Google Cloud

# Networking in Google Cloud

Private Connection Options

# Today's agenda

01 Private access overview

02 Private Google Access

03 Private Service Connect

04 Private services access

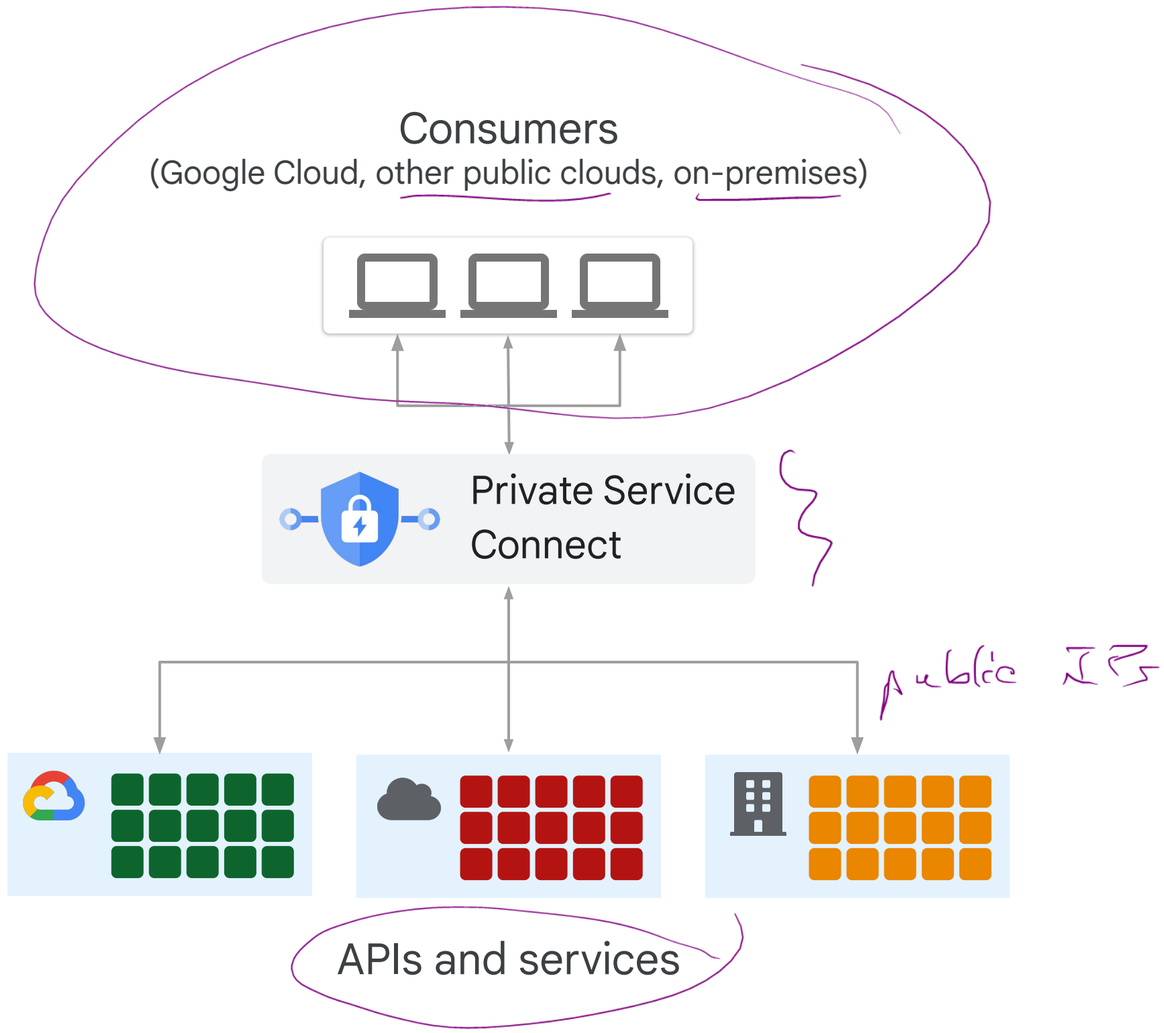
05 Cloud NAT

06 Lab: Implement Private Google Access with Cloud NAT

07 Quiz

# Private access for Google APIs and services

- Private access uses internal IP addresses.
- *Private access* refers to the ability to connect to APIs and services locally.
- Access is quicker and more secure.
- Choose a private access option based on your needs.
- All Google Cloud APIs and services support private access.



# Private access options

| Option | Connection | Usage |
| --- | --- | --- |
| Private Google Access | Connect to the public IP addresses of Google APIs and services through the default internet gateway of the VPC network. | Lets you use Google APIs and services without giving your Google Cloud resources external IP addresses. |
| Private Service Connect | Connect to Google, third-party, or your own services by using internal IP addresses. | Lets you use internal IP addresses to consume, produce, and make services available. |
| Serverless VPC Access | Connect serverless products to your VPC network to access Google, third-party, or your own services with internal IP addresses. | Lets Cloud Run, App Engine standard, and Cloud Functions connect to the internal IPv4 addresses in a VPC network. |
| Private services access | Connect Google and third-party services privately and directly to your VPC network with VPC Network Peering. | Lets you use internal IP addresses to connect to specific Google and third-party services by using VPC Network Peering. |

# Today's agenda

01 Private access overview

02 Private Google Access

03 Private Service Connect

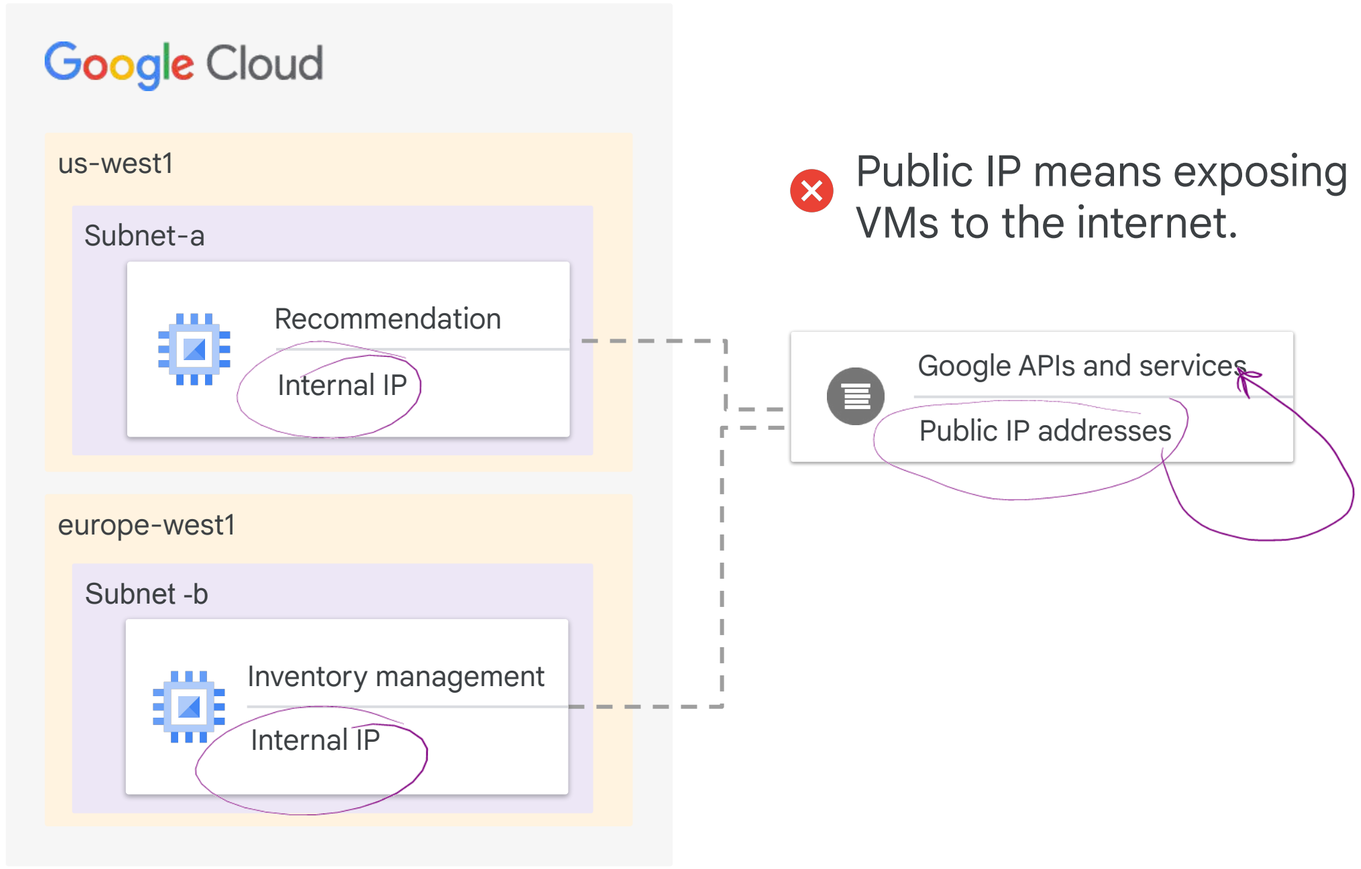
04 Private services access

05 Cloud NAT

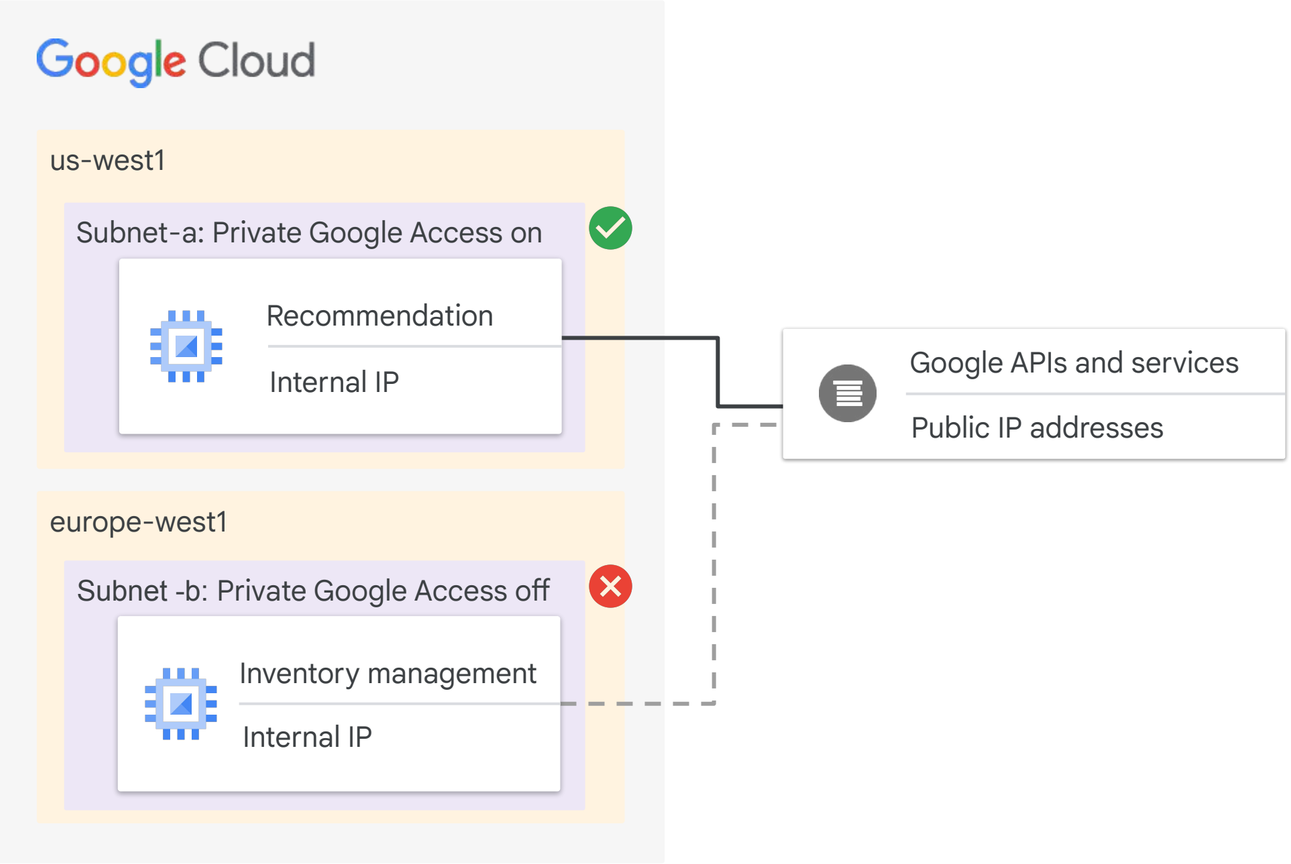
06 Lab: Implement Private Google Access with Cloud NAT

