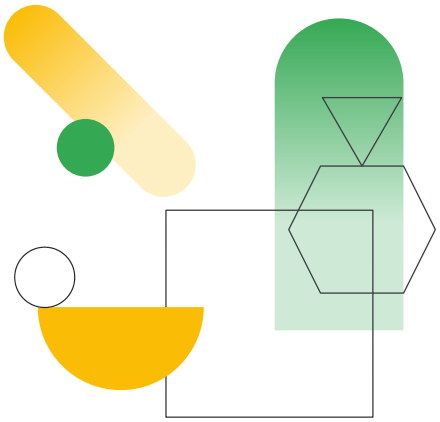
Proprietary + Confidential

Google Cloud

Google Cloud and Hybrid Network Architecture



Proprietary + Confidential

Learning objectives

01 Design VPC networks to optimize for cost, security, and performance.

02 Configure global and regional load balancers to provide access to services.

03 Leverage Cloud CDN to provide lower latency and decrease network egress.

04 Evaluate network architecture using the Network Intelligence Center.

05 Connect networks using peering, VPNs and Cloud Interconnect.

Google Cloud

This module discusses the Google Cloud network architecture. It includes load balancing and the range of load balancing options—global, regional, internal, external—and the traffic type. The connection of on-premises networks with Google Cloud networks is also discussed with the various interconnection options. The different options and how they impact performance, security, and cost and how CDN can be leveraged to manage costs are examined. Managing and diagnosing networks through the Network Intelligence Center is also covered.

Proprietary + Confidential

Agenda

01	Designing Google Cloud Networks
02	Connecting Networks
03	Quiz
04	Review

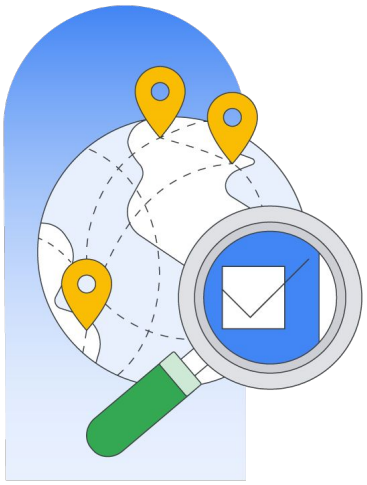
Proprietary + Confidential

Designing Google Cloud Networks

Proprietary + Confidential

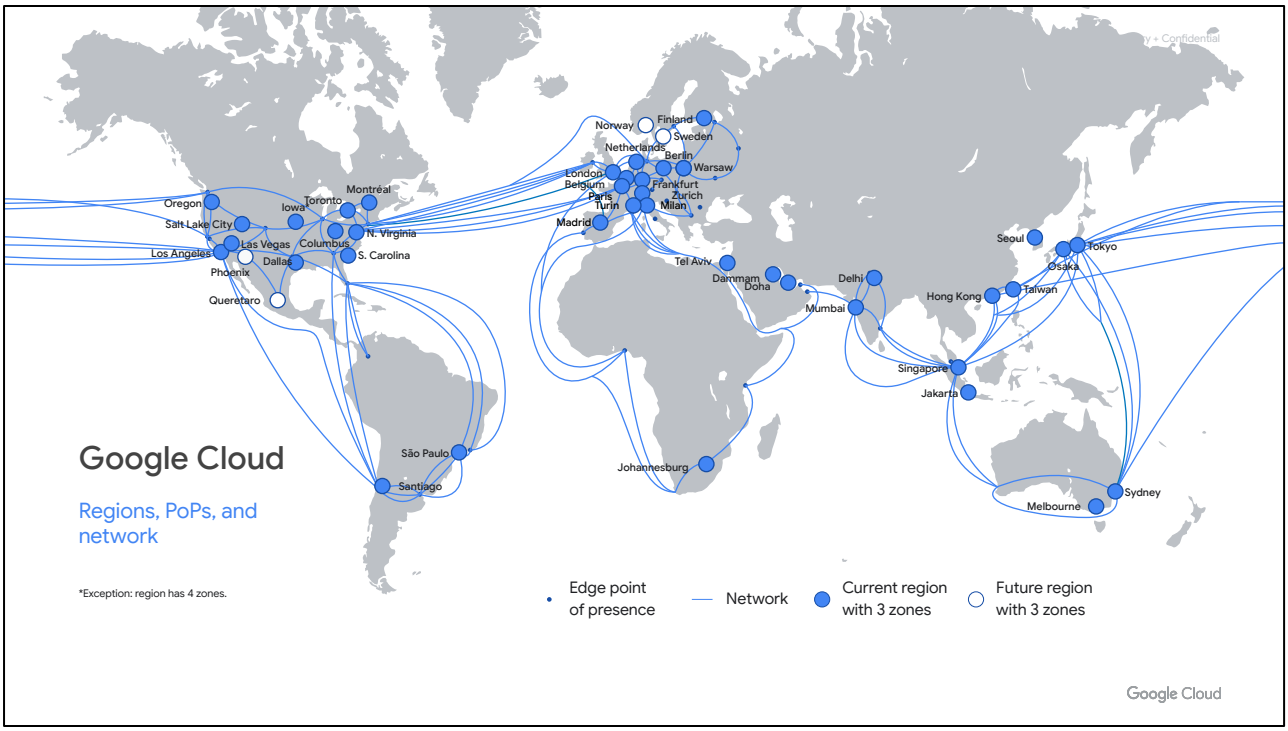
Google runs a worldwide network that connects regions all over the world

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



Google Cloud

Google Cloud's footprint spans 121 zones across 40 regions and 187 network edge locations across more than 200 countries and territories. High bandwidth connectivity via subsea cables provides unrivalled network performance. Google Cloud customers can use this high bandwidth infrastructure for their own cloud networking needs.



The number of regions and zones is continually increasing. An up-to-date view is here: https://cloud.google.com/about/locations/.

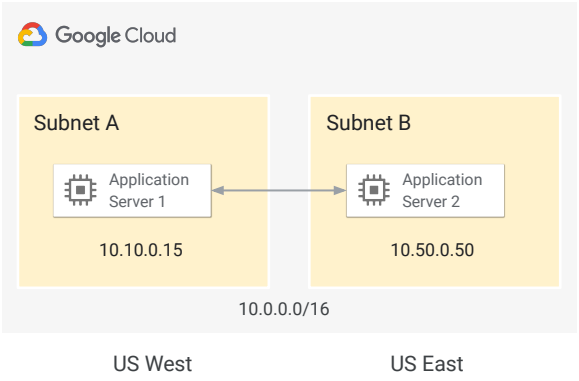
The network and points of presence are here: https://cloud.google.com/about/locations/?tab=network.

