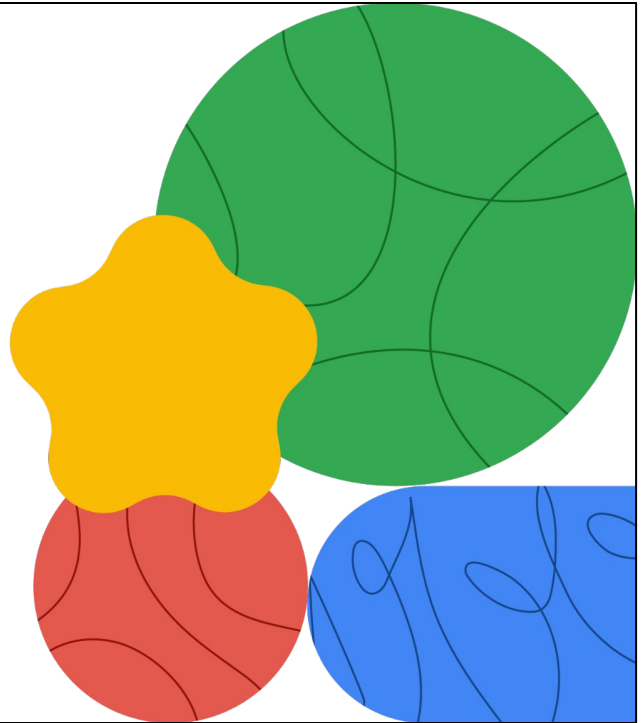





# Networking in Google Cloud


Cloud VPN



Welcome to Cloud VPN module.



# Today's agenda



- 01 [Cloud VPN Overview](#)
- 02 [HA VPN Topologies](#)
- 03 [Influence best path selection](#)
- 04 [Lab: Configuring Google Cloud HA VPN](#)
- 05 [Quiz](#)

Let's explore Cloud VPN: a service that enables secure, encrypted connections between your on-premises networks and Google Cloud. We'll explore what Cloud VPN is, how it works, and the various use cases it supports.

## Cloud VPN securely extends your peer network to your VPC

- Cloud VPN securely connects your peer network to a Virtual Private Cloud (VPC) network through IPsec tunnels.
- Use Cloud VPN when you:
  - Don't need the connection speed of Cloud Interconnect.
  - Must encrypt data in transit.
  - Prefer the economics of an IPsec tunnel over the internet.
  - When your network infrastructure cannot support dedicated fiber connections to Google Cloud.
  - Want to selectively advertise routes between VPC networks.

Google Cloud

Use Cloud VPN when you don't need the connection speed of Cloud Interconnect. Cloud VPN is cheaper and easier to set up than Cloud Interconnect. Thus, Cloud VPN is useful for low-volume or low-bandwidth data connections. When you prefer the economics of an IPsec tunnel over the internet and when your network infrastructure cannot support dedicated fiber connections to Google Cloud, choose Cloud VPN.

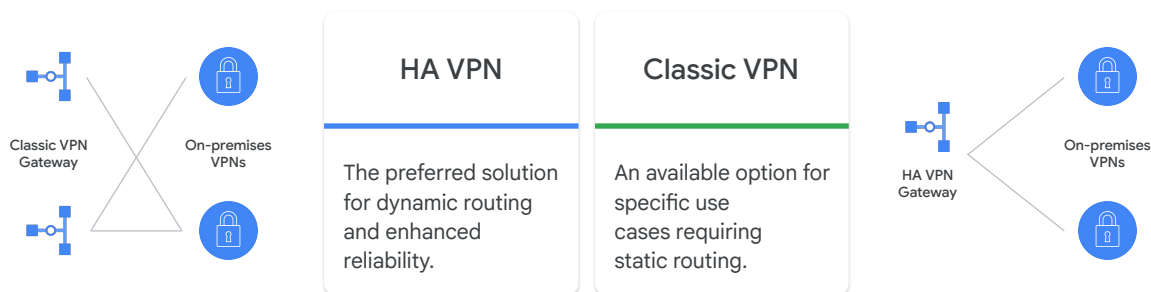
You also use Cloud VPN to encrypt data in transit.

With Cloud VPN, you can selectively advertise routes between VPC networks. In contrast, when you set up peering between two VPC networks, all the subnet routes are advertised.

Cloud VPN securely connects your peer network to your Virtual Private Cloud (VPC) network through IPsec tunnels. The data is encrypted as it passes through the tunnels. The traffic traveling between the two networks is encrypted by one VPN gateway and then decrypted by the other VPN gateway. This action protects your data as it travels over the internet.

# HA VPN and Classic VPN

There are two types of Cloud VPN – HA (high availability) VPN and Classic VPN.



