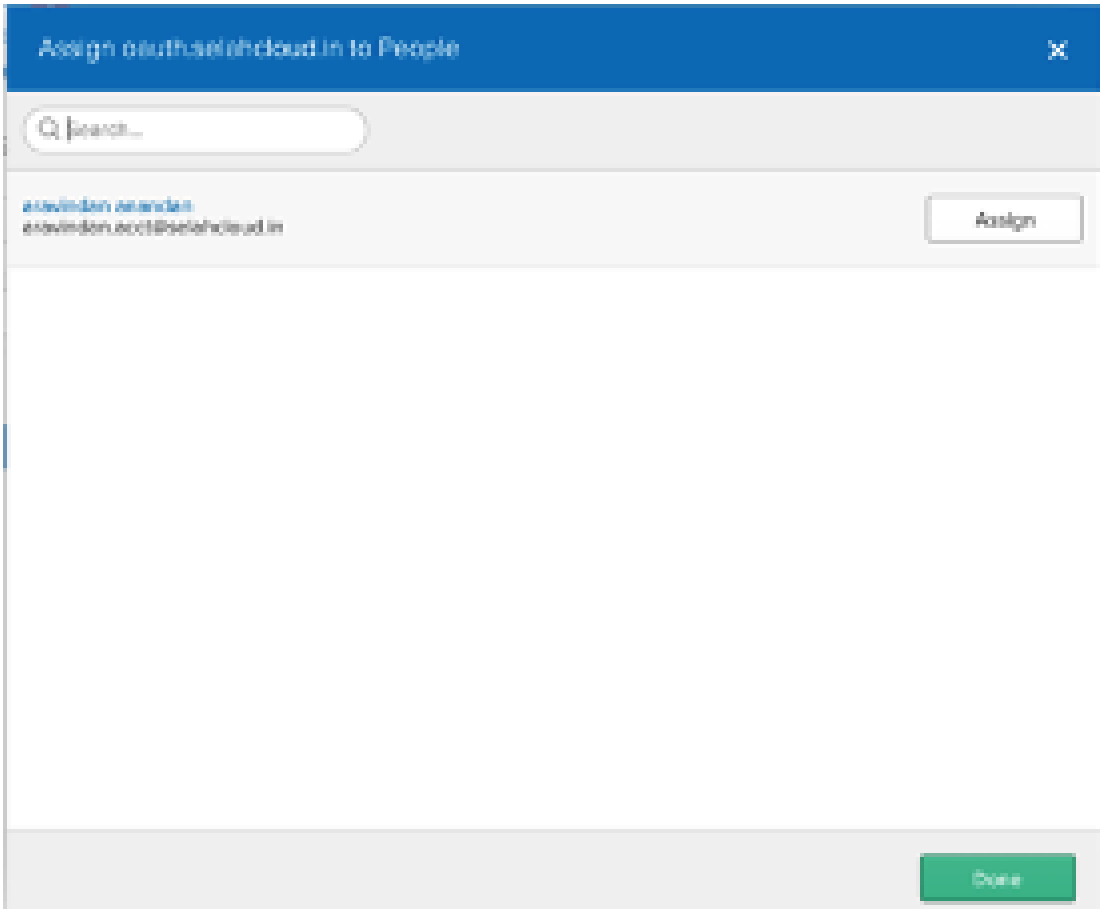
After installing OKTA, users will authenticate with OKTA through OpenID Connect for accessing the service hosted on the Barracuda Web Application Firewall. The authentication is done before allowing access to the application protected by the service on the WAF.

