

[Cloud VPN](https://cloud.google.com/vpn/) (<https://cloud.google.com/vpn/>)

[Documentation](https://cloud.google.com/vpn/docs/) (<https://cloud.google.com/vpn/docs/>) [Guides](#)

# Creating Google Cloud to Google Cloud HA VPN gateways

This page describes how to connect two Virtual Private Cloud networks together using a HA VPN gateway configuration. You can connect two existing VPC networks together as long as the primary and secondary subnet IP address ranges in each network don't overlap.

For a diagram of this topology, see [the Topologies page](https://cloud.google.com/vpn/docs/concepts/topologies#2-gcp-gateways) (<https://cloud.google.com/vpn/docs/concepts/topologies#2-gcp-gateways>).

For more information on how to choose a VPN type, see the [Choosing a VPN Option](https://cloud.google.com/vpn/docs/how-to/choosing-a-vpn) (<https://cloud.google.com/vpn/docs/how-to/choosing-a-vpn>).

## Requirements

Make sure that you meet the following requirements when creating this configuration to ensure that you receive a 99.99% SLA:

- Place one HA VPN gateway in each [VPC network](https://cloud.google.com/vpc/docs/vpc) (<https://cloud.google.com/vpc/docs/vpc>).
- Place both HA VPN gateways in the same [Google Cloud region](https://cloud.google.com/compute/docs/regions-zones) (<https://cloud.google.com/compute/docs/regions-zones>).
- Configure a tunnel on each interface of each gateway.
- Match gateway interfaces as described in the statement below.

**Important:** To assure 99.99% availability for VPC to VPC gateways, a tunnel on Interface 0 on the first gateway must connect to Interface 0 on the second gateway and a tunnel on Interface 1 on the first gateway

must connect to Interface 1 on the second gateway.

Although it is also possible to connect two VPC networks together using a single tunnel between HA VPN gateways or by using Classic VPN gateways, this type of configuration is not considered highly available and does not meet the HA SLA of 99.99% availability.

**Caution:** If one or both of the VPN gateways are Classic VPN gateways, your configuration does not meet the 99.99% SLA.

## Permissions requirements

Since HA VPN gateways don't always belong to you or your Google Cloud organization, consider the following permissions requirements when you create an HA VPN gateway, or connect to one owned by someone else:

- If you own the project where you create a HA VPN gateway, configure the [recommended permissions](#) (#permissions) on it.
- If you want to connect to an HA VPN gateway that resides in a Google Cloud organization or project that you don't own, you need to request the `compute.vpnGateways.use` permission from the owner.

## Before you begin

- Review information about how [dynamic routing](#) (<https://cloud.google.com/vpn/docs/concepts/choosing-networks-routing#dynamic-routing>) works in Google Cloud.
- Make sure your [peer](#) (<https://cloud.google.com/vpn/docs/concepts/overview#peer-definition>) VPN gateway supports BGP.

Setting up the following items in Google Cloud makes it easier to configure Cloud VPN:

1. [Sign in](#) (<https://accounts.google.com/Login>) to your Google Account.

If you don't already have one, [sign up for a new account](#) (<https://accounts.google.com/SignUp>).

2. In the Cloud Console, on the project selector page, select or create a Google Cloud project.

★ **Note:** If you don't plan to keep the resources that you create in this procedure, create a project instead of selecting an existing project. After you finish these steps, you can delete the project, removing all resources associated with the project.

[GO TO THE PROJECT SELECTOR PAGE \(HTTPS://CONSOLE.CLOUD.GOOGLE.COM/PROJECTSELECT\)](https://console.cloud.google.com/projectselect)

3. Make sure that billing is enabled for your Google Cloud project. [Learn how to confirm billing is enabled for your project](https://cloud.google.com/billing/docs/how-to/modify-project) (https://cloud.google.com/billing/docs/how-to/modify-project).
4. [Install and initialize the Cloud SDK](https://cloud.google.com/sdk/docs/) (https://cloud.google.com/sdk/docs/).
4. If you are using `gcloud` commands, set your project ID with the following command. The `gcloud` instructions on this page assume that you have set your project ID before issuing commands.

```
gcloud config set project project-id
```



You can also view a project ID that has already been set:

```
gcloud config list --format='text(core.project)'
```



## ⌵ Permissions required for this task

To perform this task, you must have been granted the following permissions **OR** the following IAM roles.

