



KubeCon



CloudNativeCon

Europe 2023

Operate Multi-Tenancy Service Mesh with ArgoCD in Production

Lin Sun, solo.io

Faseela K, Ericsson Software Technology



Director of Open Source, Solo.io

 @linsun_unc

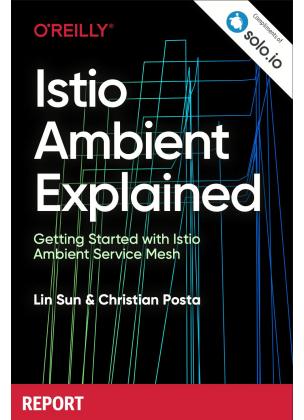
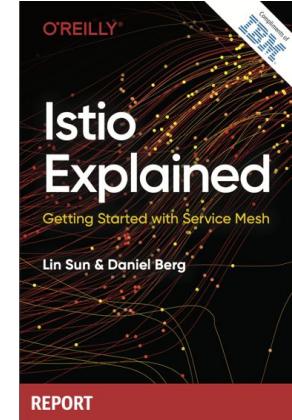
 lin.sun@solo.io

 [linkedin.com/pub/linsun/1/...](https://linkedin.com/pub/linsun/1/)



8300+ contributions

TOC Member



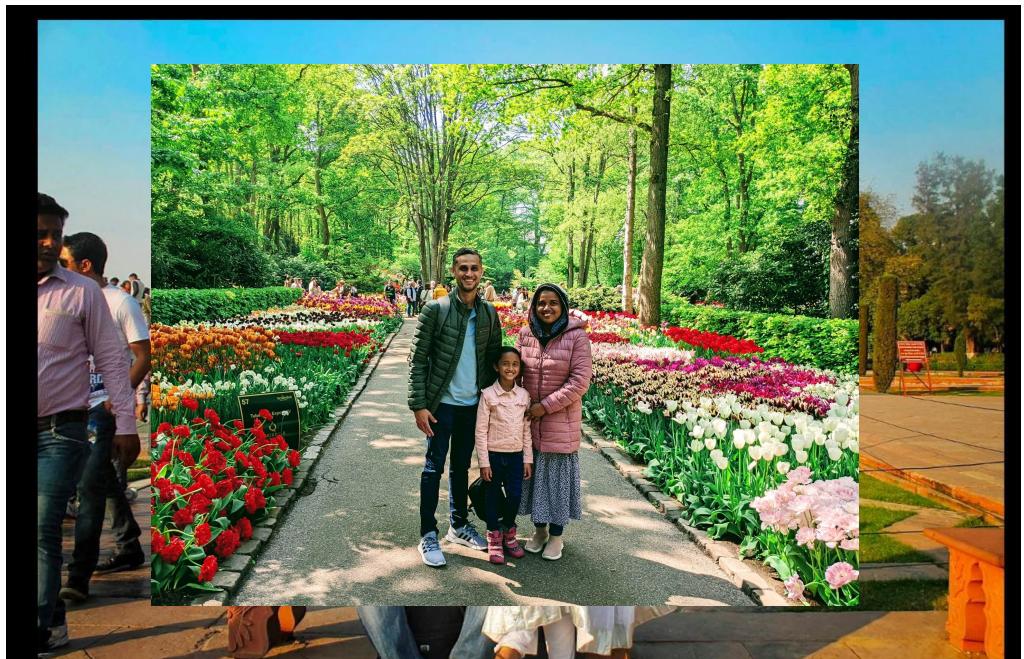
Book signing tonight at 6pm!



Faseela K



1000+ contributions
Steering Member



Cloud Native Developer, EST

 @faseeladilshan

 faseela.k@est.tech

 <https://www.linkedin.com/in/faseela-k-42178528>

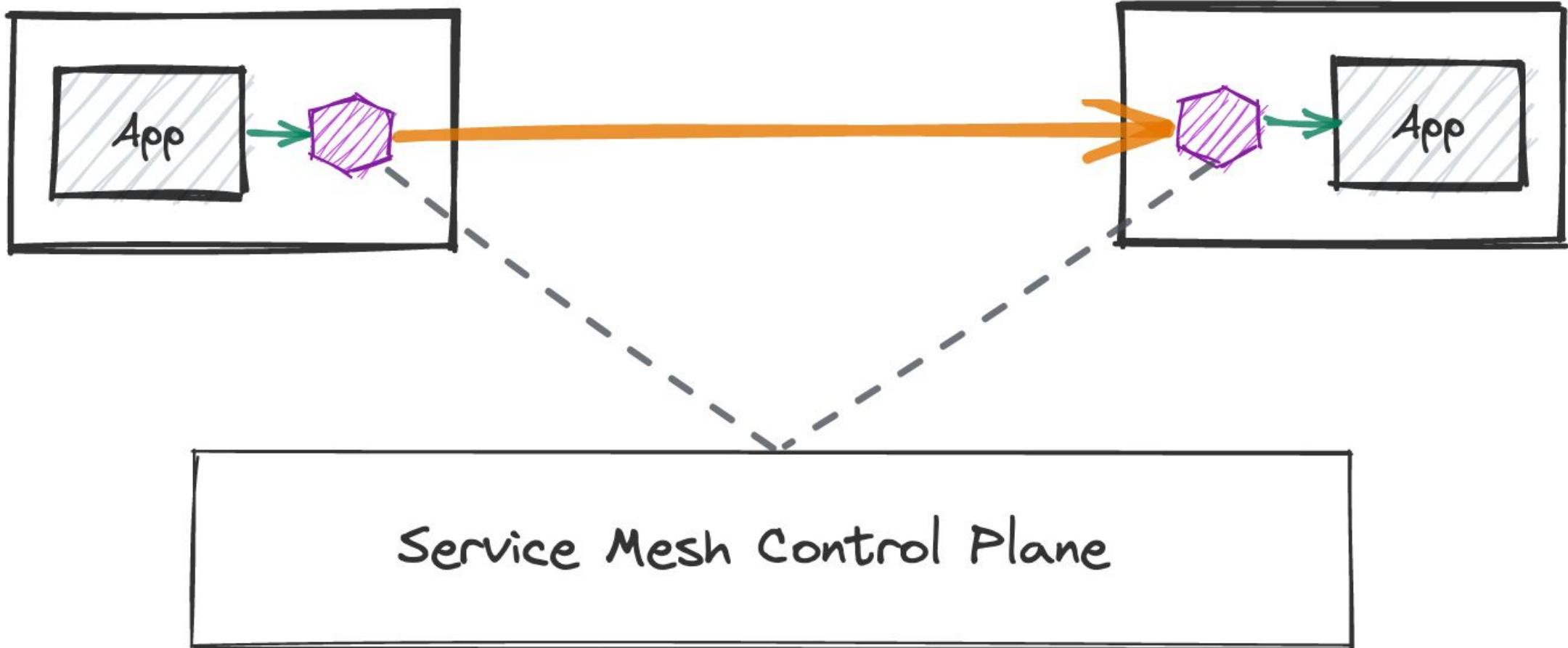
Agenda

- Overview of Service Mesh
- Introduction of Multi-Tenancy Istio Service Mesh
- Operate Multi-Tenancy Istio with ArgoCD
- Best Practice of Multi-Tenancy Istio Service Mesh

