KubeCon | CloudNativeCon

North America 2024

KubeCon CloudNativeCon

North America 2024

Life of a Packet

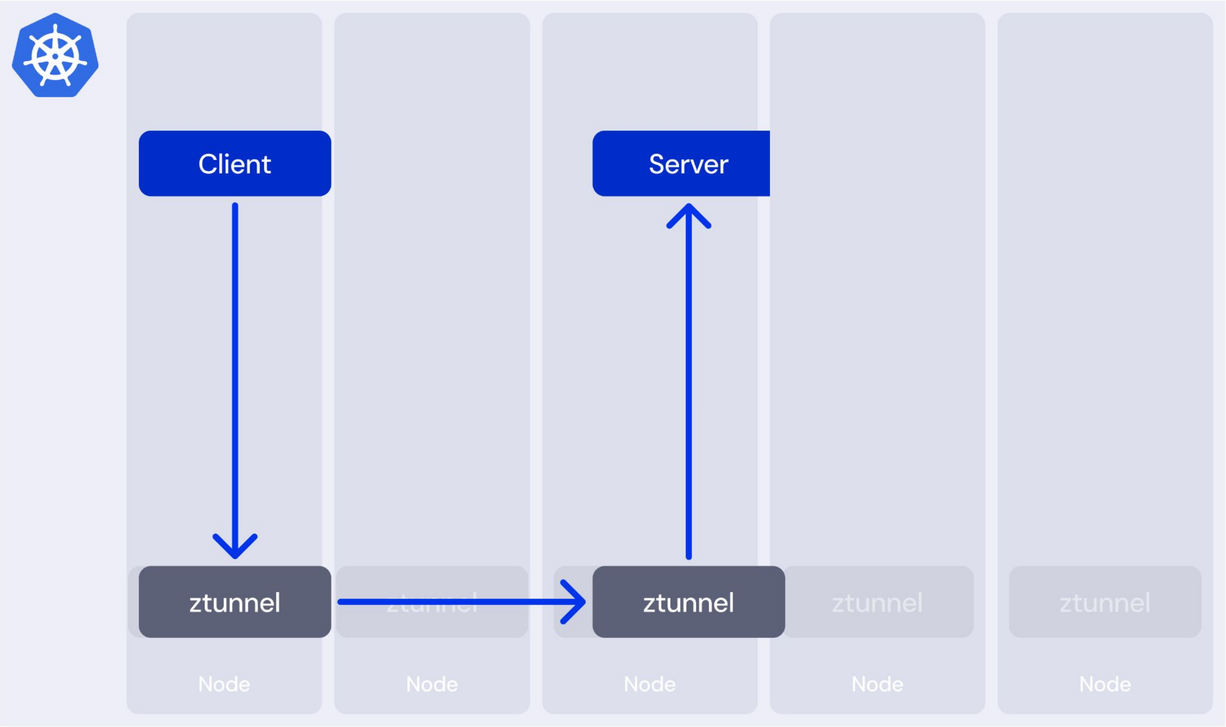
Ambient Edition

John Howard (Solo.io), Keith Mattix (Microsoft)

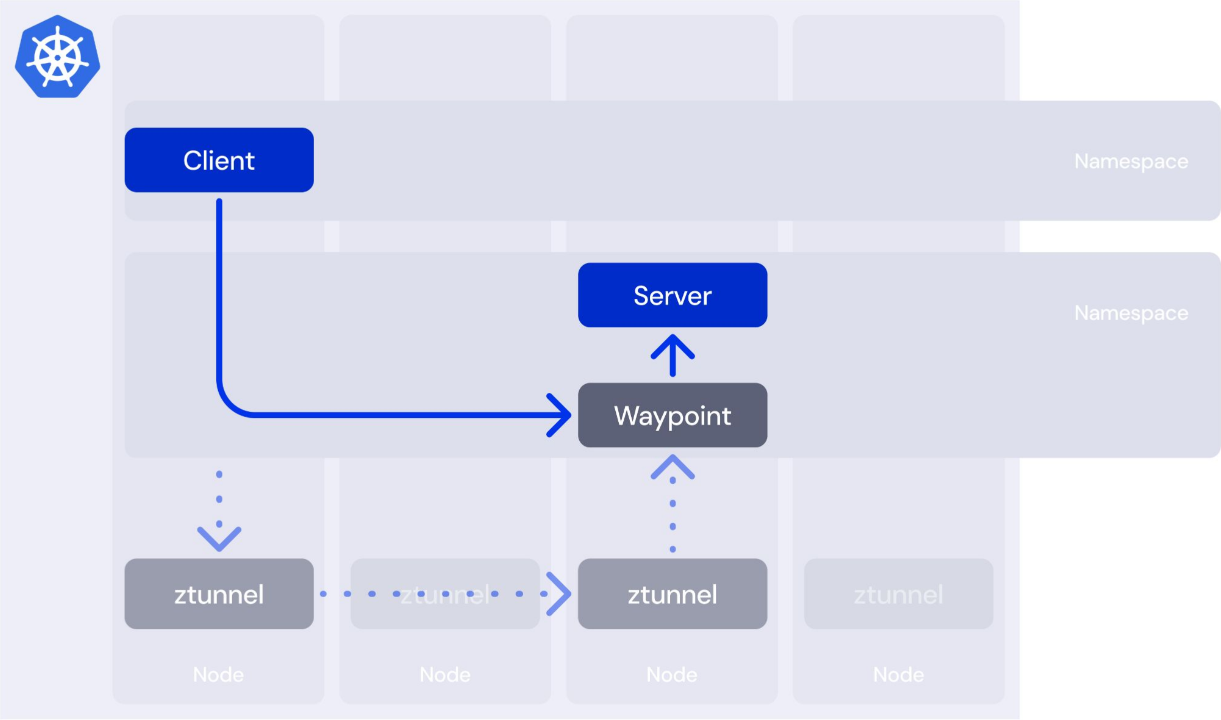
Overview

- Architecture Overview
- How outbound traffic gets to Ztunnel
    - IPtables redirection
    - Aside: How ipod works
        - CNI plugin
        - Dynamic onboarding
- How Ztunnel picks a destination
    - WDS, etc
- HBONE
- How Ztunnel accepts traffic: HBONE and plaintext
- Waypoints

