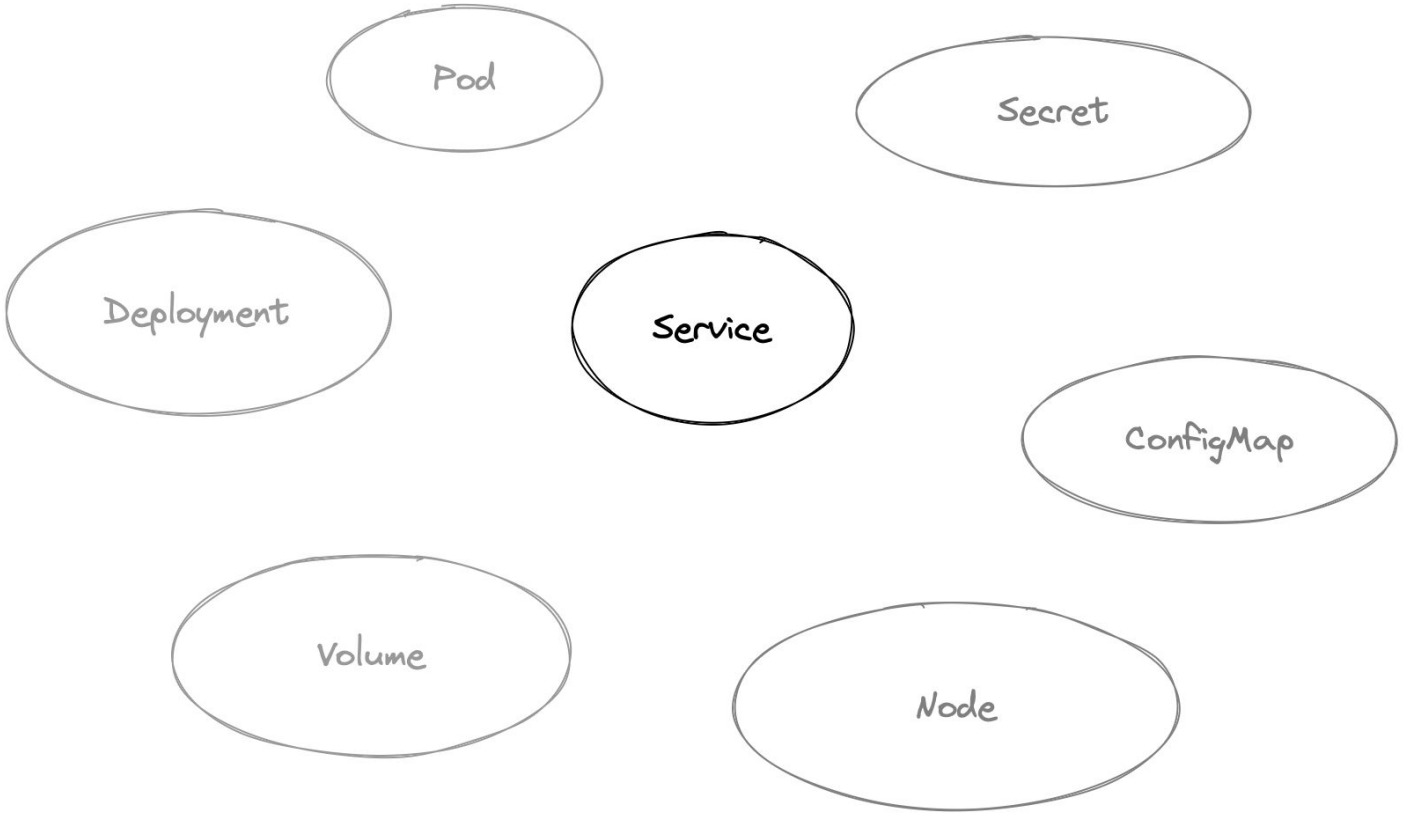
KubeCon
CloudNativeCon
Europe 2023
TiKV

Developing a Mental Model of Istio: From Kubernetes to Sidecars to Ambient

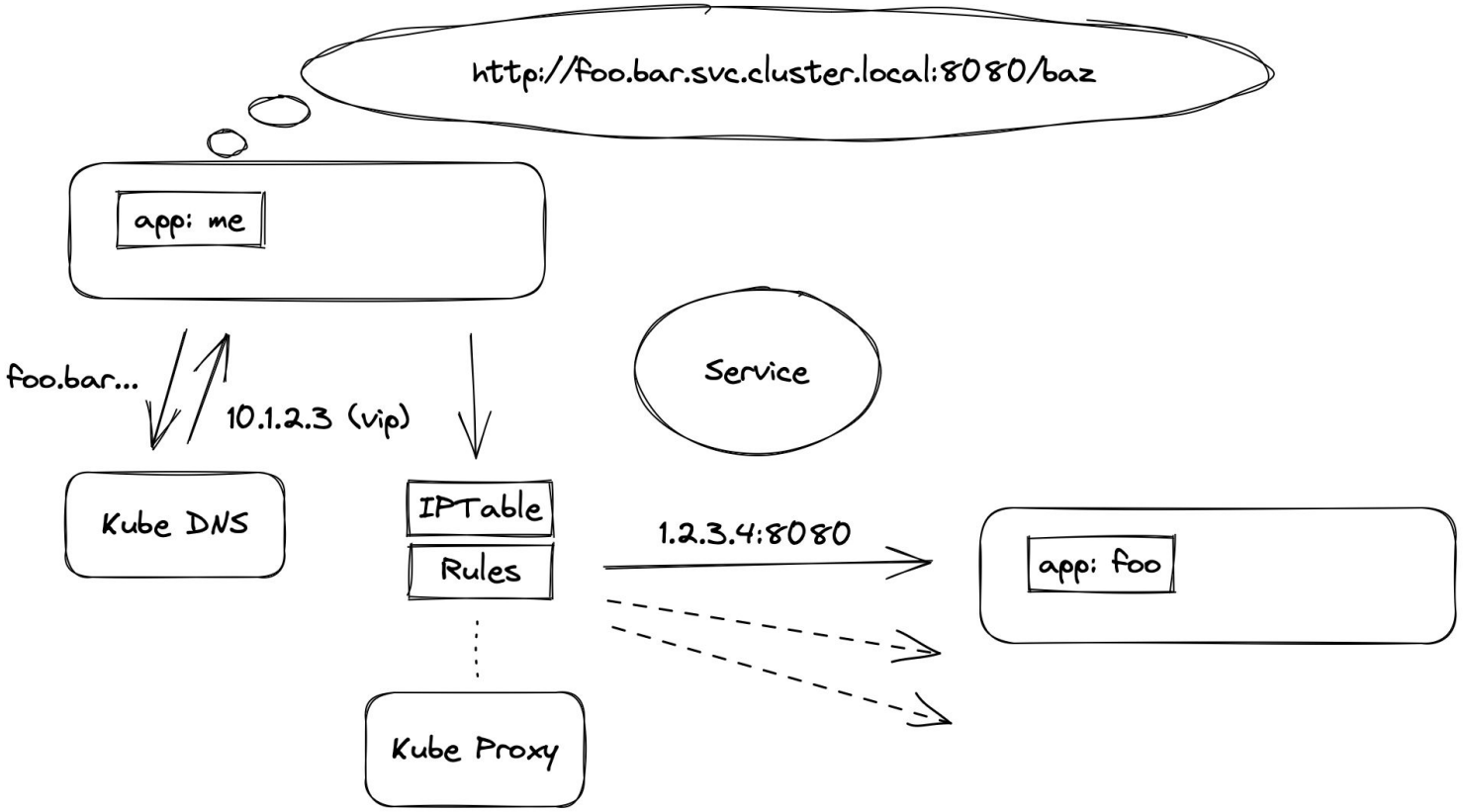
Aaron Birkland & Nina Polshakova

solo.io

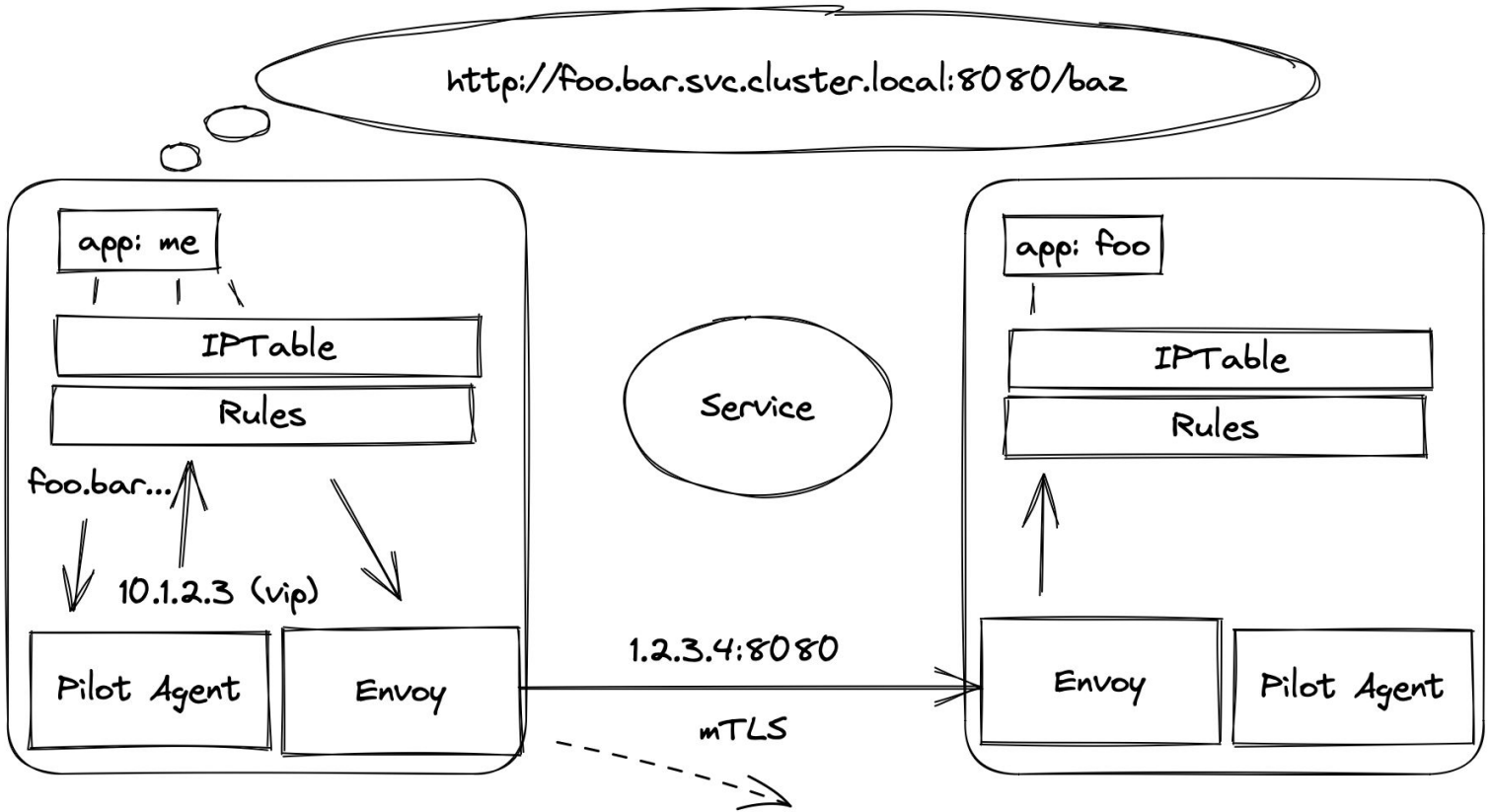
Abstractions



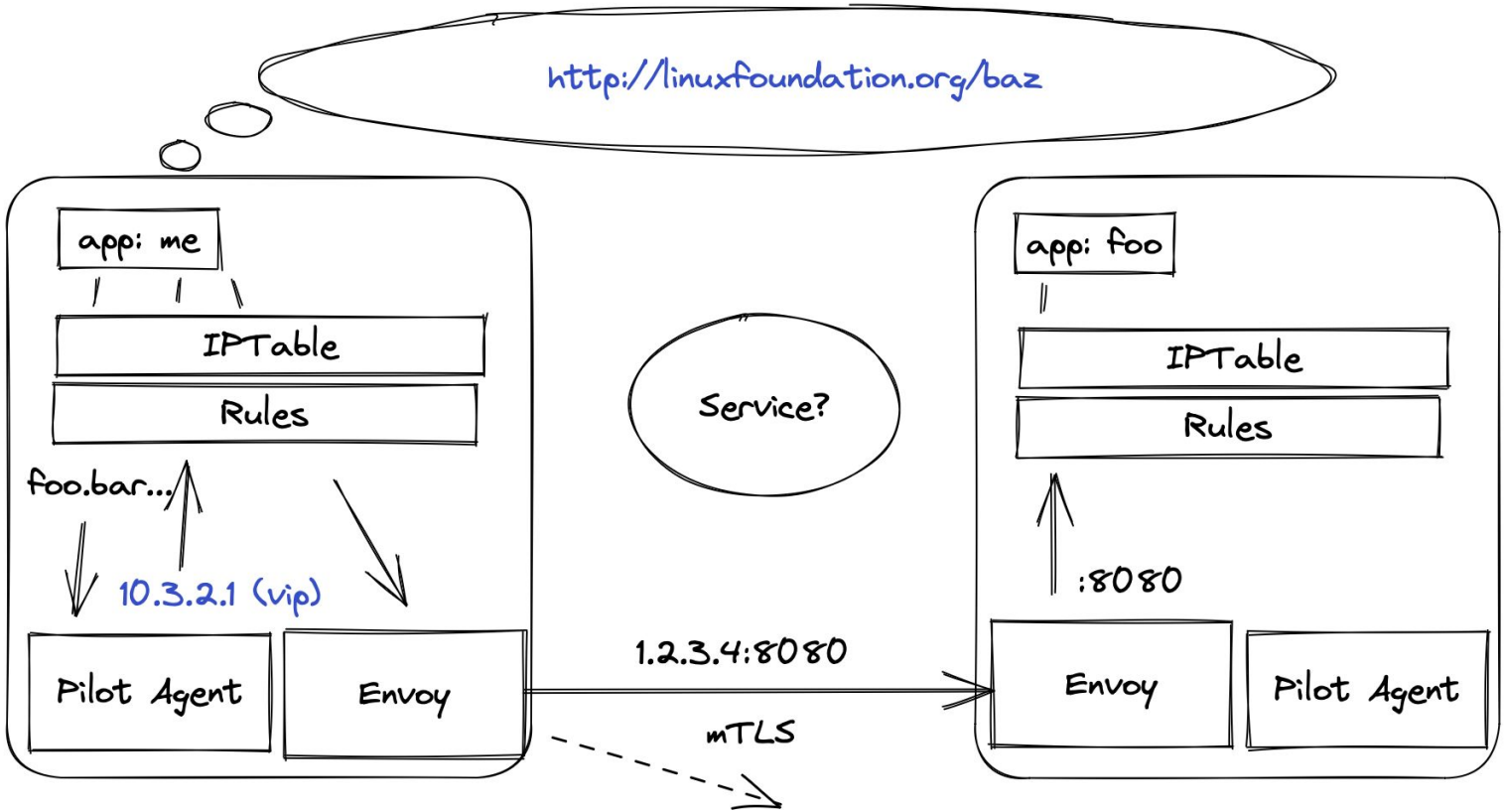
Implementing Abstractions



Implementing Abstractions Differently



Implementing Different Abstractions



