

CNI or Service Mesh? Comparing Security Policies Across Providers

Christine Kim - Isovalent
@xtineskim



Rob Salmond - SuperOrbital
mastodon.social/@rsalmond



What we'll cover . . .

- What's a CNI? What's a Service Mesh?
- The What and How of Policy Enforcement
- Security Gotchas
- Mitigation and How the Field is Evolving
- What You Can Do



cilium



Istio



cilium



Istio

Top Ten CNCF Projects by:



cilium



Istio

Top Ten CNCF Projects by: commits



cilium



Istio

Top Ten CNCF Projects by: contributors



cilium



Istio

Top Ten CNCF Projects by: comments



cilium



Top Ten CNCF Projects by: issues



cilium

The screenshot shows a web browser window with the URL isovalent.com. The page title is "ISOVALENT". The main content features the heading "Cilium Service Mesh – Everything You Need to Know" and the date "Jul 20, 2022". Below the heading is a "Cilium" tag and the Cilium logo at the bottom.

Cilium Service Mesh – Everything You Need to Know

Jul 20, 2022 Cilium

 cilium
Service Mesh

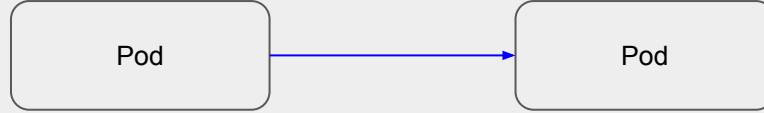


The screenshot shows a web browser window with the URL istio.io. The page title is "Istio". The main content features the heading "Introducing Ambient Mesh" and the text "A new dataplane mode for Istio without sidecars.". At the bottom, there is copyright information: "Sep 7, 2022 | By John Howard - Google, Ethan J. Jackson - Google, Yuval Kohavi - Solo.io, Idit Levine - Solo.io, Justin Pettit - Google, Lin Sun - Solo.io".

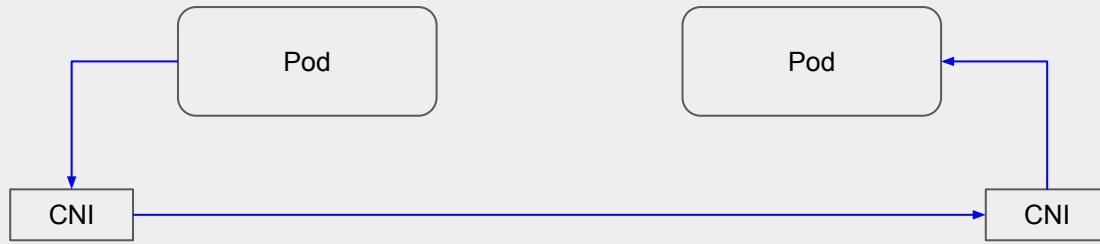
Introducing Ambient Mesh

A new dataplane mode for Istio without sidecars.

Sep 7, 2022 | By John Howard - Google, Ethan J. Jackson - Google, Yuval Kohavi - Solo.io, Idit Levine - Solo.io, Justin Pettit - Google, Lin Sun - Solo.io

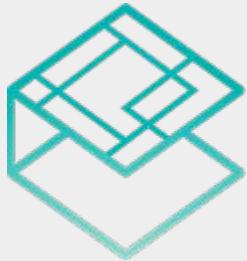


“pods can communicate with all other pods on any other node without NAT”



→ data

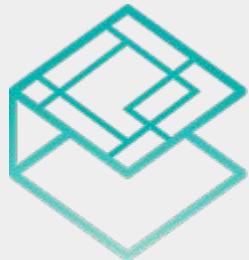
What is CNI?



C N I

Container
Network
Interface

What is CNI?



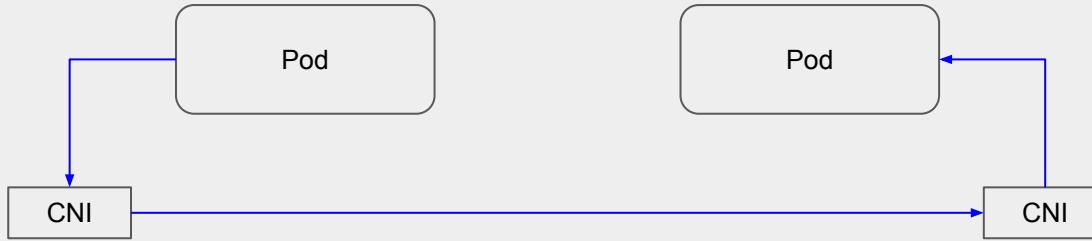
C N I

Container
Network
Interface

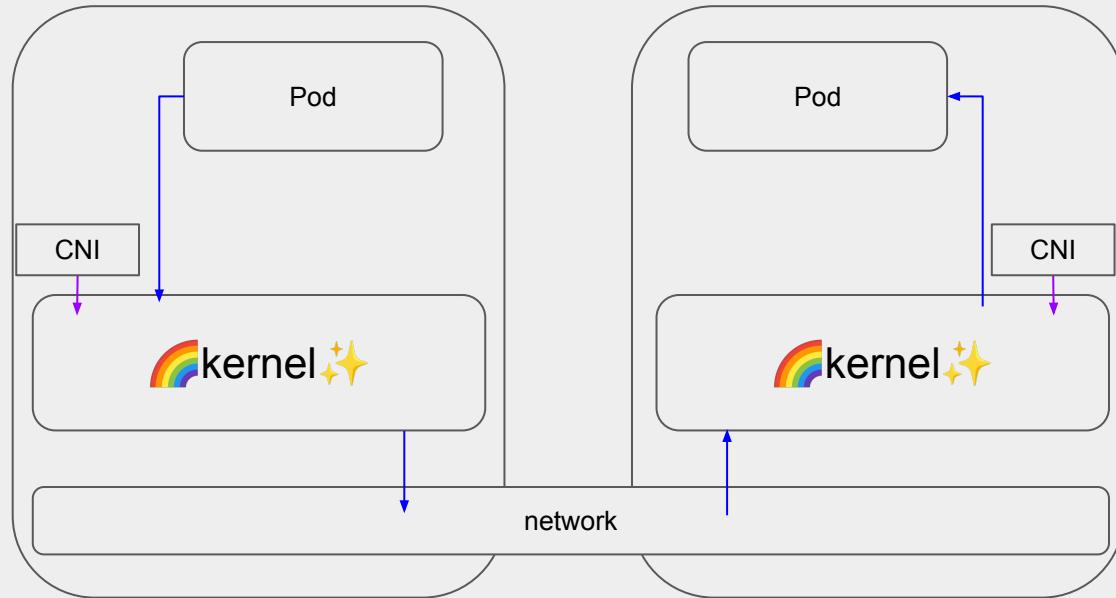
“A way to ask for changes to be made to a container’s network config.”

What kind of changes?

What kind of changes?

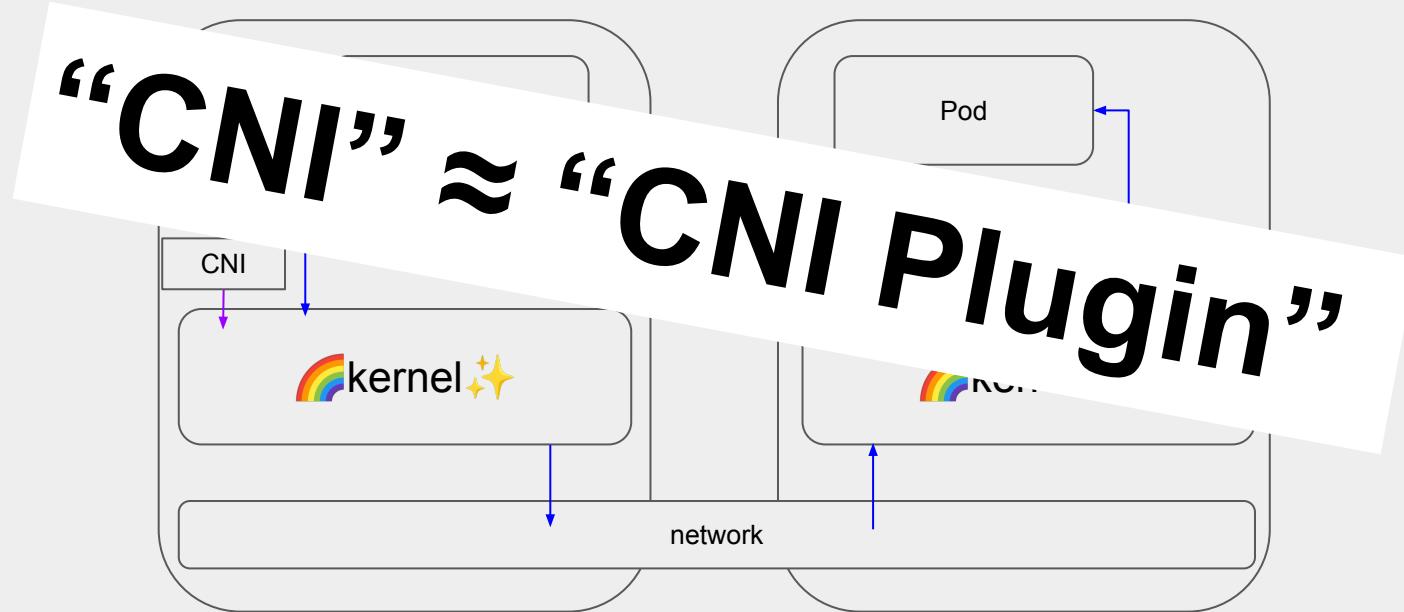


What kind of changes?



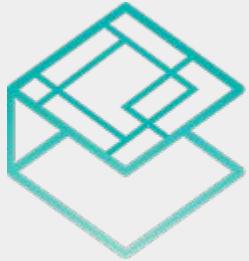
—→ control
—→ data

What kind of changes?

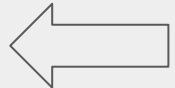


→ control
→ data

What is a CNI plugin?

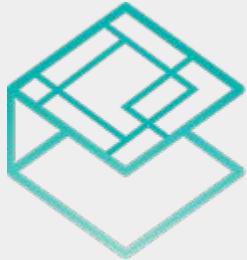


C N I

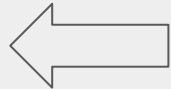


implements

What is a CNI plugin?



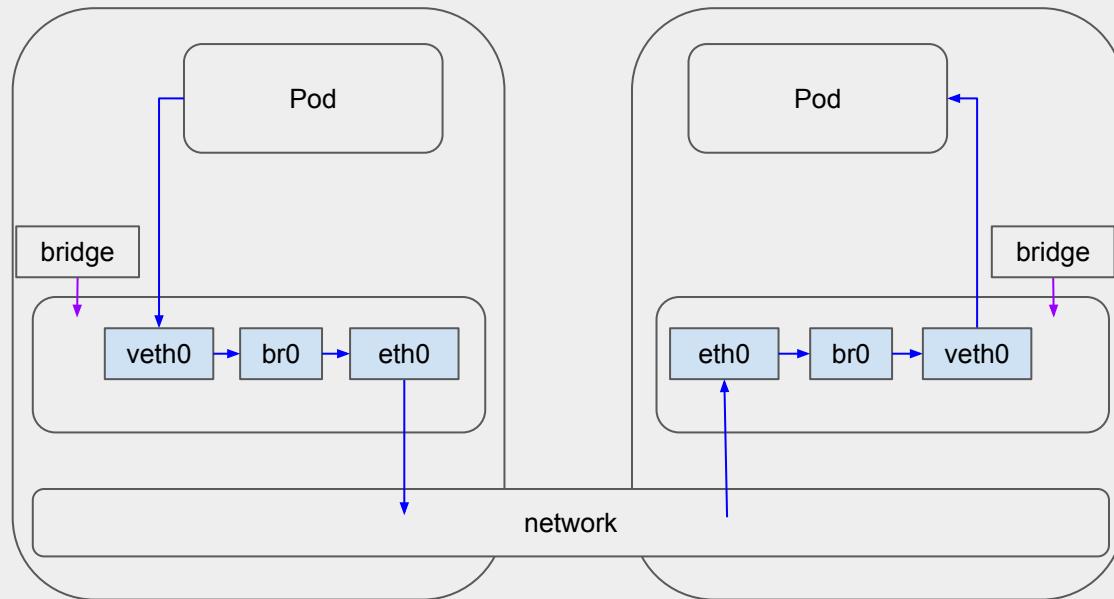
C N I



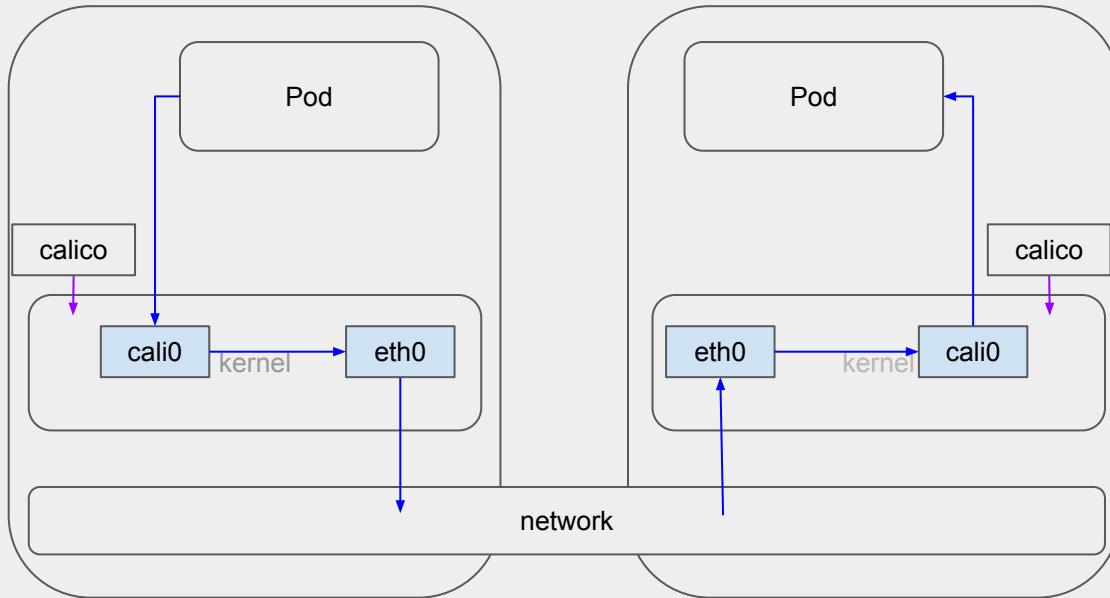
implements

“A thing that can make container networking changes.

bridge plugin

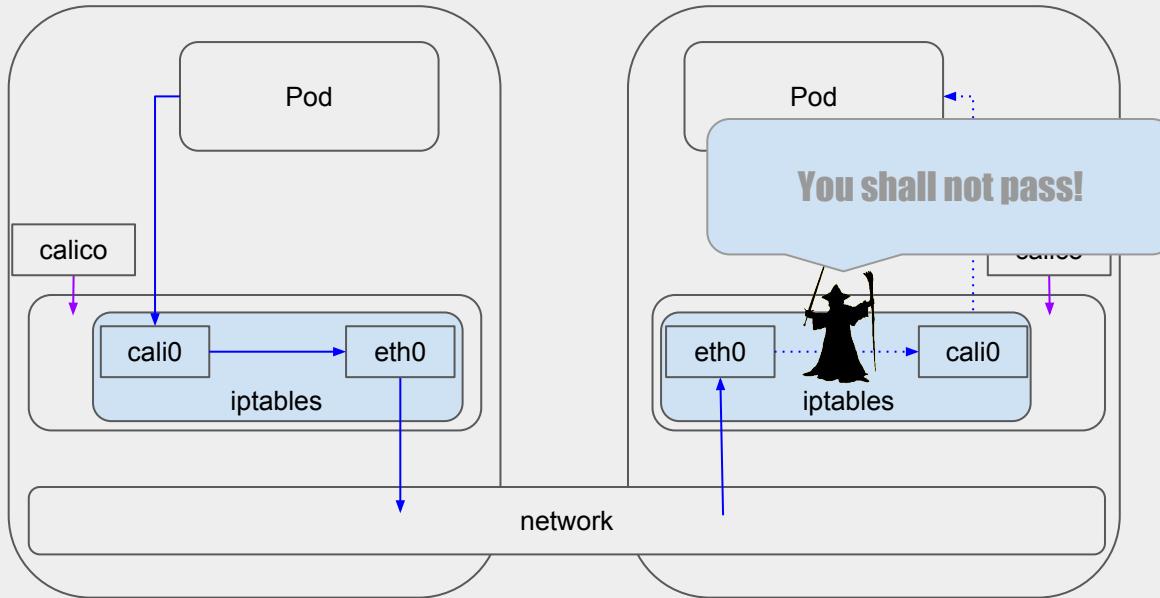


Calico plugin



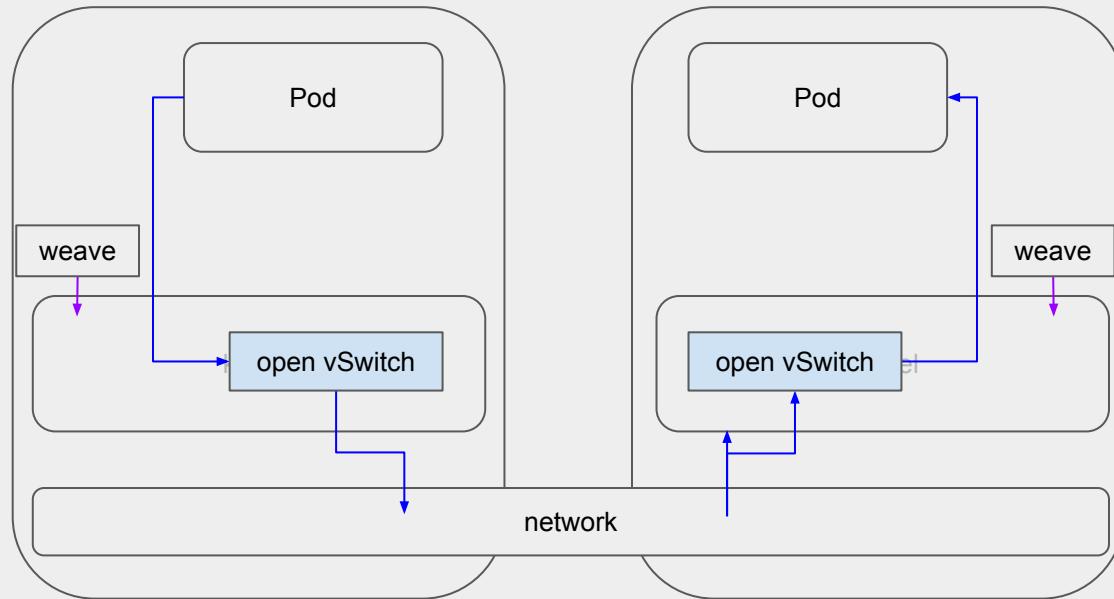
→ control
→ data

Calico plugin



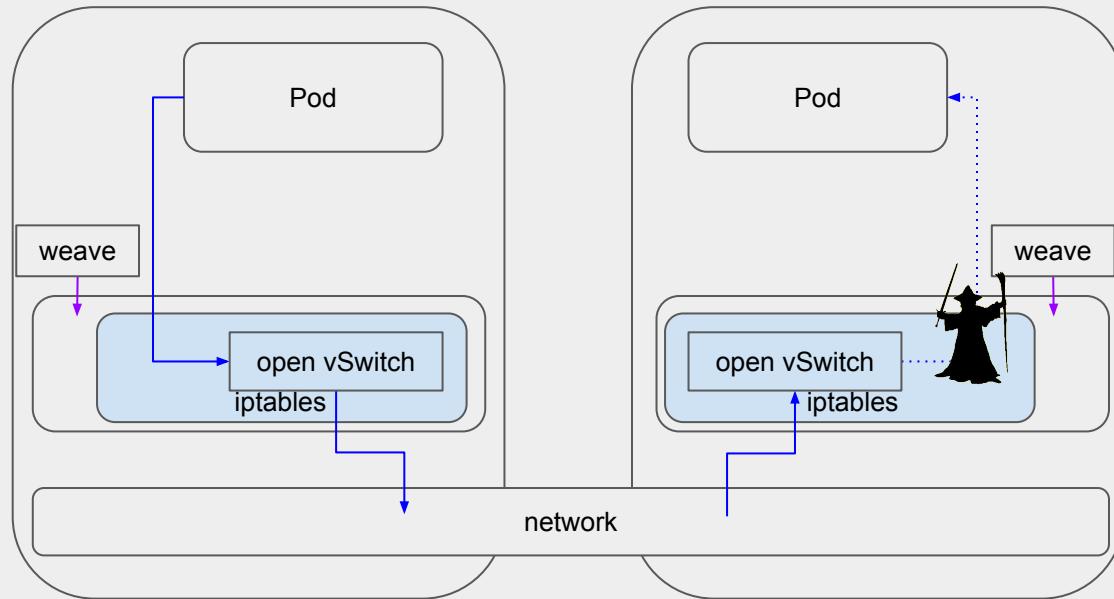
— control
— data

weave plugin



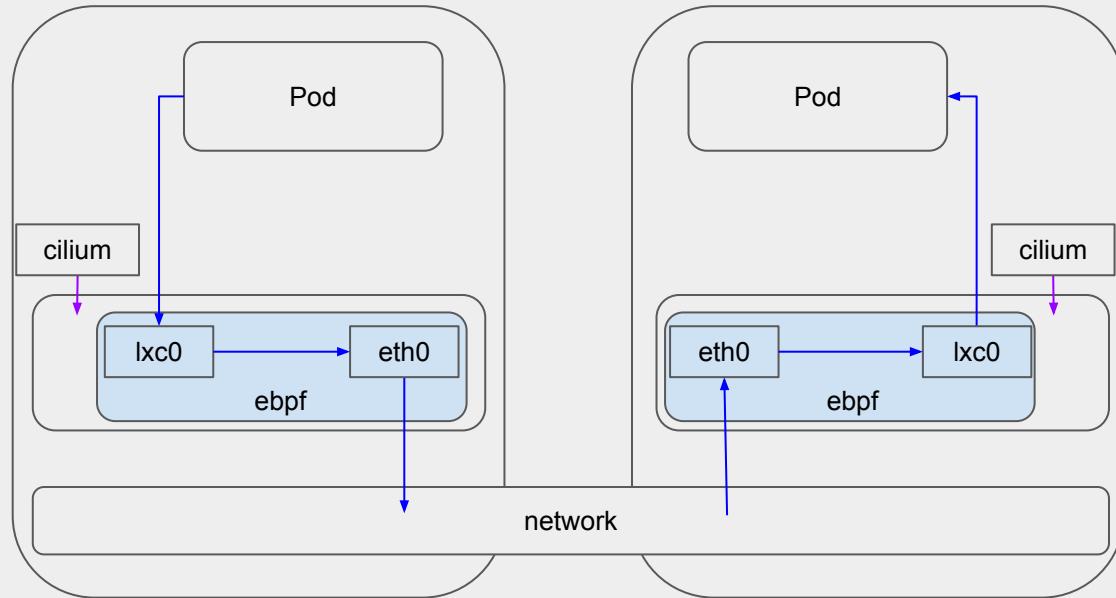
→ control
→ data

weave plugin



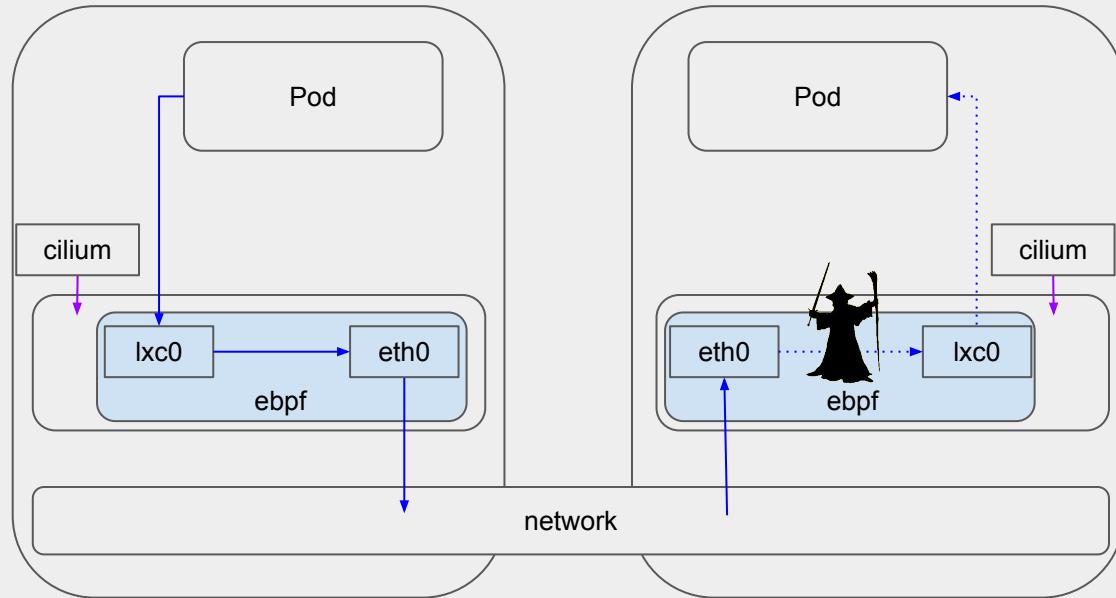
→ control
→ data

cilium plugin



→ control
→ data

cilium plugin



→ control
→ data

Most of the popular CNI Plugins:

Most of the popular CNI Plugins:

- Configure pod to pod networking

Most of the popular CNI Plugins:

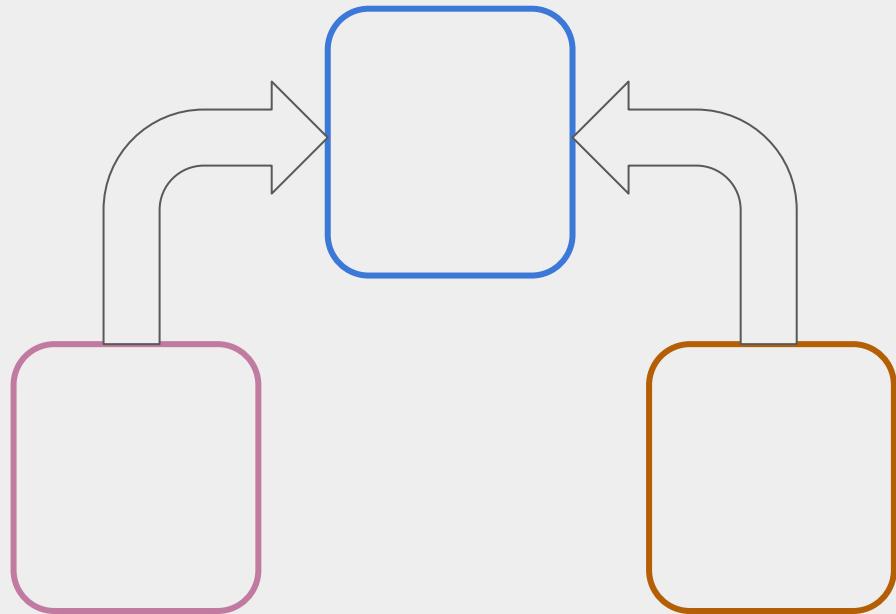
- Configure pod to pod networking
- Support NetworkPolicy enforcement

Most of the popular CNI Plugins:

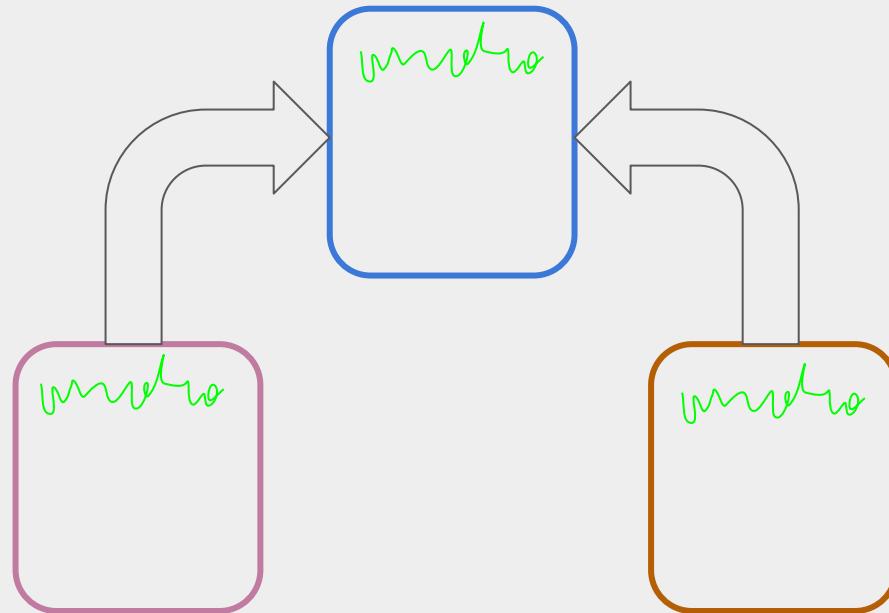
- Configure pod to pod networking
- Support NetworkPolicy enforcement
- ≈ Cloud Native software defined network

What is a Service Mesh?

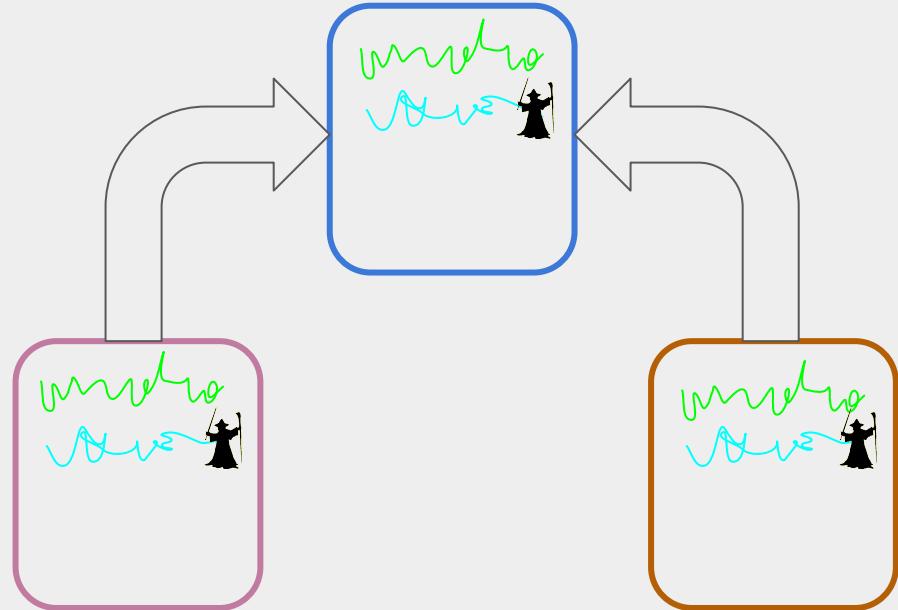
What is a Service Mesh?



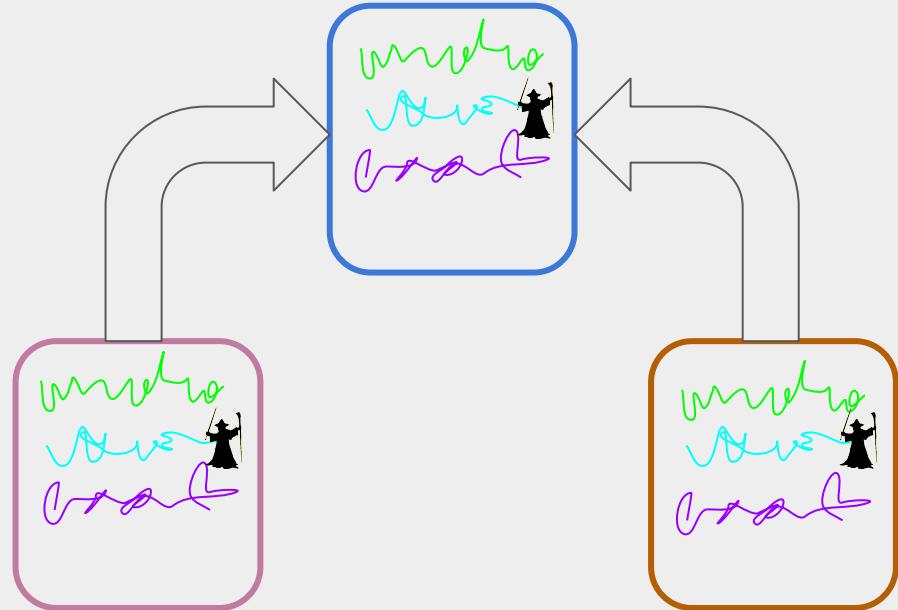
What is a Service Mesh?



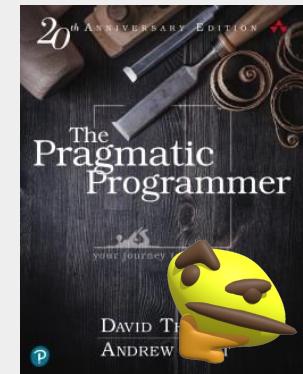
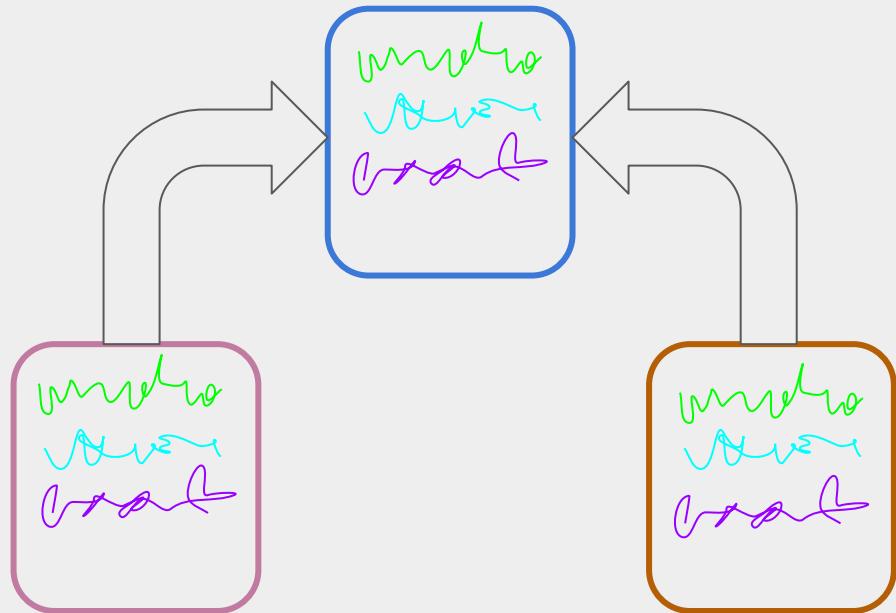
What is a Service Mesh?



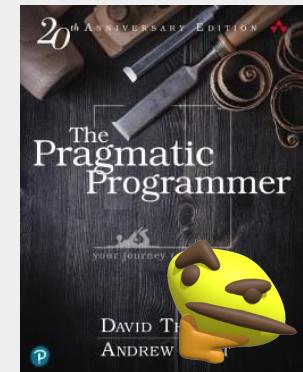
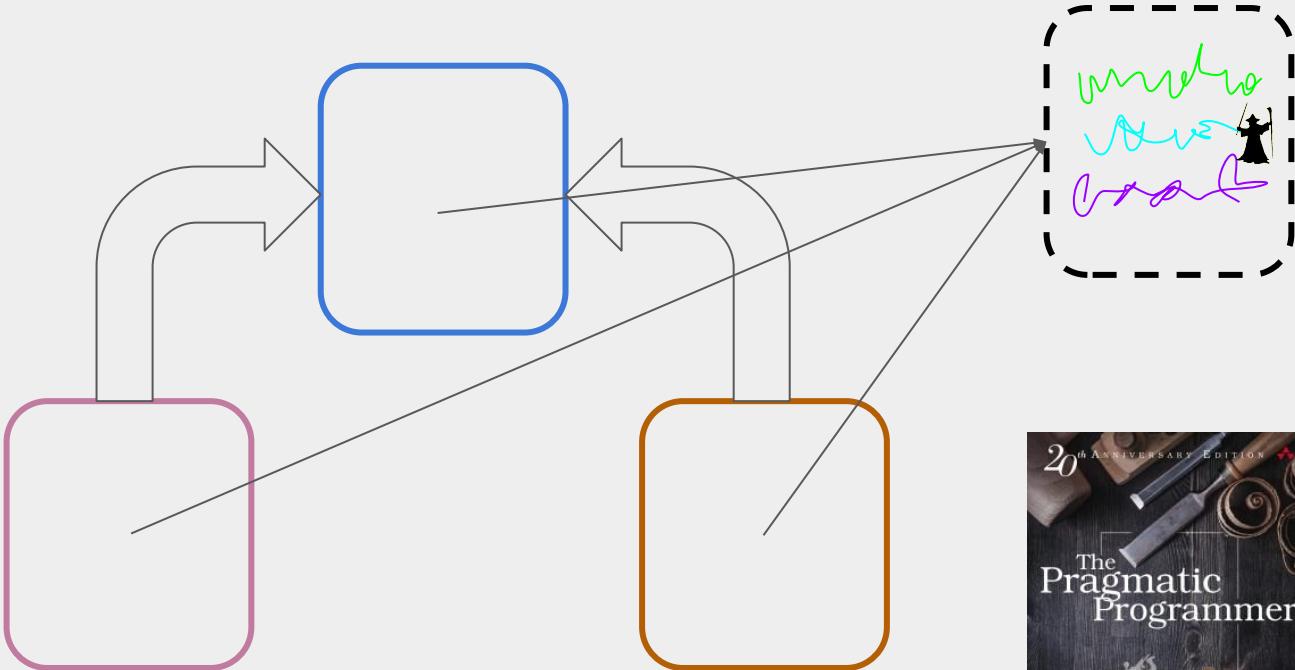
What is a Service Mesh?



