Google Cloud

Google Cloud and Hybrid Network Architecture

Learning objectives

- Design VPC networks to optimize for cost, security, and performance.
- Configure global and regional load balancers to provide access to services.
- Leverage Cloud CDN to provide lower latency and decrease network egress.
- Evaluate network architecture using the Network Intelligence Center.
- Connect networks using peering, VPNs and Cloud Interconnect.

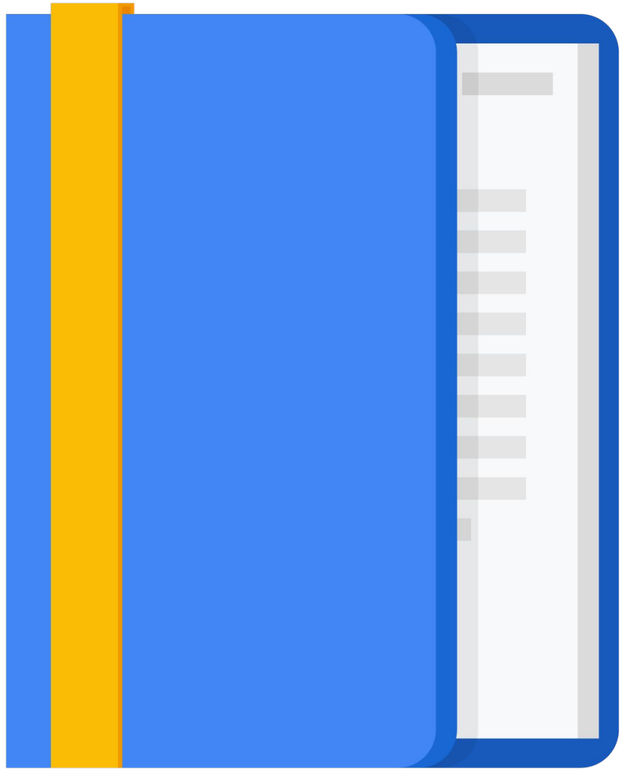
Agenda

Designing Google Cloud Networks

Design Activity #8

Connecting Networks

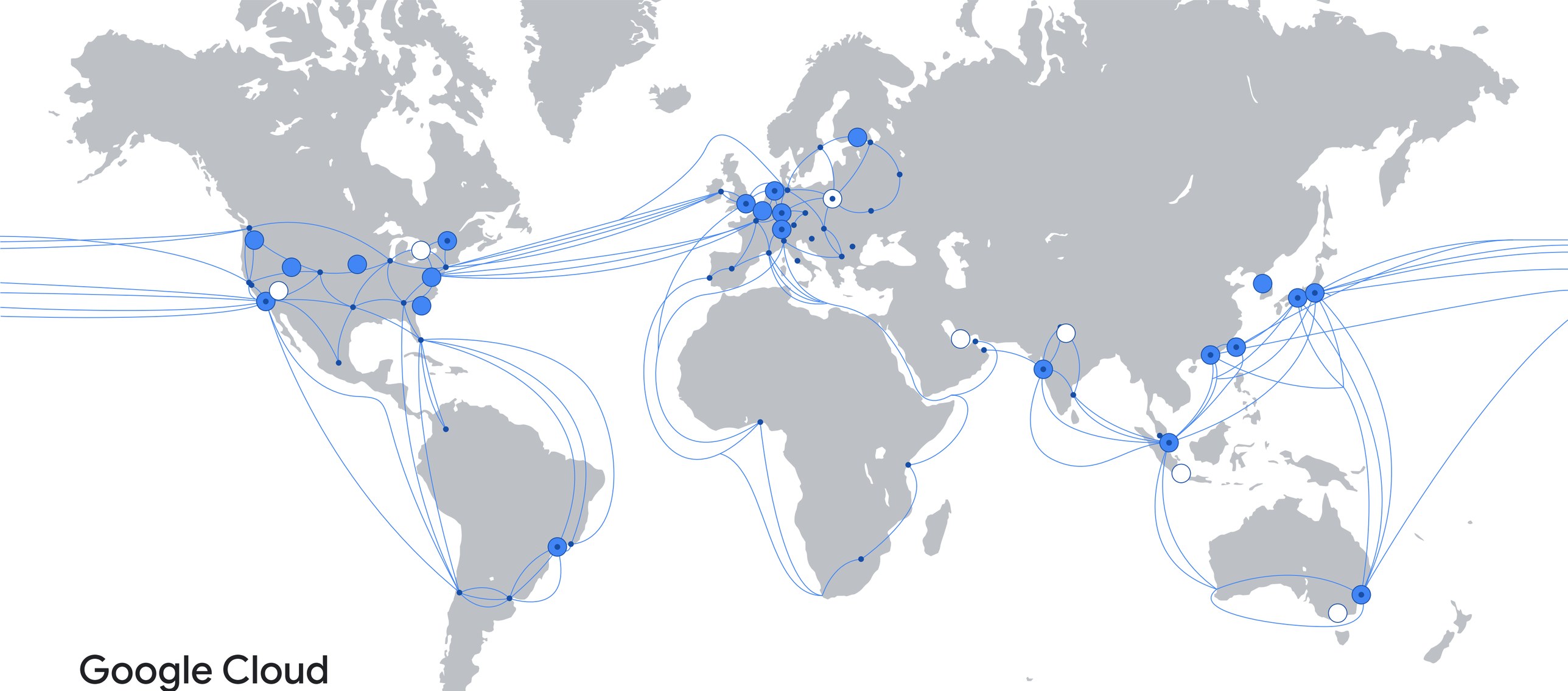
Design Activity #9



Google runs a worldwide network that connects regions all over the world

Design your networks based on location, number of users, scalability, fault tolerance, and other service requirements.

