Disclaimer

Thank you for your interest in using Google Cloud training material. We are excited about the content we are able to provide you (collectively, “Teaching Resources”) and hope you are too.

By using Teaching Resources, you agree to be bound by all of the following terms, as well as the Google terms of service and the Google privacy policy. Unless otherwise specified, terms used below will have the meanings described in the Google terms of service.

1. **Educational Use Only**. Teaching Resources is intended only for use teaching courses at regionally accredited or higher learning institutions. The content may be adapted, customize, remixed, and shared for educational use. Content may not be distributed, or otherwise exploited for any commercial purpose, commercial advantage, or private monetary compensation.

2. **Attribution Requirements**. If you distribute, publicly perform, display, transmit, publish, or otherwise make available any Teaching Resources or any derivative works thereof, you must attribute the material you use back to the Teaching Resources, but not in any way that suggests Google, any of its affiliates, or any of its third party content providers endorse you or your use of such materials. If you adapt, remix, or customize the Teaching Resources please include the following text on each edited slide: *“The original content was provided by Google LLC and modified for the purpose of the course, without input or endorsement from Google LLC.”*

3. Descriptions of Google products, services, infrastructure and processes contained in the Teaching Resources are descriptions for teaching and learning purposes only and do not constitute a guarantee, promise, or representation of accuracy by Google. Pricing, availability or features of Google Cloud products and services described in the Teaching Resources may change.

It Helps to Network

Course map

Module 1	Module 2	Module 3	Module 4	Module 5
So, What's the Cloud Anyway?	Start with a Solid Platform	Use Google Cloud to Build Your Apps	Where Do I Store This Stuff?	There's an API for That!
Module 6	**Module 7**	**Module 8**	**Module 9**	**Module 10**
You Can't Secure the Cloud, Right?	It Helps to Network	Let Google Keep an Eye on Things	You Have the Data, but What Are You Doing with It?	Let Machines Do the Work

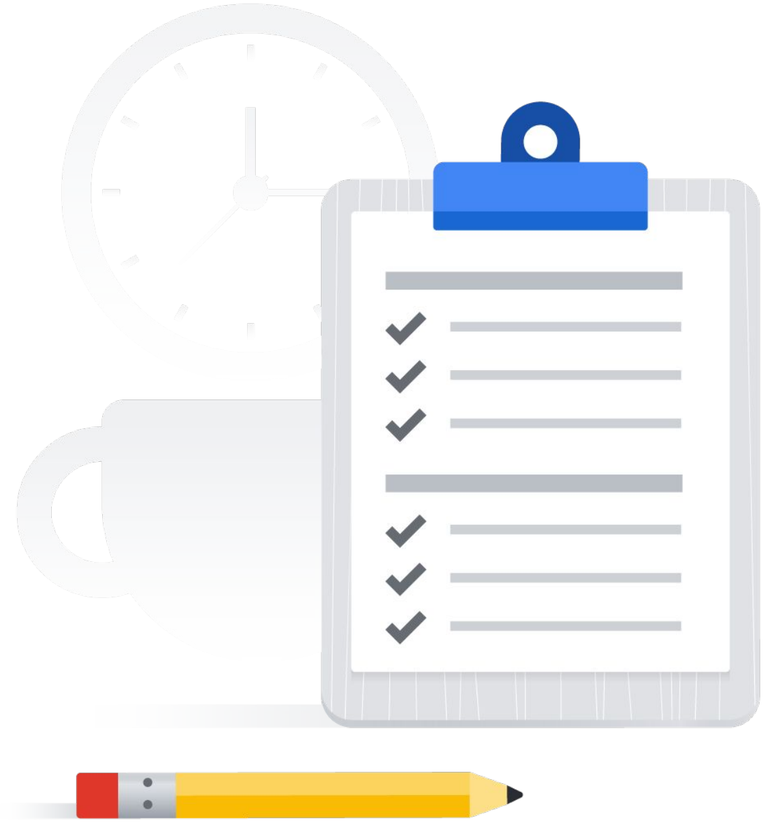
Google Cloud skills badges

Google Cloud

Learn how to ... (1/2)

Demonstrate how to build secure networks in the cloud

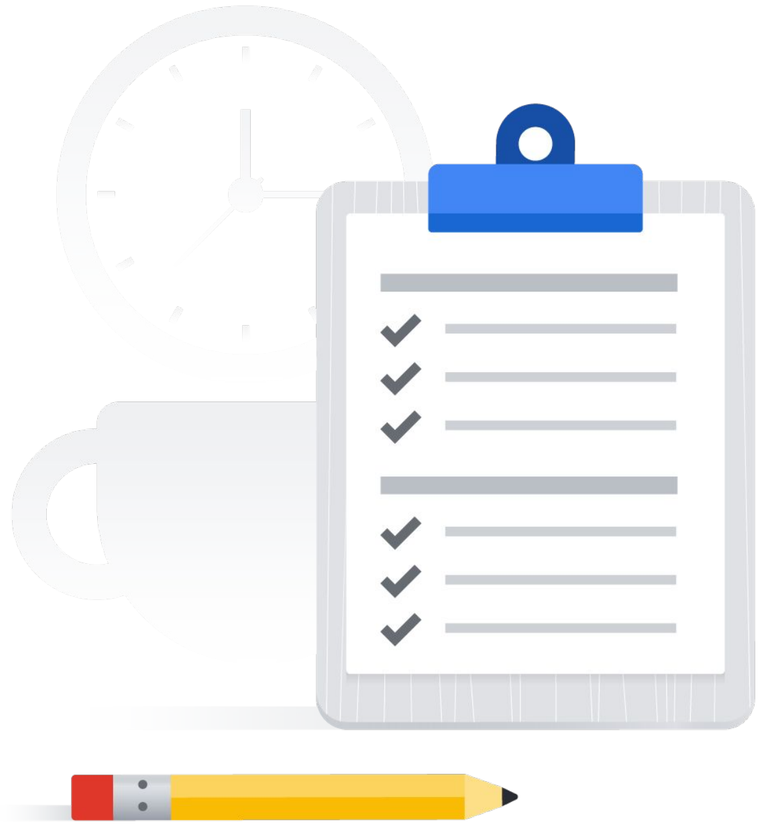
- Explore basic networking in the cloud
- Discuss how to build virtual private clouds (VPCs)
- Explain the use of public and private IP addresses in the cloud
- Describe the Google Network, including regions, zones, cache nodes, points of presence (PoPs), and fiber architecture
- Explore the role of firewall rules and routes



Google Cloud

Learn how to ... (2/2)

- Explore hybrid cloud networking options including virtual private networks (VPNs), interconnect, and direct peering
- Differentiate between load balancing options in the cloud



Google Cloud

Agenda (1/3)

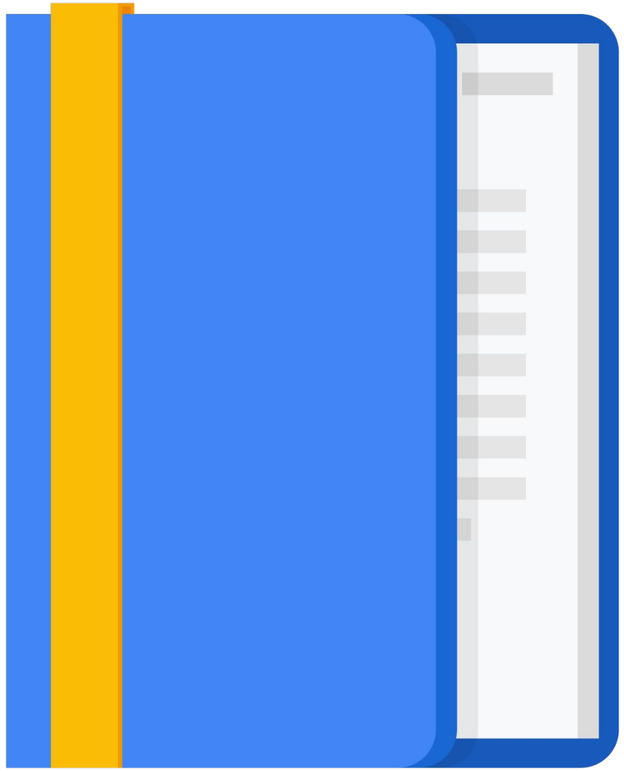
Introduction to Networking in the Cloud

Defining a Virtual Private Cloud

Public and Private IP Address Basics

Google’s Network Architecture

Routes and Firewall Rules in the Cloud



Google Cloud

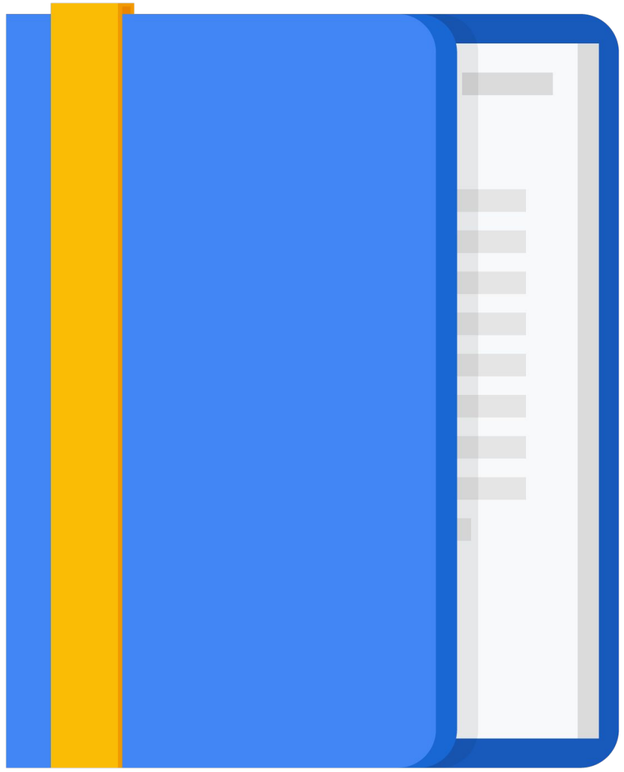
Agenda (2/3)

Multiple VPC Networks

Lab: Multiple VPC Networks

Lab: VPC Networks - Controlling Access

Building Hybrid Clouds using VPNs, Interconnecting, and Direct Peering



Google Cloud

Agenda (3/3)

