

HashiCorp

Consul



Connect and Secure Any Service

A multi-cloud service networking platform to connect and secure any service across any runtime platform and public or private cloud

Christoph Puhl
Consul Technology Specialist | Field CTO Office | HashiCorp
cpu@hashicorp.com | [@cpu601](https://twitter.com/cpu601)



The Road to Service Mesh



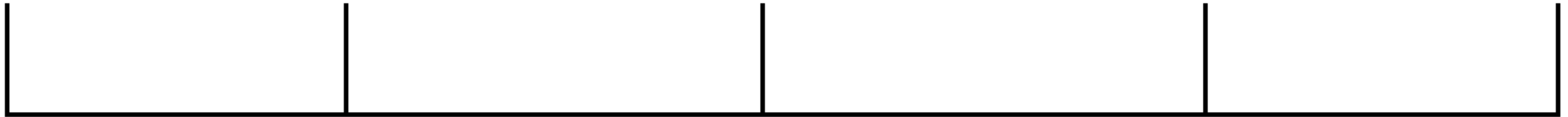
Mainframe

Bare Metal

Virtual Machine

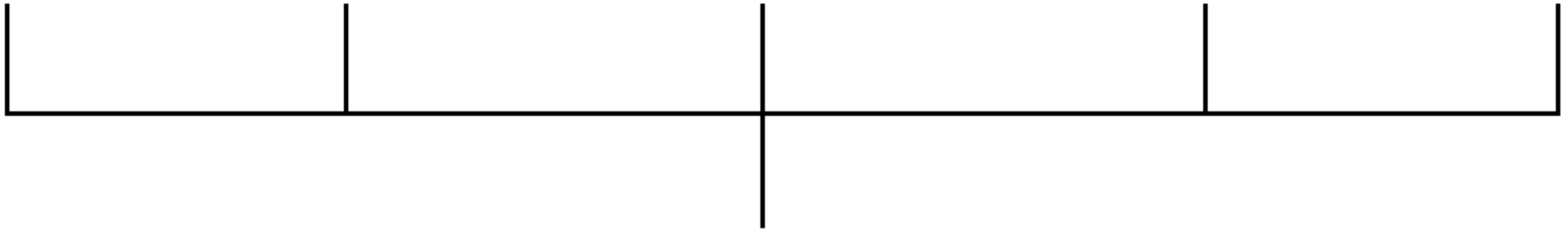
Container

Serverless



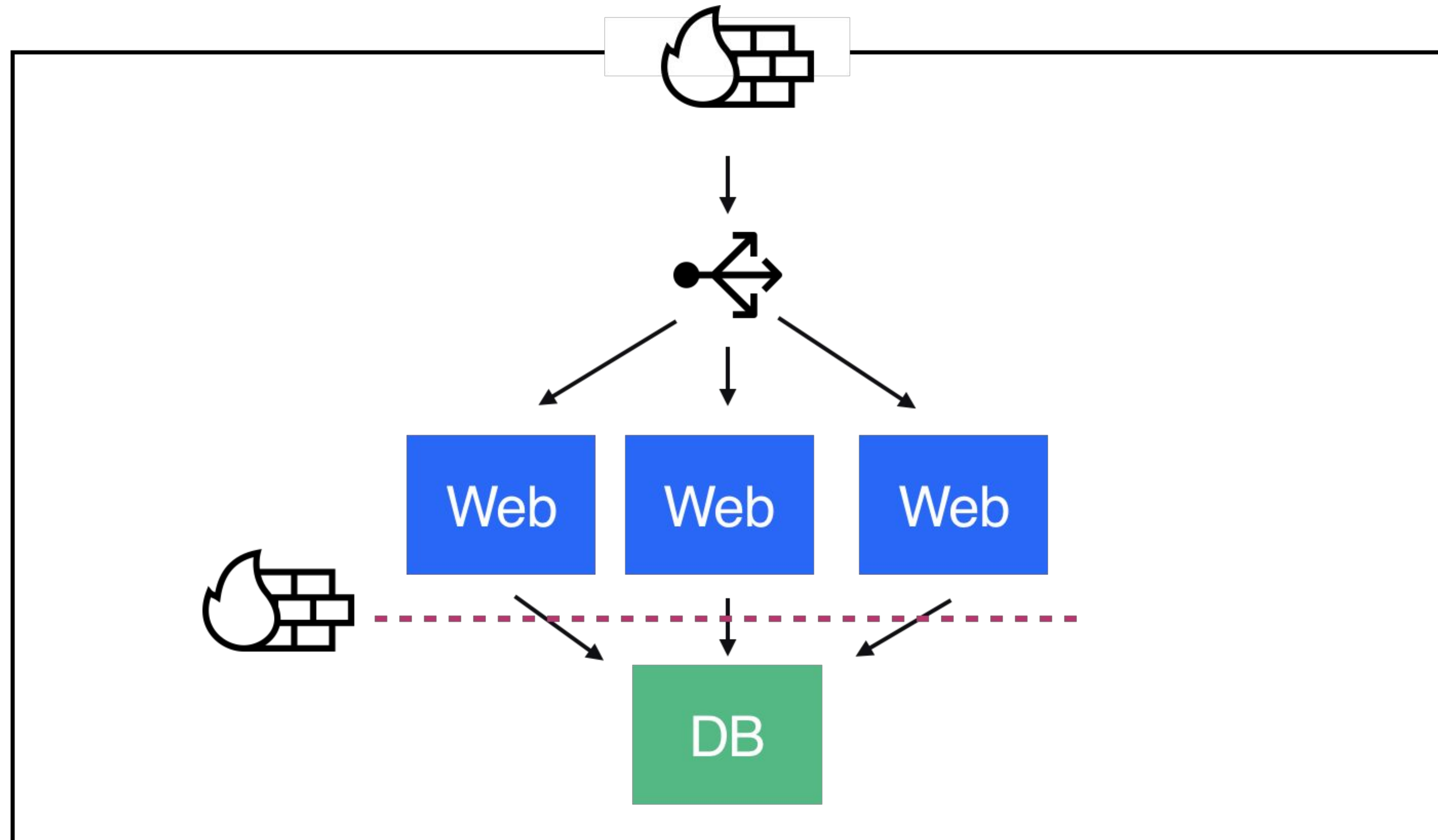


Mainframe Bare Metal Virtual Machine Container Serverless

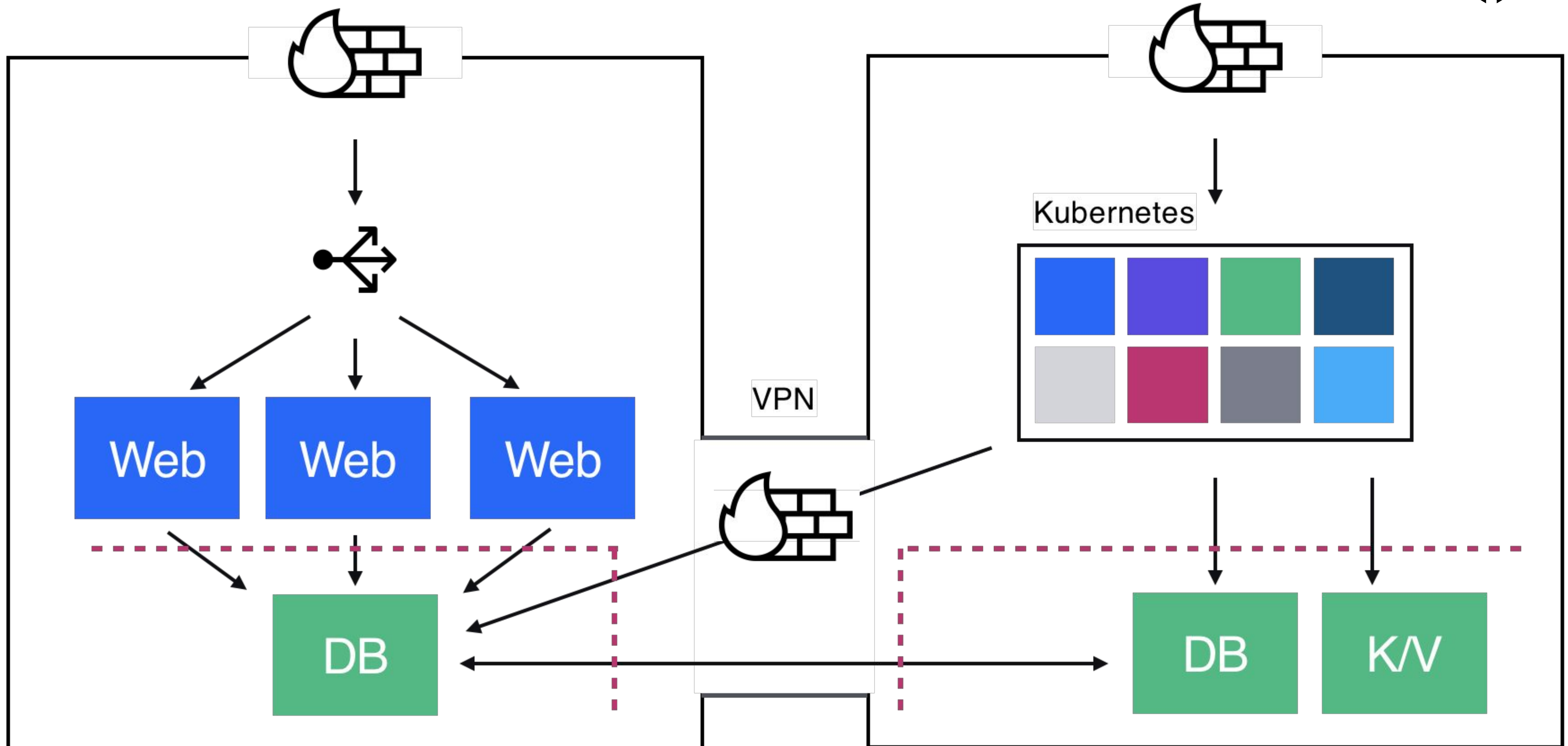


Network

Traditional Datacenter



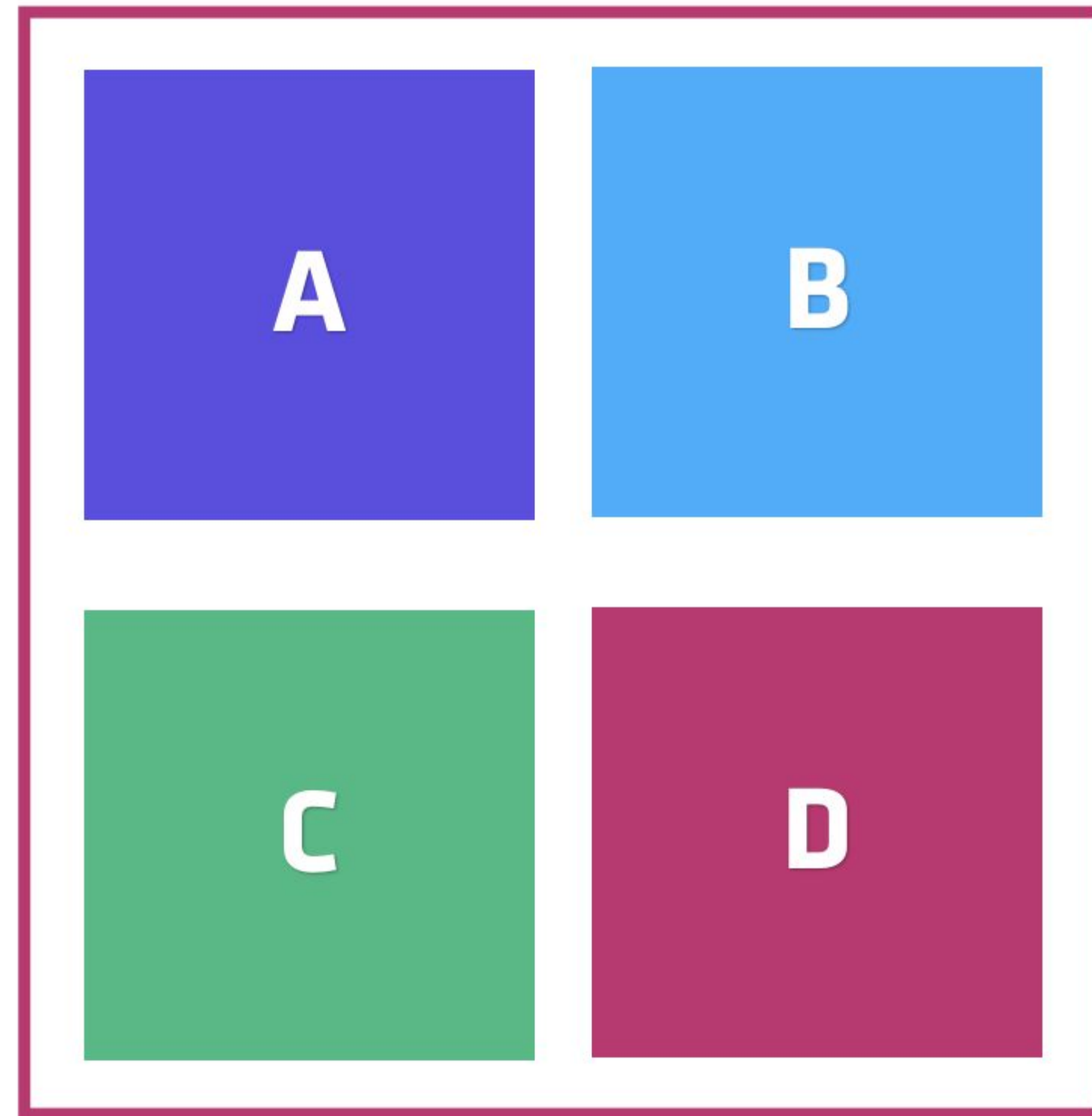
Modern Datacenter



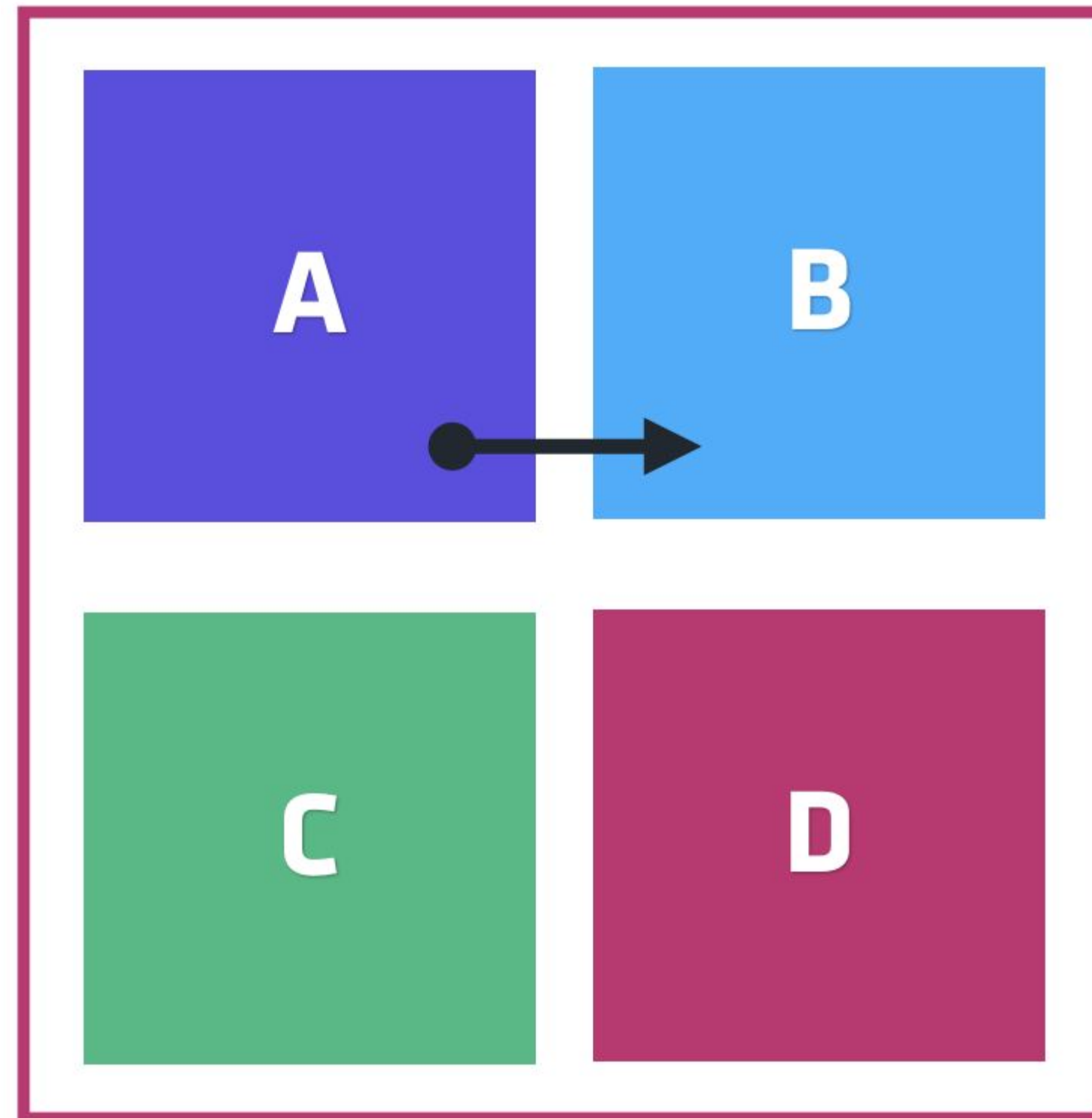


Monoliths & Microservices

