ISOVALENT

Networking Beyond Kubernetes with Cilium

Speakers: **Rastislav Szabo**

Nikolay Nikolaev

What CNCF says about Cilium

Cloud Native Computing Foundation Announces Cilium Graduation

eBPF-powered tool has been adopted by well over 100 organizations SAN FRANCISCO, Calif. – October 11, 2023 – The Cloud Native Computing Foundation® (CNCF®), which builds sustainable ecosystems for cloud native software, today announced the graduation of Cilium....

October 11, 2023

cilium

eBPF-based Networking, Security, and Observability

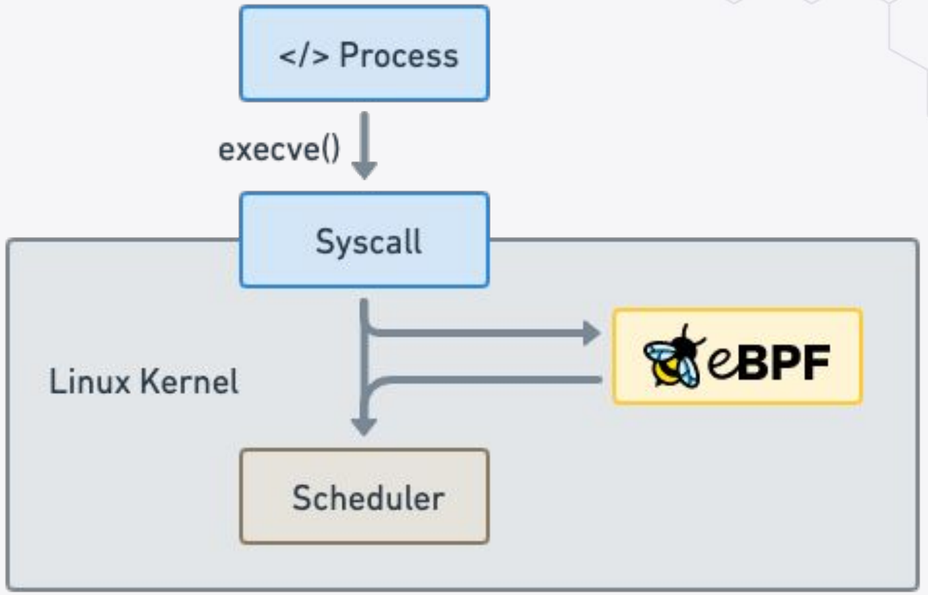
Cilium was accepted to CNCF on October 13, 2021 at the **Incubating** maturity level and then moved to the **Graduated** maturity level on October 11, 2023.

VISIT PROJECT WEBSITE

eBPF

Makes the Linux kernel programmable in a secure and efficient way.

“What JavaScript is to the browser, eBPF is to the Linux Kernel”

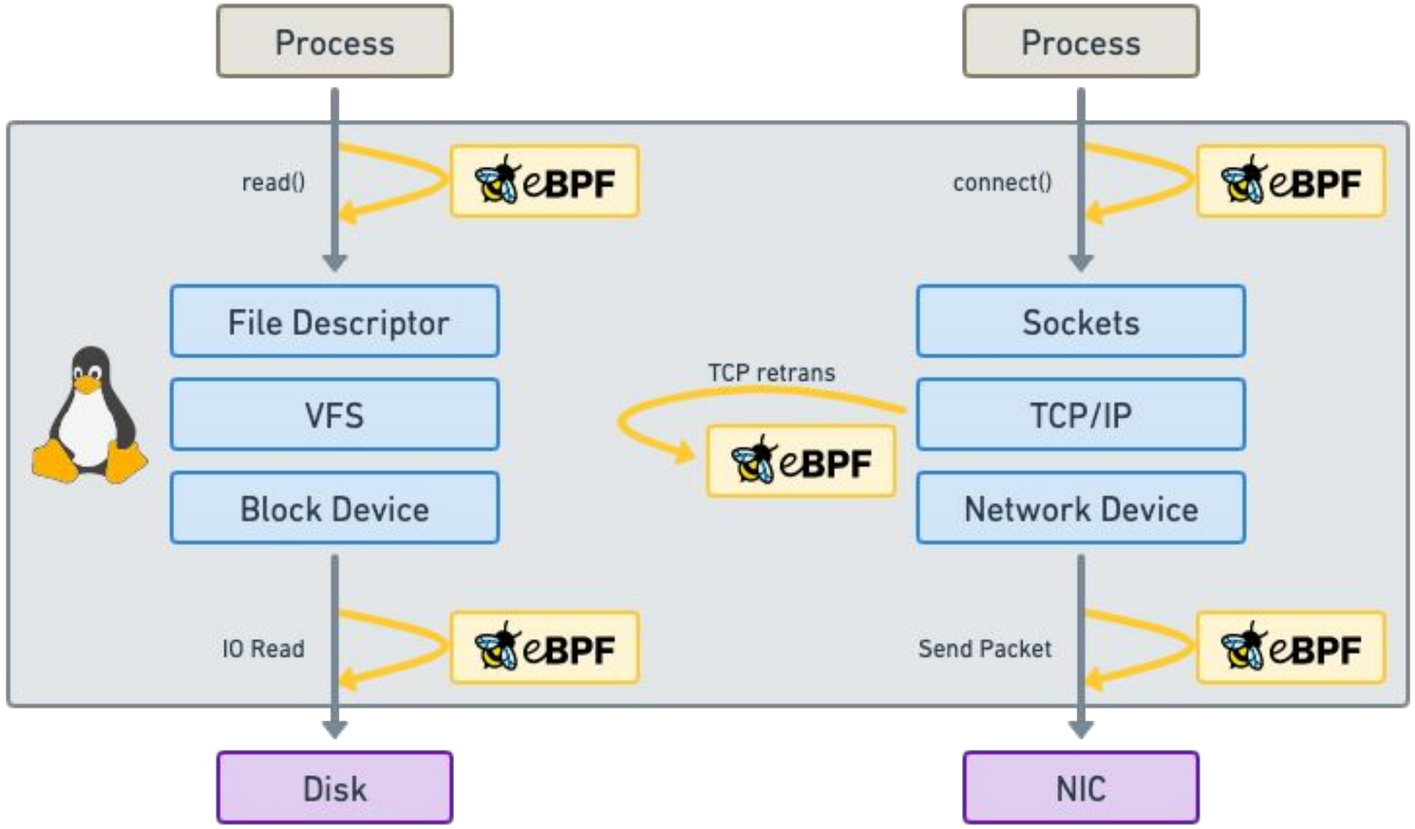



```c
int syscall__ret_execve(struct pt_regs *ctx)
{
        struct comm_event event = {
                .pid = bpf_get_current_pid_tgid() >> 32,
                .type = TYPE_RETURN,
        };

        bpf_get_current_comm(&event.comm, sizeof(event.comm));
        comm_events.perf_submit(ctx, &event, sizeof(event));

        return 0;
}
```

Run eBPF programs on events

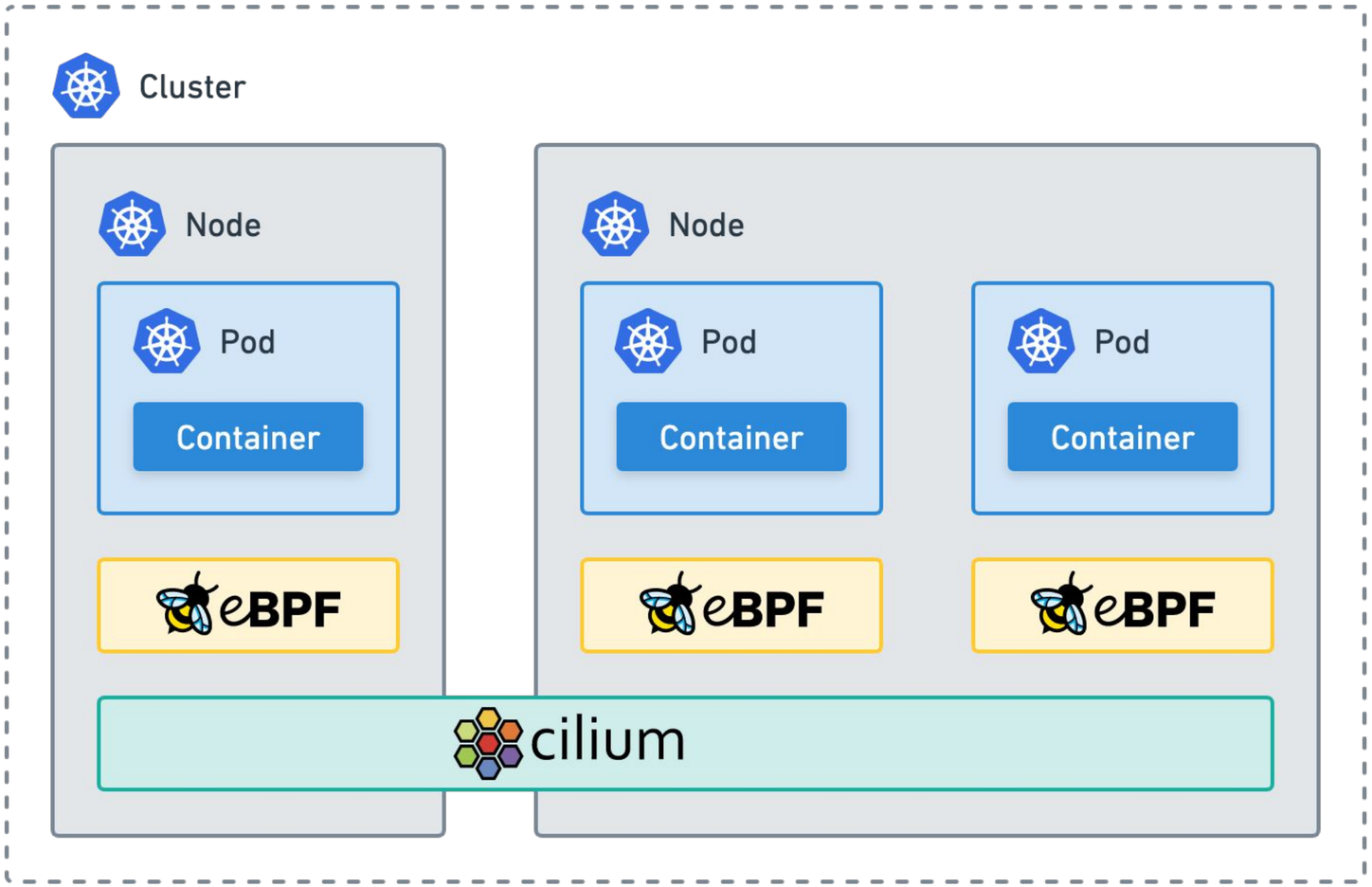


Attachment points

- Kernel functions (kprobes)
- Userspace functions (uprobe)
- System calls
- Tracepoints
- Sockets (data level)
- Network devices (packet level)
- Network device (DMA level) [XDP]
- ...


SPEAKEASY
PRODUCTIONS
eBPF
UNLOCKING
THE KERNEL
PREMIERING NOV 8TH
AT KUBECON + CLOUDNATIVECON CHICAGO
eBPF FOUNDATION
ISOVALENT
intel

Kubernetes Networking with Cilium



- Agent on each node
- Tunneling or Direct Routing
- eBPF native dataplane
- kube-proxy replacement.

cilium Service Mesh

Service Mesh

Ingress | Authentication | Traffic Management | spiffe | Gateway API

cilium hubble

Observability

Metrics | Tracing | Service Map | Logs | SIEM | fluentd | Grafana | OpenTelemetry

cilium CNI

Networking

Network Policy: DNS | L3/L4 | L7

Encryption: IPsec | Wireguard

Load-Balancing: K8s | Maglev | DSR

Networking: Multi-Cluster | NAT46 | IPv4 | IPv6 | Cloud SDN | BGP | Overlay | SRv6 | Egress Gateway

Runtime Security

Tetragon

SIEM | fluentd | Grafana

Observability

Enforcement

Kubernetes | Container | VM | Metal

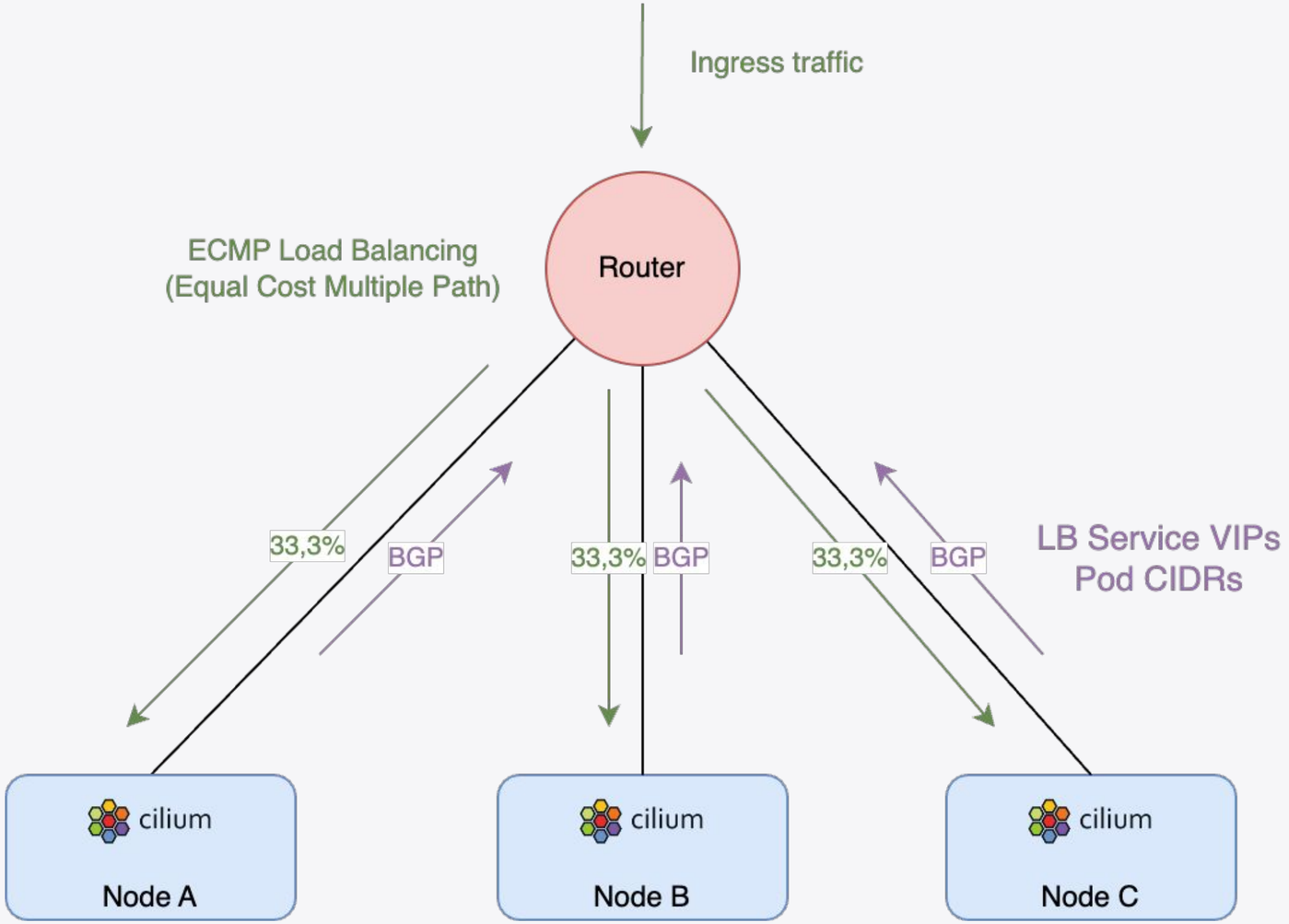
aws | Google Cloud | Azure | Alibaba Cloud | RED HAT OPENSHIFT | vmware

Cilium Networking Beyond Kubernetes (Agenda)

- Datacenter / Corporate network integration
  - Exposing cluster Services in an on-prem network
    - BGP Control Plane
    - L2 Announcements
    - Standalone L4LB
  - Passing traffic over corporate firewalls
    - Egress Gateway
- Multi-Cluster connectivity
  - Cluster Mesh
- Interconnecting clusters with external networks
  - NAT46/64 Gateway
  - SRv6

Datacenter / Corporate Network Integration

BGP Control Plane - Announcing Cluster Prefixes to the Network



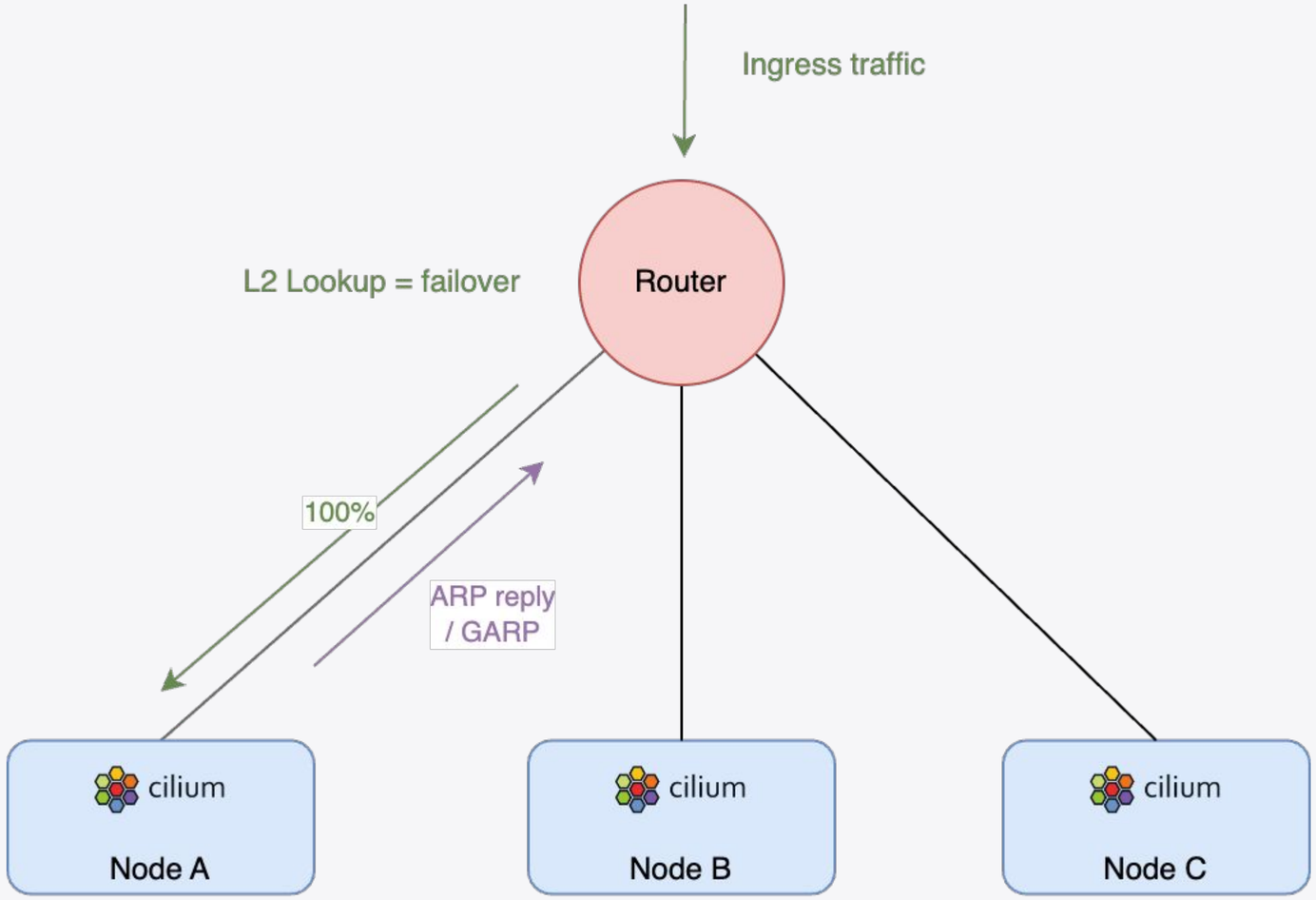

```yaml
apiVersion: v1
kind: Service
metadata:
 name: my-service
spec:
 selector:
   app.kubernetes.io/name: MyApp
 ports:
   - protocol: TCP
     port: 80
 type: LoadBalancer
status:
 loadBalancer:
   ingress:
   - ip: 1.2.3.4
```

Announcing LB Service IPs & Pod CIDRs over BGP

```yaml
apiVersion: "cilium.io/v2alpha1"
kind: CiliumLoadBalancerIPPool
metadata:
  name: "blue-pool"
spec:
  cidrs:
  - cidr: "20.0.10.0/24"
  serviceSelector:
    matchExpressions:
       - {key: color, operator: In, values: [blue]}
```

```yaml
apiVersion: "cilium.io/v2alpha1"
kind: CiliumBGPPeeringPolicy
metadata:
 name: 01-bgp-peering-policy
spec:
 nodeSelector:
   matchLabels:
     bgp-policy: bgp-node
 virtualRouters:
 - localASN: 64512
   exportPodCIDR: true
   serviceSelector:
      matchExpressions:
           - {key: color, operator: In, values: [blue]}
   neighbors:
    - peerAddress: 172.16.30.100
      peerASN: 64512
```

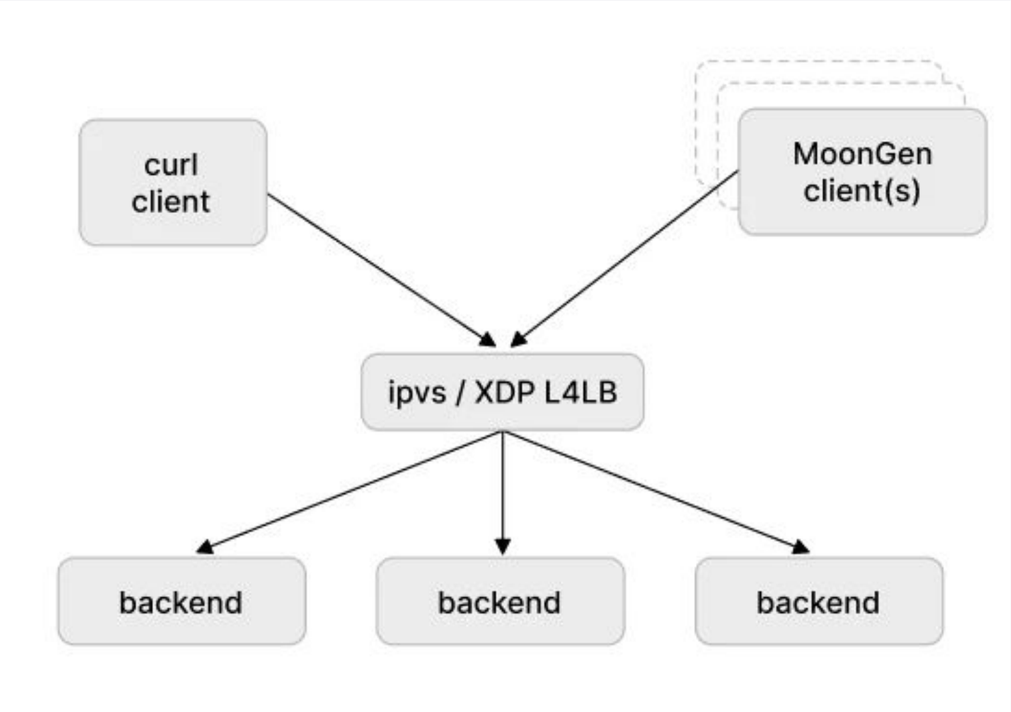
L2 Announcements

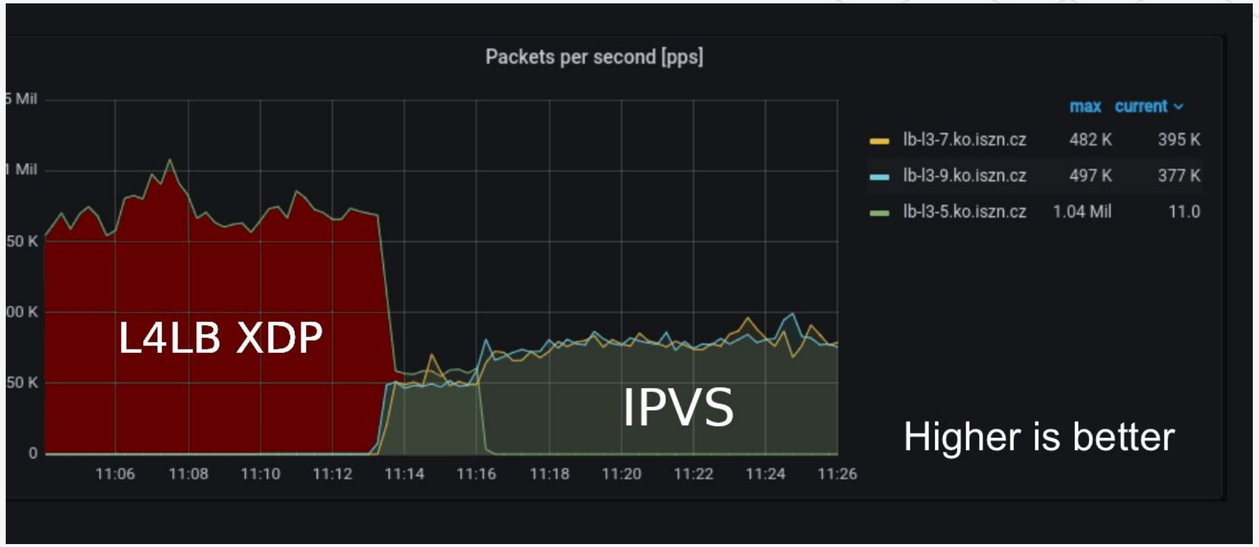


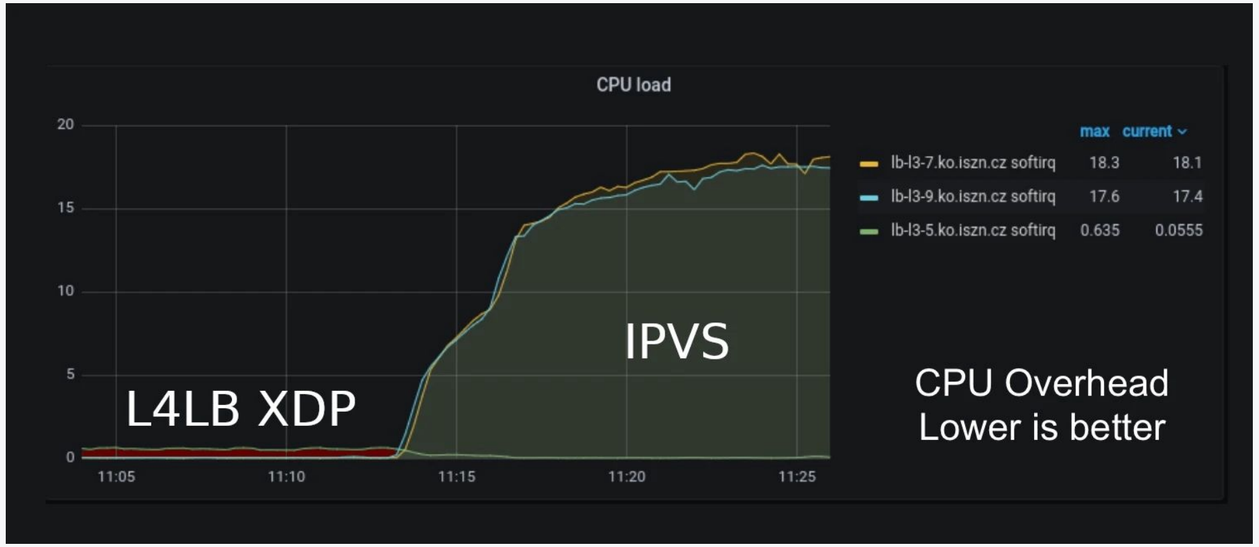

```yaml
apiVersion: "cilium.io/v2alpha1"
kind: CiliumL2AnnouncementPolicy
metadata:
  name: policy1
spec:
  serviceSelector:
    matchLabels:
      color: blue
  nodeSelector:
    matchExpressions:
      - key: node-role.kubernetes.io/control-plane
        operator: DoesNotExist
  interfaces:
  - ^eth[0-9]+
  externalIPs: true
   loadBalancerIPs: true
```