07 Quiz

# Use case: Securely connect to Google Cloud API

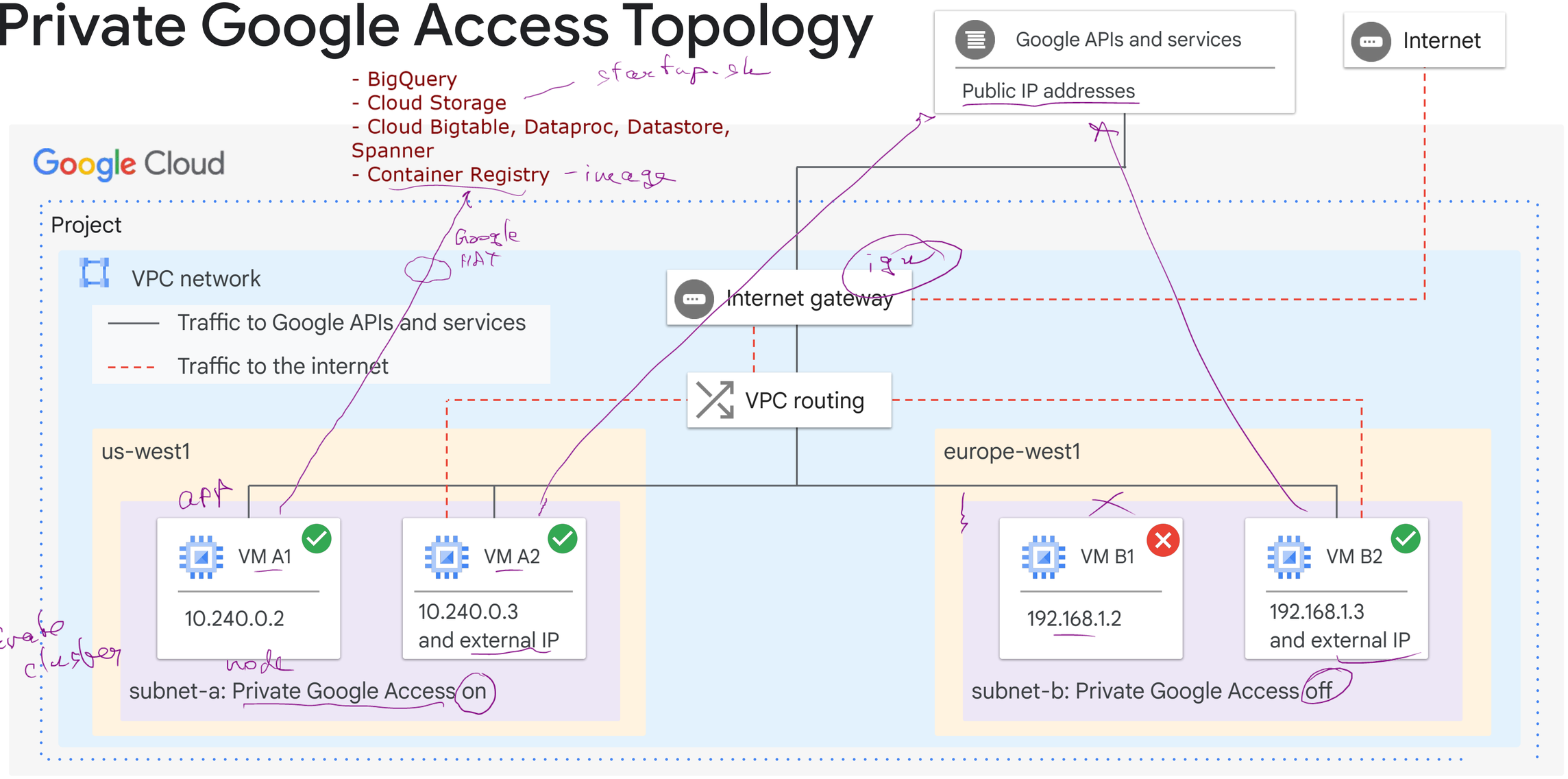



# Private Google Access is enabled at a subnet level

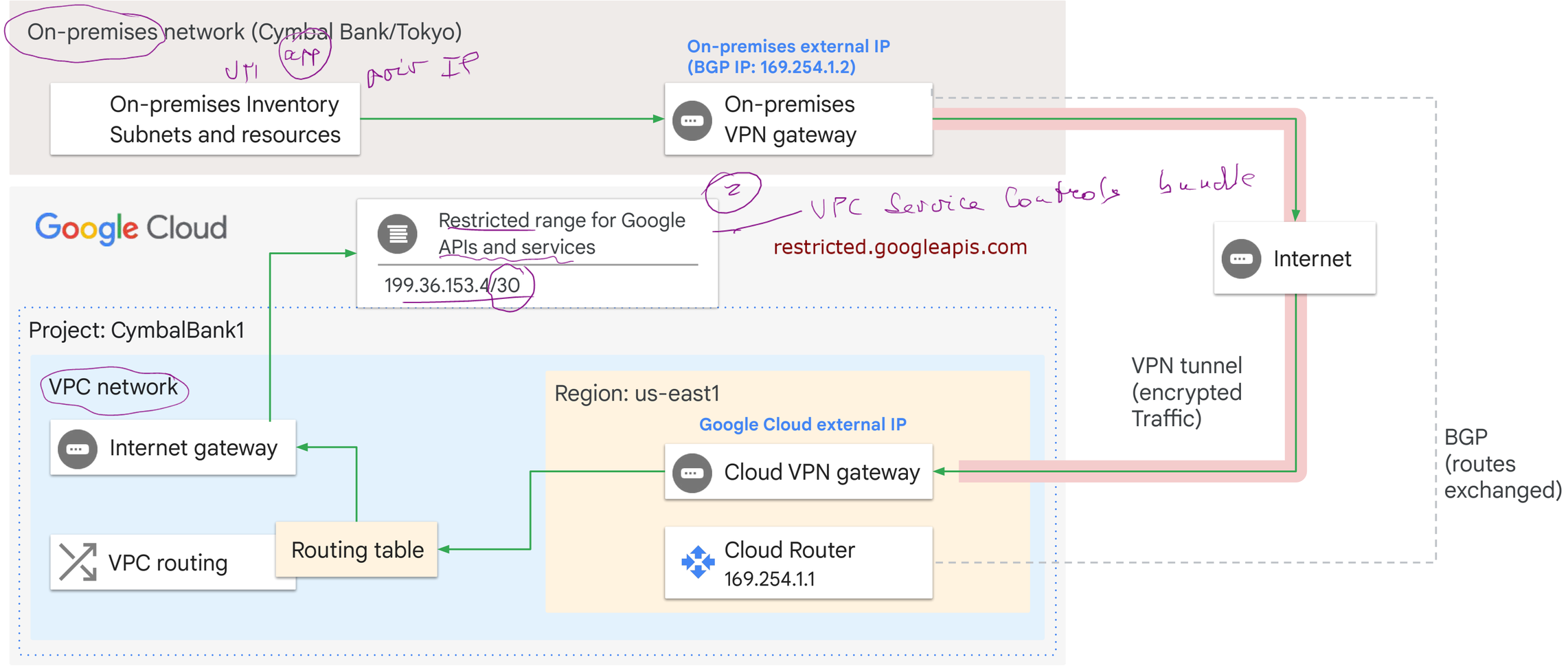



- Securely connecting VMs without external IP addresses to essential Google APIs and services.
- Private Google Access is enabled on a subnet-by-subnet basis.
- If you disable Private Google Access for a subnet, VMs with internal IP addresses can only send traffic within the VPC network.
- Private Google Access has no effect on VMs with external IP addresses.

# Private Google Access Topology



# Private Google Access for on-premises hosts



# Caveats: Private Google Access

- Legacy networks are not supported because they don't support subnets.
- You must enable the Google APIs to use them
- Your VPC network must have appropriate routes and egress firewalls defined.
- If you use the private.googleapis.com or the restricted.googleapis.com domain names, you must create DNS records for them.

# Caveats: Private Google Access that uses IPv6

If you want to use IPv6 to connect to Google APIs and services:

- Your VM must be configured with a /96 IPv6 address range.
- The software running on the VM must send packets whose sources match one of those IPv6 addresses from that range.
- You must send the packets to the IPv6 addresses for the default domains.

