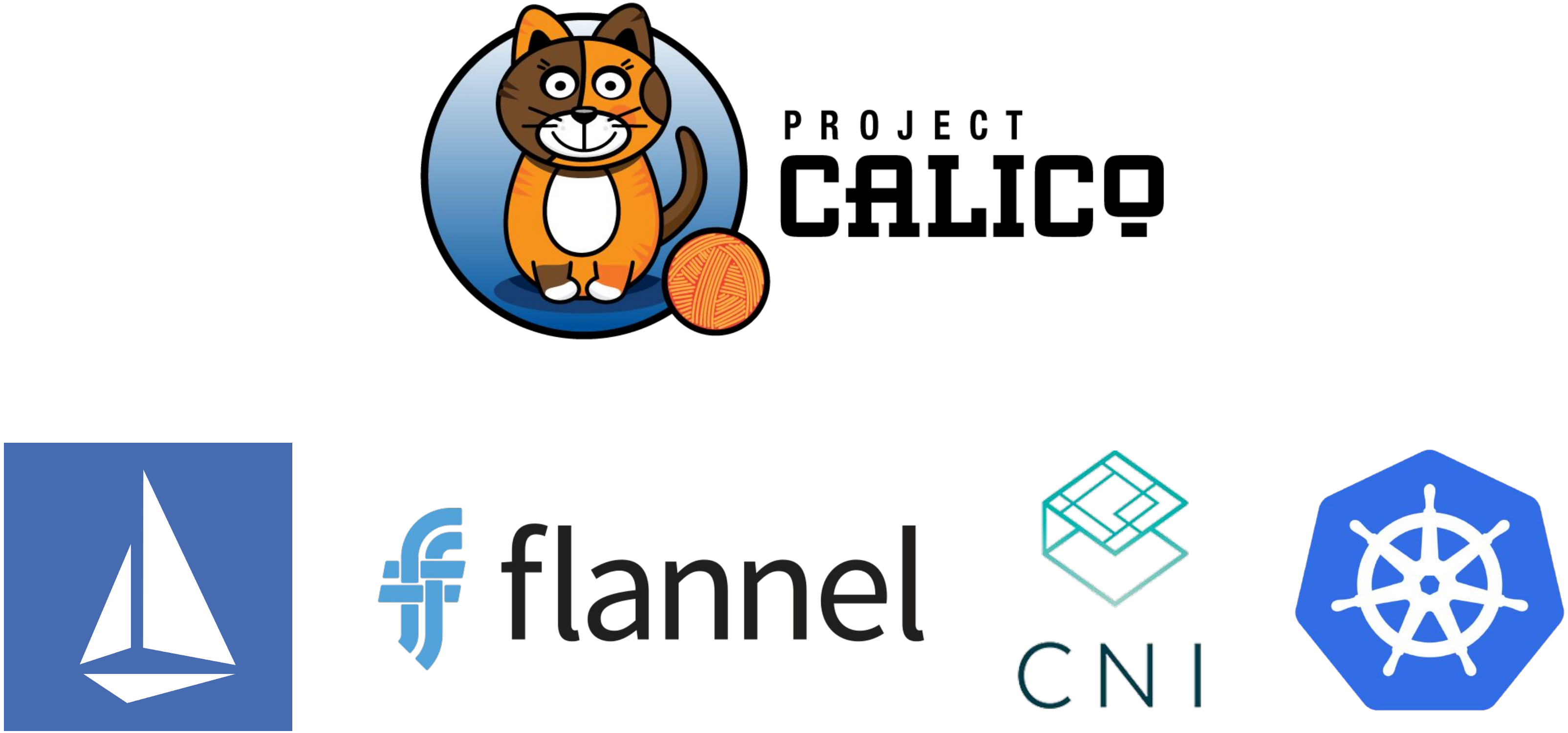
ZERO TRUST KUBERNETES NETWORKS

SPIKE CURTIS

TIGERA

What do we do?



What do we do?

Google Cloud Platform

aws

Azure

IBM Cloud

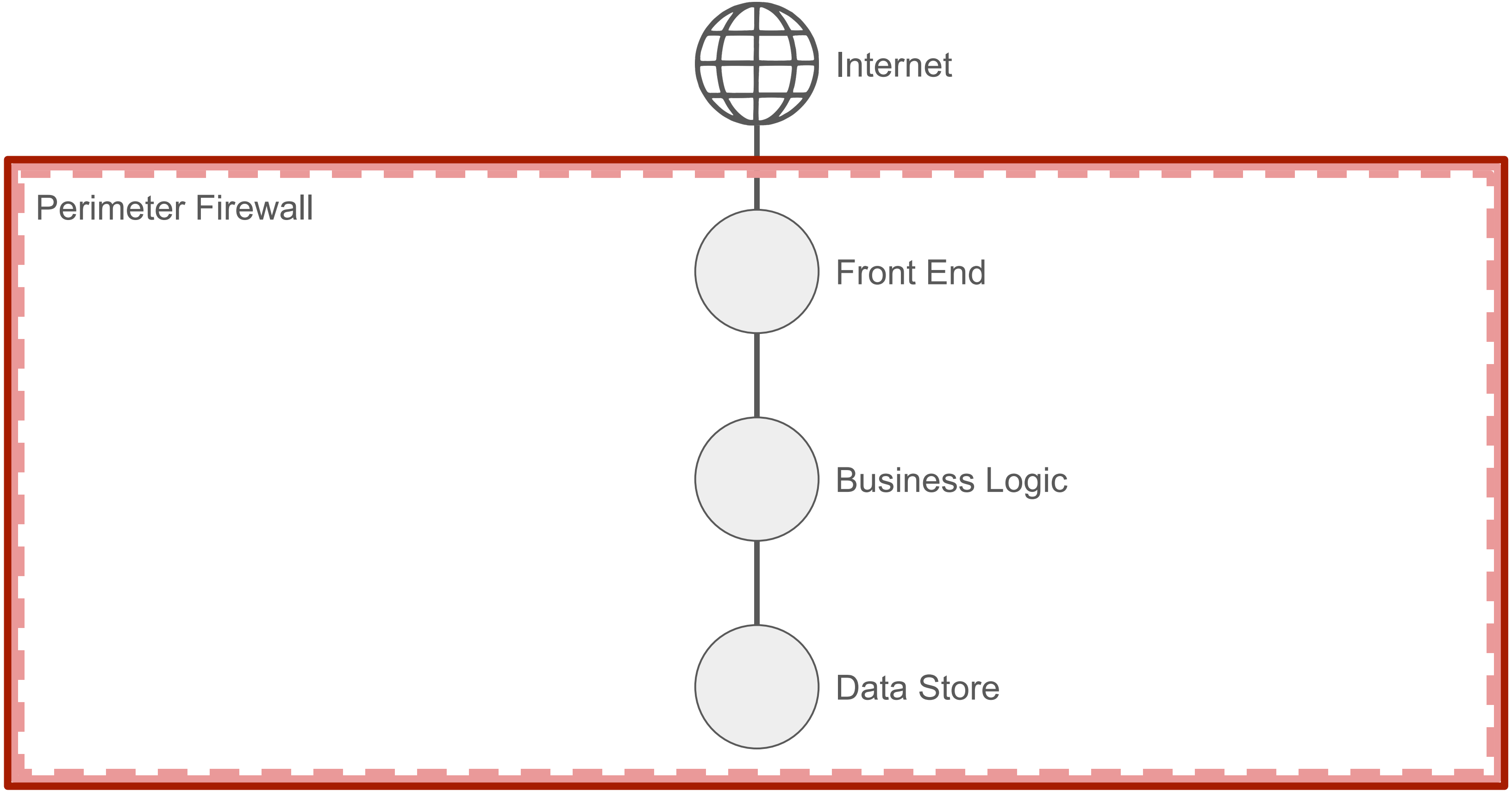
Why?

