intuit turbotax quickbooks mint credit karma mailchimp

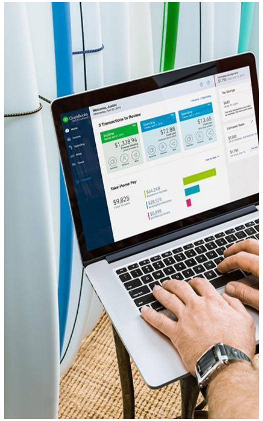
API Gateway on Service Mesh - Complete Zero Trust

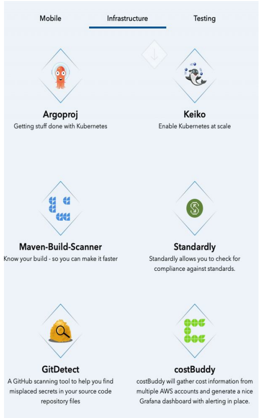
IstioCon, Apr 2022

Anil Attuluri
Shriram Sharma

Who We Are

1983	Founded
1993	IPO
19	Locations
$9.6B FY21	Revenue
60M	Customers
75	Projects





Argoproj
Getting stuff done with Kubernetes

Keiko
Enable Kubernetes at scale

Maven-Build-Scanner
Know your build - so you can make it faster

Standardly
Standardly allows you to check for compliance against standards.

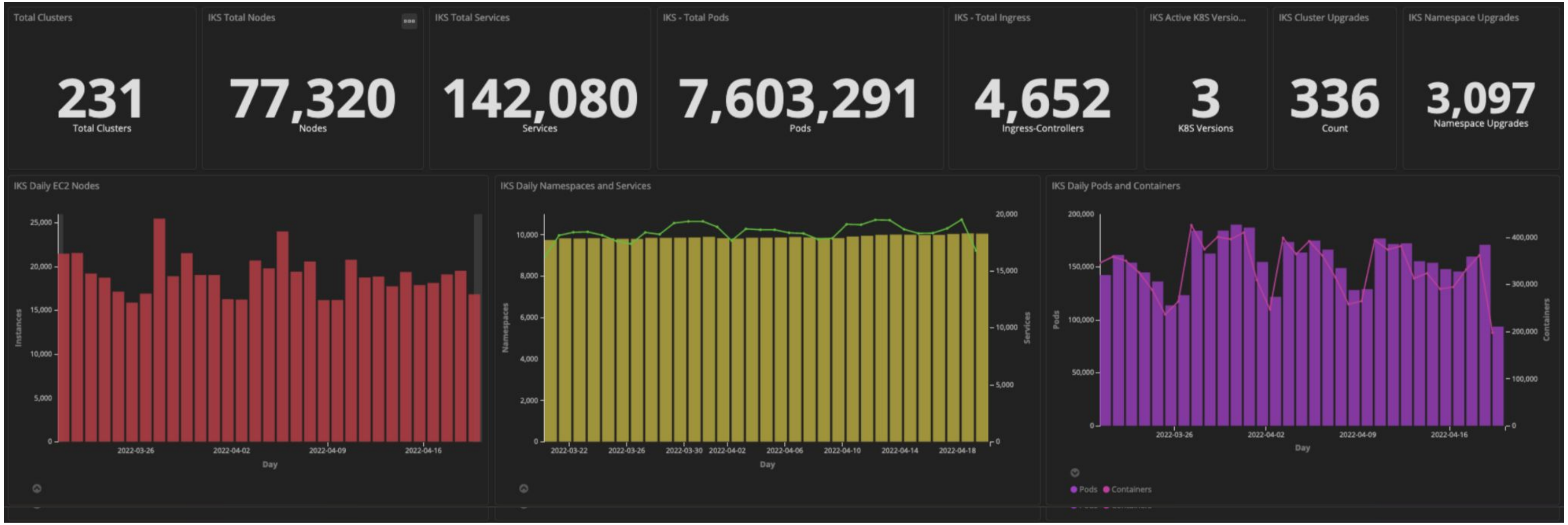
GitDetect
A GitHub scanning tool to help you find misplaced secrets in your source code repository files

costBuddy
costBuddy will gather cost information from multiple AWS accounts and generate a nice Grafana dashboard with alerting in place.

