Google Cloud

Networking in Google Cloud

Sharing VPC Networks

Today's agenda

01 VPC Network Peering

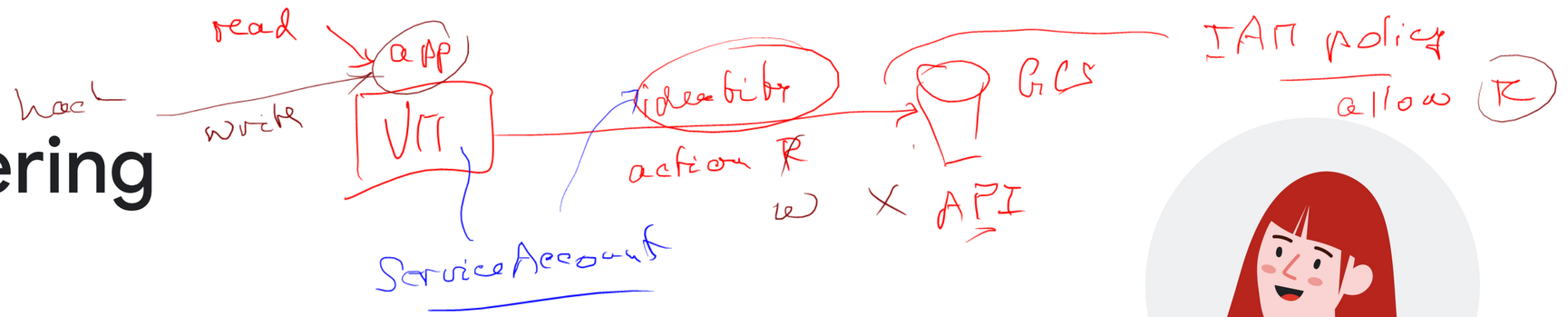
02 Shared VPC

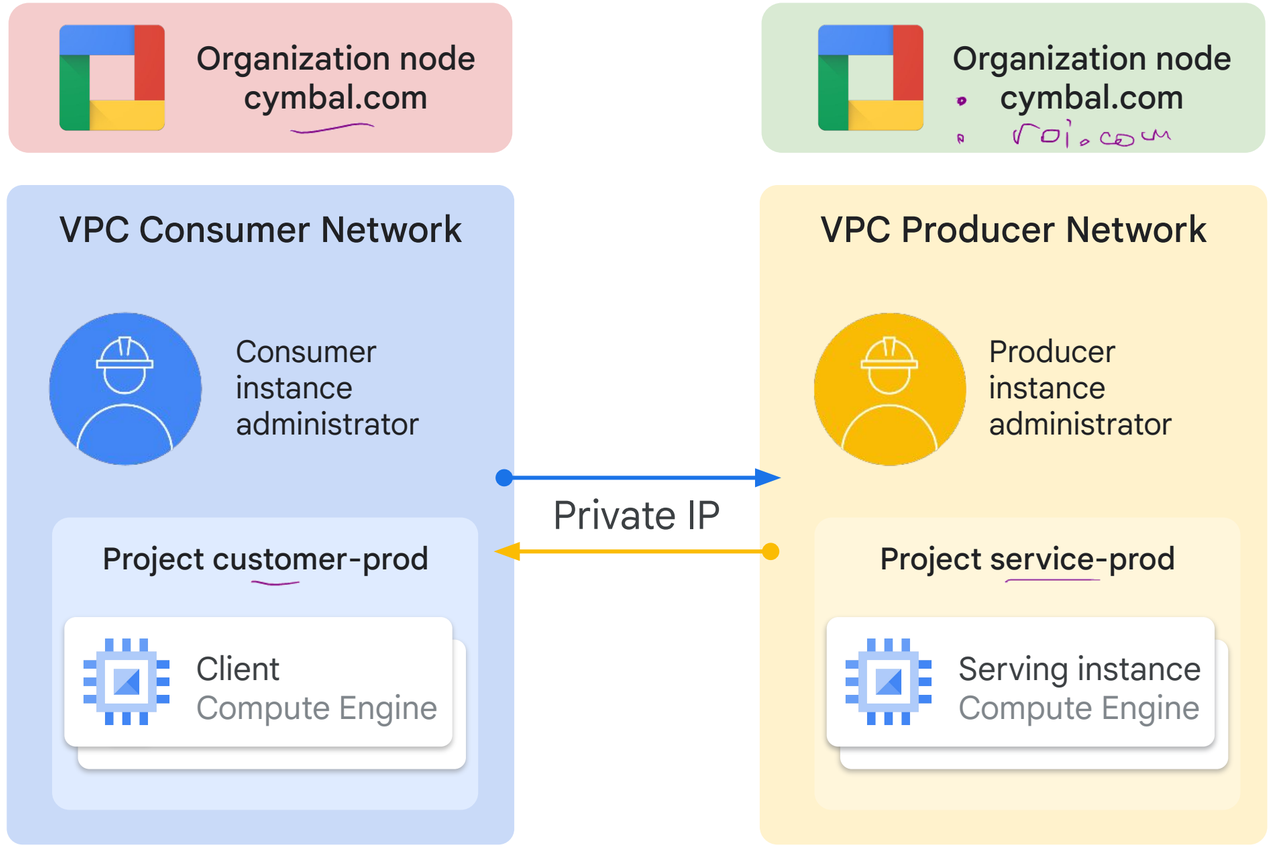
03 Lab: Configuring VPC Network Peering

04 Migrating a VM between networks

05 Quiz

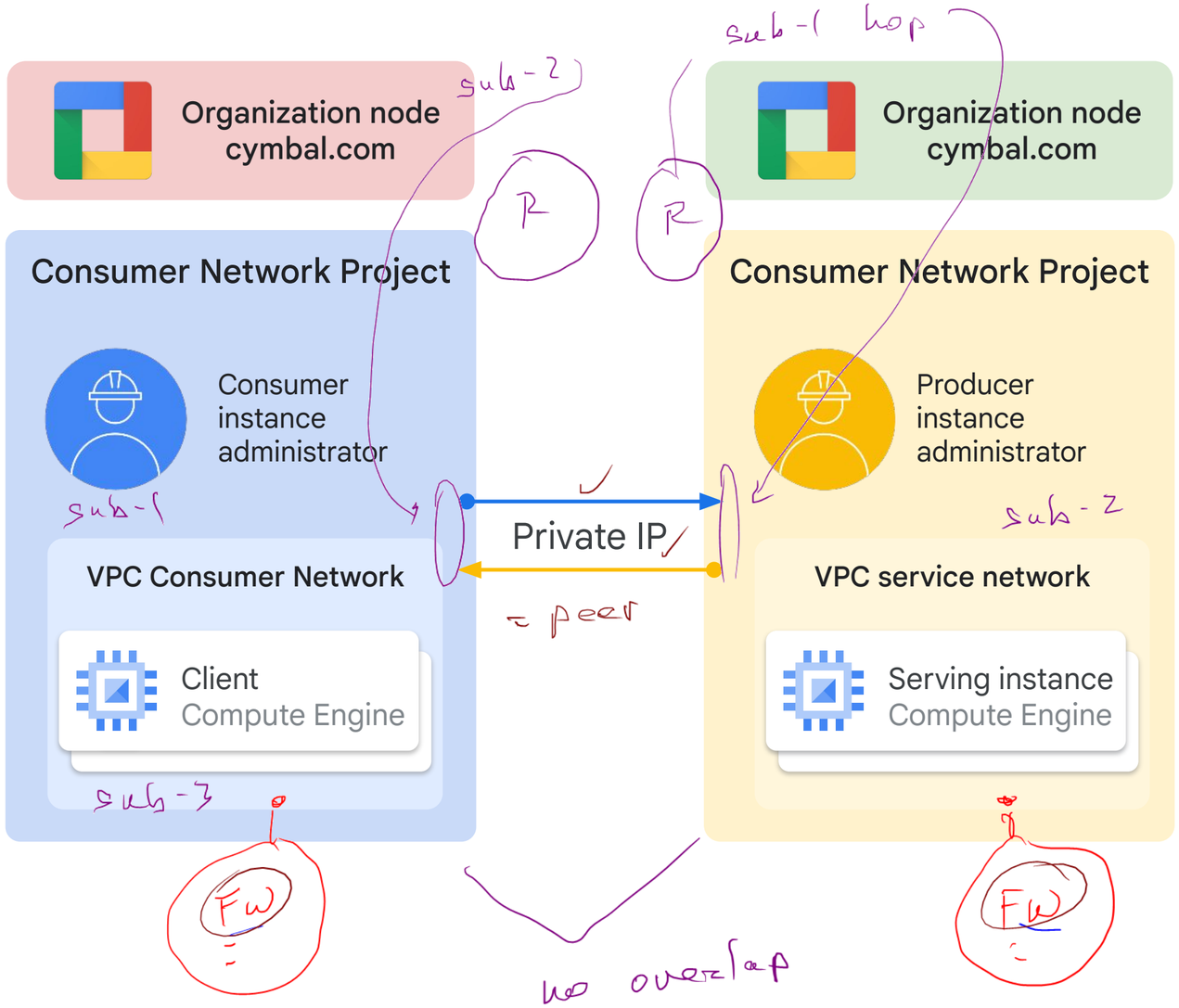
VPC Network Peering





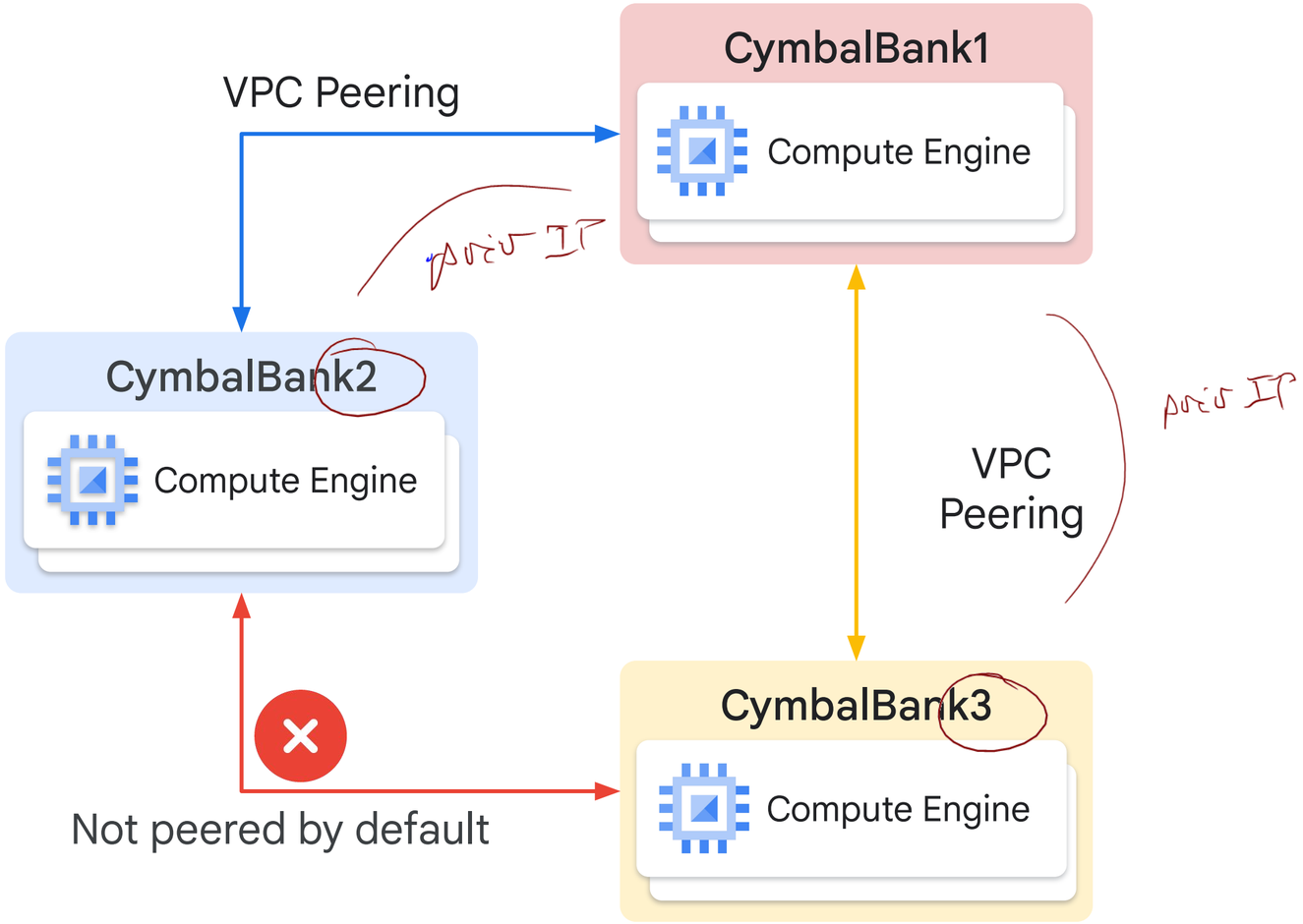
VPC Network Peering

- VPC Network Peering allows private connectivity across two VPC networks.
