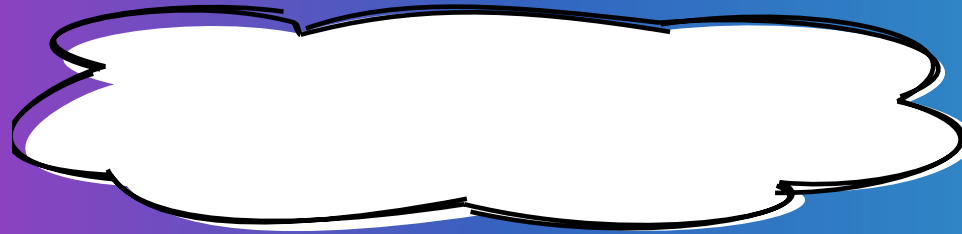# WHO NEEDS USERS
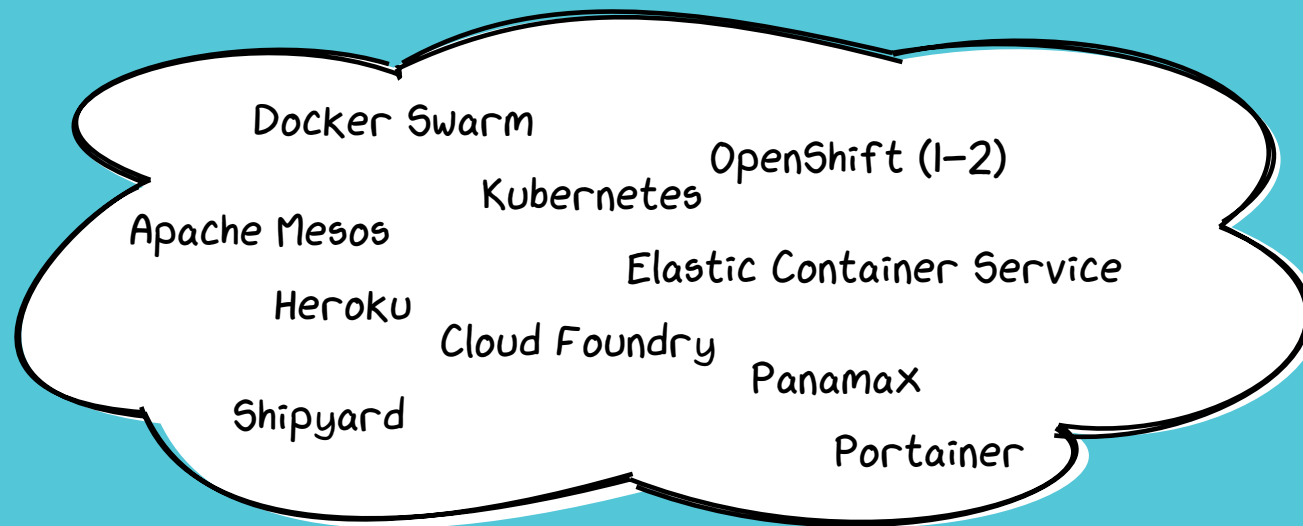# IN THIS BRAVE **CLOUD NATIVE** WORLD?

END USERS BEWARE

Kubernetes is for people building platforms. If you are a developer building your own platform (AppEngine, Cloud Foundry, Heroku clone), then Kubernetes is for you.

