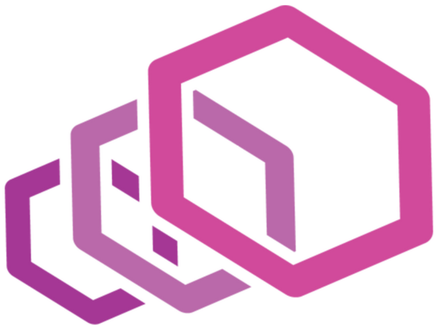
Ingress by Policy



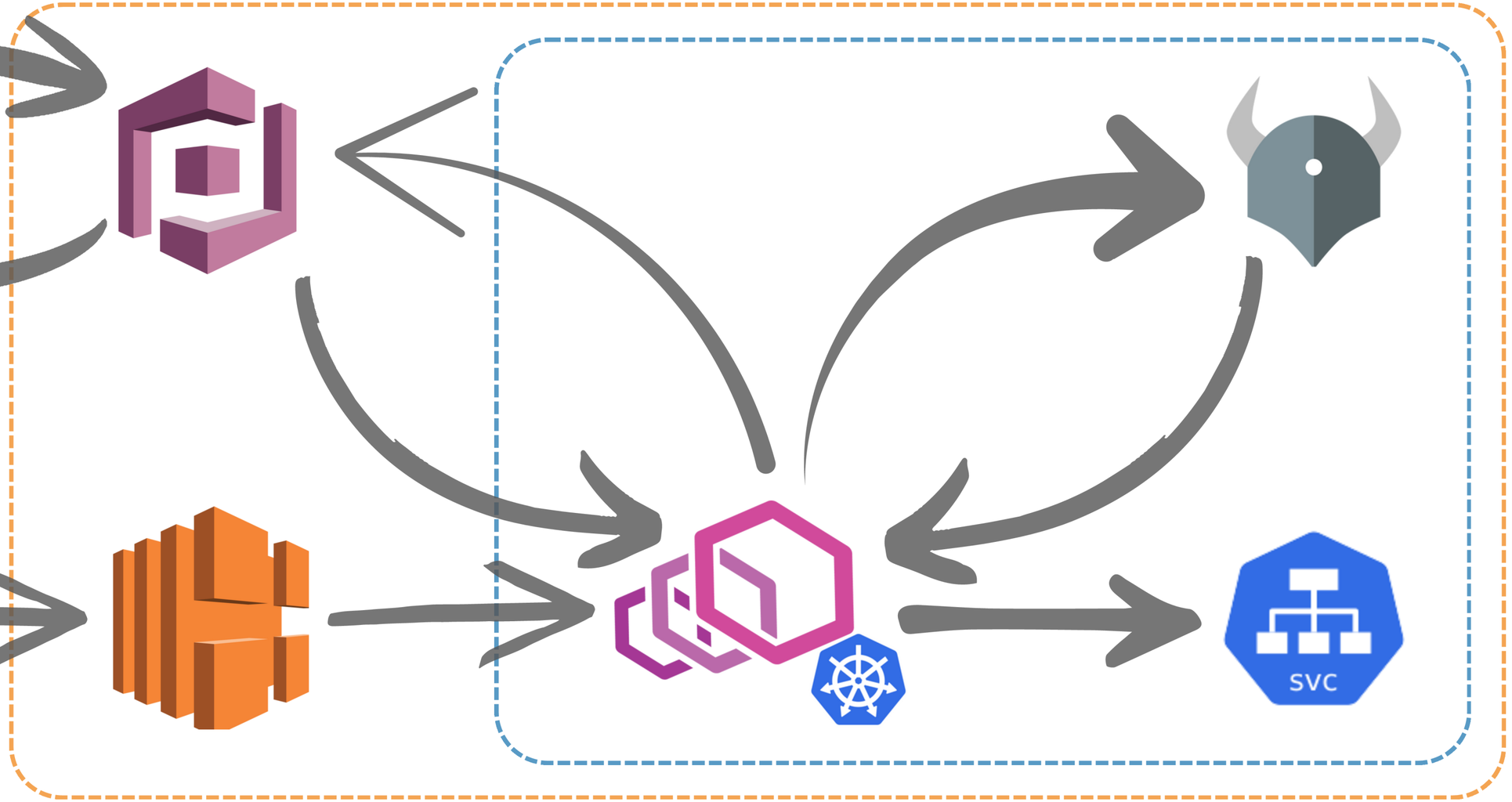
Colin J Lacy
Sr. Software Engineer
Cisco

@colinjcodesalot

Agenda

1. What are we building?
2. The YAMLs
3. And you are...?
4. You shall maybe pass...
5. Wrapping up!

What are we building?