The edge points of presence are the locations where Google networks are connected with internet service providers to allow users to connect. The Google Cloud network strongly distinguishes Google from other cloud service providers. The points of presence allow Google to provide very low latency network performance.

Proprietary + Confidential

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.



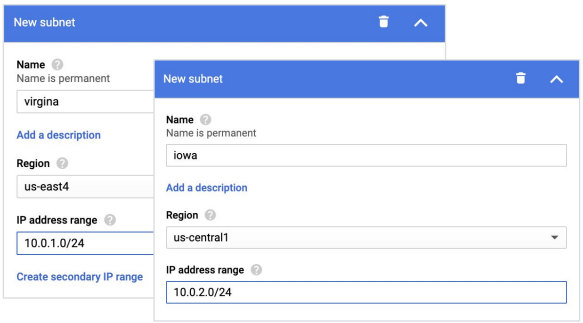
Google Cloud

VPCs are software-designed versions of physical networks; VPC has global scope and so spans regions. When creating a VPC, you can create subnetworks for the regions you want to operate in. Automatic subnet creation mode will create a subnetwork in each region by default. A VPC is associated with a project or an organization. Projects can have multiple VPCs.

Proprietary + Confidential

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.



Google Cloud

Subnets are regional resources, and each subnet has a range of IP addresses. A network must have at least one subnetwork before it can be used. When a subnet is created, the primary IP address range must be specified. It is possible to select any private CIDR block for the primary IP address range of the subnet. These addresses can be used for VM primary internal IP addresses, VM alias IP addresses, and the IP addresses of internal load balancers. Alias IP addresses are a feature that allows a range of IP addresses to be assigned to a VM's network interfaces. The use case is if multiple services are running on a VM, and each service needs a different IP address. Secondary IP address ranges can be defined, which are separate CIDR blocks and are used for alias IP addresses.

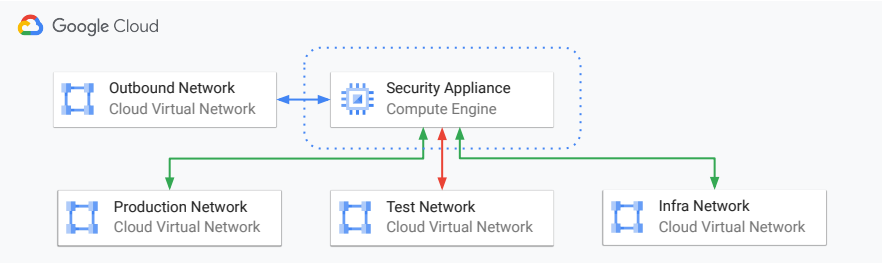
When CIDR blocks are assigned, subnetworks do not need to form a contiguous block, although automode VPC networks create a subnet in each region automatically with contiguous CIDR blocks.

Machines on the same VPC but different subnetworks can communicate using their internal IP addresses.

Proprietary + Confidential

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.



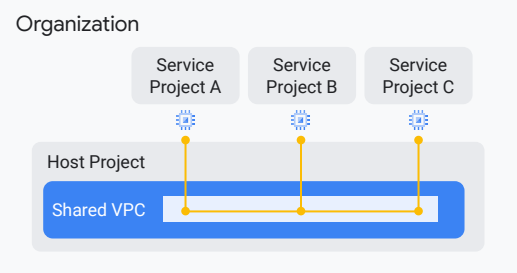
By default, every instance in a VPC network has a single default network interface. It is possible to add more interfaces, up to a maximum of 8. Each interface must be connected to a different VPC network. Network interfaces can only be added at instance creation and can only be removed by instance deletion.

Proprietary + Confidential

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.