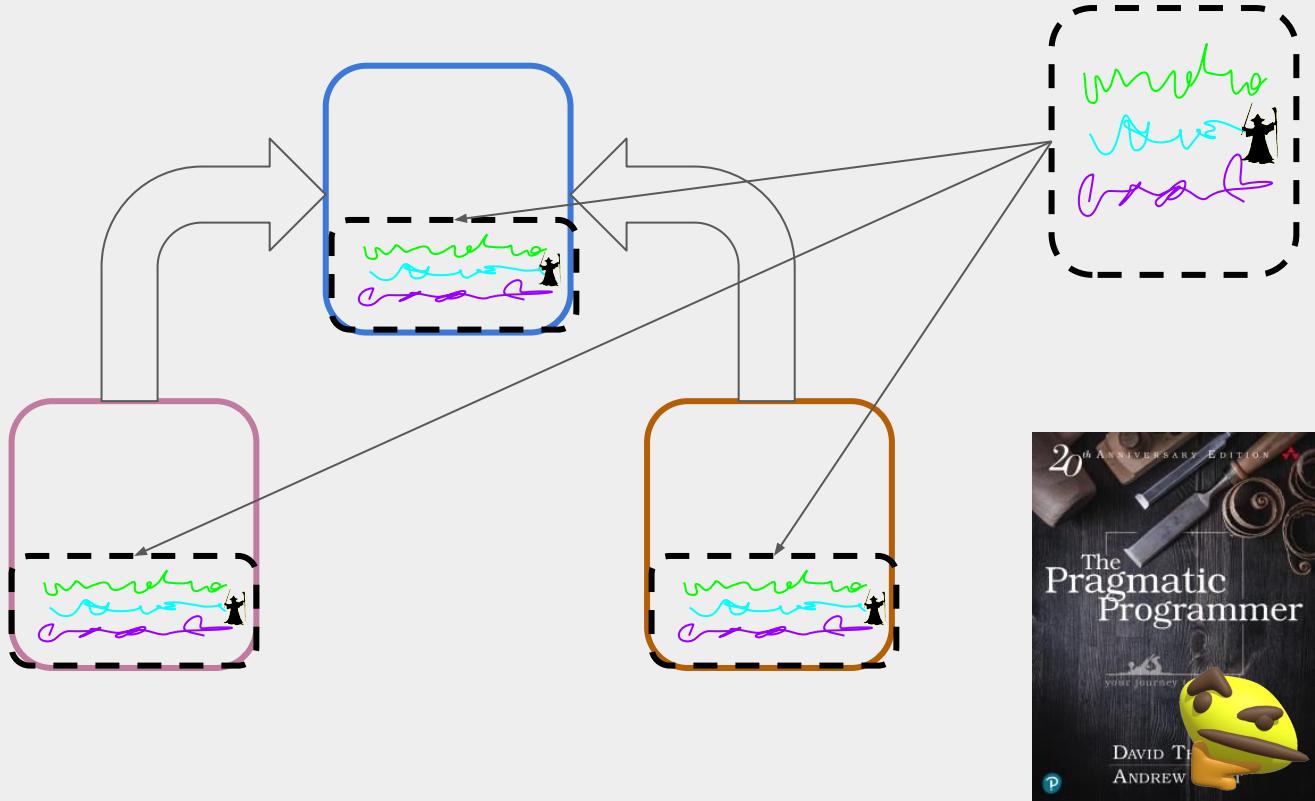
What is a Service Mesh?



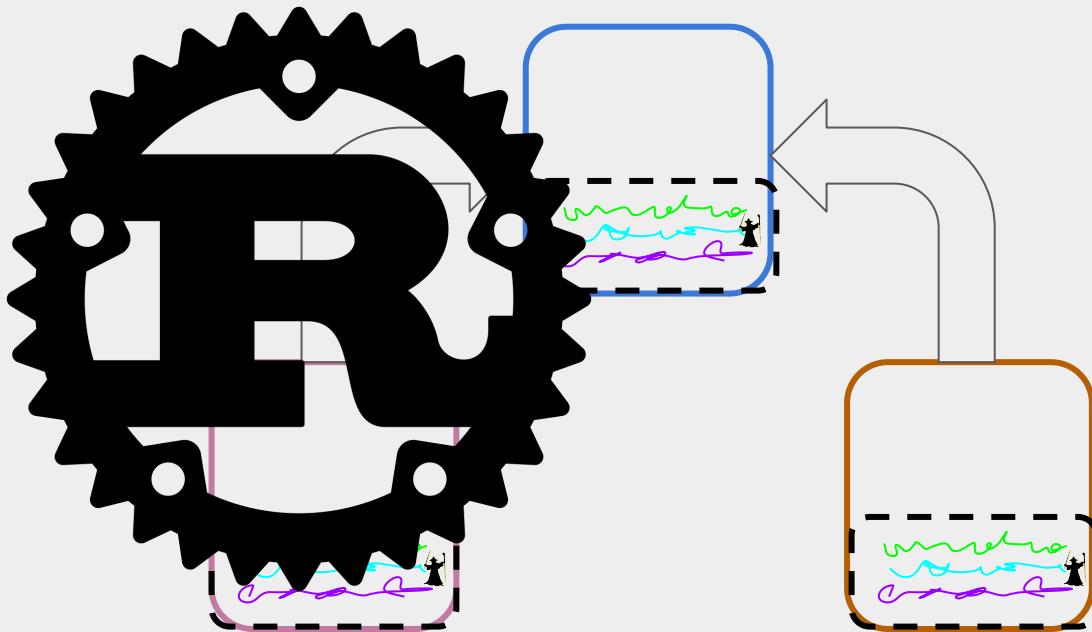
What is a Service Mesh?



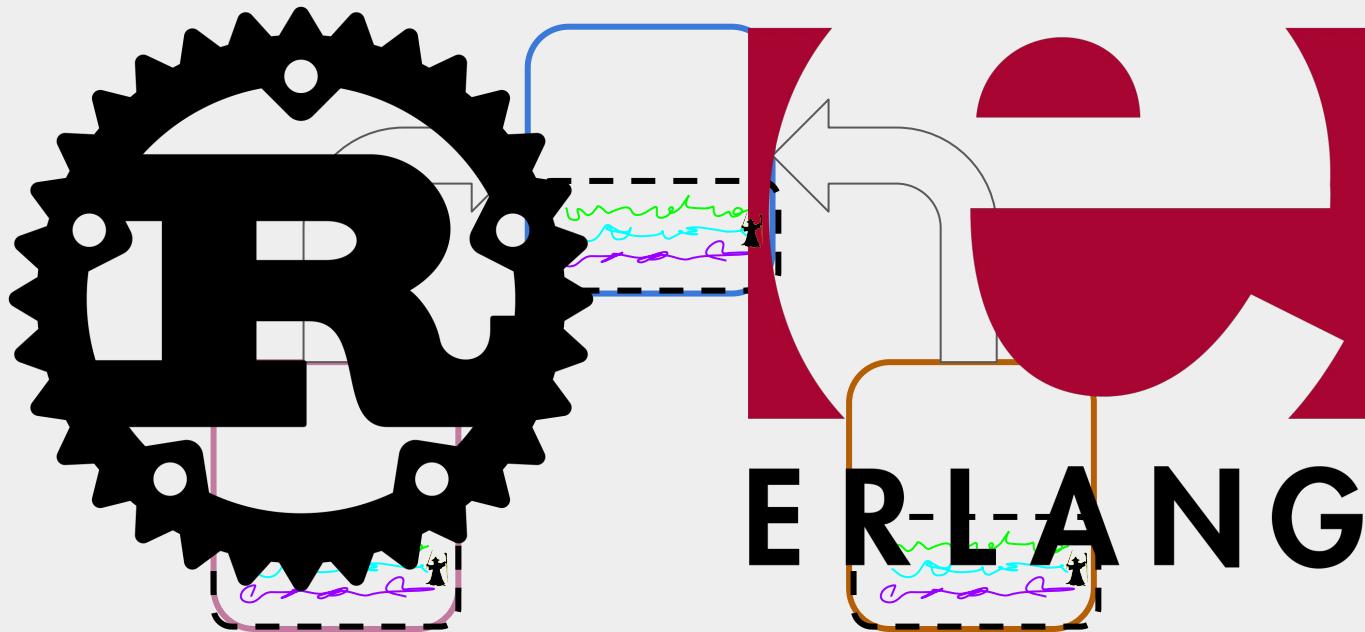
What is a Service Mesh?



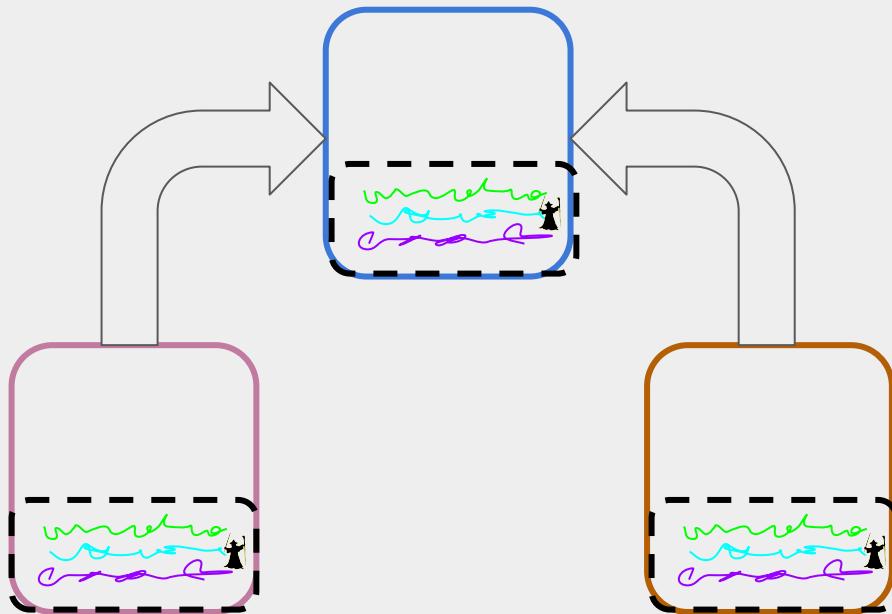
What is a Service Mesh?



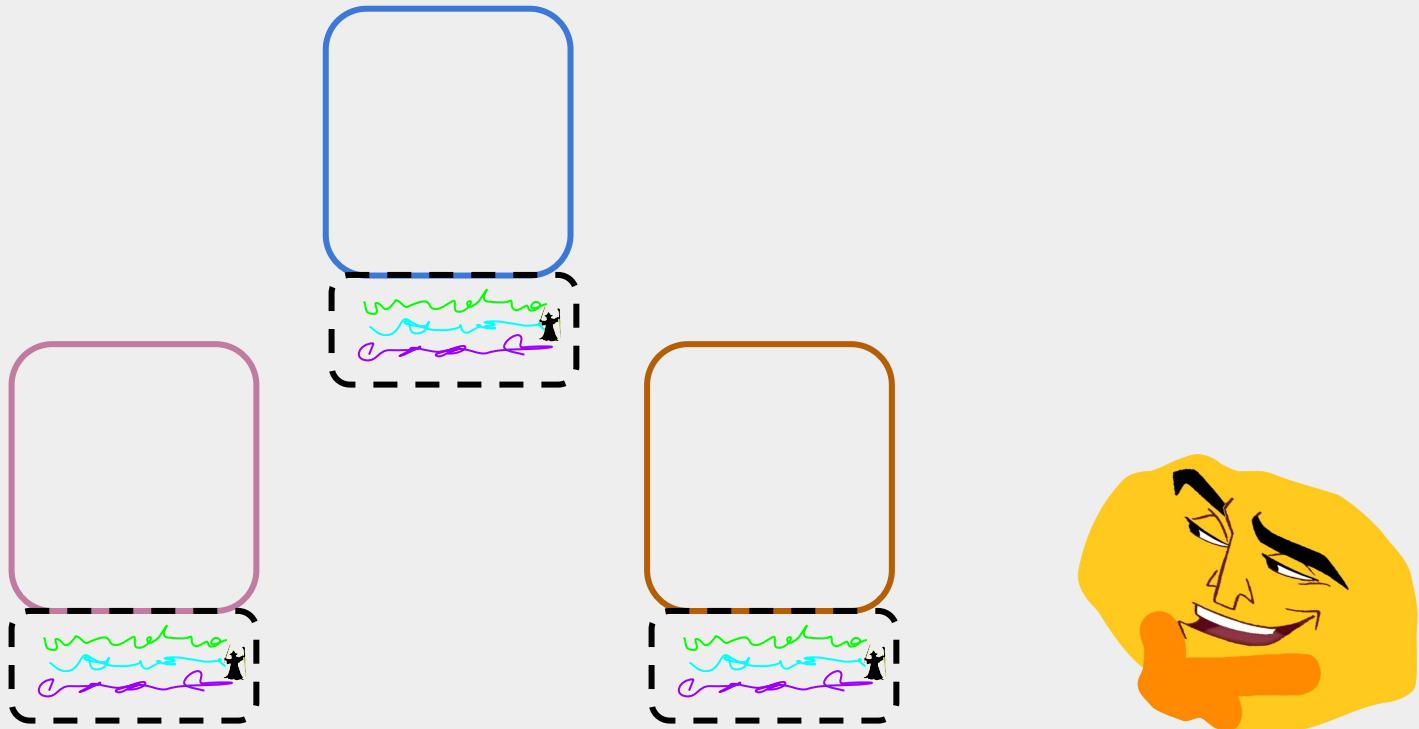
What is a Service Mesh?



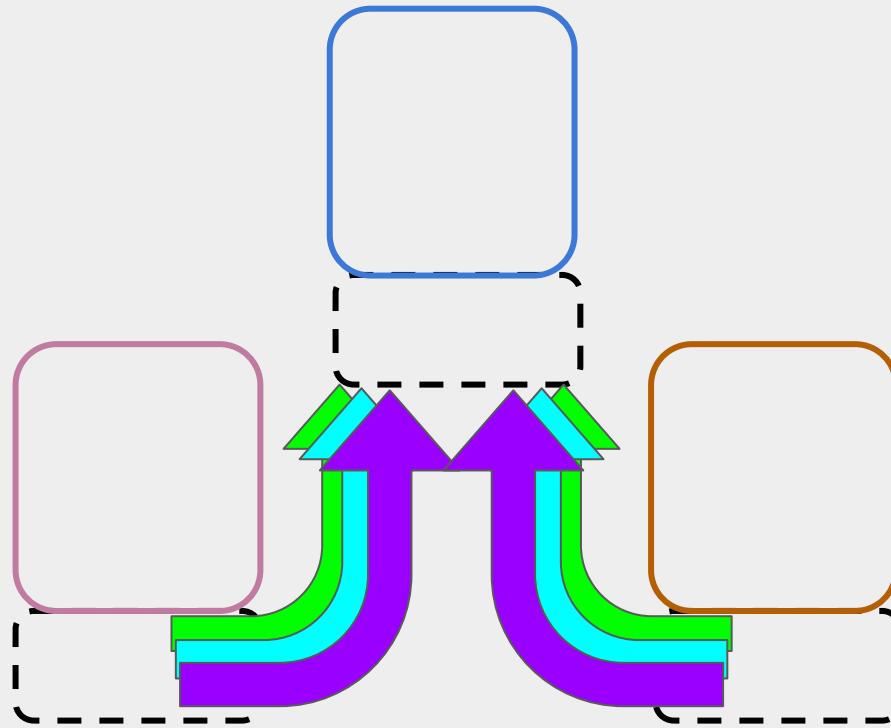
What is a Service Mesh?



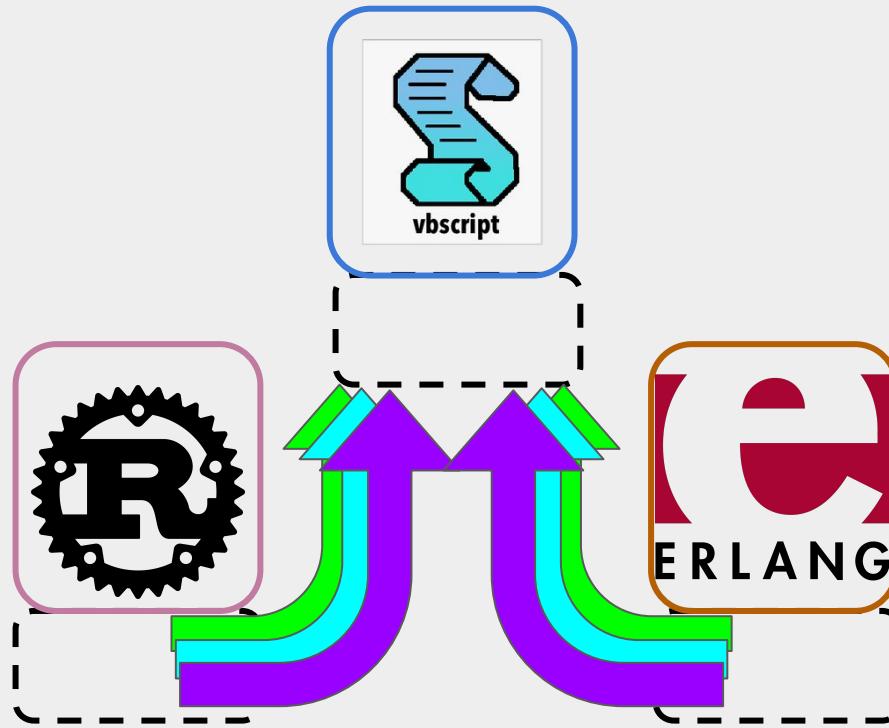
What is a Service Mesh?



What is a Service Mesh?



What is a Service Mesh?

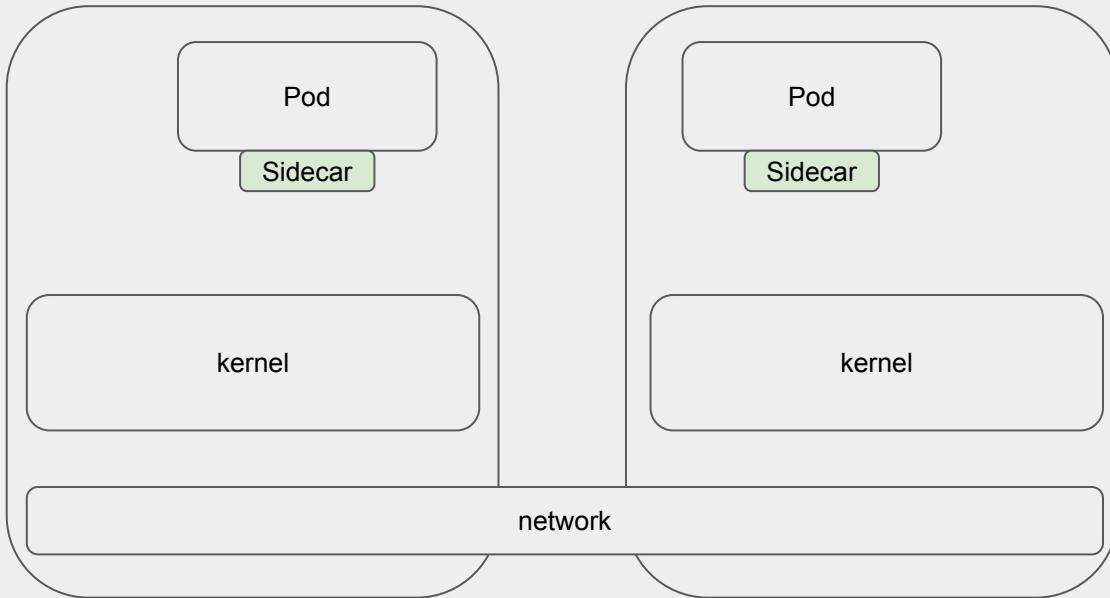


The most popular Meshes offer:

- Observability
- Identity
- Encryption
- Access Control
- Load Balancing

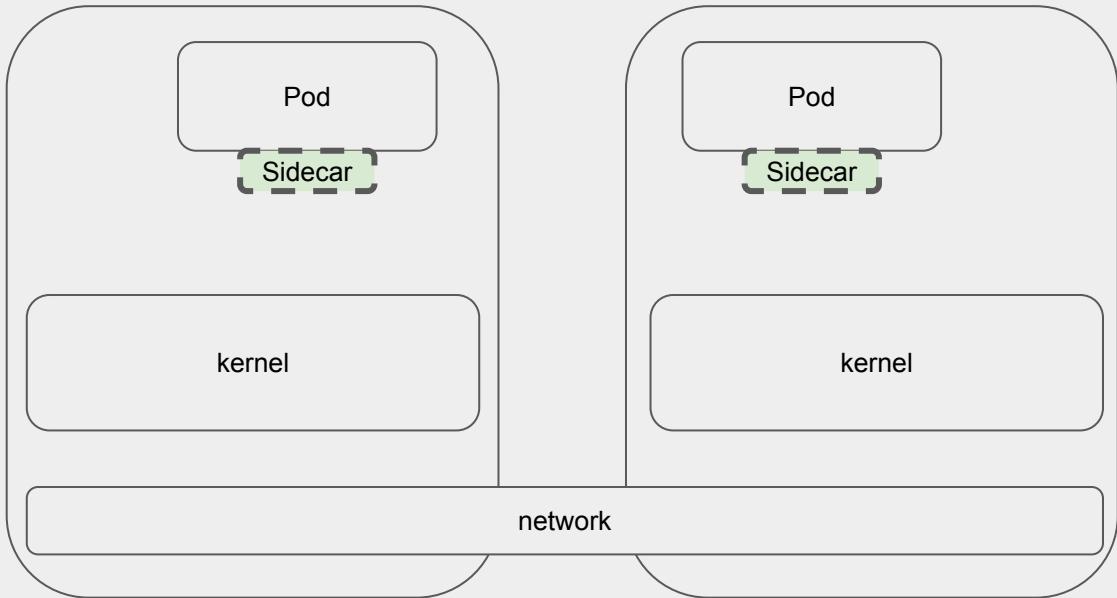


service mesh



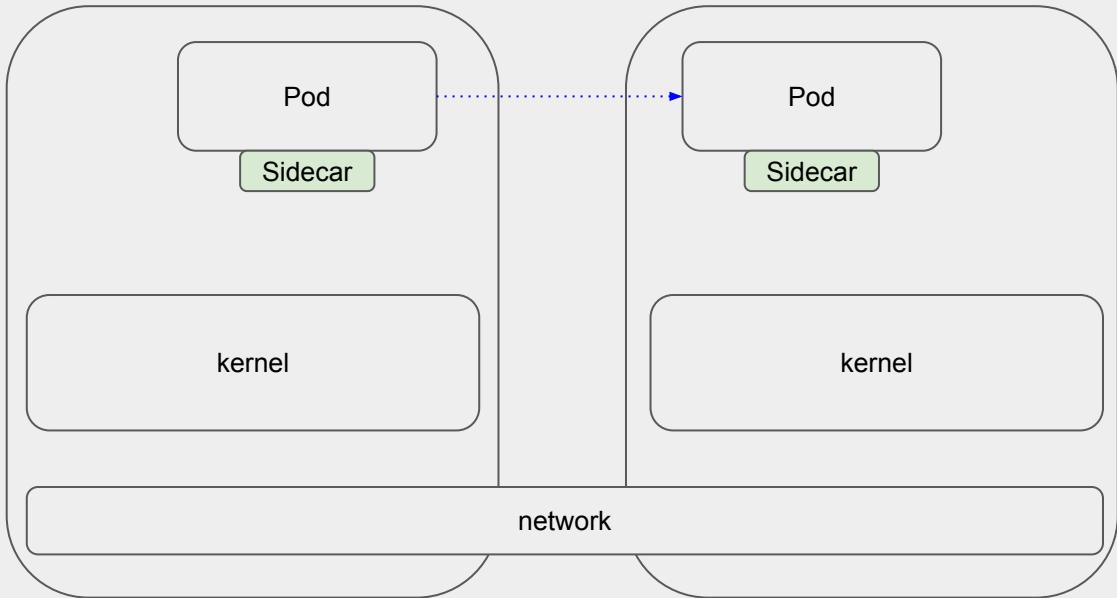
→ control
→ data

service mesh



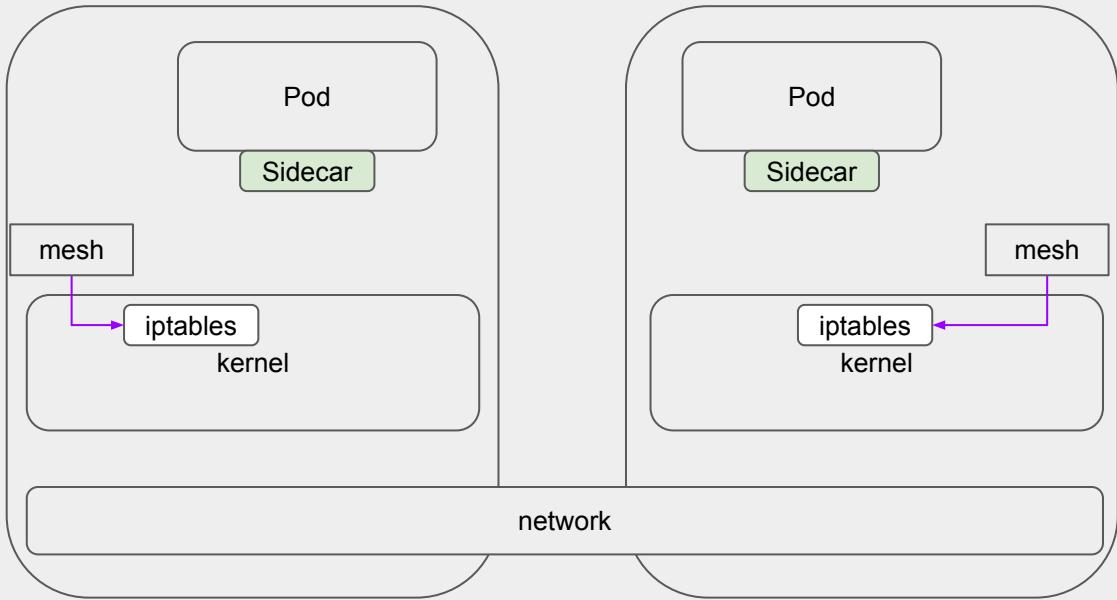
→ control
→ data

service mesh



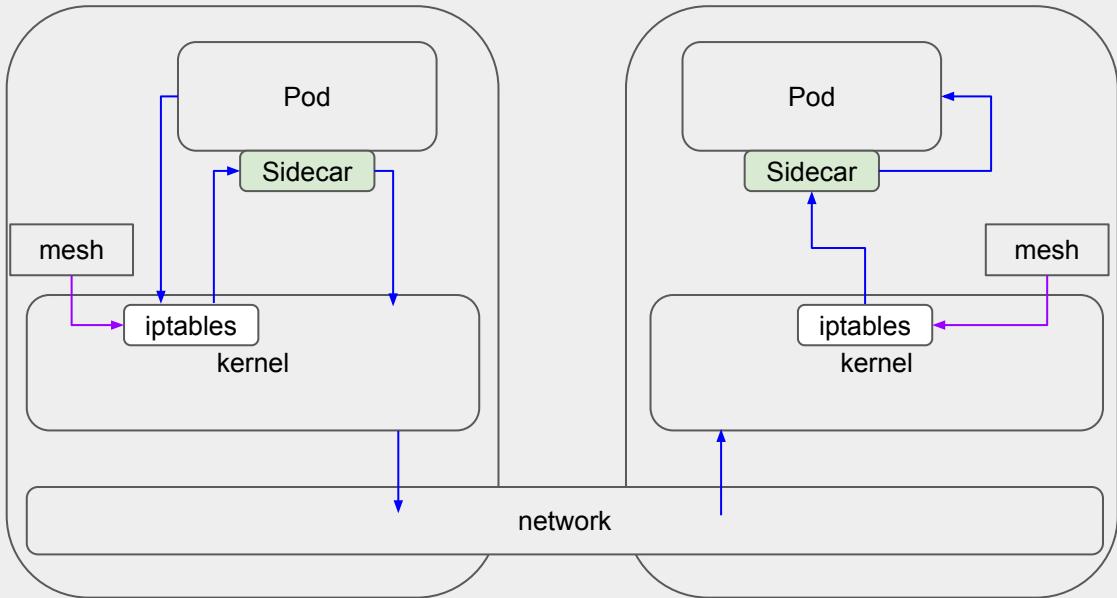
→ control
→ data

service mesh



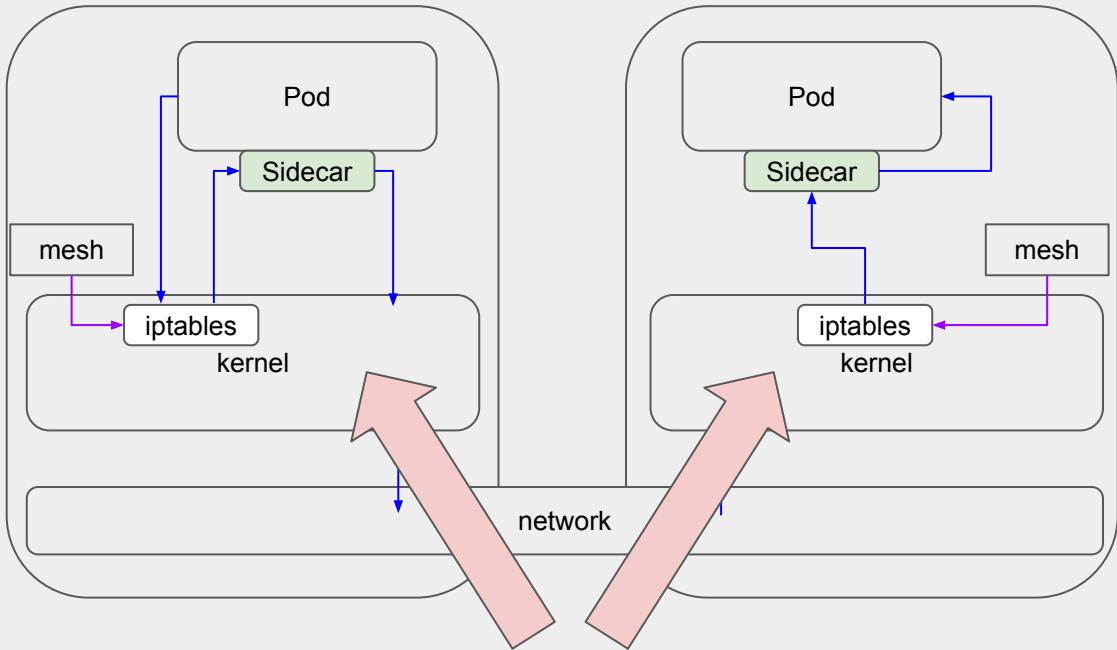
→ control
→ data

service mesh



— control
— data

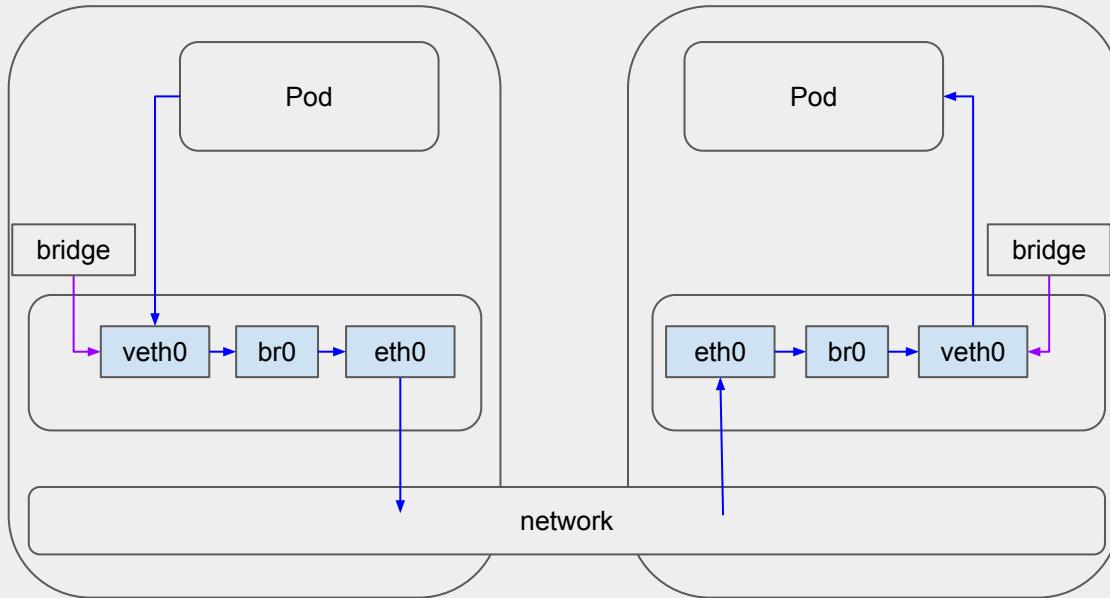
service mesh



No Interfaces?