# Today's agenda

01 Private access overview

02 Private Google Access

03 Private Service Connect

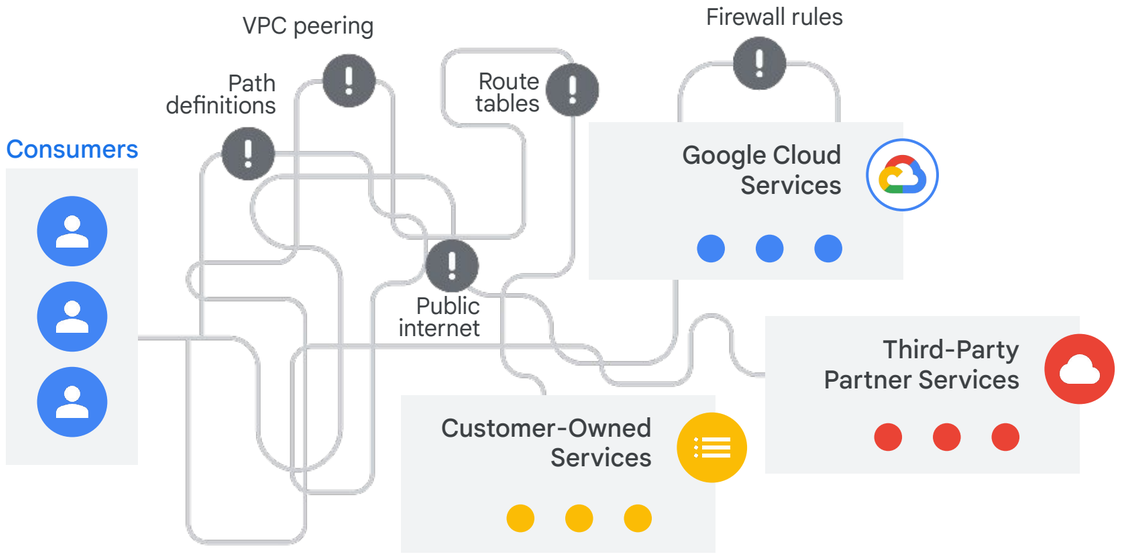
04 Private services access

05 Cloud NAT

06 Lab: Implement Private Google Access with Cloud NAT

07 Quiz

# Use case:  Access managed services privately




Without Private Service Connect

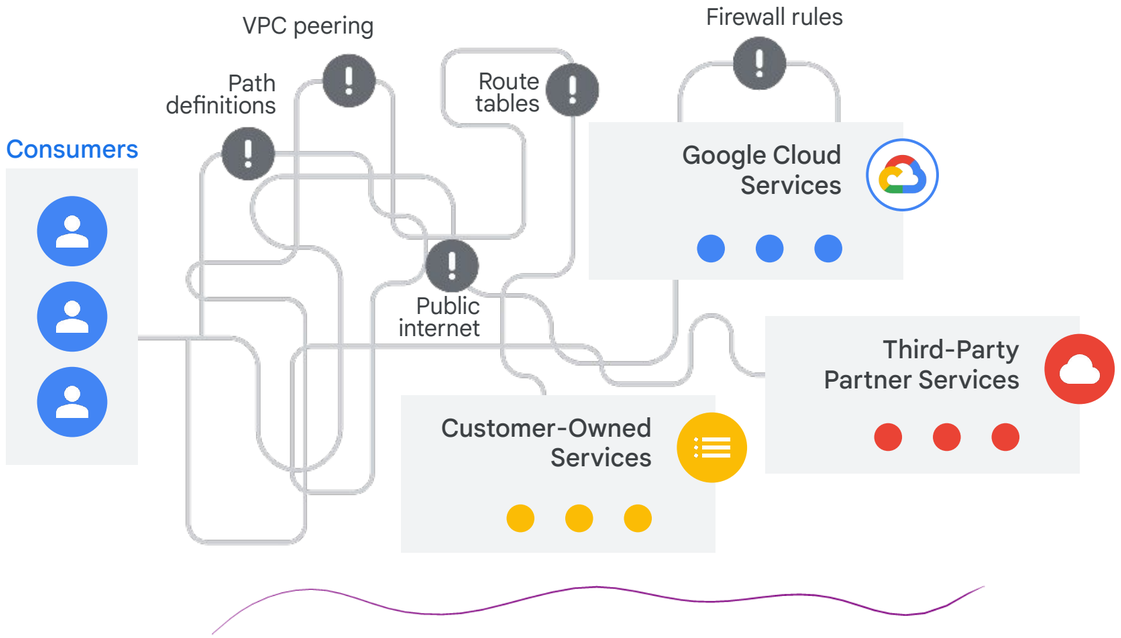
Challenges without PSC

Security

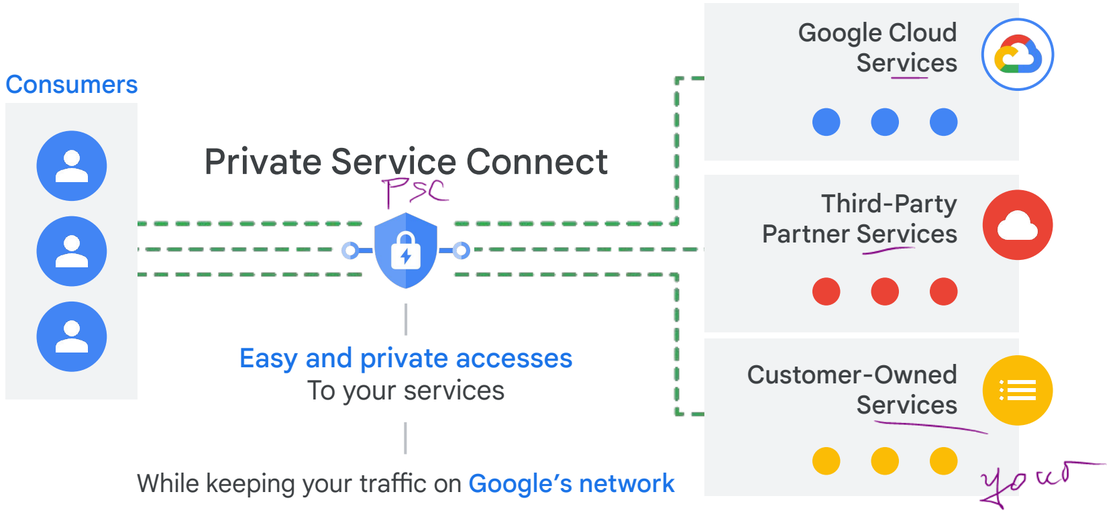
Control

Flexibility

# Use case:  Access managed services privately



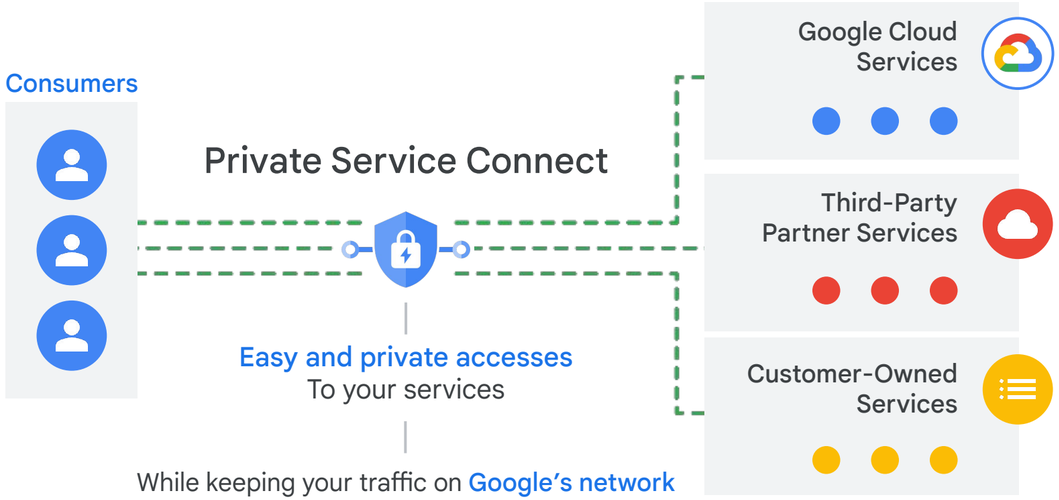

Without Private Service Connect




With Private Service Connect

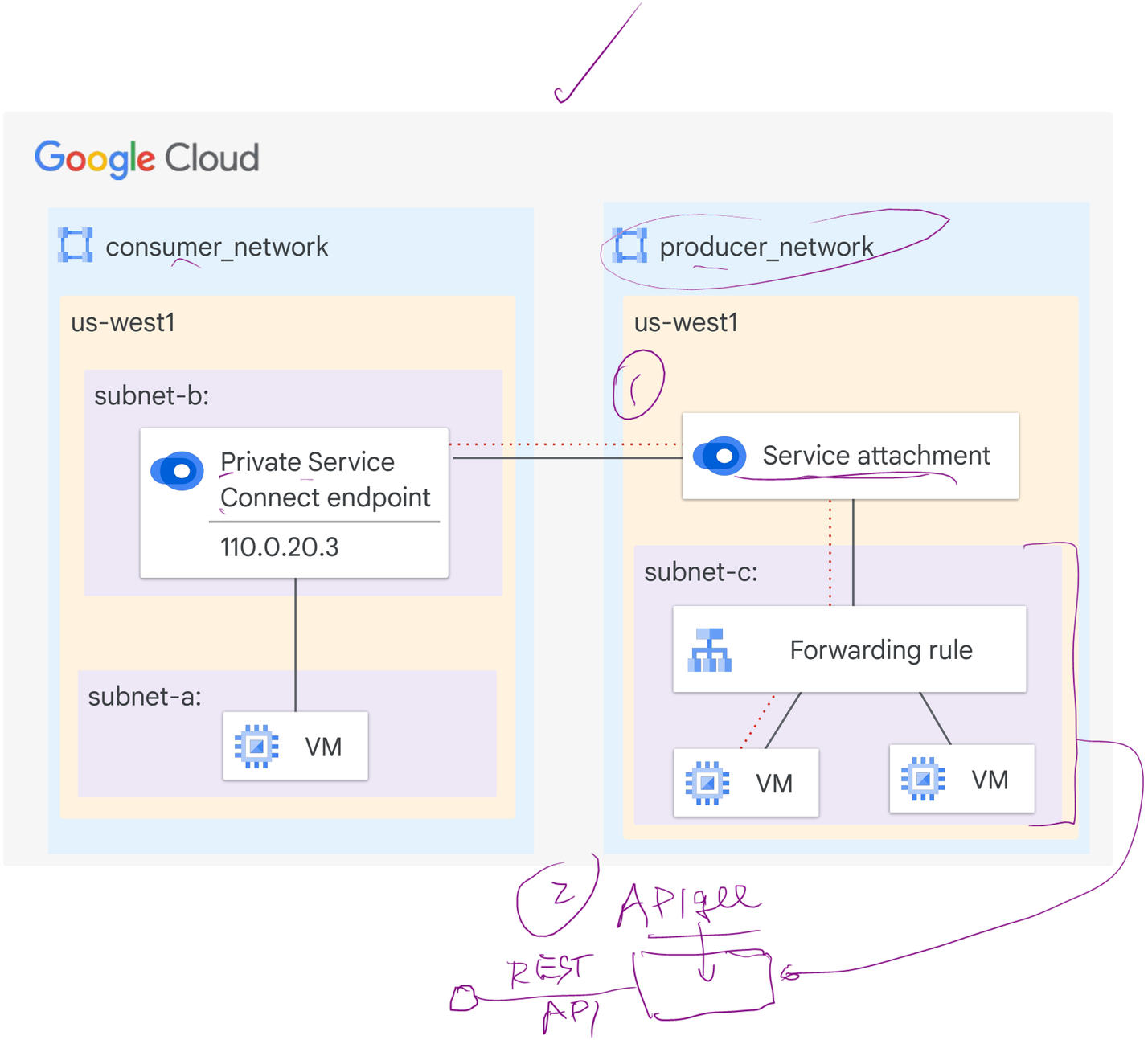
# Private Service Connect

- With Private Google Access, Google APIs and services can be accessed with internal IP addresses.
- With Private Service Connect, third-party resources and intra-organization published services can be also accessed with internal IP addresses.
- You can access resources through a Private Service Connect endpoint or a backend.
- Private Service Connect is fast and scalable.



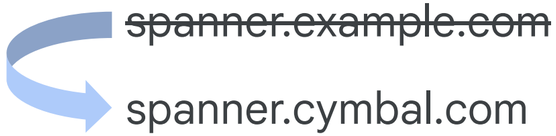
# Using a forwarding rule

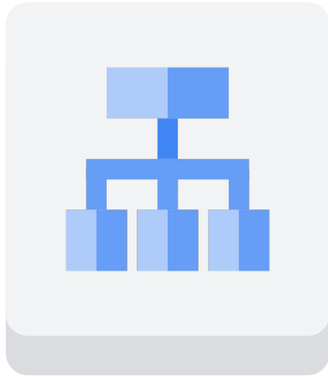
- The service attachment:
  - Receives requests redirected from the Private Service Connect endpoint.
  - Sends them to a forwarding rule.
- The forwarding rule sends the traffic to the correct VM or service.



# Use a load balancer to access PSC service

- Private Service Connect backends let Google Cloud load balancers send traffic through Private Service Connect to reach published services or Google APIs.
- Rename services and map them to URLs of your choice.
- You can configure the load balancer to log all requests to Cloud Logging.



