ISOVALENT

The Swiss Army Knife of Cloud-Native Networking

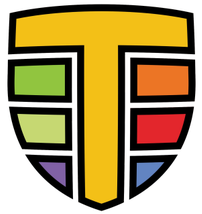
Speaker: **Raymond de Jong**

Introduction

Raymond de Jong
Field CTO EMEA

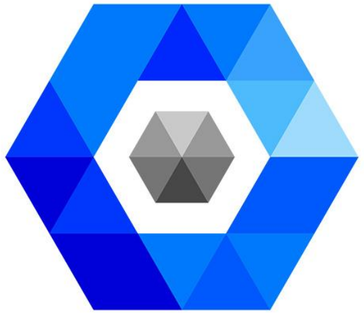
ISOVALENT
now part of cisco

cilium



Tetragon

- Open Source Projects



ISOVALENT

now part of CISCO

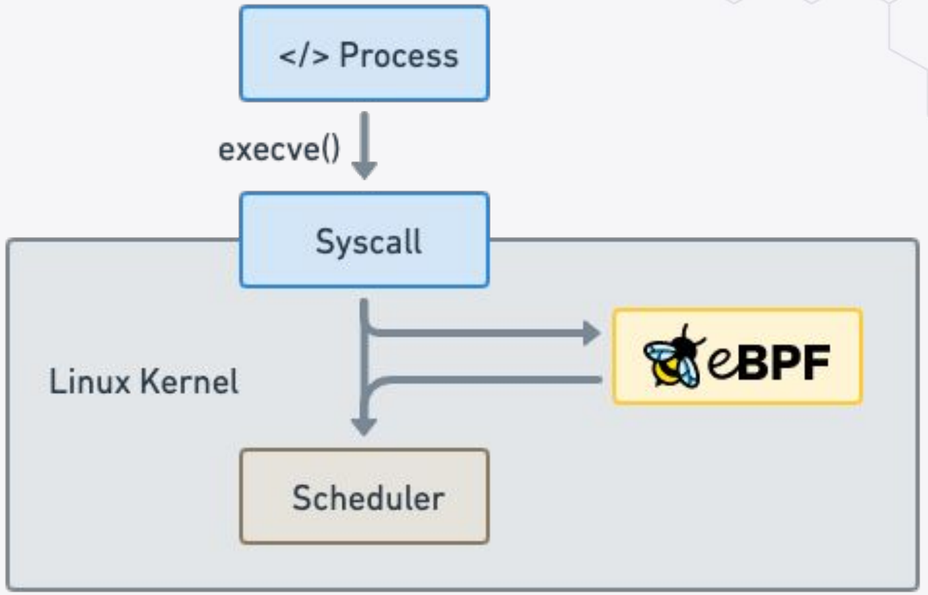
- Company behind Cilium & Tetragon
- Provides Cilium Enterprise


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”

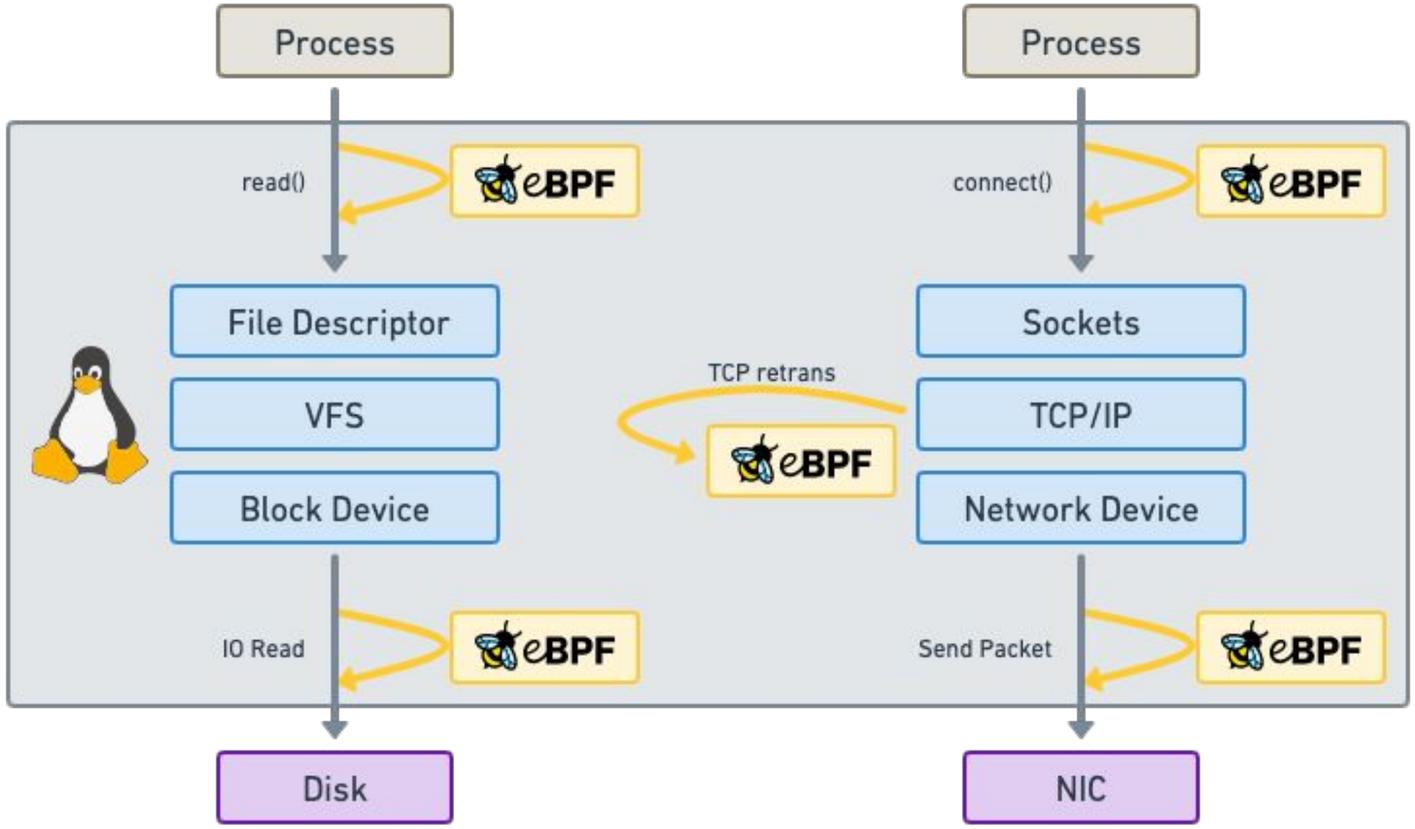



```c
int syscall__ret_execve(struct pt_regs *ctx)
{
        struct comm_event event = {
                .pid = bpf_get_current_pid_tgid() >> 32,
                .type = TYPE_RETURN,
        };

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

        return 0;
}
```