There are two types of Cloud VPN: HA (high availability) VPN and Classic VPN. Google Cloud VPN primarily offers HA VPN (High Availability), the recommended solution for dynamic routing and enhanced reliability. Classic VPN is available for specific use cases requiring static routing.

Next, let's discuss both Cloud VPN products.

## Use case: High availability connection between on-prem and Google Cloud

### Requirements

01 Eliminate connectivity issues

02 Enhance network reliability

03 Improve network performance



HA VPN is the pragmatic choice.



Jack is responsible for optimizing the company's cloud infrastructure, and he's currently focused on updating their networking strategy within Google Cloud. Cymbal Corporation has been relying on Classic VPNs to connect their on-premises data center to Google Cloud, but they've experienced occasional connectivity issues. They are now looking to enhance their network reliability and performance.

## Use case: High availability connection between on-prem and Google Cloud

HA VPN provides

01 High availability

02 A secure and simplified connection

03 Automatic failover capabilities




HA VPN is the pragmatic choice.




Google Cloud

Considering the critical nature of Cymbal's operations, the switch to High Availability (HA) VPNs in Google Cloud will be suitable. The company's applications demand a highly available, secure connection to cloud services and a simplified setup. HA VPNs could provide the necessary redundancy and failover capabilities to ensure uninterrupted connectivity. The advantages of HA VPNs over Classic VPNs include improved availability, automatic failover, and better performance. The switch to HA VPN will meet the networking requirements and contribute to a more resilient and efficient infrastructure.



# Today's agenda



- |    |                                      |
|----|--------------------------------------|
| 01 | Cloud VPN Overview                   |
| 02 | <b>HA VPN Topologies</b>             |
| 03 | Influence best path selection        |
| 04 | Lab: Configuring Google Cloud HA VPN |
| 05 | Quiz                                 |

Let us next cover some of the HA VPN Topologies.

# HA VPN topologies

HA VPN supports site-to-site VPN for different configuration topologies:

- 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.
- HA VPN to Compute Engine VM instances.

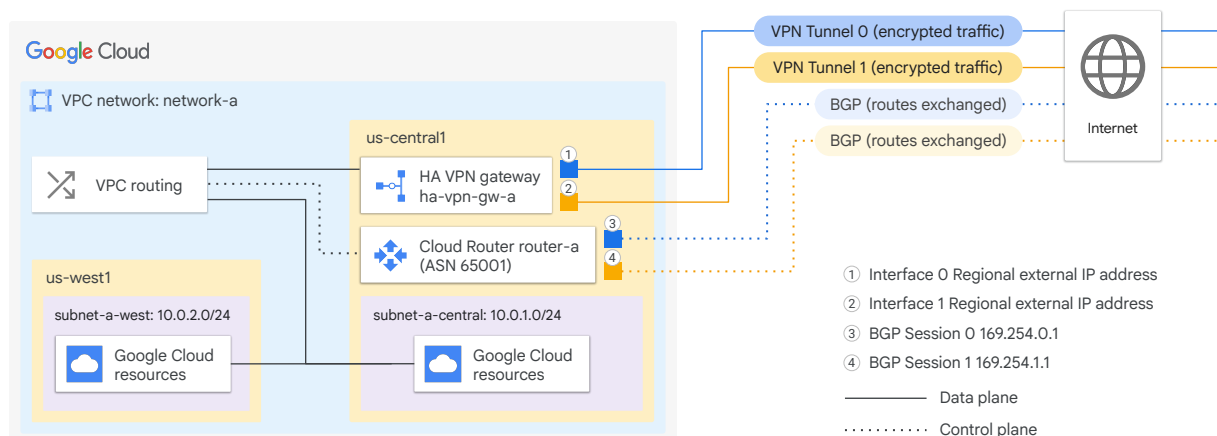
HA VPN supports site-to-site VPN for different configuration topologies. These topologies are:

- 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.
- HA VPN to Compute Engine VM instances.

Let's look at each of these topologies.