Standalone L4LB

XDP (eXpress Data Path) -based Load Balancer that can be used standalone (non-CNI / non K8s mode):

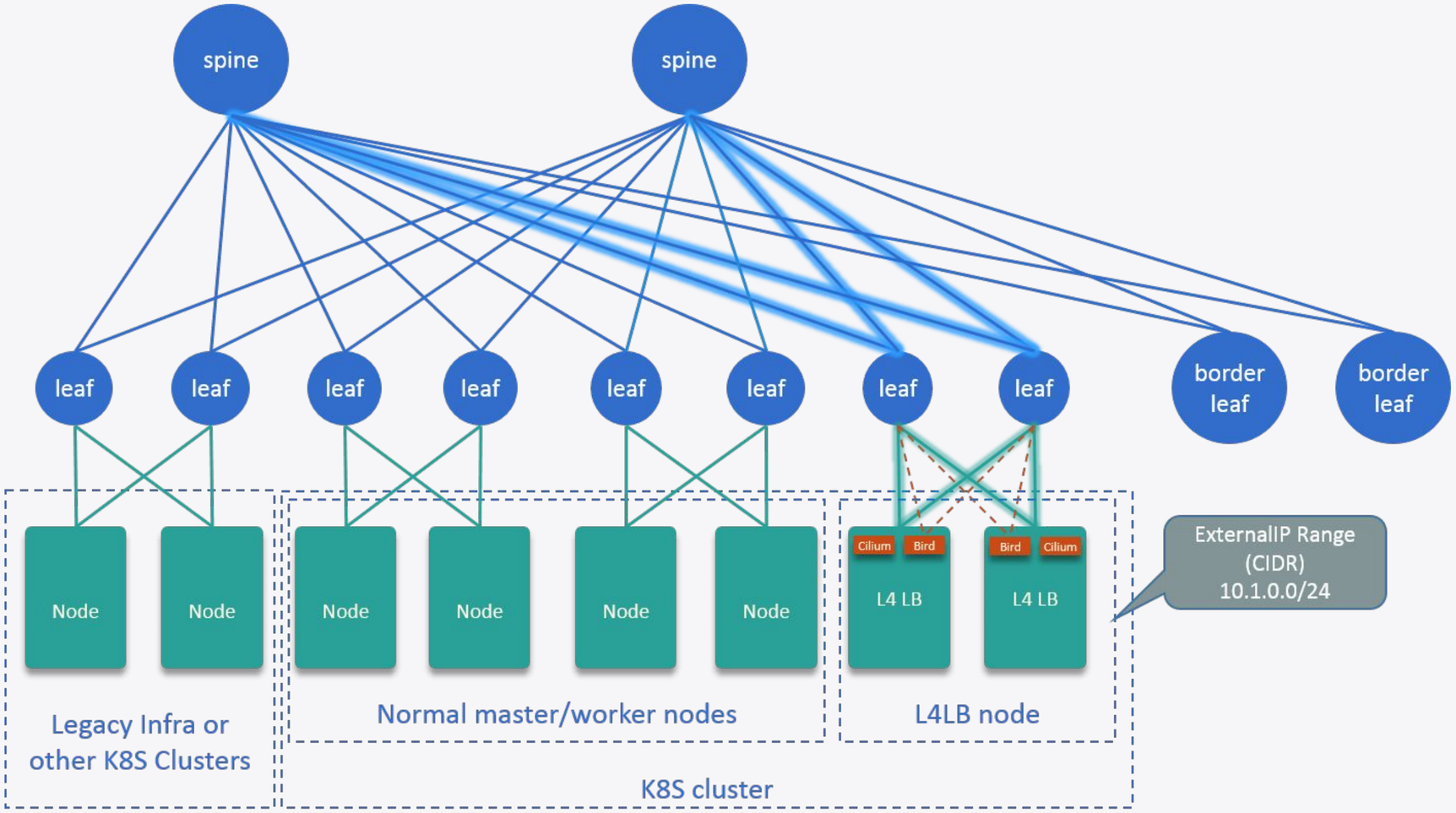






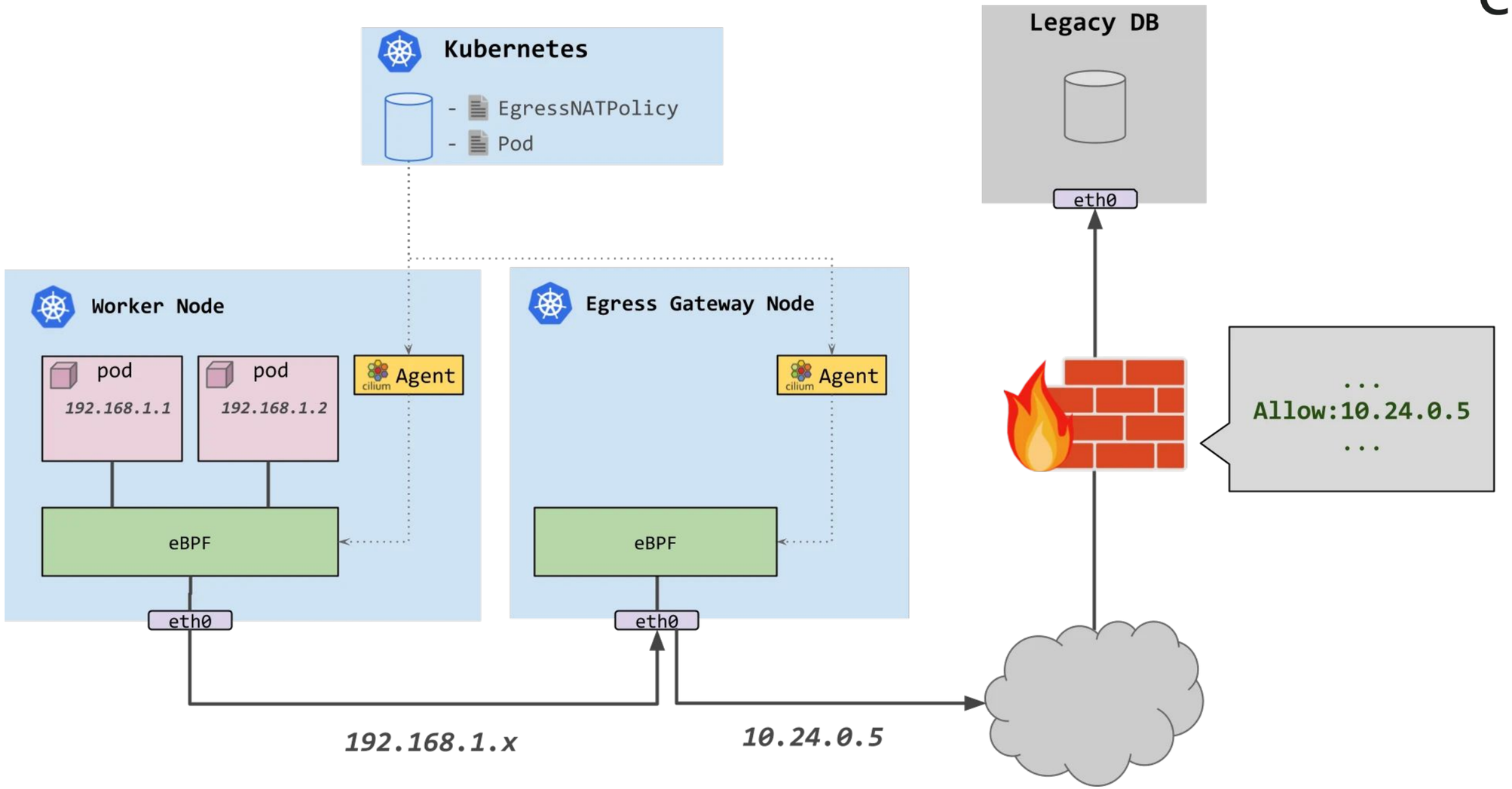
https://cilium.io/blog/2022/04/12/cilium-standalone-L4LB-XDP/

Standalone L4LB (Datacenter Example)



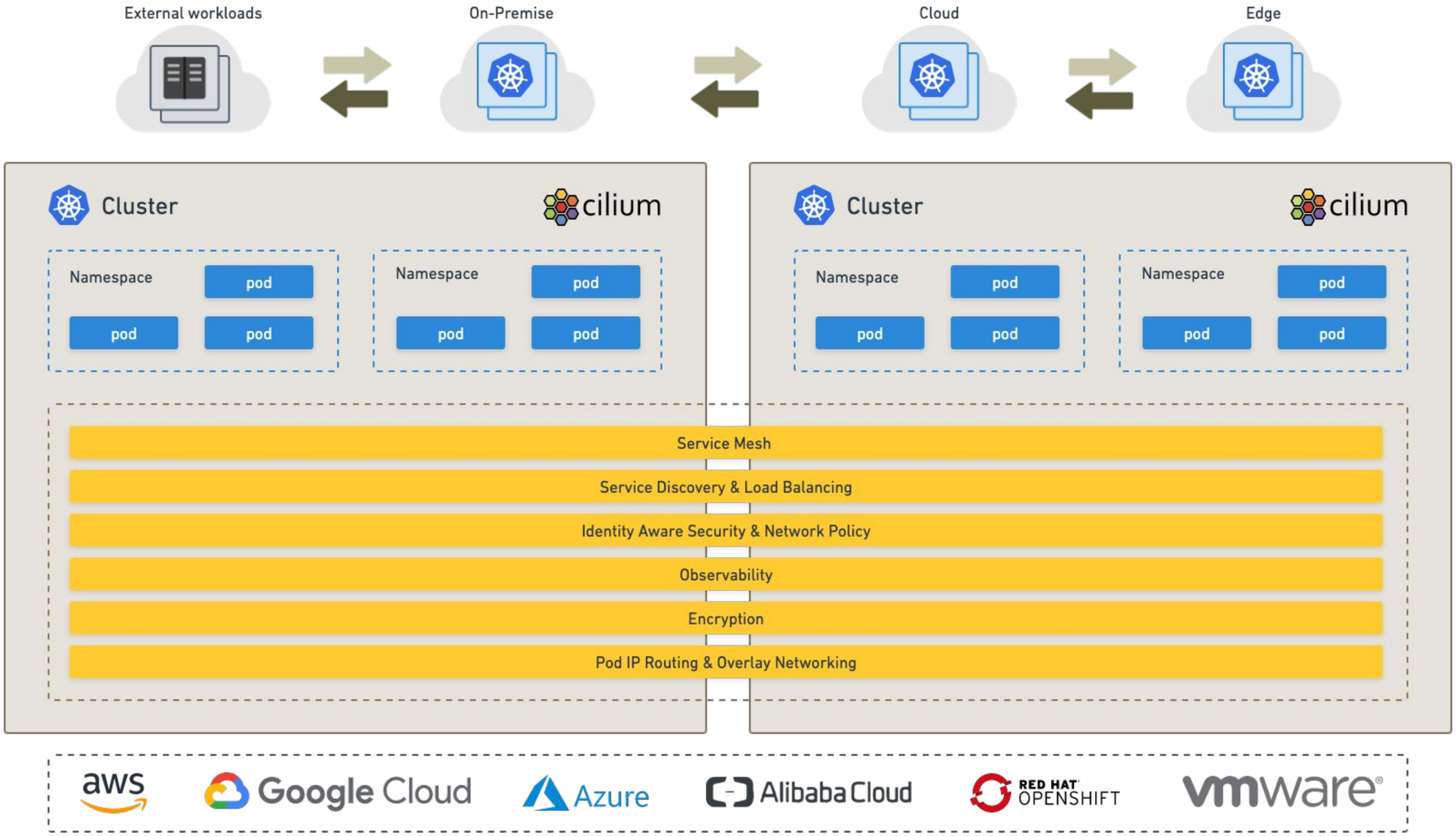
https://arthurchiao.art/blog/k8s-l4lb/

Egress Gateway

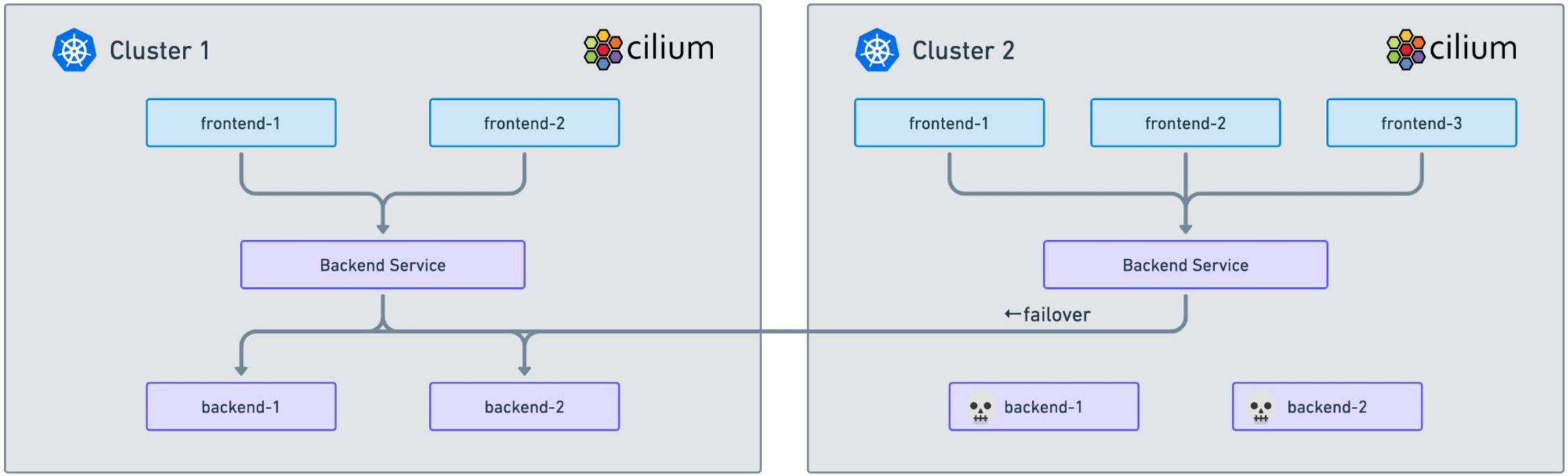


Multi-Cluster Connectivity (Cluster Mesh)

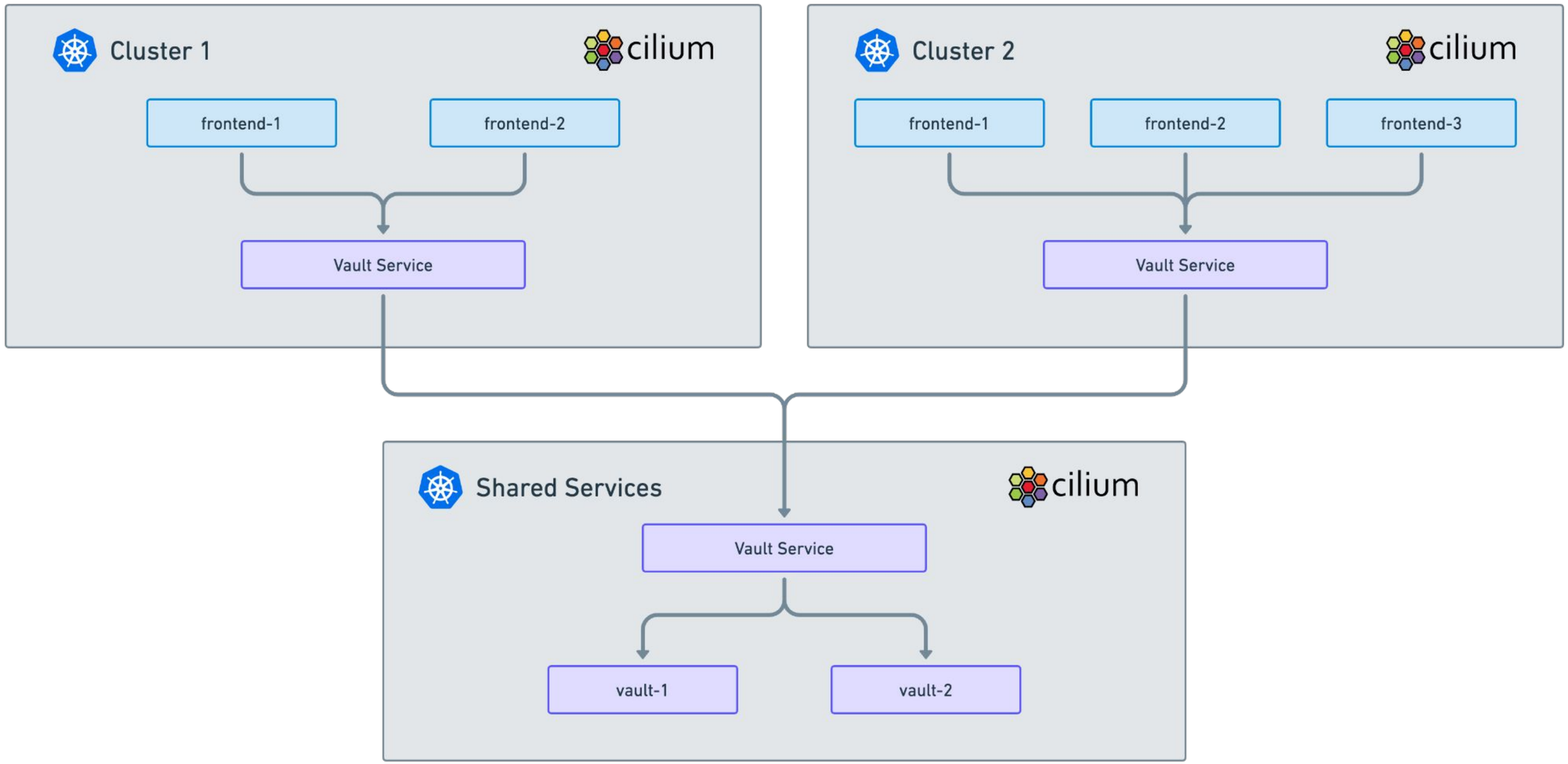
Cluster Mesh - Introduction



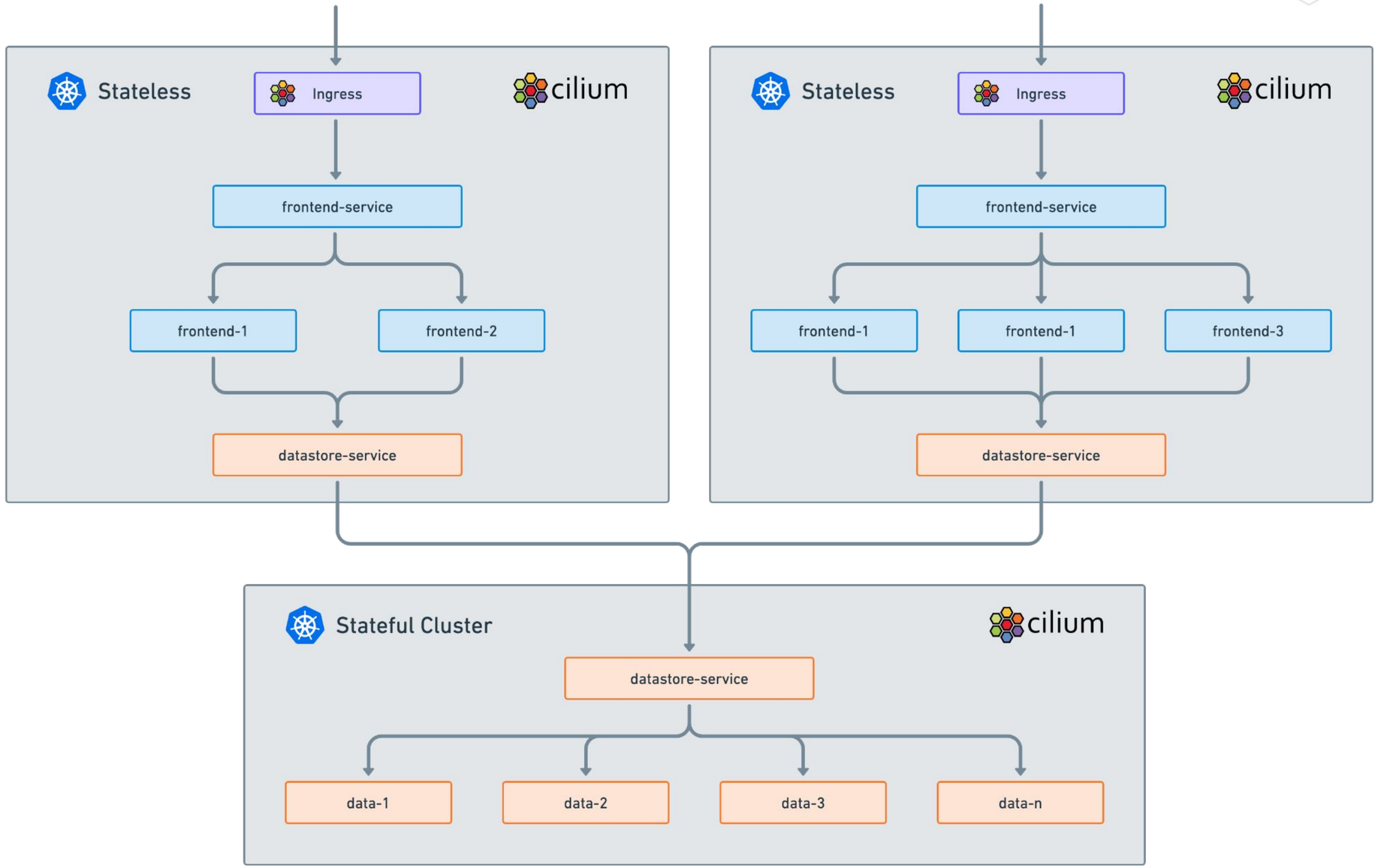
Cluster Mesh - High Availability



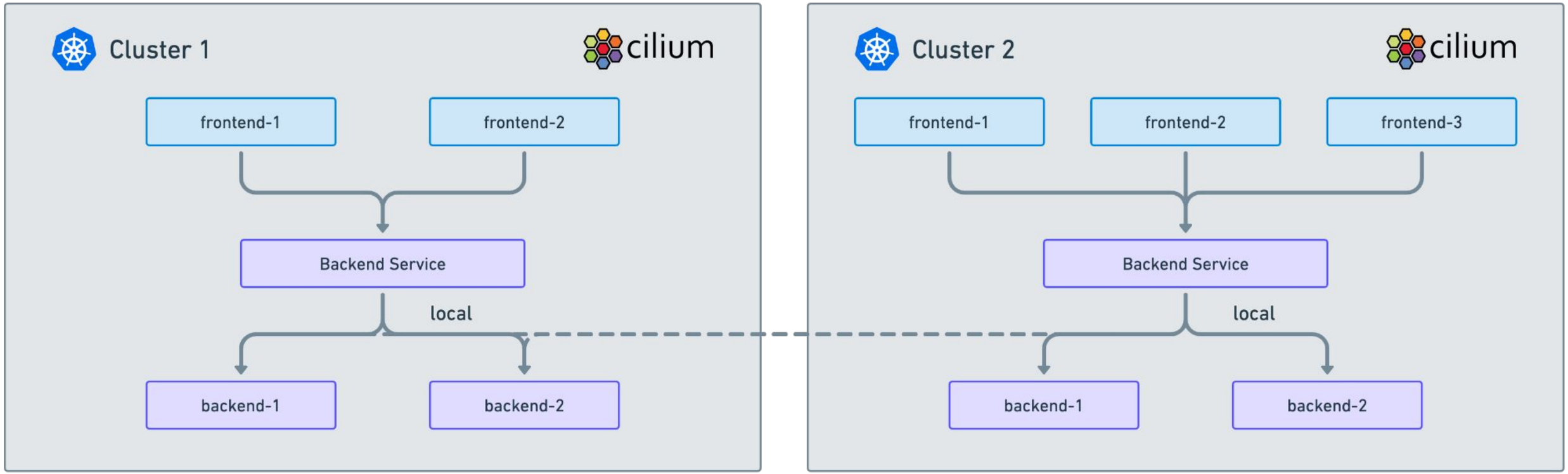
Cluster Mesh - Shared Services



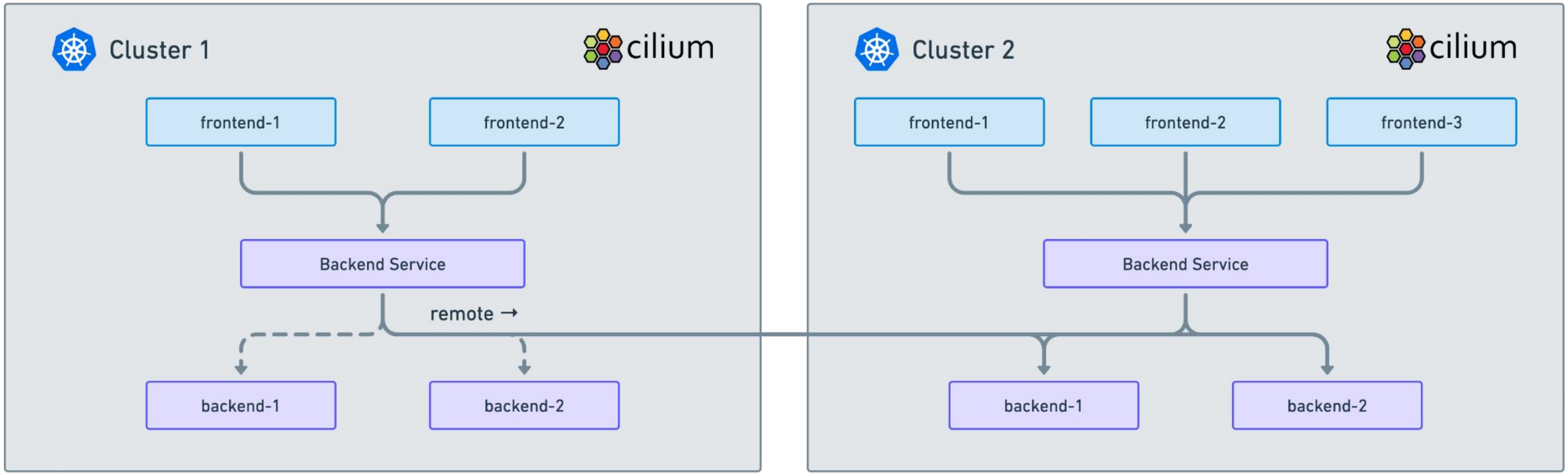
Cluster Mesh - Splitting Services



Cluster Mesh - Local Service Affinity



Cluster Mesh - Remote Service Affinity



Cluster Mesh - Local Service Affinity


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

Cluster Mesh - Remote Service Affinity

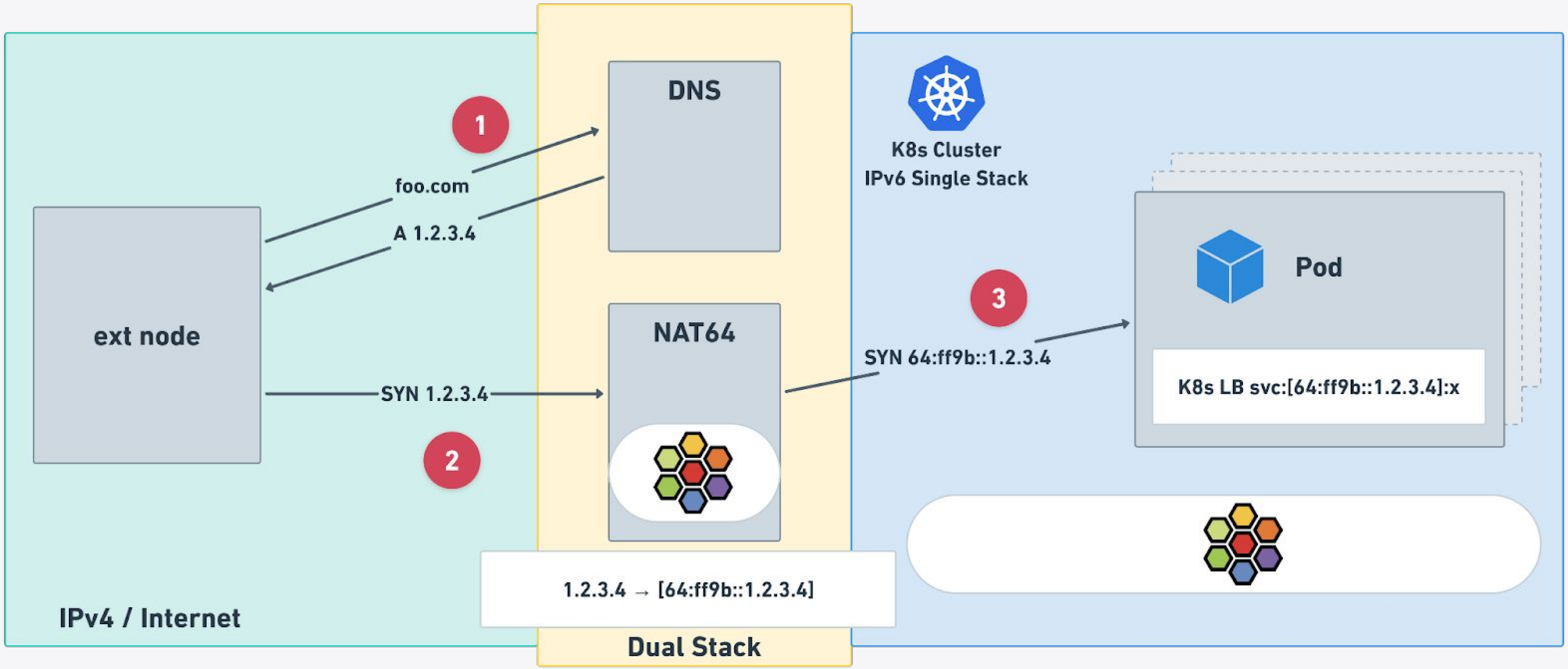

```yaml
apiVersion: v1
kind: Service
metadata:
  name: backend-service
  annotations:
    io.cilium/global-service: "true"
    io.cilium/service-affinity: remote
spec:
  type: ClusterIP
  ports:
  - port: 80
  selector:
    name: backend
```

