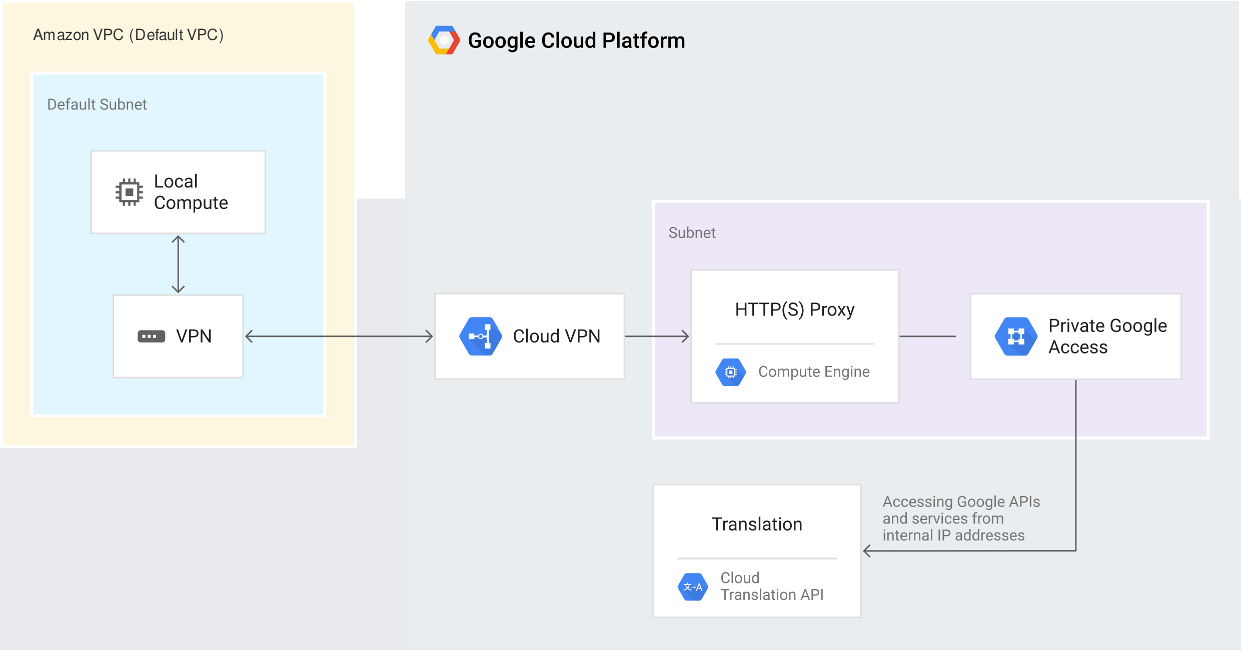
**Important:** Private Google Access for on-premises hosts (/vpc/docs/private-access-options#pga-onprem) is now the preferred solution for providing access to Google APIs and services from an on-premises network or from another Cloud provider's network.

This tutorial demonstrates how to use APIs for Google Cloud services from an external network, such as your on-premises private network or another cloud provider's network. This approach allows your on-premises servers that are connected to your private network to access Google Cloud services without using public IP addresses. This tutorial presents an example in which you use a private network on Amazon Virtual Private Cloud (Amazon VPC) to emulate an on-premises private network.

The following diagram summarizes the overall architecture that you create in this tutorial.

- You connect a private network in Amazon VPC to a virtual network in your Google Cloud project through IPsec VPN. If you use an on-premises private network instead of Amazon VPC, you would use Cloud Interconnect (/interconnect/docs/) to have a private network connection to your Google Cloud project.
- You use Private Google Access (/vpc/docs/private-google-access) from Google Cloud projects. Servers running outside Google Cloud projects cannot reach Google Cloud APIs, such as the Cloud Translation, by using an internal IP address, even when Private Google Access is enabled. Therefore, you use an HTTP or HTTPS proxy in your Google Cloud project to transfer API requests from external servers to Google Cloud APIs and services using internal IP addresses.



- Enable Private Google Access in order to allow Compute Engine VM instances to access Google Cloud APIs without using public IP addresses.
- Set up an HTTP or HTTPS proxy using a Compute Engine instance to allow servers in Amazon VPC to access Google Cloud APIs without using public IP addresses.

This tutorial uses the following billable components of Google Cloud:

- Compute Engine (/compute/)
- Cloud VPN (/vpn/docs/)
- Cloud Translation

To generate a cost estimate based on your projected usage, use the pricing calculator (/products/calculator). New Google Cloud users might be eligible for a free trial (/free-trial).

Additionally, you might incur costs for Amazon Web Services (https://calculator.s3.amazonaws.com/index.html) (AWS) services, such as Amazon VPC, VPN, and Amazon Elastic Compute Cloud (Amazon EC2) instances.

