Setting up Auth0 as an OpenID Connect provider

- Sign up for a free account at Auth0.
- Create an API:
  - Name: Border Gateway <bgw_domain>
  - Identifier: https://<bgw_domain>:443
  - Signing Algorithm: RS256
- This automatically creates an application named "Border Gateway <bgw_domain> (Test Application)".
- Adapt settings for this application:
  - Allow "Password" at Advanced settings / Grant types.
  - Enter "https://<bgw_domain>:443/callback" in field "Allowed Callback URLs"
- Create a User:
  - Email
  - Connection: Username-Password-Authentication
  - Check your e-mail to verify this account.
  - Add the following to field "user_metadata" (this is where you maintain the authorization rules for each user):

```
{
  "bgw_rules": "MQTT/# HTTPS/#"
}
```

- Tenant Settings:
  - Default Directory: "Username-Password-Authentication"
- Create rule:
  - Select template for an empty rule.
  - Rule name: Add bgw rules as additional claim
  - Code:

```
function (user, context, callback) {
  const namespace = 'https:///<bgw_domain>:443/';
  context.accessToken[namespace + 'bgw_rules'] = user.user_metadata.bgw_rules;
  callback(null, user, context);
}
```