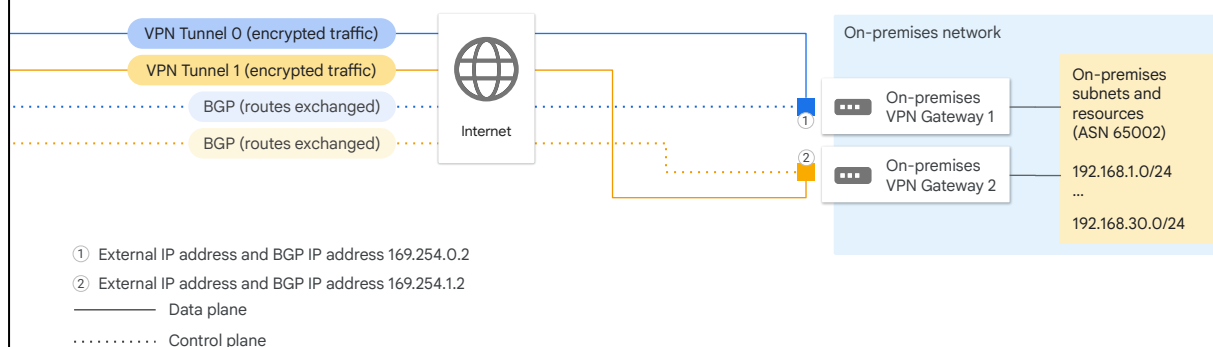
# HA VPN to VPN Peer gateway: Google Cloud to internet



HA VPN has three typical peer gateway configurations: an HA VPN gateway to two separate peer VPN devices, each with its own IP address; one peer VPN device that uses two separate IP addresses; and 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. Here, we see the HA VPN gateway and two VPN tunnels that connect to the peer devices. Next, we'll look at the peer devices in the on-premises network.

## HA VPN to VPN Peer gateway: Internet to the on-premises network

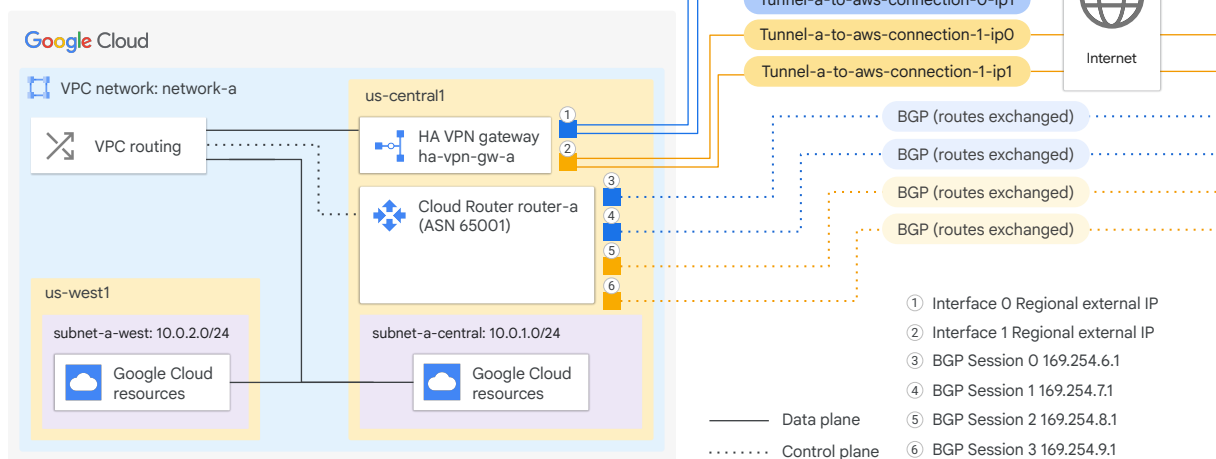


Here, you can see the on-premises network and the tunnels that come from the HA VPN gateway.

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.

In Google Cloud, the REDUNDANCY\_TYPE for this configuration takes the value TWO\_IPS\_REDUNDANCY. The example shown here provides 99.99% availability.

