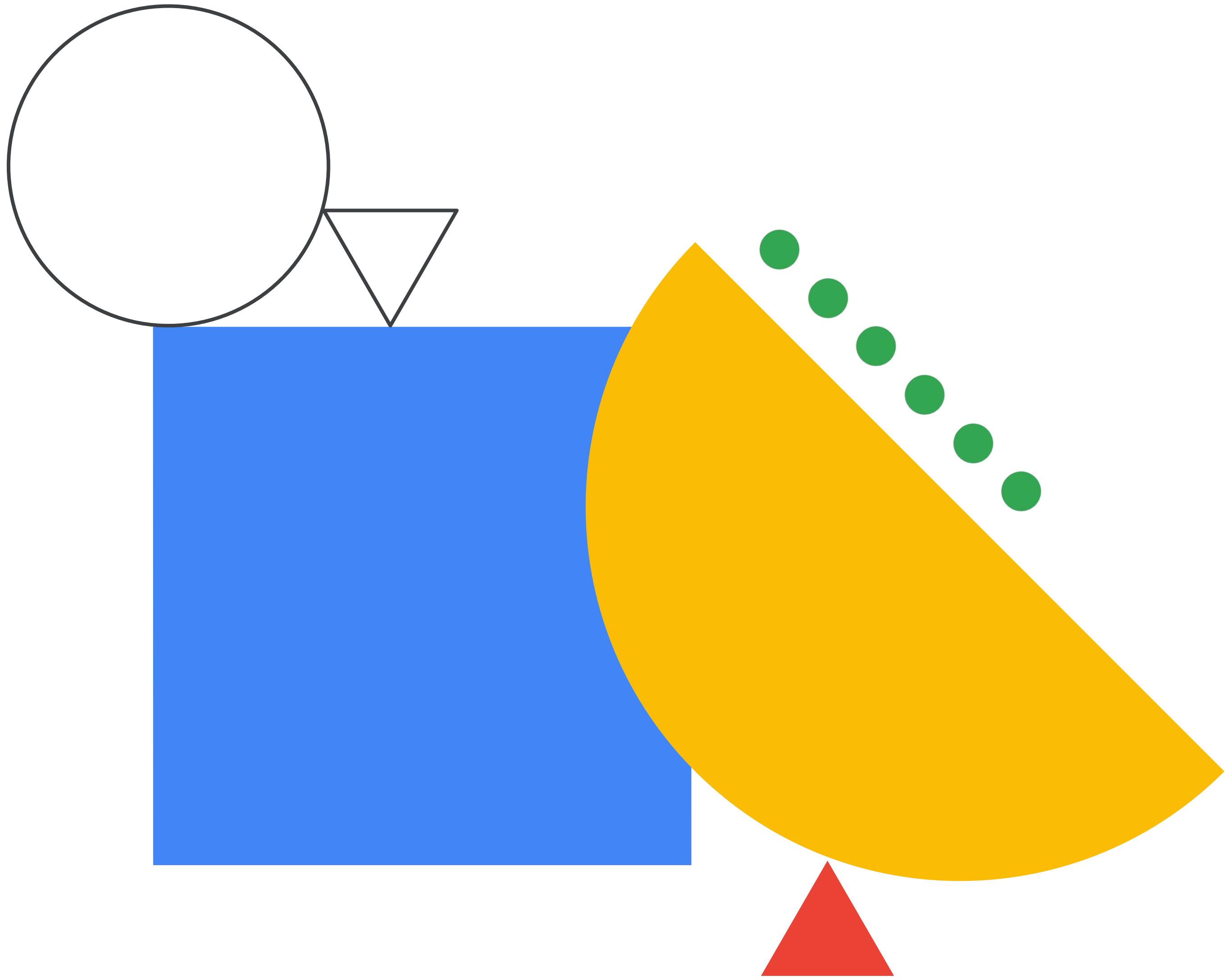
Google Cloud

Virtual Networks



Agenda

01 Virtual Private Cloud (VPC)

02 Projects, Networks, and Subnetworks

03 IP Addresses

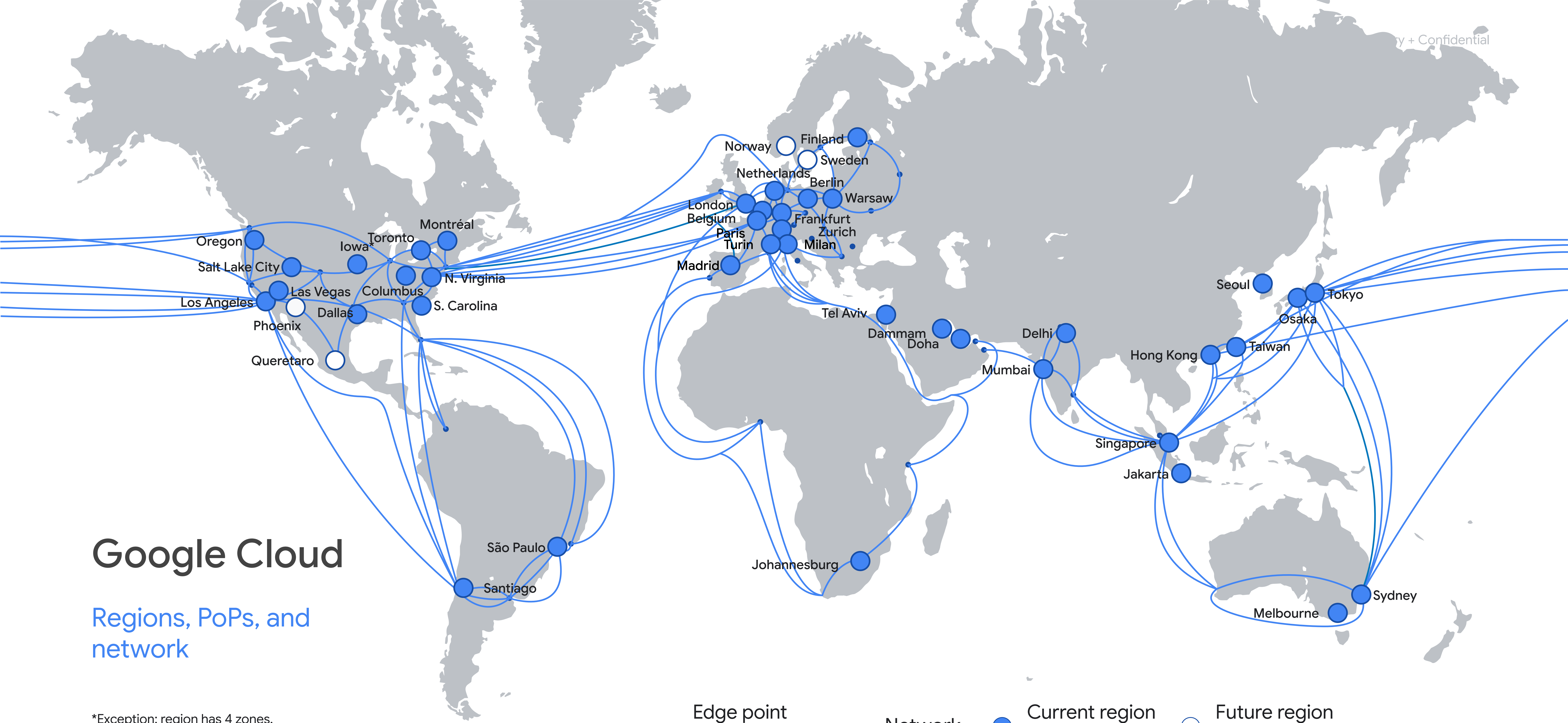
04 Routes and Firewall Rules

05 Pricing

Lab: VPC Networking

06 Common Network Designs

Lab: Implement Private Google Access and Cloud NAT



Google Cloud

Regions, PoPs, and network

*Exception: region has 4 zones.

• Edge point of presence

— Network

● Current region with 3 zones

○ Future region with 3 zones

https://cloud.google.com/about/locations/

01

Virtual Private Cloud (VPC)

VPC objects

Virtual Private Cloud

- Projects
- Networks
  - Default, auto mode, custom mode
- Subnetworks
- Regions
- Zones

- IP addresses
  - Internal, external, range
- Virtual machines (VMs)
- Routes
- Firewall rules

02

Projects, Networks, and Subnetworks

Projects and networks

A project:

- Associates objects and services with billing.
- Contains networks (up to 15) that can be shared/peered.

A network:

- Has no IP address range.
- Is global and spans all available regions.
- Contains subnetworks.
- Is available as default, auto, or custom.

3 VPC network types

Default

- Every project
- One subnet per region
- Default firewall rules

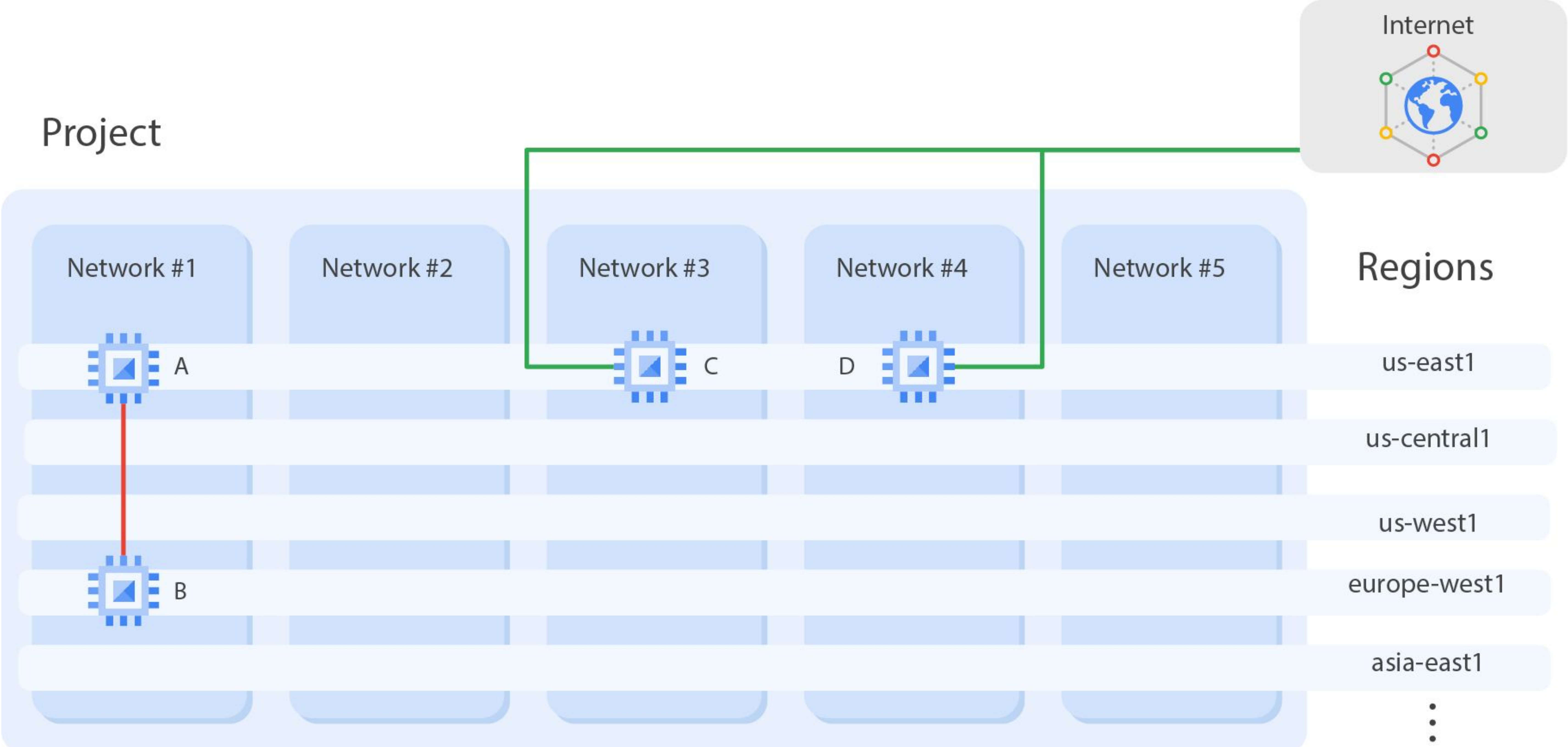
Auto Mode

- Default network
- One subnet per region
- Regional IP allocation
- Fixed /20 subnetwork per region
- Expandable up to /16