Run eBPF programs on events



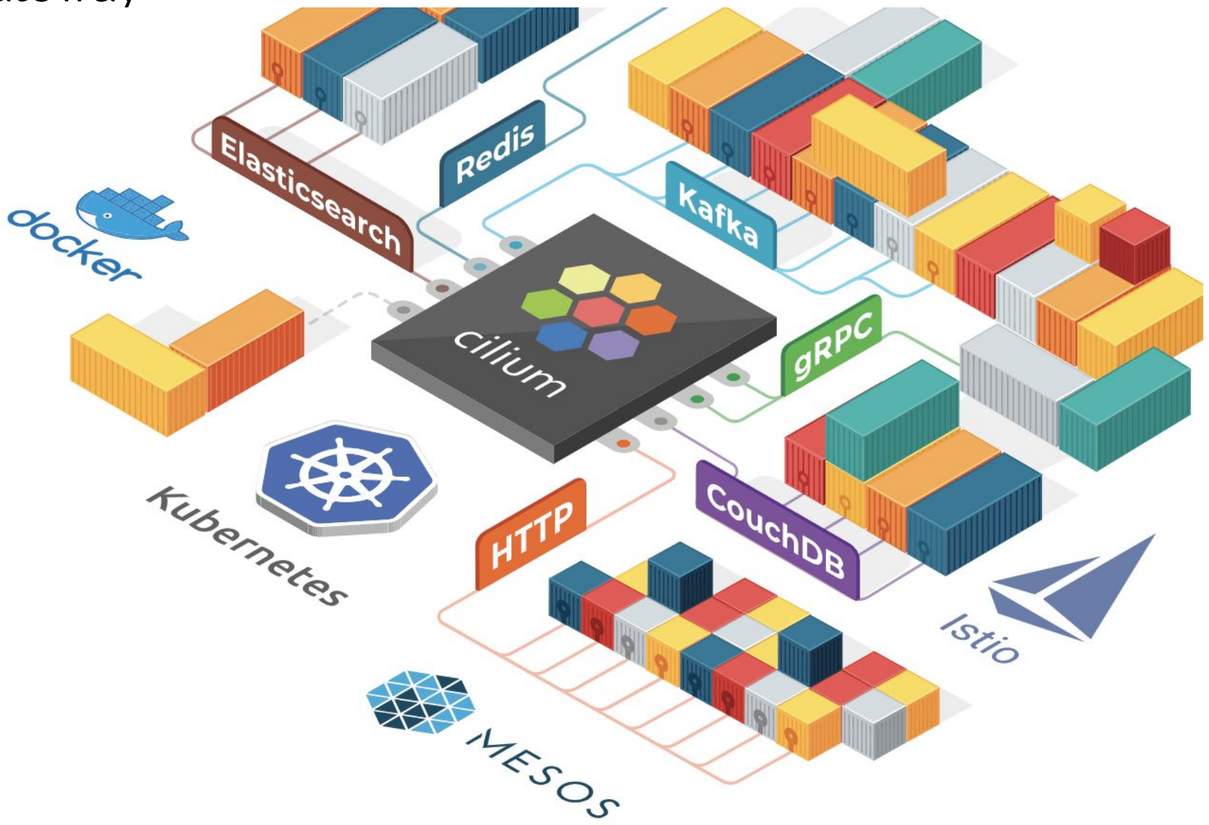
Attachment points

- 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



In this Session

Cilium Features Deep Dive

BGP Control Plane

BGP

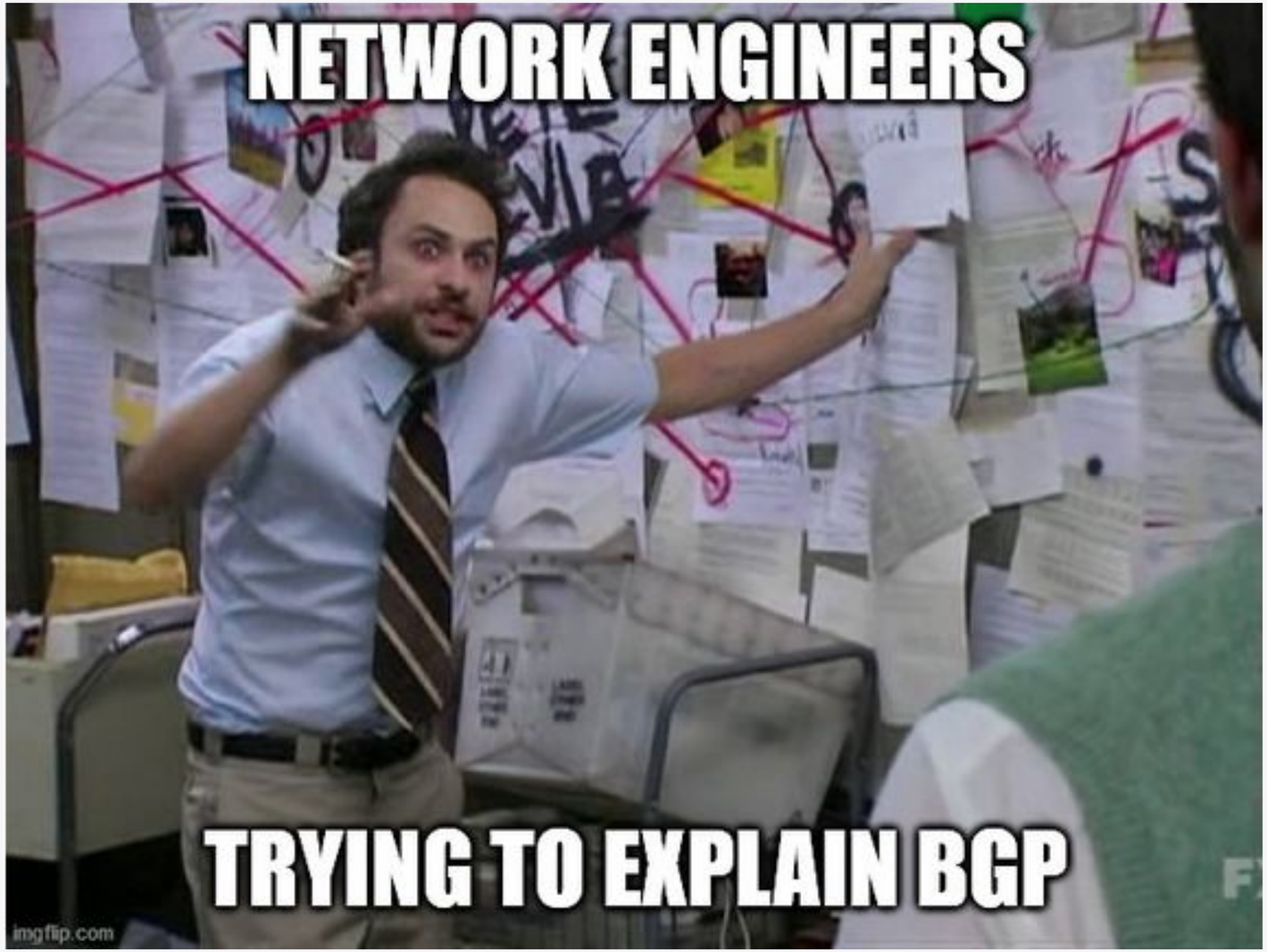
BGP

Use Cases

- External Network Connectivity
  - Ingress
  - Egress
- Automation
- Availability
- Recoverability
- Traffic Engineering

Challenges

- Multi-Tenancy
- Security
- Traffic Optimization

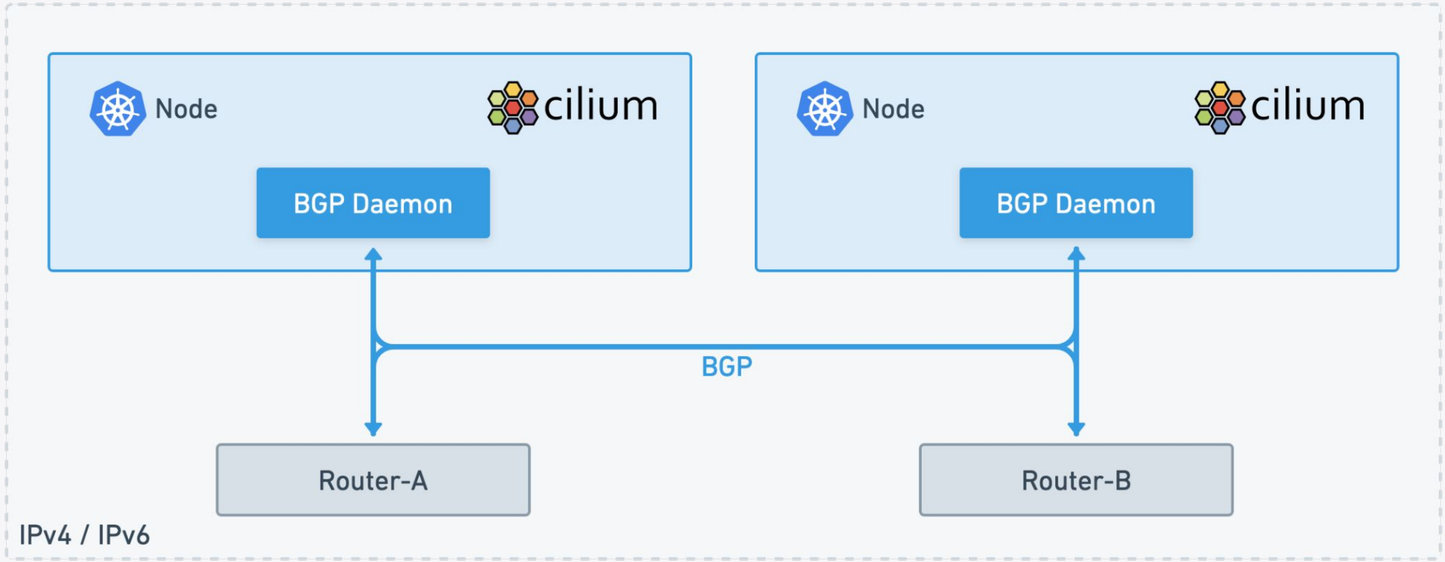

NETWORK ENGINEERS
TRYING TO EXPLAIN BGP
imgflip.com

BGP Introduction

- BGP is a dynamic routing protocol. It uses TCP port 179.
- BGP neighbours exchange routing information over a peering session.
- A given router can build a BGP peering session with one or multiple other routers.

