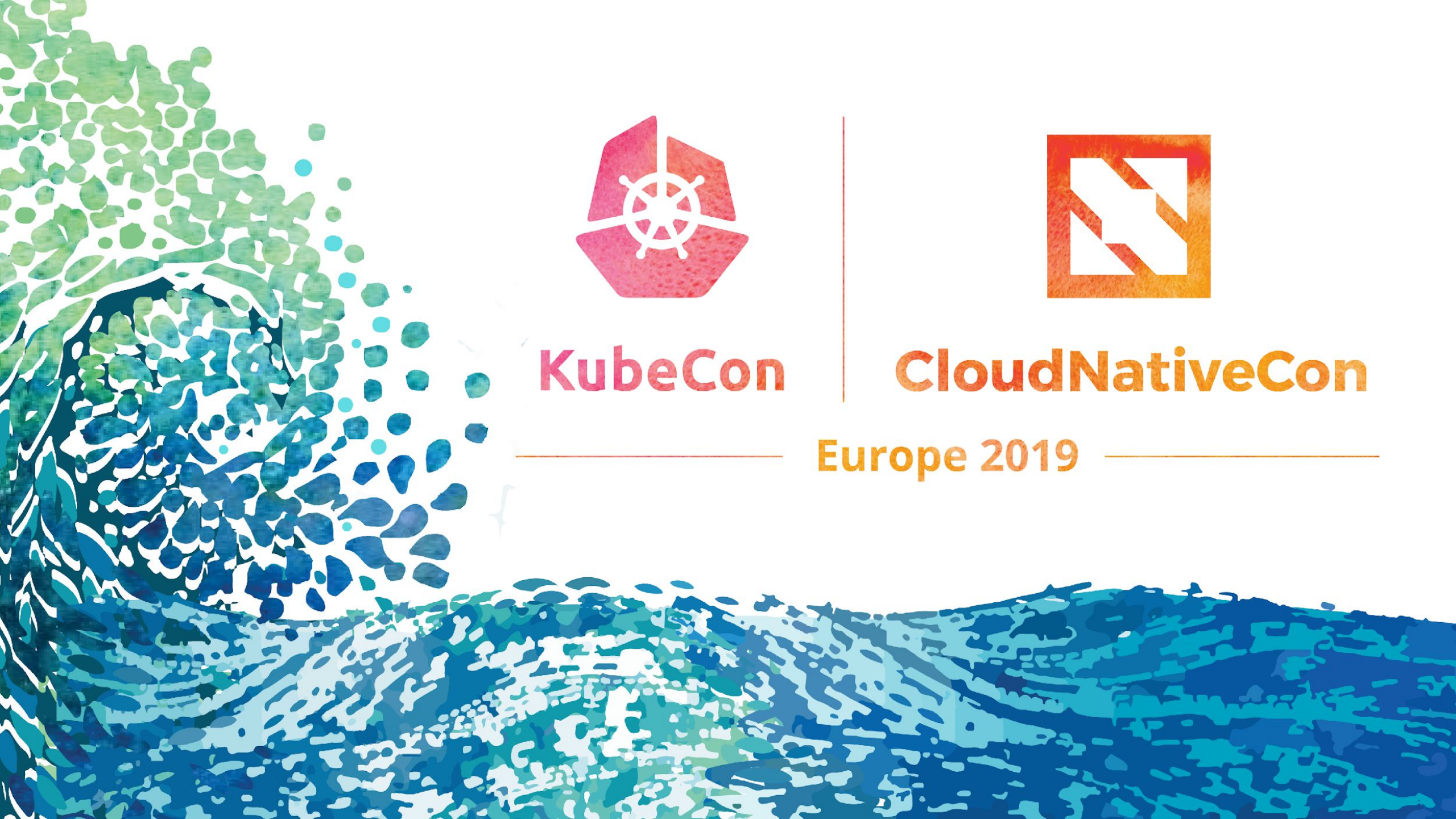

KubeCon
CloudNativeCon
Europe 2019

# Zero Trust service mesh with Calico, SPIRE, and Envoy

Evan Gilman (Scytale) and Shaun Crampton (Tigera)

# Agenda



What is Zero Trust?

What is a Service Mesh?

