

KubeCon



CloudNativeCon

Europe 2019



KubeCon



CloudNativeCon

Europe 2019

Reinventing Networking

A Deep Dive into Istio's Multicluster Gateways

Steve Dake (@steven_dake) - Independent

What is an Istio Service Mesh?

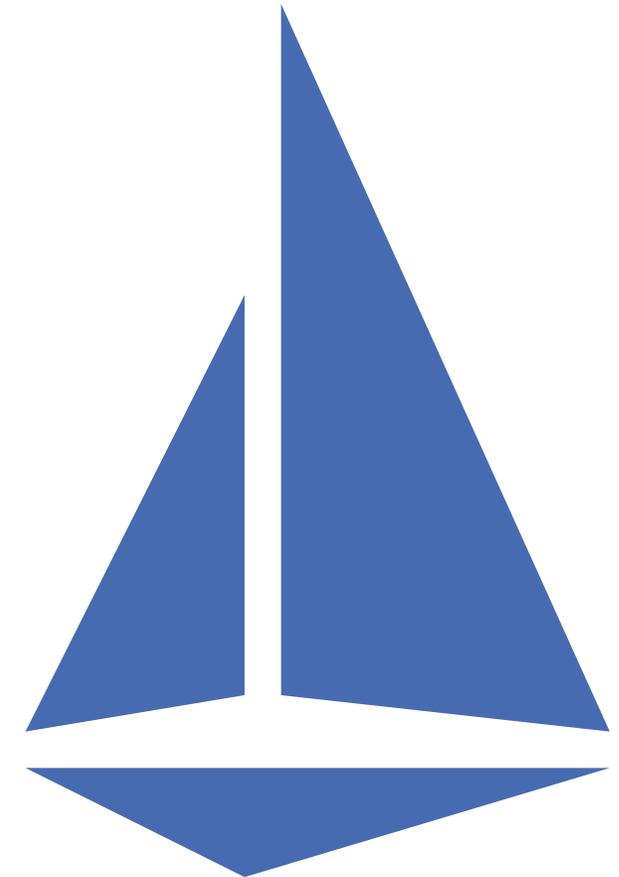
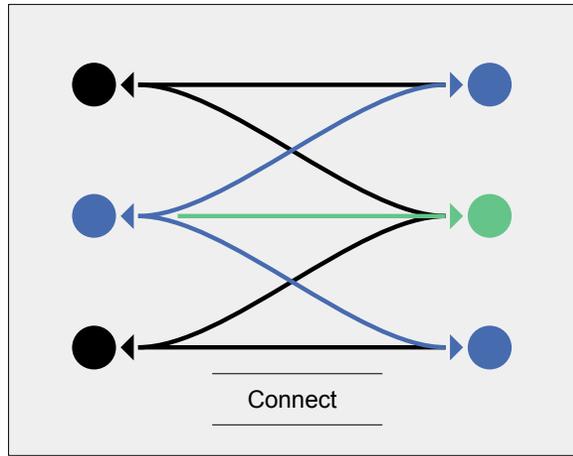


KubeCon



CloudNativeCon

Europe 2019



Connect

What is an Istio Service Mesh?

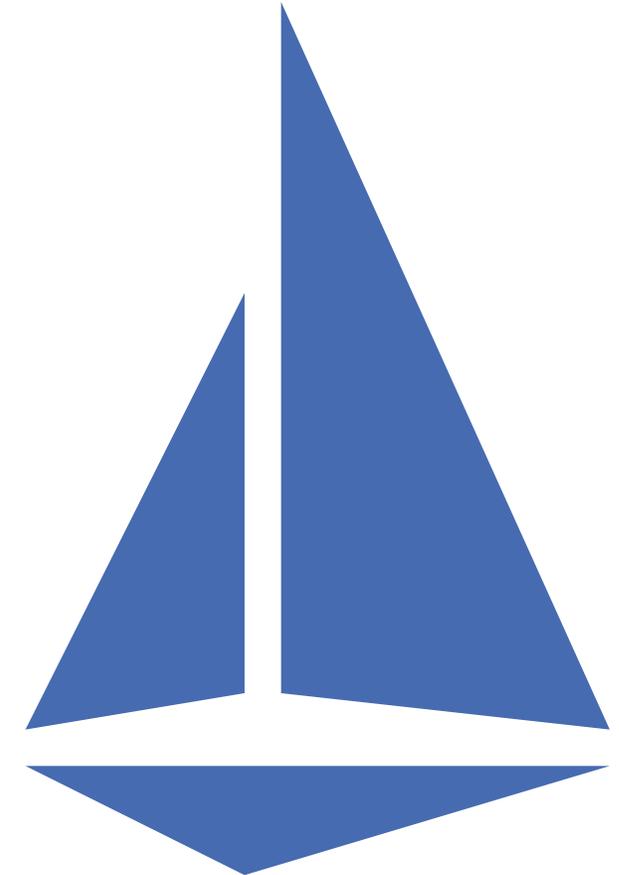
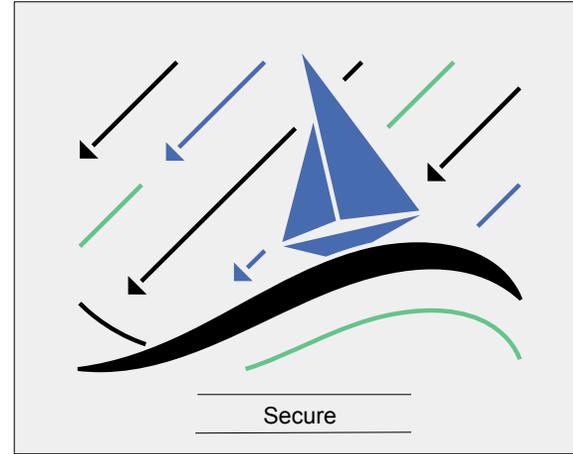
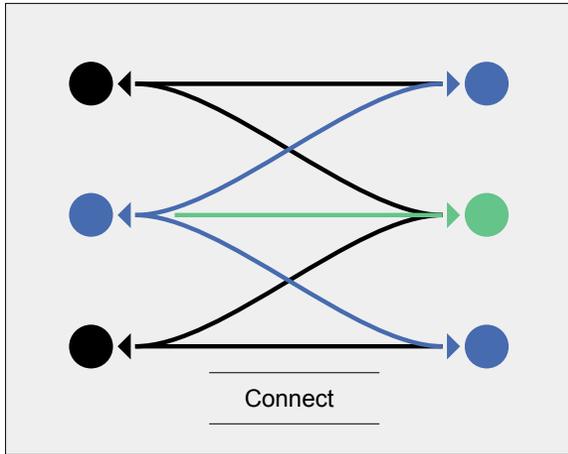


KubeCon



CloudNativeCon

Europe 2019



Connect, Secure

What is an Istio Service Mesh?

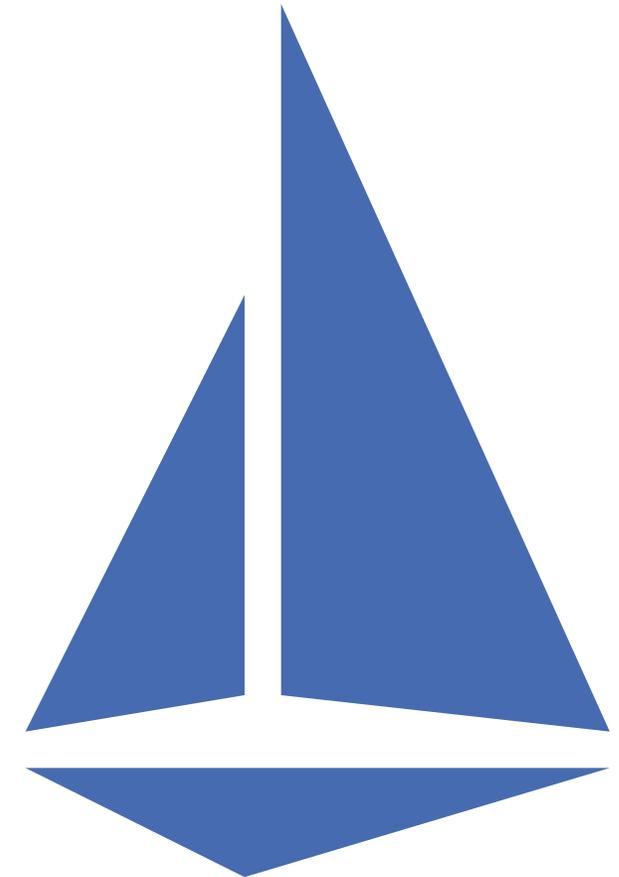
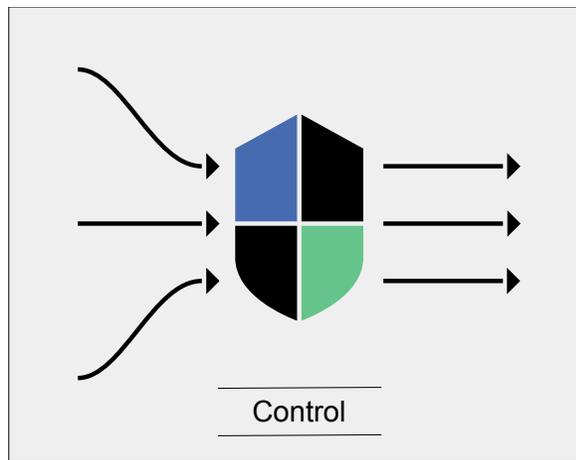
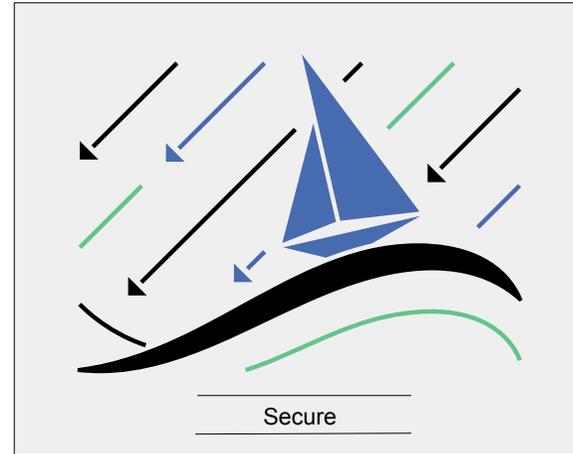
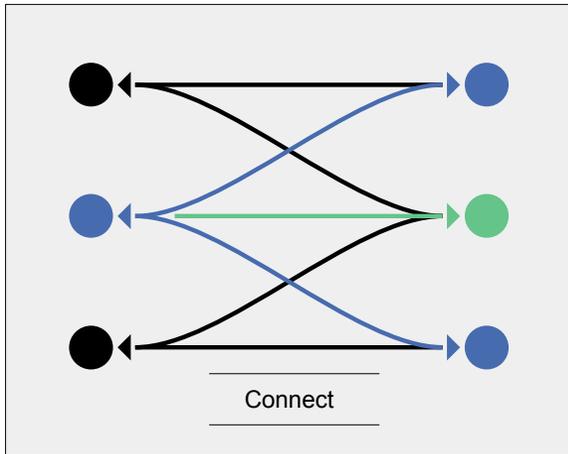


KubeCon



CloudNativeCon

Europe 2019



Connect, Secure, Control

What is an Istio Service Mesh?