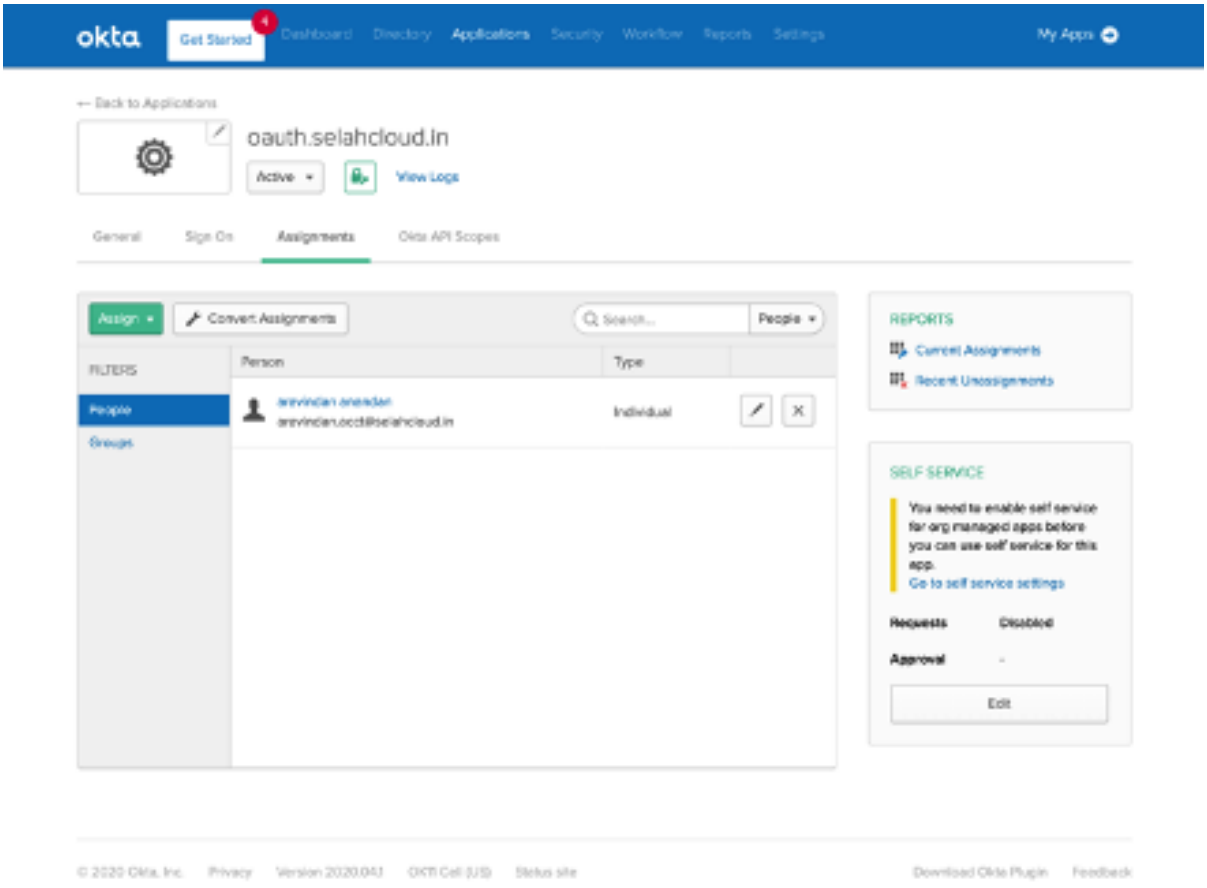
Step 1 : Configuring OKTA

Note: Before starting the configuration, ensure that you have an active account created on OKTA.

1. Log into the Okta Developer Dashboard and click **Applications** > **Create New App.**
2. In the **Create a New Application Integration** dialog box, select **OpenID Connect** and then click **Create**.
3. Enter the following details:
    1. Add the domain name of the application that you want to provide authentication.
    2. Configure the **Login Redirect URI** as *https://domain/openid-connect/redirect*
    3. Click **Save** to save the configuration. Also, make a note of the *client ID* and *Client Secret* strings.
4. Bind users to the application in OKTA. You can follow the instructions of the OKTA screens to assign users.




Assign
Done



5. OKTA OpenID Connect Discovery URL.
   The discovery URL is of the format: https://<oktadomain>/.well-known/openid-configuration
   Example https://selahcloudoauth.okta.com/.well-known/openid-configuration
   The domain name can be retrieved from the **Single Sign On** tab as shown below:

Step 2 : Configuring OKTA for OpenID Connect on the Barracuda Web Application Firewall

1. Log into the Barracuda Web Application Firewall and navigate to **ACCESS CONTROL > Authentication Services > Open ID Connect**.
2. In the **Realm Name** box, specify a name to identify the authentication service on the Barracuda Web Application Firewall. The **OpenID Connect Alias** name for the identity provider displays the application login page.
3. Enter the discovery URL and click **Retrieve** to display the end point URLs in the fields by default (except for client/clientsec).
4. Configure the client ID and client secret that you noted in the OKTA configuration. Also, ensure that the Scope field has the OpenID displayed.
5. Click **Add**. The OKTA OpenID Connect authentication service is displayed in the **Existing Authentication Service** section.
6. Configure the authentication policy and authorization rule for the service.

Step 3 - 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 OKTA server. For example, if the redirect URL configured on the OKTA server is *https://www.oauthtest.com/redirect.html*, then you can use */redirect.html* here.
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 4 - Configure the Authorization Policy for the Service

1. Go to the **ACCESS CONTROL > Authentication Policies** page.
2. In the **Authentication Policies** section, click **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.
4. Click **Save.**

Step 5 : Validating the Integration

1. Go to the URL for which the authorization rule exists. In this example the URL is https://oauth.selahcloud.in/index.html.
2. Select the OpenID Connect Realm and then click **Submit.**
3. Enter the credentials to log in.

Figures

1. okta4.png
2. okta5.png
3. okta6.png