– Kelsey Hightower

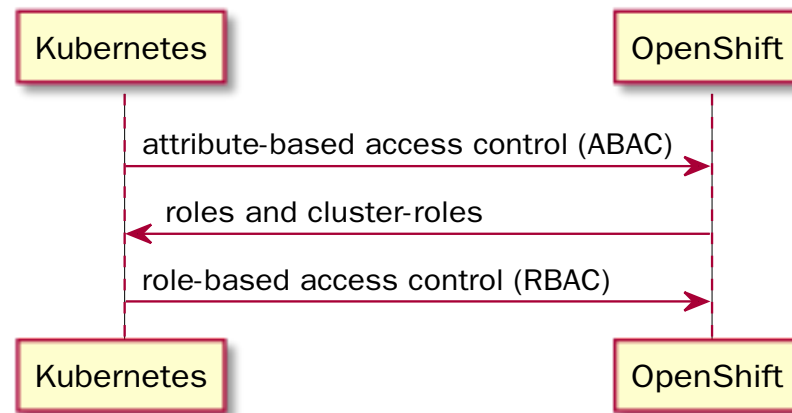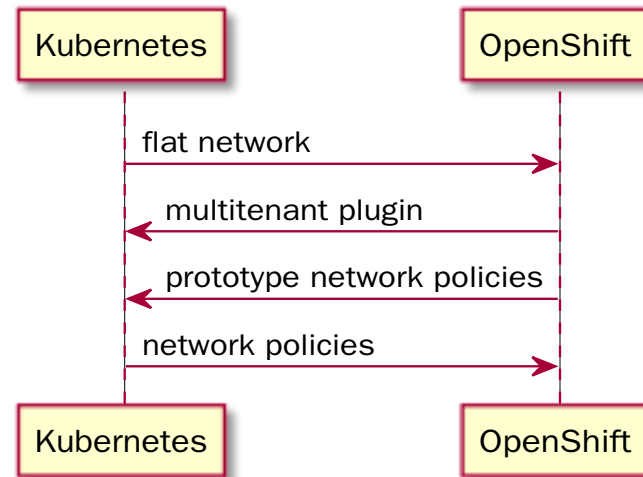Source: @kelseyhightower on 24 Feb 2019.

ALL HAPPY FAMILIES

Docker Swarm

OpenShift (1-2)

Kubernetes

Apache Mesos

Elastic Container Service

Heroku

Cloud Foundry

Panamax

Shipyard

Portainer

SPLENDID ISOLATION

Kubernetes

PIZZA EFFECTS: IDENTITY

Kubernetes   OpenShift

attribute-based access control (ABAC) →

← roles and cluster-roles
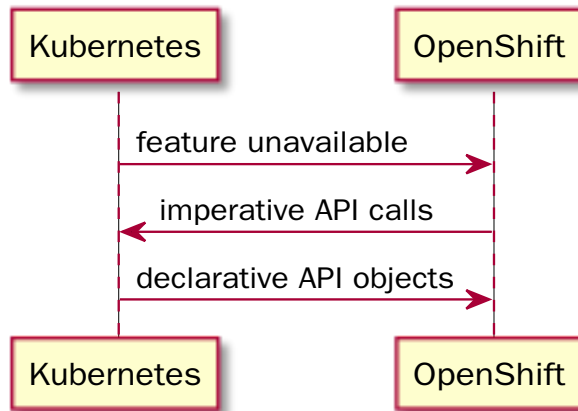
role-based access control (RBAC) →