# HA VPN to the internet

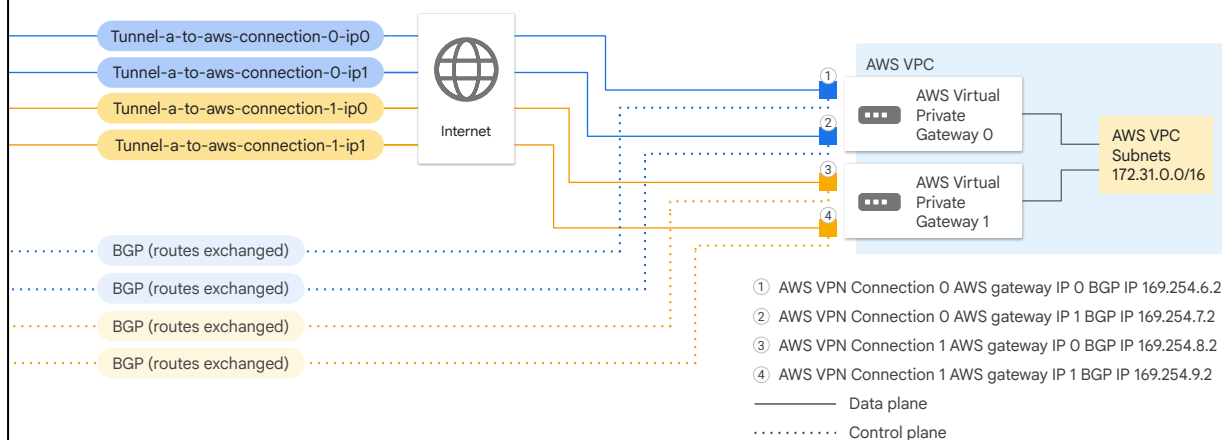


When configuring an HA VPN external VPN gateway to Amazon Web Services (AWS), you can use either a transit gateway or a virtual private gateway. Only the transit gateway supports equal-cost multipath (ECMP) routing. When enabled, ECMP distributes traffic equally across active tunnels. Let's walk through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

In this topology, you configure three major gateway components: an HA VPN gateway in Google Cloud with two interfaces; two AWS virtual private gateways that 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.

Here you can see the Google Cloud components and their connections through the internet to the AWS components.

# HA VPN to AWS peer gateway topology: Internet to AWS



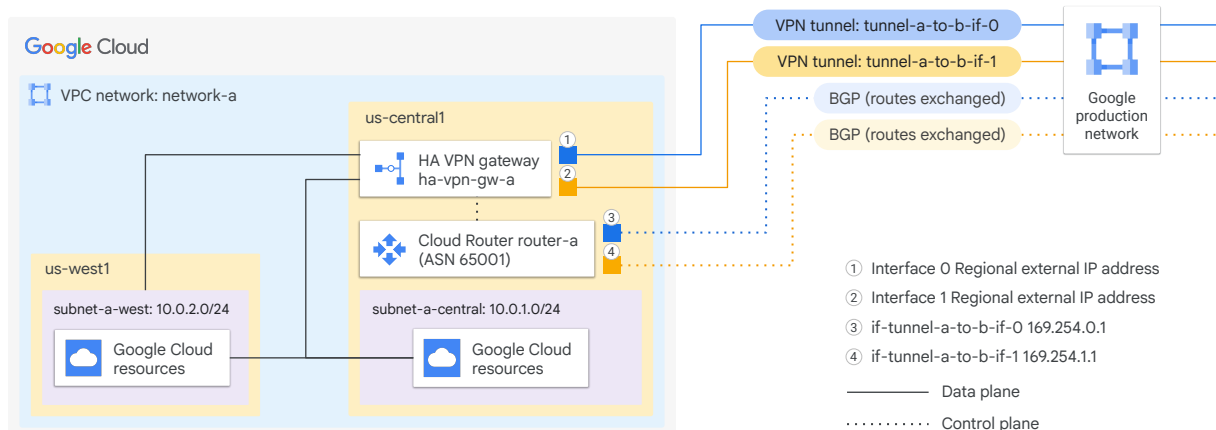
Google Cloud

The AWS components in this topology are shown here, along with their connections to the HA VPN Gateway and Cloud Router in Google Cloud.

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.

For information regarding using HA VPN to connect to a Microsoft Azure gateway, see [Using Cloud VPN With Microsoft Azure\(TM\) VPN Gateway](#).

## HA VPN to peer VPN gateway topology: Left side



Google Cloud

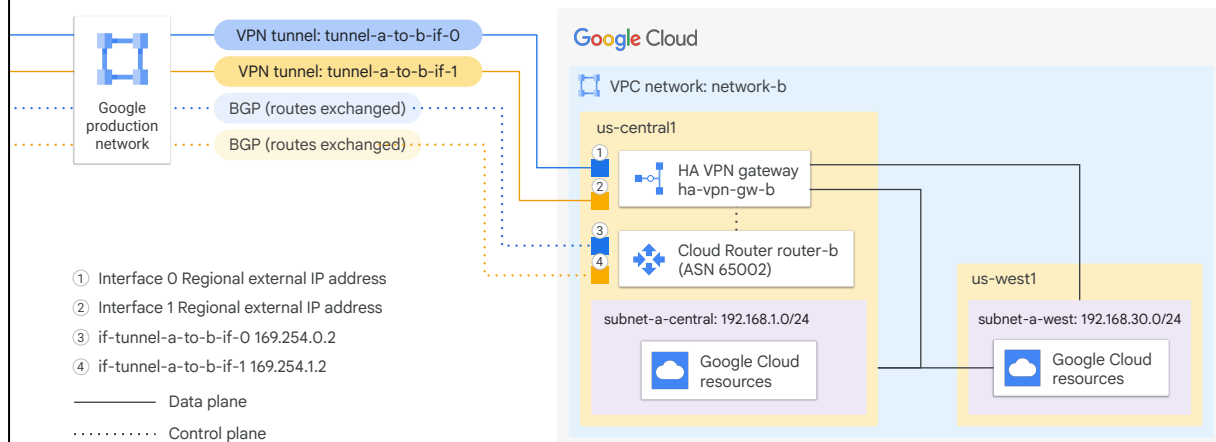
You can connect two Google Cloud VPC networks together by using an HA VPN gateway in each network. Let's walk through a sample topology. Like the other two samples that you've seen, it's divided into two parts.

