Container Networking

State of the Ecosystem

Karthik Prabhakar
kp@tigera.io

PROJECT CALICO

TIGERA
CLOUD NETWORKS, SECURED

Topics

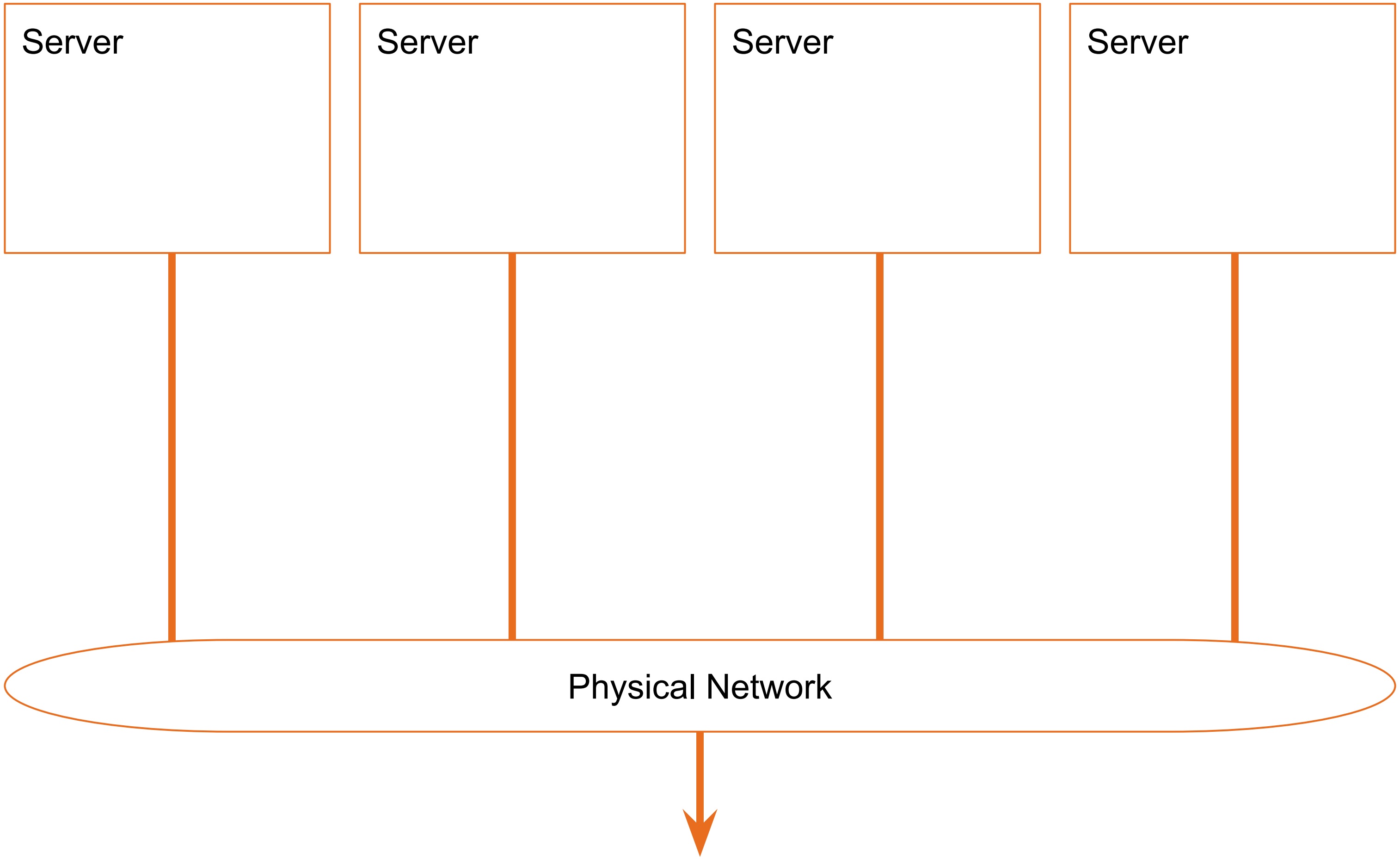
- Network Architecture Redux
- State of the Ecosystem
- Security and Policy
- Looking Forward

Why Should -You- Care?

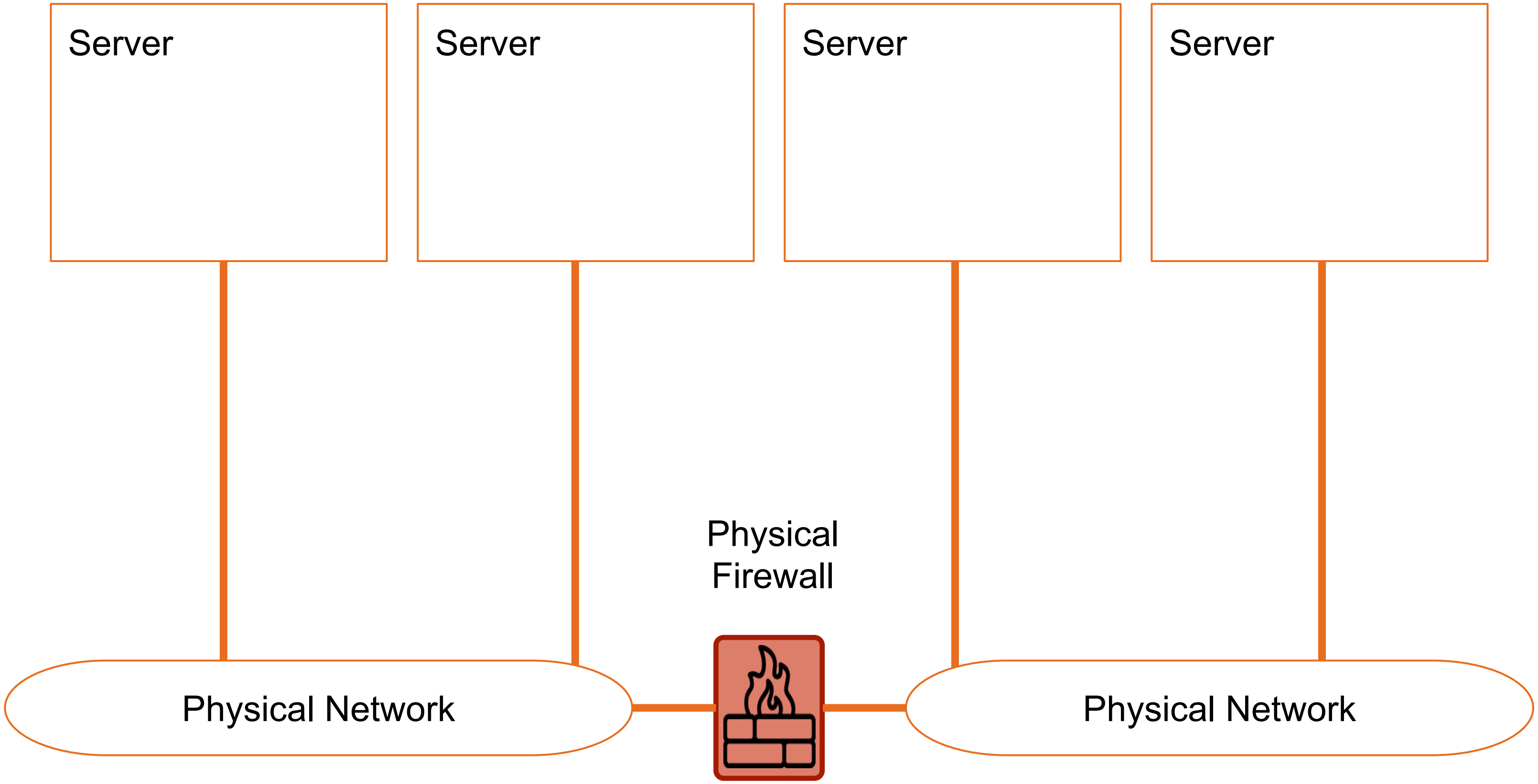
- Network Architecture Redux
  - Lessons learned from decades of Internetwork deployment experience
- State of the Ecosystem
  - Abstractions & Architectures: Understand tradeoffs.
- Security and Policy
  - Enable app isolation with labels and policy automation
- Looking Forward
  - Facilitate planning for new capabilities