### Permissions

- `compute.vpnGateways.get`
- `compute.vpnGateways.list`
- `compute.externalVpnGateways.get`
- `compute.externalVpnGateways.list`
- `compute.vpnGateways.create`
- `compute.vpnGateways.delete`
- `compute.vpnGateways.get`
- `compute.vpnGateways.list`

- `compute.vpnGateways.use`
- `compute.vpnGateways.setLabels`
- `compute.externalVpnGateways.create`
- `compute.externalVpnGateways.delete`
- `compute.externalVpnGateways.get`
- `compute.externalVpnGateways.list`
- `compute.externalVpnGateways.use`
- `compute.externalVpnGateways.setLabels`

## Roles

- `roles/compute.networkAdmin`

## Creating a custom Virtual Private Cloud network and subnet

**Note:** The examples in this document use two VPC networks. Each network has one subnet in one region and another subnet in another region. However, your requirements might be different. For an example, refer to [the Google Cloud-to-Google Cloud HA VPN topology](https://cloud.google.com/vpn/docs/concepts/topologies#2-gcp-gateways) (<https://cloud.google.com/vpn/docs/concepts/topologies#2-gcp-gateways>).

Before creating an HA VPN gateway and tunnel pair, you must create a Virtual Private Cloud network and at least one subnet in the region where the HA VPN gateway will reside.

- To create a custom mode (recommended) VPC network, see [Creating a custom mode network](https://cloud.google.com/vpc/docs/using-vpc#create-custom-network) (<https://cloud.google.com/vpc/docs/using-vpc#create-custom-network>).
- To create subnets, see [Working with subnets](https://cloud.google.com/vpc/docs/using-vpc#subnet-rules) (<https://cloud.google.com/vpc/docs/using-vpc#subnet-rules>).

The examples in this document also use [VPC global dynamic routing mode](https://cloud.google.com/vpc/docs/vpc#routing_for_hybrid_networks) ([https://cloud.google.com/vpc/docs/vpc#routing\\_for\\_hybrid\\_networks](https://cloud.google.com/vpc/docs/vpc#routing_for_hybrid_networks)), which behaves in the following way:

- All instances of Cloud Router apply the "to on-premises" routes they learn to all subnets of the VPC network.
- Routes to all subnets in the VPC network are shared with on-premises routers.

For reference, this document creates a HA VPN gateway in each of two different VPC networks:

**network-1** contains the following subnets:

- A subnet named **subnet-name-1** in **region-1** that uses the IP range **range-1**
- A subnet named **subnet-name-2** in **region-2** that uses the IP range **range-2**

**network-2** contains the following subnets:

- A subnet named **subnet-name-3** in **region-1** that uses the IP range **range-3**
- A subnet named **subnet-name-4** in **region-3** that uses the IP range **range-4**.

## Creating only an HA VPN gateway

**Note:** It can help to have two console or terminal sessions open when configuring two HA VPN gateways that connect to each other.

You can create a HA VPN gateway without gateway, tunnels, a peer VPN gateway resource, or BGP sessions and configure these additional resources later.

You must [create these resources](https://cloud.google.com/vpn/docs/how-to) (https://cloud.google.com/vpn/docs/how-to) before your gateway can become operational.

CONSOLE

G-CLOUD

API

1. Go to the VPN page in the Google Cloud Console.

**GO TO THE VPN PAGE** ([HTTPS://CONSOLE.CLOUD.GOOGLE.COM/HYBRID/VPN/LIST&TAB=GATEW](https://console.cloud.google.com/hybrid/vpn/list&tab=gatew))

- a. If you are creating a gateway for the first time, select the **Create VPN connection** button.
- b. If you already have VPN gateways, select the gray **Create VPN gateways** button.

2. Specify a **VPN gateway name**

3. Select a **VPC network** for your gateway.

4. Select a **region** for your gateway.

5. Click **Create**.

6. On the **VPN** status screen, you can view the details for your new gateway.

# Creating two fully configured HA VPN gateways that connect to each other

**Note:** It can help to have two Cloud Console or terminal sessions open when configuring two HA VPN gateways that connect to each other.

