Network Policy Controller in Weave Net

Blocking unwanted network traffic in Kubernetes

Bryan Boreham

@bboreham

weaveworks

Who knows...

- Kubernetes
- Docker
- Linux
- iptables

Ancient wisdom

For survival, your group needs:

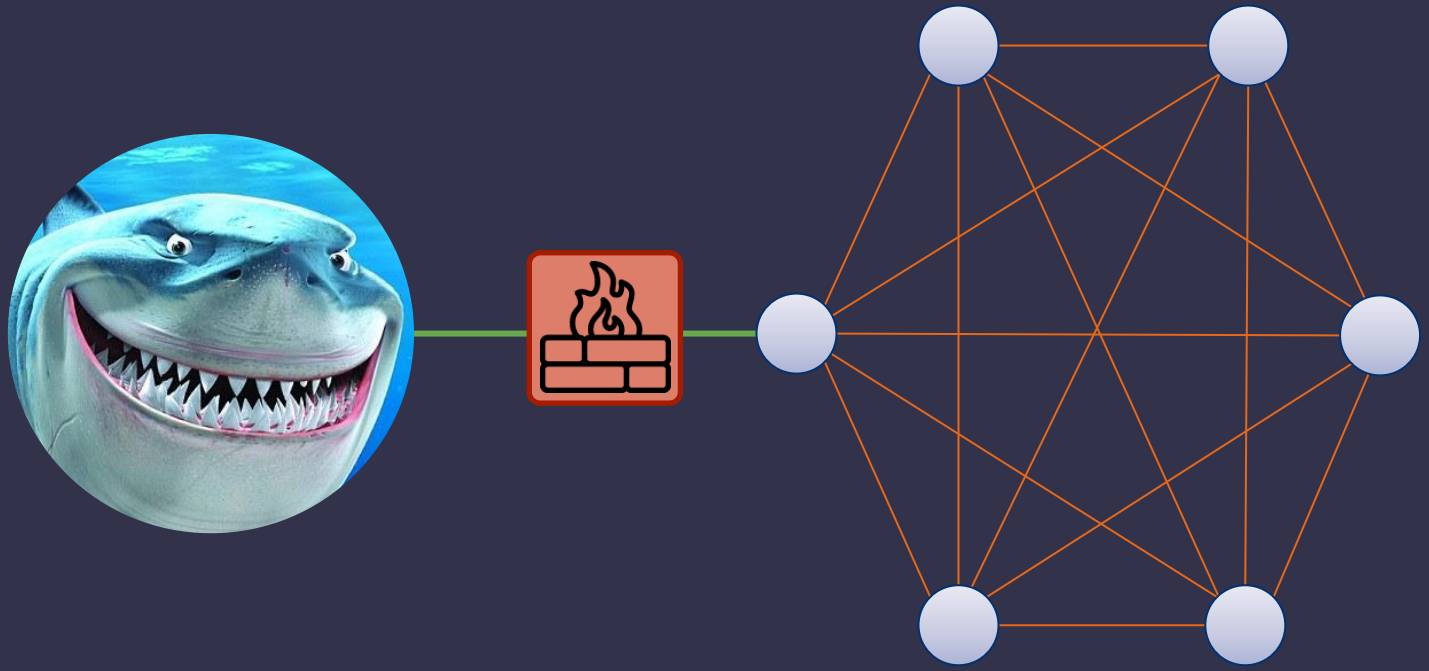
- Leadership
- Hunting skills
- Medical skills
- Someone who knows iptables

