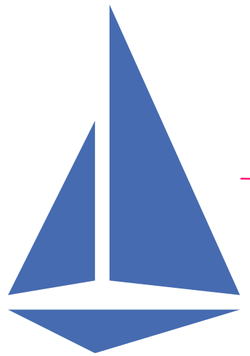
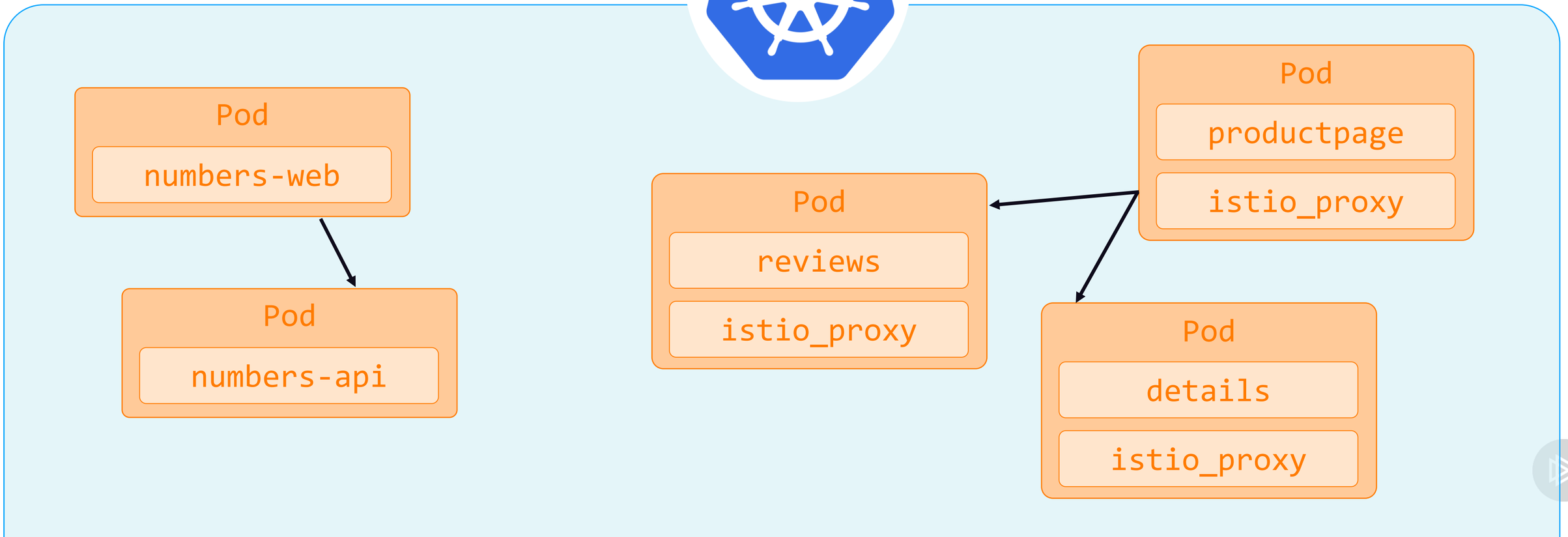
Running Istio in Production

Elton Stoneman
Freelance Consultant and Trainer

@EltonStoneman | blog.sixeyed.com



- Configuration
- Process
- Migration



```
helm upgrade --install istio-base istio/base
helm upgrade --install istiod istio/istiod
helm upgrade --install istio-ingress istio/gateway
```

