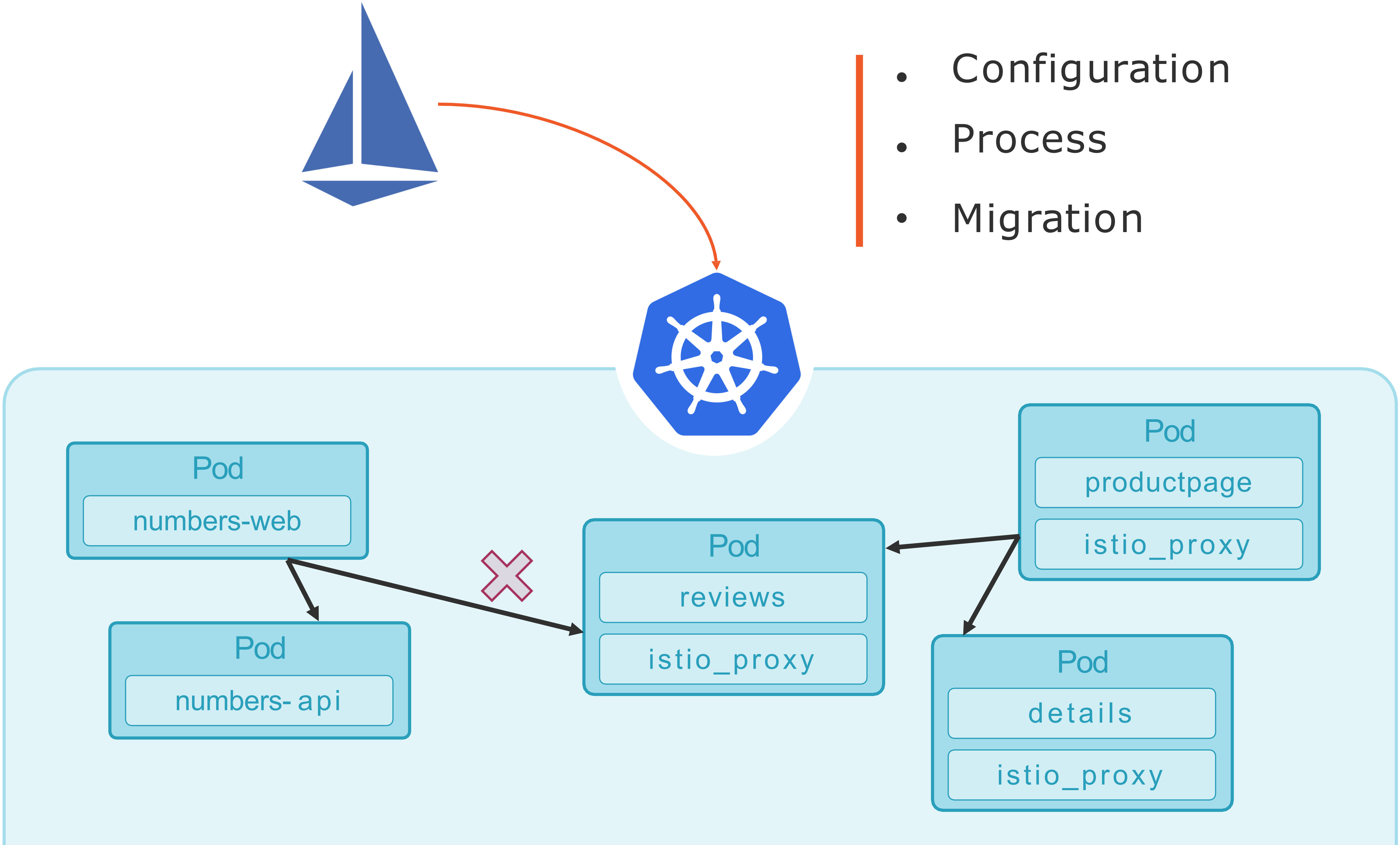
Running Istio in Production

Kien Bui
DevOps & Platform Engineer



- Configuration
- Process
- Migration

```
kubectl apply -f istio-crds.yaml

kubectl apply -f istio.yaml
```

Manifest Deployment

Manual ownership

No configuration options

20K lines?

```
helm install install/kubernetes/helm/istio-init --name istio-init -n
istio-system
```

```
helm install install/kubernetes/helm/istio --name istio --namespace istio-
system
```