Network Architecture & Design

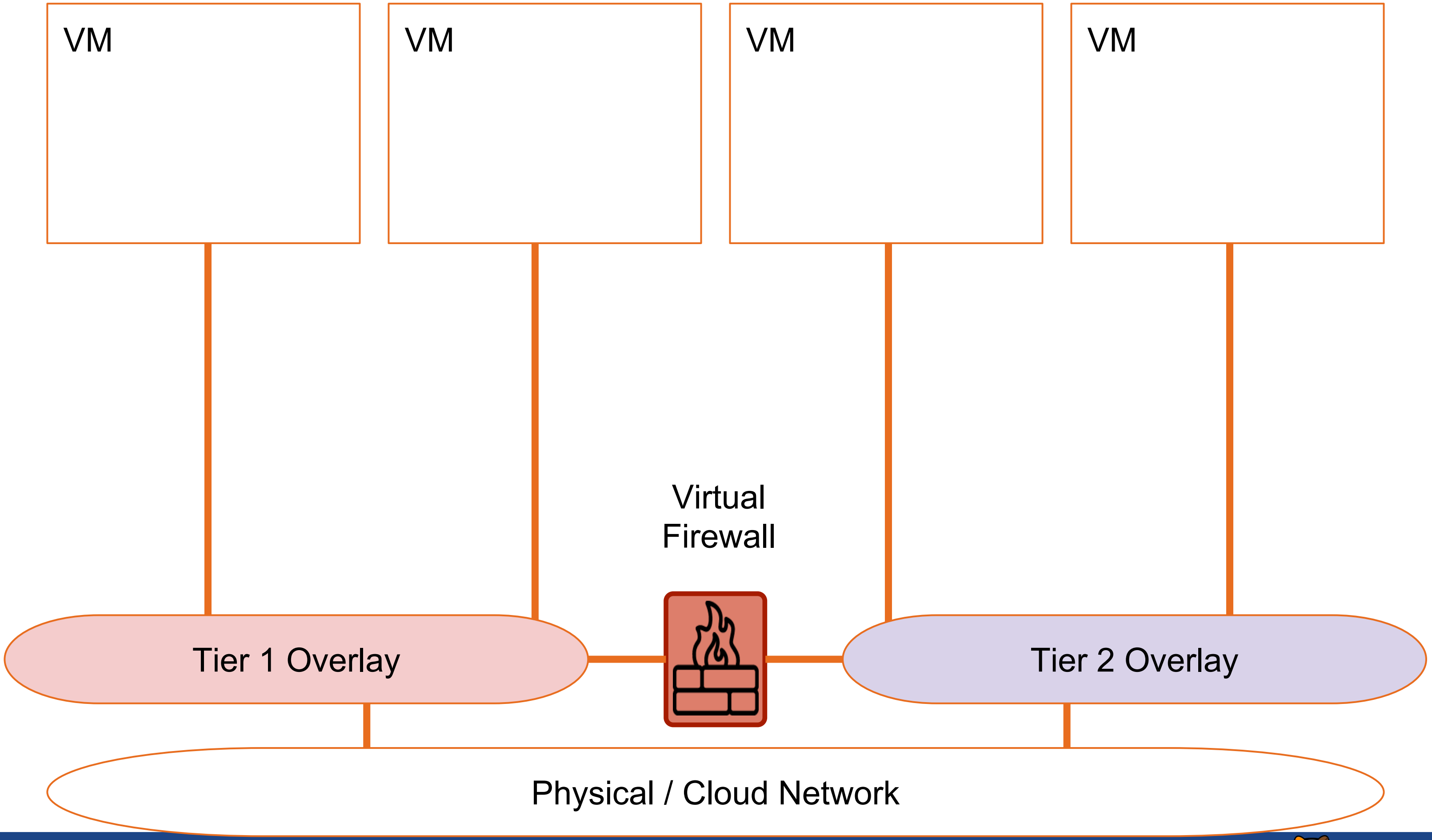
Simple enterprise network



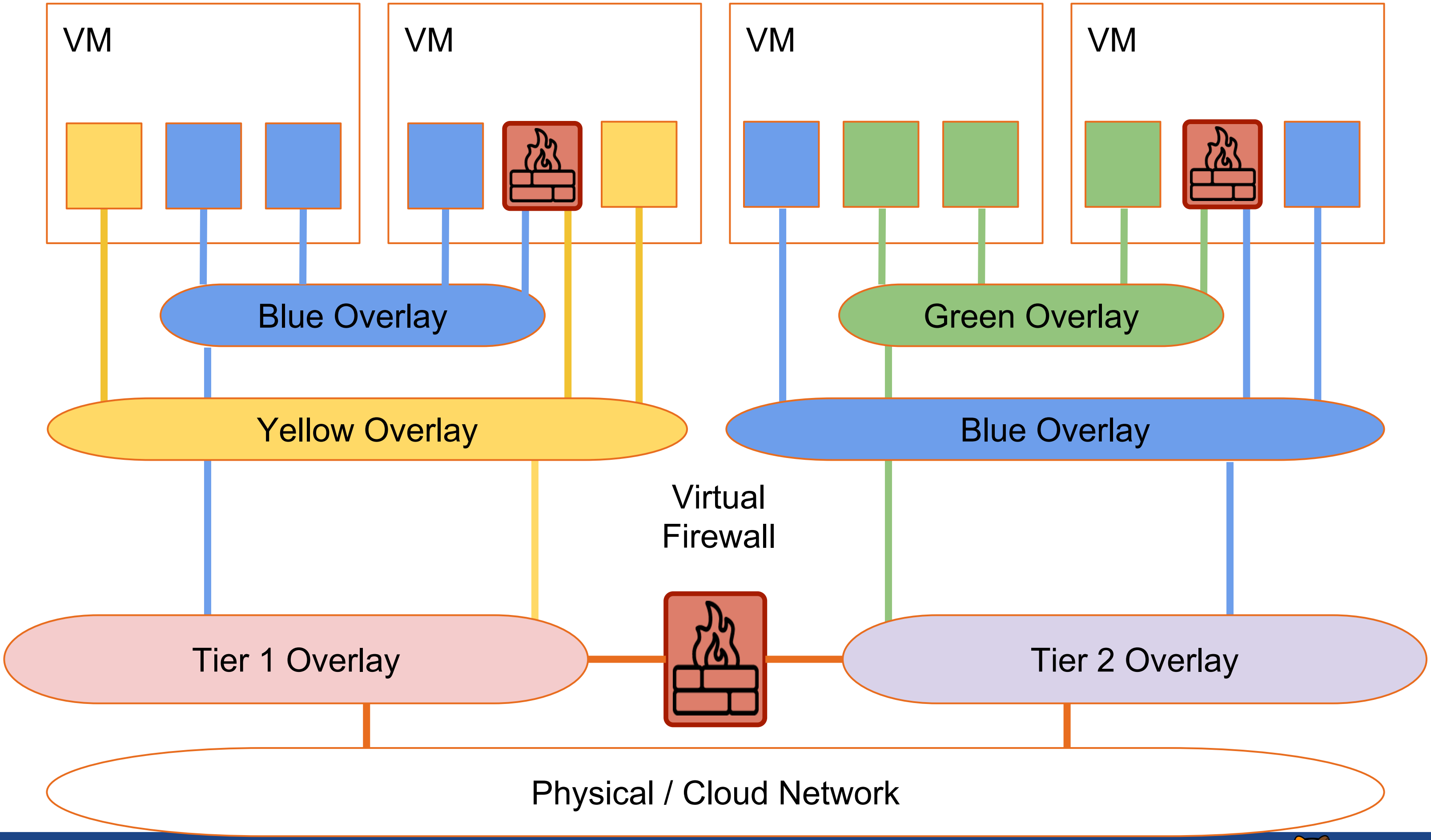
We should probably have some kind of security...



Then came virtualization...



Then came containers...



Scale & Churn

Thousands of instances
Low churn

Millions of containers
High churn

“In networking,...

https://upload.wikimedia.org/wikipedia/commons/1/1b/MSC_Oscar_(ship,_2014)_002.jpg

http://theunholycow.com/wp-content/uploads/2014/03/delivery-man.jpg

… there is no substitute for thinking”

