ISOVALENT

When is a secure connection not encrypted?

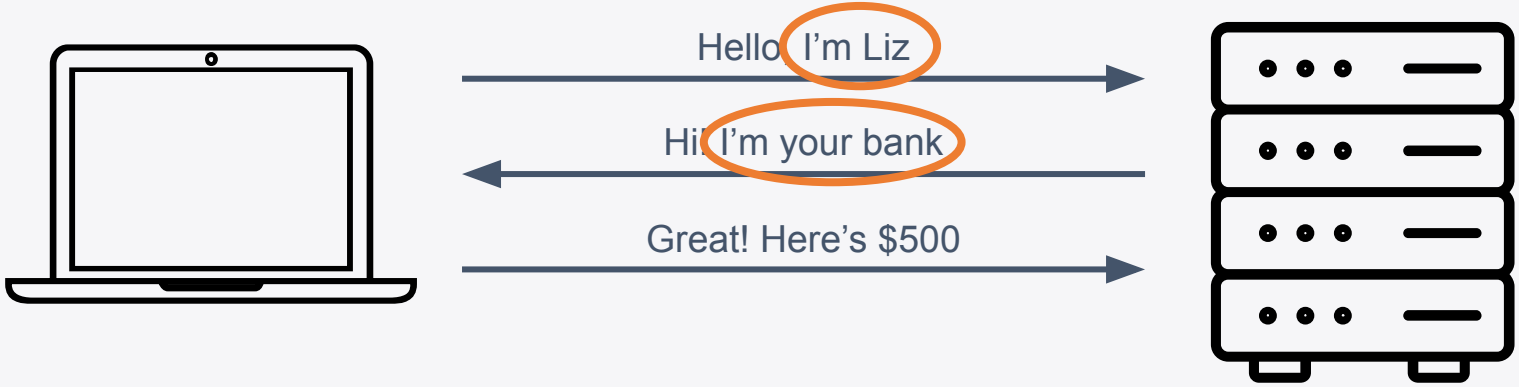
And other stories

Liz Rice | @lizrice
Chief Open Source Officer, Isovalent
Emeritus Chair, CNCF Technical Oversight Committee | CNCF & OpenUK boards

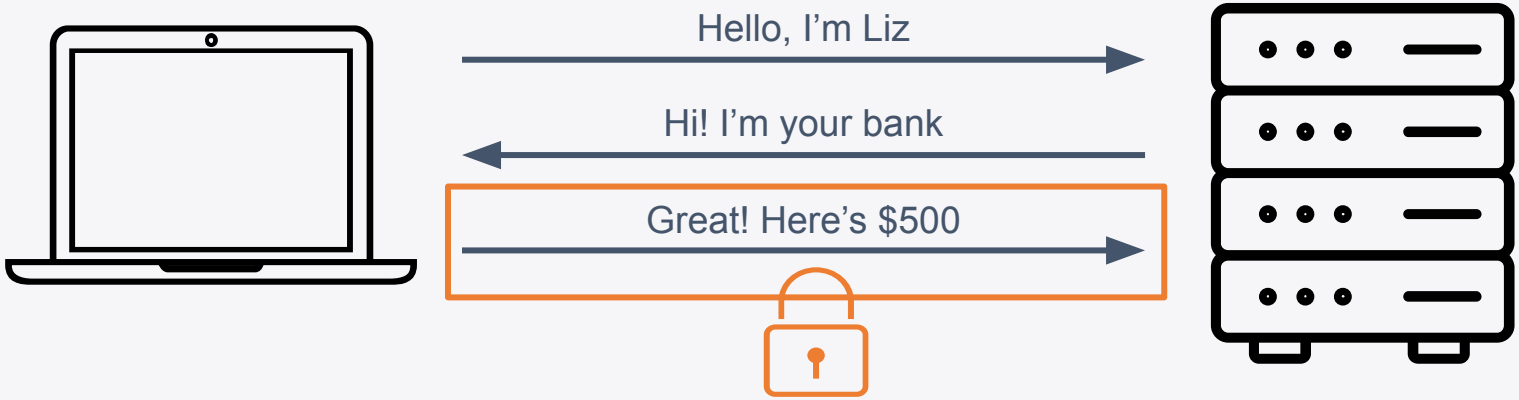
ISOVALENT

What do we mean by “secure connection”?