Secure Application Connectivity

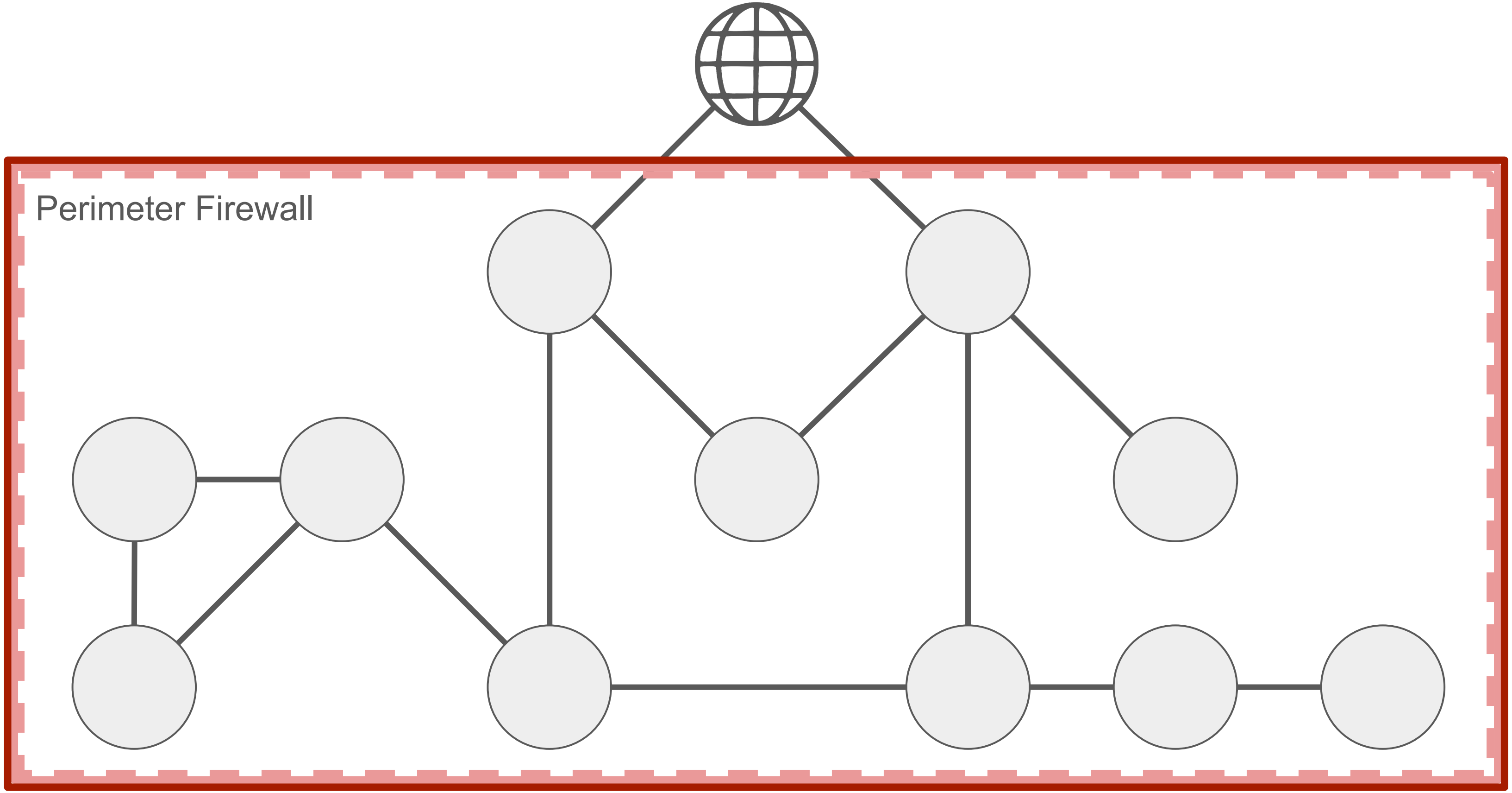
for the

Cloud Native World

The evolution of secure application connectivity