Kubernetes   OpenShift

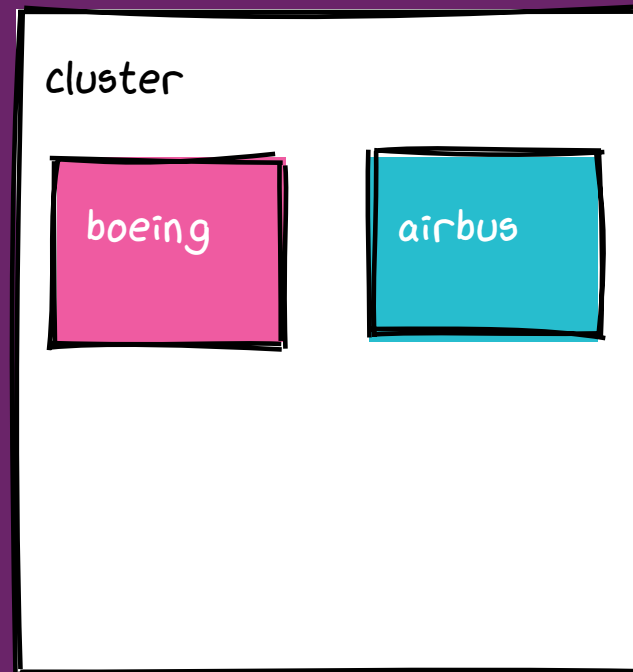# PIZZA EFFECTS: NETWORKING

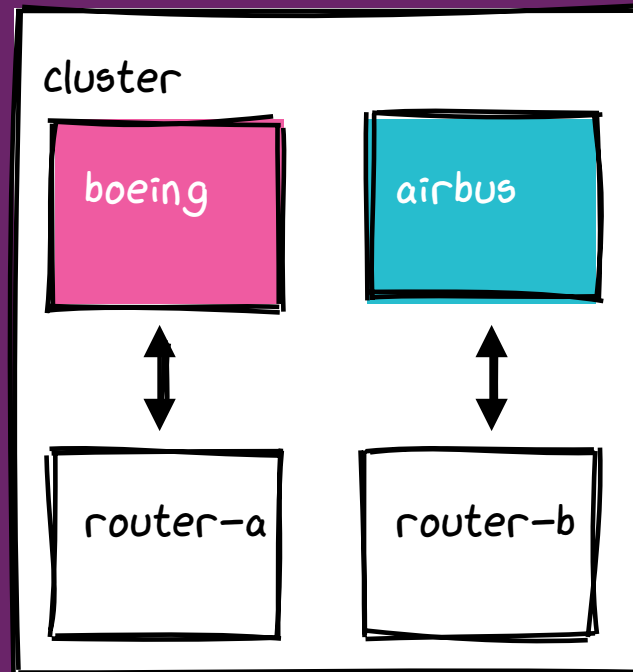# PIZZA EFFECTS: GENERIC

MULTITENANCY

ENABLE ROUTER ACCESS
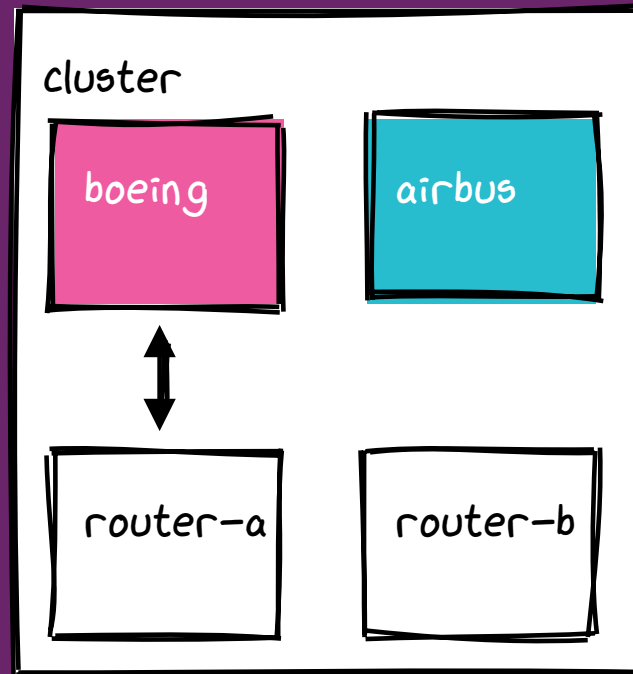


```
$ oc adm pod-network join-projects --to router-a boeing
$ oc adm pod-network join-projects --to router-b airbus
$ oc get netnamespace airbus boeing router-a router-b
NAME          NETID
airbus        1064346
boeing        1086658
router-a      1064346
router-b      1086658
```
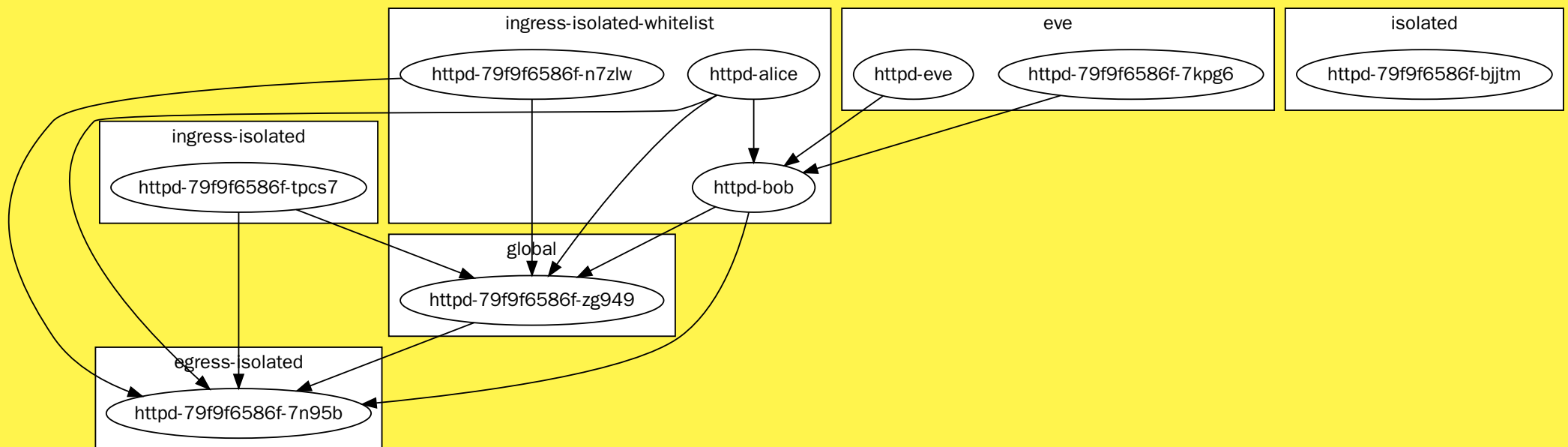
SELECTIVE ISOLATION


```
$ oc adm pod-network isolate-projects airbus
$ oc get netnamespace airbus boeing router-a router-b
NAME            NETID
airbus          1020181
boeing          1086658
router-a        1086658
