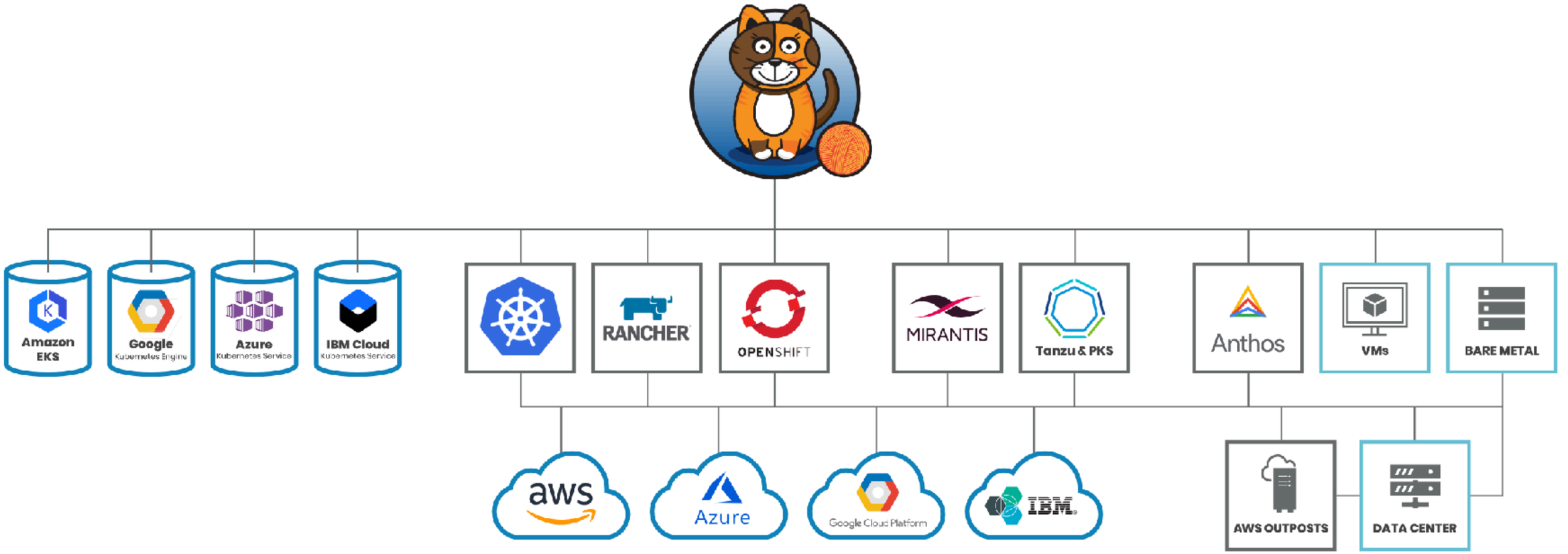
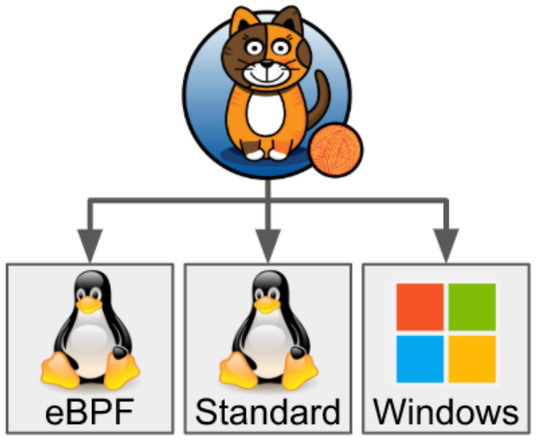
Calico изнутри

Архитектура и возможности

Александров Андрей

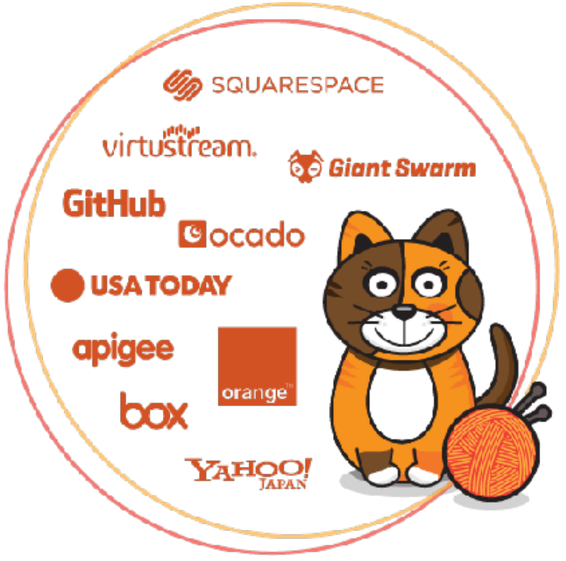
Industry Standard for Kubernetes Network Security





Best Practices

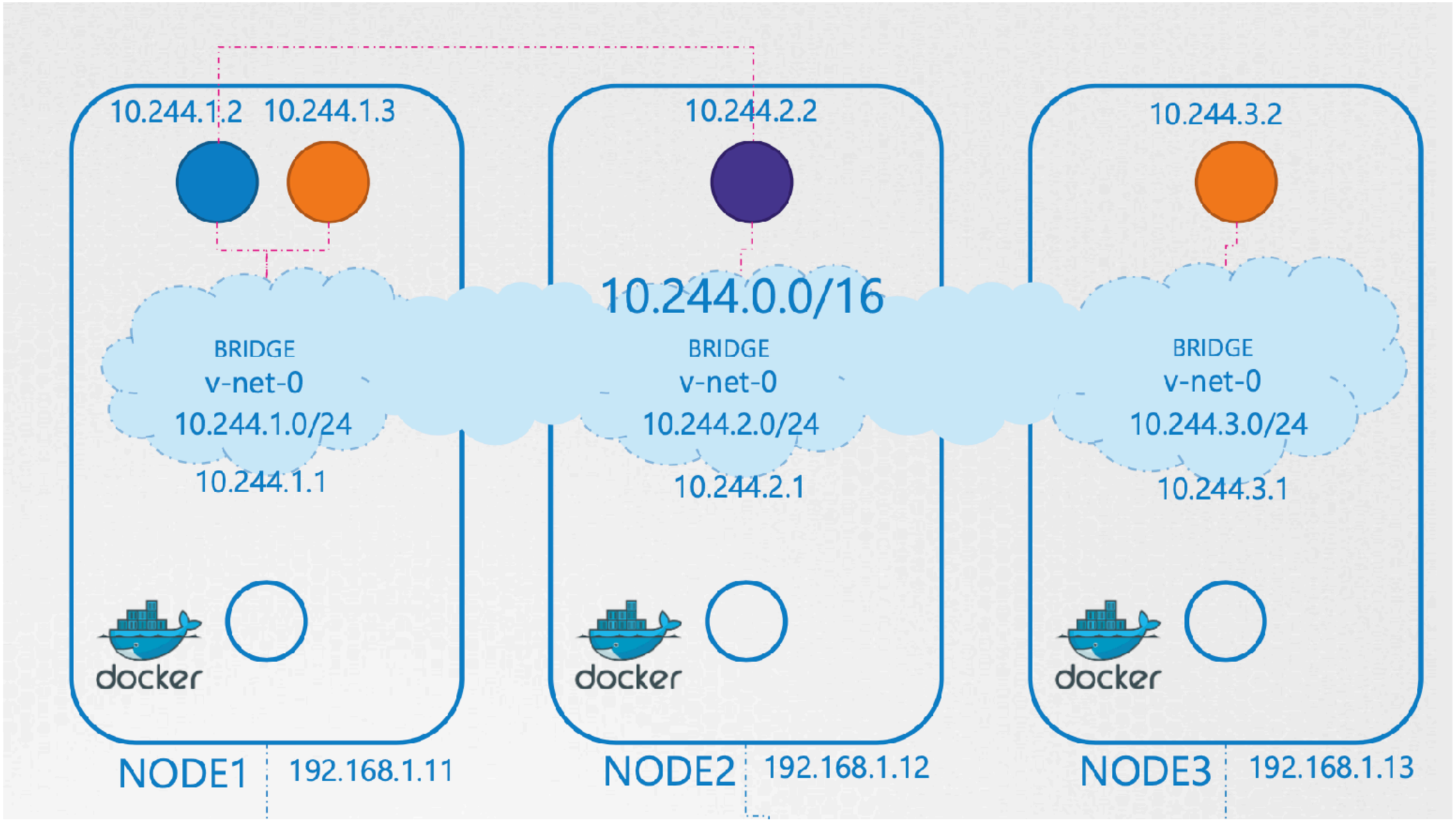
- Adopt zero trust network security model
- Infrastructure as code