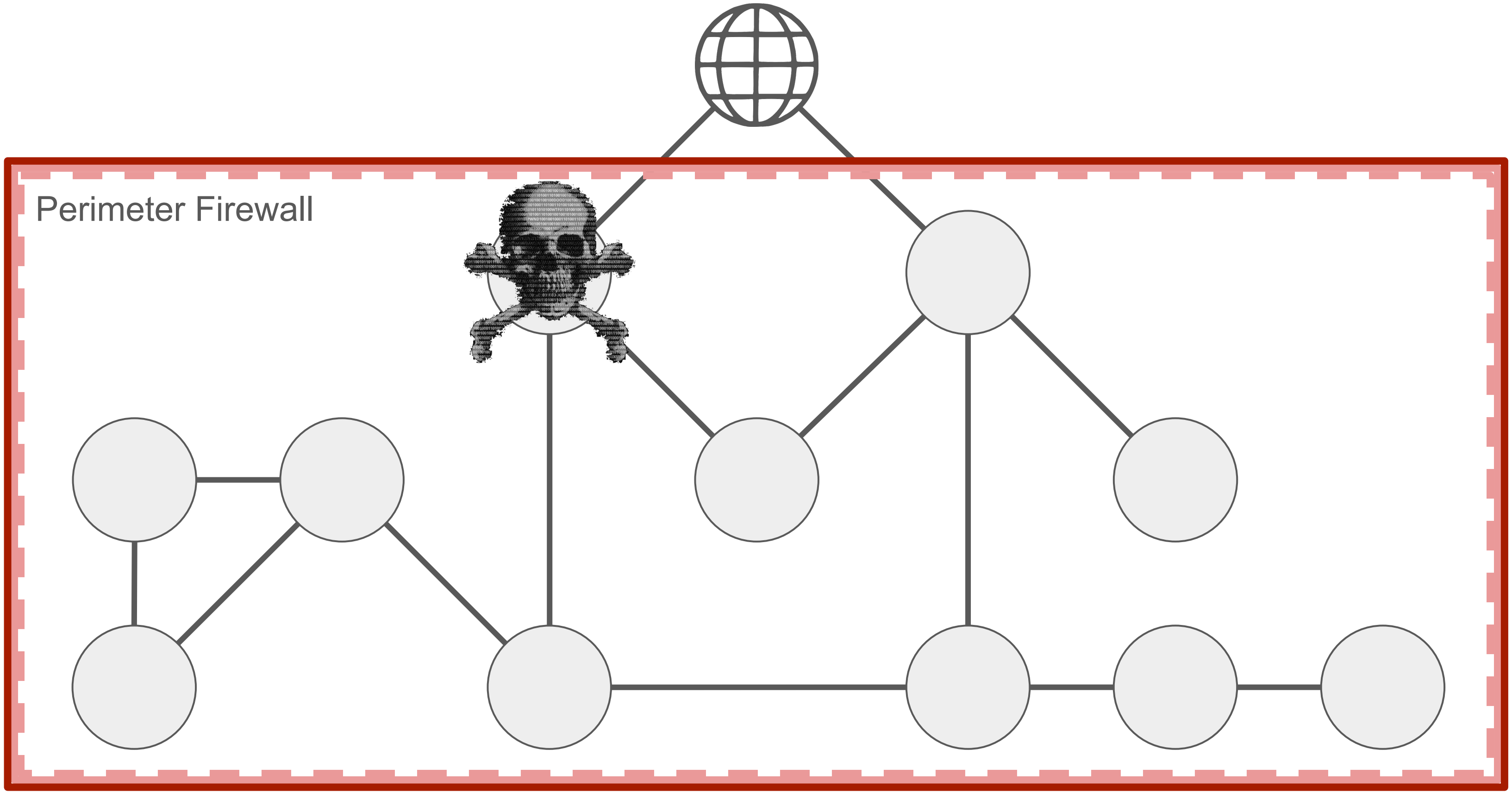


The evolution of secure application connectivity

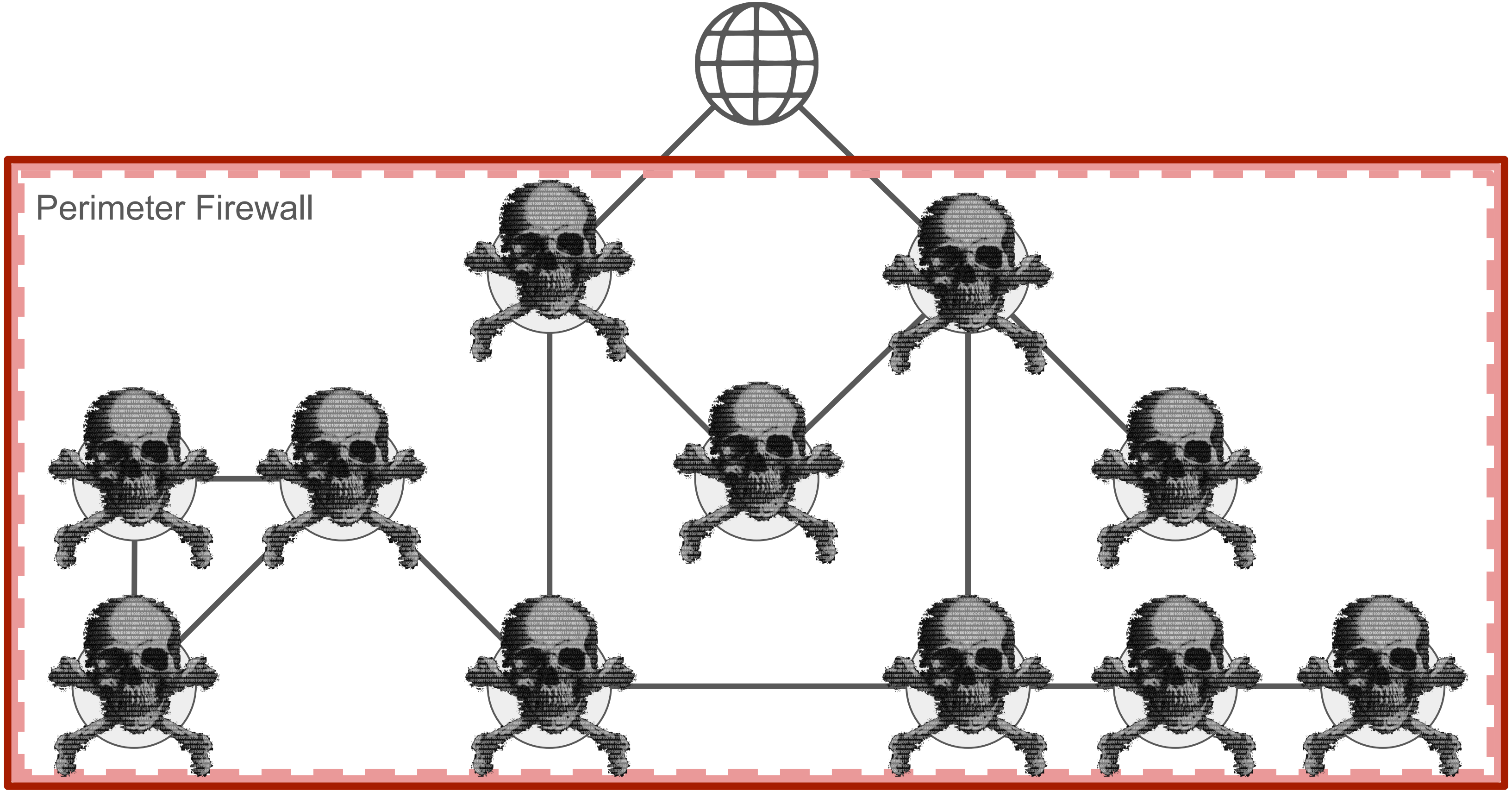


DOOD
LOL
XXORS
WTF
PWND
SUXS

