Current scope of submariner (1)

k8s cluster #1

k8s cluster #2

k8s cluster #3

- Connects k8s clusters by connecting pod networks.
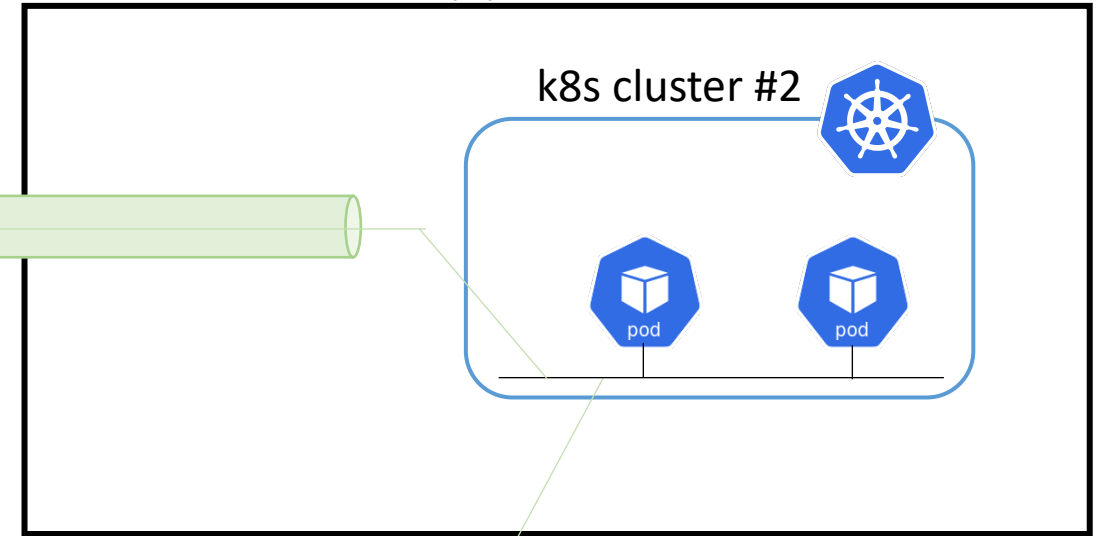
Current scope of submariner (2)

Cloud (A)

Cloud (B)

