

# Service Mesh AND API Management Teamwork at its Best

Sven Walther

API Conference Berlin 2022

# Sven Walther

Principal Solutions Engineer EMEA, Kong

@svenwal

- ~10 years in API Management
- ~20 years being an API consumer
- “XML-over-http” years old
- Located in Berlin
- Amiga > Mac >= Linux > Windows

sven@konghq.com  
<https://svenwal.de>

# Some questions



Background:  
Olga Kobruseva <https://www.pexels.com/de-de/foto/fragezeichen-auf-papierhandwerk-5428836/>

# Who is using an API Gateway?

# Who is using Kubernetes\*?

\* includes OpenShift

# Who is using Kubernetes\* ... in production?

\* includes OpenShift

Who is using **only** Kubernetes\* in production?

\* includes OpenShift

Who knows what a service mesh is?



Who is already using a service mesh?

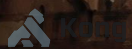
Who is already using a service mesh  
... in production?

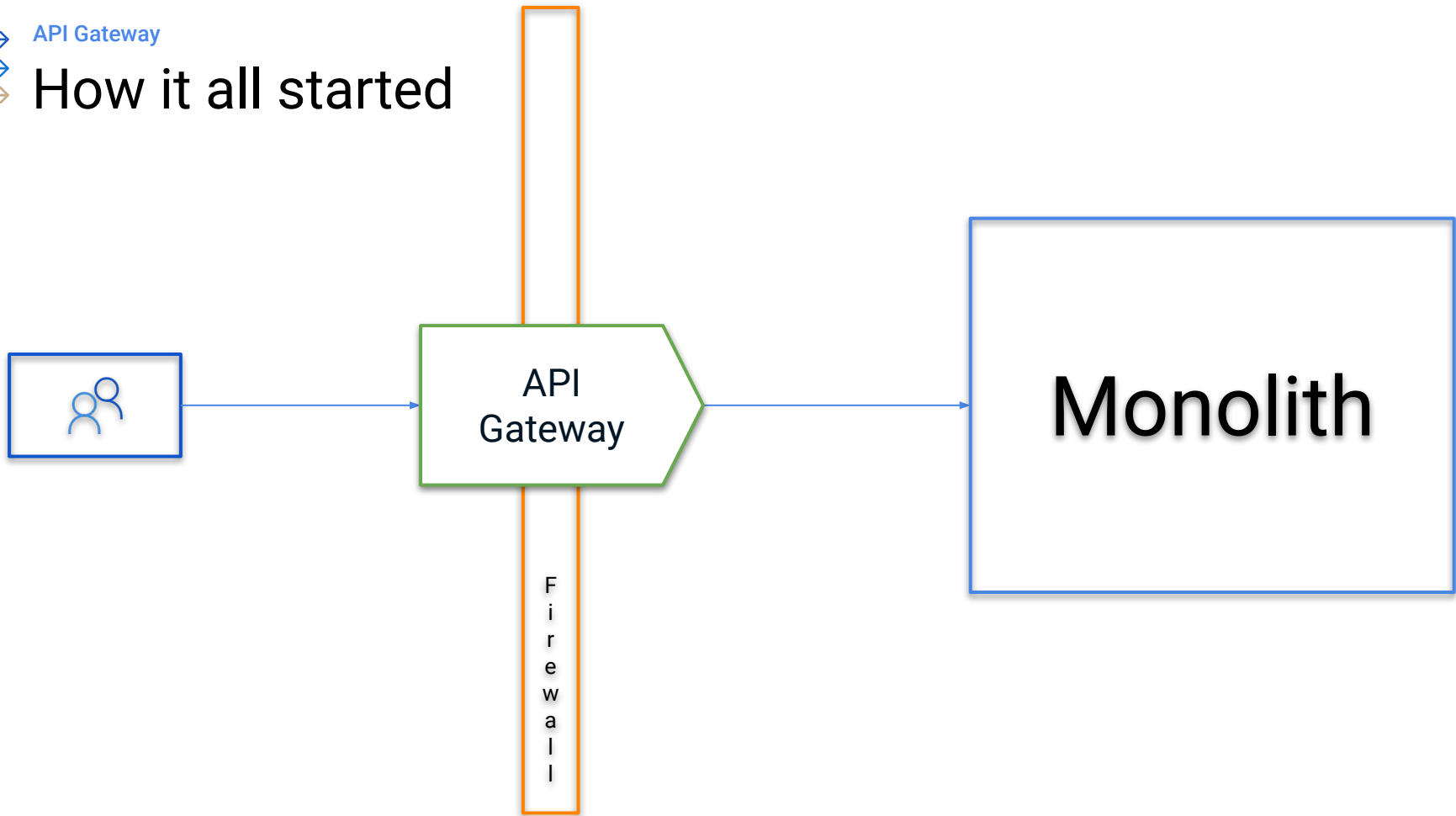
# Who is multi-cloud?

# API Gateways

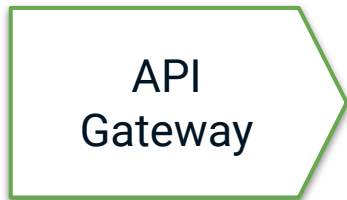
Serving the world since more than 20 years

Background: Frans van Heerden <https://www.pexels.com/de-de/foto/foto-von-schloss-unter-wolken-1022698/>



