


KubeCon | CloudNativeCon

Europe 2020

Virtual

Mesh in a Mesh

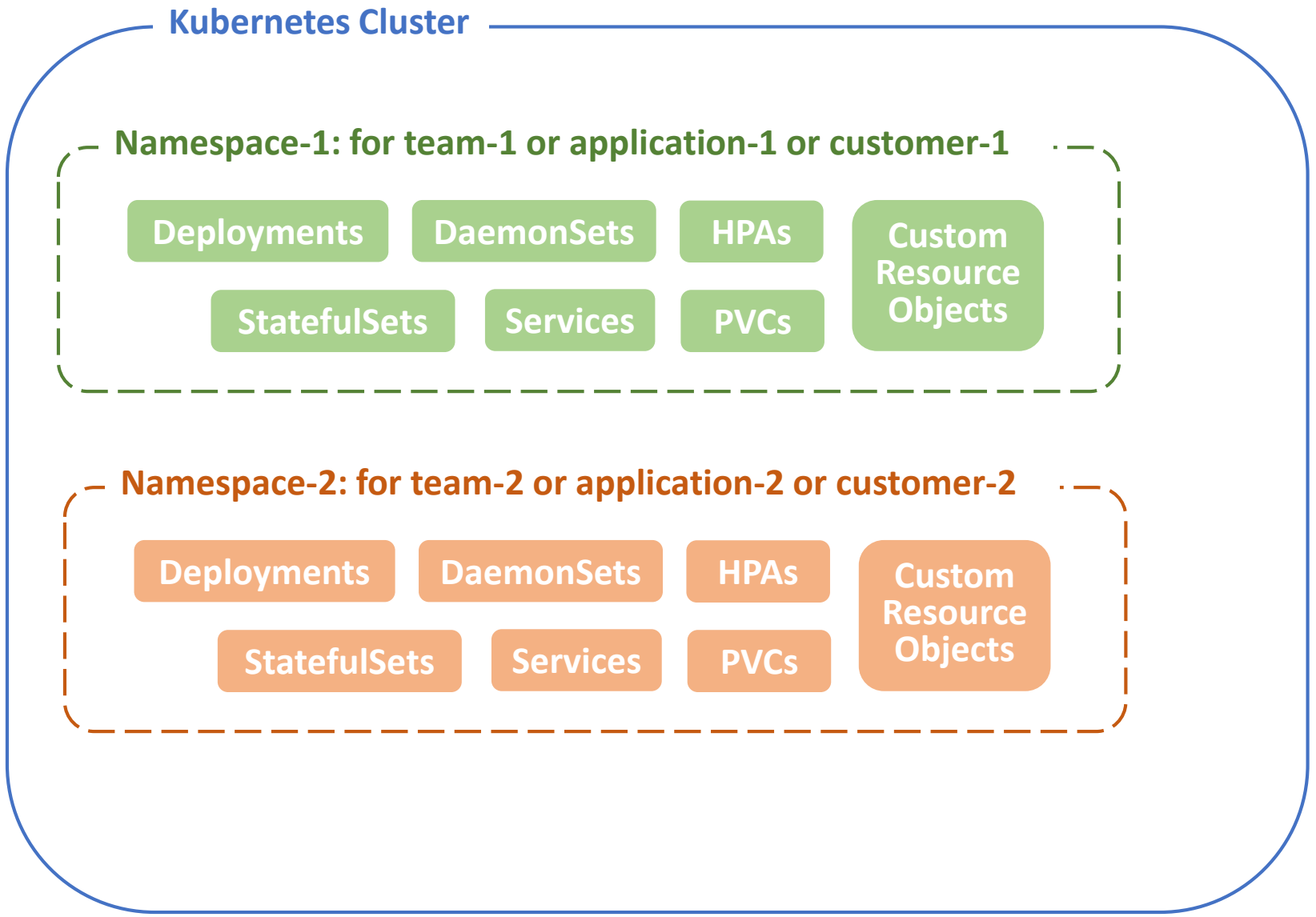
A Model for Stronger Multi-tenancy of Kubernetes Workloads

