Google Cloud VPC Networking Fundamentals

Google Cloud

Agenda

Projects, Networks, and Subnetworks

IP Addresses

Routes and Firewall Rules

Lab: Getting Started with VPC Networking

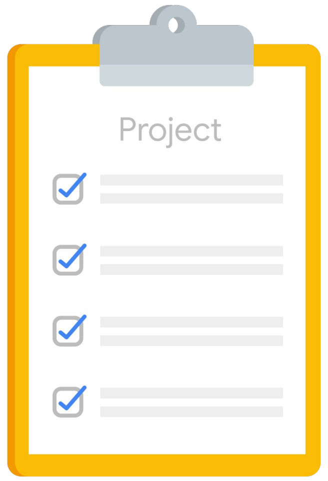
Multiple Network Interfaces

Lab: Working with Multiple VPC Networks

Quiz

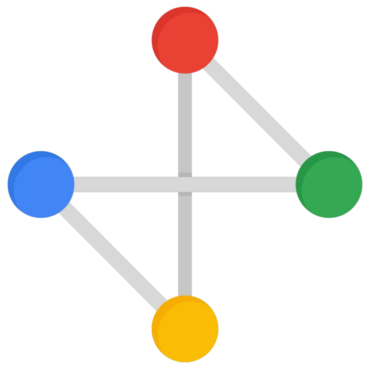
Projects and networks

A project:



- Associates objects and services with billing
- Contains networks (up to 5)
- Networks can be shared/peered

A network:



- No IP address range
- Global and spans all available regions
- Contains subnetworks
- Type: default, auto, or custom

VPC objects

- Projects
- Networks
- Default, auto mode, custom mode
- Subnetworks
- Regions
- Zones
- IP addresses
- Internal, external, range
- Virtual machines (VMs)
- Routes
- Firewall rules

Virtual Private Cloud

There are 3 VPC network types

Default

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

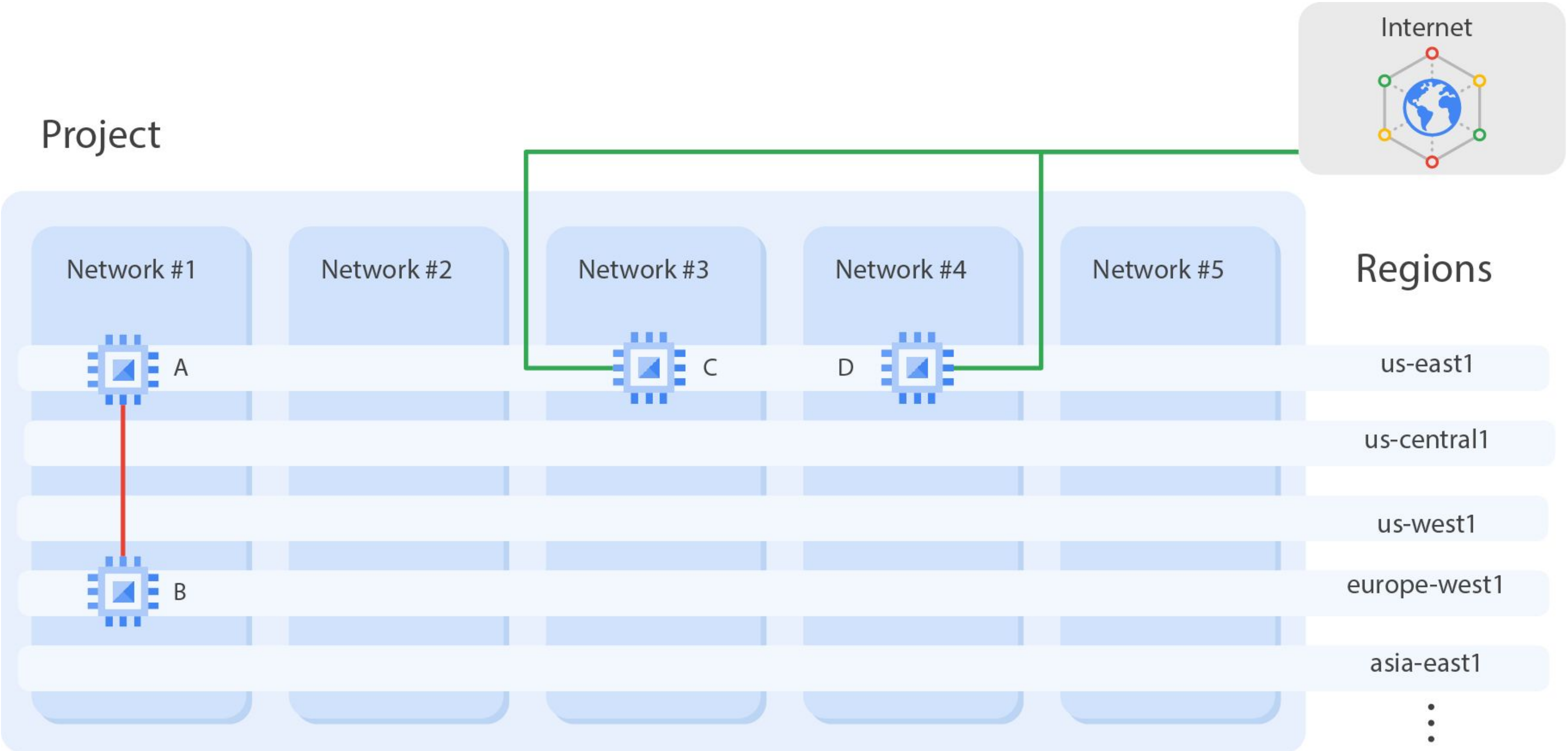
Auto Mode

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

Custom Mode

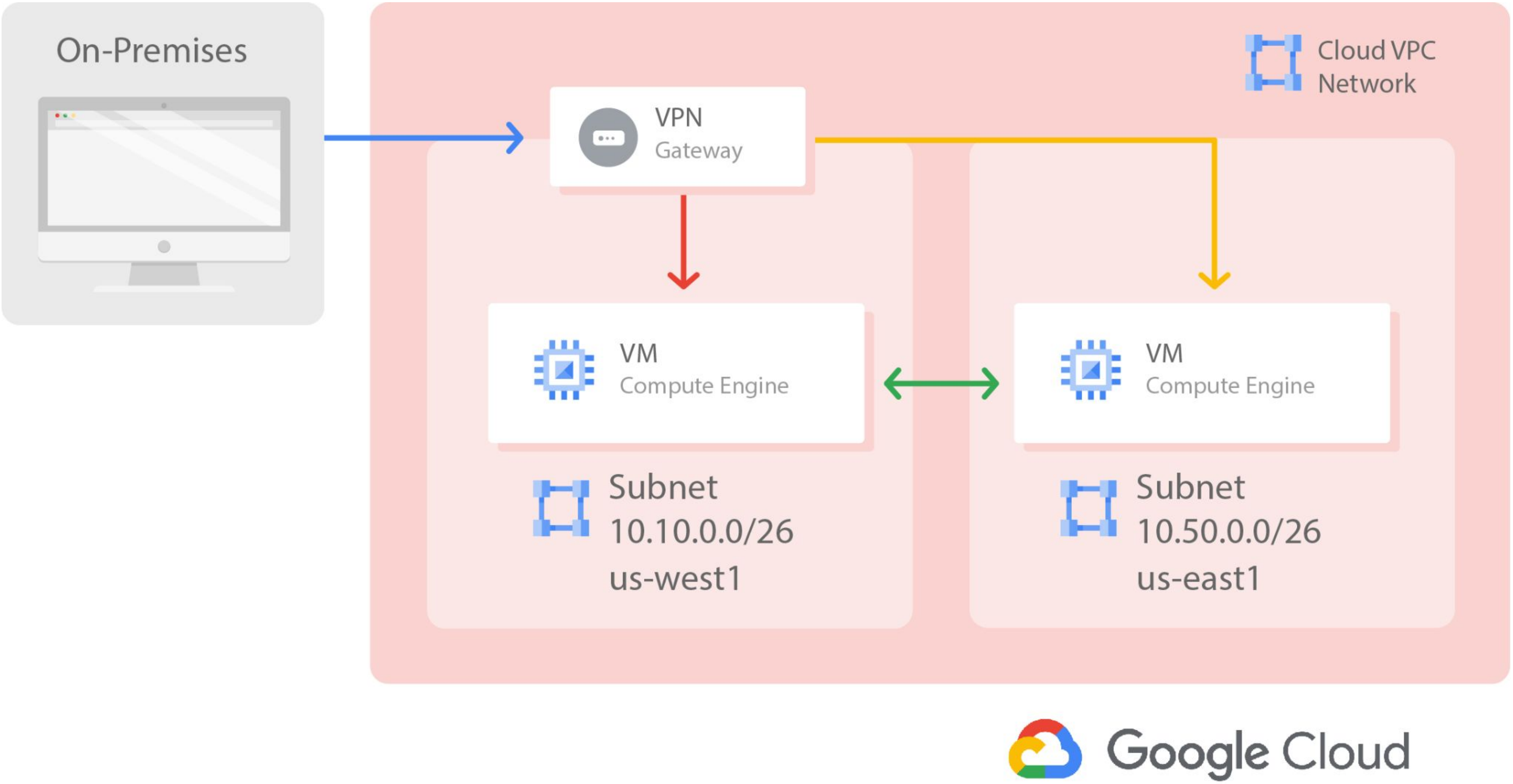
- No default subnets created
- Full control of IP ranges
- Regional IP allocation
- Expandable to any RFC 1918 size