Cilium BGP Control Plane

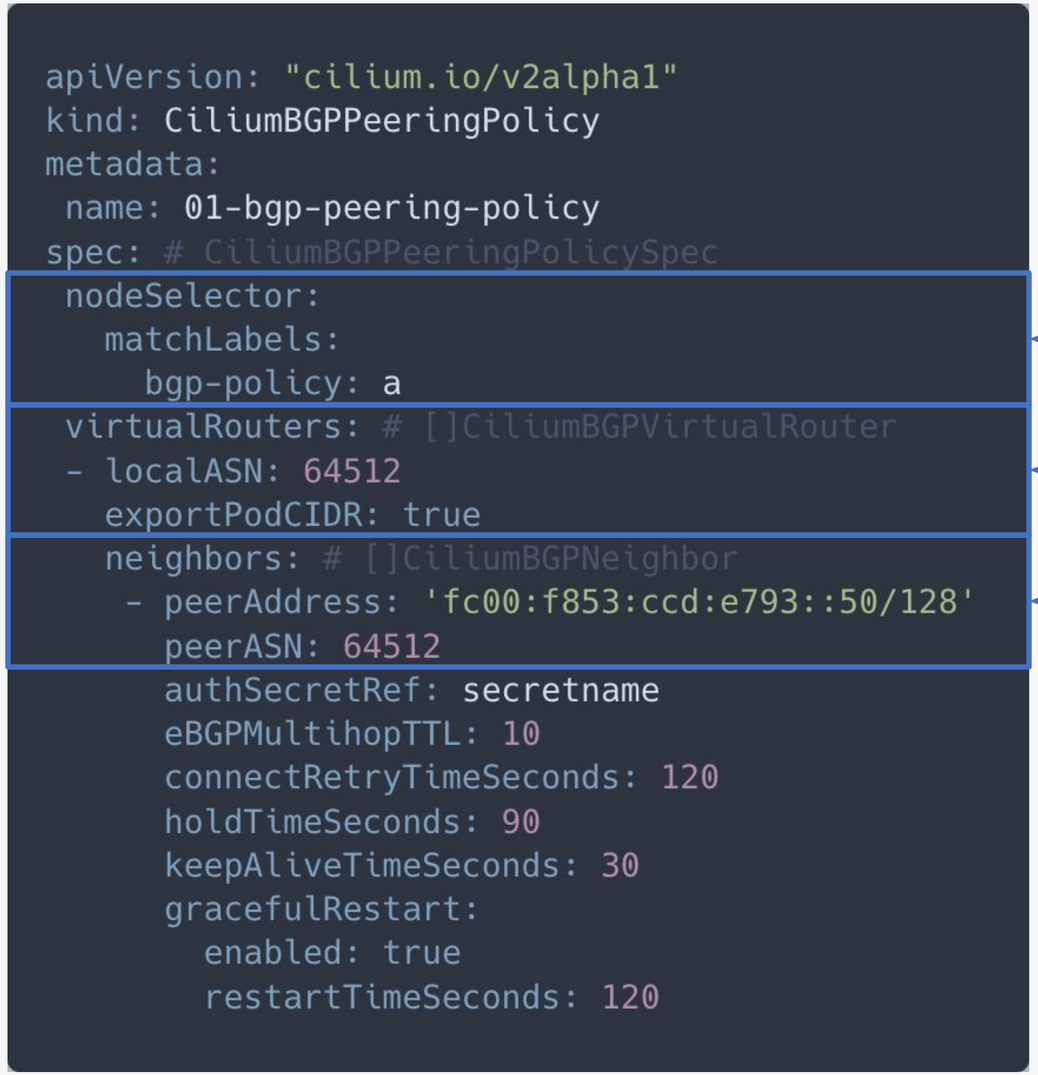
- BGP natively supported in Cilium
- GoBGP-based
- Feature-rich BGP support
  - IPv4 & IPv6
  - PodCIDR and/or Service IPs Advertisements
  - Hold/Keepalive Timers
  - MD5 Password
  - Graceful Restart
  - Multihop
  - Communities
- BGP Operational Tooling



https://isovalent.com/blog/post/connecting-your-kubernetes-island-to-your-network-with-cilium-bgp/

ISOVALENT

CiliumBGPPeeringPolicy CRD



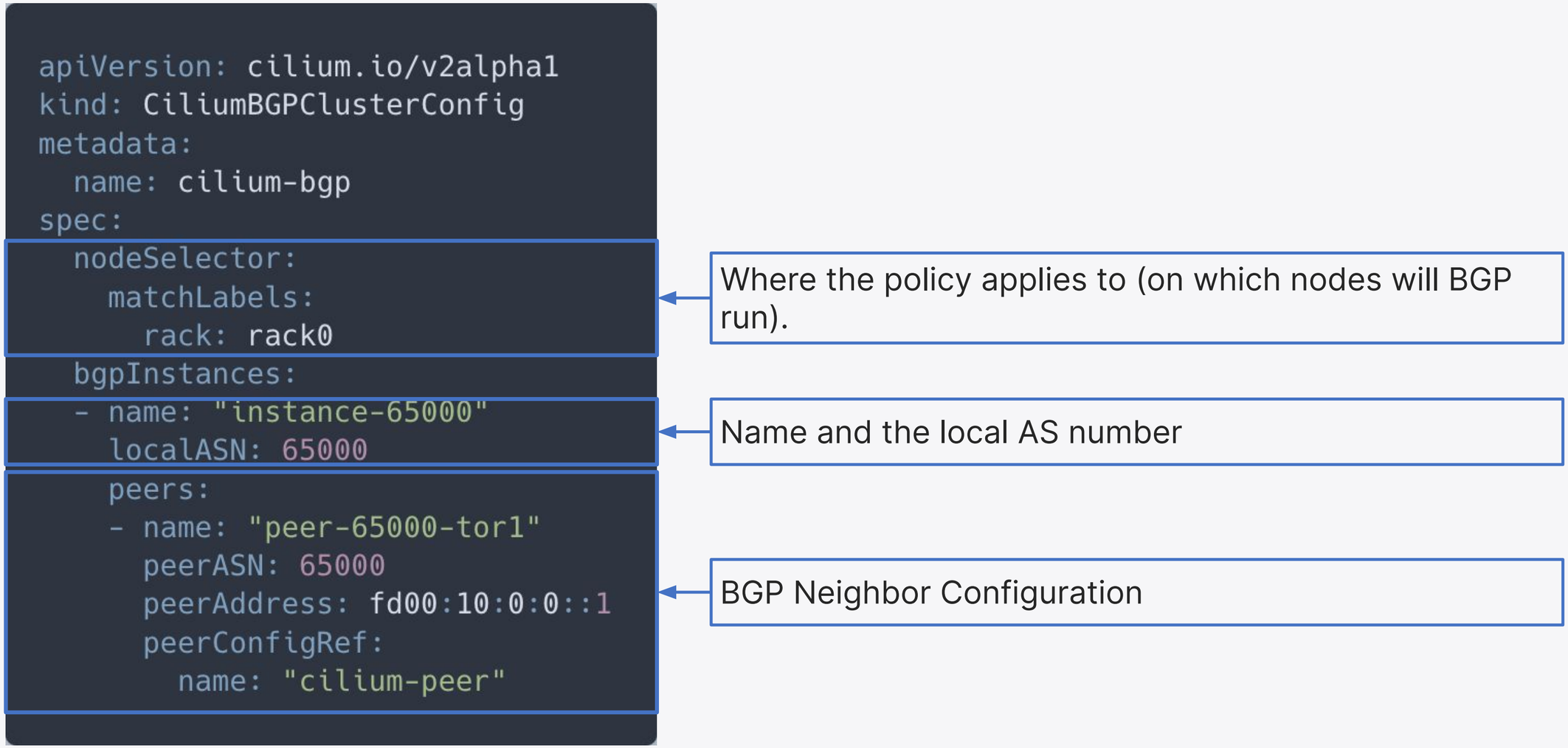
```yaml
apiVersion: "cilium.io/v2alpha1"
kind: CiliumBGPPeeringPolicy
metadata:
 name: 01-bgp-peering-policy
spec: # CiliumBGPPeeringPolicySpec
 nodeSelector:
   matchLabels:
     bgp-policy: a
 virtualRouters: # []CiliumBGPVirtualRouter
 - localASN: 64512
   exportPodCIDR: true
   neighbors: # []CiliumBGPNeighbor
    - peerAddress: 'fc00:f853:ccd:e793::50/128'
      peerASN: 64512
      authSecretRef: secretname
      eBGPMultihopTTL: 10
      connectRetryTimeSeconds: 120
      holdTimeSeconds: 90
      keepAliveTimeSeconds: 30
      gracefulRestart:
        enabled: true
        restartTimeSeconds: 120
```

Where the policy applies to (on which nodes will BGP run).