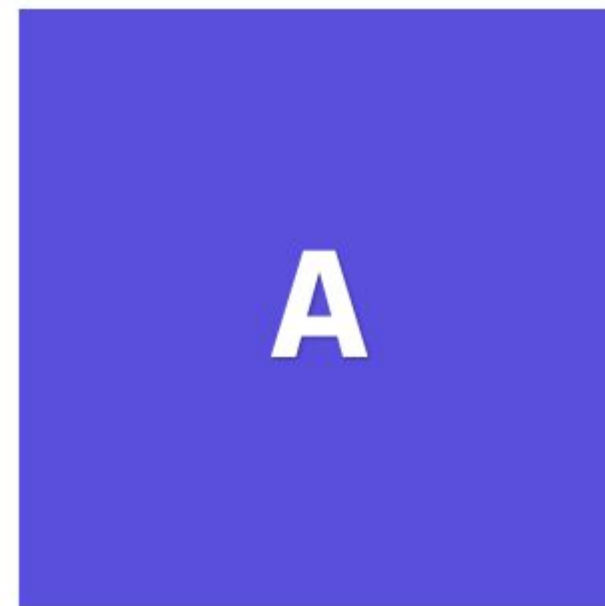
This is a monolith



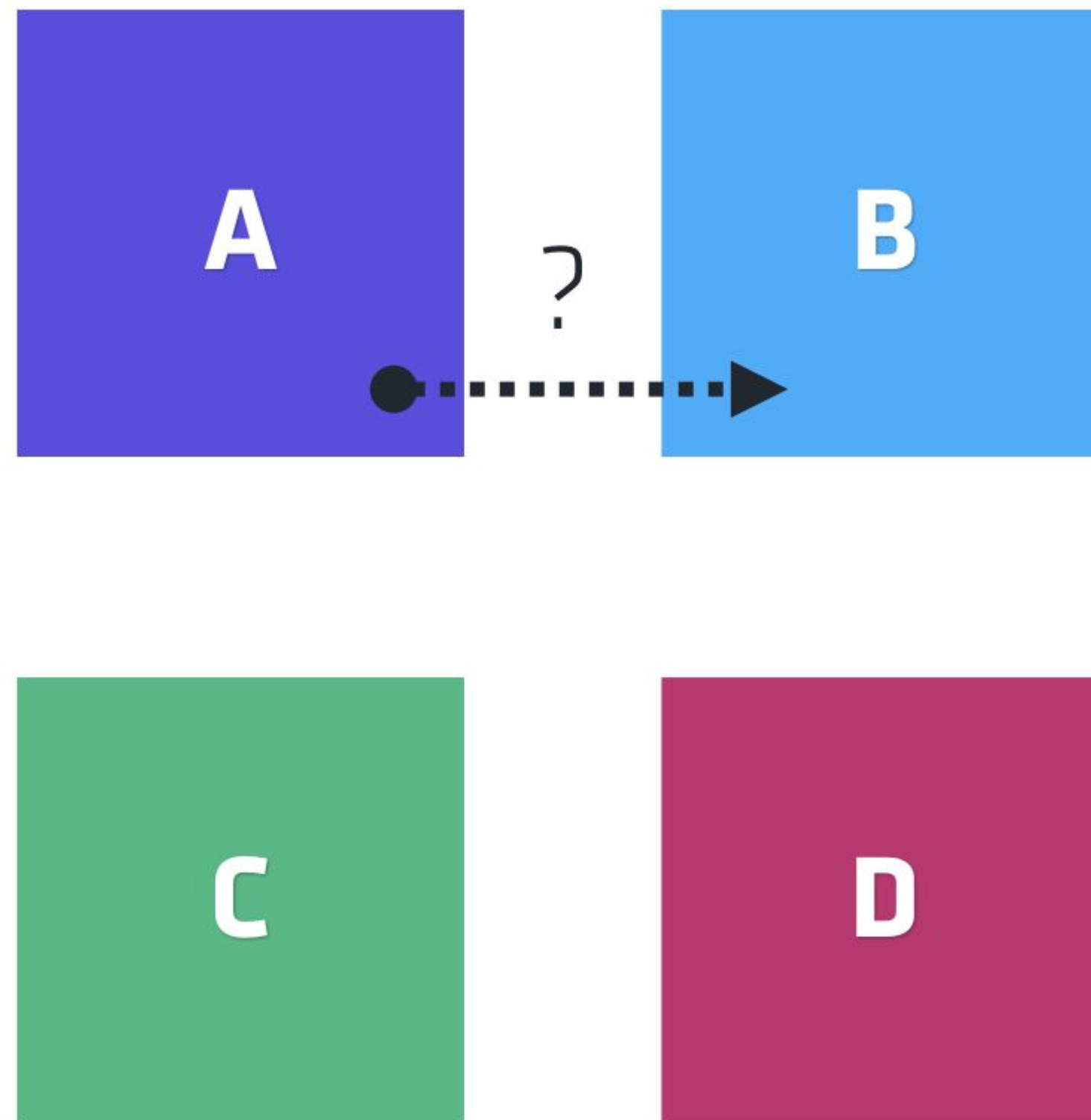
Monoliths



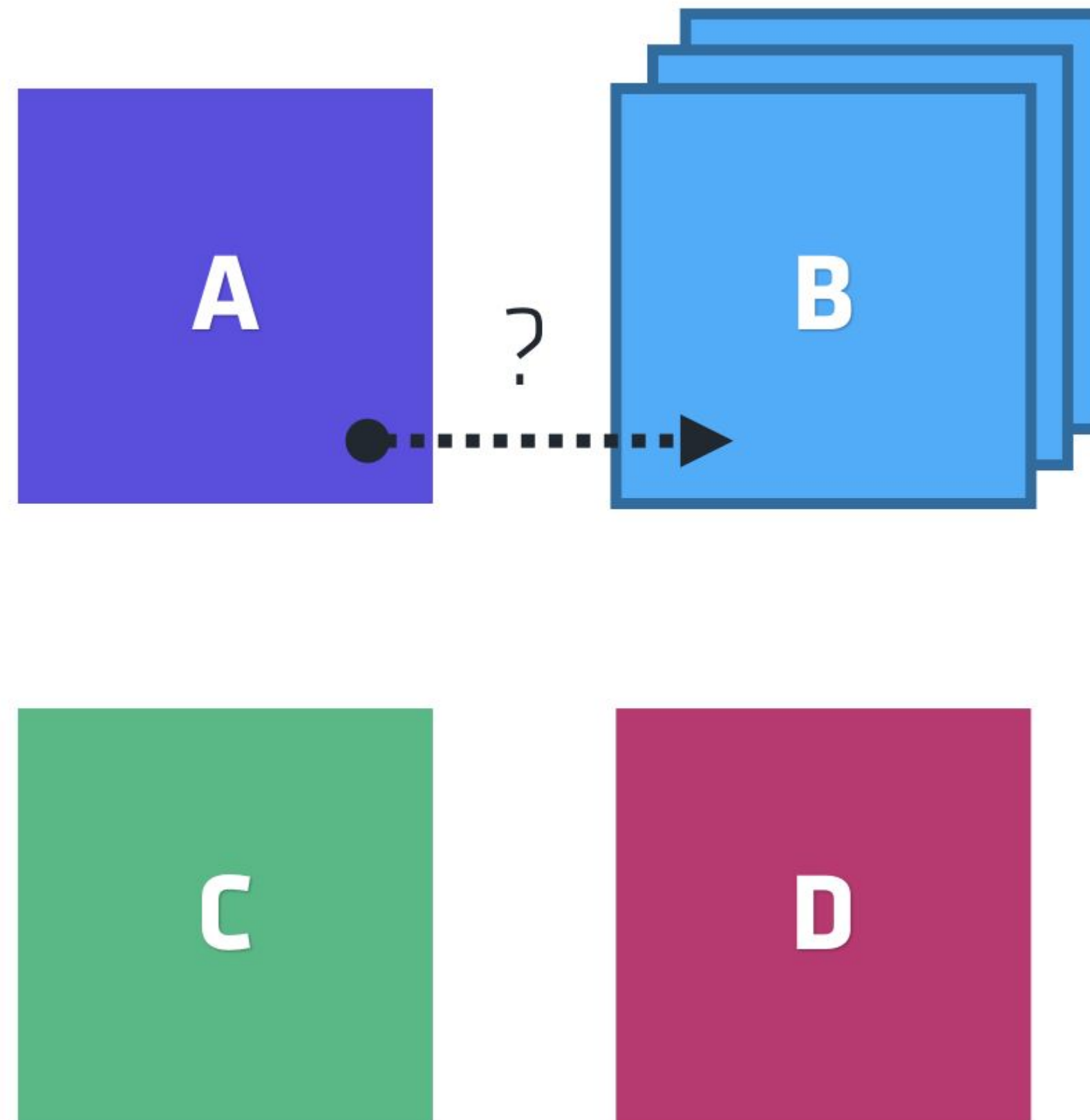
These are microservices



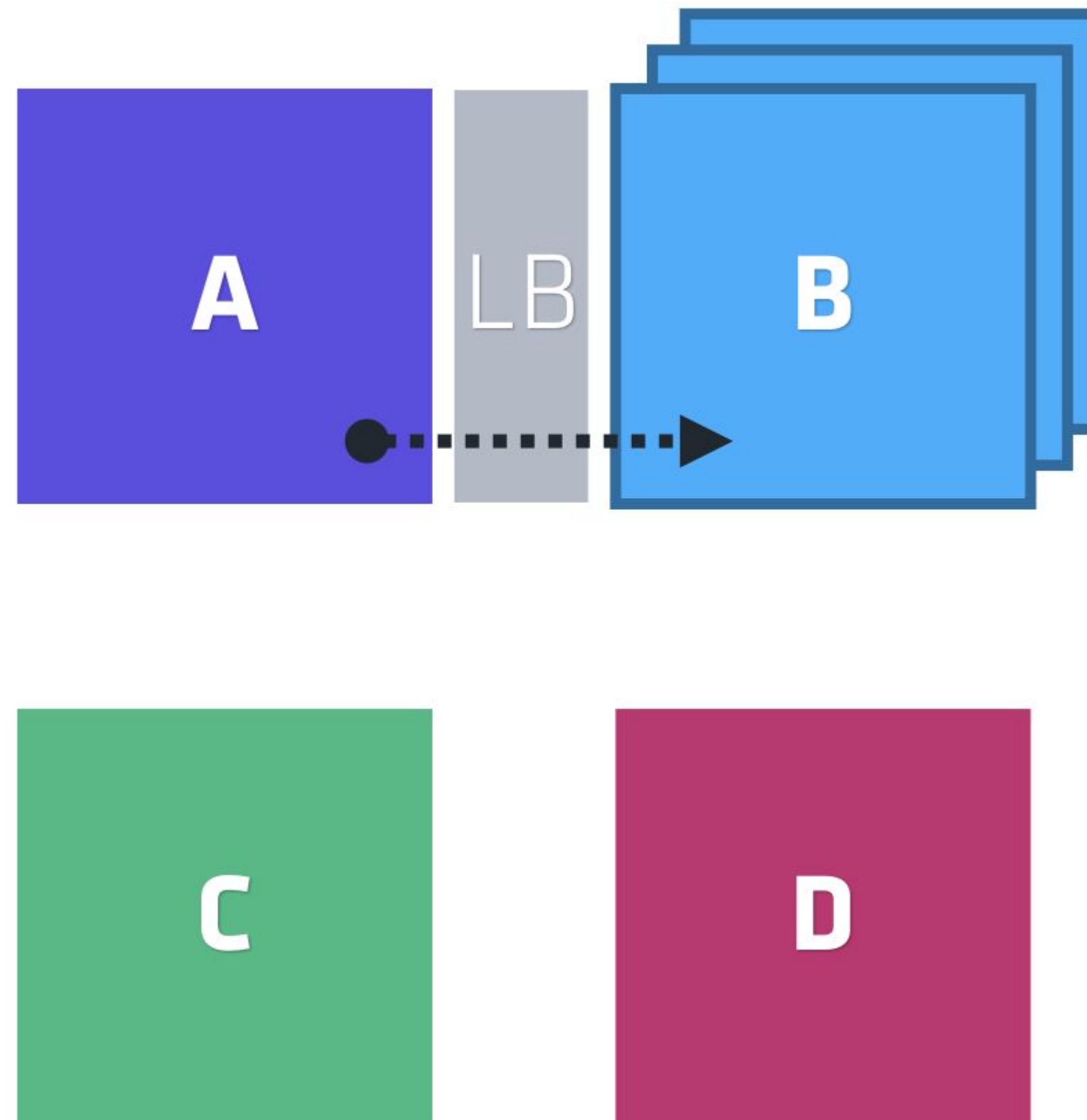
Microservices



Microservices

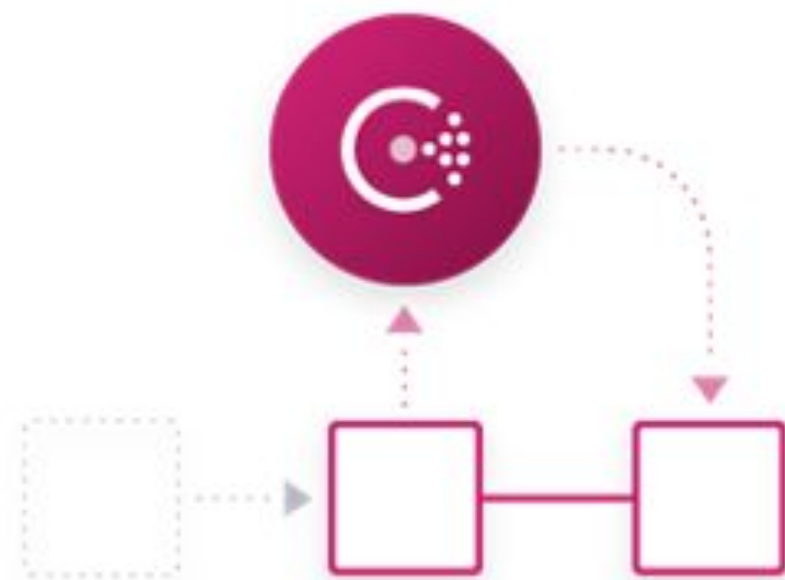


Microservices





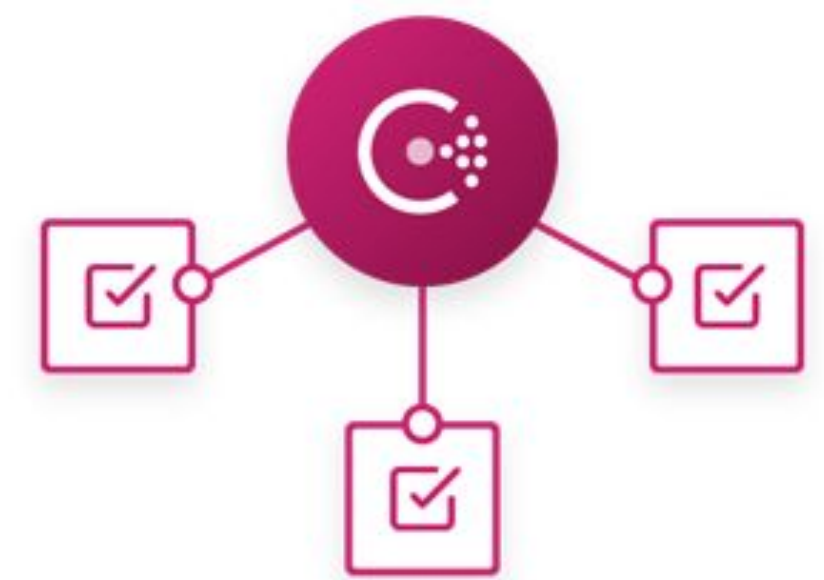
Dynamic Infrastructure Challenges



**Service
Discovery**



**Service
Mesh**

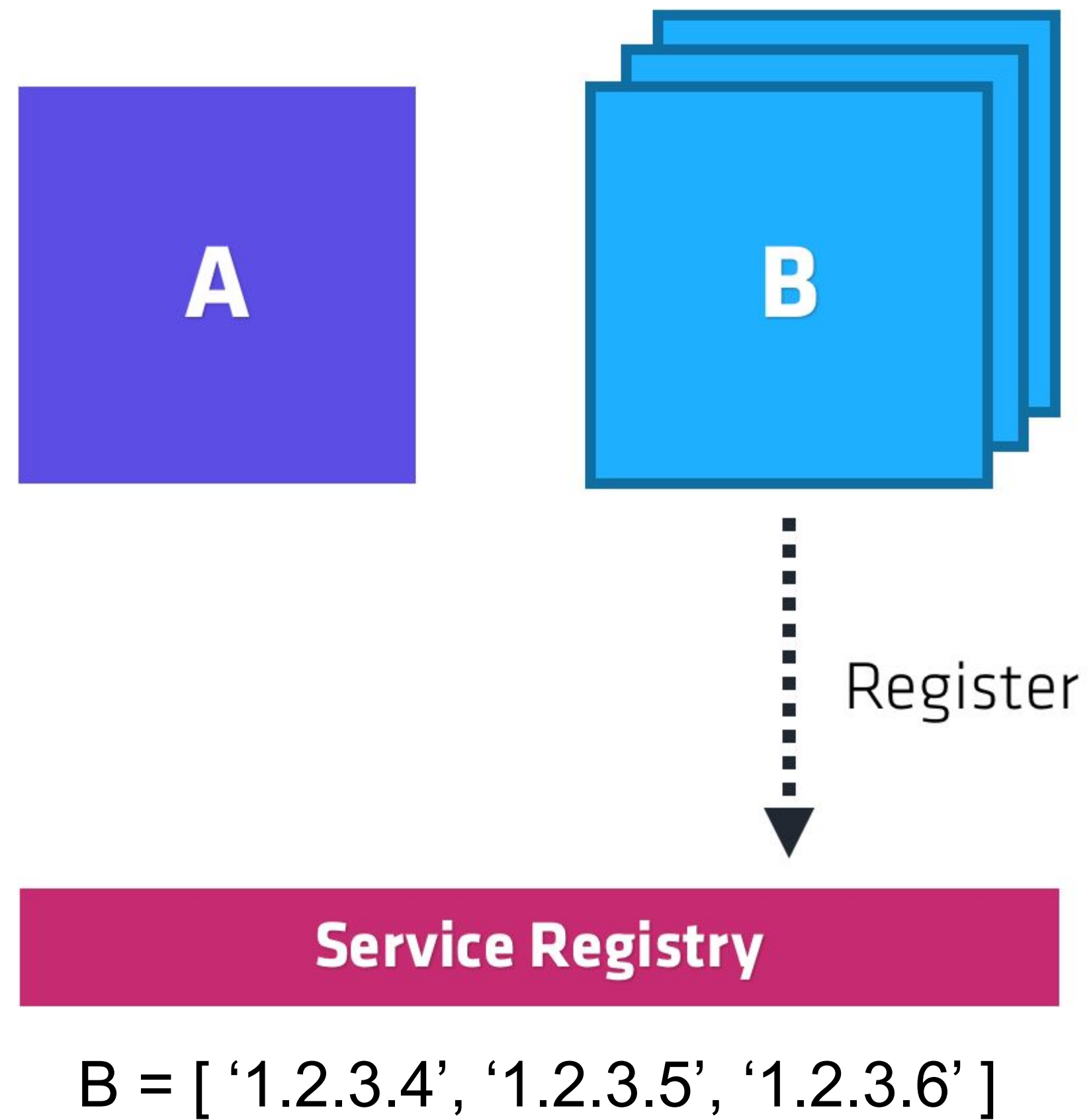


**Service
Configuration**

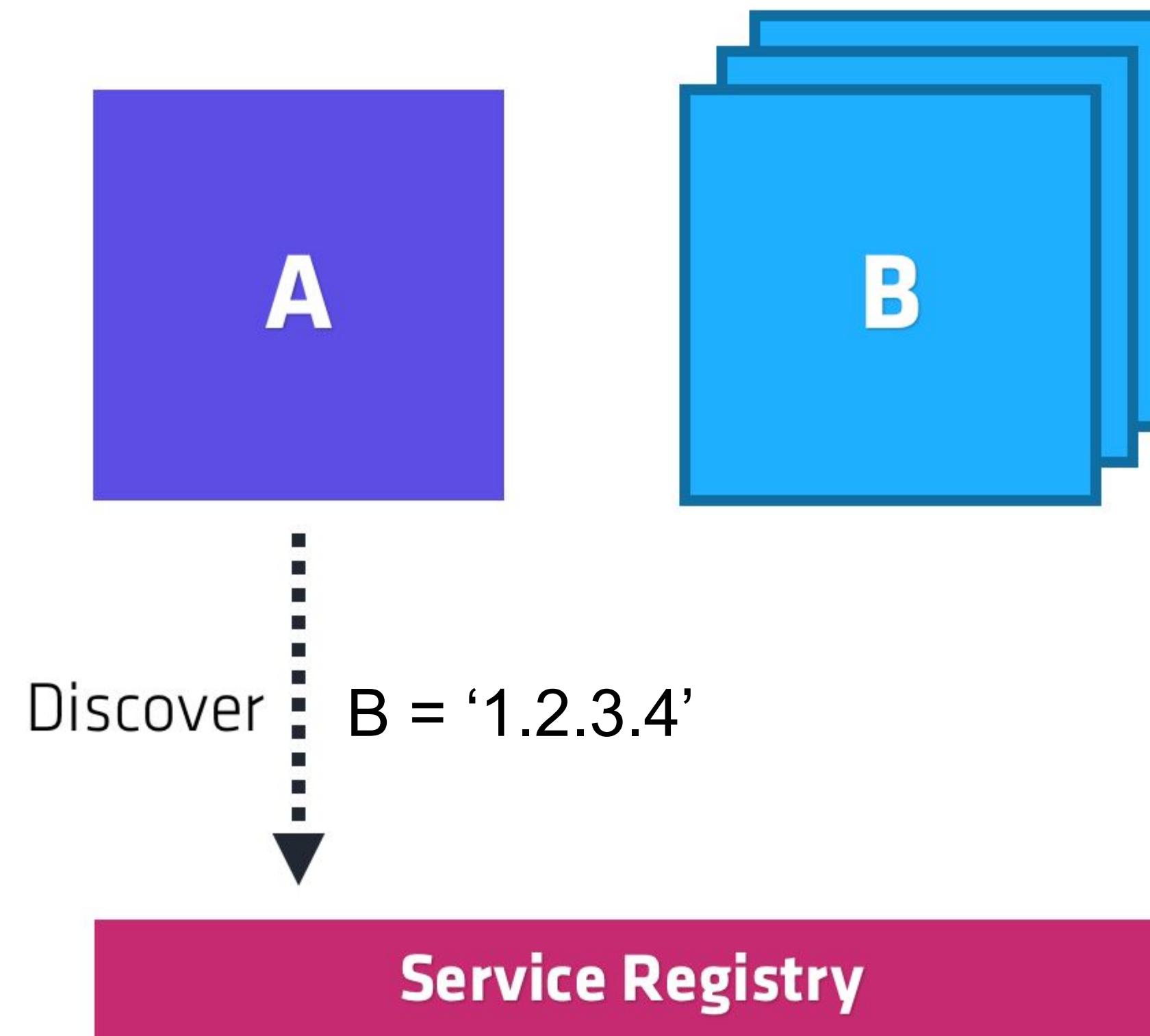


Service Registry & Discovery

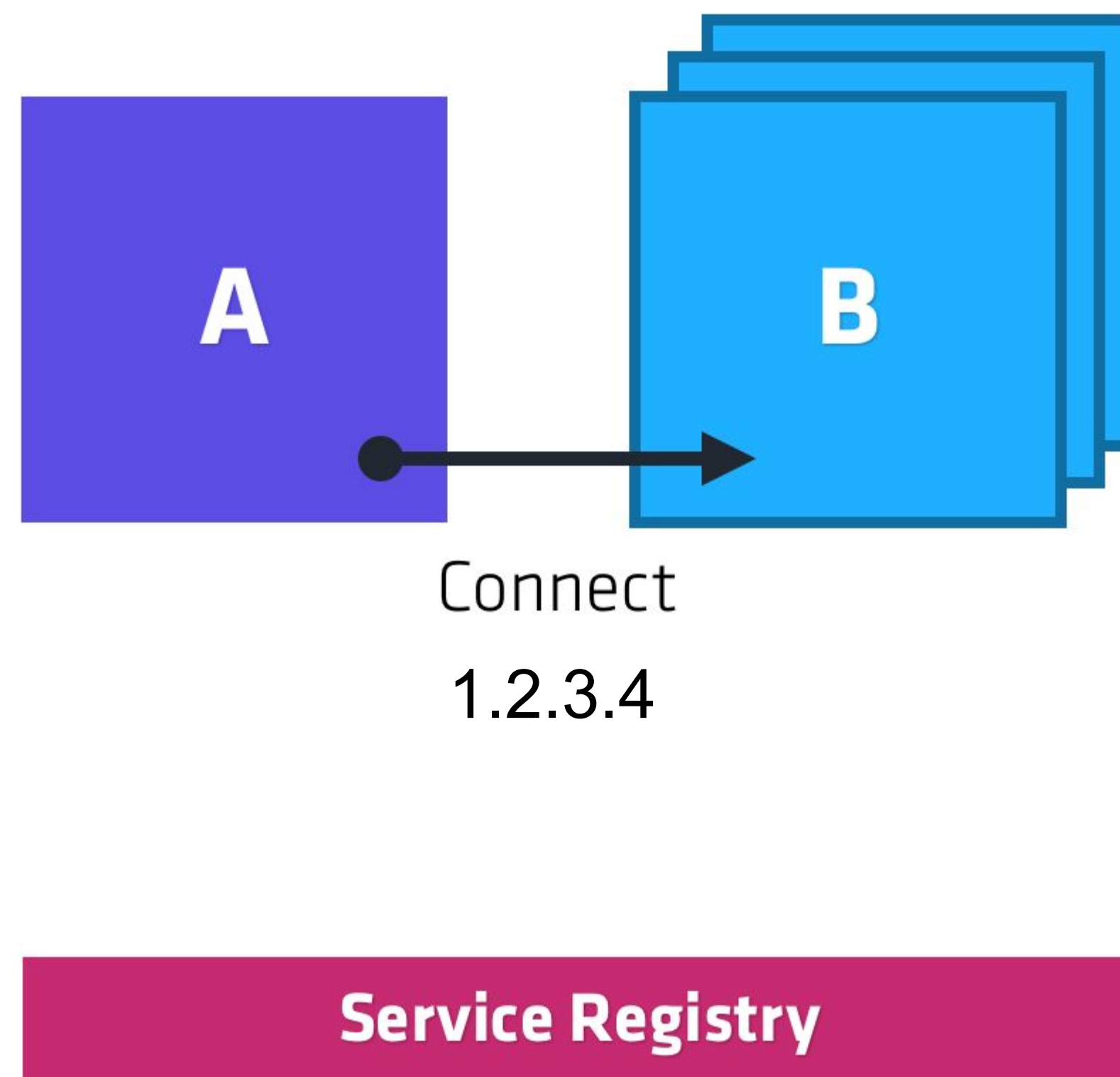
Service Discovery



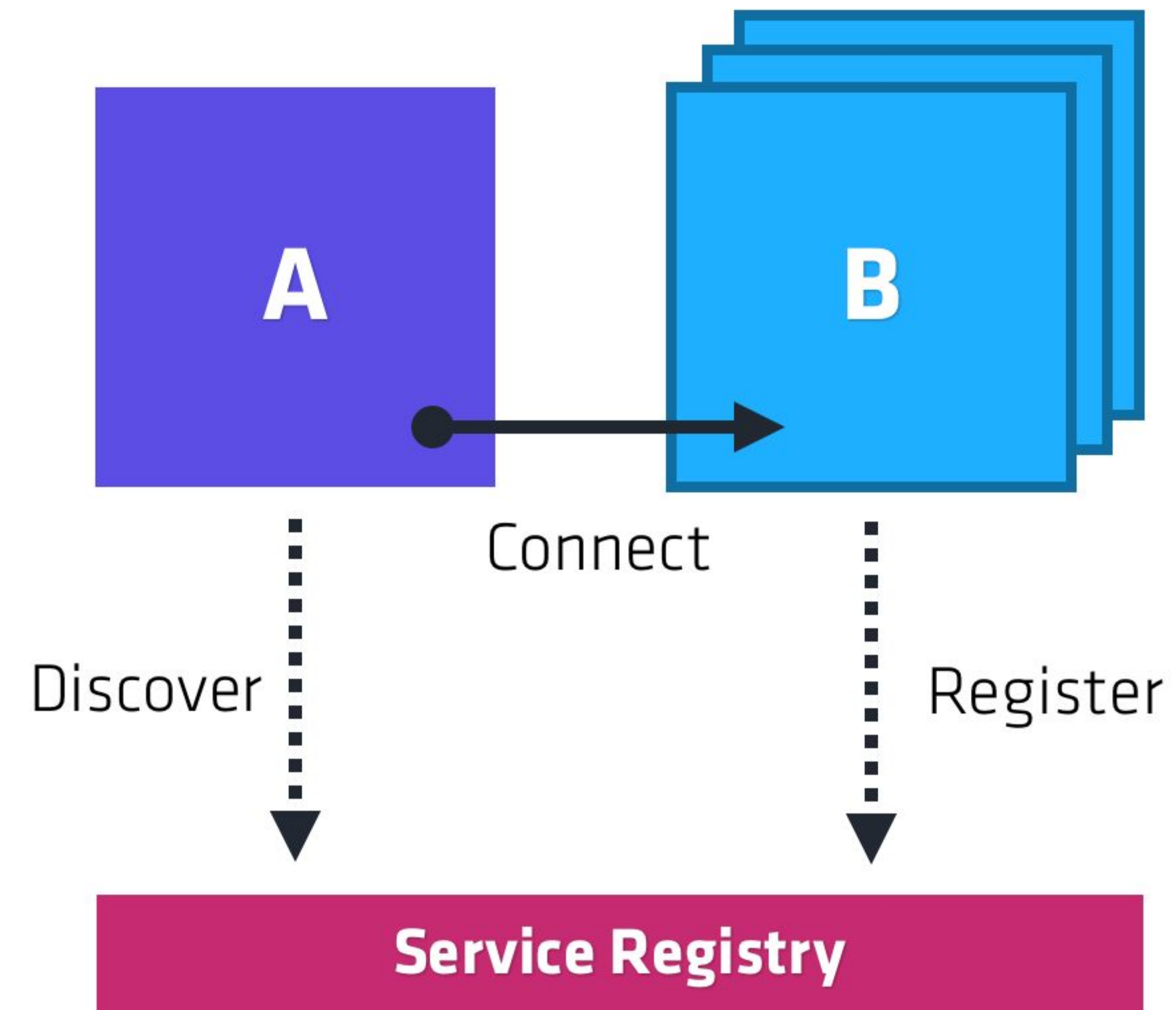
Service Discovery



Service Discovery



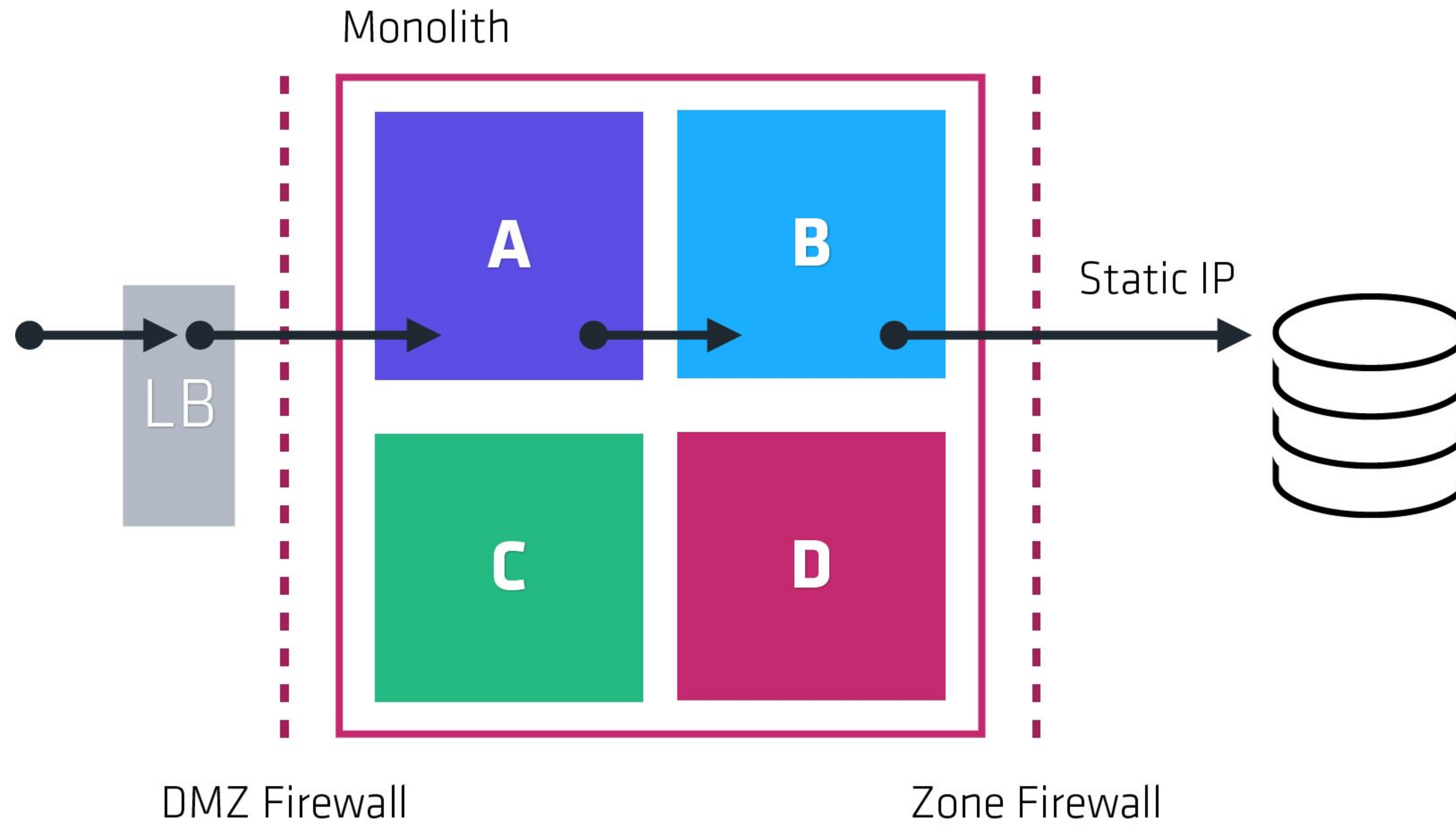
Service Discovery