Our Team

Arvis

Cloud Admin

Has the keys to the AWS account

Ringo

Cluster Operator

kubectl commander

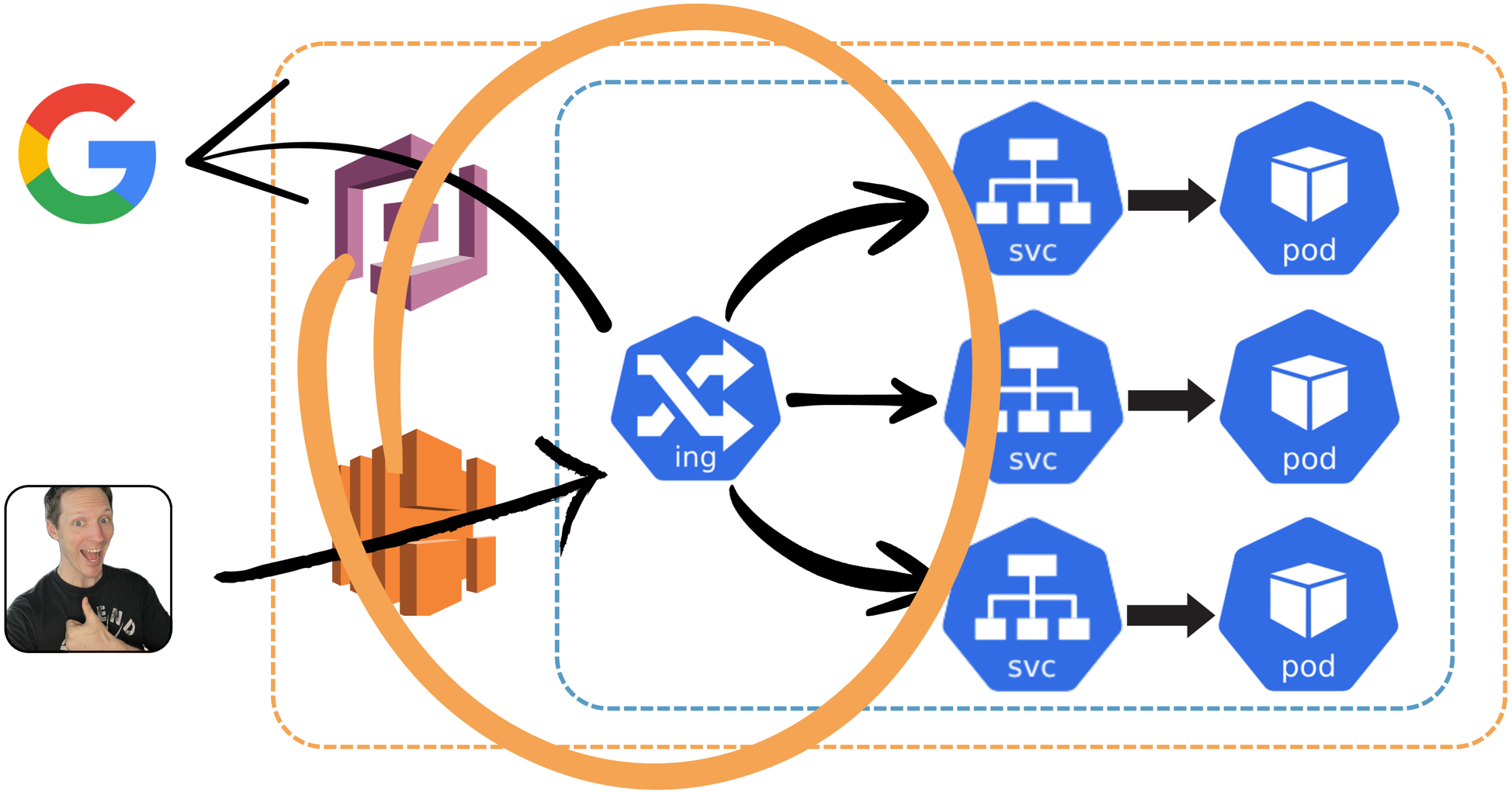
Gunther

Developer

But Claude said it was the optimal solution!