Google Cloud



Google Cloud Platform

Current region with 3 zones

Future region with 3 zones

Edge point of presence

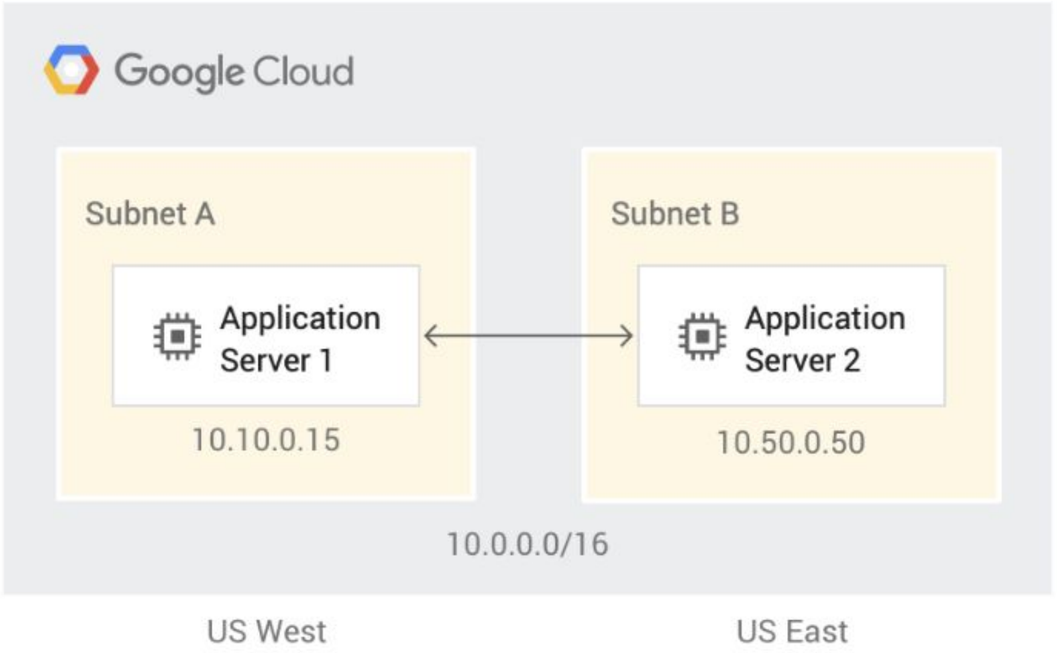
Network

Regions, PoPs, and network

Google Cloud

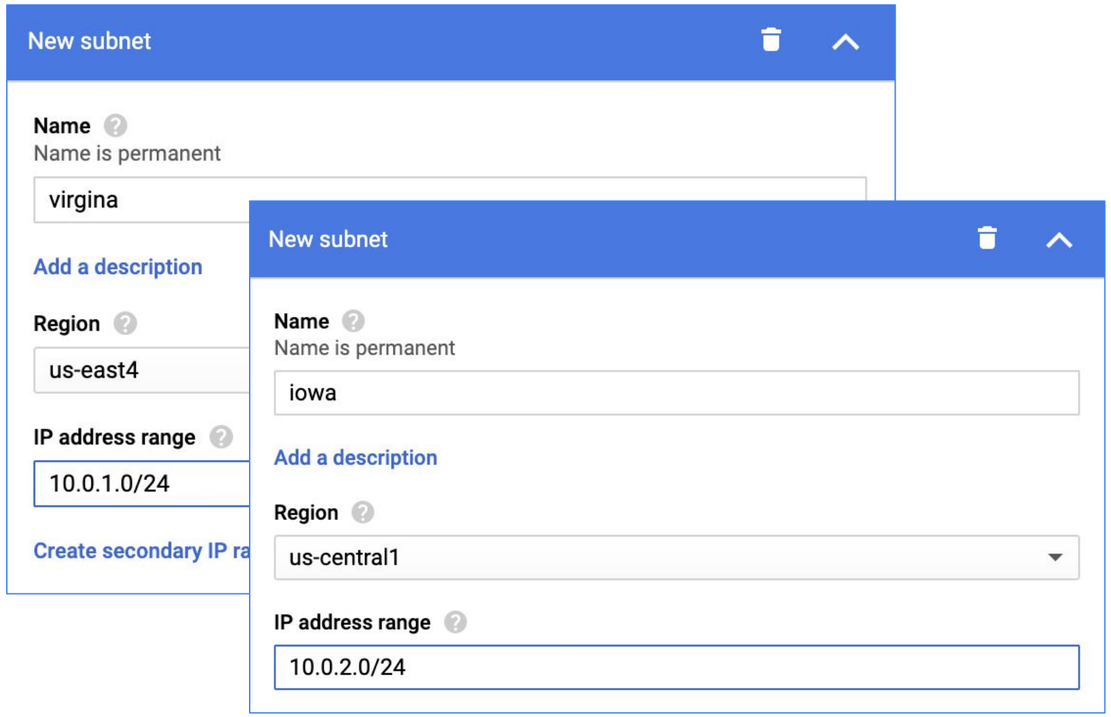
In Google Cloud, VPC networks are global

- When creating networks, create subnets for the regions you want to operate in.
- Resources across regions can reach each other without any added interconnect.
- If you are a global company, choose regions around the world.
- If your users are close together, choose the region closest to them plus a backup region.
- A project can have multiple networks.



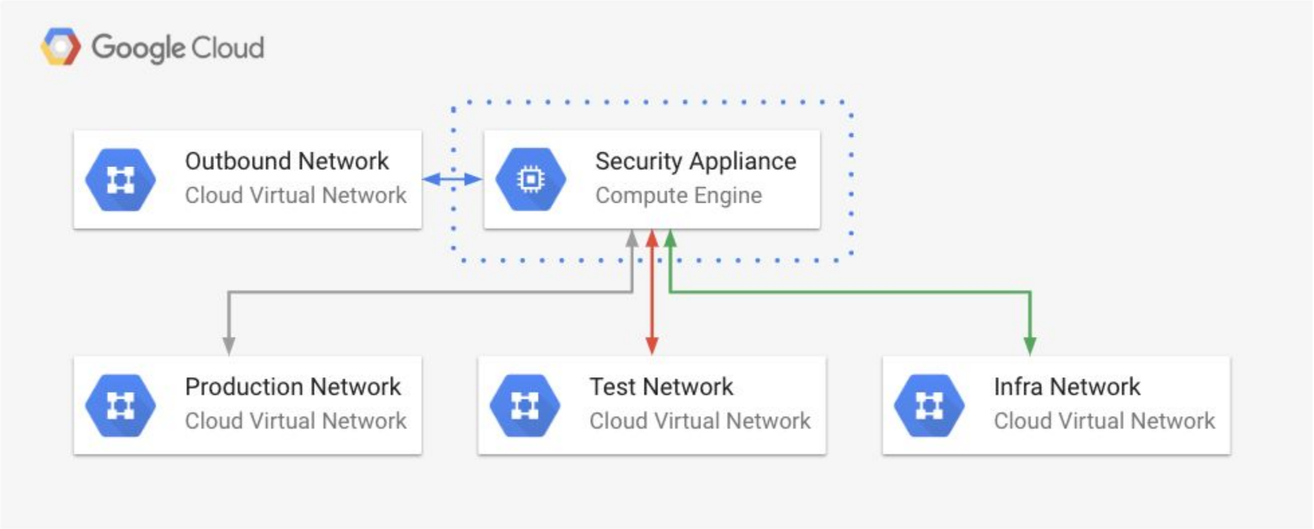
When creating custom subnets, specify the region and the internal IP address range

- IP address ranges cannot overlap.
- Machines in the same VPC can communicate via their internal IP address regardless of the subnet region.
- Subnets don't need to be derived from a single CIDR block.
- Subnets are expandable without down time.
- IP Aliasing or Secondary range can be set on the subnet.