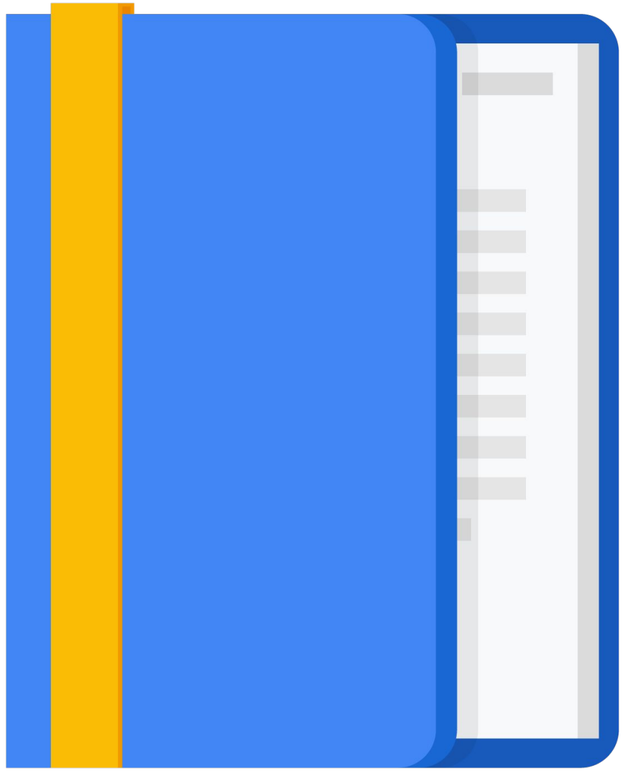
Different Options for Load Balancing

Lab: HTTP Load Balancer with Cloud Armor

Lab: Create an Internal Load Balancer

Quiz

Summary



Google Cloud

Agenda

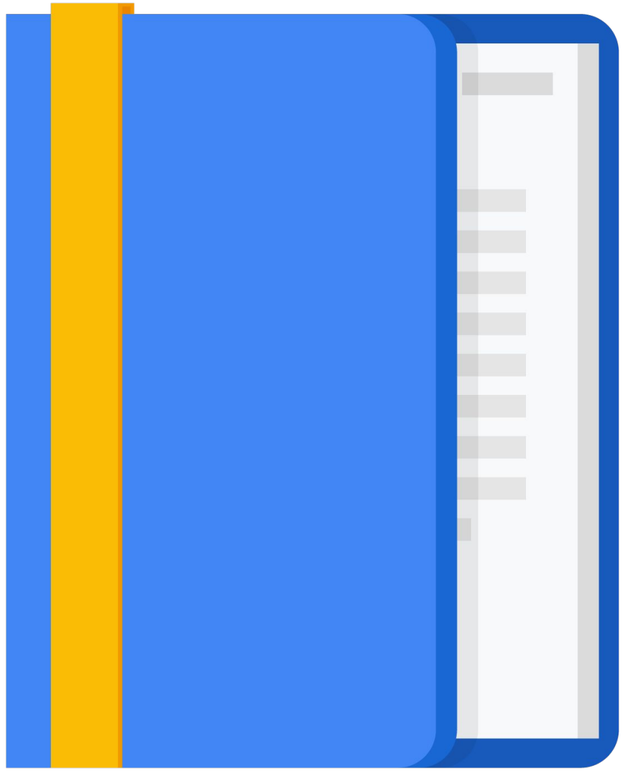
Introduction to Networking in the Cloud

Defining a Virtual Private Cloud

Public and Private IP Address Basics

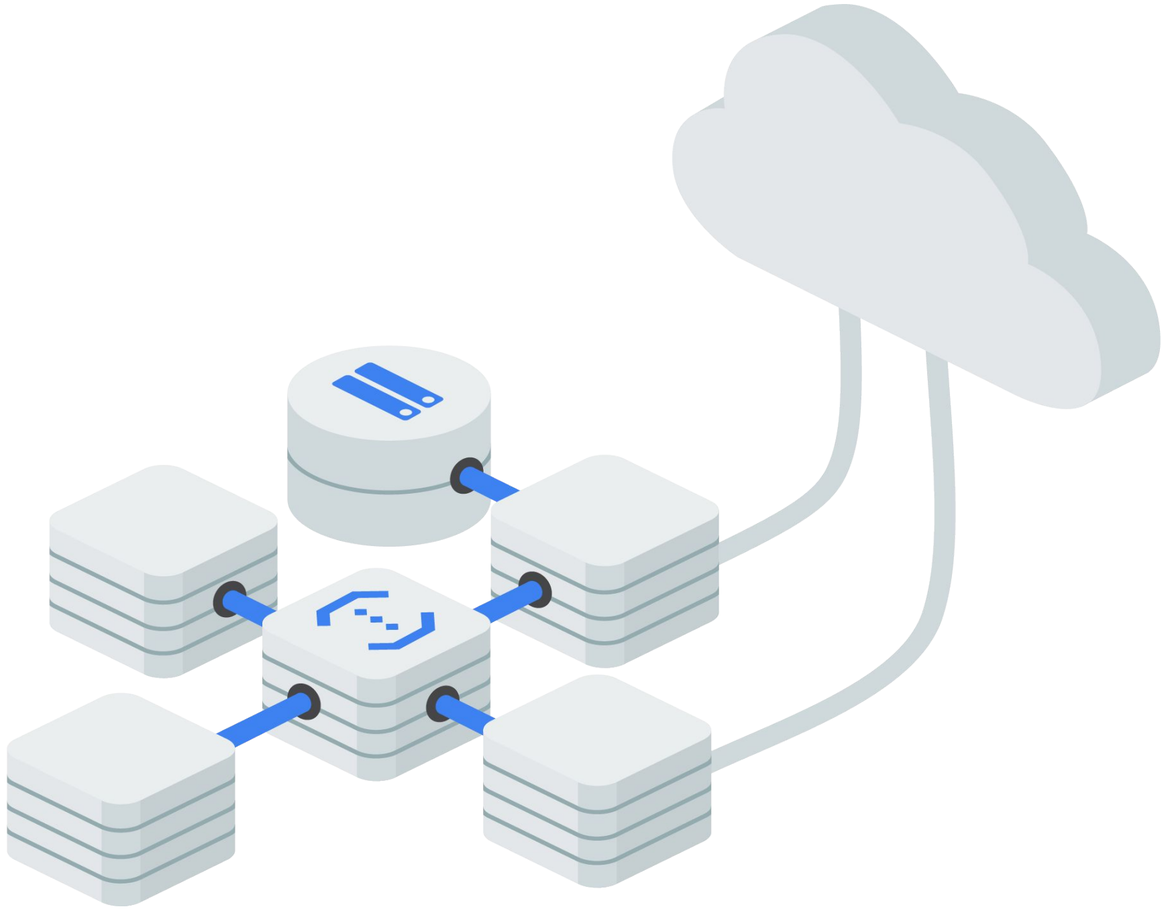
Google’s Network Architecture

Routes and Firewall Rules in the Cloud

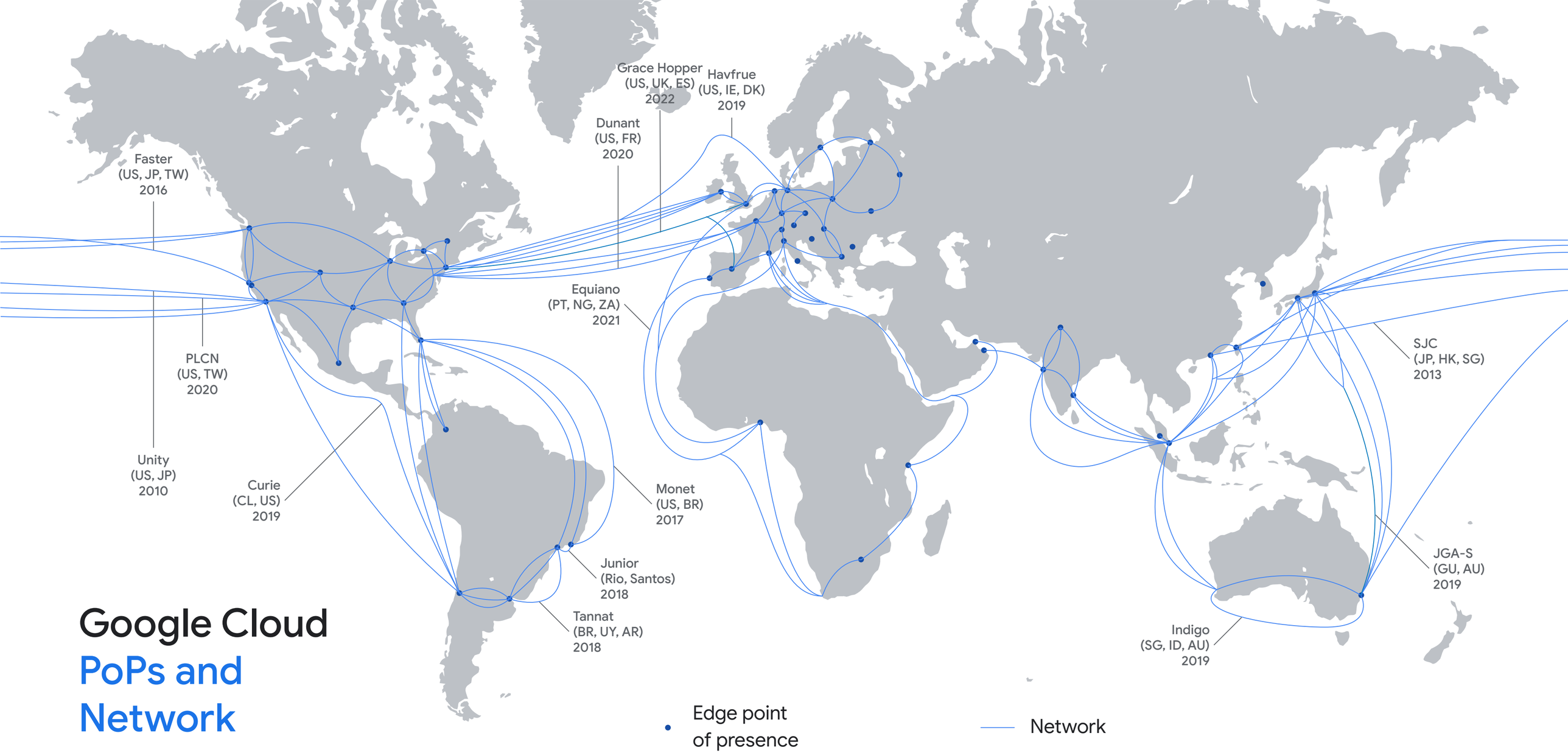


Google Cloud

A background to networking



Google Cloud



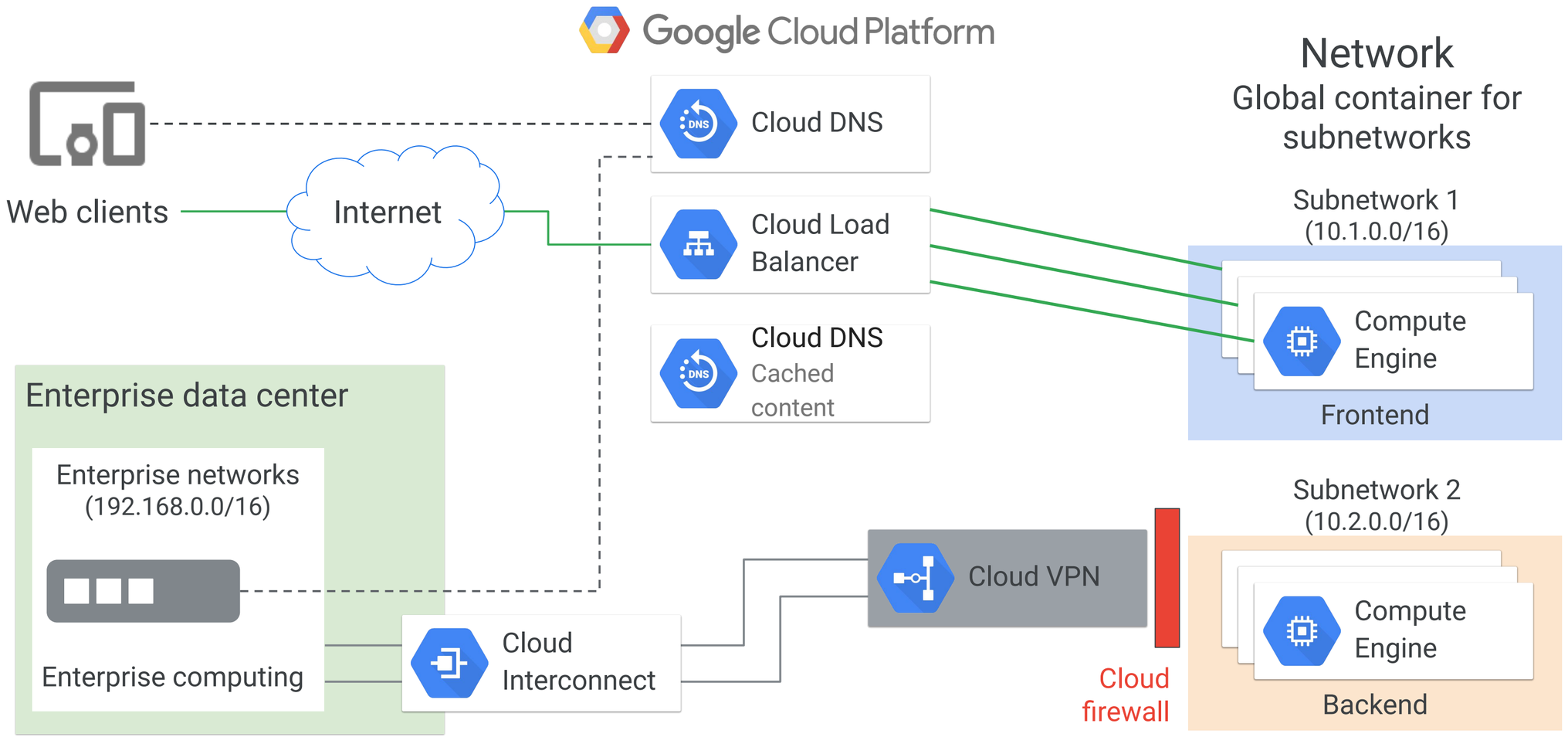
Google Cloud
PoPs and Network

Edge point of presence

Network

Google Cloud

How Google networking works



Google Cloud

Agenda

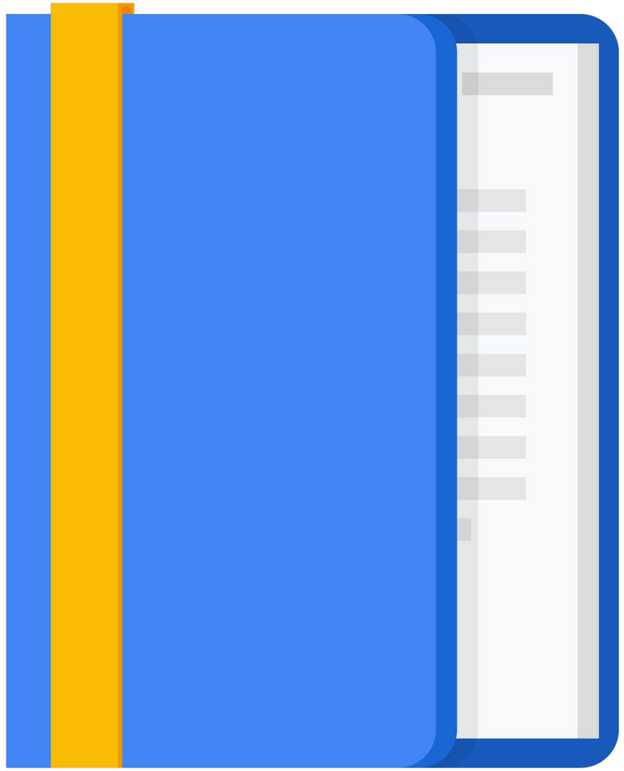
Introduction to Networking in the Cloud

Defining a Virtual Private Cloud

Public and Private IP Address Basics

Google's Network Architecture

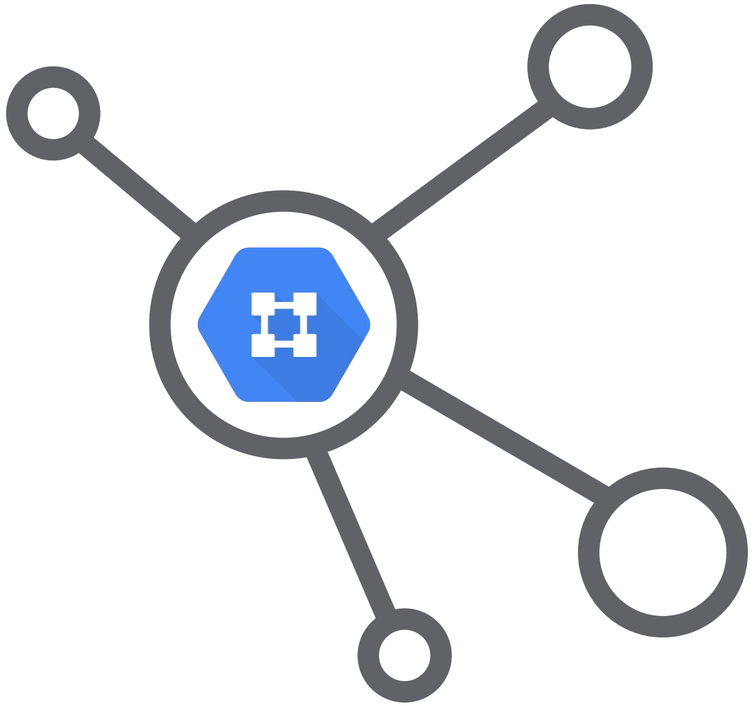
Routes and Firewall Rules in the Cloud



Google Cloud

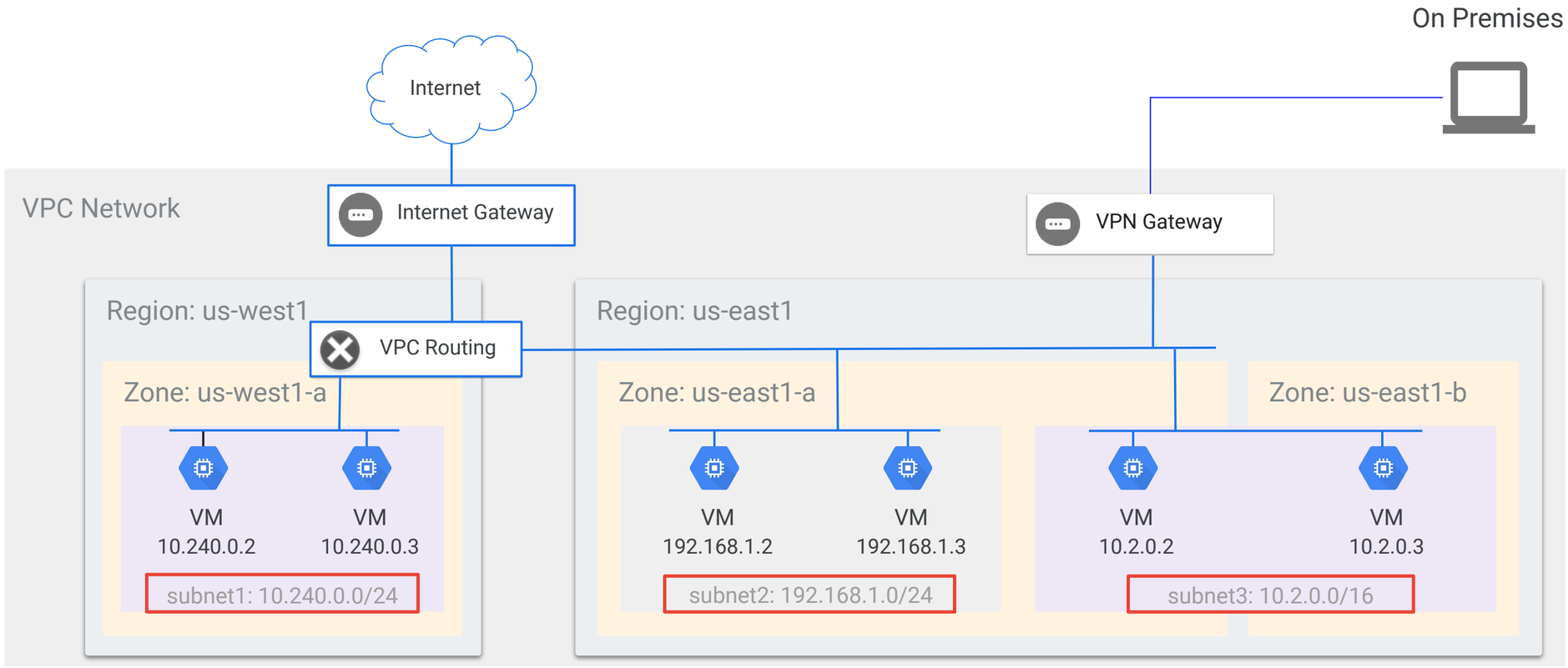
VPCs are software defined network (SDN) constructs

- Allow the deployment of IaaS resources
- No IP address ranges
- Global
- Contain subnets



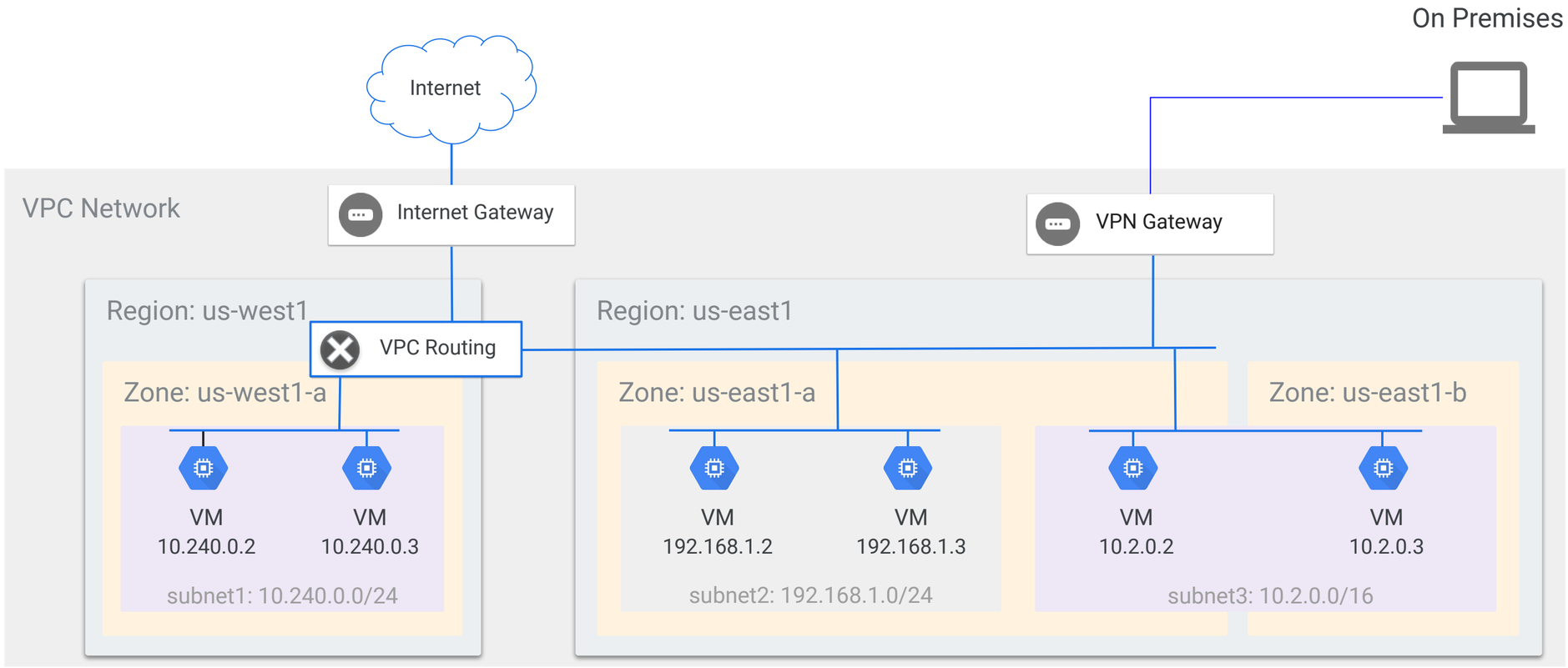
Google Cloud

A VPC network is a virtual version of a physical network and is a global resource



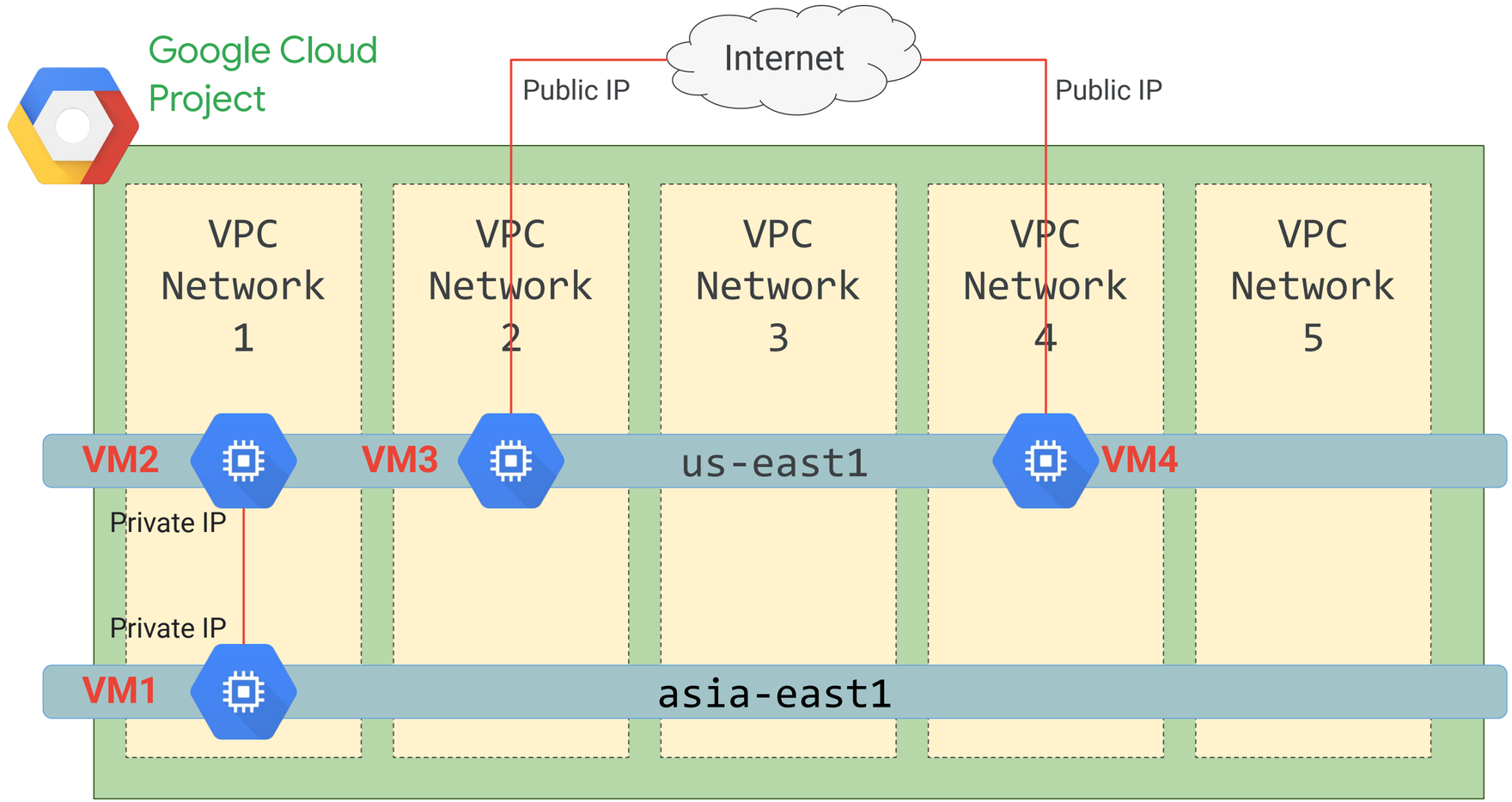
Google Cloud

Subnets are regional and extend across zones in the same region



Google Cloud

Network behavior within a project



Google Cloud

The differences between auto and custom networks

Auto subnet mode

- One subnet from each region is automatically created
- Set of predefined IP ranges
- Comes with default firewall rules
- Expandable up to /16 only
- Good for isolated use cases (Proof of concepts (PoCs), testing, etc.)

Custom subnet mode

- No subnets are automatically created
- Subnets and IP ranges are defined
- No default firewalls rules
- Expandable to any RFC 1918 size
- Recommended for Production environments

Google Cloud

Agenda

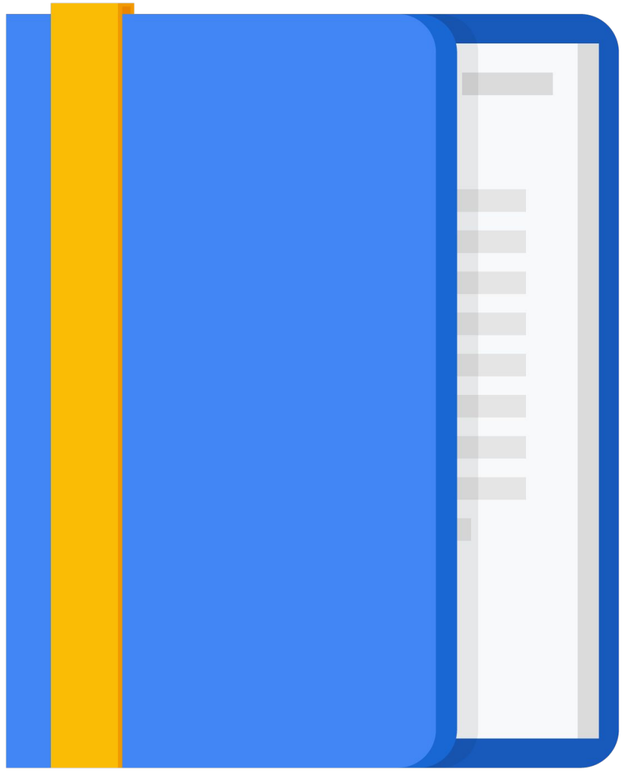
Introduction to Networking in the Cloud

Defining a Virtual Private Cloud

Public and Private IP Address Basics

Google's Network Architecture

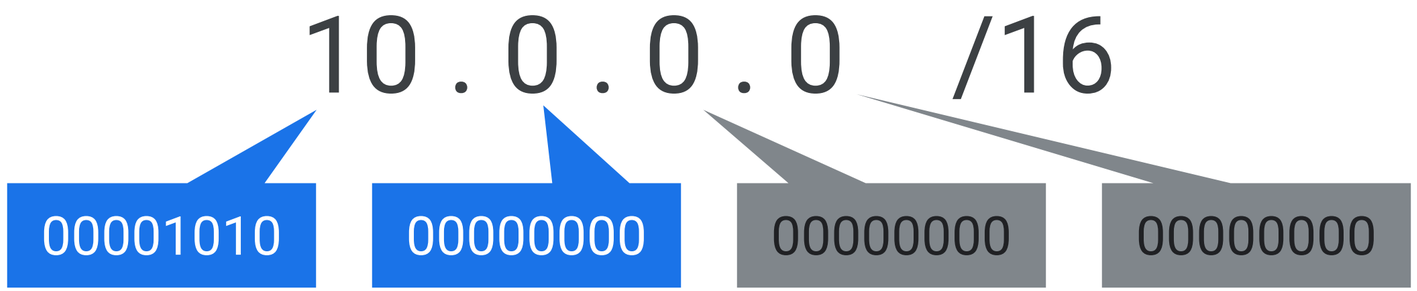
Routes and Firewall Rules in the Cloud



Google Cloud

A VPC is made up of subnets

- Subnets need to be configured with a private IP address range.
- IP addresses are used for internal network communication.
- Each octet is represented by 8 bits.
- The /## determines the number of address bits that are static.



/16 freezes first two octets

Google Cloud

A /16 range will provide 65,536 available IP addresses

- The CIDR range determines how many IP addresses are available.
- Adding 1 to the /## will cut the available IP addresses in half.