k8s cluster #1

k8s cluster #2

pod pod

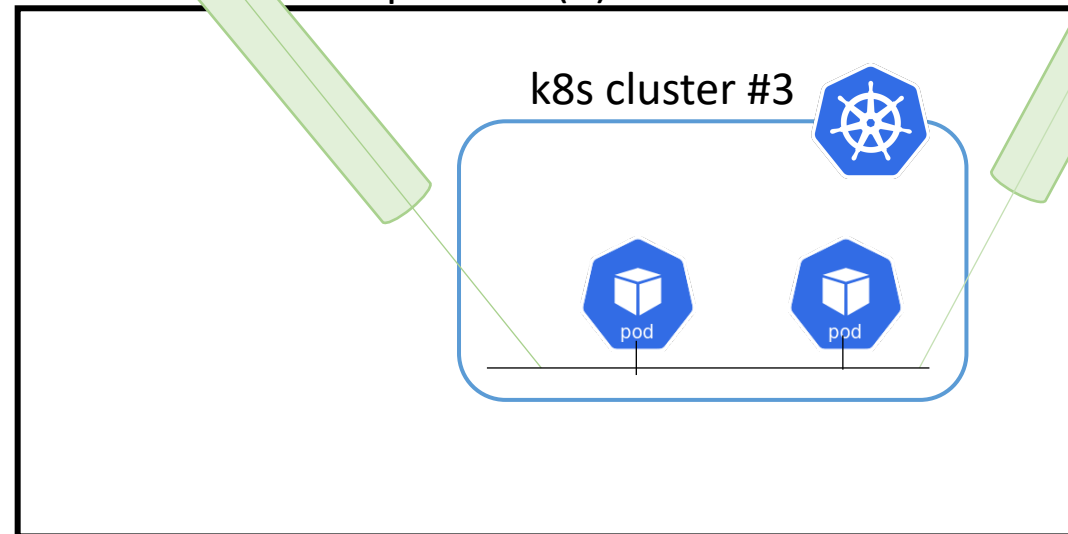pod pod
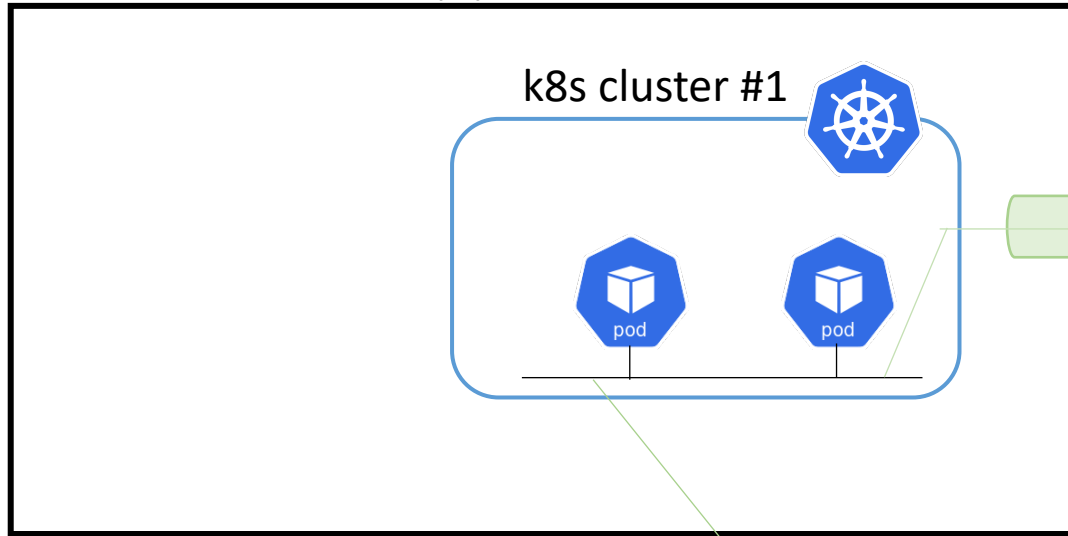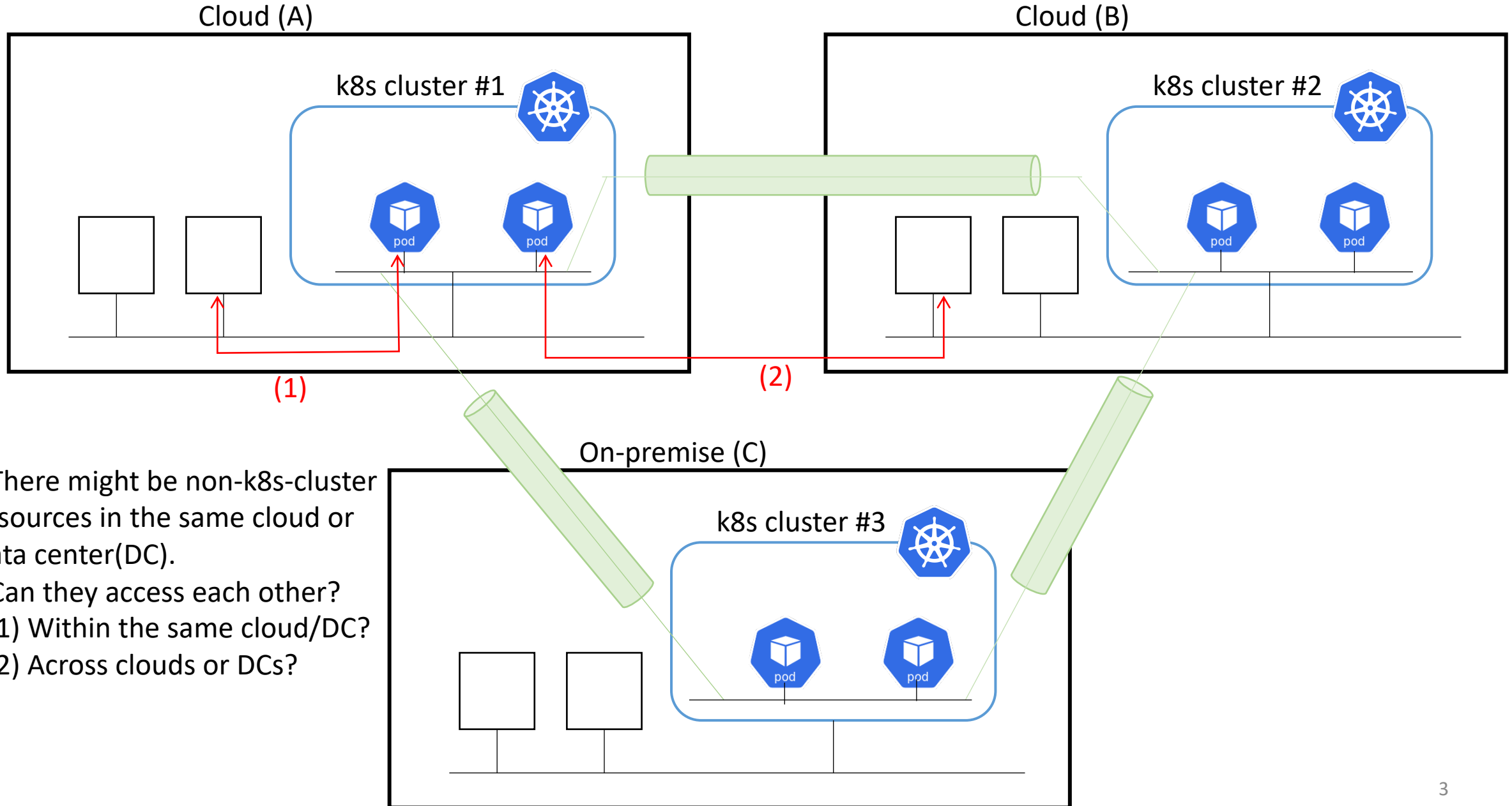
On-premise (C)