A single VM can have multiple network interfaces connecting to different networks

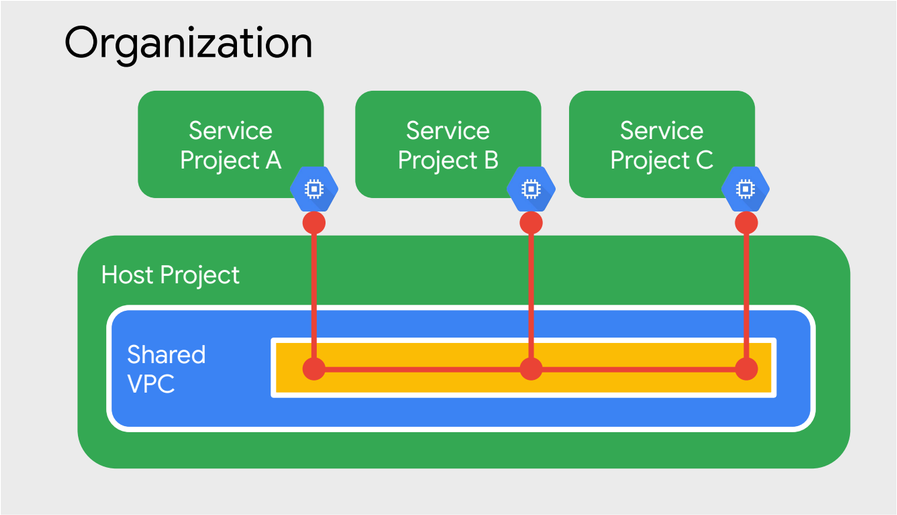
- Each network must have a subnet in the region the VM is created in.
- Each interface must be attached to a different VPC.
- Maximum of 8 interfaces per VM.



A Shared VPC is created in one project, but can be shared and used by other projects

Requires an organization

- Create the VPC in the host project.
- Shared VPC admin shares the VPC with other service projects.

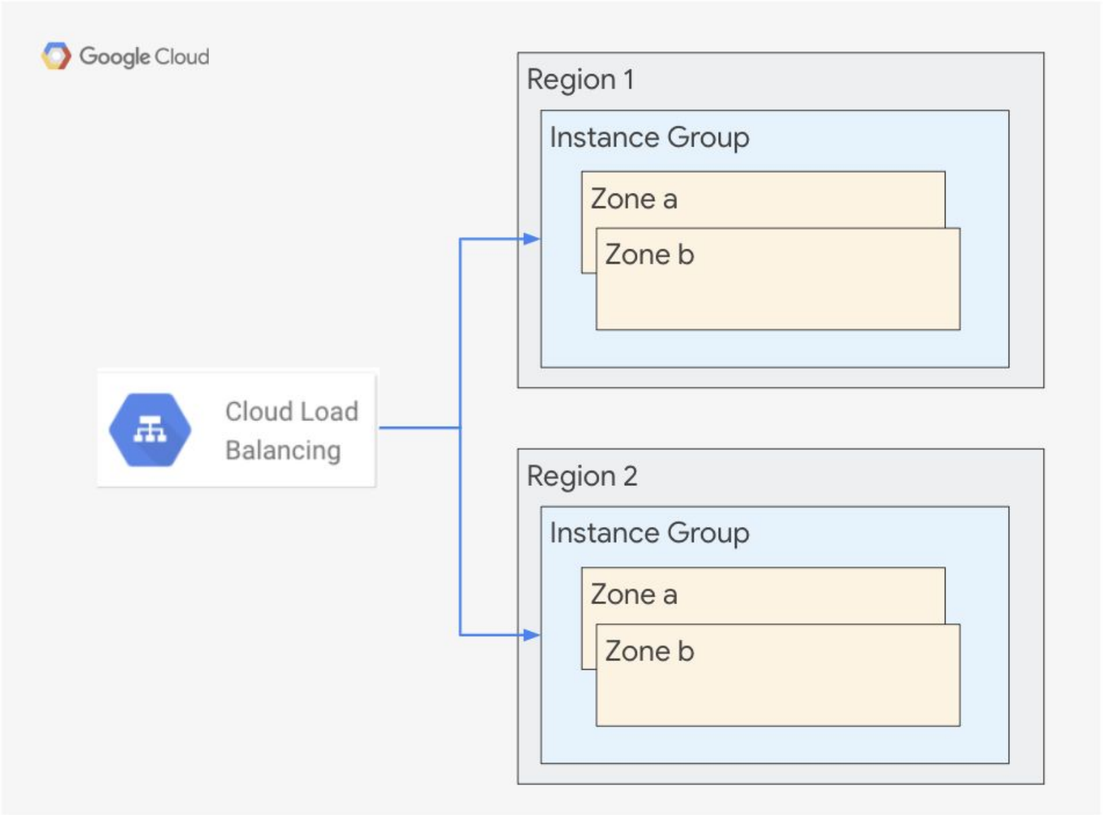


Allows centralized control over network configuration

- Network admins configure subnets, firewall rules, routes, etc.
- Remove network admin rights from developers.
- Developers focus on machine creation and configuration in the shared network.
- Disable the creation of the default network using an organizational policy.

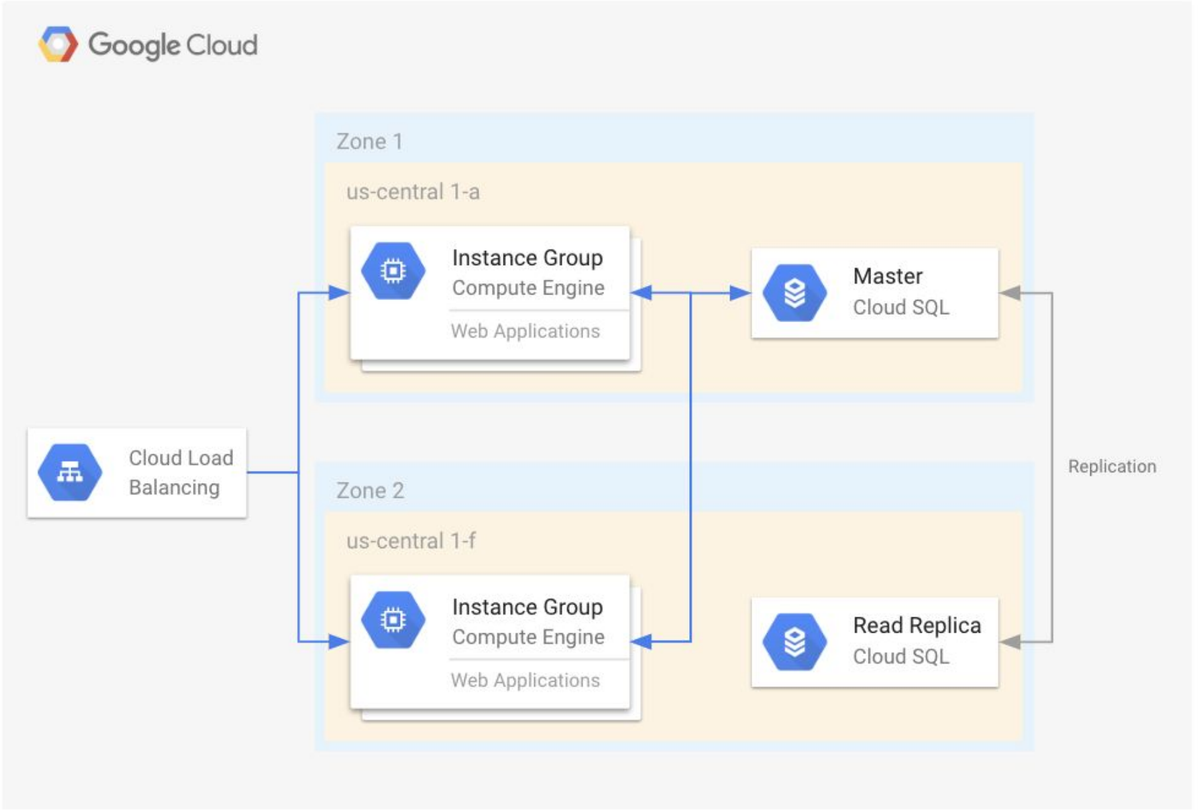
Use a global load balancer to provide access to services deployed in multiple regions

- Global load balancing supported by HTTP load balancer and TCP and SSL proxies.
- HTTP load balancer routes requests to the region closest to the user.
  - Uses a global, anycast IP address.



