KubeCon

CloudNativeCon

THE LINUX FOUNDATION

OPEN SOURCE SUMMIT

AI_dev

Open Source GenAI & ML Summit

China 2024

KubeCon
CloudNativeCon
THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
AI_dev
Open Source GenAI & ML Summit
China 2024
ZTM-based Multicluster
Implementing Seamless Connectivity and Service Governance

Introduction

Xiaohui Zhang

Senior Architect/Technical Evangelist at Flomesh

Senior programmer, CNCF Ambassador, LFAPAC Open Source Evangelist, Microsoft MVP. Years of practical experience in microservices and cloud-native, the main work involves microservices, containers, Kubernetes, DevOps, etc.

Agenda

- Discussion of Mutlicluster
- Multicluster Service API
- Introduce Zero Trust Mesh
- Mutlicluster Traffic Management with ZTM

Multicluster

Drivers of Multicluster

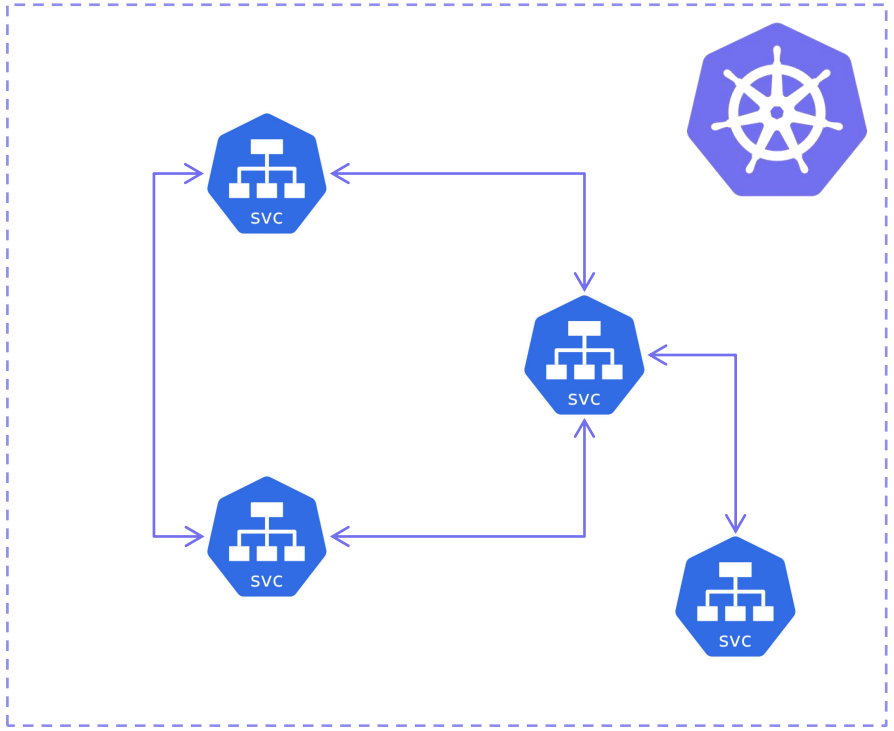
- Geographic distribution and latency optimization
- Scale and resource isolation
- Multi-cloud and hybrid cloud strategies
- Fault isolation and disaster recovery
- Seamless upgrades reduce risk