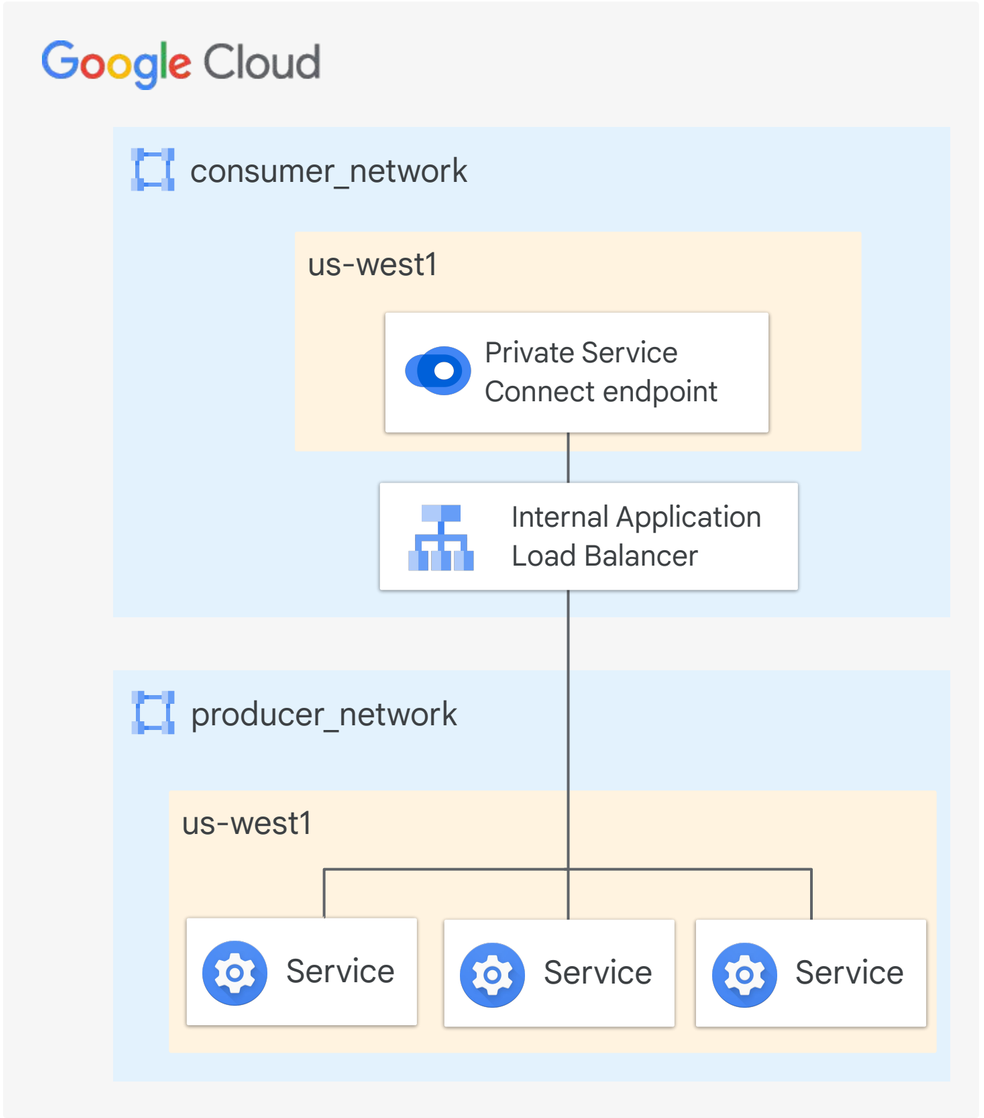



Load balancer

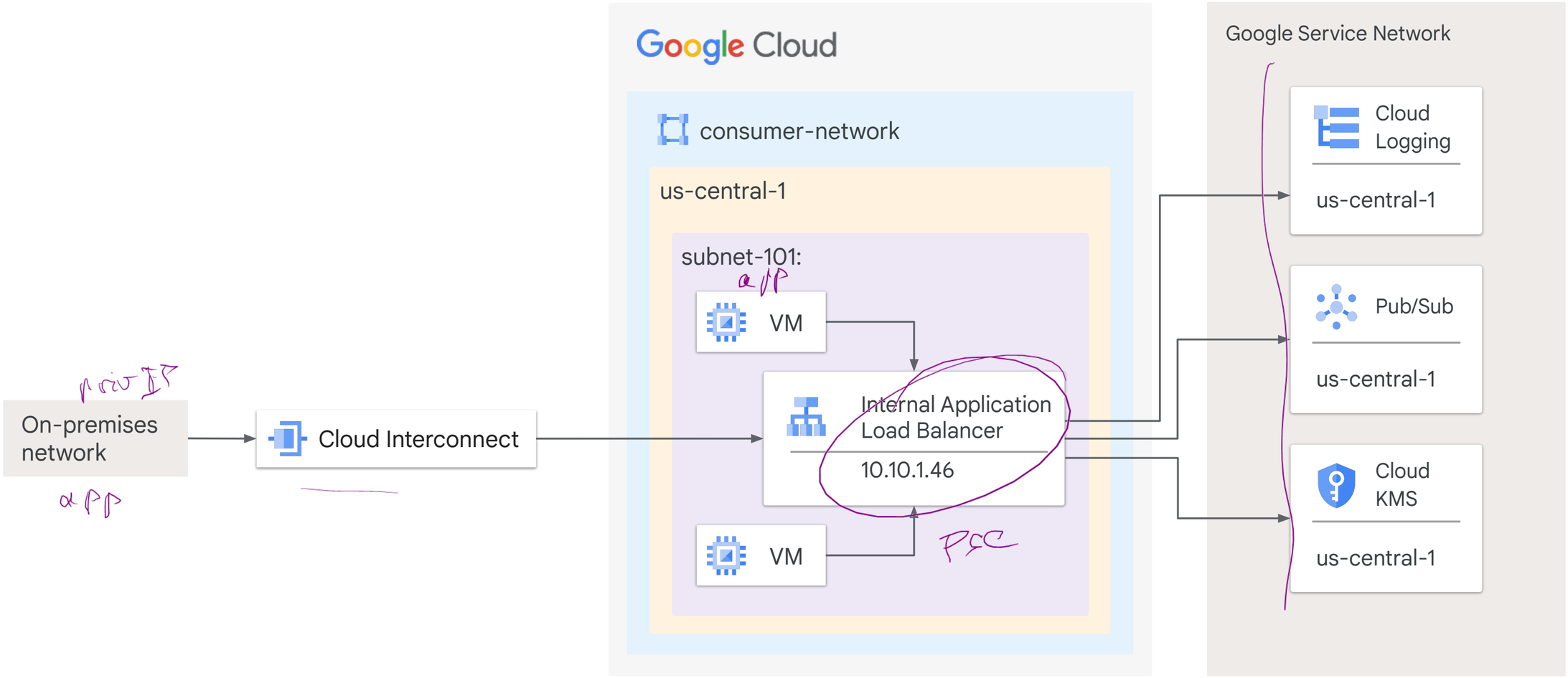
# Using an internal Application Load Balancer

With Private Service Connect and an Application Load Balancer, you can:

- Use a URL map to evaluate requests and route them to the correct VM or service.
- Use customer-managed TLS certificates.
- Enable data residency in-transit by connecting to regional endpoints for Google APIs from workloads in that same region.

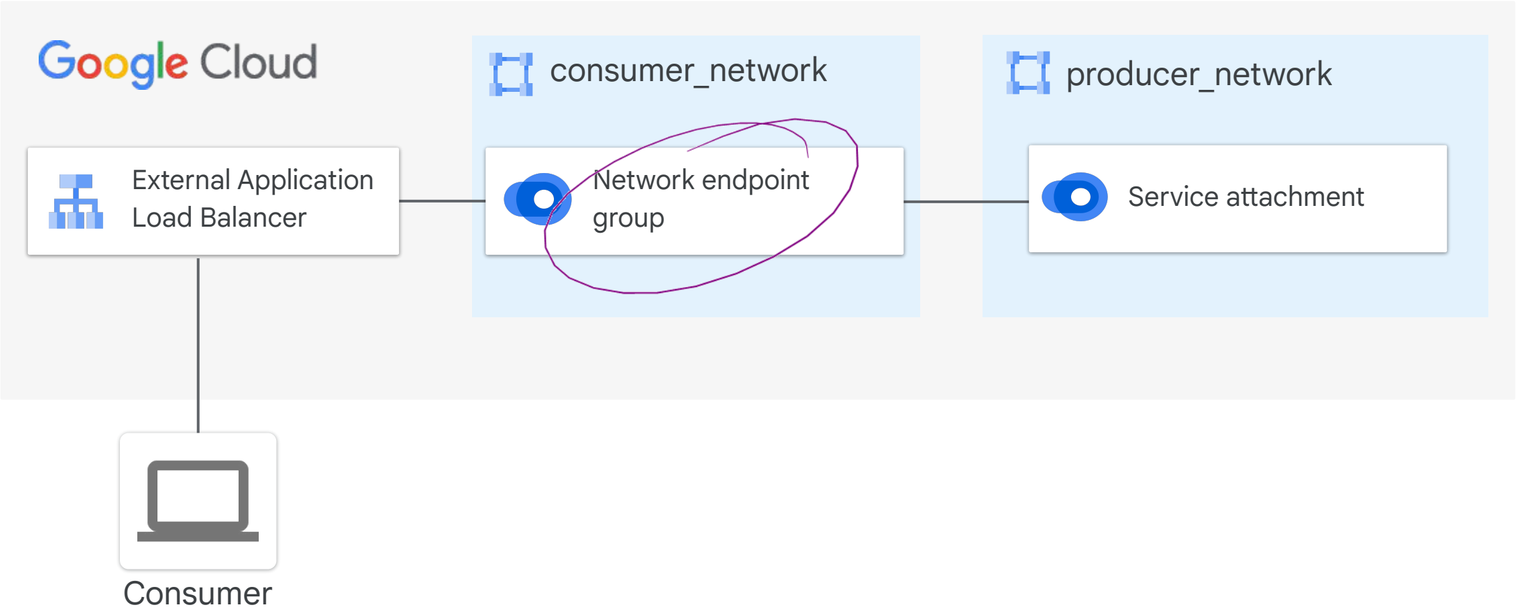


# Sample topology

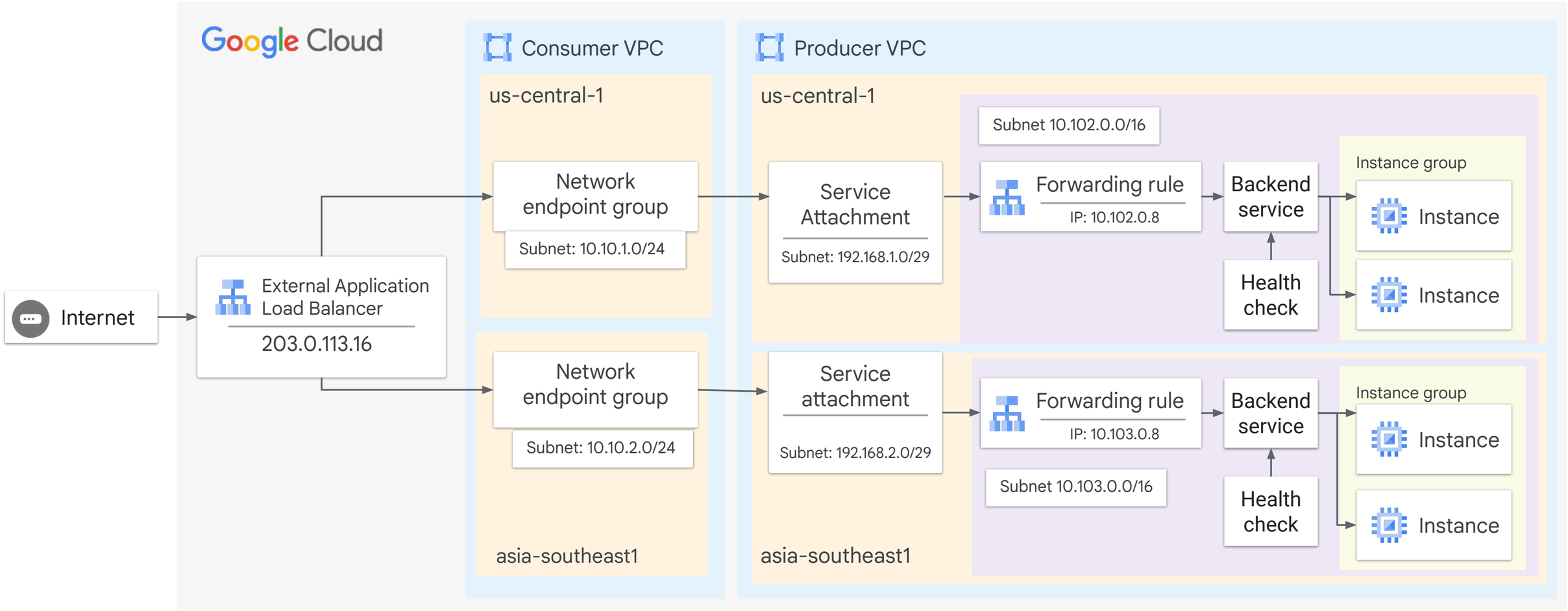


# Using a global external Application Load Balancer

- Consumers connect to an external IP address.
- Private Service Connect uses a network endpoint group to route the request to the service producer.

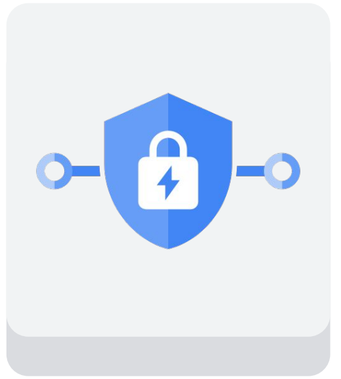


# Sample topology



# General benefits

- Except for the global external Application Load Balancer use case, connections use internal IP addresses.
- Traffic stays on the Google backbone network.
- Configuration is simple.



Private Service Connect

# Benefits for consumers

Consumers:

- Can control the internal IP address that is used to connect to a managed service.
- Do not need to reserve internal IP address ranges for backend services that are consumed in their VPC network.
- Must initiate traffic to the service provider, which improves security.

# Benefits for producers

Producers:

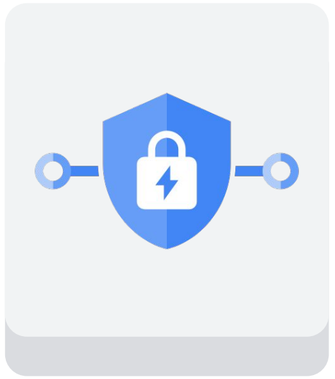
- Can choose to deploy a multi-tenant model, serving multiple consumer VPC networks.
- Can scale services to as many VM instances as required without asking consumers for more IP addresses.
- Don’t need to change firewall rules based on the subnet ranges in the consumer VPC networks.

# Private Service Connect interfaces

A Private Service Connect interface is a special type of network interface that refers to a network attachment.

