
KubeCon
CloudNativeCon
North America 2024

KubeCon

CloudNativeCon

North America 2024

Kubernetes Multi-Cluster Networking 101

Niranjan Shankar, Microsoft & Ram Vennam, Solo.io

About Us

Niranjan Shankar

Software Engineer
Microsoft - AKS Traffic Team

Ram Vennam

Product Manager
Solo.io

Overview

1. Multi-Cluster Benefits and Challenges
2. North-South Traffic Management
3. East-West Connectivity and Traffic Management
4. Multi-Cluster Service Discovery and DNS
5. Securing Cross-Cluster Traffic
6. Recommendations and Takeaways

Multi-Cluster Benefits

Performance & Scale

Multi-Cloud & Hybrid Flexibility

HA & Resilience

Security & Compliance

Cost & Resource Efficiency

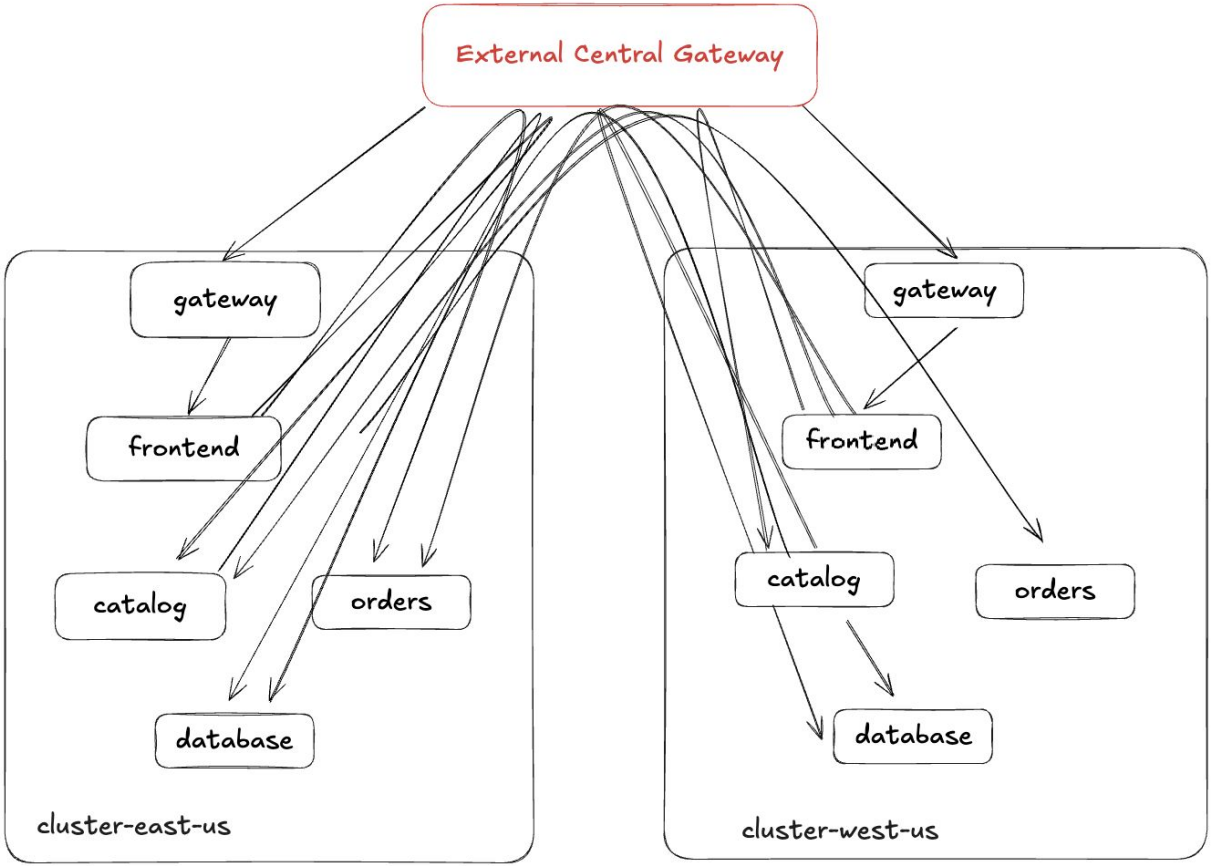
Isolation & Multi-Tenancy

Multi-Cluster Networking Challenges

- Network connectivity and latency
- Secure communication
- Service discovery & DNS
- Access control
- Load balancing

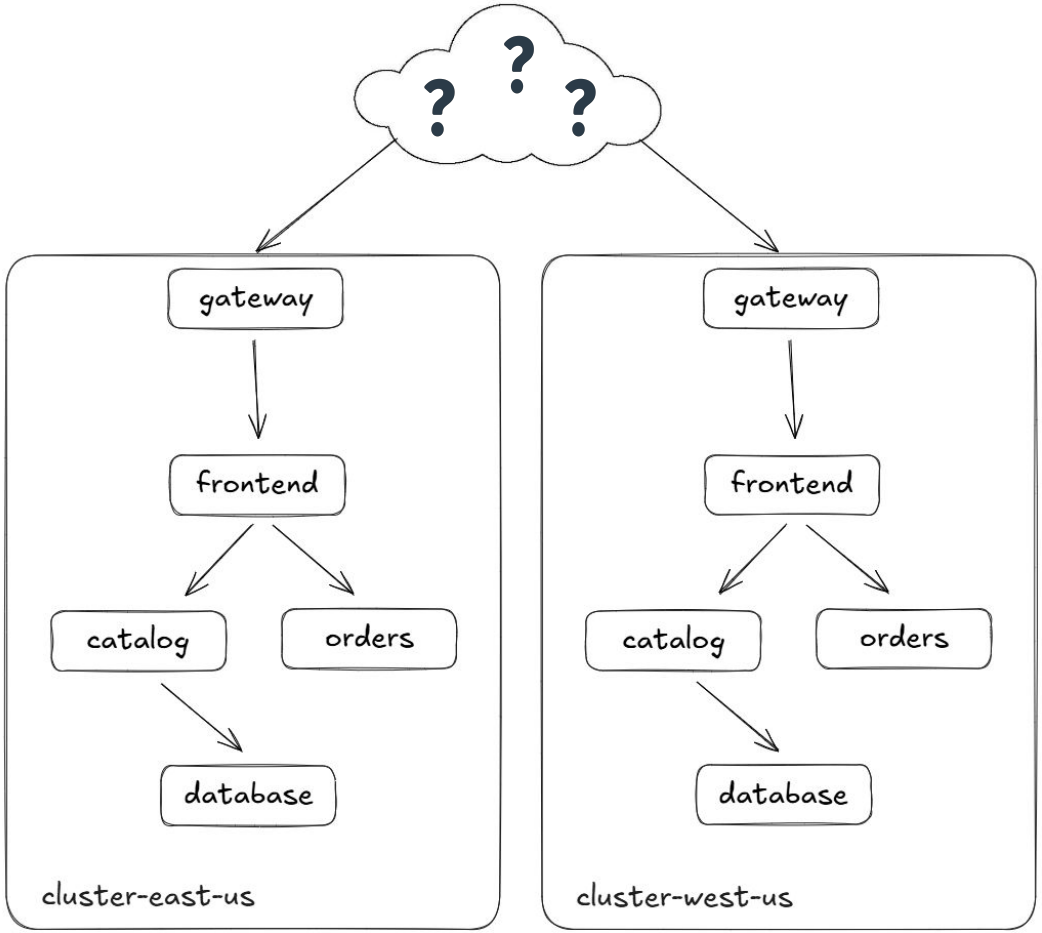
+ All the challenges of single cluster!