Network isolate systems

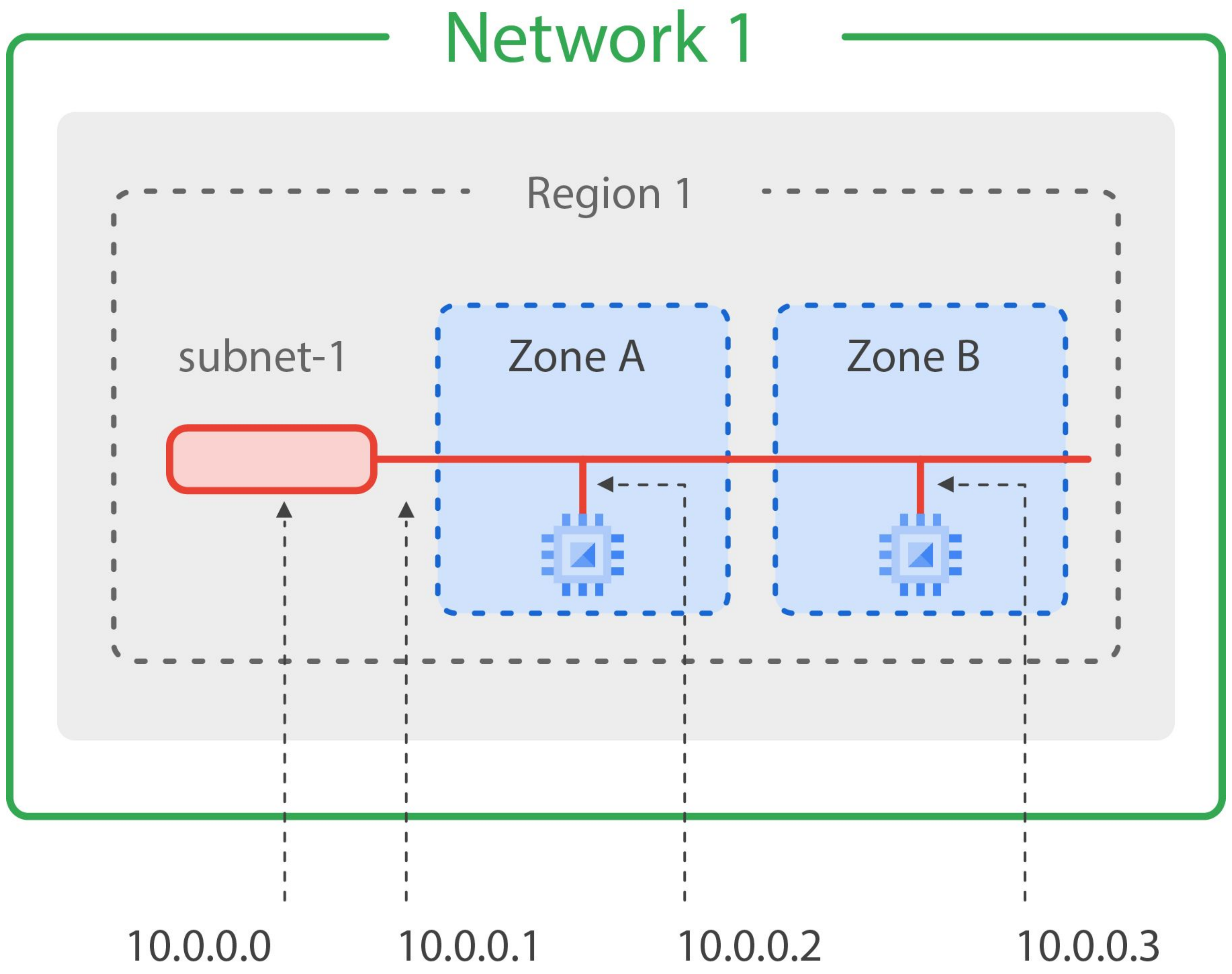


- **A** and **B** can communicate over internal IPs *even though they are in different regions.*
- **C** and **D** must communicate over external IPs *even though they are in the same region.*