SPIFFE/SPIRE Overview

Calico Overview

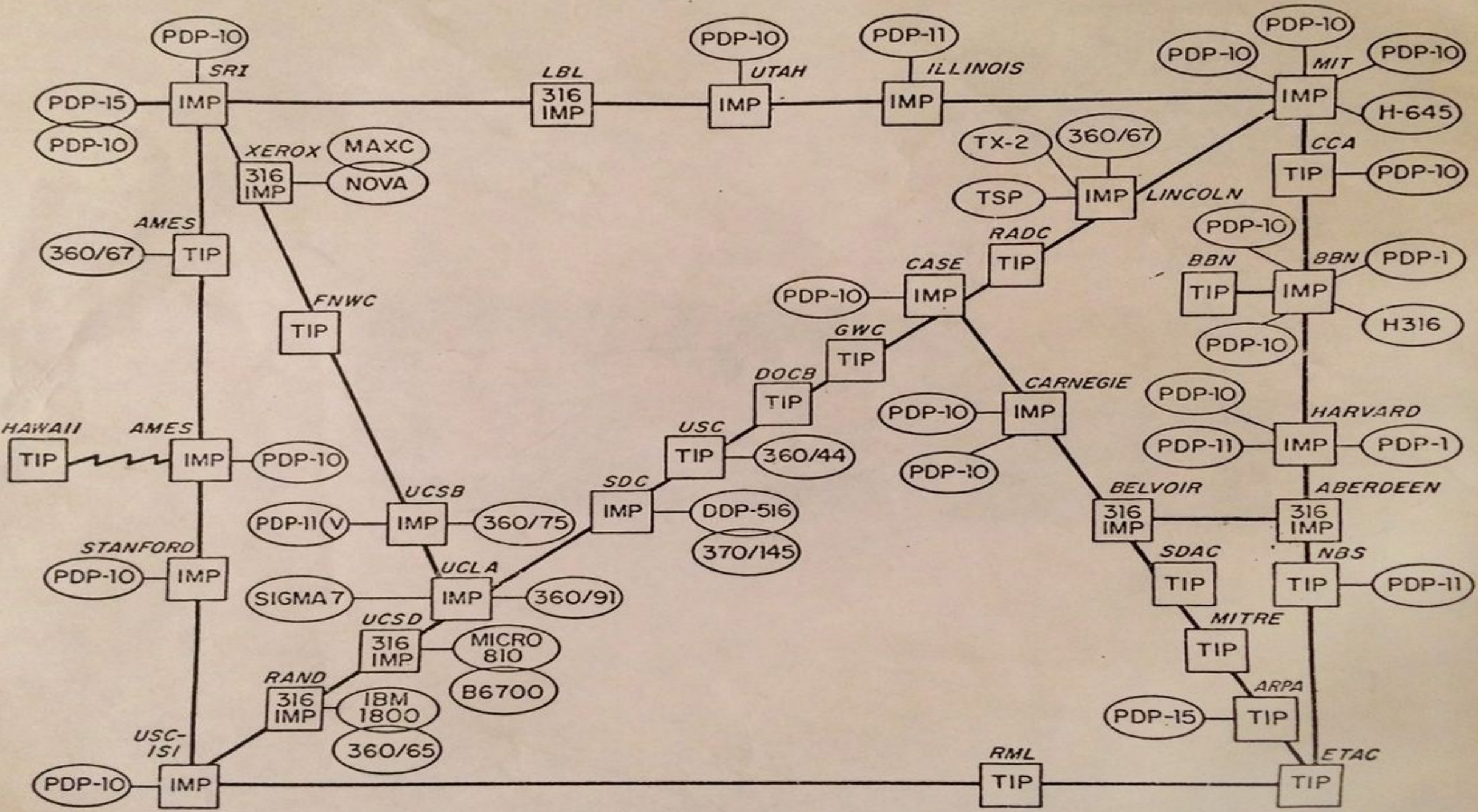
Pulling it All Together

Demo Time!

