Cloud VPN (https://cloud.google.com/vpn/)
Documentation (https://cloud.google.com/vpn/docs/) Guides

Creating an HA VPN gateway to a Peer VPN gateway

This page describes how to create a highly available VPN gateway that connects to a peer (https://cloud.google.com/vpn/docs/concepts/overview#peer-definition) VPN gateway.

HA VPN gateways use the HA VPN API and provide a 99.99% SLA. This configuration uses a tunnel pair, with one tunnel on each HA VPN gateway interface.

Warning: You must configure VPN tunnels on both HA VPN gateway interfaces to receive a 99.99% SLA.

There are two gateway components to configure for HA VPN:

- **An HA VPN gateway** in Google Cloud.
- **Your peer VPN gateway or gateways**—one or more physical VPN gateway devices or software applications in the peer network to which the HA VPN gateway connects. The peer gateway can be either an on-premises VPN gateway or one hosted by another cloud provider. You need to create **an external VPN gateway** resource in Google Cloud for each peer gateway device or service.

Note: All peer gateway scenarios are represented in Google Cloud by a single External Peer VPN resource.

Caution: When creating an HA VPN gateway for use with a peer gateway, correctly match the IP addresses for the peer interfaces with the IP addresses for the interfaces on the HA VPN gateway.

For an example, see the `gcloud` commands in the **To verify the Cloud Router configuration** section on this page. If these IP addresses are mismatched, the tunnels aren't established. See Checking tunnel status (https://cloud.google.com/vpn/docs/how-to/checking-vpn-status) for instructions on how to verify your tunnel configuration.

For diagrams of this topology, see the Topologies page (https://cloud.google.com/vpn/docs/concepts/topologies#to_peer_vpn_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).

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 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

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).