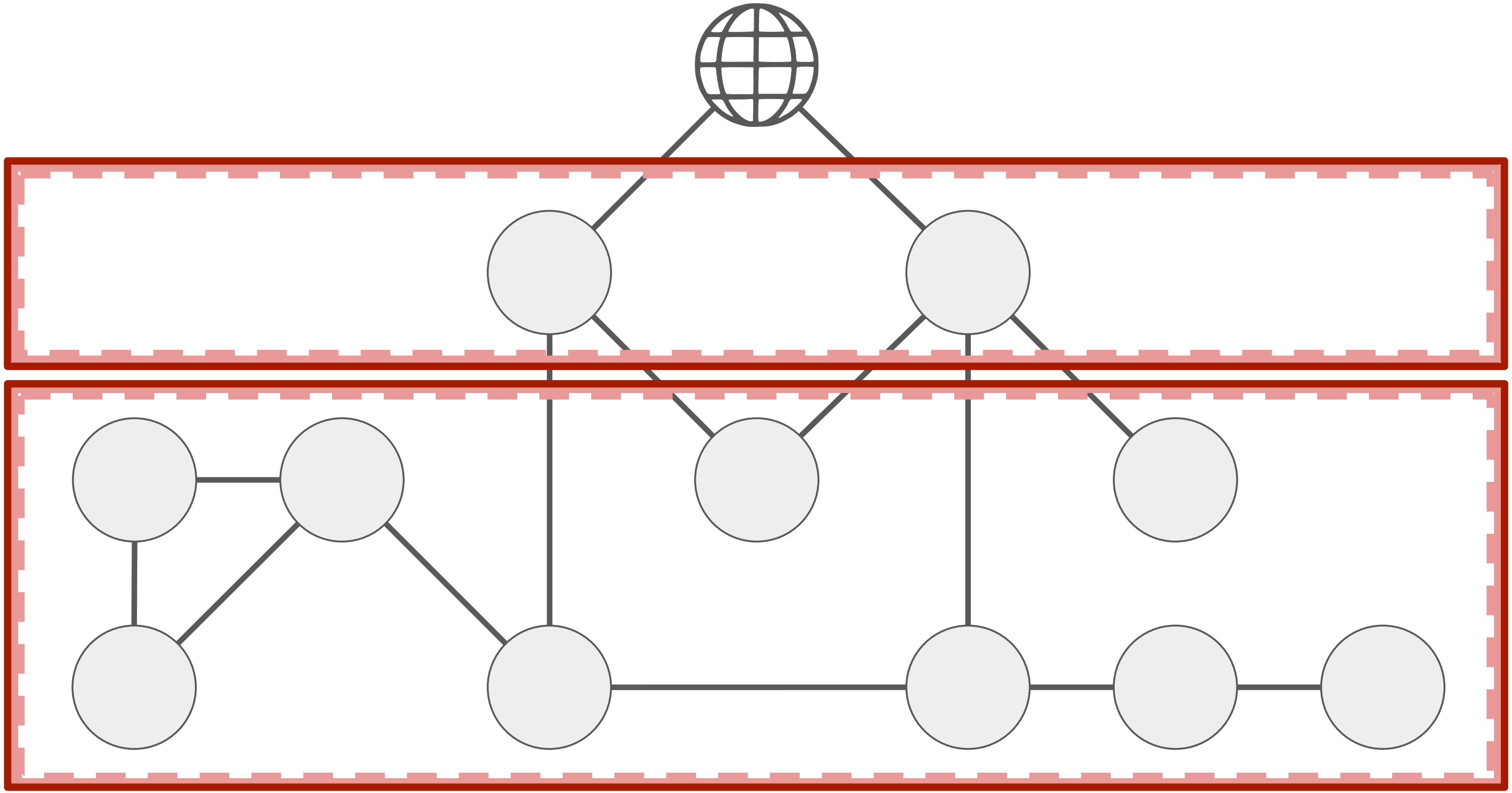
The evolution of secure application connectivity



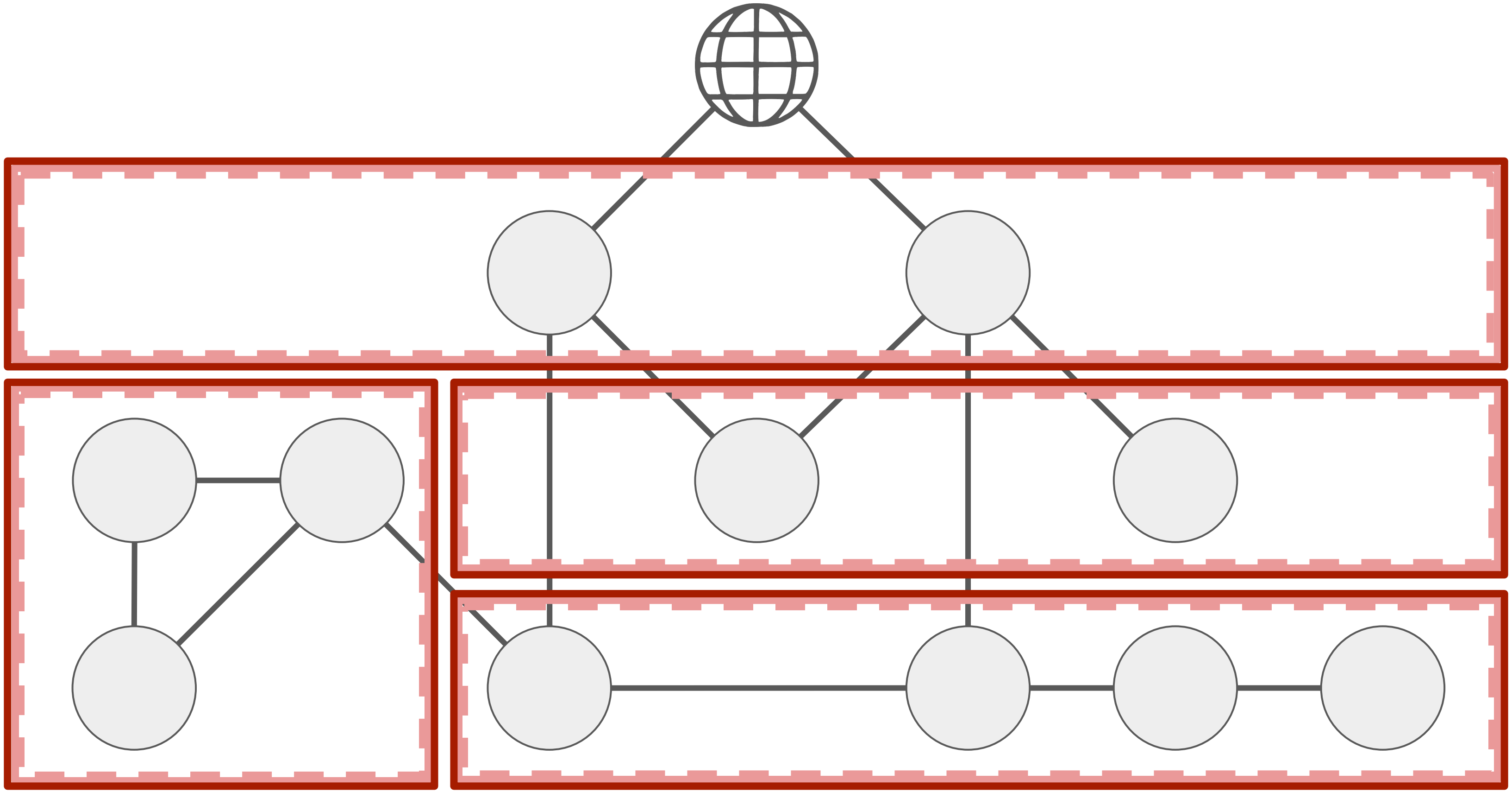
The evolution of secure application connectivity