CIDR IP address totals						
/16	/17	/18	/19	/20	/21	/22
65,536	**32,768**	**16,384**	**8,192**	**4,096**	**2,048**	**1,024**
/23	/24	/25	/26	/27	/28	
512	**256**	**128**	**64**	**32**	**16**	

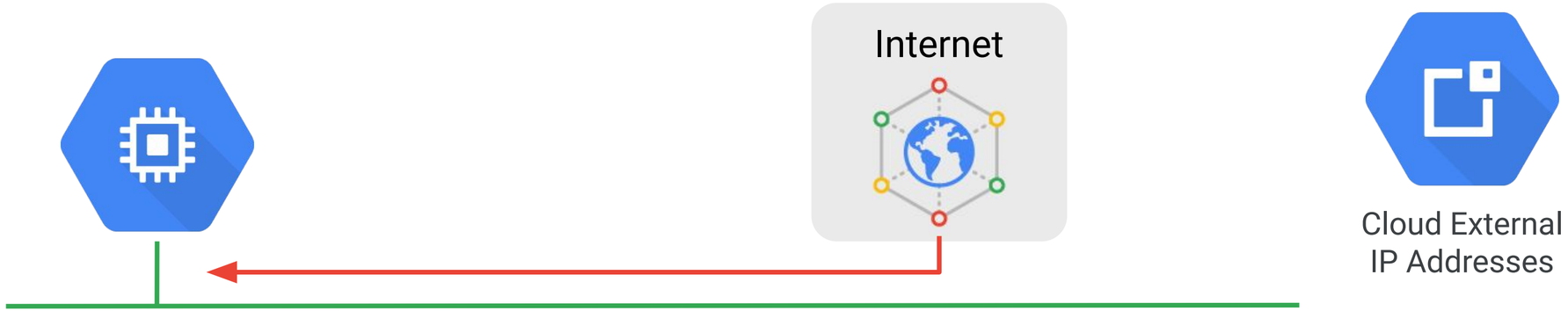
Google Cloud

https://serverfault.com/questions/12854/cidr-for-dummies

CIDR	Dotted Quad
/8	255.0.0.0
/16	255.255.0.0
/24	255.255.255.0
/32	255.255.255.255

CIDR	Dotted Quad
/24	255.255.255.0
/25	255.255.255.128
/26	255.255.255.192
/27	255.255.255.224
/28	255.255.255.240
/29	255.255.255.248
/30	255.255.255.252
/31	255.255.255.254
/32	255.255.255.255

Public and Private IP address basics



Internal IP

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

External IP

- Can be assigned from pool (ephemeral) or reserved (static).
- Billed when not attached to a running VM.
- VM doesn't know the external IP; it's mapped to the internal IP.

Google Cloud

Agenda

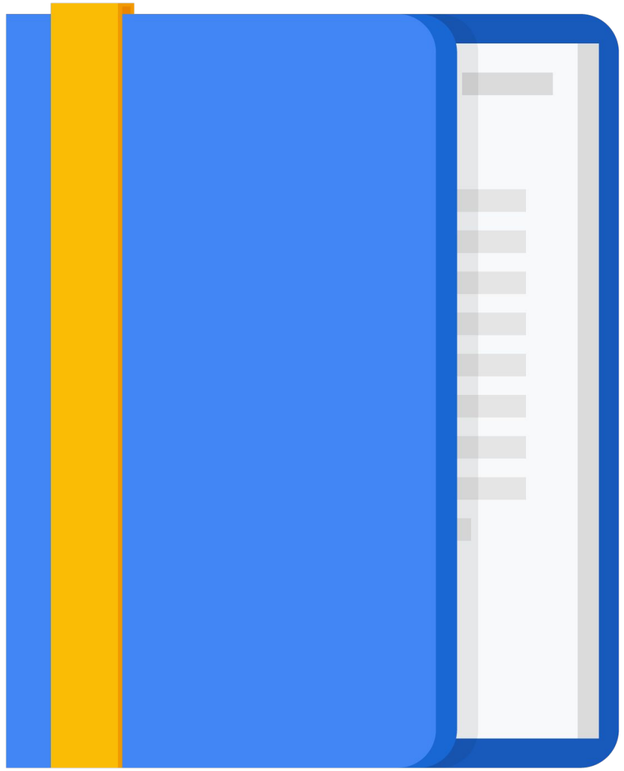
Introduction to Networking in the Cloud

Defining a Virtual Private Cloud

Public and Private IP Address Basics

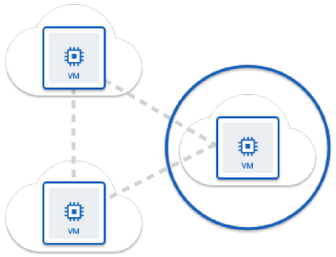
Google’s Network Architecture

Routes and Firewall Rules in the Cloud



Google Cloud

The primary products included in Google networking

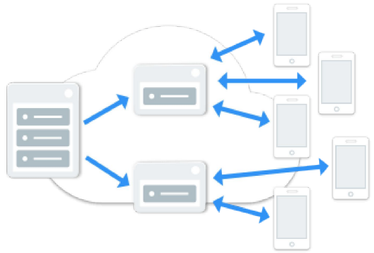


Virtual Private Cloud

Manage networking for resources

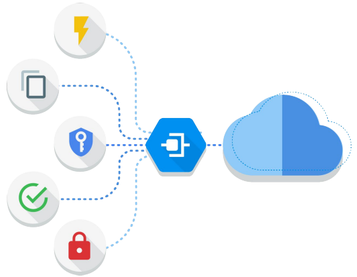
Cloud Load Balancer

Worldwide autoscaling and load balancing



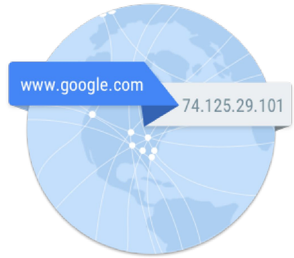
Cloud CDN

Content delivery network



Cloud Interconnect

Fast, high availability interconnect



Cloud DNS

Highly available global DNS network

Google Cloud

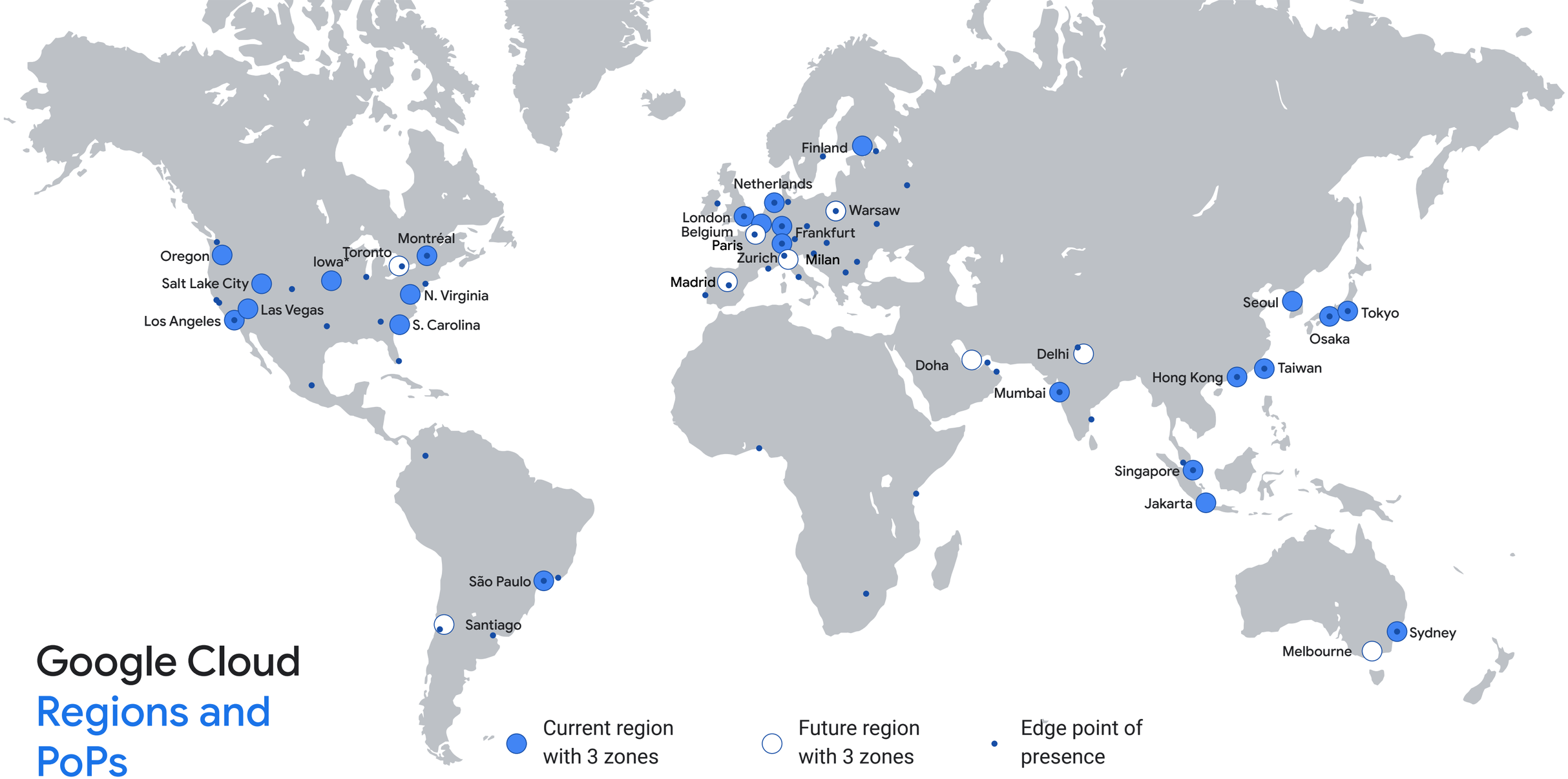
Google Cloud
Regions and Zones

Current region with 3 zones

Future region with 3 zones

* Exception: region has 4 zones.

Google Cloud



Google Cloud
Regions and PoPs

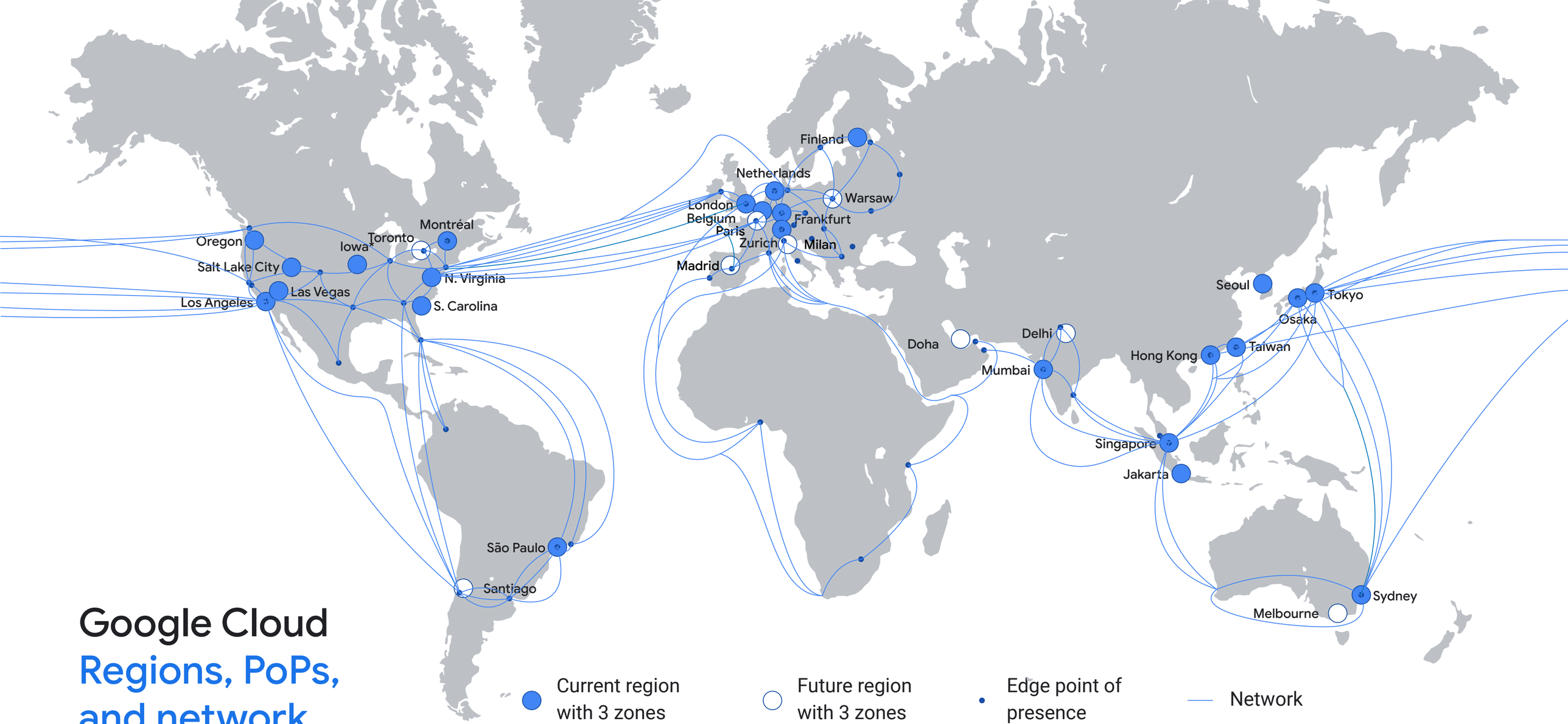
Current region with 3 zones

Future region with 3 zones

Edge point of presence

* Exception: region has 4 zones.

Google Cloud



Google Cloud
Regions, PoPs, and network

Current region with 3 zones

Future region with 3 zones

Edge point of presence

Network

* Exception: region has 4 zones.

Google Cloud

Agenda

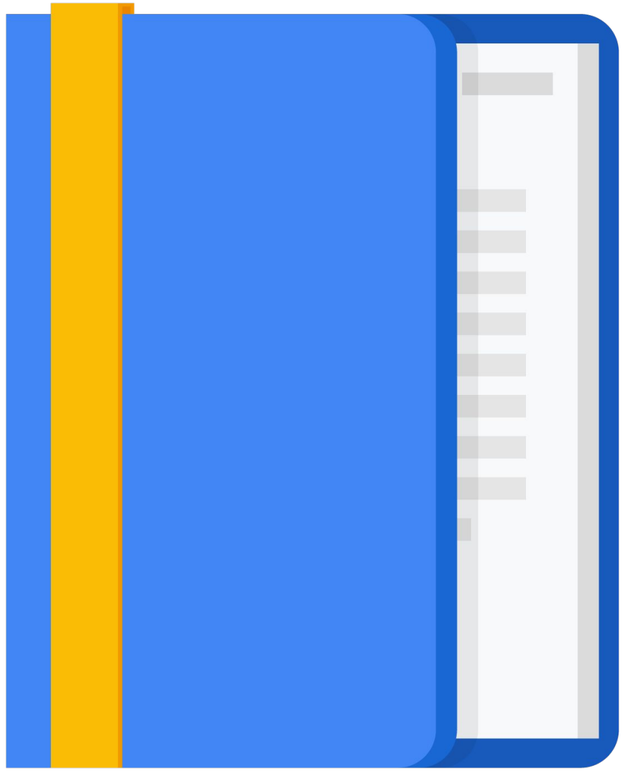
Introduction to Networking in the Cloud

Defining a Virtual Private Cloud

Public and Private IP Address Basics

Google's Network Architecture

Routes and Firewall Rules in the Cloud



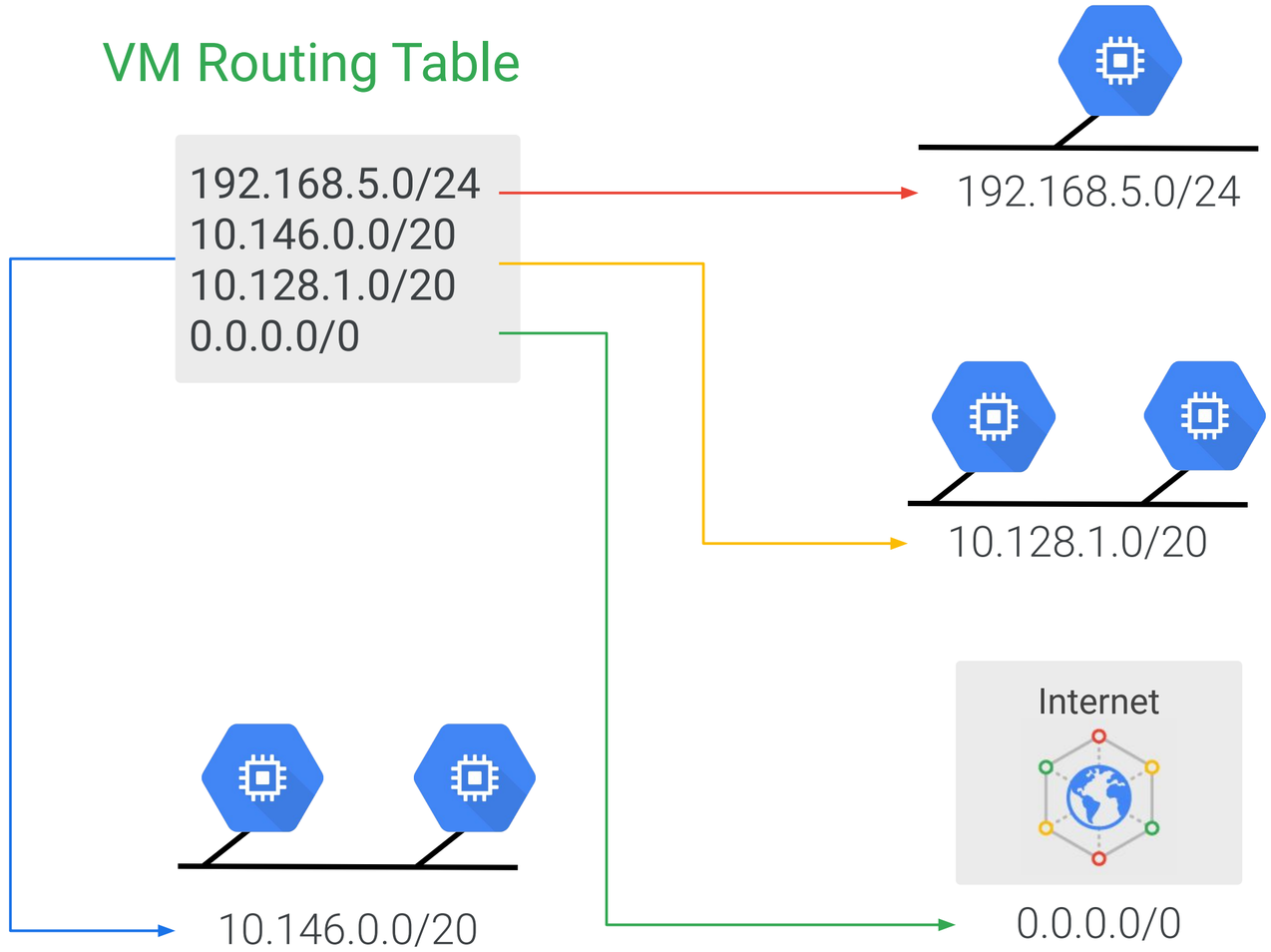
Google Cloud

A route maps an IP range to a destination

- Every network has routes that let instances in a network send traffic directly to each other.
- Every network has a default route that directs packets to destinations that are outside the network.
- Firewall rules must also allow the packet.

