



CLOUDNATIVE **SECURITYCON**

NORTH AMERICA 2023





CNI or Service Mesh? Comparing Security Policies Across Providers





Christine Kim - Google
@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





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



Istio

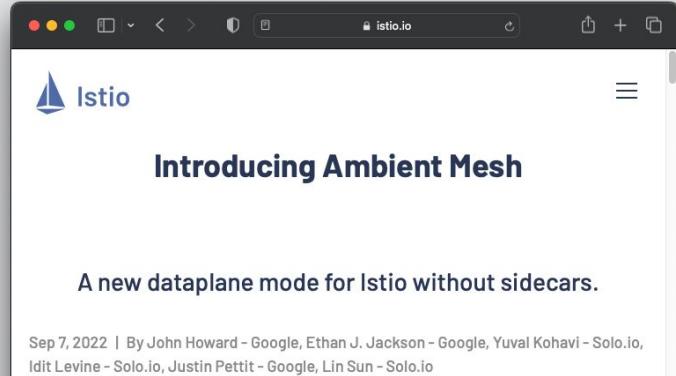
Top Ten CNCF Projects by: issues



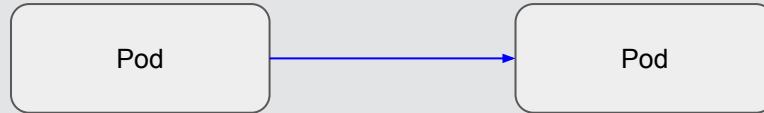
cilium



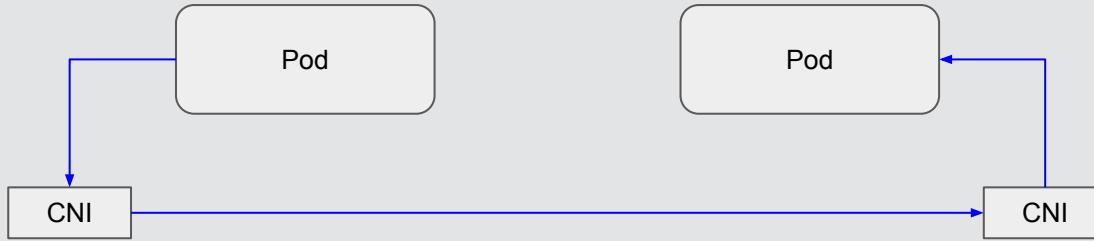
The screenshot shows a web browser window with the URL isovalent.com. The page title is "ISOVALENT". The main content features the text "Cilium Service Mesh – Everything You Need to Know" and the date "Jul 20, 2022". At the bottom, there is a "Cilium" tag and the Cilium logo.



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 a footer with the text "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”



What is CNI?



Container
Network
Interface

What is CNI?



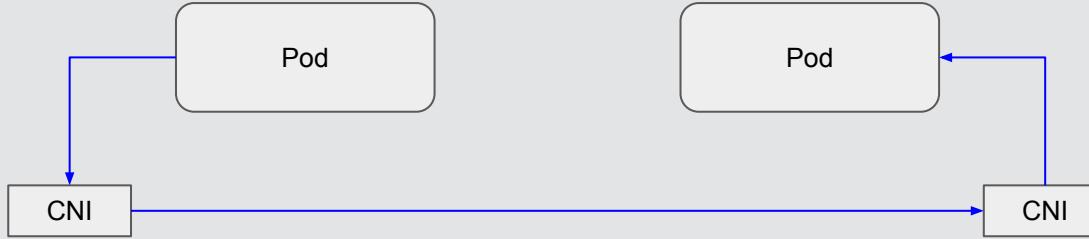
Container
Network
Interface

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

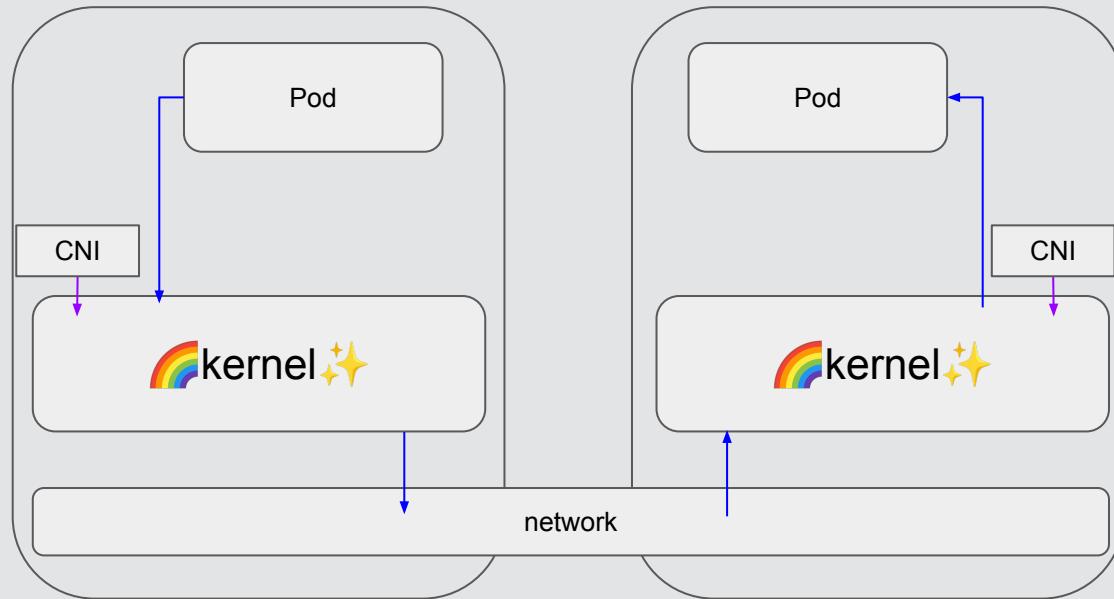
What kind of changes?



What kind of changes?



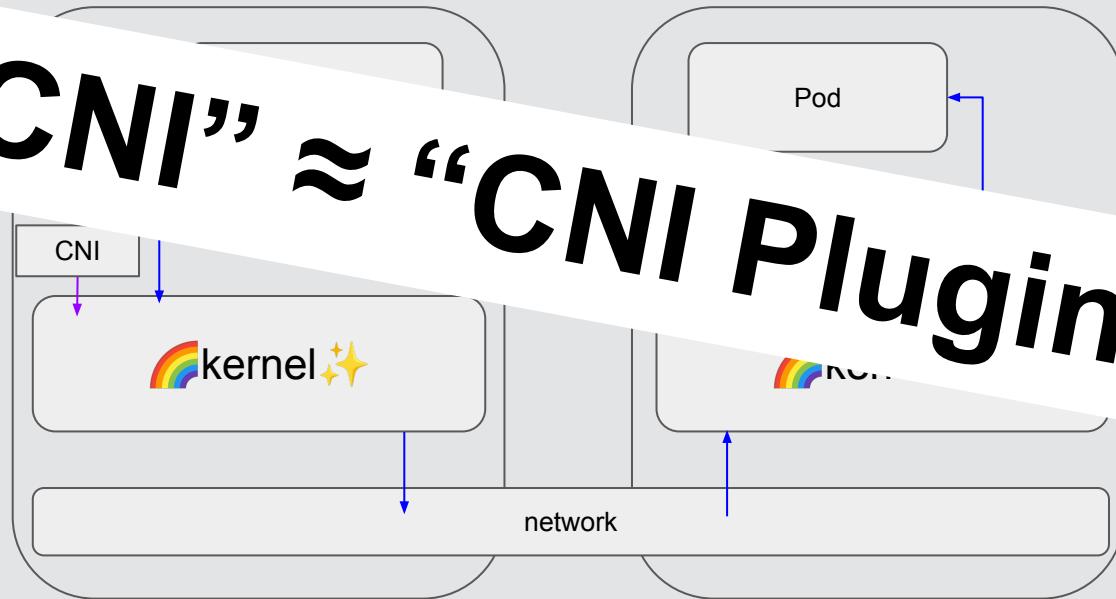
What kind of changes?



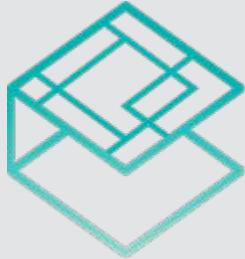
→ control
→ data

What kind of changes?

“CNI” ≈ “CNI Plugin”,



What is a CNI plugin?



C N I

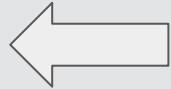


implements

What is a CNI plugin?



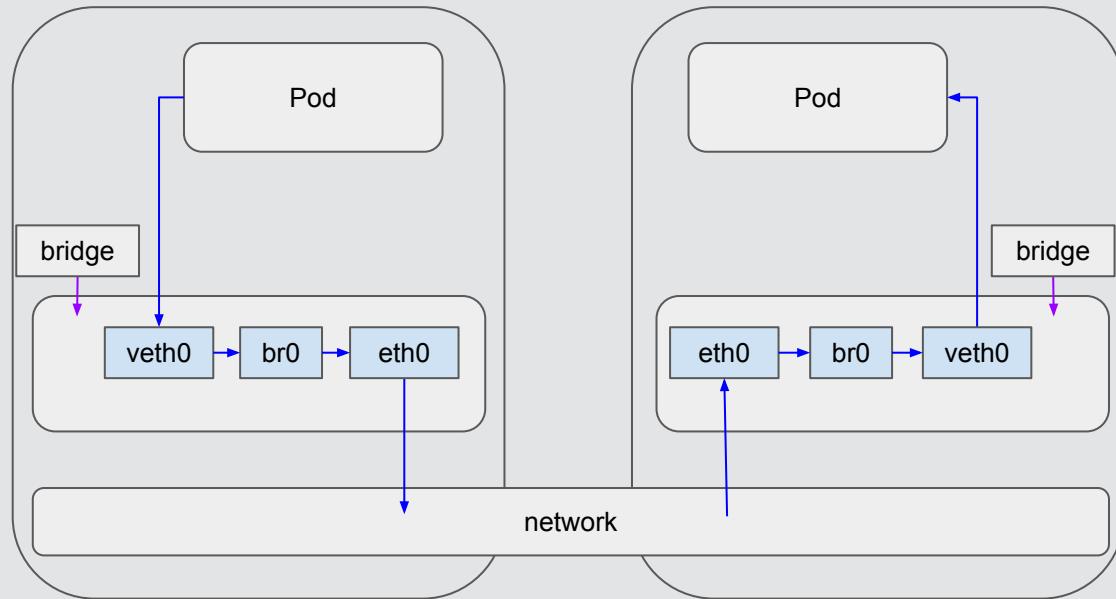
C N I



implements

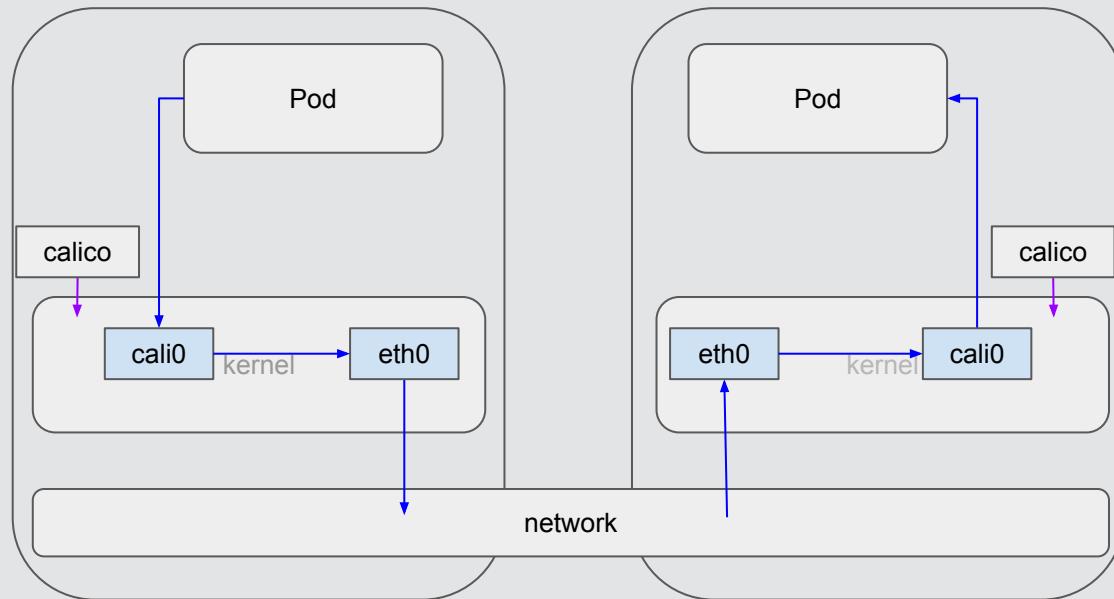
"A thing that can make container networking changes.

bridge plugin



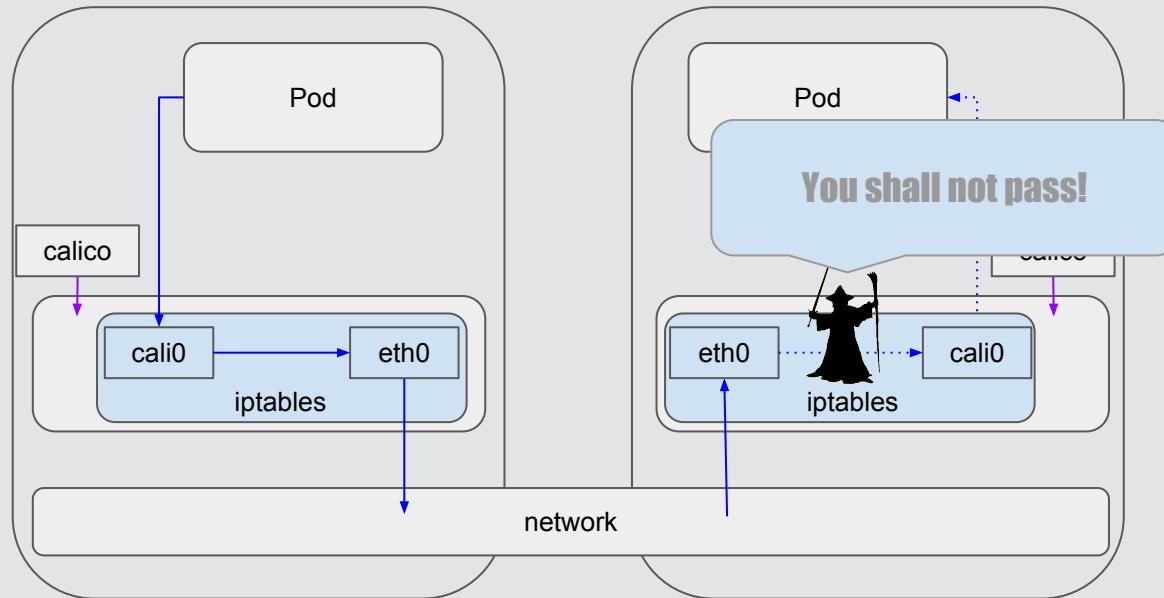
→ control
→ data

Calico plugin

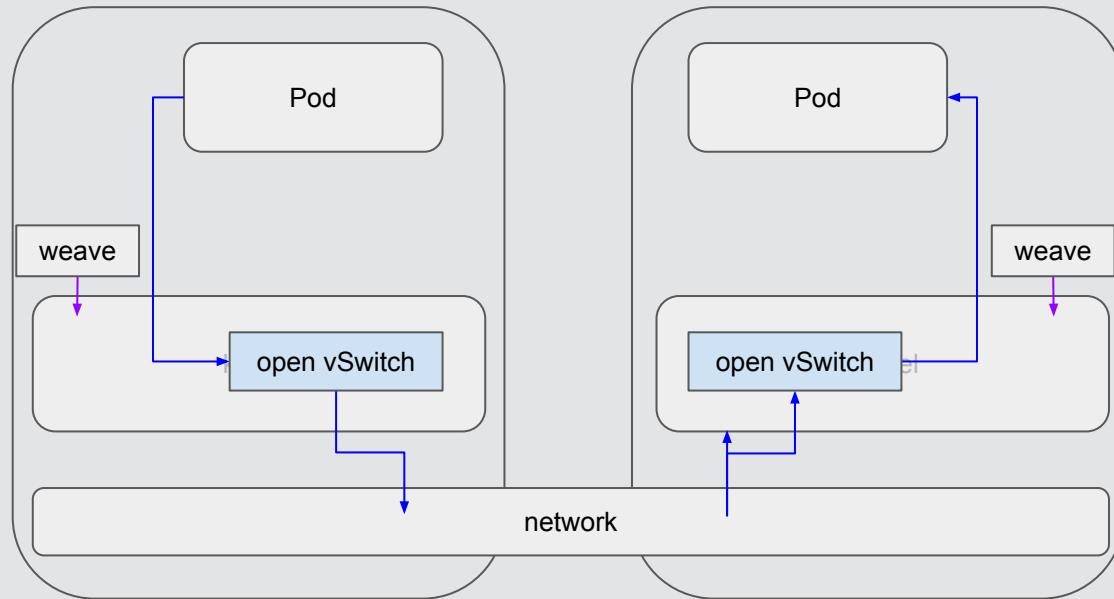


→ control
→ data

Calico plugin

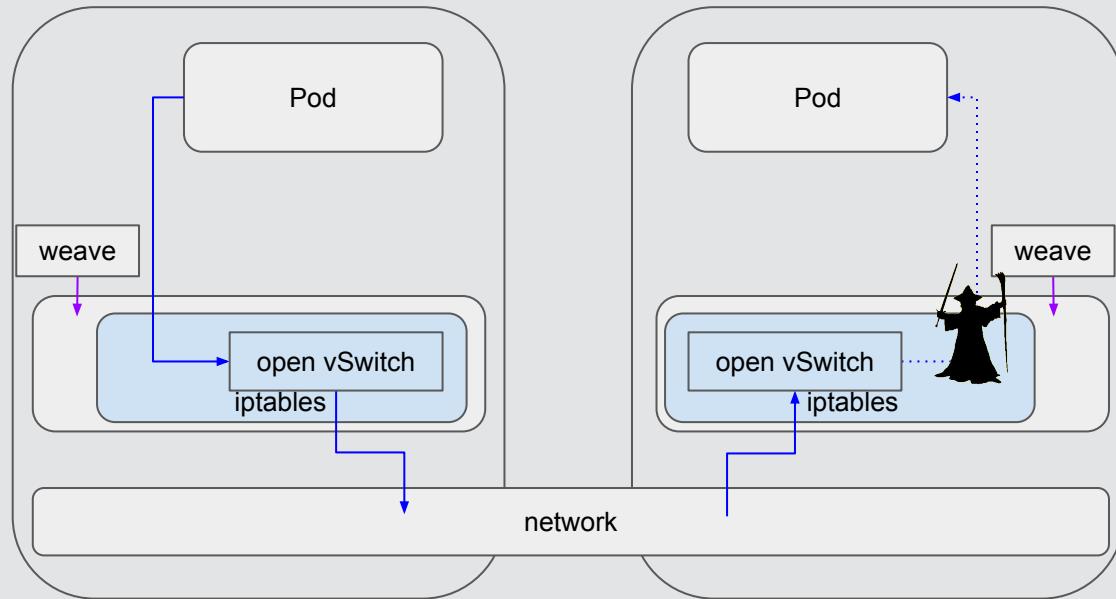


weave plugin



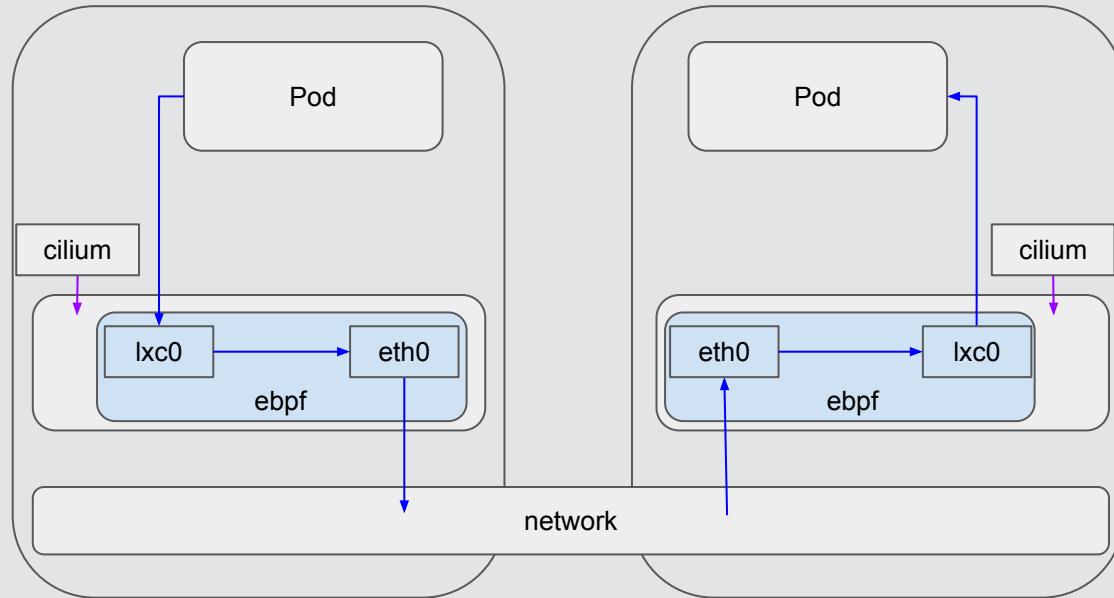
→ control
→ data

weave plugin



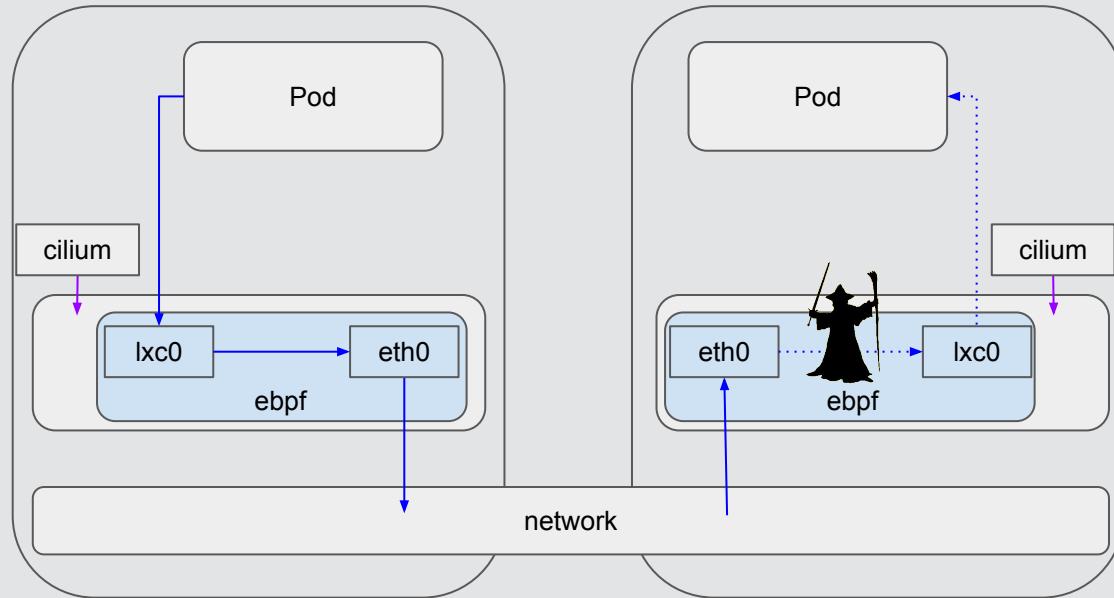
→ control
→ data

cilium plugin



→ control
→ data

cilium plugin



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

→ 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:

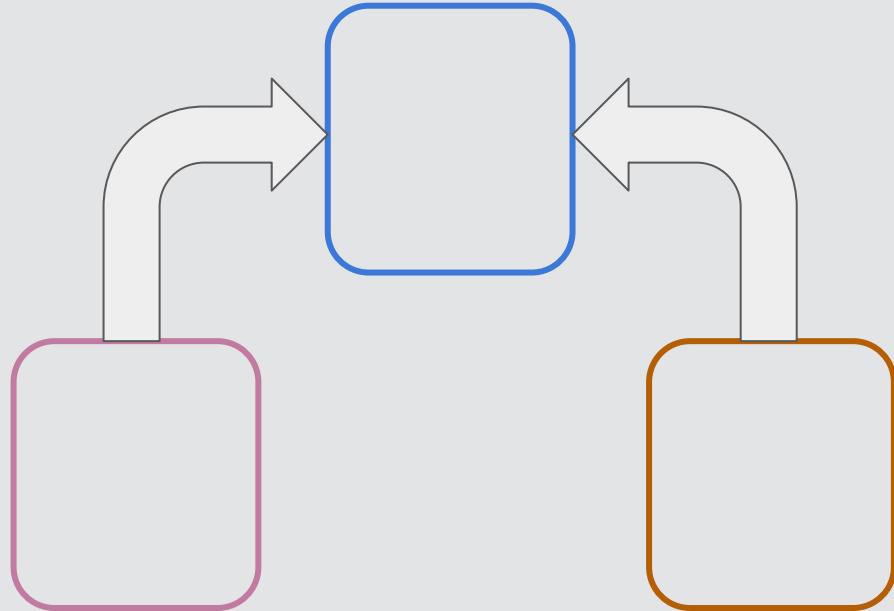


- Configure pod to pod networking
- Support NetworkPolicy enforcement
- ≈ Cloud Native software defined network

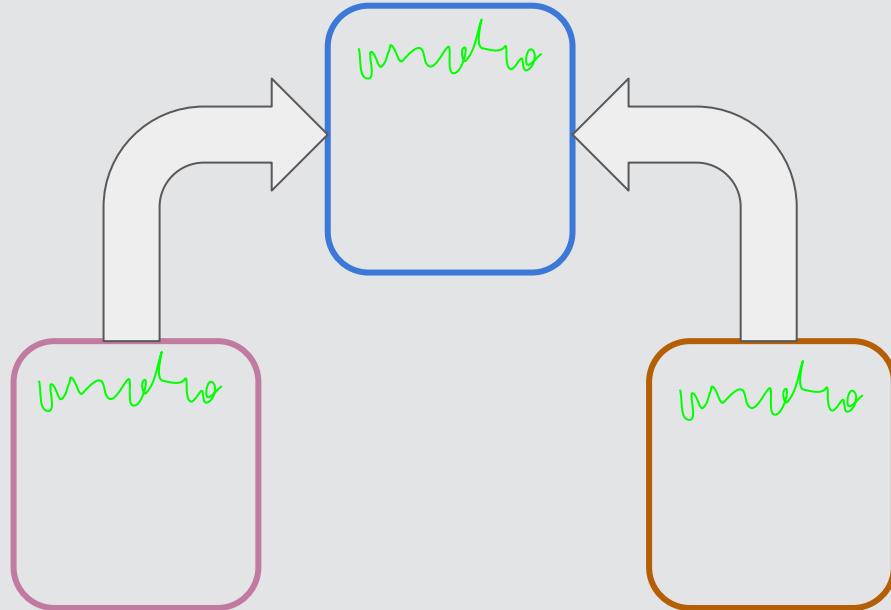
What is a Service Mesh?



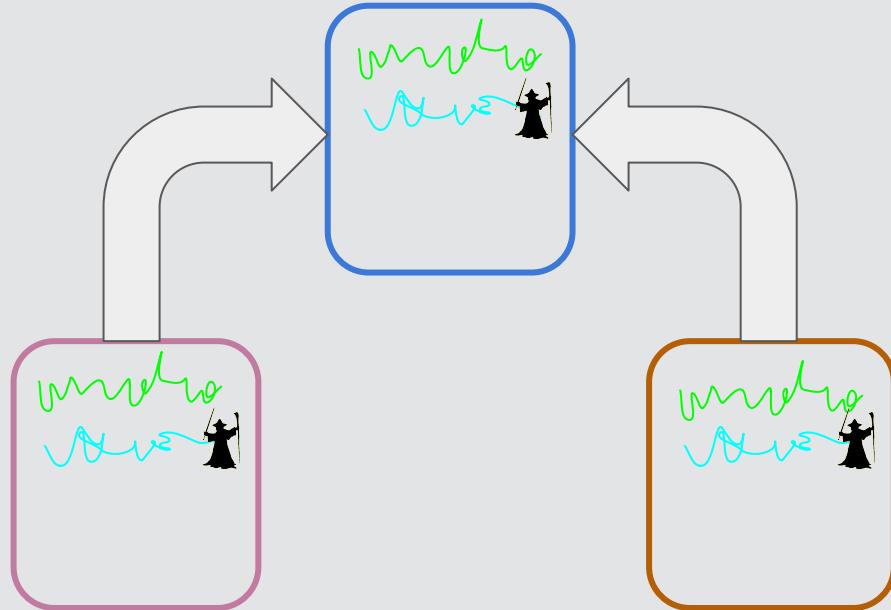
What is a Service Mesh?



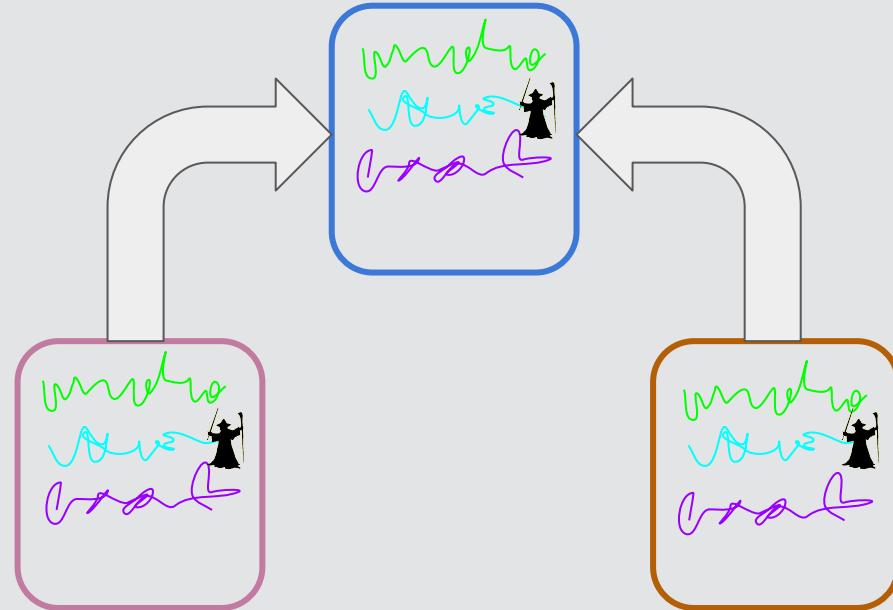
What is a Service Mesh?



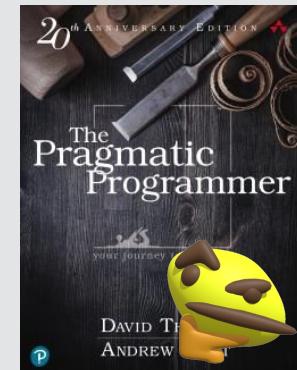
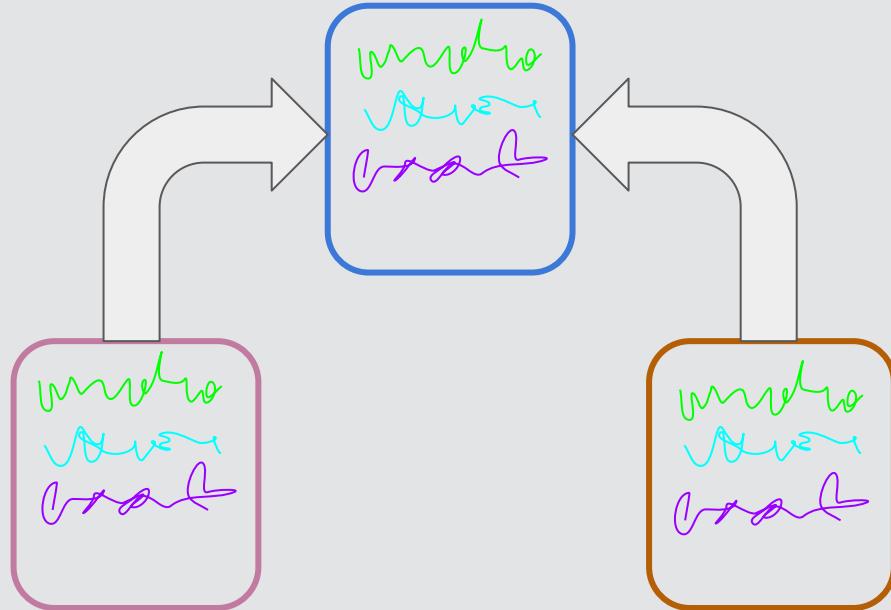
What is a Service Mesh?



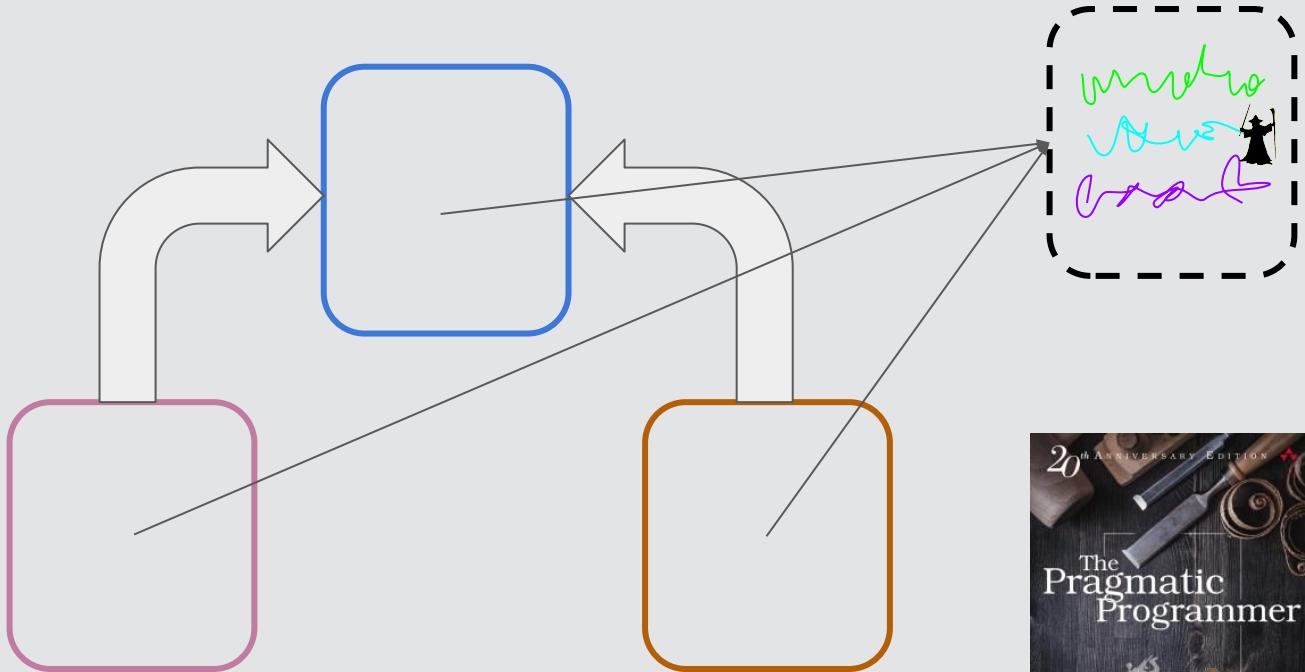
What is a Service Mesh?