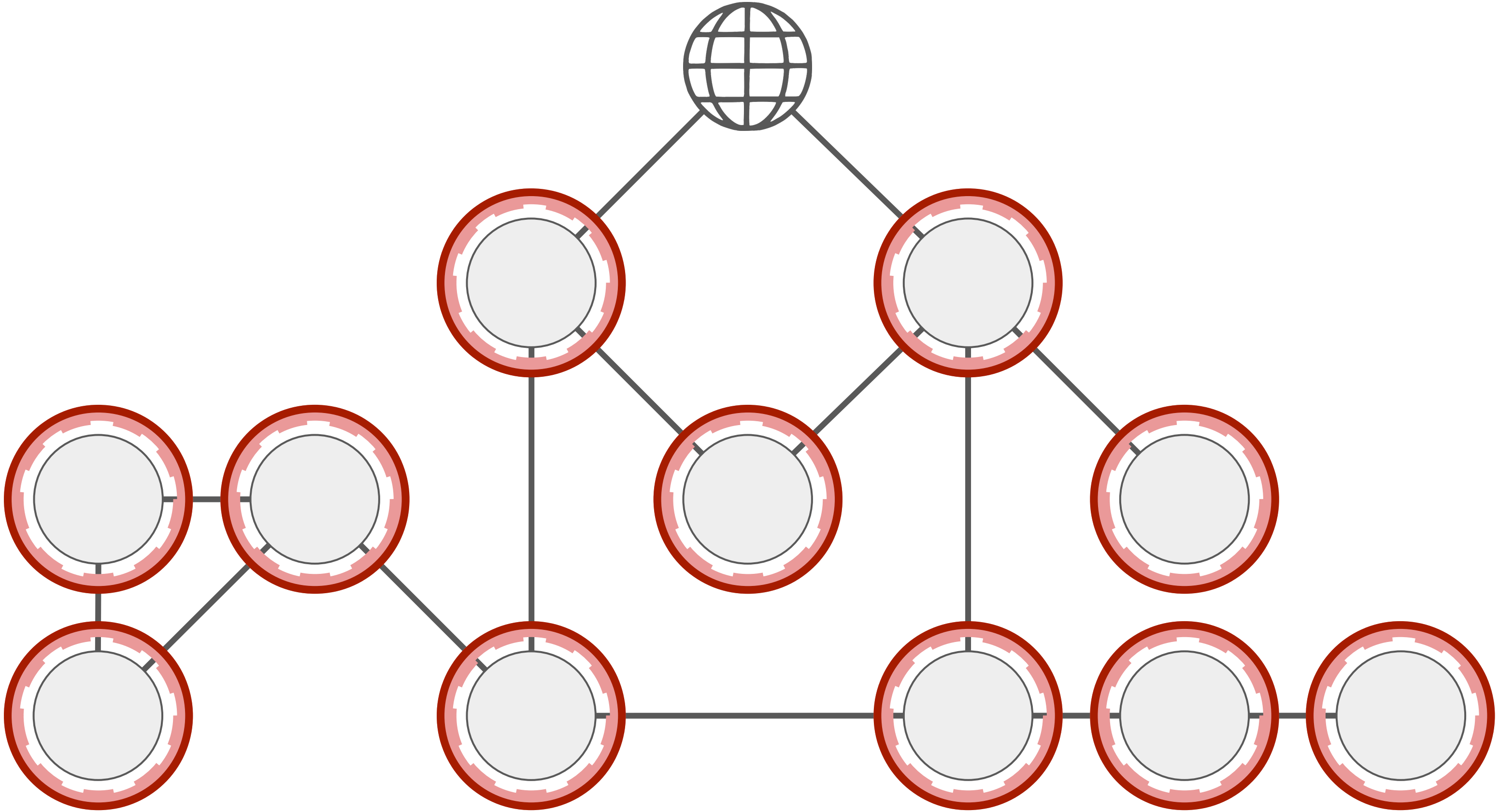
The evolution of secure application connectivity



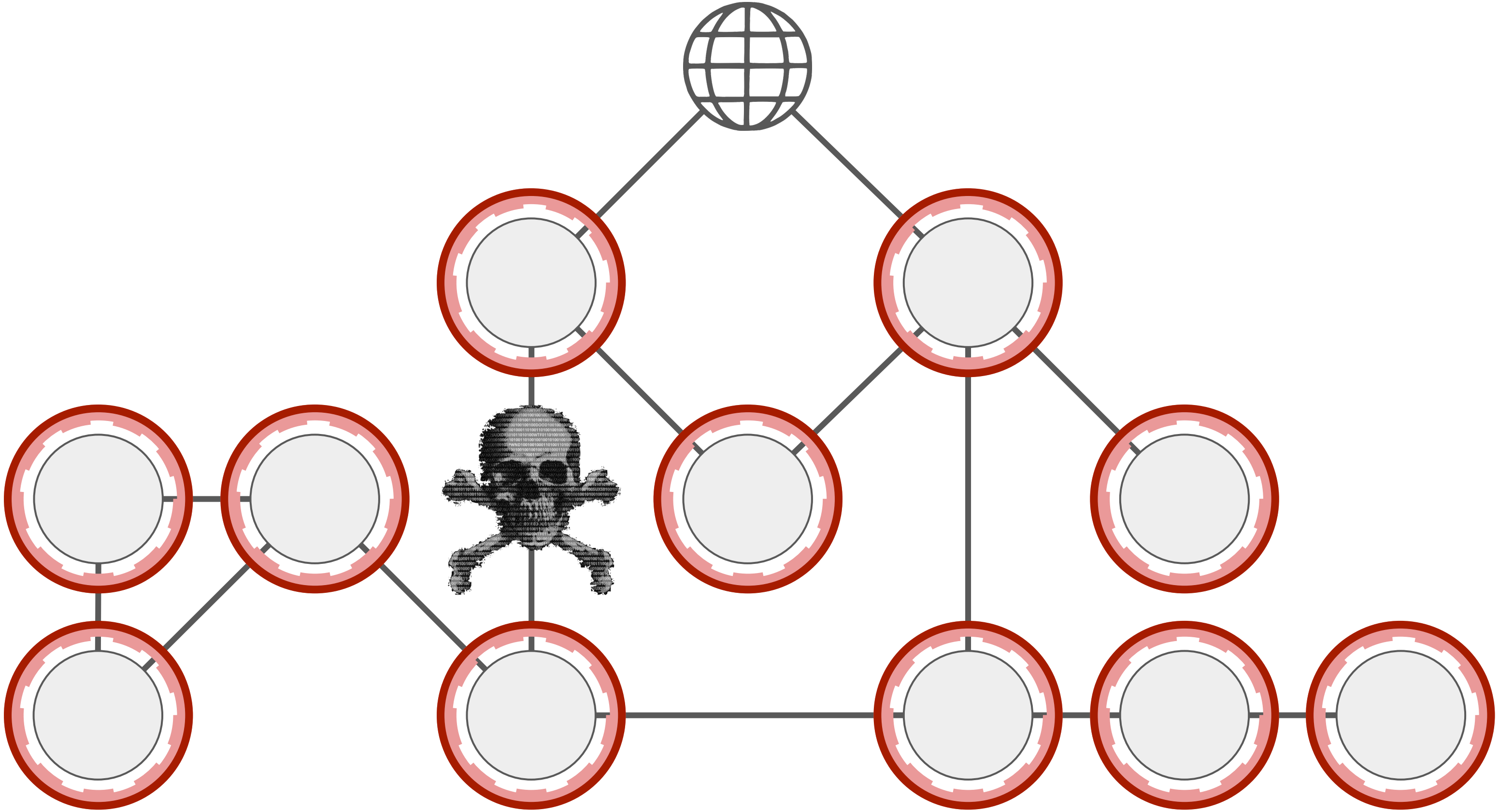
The evolution of secure application connectivity



