
KubeCon
CloudNativeCon
North America 2022
BUILDING FOR THE ROAD AHEAD
DETROIT 2022
TiKV
TiKV
HELM

BUILDING FOR THE ROAD AHEAD

DETROIT 2022

Putting Hackers Breaching Your Cluster in Automatic Quarantine

Ziv Nevo

Talk proposed by Shmulik Froimovich

A scary thing…

A scarier thing…

TOO MANY CLOUD APPLICATIONS DO NOT APPLY EGRESS CONTROL

Why is it so scary?

- Without egress control, any intrusion may result in a data leak
- Intrusions can no longer be prevented by just enforcing a tight ingress control
  - Insider threats
  - Social engineering and spear phishing attacks
  - Supply chain attacks

- **It’s not a question of if, it’s a question of when**

Some famous breaches

KubeCon CloudNativeCon North America 2022

SolarWinds: Hacked firm issues urgent security fix

24 December 2020

The Telegraph News Sport Business Opinion Ukraine Money Life Style Travel Culture Puzzles

Alex Economy Companies Markets Tech

Passwords from 100 million Quora users stolen in dat

Could be prevented with tighter egress control

TECHNOLOGIES INTERVIEWS EVENTS

ata breach, a hacker accessed user data

ars TECHNIC

POISONING THE WELL —

Widely used open sou bitcoin-stealing back

Malicious code that crept into event-stream JavaScript library went undetected for weeks.

DAN GOODIN - 11/27/2018, 12:55 AM

Hacking

Reddit discloses a data breach, a hacker accessed user data

Haythem Elmir 4 ans ago

And there is compliance…

NIST Special Publication 800-53 Revision 4, SC-7(5):

Deny network communications traffic by default and allow network communications traffic by exception at managed interfaces.

…only those system connections which are essential and approved are allowed.

Why then is egress so exposed?

- Lack of awareness
- Trusting cloud vendors
- Trusting 3rd party components
- Considered hard to configure / maintain
- Not knowing the configuration is wrong
- Unclear whose task it is

Why then is egress so exposed?

- Lack of awareness – now you are aware
- Trusting cloud vendors
- Trusting 3rd party components
- Considered hard to configure / maintain
- Not knowing the configuration is wrong
- Unclear whose task it is

Why then is egress so exposed?

- Lack of awareness – now you are aware
- Trusting cloud vendors – don’t. Defaults are permissive
- Trusting 3rd party components
- Considered hard to configure / maintain
- Not knowing the configuration is wrong
- Unclear whose task it is

Why then is egress so exposed?

- Lack of awareness – now you are aware
- Trusting cloud vendors – don’t. Defaults are permissive
- Trusting 3rd party components – don’t (details soon)
- Considered hard to configure / maintain
- Not knowing the configuration is wrong
- Unclear whose task it is

Why then is egress so exposed?

- Lack of awareness – now you are aware
- Trusting cloud vendors – don't. Defaults are permissive
- Trusting 3rd party components – don't (details soon)
- Considered hard to configure / maintain
- Not knowing the configuration is wrong
- Unclear whose task it is