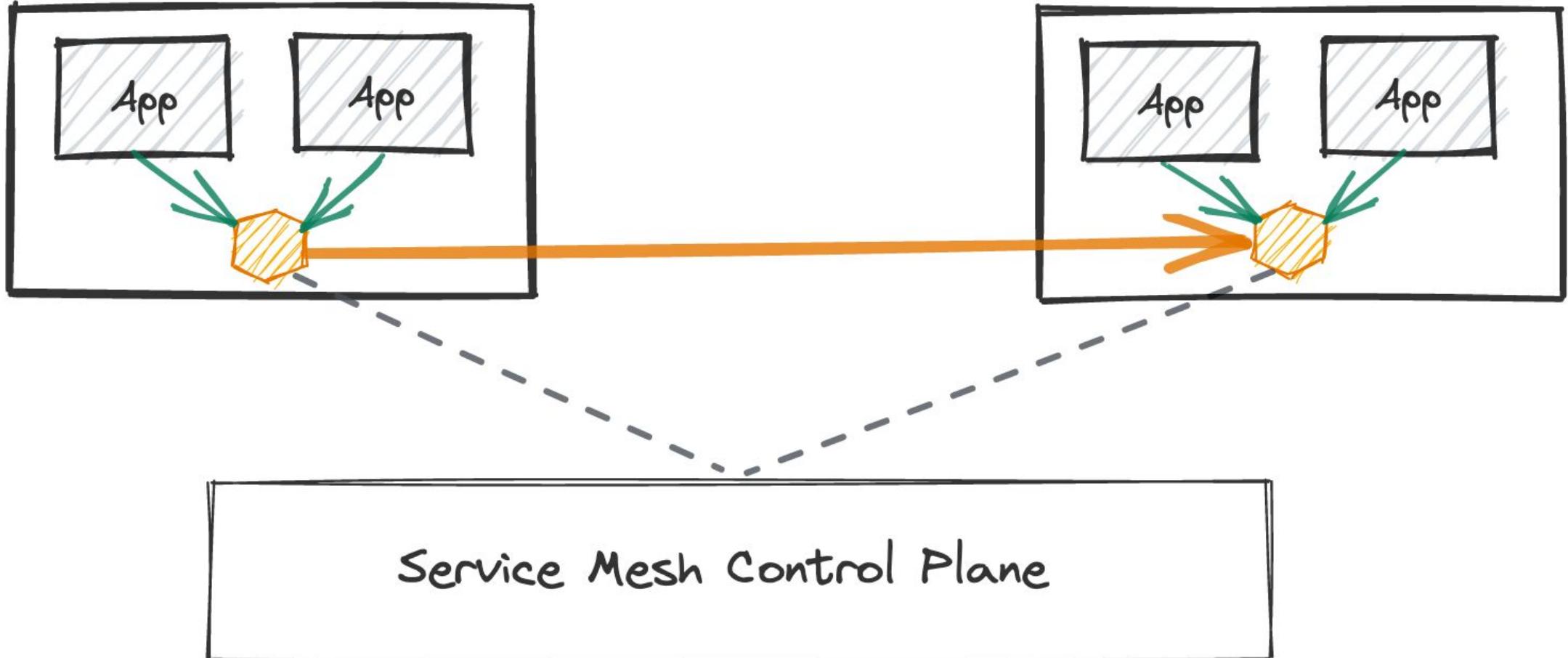
What is a Service Mesh?

A service mesh is a **programmable** framework that allows you to **observe, secure and connect** microservices.