What I am going to talk about

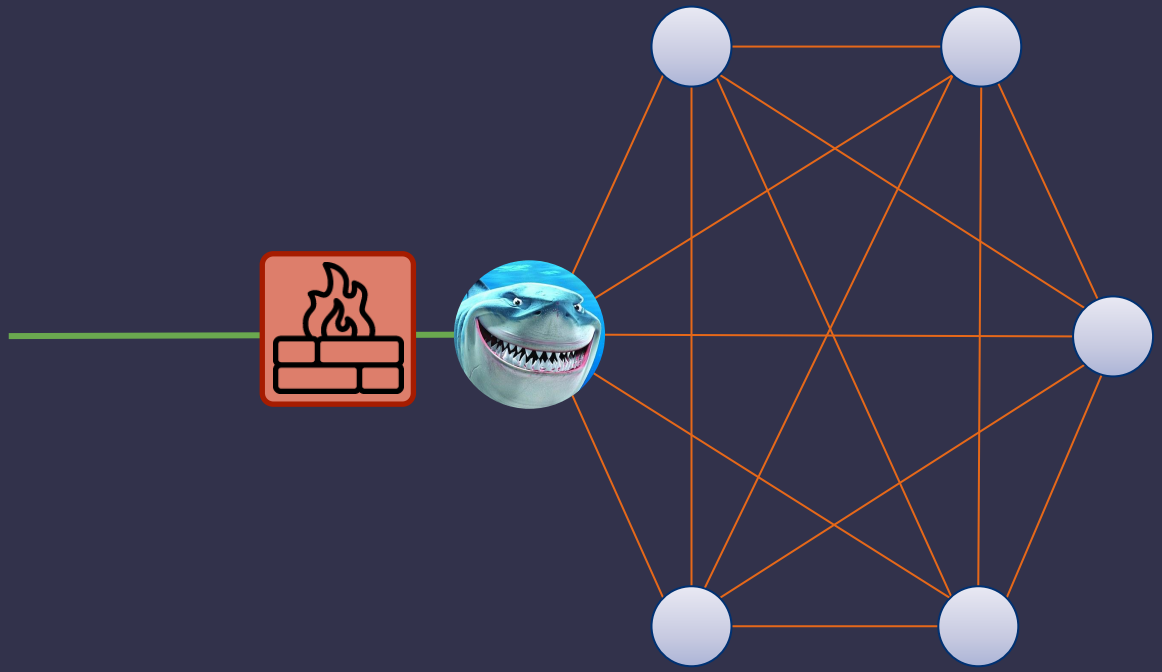
- Weave Network Policy Controller
  - Blocking unwanted network traffic in Kubernetes