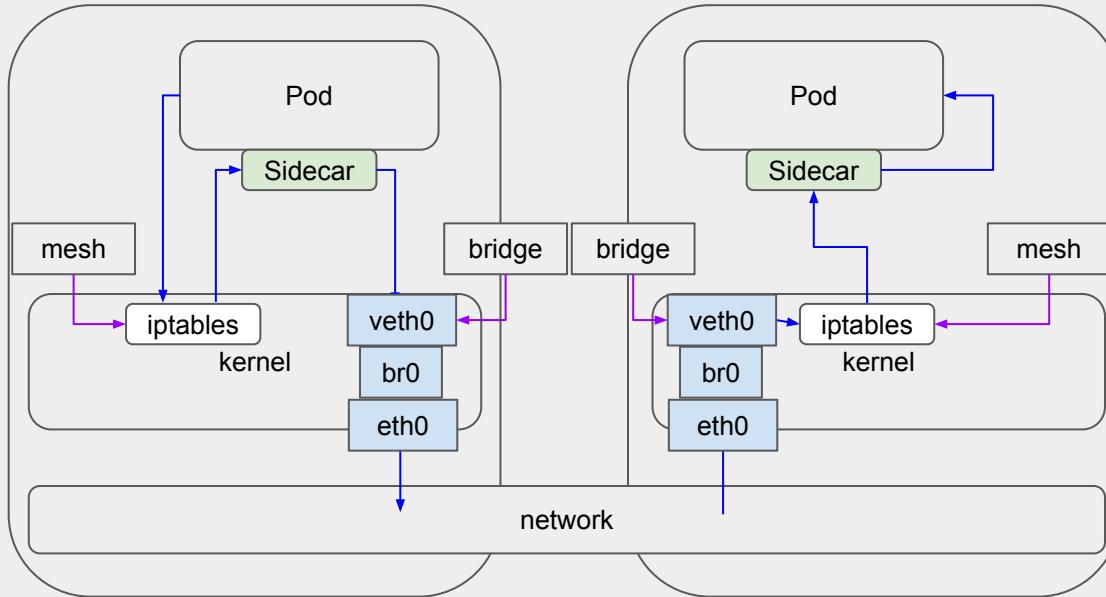
— control
— data

bridge plugin



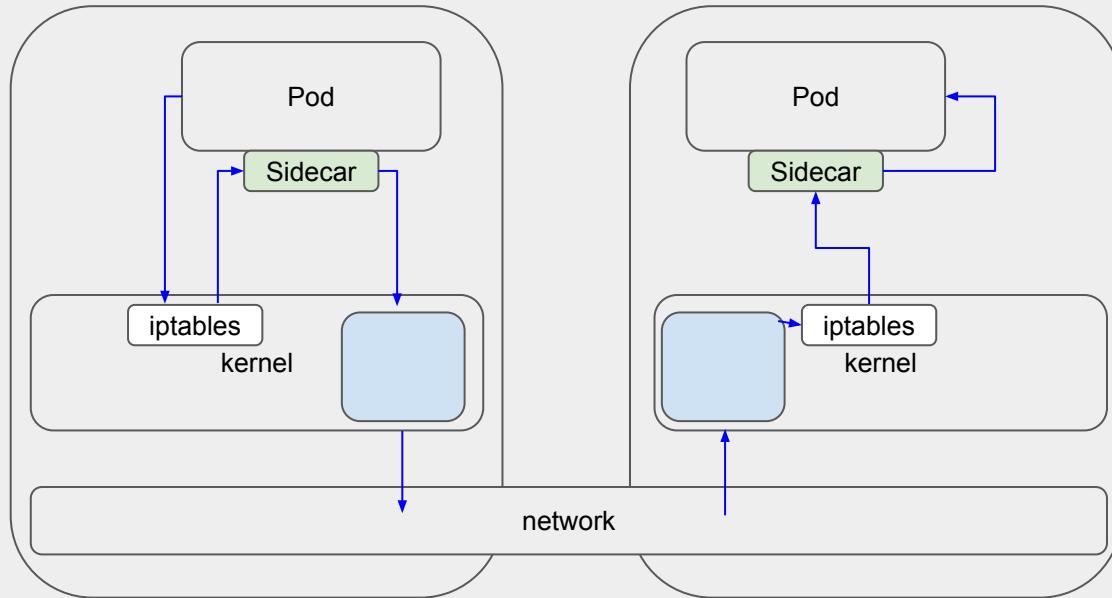
→ control
→ data

service mesh with bridge plugin



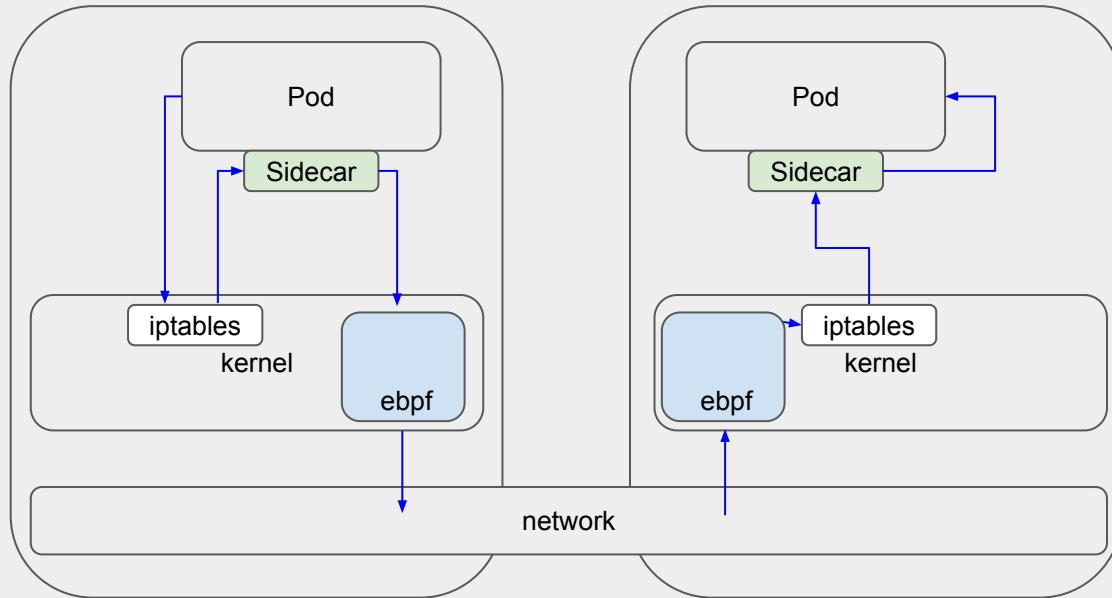
→ control
→ data

CNI + service mesh



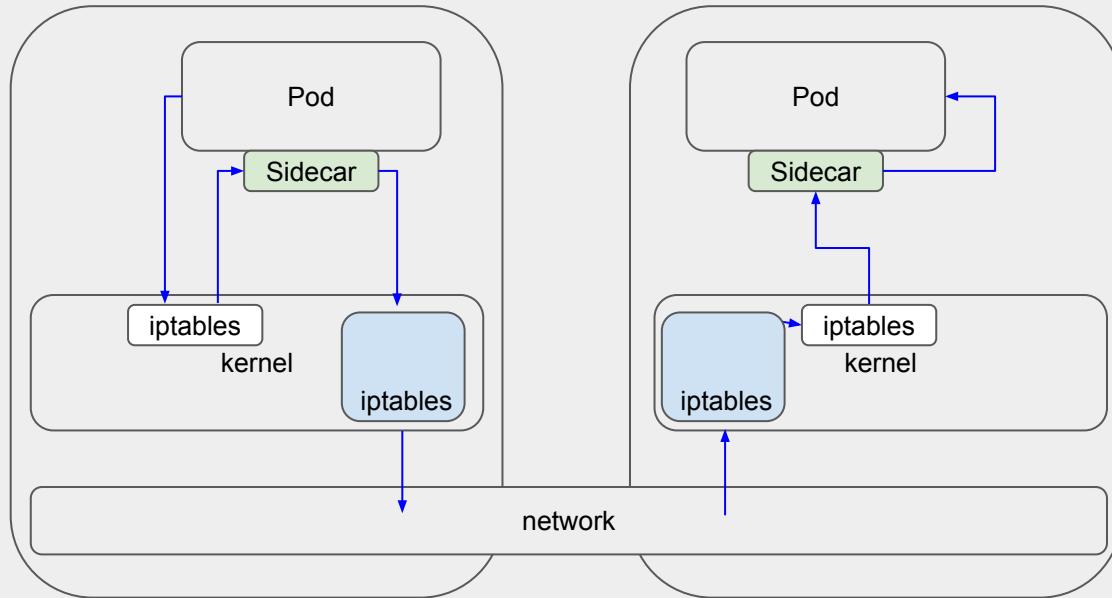
→ control
→ data

CNI + service mesh



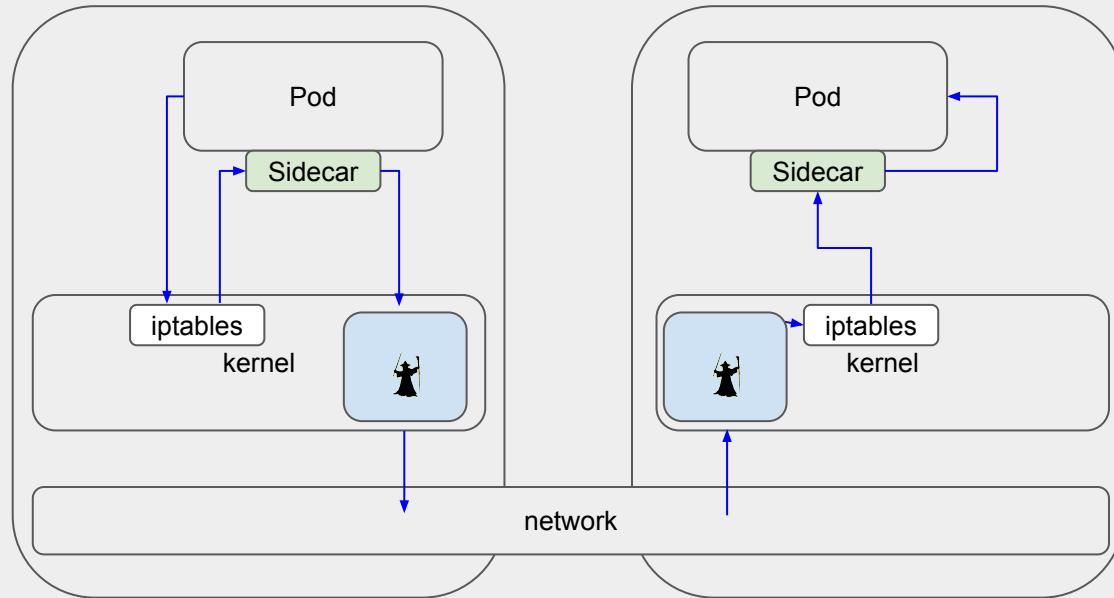
→ control
→ data

CNI + service mesh



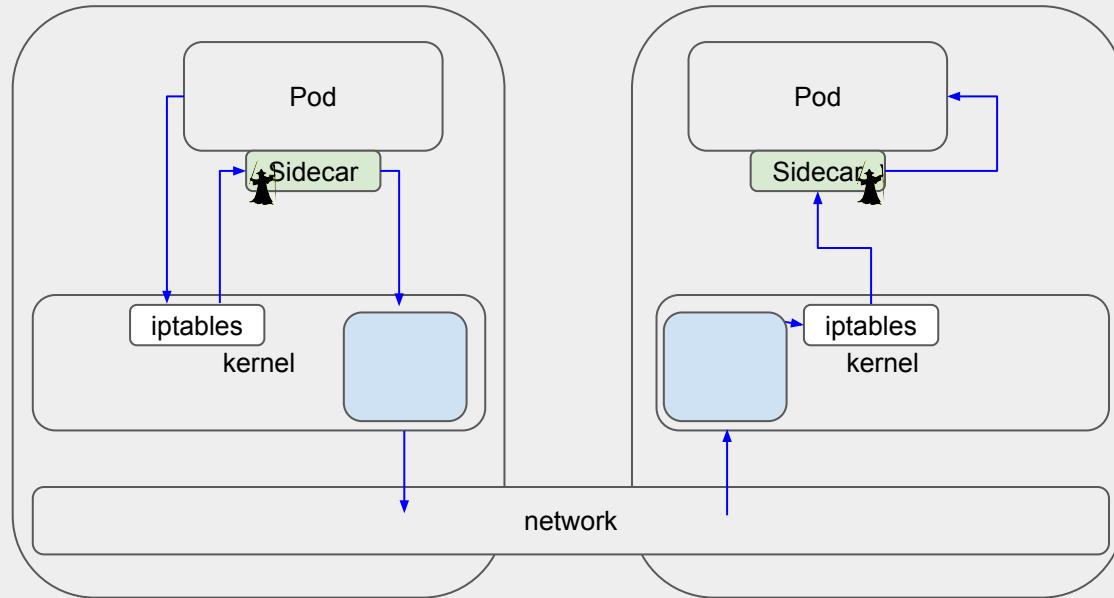
→ control
→ data

CNI + service mesh



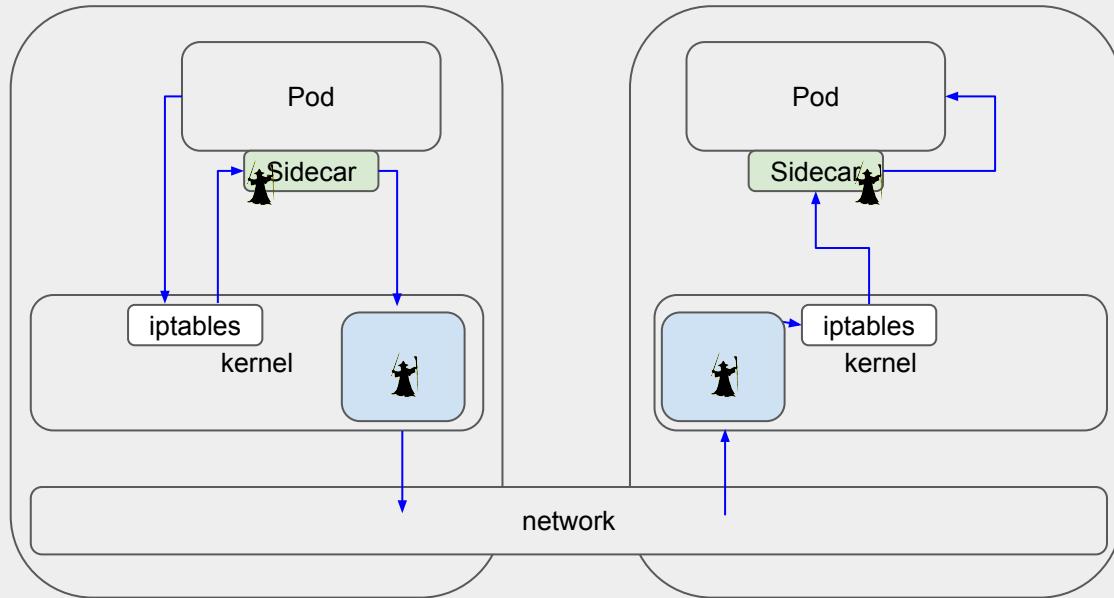
— control
— data

CNI + service mesh



→ control
→ data

CNI + service mesh



→ control
→ data



CNI - what shall not pass?

**CNI - what shall not pass?
- what is enforceable?**

CNI - what is enforceable?

```
$ kubectl explain networkpolicy.spec
```

- Allows you to apply policy on traffic which:
 - is going to any* IP or CIDR
 - is going to pods that match some label selector
 - is going to specific port(s)
 - is going to a specific namespace(s)

* except loopback or host traffic

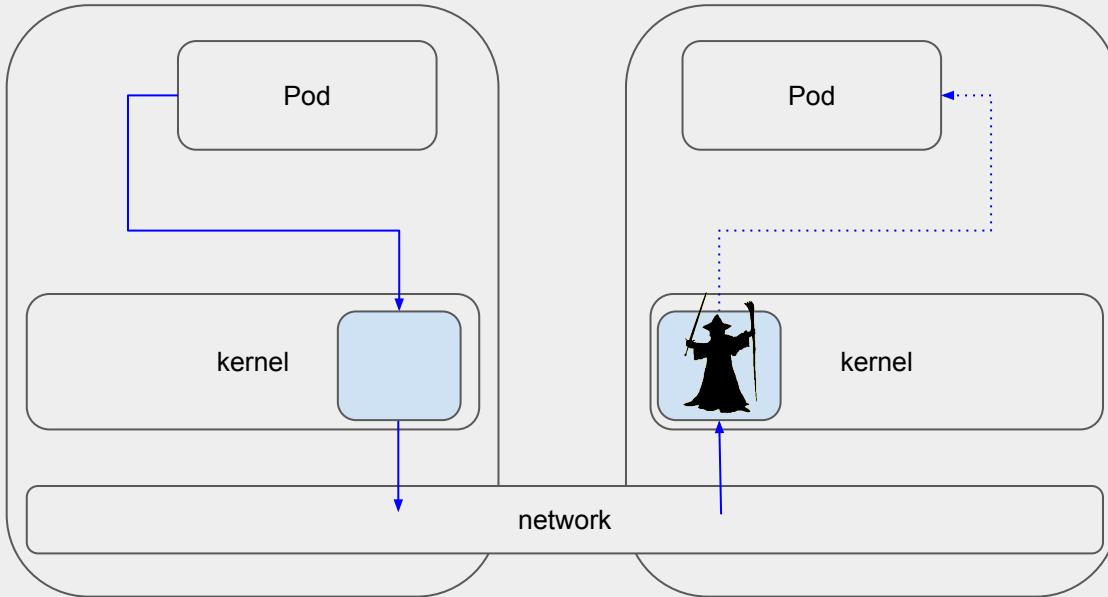
CNI - what is enforceable?

```
$ kubectl explain networkpolicy.spec
```

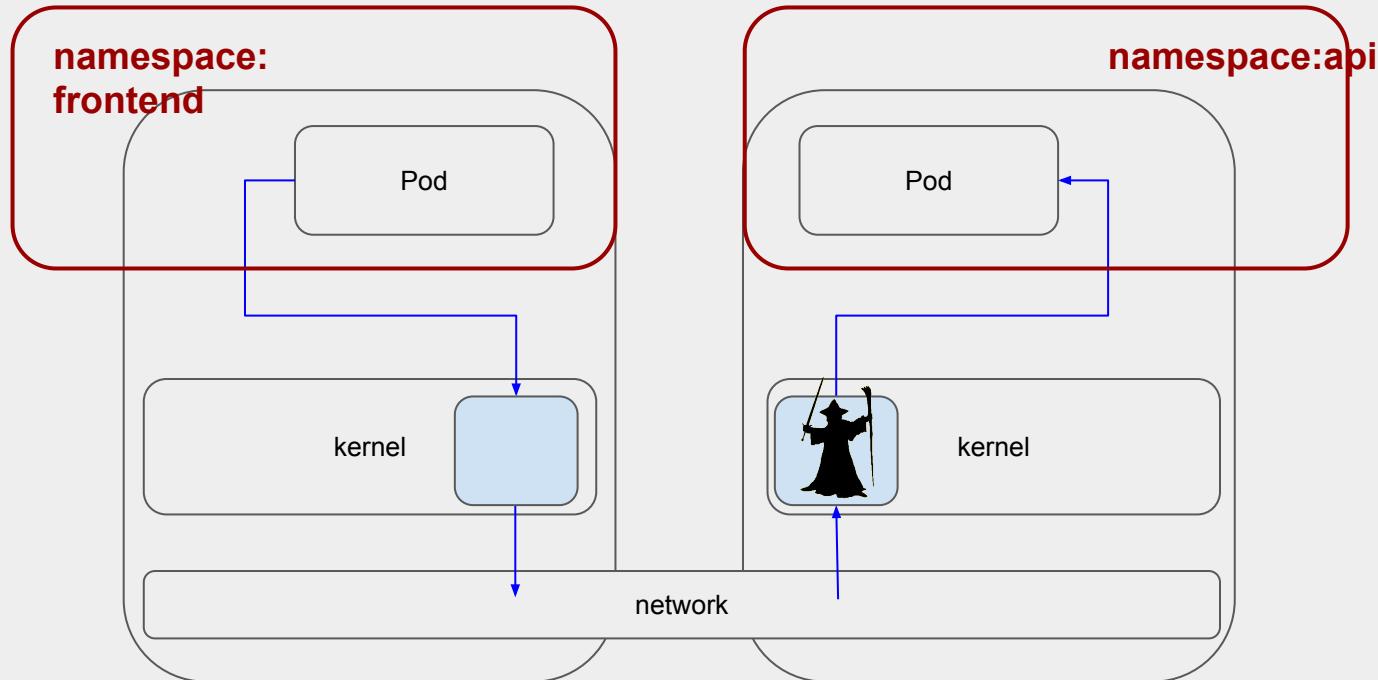
- Allows you to apply policy on traffic which:
 - is going to any* IP or CIDR
 - is going to pods that match some label selector
 - is going to specific port(s)
 - is going to a specific namespace(s)
- Allows you to conditionally block/permit traffic based on:
 - source IP or CIDR
 - source pods that match some label selector
 - source namespace

* except loopback or host traffic

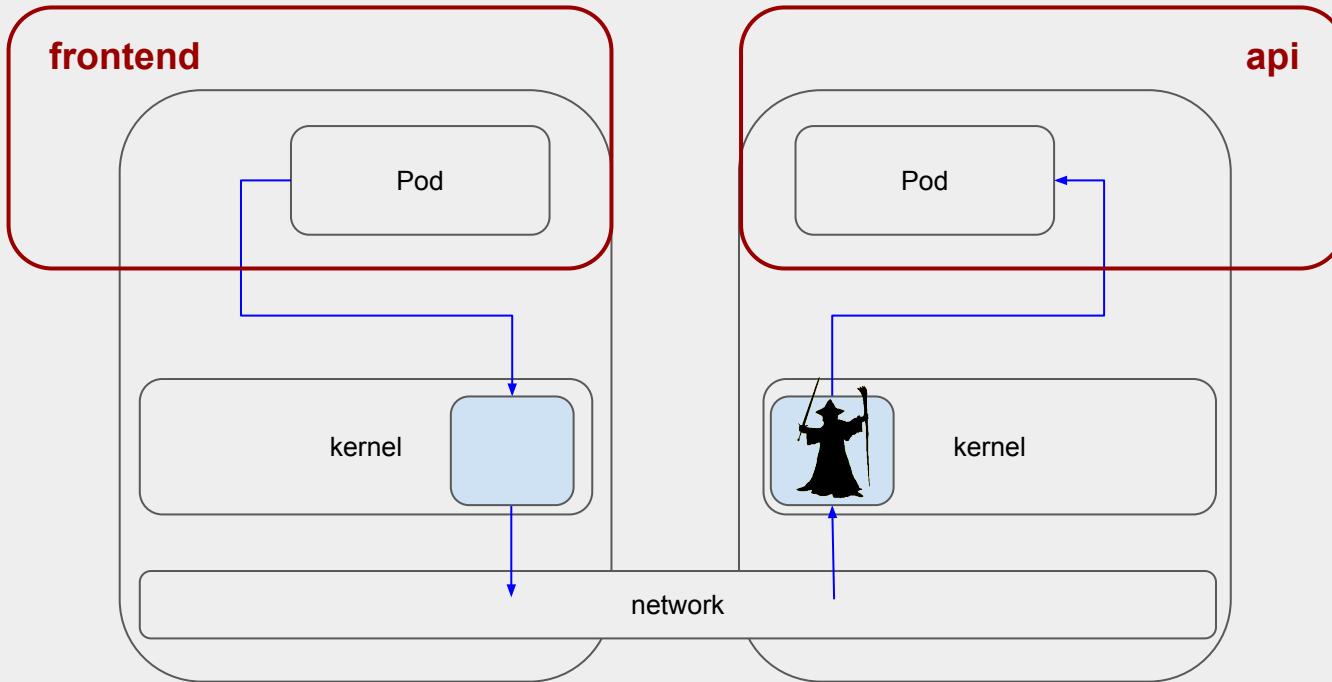
CNI - how is it enforced?



CNI - how is it enforced?

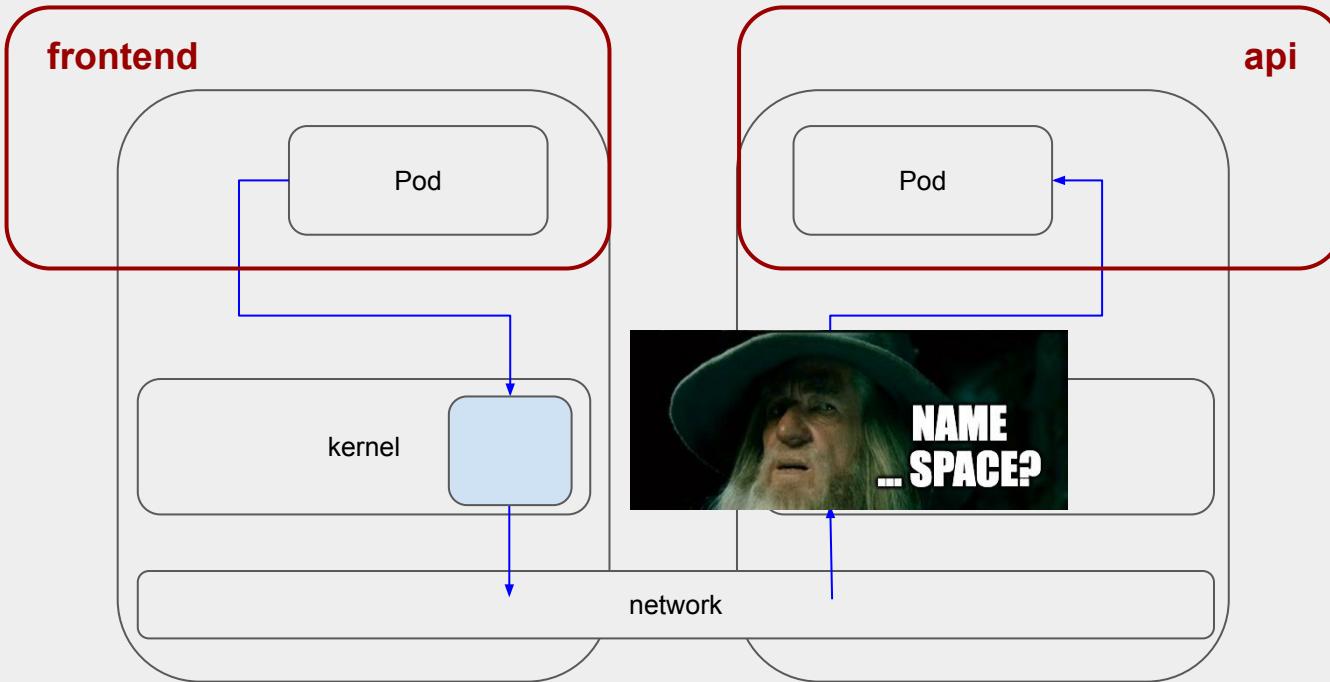


CNI - how is it enforced?



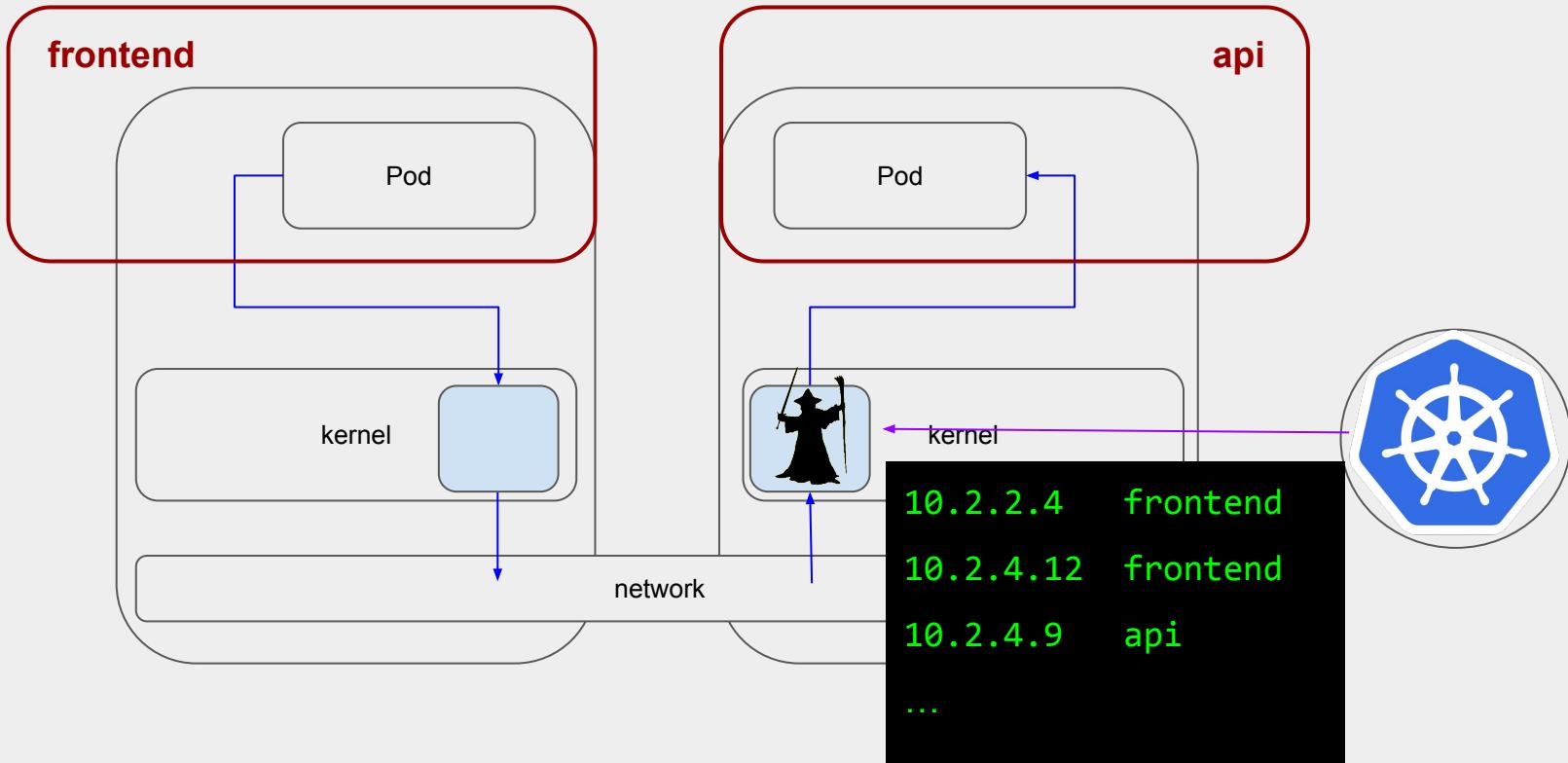
```
$ dear CNI: [pods in frontend] => [pods in api] == OK!
```

CNI - how is it enforced?

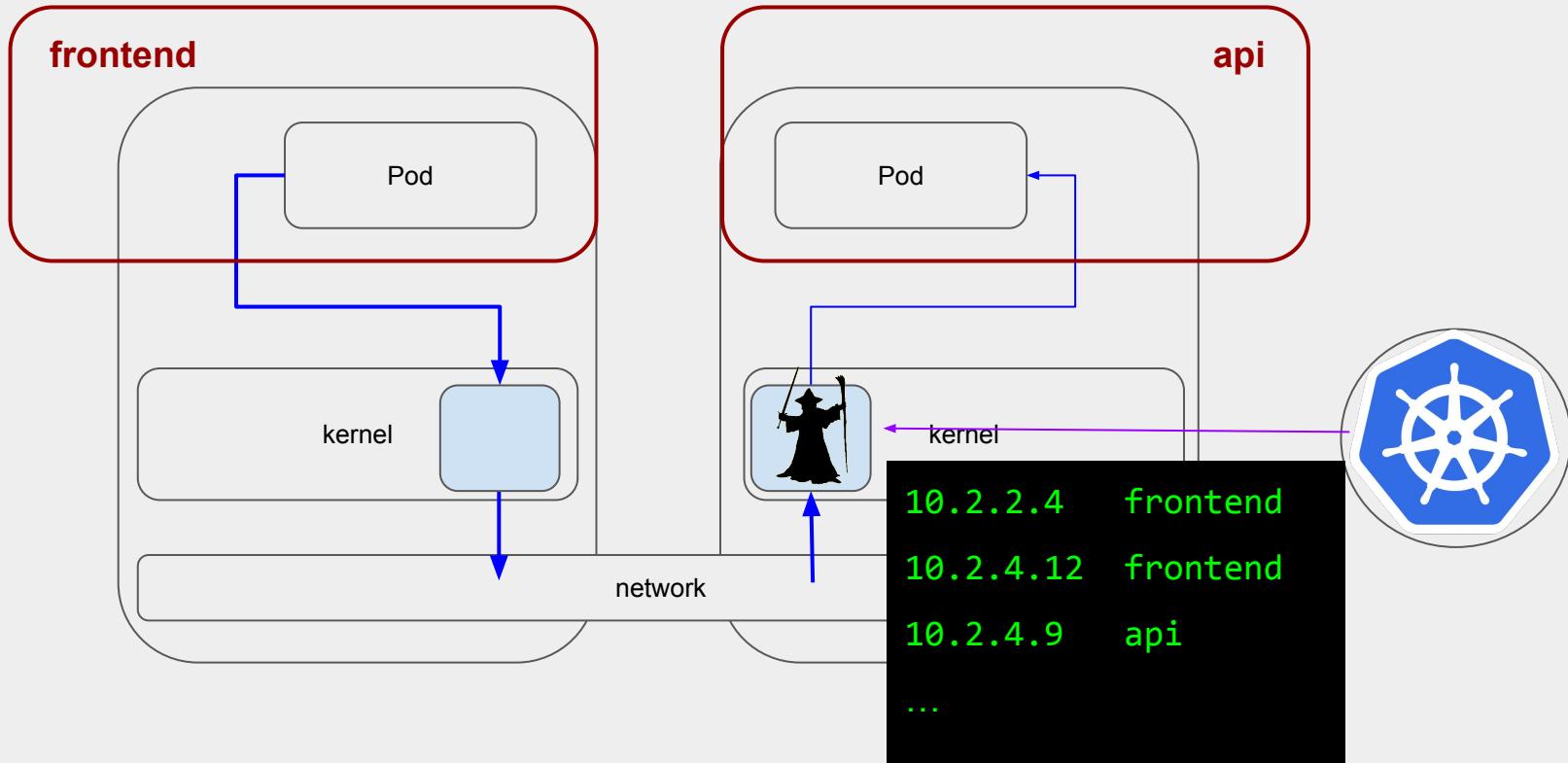


```
$ dear CNI: [pods in frontend] => [pods in api] == OK!
```

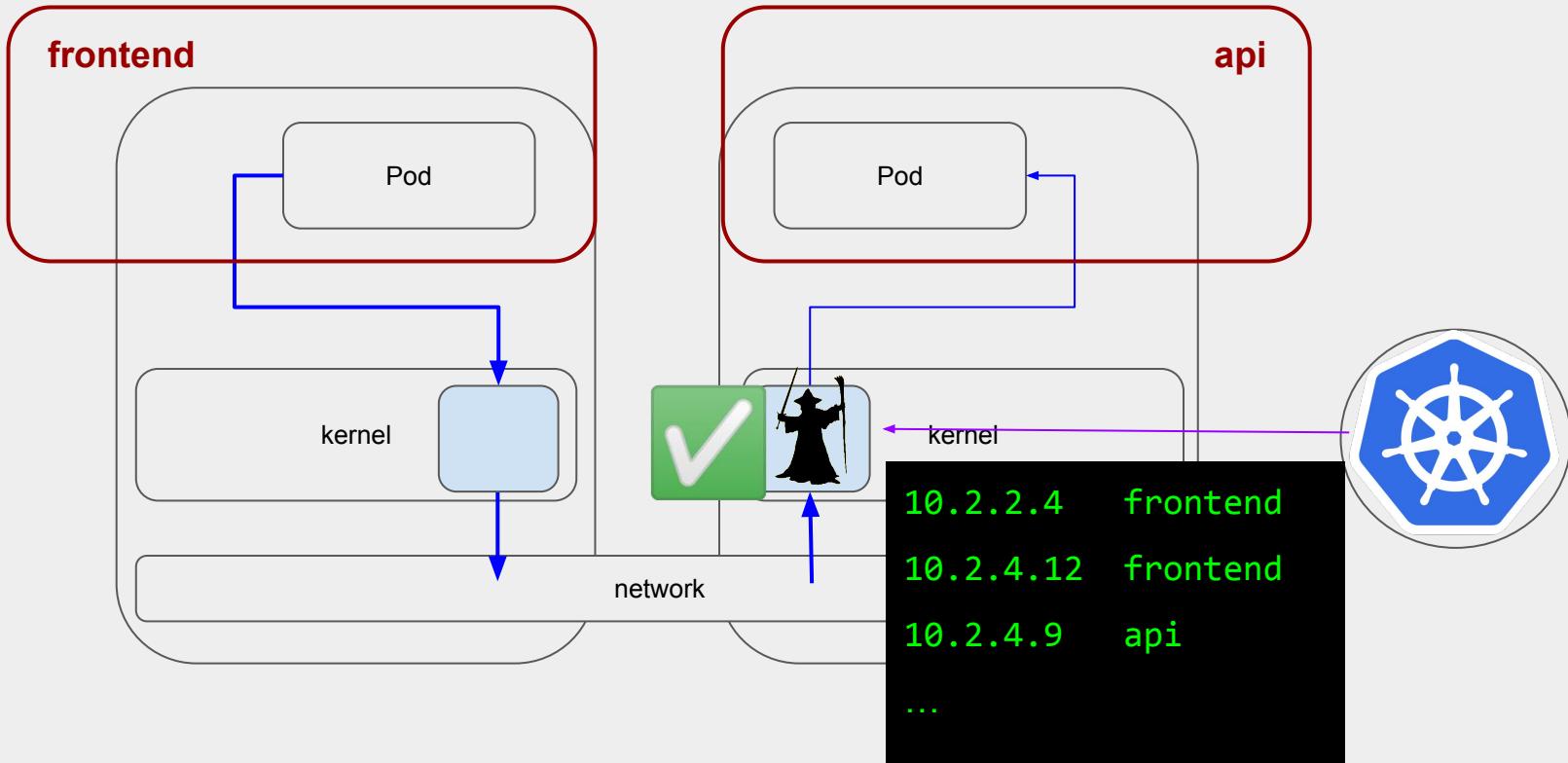
CNI - how is it enforced?



CNI - how is it enforced?

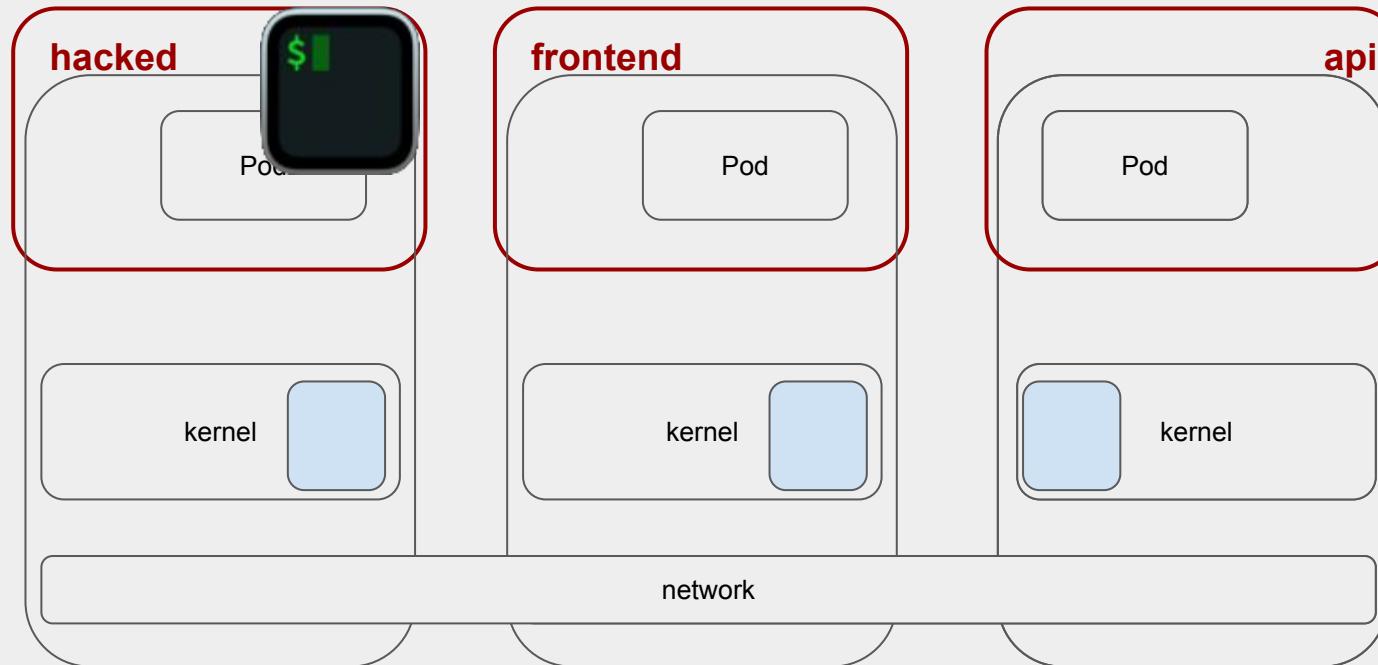


CNI - how is it enforced?