Multi-Cluster Networking: Patterns to Avoid



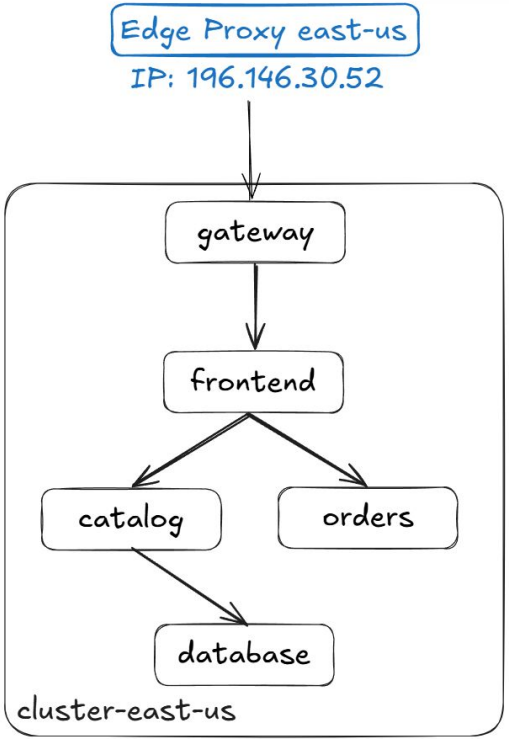
North-South Traffic Management

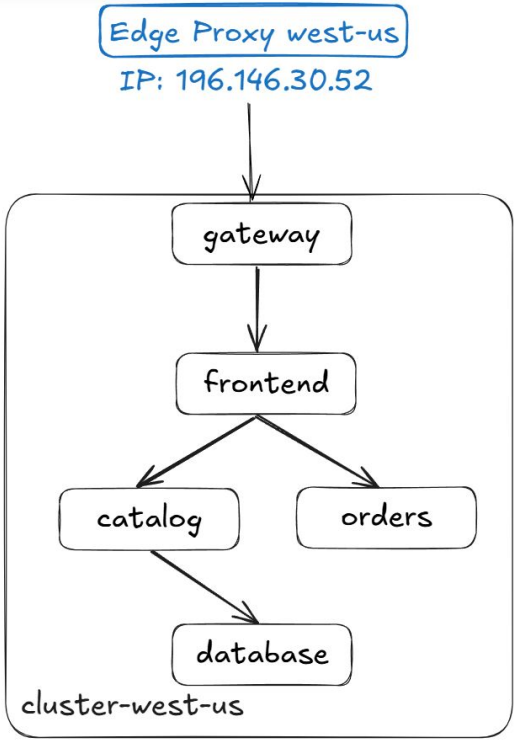
Multi-Cluster Networking: Ingress



Multi-Cluster Ingress: IP-Based with Anycast

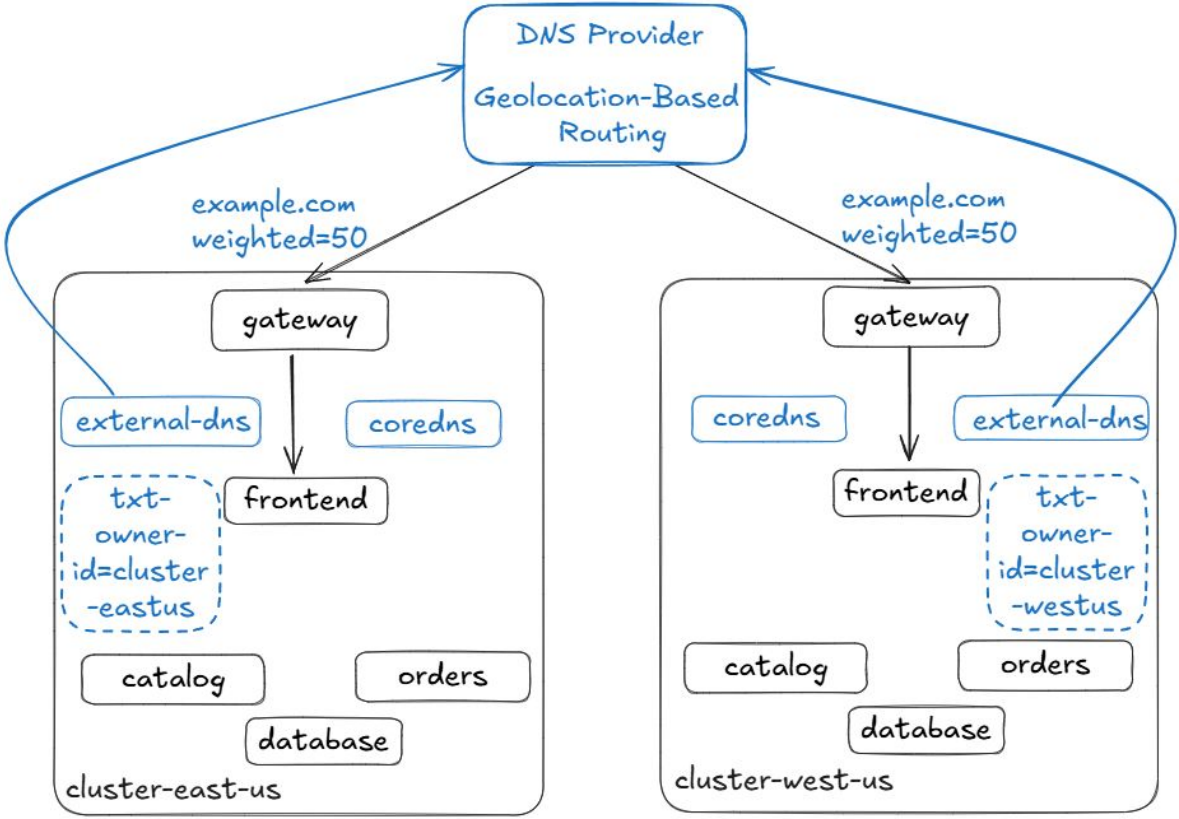
- Options:
  - GKE Multi-Cluster Gateway
  - AWS Global Accelerator





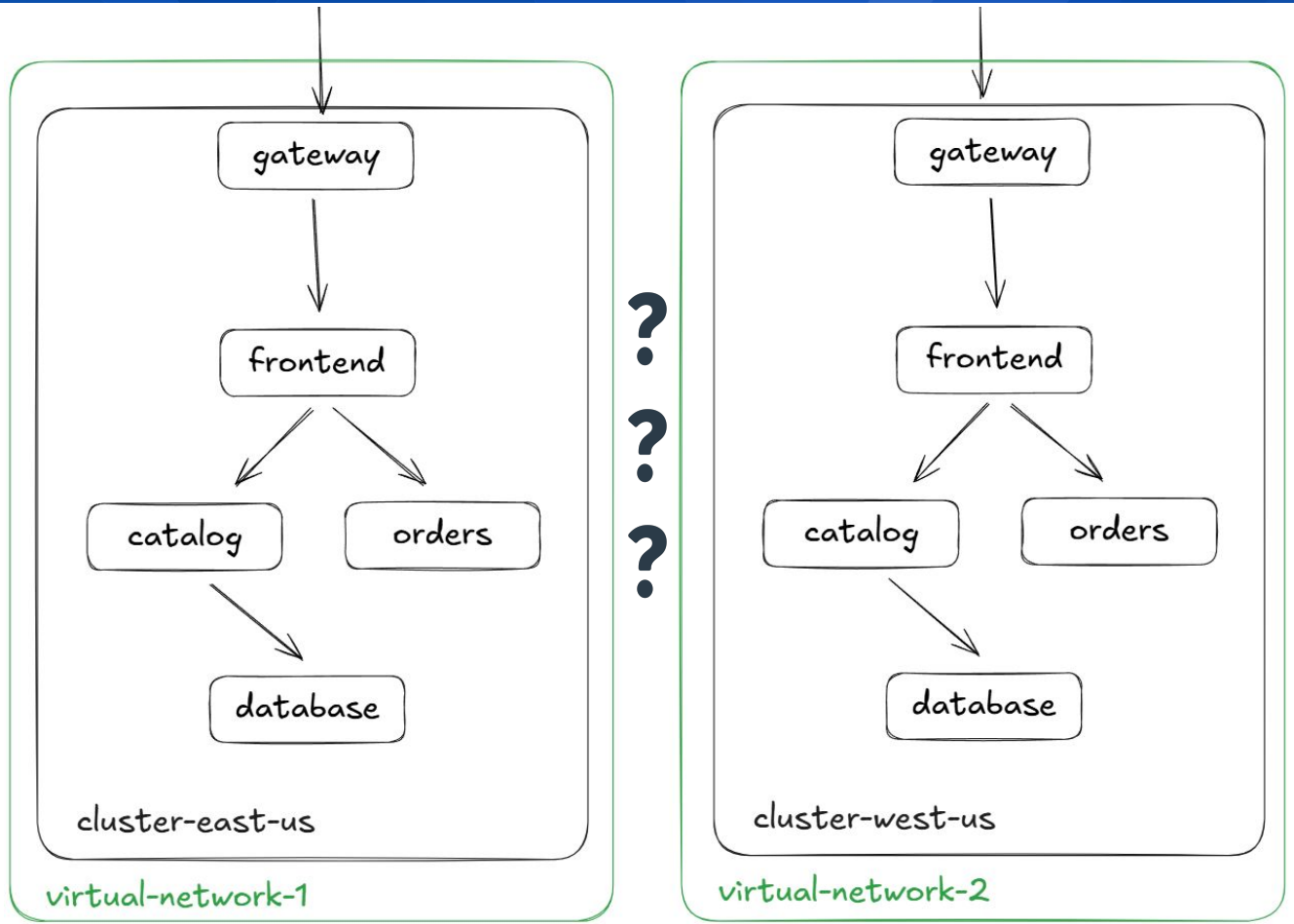
Multi-Cluster Ingress: DNS-based

- Ingress options:
  - K8GB
  - Azure Traffic Manager
- DNS:
  - Route43
  - Azure DNS
  - Cloud DNS