Helm Deployment

Central management

Configurable profiles & settings

Industry standard

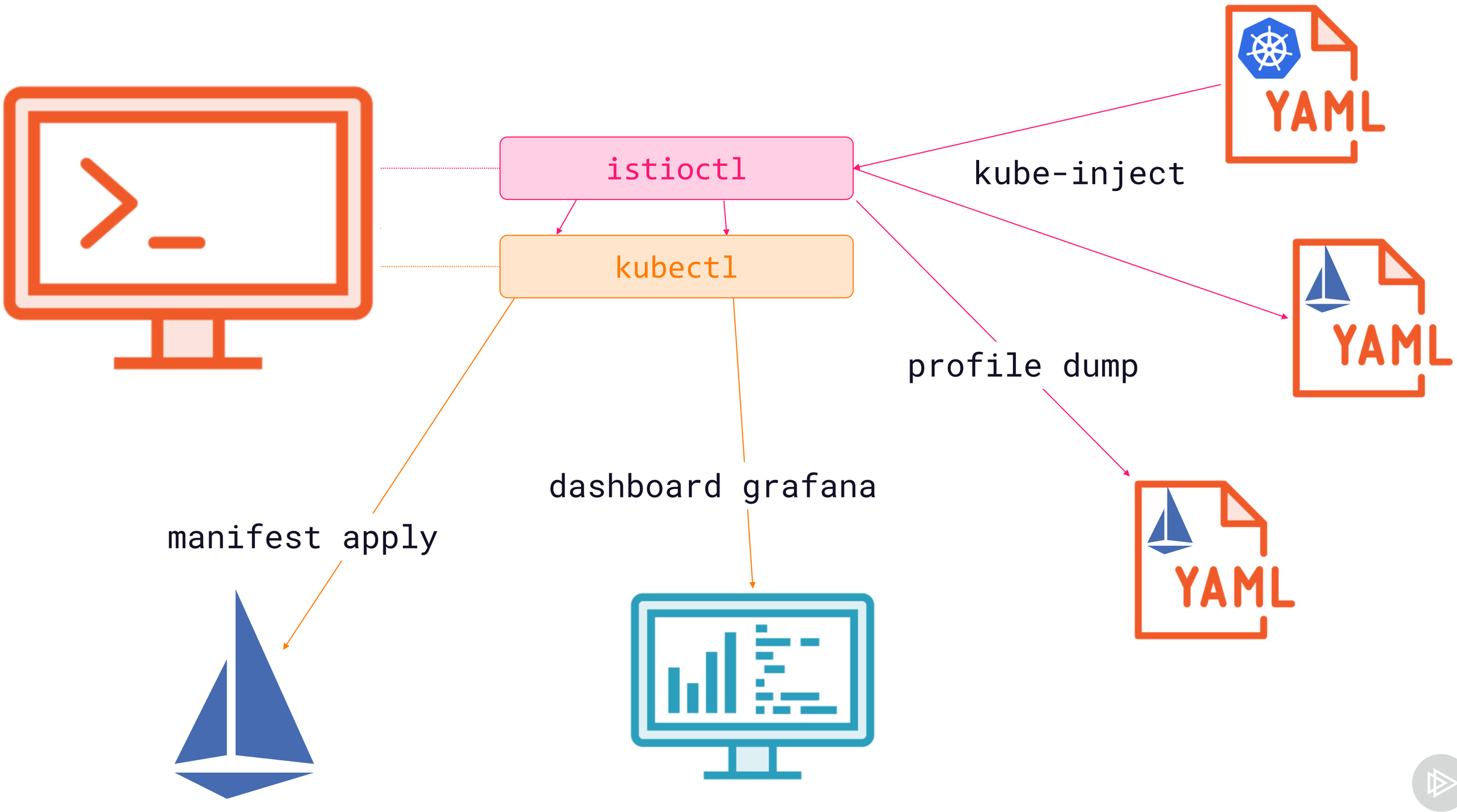
```
istioctl manifest apply
```

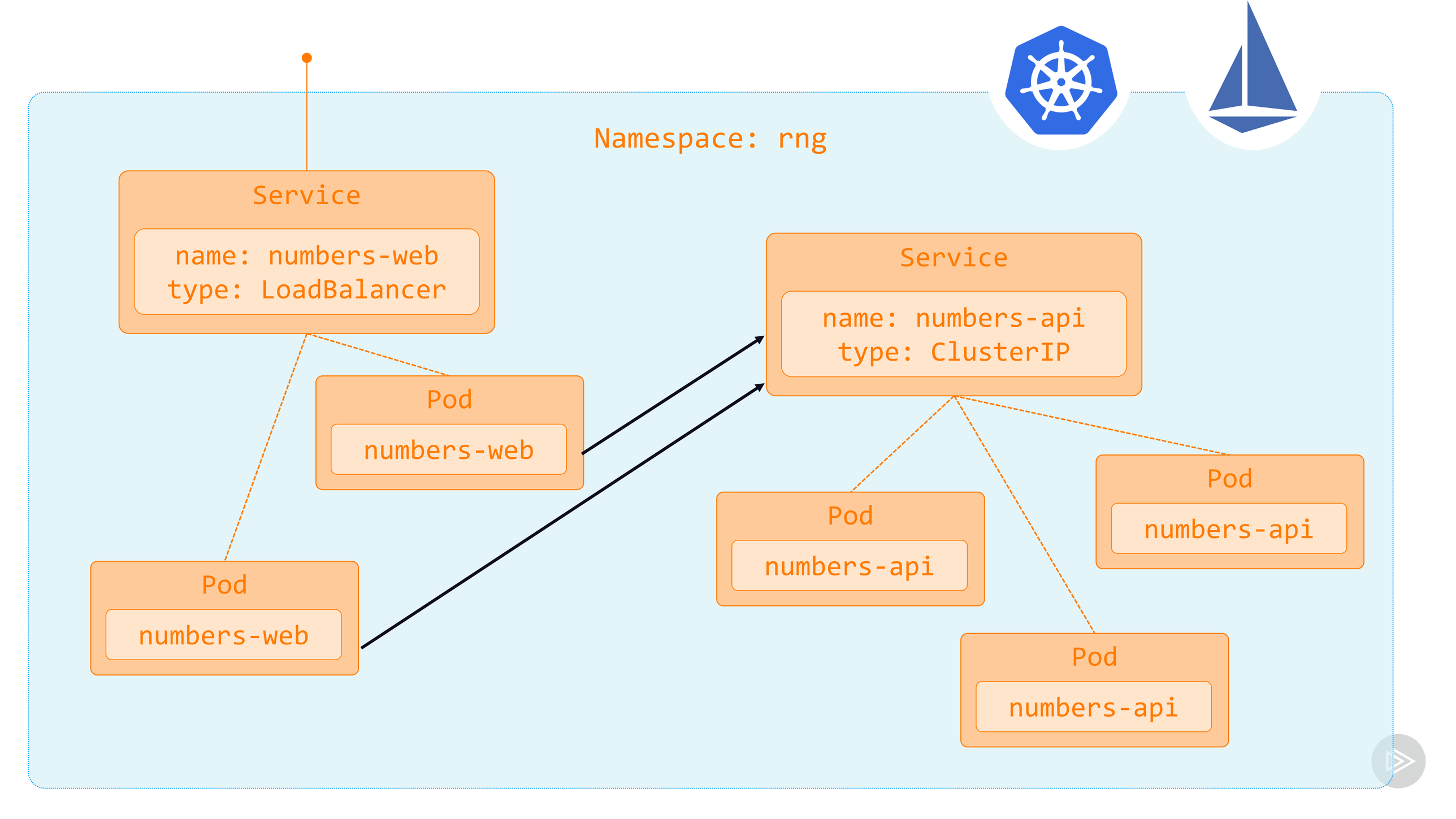
Istioctl Deployment

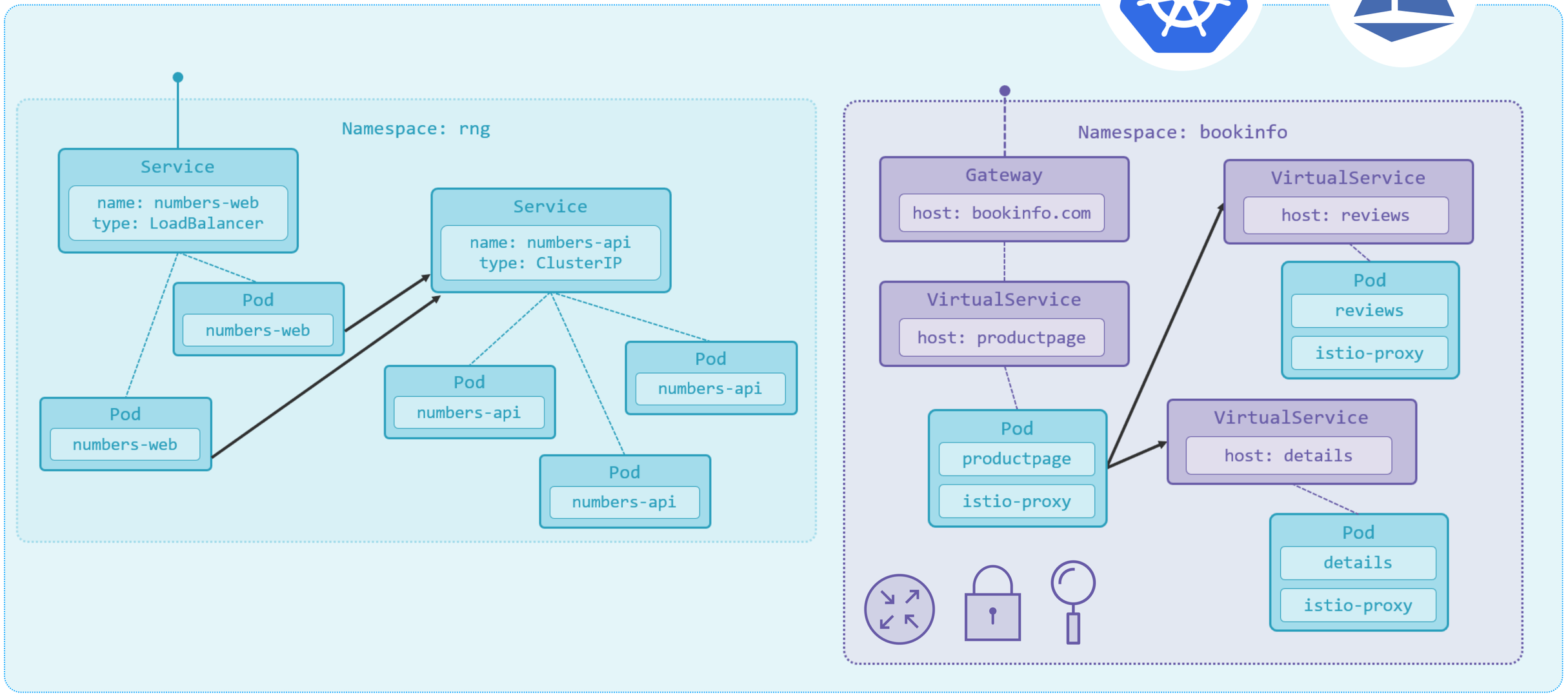
Centralized management

Configurable profiles & settings

Multi-purpose control tool


istioctl
kubectl
kube-inject
profile dump
manifest apply
dashboard grafana
YAML
YAML
YAML

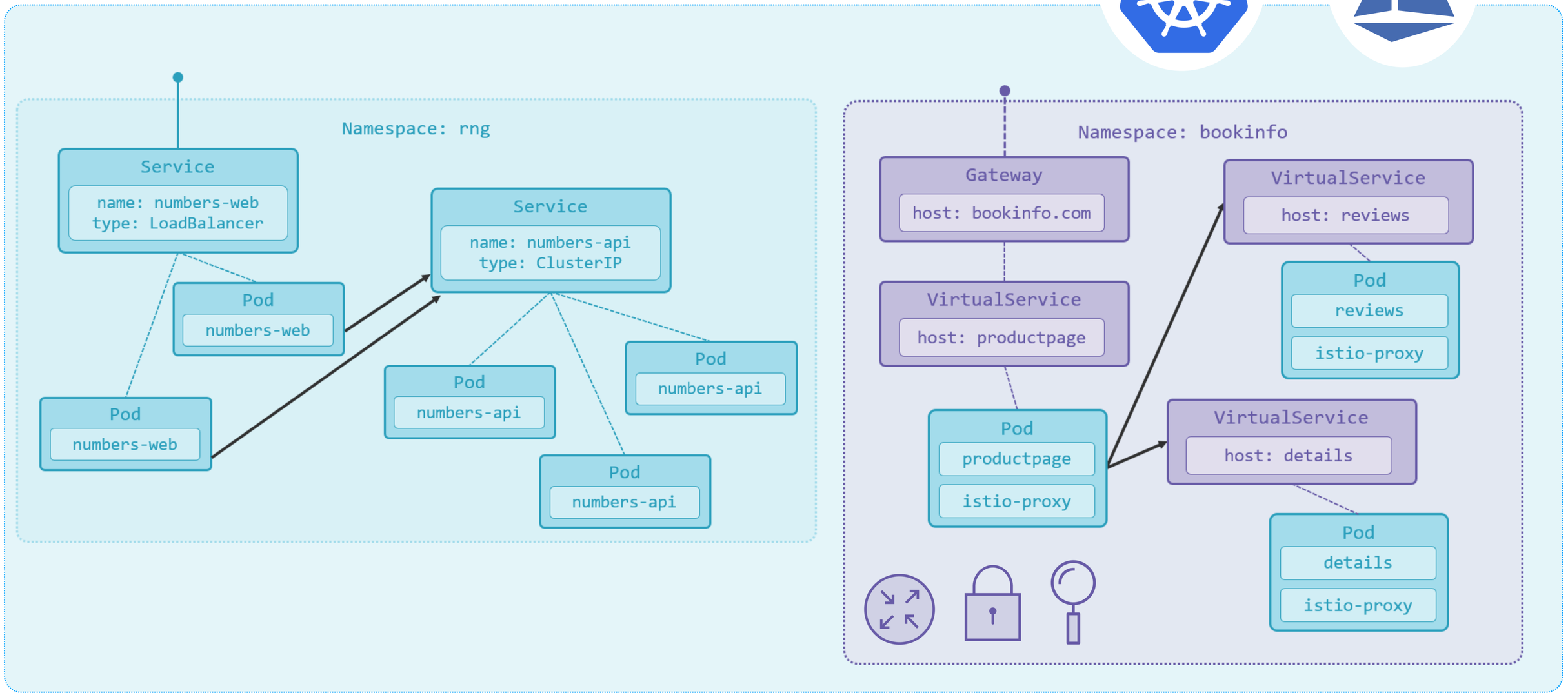

Namespace: rng
Service
name: numbers-web
type: LoadBalancer
Pod
numbers-web
Pod
numbers-web
Service
name: numbers-api
type: ClusterIP
Pod
numbers-api
Pod
numbers-api
Pod
numbers-api


Namespace: rng
Service
name: numbers-web
type: LoadBalancer
Service
name: numbers-api
type: ClusterIP
Pod
numbers-web
Pod
numbers-web
Pod
numbers-api
Pod
numbers-api
Pod
numbers-api
Namespace: bookinfo
Gateway
host: bookinfo.com
VirtualService
host: productpage
VirtualService
host: reviews
Pod
reviews
istio-proxy
Pod
productpage
istio-proxy
VirtualService
host: details
Pod
details
istio-proxy

Demo

Deploying Istio on a Production Cluster

- Configure the deployment
- Don’t touch existing apps
- Deploy an Istio-managed app


Namespace: rng
Service
name: numbers-web
type: LoadBalancer
Service
name: numbers-api
type: ClusterIP
Pod
numbers-web
Pod
numbers-web
Pod
numbers-api
Pod
numbers-api
Pod
numbers-api
Namespace: bookinfo
Gateway
host: bookinfo.com
VirtualService
host: productpage
VirtualService
host: reviews
Pod
reviews
istio-proxy
Pod
productpage
istio-proxy
VirtualService
host: details
Pod
details
istio-proxy

```
istioctl profile list

istioctl profile dump
```

◀ Explore deployment profiles

```
istioctl manifest generate
```

◀ Generate deployment manifests

```
istioctl manifest apply
    -f istio-overrides/aks.yaml
```

