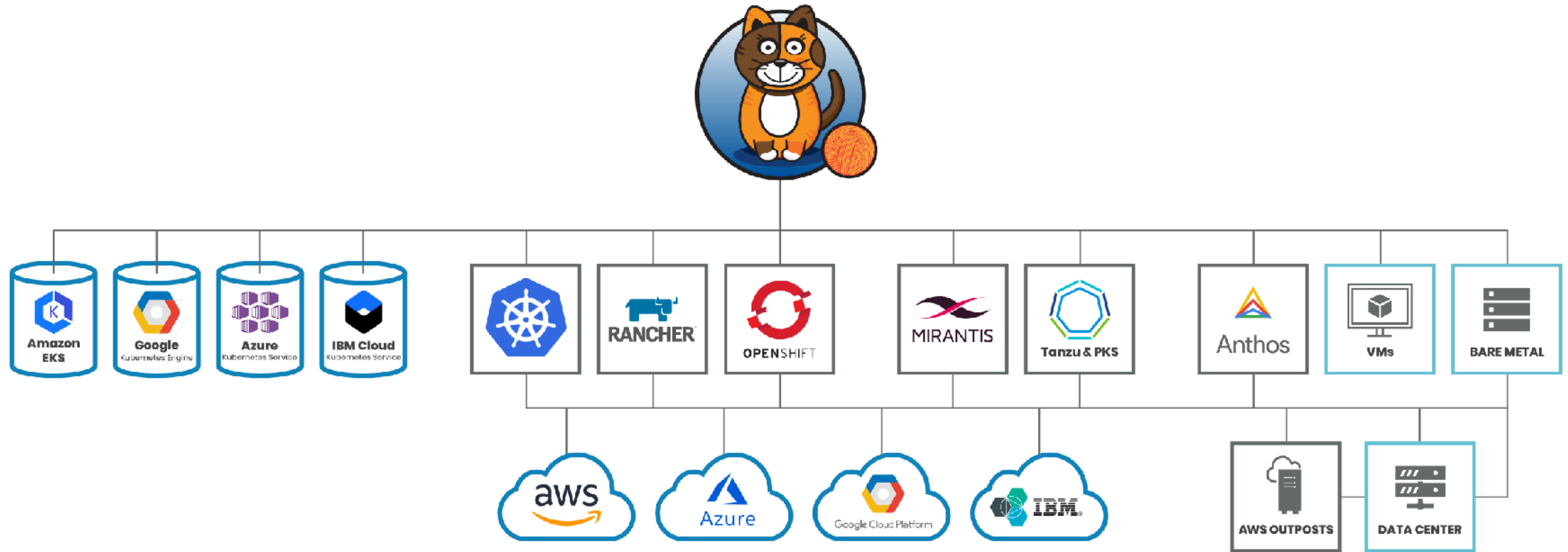


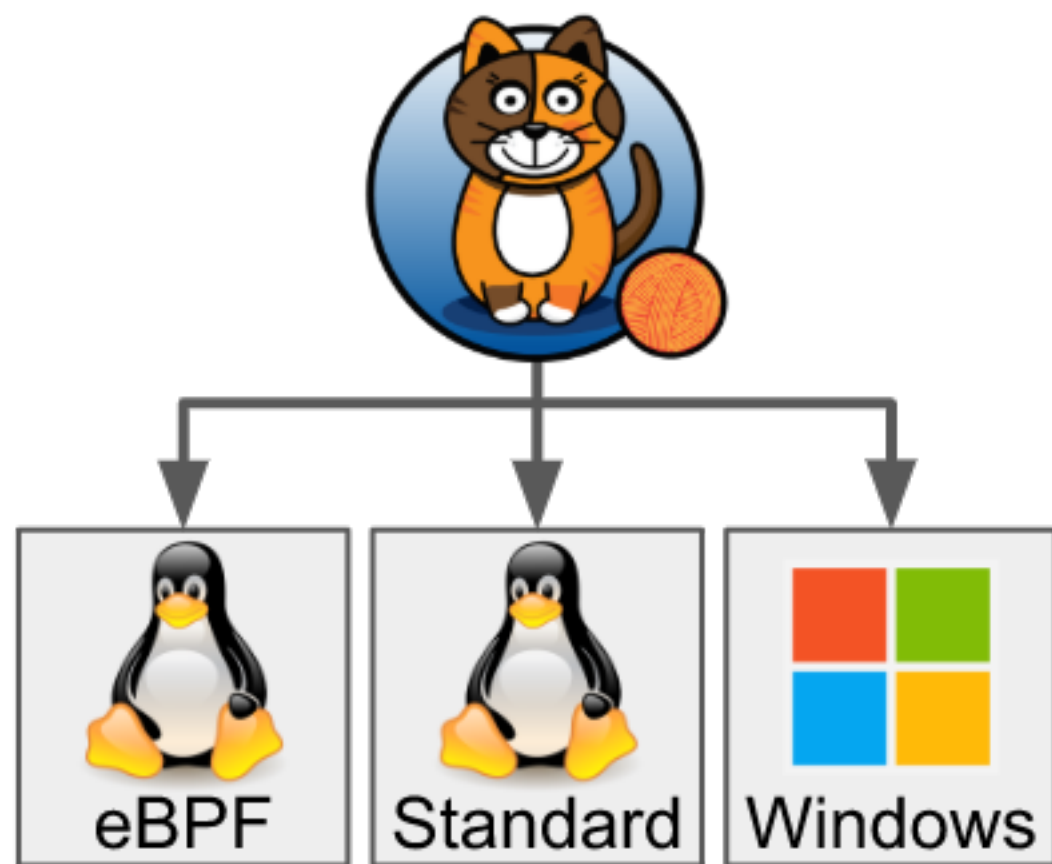
Calico изнутри

Архитектура и возможности

Александров Андрей

Industry Standard for Kubernetes Network Security

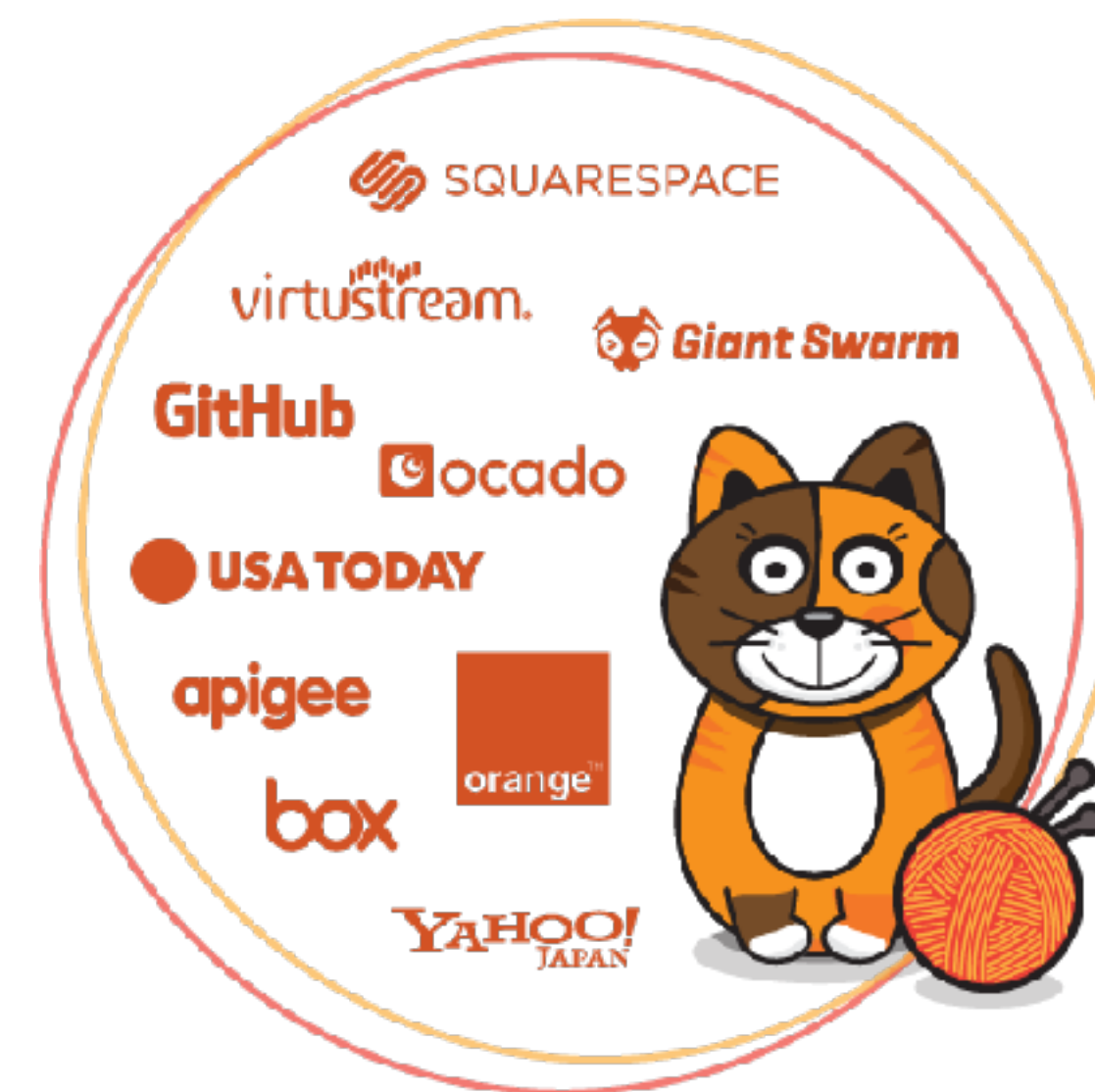




Best Practices

- ✓ Adopt zero trust network security model