Authentication = establishing identity



Encryption

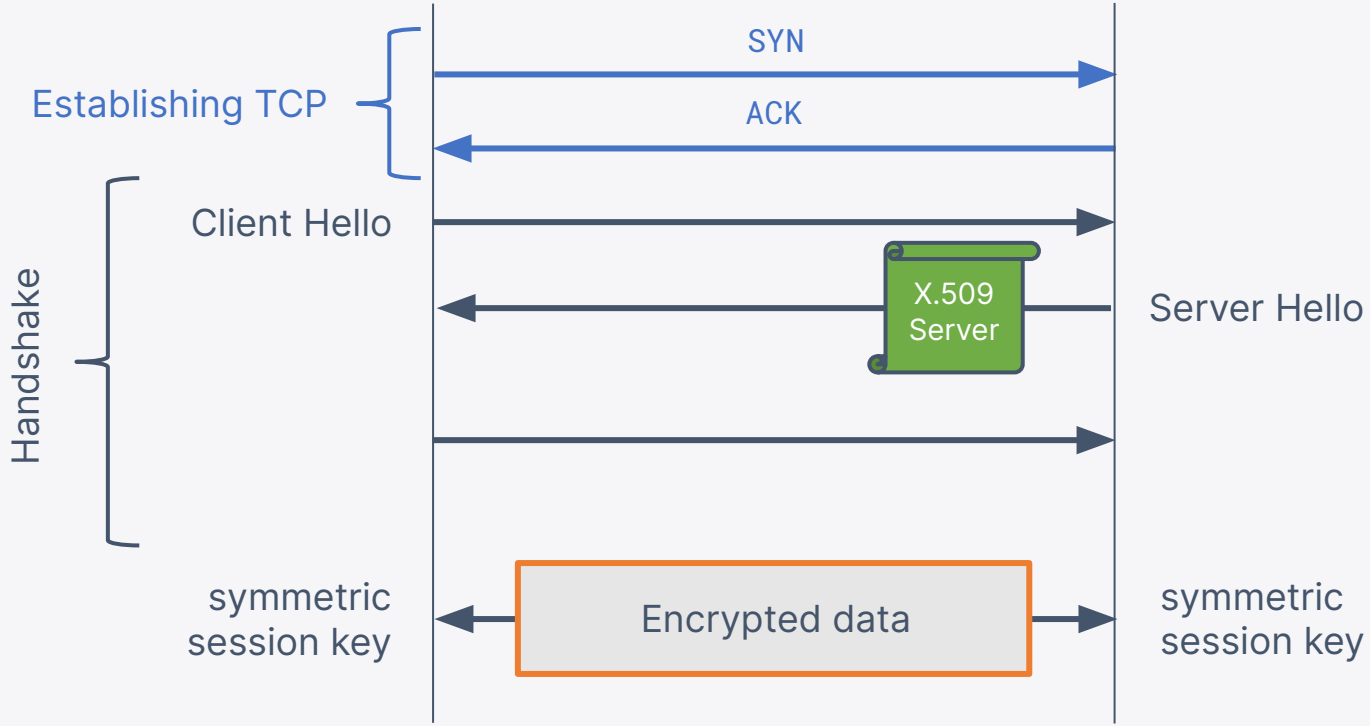


ISOVALENT

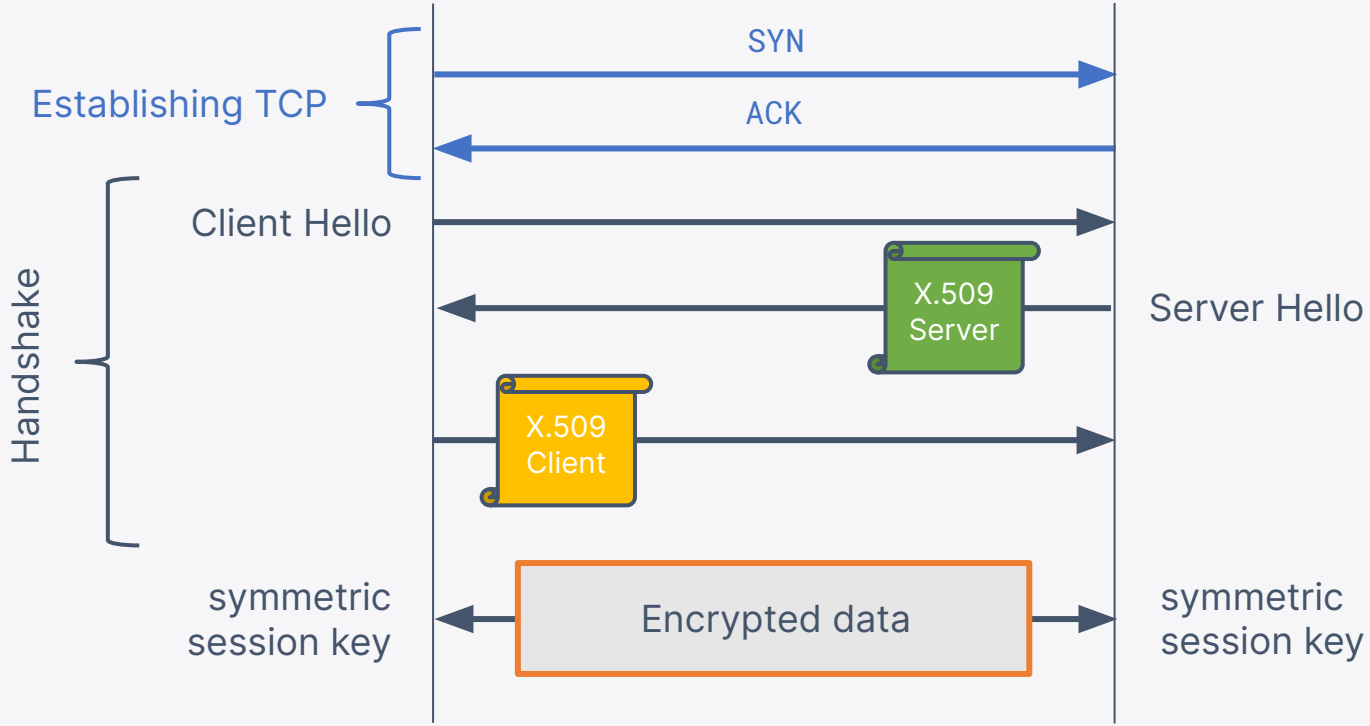
TLS and Mutual TLS

@lizrice

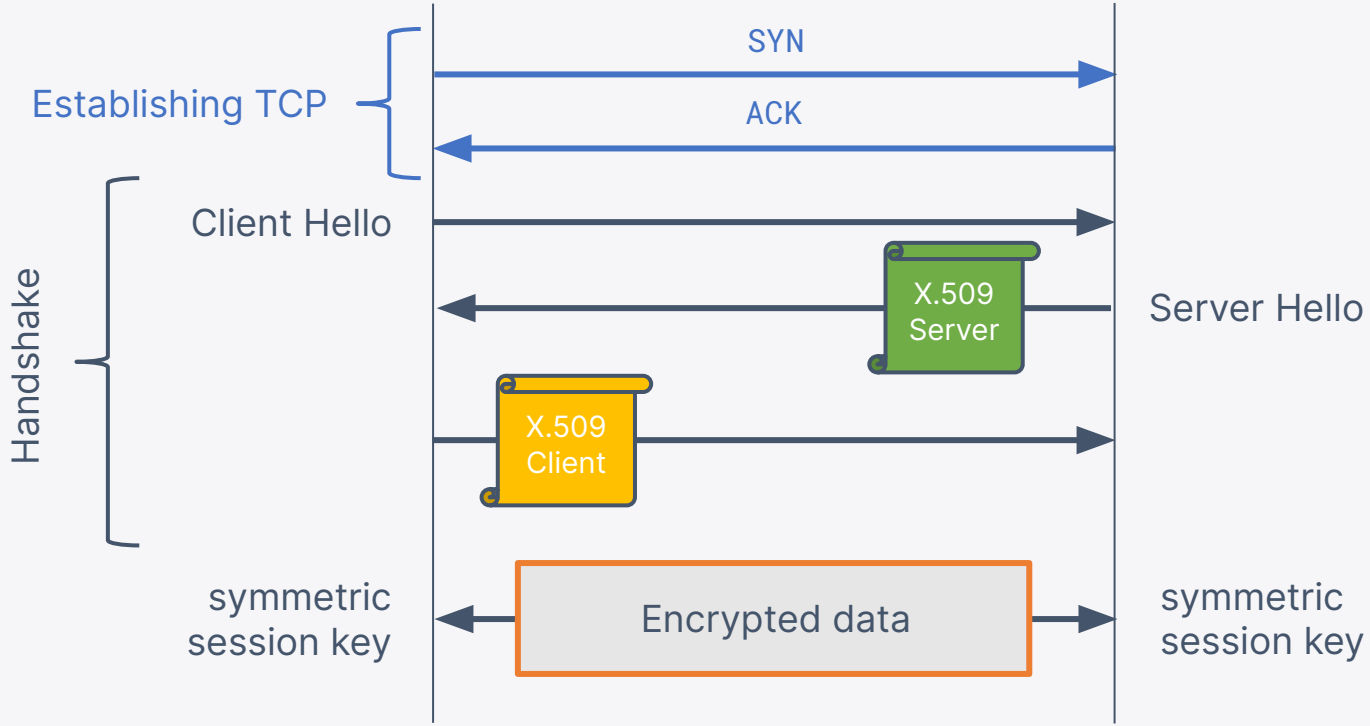
TLS handshake



mTLS handshake



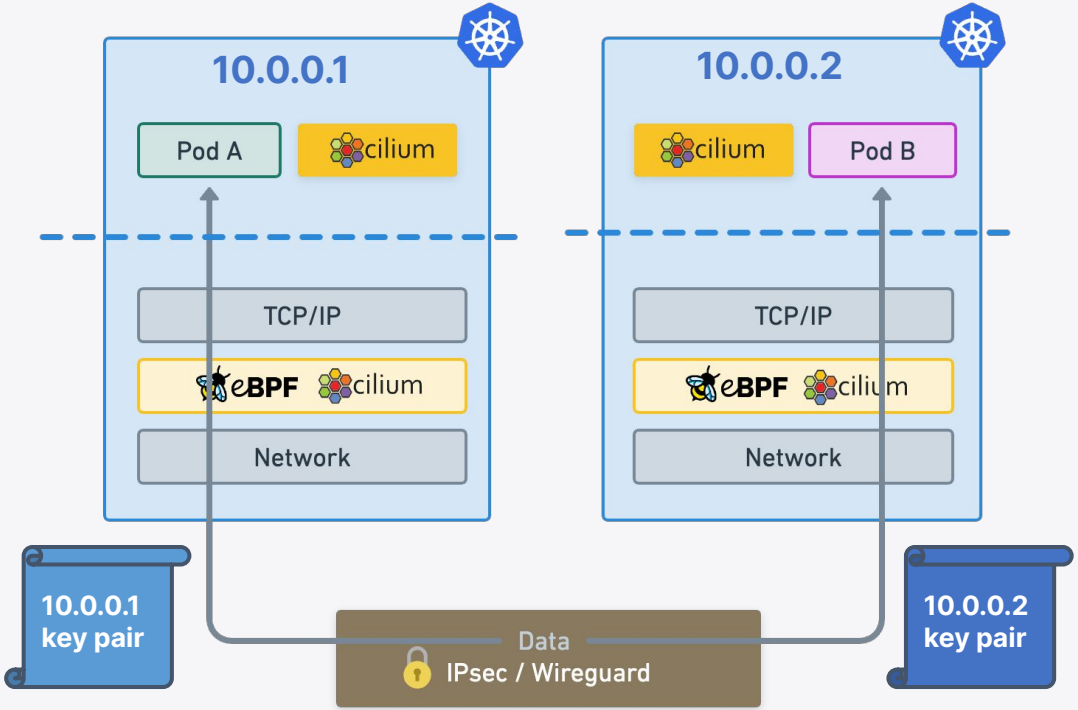
mTLS handshake upgrades a TCP connection to be authenticated and encrypted



ISOVALENT

Transparent encryption

Transparent encryption between nodes



WireGuard / IPsec

Typically used for VPNs, tunnelling encrypted IP traffic encapsulated in UDP packets

WireGuard

“You add a WireGuard interface, configure it with your private key and your peers' public keys, and then you send packets across it.”

