

# Understanding The Data Plane

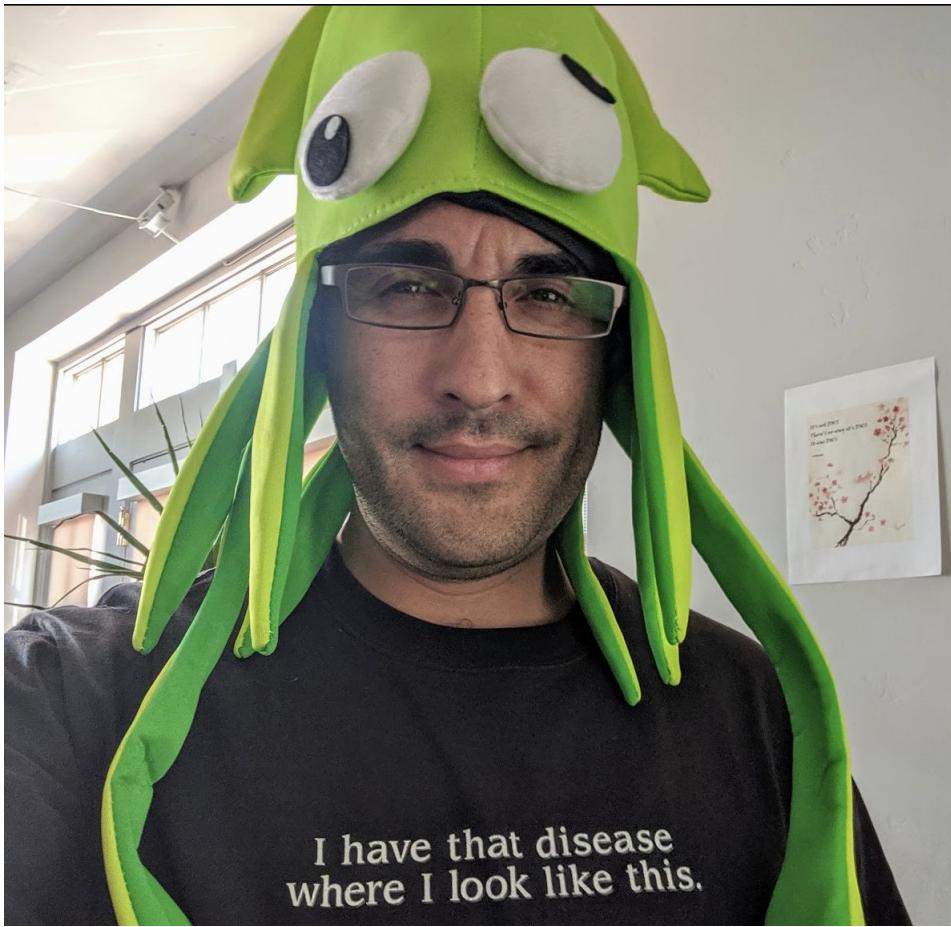
## What Envoy Hears When Istio Speaks



you are here



istio nirvana



Rob Salmond

SRE Here

Istio in Prod for >2yrs

 @phro

# Map of These Territories

Istiod

WTF is an Envoy

Envoy Operation

Envoy  
Configuration

A tall, dark, vertical pillar stands prominently in a red, rocky landscape, resembling a desert or canyon floor. The pillar is positioned centrally and appears to be made of a dark material like metal or stone. The background consists of reddish-brown rock formations with various textures and shadows.

istiod

An Envoy “management server”

# You had ~~one~~ three jobs!

## Galley

Understand  
Kubernetes

## Pilot

Program  
Sidecars

## Citadel

Autograph  
Certificates

# You had ~~one~~ three many jobs!

## Galley

Understand  
Kubernetes

## Pilot

Program  
Sidecars

## Citadel

Autograph  
Certificates

sidecar injection  
webhook handler!

cinnamon flavor  
crystals!