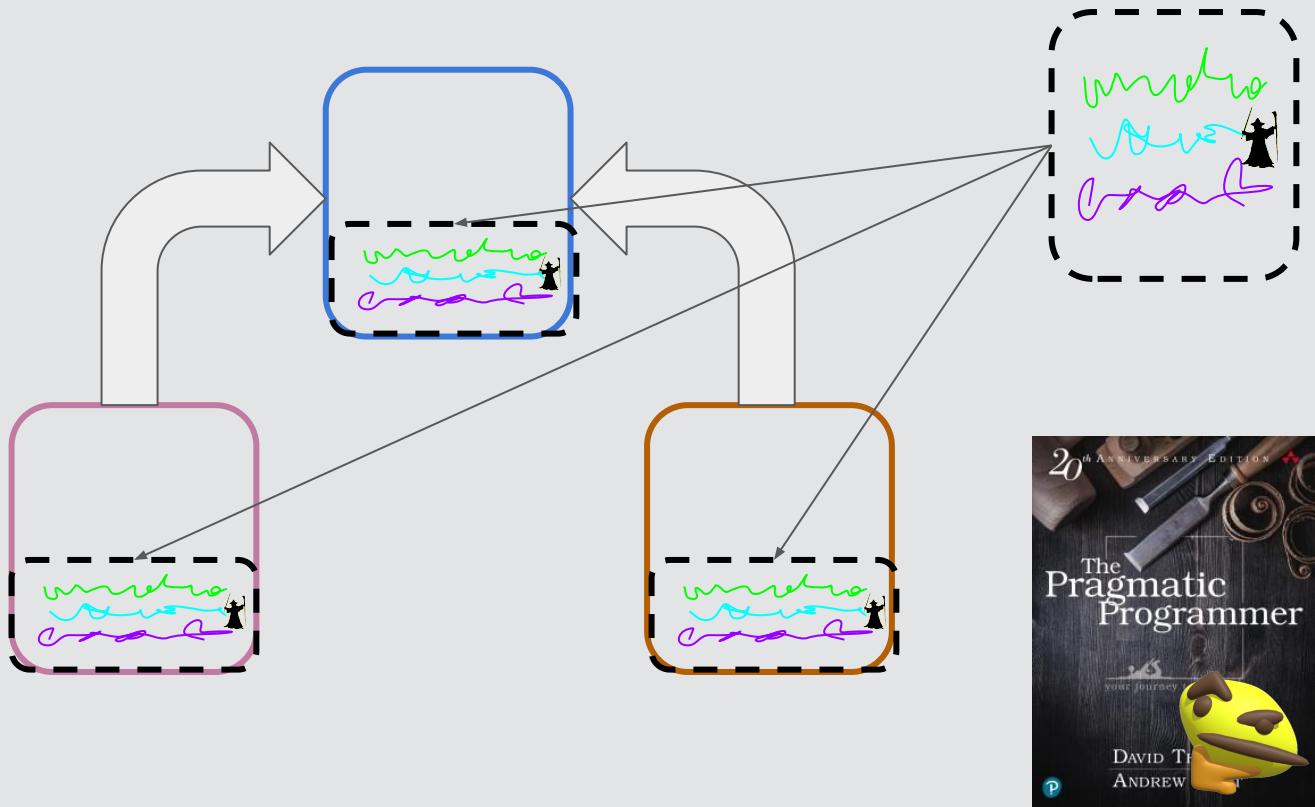
What is a Service Mesh?



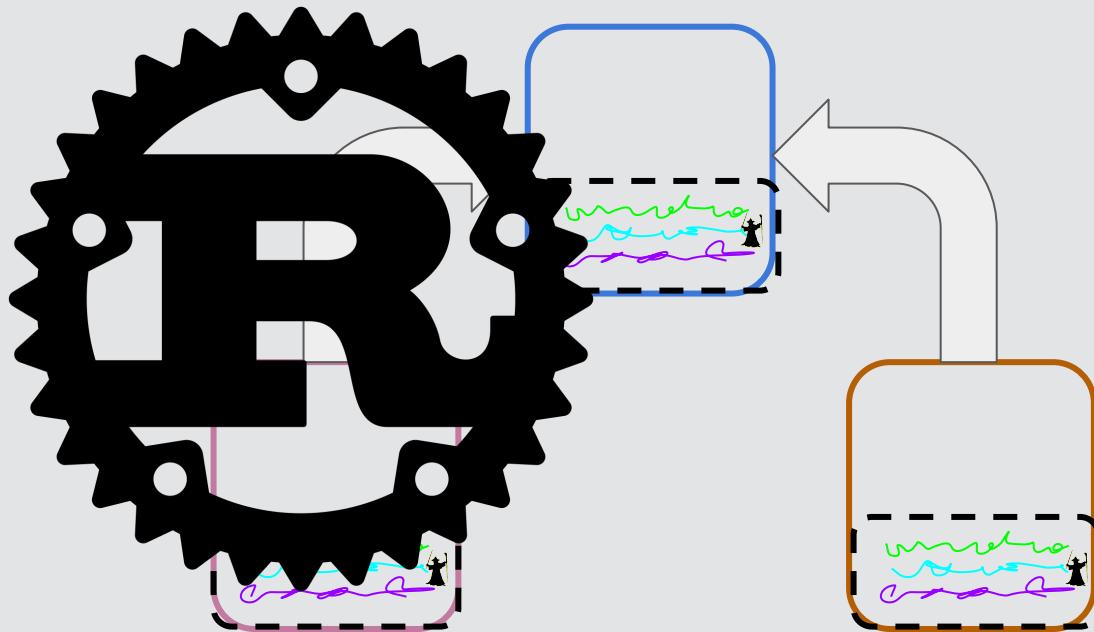
What is a Service Mesh?



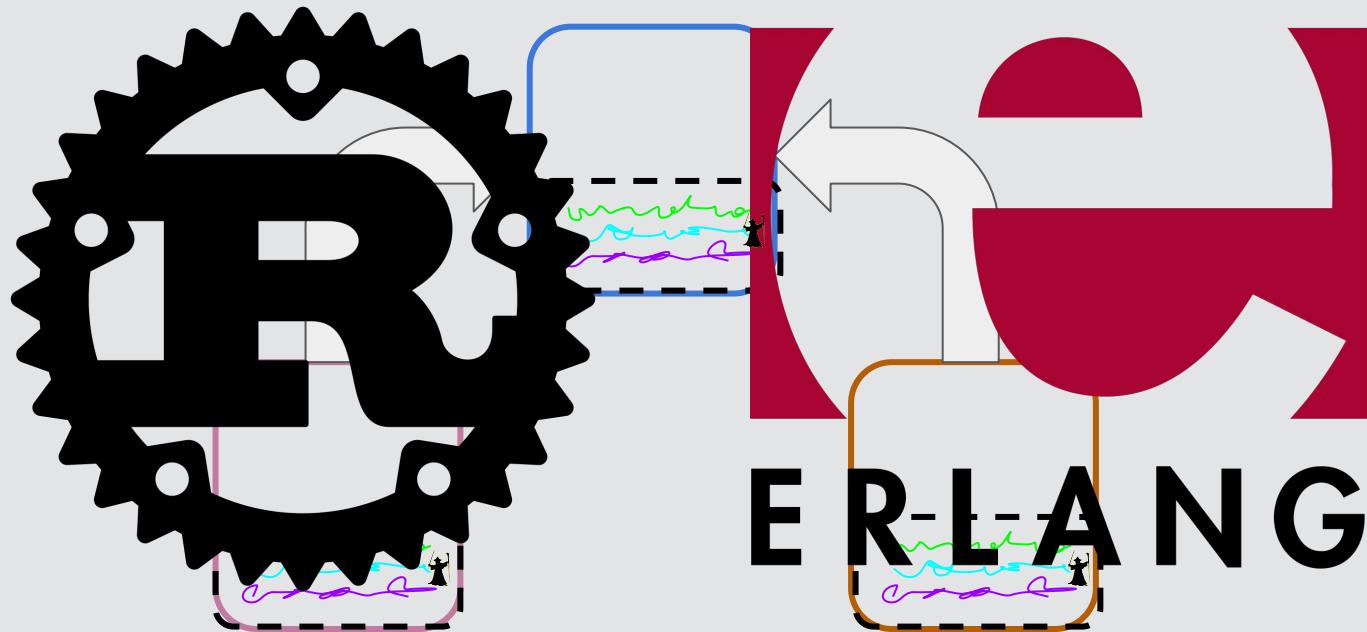
What is a Service Mesh?



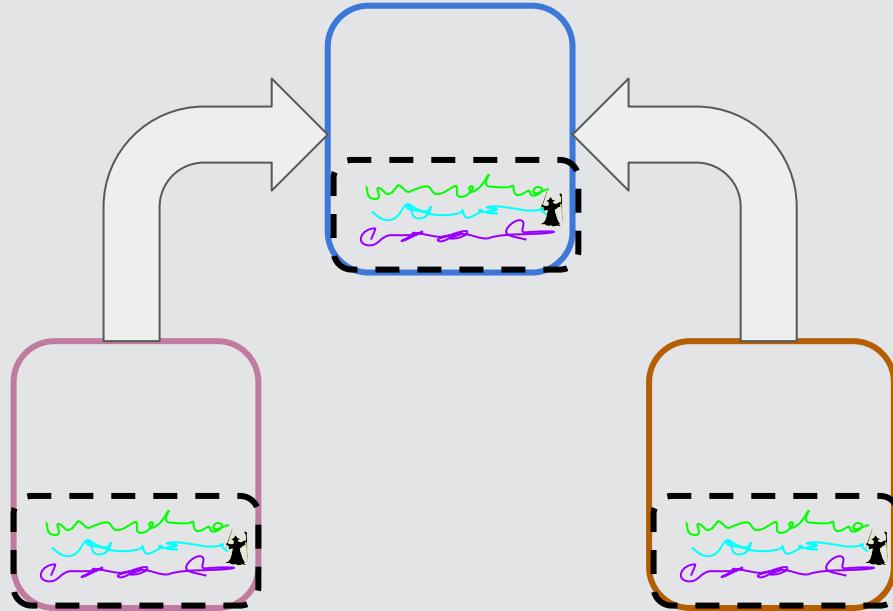
What is a Service Mesh?



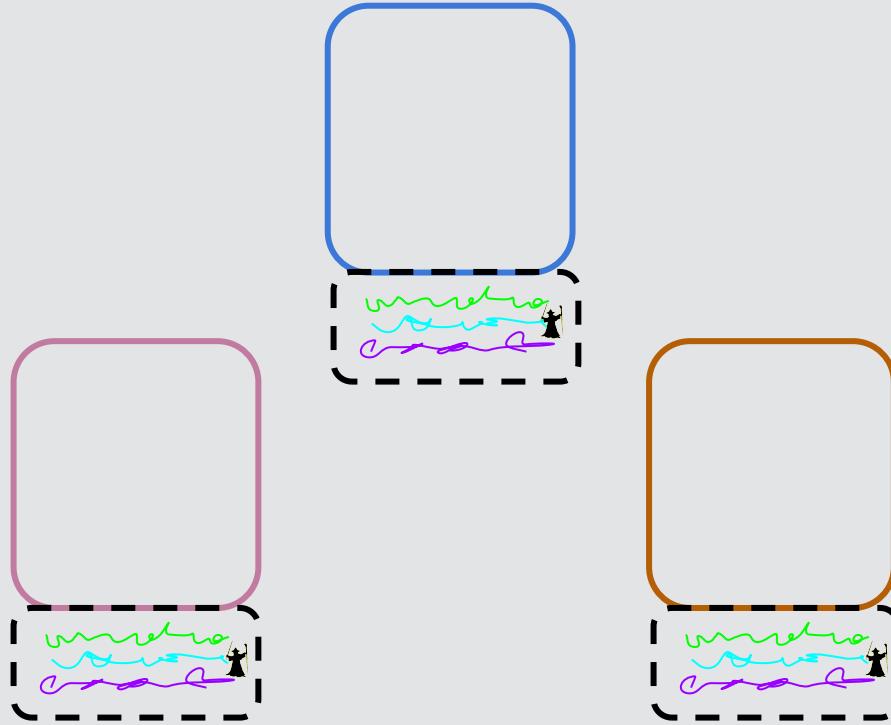
What is a Service Mesh?



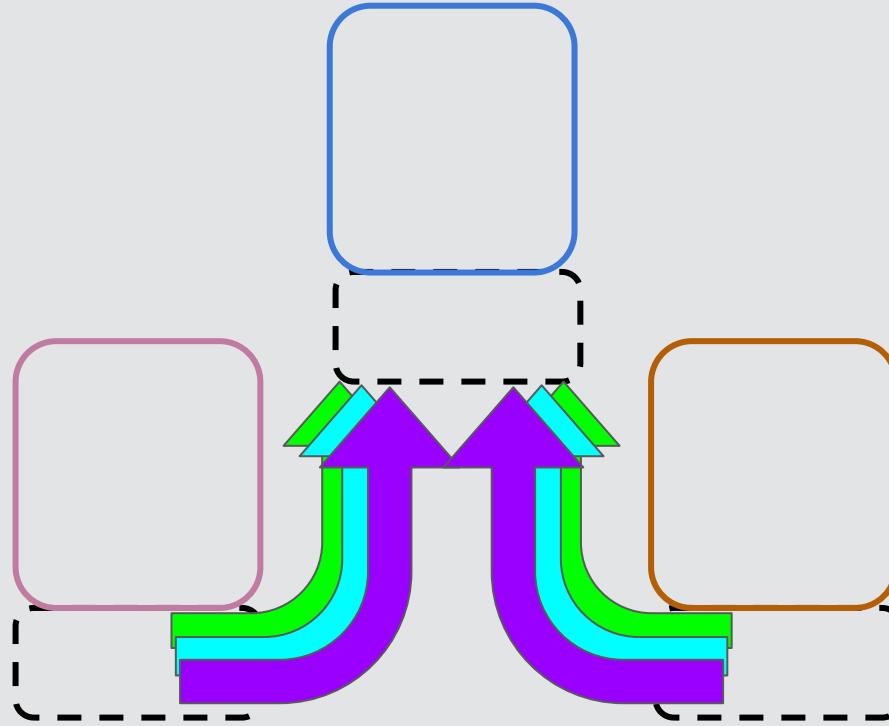
What is a Service Mesh?



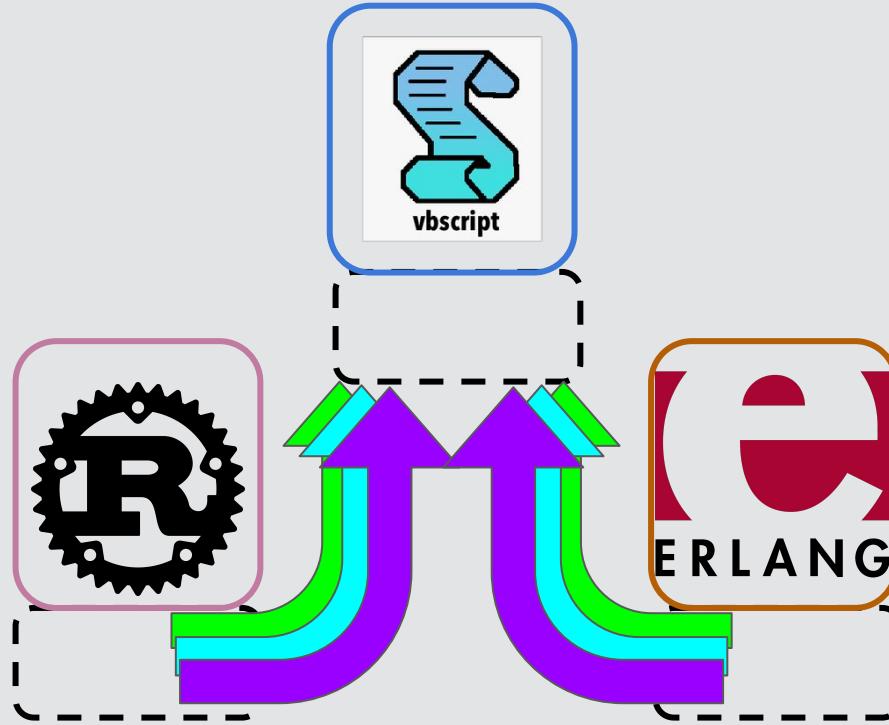
What is a Service Mesh?



What is a Service Mesh?



What is a Service Mesh?



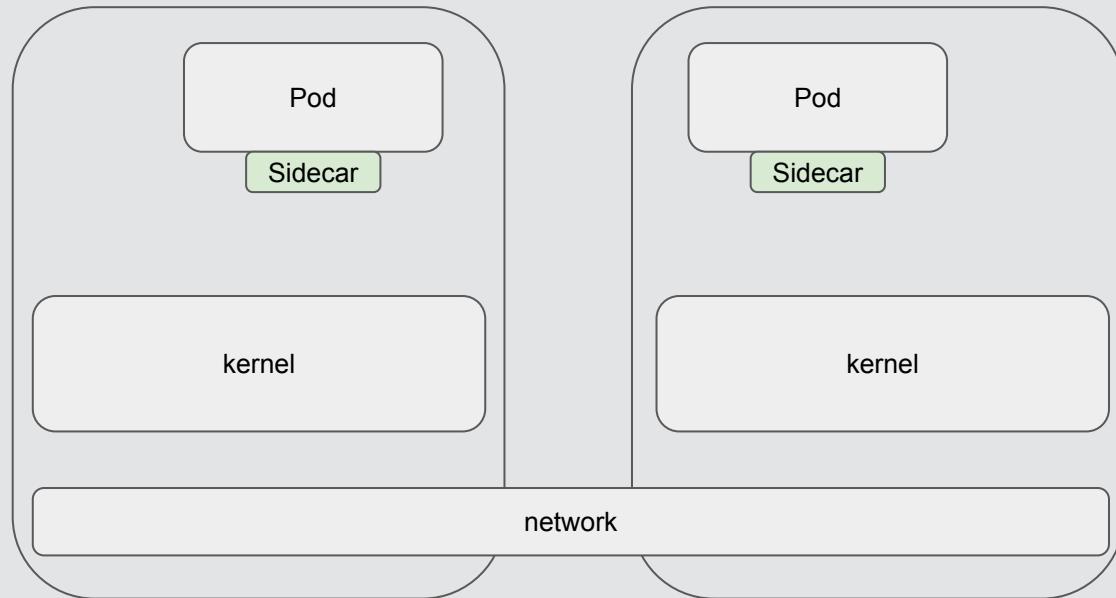
The most popular Meshes offer:



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

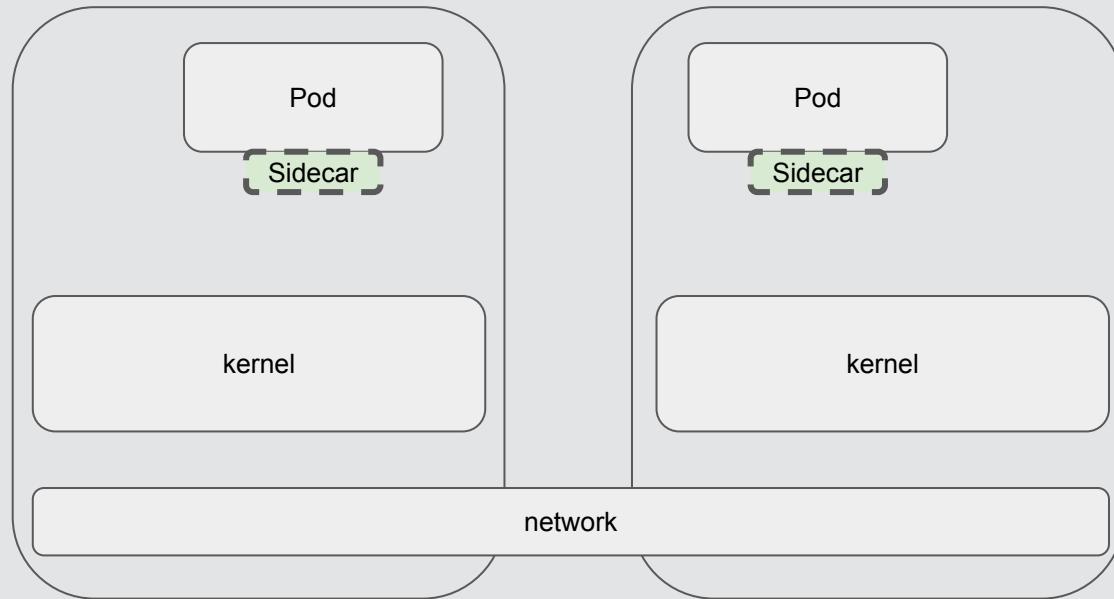


service mesh



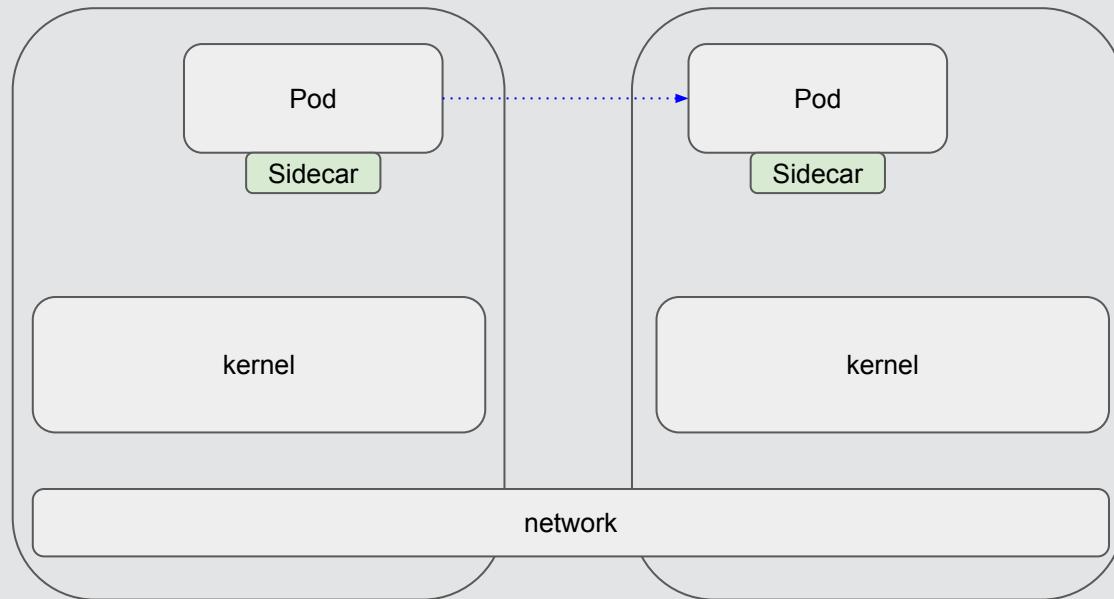
control
data

service mesh



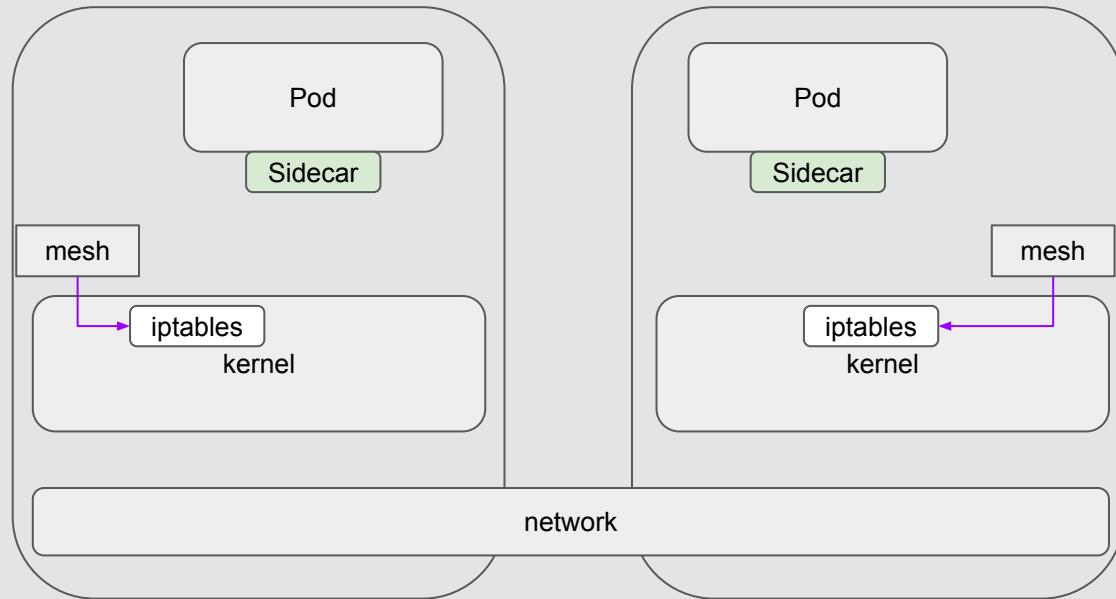
control
data

service mesh



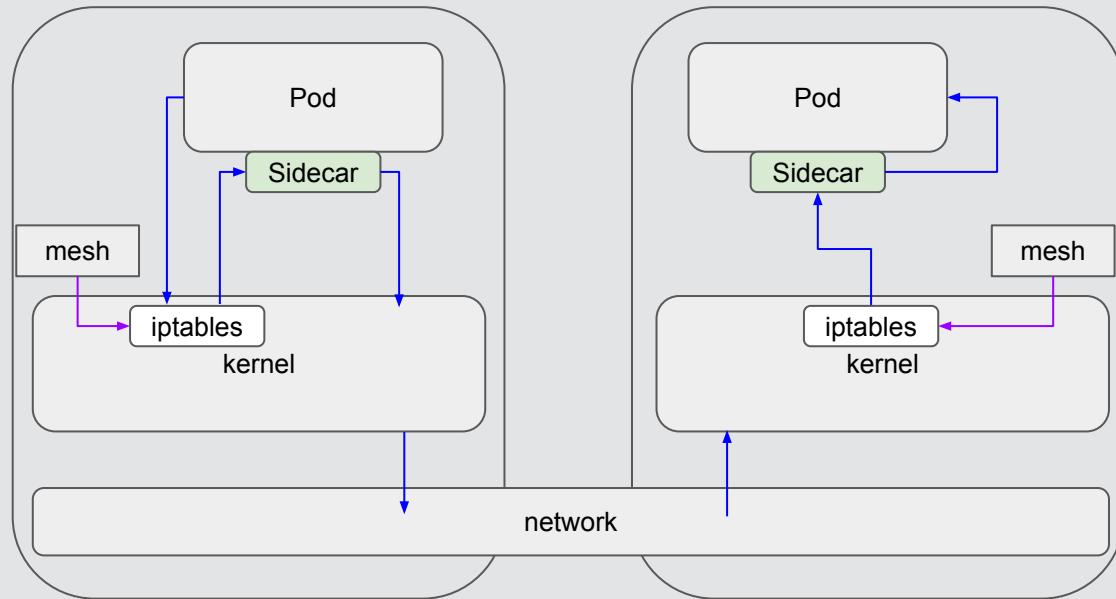
—> control
—> data

service mesh



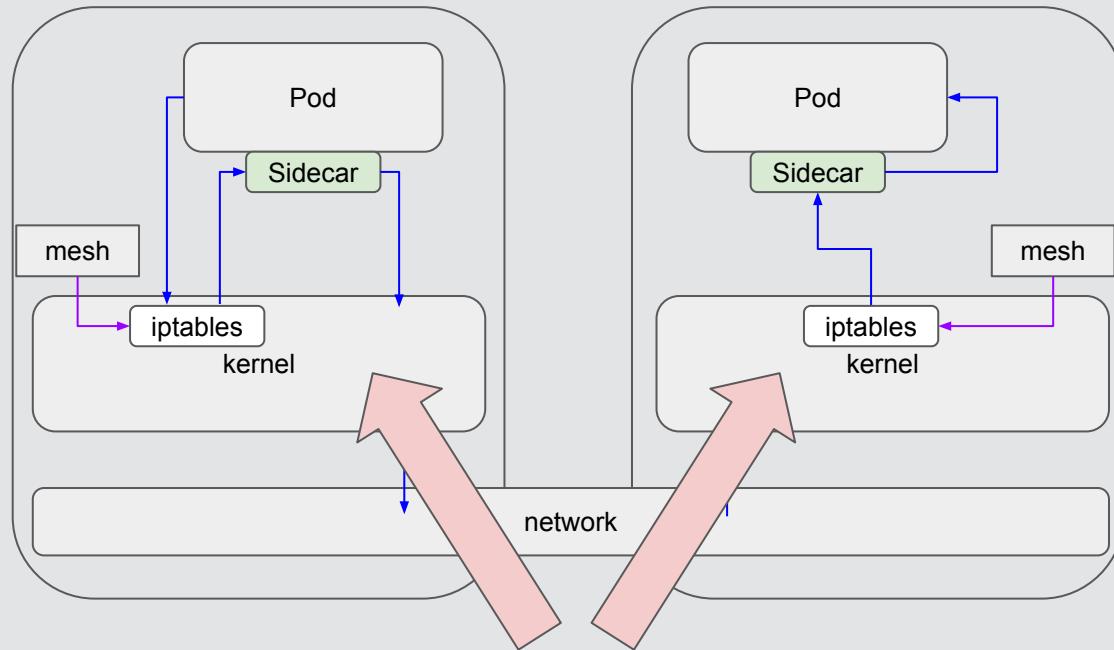
→ control
→ data

service mesh



—→ control
—→ data

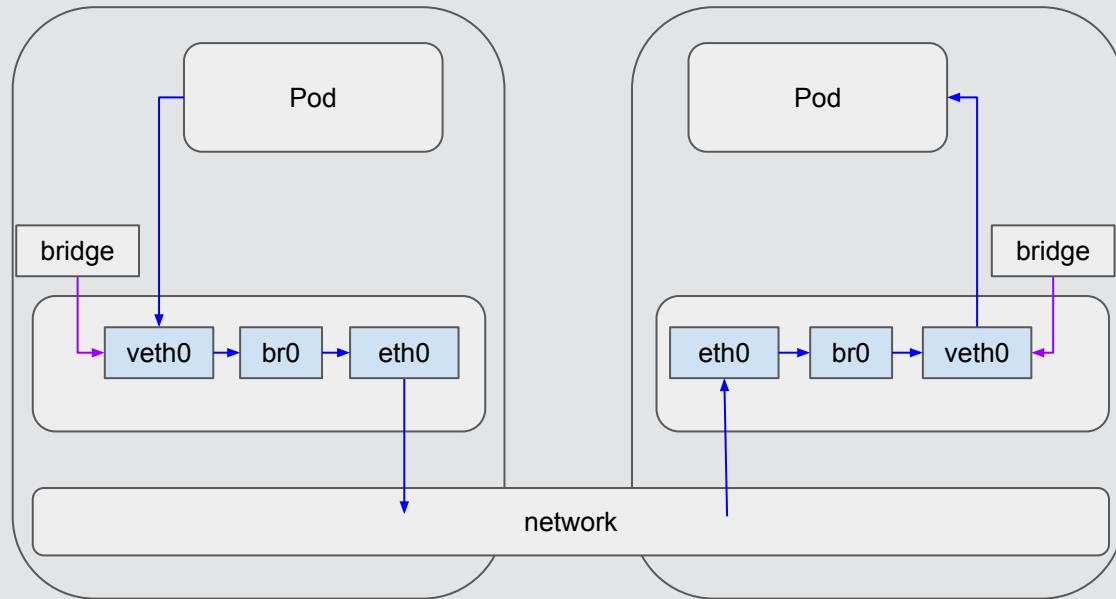
service mesh



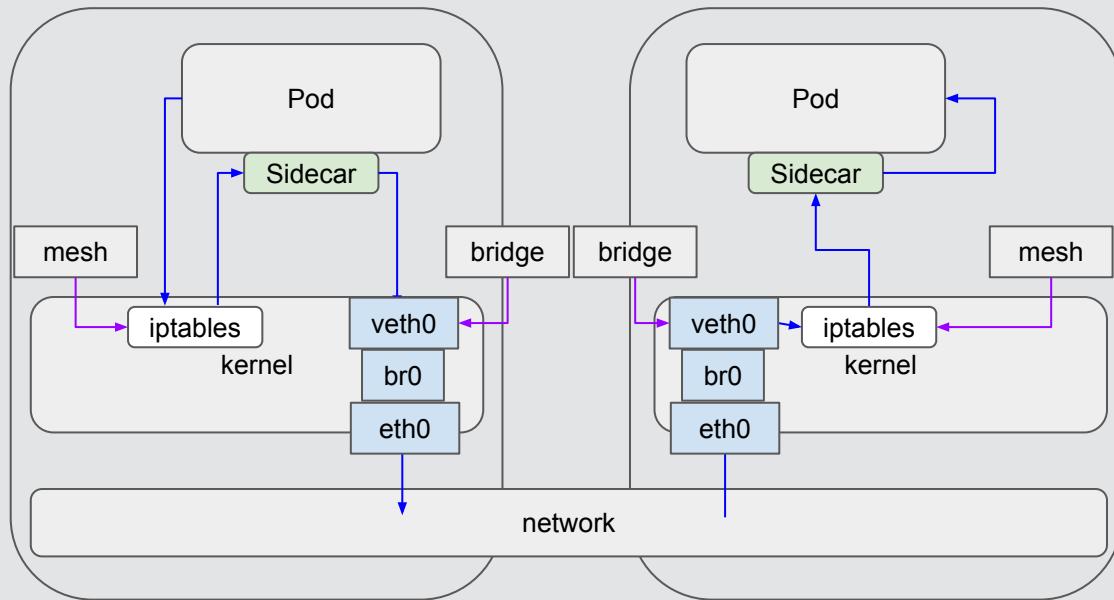
No Interfaces?

