Service Meshes:

The Production Readiness Checklist for the Rest of Us

Austin Adams & Zach Arnold

Who/What is Ygrene?

- Financial Services Sector
- Privately Held, Publicly Good
- PACE = Property Assessed Clean Energy
- Ygrene = The word “Energy” spelled backwards
- Our mission is to make sure that Earth is still a thing in the future.

Who is this for?

- You are probably:
  - At KubeCon/CloudNativeCon NA in 2018
  - Aware of what a *Service Mesh* is at a high level
  - Managing a production collection of services (micro or otherwise) that communicate over TCP with each other
  - Experiencing the pain that comes with running these services at some scale
  - Needing a solution to your TCP based problems and don't have time for a complete rework of your application's architecture
  - In a small to mid-size business

Who is this probably *not* for?

- You are probably not:
  - Able to dedicate an army of engineers to solving this problem specifically for your business
  - Currently holding a PhD in Computer Science in the specific field of networking
  - Already running a service mesh in production

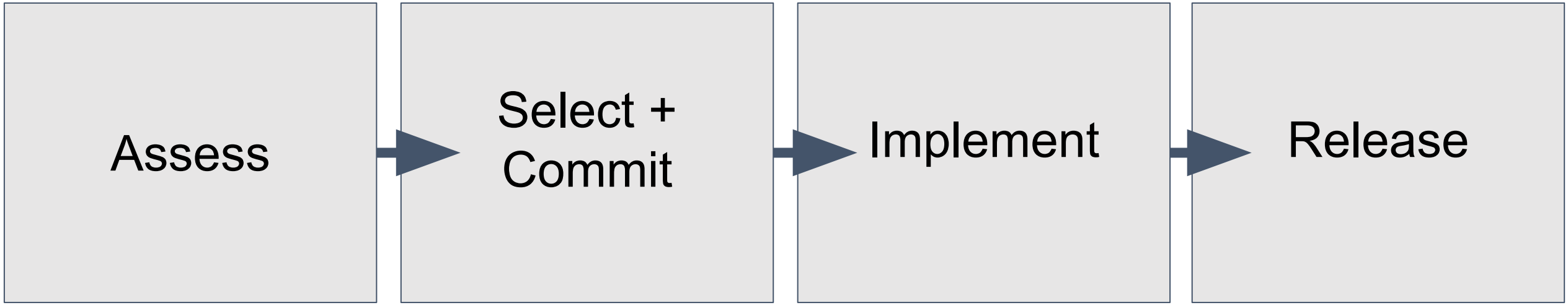
Service Meshes Distilled

- With every “Mesh” worth using you’ll get some form of the following:
  - TCP proxying
    - (HTTP1,1.1,2.0,gRPC…)
  - Traffic Flow Control:
    - DNS (or Service Discovery)
    - Load Balancing
    - Timeouts/Retries/Fault Injection/Circuit Breaking
  - Security
    - mTLS
    - Auth-n/Auth-z
  - Observability
    - Metrics
    - Distributed Tracing

The Landscape...more or less

- Linkerd 2.0 (CNCF project formerly Conduit)
- Istio (IBM + Google) with a proxy:
  - Envoy (CNCF Proxy Project)
  - Nginx
- Aspen Mesh (Managed Istio)
- AWS App Mesh
- Azure Service Fabric Mesh
- GKE Managed Istio (Managed Istio)

The Roadmap to Production



Assess

- Do we *need* a service mesh?
  - What problem does it solve?
    - Common problems
  - Can we handle the complexity?
    - More configuration to manage
- We need one, but what features to we need?
  - Security?
  - Observability?
  - Reliability?

Select + Commit

- The *Austin Adams* Litmus Test for choosing open-source Technology:
  - How long has it existed?
  - How popular is it in terms of contribution/usage?
  - How well sponsored is it and by whom?
  - How recently has it changed?
- Our general rule of thumb is to use a managed service where possible...it lets us concentrate on Ygrene stuff
  - But we couldn’t (EKS) so we went open source.