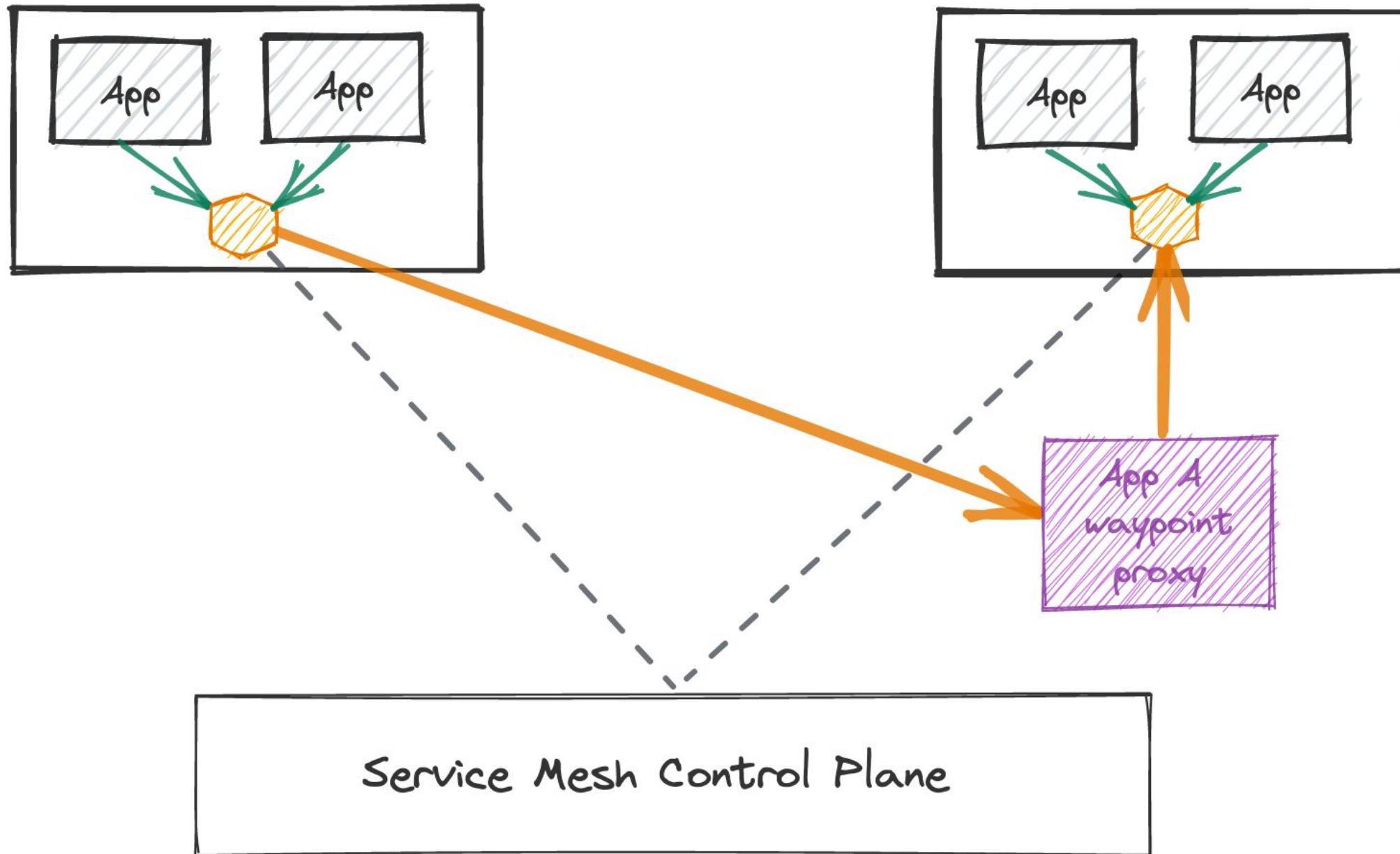
Service Mesh Architecture



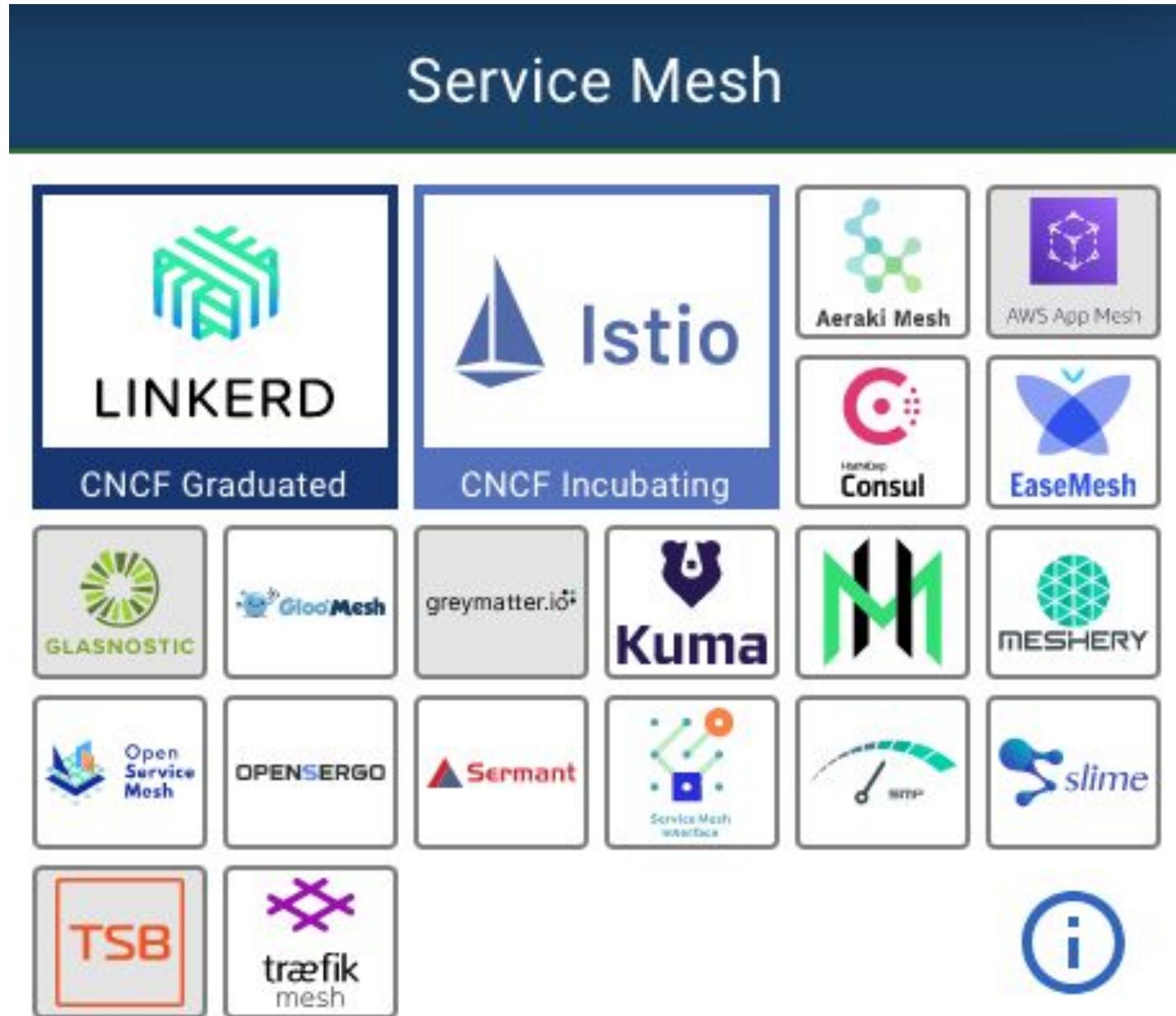
Service Mesh Architecture Evolution



Service Mesh Architecture Evolution



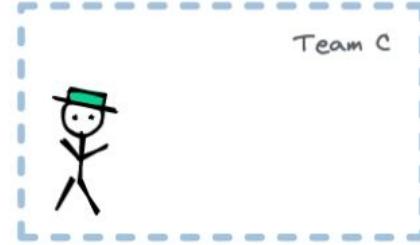
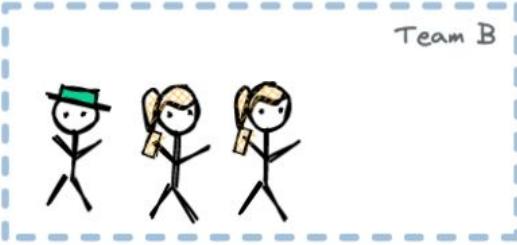
