Trust is good, control is better
A short story about Network Policies

Maximilian Bischoff,
Johannes M. Scheuermann

Hamburg, 26. June 2019
Maximilian Bischoff
Cloud Platform Engineer

Johannes M. Scheuermann
Cloud Platform Engineer

Unofficial: Chaos Monkey
@johscheuer
What can you expect?

- Get an overview about challenges with network policies
- Get an overview on different aspects of testing / validating your setup
What about you?
Why should I test my network policies?
Why should I test my policies?

Many adjustment screws

https://www.pexels.com/photo/colorful-toothed-wheels-171198
Why should I test my policies?

Kubernetes doesn’t implement the policies
Why should I test my policies?

Kubernetes doesn’t implement the policies
Why should I test my policies?
I choose you!

This list is not complete!
Why should I test?

Hard to read policies

```yaml
spec:
ingress:
  - from:
    - namespaceSelector:
      matchLabels:
        team: operations
    podSelector:
      matchLabels:
        type: monitoring

... and ...

spec:
ingress:
  - from:
    - namespaceSelector:
      matchLabels:
        team: operations
    podSelector:
      matchLabels:
        type: monitoring

... or ...
```

Why should I test my policies?

Component updates
Why should I test my policies?

Component updates

Is everything still working after an update?
Why should I test my policies?

Component updates

Conformance tests don’t test network policies!
What to test
What to test

- Effect of policies
- Synchronisation
How to test
How to test

Conformance

- Effect of policies
- Synchronisation
Testing strategies

Copy-pod

```
kind: pod
apiVersion: v1
metadata:
  name: foo
  namespace: default
labels:
  app: foo
spec:
  containers:
    - name: foo
      image: foo:latest
...
```

```
kind: pod
apiVersion: v1
metadata:
  name: foo-test-copy
  namespace: default
labels:
  app: foo
  testing.framework: ""
spec:
  containers:
    - name: test
      image: test/runner:latest
...
Testing strategies

Docker networking
Testing strategies

Linux namespaces

pause (of pod foo)

IPC

Network

... ...

underlying OS

test-runner

CGroup

IPC

CGroup

...
kubectl exec -it foo -- wget -qO - --timeout=2 http://bar.default
wget: download timed out

customizable

```yaml
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  name: default-deny-all
  namespace: default
spec:
  podSelector: {}
  ingress: []
```

netassert

config.yaml
---

k8s:
deployment:
  default:foo:
  default:bar: TCP:80

```bash
ssh docker run --net ...
```

```javascript
netassert
```

```yaml
test.js
```

```bash
nmap
```

```bash
node 1
```

```bash
bar
```

```bash
foo
```
Test case generation

Preface

```yaml
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  name: demo
  namespace: default
spec:
  podSelector:
    matchLabels:
      app: prometheus
  ingress:
    ...
```

isolated from every pod except for those matching
Test case generation

Two kinds of tests

... 
spec:
podSelector:
  matchLabels:
    app: prometheus
ingress:
  - from:
    podSelector:
      matchLabels:
        app: grafana

pod A
app=prometheus

pod B
app=grafana

pod C
Test case generation

Multiple policies

... spec:
  podSelector:
    matchLabels:
      app: prometheus
  ingress:
    - from:
      podSelector:
        matchLabels:
          app: grafana

pod A

app=prometheus

pod B

app=foo

spec:
  podSelector: {}
  ingress:
    - from:
      podSelector:
        matchLabels:
          team: ops
          namespaceSelector: {}
Wrap up
How do these tools complement

Policy

SDN Control Plane

Data Plane

illuminatio / netassert

/ kubeaudit
Recap

● Test your assumptions!

● Regression testing makes your life easier

● Network Policies are still hard to get right
  ○ Missing feedback
  ○ Does it work for Services and Pods?
Thank You

Maximilian Bischoff
IT Engineering & Operations

inovex GmbH
Ludwig-Erhard-Allee 6
76131 Karlsruhe

maximilian.bischoff@inovex.de

Johannes Scheuermann
IT Engineering & Operations

inovex GmbH
Ludwig-Erhard-Allee 6
76131 Karlsruhe

johannes.scheuermann@inovex.de