Configuring OpenID Connect on the Barracuda Web Application Firewall

https://campus.barracuda.com/doc/92767152/

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

Step 1. 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 2. Configure an OpenID Connect Authentication Service

1. Go to the **ACCESS CONTROL > Authentication Service** page, **OpenID Connect** tab.
2. Enter information about your ClientID Connect:
   1. **Real Name** - Specify a name to identify the OpenID Connect provider on the Barracuda Web Application Firewall.
   2. **OpenID Connect Alias** - Specify the name of the OpenID Connect provider.
   3. **Endpoint Configuration** - Specify the mode identity provider's endpoint configuration.
   4. **Metadata URL** - Specify OpenID identity provider’s discovery URL.
   5. **Issuer** - Specify the issuer of the OpenID Connect provider.
   6. **Auth Endpoint** - Specify the endpoint of the OpenID Connect authorization.

7. **Token Endpoint** - Specify the token endpoint of the OpenID Connect provider.
8. **Client ID** - Specify the client ID of the OpenID Connect provider.
9. **Client Secret** - Specify the client secret of the OpenID Connect provider.
10. **JSON Web Key(JWK) URL** - Specify the endpoint URL of the OpenID Connect JSON web token.
11. **UserInfo Endpoint** - Specify the endpoint OpenID Connect user info

3. Click **OK.**

To modify OpenID Connect parameters, click **Edit** from the **Existing Authentication Services**.

Step 3. Enable Authentication and Configure OpenID Connect Claim Configuration

1. Go to the **ACCESS CONTROL > Authentication Policies** page.
2. In the **Authentication Policies** section, click the **Select** drop-down list under **Options** and select **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 OpenID Connect authentication service created in **Step 2 - Configure a OpenID Connect Authentication Service** from the **Authentication Service** drop-down list.
        3. Click **Show Advanced Settings** and configure the following:
            1. **Trusted Hosts**
                1. **Action** - Select the action (**Allow** or **Process**) to be taken for the trusted hosts accessing the service.
                2. **Group** - Select the trusted hosts group to which the selected trusted hosts **Action** needs to be applied.
            2. **Secure Access**
                1. **Login Processor Path** - Specify the URL that is handled by the proxy service for Authentication. This URL is not forwarded to the backend server. The request is served by reverse proxy service.
                2. **Redirect URL** - Specify the redirect URL. The authorization server redirects the user to the specified URL after the user is successfully authorized to access the application.

OpenID Connect Logout:

To log out the user session, you can redirect the user to the "REDIRECT URL" with a parameter named "logout". The value of the parameter contains the (encoded) URL to which the user is supposed to be redirected after the session ends.
For example, consider www.example.com as your application. To

end the user session, you should configure the logout button of www.example.com's as follows:
Logout

3. **Session Control**
    1. Configure the session control parameters with appropriate values.
2. Select the login, logout, or access denied page to authenticate users accessing the web applications that are protected by the OpenID Connect authentication service in the **Access Control Pages** section.
3. Configure the following in the **OpenID Connect Claim Configuration** section:
    1. **Claim Name** - Specify the claim received from the identity provider.
    2. **Local ID** - Specify the local ID name that needs to be sent to the application server.
    3. Click **Add**.
4. Click **Save**.

Step 4. 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".
    5. **Extended Match** - Enter an expression that consists of a combination of HTTP headers and/or query string parameters.
    6. **Extended Match Sequence** - Enter a number to indicate the order in which the extended match rule must be evaluated in the requests.
    7. **Login Method** - Select the login method (HTML Form, HTTP Basic Authentication or HTTP ActiveSync) to be used for authenticating the users.
    8. **Use Persistent Cookie** - When set to *Yes*, the authentication cookies set in the browser by the Barracuda Web Application Firewall are valid for the time period specified in **Persistent Cookie Timeout**.
    9. **Persistent Cookie Timeout** - Specify the time in minutes to keep the persistent cookie valid, after which the cookie expires.

10. **OpenID Connect Scope** - Specify the scopes supported by the OpenID provider.
    Each scope should be separated by a space.
11. Click **Save**

The following OpenID Connect configuration parameters are available when you edit an authorization policy:

- **Allow any Authenticated User** - Select **Yes** if you want to allow any authenticated user to access the specified URL.
- **Allowed Users** - Enter the list of allowed users to access the URL. For the OpenID Connect authentication method, users configured in the "Allowed Users" are matched against the "name" claim of the ID Token provided by the authorization server. Ensure that the ID Token contains the "name" claim for this feature to work.
- **Auth Not Done URL** - Enter the URL to redirect a user who attempts to access a protected URL before being authenticated. If the URL is not specified, the user is redirected to a login page generated by the Barracuda Web Application Firewall.
  To display your own web page instead of the login page generated by the Barracuda Web Application Firewall, use this parameter to redirect the user to a customized login page or an error page stating "Access to this page is restricted, and you have not logged in. Please visit the _login page_ to login."
  The redirect URLs need not reside in the same service. Also, these pages must be hosted outside the Barracuda Web Application Firewall, typically in the server of the application. The internal Barracuda Web Application Firewall pages cannot be customized.