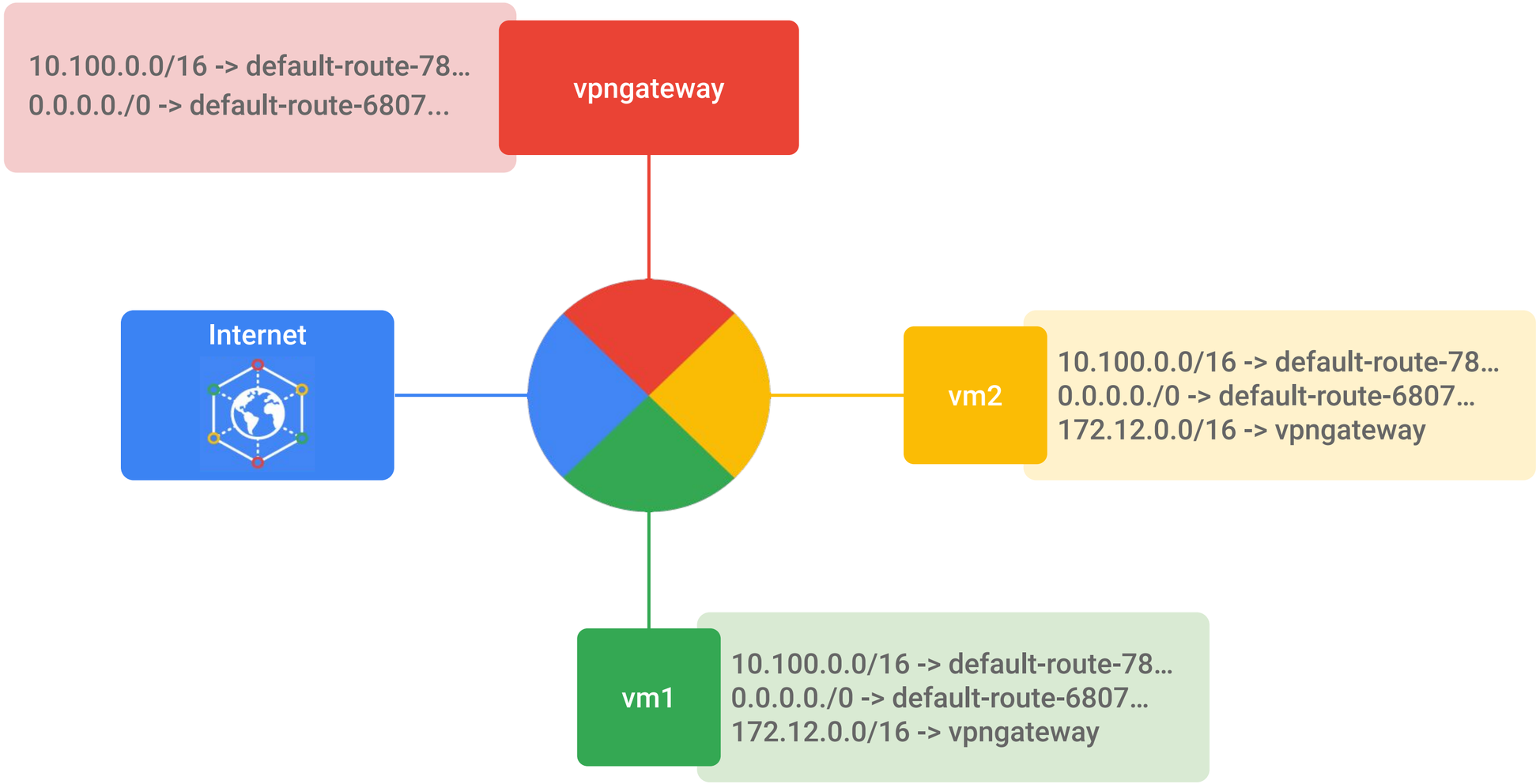
Google Cloud

Routes map traffic to destination networks



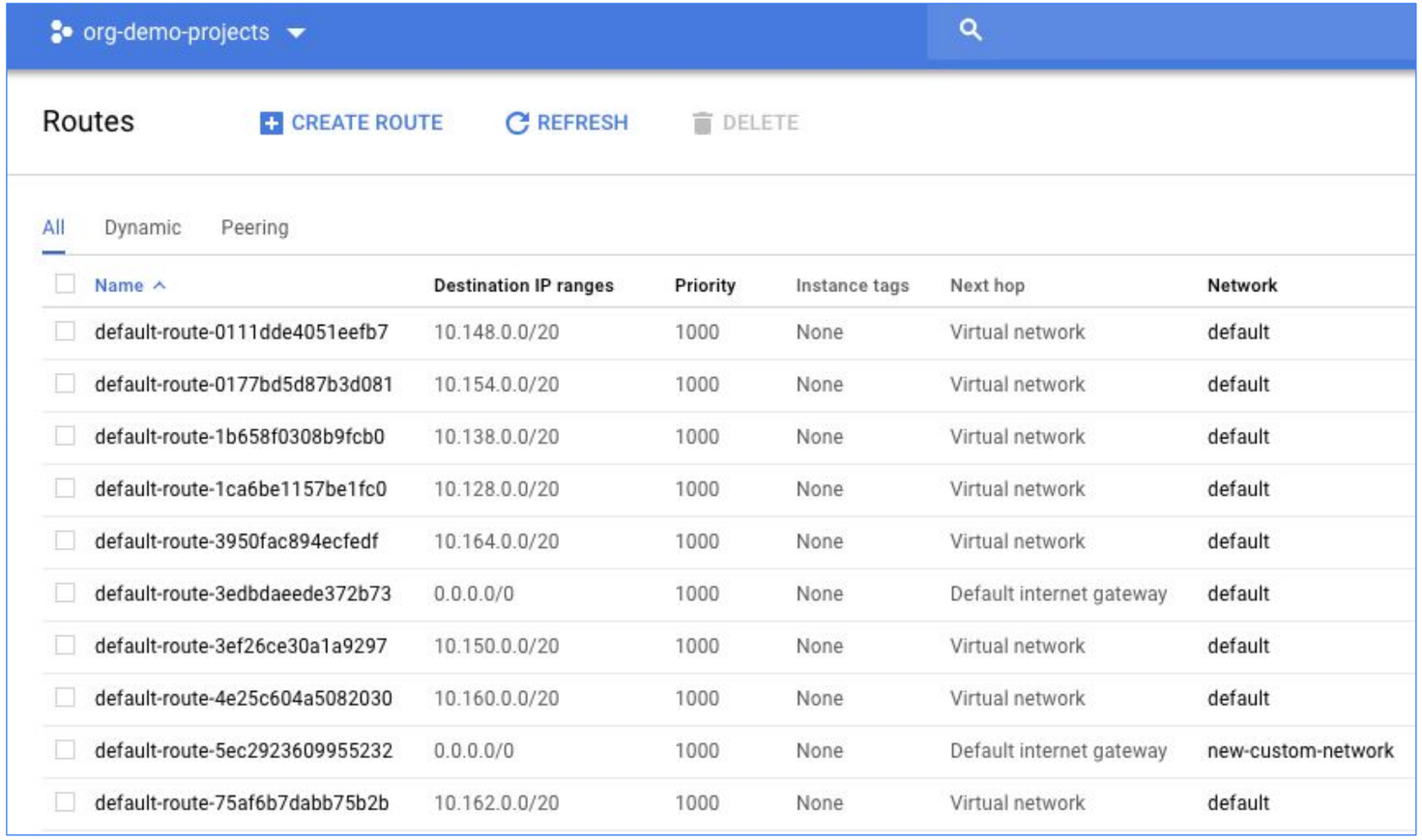
Google Cloud

Instance routing tables



Google Cloud

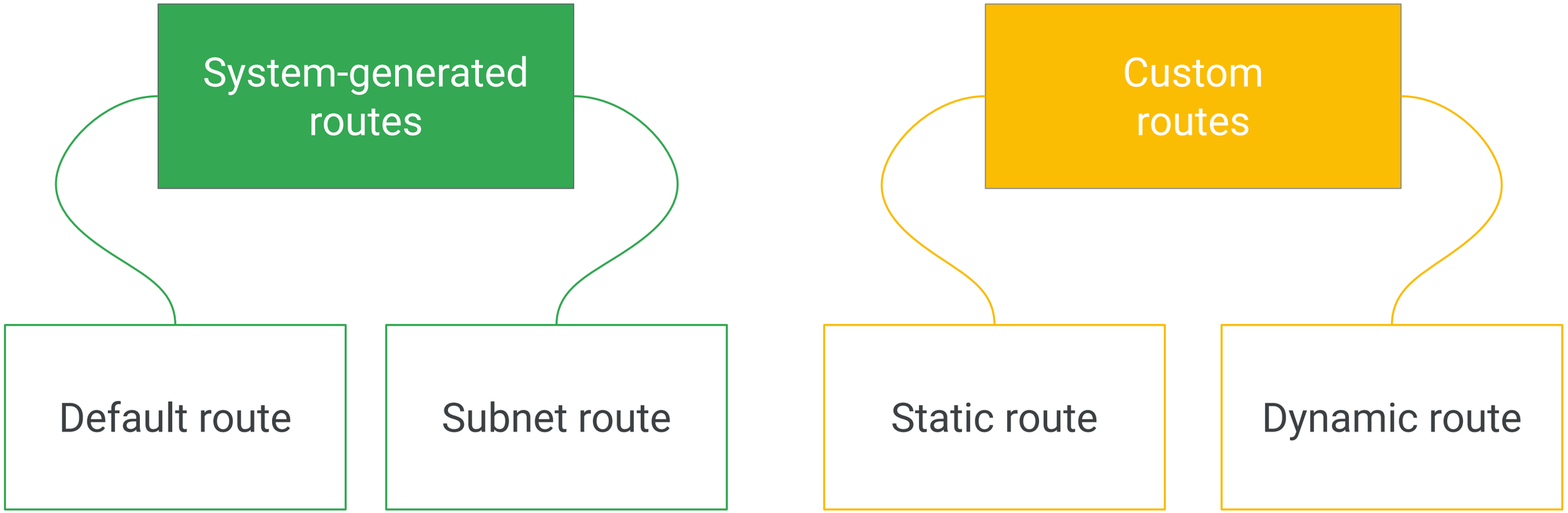
Routes define the paths network traffic takes from a VM instance to other destinations



Name	Destination IP ranges	Priority	Instance tags	Next hop	Network
default-route-0111dde4051eefb7	10.148.0.0/20	1000	None	Virtual network	default
default-route-0177bd5d87b3d081	10.154.0.0/20	1000	None	Virtual network	default
default-route-1b658f0308b9fcb0	10.138.0.0/20	1000	None	Virtual network	default
default-route-1ca6be1157be1fc0	10.128.0.0/20	1000	None	Virtual network	default
default-route-3950fac894ecfedf	10.164.0.0/20	1000	None	Virtual network	default
default-route-3edbdaeede372b73	0.0.0.0/0	1000	None	Default internet gateway	default
default-route-3ef26ce30a1a9297	10.150.0.0/20	1000	None	Virtual network	default
default-route-4e25c604a5082030	10.160.0.0/20	1000	None	Virtual network	default
default-route-5ec2923609955232	0.0.0.0/0	1000	None	Default internet gateway	new-custom-network
default-route-75af6b7dabb75b2b	10.162.0.0/20	1000	None	Virtual network	default

Google Cloud

There are four different types of routes



Google Cloud

The routing order

1. Subnet routes are considered first.
2. Google Cloud then looks for another route with the most specific destination.
3. If more than one route has the same most specific destination, Google Cloud considers the priority of the route.
4. If no applicable destination is found, Google Cloud drops the packet.

Google Cloud

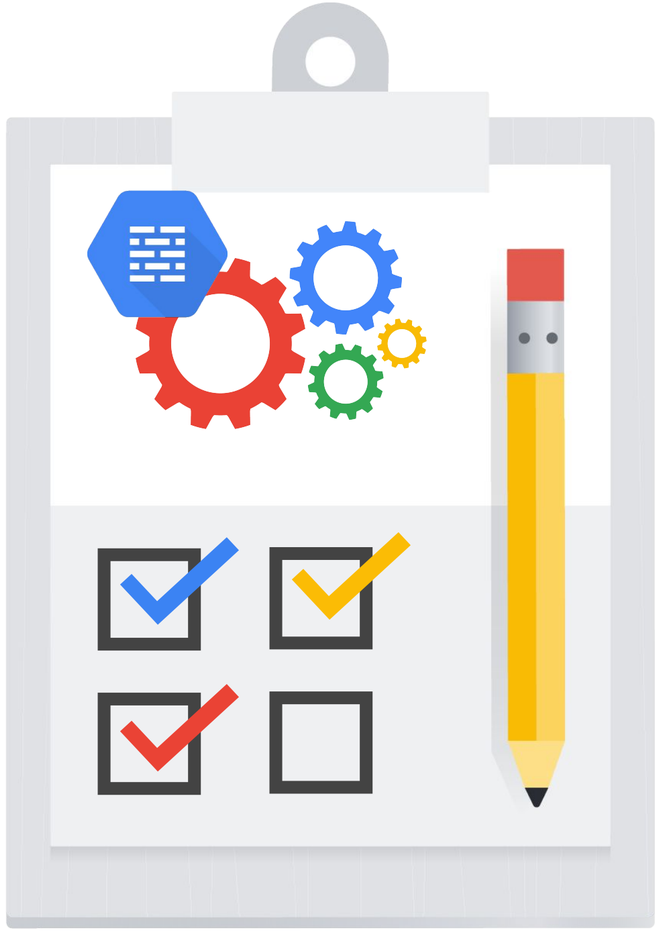
Firewalls protect virtual machine instances from unapproved connections

- 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.

Google Cloud

Express your desired firewall configuration as a set of firewall rules

- Direction of the rule
- Source or destination of the connection
- Protocol and port of the connection
- Action of the rule
- Priority of the rule
- Rule assignment



Google Cloud

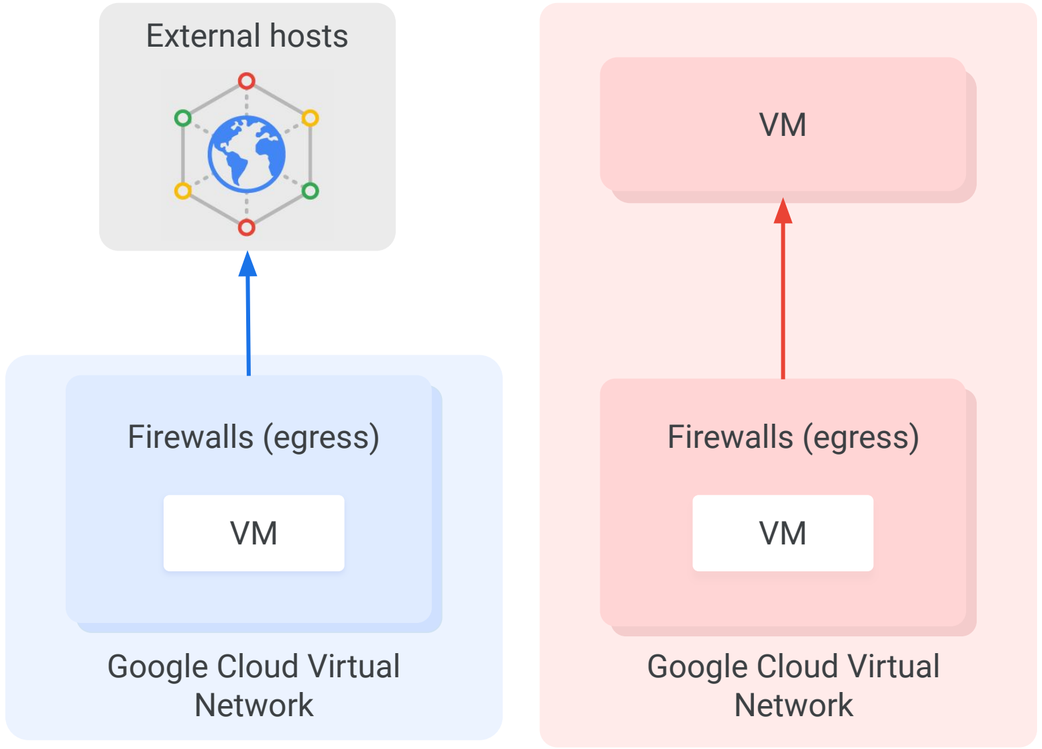
Google Cloud firewall use case: Egress

Conditions:

- Destination CIDR ranges
- Protocols
- Ports

Action:

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



Google Cloud

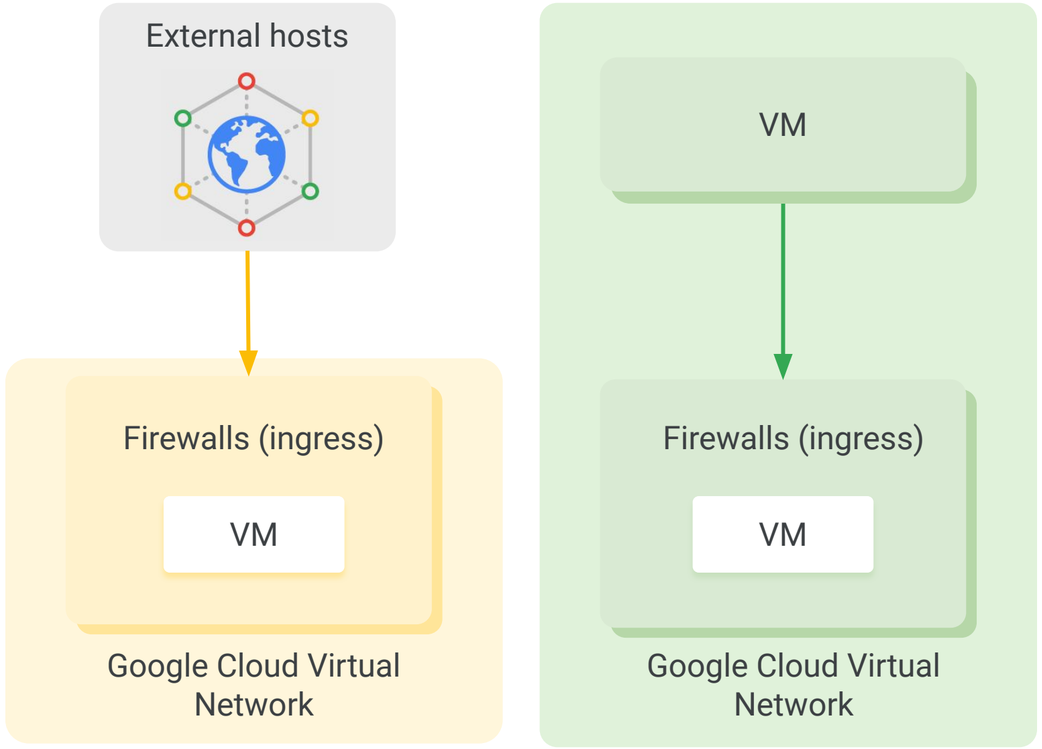
Google Cloud firewall use case: Ingress

Conditions:

- Source CIDR ranges
- Protocols
- Ports

Action:

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



Google Cloud

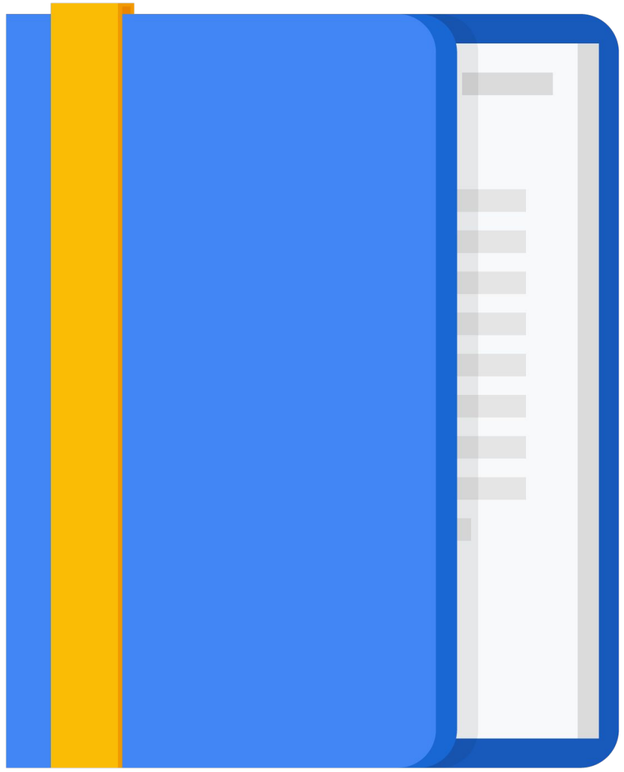
Agenda

Multiple VPC Networks

Lab: Multiple VPC Networks

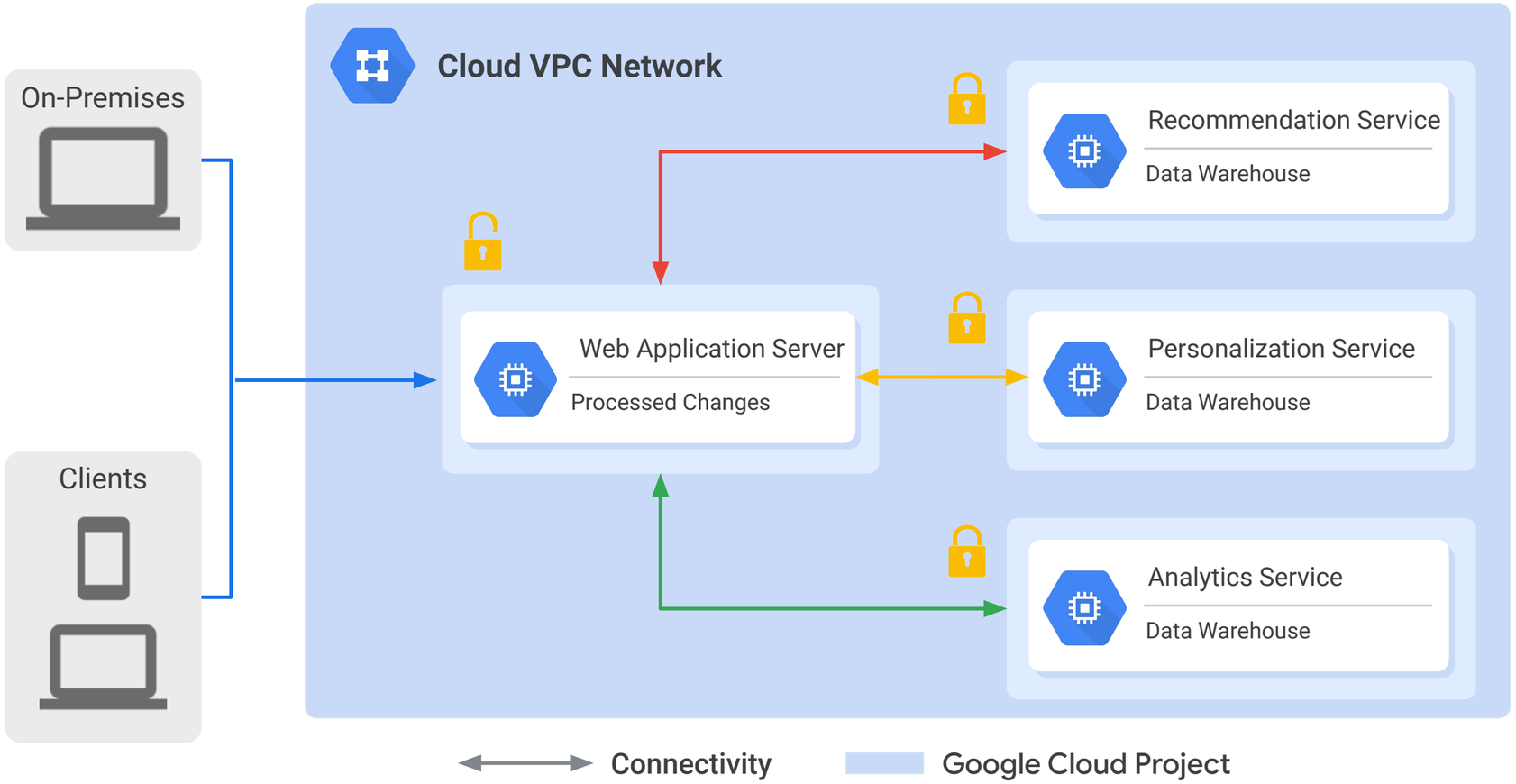
Lab: VPC Networks - Controlling Access

Building Hybrid Clouds using VPNs, Interconnecting, and Direct Peering



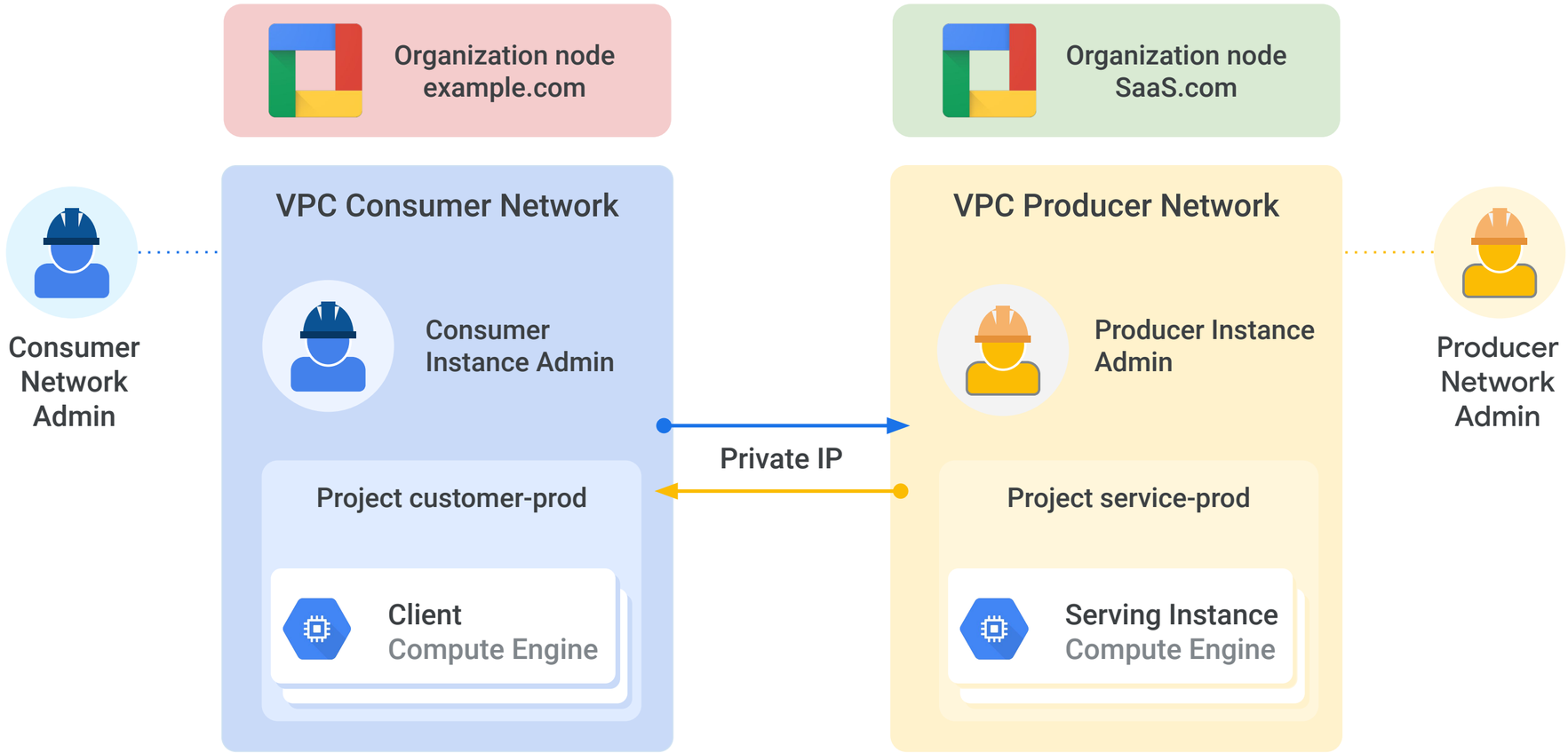
Google Cloud

Connect resources from multiple projects to a common VPC network



Google Cloud

VPC Network Peering allows private RFC 1918 connectivity across two VPC networks



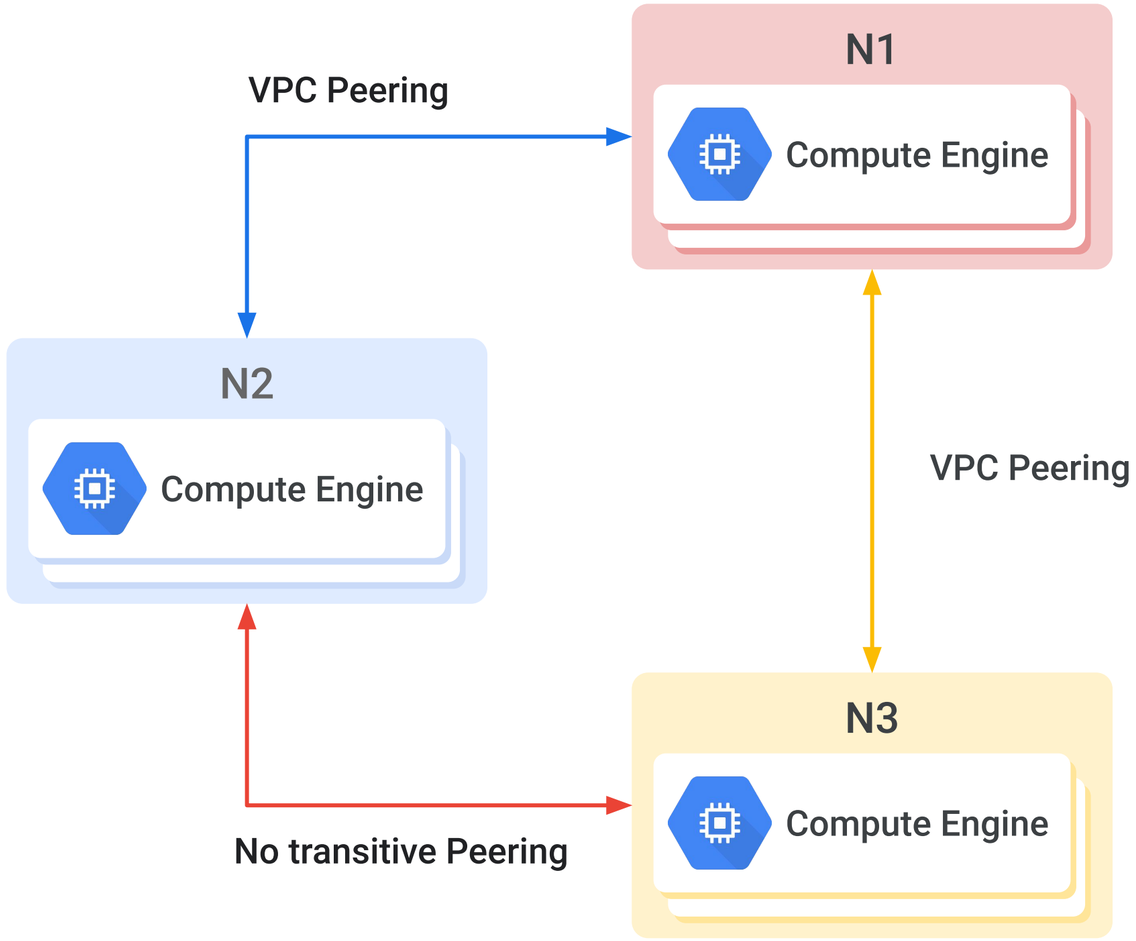
Google Cloud

Considerations for VPC Network Peering

- Works with Compute Engine, Google 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 range overlap across peered VPC networks.

Google Cloud

Only directly peered networks can communicate



Google Cloud

Shared VPC versus VPC peering

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

Google Cloud

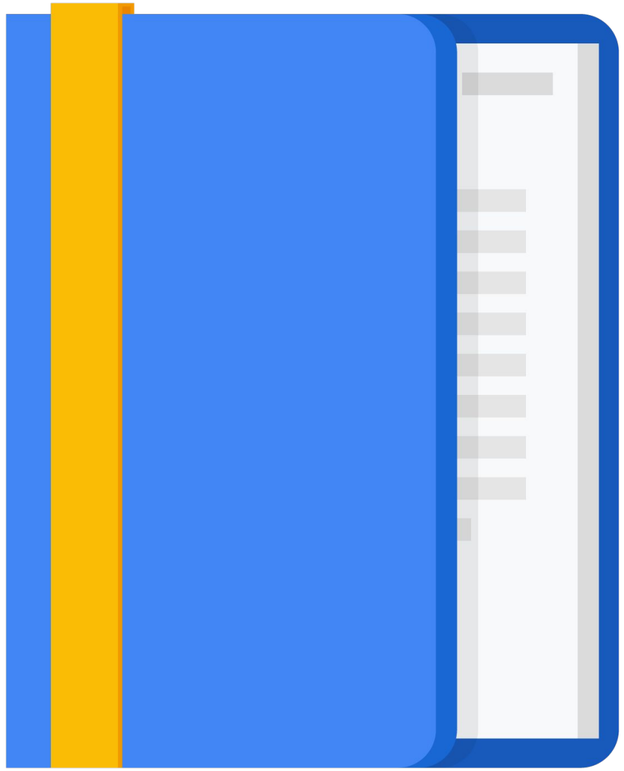
Agenda

Multiple VPC Networks

Lab: Multiple VPC Networks

Lab: VPC Networks - Controlling Access

Building Hybrid Clouds using VPNs, Interconnecting, and Direct Peering



Google Cloud

Lab Intro

Multiple VPC Networks

Create several VPC networks and virtual machine instances and test connectivity across networks.

The lab can be found here.

Google Cloud

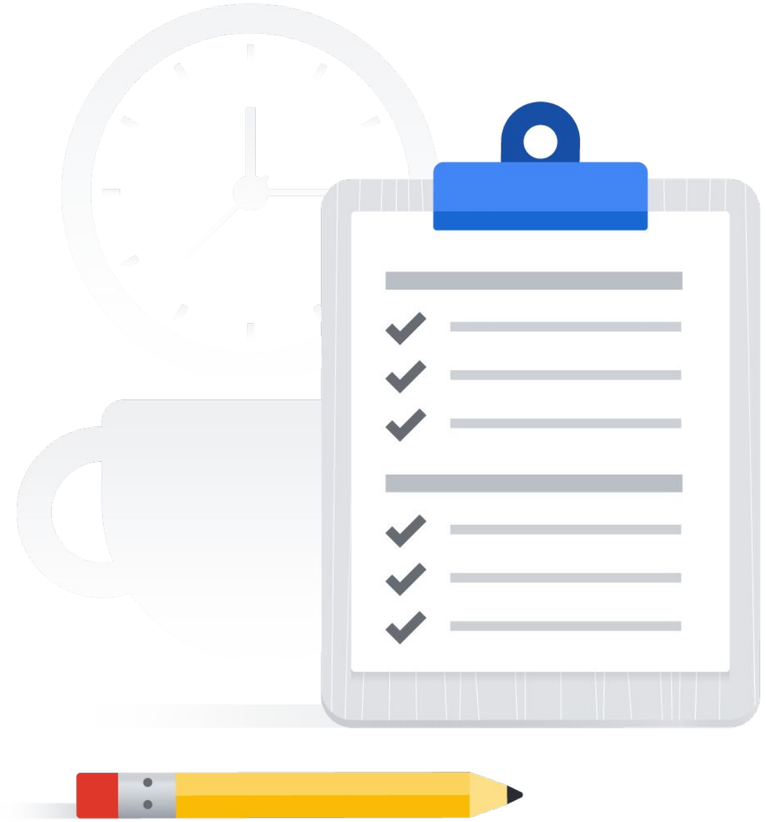
Lab objectives

Create custom mode VPC networks with firewall rules.

Create virtual machine instances using Compute Engine.

Explore the connectivity for virtual machine instances across VPC networks.

Create a virtual machine instance with multiple network interfaces.



Google Cloud

Lab Intro

Networking 101 (Alternative)

Develop a network and three subnetworks.

The lab can be found here.

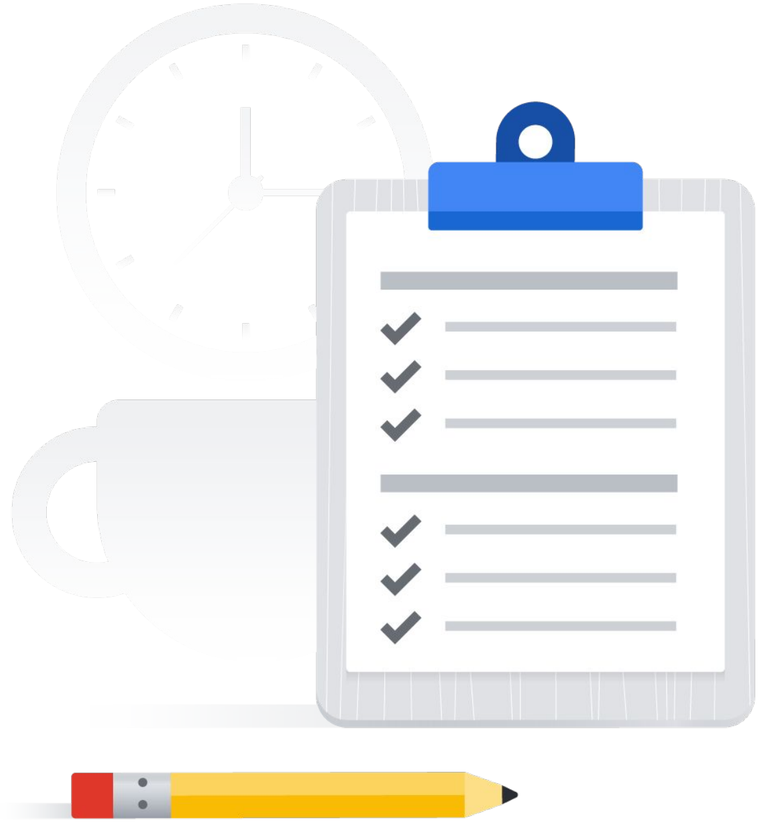
Google Cloud

Lab objectives

Set up your lab environment and learn how to work with your Google Cloud environment.

Deploy a common network with subnets and multiple regions using common open source tools to explore your network around the world.

Test and monitor your network and instances.



Google Cloud

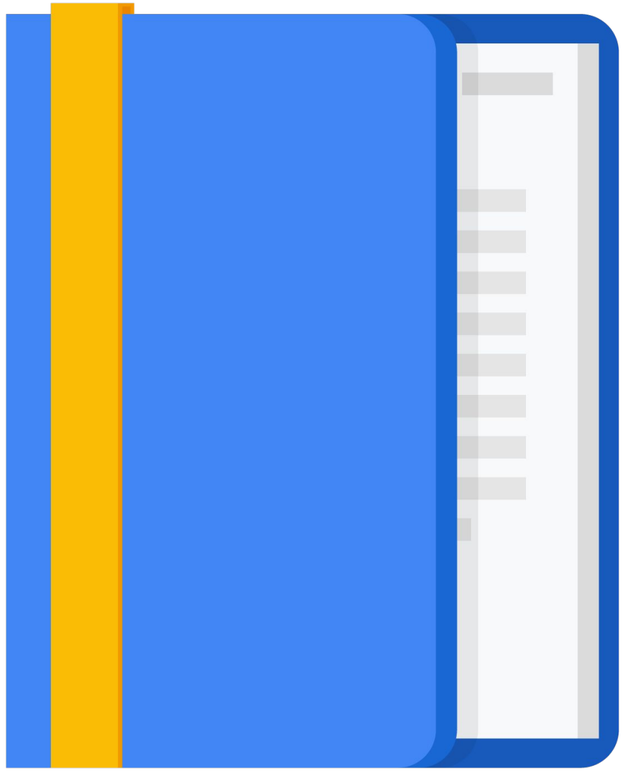
Agenda

Multiple VPC Networks

Lab: Multiple VPC Networks

Lab: VPC Networks - Controlling Access

Building Hybrid Clouds using VPNs, Interconnecting, and Direct Peering



Google Cloud

Lab Intro

VPC Networks - Controlling Access

Create NGINX web servers, control external HTTP access to the web servers using tagged firewall rules, and explore IAM roles and service accounts.

The lab can be found here.

Google Cloud

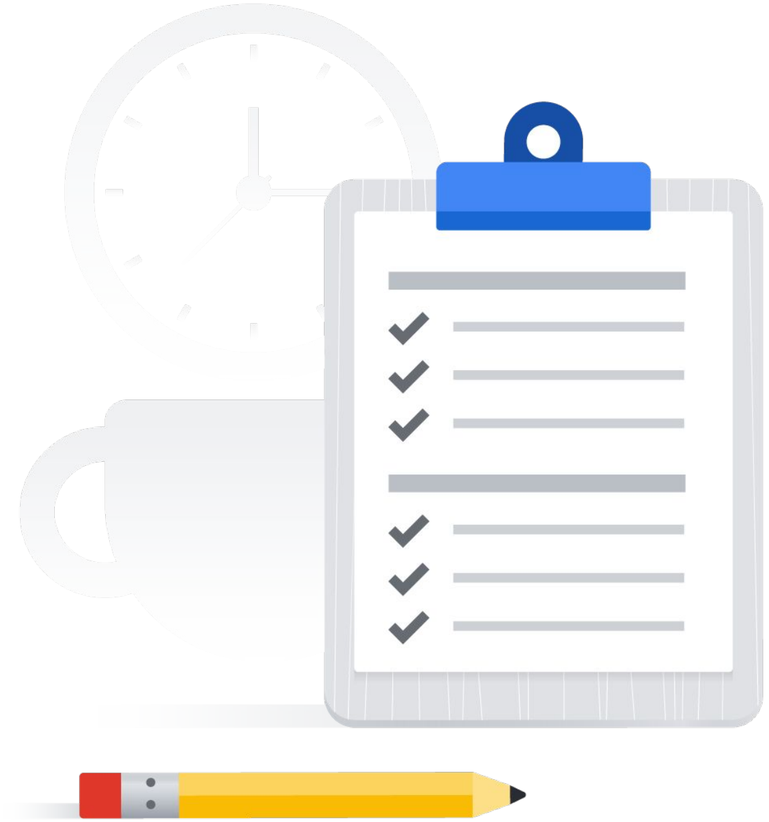
Lab objectives

Create an NGINX web server.

Create tagged firewall rules.

Create a service account with IAM roles.

Explore permissions for the Network Admin and Security Admin roles.



Google Cloud

Lab Intro

Using VPC Network Peering (Alternative)

Configure VPC Network Peering between two networks.

The lab can be found here.

Google Cloud

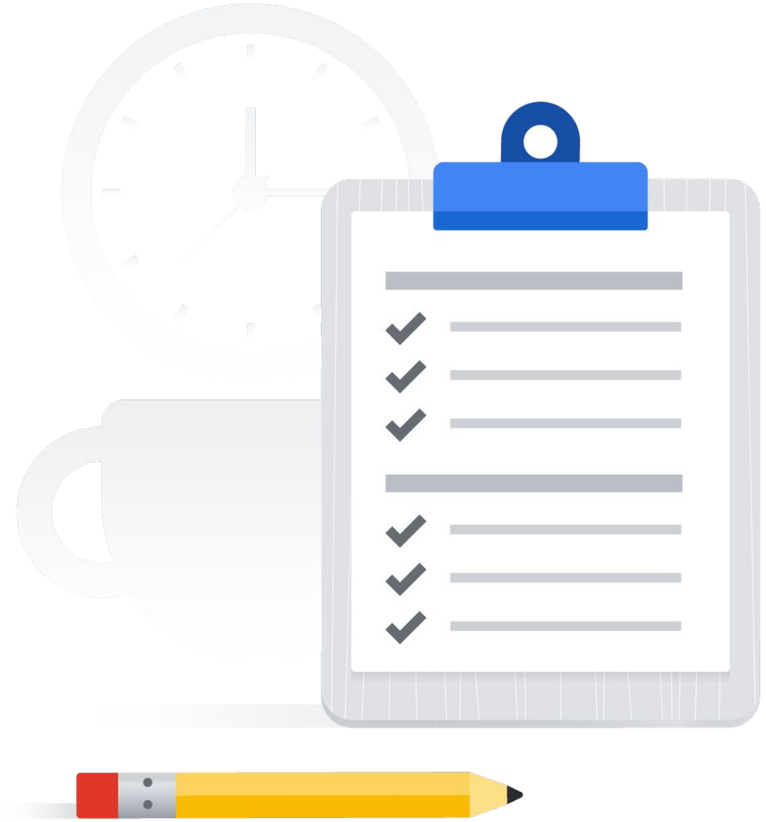
Lab objectives

Explore connectivity between non-peered VPC networks.

Configure VPC Network Peering.

Verify private communication between peered VPC networks.

Delete VPC Network Peering.