Follow the instructions in this section to create a HA VPN gateway, tunnels, a peer VPN gateway resource, and BGP sessions.

CONSOLE

G CLOUD

API

The **VPN setup wizard** includes all required configuration steps for creating an HA VPN gateway, tunnels, a peer VPN gateway resource, and BGP sessions.

## Create a Cloud VPN gateway

1. Go to the VPN page in the Google Cloud Console.

**GO TO THE VPN PAGE** ([HTTPS://CONSOLE.CLOUD.GOOGLE.COM/HYBRID/VPN/LIST](https://console.cloud.google.com/hybrid/vpn/list))

- a. If you are creating a gateway for the first time, select the **Create VPN connection** button.
  - b. Select the **VPN setup wizard**.
2. Select the radio button for an HA VPN gateway.
  3. Click **Continue**.
  4. Specify a **VPN gateway name**.
  5. Under **VPC network**, select an existing network or the default network.
  6. Select a **Region**.
  7. Click **Create and Continue**.
  8. The console screen refreshes and displays your gateway information. Two public IP addresses are automatically allocated for each of your gateway interfaces. For future configuration steps, make note of the details of your gateway configuration.

## Create a Peer VPN gateway resource


The peer VPN gateway resource represents your non-Google Cloud gateway in Google Cloud.

**Caution:** If you specify a peer VPN gateway resource with one interface, the Cloud Console creates only one tunnel on one interface of the HA VPN gateway. If you want your configuration to meet the 99.99% SLA, you must follow the instructions at the end of this procedure for creating an additional tunnel.

1. On the **Create a VPN** screen, under **Peer VPN gateway**, select **Google Cloud**.
2. Under **Project**, select a Google Cloud project that will contain the new gateway.
3. Under **VPN gateway name**, choose the other HA VPN that you are configuring at the same time.
4. Continue on to **Create VPN tunnels**

### Create VPN tunnels

- If you select **Create a single VPN tunnel**, you configure your single tunnel on the rest of the **Create VPN** screen. However, you must create a second tunnel later to get a 99.99% SLA to the other HA VPN gateway.

 **Caution:** If you configure a single tunnel, you do not receive a 99.99% SLA for this configuration.

- If you select, **Create a pair of VPN tunnels** (recommended) you must configure the two tunnel dialog boxes that appear at the bottom of the **Create VPN** screen.
  1. Under **High Availability**, you can select either a pair of tunnels to the other HA VPN gateway, or one tunnel. You can add a second tunnel later as described at the end of this entire procedure.
  2. Under **Cloud Router**, If you haven't already, create a Cloud Router specifying the options as noted below. You can use an existing Cloud Router as long as the router does not already manage a BGP session for an interconnect attachment associated with a Partner Interconnect.
    - a. To create a Cloud Router, specify a **Name**, an optional **Description**, and **Google ASN** for the new router. You can use any private ASN (64512 through 65534, 4200000000 through 4294967294) that you are not using elsewhere in your network. The Google ASN is used for all BGP sessions on the same Cloud Router and it cannot be changed later.
    - b. Click **Create** to create the router.
  3. Complete the following steps either in the same screen, or in each tunnel's dialog box at the bottom of the screen.
  4. If you are configuring one tunnel, under **Associated Cloud VPN gateway interface**, select the HA VPN interface/IP address combination for this gateway to associate it with the gateway interface on the other HA VPN gateway. For two-tunnel configurations, this option and the **Associated peer VPN gateway interface** option are both unavailable because the correct interface combinations are configured for you.
    - a. Specify a **Name** for the tunnel.
    - b. Specify an optional **Description**.
    - c. Specify the **IKE version**. IKE v2, the default setting, is recommended if your peer router supports it.
    - d. Specify an **IKE pre-shared key** using your shared secret, which must correspond with the shared secret for the partner tunnel you create on your peer gateway. If you haven't configured a shared secret on your peer VPN gateway and want to generate one, click the

**Generate and copy** button. Make sure that you record the pre-shared key in a secure location, as it cannot be retrieved once you create your VPN tunnels.

e. Click **Done**.

f. Repeat the tunnel creation steps for any remaining tunnel dialog boxes on the **Create VPN** screen.