Helm Deployment

Central management

Configurable profiles & settings

Industry standard

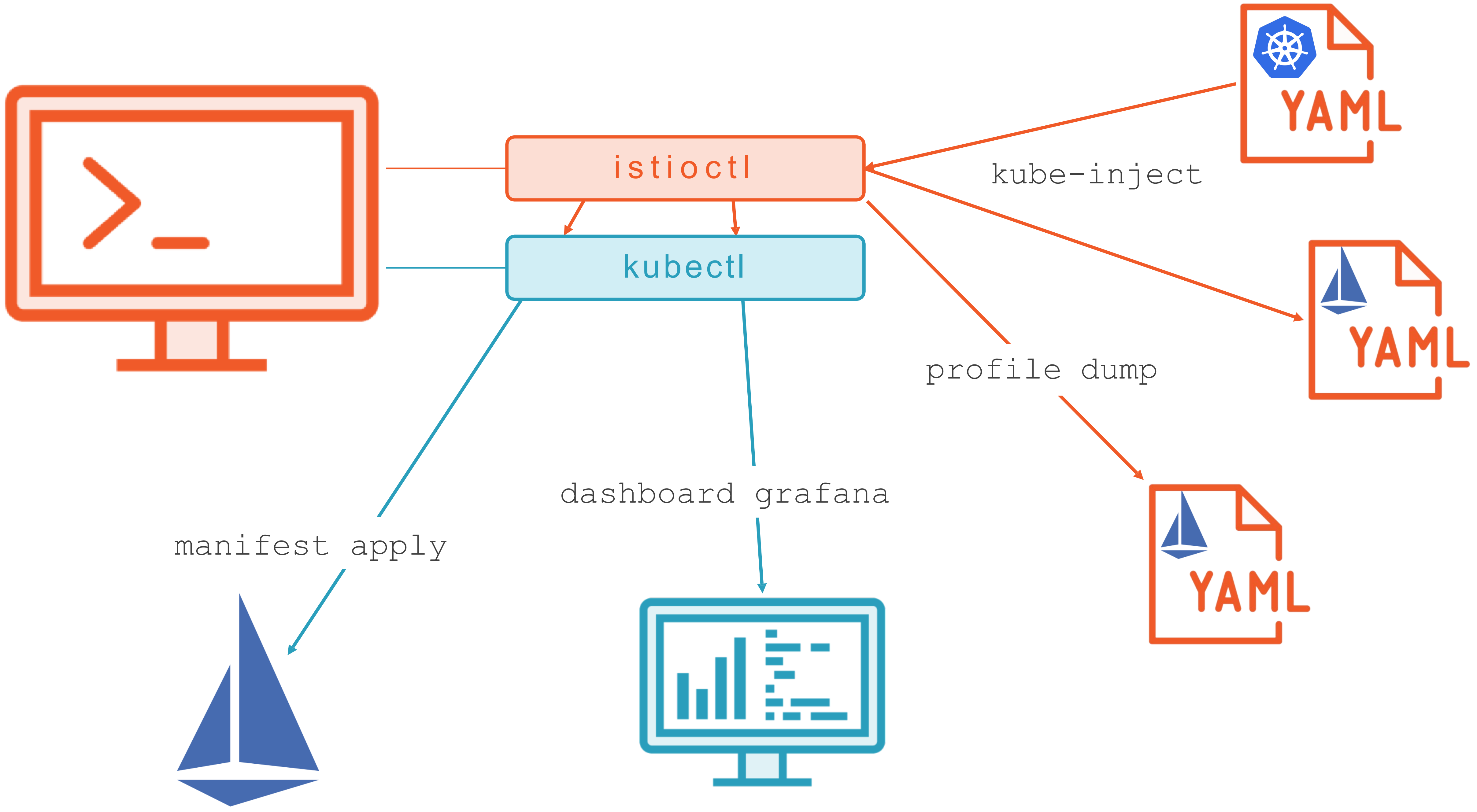
```
istioctl manifest apply
```

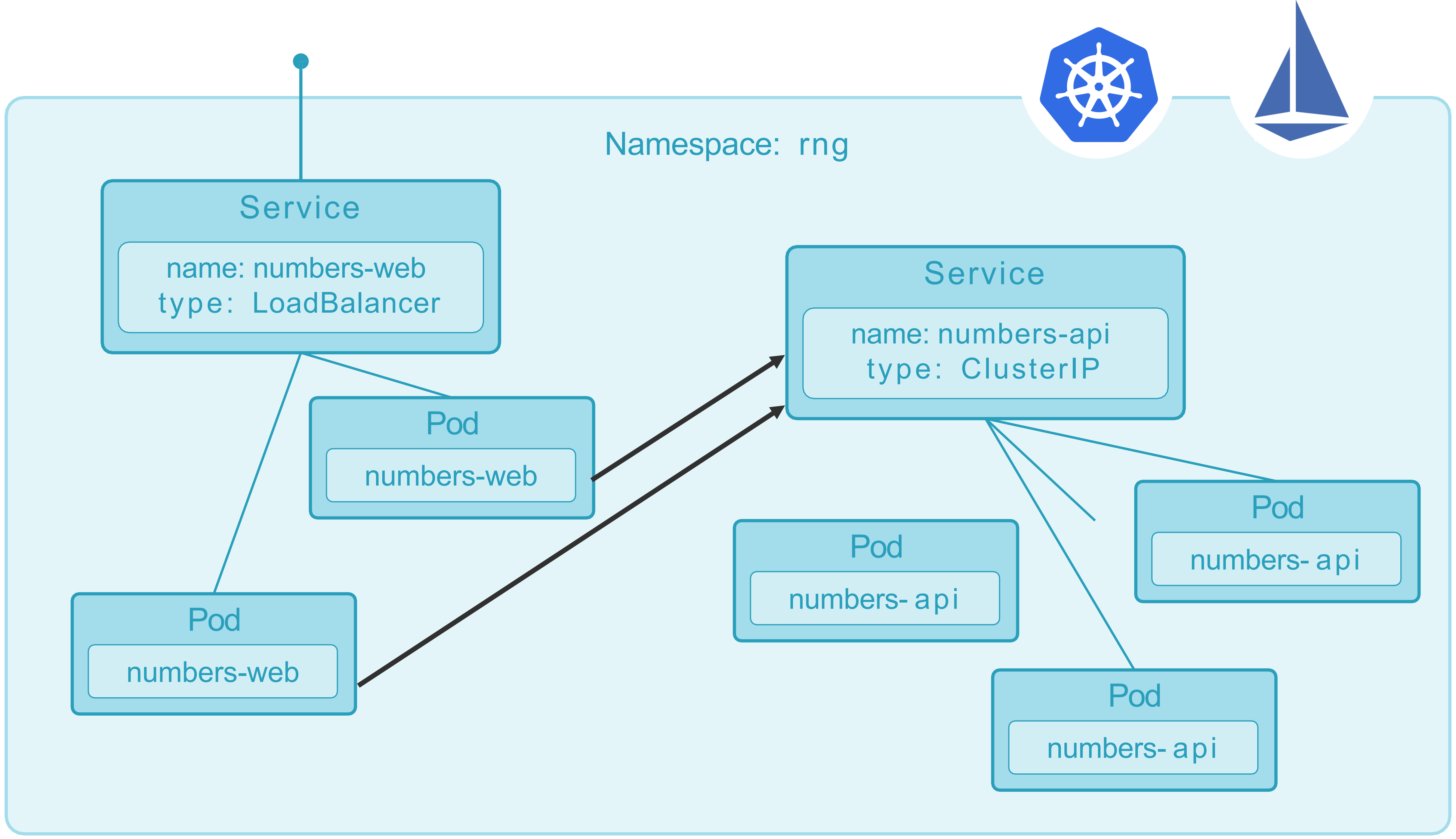
Istioctl Deployment

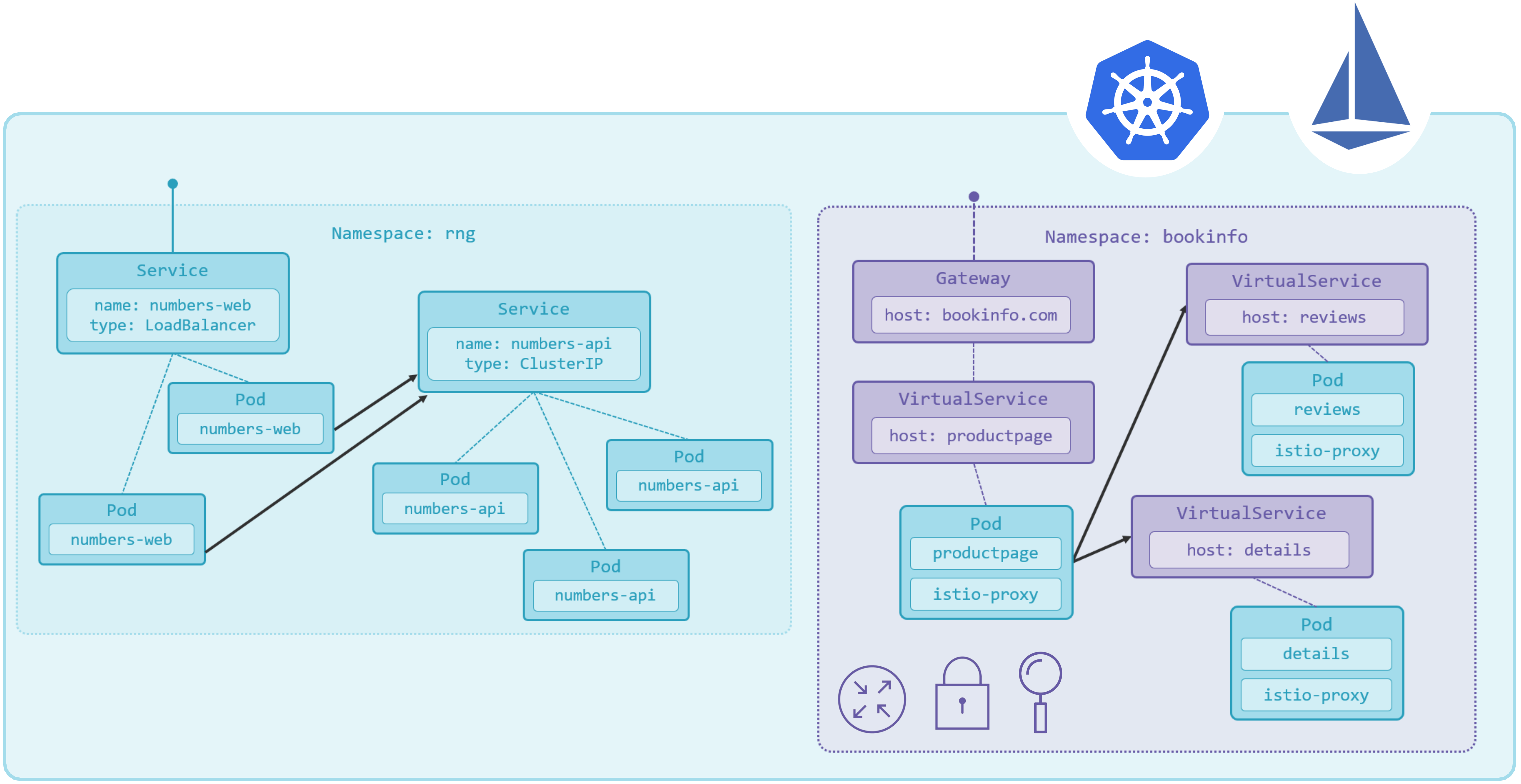
Centralized management

Configurable profiles & settings

Multi-purpose control tool


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

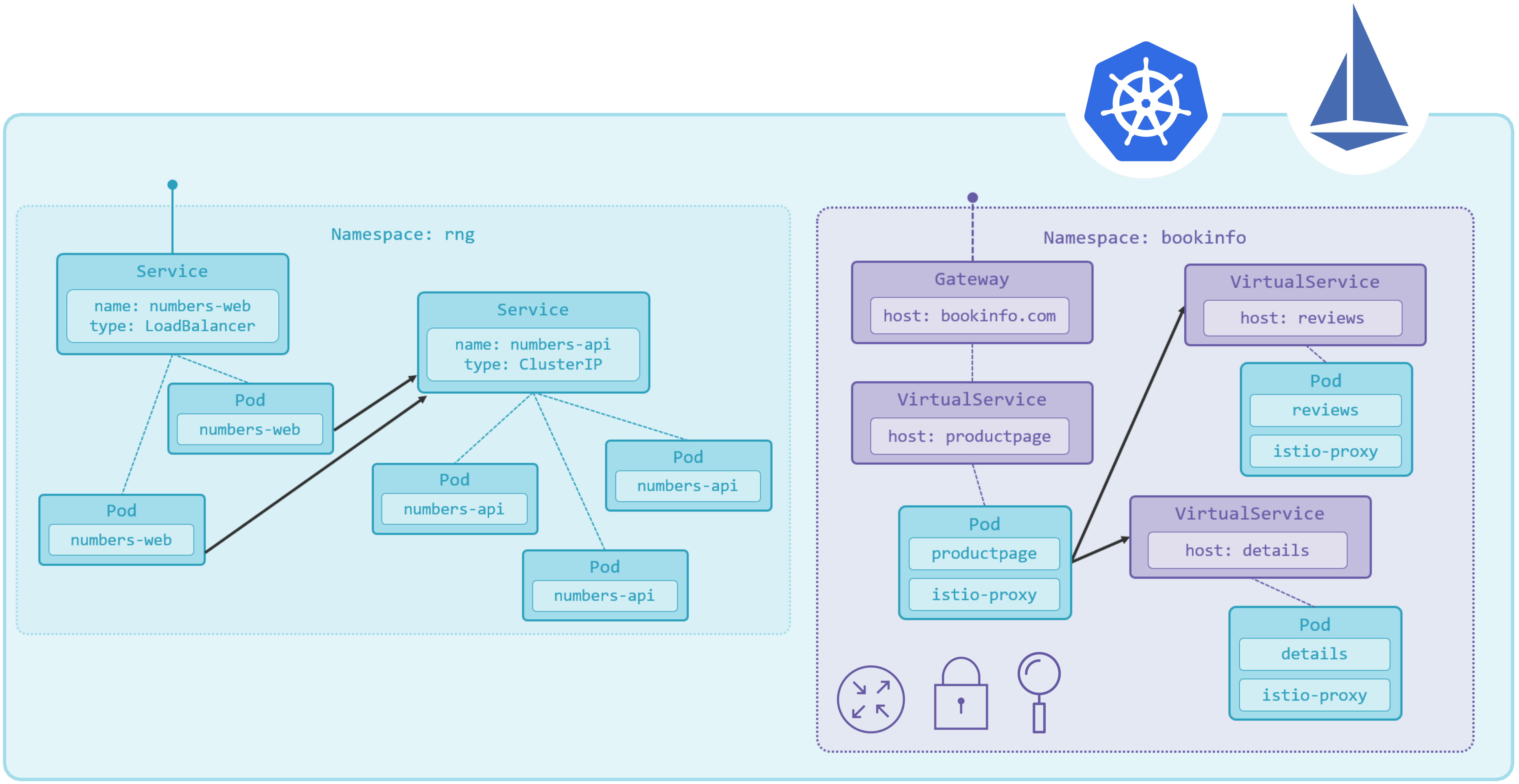

Namespace: rng
Service
name: numbers-web
type: LoadBalancer
Pod
numbers-web
Pod
numbers-web
Service
name: numbers-api
type: ClusterIP
Pod
numbers-api
Pod
numbers-api
Pod
numbers-api


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

Deploy 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
```

t Explore deployment profiles

```
istioctl manifest generate
     --set values.kiali.enabled=true

istioctl manifest generate
     -f istio-custom/kiali-enable.yaml
```

t Generate custom deployment manifest