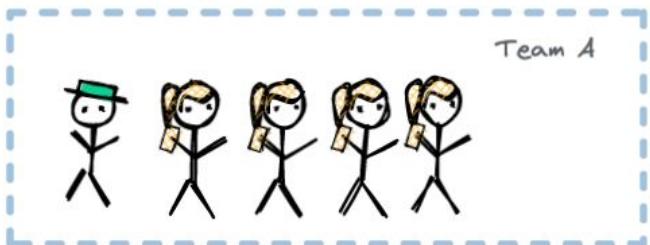
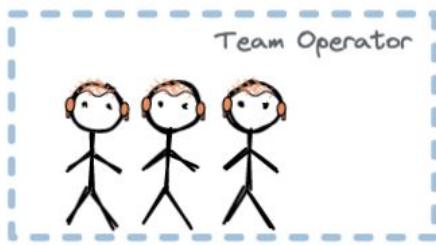
CNCF Service Mesh Landscape



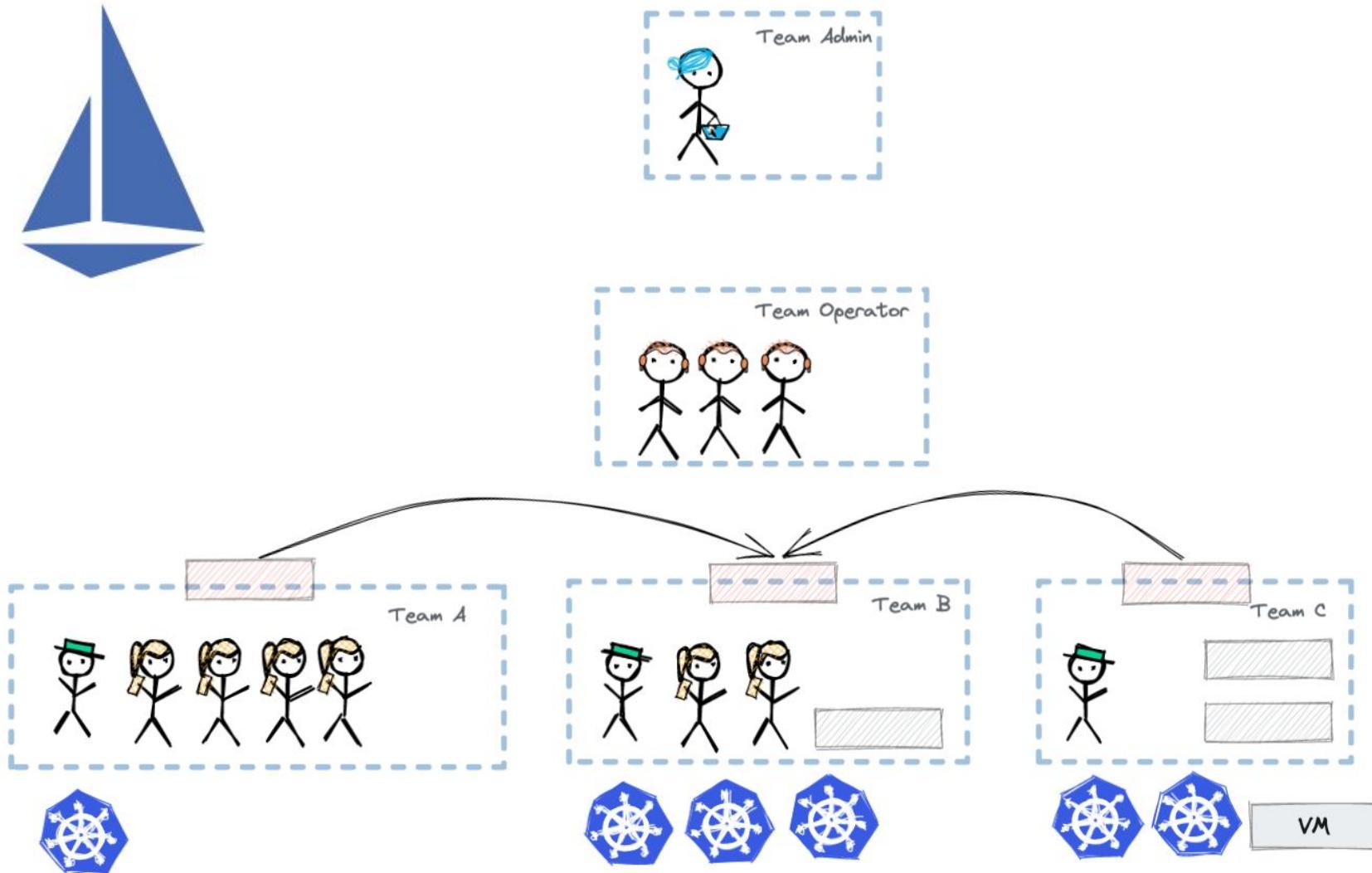
Multi-Tenancy Istio Service Mesh

- Single Mesh with multiple teams
- Multiple Mesh - Single cluster
- Multiple Mesh - Multiple clusters