◀ Deploy with settings override file

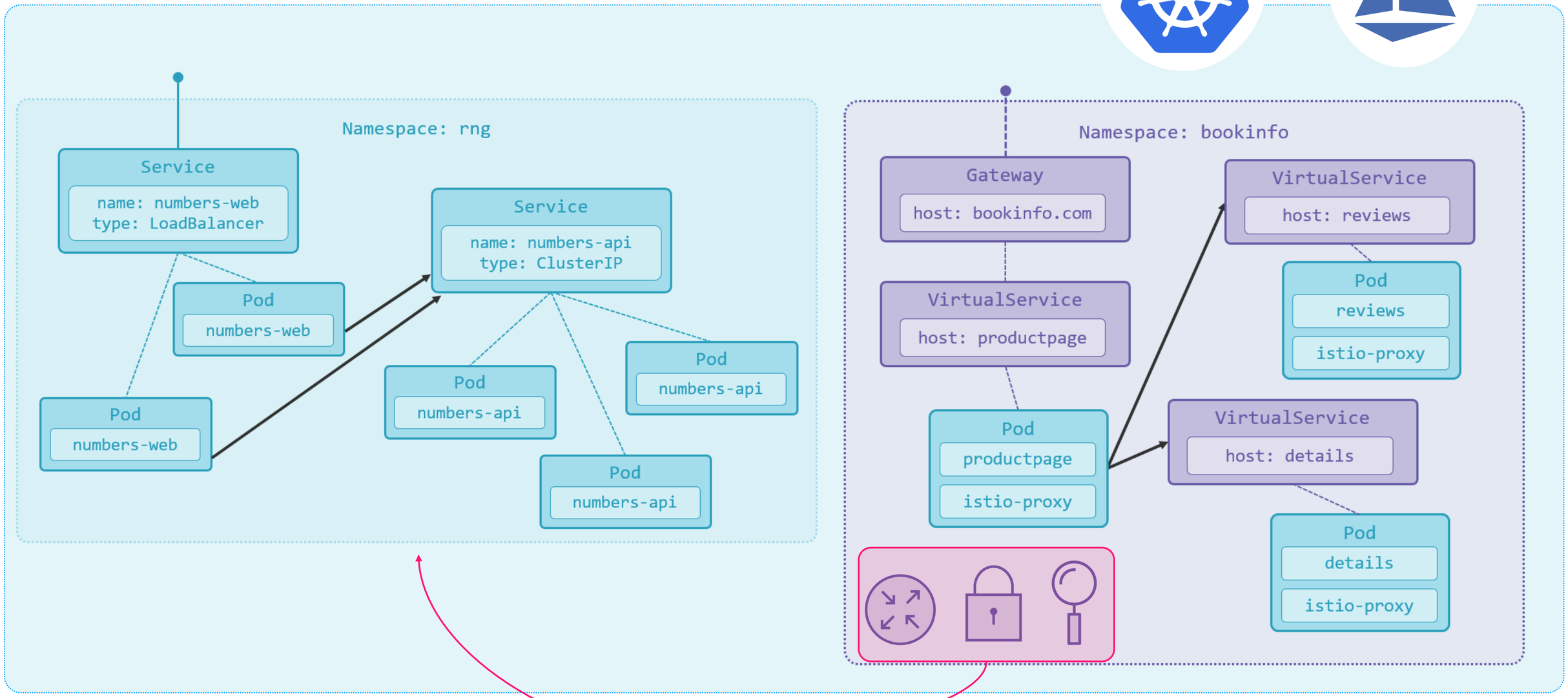
```
istioctl dashboard kiali
```

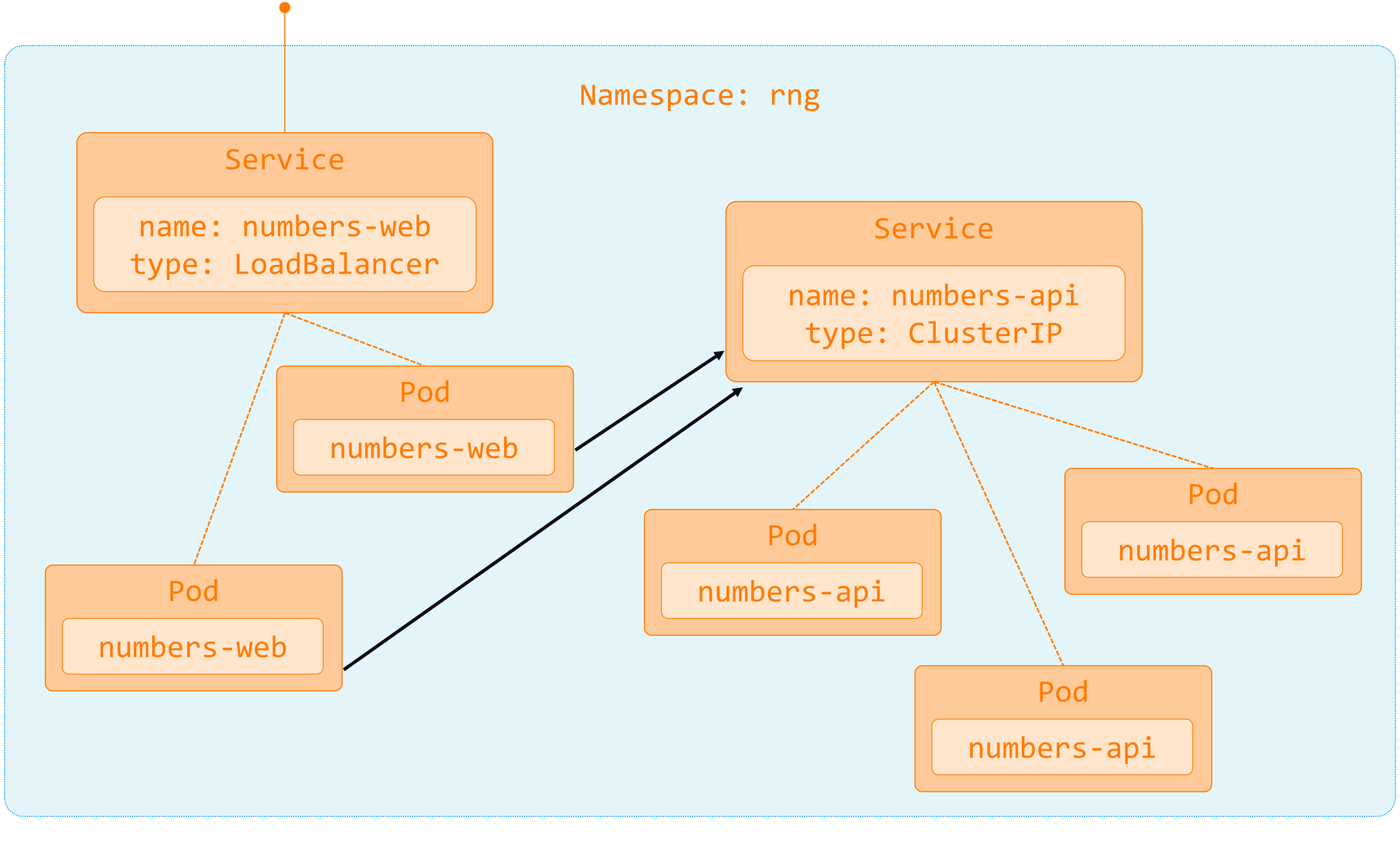
◀ Temporarily enable dashboard access

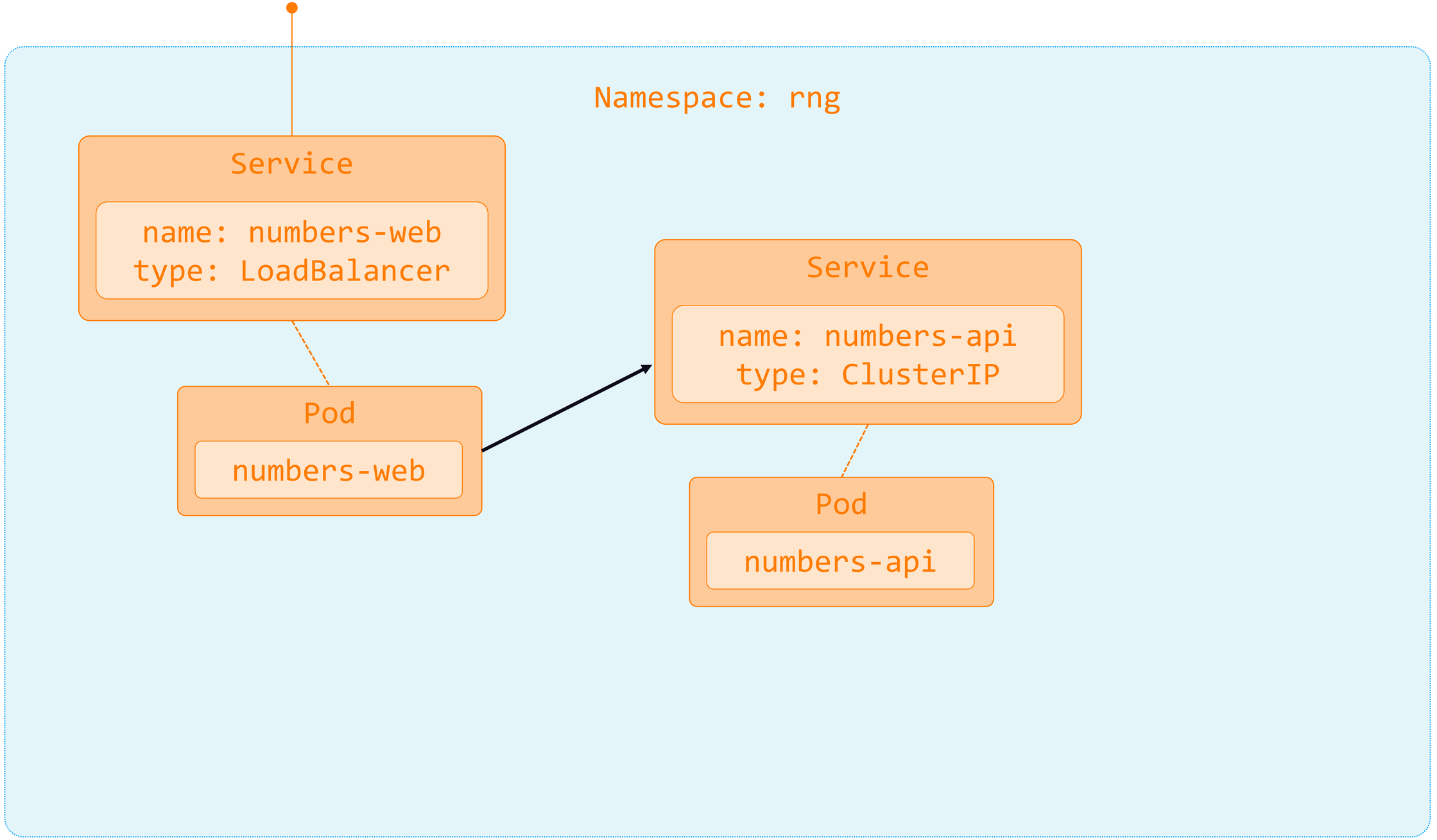
Customized Istio Deployment

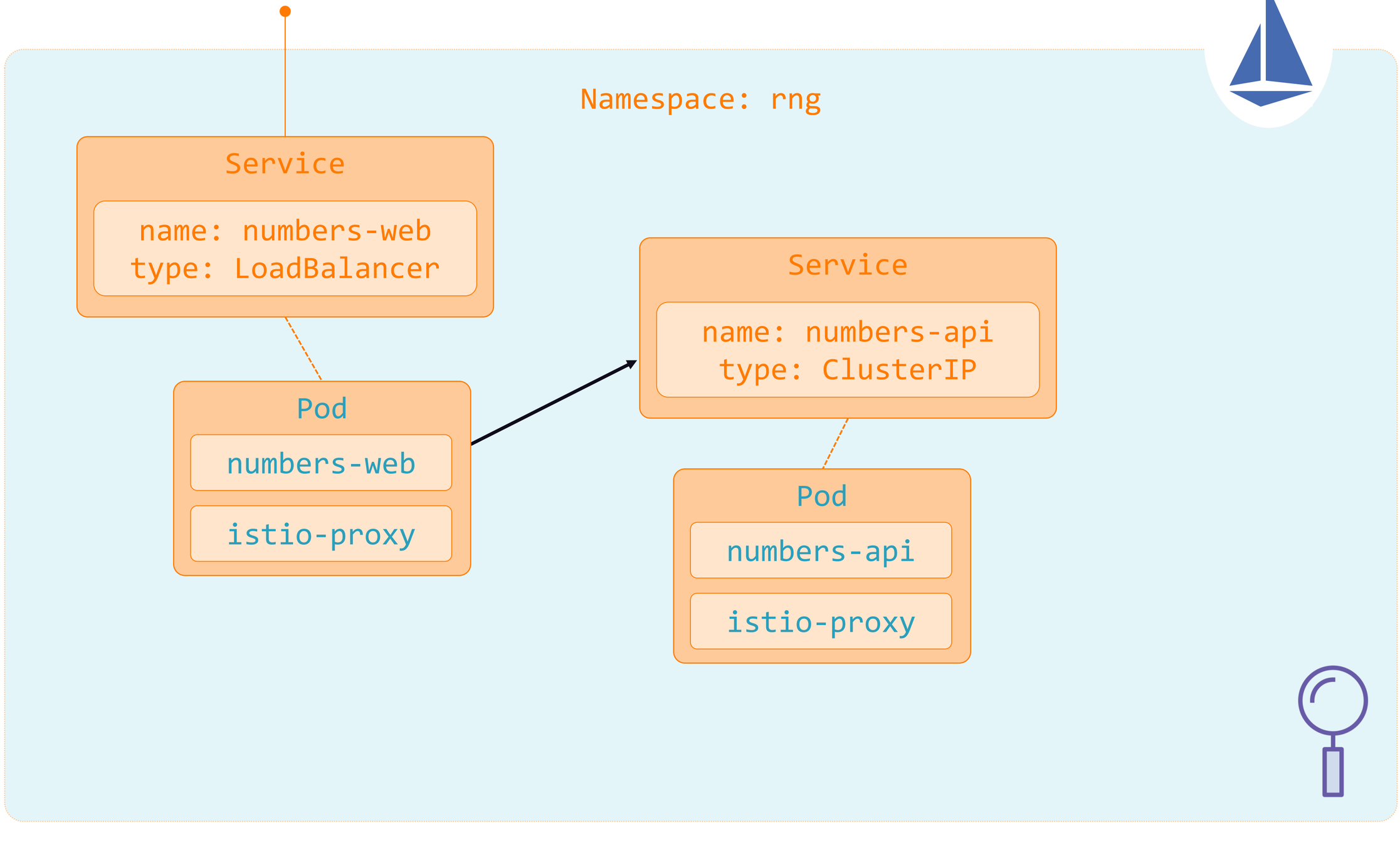
istio-override.yaml