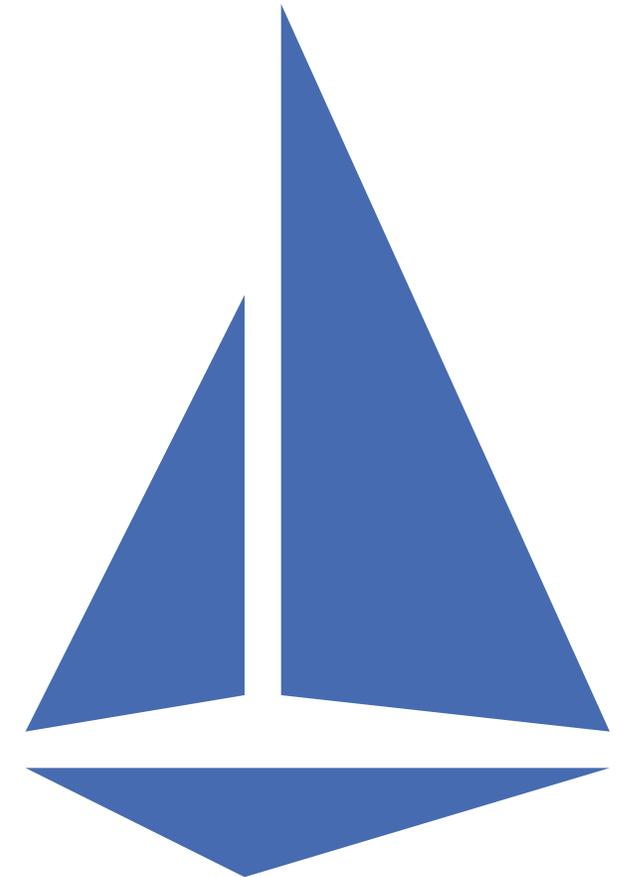
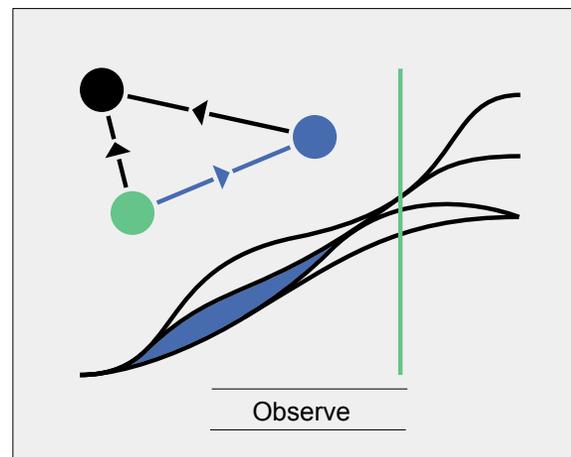
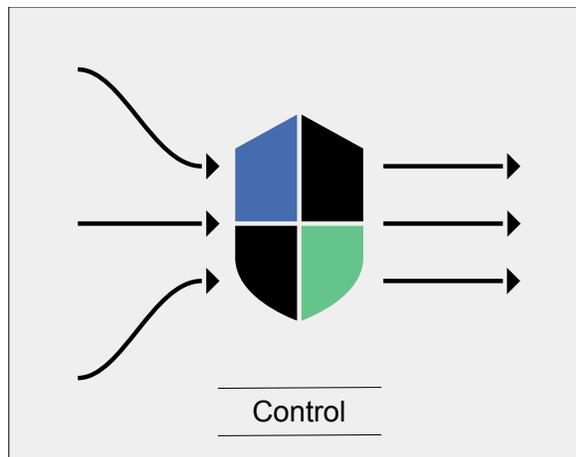
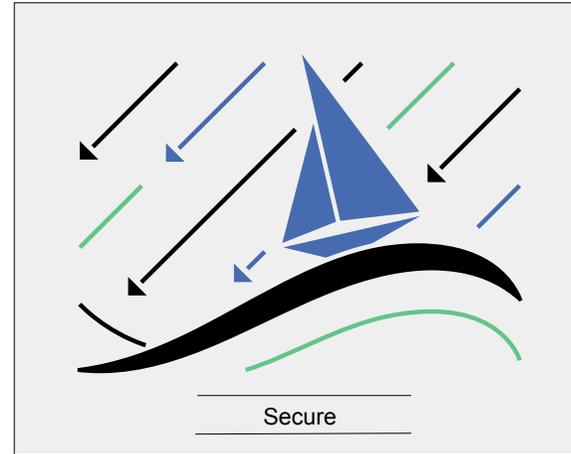
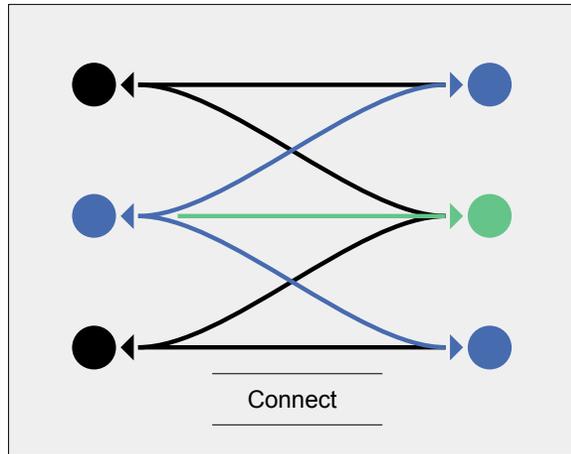


KubeCon



CloudNativeCon

Europe 2019



Connect, Secure, Control, and Observe services.

Evolution of Traditional Networking



KubeCon



CloudNativeCon

Europe 2019

In the beginning...

Platform

Evolution of Traditional Networking



KubeCon



CloudNativeCon

Europe 2019



Leonard Kleinrock
Distinguished Professor
[UCLA Computer Science Department](#)

Evolution of Traditional Networking



KubeCon



CloudNativeCon

Europe 2019



Precursor to the Internet Born on Friday, October 29, 1969, at 10:30 p.m.

Evolution of Traditional Networking



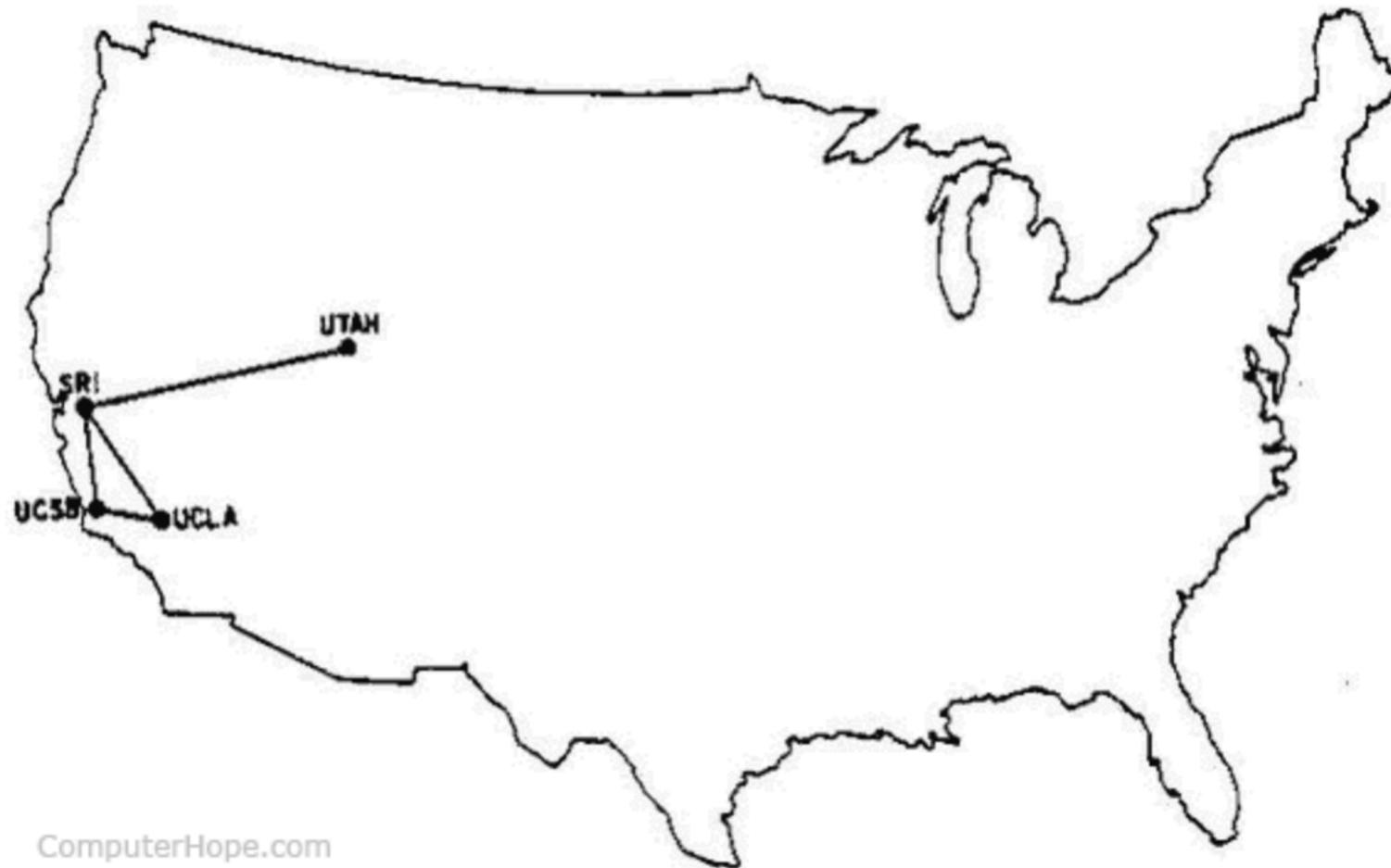
KubeCon



CloudNativeCon

Europe 2019

The entire Internet in 1969



ComputerHope.com

Evolution of Traditional Networking



KubeCon



CloudNativeCon

Europe 2019



Bob Metcalf
3COM Founder

Evolution of Traditional Networking

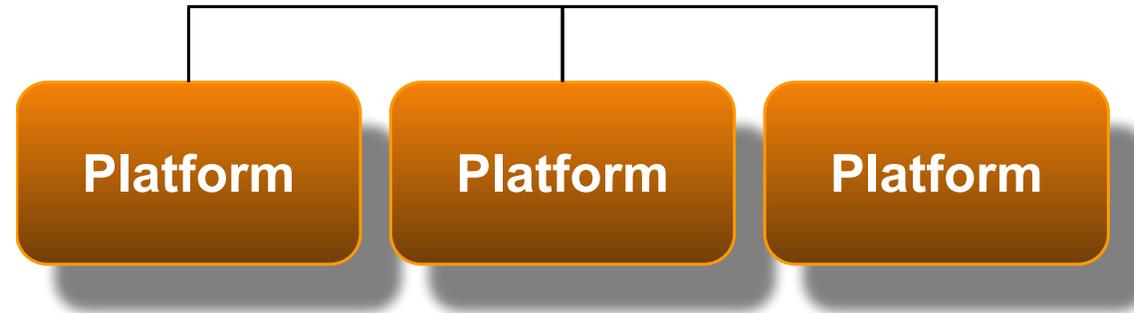


KubeCon



CloudNativeCon

Europe 2019



The LAN is born in 1973.