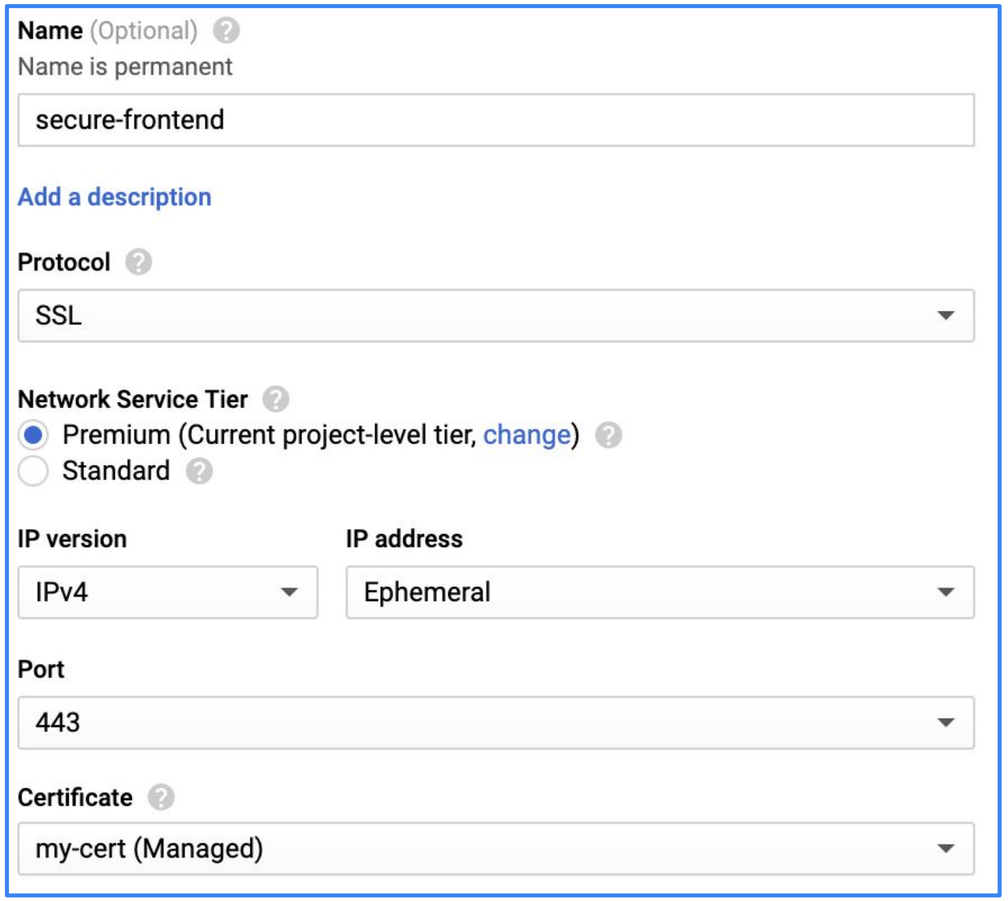
Use a regional load balancer to provide access to services deployed in a single region

- Supported by HTTP, TCP, and UDP load balancers.
- Can have a public or private IP address.
- Can use any TCP or UDP port.



If your load balancers have public IPs, secure them using SSL

- Supported by HTTP and TCP load balancers
- Self-managed and Google-managed SSL certificates



Google Cloud

For lower-latency and decreased egress cost leverage Cloud CDN

- Can be enabled when configuring the HTTP global load balancer.
- Caches static content worldwide using Google Cloud edge-caching locations.
- Cache static data from web servers in Compute Engine instances, GKE pods, or Cloud Storage buckets.

Google Cloud load balancer types and capabilities

HTTP(S) Load Balancing

Layer 7 load balancing for HTTP and HTTPS applications Learn more

Configure
HTTP LB
HTTPS LB (includes HTTP/2 LB)

Options
Internet-facing or internal
Single or multi-region

Start configuration

TCP Load Balancing

Layer 4 load balancing or proxy for applications that rely on TCP/SSL protocol Learn more

Configure
TCP LB
SSL Proxy
TCP Proxy

Options
Internet-facing or internal
Single or multi-region

Start configuration

UDP Load Balancing

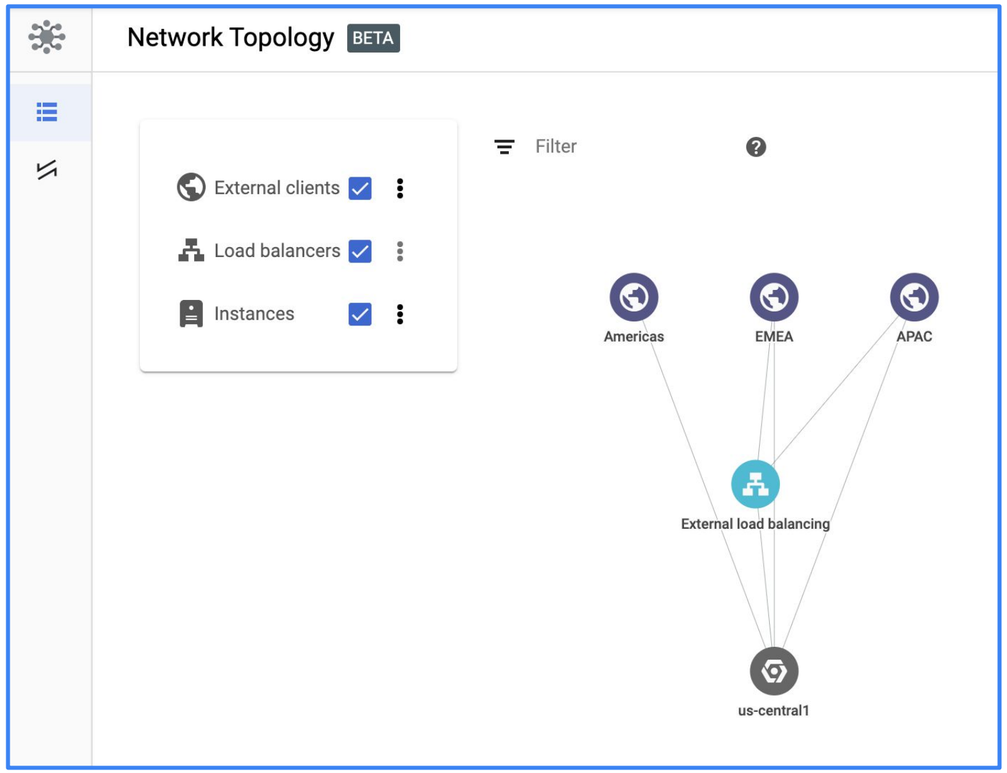
Layer 4 load balancing for applications that rely on UDP protocol Learn more