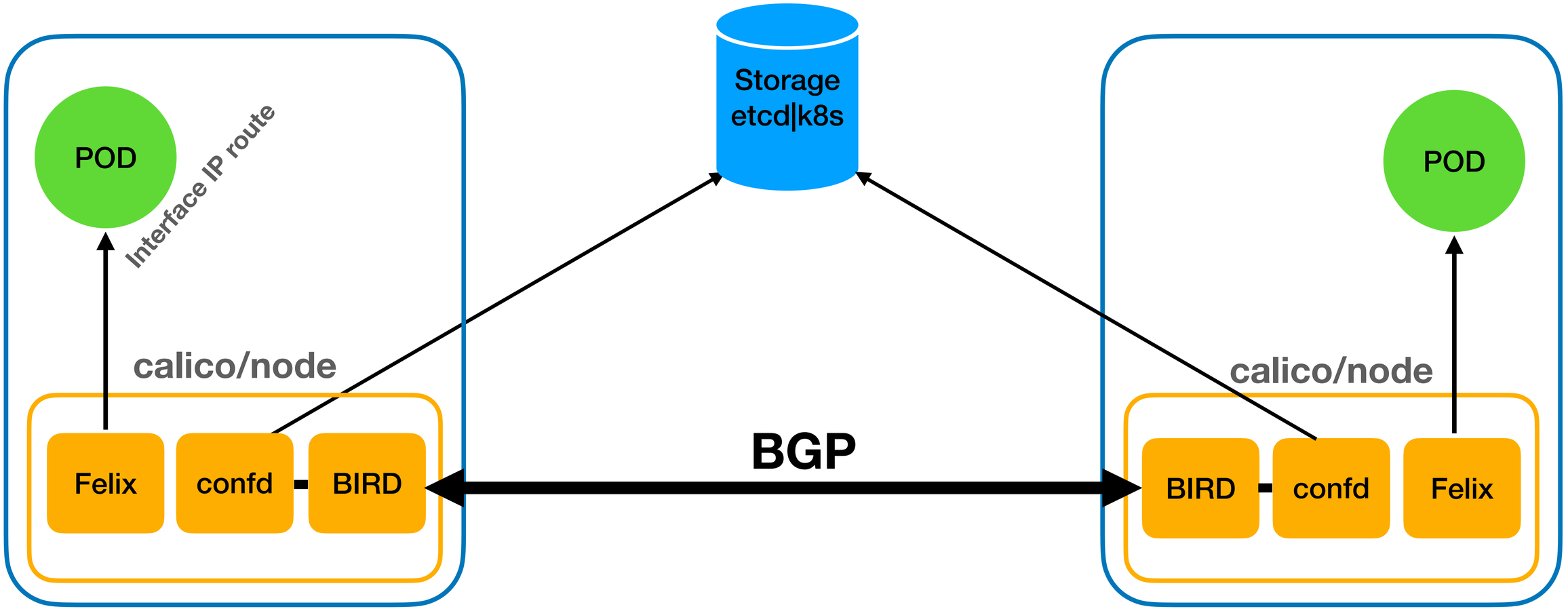
Kubernetes Network Model

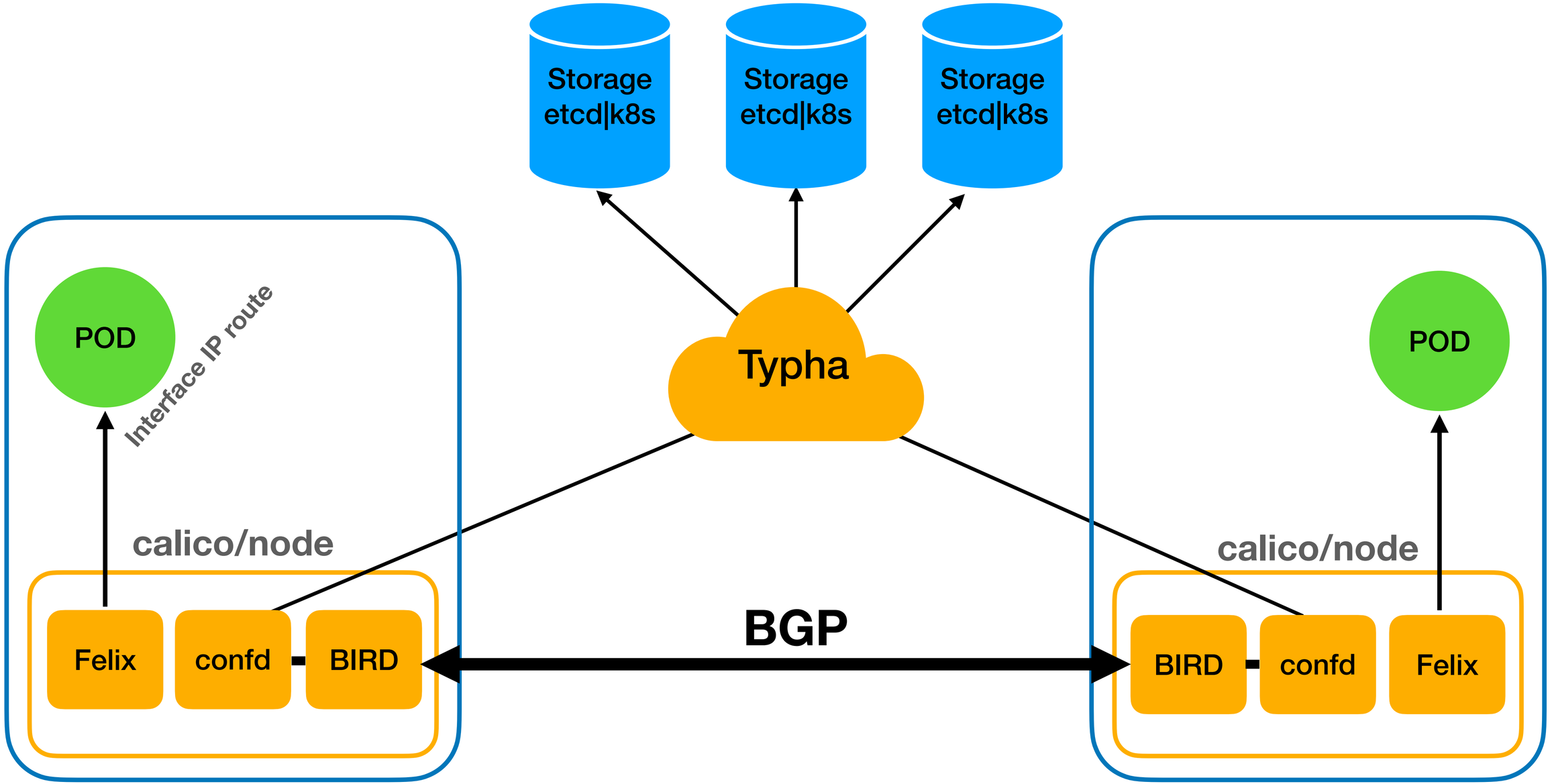
- Every pod gets its own IP address
- Containers within a pod share the pod IP address and can communicate freely with each other
- Pods can communicate with all other pods in the cluster using pod IP addresses (without NAT)