— control
— data

bridge plugin

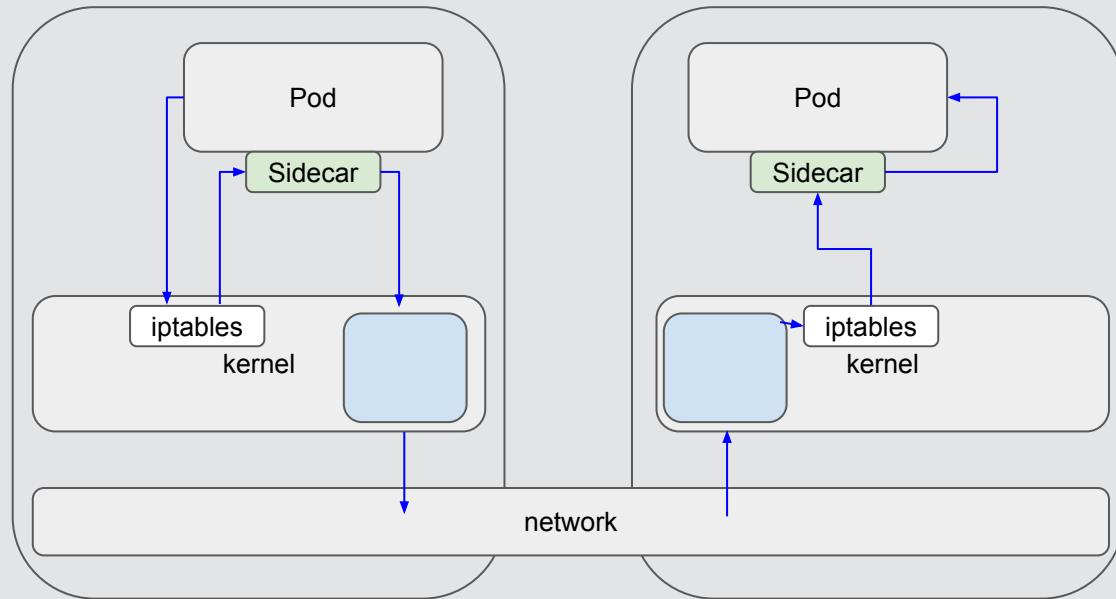


service mesh with bridge plugin



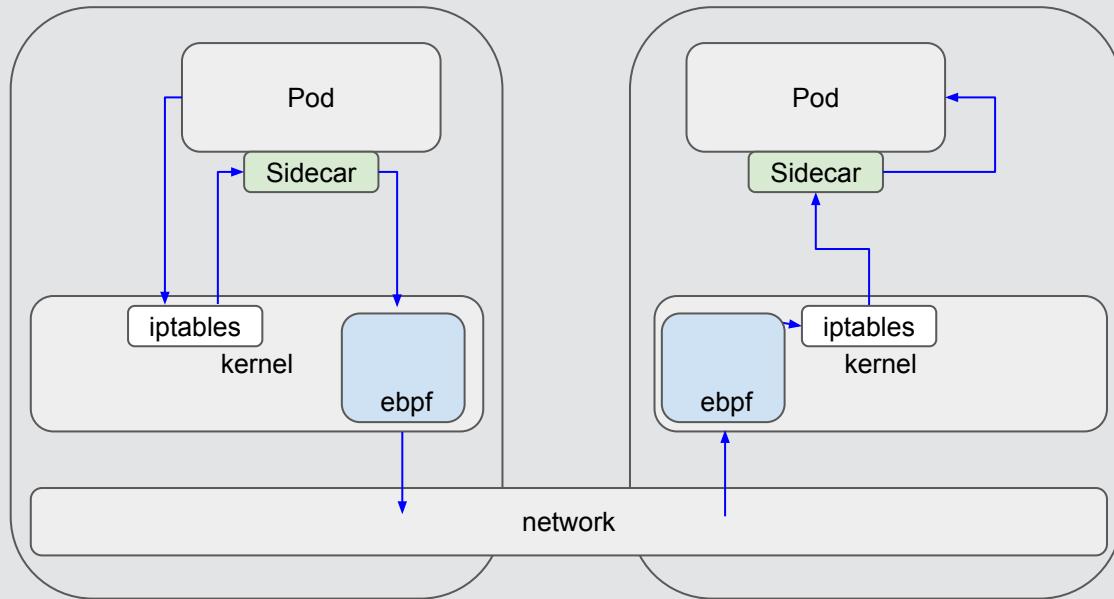
— control
— data

CNI + service mesh



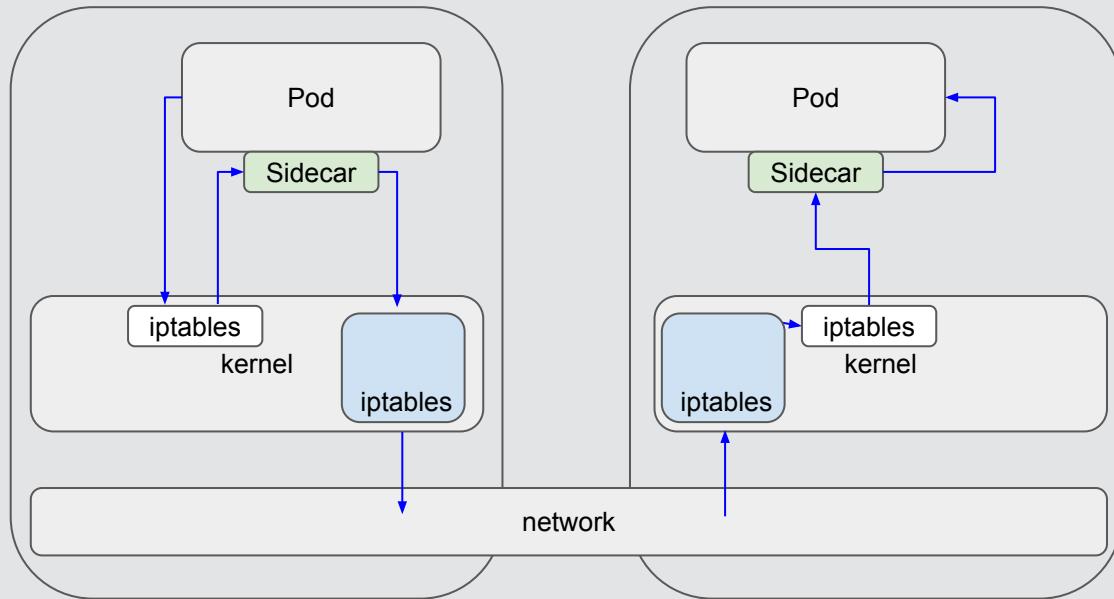
—→ control
—→ data

CNI + service mesh



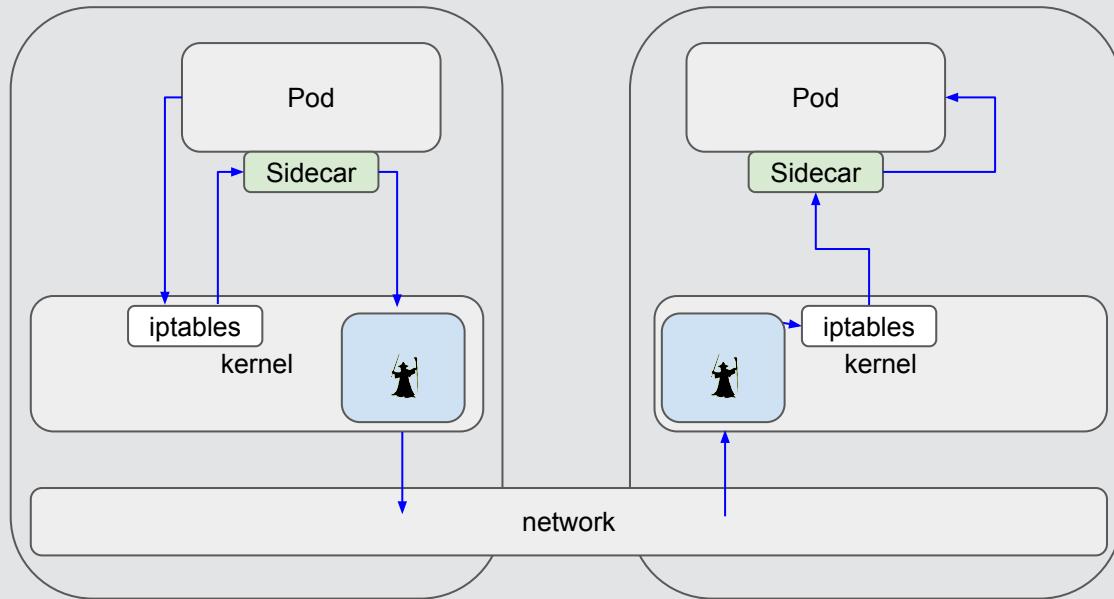
—> control
—> data

CNI + service mesh



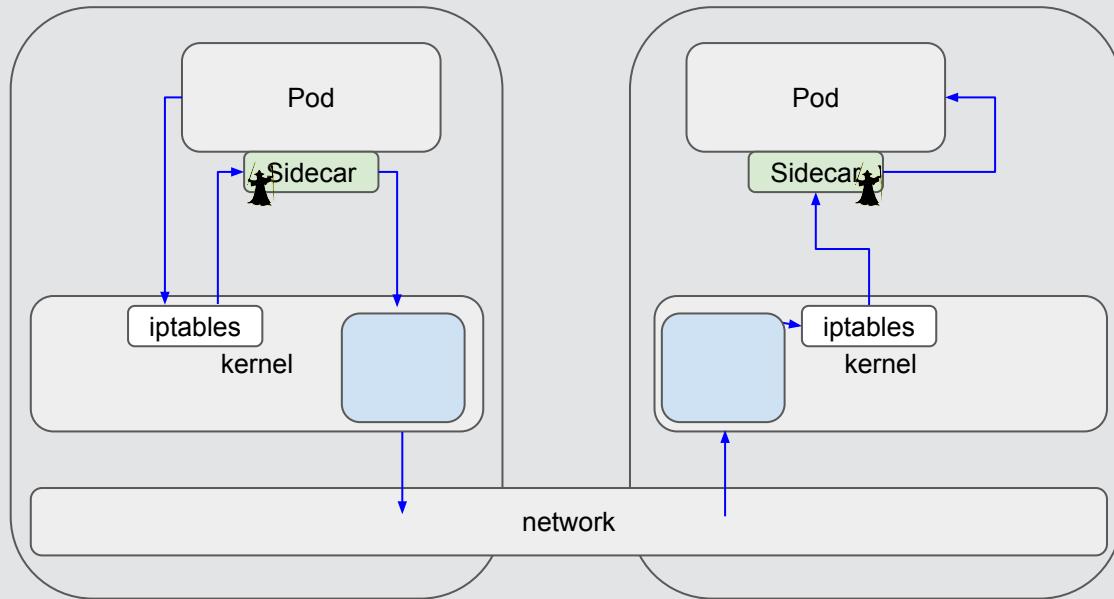
— control
— data

CNI + service mesh



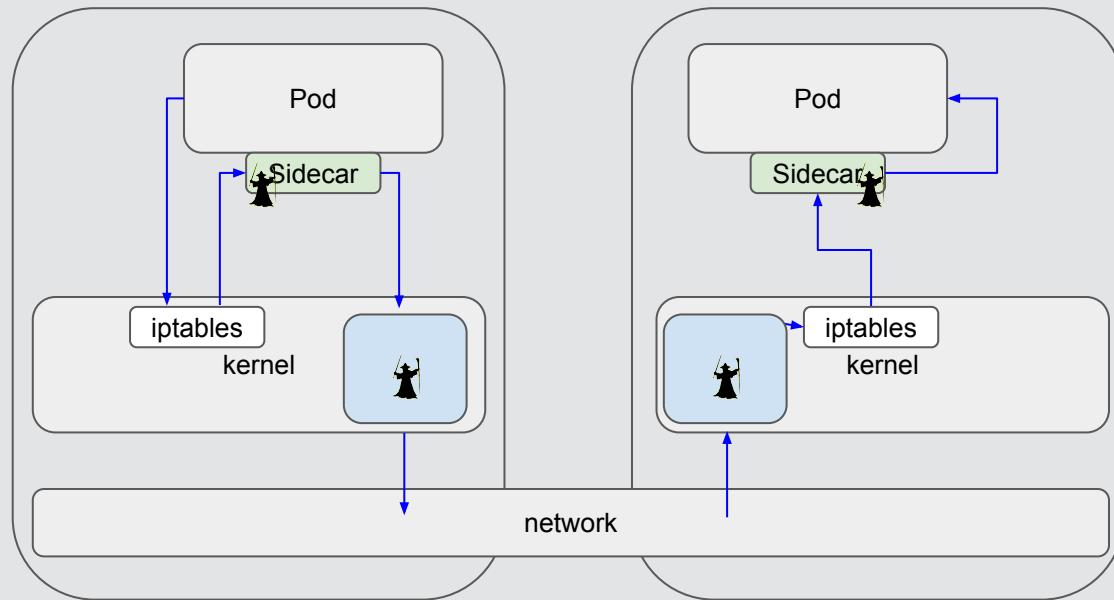
control
data

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?

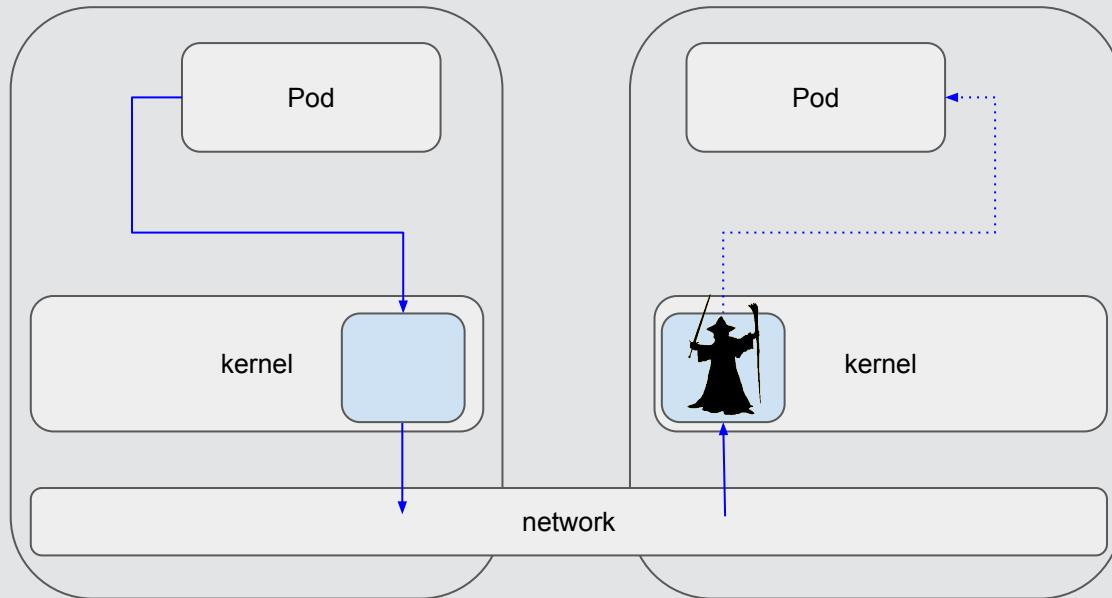


```
$ kubectl explain networkpolicy.spec
```

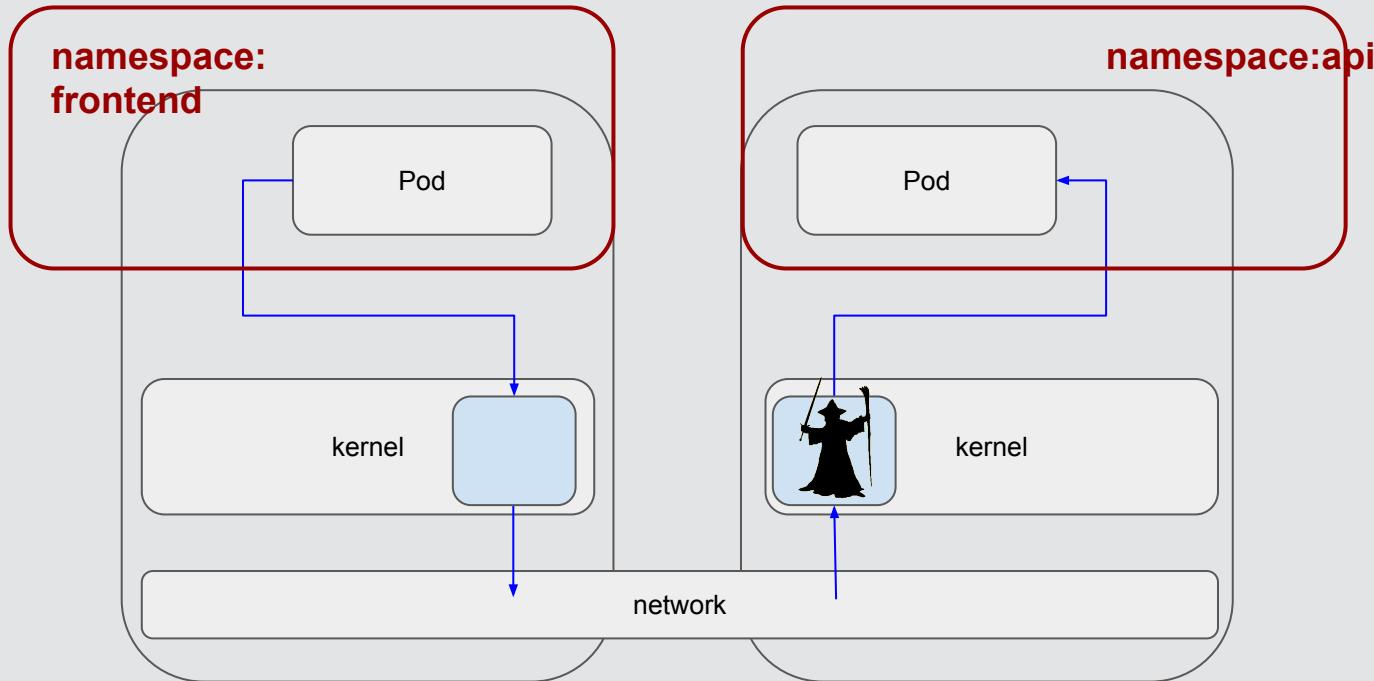
- Allows you to apply policy on traffic which:
 - is going to any* IP or CIDR
 - is going to pods that match some label selector
 - is going to specific port(s)
 - is going to a specific namespace(s)
- Allows you to conditionally block/permit traffic based on:
 - source IP or CIDR
 - source pods that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

* except loopback or host traffic

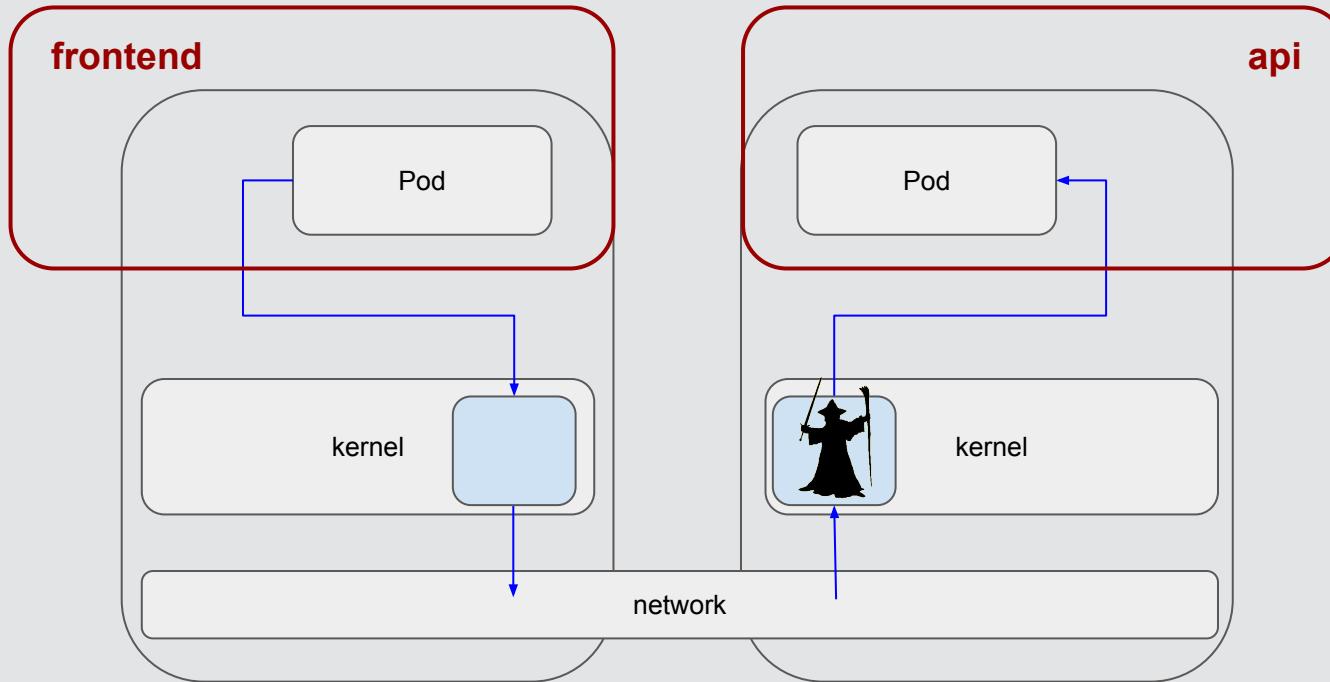
CNI - how is it enforced?



CNI - how is it enforced?

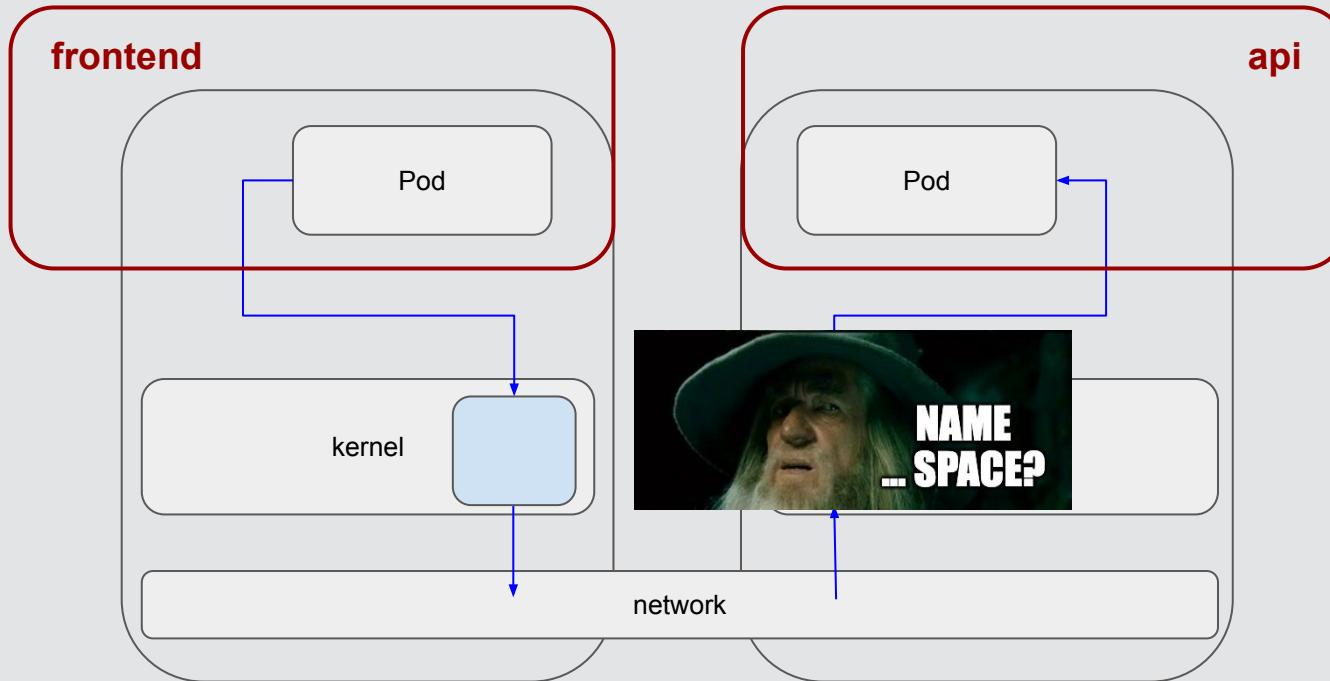


CNI - how is it enforced?



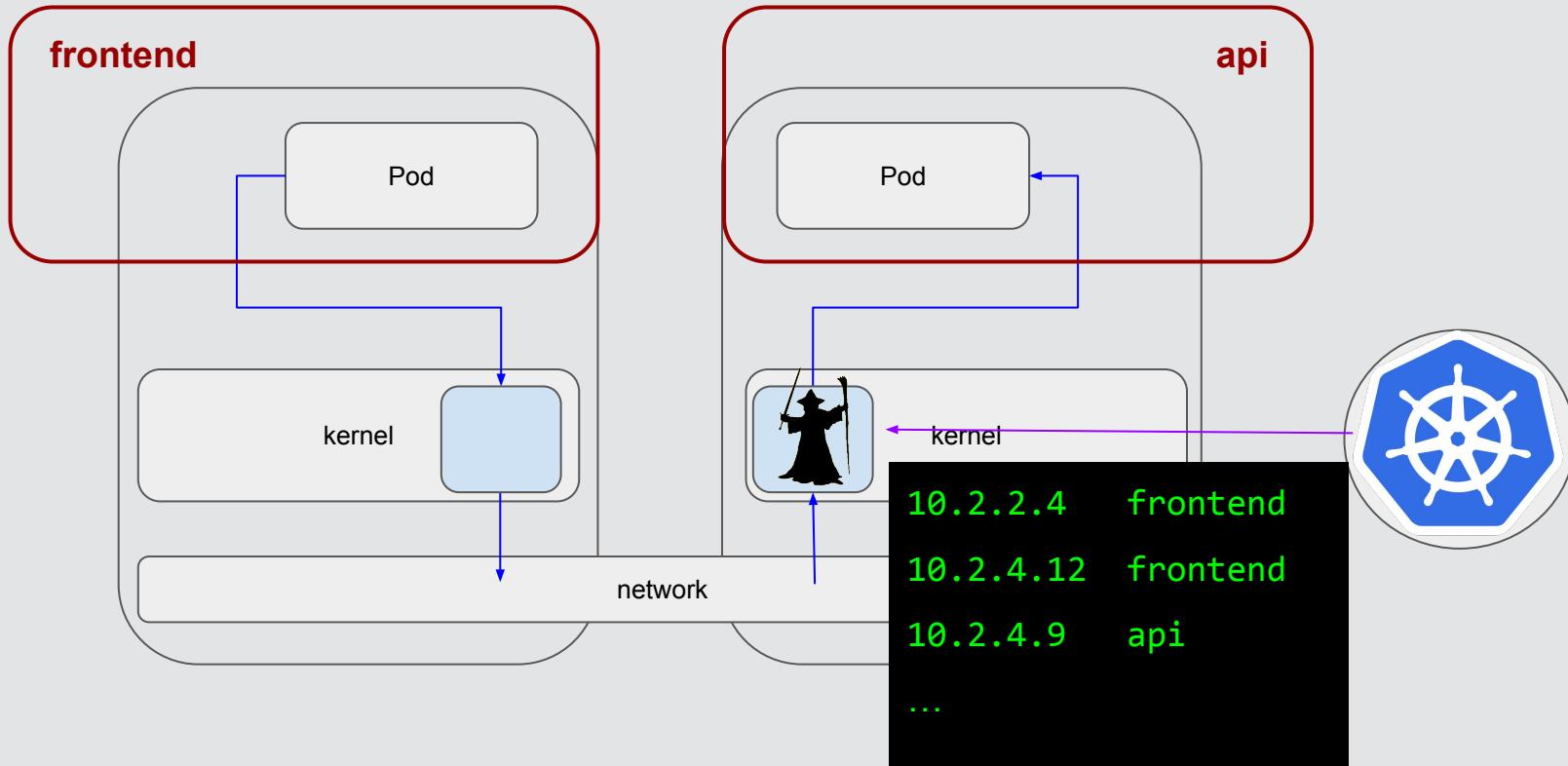
```
$ dear CNI: [pods in frontend] => [pods in api] == OK!
```

CNI - how is it enforced?

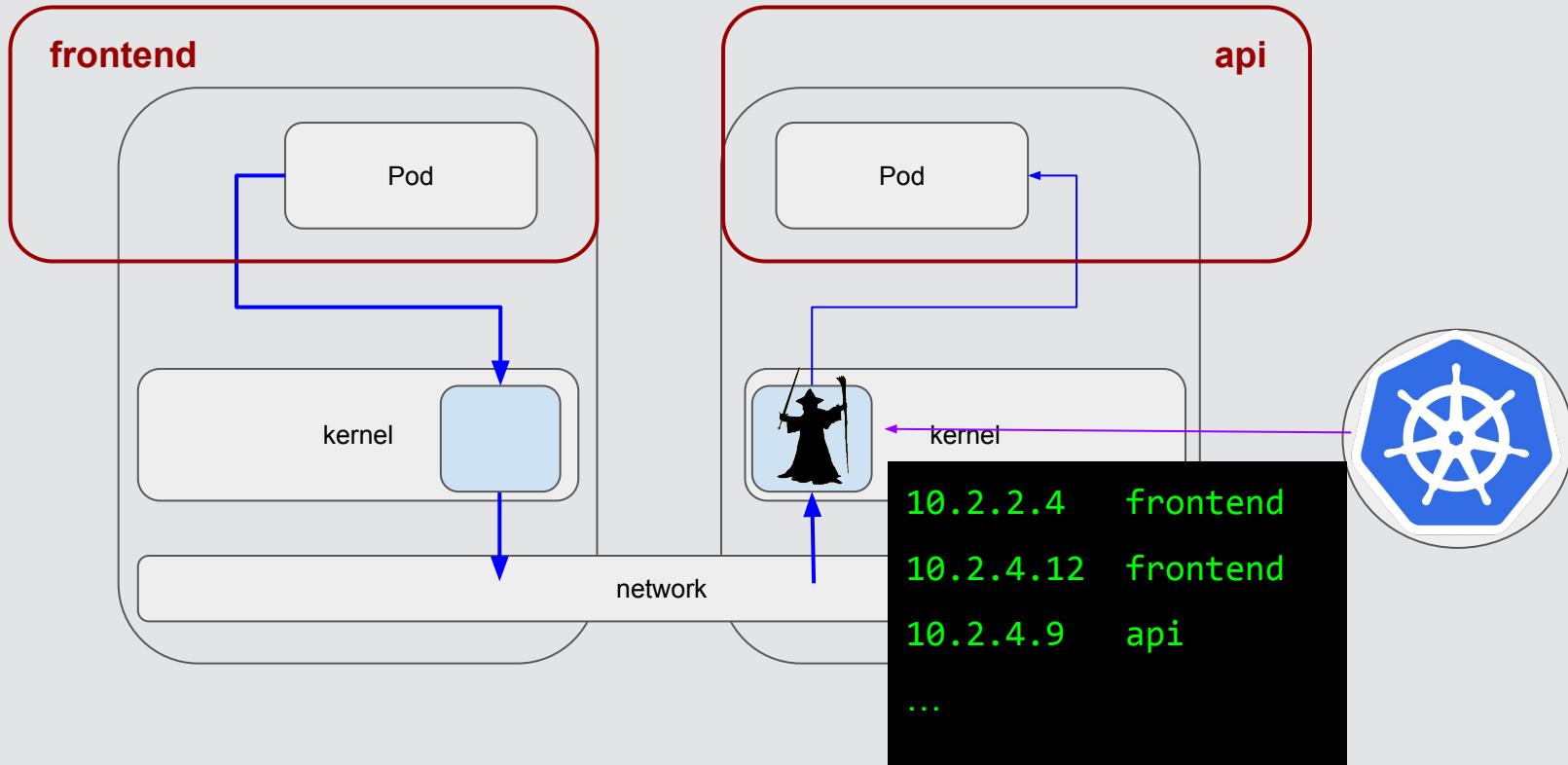


```
$ dear CNI: [pods in frontend] => [pods in api] == OK!
```

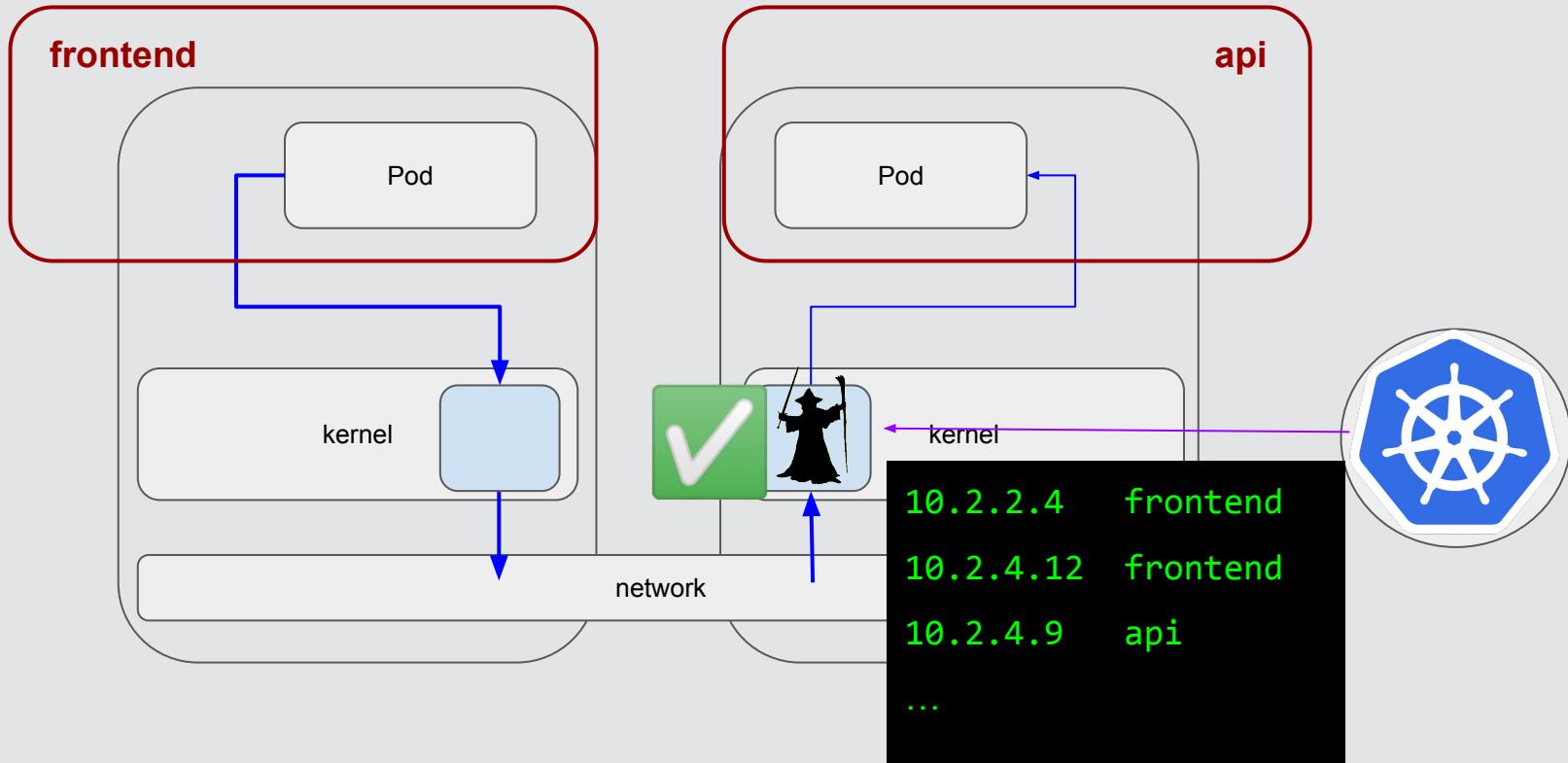
CNI - how is it enforced?



CNI - how is it enforced?

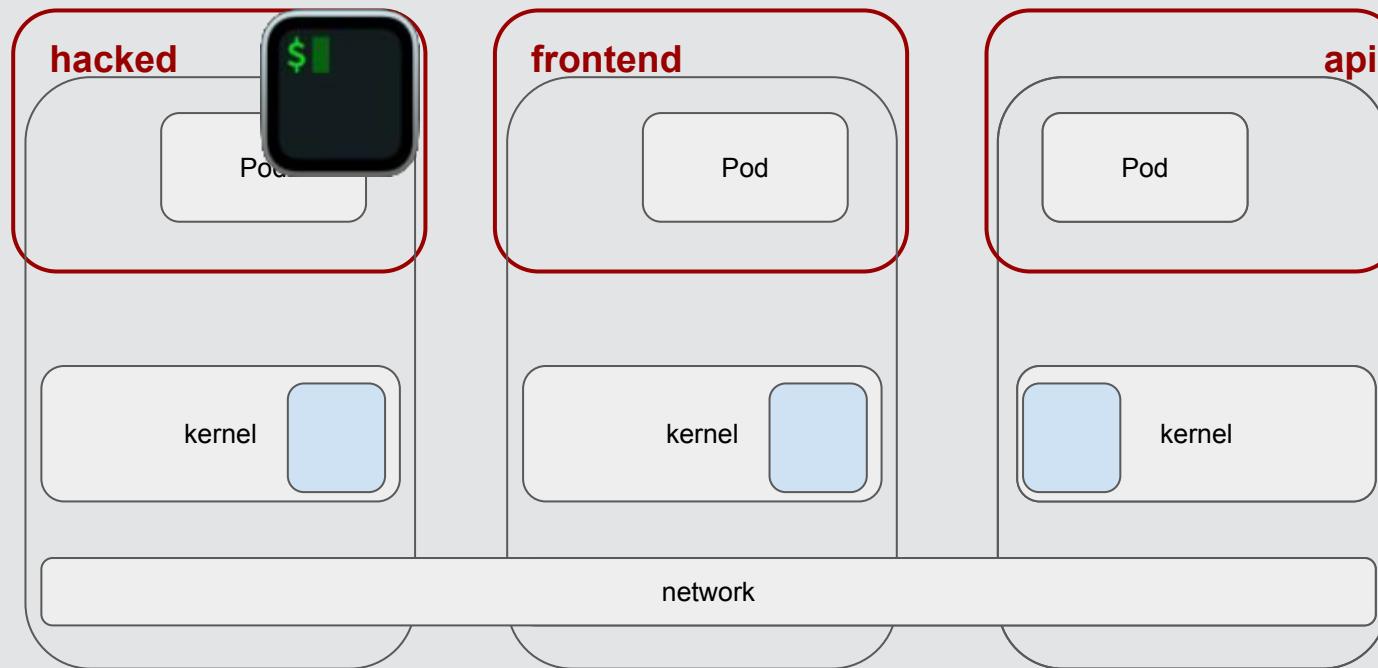


CNI - how is it enforced?



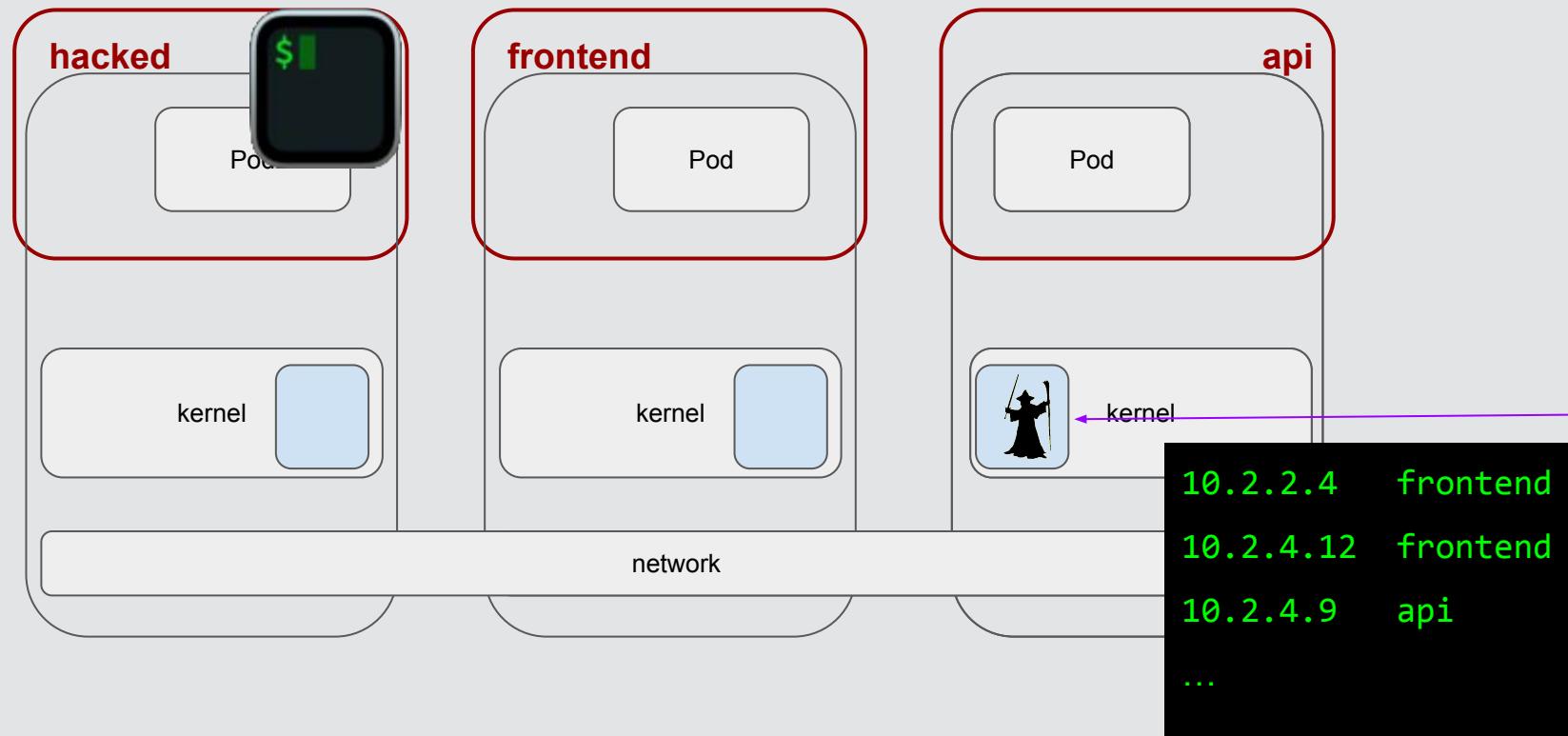
It's time for a
contrived
scenario!

