Leveraging Shared VPCs

Janani Ravi
CO-FOUNDER, LOONYCORN

www.loonycorn.com

Overview

Shared VPCs span multiple projects

One designated host project

Several designated service projects

Delegation of administrative responsibilities to Service Project Admins

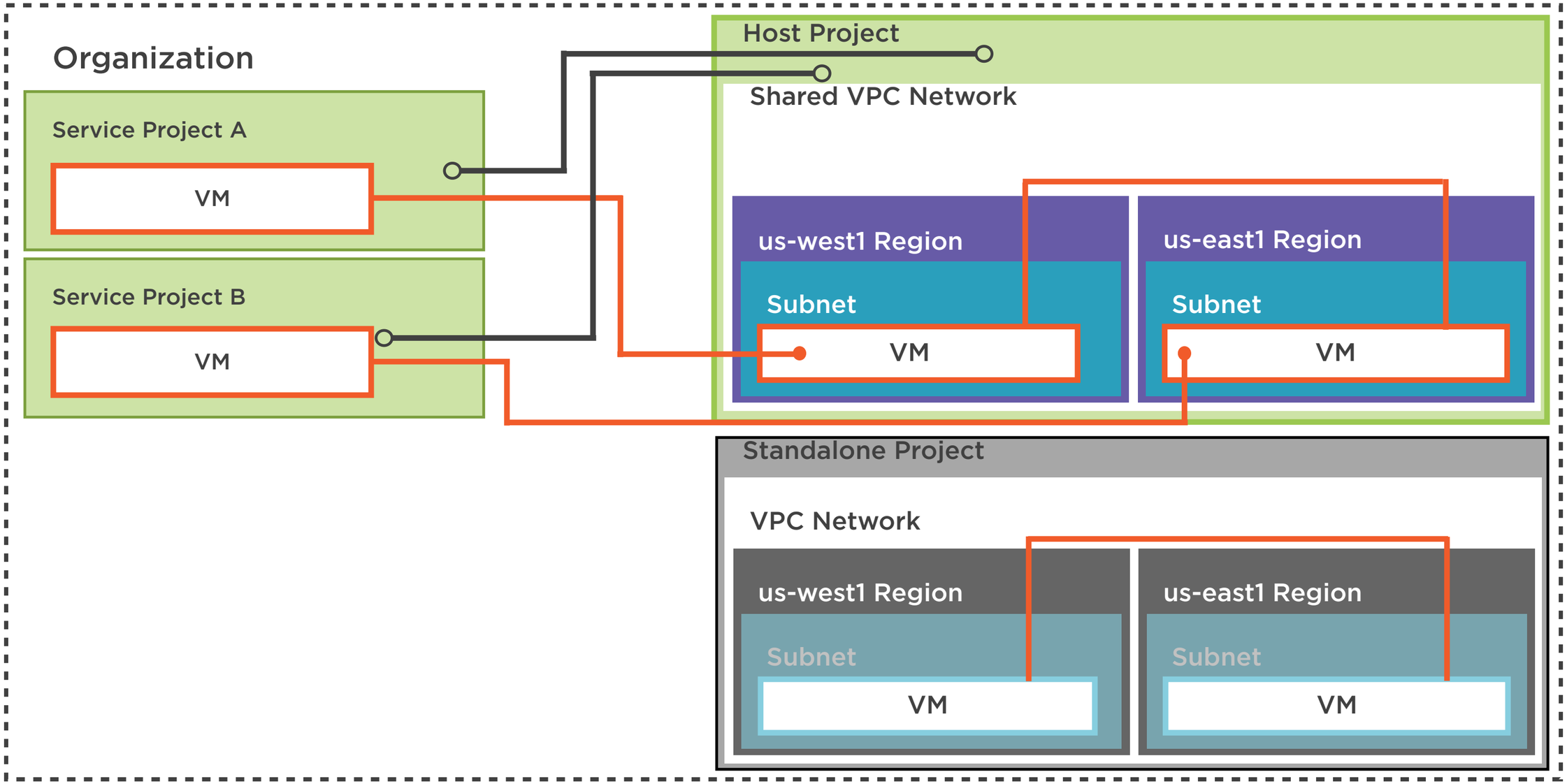
Least privilege for network administration, auditing and access control