Your cluster needs an ingress

Using Kubernetes Ingress



Ingress Resource

- Defines underlying and accompanying infrastructure
- Can define security rules, e.g. federated authentication
- All traffic rules for routing to backend services
- No standard* support for any protocol beyond HTTP
- Requires a restart every time you change something

Gateway API

- Provides resources that target different roles in the team
- Flexibility beyond HTTP
- Scales for multiple use cases with resource-based configuration
- Extensible by design via the Policy Attachment model
- Plus other cool stuff (like weighted routing for A/B testing)!

Roles & Resources

GatewayClass

Defines **the implementation tooling**, and how a Gateway instance will interact with underlying infrastructure

Gateway

Instance of a **GatewayClass**, deploys the ingress pod, plus the underlying infra (e.g. load balancers) defined by the **GatewayClass**

<Proto>Route

Routing behavior for traffic coming in through a **Gateway** to a backend resource, with multiple protocols supported (e.g. **GRPCRoute**, **HTTPRoute**)

Implementations

- Acnodal EPIC
- Agent Gateway
- Airlock Microgateway
- Amazon Elastic Kubernetes Service (GA)
- Apache APISIX (beta)
- Avi Kubernetes Operator
- Azure Application Gateway for Containers (GA)
- Cilium (beta)
- Contour (GA)
- [illegible]segres[illegible](GA)
- [illegible](Ambassador API Ga[illegible](alph[illegible]
- Envoy Gateway (GA)
- Flomesh Service Mesh (beta)
- Gloo Gateway (GA)
- Google Kubernetes Engine (GA)
- HAProxy Ingress (alpha)
- HAProxy Kubernetes Ingress Controller (GA)
- HashiCorp Consul
- Istio (GA)
- kgateway (GA)
- Kong Ingr[illegible]ntroller (GA)
- Kon[illegible]way Operator (GA)
- [illegible]ernor(work in progress)
- Kuma (GA)
- LiteSpeed Ingress Controller
- LoxiLB (beta)
- NGINX Gateway Fabric (GA)
- ngrok (preview)
- STUNner (beta)
- Traefik Proxy (GA)
- Tyk (work in progress)
- WSO2 APK (GA)

- Built on top Envoy Proxy, a CNCF Graduated project
- Extends the Gateway API with additional resources
- Allows broad and fine-grained security policy assertion
- Supports multiple security policies within the same Gateway
- Can also handle authorization, or configure external authorization