CNI - contrived scenario

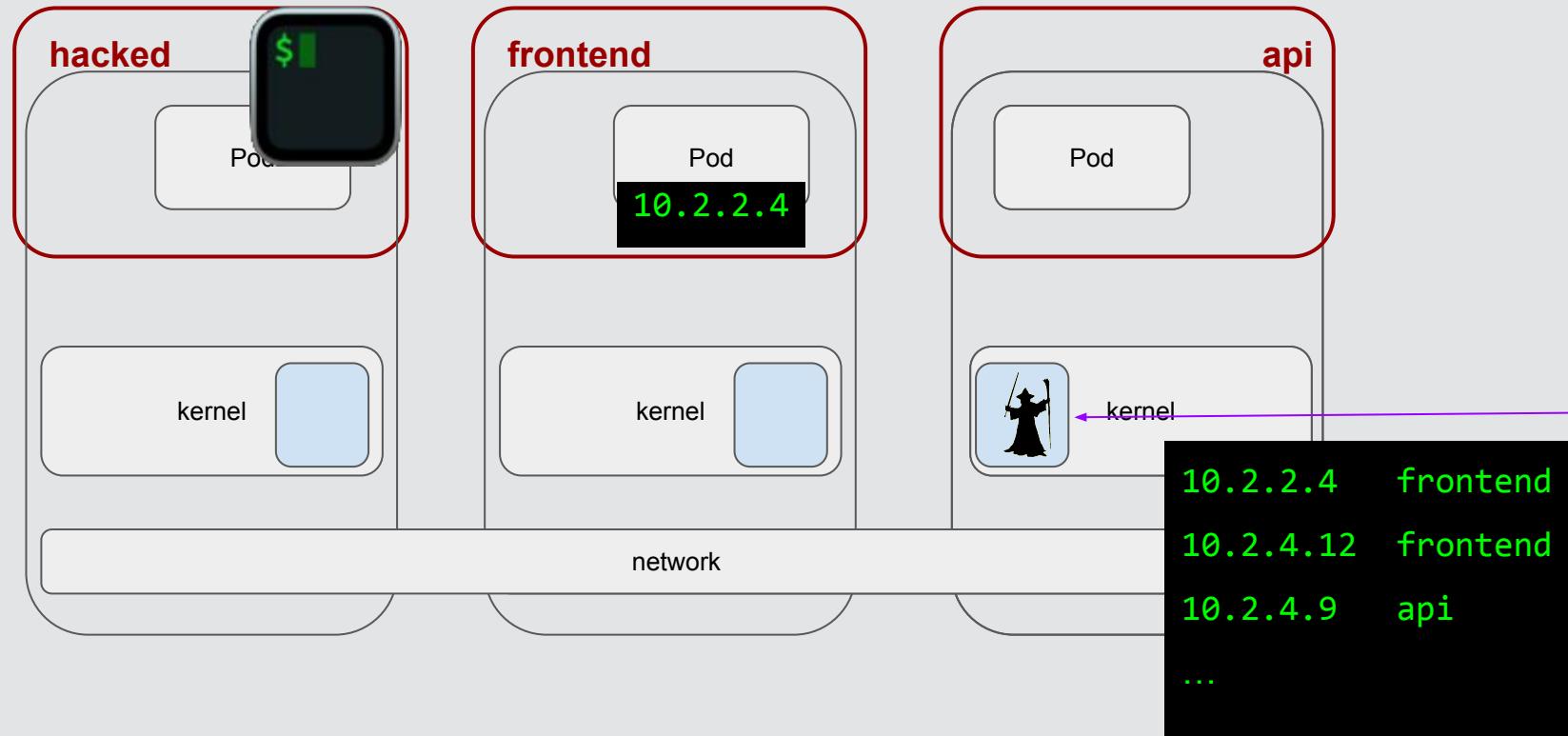


```
$ dear CNI: [pods in frontend] => [pods in api] == OK!
```

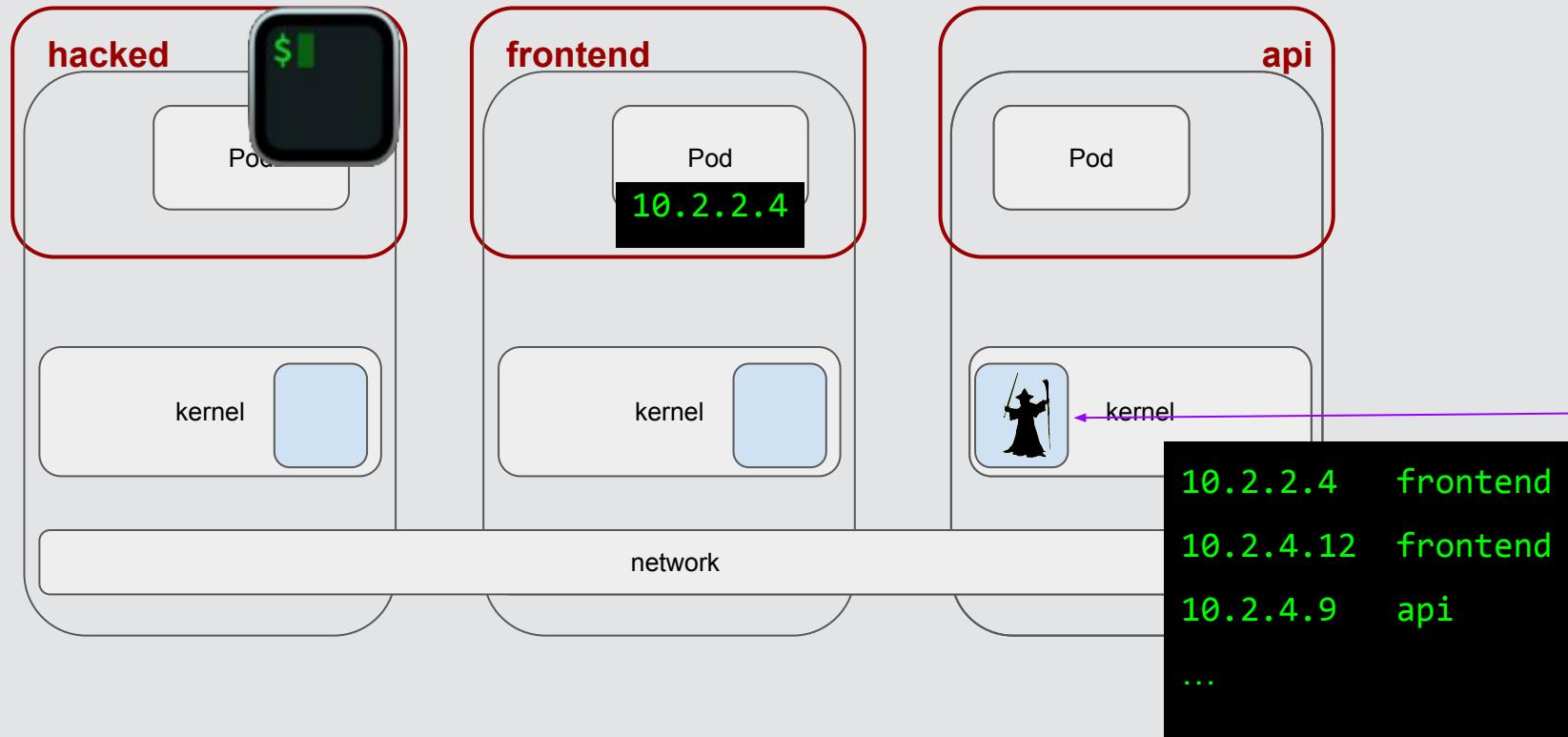
CNI - contrived scenario



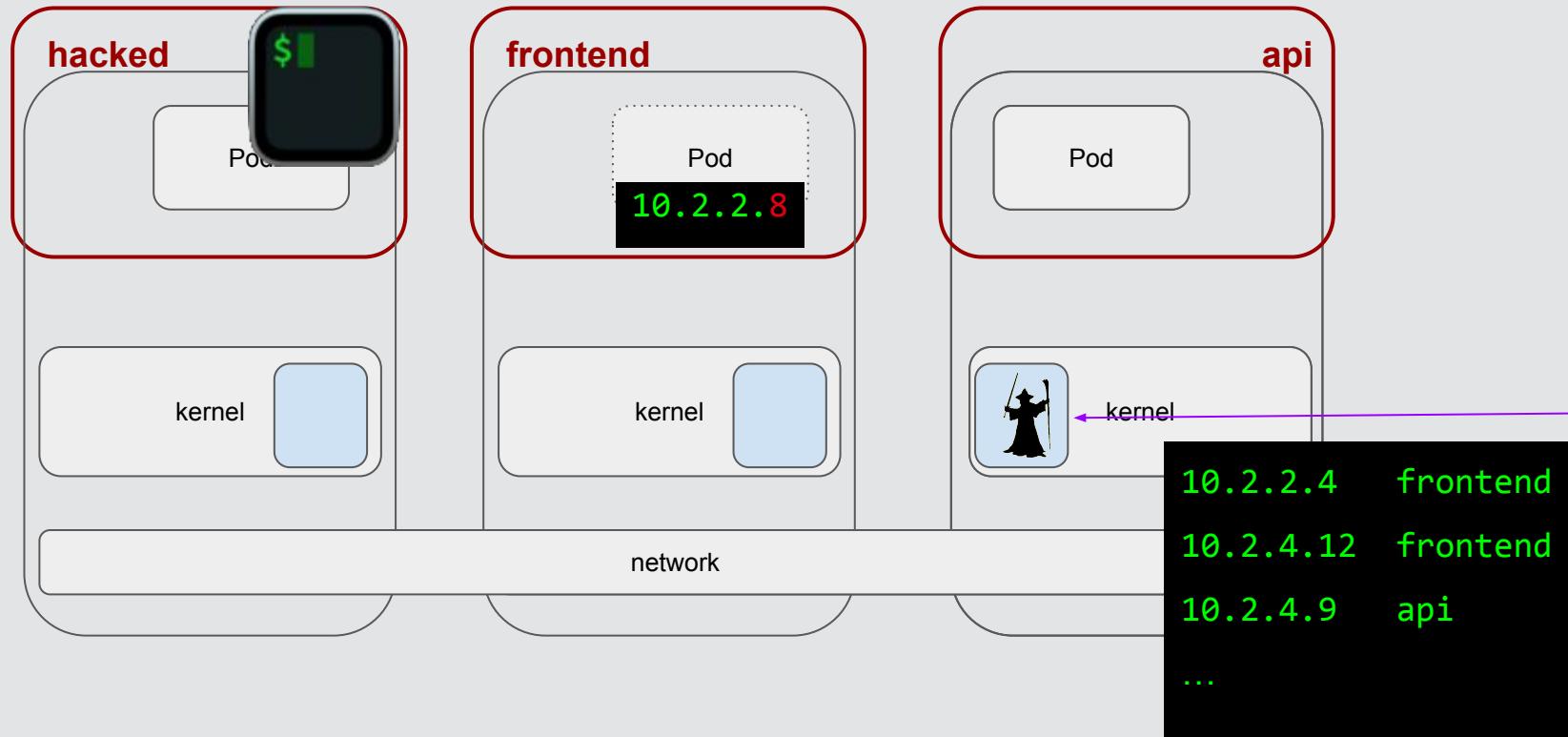
CNI - contrived scenario



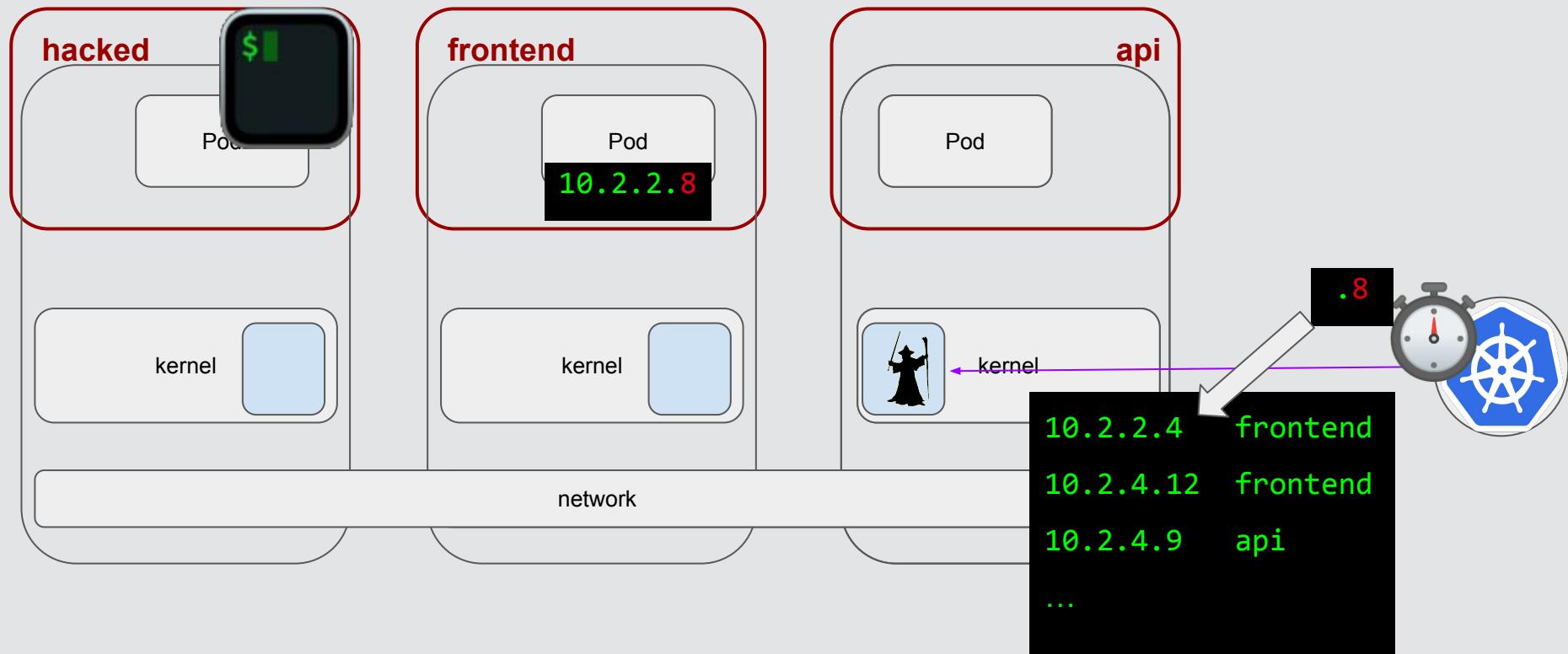
CNI - contrived scenario



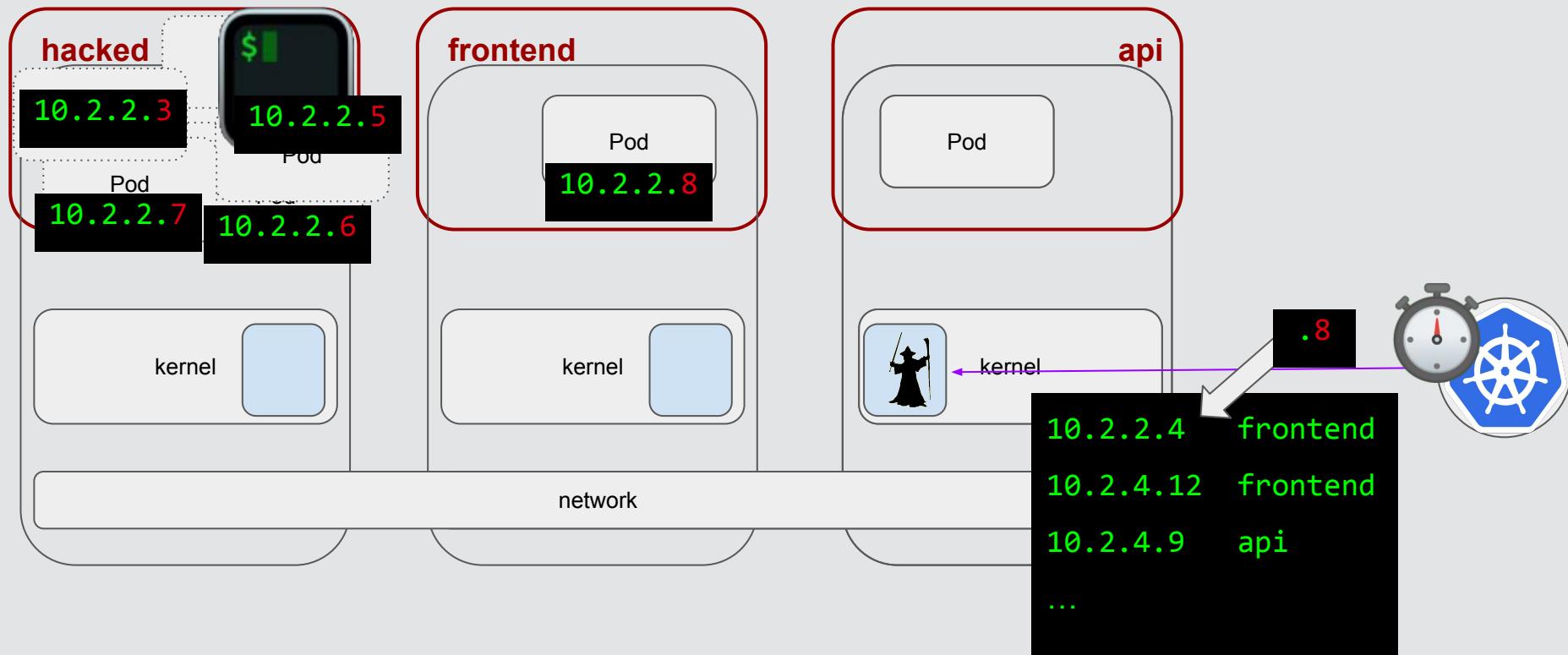
CNI - contrived scenario



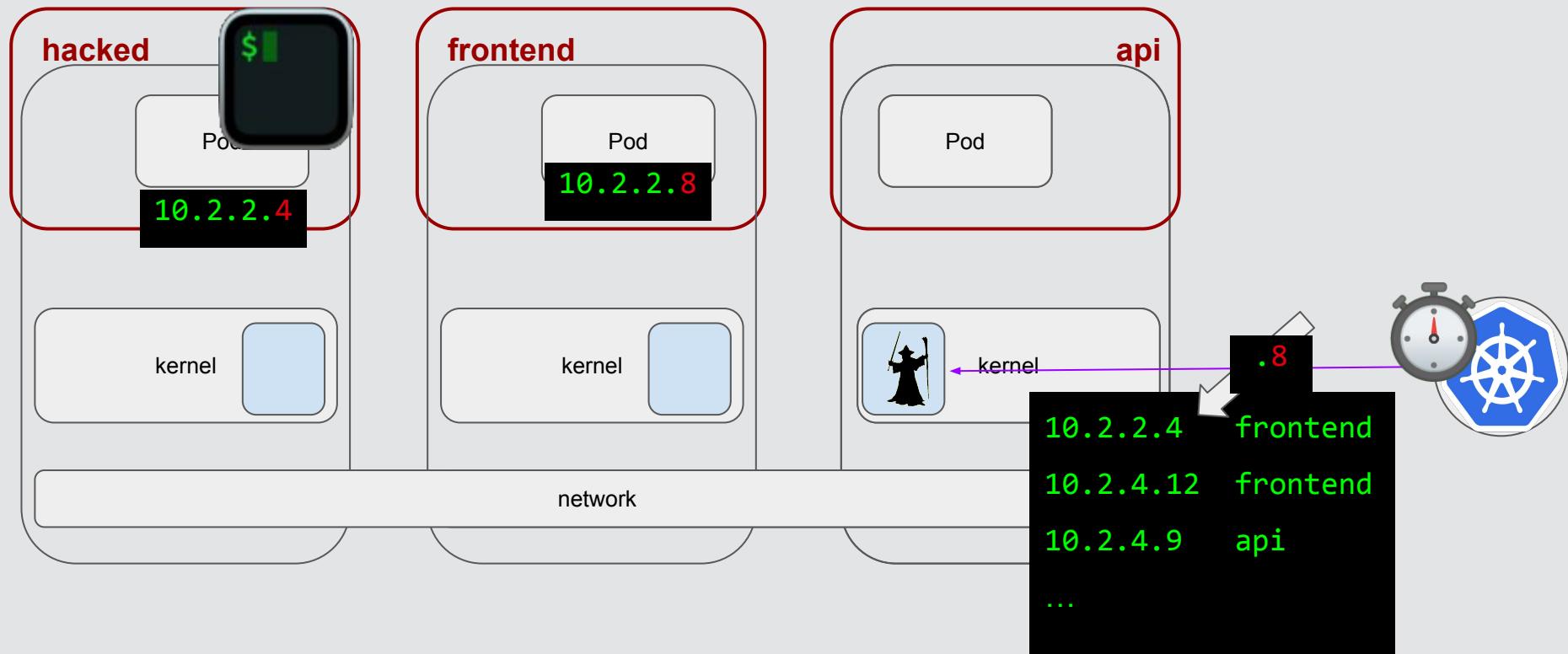
CNI - contrived scenario



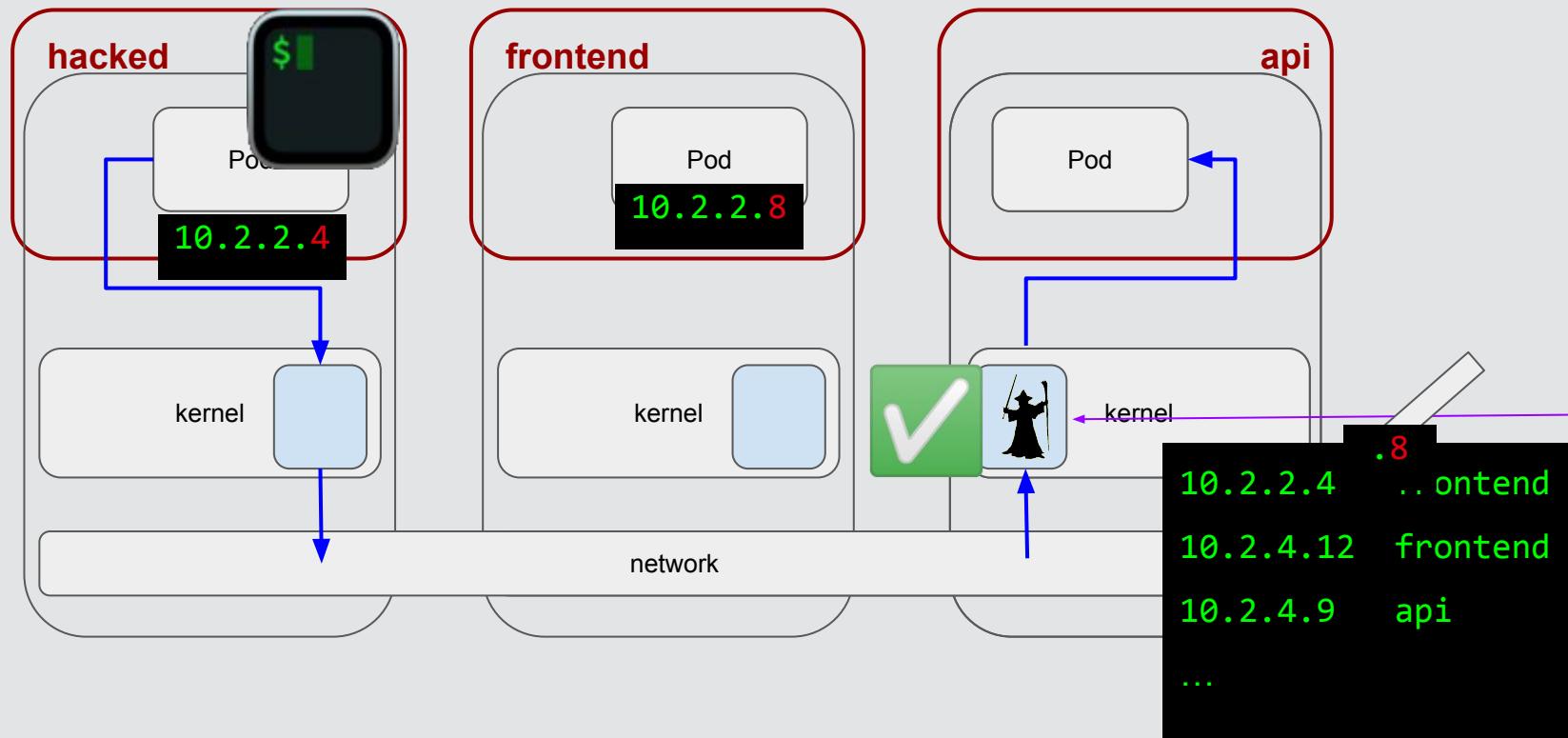
CNI - contrived scenario



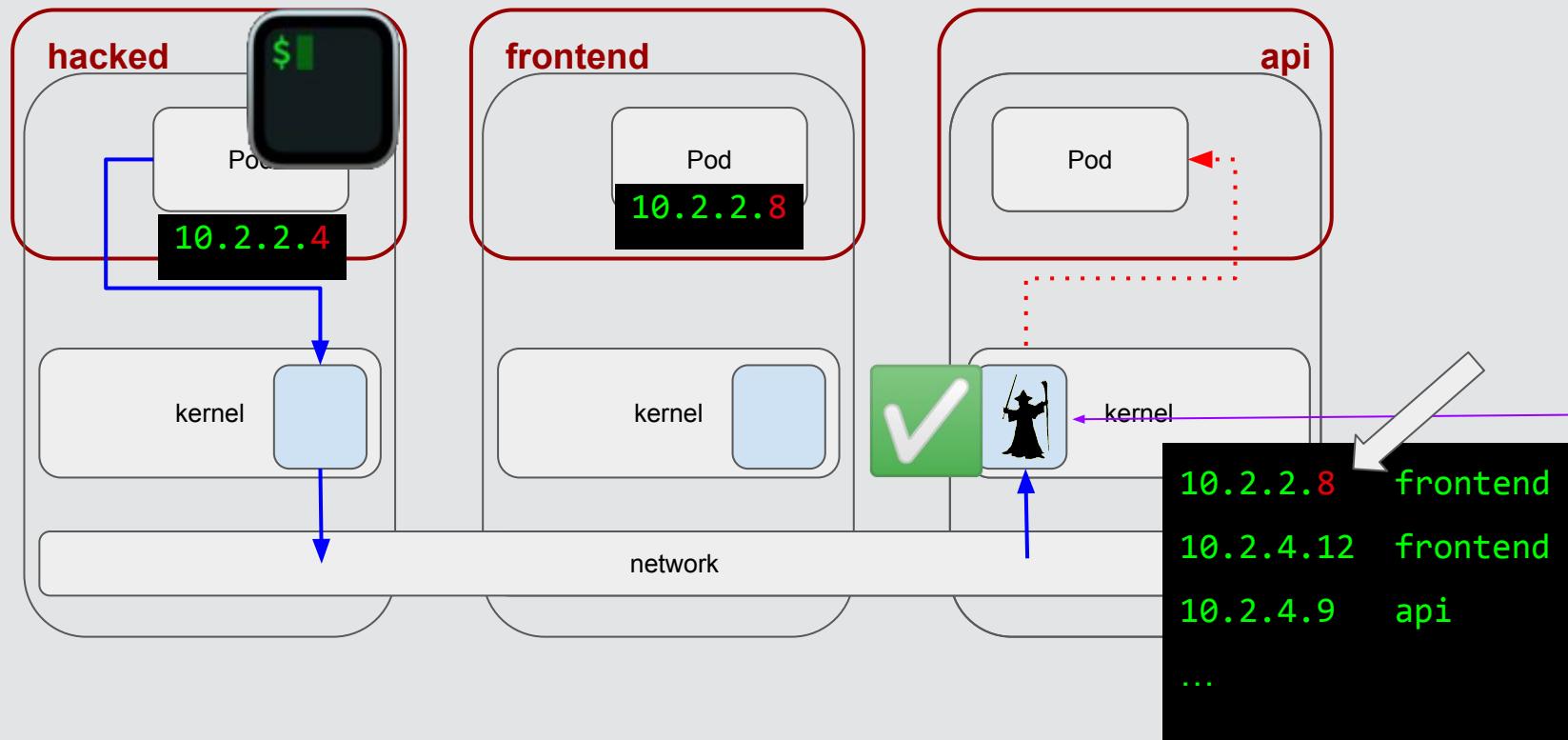
CNI - contrived scenario



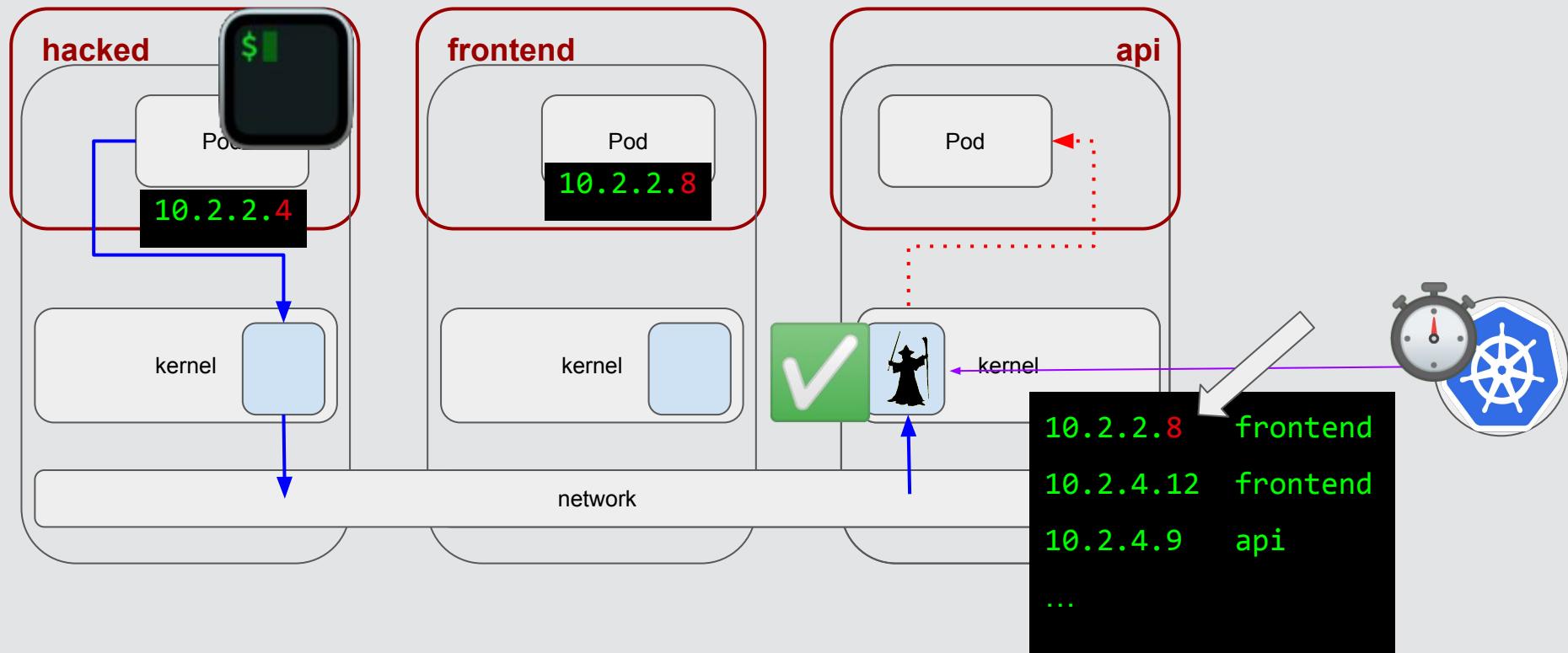
CNI - contrived scenario



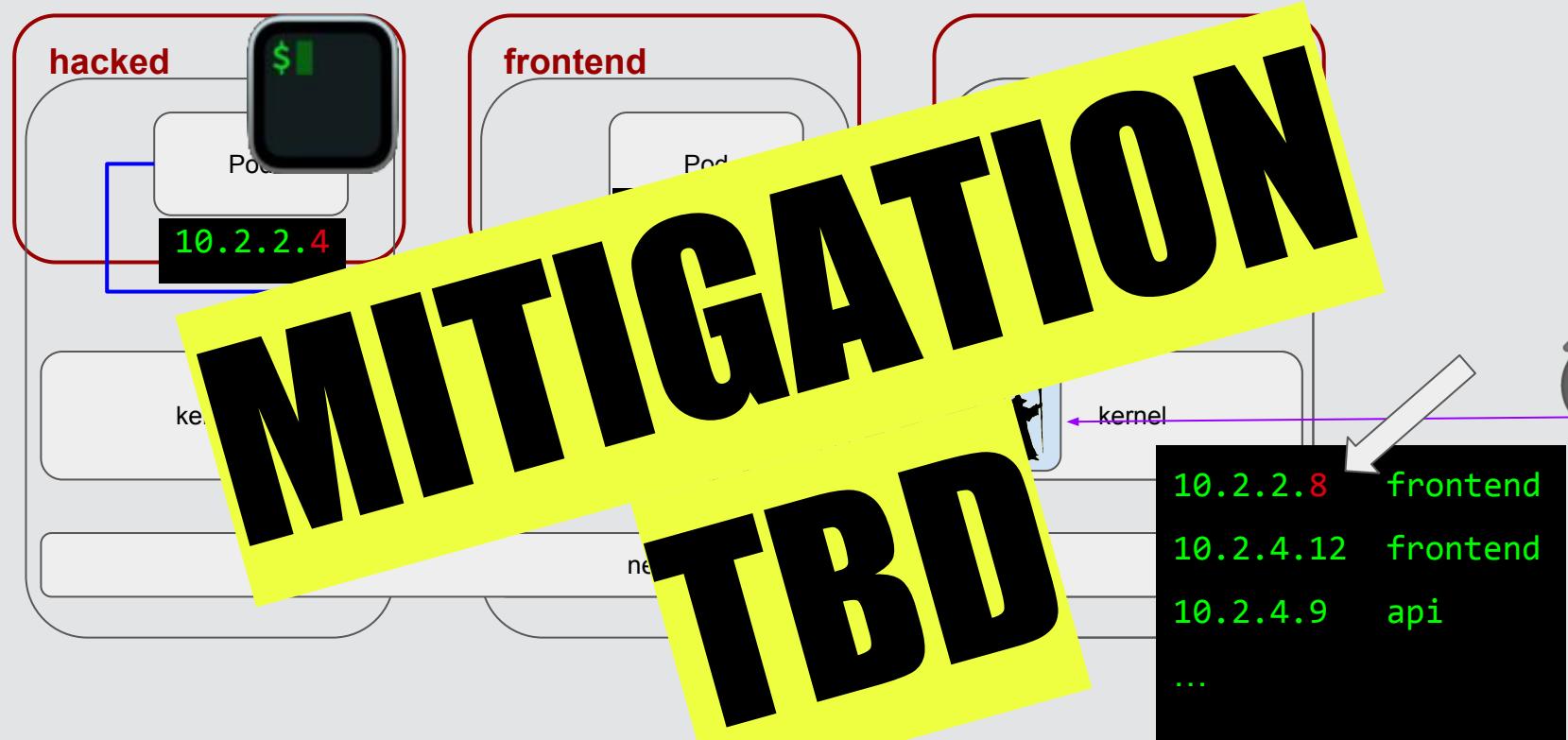
CNI - contrived scenario



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?