Shared VPC

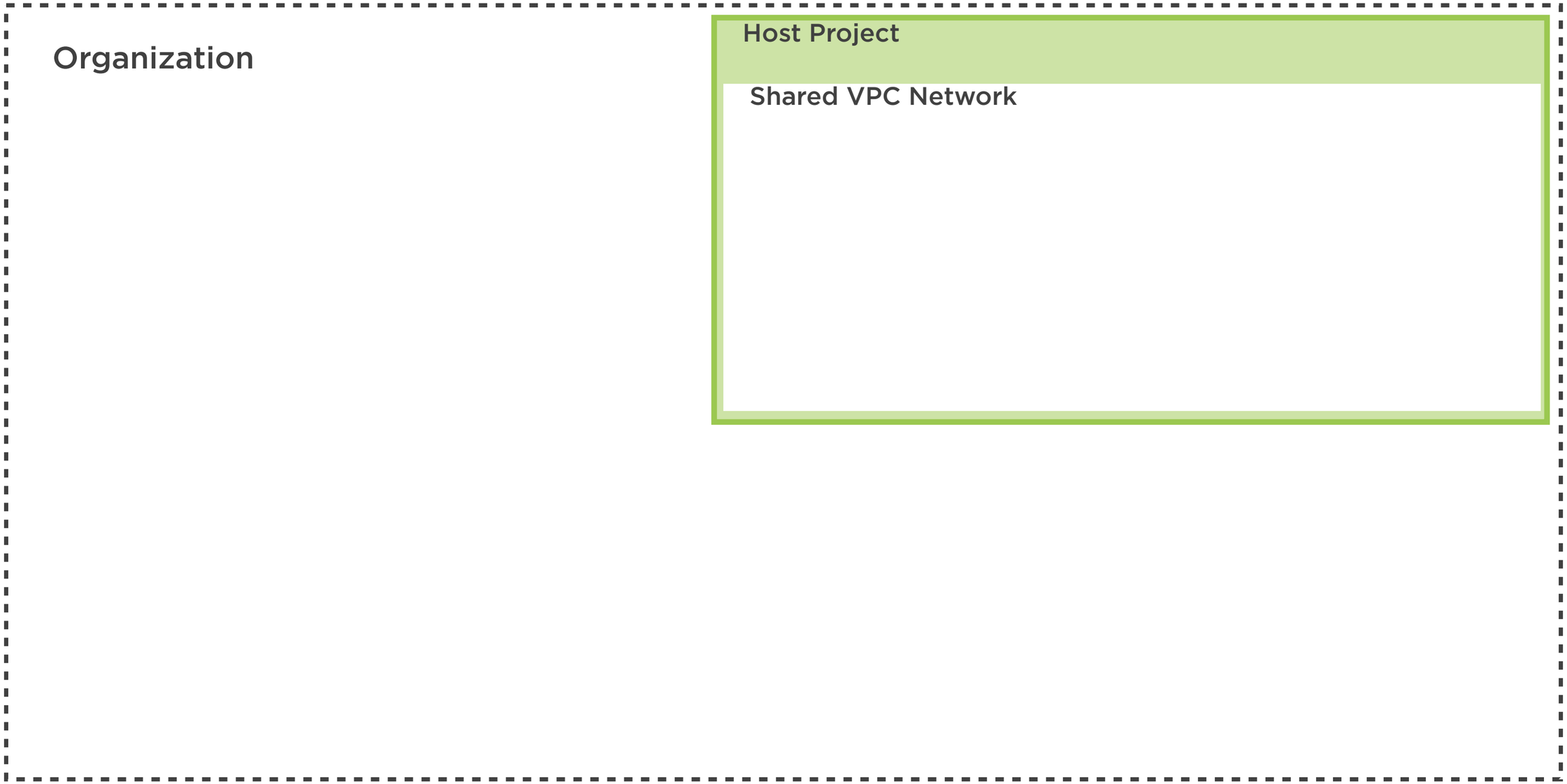
Shared VPC

A mechanism to connect resources from multiple projects into a single VPC network