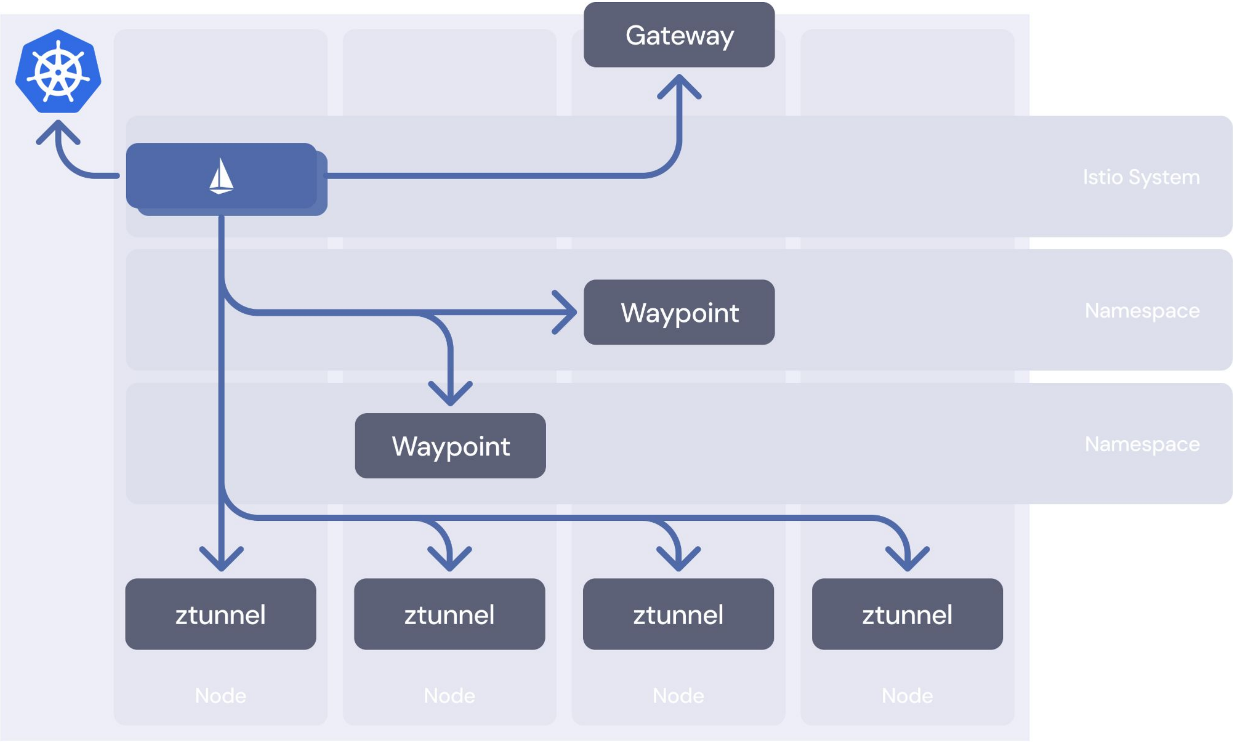
Architecture Overview



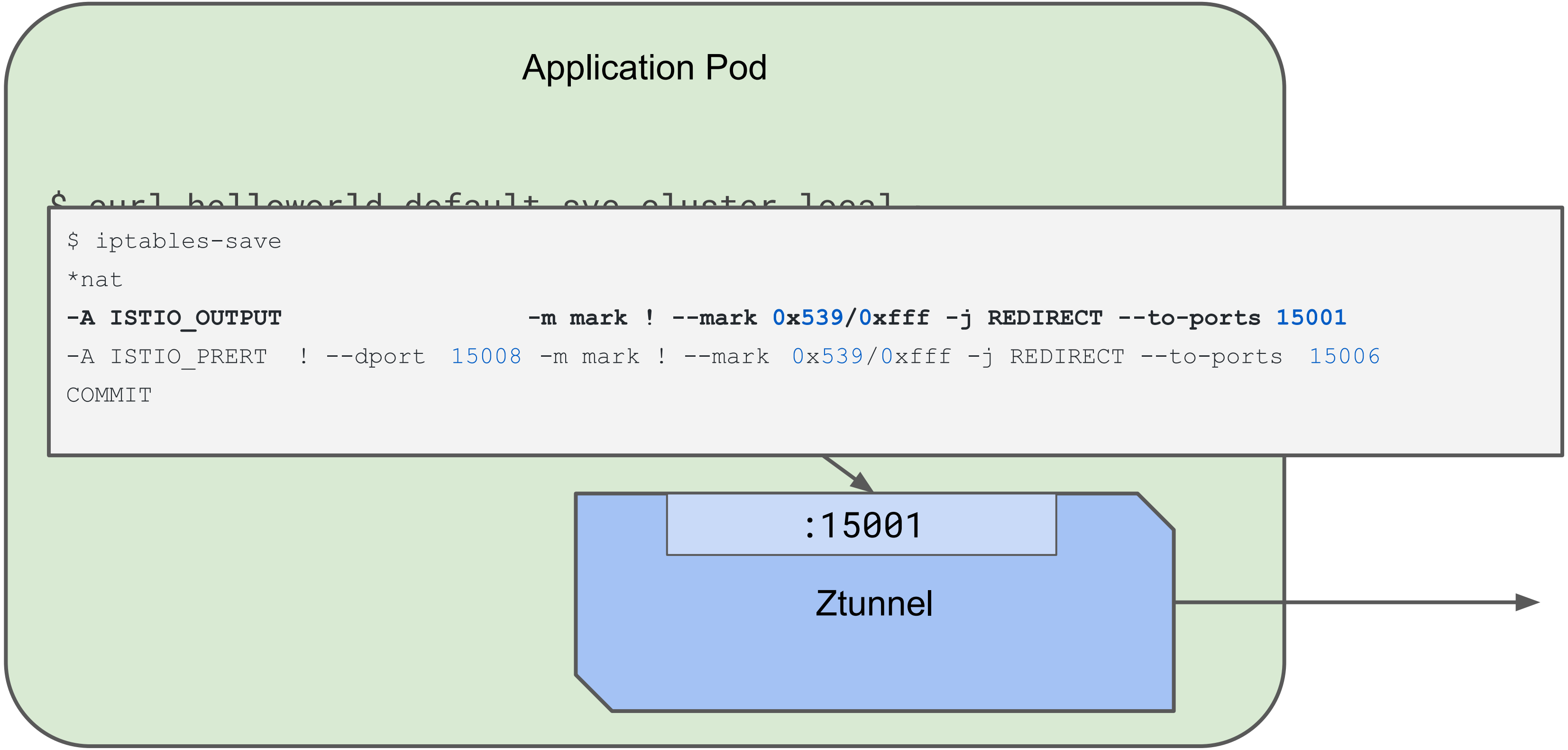
Architecture Overview



Architecture Overview



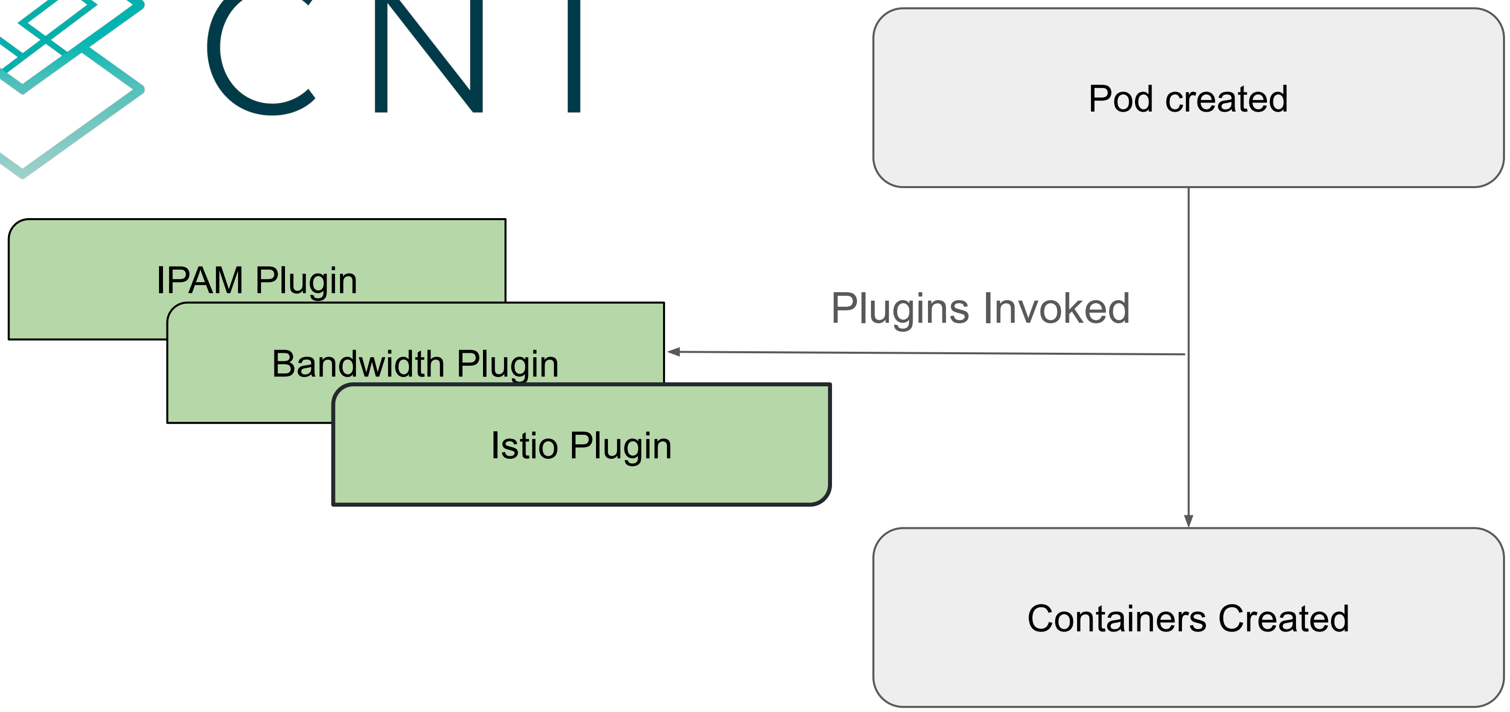
The beginning: getting traffic to Ztunnel