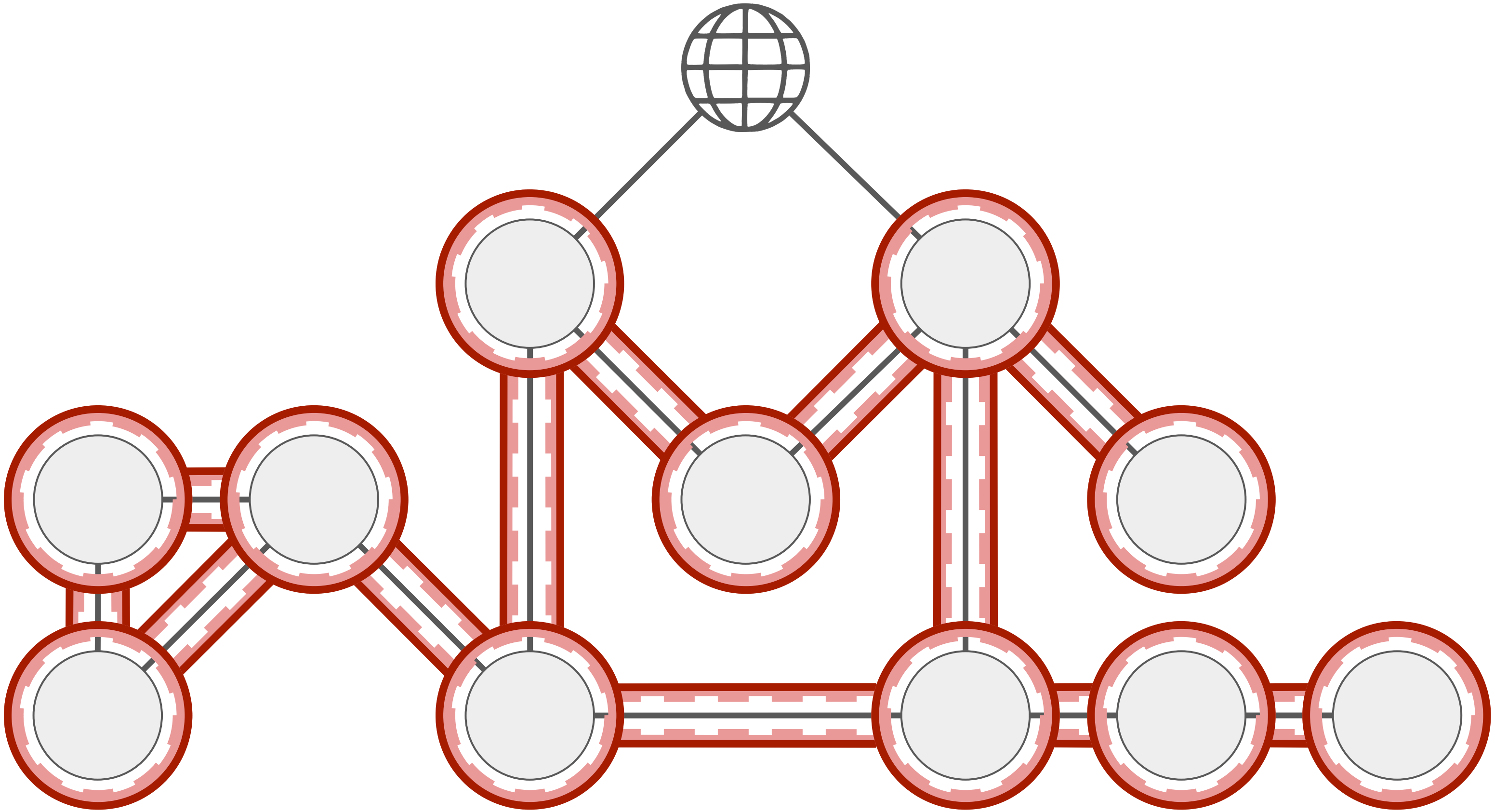
The evolution of secure application connectivity