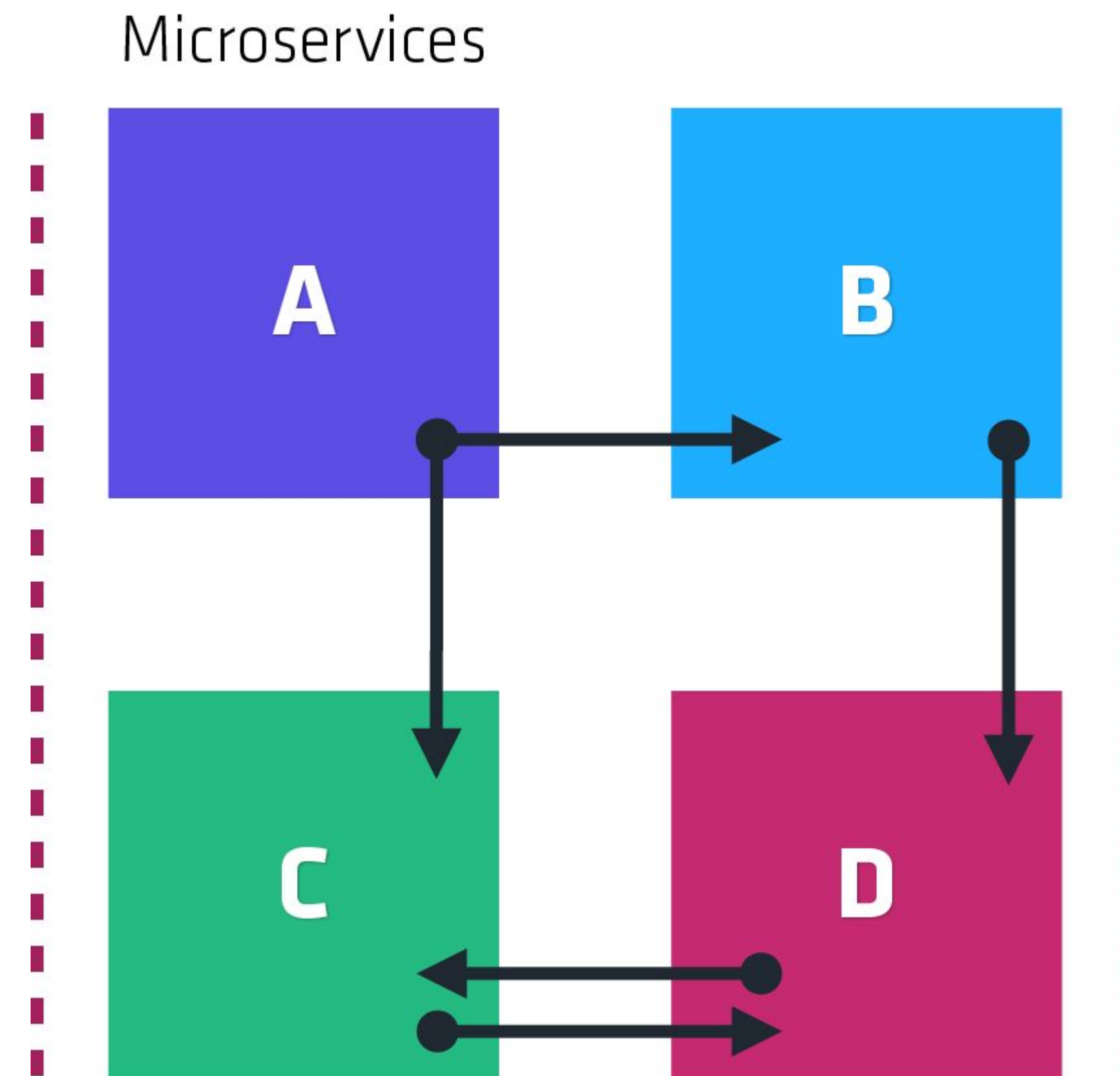


Service Mesh

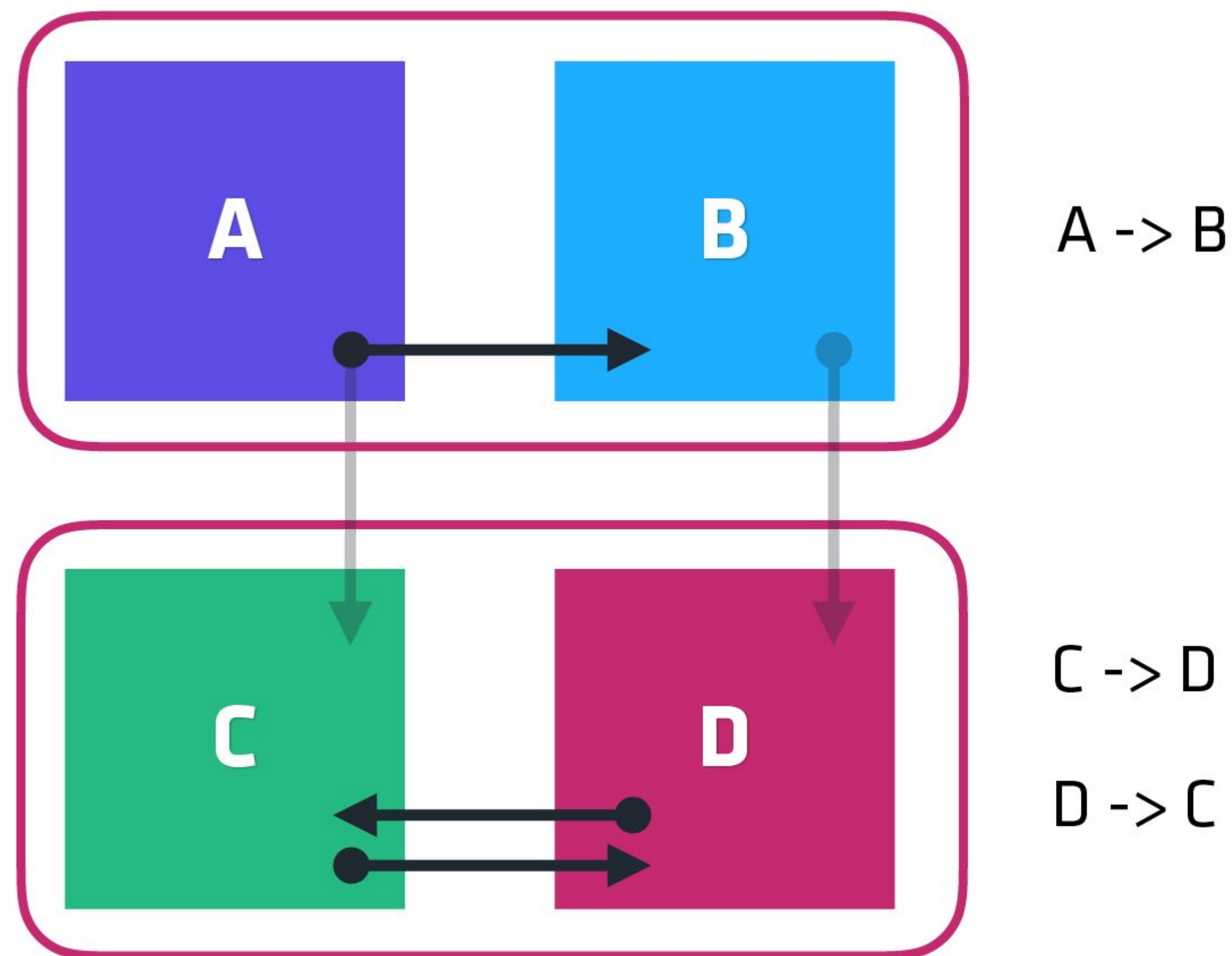
Service Segmentation



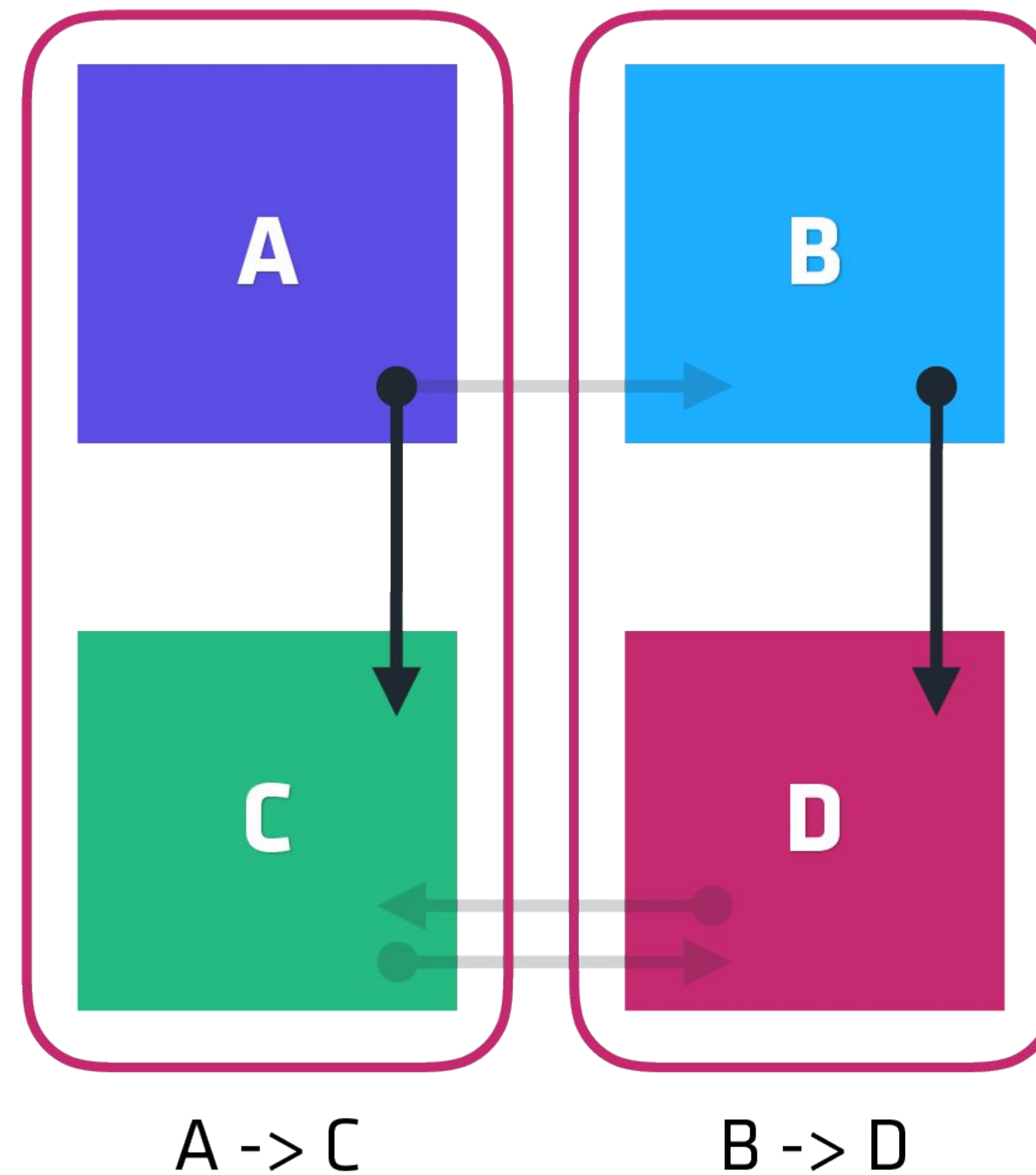
Service Segmentation



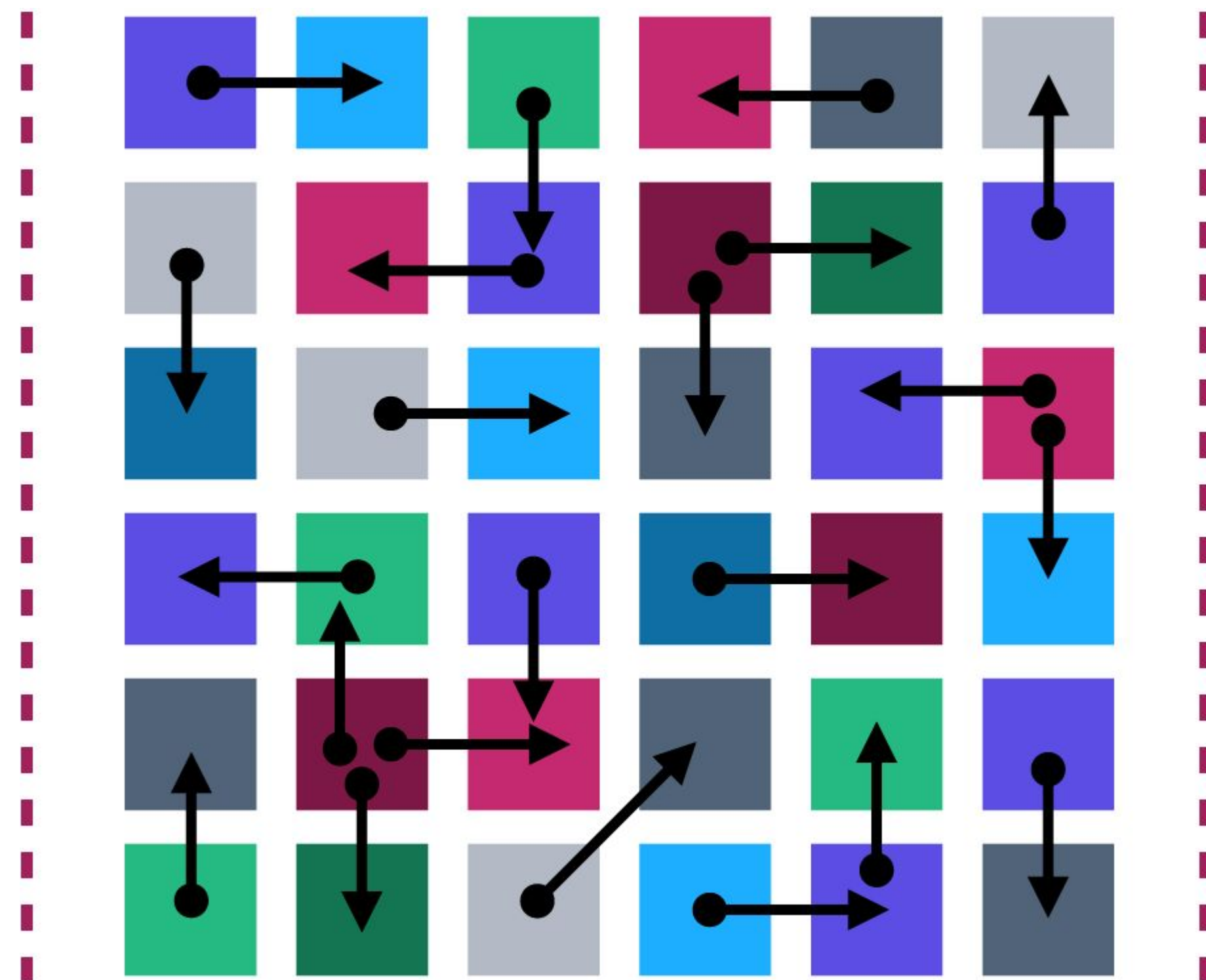
Service Segmentation



Service Segmentation



Service Segmentation



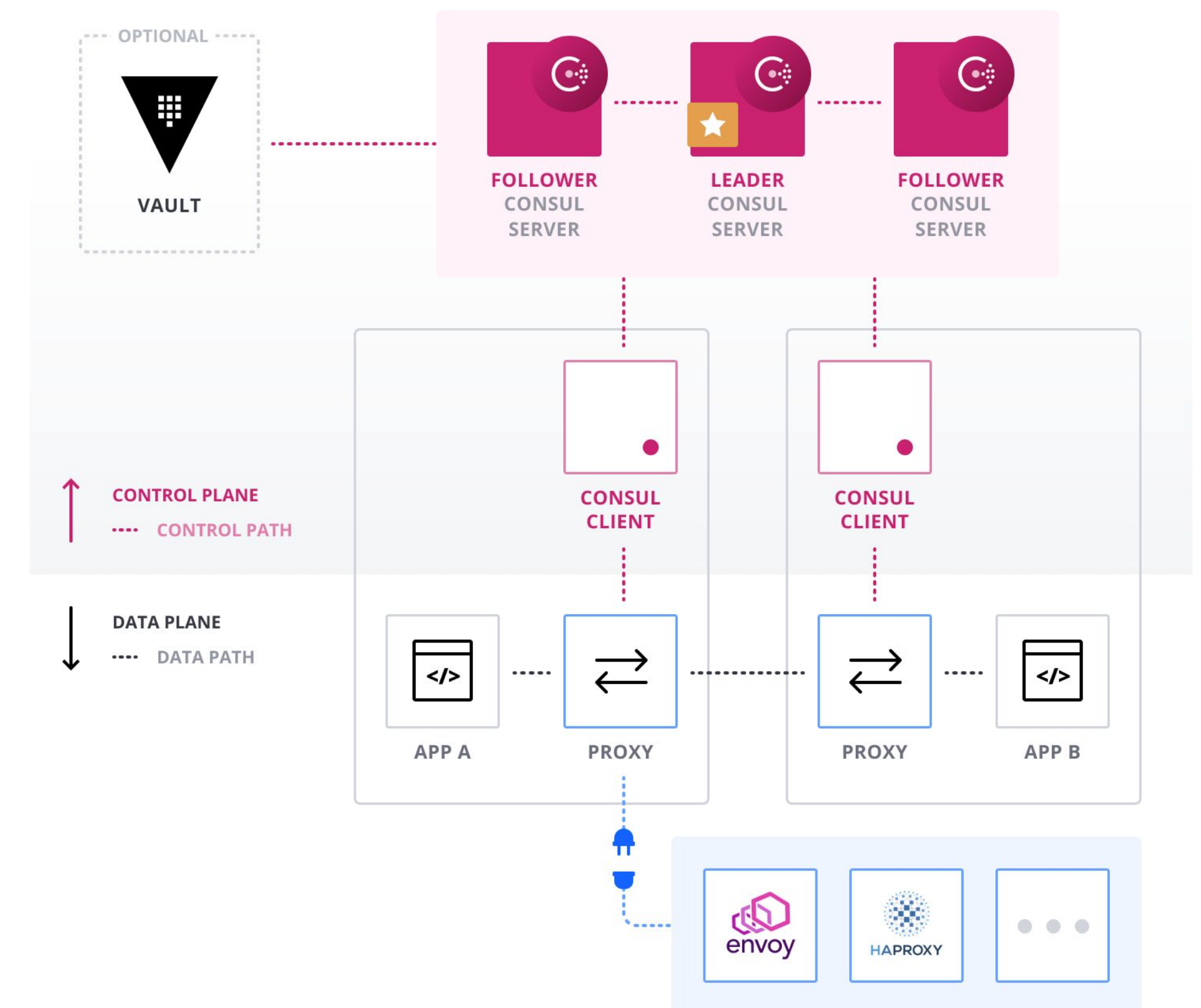


Consul Service Mesh

Control Plane vs. Data Plane



- Consul as Control Plane
- Pluggable Proxies as Data Plane
- Instructions to proxies are cached on the Consul agent
- New instructions are pulled only on changes



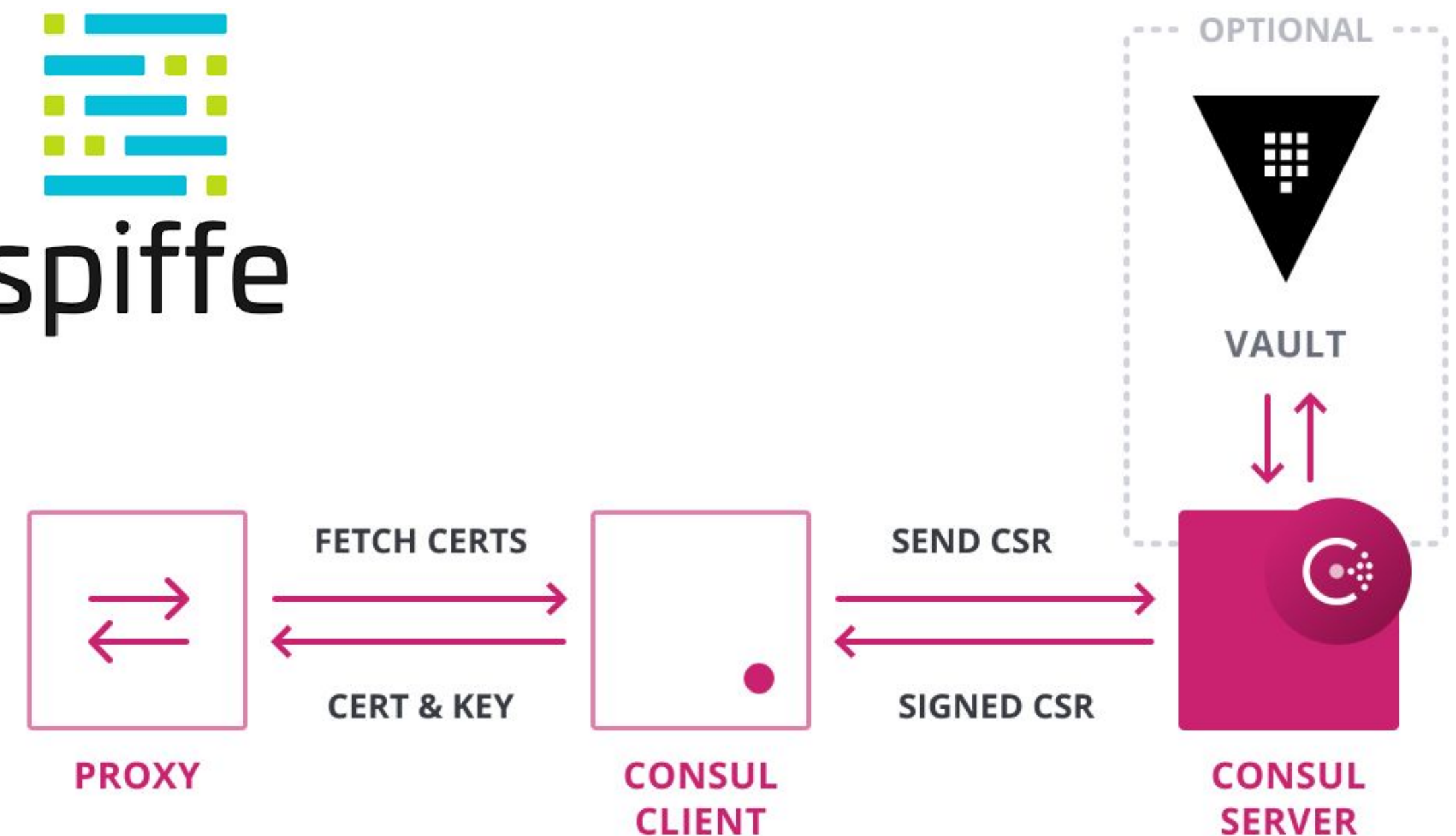


Certificate Authority

Certificate Generation



- X.509 Certificate
- SPIFFE Compatible
- Automatic Generation & Rotation
- Provides Identity and Encryption






Service Access Graph

Service Graph

Codify Intentions