Threat
Model

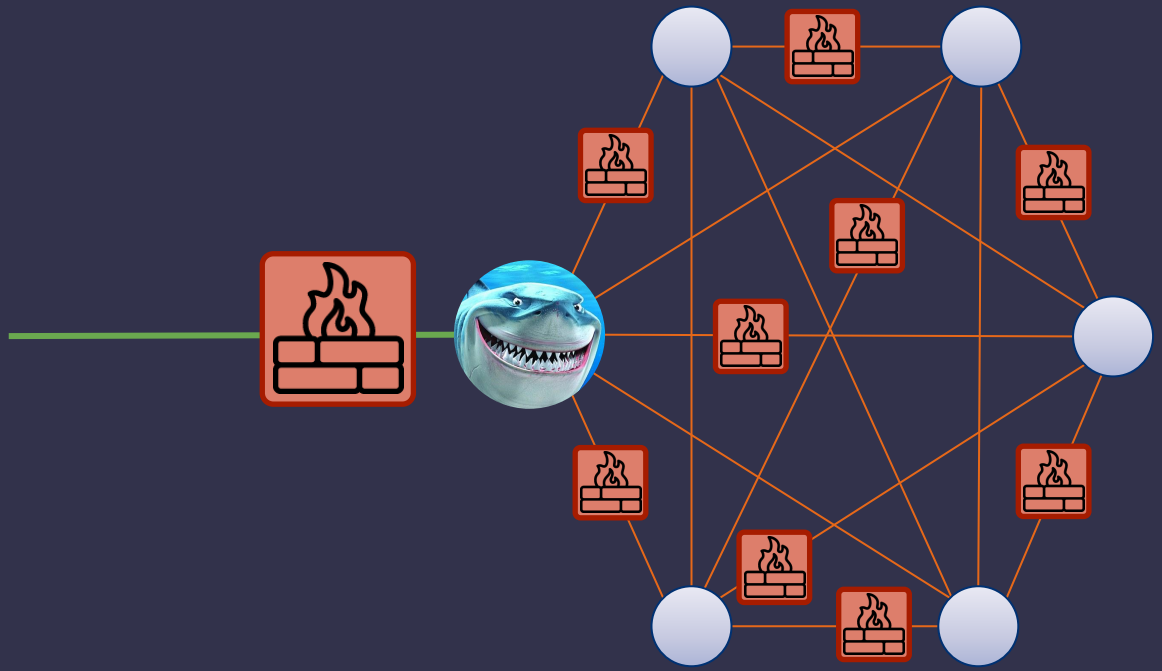
Traditional defence



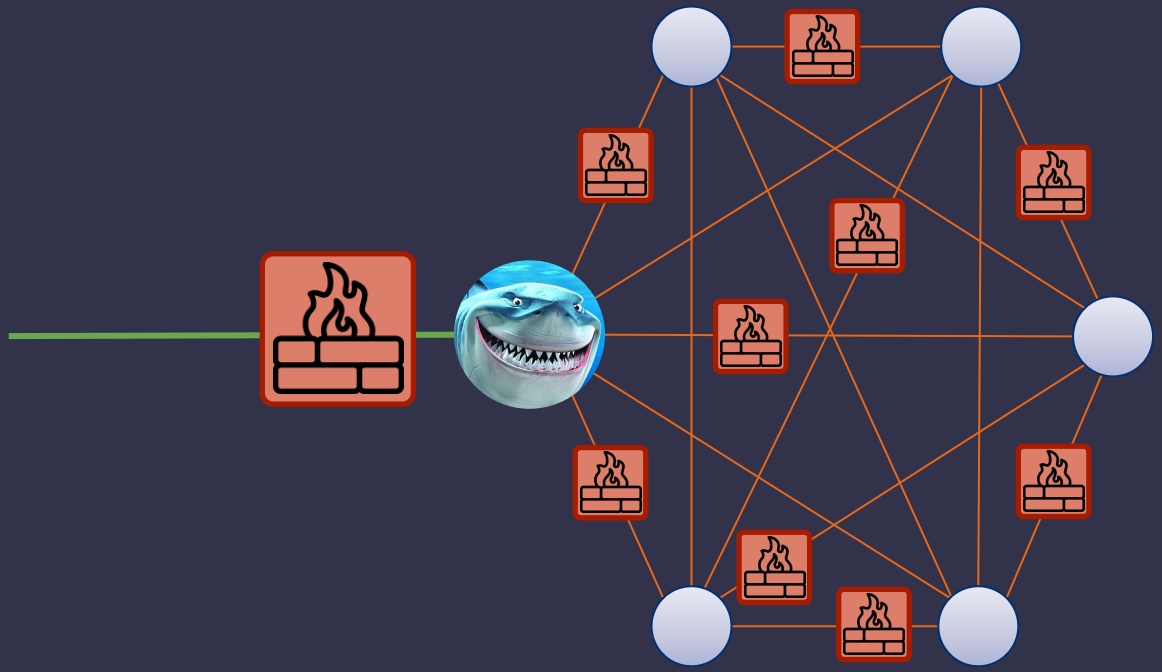
Problem



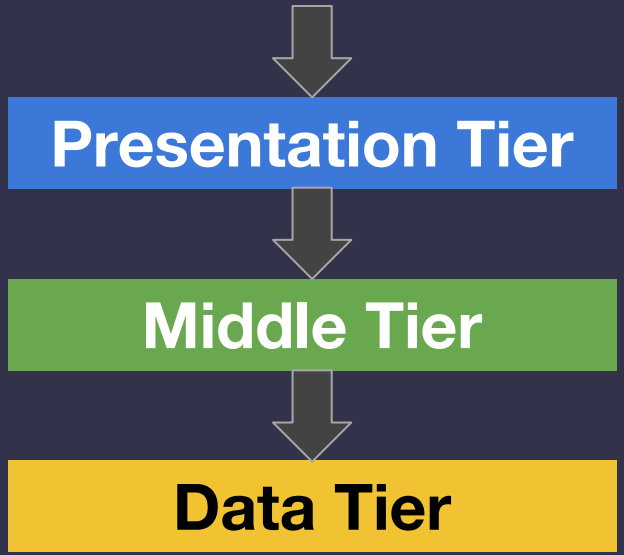
Solution