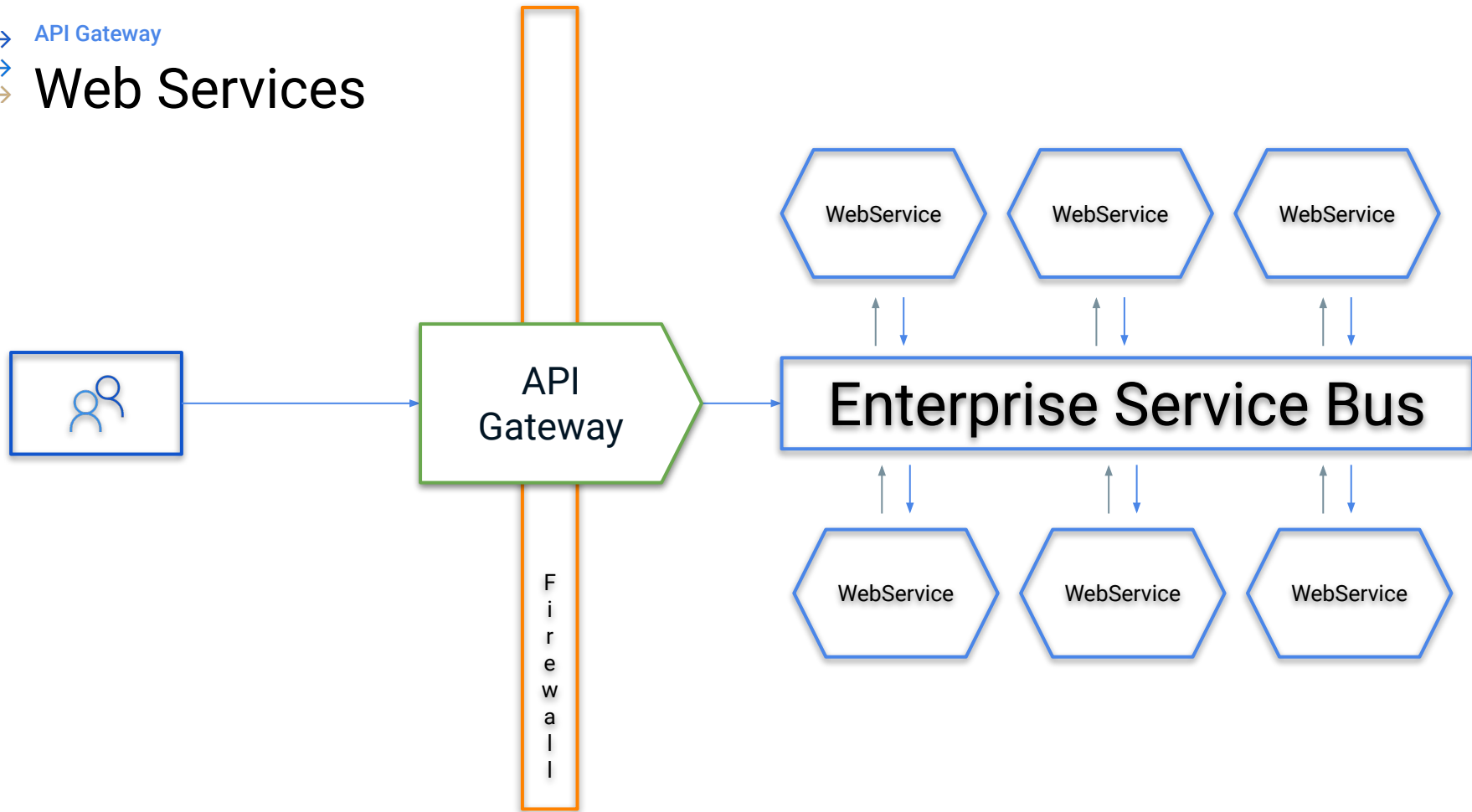


# Functionality

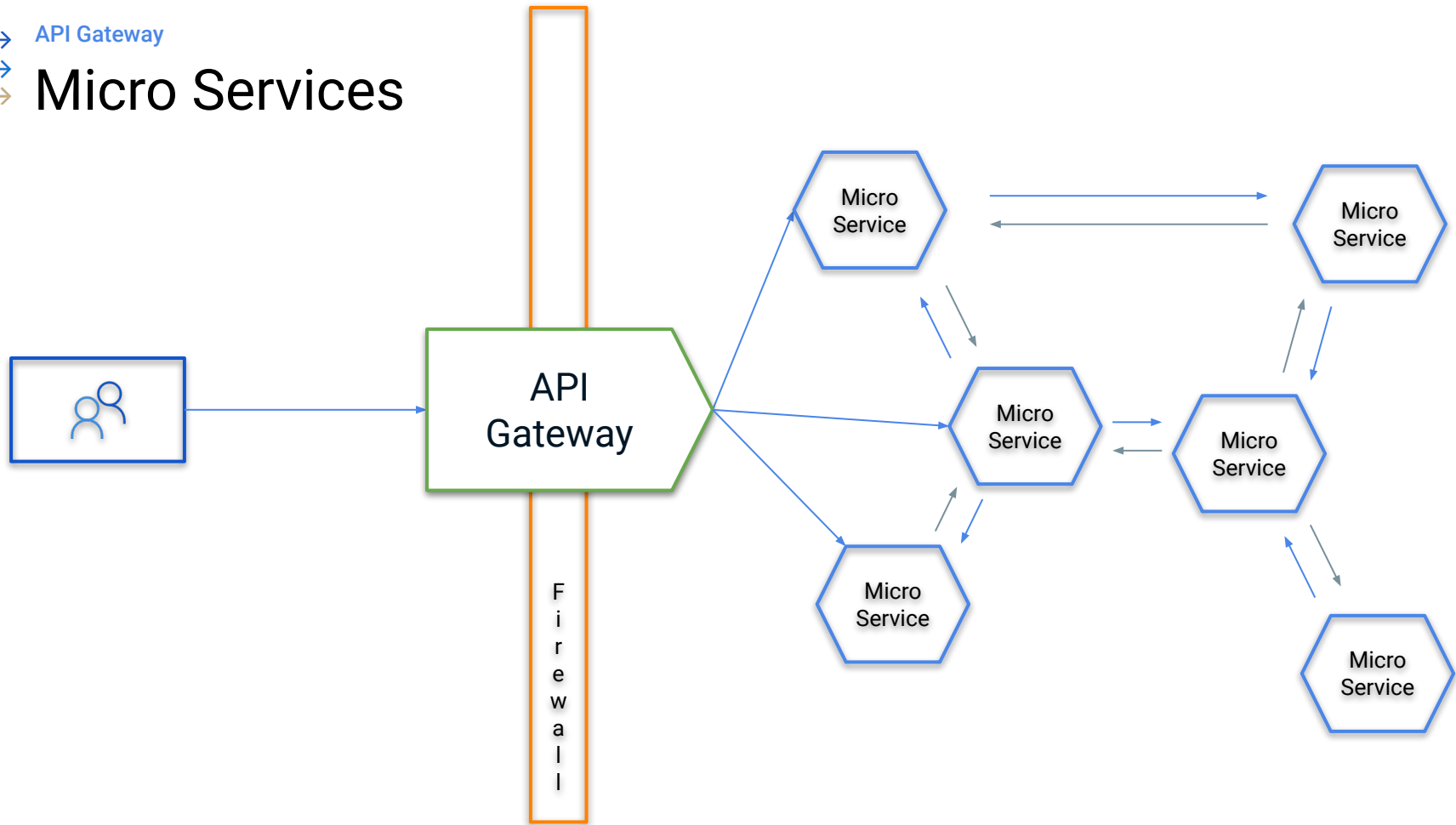


- Routing
- Authentication
- Authorization
- Monitoring
- Logging
- Rate Limiting
- Caching
- ...