- ✓ Infrastructure as code

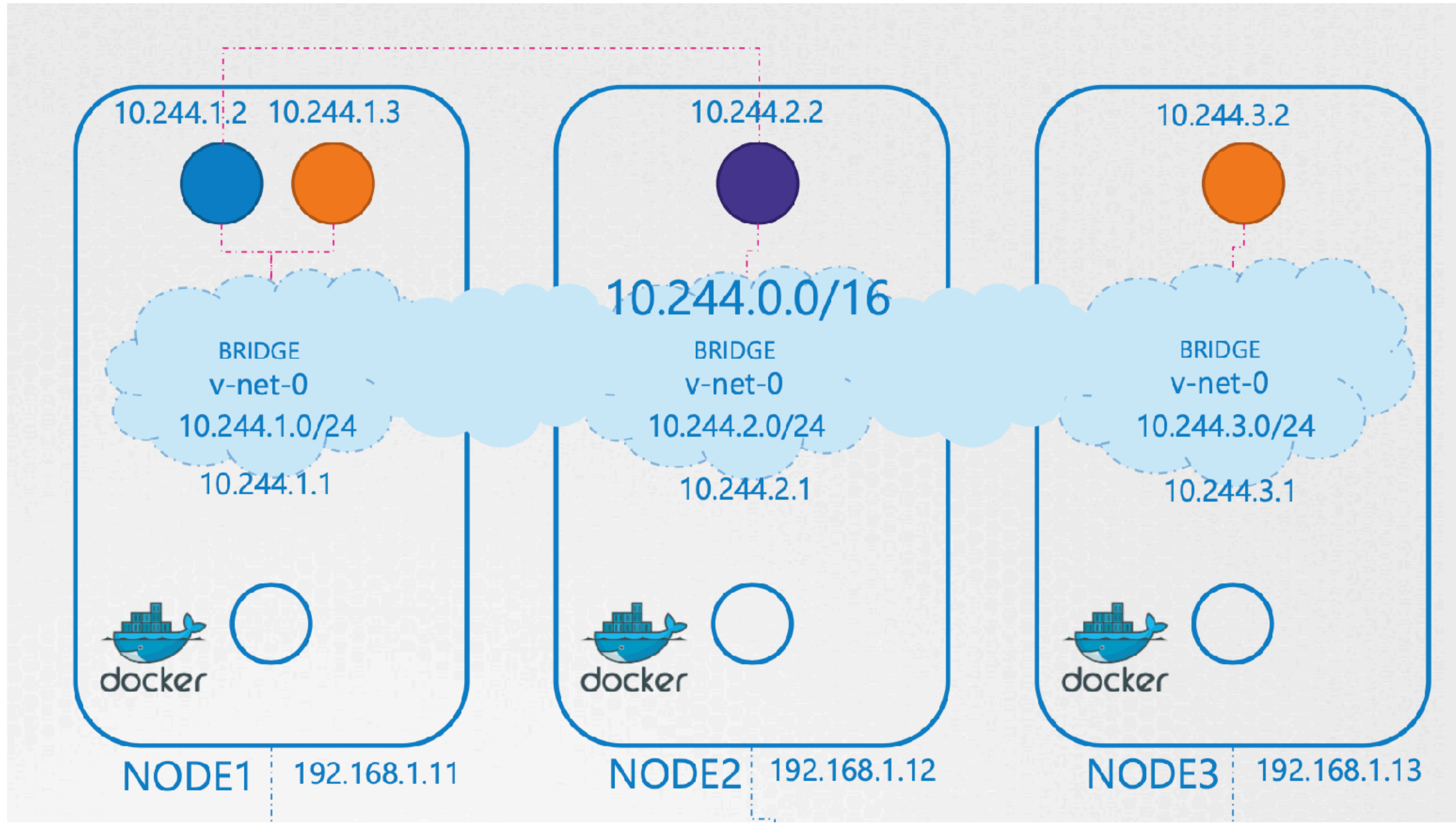
A presentation slide titled 'Best Practices' with two bullet points, each preceded by a checkmark. To the right, a cat icon is shown holding a pen, standing next to a blue box featuring a white cat silhouette.