*CRD validation!*

# Several jobs are typing ...

## Galley

Understand  
Kubernetes

## Pilot

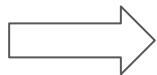
Program  
Sidecars

## Citadel



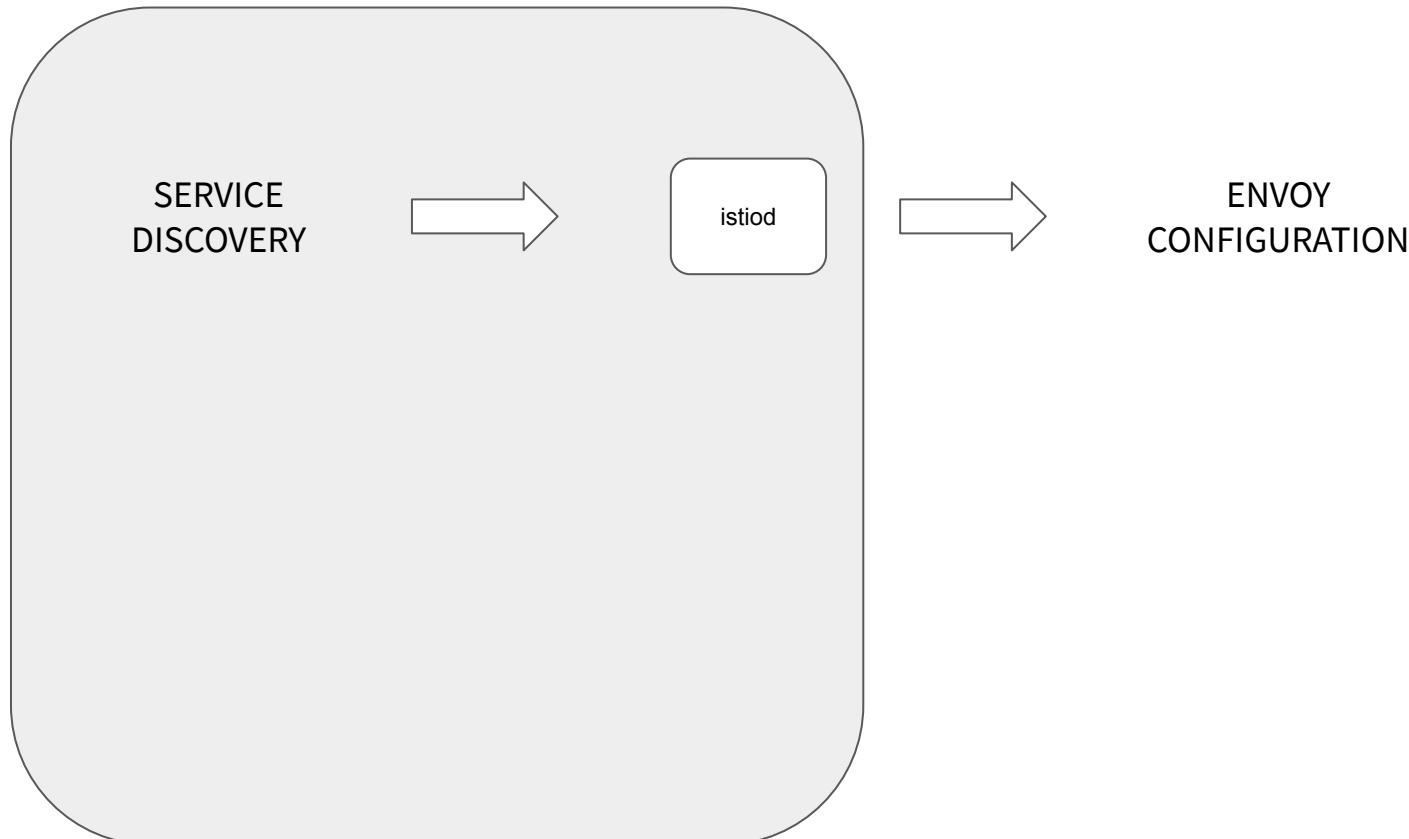
# istiod

SERVICE  
DISCOVERY

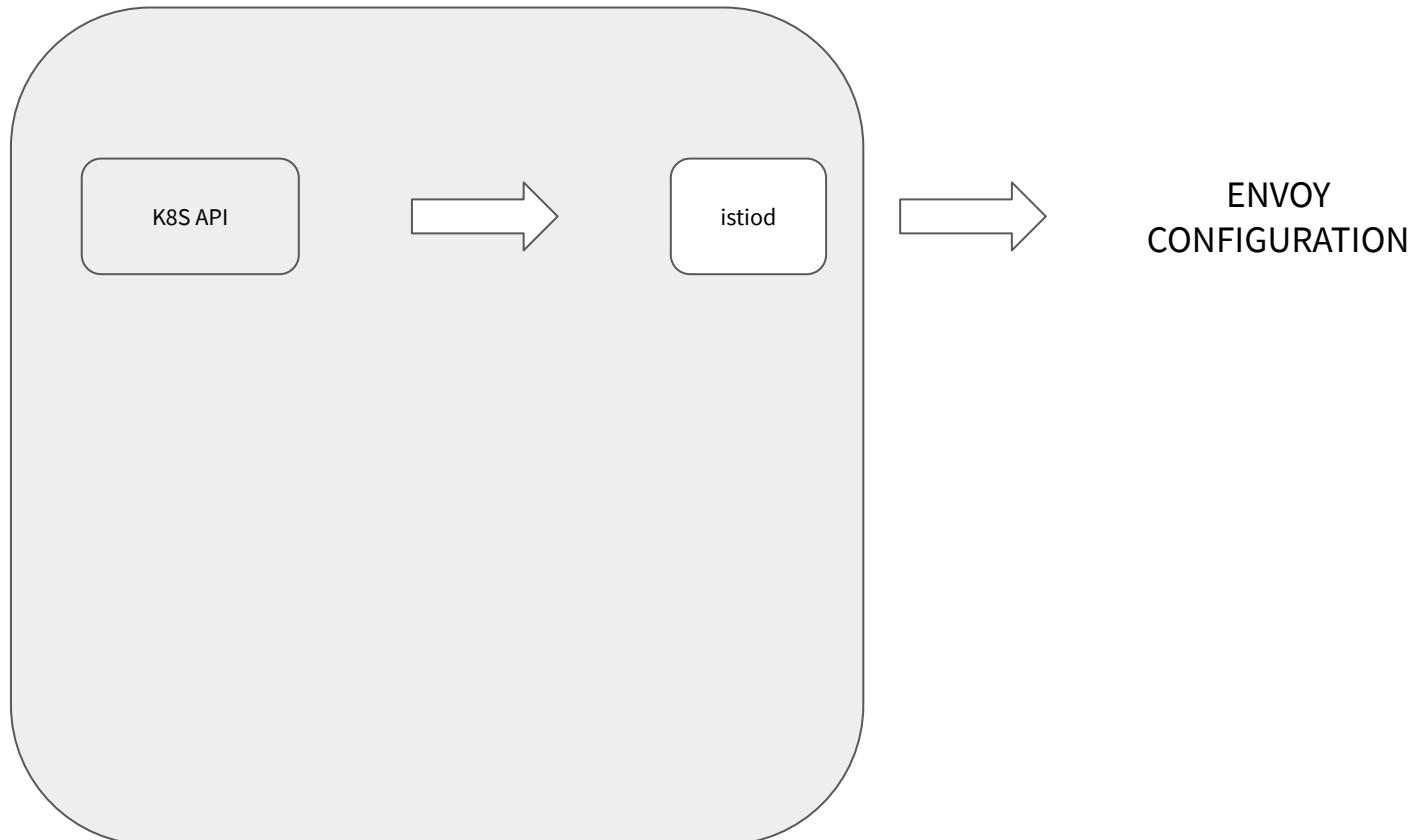


ENVOY  
CONFIGURATION

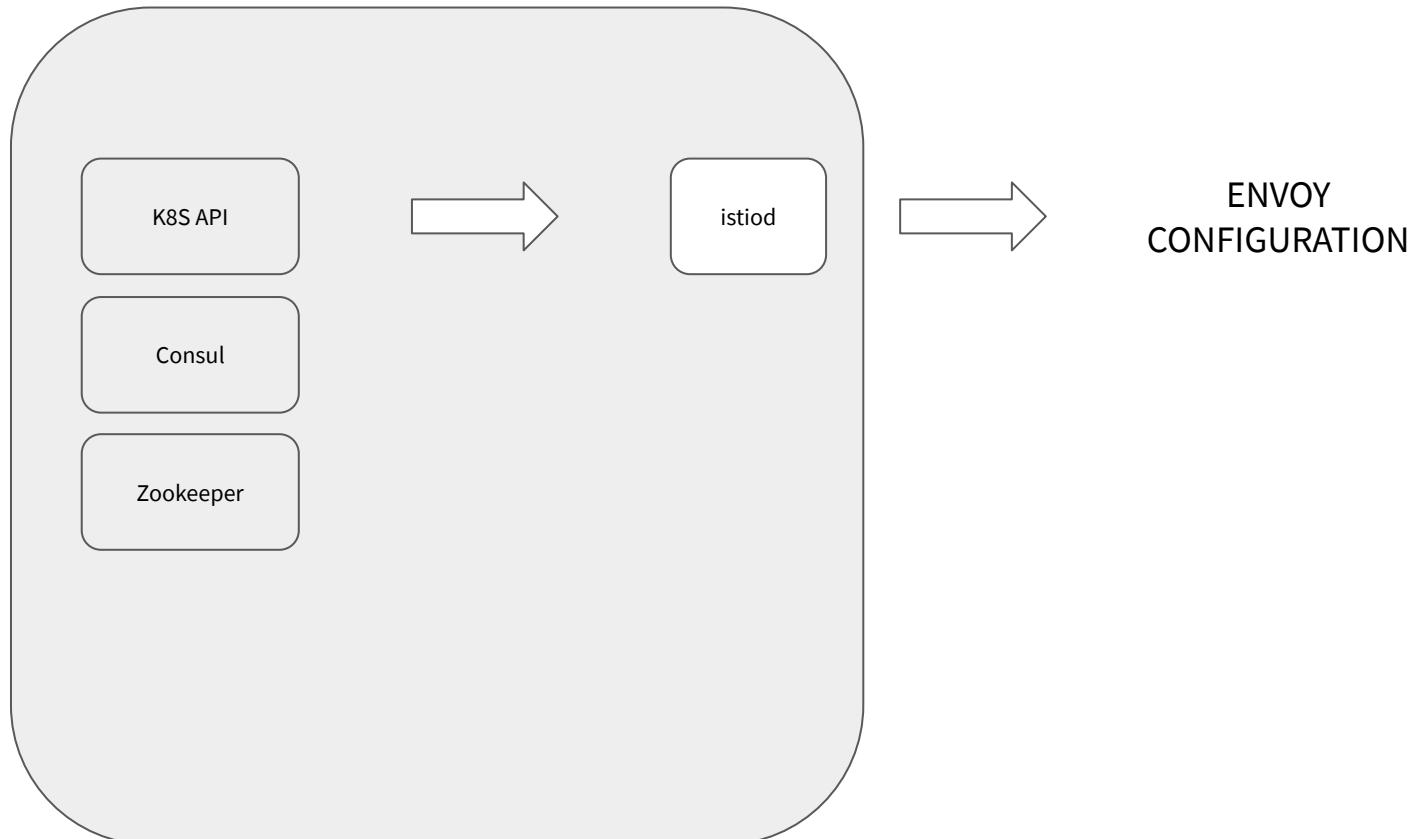
# istiod - gallery



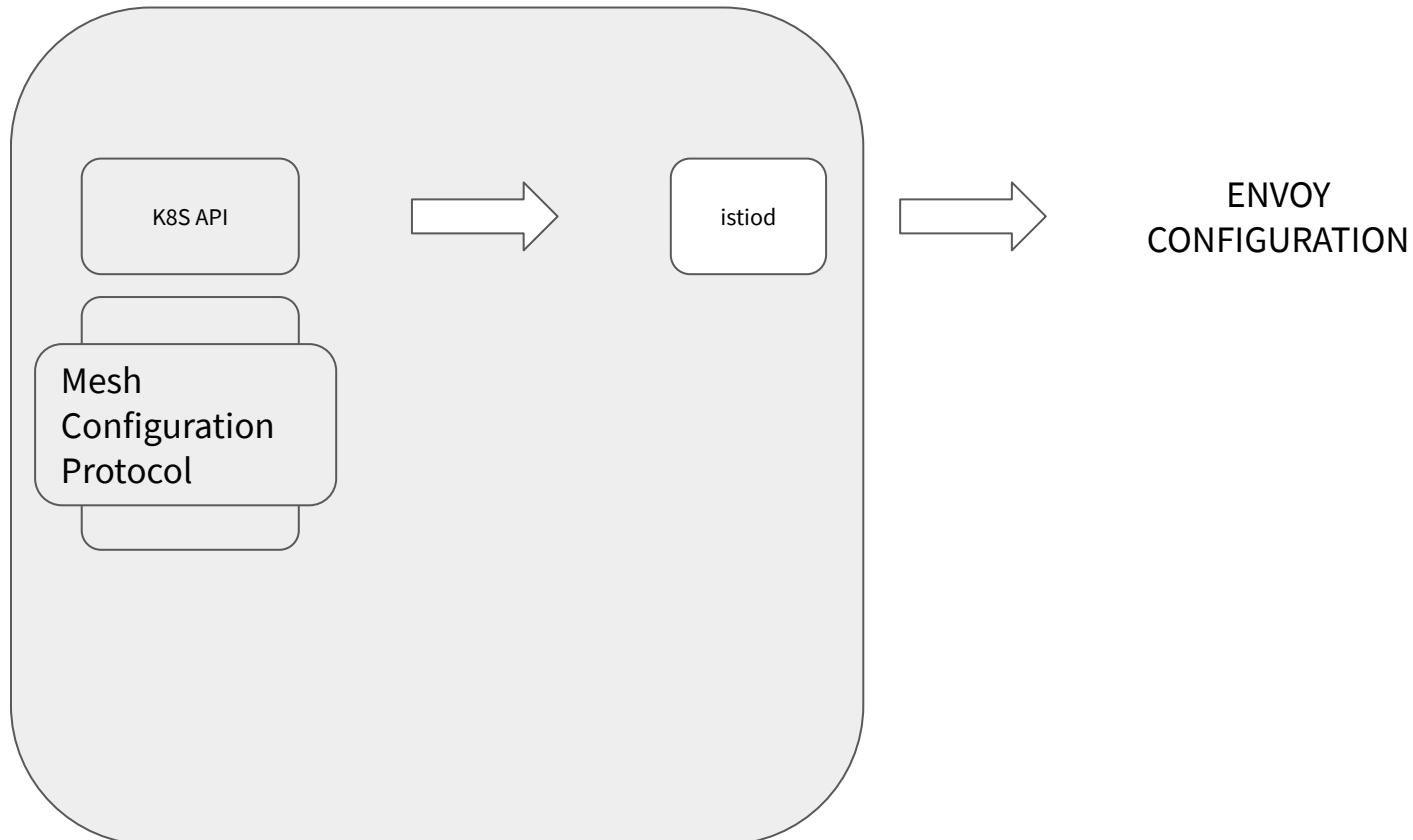
# istiod - gallery



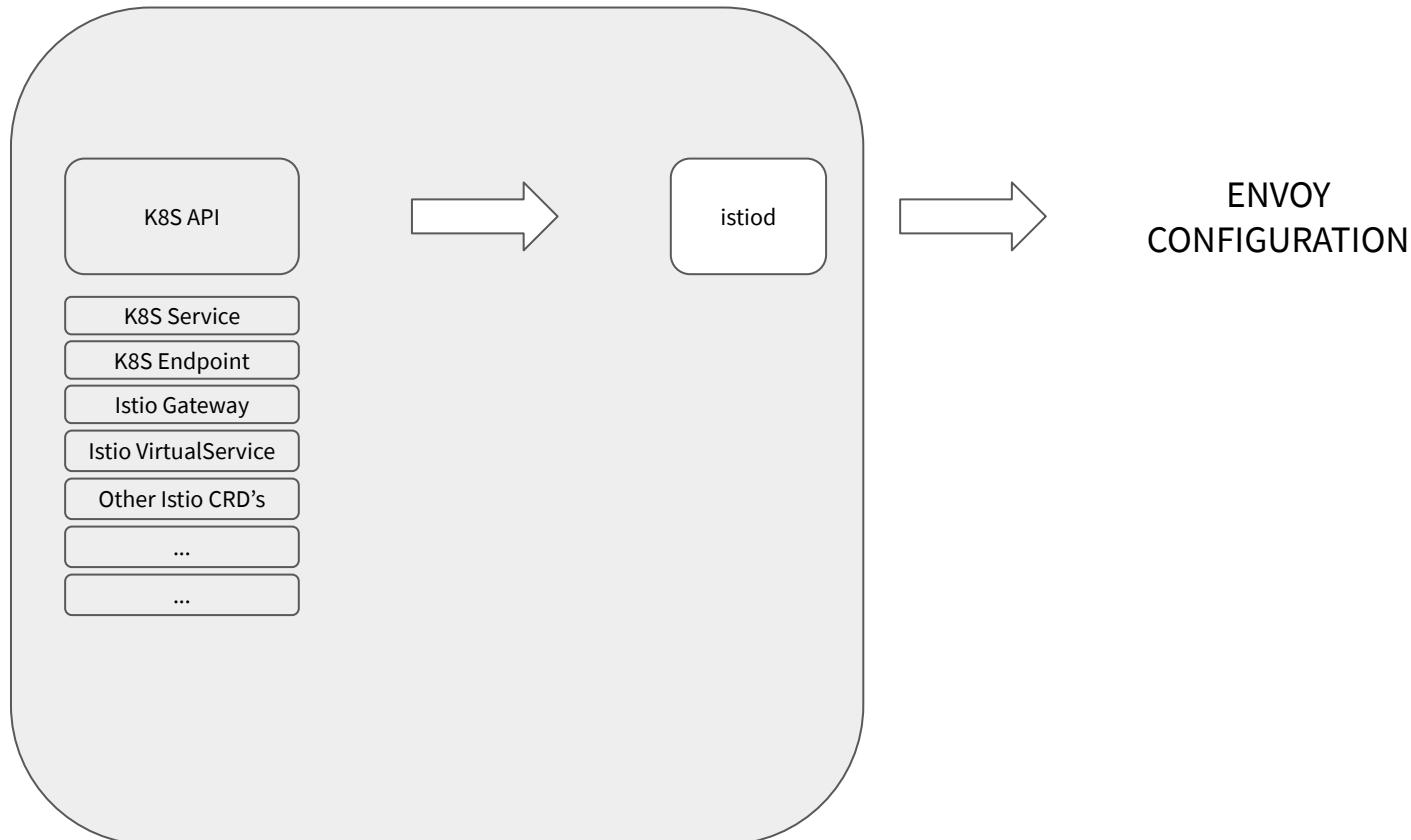
# istiod - gallery



# istiod - gallery



# istiod - gallery



## istiod - gallery

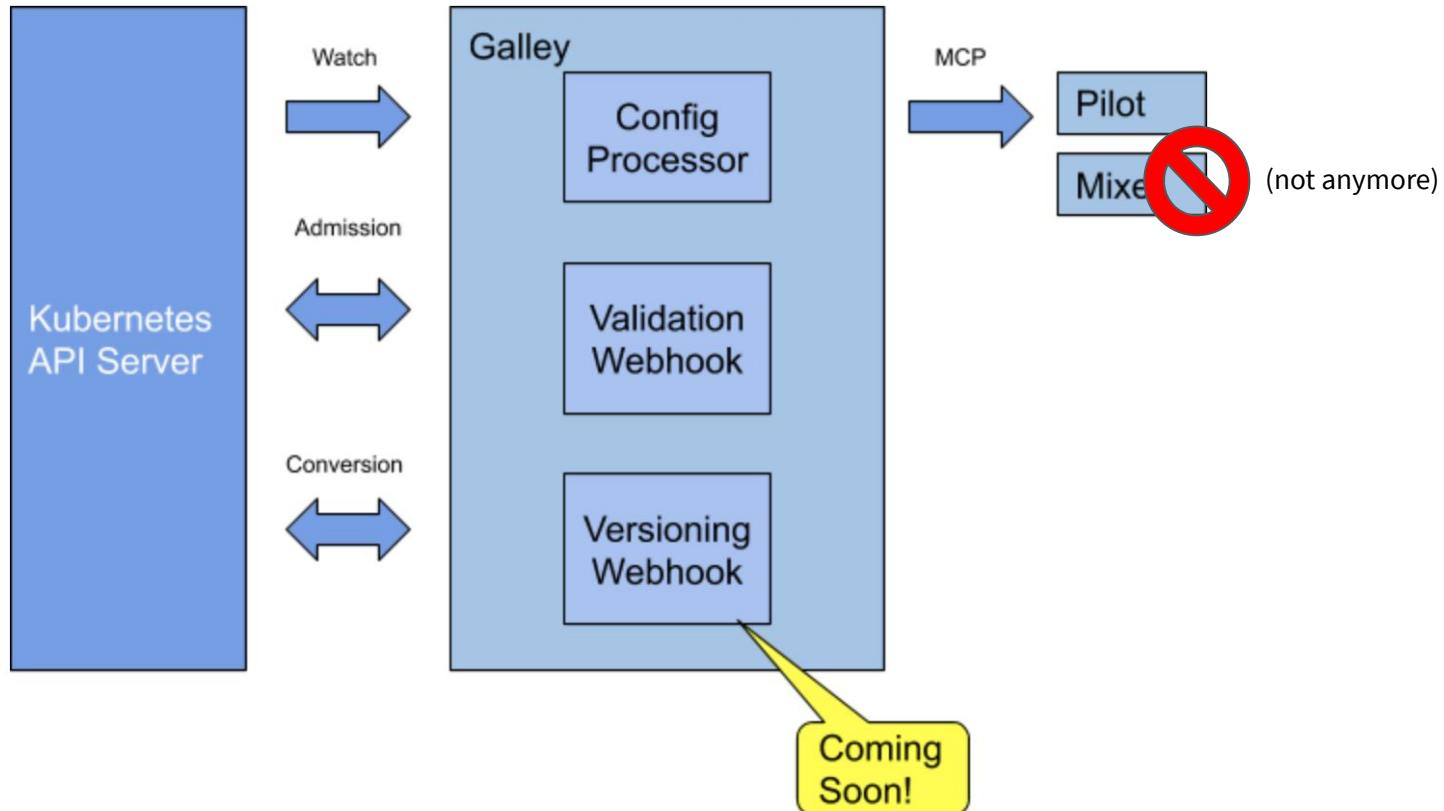
```
rob@ayyyyylmao:~ kubectl port-forward po/istiod-58f84ffddc-r8nqf 8080
Forwarding from 127.0.0.1:8080 -> 8080
Forwarding from [::1]:8080 -> 8080
```

# istiod - gallery

← → ⌂ ⓘ localhost:8080/debug/registryz

```
[
  {
    "Attributes": {
      "ServiceRegistry": "Kubernetes",
      "Name": "api",
      "Namespace": "master",
      "UID": "istio://master/services/api",
      "ExportTo": null,
      "ClusterExternalAddresses": null,
      "ClusterExternalPorts": {
        "Kubernetes": {
          "8000": 30731
        }
      }
    },
    "ports": [
      {
        "name": "grpc-web-port",
        "port": 8000,
        "protocol": "GRPC-Web"
      }
    ],
    "creationTime": "2021-01-28T20:46:33Z",
    "hostname": "api.master.svc.cluster.local",
    "address": "10.56.3.75",
    "Mutex": {},
    "cluster-vips": {
      "Kubernetes": "10.56.3.75"
    },
    "Resolution": 0,
    "MeshExternal": false
  }
]
```

# istiod - galley



# istiod - galley - validation

```
apiVersion: admissionregistration.k8s.io/v1
kind: ValidatingWebhookConfiguration
metadata:
  name: istiod-istio-system
webhooks:
- admissionReviewVersions:
  - v1beta1
  clientConfig:
    service:
      name: istiod
      namespace: istio-system
      path: /validate
      port: 443
    failurePolicy: Fail
    matchPolicy: Exact
    name: validation.istio.io
    namespaceSelector: {}
    objectSelector: {}
    rules:
    - apiGroups:
      - config.istio.io
      - rbac.istio.io
      - security.istio.io
      - authentication.istio.io
      - networking.istio.io
    apiVersions:
    - '*'
    operations:
    - CREATE
    - UPDATE
    resources:
    - '*'
    scope: '*'
    sideEffects: None
    timeoutSeconds: 30
```

# istiod - galley - sidecar injection

```
apiVersion: admissionregistration.k8s.io/v1
kind: MutatingWebhookConfiguration
metadata:
  name: istio-sidecar-injector
webhooks:
- admissionReviewVersions:
  - v1beta1
  clientConfig:
    service:
      name: istiod
      namespace: istio-system
      path: /inject
      port: 443
    failurePolicy: Fail
    matchPolicy: Exact
    name: sidecar-injector.istio.io
    namespaceSelector:
      matchLabels:
        istio-injection: enabled
    objectSelector: {}
    reinvocationPolicy: Never
    rules:
- apiGroups:
  - ""
    apiVersions:
    - v1
    operations:
    - CREATE
    resources:
    - pods
    scope: "*"
  sideEffects: None
  timeoutSeconds: 30
```

# sidecar injection sidebar

```
$ istioctl kube-inject -f mypod.yaml -o sidecarpod.yaml
```

# You had ~~one~~ three jobs!

Galley



Understand  
Kubernetes

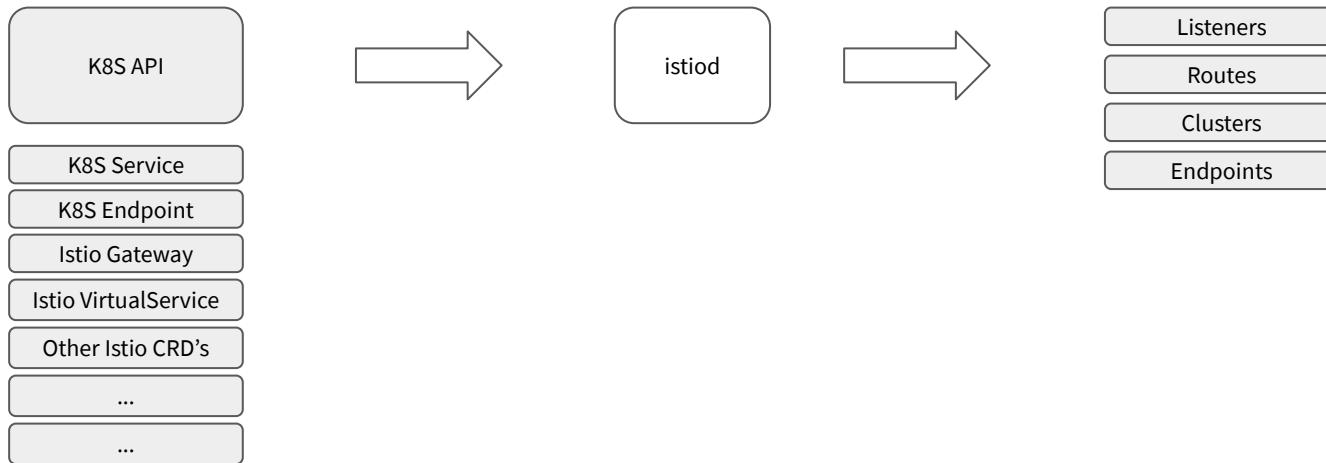
Pilot

Program  
Sidecars

Citadel



# istiod - pilot



# istiod - pilot

## Mapping Resources to Envoy Configuration

Resource Type	Envoy Configuration	Notes
Kubernetes Services	Listeners Routes Clusters	New listeners if port/protocol combo is unique Add virtual hosts for existing routes One cluster per Service/Port/Subset
Kubernetes Endpoints	Endpoints	
Istio Gateway	Listeners	Apply to Ingress/Egress Gateways
Istio VirtualService	Listeners Routes	Client side proxies TLS/TCP affect listeners HTTP match blocks affect routes
Istio DestinationRule	Clusters Endpoints	Client side proxies Connection/HTTP/TLS settings
Istio ServiceEntry	Clusters Endpoints	Client side proxies
Istio PeerAuthentication	Listeners Clusters	Server side proxies
Istio RequestAuthentication	Listeners	Server side proxies
Istio Authorization Policies	Listeners	Server side proxies
Istio EnvoyFilter	All	Break glass API to directly manipulate Envoy
Istio Sidecar	All	Client or server side proxies Sidecar scope sets config visibility

# You had ~~one~~ three jobs!

Galley



Understand  
Kubernetes

Pilot ✓

Program  
Sidecars

Citadel



# WTF Is An Envoy?

Isn't that the dude who pissed off King Leonidas and got kicked down a well?



# envoy - was ist das?



# envoy

1.17.0-dev-3736b5

Search docs

About the documentation

Introduction

What is Envoy

envoyproxy.io/docs/envoy/latest/intro/what\_is\_envoy

☆ ⚙️ ⚡ 📁 🌐 🌐 🌐 🌐 🌐 🌐

View page source

# envoy - was ist das?

## Envoy refresher

- **Out of process architecture:** Let's do a lot of really hard stuff in one place and allow application developers to focus on business logic.
- **Modern C++11 code base:** Fast and productive.
- **L3/L4 filter architecture:** A byte proxy at its core. Can be used for things other than HTTP (e.g., MongoDB, redis, stunnel replacement, TCP rate limiter, etc.).
- **HTTP L7 filter architecture:** Make it easy to plug in different functionality.
- **HTTP/2 first!** (Including **gRPC** and a nifty gRPC HTTP/1.1 bridge).
- **Service discovery and active/passive health checking.**
- **Advanced load balancing:** Retry, timeouts, circuit breaking, rate limiting, shadowing, outlier detection, etc.
- Best in class **observability**: stats, logging, and tracing.
- **Edge proxy:** routing and TLS.

# envoy - was ist das?

[github.com/istio/proxy](https://github.com/istio/proxy)

Search or jump to... / Pulls Issues Marketplace Explore

Watch 98 Star 502 Fork 321

Code Pull requests 9 Actions Security Insights

master Go to file Add file Code

**istio-testing** Automator: update common-files@master in i... 6 days ago 1,612

- .github Update PULL\_REQUEST\_TEMPLATE.md (#3036) 2 months ago
- bazel Wrap Wasm related library import into a rule (#...) 11 days ago
- common-protos/googl... add gen doc for extension protos (#2803) 7 months ago
- common Automator: update common-files@master in ist... 6 days ago
- extensions Update envoy sha (#3111) 8 days ago
- prow Make test framework usable for external repo (...) 2 months ago
- scripts Add Rbac Access Denied Policy Info in Access l... 14 days ago

About

The Istio proxy components.

proxy discovery monitoring sidecar lyft-envoy

Readme Apache-2.0 License

Releases 205

1.0.2 Latest on Sep 10, 2018

## envoy - was ist das?

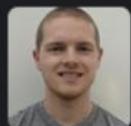


**Fraser** Today at 1:30 AM

Whats the plan for the istio fork of envoy, once envoy-wasm is merged into upstream envoy will istio fork the main envoy? or will it use the upstream envoy?

2 replies

---



**John Howard** 1 hour ago

Still fork main envoy until we have no more custom filters



**John Howard** 1 hour ago

Which will happen eventually once they move to wasm

# envoy - terminology

Upstream

Downstream

## envoy - terminology

Where Envoy  
connections  
come from

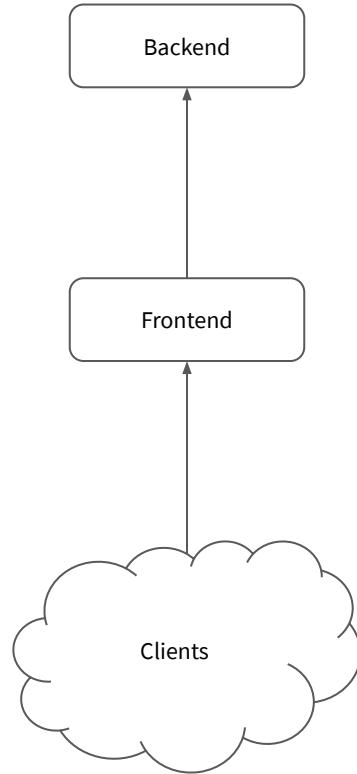
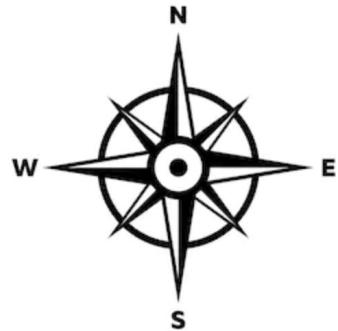
Downstream