Load Balancer

Proxy

Service

---

may control

controls

configure behavior

Gateway

Extensions

Essential extensions

GatewayClass

↓

EnvoyProxyConfig

Gateway

↓

SecurityPolicy

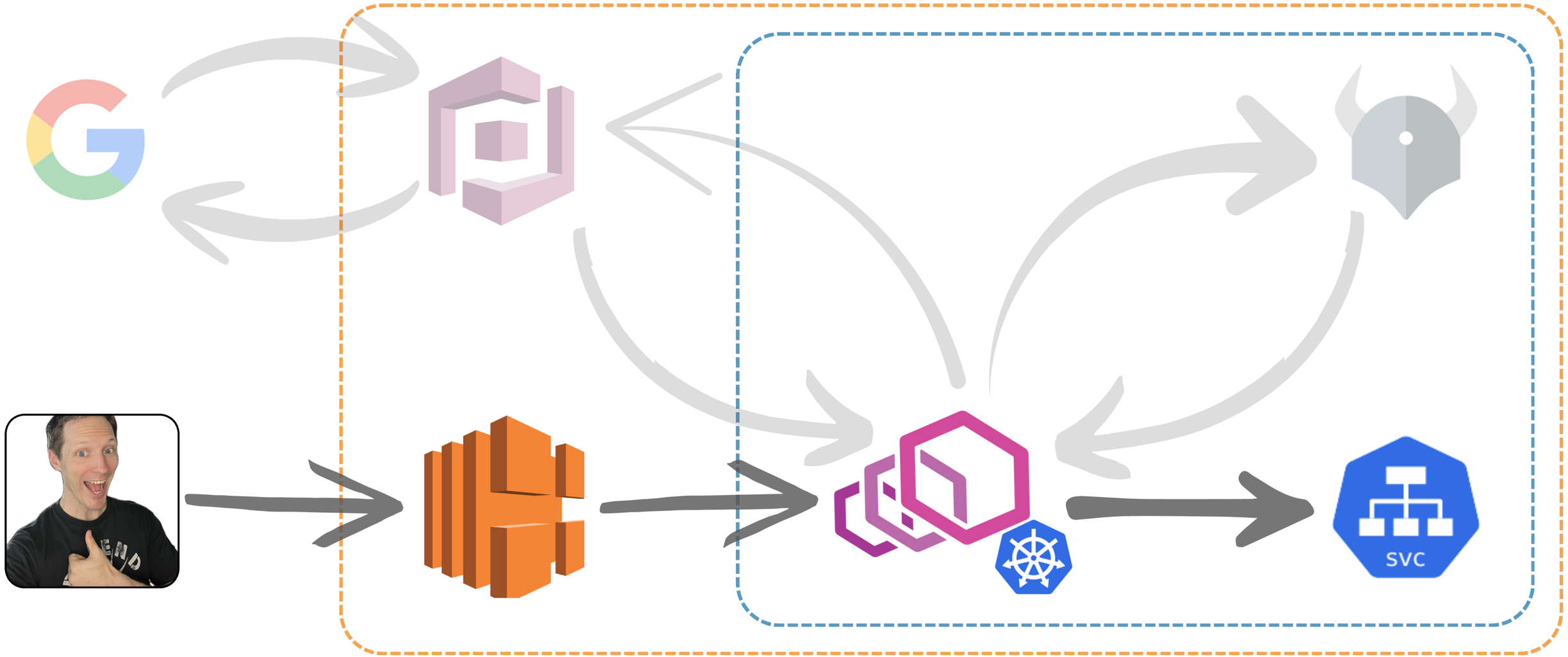
<Proto>Route

↓

Backend

Admittedly, the lines can get a little blurred…

The YAMLs


SVC

And you are...?

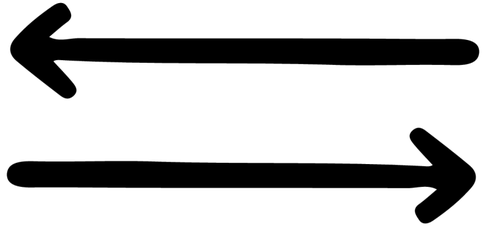
SecurityPolicy Resource

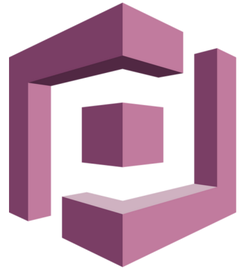
- Sets security behavior for a target resource
- Policies can be set on a specific route, or an entire gateway
- Both authentication and authorization supported
- Allows Lua and Golang scripting for programmatic logic
- Supports OIDC, JWT, API Key, and Basic authn mechanisms