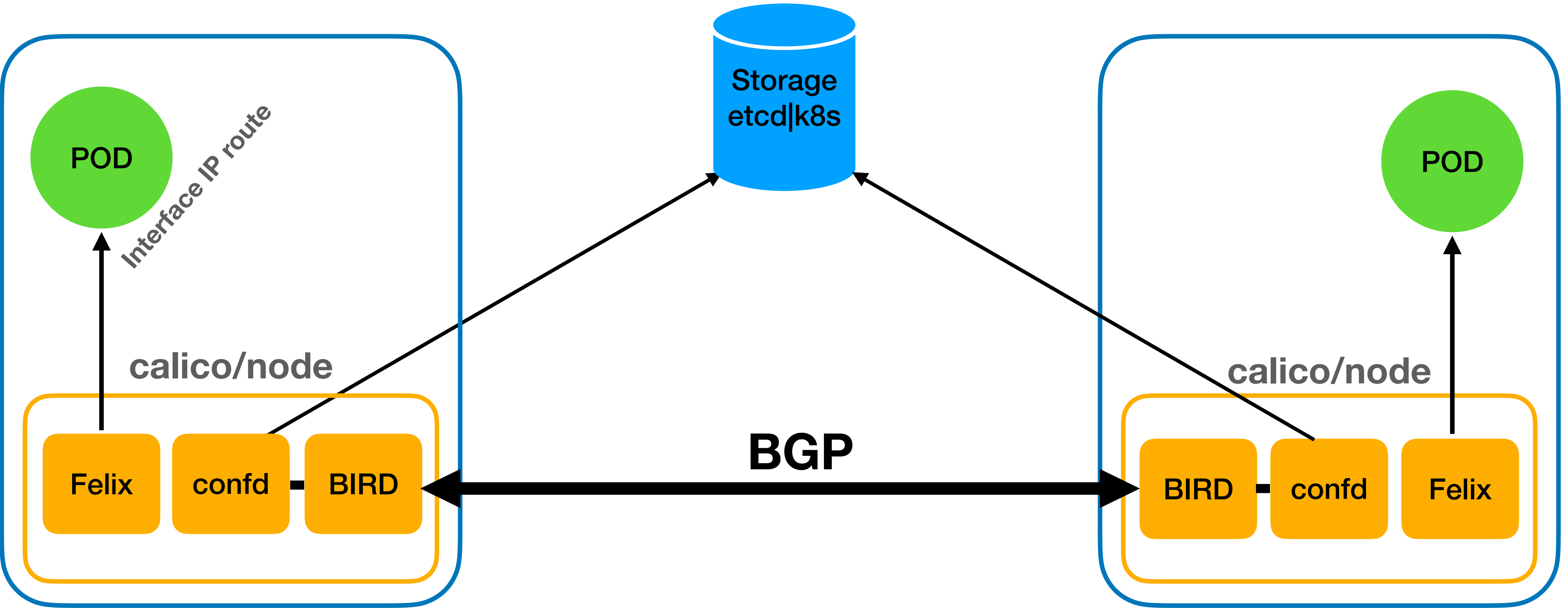
Kubernetes Network Model

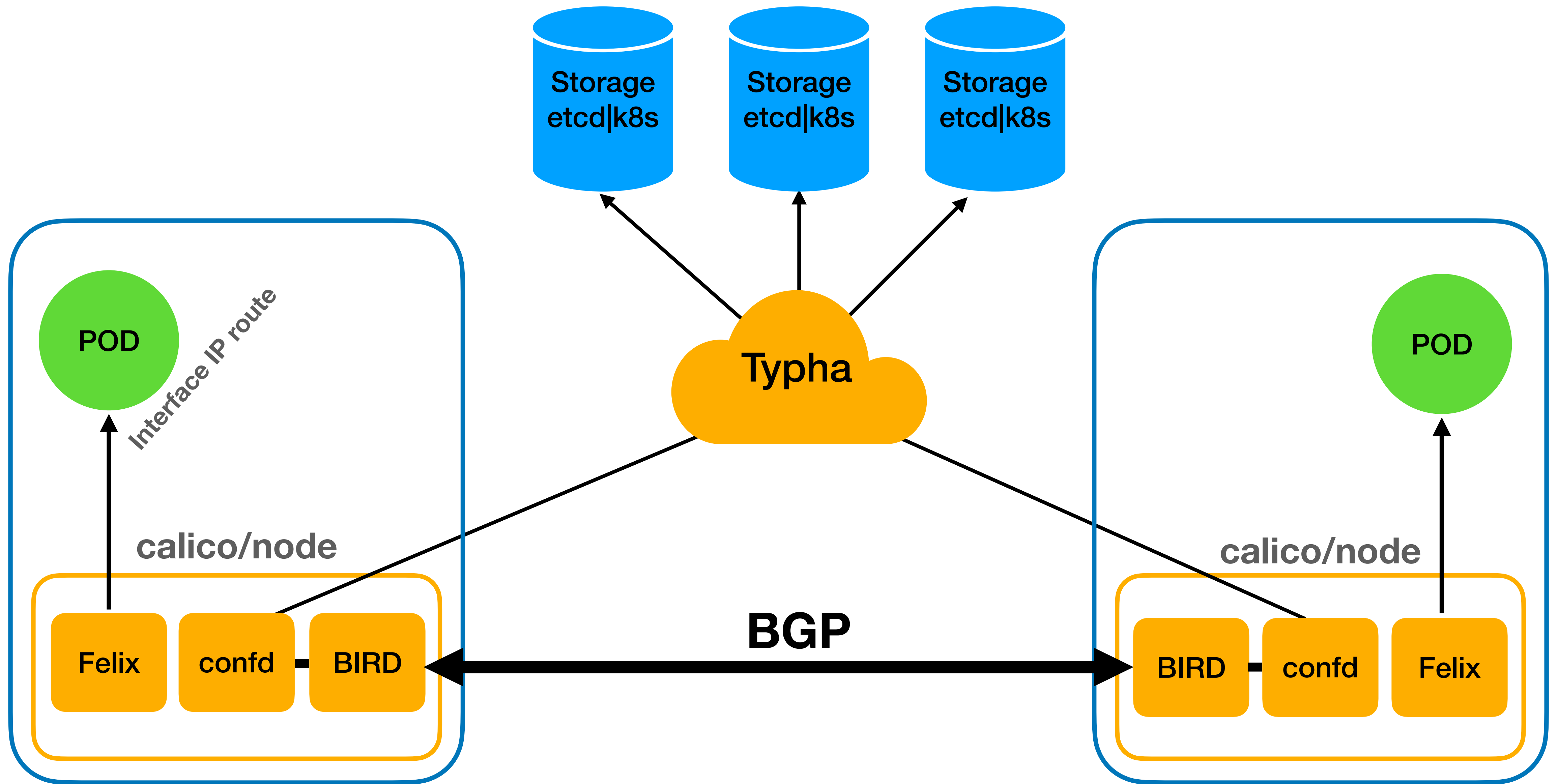
- Every pod gets its own IP address
- Containers within a pod share the pod IP address and can communicate freely with each other
- Pods can communicate with all other pods in the cluster using pod IP addresses (without [NAT](#))