```
istioctl dashboard kiali
```

t Temporarily enable dashboard access

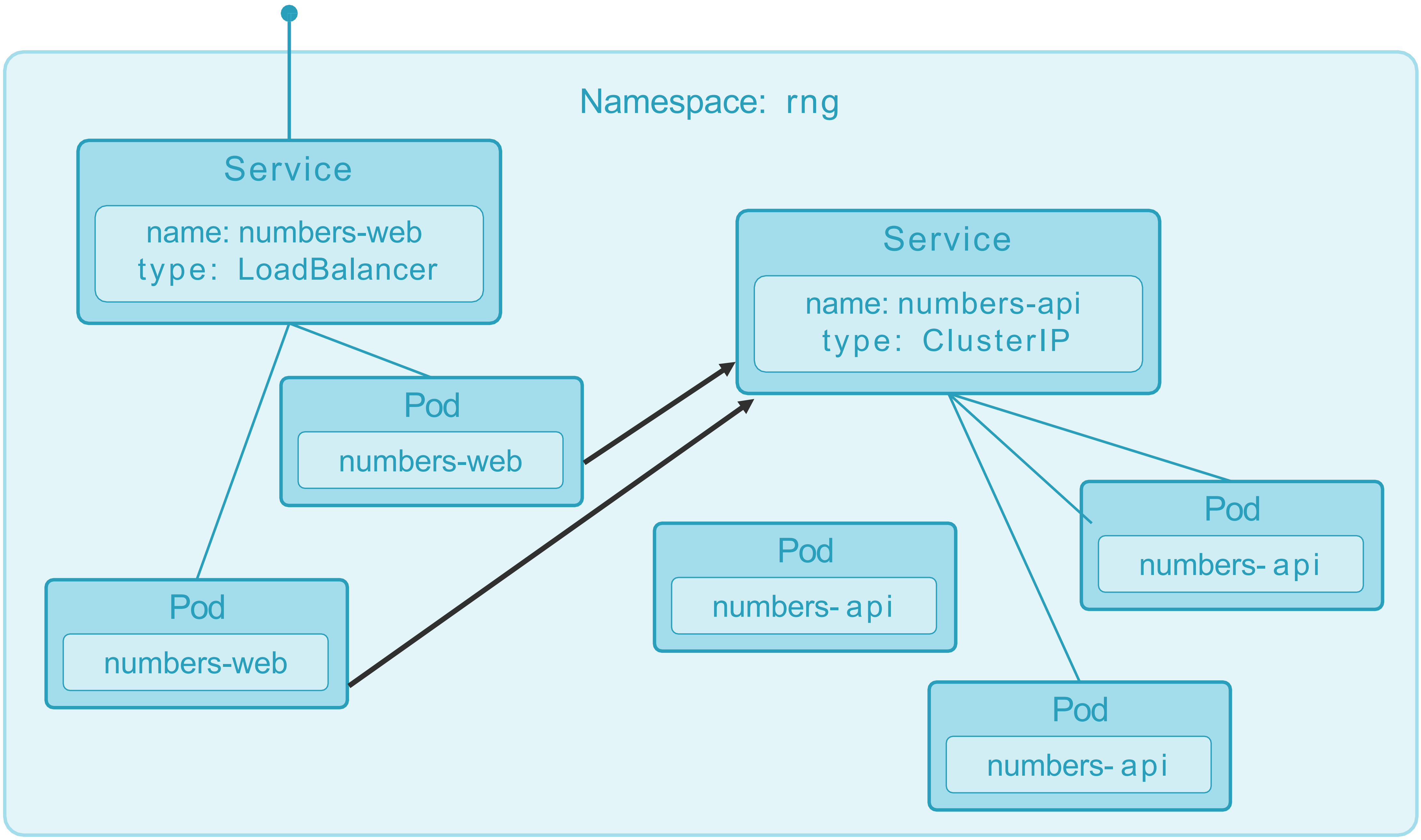
Customized Istio Deployment

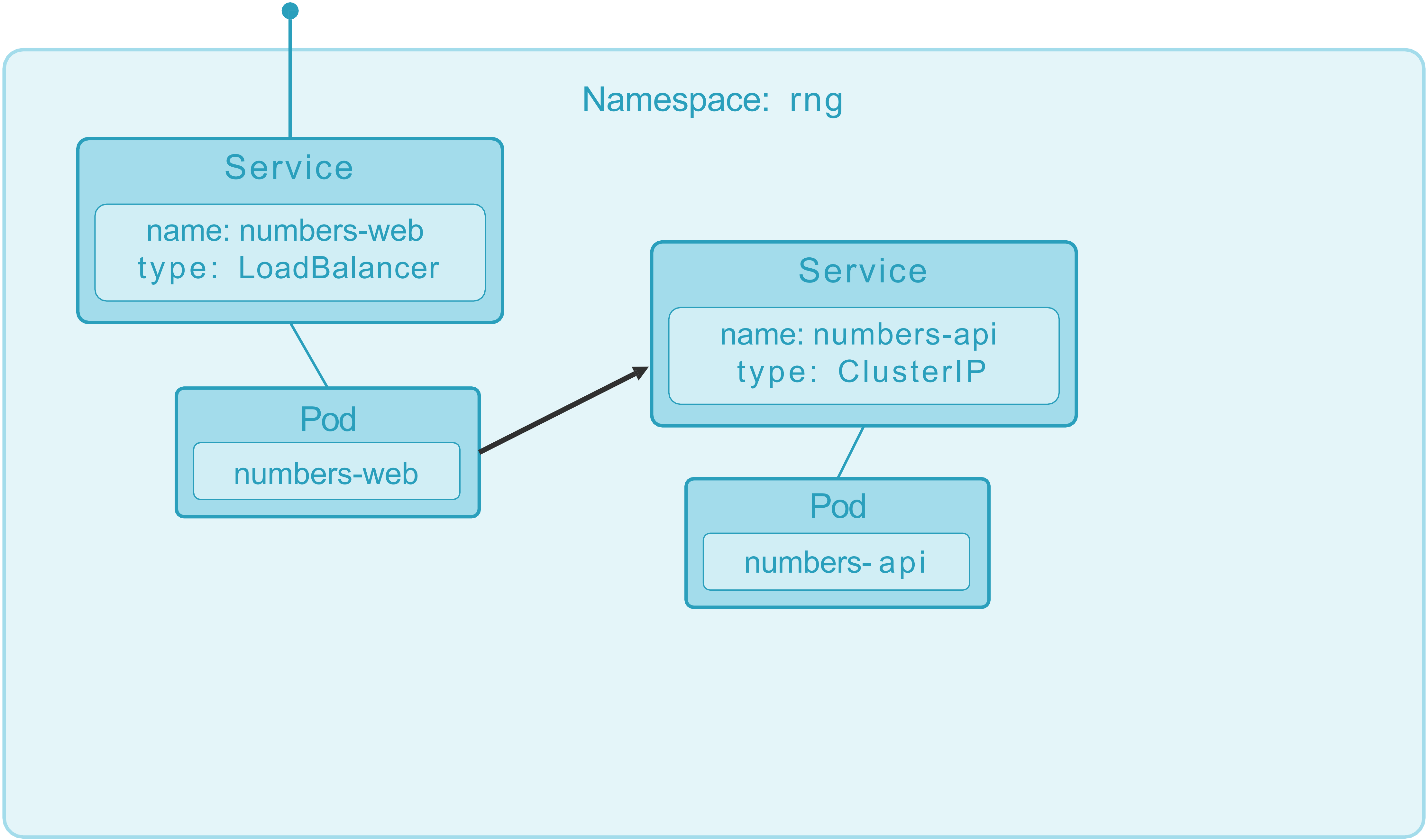
kiali-enable.yaml

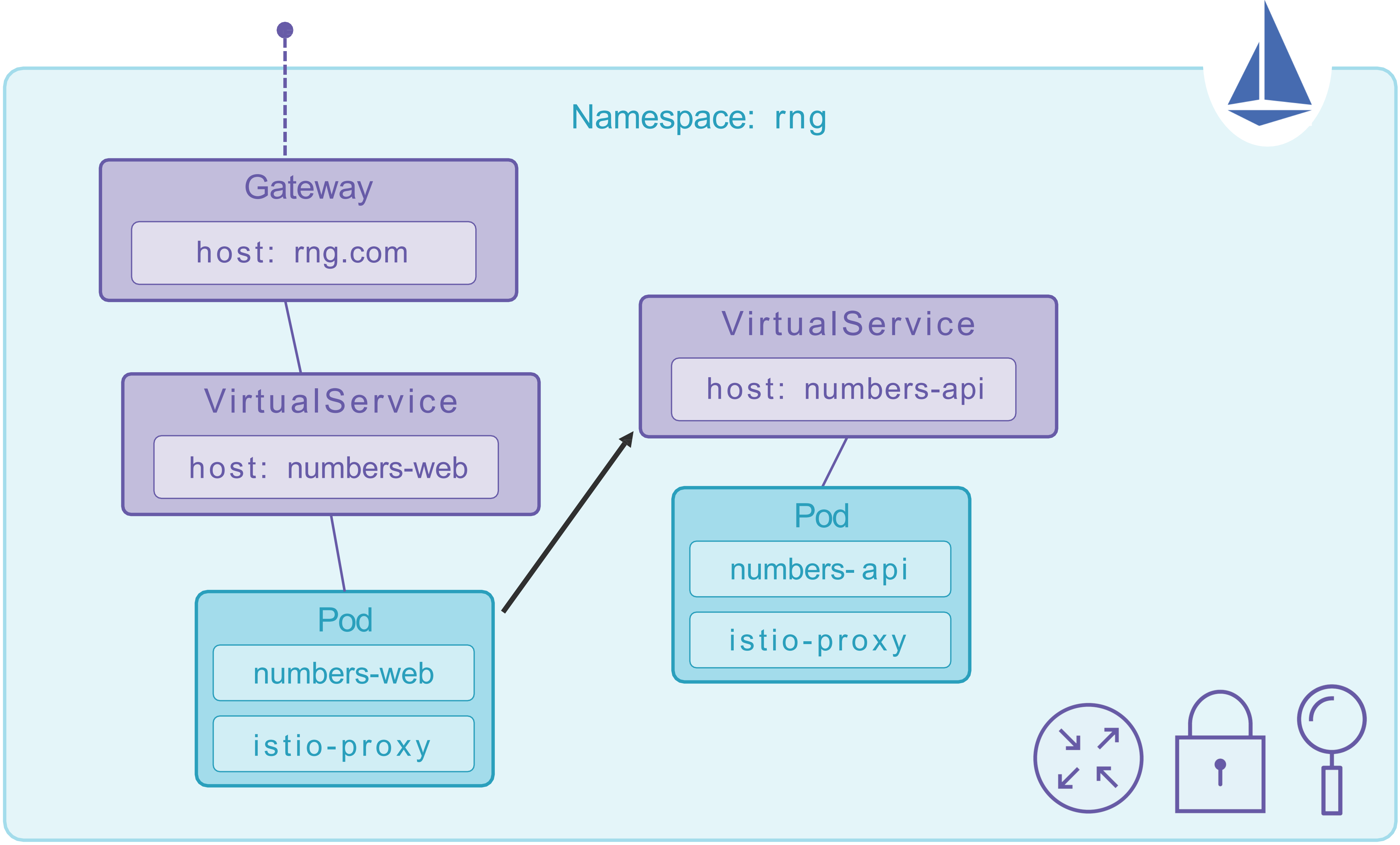