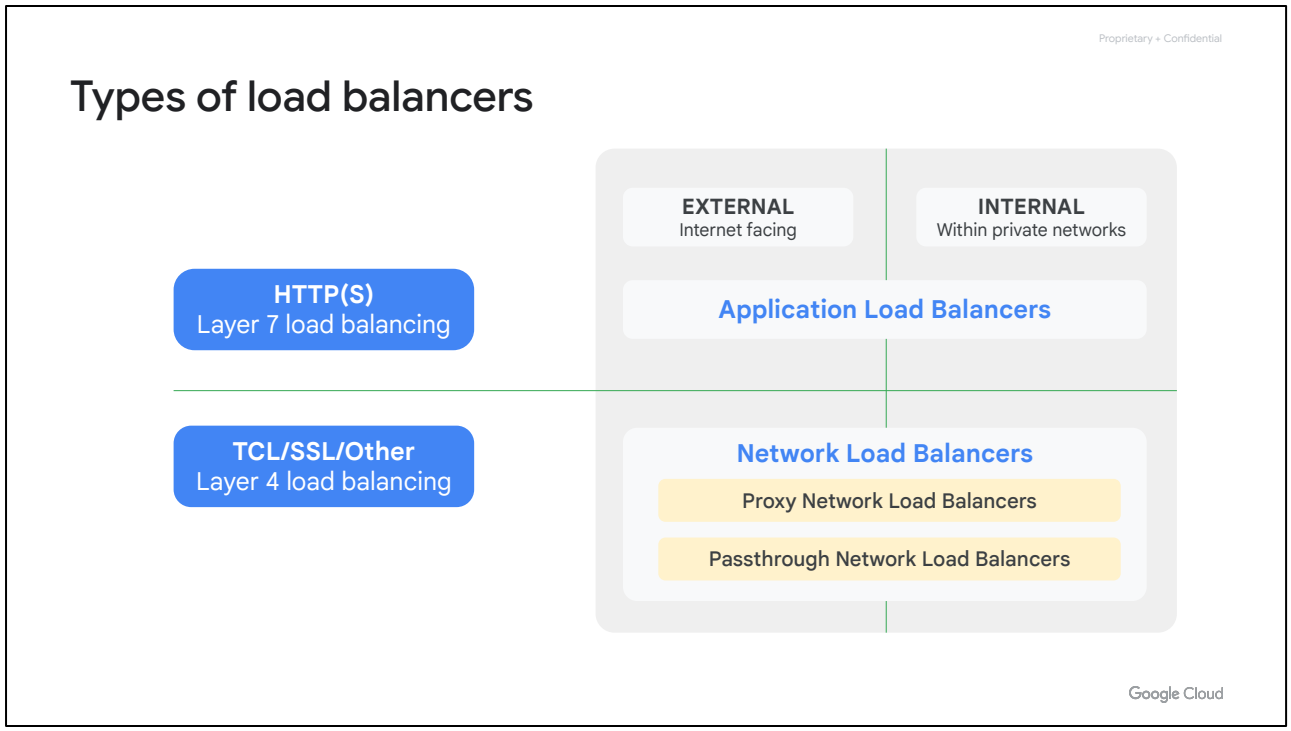
Google Cloud

Shared VPC allows an organization to connect resources from multiple projects to a common VPC network so that they can communicate with each other securely and efficiently using internal IPs from that network. When you use Shared VPC, you designate a project as a host project and attach one or more other service projects to it. The VPC networks in the host project are called Shared VPC networks. Eligible resources from service projects can use subnets in the Shared VPC network. Eligible resources include Compute Engine resources, GKE clusters, and App Engine flexible instances.

More details of eligible resources can be found here: https://cloud.google.com/vpc/docs/shared-vpc#resources_that_can_be_attached_to_shared_vpc_networks_from_a_service_project

Shared VPC lets organization administrators delegate administrative responsibilities, such as creating and managing instances, to Service Project Admins while maintaining centralized control over network resources like subnets, routes, and firewalls. This model allows organizations to do the following:

1. Implement the security best practice of least privilege for network admin, auditing, and access control. Shared VPC admins delegate admin tasks to admins in the shared network without allowing service project admins to make network-affecting changes. They can only create and manage instances that use the shared VPC.
2. Apply and enforce consistent access control policies at the network level for multiple service projects.



Application Load Balancers and **Network Load Balancers** are two primary types of load balancers offered by Google Cloud, each designed for specific use cases.

Application Load Balancers operate at the application layer (Layer 7) of the OSI model. They are ideal for applications that require load balancing based on HTTP(S) headers, cookies, or URL paths. **Application Load Balancers** provide features like SSL/TLS termination, session affinity, and content-based routing.

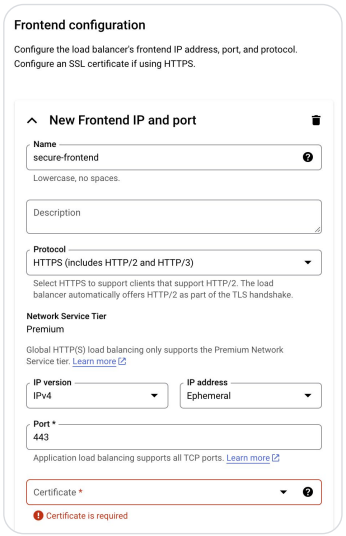
Network Load Balancers operate at the network layer (Layer 4) of the OSI model. They are suitable for load balancing based on IP addresses and ports. **Network Load Balancers** are often used for TCP and UDP traffic, as well as for scenarios where low latency and high throughput are critical. They support features like TCP/UDP load balancing and health checks.

For more information on Load Balancers, please refer to Cloud Load Balancing Overview.

Proprietary + Confidential

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

- Supported by Application Load Balancers and proxy Network Load Balancers.
- Self-managed and Google-managed SSL certificates.



Google Cloud

With public IPs, traffic will be traversing the internet, so it is a best practice to use SSL for both Application Load Balancers and proxy Network Load Balancers. When configuring an Application Load Balancer, HTTP is the default protocol in the Google Cloud console for the frontend configuration, and HTTPS requires explicit selection together with the certificate. For a proxy Network Load Balancer, SSL is the default in the frontend configuration.

There are two types of certificates supported: self-managed and Google-managed certificates. Details on managing certificates is here: https://cloud.google.com/load-balancing/docs/ssl-certificates

Proprietary + Confidential

For lower-latency and decreased egress cost leverage Cloud CDN

- Can be enabled when configuring the global external Application 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

Cloud CDN uses the globally distributed edge points of presence to speed content delivery for content served. Content sources can be Compute Engine, GKE pods, or Cloud Storage.

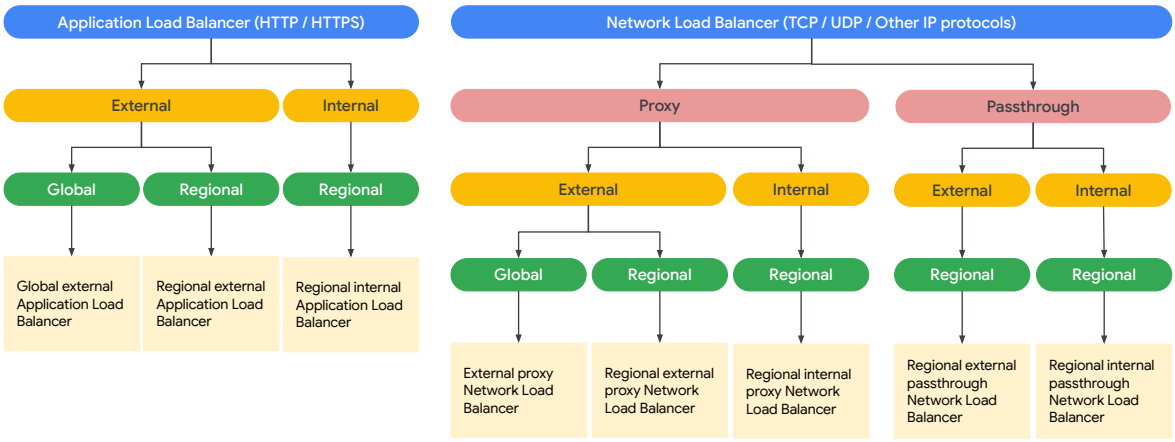
Some of the advantages of using Cloud CDN are better user experience through lower network latency and a reduction in serving costs. Cloud CDN is used with global external Application Load Balancers.

At a high level, Cloud CDN works as follows:

- When a request for content is made to an Application Load Balancer, the request arrives at a Google Front End (GFE) located at a point of presence as close as possible to the user.
- Assuming that the backend has Cloud CDN configured, then the GFE looks in the Cloud CDN cache for a response to the request. If the GFE finds a cached response, the GFE sends the cached response to the requestor.
- Otherwise, if the GFE can't find a cached response for the request, the GFE makes a request to the appropriate backend (the origin server). If the response to this request is cacheable, the GFE stores the response in the Cloud CDN cache so that the cache can be used for subsequent requests.
- To use Cloud CDN, the load balancer must use premium network tiers.