Same intentions are applied
no matter where the service
exists

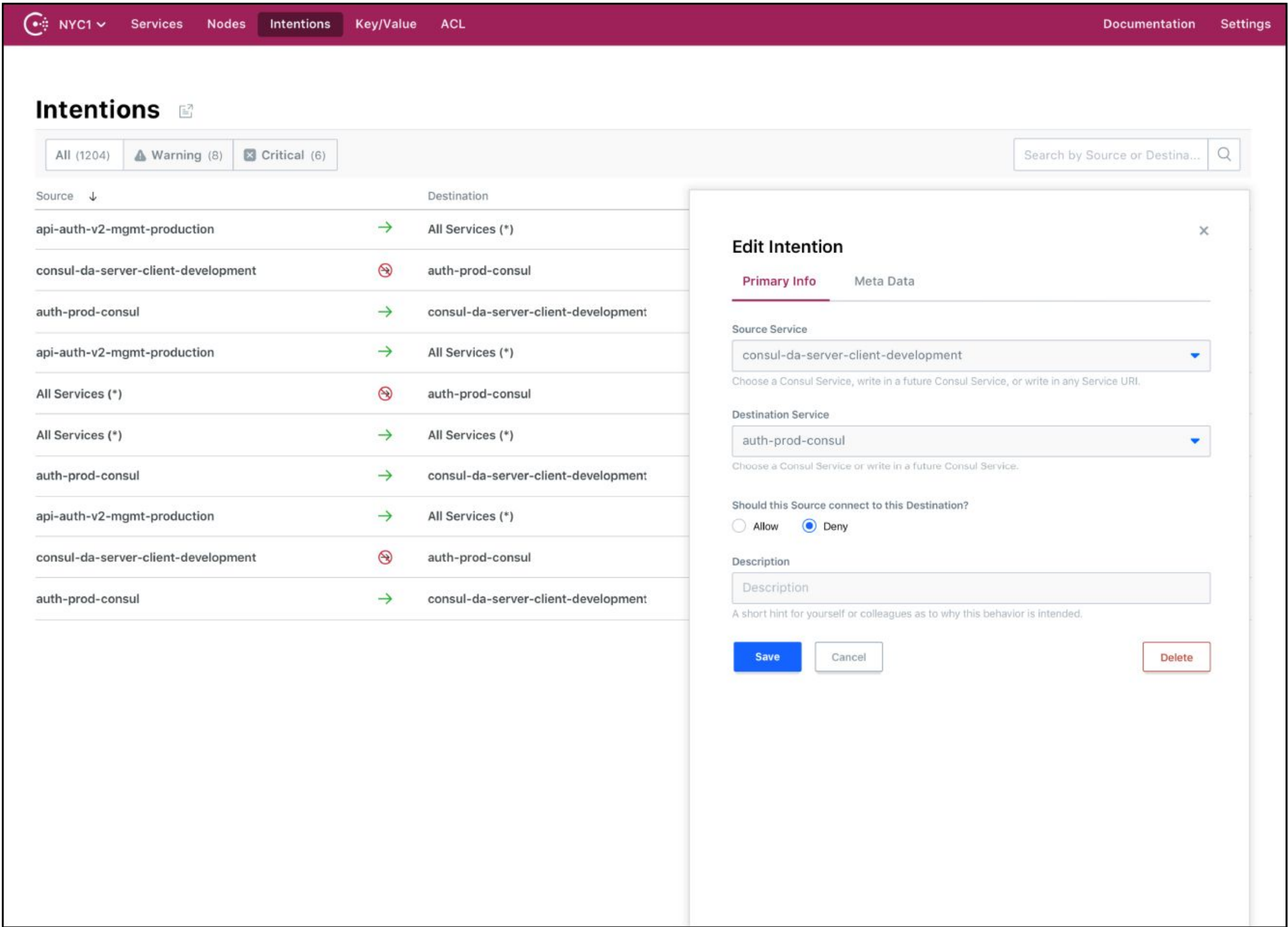
A terminal window with a dark background and light gray text. The title bar at the top right says "TERMINAL". There are three small gray circles in the top left corner of the terminal area. The terminal shows two commands and their outputs.

```
$ consul intention create -deny web '*'
Created: web => * (deny)

$ consul intention create -allow web db
Created: web => db (allow)
```


Web UI

Manage intentions via web interface





Application Integration

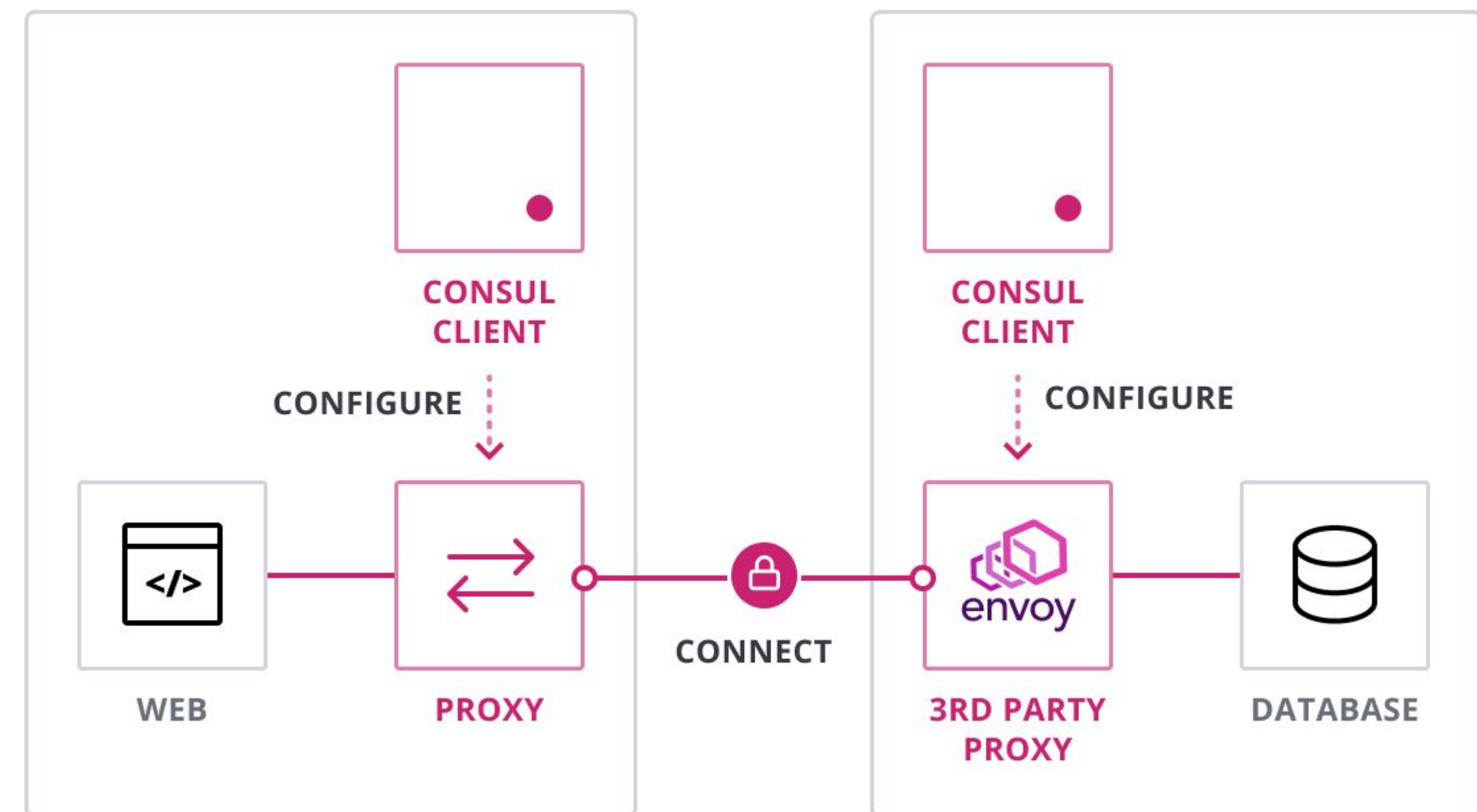
Sidecar Proxies



Sidecar proxy to secure traffic for any application

Consul provides sidecar proxies running alongside applications to transparently wrap traffic in TLS and enforces the intentions.