Widely considered more secure but uses non-FIPS-compliant cryptography protocols

Automated key rotation

IPsec

Sets up and maintains tunnels between endpoints

Can be FIPS-compliant

Droid conversation

```
$ k get pods -o wide
NAME      READY   STATUS    RESTARTS        AGE     IP              NODE
c-3po     1/1     Running   0               3d17h   10.244.2.2      kind-worker2
r2-d2     1/1     Running   0               2d      10.244.1.16     kind-worker

$ k exec -it c-3po -- curl r2-d2
beep! beep-bee-beep! beepeebeep!!
```

Examine traffic flowing on eth0 port

No encryption

```
root@kind-worker:/#  tcpdump -i eth0  -A | grep beep
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
beep! beep-bee-beep! beepeebeep!!
```

With WireGuard enabled

```
$ cilium upgrade --reuse-values --set encryption.enabled=true
--set encryption.type=wireguard

root@kind-worker:/#  tcpdump -i eth0  -A | grep beep
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

ISOVALENT

Restrict traffic with Cilium Network Policy

@lizrice

Network policy restricts traffic

```
apiVersion: "cilium.io/v2"
kind: CiliumNetworkPolicy
metadata:
  name: "droid"
  namespace: farfaraway
spec:
  description: "Droid communication policy"
  endpointSelector:
    matchLabels:
      class: droid
    ingress:
    - fromEndpoints:
      - matchLabels:
        org: rebel-alliance
```

Cilium identity is derived from Kubernetes lables

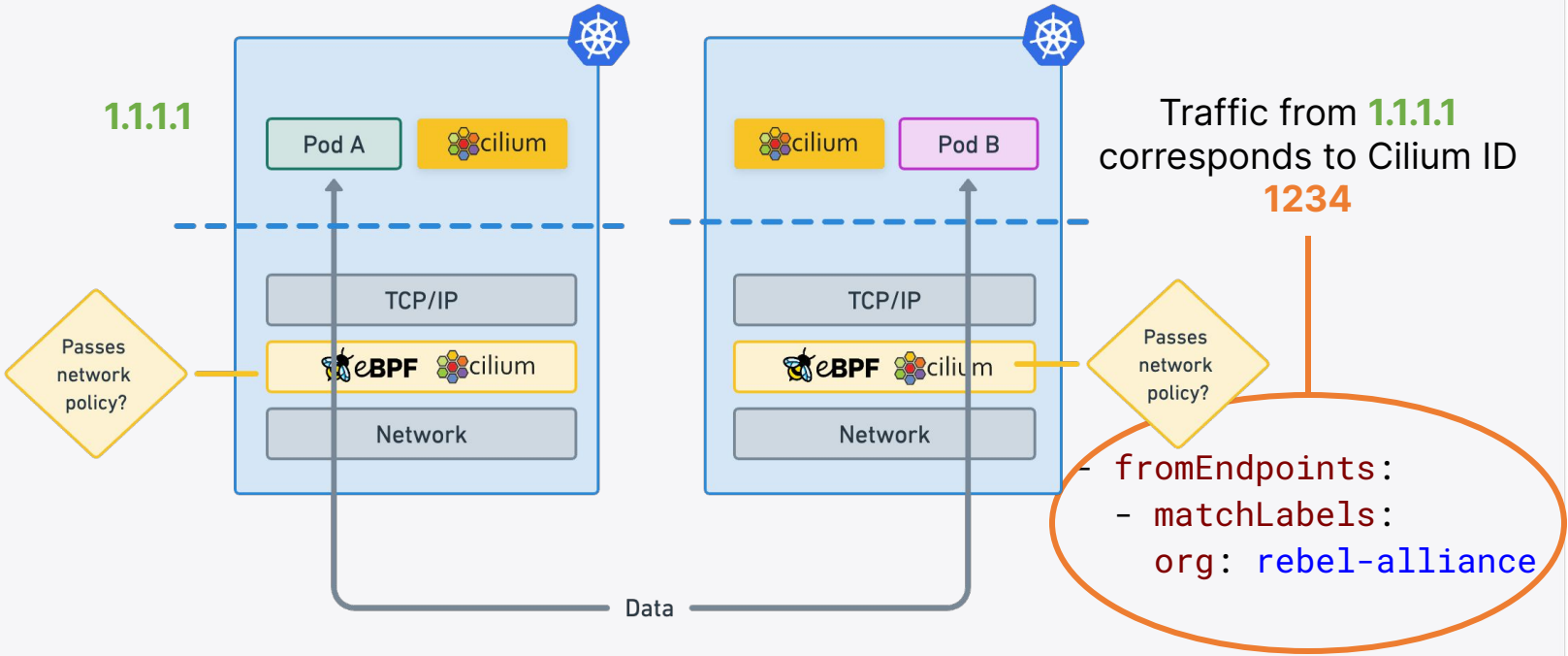
```
kubectl get ciliumidentities --show-labels