- Connects k8s clusters by connecting pod networks.
- k8s clusters can be across clouds and on-premises.

k8s cluster #3

pod pod

How about k8s-clusters and non-k8s-clusters?
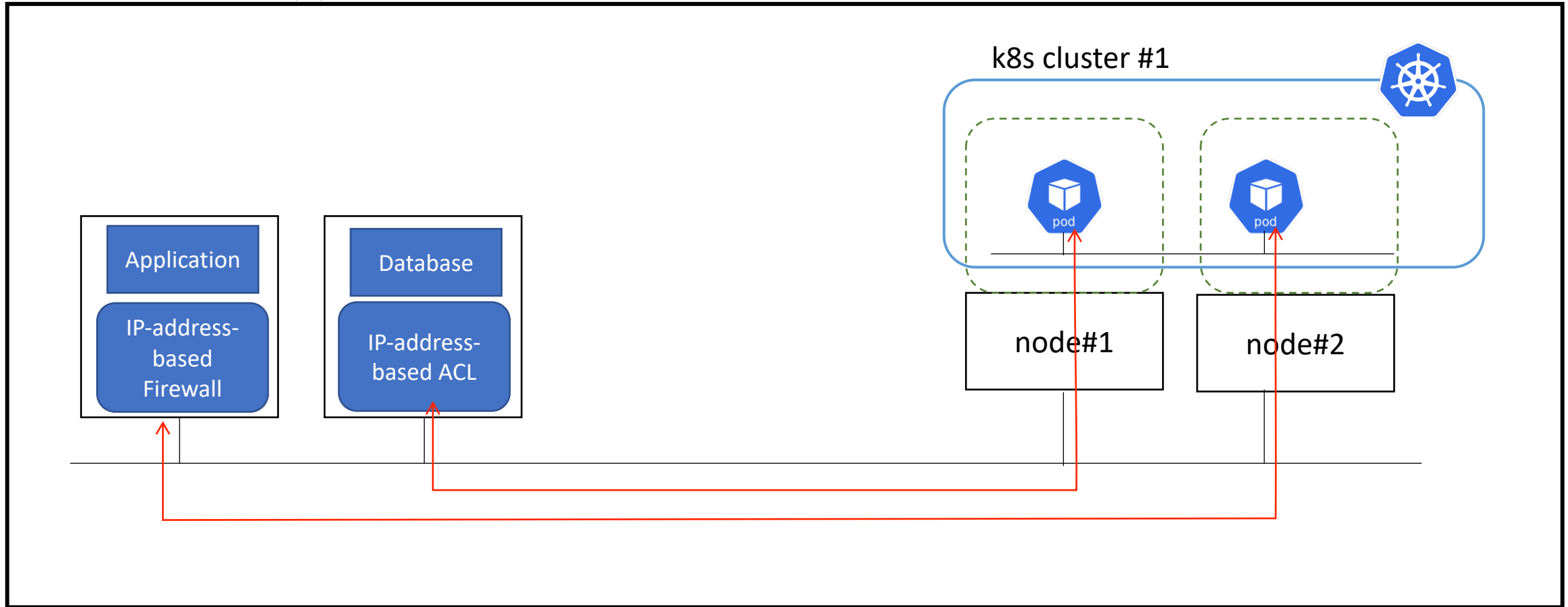

Cloud (A)

k8s cluster #1

(1)

Cloud (B)

k8s cluster #2

(2)

On-premise (C)

k8s cluster #3

- There might be non-k8s-cluster resources in the same cloud or data center(DC).
- Can they access each other?
  (1) Within the same cloud/DC?
  (2) Across clouds or DCs?