# “Zero Trust”

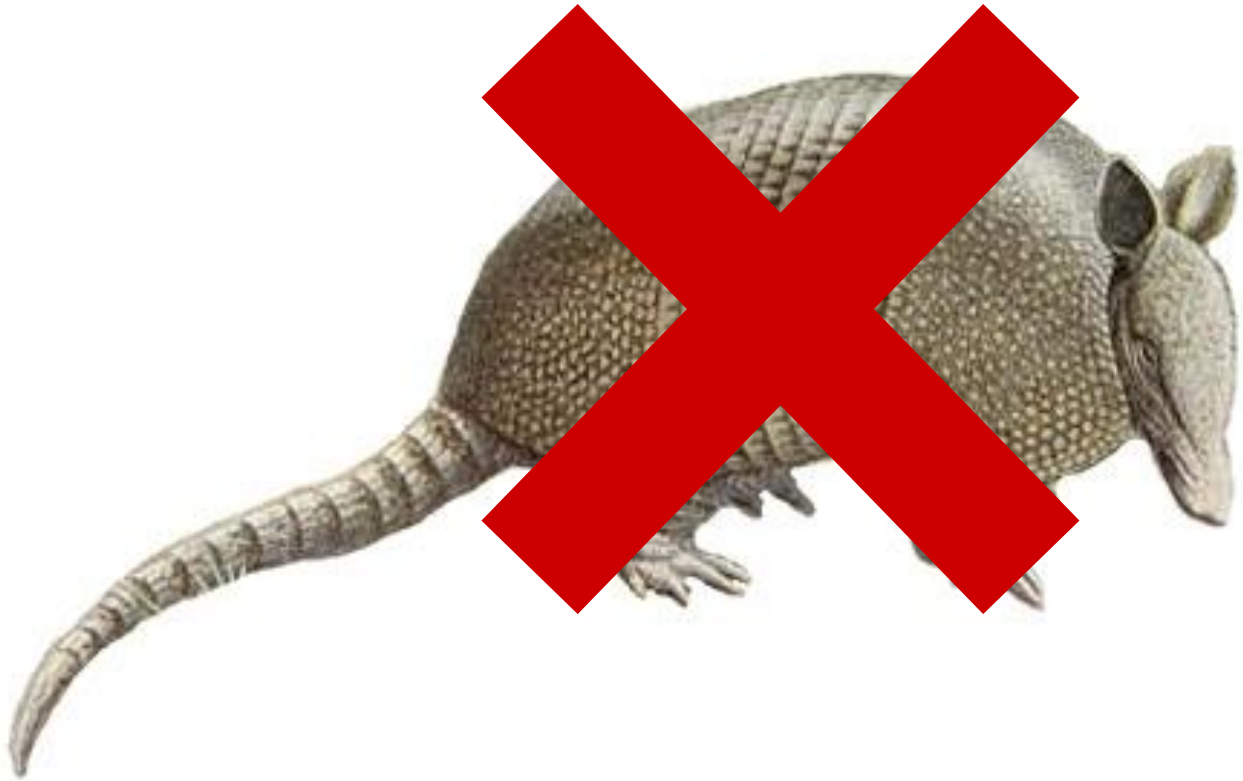
# “Zero Trust” (Networks)