Automation can help

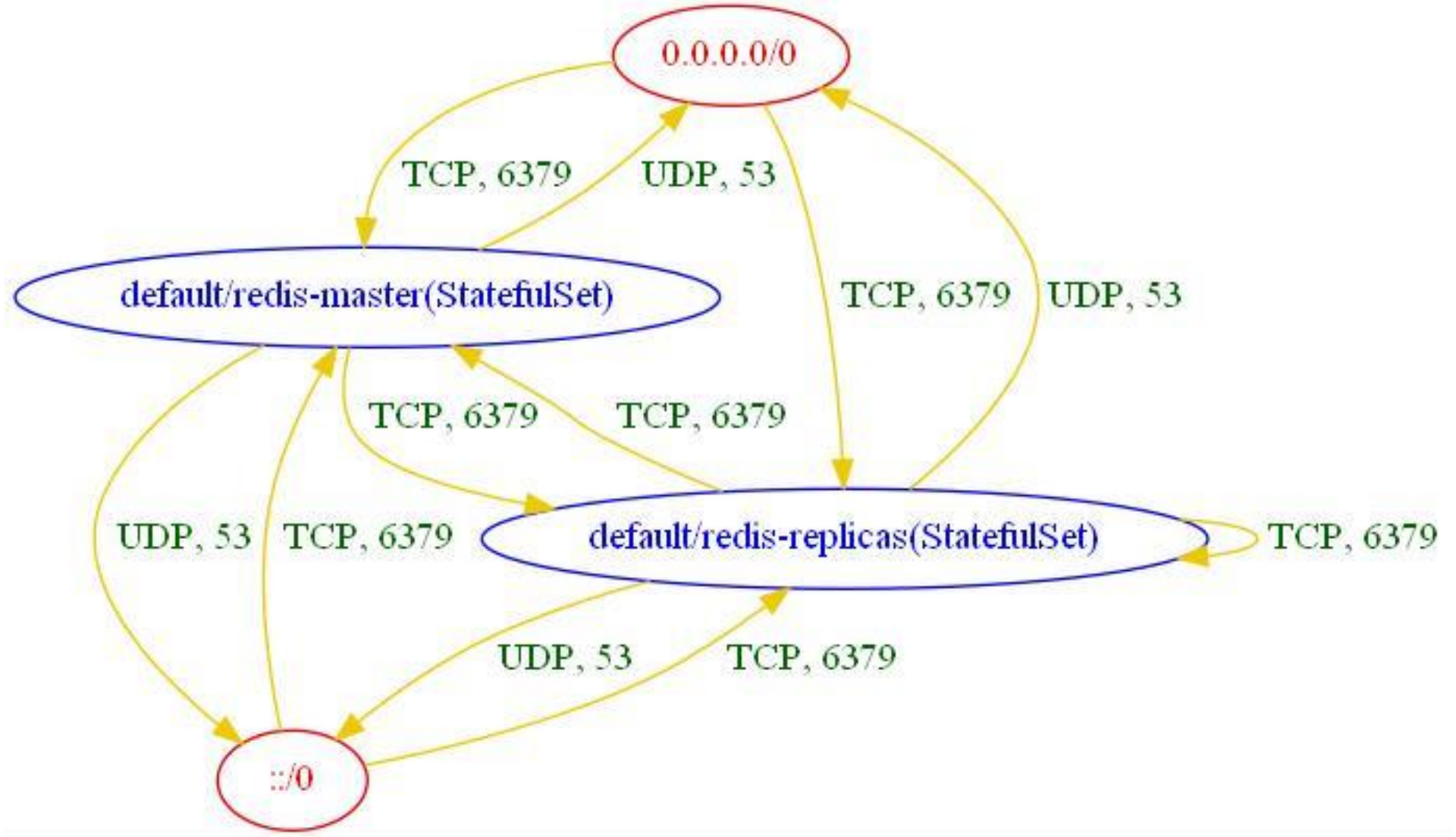
A word about controlling egress

- The best place to control egress is as close as possible to where your data lives
- In K8s-based apps this means controlling pod traffic
- Resources to control pod network traffic:
  - **K8s NetworkPolicy**
  - CNI-specific network policies
  - Also, service-mesh-specific network policies (layer 7 only)

A mini-survey of common OSS

- Looking at 15 highly popular helm packages from Artifact Hub and Bitnami
  - Including DBs, registries, event systems, …
- Most come with some ingress control
  - Typically, requires setting a specific flag to a non-default value
- **Only 4 include some egress control**
- **Never trust others' security – "zero trust"**