Cluster Mesh - Cilium Network Policies


```yaml
apiVersion: "cilium.io/v2"
kind: CiliumNetworkPolicy
metadata:
  name: "ingress-to-rebel-base"
spec:
  description: "Allow x-wing in cluster-1 to contact rebel-base in cluster2"
  endpointSelector:
    matchLabels:
      name: rebel-base
      io.cilium.k8s.policy.cluster: cluster-2
  ingress:
  - fromEndpoints:
    - matchLabels:
        name: x-wing
        io.cilium.k8s.policy.cluster: cluster-1
    toPorts:
    - ports:
      - port: "80"
        protocol: TCP
```

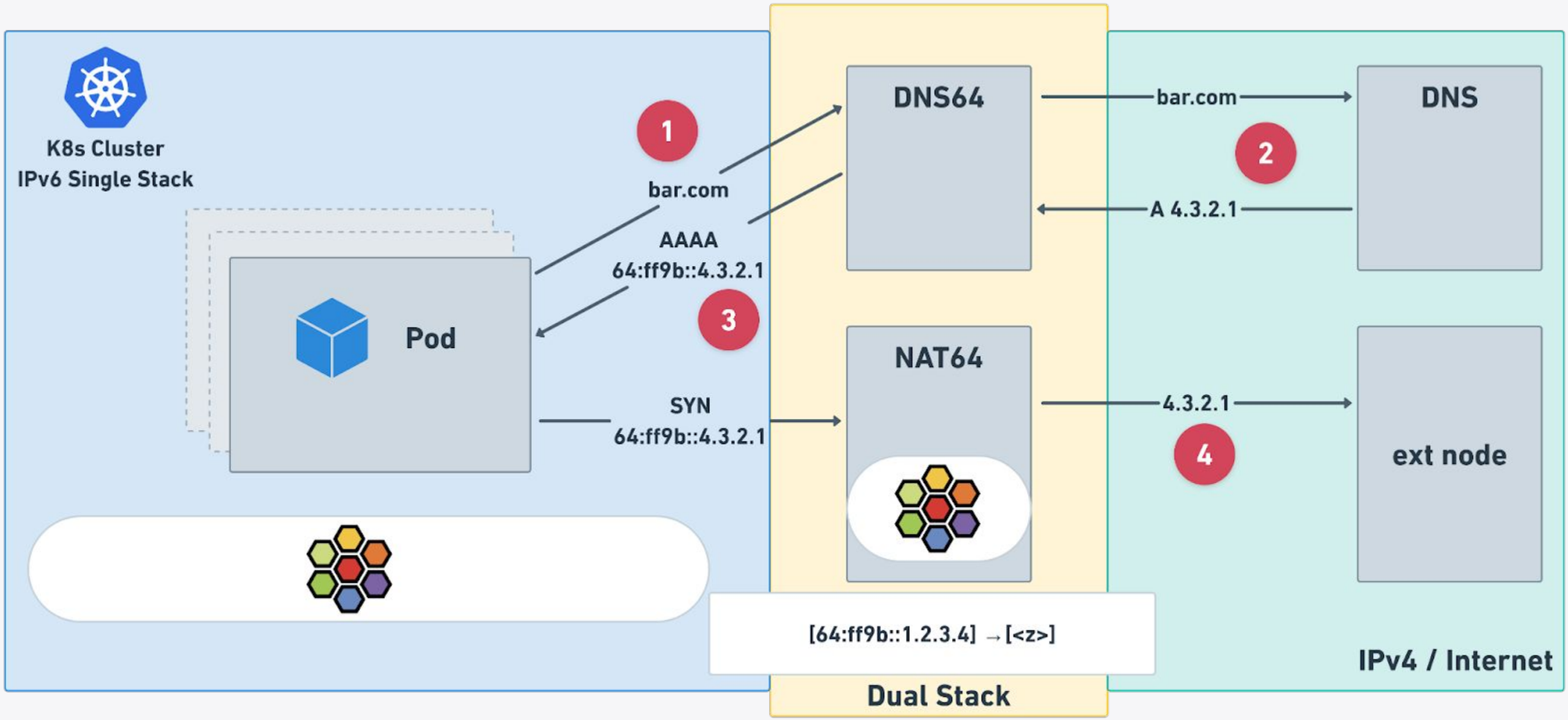
Interconnecting Clusters with External Networks

Dual-Stack via NAT46/64 Gateway - Ingress



https://isovalent.com/blog/post/cilium-release-113/

Dual-Stack via NAT46/64 Gateway - Egress

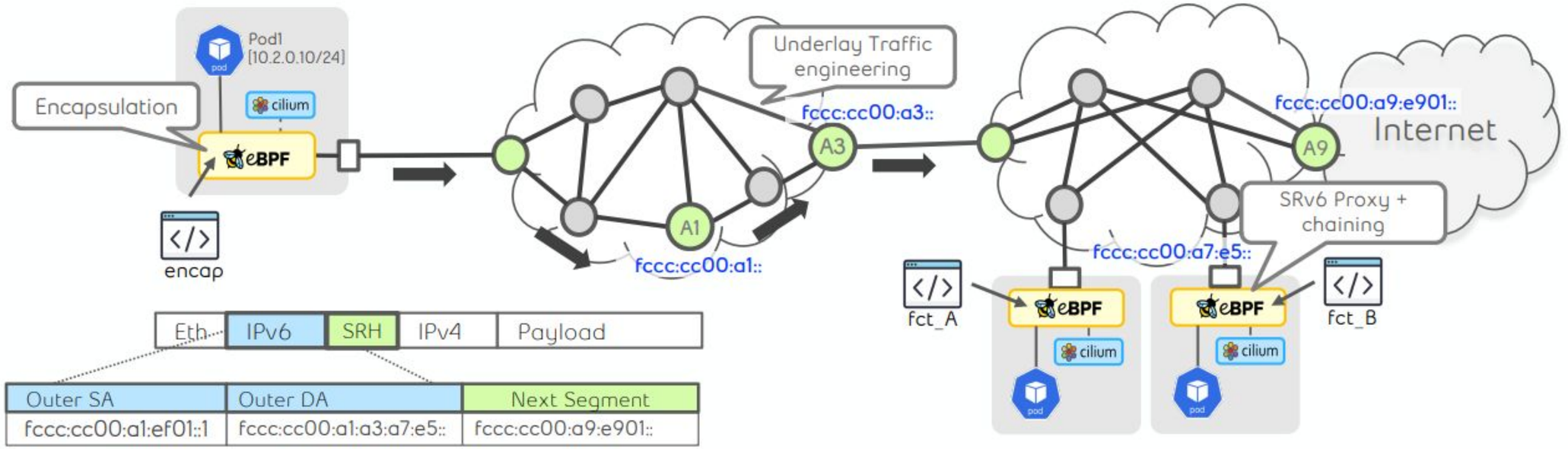


https://isovalent.com/blog/post/cilium-release-113/

Segment Routing for IPv6 (SRv6)

Network programming framework built on IPv6 (RFC8986)

- Leverages Source Routing paradigm (path is encoded at source)
- Packet processing program encoded as a sequence of instructions in the IPv6 packet header
- Traffic Engineering, VPNs, Network Service Function Chaining etc. natively via any IPv6 network



Simplifying and Making the Network Programmable with Kubernetes and SRv6 - KubeCon NA 2022: Daniel Bernier, Bell Canada & Louis De Los Santos, Isovalent

Visit our labs to learn more about Cilium

Learn more!

ISOVALENT

For the Enterprise

Hardened, enterprise-grade eBPF-powered networking, observability, and security.

isovalent.com/product
isovalent.com/labs

OSS Community

eBPF-based Networking, Observability, Security

cilium.io
cilium.slack.com
Regular news

Base technology

The revolution in the Linux kernel, safely and efficiently extending the capabilities of the kernel.

ebpf.io
What is eBPF? - ebook

ISOVALENT

Thank you!

ISOVALENT

Agenda

- Cilium & eBPF Introduction
- Networking
- Security
- Observability
- Cilium Mesh
  - Cluster Mesh
  - Service Mesh
- Tetragon

Cilium & eBPF

Introduction

- Open Source Projects

ISOVALENT

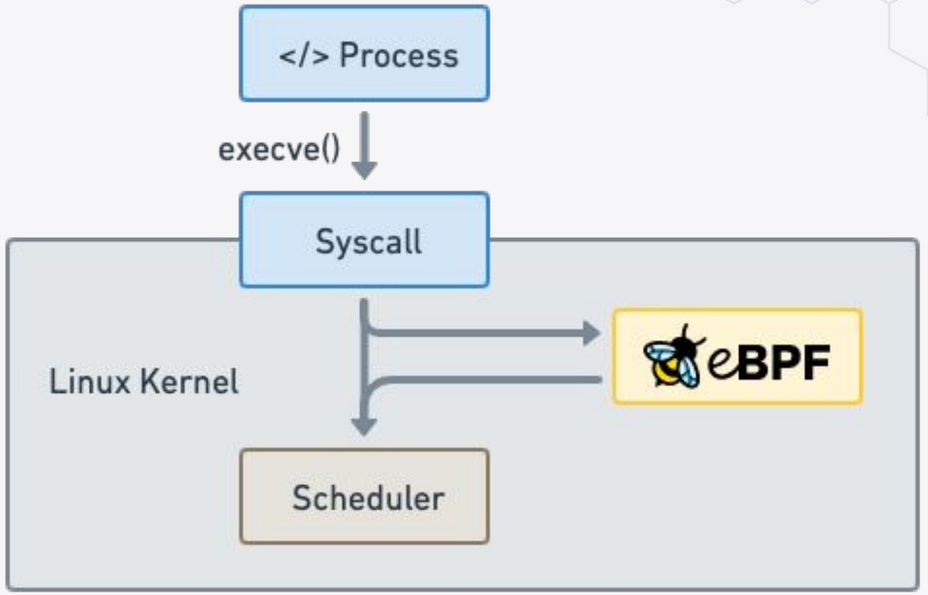
- Company behind Cilium
- Provides Cilium Enterprise


eBPF

eBPF

Makes the Linux kernel programmable in a secure and efficient way.

“What JavaScript is to the browser, eBPF is to the Linux Kernel”

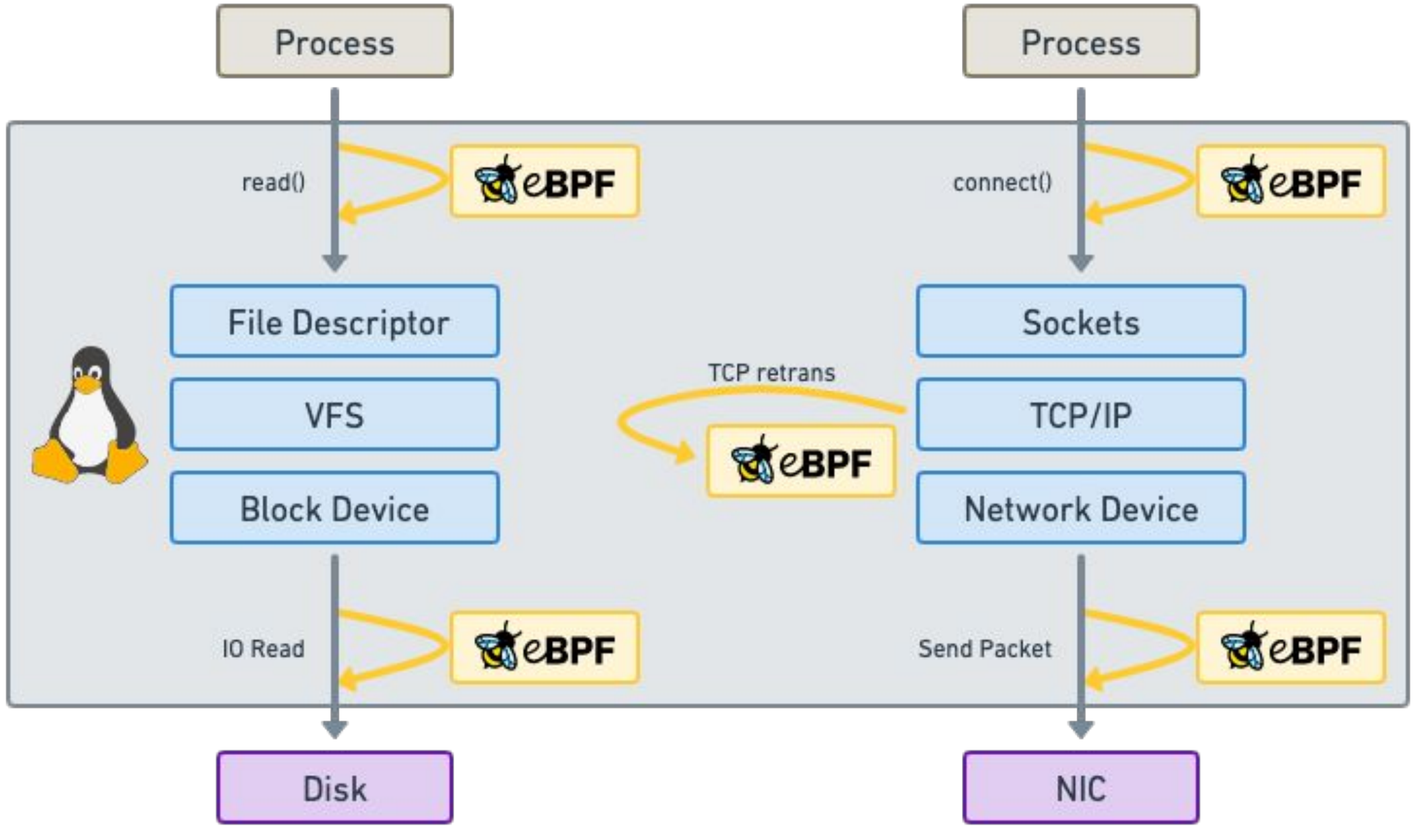



```c
int syscall__ret_execve(struct pt_regs *ctx)
{
        struct comm_event event = {
                .pid = bpf_get_current_pid_tgid() >> 32,
                .type = TYPE_RETURN,
        };

        bpf_get_current_comm(&event.comm, sizeof(event.comm));
        comm_events.perf_submit(ctx, &event, sizeof(event));

        return 0;
}
```

Run eBPF programs on events



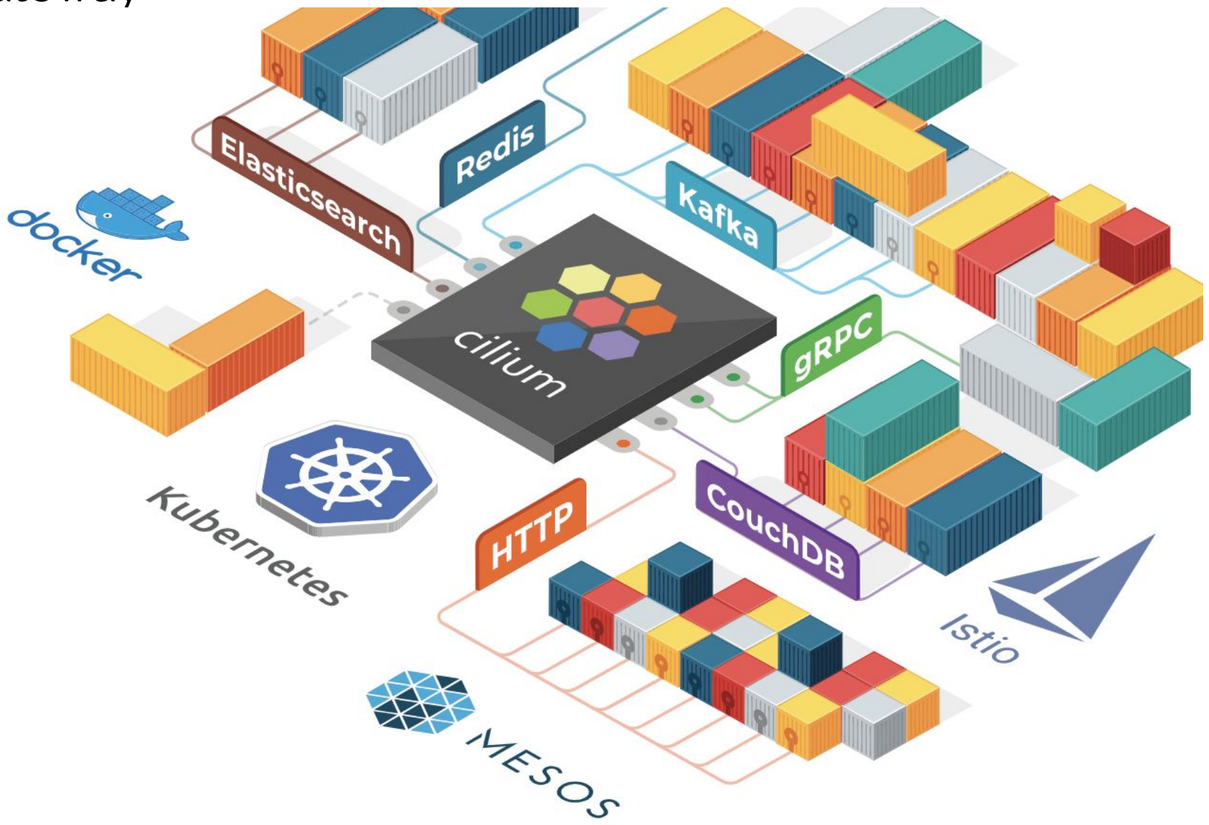
Attachment points

- Kernel functions (kprobes)
- Userspace functions (uprobe)
- System calls
- Tracepoints
- Sockets (data level)
- Network devices (packet level)
- Network device (DMA level) [XDP]
- ...

What is Cilium?

- **Networking & Load-Balancing**
  - CNI, Kubernetes Services, Multi-cluster, VM Gateway
- **Network Security**
  - Network Policy, Identity-based, Encryption
- **Observability**
  - Metrics, Flow Visibility, Service Dependency

At the foundation of Cilium is the new Linux kernel technology eBPF, which enables the dynamic insertion of powerful security, visibility, and networking control logic within Linux itself. Besides providing traditional network level security, the flexibility of BPF enables security on API and process level to secure communication within a container or pod.
Read More



cilium Service Mesh

Service Mesh

Ingress | Authentication | Traffic Management | spiffe | Gateway API

cilium hubble

Observability

Metrics | Tracing | Service Map | Logs | SIEM | fluentd | Grafana | OpenTelemetry

cilium CNI

Networking

Network Policy: DNS | L3/L4 | L7

Encryption: IPsec | Wireguard

Load-Balancing: K8s | Maglev | DSR

Networking: Multi-Cluster | 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 OPENSHIFT | vmware

cilium

Created by ISOVALENT

eBPF-based:

- Networking
- Security
- Observability
- Service Mesh & Ingress

Foundation

CLOUD NATIVE COMPUTING FOUNDATION

Technology

eBPF envoy

Building a Global Multi Cluster Gaming Infrastructure with Cilium

---

What Makes a Good Multi-tenant Kubernetes Solution

Building a Secure and Maintainable PaaS

Building High-Performance Cloud-Native Pod Networks

Scaling a Multi-Tenant k8s Cluster in a Telco

First step towards cloud native networking

Cloud Native Networking with eBPF

Managed Kubernetes: 1.5 Years of Cilium Usage at DigitalOcean

---

Google chooses Cilium for Google Kubernetes Engine (GKE) networking

---

Why eBPF is changing the Telco networking space?

Kubernetes Network Policies in Action with Cilium

AWS picks Cilium for Networking & Security on EKS Anywhere

Scaleway uses Cilium as the default CNI for Kubernetes Kapsule

---

Sportradar is using Cilium as their main CNI plugin in AWS (using kops)

Utmost is using Cilium in all tiers of its Kubernetes ecosystem to implement zero trust

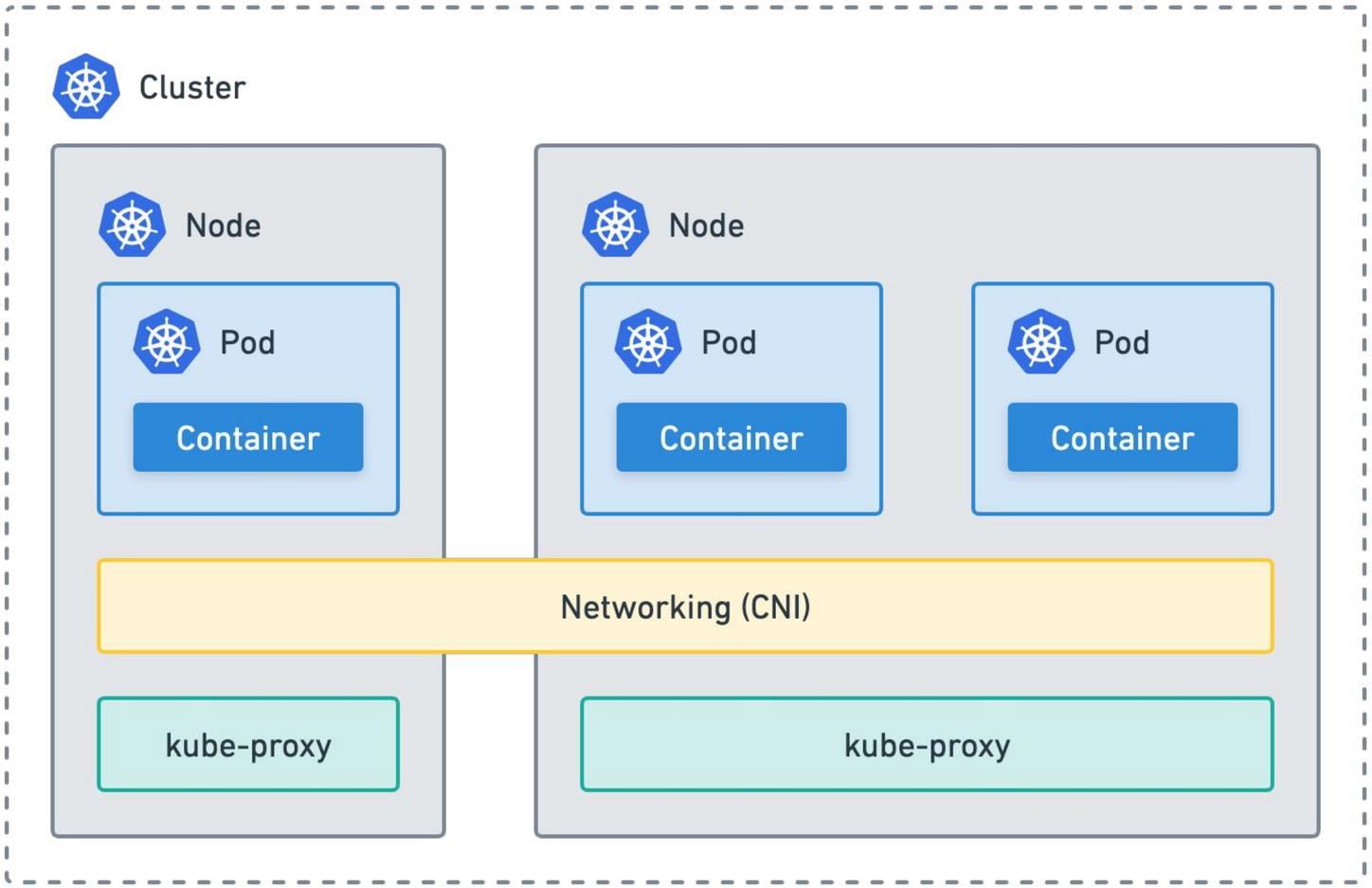
---

Yahoo is using Cilium for L4 North-South Load Balancing for Kubernetes Services

ISOVALENT

Networking

Kubernetes Networking



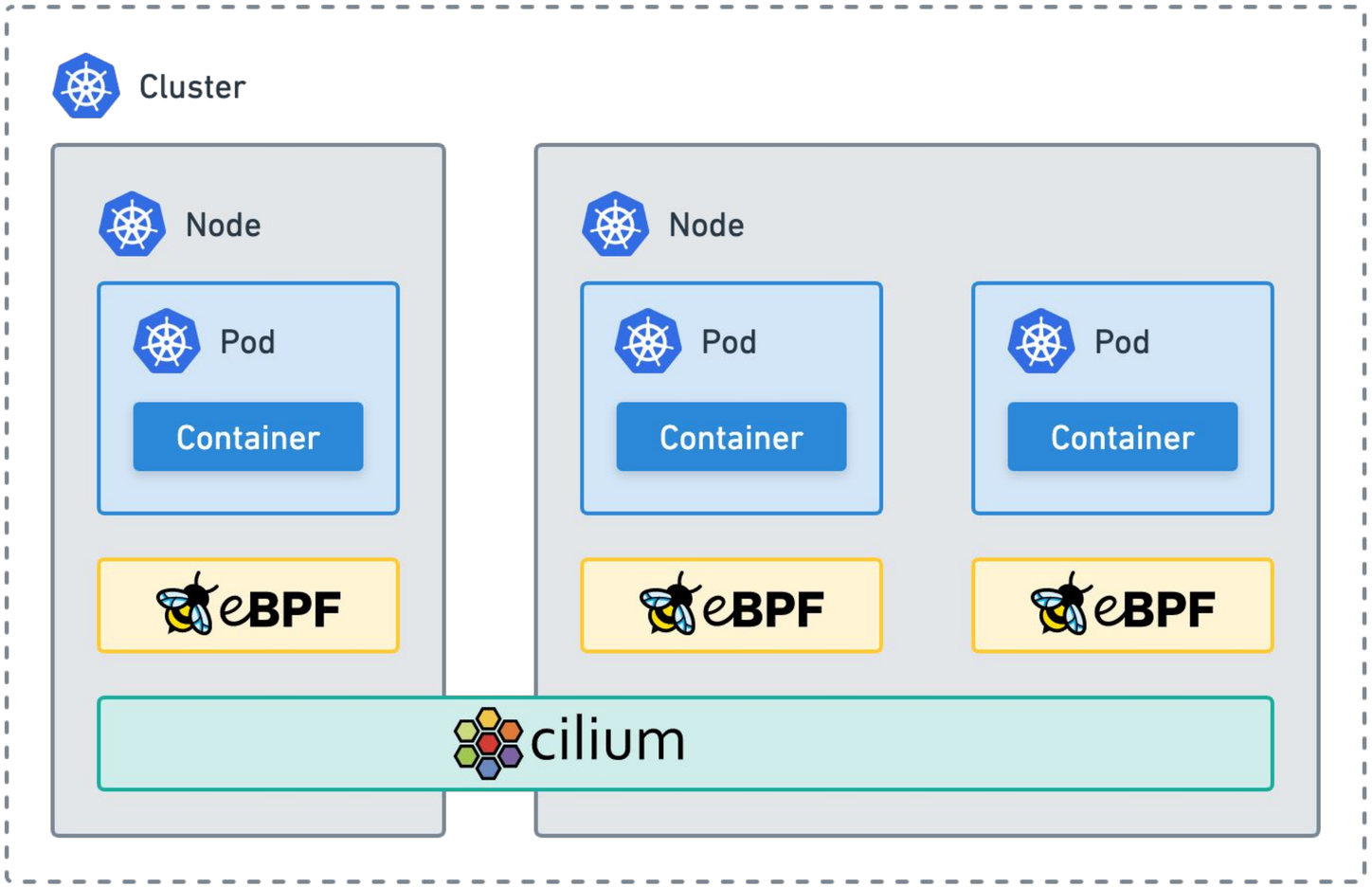
Networking plugin

- Network devices
- IP Address Management
- Intra-node connectivity
- Inter-node connectivity