- No code modification required
- Minimal performance overhead
- Pluggable data plane: Built-in Layer 4 proxy, native Envoy integration or other third-party proxy integration
- Operational flexibility, decoupling security concern from the application itself



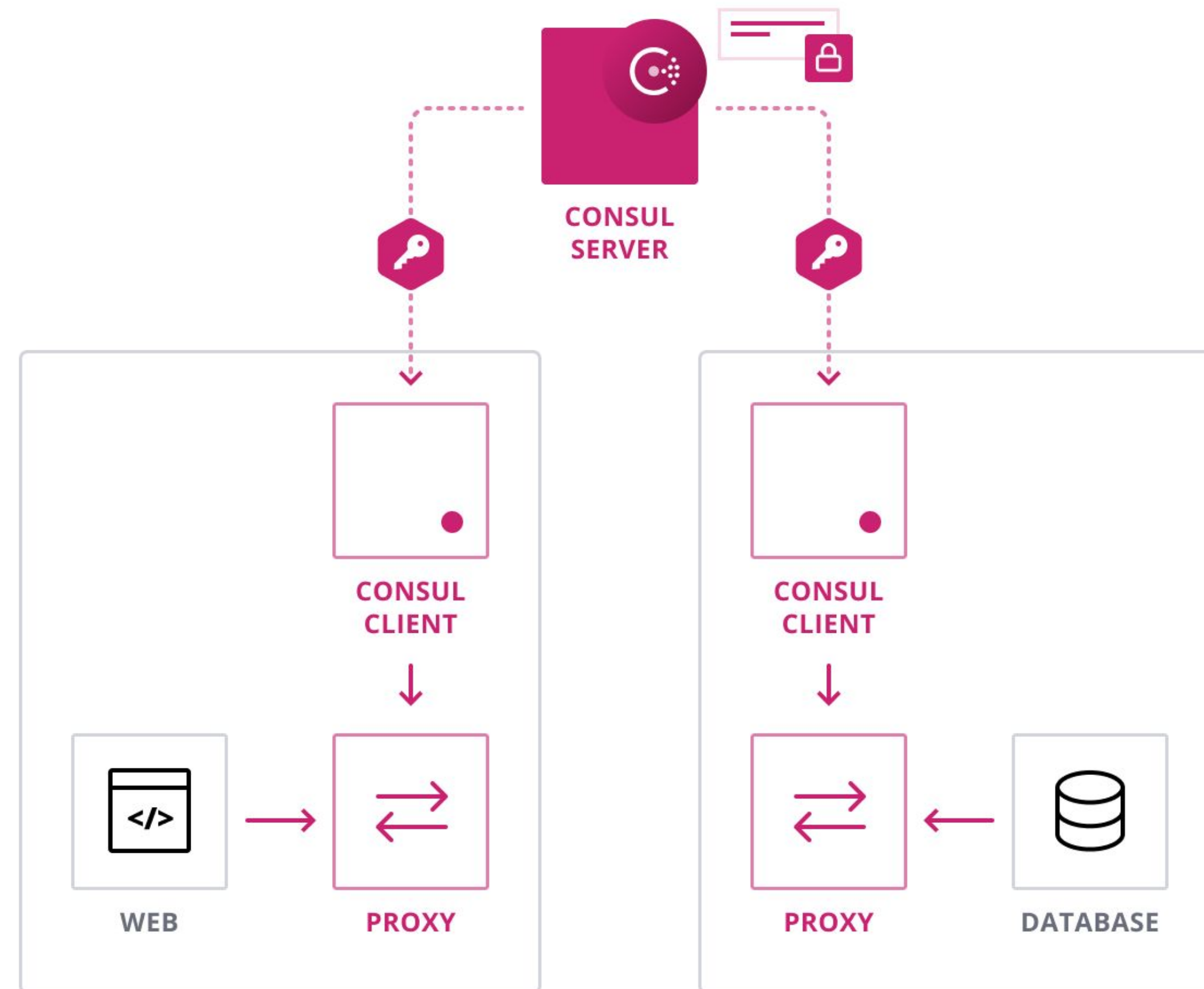
Proxy Registration

Kubernetes

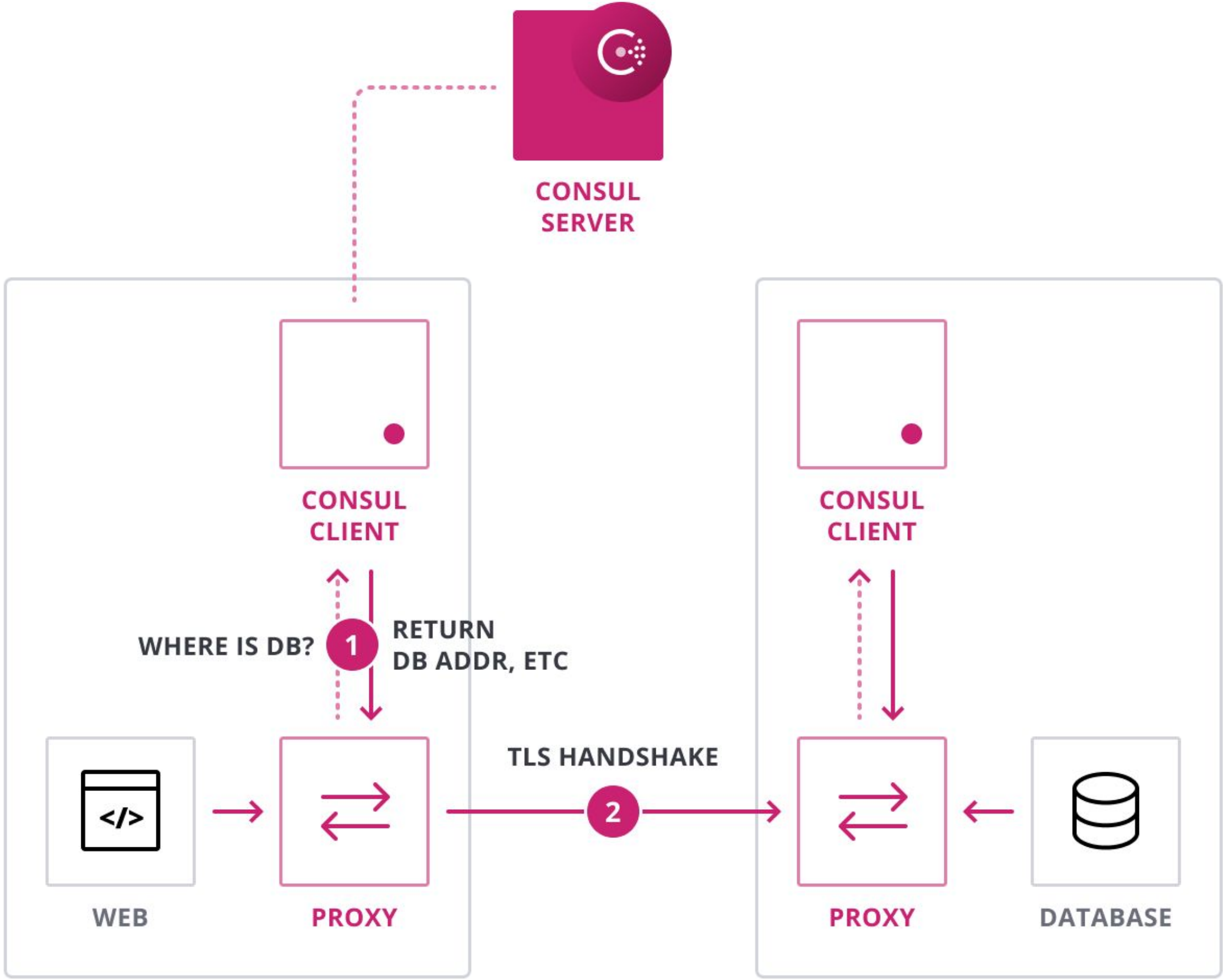
TERMINAL

```
apiVersion: v1
kind: Pod
metadata:
  name: cats
  annotations:
    "consul.hashicorp.com/connect-inject": "true"
spec:
  containers:
  - name: cats
    image: grove-mountain/cats:1.0.1
    ports:
    - containerPort: 8000
      name: http
```

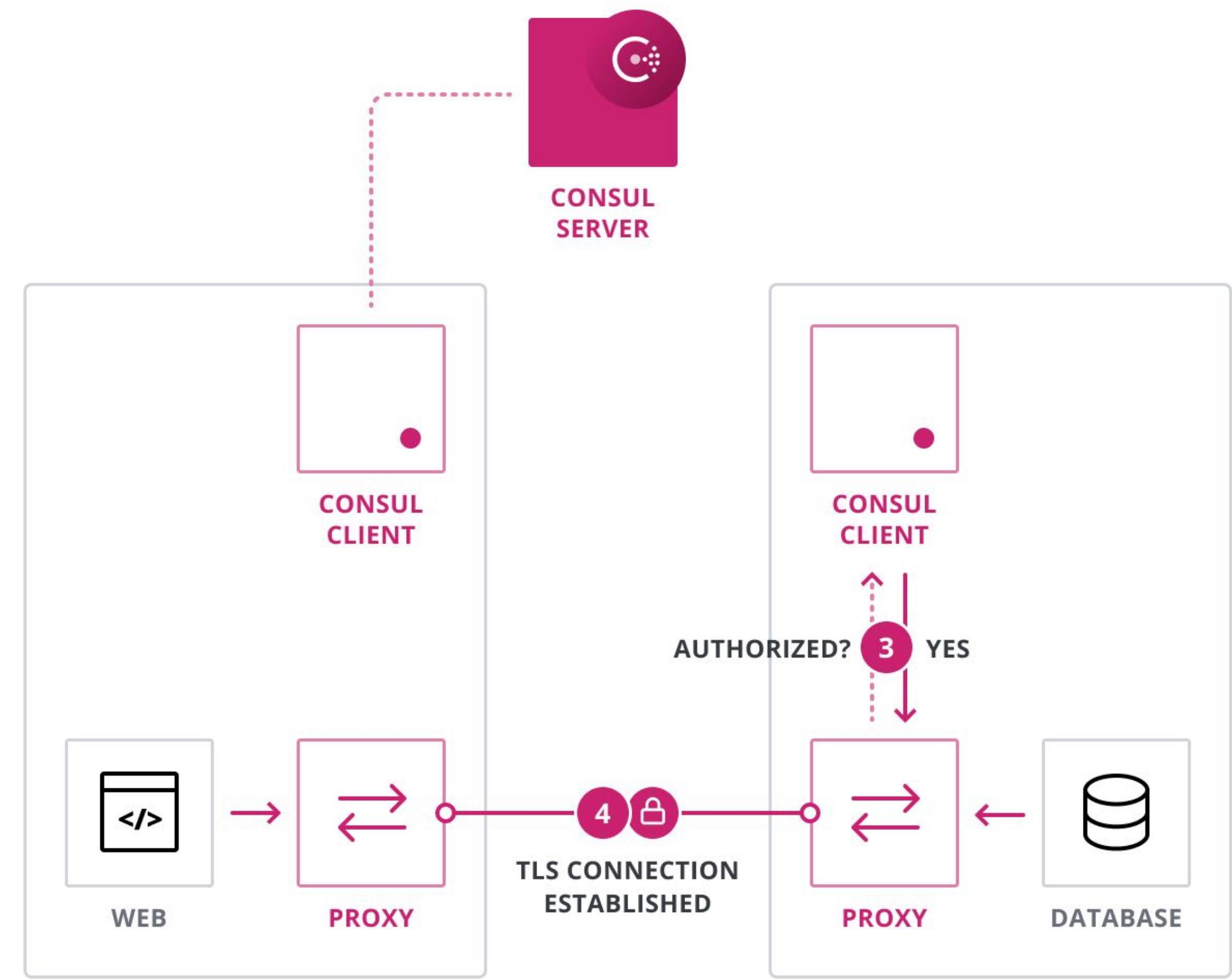
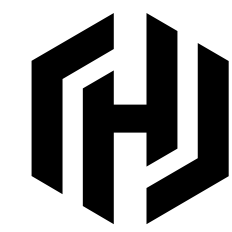

Sidecar Proxies



Sidecar Proxies



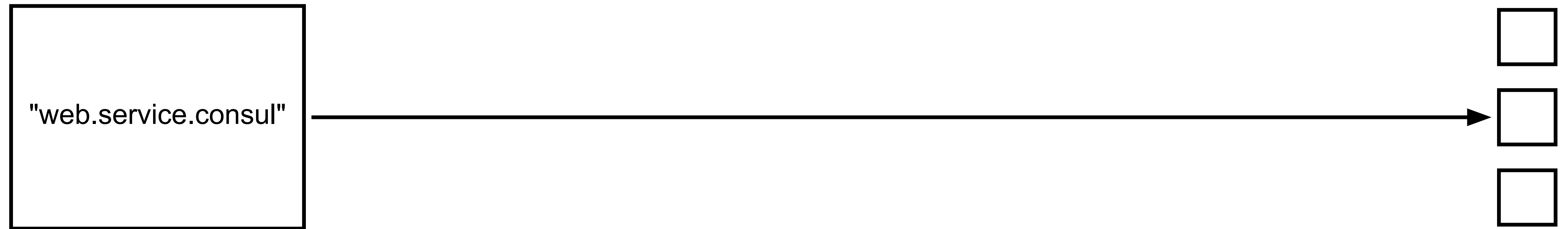
Sidecar Proxies



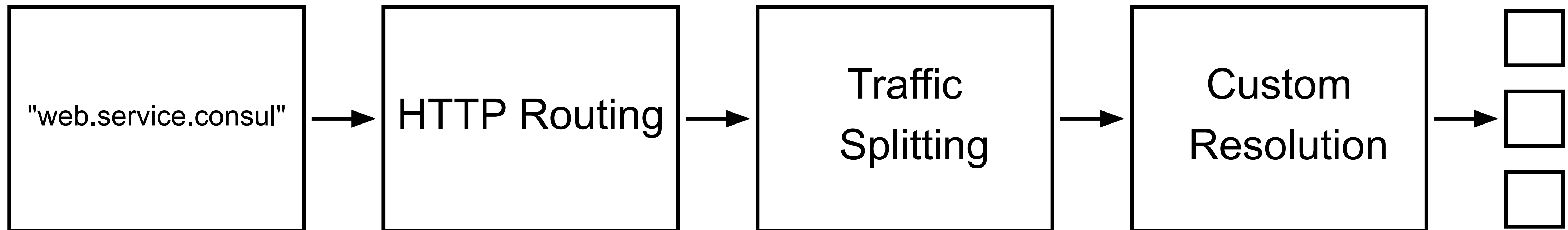


L7 Traffic Management

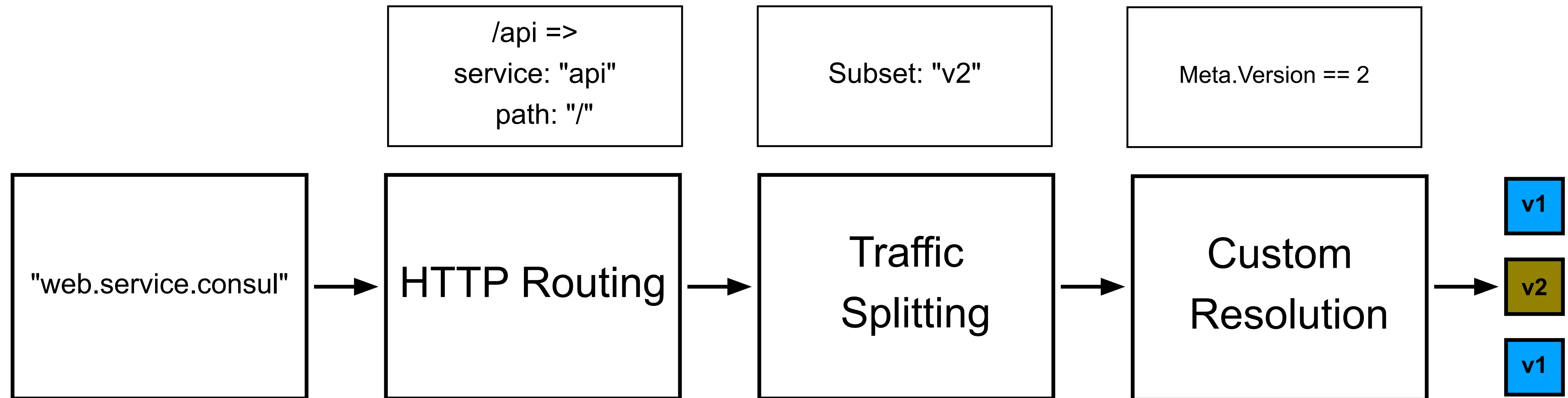
L4 Traffic



L7 Traffic Management



L7 Traffic Management



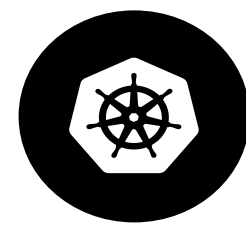


Mesh Gateways

Mesh Gateways

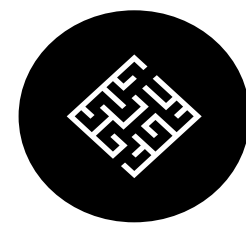


Multi-Cloud and -Cluster challenge



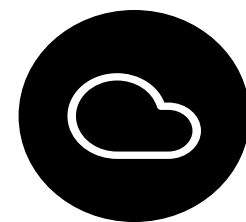
Single Kubernetes cluster

Most Service Meshes are build for a single cluster



Multi-cluster Service Mesh

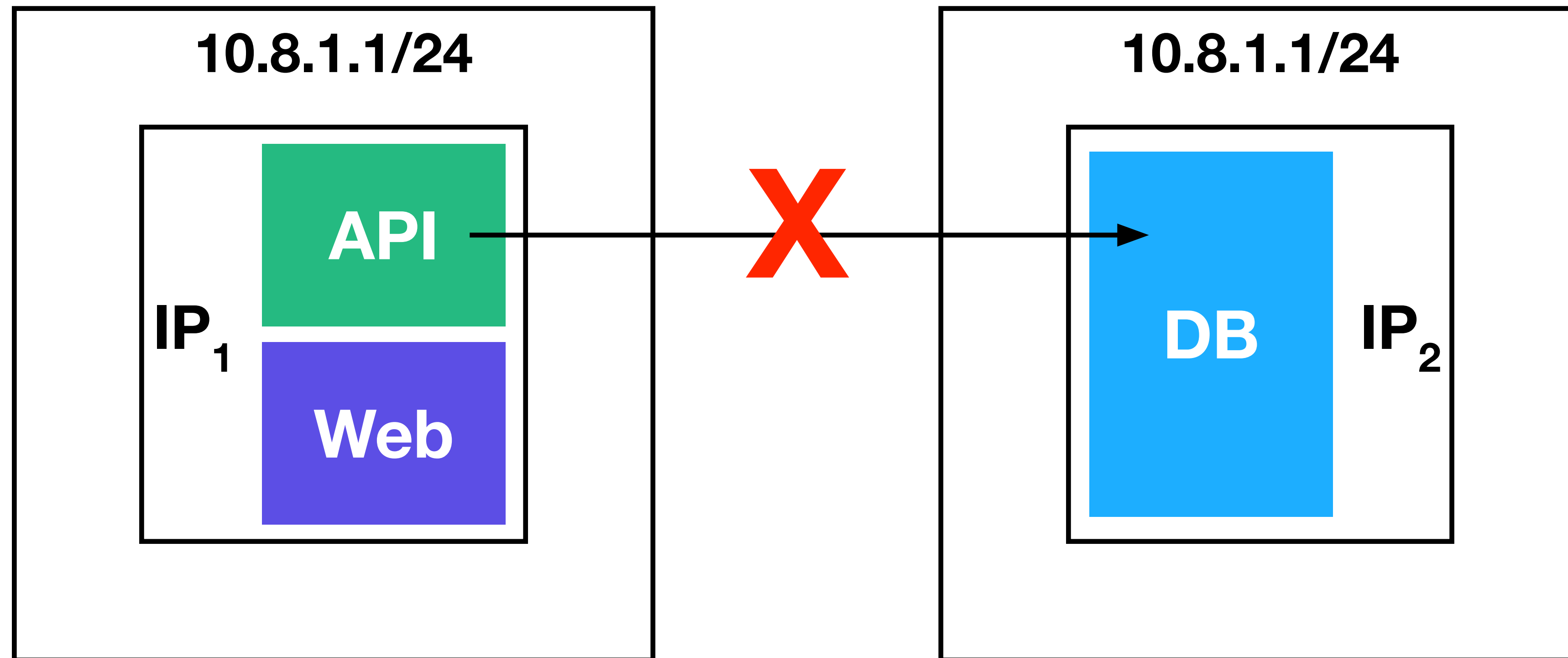
Connection multiple Service Meshes across different Kubernetes clusters not solved yet



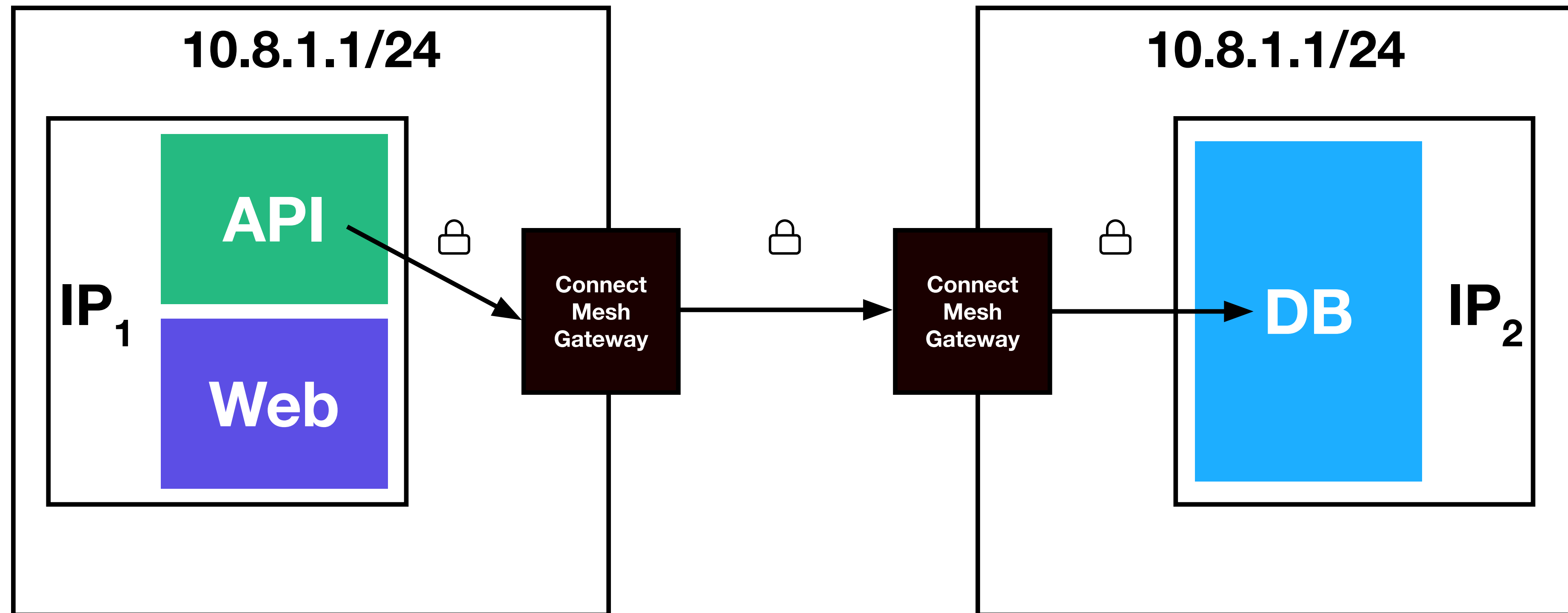
Service Mesh across clouds

Connection Services Meshes across different environments (Clouds, On-Prem, etc.) requires a lot of work