Common Considerations

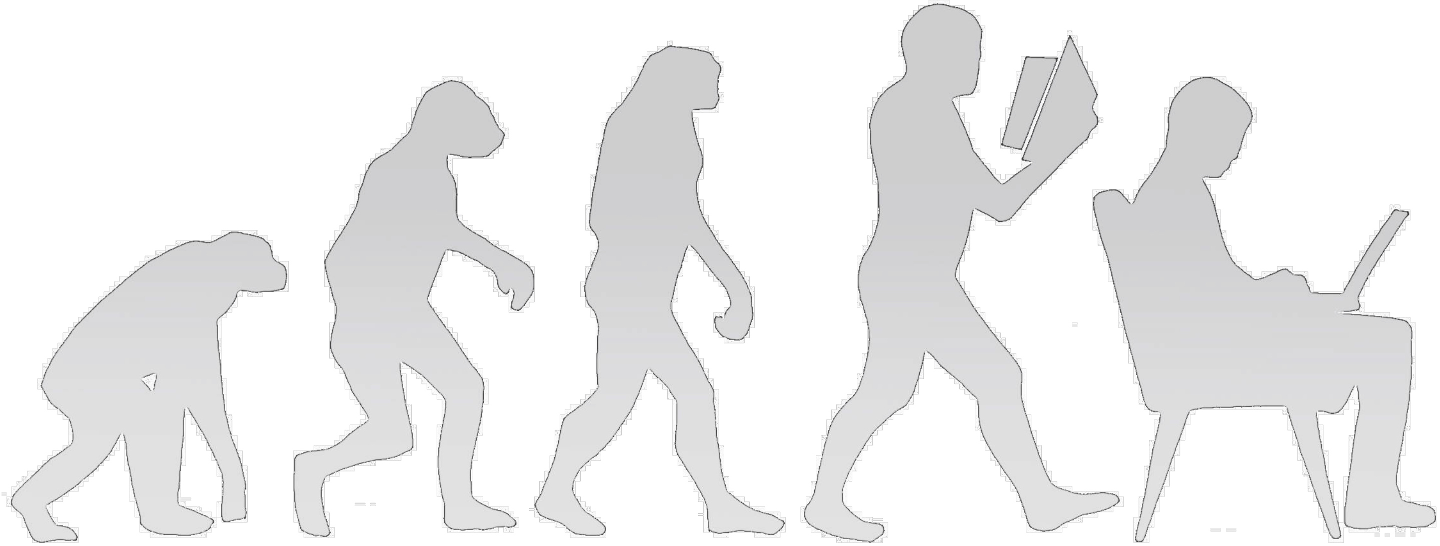
Network Abstraction: L2 (Ethernet) vs. L3 (IP)

Interconnectivity: Overlay vs. Native

Address Space: Admin-assigned vs. Overlapping/BYOA

Visibility: Private vs. DC-wide vs. Filtered

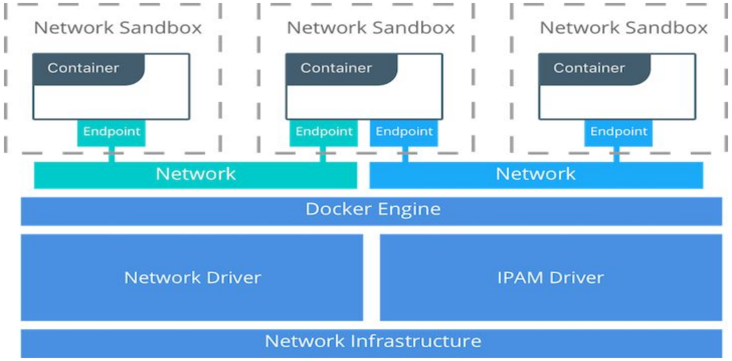
Network State: Centralized vs. Distributed



State of the Ecosystem

Evolution to Alternative Network Abstractions

Container Networking Model (CNM)



Network Sandbox
Container
Endpoint

Network Sandbox
Container
Endpoint
Endpoint

Network Sandbox
Container
Endpoint

Network
Network

Docker Engine

Network Driver
IPAM Driver

Network Infrastructure

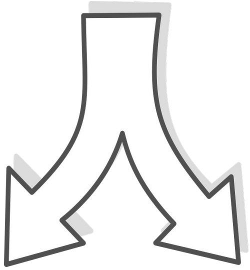
Source: https://success.docker.com/Datacenter/Apply/Docker_Reference_Architecture:_Designing_Scalable,_Portable_Docker_Container_Networks

Orchestrators

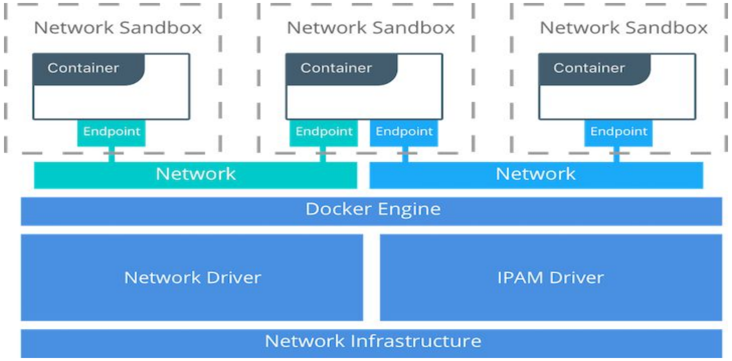
Bridge | Overlay | macvlan | Kuryr | Calico | weavenet ●●●

Drivers / Plugins

Alternative Container Networking Abstractions



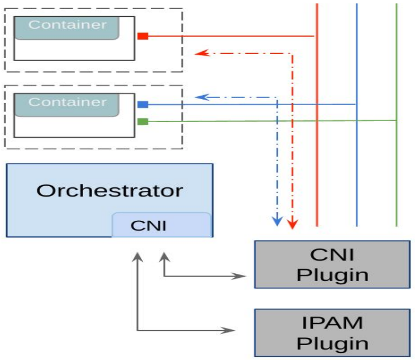
Container Networking Model (CNM)



Source: https://success.docker.com/Datacenter/Apply/Docker_Reference_Architecture:_Designing_Scalable,_Portable_Docker_Container_Networks

docker

Container Networking Interface (CNI)



Orchestrators

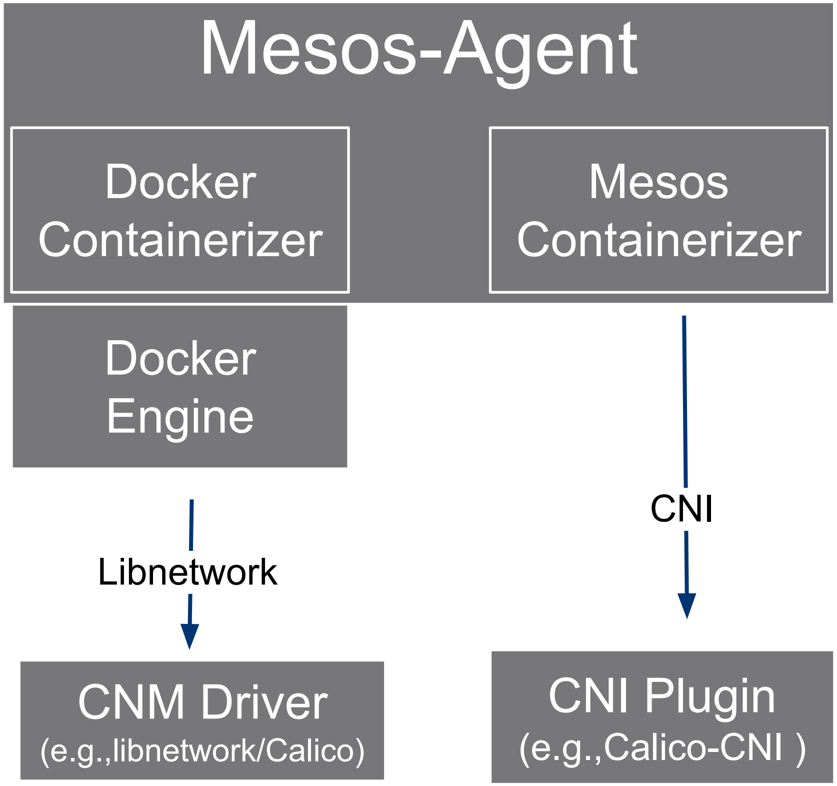
MESOS kubernetes APPRENDA TECTONIC OPENSHIFT RANCHER CLOUD FOUNDRY

Drivers / Plugins

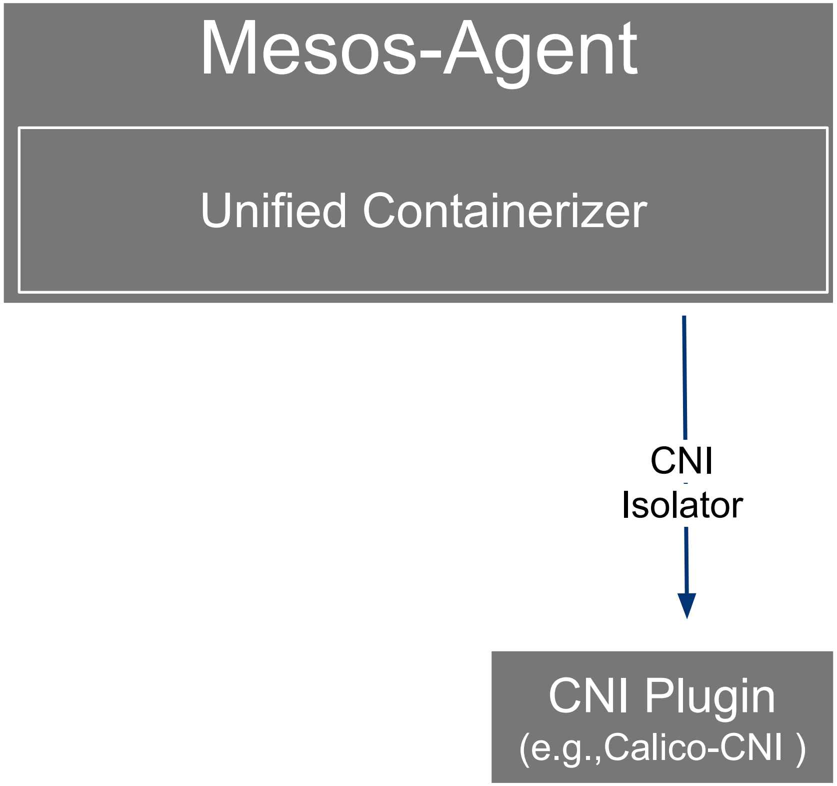
Bridge | Overlay | macvlan | Kuryr | Calico | weavenet | ●●●