NAME  NAMESPACE    AGE    LABELS
2252  farfaraway   2d19h  app=r2-d2,class=droid,io.cilium.k8s.policy.cluster=default,
                          io.cilium.k8s.policy.serviceaccount=default,
                          io.kubernetes.pod.namespace=farfaraway,org=rebel-alliance

32496 farfaraway   2d23h  app.kubernetes.io/name=tiefighter,class=tiefighter,
                          io.cilium.k8s.policy.cluster=default,
                          io.cilium.k8s.policy.serviceaccount=default,
                          io.kubernetes.pod.namespace=farfaraway,org=empire

60812 farfaraway   2d19h  app.kubernetes.io/name=c-3po,
                          class=droid,io.cilium.k8s.policy.cluster=default,
                          io.cilium.k8s.policy.serviceaccount=default,
                          io.kubernetes.pod.namespace=farfaraway,org=rebel-alliance
```

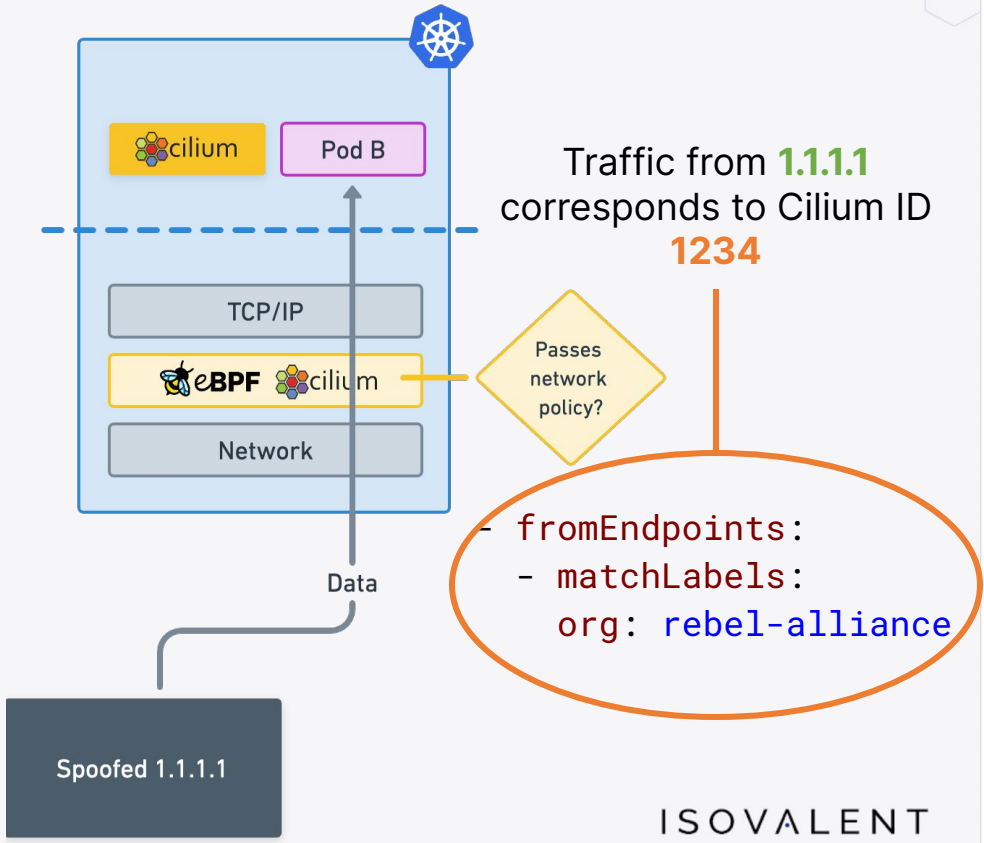
Is this traffic allowed?



Rebel alliance?

Photo by Josh Tere on Unsplash

Identity / address spoofing



ISOVALENT

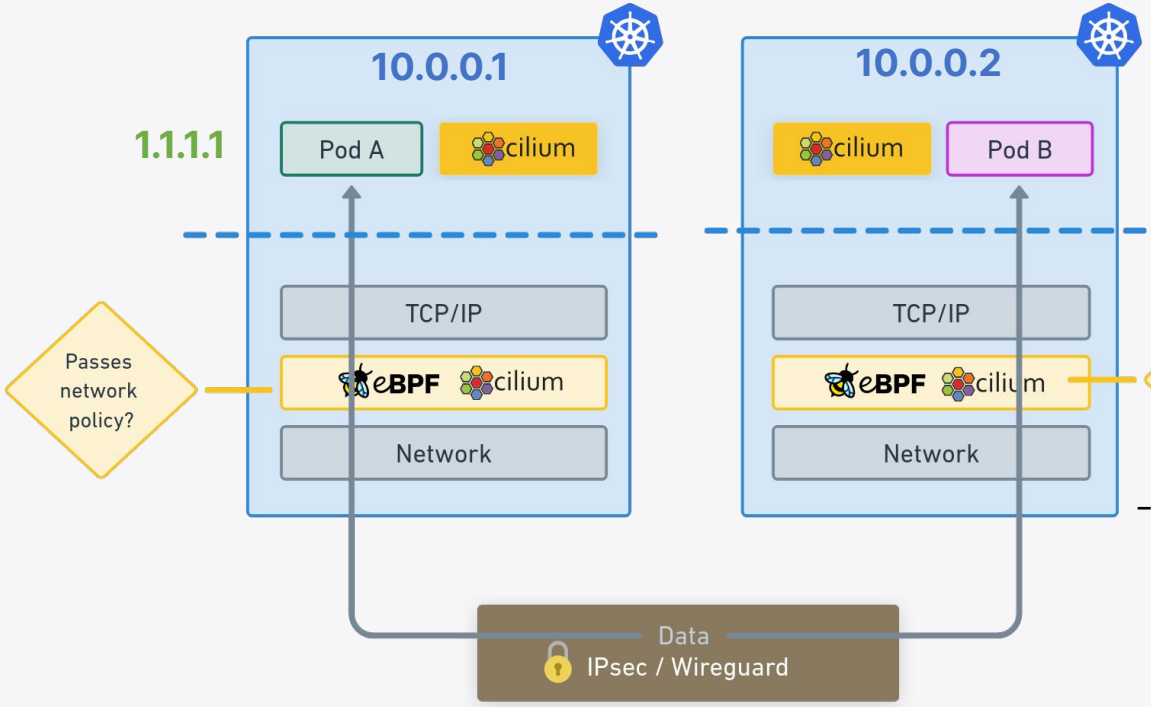
Let’s come back to Network Policy

@lizrice

Network policy restricts traffic