Google's VPC is global



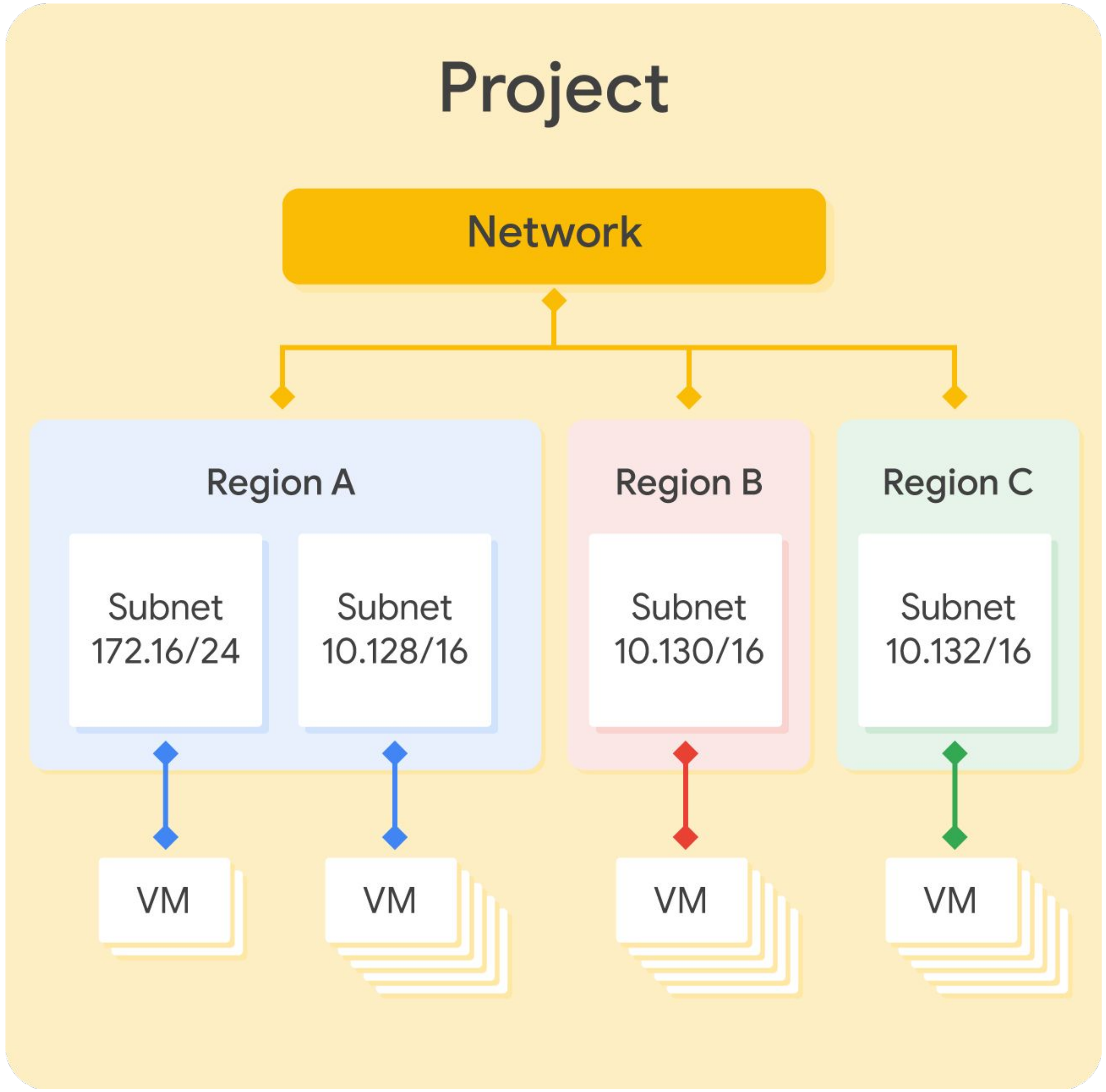
Subnetworks cross zones



- 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
- Inside the RFC 1918 address spaces
- Can expand but not shrink
- Auto mode can be expanded from /20 to /16
- Avoid large subnets



Google Cloud

Migrate a VM between networks

- From legacy network to a VPC network in the same project.
- From one VPC network to another VPC network in the same project.
- From one subnet of a VPC network to another subnet of the same network.
- From a service project network to the shared network of a Shared VPC host project.

Agenda

Projects, Networks, and Subnetworks

IP Addresses

Routes and Firewall Rules

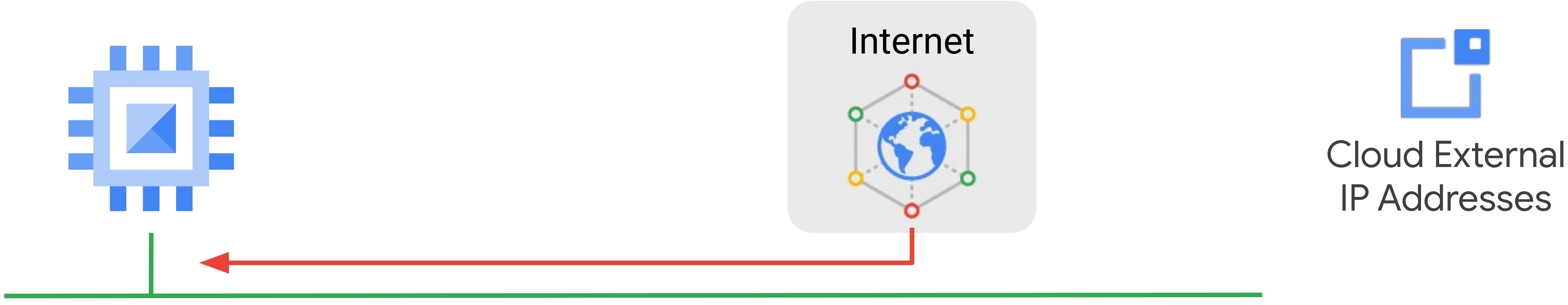
Lab: Getting Started with VPC Networking

Multiple Network Interfaces

Lab: Working with Multiple VPC Networks

Quiz

VMs can have internal and external IP addresses



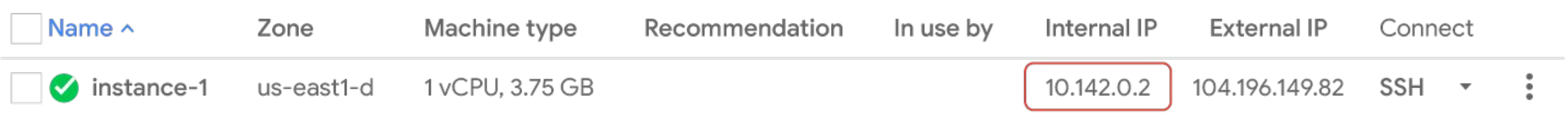
Internal IP

- 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

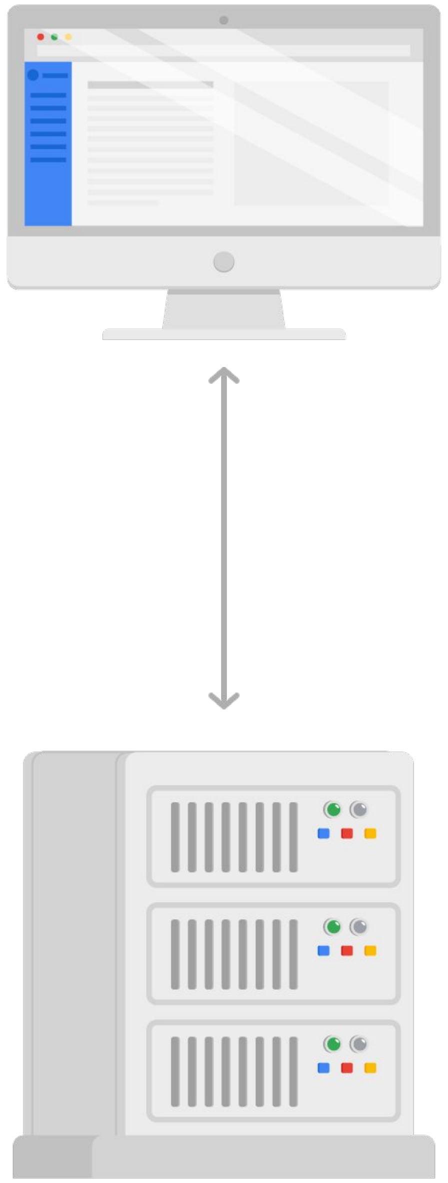
External IPs are mapped to internal IPs



□ 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



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

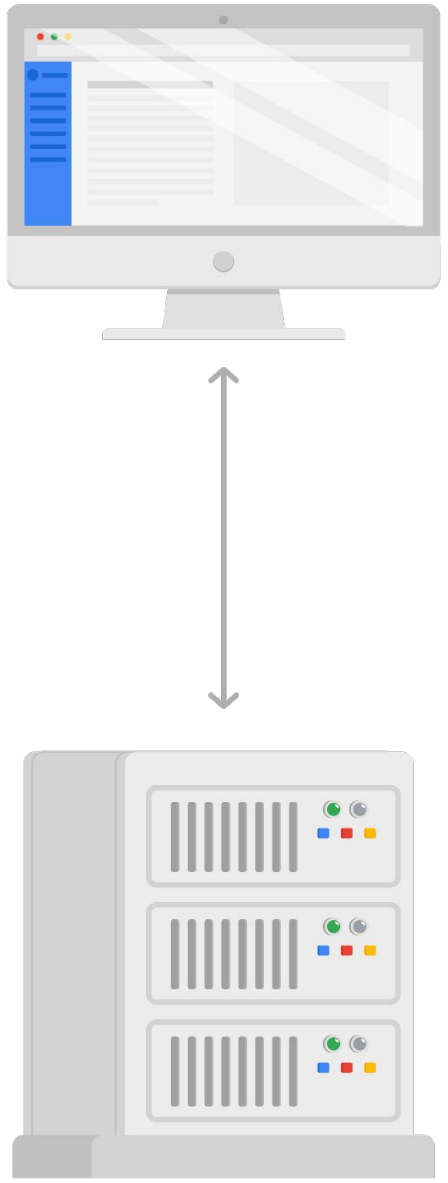
- The hostname is the same as the instance name.
- FQDN is `[hostname].[zone].c.[project-id].internal`.