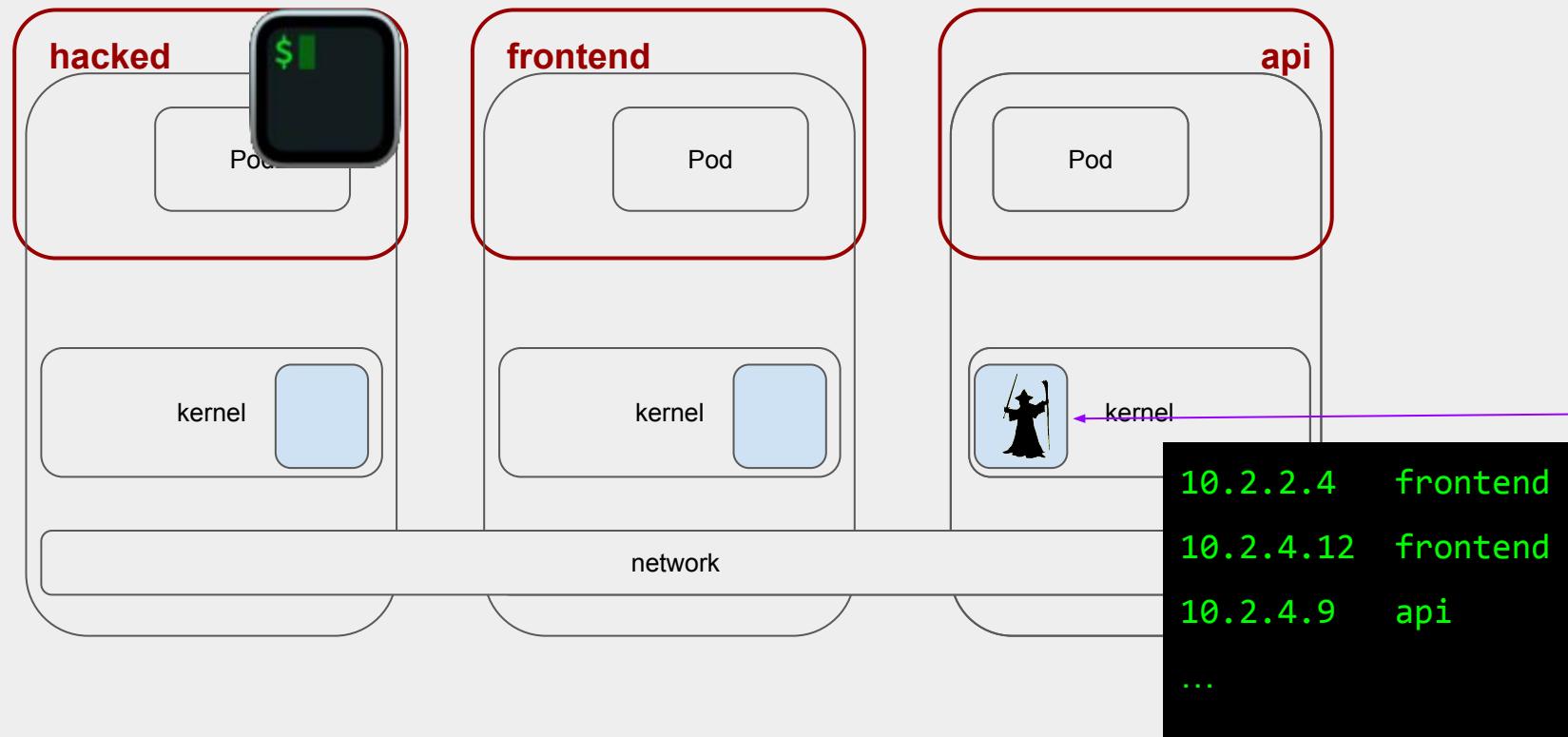
It's time for a
contrived
scenario!

CNI - contrived scenario

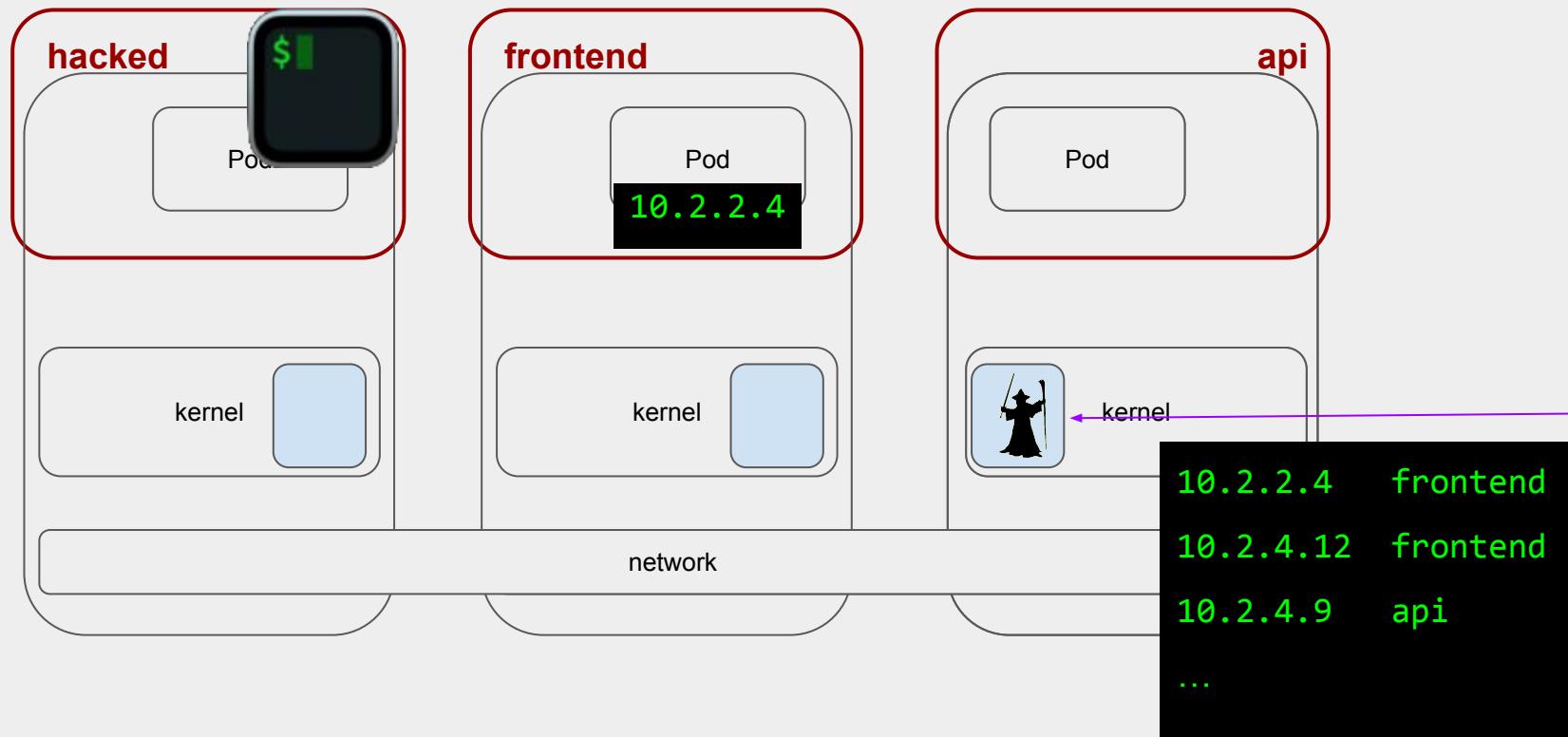


```
$ dear CNI: [pods in frontend] => [pods in api] == OK!
```

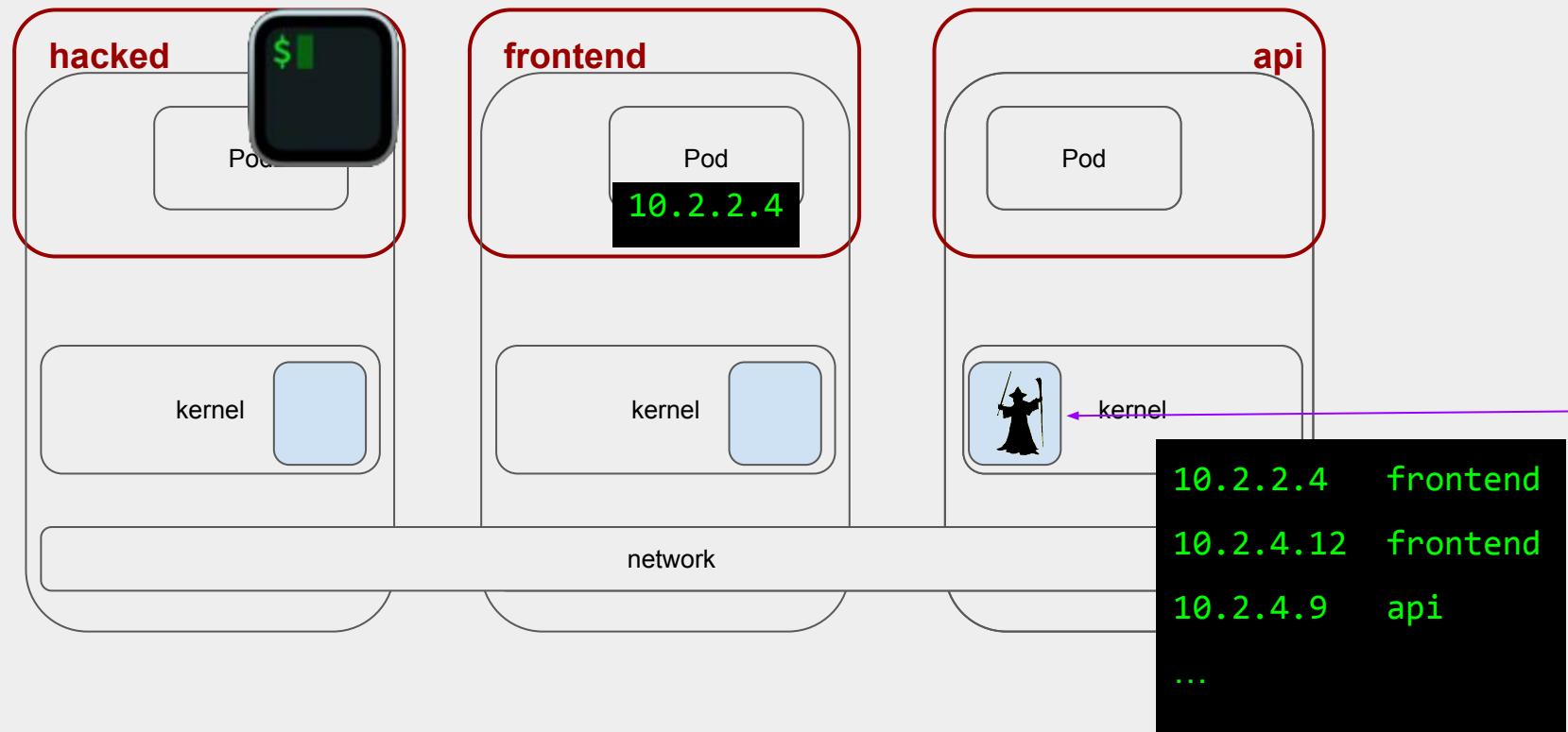
CNI - contrived scenario



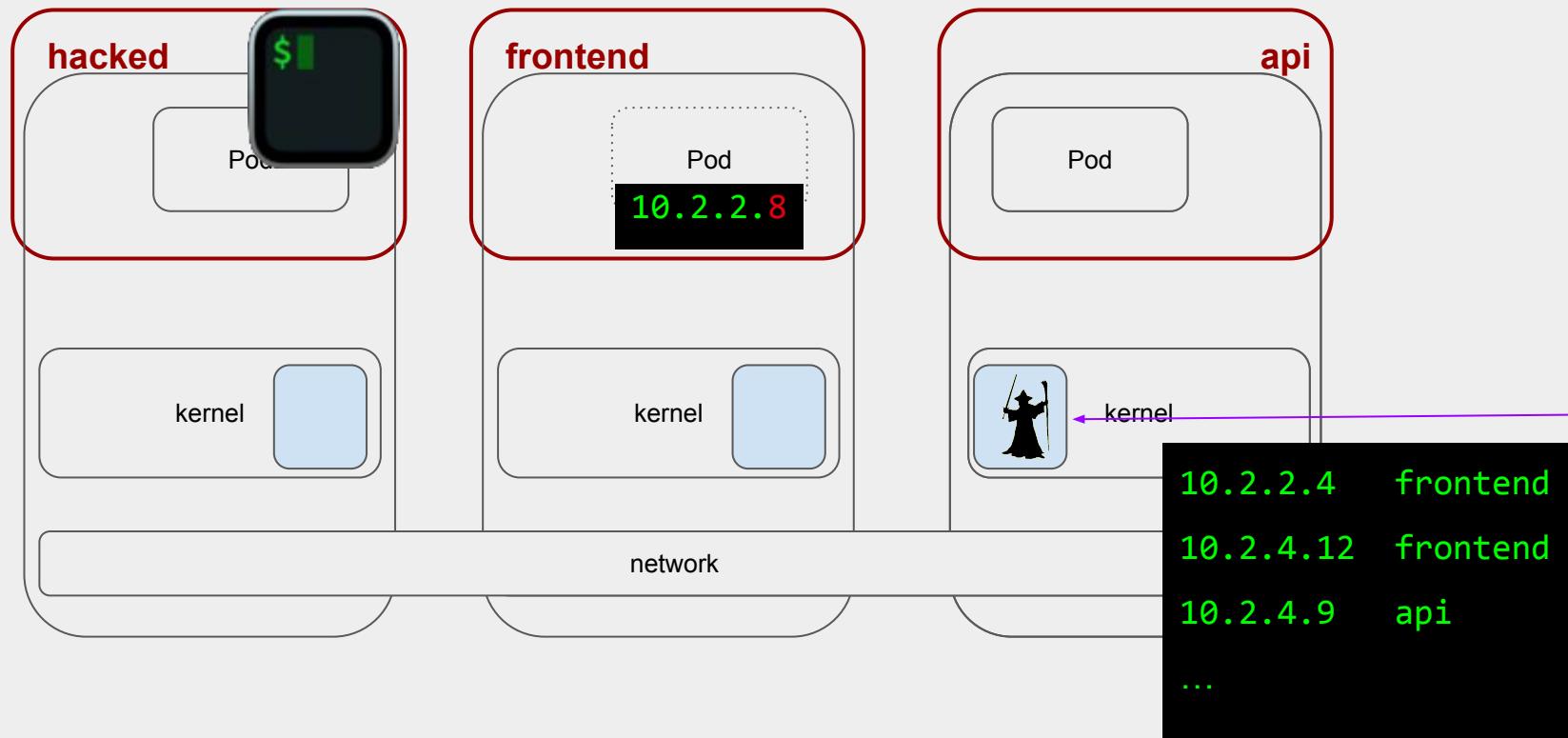
CNI - contrived scenario



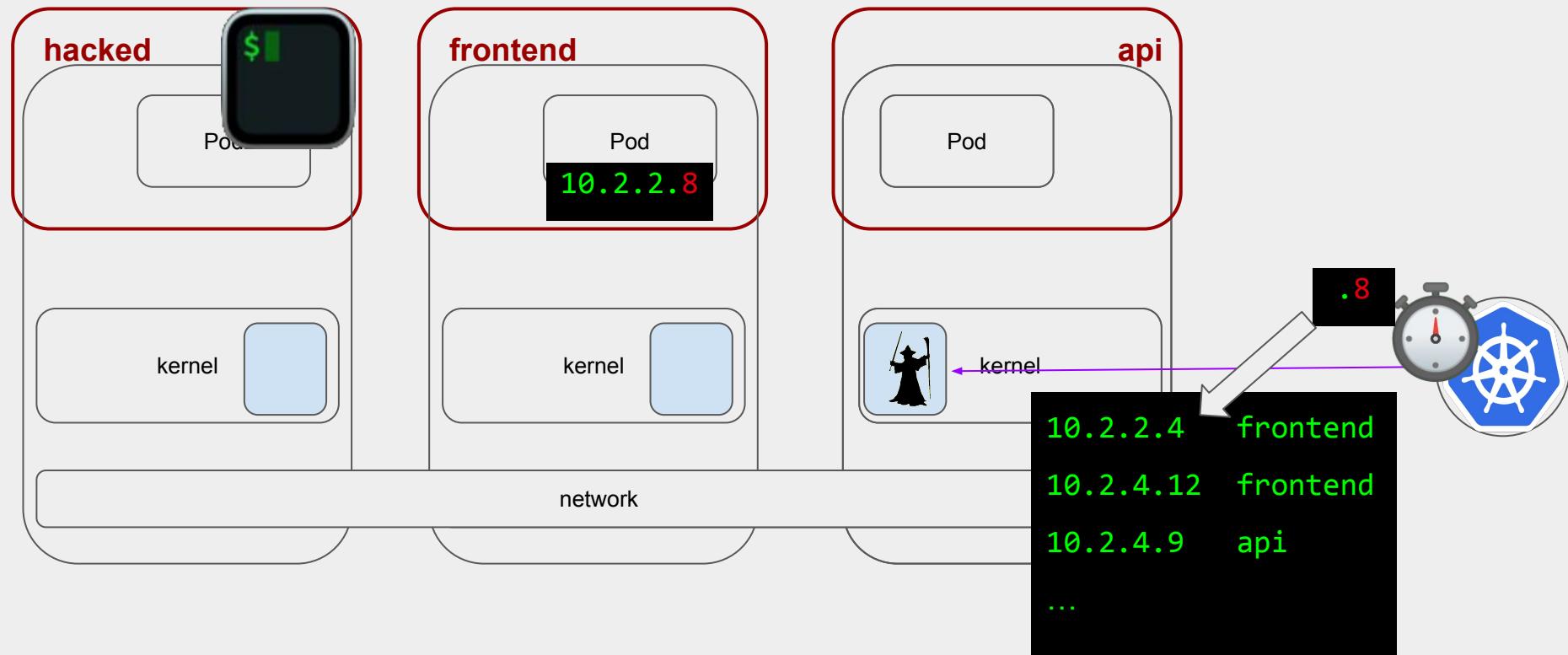
CNI - contrived scenario



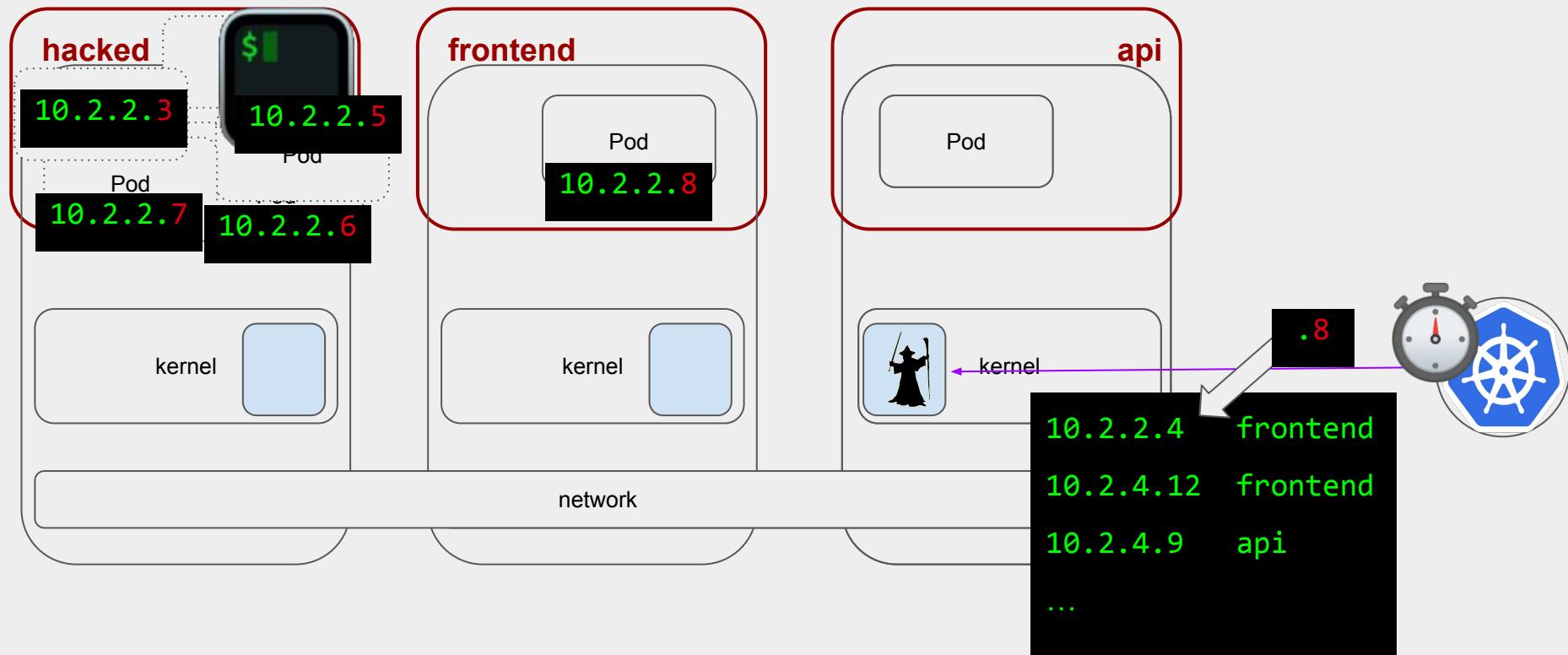
CNI - contrived scenario



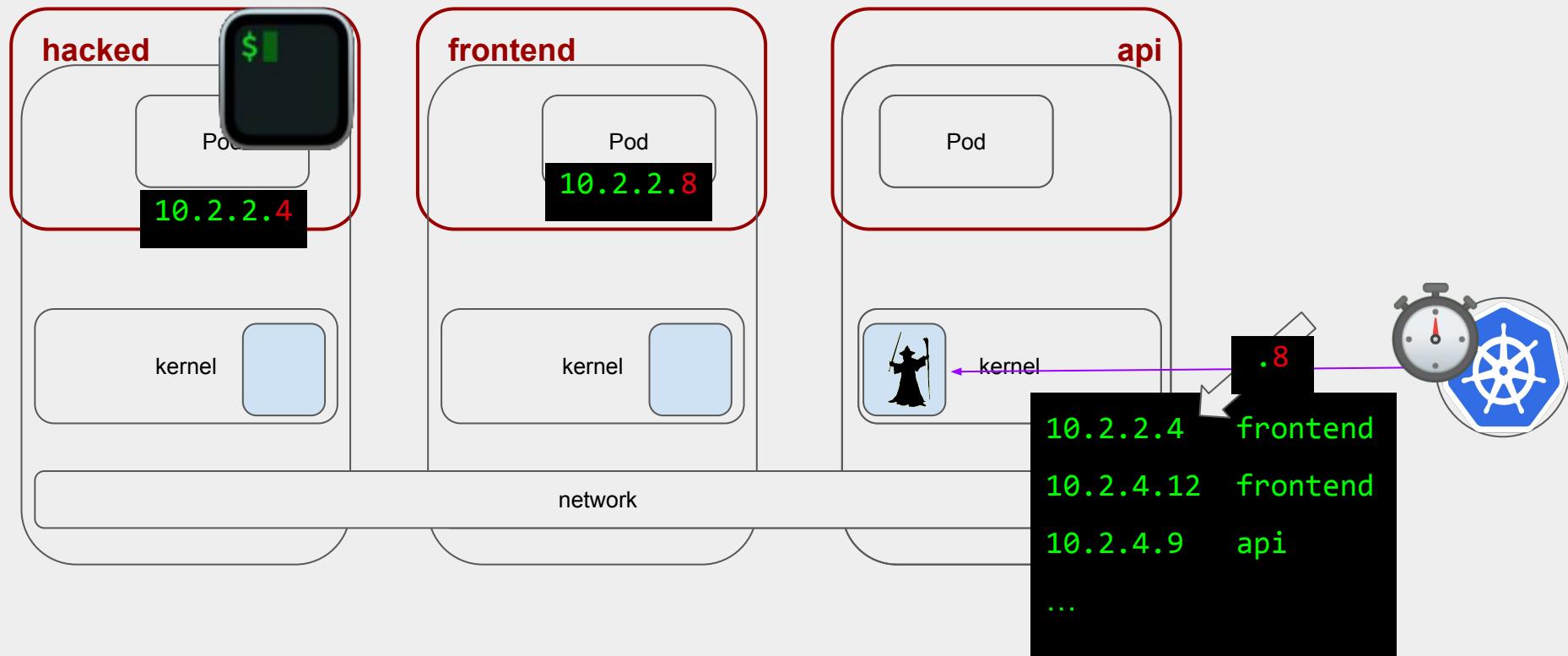
CNI - contrived scenario



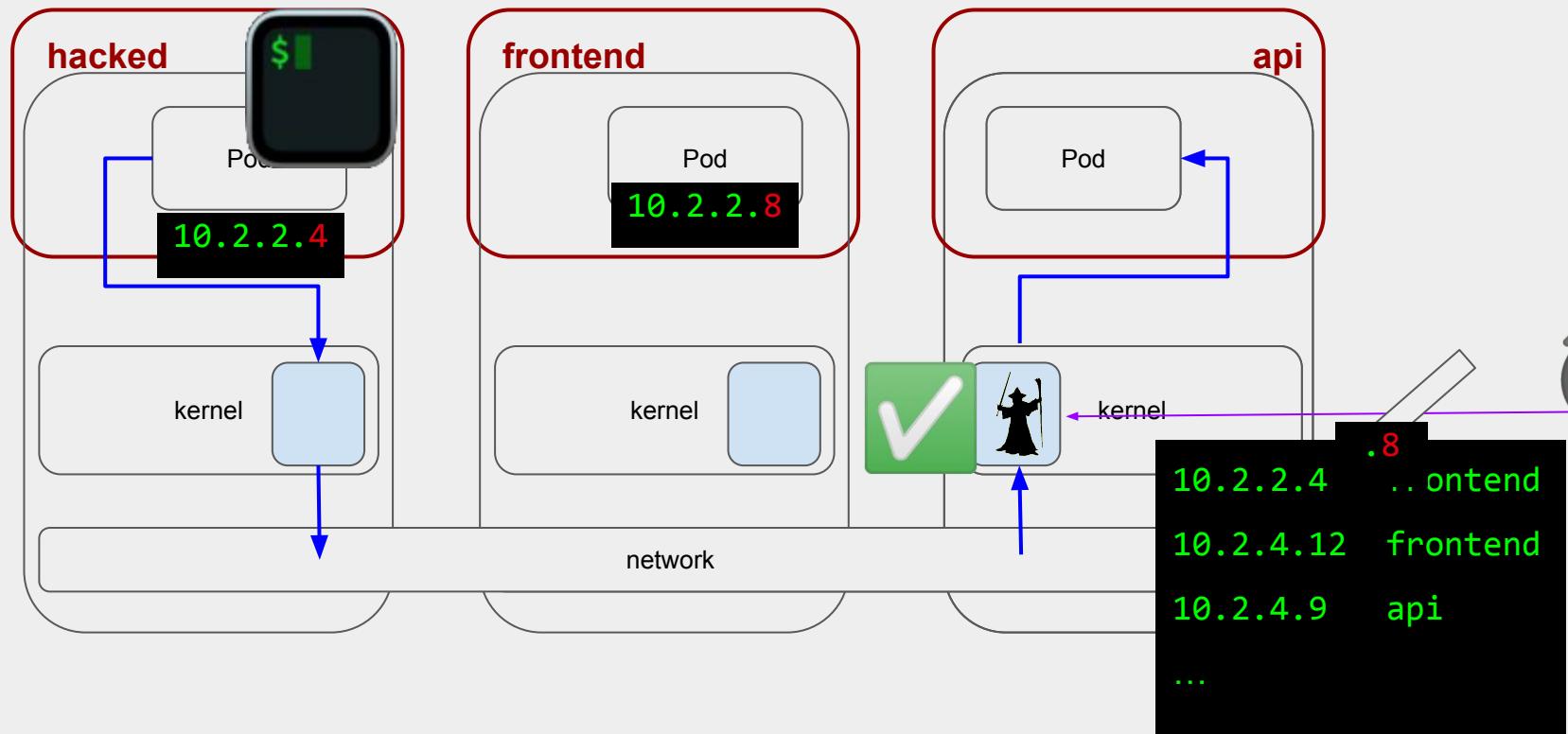
CNI - contrived scenario



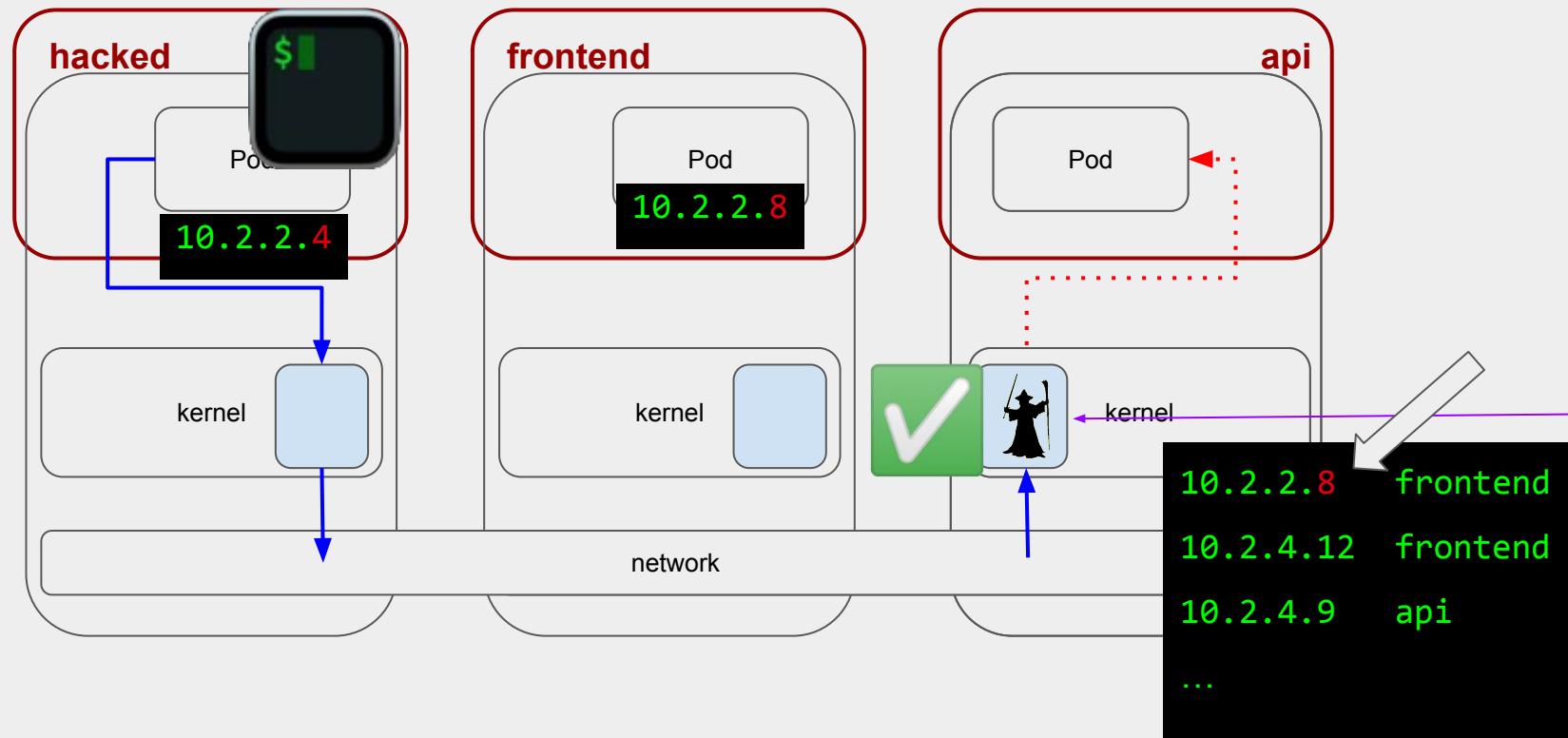
CNI - contrived scenario



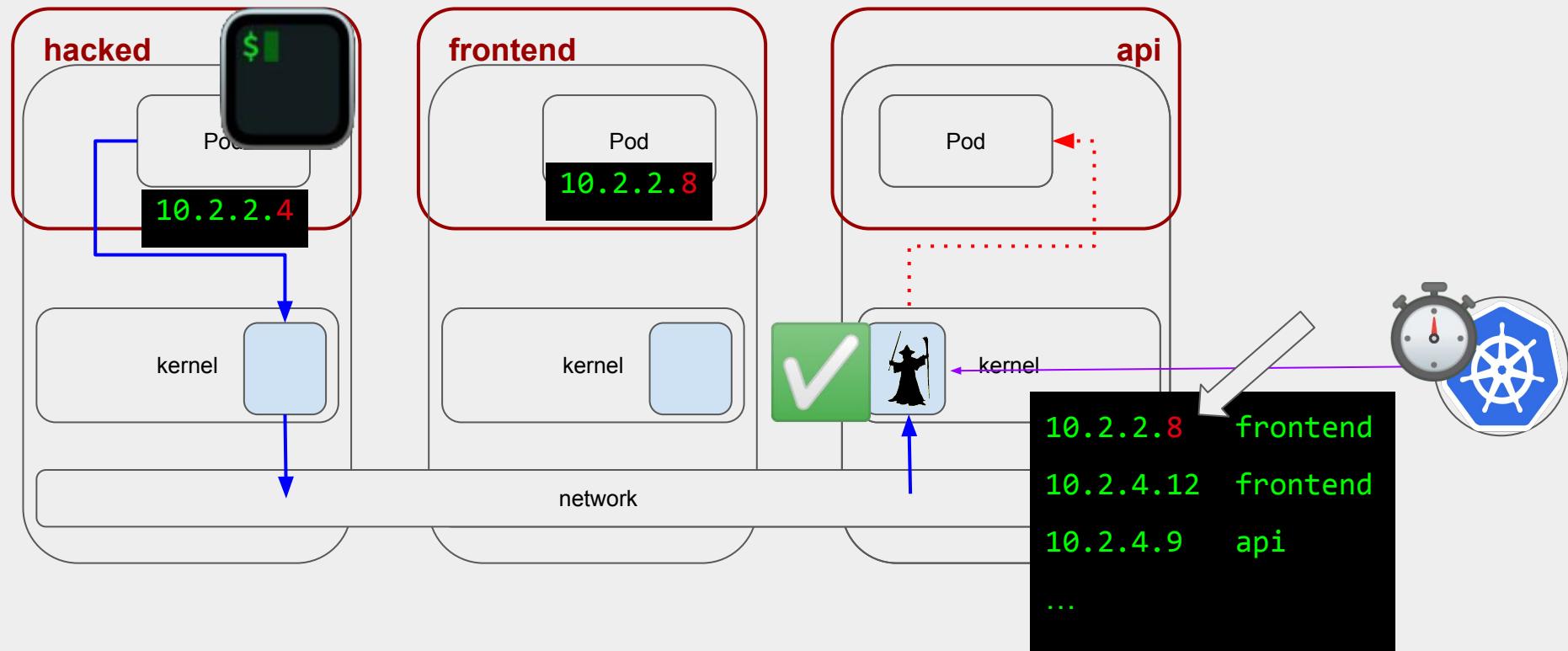
CNI - contrived scenario



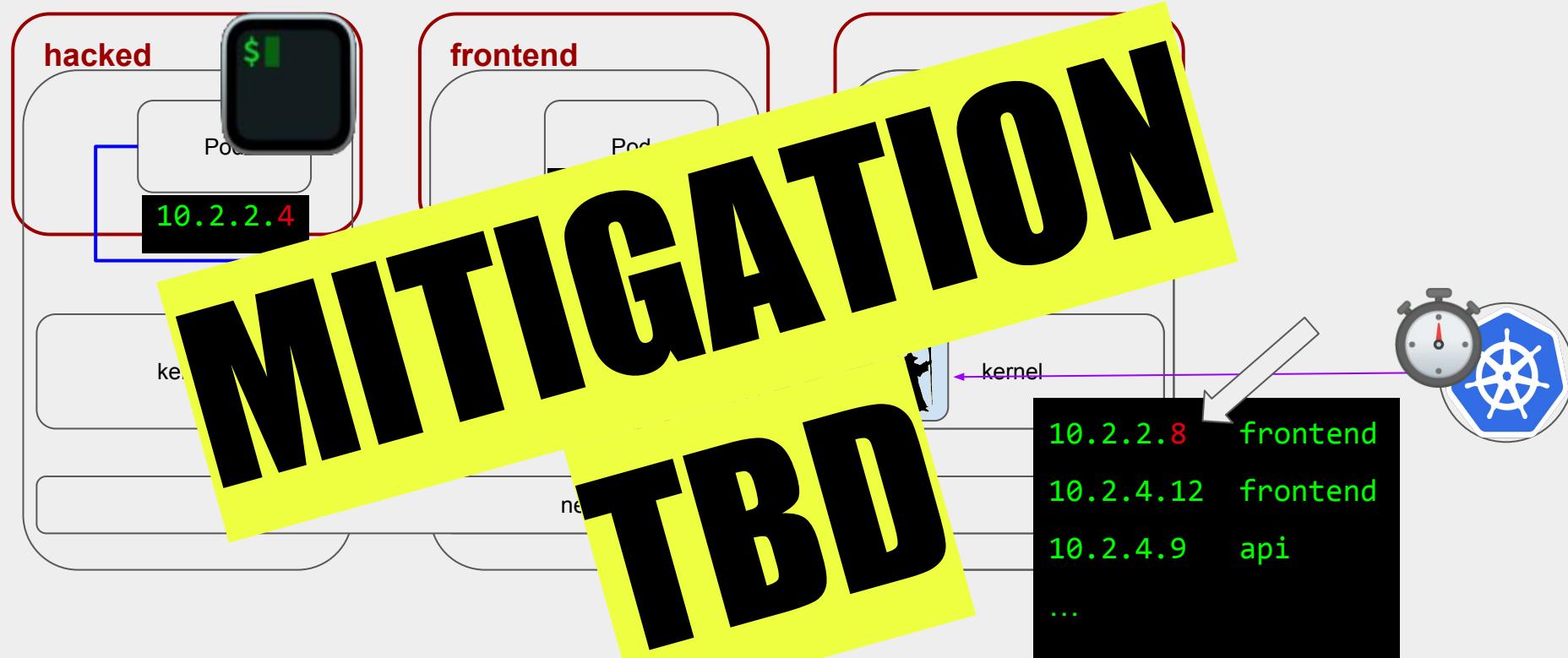
CNI - contrived scenario



CNI - contrived scenario



CNI - contrived scenario



Svc Mesh - what is enforceable?