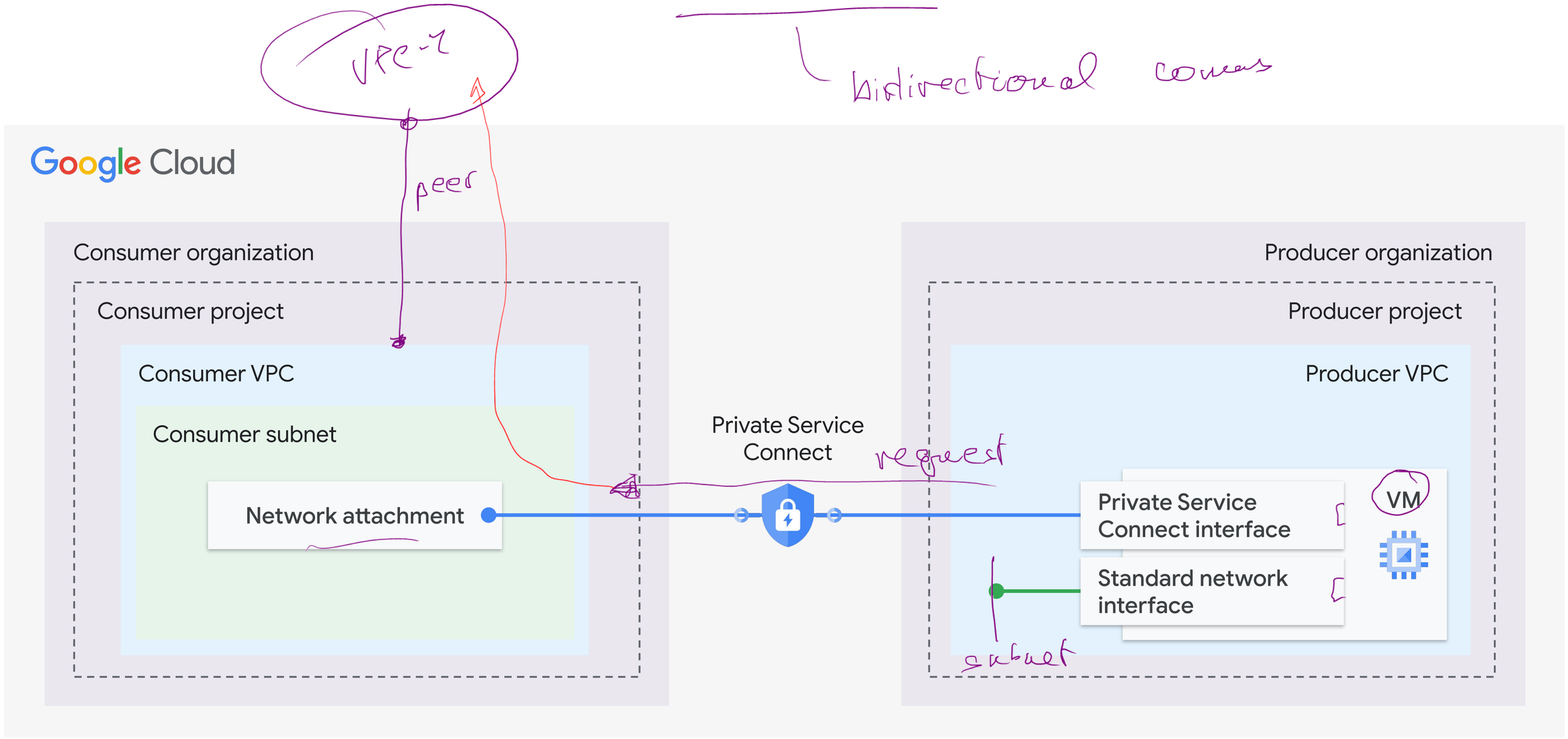
A Private Service Connect Interface enables services in a producer VPC network to securely reach resources and destinations within a consumer VPC network.

Producer and consumer networks can be in different projects and organizations.



Private Service Connect

# Private Service Connect interfaces



# Making Private Service Connect easier to use

A consumer network administrator and a consumer service administrator are working together to get:

- An easier way to configure Private Service Connect.
- The producer network to be able to initiate a connection to the consumer network.

Satisfy both of these needs using service connection policies.

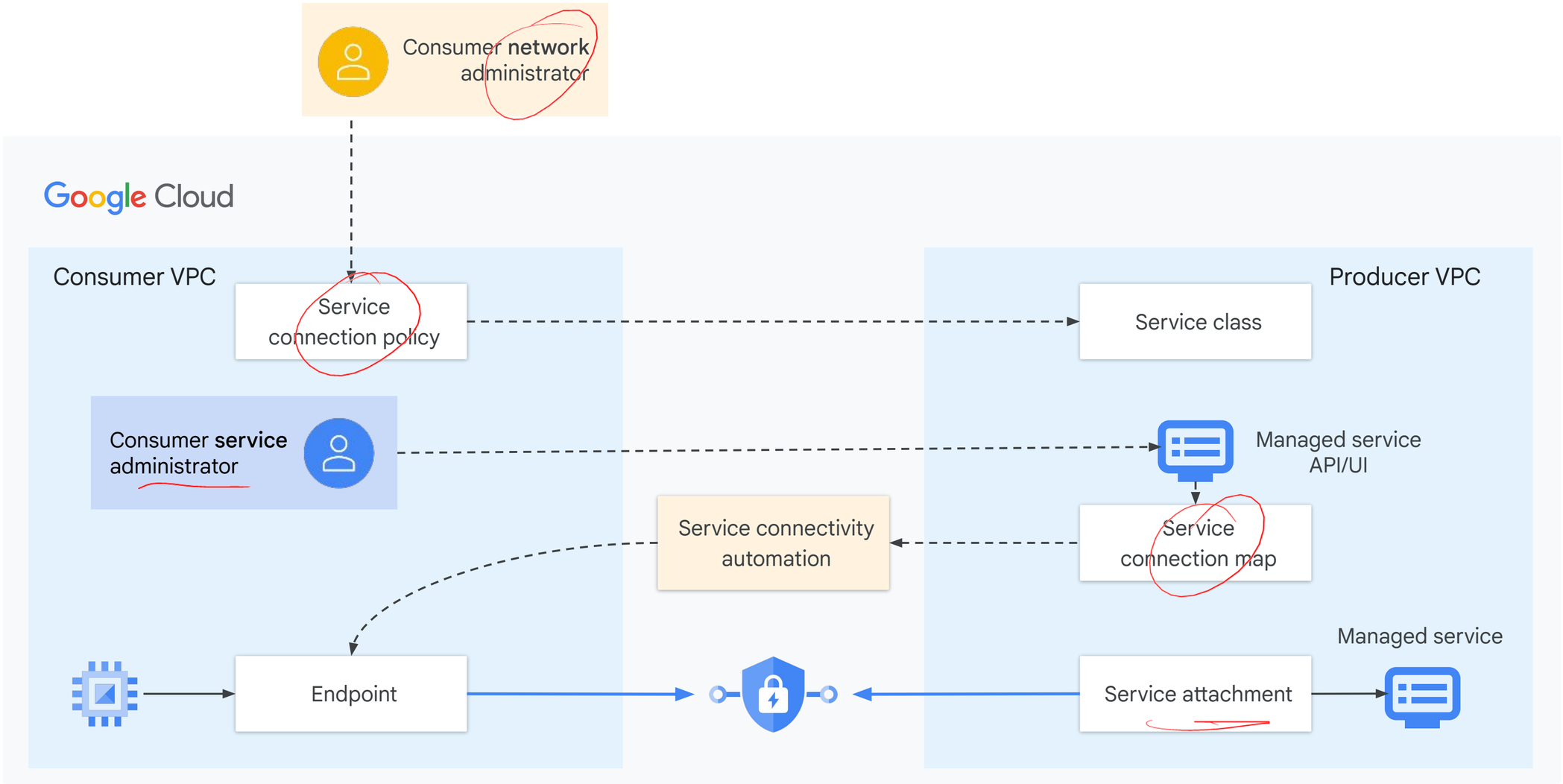
# Using service connection policies

- A regional Google Cloud resource
- Network admins specify producer services
- Consumer service admins can deploy services

Service connection policies have the following fields:

- Service class
- VPC network
- Subnets
- Connection limit

# Service instance deployment

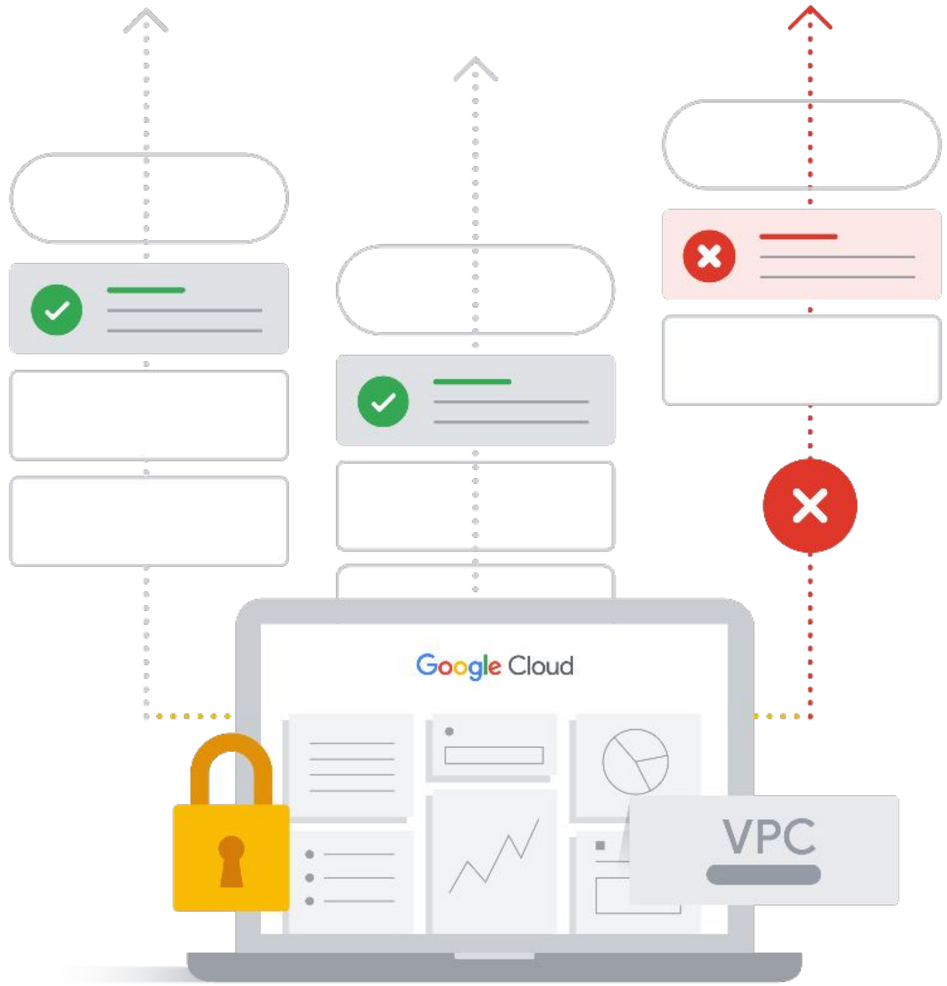


# Caveats: Private Service Connect

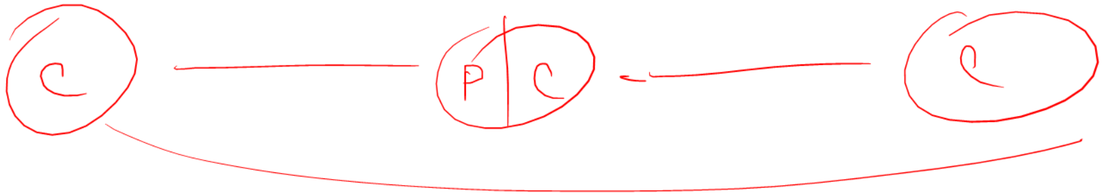
01 You can't create a Private Service Connect endpoint in the same VPC network as the published service that you are accessing.

02 The IP address that you use for the Private Service Connect endpoint counts toward the project quota for global internal IP addresses.