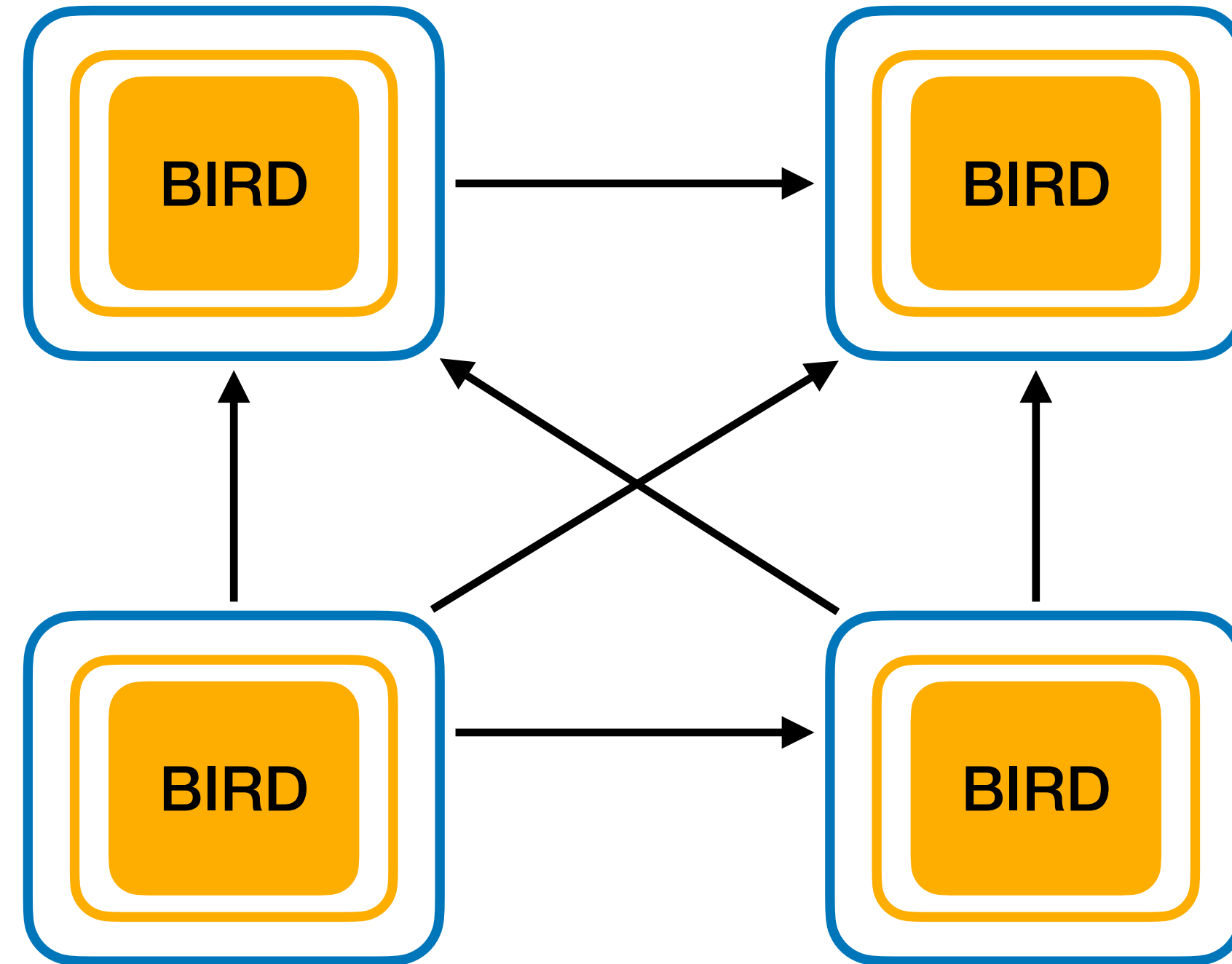
Kubernetes Network Model

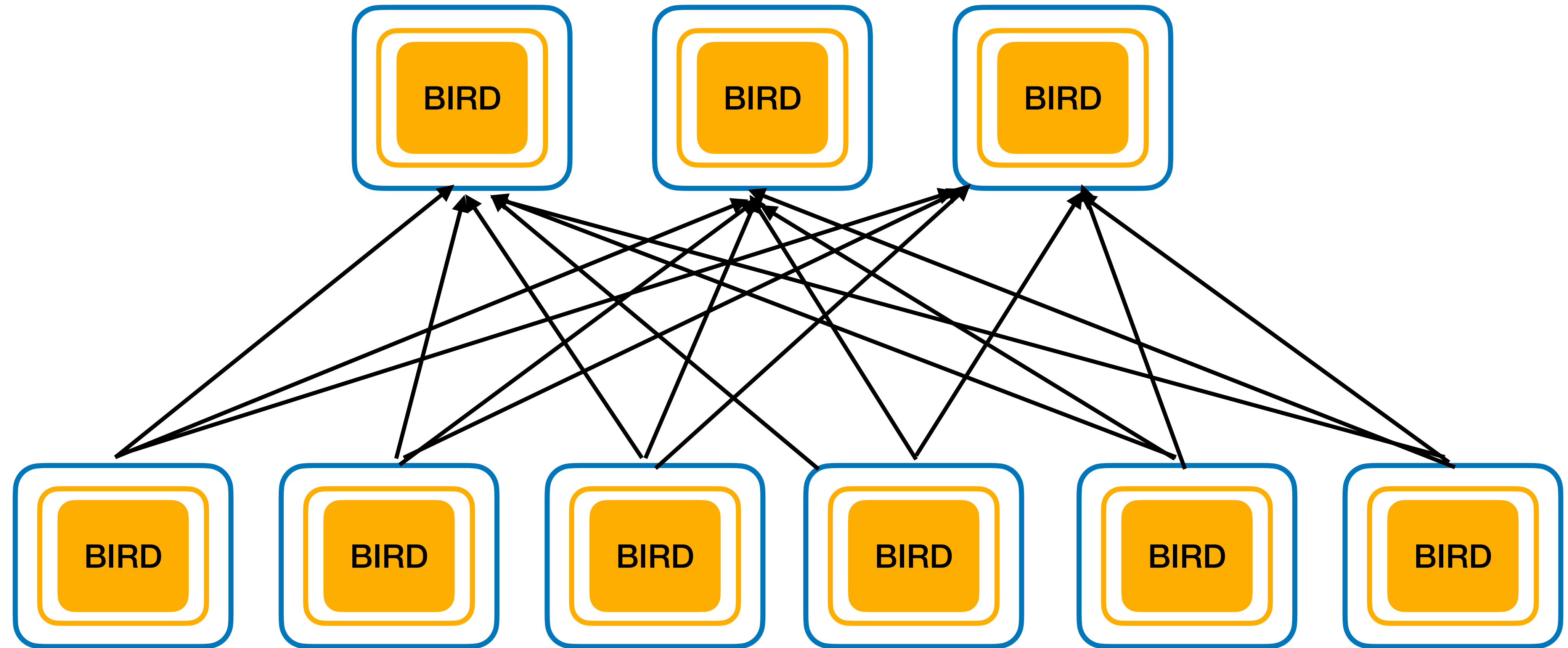


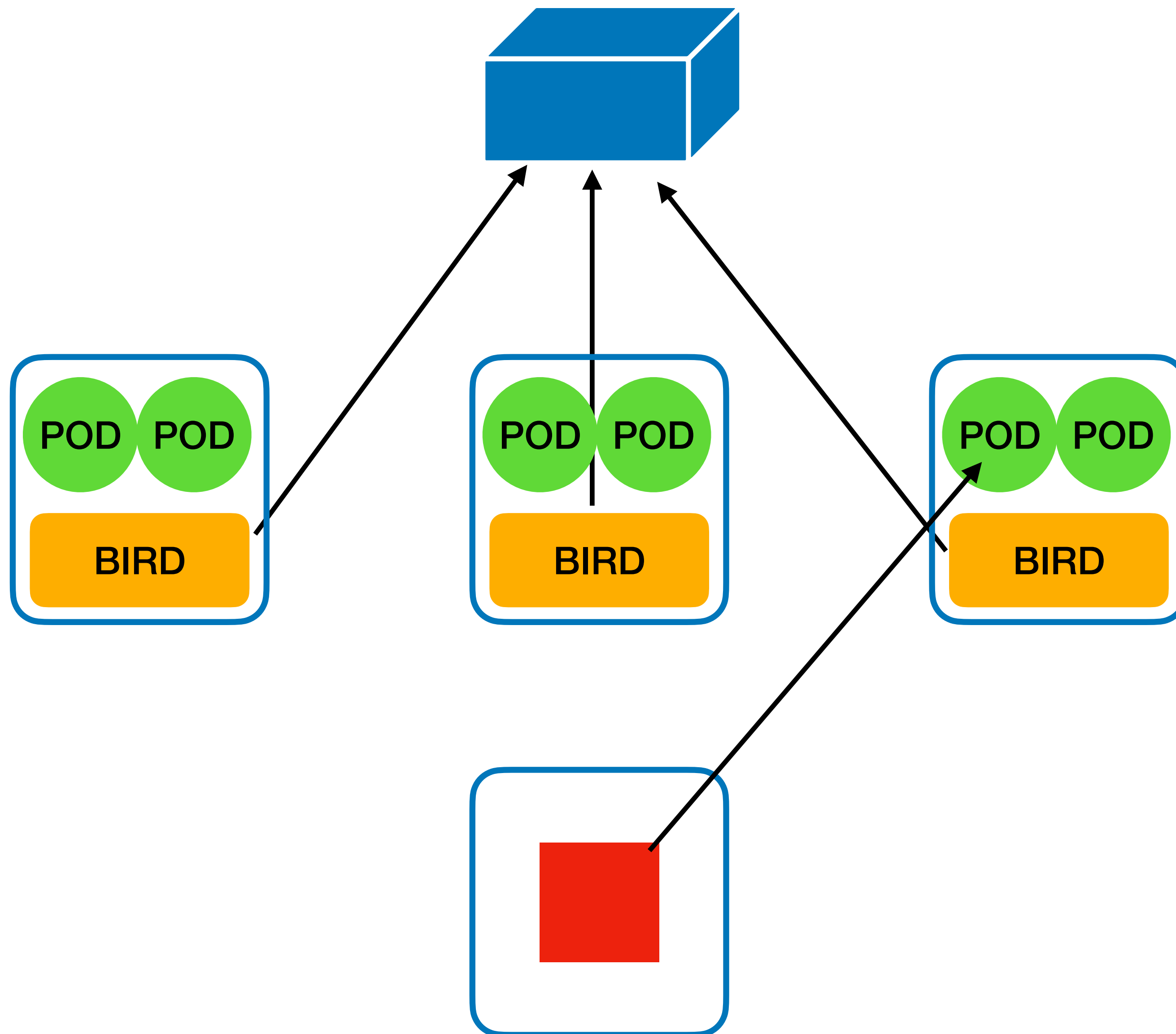
Calico Architecture



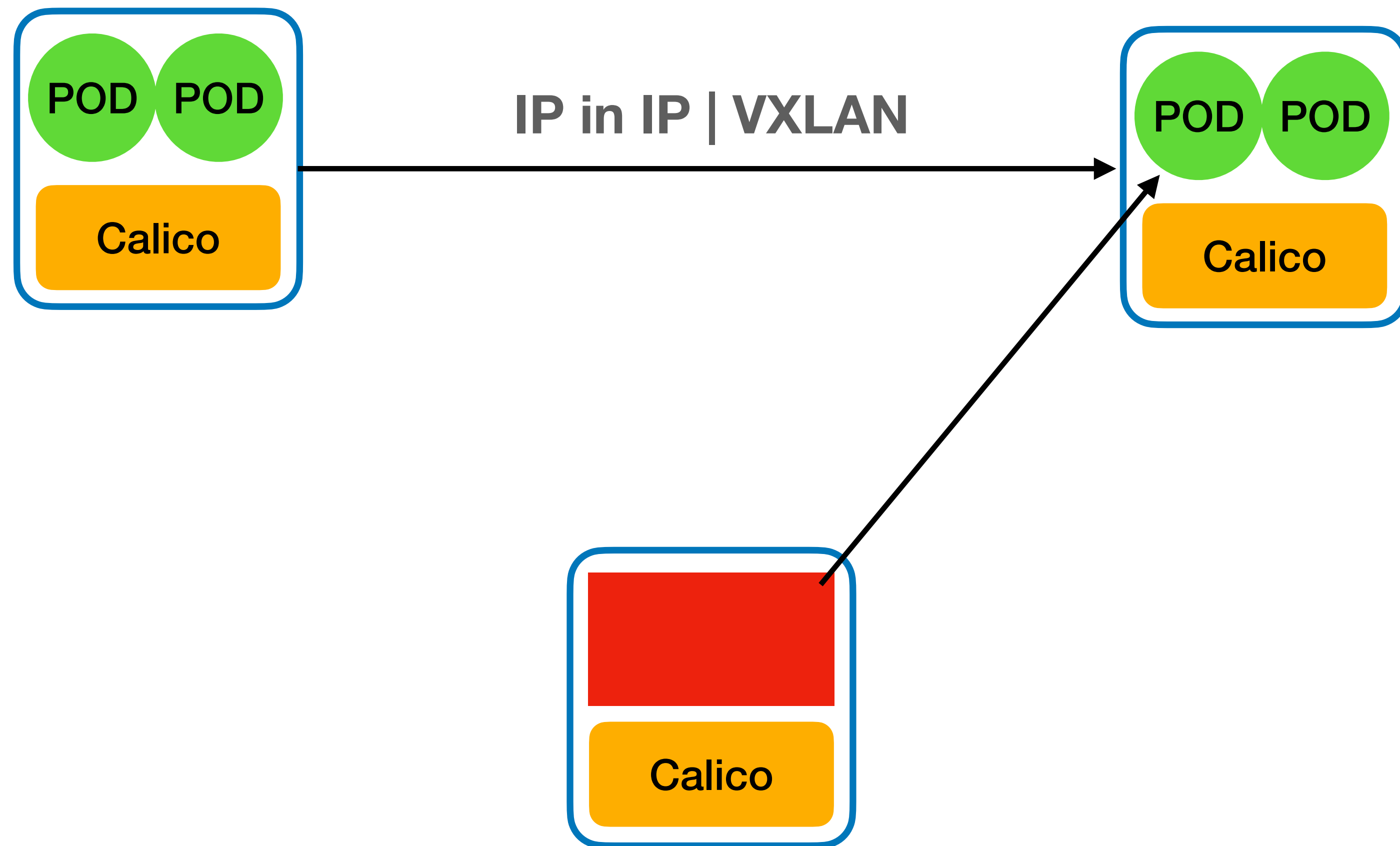








Overlay Network



Если все открыто, мы в опасности!

- k8s API / etcd
- Попад в один контейнер, атакуют все остальные
- Скомпрометировав один хост, атакуем все что хотим

Zero Trust Network Model

- Все соединения подчиняются политикам
- Все ожидаемые соединения явно разрешены
- Скомпрометированные хосты не могут обойти примененные политики
- Идентификация эндпоинта устанавливается по IP/port и криптографии(SSL)
- Шифрование трафика

Calicoctl

\$ calicoctl node status

Calico process is running.

IPv4 BGP status

+-----+-----+-----+-----+-----+					
PEER ADDRESS	PEER TYPE	STATE	SINCE	INFO	
+-----+-----+-----+-----+-----+					
10.234.3.104	node-to-node mesh	up	2020-08-27	Established	
10.234.3.103	node-to-node mesh	up	2020-08-27	Established	
10.234.2.228	node-to-node mesh	up	2020-08-27	Established	
+-----+-----+-----+-----+-----+					

\$ calicoctl apply -f file.yml

\$ calicoctl get --help

- * bgpConfiguration
- * bgpPeer
- * felixConfiguration
- * globalNetworkPolicy
- * globalNetworkSet
- * hostEndpoint
- * ipPool
- * kubeControllersConfiguration
- * networkPolicy
- * networkSet
- * node
- * profile
- * workloadEndpoint

Network Policy

- Применяются к любым эндпоинтам: pods/containers, VMs, and/or to host interfaces
- Контролирует входящий/исходящий трафик
- Работает по критериям:
 - port, port-range
 - HTTP-attributes(istio)
 - IP/CIDR
 - **selector!**
 - **namespace!**