Proprietary + Confidential

Deployment modes available for Cloud Load Balancing



Google Cloud

To determine which Cloud Load Balancing product to use, you must first determine what traffic type your load balancers must handle. As a general rule, you'd choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP(S) traffic. You'd choose a proxy Network Load Balancer to implement TLS offload, TCP proxy, or support for external load balancing to backends in multiple regions. You'd choose a passthrough Network Load Balancer to preserve client source IP addresses, avoid the overhead of proxies, and to support additional protocols like UDP, ESP, and ICMP. UDP, or if you need to expose client IP addresses to your applications.

You can further narrow down your choices depending on your application's requirements: whether your application is external (internet-facing) or internal and whether you need backends deployed globally or regionally.

Proprietary + Confidential

Summary of Google Cloud load balancers

Load balancer	Deployment mode	Traffic type	Network Service Tier	Load-balancing scheme
Application Load Balancers	**Global external**	HTTP or HTTPS	Premium	EXTERNAL_MANAGED
	Regional external	HTTP or HTTPS	Standard	EXTERNAL_MANAGED
	Classic	HTTP or HTTPS	Global in Premium Regional in Standard	EXTERNAL
	Internal Always regional	HTTP or HTTPS	Premium	INTERNAL_MANAGED
Proxy Network Load Balancers	**Global external**	TCP with optional SSL offload	Global in Premium Regional in Standard	EXTERNAL
	Regional external	TCP	Standard only	EXTERNAL_MANAGED
	Internal Always regional	TCP without SSL offload	Premium only	INTERNAL_MANAGED
Passthrough Network Load Balancers	**External** Always regional	TCP, UDP, ESP, GRE, ICMP, and ICMPv6	Premium or Standard	EXTERNAL
	Internal Always regional	TCP or UDP	Premium only	INTERNAL

Google Cloud

If you prefer a table over a flow chart, we recommend this summary table.

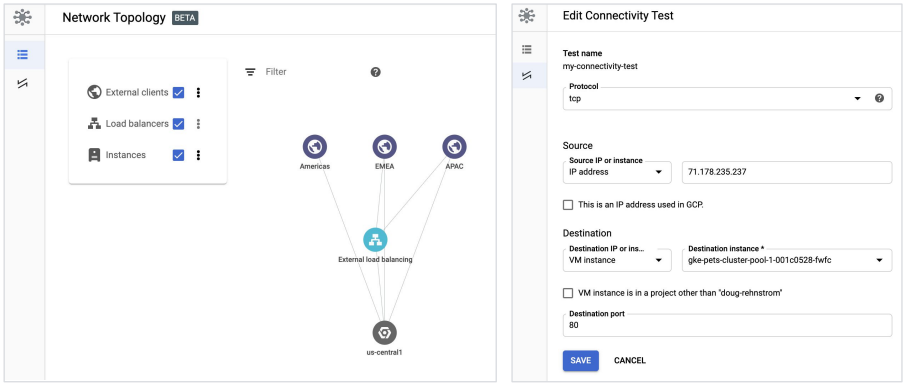
The load-balancing scheme is an attribute on the forwarding rule and the backend service of a load balancer and indicates whether the load balancer can be used for internal or external traffic.

The term *_MANAGED in the load-balancing scheme indicates that the load balancer is implemented as a managed service either on Google Front Ends (GFEs) or on the open source Envoy proxy. In a load-balancing scheme that is *_MANAGED, requests are routed either to the GFE or to the Envoy proxy.

For more information on Network Service Tiers, refer to the documentation: https://cloud.google.com/network-tiers/docs/overview.

Proprietary + Confidential

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



Google Cloud

Network Intelligence Center, available from the Cloud Console, provides visibility into network topology and a centralized monitoring facility. This helps with troubleshooting and security. The center provides the ability to test connectivity, which supports security and compliance checks.The ability to view traffic flows is very powerful, and metrics support the planning and optimizing of architecture.

There is no need for any configuration: the telemetry data is automatically collected to produce the visualizations. By default, two days' history is preserved, although up to six weeks can be configured to be retained. An important point to note is that the visualization will only display resources that communicated during the selected display period.

Proprietary + Confidential

Activity 8

15 min

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.

Proprietary + Confidential

Connecting Networks

Google Cloud

This chapter will introduce the different ways of connecting networks to Google VPC networks.

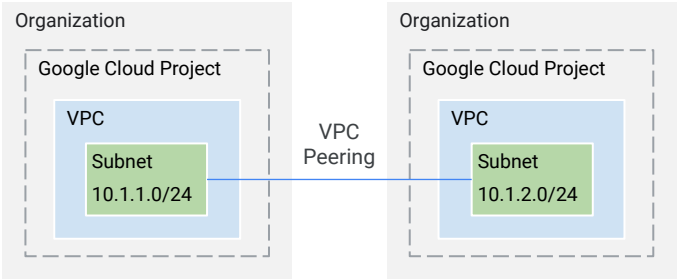
The options discussed are:

- VPC Peering
- Virtual private networks - Cloud VPNs
- Cloud Interconnect - both Dedicated Interconnect and Partner Interconnect

Proprietary + Confidential

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.



Google Cloud

VPC Network Peering allows services to be made available privately across different VPC networks. The networks can be in the same project, different projects, or projects in different organizations.

All communication happens by using private RFC 1918 IP addresses. VM instances in each peered network can communicate with one another without using external IP addresses, assuming firewall rules allow this.

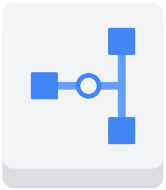
Peered networks share subnet routes. Optionally, both networks can be configured to share custom static and dynamic routes too. Network administration for each peered network is unchanged: network admins and security admins for one network do not automatically get those roles for the other network in the peering relationship. If two networks from different projects are peered, project owners, editors, and Compute Instance admins in one project do not automatically receive those roles in the project that contains the other network.

When using VPC peering, care should be taken on VPC limits. The per network VPC limits are no longer relevant, and peer network group limits are applied. As an example, the VPC limit per network for VM instances that can be connected to a VPC is 15,500. But the peer network group limit is also 15,500. So in the slide above, the total number of VM instances across the two VPC networks is 15,500, not 15,500 per network. For more details on VPC peering limits, see: https://cloud.google.com/vpc/docs/quota#vpc-peering.