## envoy - terminology

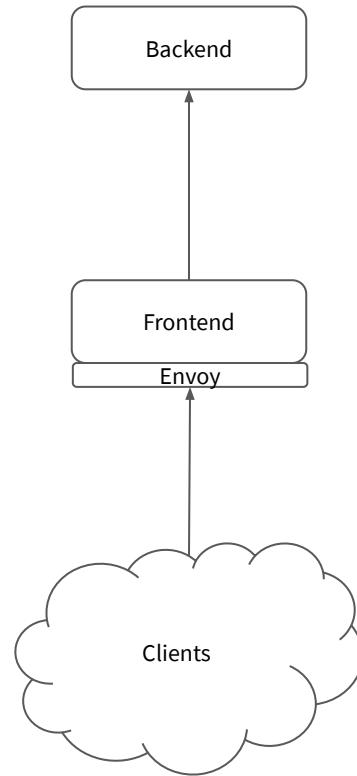
Upstream

Where Envoy  
connections go  
to

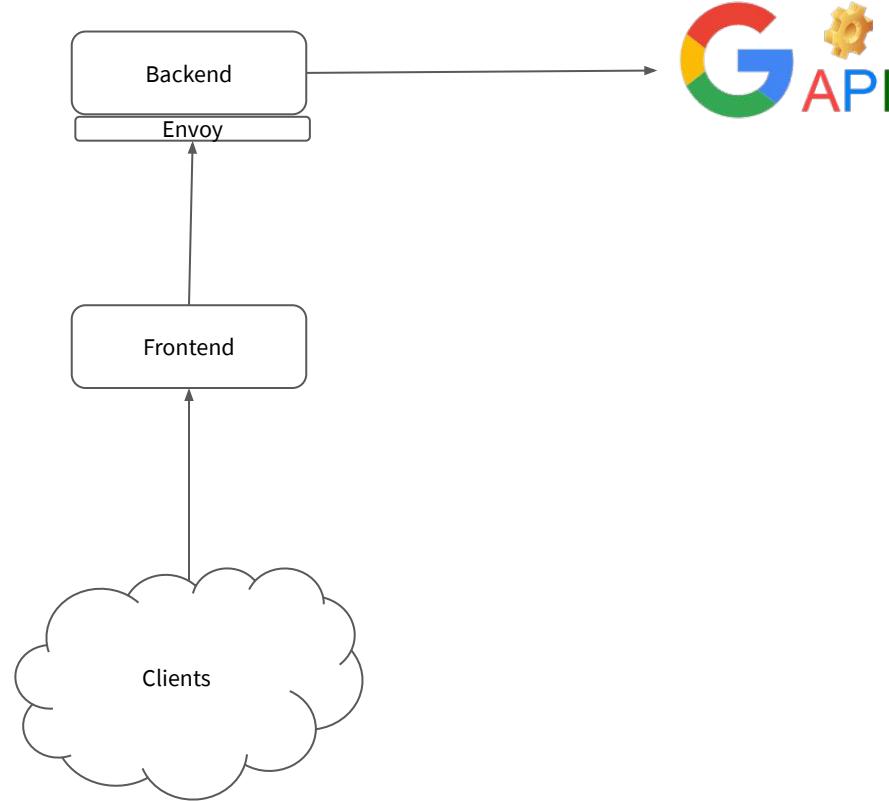
# “North-South” Traffic



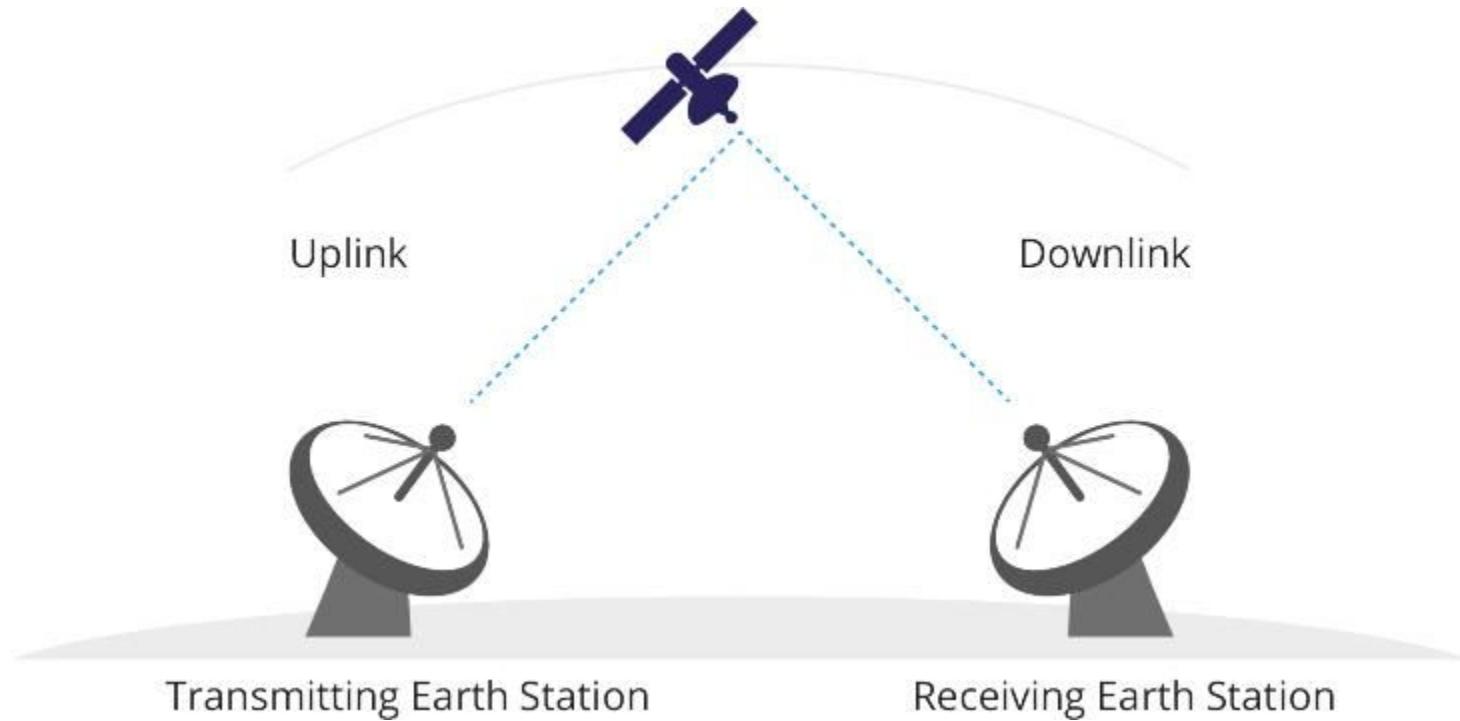
# envoy - upstream and downstream



# envoy - upstream and downstream



## envoy - upstream and downstream



# envoy - terminology

Clusters  
&  
Endpoints

Listeners  
&  
Routes

## envoy - terminology

Clusters  
&  
Endpoints



Hostnames  
&  
IP Addresses

# envoy - terminology

## Clusters & Endpoints

outbound|443||kubernetes.default.svc.cluster.local

10.4.0.10\_53

xds-grpc

## envoy - terminology

What to accept  
How to process it  
&  
Where to send it

Listeners  
&  
Routes

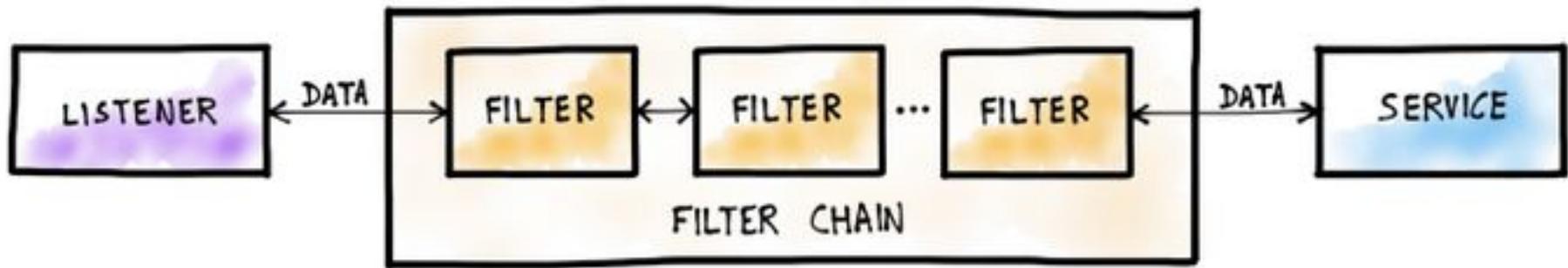


## Envoy: Operation

\*professional SRE

Sidecars and lions and bears!

# envoy - operation



## envoy - operation

```
from wsgiref.simple_server import make_server
from cgi import parse_qs

def application (environ, start_response):

    query = parse_qs(environ['QUERY_STRING'])
    foo_val = query.get('foo')

    print "lol, this guy wants his foo like {}".format(foo_val)

    start_response('200 OK', [])
    return ['cool query bro']

httpd = make_server ('localhost', 8051, application)
httpd.handle_request()
```

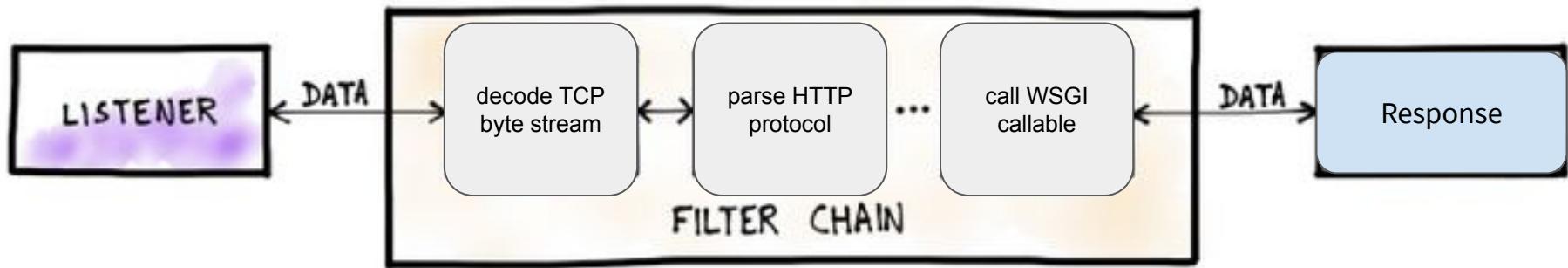
## envoy - operation

```
$ echo -e "GET /?foo=bar HTTP/1.1\r\n" | nc localhost 8051
HTTP/1.0 200 OK
Date: Sat, 05 Dec 2020 22:28:28 GMT
Server: WSGIServer/0.1 Python/2.7.18rc1
Content-Length: 14
```

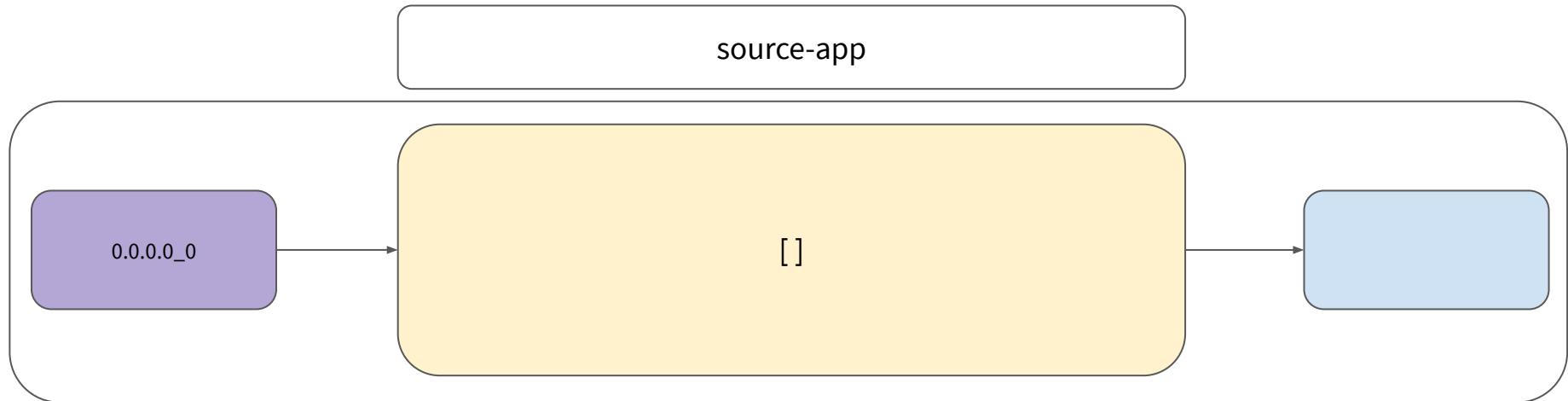
cool query bro

```
$ python web.py
lol, this guy wants his foo like ['bar']
127.0.0.1 - - [05/Dec/2020 15:28:28] "GET /?foo=bar HTTP/1.1" 200 14
```

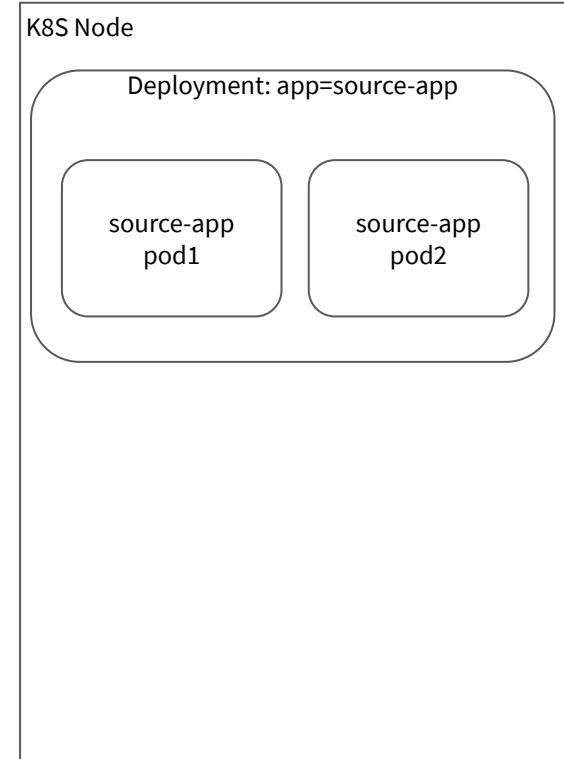
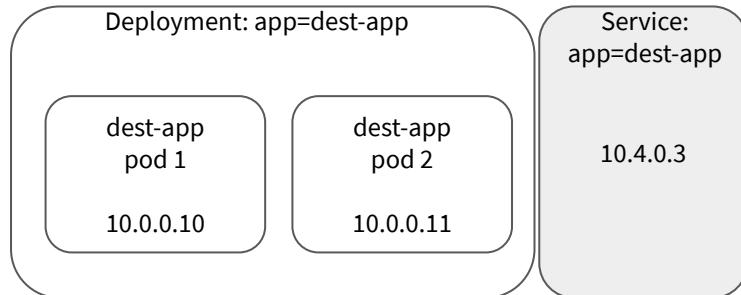
# envoy - operation



# envoy - operation



# k8s networking - classic

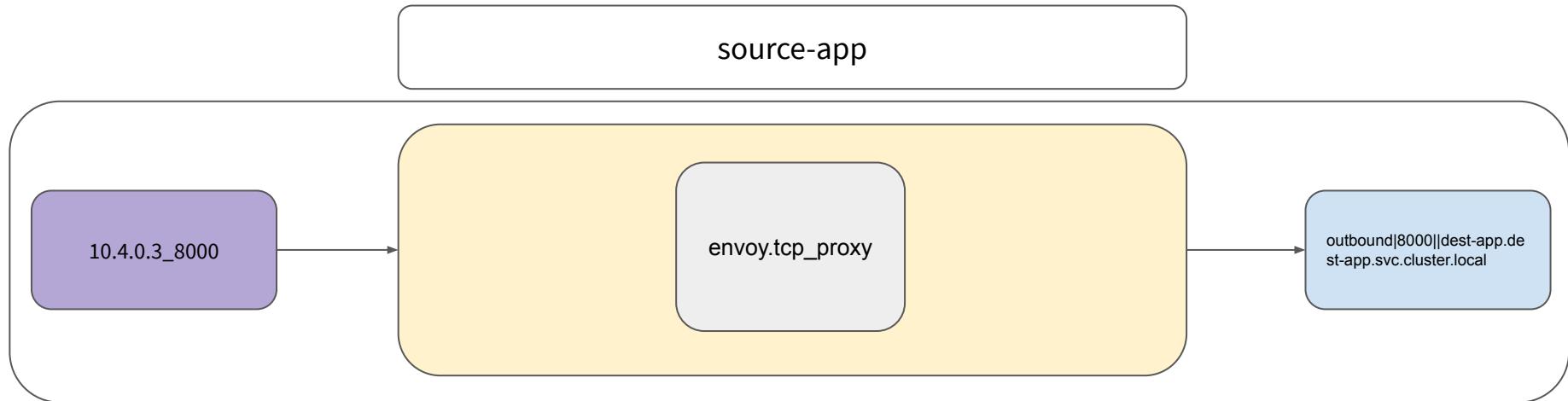


# envoy - operation

```
apiVersion: v1
kind: Service
metadata:
  labels:
    app: dest-app
    name: dest-app
    namespace: dest-app
spec:
  clusterIP: 10.4.0.3
  ports:
  - name: tcp-sweetport
    port: 8888
    protocol: TCP
    targetPort: 8888
  selector:
    app: dest-app
  sessionAffinity: None
  type: ClusterIP
```



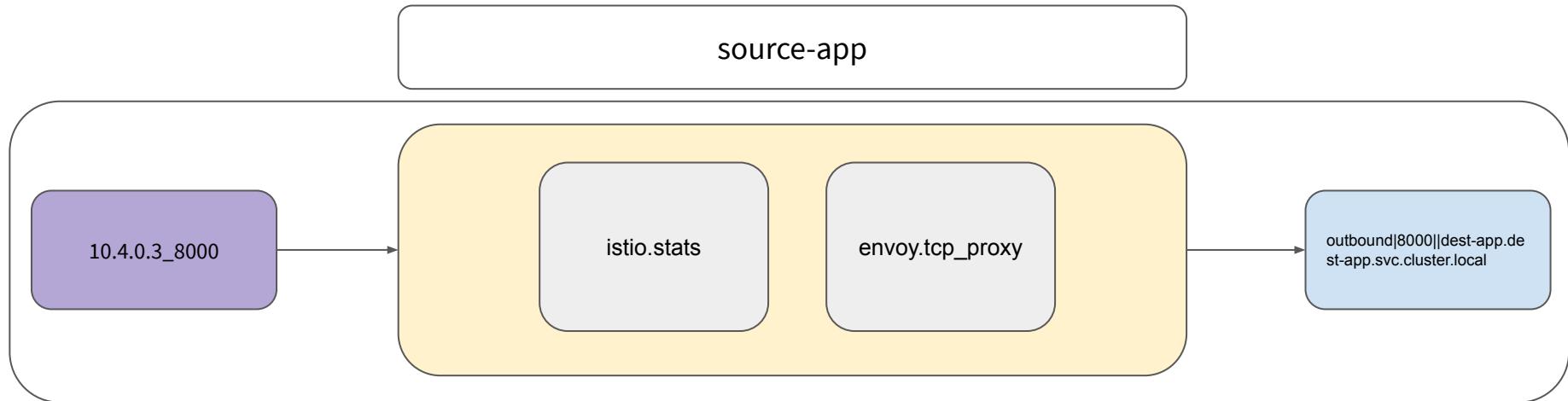
# envoy - operation



# envoy - operation

```
[  
  {  
    "name": "10.4.0.3_8000",  
    "address": {  
      "socketAddress": {  
        "address": "10.4.0.3",  
        "portValue": 8000  
      }  
    },  
    "filterChains": [  
      {  
        "filters": [  
          {  
            "name": "envoy.tcp_proxy",  
            "typedConfig": {  
              "@type": "type.googleapis.com/envoy.config.filter.network.tcp_proxy.v2.TcpProxy",  
              "statPrefix": "outbound|8000||dest-app.dest-app.svc.cluster.local",  
              "cluster": "outbound|8000||dest-app.dest-app.svc.cluster.local"  
            }  
          }  
        ]  
      }  
    ],  
    "deprecatedV1": {  
      "bindToPort": false  
    },  
    "trafficDirection": "OUTBOUND"  
  }  
]
```