3

Even within the same cloud/DC, there's an issue

Cloud (A)

k8s cluster #1

Application

IP-address-based Firewall

Database

IP-address-based ACL

node#1

node#2

pod

pod

- PodIPs are not static.
- Some CNI implementation SNATs source IP to the node's IP when going out from k8s cluster.
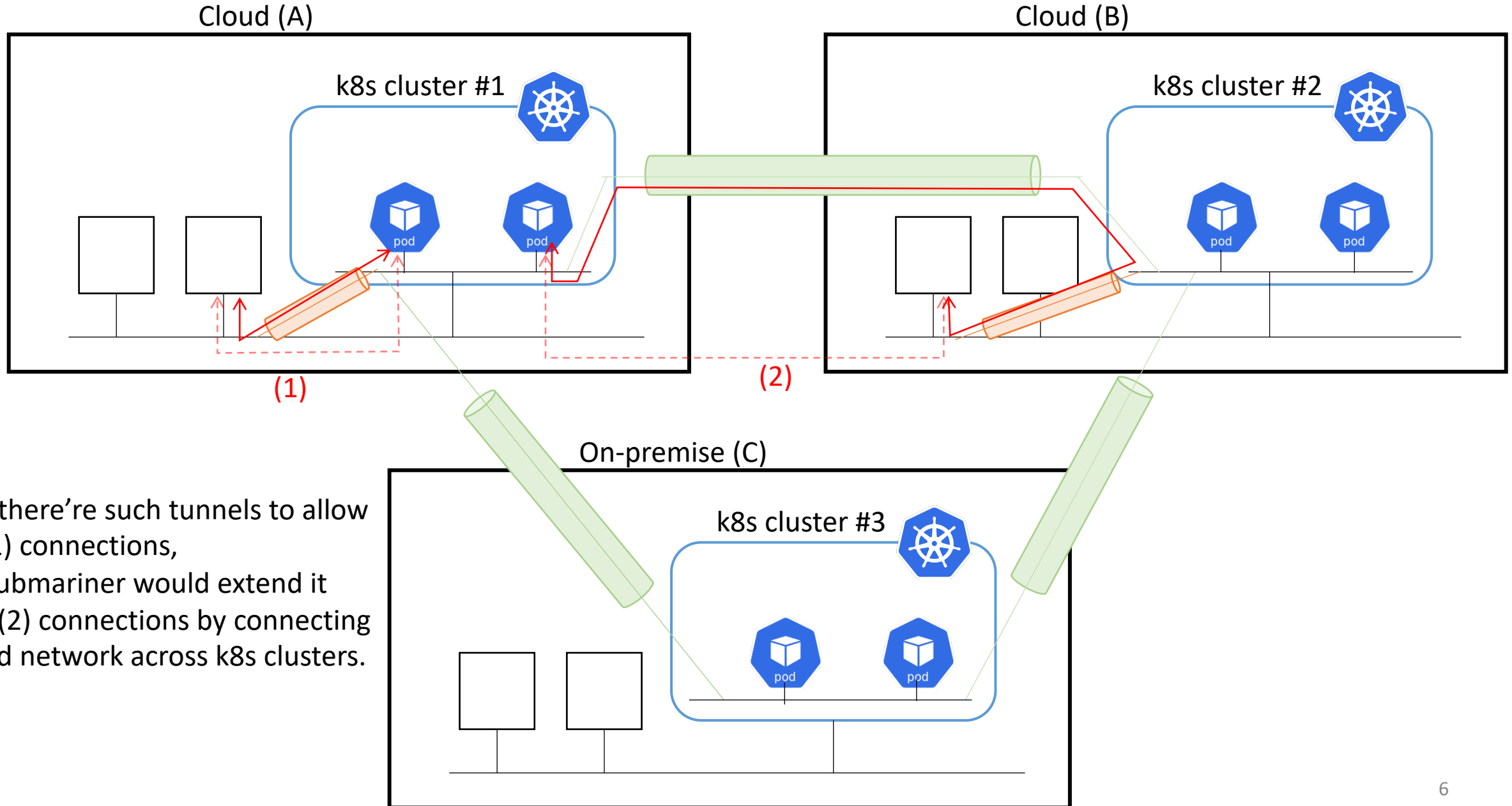=> IP address-based firewall and ACL will block the packets from k8s cluster.