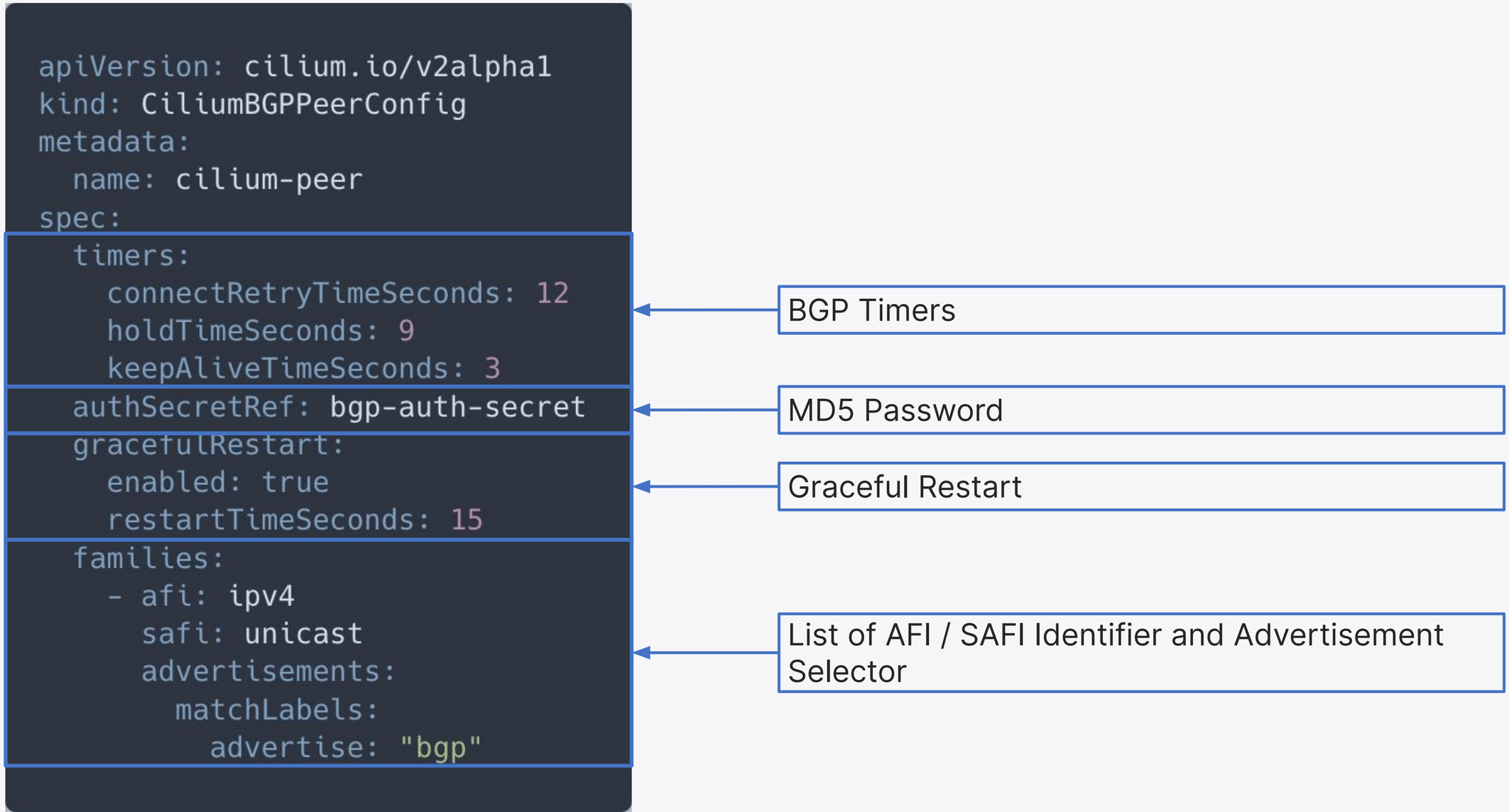
In which Autonomous System the router operate and whether Cilium advertises PodCIDRs