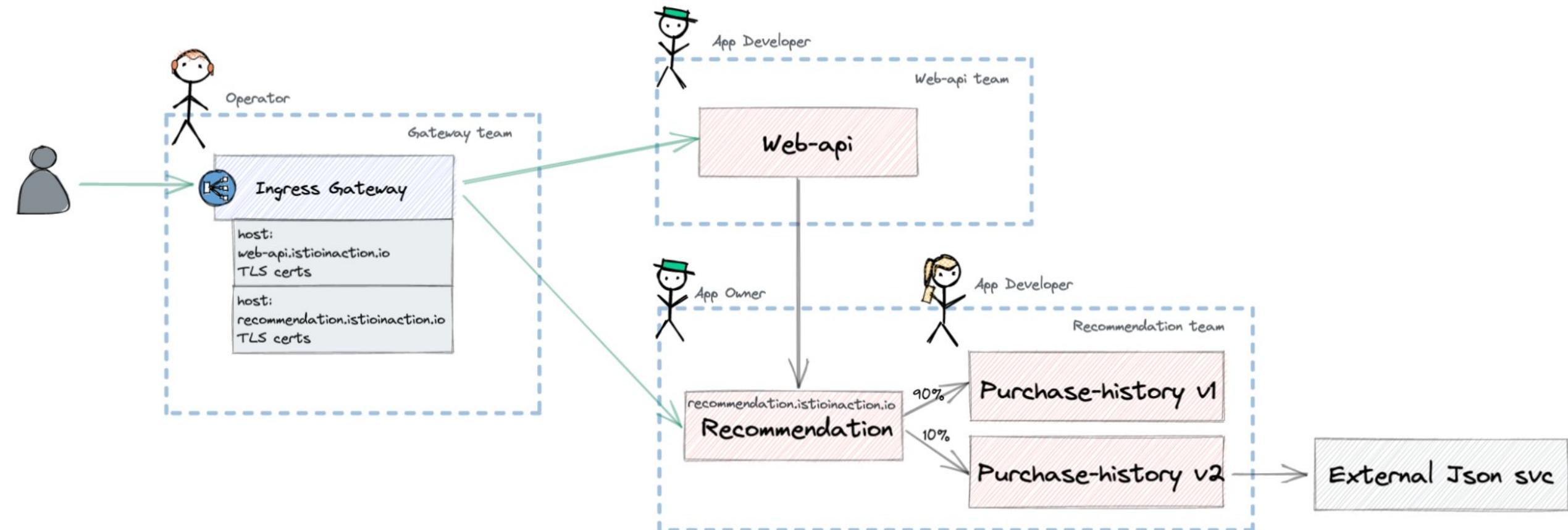
Single Istio Multiple Teams



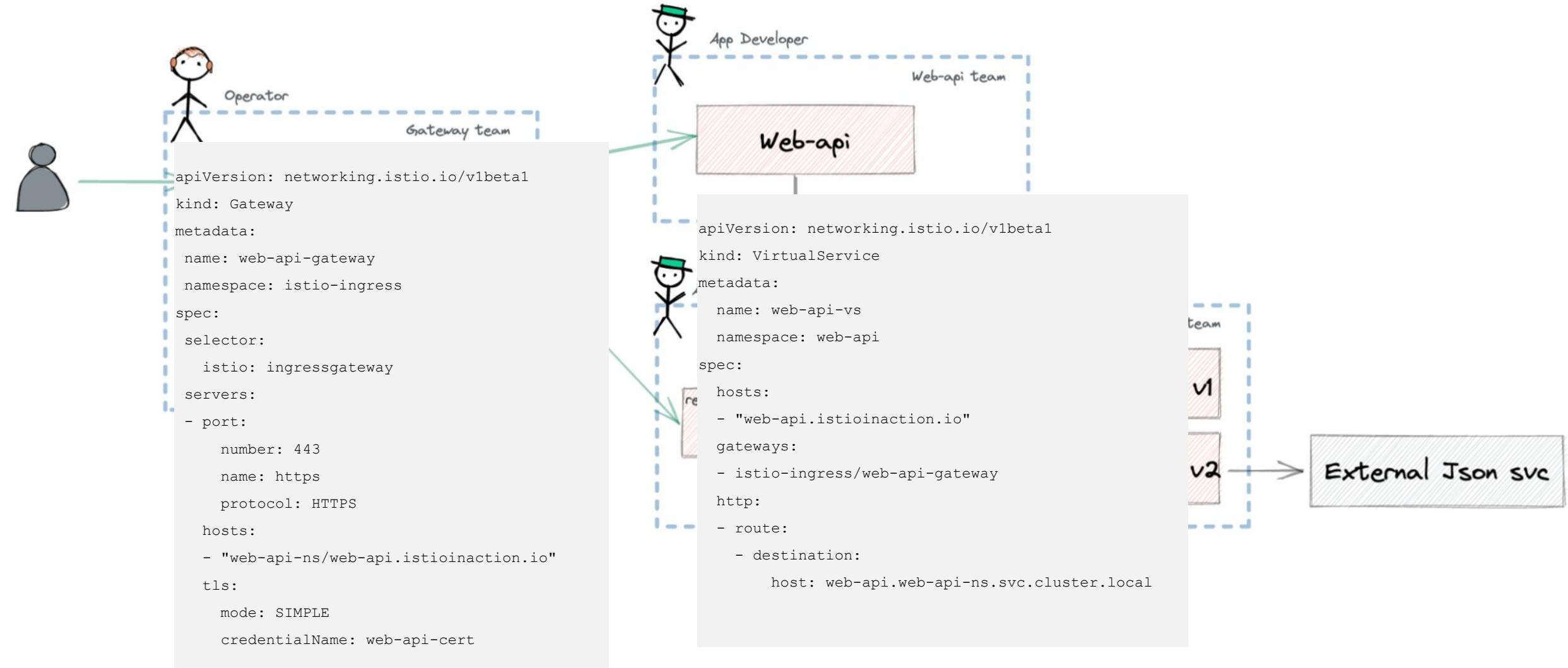
Single Istio Multiple Teams & Services



Examples



Examples With Istio



Config Isolation Per Team

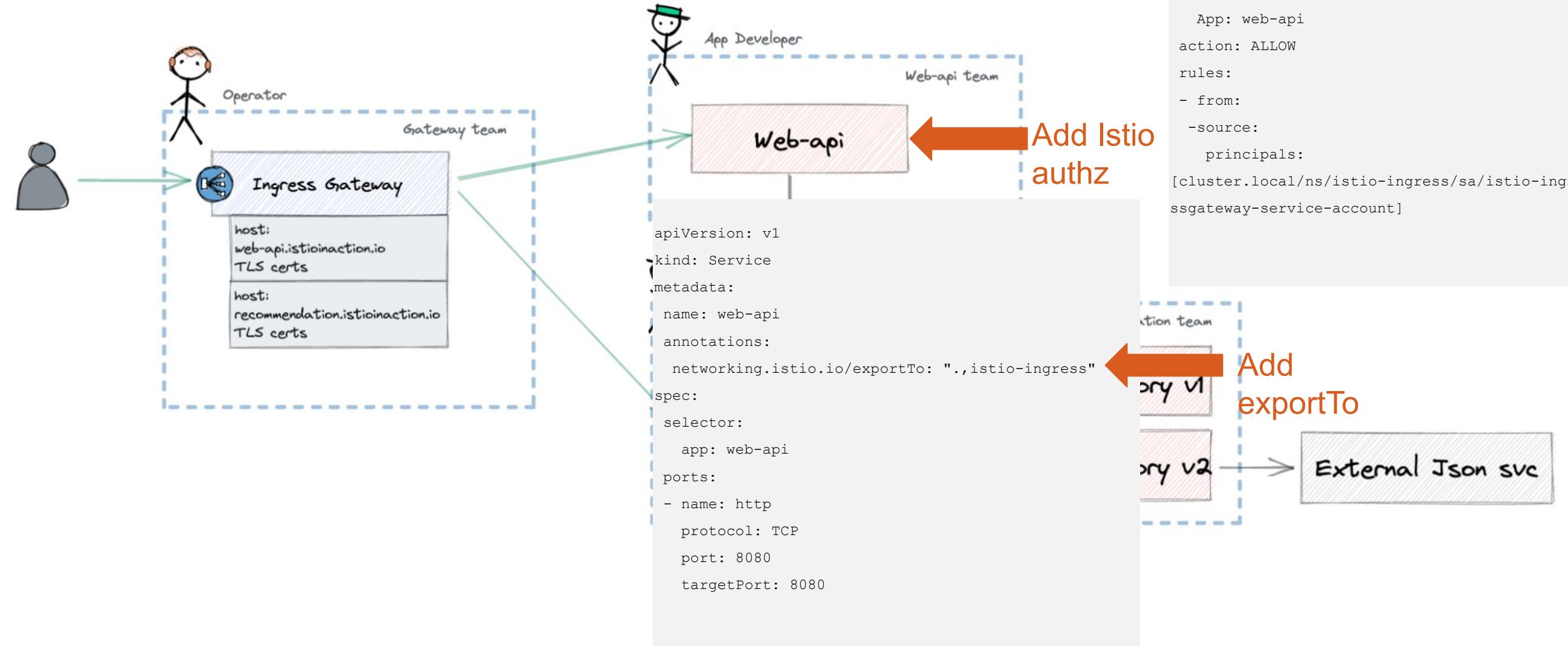
- Team may own 1 or more namespaces
- Istio resources are made available to all namespaces by default
 - **Service Consumer**
 - Sidecar resource
 - `exportTo` configuration on
 - `VirtualService` resource
 - `DestinationRule` resource
 - `ServiceEntry` resource
 - **Service Producer**
 - `networking.istio.io/exportTo` annotation on
 - Kubernetes service
 - `AuthorizationPolicy`