flannel | Kuryr | Calico | weavenet | ●●●

Mesos Containerizers



Mesos Containerizers - Unified Containerizer



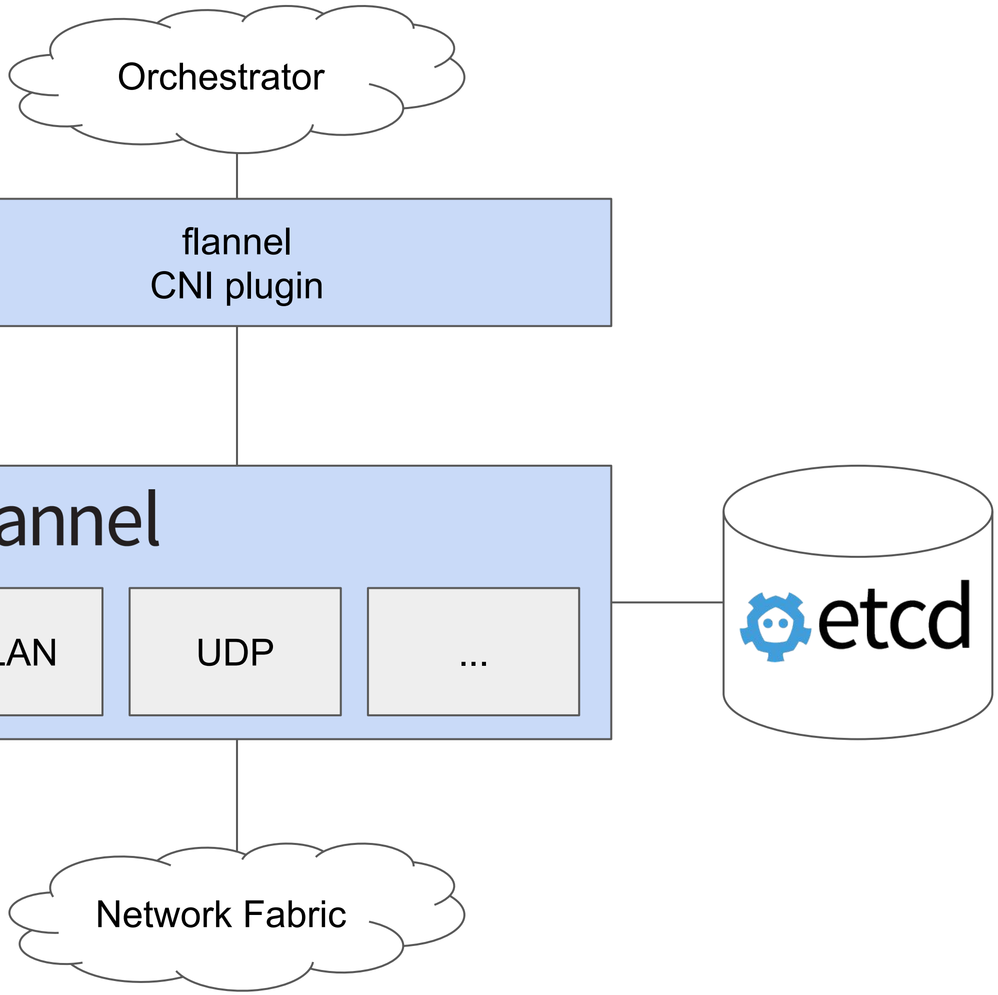
Mesos-Agent

Unified Containerizer

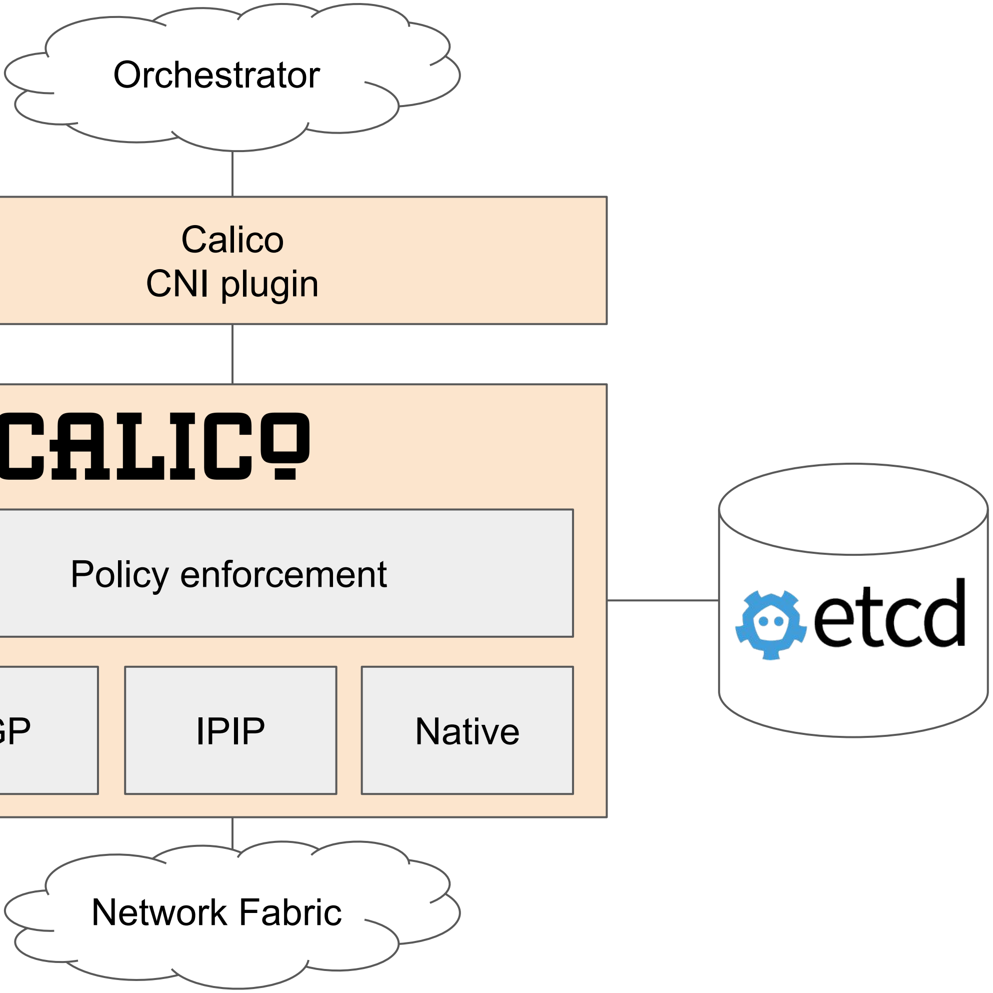
CNI Isolator

CNI Plugin
(e.g.,Calico-CNI)

