

ISOVALENT

# Cilium Mesh

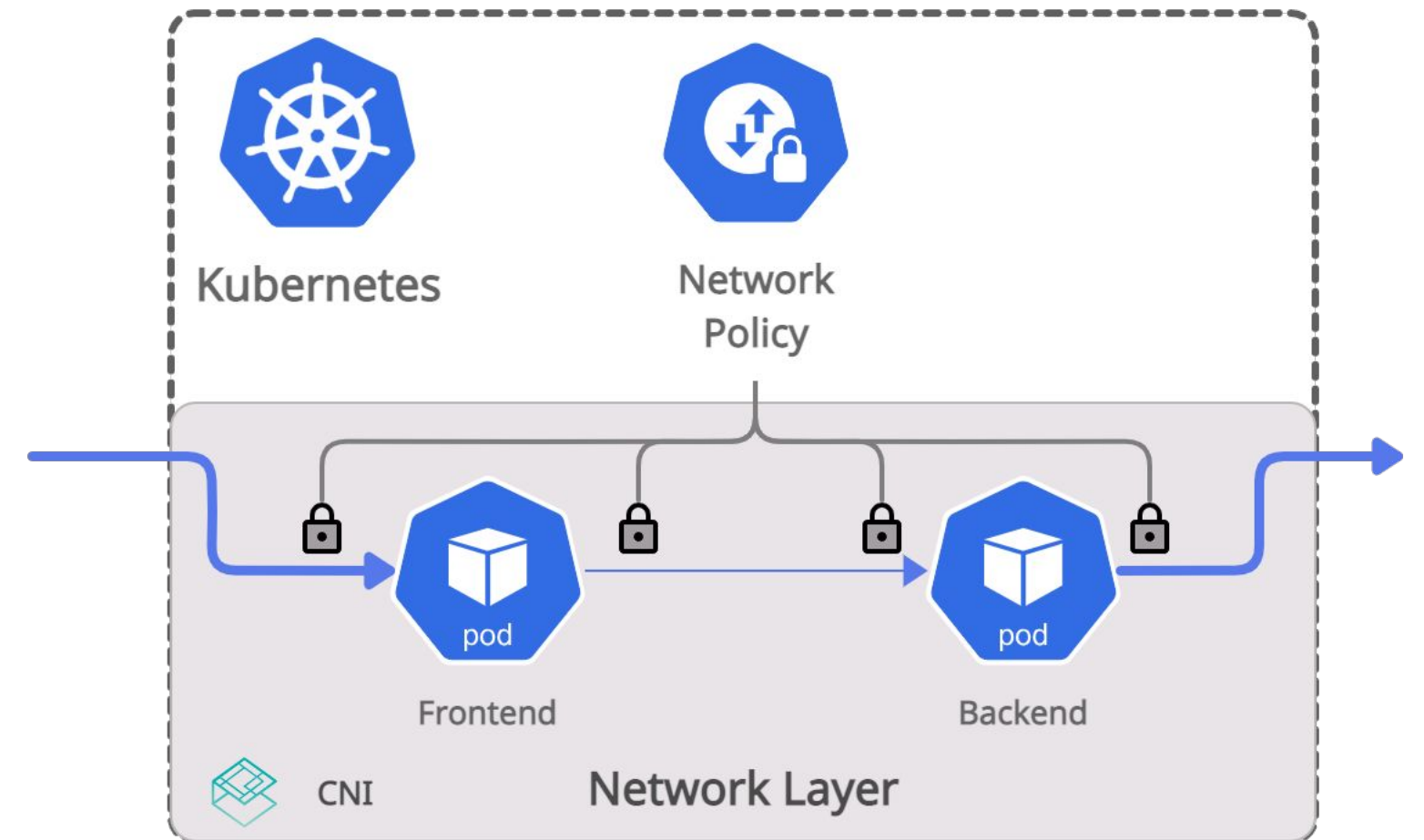
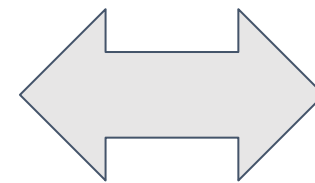
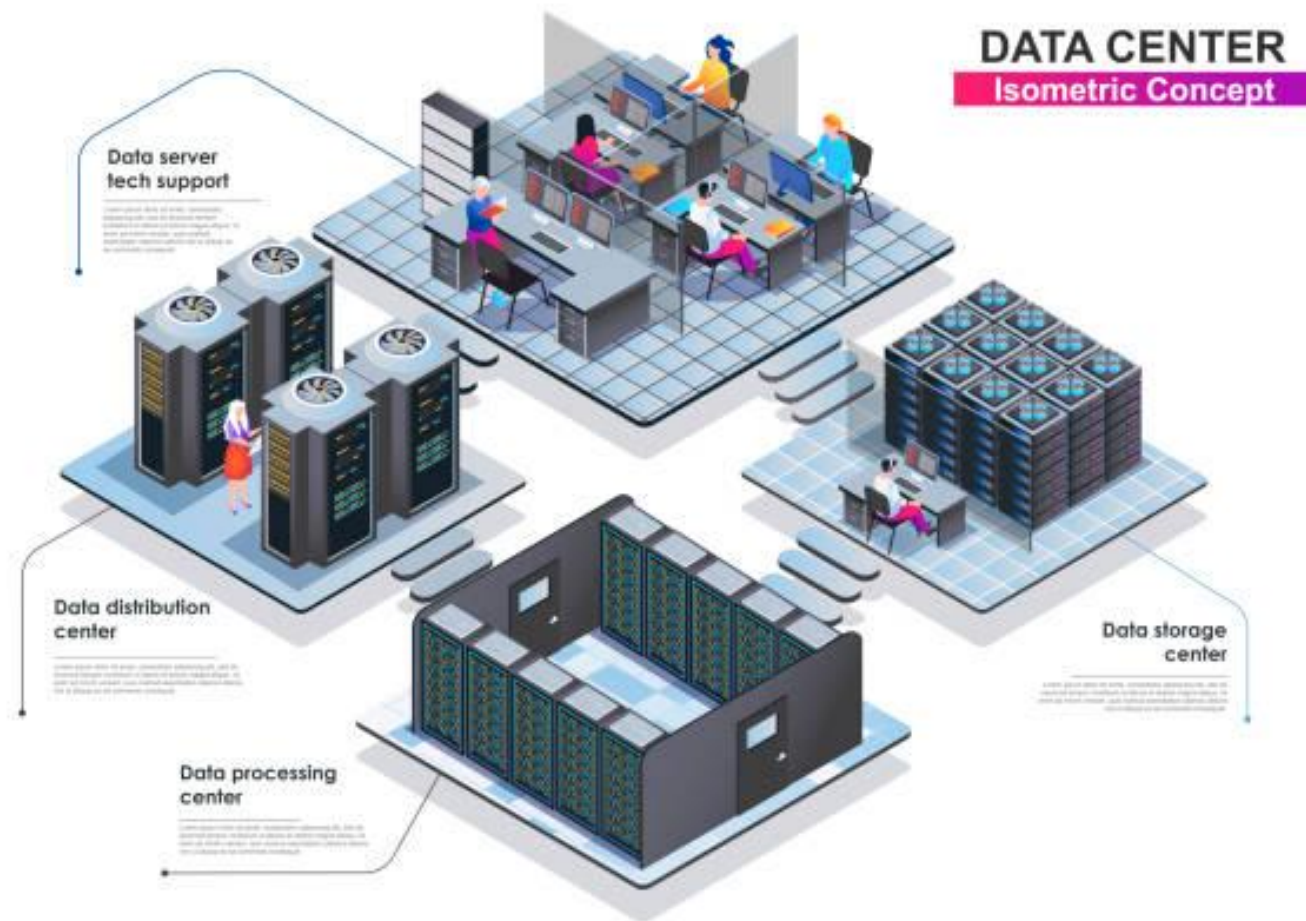
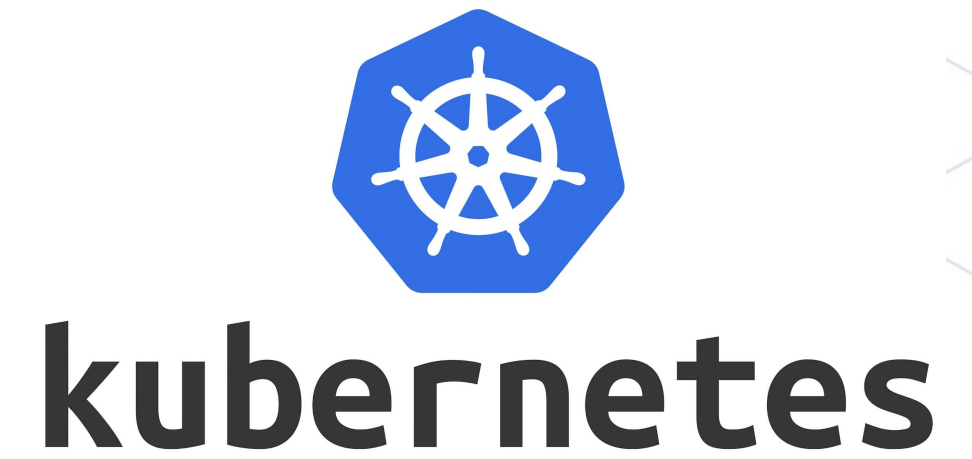
Connecting Kubernetes  
with Legacy  
Infrastructure