Select + Commit

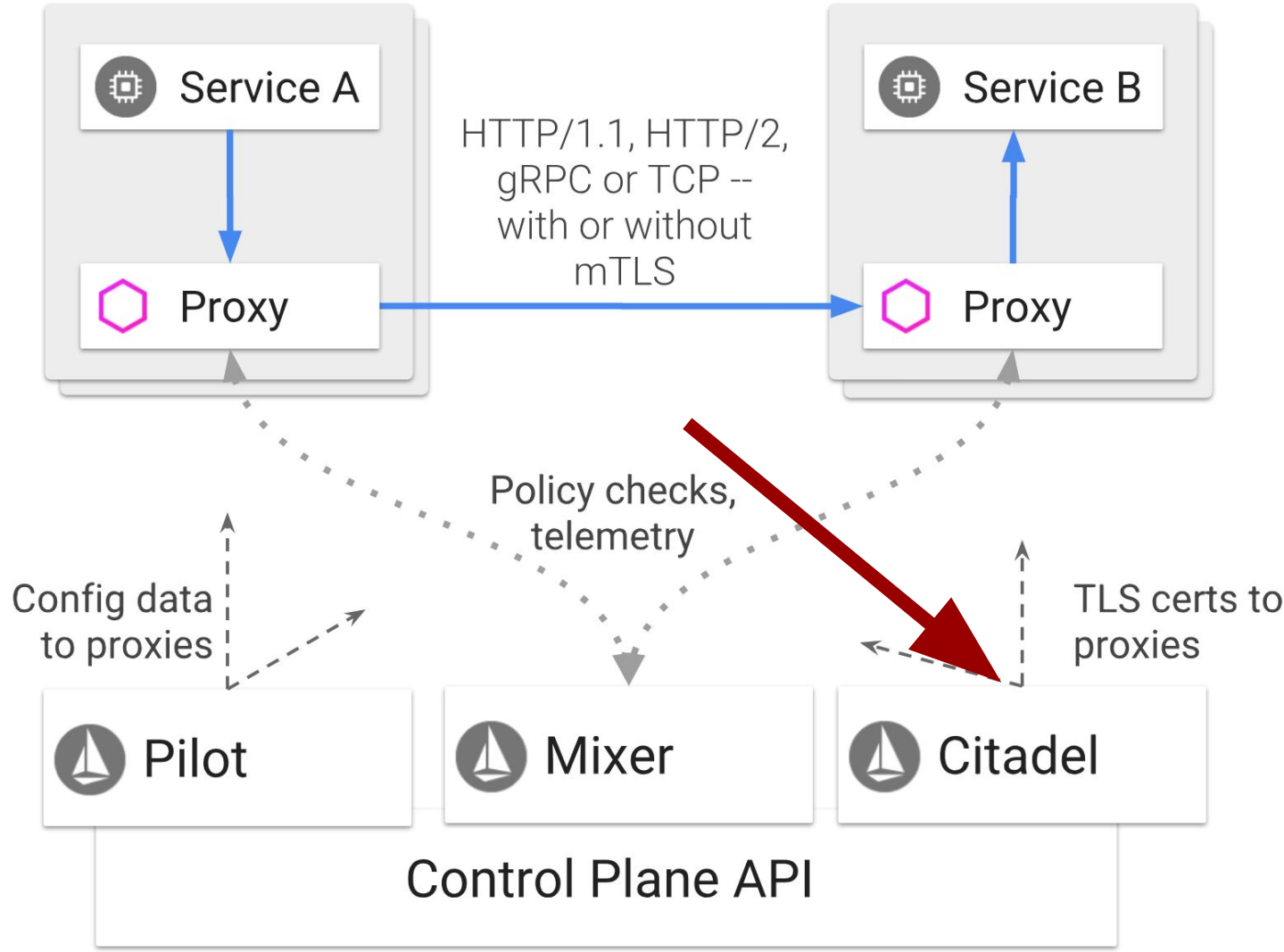
- Our take on the landscape
  - Small Team that needs telemetry, easy install and tracing
    - Linkerd 2
  - Any size team that needs security or flexibility or routing
    - Istio
  - Managed Cluster
    - Use their built-in, just do it.