# ARPA NETWORK, LOGICAL MAP, MAY 1973



# Intro to Zero Trust

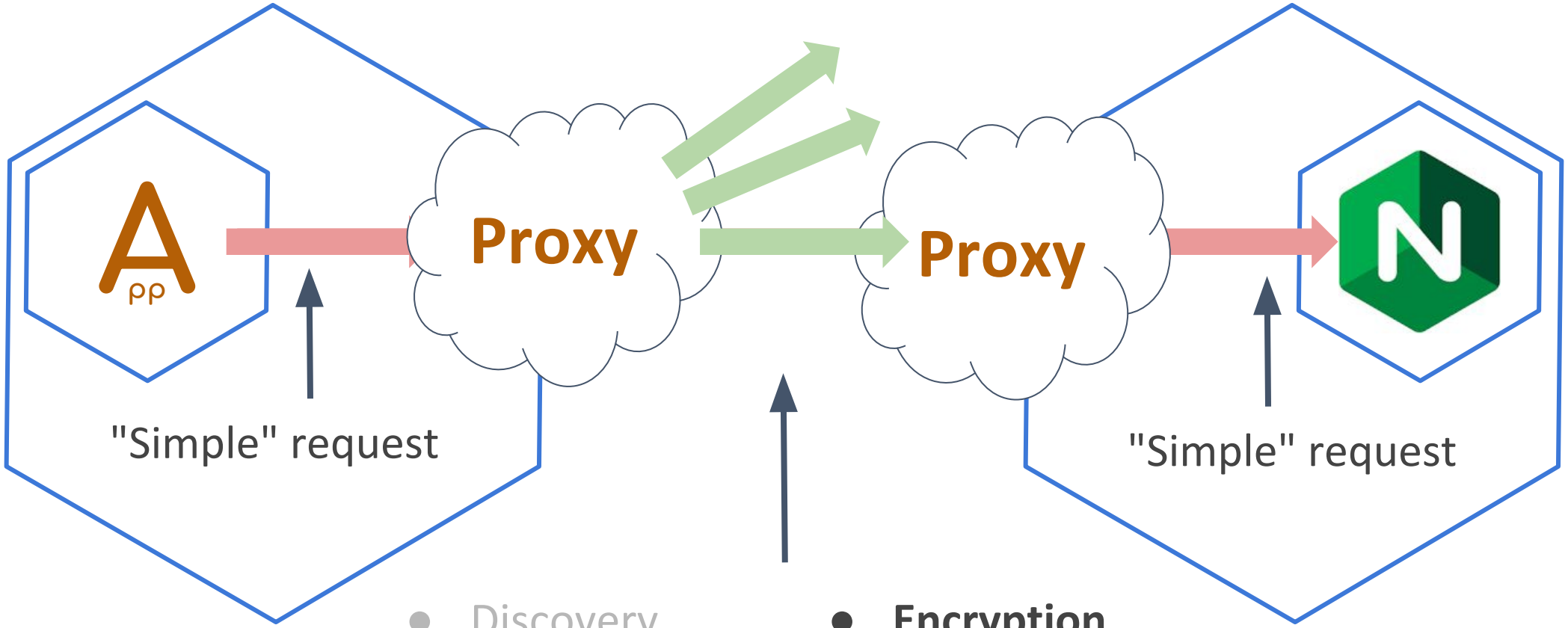




# Service mesh

# Service mesh



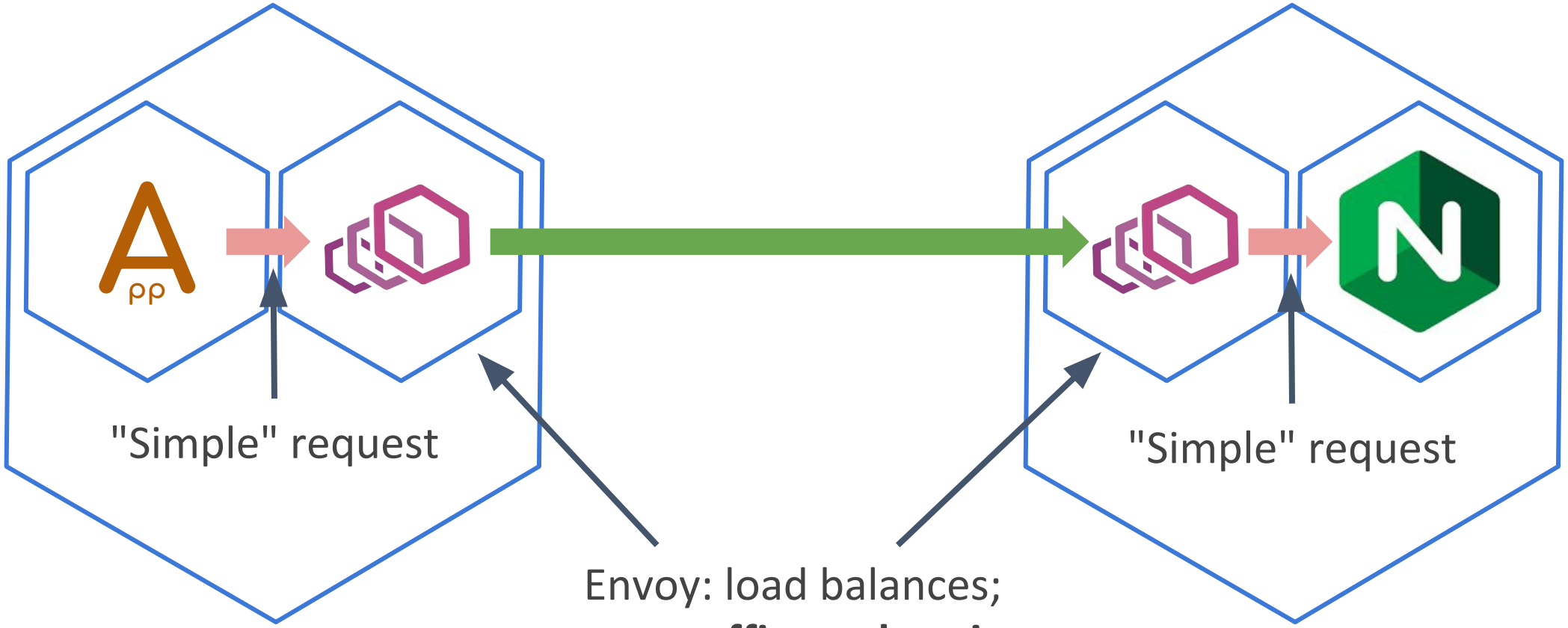



- Discovery
- Load balancing
- Observability

- **Encryption**