 - **serviceaccount!**

Allow Ingress in Production from a pod with labels

```
apiVersion: projectcalico.org/v3
kind: NetworkPolicy
metadata:
  name: allow-tcp-6379
  namespace: production
spec:
  selector: type == 'db'
  ingress:
  - action: Allow
    protocol: TCP
    source:
      selector: type == 'app'
    destination:
      ports:
      - 6379
```

Allow Ingress in Production from another NS

```
apiVersion: projectcalico.org/v3
kind: NetworkPolicy
metadata:
  name: allow-tcp-6379
  namespace: production
spec:
  selector: type == 'db'
  ingress:
    - action: Allow
      protocol: TCP
      source:
        selector: type == 'app'
        namespaceSelector: services == 'backend'
  destination:
    ports:
      - 6379
```

Host endpoint

```
- apiVersion: projectcalico.org/v3
  kind: HostEndpoint
  metadata:
    name: <name of endpoint>
    labels:
      role: webserver
      environment: production
  spec:
    interfaceName: eth0
    node: <node name or hostname>
    profiles: [<list of profile IDs>]
    expectedIPs: ["10.0.0.1"]
```


Host endpoint

```
apiVersion: projectcalico.org/v3
kind: GlobalNetworkPolicy
metadata:
  name: k8s-worker
spec:
  selector: "role == 'k8s-worker'"
  order: 0
  ingress:
  - action: Allow
    protocol: TCP
    source:
      nets:
      - "<your management CIDR>"
    destination:
      ports: [22, 10250]
```

```
egress:
  - action: Allow
    protocol: TCP
    destination:
      nets:
      - "<your etcd IP>/32"
      ports: [2379]
  - action: Allow
    protocol: UDP
    destination:
      ports: [53, 67]
```

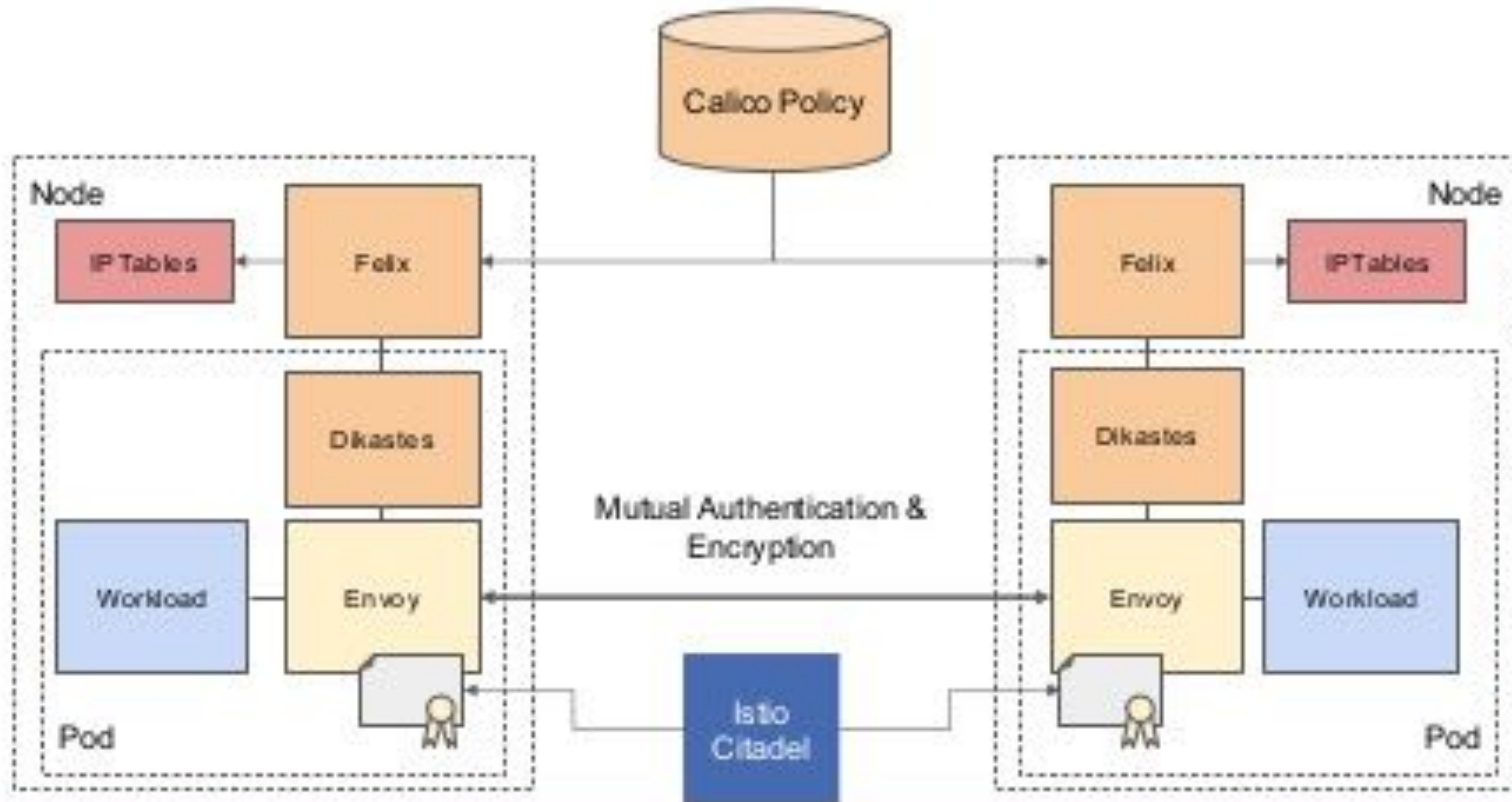
Защита от дурака!