Implement...a suggested strategy

- If you can...use Helm
- Using your selected features,

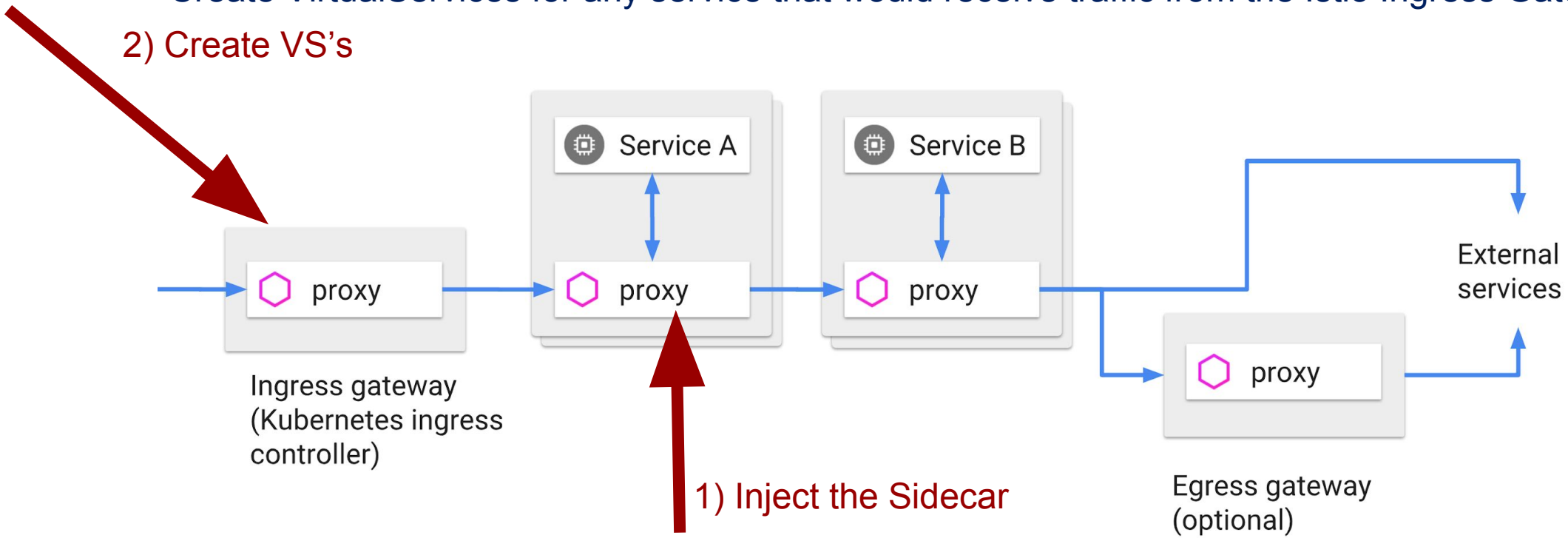
focus on the components you need

- For us, that was Citadel (mTLS)