Kube Proxy

- Services
- iptables or ipvs
- Service discovery

Kubernetes Networking

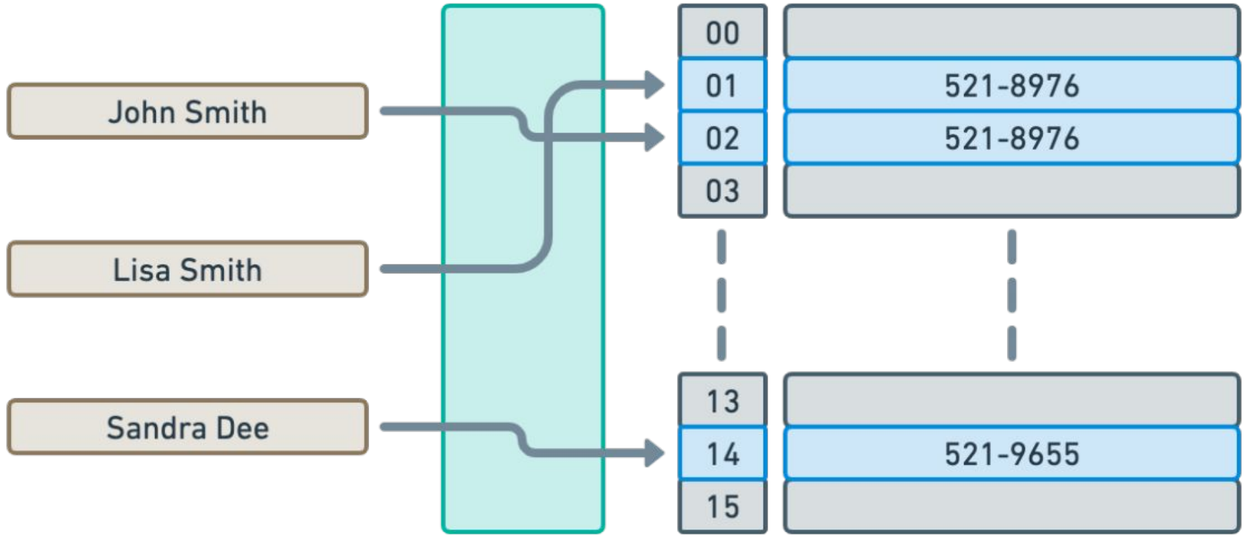


- Agent on each node
- Tunneling or Direct Routing
- eBPF native dataplane
- kube-proxy replacement.