22	TCP	Inbound	SSH access
53	UDP	Outbound	DNS queries
67	UDP	Outbound	DHCP access
68	UDP	Inbound	DHCP access
179	TCP	Inbound & Outbound	BGP access (Calico networking)
2379	TCP	Inbound & Outbound	etcd access
2380	TCP	Inbound & Outbound	etcd access
6443	TCP	Inbound & Outbound	Kubernetes API server access
6666	TCP	Inbound & Outbound	etcd self-hosted service access
6667	TCP	Inbound & Outbound	etcd self-hosted service access

Но защиту можно ОТКЛЮЧИТЬ :)

```
apiVersion: projectcalico.org/v3
kind: FelixConfiguration
metadata:
  name: default
spec:
  ipv6Support: false
  ipipMTU: 1400
  failsafeInboundHostPorts:
    -
    -
  failsafeOutboundHostPorts:
    -
    -
```

Zero Trust Network Model



Zero Trust Network Model



```
$ calicoctl patch felixconfiguration default  
  --type='merge' -p '{"spec":  
    {"wireguardEnabled":true}}'
```

...

status:

..

wireguardPublicKey: jlkVyQYooZYzI2wFfNhSZez5e

...



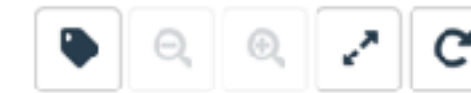
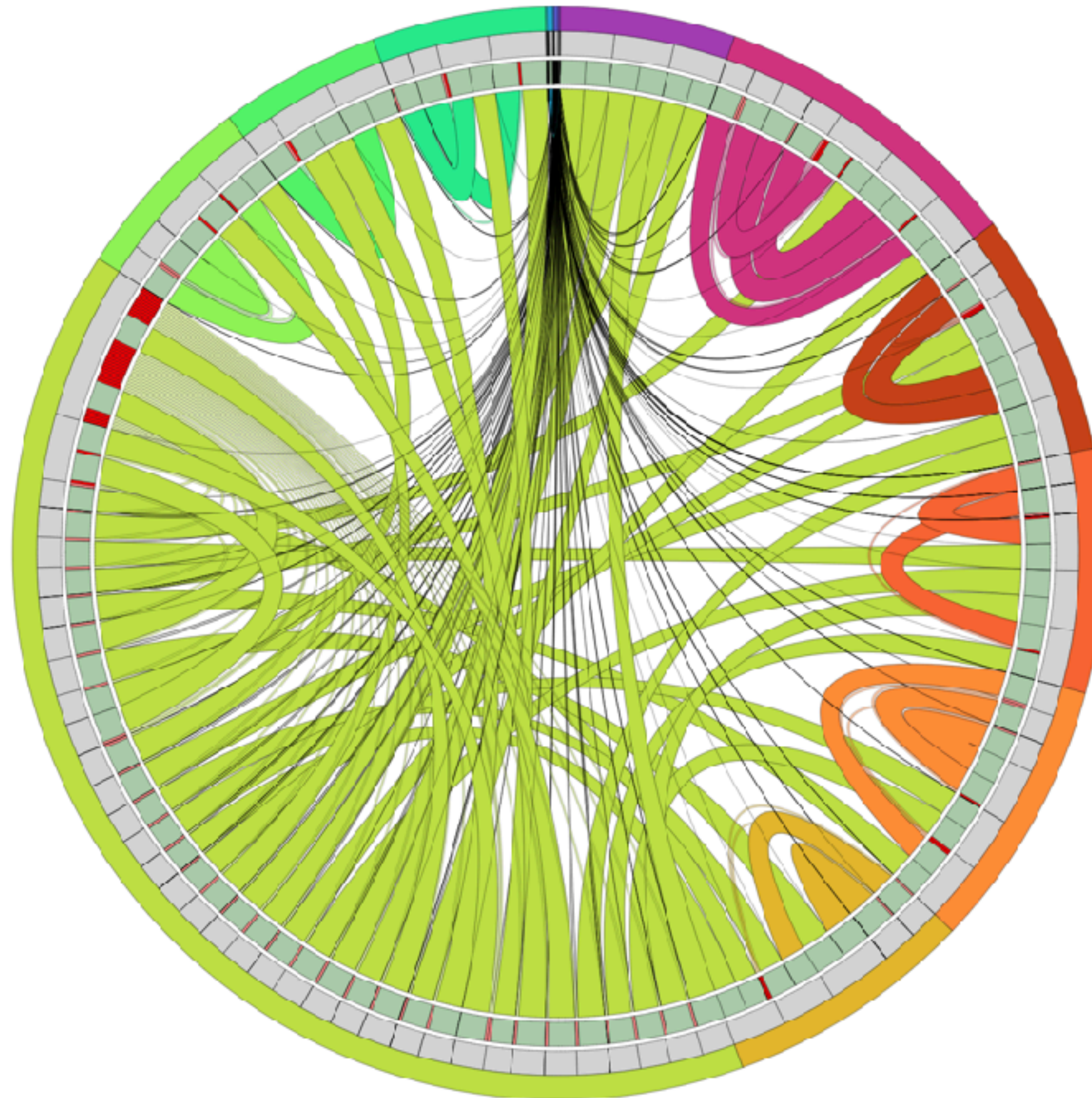
CALICO

ENTERPRISE

- Hierarchical network policy
- Egress access controls (DNS policies, egress gateways)
- Network visualization and troubleshooting
- Network policy recommendations
- Network policy preview and staging
- Compliance controls and reporting
- Intrusion detection (suspicious activity, anomaly detection)
- Multi-cluster management with multi-cloud federation

Flow Visualizations

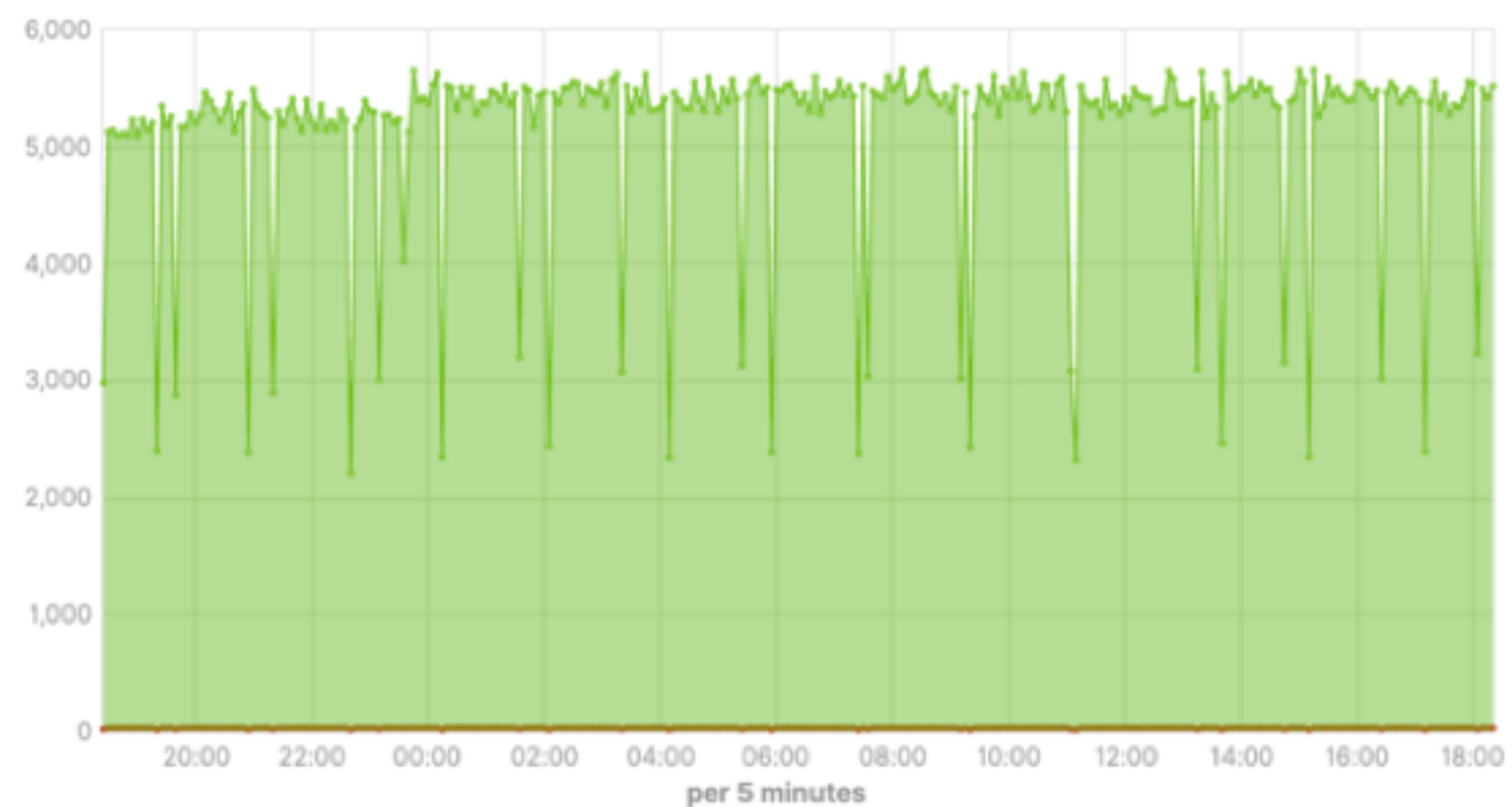
Filter: Source type: [net,ns,wep,hep], Destination type: [net,ns,wep,hep], Time range: [From: 15 minutes ago]