Evolution of Traditional Networking



KubeCon



CloudNativeCon

Europe 2019



Ginny Strazisar
BBN

Evolution of Traditional Networking

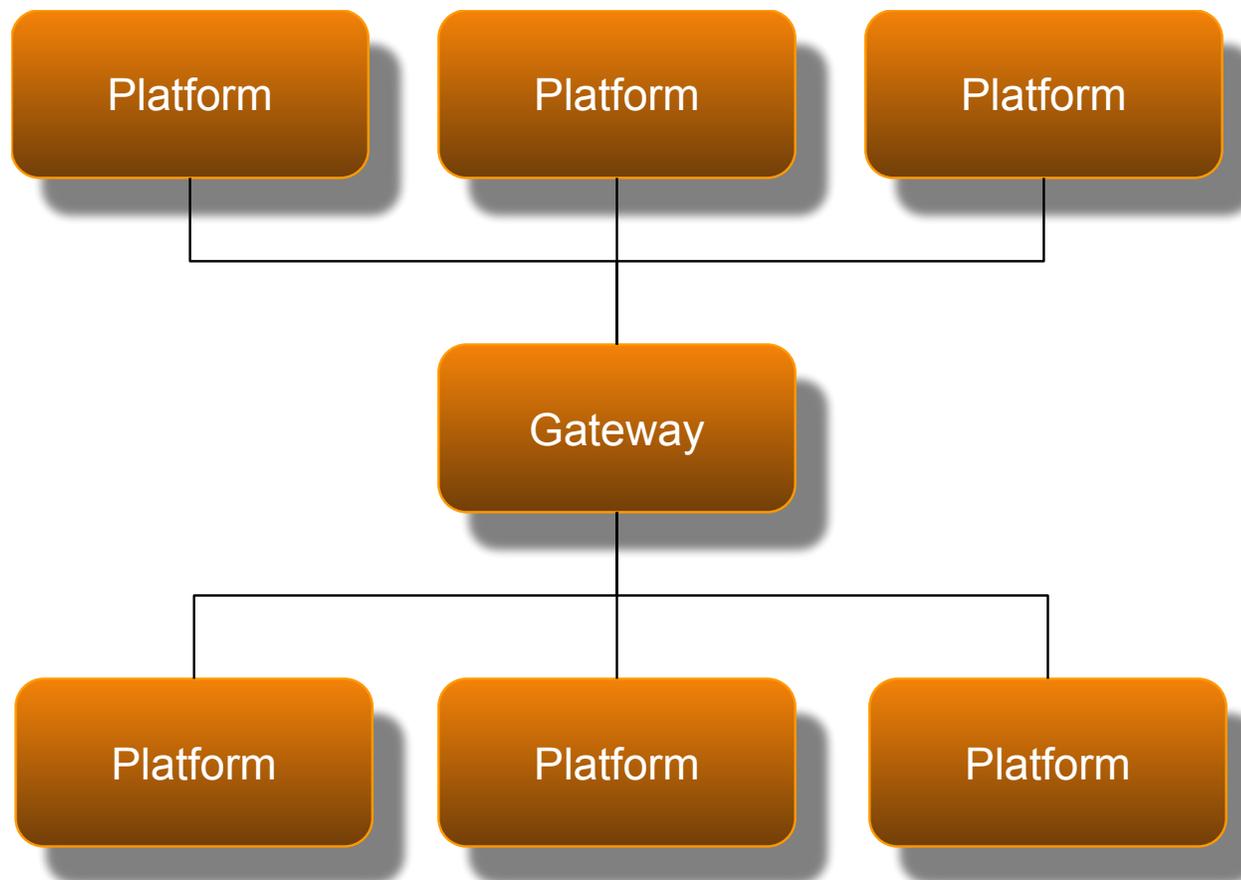


KubeCon



CloudNativeCon

Europe 2019



Reinventing Networking with Istio

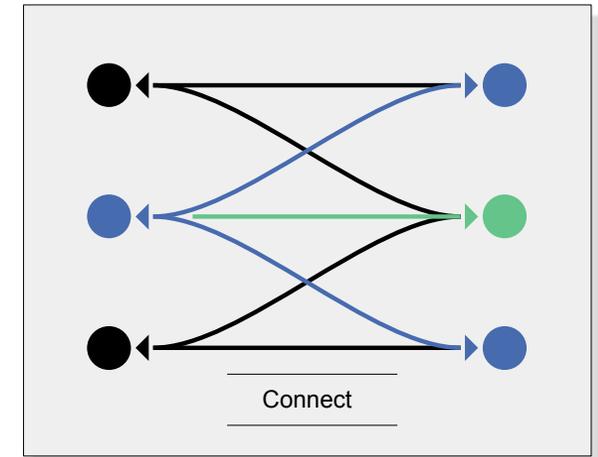
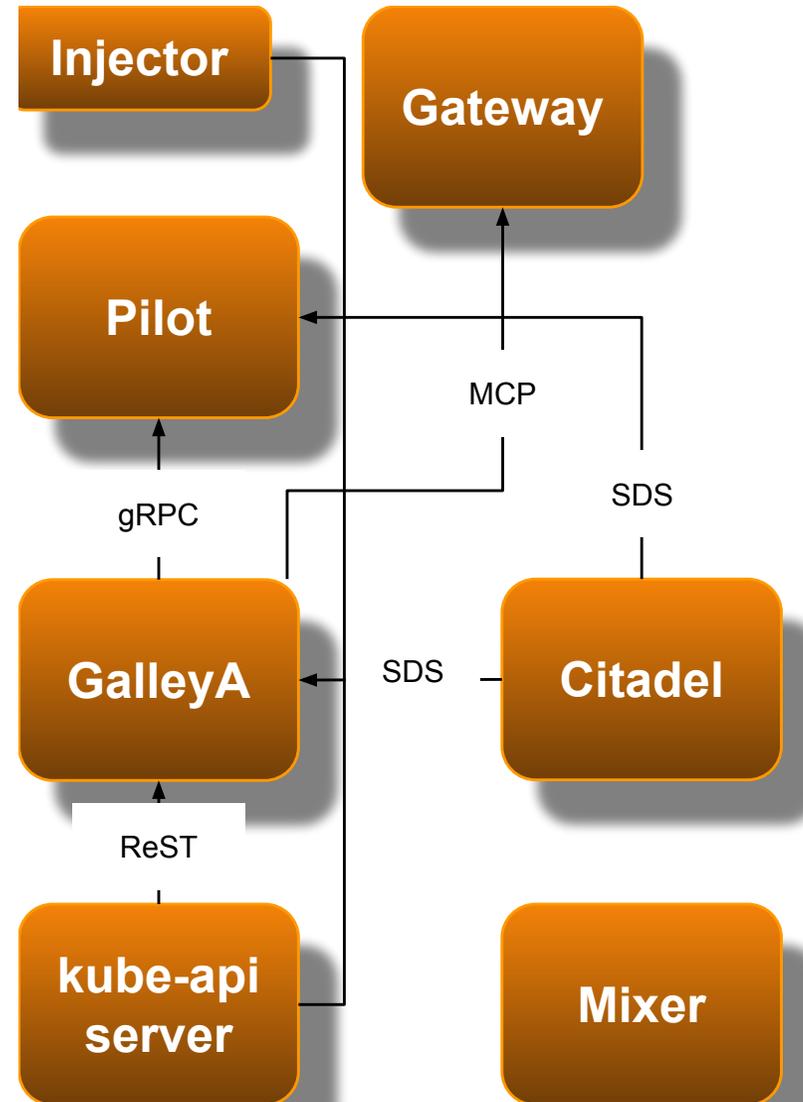


KubeCon



CloudNativeCon

Europe 2019



Reinventing Networking with Istio

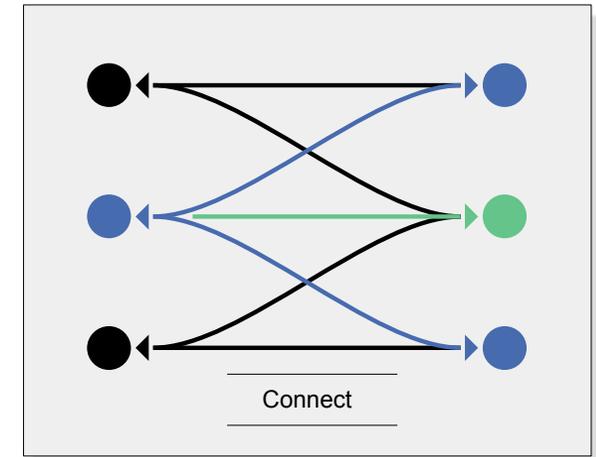
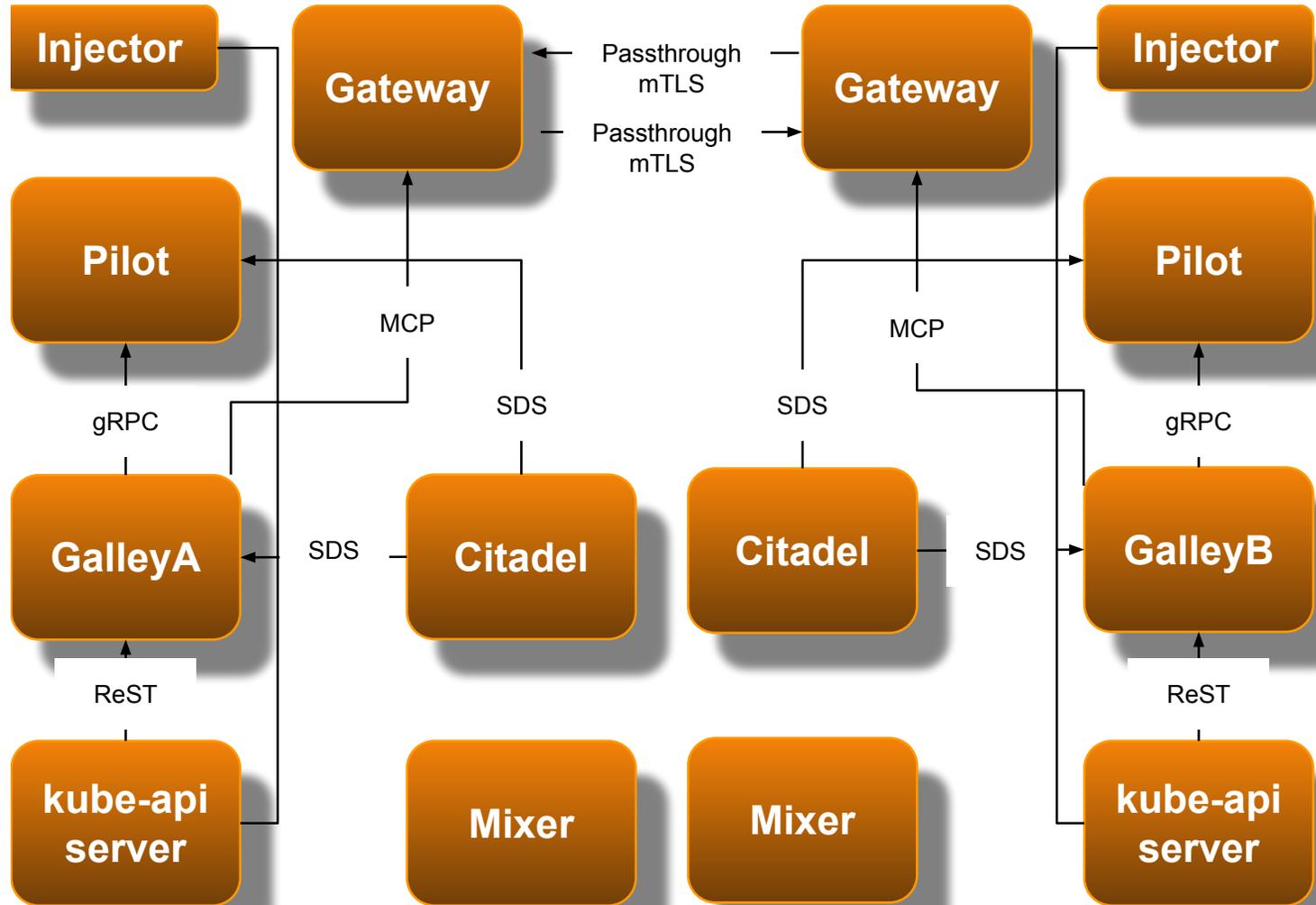


KubeCon



CloudNativeCon

Europe 2019



Reinventing Networking with Istio

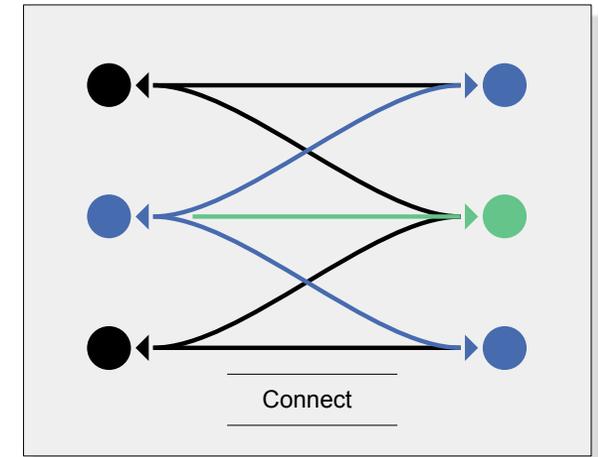
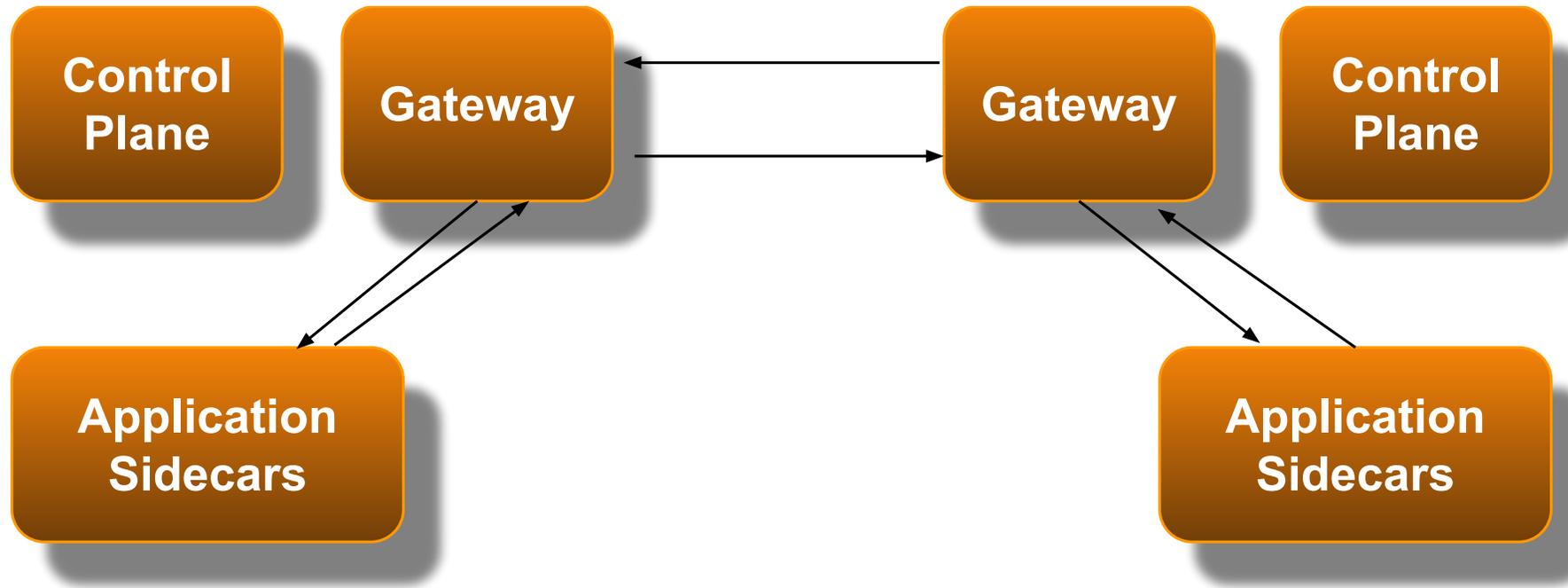