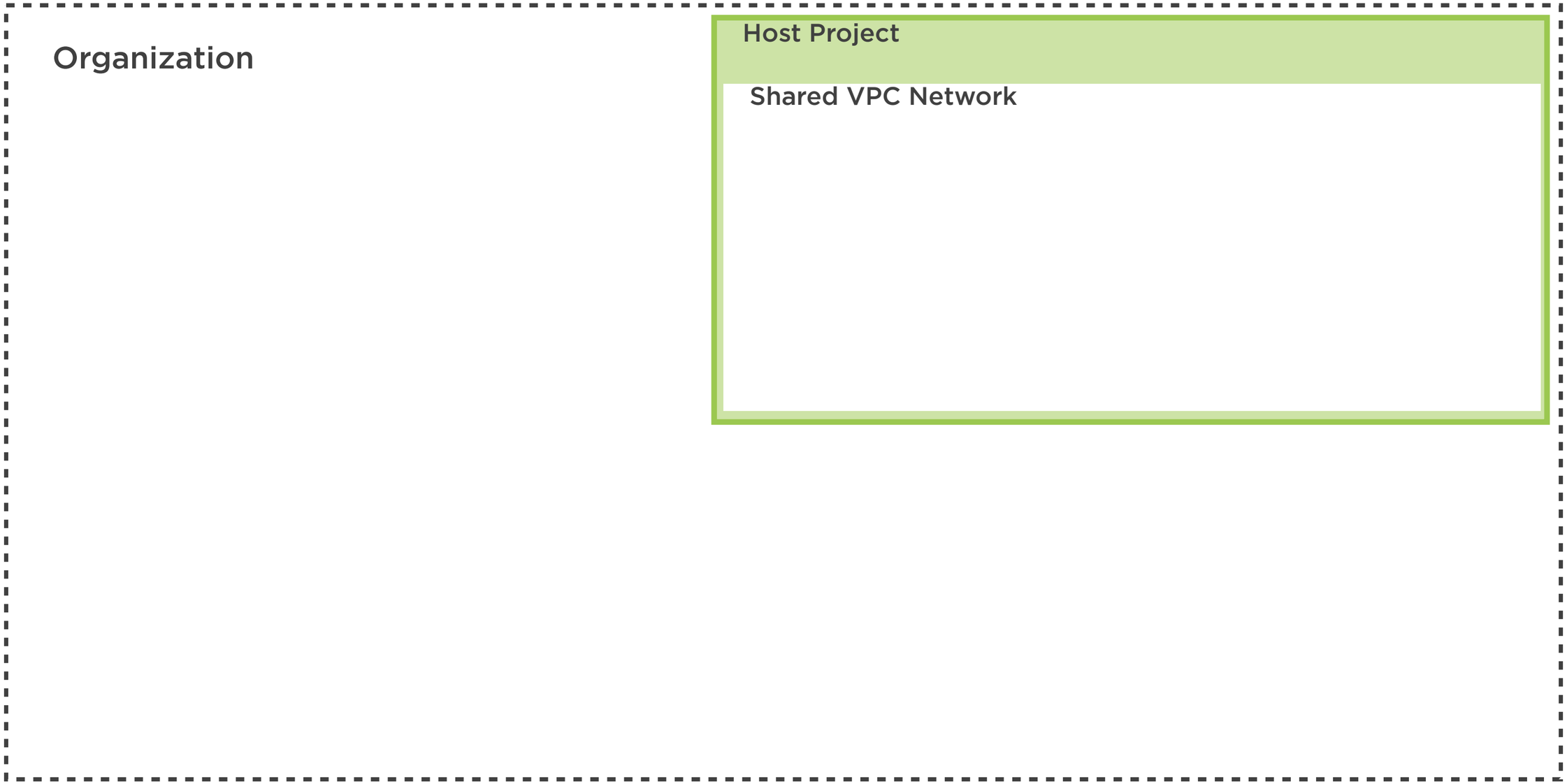
Shared VPC


Organization
Service Project A
VM
Service Project B
VM
Host Project
Shared VPC Network
us-west1 Region
Subnet
VM
us-east1 Region
Subnet
VM
Standalone Project
VPC Network
us-west1 Region
Subnet
VM
us-east1 Region
Subnet
VM

