Kubernetes Networking
Calico IPIP + Kubeproxy (iptables)

Jeff Barnes
GC Micro-mission

Calico for Kubernetes

Calico enables networking and network policy in Kubernetes clusters across the cloud. Calico works everywhere - on all major public cloud providers and private cloud as well.

Calico uses a pure IP networking fabric to provide high performance networking, and its battle-tested policy engine enforces high-level, intent-focused network policy. Together, Calico and Kubernetes provide a secure, cloud-native platform that can scale your infrastructure to hundreds of thousands of workloads.

https://docs.projectcalico.org/v2.0/getting-started/kubernetes/

https://github.com/projectcalico/calico

https://www.projectcalico.org/

TIGERA

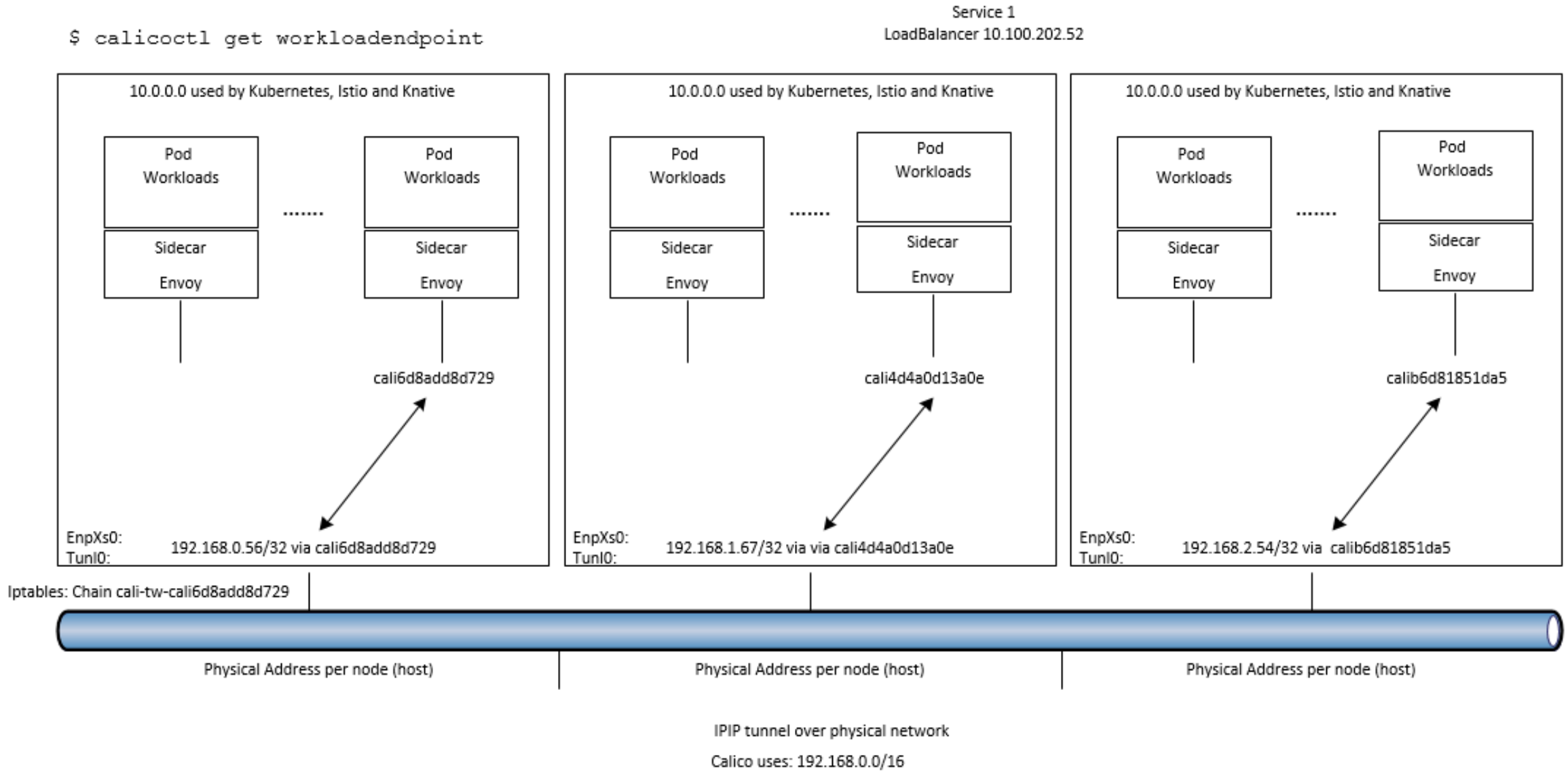
Calico for Kubernetes

Example Network Policies

```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  name: prevent-egress
  namespace: default
spec:
  podSelector:
    # Match all pods in this ns
    matchLabels: {}
  egress:
    # Allow egress only to dev
    - to:
      - namespaceSelector:
          matchLabels:
            role: dev
```

```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  name: prevent-egress
  namespace: default
spec:
  podSelector:
    # Match all pods in this ns
    matchLabels: {}
  egress:
    # Allow only to a specific network
    - to:
      - ipBlock:
          cidr: 10.0.0.0/8
  ingress:
    # Allow only from a specific network
    - from:
      - ipBlock:
          Cidr: 10.0.0.0/8
```