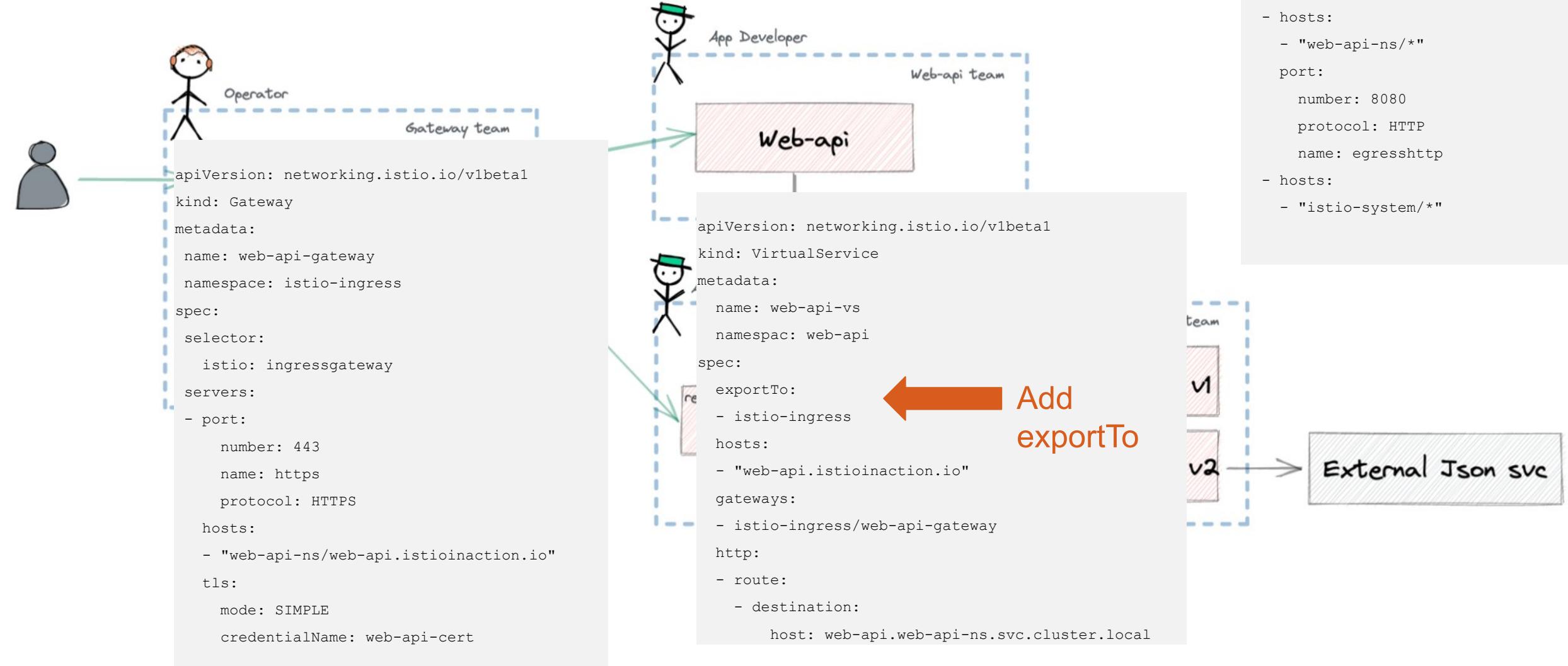
Service Consumer

Service Producer

Service Producer Config Isolation

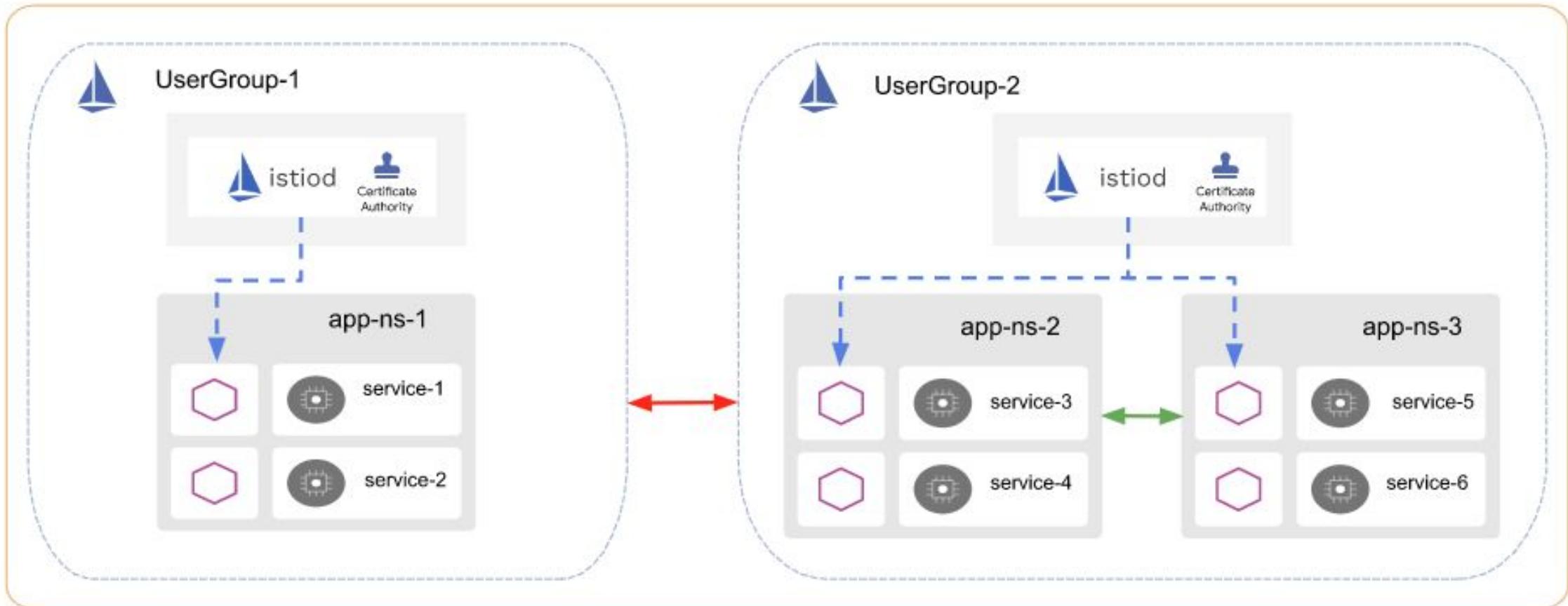


Service Consumer Config Isolation



Multiple Istio Multiple Applications

Cluster

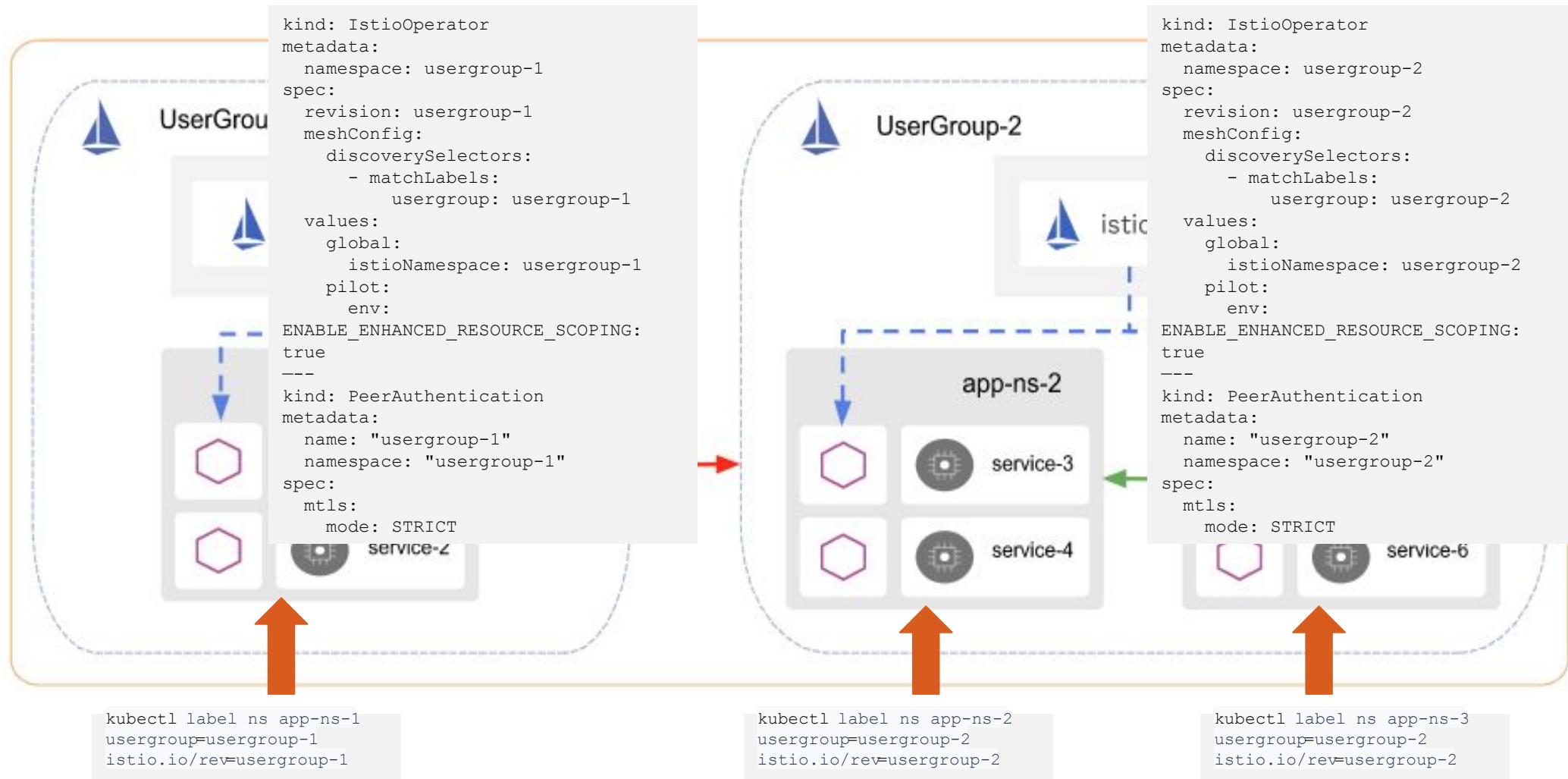


Multiple meshes in a single cluster

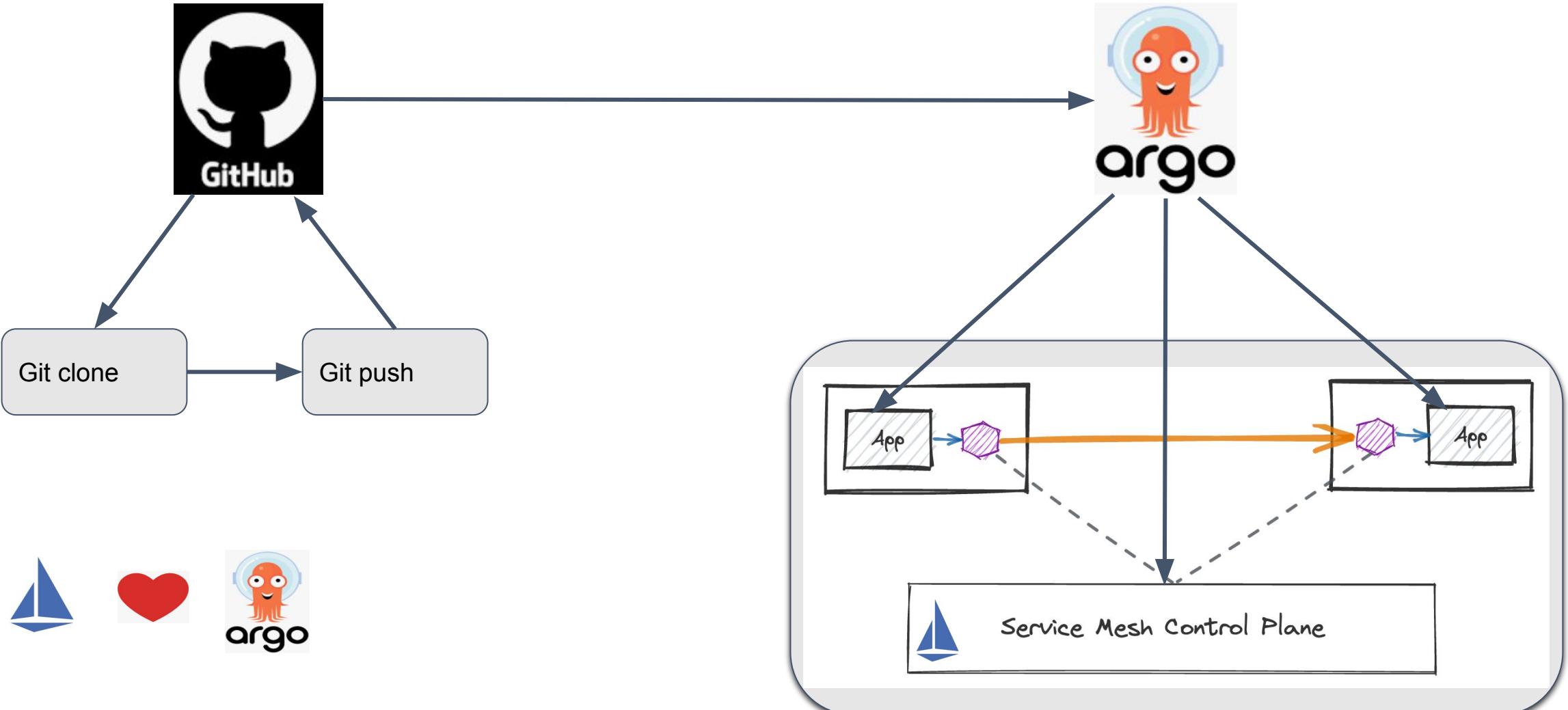
Config Isolation Per Tenant

- A tenant may own 1 or more application namespaces