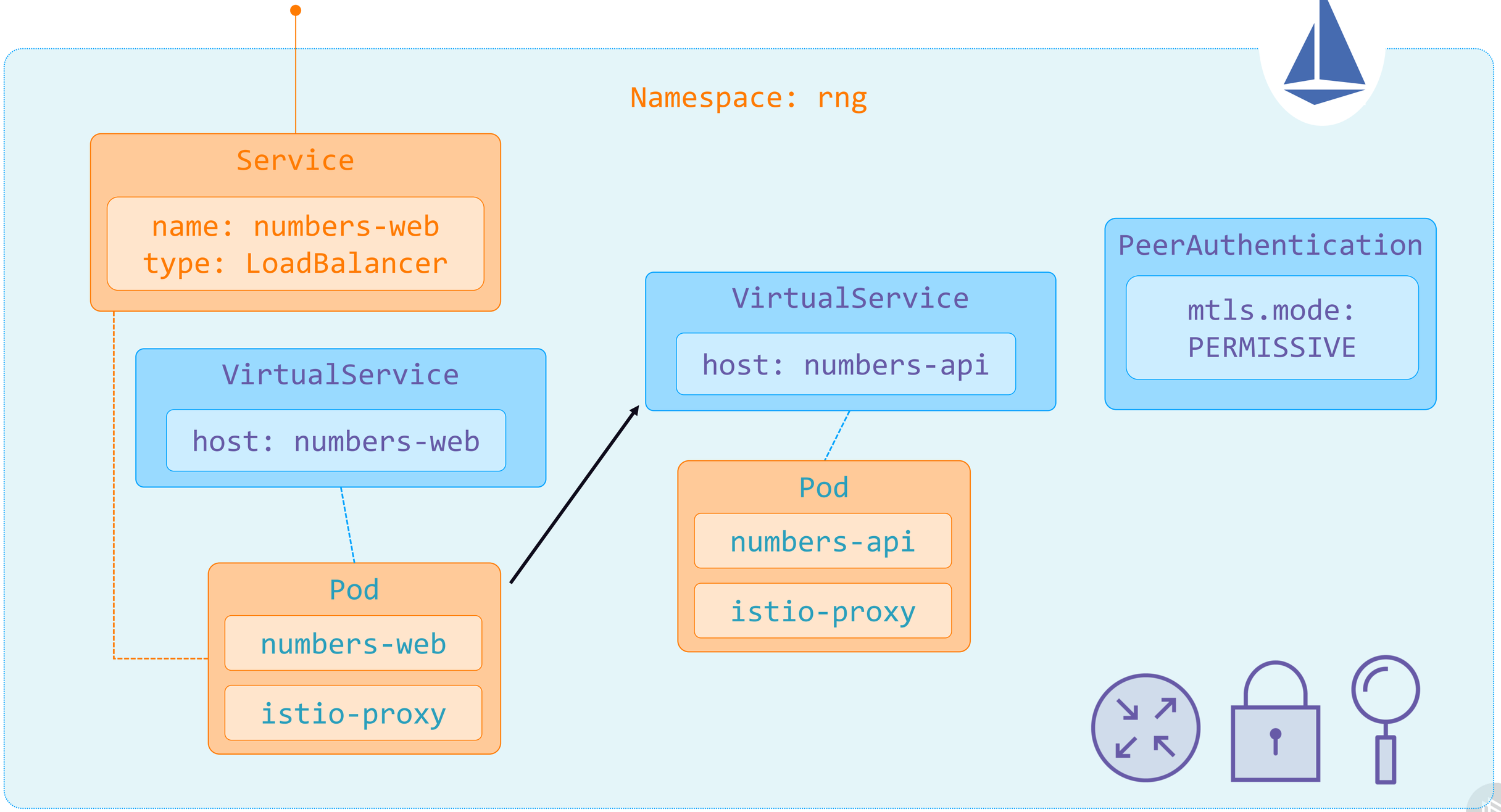
```
apiVersion: install.istio.io/v1alpha1
kind: IstioOperator
metadata:
  namespace: istio-system
  name: istiod
spec:
  profile: default
  values:
    gateways:
      istio-ingressgateway:
        serviceAnnotations:
service.beta.kubernetes.io/azure-dns-label-name:
gatewaysixeyedcom
```