Proprietary + Confidential

Cloud VPN securely connects your on-premises network to your Google Cloud VPC network

- Useful for low-volume data connections
- Classic VPN: 99.9% SLA
- High-availability (HA) VPN: 99.99% SLA
- Supports:
  - Site-to-site VPN
  - Static routes (Classic VPN only)
  - Dynamic routes (Cloud Router)
  - IKEv1 and IKEv2 ciphers



Cloud VPN

Google Cloud

Cloud VPN securely connects your on-premises network to your Google Cloud VPC network through an IPsec VPN tunnel. Traffic traveling between the two networks is encrypted by one VPN gateway, then decrypted by the other VPN gateway. This protects your data as it travels over the public internet, and that's why Cloud VPN is useful for low-volume data connections.

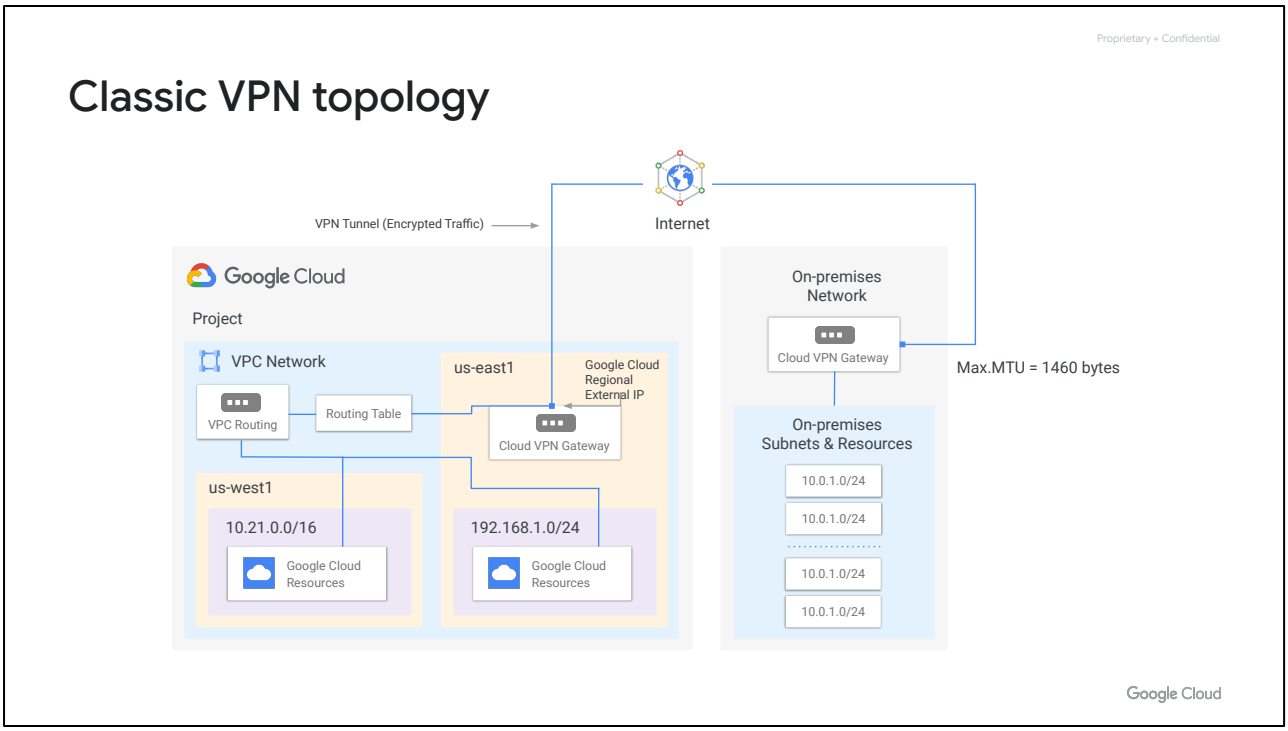
As a managed service, Cloud VPN provides an SLA of 99.9% monthly uptime for the Classic VPN configuration and 99.99% monthly uptime for the High-availability (HA) VPN configuration. The Classic VPN gateways have a single interface and a single external IP address whereas high-availability VPN gateways have two interfaces with two external IP addresses (one for each gateway). The choice of VPN gateway comes down to your SLA requirement and routing options.

Cloud VPN supports site-to-site VPN, static routes and dynamic routes using Cloud Router and IKEv1 and IKEv2 ciphers. However, static routes are only supported by Classic VPN.

Also, Cloud VPN doesn't support use cases where client computers need to “dial in” to a VPN using client VPN software.

For more information on the SLA and these features, refer to the documentation:

https://cloud.google.com/vpn/docs/concepts/overview



Let’s walk through an example of Cloud VPN. This diagram shows a Classic VPN connection between your VPC and on-premises network. Your VPC network has subnets in us-east1 and us-west1, with Google Cloud resources in each of those regions.

These resources are able to communicate using their internal IP addresses because routing within a network is automatically configured (assuming that firewall rules allow the communication).

Now, in order to connect to your on-premises network and its resources, you need to configure your Cloud VPN gateway, on-premises VPN gateway, and two VPN tunnels. The Cloud VPN gateway is a regional resource that uses a regional external IP address.

You on-premises VPN gateway can be a physical device in your data center or a physical or software-based VPN offering in another cloud provider's network. This VPN gateway also has an external IP address.

A VPN tunnel then connects your VPN gateways and serves as the virtual medium through which encrypted traffic is passed. In order to create a connection between two VPN gateways, you must establish two VPN tunnels. Each tunnel defines the

connection from the perspective of its gateway, and traffic can only pass when the pair of tunnels is established.

Now, one thing to remember when using Cloud VPN is that the maximum transmission unit (MTU) for your on-premises VPN gateway cannot be greater than 1460 bytes. This is because of the encryption and encapsulation of packets. For more information on this MTU consideration, refer to the documentation https://cloud.google.com/vpn/docs/concepts/mtu-considerations.

In addition to Classic VPN, Google Cloud also offers a second type of Cloud VPN gateway, HA VPN.

Proprietary + Confidential

HA VPN overview

- Provides 99.99% service availability.
- Google Cloud automatically chooses two external IP addresses.
  - Supports multiple tunnels
  - VPN tunnels connected to HA VPN gateways must use dynamic (BGP) routing
- Supports site-to-site VPN for different topologies/configuration scenarios:
  - An HA VPN gateway to peer VPN devices
  - An HA VPN gateway to an Amazon Web Services (AWS) virtual private gateway
  - Two HA VPN gateways connected to each other

Google Cloud

HA VPN is a high availability Cloud VPN solution that lets you securely connect your on-premises network to your Virtual Private Cloud (VPC) network through an IPsec VPN connection in a single region. HA VPN provides an SLA of 99.99% service availability. To guarantee a 99.99% availability SLA for HA VPN connections, you must properly configure two or four tunnels from your HA VPN gateway to your peer VPN gateway or to another HA VPN gateway.