```
apiVersion: "cilium.io/v2"
kind: CiliumNetworkPolicy
metadata:
  name: "droid"
  namespace: farfaraway
spec:
  description: "Droid communication policy"
  endpointSelector:
    matchLabels:
      class: droid
    ingress:
    - fromEndpoints:
      - matchLabels:
        org: rebel-alliance
      authentication:
        mode: "required"
```

Is this traffic authenticated?

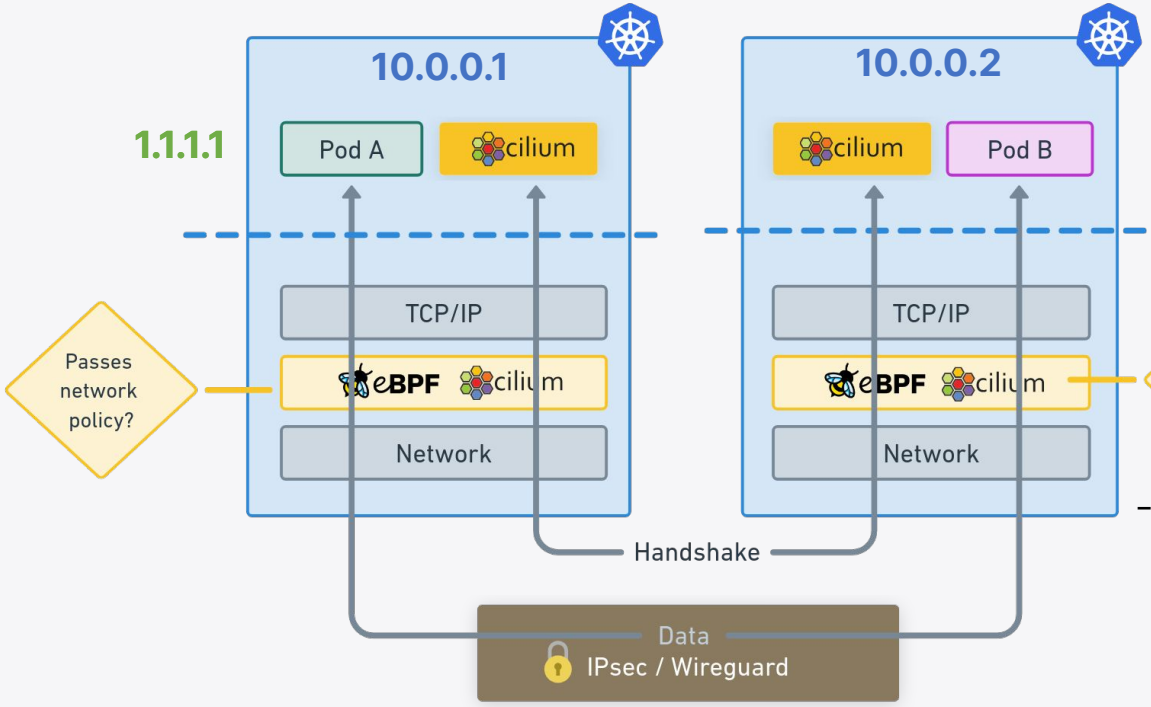


Traffic from 1.1.1.1 corresponds to Cilium ID 1234

1.1.1.1 should be on Node 10.0.0.1