East-West Connectivity and Traffic Management

Multi-Cluster: East-West Connectivity

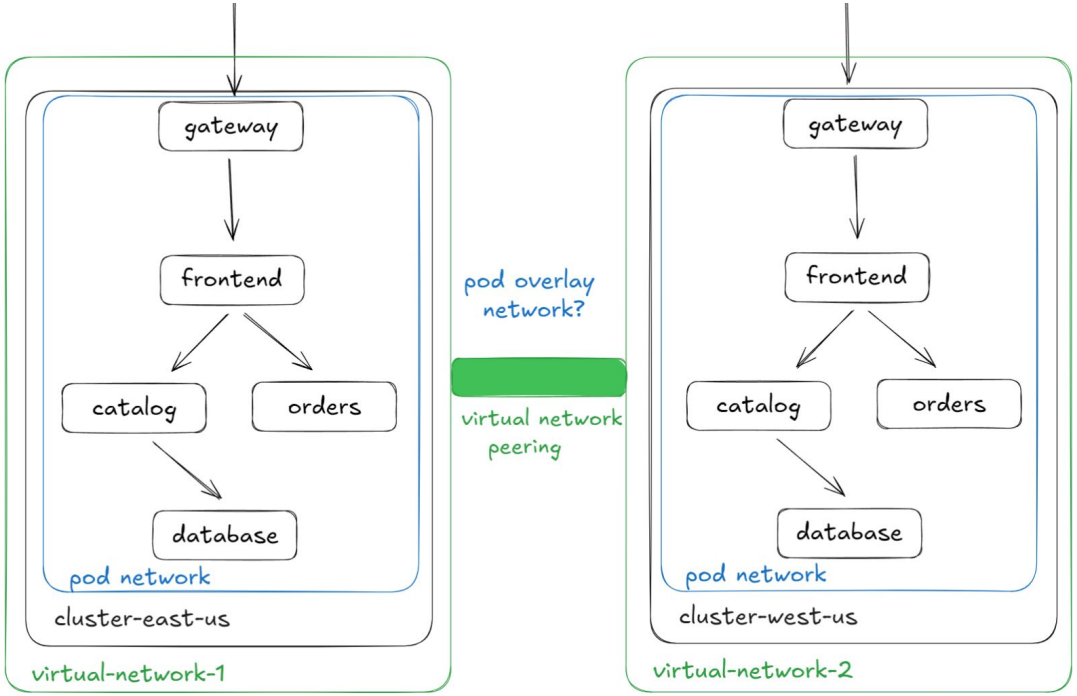


Multi-Cluster: Flat Network

- Both clusters part of the same virtual network OR
- Direct network connection between two virtual networks
  - Low latency, high bandwidth
  - Private communication - cloud “backbone” network
  - Options: Virtual Network / VPC Peering
- Requires non-overlapping CIDRs

Multi-Cluster: Flat Network

- Pod overlay network
  - Gateways
  - Tunneling (VXLAN, IPSec, Wireguard)
    - CNI - Cilium/Calico ClusterMesh
    - Submariner

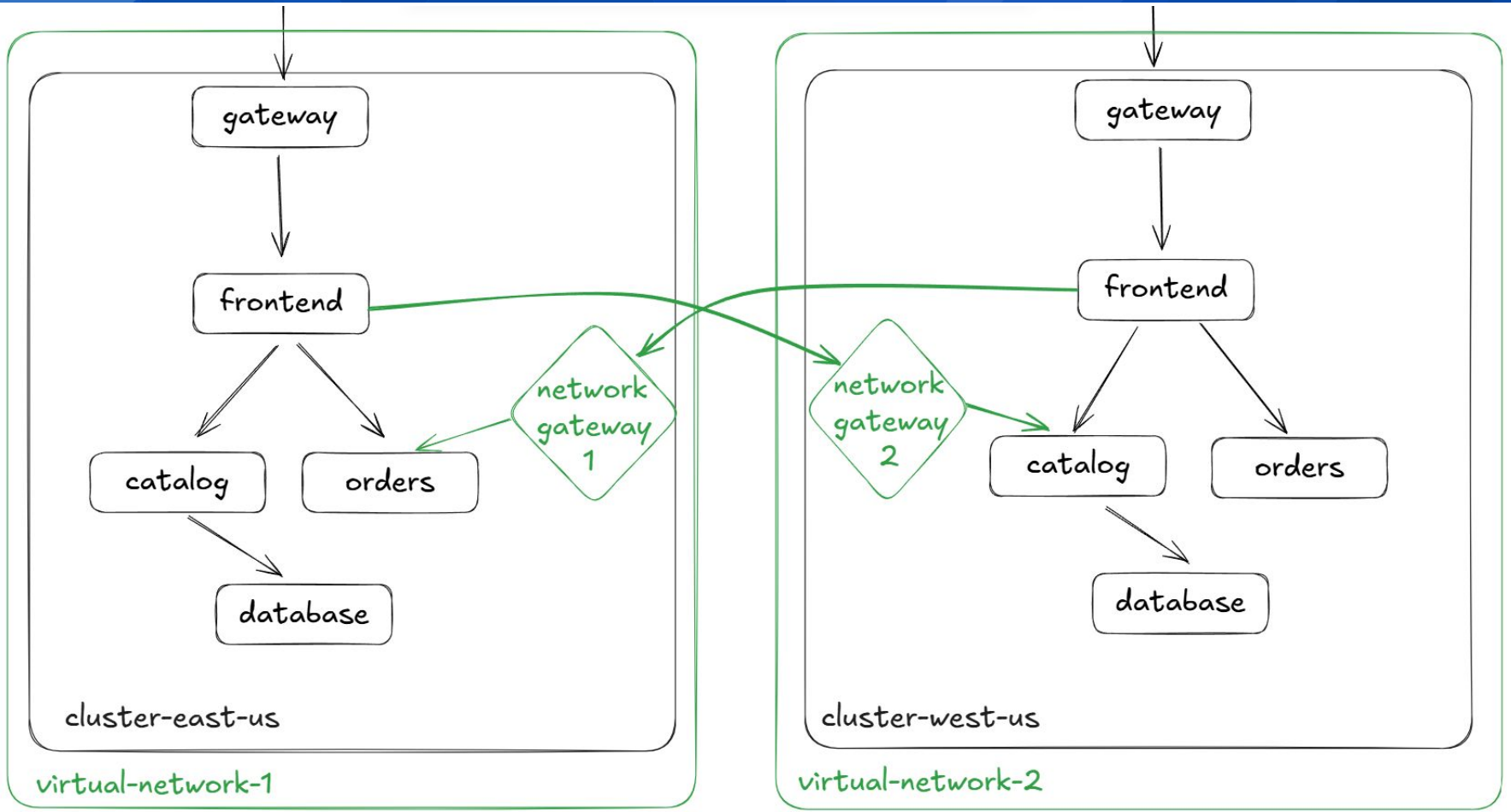


Multi-Cluster: Multi-Network

- Networks are separate and isolated
  - IP range flexibility
- Gateways
  - Cloud provider: VPN Gateway*
  - Third-party and open source solutions
    - Istio east-west gateway, Linkerd network gateway
    - K8s Load Balancers (Nginx)