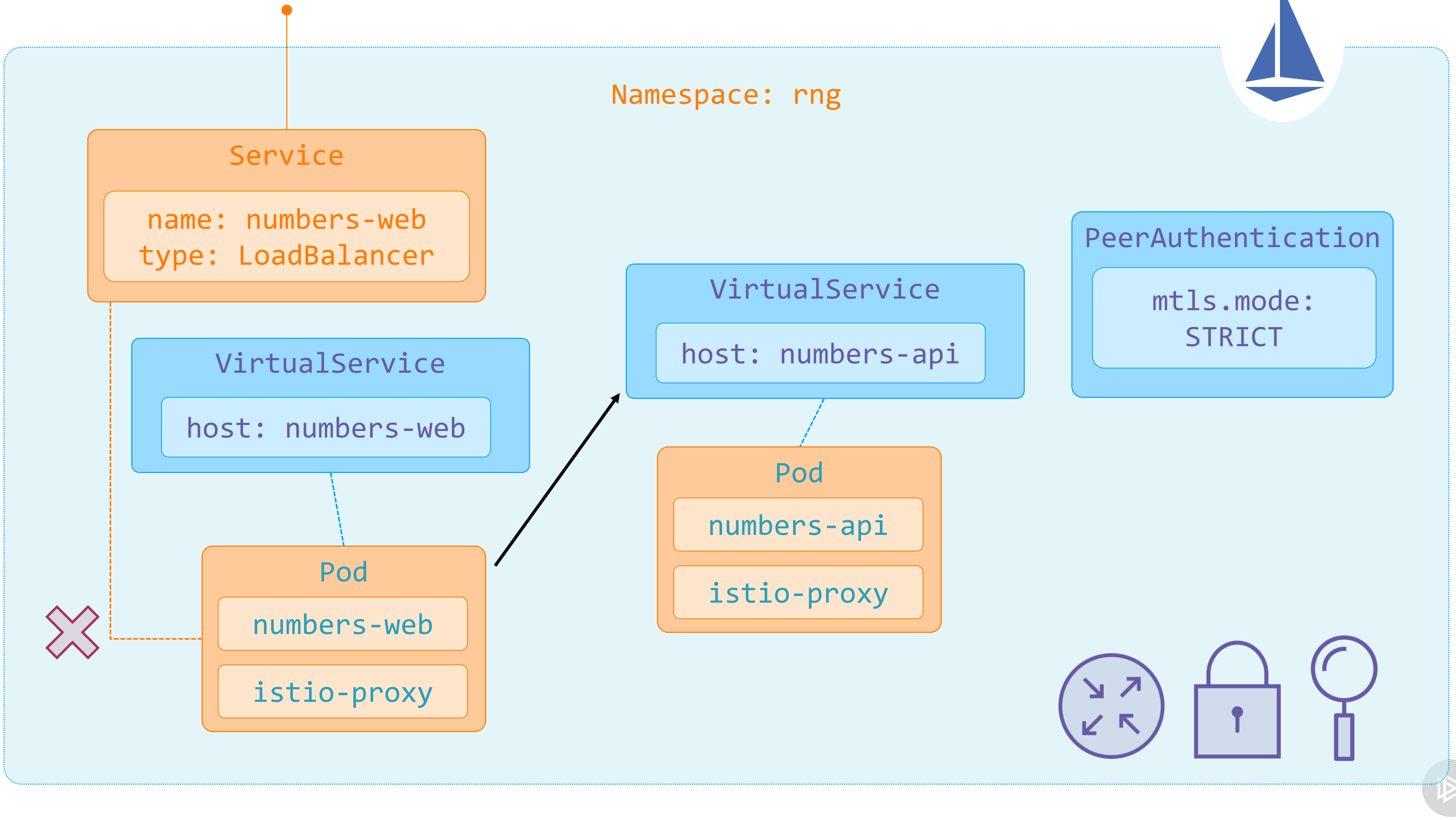

Namespace: rng
Service
name: numbers-web
type: LoadBalancer
Service
name: numbers-api
type: ClusterIP
Pod
numbers-web
Pod
numbers-web
Pod
numbers-api
Pod
numbers-api
Pod
numbers-api
Namespace: bookinfo
Gateway
host: bookinfo.com
VirtualService
host: productpage
VirtualService
host: reviews
Pod
reviews
istio-proxy
Pod
productpage
istio-proxy
VirtualService
host: details
Pod
details
istio-proxy

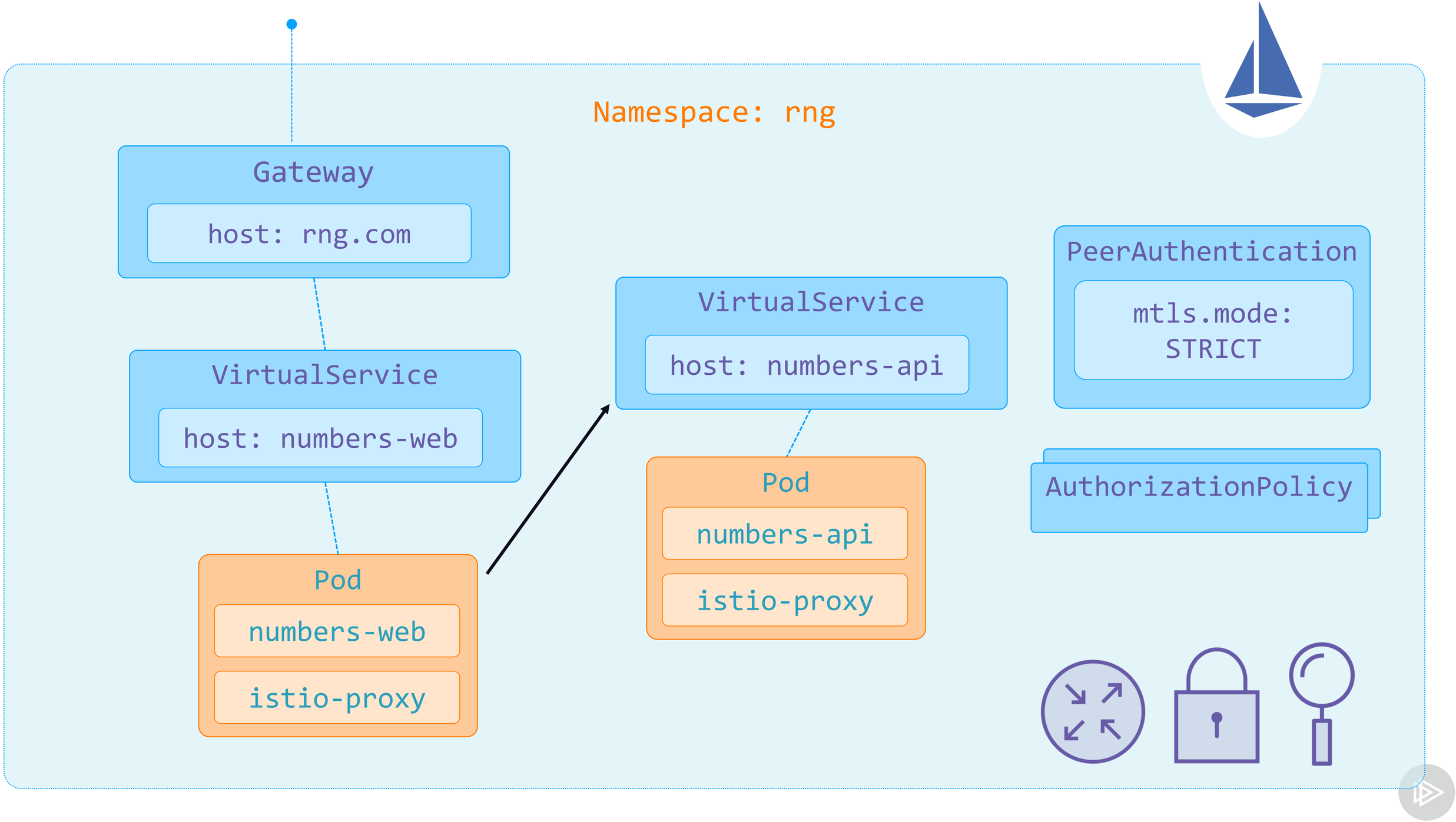

Namespace: rng
Service
name: numbers-web
type: LoadBalancer
Service
name: numbers-api
type: ClusterIP
Pod
numbers-web
Pod
numbers-web
Pod
numbers-api
Pod
numbers-api
Pod
numbers-api

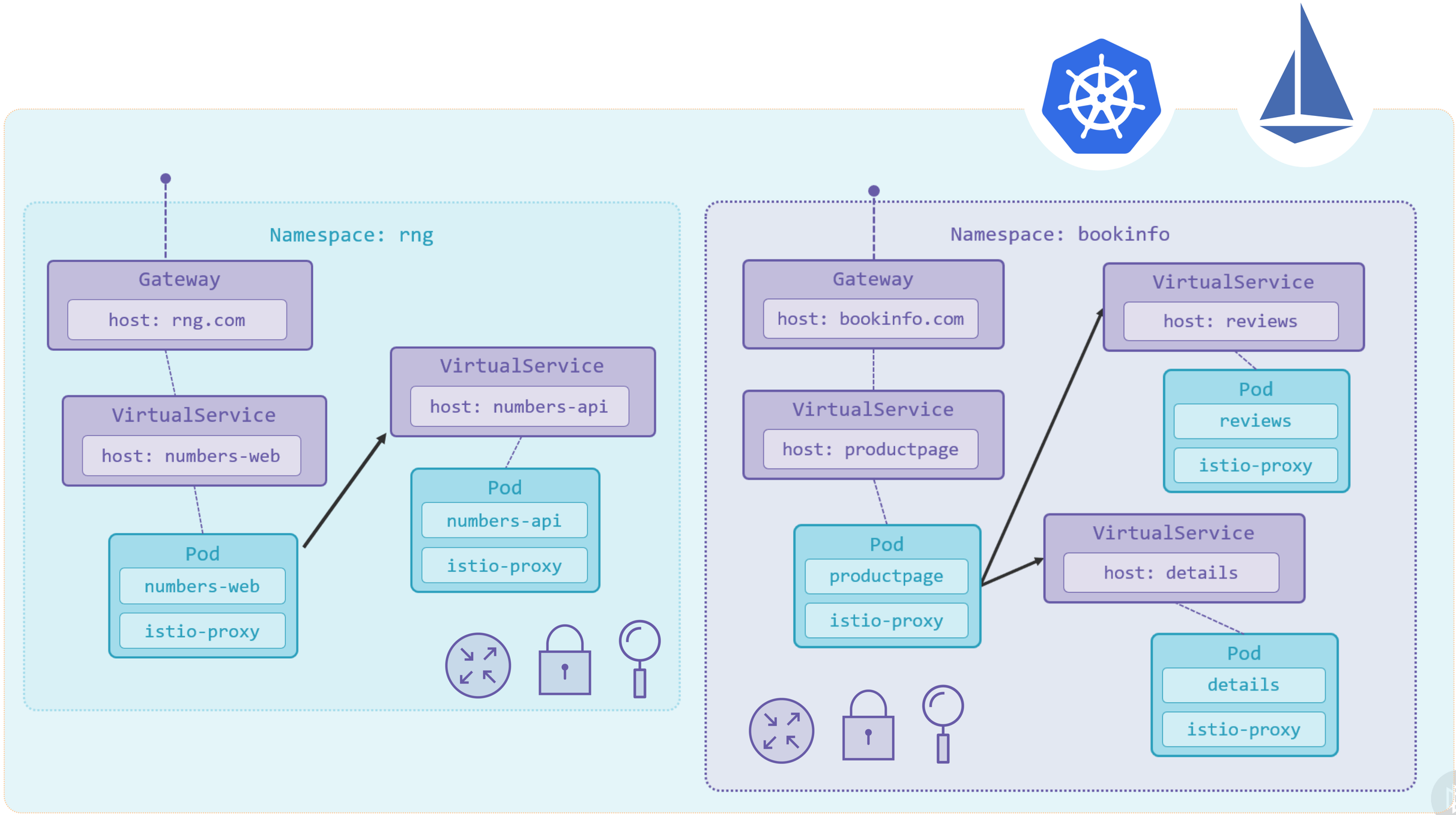

Namespace: rng
Service
name: numbers-web
type: LoadBalancer
Pod
numbers-web
Service
name: numbers-api
type: ClusterIP
Pod
numbers-api