router-b        1064346
```
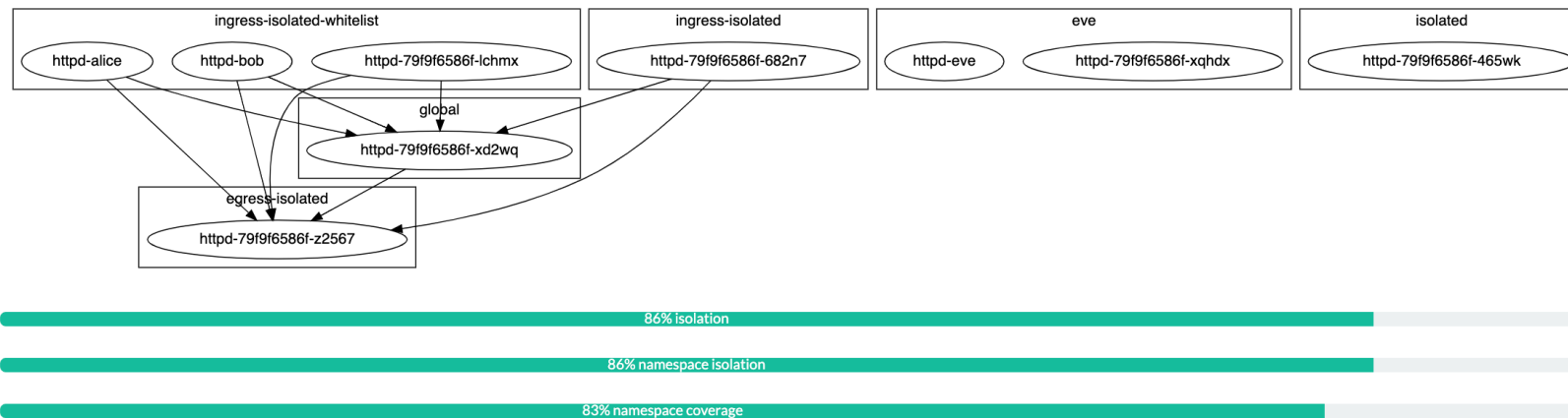
NETWORK POLICIES

AUDIT

Source: github.com/gerald1248/k8s-network-policy-viewer

IMPLEMENTATION

Somebody else's problem

WHAT THE USER SAW

```yaml
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: ingress-whitelist-pod
spec:
  podSelector:
    matchLabels:
      app: httpd-bob
  policyTypes:
  - Ingress
  ingress:
  - from:
    - podSelector:
        matchLabels:
          app: httpd-alice
```

USER ALL AT SEA (1)

```
podSelector: {}
```

is the opposite of:

```
podSelector: []
```

This is a very minor issue (and really a point of YAML syntax rather than NetworkPolicy objects), but it still leads to some policies in the wild whose effect is the exact opposite of what the author intended.