# envoy - operation

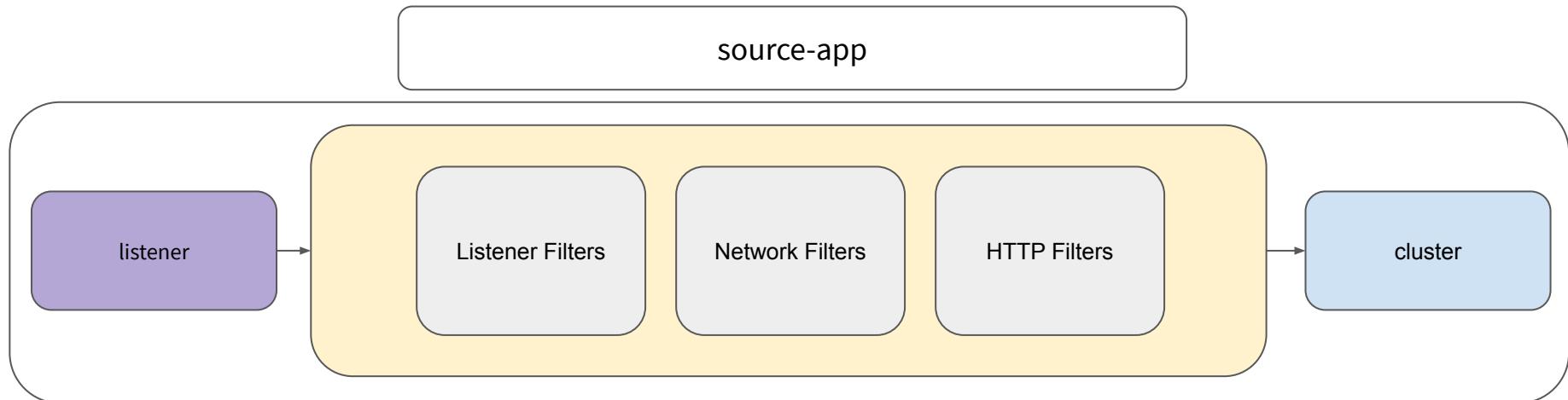


## envoy - operation - terminology

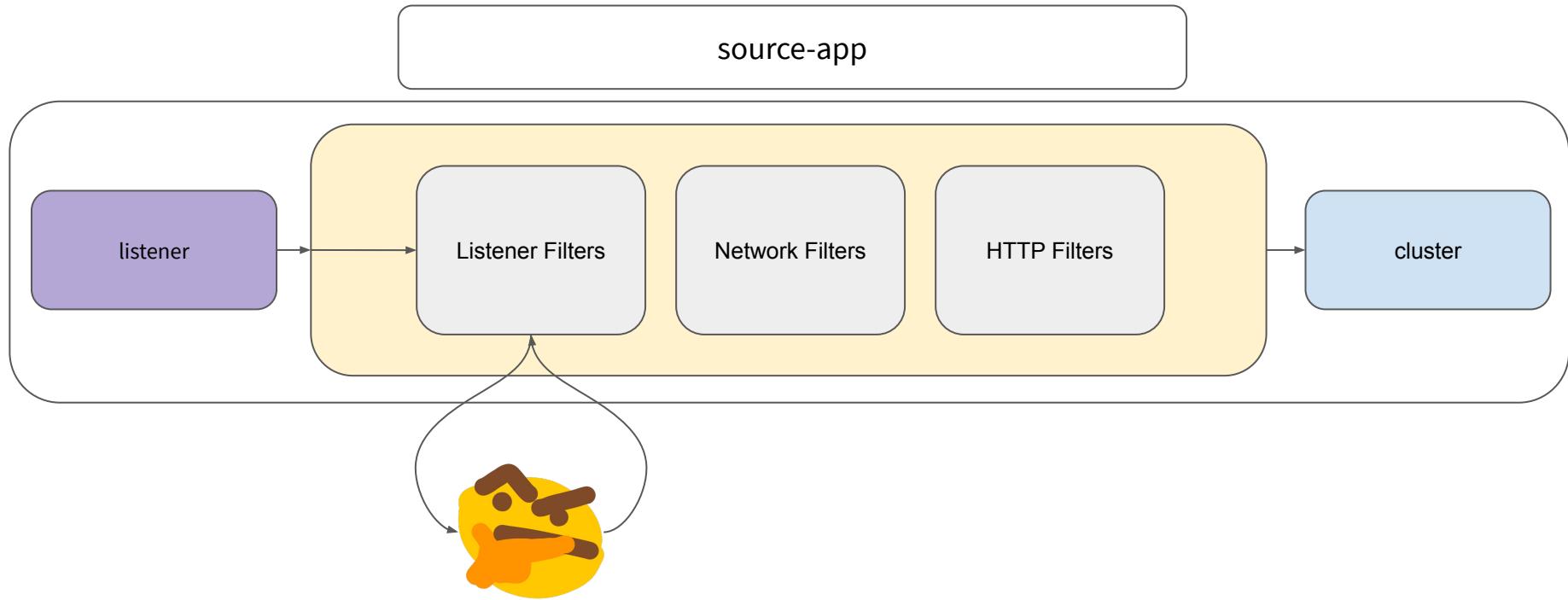
# Extensions & Plugins

- Access loggers
- Retry implementations
- Tracers
- Resource Monitors
- Credential Providers

# envoy - operation - filters

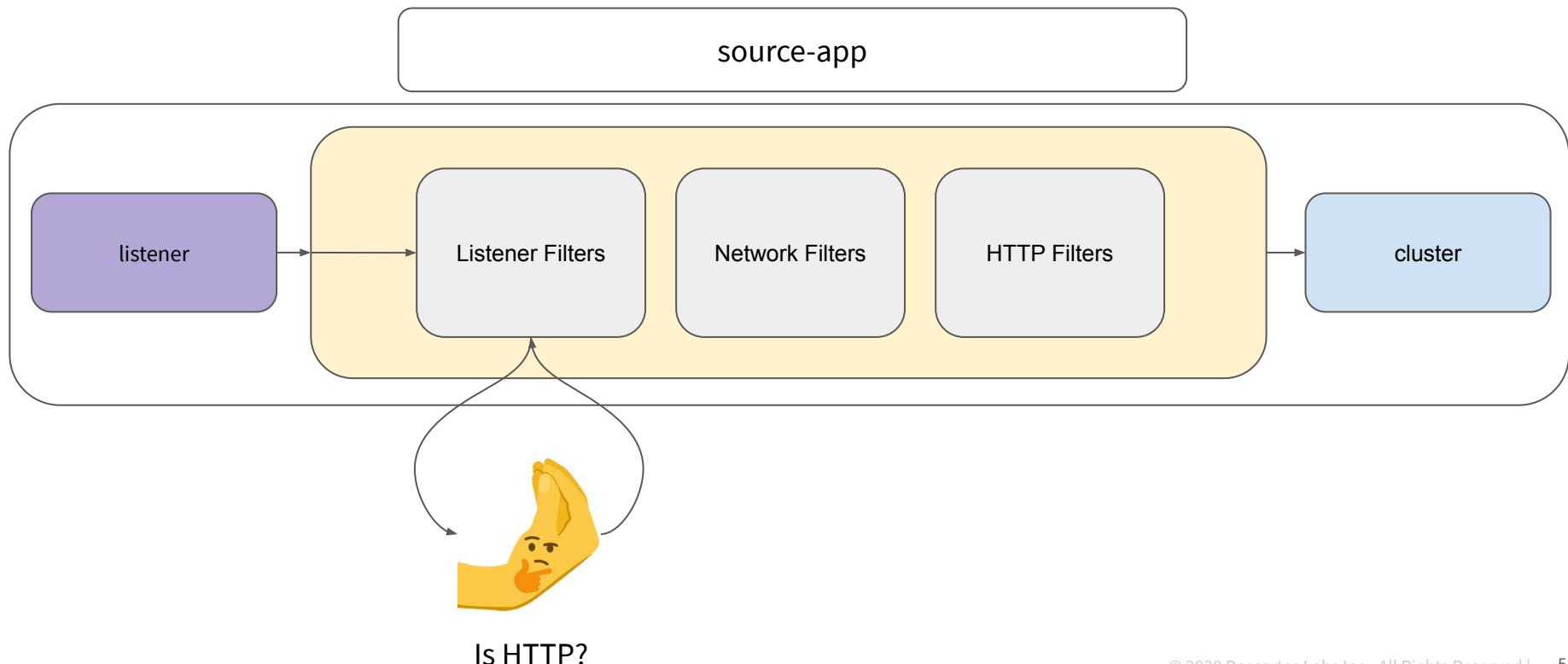


# envoy - operation - filter chains

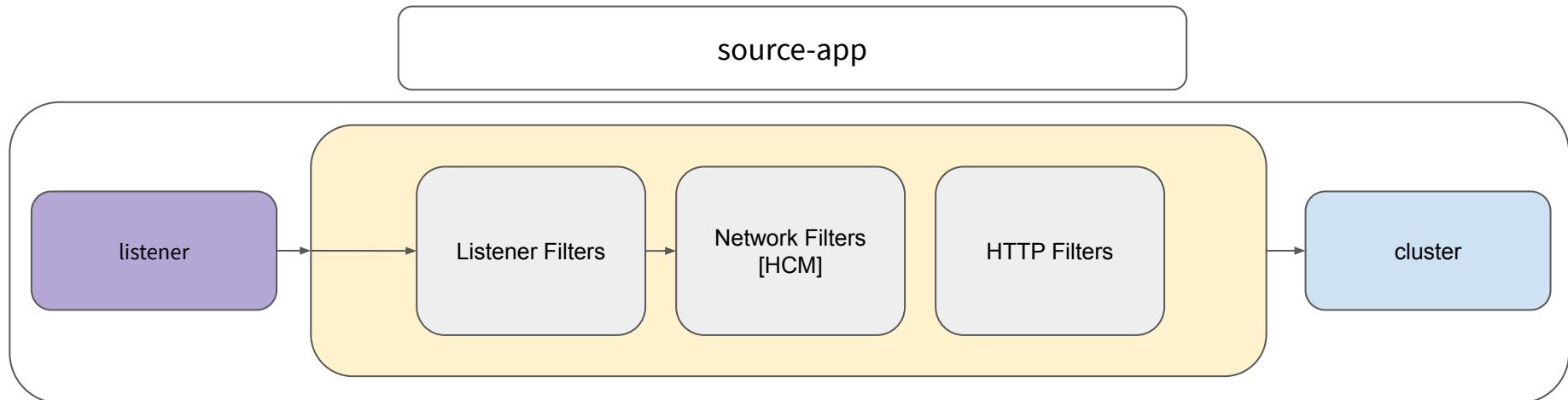


Is TLS?