```yaml
apiVersion: install.istio.io/v1alpha2
kind: IstioControlPlane
spec:
  values:
    kiali:
      enabled: true
      dashboard:
        viewOnlyMode: true
```

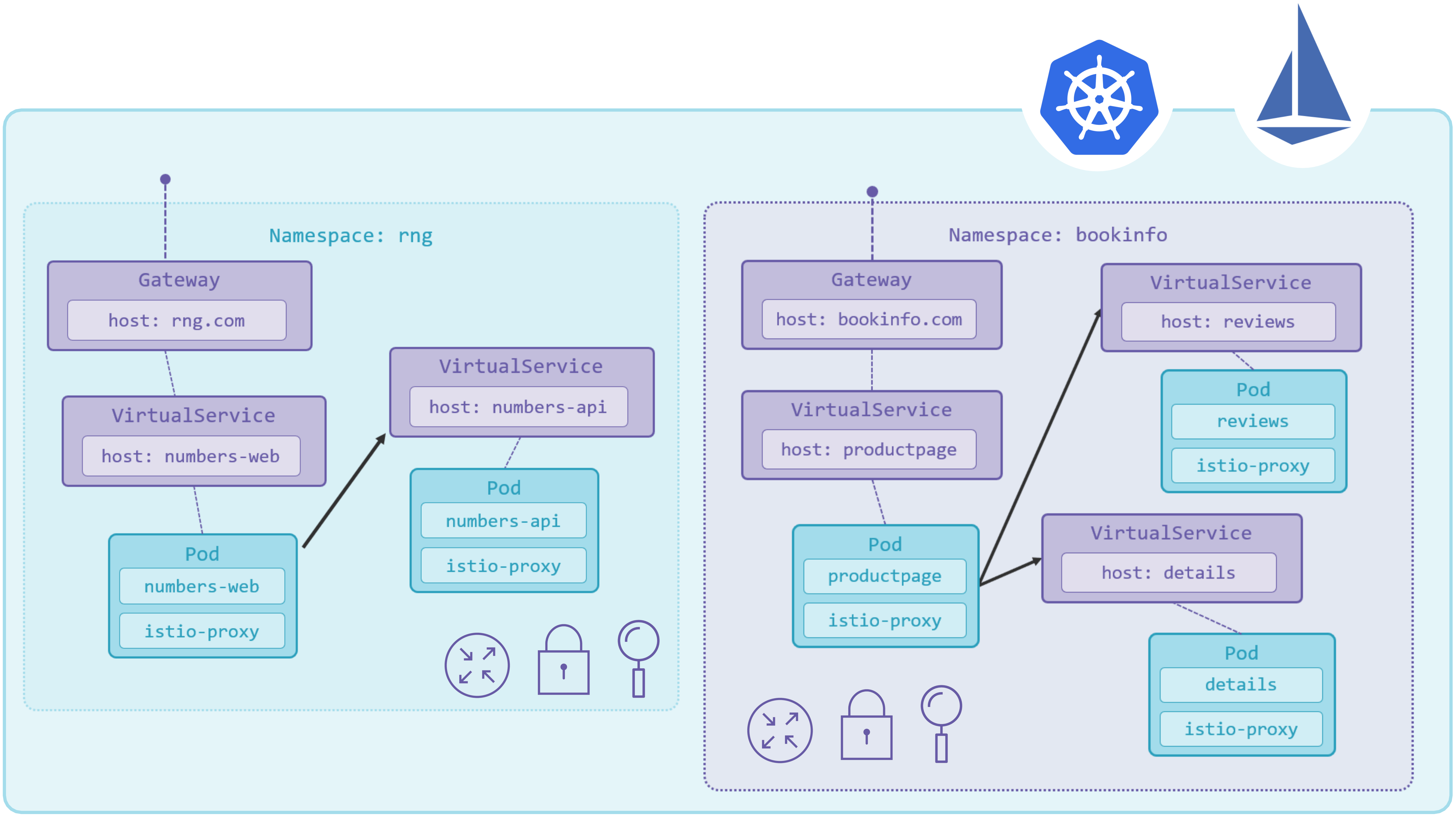
istio-custom-manifest.yaml