**Requires NAT support*

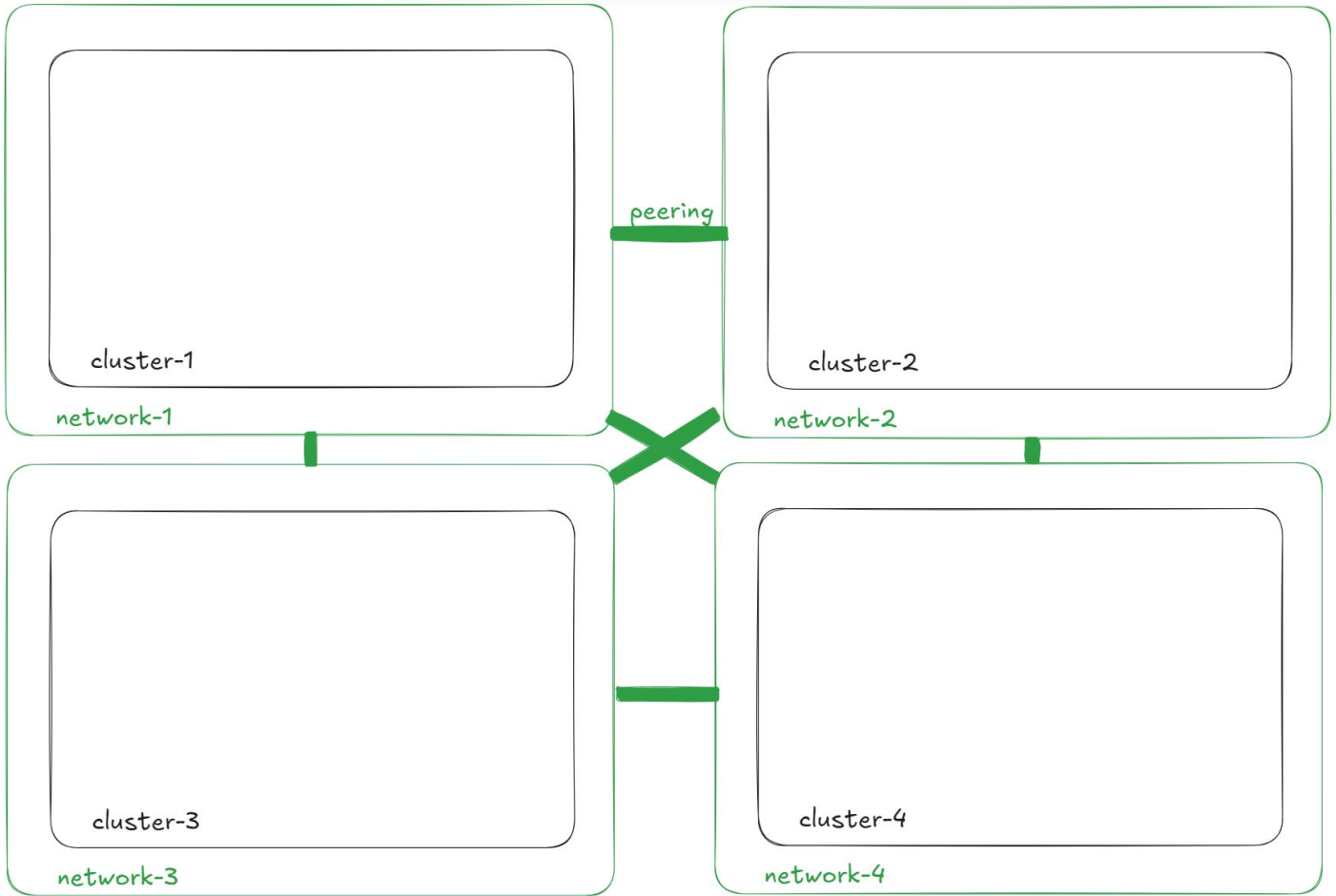
Multi-Cluster: Multi-Network



Multi-Cluster Network Topologies: Comparison

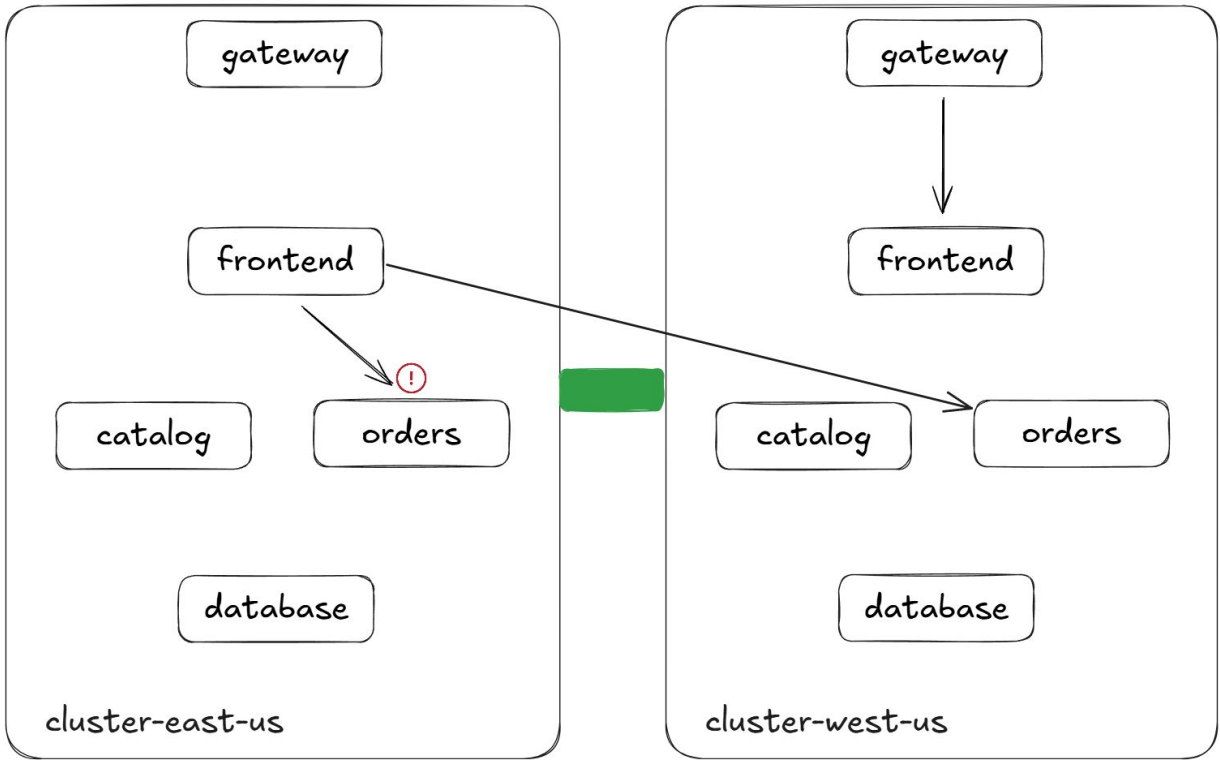
	Flat Network	Multi-Network
Pros	- Low latency, high bandwidth - Secure and private connection - More cost-effective and easier to establish for smaller setups	- IP address / CIDR range flexibility - Network segmentation and isolation - Scalability - Service discovery and endpoint aggregation is easier
Cons	- IP address management more challenging (non-overlapping CIDRs) - Poor scalability (peering = non-transitive)	- Additional hops from gateway - Traffic typically traverses public Internet

Multi-Cluster Network: Full Mesh Architecture



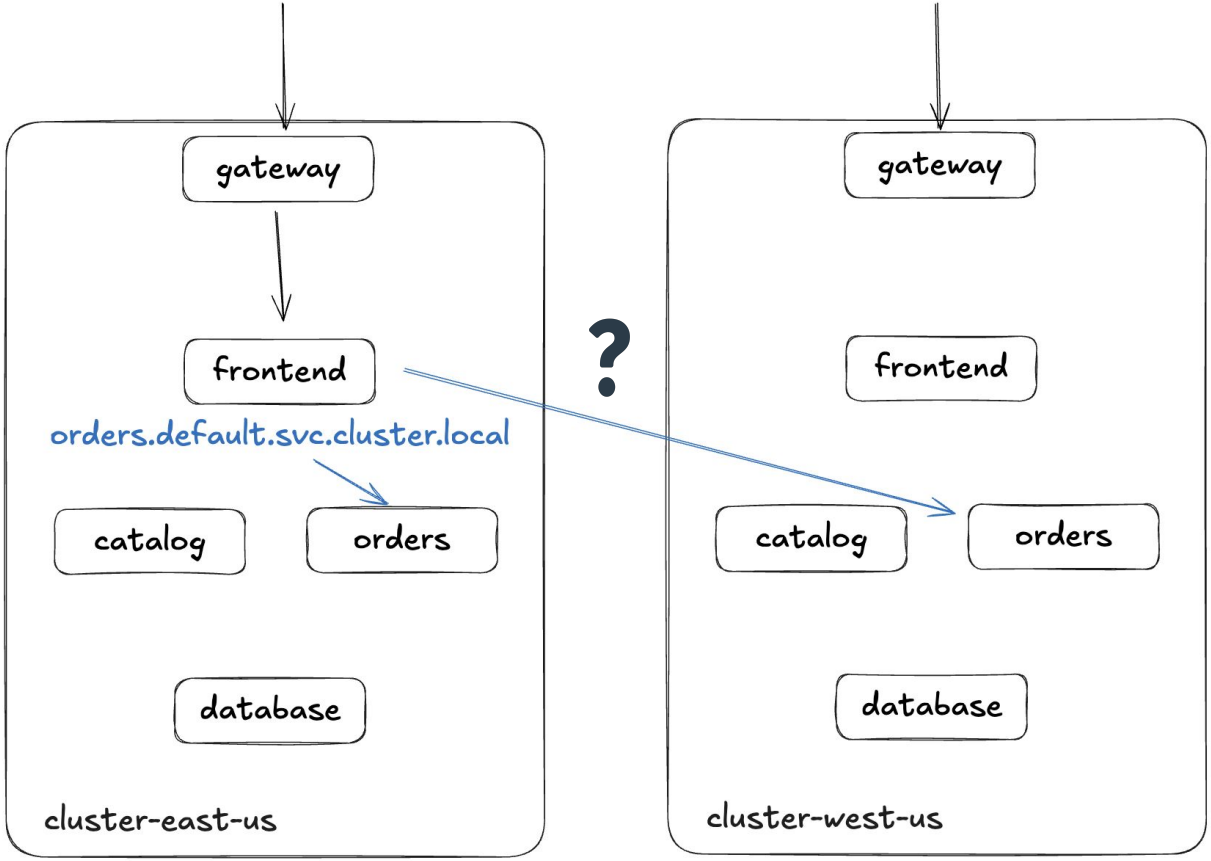
Multi-Cluster: East-West Traffic Management

- Load Balancing
  - Locality
  - Custom
  - Mirroring
- Failover
  - When?
  - Where?