Custom Mode

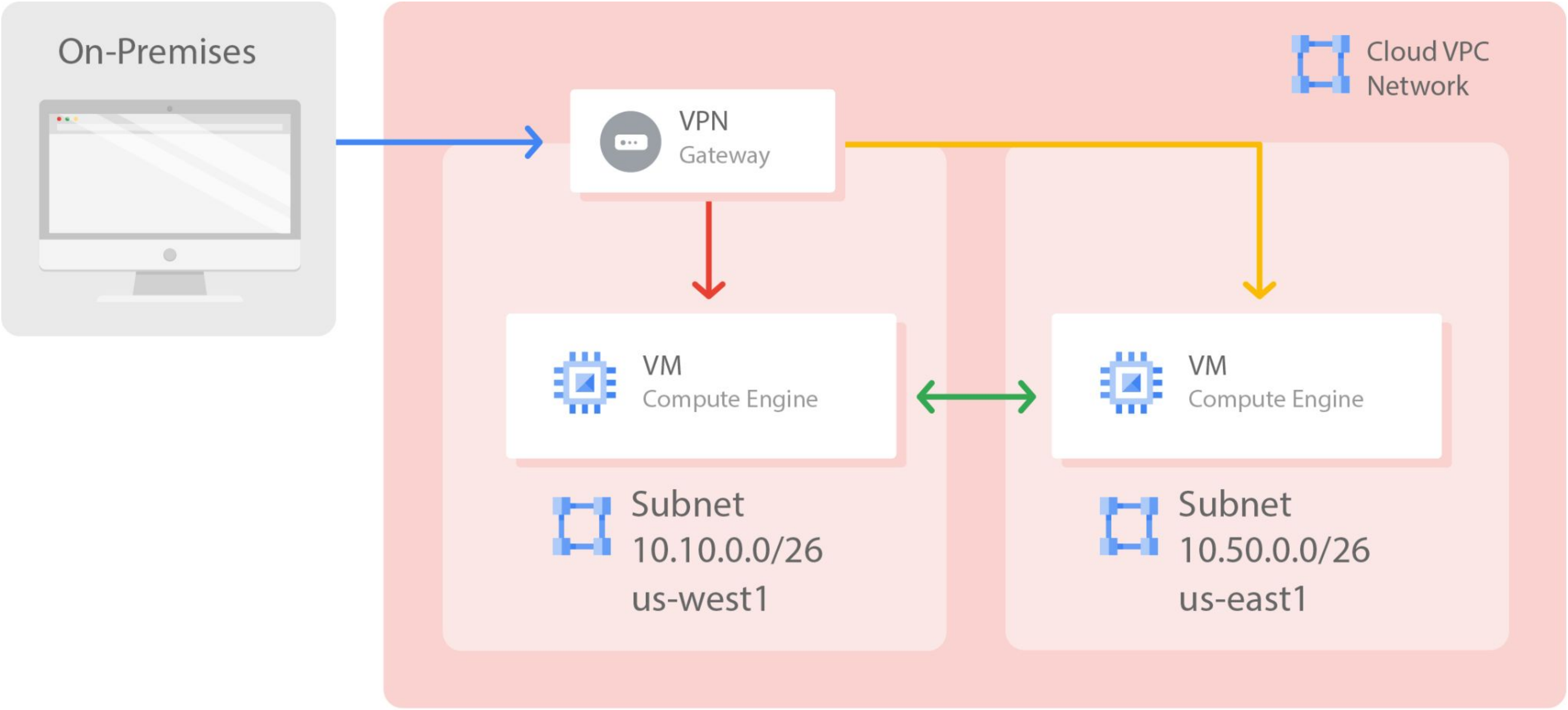
- No default subnets created
- Full control of IP ranges
- Regional IP allocation
- Expandable to IP ranges you specify

Networks isolate systems

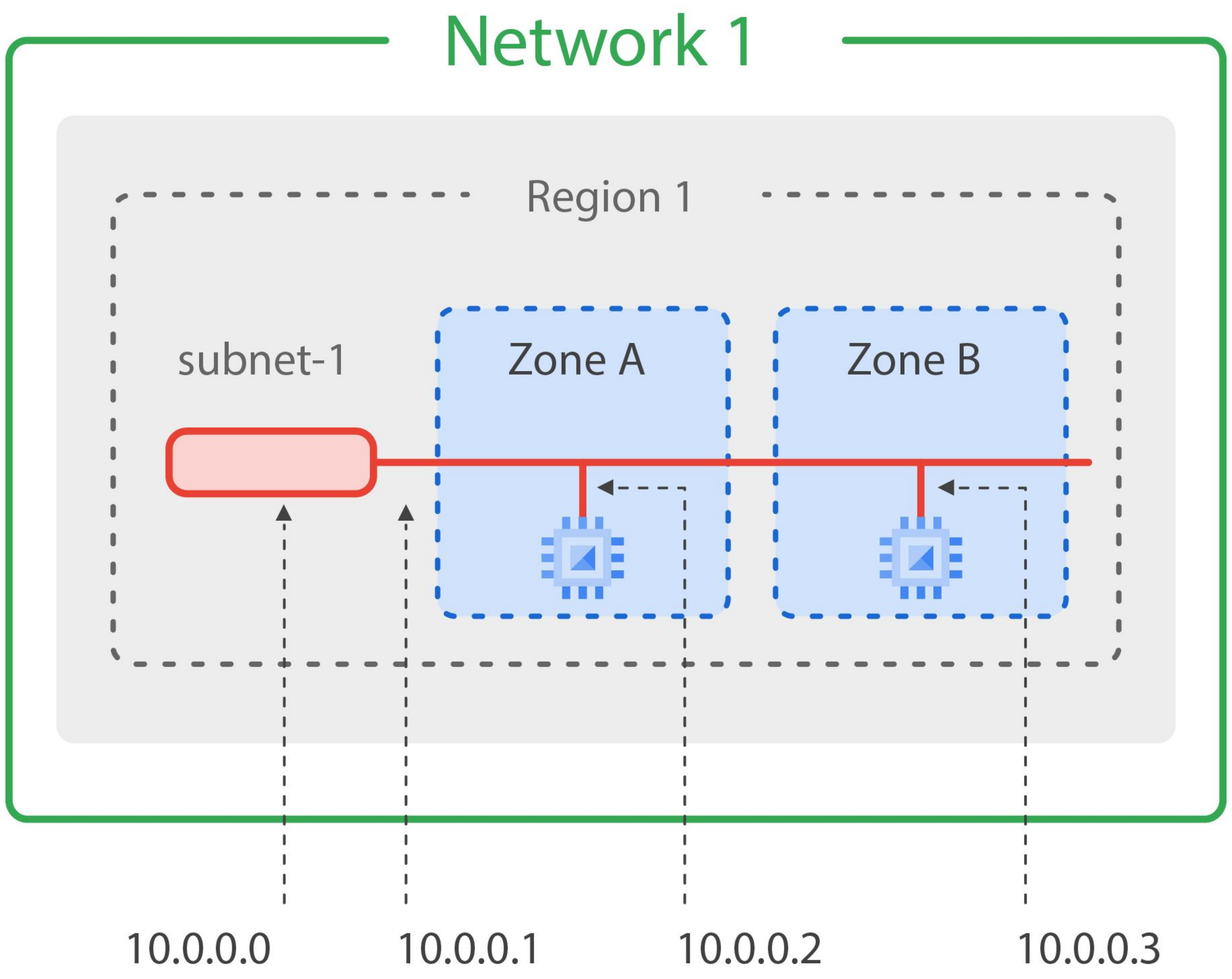


- **A** and **B** can communicate over internal IPs *even though they are in different regions.*
- **C** and **D** must communicate over external IPs *even though they are in the same region.*

Google's VPC is global



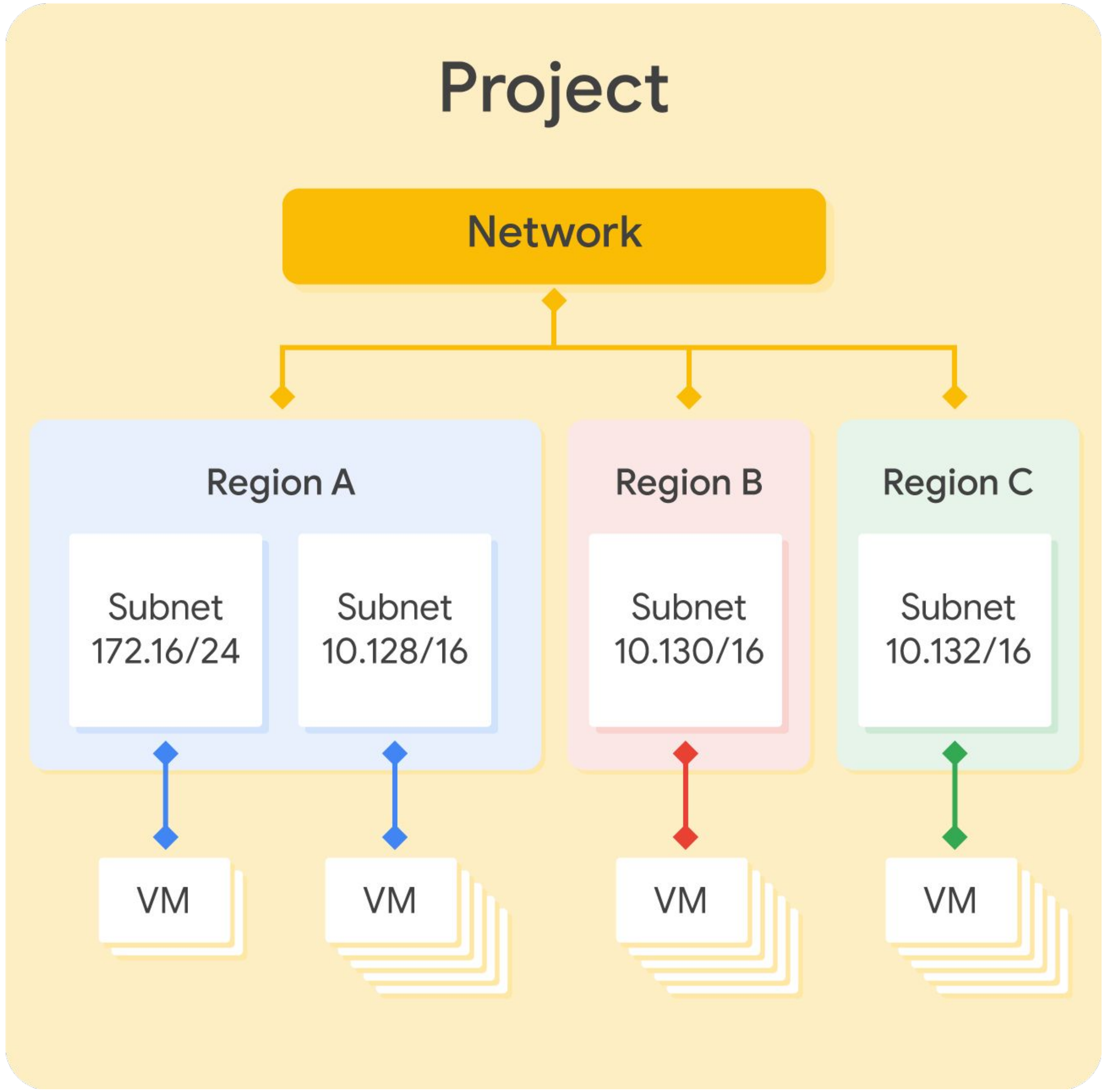
Subnetworks cross zones



- VMs can be on the same subnet but in different zones.
- A single firewall rule can apply to both VMs.