*Thomas Graf, Isovalent*

*Co-Founder & CTO*

# Datacenters & Existing Infrastructure



**How do we connect them together?**



# cilium

Created by ISOVALENT

 **eBPF**-based:

- Networking
- Security
- Observability
- Service Mesh & Ingress

Foundation



Technology



Scalable, Secure,  
High Performance  
Networking



















































Sidecar-free Service  
Mesh, Ingress, &  
Gateway API

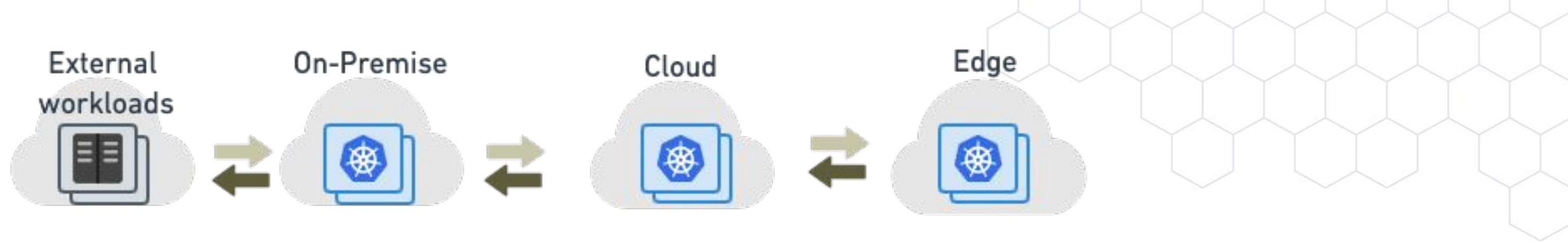


Network  
Observability &  
Monitoring



Security Observability &  
Runtime Enforcement

 What Makes a Good Multi-tenant Kubernetes Solution <a href="#">VIDEO 1</a> · <a href="#">VIDEO 2</a>	 Building High-Performance Cloud Native Pod Networks <a href="#">READ BLOG</a>	 AWS picks Cilium for Networking & Security on EKS Anywhere <a href="#">READ BLOG</a>	 Bell uses Cilium and eBPF for telco networking <a href="#">VIDEO 1</a> · <a href="#">VIDEO 2</a>	 AccuKnox uses Cilium for network visibility and network policy enforcement	 ACOSS uses Cilium as their main CNI plugin for self-hosted Kubernetes	 ArangoDB Oasis uses Cilium to separate database deployments in a multi-tenant cloud environment	 Ayedo builds and operates cloud native platforms using Cilium
 Building a Secure and Maintainable PaaS <a href="#">WATCH VIDEO</a>	 Cloud Native Networking with eBPF <a href="#">WATCH VIDEO</a>	 Datadog is using Cilium in AWS (self-hosted k8s) <a href="#">WATCH VIDEO</a>	 Managed Kubernetes: 1.5 Years of Cilium Usage at DigitalOcean <a href="#">WATCH VIDEO</a>	 ByteDance uses Cilium as their CNI for self-hosted Kubernetes clusters	 Canonical's Kubernetes distribution microk8s uses Cilium as CNI plugin	 Civo is offering Cilium as the CNI option for Civo users to choose it for their Civo Kubernetes clusters	 Cognite uses Cilium as the CNI plugin for industrial DataOps
 ect188 uses Cilium as their CNI and for load balancing <a href="#">READ BLOG</a>	 Kubernetes Network Policies in Action with Cilium <a href="#">VIDEO</a>	 Google chooses Cilium for Google Kubernetes Engine (GKE) networking <a href="#">READ BLOG</a>	 IKEA uses Cilium for their self-hosted bare-metal private cloud <a href="#">WATCH VIDEO</a>	 Elastic Path uses Cilium in their production CloudOps Kubernetes clusters	 F5 uses Cilium VXLAN tunnel integration with BIG-IP	 finleap connect uses Cilium on a bare metal private cloud	 Form3 is using Cilium in their production clusters (self-hosted, bare-metal, private cloud)
 Scaling a Multi-Tenant Kubernetes Clusters in a Telco <a href="#">WATCH VIDEO</a>	 Meltwater is using Cilium in AWS on self-hosted multi-tenant k8s clusters as the CNI plugin <a href="#">WATCH VIDEO</a>	 Mobilabs uses Cilium as the CNI for their internal cloud <a href="#">READ BLOG</a>	 Nexxiot using Cilium as the CNI plugin on EKS for its IoT SaaS <a href="#">READ USER STORY</a>	 Infomaniak uses Cilium in self-hosted clusters on bare-metal and Openstack	 InnoQ uses Cilium to run their customer's infrastructure	 Cilium is the platform that powers Isovalent's enterprise networking, observability, and security solutions	 JUMO uses Cilium as the CNI plugin for all of their AWS-hosted EKS clusters
 PostFinance is using Cilium as their CNI for all mission critical, on premise k8s clusters <a href="#">READ CASE STUDY</a>	 eBPF & Cilium at Sky <a href="#">WATCH VIDEO</a>	 Skybet uses Cilium as their CNI <a href="#">READ BLOG</a>	 Trip.com uses Cilium both on premise and in AWS <a href="#">BLOG 1</a> · <a href="#">BLOG 2</a>	 Kryptos uses Cilium as the CNI for their on-prem Kubernetes clusters	 Kube-OVN uses Cilium to enhance the CNI service performance, security and monitoring	 Kubernetes uses Cilium as the CNI for its Kubernetes installer and platform	 KubeKey is an open-source lightweight tool for deploying Kubernetes clusters and addons
 Northflank uses Cilium as its CNI plugin across GCP, Azure, AWS and bare metal	 Overstock uses Cilium as their CNI for self-hosted bare metal clusters	 Palantir is using Cilium as their main CNI plugin in AWS (self-hosted k8s)	 Plaid uses Cilium as the CNI for its serverless database platform	 Liquid Reply is a consulting firm that uses Cilium in client projects	 Melenion uses Cilium as the CNI for its on-premise production clusters	 Mux uses Cilium on self-hosted clusters in GCP and AWS to run its video streaming/analytics platforms	 MyFitnessPal trusts Cilium with high volume user traffic on AWS and GKE