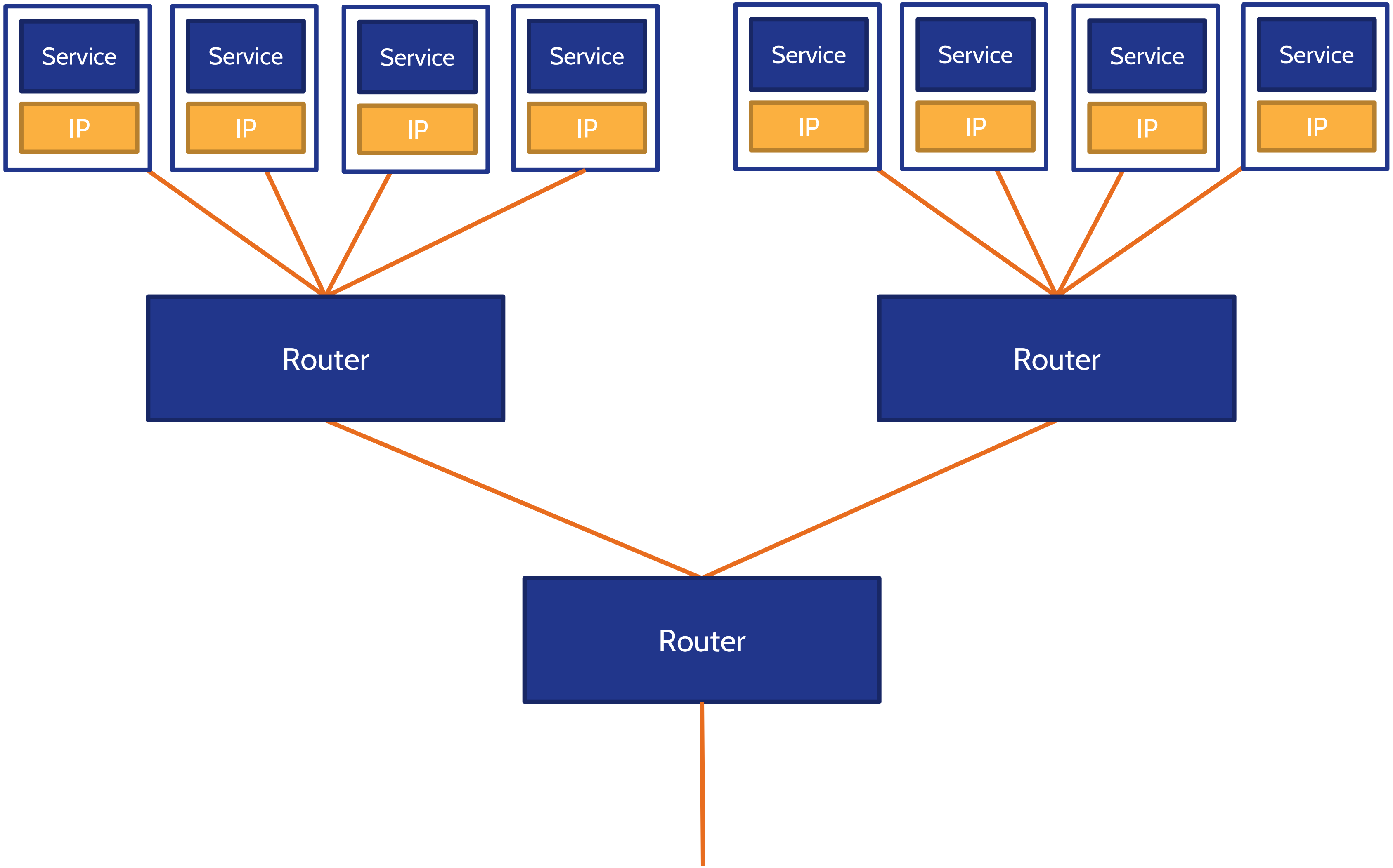
Flannel


Orchestrator
flannel
CNI plugin
flannel
VXLAN
UDP
...
etcd
Network Fabric

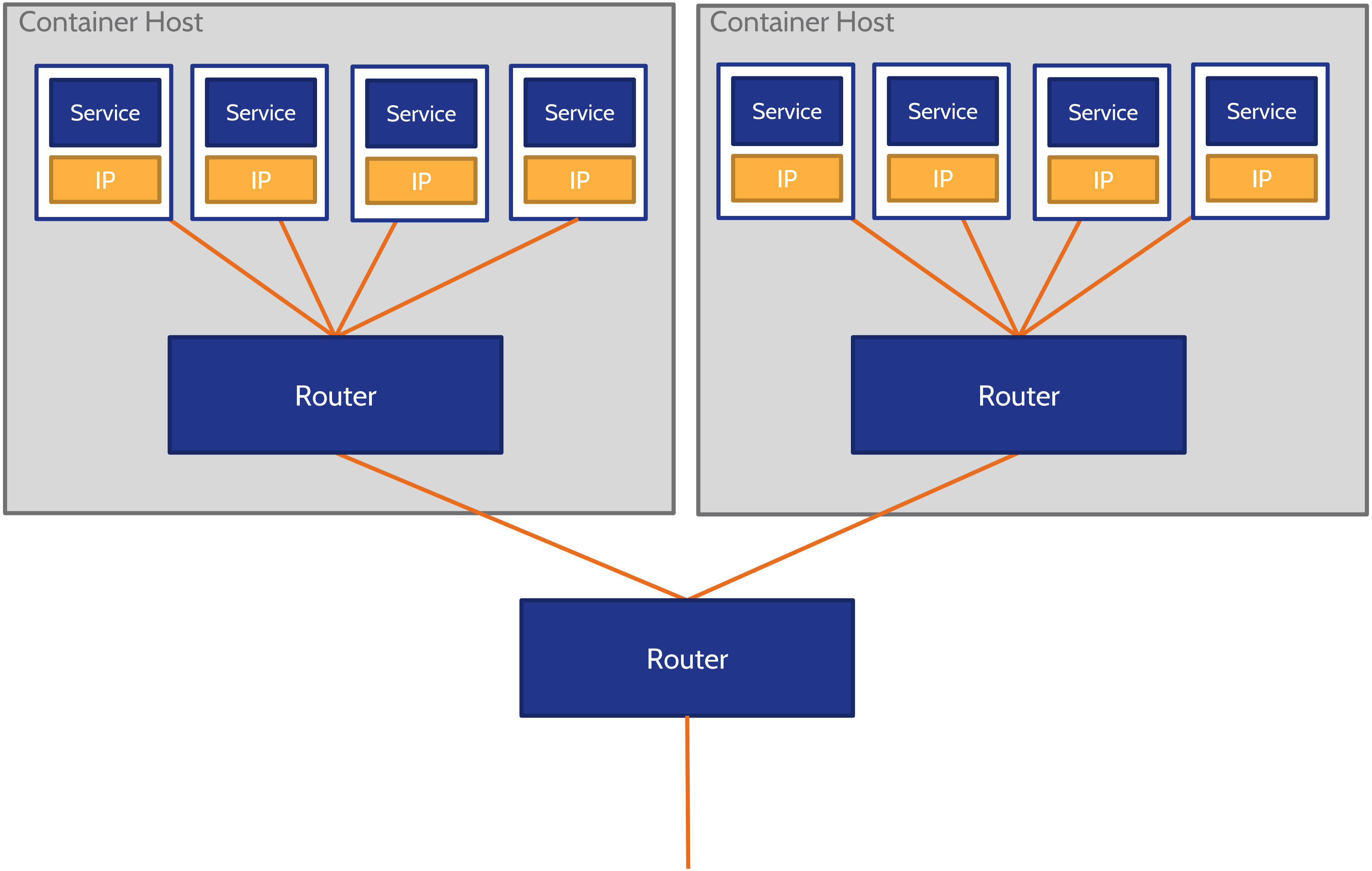
Calico


Orchestrator
Calico
CNI plugin
CALICO
Policy enforcement
BGP
IPIP
Native
etcd
Network Fabric