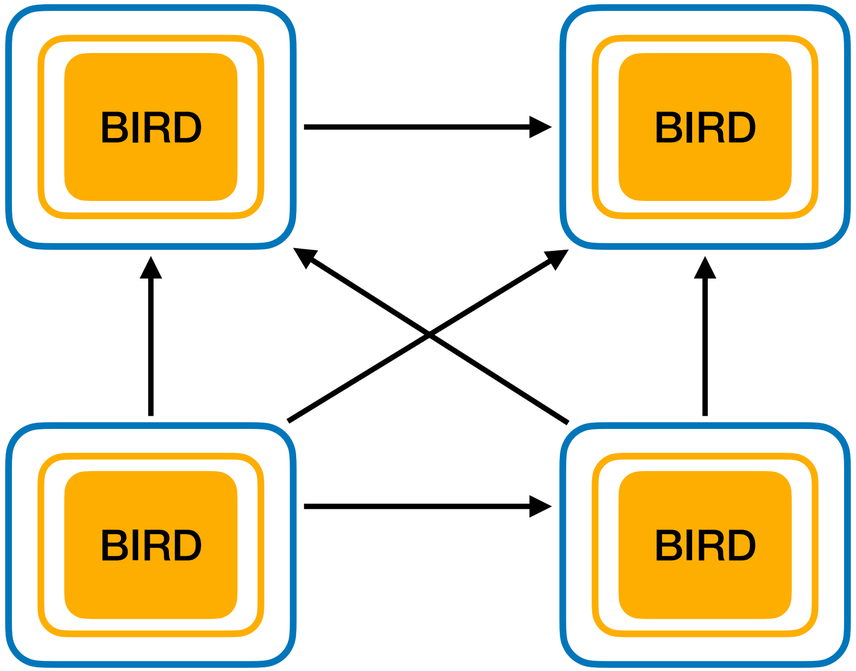
Kubernetes Network Model

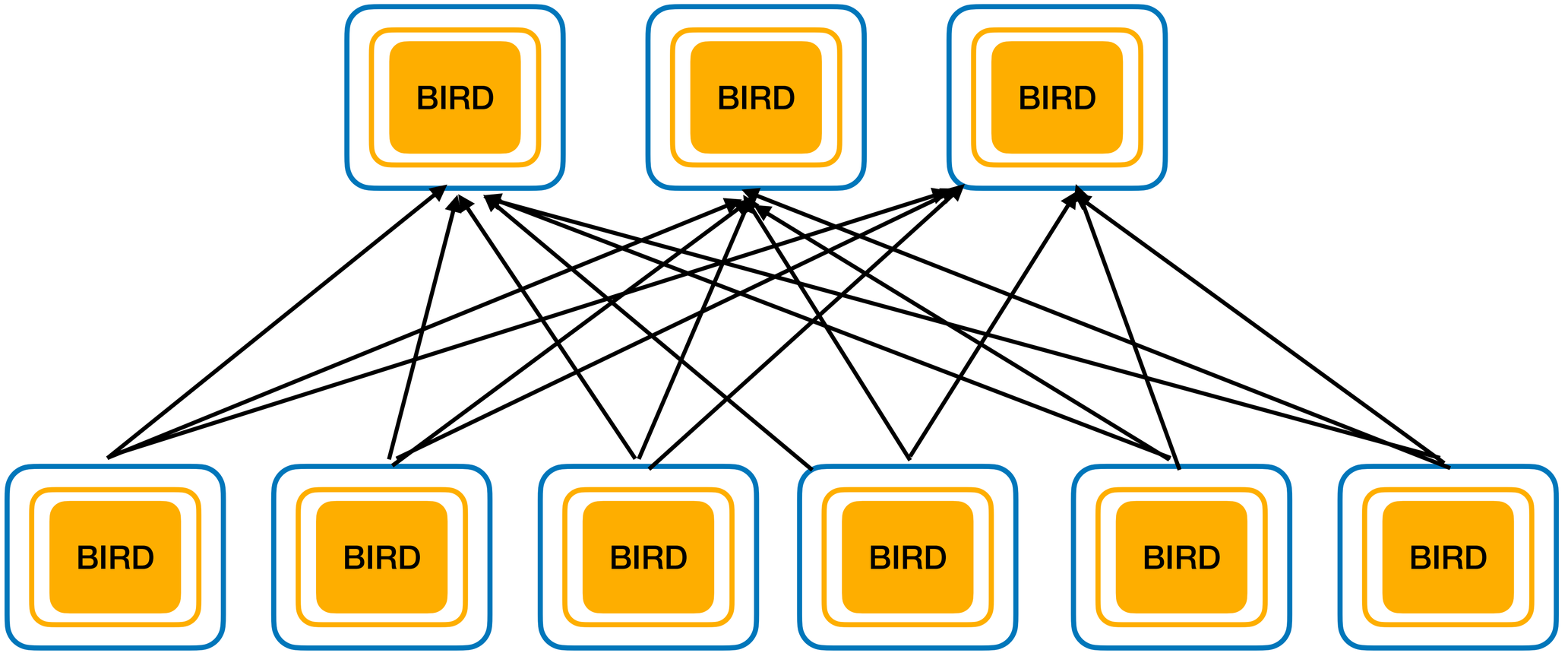


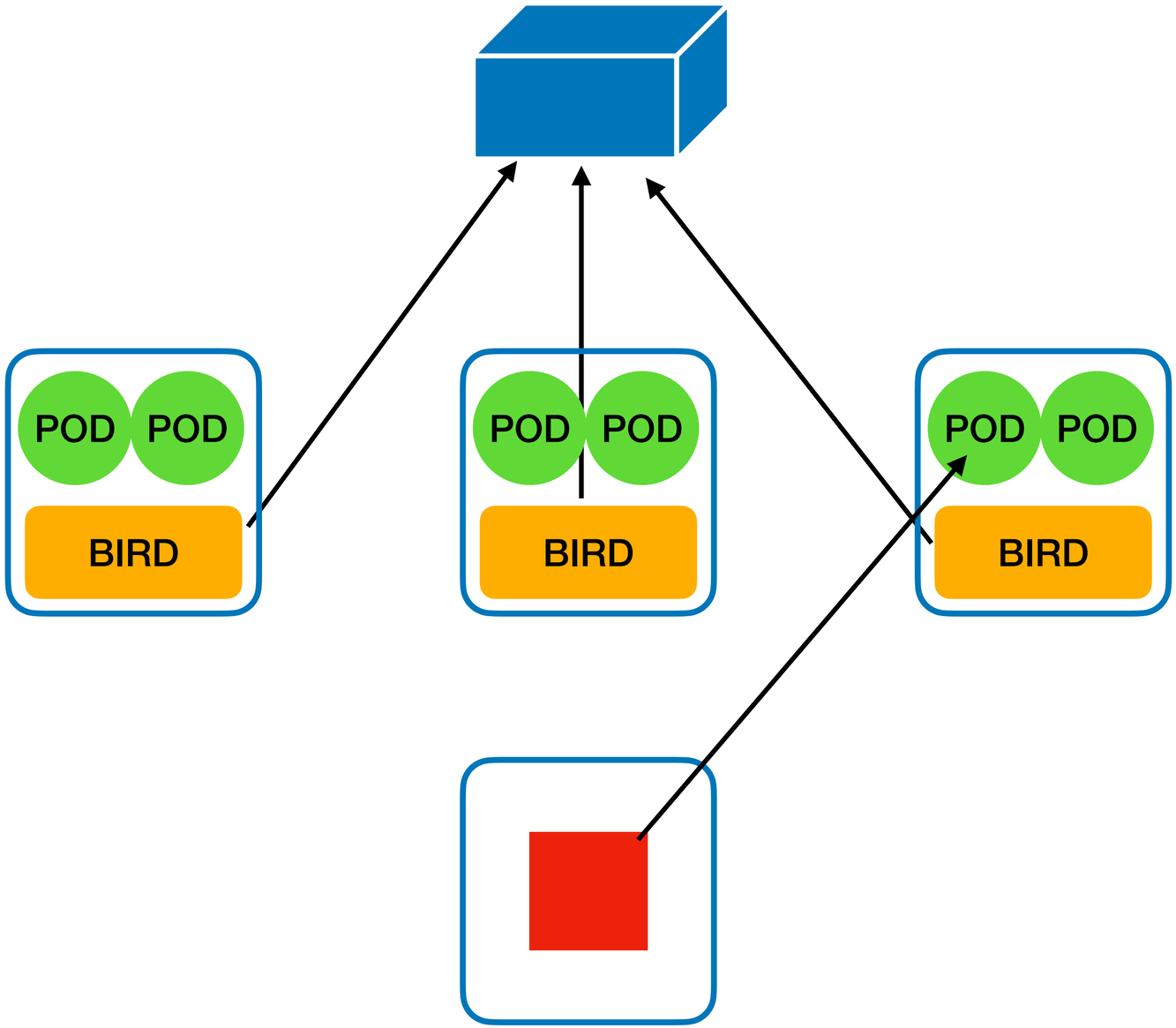
Calico Architecture



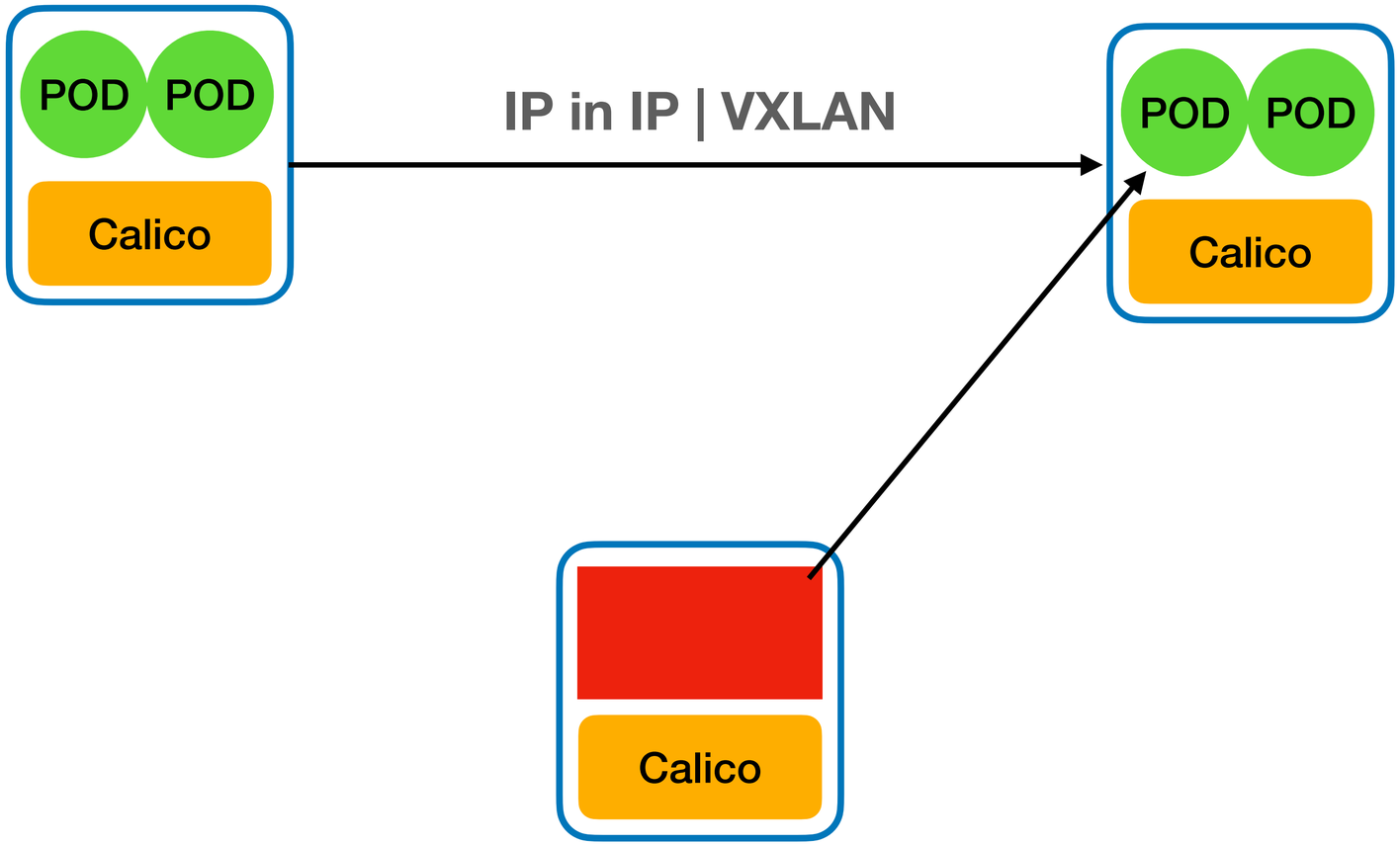

Storage
etcd|k8s
Storage
etcd|k8s
Storage
etcd|k8s
Typha
POD
Interface IP route
calico/node
Felix
confd
BIRD
BGP
POD
calico/node
BIRD
confd
Felix


BIRD
BIRD
BIRD
BIRD


BIRD
BIRD
BIRD
BIRD
BIRD
BIRD
BIRD
BIRD
BIRD


POD
POD
BIRD
POD
POD
BIRD
POD
POD
BIRD

Overlay Network



Если все открыто, мы в опасности!