- Each tenant has a unique control plane
- Istio resources are isolated using the concepts of revisions and discoverySelectors
- Guarded with an experimental flag
`ENABLE_ENHANCED_RESOURCE_SCOPING`
- No longer need `exportTo` for config isolation

Multiple CP - Config Isolation



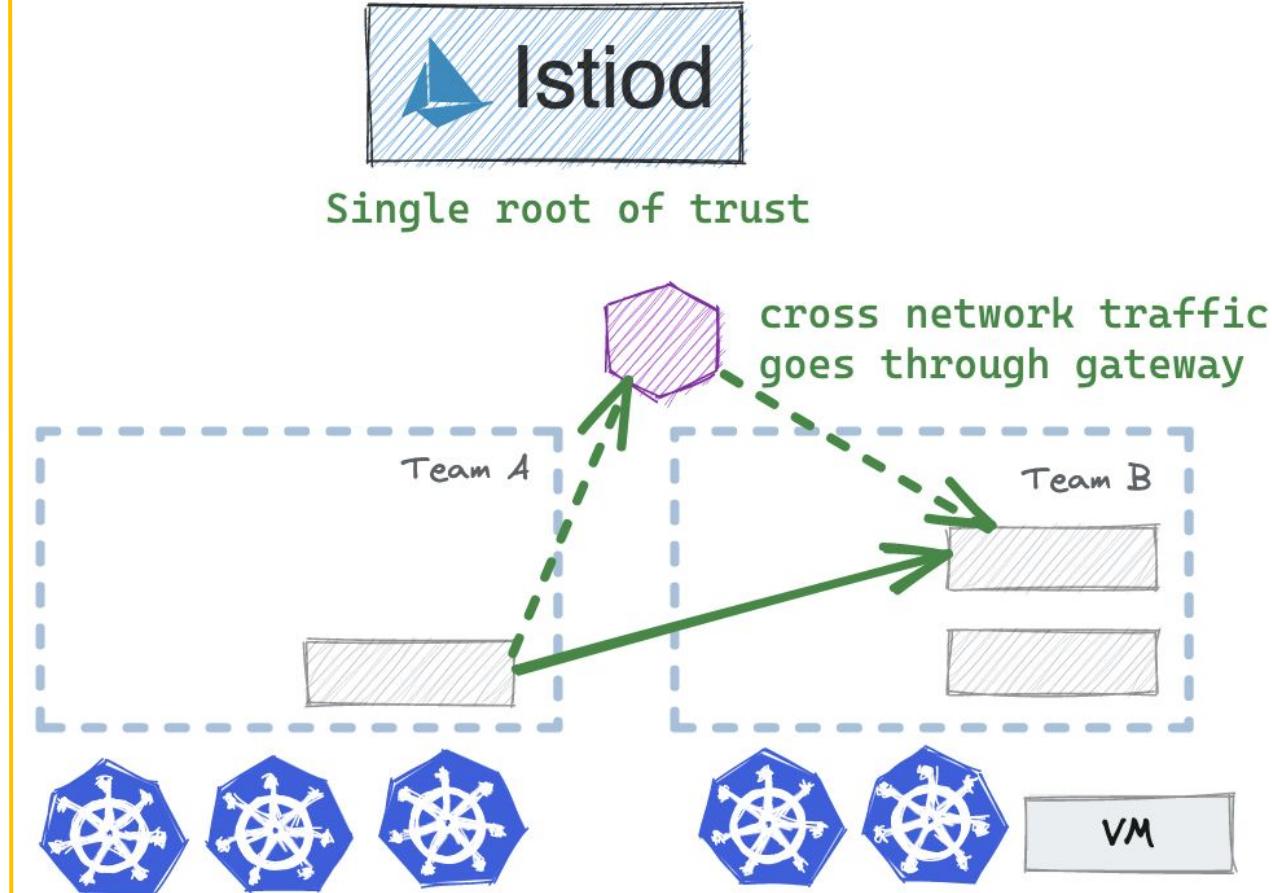
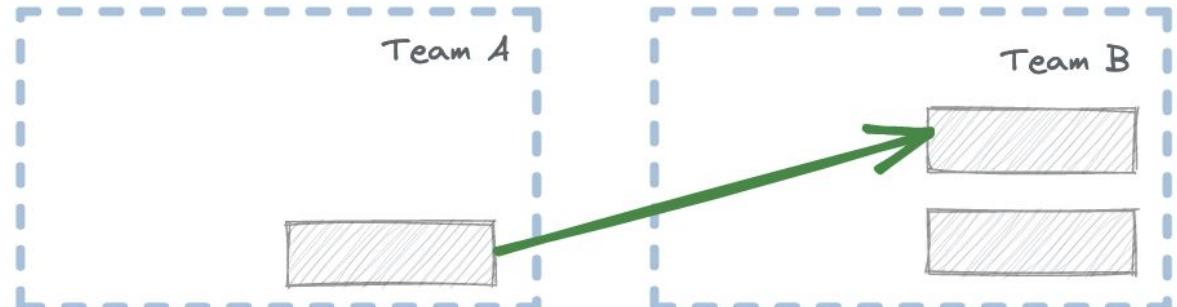
Operate with ArgoCD - Demo