```yaml
apiVersion: authentication.istio.io/...
kind: MeshPolicy
metadata:
  name: default
  labels:
    release: istio
spec:
  peers:
  - mtls:
      mode: PERMISSIVE
```


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

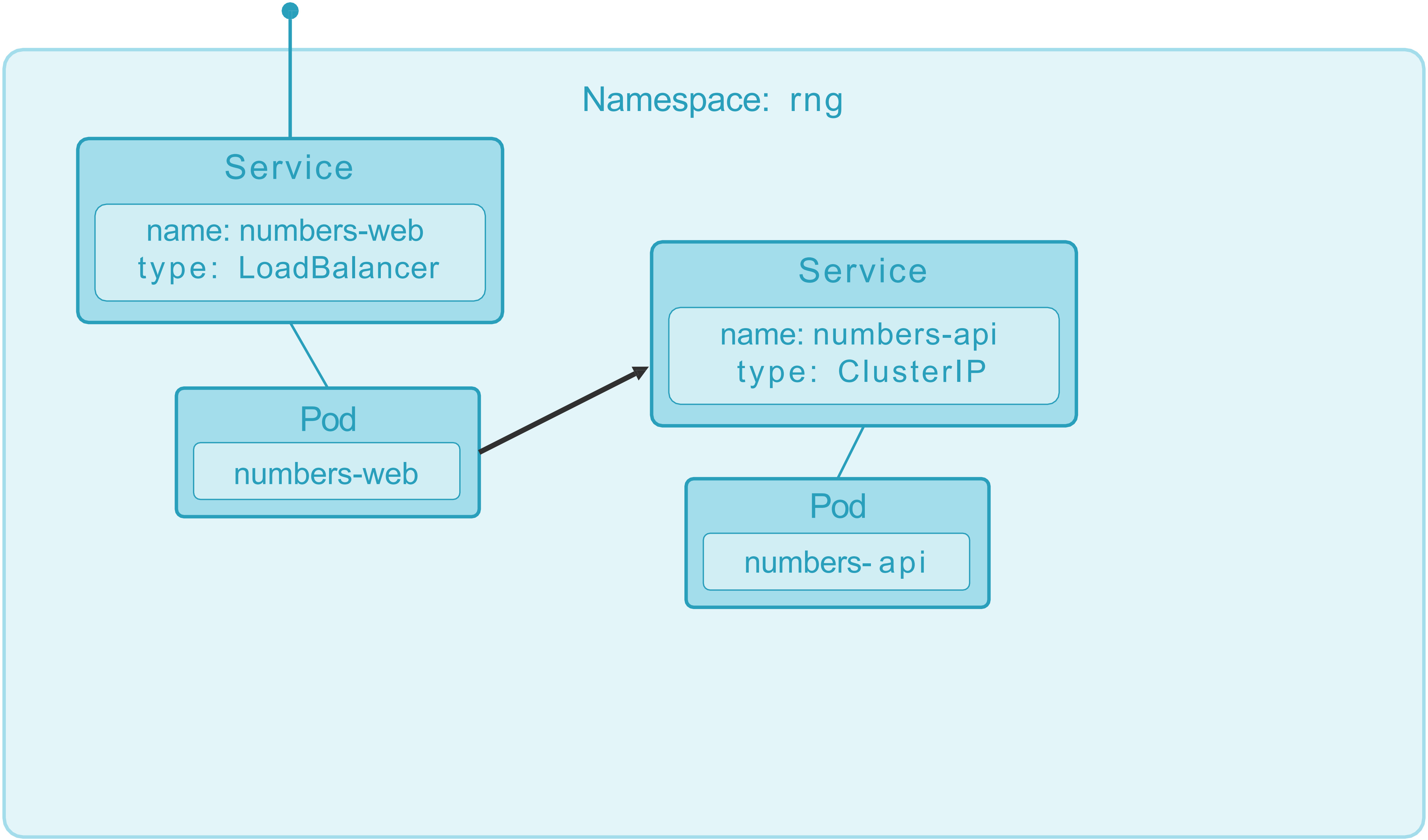

Namespace: rng
Gateway
host: rng.com
VirtualService
host: numbers-web
Pod
numbers-web
istio-proxy
VirtualService
host: numbers-api
Pod
numbers- api
istio-proxy

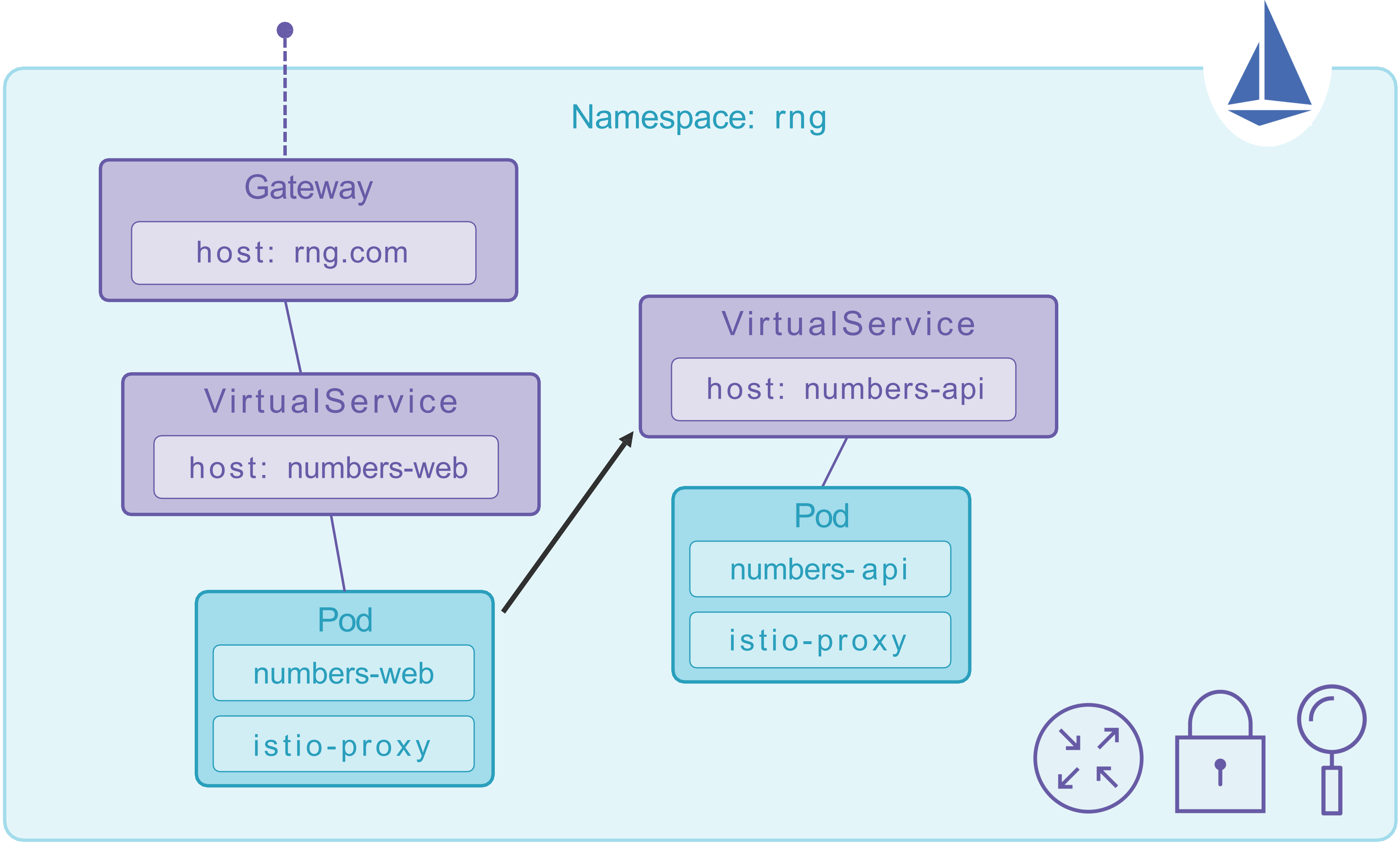

Namespace: rng
Gateway
host: rng.com
VirtualService
host: numbers-web
Pod
numbers-web
istio-proxy
VirtualService
host: numbers-api
Pod
numbers-api
istio-proxy
Namespace: bookinfo
Gateway
host: bookinfo.com
VirtualService
host: productpage
Pod
productpage
istio-proxy
VirtualService
host: reviews
Pod
reviews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