Intuit Scale Statistics

- 900+ Teams
- 5000+ Developers

- 200+ Clusters
- 7000+ Namespaces
- ~77,320 Nodes



Total Clusters
231
Total Clusters

IKS Total Nodes
77,320
Nodes

IKS Total Services
142,080
Services

IKS - Total Pods
7,603,291
Pods

IKS - Total Ingress
4,652
Ingress-Controllers

IKS Active K8S Versio...
3
K8S Versions

IKS Cluster Upgrades
336
Count

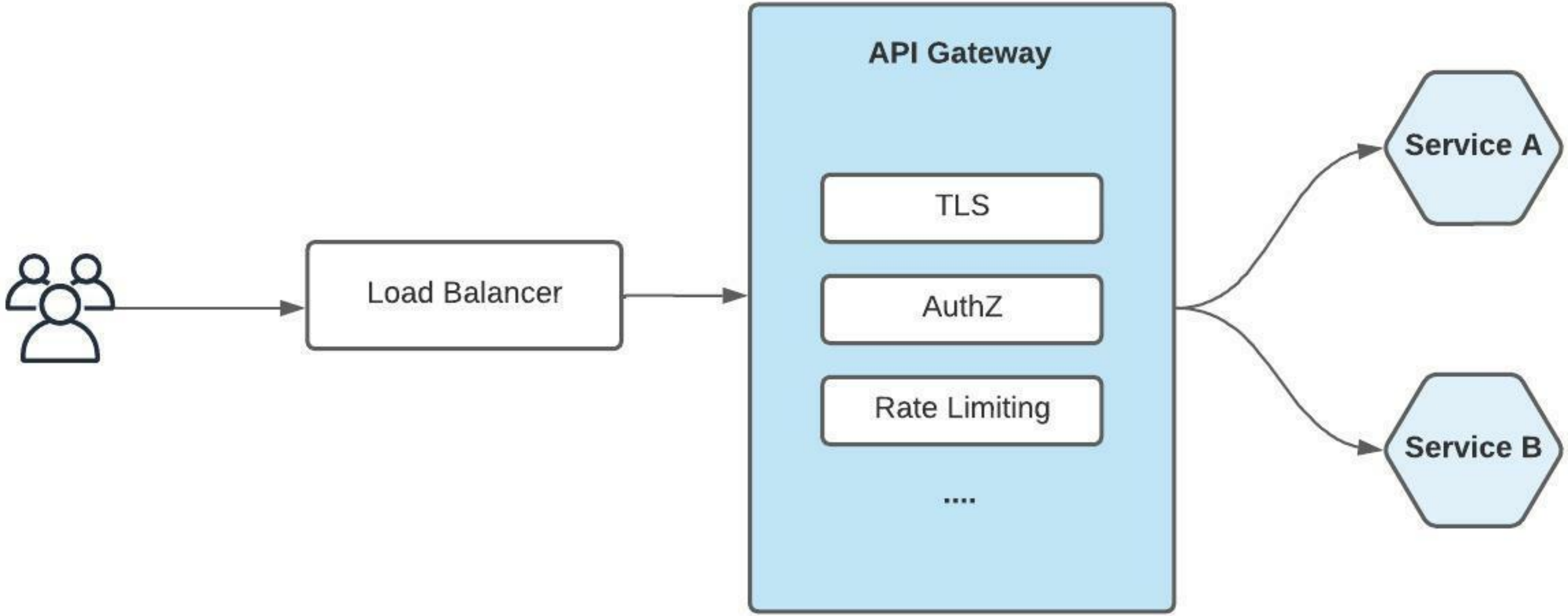
IKS Namespace Upgrades
3,097
Namespace Upgrades