Foundations of an Istio API

Client/Consumer sidecar

VirtualService

- Policies that affect traffic routing

DestinationRule

- Policies that occur after routing decisions have been made

ServiceEntry

- Explicitly describe properties of a service (DNS names, VIPs, endpoints, ports, protocols)

Server/Producer sidecar

PeerAuthentication

- Connection security (mTLS) authentication requirements

AuthorizationPolicy

- Access Control

RequestAuthentication

- User-space authentication requirements

Istio - Ambient Layers

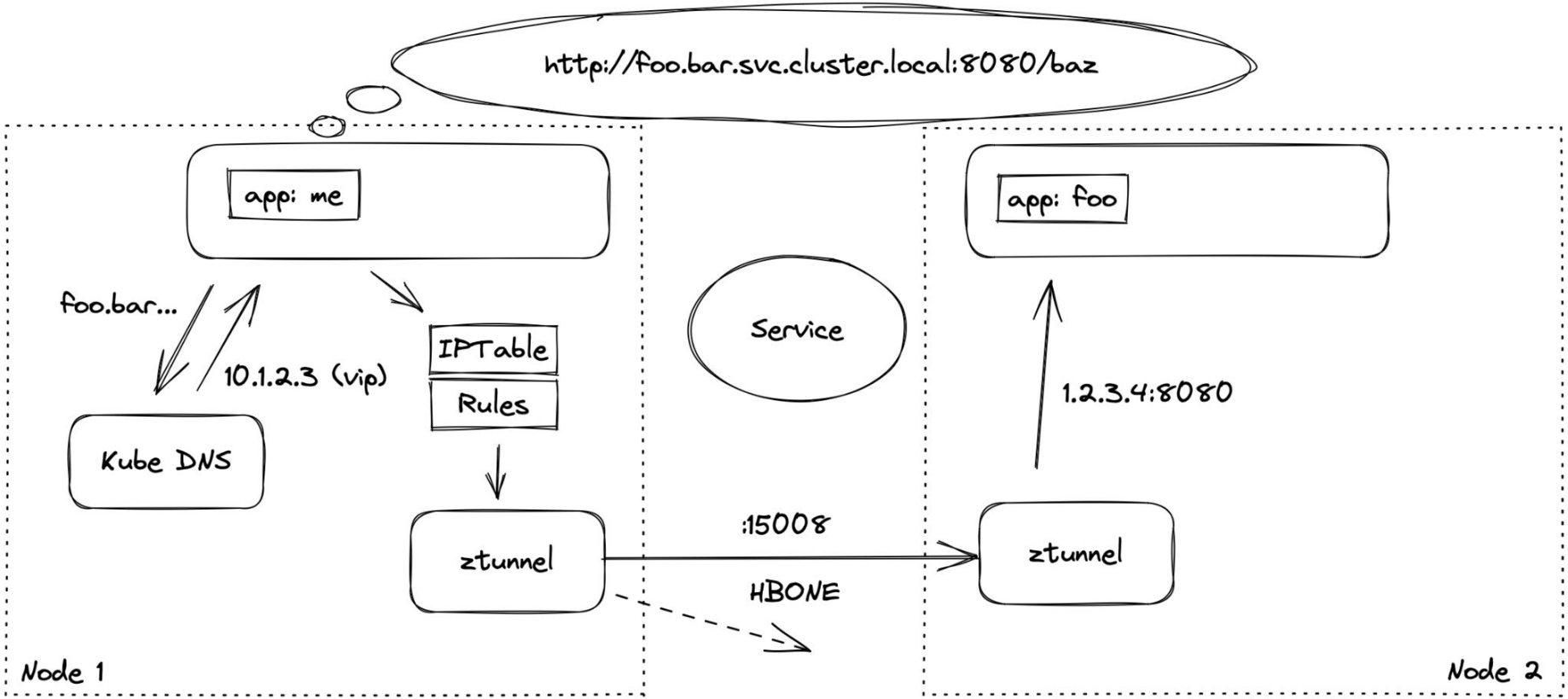
L7 Layer Processing
(Waypoint)

- Traffic Management: HTTP routing, header manipulation,
  rate limiting, fault injection, load balancing, circuit breaking, retries, timouts, etc.
- Security: L7 Authorization policies
- Observability: HTTP metrics, Access logging, tracing