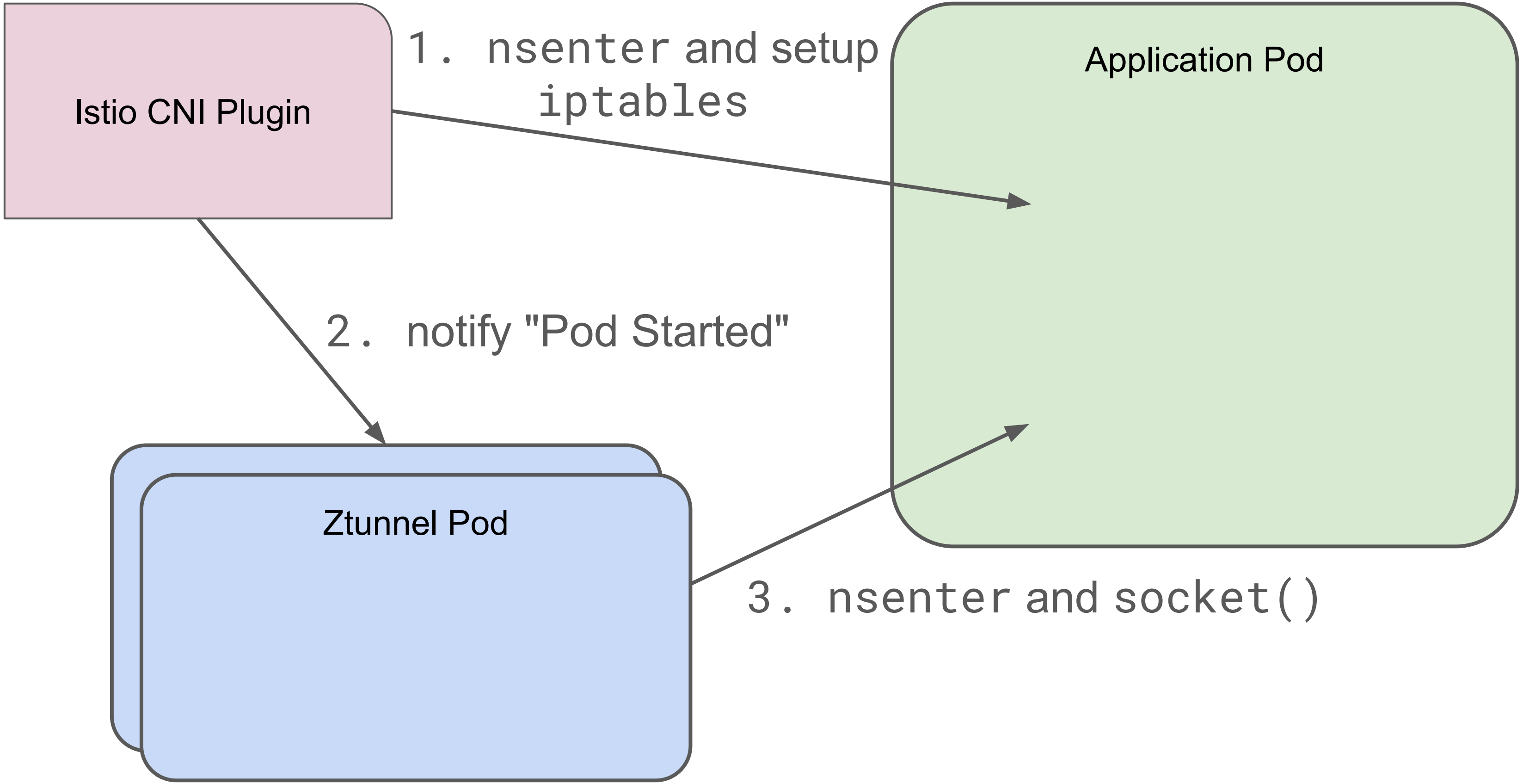
```
$ iptables-save
*nat
-A ISTIO_OUTPUT                 -m mark ! --mark 0x539/0xfff -j REDIRECT --to-ports 15001
-A ISTIO_PRERT  ! --dport  15008 -m mark ! --mark  0x539/0xfff -j REDIRECT --to-ports  15006
COMMIT
```