IKS Daily EC2 Nodes

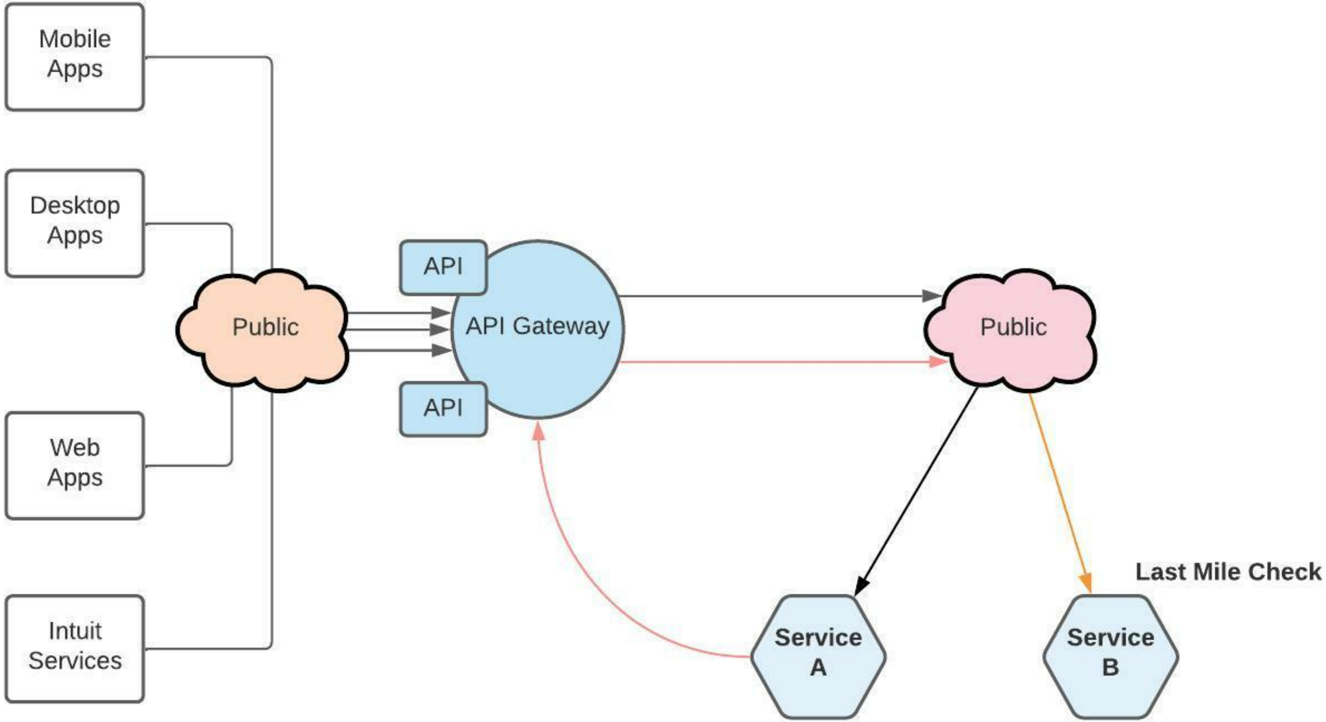
IKS Daily Namespaces and Services

IKS Daily Pods and Containers

API Gateway

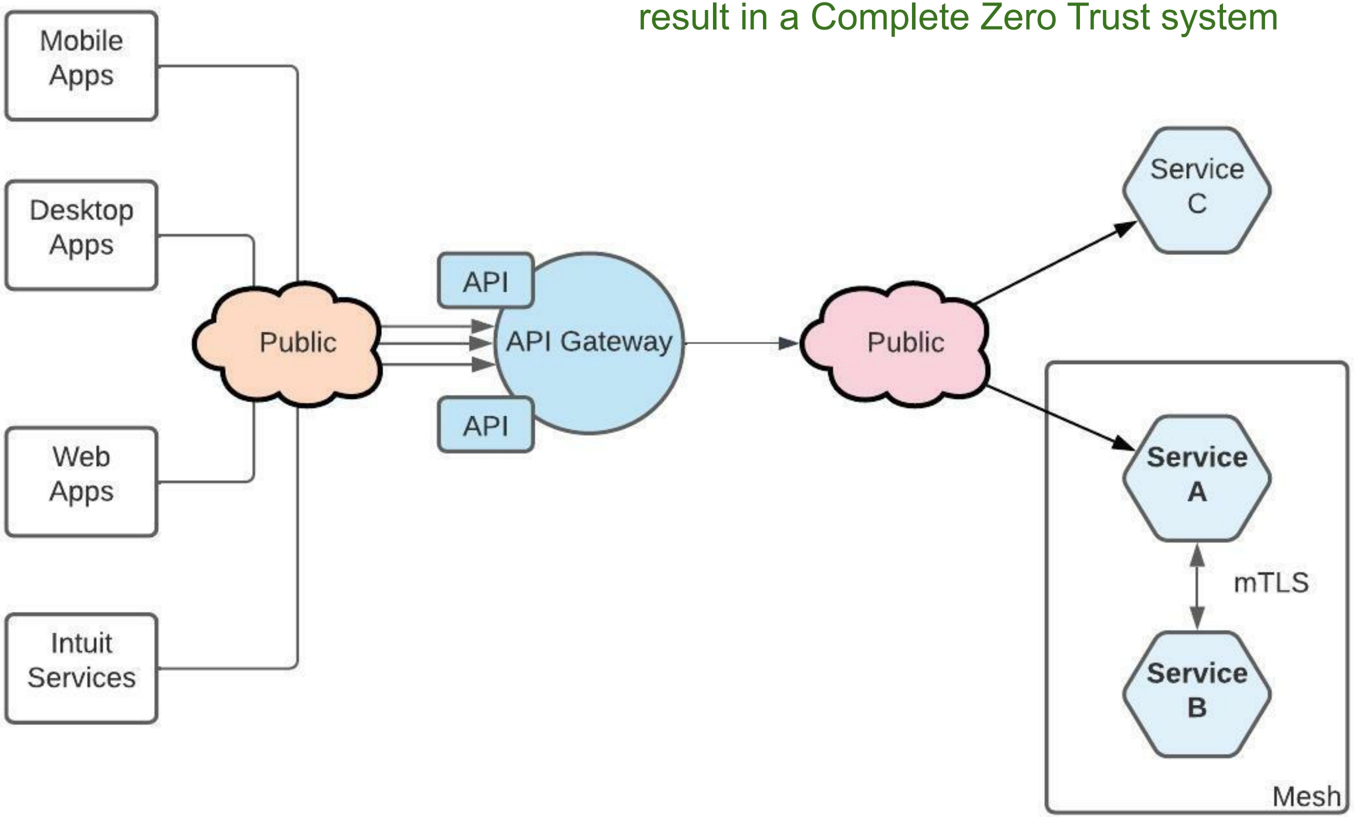

Load Balancer
API Gateway
TLS