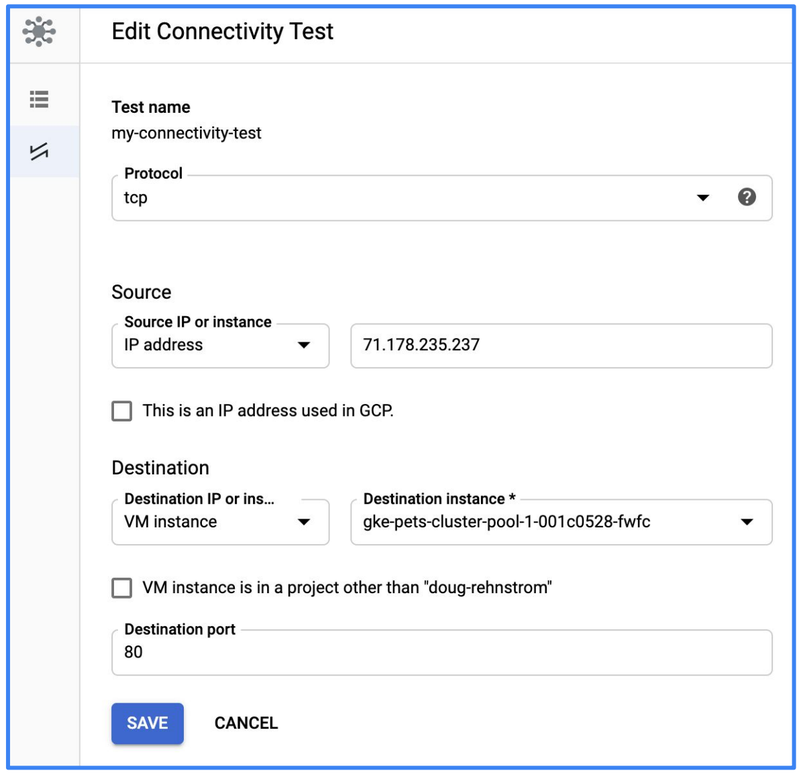
Configure
UDP LB

Options
Internet-facing or internal
Single-region

Start configuration

Network Intelligence Center can be used to visualize network topology and test network connectivity





Google Cloud

Activity 8: Defining network characteristics

Refer to your Design and Process Workbook.

- Specify the network characteristics for your case study VPC.
- Choose the type of load balancer required for each service.