Here you see a Google Cloud project with a VPC network called network-a. There's an HA VPN gateway and a Cloud Router instance that connects to VPC network-b, which is not visible here.

Each HA VPN gateway has two interfaces, shown in the graphic. You connect interface 0 on the HA VPN gateway in network\_a to interface 0 on the HA VPN in network\_b. You do the same for the interface 1, connecting from the HA VPN gateway in network-a to the HA VPN gateway in network-b.

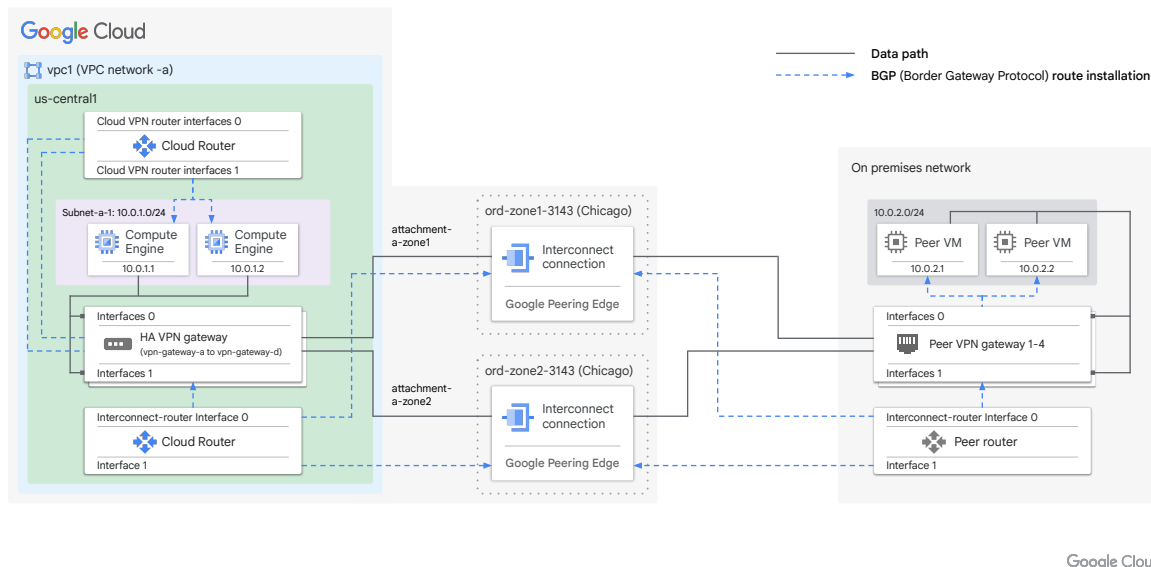
Next, let's look at network-b.

## HA VPN to peer VPN gateway topology: Right side



Here you see the Google Cloud project that contains network-b. You see all the connections from the HA VPN gateway that link to network-a.

# HA VPN over Cloud Interconnect deployment architecture



Google Cloud

When you deploy HA VPN over Cloud Interconnect, you create two operational tiers:

- The Cloud Interconnect tier, which includes the VLAN attachments and the Cloud Router for Cloud Interconnect.
- The HA VPN tier, which includes the HA VPN gateways and tunnels and the Cloud Router for HA VPN.