- Peering works:
  - Across organizations
  - Within the same project
  - Across different projects



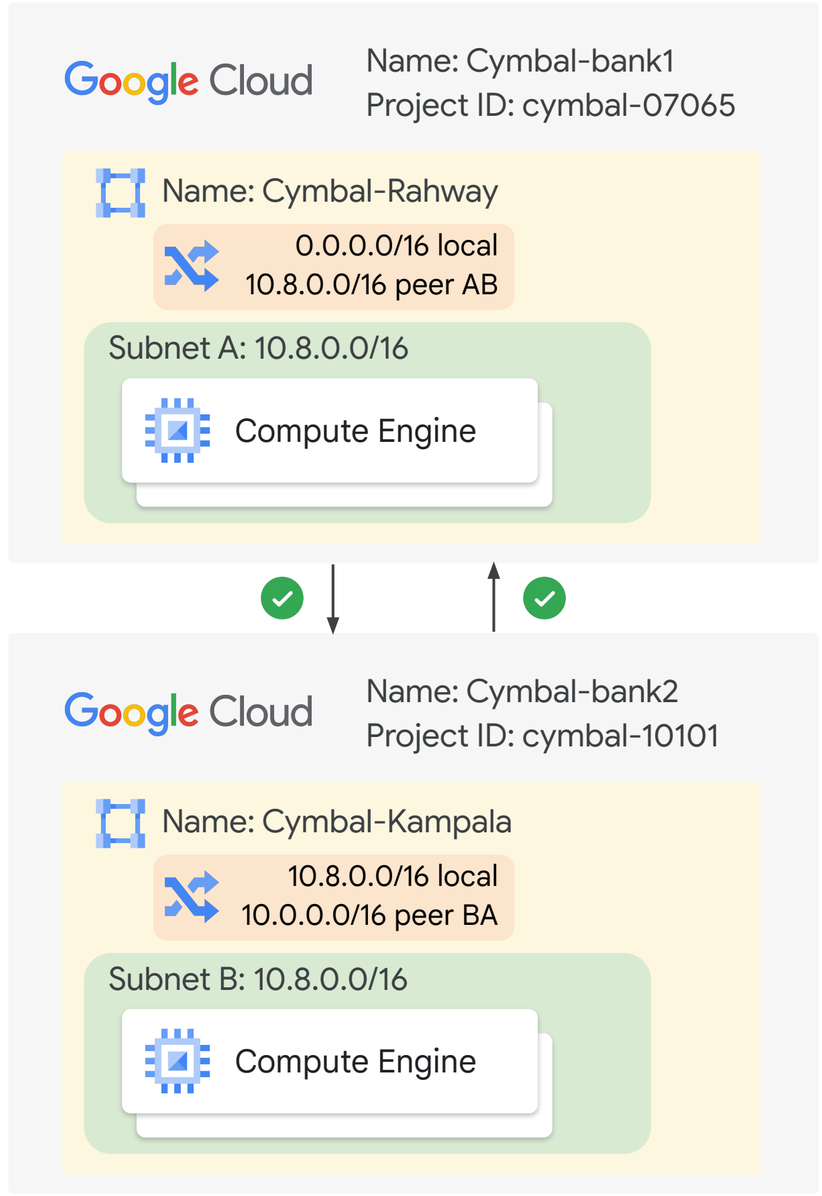
Using VPC Network Peering

- You can peer Compute Engine, Kubernetes Engine, and App Engine flexible environments.
- Peered VPC networks remain administratively separate.
- Each side of a peering association is set up independently.
- No subnet IP ranges overlap across peered VPC networks.
- Transitive peering is not supported.