USER ALL AT SEA (2)
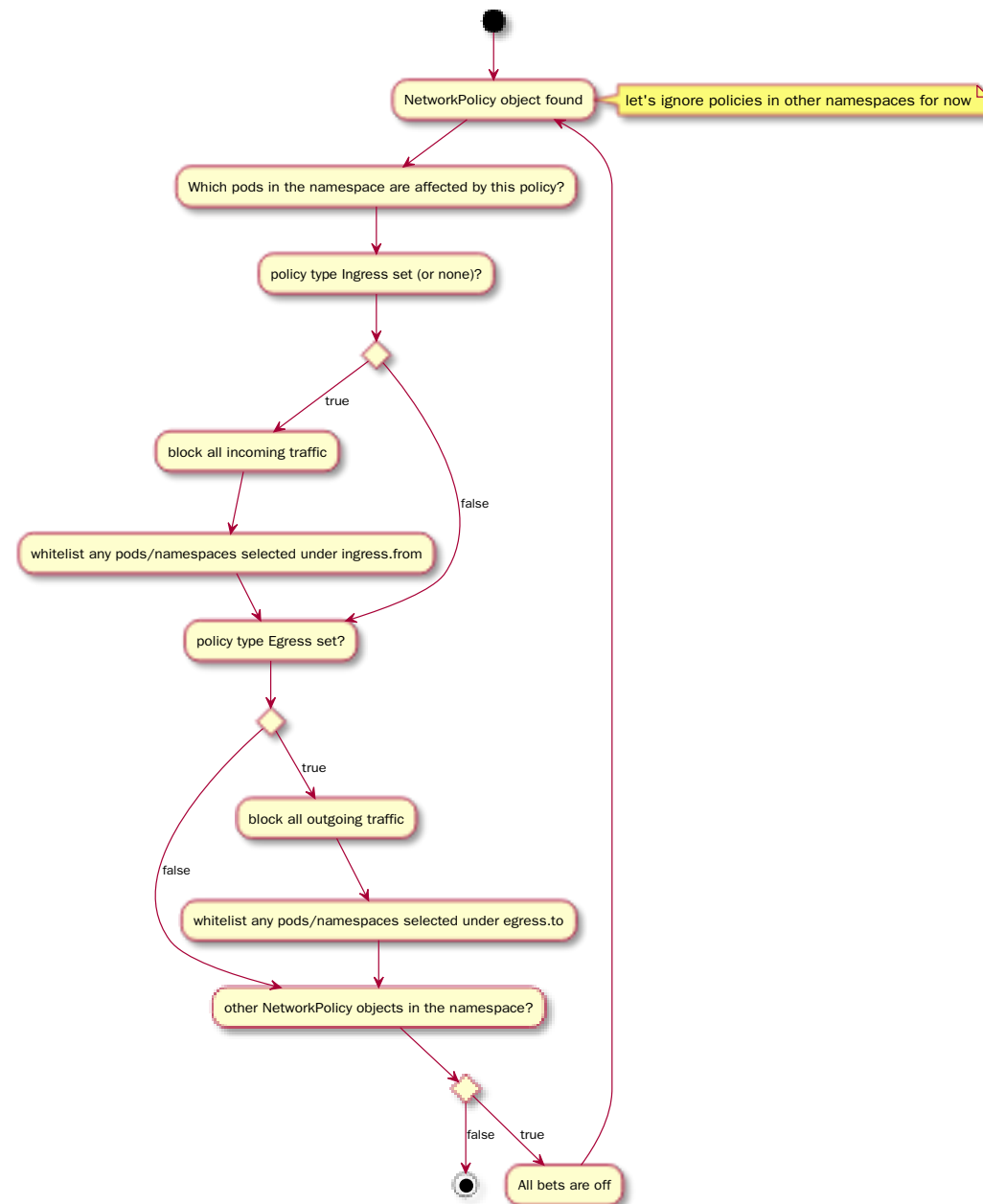
```
ingress:
- from:
  - namespaceSelector:
      matchLabels:
        user: alice
    podSelector:
      matchLabels:
        role: client
```
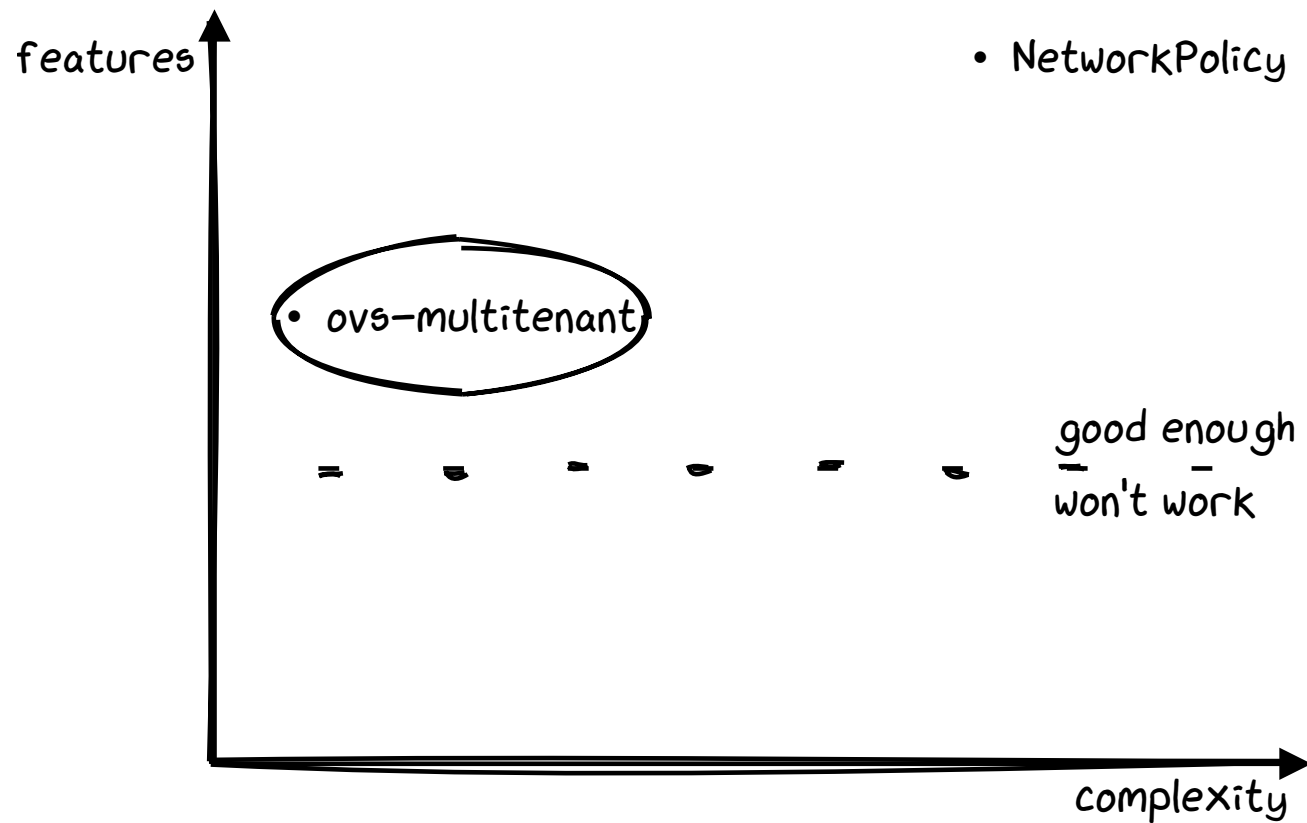
is not at all the same as:

```
ingress:
- from:
  - namespaceSelector:
      matchLabels:
        user: alice
  - podSelector:
      matchLabels:
        role: client
```

Source: kubernetes.io/docs.

WHAT THE PARSER DID

USER PREFERENCE

features

• NetworkPolicy

• ovs-multitenant

good enough
———   ———
won't work

complexity

ENTER OPERATOR

```yaml
apiVersion: v1
kind: Namespace
metadata:
  name: ingress-isolated-whitelist
  labels:
    app: ingress-isolated-whitelist
  annotations:
    networking.k8s.io/netnamespace-id: "100"
```

BEWARE ROUGH EDGES

I'm a little bit sad how complex Kubernetes is right now.
In some sense Kubernetes is not for end users, it's for
people who set up clusters and clusters are for end users.

— Wojtek Cichoń

Source: Cichoń, W. 2018. What's real and what's not.

THANK YOU

Slides built with Markdeck
 gerald1248/who-needs-users-slides
 03spirit

ThoughtWorks®