Example: guestbook.asia-east1-b.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.

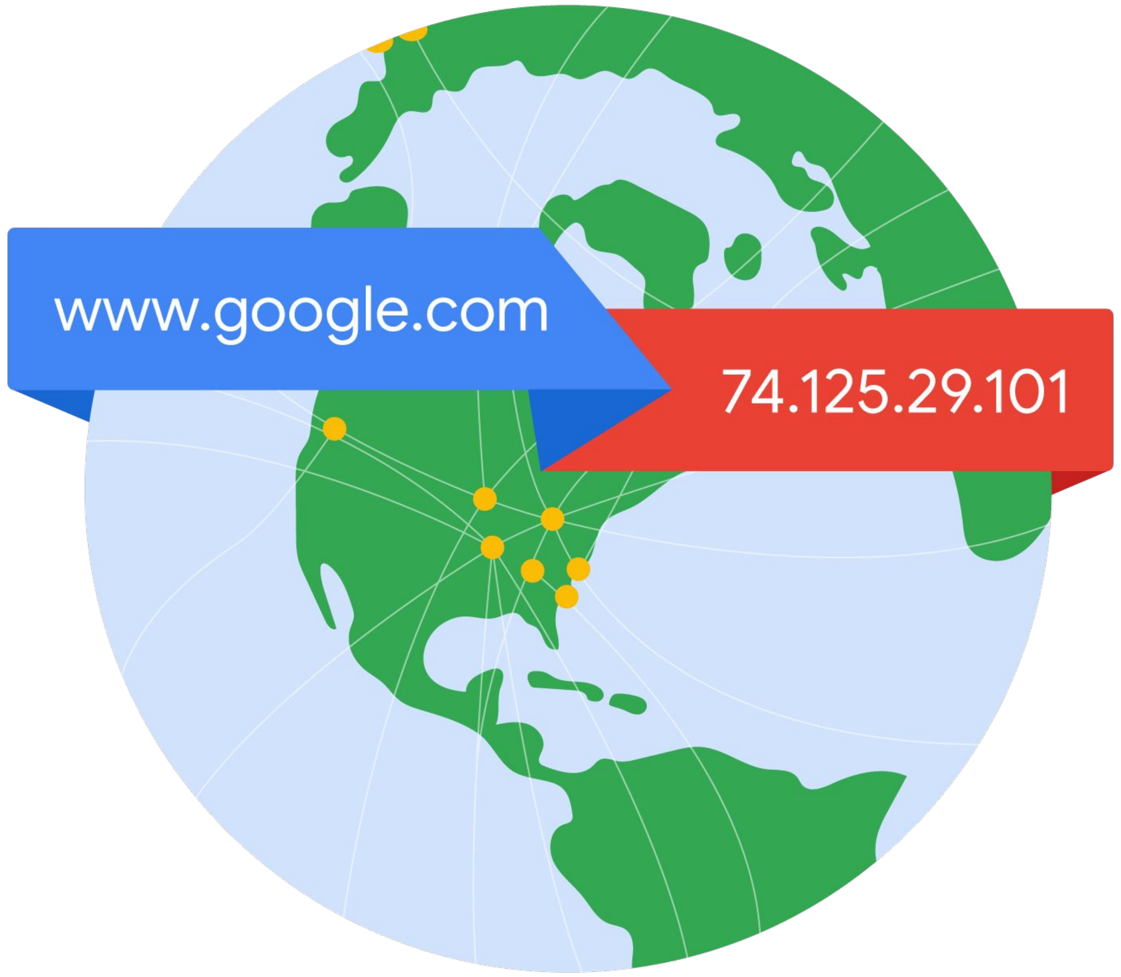
DNS resolution for external addresses



- Instances with external IP addresses can allow connections from hosts outside of 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

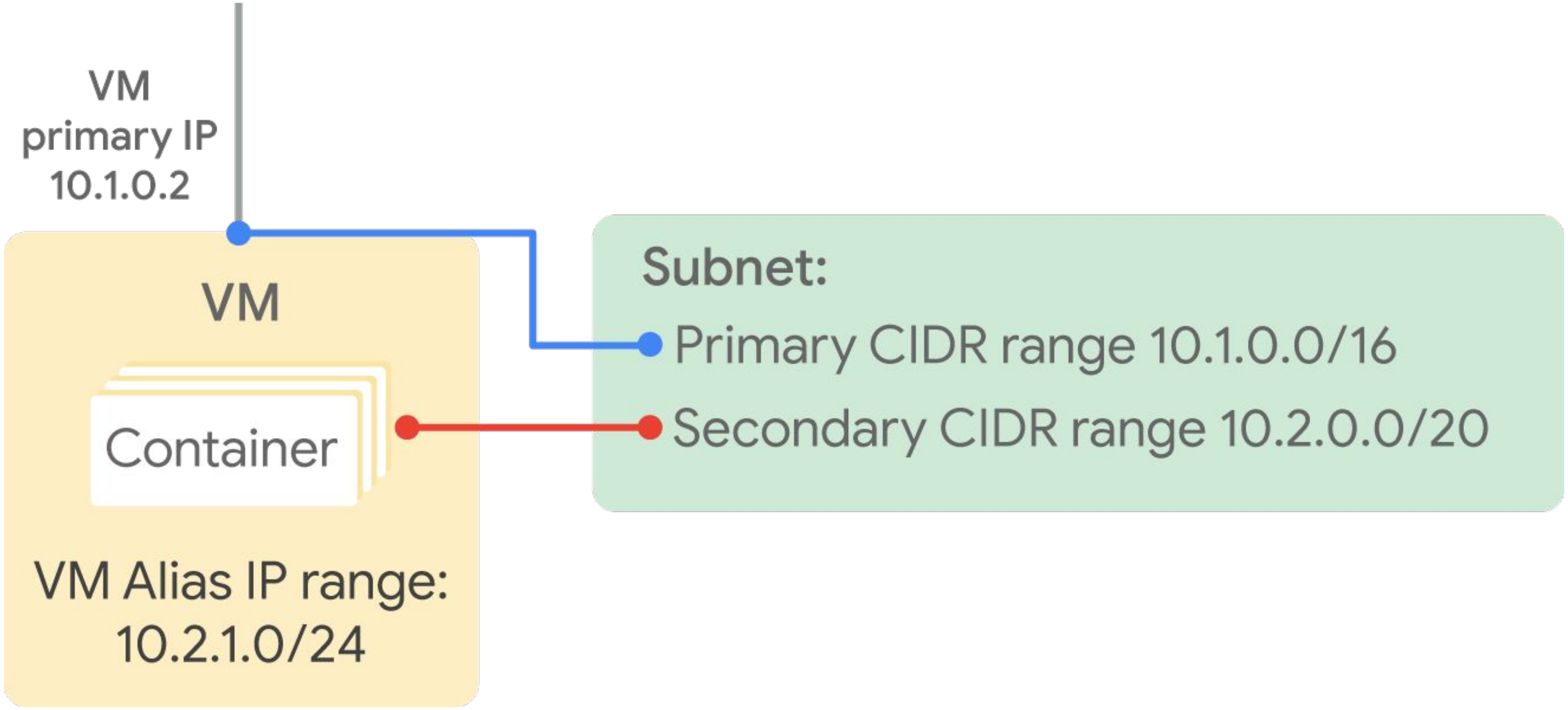
- Google's DNS service
- Translate domain names into IP address
- Low latency
- High availability (100% uptime SLA)
- Create and update millions of DNS records
- UI, command line, or API



Cloud DNS

Google Cloud

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



Agenda

Projects, Networks, and Subnetworks

IP Addresses

Routes and Firewall Rules

Lab: Getting Started with VPC Networking

Multiple Network Interfaces

Lab: Working with Multiple VPC Networks

Quiz

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

Every network has:

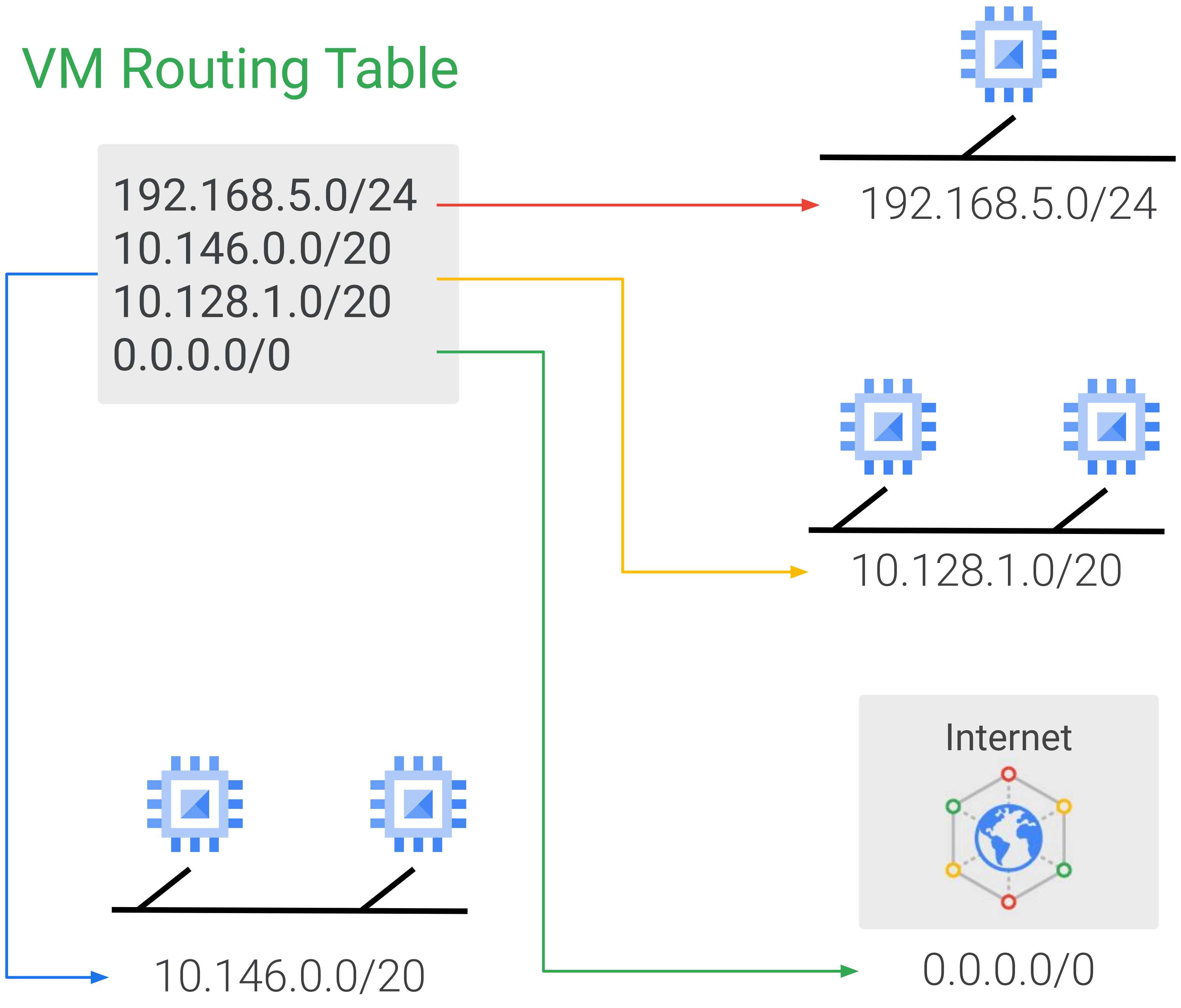
- Routes that let instances in a network send traffic directly to each other.
- A default route that directs packets to destinations that are outside the network.

Firewall rules must also allow the packet.

Cloud Routes

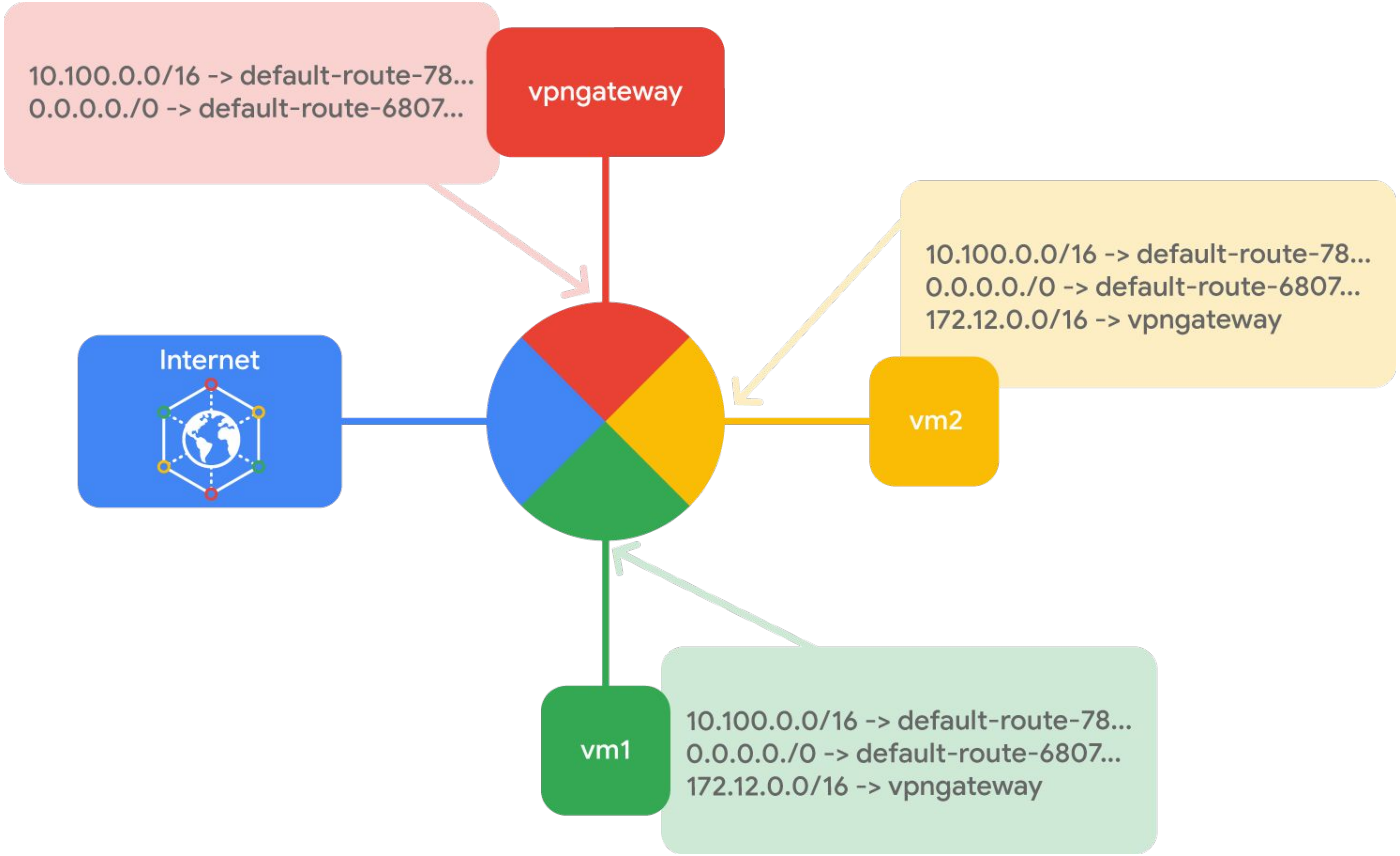
Routes map traffic to destination networks