AuthZ
Rate Limiting
....
Service A
Service B

API Gateway at Intuit

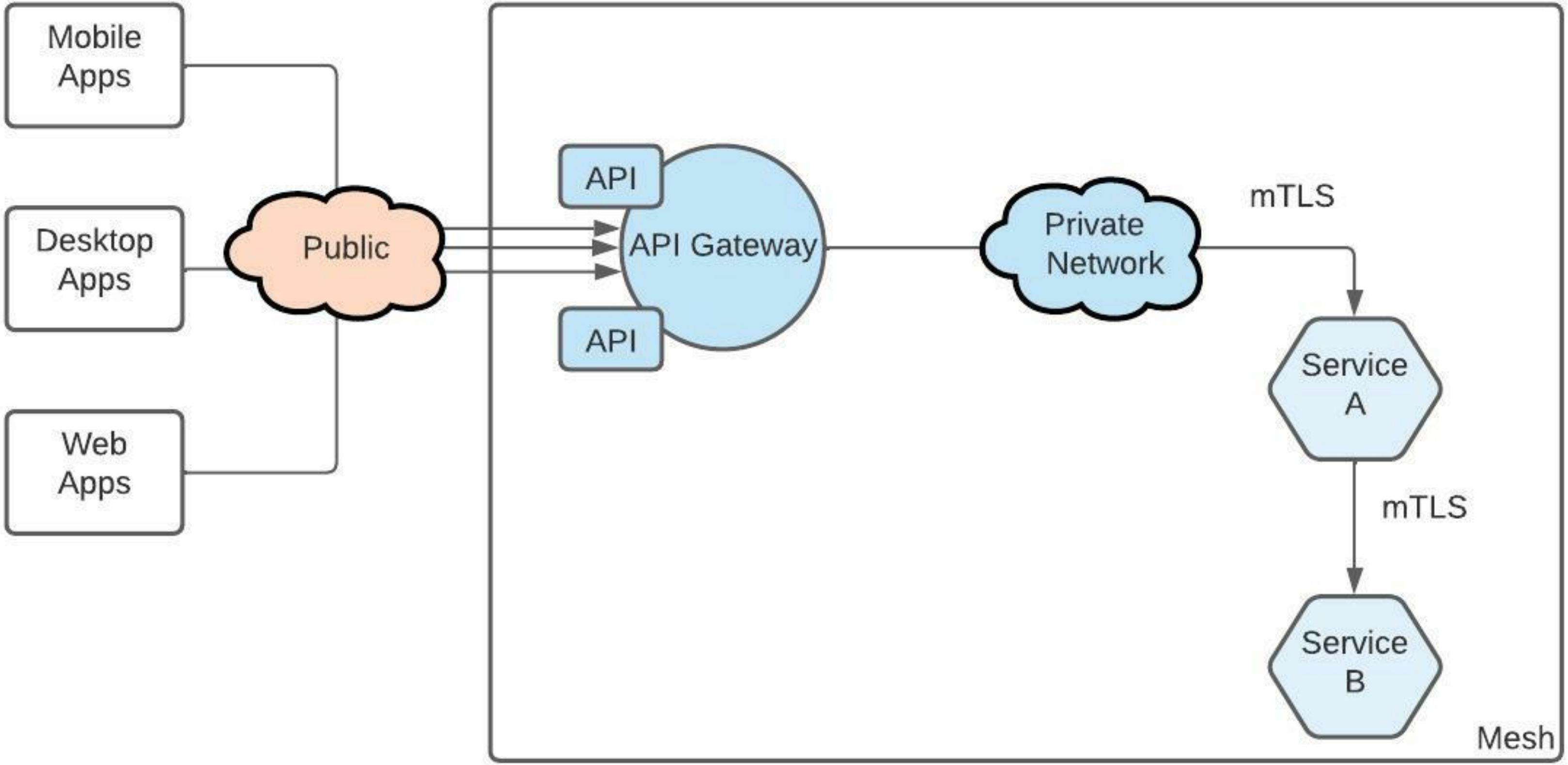


API Gateway and Mesh

Moving API Gateway on to Service Mesh would result in a Complete Zero Trust system