Location

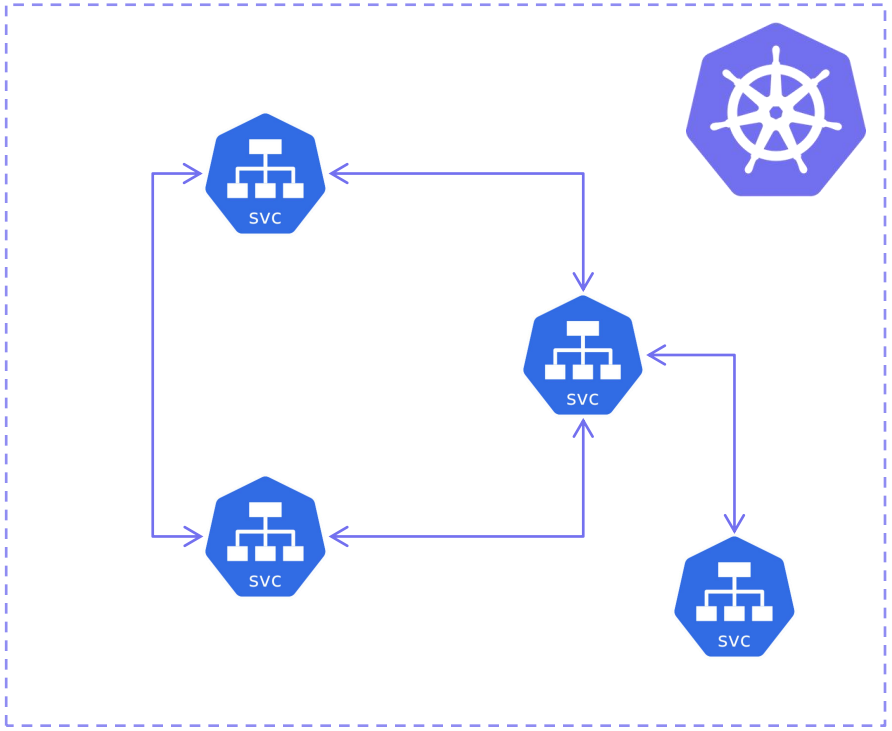
Isolation

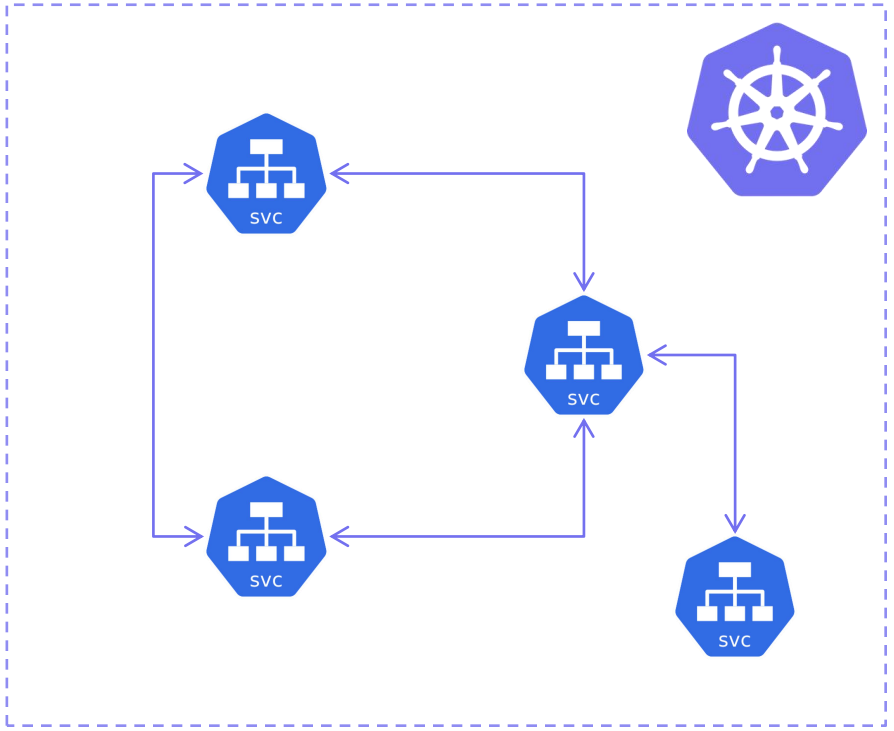
Reliability

Single Cluster

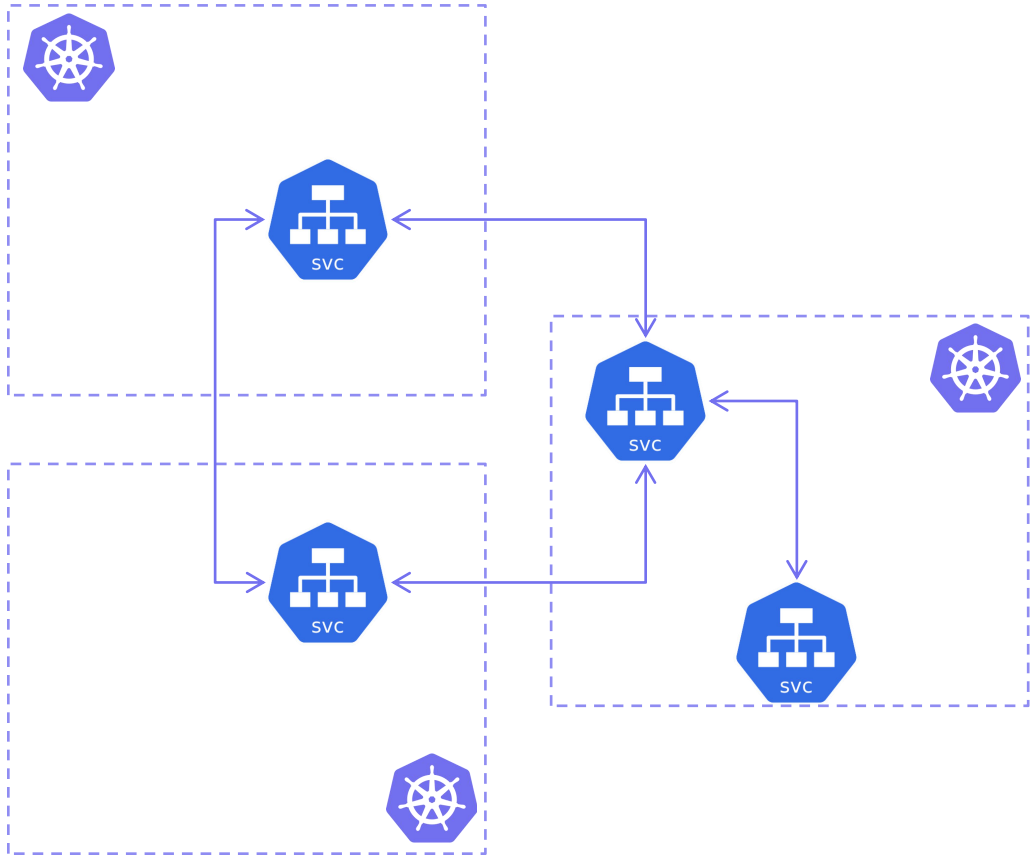


Old Multi Cluster



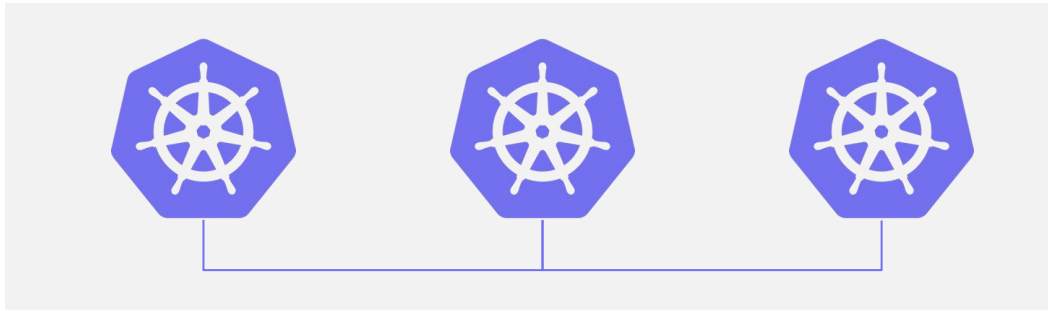


New Multi Cluster

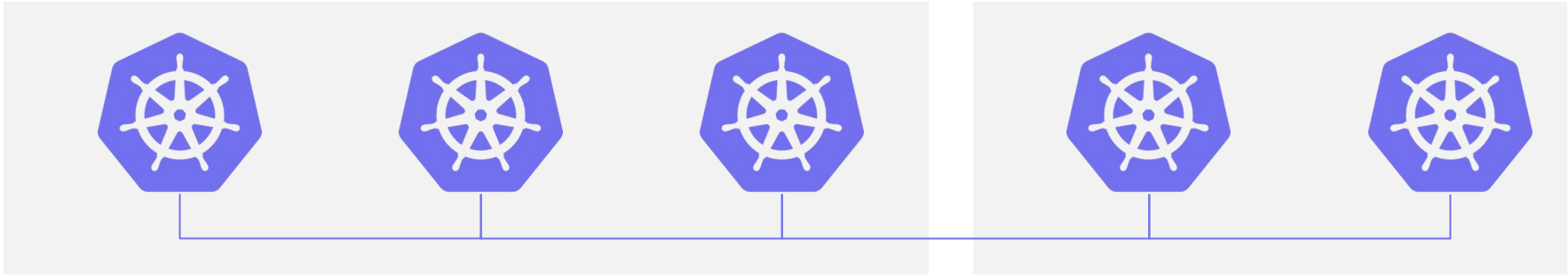


MultiCluster Mode

MutliCluster in Single DC

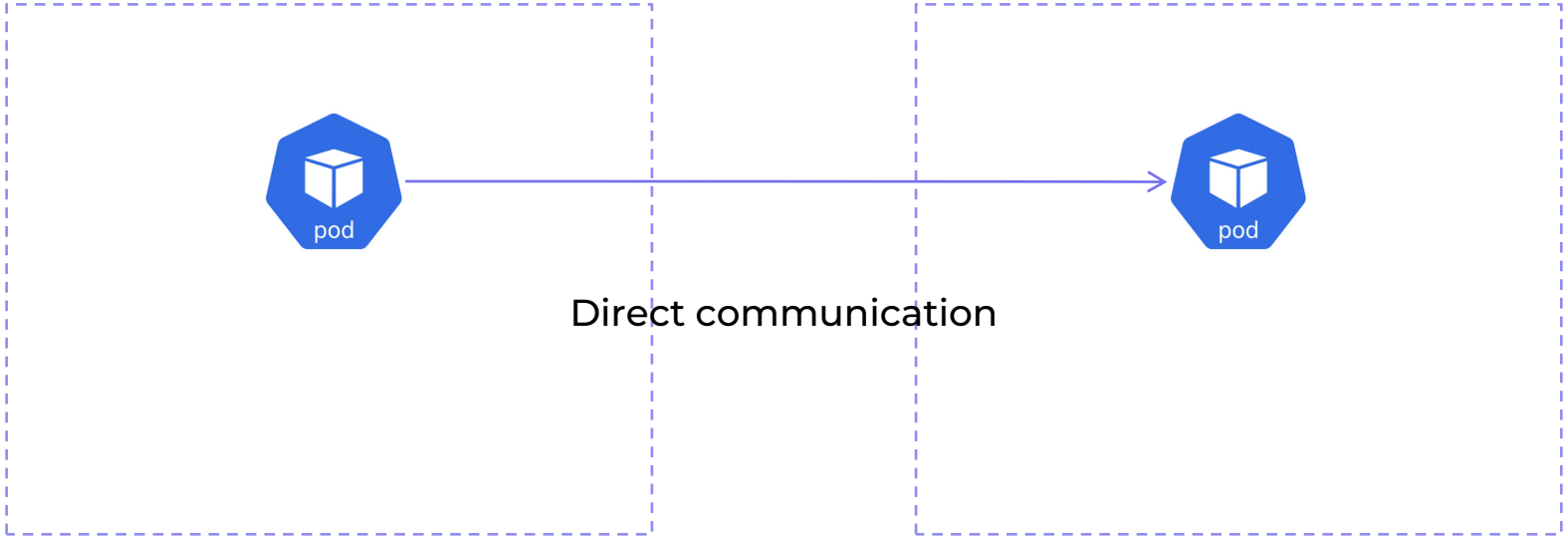


MutliCluster in Multi DCs