```
istioctl kube-inject -f api.yaml -o api-istio.yaml
```

Proxy Injection

Adds the proxy container to each pod spec

Migration to mTLS

Authn.yaml

```yaml
apiVersion: authentication.istio.io/...
kind: Policy
metadata:
  name: default
  namespace: rng
spec:
  peers:
  - mtls:
      mode: PERMISSIVE
```

DestinationRules.yaml

```yaml
apiVersion: networking.istio.io/v1alpha3
kind: DestinationRule
spec:
  host: numbers-api.rng.svc.cluster.local
  trafficPolicy:
    tls:
      mode: ISTIO_MUTUAL
  subsets:
  - name: v1
    labels:
      version: v1
```

Ingress Migration

GatewayVirtualService.yaml

```yaml
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
spec:
  hosts:
  - rng.sixeyed.com
  gateways:
  - ingressgateway.istio-system
  http:
  - route:
    - destination:
        host: numbers-web.rng
        subset: v1
```

ServiceToInternal.yaml

```yaml
apiVersion: v1
kind: Service
spec:
  ports:
  - port: 80
    name: http
  selector:
    app: numbers-web
  type: ClusterIP
```

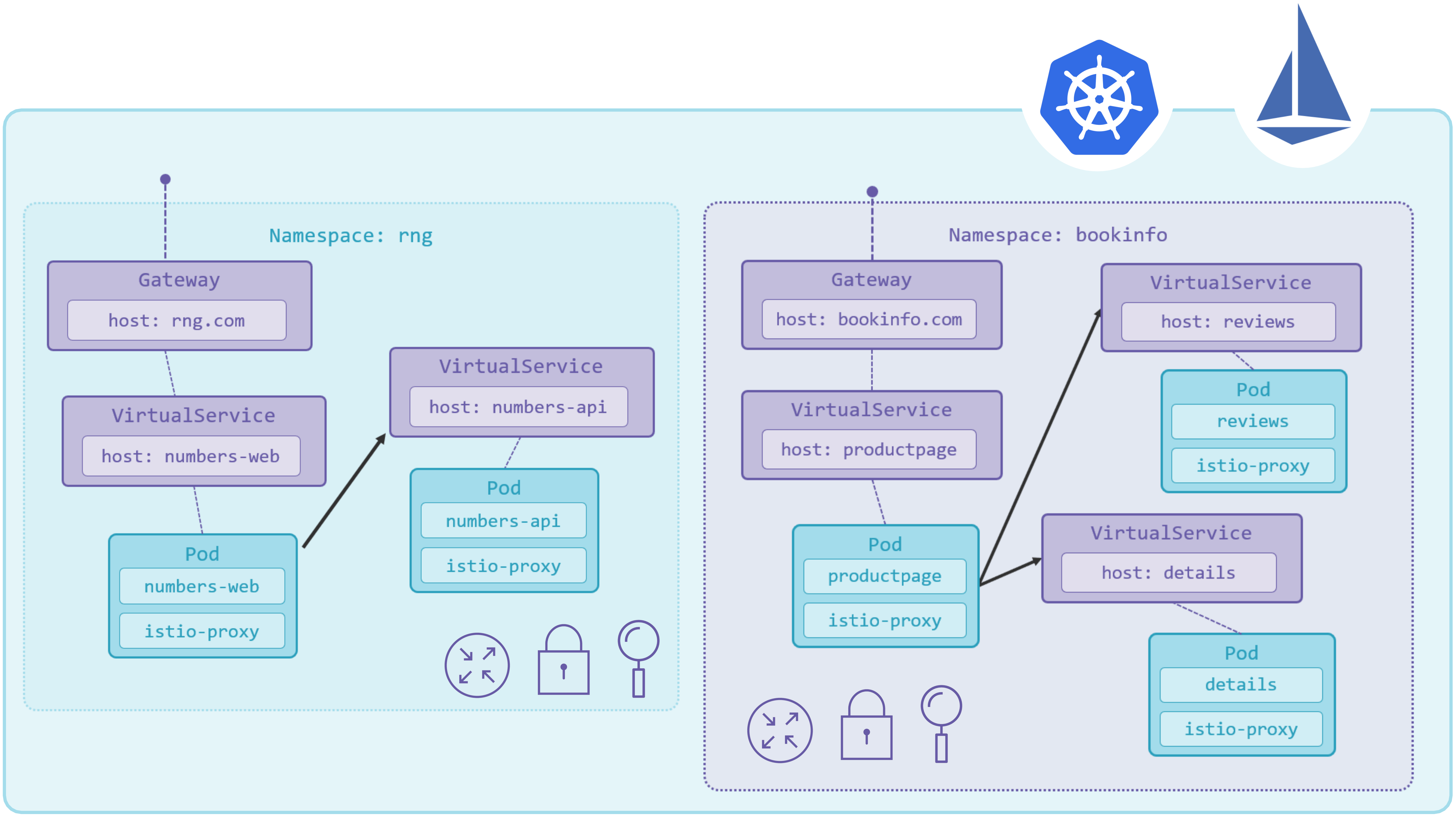
Post-mTLS Migration