03 Private Service Connect endpoints are not accessible from peered VPC networks.



# Today's agenda




01 Private access overview

02 Private Google Access

03 Private Service Connect

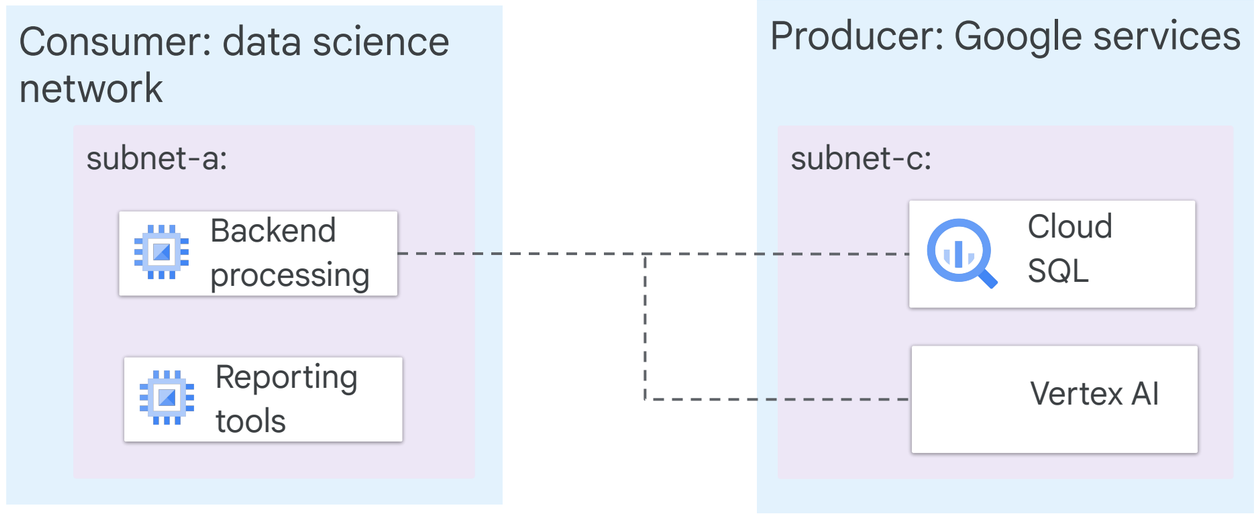
04 **Private services access**

05 Cloud NAT

06 Lab: Implement Private Google Access with Cloud NAT

07 Quiz

# Use case: Connect to specific Google services without an external IP address

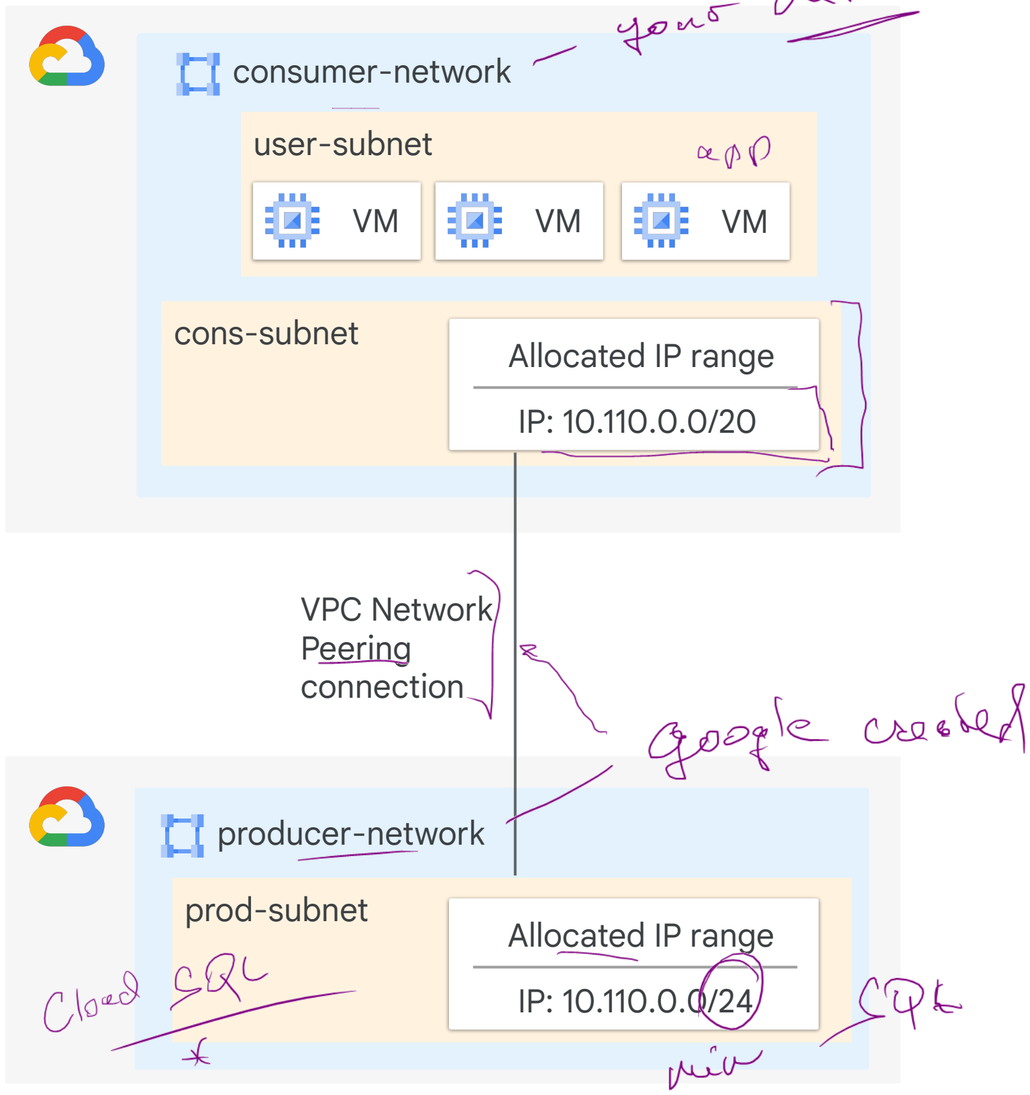



VMs on consumer network have no external IP addresses

# Private services access

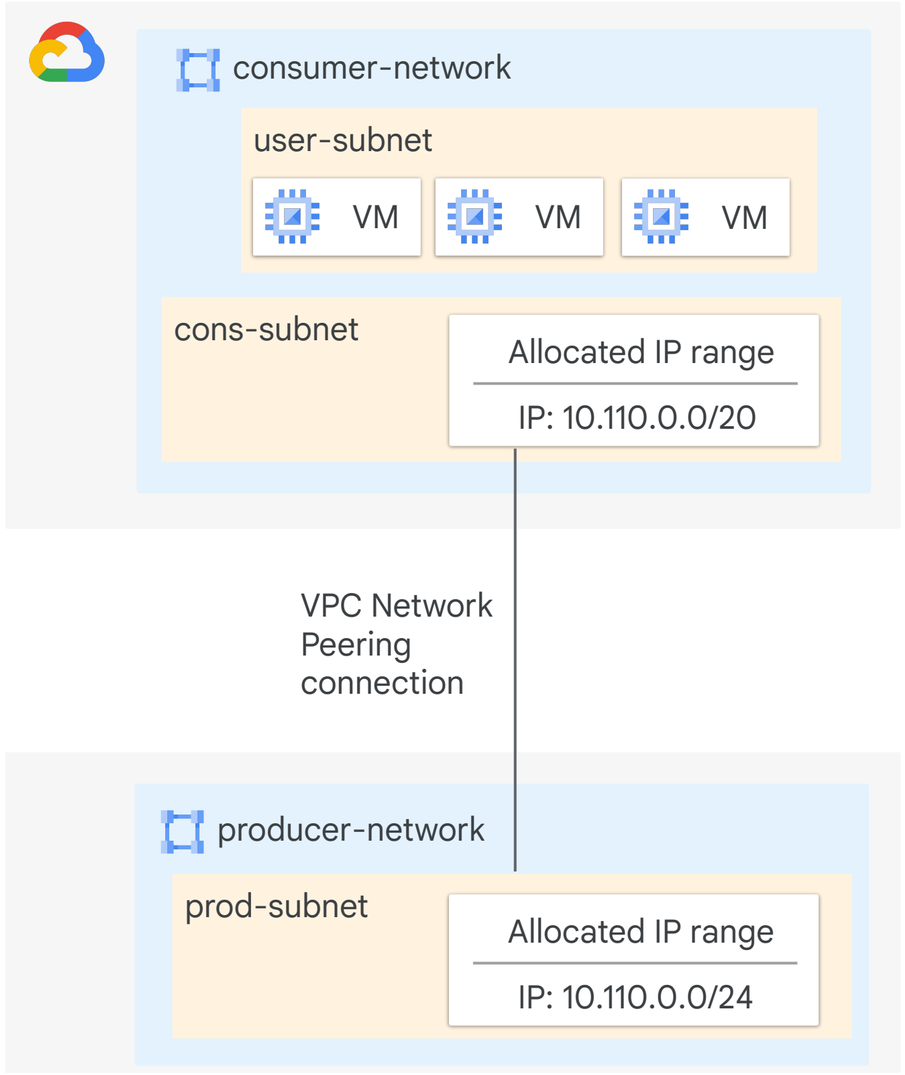
- App Engine Memcache
- Cloud Filestore
- Cloud Memorystore
- Cloud SQL

- Uses internal IPv4 addresses.
- Uses VPC Network Peering to connect consumer and producer VPC networks.
- Automates much of the VPC Network Peering configuration.
- Doesn't require explicitly importing and exporting routes.
- Is only available for some producer services, like Apigee, Cloud SQL, and Cloud TPU.



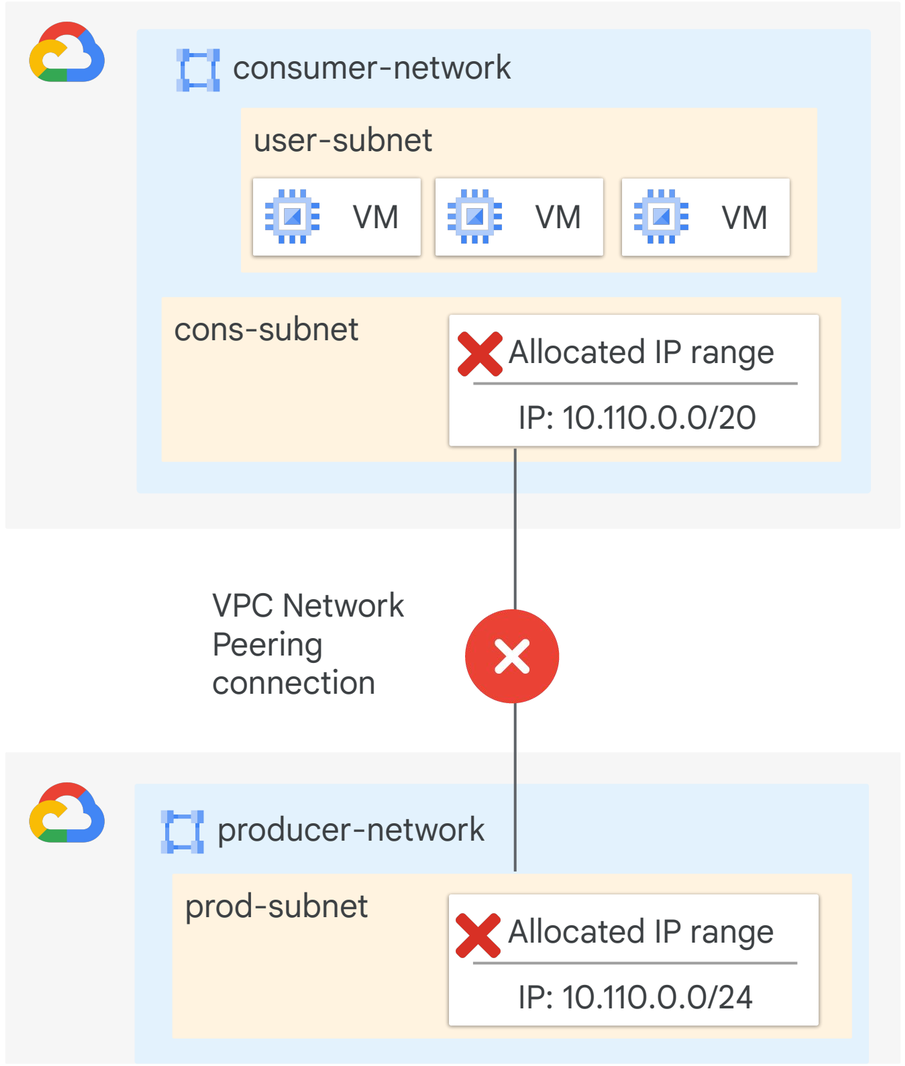
# Configuring private services access

- The service producer and consumer must activate the Service Networking API in their projects.
- Service producers must allocate an IPv4 address range in the VPC network that contains the service.
- Consumers must:
  - Allocate an IPv4 address range in their VPC network.
  - Create a private connection to a service producer.