Svc Mesh - what is enforceable?

```
$ kubectl explain ${SERVICE_MESH_AUTH_POLICY}
```

- Allows you to apply policy on traffic which:
 - is going anywhere*
 - is going to a specific K8s Service
 - is going to a specific port(s)

* including loopback or host traffic

Svc Mesh - what is enforceable?

```
$ kubectl explain ${SERVICE_MESH_AUTH_POLICY}
```

- Allows you to apply policy on traffic which:
 - is going anywhere*
 - is going to a specific K8s Service
 - is going to a specific port(s)
 - Allows you to conditionally block/permit requests based on:
 - source IP address or CIDR
 - source kubernetes namespace
 - source kubernetes service account

* including loopback or host traffic

Svc Mesh - what is enforceable?

```
$ kubectl explain ${SERVICE_MESH_AUTH_POLICY}
```

- Allows you to apply policy on traffic which:
 - is going anywhere*
 - is going to a specific K8s Service
 - is going to a specific port(s)
 - Allows you to conditionally block/permit requests based on HTTP properties:
 - specific Host / Authority
 - specific HTTP method
 - specific URI (or prefix)
 - specific header is present or set to a specific value
 - JWT claims (Istio only)

* including loopback or host traffic

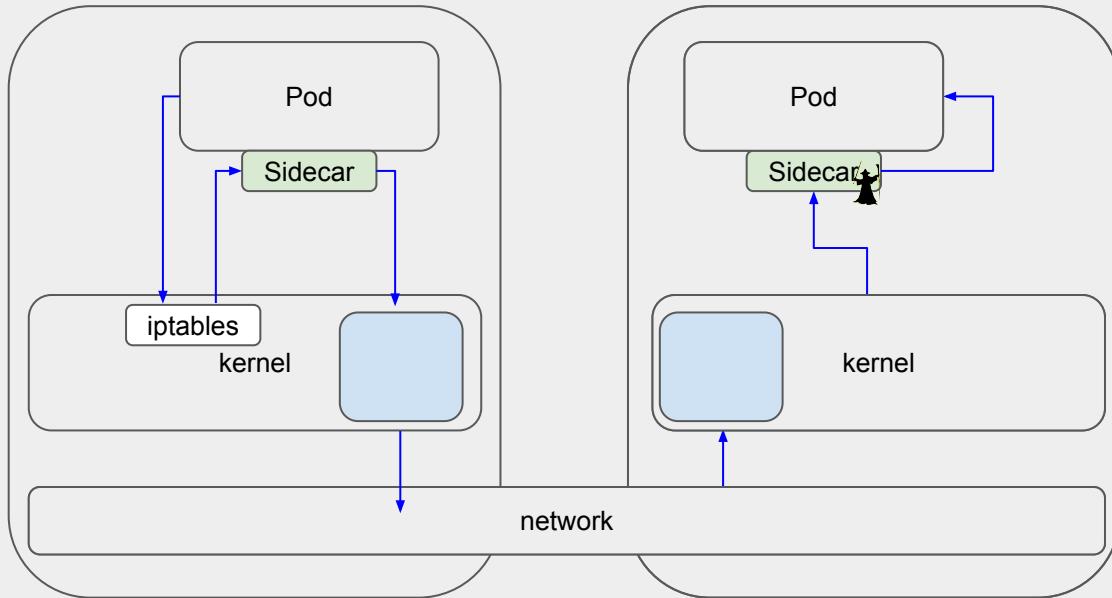
Svc Mesh - what is enforceable?

```
$ kubectl explain ${SERVICE_MESH_AUTH_POLICY}
```

- Allows you to apply policy on traffic which:
 - is going anywhere*
 - is going to a specific K8s Service
 - is going to a specific port(s)
 - Allows you to conditionally block/permit requests based on:
 - source IP address or CIDR
 - source kubernetes namespace
 - source kubernetes service account

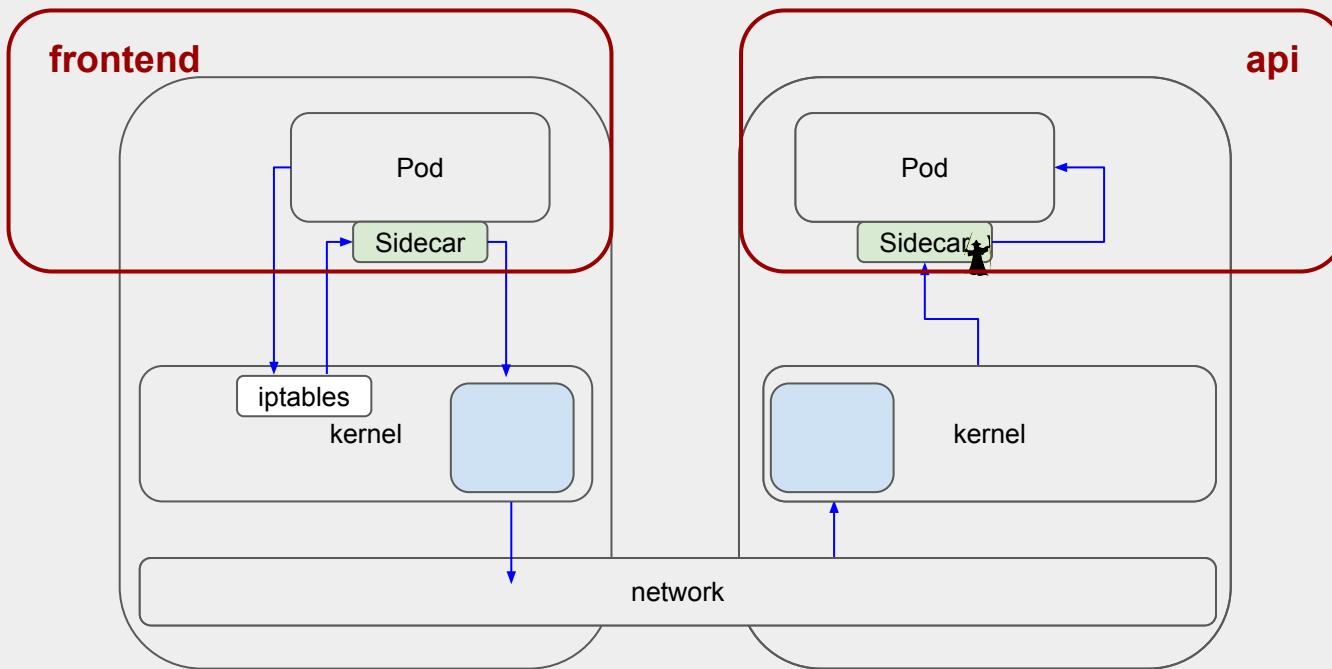
* including loopback or host traffic

Svc Mesh - how is it enforced?



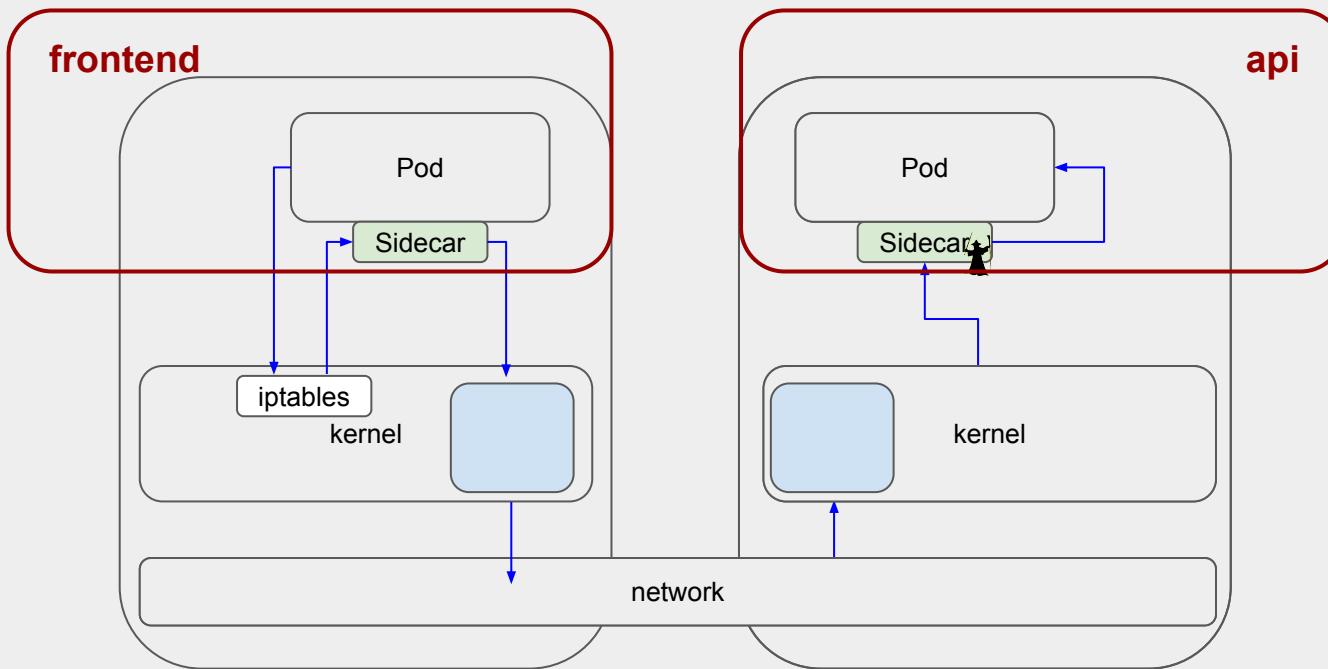
—> control
—> data

Svc Mesh - how is it enforced?



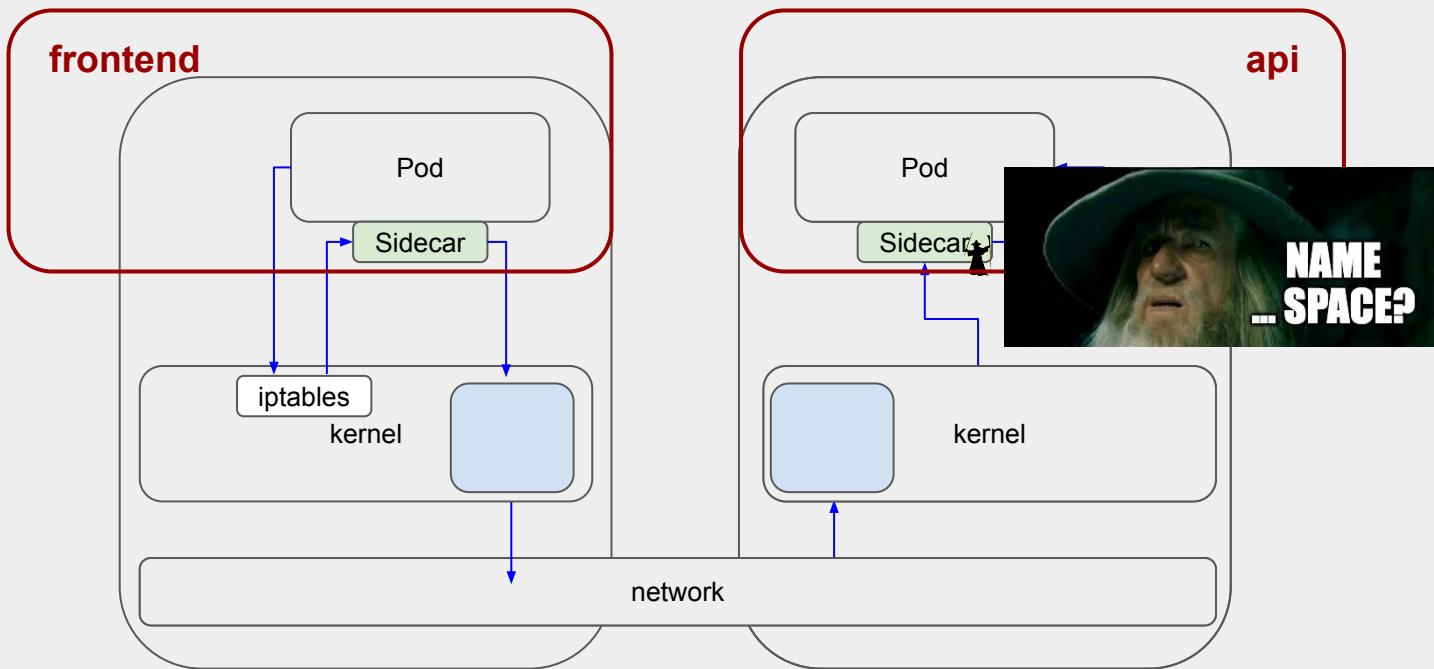
→ control
→ data

Svc Mesh - how is it enforced?



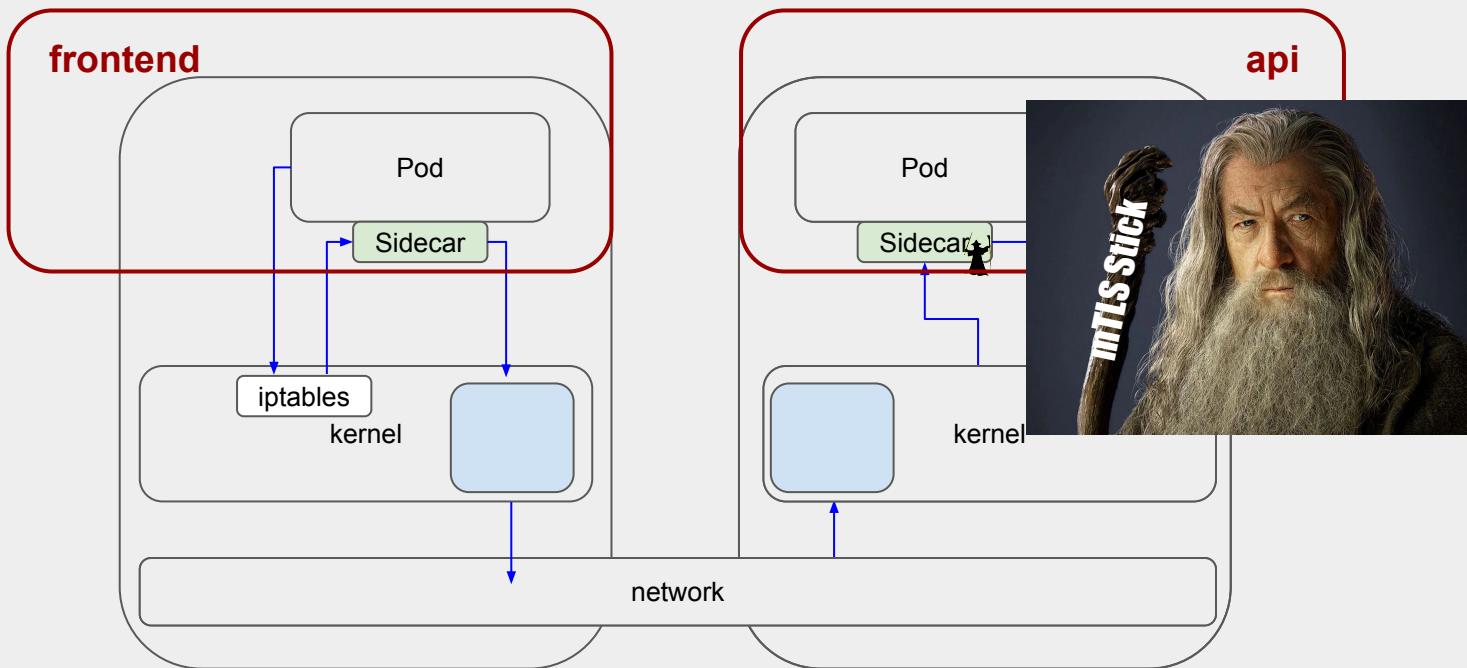
```
$ dear Service Mesh: [pods in frontend] => [pods in api] == OK!
```

Svc Mesh - how is it enforced?



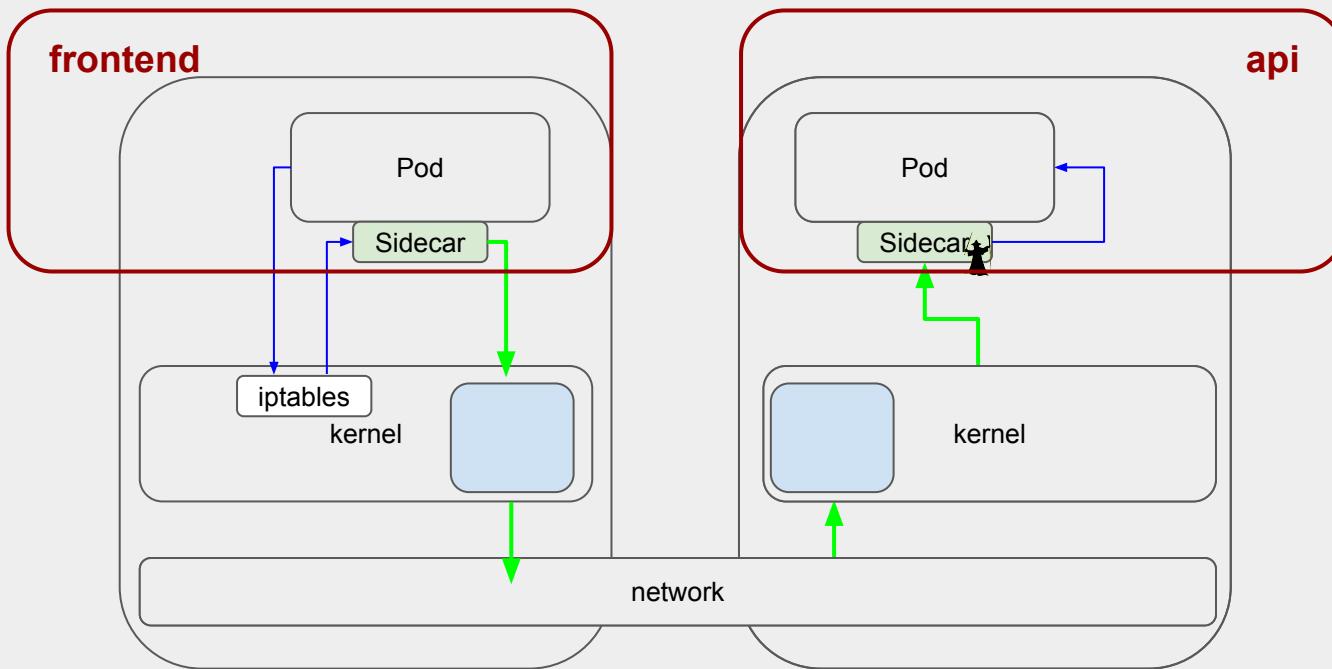
```
$ dear Service Mesh: [pods in frontend] => [pods in api] == OK!
```

Svc Mesh - how is it enforced?



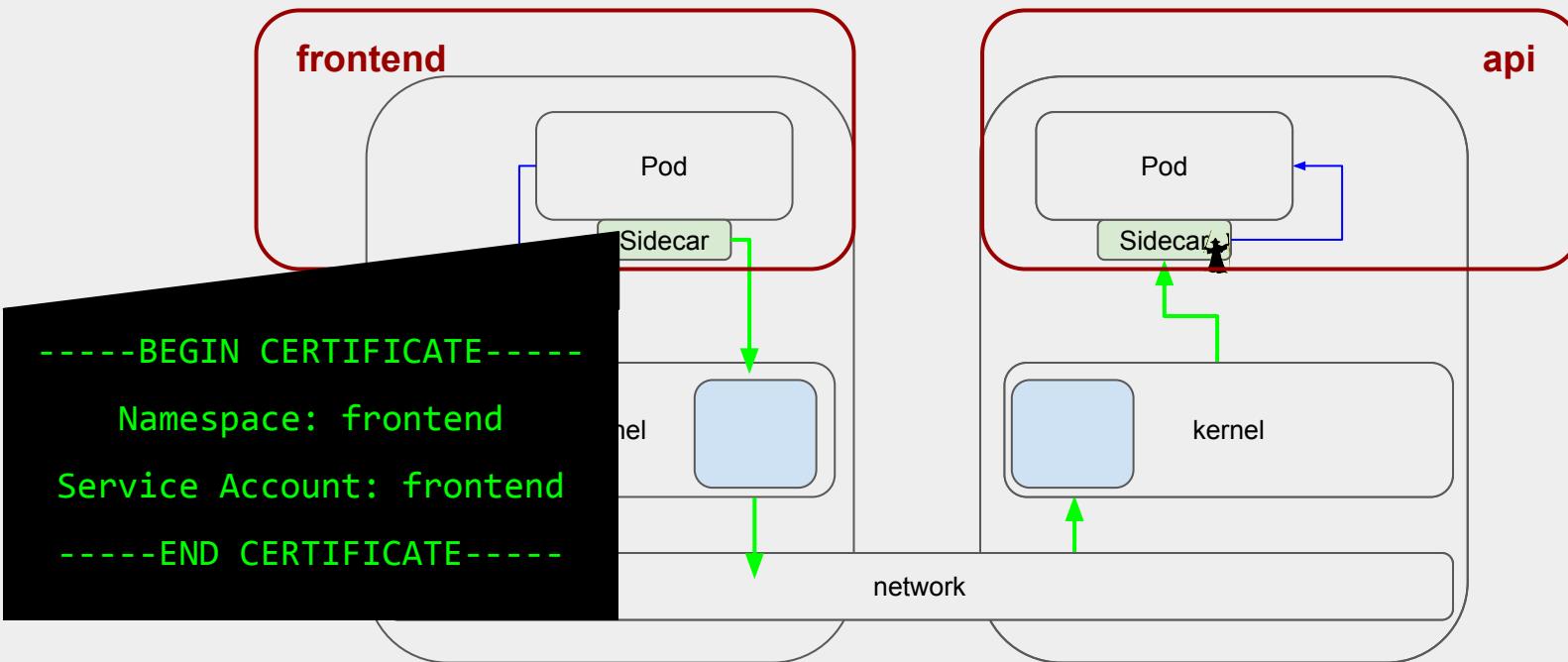
```
$ dear Service Mesh: [pods in frontend] => [pods in api] == OK!
```

Svc Mesh - how is it enforced?



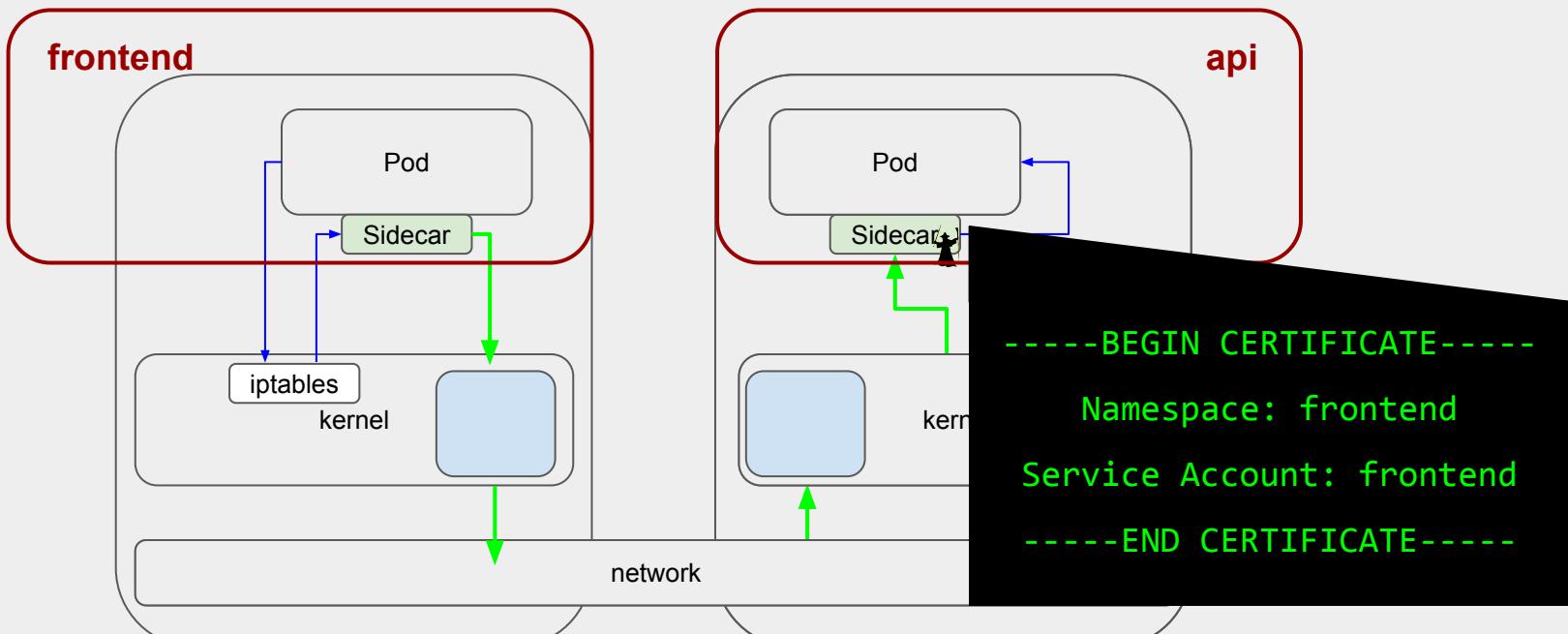
green → mTLS
purple → control
blue → data

Svc Mesh - how is it enforced?



→ mTLS
→ control
→ data

Svc Mesh - how is it enforced?



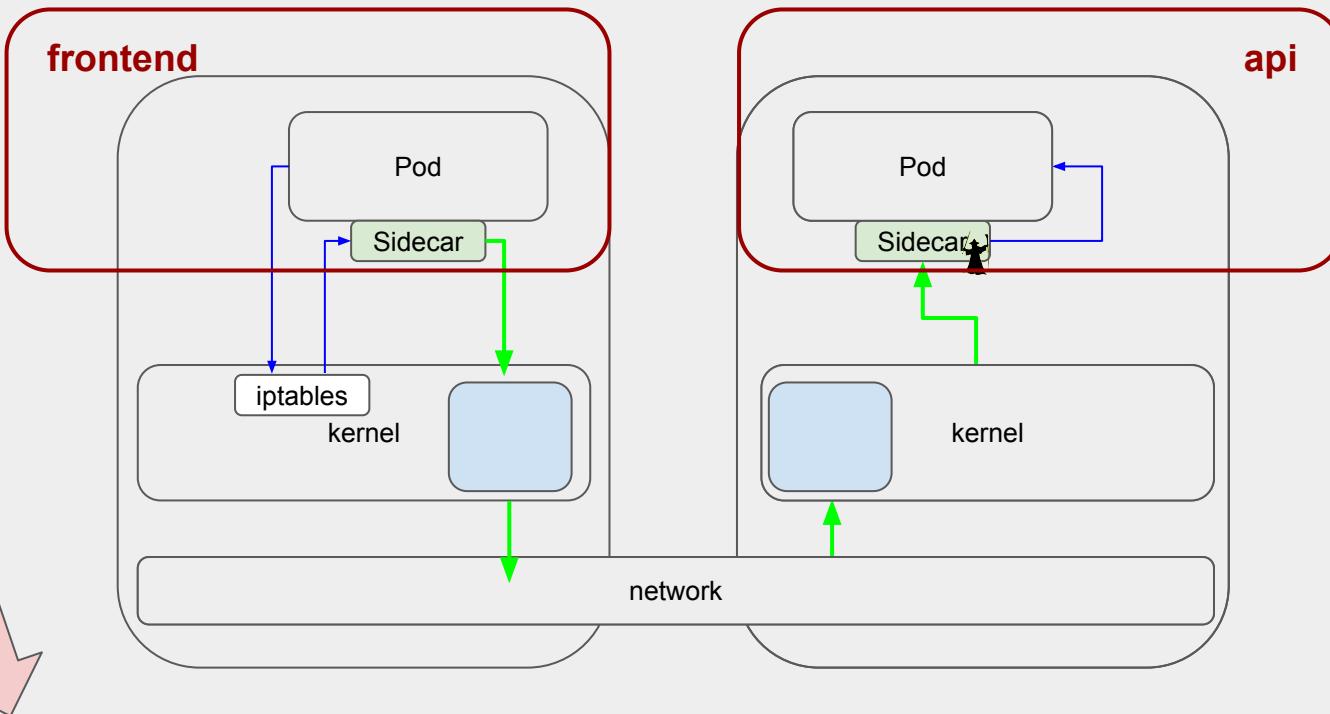
- mTLS
- control
- data

Svc Mesh - how is it enforced?



Svc Mesh - how is it enforced?

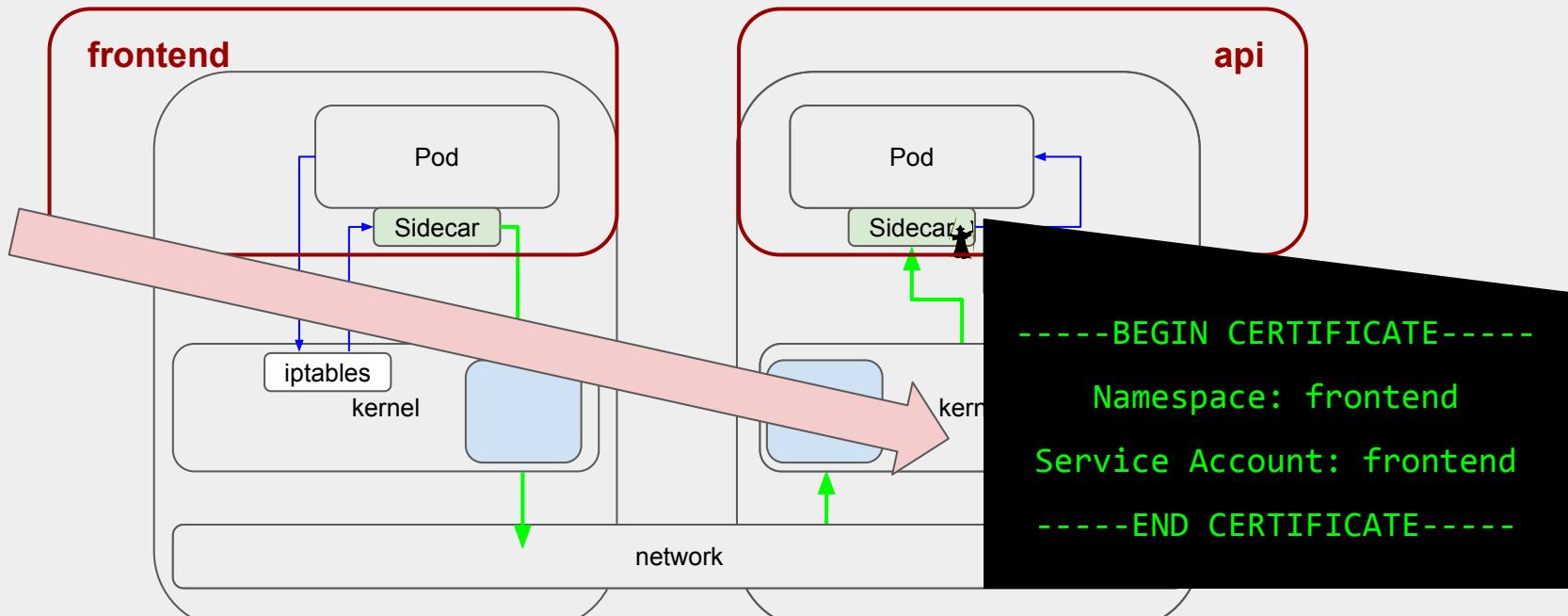
1



\$ dear Service Mesh: [pods in frontend] => [pods in api] == OK!

Svc Mesh - how is it enforced?

2



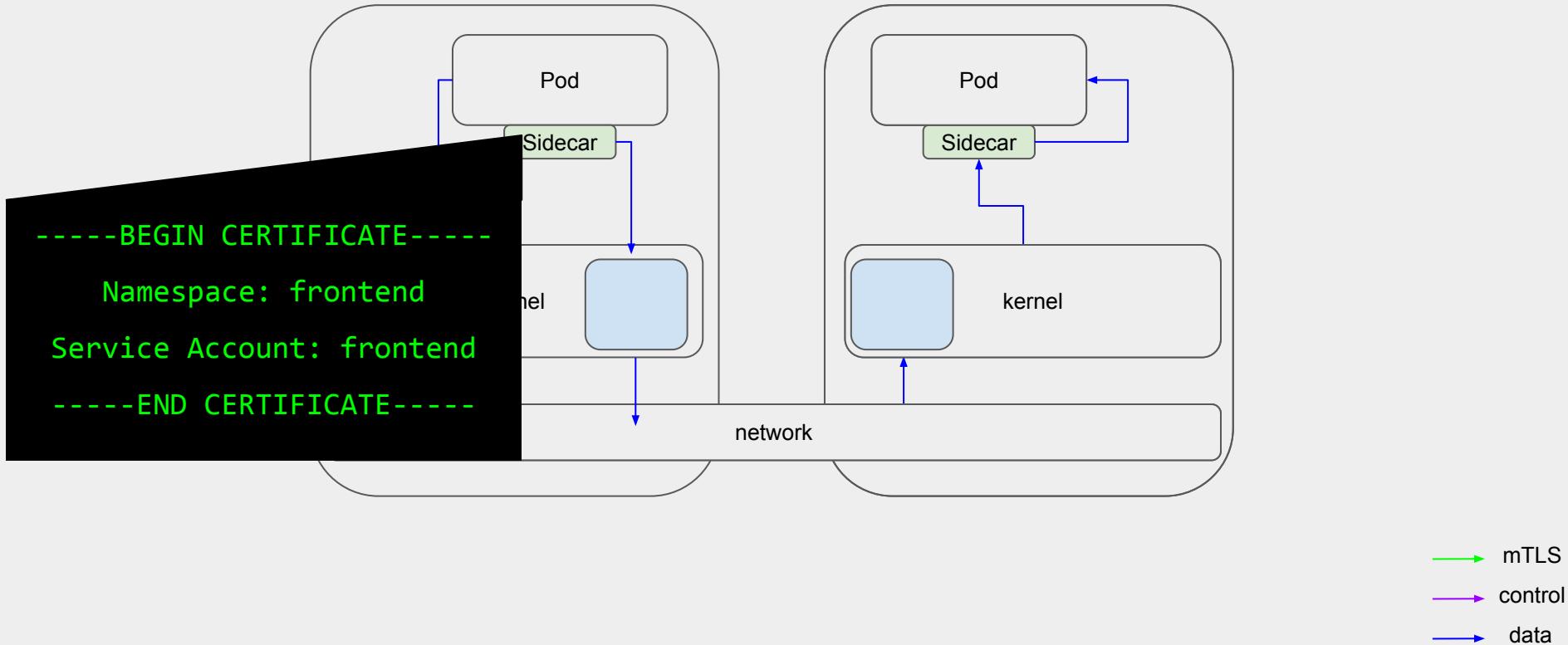
- green → mTLS
- purple → control
- blue → data

Client Cert - how is it secured?

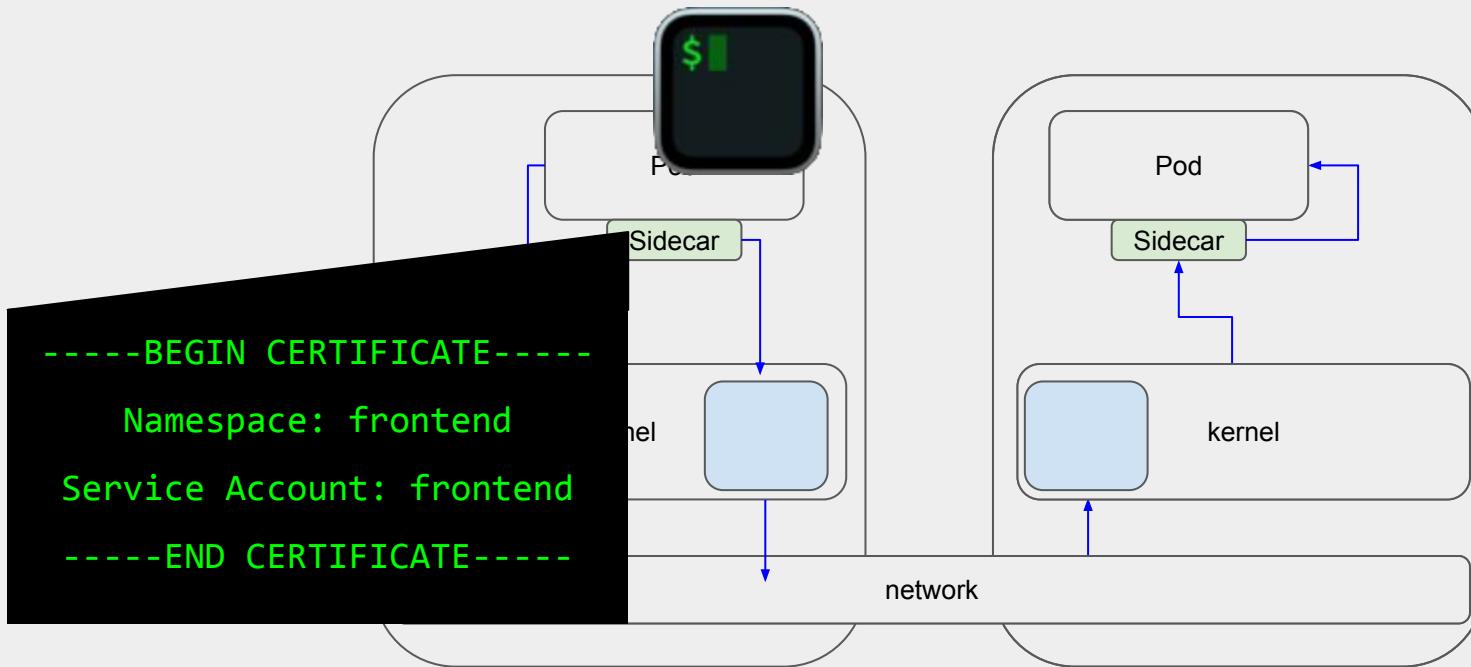
```
-----BEGIN CERTIFICATE-----  
Namespace: frontend  
Service Account: frontend  
-----END CERTIFICATE-----
```

- mTLS
- control
- data

Client Cert - how is it secured?