4. Install and initialize the Cloud SDK (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
```

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

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

Redundancy types

The HA VPN API contains an option for `REDUNDANCY_TYPE`, which represents the number of interfaces you configure for the external VPN gateway resource.

`gcloud` commands automatically infer the following values of `REDUNDANCY_TYPE` from the number of interfaces you provide in the interface ID when you configure an external VPN gateway resource:

- One external VPN interface is `SINGLE_IP_INTERNALLY_REDUNDANT`
- Two external VPN interfaces are `TWO_IPS_REDUNDANCY`
- Four external VPN interfaces are `FOUR_IPS_REDUNDANCY`

When configuring external VPN gateways, you must use the following interface identification numbers for the stated number of external VPN interfaces:

- For one external VPN interface, use a value of `0`.
- For two external VPN interfaces, use values `0` and `1`.
- For four external VPN interfaces, use values `0`,`1`,`2`, and `3`.

When configuring an HA VPN external VPN gateway to Amazon Web Services (AWS), the supported topology requires two AWS Virtual Private Gateways, `A` and `B`, each with two public IP addresses. This topology yields four public IP addresses total in AWS: `A1`, `A2`, `B1`, and `B2`.

Known issue: When configuring VPN tunnels to AWS, use the IKEv2 encryption protocol and select fewer transform sets on the AWS side, otherwise the Cloud VPN tunnel can fail to rekey. For example, select a combination of single Phase 1 and Phase 2 encryption algorithms, integrity algorithms, and DH group numbers.

This rekeying issue is caused by a large SA payload size for the default set of AWS transform sets. This large payload size results in IP fragmentation of IKE packets on the AWS side, which Cloud VPN does not support.

1. Configure the four AWS IP addresses as a single external HA VPN gateway with `FOUR_IPS_REDUNDANCY`, where:
   - AWS IP `0`=`A1`
   - AWS IP `1`=`A2`
   - AWS IP `2`=`B1`
   - AWS IP `3`=`B2`
2. Create four tunnels on the HA VPN gateway to meet the 99.99% SLA. using the following configuration:
   - HA VPN interface 0 to AWS interface 0
   - HA VPN interface 0 to AWS interface 1
   - HA VPN interface 1 to AWS interface 2
   - HA VPN interface 1 to AWS interface 3

Overview of high-level configurations steps to set up HA VPN with Amazon Web Services (AWS):

1. Create the HA VPN gateway and a Cloud Router. This creates 2 public IP addresses on the GCP side.
2. Create two AWS Virtual Private Gateways. This creates 4 public addresses on the AWS side.
3. Create two AWS Site-to-Site VPN connections and customer gateways, one for each AWS Virtual Private Gateway. Specify a non-overlapping link-local Tunnel IP Range for each tunnel, 4 total. For example, 169.254.1.4/30.
4. Download the AWS configuration files for the generic device type.
5. Create four VPN tunnels on the HA VPN gateway.
6. Configure BGP sessions on the Cloud Router using the BGP IP addresses from the downloaded AWS configuration files.

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`

Note: Instructions in this guide are written from the point of view of your Virtual Private Cloud network and Cloud VPN gateway.

Creating a custom Virtual Private Cloud network and subnet

Note: The examples in this document use one VPC network with one subnet in one region. However, your requirements might be different.

Before creating an HA VPN gateway and tunnel pair (#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).
- To create subnets, see Working with subnets (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) so that all instances of Cloud Router apply the `to on-premises` routes that they learn to all subnets of the VPC network. In global routing mode, routes to all subnets in the VPC network are shared with on-premises routers.

Creating only an HA VPN gateway

You can create a HA VPN gateway without the following resources and configure those resources later.

- VPN tunnels
- A peer VPN gateway resource
- BGP sessions

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

CONSOLE GCLOUD 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

   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 an HA VPN gateway and tunnel pair to a peer VPN

Follow the instructions in this section to create a HA VPN gateway, a pair of tunnels (#tunnel-pair), a peer VPN gateway resource, and BGP sessions.

CONSOLE GCLOUD 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)

   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. For 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 `On-prem or Non-Google Cloud`.
2. Under **Peer VPN gateway name**, choose an existing peer gateway, or click **Create a new peer VPN gateway**. If you choose an existing gateway, Cloud Console selects the number of tunnels to configure based on the number of peer interfaces you configured on the existing peer gateway. To create a new peer gateway, complete the following steps:
   a. Specify a **Name** for the peer VPN gateway.
   b. Under **Peer VPN gateway interfaces**, select `one`, `two`, or `four` interfaces, depending on the type of interfaces your peer gateway has. See the Topologies page (https://cloud.google.com/vpn/docs/concepts/topologies) for examples of each type.
   c. In the field for each peer VPN interface, specify the public IP address used for that interface. For more information, refer to Configuring the peer VPN gateway (https://cloud.google.com/vpn/docs/how-to/configuring-peer-gateway).
   d. Click **Create**.

Create VPN tunnels

- If you configured your peer VPN gateway resource with one interface, you configure your single tunnel in the single VPN tunnel dialog box on the **Create VPN** screen. You must create a second tunnel for a 99.99% SLA.
- If you configured your peer VPN gateway resource with two or four interfaces, you must configure the associated dialog boxes that appear at the bottom of the **Create VPN** screen.

1. Under **Cloud Router**, If you haven't already, create a Cloud Router specifying the following options. You can use an existing Cloud Router if the router does not already manage a BGP session for an interconnect attachment associated with a Partner Interconnect.
   a. To create a new 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 you cannot change the ASN later.
   b. Click **Create** to create the new router.
2. If applicable, under **Associated Cloud VPN gateway interface**, select the HA VPN interface and IP address combination that you want to associate with your peer VPN gateway interface for this tunnel.
3. Under **Associated peer VPN gateway interface**, select the peer VPN gateway interface and IP address combination that you want to associate with this tunnel and with the HA VPN interface. This interface must match the interface on your actual peer router.
   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 that 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, because it cannot be retrieved after 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.
4. When you have configured all tunnels, click **Create and continue**.

Create BGP sessions

1. If you don't want to configure BGP sessions now, click the **Configure BGP sessions later** button, which opens **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, use 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. Each of these addresses must 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 previous 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**.

Note on setting the advertised base route priority:
The following example creates BGP sessions on instances of Cloud Router. These BGP sessions allow each Cloud Router to advertise routes to peer networks. The advertisements use *unmodified base priorities*.

Use the configuration documented in this section for *active/active routing configurations* where the route priorities of the two VPN tunnels from the Google Cloud side and peer side match. Omit the advertised base route priority on the Google Cloud side to configure the same advertised priorities from Google Cloud to both BGP peers.

To create an *active/passive configuration*, you must configure unequal advertised base route priorities for the two HA VPN tunnels. One route priority must be higher than the other. For example:

- BGP session1/tunnel1, route priority = 10
- BGP session2/tunnel2, route priority = 20

For more information about advertised base route priority, refer to Route metrics (https://cloud.google.com/router/docs/concepts/overview#route_metrics).

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

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 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. Do this in the following circumstances:

- When you've configured a HA VPN gateway to a peer VPN gateway that has a single peer VPN interface.
- If you set up a single tunnel previously on a HA VPN for a peer VPN gateway that contains any number of interfaces, but now want a 99.99% uptime SLA for your HA 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&TAB=T

2. Click the **Create VPN tunnel** button.
3. From the drop-down menu, select the gateway that requires the second tunnel.
4. Click **Continue**.
5. Choose a Cloud Router. If you haven't configured a Cloud Router, follow the steps for creating one in the **Create VPN tunnels** procedure.
6. For **Peer VPN gateway**, select **On-prem or Non Google Cloud**.
7. For **Peer VPN gateway name**, choose the existing peer VPN gateway resource that the new tunnel will use. You can check existing peer VPN gateway names for this Cloud VPN gateway by clicking the **View all existing tunnels** link under **VPN gateway name** near the top of the screen.
8. You might receive a warning that a tunnel with the same peer VPN gateway interface is already associated with the same local Cloud VPN gateway interface. To fix this issue, under **Associated Cloud VPN gateway interface**, select the other HA VPN interface.
9. Configure the remainder of the steps as listed in the **Create VPN tunnels** procedure to finish configuring the tunnel.

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).
   - For supported peer topologies, see the 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).
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) for suggestions.

3. Check the status (https://cloud.google.com/vpn/docs/how-to/checking-vpn-status) of your VPN tunnels.

★ Note: This step includes checking the high-availability configuration of your HA VPN gateway.

What's next

- Maintain VPN tunnels and gateways (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)
- Get troubleshooting help (https://cloud.google.com/vpn/docs/support/troubleshooting)
- See Advanced Configurations (https://cloud.google.com/vpn/docs/concepts/advanced) for information on high-availability, high-throughput scenarios, or multiple subnet scenarios.

Next
Creating Google Cloud to Google Cloud HA VPN gateways →
(https://cloud.google.com/vpn/docs/how-to/creating-ha-vpn2)

Last updated November 22, 2019.