API Gateway  
Web Services

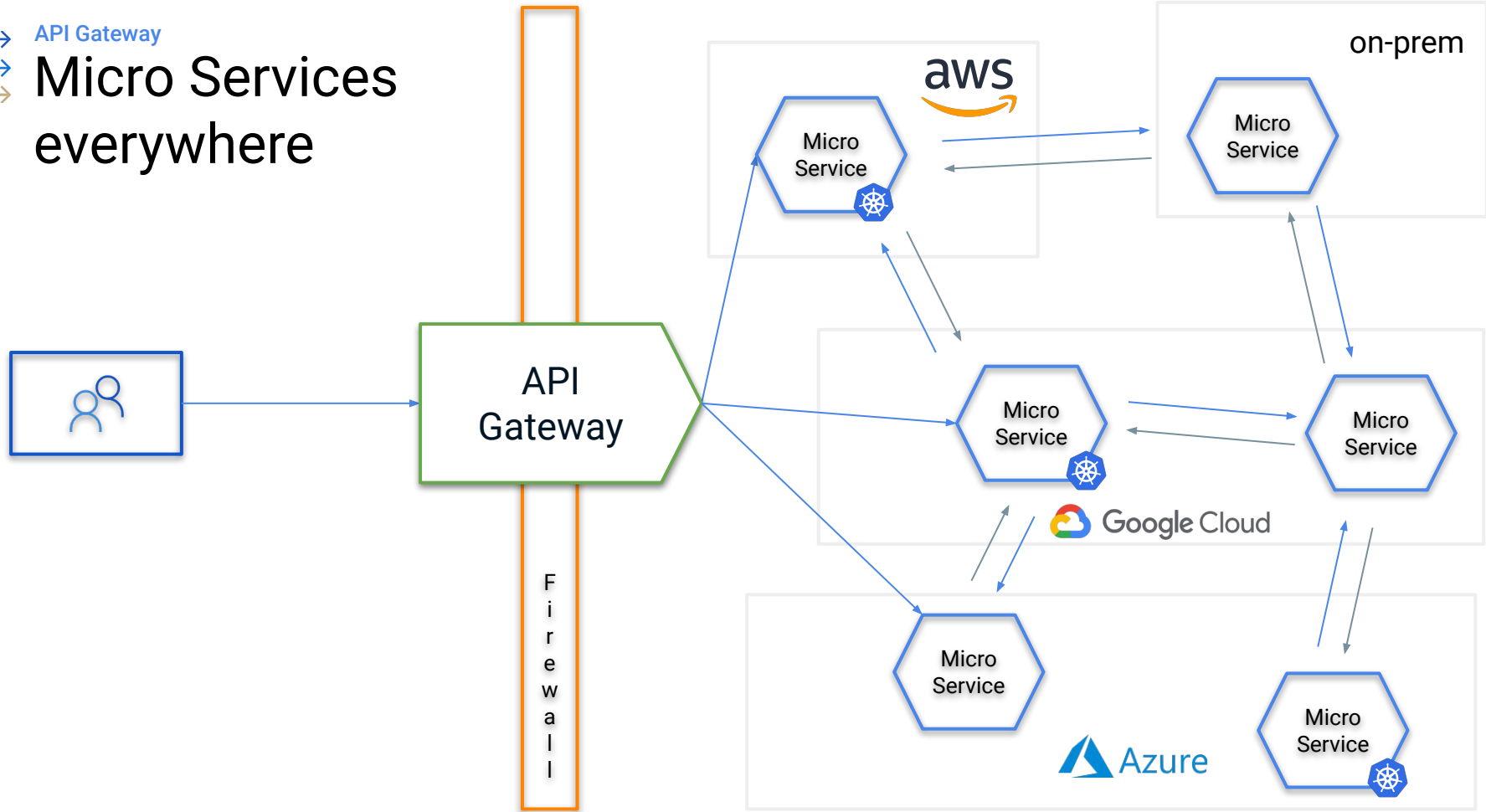


API Gateway  
Micro Services





API Gateway  
Micro Services  
everywhere



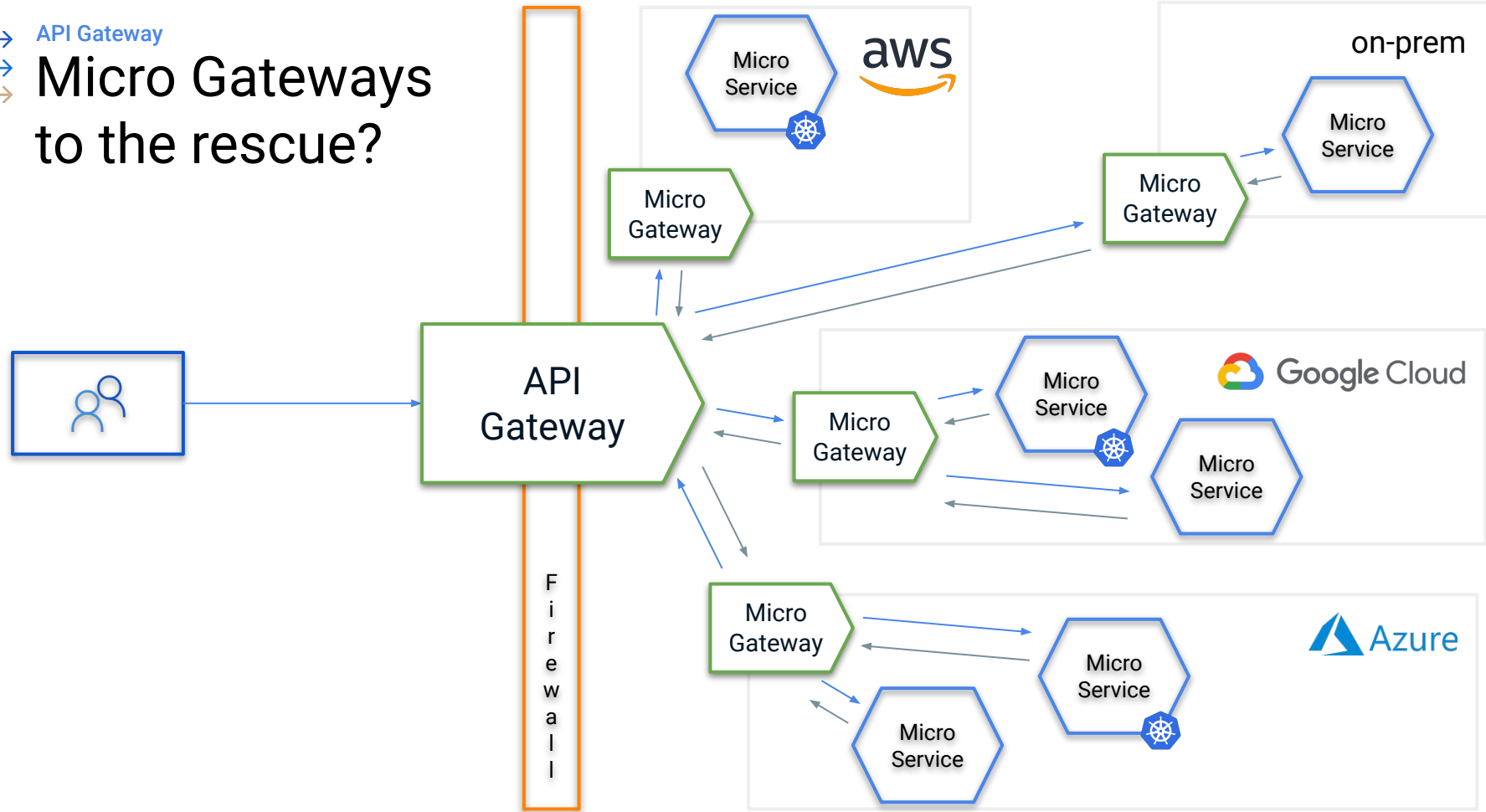
# Micro Services



Background: <https://www.pexels.com/de-de/foto/abstrakt-farbe-fix-reparieren-4480541/>

API Gateway

# Micro Gateways to the rescue?



“Give a boy a hammer and everything he meets has to be pounded”