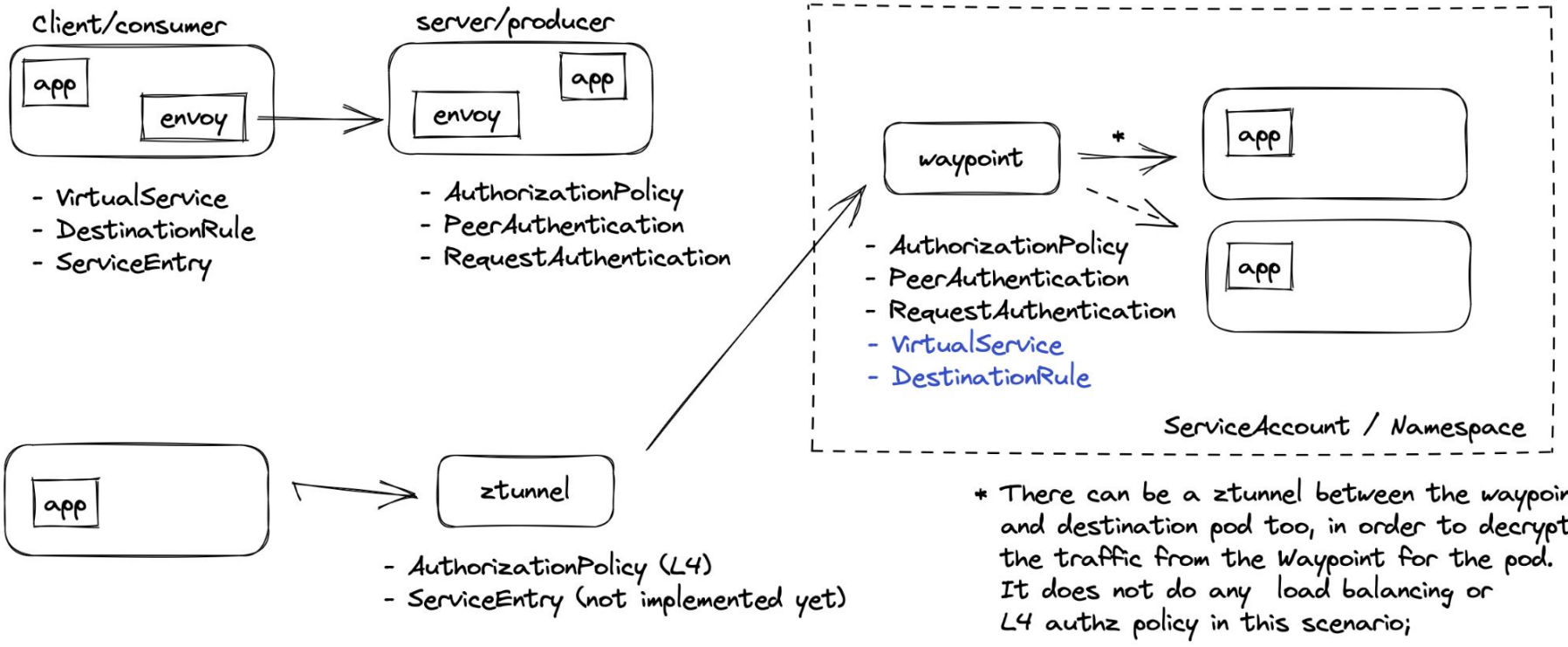
Secure Overlay Layer
(ztunnel)

- Traffic Management: TCP Routing
- Security: mTLS tunneling, Simple auth policy
- Observability: TCP metrics, logging

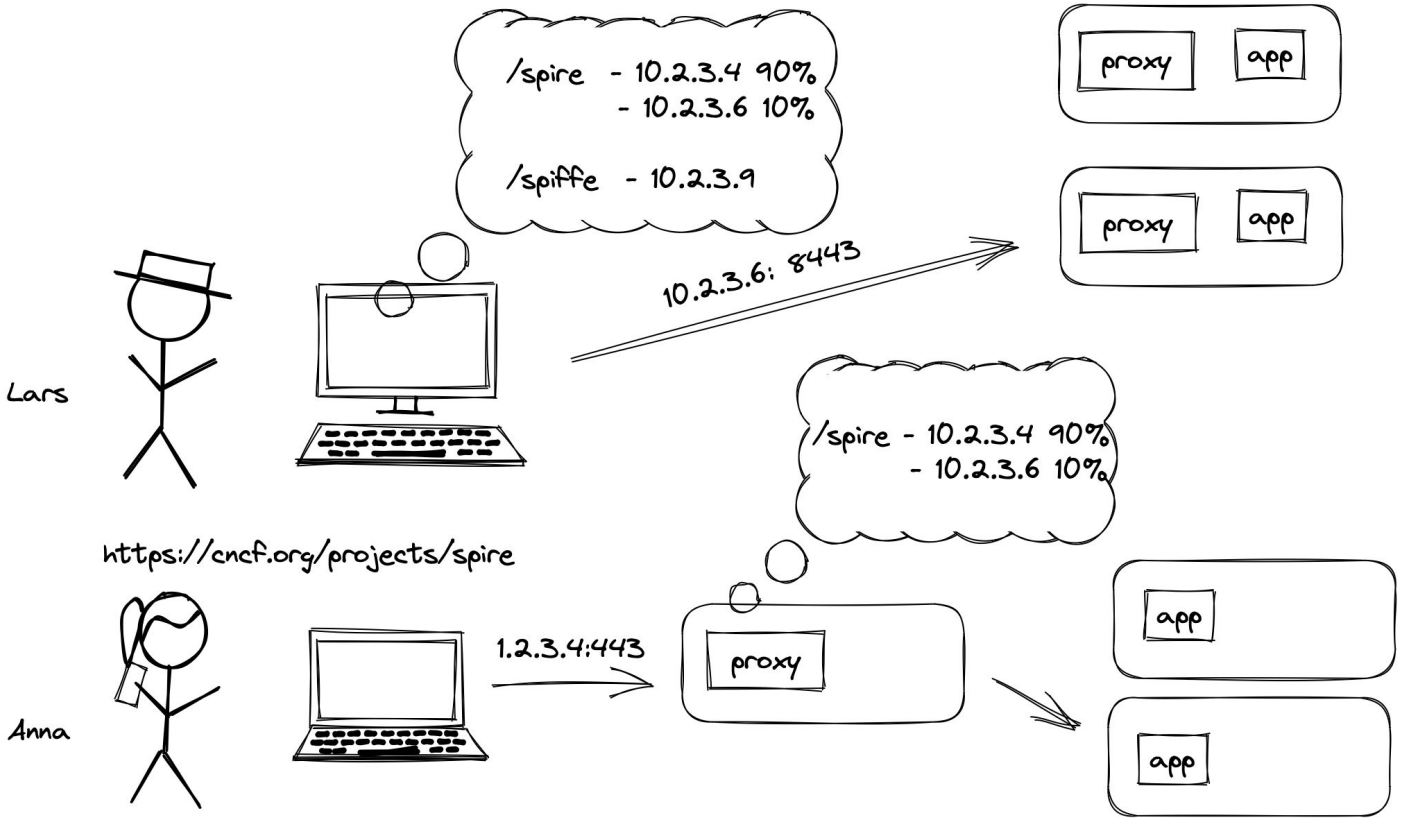
Implementing Abstractions Differently?