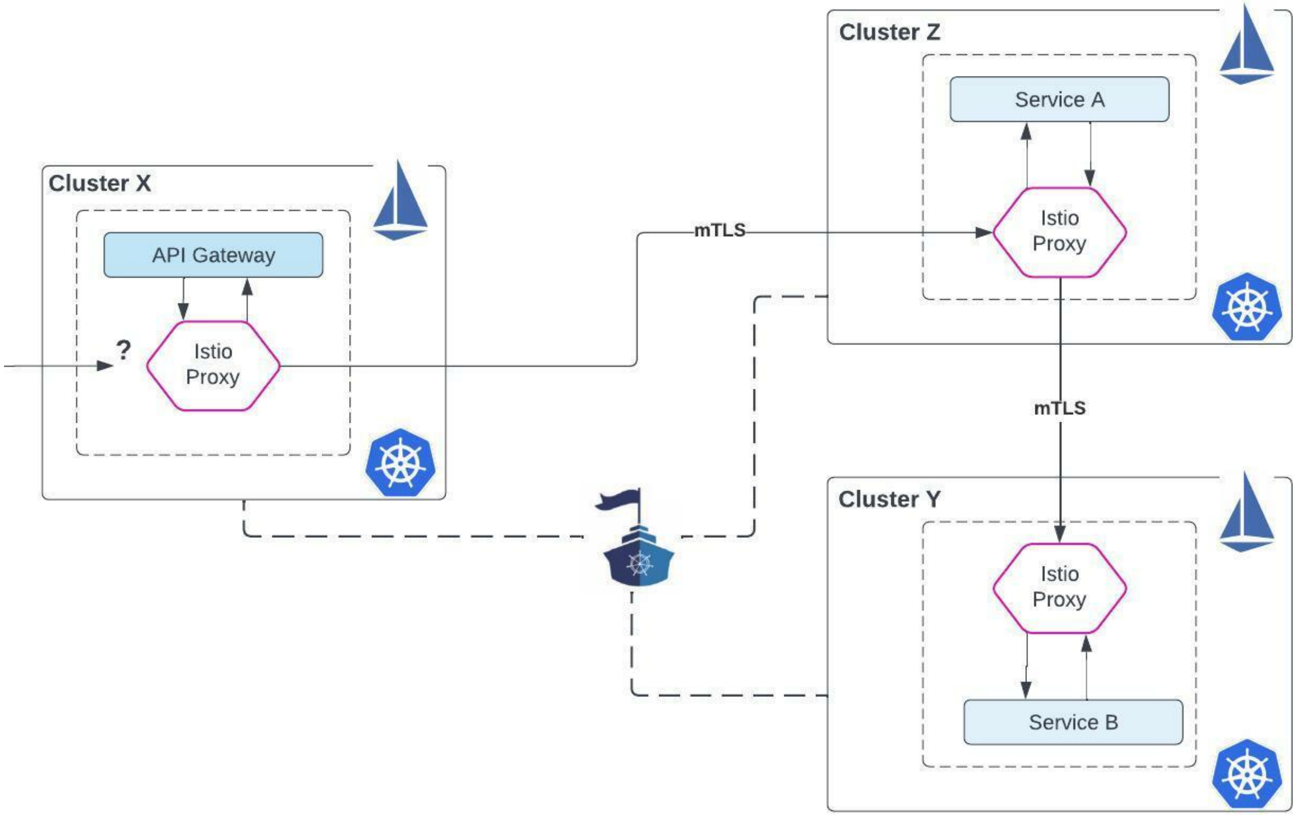


API Gateway on Mesh

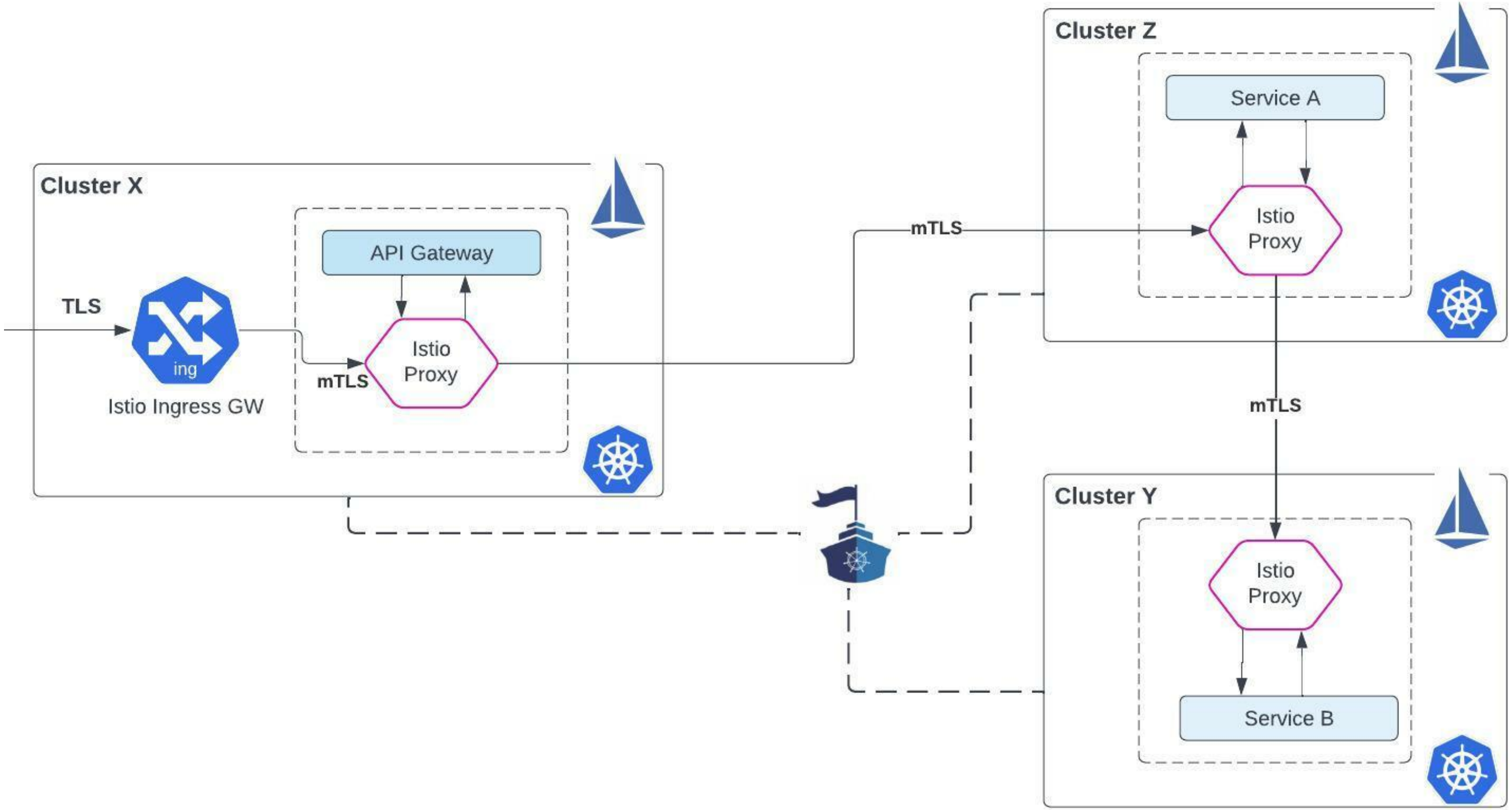


intuit

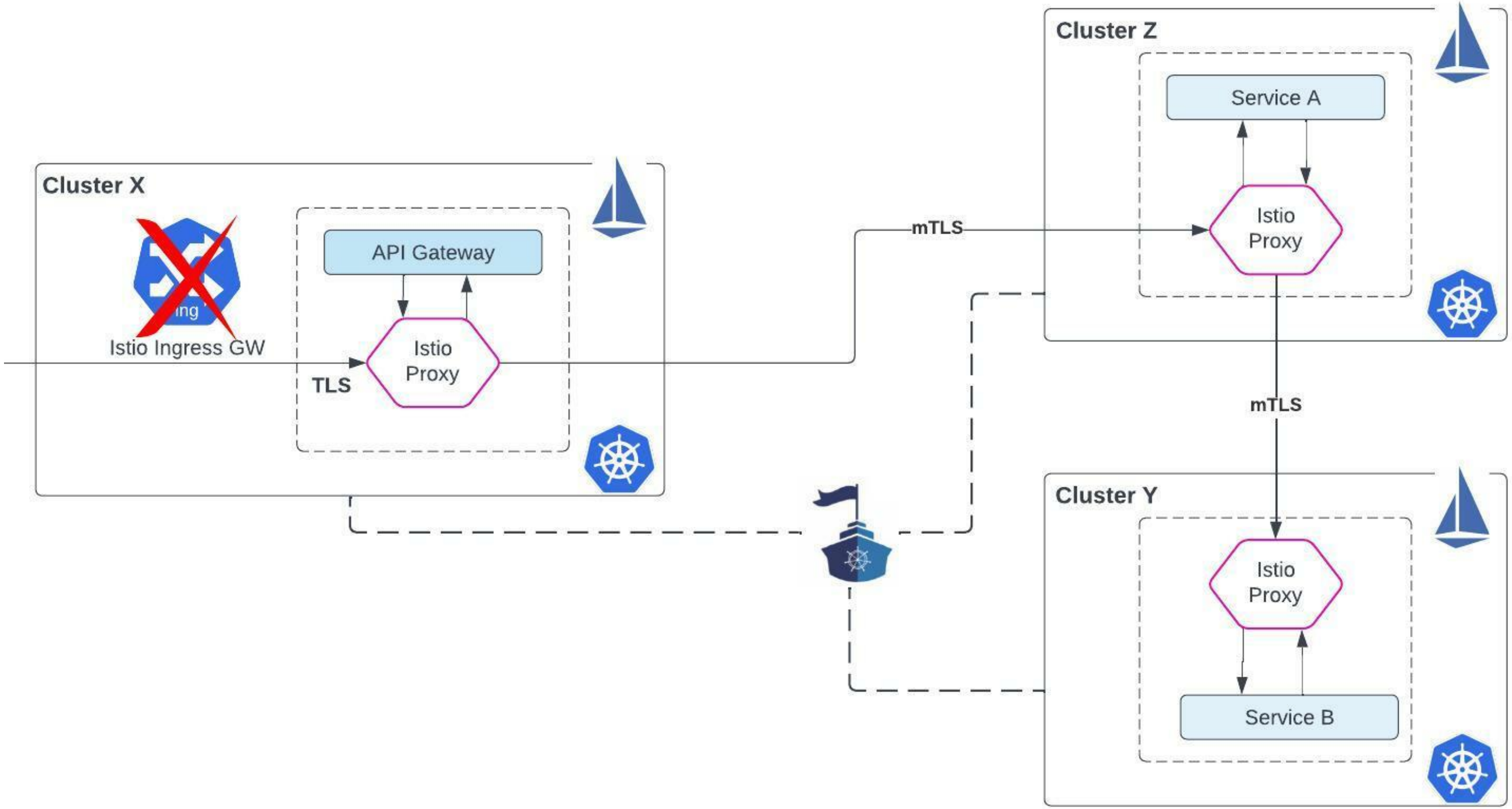
API Gateway on Mesh



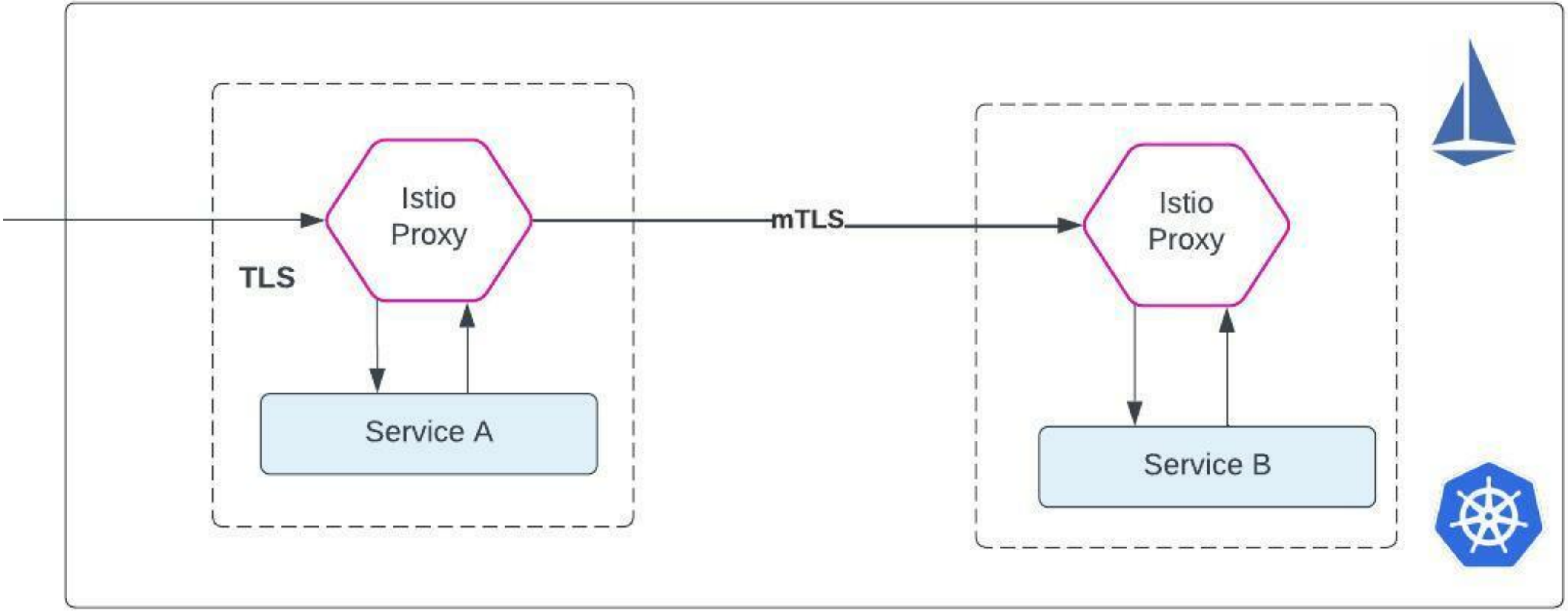
API Gateway on Mesh - TLS Termination?



API Gateway on Mesh - TLS Termination?



TLS Termination on Sidecar



TLS/mTLS on Sidecar

Service

```
apiVersion: v1
kind: Service
metadata:
  name: httpbin
  labels:
    app: httpbin
    service: httpbin
spec:
 ports:
 - name: http
   port: 8000
   targetPort: 80