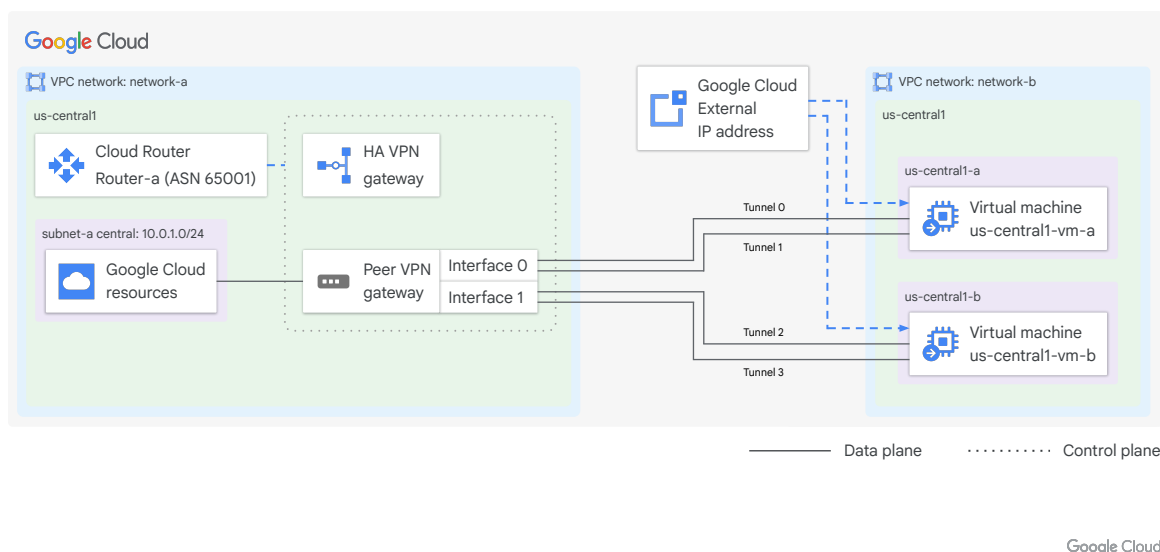
Each tier requires its own Cloud Router:

- The Cloud Router for Cloud Interconnect is used exclusively to exchange VPN gateway prefixes between the VLAN attachments. This Cloud Router is used only by the VLAN attachments of the Cloud Interconnect tier. It cannot be used in the HA VPN tier.
- The Cloud Router for HA VPN exchanges prefixes between your VPC network and your on-premises network. You configure the Cloud Router for HA VPN and its BGP sessions in the same way you would for a regular HA VPN deployment.

You build the HA VPN tier on top of the Cloud Interconnect tier. Therefore, the HA VPN tier requires that the Cloud Interconnect tier, based on either Dedicated Interconnect or Partner Interconnect, is properly configured and operational.

The diagram shown here depicts an HA VPN over Cloud Interconnect deployment. To learn more about configuration, see [Configure HA VPN over Cloud Interconnect](#).

# HA VPN to Compute Engine VM instances in multiple zones



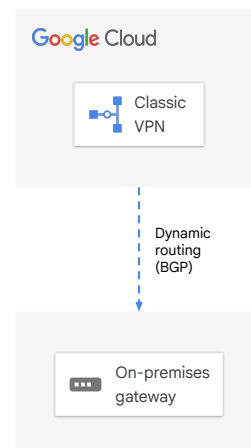
High Availability (HA) VPN allows you to establish a secure connection between an HA VPN gateway and Compute Engine virtual machines (VMs) functioning as network virtual appliances running IPsec VPN. The VM instance(s) can be deployed within a single zone or distributed across multiple zones. This configuration supports connecting an HA VPN gateway to two Compute Engine VMs, each residing in separate VPCs and zones with unique external IP addresses. The VMs act as VPN peer devices.

In the illustrated example, the HA VPN gateway is situated in a Virtual Private Cloud network named "network-a," while the two VMs are located in "network-b." Both VPC networks are within the "us-central1" region. The HA VPN gateway in "network-a" is configured to use the external IP addresses of each VM in "network-b." It's also possible to have the HA VPN gateway and VMs in different regions. This topology is recommended for enhanced availability.



# HA VPN recommendations

- HA VPN
  - Provides 99.99% service availability (instead of 99.9% for Classic VPN).
  - Supports multiple VPN tunnels.
- Google Cloud automatically chooses two external IP addresses.
- VPN tunnels connected to HA VPN gateways must use dynamic (BGP) routing.
- We recommend an active/active configuration for an increased throughput.



HA VPN also provides 99.99% service availability.

Use HA VPN for BGP routing and to support multiple tunnels. When you create an HA VPN gateway, Google Cloud automatically chooses two external IPv4 addresses, one for each of its fixed number of two interfaces. Each IPv4 address is automatically chosen from a unique address pool to support high availability.

VPN tunnels connected to HA VPN gateways must use dynamic (BGP) routing.

Use an active/passive configuration for a consistent bandwidth experience.

Active/active configurations may offer a less consistent experience. Unless combined traffic for both tunnels is within single tunnel capacity, failure can cause the available bandwidth to be cut in half.

## Let's ask Gemini



How can I connect a VPC network in Google Cloud to an on-premises private network?



There are two ways to connect a VPC in Google Cloud to an on-premises private network:


1. Cloud VPN uses encrypted tunnels to connect your VPC network to your on-premises network.
2. Cloud Interconnect uses a physical connection to connect your VPC network to your on-premises network.