Implementing an API differently



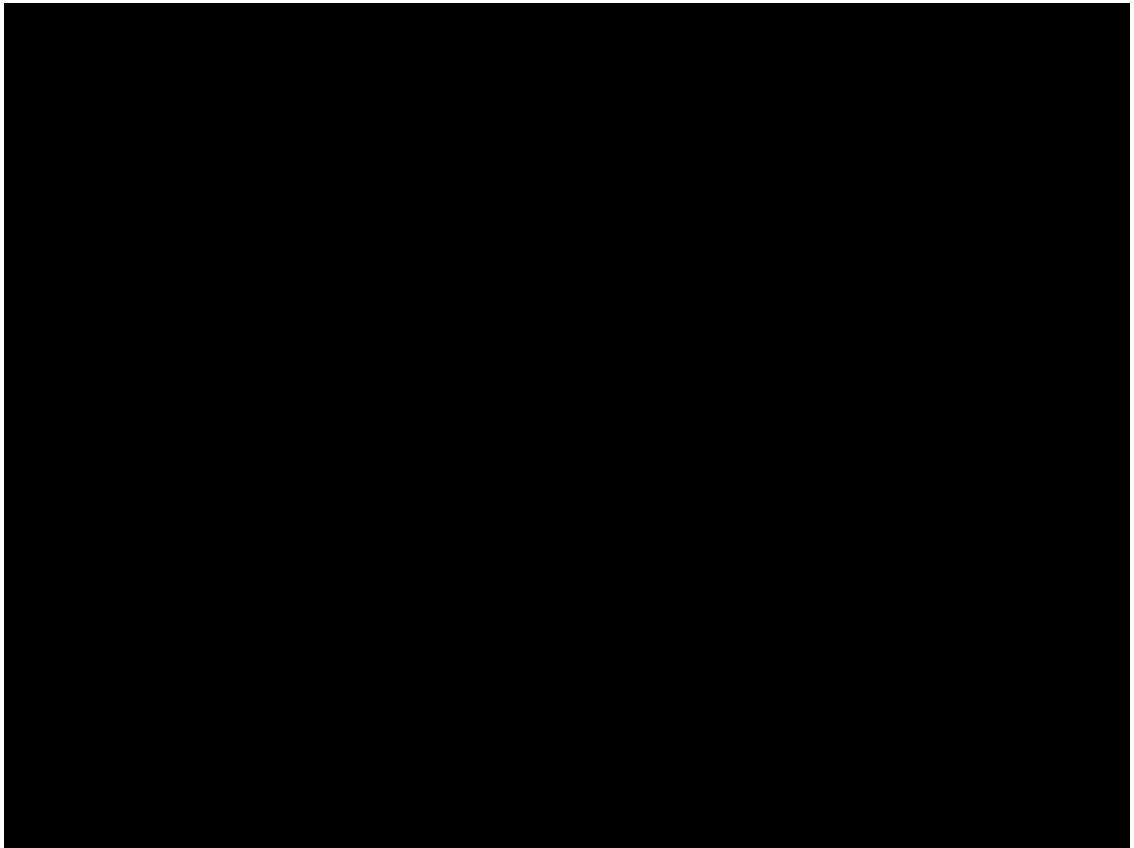
An analogy


/spire - 10.2.3.4 90%
- 10.2.3.6 10%
/spiffe - 10.2.3.9
proxy
app
proxy
app
10.2.3.6: 8443
Lars
/spire - 10.2.3.4 90%
- 10.2.3.6 10%
https://cncf.org/projects/spire
1.2.3.4:443
proxy
app
app
Anna

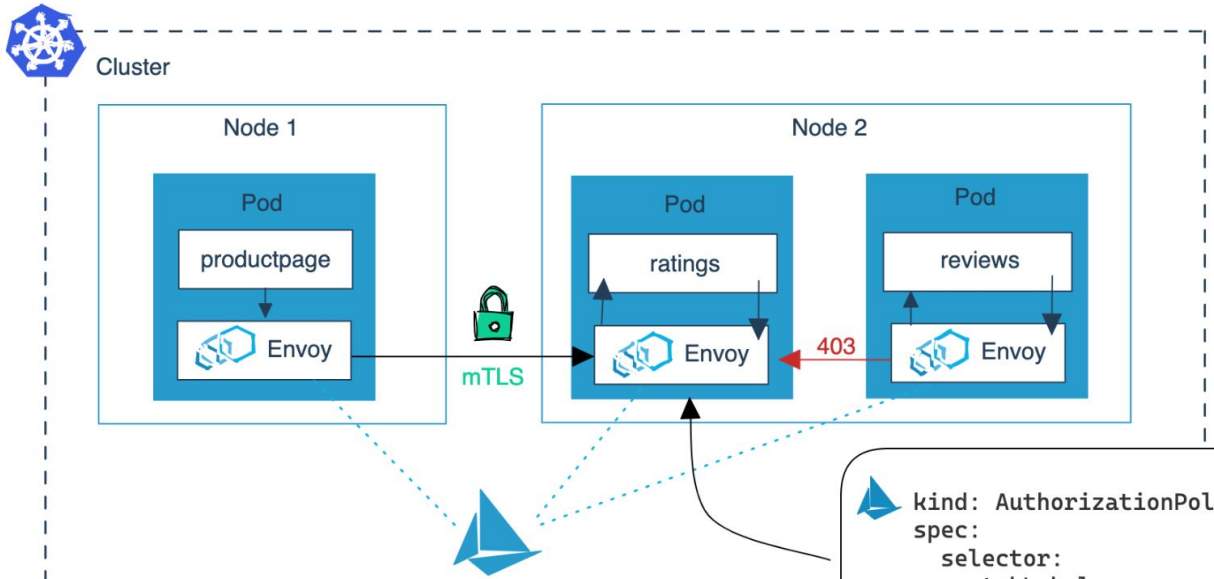
Demo Time!