BGP Neighbor Configuration

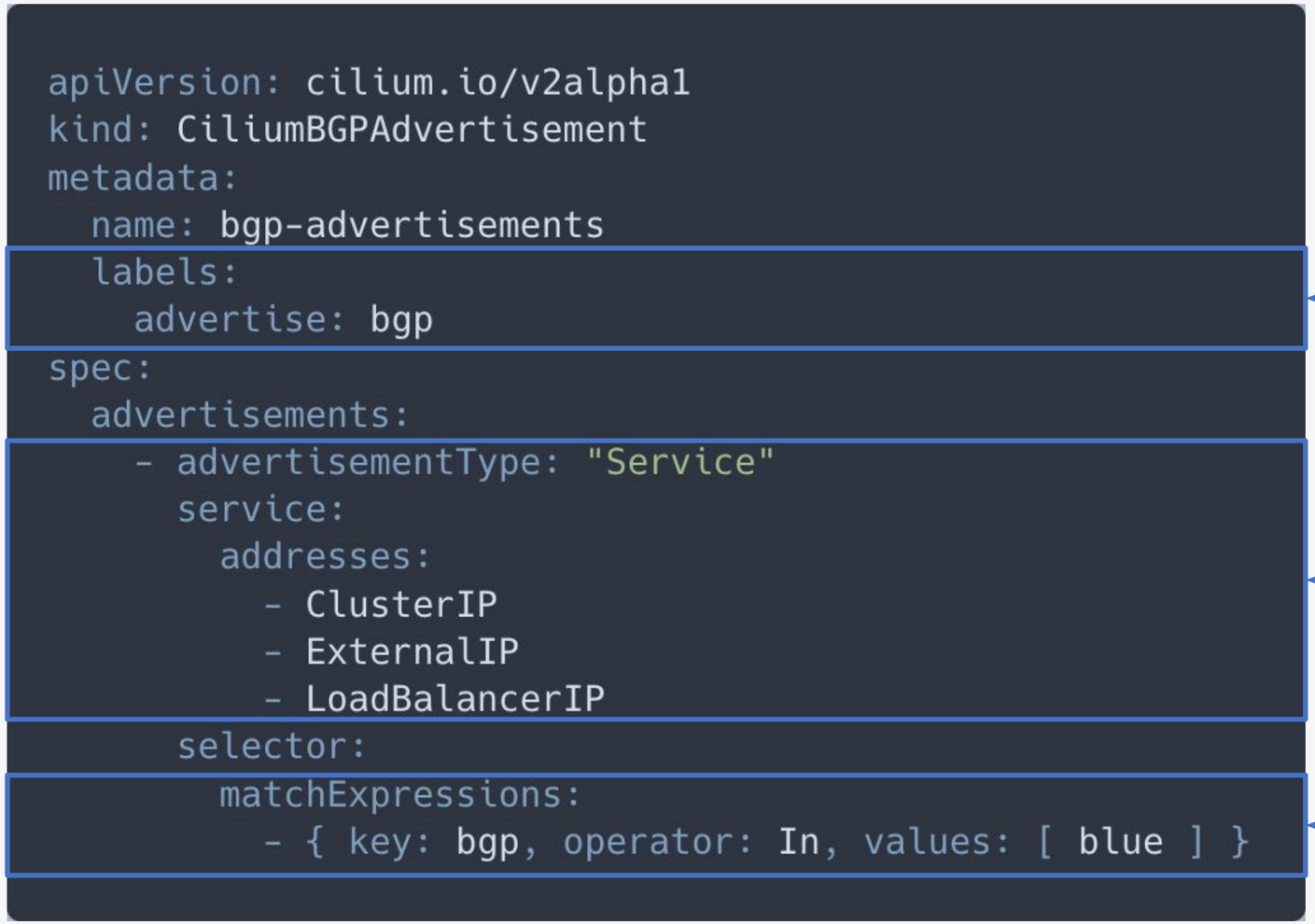
CiliumBGPClusterConfig CRD



CiliumBGPPeerConfig CRD



CiliumBGPAdvertisement CRD



```yaml
apiVersion: cilium.io/v2alpha1
kind: CiliumBGPAdvertisement
metadata:
  name: bgp-advertisements
  labels:
    advertise: bgp
spec:
  advertisements:
    - advertisementType: "Service"
      service:
        addresses:
          - ClusterIP
          - ExternalIP
          - LoadBalancerIP
      selector:
        matchExpressions:
          - { key: bgp, operator: In, values: [ blue ] }
```

Labels referenced by CiliumBGPPeerConfig

Advertisement Type and Address to Advertise:
- Pod CIDR ranges
- Service Virtual IPs
- Pod IP Pool (MultiPool IPAM)

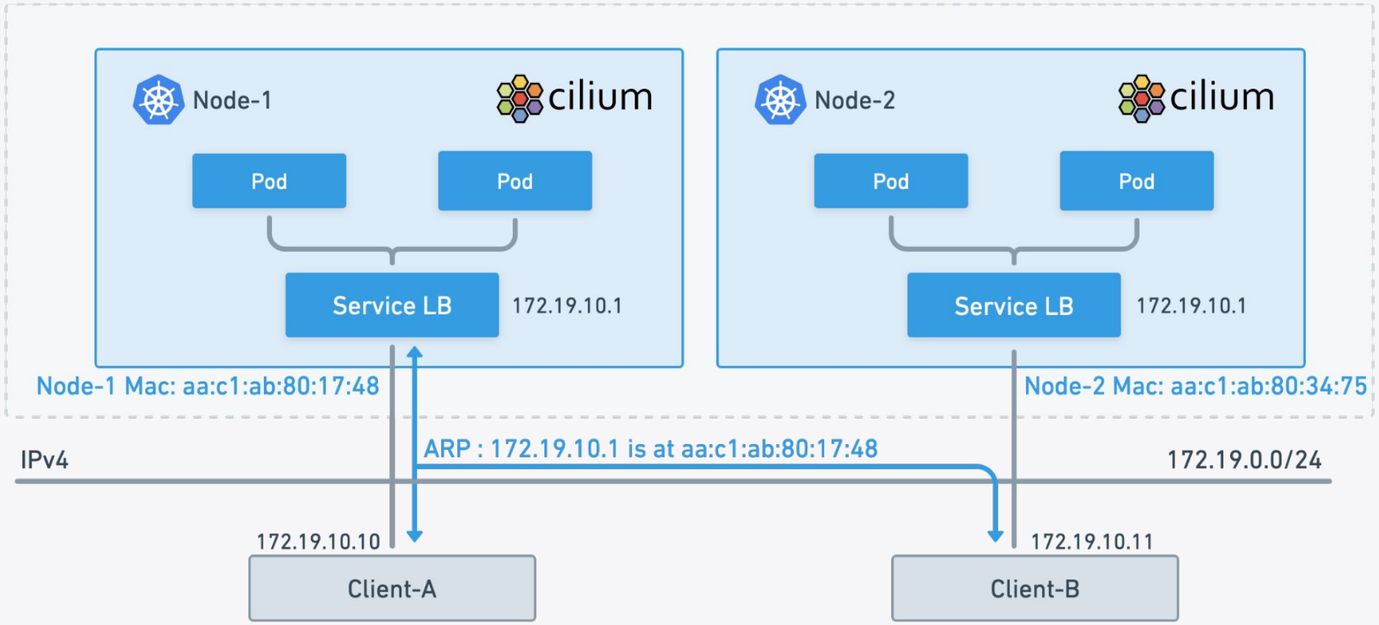
Selector for Advertisement

L2 Announcements

L2 Announcements

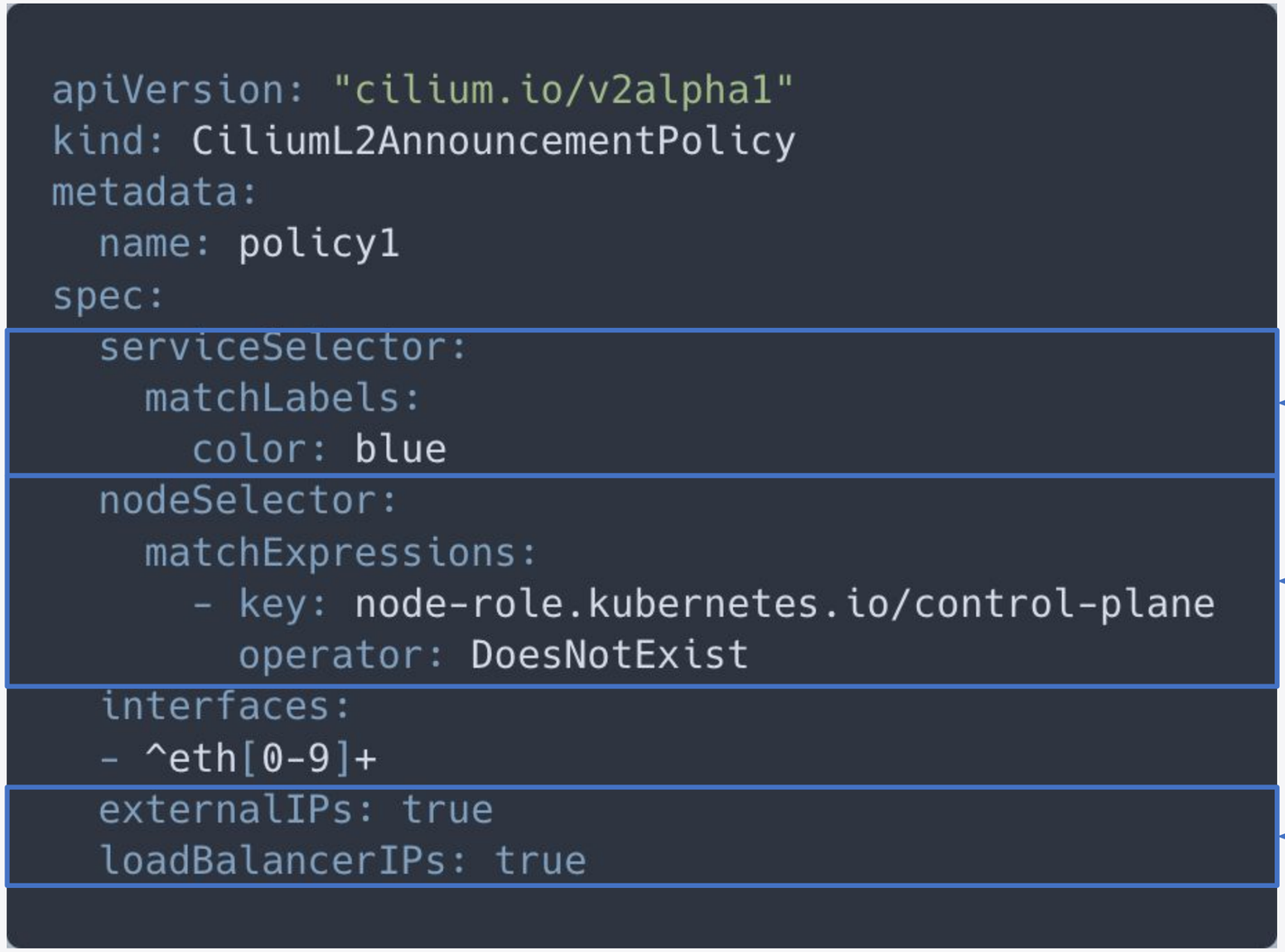
L2 Announcements

- Cilium responds to ARP queries from local clients for ExternalIPs and/or LoadBalancer IPs.
- Virtual IPs on multiple nodes, however only one Node will respond at a time and will act as a North-South LoadBalancer.