Mesh Gateways



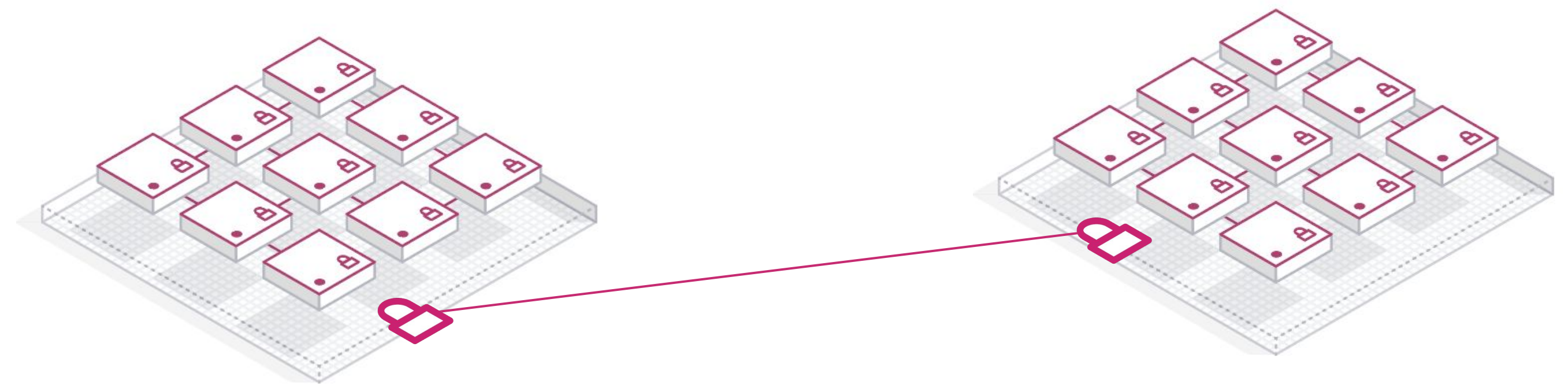
Mesh Gateways



Mesh Gateways



- Mesh gateways, built upon Envoy, will sit on the public internet and accept L4 traffic with mTLS
- Mesh gateways will perform NAT and route the traffic to correct endpoint on the private network
- All the services need NOT be exposed on public network for cross cloud service communication



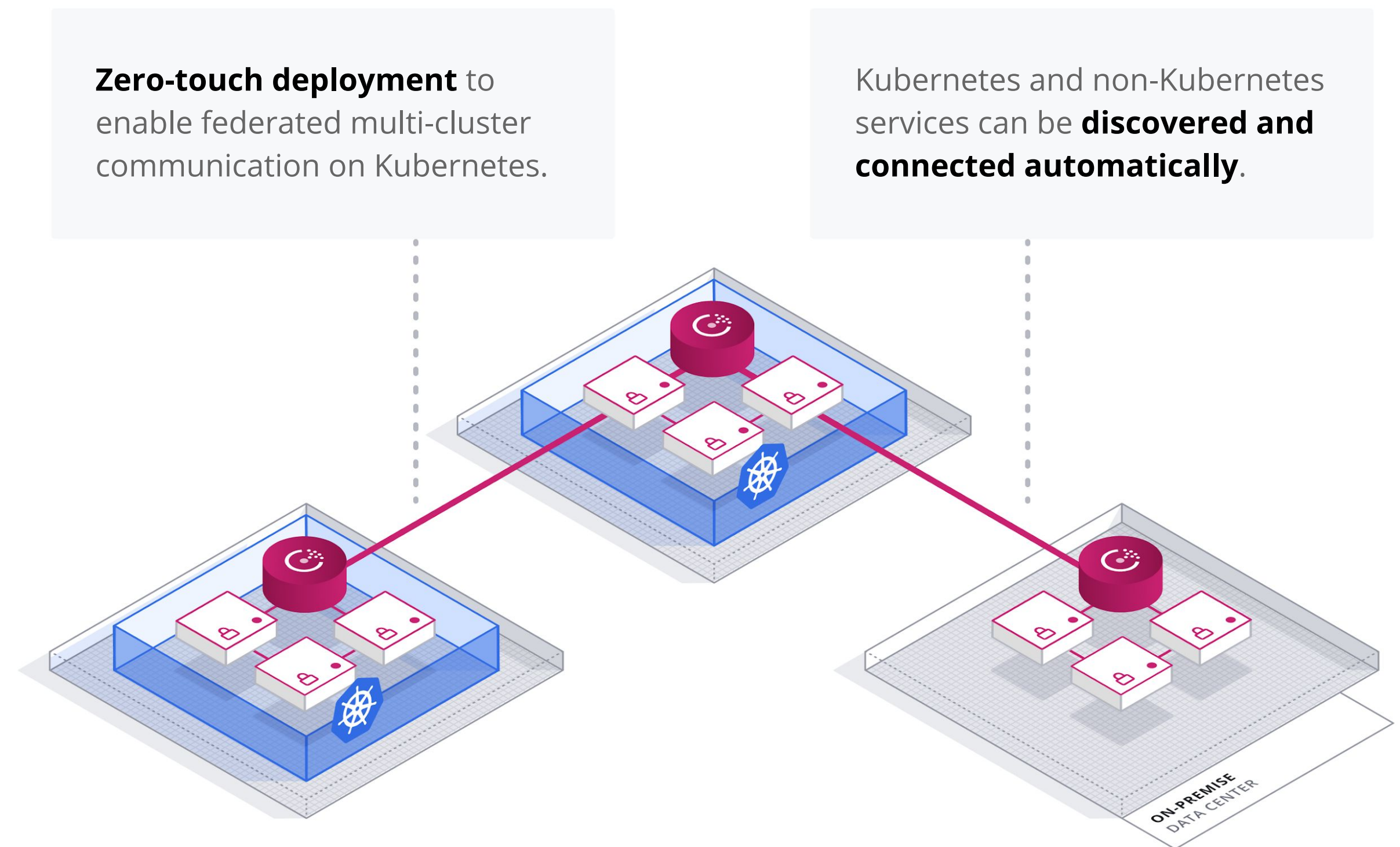


Kubernetes Integration

Native Service Mesh Integration with Kubernetes



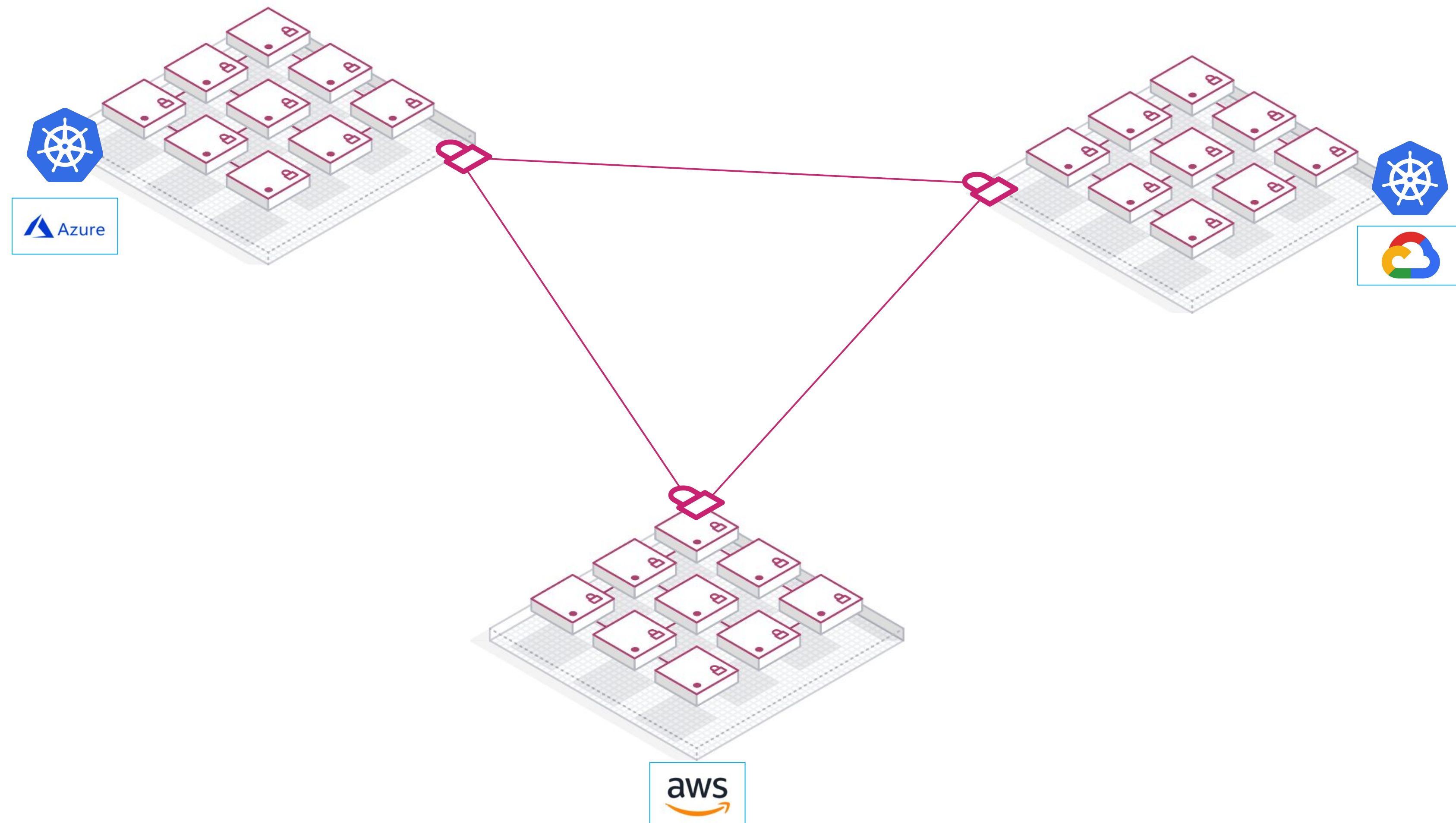
- **Consul Helm Chart:** Automatically install, configure and upgrade Consul servers and clients on Kubernetes
- **Consul Connect Auto-Inject:** Services on Kubernetes can be configured to automatically use Connect to securely communicate via mutual TLS
- **Mesh Gateway:** Easily connect multiple Kubernetes clusters



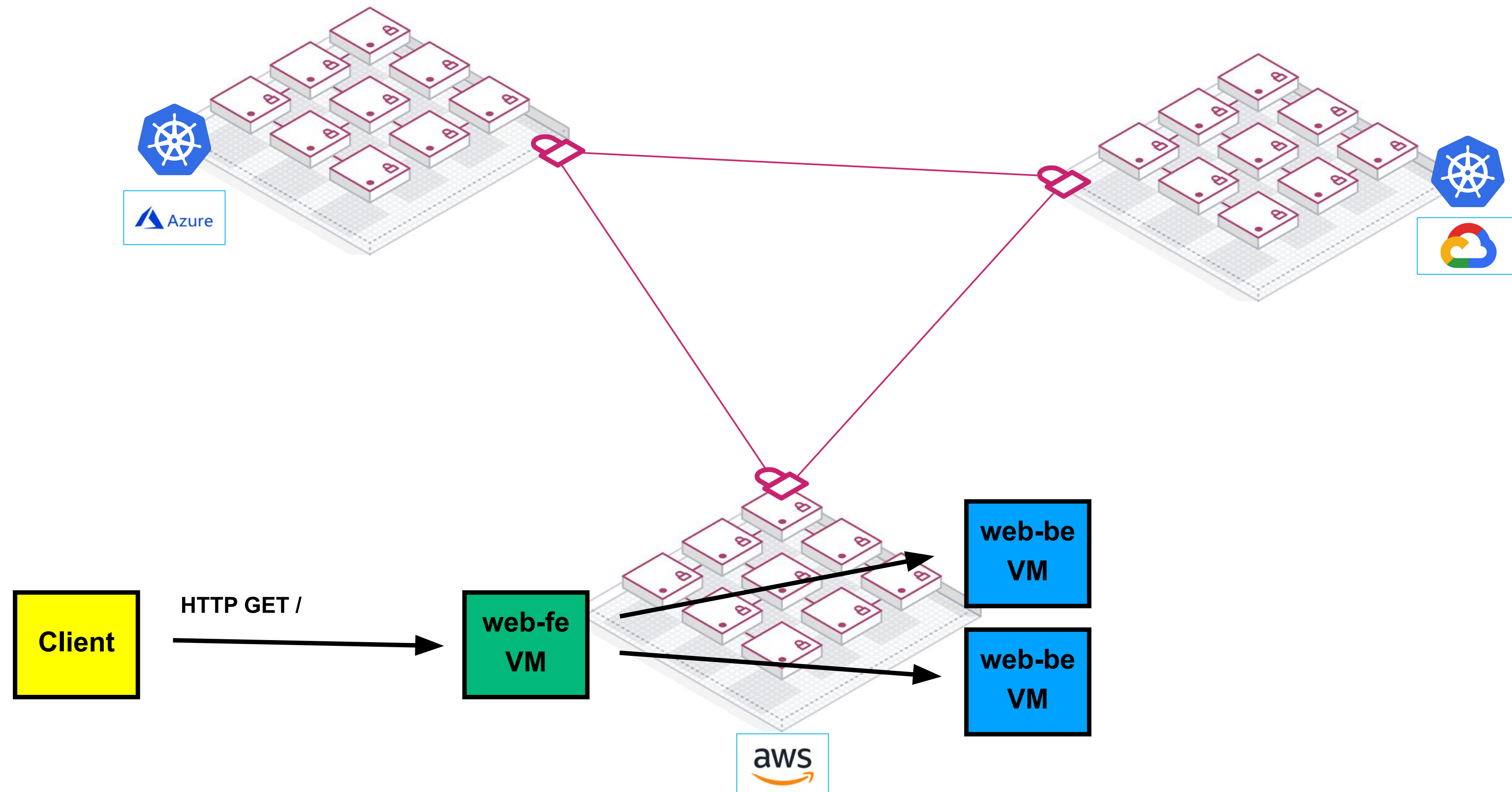


Demo

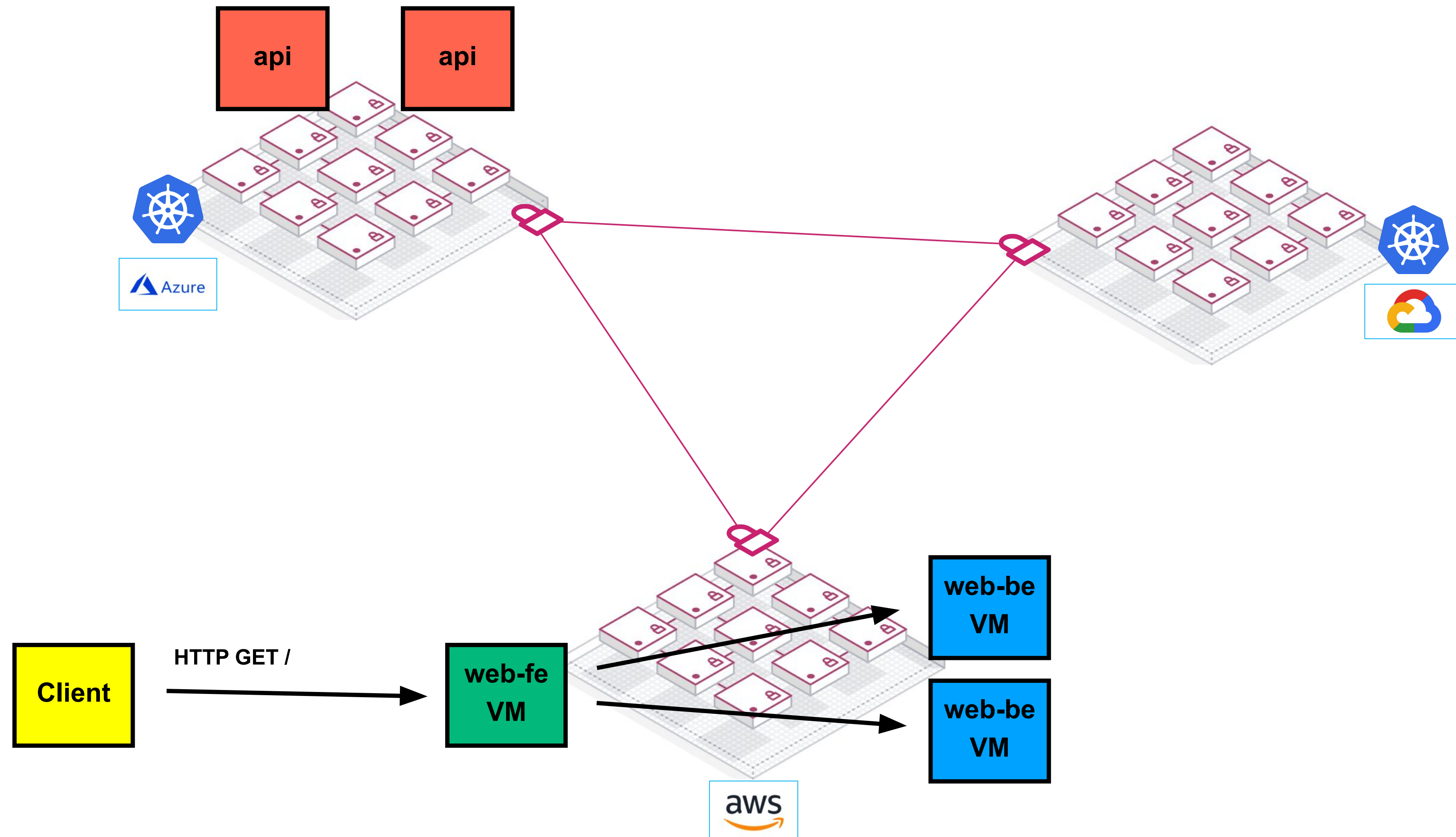
Consul Connect Multi-Cloud Demo Environment



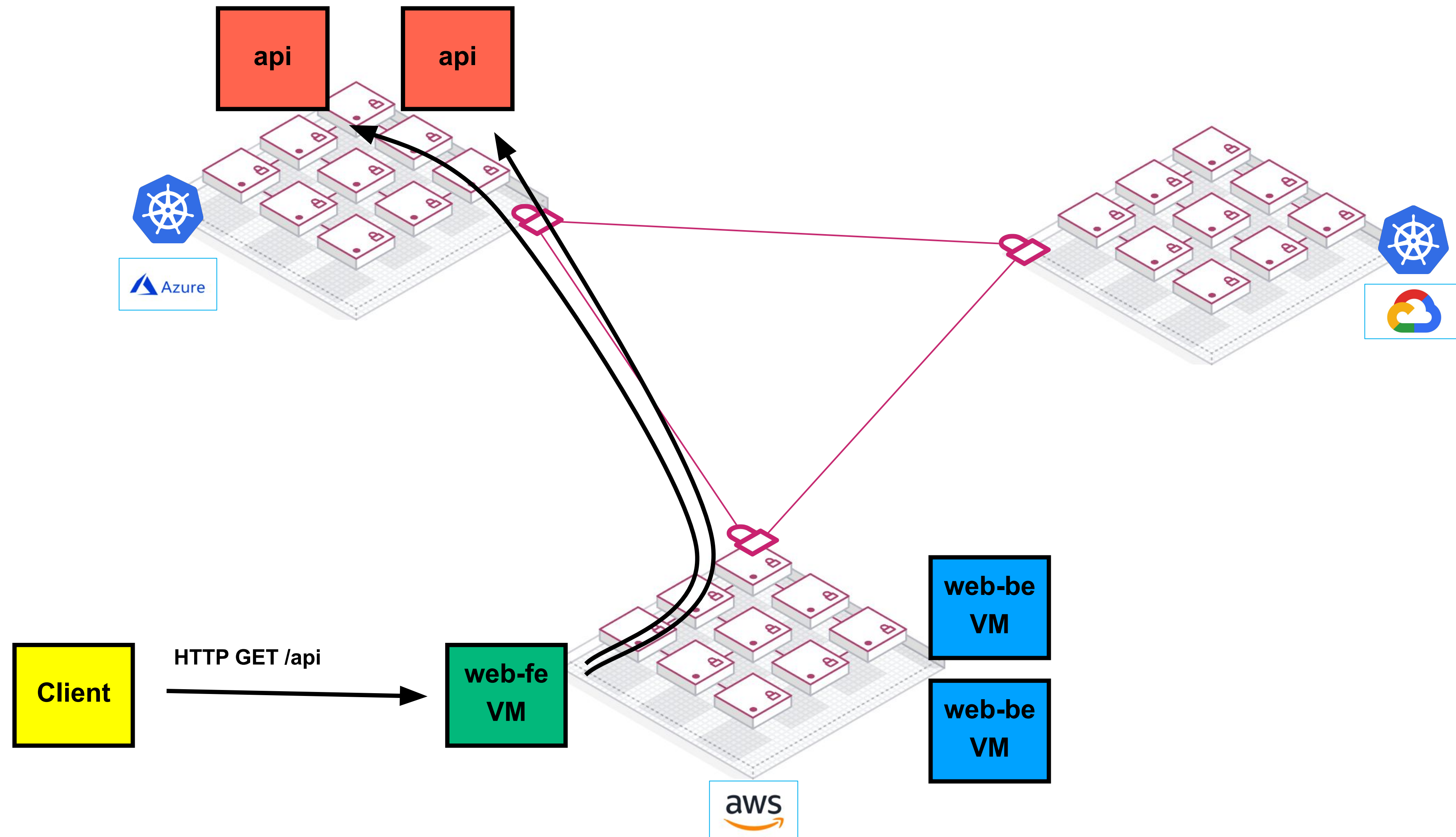
Consul Connect Multi-Cloud Demo Environment