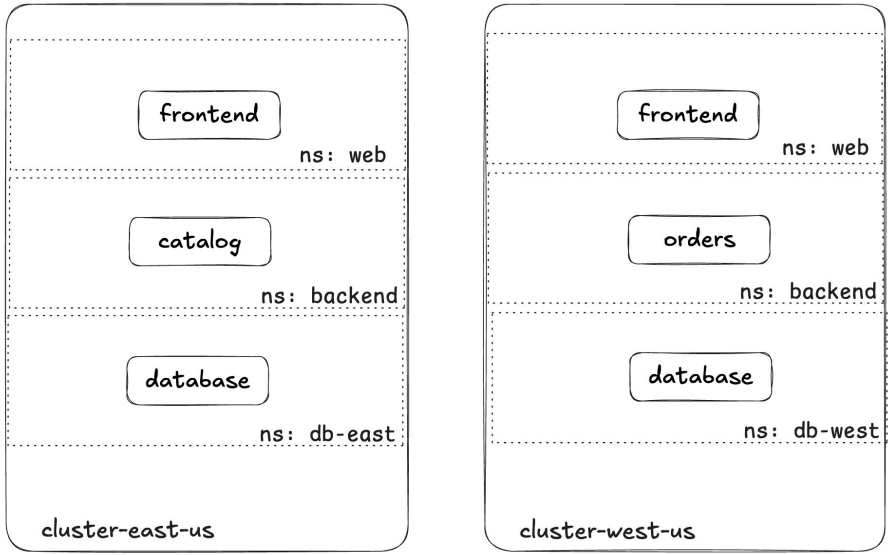


Multi-Cluster Service Discovery and DNS

Multi-Cluster Service Discovery and DNS for EW



Namespace Sameness

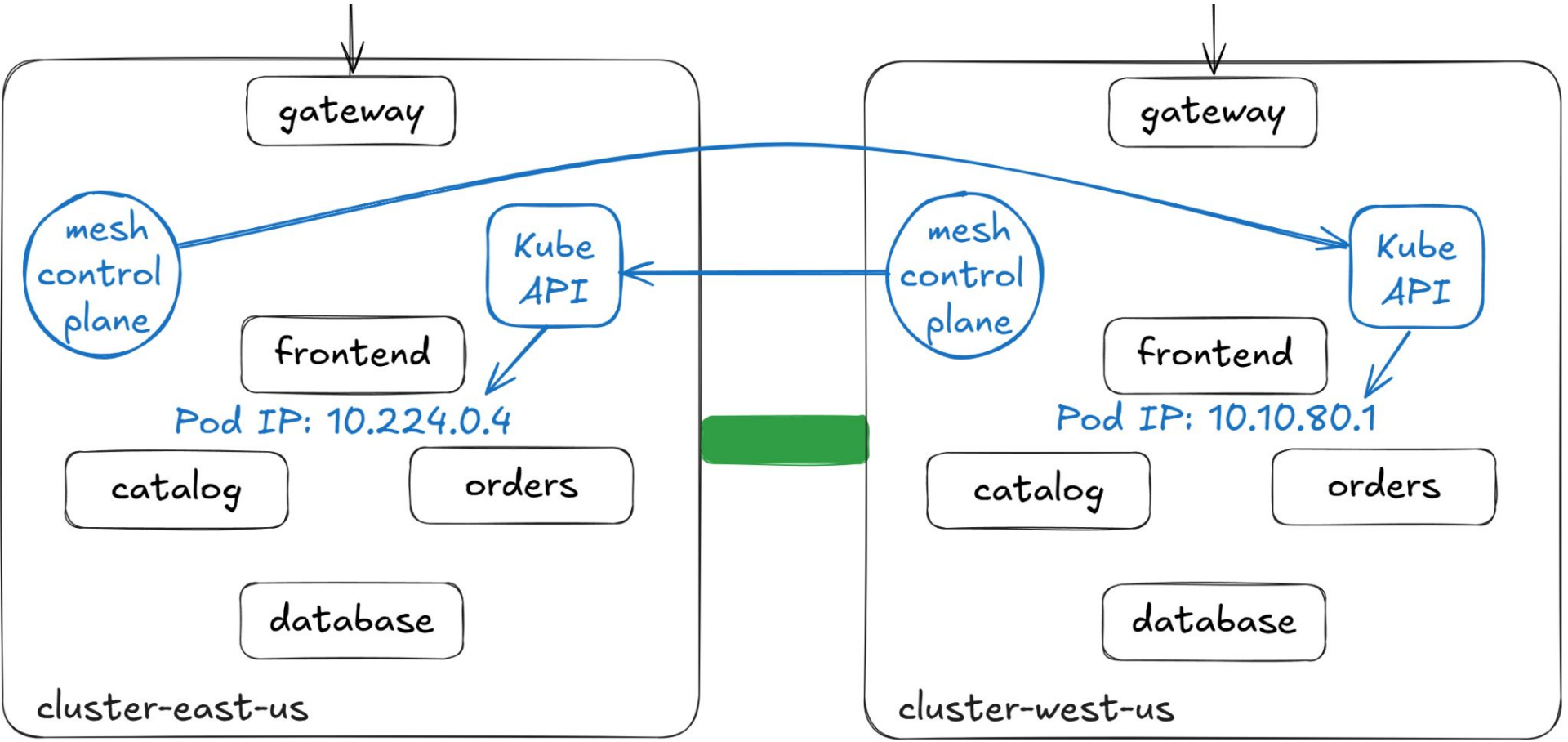


https://multicluster.sigs.k8s.io/concepts/namespace-sameness/

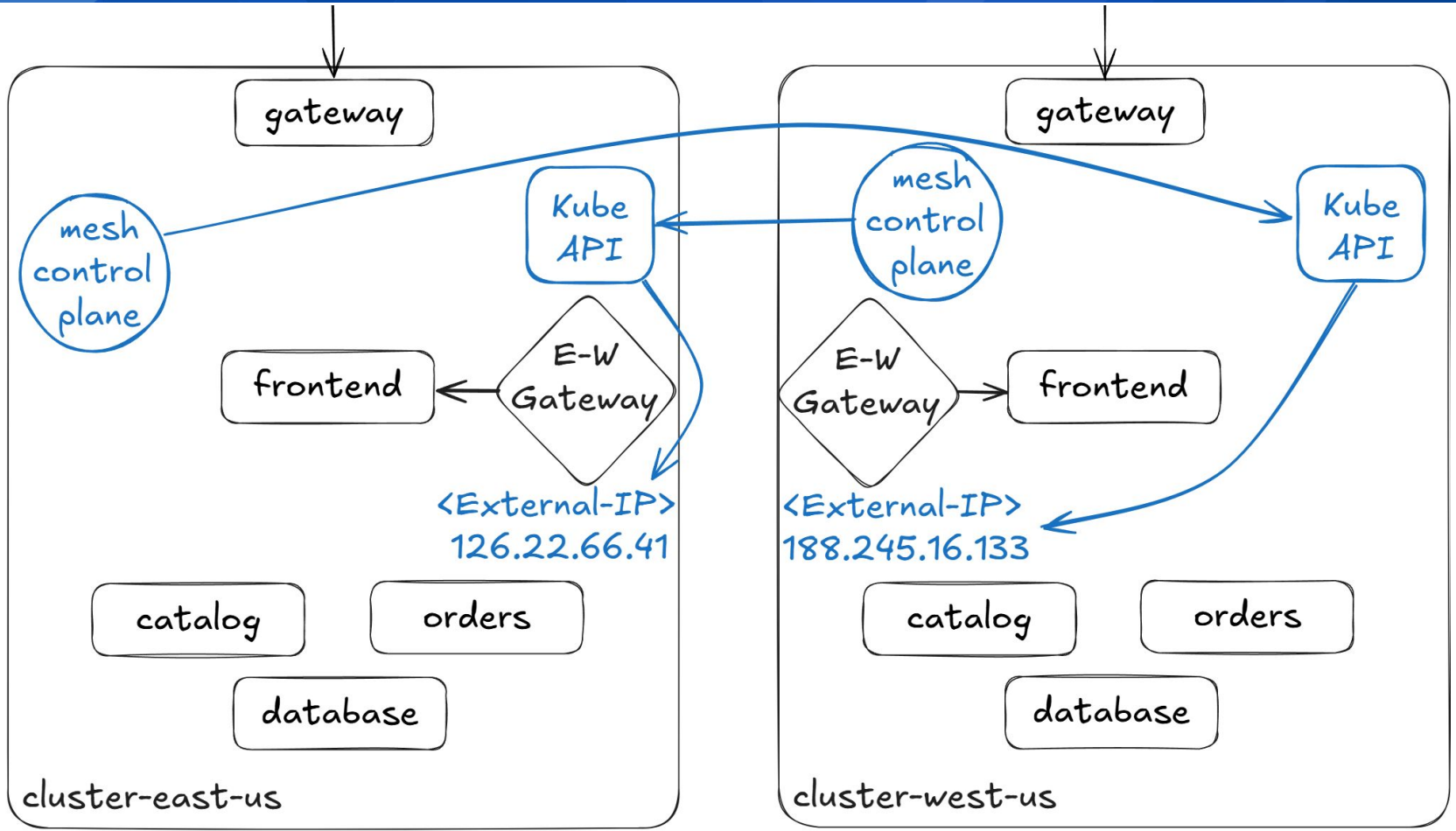
Multi-Cluster Service Discovery: East-West

- Service Mesh
  - Istio / Gloo
  - Linkerd
  - Consul
  - Kuma
- CNI
  - Cilium ClusterMesh
  - Calico ClusterMesh
- Skupper