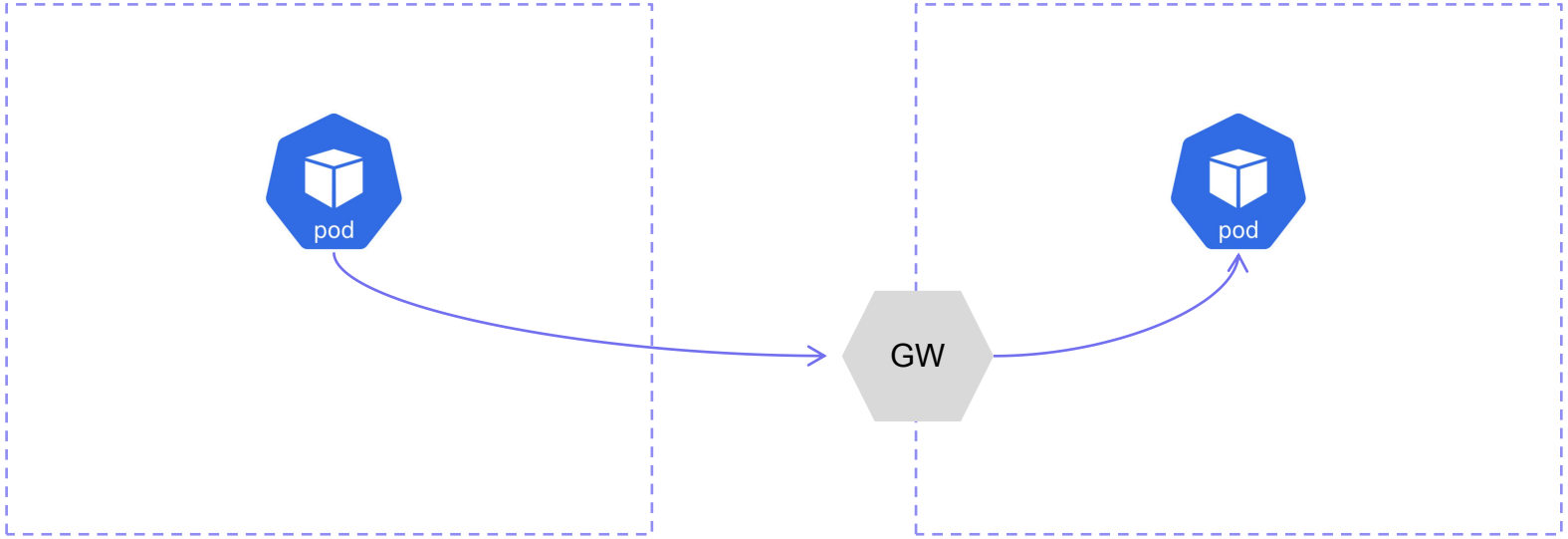
Flat Network: Pod-to-Pod Multicluster

- Each pod has a unique IP address across clusters.
- All clusters have different CIDR range.



Hierarchical network: Gateway-based Multicluster

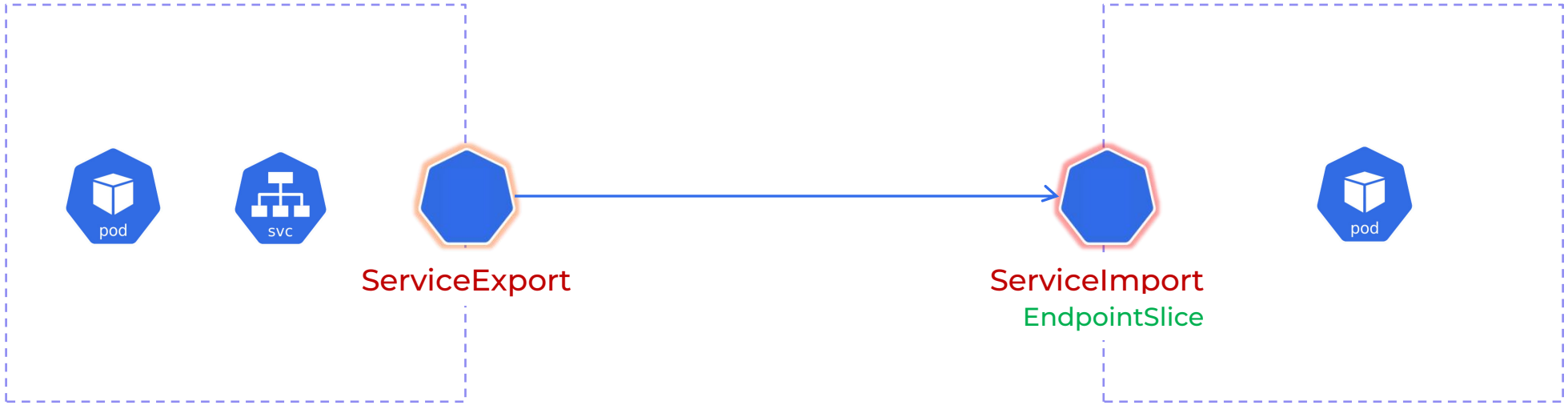
- Handle traffic through multicluster gateways.
- Gateways are IP-reachable.
- Introduce slight latency, but noticeable.