Egress control done right



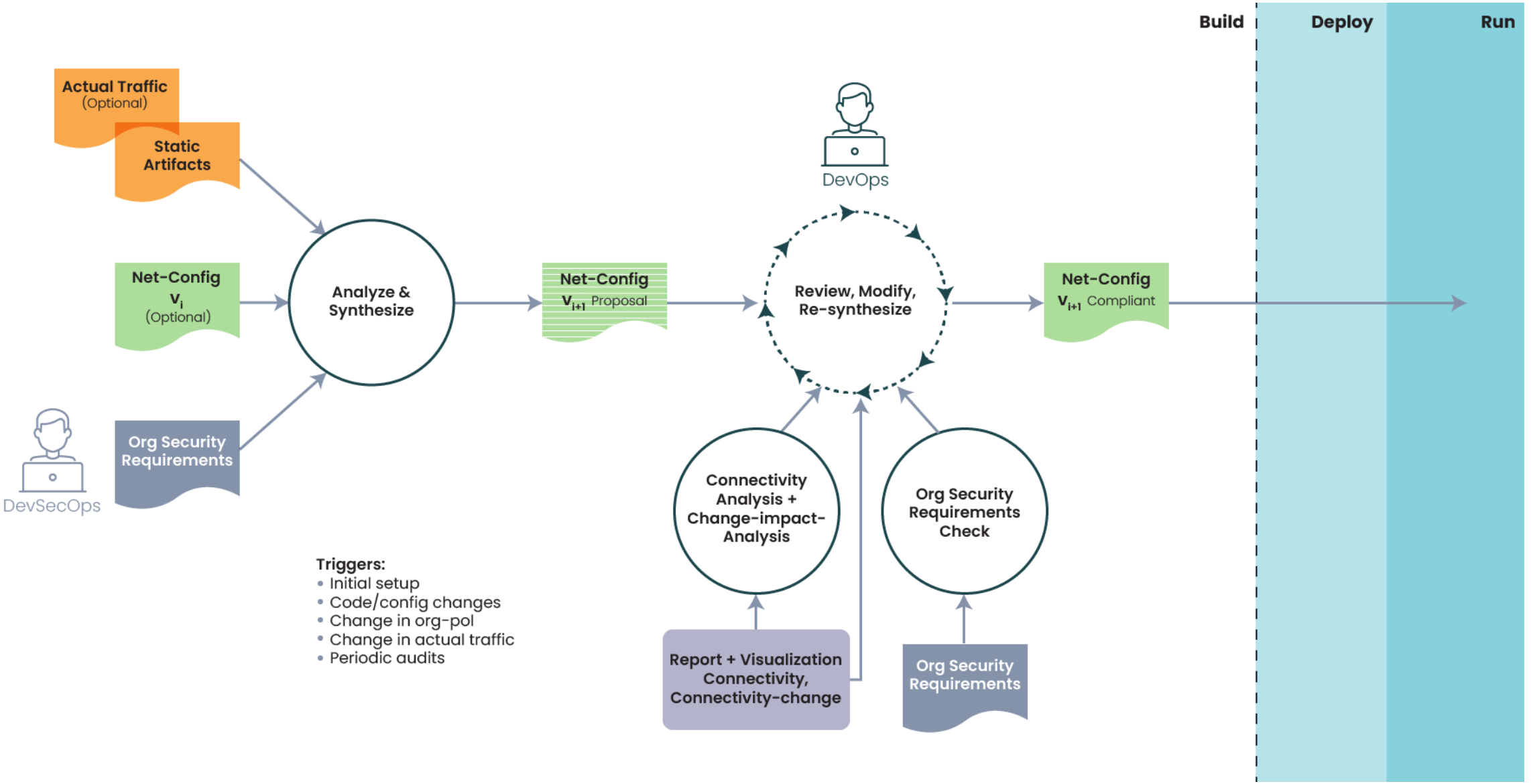
Automation can help – visualization

- Tools showing the connectivity posture of a live cluster:
  - Red Hat ACS for Kubernetes / StackRox
  - Sysdig Secure
  - Cilium Hubble
  - Calico Enterprise
  - NP-Guard
- Tools showing the expected connectivity posture, given YAML manifests (supporting shift-left methodologies):
  - NP-Guard