```
- fromEndpoints:
  - matchLabels:
    org: rebel-alliance
  authentication:
    mode: "required"
```

Is this traffic authenticated?

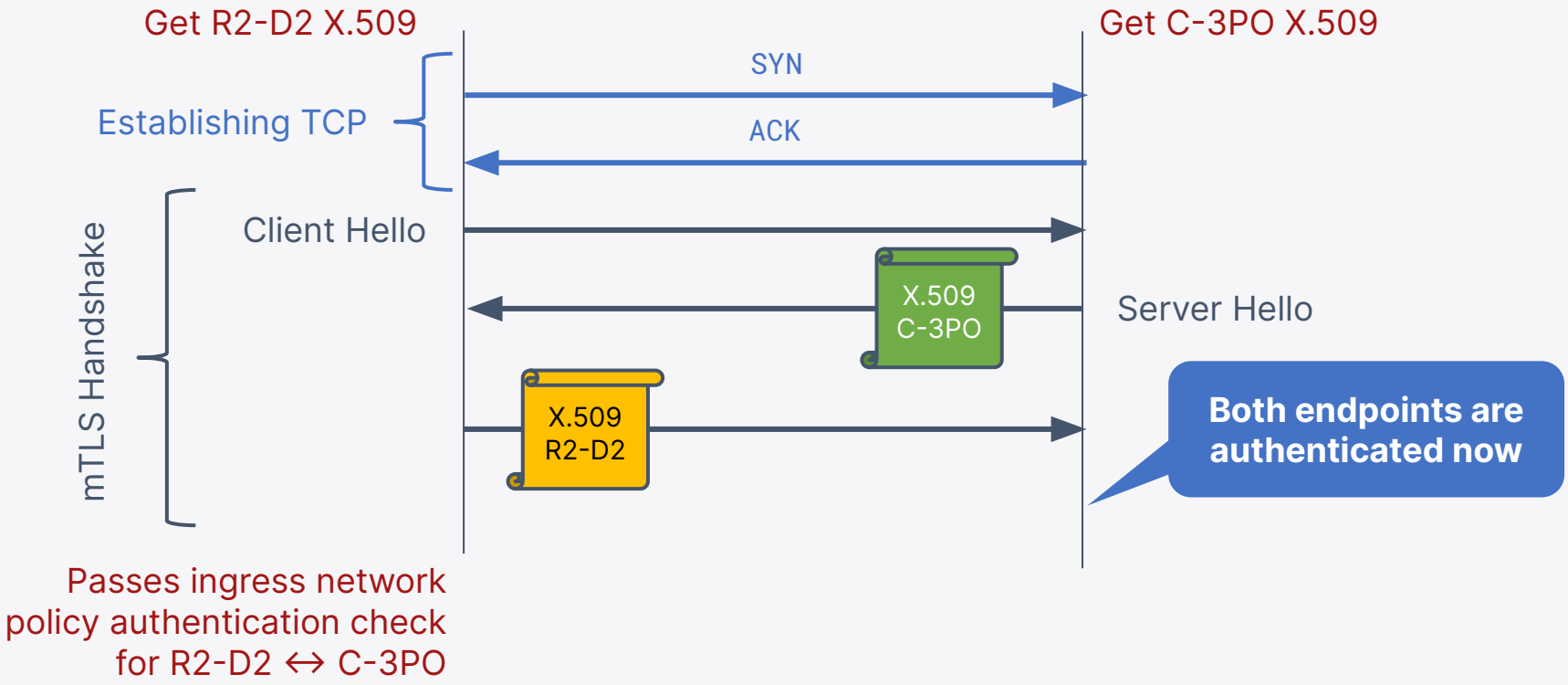


Traffic from 1.1.1.1 corresponds to Cilium ID 1234

1.1.1.1 should be on Node 10.0.0.1

```
- fromEndpoints:
  - matchLabels:
    org: rebel-alliance
authentication:
  mode: "required"
```

Cilium agents use same handshake as mTLS



ISOVALENT

Cilium + SPIRE - transparent certificate mangement

@lizrice

Transparent certificate management

Cilium Operator registers each identity with SPIRE