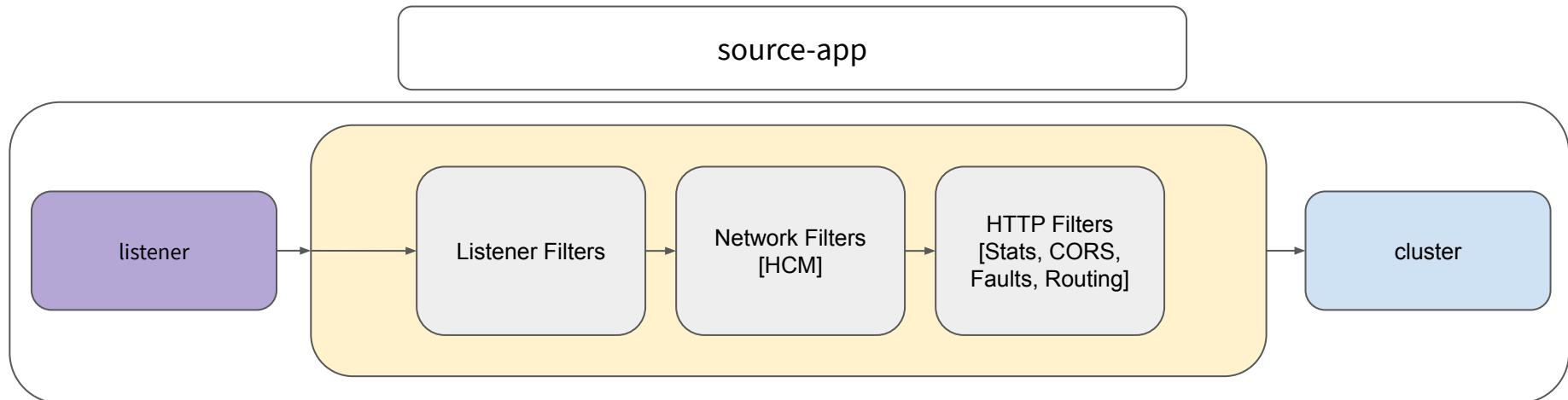
# envoy - operation - filter chains



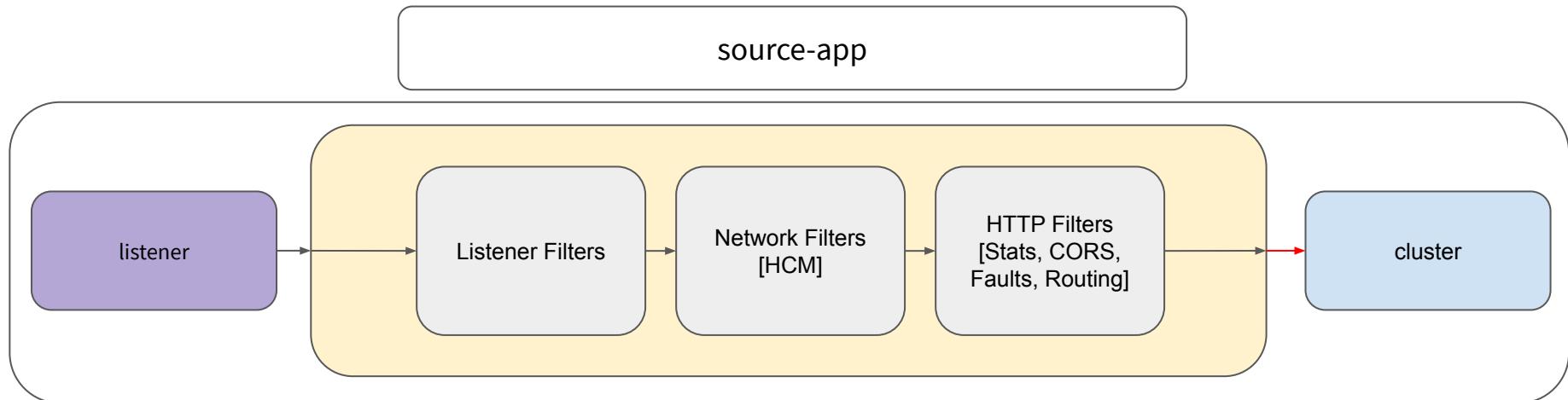
# envoy - operation - filter chains



# envoy - operation - filter chains

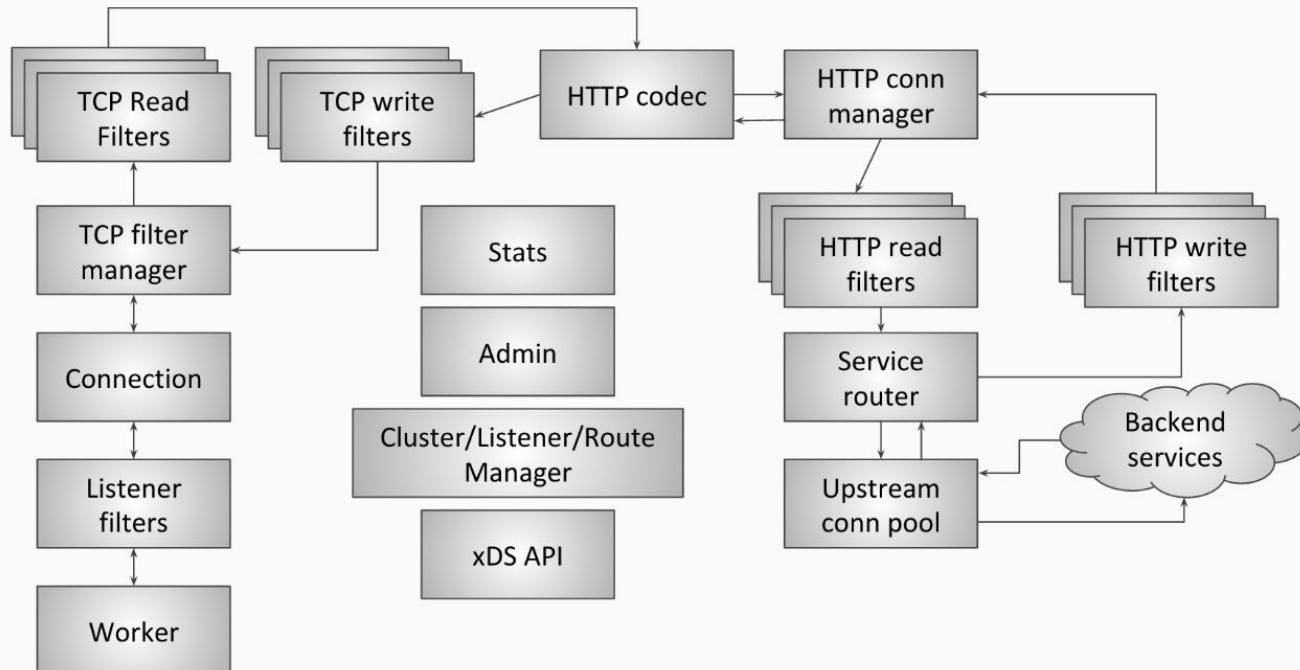


# envoy - operation - filter chains



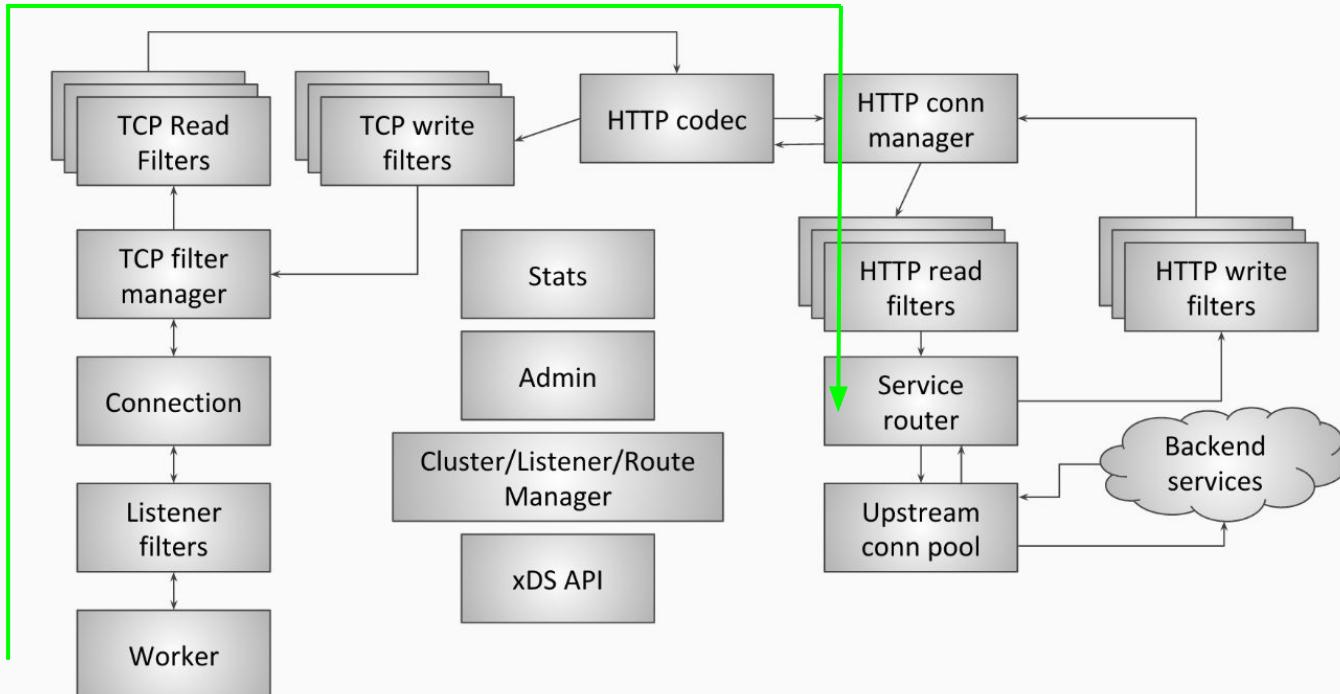
# envoy - operation - cluster manager

Envoy architecture diagram



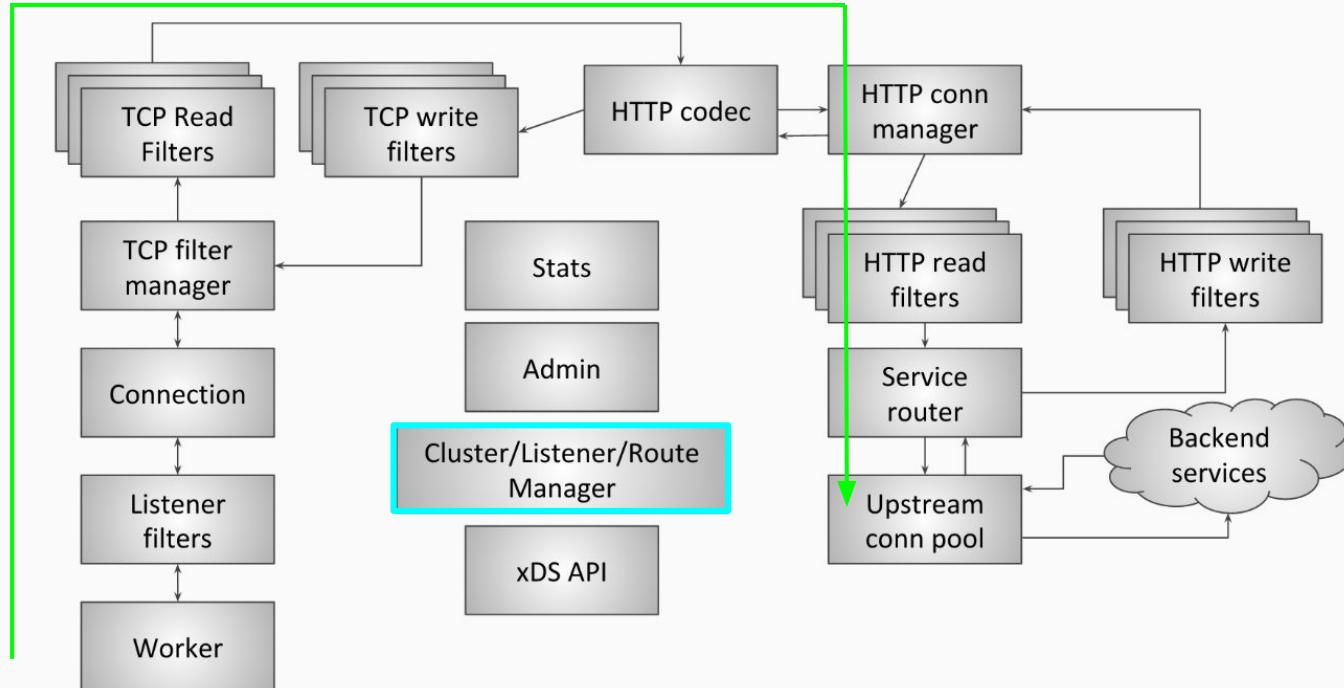
# envoy - operation - cluster manager

Envoy architecture diagram

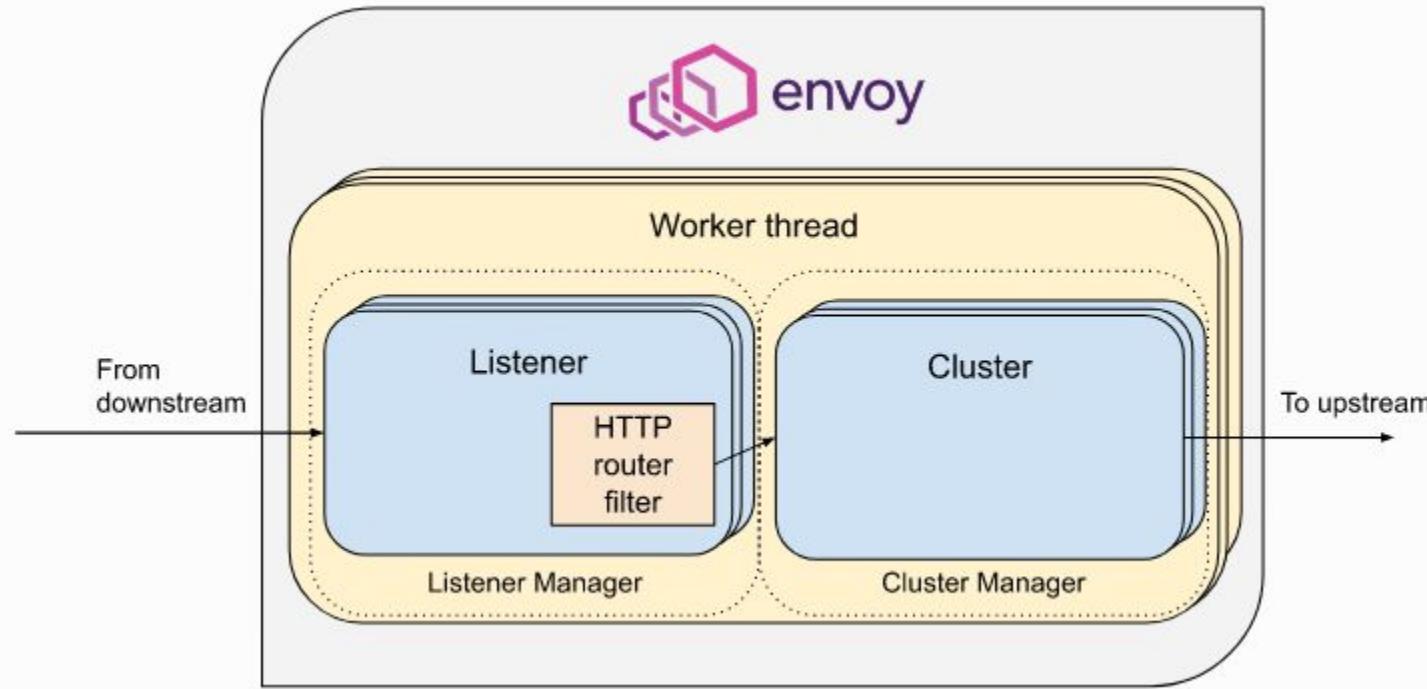


# envoy - operation - cluster manager

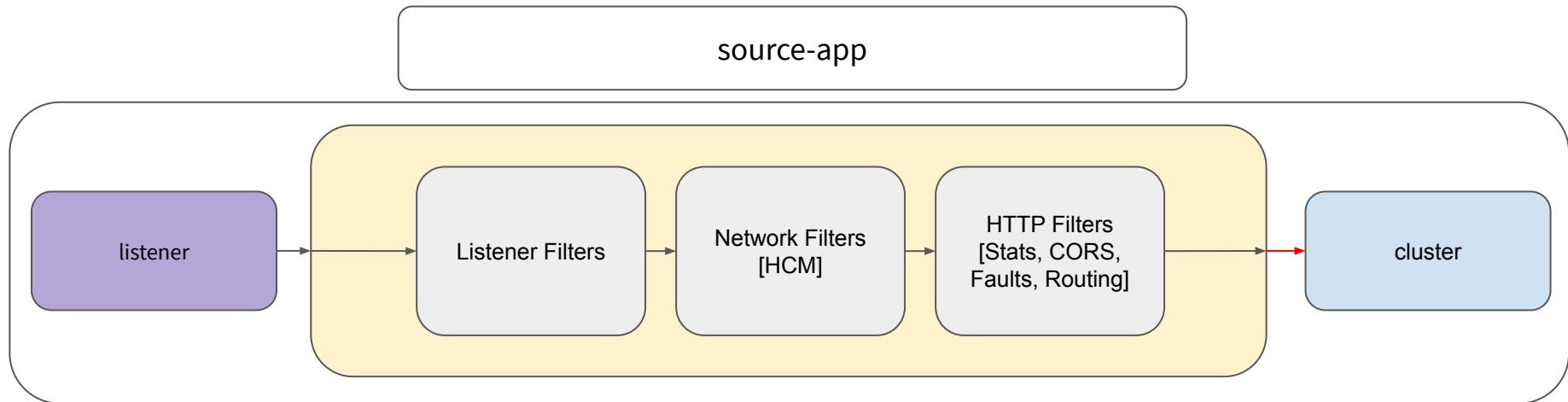
Envoy architecture diagram



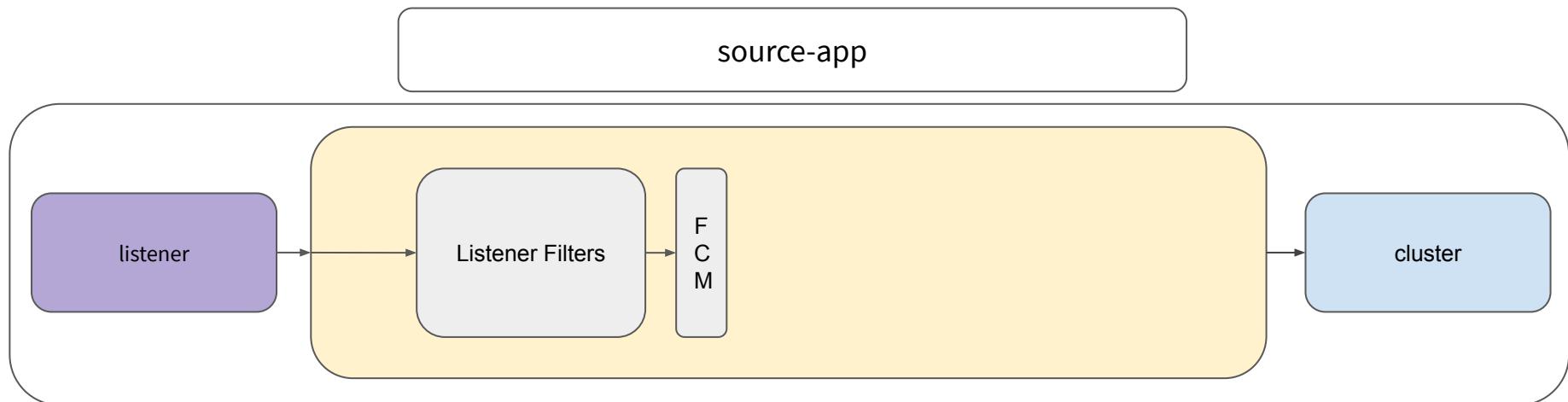
# envoy - operation - cluster manager



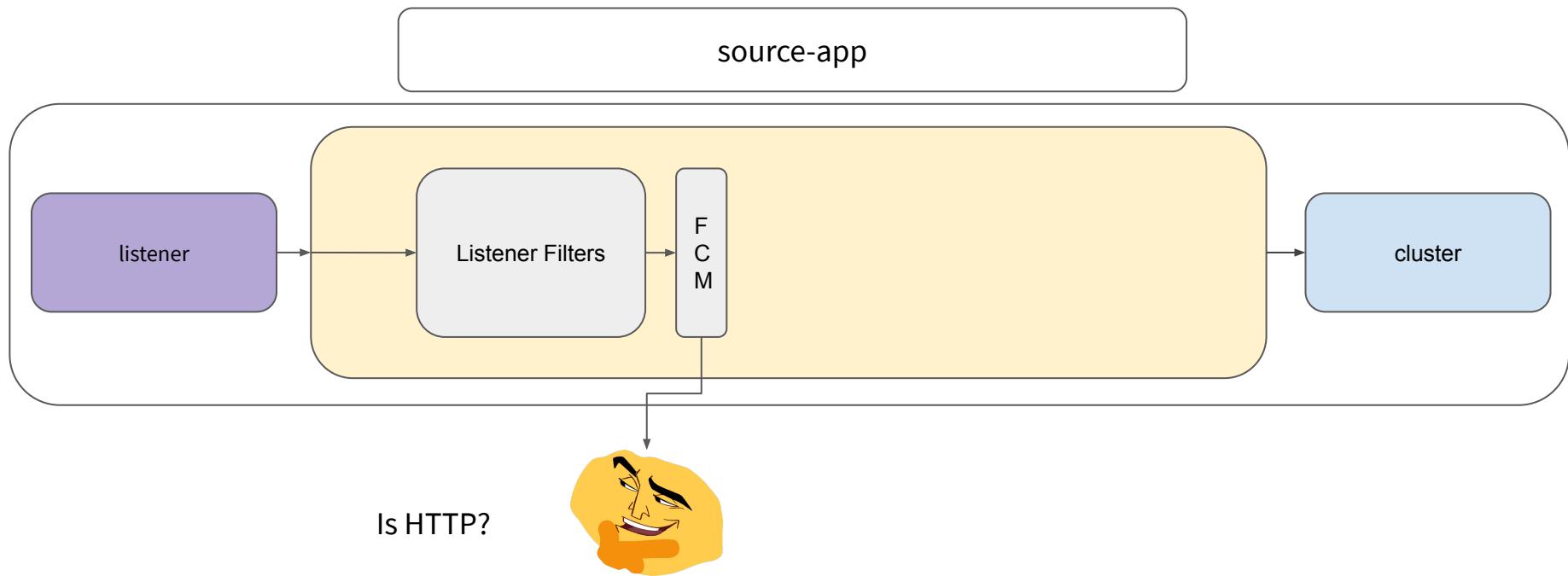
# envoy - operation - filter chains



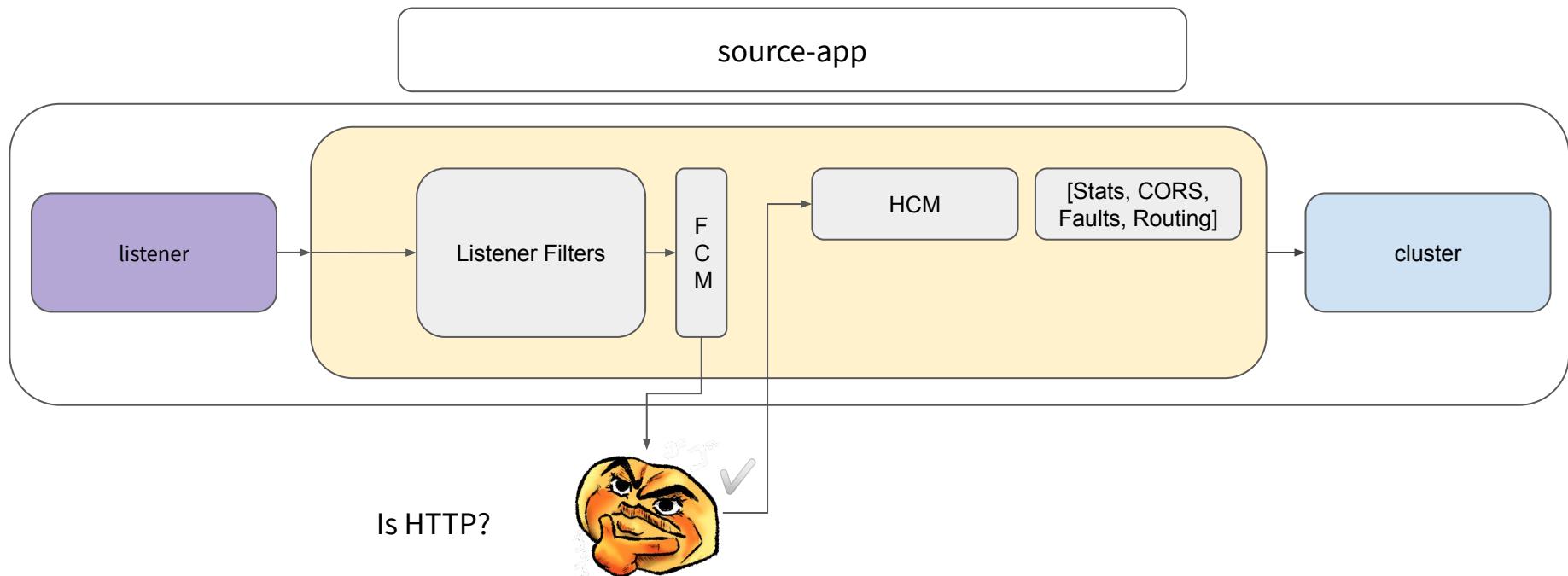
# envoy - operation - filter chain match



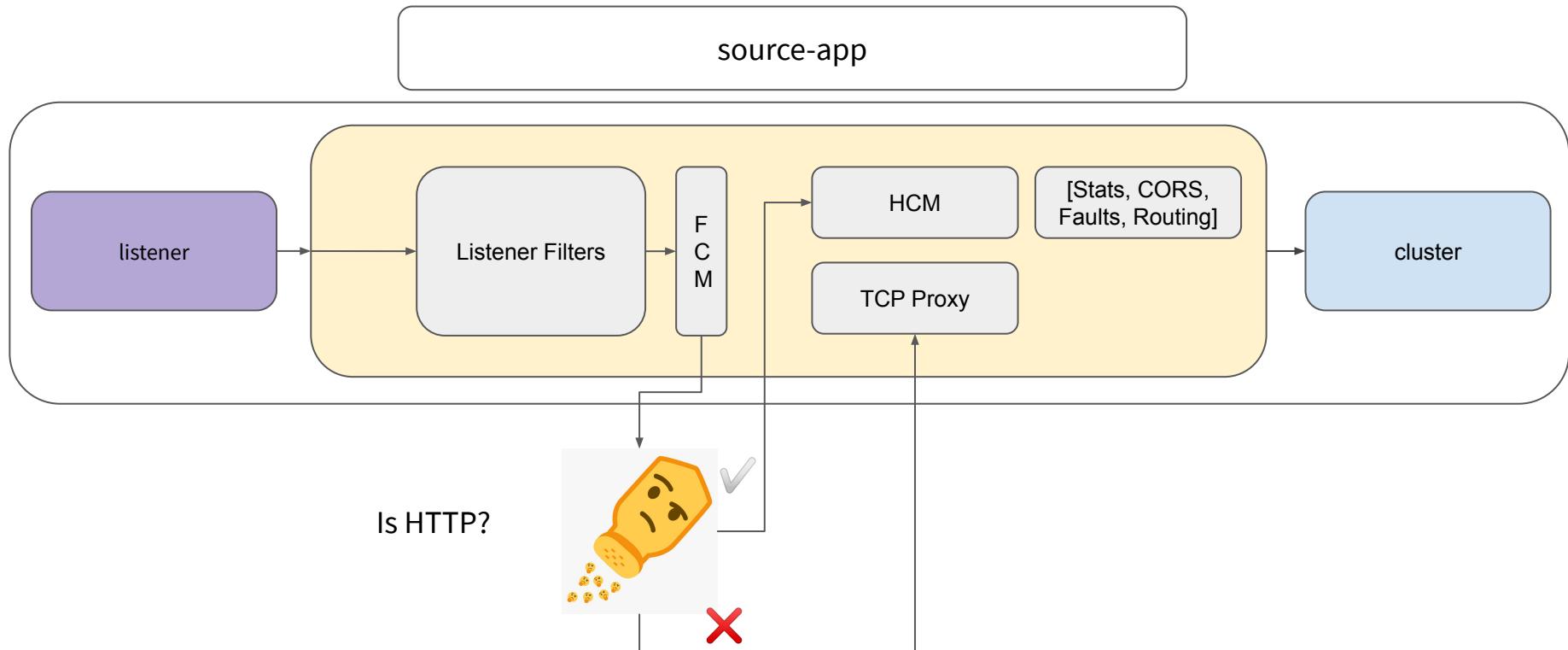
# envoy - operation - filter chain match



# envoy - operation - filter chain match



# envoy - operation - filter chain match

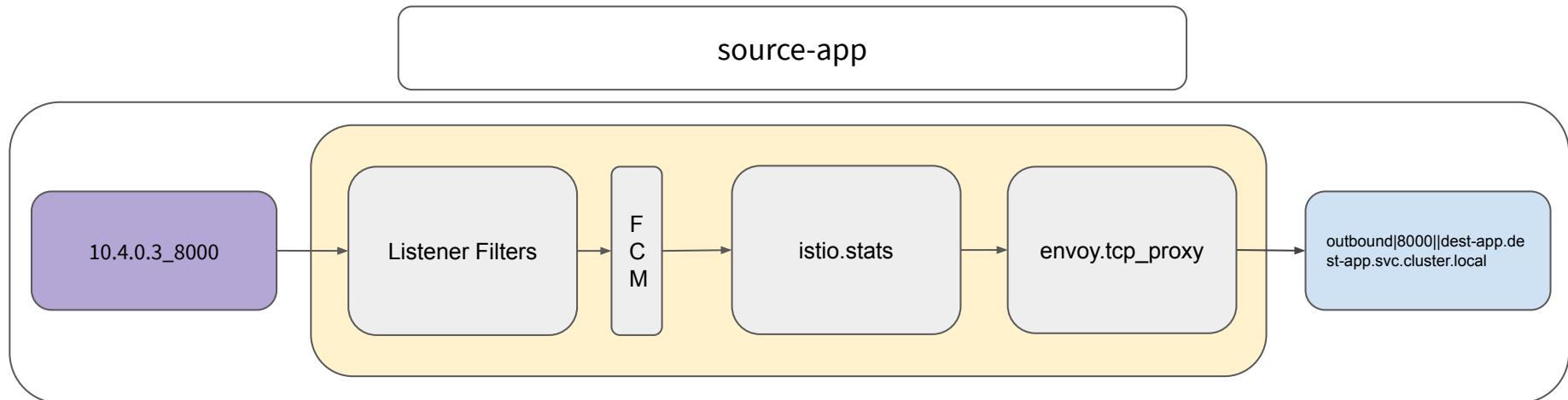


# envoy - operation - filter chain match

```

    {
      "name": "0.0.0.0_15010",
      "active_state": {
        "version_info": "2020-12-05T22:58:30Z/8",
        "listener": {
          "@type": "type.googleapis.com/envoy.api.v2.Listener",
          "name": "0.0.0.0_15010",
          "address": {
            "socket_address": {
              "address": "0.0.0.0",
              "port_value": 15010
            }
          },
          "filter_chains": [
            {
              "filter_chain_match": {
                "application_protocols": [
                  "http/1.0",
                  "http/1.1",
                  "h2c"
                ]
              },
              "filters": [ ... ] // 1 item
            },
            {
              "filter_chain_match": {},
              "filters": [ ... ], // 2 items
              "metadata": { ... }, // 1 item
              "name": "PassthroughFilterChain"
            }
          ],
          "deprecated_v1": { ... }, // 1 item
          "listener_filters": [ ... ], // 2 items
          "listener_filters_timeout": "0.100s",
          "traffic_direction": "OUTBOUND",
          "continue_on_listener_filters_timeout": true
        },
        "last_updated": "2020-12-05T23:00:19.805Z"
      }
    }
  