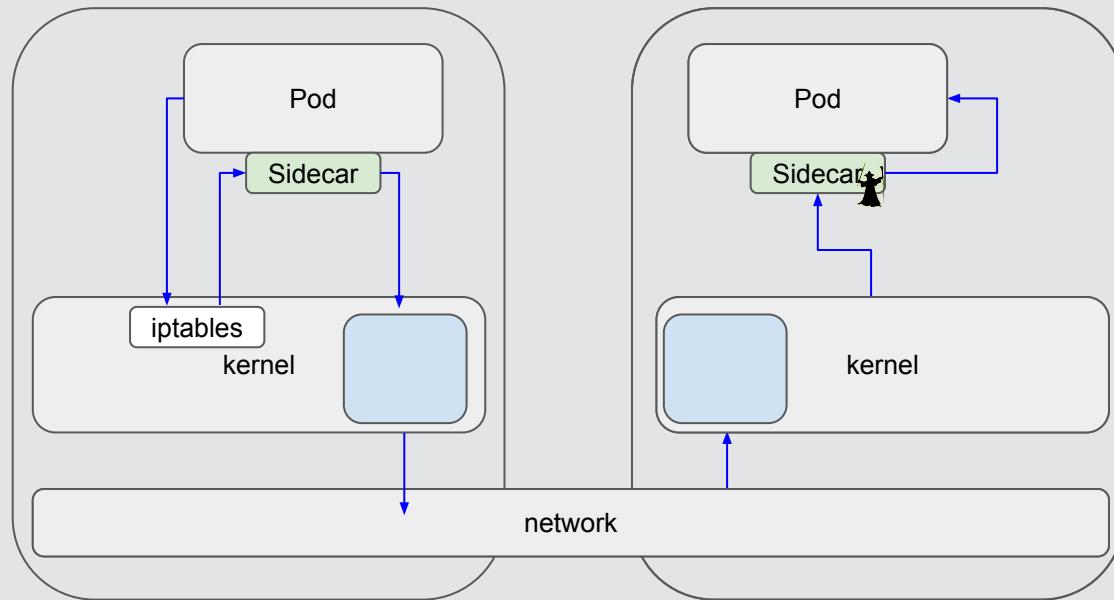


```
$ kubectl explain ${SERVICE_MESH_AUTH_POLICY}
```

- 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

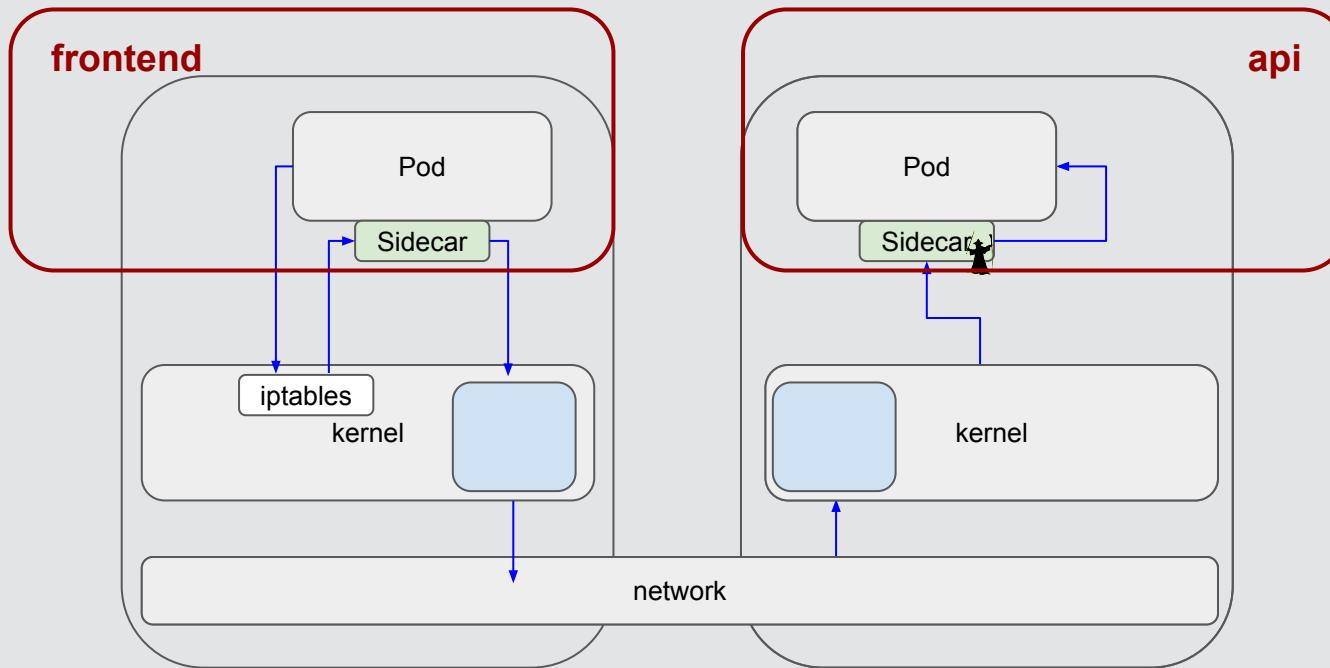
* including loopback or host traffic

Svc Mesh - how is it enforced?



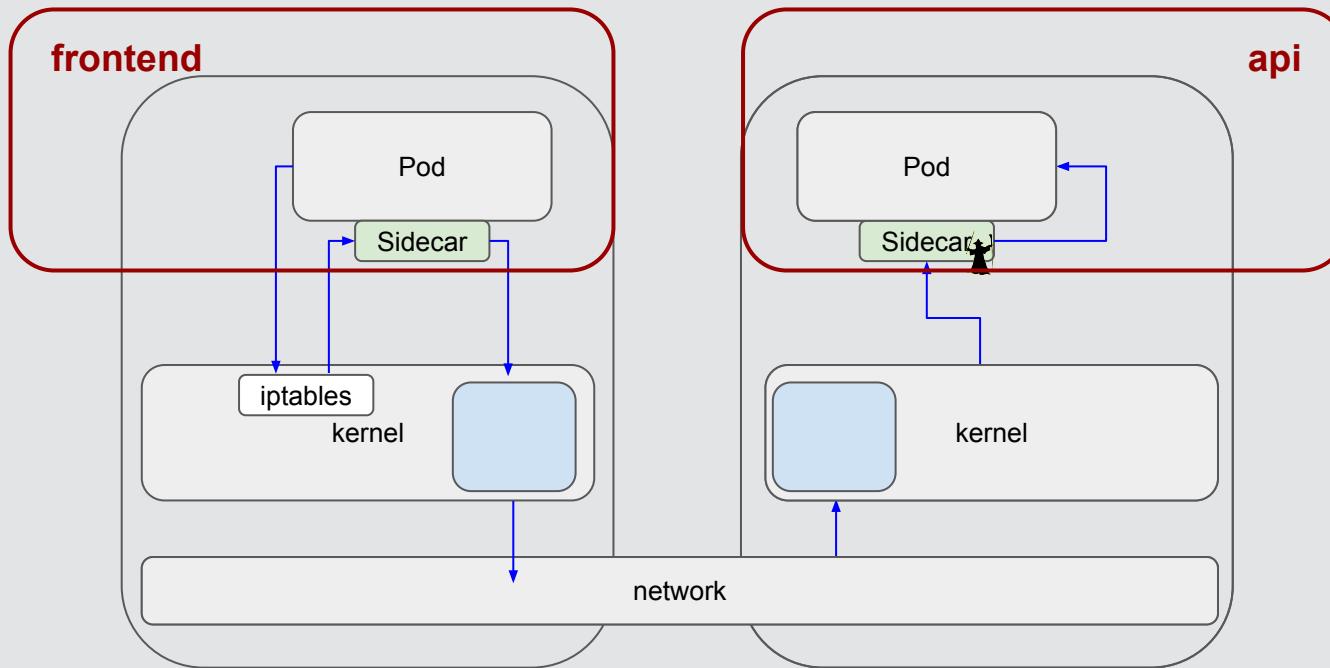
—→ control
—→ data

Svc Mesh - how is it enforced?



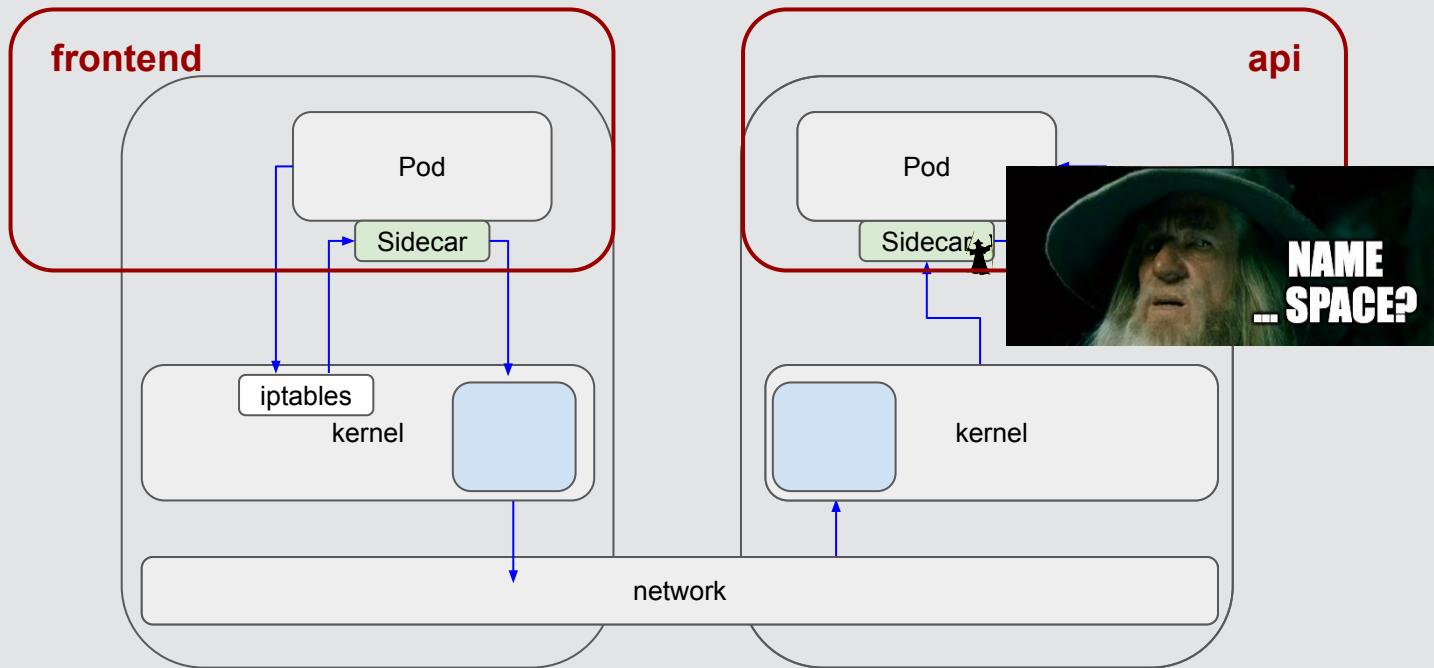
control
data

Svc Mesh - how is it enforced?



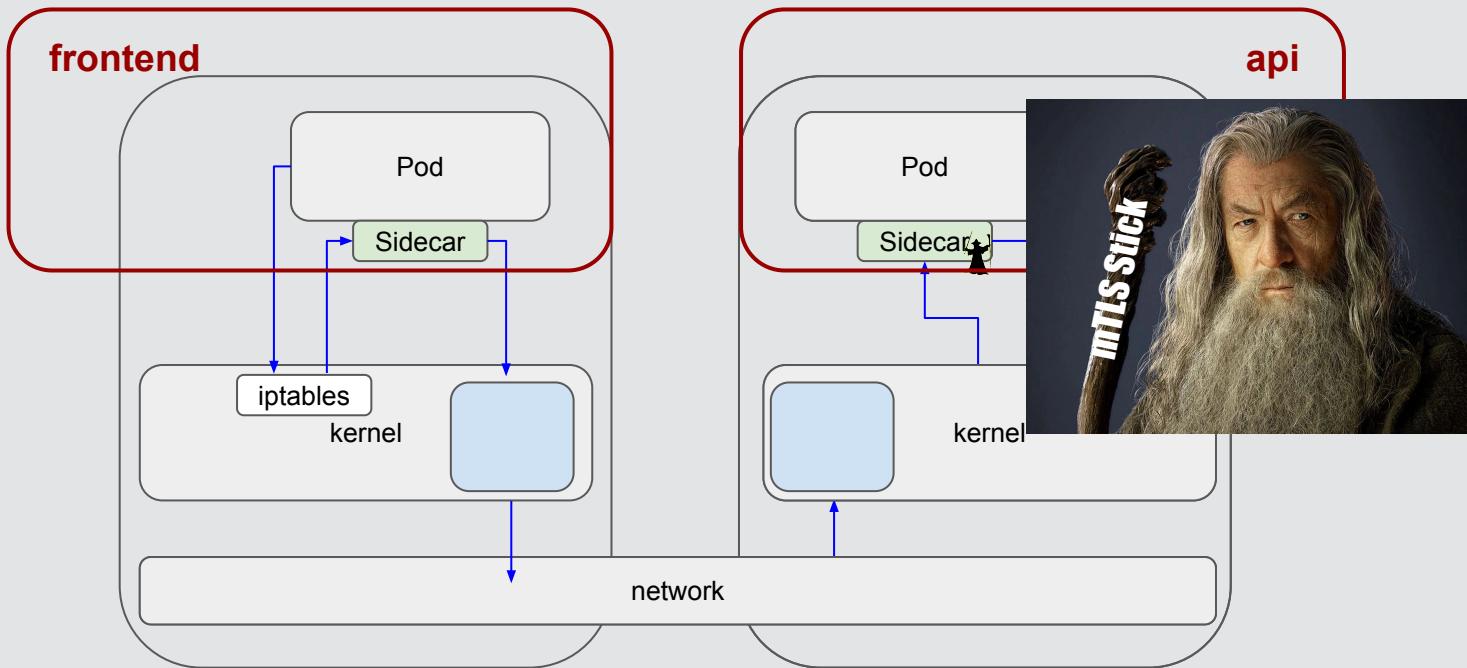
```
$ dear Service Mesh: [pods in frontend] => [pods in api] == OK!
```

Svc Mesh - how is it enforced?



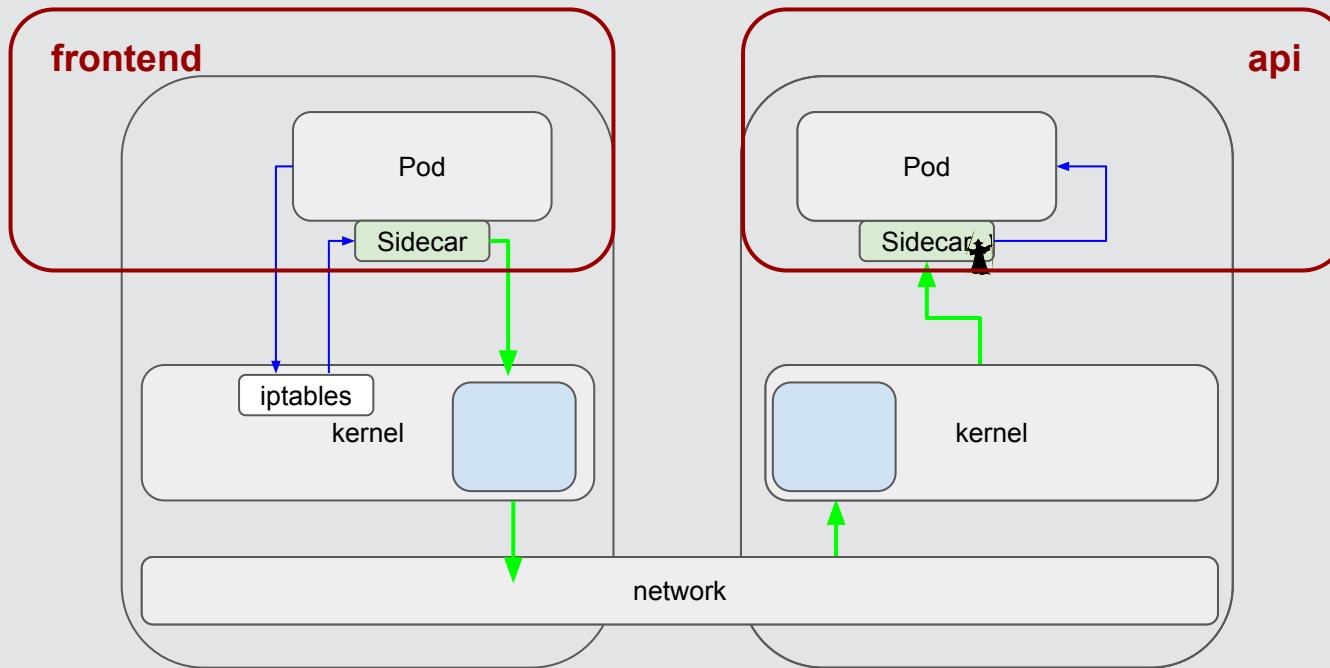
```
$ dear Service Mesh: [pods in frontend] => [pods in api] == OK!
```

Svc Mesh - how is it enforced?



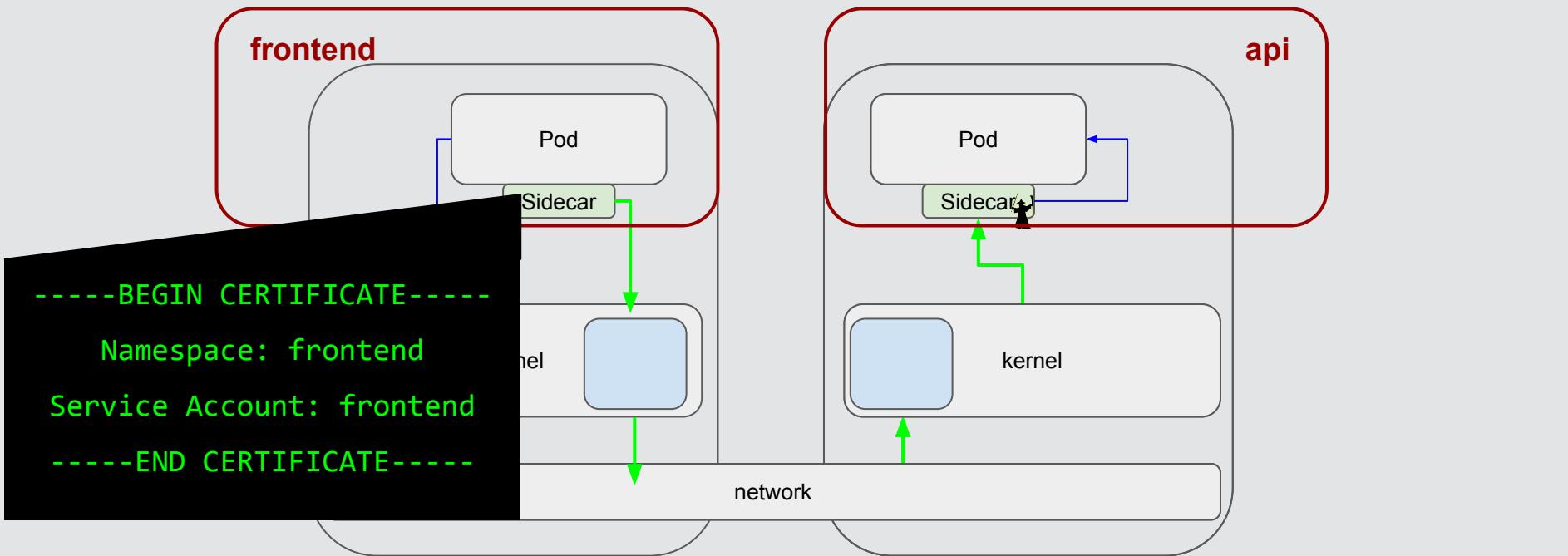
```
$ dear Service Mesh: [pods in frontend] => [pods in api] == OK!
```

Svc Mesh - how is it enforced?



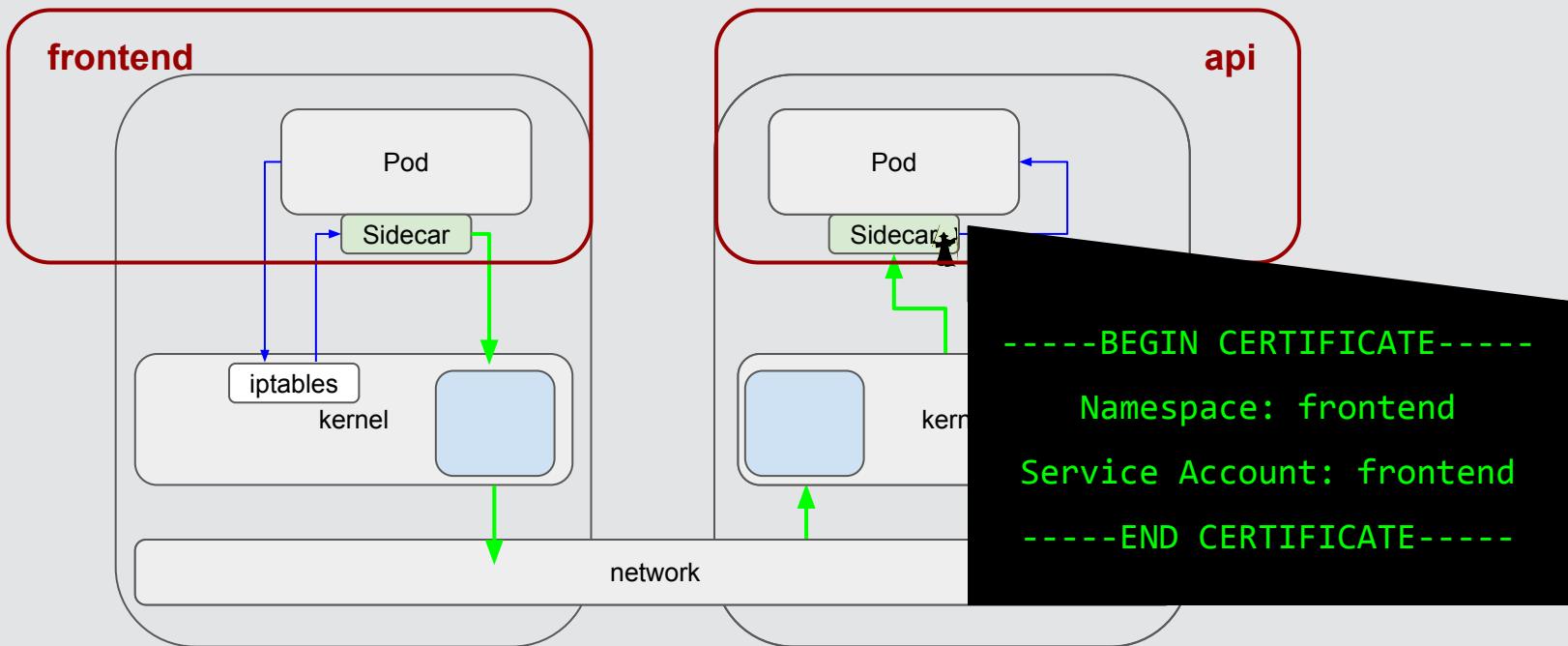
green → mTLS
purple → control
blue → data

Svc Mesh - how is it enforced?



→ mTLS
→ control
→ data

Svc Mesh - how is it enforced?



- mTLS
- control
- data

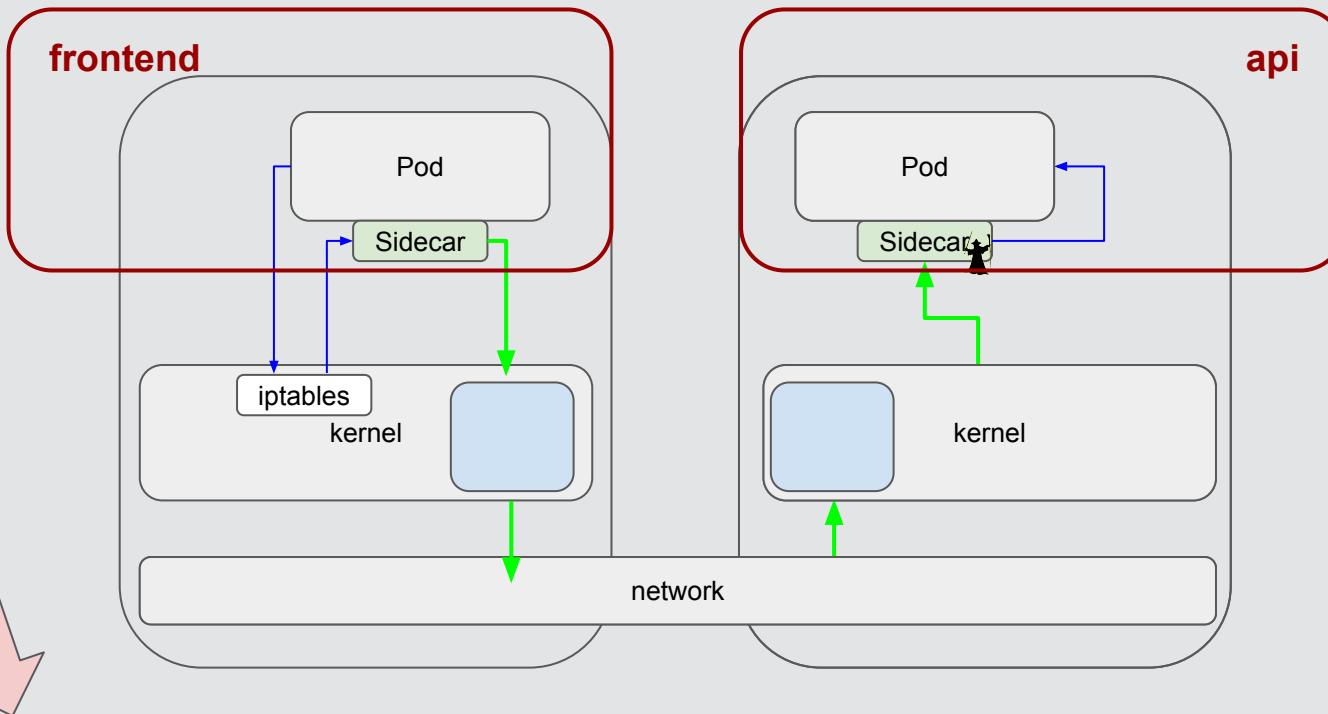
Svc Mesh - how is it enforced?



Svc Mesh - how is it enforced?



1

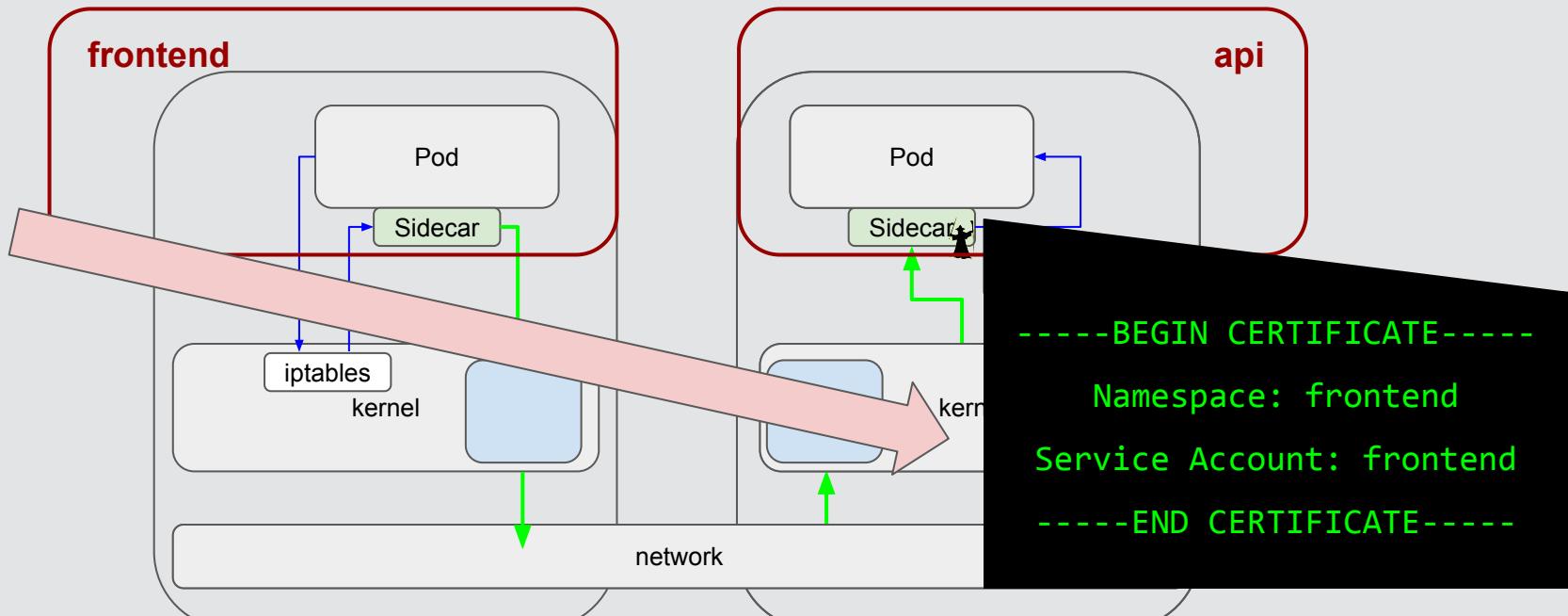


\$ dear Service Mesh: [pods in frontend] => [pods in api] == OK!

Svc Mesh - how is it enforced?



2



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

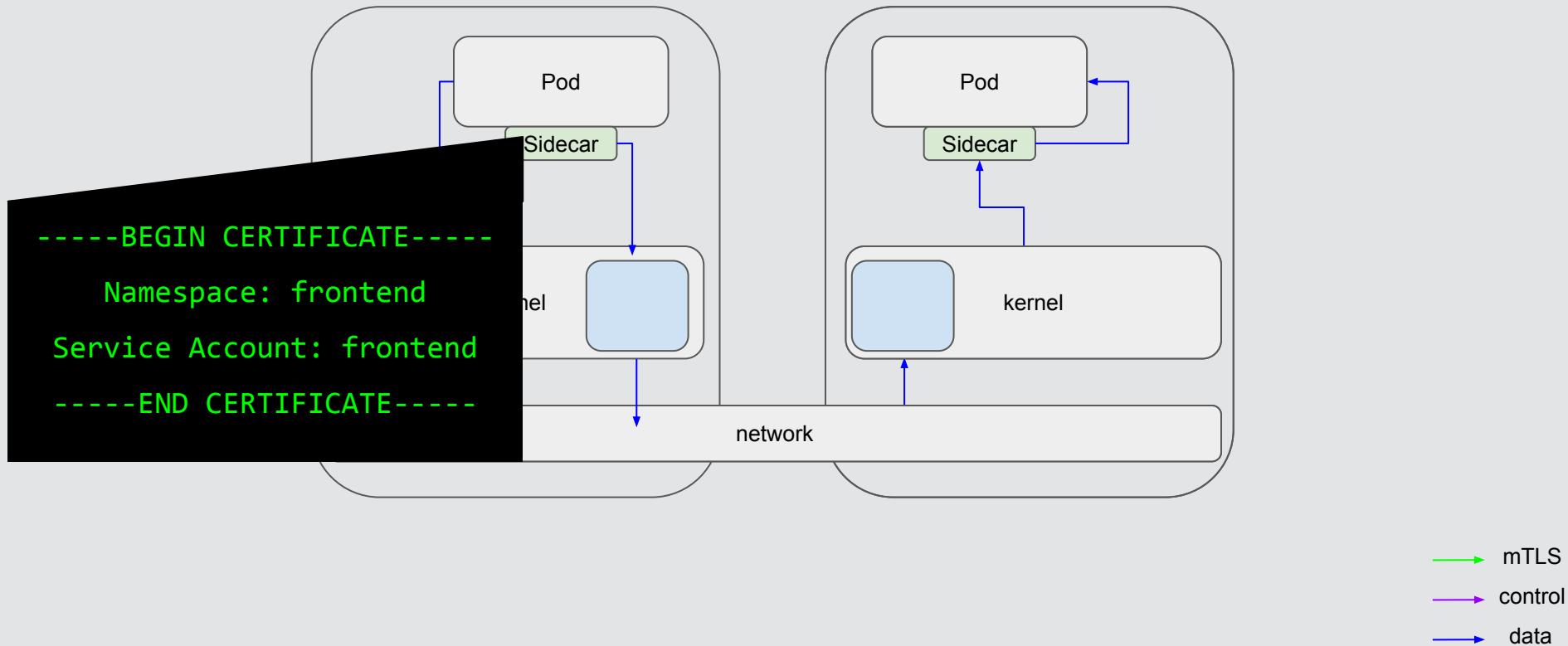
Client Cert - how is it secured?



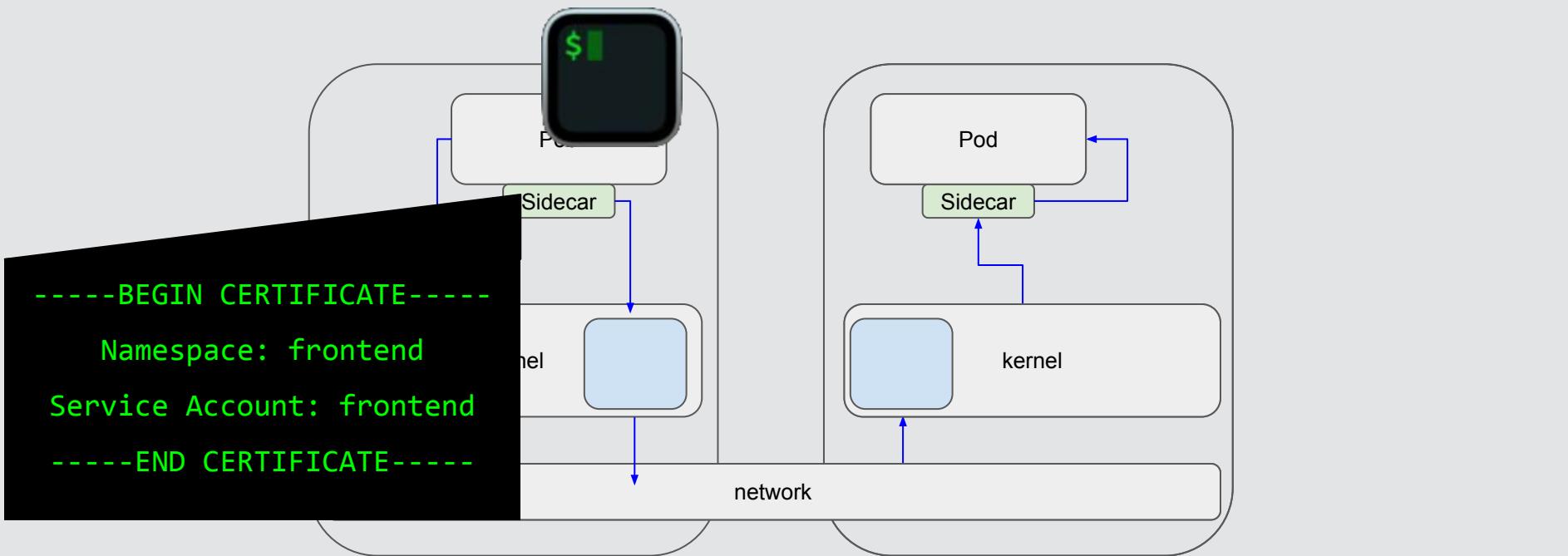
```
-----BEGIN CERTIFICATE-----  
Namespace: frontend  
Service Account: frontend  
-----END CERTIFICATE-----
```

- mTLS
- control
- data

Client Cert - how is it secured?

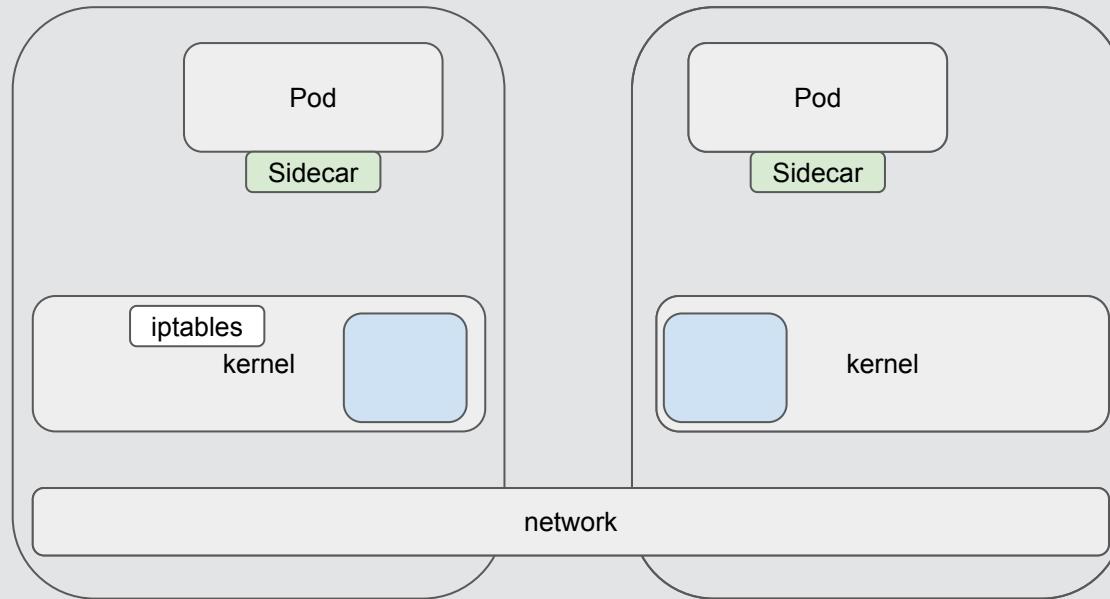


Client Cert - how is it secured?