Conceptual View



Calico Conceptual View



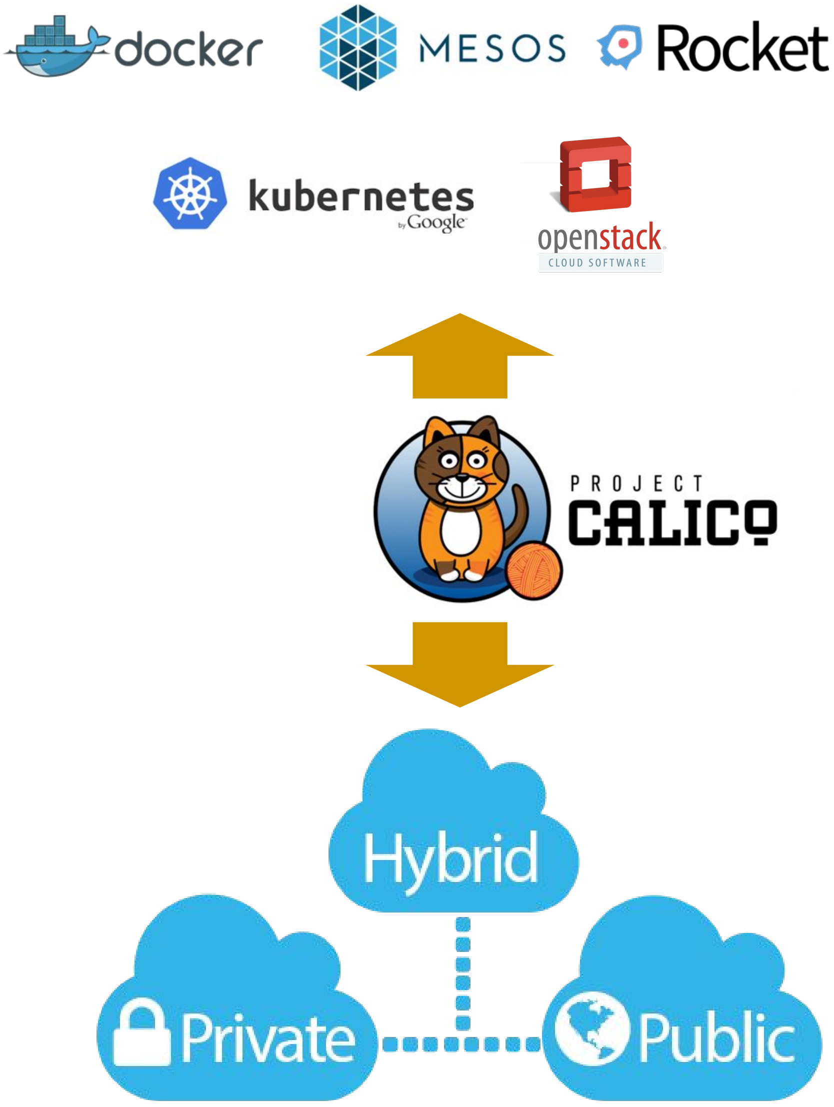
Calico

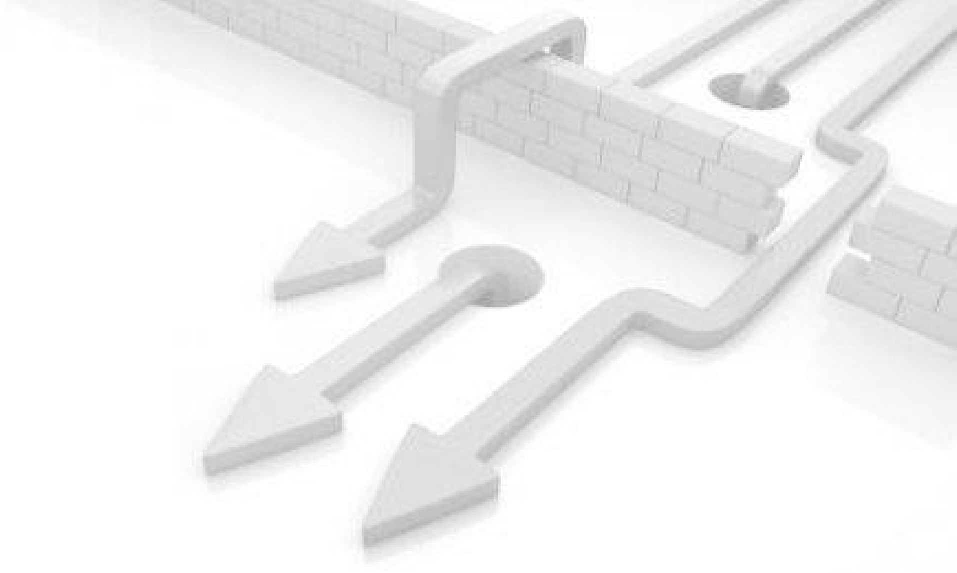
Route

- Get packets from A to B
- **Flat IP** or overlay/tunnel

Secure

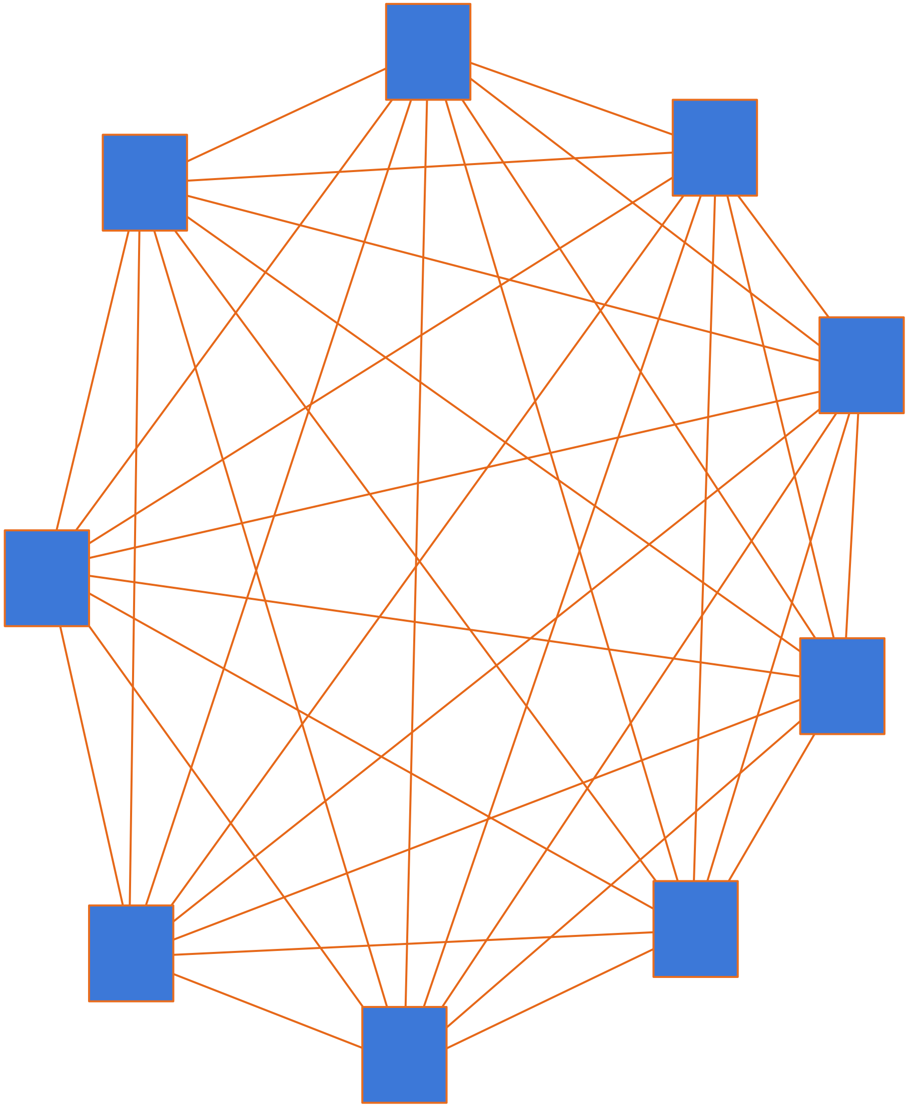
- Stop packets getting from A to B (that shouldn't, based on developer and operator intent)
- Capture suspicious flows