**cilium Service Mesh**

Ingress Authentication Traffic Management

spiffe Gateway API

**cilium hubble Observability**

Metrics Tracing Service Map Logs

SIEM fluentd Grafana OpenTelemetry

**cilium CN**

**Networking**

Network Policy: DNS, L3/L4, L7

Encryption: IPsec, Wireguard

Load-Balancing: K8s, Maglev, DSR

Multi-Cluster Networking: NAT46

IPv4, IPv6, Cloud SDN, BGP, Overlay, SRv6, Egress Gateway

**Runtime Security**

Tetragon

SIEM fluentd Grafana

Observability

Enforcement

Kubernetes Container VM Metal

aws Google Cloud Azure Alibaba Cloud RED HAT OPENSIFT vmware



**What if we could manage  
existing Infrastructure as we  
manage Kubernetes?**

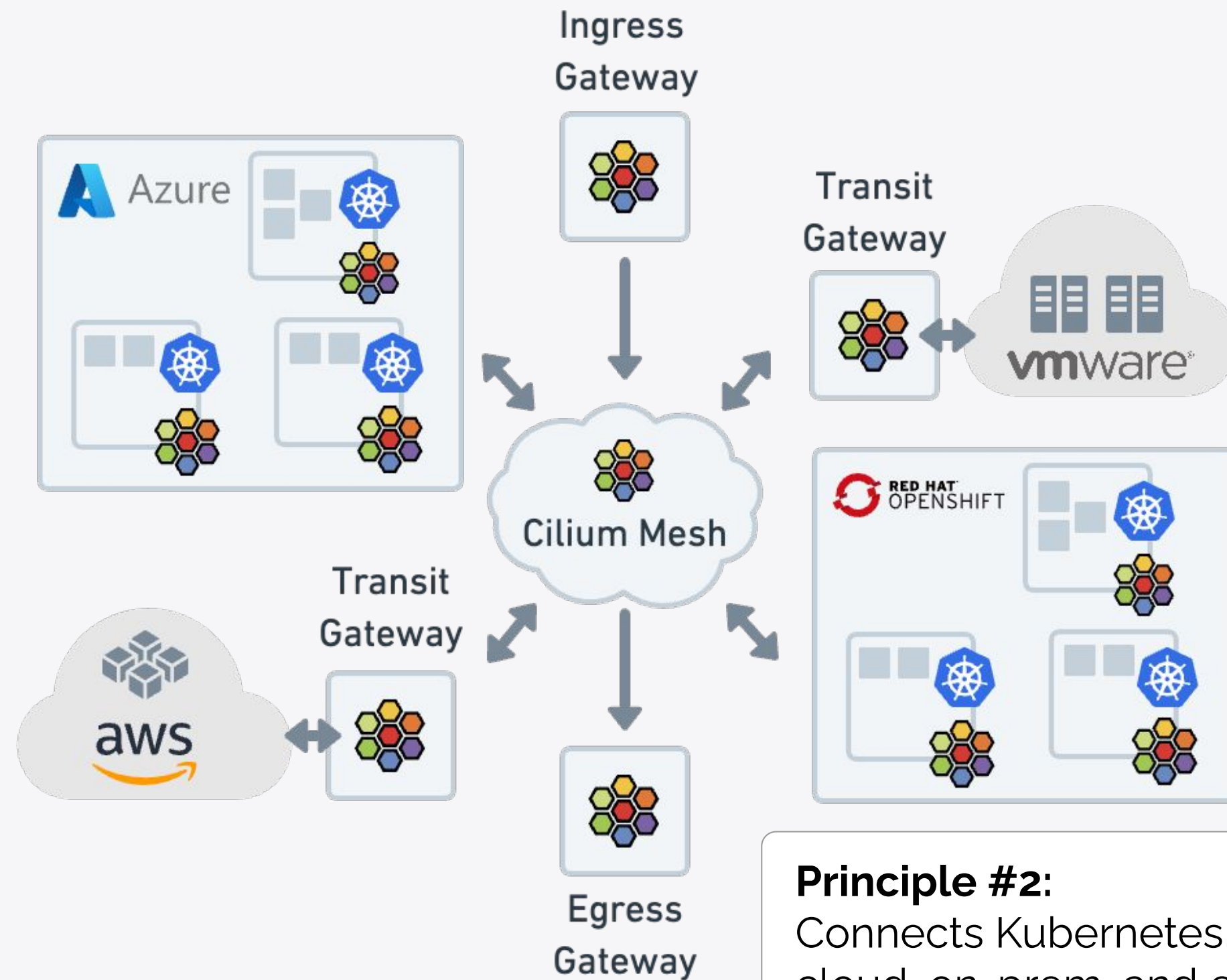
# Cilium Mesh

## One Mesh to Connect Them All

### Principle #1:

Combines all Cilium components into a single mesh:

- Kubernetes Networking (CNI)
- Cluster Mesh (Multi-Cluster)
- Ingress & Egress Gateway
- Load Balancer
- Service Mesh



### Principle #2:

Connects Kubernetes, VMs, and Servers across cloud, on-prem, and edge.

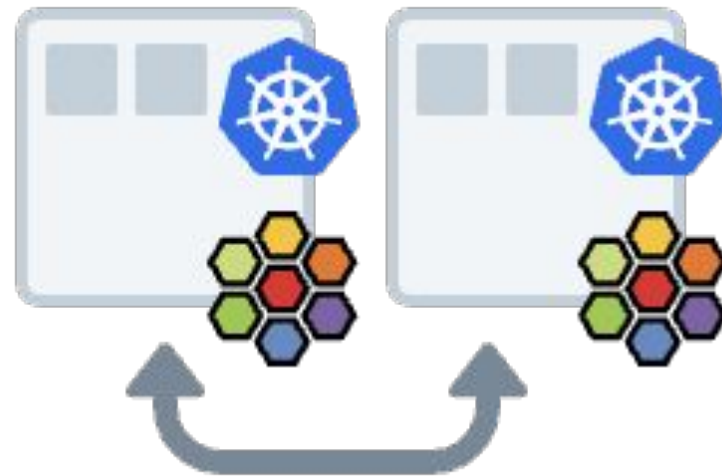
# Cilium Mesh

Connect Kubernetes, VMs, and Servers  
across Cloud, On-Prem, and Edge.