Expand subnets without re-creating instances

- Cannot overlap with other subnets
- IP range must be a unique valid CIDR block
- New subnet IP ranges have to fall within valid IP ranges
- Can expand but not shrink
- Auto mode can be expanded from /20 to /16
- Avoid large subnets

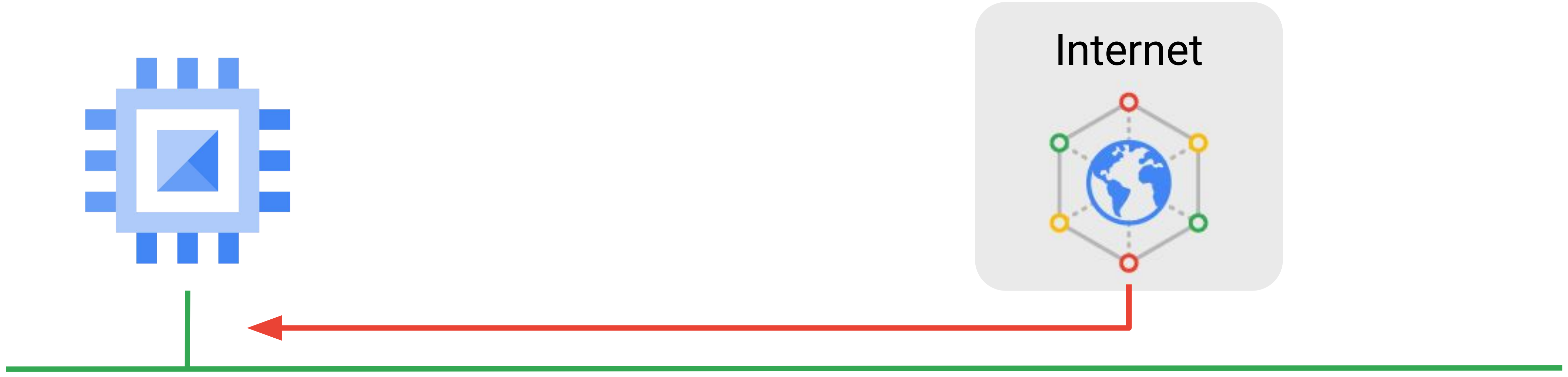


03

IP Addresses

VMs can have internal and external IP addresses

Cloud External IP Addresses



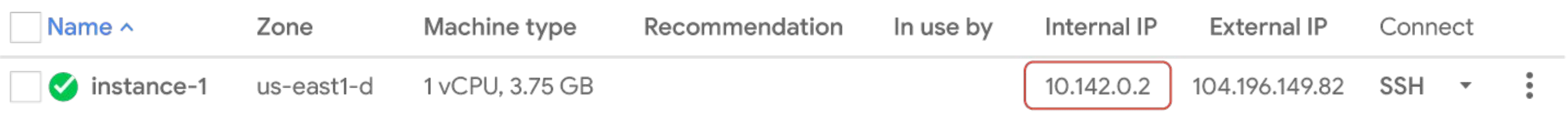
Internal IP

- Allocated from subnet range to VMs by DHCP
- DHCP lease is renewed every 24 hours
- VM name + IP is registered with network-scoped DNS

External IP

- Assigned from pool (ephemeral)
- Reserved (static)
- Bring Your Own IP address (BYOIP)
- VM doesn't know external IP; it is mapped to the internal IP