Authn.yaml

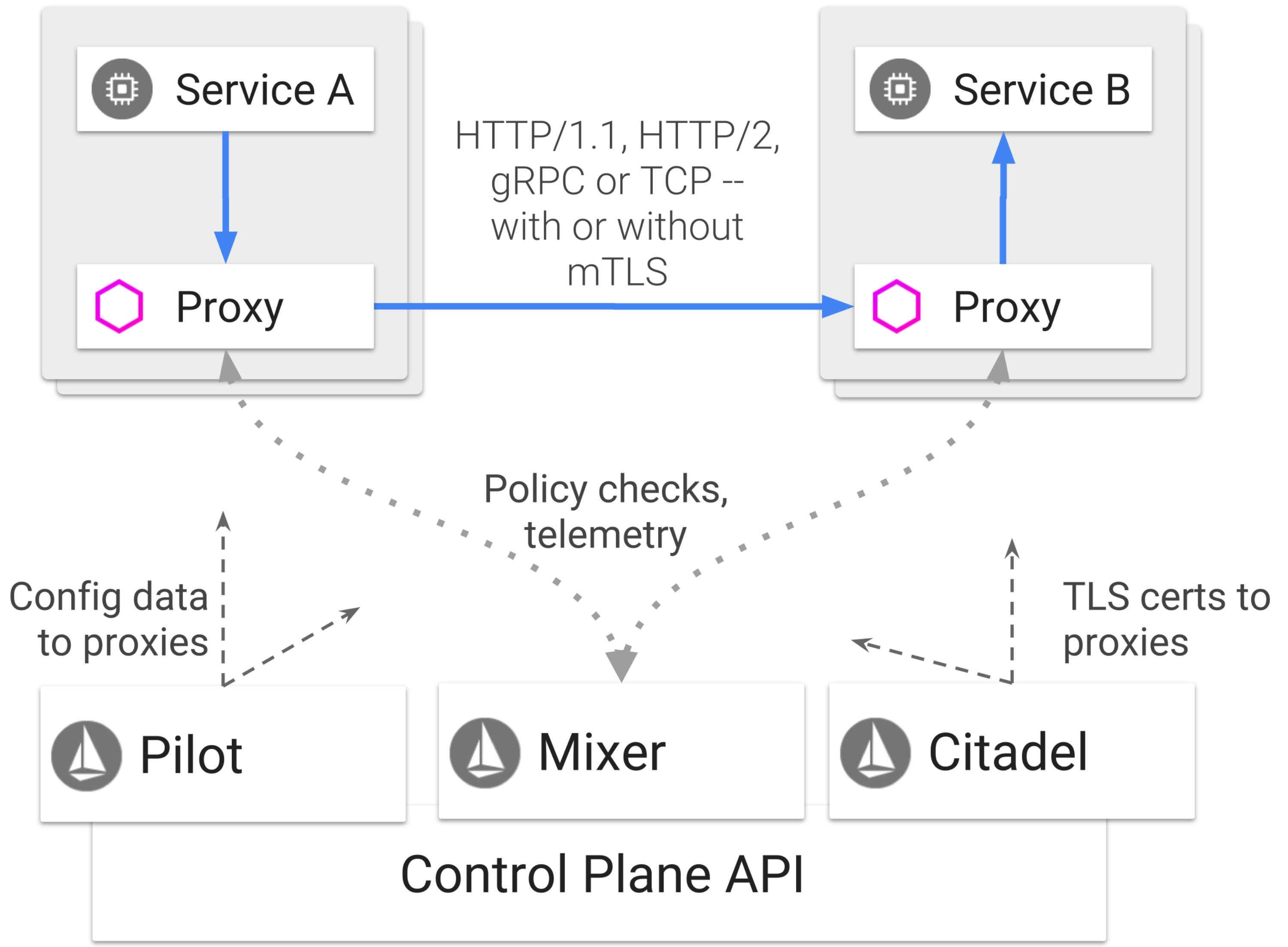
```yaml
apiVersion: authentication.istio.io/...
kind: Policy
metadata:
  name: default
  namespace: rng
spec:
  peers:
  - mtls: {}
```

Authz.yaml

```yaml
kind: AuthorizationPolicy
spec:
  selector:
    matchLabels:
      app: numbers-api
  rules:
  - from:
    - source:
        principals: [".../numbers-web"]
    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



* https://istio.io/docs/concepts/what-is-istio/

Failure Scenarios

Pilot

Proxies cache config

Existing pods get stale

New pods cannot start

Citadel

Proxies cache certs

Certificates expire

mTLS calls fail

Mixer

Mixer caches config

Policy assertions fail

Telemetry fails

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 app 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

Summar
y

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

Monitoring Containerized Application Health with Docker

- is.gd/4g8FQl

Istio docs & tasks

- is.gd/IEym5v

SMI - Service Mesh Interface

- is.gd/LYQDLF

Meshery

- is.gd/RQ1UrJ