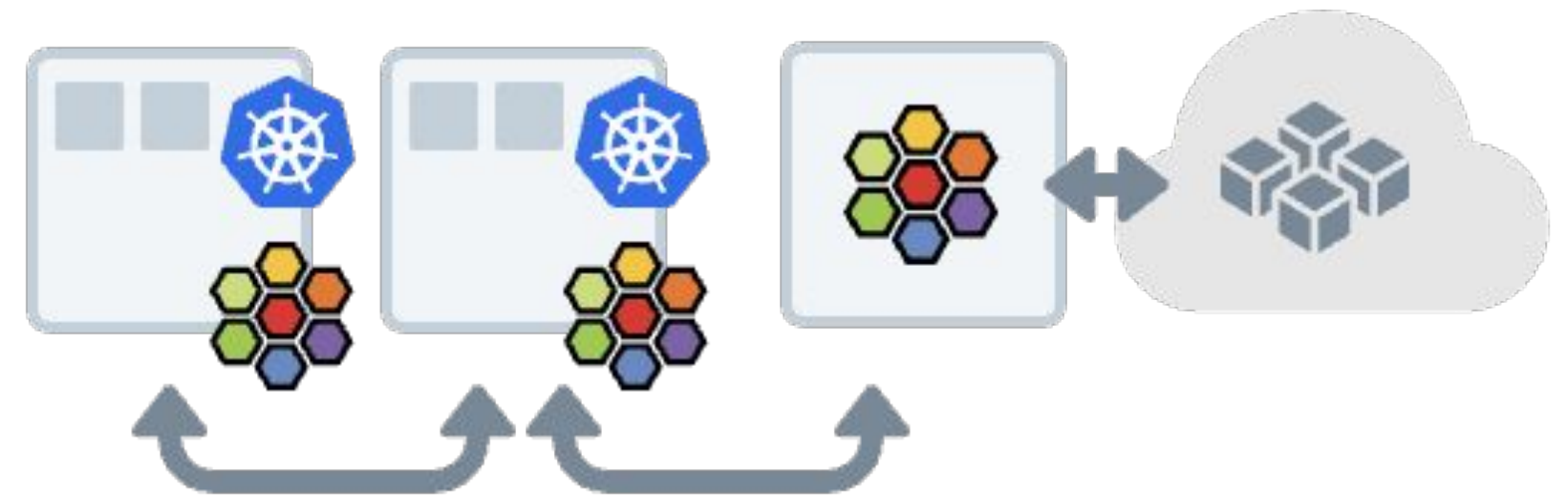
Kubernetes  
Networking



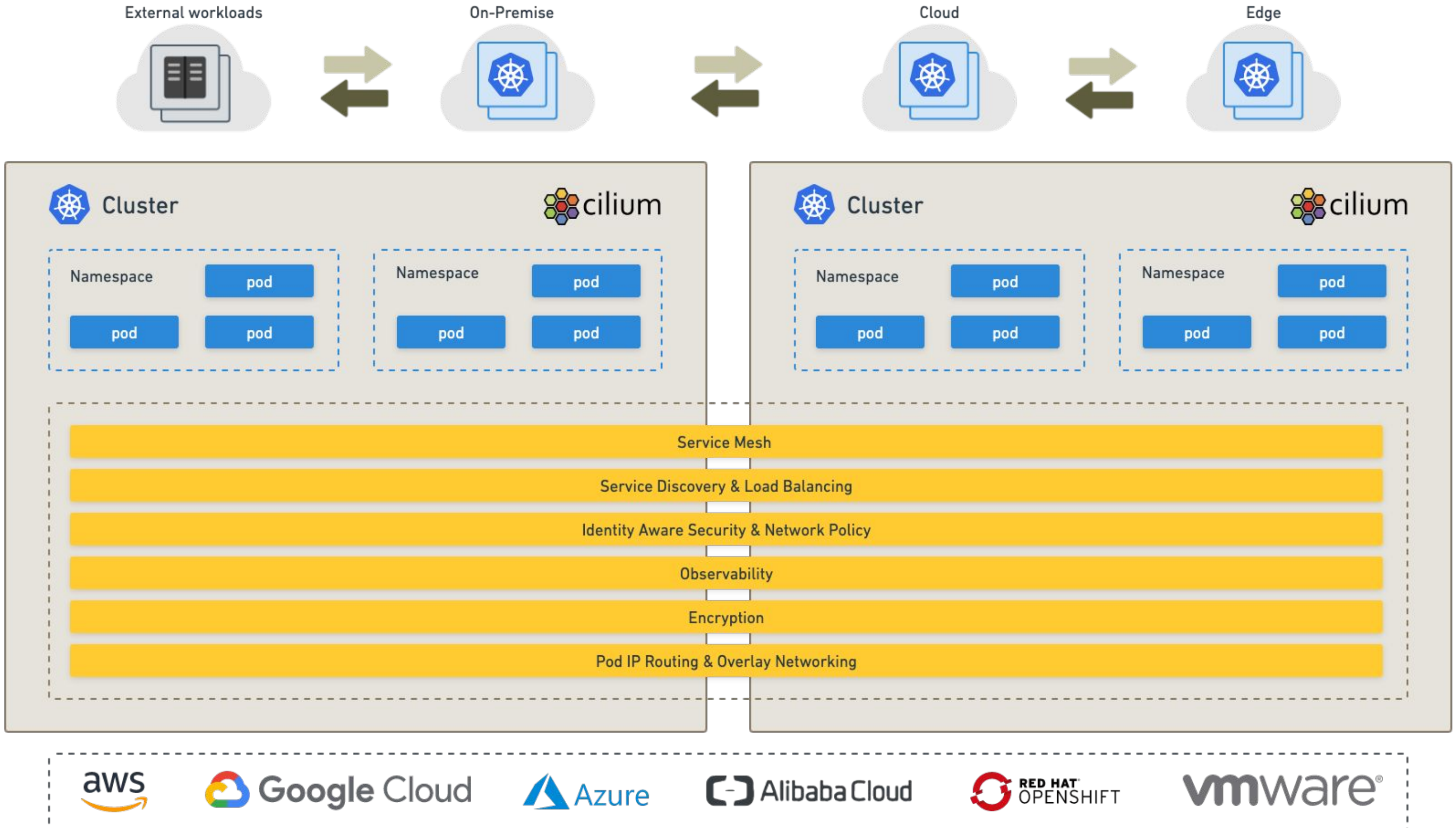
Multi-Cluster  
Networking



Multi- & Hybrid-  
Cloud Networking

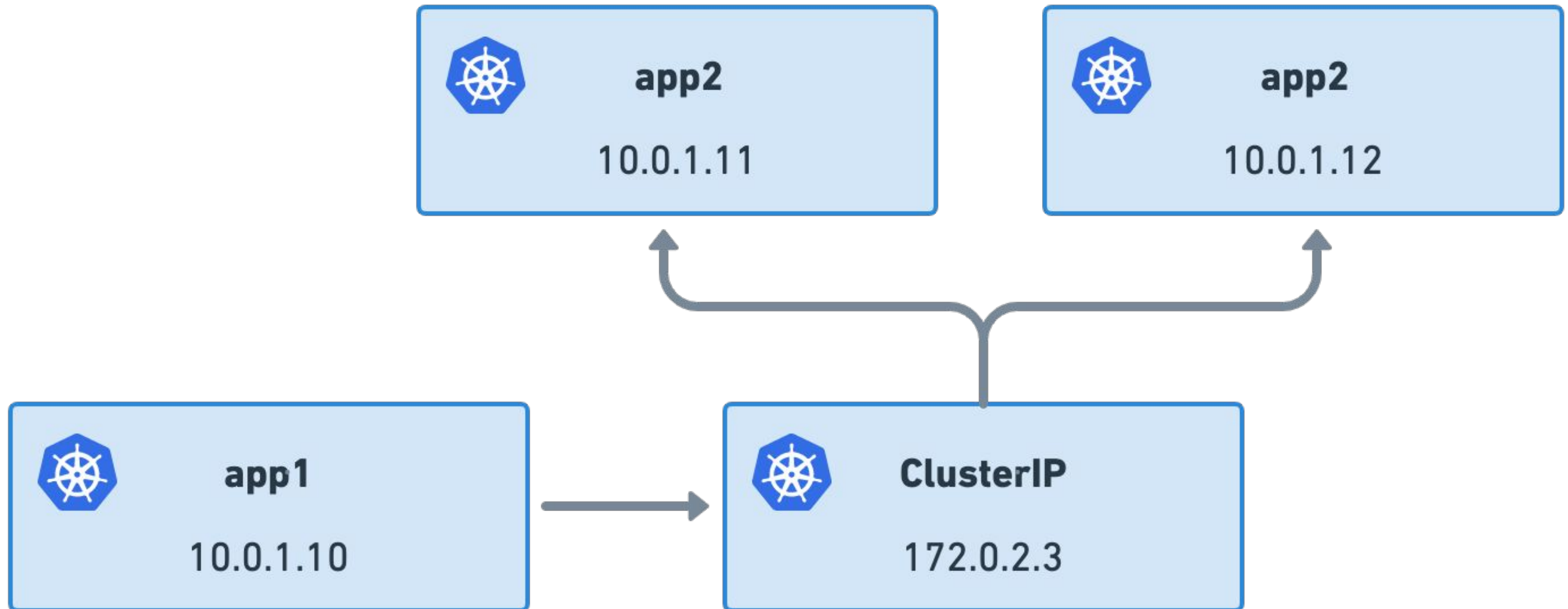


# Cluster Mesh - Introduction





# Kubernetes Services



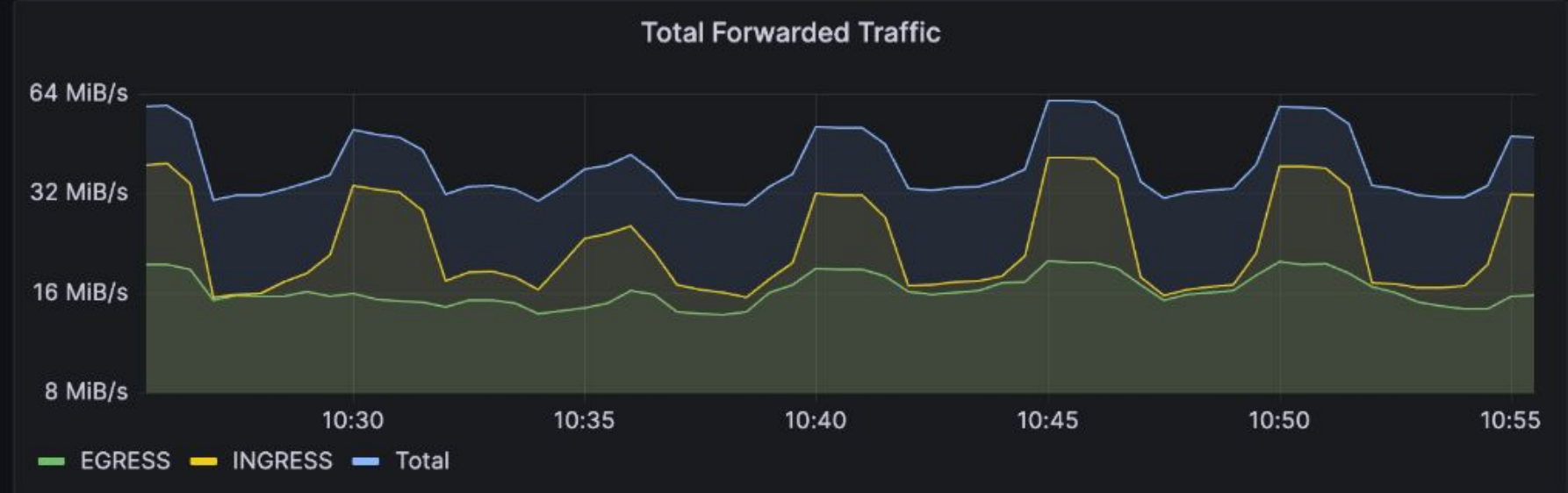
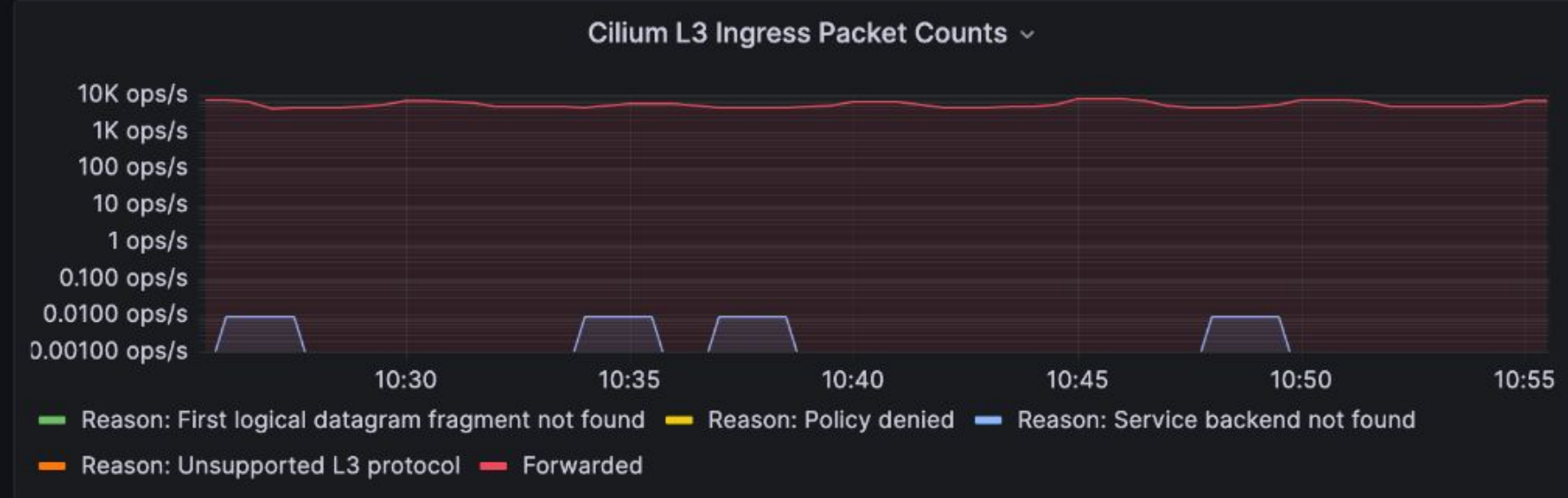