selector:
   app: httpbin
```

Sidecar

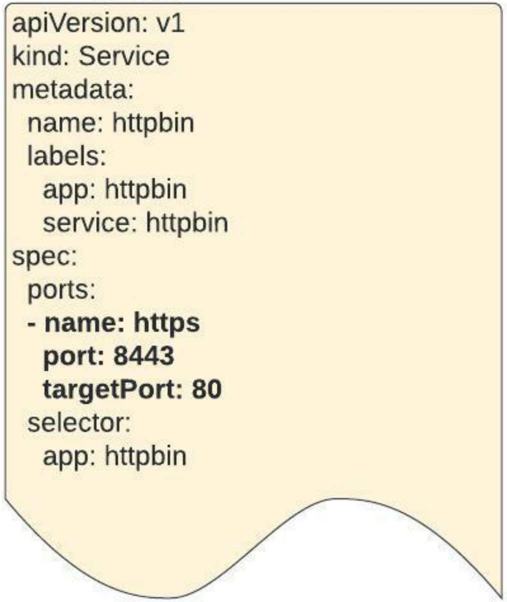
```
apiVersion:
networking.istio.io/v1alpha3
kind: Sidecar
metadata:
 ...
spec:
  workloadSelector:
     ...
  ingress:
    - port:
        number: 80
        ...
  egress:
     - hosts:
       - "./*"
       - "istio-system/*"
```

PeerAuthentication

```
apiVersion: security.istio.io/v1beta1
kind: PeerAuthentication
metadata:
  name: httpbin-pa
  namespace: app1
spec:
  selector:
    matchLabels:
      app: httpbin
  mtls:
    mode: STRICT
```