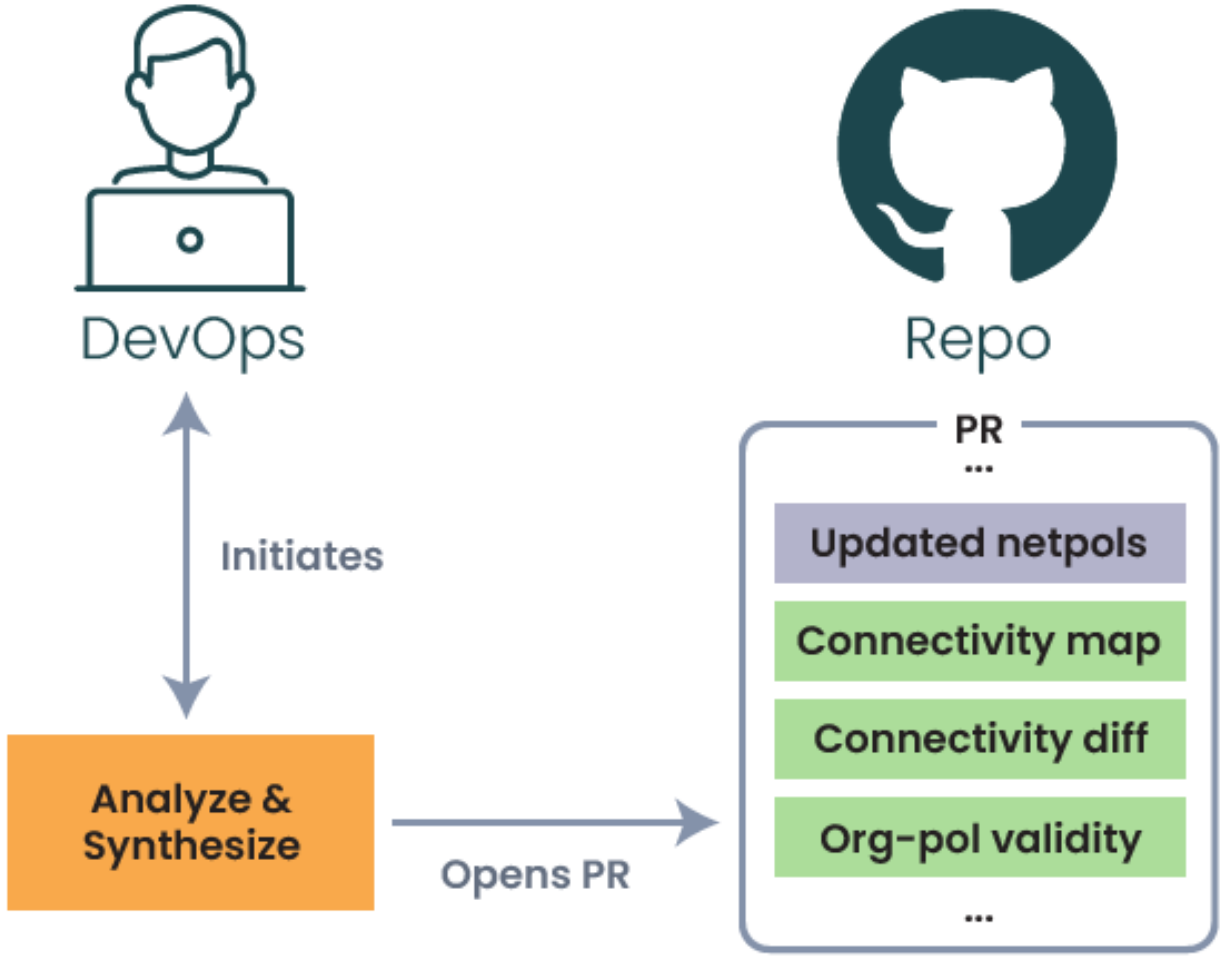
Automation can help – synthesis

- Tools based on snapshotting the traffic in a live cluster:
  - Red Hat ACS for Kubernetes / StackRox
  - Sysdig Secure
- Tools based on analyzing YAML manifests (shift-left):
  - NP-Guard