Consul Connect Multi-Cloud Demo Environment



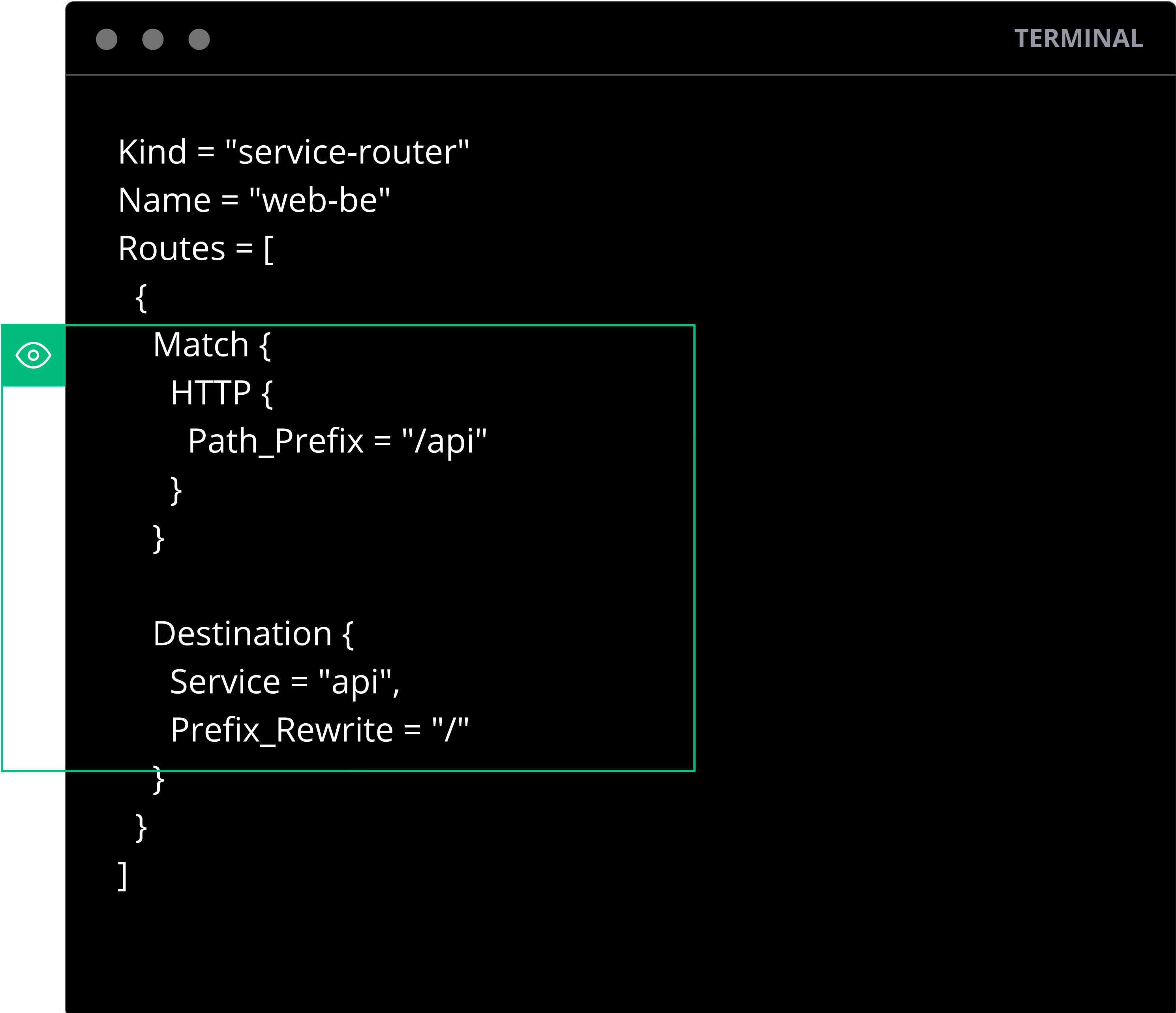
Consul Connect Multi-Cloud Demo Environment



L7 Traffic Management

HTTP Routing

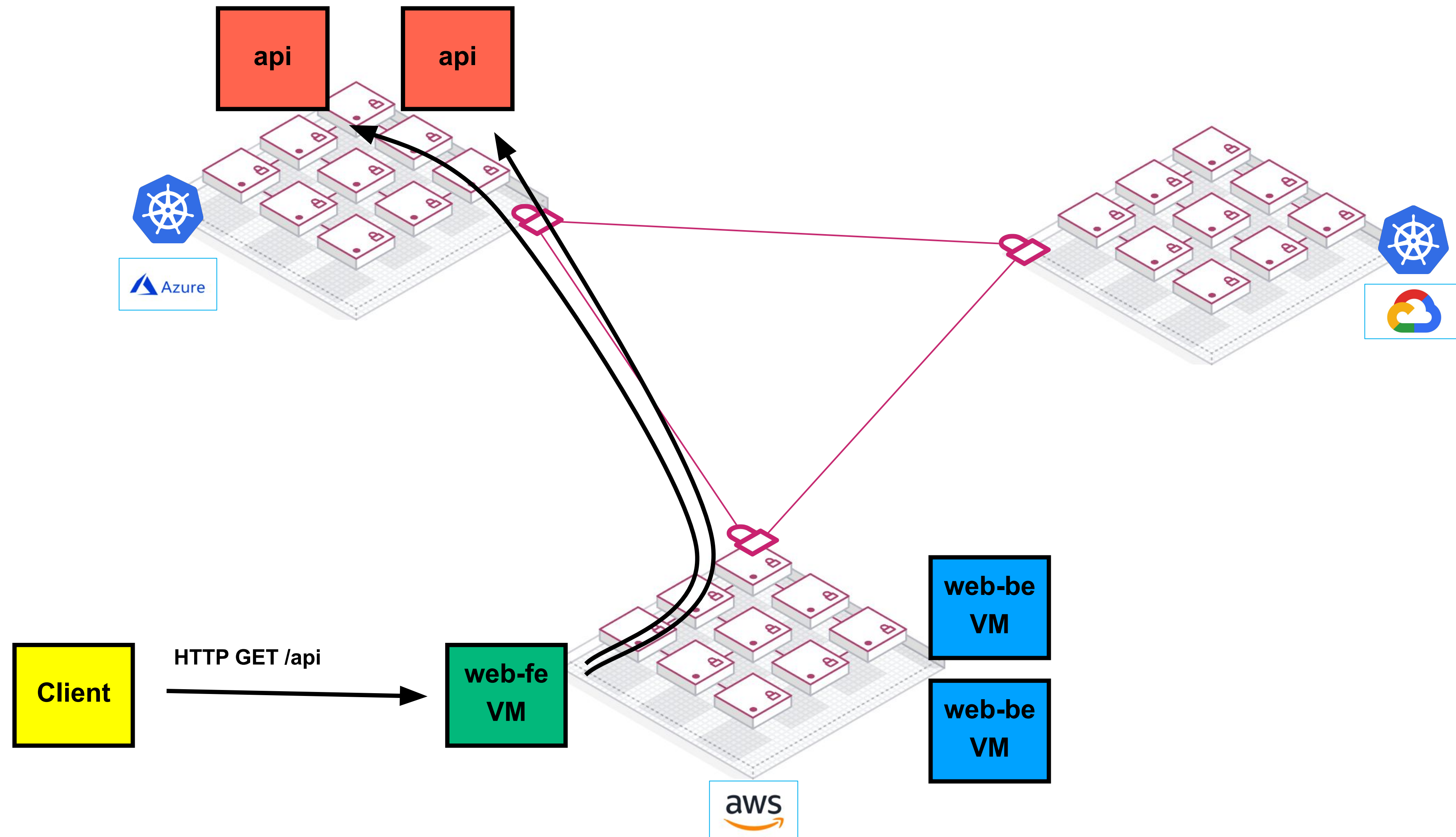
- Path (exact, prefix, regex)
- Header
- Query Params
- HTTP Methods



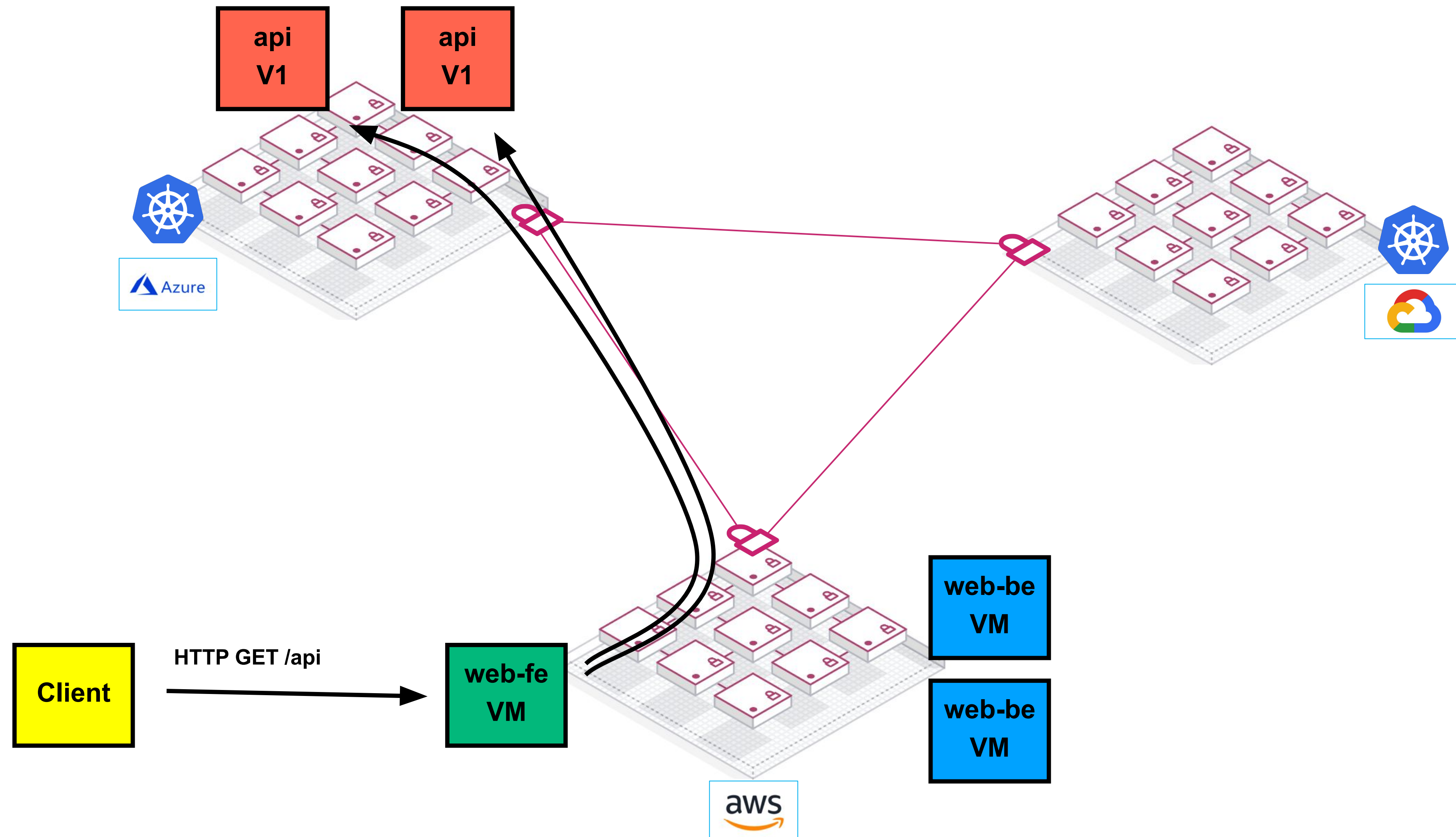
```
Kind = "service-router"
Name = "web-be"
Routes = [
  {
    Match {
      HTTP {
        Path_Prefix = "/api"
      }
    }

    Destination {
      Service = "api",
      Prefix_Rewrite = "/"
    }
  }
]
```

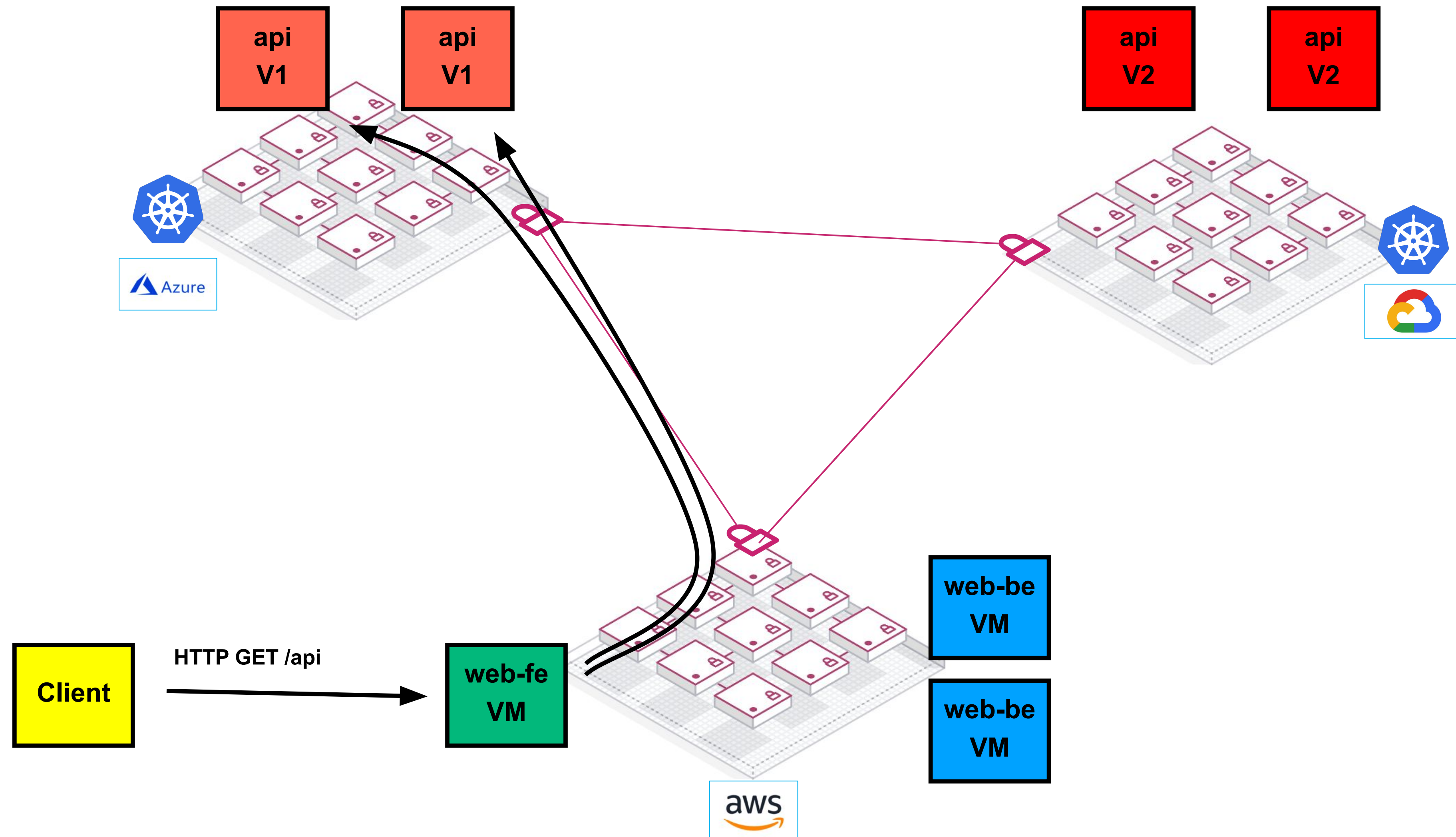
Consul Connect Multi-Cloud Demo Environment



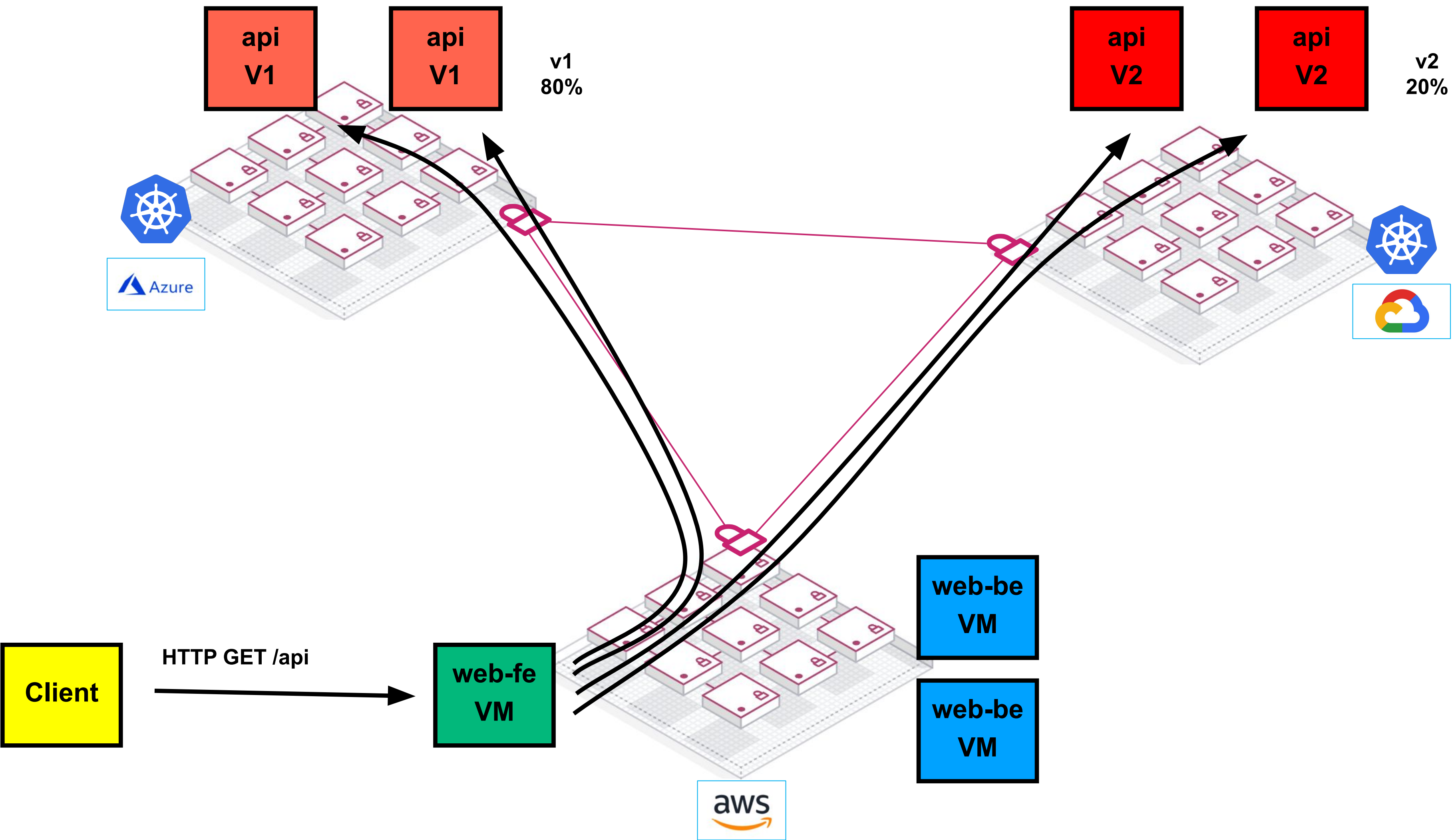
Consul Connect Multi-Cloud Demo Environment



Consul Connect Multi-Cloud Demo Environment



Consul Connect Multi-Cloud Demo Environment



L7 Traffic Management

Traffic Splitting

```
Kind = "service-splitter"
Name = "api"
Splits = [
  {
    Weight      = 80
    Service_Subset = "v1"
  },
  {
    Weight      = 20
    Service_Subset = "v2"
  }
]
```