Kubernetes Services

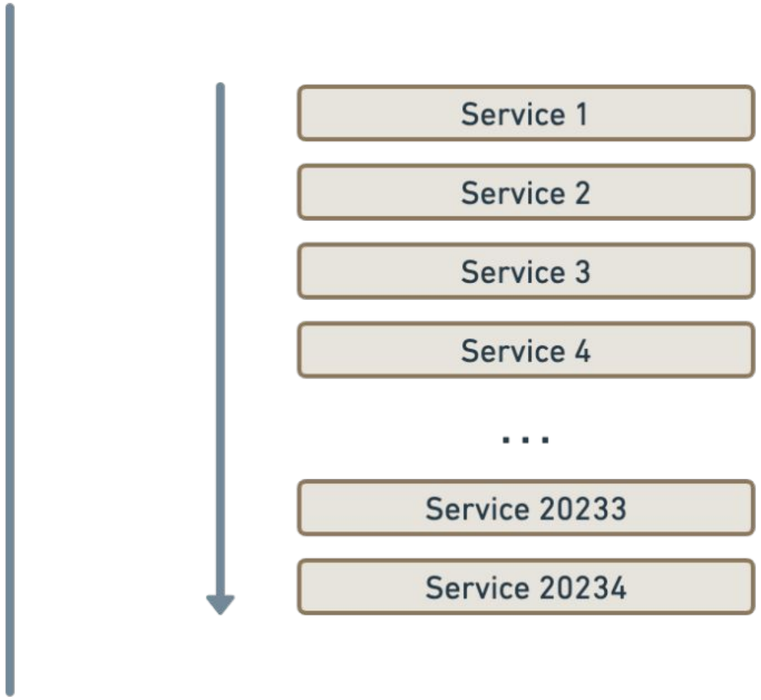
eBPF based

- Per-CPU hash table

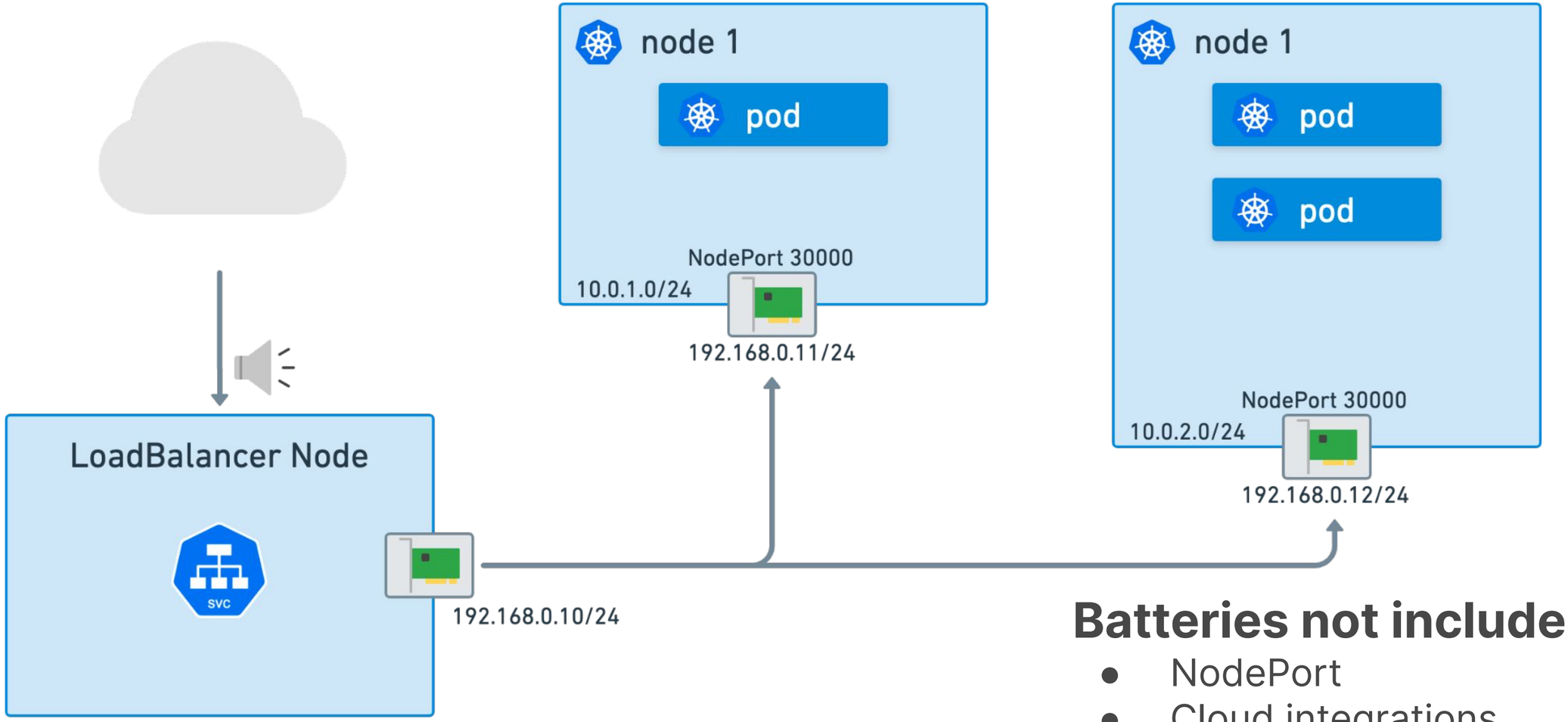


kube-proxy

- Linear list
- All rules have to be replaced as a whole



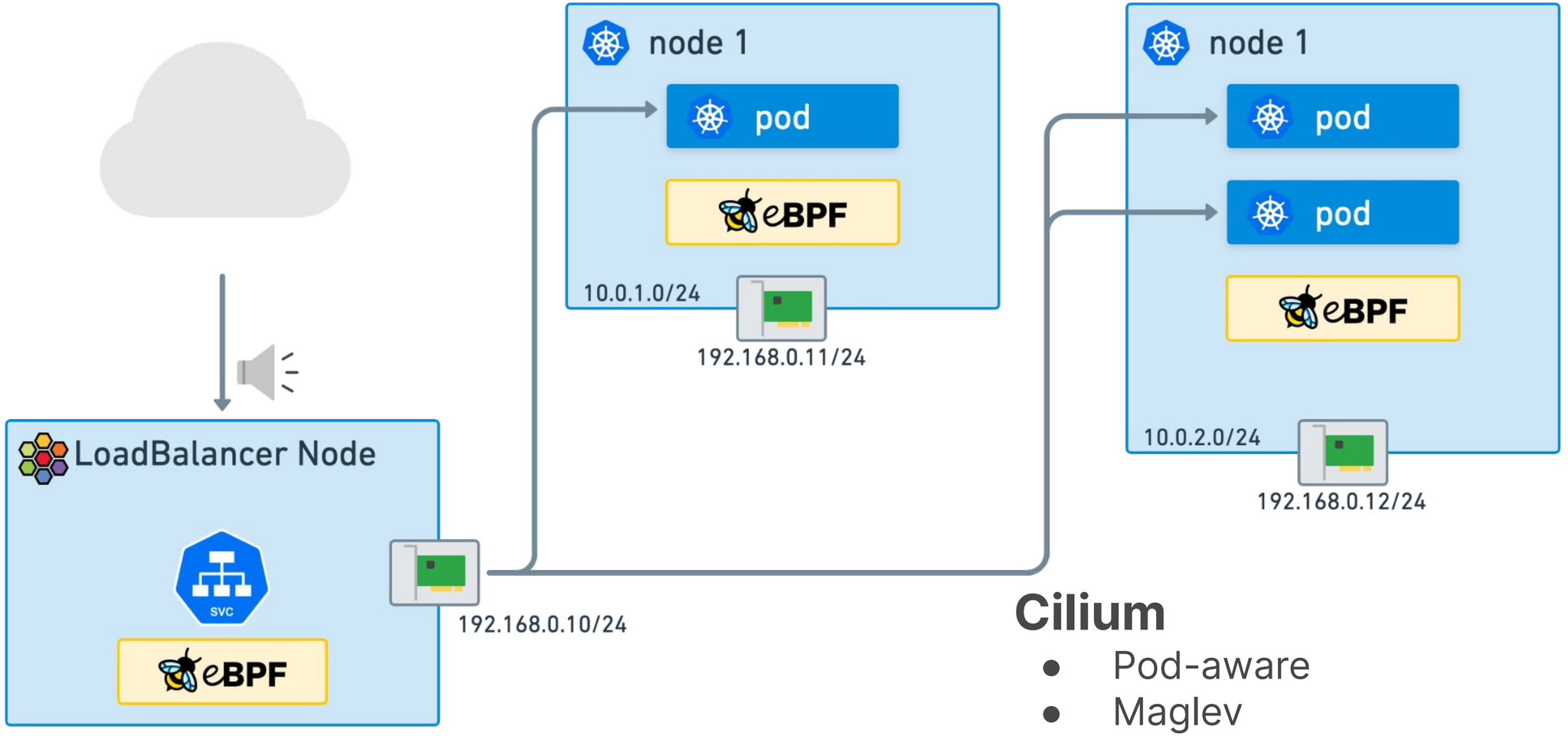
Load Balancing



Batteries not included

- NodePort
- Cloud integrations

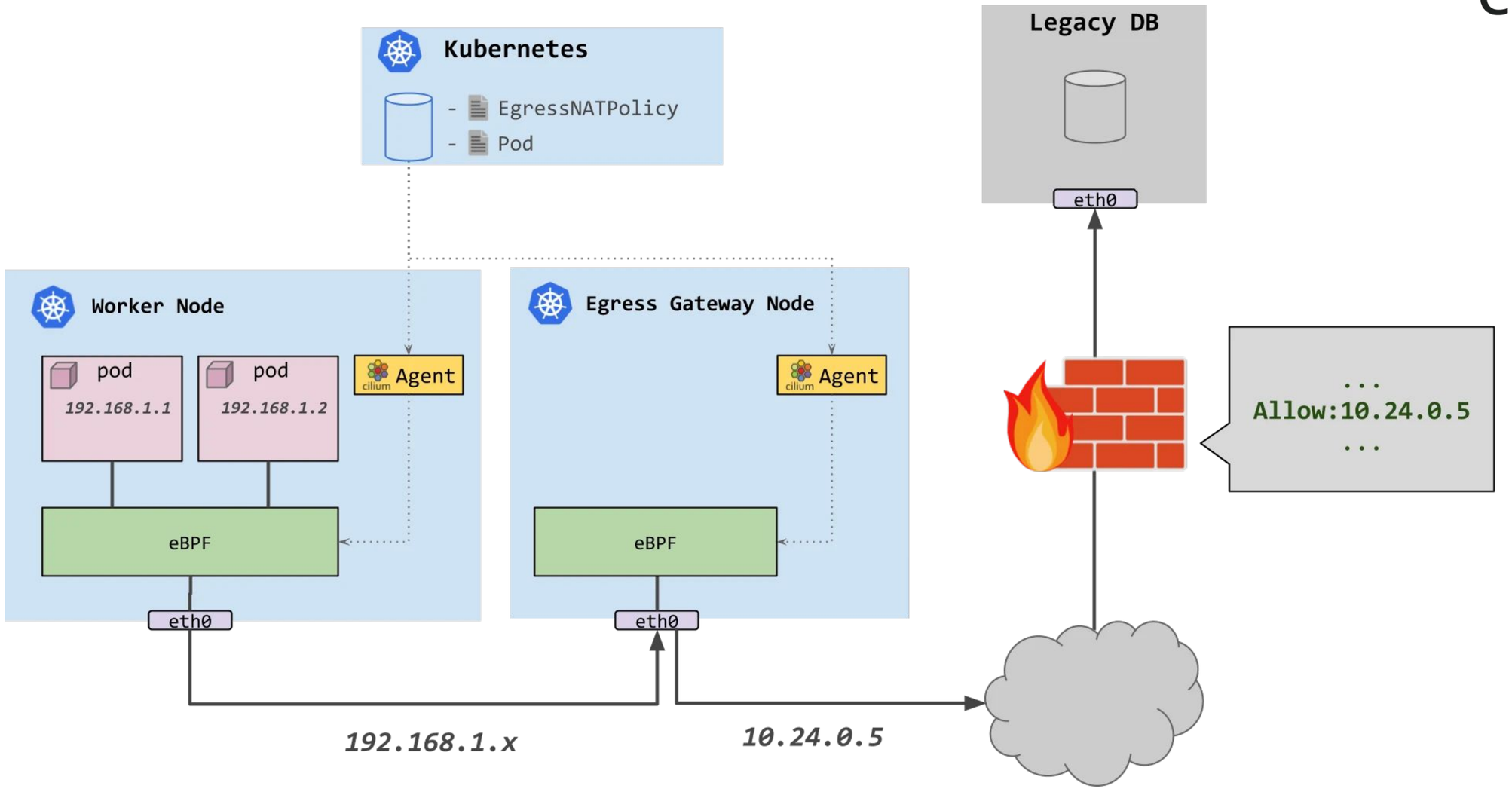
Load Balancing



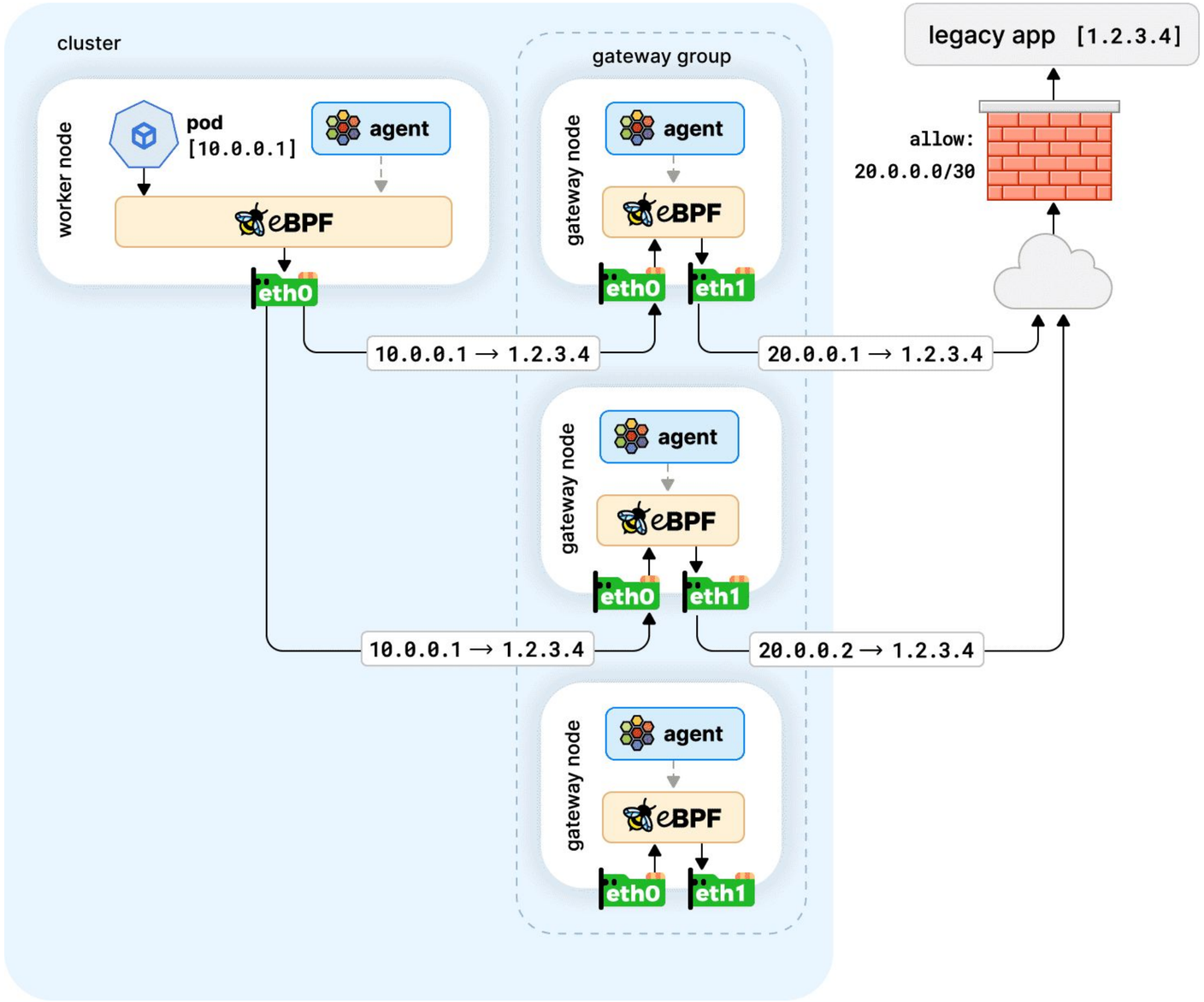
Cilium

- Pod-aware
- Maglev
- Standalone or distributed

Egress Gateway

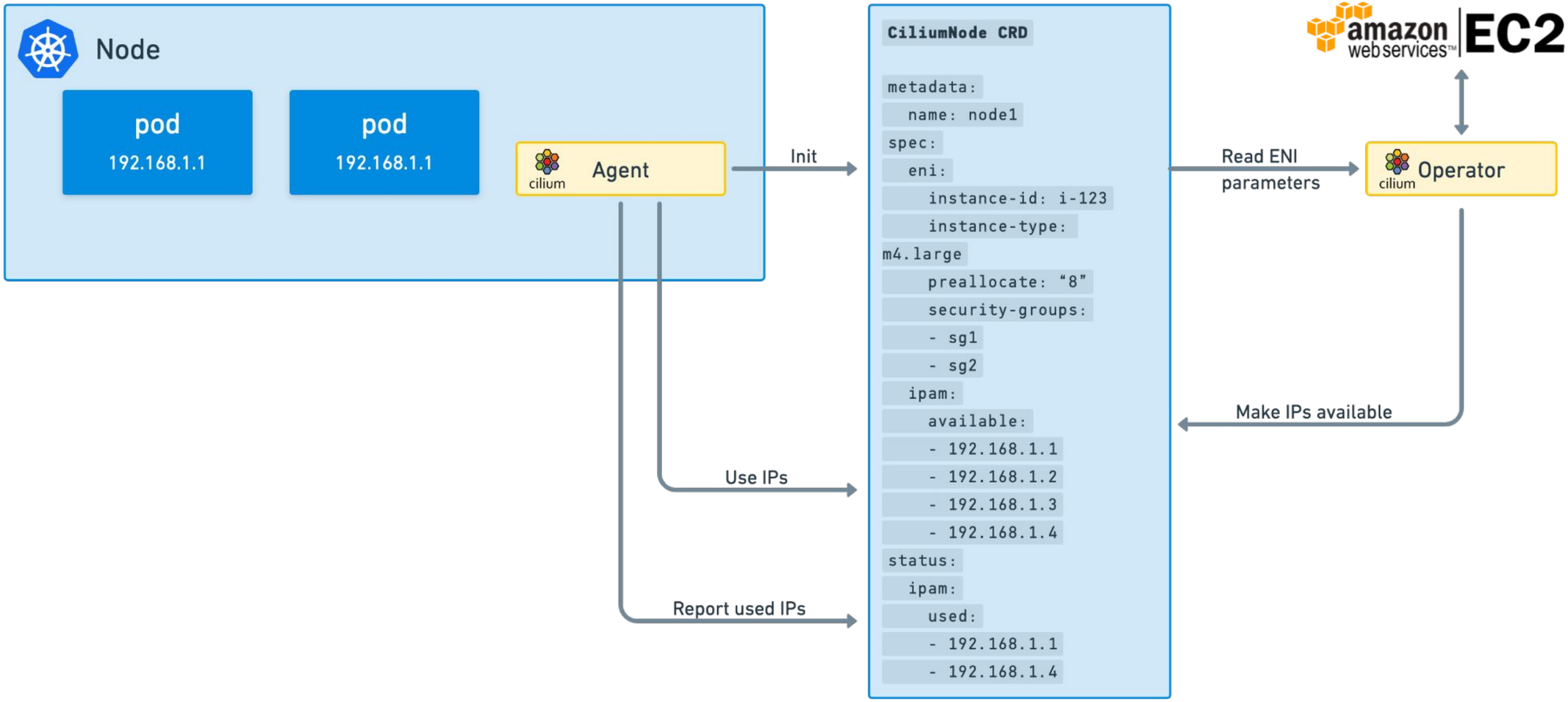


Egress Gateway HA



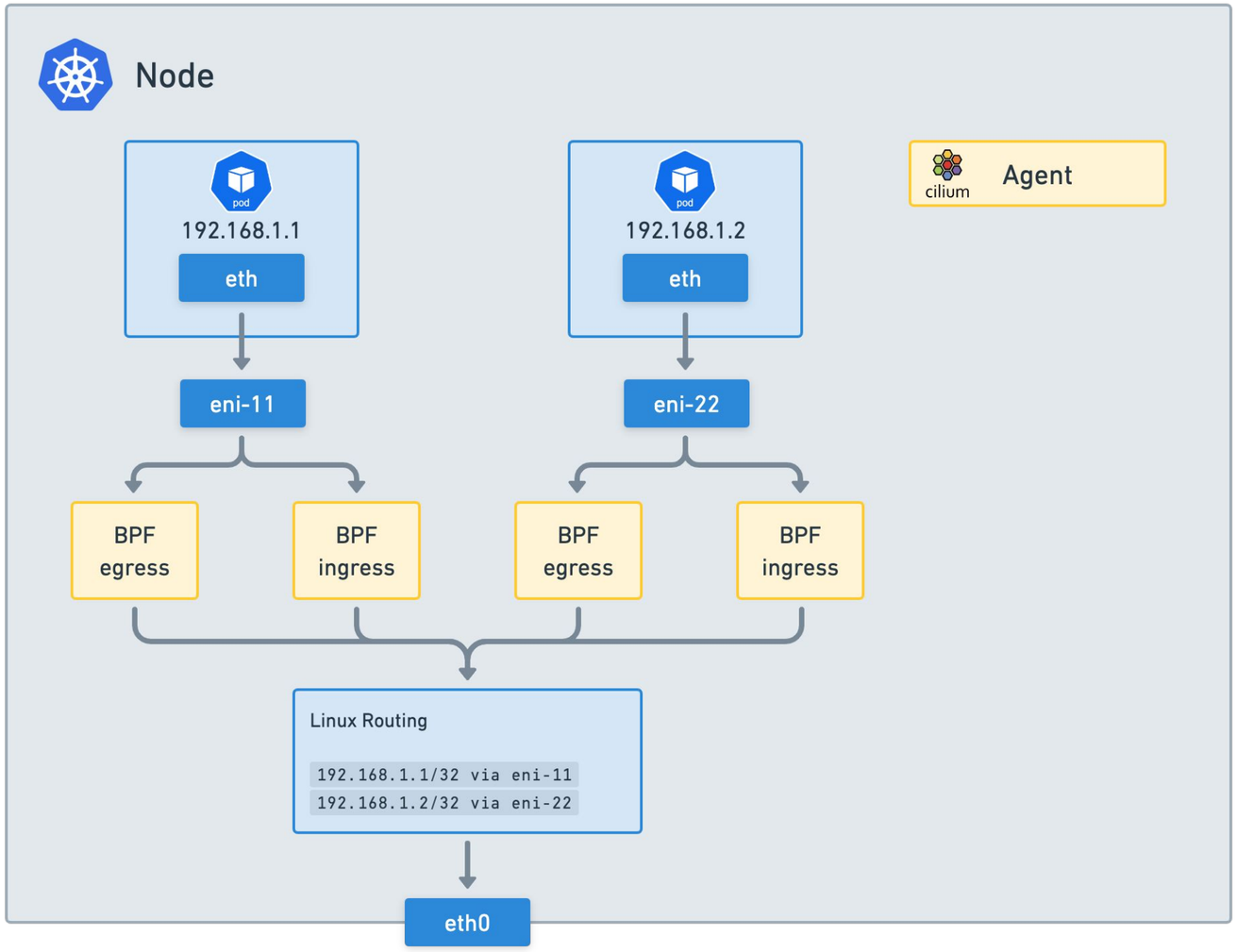
Native Cloud Support

Alibaba, AWS, Azure, Google



CNI Chaining

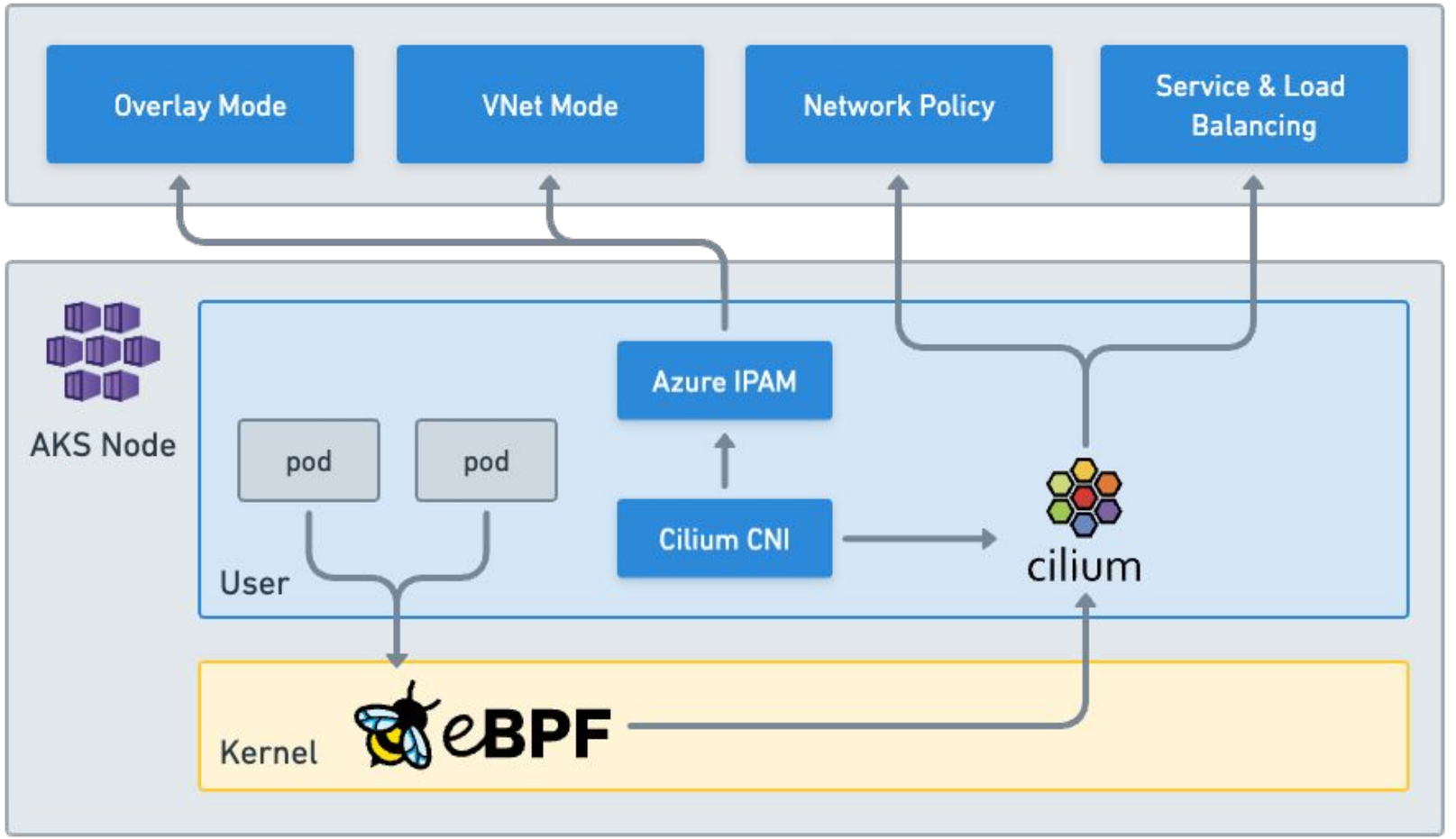
Compatible with almost all other CNIs



Other CNI:
- Device plumbing
- IPAM
- Routing

Cilium:
- Load-balancing
- Network policy
- Encryption
- Multi-cluster
- Visibility

Azure CNI Powered by Cilium



AKS BYOCNI

- AKS BYOCNI is the preferred way to run Cilium on AKS
- No Azure IPAM Integration
- The AKS cluster must be created with `--network plugin none`

Datapath	IPAM	Datastore
Encapsulation (VXLAN)	Cluster Pool	Kubernetes CRD

```
aksbyocni:
  enabled: true
hubble:
  enabled: true
  relay:
    enabled: true
hubble-ui:
  enabled: true
kubeProxyReplacement: strict
nodeinit:
  enabled: true
operator:
  prometheus:
    enabled: true
prometheus:
  enabled: true
```

Platform Integration

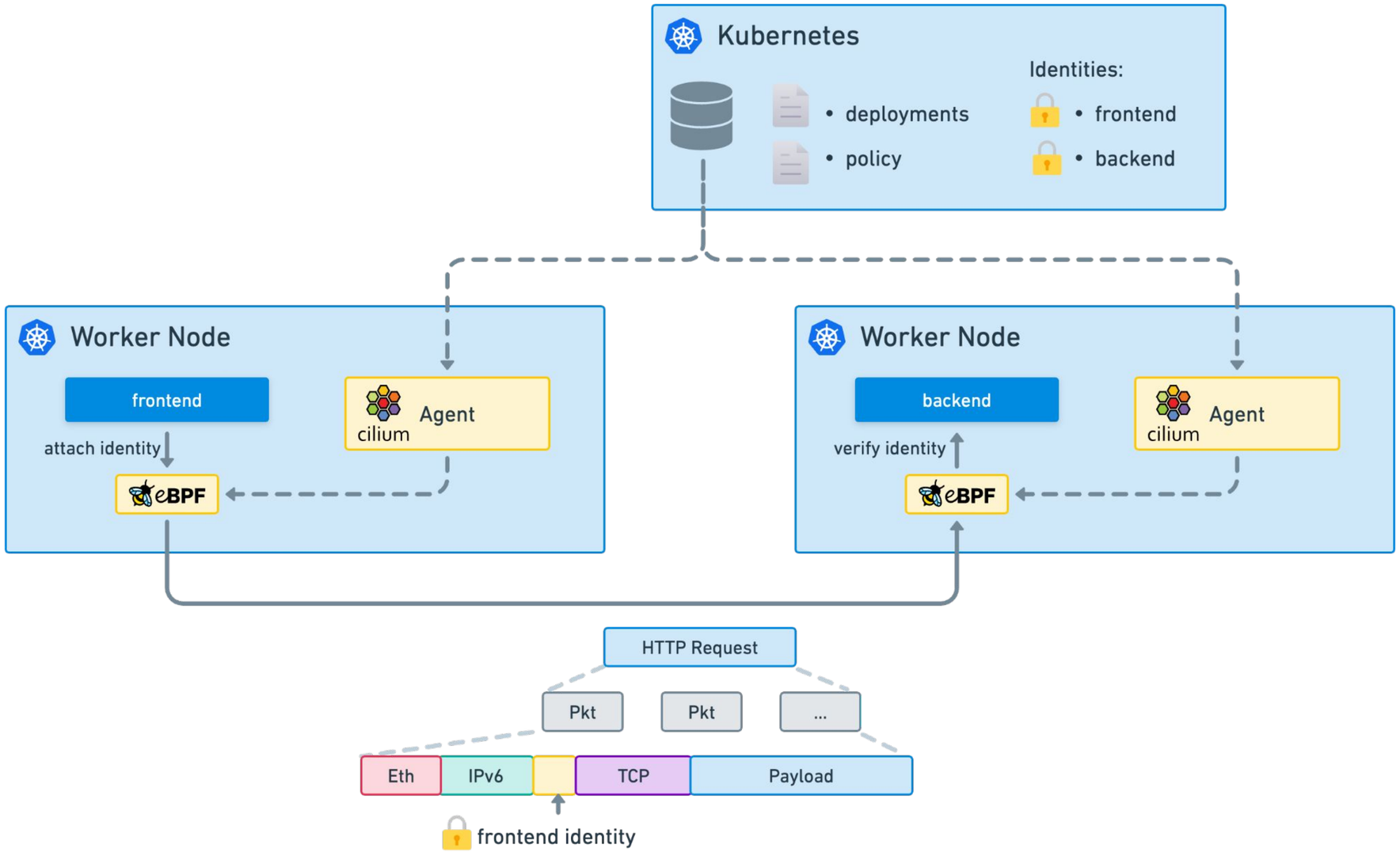
Getting Started Guides

Try Cilium on any Kubernetes distribution in under 15 minutes

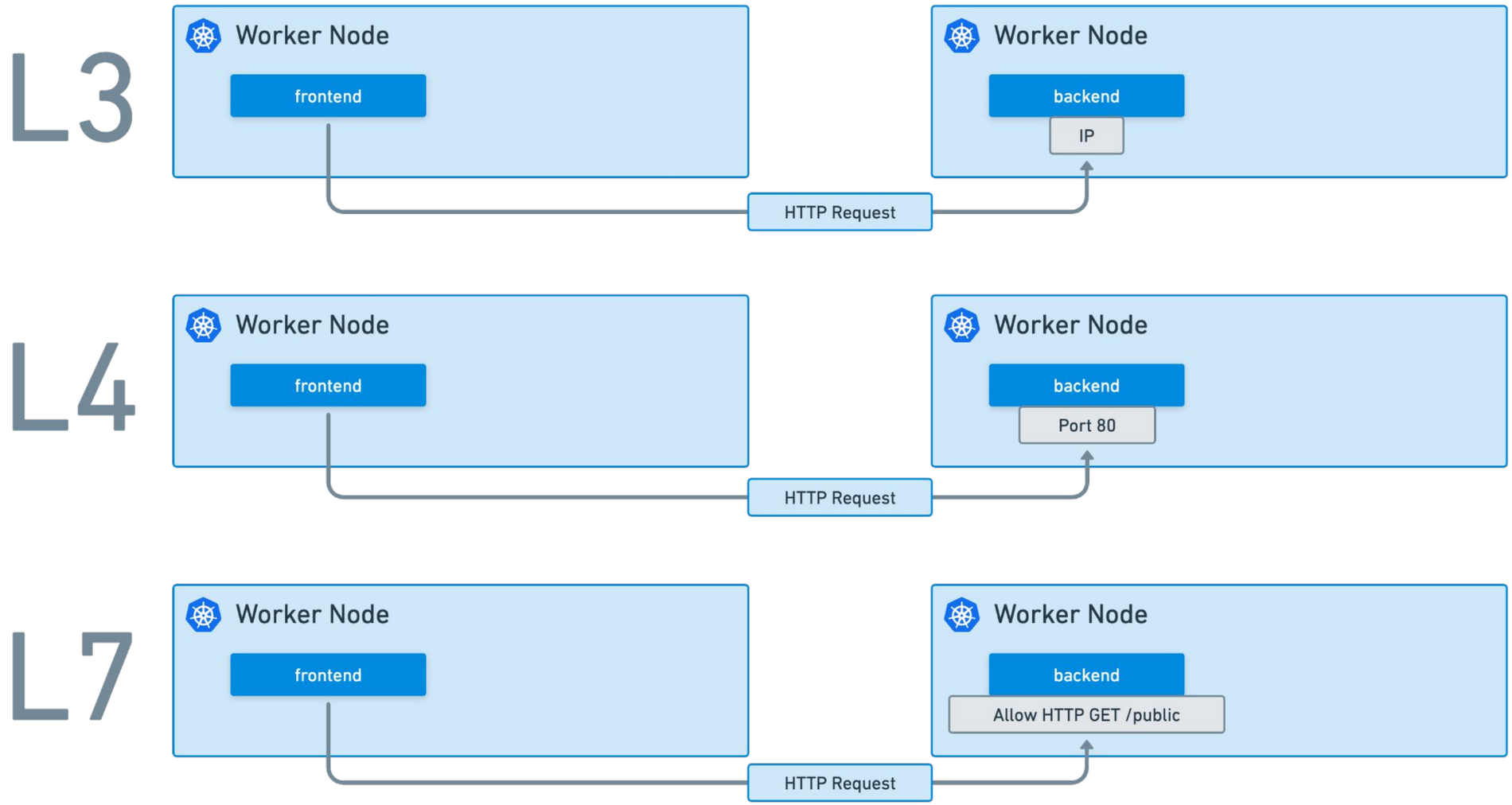
Minikube	Self-Managed Kubernetes	Amazon EKS	Google GKE	Microsoft AKS

Security

Identity-based Security



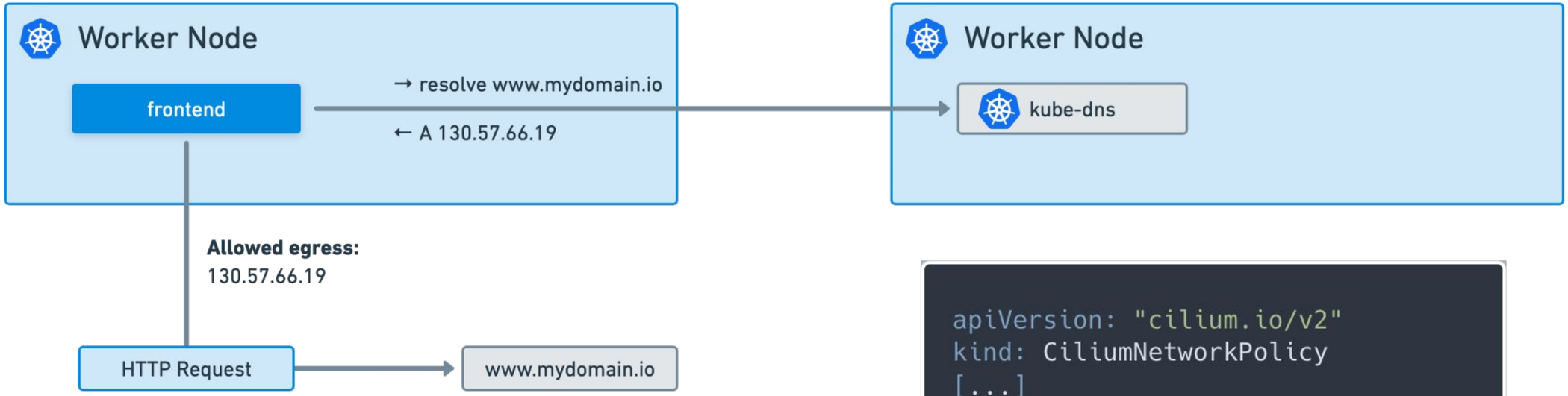
API-aware Authorization



Cassandra Cilium Network Policy Example

```yaml
apiVersion: "cilium.io/v2"
kind: CiliumNetworkPolicy
[...]
specs:
- endpointSelector:
  matchLabels:
    app: cassandra
  ingress:
  - toPorts:
    - ports:
      - port: "9042"
        protocol: TCP
        l7proto: cassandra
        l7:
        - query_action: "select"
          query_table: "myTable"
```

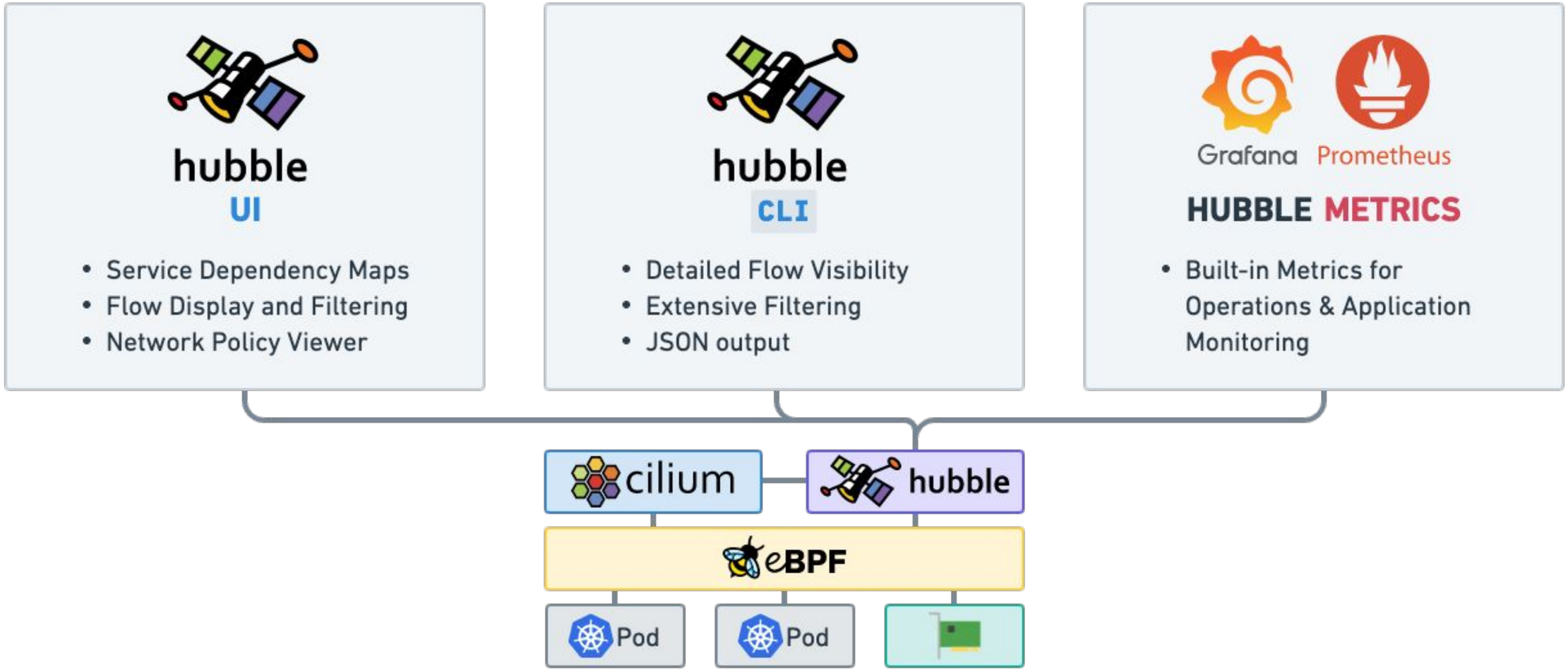
DNS-aware Cilium Network Policy




```
apiVersion: "cilium.io/v2"
kind: CiliumNetworkPolicy
[...]
specs:
- endpointSelector:
  matchLabels:
    app: frontend
  egress:
  - toFQDNs:
    - matchName: "*.mydomain.io"
    toPorts:
    - ports:
      - port: "443"
        protocol: TCP
```

Observability

What is Hubble?



Flow Visibility

```
$ kubectl get pods
NAME                          READY   STATUS    RESTARTS   AGE
tiefighter                    1/1     Running   0          2m34s
xwing                         1/1     Running   0          2m34s
deathstar-5b7489bc84-crlxh    1/1     Running   0          2m34s
deathstar-5b7489bc84-j7qwq    1/1     Running   0          2m34s

$ hubble observe --follow -l class=xwing
# DNS lookup to coredns
default/xwing:41391 (ID:16092) -> kube-system/coredns-66bff467f8-28dgp:53 (ID:453) to-proxy FORWARDED (UDP)
kube-system/coredns-66bff467f8-28dgp:53 (ID:453) -> default/xwing:41391 (ID:16092) to-endpoint FORWARDED (UDP)
# ...
# Successful HTTPS request to www.disney.com
default/xwing:37836 (ID:16092) -> www.disney.com:443 (world) to-stack FORWARDED (TCP Flags: SYN)
www.disney.com:443 (world) -> default/xwing:37836 (ID:16092) to-endpoint FORWARDED (TCP Flags: SYN, ACK)
www.disney.com:443 (world) -> default/xwing:37836 (ID:16092) to-endpoint FORWARDED (TCP Flags: ACK, FIN)
default/xwing:37836 (ID:16092) -> www.disney.com:443 (world) to-stack FORWARDED (TCP Flags: RST)
# ...
# Blocked HTTP request to deathstar backend
default/xwing:49610 (ID:16092) -> default/deathstar:80 (ID:16081) Policy denied DROPPED (TCP Flags: SYN)
```

Flow Metadata

- Ethernet headers
- IP & ICMP headers
- UDP/TCP ports, TCP flags
- HTTP, DNS, Kafka, ...

Kubernetes

- Pod names and labels
- Service names
- Worker node names

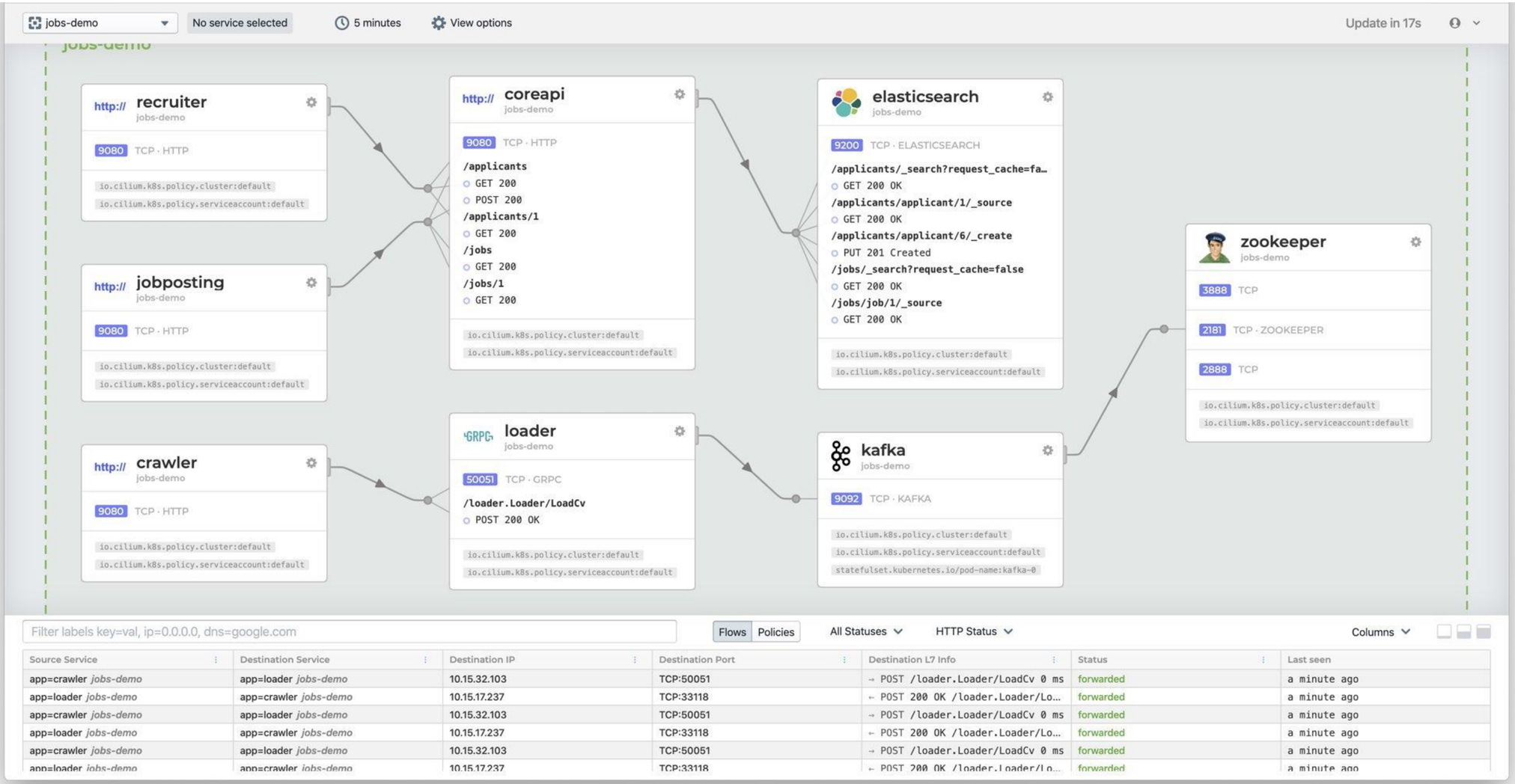
DNS (if available)