Kaplan’s Law of the Instrument:  
[https://en.wikipedia.org/wiki/Law\\_of\\_the\\_instrument](https://en.wikipedia.org/wiki/Law_of_the_instrument)

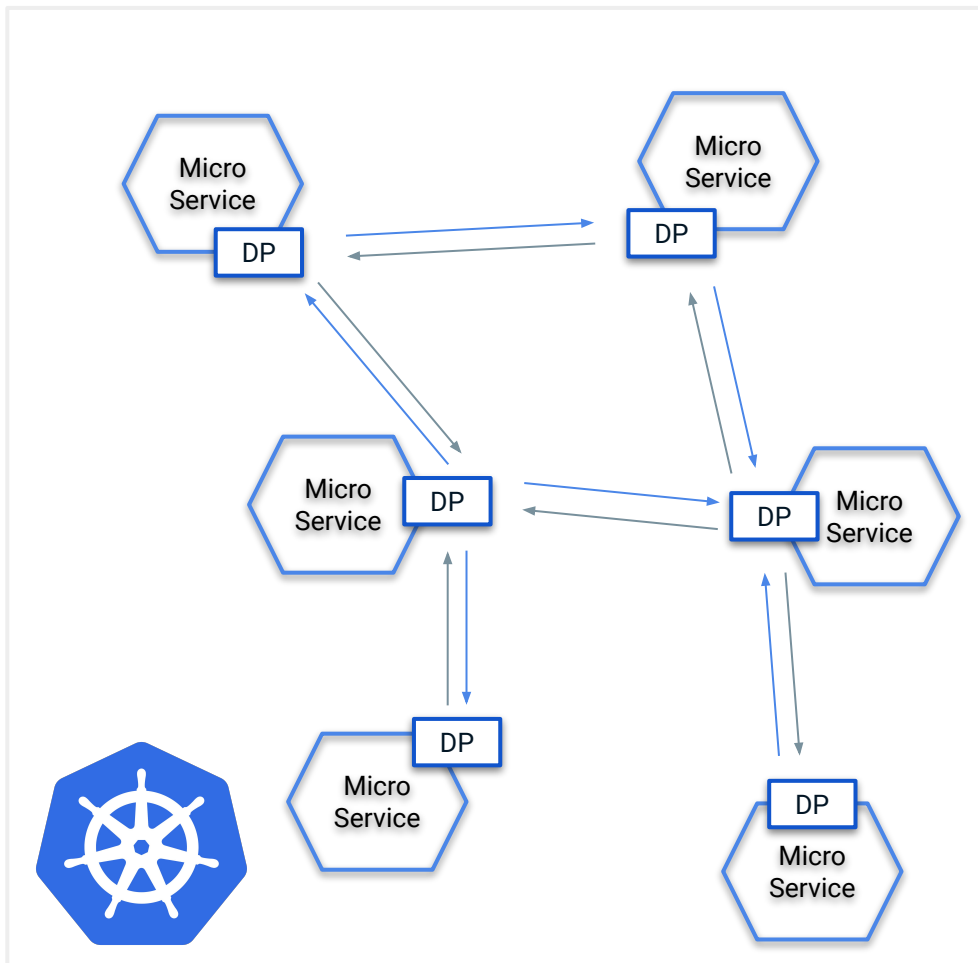
Background: Los Muertos Crew <https://www.pexels.com/de-de/foto/holz-hande-hammer-nagel-8447781/>

# Service Mesh

# The idea

- Everything encrypted (TLS)
- Everything authenticated and authorized (mTLS)
- Everything monitored
- ...