- Destination in CIDR notation
- Applies to traffic egressing a VM
- Forwards traffic to most specific route
- Traffic is delivered only if it also matches a firewall rule
- Created when a subnet is created
- Enables VMs on same network to communicate



Google Cloud

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

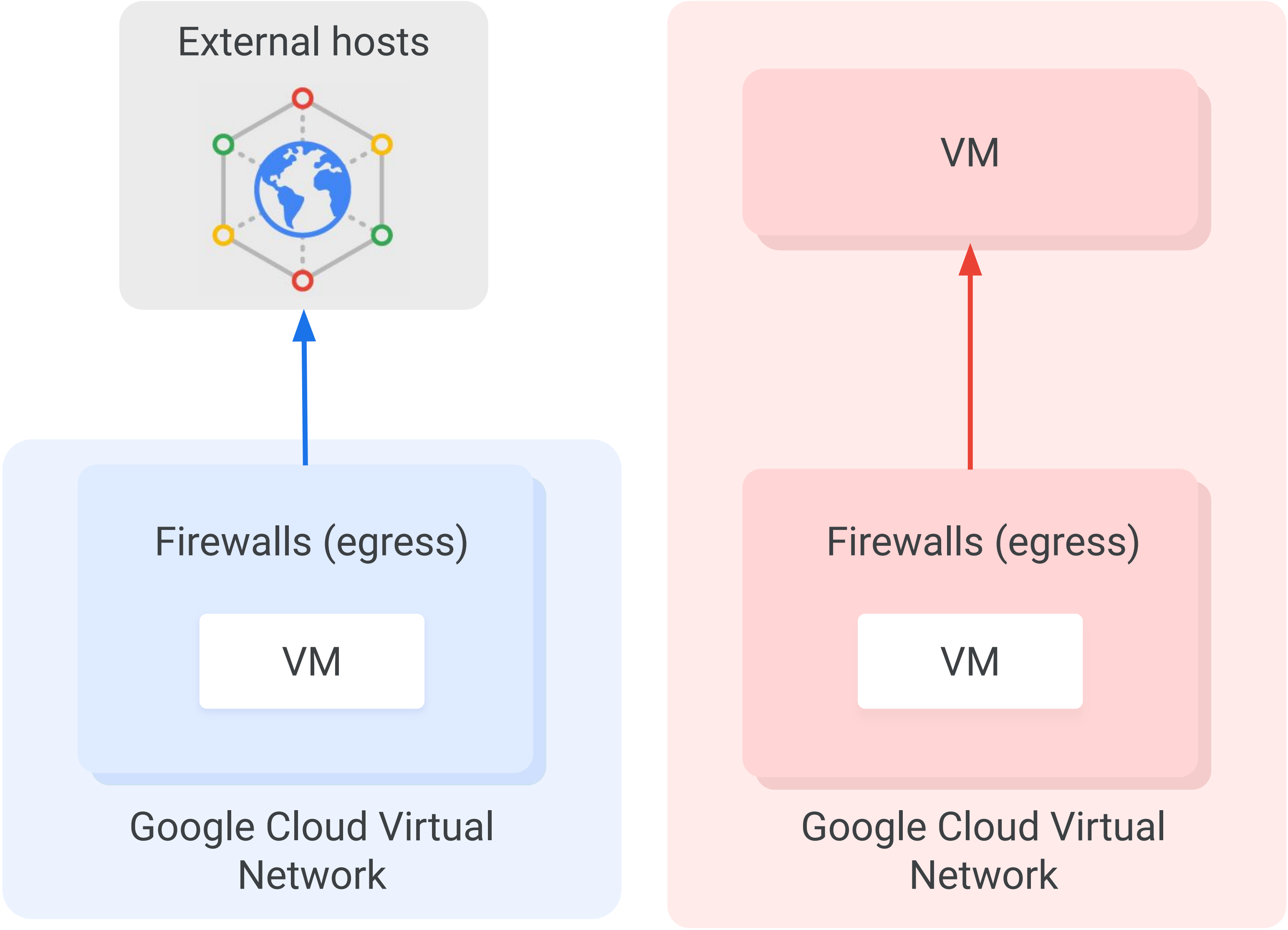
- VPC network functions as a distributed firewall.
- Firewall rules are applied to the network as a whole.
- Connections are allowed or denied at the instance level.
- Firewall rules are stateful.
- Implied deny all ingress and allow all egress.

Cloud
Firewall Rules

A firewall rule is composed of different parameters

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



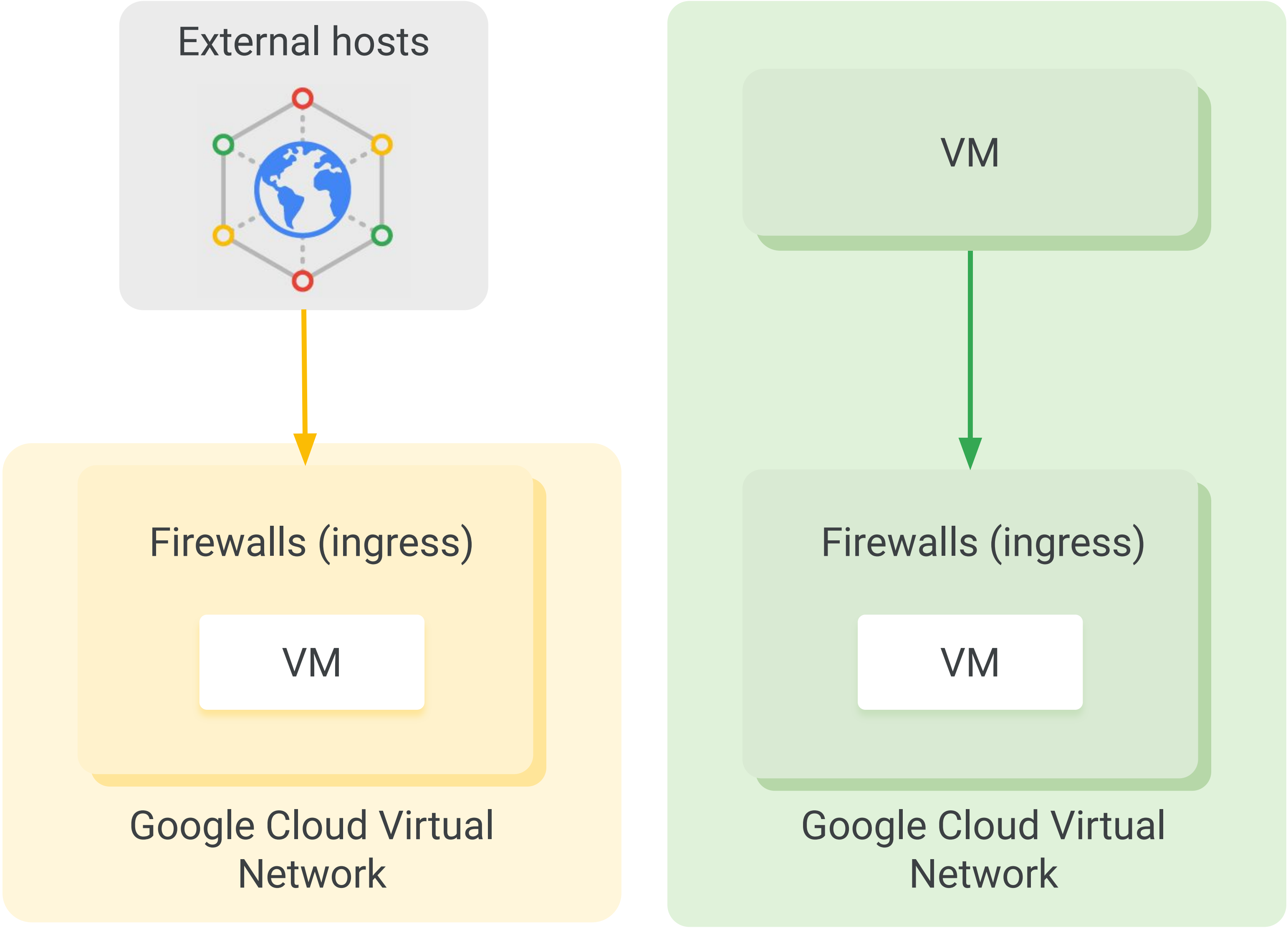
Conditions:

- Destination CIDR ranges
- Protocols
- Ports

Action:

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

Google Cloud firewall use case: Ingress



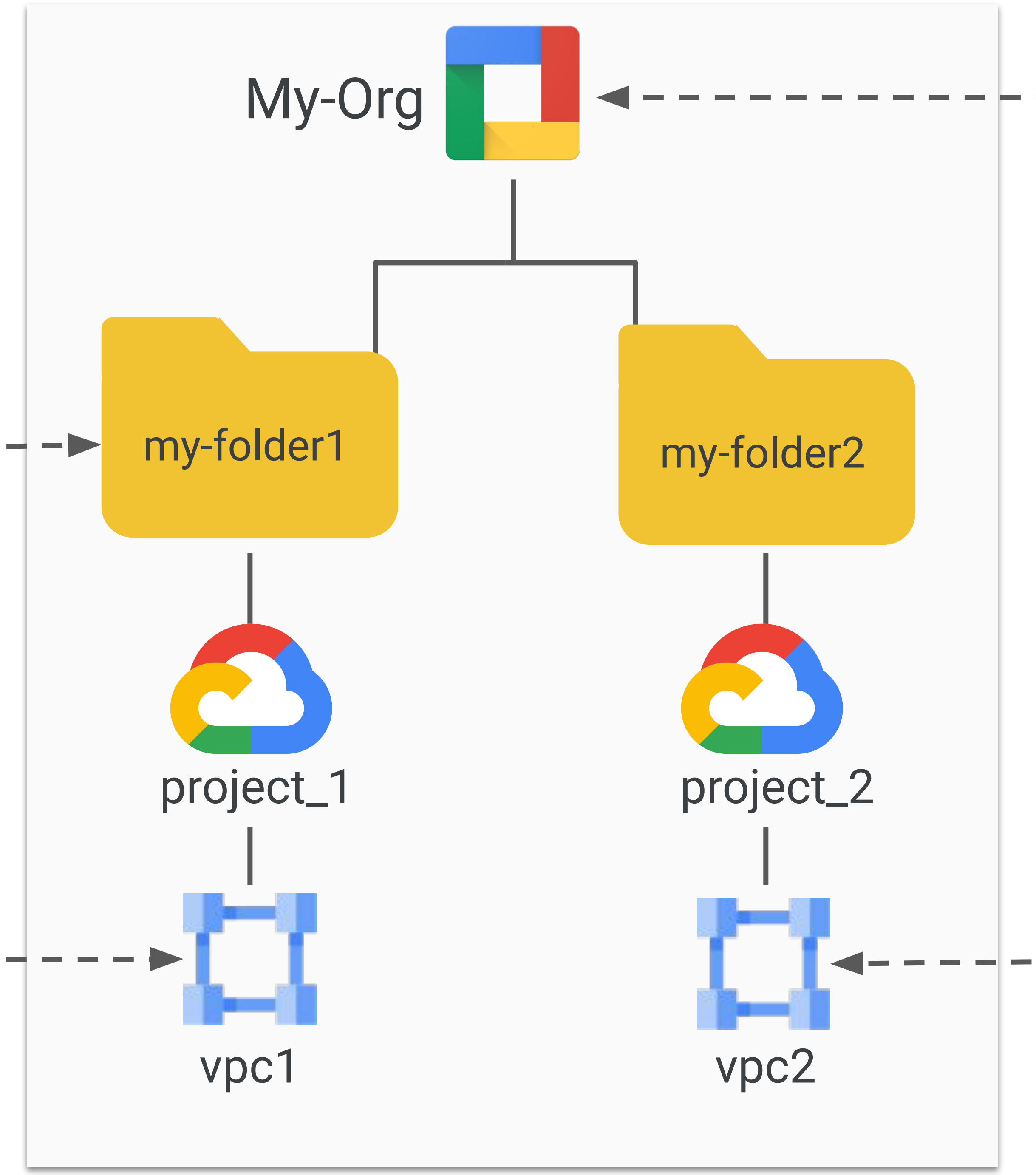
Conditions:

- Source CIDR ranges
- Protocols
- Ports

Action:

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

Hierarchical firewall policies



Ingress from 1.1.1.10/24 priority 1 go to_next
Ingress any:any priority 2 deny

Ingress tcp:80,443 priority 1 allow Ingress any:any priority 2 deny

Default ingress deny all, egress allow all

Ingress tcp:80,443,22 priority 1000 allow
Default ingress deny all, egress allow all

Agenda

Projects, Networks, and Subnetworks

IP Addresses

Routes and Firewall Rules

Lab: Getting Started with VPC Networking

Multiple Network Interfaces

Lab: Working with Multiple VPC Networks

Quiz

Lab Intro

Getting Started with VPC Networking

Duration: 30 minutes

Google Cloud

Lab objectives

Explore the default VPC network

Create an auto mode network with firewall rules

Create VM instances using Compute Engine

Explore the connectivity for VM instances

Agenda

Virtual Private Cloud (VPC)