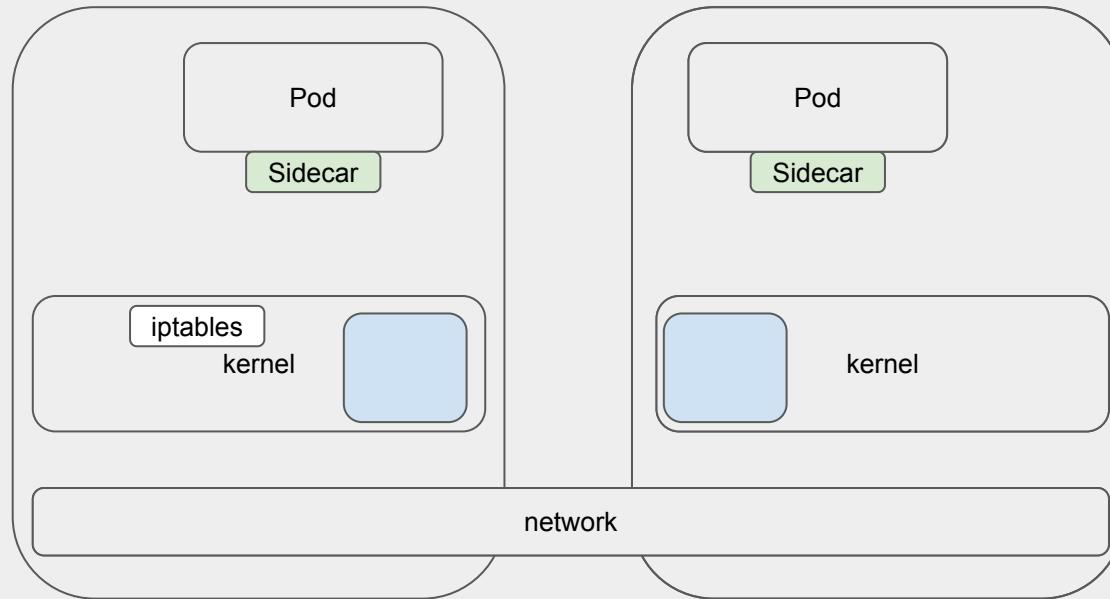


Client Cert - how is it secured?



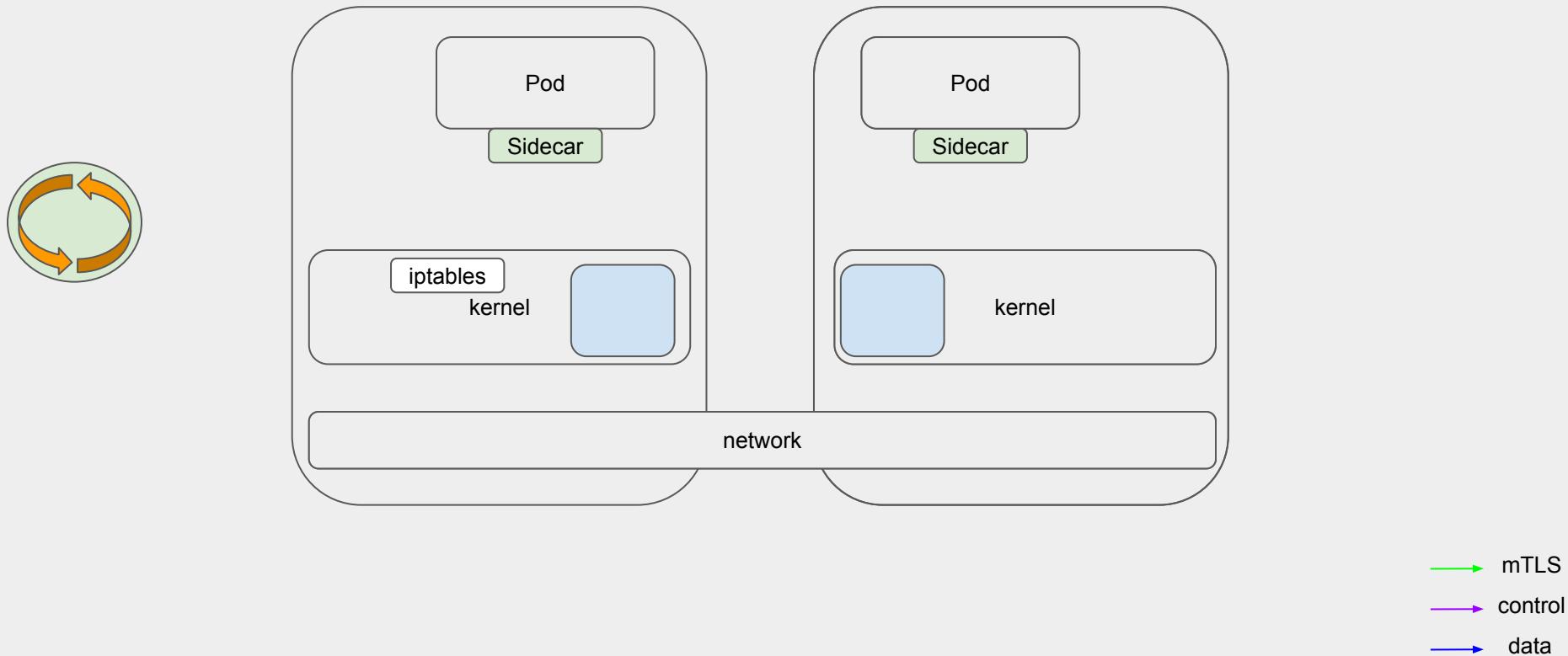
- mTLS
- control
- data

Client Cert - how is it issued?

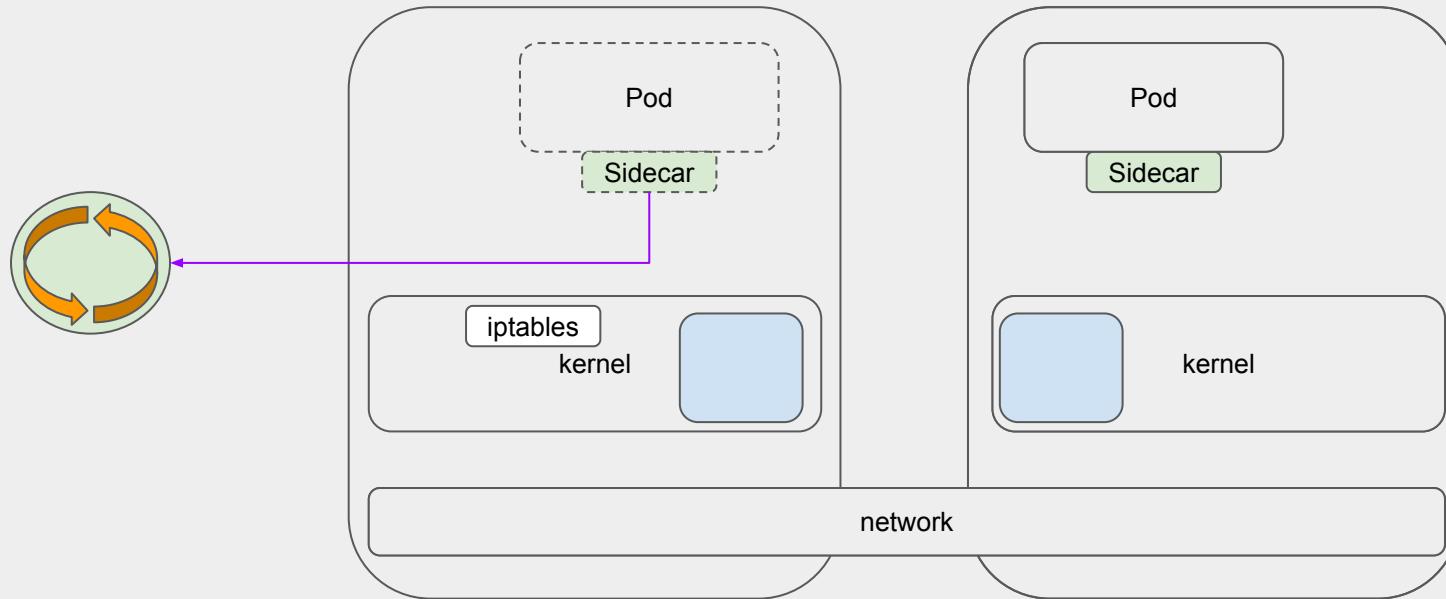


- mTLS
- control
- data

Client Cert - how is it issued?

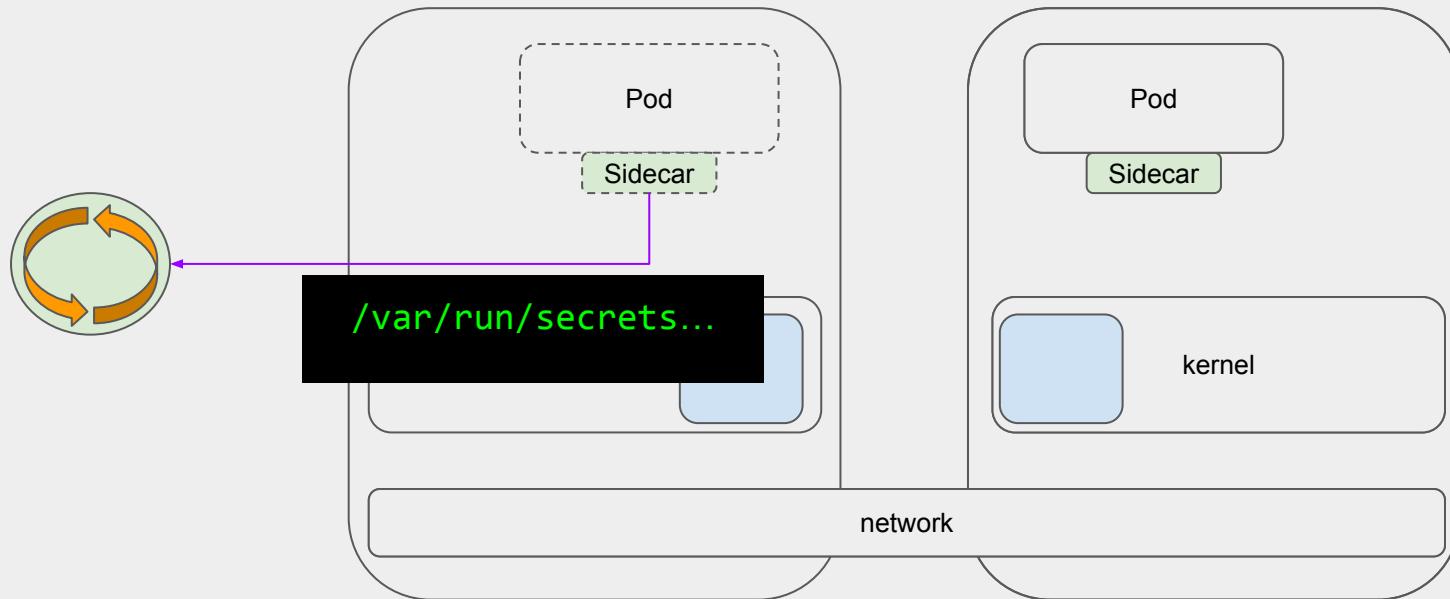


Client Cert - how is it issued?



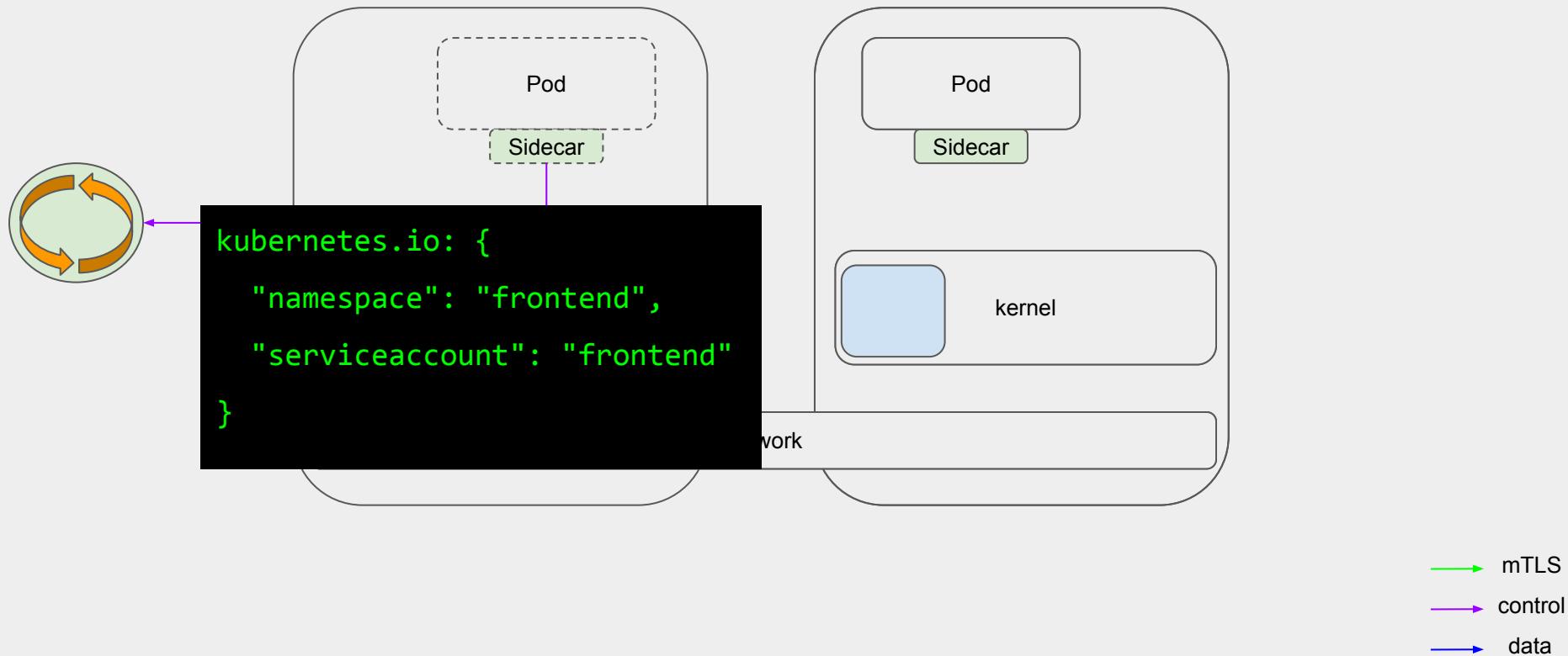
- mTLS
- control
- data

Client Cert - how is it issued?

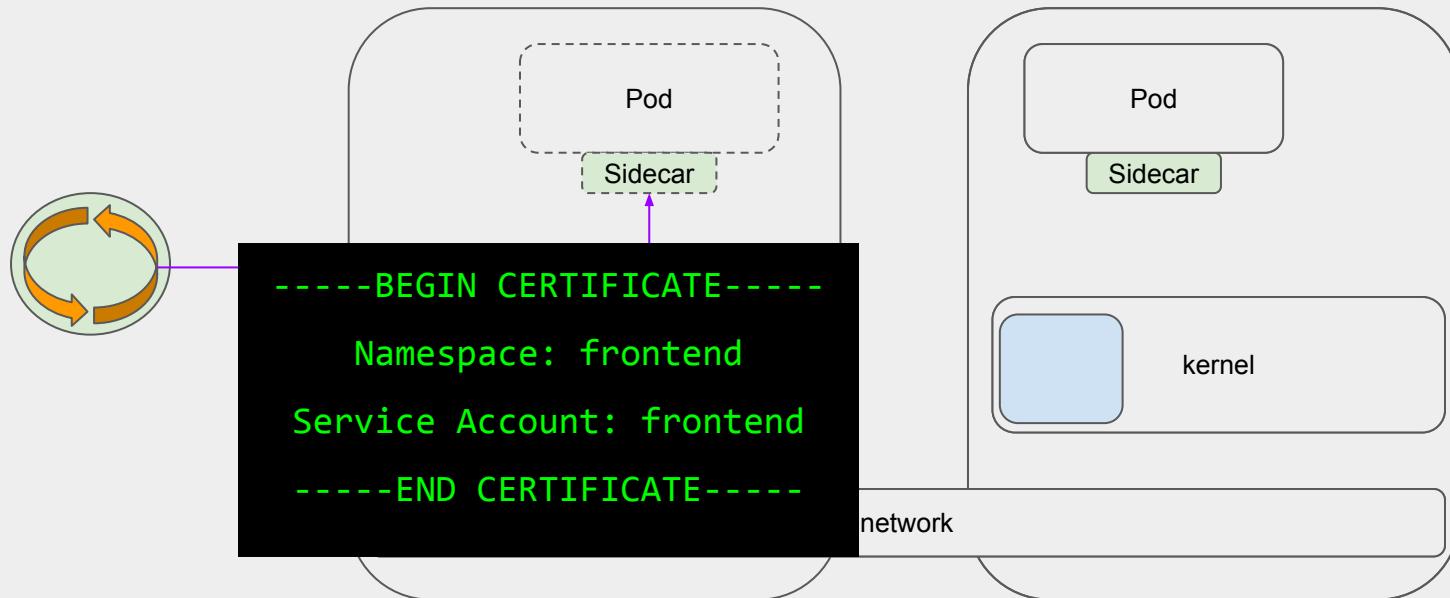


- mTLS
- control
- data

Client Cert - how is it issued?



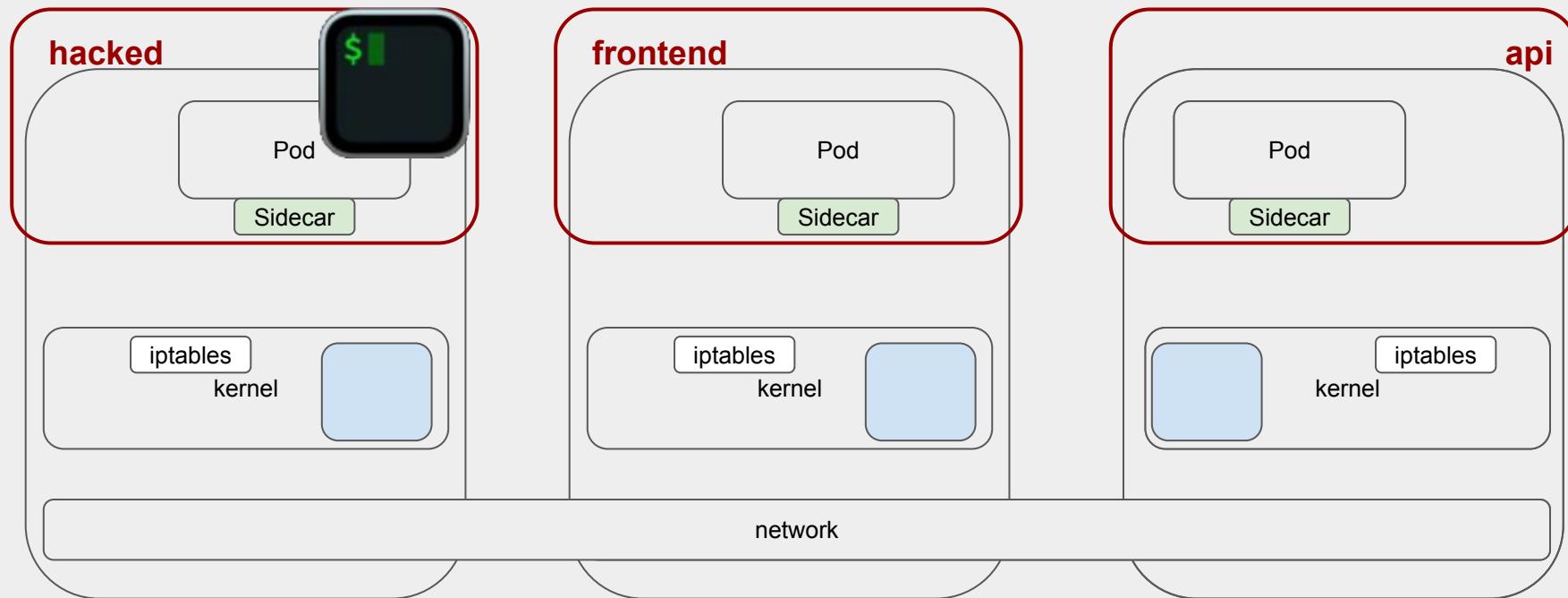
Client Cert - how is it issued?



- mTLS
- control
- data

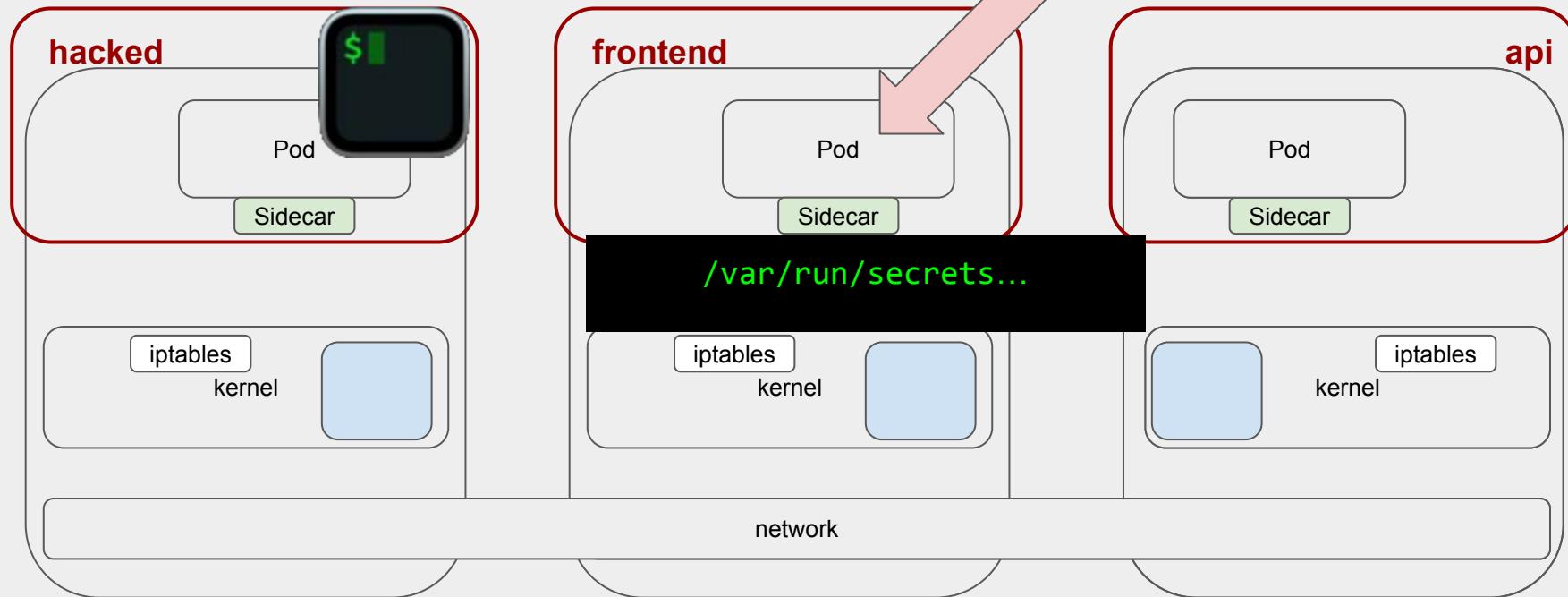
It's time for a
another
contrived
scenario!

Svc Mesh - contrived scenario



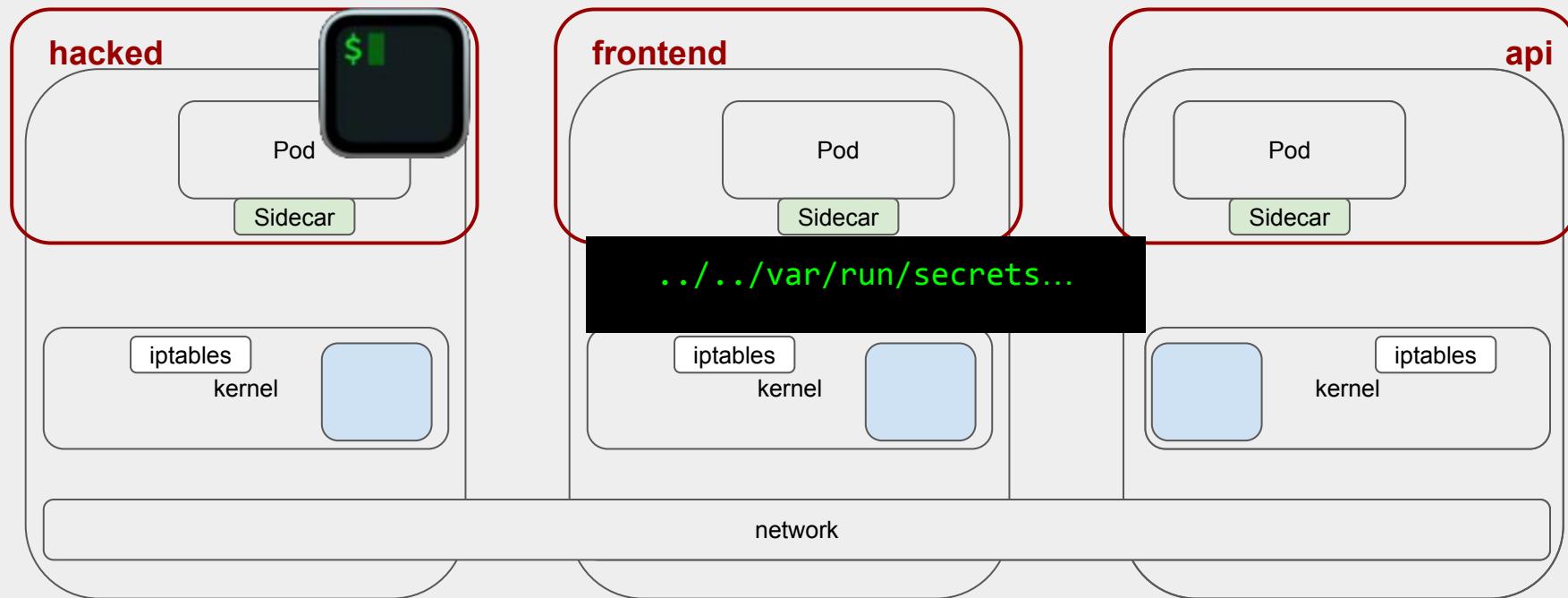
```
$ dear Service Mesh: [pods in frontend] => [pods in api] == OK!
```

Svc Mesh - contrived scenario



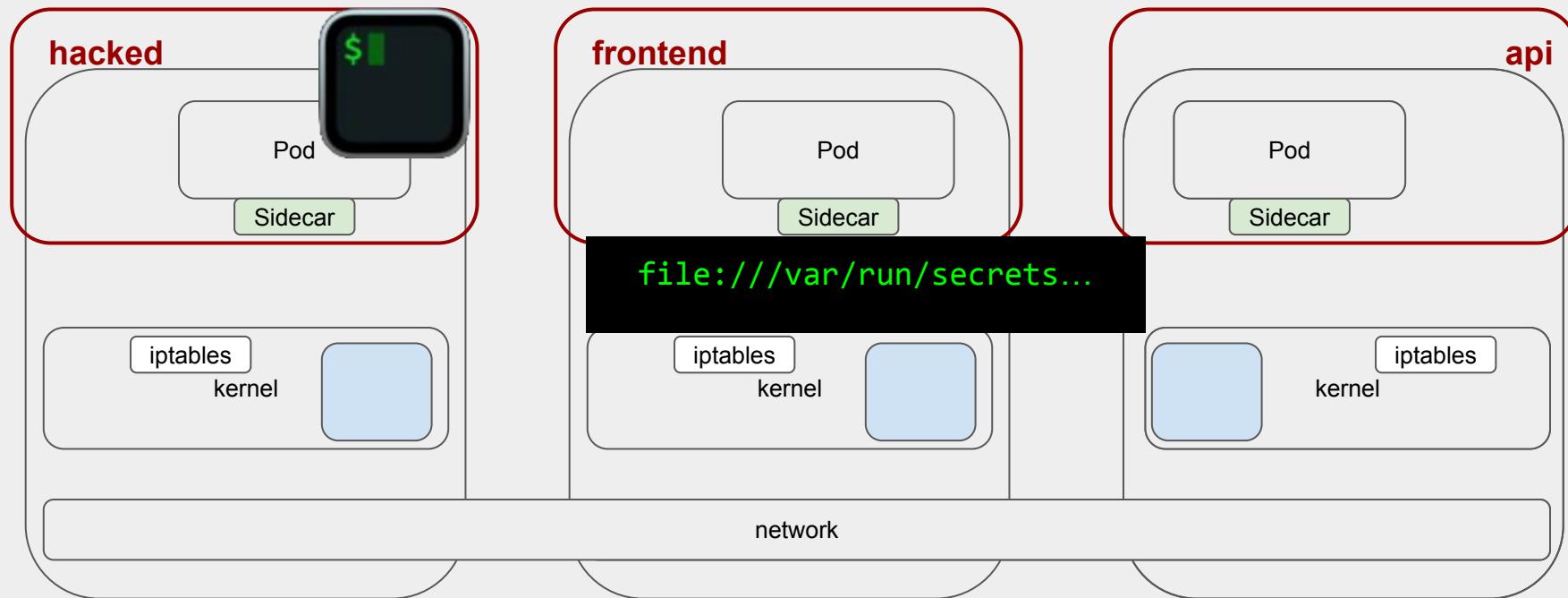
```
$ dear Service Mesh: [pods in frontend] => [pods in api] == OK!
```

Svc Mesh - contrived scenario



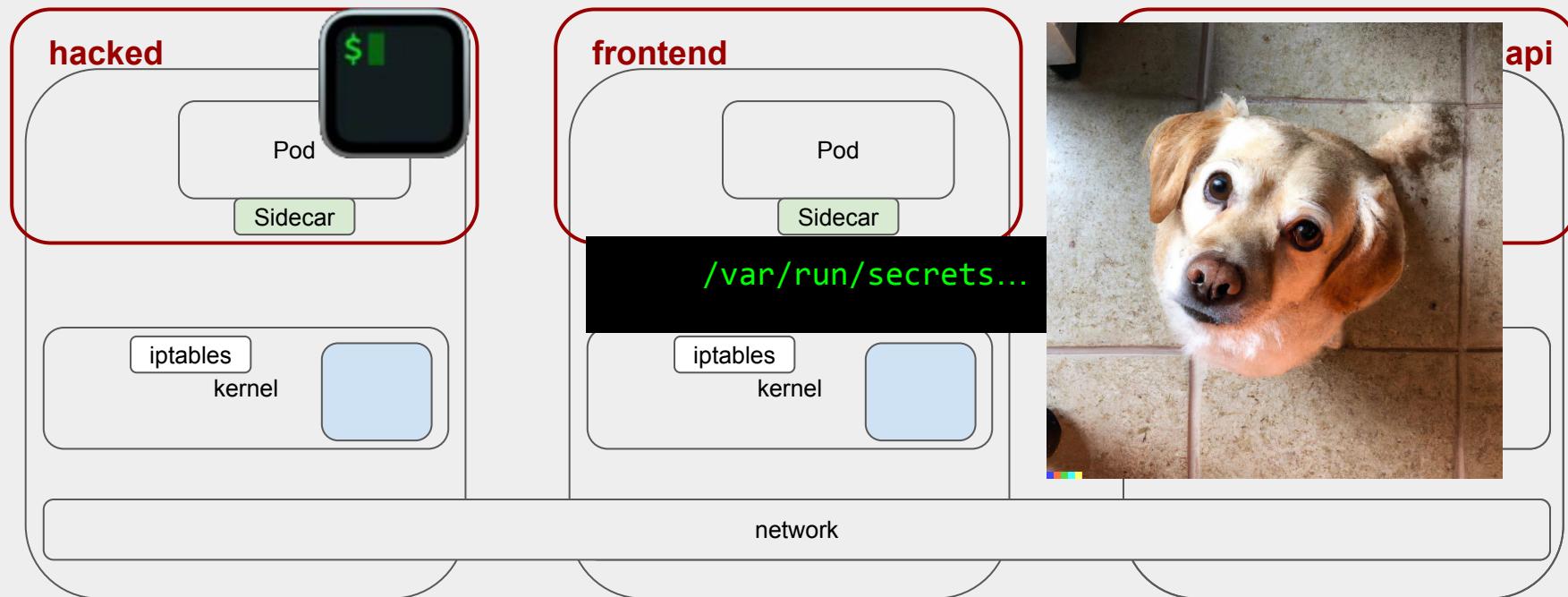
```
$ dear Service Mesh: [pods in frontend] => [pods in api] == OK!
```

Svc Mesh - contrived scenario



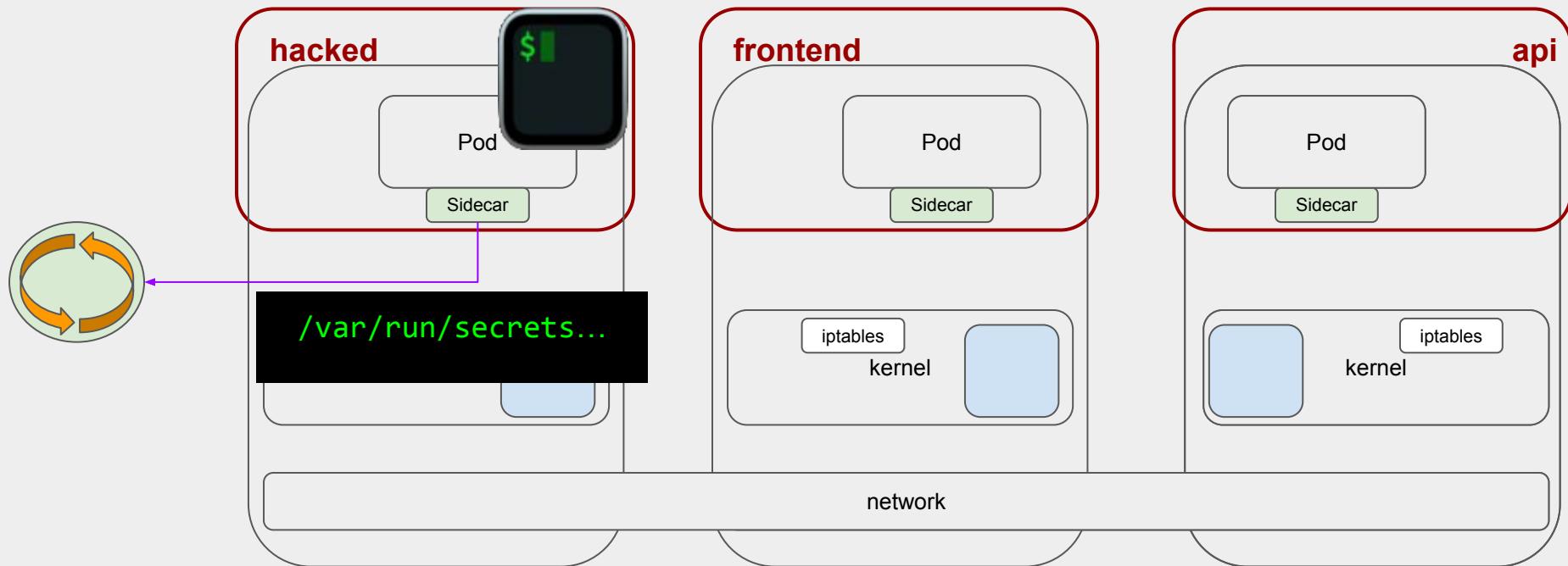
```
$ dear Service Mesh: [pods in frontend] => [pods in api] == OK!
```

Svc Mesh - contrived scenario



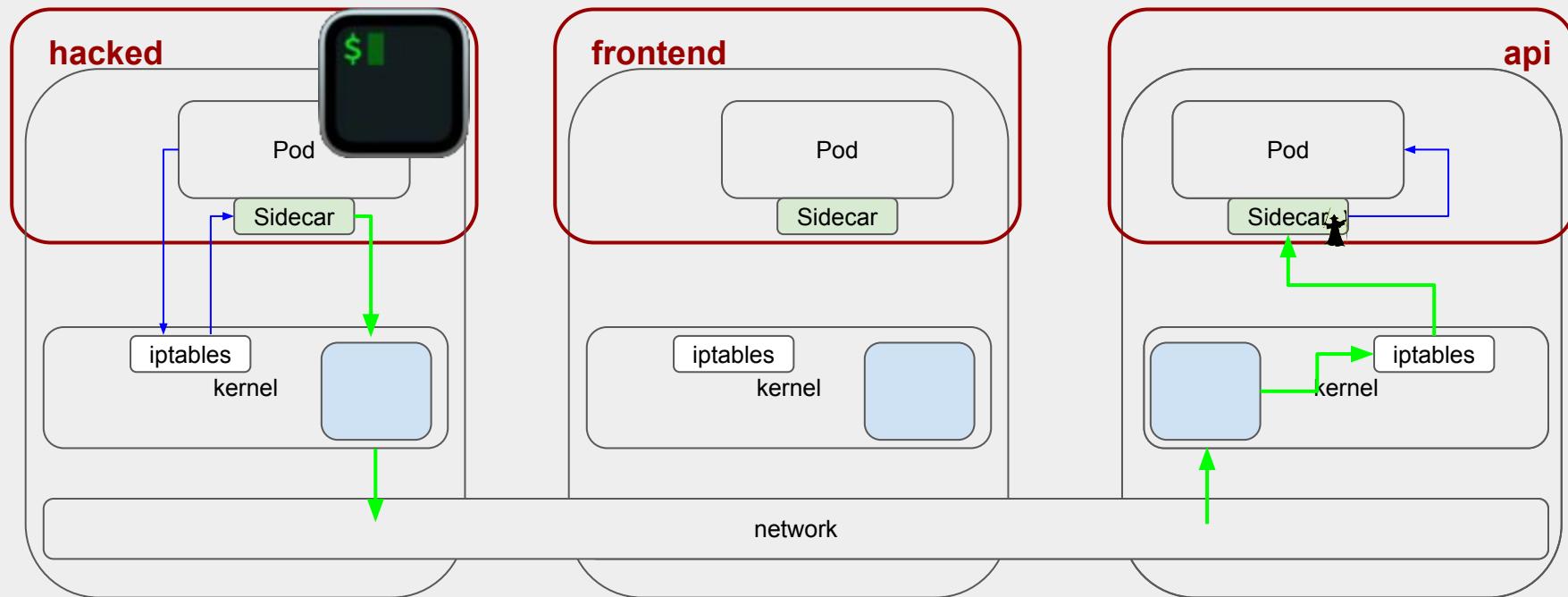
```
$ dear Service Mesh: [pods in frontend] => [pods in api] == OK!
```

Svc Mesh - contrived scenario



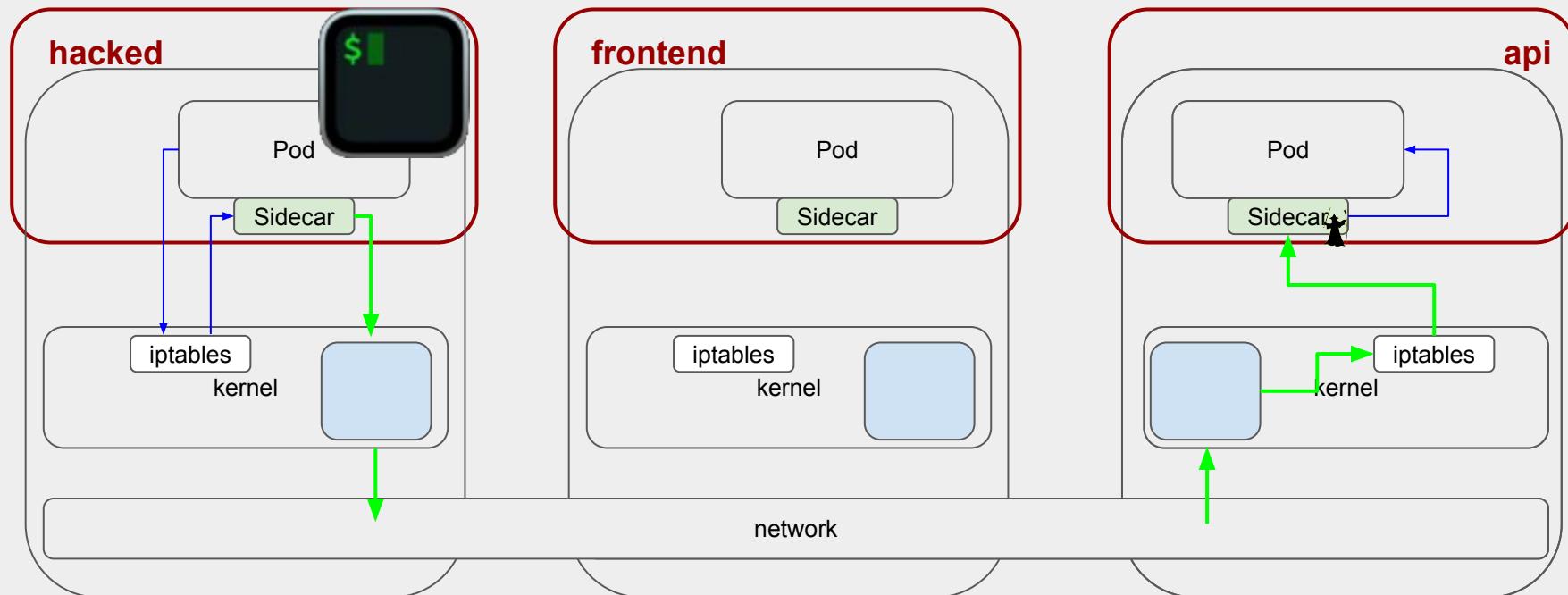
```
$ dear Service Mesh: [pods in frontend] => [pods in api] == OK!
```

Svc Mesh - contrived scenario



\$ dear Service Mesh: [pods in frontend] => [pods in api] == OK!