3. Based on Cognito client, redirects user to Google

6. Cognito exchanges auth code for user data

4. The user signs in

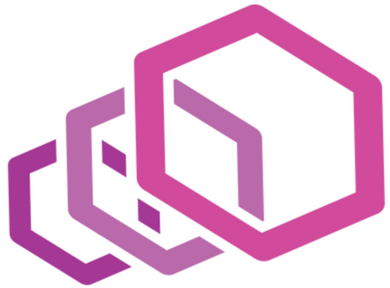




5. Redirects user with auth code

2. Redirects user to Cognito

7. Cognito issues JWT, redirects to EG

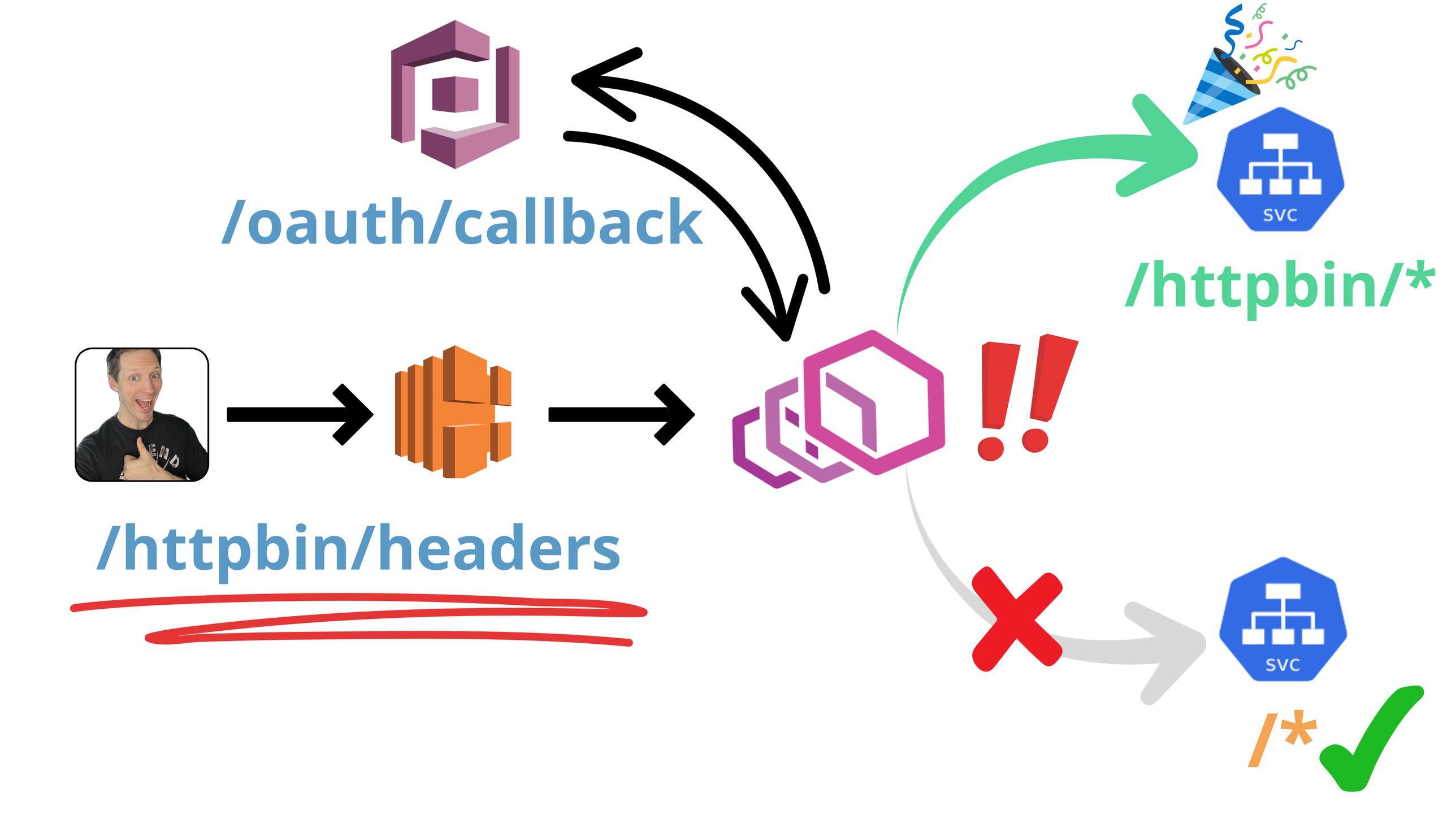


8. Encrypts JWT in cookie

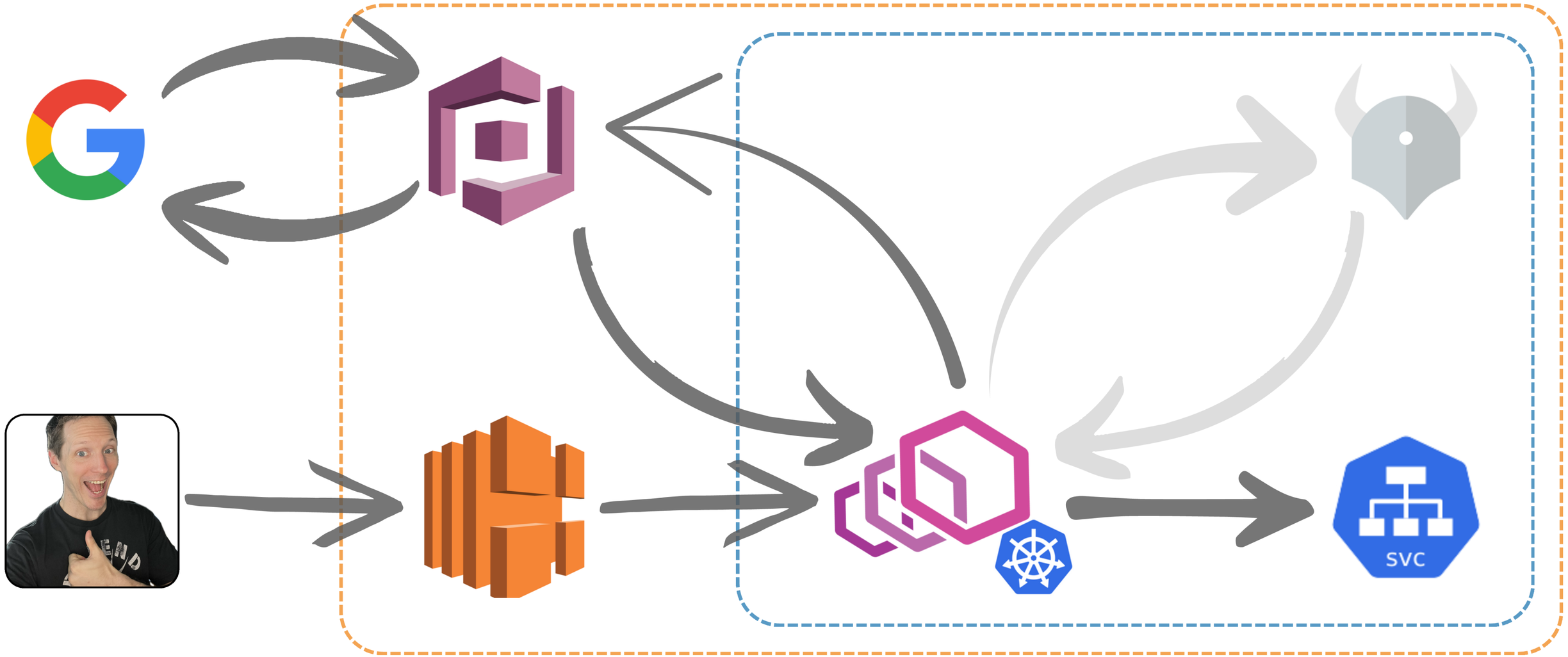
1. Looks for valid cookie

Something to be aware of

- Envoy Gateway will redirect a user back to the requested route
- The registered OIDC redirect URL **must** be a valid HTTPRoute
- Envoy Gateway will then redirect the user to the destination URL
- This is a concern for Gateway-wide SecurityPolicies


/oauth/callback
/httpbin/*
SVC
/httpbin/headers
!!
SVC
/*

You shall maybe pass...


SVC

Envoy Proxy ExtAuth

- Defers authorization to an external service
- External service can be called over HTTP or gRPC
- External service will respond with success if user is authorized
- If the external service responds with error status, user is 403'ed
- Allows for separation of concerns and independent revisions

What is OPA?

- “An open source, general-purpose policy engine that unifies policy enforcement across the stack”
- Multiple deployment models – sidecar, daemon, RESTful server/deployment, CLI
- Built-in policy testing framework
- Syncs policies from remote store (e.g. S3) on a configurable timer

What is Rego?