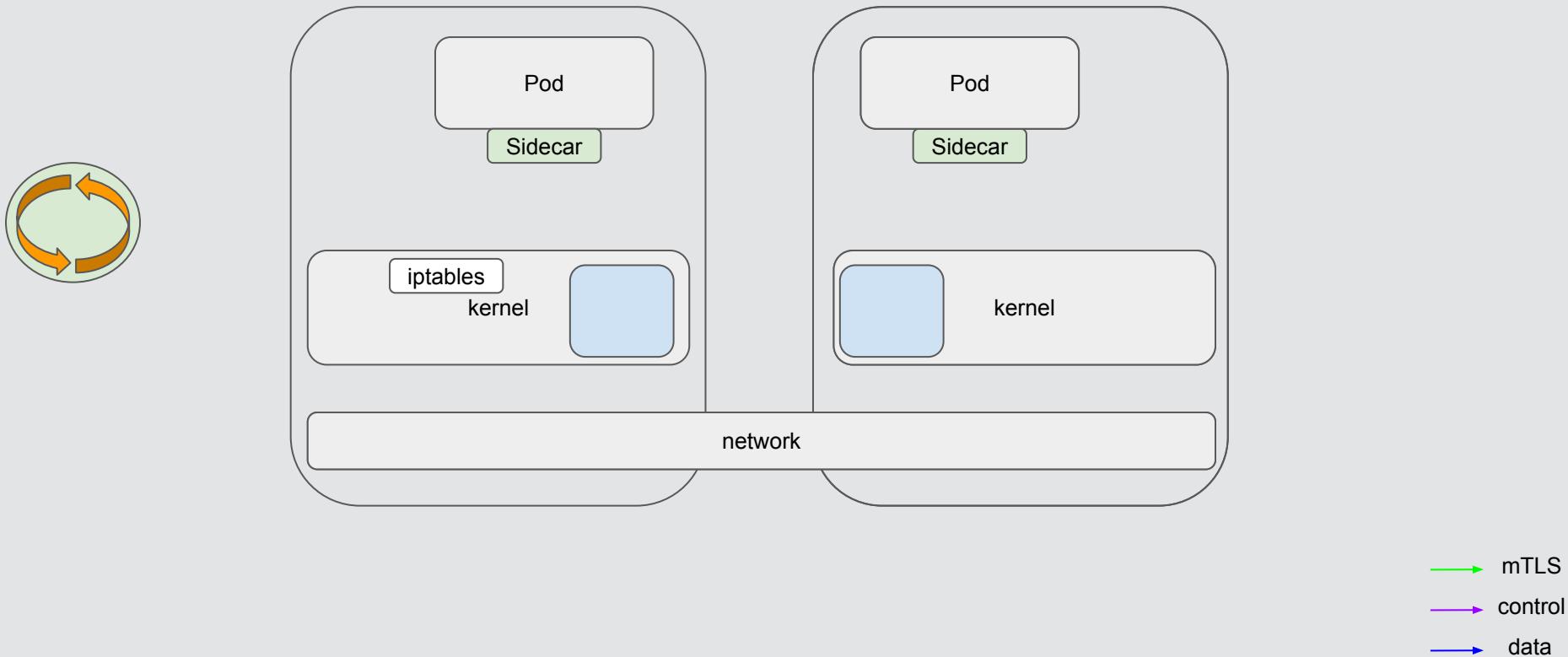
- mTLS
- control
- data

Client Cert - how is it issued?

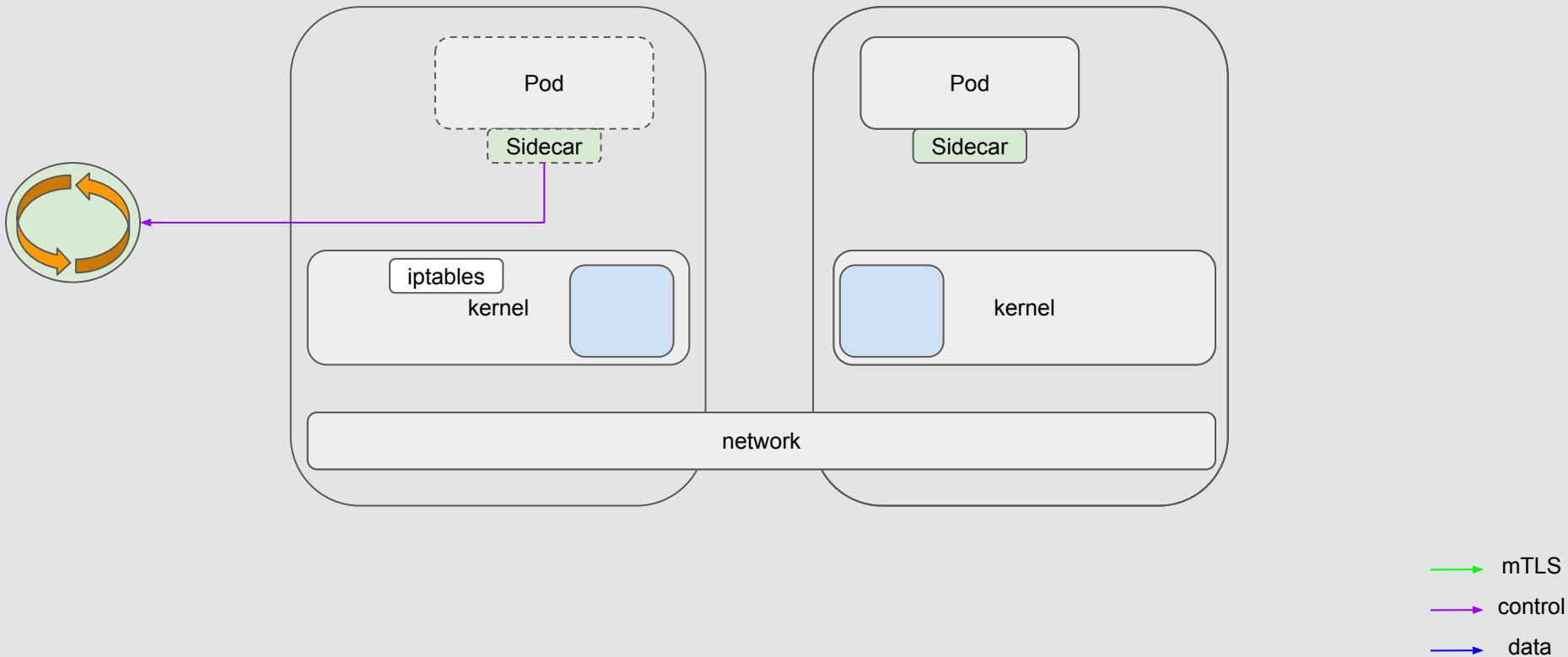


→ mTLS
→ control
→ data

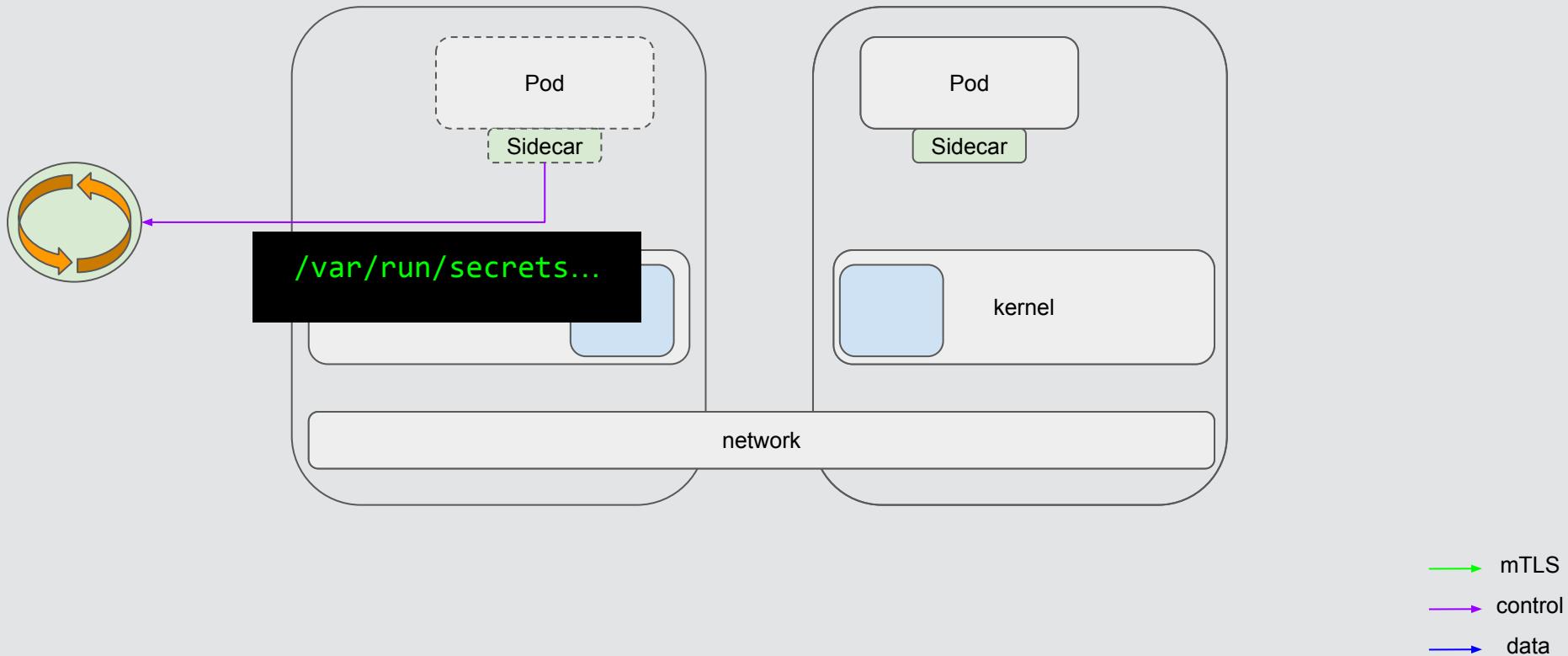
Client Cert - how is it issued?



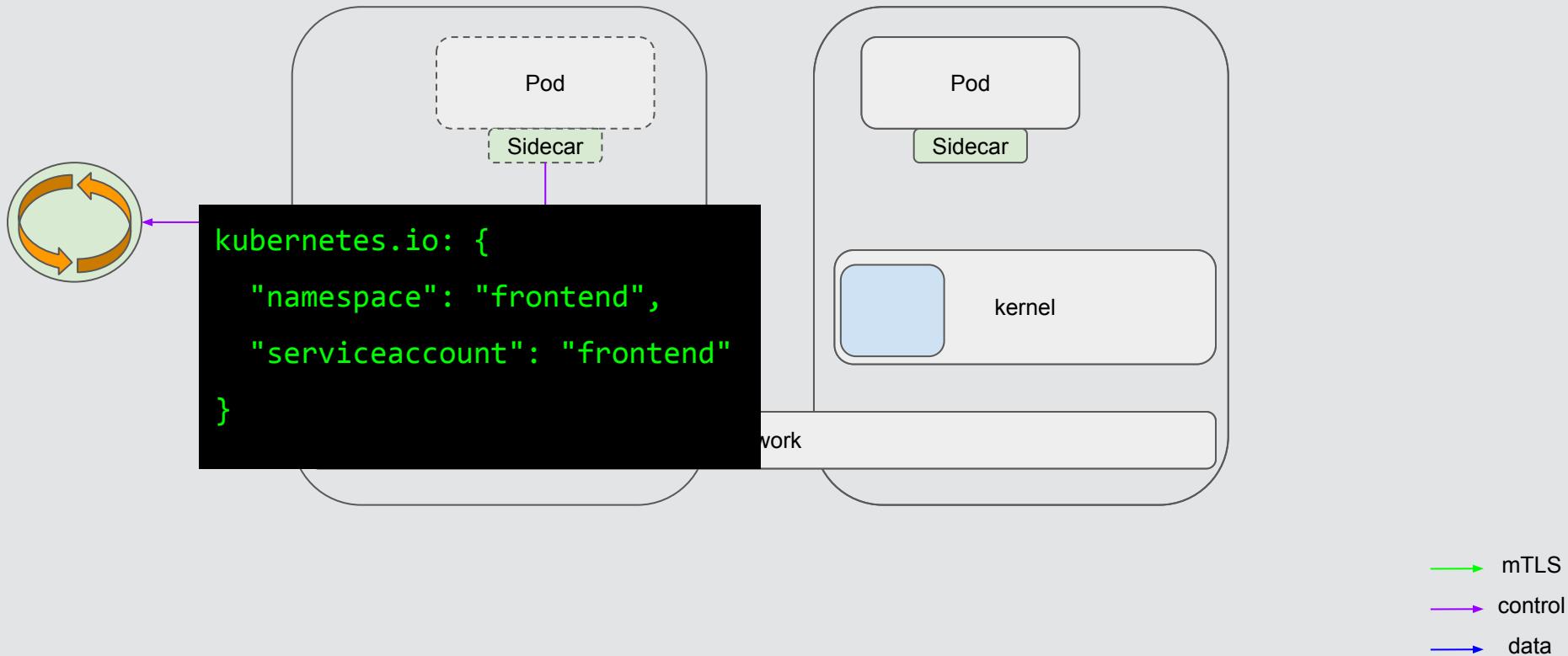
Client Cert - how is it issued?



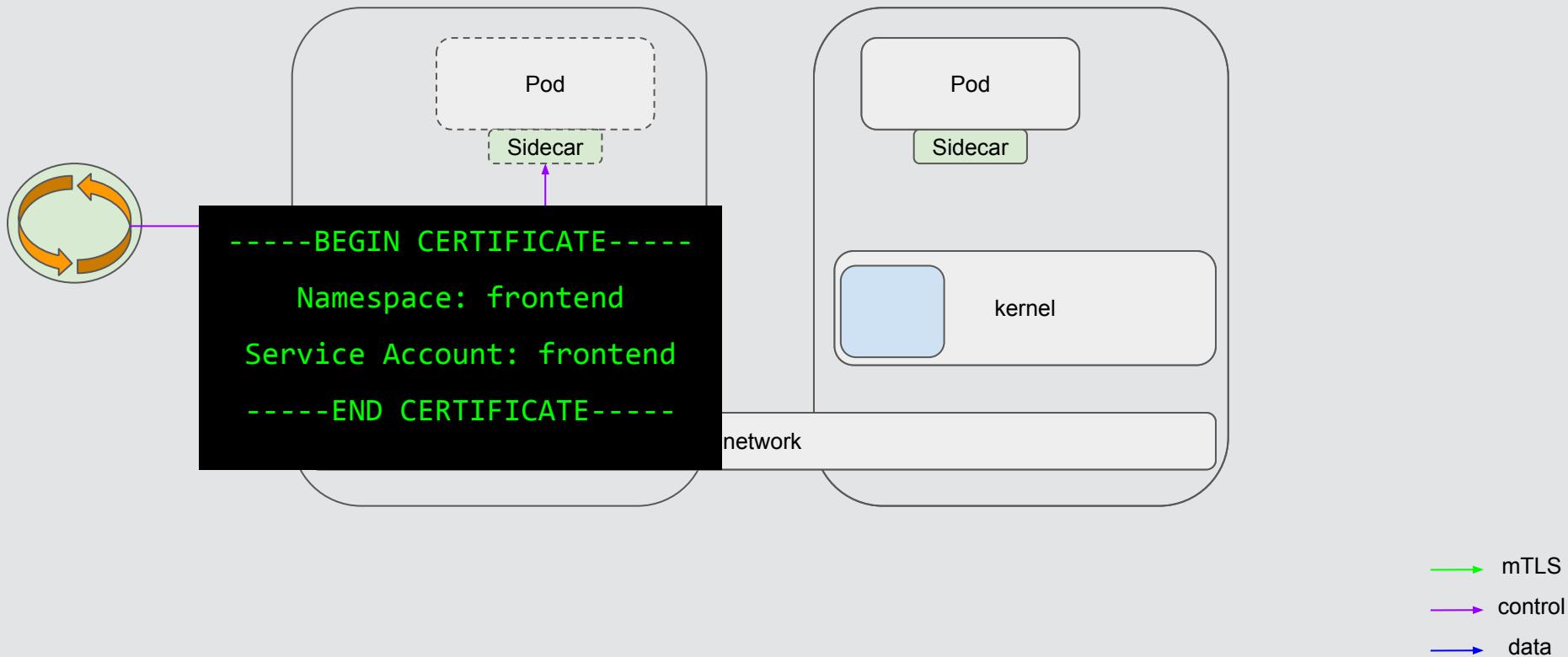
Client Cert - how is it issued?



Client Cert - how is it issued?

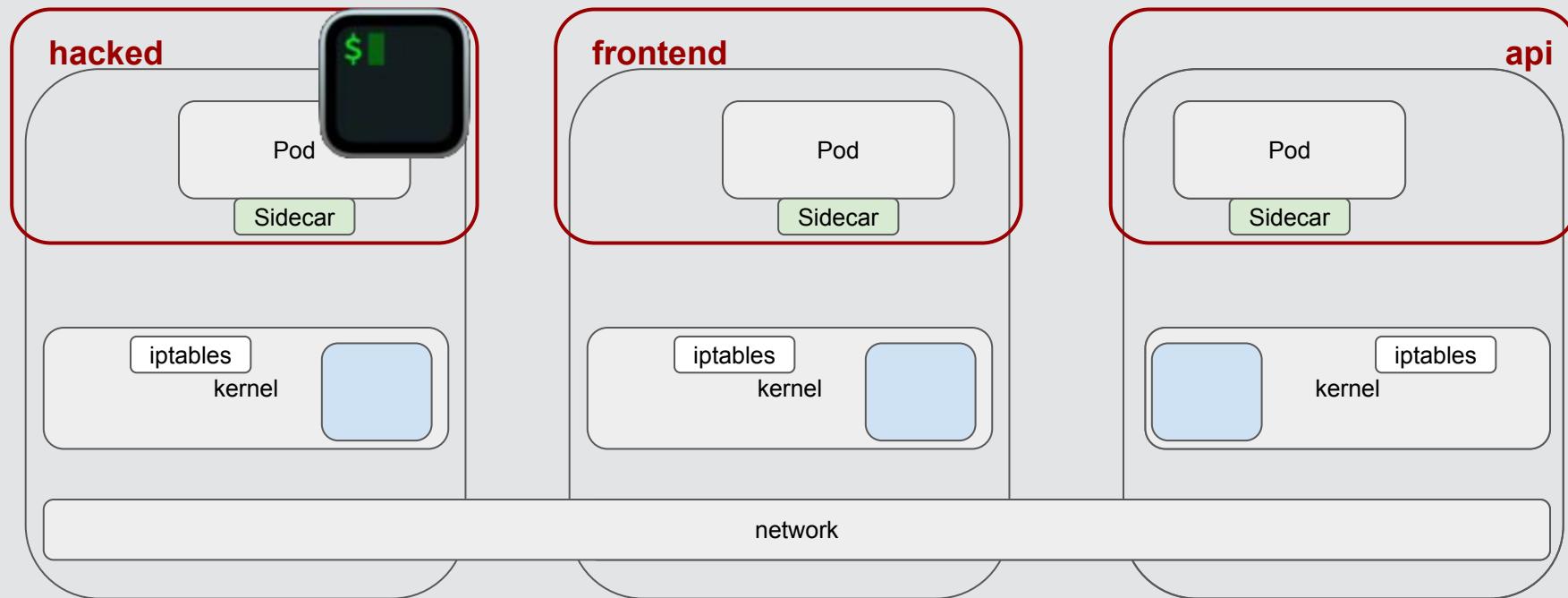


Client Cert - how is it issued?



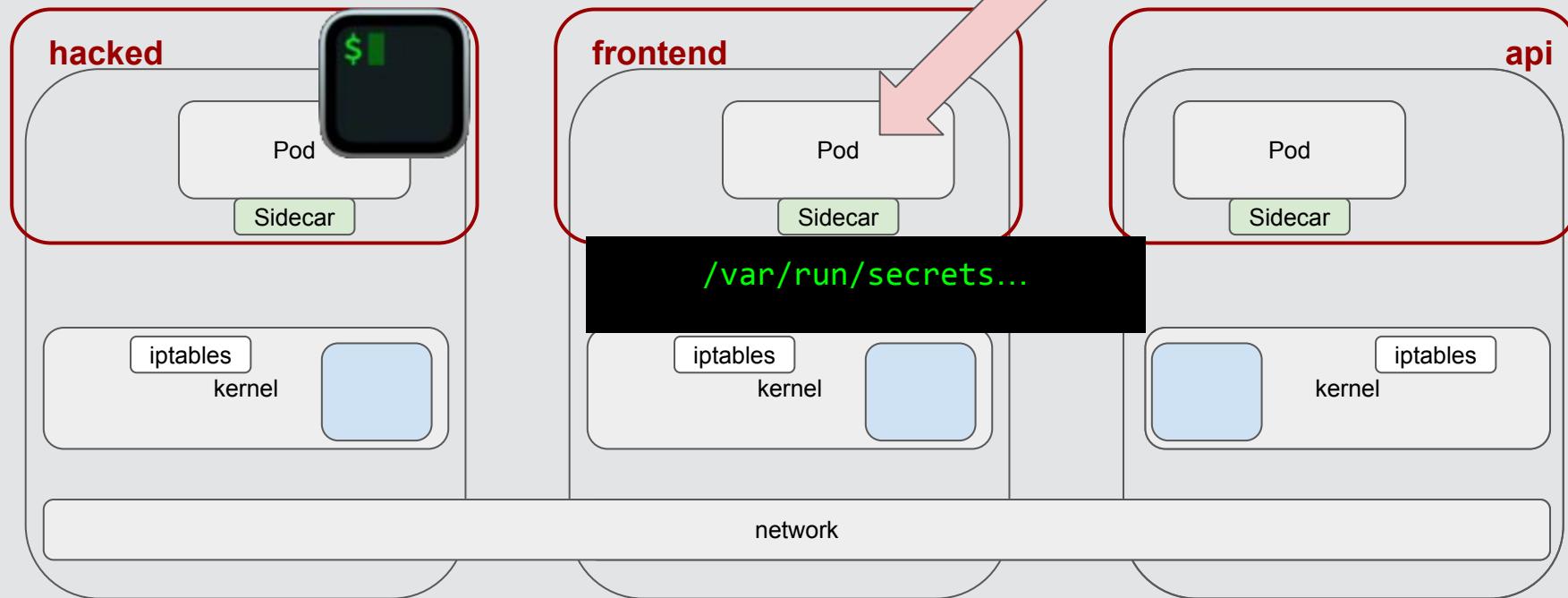
It's time for a
another
contrived
scenario!

Svc Mesh - contrived scenario



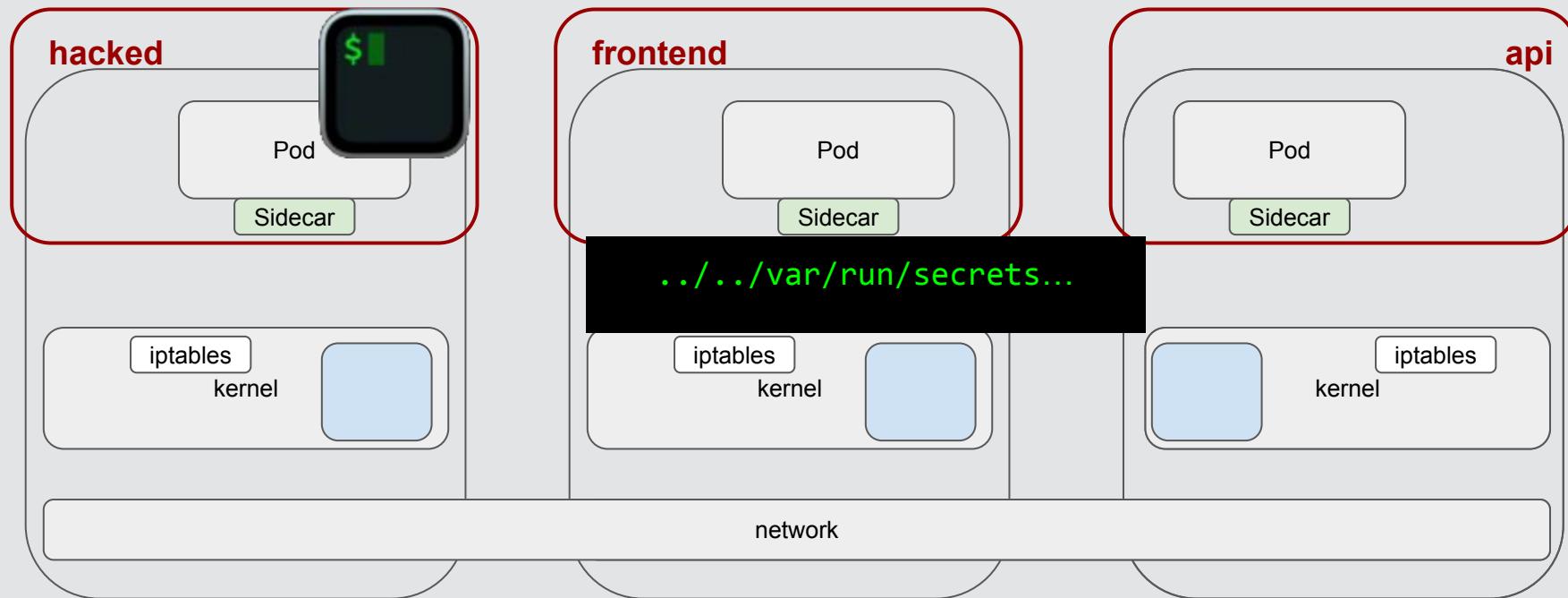
```
$ dear Service Mesh: [pods in frontend] => [pods in api] == OK!
```

Svc Mesh - contrived scenario



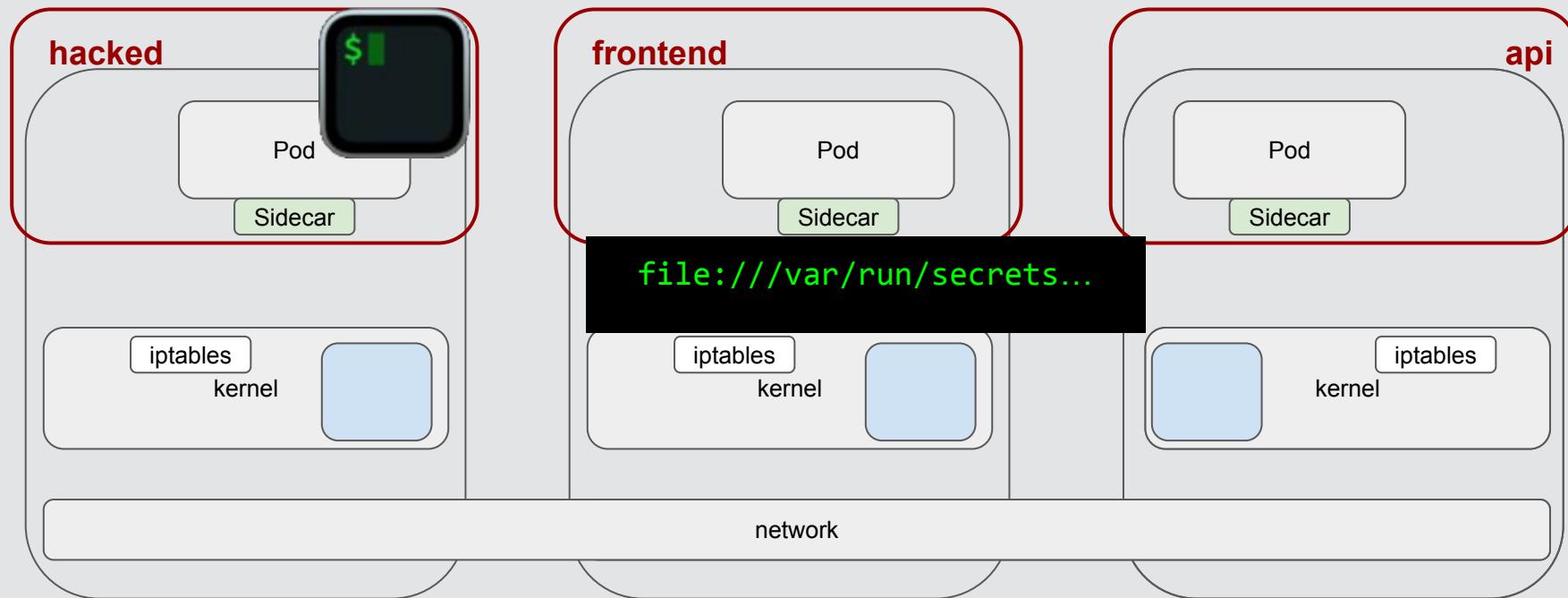
```
$ dear Service Mesh: [pods in frontend] => [pods in api] == OK!
```

Svc Mesh - contrived scenario



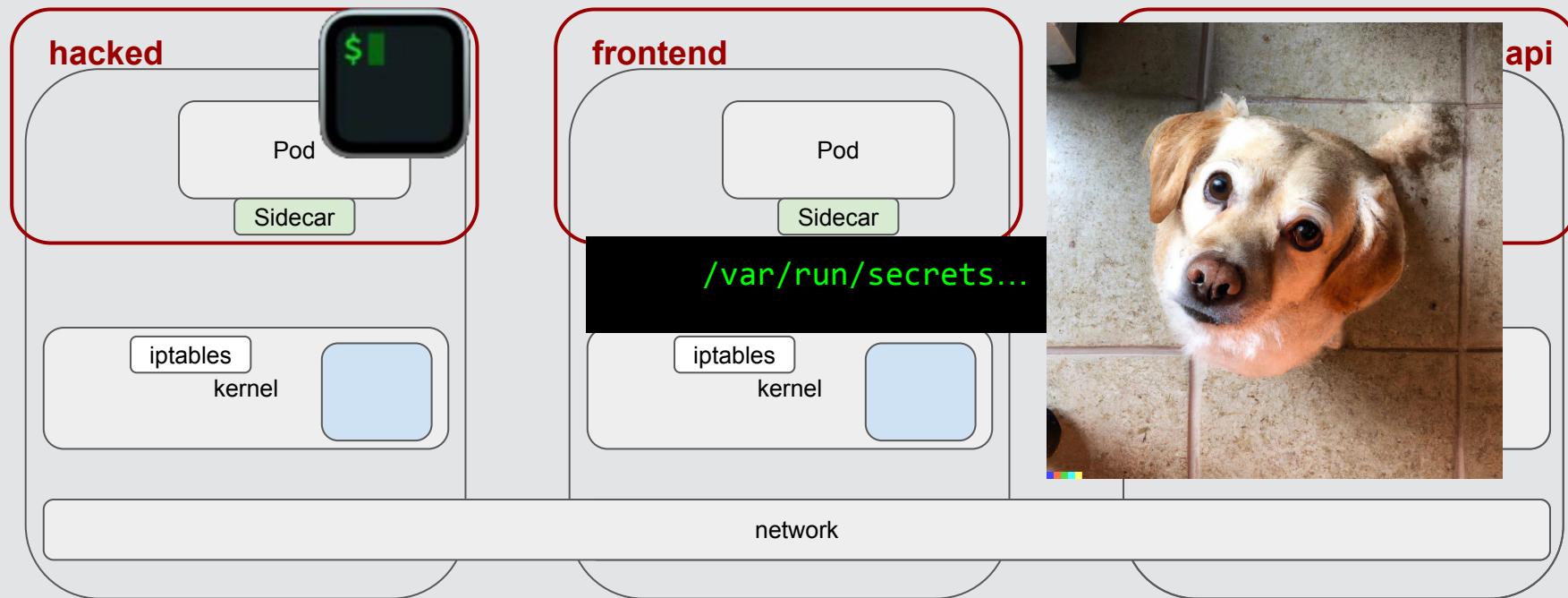
```
$ dear Service Mesh: [pods in frontend] => [pods in api] == OK!
```

Svc Mesh - contrived scenario



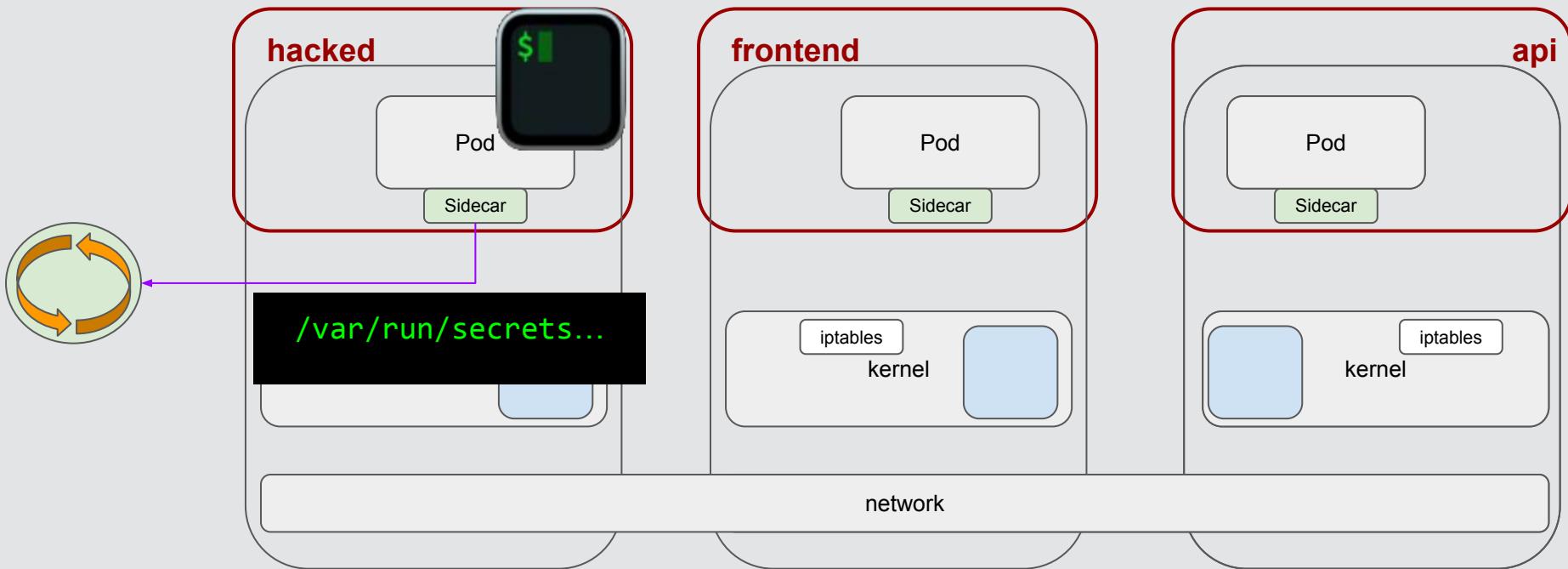
```
$ dear Service Mesh: [pods in frontend] => [pods in api] == OK!
```

Svc Mesh - contrived scenario



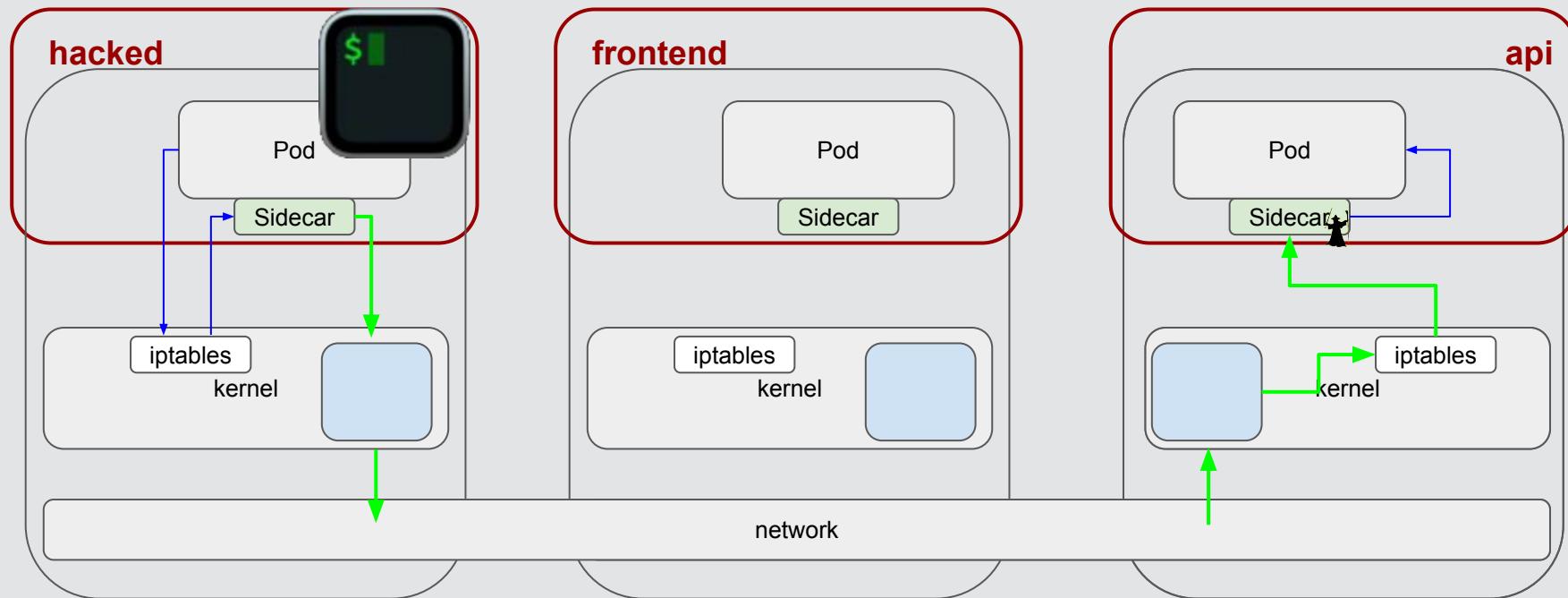
```
$ dear Service Mesh: [pods in frontend] => [pods in api] == OK!
```