\*Gemini responses may vary


You can also use some useful prompts focusing specifically on how Gemini-like AI could assist with Cloud VPN tasks and analysis:

One such example is "How can I connect a VPC network in Google Cloud to an on-premises private network?"

Gemini will provide the two options available on Google Cloud, Cloud VPN and Cloud Interconnect.



# Today's agenda



- 01 Cloud VPN Overview
- 02 HA VPN Topologies
- 03 [Influence best path selection](#)
- 04 Lab: Configuring Google Cloud HA VPN
- 05 Quiz

Let us next explore how to influence the best path selection.

## Influencing the best path selection by setting a base priority

- When a Cloud Router advertises prefixes to a BGP peer, it advertises a route priority for each prefix.
- You can change the base priority on each Cloud VPN tunnel or VLAN attachment.
- If your VPC network uses global dynamic routing mode, the base priority is added to the region-to-region cost to calculate the value of the BGP multi-exit discriminator(MED) attribute.

When a Cloud Router advertises prefixes to a BGP peer, it includes a priority for each prefix in the advertisement. The advertisement is the BGP message, and it includes a route priority. The route priority is stored in the BGP MED attribute, which influences route selection.

You can change the advertised route priority value on each Cloud VPN tunnel or VLAN attachment. This value is then assigned to the BGP multi-exit discriminator (MED) attribute. The MED value affects the BGP best path selection. By changing the advertised route priority, you influence the best path selection. For more information about other factors that influence the best path selection, see the BGP protocol standard on the [IETF.org](https://www.ietf.org) website or a networking tutorial.

The advertised route priority value applies to all prefixes advertised by the BGP session associated with the Cloud VPN tunnel or VLAN attachment.

## Setting a base priority

01

Base priorities are whole numbers from 0 to 65535.

02

The highest possible base priority is 0.

03

The default base priority is 100.

04

If you don't specify a base priority, the default priority is used.

Base priorities are whole numbers from 0 to 65535. The highest possible base priority is 0. In other words, a lower number indicates a higher priority.

The default base priority is 100. If you don't specify a base priority, the default priority is used.

Next, let's talk about the region-to-region costs that can be added to the base priority to set the MED attribute on the BGP session.