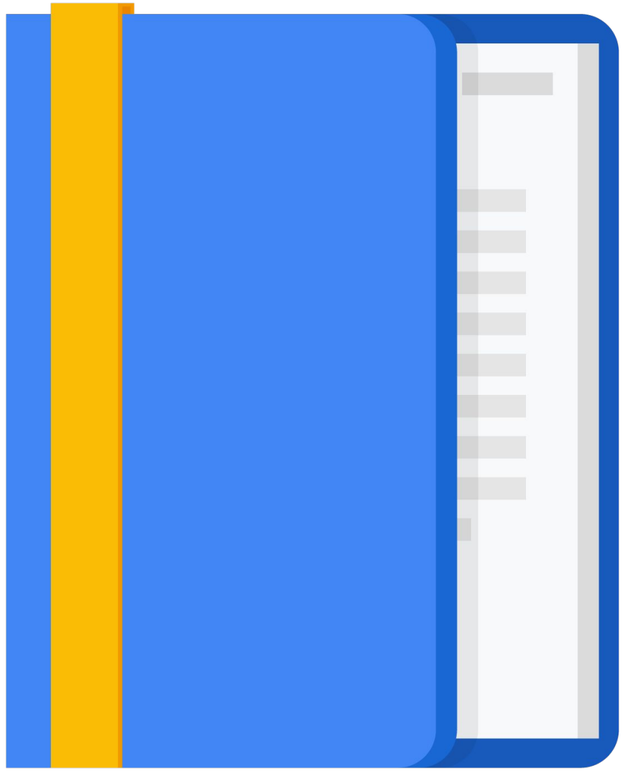
Agenda

Designing Google Cloud Networks

Design Activity #8

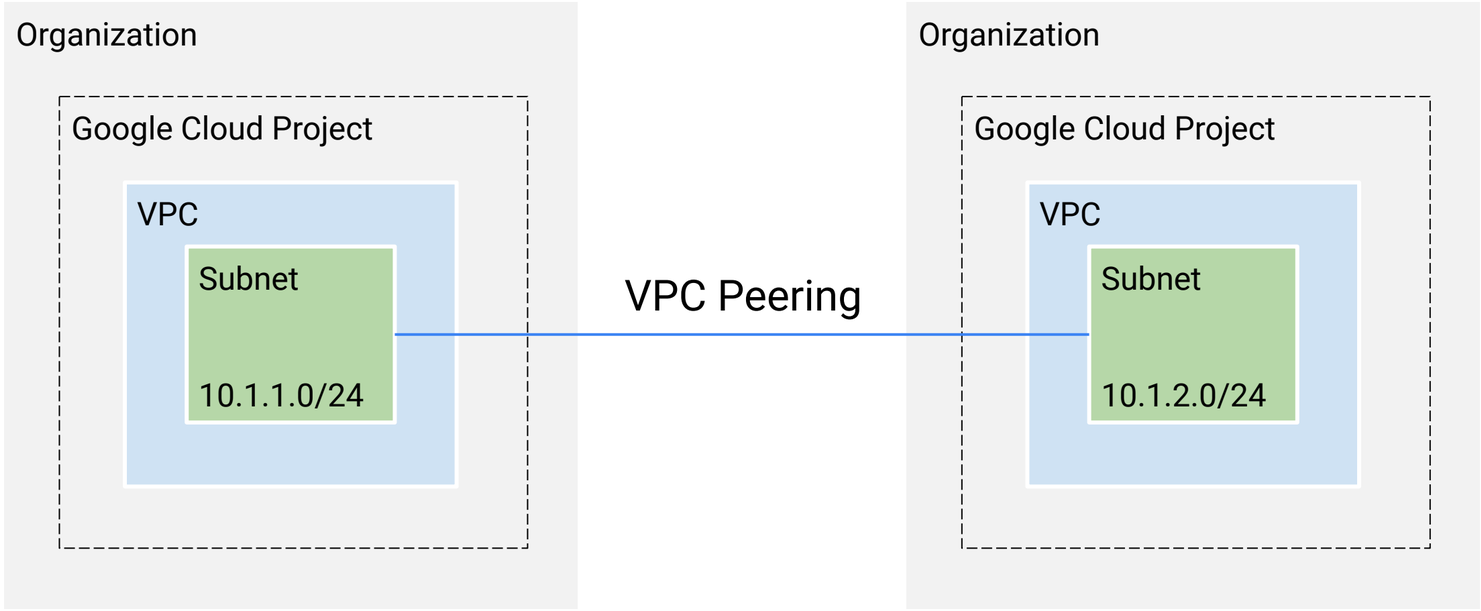
Connecting Networks

Design Activity #9



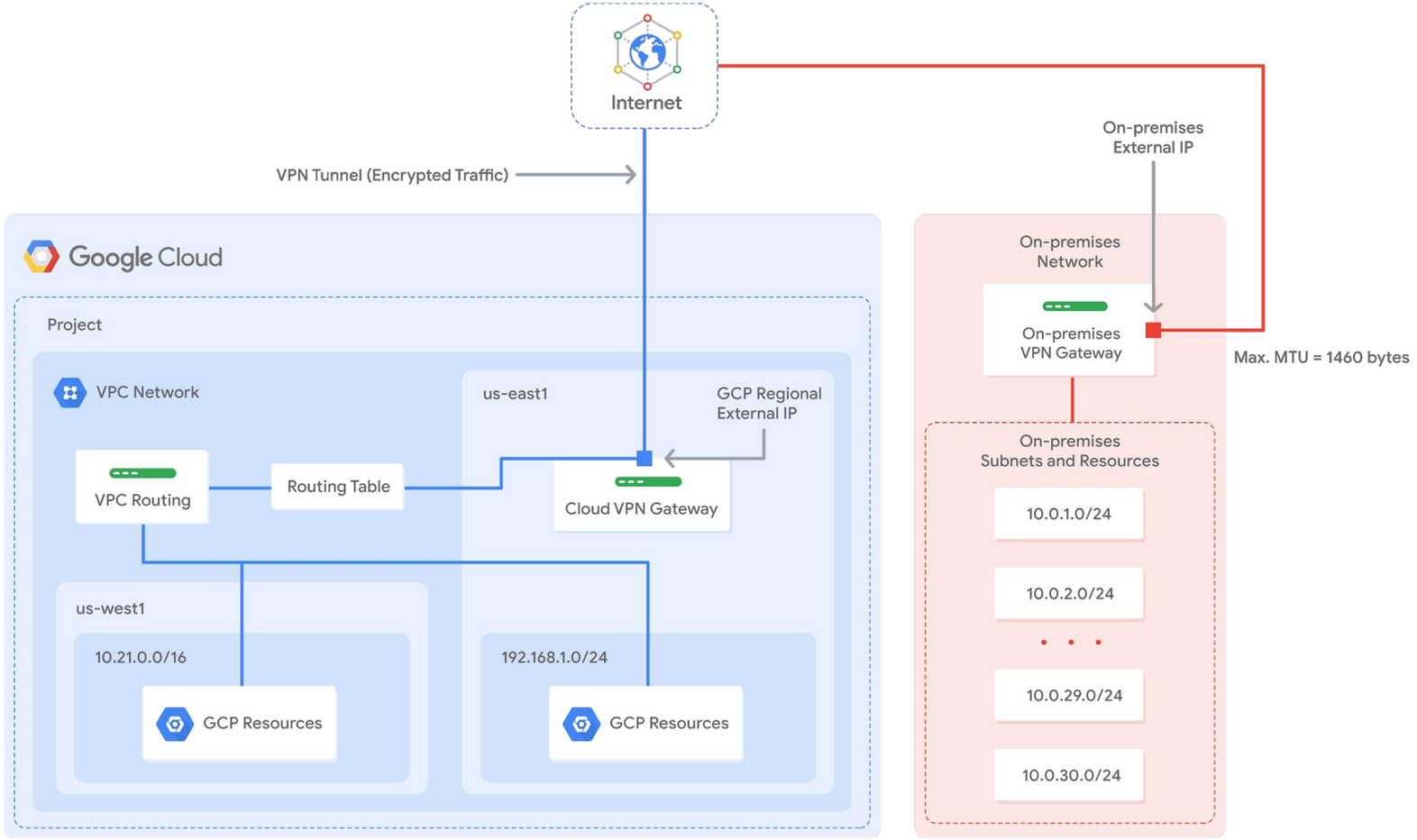
Use VPC peering to connect networks when they are both in Google Cloud

- Can be the same or different organizations.
- Subnet ranges cannot overlap.
- Network admins for each VPC must approve the peering requests.



Use Cloud VPN to connect a Google Cloud network to a network on-premises or in another cloud

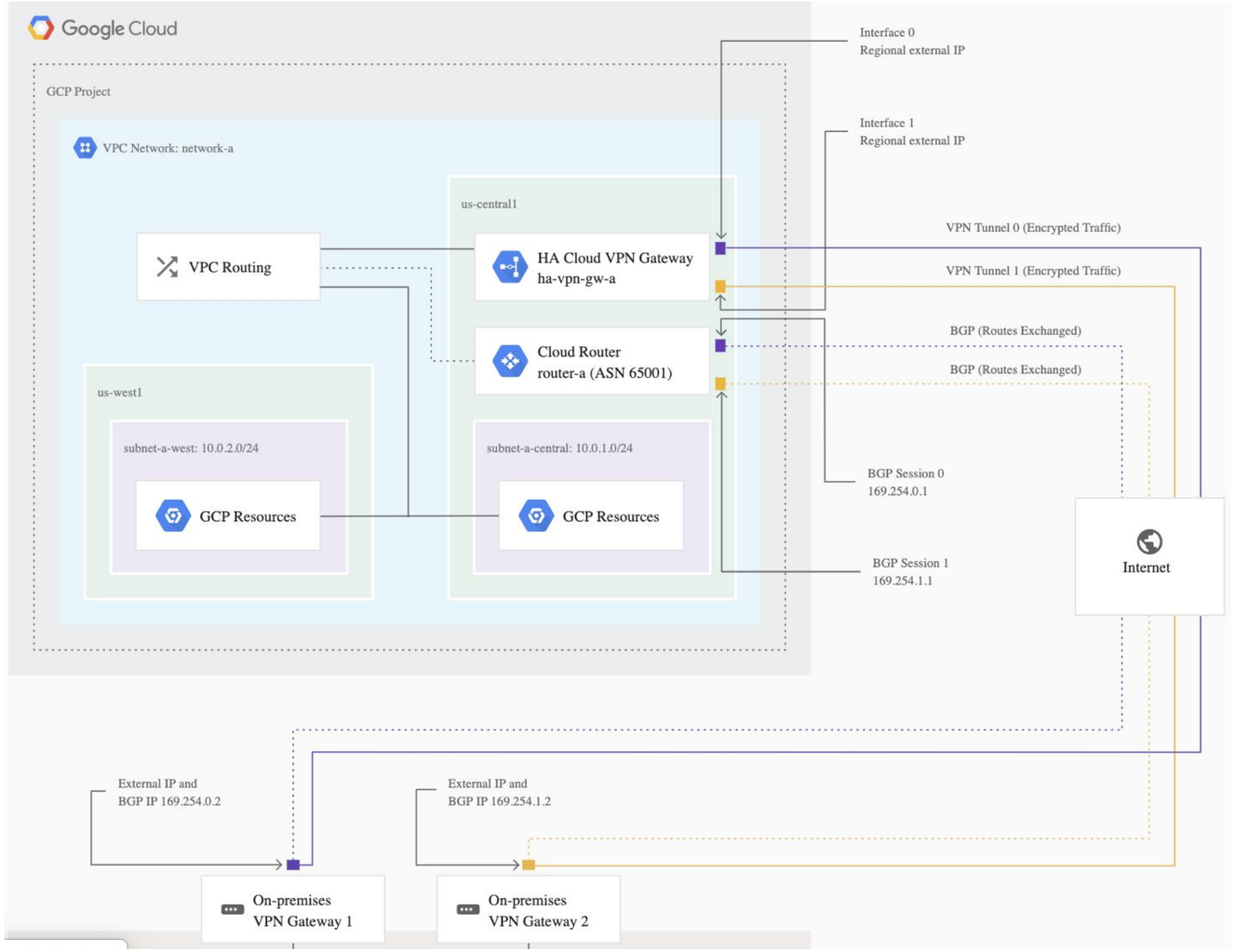
- 99.9% SLA
- For low-volume data connections
- Can configure static or dynamic routes using BGP (Border Gateway Protocol)