https://docs.cilium.io/en/stable/network/l2-announcements/#l2-announcements

CiliumL2AnnouncementPolicy



Service Selector

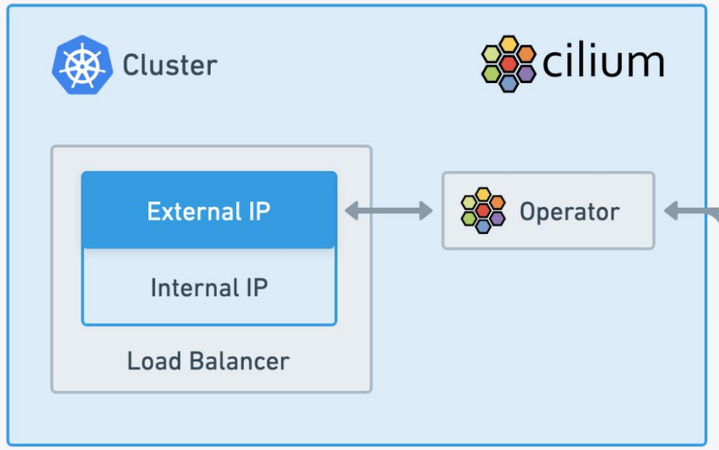
Node Selector

Announce ExternalIPs and/or LoadBalancerIPs

LB IPAM

LoadBalancer IP Address Management (LB IPAM)

- Automatically assign IP addresses to Kubernetes Services of the type LoadBalancer
- Define which services can get IPs from which pools using a label selector or based on the service name or the service namespace.
- Assigned IP addresses can then be advertised to BGP neighbors.



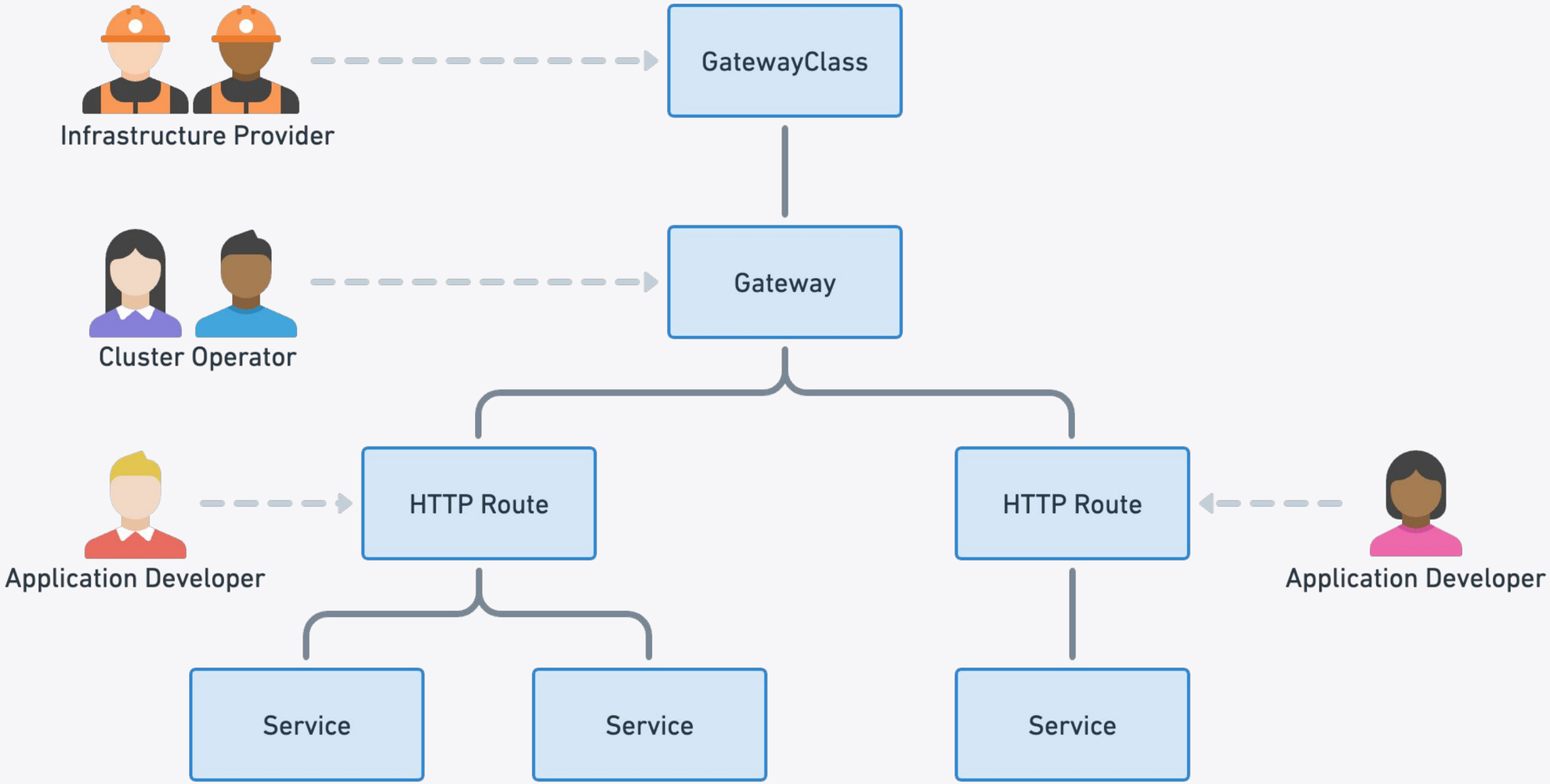

```yaml
apiVersion: "cilium.io/v2alpha1"
kind: CiliumLoadBalancerIPPool
metadata:
  name: "ip-pool-blue"
spec:
  cidrs:
  - cidr: "20.0.10.0/24"
  serviceSelector:
    matchExpressions:
      - {key: color, operator: In, values: [blue]}
```

```yaml
apiVersion: v1
kind: Service
metadata:
  name: service-blue
  namespace: blue
  labels:
    name: blue
spec:
  type: LoadBalancer
  ports:
  - port: 80
```