KubeCon



CloudNativeCon

Europe 2019



Reinventing Networking with Istio

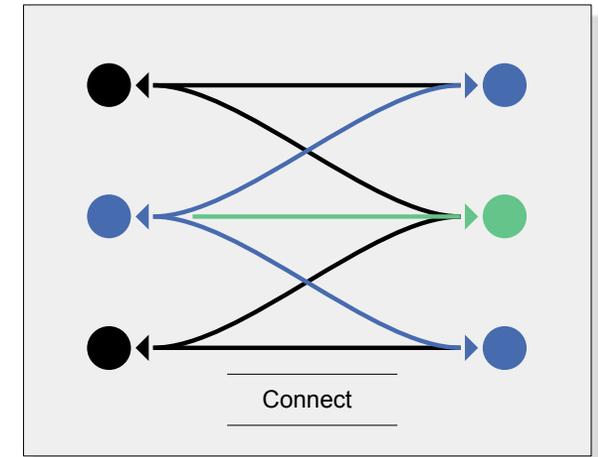
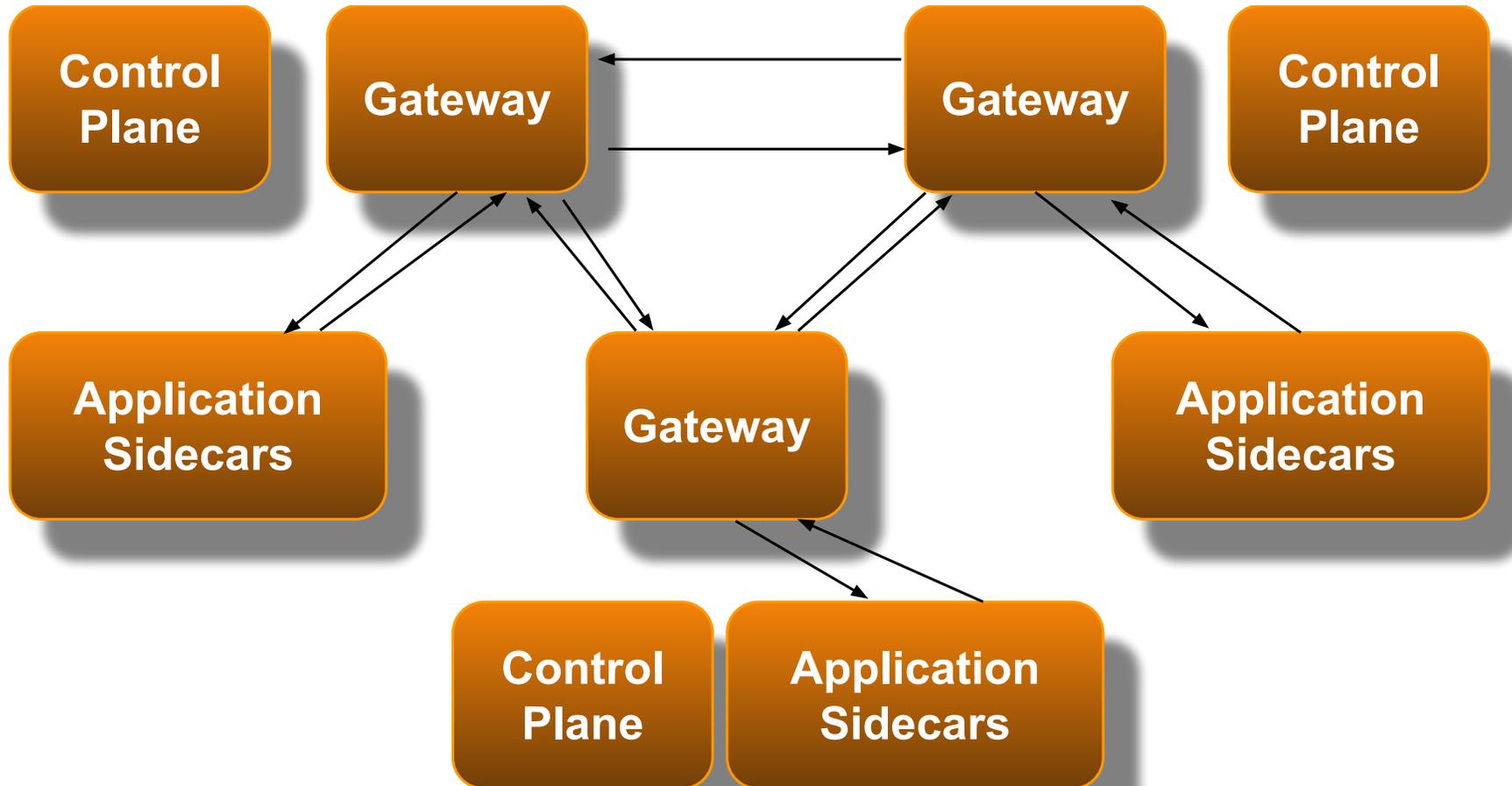


KubeCon



CloudNativeCon

Europe 2019



Reinventing Networking with Istio

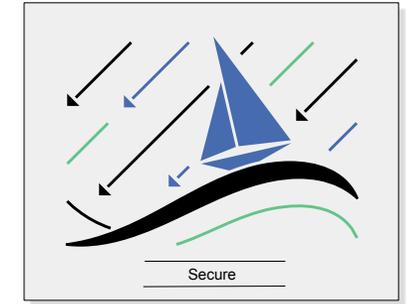
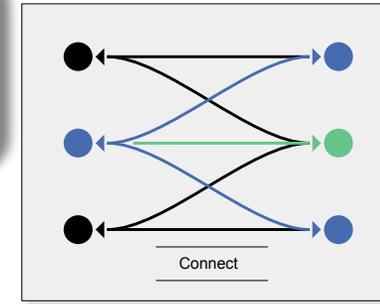
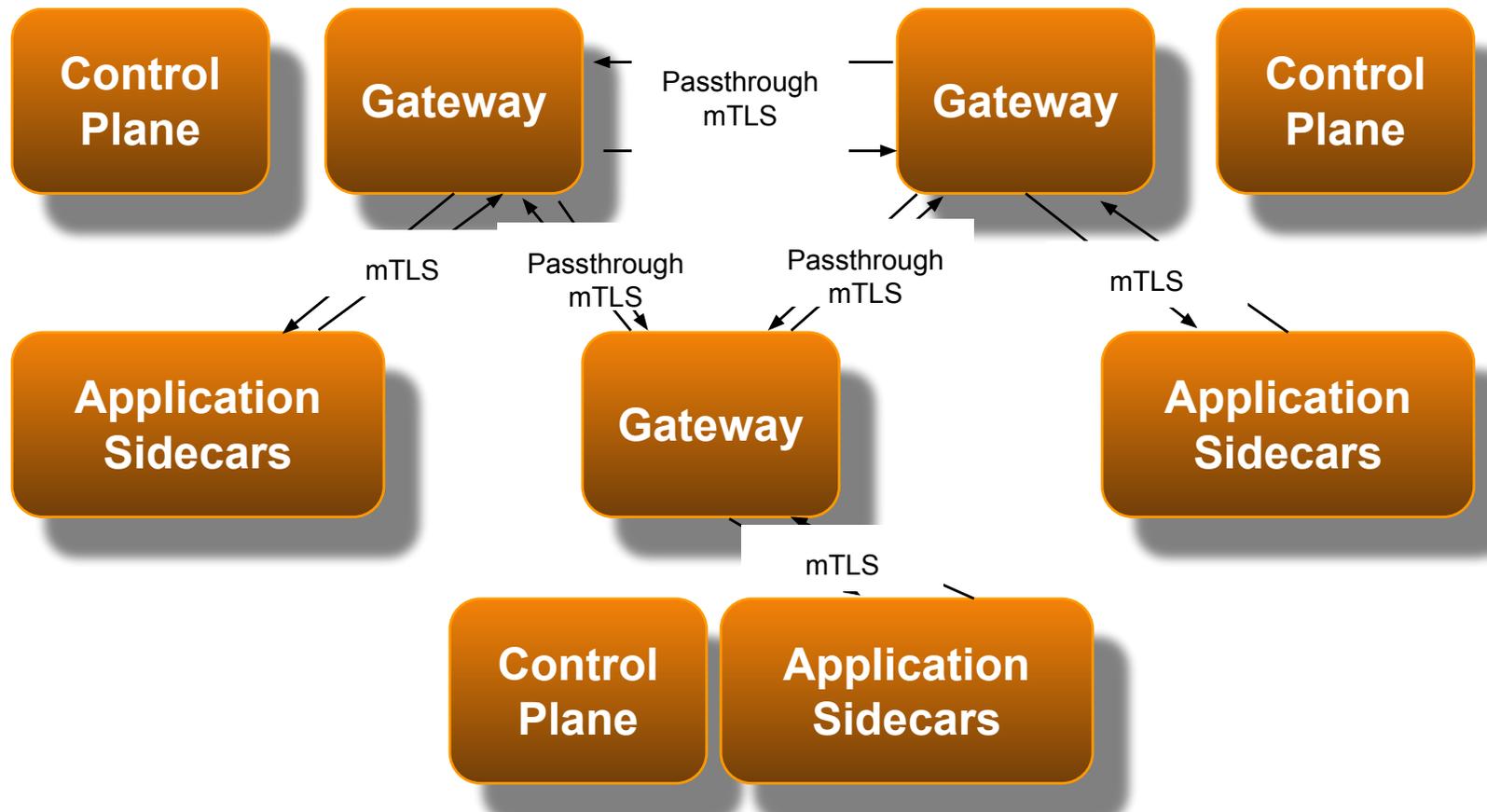