- FQDN for source and destination

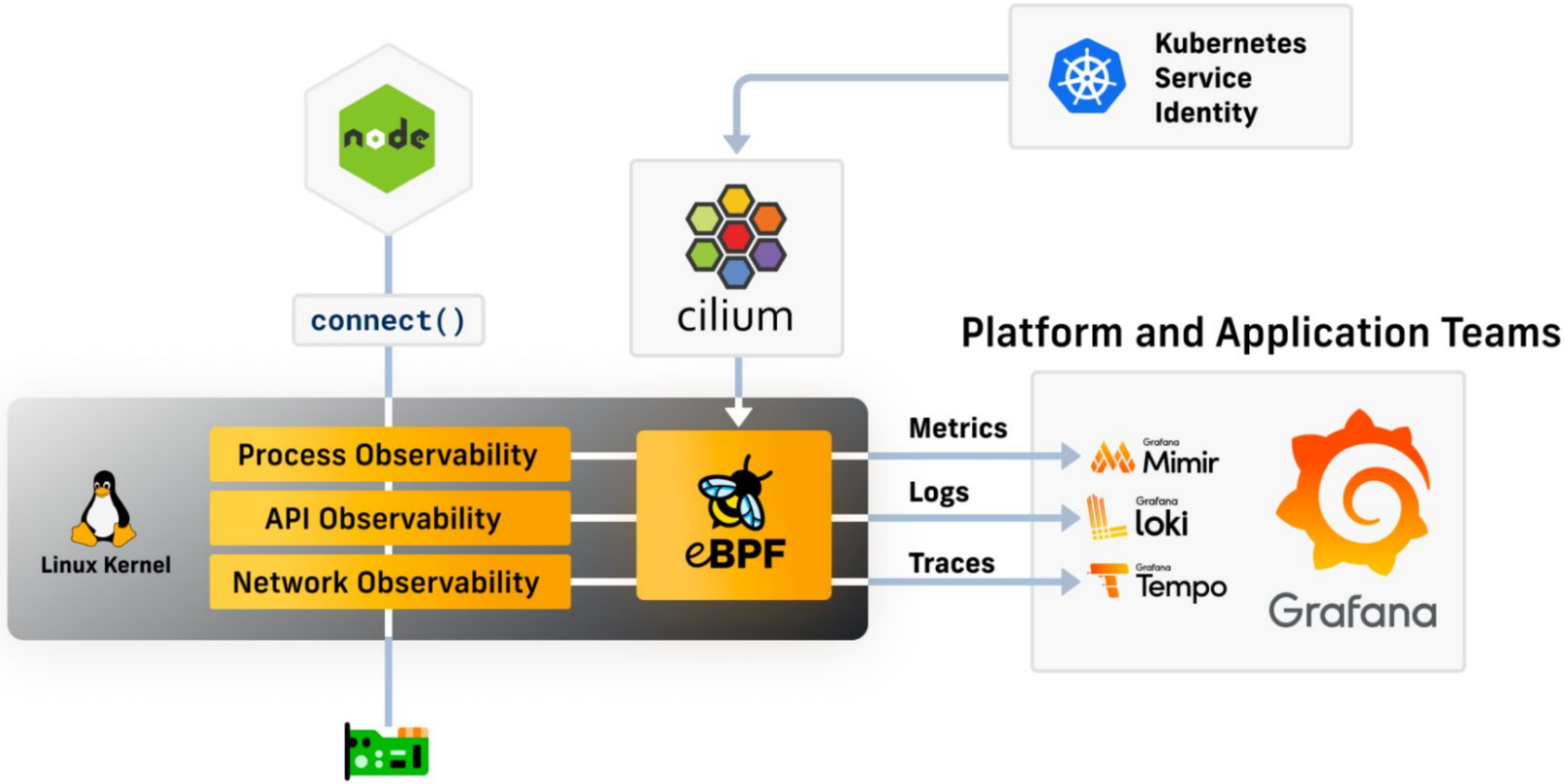
Cilium

- Security identities and endpoints
- Drop reasons
- Policy verdict matches

Service Map


jobs-demo
No service selected
5 minutes
View options
Update in 17s
http:// recruiter
jobs-demo
9080 TCP · HTTP
io.cilium.k8s.policy.cluster:default
io.cilium.k8s.policy.serviceaccount:default
http:// jobposting
jobs-demo
9080 TCP · HTTP
io.cilium.k8s.policy.cluster:default
io.cilium.k8s.policy.serviceaccount:default
http:// crawler
jobs-demo
9080 TCP · HTTP
io.cilium.k8s.policy.cluster:default
io.cilium.k8s.policy.serviceaccount:default
http:// coreapi
jobs-demo
9080 TCP · HTTP
/applicants
GET 200
POST 200
/applicants/1
GET 200
/jobs
GET 200
/jobs/1
GET 200
io.cilium.k8s.policy.cluster:default
io.cilium.k8s.policy.serviceaccount:default
GRPC loader
jobs-demo
50051 TCP · GRPC
/loader.Loader/LoadCv
POST 200 OK
io.cilium.k8s.policy.cluster:default
io.cilium.k8s.policy.serviceaccount:default
elasticsearch
jobs-demo
9200 TCP · ELASTICSEARCH
/applicants/_search?request_cache=fa…
GET 200 OK
/applicants/applicant/1/_source
GET 200 OK
/applicants/applicant/6/_create
PUT 201 Created
/jobs/_search?request_cache=false
GET 200 OK
/jobs/job/1/_source
GET 200 OK
io.cilium.k8s.policy.cluster:default
io.cilium.k8s.policy.serviceaccount:default
kafka
jobs-demo
9092 TCP · KAFKA
io.cilium.k8s.policy.cluster:default
io.cilium.k8s.policy.serviceaccount:default
statefulset.kubernetes.io/pod-name:kafka-0
zookeeper
jobs-demo
3888 TCP
2181 TCP · ZOOKEEPER
2888 TCP
io.cilium.k8s.policy.cluster:default
io.cilium.k8s.policy.serviceaccount:default
Filter labels key=val, ip=0.0.0.0, dns=google.com
Flows
Policies
All Statuses
HTTP Status
Columns
Source Service
Destination Service
Destination IP
Destination Port
Destination L7 Info
Status
Last seen
app=crawler jobs-demo
app=loader jobs-demo
10.15.32.103
TCP:50051
→ POST /loader.Loader/LoadCv 0 ms
forwarded
a minute ago
app=loader jobs-demo
app=crawler jobs-demo
10.15.17.237
TCP:33118
← POST 200 OK /loader.Loader/Lo…
forwarded
a minute ago
app=crawler jobs-demo
app=loader jobs-demo
10.15.32.103
TCP:50051
→ POST /loader.Loader/LoadCv 0 ms
forwarded
a minute ago
app=loader jobs-demo
app=crawler jobs-demo
10.15.17.237
TCP:33118
← POST 200 OK /loader.Loader/Lo…
forwarded
a minute ago
app=crawler jobs-demo
app=loader jobs-demo
10.15.32.103
TCP:50051
→ POST /loader.Loader/LoadCv 0 ms
forwarded
a minute ago
app=loader jobs-demo
app=crawler jobs-demo
10.15.17.237
TCP:33118
← POST 200 OK /loader.Loader/Lo…
forwarded
a minute ago