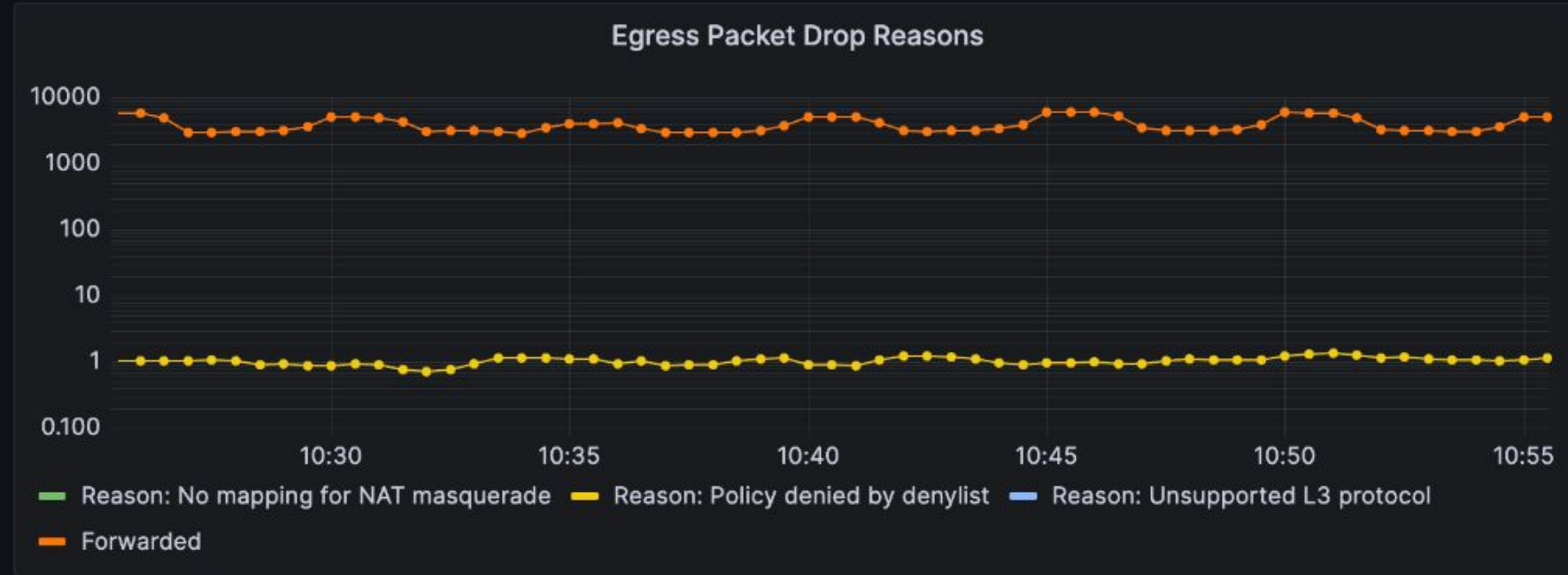
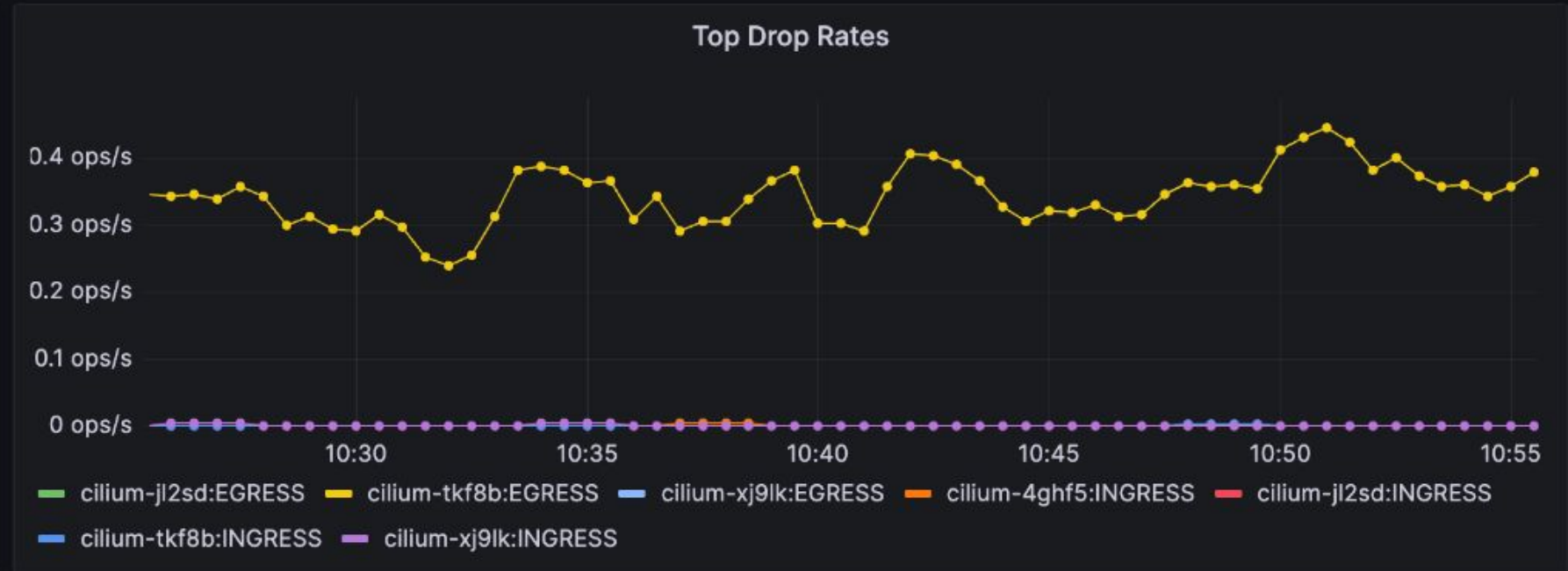
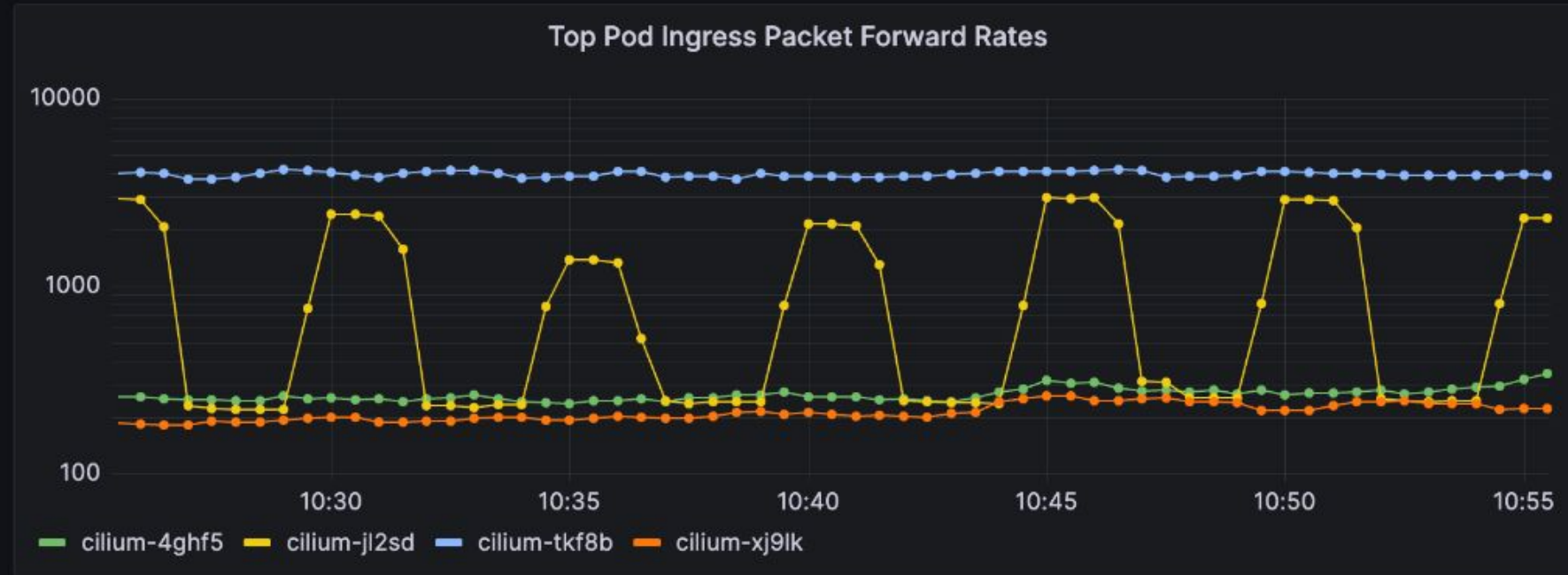
# Cluster Mesh - Service Example

```
apiVersion: v1
kind: Service
metadata:
  name: backend-service
  annotations:
    io.cilium/global-service: "true"
    io.cilium/service-affinity: remote
spec:
  type: ClusterIP
  ports:
  - port: 80
  selector:
    name: backend
```