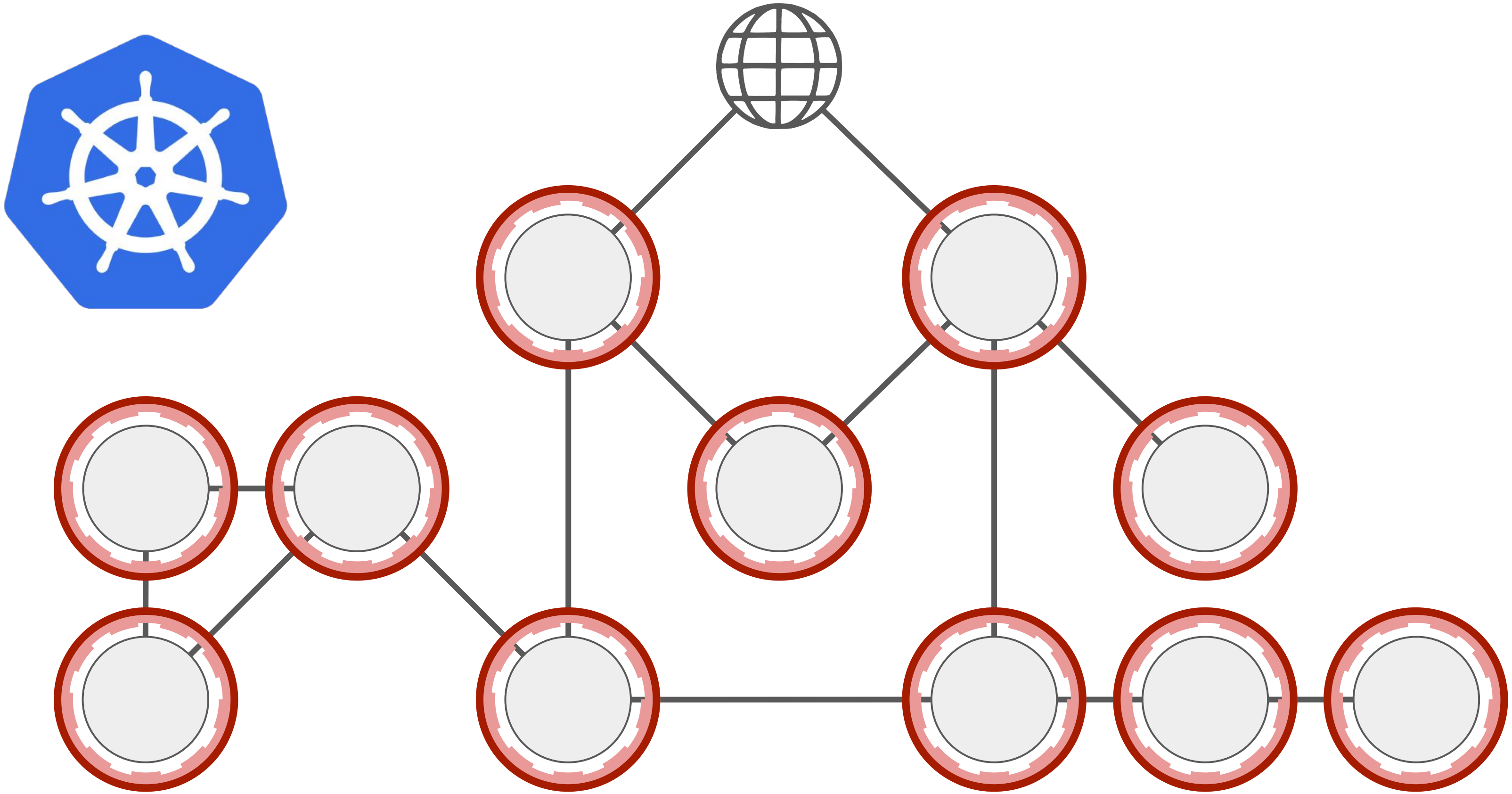
The evolution of secure application connectivity



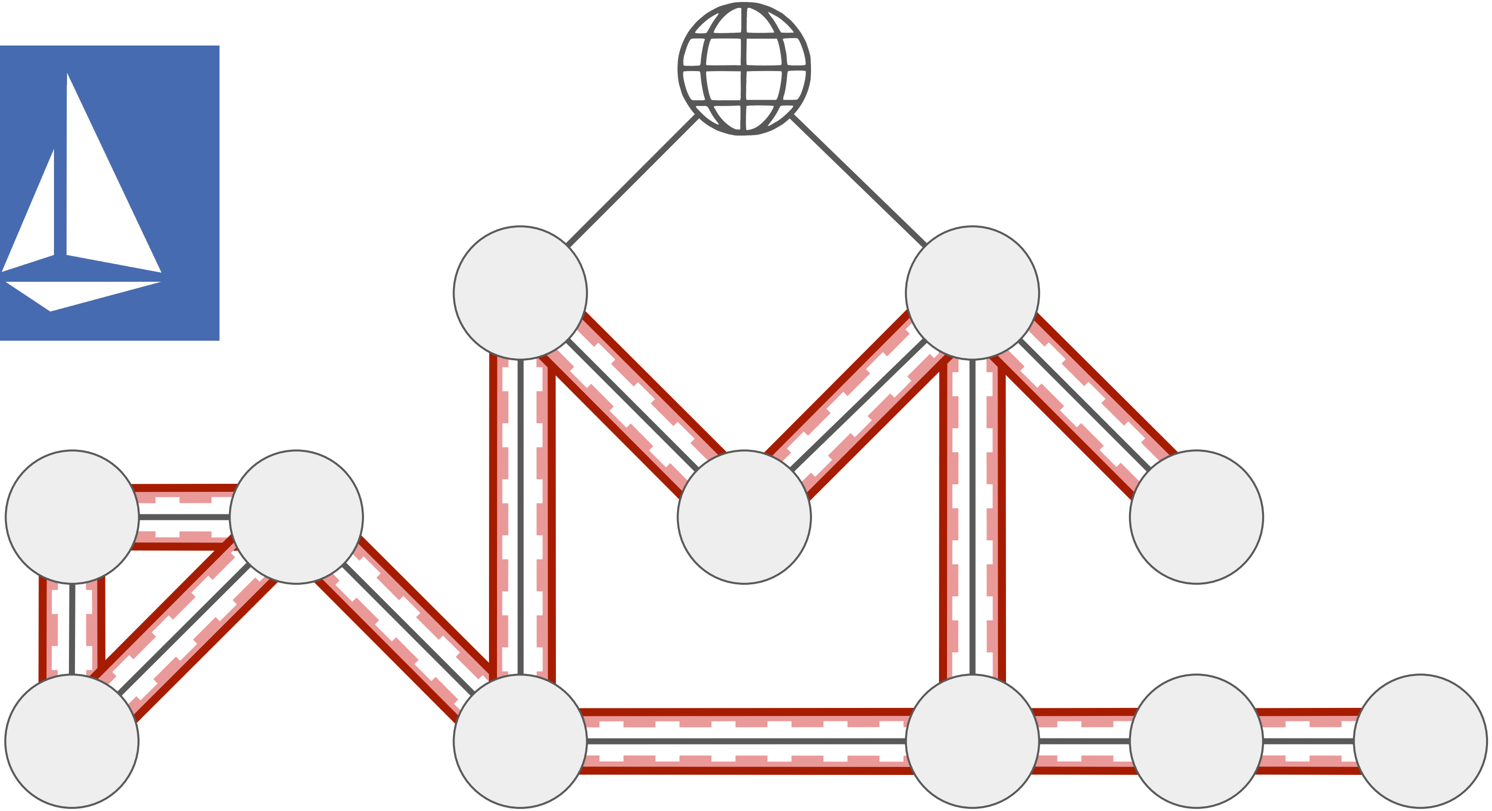
The evolution of secure application connectivity