Projects, Networks, and Subnetworks

IP Addresses

Routes and Firewall Rules

Lab: Getting Started with VPC Networking

Multiple Network Interfaces

Lab: Working with Multiple VPC Networks

Quiz

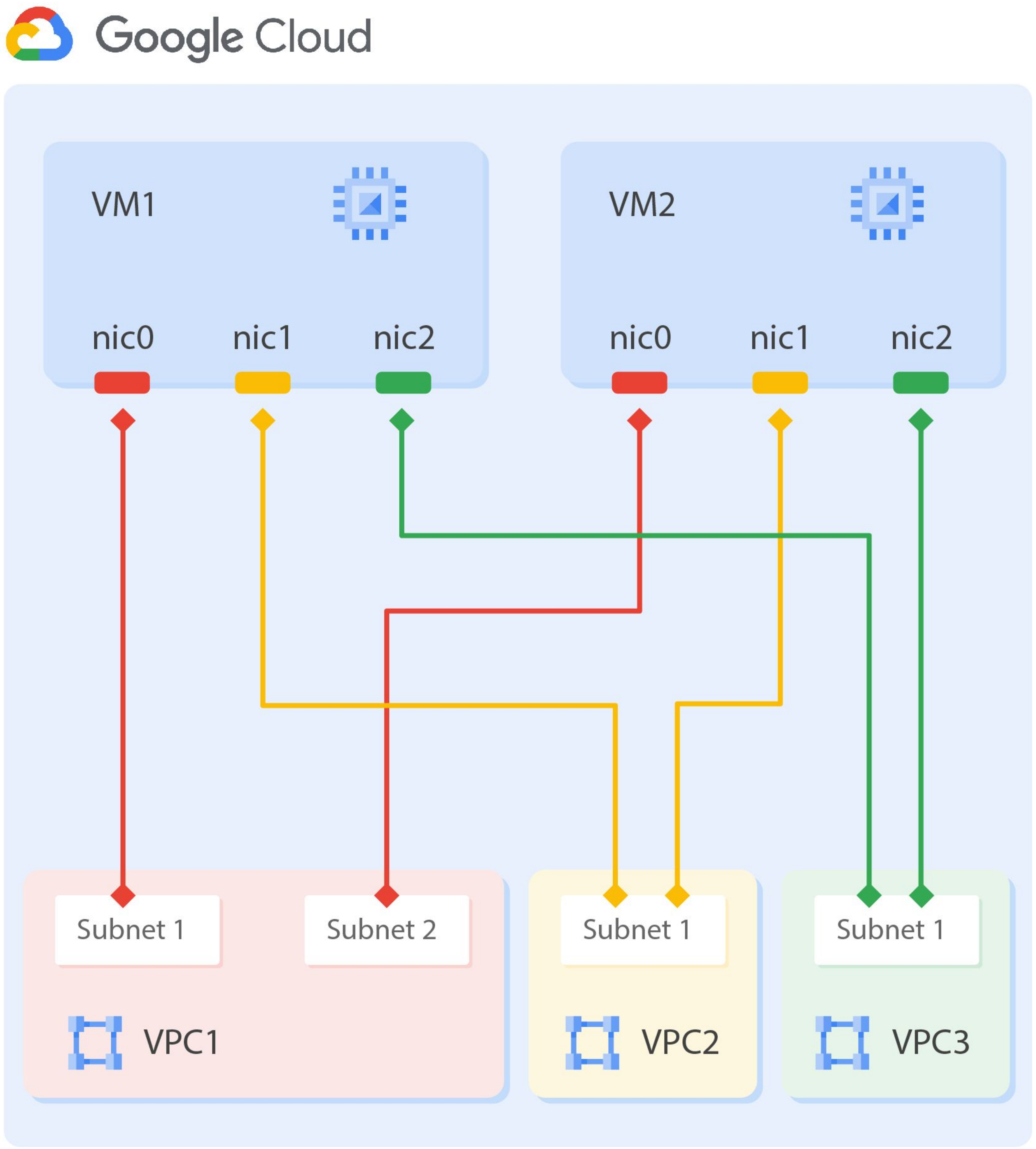
Multiple network interfaces

VPC networks are isolated (by default)

- Communicate within networks using **internal IP**
- Communicate across networks using **external IP**

Multiple Network Interfaces

- Network interface controllers (NICs)
- Each NIC is attached to a VPC network
- Communicate across networks using **internal IP**



Multiple network interfaces limitations

- Configure when you create instance
- Each interface in different network
- Networks’ IP range cannot overlap
- Networks must exist to create VM
- Cannot delete interface without deleting VM
- Internal DNS only associated to nic0
- Up to 8 NICs, depends on VM

Type of instance	# of virtual NICs
VM <= 2 vCPU	2 NICs
VM >2vCPU	1 NIC per vCPU (Max: 8)

Agenda

Virtual Private Cloud (VPC)

Projects, Networks, and Subnetworks

IP Addresses

Routes and Firewall Rules

Lab: Getting Started with VPC Networking

Multiple Network Interfaces

Lab: Working with Multiple VPC Networks

Quiz

Lab

Working with Multiple VPC Networks

Duration: 45 minutes

Google Cloud

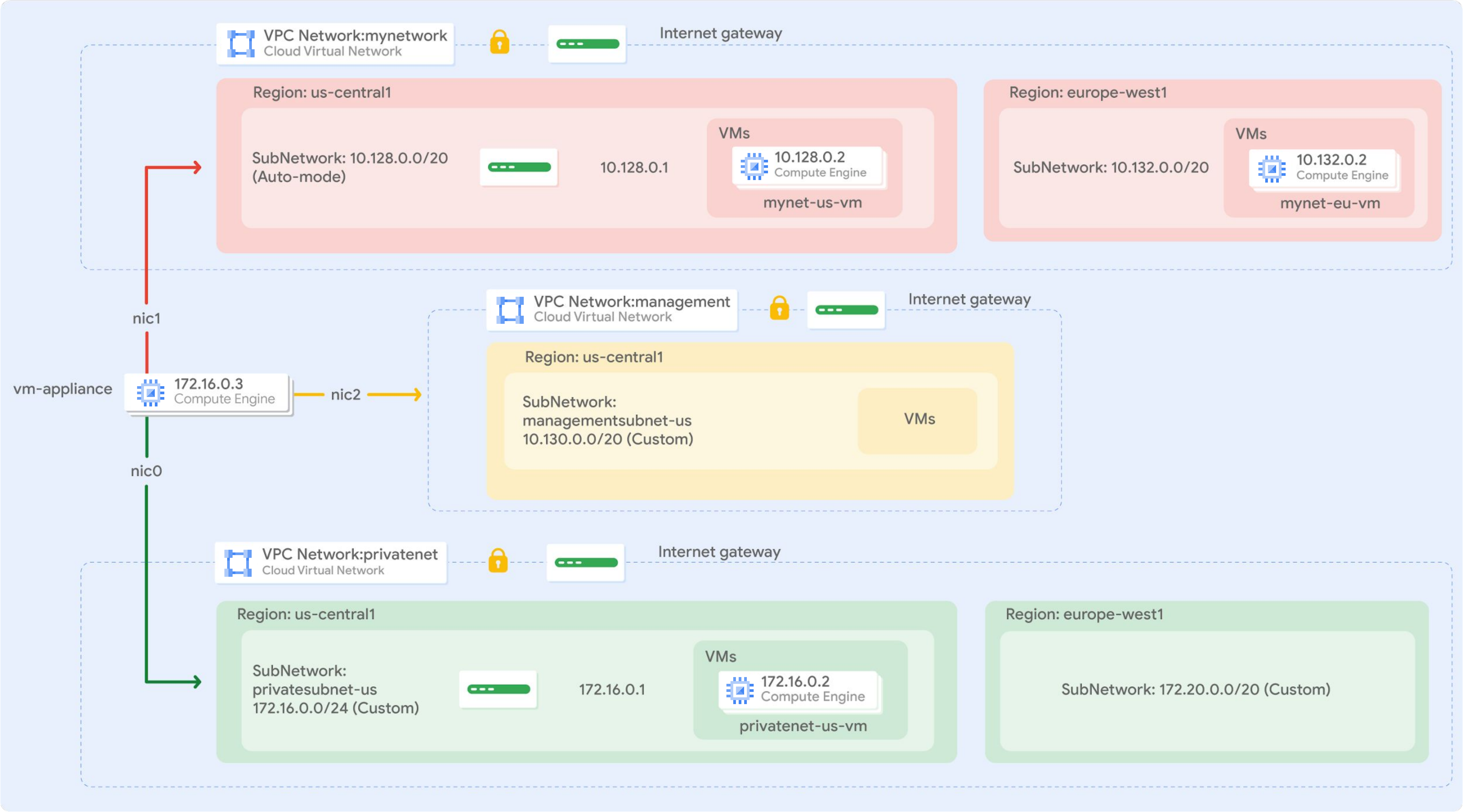
Lab objectives

Create custom mode VPC networks with firewall rules

Create VM instances using Compute Engine

Explore the connectivity for VM instances across VPC networks

Create a VM instance with multiple network interfaces


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
VMs
10.132.0.2
Compute Engine
mynet-eu-vm
nic1
vm-appliance
172.16.0.3
Compute Engine
nic2
nic0
VPC Network:management
Cloud Virtual Network
Internet gateway
Region: us-central1
SubNetwork:
managementsubnet-us
10.130.0.0/20 (Custom)
VMs
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: 172.20.0.0/20 (Custom)

Agenda

Projects, Networks, and Subnetworks

IP Addresses

Routes and Firewall Rules

Lab: Getting Started with VPC Networking

Multiple Network Interfaces

Lab: Working with Multiple VPC Networks

Quiz

Question #1

Question

In Google Cloud, a VPC network belongs to which of the following?

A. Project

B. Region

C. Zone

D. IP address range

Question #1

Answer

In Google Cloud, a VPC network belongs to which of the following?

A. Project

B. Region

C. Zone

D. IP address range

Question #2

Question

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

A. Zonal, regional, and global

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

C. Default network, auto network, and custom network

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

Question #2

Answer

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

A. Zonal, regional, and global

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

C. Default network, auto network, and custom network

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

Question #3

Question

Which Google Cloud service translates requests for domain names into external IP addresses?

A. Cloud DNS

B. Alias IP Ranges

C. Compute Engine DNS

D. Google Cloud routes

Question #3

Answer

Which Google Cloud service translates requests for domain names into external IP addresses?

A. Cloud DNS

B. Alias IP Ranges

C. Compute Engine DNS

D. Google Cloud routes

Google Cloud