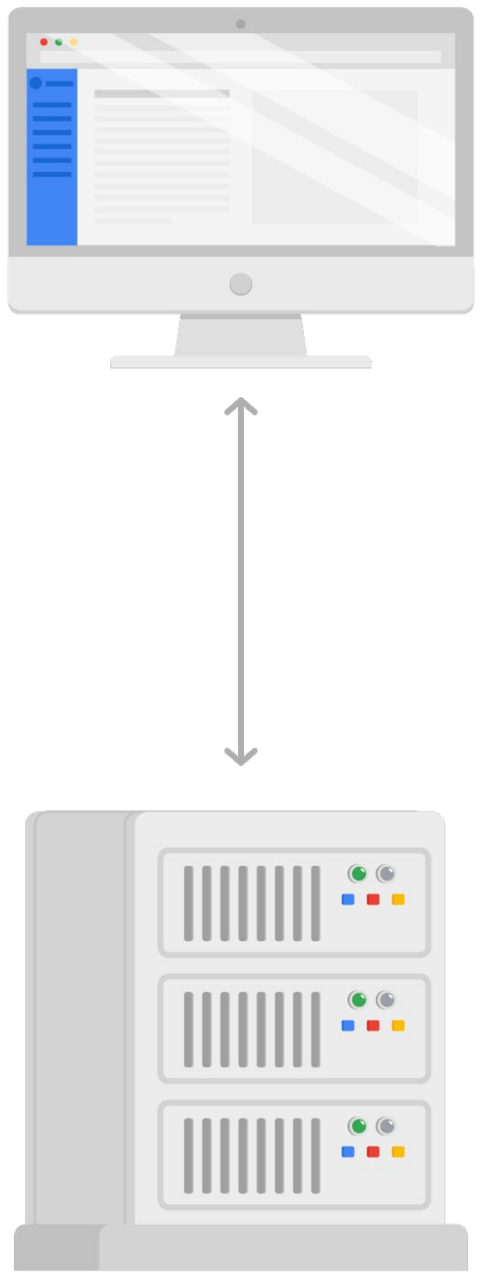
External IPs are mapped to internal IPs



☐ Name ^	Zone	Machine type	Recommendation	In use by	Internal IP	External IP	Connect	
☐ ✓ instance-1	us-east1-d	1 vCPU, 3.75 GB			10.142.0.2	104.196.149.82	SSH ▾	⋮

```
$ sudo /sbin/ifconfig
eth0
     Link encap:Ethernet  HWaddr 42:01:0a:8e:00:02
     inet addr:10.142.0.2  Bcast:10.142.0.2  Mask:255.255.255.255
     UP BROADCAST RUNNING MULTICAST  MTU:1460  Metric:1
     RX packets:397 errors:0 dropped:0 overruns:0 frame:0
     TX packets:279 errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:1000
     RX bytes:66429 (64.8 KiB)  TX bytes:41662 (40.6 KiB)
lo
     Link encap:Local Loopback
     inet addr:127.0.0.1  Mask:255.0.0.0
     inet6 addr: ::1/128 Scope:Host
     UP LOOPBACK RUNNING  MTU:65536  Metric:1
     RX packets:0 errors:0 dropped:0 overruns:0 frame:0
     TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:0
     RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

DNS resolution for internal addresses



Google Cloud has **two** types of internal DNS:

- Zonal
- Global

Each instance has a hostname that can be resolved to an internal IP address:

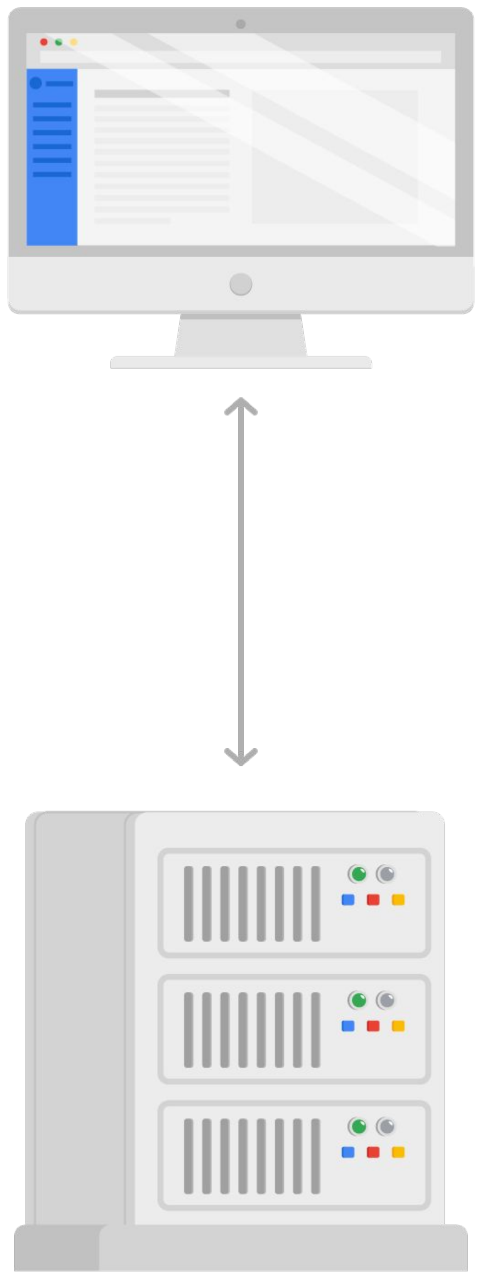
- The hostname is the same as the instance name.
- FQDN is [hostname].[zone].c.[project-id].internal

Example: my-server.us-central1-a.c.guestbook-151617.internal

Name resolution is handled by internal DNS resolver:

- Provided as part of Compute Engine (169.254.169.254).
- Configured for use on instance via DHCP.
- Provides answer for internal and external addresses.