- k8s API / etcd
- Попав 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
- Скомпроментированные хосты не могут обойти примененные политики
- Идентификация эндпоинта устанавливается по IP/port и криптографии(SSL)
- Шифрование траффика

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]
```

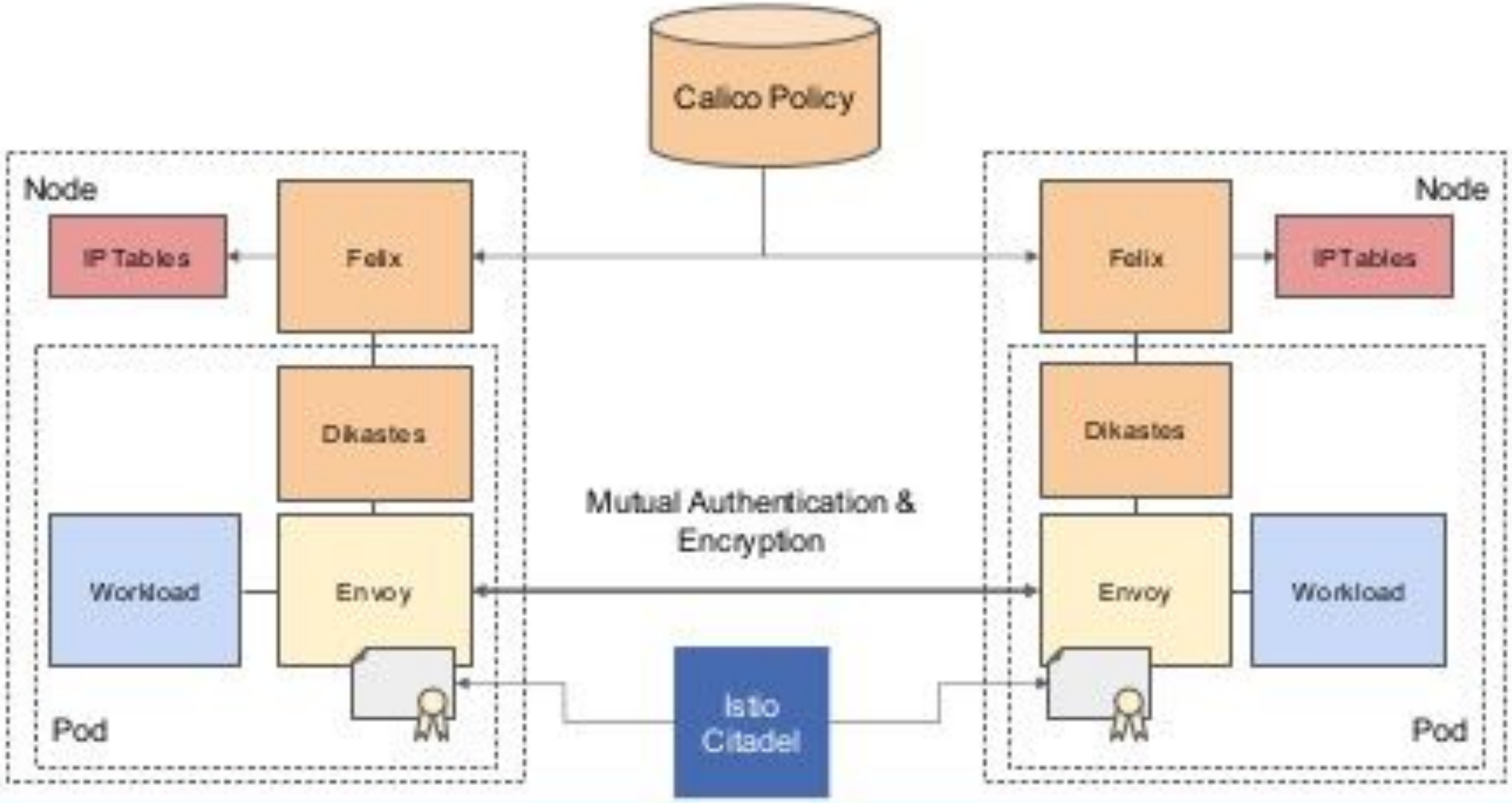
Защита от дурака!

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



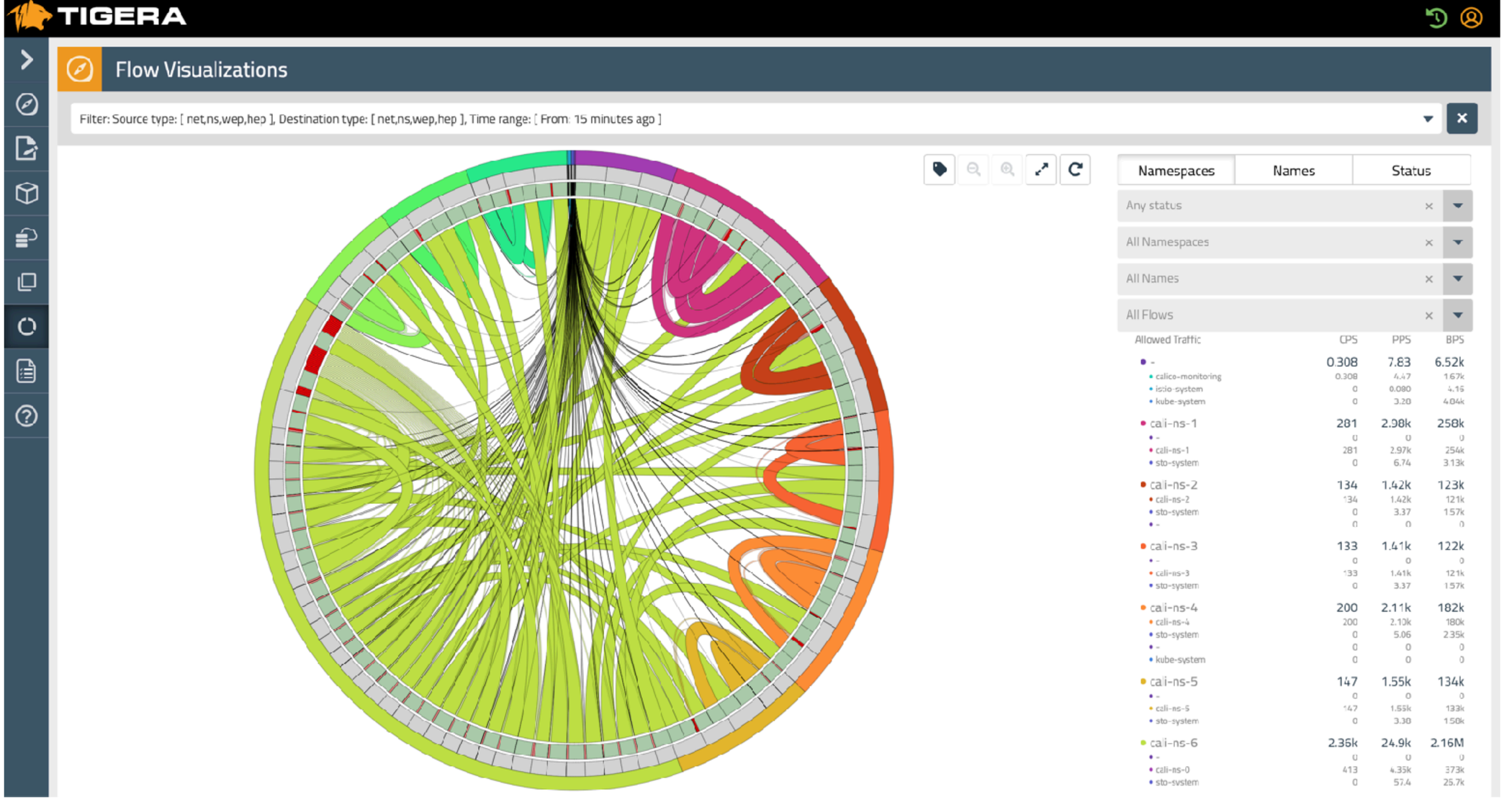
Zero Trust Network Model

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

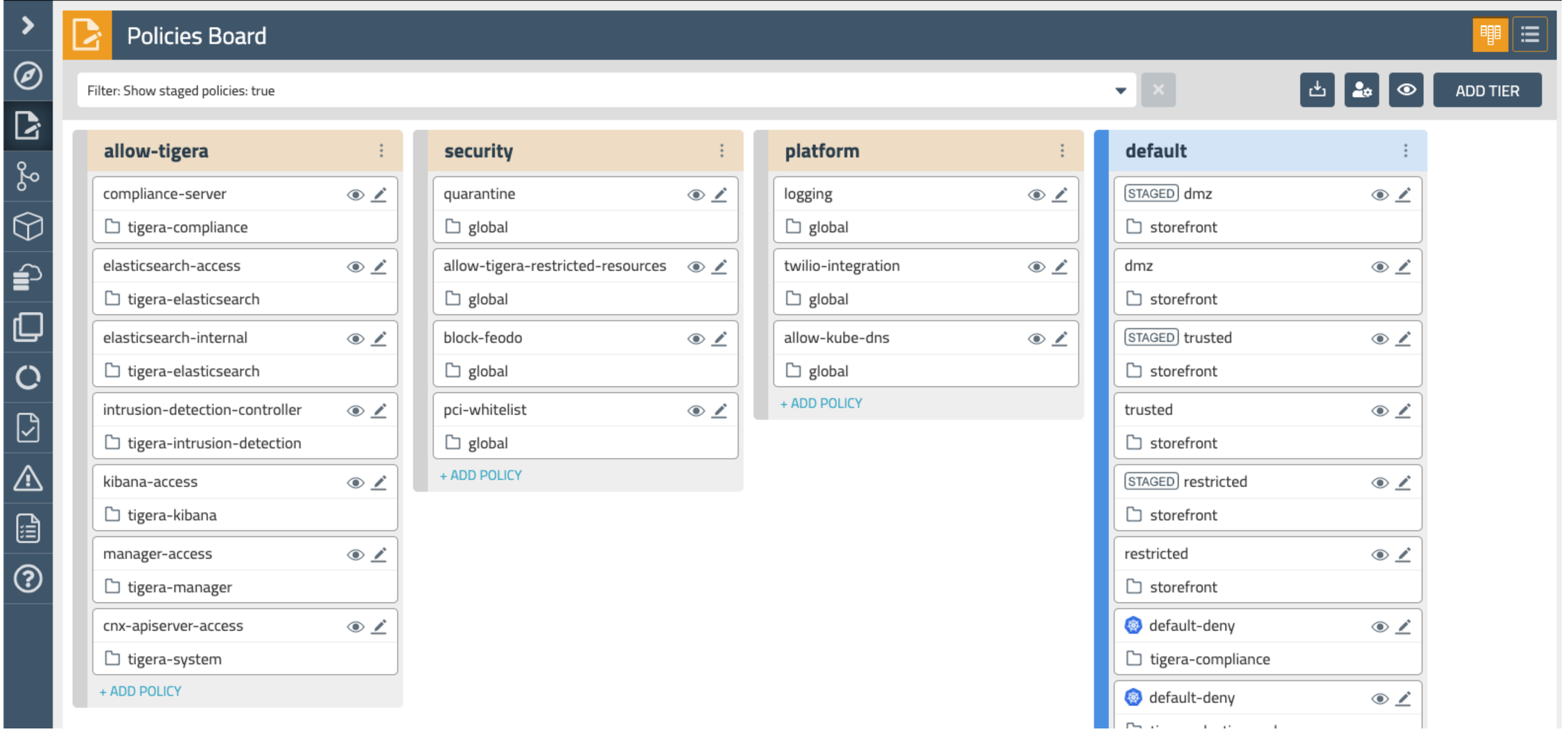
```
...
  status:
    ..