KubeCon



CloudNativeCon

Europe 2019



Reinventing Networking with Istio

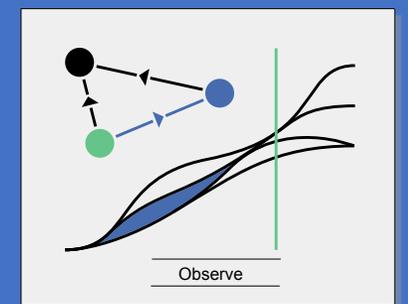
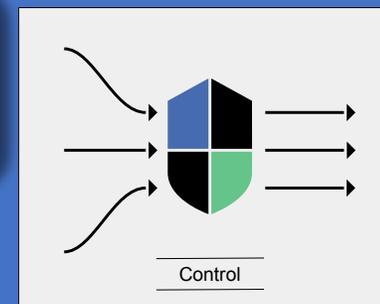
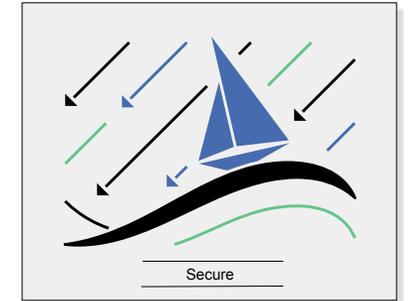
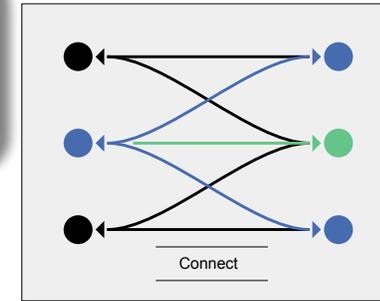
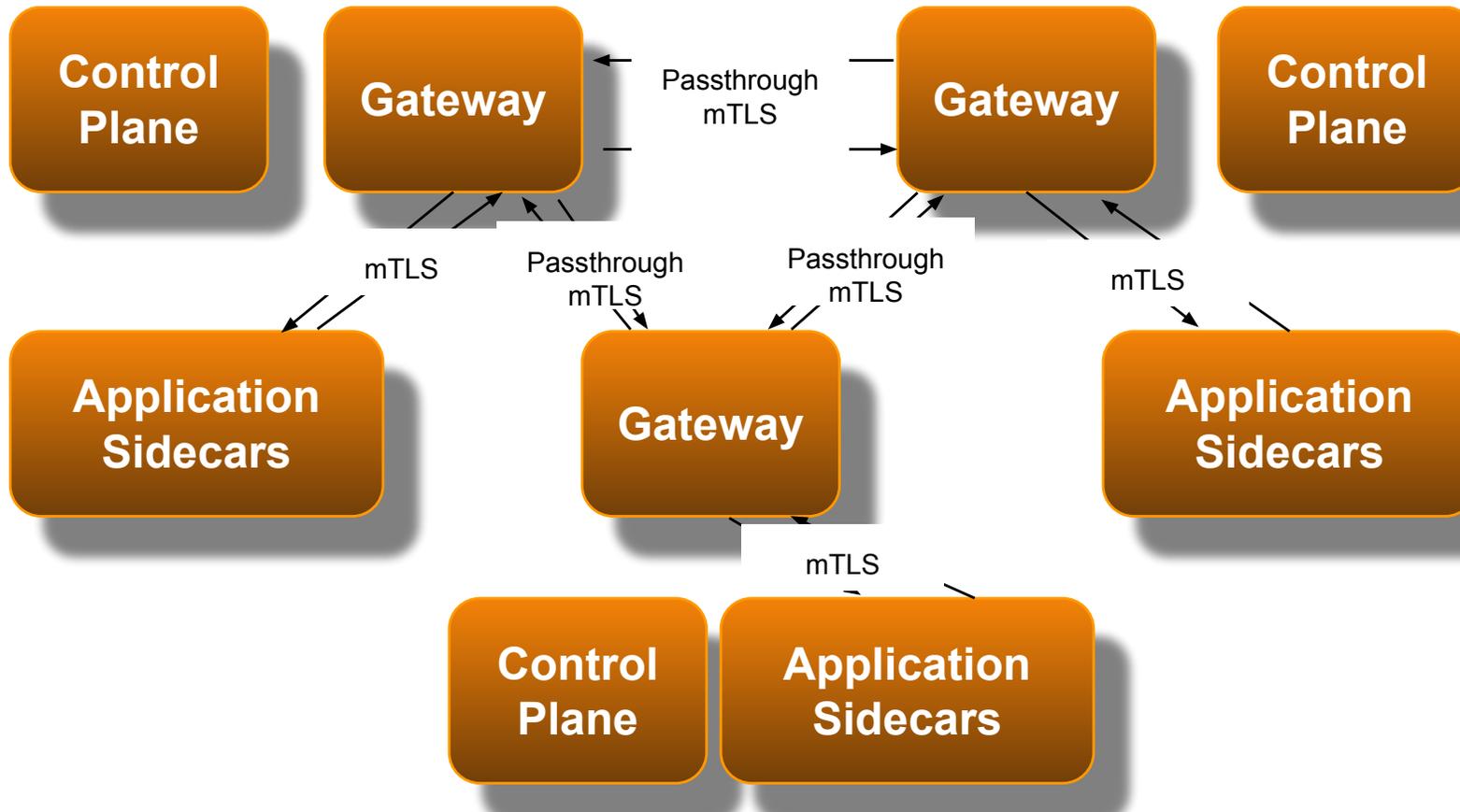


KubeCon



CloudNativeCon

Europe 2019



Istio Architecture

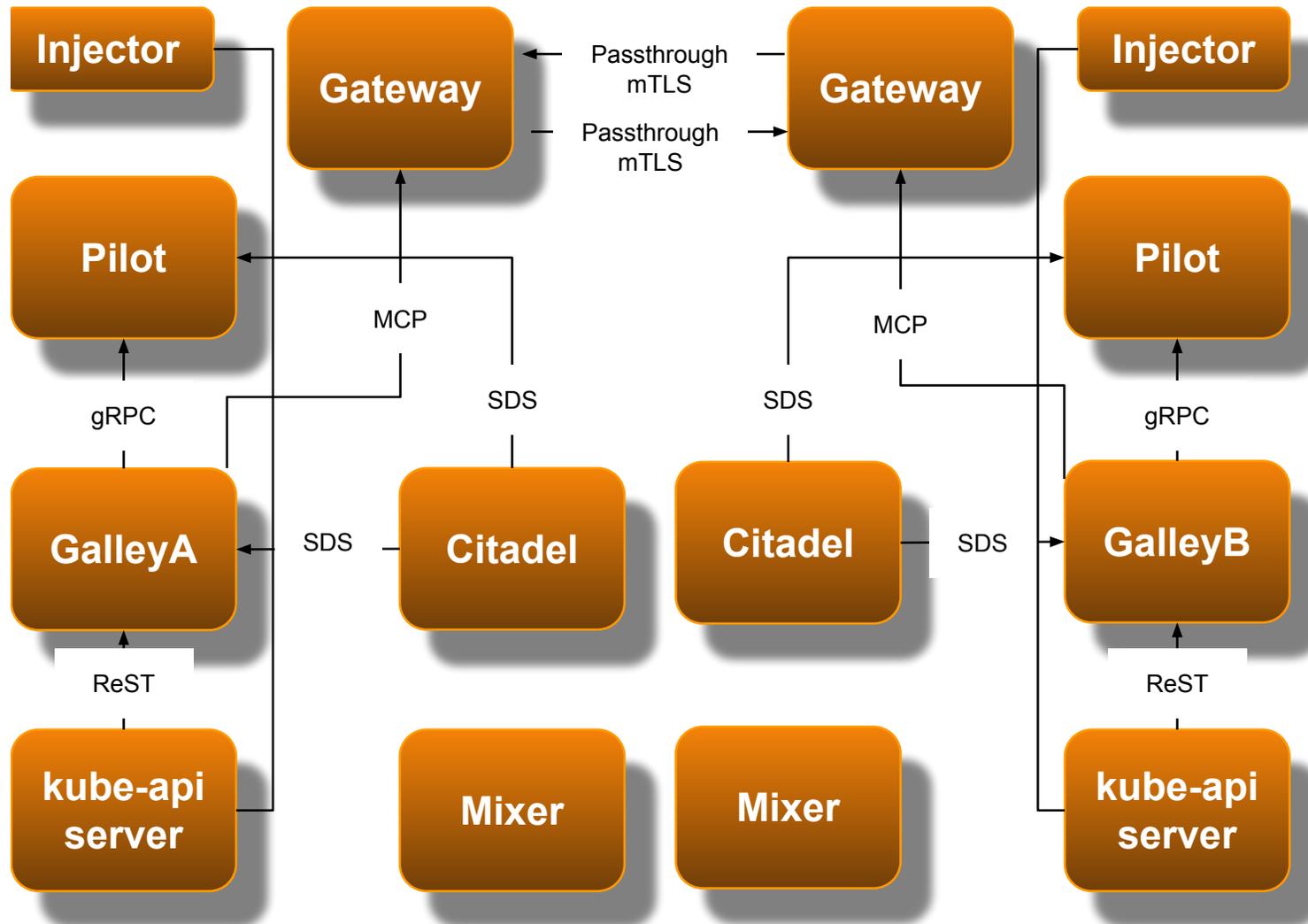


KubeCon



CloudNativeCon

Europe 2019





What is Service Discovery?