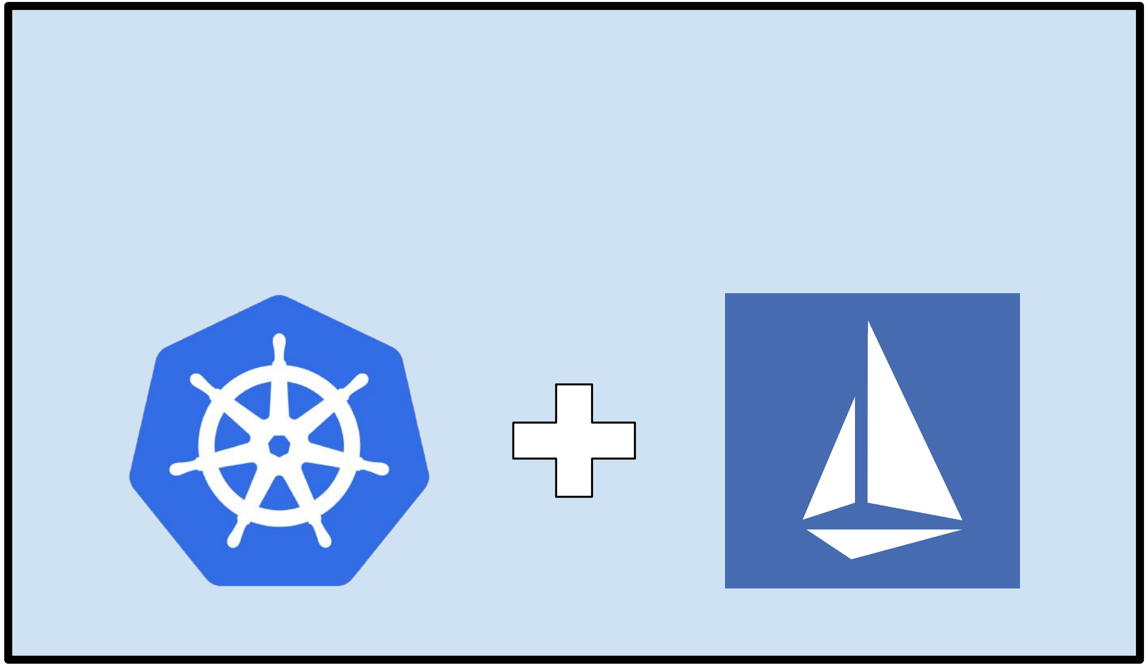
Kubernetes Network Policy



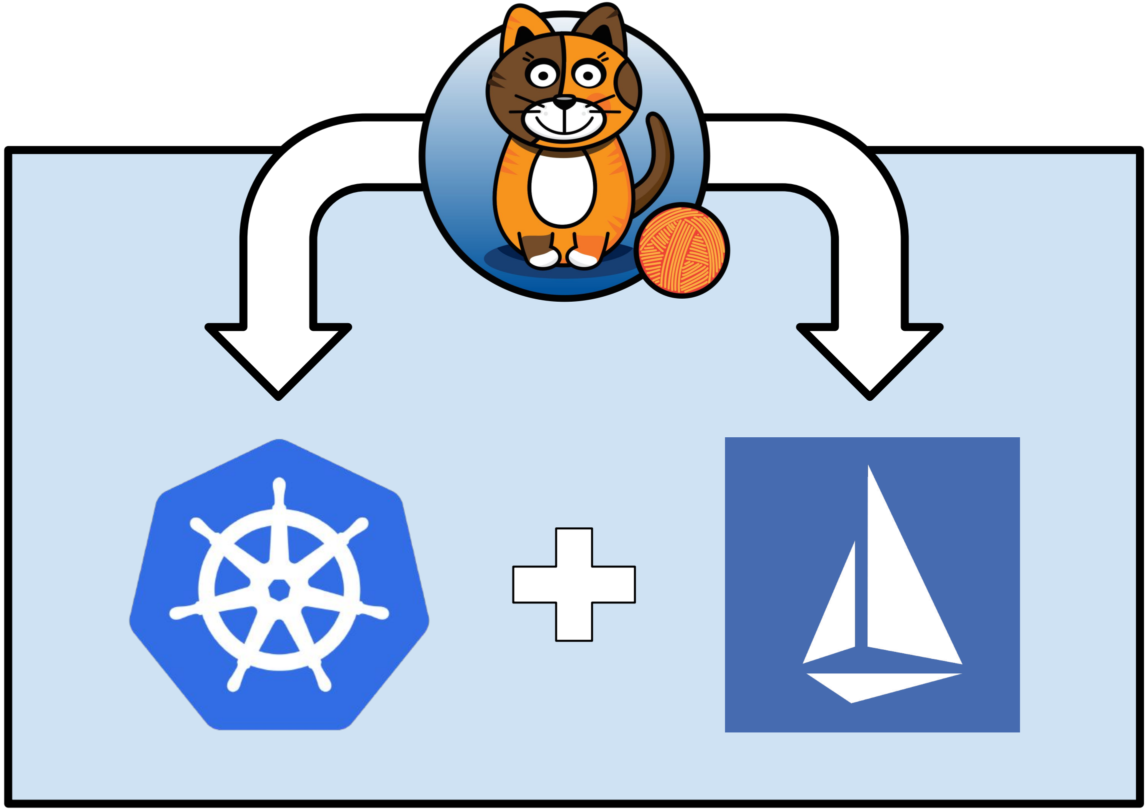
Istio Service Mesh



Kubernetes + Istio the hard way?



Unified Policy for Secure Application Connectivity



Calico Policy

```yaml
apiVersion: v1
kind: policy
metadata:
  name: summary
spec:
  selector: app == "summary"
  ingress:
    - action: allow
      source:
        serviceAccounts:
          names: ["customer"]
      http:
        methods: ["GET"]
```

Label selector: specifies which pods to apply the policy to

Calico Policy

```
apiVersion: v1
kind: policy
metadata:
  name: summary
spec:
  selector: app == "summary"
  ingress:
    - action: allow
      source:
        serviceAccounts:
          names: ["customer"]
      http:
        methods: ["GET"]
```

Label, namespace, or serviceAccount selectors: specifies allowed connections

Calico Policy

```
apiVersion: v1
kind: policy
metadata:
  name: summary
spec:
  selector: app == "summary"
  ingress:
    - action: allow
      source:
        serviceAccounts:
          names: ["customer"]
      http:
        methods: ["GET"]
```

Protocol, method and path selectors: specifies allowed application layer requests

Zero Trust Network Model

- The network is always assumed to be hostile
- External and internal threats exist on the network at all times
- Network locality is not sufficient for deciding trust
- Every device, user, and network flow is authenticated and authorized
- Policies must be dynamic and calculated from as many sources of data as possible

Zero Trust Networks by Evan Gilman & Doug Barth

Check it out!

Available today in open source:

`github.com/projectcalico/app-policy`

Istio: Sailing to a Secure Services Mesh

Friday 11:55am Ballroom A

Do you need?

- > Zero trust security
- > Multi-cloud & legacy
- > Enterprise control & compliance
- > Operational simplicity

Check out:

Tigera CNX

Find us at the Tigera booth

or

`https://tigera.io/cnx`

TIGERA