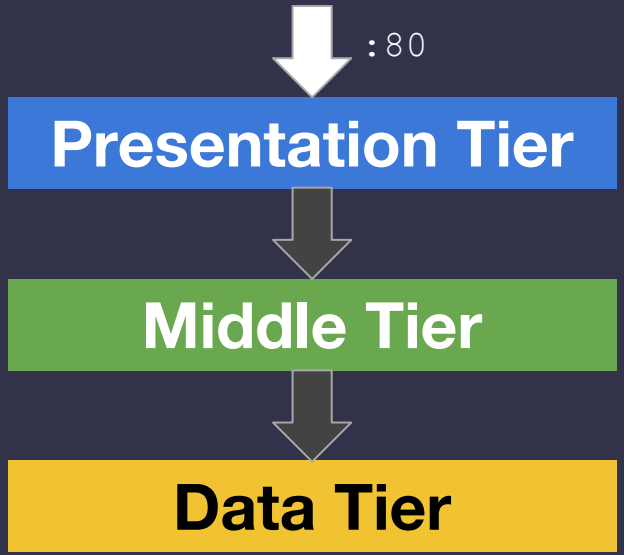
Now make it dynamic



Example

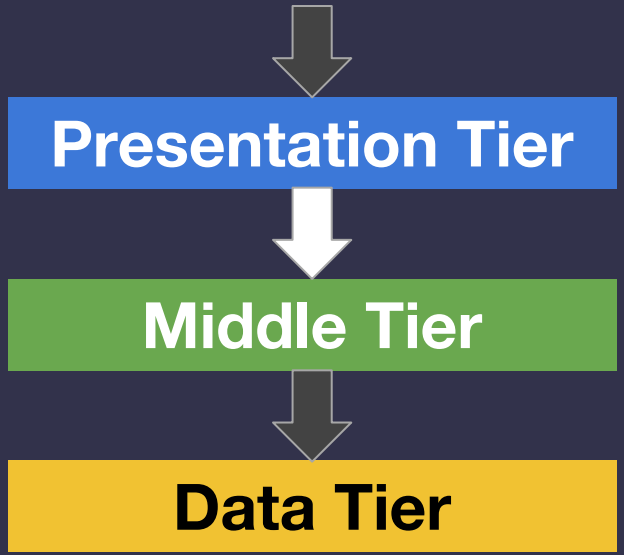


Kubernetes NetworkPolicy



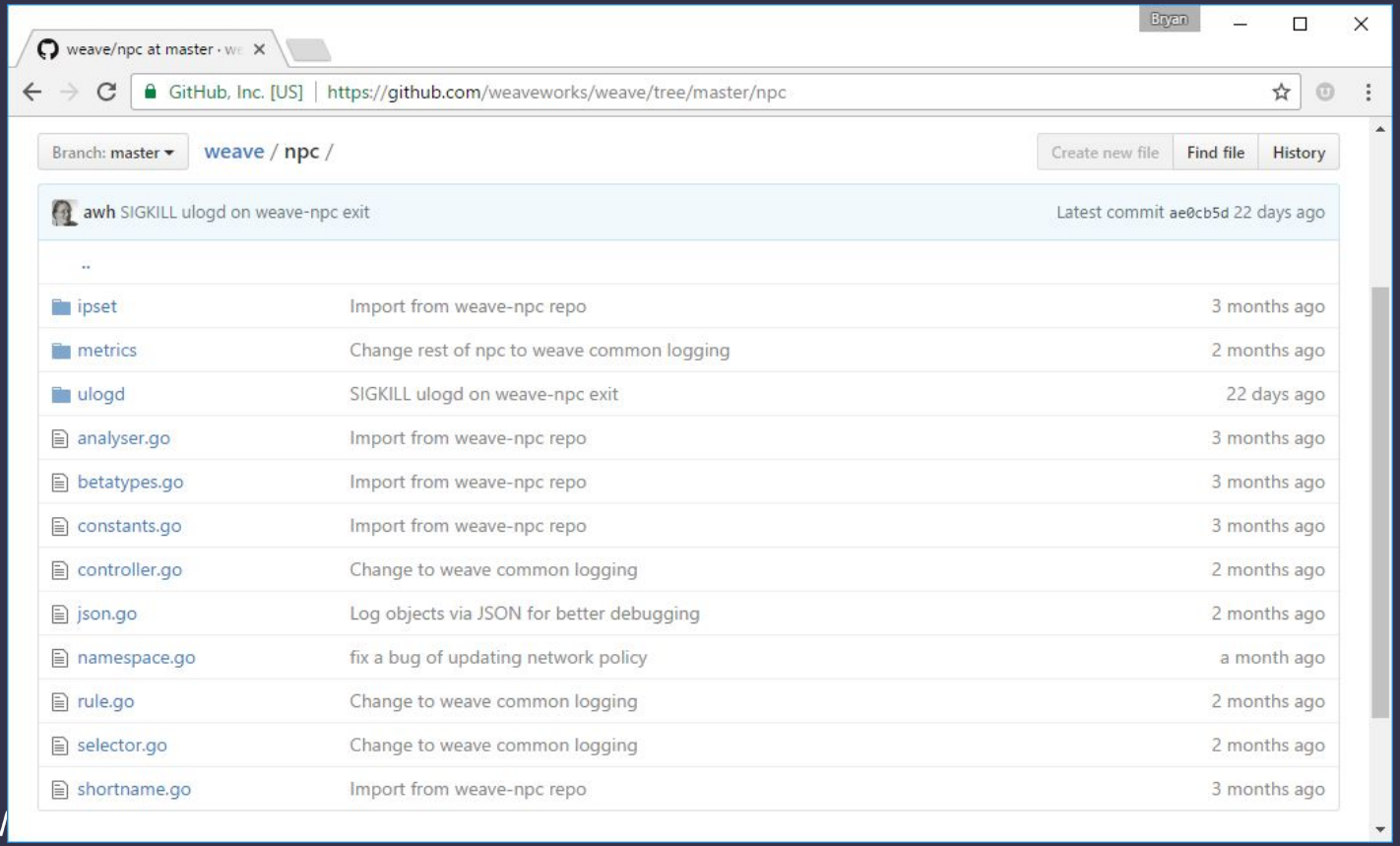

```
kind: NetworkPolicy
metadata:
  name: presentation-policy
spec:
  podSelector:
    tier: presentation
  ingress:
  - ports:
    - protocol: tcp
      port: 80
```