Multicluster Service API

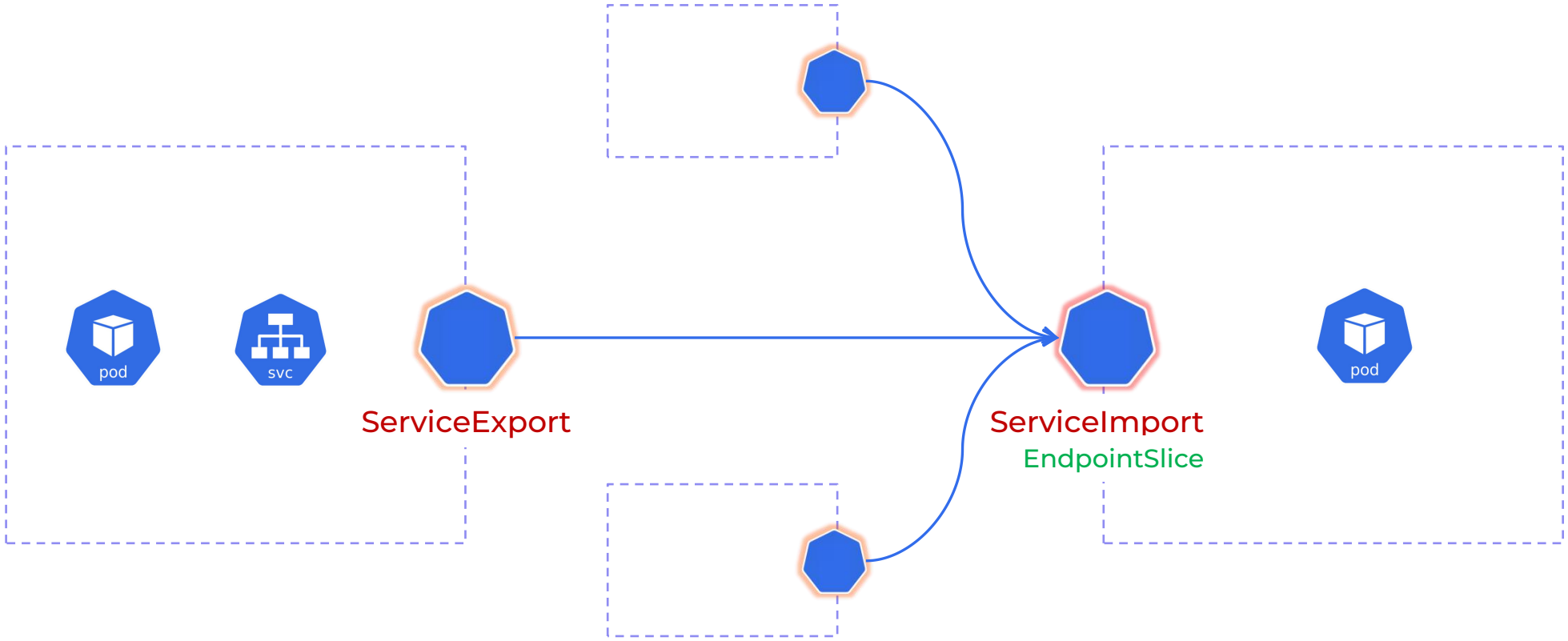
Multicluster Service API

MCS API is the bridge of multiclsuter service discovery.



Multicluster Service API

MCS API is the bridge of multiclsuter service discovery.



Zero Trust Mesh

ZTM: Zero Trust Mesh

- Open source network infrastructure software
- For running a decentralized network
- Built upon HTTP/2 tunnels
- Run on any sort of IP networks such as LANs, containerized networks and the Internet, etc.

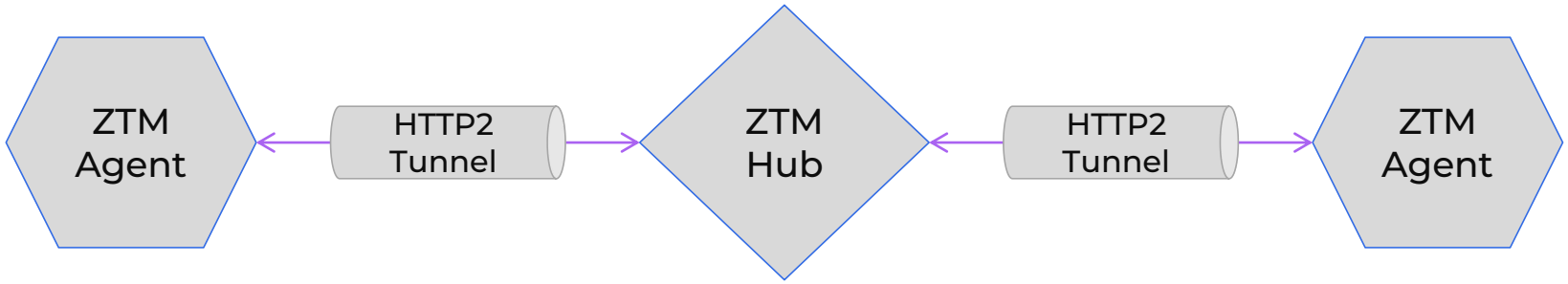
https://github.com/flomesh-io/ztm

Core Capabilities

- Network connectivity across Internet gateways and firewalls
- TLS-encrypted communication channels
- Certificate-based authentication and access control
- Decentralized application publishing and deployment
- Decentralized file discovery and data sharing