5. When you have configured all tunnels, click **Create and continue**.

## Create BGP sessions

### Setting the advertised route priority (optional)

The following example creates BGP sessions on instances of Cloud Router advertising the routes to the router's respective peer networks using *unmodified base priorities*.

Use this configuration for *active/active configurations* where the priorities of the two tunnels on both sides should match. Omitting the advertised base priority results in the same advertised priorities to both BGP peers.

For *active/passive configurations*, you can control the advertised base priority of the "to Google Cloud" routes that Cloud Router shares with your peer VPN gateway by setting the advertised route priority. To create an active/passive configuration, set a higher advertised route priority for one BGP session and its corresponding VPN tunnel, than for the other BGP session and VPN tunnel.

For more information about advertised base priority, see [Route metrics](https://cloud.google.com/router/docs/concepts/overview#route_metrics) ([https://cloud.google.com/router/docs/concepts/overview#route\\_metrics](https://cloud.google.com/router/docs/concepts/overview#route_metrics)).

You can also refine the routes that are advertised using [custom advertisements](https://cloud.google.com/router/docs/how-to/advertising-overview) (<https://cloud.google.com/router/docs/how-to/advertising-overview>), by adding the `--advertisement-mode=CUSTOM` flag and specifying IP address ranges with `--set-advertisement-ranges`.

To create BGP sessions:

1. If you don't want to configure BGP sessions now, click the **Configure BGP sessions later** button, which takes you to the **Summary and Reminder** screen.
2. If you want to configure BGP sessions now, click the **Configure** button for the first VPN tunnel.
3. On the **Create BGP session** screen, perform the following steps:
  - a. Specify a **Name** for the BGP session.
  - b. Specify the **Peer ASN** configured for the peer VPN gateway.
  - c. (Optional) Specify the **Advertised Route Priority**.
  - d. Specify the **Cloud Router BGP IP** address and the **BGP Peer IP** address. These addresses must each use a link-local address from the 169.254.0.0/16 CIDR block in the same /30 subnet. Make sure that these addresses aren't the network or broadcast address of the subnet.



- e. (Optional) Click the **Advertised routes** drop-down menu and create custom routes.
  - f. Click **Save and continue**.
4. Repeat the preceding steps for the rest of the tunnels configured on the gateway, using a different **Cloud Router BGP IP** address and **BGP Peer IP** address for each tunnel.
  5. When you have configured all BGP sessions, click **Save BGP configuration**.

### Summary and reminder

1. The **Summary** section of this screen lists information for the HA VPN gateway and the peer VPN gateway profile.
2. For each VPN tunnel, you can view the **VPN tunnel status** (<https://cloud.google.com/vpn/docs/support/troubleshooting#troubleshooting-reference>), the **BGP session name**, the **BGP session status** (<https://cloud.google.com/router/docs/support/troubleshooting>), and the MED value (advertised route priority).
3. The **Reminder** section of this screen lists the steps that you must complete to have a fully operational VPN connection between Cloud VPN and your peer VPN.
4. Click **Ok** after reviewing the information on this screen.

### Create an additional tunnel on a single-tunnel gateway.

**Caution:** You must configure a tunnel on each HA VPN interface, on each side of a HA VPN-to-HA VPN gateway configuration to receive a 99.99% uptime SLA.

Follow the steps in this section to configure a second tunnel on the second interface of a HA VPN gateway. If you've configured one tunnel on a HA VPN gateway to another HA VPN gateway but want to receive a 99.99% uptime SLA, you must configure a second tunnel.

1. Go to the VPN page in the Google Cloud Console.

**GO TO THE VPN PAGE** ([HTTPS://CONSOLE.CLOUD.GOOGLE.COM/HYBRID/VPN/LIST&TAB=GATEWAYS](https://console.cloud.google.com/hybrid/vpn/list&tab=gateways))

- a. Find the HA VPN you want to add the tunnel to.
- b. Click the **Add VPN tunnel** button.
- c. Under **Peer VPN gateway**, select Google Cloud.
- d. Under **Project**, select a Google Cloud project that will contain the new gateway.
- e. For **VPN gateway name**, choose the other HA VPN gateway that the new tunnel connects to.
- f. Select **Add the second VPN tunnel to an existing VPN tunnel for high availability**.
- g. Under **Select existing VPN tunnel**, make sure the existing tunnel is selected. You can click a link to view all existing tunnels near the top of the same screen.
- h. Specify a tunnel **Name**.

