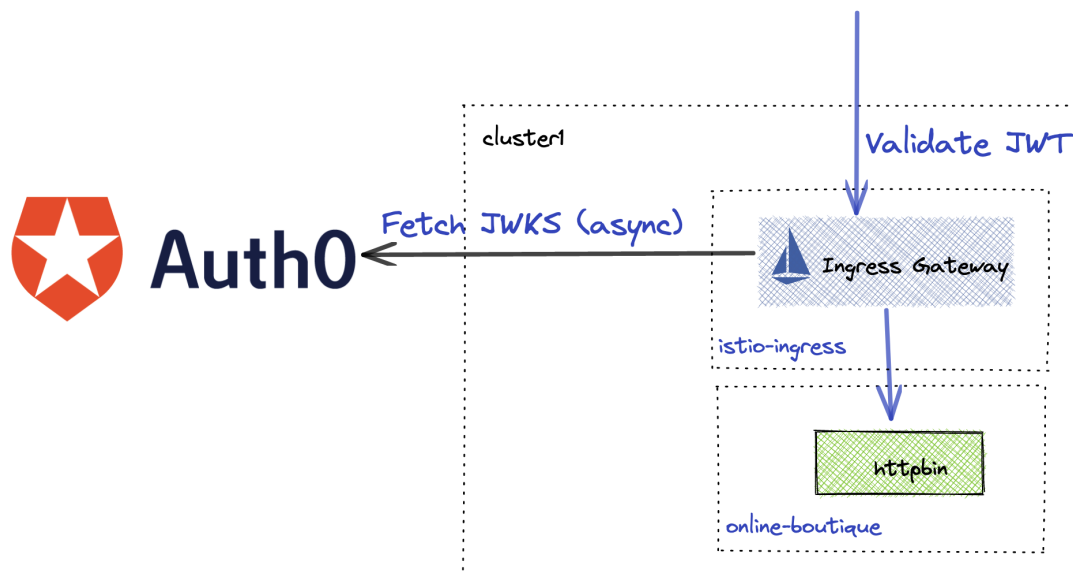# Lab 15 - Authentication / JWT + JWKS

One way for users to authenticate themselves is via JSON Web Tokens or JWT for short. Gloo Platform can validate JWT tokens against an external JSON Web Key Set (JWKS). Below is a lab that validates JWT tokens generated from an external provider Auth0.

Links:

- [External Authorization Docs](#)
- [JWTPolicy API](#)
- Reminder to set the `GLOO_GATEWAY_HTTPS` environment variable

```
export GLOO_GATEWAY_HTTPS=$(kubectl --context cluster-1 -n istio-ingress get svc -l
istio=ingressgateway -o jsonpath='{.items[0].status.loadBalancer.ingress[0].*}'):443

echo "SECURE Online Boutique available at https://$GLOO_GATEWAY_HTTPS"
```

Enforcing JWT Authentication

- Since JWT authentication is best viewed while accessing an API, first verify that the currency application is still availabile.

```
# get the available currencies
curl -k https://$GLOO_GATEWAY_HTTPS/currencies

# convert a currency
curl -k "https://$GLOO_GATEWAY_HTTPS/currencies/convert" \
--header 'Content-Type: application/json' \
--data '{
  "from": {
    "currency_code": "USD",
```

```
    "nanos": 0,
    "units": 8
  },
  "to_code": "EUR"
}'
```

- Since the Auth0 servers are not known to Gloo Platform, create an ExternalService reference.

```
kubectl apply --context management -f - <<EOF
apiVersion: networking.gloo.solo.io/v2
kind: ExternalService
metadata:
  name: auth0
  namespace: app-team
spec:
  hosts:
  - dev-64ktibmv.us.auth0.com
  ports:
  - name: https
    number: 443
    protocol: HTTPS
    clientsideTls: {}
EOF
```

- Enable JWT Authentication for the currency routes

```
kubectl apply --context management -f - <<EOF
apiVersion: security.policy.gloo.solo.io/v2
kind: JWTPolicy
metadata:
  name: currency
  namespace: app-team
spec:
  applyToRoutes:
  - route:
      labels:
        route: currency
  config:
    providers:
      auth0:
        issuer: "https://dev-64ktibmv.us.auth0.com/"
        audiences:
        - "https://currency/api"
        remote:
          url: "https://dev-64ktibmv.us.auth0.com/.well-known/jwks.json"
          destinationRef:
            ref:
              name: auth0
              namespace: app-team
              cluster: management
```

```
          kind: EXTERNAL_SERVICE
          port:
            number: 443
        enableAsyncFetch: true
      keepToken: true
EOF
```

- Call the currency API and get denied

```
curl -vk https://$GLOO_GATEWAY_HTTPS/currencies
```

Expected output

```
Jwt is missing
```

- Generate JWT from Auth0 using the below command

```
ACCESS_TOKEN=$(curl -sS --request POST \
  --url https://dev-64ktibmv.us.auth0.com/oauth/token \
  --header 'content-type: application/json' \
  --data
'{"client_id":"1QEVhZ2ERqZOpTQnHChK1TUSKRBduO72","client_secret":"J_vl_qgu0pvudTfGppm_1
kmy5KRCQDj5XHZbo5eFtxmSbpmqYT5ITv2h","audience":"https://currency/api","grant_type":"c1
| jq -r '.access_token')

printf "\n\n Access Token: $ACCESS_TOKEN\n"
```

- Call currency API using the Access token to authenticate

```
curl -vk -H "Authorization: Bearer $ACCESS_TOKEN"
https://$GLOO_GATEWAY_HTTPS/currencies
```

- Cleanup JWT policy

```
kubectl delete jwtpolicy currency --context management -n app-team
```