Service Discovery

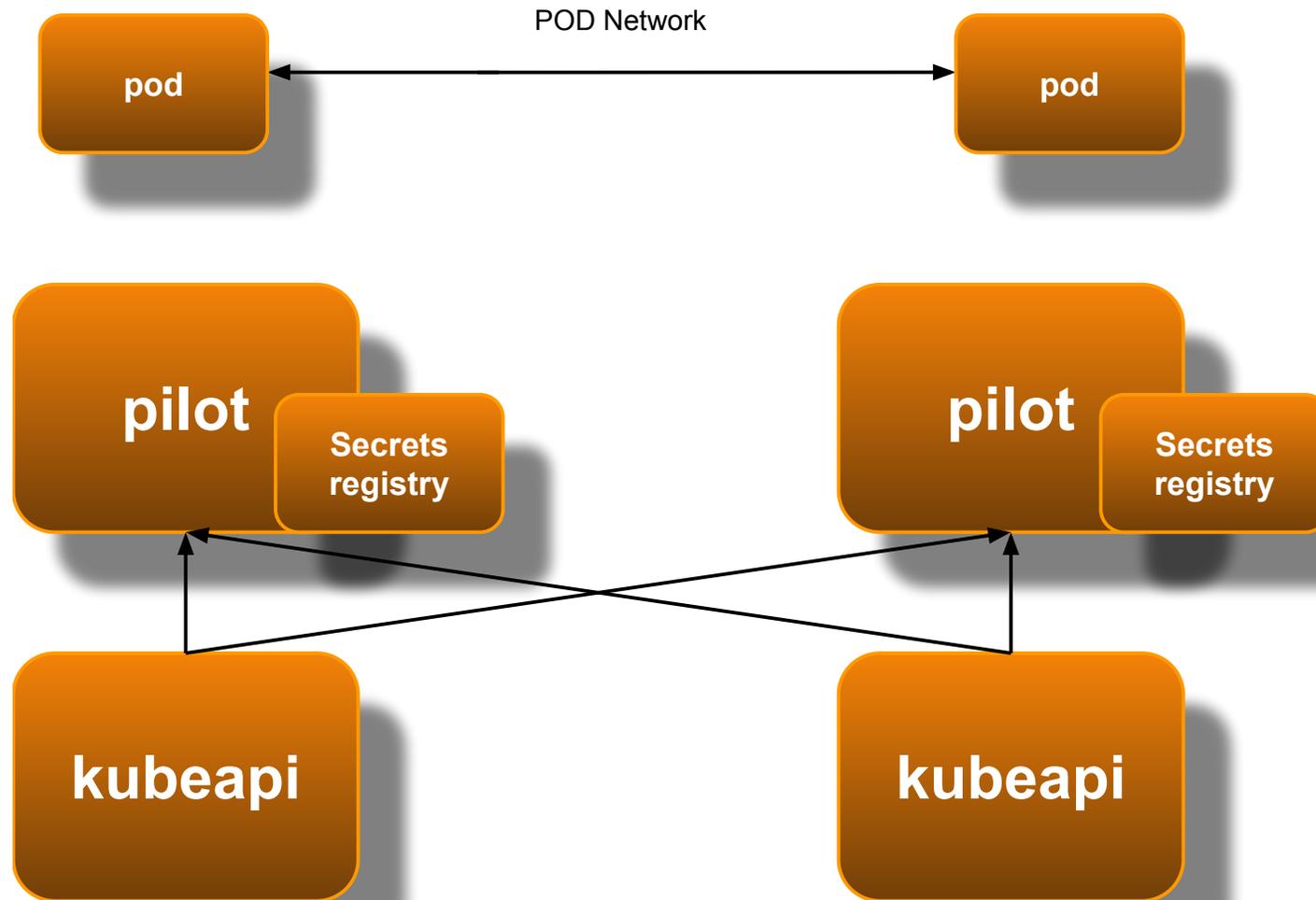


KubeCon



CloudNativeCon

Europe 2019



Service Discovery

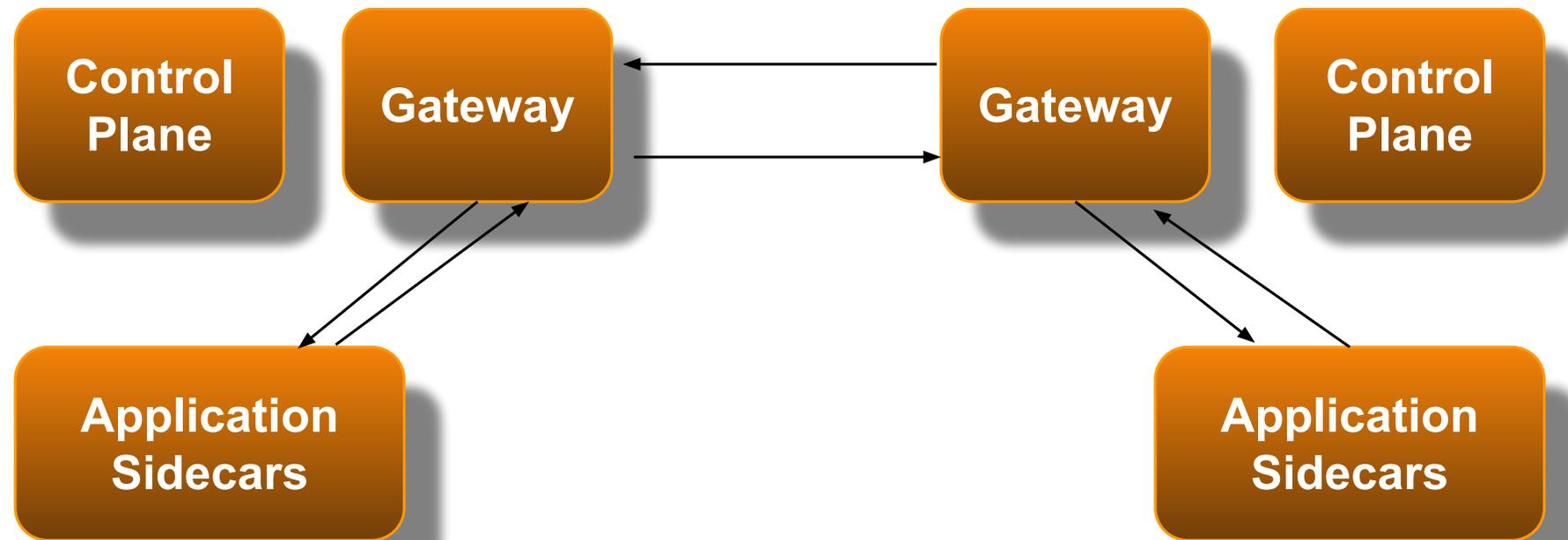


KubeCon



CloudNativeCon

Europe 2019



Connecting Gateways



KubeCon



CloudNativeCon

Europe 2019

Clusters **MUST** share a common root of trust.

Instructing Istio about root certs and intermediate certs:

```
cd $HOME/istio-1.1.6
kubectl create secret generic cacerts -n istio-system \
  --from-file=samples/certs/ca-cert.pem \
  --from-file=samples/certs/ca-key.pem \
  --from-file=samples/certs/root-cert.pem \
  --from-file=samples/certs/cert-chain.pem
```

More documentation about intermediate cert creation:

<https://jamielinux.com/docs/openssl-certificate-authority>

Connecting Gateways



KubeCon



CloudNativeCon

Europe 2019

```
apiVersion: networking.istio.io/v1alpha3
kind: ServiceEntry
metadata:
  name: redis-cart
spec:
  hosts:
  - redis-cart.default.global
  location: MESH_INTERNAL
  ports:
  - name: redis
    number: 6379
    protocol: tcp
  resolution: STATIC
  addresses:
  - 127.255.3.6
  endpoints:
  - address: 62.208.220.13
    ports:
      redis: 15443
```

Connecting Gateways



KubeCon



CloudNativeCon

Europe 2019

[ISTIO](#) / [BLOG](#) / [2019 POSTS](#) / [VERSION ROUTING IN A MULTICLUSTER SERVICE MESH](#)

Version Routing in a Multicluster Service Mesh

BY FRANK BUDINSKY (IBM) | 📅 FEBRUARY 7, 2019 | ⌚ 8 MINUTE READ

In this article, we've seen how to use Istio route rules to distribute the versions of a service across clusters in a multicluster service mesh with a [multiple control plane topology](#). In this example, we manually configured the `.global` service entry and destination rules needed to provide connectivity to one remote service, `reviews`. In general, however, if we wanted to enable any service to run either locally or remotely, we would need to create `.global` resources for every service. Fortunately, this process could be automated and likely will be in a future Istio release.

```
apiVersion: networking.istio.io/v1alpha3
kind: ServiceEntry
metadata:
  name: redis-cart
spec:
  hosts:
  - redis-cart.default.global
  location: MESH_INTERNAL
  ports:
  - name: redis
    number: 6379
    protocol: tcp
  resolution: STATIC
  addresses:
  - 127.255.3.6
  endpoints:
  - address: 62.208.220.13
    ports:
      redis: 15443
```

Connecting Gateways



KubeCon



CloudNativeCon

Europe 2019

```
sdake — sdake@beast-01: ~ — vi coredns-config.sh — 97x30
$ kubectl apply -f - <<EOF
apiVersion: v1
kind: ConfigMap
metadata:
  name: coredns
  namespace: kube-system
data:
  Corefile: |
    .:53 {
      errors
      health
      kubernetes cluster.local in-addr.arpa ip6.arpa {
        pods insecure
        upstream
        fallthrough in-addr.arpa ip6.arpa
      }
      prometheus :9153
      proxy . /etc/resolv.conf
      cache 30
      loop
      reload
      loadbalance
    }
  global:53 {
    errors
    cache 30
    proxy . $(kubectl get svc -n istio-system istiocoredns -o jsonpath={.spec.clusterIP})
  }
EOF
```