- **Authentication**
- **Authorization**

# Service proxy: Envoy





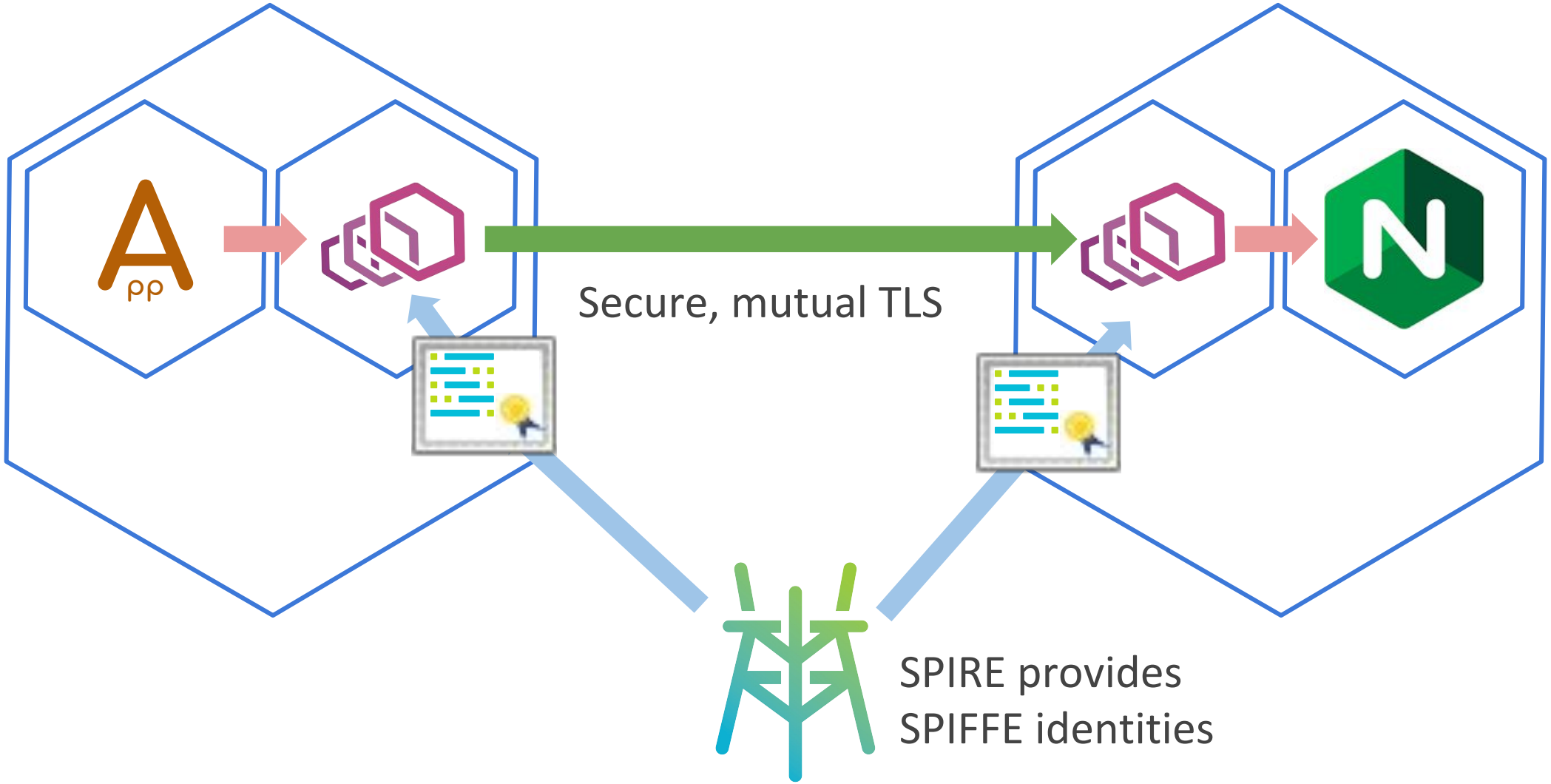

Envoy: load balances;
**encrypts traffic**; **authenticates**;
**enforces** policy decisions
(and lots more…)

But, it needs help...