Namespace: rng
Service
name: numbers-web
type: LoadBalancer
Pod
numbers-web
istio-proxy
Service
name: numbers-api
type: ClusterIP
Pod
numbers-api
istio-proxy


Namespace: rng
Service
name: numbers-web
type: LoadBalancer
VirtualService
host: numbers-web
Pod
numbers-web
istio-proxy
VirtualService
host: numbers-api
Pod
numbers-api
istio-proxy
PeerAuthentication
mtls.mode:
PERMISSIVE


Namespace: rng
Service
name: numbers-web
type: LoadBalancer
VirtualService
host: numbers-web
Pod
numbers-web
istio-proxy
VirtualService
host: numbers-api
Pod
numbers-api
istio-proxy
PeerAuthentication
mtls.mode:
STRICT

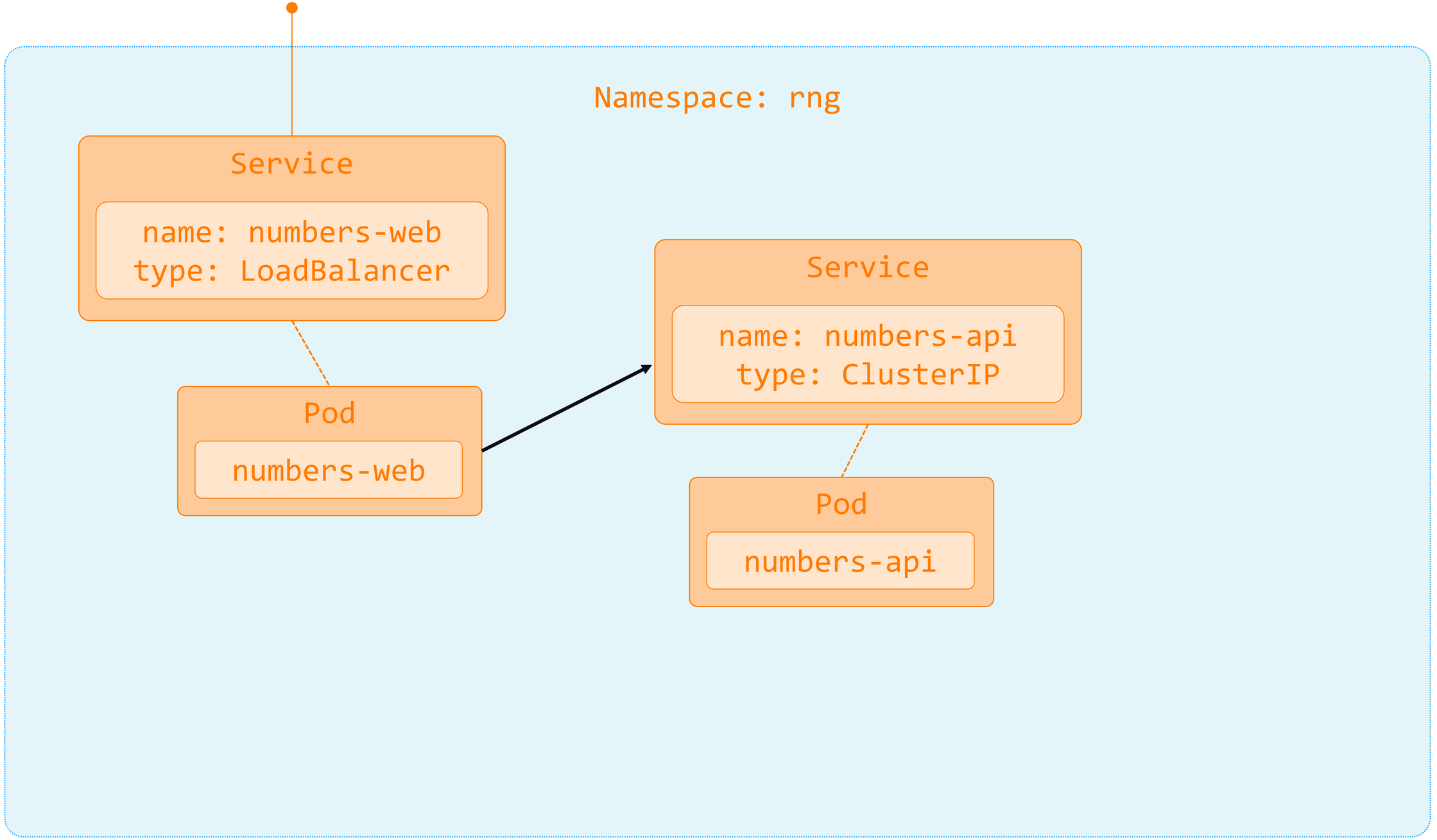

Namespace: rng
Gateway
host: rng.com
VirtualService
host: numbers-web
Pod
numbers-web
istio-proxy
VirtualService
host: numbers-api
Pod
numbers-api
istio-proxy
PeerAuthentication
mtls.mode:
STRICT
AuthorizationPolicy

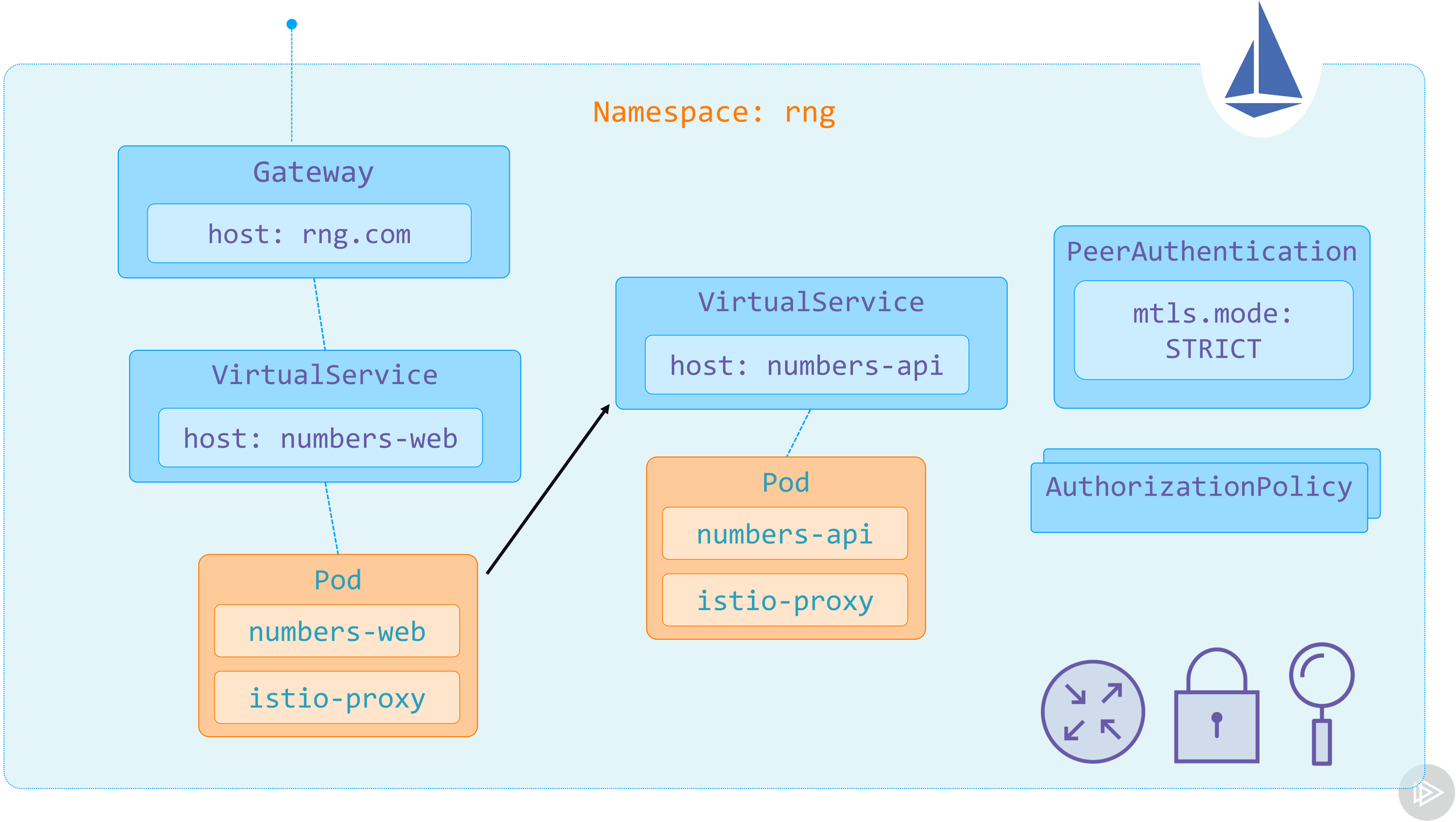

Namespace: rng
Gateway
host: rng.com
VirtualService
host: numbers-web
Pod
numbers-web
istio-proxy
VirtualService
host: numbers-api
Pod
numbers-api
istio-proxy
Namespace: bookinfo
Gateway
host: bookinfo.com
VirtualService
host: productpage
Pod
productpage
istio-proxy
VirtualService
host: reviews
Pod
reviews
istio-proxy
VirtualService
host: details
Pod
details
istio-proxy

Demo

Migrating an Existing App to Istio

- Injecting proxy side-cars
- Upgrading to mutual TLS
- Routing traffic with a gateway


Namespace: rng
Service
name: numbers-web
type: LoadBalancer
Pod
numbers-web
Service
name: numbers-api
type: ClusterIP
Pod
numbers-api


Namespace: rng
Gateway
host: rng.com
VirtualService
host: numbers-web
Pod
numbers-web
istio-proxy
VirtualService
host: numbers-api
Pod
numbers-api
istio-proxy
PeerAuthentication
mtls.mode:
STRICT
AuthorizationPolicy