Everything means:  
=> within the cluster

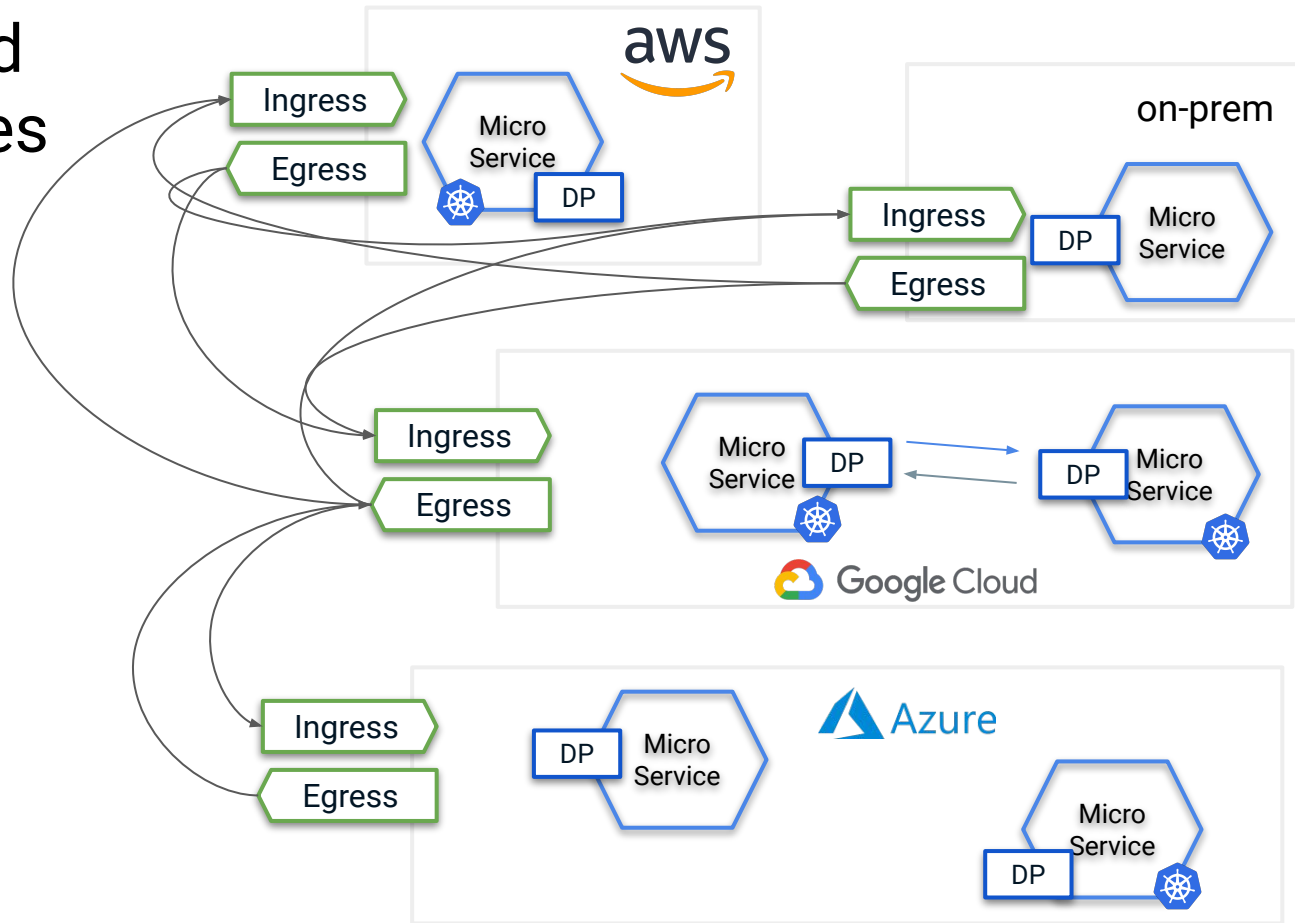


# Functionality

Service  
Mesh

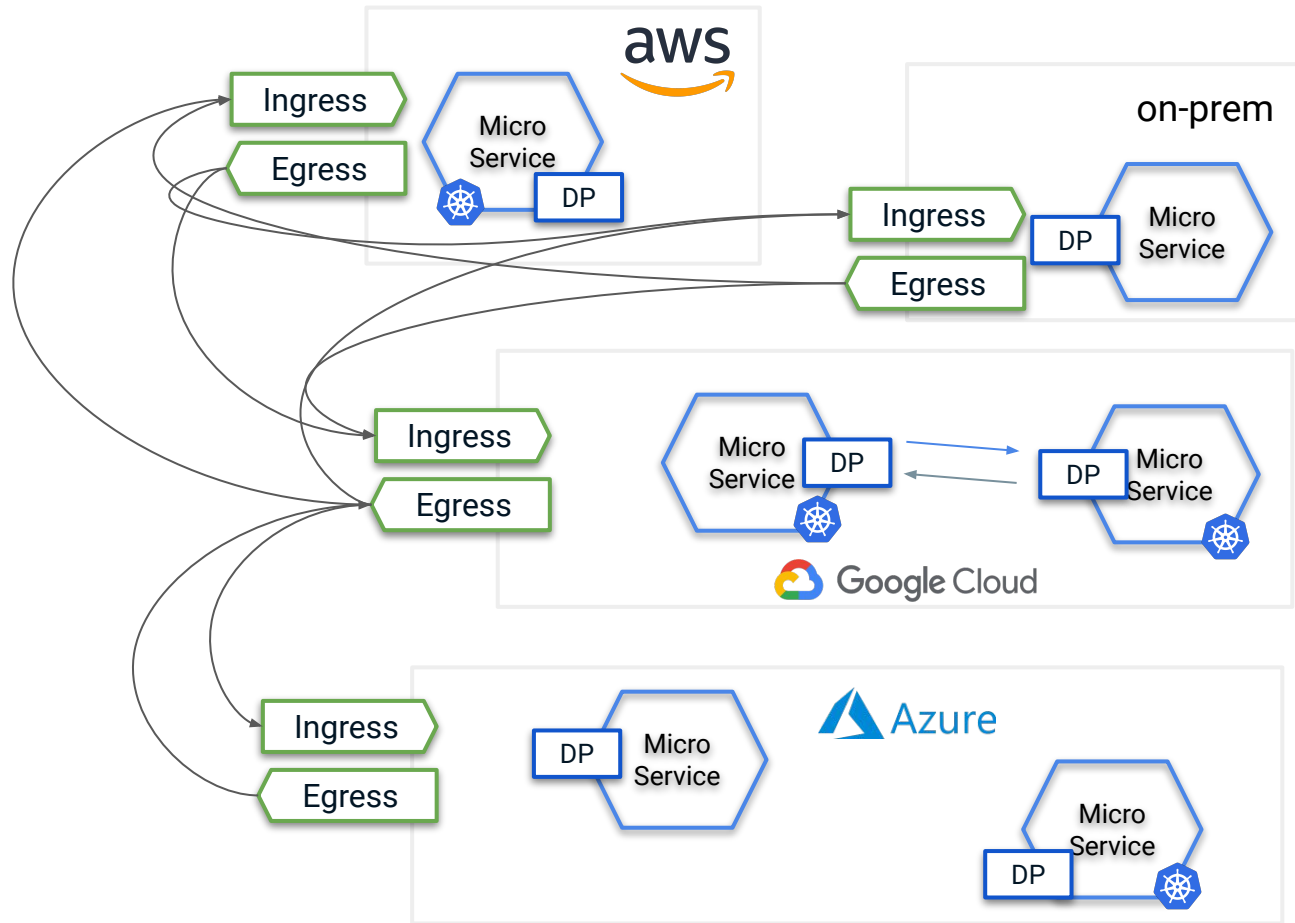
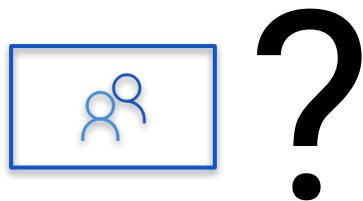
- Routing
- Encryption
- AuthN & AuthZ (mTLS)