Google Cloud

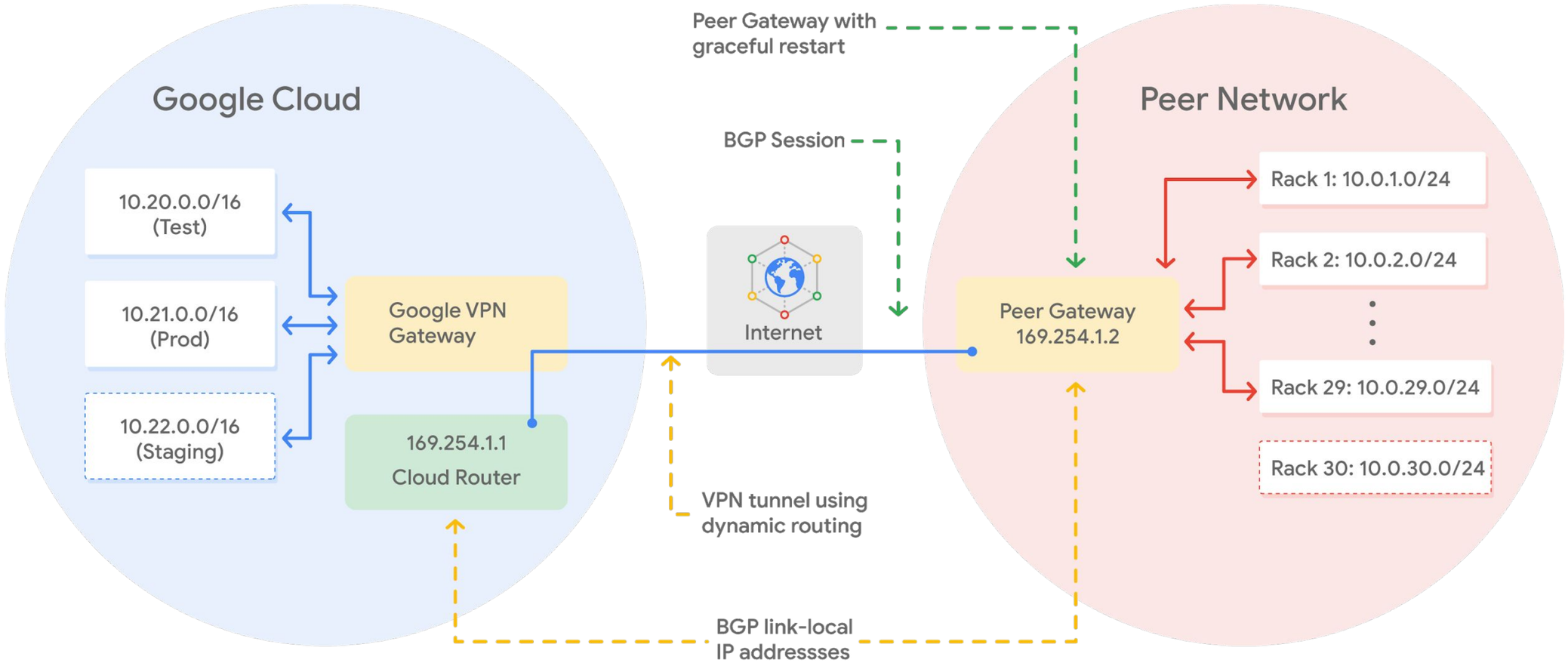
High availability VPN ensures 99.99% availability

- VPN gateway has 2 network interfaces.
- Creates two IP addresses.
- Each gateway supports multiple VPN tunnels.



Google Cloud

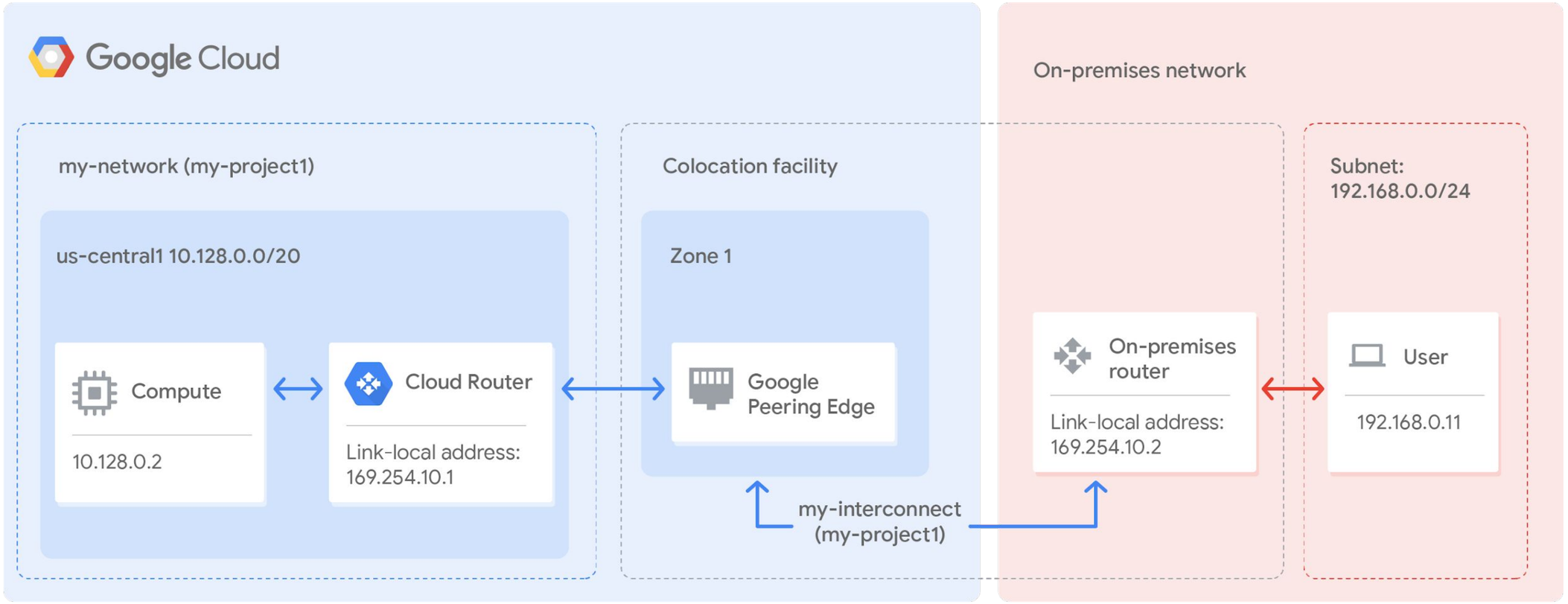
Cloud Router enables dynamic discovery of routes between connected networks