Google Cloud

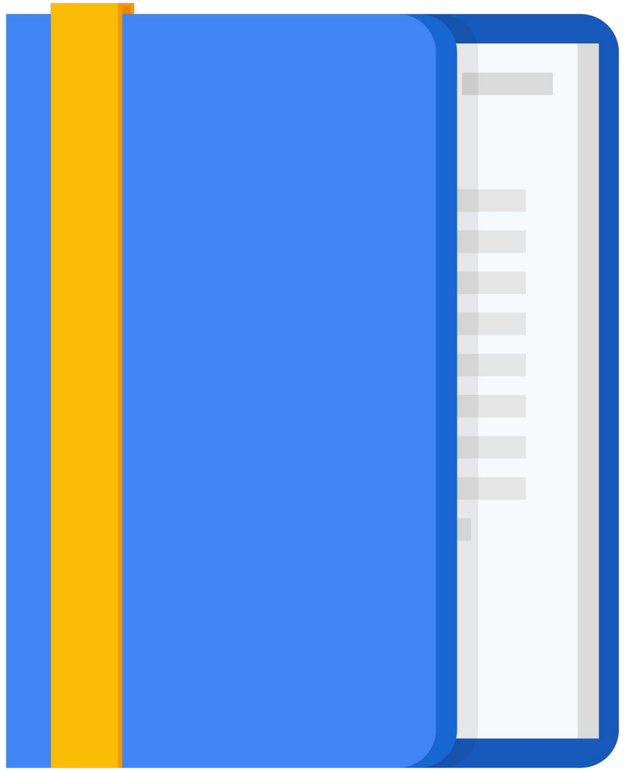
Agenda

Multiple VPC Networks

Lab: Multiple VPC Networks

Lab: VPC Networks - Controlling Access

Building Hybrid Clouds using VPNs, Interconnecting, and Direct Peering



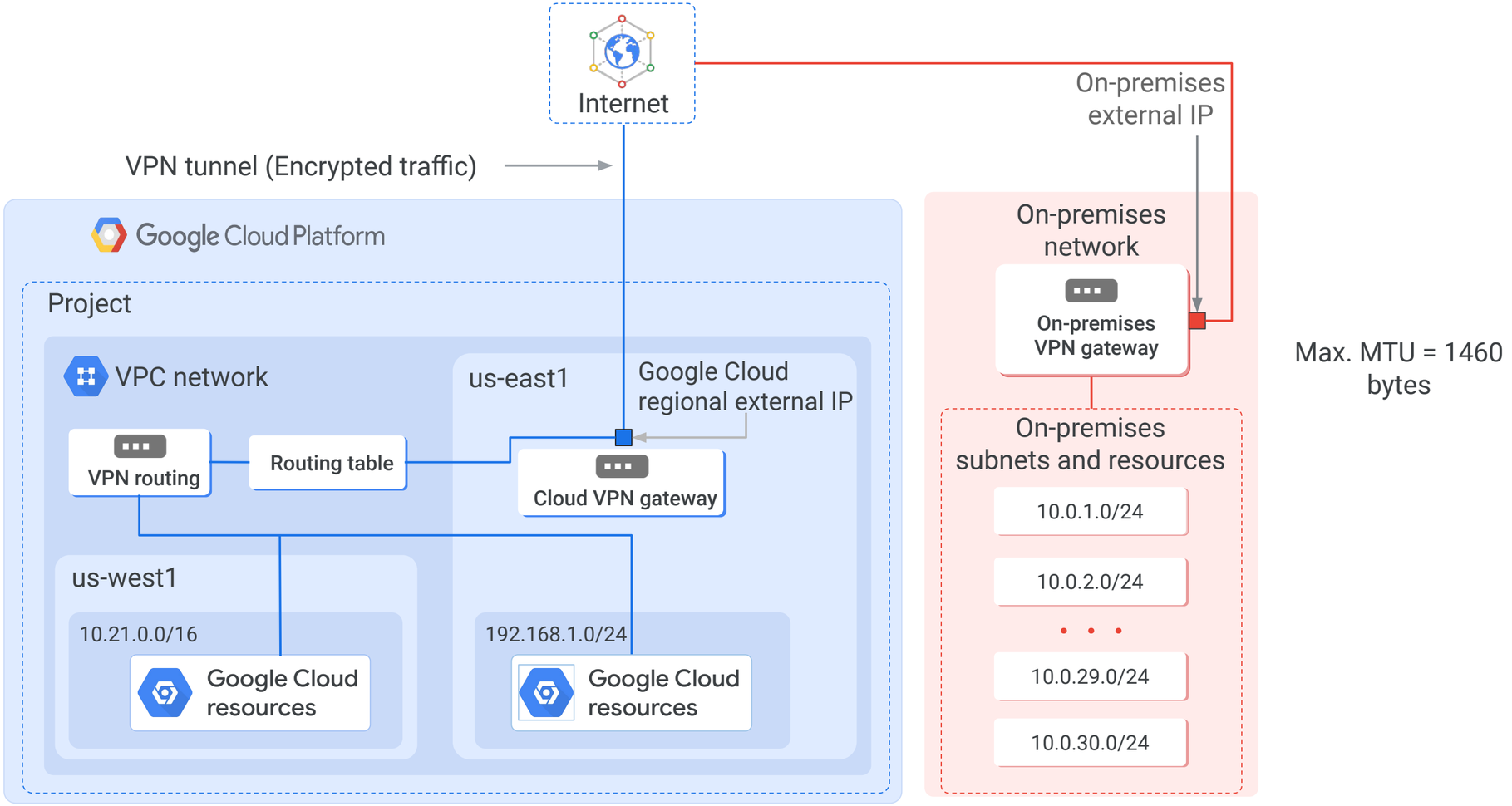
Google Cloud

Cloud VPN securely connects an on-premises network to a Google Cloud VPC network

- Useful for low-volume data connections
- 99.9% SLA
- Supports:
  - Site-to-site VPN
  - Static routes
  - Dynamic routes (Cloud Router)
  - IKEv1 and IKEv2 ciphers

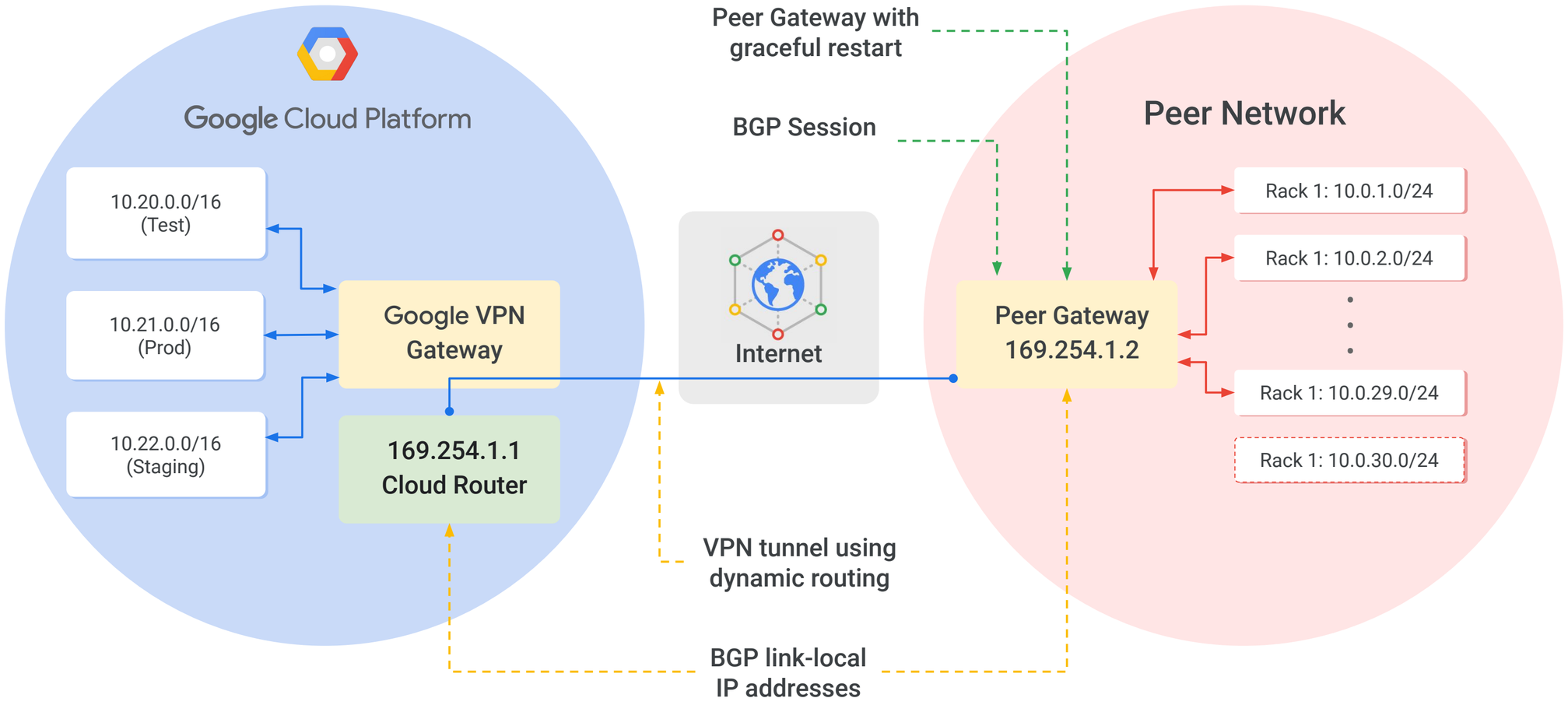
Google Cloud

Static VPN topology



Google Cloud

Dynamic routing topology with Cloud Router



Google Cloud

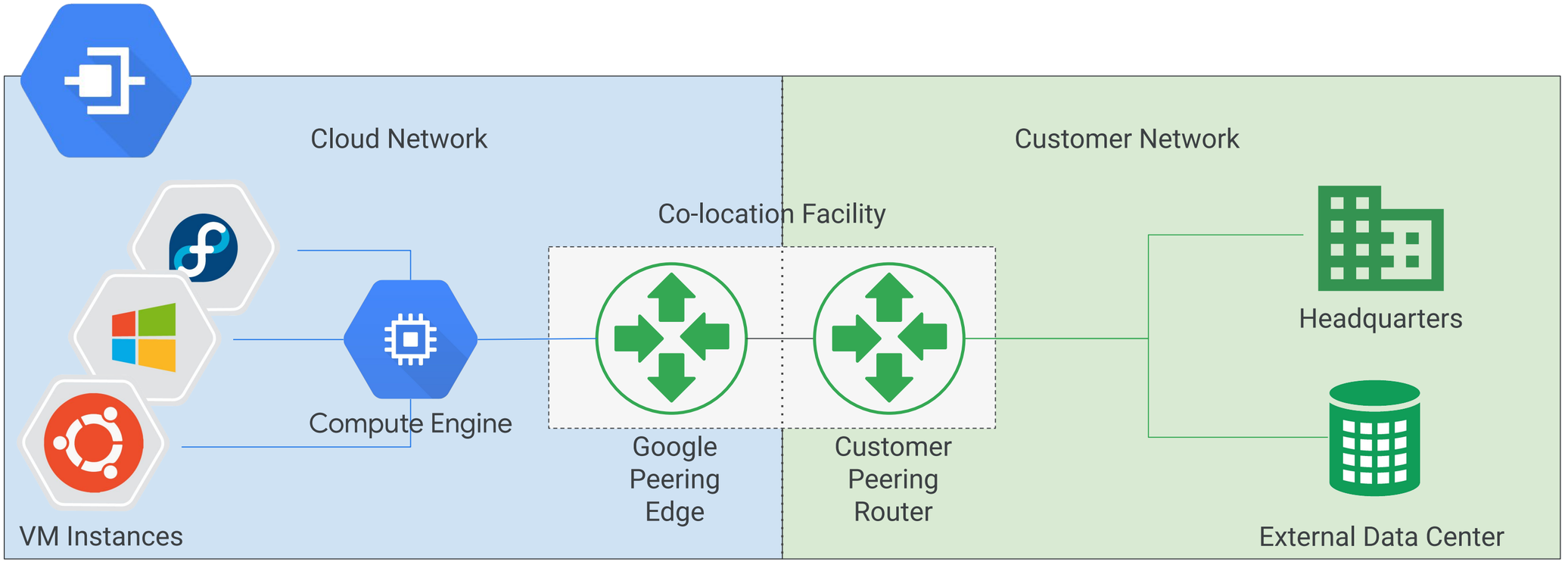
Cloud Interconnect offers two options to extend an on-premises network to a Google Cloud VPC network

Cloud Interconnect - Dedicated

Cloud Interconnect - Partner

Google Cloud

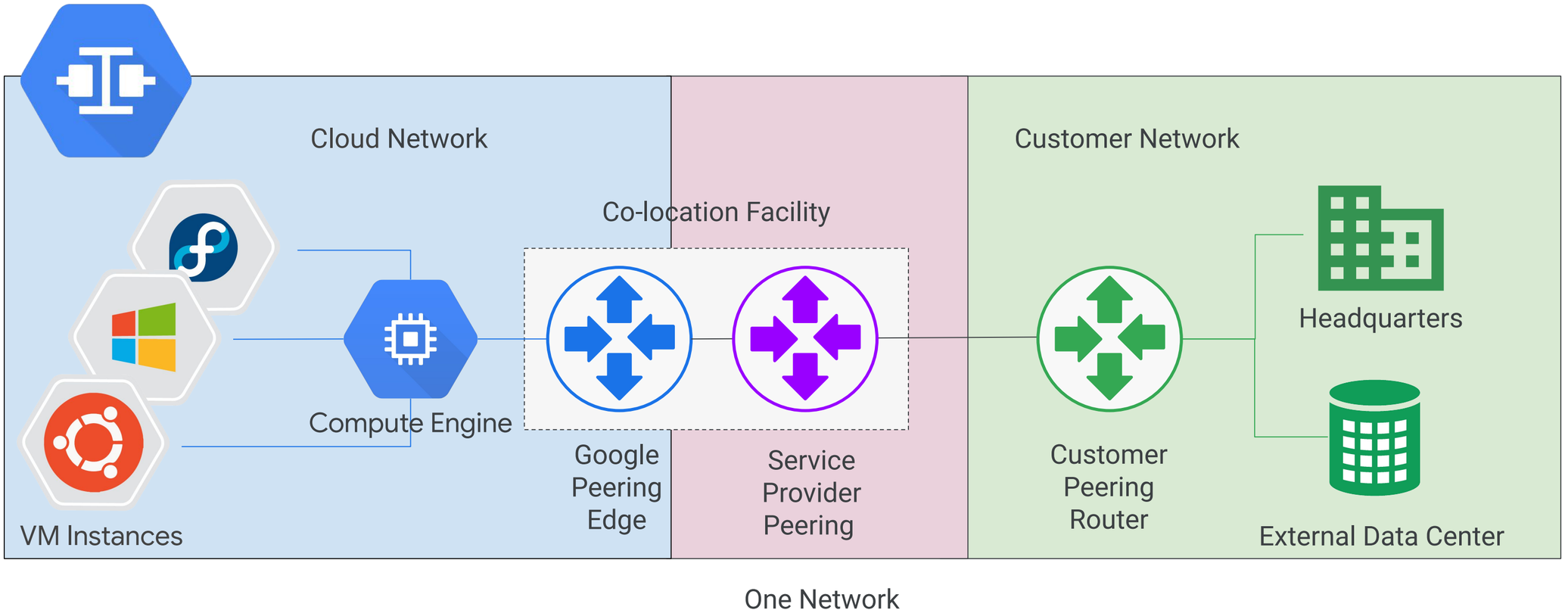
Dedicated Interconnect



One Network

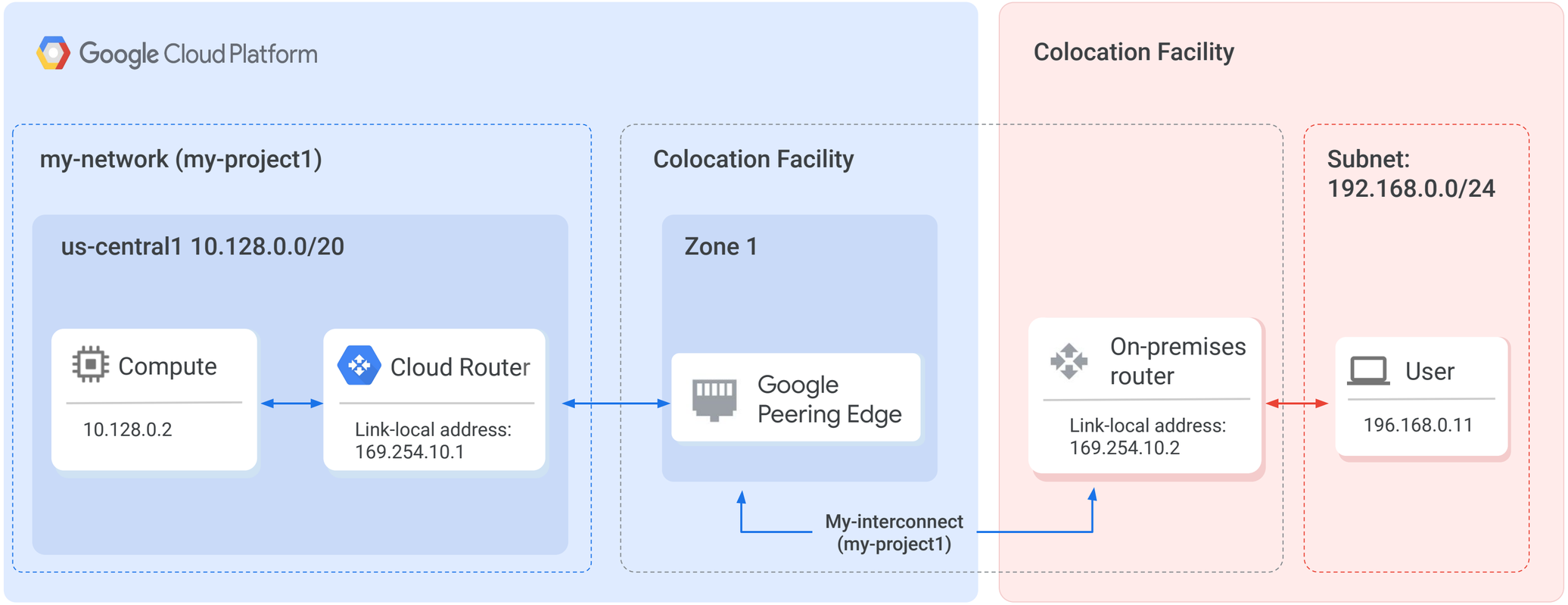
Google Cloud

Partner Interconnect



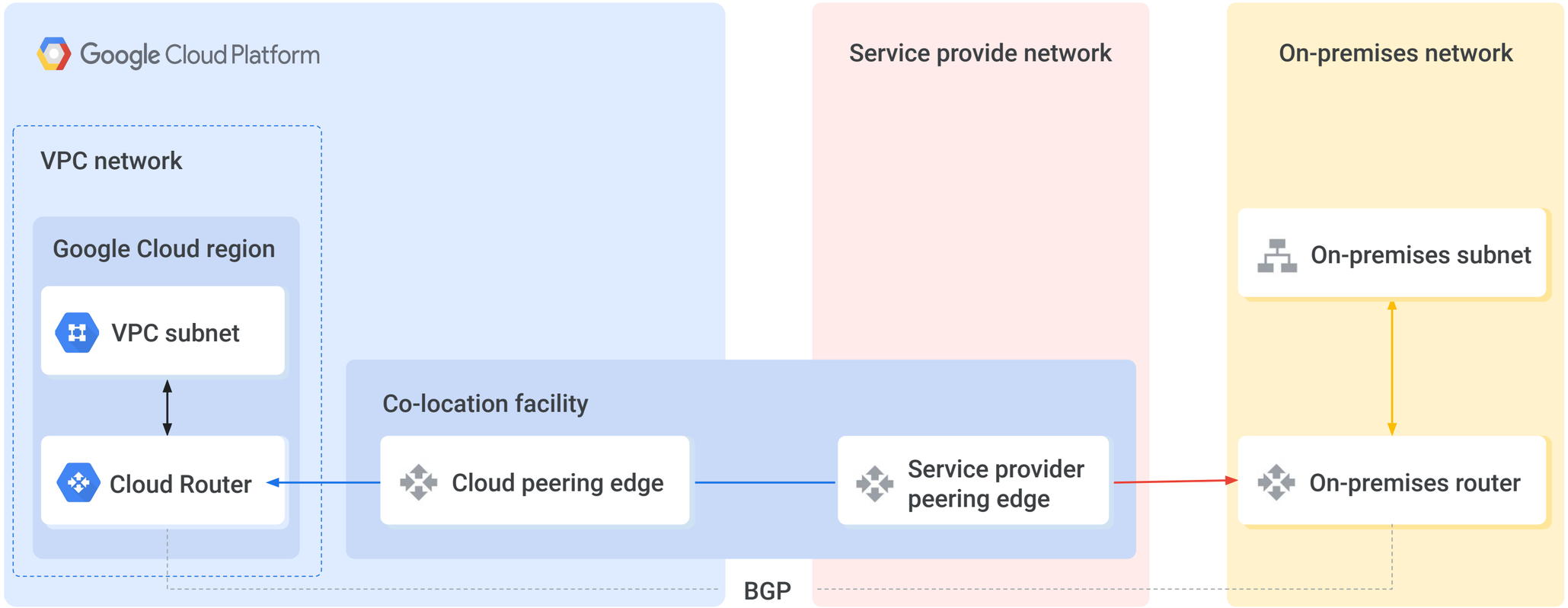
Google Cloud

Dedicated Interconnect provides direct physical connections



Google Cloud

Partner Interconnect provides connectivity through a supported service provider



Google Cloud

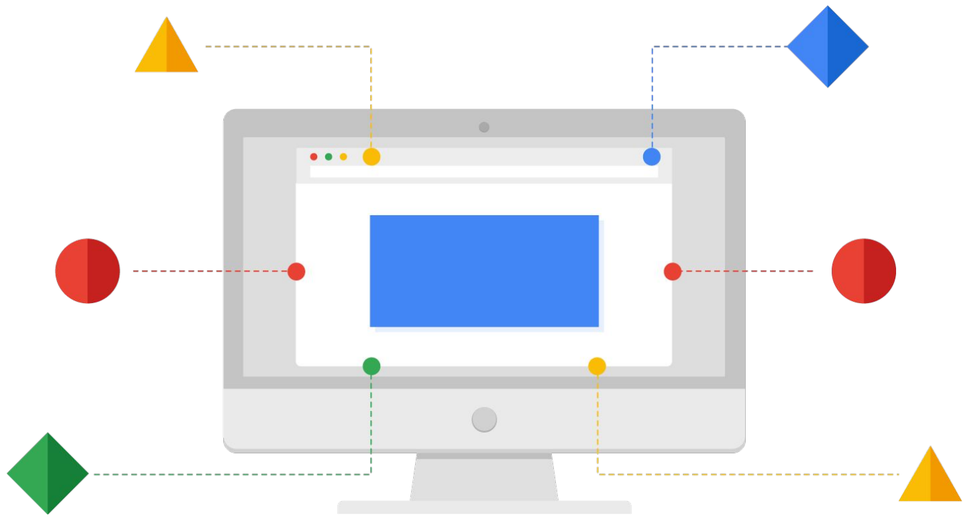
A comparison of interconnect options

Connection	Provides	Capacity	Requirements	Access type
IPsec VPN tunnels	Encrypted tunnel to VPC networks through the public internet	1.5 - 3.0 Gbps per tunnel	On-premises VPN gateway	Internal IP addresses
Dedicated Interconnect	Dedicated, direct connection to VPC networks	8 x 10 Gbps circuits, or 2 x 100 Gbps circuits per connection	Connection in a colocation facility	Internal IP addresses
Partner Interconnect	Dedicated bandwidth, connection to VPC network through a service provider	50 Mbps – 10 Gbps per connection	Service provider	Internal IP addresses

Google Cloud

Direct Peering provides a direct connection between a business network and Google's

- Leverage Google's broad-reaching edge network locations.
- Exchange BGP routes between Google and the peering entity.
- Reach all of Google's services.
- No SLA applies.
- Peering requirements must be satisfied.