Demo

https://github.com/npolshakova/ambient-examples

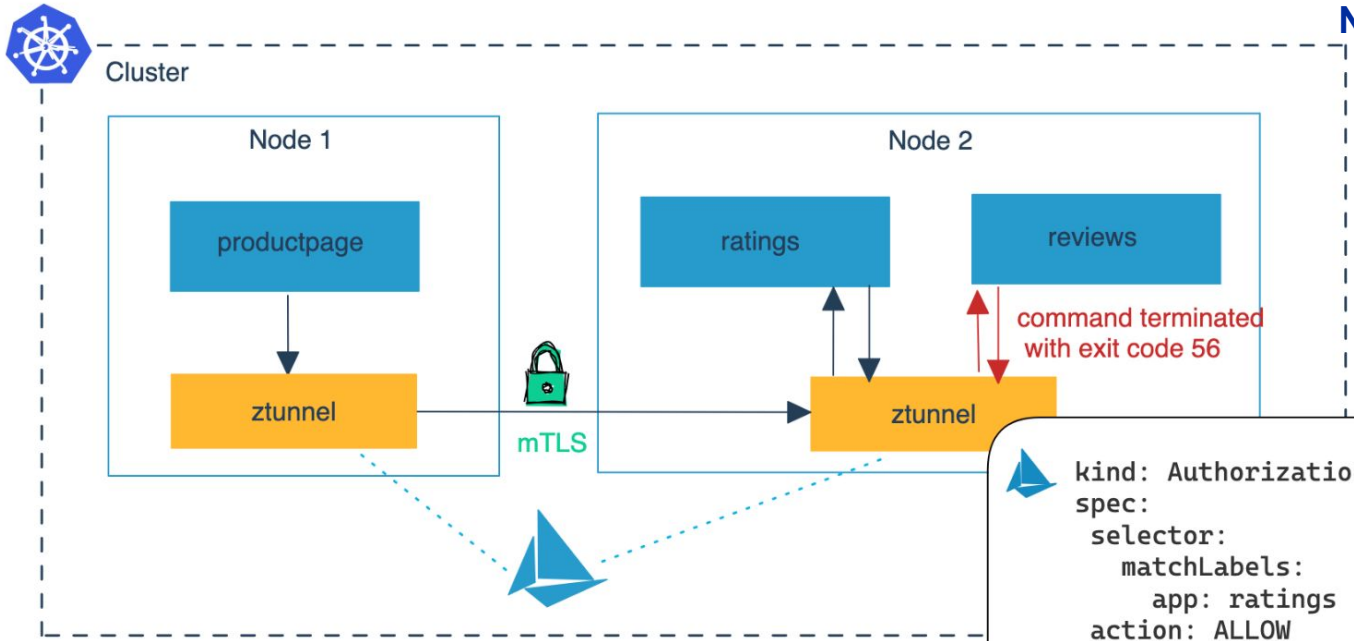


Example - Sidecar AuthorizationPolicy




```
kind: AuthorizationPolicy
spec:
  selector:
    matchLabels:
      istio.io/gateway-name: bookinfo-ratings
  action: ALLOW
  rules:
  - from:
    - source:
        principals:
        - cluster.local/ns/bookinfo/sa/productpage
    to:
    - operation:
        methods: ["GET"]
```

Example - Ambient L4 AuthorizationPolicy

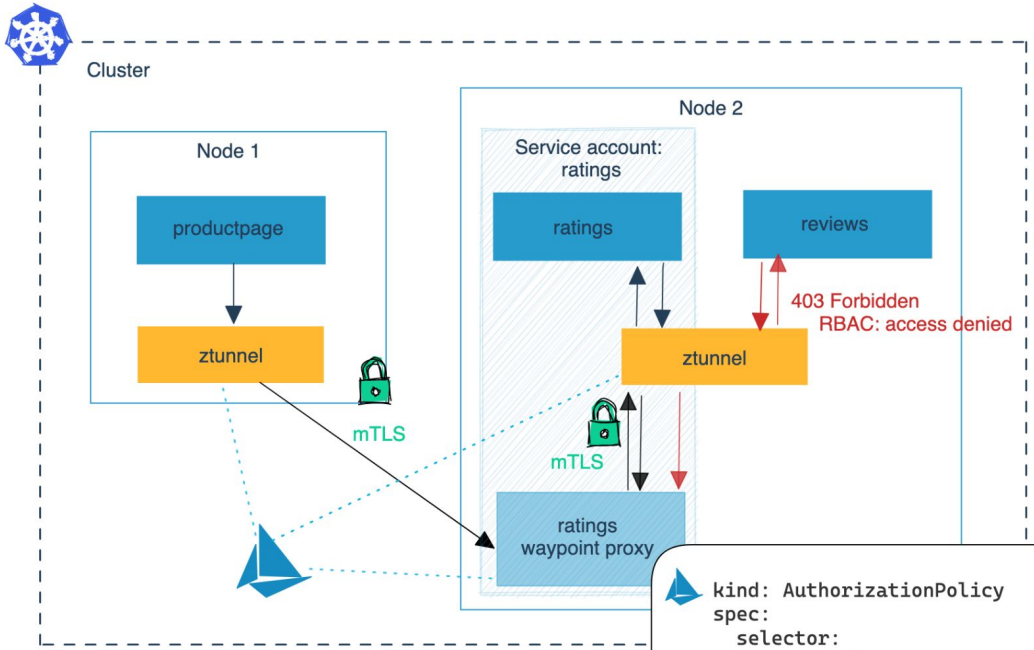


Notes:

- Same API
- Response on DENY
- Limit to L4 rules

```
kind: AuthorizationPolicy
spec:
 selector:
   matchLabels:
     app: ratings
 action: ALLOW
 rules:
 - from:
   - source:
       principals:
       - cluster.local/ns/bookinfo/sa/productpage
```

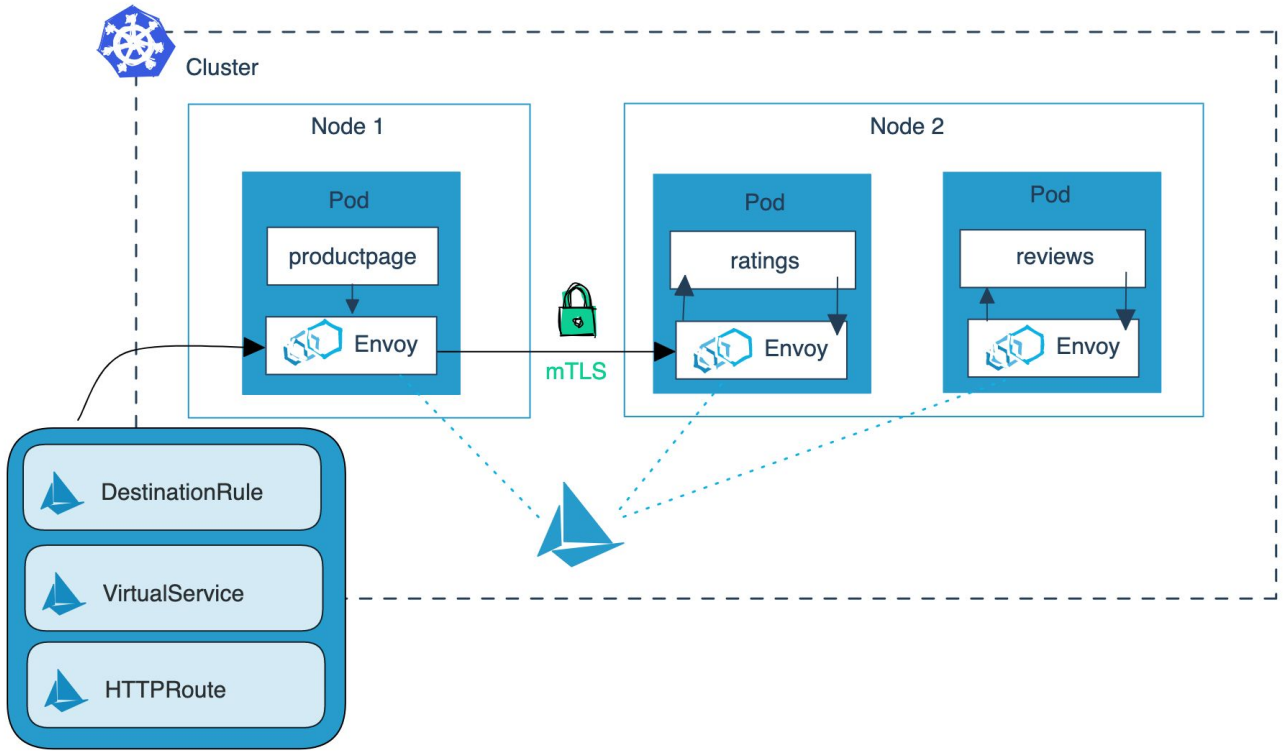
Example - Ambient L7 AuthorizationPolicy