Gateway API

Gateway API

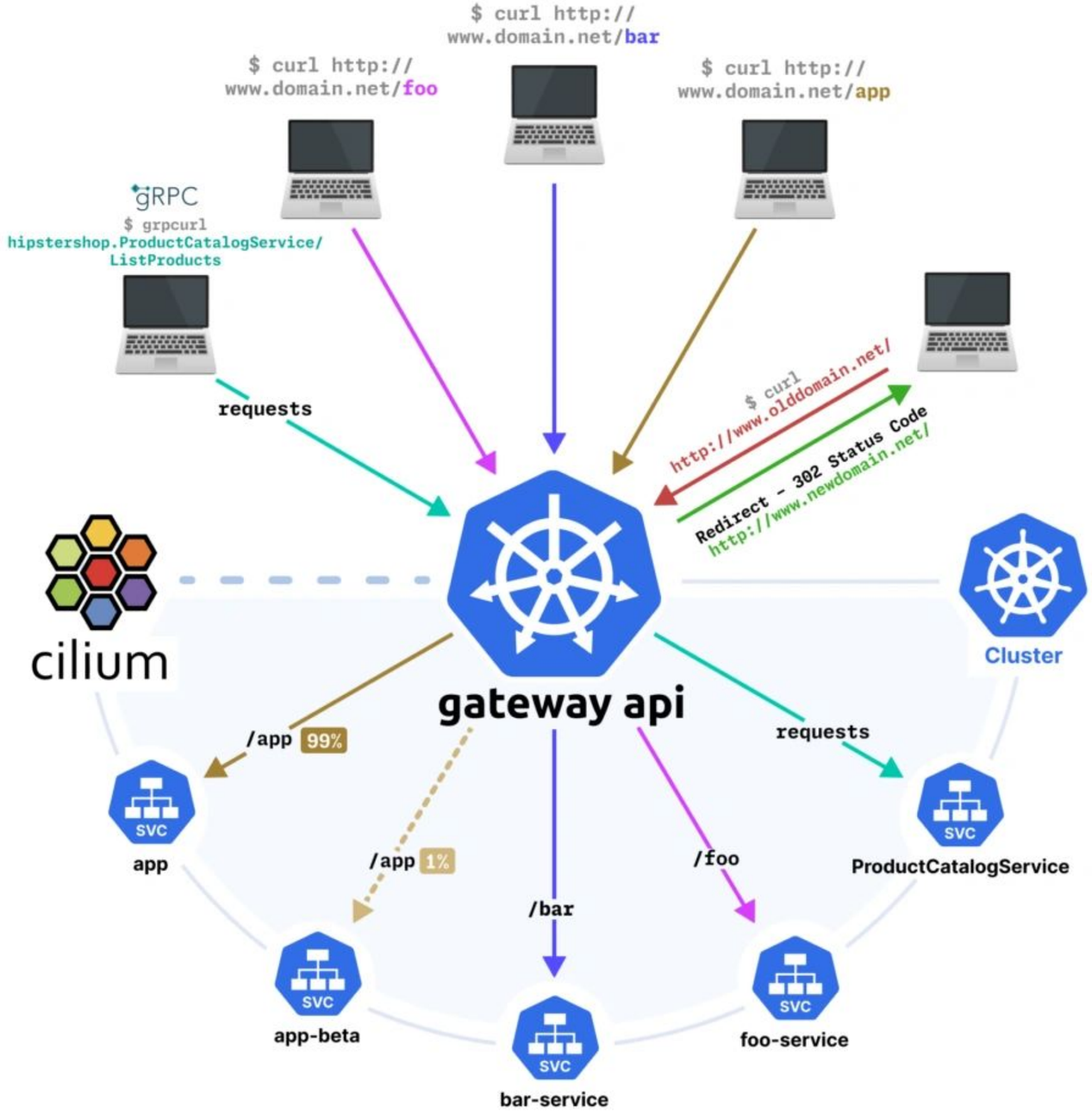
Introduction



Gateway API

Use Cases

- Traffic Management
  - Rolling deployments
  - A/B Testing
  - Traffic Splitting
  - Canary
  - Blue-Green
- Scalability
- Golden Signals

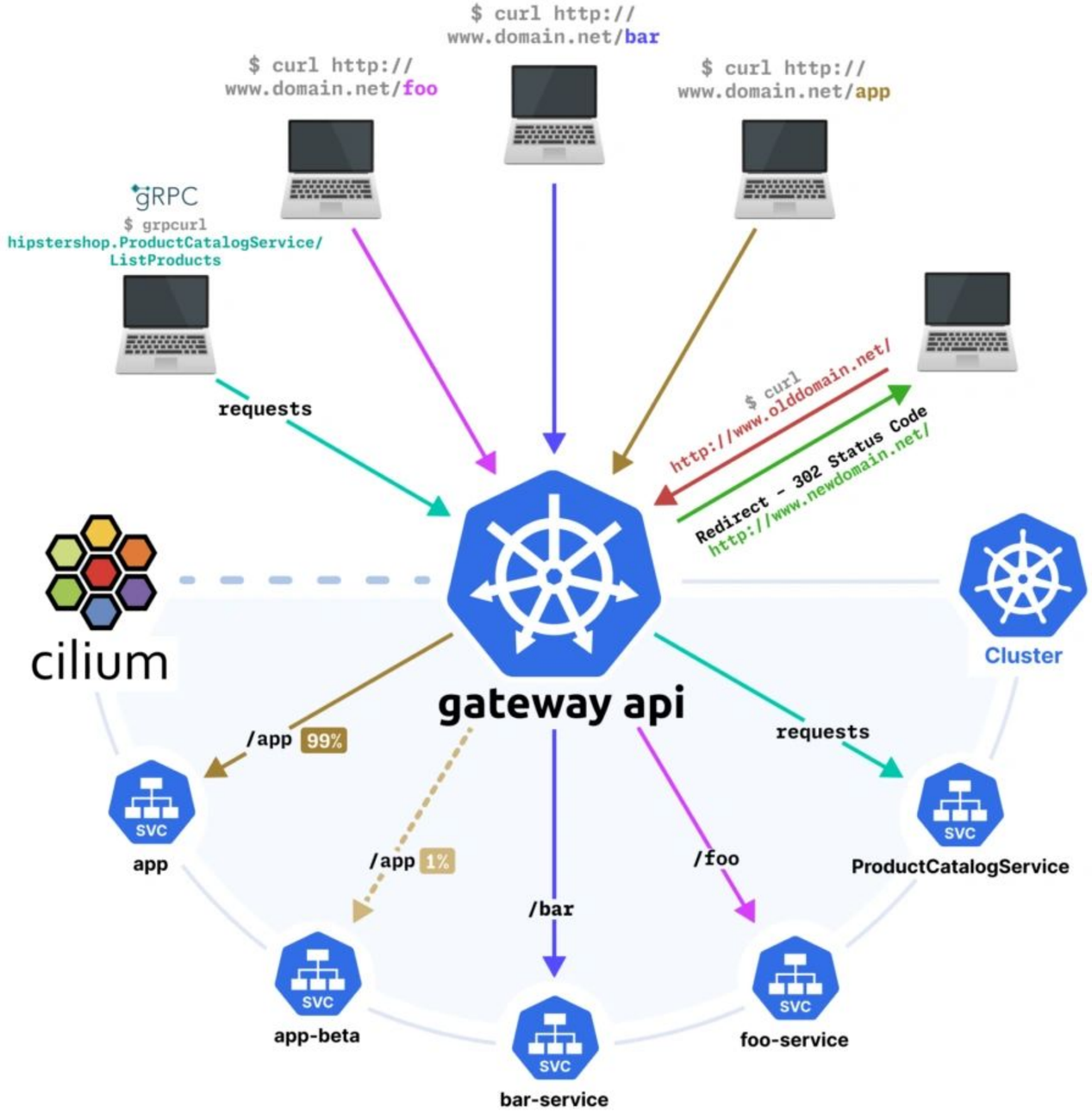


Gateway API

Cilium Supports Gateway API 1.0

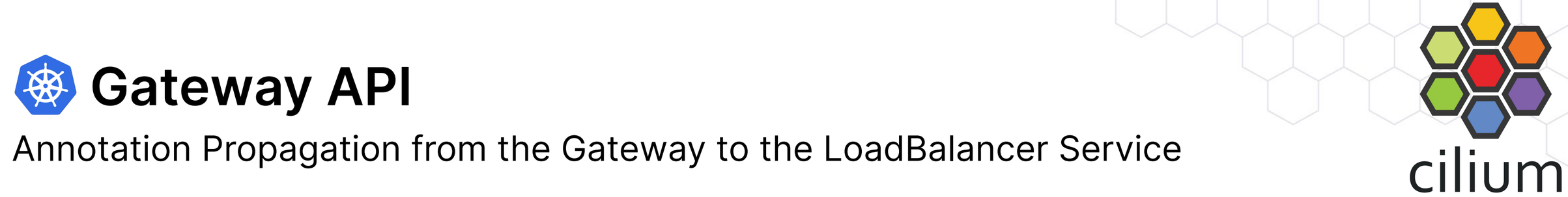
Features

- HTTP routing
- HTTP traffic splitting and load-balancing
- HTTP request and response header rewrite
- HTTP redirect and path rewrites
- HTTP mirroring
- Cross-namespace routing
- TLS termination and passthrough
- gRPC routing



Gateway API

Annotation Propagation from the Gateway to the LoadBalancer Service




```yaml
apiVersion: gateway.networking.k8s.io/v1
kind: Gateway
metadata:
  name: gateway-blue
  namespace: tenant-blue
spec:
  infrastructure:
    labels:
      color: blue
  gatewayClassName: cilium
  listeners:
  - protocol: HTTP
    port: 80
    name: gateway-blue-http
    allowedRoutes:
      namespaces:
        from: Same
```

```
# kubectl describe service -n tenant-blue cilium-gateway-gateway-blue
Name:                     cilium-gateway-gateway-blue
Namespace:                tenant-blue
Labels:                   color=blue
                          io.cilium.gateway/owning-gateway=gateway-blue
Annotations:              <none>
Selector:                 <none>
Type:                     LoadBalancer
IP Family Policy:         SingleStack
IP Families:              IPv4
IP:                       10.96.82.188
IPs:                      10.96.82.188
LoadBalancer Ingress:     20.0.10.1
Port:                     port-80  80/TCP
TargetPort:               80/TCP
NodePort:                 port-80  30610/TCP
Endpoints:
Session Affinity:         None
External Traffic Policy:  Cluster
Events:                   <none>
```