Google Cloud

Carrier Peering provides connectivity through a supported partner

- An alternative if Google's peering requirements cannot be met.
- Leverage a provider's enterprise- grade network services to access Google applications.
- Get connections with higher availability and lower latency.
- No SLA offered by Google but may be offered by the provider.

Google Cloud

A comparison of peering options

Connection	Provides	Capacity	Requirements	Access type
Direct Peering	Dedicated, direct connection to Google's network	10 Gbps per link	Connection in Google Cloud PoPs	Public IP addresses
Carrier Peering	Peering through a service provider to Google’s public network	Varies based on partner offering	Service provider	Public IP addresses

Google Cloud

Agenda

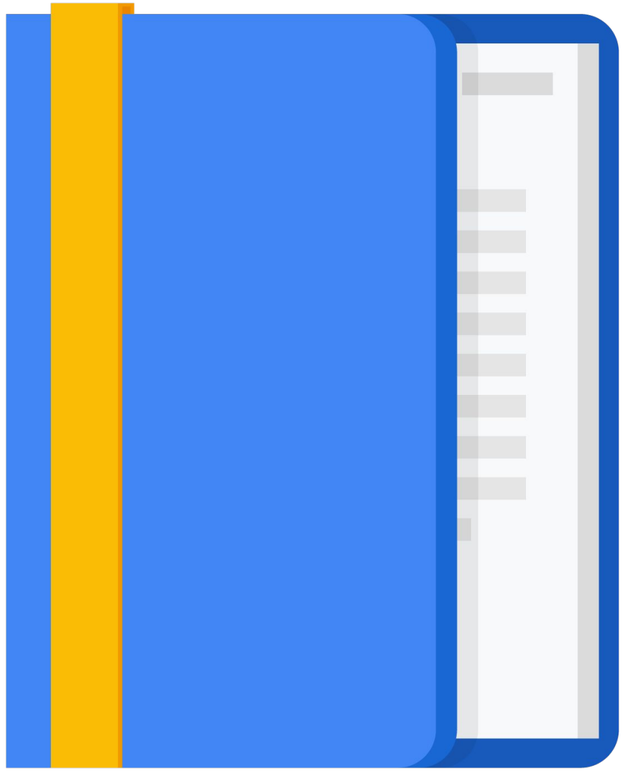
Different Options for Load Balancing

Lab: HTTP Load Balancer with Cloud Armor

Lab: Create an Internal Load Balancer

Quiz

Summary



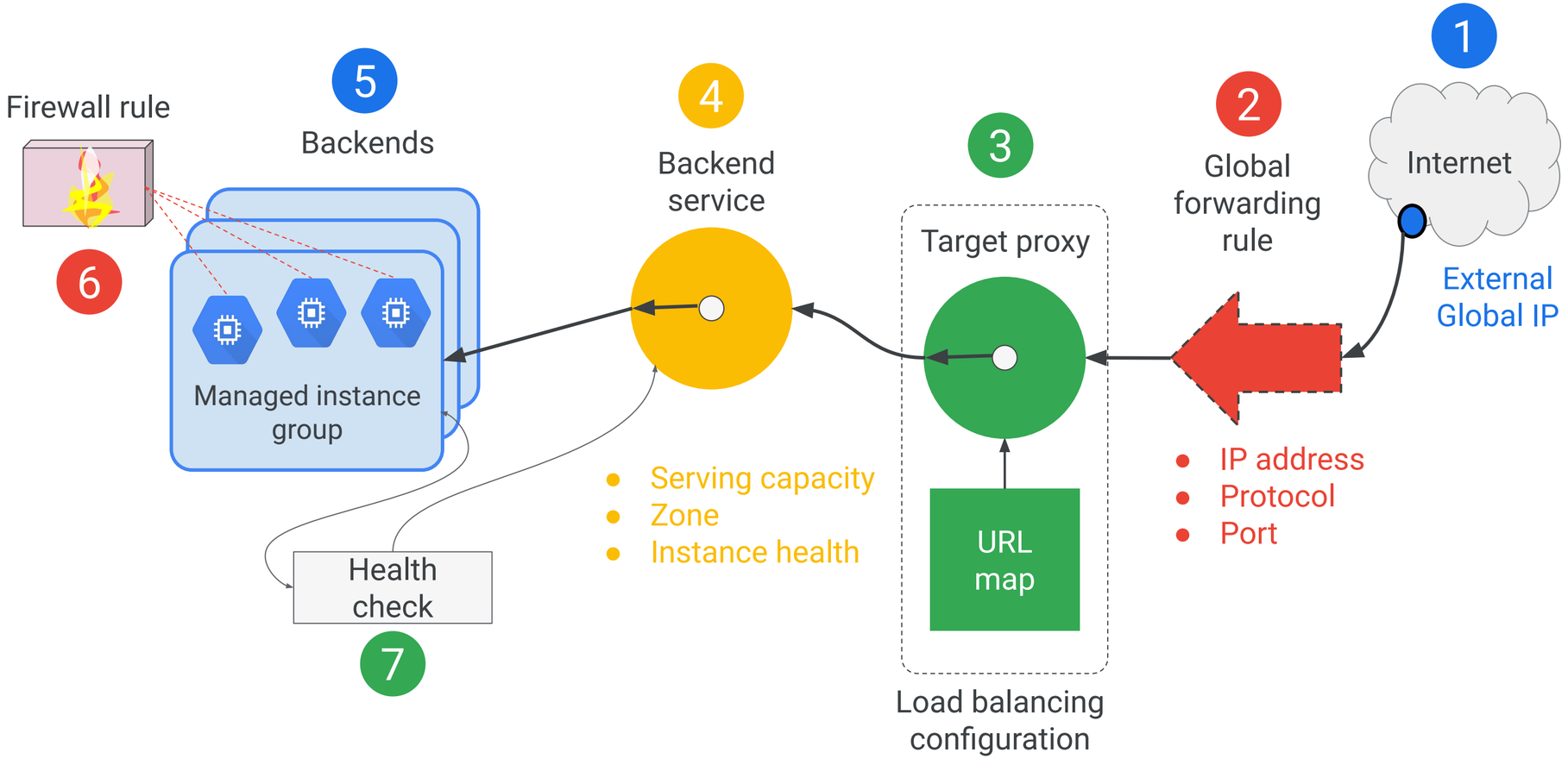
Google Cloud

Use load balancing to distribute user requests among sets of instances

Global	HTTP(S) load balancing	Distributes HTTP(S) traffic among groups of instances based on: • Proximity to the user • Requested URL • Both	External
	SSL Proxy load balancing	Distributes SSL traffic among groups of instances based on proximity to the user.	
	TCP Proxy load balancing	Distributes TCP traffic among groups of instances based on proximity to the user.	
Regional	Network load balancing	• Distributes traffic among a pool of instances within a region. • Can balance any kind of TCP/UDP traffic.	
	Internal load balancing	Distributes traffic from Google Cloud virtual machine instances to a group of instances in the same region.	Internal

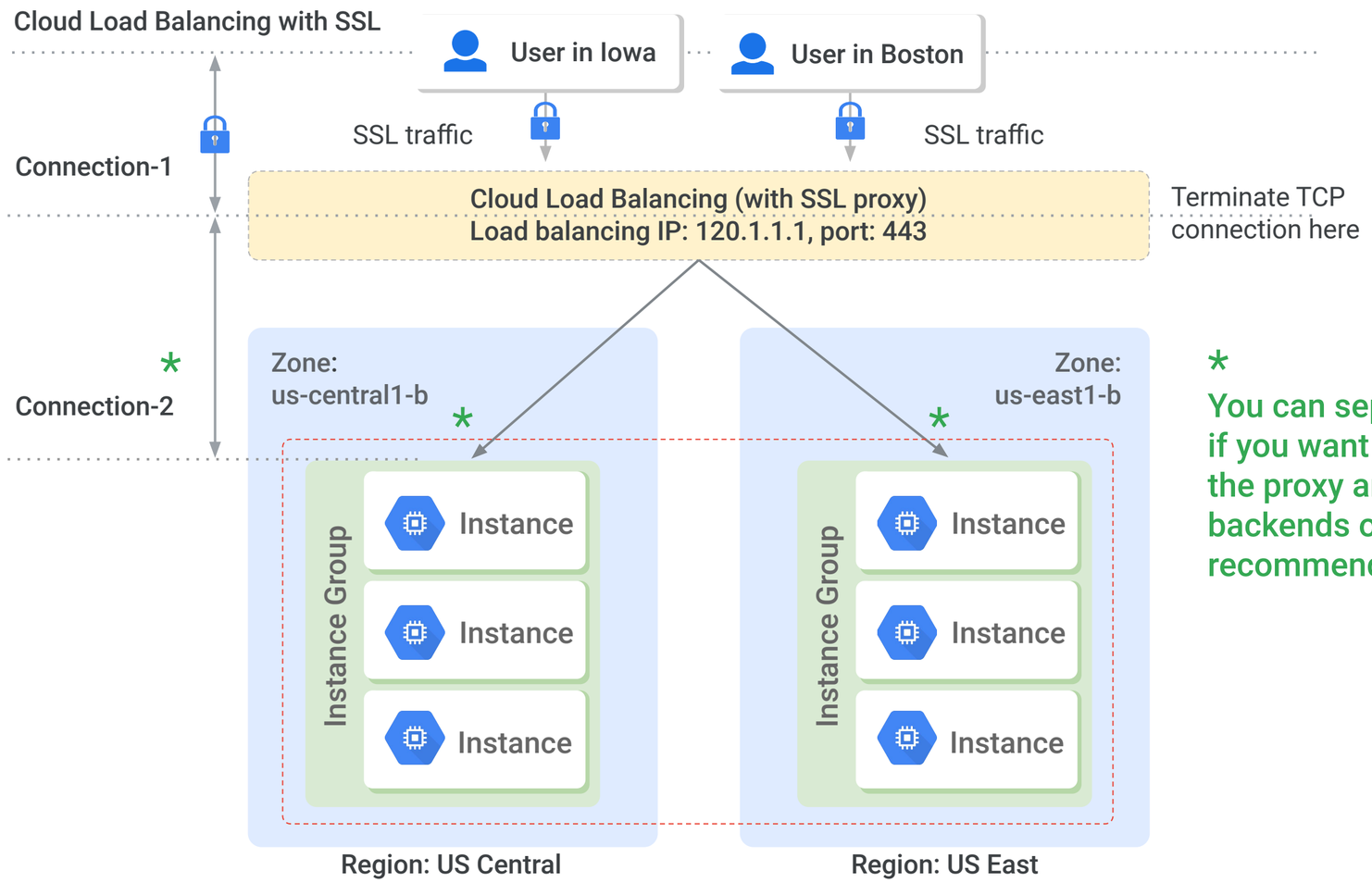
Google Cloud

Traffic flows through an HTTP(S) global load balancer in different stages



Google Cloud

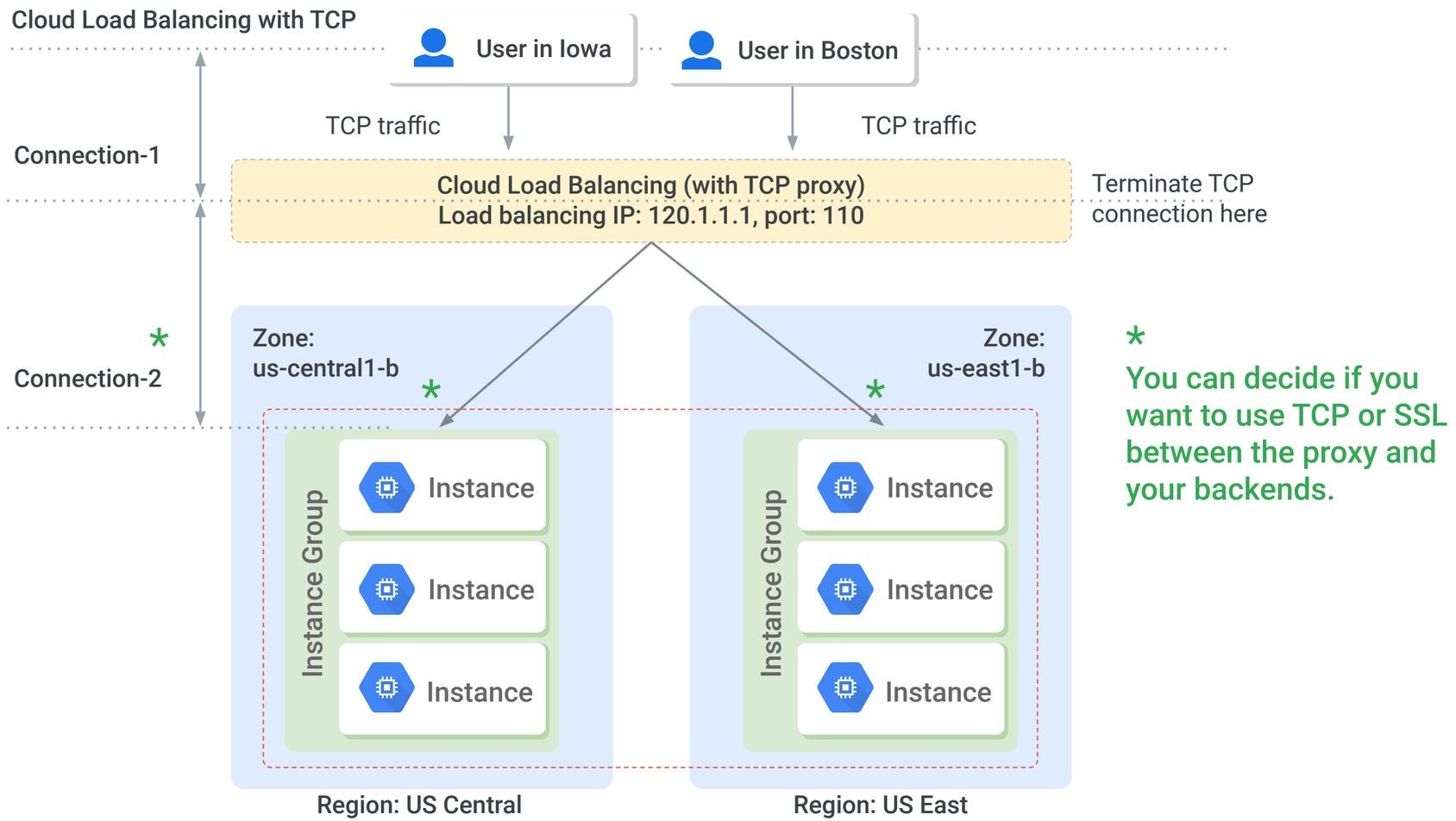
Cloud Load Balancing with SSL proxy



* You can separately decide if you want SSL between the proxy and your backends or not. Google recommends using SSL.

Google Cloud

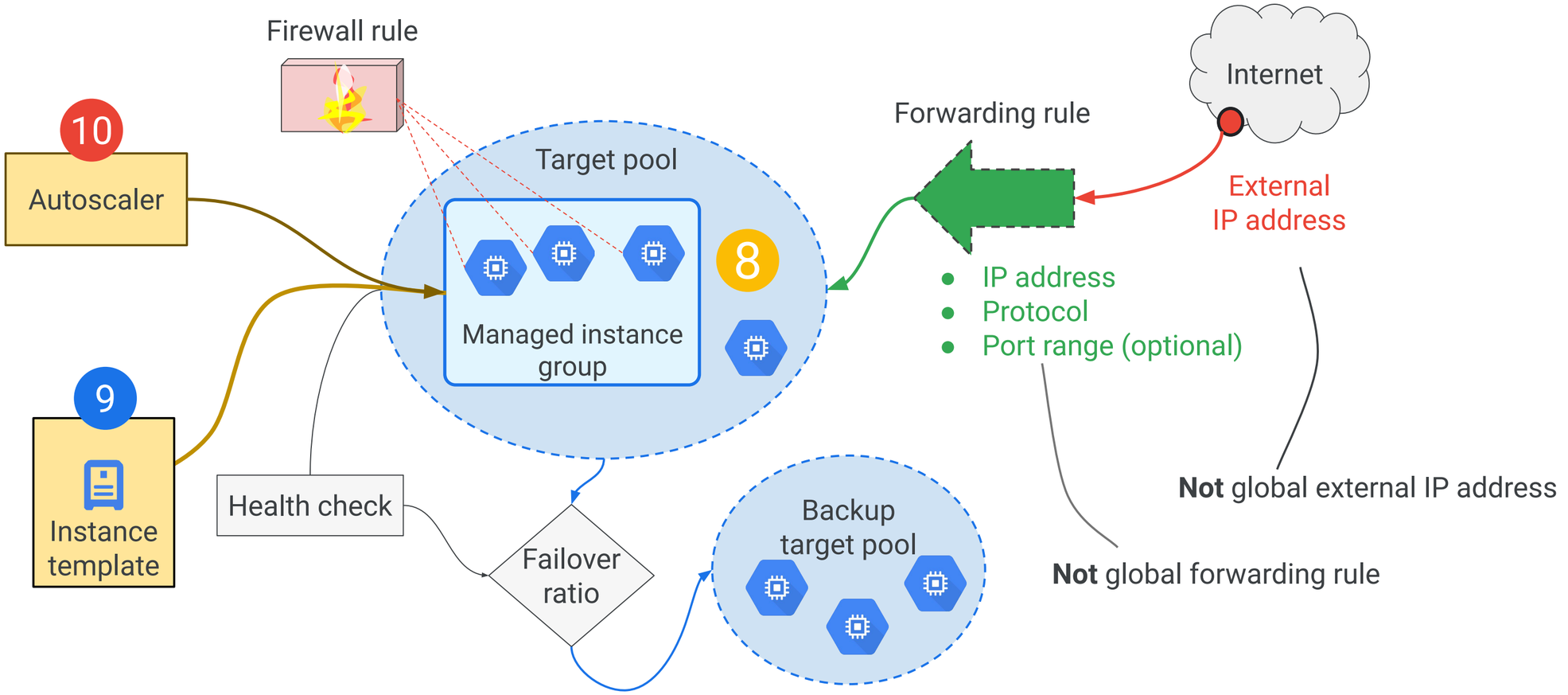
Cloud Load Balancing with TCP proxy



* You can decide if you want to use TCP or SSL between the proxy and your backends.