- i. Specify the same IKE version in use by the tunnel on the other gateway.
- j. Specify an **IKE pre-shared key** using your shared secret, which must correspond with the shared secret for the partner tunnel you create on your peer gateway. If you haven't configured a shared secret on your peer VPN gateway and want to generate one, click the **Generate and copy** button. Make sure that you record the pre-shared key in a secure location, as it cannot be retrieved once you create your VPN tunnels.
- k. Click **Create and continue**.
- l. Configure and save a BGP session as in the preceding steps. Otherwise, you can configure BGP later.
- m. Check the **Summary reminder** screen for configuration information and click **OK**.

## Completing the configuration

You must complete the following steps before you can use a new Cloud VPN gateway and its associated VPN tunnels:

1. Set up the peer VPN gateway and configure the corresponding tunnel or tunnels there.

Refer to these pages:

- For specific configuration guidance for certain peer VPN devices, see the [VPN Interoperability Guides](https://cloud.google.com/vpn/docs/how-to/interop-guides) (https://cloud.google.com/vpn/docs/how-to/interop-guides).
- For supported peer topologies, see the [Topologies](https://cloud.google.com/vpn/docs/concepts/topologies) (https://cloud.google.com/vpn/docs/concepts/topologies) page.
- For general configuration parameters, see [Configuring the Peer VPN Gateway](https://cloud.google.com/vpn/docs/how-to/configuring-peer-gateway) (https://cloud.google.com/vpn/docs/how-to/configuring-peer-gateway).

2. Configure firewall rules in Google Cloud and your peer network as required. See [the firewall rules page](https://cloud.google.com/vpn/docs/how-to/configuring-firewall-rules) (https://cloud.google.com/vpn/docs/how-to/configuring-firewall-rules) for suggestions.

3. [Check the status](https://cloud.google.com/vpn/docs/how-to/checking-vpn-status) (https://cloud.google.com/vpn/docs/how-to/checking-vpn-status) of your VPN tunnels and check the configuration of your HA VPN gateway for high availability.

## What's next

- [Maintain VPN tunnels and gateways](https://cloud.google.com/vpn/docs/how-to/maintaining-vpns)  
(<https://cloud.google.com/vpn/docs/how-to/maintaining-vpns>)
- [View logs and metrics](https://cloud.google.com/vpn/docs/how-to/viewing-logs-metrics) (<https://cloud.google.com/vpn/docs/how-to/viewing-logs-metrics>)
- [Get troubleshooting help](https://cloud.google.com/vpn/docs/support/troubleshooting) (<https://cloud.google.com/vpn/docs/support/troubleshooting>)
- See [Advanced Configurations](https://cloud.google.com/vpn/docs/concepts/advanced) (<https://cloud.google.com/vpn/docs/concepts/advanced>) for information on high-availability, high-throughput scenarios, or multiple subnet scenarios.

[Previous](#)

← [Creating an HA VPN to a peer VPN gateway](https://cloud.google.com/vpn/docs/how-to/creating-ha-vpn)

(<https://cloud.google.com/vpn/docs/how-to/creating-ha-vpn>)

[Next](#)

[Configuring firewall rules](https://cloud.google.com/vpn/docs/how-to/configuring-firewall-rules) →

(<https://cloud.google.com/vpn/docs/how-to/configuring-firewall-rules>)

---

*Except as otherwise noted, the content of this page is licensed under the [Creative Commons Attribution 4.0 License](https://creativecommons.org/licenses/by/4.0/) (<https://creativecommons.org/licenses/by/4.0/>), and code samples are licensed under the [Apache 2.0 License](https://www.apache.org/licenses/LICENSE-2.0) (<https://www.apache.org/licenses/LICENSE-2.0>). For details, see our [Site Policies](https://developers.google.com/terms/site-policies) (<https://developers.google.com/terms/site-policies>). Java is a registered trademark of Oracle and/or its affiliates.*

*Last updated November 22, 2019.*