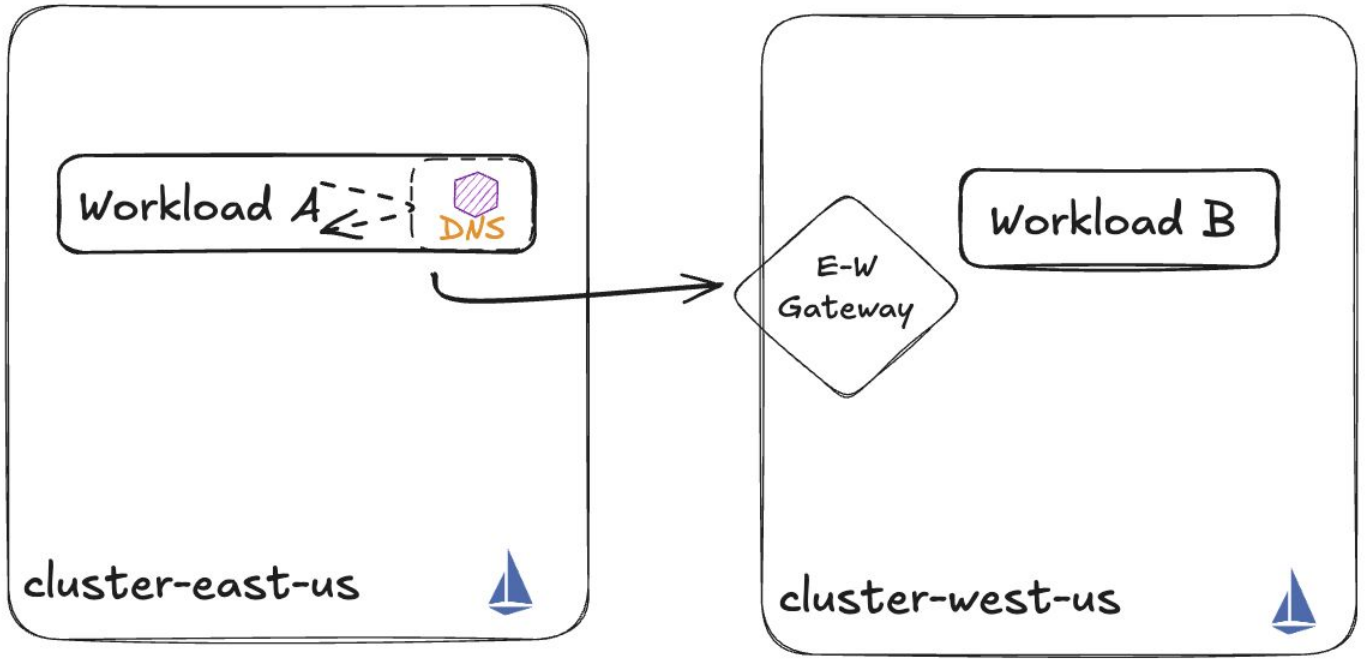
Multi-Cluster Service Discovery: Service Mesh/CNI



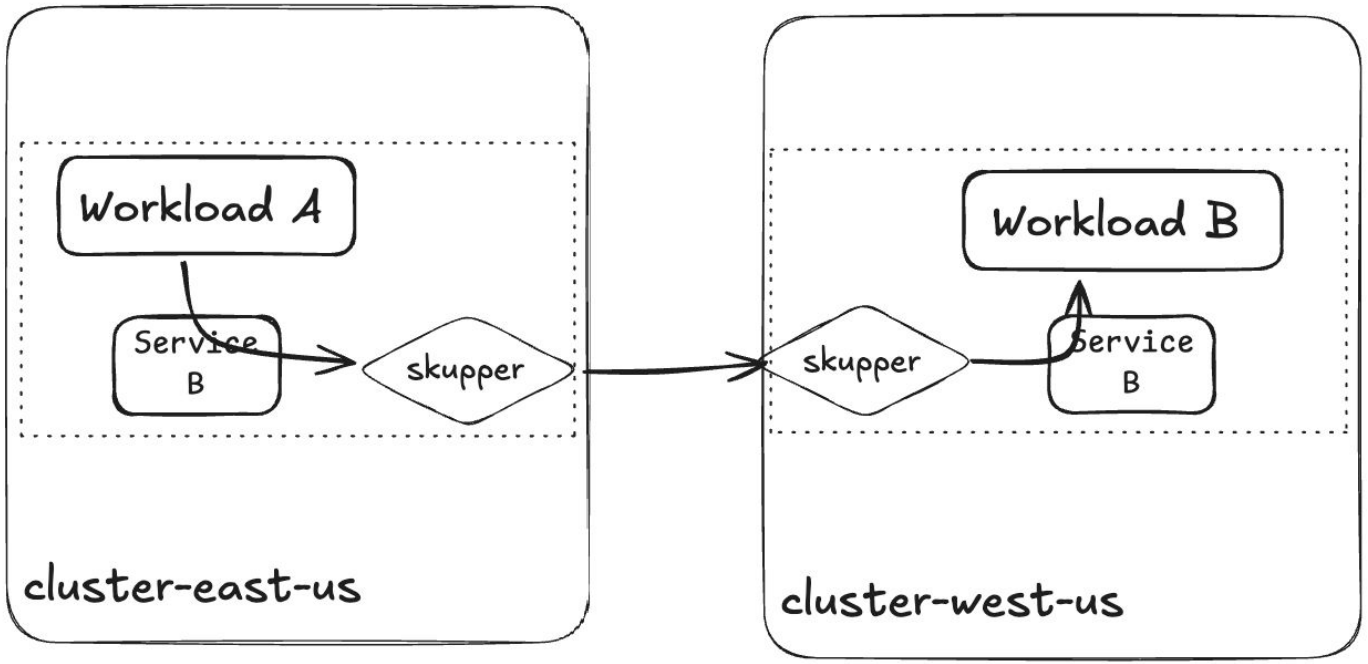
Multi-Cluster Service Discovery: Multi-Network Service Mesh



DNS Proxy with Istio



Application Network Overlay with Skupper

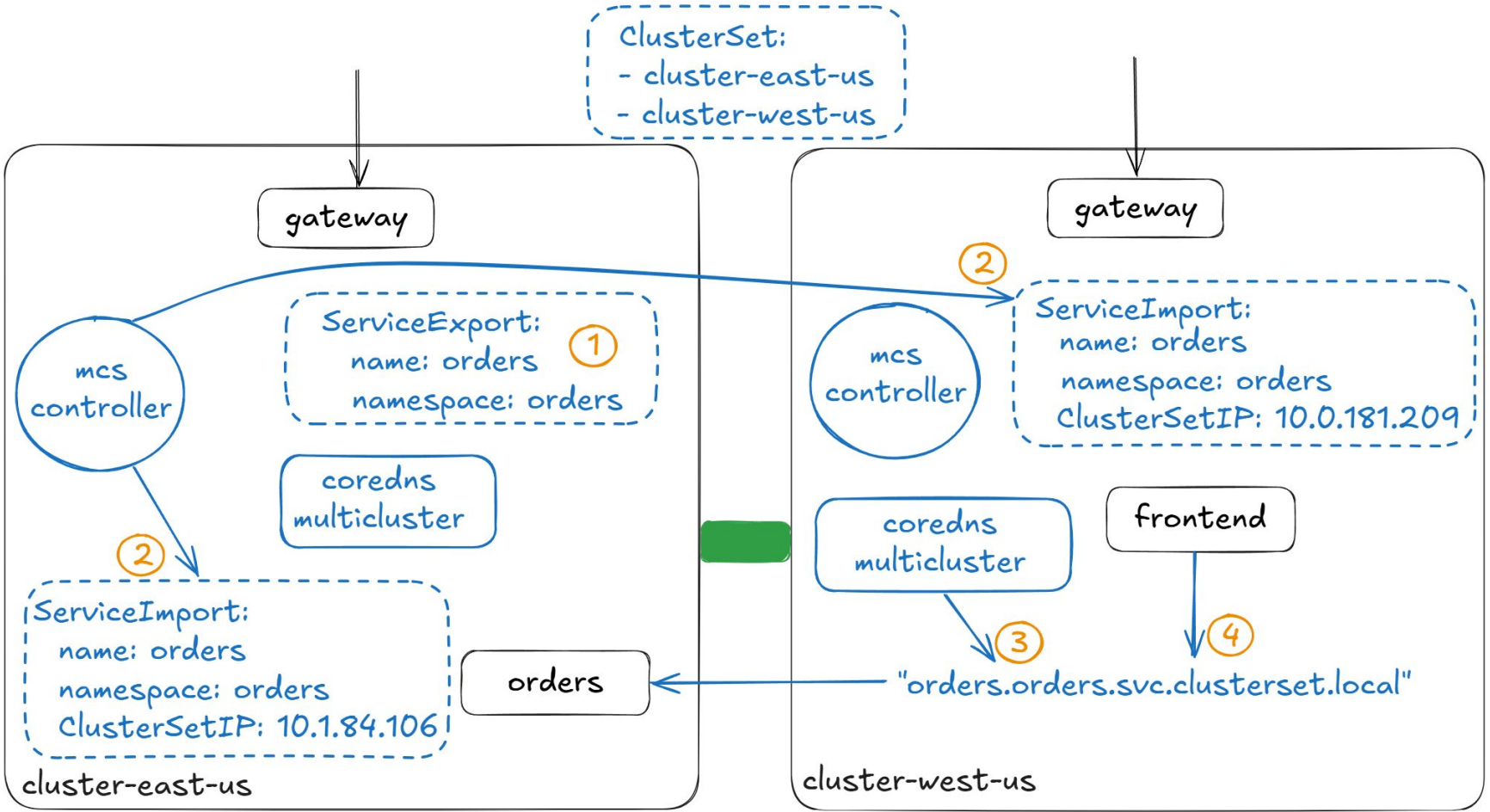


Multi-Cluster Services (MCS) API

- ClusterSet
- ServiceExport
- ServiceImport
- MCS Controller
- DNS Spec
  - CoreDNS Multi-Cluster Plugin
  - Custom DNS proxy or DNS server

https://github.com/kubernetes/enhancements/blob/master/keps/sig-multicluster/1645-multi-cluster-services-api