Configuring mTLS

auth.yaml

```
apiVersion: security.istio.io/v1beta1
kind: PeerAuthentication
metadata:
  name: default
  namespace: rng
spec:
  mtls:
   mode: PERMISSIVE
```

Proxy Injection

Configured by workload

namespace.yaml

```yaml
apiVersion: v1
kind: Namespace
metadata:
  name: rng
  labels:
    istio-injection: disabled
```

deployment.yaml

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: numbers-api
  namespace: rng
spec:
  template:
    metadata:
      labels:
sidecar.istio.io/inject: 'true'
```

Routing with mTLS

virtual-service.yaml

```
apiVersion: networking.istio.io/v1beta1
kind: VirtualService
metadata:
  namespace: rng
  name: numbers-web
spec:
  hosts:
  - rng.sixeyed.com
  gateways:
    - istio-system/ingressgateway
  exportTo:
    - istio-system
  http:
    - route:
      - destination:
          host: numbers-web
```

Securing Access – Web to API

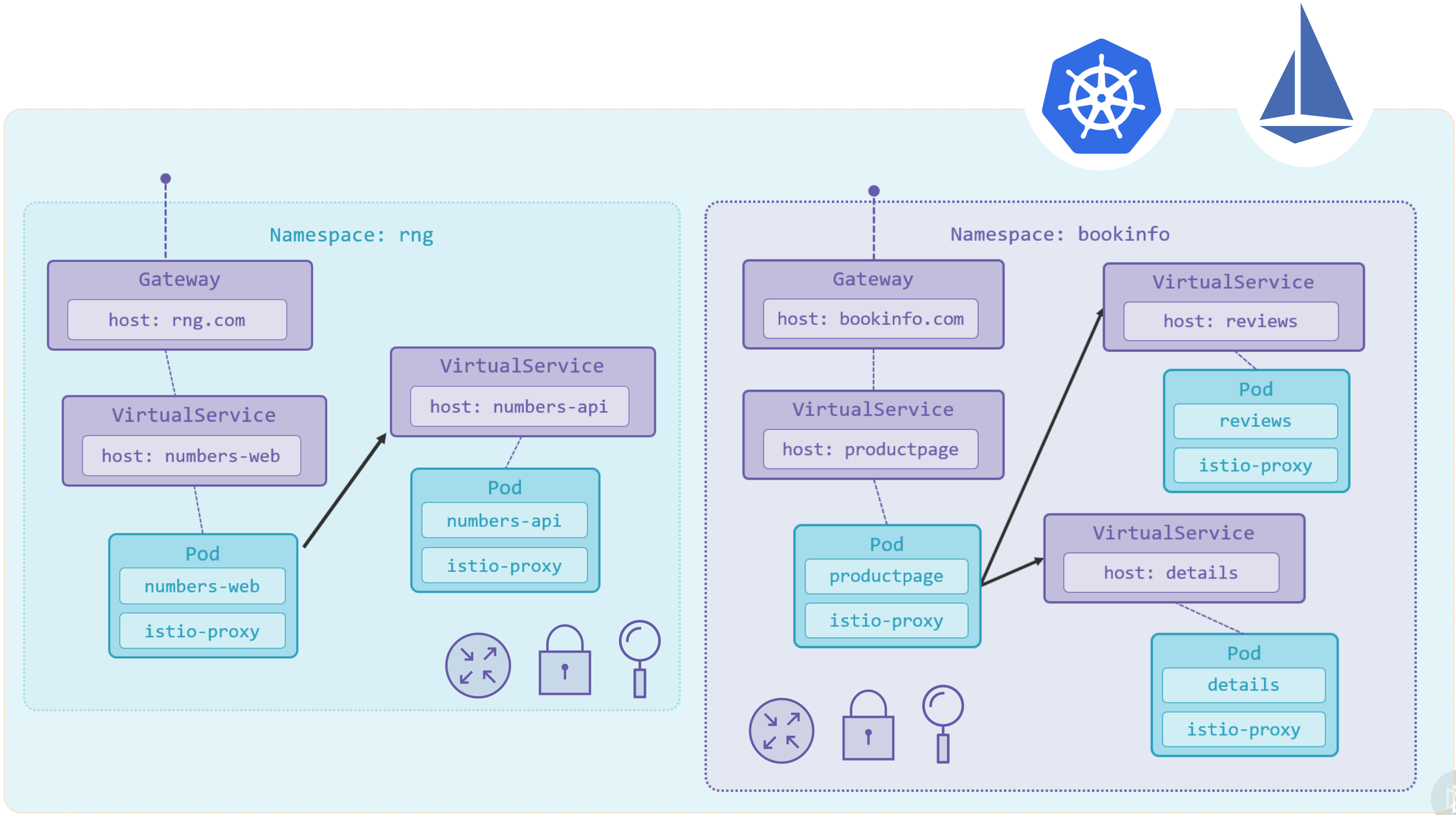
auth-api.yaml

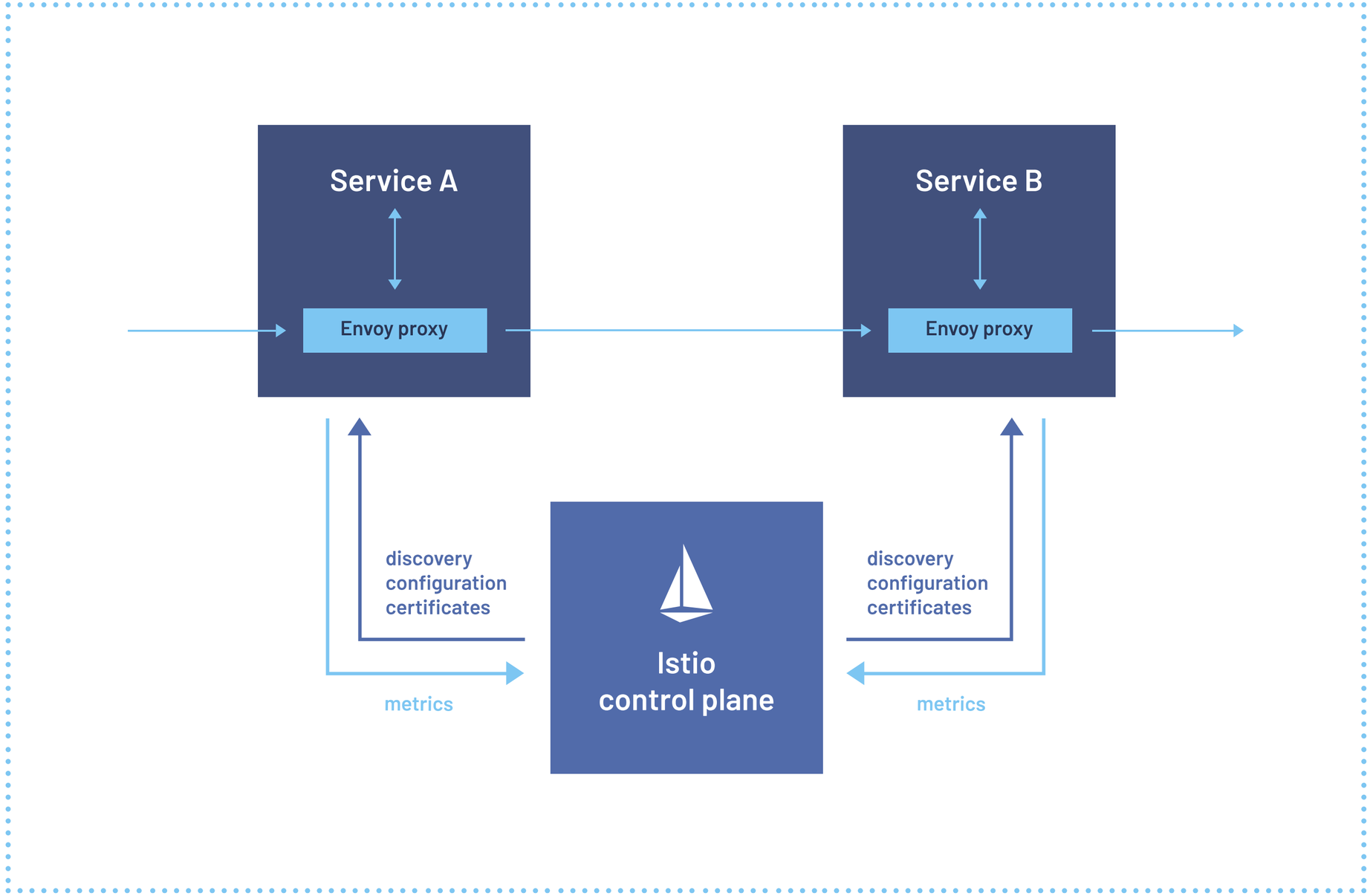
```yaml
apiVersion: security.istio.io/v1
kind: AuthorizationPolicy
metadata:
 name: numbers-api-authz
 namespace: rng
spec:
 selector:
  matchLabels:
   app: numbers-api
 action: ALLOW
 rules:
  - from:
   - source:
      principals: [".../ns/rng/sa/numbers-web"]
   to:
    - operation:
       methods: ["GET"]
```

Securing Access – Gateway to Web

auth-api.yaml