The beginning: setting up the Pod

CNI

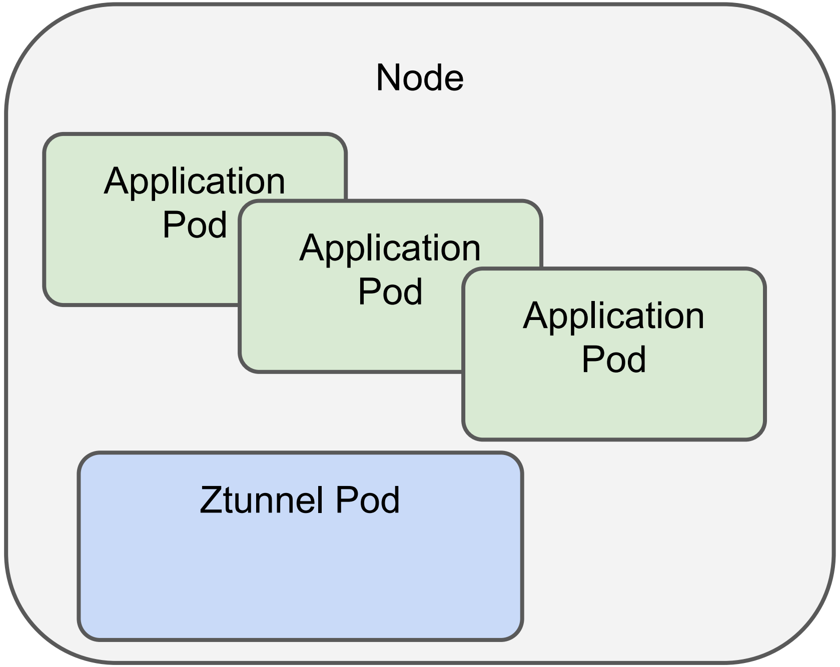


The beginning: setting up the Pod

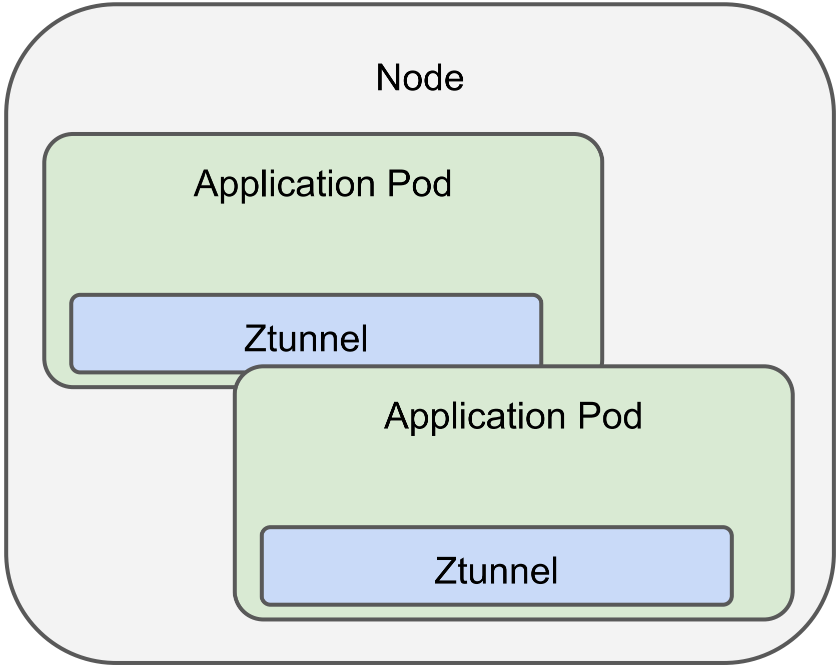


Understanding Ztunnel Networking