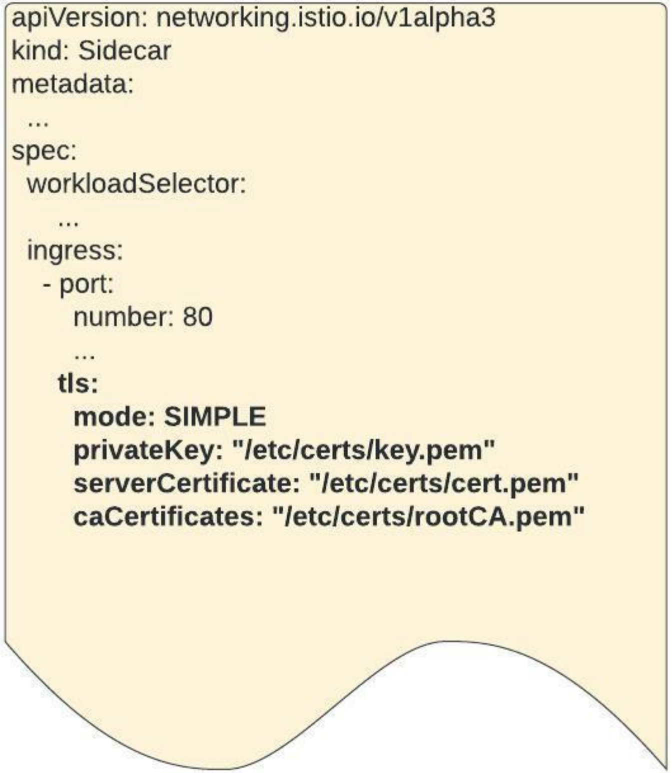
TLS/mTLS on Sidecar

Service



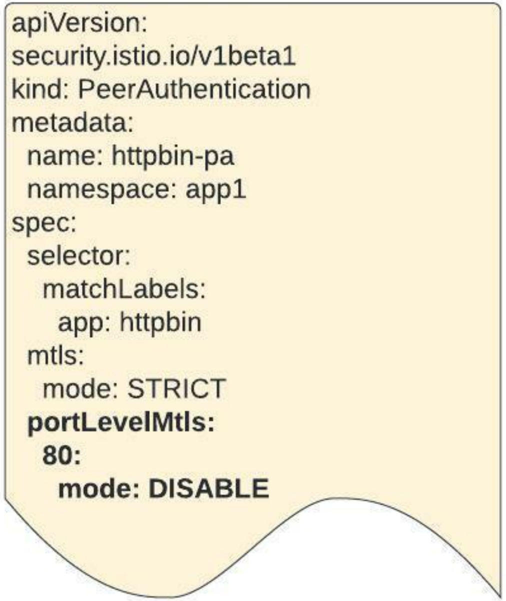
```
apiVersion: v1
kind: Service
metadata:
  name: httpbin
  labels:
    app: httpbin
    service: httpbin
spec:
  ports:
  - name: https
    port: 8443
    targetPort: 80
  selector:
    app: httpbin
```

Sidecar



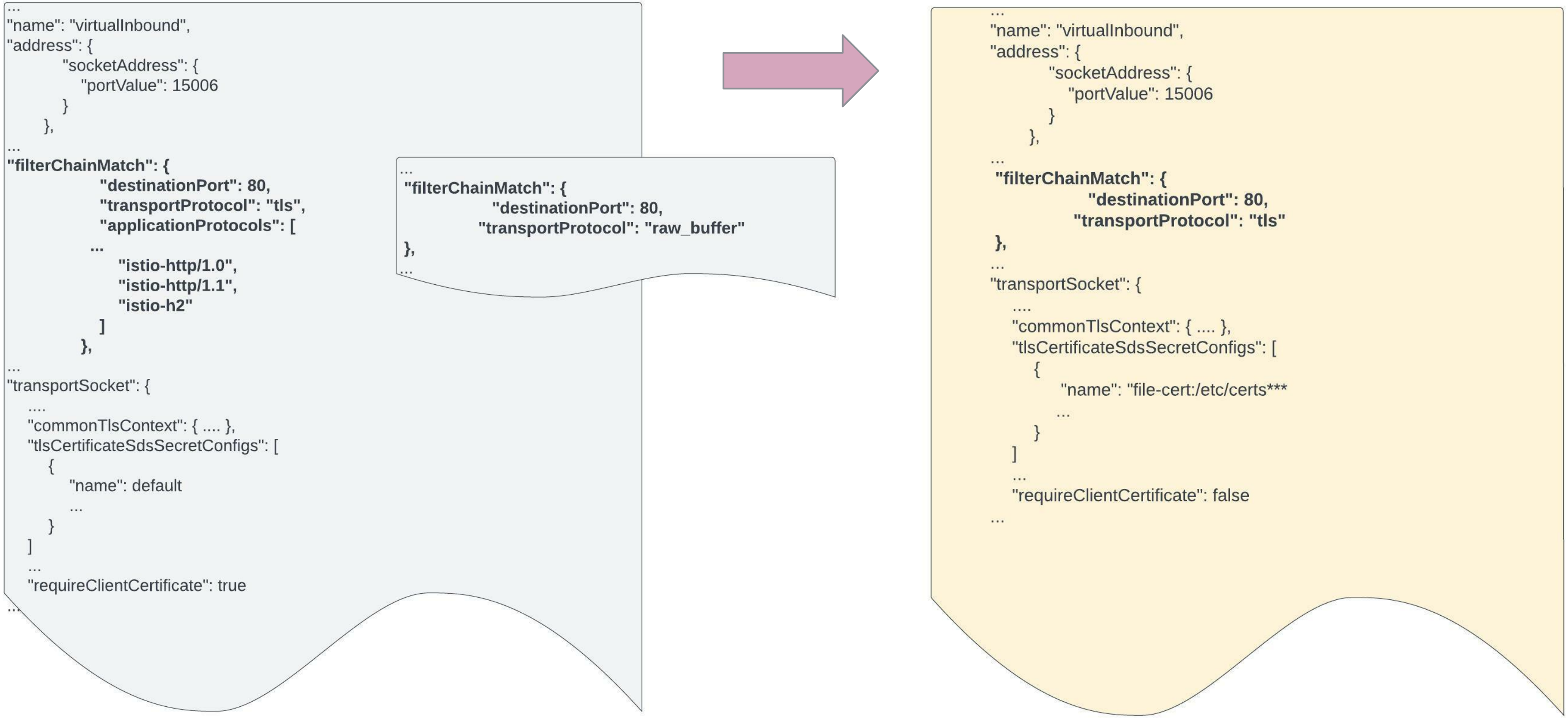
```
apiVersion: networking.istio.io/v1alpha3
kind: Sidecar
metadata:
  ...
spec:
  workloadSelector:
      ...
  ingress:
    - port:
        number: 80
        ...
      tls:
        mode: SIMPLE
        privateKey: "/etc/certs/key.pem"
        serverCertificate: "/etc/certs/cert.pem"
        caCertificates: "/etc/certs/rootCA.pem"
```