Multi-Cluster Service Discovery: MCS API



Multi-Cluster Services (MCS) API Options

- OSS
  - Karmada
  - Submariner (Lighthouse)
- Cloud Provider
  - AKS Fleet*
  - GKE / Anthos*
  - EKS - AWS Cloud Map

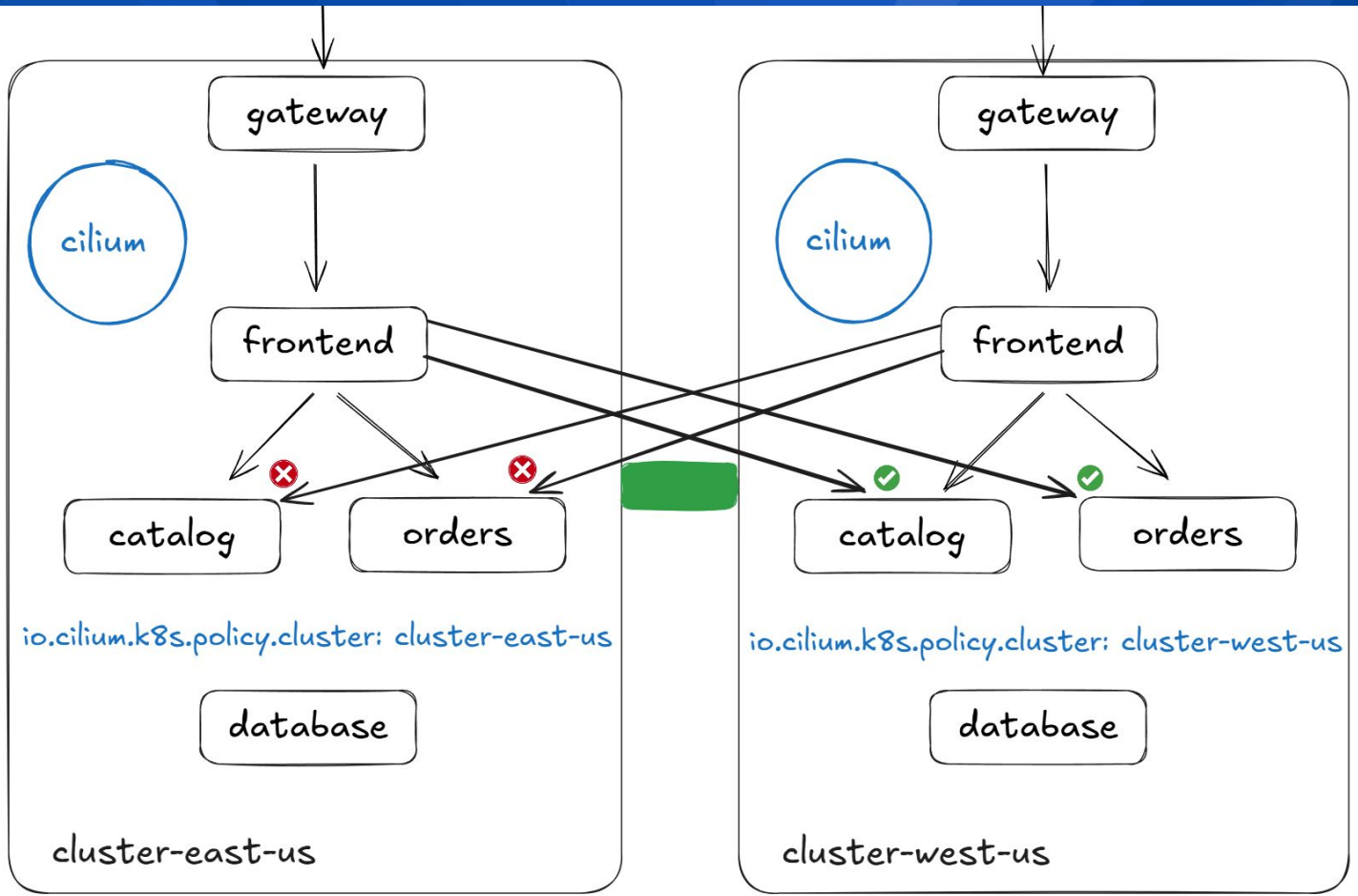
**custom MCS API built on top of upstream K8s implementation*

Securing Cross-Cluster Traffic

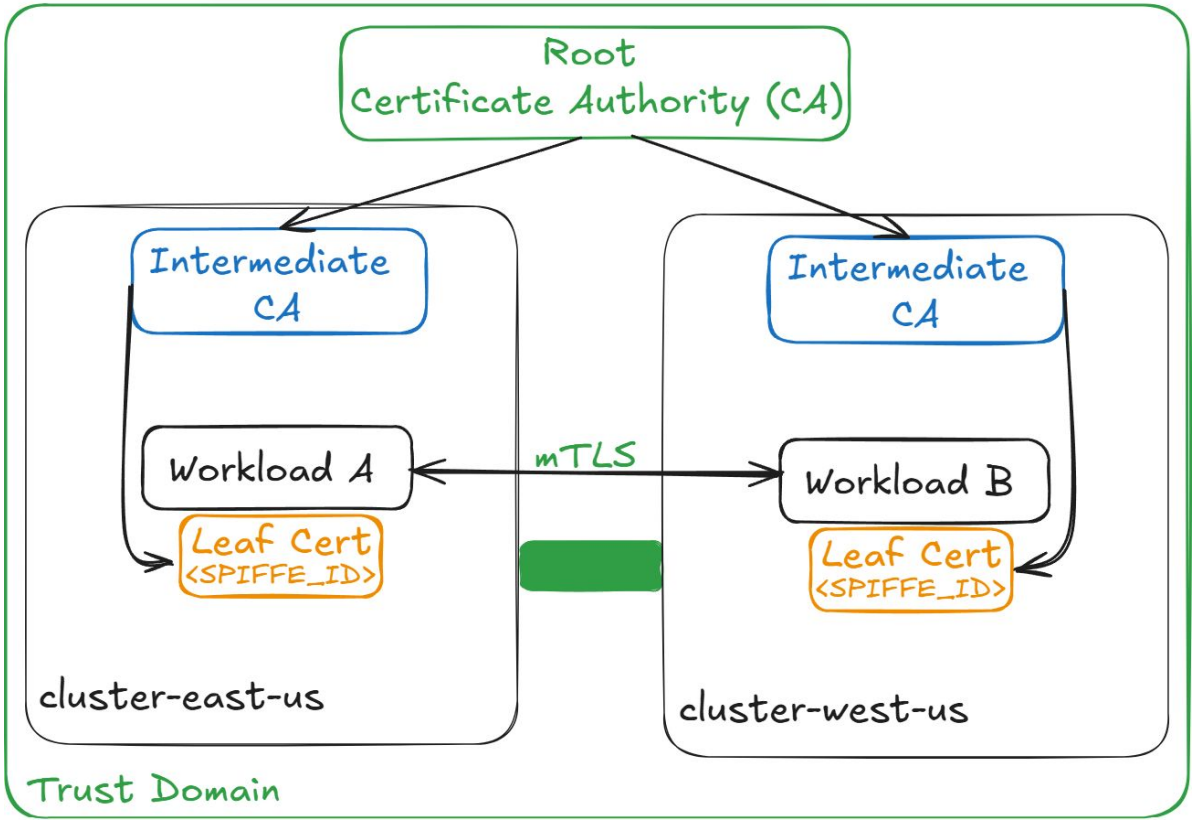
Multi-Cluster: Cloud Network Security Controls

- Peering or Private Link for private communication
- Multi-network for network isolation
  - Strict security requirements, regulations, compliance
- Encryption with VPN Gateways / Transit Gateways
- Firewalls and network security rules
  - East-West gateways
  - API Server