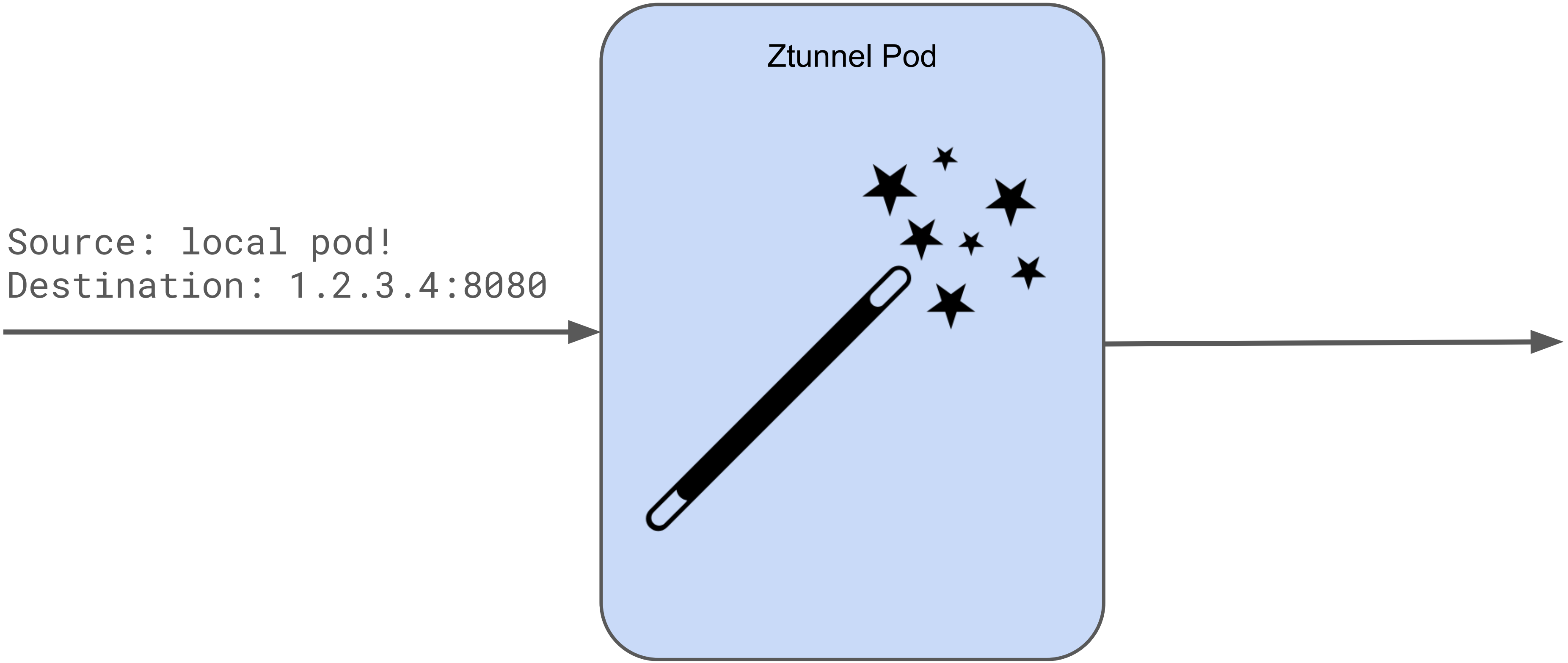
Compute View



Networking View



Ztunnel Routing



Ztunnel Pod

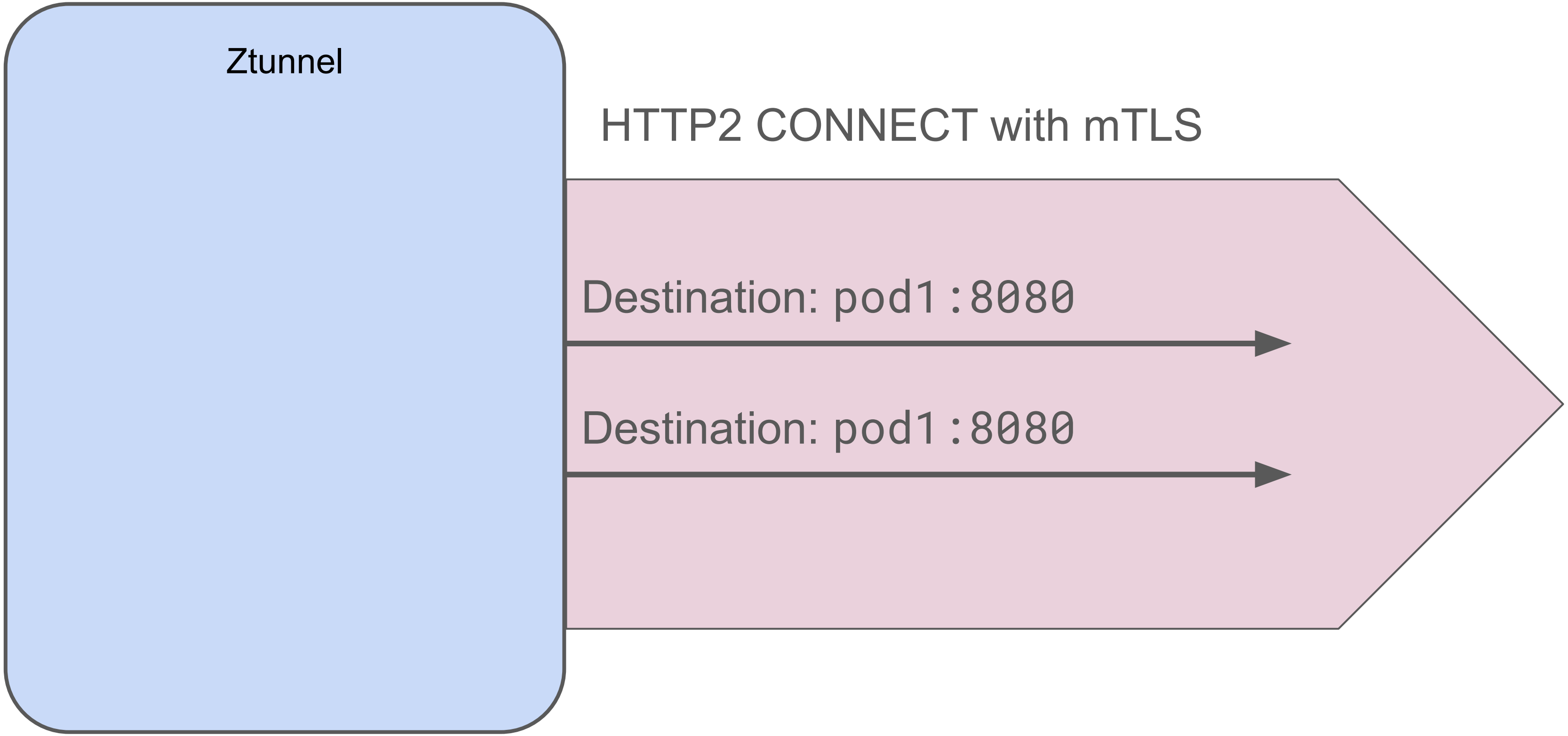
```
Source: local pod!
Destination: 1.2.3.4:8080
```