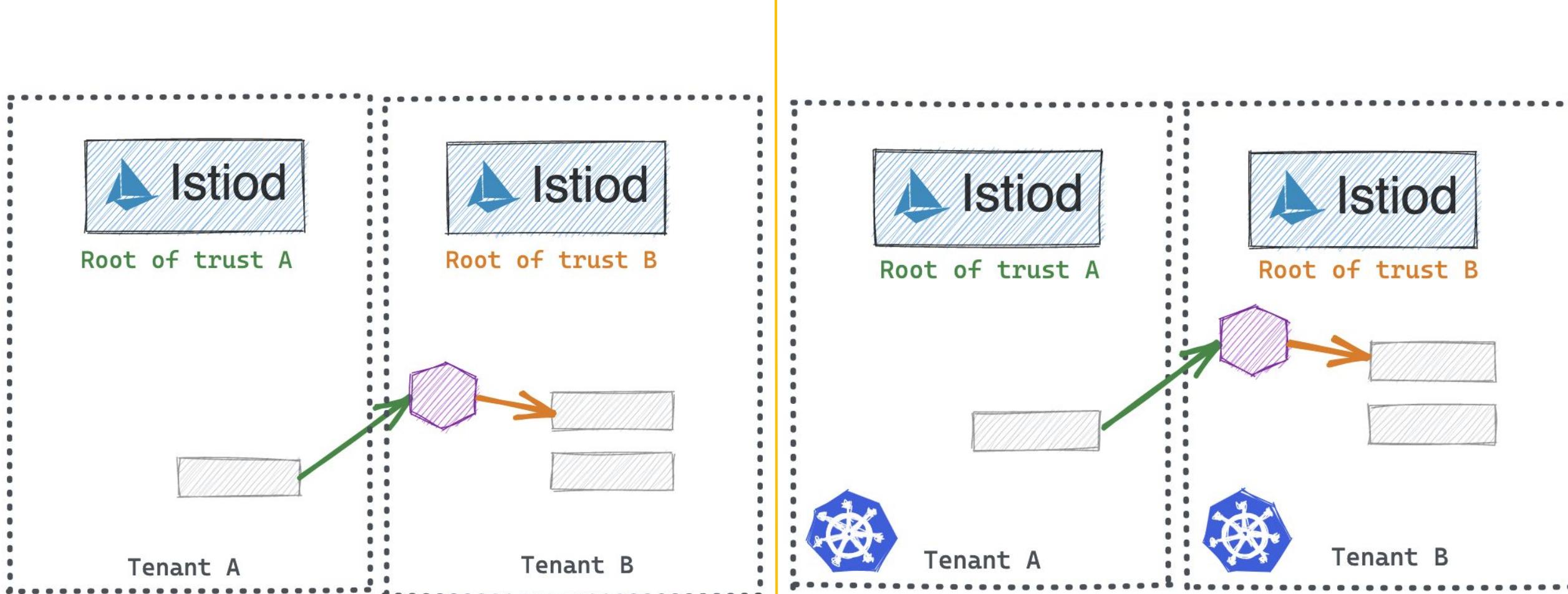
Summarize Multi-Tenancy Service Mesh



Single root of trust



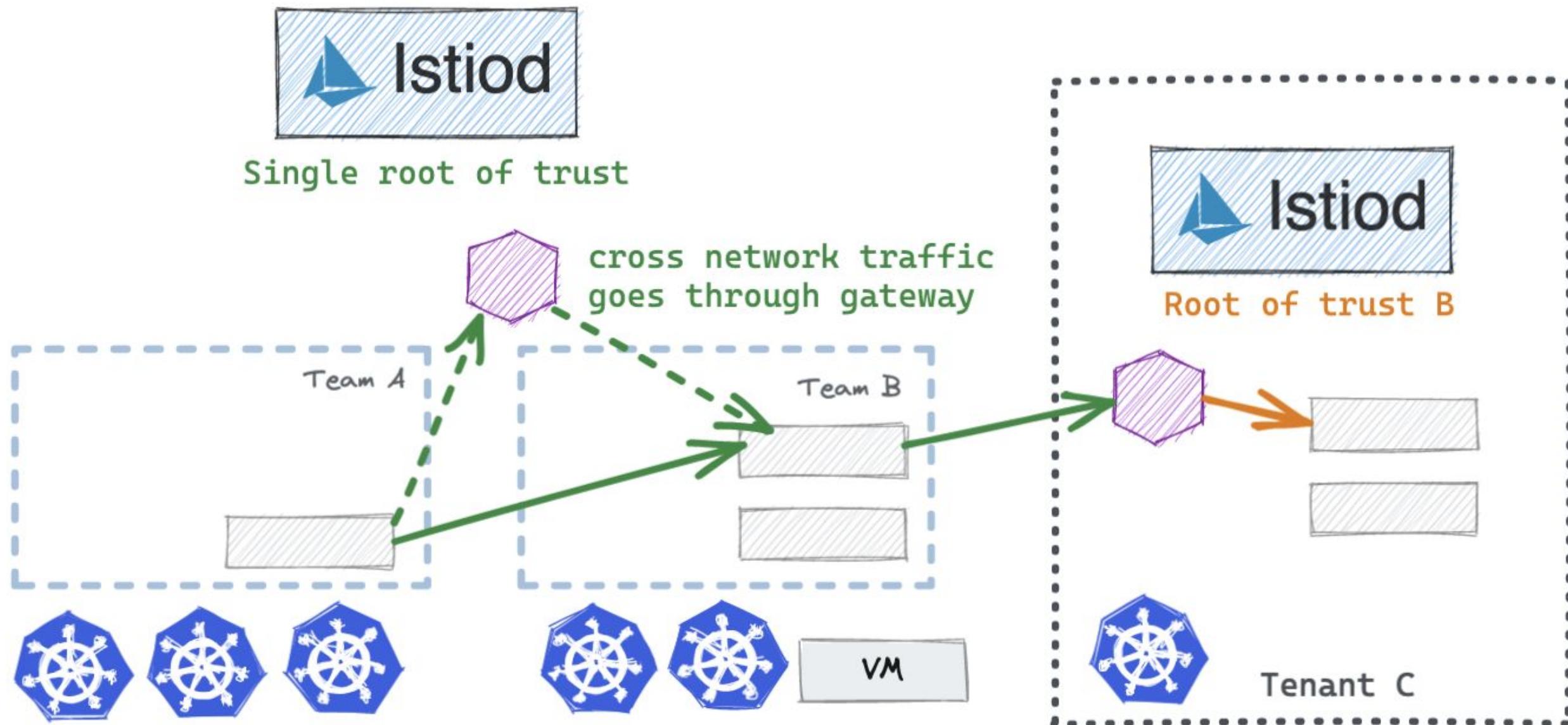
Summarize Multi-Tenancy Service Mesh



Single Mesh vs Multiple Mesh

Type	Pros	Cons
Single Mesh, Single or Multi-Clusters	<ul style="list-style-type: none">Native Istio supportWith recent enhancements, config made simpler (experimental)Only 1 control plane to manage, less resources required by control planeBattle tested and deployed in most production environments	<ul style="list-style-type: none">Careful additional config neededSingle root CA shared across tenants<ul style="list-style-type: none">Could be intended
Multiple Mesh, Single Cluster	<ul style="list-style-type: none">With recent enhancements, readily configurable using revisions and discoverySelectors (experimental)Unique root CA per tenantAligns well with the default istio paradigm of single mesh per istio control plane.Separate versions/life cycle management possible per tenant	<ul style="list-style-type: none">Shared CRDsMore resource consumption compared to Single Control Plane
Mutiple Mesh, Multiple clusters	<ul style="list-style-type: none">Multi tenant by defaultUnique root CA per tenant	<ul style="list-style-type: none">Maintenance overheadResource overhead

Mixed Multi-Tenancy Models



References

- [Getting Started - Argo CD - Declarative GitOps CD for Kubernetes \(argo-cd.readthedocs.io\)](#)
- [Istio / Traffic Management Best Practices](#)
- [Istio - Argo Rollouts - Kubernetes Progressive Delivery Controller \(argo-rollouts.readthedocs.io\)](#)
- [Istio RFC: Simplify Istio Multi Tenancy.docx - Google Docs](#)
- [Istio / Install Multiple Istio Control Planes in a Single Cluster](#)
- [Single Mesh vs Multi Mesh- trade-offs for enterprise multi-tenant support \(sched.com\)](#)
- [Manifests used for the demo](#)



KubeCon



CloudNativeCon

Europe 2023



Thank You!