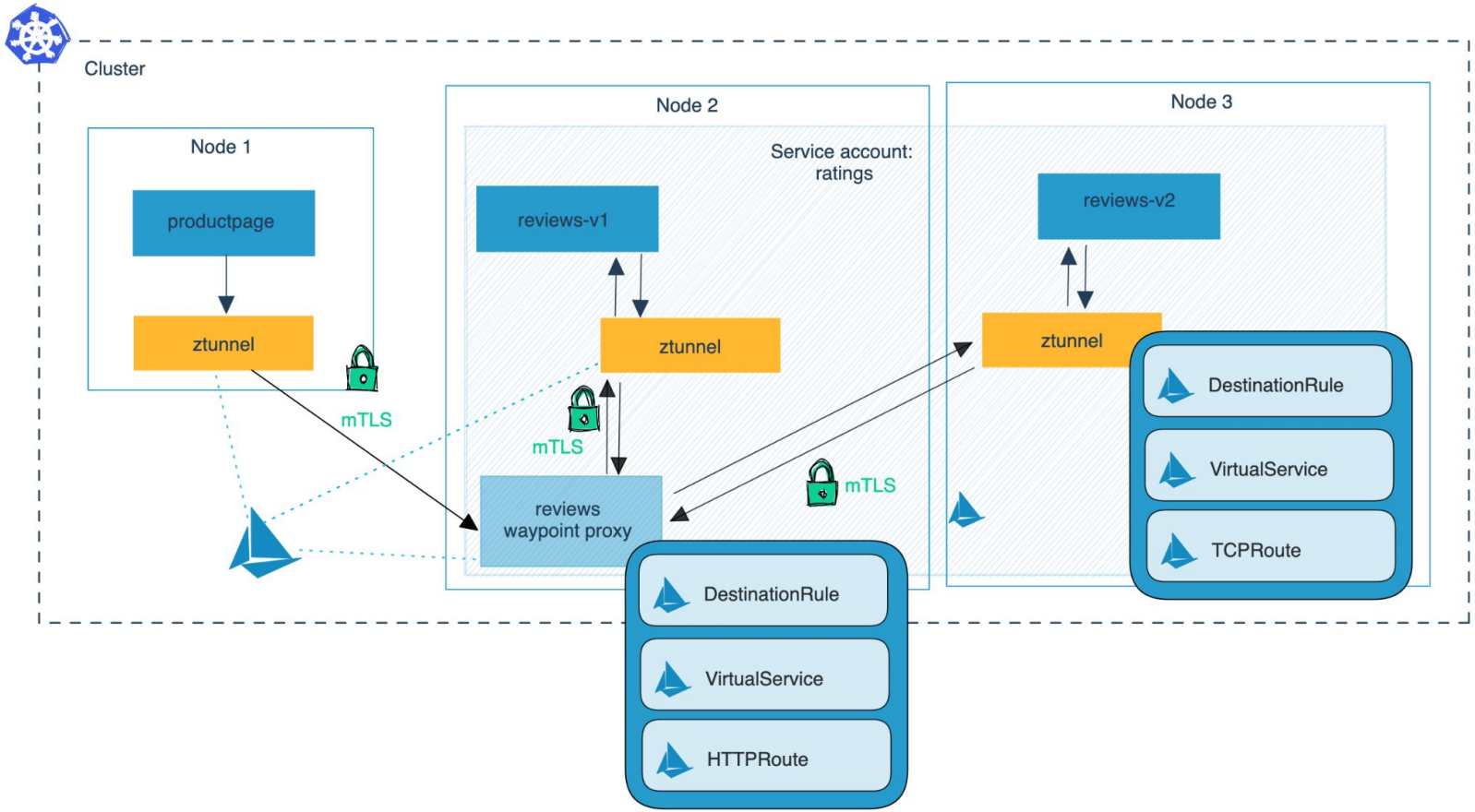

```
kind: AuthorizationPolicy
spec:
  selector:
   matchLabels:
     istio.io/gateway-name: bookinfo-ratings
 action: ALLOW
 rules:
 - from:
   - source:
       principals:
       - cluster.local/ns/bookinfo/sa/productpage
   to:
   - operation:
       methods: ["GET"]
```