DNS resolution for external addresses

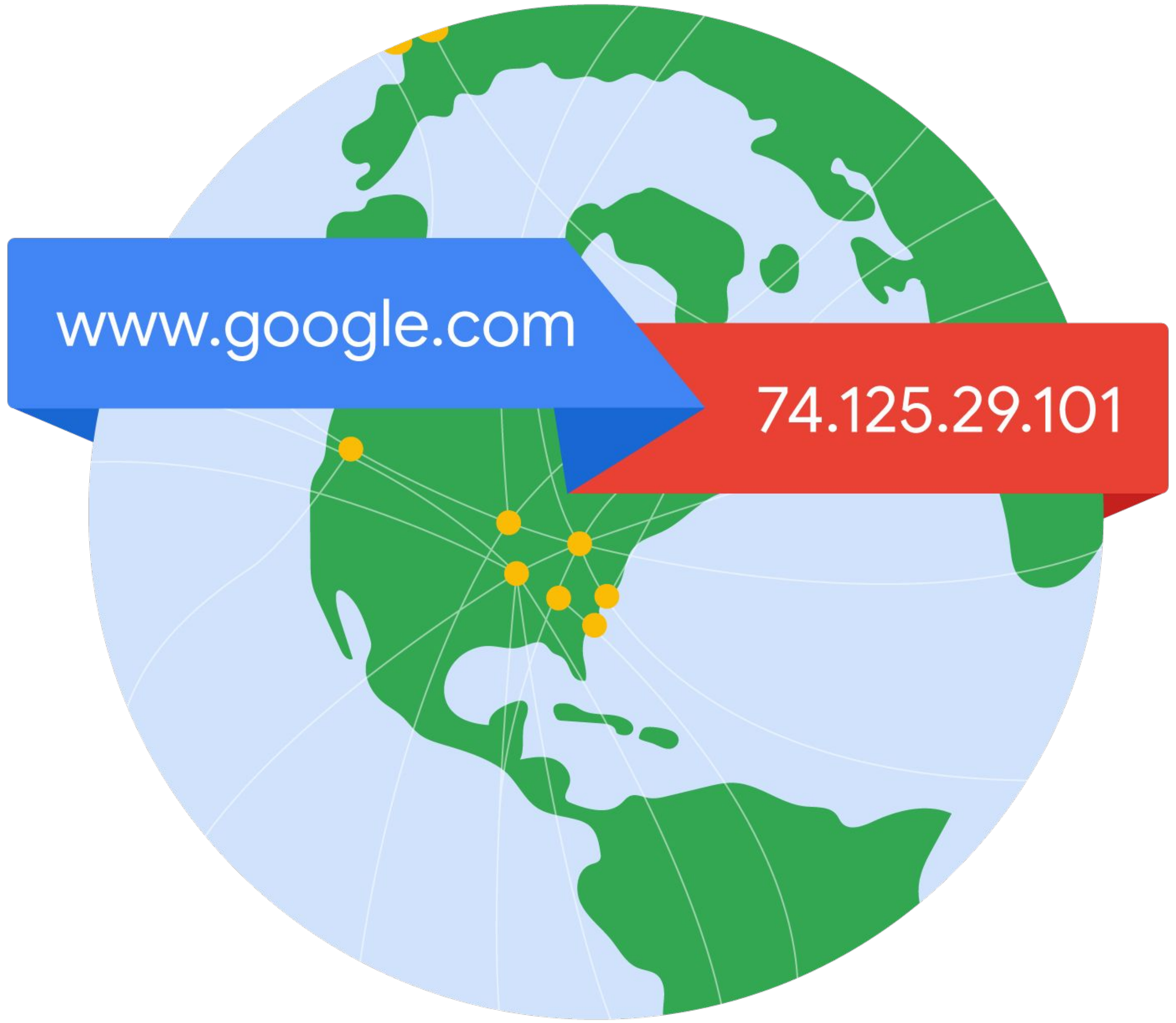


- Instances with external IP addresses can allow connections from hosts outside the project.
  - Users connect directly using external IP address.
  - Admins can also publish public DNS records pointing to the instance.
    - Public DNS records are not published automatically.
- DNS records for external addresses can be published using existing DNS servers (outside of Google Cloud).
- DNS zones can be hosted using Cloud DNS.

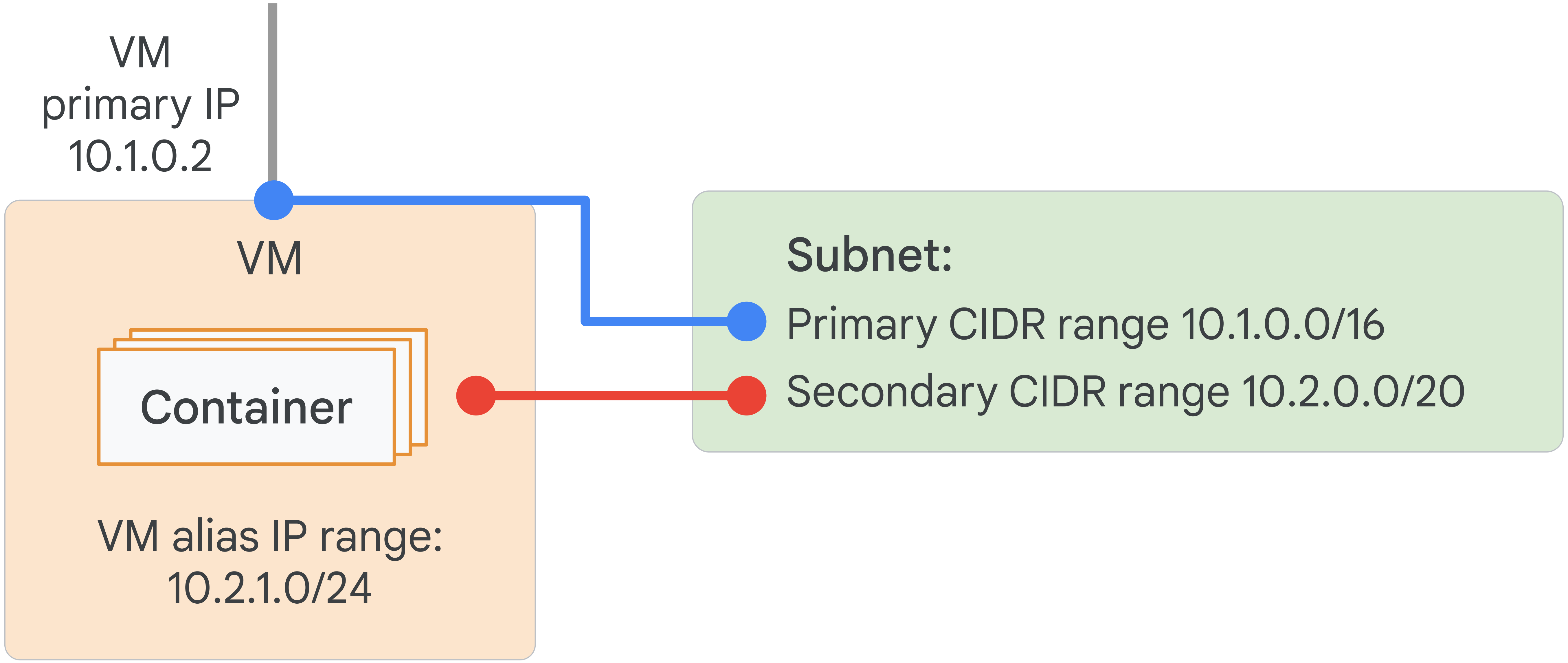
Host DNS zones using Cloud DNS

Cloud DNS

- Google's DNS service
- Translate domain names into IP address
- Low latency
- High availability (100% uptime SLA)
- Create and update millions of DNS records
- UI, command line, or API



Assign a range of IP addresses as aliases to a VM's network interface using alias IP ranges



04

Routes and Firewall Rules

A route is a mapping of an IP range to a destination

Cloud Routes

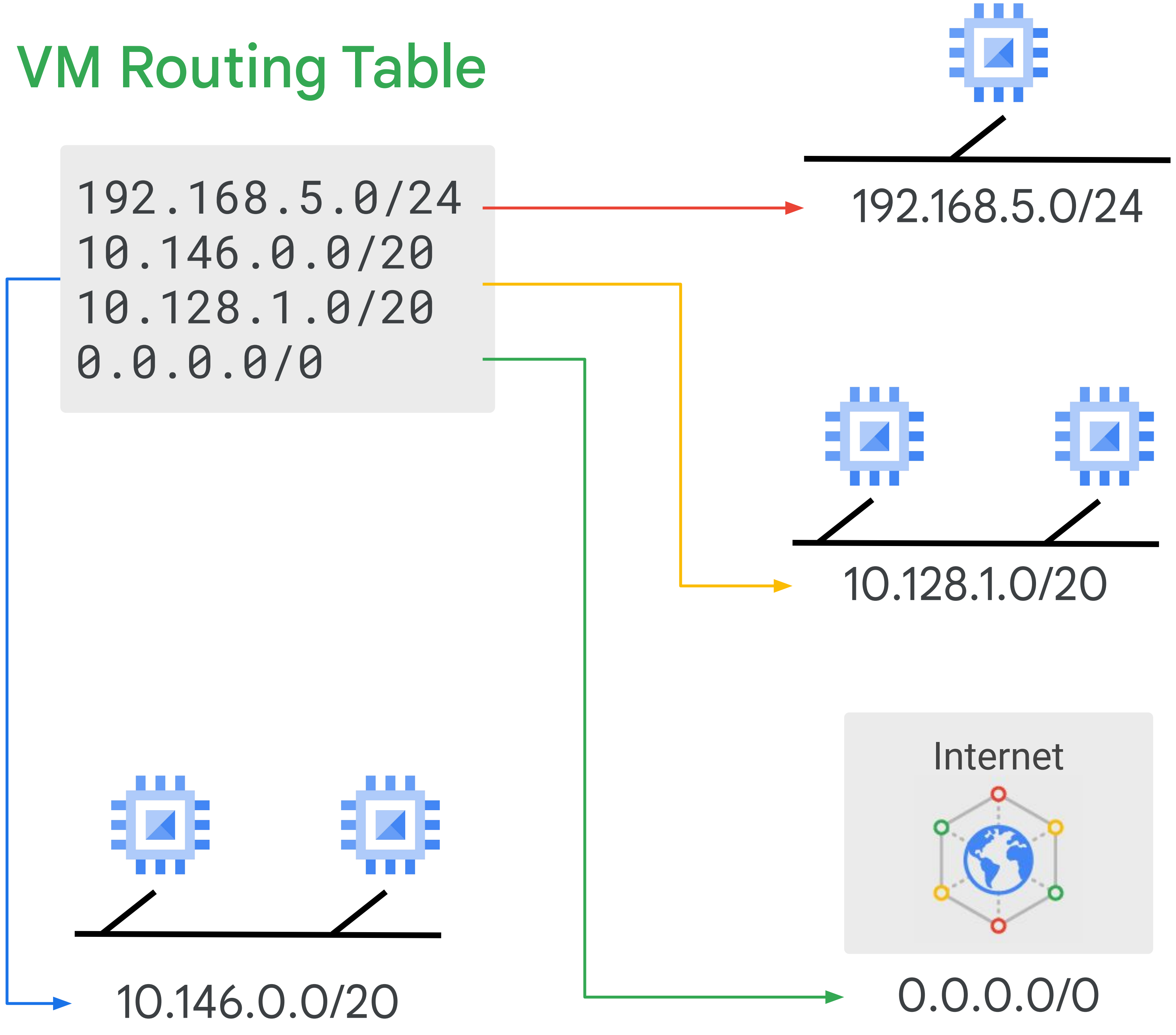
Every network has:

- Routes that let instances in a network send traffic directly to each other.
- A default route that directs packets to destinations that are outside the network.

Firewall rules must also allow the packet.

Routes map traffic to destination networks

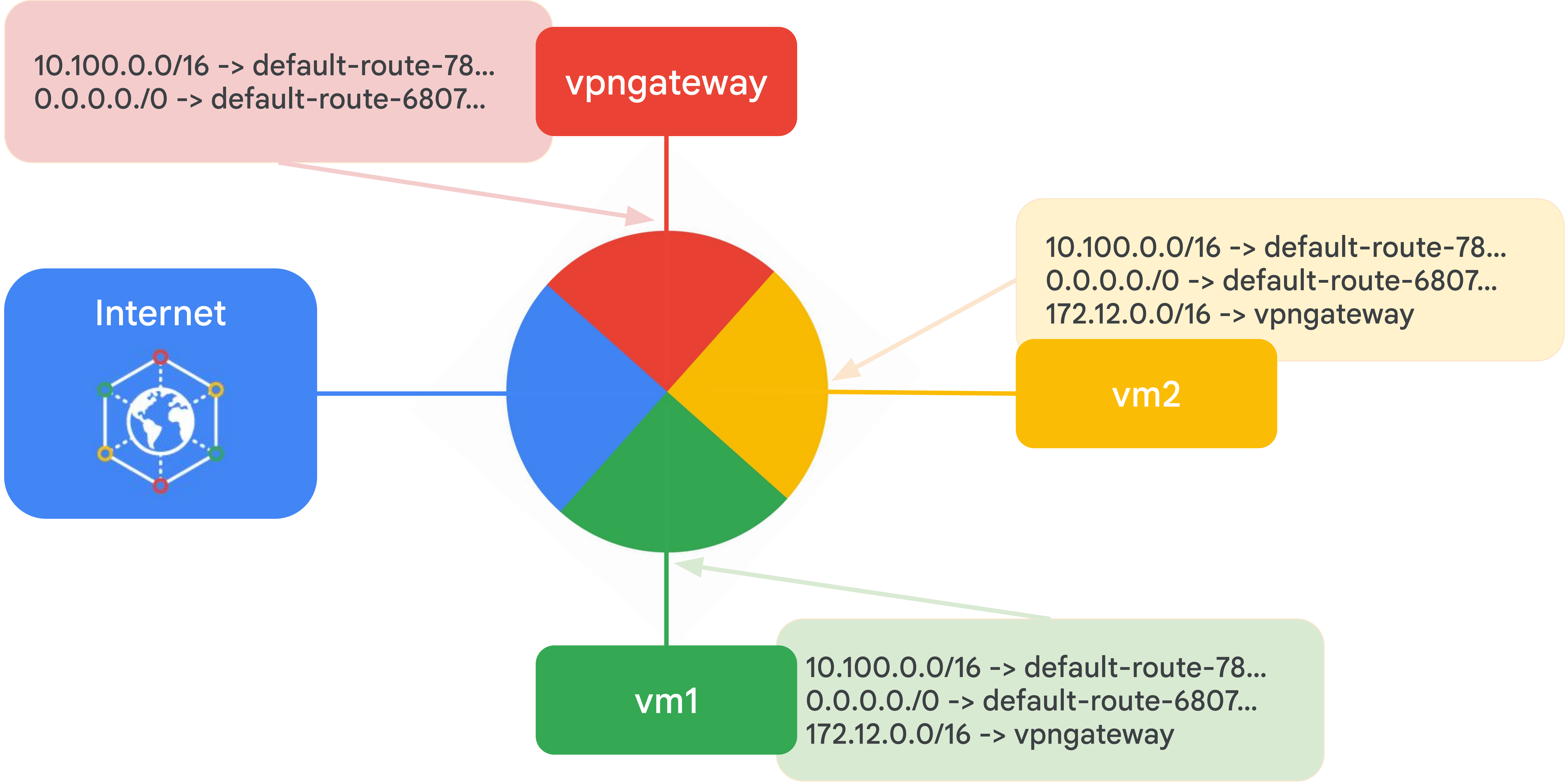
- Apply to traffic egressing a VM.
- Forward traffic to most specific route.
- Are created when a subnet is created.
- Enable VMs on same network to communicate.
- Destination is in CIDR notation.
- Traffic is delivered only if it also matches a firewall rule.



VM Routing Table