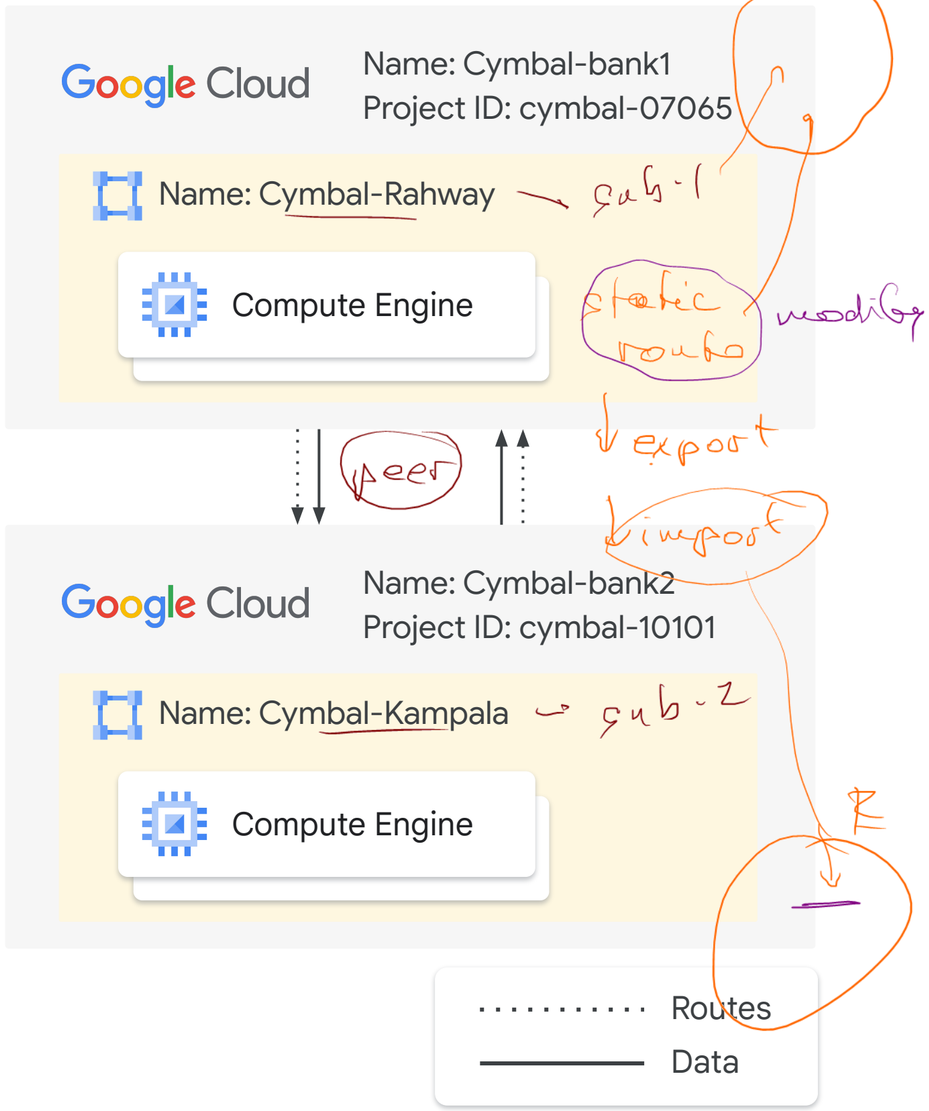
Initiating VPC Network Peering

- To initiate VPC Network Peering with another VPC network, you need the name of the other VPC network.
- If the VPC network is located in another project, you also need the project ID and network name.
- After peering is established, the two networks automatically exchange subnet routes.
- The peering connection is not active until it's initiated from both VPC networks.



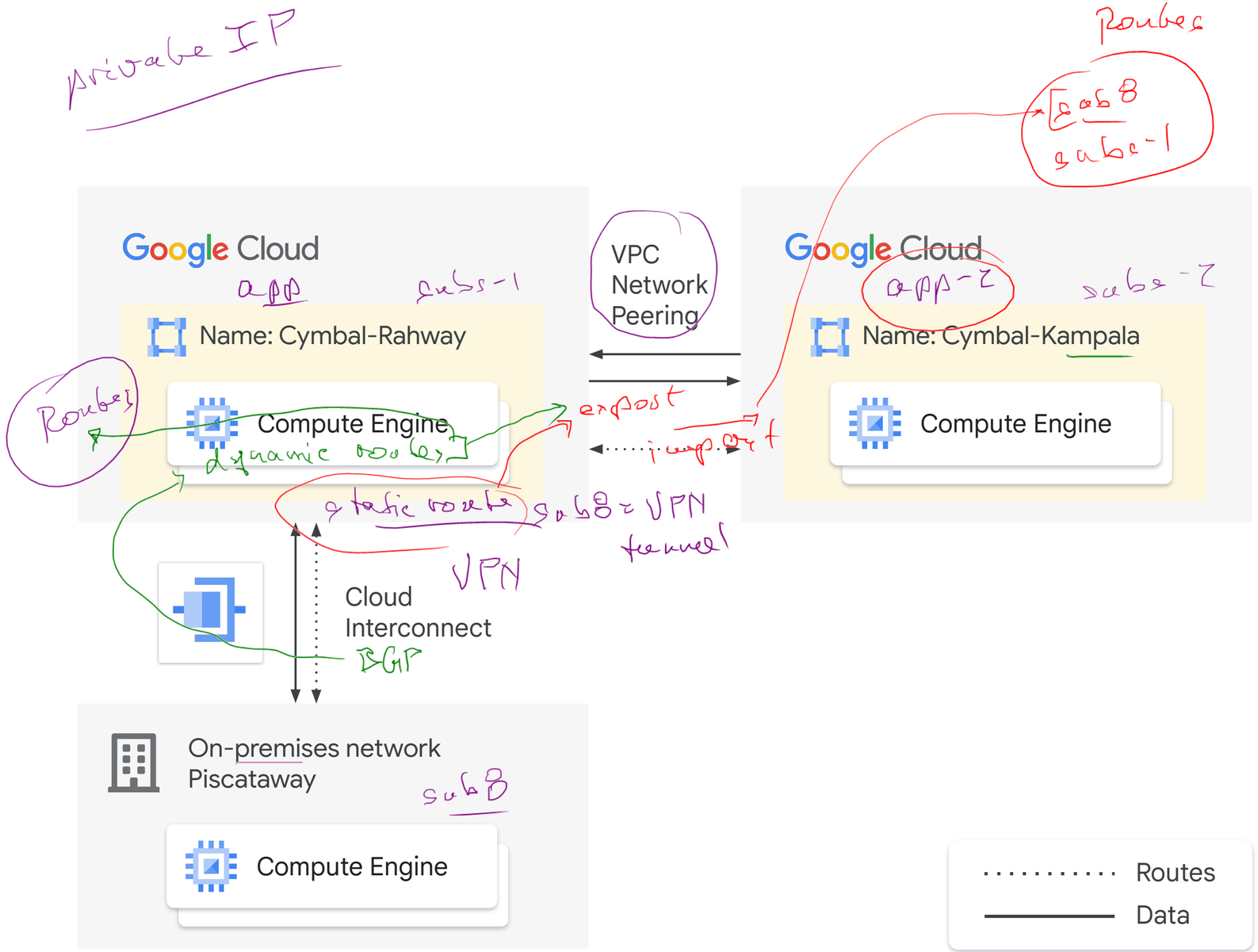
Sharing custom routes

- Custom routes help achieve a desired granularity that cannot be achieved with a default route.
- Sharing custom routes and dynamic with peered VPC networks lets networks learn routes directly from their peered networks.
- If a custom route in a peered network is updated, your VPC network automatically learns and uses the updated custom route.
- You can import and export routes.



