



solo.io

# Hoot - Extending Istio with the EnvoyFilter CRD

Scott Weiss

Architect – Solo.io

## Istio provides the following OOTB:

- Service discovery / Load balancing
- Secure service-to-service communication (mTLS)
- Traffic control / shaping / shifting
- Policy / Intention based access control
- Traffic metric collection

# Istio provides the following OOTB:

- Service discovery / Load balancing **ServiceEntry + DestinationRule**
- Secure service-to-service communication (mTLS) **DestinationRule**
- Traffic control / shaping / shifting **VirtualService**
- Policy / Intention based access control **AuthorizationPolicy**
- Traffic metric collection **(built in)**

## Istio *does not* provide OOTB:

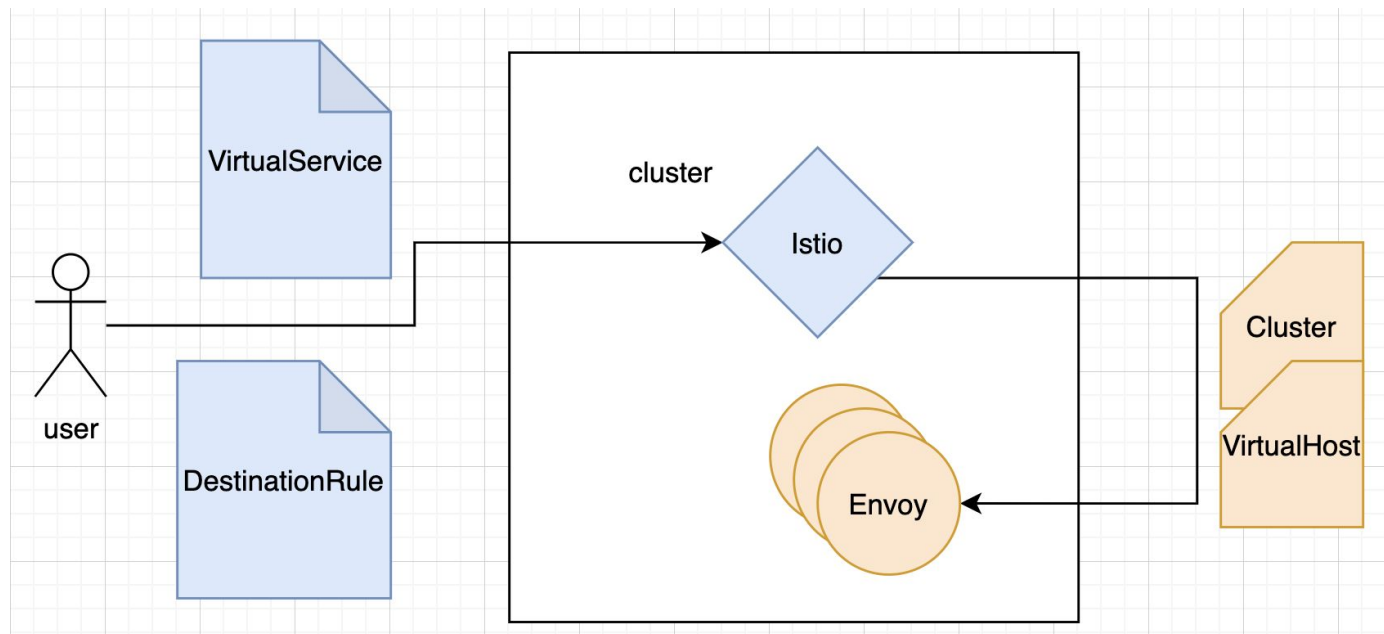
- Cross-cluster Networking **EnvoyFilter + ServiceEntry + Gateway**
- External Auth / Rate Limiting **EnvoyFilter**
- Traffic Failover **EnvoyFilter**
- WAMS Filters **EnvoyFilter**
- Access Logging / many unexposed Envoy features  
**EnvoyFilter + ?**

# What is the EnvoyFilter?

- Swiss Army Knife of customizing Istio Proxy (Envoy) configuration
- For when native Istio CRDs (VirtualService, DestinationRule) do not provide enough control over Envoy config