Ztunnel Routing

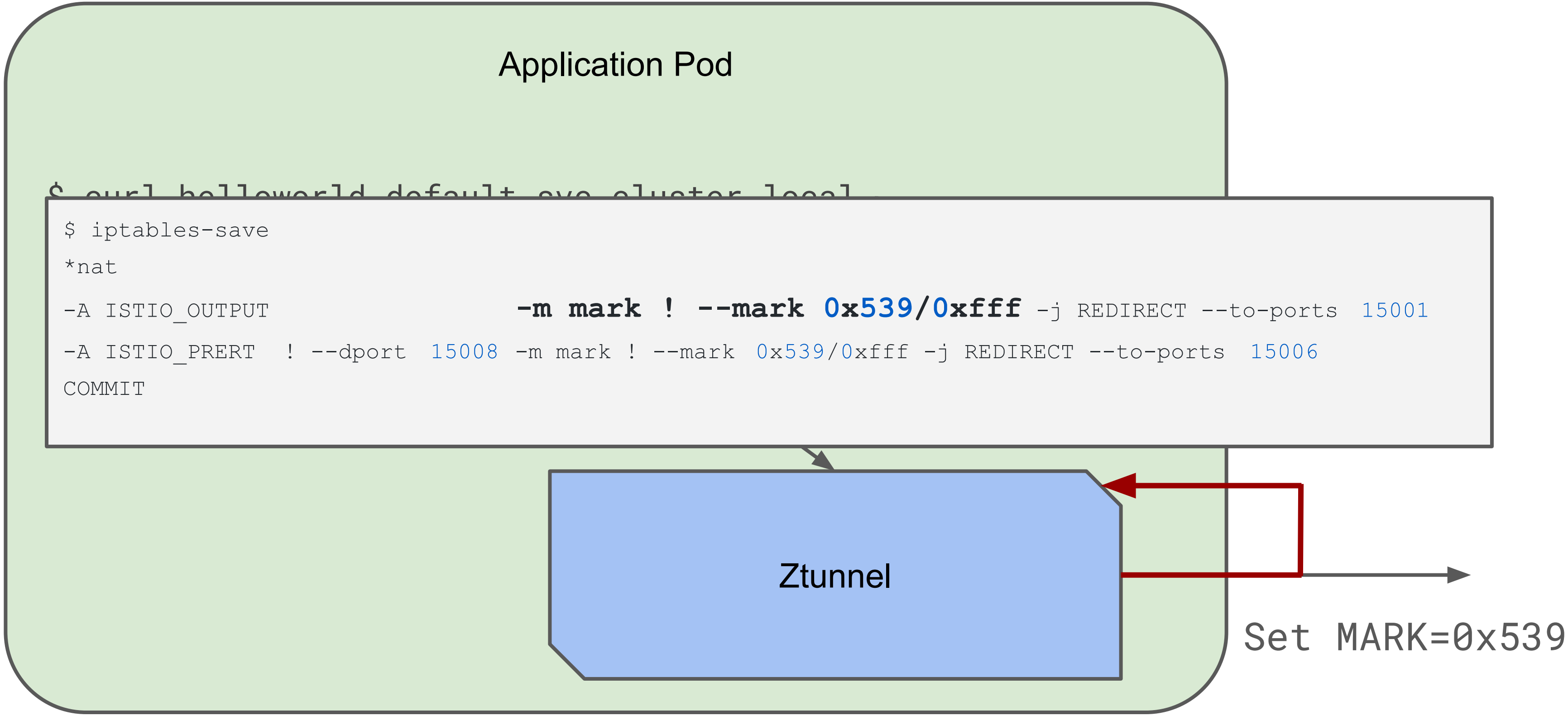
```
$ istioctl ztunnel-config services
SERVICE NAME   SERVICE VIP
details        10.96.138.231
productpage    10.96.246.176
ratings        10.96.189.100
reviews        10.96.47.40
```

```
$ istioctl ztunnel-config workloads
POD NAME                        ADDRESS
details-v1-79dfbd6fff-2nxmm     10.244.0.63
productpage-v1-dffc47f64-gdqdz  10.244.0.62
ratings-v1-65f797b499-qshmc     10.244.0.58
reviews-v1-5c4d6d447c-ntdls     10.244.0.59
```