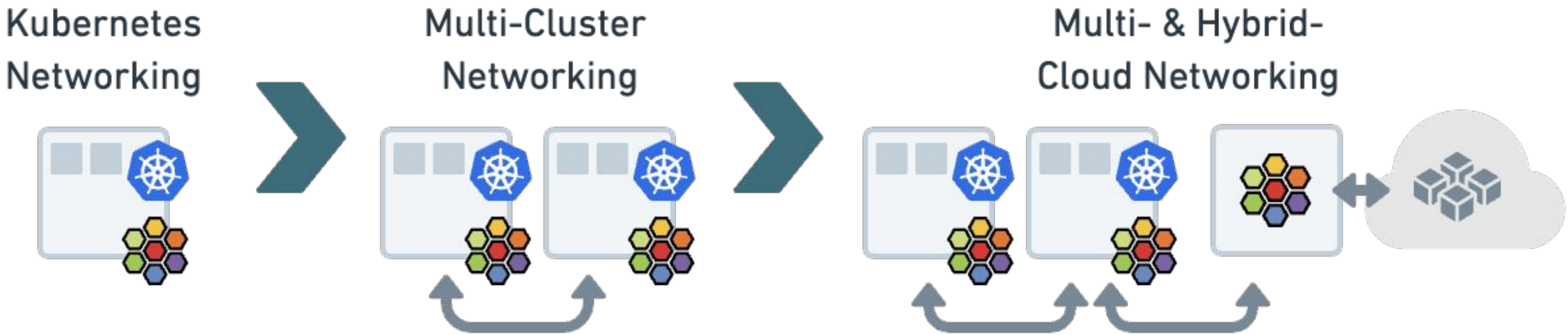
Cilium & Grafana Integration



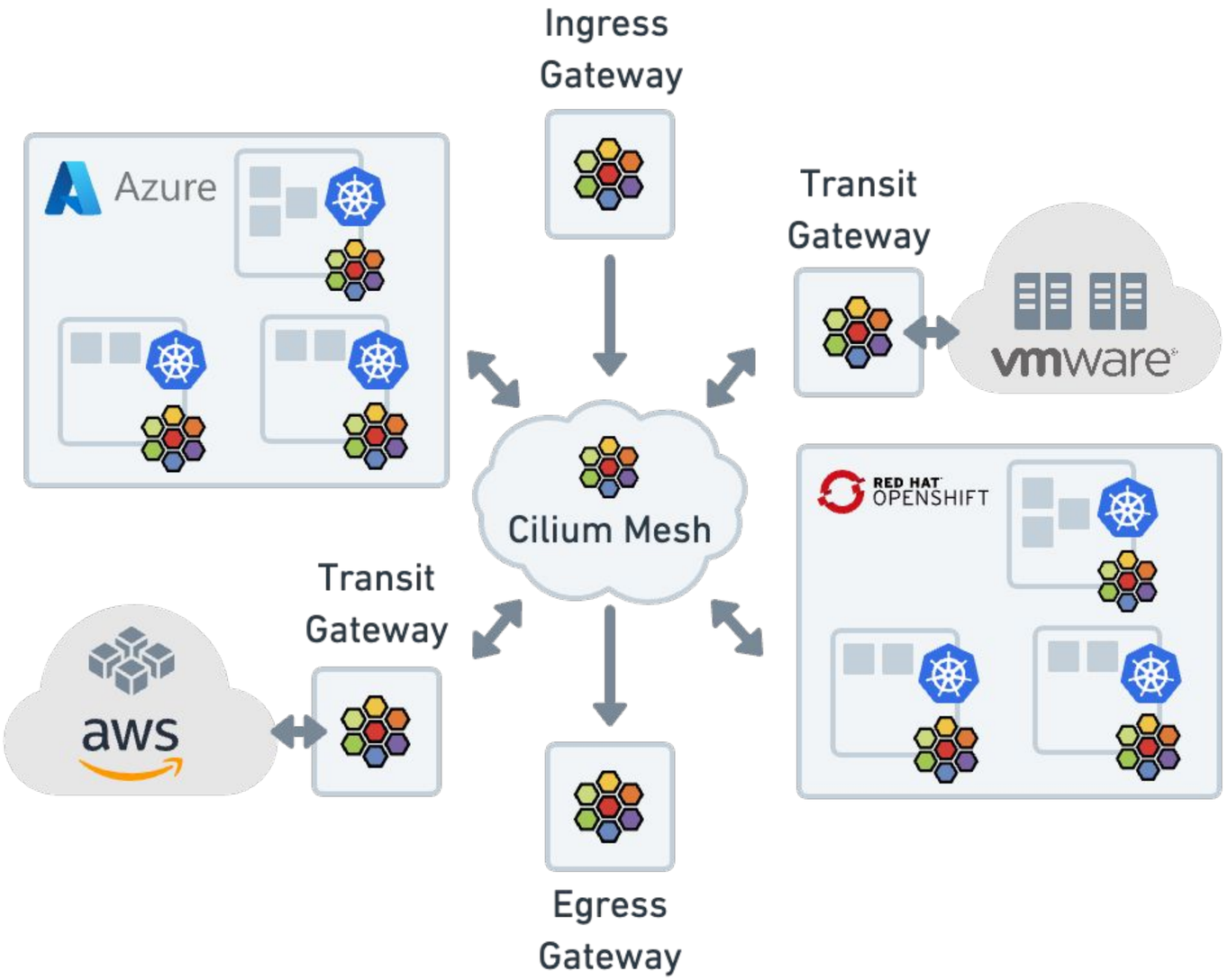
Cilium Mesh

One Mesh to Connect Them All

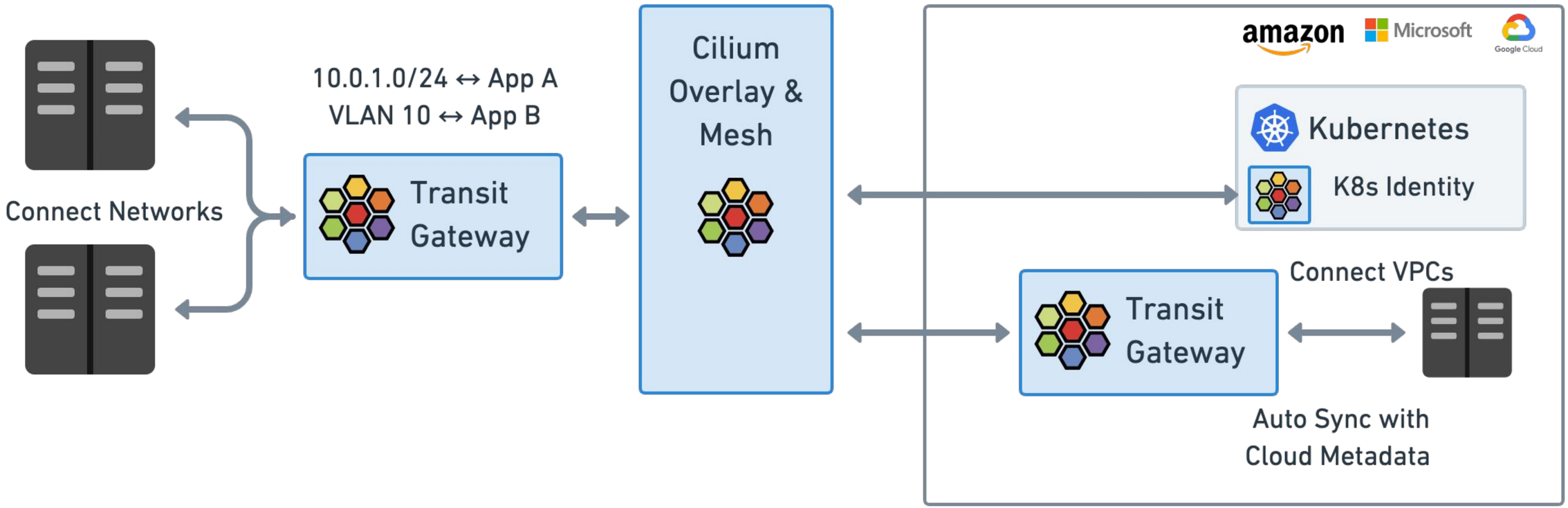
Cilium Mesh - Introduction



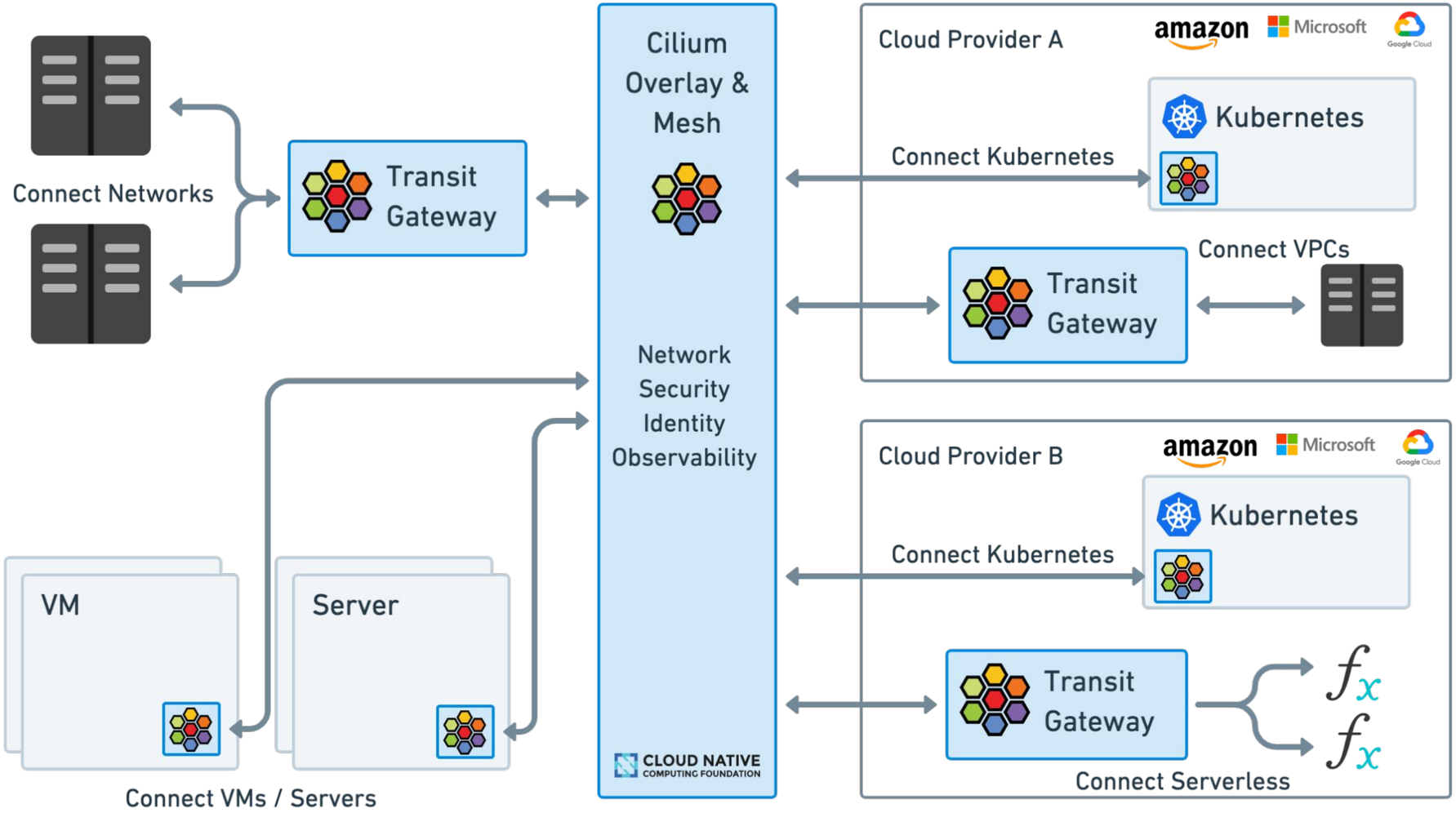
Cilium Mesh - Overview



Cilium Mesh - Hybrid Cloud

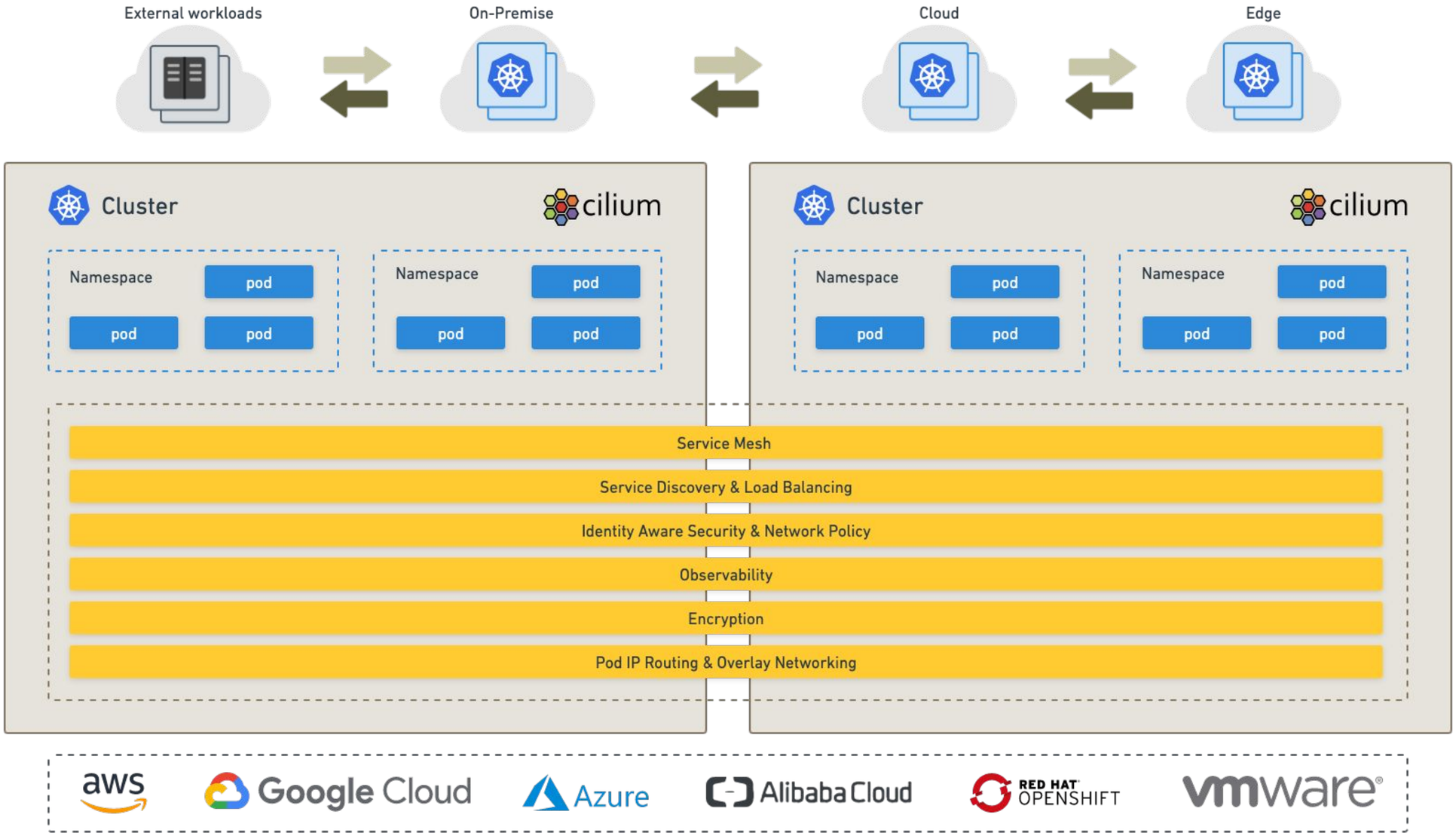


Cilium Mesh - Use Cases

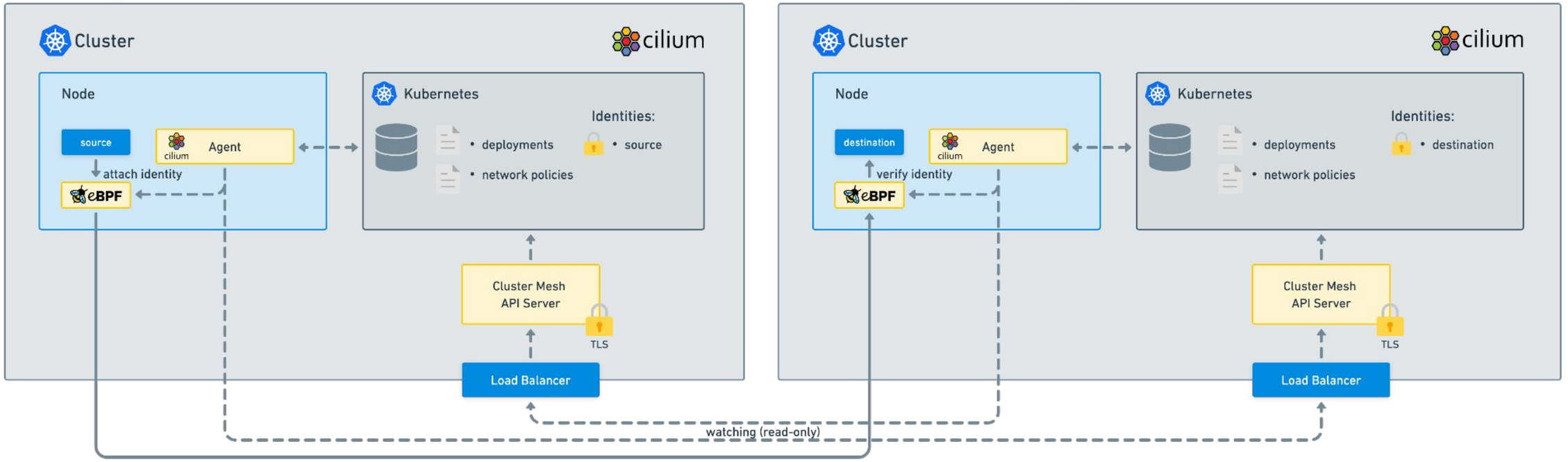


Cluster Mesh

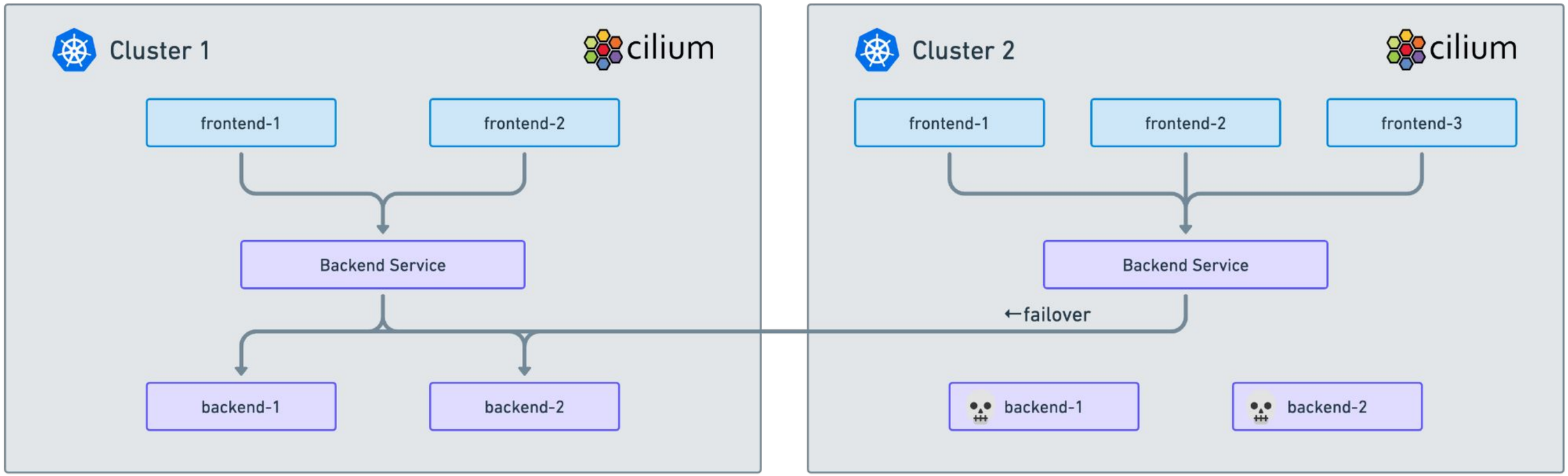
Cluster Mesh - Introduction



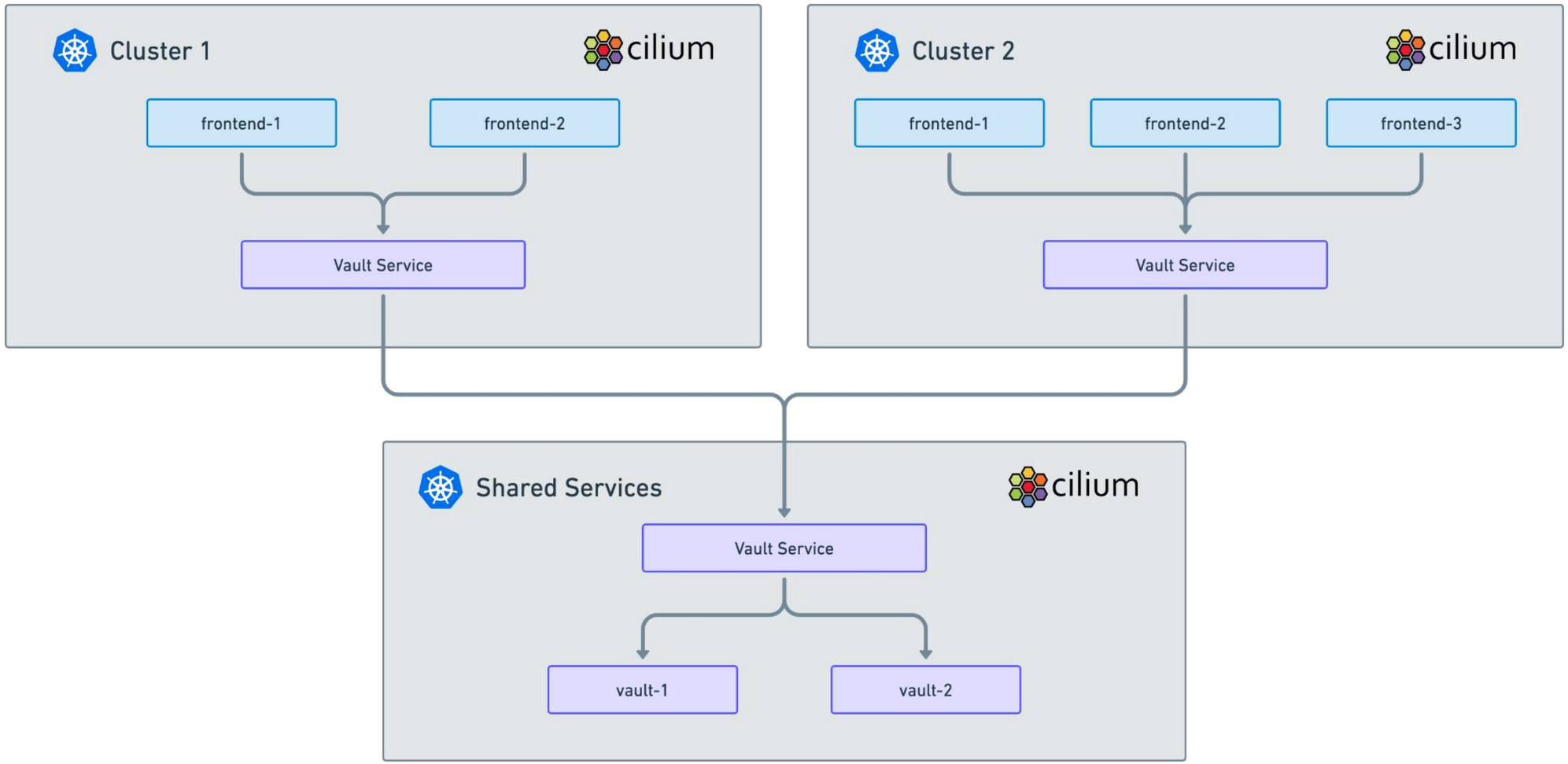
Cluster Mesh - Identity Aware Security



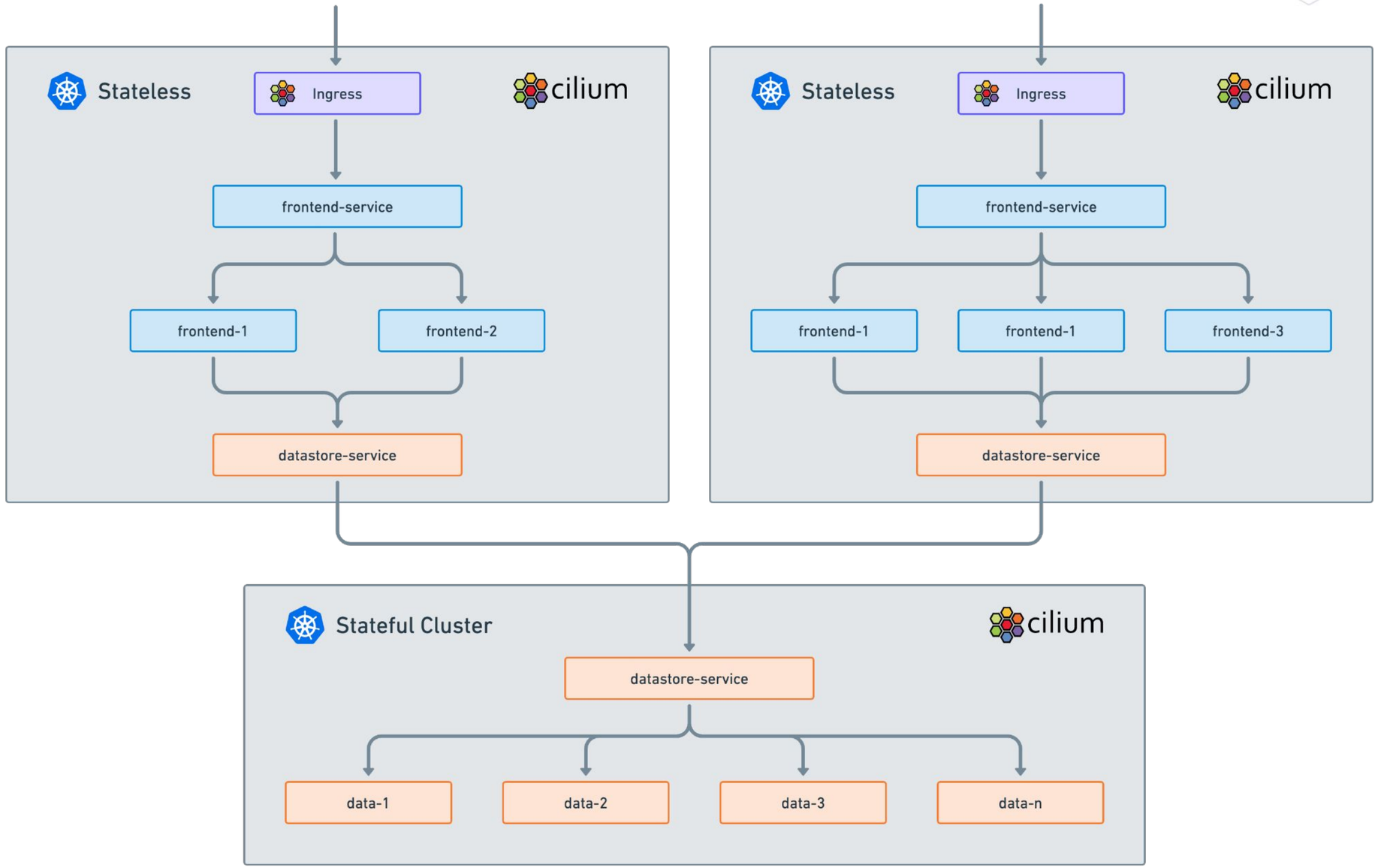
Cluster Mesh - High Availability



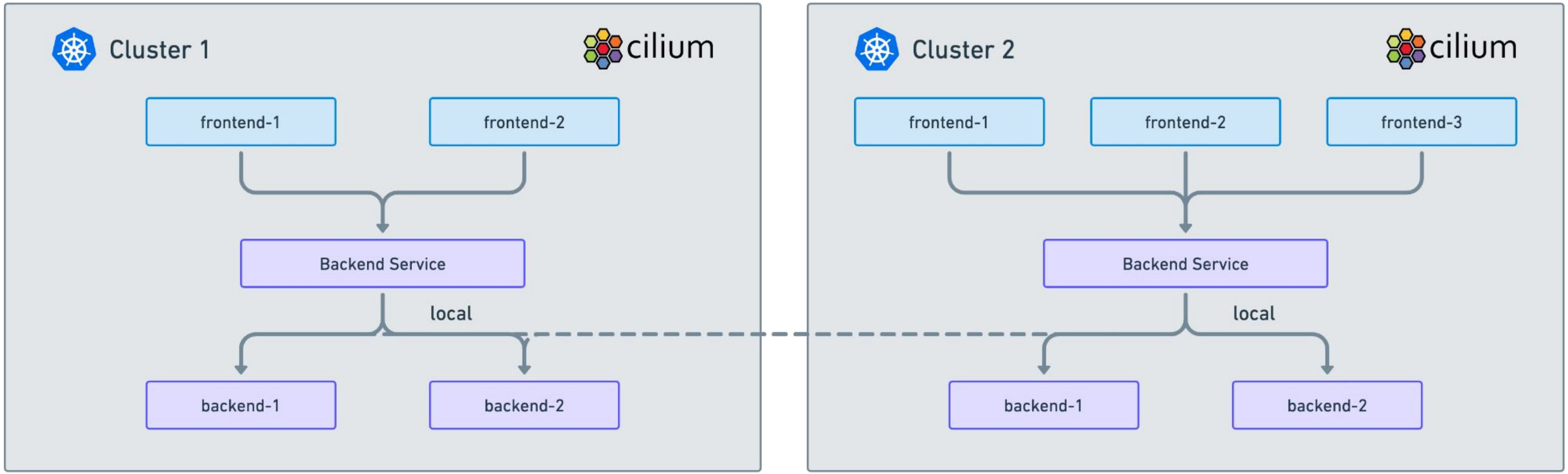
Cluster Mesh - Shared Services



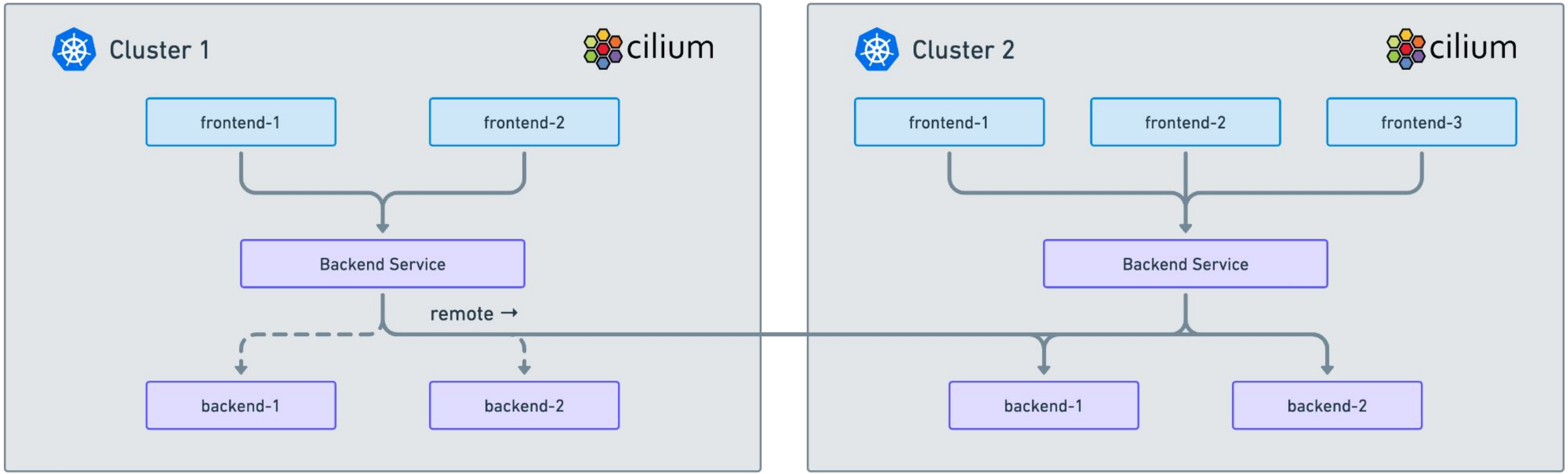
Cluster Mesh - Splitting Services



Cluster Mesh - Local Service Affinity



Cluster Mesh - Remote Service Affinity



Cluster Mesh - Local Service Affinity


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

Cluster Mesh - Remote Service Affinity

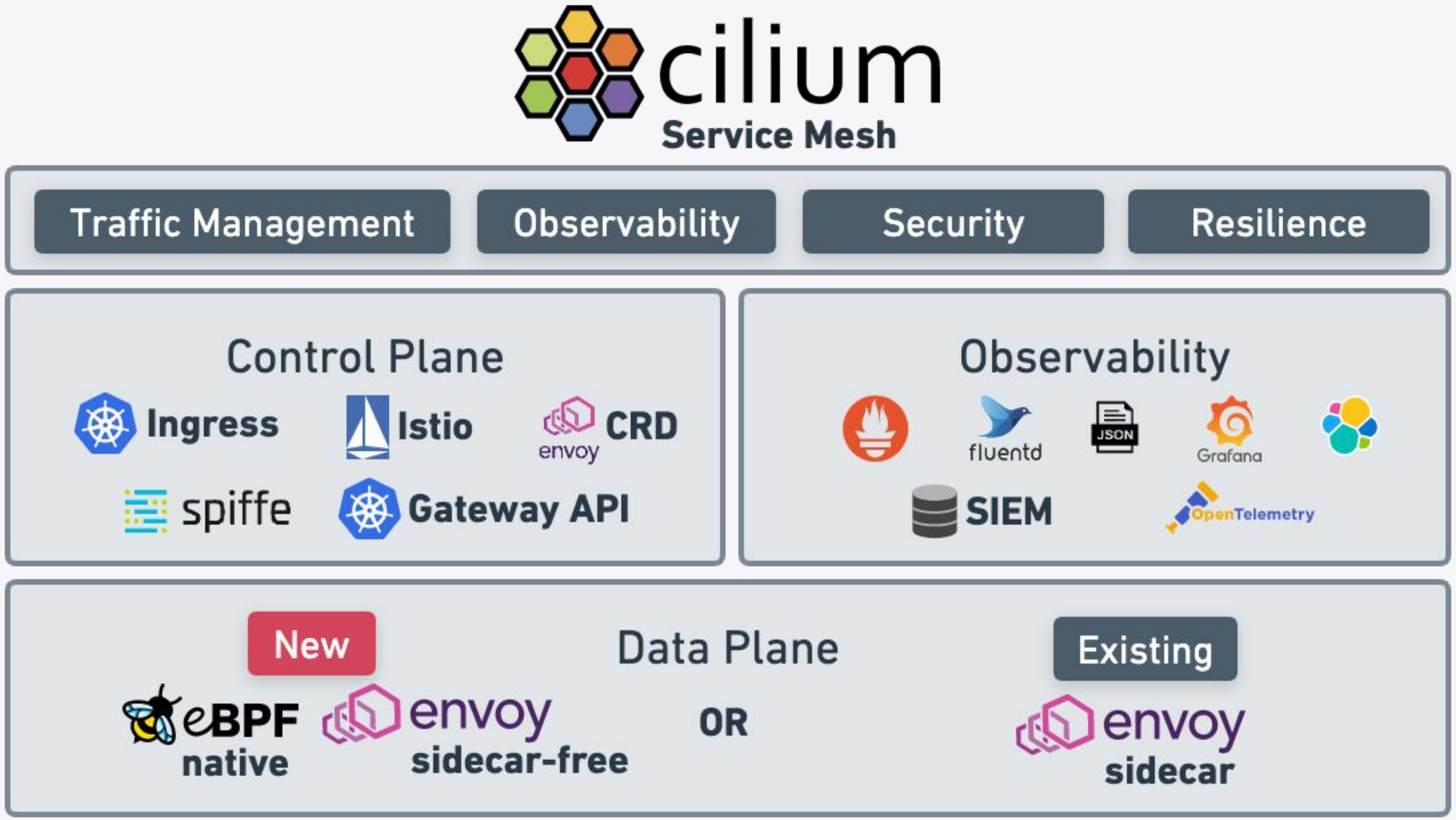

```yaml
apiVersion: v1
kind: Service
metadata:
  name: backend-service
  annotations:
    io.cilium/global-service: "true"
    io.cilium/service-affinity: remote
spec:
  type: ClusterIP
  ports:
  - port: 80
  selector:
    name: backend
```

Cluster Mesh - Cilium Network Policies


```yaml
apiVersion: "cilium.io/v2"
kind: CiliumNetworkPolicy
metadata:
  name: "ingress-to-rebel-base"
spec:
  description: "Allow x-wing in cluster-1 to contact rebel-base in cluster2"
  endpointSelector:
    matchLabels:
      name: rebel-base
      io.cilium.k8s.policy.cluster: cluster-2
  ingress:
  - fromEndpoints:
    - matchLabels:
        name: x-wing
        io.cilium.k8s.policy.cluster: cluster-1
    toPorts:
    - ports:
      - port: "80"
        protocol: TCP
```

Service Mesh

Introduction

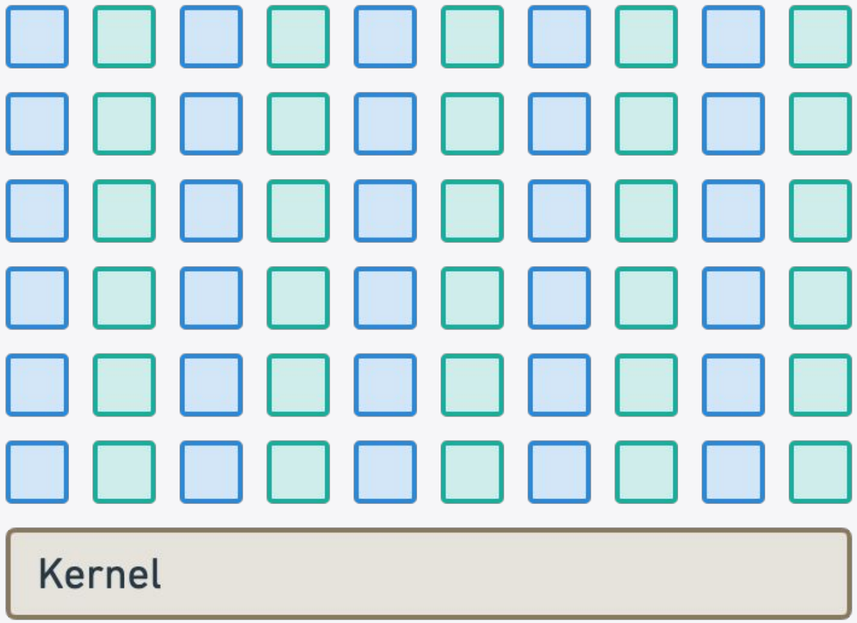


What is different with Cilium Service Mesh?

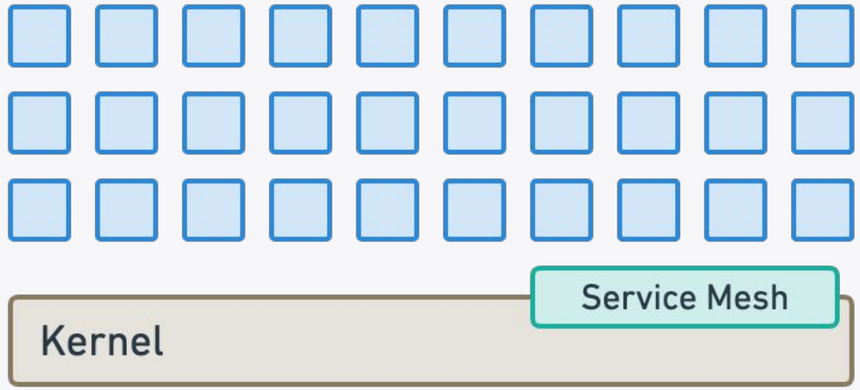
- Reduced operational complexity
- Reduced resource usage
- Better performance
- Avoid sidecar startup/shutdown race conditions

Reduce resource usage - sidecar vs proxy per node

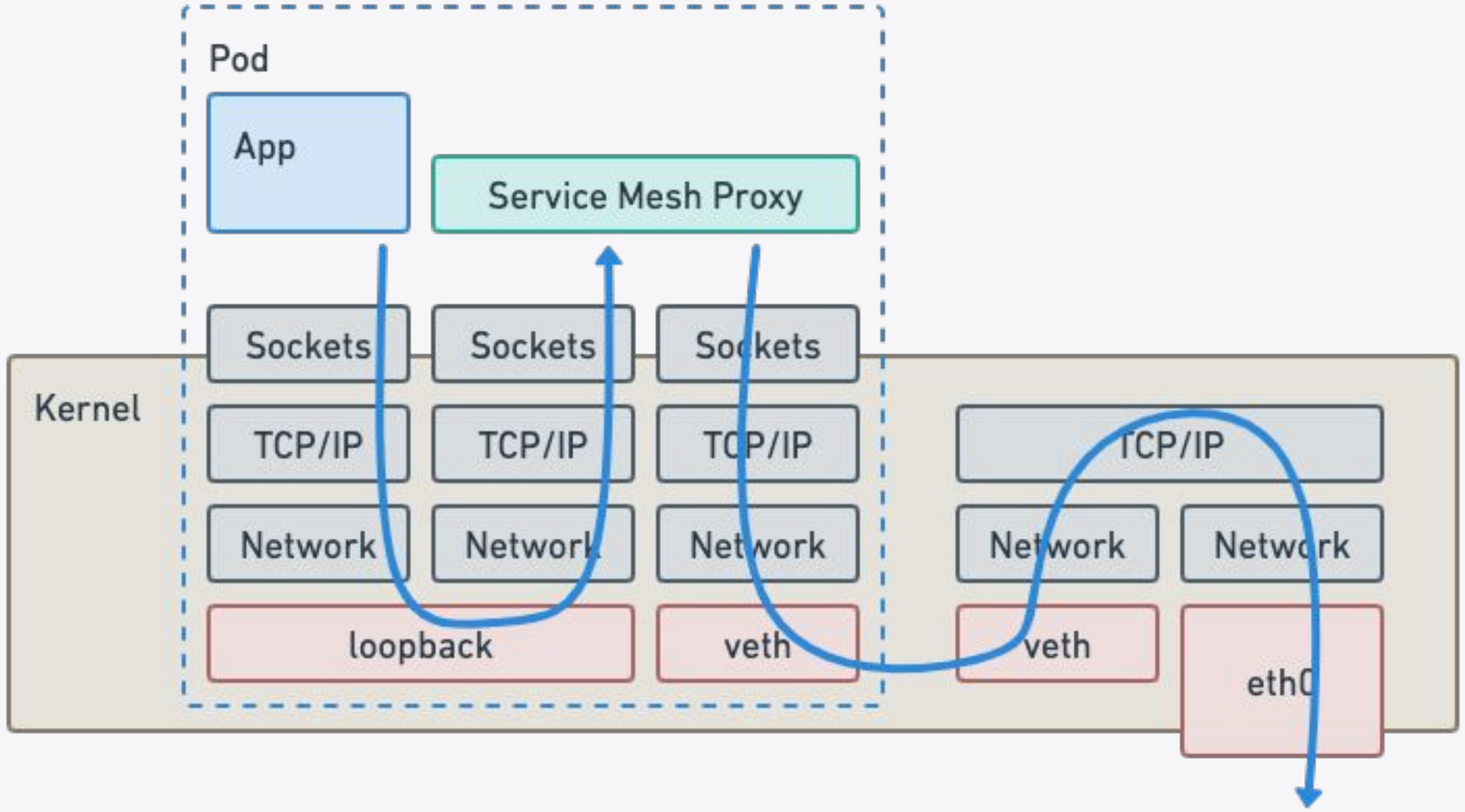
Total number of proxies required



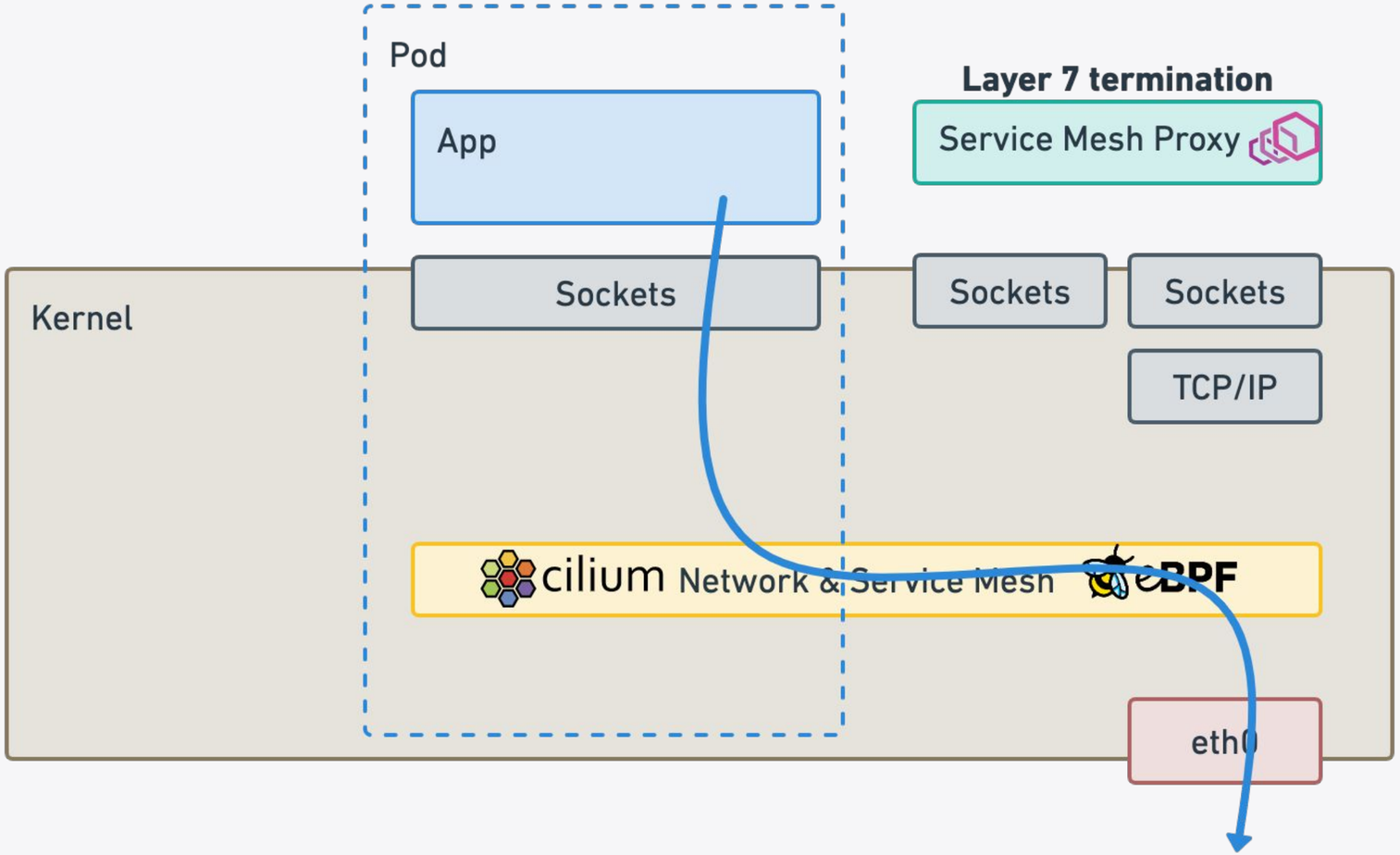
30 pods/node ⇒ 30 proxies/node



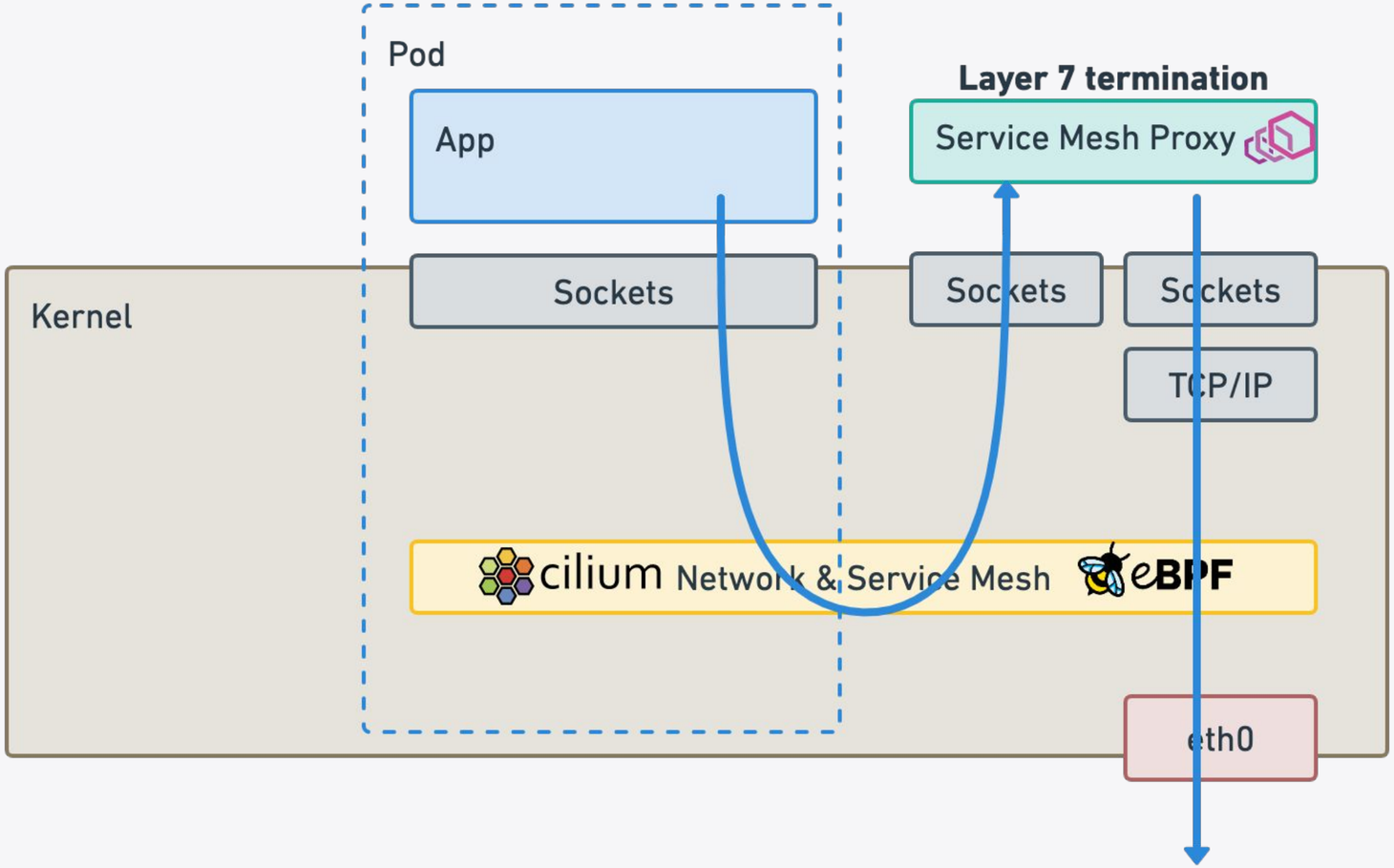
Cost of sidecar injection



eBPF powered network path for L3/L4 traffic



Envoy for Layer 7 termination when needed



Layer 7 Traffic Management Options

Ingress

Original L7 load-balancing standard in K8s

Simple

Supported since Cilium 1.12

Services

Use of K8s services with annotations

Simple

Supported since Cilium 1.13

Gateway API

Originally labelled Ingress v2. Richer in features.