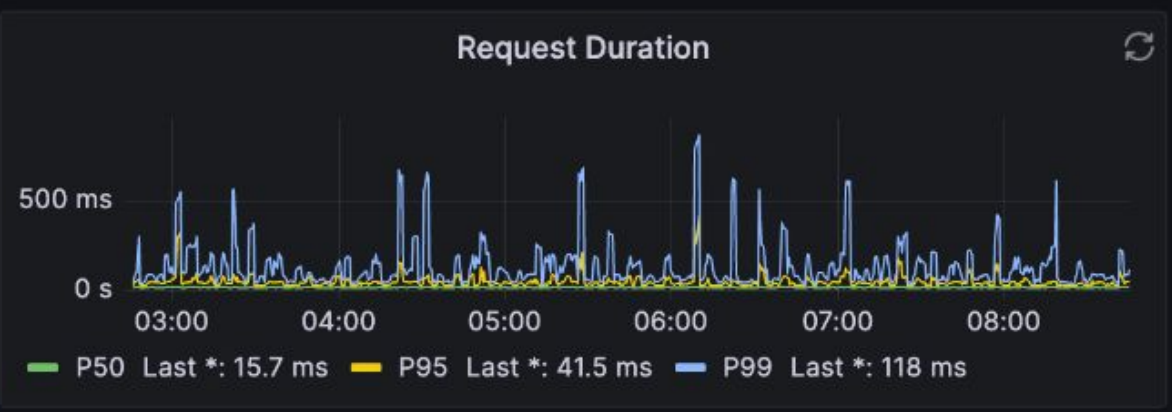
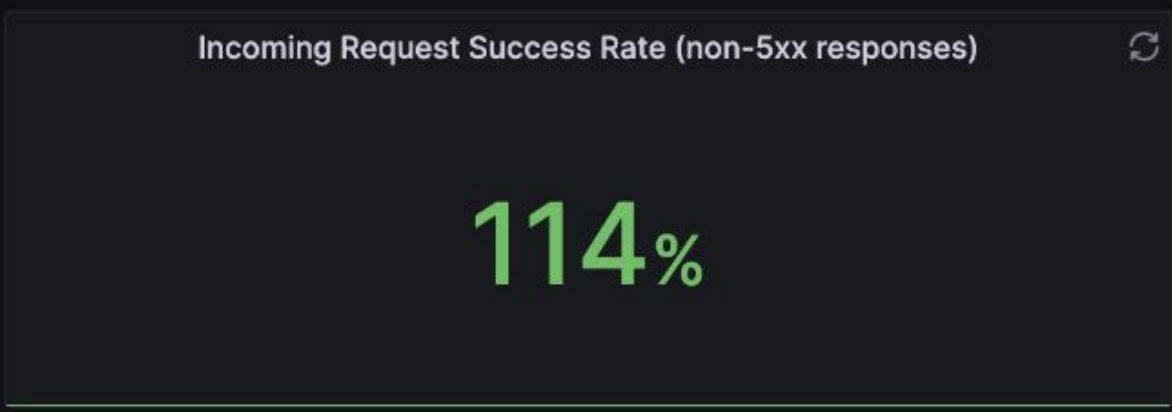