A sample scenario

Share dynamic routes so that peered networks can reach your on-premises network.



Today's agenda

01 VPC Network Peering

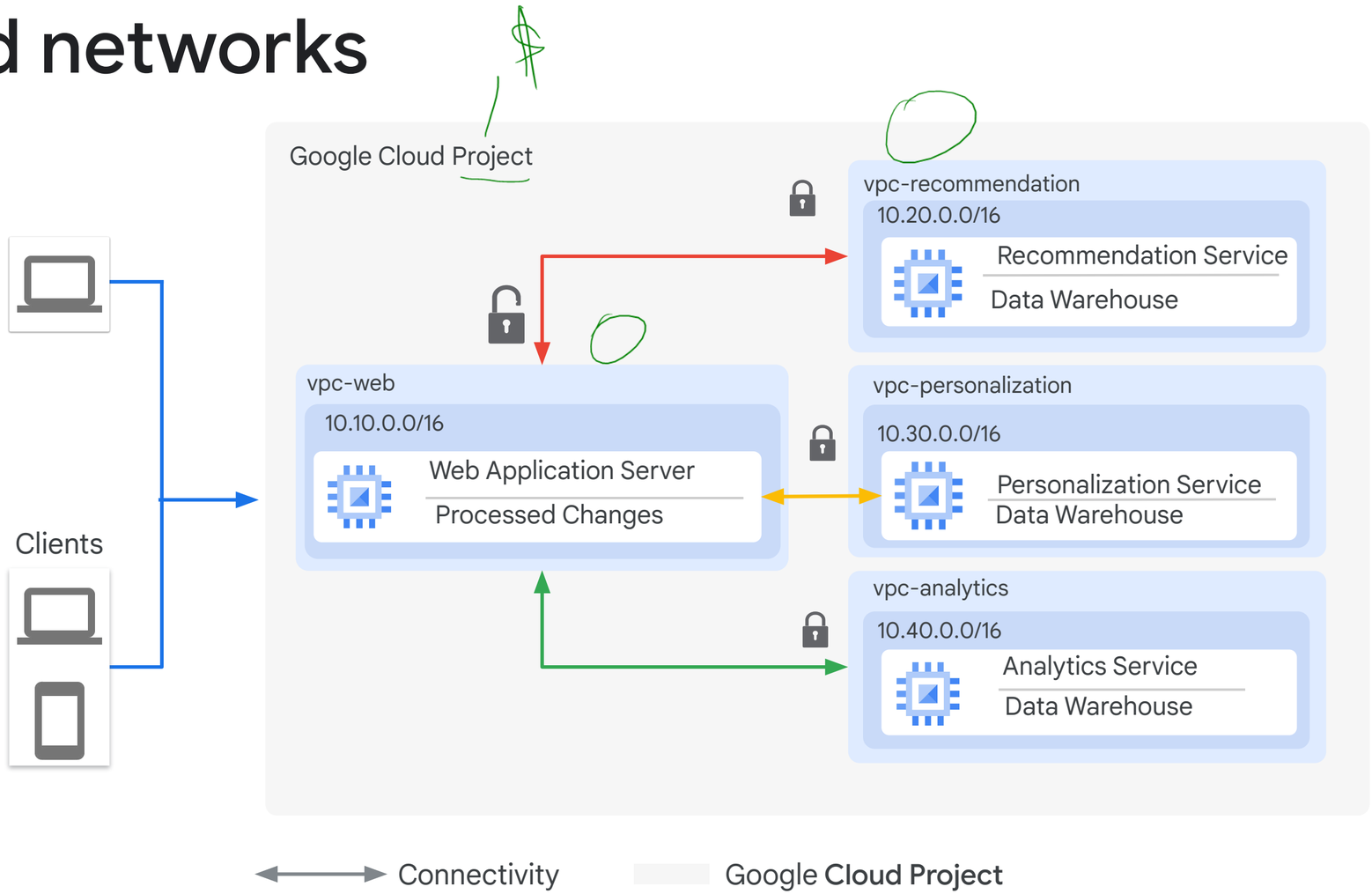
02 Shared VPC

03 Lab: Configuring VPC Network Peering

04 Migrating a VM between networks

05 Quiz

Use case: Complexity managing isolated networks

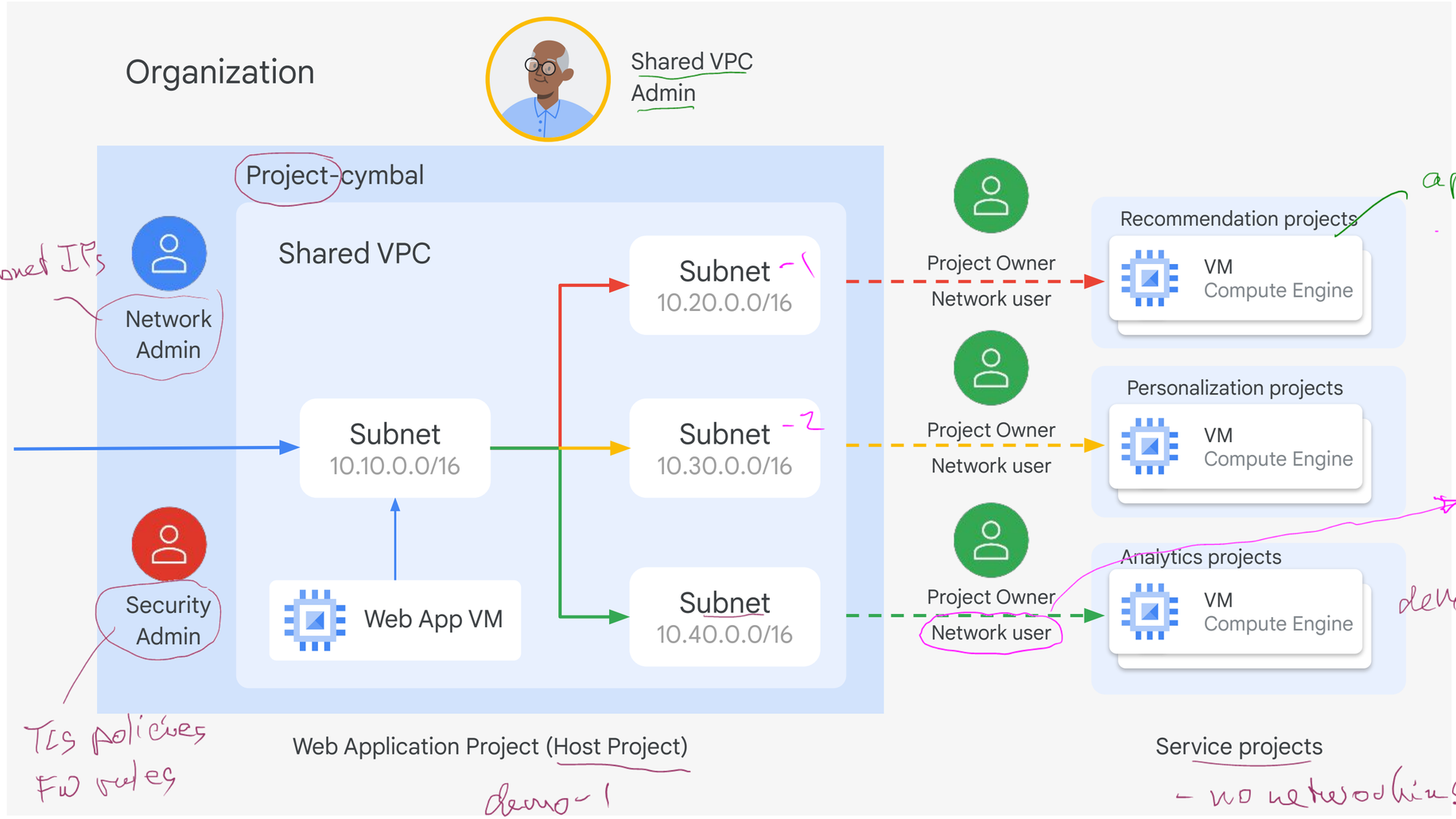


Steps to provisioning Shared VPC

Organization admin	Shared VPC admin	Service project admin

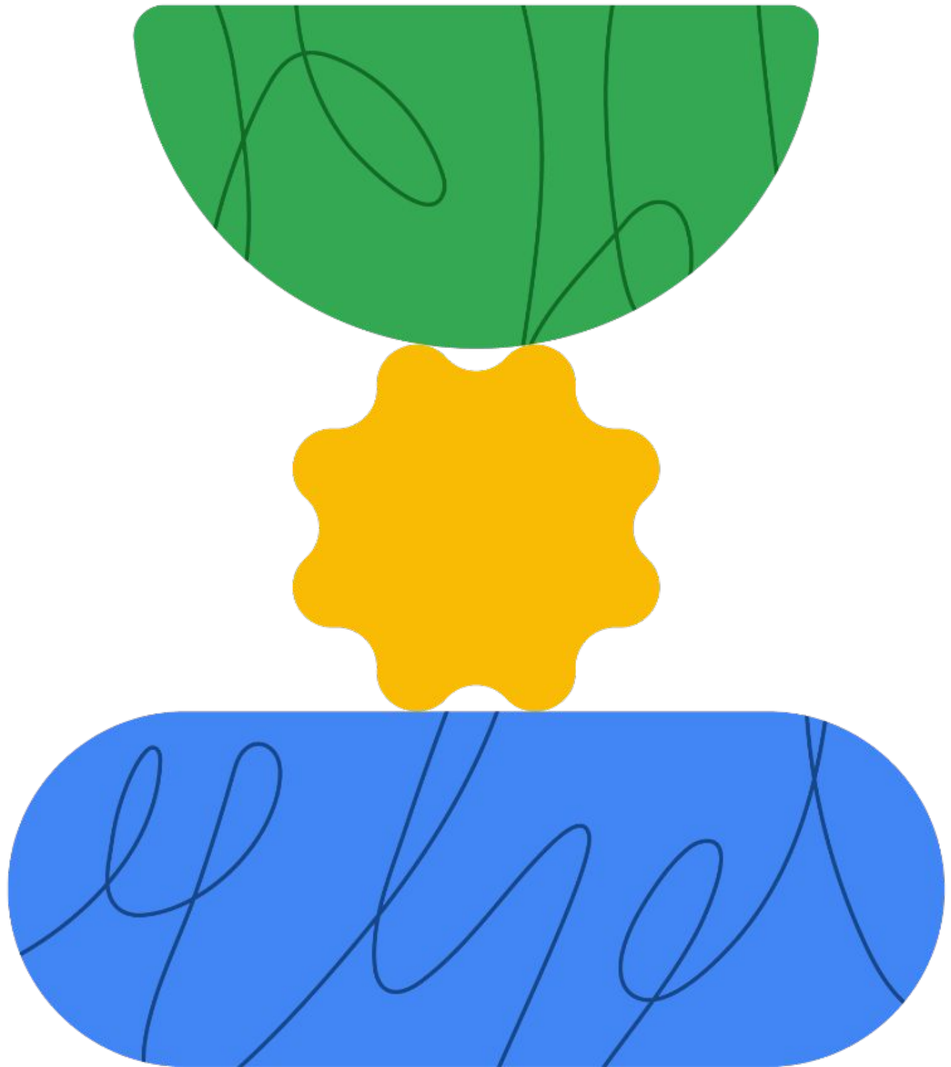
• The organization is the root node.
• Workplace or Cloud Identity super administrators assign organization administrators.
• They nominate Shared VPC administrators (compute.xpnAdmin).
	• Enables Shared VPC for a host project.
	• Attaches service projects.
	• Delegates access to some or all subnets in a Shared VPC network (compute.networkUser).
		• Network user
		• Control over service project resources:
		  ○ Compute instance administrator
		  ○ Project owner
		• Resource creation in Shared VPC:
		  ○ VM instances
		  ○ Instance templates and groups
		  ○ Static internal IP
		  ○ Load balancers