```yaml
apiVersion: security.istio.io/v1
kind: AuthorizationPolicy
metadata:
 name: numbers-web-authz
 namespace: rng
spec:
 selector:
  matchLabels:
   app: numbers-web
 action: ALLOW
 rules:
 - from:
  - source:
     principals:[".../sa/istio-ingressgateway"]
  to:
  - operation:
     methods: ["GET"]
```


Namespace: rng
Gateway
host: rng.com
VirtualService
host: numbers-web
Pod
numbers-web
istio-proxy
VirtualService
host: numbers-api
Pod
numbers-api
istio-proxy
Namespace: bookinfo
Gateway
host: bookinfo.com
VirtualService
host: productpage
Pod
productpage
istio-proxy
VirtualService
host: reviews
Pod
reviews
istio-proxy
VirtualService
host: details
Pod
details
istio-proxy



Source: github.com/istio/istio.io

Failure Scenarios

Routing

Proxies cache config

Existing pods get stale

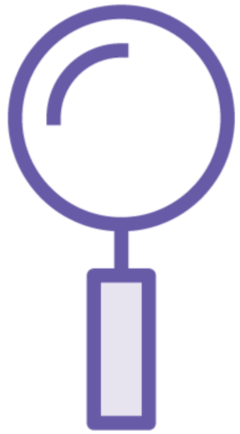
New pods cannot start

Security

Proxies cache certs

Certificates expire

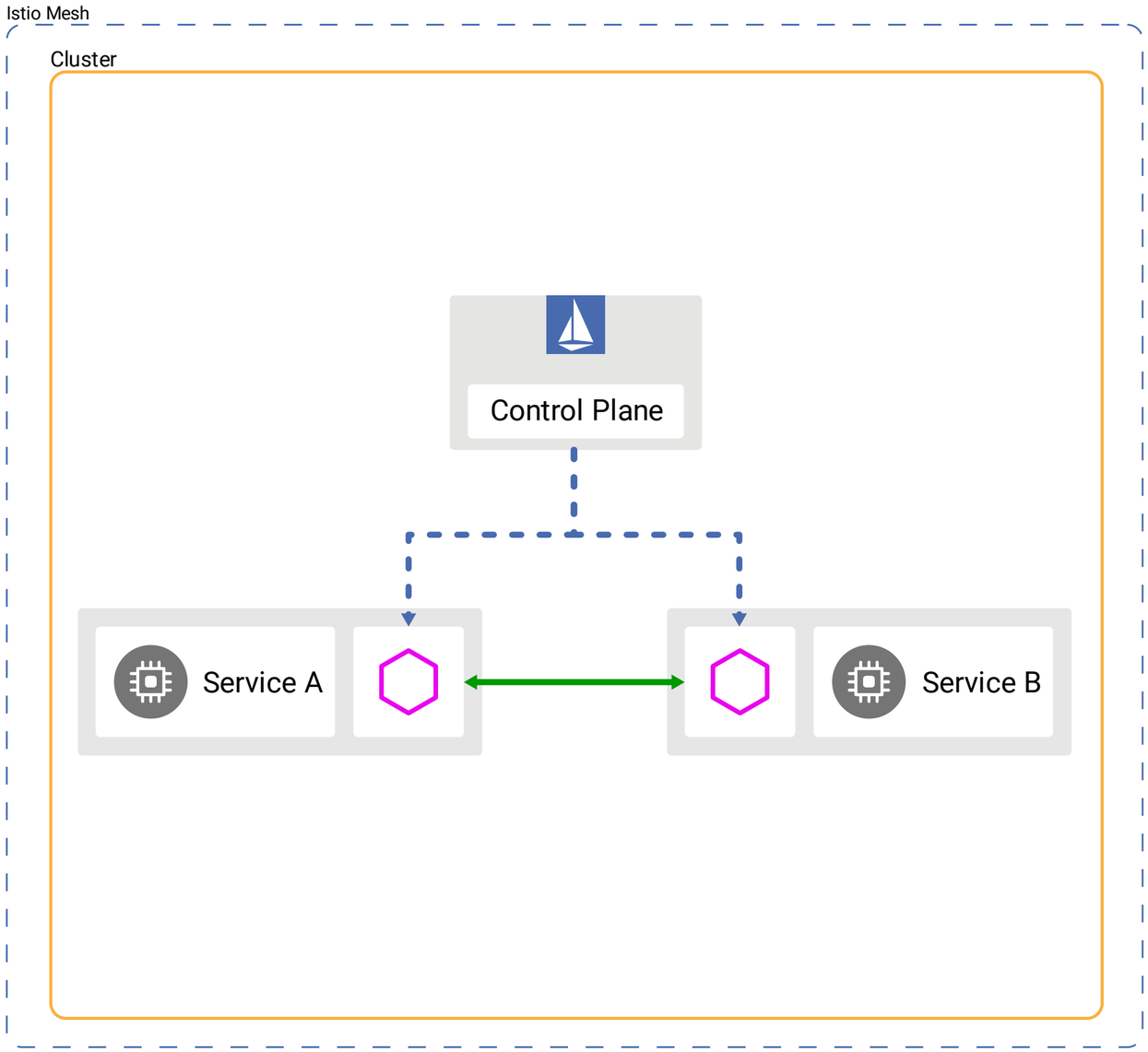
Policy assertions fail



Observability

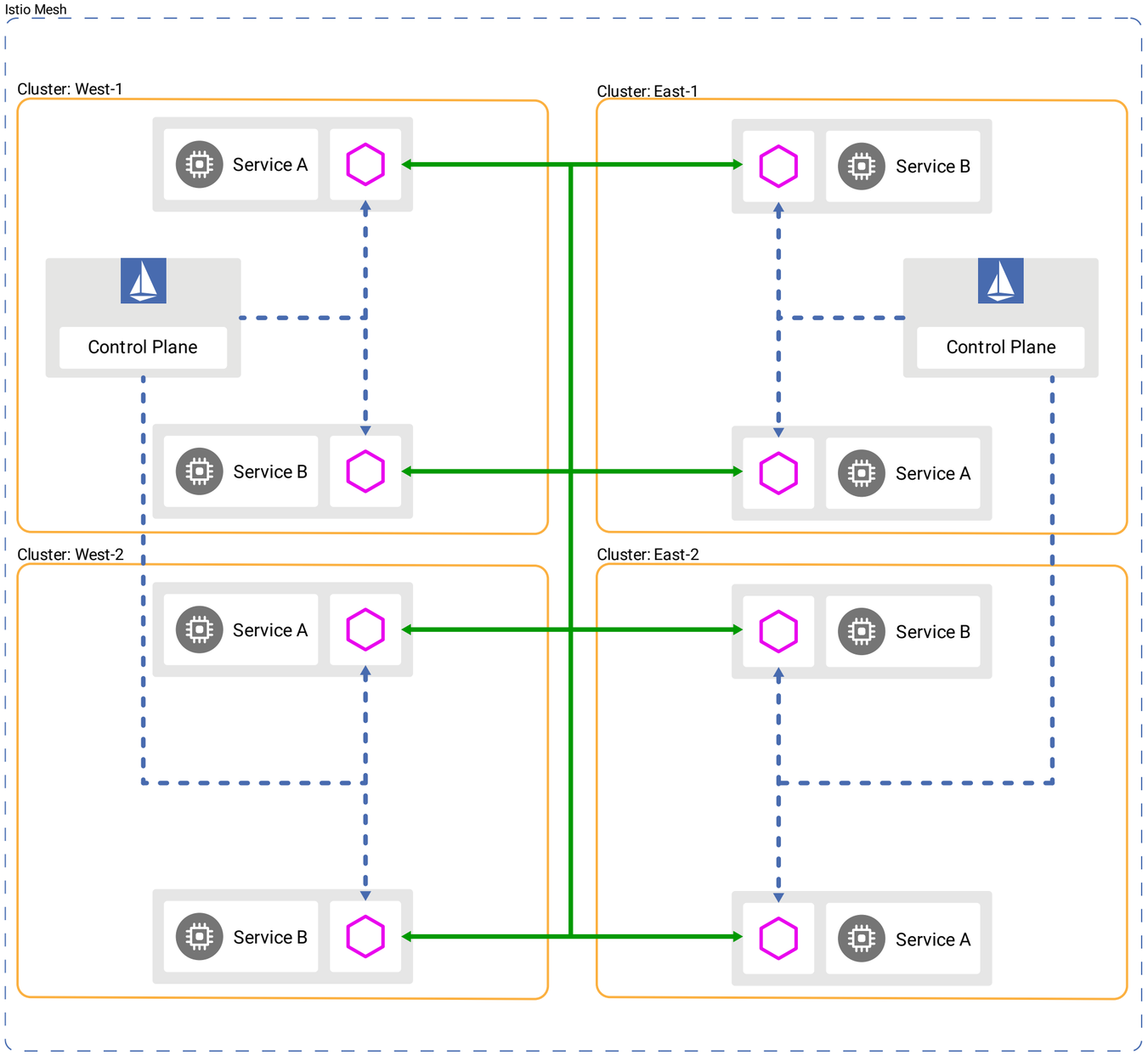
Telemetry continues

Collection impacts performance



- Single cluster
- Single control plane
- Istiod HA with Kubernetes

Source: istio.io/latest/docs/ops/deployment/deployment-models/



- Multiple clusters
- Multiple control planes
- Single logical network

Source: istio.io/latest/docs/ops/deployment/deployment-models/

Do I need a service mesh?

Service Mesh Alternatives

Traffic Management

Kubernetes labels

DNS setup

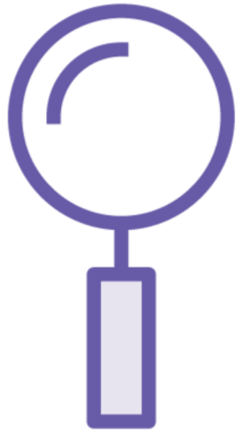
Client libraries

Security

Platform features

OpenSSL

SPIFFE



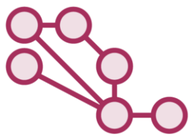
Observability

Prometheus & Grafana

OpenTelemetry

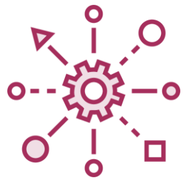
EFK Logging

Signals of Service Mesh Need



Service sprawl - utilization & health unknown

Release bottlenecks - walls of approval



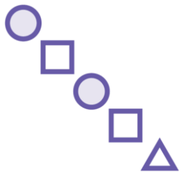
Custom implementations - no central management

Cloud-native pilot - expand scope

Have You Considered the Cost?

Lock-in - product and system design

Learning curve - Docker + Kubernetes + Istio



Environment drift - dev, test, prod - fundamentally different

Anti-DevOps - different tools in build and run - more SRE

SRE vs. DevOps

Site Reliability Engineering (SRE): The Big Picture

Elton Stoneman

Summary

Istio in Production

- Generating manifests with Istioctl
- Deployments & updates
- Zero-impact deployments

Migrating Apps to Istio

- Proxy injection
- mTLS upgrade

Understanding the Cost

- Failure modes
- Running costs
- Complexity

Next Steps

Istio documentation and tasks

- https://istio.io/latest/docs

Gateway API

- GAMMA (Mesh Management and Admin)

Other Meshes

- Linkerd
- Open Service Mesh

We're Done!

So...

- Please leave a rating
- Follow `@EltonStoneman` on X
- Check out `blog.sixeyed.com`
- Watch my other courses ☺