Data Source default cluster namespace pod top k 10

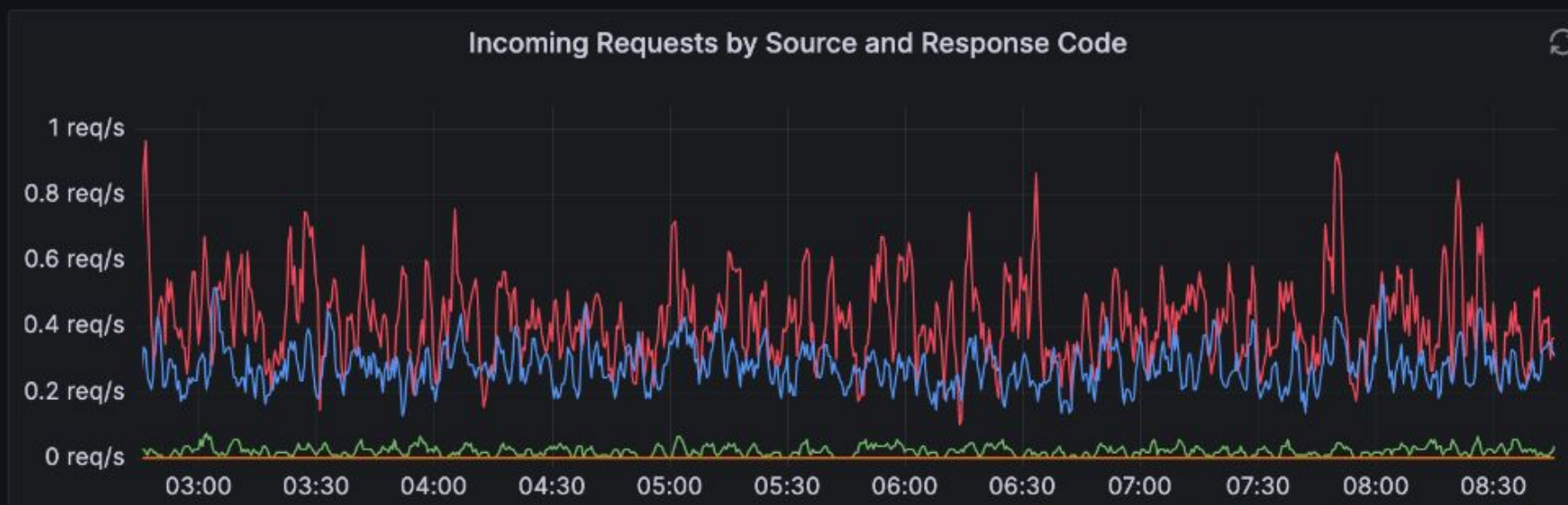
☰ Cilium Overviews ☰ Cilium Components



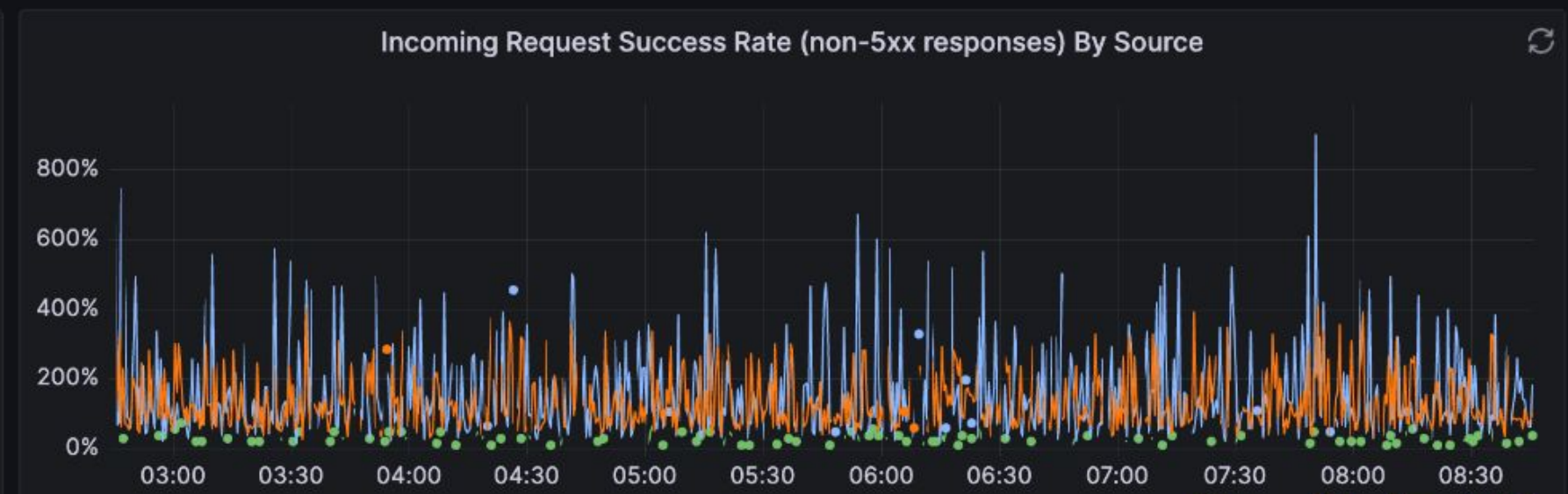
General



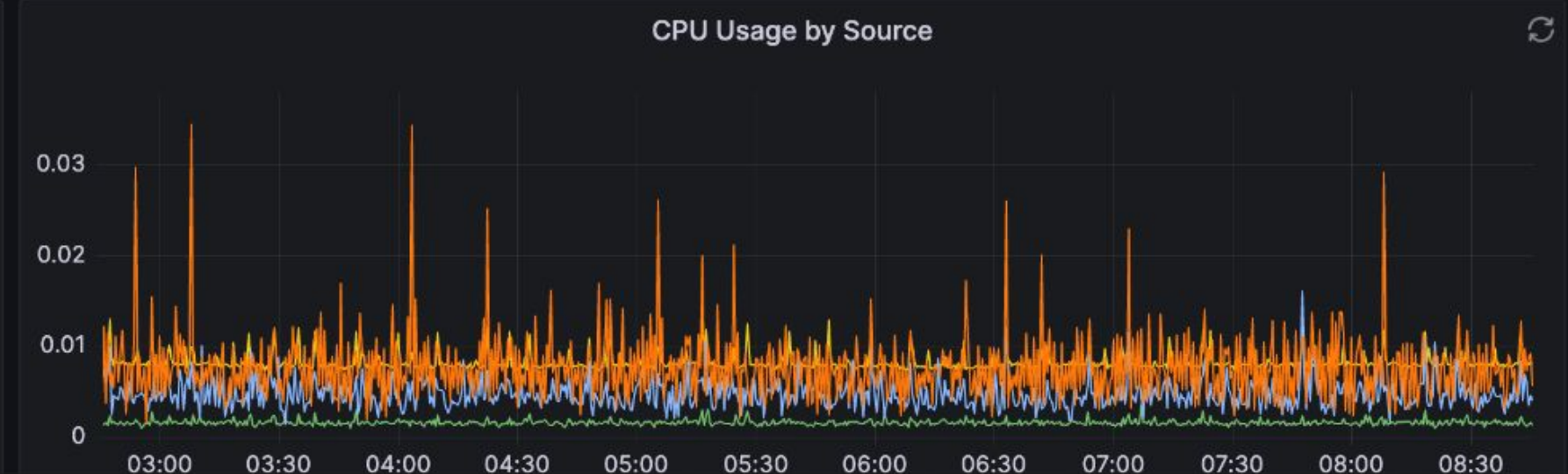
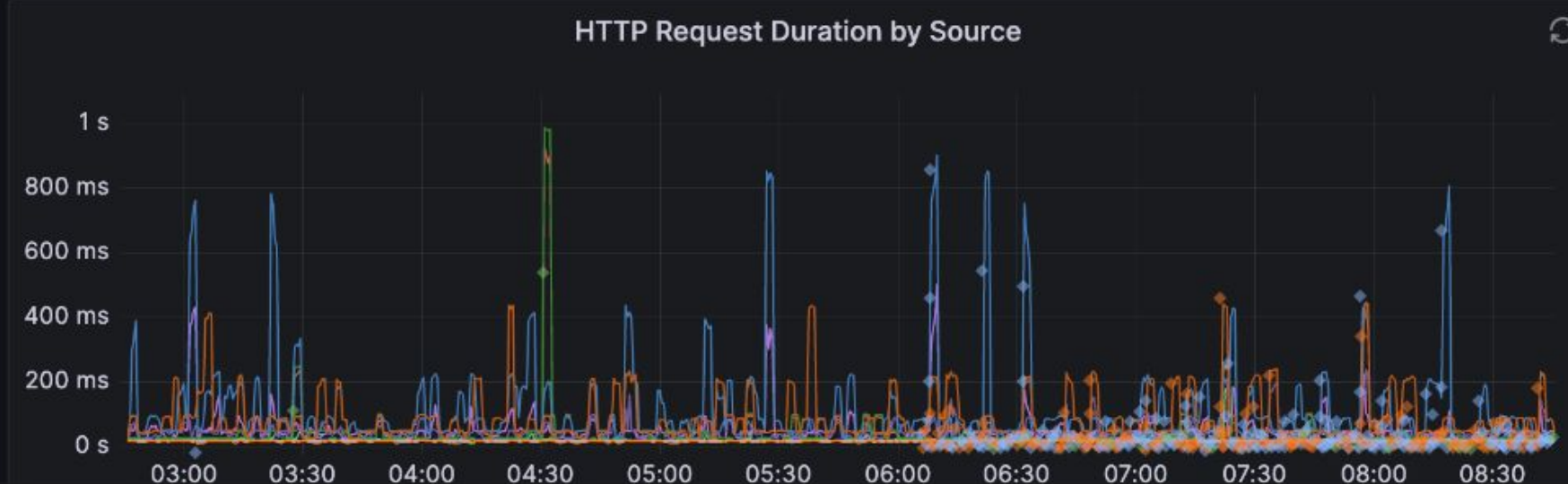
Requests by Source