Mutual TLS & Tunneling

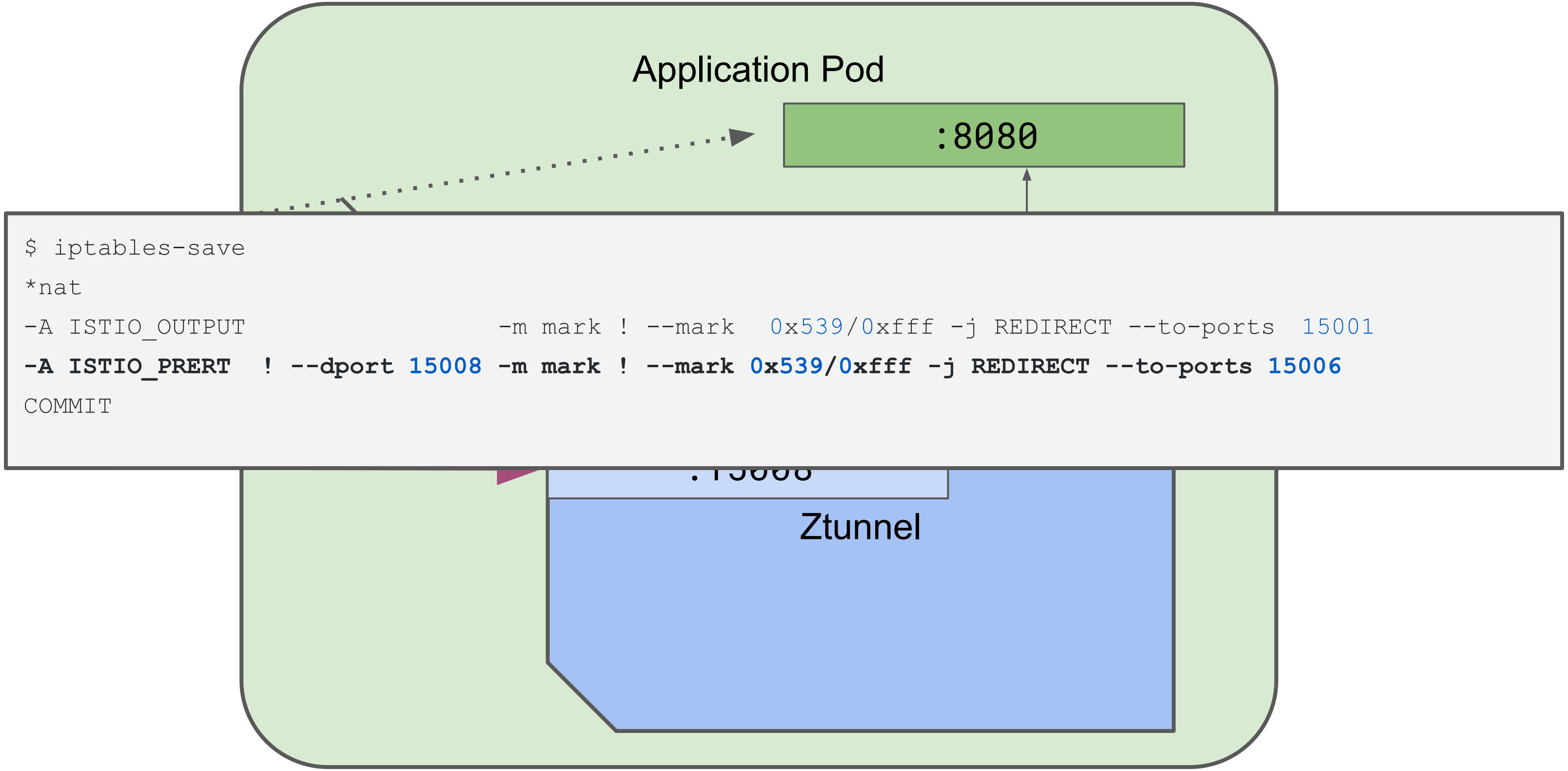


Loop Prevention



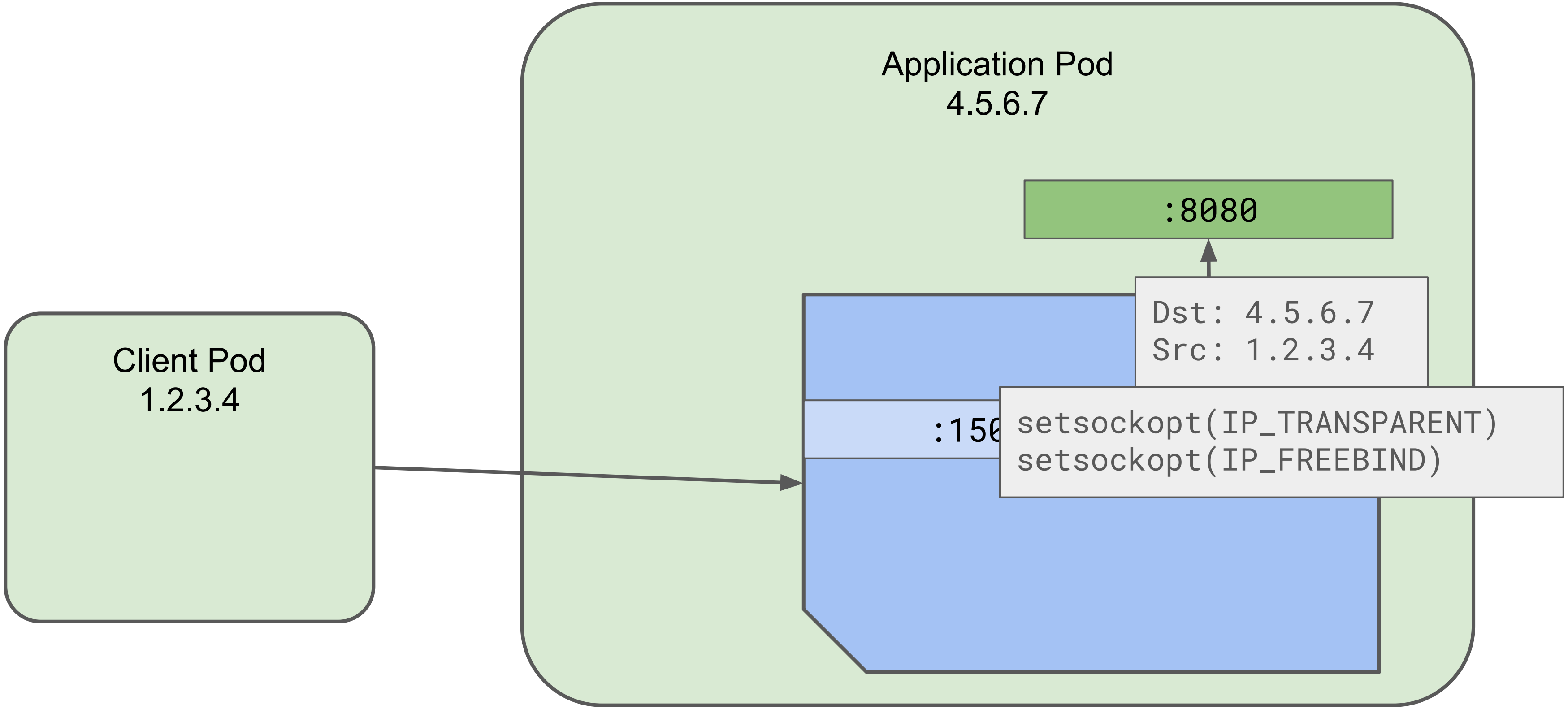
```
$ iptables-save
*nat
-A ISTIO_OUTPUT                      -m mark ! --mark 0x539/0xfff -j REDIRECT --to-ports  15001
-A ISTIO_PRERT  ! --dport  15008 -m mark ! --mark  0x539/0xfff -j REDIRECT --to-ports  15006
COMMIT
```

Accepting Connections in Ztunnel



```
$ iptables-save
*nat
-A ISTIO_OUTPUT                 -m mark ! --mark  0x539/0xfff -j REDIRECT --to-ports  15001
-A ISTIO_PRERT  ! --dport 15008 -m mark ! --mark 0x539/0xfff -j REDIRECT --to-ports 15006
COMMIT
```