Svc Mesh - contrived scenario



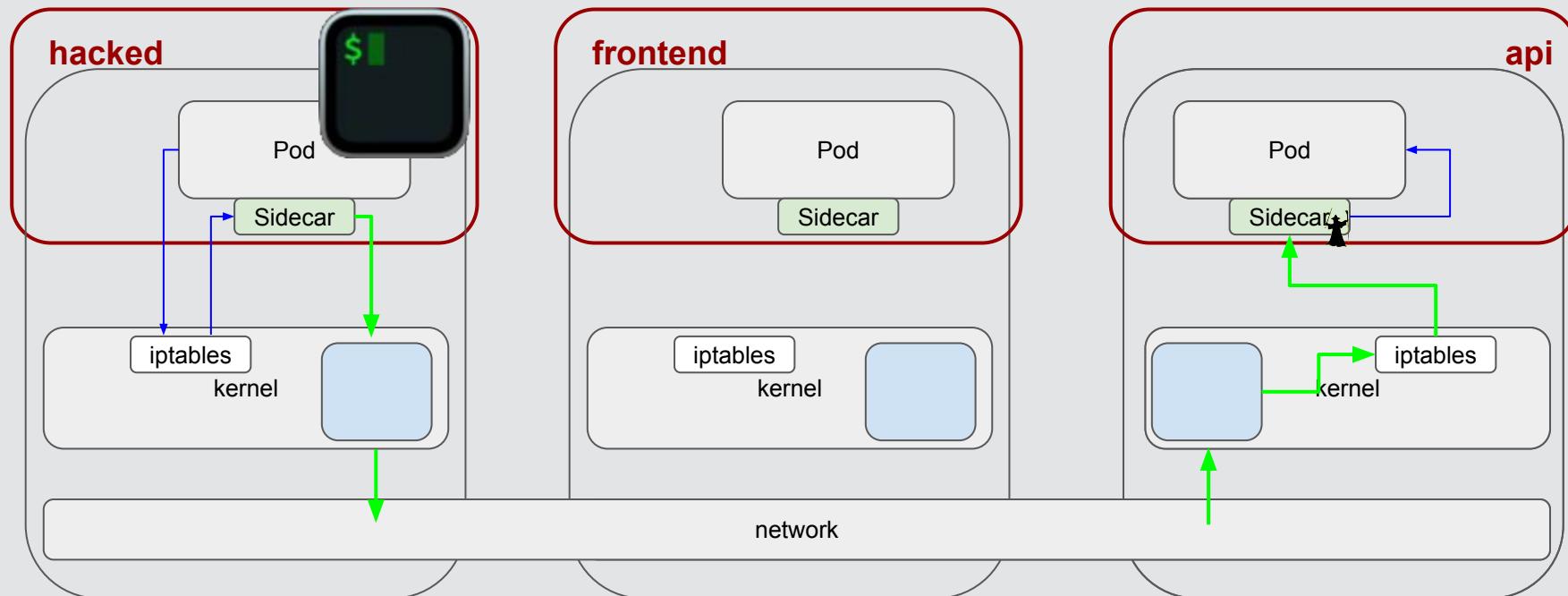
```
$ dear Service Mesh: [pods in frontend] => [pods in api] == OK!
```

Svc Mesh - contrived scenario



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

Svc Mesh - contrived scenario

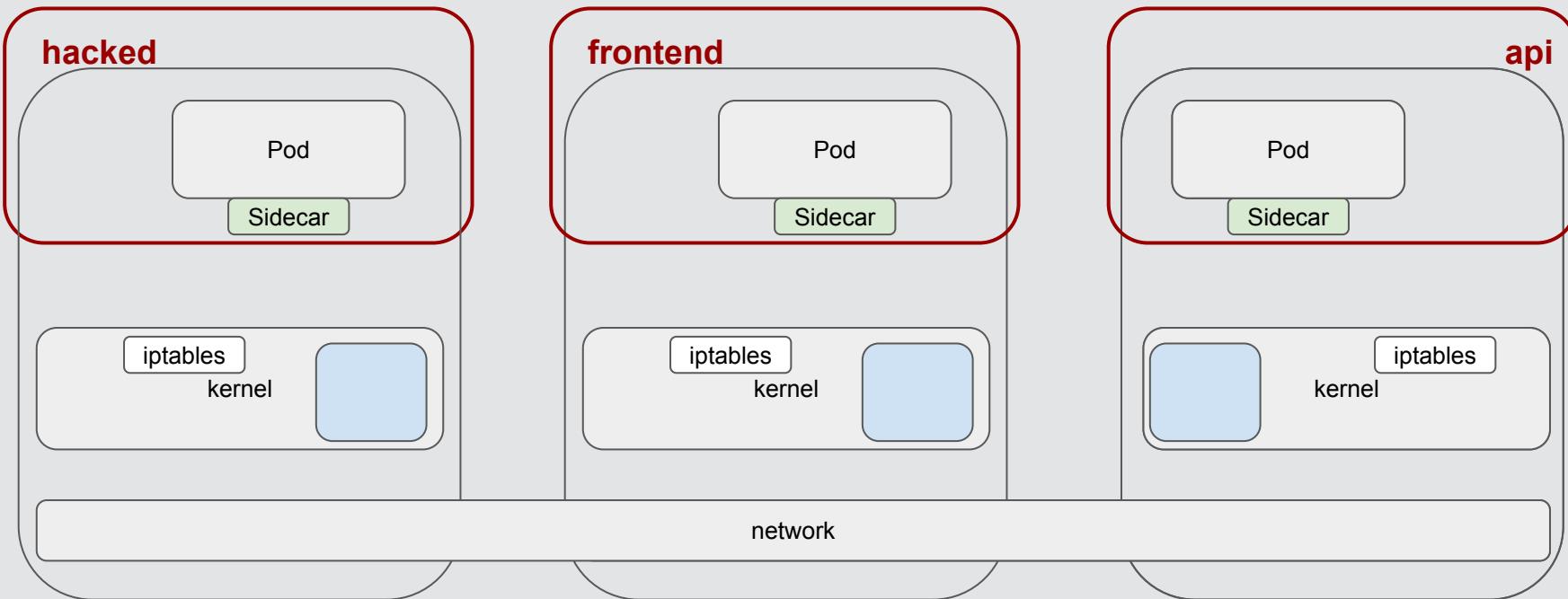


\$ dear Service Mesh: [pods in frontend] => [pods in api] == OK!

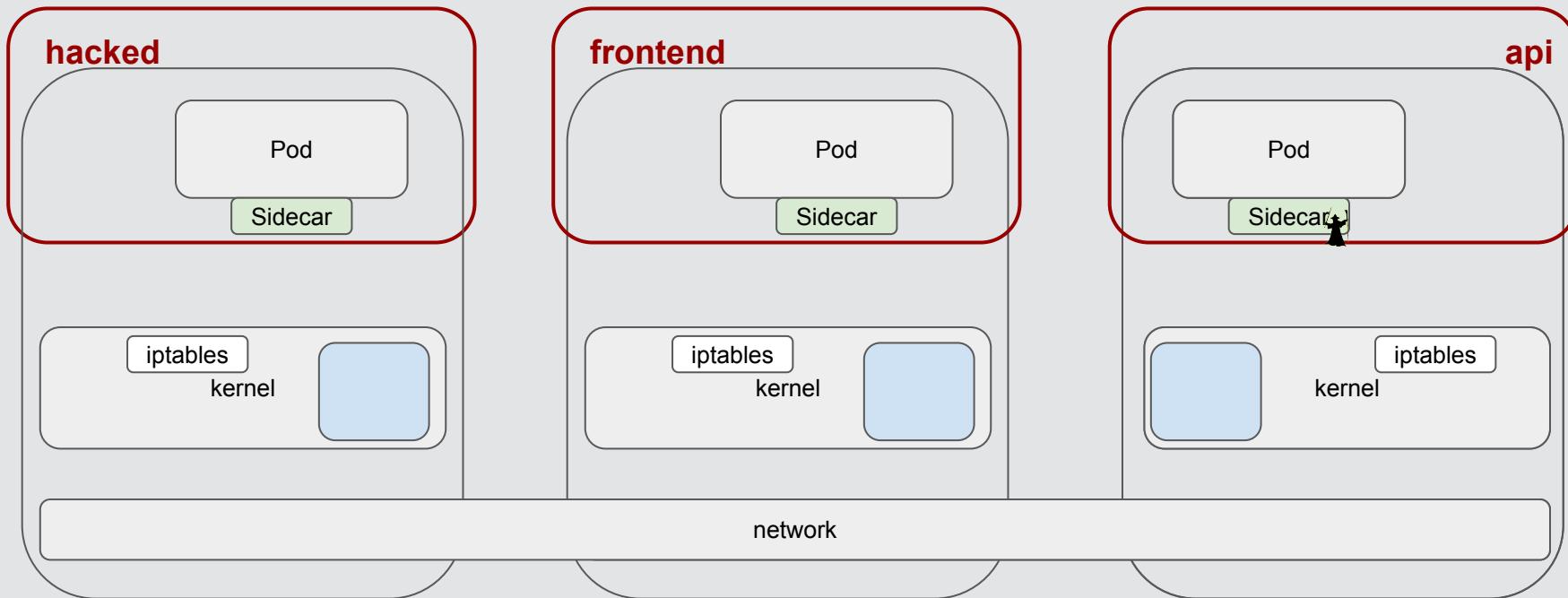
2 mitigations



#1. Right wizard tool, right job.

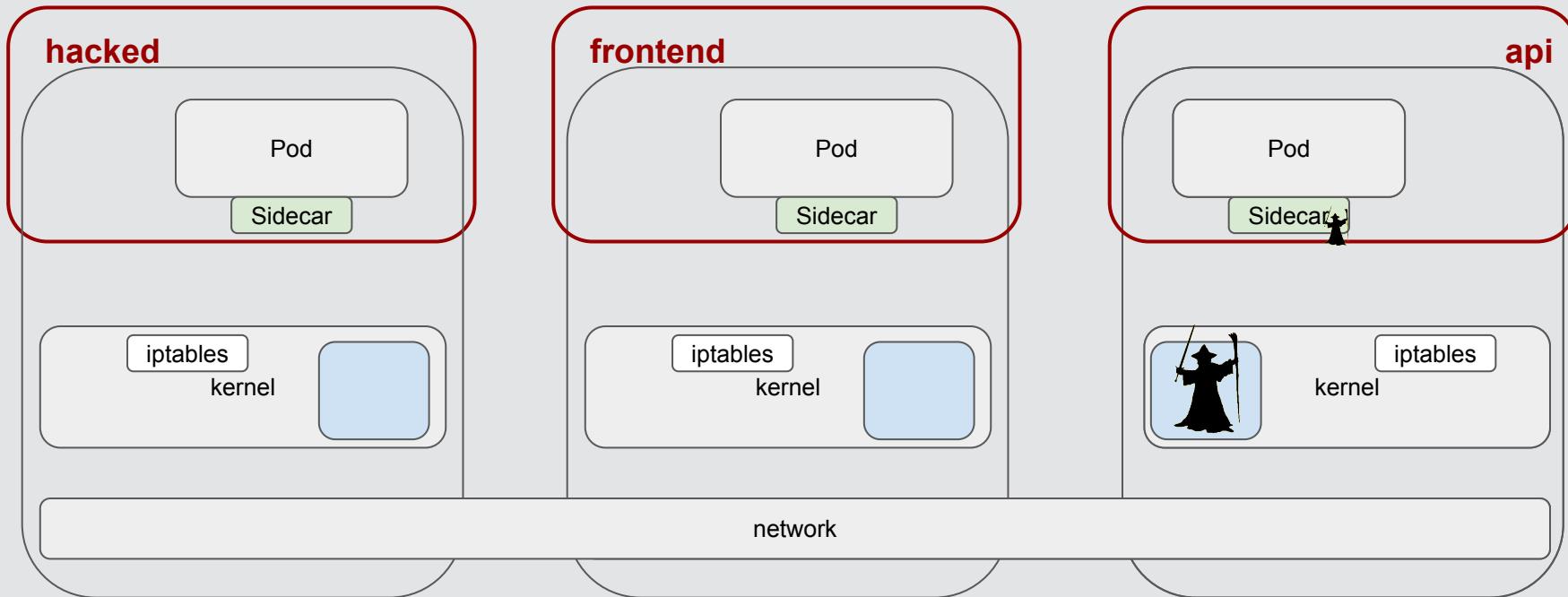


#1. Right wizard tool, right job.



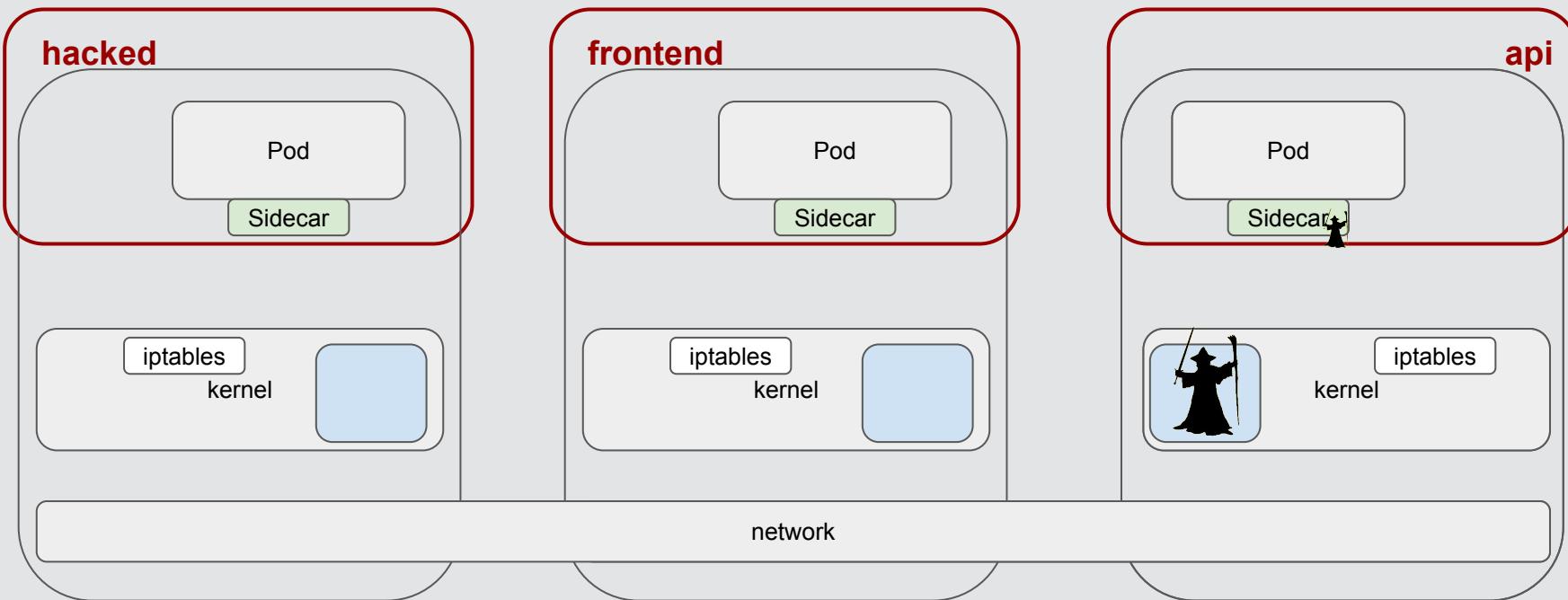
```
$ dear Service Mesh: [pods in frontend] => [pods in api] == OK!
```

#1. Right wizard tool, right job.

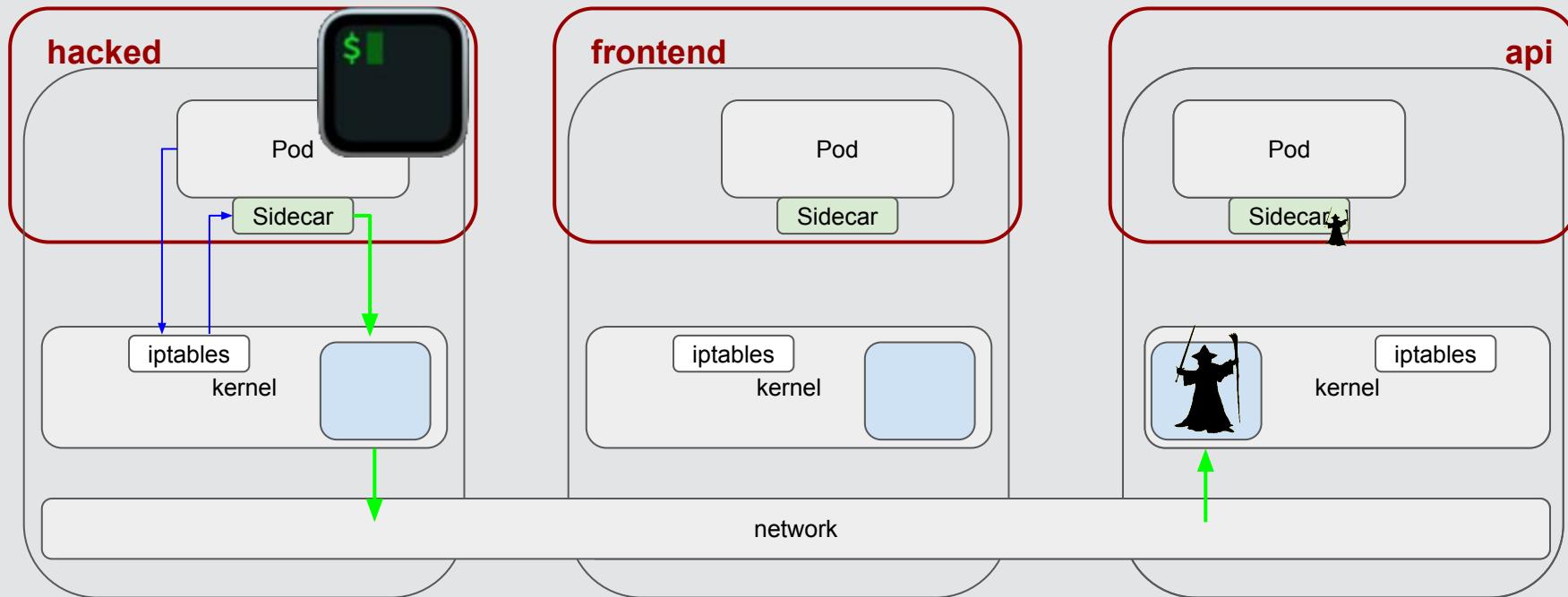


```
$ dear CNI: [pods in frontend] => [pods in api] == OK!
```

#1. Right wizard tool, right job.

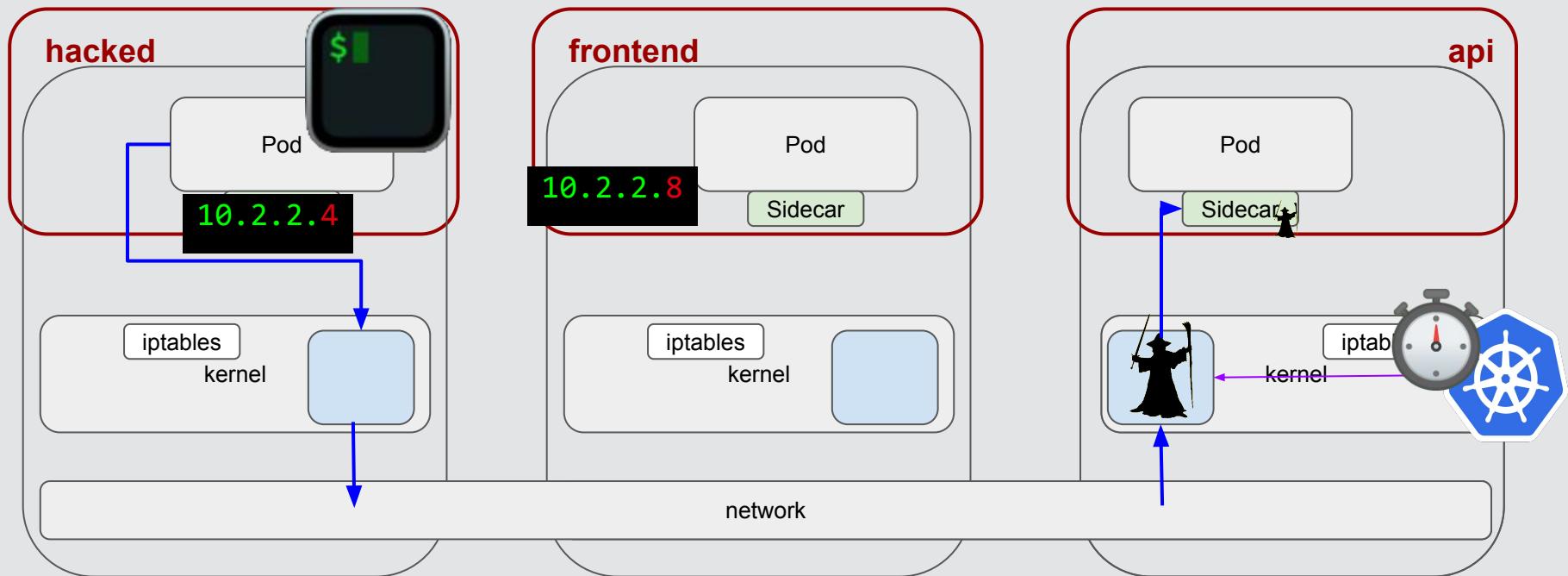


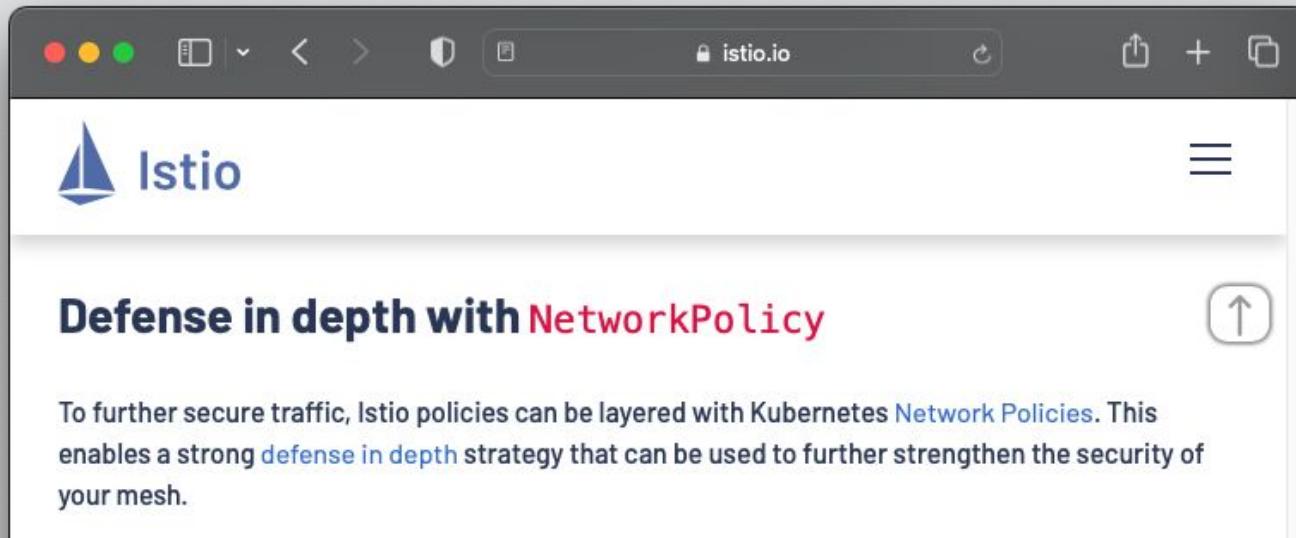
#1. Right wizard tool, right job.



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

#1. Right wizard tool, right job.





The screenshot shows a web browser window displaying the Istio website. The title bar includes standard OS X-style icons and the URL 'istio.io'. The main content area features the Istio logo (a blue sailboat icon) and the text '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. The bottom right corner of the slide has a small circular icon with an upward arrow.

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.



