Virtual Private Network

* [Overview](https://googlepluralsight.qwiklabs.com/focuses/23538640?parent=lti_session#step1)
* [Objectives](https://googlepluralsight.qwiklabs.com/focuses/23538640?parent=lti_session#step2)
* [Setup](https://googlepluralsight.qwiklabs.com/focuses/23538640?parent=lti_session#step3)
* [Task 1. Explore the networks and instances](https://googlepluralsight.qwiklabs.com/focuses/23538640?parent=lti_session#step4)
* [Task 2. Create the VPN gateways and tunnels](https://googlepluralsight.qwiklabs.com/focuses/23538640?parent=lti_session#step5)
* [Task 3. Verify VPN connectivity](https://googlepluralsight.qwiklabs.com/focuses/23538640?parent=lti_session#step6)
* [Task 4. Review](https://googlepluralsight.qwiklabs.com/focuses/23538640?parent=lti_session#step7)
* [End your lab](https://googlepluralsight.qwiklabs.com/focuses/23538640?parent=lti_session#step8)

Virtual Private Network

**Overview**

In this lab, you establish VPN tunnels between two networks in separate regions such that a VM in one network can ping a VM in the other network over its internal IP address.

**Objectives**

In this lab, you learn how to perform the following tasks:

* Create VPN gateways in each network
* Create VPN tunnels between the gateways
* Verify VPN connectivity

**Task 1. Explore the networks and instances**

Two custom networks with VM instances have been configured for you. For the purposes of the lab, both networks are VPC networks within a Google Cloud project. However, in a real-world application, one of these networks might be in a different Google Cloud project, on-premises, or in a different cloud.

**Explore the networks**

Verify that **vpn-network-1** and **vpn-network-2** have been created with subnets in separate regions.

1. In the Cloud Console, on the **Navigation menu** (Navigation menu icon), click **VPC network** > **VPC networks**.
   1. Note the **vpn-network-1** network and its **subnet-a** in **us-central1**.
   2. Note the **vpn-network-2** network and its **subnet-b** in **europe-west1**.
2. **Explore the firewall rules**
3. In the navigation pane, click **Firewall**.
   1. Note the **network-1-allow-ssh** and **network-1-allow-icmp** rules for **vpn-network-1**.
   2. Note the **network-2-allow-ssh** and **network-2-allow-icmp** rules for **vpn-network-2**.

These firewall rules allow **SSH** and **ICMP** traffic from anywhere.

**Explore the instances and their connectivity**

Currently, the VPN connection between the two networks is not established. Explore the connectivity options between the instances in the networks.

1. In the Cloud Console, on the **Navigation menu** (Navigation menu icon), click **Compute Engine** > **VM instances**.
2. Click **Column display options** icon and select **Network**.
3. From server-1, you should be able to ping the following IP addresses of server-2:
4. 
5. Internal IP address
6. checkExternal IP address
7. Submit
8. Note the external and internal IP addresses for **server-2**.
9. For **server-1**, click **SSH** to launch a terminal and connect.
10. To test connectivity to server-2's external IP address, run the following command, replacing server-2's external IP address with the value noted earlier:
11. ping -c 3 <Enter server-2's external IP address here>
12. Copied!
13. content\_copy
14. **Note:**This works because the VM instances can communicate over the internet.
15. To test connectivity to server-2's internal IP address, run the following command, replacing server-2's internal IP address with the value noted earlier:
16. ping -c 3 <Enter server-2's internal IP address here>
17. Copied!
18. **Note:**You should see 100% packet loss when pinging the internal IP address because you don't have VPN connectivity yet.
19. Exit the SSH terminal.
20. Let's try the same from **server-2**.
21. Note the external and internal IP addresses for **server-1**.
22. For **server-2**, click **SSH** to launch a terminal and connect.
23. To test connectivity to server-1's external IP address, run the following command, replacing server-1's external IP address with the value noted earlier:
24. ping -c 3 <Enter server-1's external IP address here>
25. To test connectivity to server-1's internal IP address, run the following command, replacing server-1's internal IP address with the value noted earlier:

ping -c 3 <Enter server-1's internal IP address here>

**Note:**You should see similar results.

Exit the SSH terminal.

**Note:**Why are we testing both **server-1** to **server-2** and **server-2** to **server-1**?

For the purposes of this lab, the path from subnet-a to subnet-b is not the same as the path from subnet-b to subnet-a. You are using one tunnel to pass traffic in each direction. And if both tunnels are not established, you won't be able to ping the remote server on its internal IP address. The ping might reach the remote server, but the response can't be returned.

This makes it much easier to debug the lab during class. In practice, a single tunnel could be used with symmetric configuration. However, it is more common to have multiple tunnels or multiple gateways and VPNs for production work, because a single tunnel could be a single point of failure.

**Task 2. Create the VPN gateways and tunnels**

Establish private communication between the two VM instances by creating VPN gateways and tunnels between the two networks.

**Reserve two static IP addresses**

Reserve one static IP address for each VPN gateway.

