Automate mTLS communication with GoPay partners with Istio

Vijay Dhama, Gojek
Zufar Dhiyaulhaq, Gojek

Agenda

- GoPay & Istio
- Before mutual TLS
- Implementing mutual TLS
  - Centralized Certificate Management
  - Ingress mutual TLS
  - Egress mutual TLS
- Challenge & Future Works

GoPay & Istio

gojek

About gopay

- A few hundred developers
- Multiple Kubernetes Clusters
- 250+ microservices
- 150M+ internal API calls
- 3000+ deployments every week
- REST as well as gRPC services
- Services written in Golang, Java, Clojure, Ruby

gojek

gRPC, Envoy, and gopay

- GoPay has been using gRPC since 2016
- GoPay had services running on VM and decided to using Envoy XDS and Consul for migration & load balancing the traffic across container and VM.
- Over time, managing Envoy and Consul became a burden, as we have more than +250 microservices using Envoy and Consul for service discovery.

gojek

Istio

- We were using Envoy before which made it easy to adopt existing EnvoyFilters into Istio.
- Istio have abstraction concept that make manage things easier.

Before Mutual TLS?

HTTPS + Allowlisting

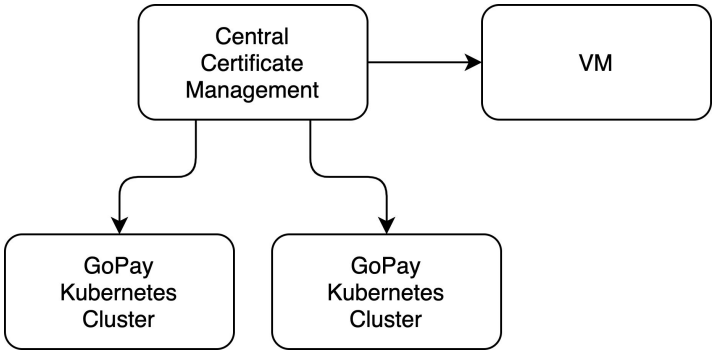
Our previous setup is using https with allow listing to only allow specific IP addresses to access our endpoints.

Drawback:

- Not the preferred approach suggested from security team
- Maintenance a lot of endpoint for each GoPay partner with specific IP seems burden job.
- Security concern about internal attacks (we don’t know who are using those IP, only service that communicate with us or it’s NAT IP that used by all services)

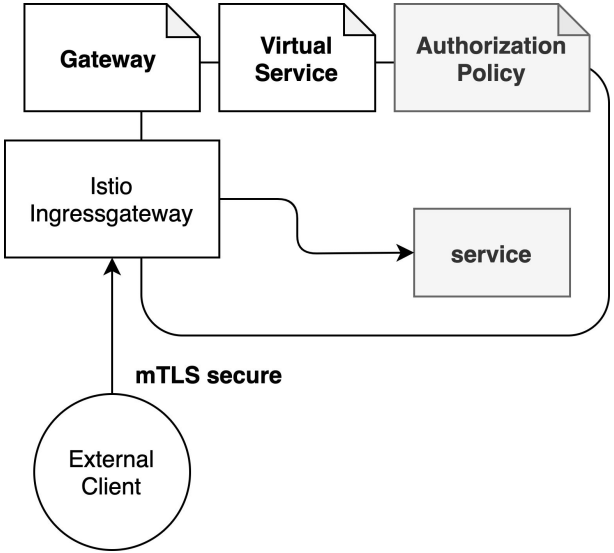
Implementing Mutual TLS

Centralized Certificate Management



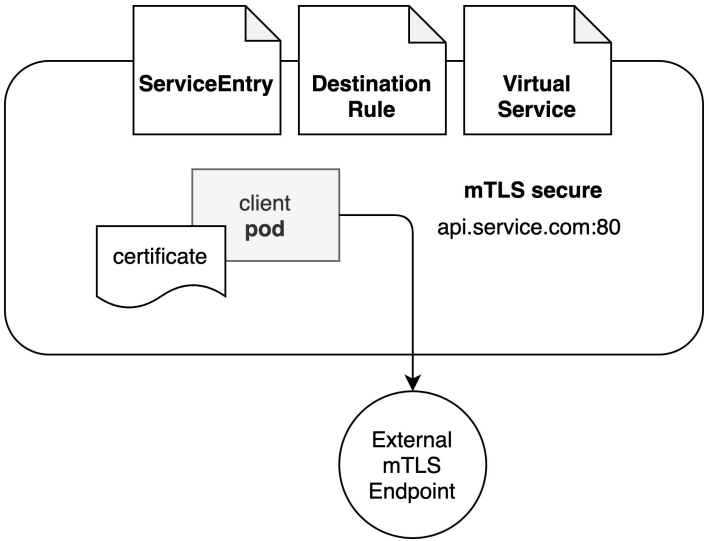
- Central certificate management manage our certificate lifecycle for HTTPS and mutual TLS communication.
- Renew & sync to our Kubernetes cluster, also support syncing to VM with an agent installed, this is also used by our partners as well.

Ingress Mutual TLS



- Using Istio Gateway mechanism with mode **MUTUAL**
- Leverage **subjectAltNames** to verify client SAN
- Additional **AuthorizationPolicy** to add IP allow listing

Egress Mutual TLS



- Using Egress TLS origination
- Certificate is mounted in the client deployments using annotation
  `sidecar.istio.io/userVolumeMount`
  `sidecar.istio.io/userVolume`
- Client talks with HTTP, upgraded automatically to mutual TLS by sidecar.

Challenge & Future Works

Challenge

- Client egress communication sometime got 503 error (Istio #26990). This is fixed by adding retry mechanism in the Virtual Service object.

Future Works

- Migrating Egress TLS origination mechanism to using Egress Gateway, we block because we are using Istio 1.6 and Egress gateway not support adding certificate via SDS (Istio #14039).

gojek

Thank You

#ThereIsAlwaysAWay