Svc Mesh - contrived scenario

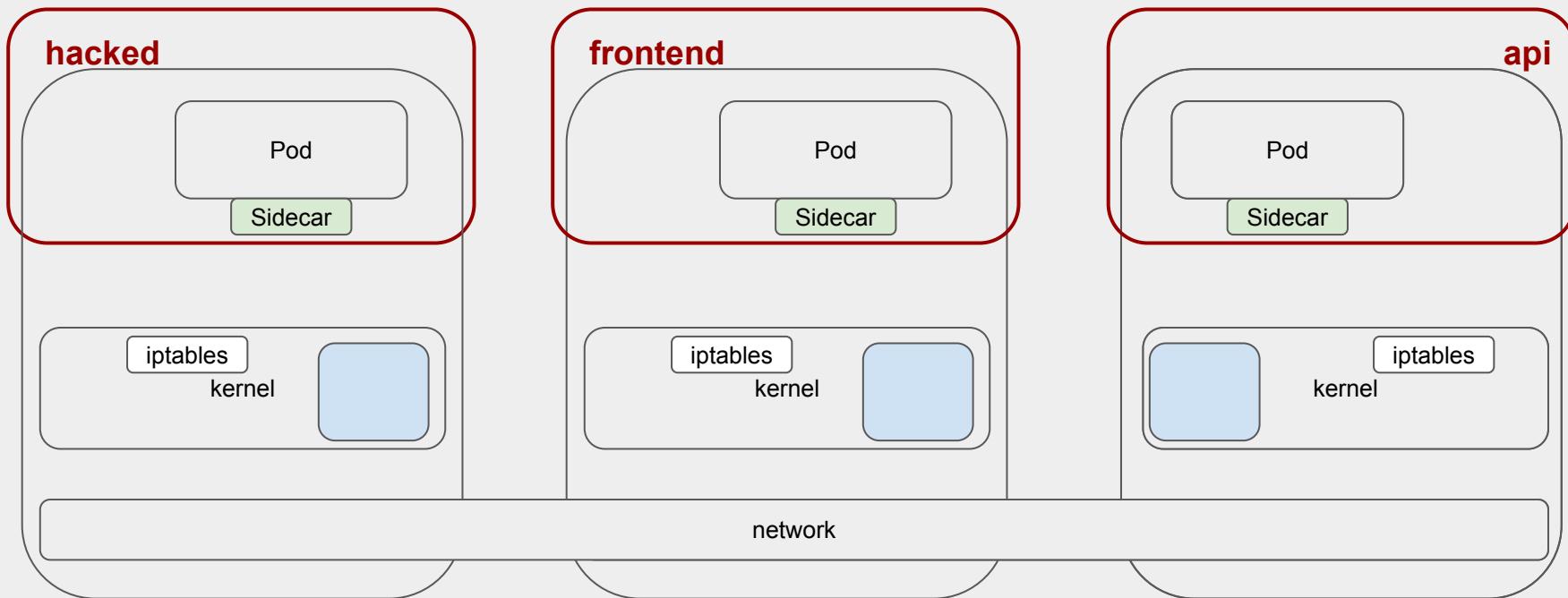


```
$ dear Service Mesh: [pods in frontend] => [pods in api] == OK!
```

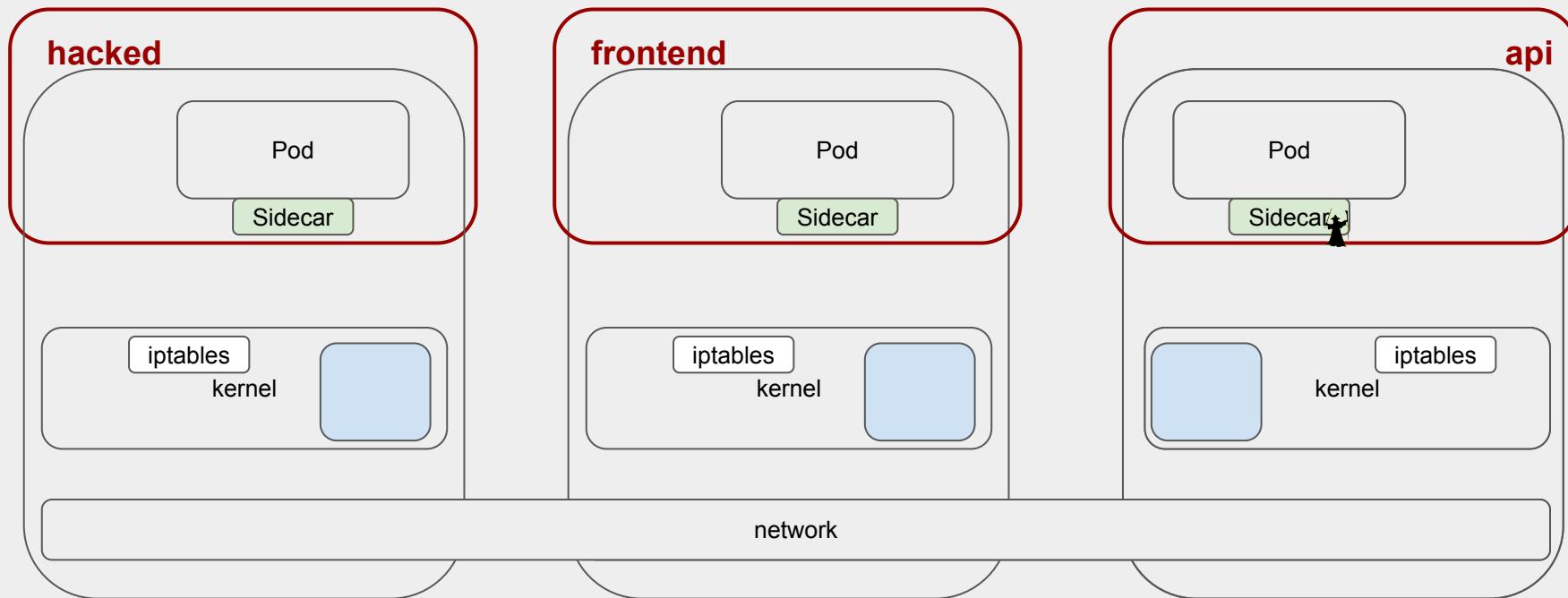
2 mitigations



#1. Right wizard tool, right job.

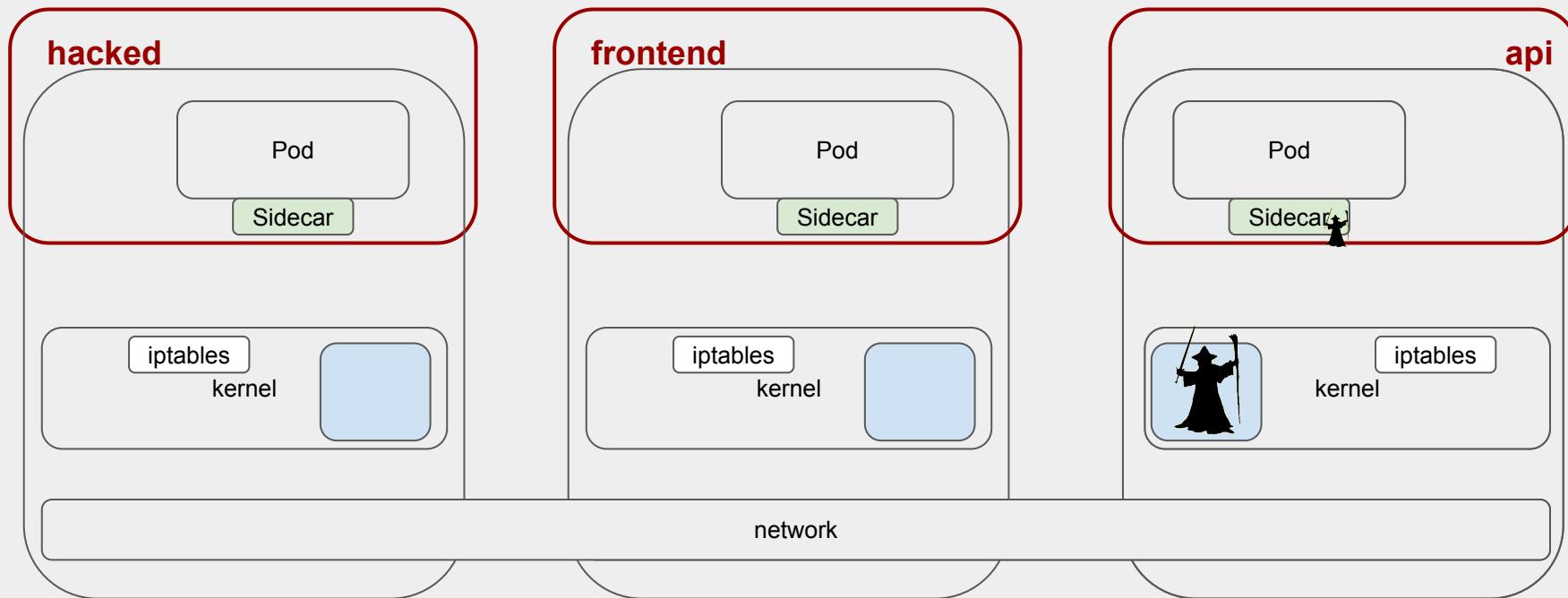


#1. Right wizard tool, right job.



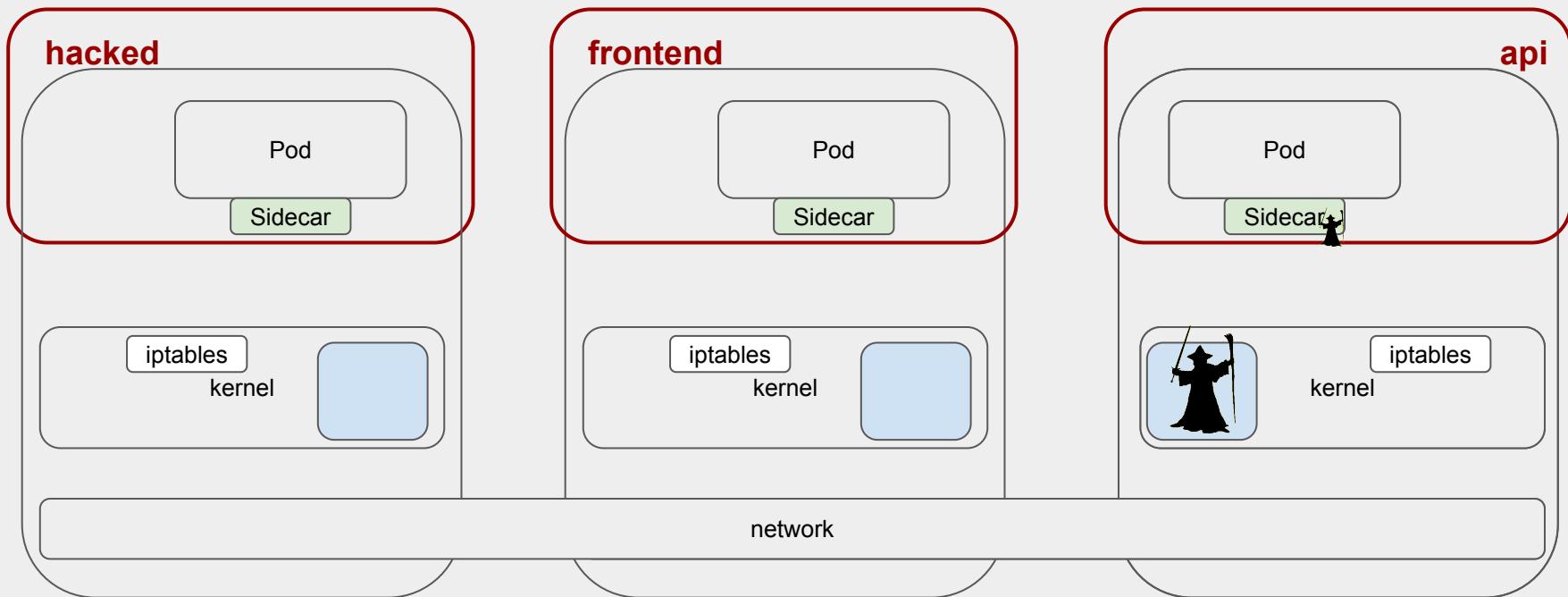
```
$ dear Service Mesh: [pods in frontend] => [pods in api] == OK!
```

#1. Right wizard tool, right job.

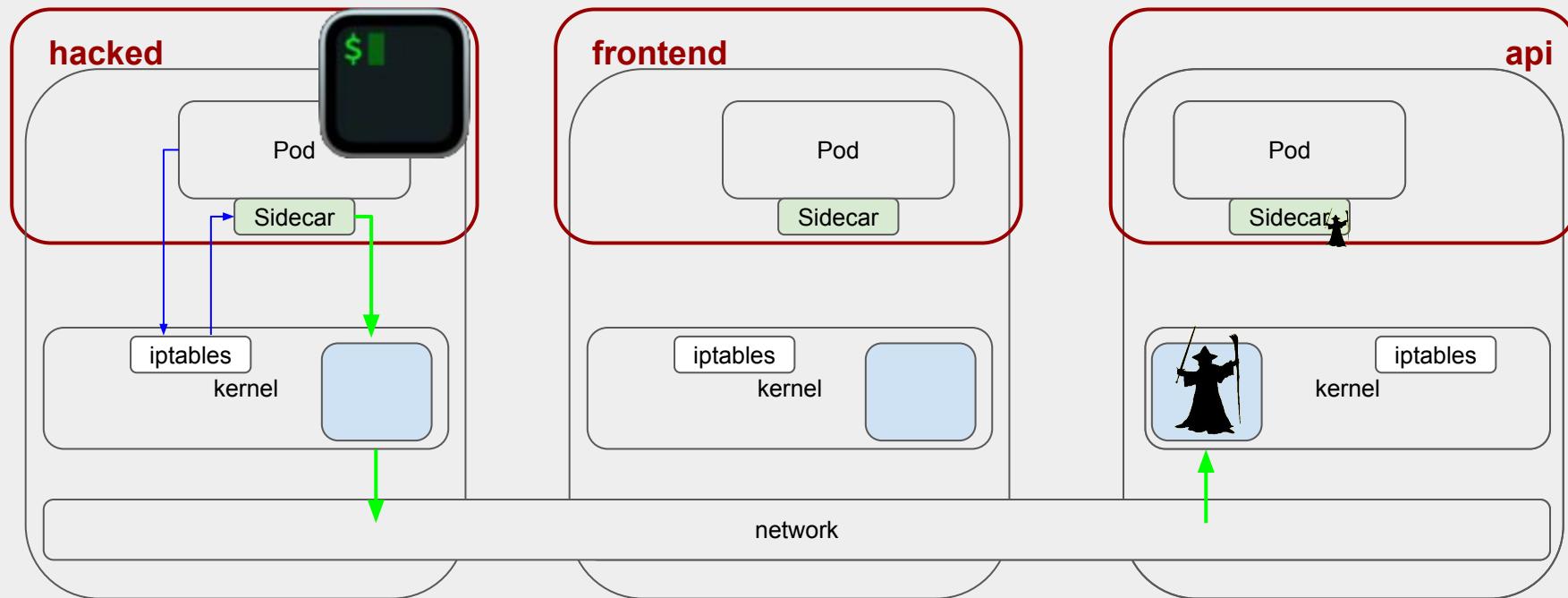


```
$ dear CNI: [pods in frontend] => [pods in api] == OK!
```

#1. Right wizard tool, right job.

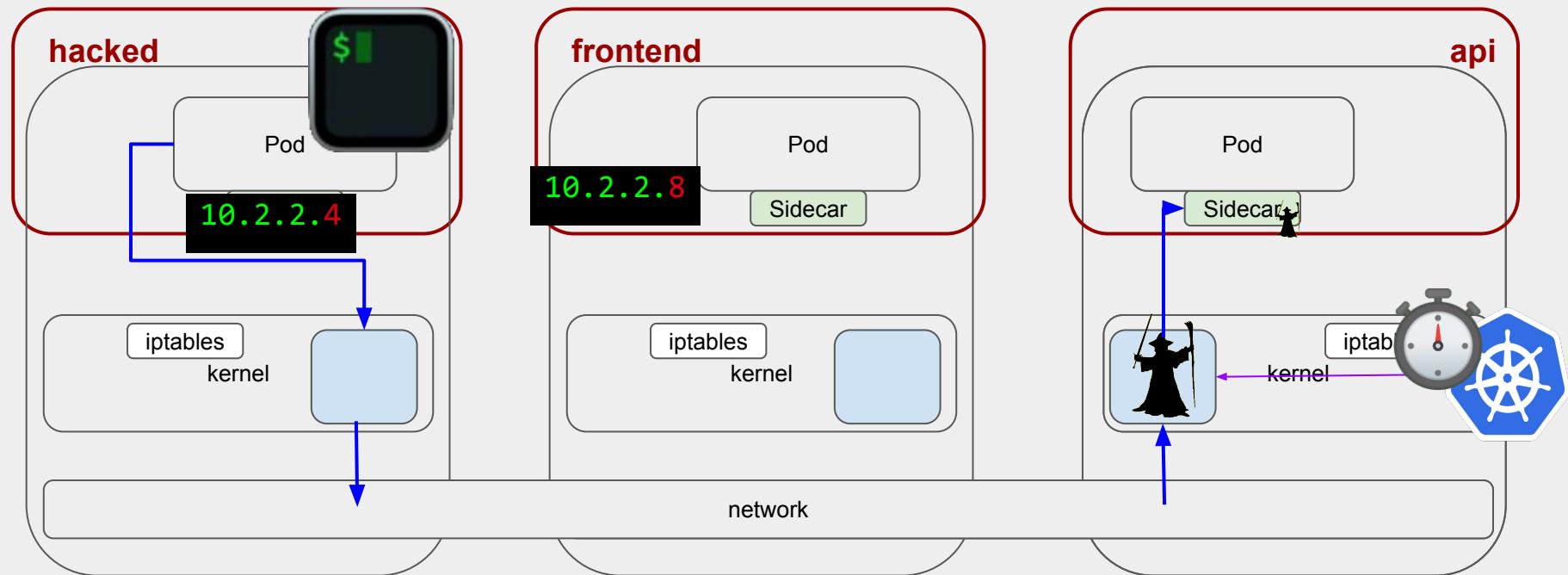


#1. Right wizard tool, right job.



```
$ dear CNI: [pods in frontend] => [pods in api] == OK!
```

#1. Right wizard tool, right job.

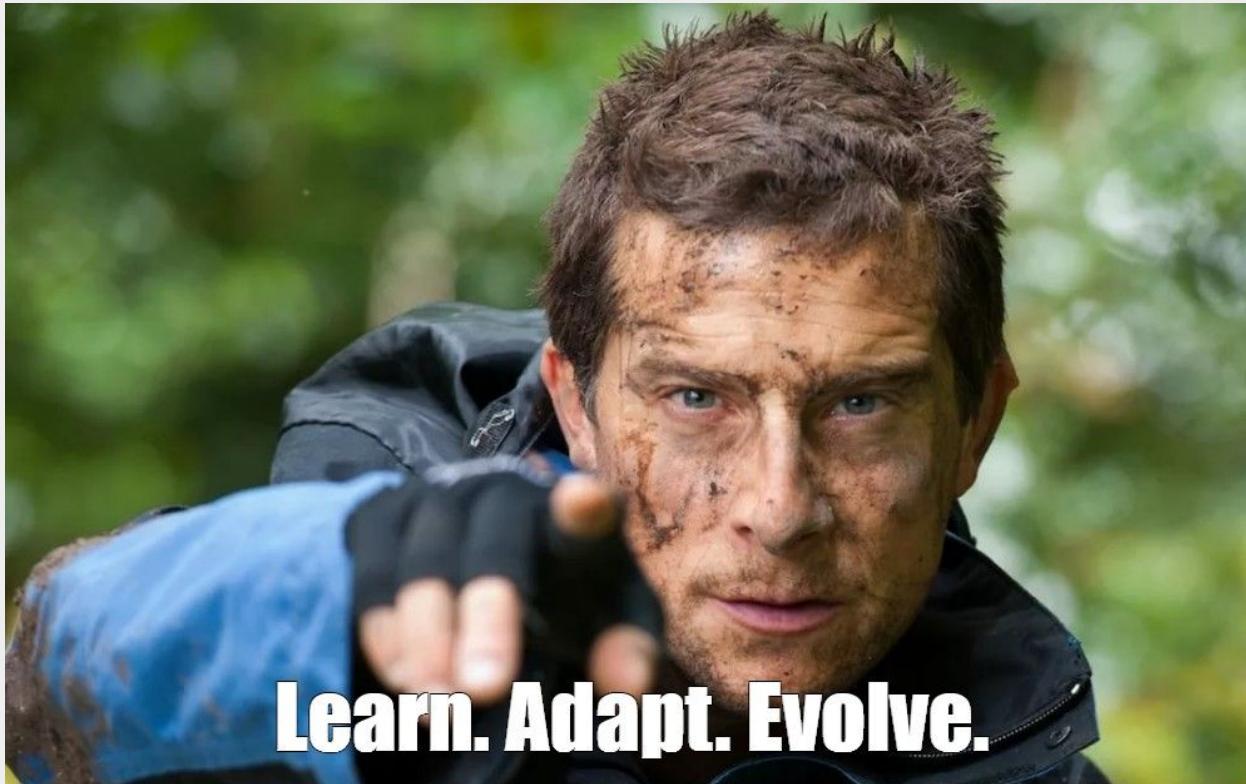


A screenshot of a web browser displaying the Istio website. The browser interface includes standard controls like minimize, maximize, and close buttons, a search bar with the URL 'istio.io', and a tab icon. The main content area shows the Istio logo (a blue sailboat icon) and the word 'Istio'. Below this, a section titled 'Defense in depth with NetworkPolicy' is highlighted in red. A paragraph explains that Istio policies can be layered with Kubernetes Network Policies to enable a strong defense-in-depth strategy. An upward arrow icon is located in the bottom right corner of the content area.

Defense in depth with NetworkPolicy

To further secure traffic, Istio policies can be layered with Kubernetes Network Policies. This enables a strong **defense in depth** strategy that can be used to further strengthen the security of your mesh.

#2. Evolution.



Learn. Adapt. Evolve.

The landscape is changing



The landscape is changing



Istio



The landscape is changing



Istio
Ambient mesh



Ambient Mesh



Ambient Mesh

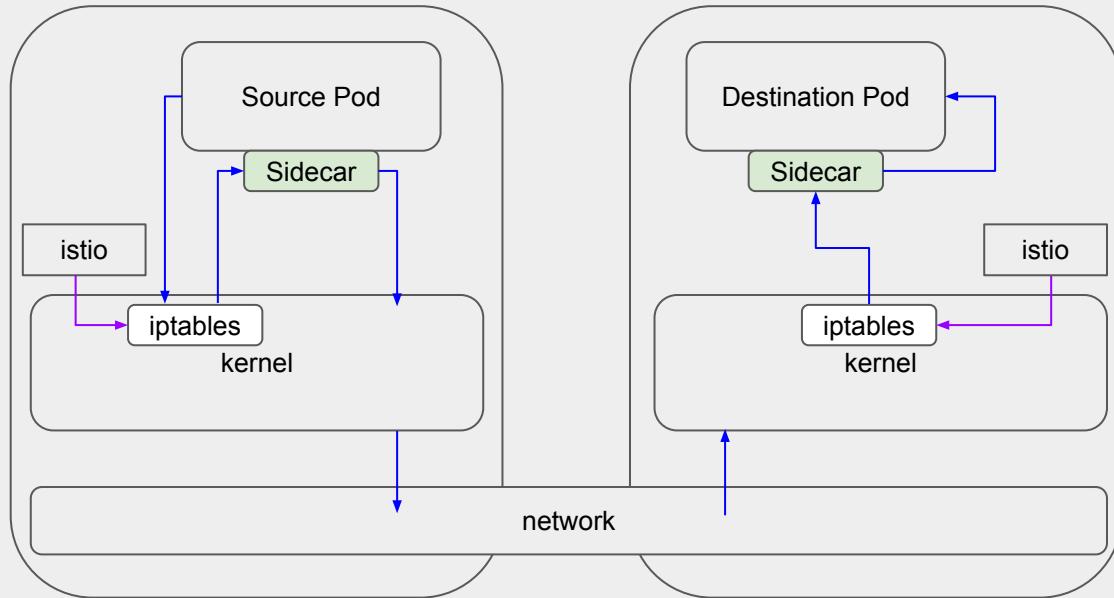
L4 Secure
Overlay

ztunnel

- mTLS,
- Svc-to-svc Authz Policies



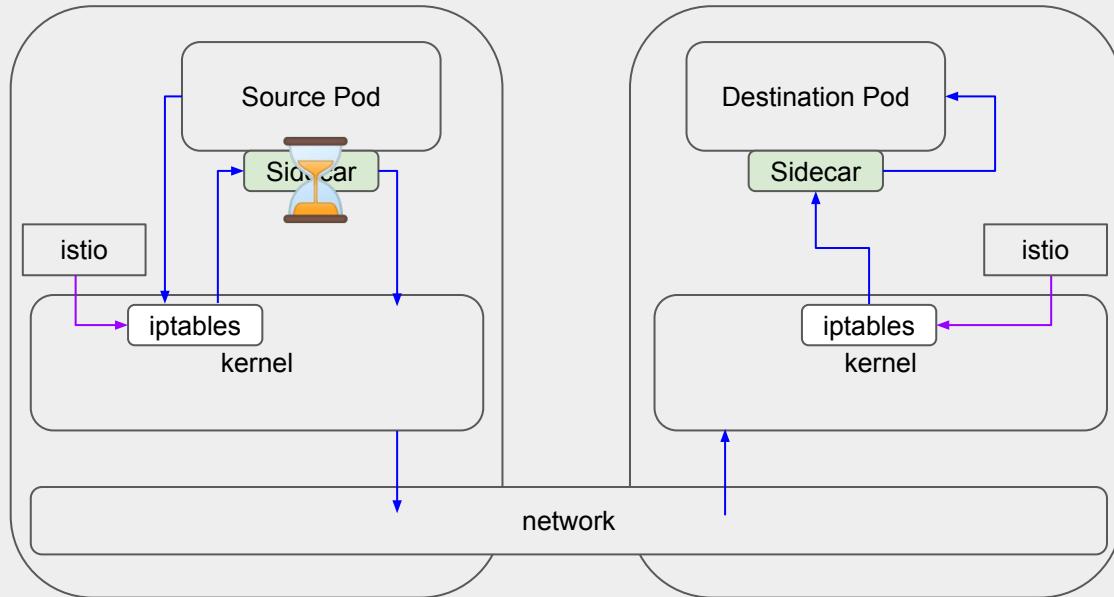
Ambient Mesh



- mTLS
- control
- data



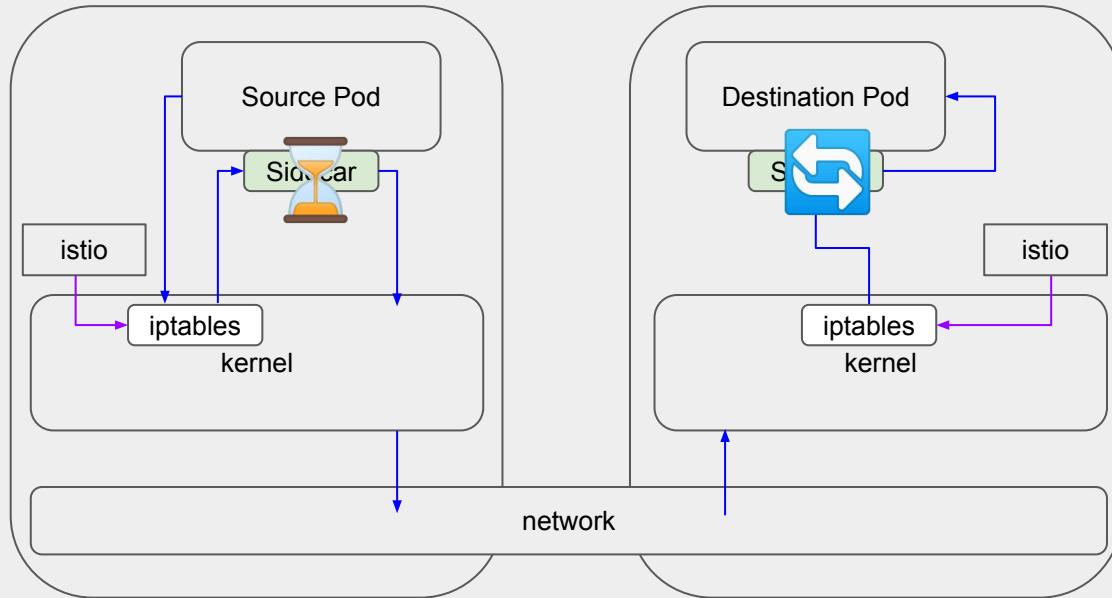
Ambient Mesh



- mTLS
- control
- data



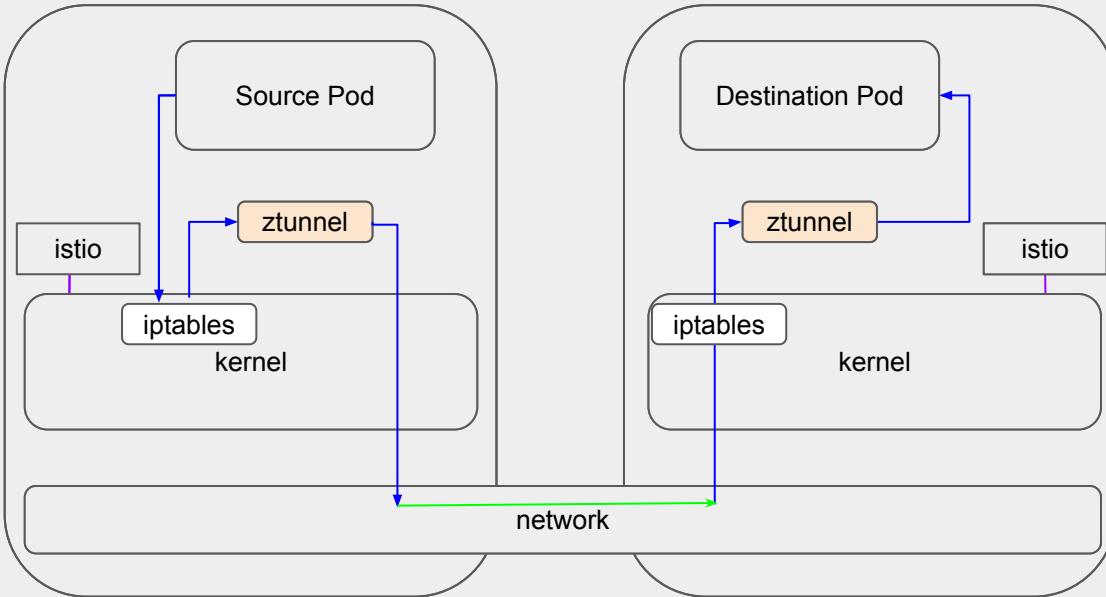
Ambient Mesh



- mTLS
- control
- data



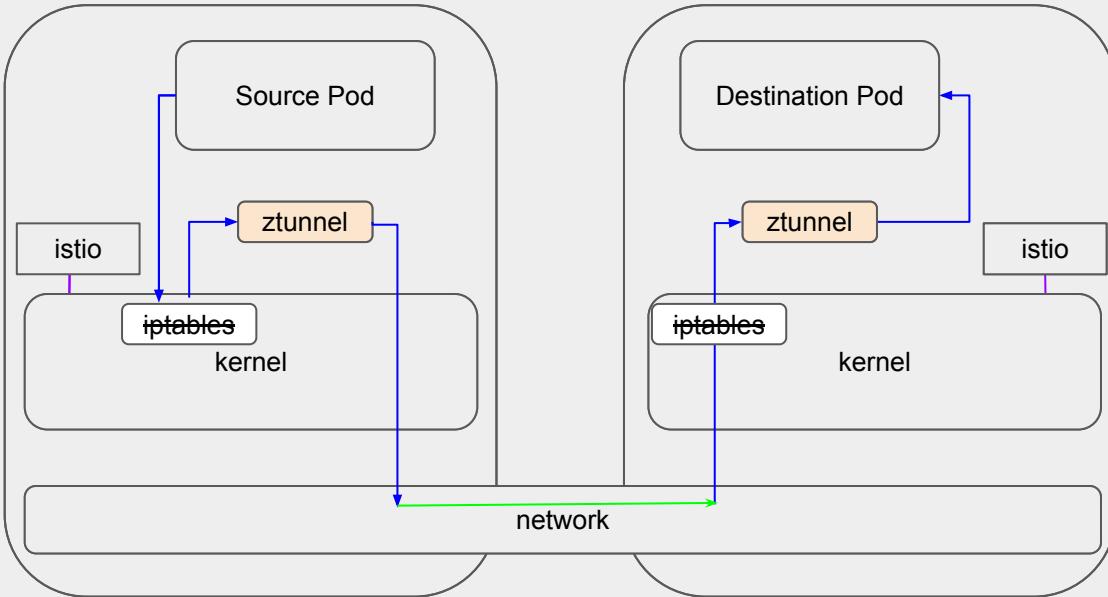
Ambient Mesh



<https://github.com/istio/istio/pull/42372>

- mTLS
- control
- data

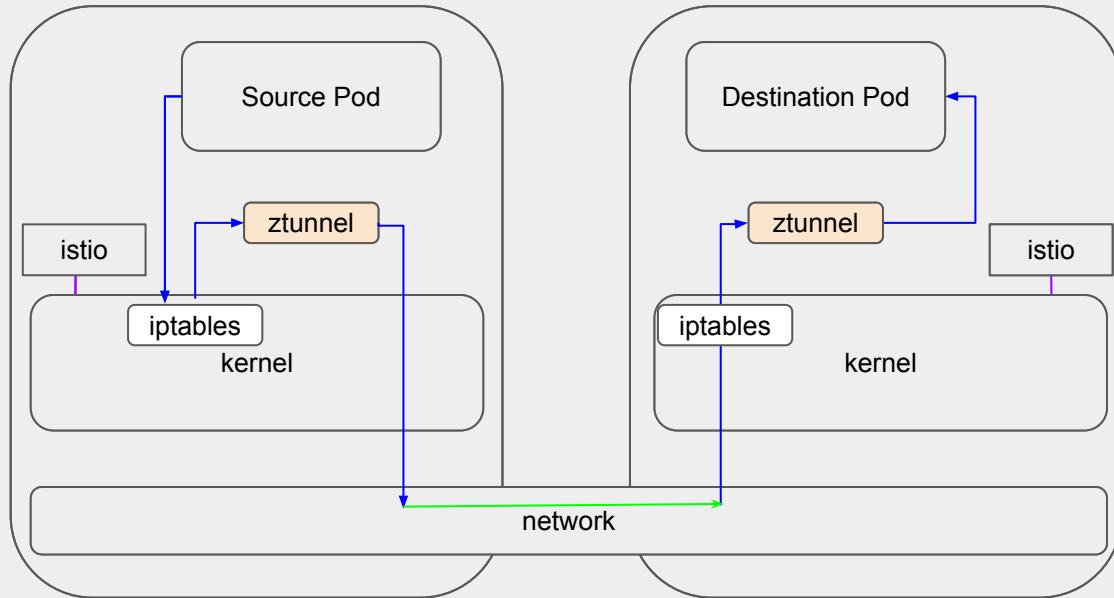
Ambient Mesh



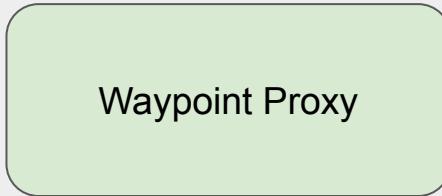
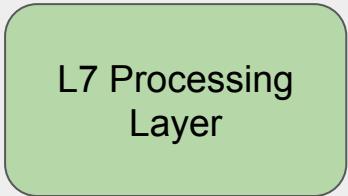
<https://github.com/istio/istio/pull/42372>