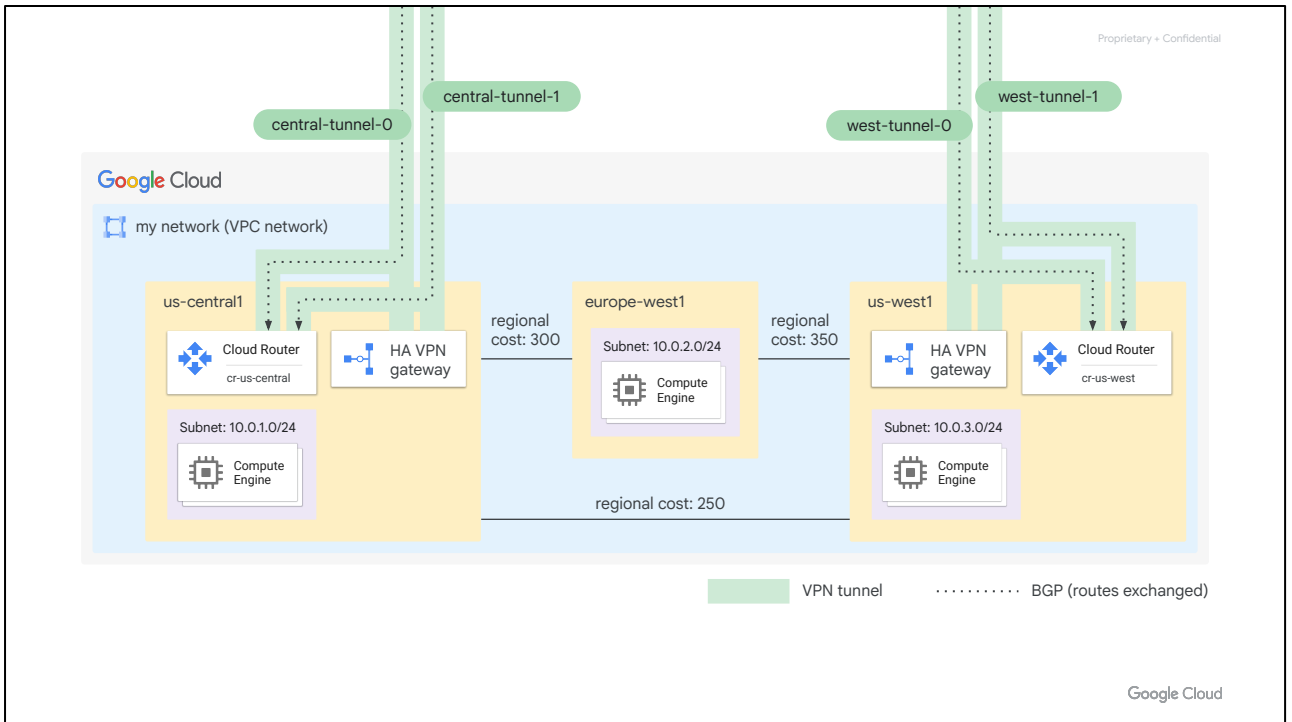
## Region-to-region costs

- This cost only applies when the VPC is in global dynamic routing mode.
- Region-to-region costs are from 201 through 9999, inclusive.
- The value depends on the distance, latency, and other factors between two regions.
- Google generates the region-to-region cost values, and you can't modify them.




This cost only applies when the VPC is in global dynamic routing mode. Region-to-region costs are from 201 through 9999. The value depends on the distance, latency, and other factors between two regions. Google generates the region-to-region cost values, and you can't modify them.

Next, let's look at a sample topology to see how this works.




In the graphic, you see an example of region-to-region costs that Google calculates. Regions that are closer have a lower region cost for traffic that flows between them. For example, the regional cost between us-central1 and europe-west1 is lower than the cost between europe-west1 and us-west1.

For more information, see [Advertised prefixes and priorities](#) in the Google Cloud documentation.



# Today's agenda



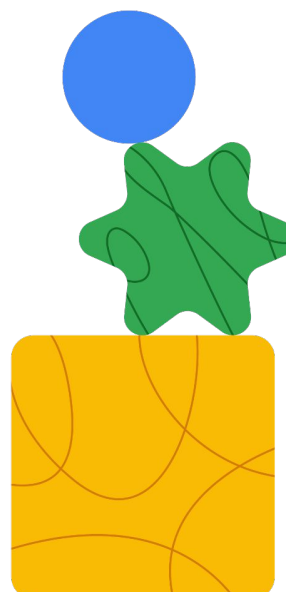
- 01 Cloud VPN Overview
- 02 HA VPN Topologies
- 03 Influence best path selection
- 04 [Lab: Configuring Google Cloud HA VPN](#)
- 05 Quiz

Let us next explore a lab on how to configure a HA VPN.




## Lab intro

Configuring Google Cloud HA VPN




Google Cloud

In this lab you create a global VPC called `vpc-demo`, with two custom subnets in REGION 2 and REGION 1. In this VPC, you add a Compute Engine instance in each region. You then create a second VPC called `on-prem` to simulate a customer's on-premises data center. In this second VPC, you add a subnet in region REGION 1 and a Compute Engine instance running in this region. Finally, you add an HA VPN and a cloud router in each VPC and run two tunnels from each HA VPN gateway before testing the configuration to verify the 99.99% SLA.



# Today's agenda



- 01 Cloud VPN Overview
- 02 HA VPN Topologies
- 03 Influence best path selection
- 04 Lab: Configuring Google Cloud HA VPN
- 05 [Quiz](#)

# Quiz | Question 1

## Question

What is the purpose of a Cloud Router, and why is that important?

- A. To create and manage virtual private networks (VPNs) between on-premises networks and Google Cloud.
- B. To load balance traffic across multiple Google Cloud regions and zones.
- C. To dynamically exchange routing information using BGP between Google Cloud VPCs and other networks.
- D. To filter and restrict traffic based on predefined security rules.

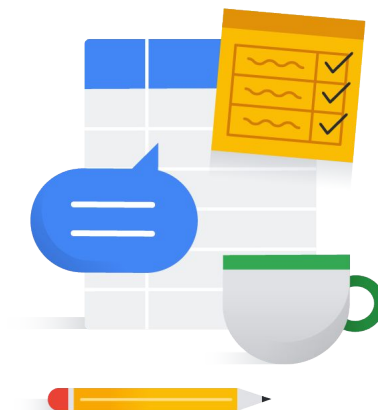
## Quiz | Question 2

### Question

In Network Connectivity Center, what are the two main types of spokes that can be connected to a hub?

- A. VPC spokes and Global spokes
- B. VPC spokes and Hybrid spokes
- C. Global spokes and Hybrid spokes
- D. Regional spokes and Global spokes

## Debrief



In this module, you learned about Cloud VPN and how it can be useful for lower bandwidth needs and to implement encrypted connections. In a lab, you explored the process of setting up Network Connectivity Center as a transit hub to route traffic between two non-Google networks using Google's backbone network.

At the end of the module, you learned how Network Connectivity Center to centrally manages hybrid, multi-site connectivity using a hub-and-spoke architecture.



THANK YOU