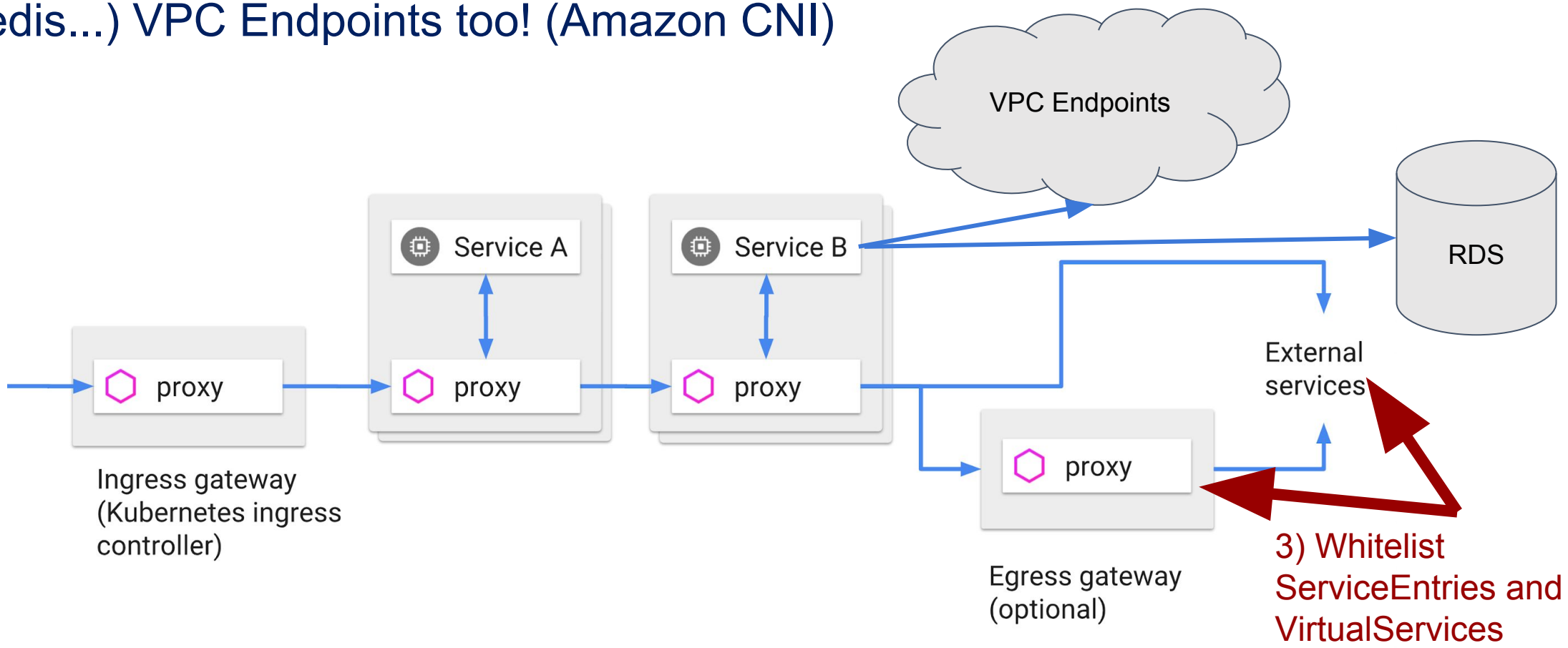
Implement...a suggested strategy

- Our focus was primarily on security, so the hardest part would be our migration to using Service Mesh tools for authz/authn
  - Create VirtualServices for any service that would receive traffic from the Istio Ingress Gateway



