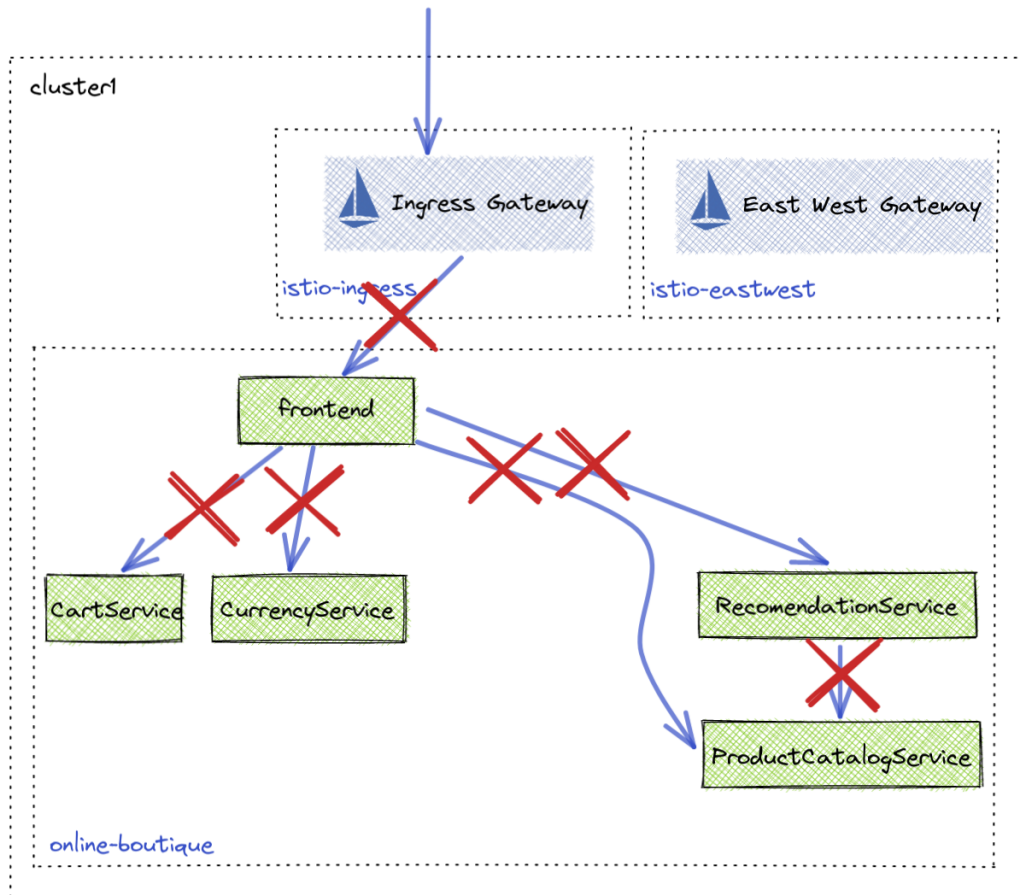


Lab 09 - Zero Trust Communication

Links:

- [Zero Trust Whitepaper](#)
- [Access Policy Docs](#)
- [AccessPolicy API](#)

Deploy Zero Trust Policy



- Disable all traffic by default for Application Team

```
kubectl apply --context management -f - <<EOF
apiVersion: security.policy.gloo.solo.io/v2
kind: AccessPolicy
metadata:
  name: allow-nothing
  namespace: app-team
spec:
  applyToWorkloads:
  - {}
  config:
```

```
authn:
  tlsMode: STRICT
authz: {}
EOF
```