```
192.168.5.0/24
10.146.0.0/20
10.128.1.0/20
0.0.0.0/0
```

Instance routing tables



10.100.0.0/16 -> default-route-78...
0.0.0.0./0 -> default-route-6807...

10.100.0.0/16 -> default-route-78...
0.0.0.0./0 -> default-route-6807...
172.12.0.0/16 -> vpngateway

10.100.0.0/16 -> default-route-78...
0.0.0.0./0 -> default-route-6807...
172.12.0.0/16 -> vpngateway

Firewall rules protect your VM instances from unapproved connections

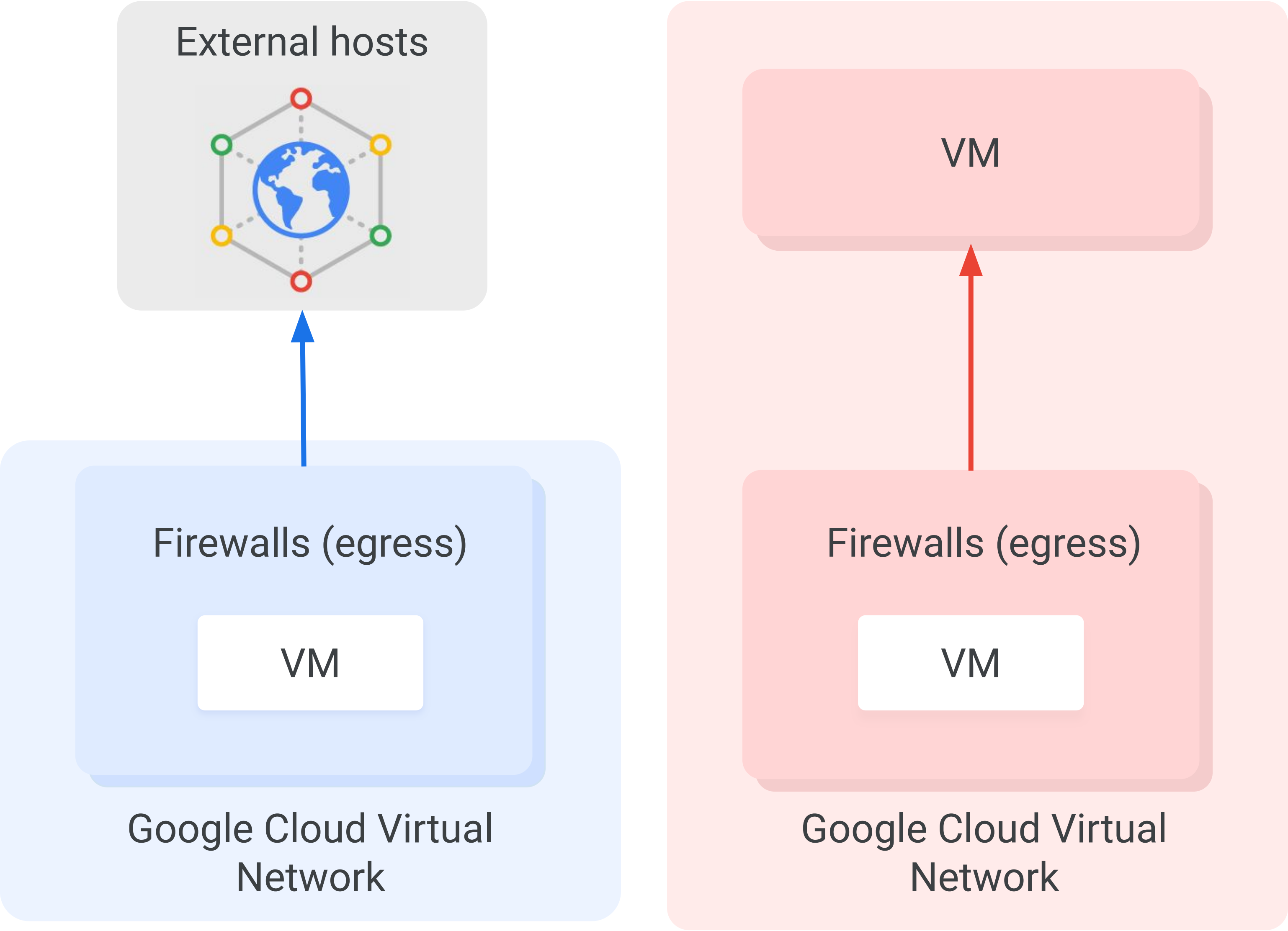
Cloud Firewall Rules

- VPC network functions as a distributed firewall.
- Firewall rules are applied to the network as a whole.
- Connections are allowed or denied at the instance level.
- Firewall rules are stateful.
- Implied deny all ingress and allow all egress.

A firewall rule is composed of...

Parameter	Details
`direction`	Inbound connections are matched against `ingress` rules only.
	Outbound connections are matched against `egress` rules only.
`source or destination`	For the `ingress` direction, `sources` can be specified as part of the rule with IP addresses, source tags or a source service account.
	For the `egress` direction, `destinations` can be specified as part of the rule with one or more ranges of IP addresses.
`protocol` **`and`** `port`	Any rule can be restricted to apply to specific protocols only or specific combinations of protocols and ports only.
`action`	To allow or deny packets that match the direction, protocol, port, and source or destination of the rule.
`priority`	Governs the order in which rules are evaluated; the first matching rule is applied.
`Rule assignment`	All rules are assigned to all instances, but you can assign certain rules to certain instances only.

Google Cloud firewall use case: Egress



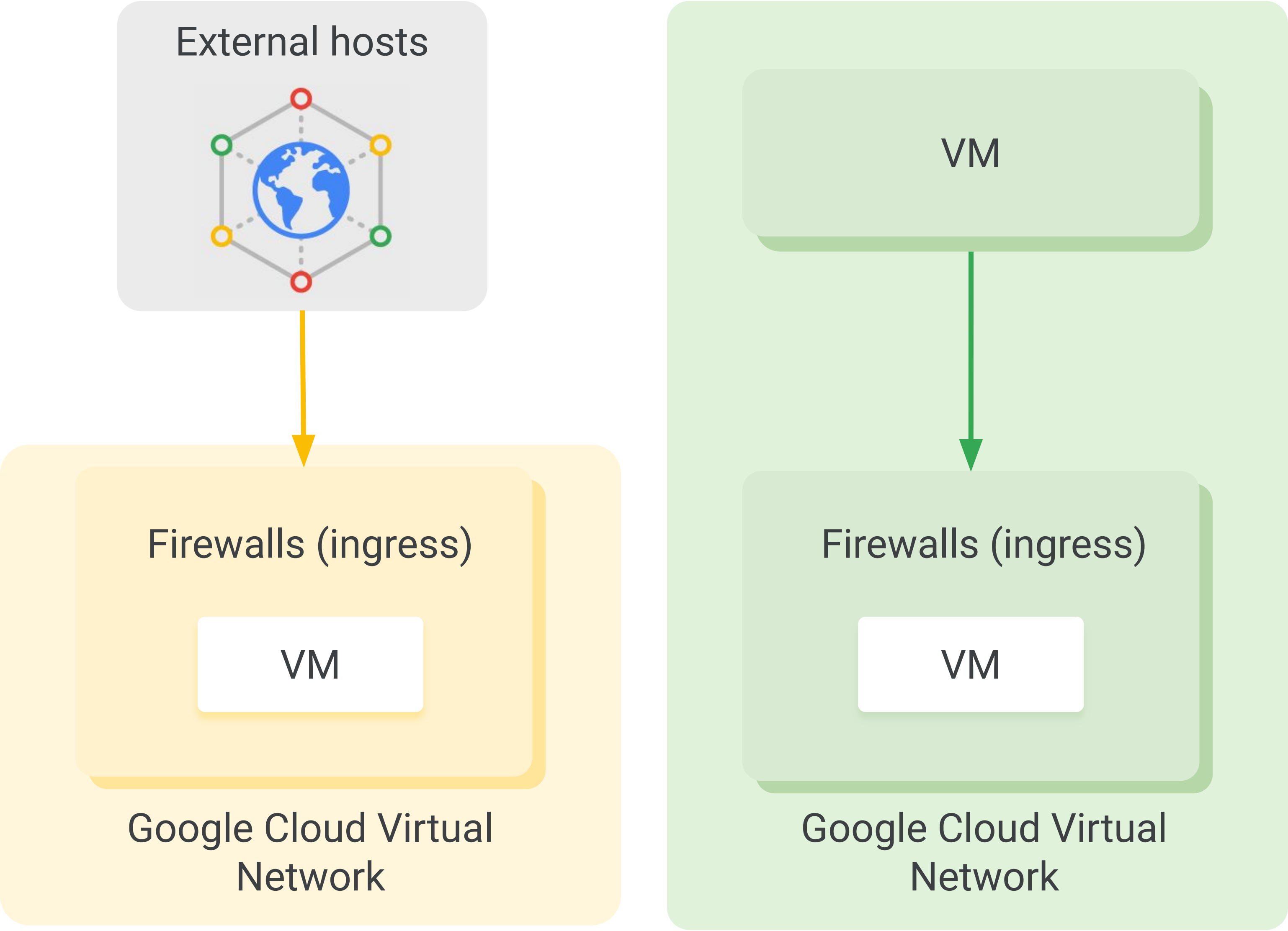
Conditions:

- Destination CIDR ranges
- Protocols
- Ports

Action:

- Allow: permit the matching egress connection
- Deny: block the matching egress connection

Google Cloud firewall use case: Ingress



Conditions:

- Source CIDR ranges
- Protocols
- Ports

Action:

- Allow: permit the matching ingress connection
- Deny: block the matching ingress connection

05

Pricing

Network pricing (subject to change)

Traffic type	Price
Ingress	No charge
Egress to the same zone (internal IP address)	No charge
Egress to Google products (YouTube, Maps, Drive)	No charge
Egress to a different Google Cloud service (within same region; exceptions)	No charge
Egress between zones in the same region (per GB)	$0.01