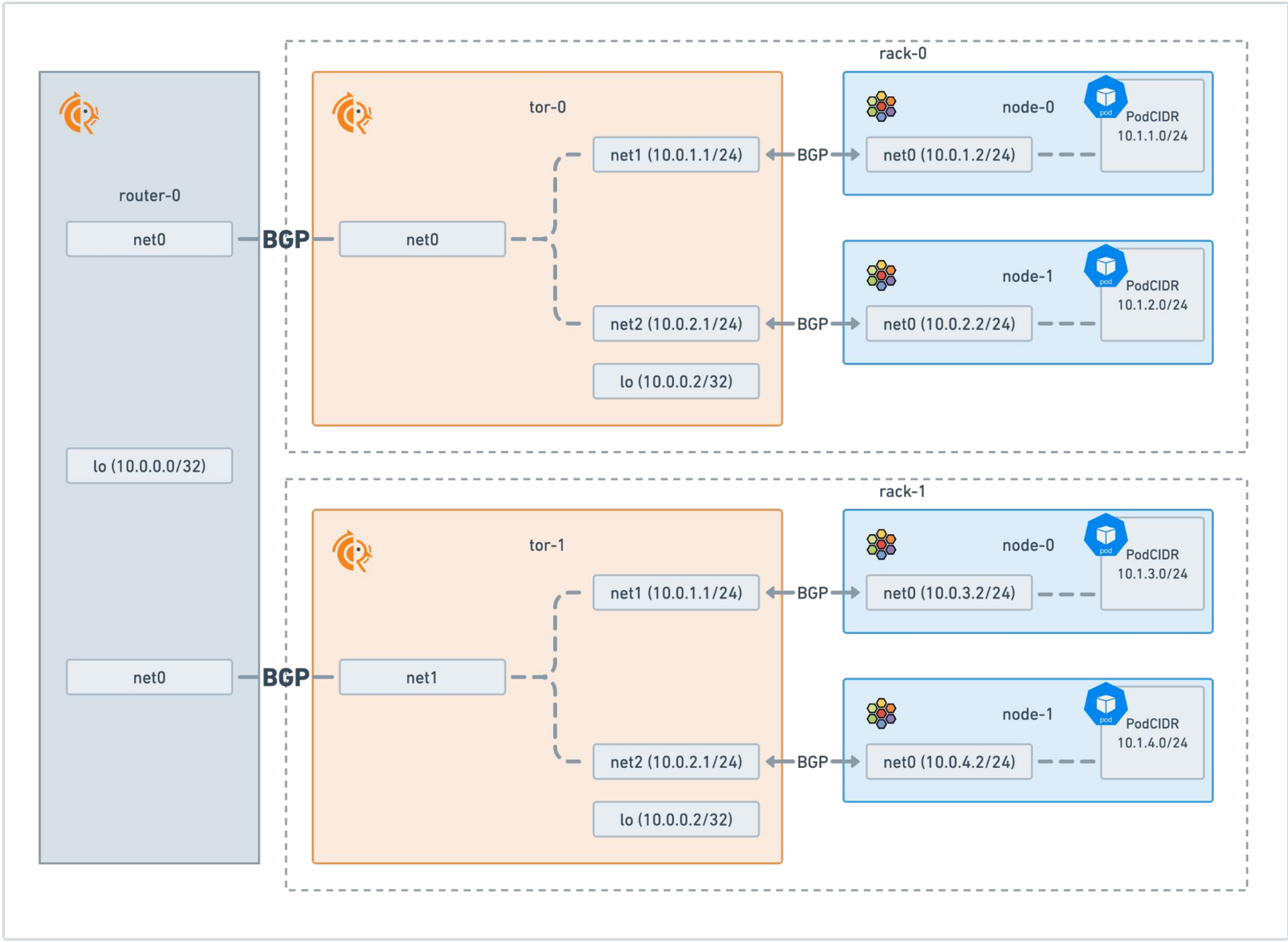
Demo

Demo

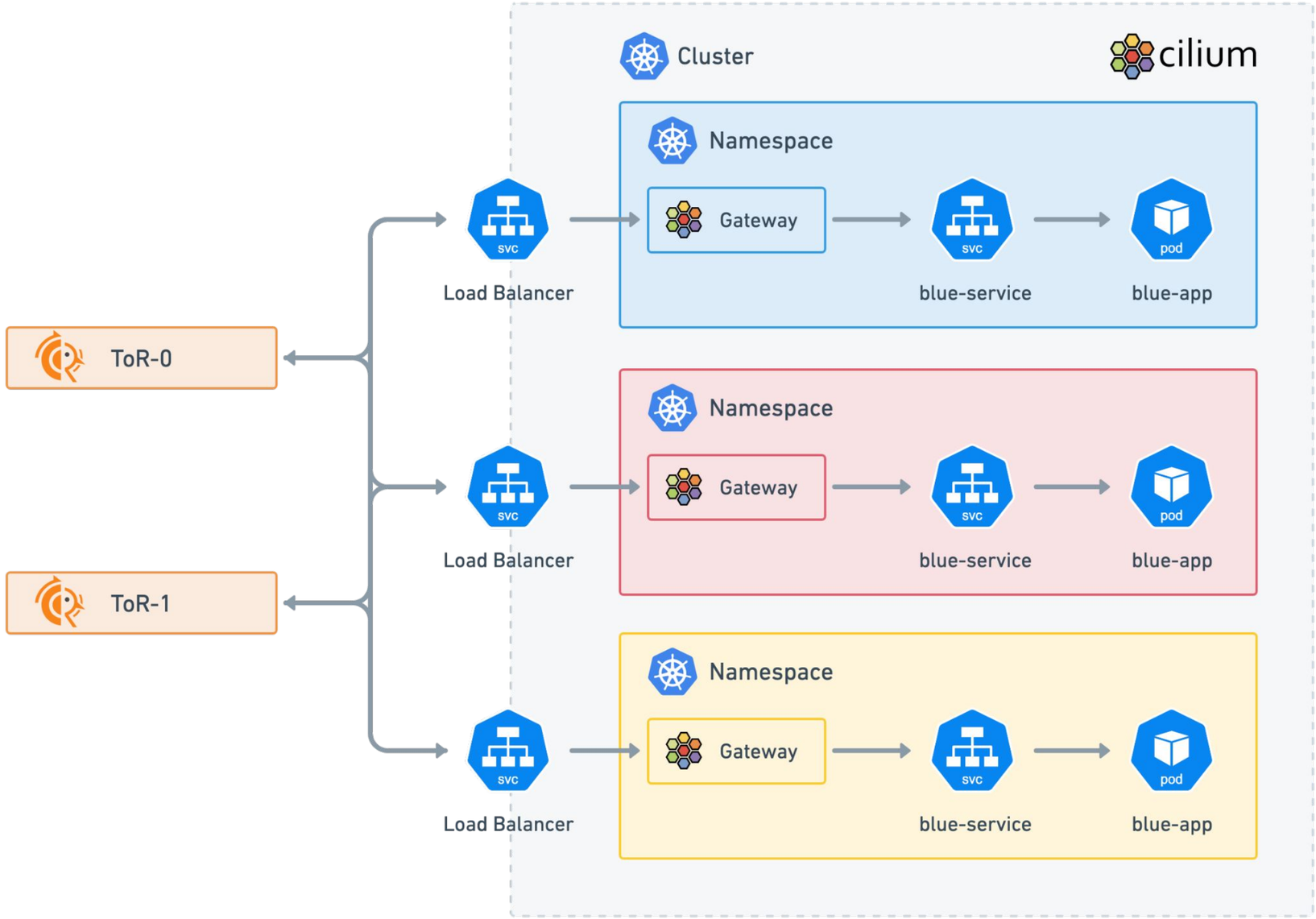
As a Platform Engineer I want to:

- Support a multi-tenant Kubernetes platform
- Provide separation and segmentation for each tenant
  - Using unique Ingress IPs per tenant
  - Using Network Policies for isolation
- Provide L7 Routing and Filtering capabilities
- Advertise LoadBalancer IPs to the external network using BGP

Demo Topology



Demo Topology



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!