When you create an HA VPN gateway, Google Cloud automatically chooses two external IP addresses, one for each of its fixed number of two interfaces. Each IP address is automatically chosen from a unique address pool to support high availability.

Each of the HA VPN gateway interfaces supports multiple tunnels. You can also create multiple HA VPN gateways. When you delete the HA VPN gateway, Google Cloud releases the IP addresses for reuse. You can configure an HA VPN gateway with only one active interface and one external IP address; however, this configuration does not provide a 99.99% service availability SLA. VPN tunnels connected to HA VPN gateways must use dynamic (BGP) routing. Depending on the way that you configure route priorities for HA VPN tunnels, you can create an active/active or active/passive routing configuration.

HA VPN supports site-to-site VPN in one of the following recommended topologies or configuration scenarios:

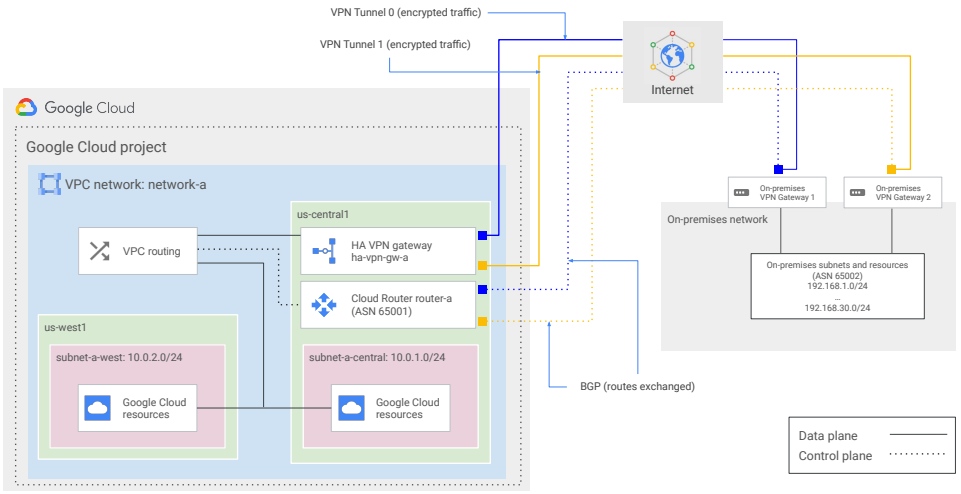
- An HA VPN gateway to peer VPN devices

- An HA VPN gateway to an Amazon Web Services (AWS) virtual private gateway
- Two HA VPN gateways connected to each other

Let's explore these configurations in a bit more detail.

Proprietary + Confidential

HA VPN to peer VPN gateway topology



Google Cloud

There are three typical peer gateway configurations for HA VPN. An HA VPN gateway to two separate peer VPN devices, each with its own IP address, an HA VPN gateway to one peer VPN device that uses two separate IP addresses and an HA VPN gateway to one peer VPN device that uses one IP address.

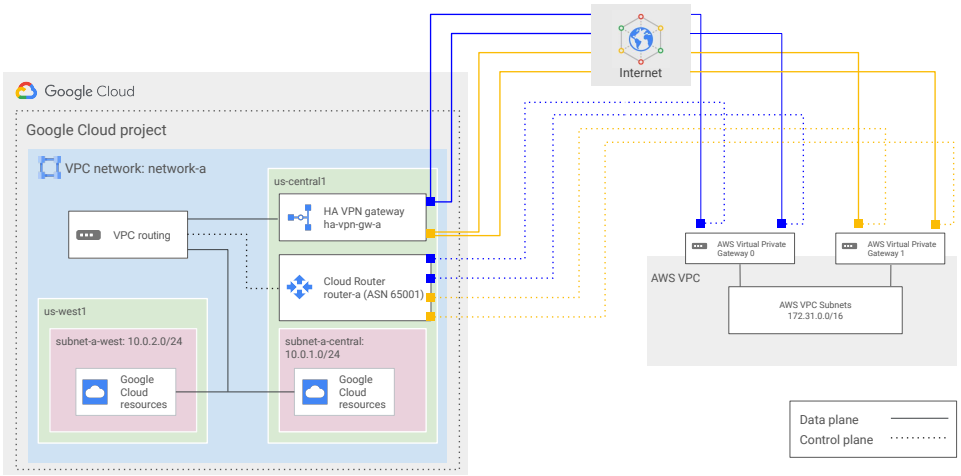
Let's walk through an example. In this topology, one HA VPN gateway connects to two peer devices. Each peer device has one interface and one external IP address. The HA VPN gateway uses two tunnels, one tunnel to each peer device. If your peer-side gateway is hardware-based, having a second peer-side gateway provides redundancy and failover on that side of the connection.

A second physical gateway lets you take one of the gateways offline for software upgrades or other scheduled maintenance. It also protects you if there is a failure in one of the devices.

In Google Cloud, the REDUNDANCY_TYPE for this configuration takes the value TWO_IPS_REDUNDANCY. The example shown here provides 99.99% availability.

Proprietary + Confidential

HA VPN to AWS peer gateway topology



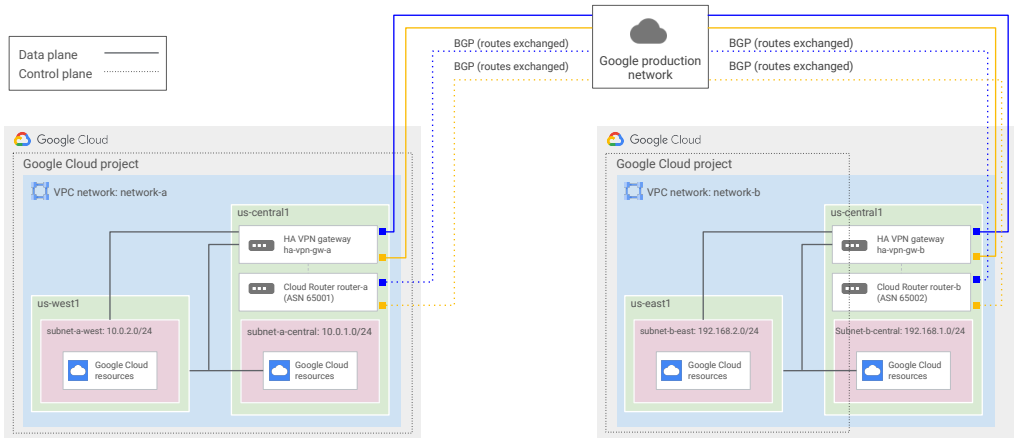
Google Cloud

When configuring an HA VPN external VPN gateway to Amazon Web Services (AWS), you can use either a transit gateway or a virtual private gateway. Only the transit gateway supports equal-cost multipath (ECMP) routing. When enabled, ECMP equally distributes traffic across active tunnels. Let's walk through an example.