Nitish Malhotra, Affirmed Networks

Akash Baid, Affirmed Networks

affirmed

Namespaces 101

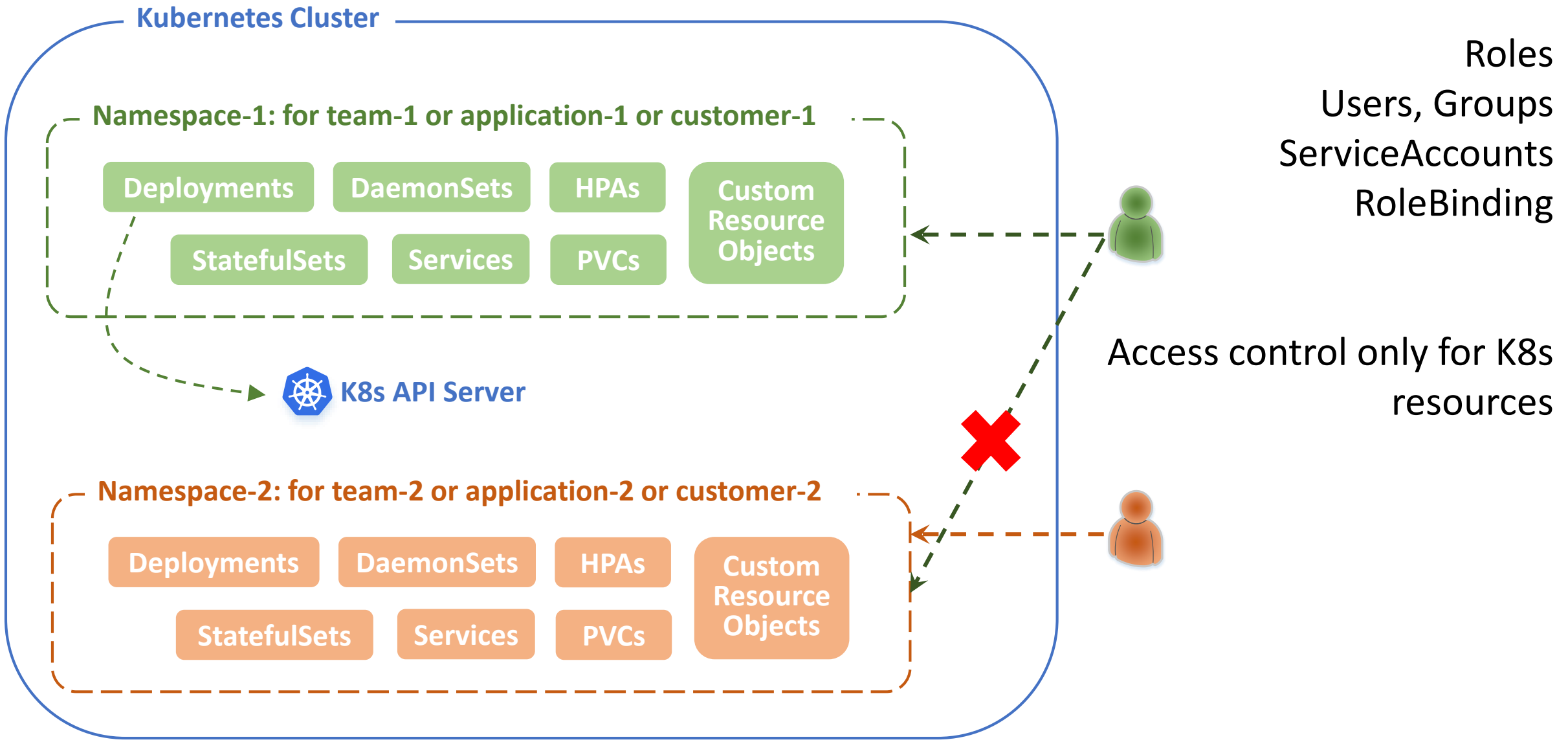


Namespaces offer a way to logically separate Kubernetes objects

Just creating objects in different namespaces gives little benefit apart from prettifying kubectl outputs