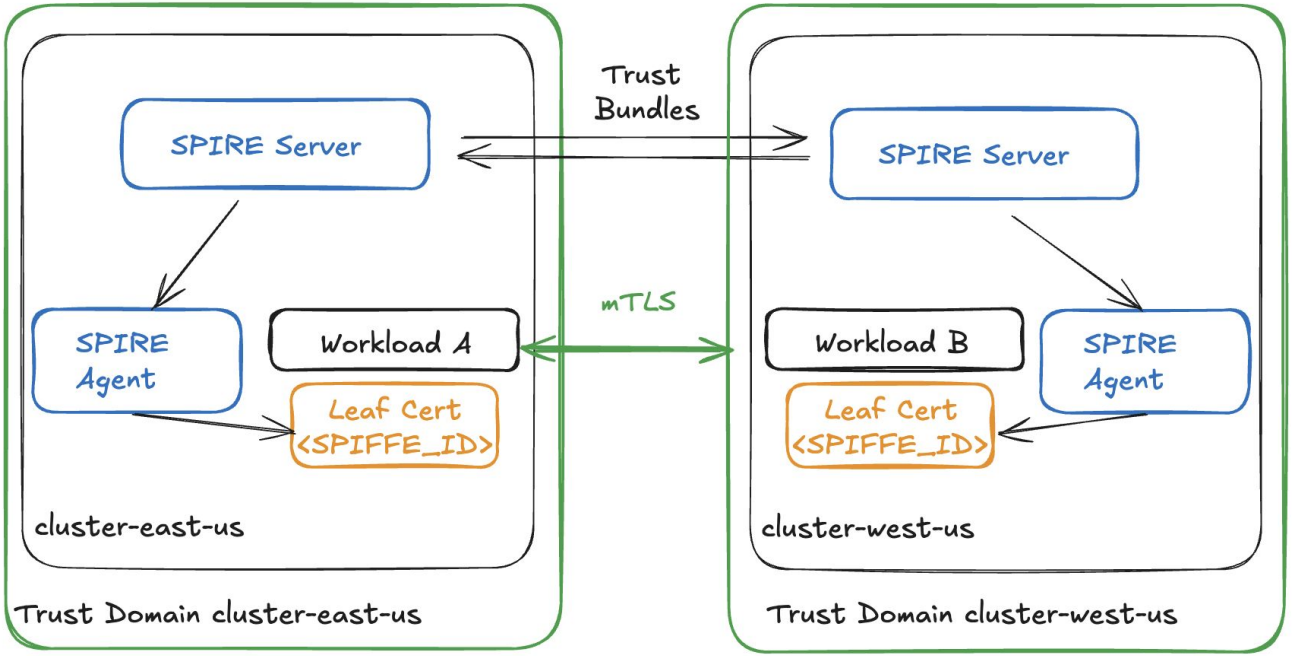
Multi-Cluster Network Policy



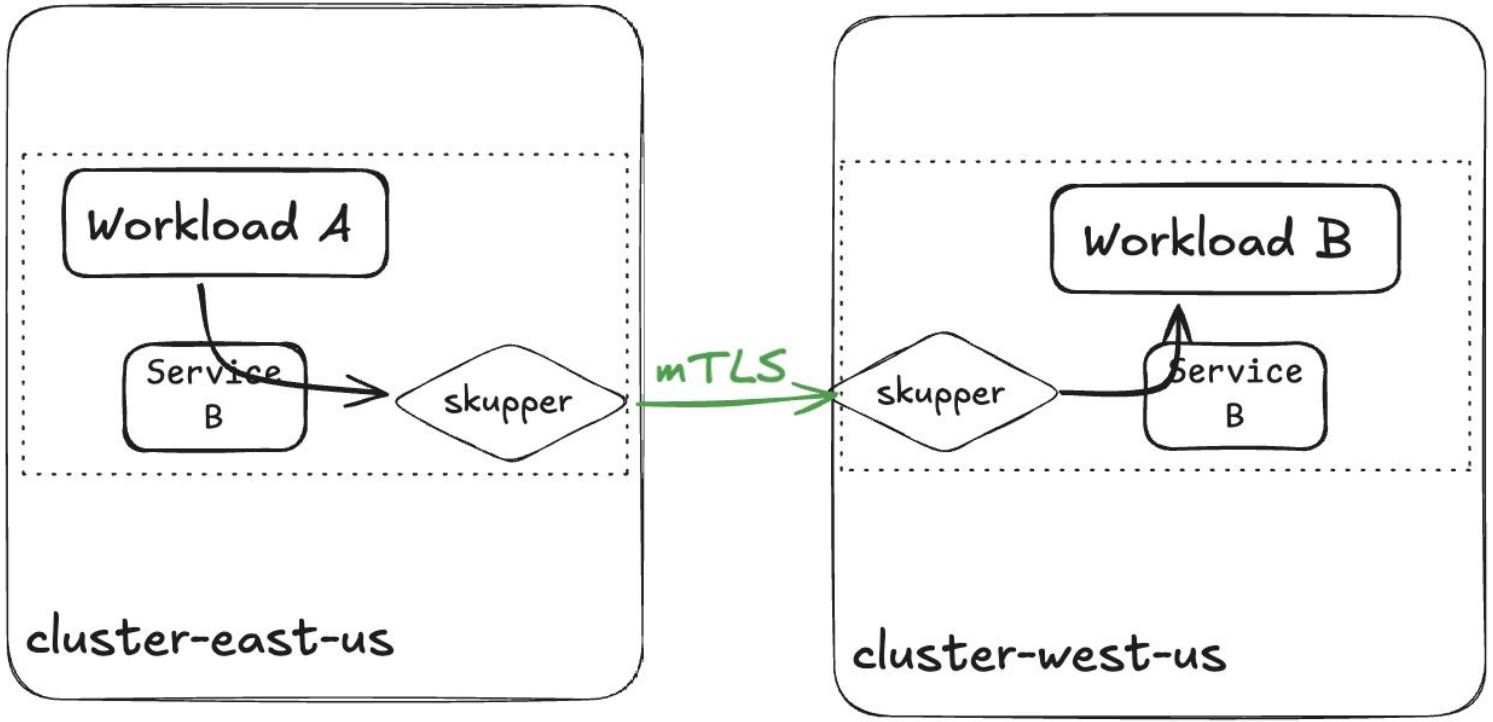
Multi-Cluster Security: Trust Domains and PKI



Multi-Cluster Security: Trust Domains and PKI



Multi-Cluster Security: Skupper mTLS



Multi-Cluster Security: Caveats and Best-Practices

- Secure API Server Access
- Selective Service Exposure
- Layered Security (Defense-In-Depth)
- Zero Trust Policies
- Consistent Policy Enforcement

Recommendations and Takeaways

Multi-Cluster Landscape: Factors to Consider

- Scale
- Requirements and features
  - Application architecture
    - How much east-west traffic?
  - Connectivity, discovery, security? All three in one?
  - Advanced routing and failover? Observability?
- Security model and PKI
- K8s native APIs

Multi-Cluster Solutions Comparison

	CNI-Based (Cilium, Calico)	Submariner	Skupper	Linkerd	Istio
Multi-Network Support	No	Yes*	Yes	Yes	Yes
Secure Tunnel Technology	IPSec, Wireguard	IPSec, Wireguard	TLS	TLS	TLS
Overall Security Posture	Medium	Medium	Medium	High	High
Complexity	Medium	Medium	Low	Medium-High	High
Feature-Set	Medium	Low-Medium	Low	High	Very High
Notes	Seamless annotation on K8s service for global load balancing and service discovery.	MCS API integration with Lighthouse. GlobalNet can handle overlapping CIDR. Multi-network requires public node IP or Gateway LoadBalancer mode (experimental).	Unencrypted traffic between Pods and Skupper router.	Label on K8s service and service mirroring for global load balancing and service discovery.	Offers various deployment models and numerous features. GitOps, upcoming Ambient Mesh multi-cluster, can streamline.

Final Thoughts and Takeaways

- **Prioritize Essentials**
  - Focus on connectivity, service discovery, and security as core building blocks for multi-cluster networking
- **Align with Business Needs and Requirements**
  - Tailor your multi-cluster strategy to meet your organization's specific needs and operational requirements
- **Empower Platform Engineering**
  - Leverage platform engineering to **simplify complexity** and **enforce operational standards** across clusters

Additional Resources

Seamless Multi-Cloud Kubernetes - KubeCon Europe 2024:
https://www.youtube.com/watch?v=D0KfsaqLc48

GKE Multi-Cluster Networking Guides:
https://cloud.google.com/kubernetes-engine/docs/concepts/multi-cluster-services

Multi-Cluster Kubernetes Networking - Are We There Yet? KCD NY 2024:
https://www.youtube.com/watch?v=ll9nYifMnjg

Google Open Source - MCS API Series:
https://learnkubernetes.withgoogle.com/multicluster-services-api-series

Understanding Multi-Cluster Connectivity Options - ONE Summit 2022:
https://www.youtube.com/watch?v=T--DgE9BUxo

Simplifying Multi-Cluster Kubernetes:
https://www.cncf.io/blog/2021/04/12/simplifying-multi-clusters-in-kubernetes/

5 Solutions for Multi-Cluster Communication in Kubernetes:
https://oilbeater.com/en/2024/05/24/five-kubernetes-multicluster-network/

KubeCon CloudNativeCon
North America 2024

Thanks!