```

# envoy - operation



# envoy - operation

```

gke-compute-stage-preemptible-n1-stan-bddbf3b-thtc /home/rob # iptables -t nat -S
-P PREROUTING ACCEPT
-P INPUT ACCEPT
-P OUTPUT ACCEPT
-P POSTROUTING ACCEPT
-N ISTIO_INBOUND
-N ISTIO_IN_REDIRECT
-N ISTIO_OUTPUT
-N ISTIO_REDIRECT
-A PREROUTING -p tcp -j ISTIO_INBOUND
-A OUTPUT -p tcp -j ISTIO_OUTPUT
-A ISTIO_INBOUND -p tcp -m tcp --dport 22 -j RETURN
-A ISTIO_INBOUND -p tcp -m tcp --dport 15090 -j RETURN
-A ISTIO_INBOUND -p tcp -m tcp --dport 15021 -j RETURN
-A ISTIO_INBOUND -p tcp -m tcp --dport 15020 -j RETURN
-A ISTIO_INBOUND -p tcp -j ISTIO_IN_REDIRECT
-A ISTIO_IN_REDIRECT -p tcp -j REDIRECT --to-ports 15006
-A ISTIO_OUTPUT -s 127.0.0.6/32 -o lo -j RETURN
-A ISTIO_OUTPUT ! -d 127.0.0.1/32 -o lo -m owner --uid-owner 1337 -j ISTIO_IN_REDIRECT
-A ISTIO_OUTPUT -o lo -m owner ! --uid-owner 1337 -j RETURN
-A ISTIO_OUTPUT -m owner --uid-owner 1337 -j RETURN
-A ISTIO_OUTPUT ! -d 127.0.0.1/32 -o lo -m owner --gid-owner 1337 -j ISTIO_IN_REDIRECT
-A ISTIO_OUTPUT -o lo -m owner ! --gid-owner 1337 -j RETURN
-A ISTIO_OUTPUT -m owner --gid-owner 1337 -j RETURN
-A ISTIO_OUTPUT -d 127.0.0.1/32 -j RETURN
-A ISTIO_OUTPUT -j ISTIO_REDIRECT
-A ISTIO_REDIRECT -p tcp -j REDIRECT --to-ports 15001

```

# envoy - operation

```

gke-compute-stage-preemptible-n1-stan-bddbf3b-thtc /home/rob # iptables -t nat -S
-P PREROUTING ACCEPT
-P INPUT ACCEPT
-P OUTPUT ACCEPT
-P POSTROUTING ACCEPT
-N ISTIO_INBOUND
-N ISTIO_IN_REDIRECT
-N ISTIO_OUTPUT
-N ISTIO_REDIRECT
-A PREROUTING -p tcp -j ISTIO_INBOUND
-A OUTPUT -p tcp -j ISTIO_OUTPUT ←
-A ISTIO_INBOUND -p tcp -m tcp --dport 22 -j RETURN
-A ISTIO_INBOUND -p tcp -m tcp --dport 15090 -j RETURN
-A ISTIO_INBOUND -p tcp -m tcp --dport 15021 -j RETURN
-A ISTIO_INBOUND -p tcp -m tcp --dport 15020 -j RETURN
-A ISTIO_INBOUND -p tcp -j ISTIO_IN_REDIRECT
-A ISTIO_IN_REDIRECT -p tcp -j REDIRECT --to-ports 15006
-A ISTIO_OUTPUT -s 127.0.0.6/32 -o lo -j RETURN
-A ISTIO_OUTPUT ! -d 127.0.0.1/32 -o lo -m owner --uid-owner 1337 -j ISTIO_IN_REDIRECT
-A ISTIO_OUTPUT -o lo -m owner ! --uid-owner 1337 -j RETURN
-A ISTIO_OUTPUT -m owner --uid-owner 1337 -j RETURN
-A ISTIO_OUTPUT ! -d 127.0.0.1/32 -o lo -m owner --gid-owner 1337 -j ISTIO_IN_REDIRECT
-A ISTIO_OUTPUT -o lo -m owner ! --gid-owner 1337 -j RETURN
-A ISTIO_OUTPUT -m owner --gid-owner 1337 -j RETURN
-A ISTIO_OUTPUT -d 127.0.0.1/32 -j RETURN
-A ISTIO_OUTPUT -j ISTIO_REDIRECT
-A ISTIO_REDIRECT -p tcp -j REDIRECT --to-ports 15001

```

# envoy - operation

```

gke-compute-stage-preemptible-n1-stan-bddbf3b-thtc /home/rob # iptables -t nat -s
-P PREROUTING ACCEPT
-P INPUT ACCEPT
-P OUTPUT ACCEPT
-P POSTROUTING ACCEPT
-N ISTIO_INBOUND
-N ISTIO_IN_REDIRECT
-N ISTIO_OUTPUT
-N ISTIO_REDIRECT
-A PREROUTING -p tcp -j ISTIO_INBOUND
-A OUTPUT -p tcp -j ISTIO_OUTPUT
-A ISTIO_INBOUND -p tcp -m tcp --dport 22 -j RETURN
-A ISTIO_INBOUND -p tcp -m tcp --dport 15090 -j RETURN
-A ISTIO_INBOUND -p tcp -m tcp --dport 15021 -j RETURN
-A ISTIO_INBOUND -p tcp -m tcp --dport 15020 -j RETURN
-A ISTIO_INBOUND -p tcp -j ISTIO_IN_REDIRECT
-A ISTIO_IN_REDIRECT -p tcp -j REDIRECT --to-ports 15006
-A ISTIO_OUTPUT -s 127.0.0.6/32 -o lo -j RETURN
-A ISTIO_OUTPUT ! -d 127.0.0.1/32 -o lo -m owner --uid-owner 1337 -j ISTIO_IN_REDIRECT
-A ISTIO_OUTPUT -o lo -m owner ! --uid-owner 1337 -j RETURN
-A ISTIO_OUTPUT -m owner --uid-owner 1337 -j RETURN
-A ISTIO_OUTPUT ! -d 127.0.0.1/32 -o lo -m owner --gid-owner 1337 -j ISTIO_IN_REDIRECT
-A ISTIO_OUTPUT -o lo -m owner ! --gid-owner 1337 -j RETURN
-A ISTIO_OUTPUT -m owner --gid-owner 1337 -j RETURN
-A ISTIO_OUTPUT -d 127.0.0.1/32 -j RETURN
-A ISTIO_OUTPUT -j ISTIO_REDIRECT
-A ISTIO_REDIRECT -p tcp -j REDIRECT --to-ports 15001

```

# envoy - operation

```

gke-compute-stage-preemptible-n1-stan-bddbf3b-thtc /home/rob # iptables -t nat -S
-P PREROUTING ACCEPT
-P INPUT ACCEPT
-P OUTPUT ACCEPT
-P POSTROUTING ACCEPT
-N ISTIO_INBOUND
-N ISTIO_IN_REDIRECT
-N ISTIO_OUTPUT
-N ISTIO_REDIRECT
-A PREROUTING -p tcp -j ISTIO_INBOUND
-A OUTPUT -p tcp -j ISTIO_OUTPUT
-A ISTIO_INBOUND -p tcp -m tcp --dport 22 -j RETURN
-A ISTIO_INBOUND -p tcp -m tcp --dport 15090 -j RETURN
-A ISTIO_INBOUND -p tcp -m tcp --dport 15021 -j RETURN
-A ISTIO_INBOUND -p tcp -m tcp --dport 15020 -j RETURN
-A ISTIO_INBOUND -p tcp -j ISTIO_IN_REDIRECT
-A ISTIO_IN_REDIRECT -p tcp -j REDIRECT --to-ports 15006
-A ISTIO_OUTPUT -j ISTIO_IN_REDIRECT
-A ISTIO_OUTPUT -j ISTIO_IN_REDIRECT
-A ISTIO_OUTPUT -j ISTIO_REDIRECT
-A ISTIO_REDIRECT -p tcp -j REDIRECT --to-ports 15001

```

# envoy - operation

```
gke-compute-stage-preemptible-n1-stan-bddbf3b-thtc /home/rob # iptables -t nat -S
-P PREROUTING ACCEPT
-P INPUT ACCEPT
-P OUTPUT ACCEPT
-P POSTROUTING ACCEPT
-N ISTIO_INBOUND
-N ISTIO_IN_REDIRECT
-N ISTIO_OUTPUT
-N ISTIO_REDIRECT
-A PREROUTING -p tcp -j ISTIO_INBOUND
-A OUTPUT -p tcp -j ISTIO_OUTPUT
-A ISTIO_INBOUND -p tcp -m tcp --dport 22 -j RETURN
-A ISTIO_INBOUND -p tcp -m tcp --dport 15090 -j RETURN
-A ISTIO_INBOUND -p tcp -m tcp --dport 15021 -j RETURN
-A ISTIO_INBOUND -p tcp -m tcp --dport 15020 -j RETURN
-A ISTIO_INBOUND -p tcp -j ISTIO_IN_REDIRECT
-A ISTIO_IN_REDIRECT -p tcp -j REDIRECT --to-ports 15006
```

```
-A ISTIO_REDIRECT -p tcp -j REDIRECT --to-ports 15001
```

# envoy - operation

```

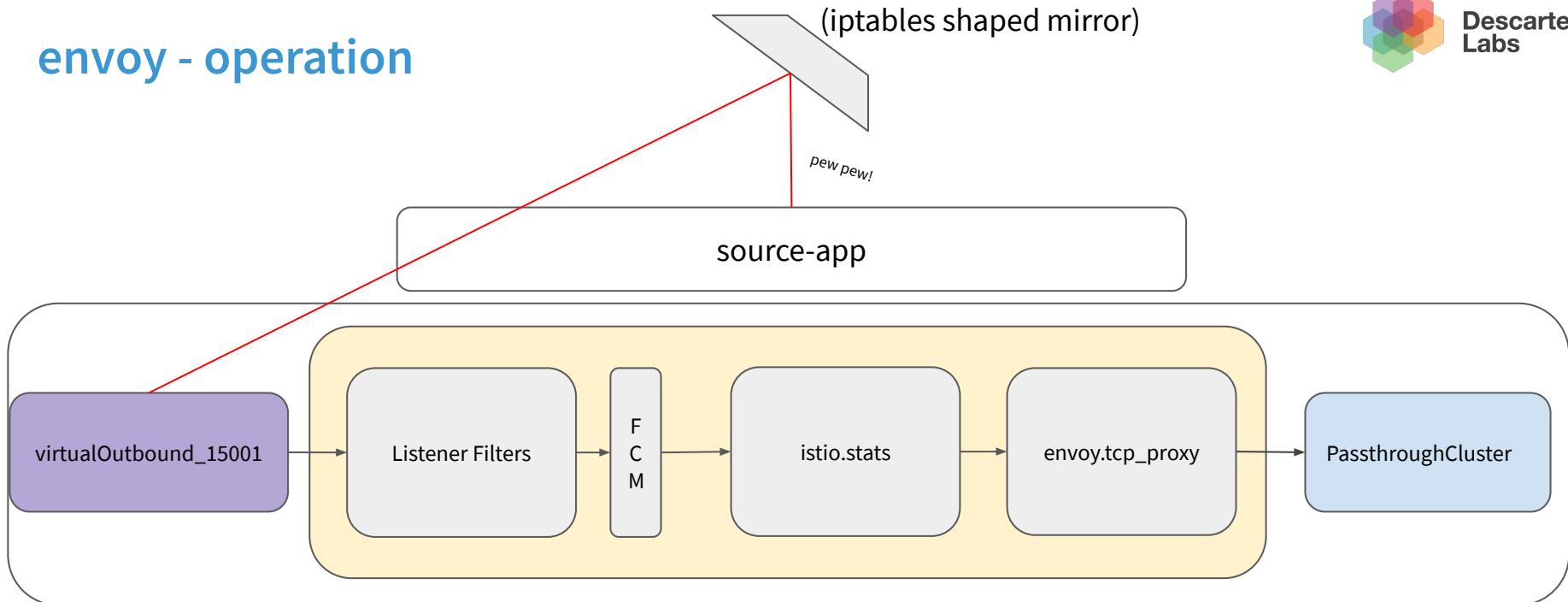
gke-compute-stage-preemptible-n1-stan-bddbf3b-thtc /home/rob # iptables -t nat -s
-P PREROUTING ACCEPT
-P INPUT ACCEPT
-P OUTPUT ACCEPT
-P POSTROUTING ACCEPT
-N ISTIO_INBOUND
-N ISTIO_IN_REDIRECT
-N ISTIO_OUTPUT
-N ISTIO_REDIRECT
-A PREROUTING -p tcp -j ISTIO_INBOUND ←
-A OUTPUT -p tcp -j ISTIO_OUTPUT
-A ISTIO_INBOUND -p tcp -j ISTIO_IN_REDIRECT
-A ISTIO_IN_REDIRECT -p tcp -j REDIRECT --to-ports 15006
-A ISTIO_OUTPUT -s 127.0.0.6/32 -o lo -j RETURN
-A ISTIO_OUTPUT ! -d 127.0.0.1/32 -o lo -m owner --uid-owner 1337 -j ISTIO_IN_REDIRECT
-A ISTIO_OUTPUT -o lo -m owner ! --uid-owner 1337 -j RETURN
-A ISTIO_OUTPUT -m owner --uid-owner 1337 -j RETURN
-A ISTIO_OUTPUT ! -d 127.0.0.1/32 -o lo -m owner --gid-owner 1337 -j ISTIO_IN_REDIRECT
-A ISTIO_OUTPUT -o lo -m owner ! --gid-owner 1337 -j RETURN
-A ISTIO_OUTPUT -m owner --gid-owner 1337 -j RETURN
-A ISTIO_OUTPUT -d 127.0.0.1/32 -j RETURN
-A ISTIO_OUTPUT -j ISTIO_REDIRECT
-A ISTIO_REDIRECT -p tcp -j REDIRECT --to-ports 15001