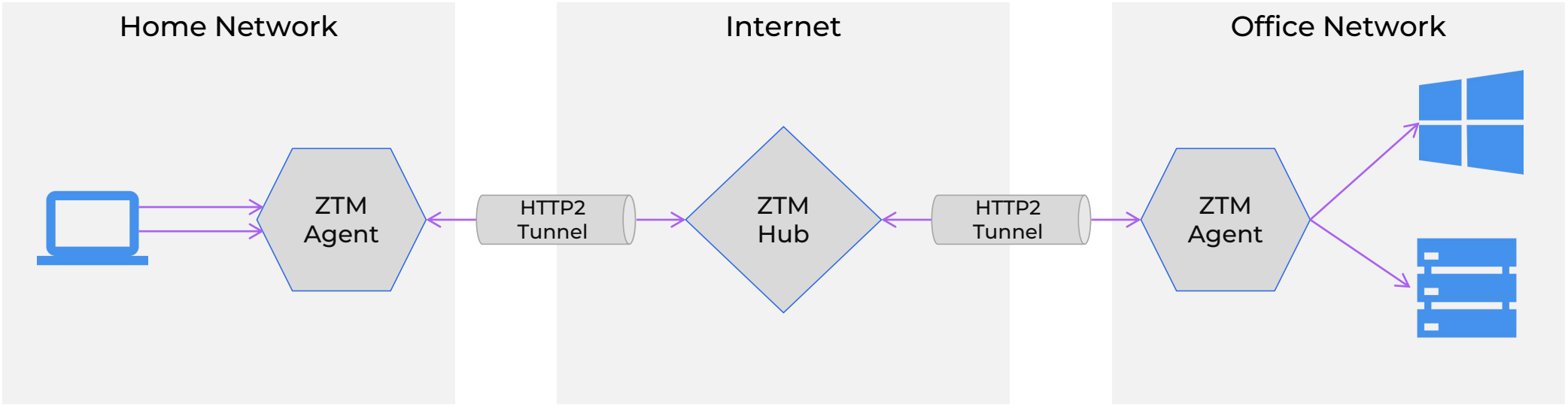
ZTM Architecture

- ZTM Agent: Deployed on devices connecting to the Zero Trust Network, it initiates encrypted tunnels to securely forward traffic to the ZTM Hub.
- ZTM Hub: A distributed access point cluster that establishes encrypted tunnels with Agents, enabling secure, multi-point access and high availability.



ZTM App: zt-tunnel

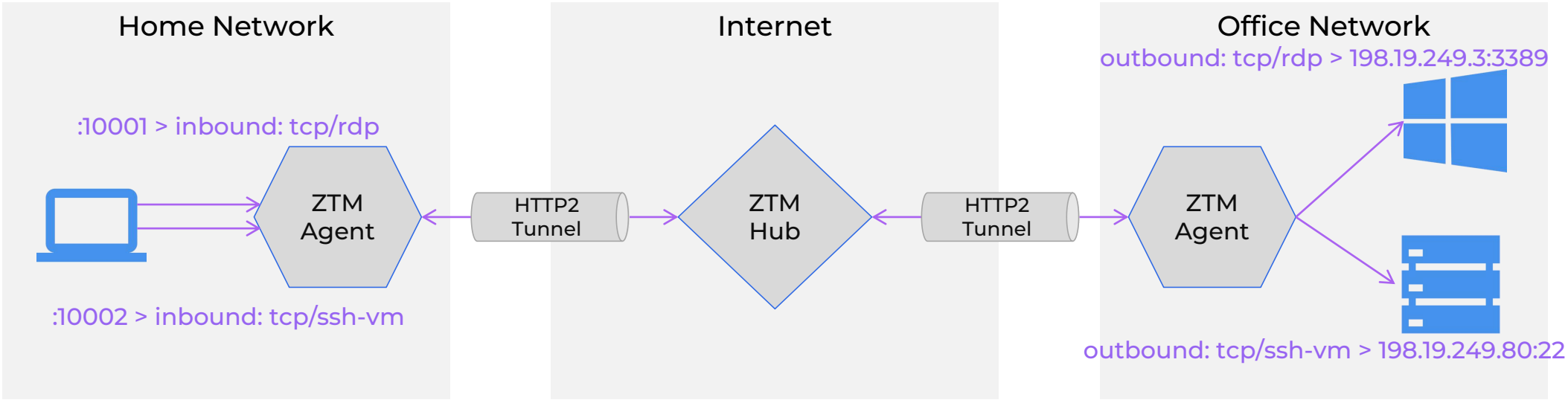
The zero-trust tunnel eliminates physical distance limitations, allowing you to access your devices from anywhere.



ZTM App: zt-tunnel

Concepts:

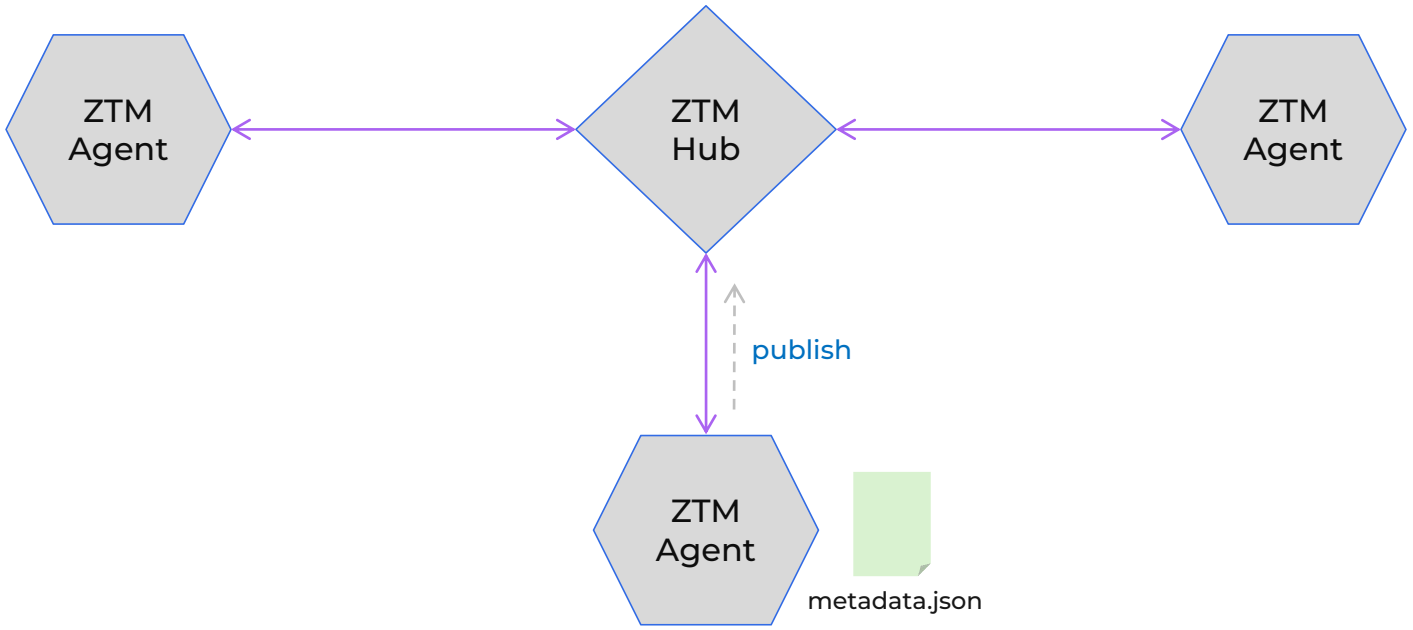
- outbound: tunnel's exit
- inbound: tunnel's entrance



ZTM FS: Distributed File System

Sync file to all agents in mesh network.