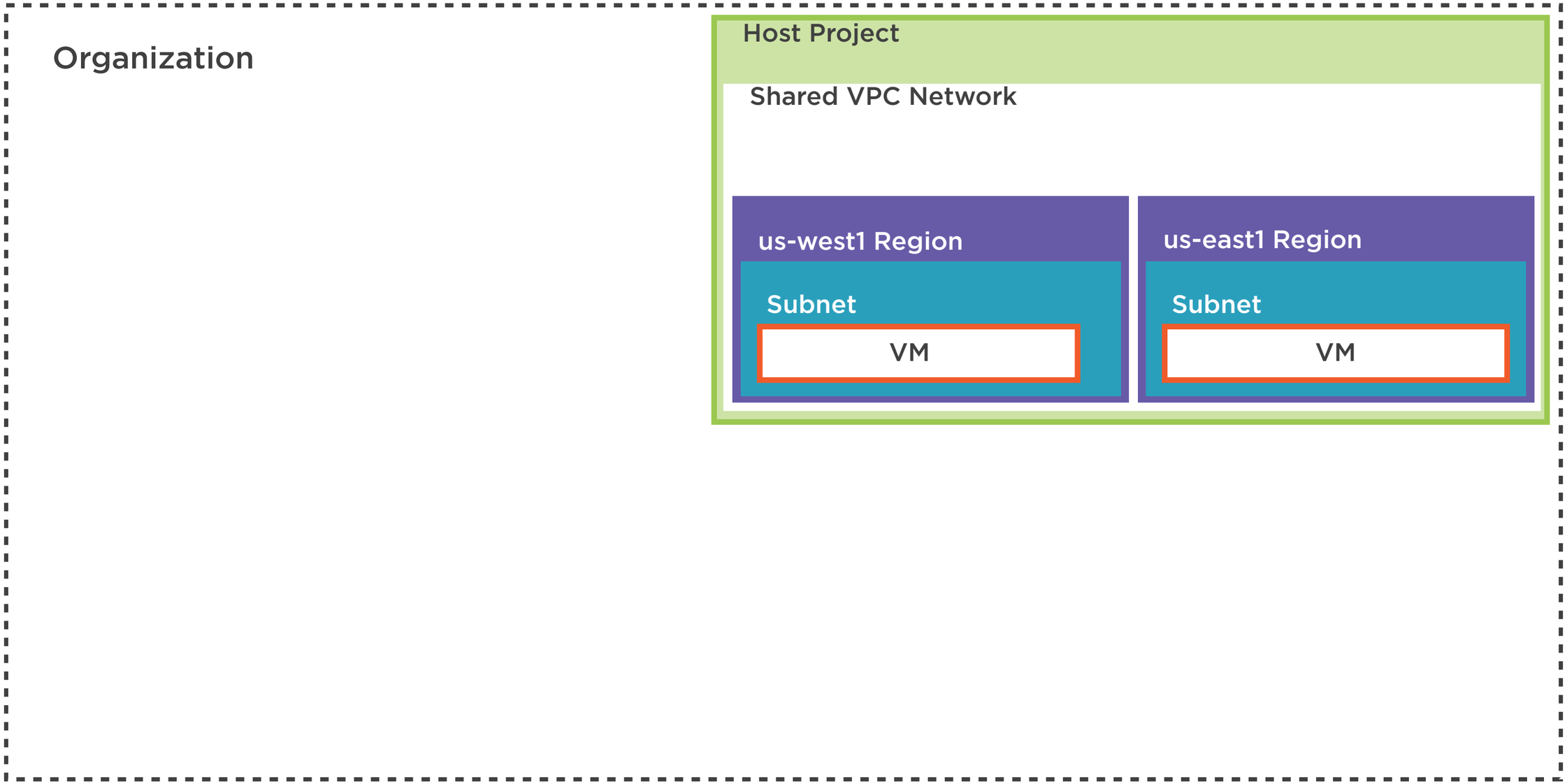
Host Project Creates Shared VPC



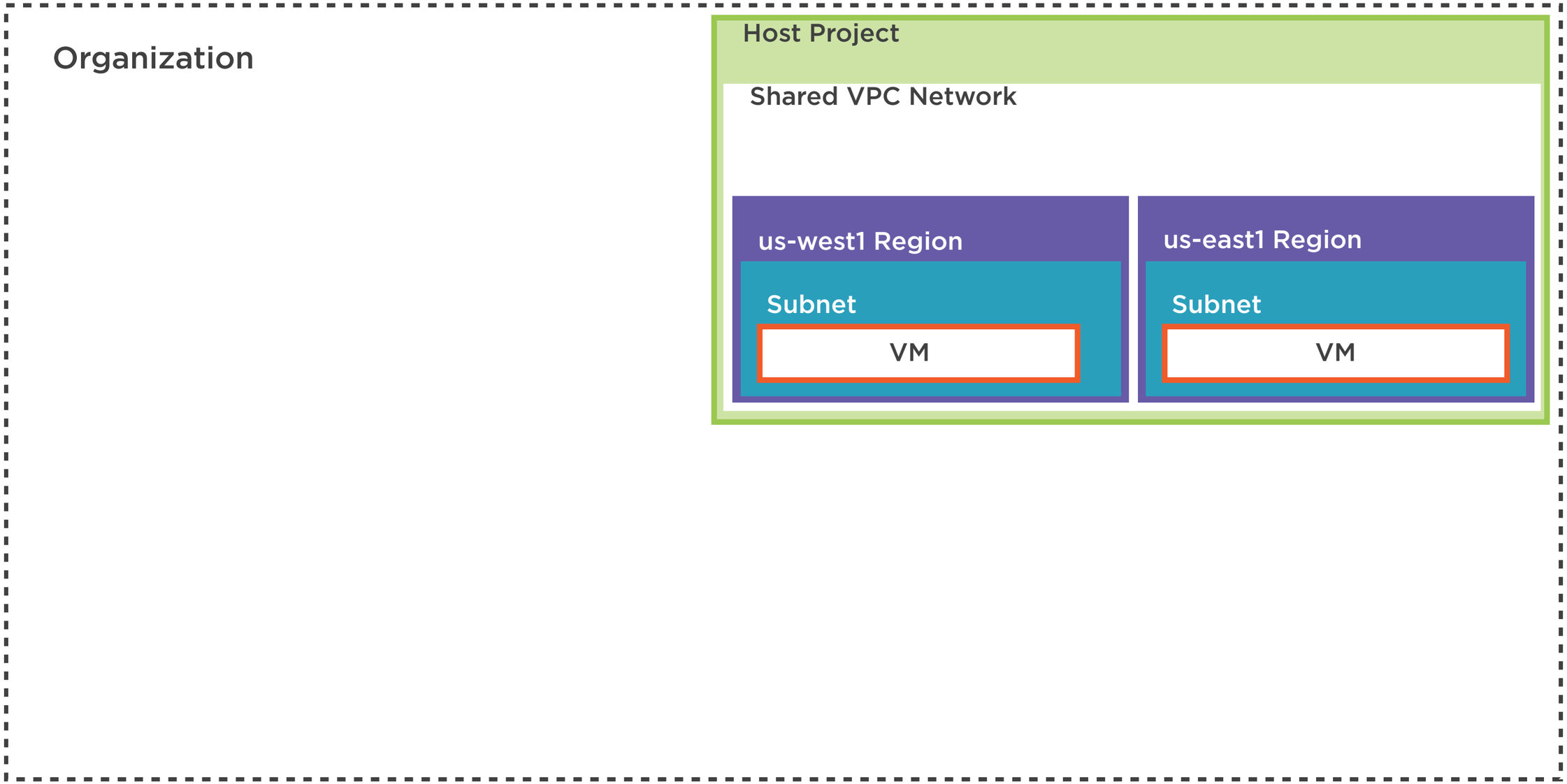