```

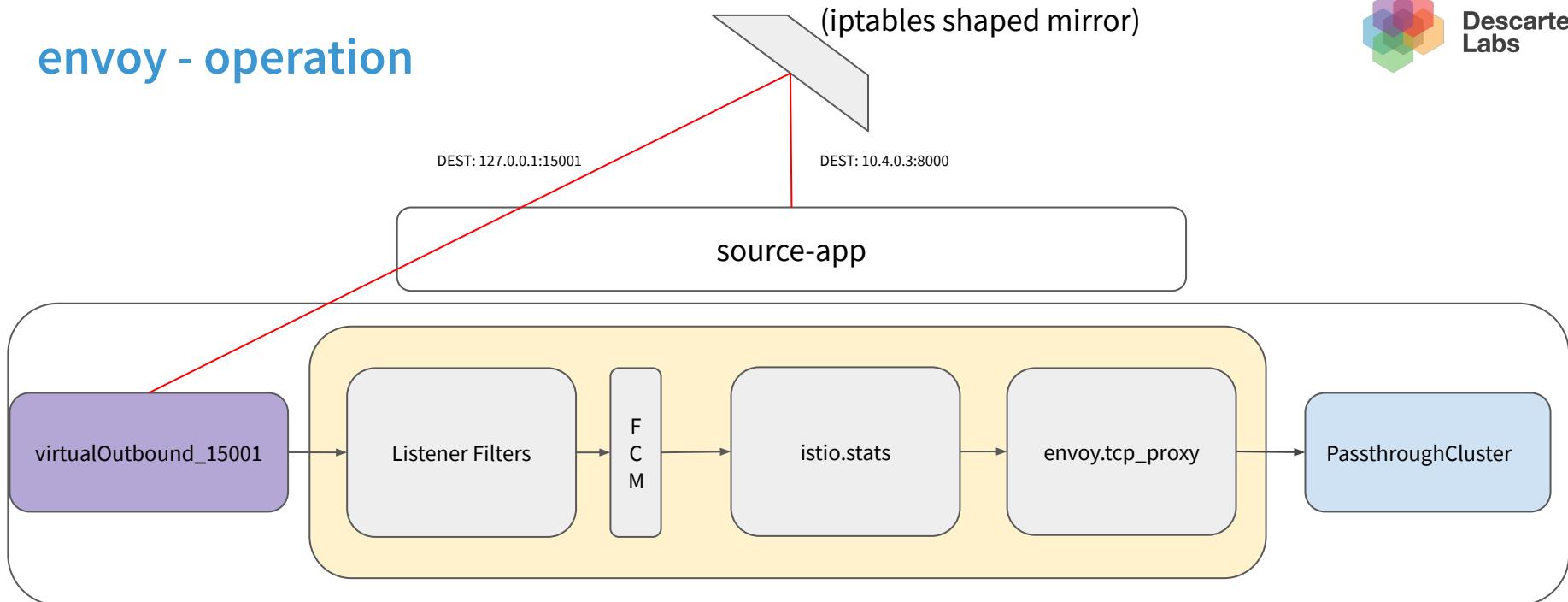
# envoy - operation

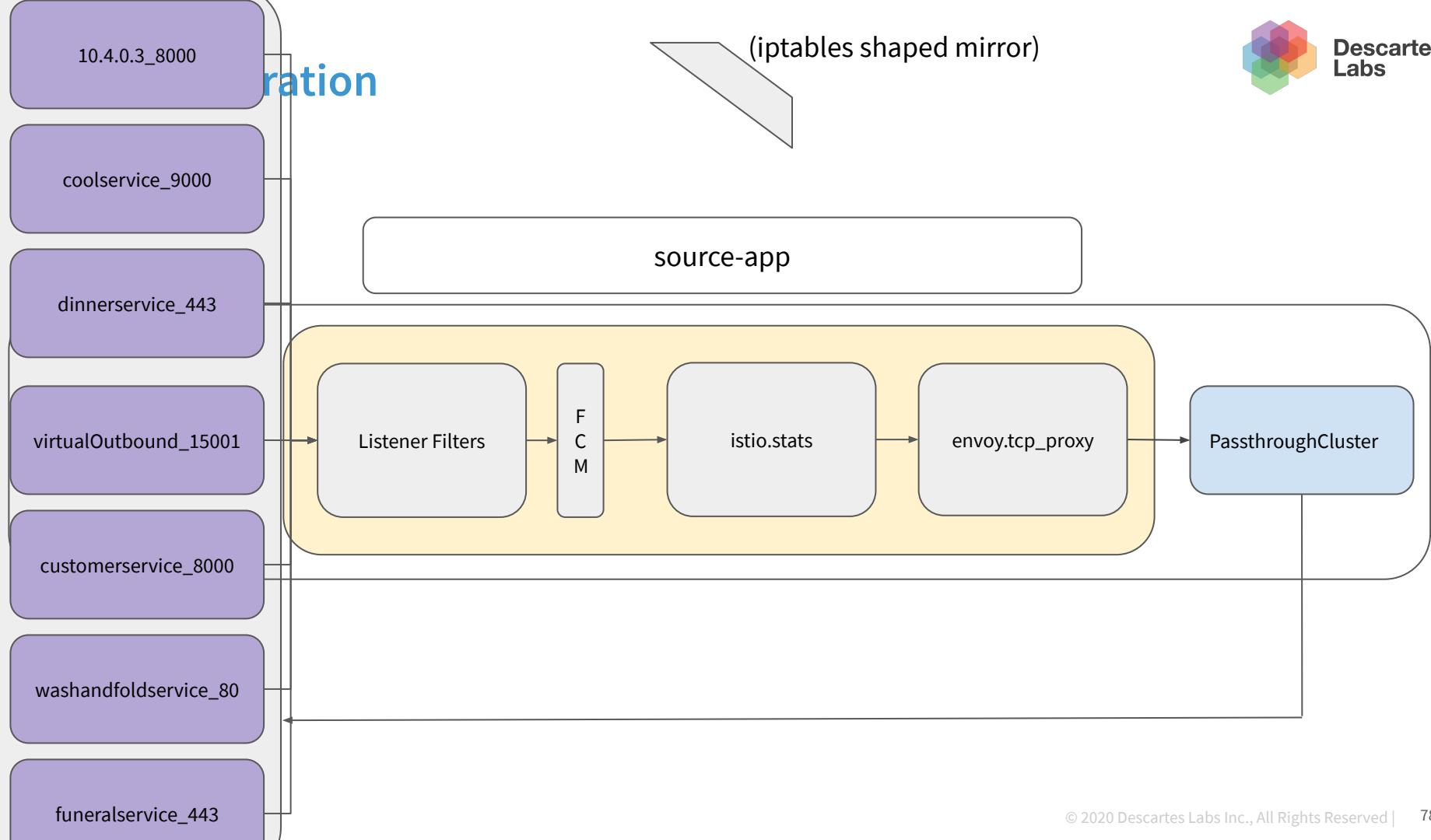
```
$ ss -ltp
State      Recv-Q      Send-Q      Local Address:Port      Peer  Address:Port
LISTEN      0            128          0.0.0.0:15021        0.0.0.0:*
LISTEN      0            128          0.0.0.0:15090        0.0.0.0:*
LISTEN      0            128          127.0.0.1:15000      0.0.0.0:*
LISTEN      0            128          0.0.0.0:15001        0.0.0.0:*
LISTEN      0            128          0.0.0.0:15006        0.0.0.0:*
LISTEN      0            1024         *:15020                *:*
$ |
```

# envoy - operation



# envoy - operation

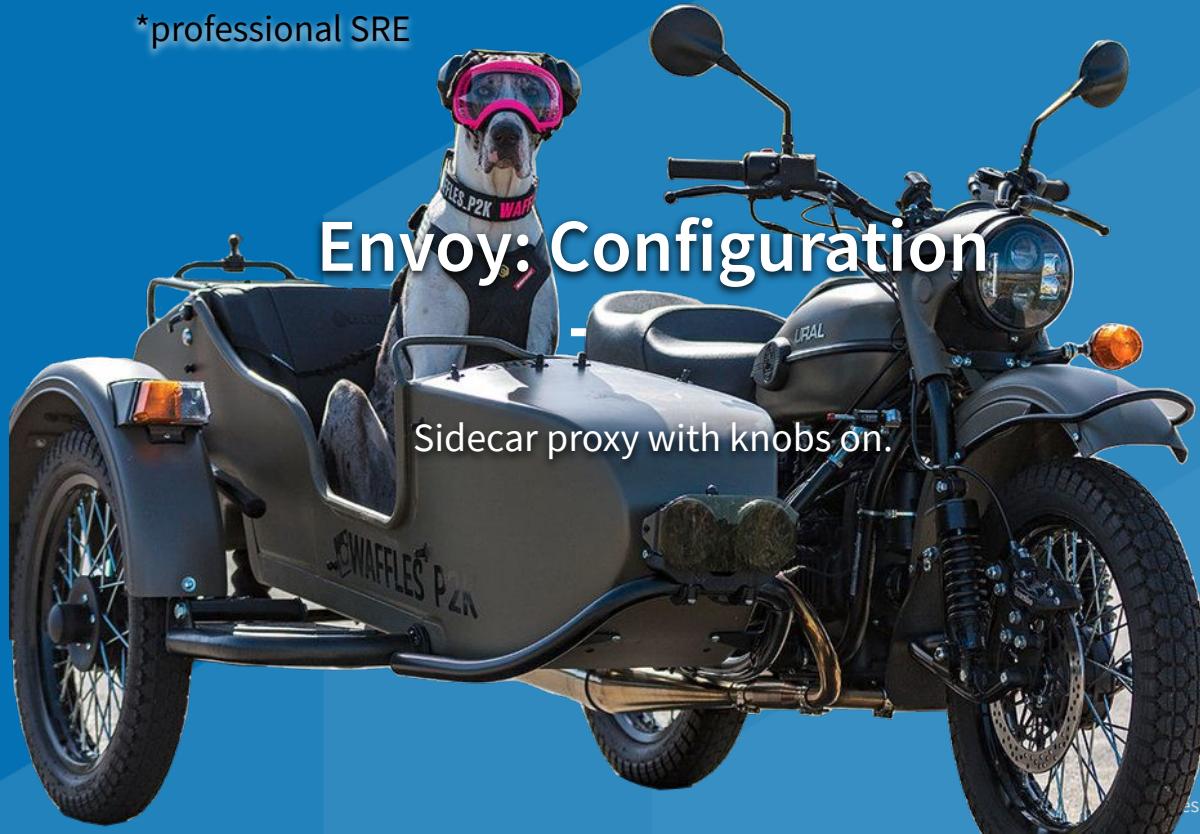




\*professional SRE

# Envoy: Configuration

- Sidecar proxy with knobs on.



# envoy - config



Yuval Kohavi

```

File Edit Selection View Go Run Terminal Help
examples.md  server_tcp.go  simple_tcp.yaml  server.go  simple.yaml  cors.yaml  Untitled-1
I cors.yaml > Cloud Code > () static_resources > [ ] listeners > [ ] filter_chains > [ ] filters > () typed_config > [ ] http_filters > name
11   filter_chains:
12     - filters:
13       - name: envoy.filters.network.http_connection_manager
14         typed_config:
15           "@type": type.googleapis.com/envoy.extensions.filters.network.http_connection_manager.v3.HttpConnectionManager
16           stat_prefix: ingress_http
17           route_config:
18             name: local_route
19             virtual_hosts:
20               - name: namespace.local_service
21                 domains: ["*"]
22                 routes:
23                   - match: { prefix: "/" }
24                     route:
25                       cluster: somecluster
26                       cors:
27                         allow_origin_string_match:
28                           - prefix: solo.io
29                         http_filters:
30                           - name: envoy.filters.http.cors
31                           - name: envoy.filters.http.router
32             clusters:
33               - name: somecluster...
34
35
36
37
38

```

envoy configuration is not meant for people it's meant for machines

**ZOOM**

# envoy - config

```

admin:
  access_log_path: /tmp/admin_access.log
  address:
    socket_address: { address: 127.0.0.1, port_value: 9901 }

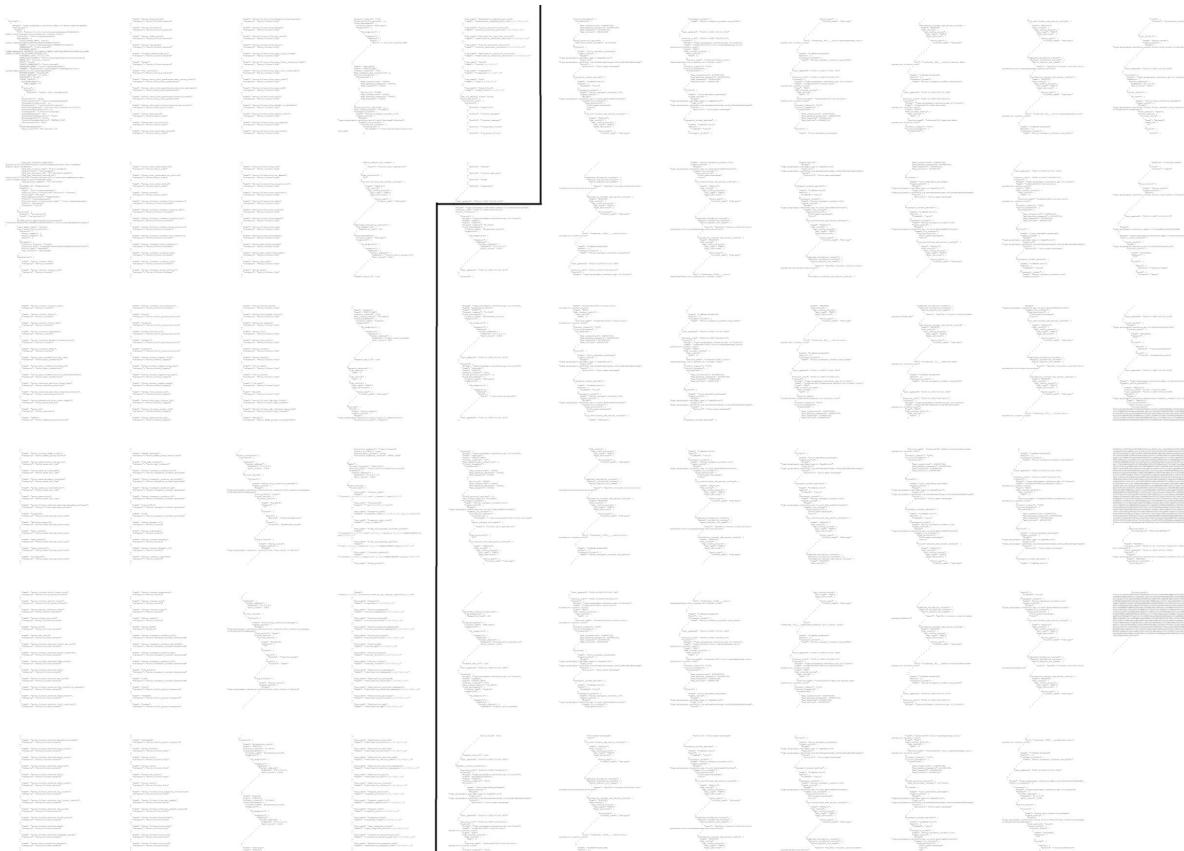
static_resources:
  listeners:
    - name: listener_0
      address:
        socket_address: { address: 127.0.0.1, port_value: 10000 }
      filter_chains:
        - filters:
            - name: envoy.filters.network.http_connection_manager
              typed_config:
                "@type": type.googleapis.com/envoy.extensions.filters.network.http_connection_manager.v3.HttpConnectionManager
                stat_prefix: ingress_http
                codec_type: AUTO
              route_config:
                name: local_route
                virtual_hosts:
                  - name: local_service
                    domains: [ "*" ]
                    routes:
                      - match: { prefix: "/" }
                        route: { cluster: some_service }
              http_filters:
                - name: envoy.filters.http.router
  clusters:
    - name: some_service
      connect_timeout: 0.25s
      type: STATIC
      lb_policy: ROUND_ROBIN
      load_assignment:
        cluster_name: some_service
        endpoints:
          - lb_endpoints:
              - endpoint:
                  address:
                    socket_address:
                      address: 127.0.0.1
                      port_value: 1234