    wireguardPublicKey: jlkVyQYooZYzI2wFfNhSZez5e
    ...
```

CALICO ENTERPRISE

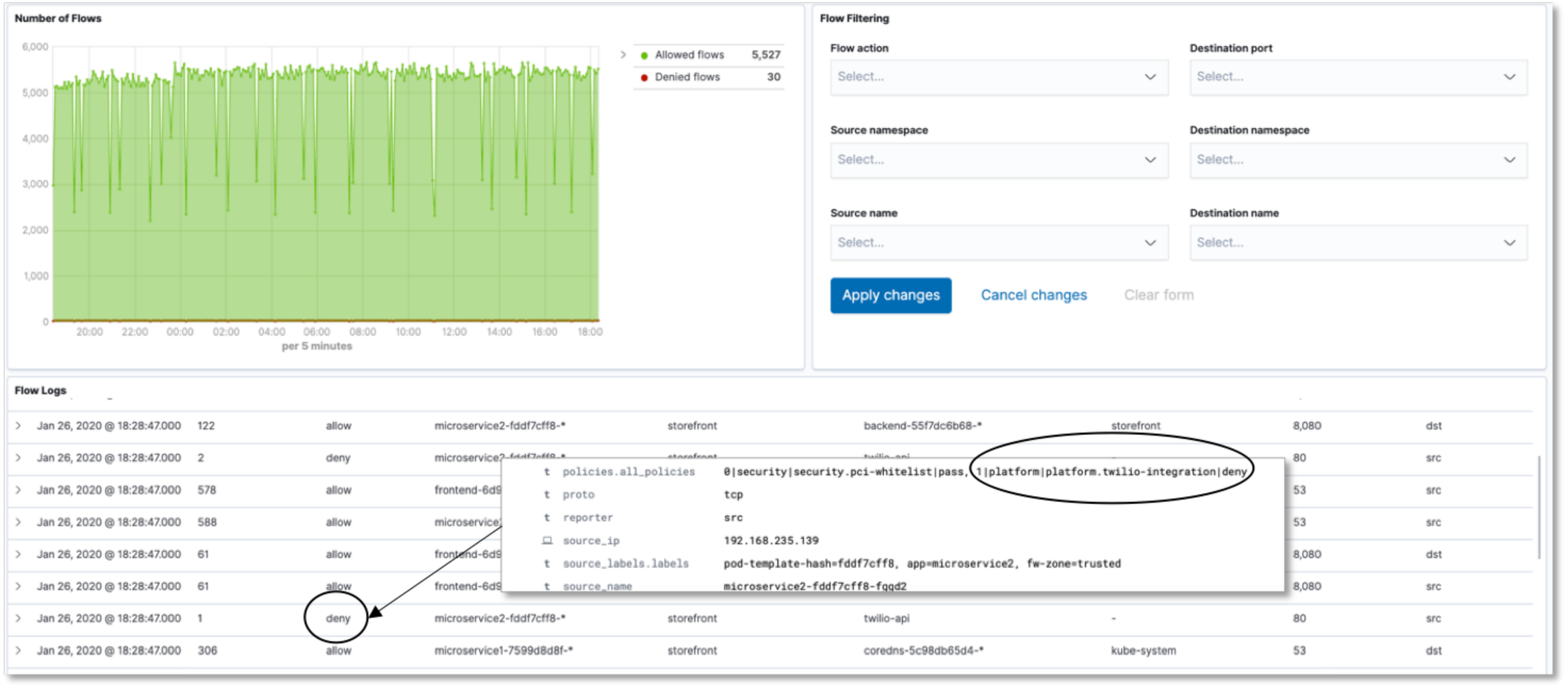
- Hierarchical network policy
- Egress access controls (DNS policies, egress gateways)
- Network visualization and troubleshooting
- Network policy recommendations
- Network policy preview and staging
- Compliance controls and reporting
- Intrusion detection (suspicious activity, anomaly detection)
-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



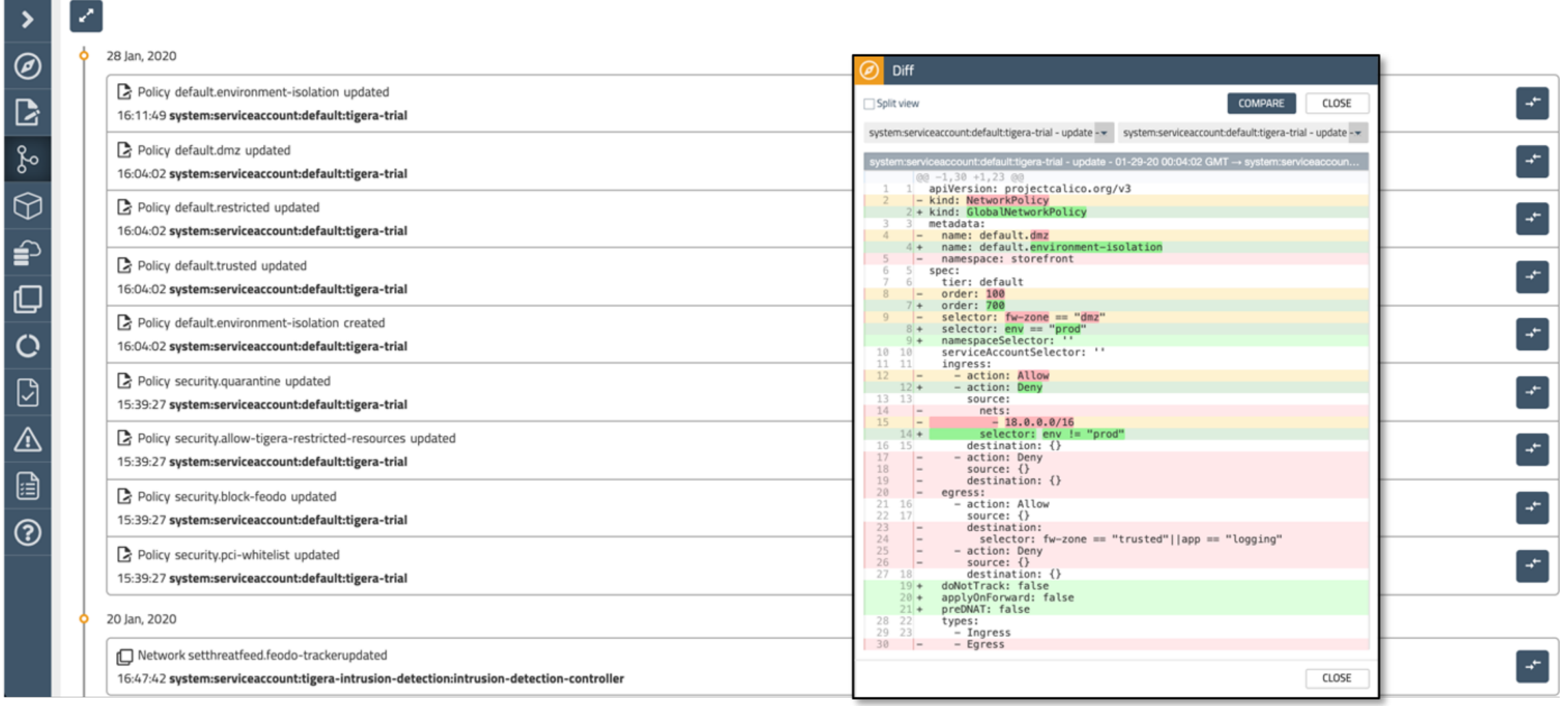
CALICO ENTERPRISE



CALICO
ENTERPRISE



CALICO ENTERPRISE



CALICO ENTERPRISE

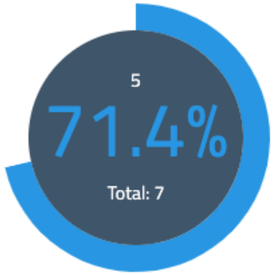