Simple

Supported for v0.5.1 since Cilium 1.13

EnvoyConfig

Raw Envoy Config via CustomResource

Advanced Users & Integrations

Supported since Cilium 1.12

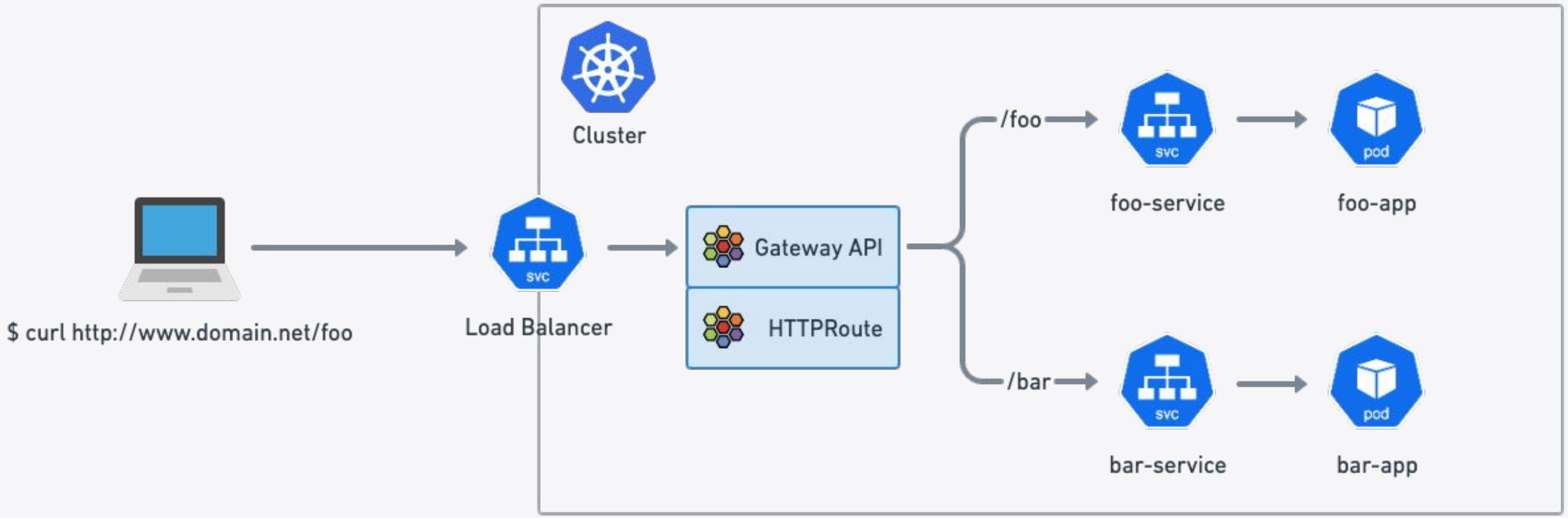
Ingress

- Ingress can be used for path-based routing and TLS termination
- Cilium manages Ingress resources without external Ingress Controller
- Cilium Service Mesh Ingress Controller requires ability to create Service of Type LoadBalancer using Cloud Provider integration or using built-in LoadBalaner
- Ingress CRD with `ingressClassName: cilium`

```yaml
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: basic-ingress
  namespace: default
spec:
  ingressClassName: cilium
  rules:
    - http:
        paths:
          - backend:
              service:
                name: details
                port:
                  number: 9080
            path: /details
            pathType: Prefix
          - backend:
              service:
                name: productpage
                port:
                  number: 9080
            path: /
            pathType: Prefix
```

Gateway API

Overview



Gateway API

Use of Gateway and HTTPRoute objects for path-based routing


```yaml
apiVersion: gateway.networking.k8s.io/v1beta1
kind: Gateway
metadata:
  name: my-gateway
spec:
  gatewayClassName: cilium
  listeners:
  - protocol: HTTP
    port: 80
    name: web-gw
    allowedRoutes:
      namespaces:
        from: Same
```

```yaml
apiVersion: gateway.networking.k8s.io/v1alpha2
kind: HTTPRoute
metadata:
  name: http-app-1
spec:
  parentRefs:
  - name: my-gateway
    namespace: default
  rules:
  - matches:
    - path:
        type: PathPrefix
        value: /details
    backendRefs:
    - name: details
      port: 9080
```

Gateway API

Use of Gateway and HTTPRoute for TLS Termination

```yaml
apiVersion: gateway.networking.k8s.io/v1beta1
kind: Gateway
metadata:
  name: tls-gateway
spec:
  gatewayClassName: cilium
  listeners:
  - name: https
    protocol: HTTPS
    port: 443
    hostname: "bookinfo.cilium.rocks"
    tls:
      certificateRefs:
      - kind: Secret
        name: demo-cert
```

```yaml
apiVersion: gateway.networking.k8s.io/v1beta1
kind: HTTPRoute
metadata:
  name: https-app-route
spec:
  parentRefs:
  - name: tls-gateway
  hostnames:
  - "bookinfo.cilium.rocks"
  rules:
  - matches:
    - path:
        type: PathPrefix
        value: /details
    backendRefs:
    - name: details
      port: 9080
```

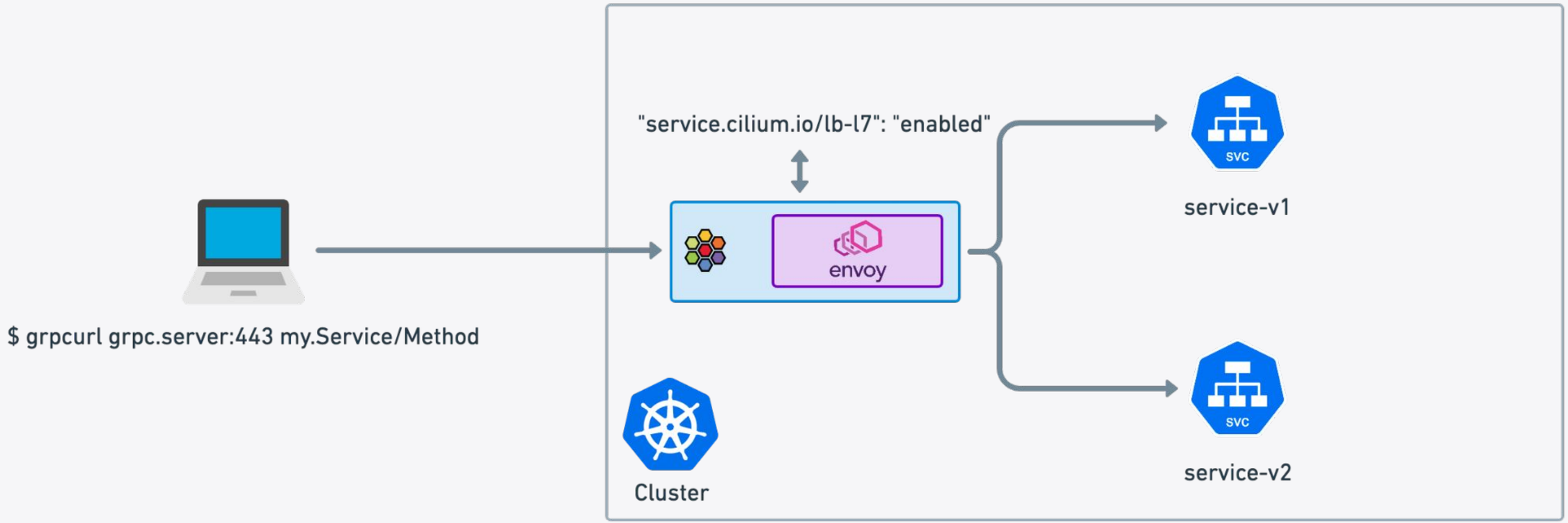
Gateway API

Traffic Splitting with Weighted Routes

cilium

```yaml
apiVersion: gateway.networking.k8s.io/v1alpha2
kind: HTTPRoute
metadata:
  name: example-weighted-route
spec:
  parentRefs:
  - name: my-gateway
  rules:
  - matches:
    - path:
        type: PathPrefix
        value: /echo
    backendRefs:
    - kind: Service
      name: echo-1
      port: 8080
      weight: 75
    - kind: Service
      name: echo-2
      port: 8090
      weight: 25
```

L7 Load Balancing for Kubernetes Services with Annotations



Service + Annotations

Simple way to enable L7 load balancing

```yaml
kind: Service
apiVersion: v1
metadata:
  name: backend
  labels:
    service.cilium.io/lb-l7: "enabled"
    service.cilium.io/lb-l7-algorithm: "least-request"
spec:
  type: ClusterIP
  ports:
    - port: 80
  selector:
    name: backend
```

Possible values: round_robin, least_request, random

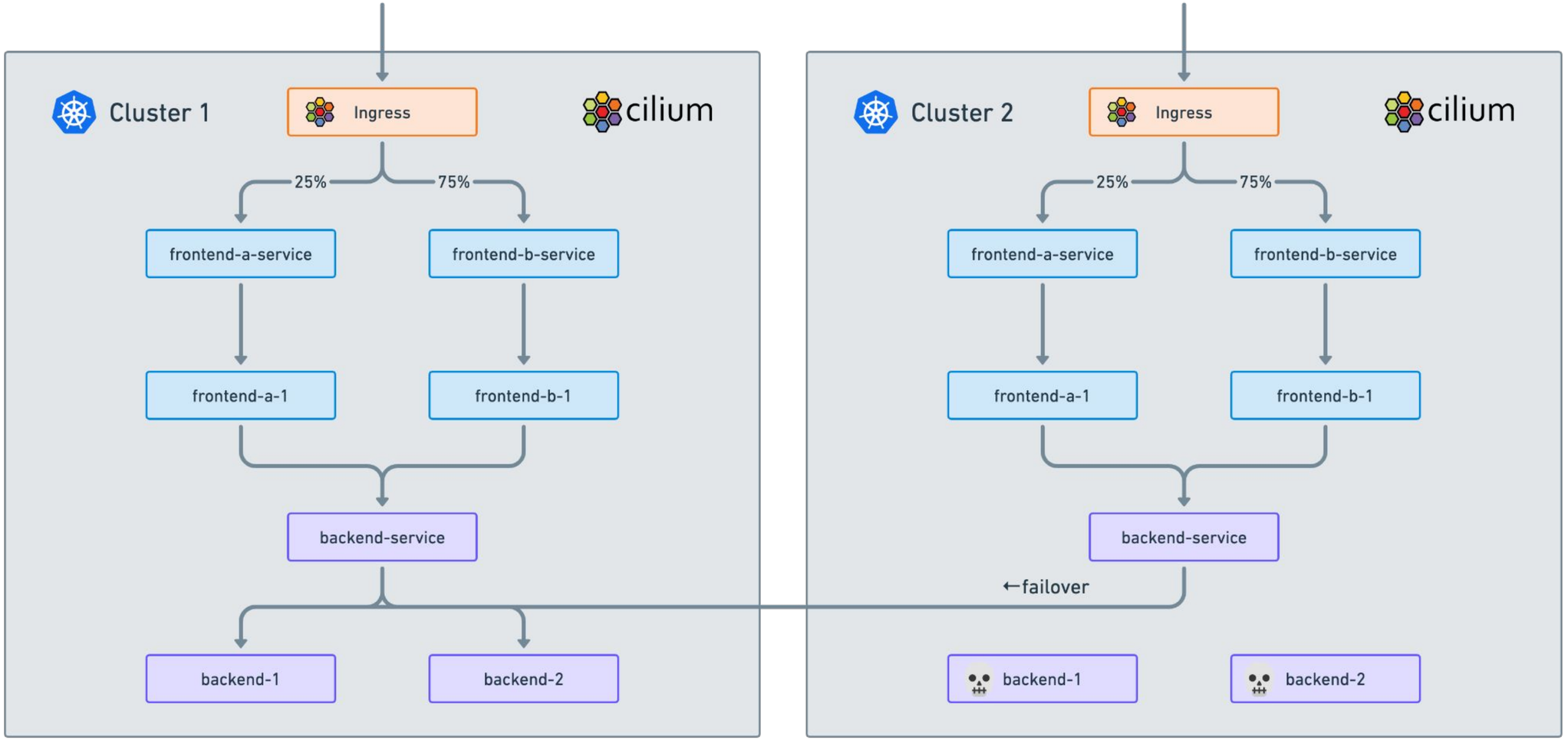
Service + Annotations + Cluster Mesh

Compatible with Cluster Mesh load balancing


```yaml
kind: Service
apiVersion: v1
metadata:
  name: backend
  labels:
    service.cilium.io/lb-l7: "enabled"
    service.cilium.io/lb-l7-algorithm: "least-request"
    service.cilium.io/global: "true"
spec:
  type: ClusterIP
  ports:
    - port: 80
  selector:
    name: backend
```

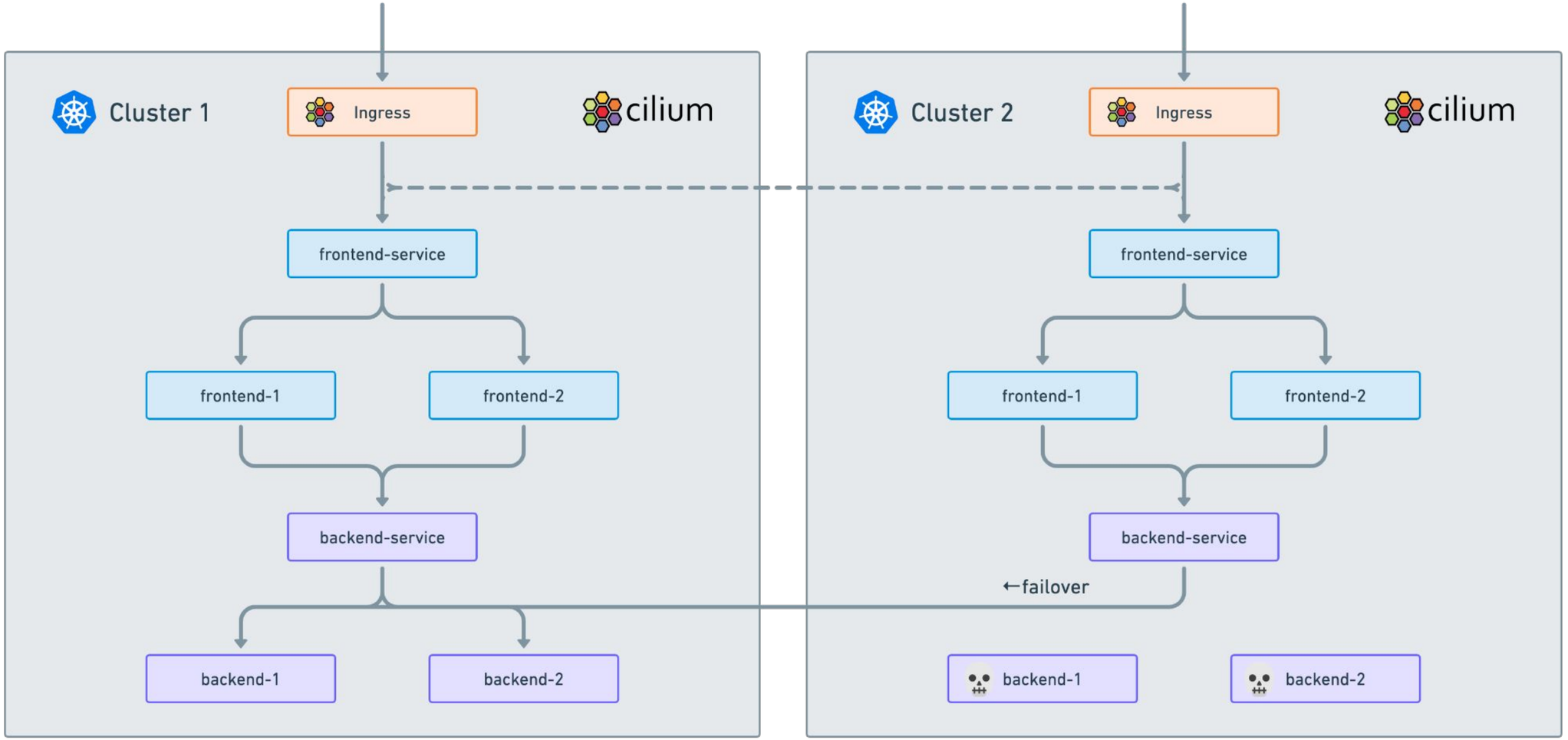
Cluster Mesh with Service Mesh

Percentage Based Routing



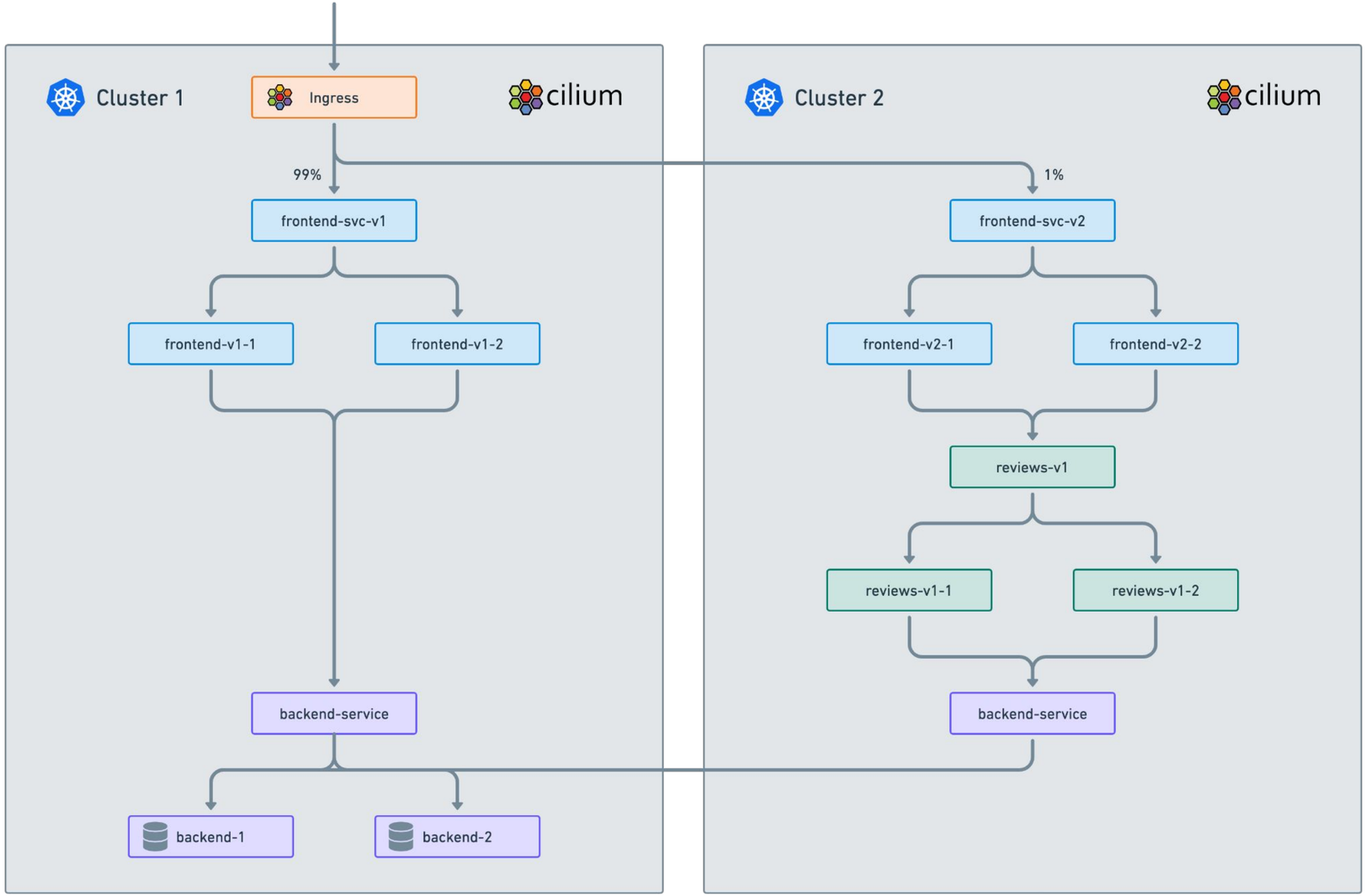
Cluster Mesh with Service Mesh

Topology Aware Routing



Cluster Mesh with Service Mesh

Canary Rollout to other Cluster



Tetragon

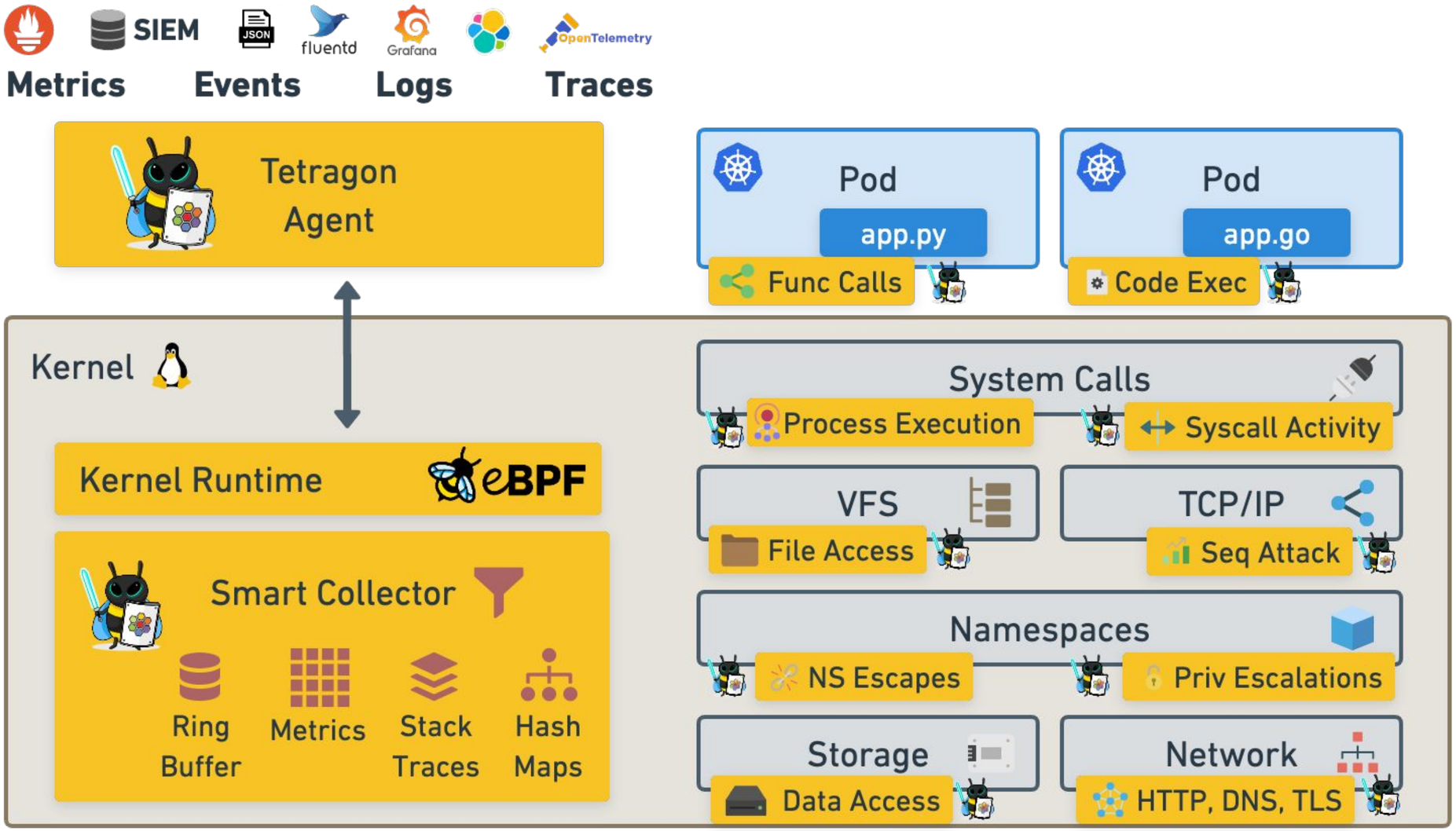
ISOVALENT

Cilium Tetragon

- New open source project in Cilium
- eBPF based = high performance and zero modifications required to app
- Hooks into kernel functions after parameters are copied
- Adds contextual information about Kubernetes objects
- Preventative capabilities

github.com/cilium/tetragon

Tetragon


SIEM
JSON
fluentd
Grafana
OpenTelemetry
Metrics
Events
Logs
Traces
Tetragon Agent
Pod
app.py
Func Calls
Pod
app.go
Code Exec
Kernel
Kernel Runtime
eBPF
Smart Collector
Ring Buffer
Metrics
Stack Traces
Hash Maps
System Calls
Process Execution
Syscall Activity
VFS
File Access
TCP/IP
Seq Attack
Namespaces
NS Escapes
Priv Escalations
Storage
Data Access
Network
HTTP, DNS, TLS

Process Tree View