PeerAuthentication



```
apiVersion:
security.istio.io/v1beta1
kind: PeerAuthentication
metadata:
  name: httpbin-pa
  namespace: app1
spec:
  selector:
    matchLabels:
      app: httpbin
  mtls:
    mode: STRICT
  portLevelMtls:
    80:
      mode: DISABLE
```

TLS/mTLS on Sidecar



Before

```
...
"name": "virtualInbound",
"address": {
          "socketAddress": {
             "portValue": 15006
          }
      },
...
"filterChainMatch": {
                "destinationPort": 80,
                "transportProtocol": "tls",
                "applicationProtocols": [
              ...
                   "istio-http/1.0",
                   "istio-http/1.1",
                   "istio-h2"
                ]
            },
...
"transportSocket": {
    ....
    "commonTlsContext": { .... },
    "tlsCertificateSdsSecretConfigs": [
        {
           "name": default
           ...
        }
    ]
    ...
    "requireClientCertificate": true
...
```

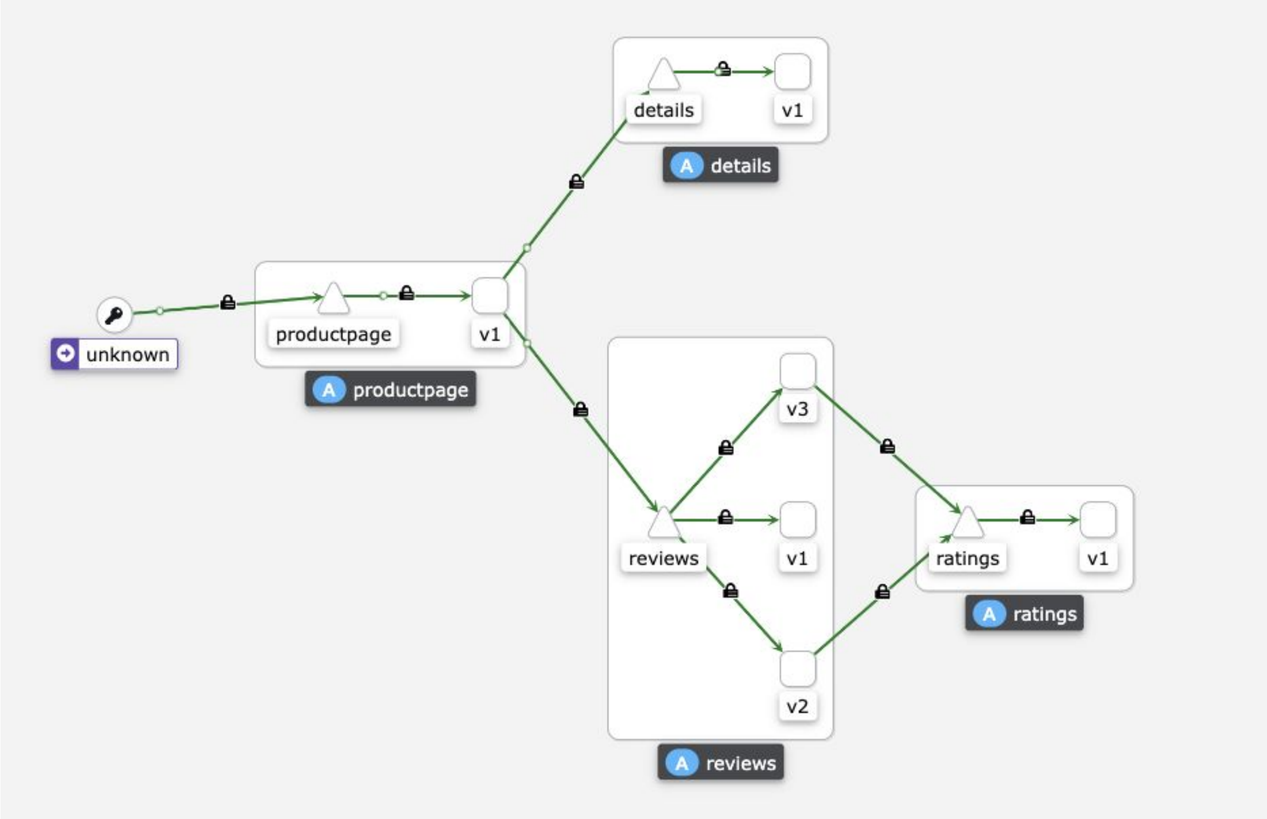
```
...
"filterChainMatch": {
              "destinationPort": 80,
            "transportProtocol": "raw_buffer"
},
...
```

After

```
...
"name": "virtualInbound",
"address": {
          "socketAddress": {
             "portValue": 15006
          }
      },
...
 "filterChainMatch": {
               "destinationPort": 80,
             "transportProtocol": "tls"
 },
...
"transportSocket": {
    ....
    "commonTlsContext": { .... },
    "tlsCertificateSdsSecretConfigs": [
        {
           "name": "file-cert:/etc/certs***
           ...
        }
    ]
    ...
    "requireClientCertificate": false
...
```

Demo

TLS/mTLS on Sidecar - Demo!



TLS/mTLS on Sidecar - What's next?

Github Issue for better UX

Resources/Links

Istio RFC - Sidecar TLS Termination

Implementation - PR

Related Talk at IstioCon 2022 - API Runtime Orchestration with Istio and OpenAPI 3

Admiral - An Istio Ecosystem Project for automatic multi-cluster configuration

Thank You