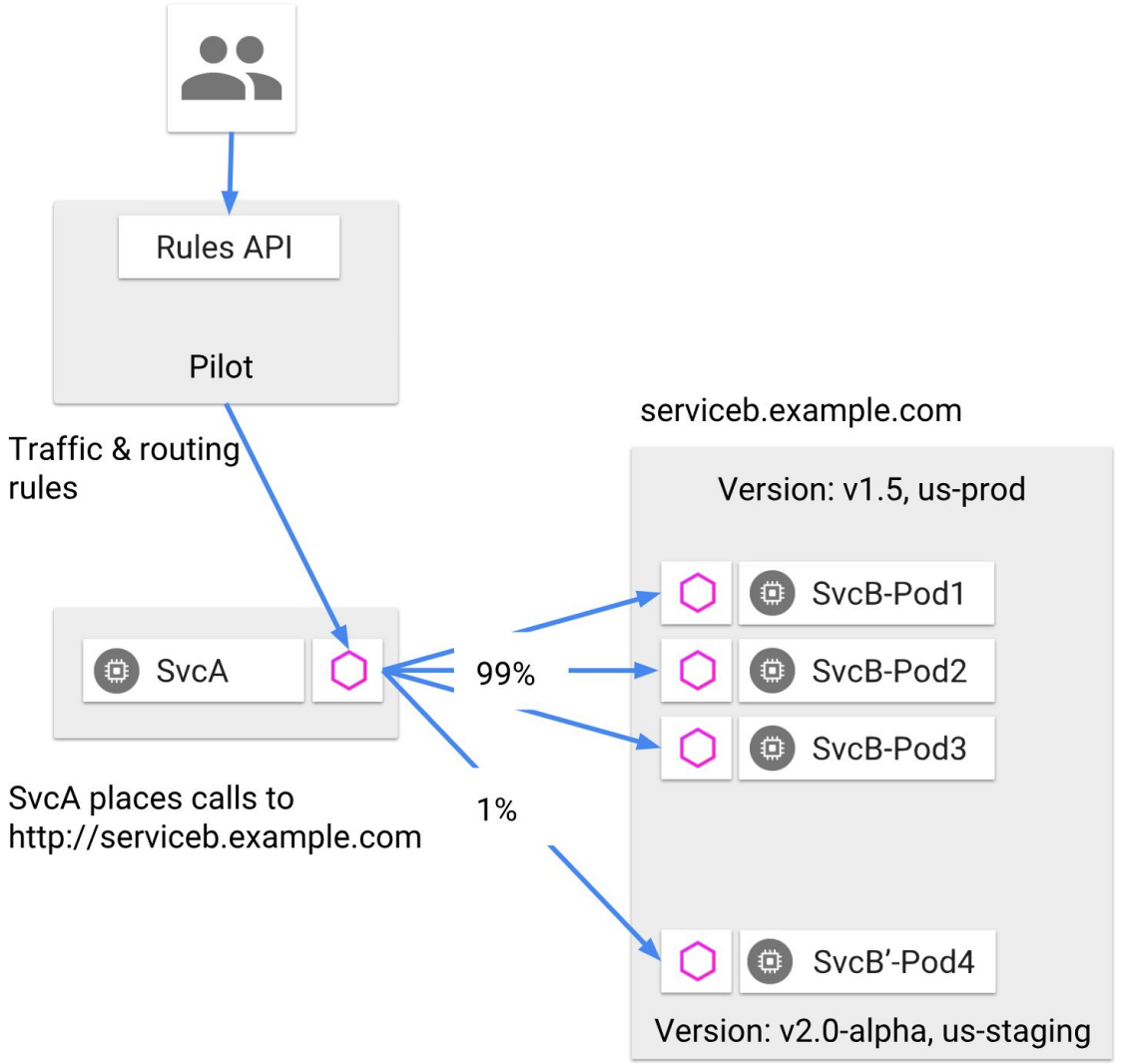
Implement...a suggested strategy

- Whitelist all outbound HTTPS/TCP traffic to 3rd party vendors (RDS, Stripe, Redis...) VPC Endpoints too! (Amazon CNI)