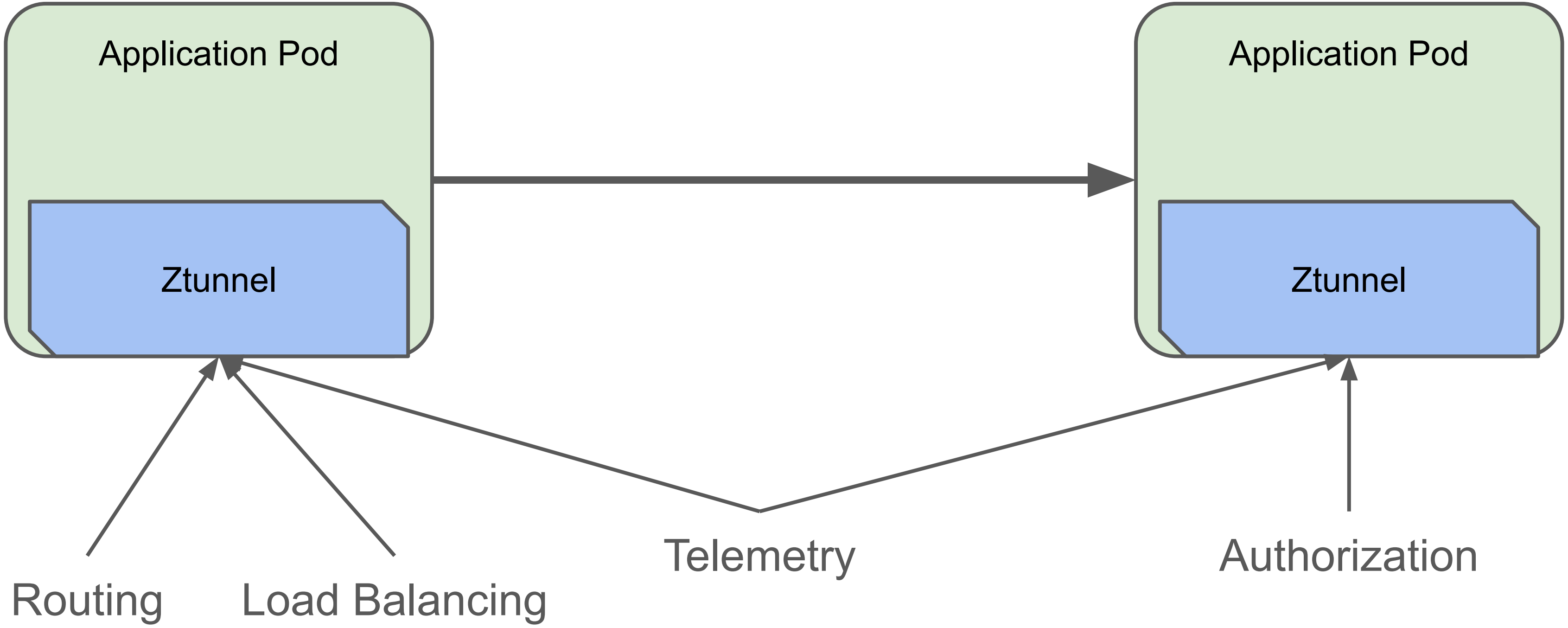
Source IP Preservation



```
Dst: 4.5.6.7
Src: 1.2.3.4
```

```
setsockopt(IP_TRANSPARENT)
setsockopt(IP_FREEBIND)
```

Feature location



Application Pod

Ztunnel

Application Pod

Ztunnel

Routing

Load Balancing

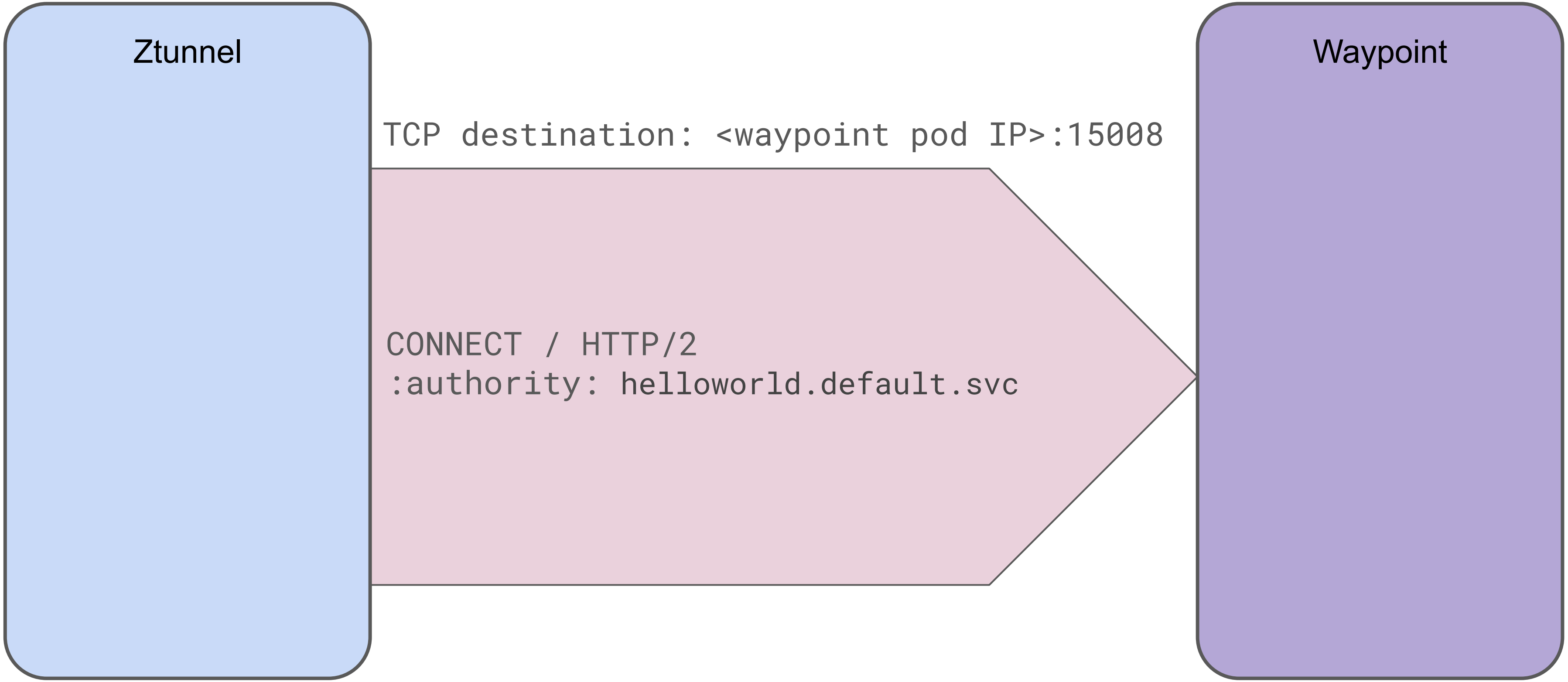
Telemetry

Authorization

Waypoint Routing

```
$ istioctl ztunnel-config services
SERVICE NAME   SERVICE VIP    WAYPOINT
details        10.96.138.231  None
productpage    10.96.246.176  None
ratings        10.96.189.100  ratings-waypoint
reviews        10.96.47.40    None
```

Waypoint Routing



TCP destination: <waypoint pod IP>:15008

```
CONNECT / HTTP/2
:authority: helloworld.default.svc
```

KubeCon CloudNativeCon

North America 2024

Life of a Packet

Ambient Edition

John Howard (Solo.io), Keith Mattix (Microsoft)