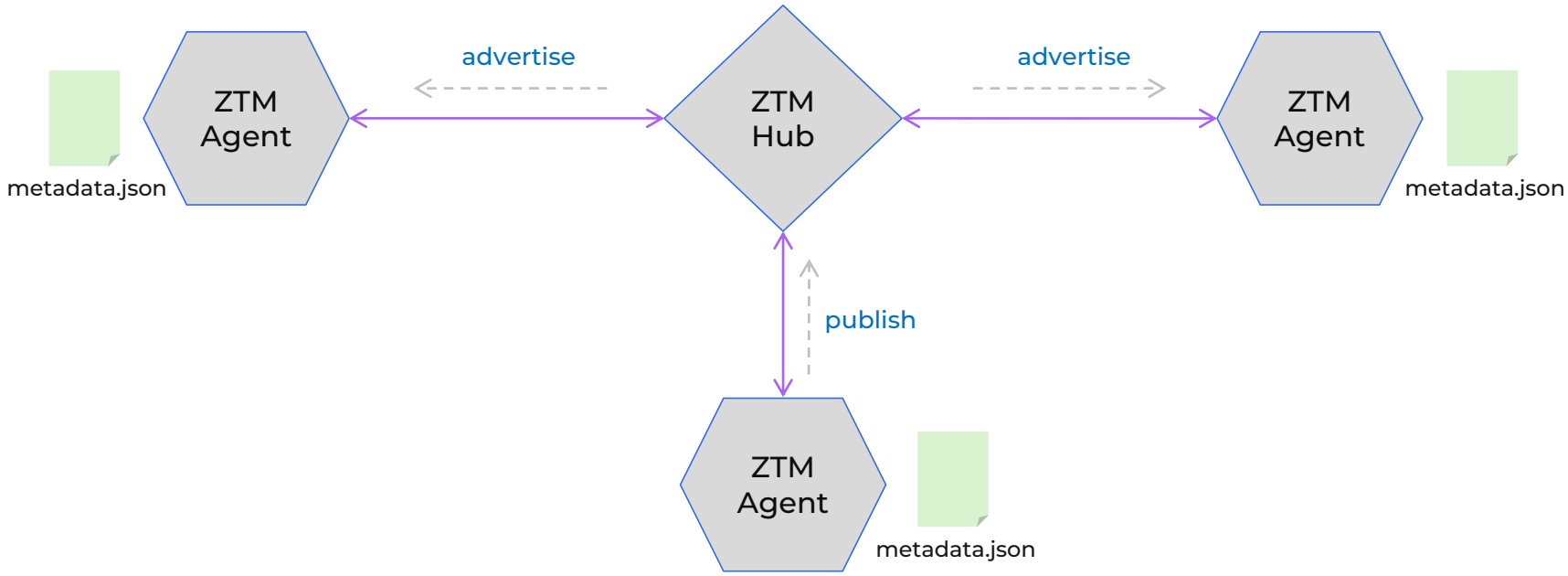
$ ztm publish file /path/metadata.json



ZTM FS: Distributed File System

Sync file to all agents in mesh network.

$ ztm publish file /path/metadata.json

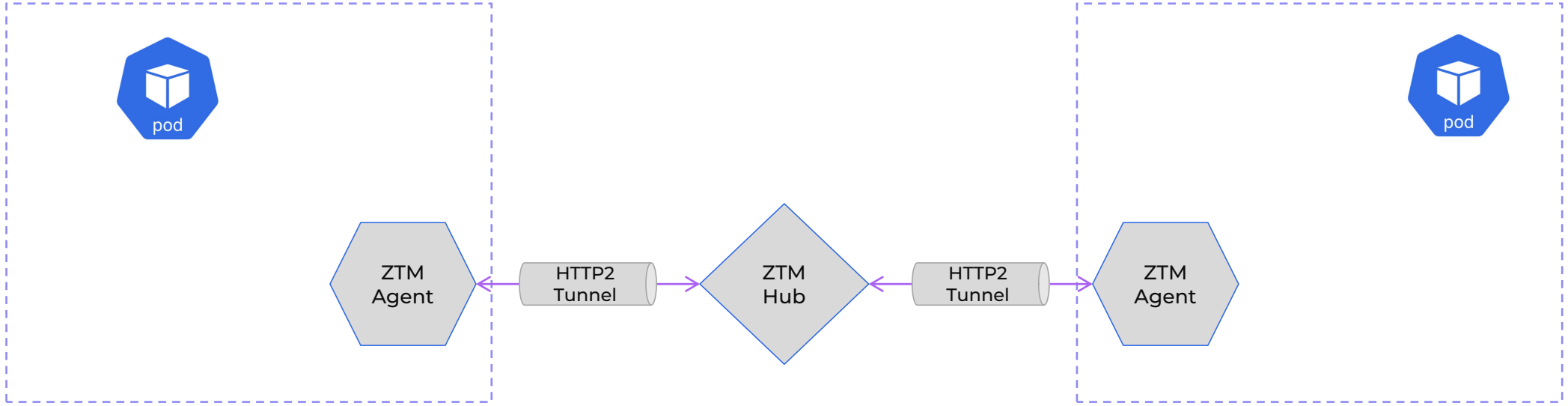


ZTM-based Multicluster

zt-tunnel in Multicluster

Connectivity

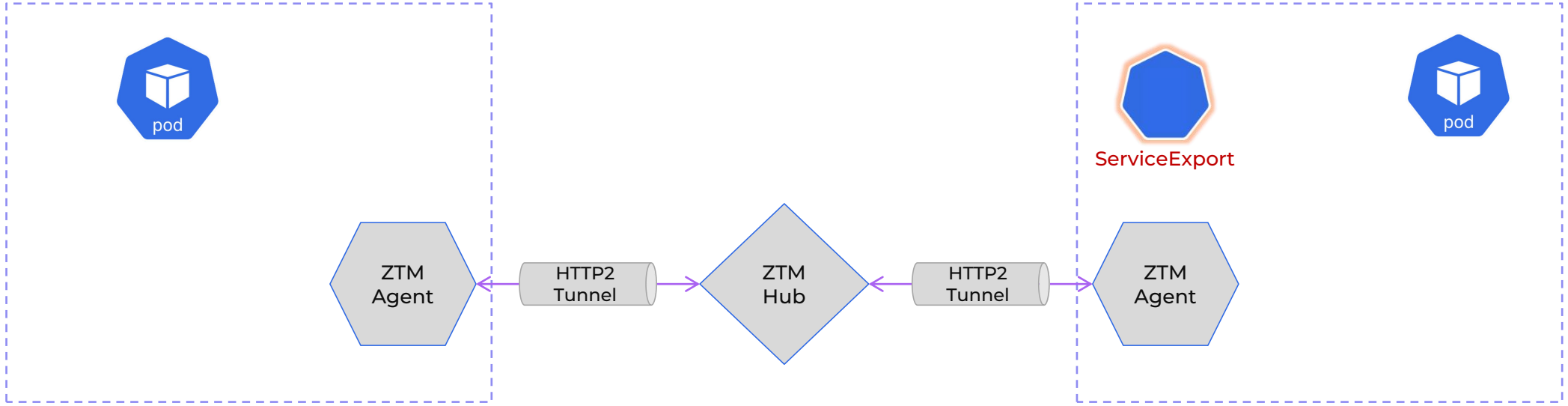
- Secure HTTP2 tunnel
- IP-reachable (Cluster/Pod) NOT necessary