Need to define/use Namespace Controls

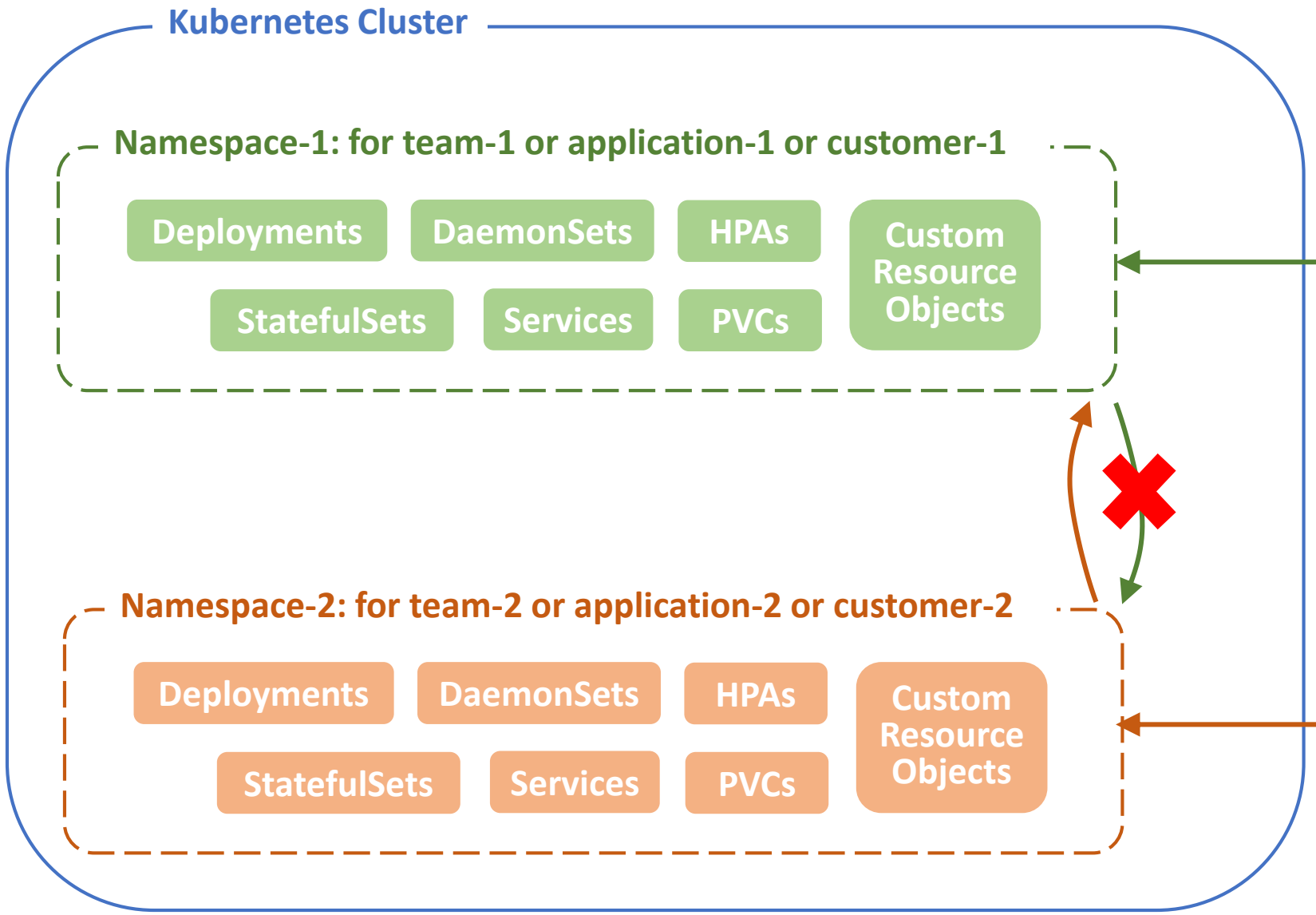
Namespace Controls - RBAC



Roles
Users, Groups
ServiceAccounts
RoleBinding

Access control only for K8s resources

Namespace Controls - NetworkPolicy



NetworkPolicy

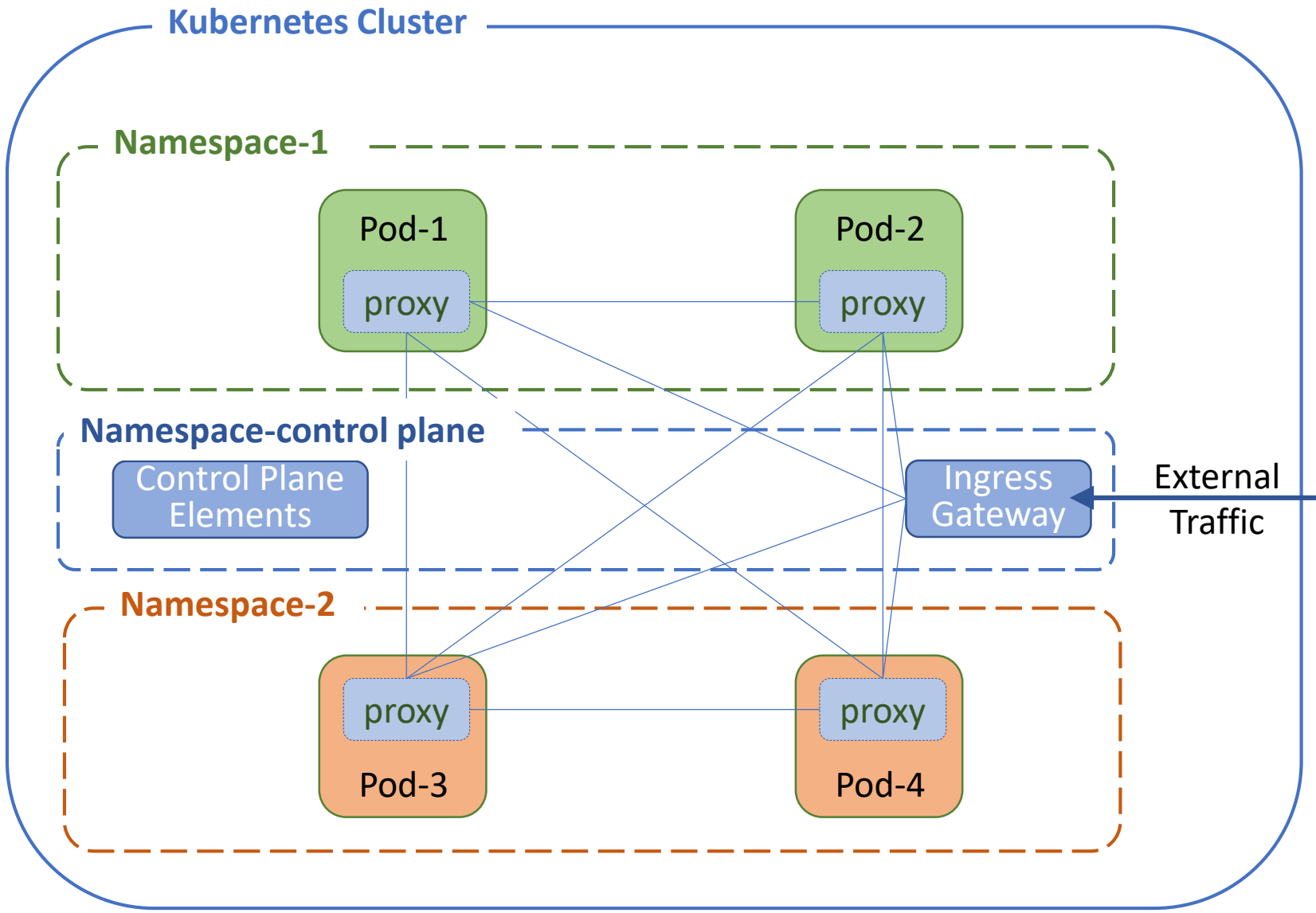
Allow/Deny List for incoming & outgoing traffic per namespace

L3 & L4 only mechanism

Need more

- L7 traffic policies per tenant
- Security enforcement per tenant
  - transport authentication using mTLS
  - origin authentication using JWT
  - authorization using OAuth2.0
- Accounting and Auditing per tenant