Compliance Reports

Filter: none

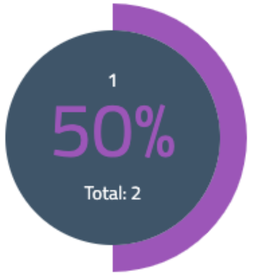
	Name	Type	Date Range	Created On
▶	daily-cis-results	cis-benchmark	01-26-20 00:00:00 GMT - 01-27-20 00:00:00 GMT	01-27-20 00:30:09 GMT
▼	daily-storefront-inventory	inventory	01-26-20 00:00:00 GMT - 01-27-20 00:00:00 GMT	01-27-20 00:30:09 GMT

Inscope vs Protected

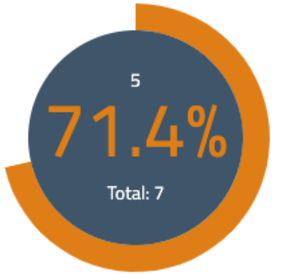
Protected Ingress Endpoints: 5



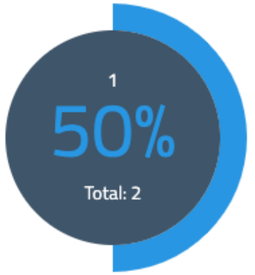
Protected Ingress Namespaces: 1



Protected Egress Endpoints: 5



Protected Egress Namespaces: 1



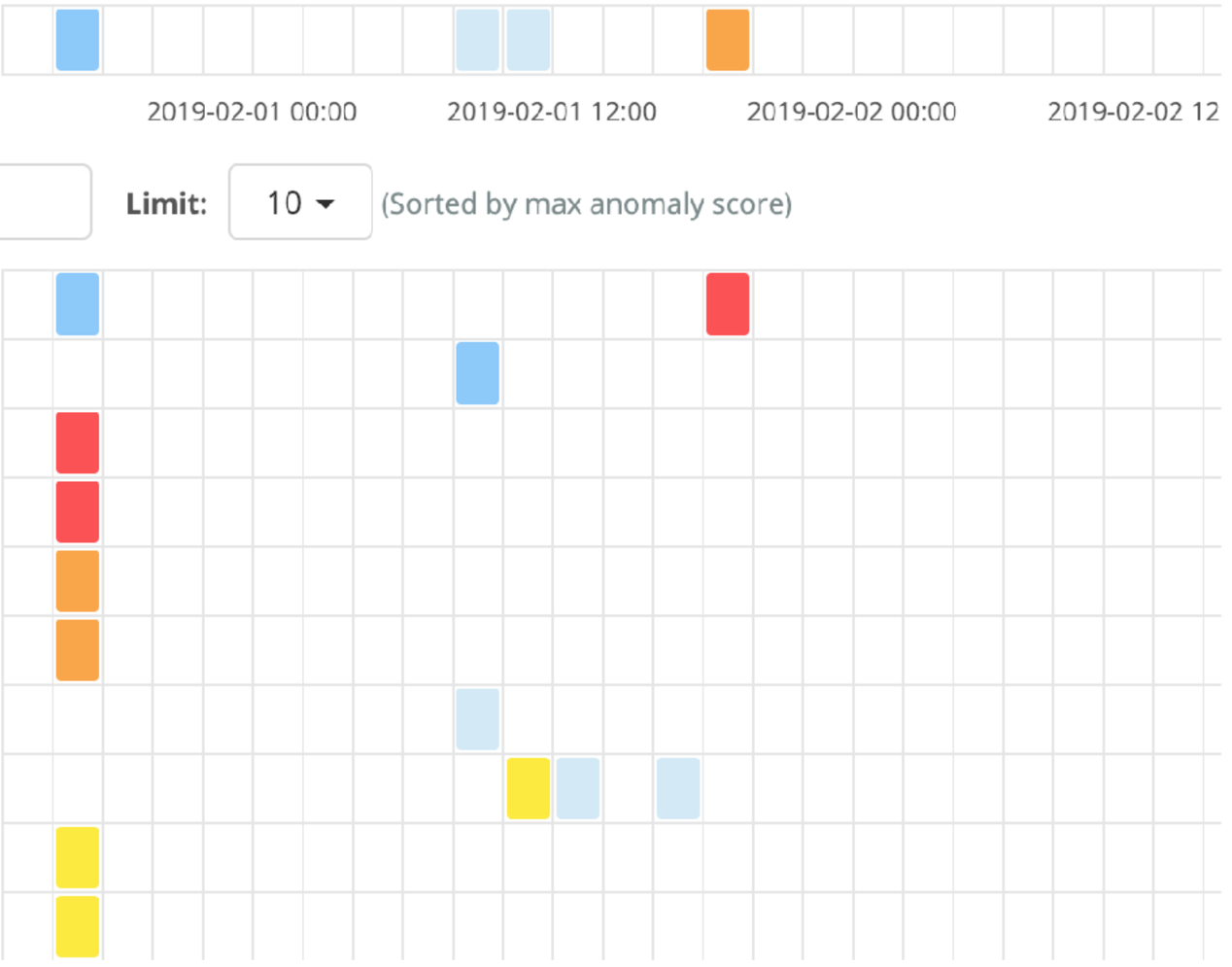