Egress to the same zone (external IP address, per GB)	$0.01
Egress between regions within the US and Canada (per GB)	$0.01
Egress between regions, not including traffic between US regions	Varies by region

External IP address pricing (us-central1)

(Subject to change)

Type	Price/Hour (USD)
Static IP address (assigned but unused)	$0.010
Static and ephemeral IP addresses in use on **standard** VM instances	$0.005
Static and ephemeral IP addresses in use on **preemptible and Spot** VM instances	$0.0025
Static and ephemeral IP addresses used by Cloud NAT	$0.005
Static and ephemeral IP addresses attached to forwarding rules, or used as a public IP for a Cloud VPN tunnel	No charge

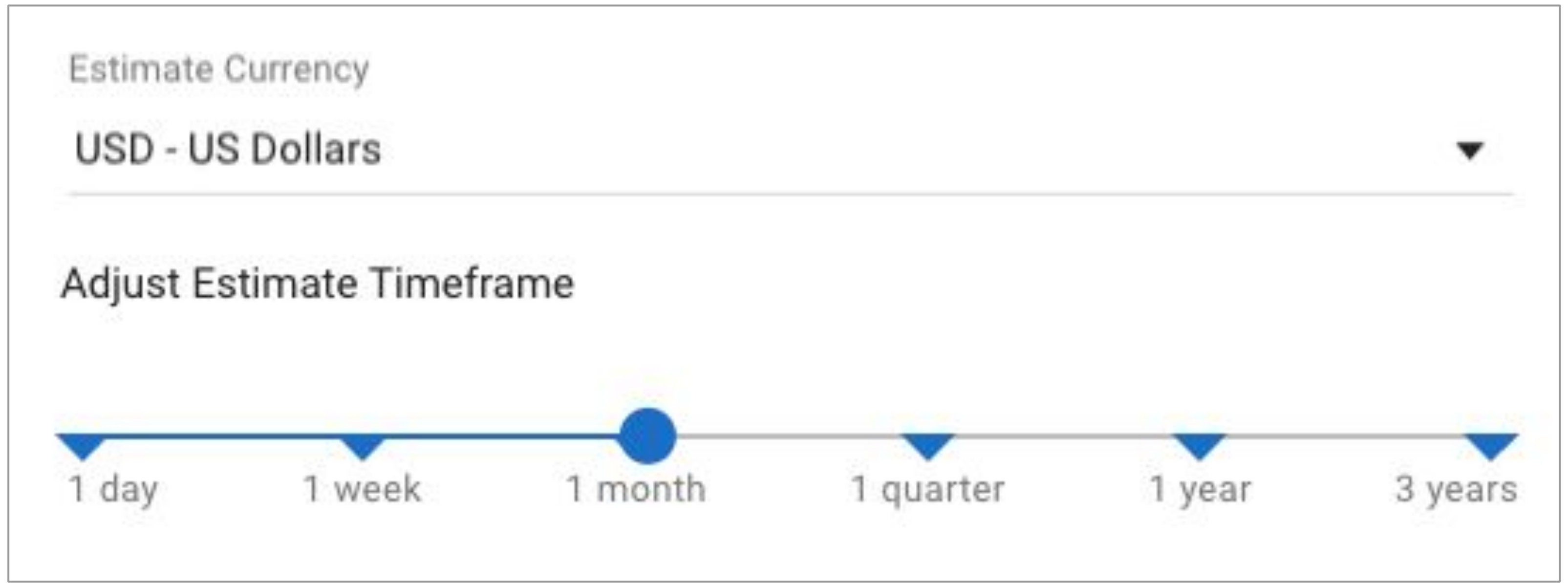
Estimate costs with the Google Cloud Pricing Calculator

Compute Engine

n1-standard-1
us-central1

Cloud Network

100-GB egress/monthly
Americas and EMEA



Estimate Currency

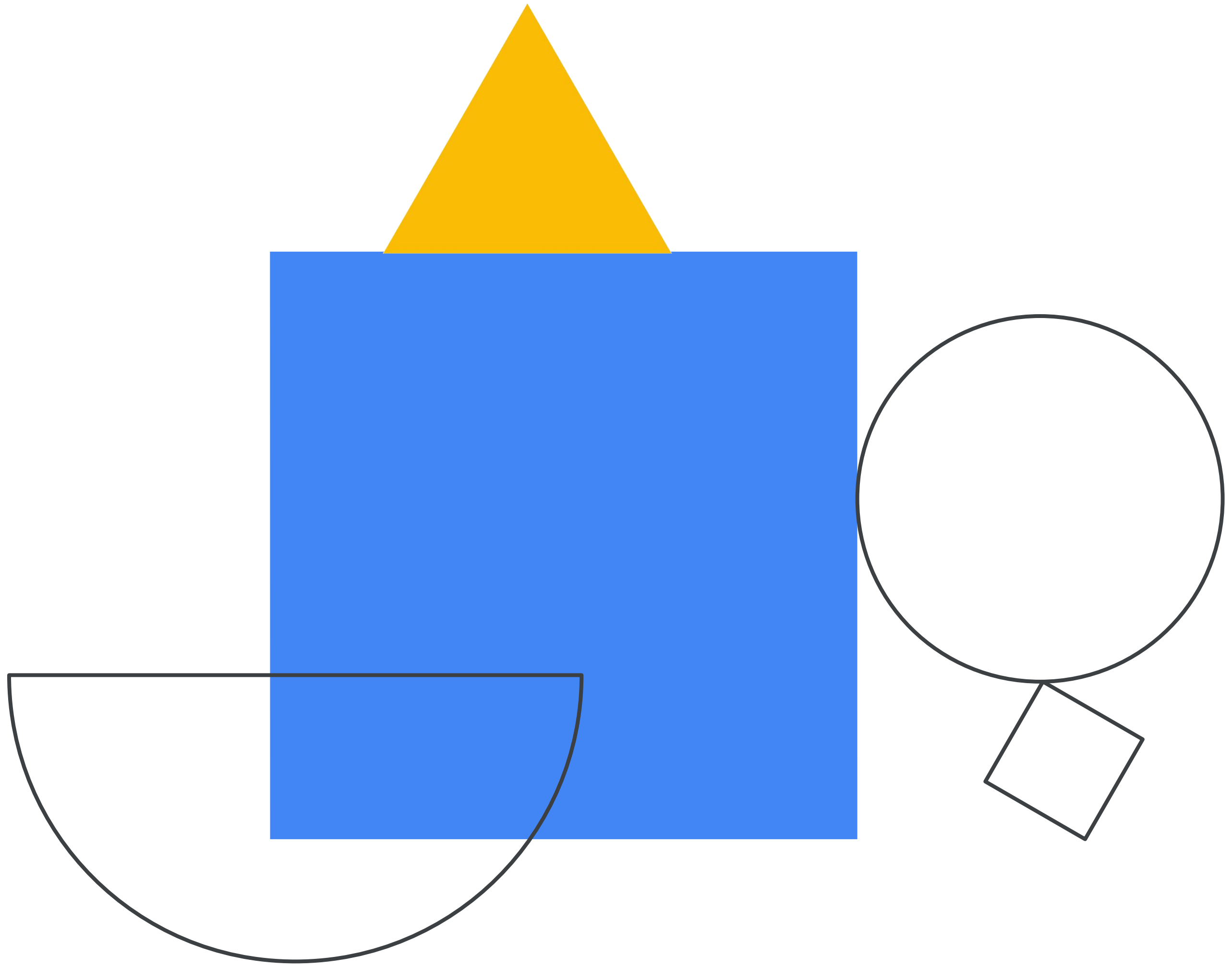
USD - US Dollars

Adjust Estimate Timeframe

1 day · 1 week · [✓ 1 month] · 1 quarter · 1 year · 3 years

Lab Intro

VPC Networking



Lab objectives

01 Explore the default VPC network

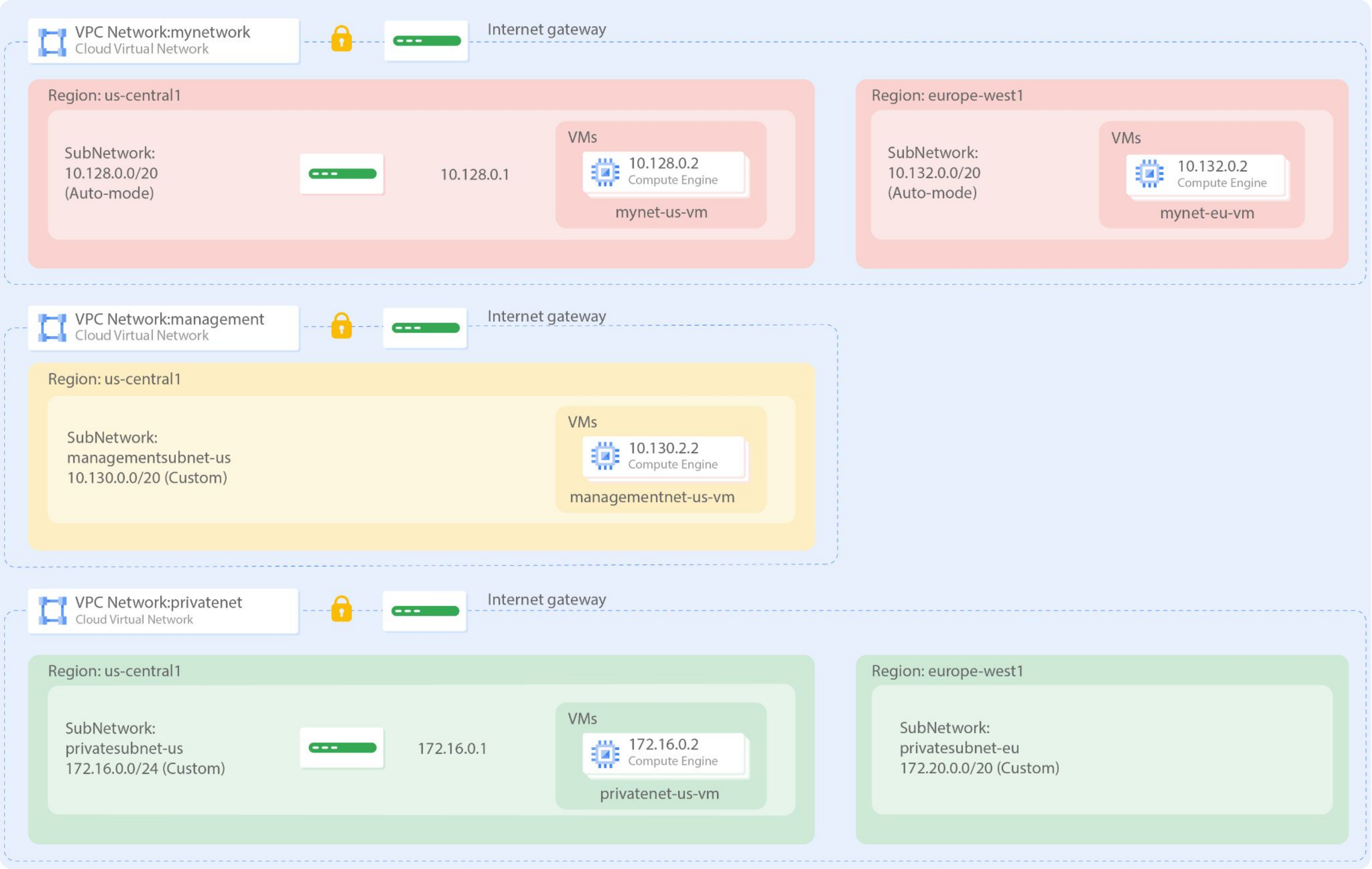
02 Create an auto mode network with firewall rules

03 Convert an auto mode network to a custom mode network

04 Create custom mode VPC networks with firewall rules

05 Create VM instances using Compute Engine

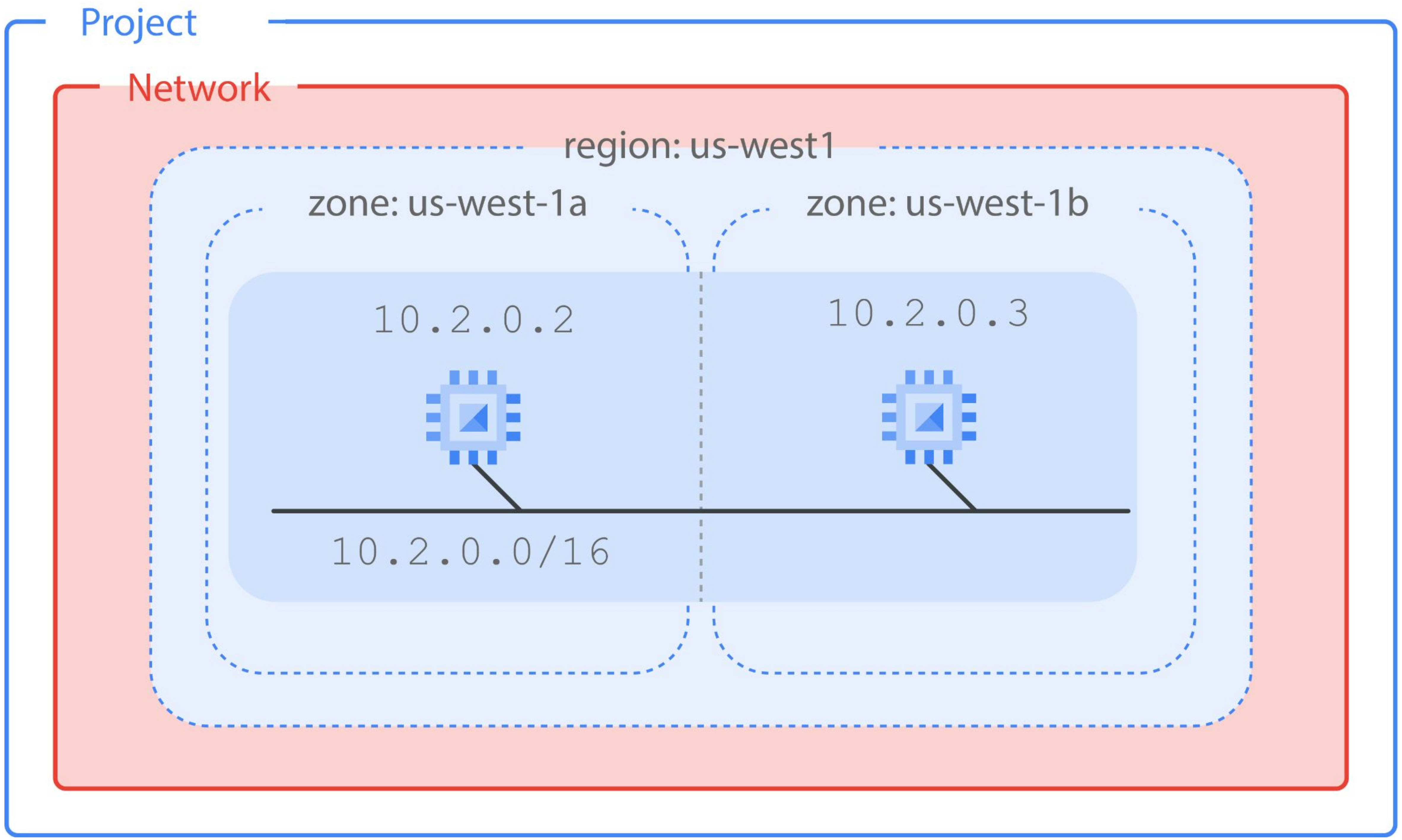
06 Explore the connectivity for VM instances across VPC networks


VPC Network:mynetwork
Cloud Virtual Network
Internet gateway
Region: us-central1
SubNetwork:
10.128.0.0/20
(Auto-mode)
10.128.0.1
VMs
10.128.0.2
Compute Engine
mynet-us-vm
Region: europe-west1
SubNetwork:
10.132.0.0/20
(Auto-mode)
VMs
10.132.0.2
Compute Engine
mynet-eu-vm
VPC Network:management
Cloud Virtual Network
Internet gateway
Region: us-central1
SubNetwork:
managementsubnet-us
10.130.0.0/20 (Custom)
VMs
10.130.2.2
Compute Engine
managementnet-us-vm
VPC Network:privatenet
Cloud Virtual Network
Internet gateway
Region: us-central1
SubNetwork:
privatesubnet-us
172.16.0.0/24 (Custom)
172.16.0.1
VMs
172.16.0.2
Compute Engine
privatenet-us-vm
Region: europe-west1
SubNetwork:
privatesubnet-eu
172.20.0.0/20 (Custom)

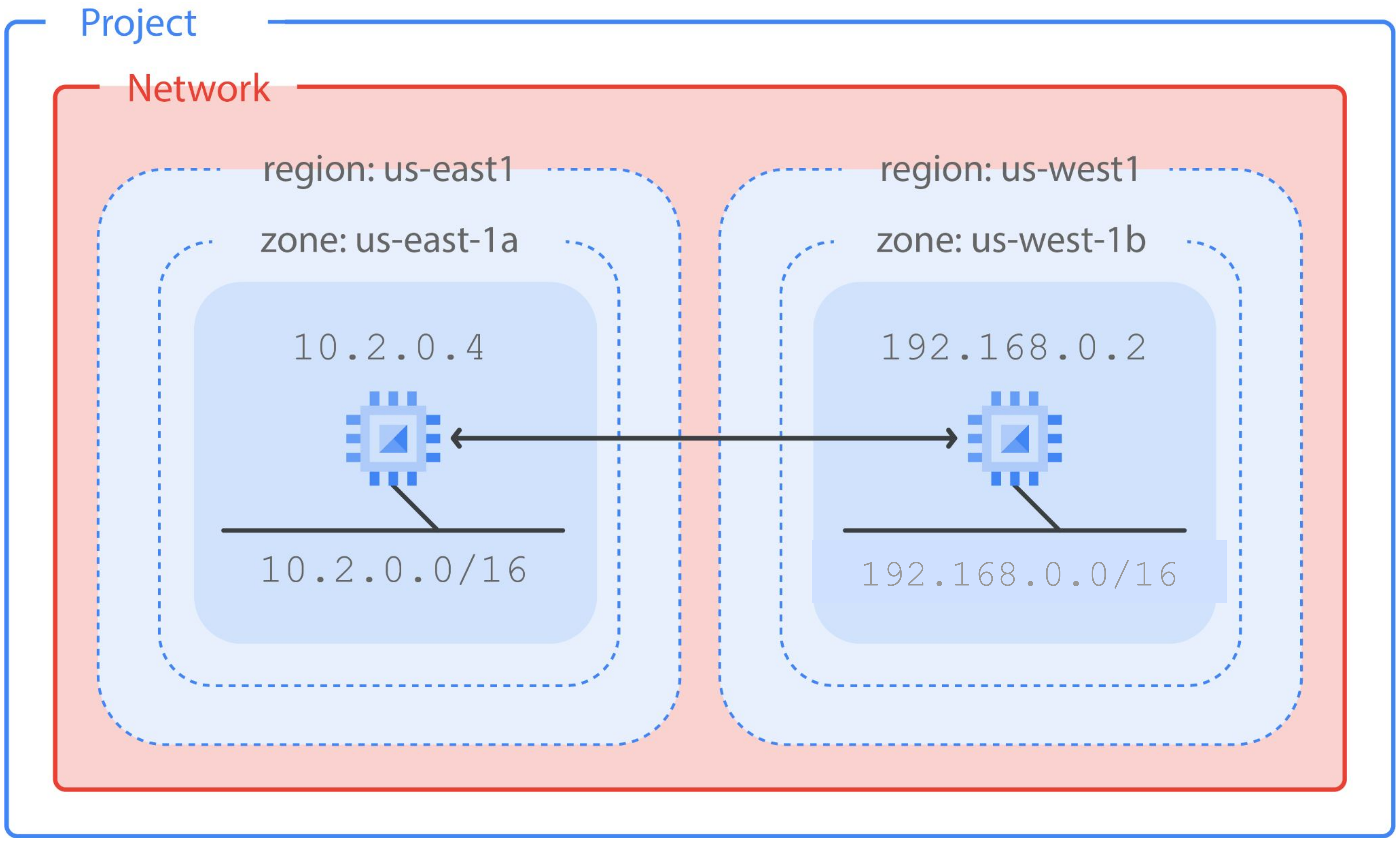
06

Common Network Designs

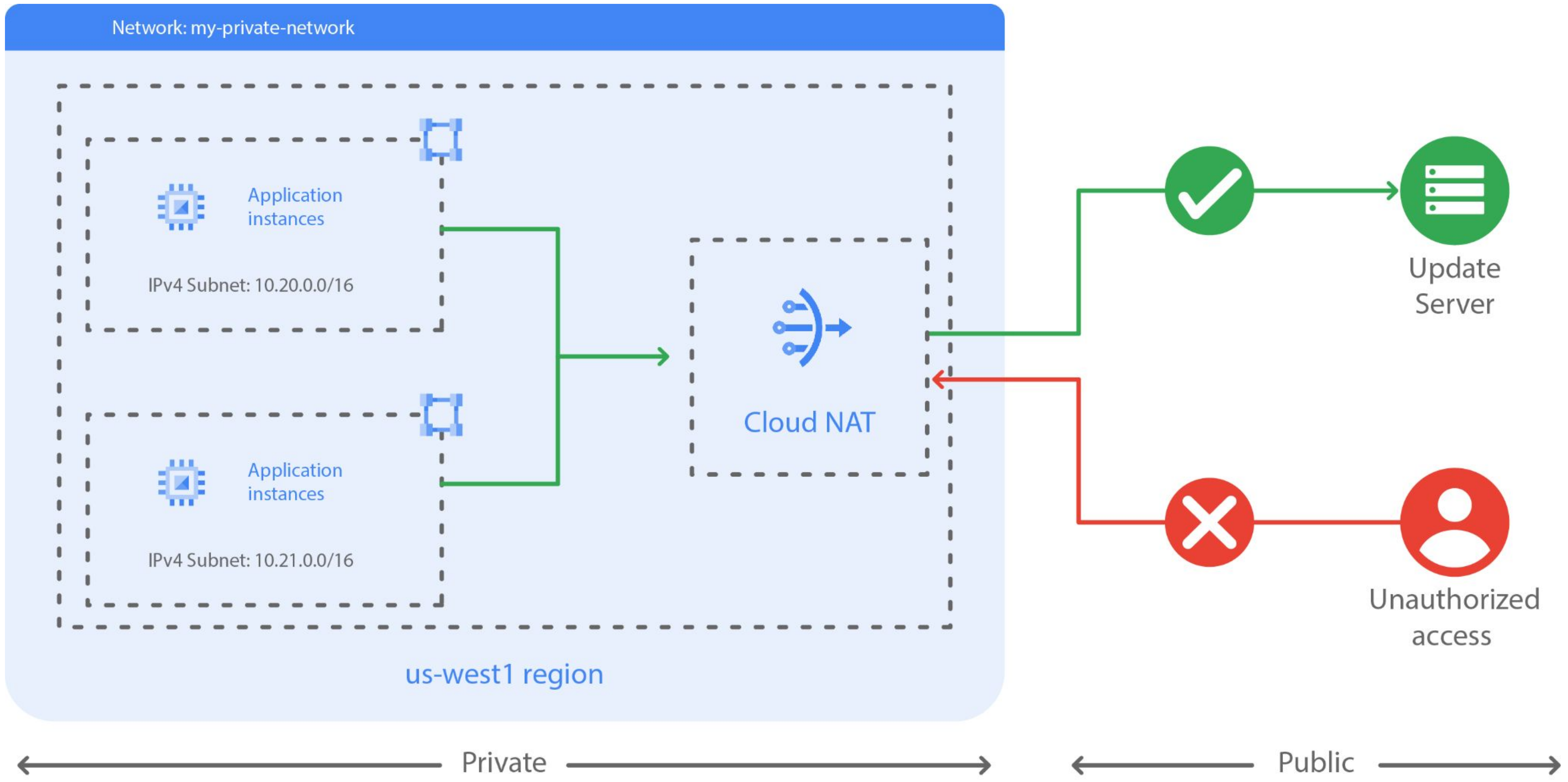
Increased availability with multiple zones



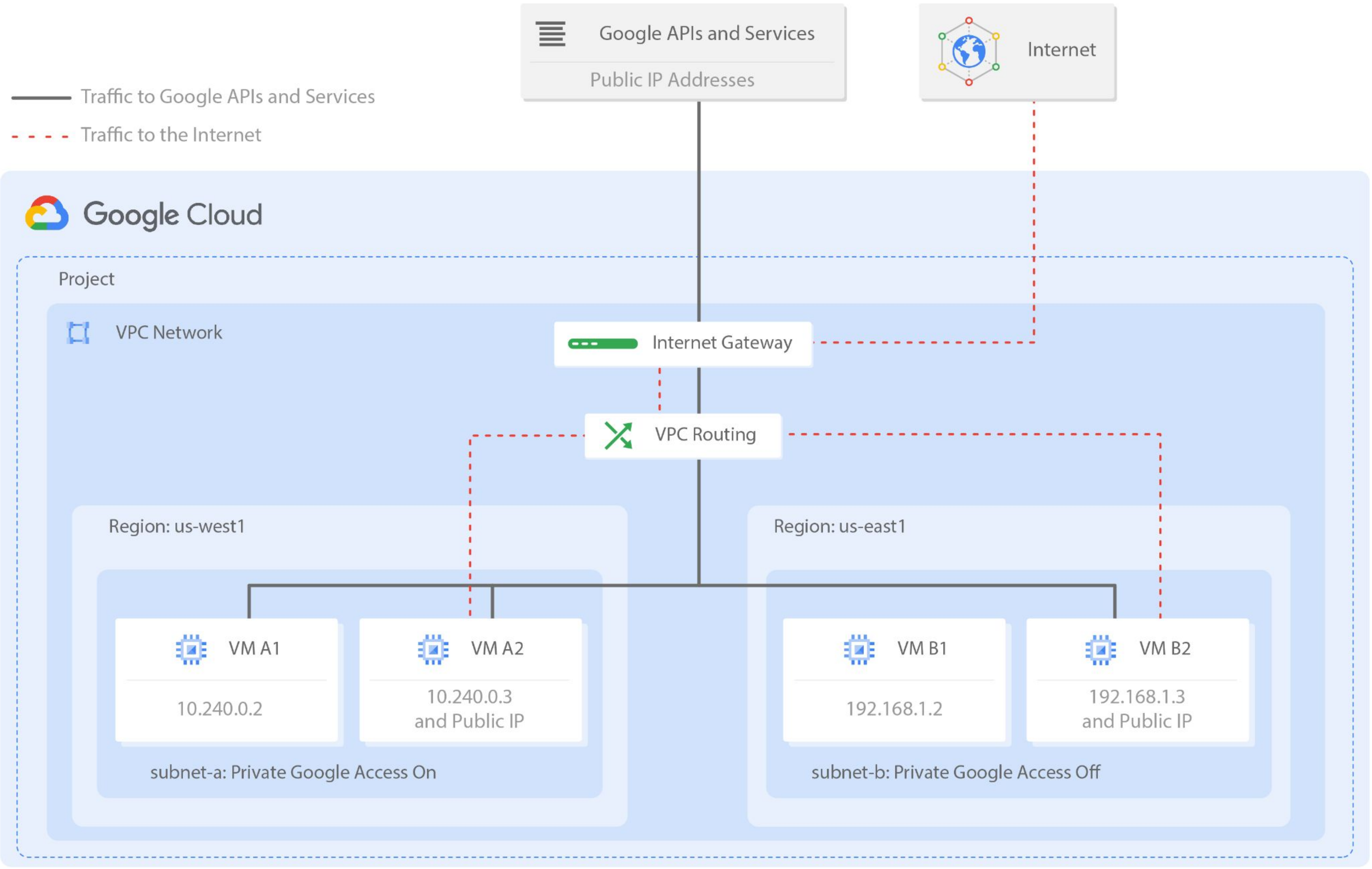
Globalization with multiple regions



Cloud NAT provides internet access to private instances