Adding Service Mesh to the mix



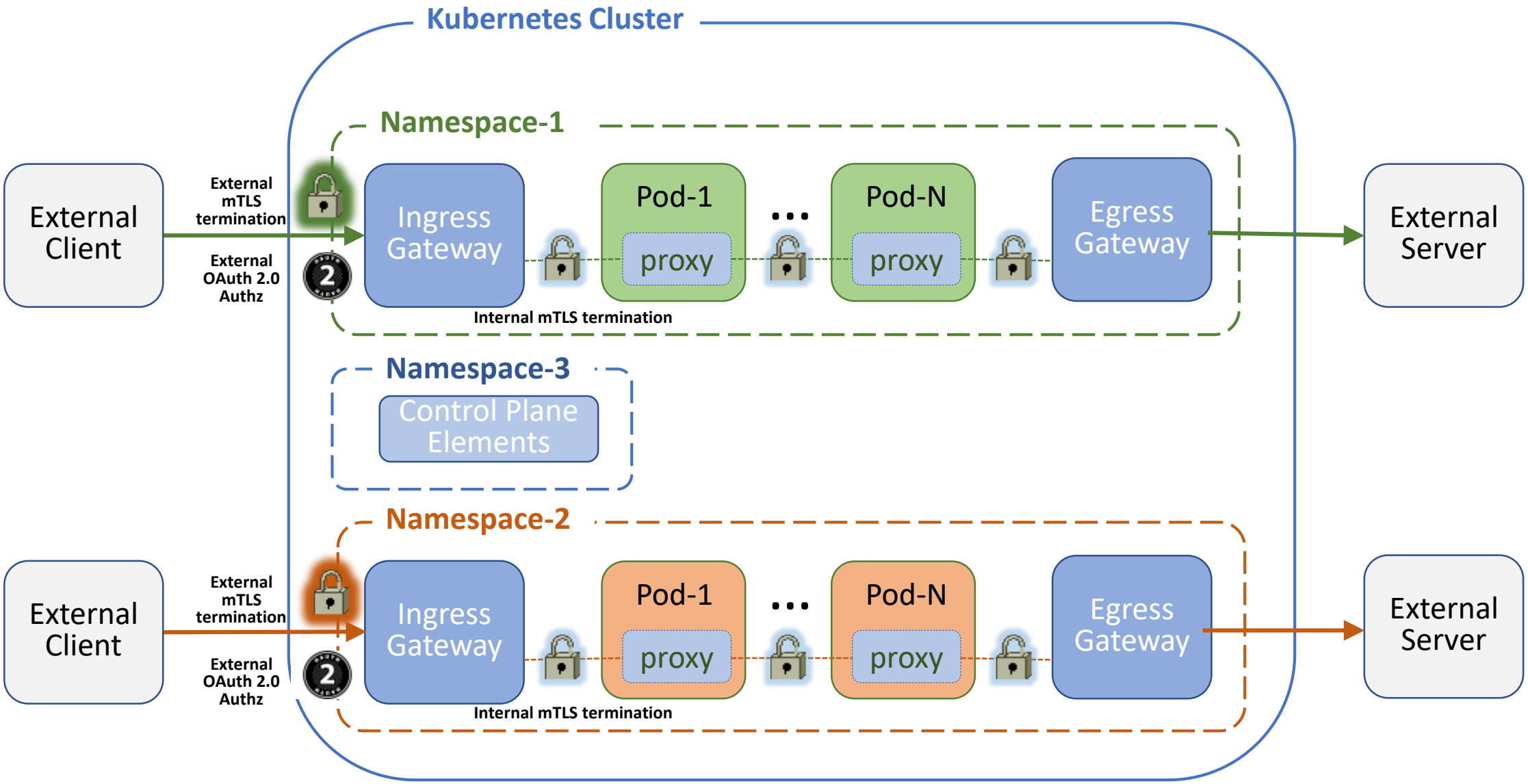
Typical Deployment

- Control plane in its own namespace
- Fully connected mesh
- Common Ingress-Gateway in control plane namespace
- Cluster-wide mesh policies

Need even more

- No shared path for incoming/outgoing requests of tenants
- Independent & automated scaling of gateways
- Hiding of tenant application topology when communicating with external entities
- Share mesh control plane resources across tenants

Mesh-in-a-mesh




KubeCon
CloudNativeCon
Europe 2020
Virtual
HELM
KEEP CLOUD NATIVE
CONNECTED