- mTLS
- control
- data

Ambient Mesh



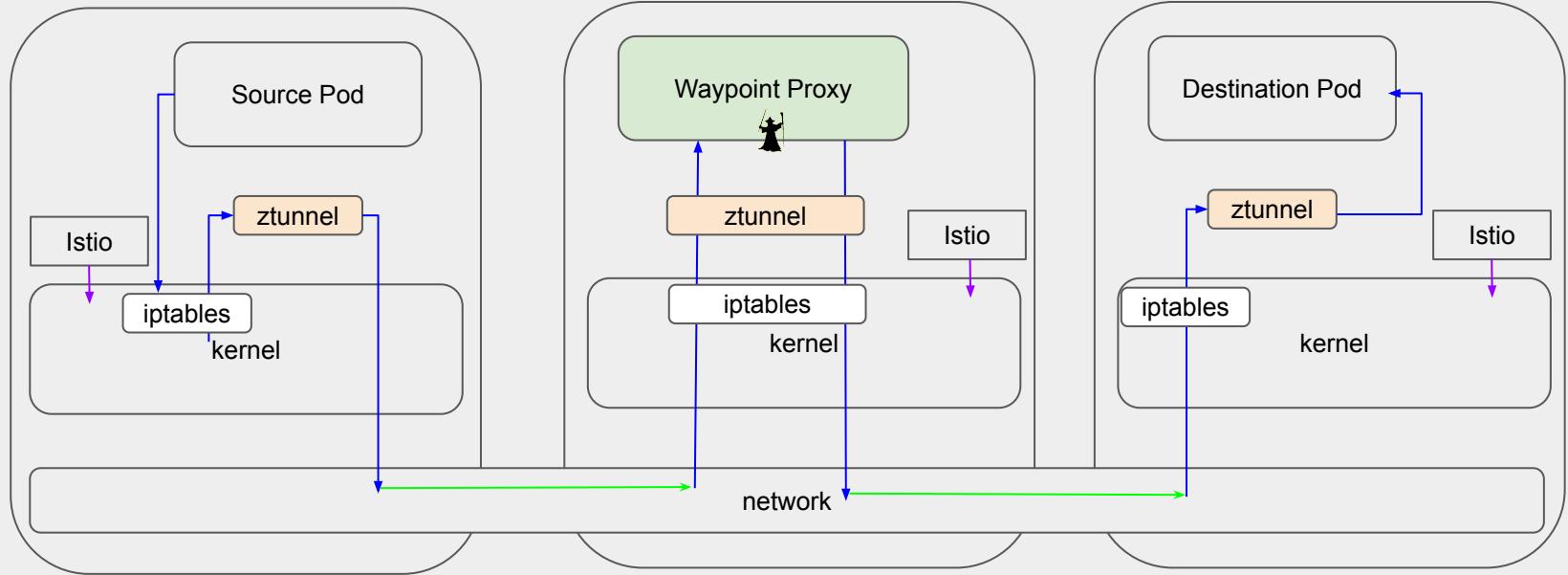
Ambient Mesh



- Rich Authz Policies
- mTLS,
- Svc-to-svc Authz Policies

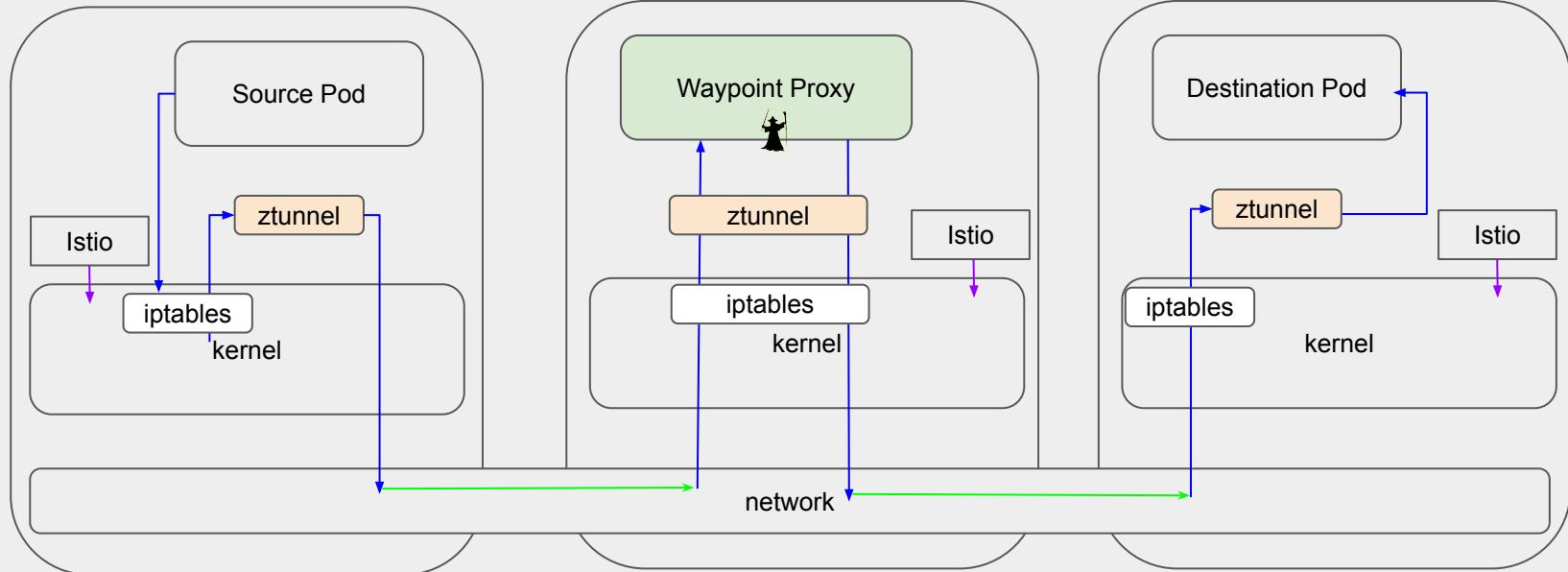


Ambient Mesh



→ mTLS
→ control
→ data

Ambient Mesh



A Packet Eye View of the Istio Ambient Mesh- Justin Pettit, Google & Lin Sun, Solo.io
772 views • 6 months ago

CNCF [Cloud Native Computing Foundation]

A Packet Eye View of the Istio Ambient Mesh- Justin Pettit, Google & Lin Sun, Solo.io While service mesh has been widely ...

Justin Pettit | Challenges With Sidecars - Transparency | Ambient Mesh Datapath Goals | Traditiona... 6 moments



→ mTLS
→ control
→ data



The landscape is changing



Istio
Ambient mode



Cilium



The landscape is changing

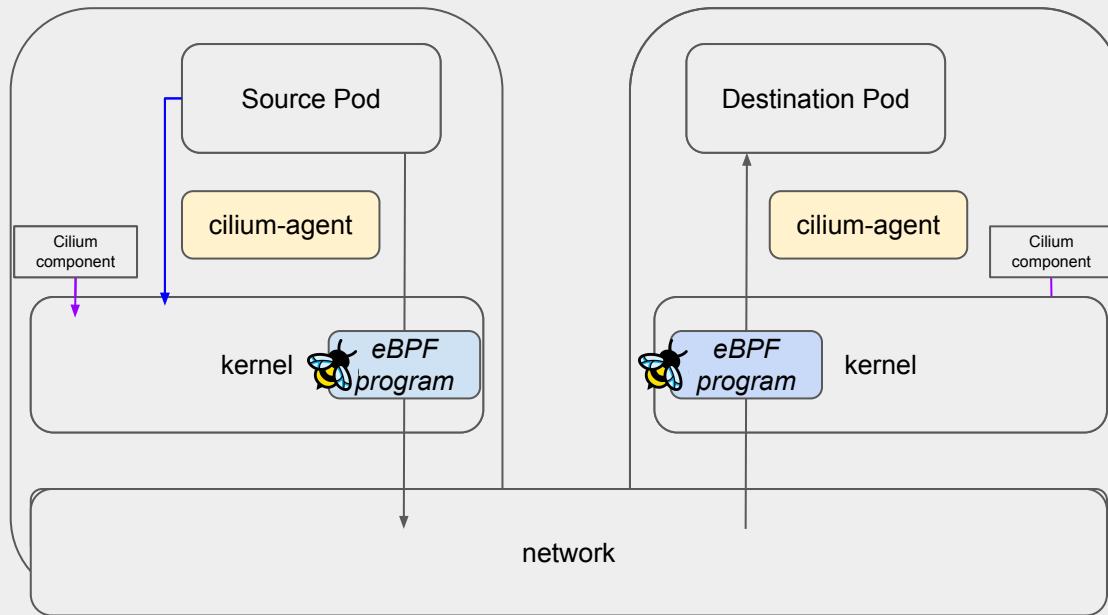


Istio
Ambient mode

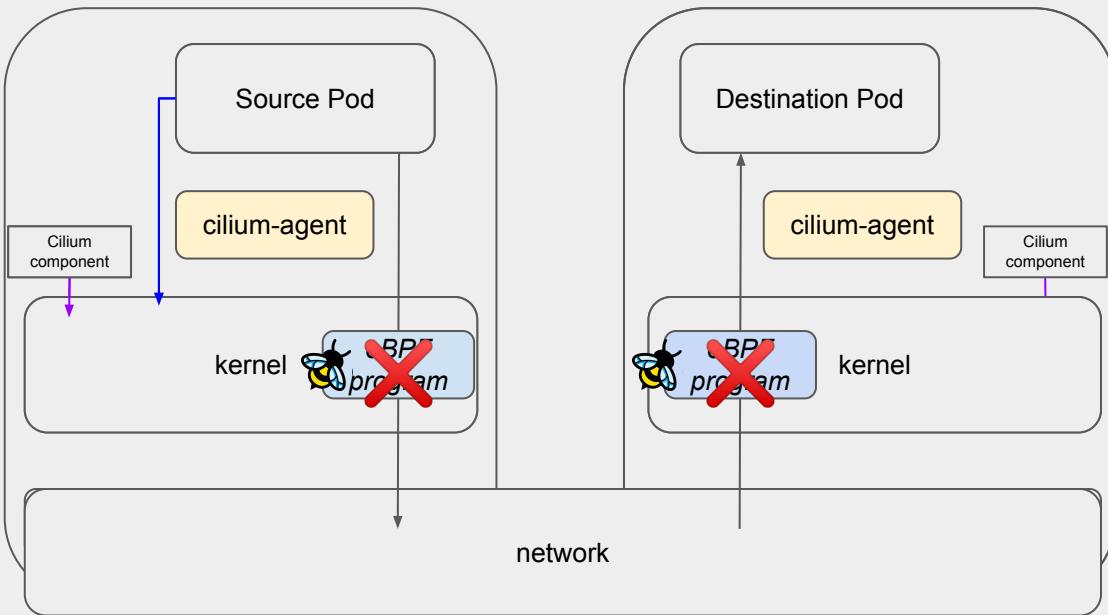


Cilium
Service Mesh

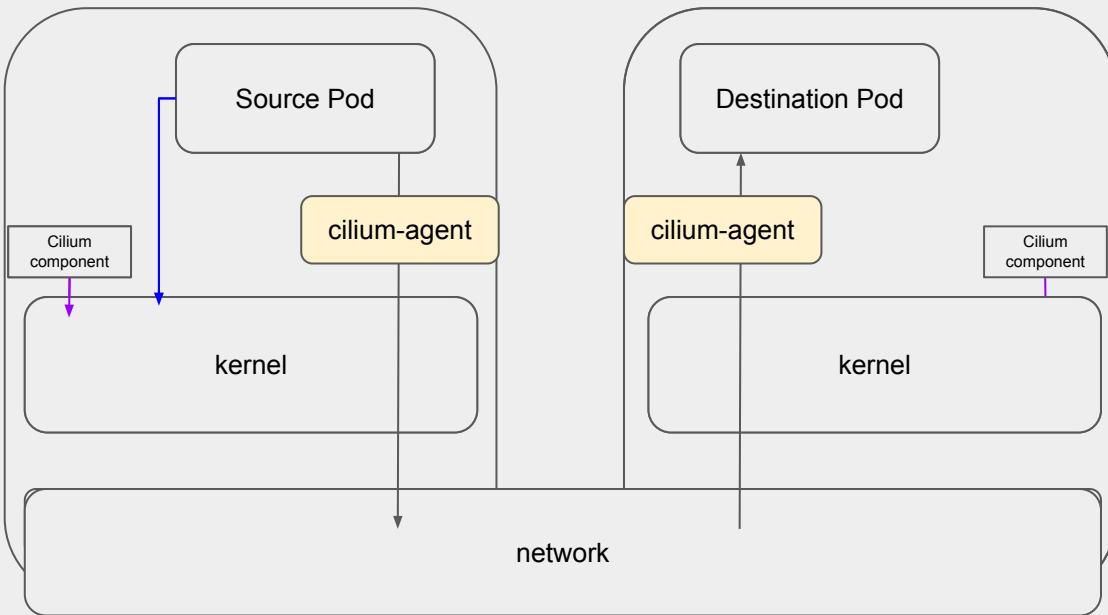
Cilium Service Mesh



Cilium Service Mesh



Cilium Service Mesh



Cilium Service Mesh

- <https://github.com/cilium/cilium/issues/22215>

The screenshot shows a GitHub issue page for the repository `cilium / cilium`. The issue is titled `CFP: Mutual Authentication for Service Mesh #22215`. It is marked as `Open` and has `2 of 7 tasks` completed. The issue was opened by `joestringr` on Nov 16, 2022, with 0 comments. The description states: "This meta issue tracks progress on the Next-Generation Mutual Authentication with Cilium Service Mesh implementation." The tasks listed are:

- Discuss the `CFP` with the community
- Implementation
 - Datapath implementation ([Draft PR](#))
 - SPIFFE integration
 - Automated testing
- Other related work

Assignees: No one assigned. Labels: `kind/feature`, `sig/agent`. Projects: None yet.



The landscape is changing



Istio
Ambient mode



Cilium
Service Mesh

The landscape is changing



converging



Istio
Ambient mode

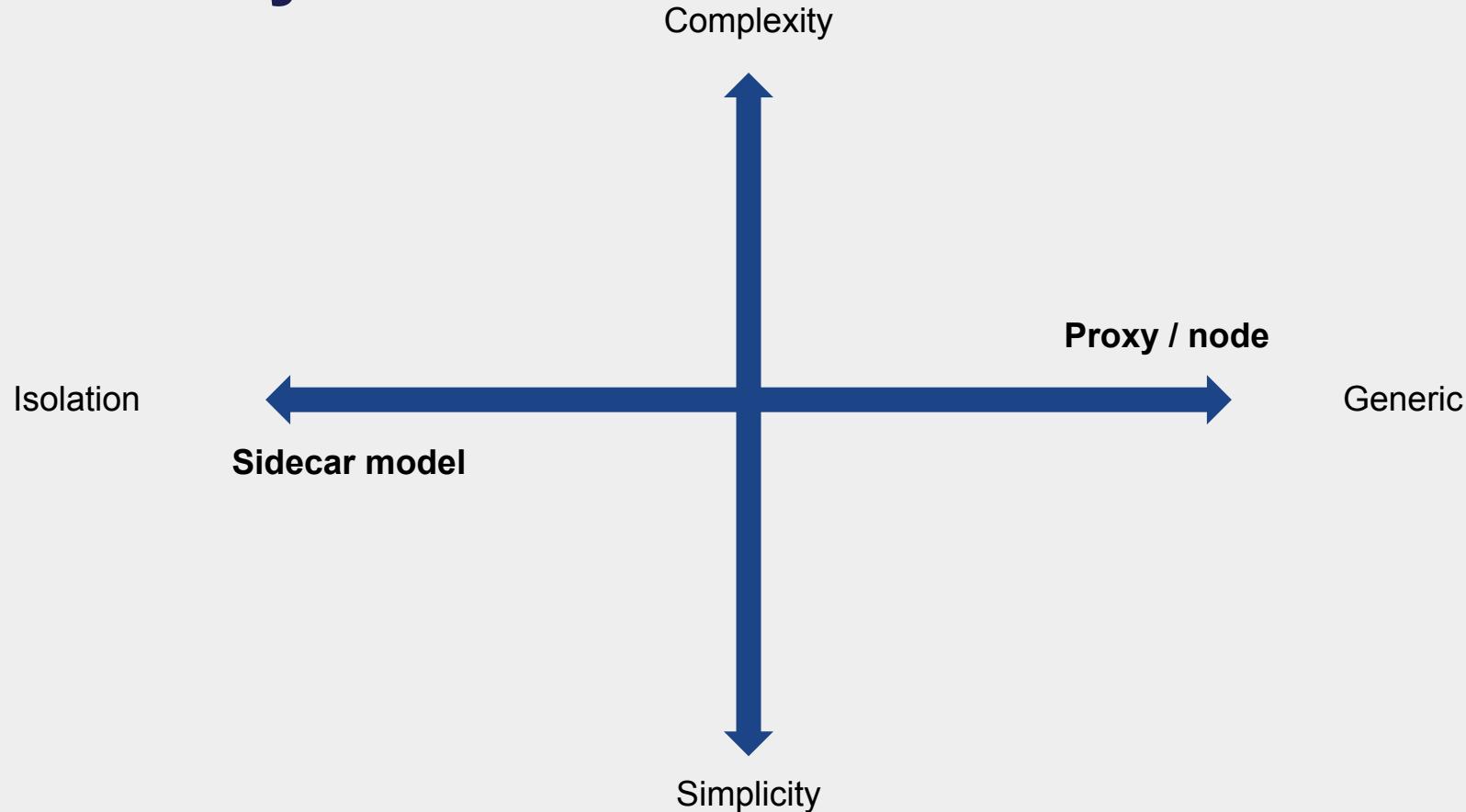


Cilium
Service Mesh

Takeaways



Takeaways



eBPF



eBPF- CNI



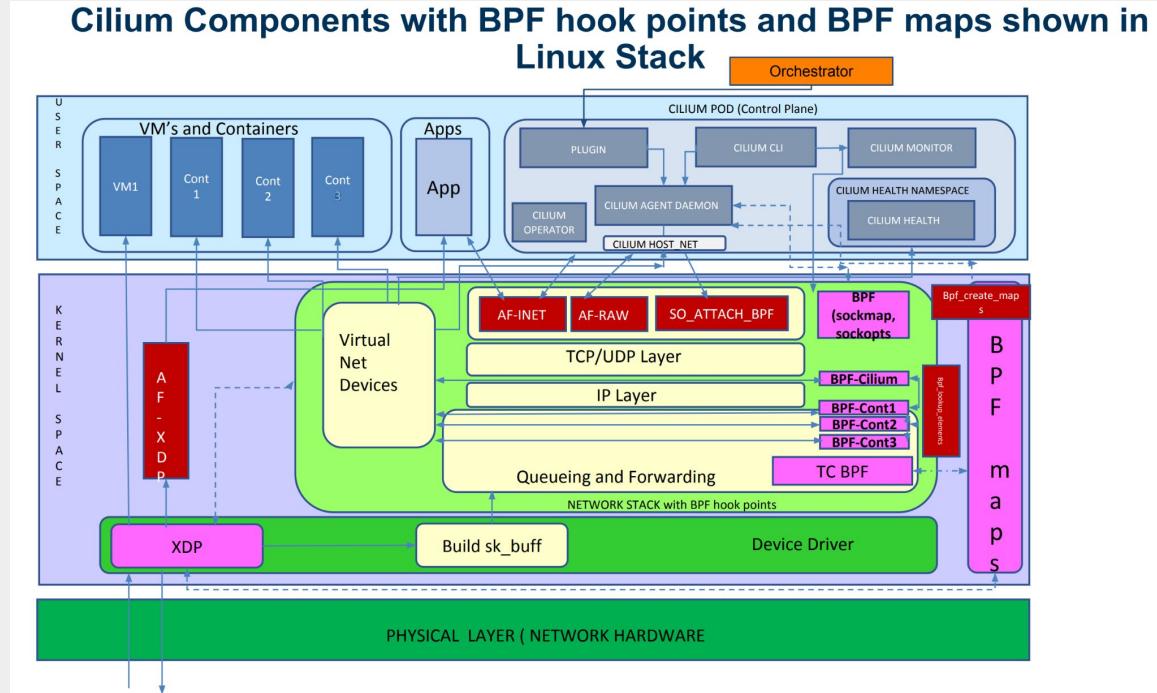
- L3 Observability
- L3 Routing
- L3 Network policy

Replacing iptables with eBPF in Kubernetes with Cilium - bit.ly/3DuNNgt

eBPF



- L3 Observability
- L3 Routing
- L3 Network policy



Replacing iptables with eBPF in Kubernetes with Cilium - bit.ly/3DuNNgt

eBPF



A screenshot of a Twitter thread on a dark-themed interface. The thread is by William Morgan (@wm) and discusses the announcement of sidecar-free @Linkerd using eBPF.

Thread

William Morgan (@wm)

I'm thrilled to announce sidecar-free @Linkerd! In the next release, we will ship a fork of kubectl that uses **#eBPF** to remove references to linkerd-proxy from its output. This allows us to shift L7 processing "down" into underlying infrastructure, using the magic of eBPF! ✨

4:42 PM · Oct 3, 2022

52 Retweets 16 Quote Tweets 405 Likes

New to Twitter?

Sign up now to get your own personalized timeline!

[Sign up with Google](#)

[Sign up with Apple](#)

[Create account](#)

By signing up, you agree to the [Terms of Service](#) and [Privacy Policy](#), including [Cookie Use](#).

Relevant people

Takeaways



Takeaways



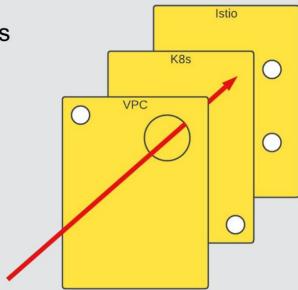
Takeaways



Takeaways

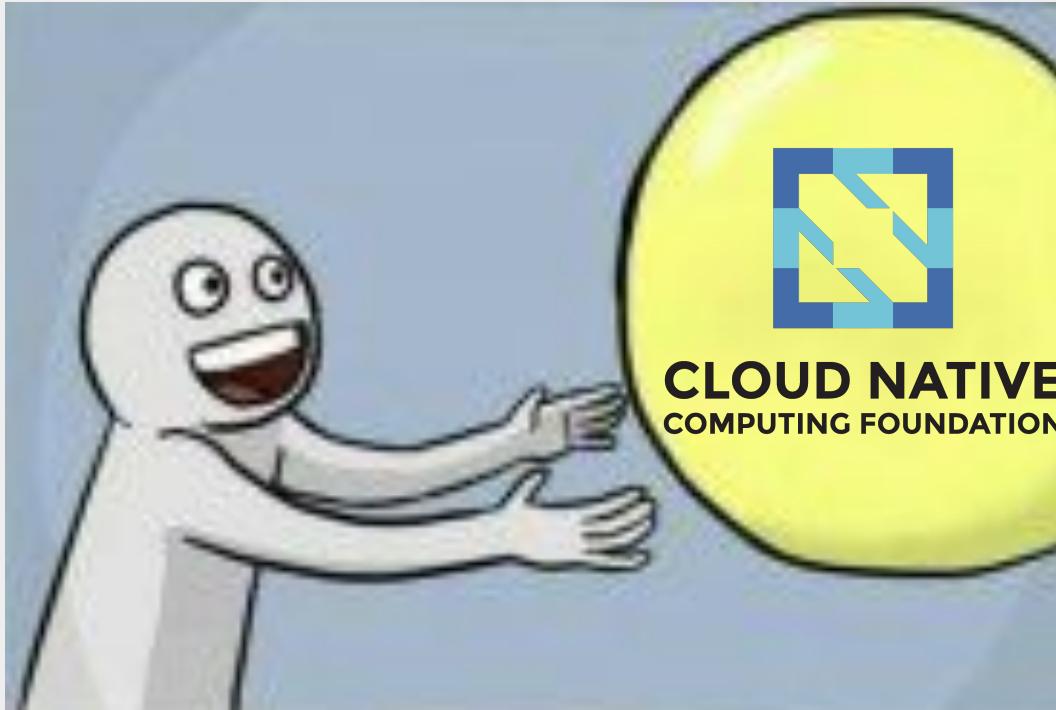


- **Self-service platforms are hard**
 - Safeguards to avoid users shooting themselves in the foot
 - Provide a Golden Path to avoid configuration errors
- **Defense in depth:** Add redundant security at all layers
- **Observability is key**
 - Help debug
 - Detect misconfiguration

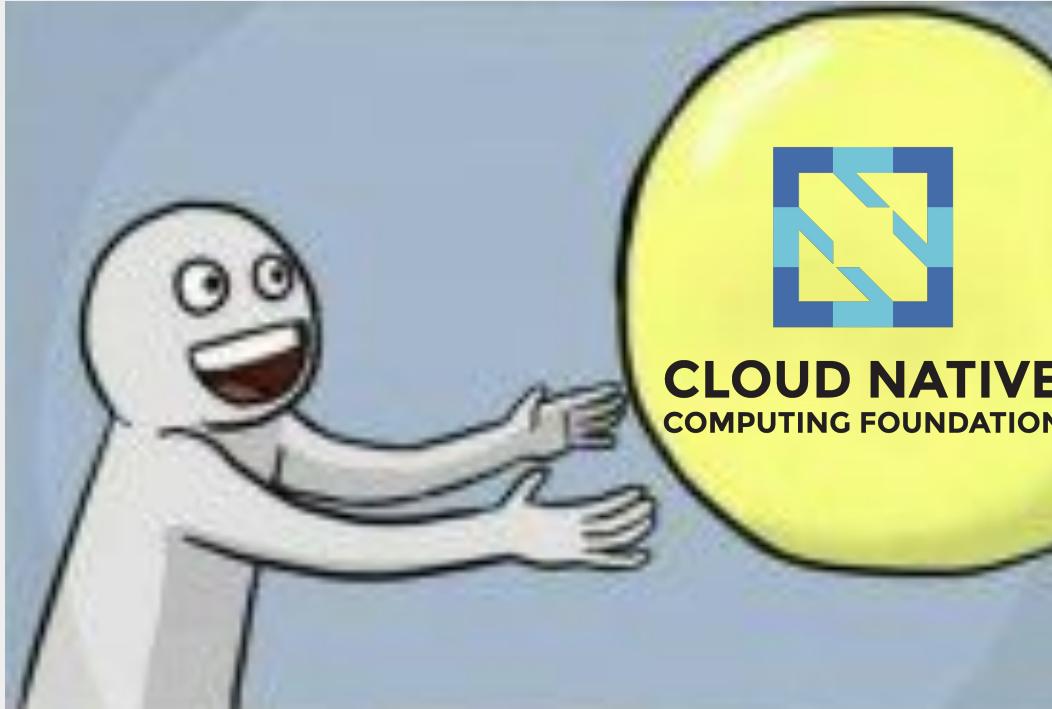


Call to action

Call to action

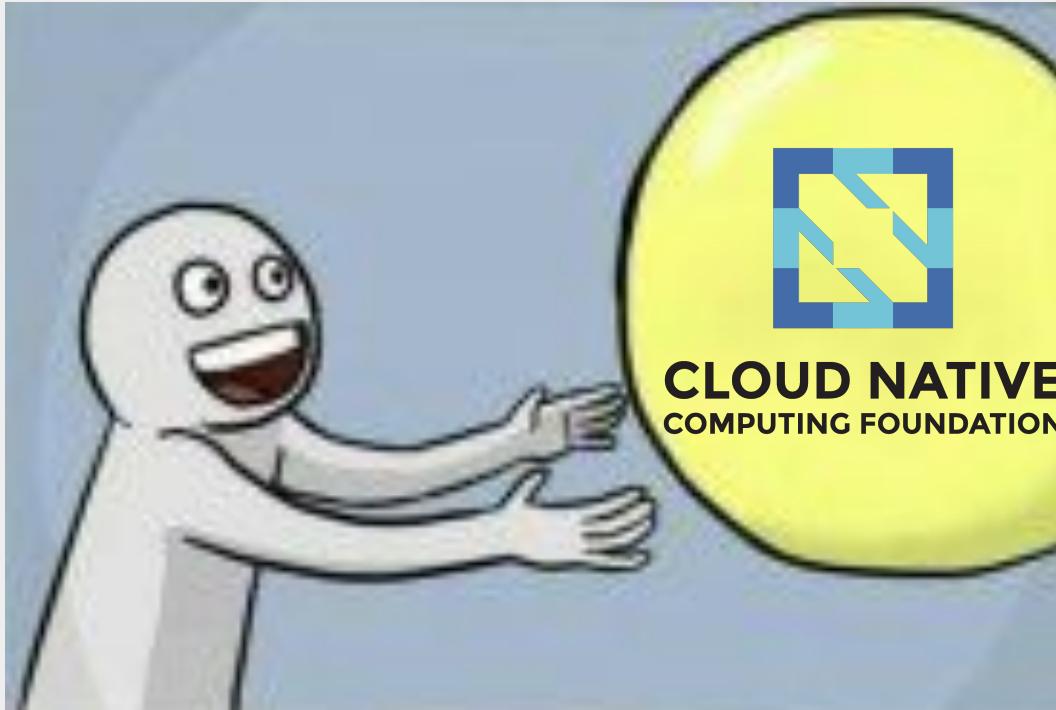


Call to action



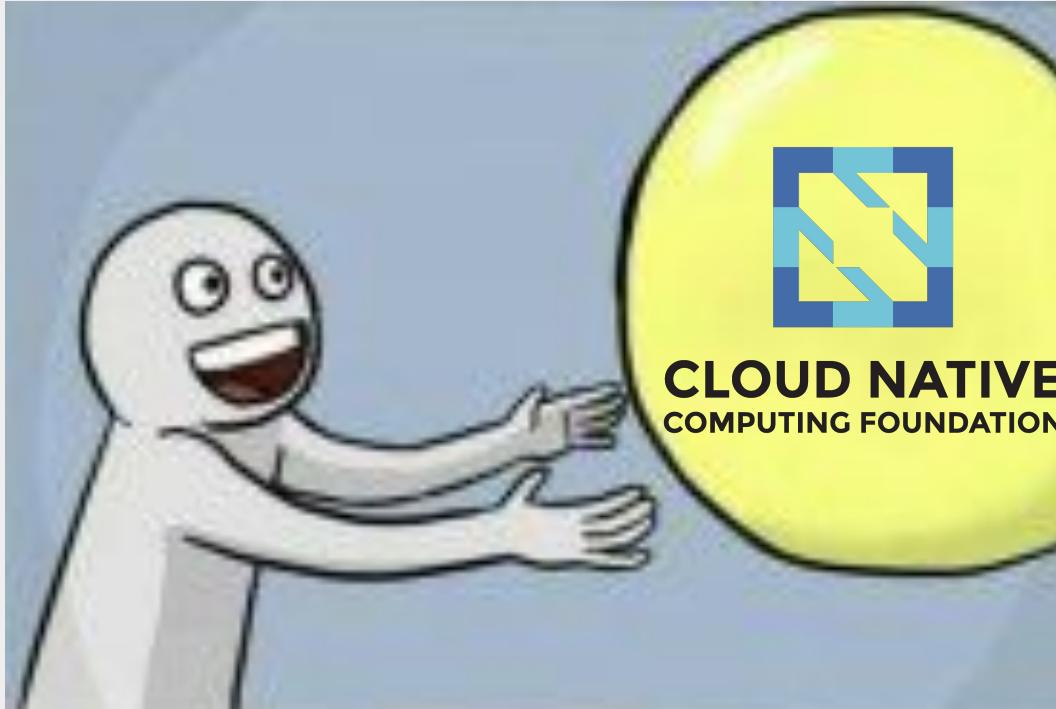
<https://istio.io/latest/blog/2022/get-started-ambient/>

Call to action

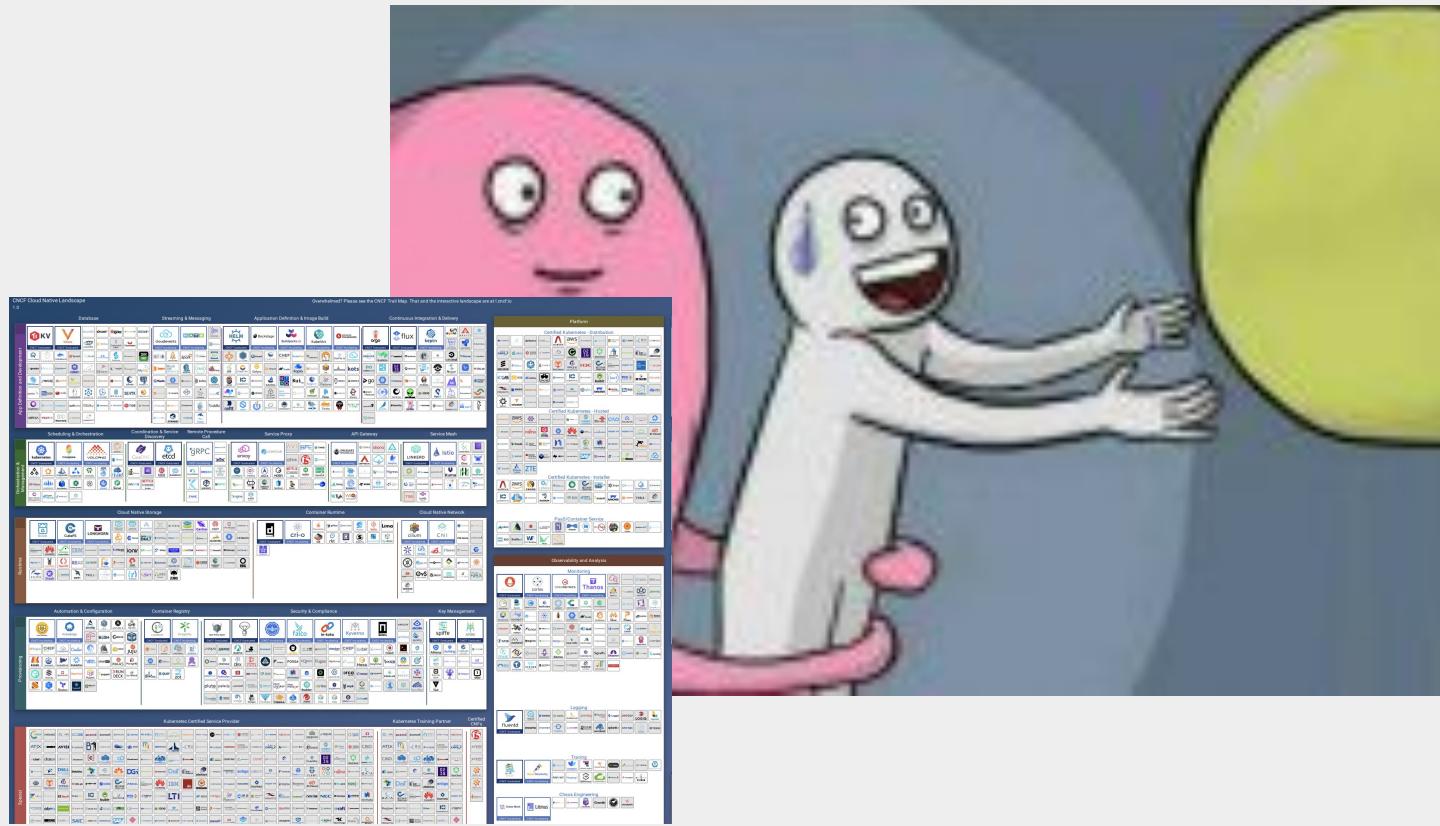


<https://github.com/cilium/cilium/issues/22215>

Call to action



Call to action





cilium

The screenshot shows a web browser window with the URL isovalent.com. The page title is "ISOVALENT". The main content features the heading "Cilium Service Mesh – Everything You Need to Know" and the date "Jul 20, 2022". Below the heading is a "Cilium" tag. At the bottom is the "cilium Service Mesh" logo.

Cilium Service Mesh – Everything You Need to Know

Jul 20, 2022 Cilium

cilium
Service Mesh



The screenshot shows a web browser window with the URL istio.io. The page title is "Istio". The main content features the heading "Introducing Ambient Mesh" and the text "A new dataplane mode for Istio without sidecars.". At the bottom is the "Sep 7, 2022" footer.

Introducing Ambient Mesh

A new dataplane mode for Istio without sidecars.

Sep 7, 2022 | By John Howard - Google, Ethan J. Jackson - Google, Yuval Kohavi - Solo.io, Idit Levine - Solo.io, Justin Pettit - Google, Lin Sun - Solo.io

Christine Kim - Isovalent



Rob Salmon - SuperOrbital