- Load Balancing
- Monitoring
- Logging
- Tracing

# Multi Cloud and more challenges



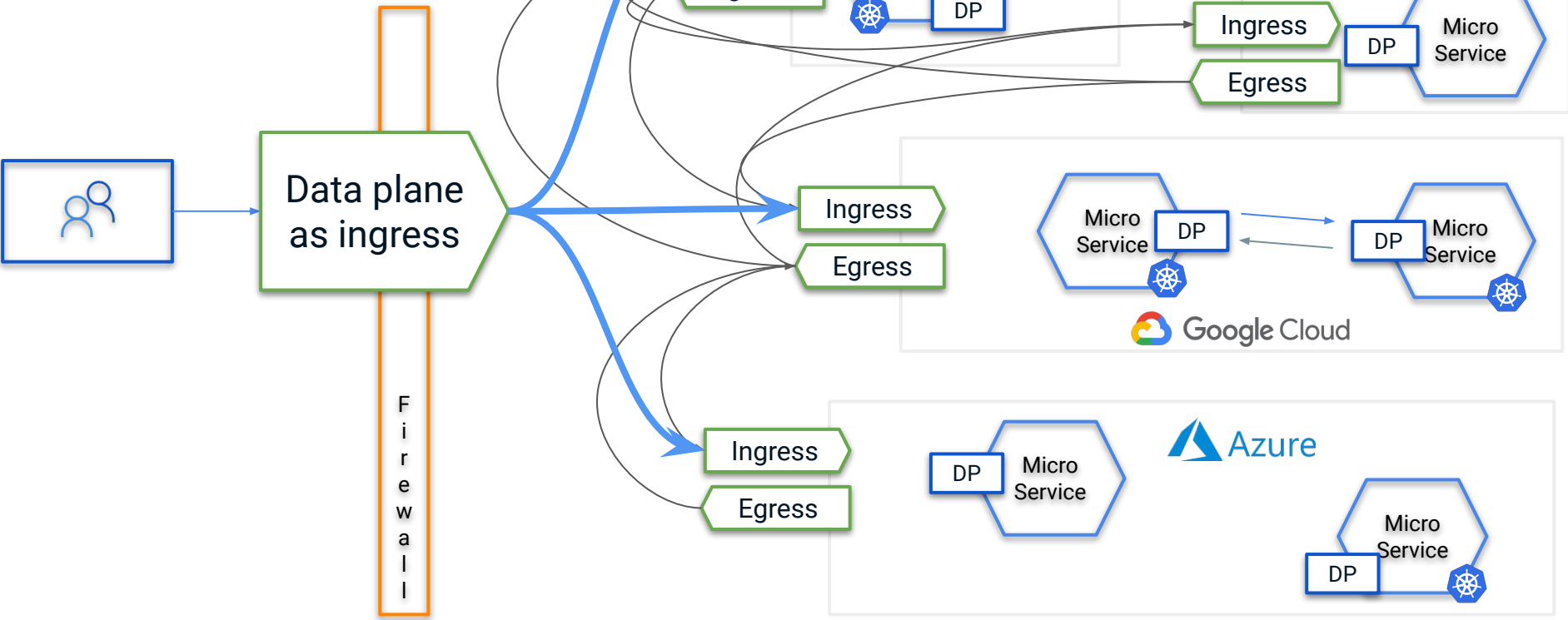


What about our customers, clients,  
partners, ...





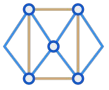
# Data plane as ingress gateway?



