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

Creating a Classic VPN using static routing

This page describes how to create a Classic VPN gateway and one tunnel using static routing, which in this case means using a policy based
 (https://cloud.google.com/vpn/docs/concepts/choosing-networks-routing#static-routing) or route based
 (https://cloud.google.com/vpn/docs/concepts/choosing-networks-routing#static-routing) static routing option.

With route based VPN, you specify only the remote traffic selector. If you need to specify a local traffic selector, create a Cloud VPN tunnel that uses policy based routing instead.

> **Note:** HA VPN *does not* support static routing.

> **Caution:** If you convert an auto mode Virtual Private Cloud network to a custom mode VPC network, you might have to delete and re-create VPN tunnels that use policy based routing if the tunnel relied on default values for local IP ranges. Changing the mode of a VPC network with active VPN tunnels can lead to outages. See considerations for auto mode networks
> (https://cloud.google.com/vpc/docs/vpc#subnet-ranges) for more information.

Routing option differences

Policy based routing should be considered when a peer
 (https://cloud.google.com/vpn/docs/concepts/overview#peer-definition) VPN gateway cannot use
Border Gateway Protocol (BGP)
 (https://cloud.google.com/vpn/docs/concepts/overview#bgp-definition) to dynamically exchange

routes. With this option, local IP ranges (left side) and remote IP ranges (right side) are defined. These local and remote IP are the *traffic selectors* for the tunnel.

Policy based routing uses local and a remote traffic selectors.

Route based VPN tunnels are similar to tunnels that use policy based routing, except that only the remote IP ranges (right side) are specified. The list of local IP ranges is assumed to be any network (`0.0.0.0/0`), so you only specify the remote traffic selector.

As with policy based routing, Google Cloud automatically creates a static route for each remote IP address range.

Review the following documentation for background information before setting up either type of static routing option:

- Information about traffic selectors
  (https://cloud.google.com/vpn/docs/concepts/choosing-networks-routing#static-routing-networks)

- How Cloud VPN handles multiple IP ranges
  (https://cloud.google.com/vpn/docs/concepts/choosing-networks-routing#ts-ip-ranges) in traffic selectors.

- See the Classic VPN Topologies page
  (https://cloud.google.com/vpn/docs/concepts/classic-topologies) for sample topologies.

For even more details see the entire Networks and tunnel routing
 (https://cloud.google.com/vpn/docs/concepts/choosing-networks-routing) page.

> **Important:** The traffic selectors cannot be changed after a tunnel has been created. If traffic selectors need to be changed in the future, you must delete and re-create the tunnel.

Before you begin

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]
```

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.targetVpnGateways.get`
- `compute.targetVpnGateways.list`
- `compute.targetVpnGateways.create`
- `compute.targetVpnGateways.delete`
- `compute.targetVpnGateways.get`
- `compute.targetVpnGateways.list`
- `compute.targetVpnGateways.use`
- `compute.targetVpnGateways.setLabels`

Roles

- `roles/compute.networkAdmin`

Creating a custom Virtual Private Cloud network and subnet

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

Creating a gateway and tunnel

The **VPN setup wizard** is the only console option for creating a Classic VPN gateway. The wizard includes all required configuration steps for creating a Classic VPN gateway, tunnels, BGP sessions, and an external VPN gateway resource. However, you can complete certain steps later. For example, configuring BGP sessions.

The **Create a VPN** button only supports creating HA VPN gateways.

VPN WIZARD   GCLOUD

Configure the 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)

2. Click **VPN setup wizard**.

3. On the **Create a VPN** page, specify **Classic VPN**.

4. Click **Continue**.

5. On the **Create a VPN connection** page, specify the following gateway settings:
   - **Name** — The name of the VPN gateway. The name cannot be changed later.
   - **Description** — Optionally, add a description.
   - **Network** — Specify an existing VPC network in which to create the VPN gateway and tunnel.

- **Region** — Cloud VPN gateways and tunnels are regional objects. Choose a Google Cloud region (https://cloud.google.com/compute/docs/regions-zones/) where the gateway will be located. Instances and other resources in *different regions* can use the tunnel for egress traffic subject to the order of routes (https://cloud.google.com/vpn/docs/concepts/order-of-routes). For best performance, locate the gateway and tunnel in the same region as relevant Google Cloud resources.

- **IP address** — Create or choose an existing regional external IP address (https://cloud.google.com/compute/docs/ip-addresses#reservedaddress).

Configure Tunnels

1. Specify the following settings in the **Tunnels** section for the new tunnel:

   - **Name** — The name of the VPN tunnel. The name cannot be changed later.

   - **Description** — Optionally, type a description.

   - **Remote peer IP address** — Specify the public IP address of the peer VPN gateway.

   - **IKE version** — Choose the appropriate IKE version supported by the peer VPN gateway. IKEv2 is preferred if it's supported by the peer device.

   - **Shared secret** — Provide a pre-shared key used for authentication. The shared secret for the Cloud VPN tunnel must match the one used when you configure the counterpart tunnel on the peer VPN gateway. You can follow these directions (https://cloud.google.com/vpn/docs/how-to/generating-pre-shared-key) to generate a cryptographically strong shared secret.

   For Policy based tunnels

   - Under **Routing options**, select **Policy-based**.

   - Under **Remote network IP ranges**, provide a space-separated list of the IP ranges used by the peer network. This is the **remote traffic selector**: the "right side" from the perspective of Cloud VPN.

   - Under **Local IP ranges**, select one of the following methods:

     - Use the **Local subnetworks** menu to choose an existing local IP range, or

     - Use the **Local IP ranges** field to enter a list of space-separated IP ranges used in your VPC network. Refer to traffic selectors (https://cloud.google.com/vpn/docs/concepts/choosing-networks-routing#static-routing-networks) for important considerations.

   For Route based tunnels

   - **Routing options** — Select **Route-based**.

   - **Remote network IP ranges** — Provide a space-separated list of the IP ranges used by the peer network. These ranges are used to create custom static routes whose next hop is this VPN

tunnel.

2. If you need to create more tunnels on the same gateway, click **Add tunnel** and repeat the previous step. You can also add more tunnels later (https://cloud.google.com/vpn/docs/how-to/adding-a-tunnel).

3. Click **Create**.

Note: Google Cloud automatically creates one route for each remote IP range you specify. The destination of the route is the remote IP range, its next hop set to the Cloud VPN tunnel, and its priority is `1000`. You *cannot* set the priority of this automatically-created route, but you can delete and replace it. If you need greater control over the priority of VPN routes, follow the `gcloud` directions instead.

Follow-up steps

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

1. Set up the peer VPN gateway and configure the corresponding tunnel there. Refer to these pages:

   - For specific configuration guidance for certain VPN devices, refer to the VPN Interoperability Guides (https://cloud.google.com/vpn/docs/how-to/interop-guides).

   - For general configuration parameters, refer to 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. Refer to 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 tunnel, including forwarding rules (https://cloud.google.com/vpn/docs/how-to/checking-vpn-status#forwarding-rules).

4. You can view your VPN routes BY VISITING THE PROJECT ROUTING TABLE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/NETWORKI and filtering for 'Next hop type:VPN tunnel'.

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.