Shared VPC Admin Permissions



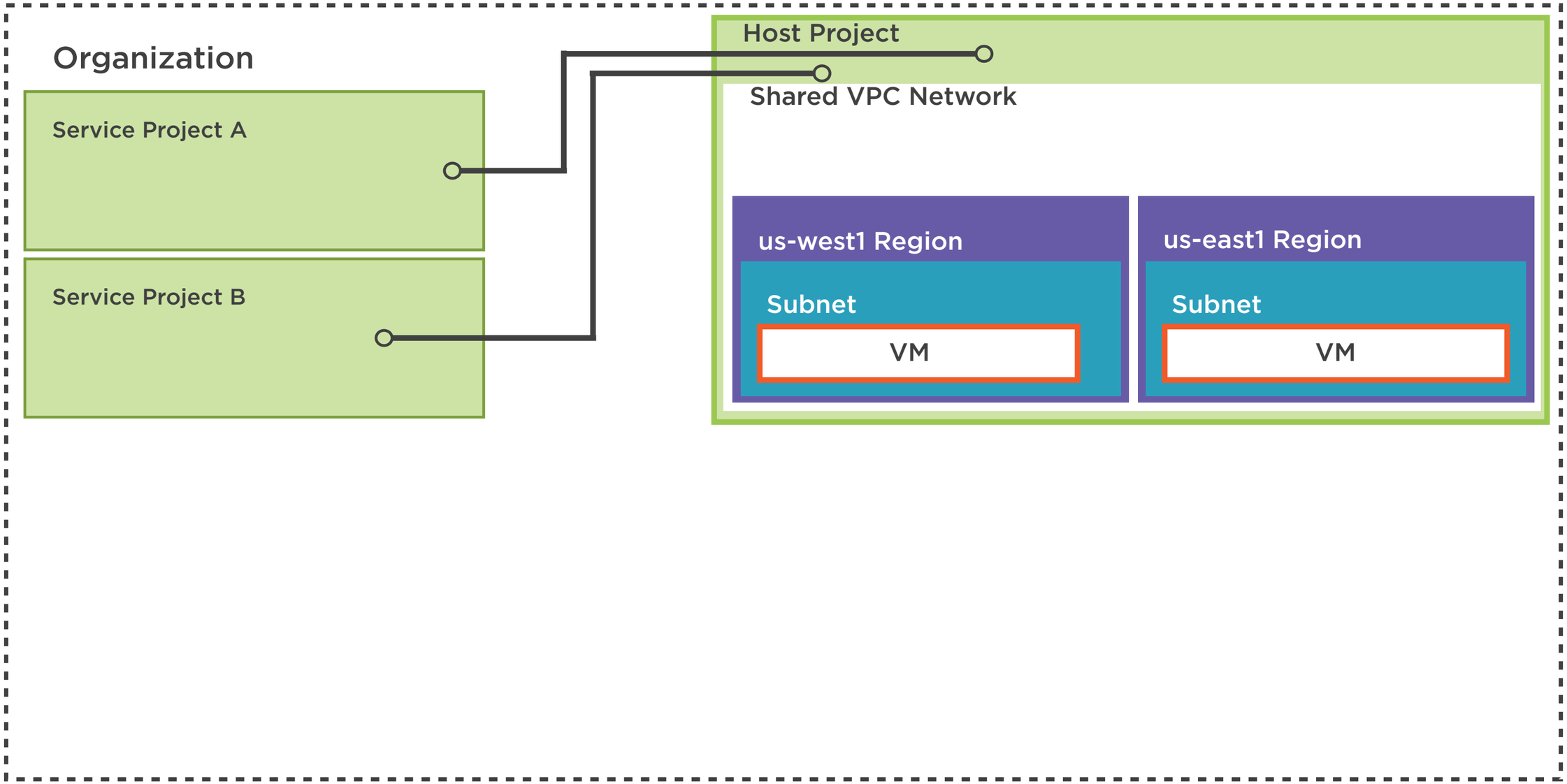
Subnets in Multiple Regions