- A purpose-built language for writing and evaluating policy as code
- Uses a declarative syntax for matching inputs to conditions
- If at any point there is a mismatch, the data does not adhere to the policy

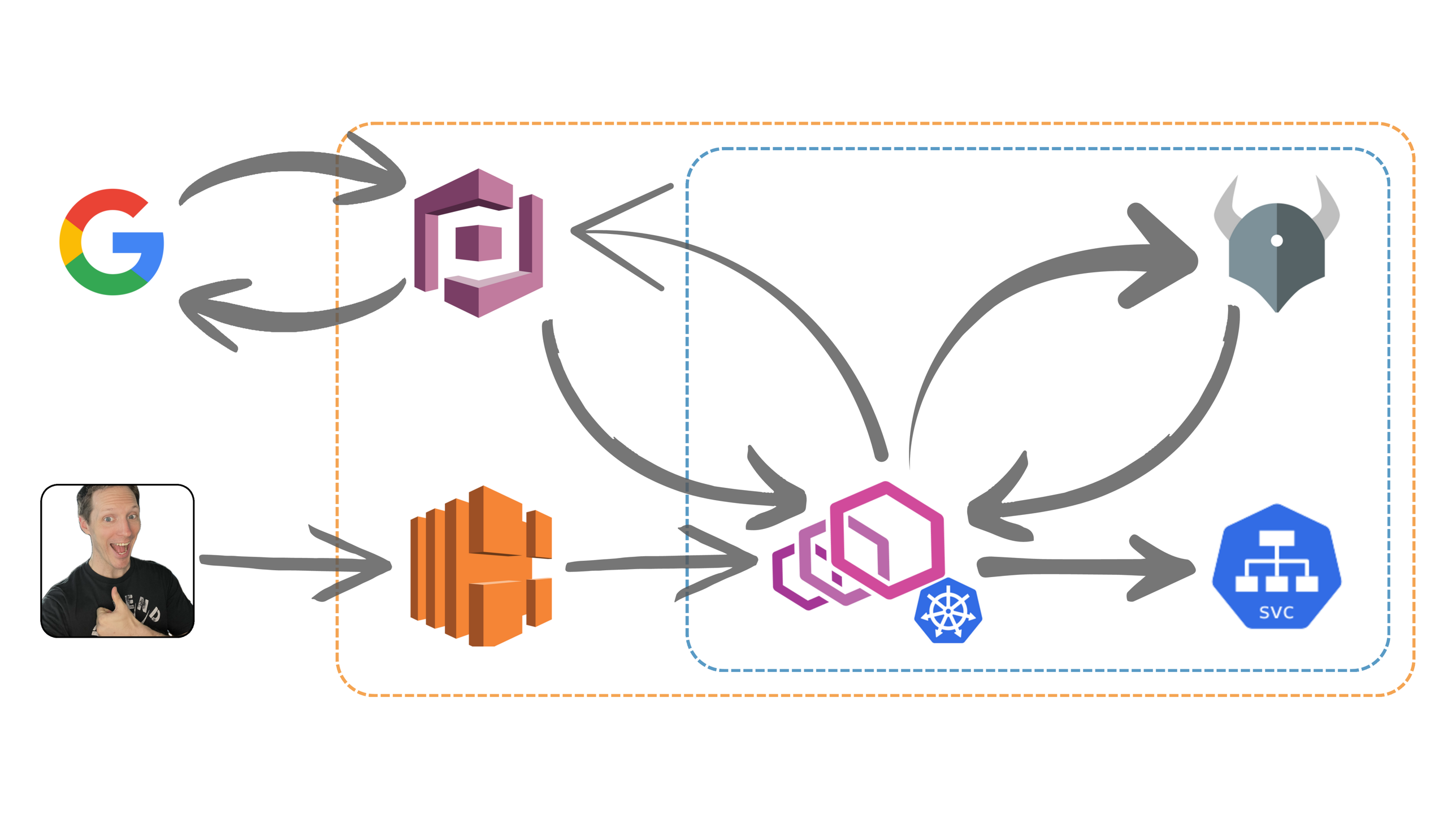
Rego Playground has useful examples

ReferenceGrant Resource

- By default, a Gateway API resource can only reference things in its own Namespace
- This is a security setting imposed by the Kubernetes Gateway API
- In order to reference things outside of the Gateway's Namespace, we add a ReferenceGrant to the target Namespace

The other thing...