In this topology, there are three major gateway components to set up for this configuration. An HA VPN gateway in Google Cloud with two interfaces, two AWS virtual private gateways, which connect to your HA VPN gateway, and an external VPN gateway resource in Google Cloud that represents your AWS virtual private gateway. This resource provides information to Google Cloud about your AWS gateway. The supported AWS configuration uses a total of four tunnels. Two tunnels from one AWS virtual private gateway to one interface of the HA VPN gateway, and two tunnels from the other AWS virtual private gateway to the other interface of the HA VPN gateway.

Proprietary + Confidential

HA VPN to peer VPN gateway topology



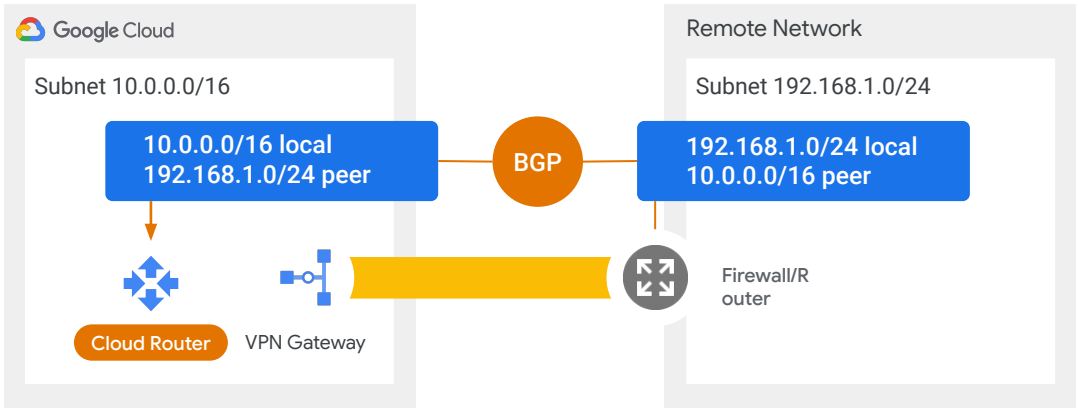
Google Cloud

You can connect two Google Cloud VPC networks together by using an HA VPN gateway in each network. The configuration shown provides 99.99% availability. From the perspective of each HA VPN gateway you create two tunnels. You connect `interface 0` on one HA VPN gateway to `interface 0` on the other HA VPN, and `interface 1` on one HA VPN gateway to `interface 1` on the other HA VPN.

For more information on HA VPN, refer to the documentation Cloud VPN topologies. For information on moving to HA VPN, see Moving to HA VPN.

Proprietary + Confidential

Cloud Router enables dynamic discovery of routes between connected networks



Google Cloud

Cloud Router enables dynamic route updates between a Cloud VPN and a non-Google network. Cloud Router eliminates the need to configure static routes and automatically discovers network topology changes. It peers with the peer network VPN gateway or router and exchanges topology information using BGP. Any topology changes are automatically propagated in both directions.

Static routes could be configured on Cloud Router, but these must be manually maintained because topology changes and traffic cannot be rerouted when link failures occur.

Proprietary + Confidential

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.

Google Cloud

Cloud Interconnect provides low latency, highly available connections that enable you to reliably transfer data between on-premises and Virtual Private Cloud networks. Cloud Interconnect connections provide RFC 1918 communication, meaning internal (private) IP addresses are directly accessible from both networks.

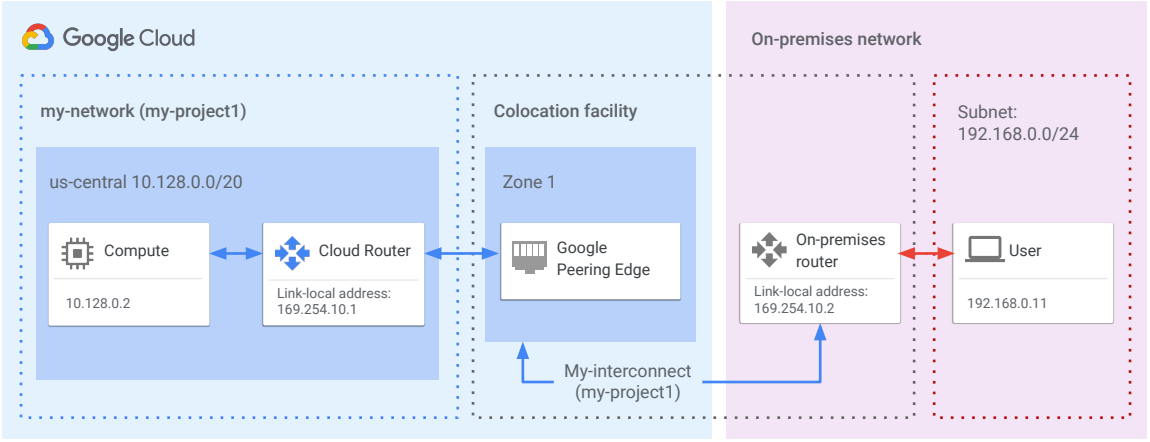
Two options are available for extending on-premises networks:

1. Dedicated Interconnect, which provides a direct physical connection between an on-premises network and Google's network.
2. Partner Interconnect, which provides connectivity between on-premises and Google Cloud VPC networks through a supported service provider.

Traffic using Cloud Interconnect does not travel the public internet, which means fewer network hops and with fewer points of failure. The bandwidth can be scaled to meet your requirements incrementally. The scaling units depend on the type of interconnect and are discussed on the next slides.