Namespaces	Names	Status	
Any status		×	
All Namespaces		×	
All Names		×	
All Flows		×	
Allowed Traffic	CPS	PPS	BPS
<div><div></div><div>-</div></div>	0.308	7.83	6.52k
<div><div></div><div>calico-monitoring</div></div>	0.308	4.47	1.67k
<div><div></div><div>istio-system</div></div>	0	0.080	4.15
<div><div></div><div>kube-system</div></div>	0	3.20	4.04k
<div><div></div><div>cali-ns-1</div></div>	281	2.98k	258k
<div><div></div><div>-</div></div>	0	0	0
<div><div></div><div>cali-ns-1</div></div>	281	2.97k	254k
<div><div></div><div>sto-system</div></div>	0	6.74	3.13k
<div><div></div><div>cali-ns-2</div></div>	134	1.42k	123k
<div><div></div><div>cali-ns-2</div></div>	134	1.42k	121k
<div><div></div><div>sto-system</div></div>	0	3.37	1.57k
<div><div></div><div>-</div></div>	0	0	0
<div><div></div><div>cali-ns-3</div></div>	133	1.41k	122k
<div><div></div><div>-</div></div>	0	0	0
<div><div></div><div>cali-ns-3</div></div>	133	1.41k	121k
<div><div></div><div>sto-system</div></div>	0	3.37	1.57k
<div><div></div><div>cali-ns-4</div></div>	200	2.11k	182k
<div><div></div><div>cali-ns-4</div></div>	200	2.10k	180k
<div><div></div><div>sto-system</div></div>	0	5.06	2.35k
<div><div></div><div>-</div></div>	0	0	0
<div><div></div><div>kube-system</div></div>	0	0	0
<div><div></div><div>cali-ns-5</div></div>	147	1.55k	134k
<div><div></div><div>-</div></div>	0	0	0
<div><div></div><div>cali-ns-5</div></div>	147	1.55k	133k
<div><div></div><div>sto-system</div></div>	0	3.30	1.50k
<div><div></div><div>cali-ns-6</div></div>	2.36k	24.9k	2.16M
<div><div></div><div>-</div></div>	0	0	0
<div><div></div><div>cali-ns-0</div></div>	413	4.35k	373k
<div><div></div><div>sto-system</div></div>	0	57.4	25.7k

**CALICO**
ENTERPRISE

Number of Flows



> ● Allowed flows 5,527
● Denied flows 30

Flow Filtering

Flow action

Select...

Destination port

Select...

Source namespace

Select...

Destination namespace

Select...

Source name

Select...

Destination name

Select...

Apply changes

Cancel changes

Clear form

Flow Logs

>	Jan 26, 2020 @ 18:28:47.000	122	allow	microservice2-fddf7cff8-*	storefront	backend-55f7dc6b68-*	storefront	8,080	dst
>	Jan 26, 2020 @ 18:28:47.000	2	deny	microservice2-fddf7cff8-*	storefront	twilio-api	-	80	src
>	Jan 26, 2020 @ 18:28:47.000	578	allow	frontend-6d9				53	src
>	Jan 26, 2020 @ 18:28:47.000	588	allow	microservice2-fddf7cff8-*				53	src
>	Jan 26, 2020 @ 18:28:47.000	61	allow	frontend-6d9				8,080	dst
>	Jan 26, 2020 @ 18:28:47.000	61	allow	frontend-6d9				8,080	src
>	Jan 26, 2020 @ 18:28:47.000	1	deny	microservice2-fddf7cff8-*	storefront	twilio-api	-	80	src
>	Jan 26, 2020 @ 18:28:47.000	306	allow	microservice1-7599d8d8f-*	storefront	coredns-5c98db65d4-*	kube-system	53	dst

t policies.all_policies 0|security|security.pci-whitelist|pass, 1|platform|platform.twilio-integration|deny
t proto tcp
t reporter src
source_ip 192.168.235.139
t source_labels.labels pod-template-hash=fddf7cff8, app=microservice2, fw-zone=trusted
t source_name microservice2-fddf7cff8-fqqd2



Compliance Reports

Filter: none

	Name	Type	Date Range	Created On
▶	daily-cis-results	cis-benchmark	01-26-20 00:00:00 GMT - 01-27-20 00:00:00 GMT	01-27-20 00:30:09 GMT
▼	daily-storefront-inventory	inventory	01-26-20 00:00:00 GMT - 01-27-20 00:00:00 GMT	01-27-20 00:30:09 GMT