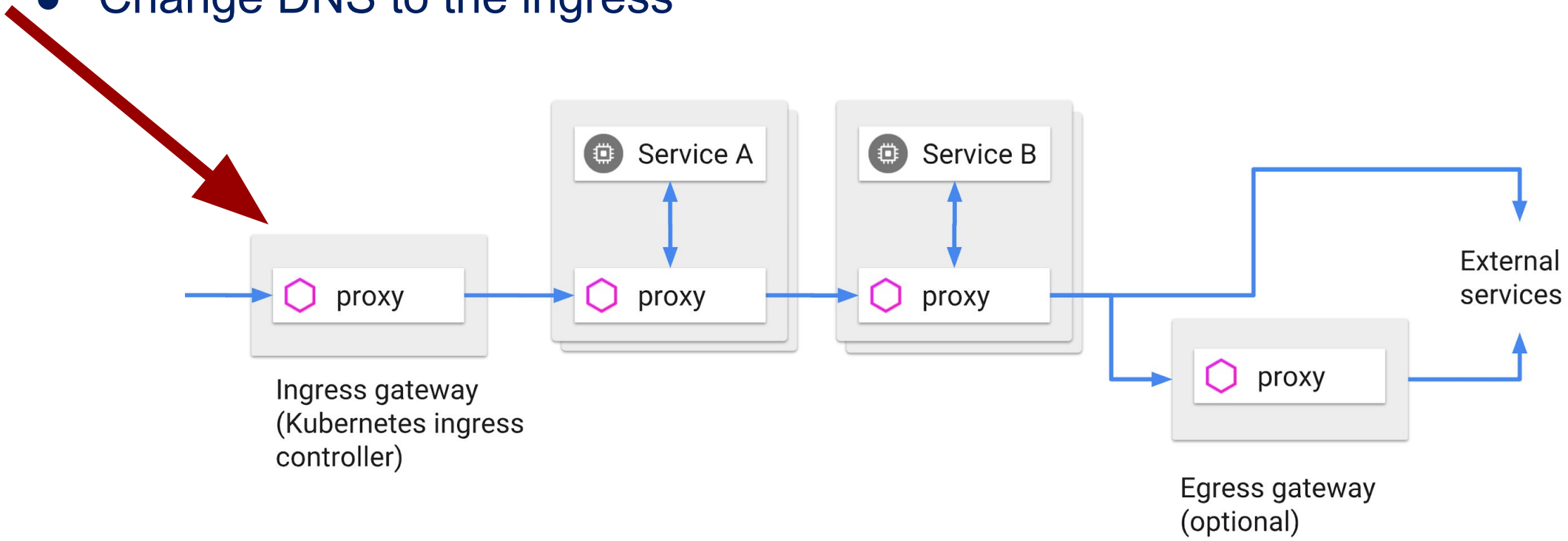
Implement...a suggested strategy

- Get ready for deployments, and leverage Istio DestinationRules
  - (if you do Blue/Green or Canary deployments)
  - Otherwise Istio just works like Kubernetes services