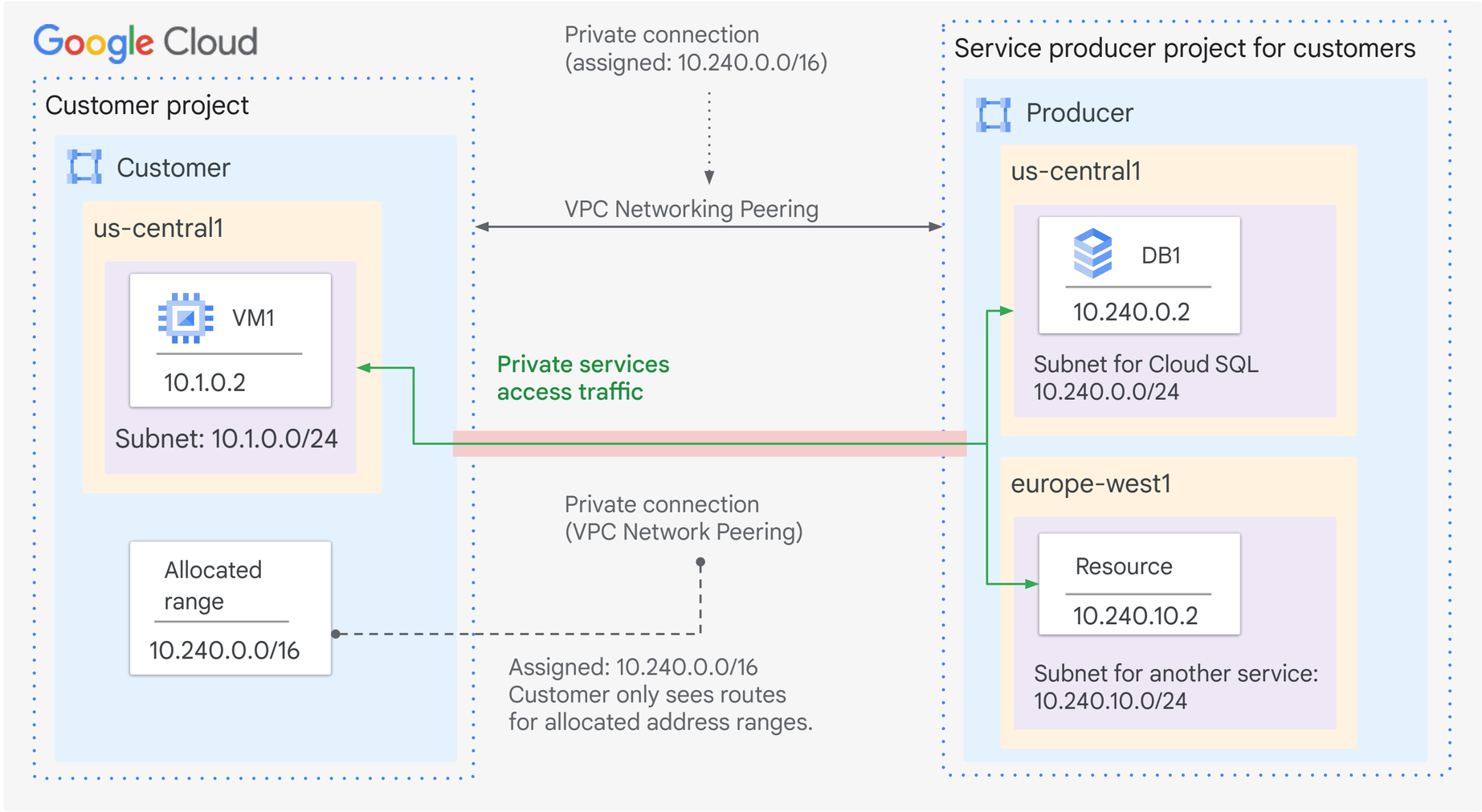


# Deleting the connection

- Consumers can disable the private services access connection between their VPC network and the producer VPC network.
- Disabling the connection does not:
  - Delete the VPC Network Peering connection.
  - Release the IPv4 address range.



# Sample topology



# Caveats: Private services access

01 If you connect on-premises networks, you must export the routes to the VPC producer network.

02 Not all Google services are supported.

03 The same quota and limits that apply to VPC Network Peering also apply to private services access.

# A quick summary

| Private Google Access | Private Service Connect | Private service access |
| --- | --- | --- |
| Helps VMs reach Google services with an internal IP address. | Helps expose *your* / Google-produced / third-party services to others. | Reaches producer services privately. |

# Today's agenda

01 Private access overview

02 Private Google Access

03 Private Service Connect

04 Private services access

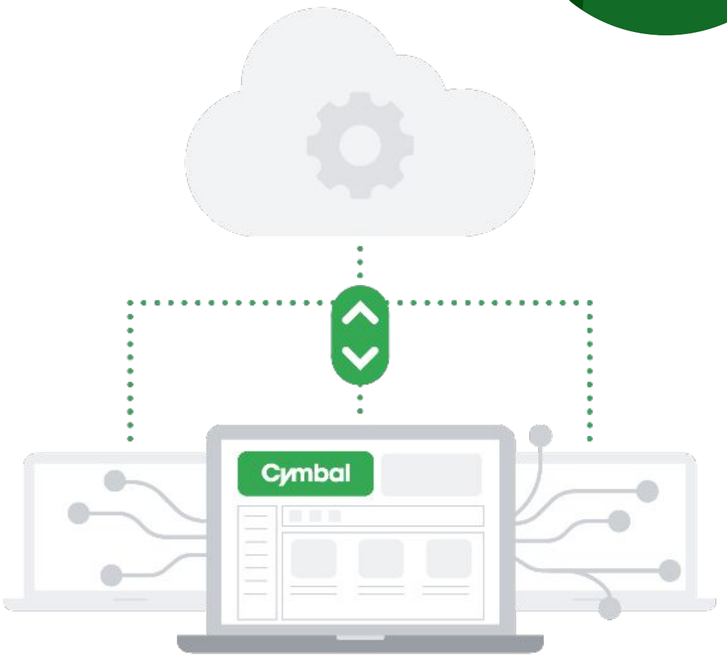
05 Cloud NAT

06 Lab: Implement Private Google Access with Cloud NAT

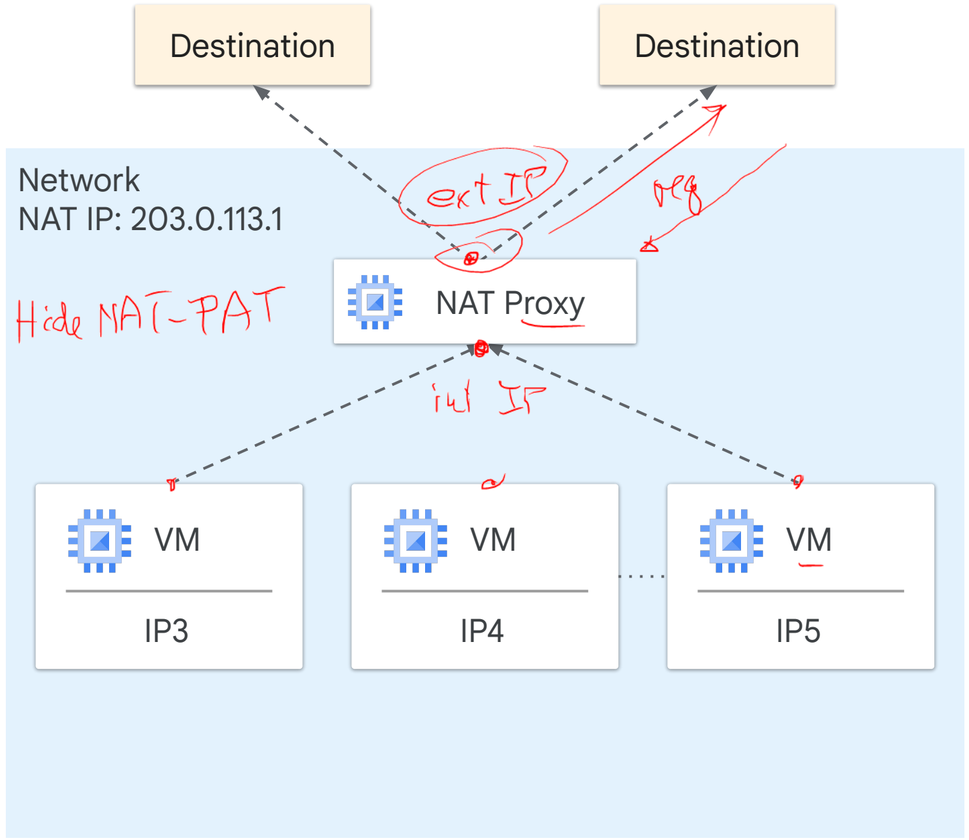
07 Quiz

# Use case: Allow access to internet without a public IP address

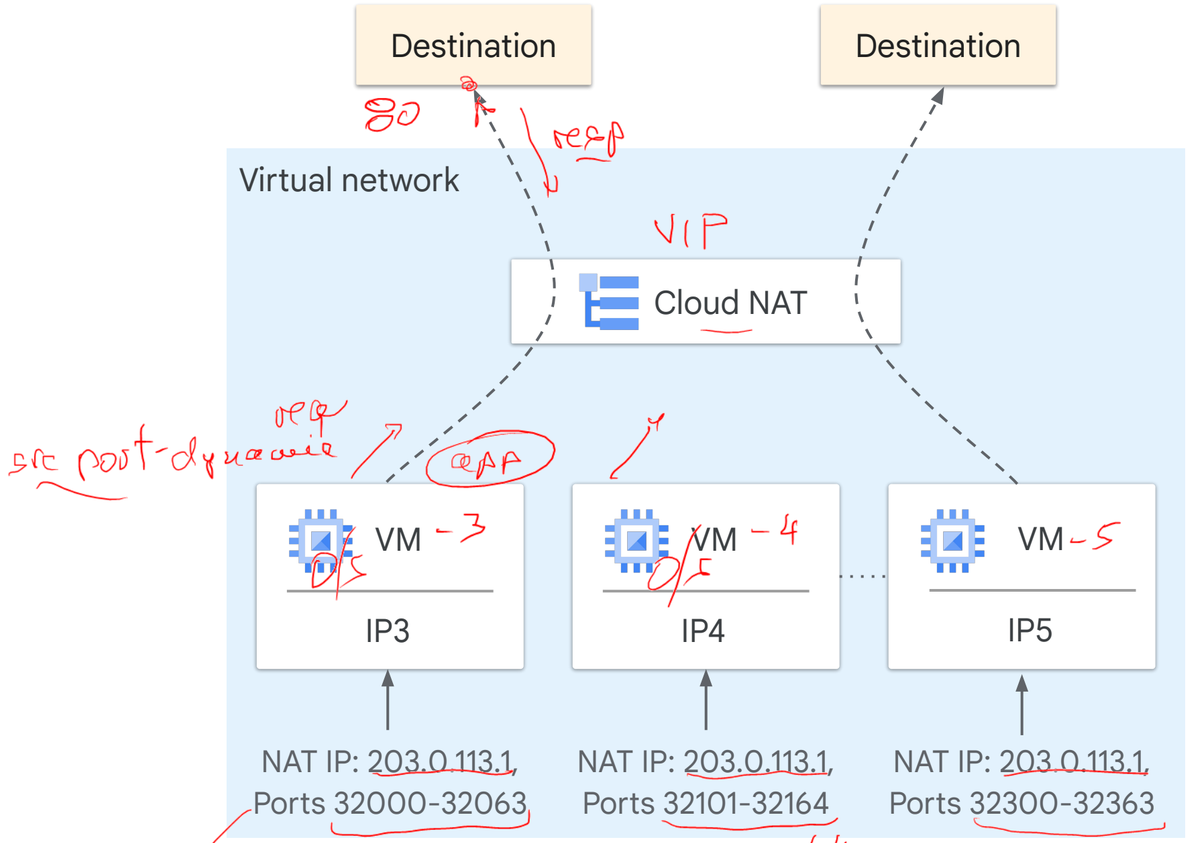
- Cymbal has several non-production environments (development, testing, staging) on Google Cloud.
- These environments host various VMs that need occasional outbound internet access for tasks such as:
  - Downloading software updates and dependencies.
  - Accessing external testing tools or resources.