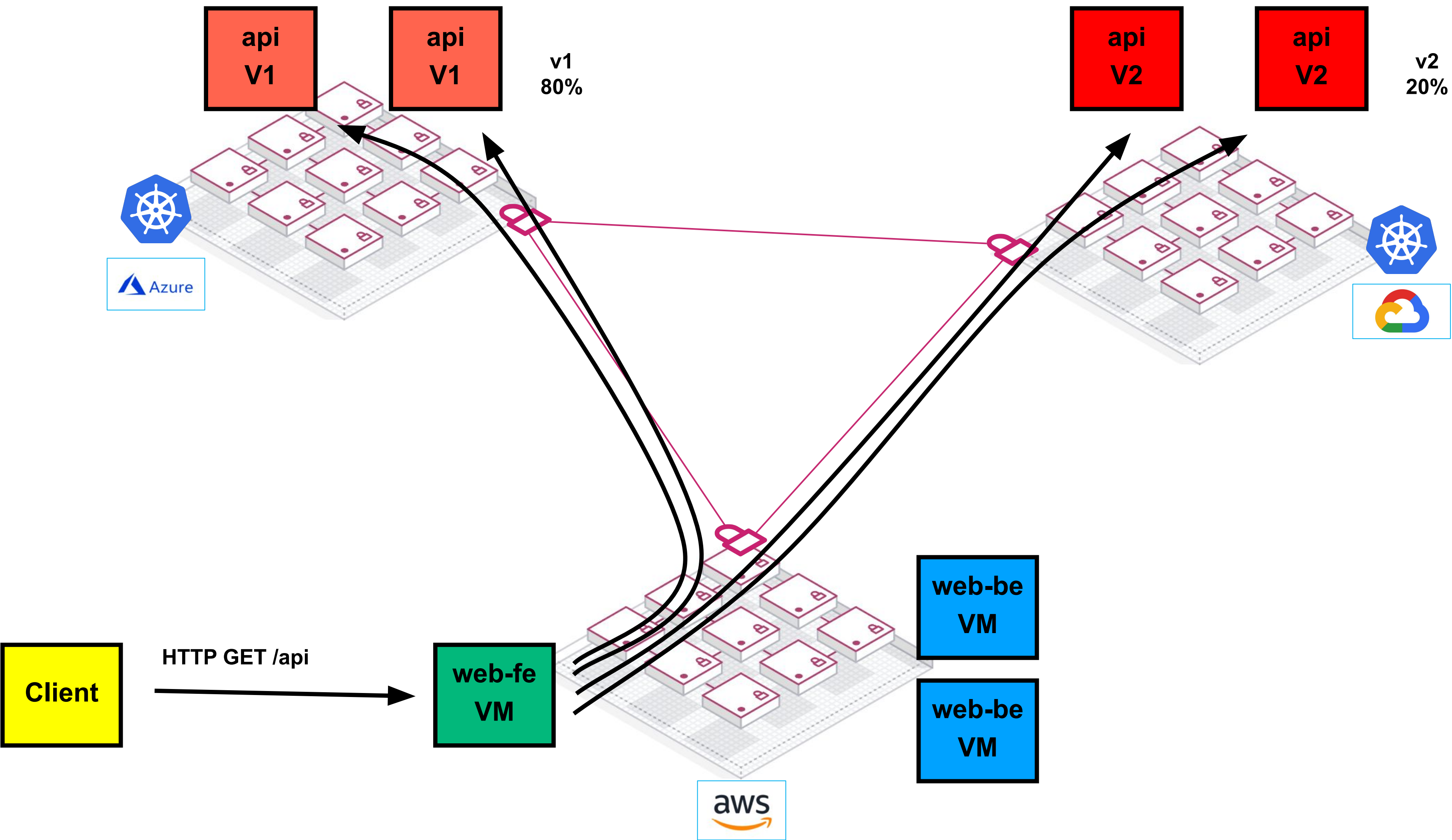

L7 Traffic Management

Custom Resolution

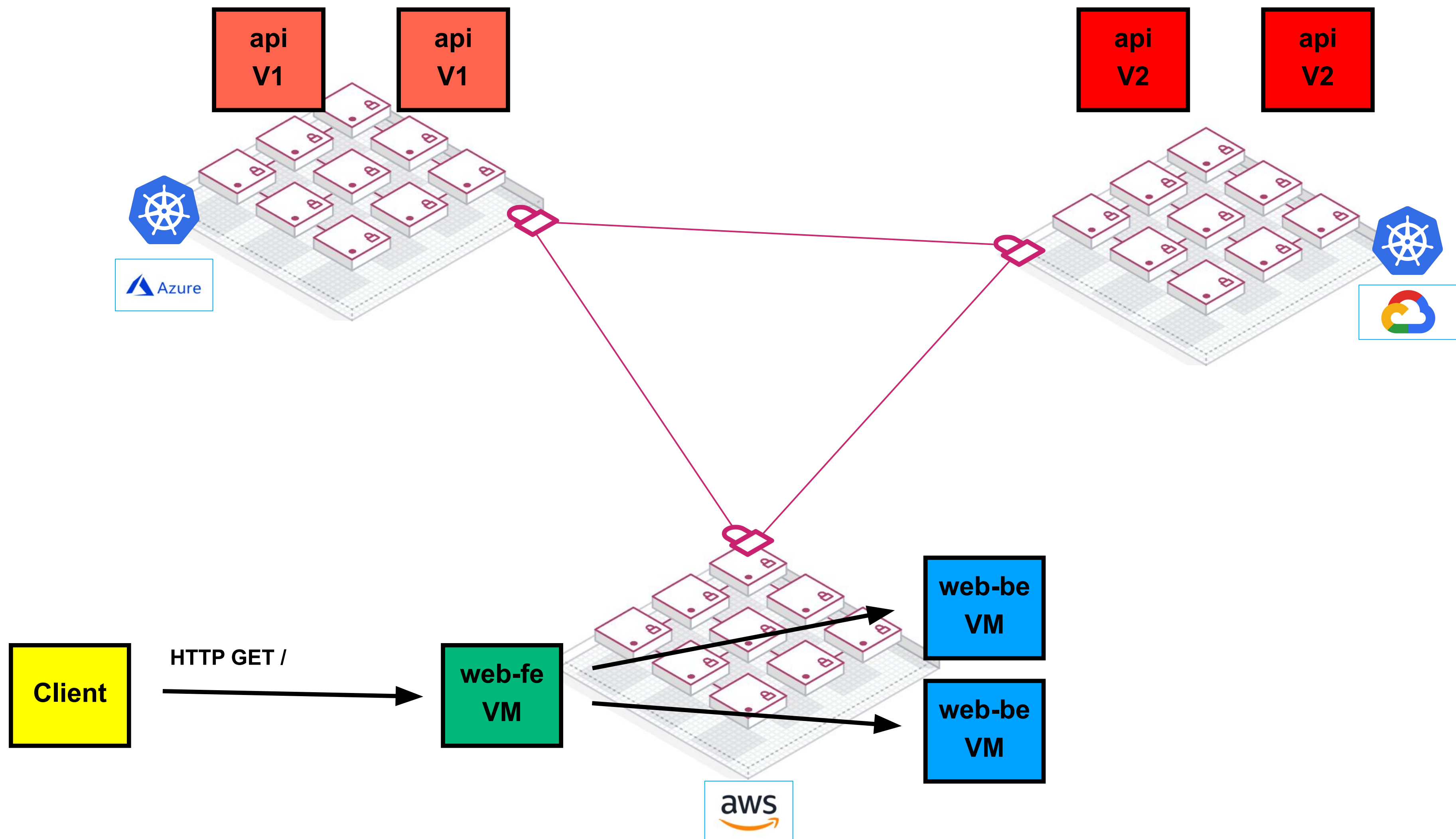
TERMINAL

```
Kind = "service-resolver"
Name = "api"
DefaultSubset = "v1"
Subsets = {
  "v1" = {
    Filter = "Service.Meta.version == v1"
  },
  "v2" = {
    Filter = "Service.Meta.version == v2"
  },
}
```

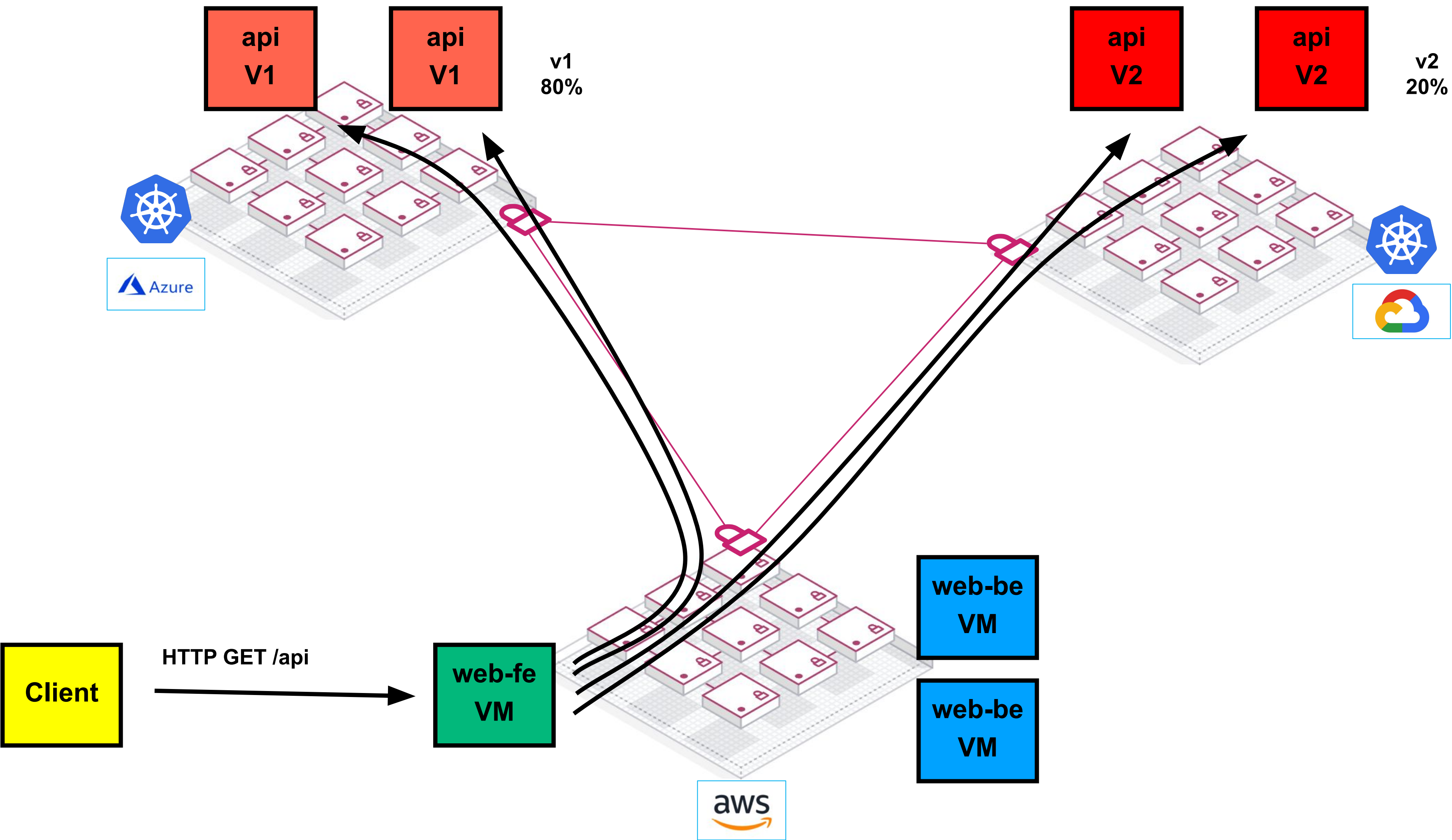
Consul Connect Multi-Cloud Demo Environment



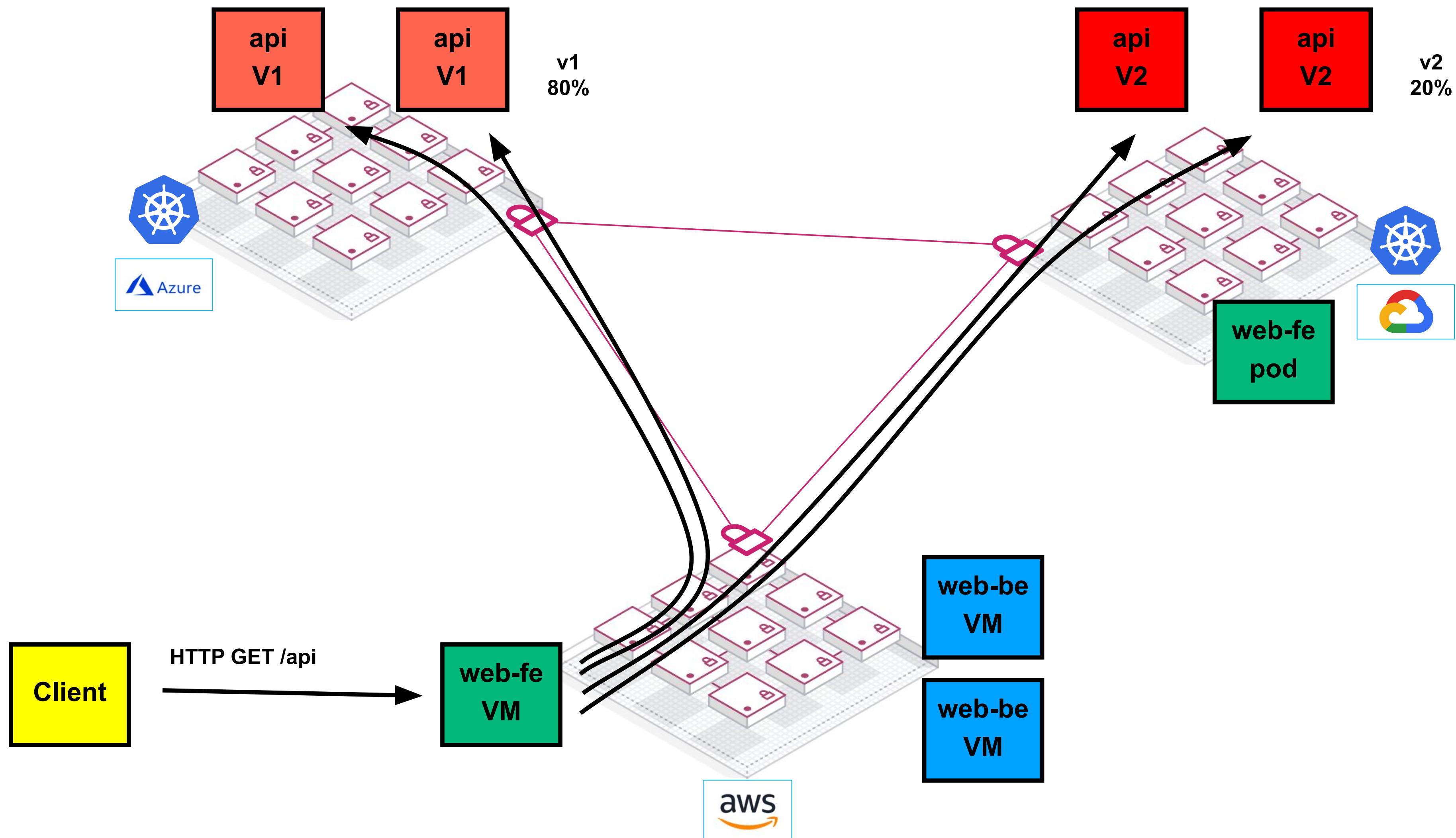
Consul Connect Multi-Cloud Demo Environment



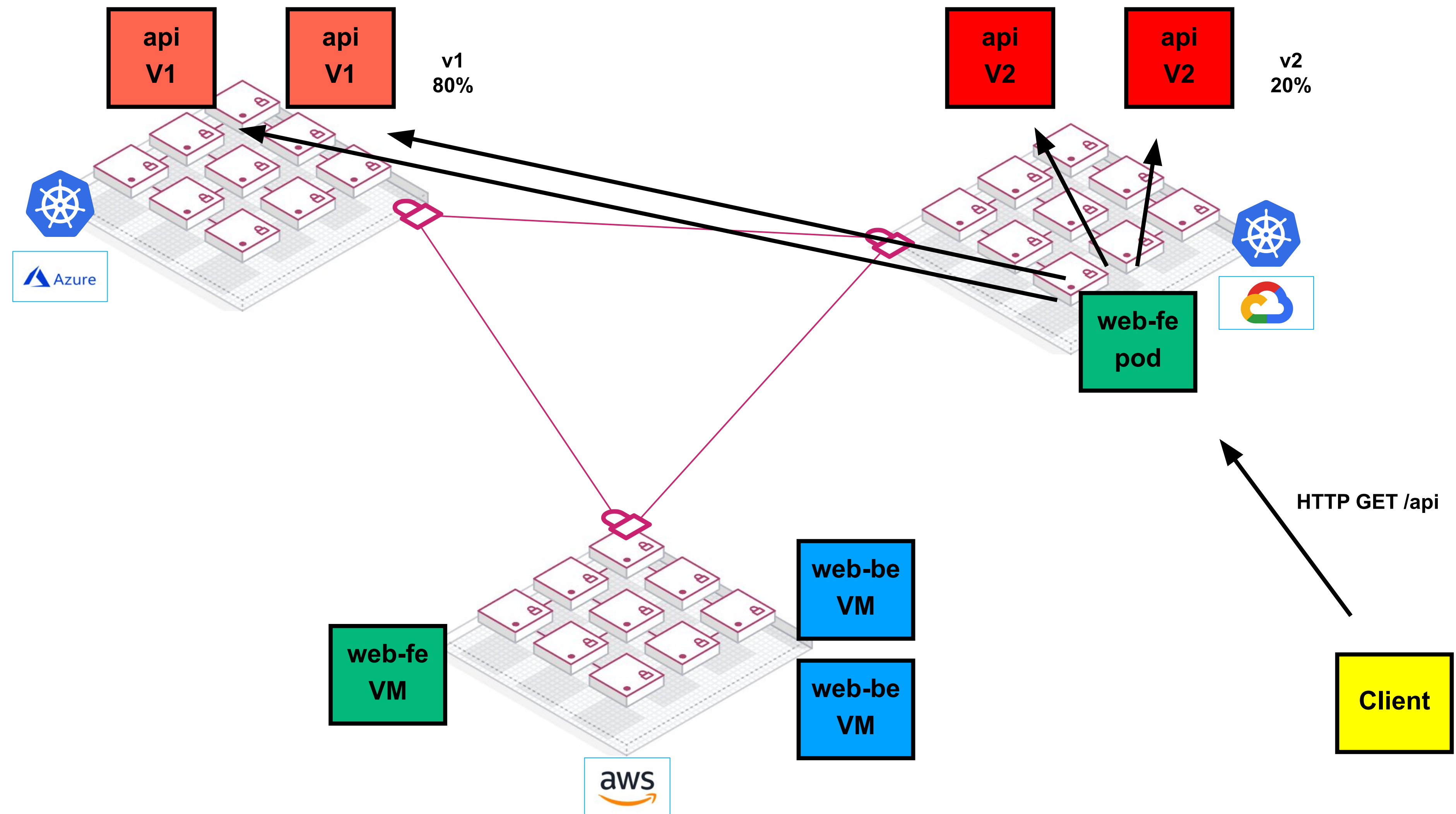
Consul Connect Multi-Cloud Demo Environment



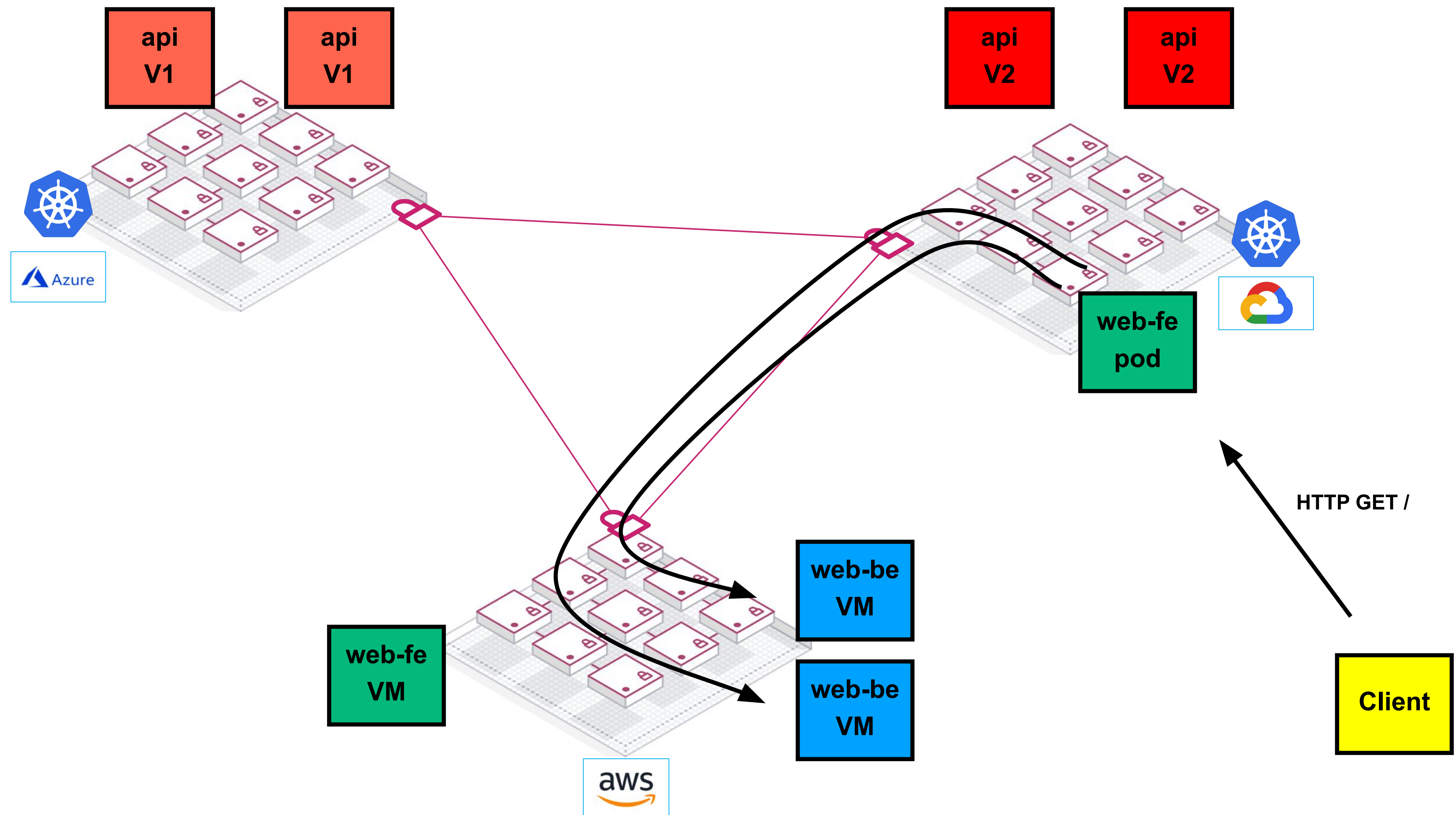
Consul Connect Multi-Cloud Demo Environment



Consul Connect Multi-Cloud Demo Environment



Consul Connect Multi-Cloud Demo Environment





Thank you

hello@hashicorp.com

www.hashicorp.com