Kubernetes NetworkPolicy

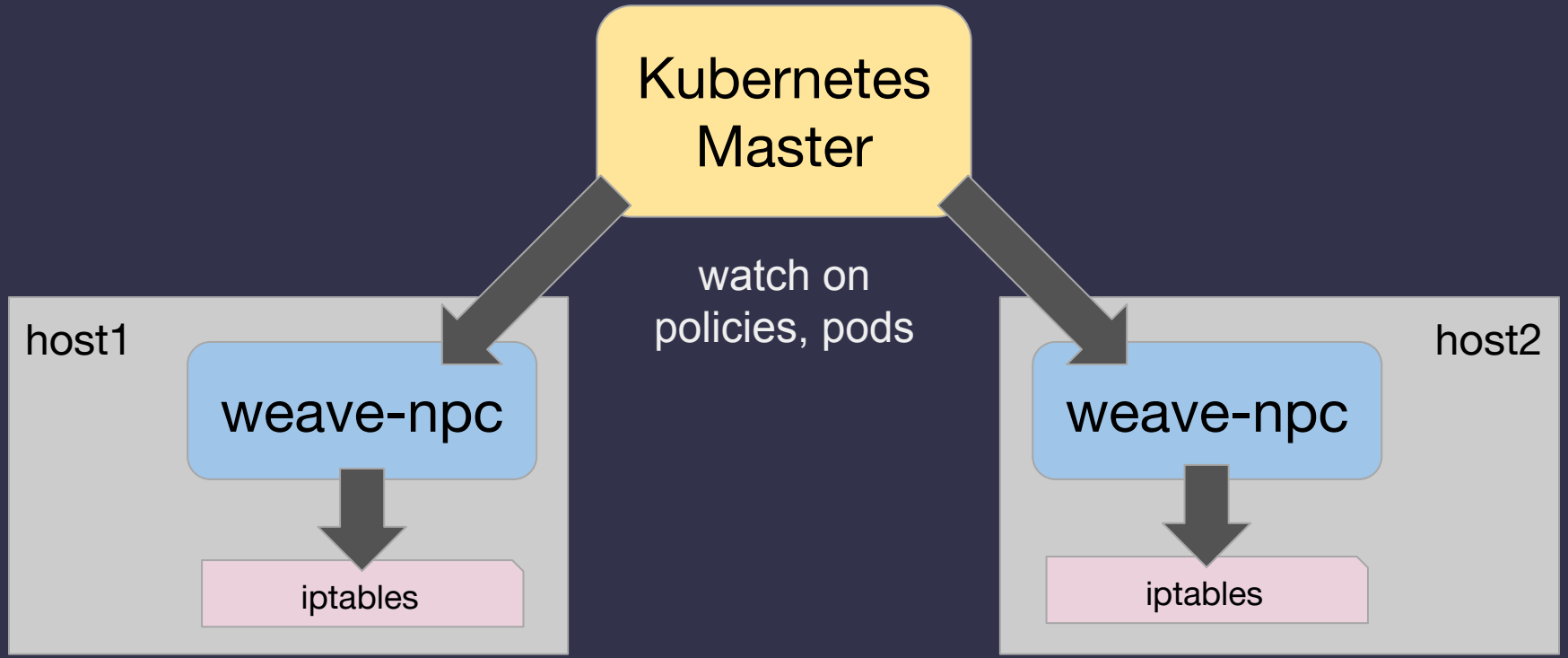



```
kind: NetworkPolicy
metadata:
  name: middle-tier-policy
spec:
  podSelector:
    tier: middle
  ingress:
  - from:
    - podSelector:
        matchLabels:
          tier: presentation
```

So how do we implement this?



Controller


Kubernetes Master
watch on policies, pods
host1
weave-npc
iptables
host2
weave-npc
iptables