“Give a boy a hammer and everything he meets has to be pounded”

Kaplan’s Law of the Instrument:  
[https://en.wikipedia.org/wiki/Law\\_of\\_the\\_instrument](https://en.wikipedia.org/wiki/Law_of_the_instrument)

Background: Los Muertos Crew <https://www.pexels.com/de-de/foto/holz-hande-hammer-nagel-8447781/>



# Different use cases - different tools!

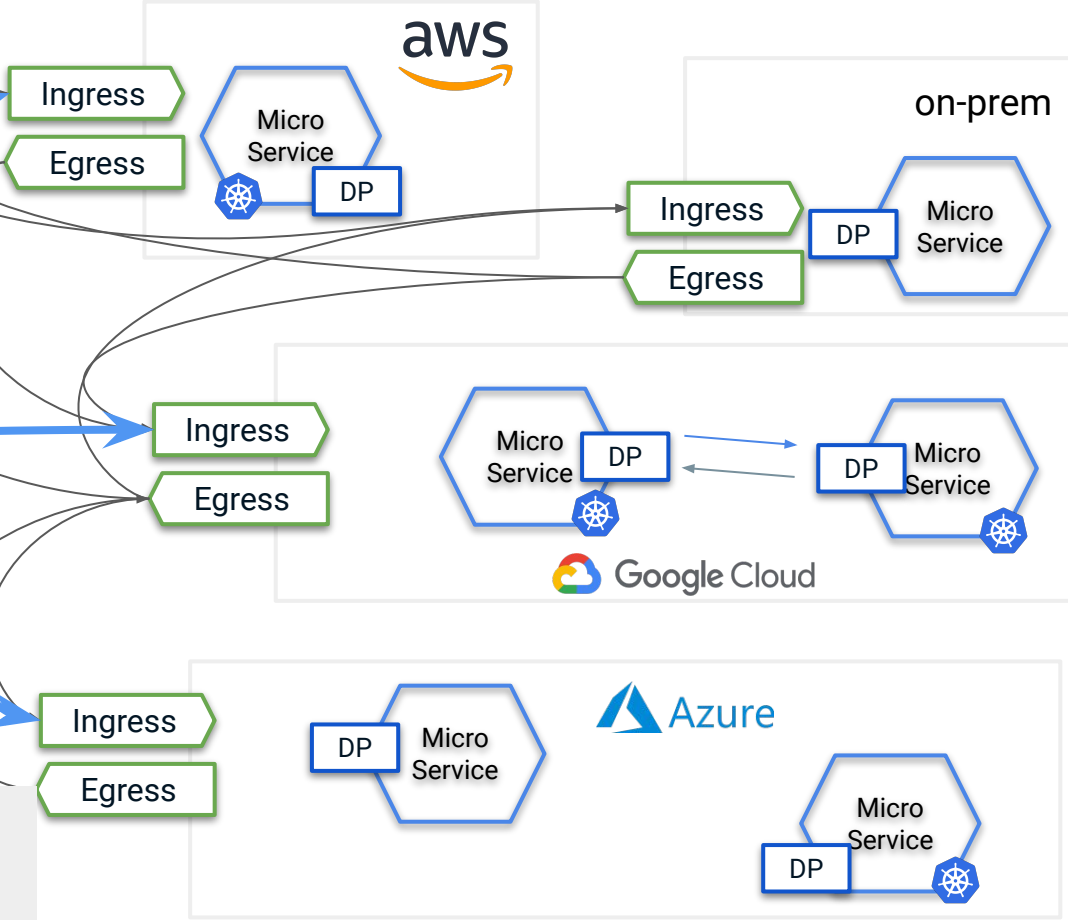
## Data plane as ingress



Firewall

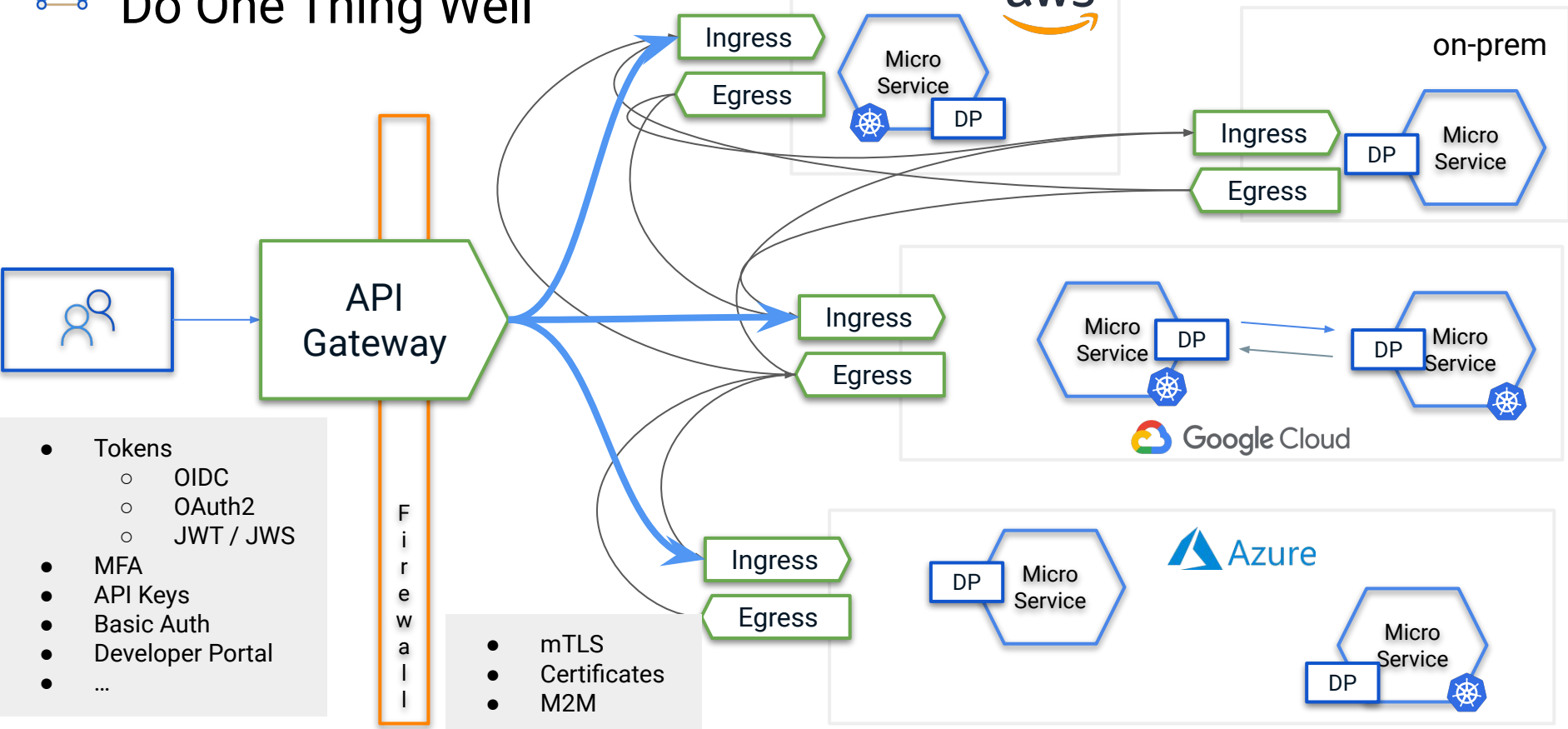
- Tokens
  - OIDC
  - OAuth2
  - JWT / JWS
- MFA
- API Keys
- Basic Auth
- Developer Portal
- ...