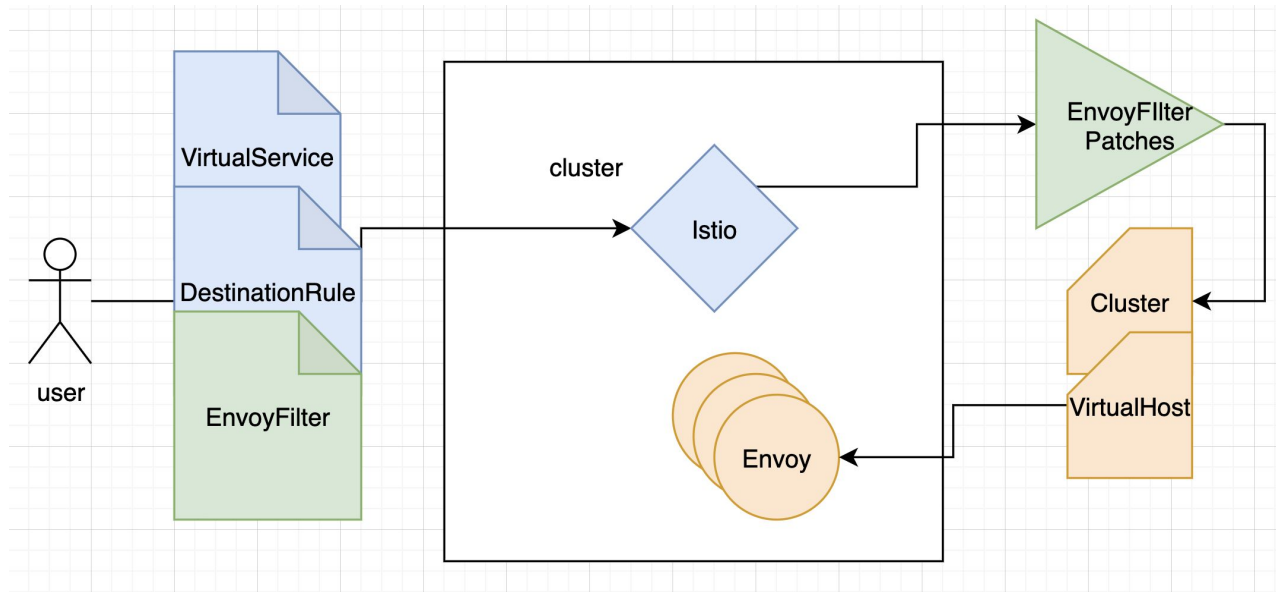
# Istio -> Envoy Config Architecture

Istio can be understood as a *translation engine*, translating high-level Istio CRDs into low-level Envoy config resources.



# Istio -> Envoy Config Architecture + *EnvoyFilter*

The EnvoyFilter CRD exposes an opaque Patching mechanism for customizing Envoy configuration beyond what Istio exposes natively.



# Istio -> Envoy Config Example

```
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: reviews-route
  namespace: bookinfo
spec:
  hosts:
  - reviews.bookinfo.svc.cluster.local
  http:
  - name: "reviews-v2-routes"
    match:
    - uri:
        prefix: "/"
    route:
    - destination:
        host: reviews.bookinfo.svc.cluster.local
        subset: v2
```

```
{
  "name": "reviews-v2-routes",
  "match": {
    "prefix": "/",
    "caseSensitive": true
  },
  "route": {
    "cluster": "outbound|80|v2|reviews.bookinfo.svc.cluster.local",
    ...
  }
}
```



# Istio -> Envoy Config Example + EnvoyFilter

```
# auth example
apiVersion: networking.istio.io/v1alpha3
kind: EnvoyFilter
metadata:
  name: reviews-external-auth
  namespace: istio-system
spec:
  configPatches:
    - applyTo: HTTP_ROUTE
      match :
        context: SIDECAR_OUTBOUND
        vhost:
          route:
            name: "reviews-v2-routes"
            action: "ROUTE"
      patch:
        operation: MERGE
        value:
          route:
            typed_per_filter_config:
              envoy.ext_authz:
                '@type': type.googleapis.com/envoy.config.filter.http.ext_authz.v2.ExtAuthzPerRoute
            check_settings:
              context_extensions:
                config_id: custom-ext-auth
```

# Istio -> Envoy Config Example + EnvoyFilter

```
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: reviews-route
  namespace: bookinfo
spec:
  ...
```

```
apiVersion: networking.istio.io/v1alpha3
kind: EnvoyFilter
metadata:
  name: reviews-external-auth
  namespace: bookinfo
spec:
  ...
```

```
{
  "name": "reviews-v2-routes",
  "match": {
    "prefix": "/",
    "caseSensitive": true
  },
  "route": {
    "cluster": "outbound|80|v2|reviews.bookinfo.svc.cluster.local",
  },
  "typedPerFilterConfig": {
    "envoy.ext_authz": {
      "@type": "type.googleapis.com/envoy.config.filter.http.ext_authz.v2.ExtAuthzPerRoute",
      "checkSettings": {
        "contextExtensions": {
          "config_id": "default.dev"
        }
      }
    }
  }
}
```

# Istio -> Envoy Config Demo