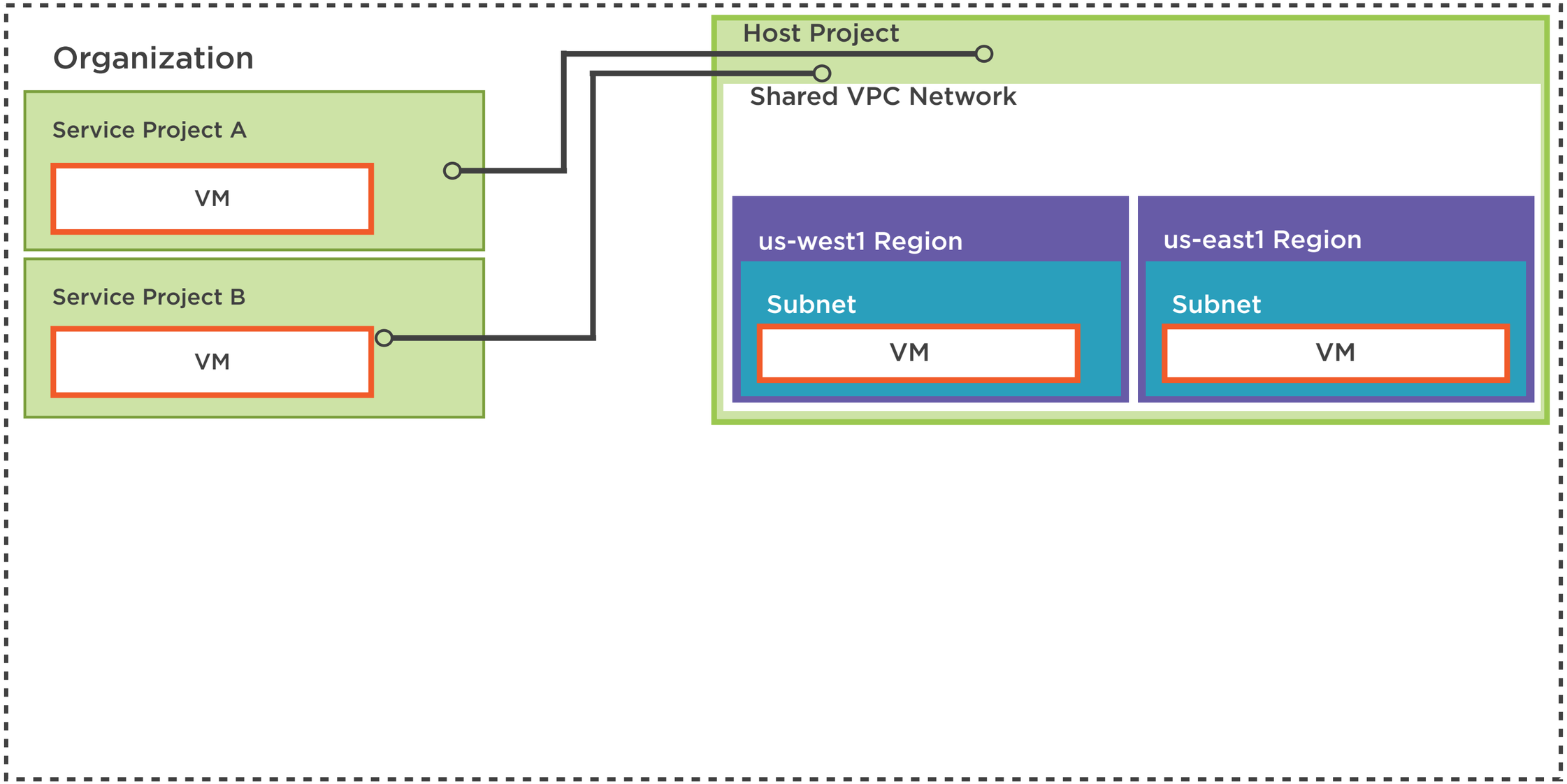
Can Share Specific Subnets



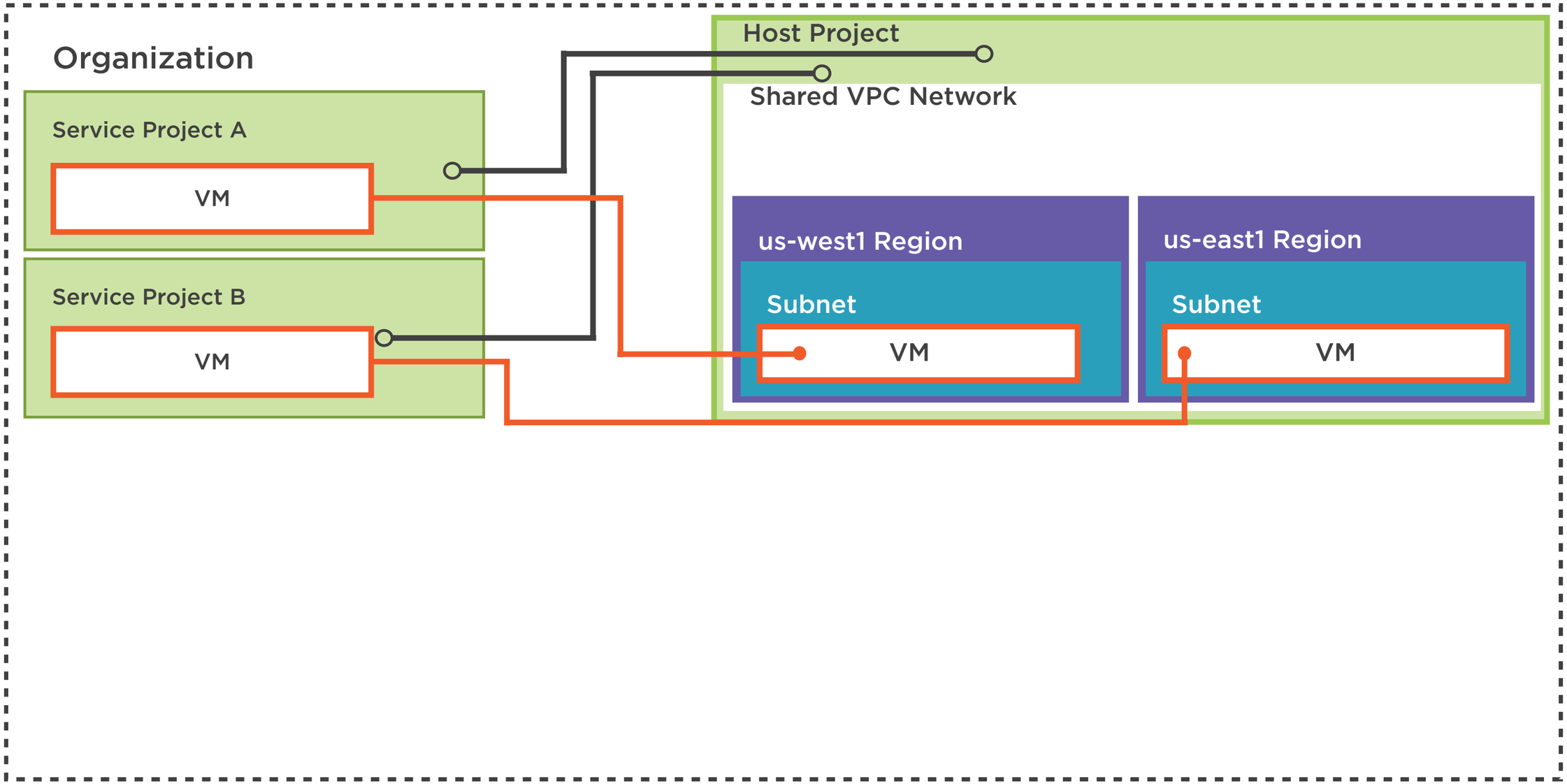