Hipster Shop Anatomy

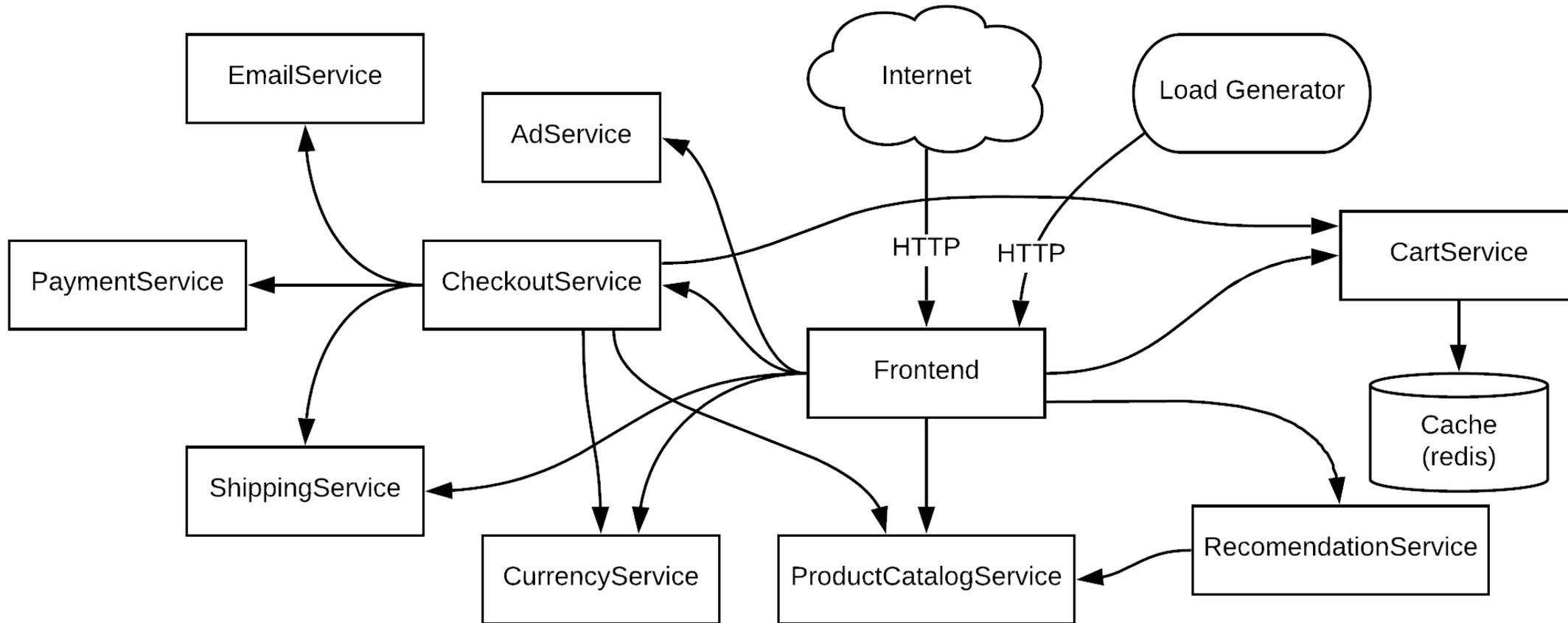


KubeCon



CloudNativeCon

Europe 2019



<https://github.com/GoogleCloudPlatform/microservices-demo>

Hipster Shop Demo

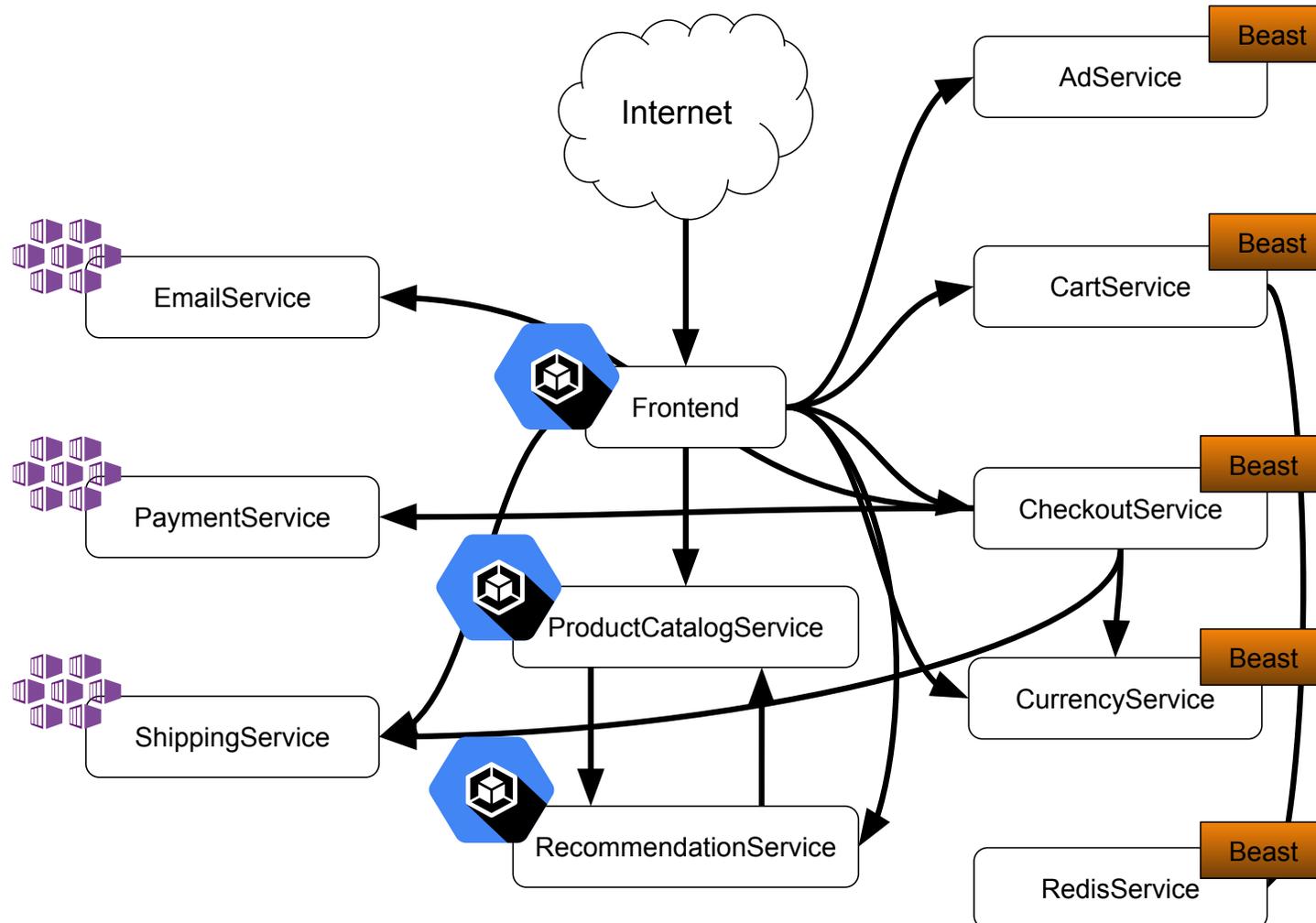


KubeCon



CloudNativeCon

Europe 2019



Automation with MCP

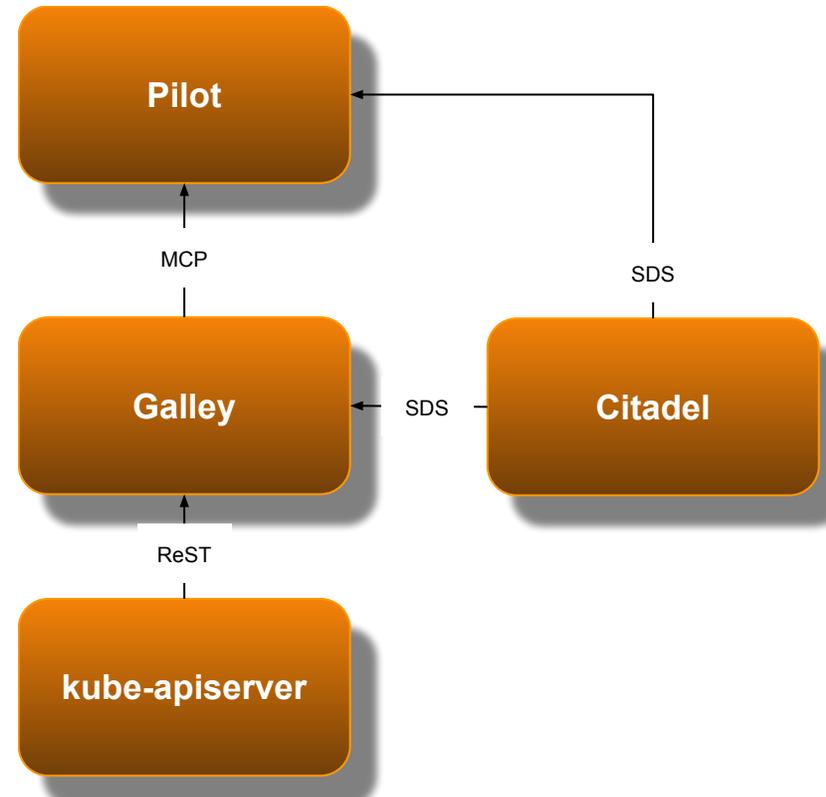


KubeCon



CloudNativeCon

Europe 2019



Automation with MCP



KubeCon



CloudNativeCon

Europe 2019

```
apiVersion: networking.istio.io/v1alpha3
kind: EnvoyFilter
metadata:
  name: galley-replacement-X
filters:
- filterConfig:
  cluster_pattern: galley-X.istio-system.svc.cluster.local
  cluster_replacement: galley.istio-system.svc.cluster.local
  filterName: envoy.filters.network.tcp_cluster_rewrite
  filterType: NETWORK
  insertPosition:
    index: AFTER
    relativeTo: envoy.filters.network.sni_cluster
  listenerMatch:
    listenerType: GATEWAY
    portNumber: 15443
```