**Note:** This tutorial requires that you have an AWS account to use Amazon VPC.

Before you begin this tutorial, use the Cloud Console to create a Google Cloud project and enable billing. Don't use an existing project, because when you're done, you need to delete the project to avoid incurring further costs.

1. Create a Google Cloud project for the tutorial.

   GO TO THE MANAGE RESOURCES PAGE (https://console.cloud.google.com/project)

2.

3. Make sure that billing is enabled for your Google Cloud project. Learn how to confirm billing is enabled for your project (/billing/docs/how-to/modify-project).

4. Enable the Translation.

   ENABLE THE Translation (https://console.cloud.google.com/flows/enableapi?apiid=translate)

   The Compute Engine API is automatically enabled in new projects.

5. In the Cloud Console, open the **Credentials** page.

   GO TO CREDENTIALS (https://console.cloud.google.com/apis/credentials)

6. For **Create credentials**, select **API key**, and then click **Close**.

7. Take note of the API key string displayed in the console.

In this tutorial, you use Amazon VPC to emulate your on-premises data center. To establish the Amazon VPC, follow the instructions in Using Cloud VPN with Amazon Web Services (/files/CloudVPNGuide-UsingCloudVPNwithAmazonWebServices.pdf), in the sections "Policy Based IPsec VPN: Configuration - AWS" and "Policy Based IPsec VPN: Configuration - GCP UI."

- Use the default VPC with the network address `172.31.0.0/16 CIDR`.
- Use the default subnet with the network address `172.31.0.0/16 CIDR`.
- Create a VPN connection with AWS using the static IP address `aws-vpn` as a Compute Engine VPN gateway.

**Note:** The AWS region can be arbitrary. You might use Asian regions in this step because this tutorial uses **`asia-east1`** on Google Cloud.

You use IPsec VPN to connect Amazon VPC to the Google Cloud virtual network that you create in Google Cloud.

**Note:** If you want to use custom subnets instead of the automatic option, choose the IP addresses in the following steps according to your subnet configuration.

To enable the Amazon EC2 instances to access the Google Cloud virtual network in your project, follow these steps:

1. In the AWS Management Console, click the **Route Table** tab.
2. Select **Route Propagation** and click **Edit**.
3. Select **Propagate** in your VPC network private IP range, and then click **Save**.

You enable Private Google Access on the subnet connected to Amazon VPC.

The next step is to add firewall rules that allow the proxy connection from Amazon VPC, and an SSH connection from all external networks. The SSH connection is used only for configuring the HTTP or HTTPS proxy instance. To configure the proxy without manually signing in to the instance, you can use a startup script, in which case you don't need to create the firewall rule for the SSH connection.

Next, you need to create a Compute Engine instance, configure it as an HTTP or HTTPS proxy, and sign in.

At this point, you don't need the SSH connection to the instance anymore. If your security standards require you to remove the firewall rule that allows the SSH connection, do the following operation:

You must prevent the proxy instance from accidentally using a public IP address to reach Google Cloud APIs. This section shows how to remove the external IP address from the proxy instance.

In this section, you use the Cloud Translation to verify that you can use a Google Cloud API from an Amazon EC2 instance that is running on Amazon VPC.

1. Launch an Amazon EC2 instance in the Amazon VPC that you created.
2. Connect to the Amazon EC2 instance by using the SSH terminal.
3. Create an API request message file:

4. Post a request that specifies the proxy address. Replace `[YOUR_API_KEY]` with the API key string you created earlier (#before-you-begin).

   The Translation service replies as follows:

When you have completed this tutorial, delete your project to avoid incurring further costs.

**Caution**: Deleting a project has the following effects:

- **Everything in the project is deleted.** If you used an existing project for this tutorial, when you delete it, you also delete any other work you've done in the project.
- **Custom project IDs are lost.** When you created this project, you might have created a custom project ID that you want to use in the future. To preserve the URLs that use the project ID, such as an **`appspot.com`** URL, delete selected resources inside the project instead of deleting the whole project.

1. In the Cloud Console, go to the **Manage resources** page.

   Go to the Manage resources page (https://console.cloud.google.com/iam-admin/projects)

2. In the project list, select the project you want to delete and click **Delete** 🗑.
3. In the dialog, type the project ID, and then click **Shut down** to delete the project.

- Visit the Virtual Private Cloud (/vpc/) and Compute Engine (/compute/) documentation for in-depth information about how to get the most out of each product.
- Learn more about interconnect options by watching the Cloud networking solutions (https://youtu.be/WeRRlIt_inI) video from Google Cloud Next ‘17.
- Try out other Google Cloud features for yourself. Have a look at our tutorials (/docs/tutorials).