Use case: Centralize Control using Shared VPC



Demo

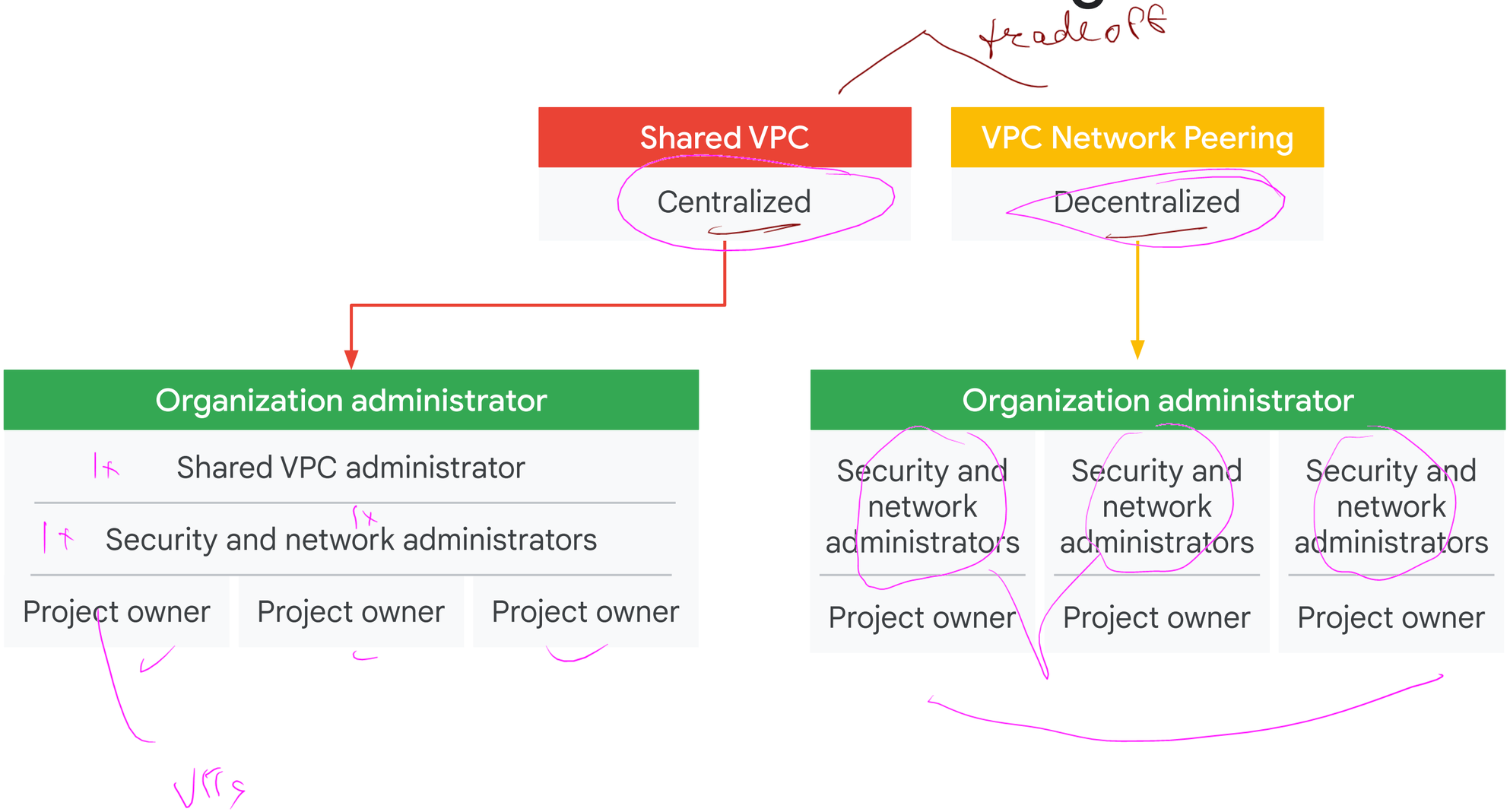
Shared VPC



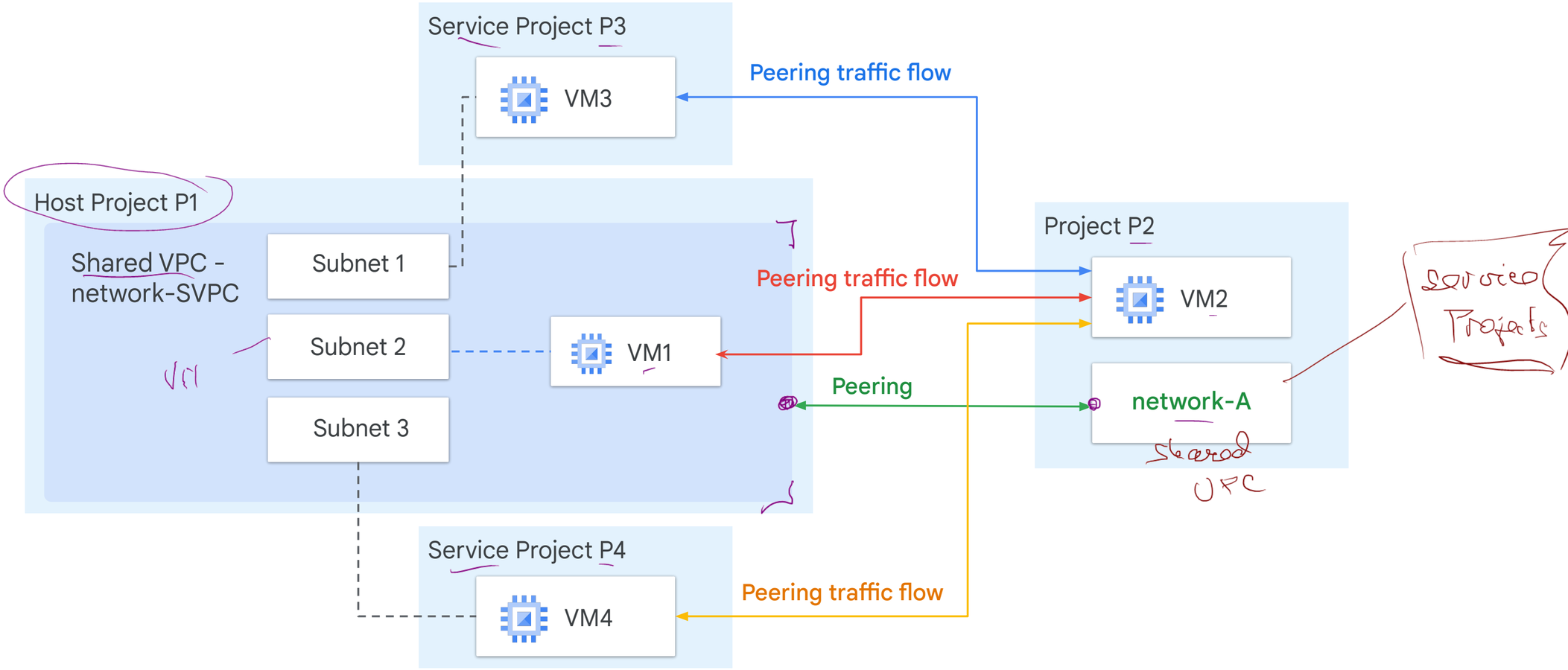
Shared VPC versus VPC Network Peering

Consideration	Shared VPC	VPC Network Peering
Across organizations	No	Yes
Within project	No	Yes
Network administration	Centralized	Decentralized

Shared VPC versus VPC Network Peering



Peering with a Shared VPC network



Let’s ask Gemini

I need VM instances in network A Org1 to access services from two different external organizations, Org2 and Org3, using internal IP addresses. Is this possible with peering?

Yes, it is possible to use peering to access services from two different external organizations. To do this, you will need to create two peering connections: one between network A and Org2, and one between network A and Org3.