Attach Service Projects to Shared VPC



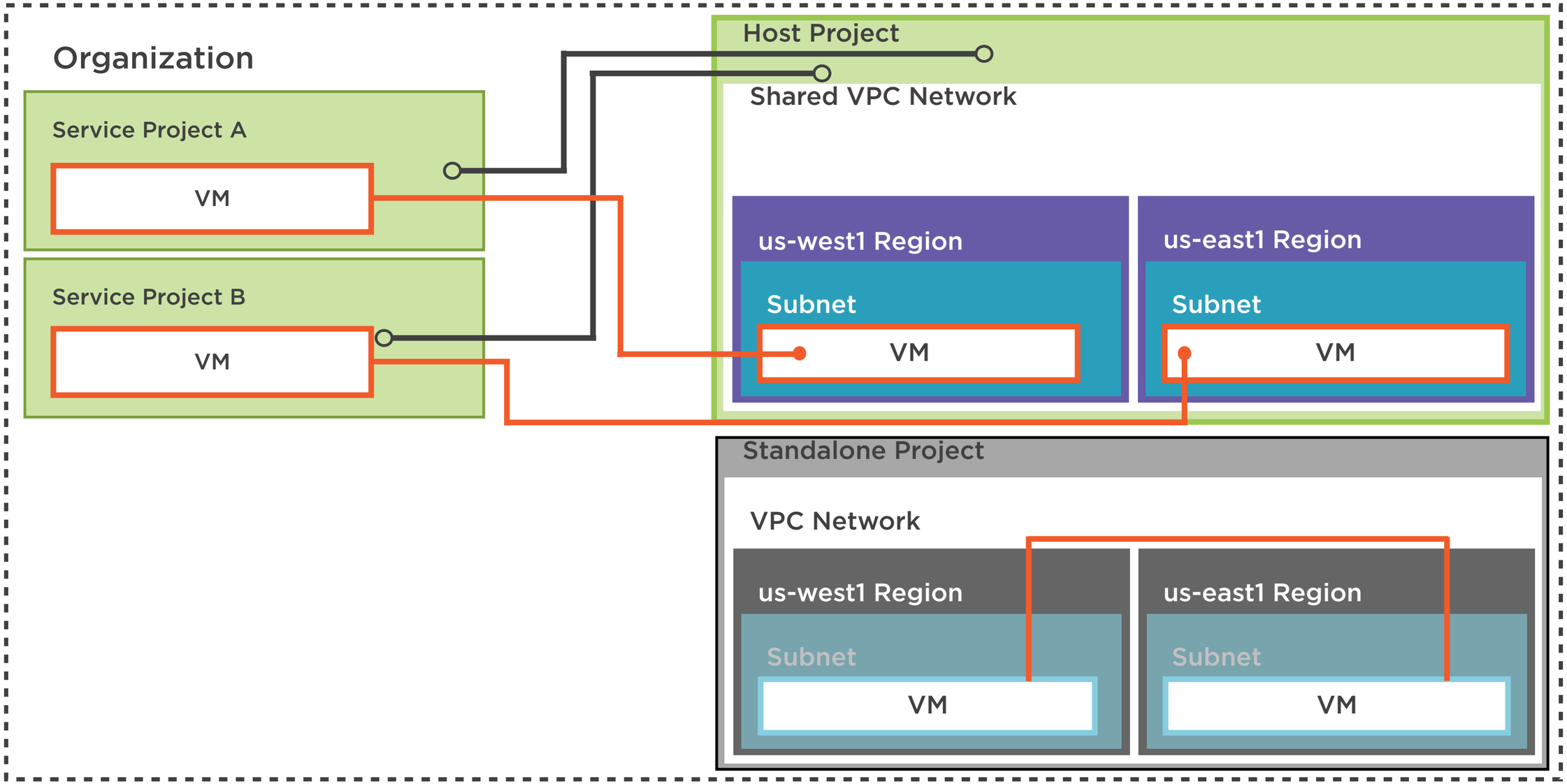
Service Projects Create VMs on Shared VPC