Example - Sidecar Routing

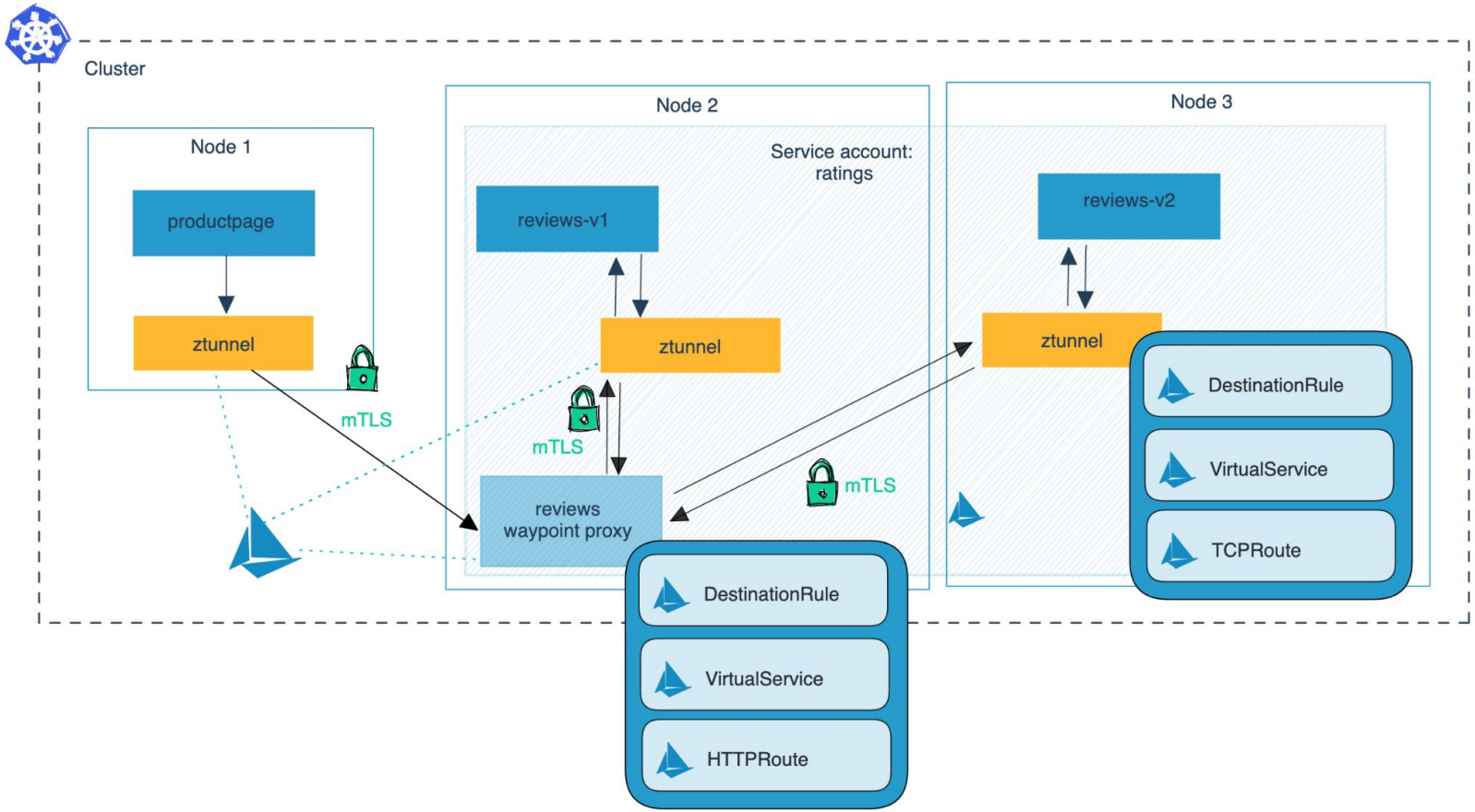
- VirtualService
  - Gateway API: HTTPRoute (L7) or TCPRoute (L4)
- Client side



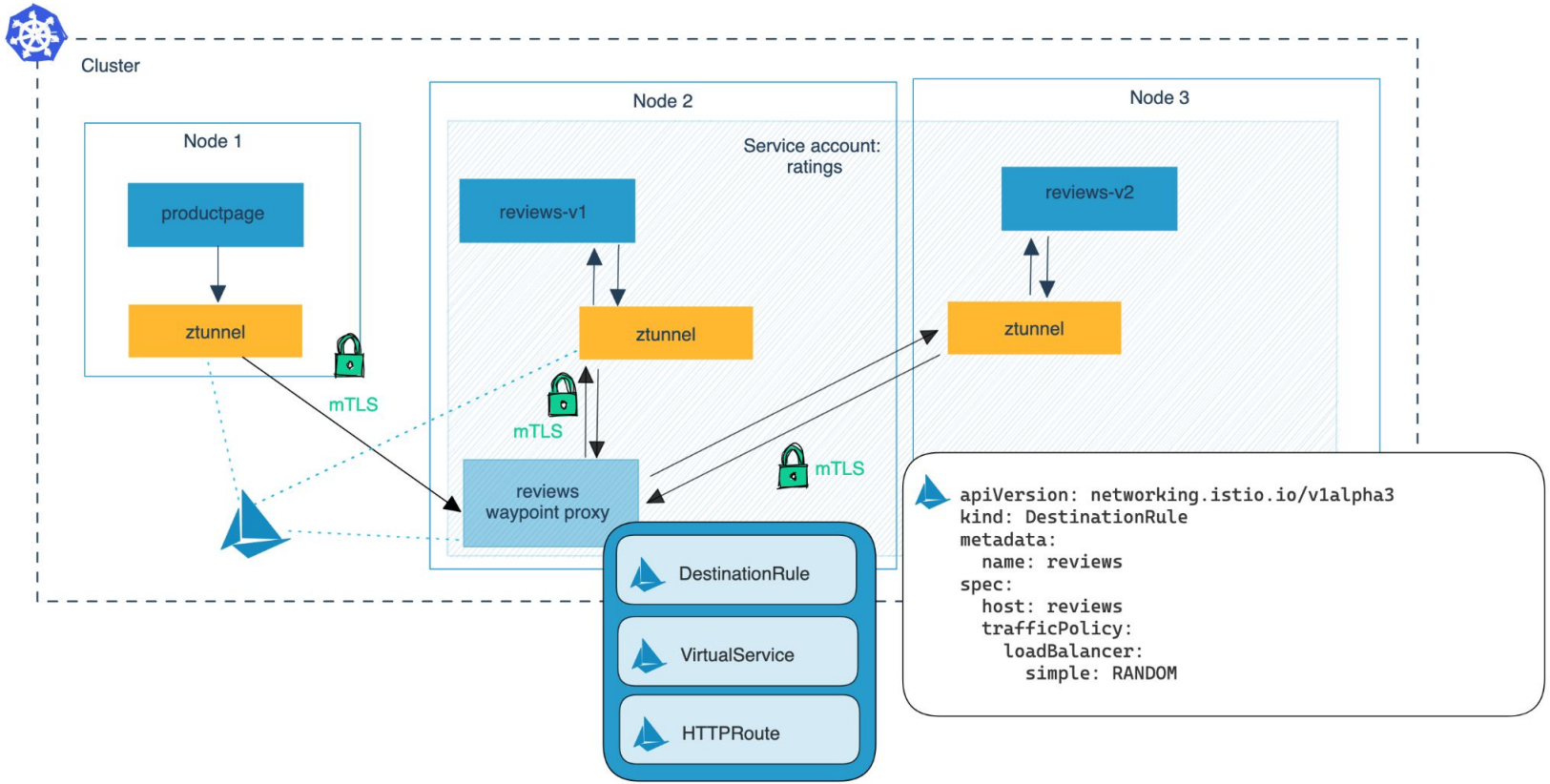
Example - Ambient Routing



Example - Ambient Policy



Example - Ambient Traffic Shift



Resources

- Getting Started with Ambient

- Come to the Panel and ask questions!
  - (Friday April 21, 16:00 CEST): *Future of Service Mesh - Sidecar or Sidecarless or Proxyless?*

Please scan the QR Code above
to leave feedback on this session