*Gemini responses may vary

Today's agenda

01 VPC Network Peering

02 Shared VPC

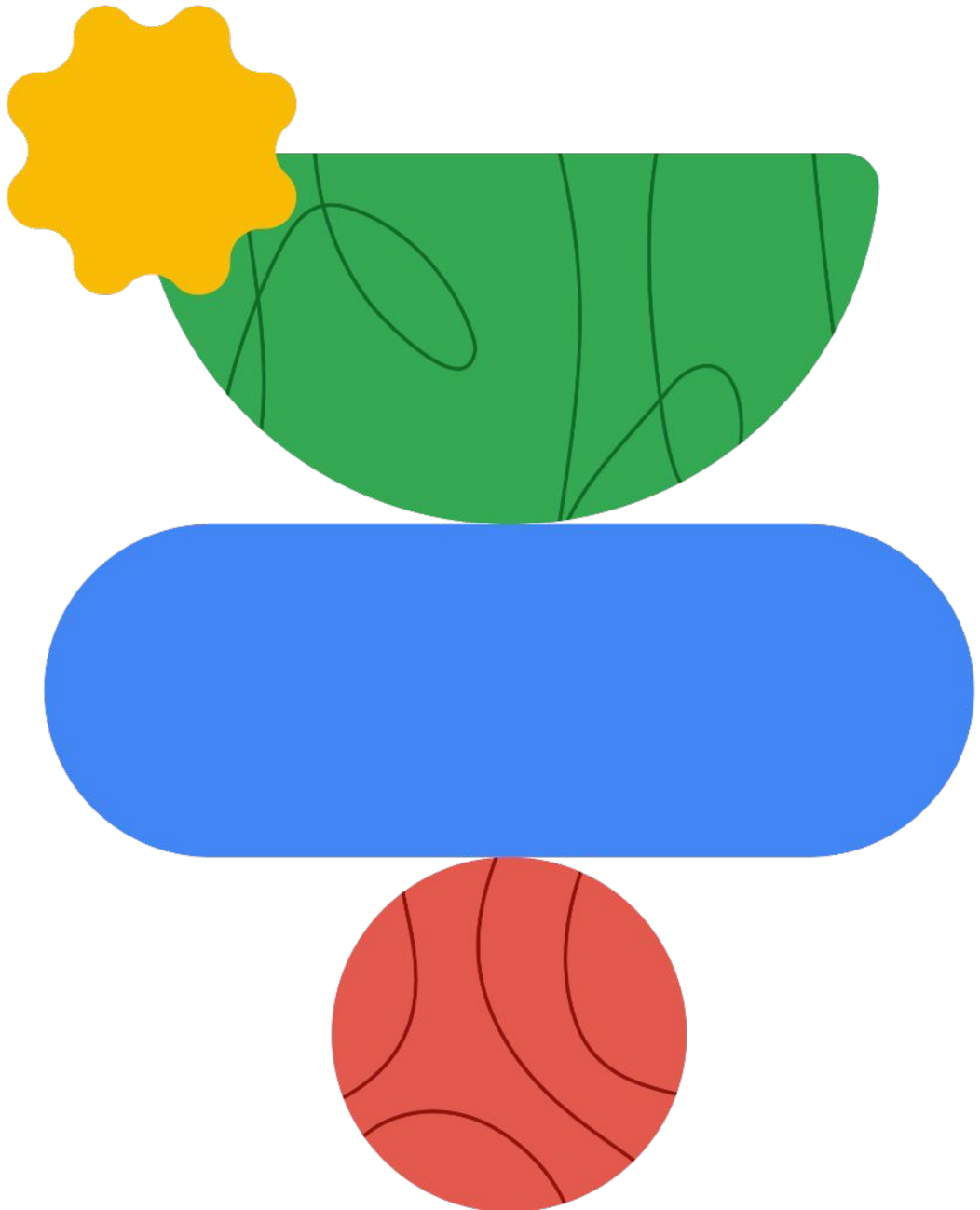
03 Lab: Configuring VPC Network Peering

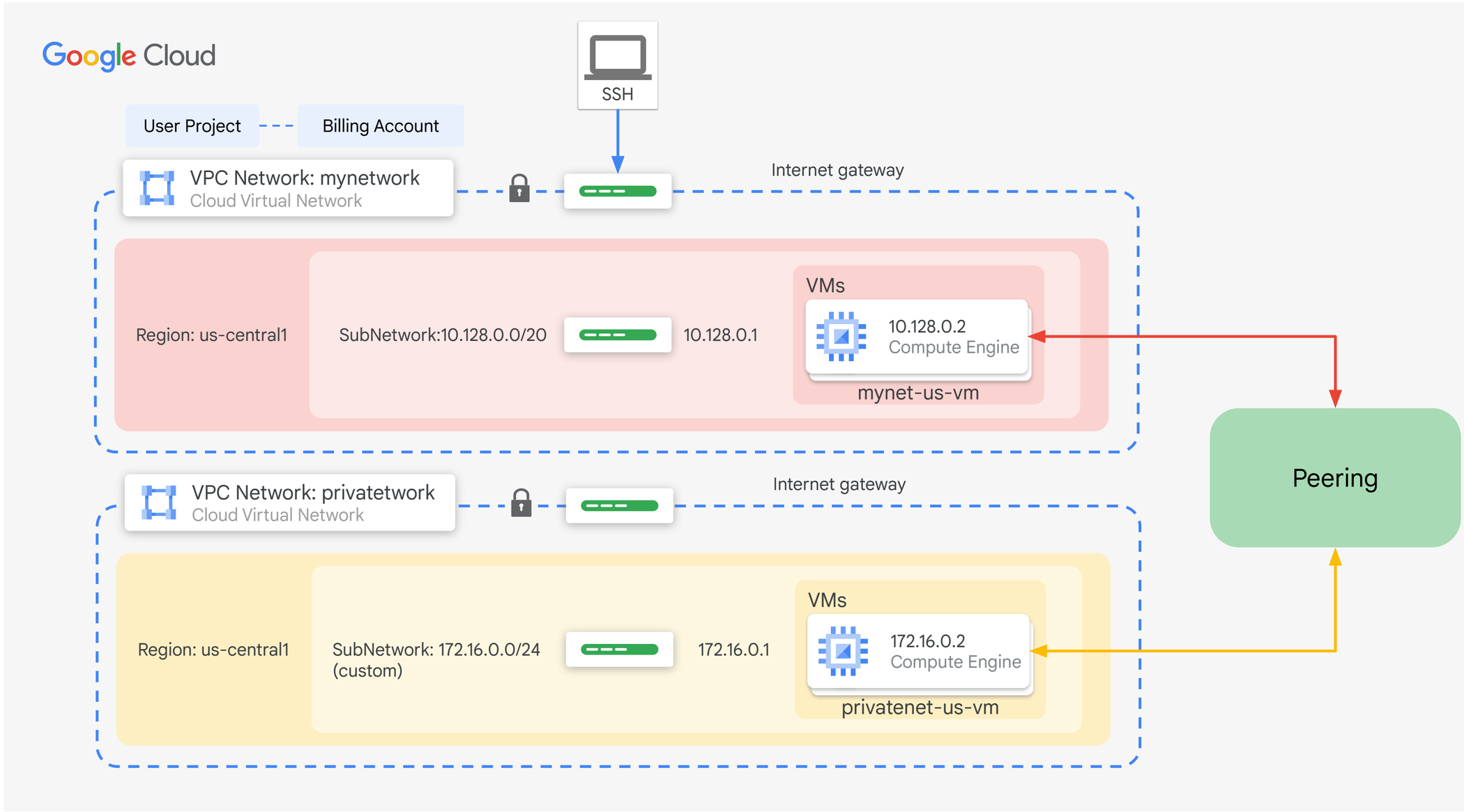
04 Migrating a VM between networks

05 Quiz

Lab intro

Configuring VPC Network Peering




Google Cloud
SSH
User Project
Billing Account
VPC Network: mynetwork
Cloud Virtual Network
Internet gateway
Region: us-central1
SubNetwork:10.128.0.0/20
10.128.0.1
VMs
10.128.0.2
Compute Engine
mynet-us-vm
Peering
VPC Network: privatetwork
Cloud Virtual Network
Internet gateway
Region: us-central1
SubNetwork: 172.16.0.0/24
(custom)
172.16.0.1
VMs
172.16.0.2
Compute Engine
privatenet-us-vm