Proprietary + Confidential

Dedicated Interconnect provides direct physical connections



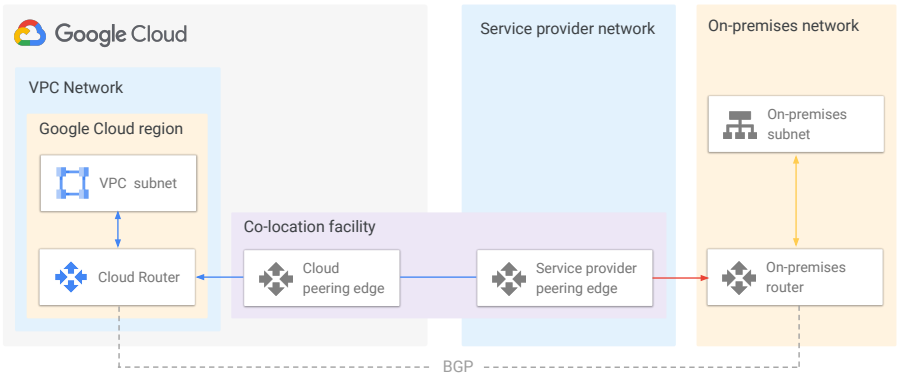
Google Cloud

For high bandwidth needs, Dedicated Interconnect is often a cost-effective solution. It requires the provisioning of a cross connect, dedicated internet connection between the Google network and your own router in a colocation facility. The diagram on the slide above shows a basic setup. A cross connect is provisioned between the Google network and the on-premises router in a common colocation facility. To exchange routes, a BGP session is configured over the interconnect between the Cloud Router and on-premises router. Then, traffic from the on-premises network can reach the VPC network, and vice versa.

A single interconnect can be a single 10-Gb link, a single 100-Gb link, or a link bundle (up to 8 x 10Gbps or 2 x 100Gbps), connected to a single Cloud Router.

Proprietary + Confidential

Partner Interconnect provides connectivity through a supported service provider



Google Cloud

The use case is for those that have high bandwidth needs but cannot physically meet Google's network in a colocation facility. In this scenario, it is possible to use Partner Interconnect to connect via one of a variety of service providers that connect directly to Google. The connection capacities for each interconnect attachment (VLAN) supported are from 50 Mbps to 10 Gbps with a maximum capacity of 8 x 10 Gbps VLANs.

Proprietary + Confidential

Activity 9

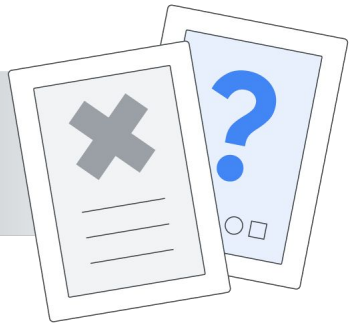
25 min

Diagramming your network

Refer to your Design and Process Workbook.

- Draw a diagram that depicts your network requirements.

Proprietary + Confidential



Quiz

Proprietary + Confidential

Question #1

Question

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. Network Load Balancer with SSL configured
B. Application Load Balancer with SSL configured
C. Application Load Balancer with SSL configured and the CDN enabled
D. Network Load Balancer with SSL configured and the CDN enabled

Google Cloud

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. Network Load Balancer with SSL configured
B. Application Load Balancer with SSL configured
C. Application Load Balancer with SSL configured and the CDN enabled
D. Network Load Balancer with SSL configured and the CDN enabled

Proprietary + Confidential

Question #1

Answer

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. Network Load Balancer with SSL configured

B. Application Load Balancer with SSL configured

C. Application Load Balancer with SSL configured and the CDN enabled 

D. Network Load Balancer with SSL configured and the CDN enabled

Google Cloud

A. This answer is not correct. Network Load Balancers are not intended for HTTP(S) traffic. In addition, the static content suggests the use of CDN, which is not supported with TCP load balancers.

B. This answer is not correct. An Application Load Balancer with SSL configured is a good fit but not the best because CDN is not enabled, which would help with the large amount of static content.

C. This answer is correct. The traffic is HTTP(S). A global external Application Load Balancer with CDN enabled will help performance and cost.

D. This answer is not correct. The traffic type is not UDP.

Proprietary + Confidential

Question #2

Question

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

Google Cloud

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

Proprietary + Confidential

Question #2

Answer

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

Google Cloud

A. This answer is not correct. VPN is an option for low data volumes.

B. This answer is not correct. HTTPS will not be able to provide bandwidth; there may be internet costs, and the traffic will be moved over the public internet.

C. This answer is correct. Cloud Interconnect provides high bandwidth and low latency. It does need encryption at the application level.

D. This answer is not correct. Peering is for connectivity to services such as Google Workspace.

Proprietary + Confidential

Question #3

Question

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

Google Cloud

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

Proprietary + Confidential

Question #3

Answer

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** 

Google Cloud

A, B, and C are not correct. These options are all for connecting external networks to a VPC.

D. This answer is correct. VPC peering allows connectivity across two VPC networks regardless of whether they belong to the same project or same organization.

Proprietary + Confidential

Question #4

Question

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

Google Cloud

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

Proprietary + Confidential

Question #4

Answer

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

Google Cloud

A. This answer is not correct. VPN is the correct connectivity choice but does not offer HA.

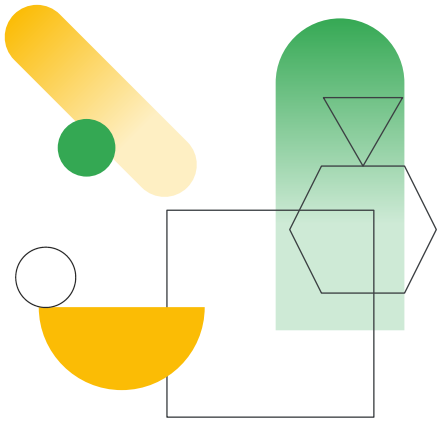
B. This is the correct choice. This offers a secure extremely reliable connection and is more cost-effective than Cloud Interconnect.

C. This answer is not correct. Cloud Interconnect is for high data volumes.

D. This answer is not correct. VPC peering is for interconnection two VPC networks.

Proprietary + Confidential

Review: Google Cloud and Hybrid Network Architecture



Google Cloud

In this module, you learned about Google Cloud networking and how to design networks that meet your application's security, performance, reliability, and scalability requirements.

We also covered the different options to connect networks using peering, VPN and Cloud Interconnect.

Proprietary + Confidential

More resources

Cloud networking products

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

Google Cloud Hybrid Connectivity

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

Google Cloud

The links provide access to some useful resources on Google Cloud networking.


Google Cloud