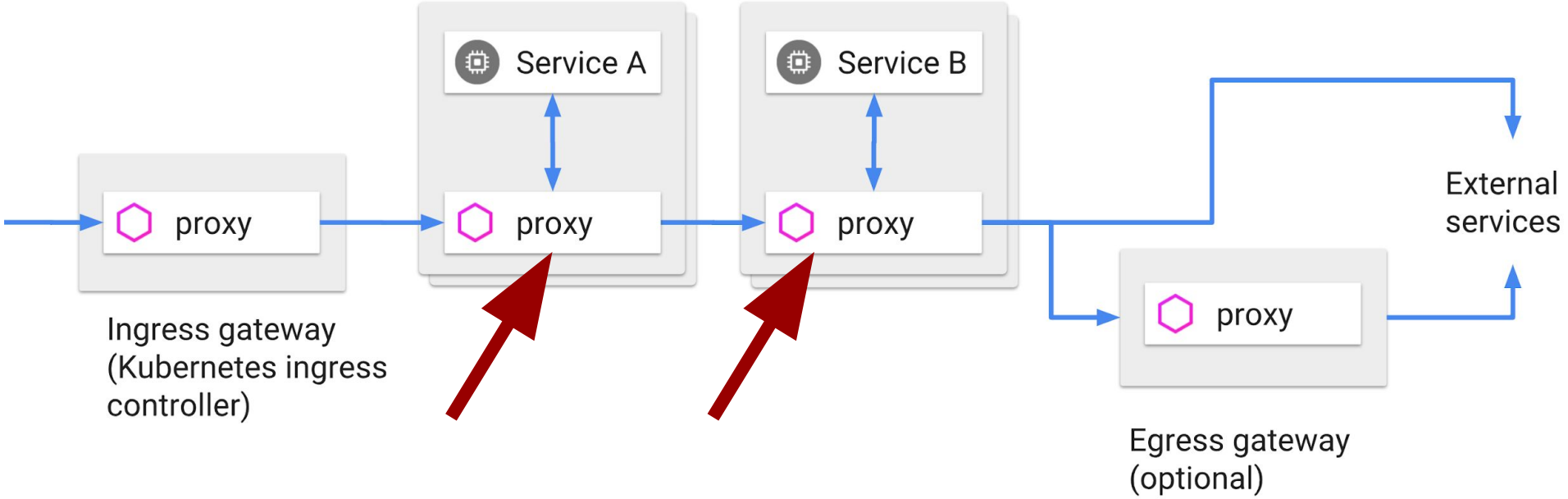
Release...with no interruptions

- Provision SSL certs for public domains that you want routable in the mesh *early*
  - *We used the Jetstack Certmanager (Open Source)*
- Change DNS to the ingress



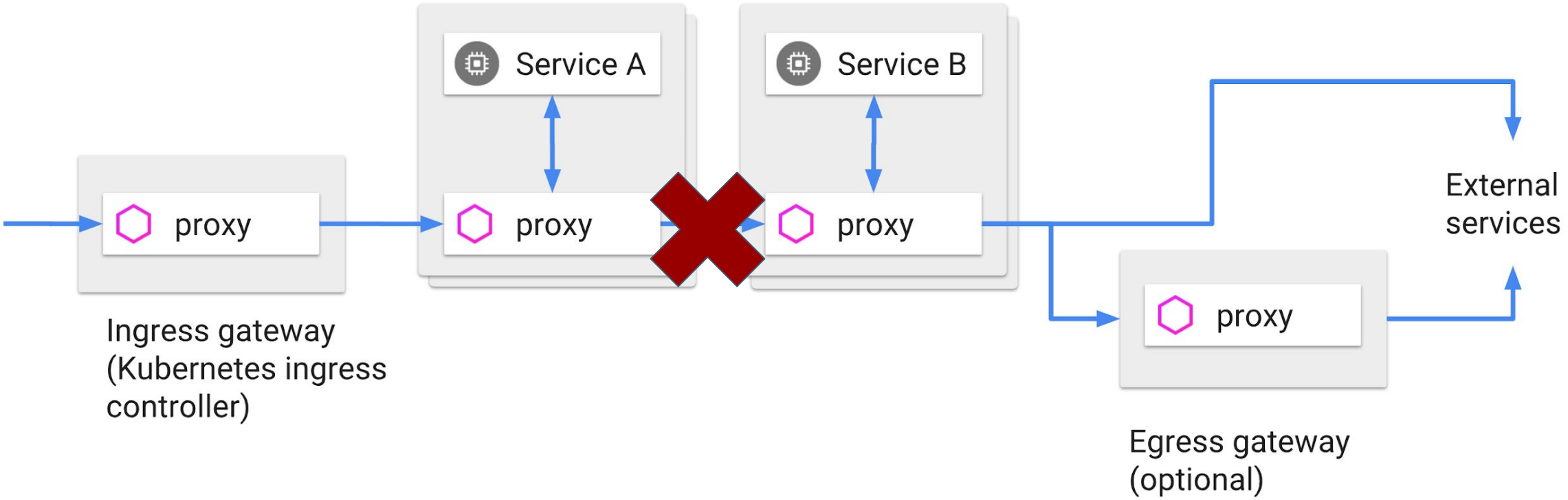
Release...with no interruptions

- Change the internal mesh policy to accept mixed auth traffic and change senders of traffic to use TLS
- Enforce TLS everywhere by policy



Release...with no interruptions

- Enforce communication restrictions via RBAC (if necessary)




KubeCon
CloudNativeCon
North America 2018
QUESTIONS?


KubeCon
CloudNativeCon
North America 2018