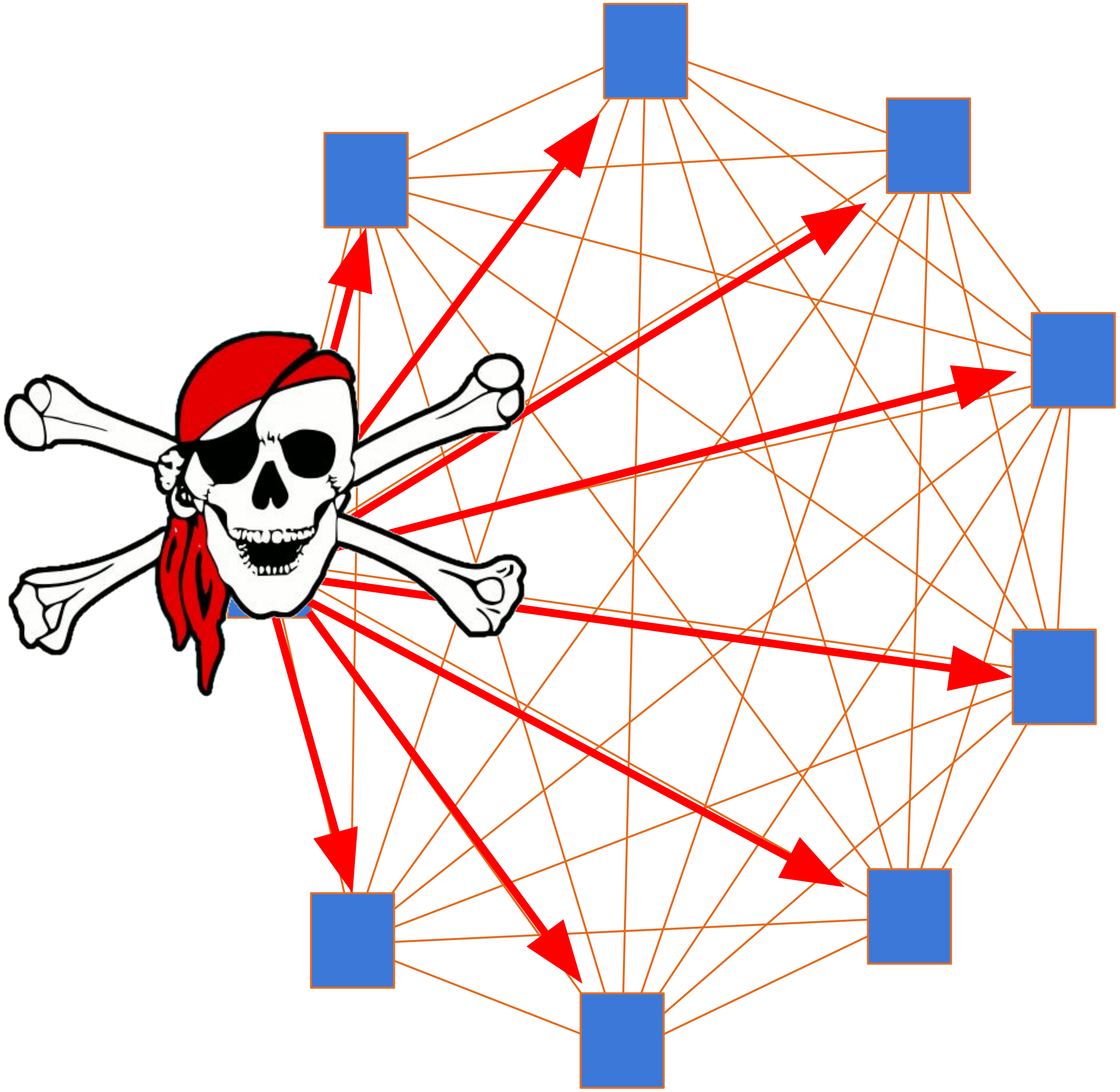


Security and Policy

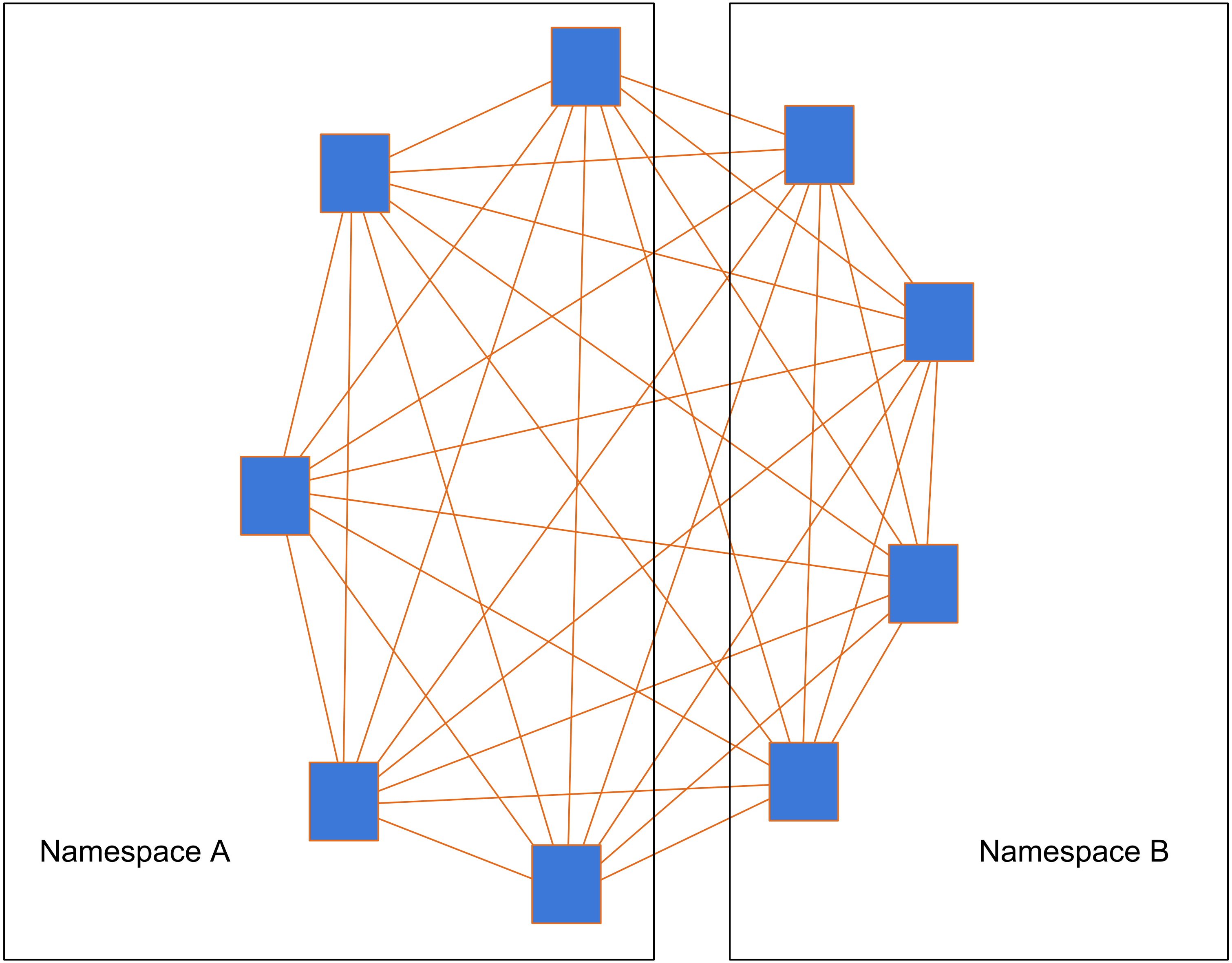
Open By Default



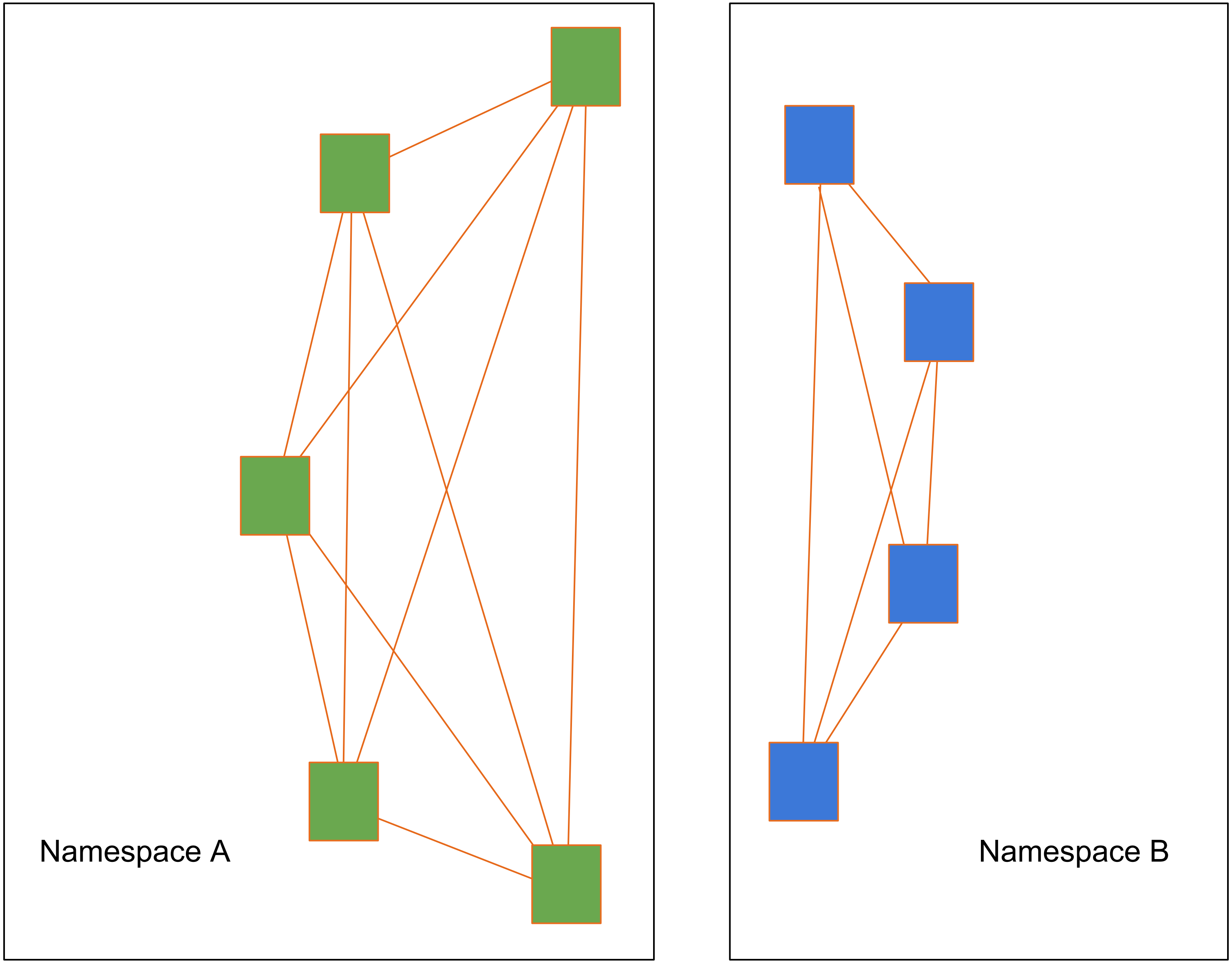
Issue With Default Open



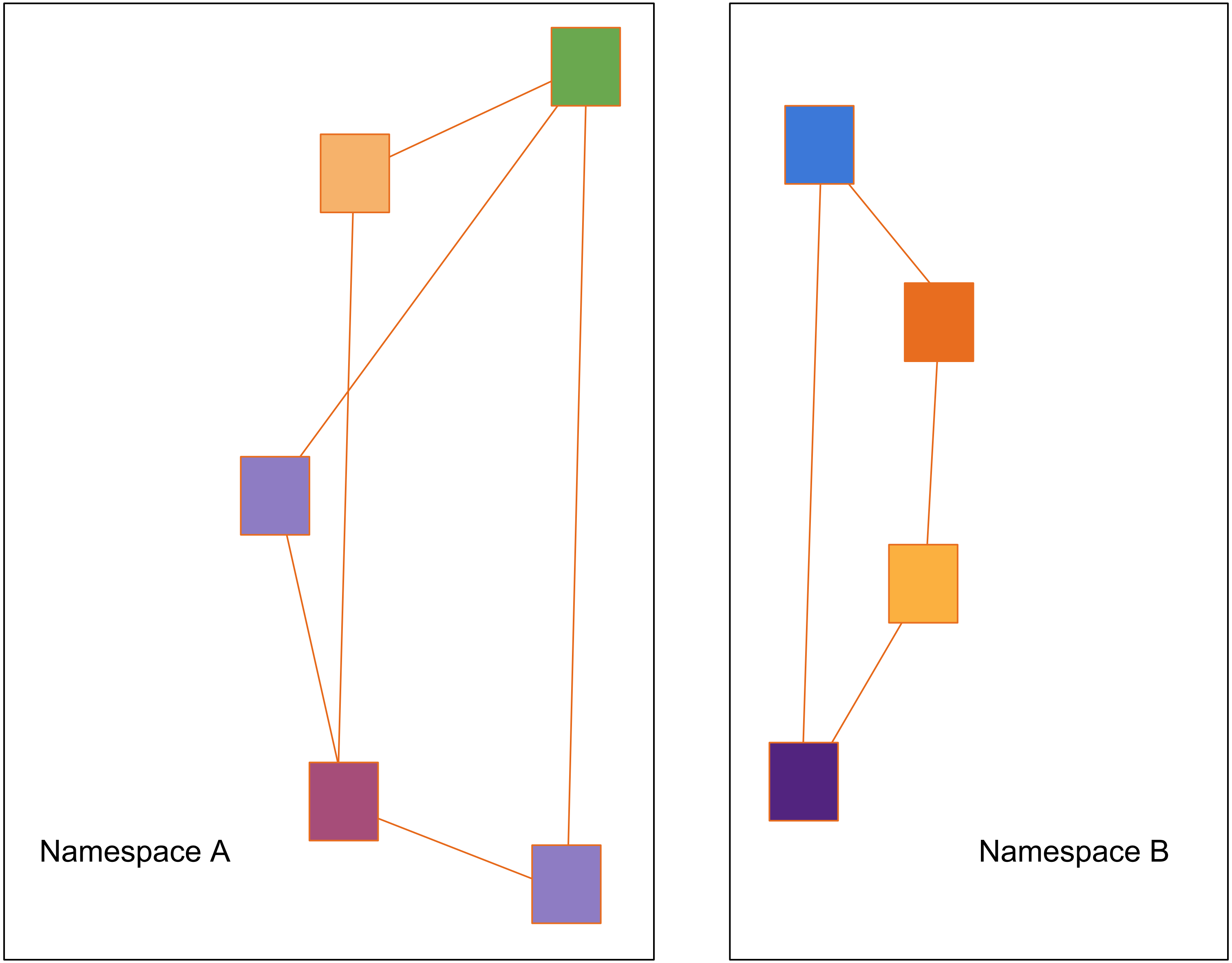
Namespaces



Namespaces With Default Open



Namespaces With Labels and Policy



~DEMO~

Demo example: nginx policy

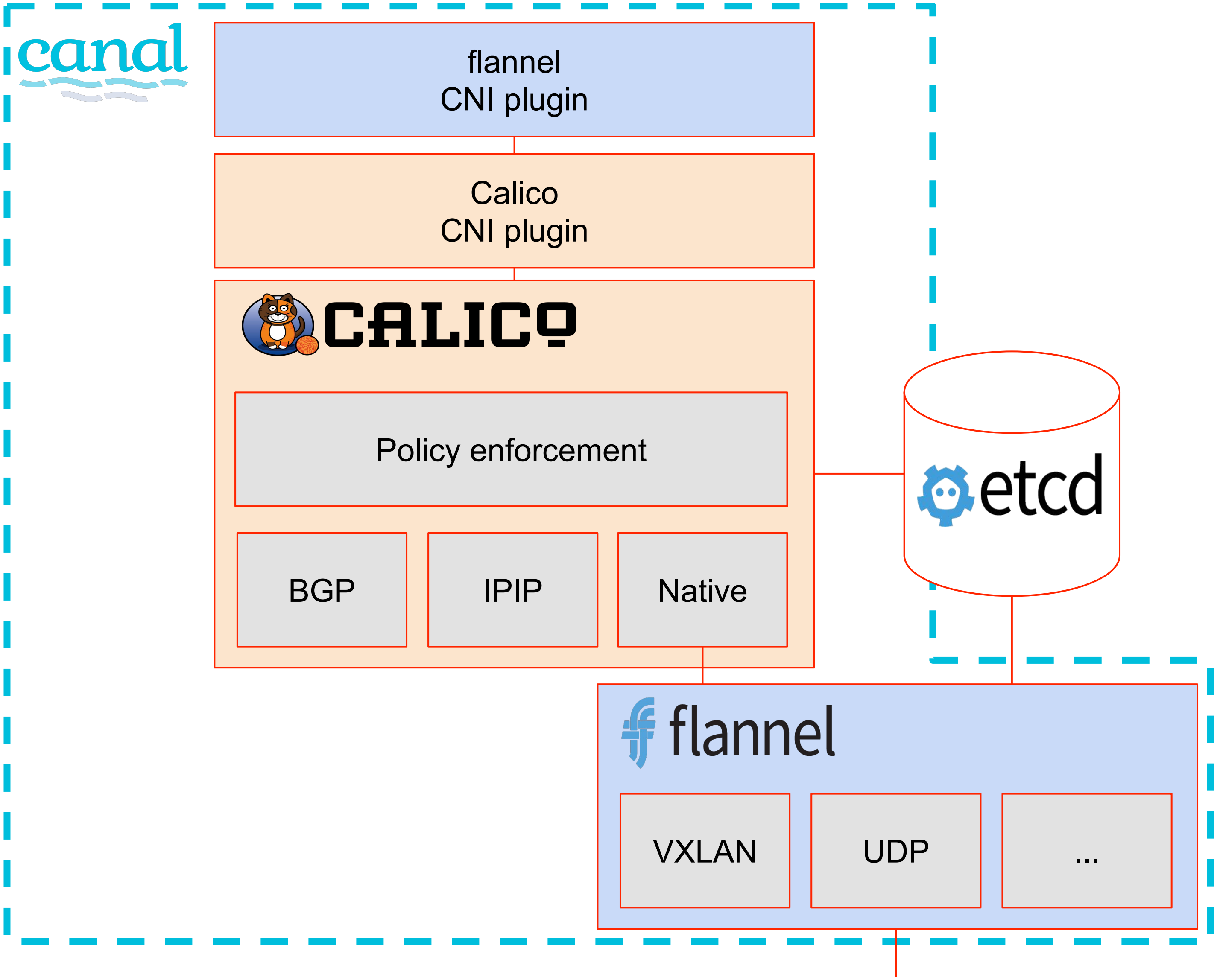
```
kind: NetworkPolicy
apiVersion: extensions/v1beta1
metadata:
  name: access-nginx
  namespace: policy-demo
spec:
  podSelector:
    matchLabels:
      run: nginx
  ingress:
    - from:
      - podSelector:
          matchLabels:
            run: access
```

Metadata

Rich selector for pods to apply to

Fine-grained rules

Canal: Calico Policy Enforcement with Flannel Networking



Looking Forward

Future Plans & Ongoing Initiatives

- Egress Policy & Filtering
- Tracing & Troubleshooting
- Federation
- Service Routing / Cluster-IP’s
- Policy API’s for Docker & Mesos
- Application Authentication

TiGERA

CLOUD NETWORKS, SECURED

We’re Hiring!

PROJECT CALICO

http://www.projectcalico.org/

github.com/projectcalico

@projectcalico

slack.projectcalico.org