KubeCon CloudNativeCon THE LINUX FOUNDATION OPEN SOURCE SUMMIT AI_dev China 2024

Multicluster service discovery

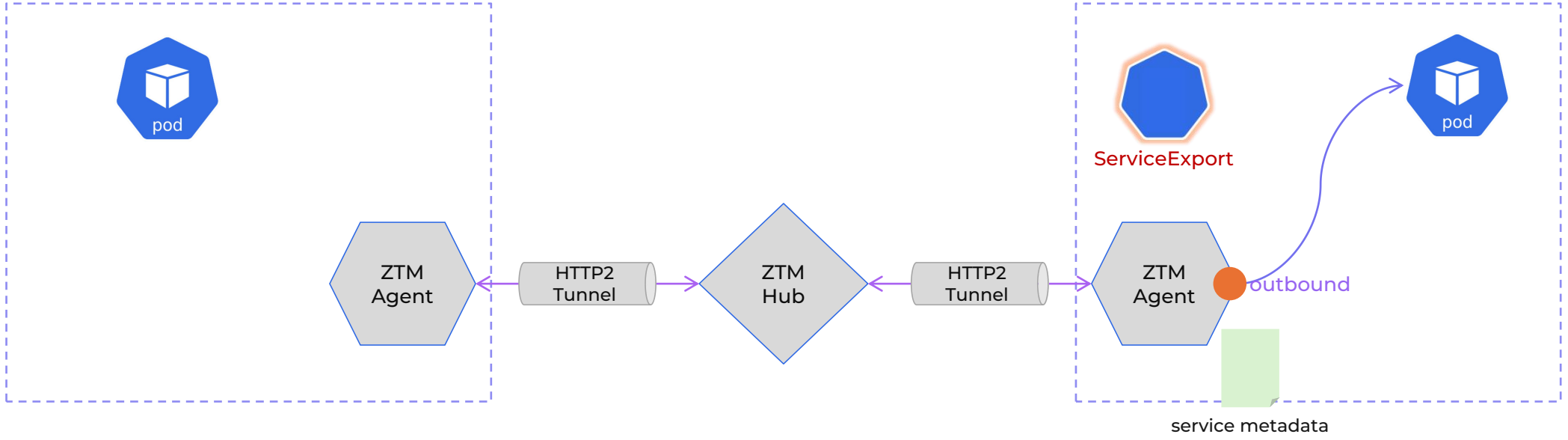
- Compatible with the MCS API*



zt-tunnel in Multicluster

Multicluster service discovery

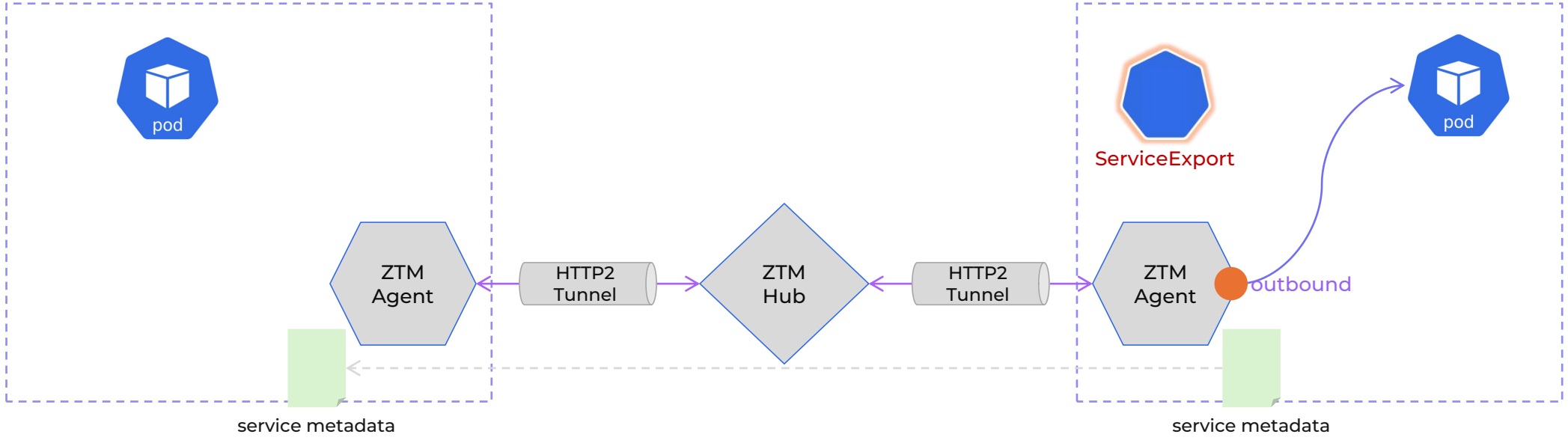
- Compatible with the MCS API*



zt-tunnel in Multicluster

Multicluster service discovery

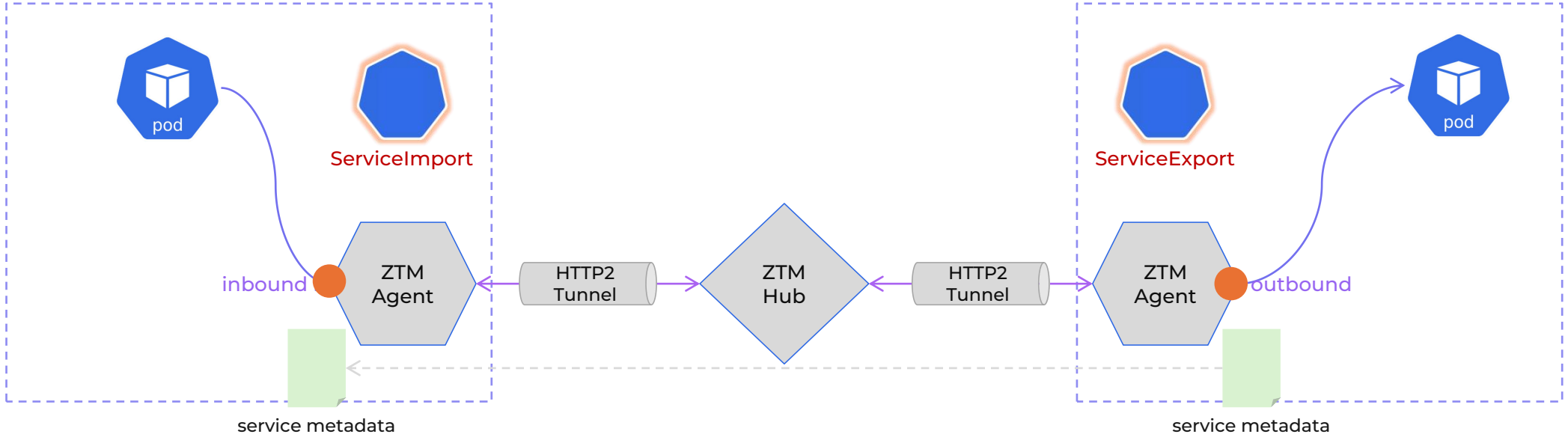
- Compatible with the MCS API*



zt-tunnel in Multicluster

Multicluster service discovery

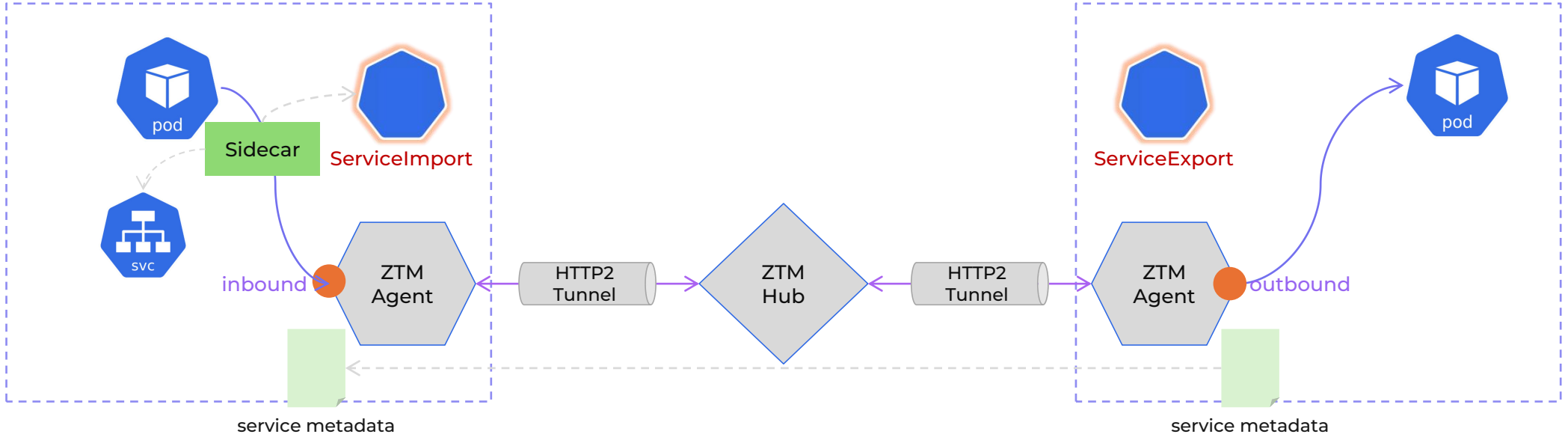