* In the Cloud Console, on the **Navigation menu** (Navigation menu icon), click **VPC network** > **IP addresses**.
* Click **Reserve external static address**.
* Specify the following, and leave the remaining settings as their defaults:

|  |  |
| --- | --- |
| **Property** | **Value (type value or select option as specified)** |
| Name | vpn-1-static-ip |
| IP version | IPv4 |
| Region | us-central1 |

1. Click **Reserve**.
2. Repeat the same for **vpn-2-static-ip**.
3. Click **Reserve external static address**.
4. Specify the following, and leave the remaining settings as their defaults:

|  |  |
| --- | --- |
| **Property** | **Value (type value or select option as specified)** |
| Name | vpn-2-static-ip |
| IP version | IPv4 |
| Region | europe-west1 |

1. Click **Reserve**.

Note both IP addresses for the next step. They will be referred to as [VPN-1-STATIC-IP] and [VPN-2-STATIC-IP].

**Create the vpn-1 gateway and tunnel1to2**

* In the Cloud Console, on the **Navigation menu** (Navigation menu icon), click **Hybrid Connectivity** > **VPN**.
* Click **Create VPN Connection**.
* If asked, select **Classic VPN**, and then click **Continue**.
* Specify the following in the **VPN gateway** section, and leave the remaining settings as their defaults:

|  |  |
| --- | --- |
| **Property** | **Value (type value or select option as specified)** |
| Name | vpn-1 |
| Network | vpn-network-1 |
| Region | us-central1 |
| IP address | vpn-1-static-ip |

* 1. Specify the following in the **Tunnels** section, and leave the remaining settings as their defaults:

|  |  |
| --- | --- |
| **Property** | **Value (type value or select option as specified)** |
| Name | tunnel1to2 |
| Remote peer IP address | [VPN-2-STATIC-IP] |
| IKE pre-shared key | gcprocks |
| Routing options | Route-based |
| Remote network IP ranges | 10.1.3.0/24 |

1. Make sure to replace [VPN-2-STATIC-IP] with your reserved IP address for **europe-west1**.
2. Click **equivalent command line**.
3. **Note:**The **gcloud command line** window shows the gcloud commands to create the **VPN gateway** and **VPN tunnels** and it illustrates that three forwarding rules are also created.
4. Click **Close**.
5. Click **Create**.

Create the 'vpn-1' gateway and tunnel

**Create the vpn-2 gateway and tunnel2to1**

* Click **VPN setup wizard**.
* If asked, select **Classic VPN**, and then click **Continue**.
* Specify the following in the **VPN gateway** section, and leave the remaining settings as their defaults:

|  |  |
| --- | --- |
| **Property** | **Value (type value or select option as specified)** |
| Name | vpn-2 |
| Network | vpn-network-2 |
| Region | europe-west1 |
| IP address | vpn-2-static-ip |

1. Specify the following in the **Tunnels** section, and leave the remaining settings as their defaults:

|  |  |
| --- | --- |
| **Property** | **Value (type value or select option as specified)** |
| Name | tunnel2to1 |
| Remote peer IP address | [VPN-1-STATIC-IP] |
| IKE pre-shared key | gcprocks |
| Routing options | Route-based |
| Remote network IP ranges | 10.5.4.0/24 |

Make sure to replace [VPN-1-STATIC-IP] with your reserved IP address for **us-central1**.

Click **Create**.

Create the 'vpn-2' gateway and tunnel

1. Click **Cloud VPN Tunnels**.
2. Wait for the **VPN tunnels status** to change to **Established** for both tunnels before continuing.

**Task 3. Verify VPN connectivity**

**Verify server-1 to server-2 connectivity**

1. In the Cloud Console, on the **Navigation menu**, click **Compute Engine** > **VM instances**.
2. For **server-1**, click **SSH** to launch a terminal and connect.
3. To test connectivity to **server-2**'s internal IP address, run the following command:

**ping -c 3 <insert server-2's internal IP address here>**

1. Exit the **server-1** SSH terminal.
2. For **server-2**, click **SSH** to launch a terminal and connect.
3. To test connectivity to **server-1**'s internal IP address, run the following command:

**ping -c 3 <insert server-1's internal IP address here>**

**Remove the external IP addresses**

Now that you verified VPN connectivity, you can remove the instances' external IP addresses. For demonstration purposes, just do this for the **server-1** instance.

1. On the **Navigation menu**, click **Compute Engine** > **VM instances**.
2. Select the **server-1** instance and click **Stop**. Wait for the instance to stop.
3. **Note:**Instances need to be stopped before you can make changes to their network interfaces.
4. Click on the name of the **server-1** instance to open the **VM instance details** page.
5. Click **Edit**.
6. For **Network interfaces**, click **Edit** (Edit icon).
7. Change **External IPv4 address** to **None**.
8. Click **Done**.
9. Click **Save** and wait for the instance details to update.
10. Click **Start**.
11. Click **Start** again to confirm that you want to start the VM instance.
12. Return to the **VM instances** page and wait for the instance to start.
13. Notice that **External IP** is set to **None** for the **server-1** instance.

Feel free to SSH to **server-2** and verify that you can still ping the **server-1** instance's internal IP address. You should still be able to SSH to **server-1** from the Cloud Console using Cloud IAP as described in the Cloud Architecture Center, [Configuring IAP tunnels for interacting with instances](https://cloud.google.com/solutions/building-internet-connectivity-for-private-vms#configuring_iap_tunnels_for_interacting_with_instances).

**Note:**External IP addresses that don’t fall under the [Free Tier](https://cloud.google.com/free/docs/gcp-free-tier#always-free-usage-limits) will incur a [small cost](https://cloud.google.com/compute/network-pricing#ipaddress). Also, as a general security best practice, it’s a good idea to use internal IP addresses where applicable and since you configured Cloud VPN you no longer need to communicate between instances using their external IP address.