- Test traffic to online-boutique

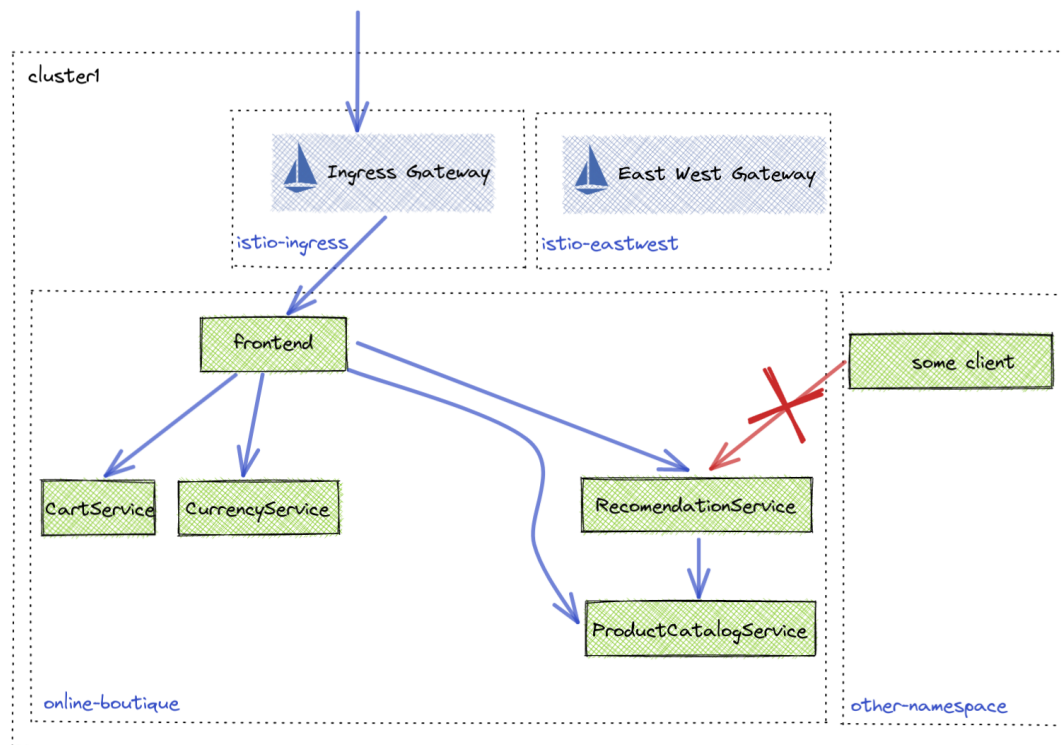
```
https://$GLOO_GATEWAY_HTTPS
```

- Optional curl

```
curl -k --write-out '%{http_code}' https://$GLOO_GATEWAY_HTTPS
```

Allow Fine Grain Access

Now that all traffic is denied by default, traffic needs to be allowed between the microservices for the Online Boutique to function.



- Allow access to the frontend from the ingress gateway

```
kubectl apply --context management -f - <<EOF
apiVersion: security.policy.gloo.solo.io/v2
kind: AccessPolicy
metadata:
```

```



name: frontend-ingress-access
namespace: app-team
spec:
  applyToDestinations:
  - selector:
      workspace: app-team
  config:
    authz:
      allowedClients:
      - serviceAccountSelector:
          workspace: ops-team
EOF

```

- Open online-boutique

```
https://$GLOO_GATEWAY_HTTPS
```

Cluster Name: cluster1 Locality: us-east-1/us-east-1a



Log out

Uh, oh!

Something has failed. Below are some details for debugging.

HTTP Status: 500 Internal Server Error

```

rpc error: code = PermissionDenied desc = RBAC: access denied
could not retrieve currencies
main.(*frontendServer).homeHandler
    /src/handlers.go:63
net/http.HandlerFunc.ServeHTTP
    /usr/local/go/src/net/http/server.go:2084
github.com/gorilla/mux.(*Router).ServeHTTP
    /go/pkg/mod/github.com/gorilla/mux@v1.8.0/mux.go:210
main.(*logHandler).ServeHTTP
    /src/middleware.go:81
main.ensureSessionID.func1
    /src/middleware.go:103
net/http.HandlerFunc.ServeHTTP
    /usr/local/go/src/net/http/server.go:2084
go.opencensus.io/plugin/ochttp.(*Handler).ServeHTTP
    /go/pkg/mod/go.opencensus.io@v0.23.0/plugin/ochttp/server.go:92
net/http.serverHandler.ServeHTTP
    /usr/local/go/src/net/http/server.go:2916
net/http.(*conn).serve
    /usr/local/go/src/net/http/server.go:1966
runtime.goexit
    /usr/local/go/src/runtime/asm_amd64.s:1571

```

- Allow frontend to reach apis in same namespace

```

kubectl apply --context management -f - <<EOF
apiVersion: security.policy.gloo.solo.io/v2
kind: AccessPolicy
metadata:
  name: in-namespace-access
  namespace: app-team
spec:

```

```
applyToDestinations:
- selector:
  workspace: app-team
config:
  authz:
    allowedClients:
      - serviceAccountSelector:
        workspace: app-team
EOF
```

- Refresh page