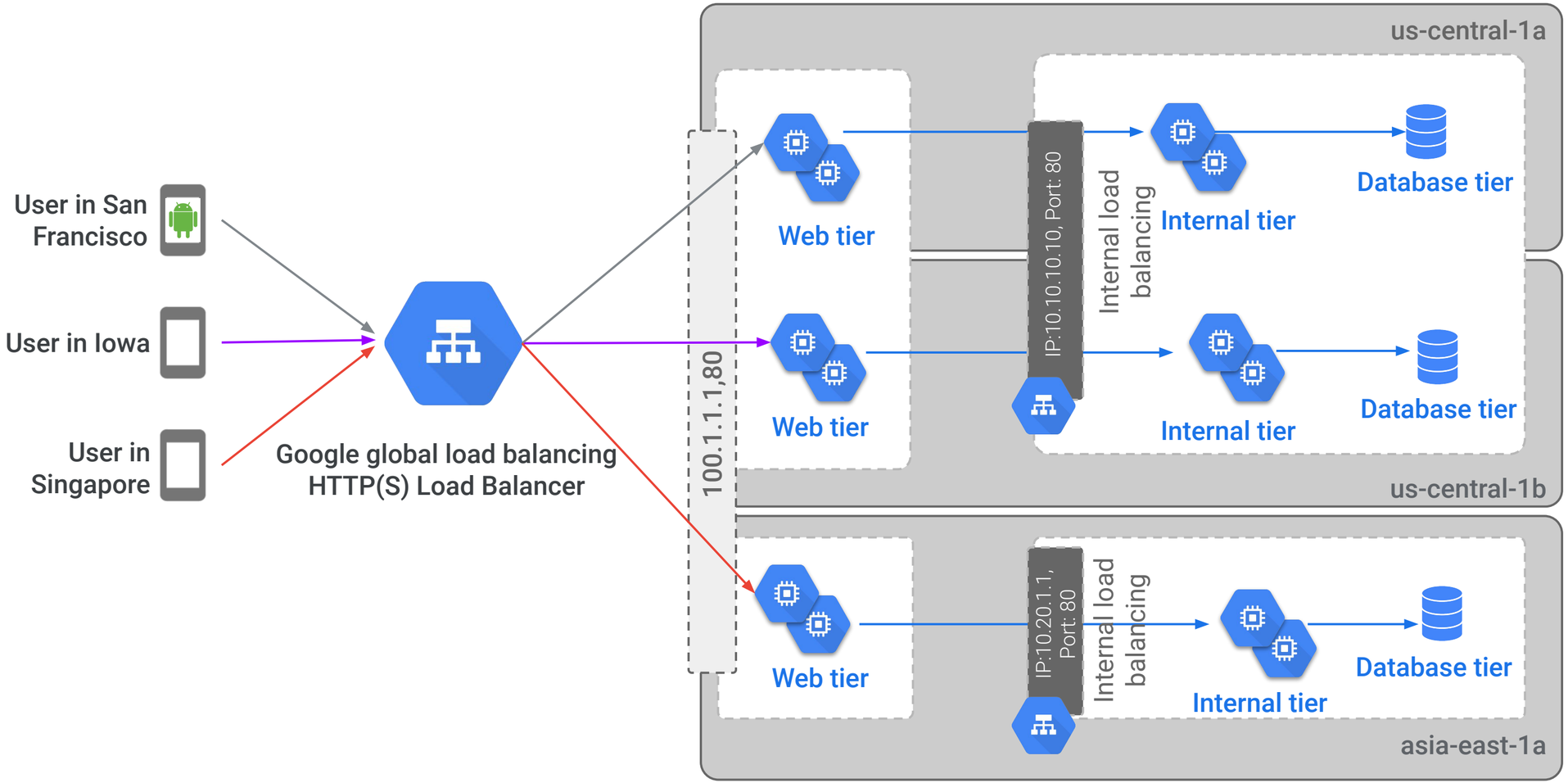
Google Cloud

Network load balancing when running a managed instance group



Google Cloud

HTTP(S) and internal load balancing example



Google Cloud

Agenda

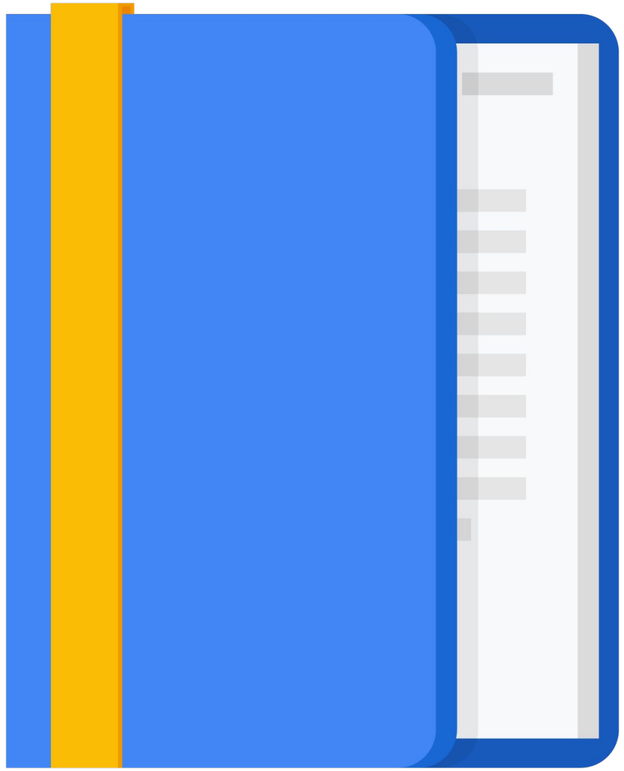
Different Options for Load Balancing

Lab: HTTP Load Balancer with Cloud Armor

Lab: Create an Internal Load Balancer

Quiz

Summary



Google Cloud

Lab Intro

HTTP Load Balancer with Cloud Armor

Configure an HTTP load balancer with global backends and stress test the load balancer and blocklist the stress test IP with Cloud Armor.

The lab can be found here.

Google Cloud

Lab objectives

Create HTTP and health check firewall rules.

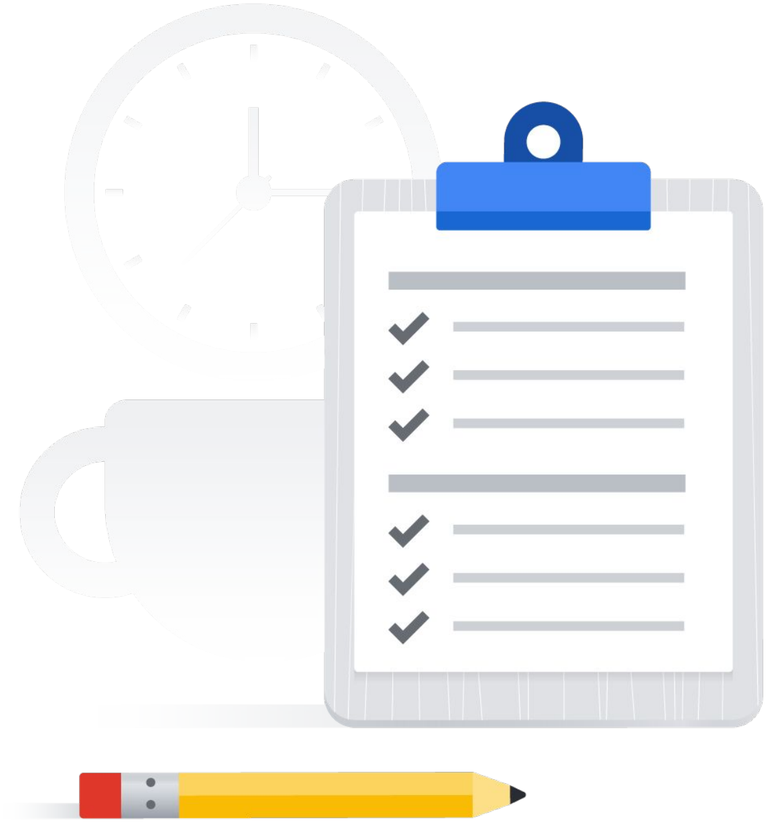
Configure two instance templates.

Create two managed instance groups.

Configure an HTTP load balancer with IPv4 and IPv6.

Stress test an HTTP load balancer.

Blocklist an IP address to restrict access to an HTTP load balancer.



Google Cloud

Lab Intro

HTTP Load Balancer (Alternative)

Set up an HTTP global load balancer and learn how load balancing can help scale your applications on Compute Engine.

The lab can be found here.

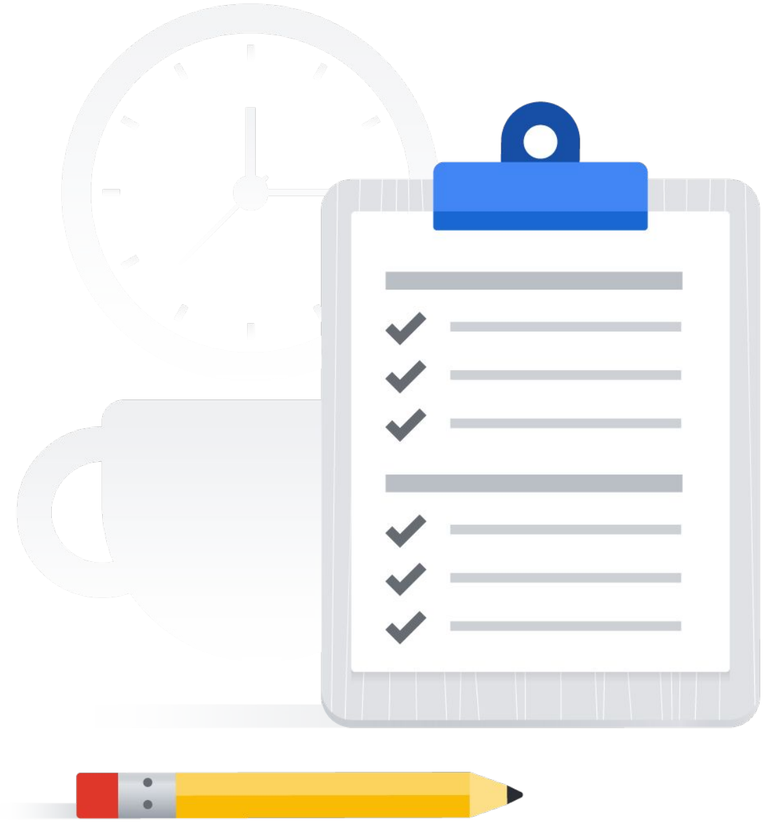
Google Cloud

Lab objectives

Add an HTTP firewall rule allowing network access to the Backend VM instances.

Create Managed Instance Groups with the VM instance configurations.

Create the HTTP Load Balancer with backends to route requests to available instances.



Google Cloud

Agenda

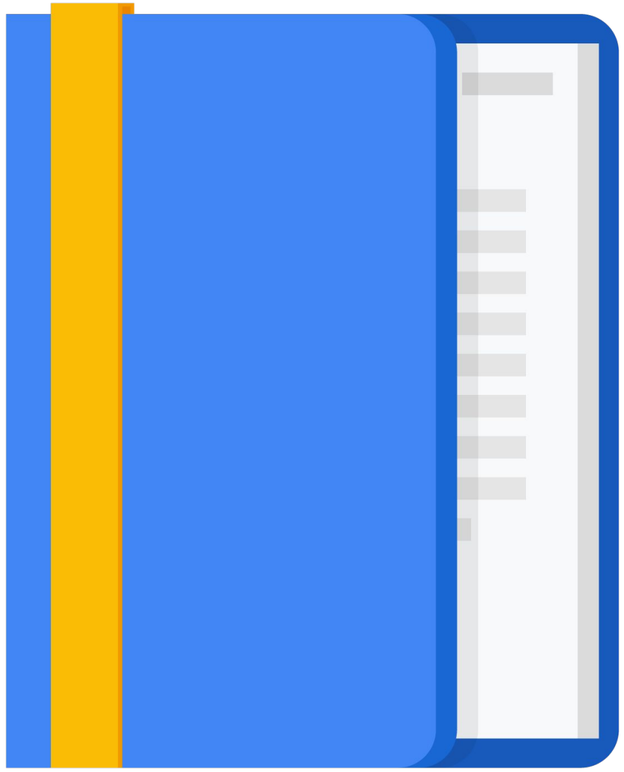
Different Options for Load Balancing

Lab: HTTP Load Balancer with Cloud Armor

Lab: Create an Internal Load Balancer

Quiz

Summary



Google Cloud

Lab Intro

Create an Internal Load Balancer

Create managed instance groups in the same region and configure and test an internal load balancer with the instance groups as the backends.

The lab can be found here.

Google Cloud

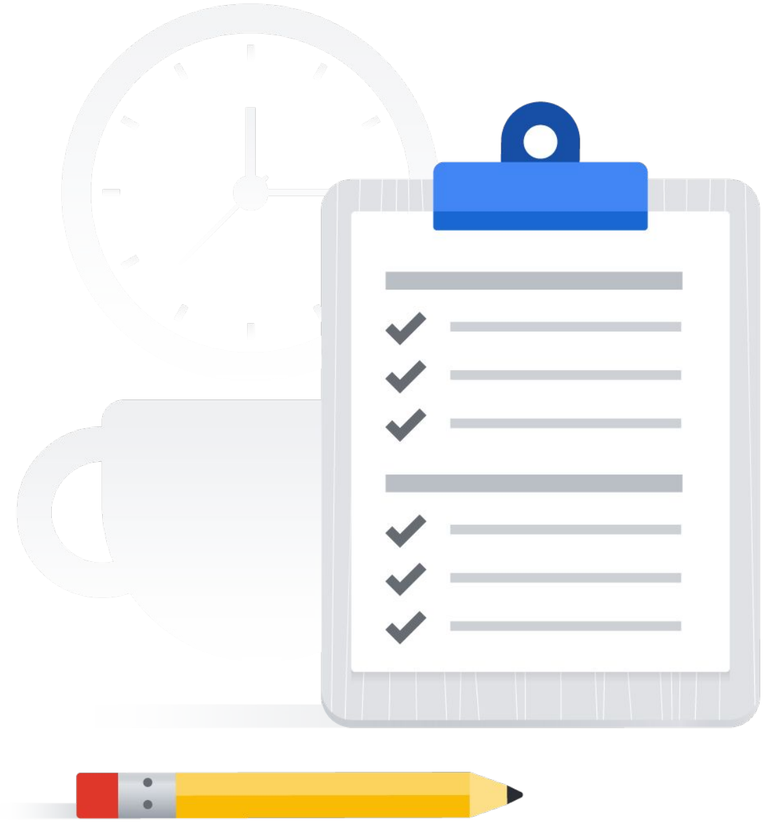
Lab objectives

Create HTTP and health check firewall rules.

Configure two instance templates.

Create two managed instance groups.

Configure and test an internal load balancer.



Google Cloud

Lab Intro

Internal Load Balancer (Alternative)

Create a public-facing web server to serve the result of several "complex" calculations, in this case, calculating prime numbers.

The lab can be found here.

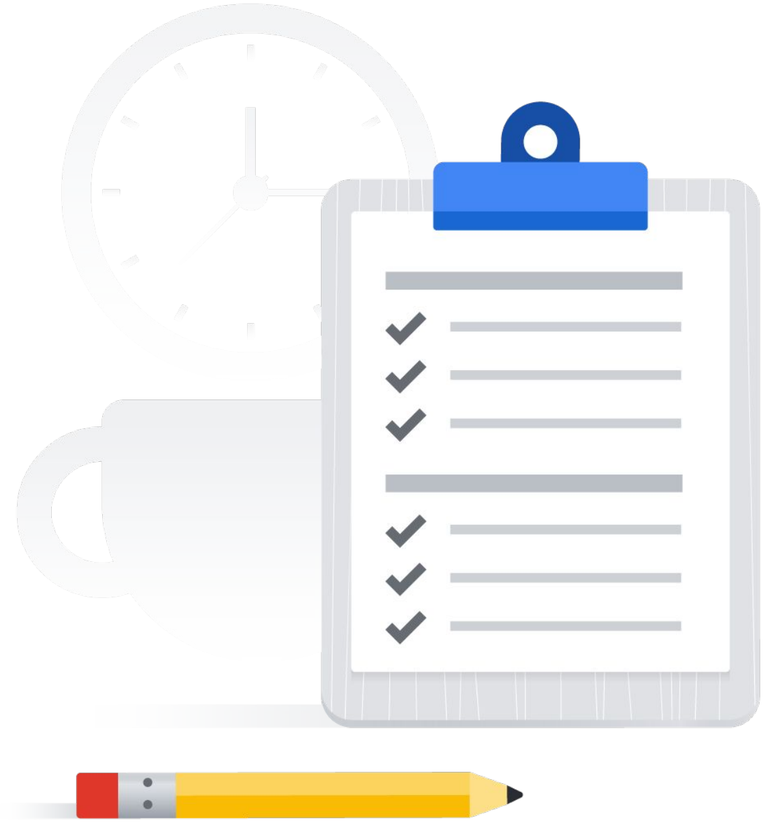
Google Cloud

Lab objectives

Create a managed instance group of backends.

Point an internal load balancer to the backends.

Test the internal load balancer, and call it from a public facing web server.



Google Cloud

Agenda

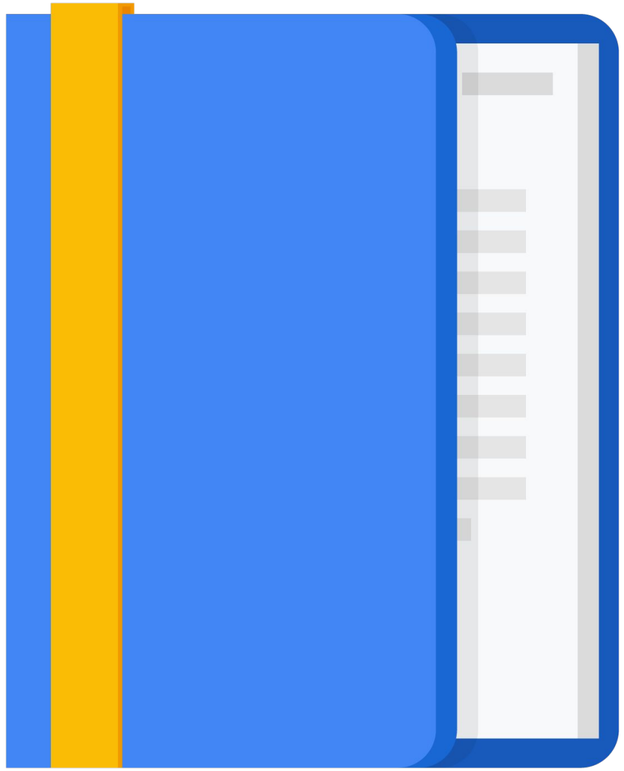
Different Options for Load Balancing

Lab: HTTP Load Balancer with Cloud Armor

Lab: Create an Internal Load Balancer

Quiz

Summary



Google Cloud

Scenario #1

Question

What is a key distinguishing feature of networking in Google Cloud?

A. Unlike other cloud providers, access lists and firewall rules are available.

B. Network topology is not dependent on IP address layout.

C. Network topology is dependent on IP address layout.

D. IPV4 is supported.

Scenario #1

Answer

What is a key distinguishing feature of networking in Google Cloud?

A. Unlike other cloud providers, access lists and firewall rules are available.

B. Network topology is not dependent on IP address layout.

C. Network topology is dependent on IP address layout.

D. IPV4 is supported.

Scenario #2

Question

Which one of the following is true?

A. VPCs are global and subnets are regional.

B. VPCs are regional and subnets are zonal.

C. VPCs are regional. Subnets are not used in Google Cloud.

D. Both VPCs and subnets are global.

Scenario #2

Answer

Which one of the following is true?

A. VPCs are global and subnets are regional.

B. VPCs are regional and subnets are zonal.

C. VPCs are regional. Subnets are not used in Google Cloud.

D. Both VPCs and subnets are global.

Scenario #3

Question

Select the global load balancer from the list.

A. Internal

B. Network

C. Elastic

D. TCP Proxy

Google Cloud

Scenario #3

Answer

Select the global load balancer from the list.

A. Internal

B. Network

C. Elastic

D. TCP Proxy

Google Cloud

Agenda

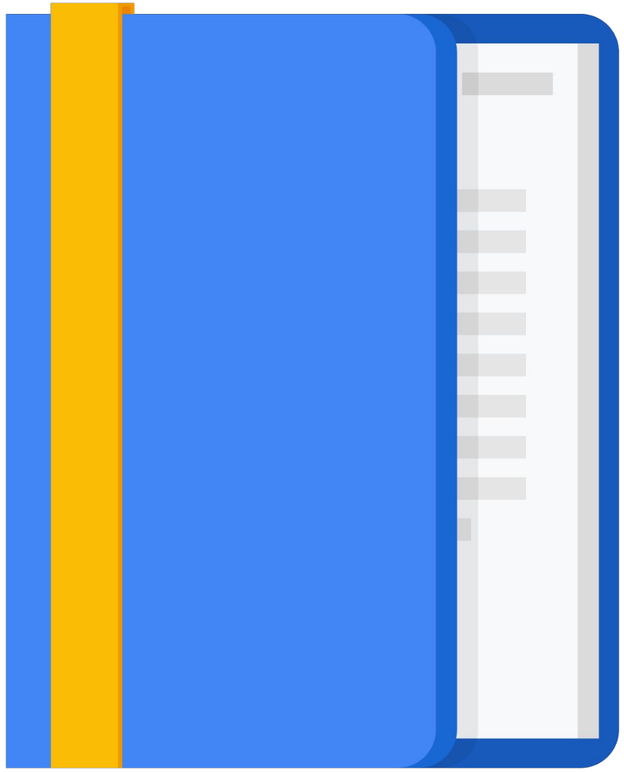
Different Options for Load Balancing

Lab: HTTP Load Balancer with Cloud Armor

Lab: Create an Internal Load Balancer

Quiz

Summary



Google Cloud

Summary (1/3)

- Computers connect via networks. Google Cloud delivers millions of customers' software and services around the globe through its online Cloud network.
- IP addresses allow networks to connect internally. They can be either public or private.
- Google's networking products include: Virtual Private Cloud, Cloud Load Balancer, Cloud CDN, Cloud Interconnect and Cloud DNS.
- VPCs are software defined network constructs. Google's VPC is global.
- A route is a mapping of an IP range to a destination that also consider firewall rules. Firewalls protect networks from unapproved connections.

Summary (2/3)

- Shared VPC allows an organization to connect resources from multiple projects to a common VPC network.
- VPC Network Peering allows private RFC 1918 connectivity across two VPC networks.
- A connection can be made to Google Cloud using IPsec VPN.
- Cloud Interconnect - Dedicated provides direct physical connectivity between a customer on-premise network and the Google Cloud network edge. Cloud Interconnect - Partner provides a Service Provider enabled connectivity between a customer on-premise network and the Google Cloud network edge.

Summary (3/3)

- Cloud VPN securely connects an on-premises network to a Google Cloud VPC network.
- Direct Peering provides a direct connection between a business network and Google's. Carrier Peering provides connectivity through a supported partner.
- Load balancing can be used to take advantage of an augmented infrastructure.


Google Cloud