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

Maximilian Bischoff,
Johannes M. Scheuermann

Remote, 28. May 2020
Maximilian Bischoff
Cloud Platform Engineer
@bisch_off_max

Johannes M. Scheuermann
Bob the cloud builder
“Can we fix it? Yes we can!”
@johscheuer
What can you expect?

- Know some challenges with network policies
- See different aspects of testing / validating your setup
- See how different testing strategies in a containerized world can work
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*

*and not part of CNI!
Why should I test my policies?
Kubernetes doesn’t implement the policies*

* and not part of CNI!
Why should I test my policies?

I choose you!

This list is not complete!
Why should I test?

Hard to read policies

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

Why should I test my policies?

Component updates

Node

kube-proxy

iptables

CNI-Plugins

Node

kube-proxy

iptables

CNI-Plugins

Node

kube-proxy

iptables

CNI-Plugins

Node

kube-proxy

iptables

CNI-Plugins

Node

kube-proxy

iptables

CNI-Plugins
Why should I test my policies?

Component updates

Is everything still working after an update?

Node

kube-proxy

iptables

CNI-Plugins

Node

kube-proxy

iptables

CNI-Plugins

Node

kube-proxy

ipvs

CNI-Plugins

Node

kube-proxy

iptables

CNI-Plugins v1

Node

kube-proxy

iptables

CNI-Plugins v2
Why should I test my policies?

Component updates

Node

kube-proxy

iptables

CNI-Plugins

Node

kube-proxy

ipvs

CNI-Plugins

Node

kube-proxy

iptables

CNI-Plugins

Node

kube-proxy

iptables

CNI-Plugins v1

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

Conformance
- 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)

CGroup
IPC
Network
...
underlying OS

test-runner

CGroup
IPC
Tools

kubectl + wget/curl

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

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

Tools

netassert

```yaml
---
k8s:
  deployment:
    default:foo:
    default:bar: TCP:80
```

docker run --net ...

- foo
- bar
- bar

node 1

test.js

nmap

https://github.com/controlplaneio/netassert
Tools

illuminatio

https://github.com/inovex/illuminatio
Test case generation

Preface

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

Two kinds of tests

```yaml
... 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
team=ops
app=foo
Demo
Wrap up
How to complement these tools

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?
Outlook

• Make use of ephemeral containers
  ◦ [https://github.com/kubernetes/enhancements/issues/277](https://github.com/kubernetes/enhancements/issues/277)

• Provide a conformance test suite for CNI Policies [1]

• Add more (Network)Policies solutions
  ◦ cilium, Calico, Istio, ...

illuminatio

Feel free to use it and give us feedback!

https://github.com/innex/illuminatio
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