- Compatible with the MCS API*



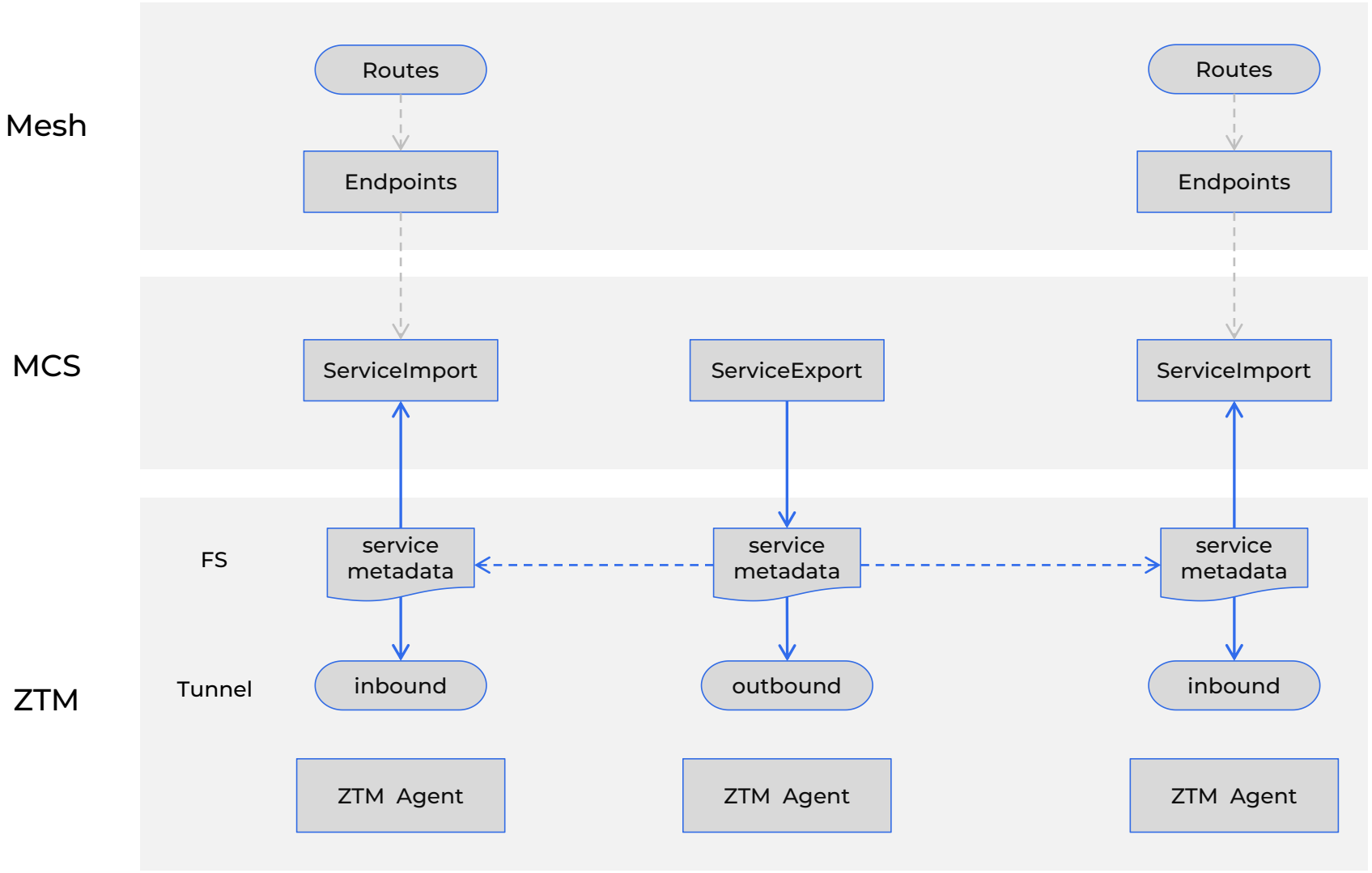
zt-tunnel in Multicluster

Multicluster service discovery

- Compatible with the MCS API*
- Interoperable with service mesh



Interoperate with service mesh



DEMO

https://github.com/cybwan/fsm-start-demo/tree/ztm

- Flomesh Service Mesh (FSM)
- Flomesh MCS API (L7-based)

Future

- ZTM Hub cluster support
- Official MCS API support
- Standlone ZTM controller

Join US

blog.flomesh.io

Flomesh flomesh.io

github.com/flomesh-io

flomesh-io.slack.com