- mTLS
- Certificates
- M2M





# Do One Thing Well



**API Gateway**

- Tokens
  - OIDC
  - OAuth2
  - JWT / JWS
- MFA
- API Keys
- Basic Auth
- Developer Portal
- ...

**Firewall**

- mTLS
- Certificates
- M2M

# The right tool for the right audience

## API Gateway

- (Mainly) external focused
- Human being and machine to machine
- Hard to provision certificates to external machines
- Token focused (but also api keys and similar)
- Documentation for developers
- Routing and load balancing from external to internal
- Automation is a strong should be

## Service Mesh

- Internal focused
- Everything machine to machine
- Certificates can be issued and updated automatically
- Untrusted wire
- Routing and load balancing
- Automation is a must be
- Sidecar and eBPF pattern enforce minimal data plane size (hardware needs)

# Teamwork



Background: fauxels <https://www.pexels.com/de-de/foto/foto-von-menschen-in-der-nahe-von-holztisch-3184418/>



# Collaboration

Where is the teamwork?

Gateway and mesh share central solutions

- Common pattern of configuration
- Logging
- Monitoring
- Tracing
- Service to service security patterns
- IdP / tokens (OpenPolicyAgent)
- Gateway routes to mesh, mesh routes to active and healthy endpoints

# Live Demo



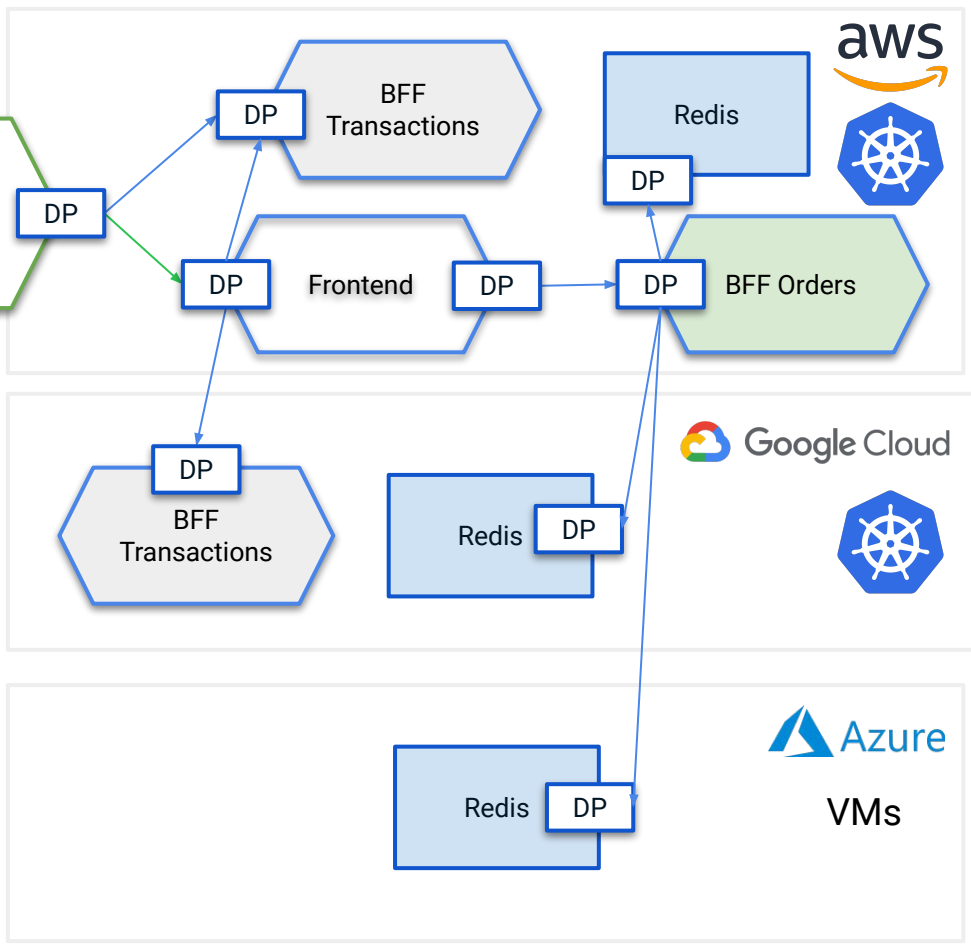
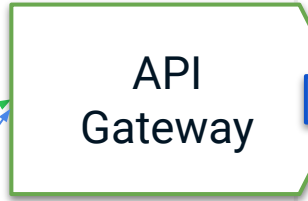
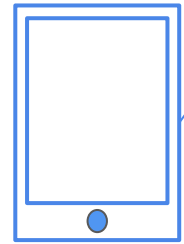
API Gateway AND Service Mesh

Live



Browser  
OIDC

API  
apikey  
rate limited



# Q&A

# Thank you

Slides available at <https://bio.walther.world/>