CALICO ENTERPRISE

Top Influencers

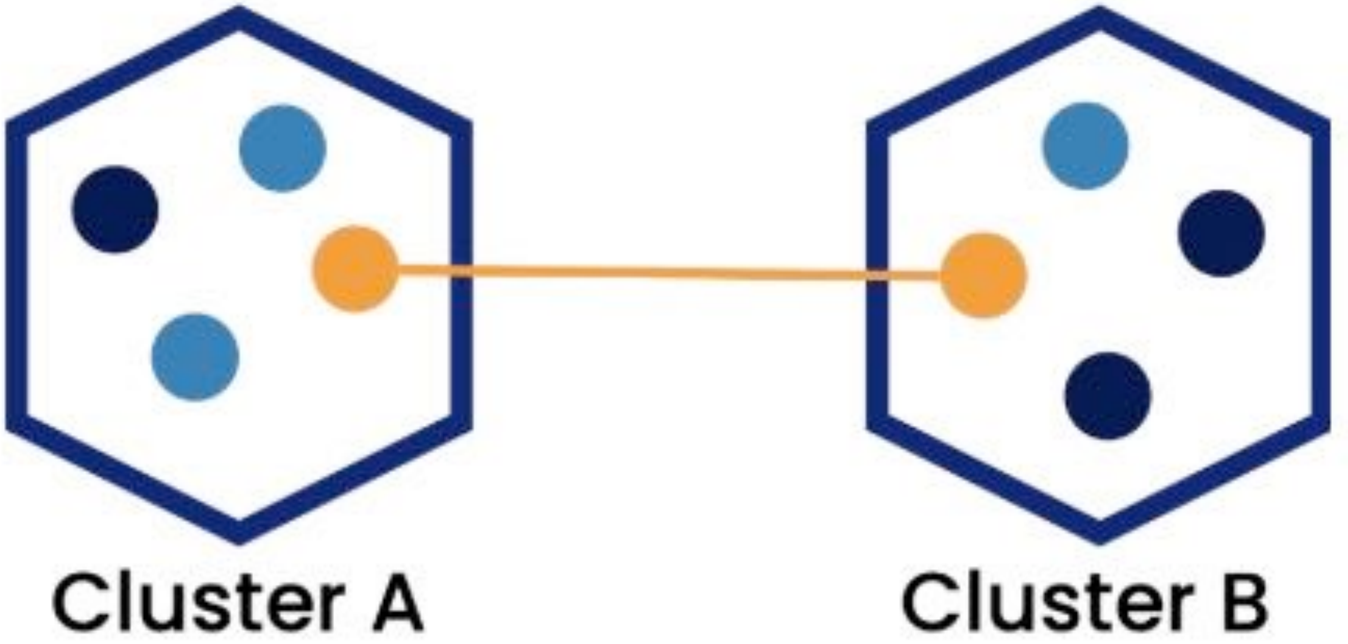
dest_name

-	98	110
alertmanager-calico-node-alert...	93	139
server9-cali-ns-9-6b5656bb79-...	76	143
server9-cali-ns-9-6b5656bb79-r...	75	132
server9-cali-ns-9-6b5656bb79-...	69	130
server9-cali-ns-9-6b5656bb79-g...	65	106
alertmanager-calico-node-alert...	54	56
server9-cali-ns-9-6b5656bb79-k...	29	32
server19-cali-ns-9-f7bbb96cf-7l...		

Anomaly timeline

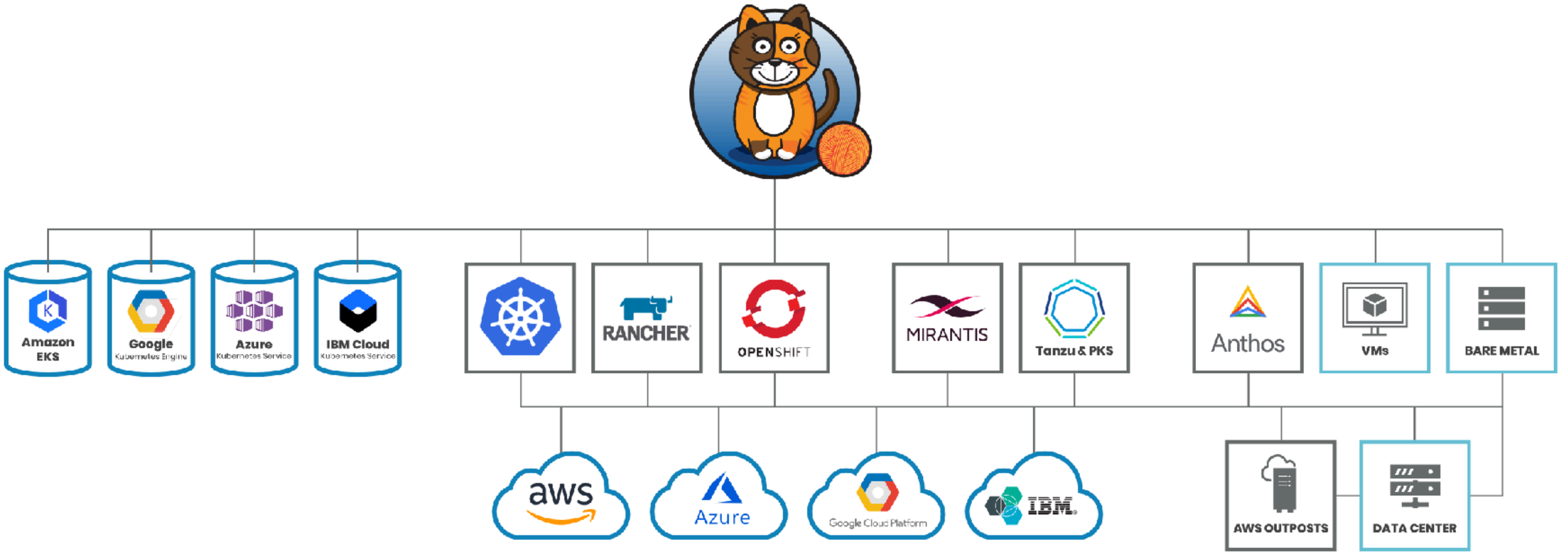


CALICO ENTERPRISE



CALICO
ENTERPRISE

Industry Standard for Kubernetes Network Security



TG: @aladmit

TG channel: @aladmit_world