```

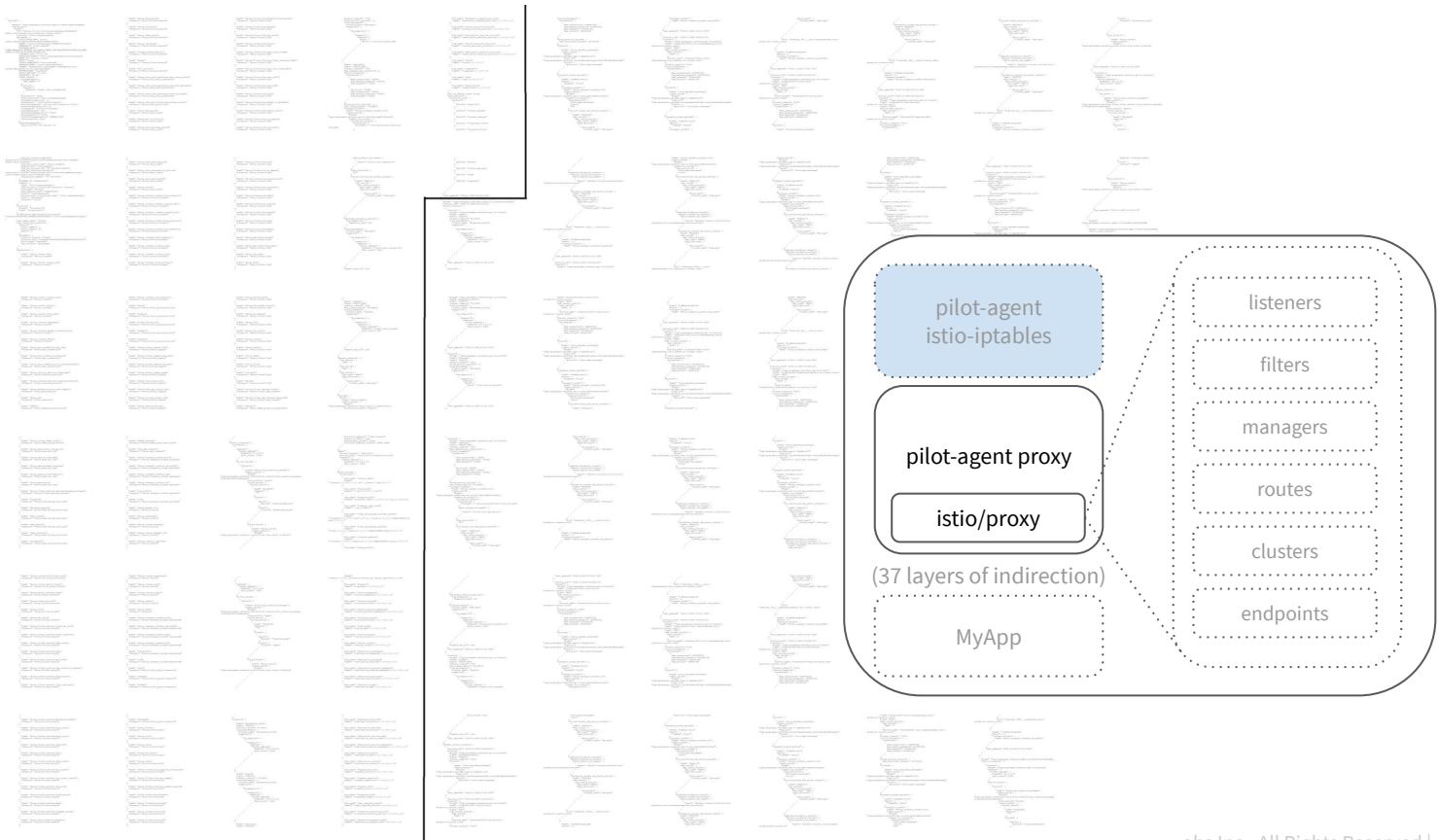
# envoy - config



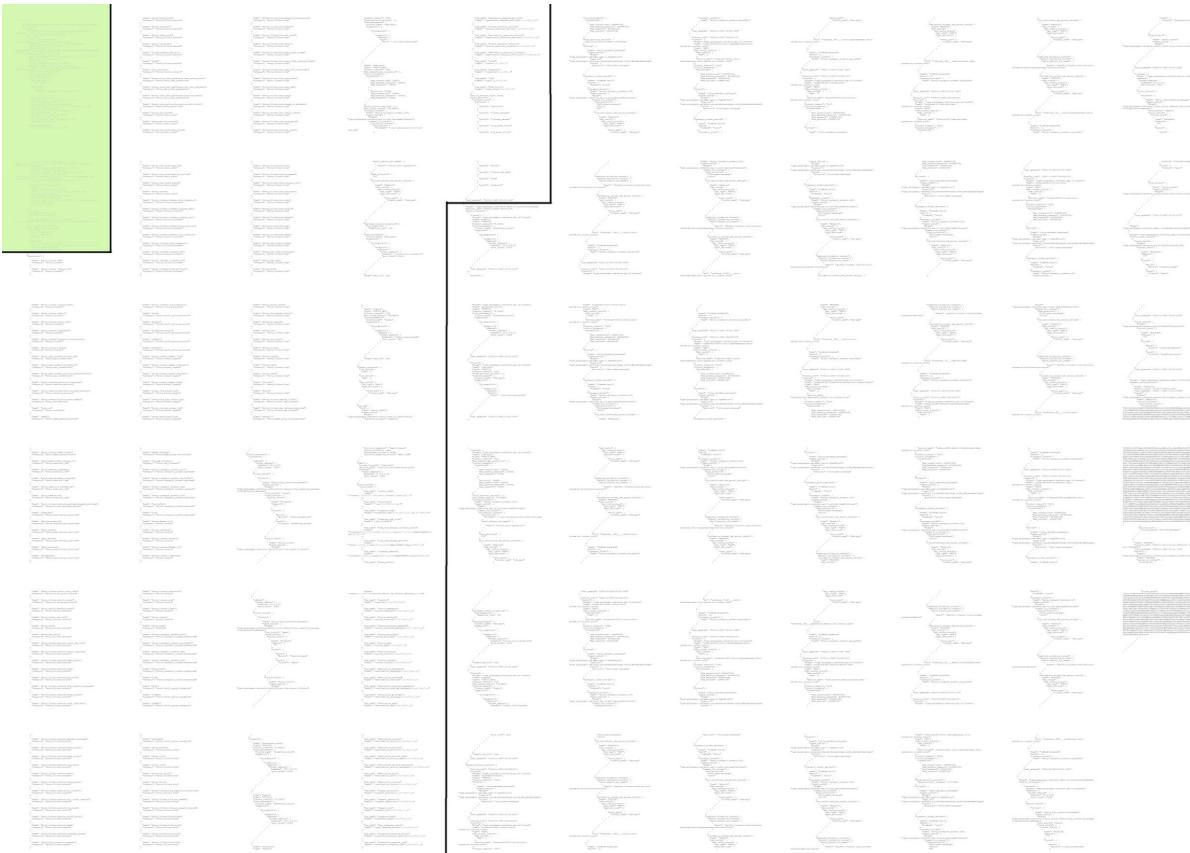
# envoy - config - bootstrap



# envoy - config - bootstrap



# envoy - config - bootstrap



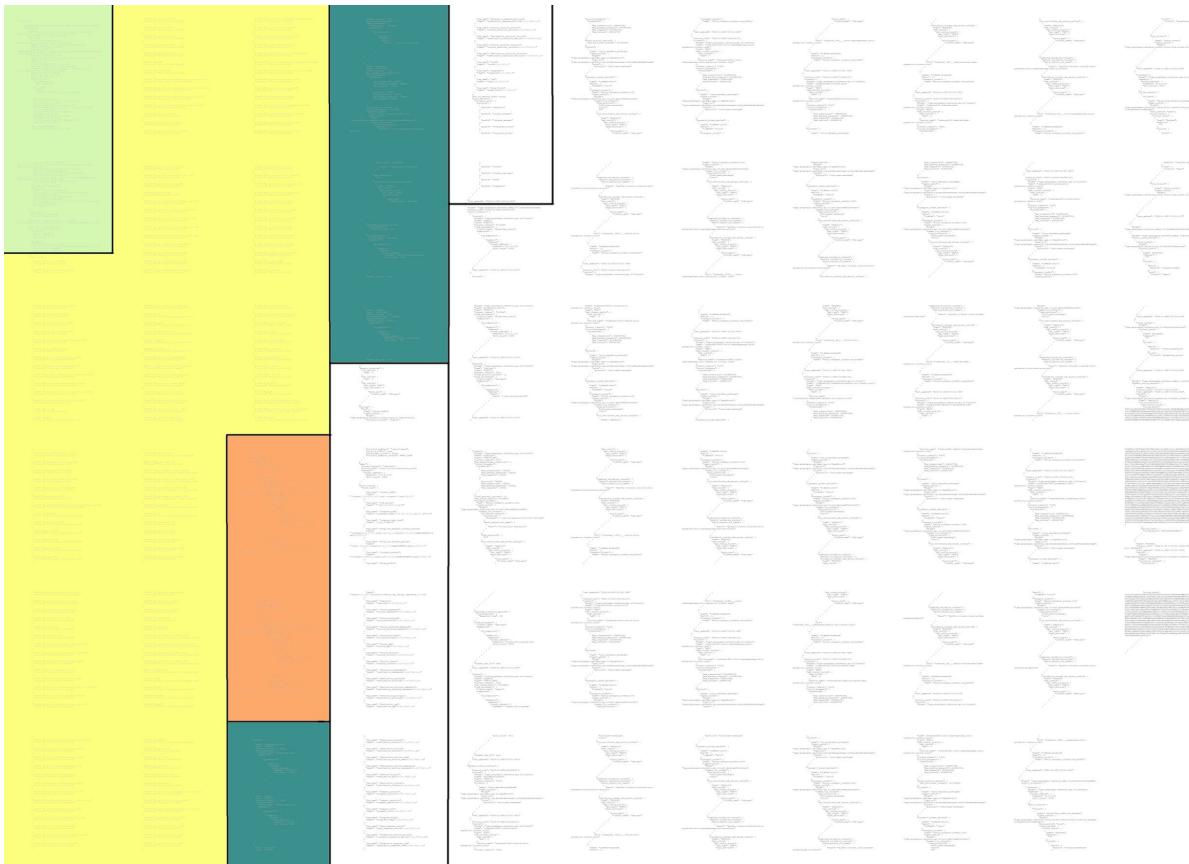
# envoy - config - bootstrap



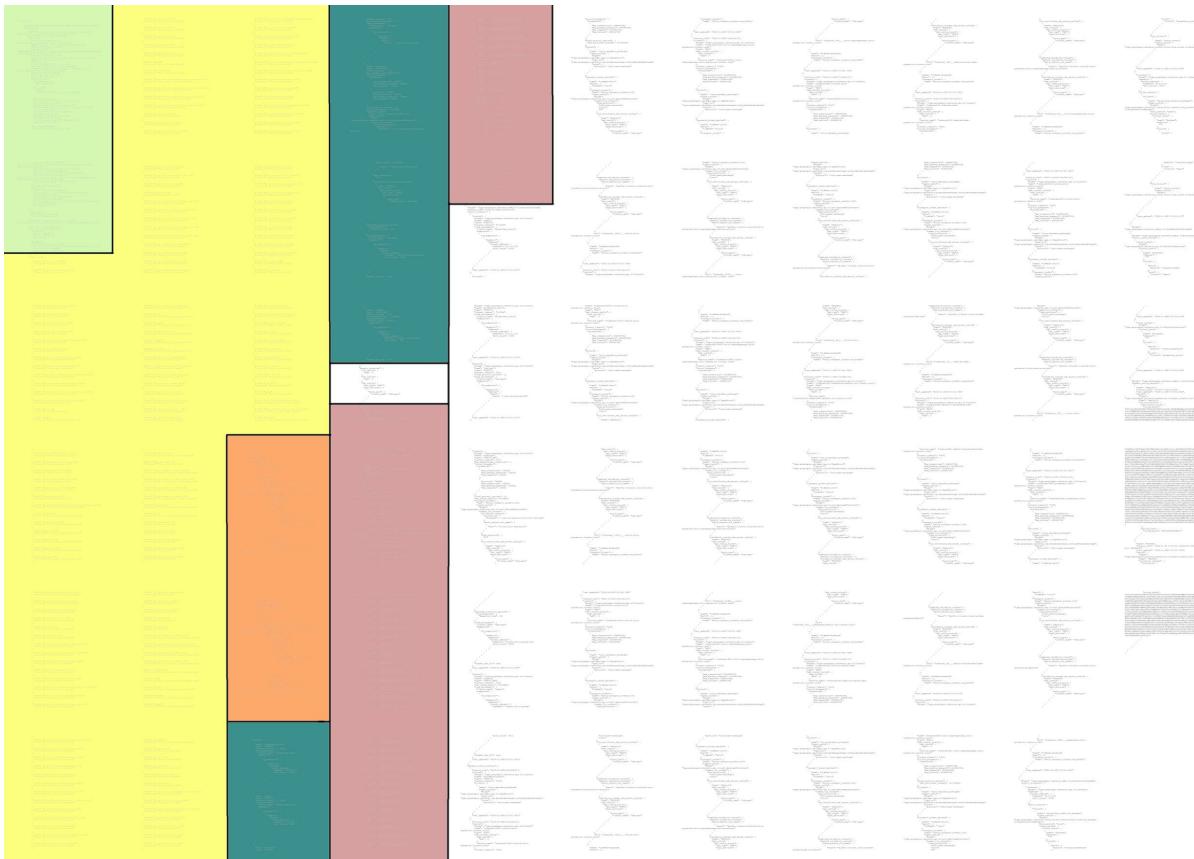
# envoy - config - bootstrap



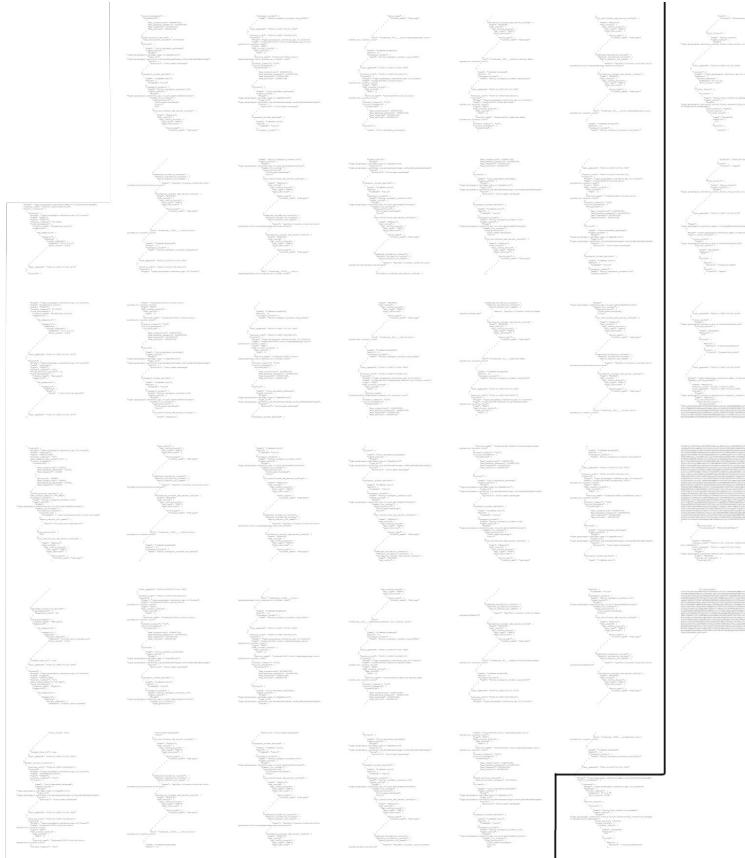
# envoy - config - bootstrap



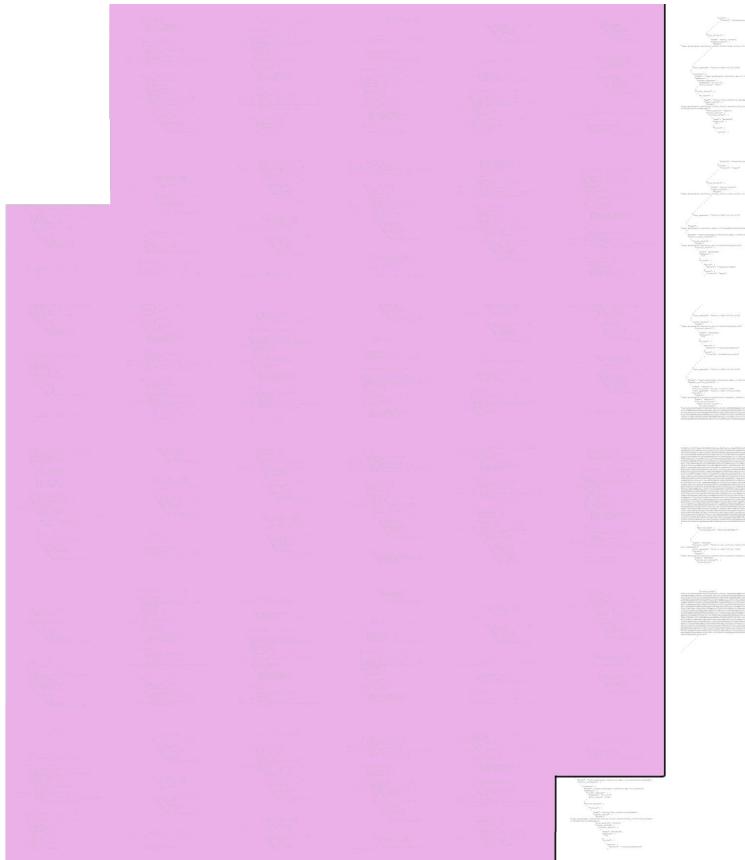
# envoy - config - bootstrap



# envoy - config



# envoy - config - clusters



# envoy - config



# envoy - config - listeners



# envoy - config - routes



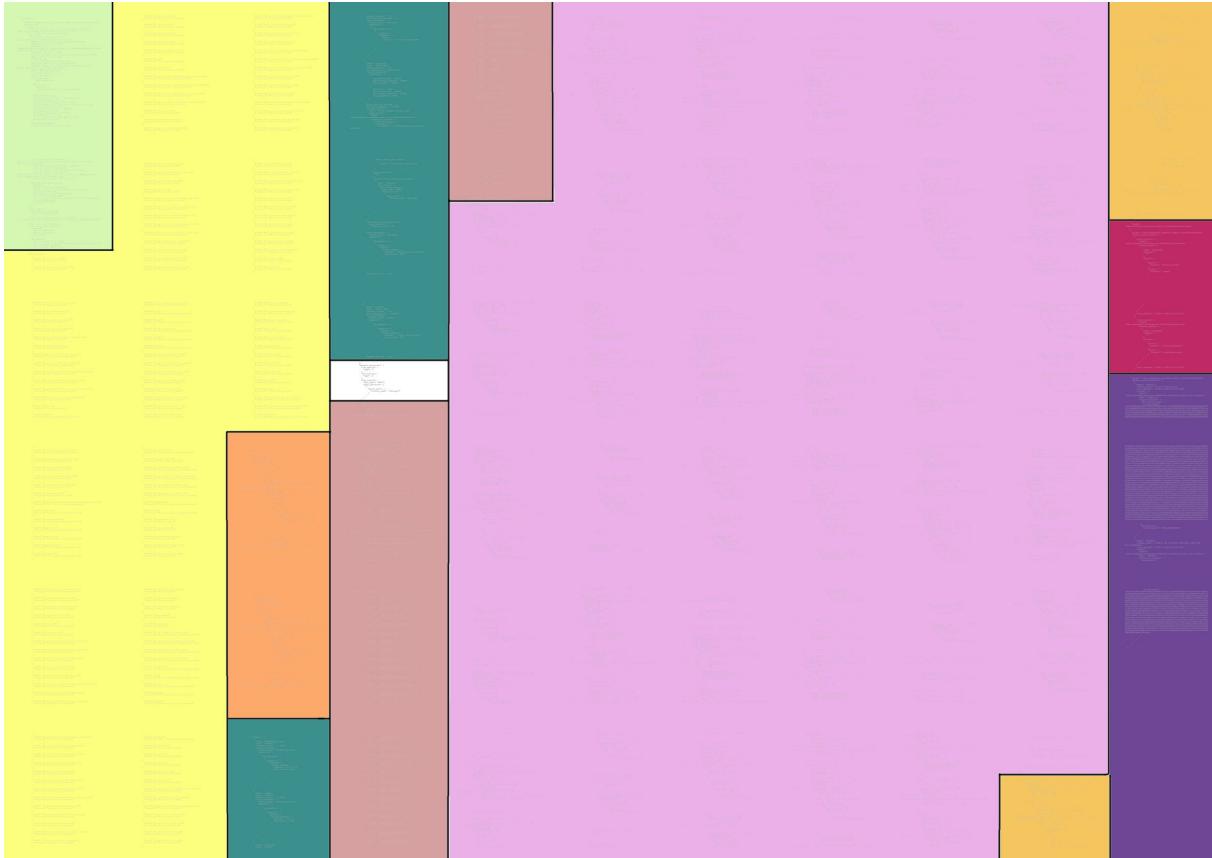
⋮



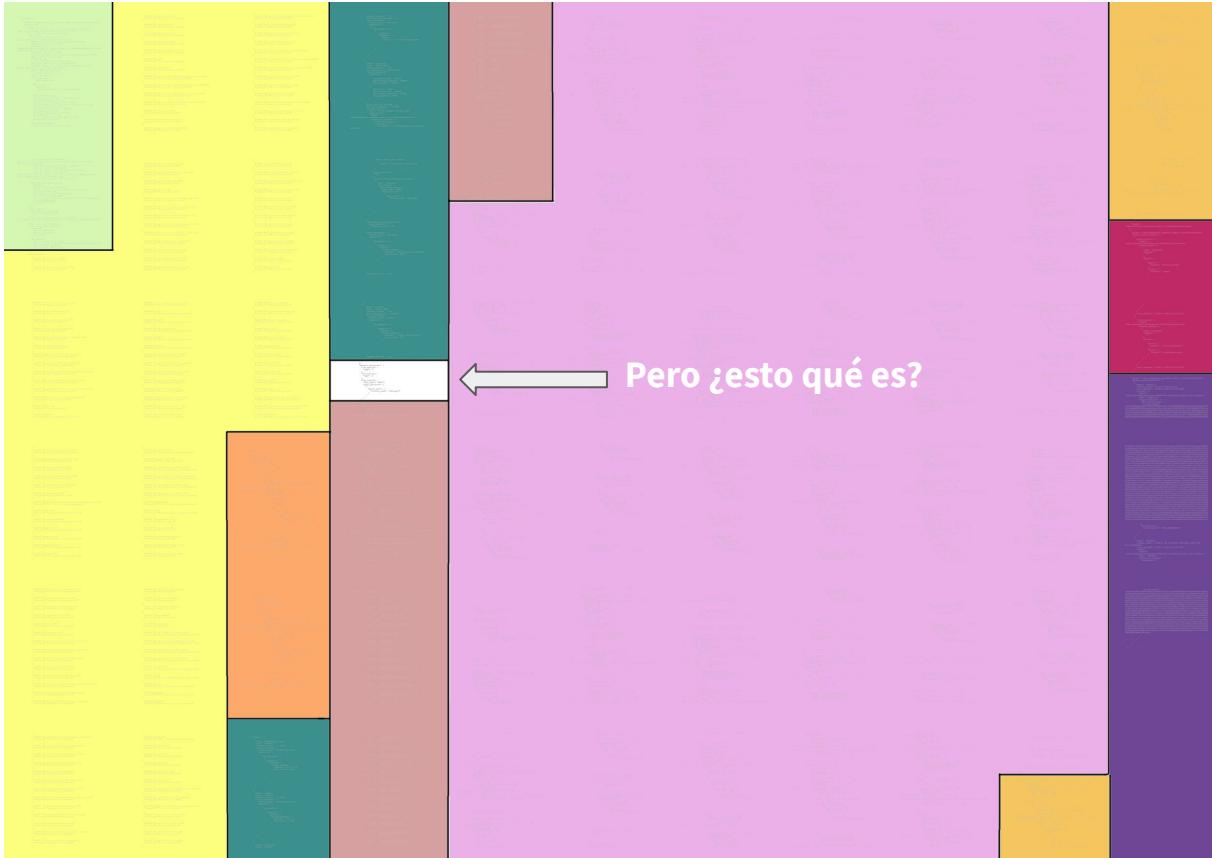
# envoy - config - secrets



# envoy - config



# envoy - config



# envoy - config



```
    "dynamic_resources": {
        "lds_config": {
            "ads": {}
        },
        "cds_config": {
            "ads": {}
        },
        "ads_config": {
            "api_type": "GRPC",
            "grpc_services": [
                {
                    "envoy_grpc": {
                        "cluster_name": "xds-grpc"
                    }
                }
            ],
            "ads": {}
        }
    }
```

# envoy - config

```

    ▼ "static_resources": {
        ▶ "listeners": [ ... ], // 2 items
        ▼ "clusters": [
            ▶ { ... }, // 4 items
            ▶ { ... }, // 4 items
            ▶ { ... }, // 5 items
            ▼ {
                "name": "xds-grpc",
                "type": "STRICT_DNS",
                "connect_timeout": "1s",
                "max_requests_per_connection": 1,
                ▶ "circuit_breakers": { ... }, // 1 item
                "http2_protocol_options": {},
                "dns_lookup_family": "V4_ONLY",
                ▶ "transport_socket": { ... }, // 2 items
                ▶ "upstream_connection_options": { ... }, // 1 item
                ▼ "load_assignment": {
                    "cluster_name": "xds-grpc",
                    ▼ "endpoints": [
                        ▼ {
                            ▼ "lb_endpoints": [
                                ▼ {
                                    ▼ "endpoint": {
                                        ▼ "address": {
                                            ▼ "socket_address": {
                                                "address": "istiod.istio-system.svc",
                                                "port_value": 15012
                                            }
                                        }
                                    }
                                ]
                            ]
                        }
                    ],
                    "respect_dns_ttl": true
                },
                ▶ { ... } // 6 items
            }
        ]
    }
}

```

[FIN, ACK]



Cuteness to soothe the spirit.

# Metadata

This document URL: <https://bit.ly/3pFMT78>

References include links to [Istio Community documents in gdrive](#). To access these documents you need to be a member of [this google group](#).

# Istio Acronyms

CR - Custom Resource - a specific instance of the defined spec

CRD - Custom Resource Definition - the spec for a Custom Resource

SD - Service Discovery

MX - Metadata Exchange - Istio specific Envoy extension providing “mixer like” attribute data without mixer

MCP - Mesh Configuration Protocol - how Istio components communicate

# Envoy Acronyms

FCM - Filter Chain Match

ALS - Access Log Service

xDS - x Discovery Service (like the x in DirectX)

- Current version as of writing is v3, v2 supported but deprecated
- CDS cluster discovery service
- LDS listener discovery service
- RDS route discovery service
- SDS secret discovery service
- There are a few other more obscure ones in here too

[UDPA - Universal Data Plane API \(XDS v4\)](#)

UDPA-TP - UDPA Transport Protocol

UDPA-DM - UPDA Data Model

ORCA - Open Request Cost Aggregation - load reporting

DPLB - Data Plane Load Balancer

- This appears to refer to xDS / UDPA clients, like Envoy itself

# Terminology

Upstream - where envoy sends requests to

Downstream - where envoy receives requests from

Management Server - xDS Server AKA control plane AKA istiod