# Cloud NAT is a fully managed, software-defined service

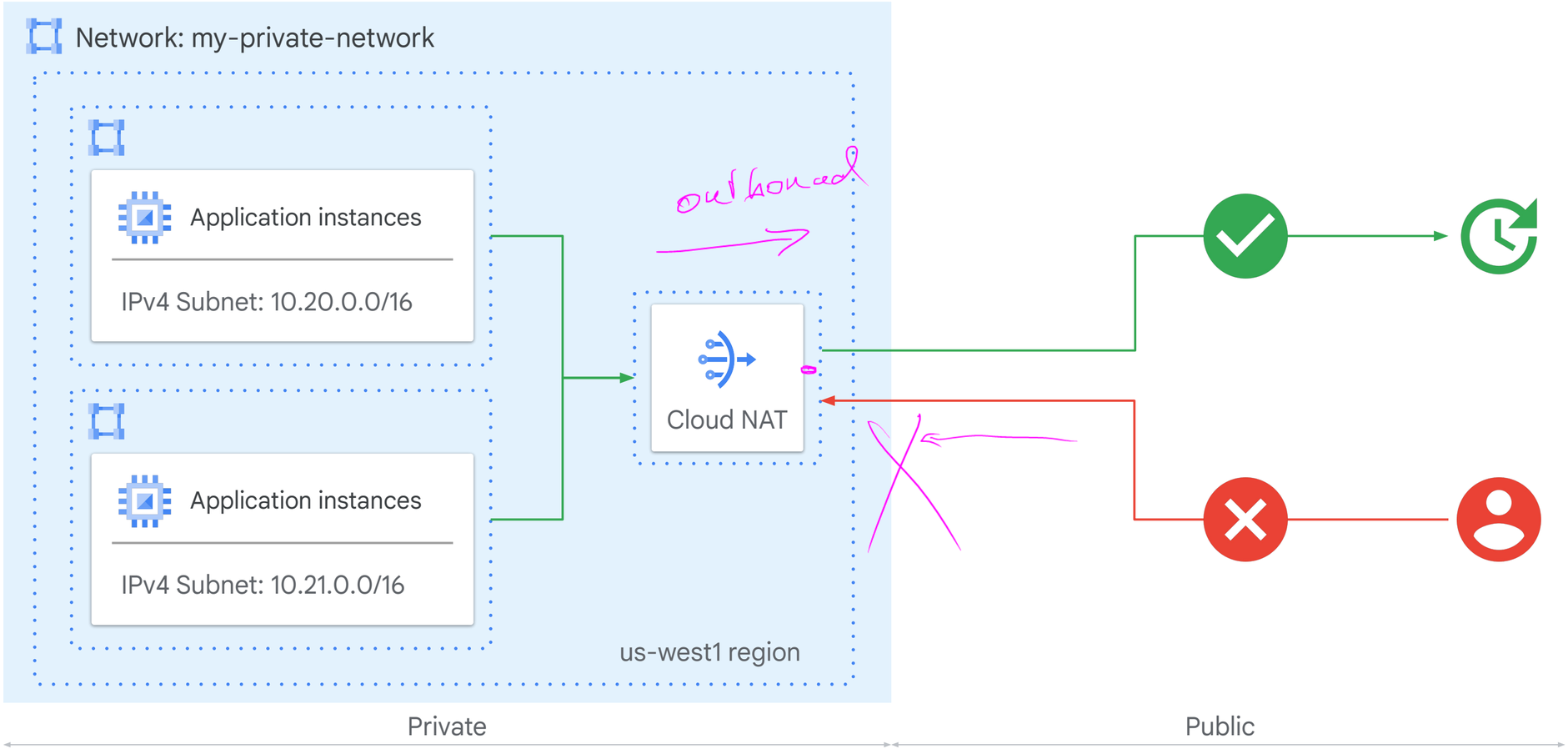



1. Typical NAT proxies



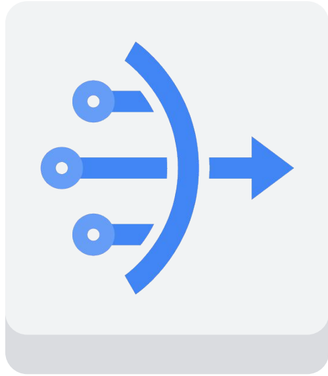

2. Cloud NAT

# Cloud NAT provides internet access to private instances



# Benefits of Cloud NAT

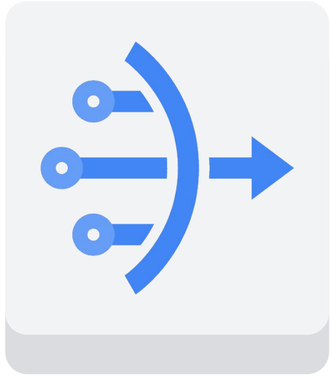
- Reduces the need for individual VMs to each have external IP addresses.
- Automatically scales the number of NAT IP addresses that it uses.
- Is not dependent on a single physical gateway device.



Cloud NAT

# How Cloud NAT works with Private Google Access

- Cloud NAT never performs NAT for traffic that is sent to the select external IP addresses for Google APIs and services.
- When you configure a Cloud NAT gateway to apply to a subnet range, Google Cloud automatically enables Private Google Access for that range.
- If the gateway provides NAT for a subnet range, Private Google Access can't be disabled manually.



Cloud NAT

# Types of Cloud NAT

## Public NAT

- Enables your private resources (without public IPs) to access the internet.
- Shares a pool of public IP addresses, assigning them as needed for secure outbound connections.

## Private NAT

- Facilitates private communication between different networks.
- Inter-VPC NAT: Translates addresses between VPCs connected to a central hub.

# Let’s ask Gemini

How can I use private service access to connect my VMs to third-party services?

Sure, here are the steps on how you can use private service access to connect your VMs to third-party services:

...

1.Enable the Private Service Access API.

2.Create a service attachment.

- gcloud services attachments create my-service-attachment \
- --project=my-project \
- --region=us-central1 \
- --network=my-network \
- --service=serviceproducer.googleapis.com

# Today's agenda

01 Private access overview

02 Private Google Access

03 Private Service Connect

04 Private services access

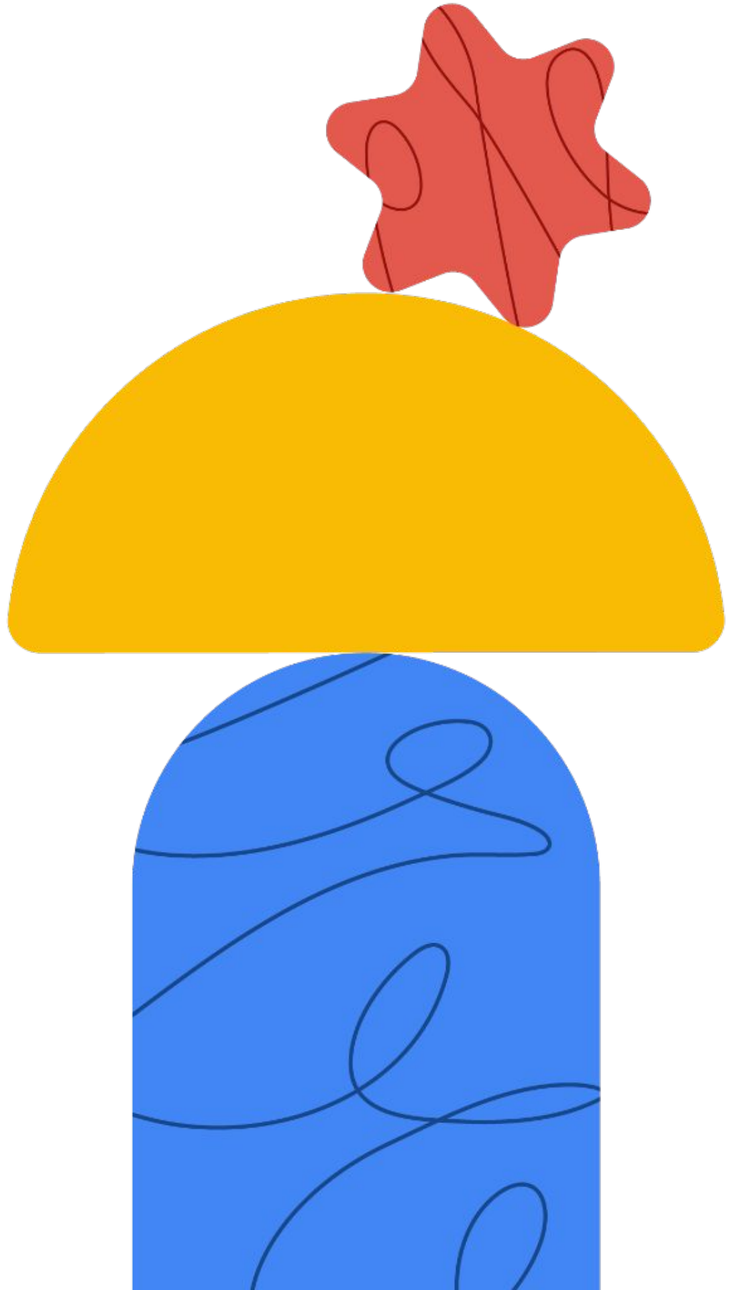
05 Cloud NAT

06 Lab: Implement Private Google Access with Cloud NAT

07 Quiz

# Lab intro

Implement Private Google Access and Cloud NAT



# Today's agenda

01 Private access to Google APIs and services

02 Private Google Access

03 Private Service Connect

04 Cloud NAT

05 Lab: Implement Private Google Access and Cloud NAT

06 Quiz

# Quiz | Question 1

## Question

You want to provide access to services that you created in a VPC network. The services should be available to other specified VPC networks through endpoints that have internal IP addresses. Some of these VPC networks have subnets with overlapping internal IP addresses. Which product can you use?

A. Private Google Access

B. Private services access

C. Private Service Connect

D. Cloud NAT

# Quiz | Question 1

## Answer

You want to provide access to services that you created in a VPC network. The services should be available to other specified VPC networks through endpoints that have internal IP addresses. Some of these VPC networks have subnets with overlapping internal IP addresses. Which product can you use?

A. Private Google Access

B. Private services access

C. Private Service Connect 

D. Cloud NAT

# Quiz | Question 2

## Question

To enable Private Google Access for a VPC network:

A. Enable it on the VPC network.

B. Enable it on all desired subnets in the VPC network.

C. Enable it on all desired subnets and on Cloud Router.

D. Enable it on the VPC network, on the desired subnets, and on Cloud Router.

# Quiz | Question 2

## Answer

To enable Private Google Access for a VPC network:

A. Enable it on the VPC network.

B. Enable it on all desired subnets in the VPC network. 

C. Enable it on all desired subnets and on Cloud Router.

D. Enable it on the VPC network, on the desired subnets, and on Cloud Router.

# Quiz | Question 3

## Question

Private services access automatically configures which Google Cloud product to implement communication between the producer and consumer VPC networks?

A. Shared VPC

B. VPC Network Peering

C. Private Google Access

D. Cloud NAT

# Quiz | Question 3

## Answer

Private services access automatically configures which Google Cloud product to implement communication between the producer and consumer VPC networks?

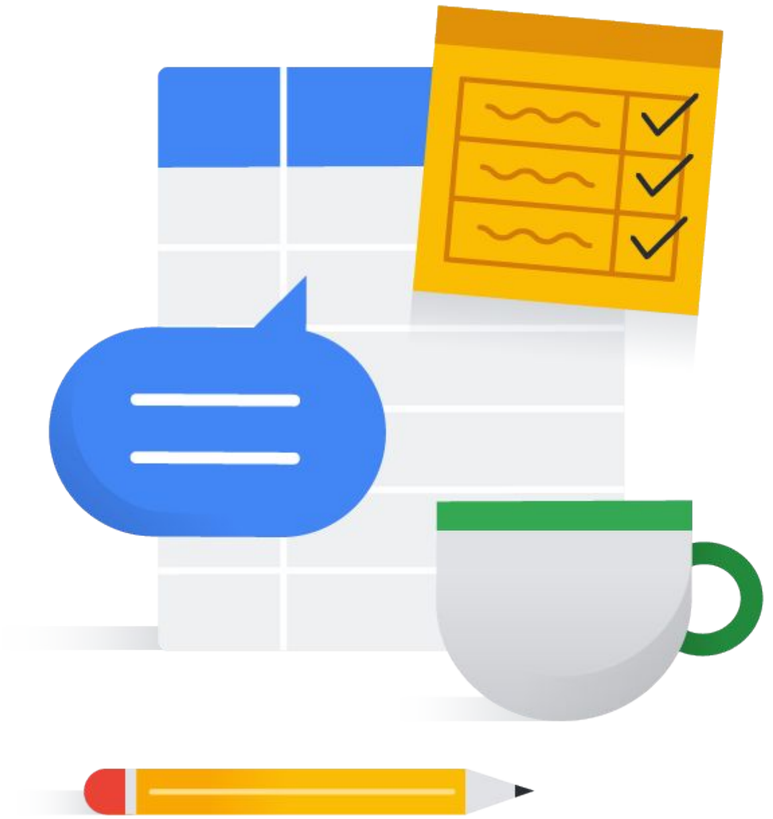
A. Shared VPC

B. VPC Network Peering 

C. Private Google Access

D. Cloud NAT

# Debrief



Thank you.