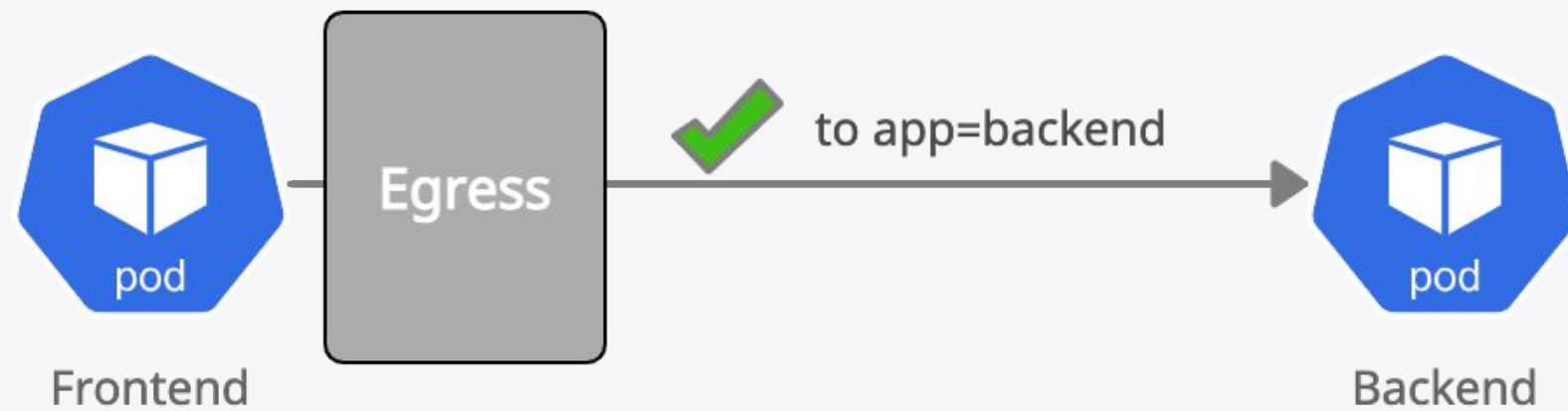
	Max	Mean	Total	Last *
otel-demo/otel-demo-adservice: 200	0.0730 req/s	0.0218 req/s	15.7 req/s	0.0360 req/s
otel-demo/otel-demo-frontendproxy: 200	0 req/s	0 req/s	0 req/s	0 req/s
otel-demo/otel-demo-frontendproxy: 302	0 req/s	0 req/s	0 req/s	0 req/s
otel-demo/otel-demo-frontendproxy: 404	0 req/s	0 req/s	0 req/s	0 req/s



	Mean	Min	Max	Last *
otel-demo/otel-demo-adservice	NaN	9.09%	∞%	36.4%
otel-demo/otel-demo-frontendproxy	NaN			NaN
otel-demo/otel-demo-productcatalogservice	∞%	14.7%	∞%	182%
otel-demo/otel-demo-recommendationservice	∞%	24.7%	∞%	103%



# Kubernetes Network Policy



```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  name: frontend-egress-allow-to-backend
spec:
  podSelector:
    matchLabels:
      app: frontend
  egress:
    - to:
      - podSelector:
          matchLabels:
            app: backend
```

Overview

Network

Flows

Metrics

Policies

Runtime

Metrics

Processes

Live View

Namespace

Show clusterwide data

anna-otel-demo

Flows verdict

Any verdict

Forwarded

Dropped

Aggregate flows

Visual filters

Host service

Kube-DNS:53 pod

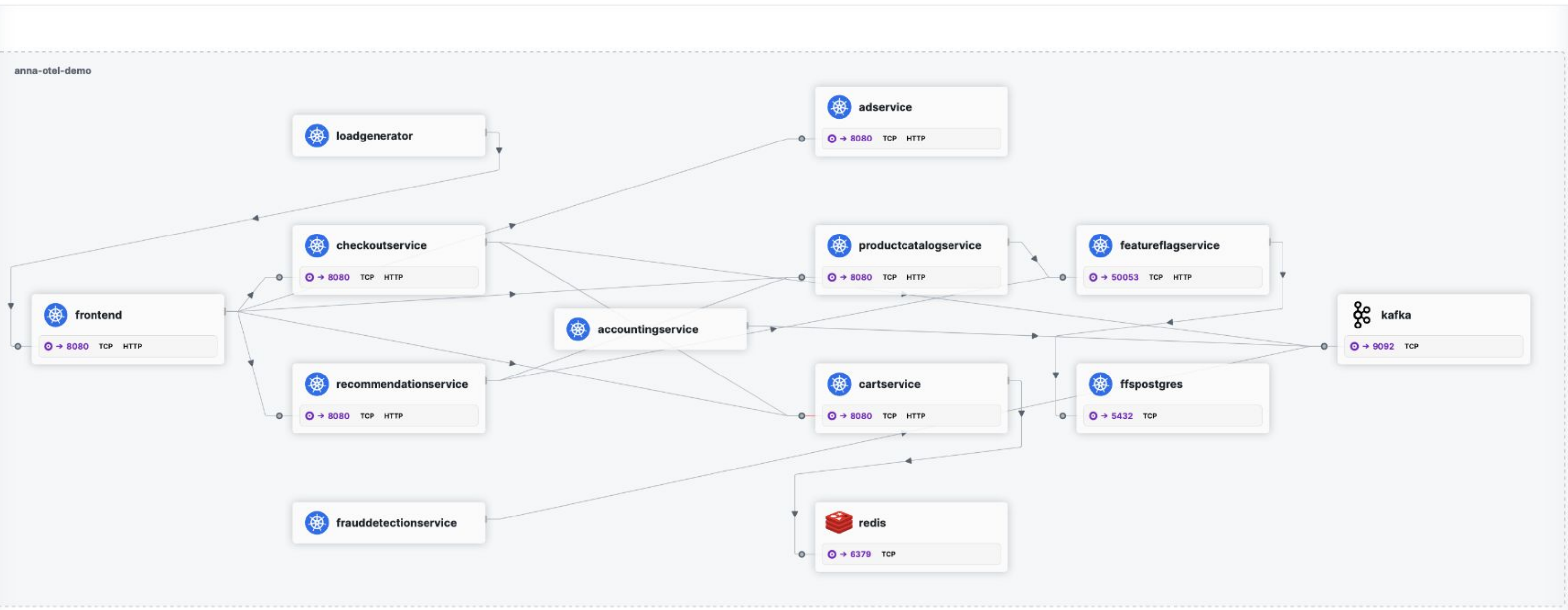
Remote node

Prometheus app

Notifications

1.8K flows/s • 4/4 nodes

Filter by: label key=val, ip=1.1.1.1, dns=google.com, identity=42, pod=frontend



2023-04-15T08:52:22.000Z

Flows Metrics Services

Columns

Source Identity	Destination Identity	Destination Port	L7 info	Traffic Direction	Verdict	TCP Flags	Timestamp
loadgenerator anna-otel-demo	frontend anna-otel-demo	8080	→ GET /api/products/66VCHSJNUP 0ms	ingress	forwarded		2023/04/15 10:52:32 (+02)
checkoutservice anna-otel-demo	kafka anna-otel-demo	9092	—	egress	forwarded	ACK	2023/04/15 10:52:31 (+02)
loadgenerator anna-otel-demo	frontend anna-otel-demo	8080	→ GET / 0ms	ingress	forwarded		2023/04/15 10:52:28 (+02)
loadgenerator anna-otel-demo	frontend anna-otel-demo	8080	→ GET /api/products/L9ECAV7KIM 0ms	ingress	forwarded		2023/04/15 10:52:26 (+02)
cartservice anna-otel-demo	redis anna-otel-demo	6379	—	egress	forwarded	ACK PSH	2023/04/15 10:52:26 (+02)
productcatalogservice anna-otel-demo	featureflagservice anna-otel-demo	50053	→ POST /oteldemo.FeatureFlagService/...	ingress	forwarded		2023/04/15 10:52:25 (+02)
productcatalogservice anna-otel-demo	featureflagservice anna-otel-demo	50053	—	egress	forwarded	SYN	2023/04/15 10:52:25 (+02)
loadgenerator anna-otel-demo	frontend anna-otel-demo	8080	→ GET /api/products/OLJCESPC7Z 0ms	ingress	forwarded		2023/04/15 10:52:25 (+02)
loadgenerator anna-otel-demo	frontend anna-otel-demo	8080	→ GET /api/products/2ZYFJ3GM2N 0ms	ingress	forwarded		2023/04/15 10:52:24 (+02)
frontend anna-otel-demo	cartservice anna-otel-demo	8080	→ POST /oteldemo.CartService/GetCart...	ingress	forwarded		2023/04/15 10:52:22 (+02)
loadgenerator anna-otel-demo	frontend anna-otel-demo	8080	→ GET /api/cart 0ms	ingress	forwarded		2023/04/15 10:52:22 (+02)
frontend anna-otel-demo	checkoutservice anna-otel-demo	8080	→ POST /oteldemo.CheckoutService/Pla...	ingress	forwarded		2023/04/15 10:52:22 (+02)
loadgenerator anna-otel-demo	frontend anna-otel-demo	8080	→ POST /api/checkout 0ms	ingress	forwarded		2023/04/15 10:52:22 (+02)
frontend anna-otel-demo	cartservice anna-otel-demo	8080	→ POST /oteldemo.CartService/Addlte...	ingress	forwarded		2023/04/15 10:52:22 (+02)

# ISOVALENT

CREATORS OF



# Thank you!



[isovalent.com](https://isovalent.com)