Inscope vs Protected

Protected Ingress Endpoints: 5

5

71.4%

Total: 7

Protected Ingress Namespaces: 1

1

50%

Total: 2

Protected Egress Endpoints: 5

5

71.4%

Total: 7

Protected Egress Namespaces: 1

1

50%

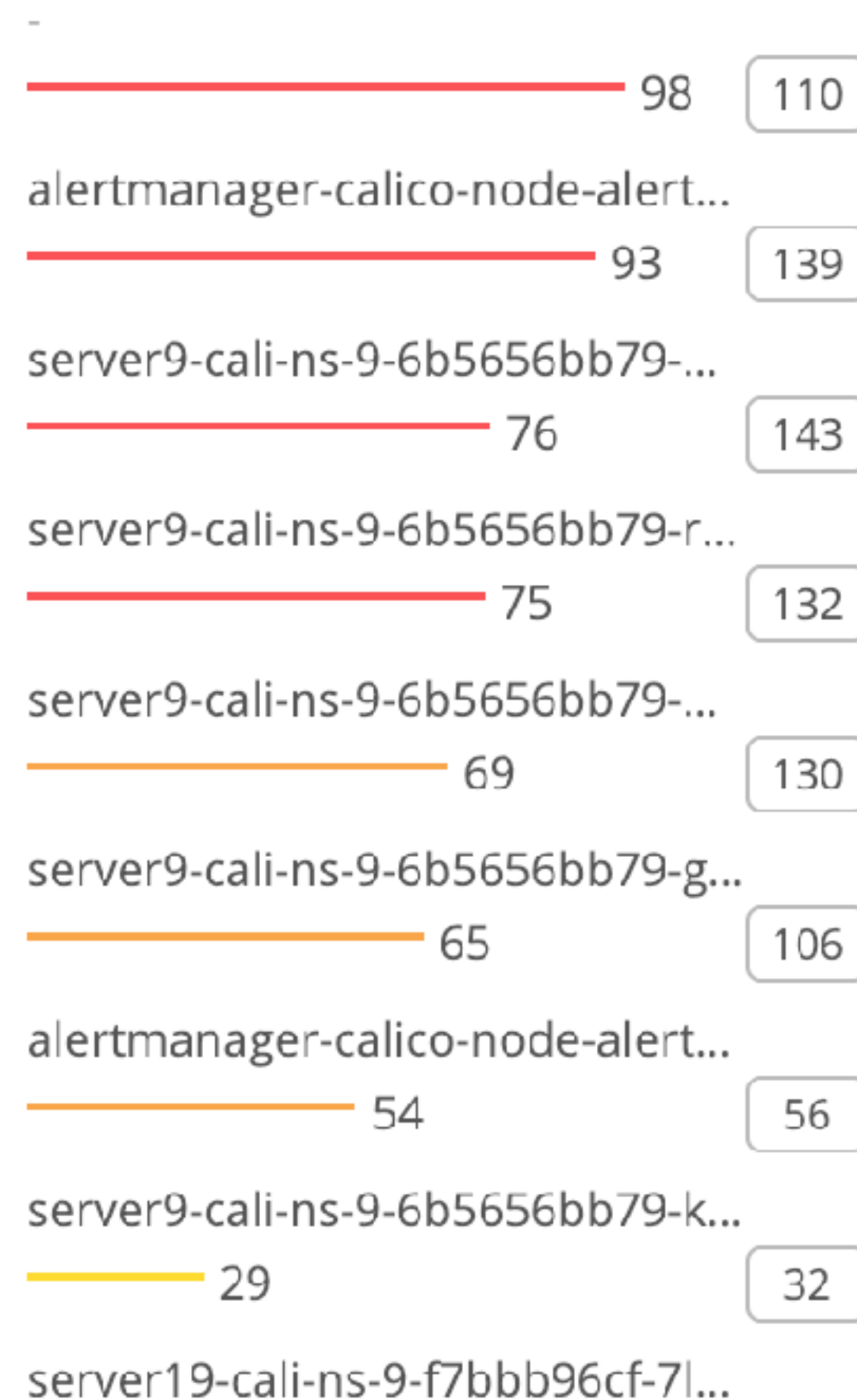
Total: 2

CALICO

ENTERPRISE

Top Influencers

dest_name



Anomaly timeline

Overall



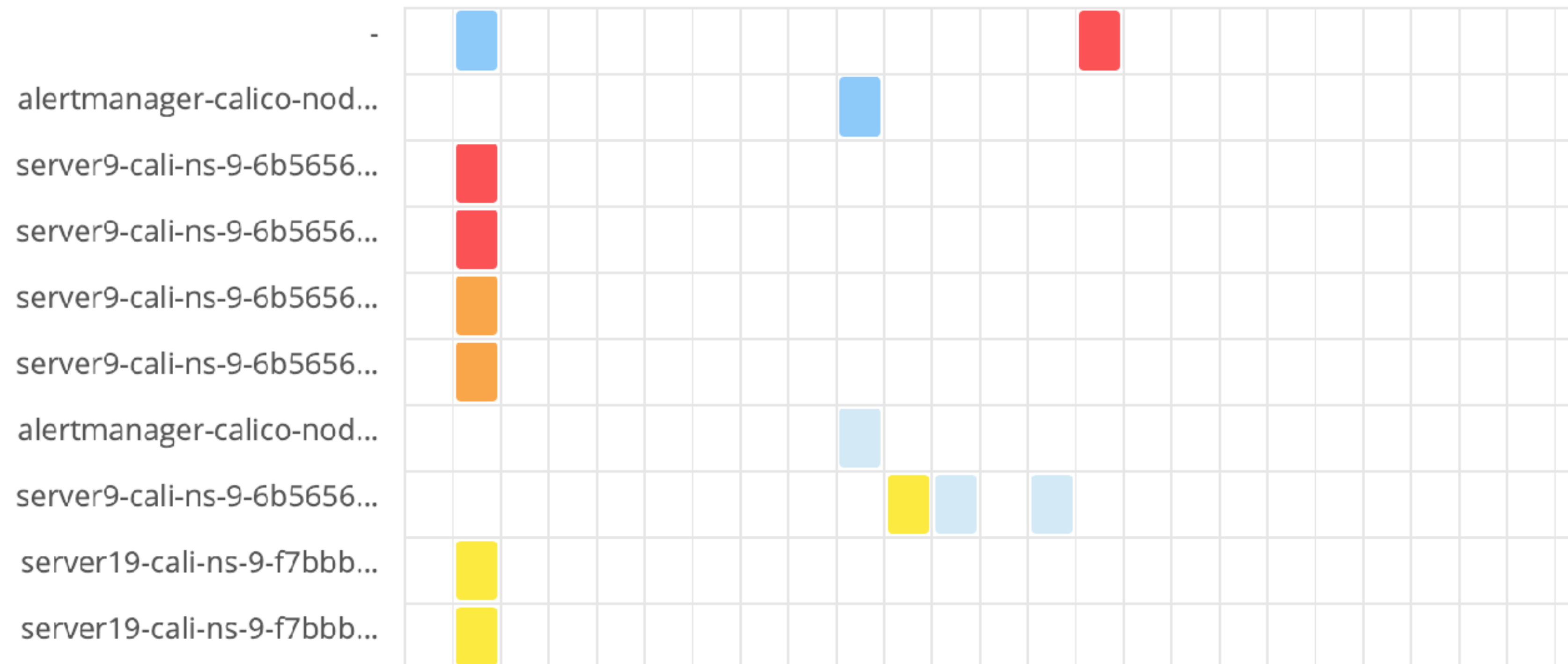
View by:

dest_name ▼

Limit:

10 ▼

(Sorted by max anomaly score)





Cluster A

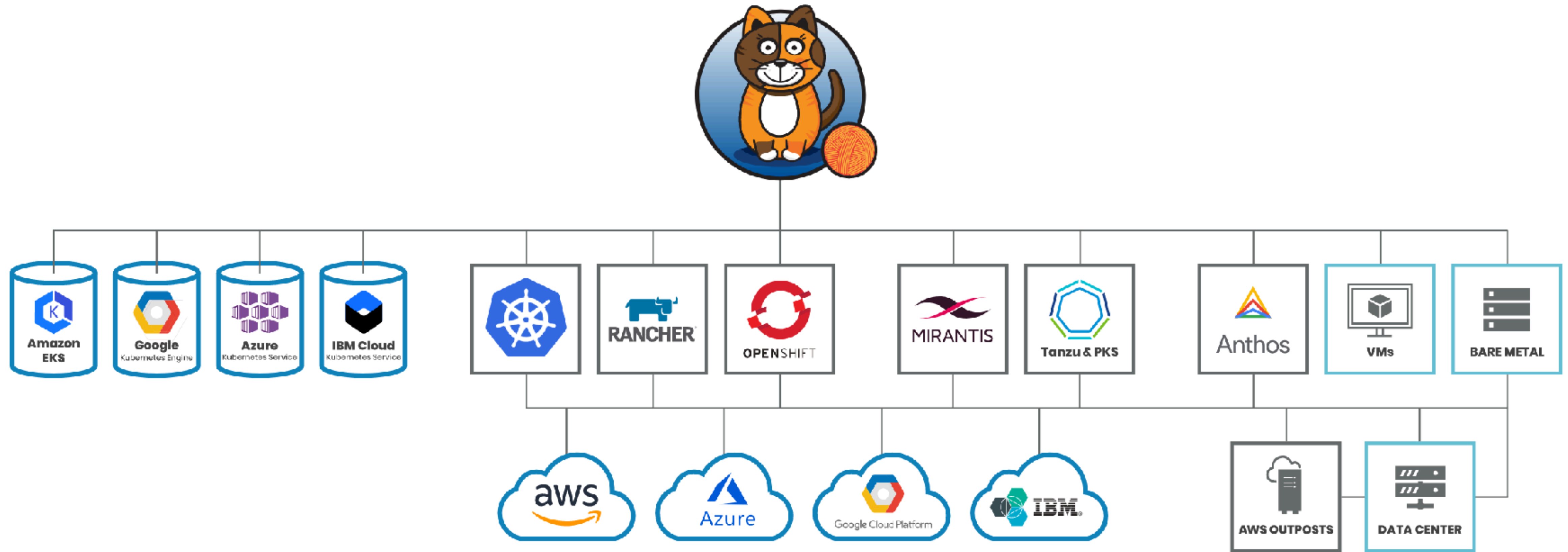


Cluster B



CALICO
ENTERPRISE

Industry Standard for Kubernetes Network Security



TG: @aladmit

TG channel: @aladmit_world