Calico for Kubernetes



Calicoctl

```
$ calicoctl get workloadendpoint
WORKLOAD                            NODE      NETWORKS           INTERFACE
details-v1-68c7c8666d-x57tf         ubuntu2   192.168.1.62/32    cali8c5ecab8e58
main-699dd9dc98-6fz62               ubuntu3   192.168.2.54/32    calib6d81851da5
main-699dd9dc98-nlxss               ubuntu2   192.168.1.67/32    cali4d4a0d13a0e
main-699dd9dc98-vb9c5               ubuntu1   192.168.0.56/32    cali6d8add8d729
productpage-v1-54d799c966-h96dv     ubuntu3   192.168.2.63/32    calic30c889d0d0
ratings-v1-8558d4458d-86mtm         ubuntu3   192.168.2.55/32    cali21230f2dafe
reviews-v1-cb8655c75-9tz9q          ubuntu1   192.168.0.52/32    calida284fa5314
reviews-v2-7fc9bb6dcf-45d6z         ubuntu2   192.168.1.66/32    calie03b469bdcb
reviews-v3-c995979bc-78g8r          ubuntu3   192.168.2.58/32    cali3ce30d54769

$ calicoctl node status
Calico process is running.

IPv4 BGP status
+---------------+-------------------+-------+------------+-------------+
|  PEER ADDRESS  |     PEER TYPE     | STATE |   SINCE    |    INFO     |
+---------------+-------------------+-------+------------+-------------+
| V.W.X.Y        | node-to-node mesh | up    | 2019-01-10 | Established |
| V.W.X.Z        | node-to-node mesh | up    | 2019-01-10 | Established |
+---------------+-------------------+-------+------------+-------------+
```

```
$ iptables --list-rules |grep KUBE | more
-N KUBE-EXTERNAL-SERVICES
-N KUBE-FIREWALL
-N KUBE-FORWARD
-N KUBE-SERVICES
-A INPUT -m conntrack --ctstate NEW -m comment --comment "kubernetes externally-visible service portals" -j KUBE-EXTERNAL-SERVI
CES
-A INPUT -j KUBE-FIREWALL
-A FORWARD -m comment --comment "kubernetes forwarding rules" -j KUBE-FORWARD
-A OUTPUT -m conntrack --ctstate NEW -m comment --comment "kubernetes service portals" -j KUBE-SERVICES
-A OUTPUT -j KUBE-FIREWALL
-A KUBE-FIREWALL -m comment --comment "kubernetes firewall for dropping marked packets" -m mark --mark 0x8000/0x8000 -j DROP
-A KUBE-FORWARD -m comment --comment "kubernetes forwarding rules" -m mark --mark 0x4000/0x4000 -j ACCEPT
-A KUBE-FORWARD -s 192.168.0.0/16 -m comment --comment "kubernetes forwarding conntrack pod source rule" -m conntrack --ctstate
 RELATED,ESTABLISHED -j ACCEPT
-A KUBE-FORWARD -d 192.168.0.0/16 -m comment --comment "kubernetes forwarding conntrack pod destination rule" -m conntrack --ct
state RELATED,ESTABLISHED -j ACCEPT
-A KUBE-SERVICES -d 10.101.168.10/32 -p tcp -m comment --comment "knative-monitoring/fluentd-ds:fluentd-tcp has no endpoints" -
m tcp --dport 24224 -j REJECT --reject-with icmp-port-unreachable
-A KUBE-SERVICES -d 10.101.168.10/32 -p udp -m comment --comment "knative-monitoring/fluentd-ds:fluentd-udp has no endpoints" -
m udp --dport 24224 -j REJECT --reject-with icmp-port-unreachable
-A KUBE-SERVICES -d 10.102.7.108/32 -p tcp -m comment --comment "default/helloworld-go-00001-service:metrics has no endpoints"
-m tcp --dport 9090 -j REJECT --reject-with icmp-port-unreachable
-A KUBE-SERVICES -d 10.102.215.106/32 -p tcp -m comment --comment "kube-system/calico-typha:calico-typha has no endpoints" -m t
cp --dport 5473 -j REJECT --reject-with icmp-port-unreachable
-A KUBE-SERVICES -d 10.102.7.108/32 -p tcp -m comment --comment "default/helloworld-go-00001-service:http has no endpoints" -m
tcp --dport 80 -j REJECT --reject-with icmp-port-unreachable
```

```
iptables --list-rules
iptables –list
crictl ps |more
crictl images |more
```