- Envoy Proxy was born 7 years before the Gateway API
- Use cases well beyond authorization and cluster ingress
- Has a default filter order that can be rearranged
- ...and must be in order for the ExtAuth check to happen after the OIDC login flow


SVC

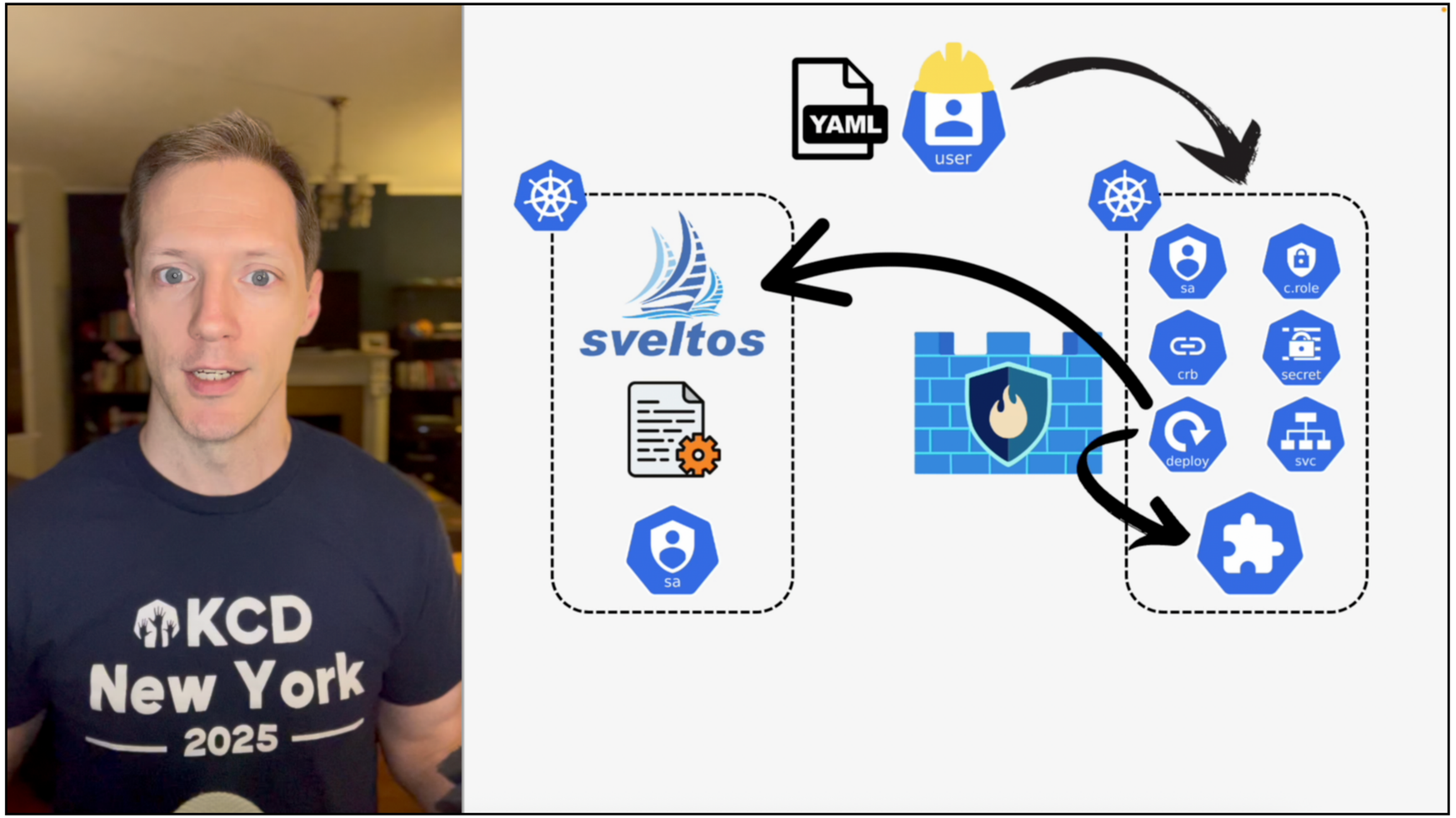
Wrapping up!

Where to go from here?

- Try using JWT clients to authenticate
- Route-specific SecurityPolicies with different secrurity settings
- Traffic policies around rate limiting, failover, circuit breaking
- Extension management that I don’t even know about
- Experiment with OPA’s Rego policies
- Set policies on Envoy Gateway resources with OPA Gatekeeper

AWS Network Load Balancers

Subscribe on YouTube



Looking for contributors?

“Yes.”

Anders Eknert

OPA Maintainer

“Yes.”

Arko Dasgupta

Envoy Gateway Maintainer