Automation with MCP

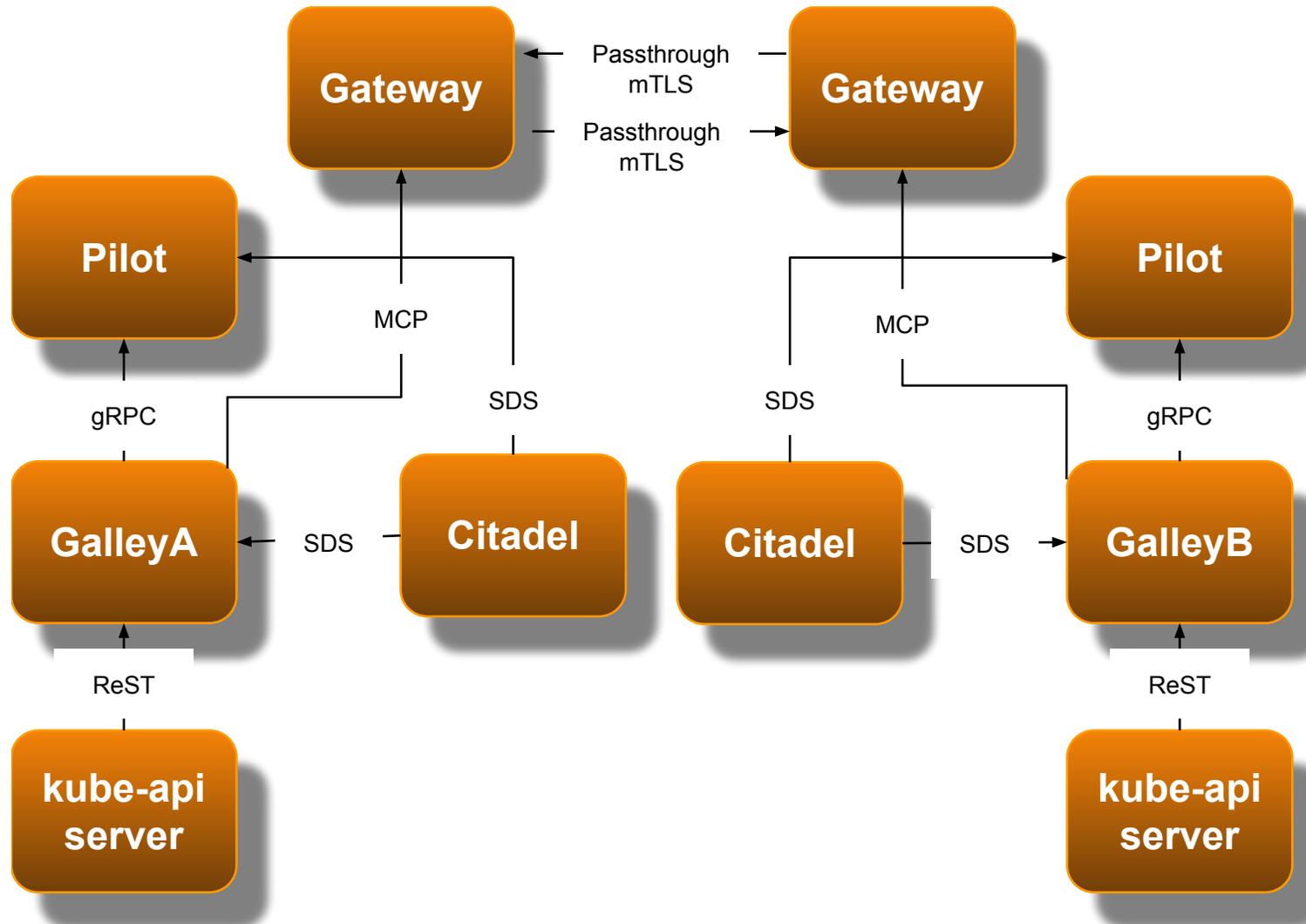


KubeCon



CloudNativeCon

Europe 2019



Automation with MCP

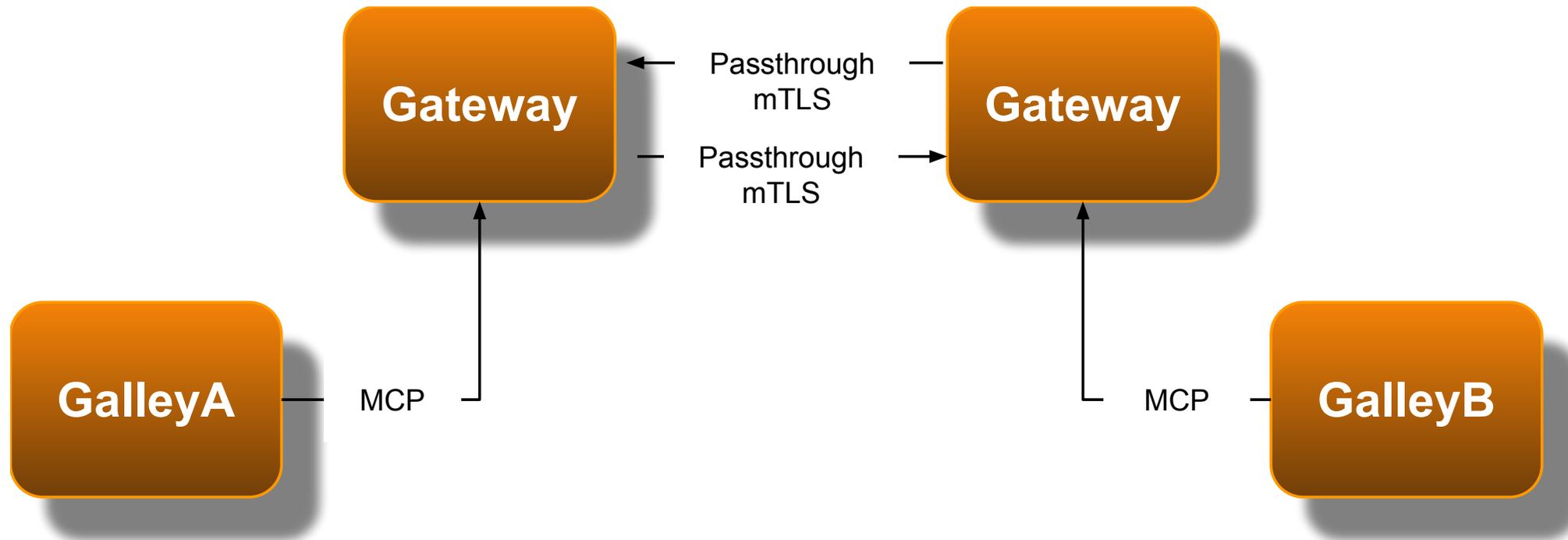


KubeCon



CloudNativeCon

Europe 2019



Automation with MCP

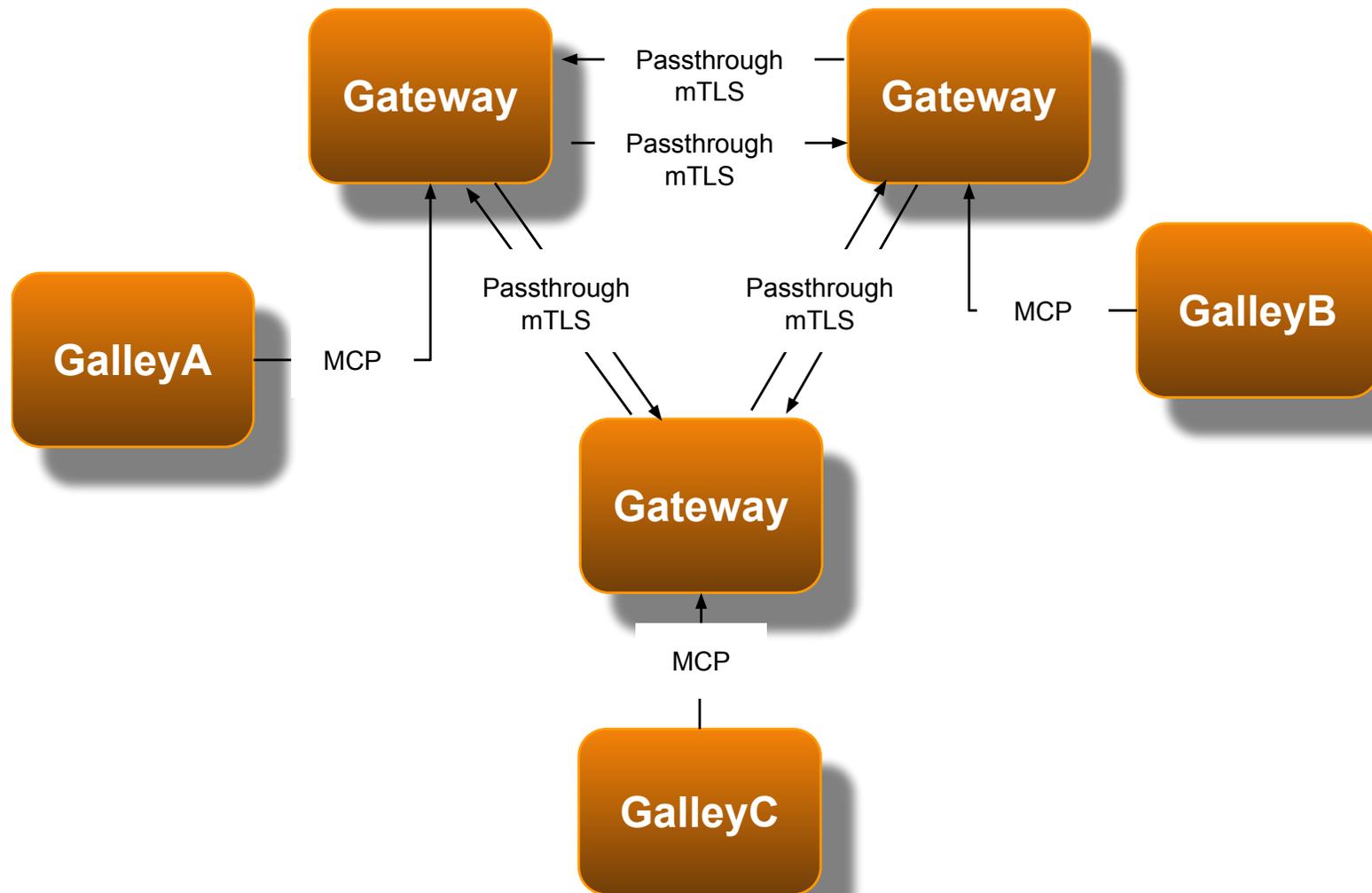


KubeCon



CloudNativeCon

Europe 2019



Automation with MCP

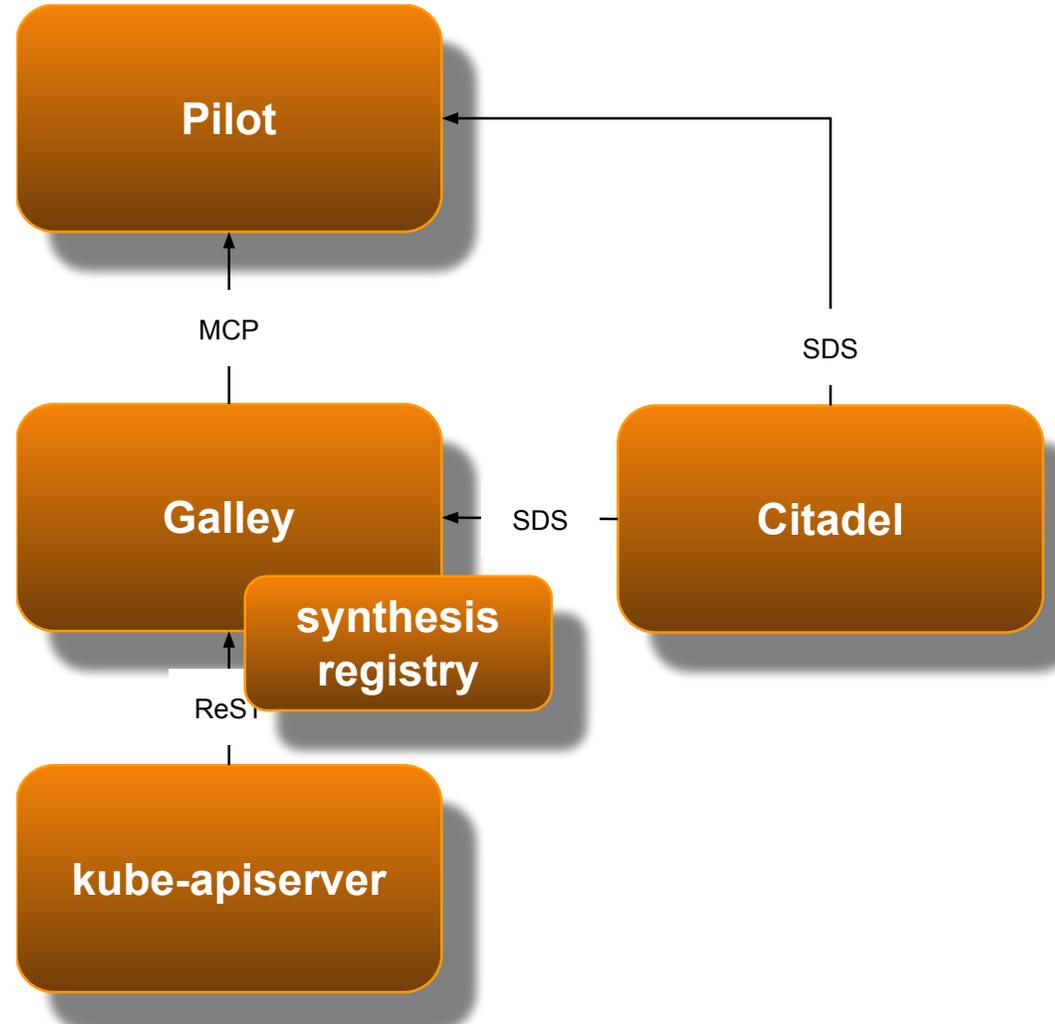


KubeCon



CloudNativeCon

Europe 2019



Automation with MCP

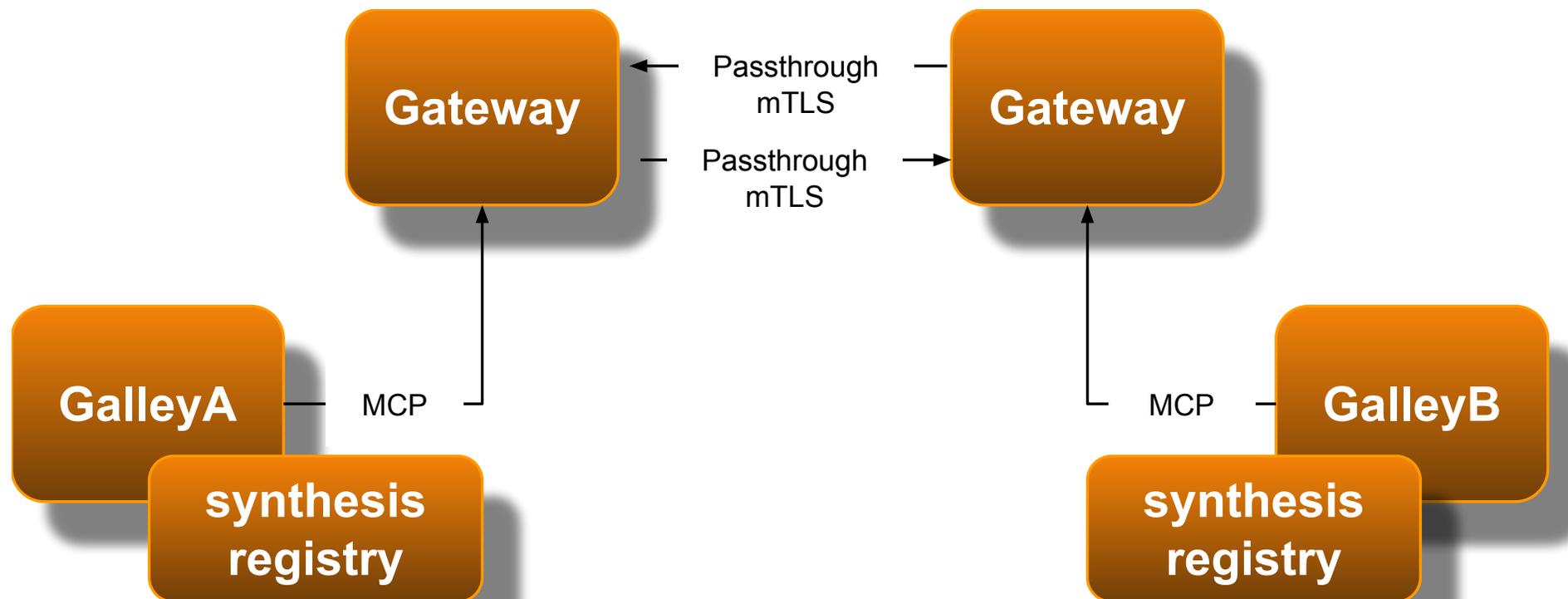


KubeCon



CloudNativeCon

Europe 2019



Automation with MCP

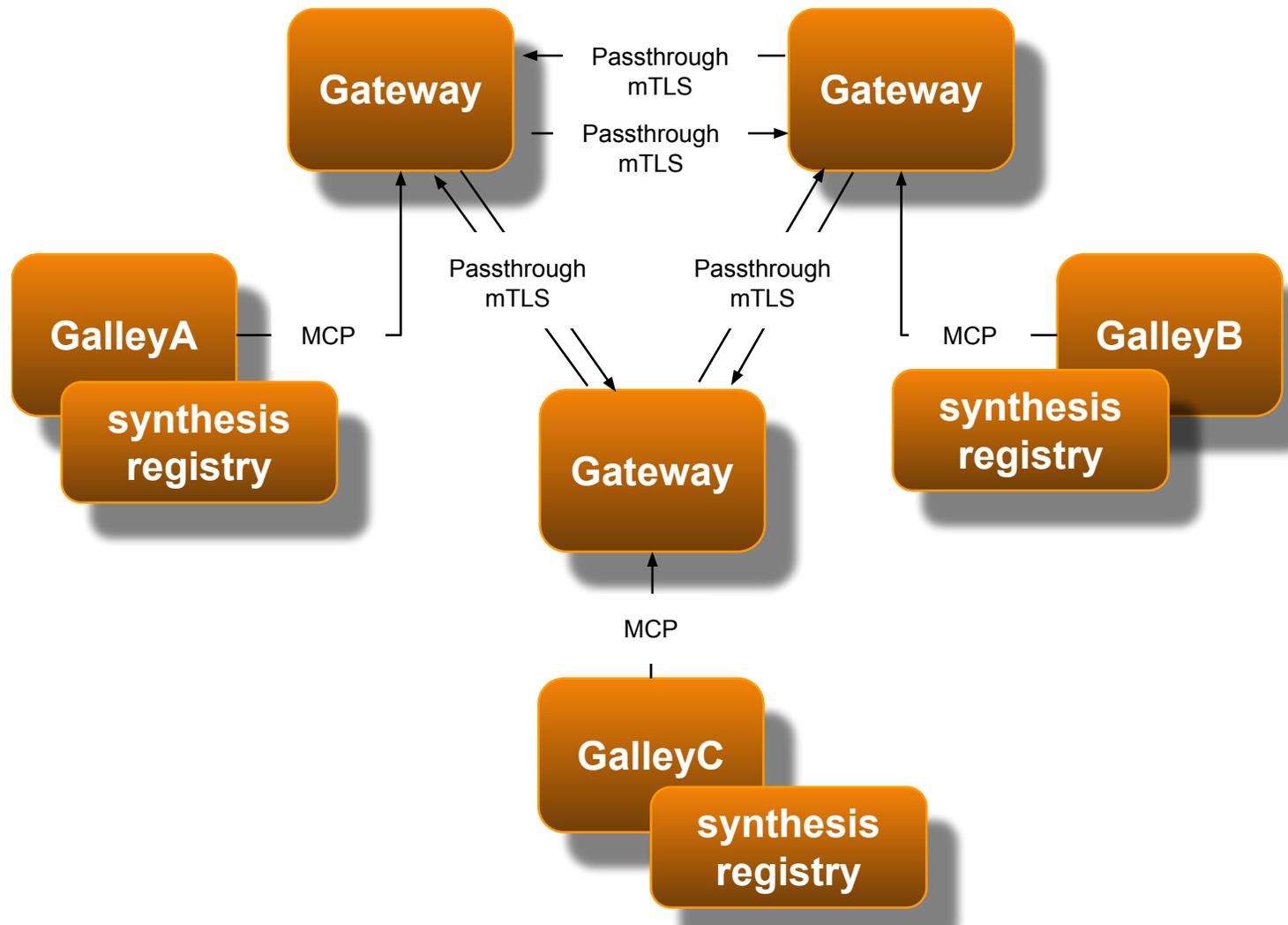


KubeCon



CloudNativeCon

Europe 2019



Potential User Interface



KubeCon



CloudNativeCon

Europe 2019

```
sdake@beast-01:~$ istioctl mc --join 192.168.7.108
Istio is aware of the following gateways:
192.168.7.105
192.168.7.106
Istio is attempting to add the gateway 192.168.7.108
Istio was successful in adding the gateway 192.168.7.108
sdake@beast-01:~$
```

Answer Time



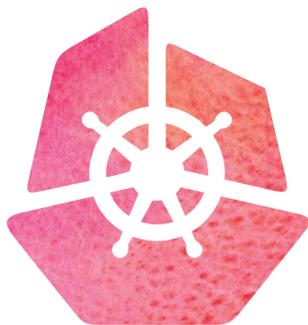
KubeCon



CloudNativeCon

Europe 2019

<https://istio.io>



KubeCon



CloudNativeCon

Europe 2019