# Intro to SPIFFE and SPIRE

# Intro to SPIFFE and SPIRE



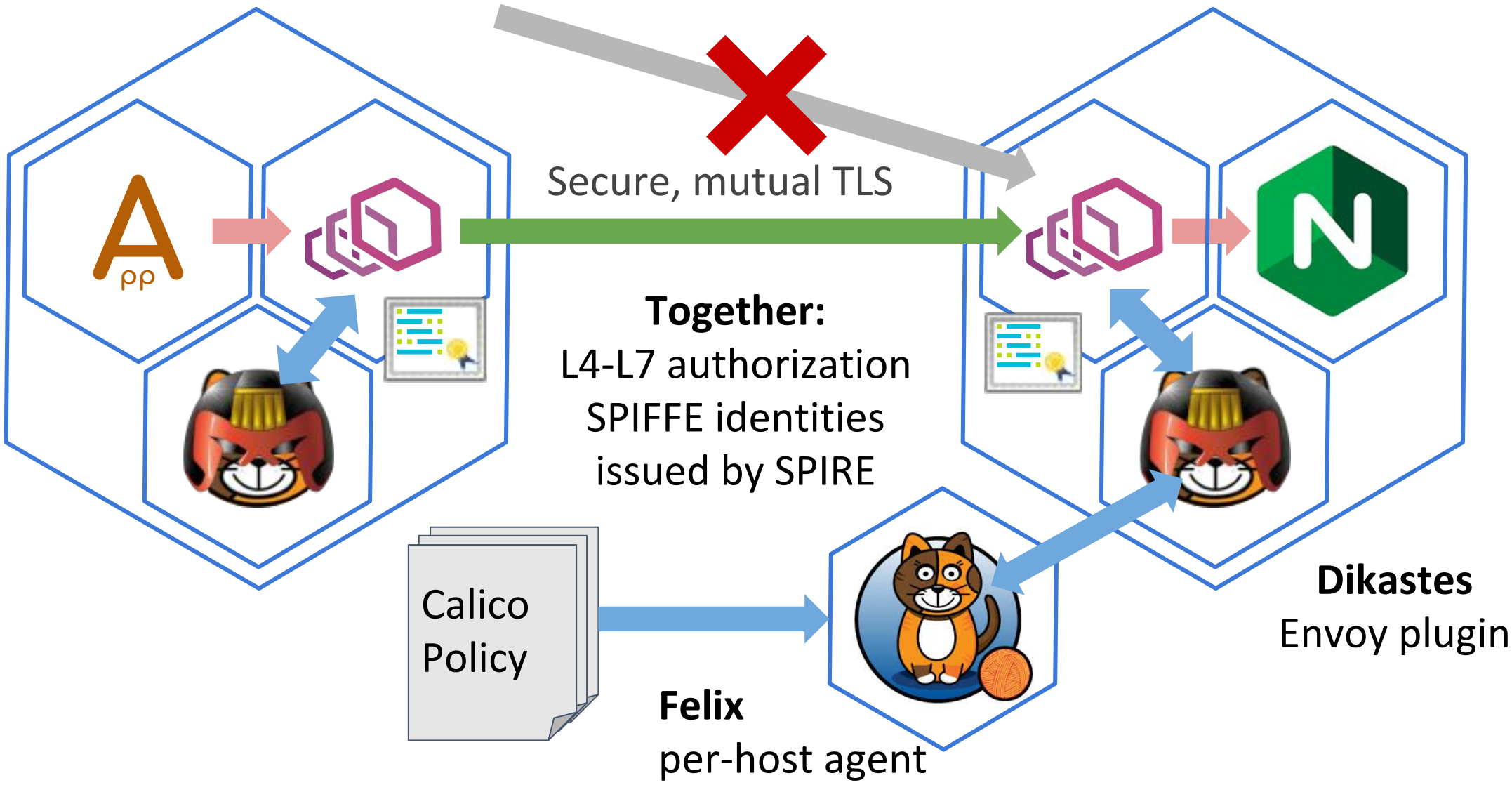


# More about SPIFFE and SPIRE

# Policy enforcement

# Authorization with Calico





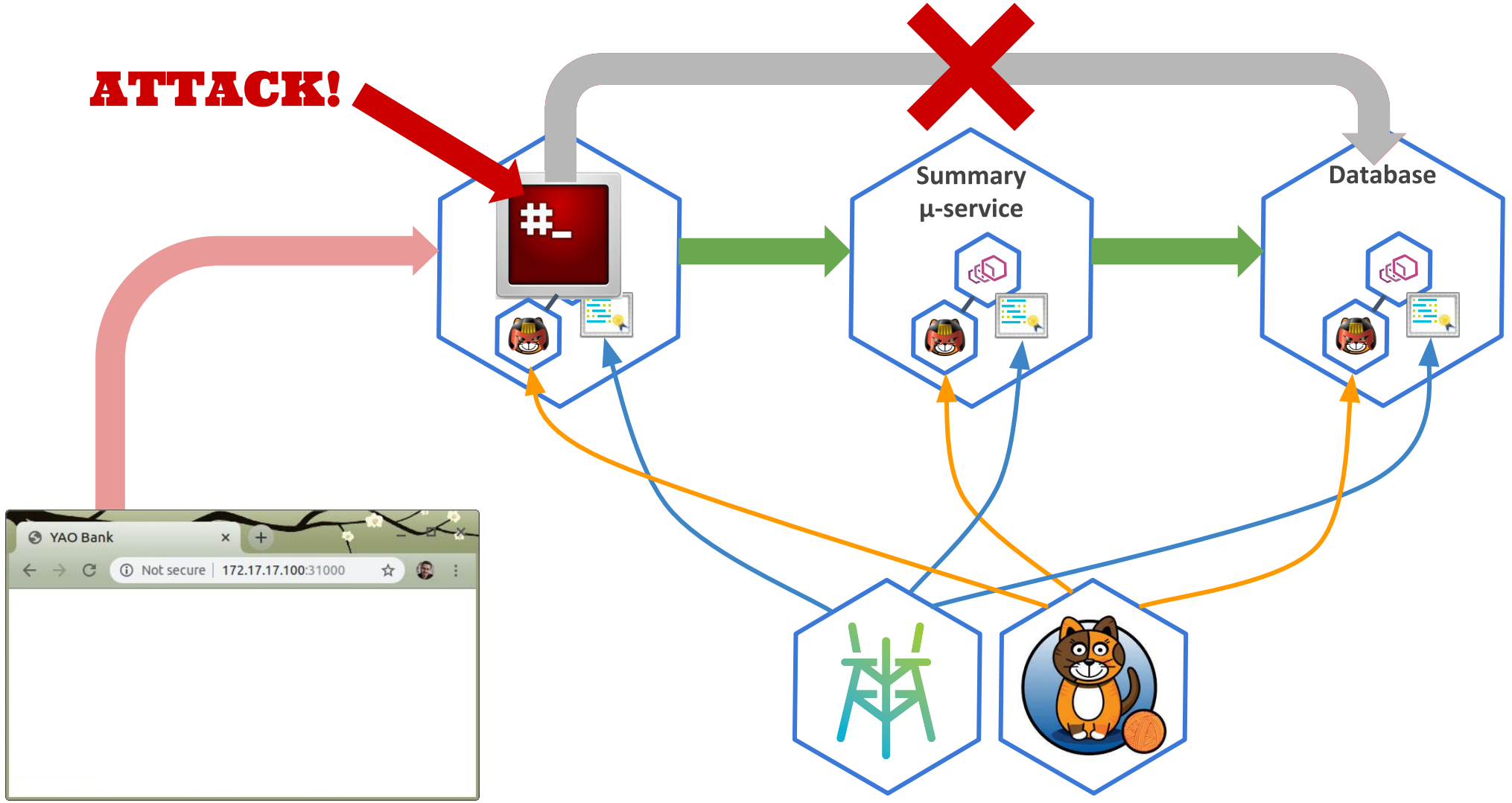
# DEMO



- Let's rob a bank...

# DEMO




ATTACK!
Summary
µ-service
Database
YAO Bank
Not secure
172.17.17.100:31000

# DEMO

# Q&A

KubeCon

CloudNativeCon

Europe 2019