Today's agenda

01 VPC Network Peering

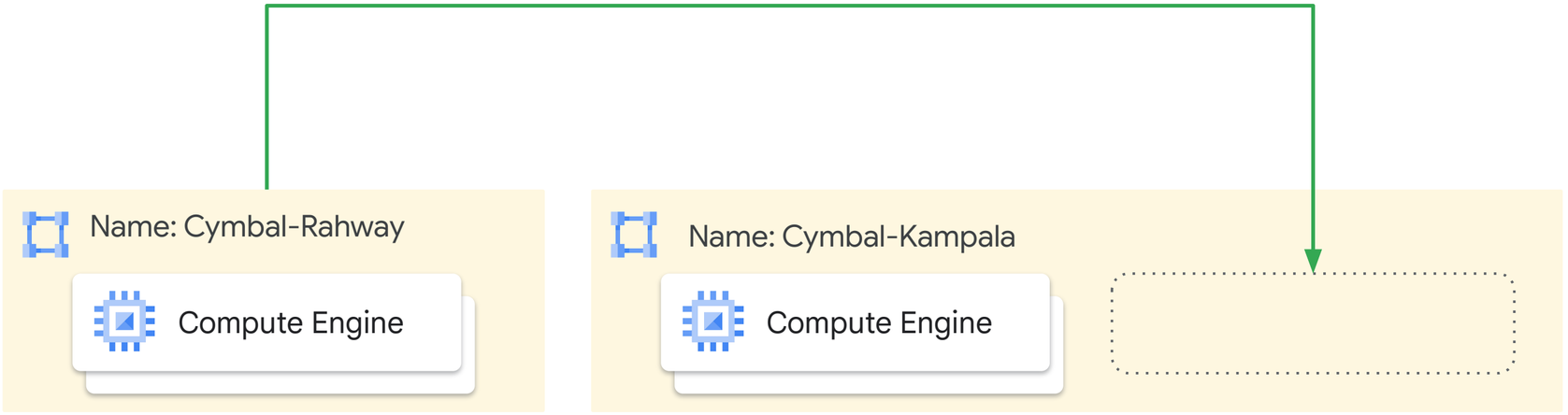
02 Shared VPC

03 Lab: Configuring VPC Network Peering

04 Migrating a VM between networks

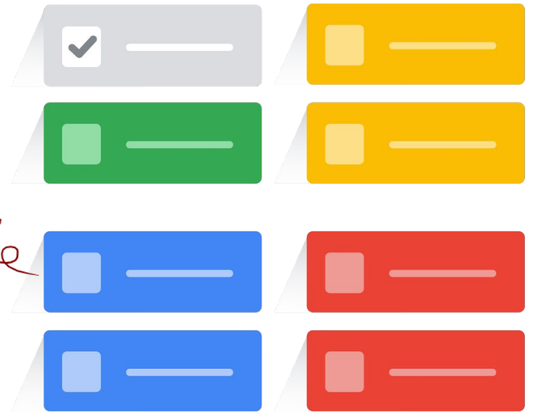
05 Quiz

Supported migrations



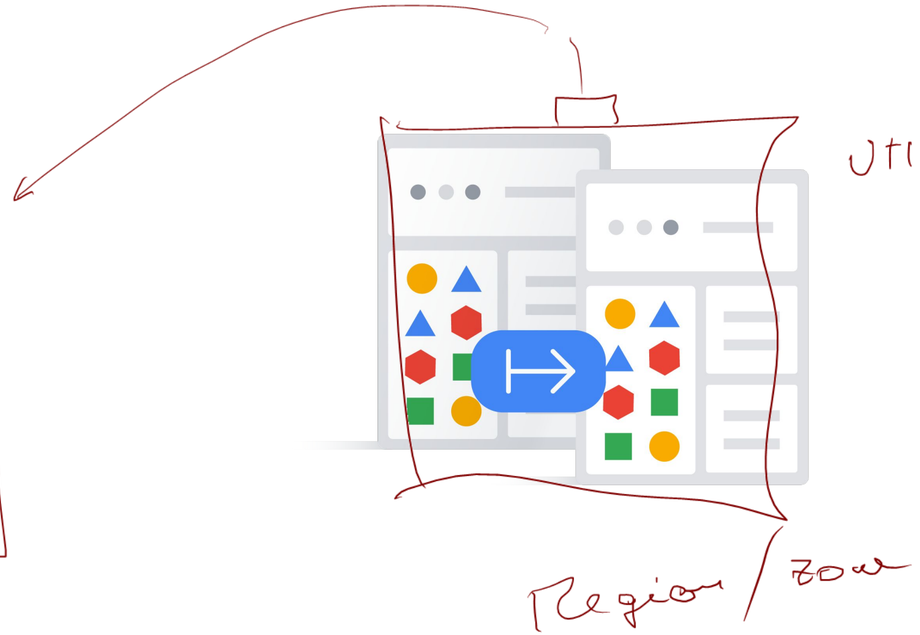
Migration requirements

- The VM must be stopped before it can be migrated.
- The VM must not be in an instance group or network endpoint group (NEG).
  - If the VM is in an unmanaged instance group or NEG, you must take it out of the group before migrating it.
  - VMs in managed instance groups cannot be migrated.
  - You can move instances in target pools without removing them first.



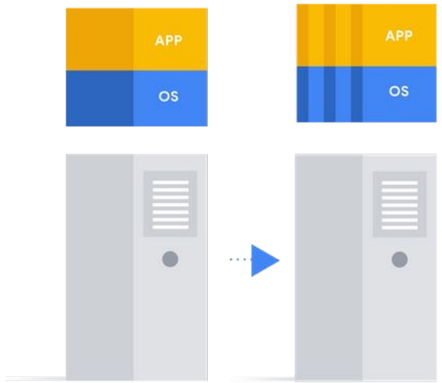
Supported migrations

- Legacy network to a VPC network in the same project.
- One VPC network to another VPC network in the same project.
- One subnet of a VPC network to another subnet of the same network.
- A service project network to the shared network of a Shared VPC host project.



Migration limitations

- A VM interface cannot be migrated to a legacy network.
- The MAC address allocated to the network interface changes during the migration.
- If migrating the VM to a network or subnet with a different IP range, the internal IP address of your instance must change.
- If migrating to a subnet with the same IP range, the old IP address can be kept (if not in use at destination).
- An existing external IP address can be kept in the new location subject to permissions.



Today's agenda

01 VPC Network Peering

02 Shared VPC

03 Lab: Configuring VPC Network Peering

04 Migrating a VM between networks

05 Quiz

Quiz | Question 1

Question

Sort the following steps for provisioning Shared VPC in Google Cloud:

A. A Shared VPC administrator enables Shared VPC for the host project.

B. An organization administrator nominates a Shared VPC administrator.

C. A Shared VPC Admin delegates access to some or all subnets of a shared VPC network by granting the Network User role.

D. A Network User creates resources in their Service Project.

Quiz | Question 1

Answer

Sort the following steps for provisioning Shared VPC in Google Cloud:

B. An Organization Admin nominates a Shared VPC Admin.

A. A Shared VPC Admin enables shared VPC for the host project.

C. A Shared VPC administrator delegates access to some or all subnets of a Shared VPC network by granting the network user role.

D. A network user creates resources in their service project.

Quiz | Question 2

Question

Which of the following statements about VPC Network Peering is correct?

A. Transitive peering is not supported.

B. Peered VPC networks do not remain administratively separate.

C. Subnet IP ranges can overlap across peered VPC networks.

D. Both sides of a peering association are set up in one single step.

Quiz | Question 2

Answer

Which of the following statements about VPC Network Peering is correct?

A. Transitive peering is not supported.

B. Peered VPC networks do not remain administratively separate.

C. Subnet IP ranges can overlap across peered VPC networks.

D. Both sides of a peering association are set up in one single step.

Quiz | Question 3

Question

Which of the following approaches to multi-project networking uses a centralized network administration model?

A. VPC Network Peering

B. Shared VPC

C. Cloud VPN

D. Cloud VPN and Shared VPC

Quiz | Question 3

Answer

Which of the following approaches to multi-project networking uses a centralized network administration model?

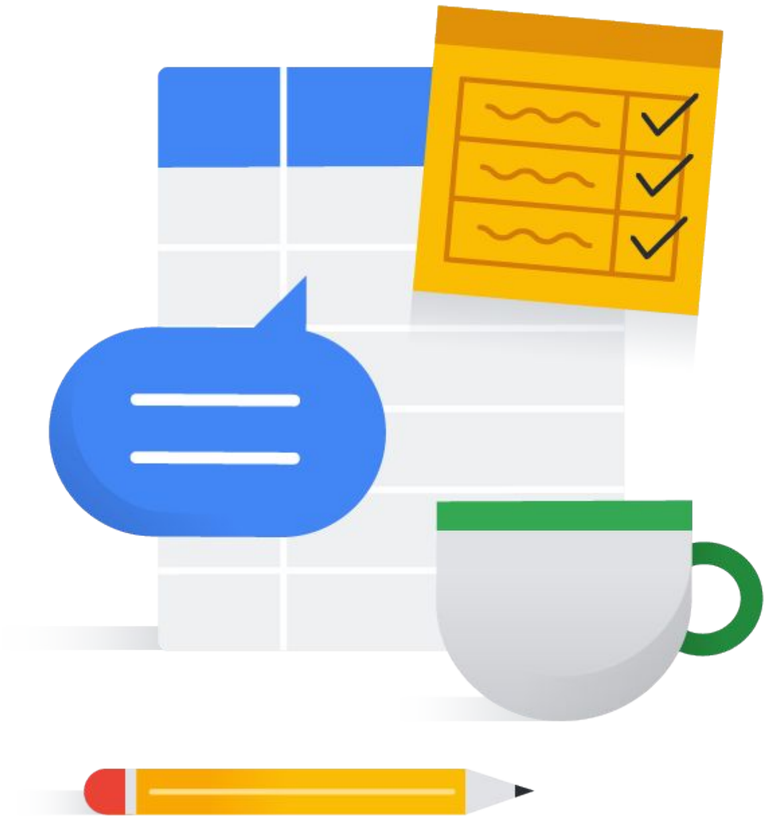
A. VPC Network Peering

B. Shared VPC 

C. Cloud VPN

D. Cloud VPN and Shared VPC

Debrief



Thank you.