The landscape is changing



The landscape is changing



Istio



The landscape is changing



Istio
Ambient mesh



Ambient Mesh



Ambient Mesh



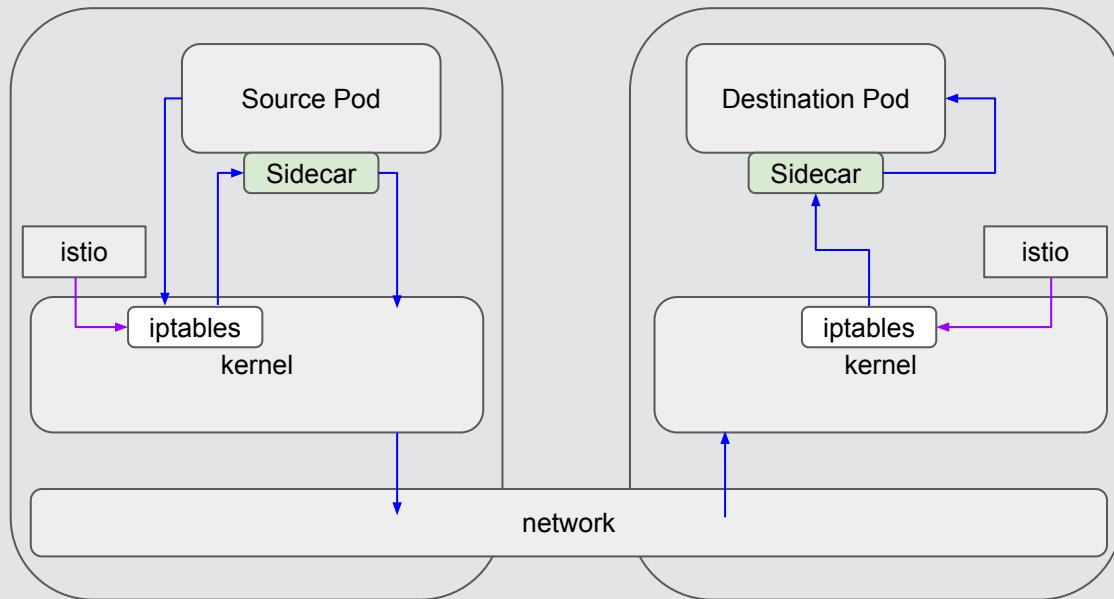
L4 Secure
Overlay

ztunnel

- mTLS,
- Svc-to-svc Authz Policies

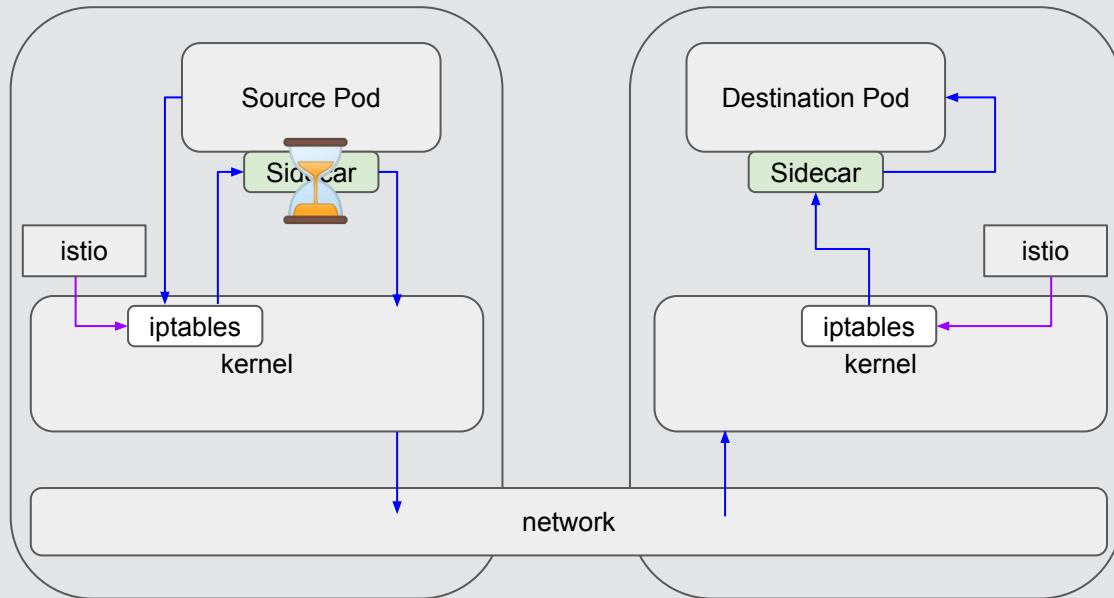


Ambient Mesh



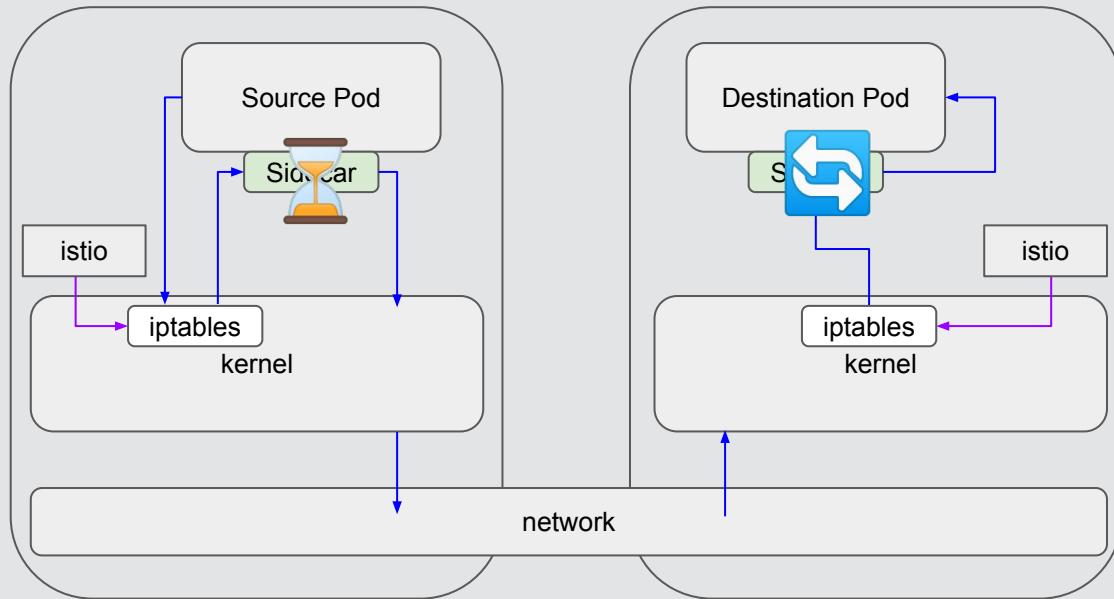
- mTLS
- control
- data

Ambient Mesh



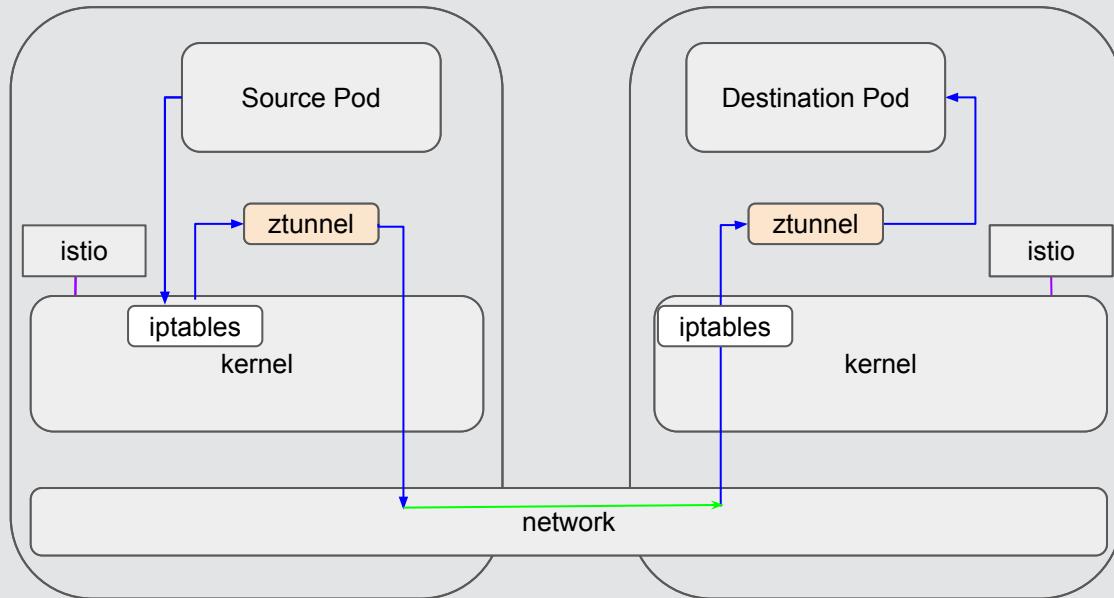
→ mTLS
→ control
→ data

Ambient Mesh

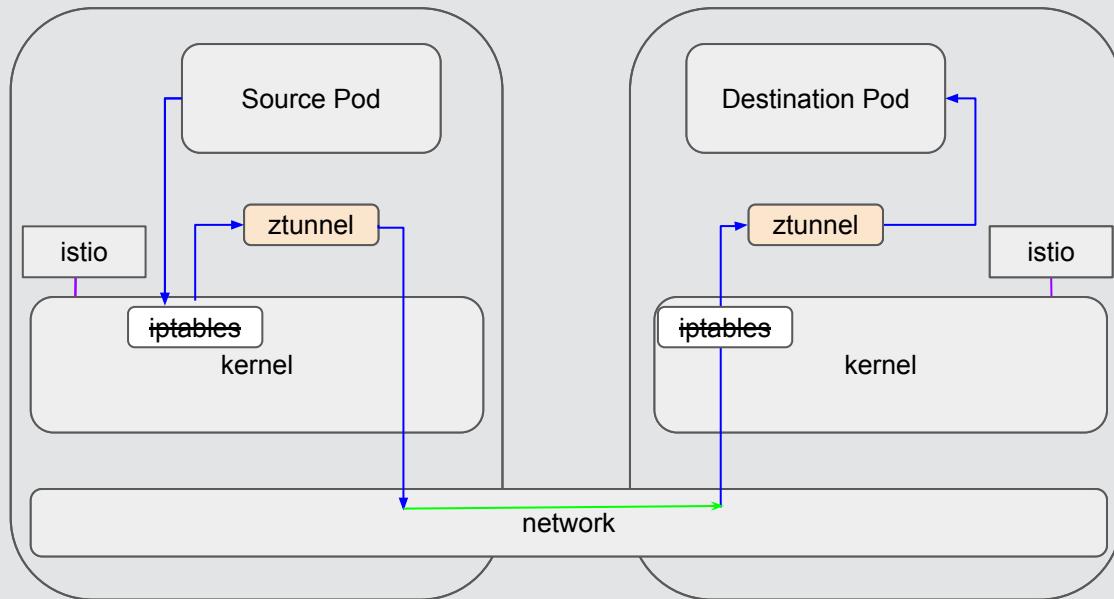


- mTLS
- control
- data

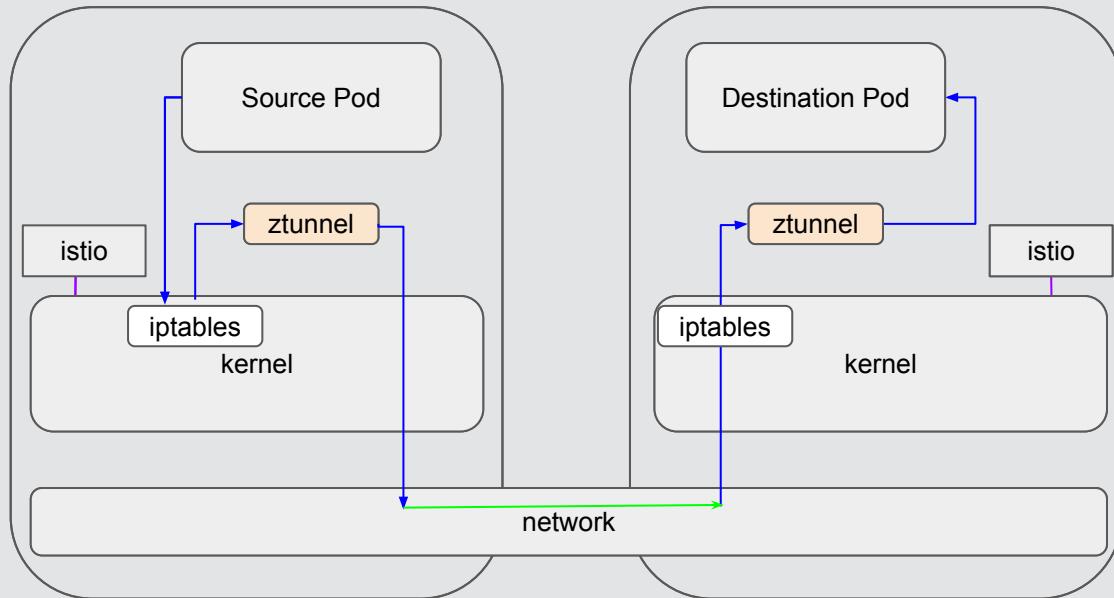
Ambient Mesh



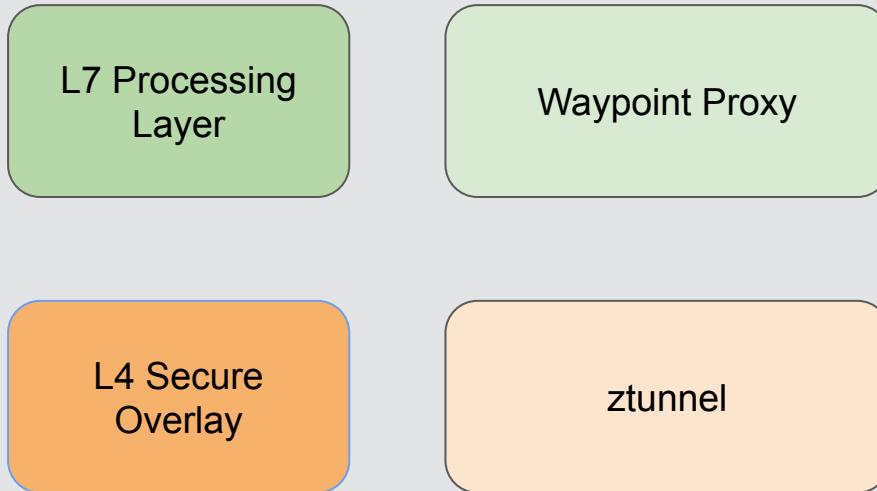
Ambient Mesh



Ambient Mesh



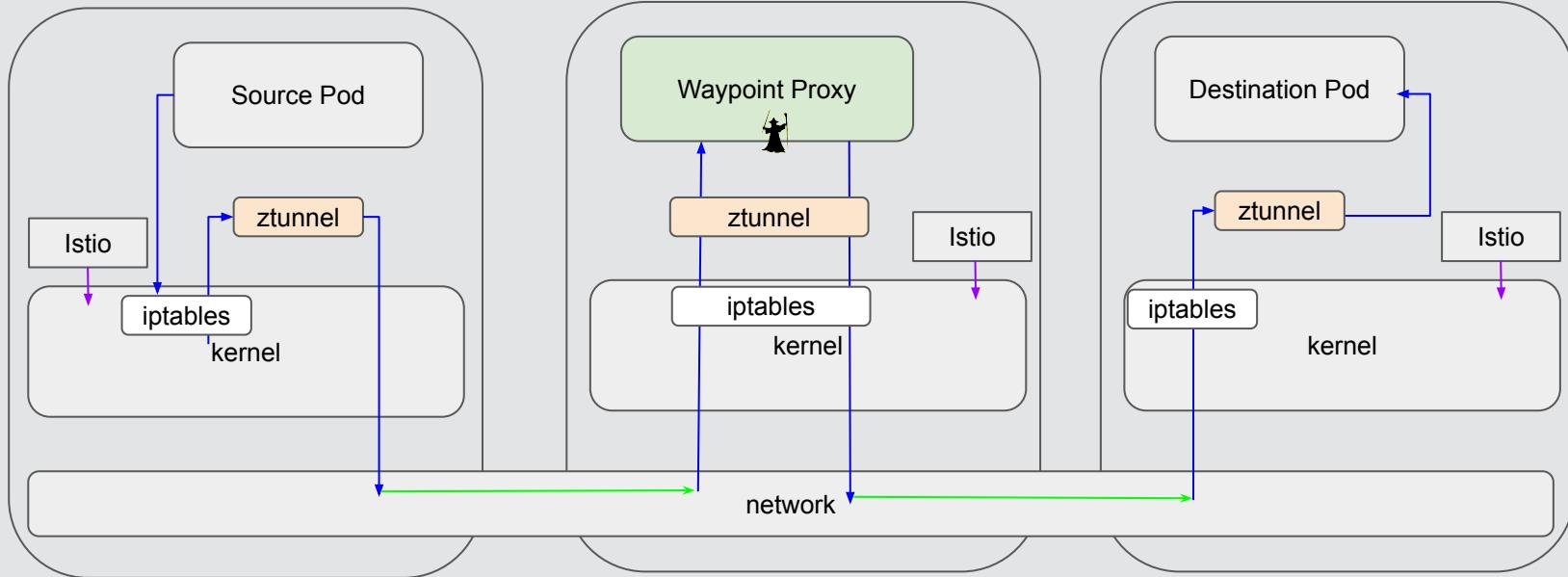
Ambient Mesh



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

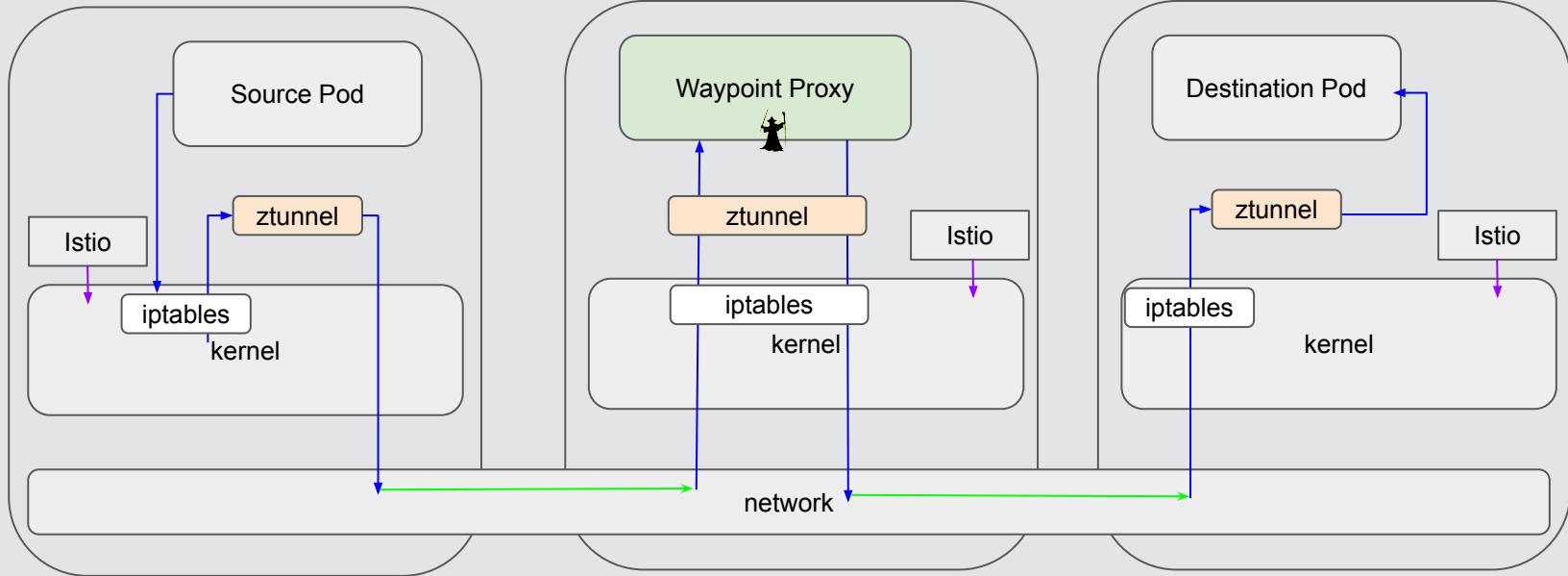


Ambient Mesh



- mTLS
- control
- data

Ambient Mesh

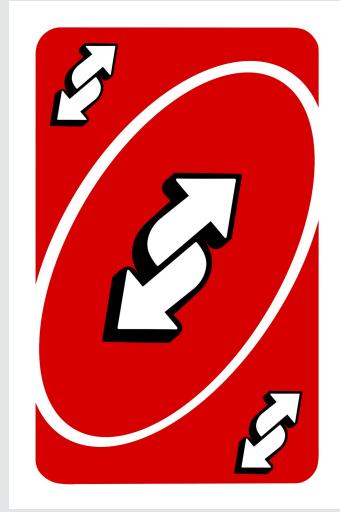


What's a Zero-Trust Tunnel? Exploring Security and Simpler Operations with Istio Ambient Mesh -
Jim Barton & Marino Wijay, Solo.io

Room 609

bit.ly/3I00k4Z

→ mTLS
→ control
→ data



The landscape is changing



Istio
Ambient mode



Cilium



The landscape is changing



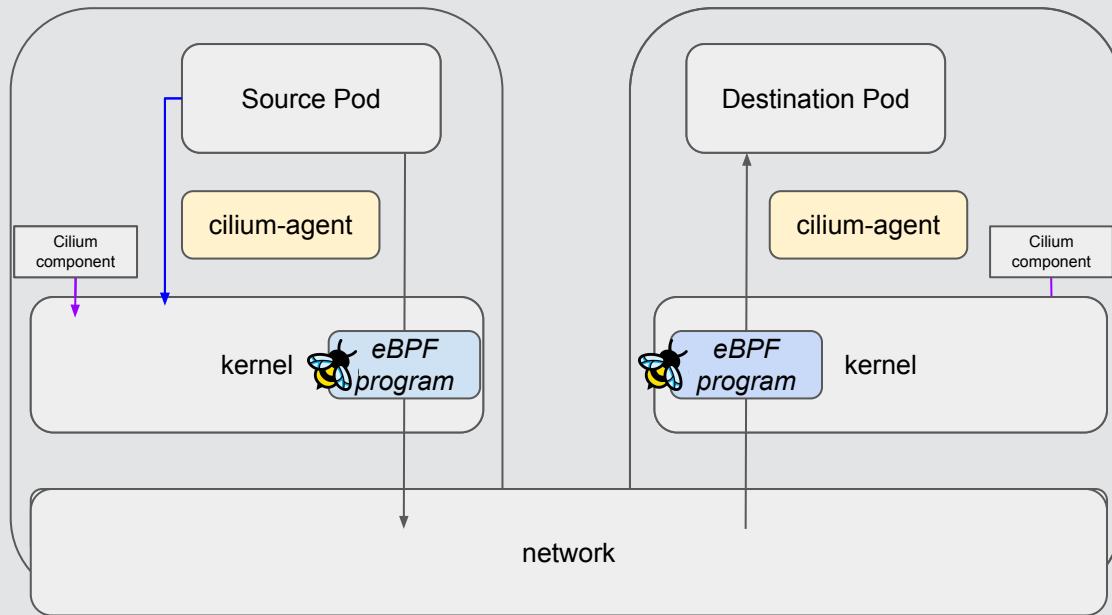
Istio
Ambient mode



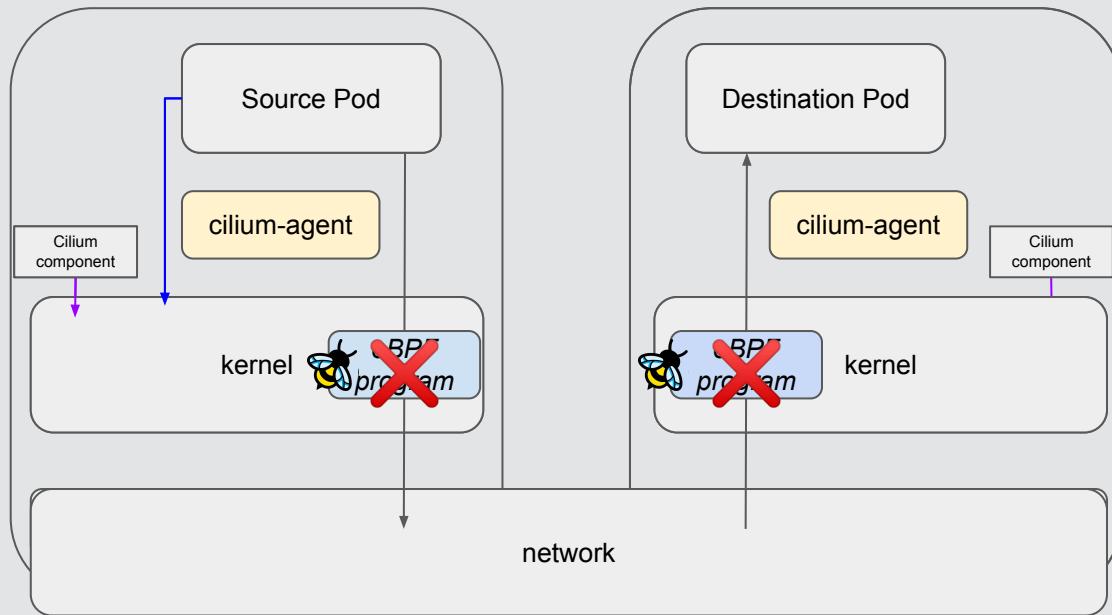
Cilium
Service Mesh



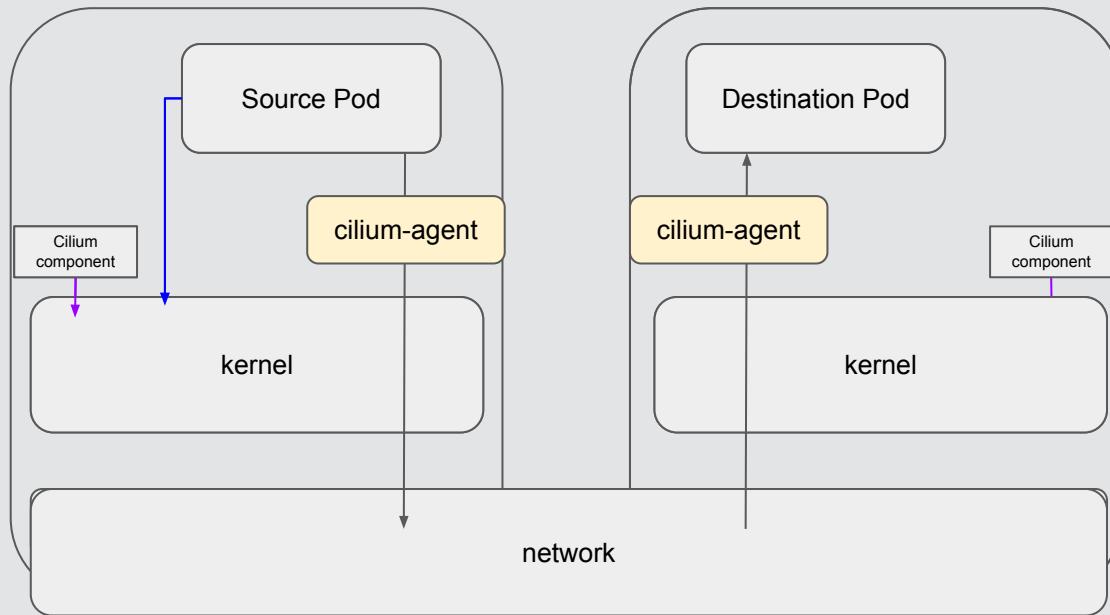
Cilium Service Mesh



Cilium Service Mesh



Cilium Service Mesh



Cilium Service Mesh



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

CFP: Mutual Authentication for Service Mesh #22215

Open 2 of 7 tasks joestringr opened this issue on Nov 16, 2022 · 0 comments

joestringr commented on Nov 16, 2022 · edited

This meta issue tracks progress on the Next-Generation Mutual Authentication with Cilium Service Mesh implementation.

Tasks:

- Discuss the CFP with the community
- Implementation
 - Datapath implementation (Draft PR)
 - SPIFFE integration
 - Automated testing

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



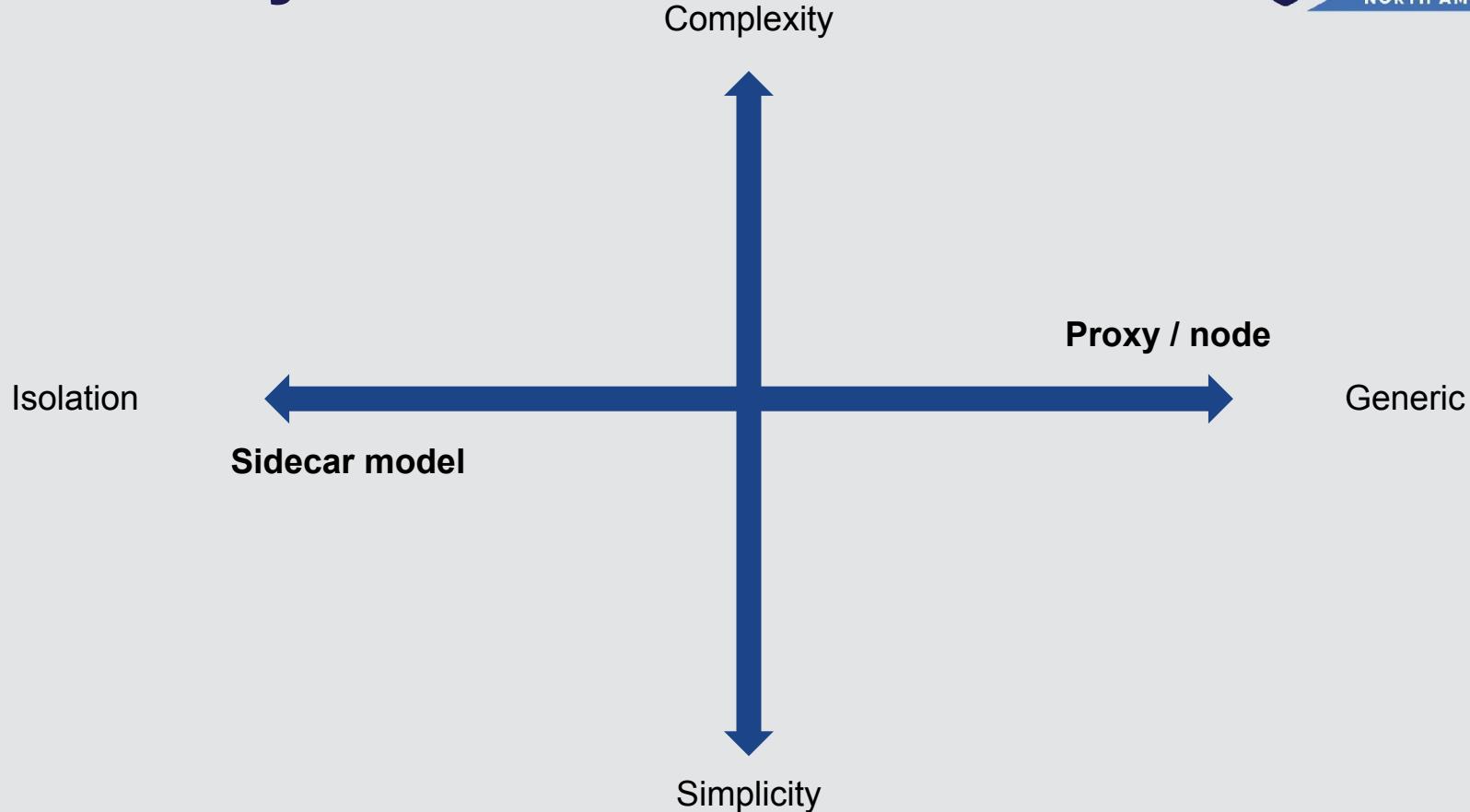
Cilium
Service Mesh



Takeaways



Takeaways



eBPF



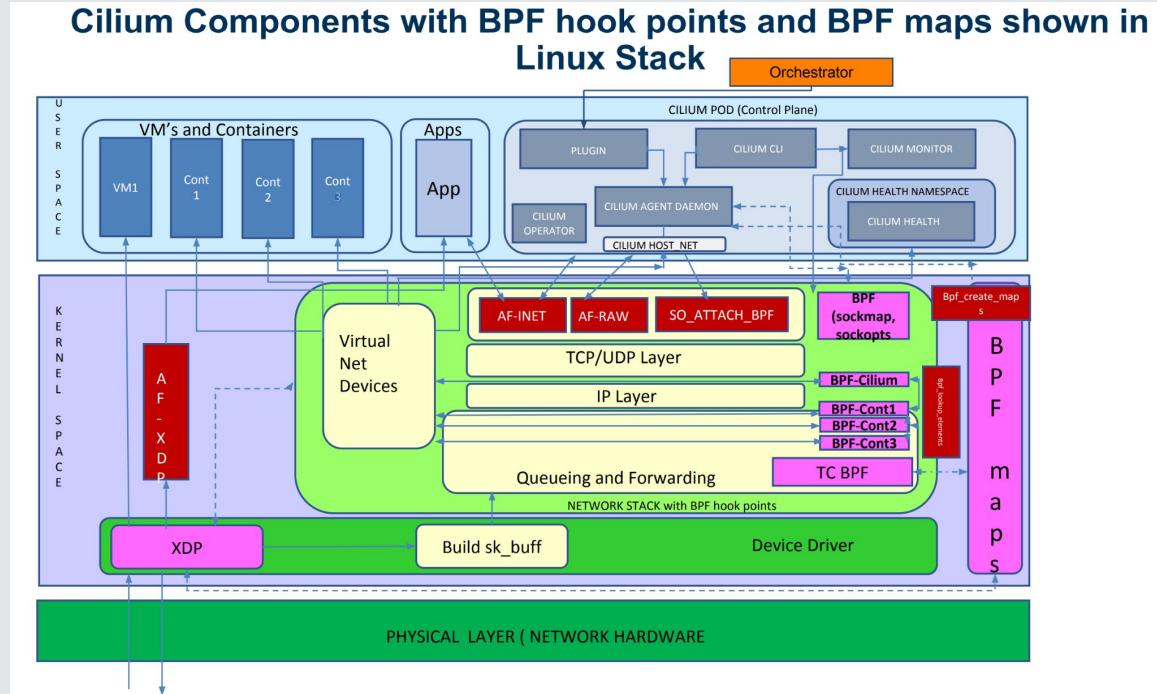


- L3 Observability
- L3 Routing
- L3 Network policy

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



- L3 Observability
- L3 Routing
- L3 Network policy



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



twitter.com

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

Search Twitter

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



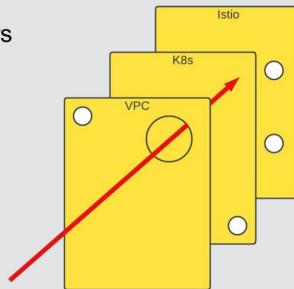
Takeaways



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



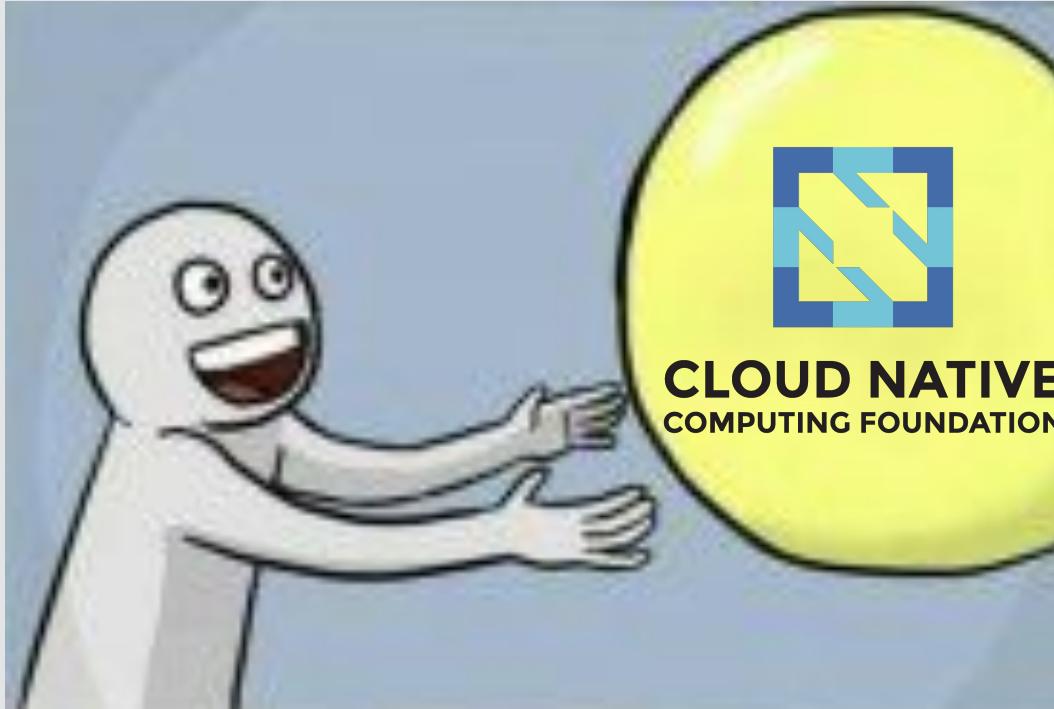
Network Security at Scale: L3 Through L7 at Splunk - Mitch Connors, Aviatrix & Bernard Van De Walle, Splunk

Room 612

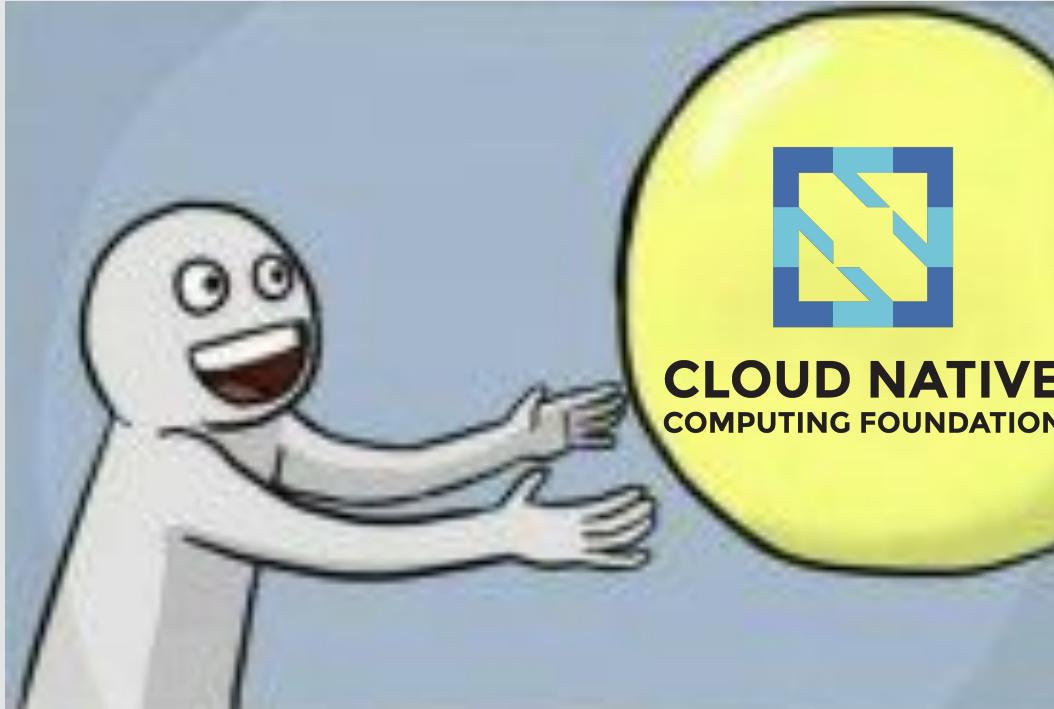
Call to action



Call to action

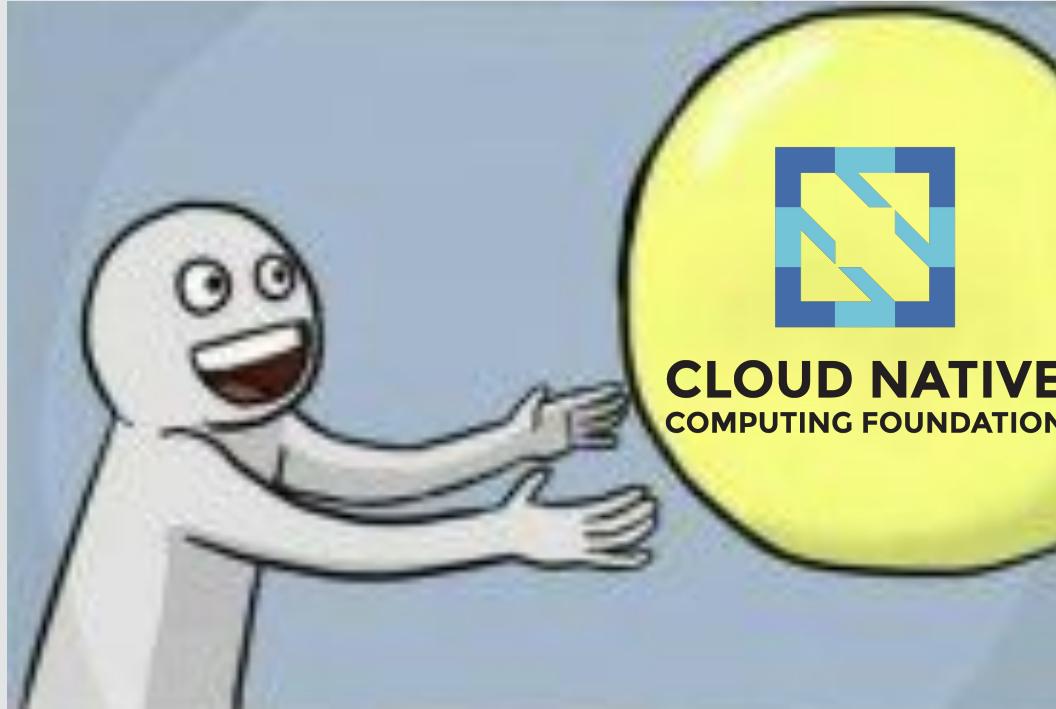


Call to action



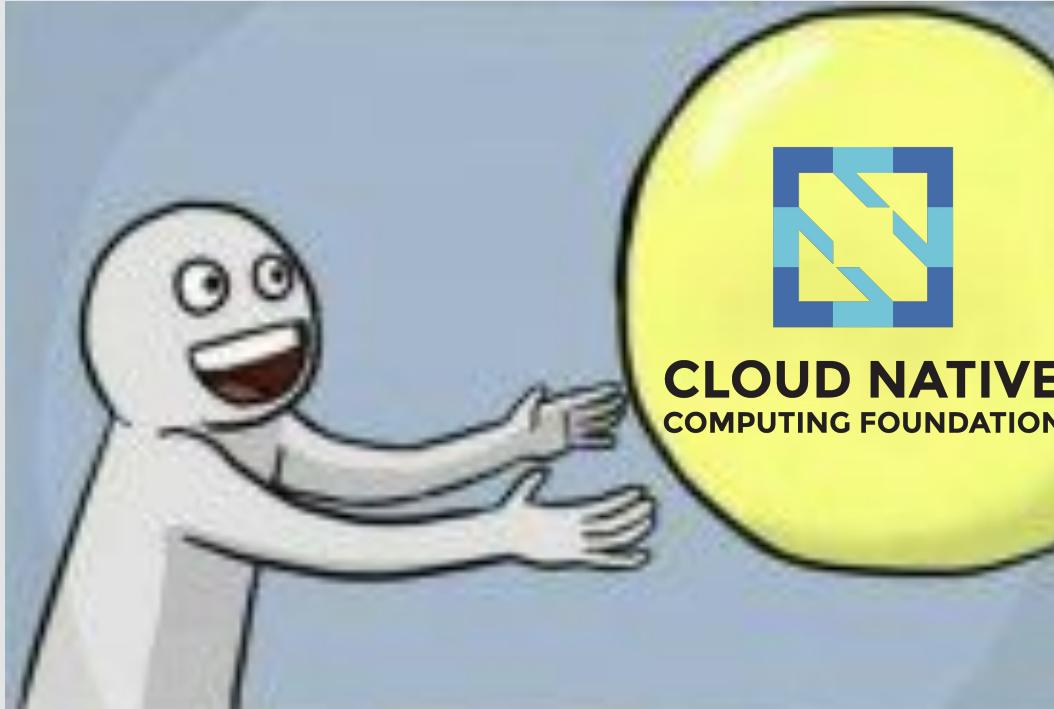
<https://istio.io/latest/blog/2022/get-started-ambient/>

Call to action

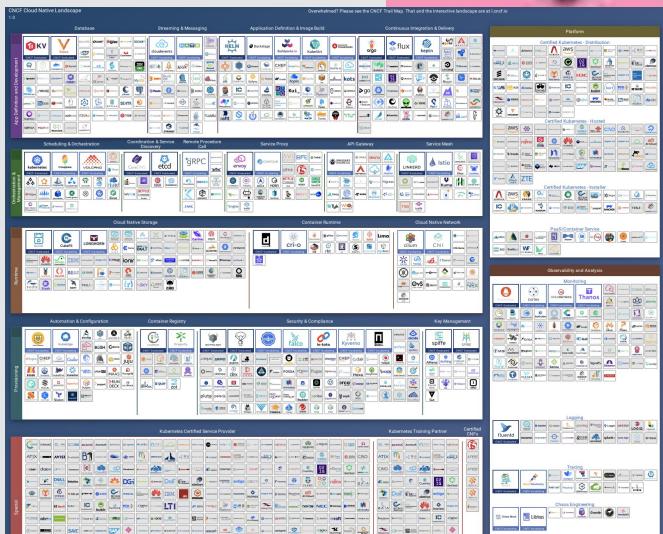
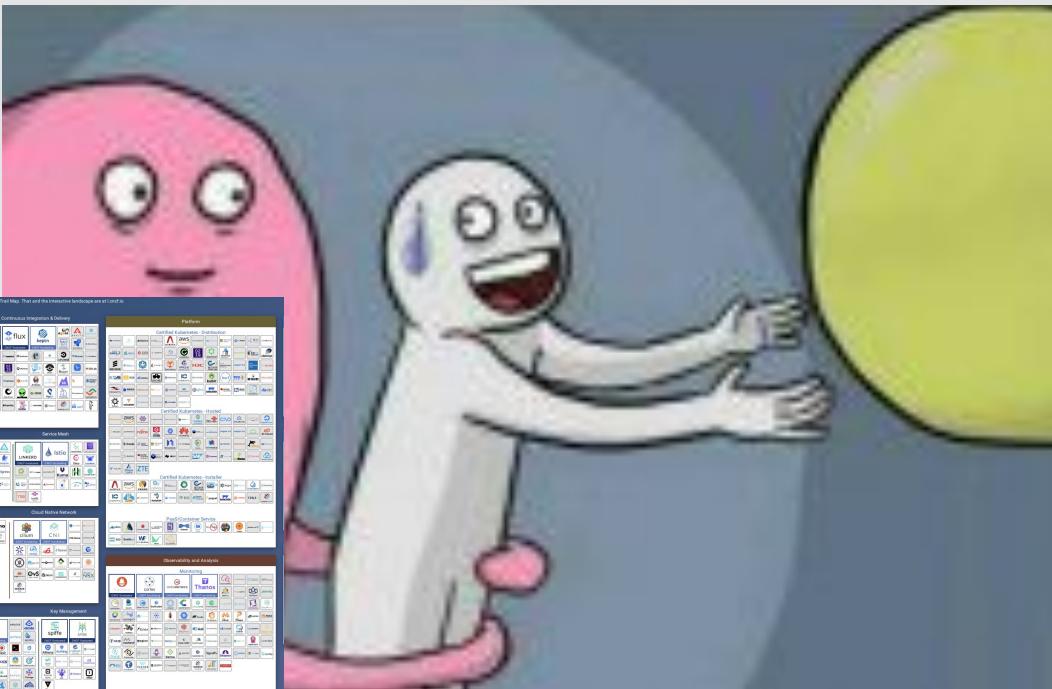


<https://github.com/cilium/cilium/issues/22215>

Call to action



Call to action





cilium



The screenshot shows a web browser window with the Isovalent logo at the top left. The main content area features the Cilium logo and the text "Cilium Service Mesh – Everything You Need to Know". Below this, the date "Jul 20, 2022" and the word "Cilium" are visible. At the bottom, there is a footer with the Cilium logo and the text "Service Mesh".

Cilium Service Mesh – Everything You
Need to Know

Jul 20, 2022 Cilium

cilium
Service Mesh

The screenshot shows a web browser window with the Istio logo at the top left. The main content area features the text "Introducing Ambient Mesh" and "A new dataplane mode for Istio without sidecars.". Below this, the date "Sep 7, 2022" and a list of contributors are visible. The background of the slide features a dark forest silhouette.

Istio

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 - Google



Rob Salmond - SuperOrbital



Thanks for Listening!

Scan or visit
sched.co/1FV12
to get slides and
share feedback.

Demo? Questions?