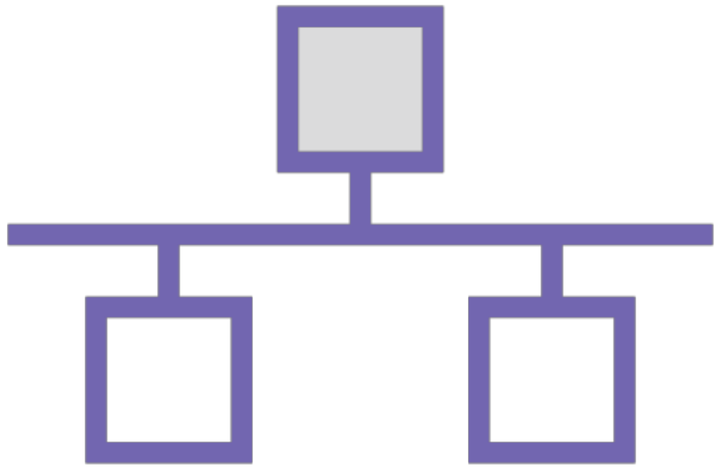


VMs Communicate Using Internal IPs



Organization May Have Standalone Projects





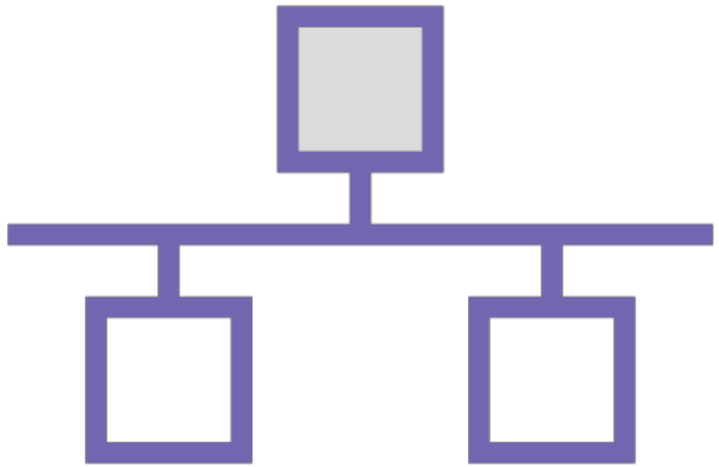
Shared VPC Mechanics

Designate one project as host

- VPC networks in host are Shared VPC networks

Attach service projects to it

- Eligible resources in service projects can access Shared VPC

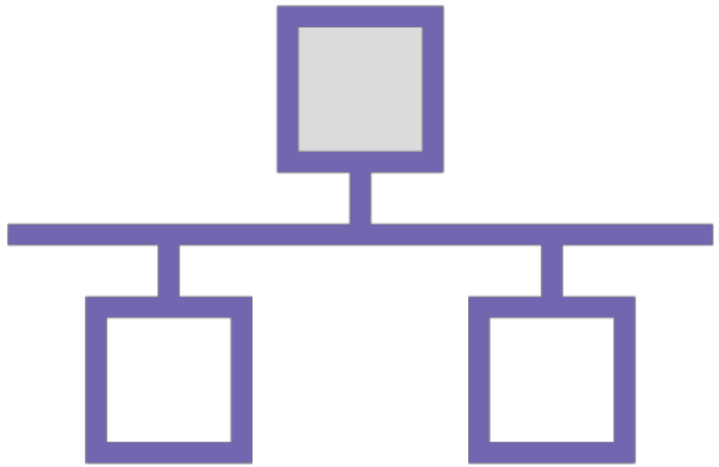


Shared VPC Mechanics

Projects must be in same organization

Host project can not also be service project

Each service project can be attached only to a single host



Shared VPC Mechanics

So, any project is of one of the following types:

- Host
- Service
- Standalone

Host Project

All existing VPC networks become Shared VPC networks

Any new VPC will automatically be a Shared VPC as well

Host Project

Project-level permissions:

- Service projects can use all subnets in host project
- Including VPCs and subnets added in the future

Subnet-level permissions:

- More restrictive set of permissions
- Service projects can only use selected subnets

Service Projects

Eligible resources include:

- GCE VM instances
- Instance templates
- Instance groups
- Internal IP addresses
- Internal DNS
- Load balancers

VPC Network Peering

A mechanism for RFC 1918 connectivity (i.e. the use of internal IP addresses) across two VPC networks regardless of project and organization boundaries

Shared VPCs vs. Network Peering

Shared VPCs	Network Peering
Only within same organization	Across organization boundaries
One VPC used across projects	Multiple VPCs share resources
Host and service projects are not peers	Connected VPCs are peers
Only single level of sharing possible	Multiple levels of peering possible

Demo

Configuring and working with a Shared VPC

Summary

Shared VPCs span multiple projects

One designated host project

Several designated service projects

Delegation of administrative responsibilities to Service Project Admins

Least privilege for network administration, auditing and access control

Clean Up Resources

Delete VM instances

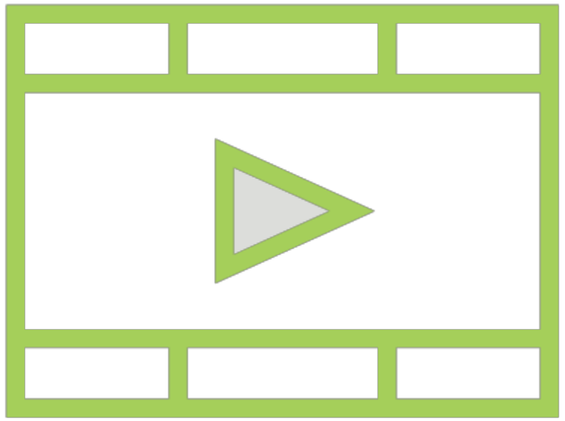
Delete firewall rules

If custom mode network

- delete subnets

Finally, delete VPC network

Related Courses



Leveraging Network Interconnection Options on the GCP

AWS Networking Deep Dive: Virtual Private Cloud (VPC)