Top-level iptables rules

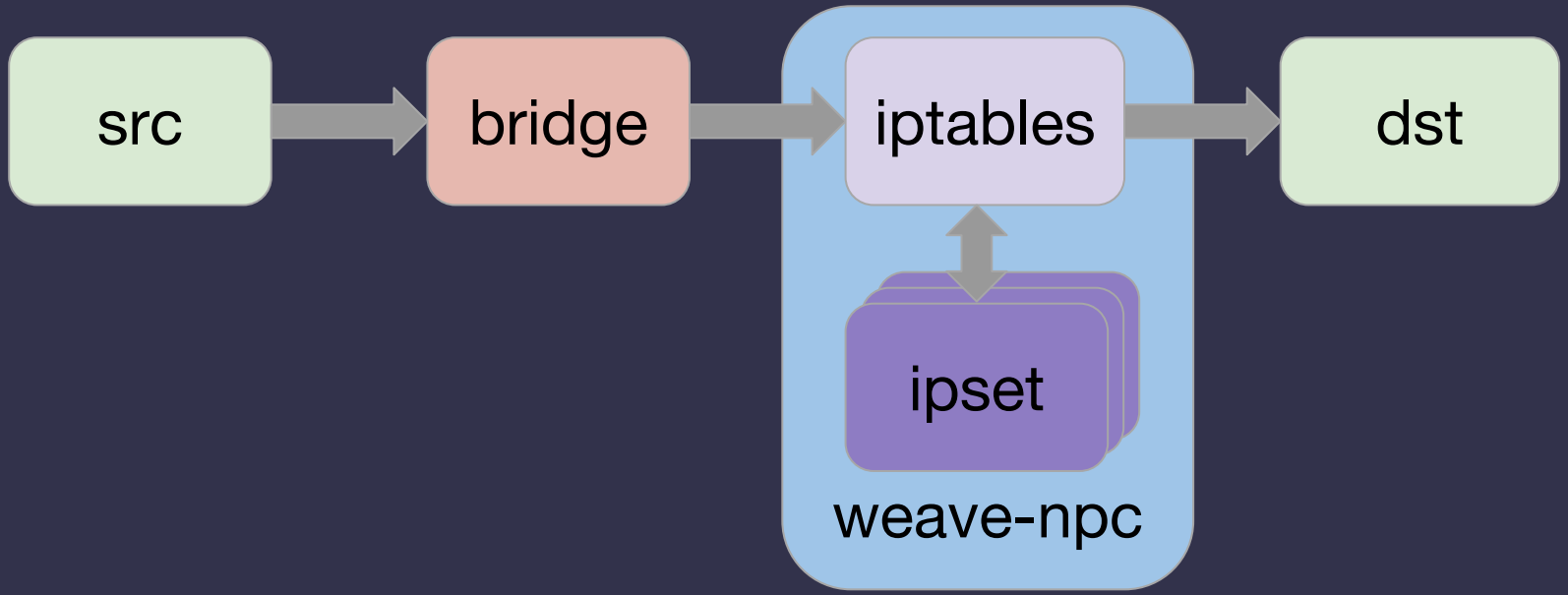
FORWARD chain:

```
-o weave -j WEAVE-NPC
-o weave -j DROP
```

WEAVE_NPC chain:

```
-m state --state RELATED,ESTABLISHED -j ACCEPT
-m state --state NEW -j WEAVE-NPC-DEFAULT
-m state --state NEW -j WEAVE-NPC-INGRESS
```

Overall flow



Per-policy iptables rules

WEAVE-NPC-DEFAULT chain:

```
-m set --match-set weave-v/q_G.;Q?uK]BuDs2 dst -j ACCEPT
-m set --match-set weave-k?Z;25^M}|1s7P3|H dst -j ACCEPT
...
```

WEAVE-NPC-INGRESS chain:

```
-m set --match-set weave-LuMDZrBg:KsT9Xll[ src
  -m set --match-set weave-hR9K[Olp~d>@1wQu/ dst -j ACCEPT
-m set --match-set weave-hR9K[Olp~d>@1wQu/ src
  -m set --match-set weave-hR9K[Olp~d>@1wQu/ dst -j ACCEPT
...
```

What could possibly go wrong?

Back in the FORWARD chain:

```
-o weave -m state --state NEW -j NFLOG --nflog-group 86
```

We subscribe to this via `ulogd` so we can print:

```
TCP connection from 10.32.0.7:56648 to 10.32.0.11:80
blocked by Weave NPC.
```

Also exported as a Prometheus metric

Interested?

Try it out!

https://weave.works/securing-microservices-kubernetes/

Take a look at the code!

https://github.com/weaveworks/weave/

Visualize, manage and monitor containers and services

https://cloud.weave.works

Fin

3-tier Illustration