SCALEOUT

Configuration Management Tools -
Istio

Max Andersson

- Service Mesh
  - Is the network of microservices
  - With great power comes great responsibility
  - "Batteries Included"
    - Discovery
    - Load balancing
    - Failure recovery
    - Metrics & Monitoring
  - Simplifies
    - A/B Testing
    - Canary rollouts
    - Rate limiting
    - Access Control
    - End-to-end Authentication

- Istio
  - Connect
  - Secure
  - Control
  - Observe

- Control Plane
  - Pilot, Mixer & Citadel

- Data Plane
  - Envoy Proxy
- Mixer
  - Telemetry
  - Metrics
  - To Grafana, Prometheus
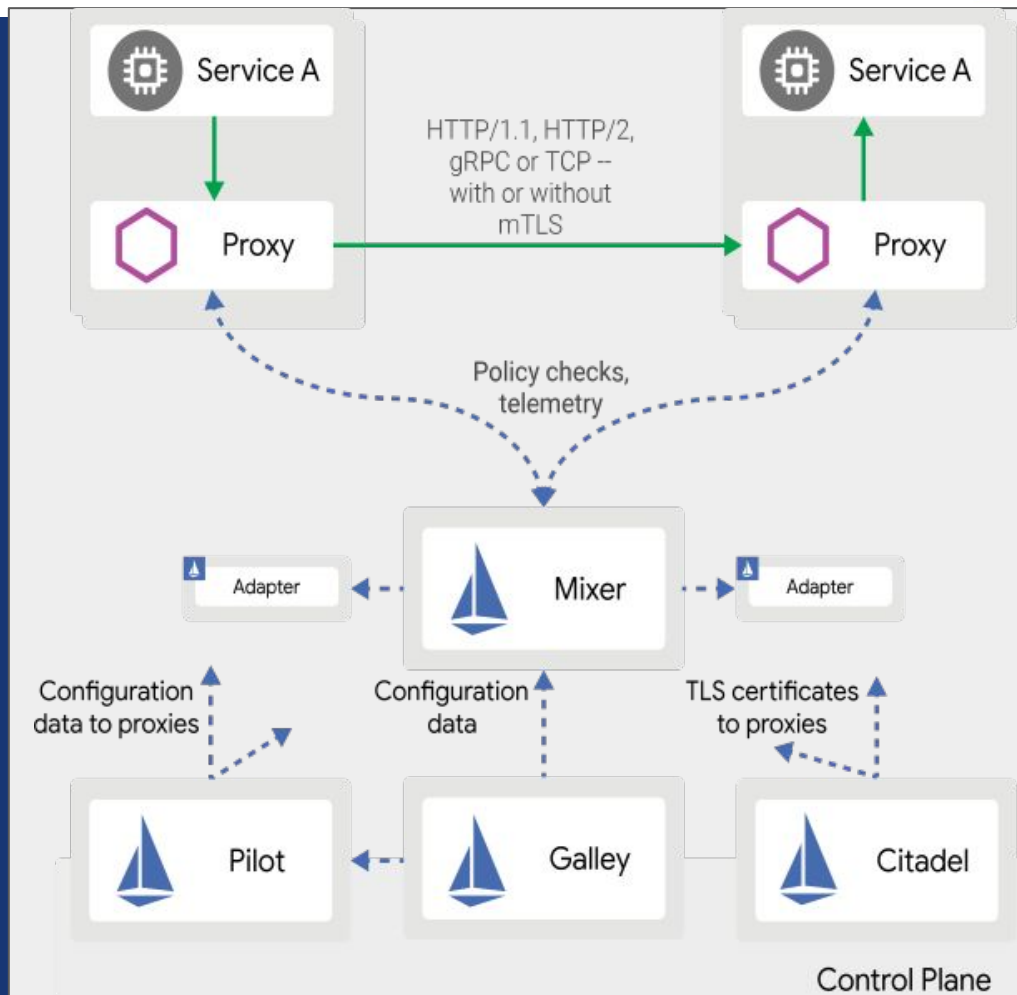
- Observing services
  - Get automatic tracing monitoring and logging of all your services
  - Adapter API

Connecting services
- VirtualService, DestinationRule, Gateway, ServiceEntry
- Traffic splitting
- Traffic steering
- Fault injection
- Circuit Breaking
- Egress control

- Securing Services
  - Traffic encryption
  - Service auth
  - Auditing controls
  - Access Policies

- Sidecar proxy Injection
  - Manual or Automatic (per namespace)

- Security
  - Defense against MITM attacks, need traffic encryption
  - Service Access Control, mutual TLS, fine-grained access policies
  - Audibility

- Security
    - Security by default
    - Defense in depth
    - Zero-trust networks

- Security
  - Citadel - Keys and certificates
  - Sidecars & perimeter proxies - secure communication
  - Pilot - distributing authentication policies and naming information to proxies
  - Mixer - manages auth and audit

- Citadel
  - Watches apiserver then creates and strores certs and keys as kubernetes sexrets.
  - Mounts credentials for corresponding service account as a secret volume.
  - Automatically rotates certs and rewrites secrets
  - Pilot generates naming information, distributes it to the sidecar for respective service.

- Security
  - mTLS
    - Permissive mode

- Traffic Management
  - VirtualServices
    - Rule Destinations
      - Splitting between versions
      - Timeouts & reties
      - Fault injection
    - Conditional rules

  - Destination rules
    - Circuit Breakers
    - Rule Evaluation

  - Gateways
  - Sidecar

- Traffic Management
  - Virtual Services
    - Rule Destinations
      - Splitting between versions
      - Timeouts & retires
      - Fault injection
    - Conditional rules

  - Destination rules
    - Circuit Breakers
    - Rule Evaluation

  - Gateways
  - Sidecar

ISTIO