```
kubectl exec -n cilium-spire spire-server-0 -c spire-server --
/opt/spire/bin/spire-server entry show -selector cilium:mutual-auth
Found 10 entries
Entry ID         : 8e1cc610-69b0-474d-aa89-32fc2003fe81
SPIFFE ID        : spiffe://spiffe.cilium/identity/2252
Parent ID        : spiffe://spiffe.cilium/cilium-operator
Revision         : 0
X509-SVID TTL    : default
JWT-SVID TTL     : default
Selector         : cilium:mutual-auth
…
```

Authenticated connection

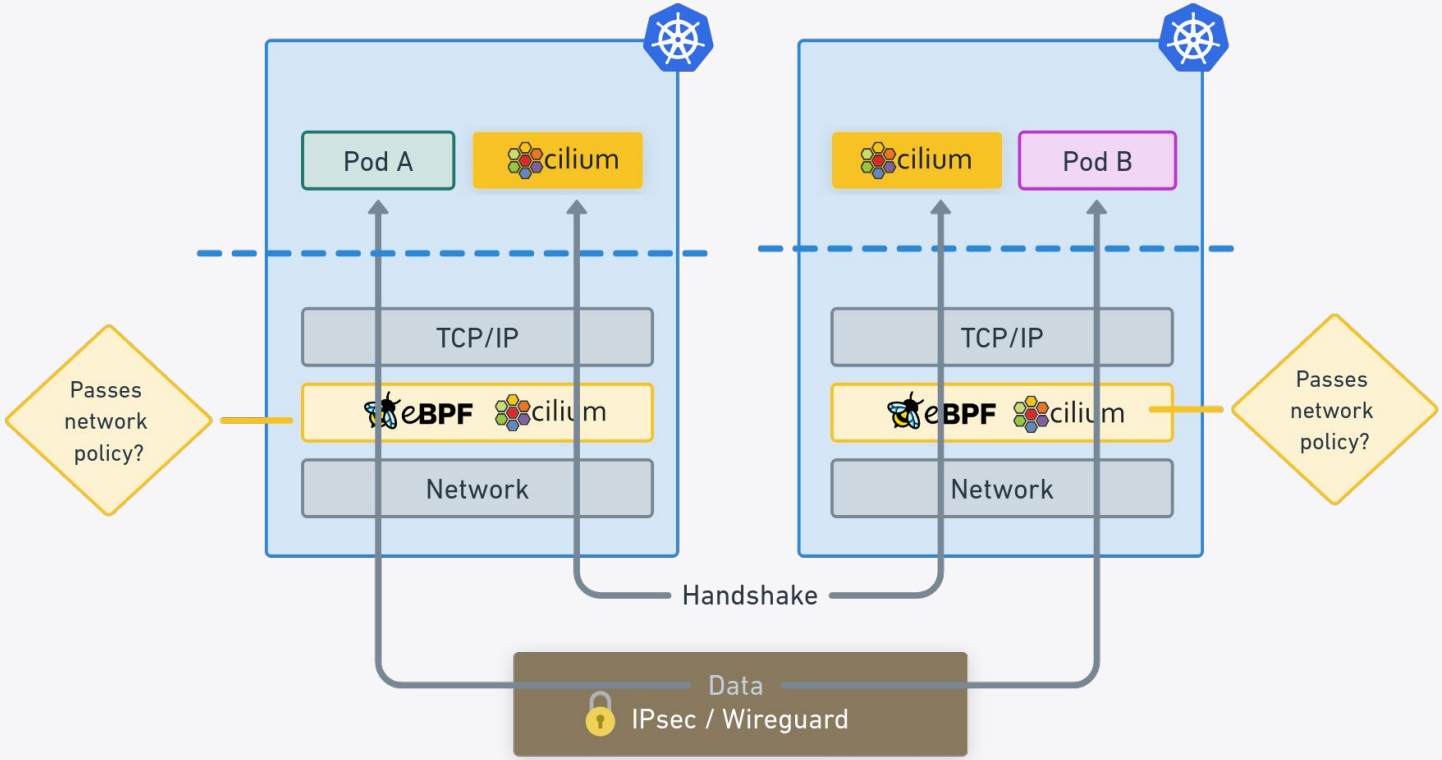
```
Nov  7 13:54:13.518: farfaraway/c-3po:44494 (ID:52452) ->
farfaraway/r2-d2:80 (ID:18777) policy-verdict:L3-Only INGRESS ALLOWED
(TCP Flags: SYN; Auth: SPIRE)
```

ISOVALENT

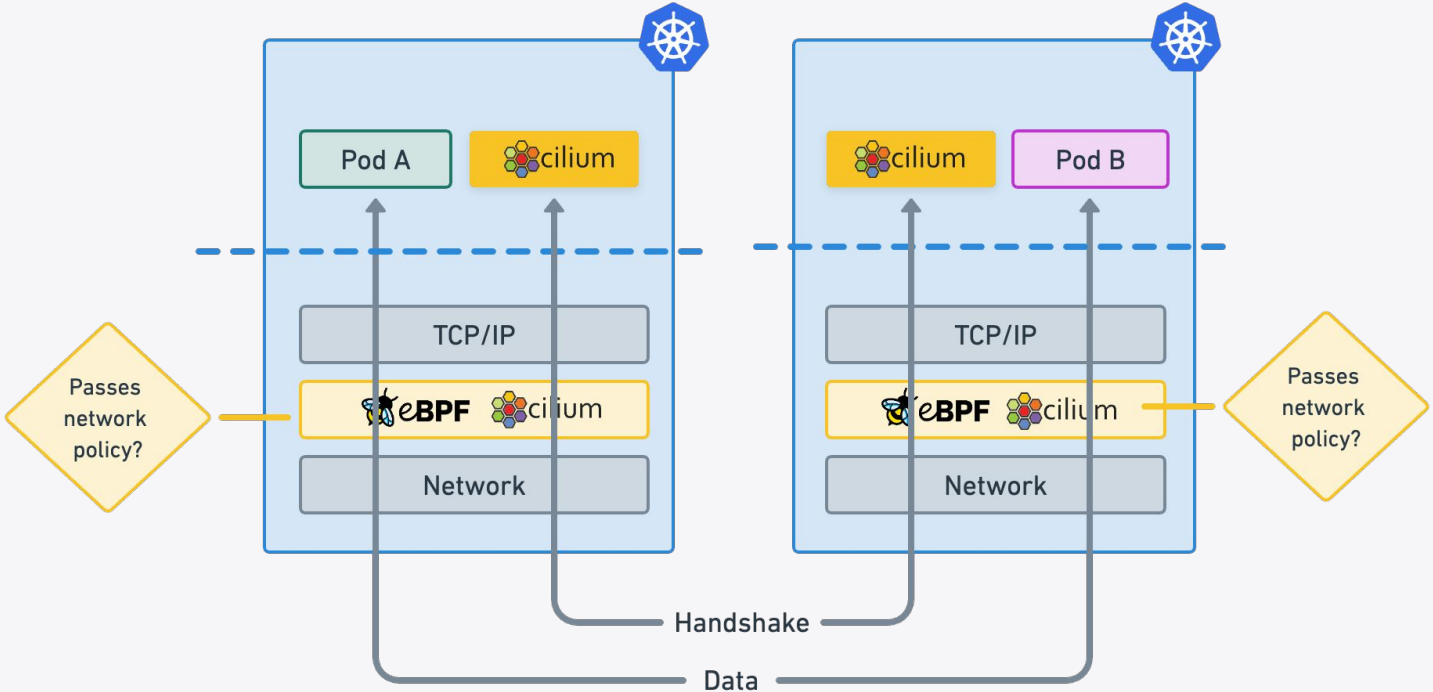
Cilium next-gen mutual authentication

@lizrice

After handshake, the traffic doesn't have to be TCP



Authenticated connections don’t have to be encrypted



ISOVALENT

@lizrice

ISOVALENT

Thank you

cilium/cilium

@ciliumproject

cilium.io