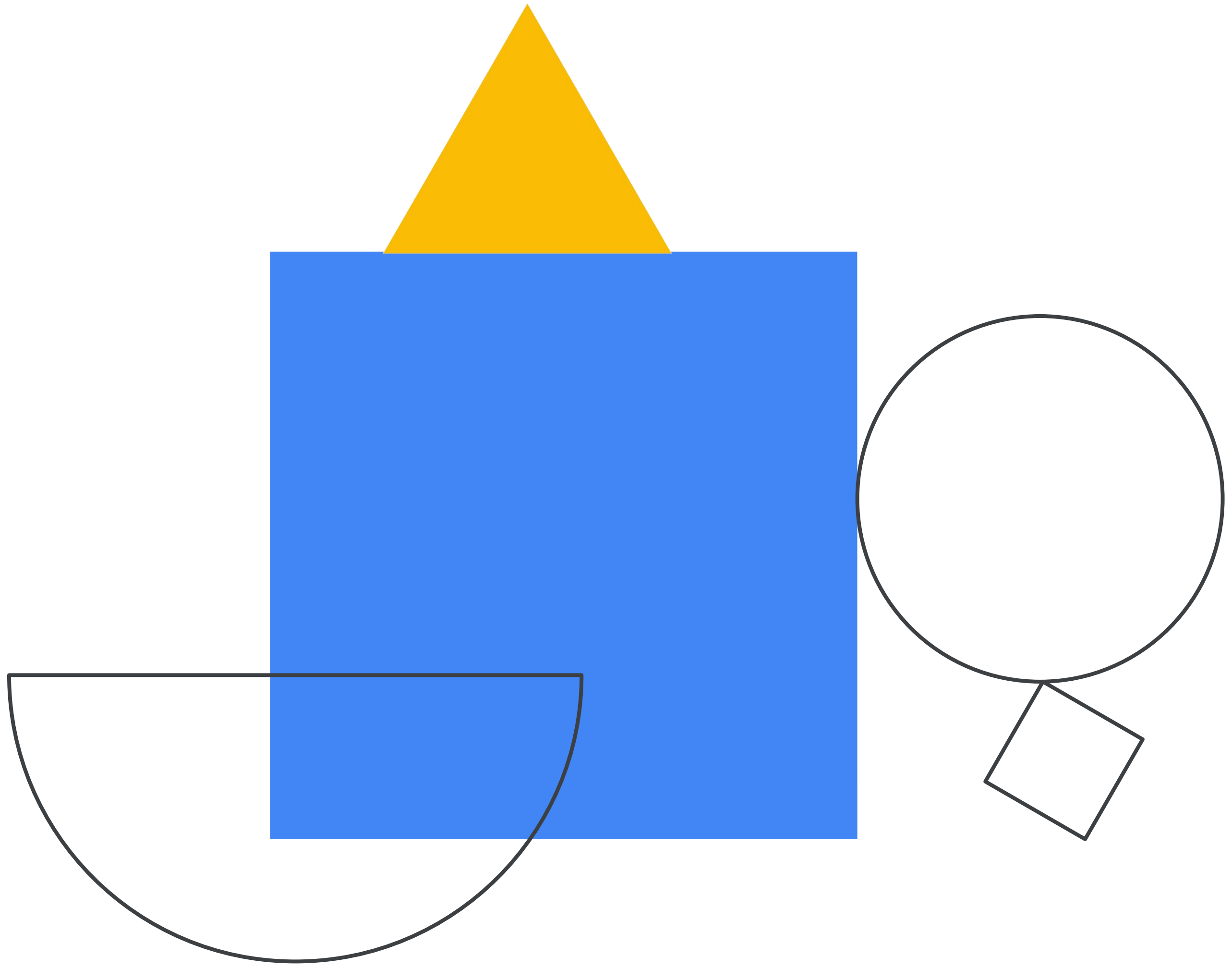


Private Google Access to Google APIs and services



Lab Intro

Implement Private Google Access and Cloud NAT



Lab objectives

01 Configure a VM instance that doesn't have an external IP address

02 Connect to a VM instance using an Identity-Aware Proxy (IAP) tunnel

03 Enable Private Google Access on a subnet

04 Configure a Cloud NAT gateway

05 Verify access to public IP addresses of Google APIs and services and other connections to the internet

Quiz

Question #1

Question

In Google Cloud, what is the minimum number of IP addresses that a VM instance needs?

A. One: Only an internal IP address

B. Two: One internal and one external IP address

C. Three: One internal, one external and one alias IP address

Question #1

Answer

In Google Cloud, what is the minimum number of IP addresses that a VM instance needs?

- **A. One: Only an internal IP address** ✓
- B. Two: One internal and one external IP address
- C. Three: One internal, one external and one alias IP address

Question #2

Question

What are the three types of networks offered in the Google Cloud?

A. Zonal, regional, and global

B. Gigabit network, 10-gigabit network, and 100-gigabit network

C. Default network, auto-mode network, and custom-mode network

D. IPv4 unicast network, IPv4 multicast network, IPv6 network

Question #2

Answer

What are the three types of networks offered in the Google Cloud?

A. Zonal, regional, and global

B. Gigabit network, 10-gigabit network, and 100-gigabit network

C. Default network, auto-mode network, and custom-mode network ✓

D. IPv4 unicast network, IPv4 multicast network, IPv6 network

Question #3

Question

What is one benefit of applying firewall rules by tag rather than by address?

A. Tags help organizations track firewall billing

B. Tags in network traffic help with network sniffing

C. Tags on firewall rules control which ephemeral IP addresses VMs will receive

D. When a VM is created with a matching tag, the firewall rules apply irrespective of the IP address it is assigned

Question #3

Answer

What is one benefit of applying firewall rules by tag rather than by address?

A. Tags help organizations track firewall billing

B. Tags in network traffic help with network sniffing

C. Tags on firewall rules control which ephemeral IP addresses VMs will receive

D. When a VM is created with a matching tag, the firewall rules apply irrespective of the IP address it is assigned ✓

Review: Virtual Networks