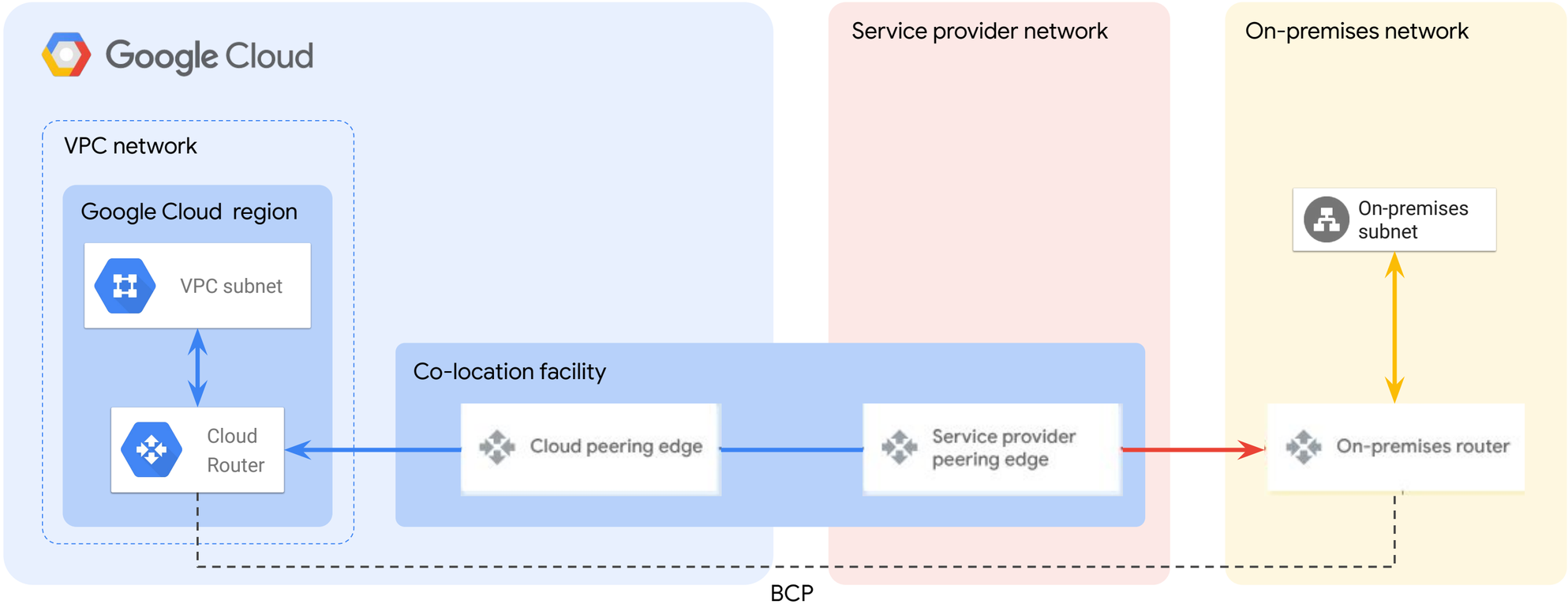
Use Cloud Interconnect when a dedicated high-speed connection is required between networks

- Dedicated Interconnect provides a direct connection to a colocation facility.
  - From 10 to 200 Gbps
- Partner Interconnect provides a connection through a service provider.
  - Can purchase less bandwidth from 50 Mbps
- Allows access to VPC resources using internal IP address space.
- Private Google Access allows on-premises hosts to access Google services using private IPs.

Dedicated Interconnect provides direct physical connections



Partner Interconnect provides connectivity through a supported service provider



Activity 9: Diagramming your network

Refer to your Design and Process Workbook.

- Draw a diagram that depicts your network requirements.

Quiz

You are deploying a large-scale web application with users all over the world and a lot of static content. Which load balancer configuration would likely be the best?

A. TCP load balancer with SSL configured

B. HTTP load balancer with SSL configured

C. HTTP load balancer with SSL configured and the CDN enabled

D. UDP load balancer with SSL configured and the CDN enabled

Quiz

You are deploying a large-scale web application with users all over the world and a lot of static content. Which load balancer configuration would likely be the best?

A. TCP load balancer with SSL configured

B. HTTP load balancer with SSL configured

C. HTTP load balancer with SSL configured and the CDN enabled

D. UDP load balancer with SSL configured and the CDN enabled

Quiz

You are a large bank deploying an online banking service to Google Cloud. The service needs high-volume access to mainframe data on-premises. Which connectivity option would likely be best?

A. VPN

B. HTTPS

C. Cloud Interconnect

D. Peering

Quiz

You are a large bank deploying an online banking service to Google Cloud. The service needs high-volume access to mainframe data on-premises. Which connectivity option would likely be best?

A. VPN

B. HTTPS

C. Cloud Interconnect

D. Peering

Quiz

You have a contract with a service provider to manage your Google VPC networks. You want to connect a network they own to your VPC. Both networks are in Google Cloud. Which connection option should you choose?

A. VPN

B. VPN with high availability and Cloud Router

C. Cloud Interconnect

D. VPC peering

Quiz

You have a contract with a service provider to manage your Google VPC networks. You want to connect a network they own to your VPC. Both networks are in Google Cloud. Which connection option should you choose?

A. VPN

B. VPN with high availability and Cloud Router

C. Cloud Interconnect

D. VPC peering

Quiz

You want a secure, private connection between your network and a Google Cloud network. There is not a lot of volume, but the connection needs to be extremely reliable. Which configuration below would you choose?

A. VPN

B. VPN with high availability and Cloud Router

C. Cloud Interconnect

D. VPC peering

Quiz

You want a secure, private connection between your network and a Google Cloud network. There is not a lot of volume, but the connection needs to be extremely reliable. Which configuration below would you choose?

A. VPN

B. VPN with high availability and Cloud Router

C. Cloud Interconnect

D. VPC peering

Review

Google Cloud and Hybrid Network Architecture

More resources

Cloud networking products

https://cloud.google.com/products/networking/

Google Cloud Hybrid Connectivity

https://cloud.google.com/hybrid-connectivity/


Google Cloud