NP-Guard's shift-left vision



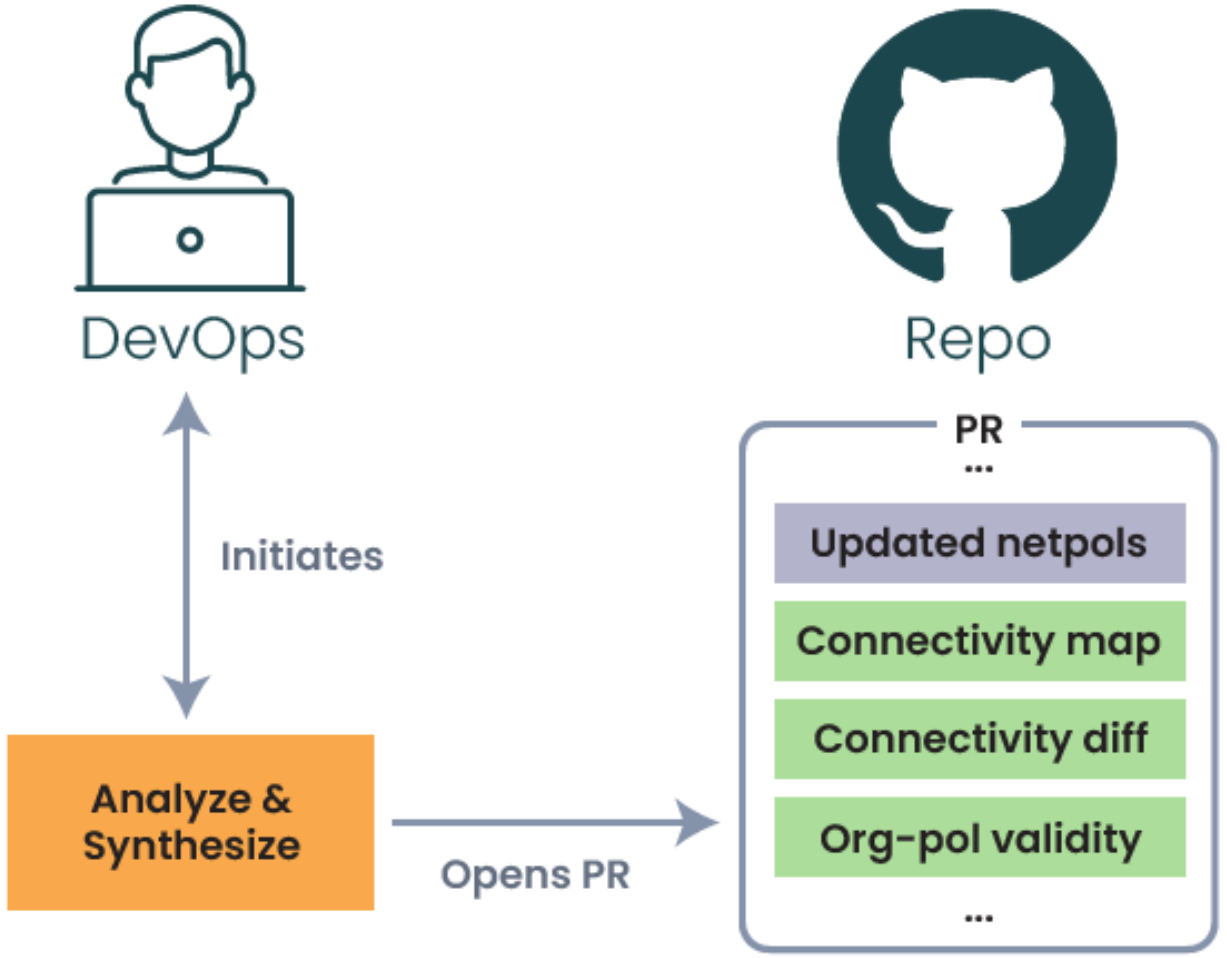
NP-Guard demo



NP-Guard demo

Here be a video…

NP-Guard demo



Summary

- Always secure both ingress and egress **at the microservice level**
- Always know your current connectivity posture – there are tools for this
- Also use tools to synthesize network policies
- Integrate the above into your CI/CD pipelines

Summary

Oh, and always wear high-top shoes when centipedes are around…

Putting Hackers Breaching Your Cluster In Automatic Quarantine

KubeCon CloudNativeCon North America 2022
BUILDING FOR THE ROAD AHEAD
DETROIT 2022

Ziv Nevo
Senior Research Scientist,
IBM Research - Israel

October 24-28, 2021

KubeCon | CloudNativeCon
North America 2022

BUILDING FOR THE ROAD AHEAD

DETROIT 2022

Please scan the QR Code above to
leave feedback on this session