Basic idea of solving issue within the same cloud/DC
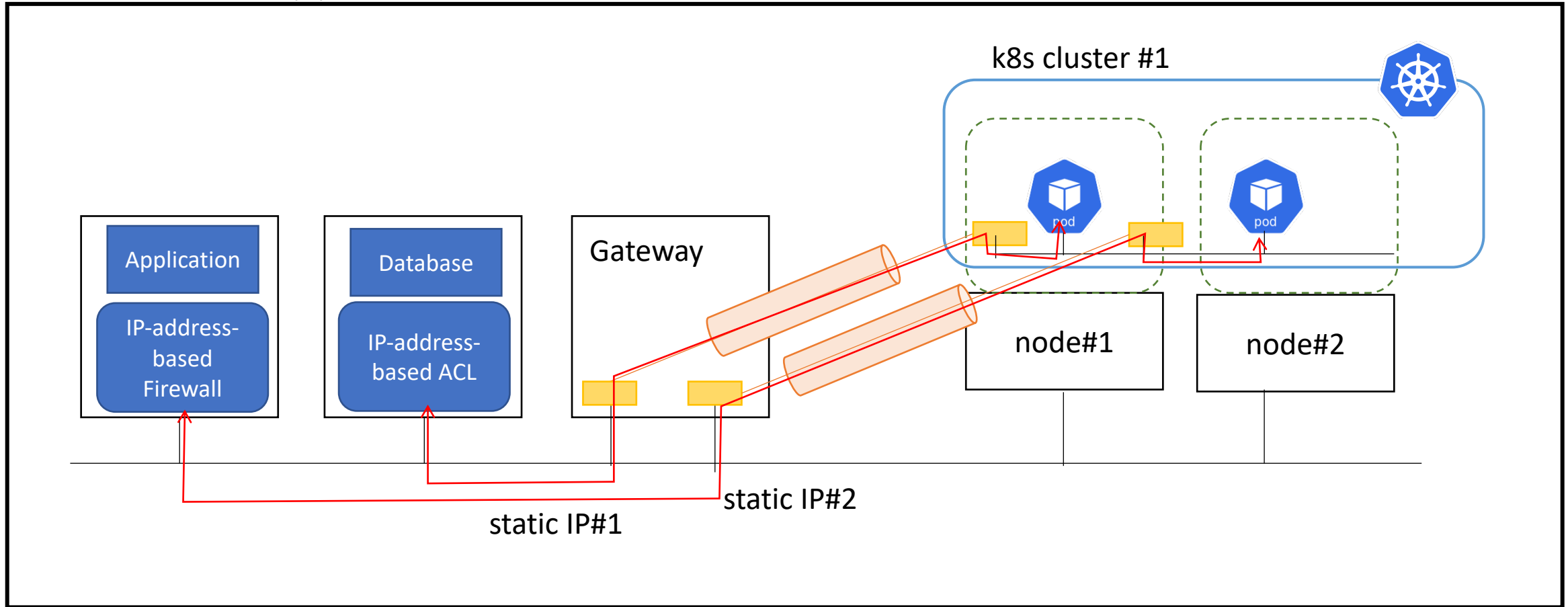
- Connect pod network to certain static IPs through tunnel.

Access across clouds/DC when there're such tunnels

Cloud (A)

Cloud (B)

k8s cluster #1

k8s cluster #2

(1)

(2)

On-premise (C)

-If there're such tunnels to allow
  (1) connections,
- Submariner would extend it
to (2) connections by connecting
pod network across k8s clusters.

k8s cluster #3

Current status

- Discussion in k8s community:
  - sig-network: Add egress-source-ip-support KEP
    https://github.com/kubernetes/enhancements/pull/1105

- PoC implementation:
  - mkimuram/k8s-ext-connector
    https://github.com/mkimuram/k8s-ext-connector
  - How it works:
    - connection from k8s to external server:
      https://github.com/kubernetes/enhancements/pull/1105#issuecomment-571694606
    - connection from external server to k8s:
      https://github.com/kubernetes/enhancements/pull/1105#issuecomment-575424609