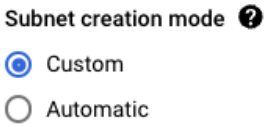
Securely Connecting GKE to Cloud SQL for MySQL Across Projects via VPN

Connecting Google Kubernetes Engine (GKE) to a Cloud SQL instance in a different Google Cloud project using a Virtual Private Network (VPN) involves setting up a secure network bridge between the two projects. This approach uses VPC (Virtual Private Cloud) peering or VPN to enable communication between GKE and Cloud SQL instances. Below is a detailed guide to accomplish this setup using a VPN.

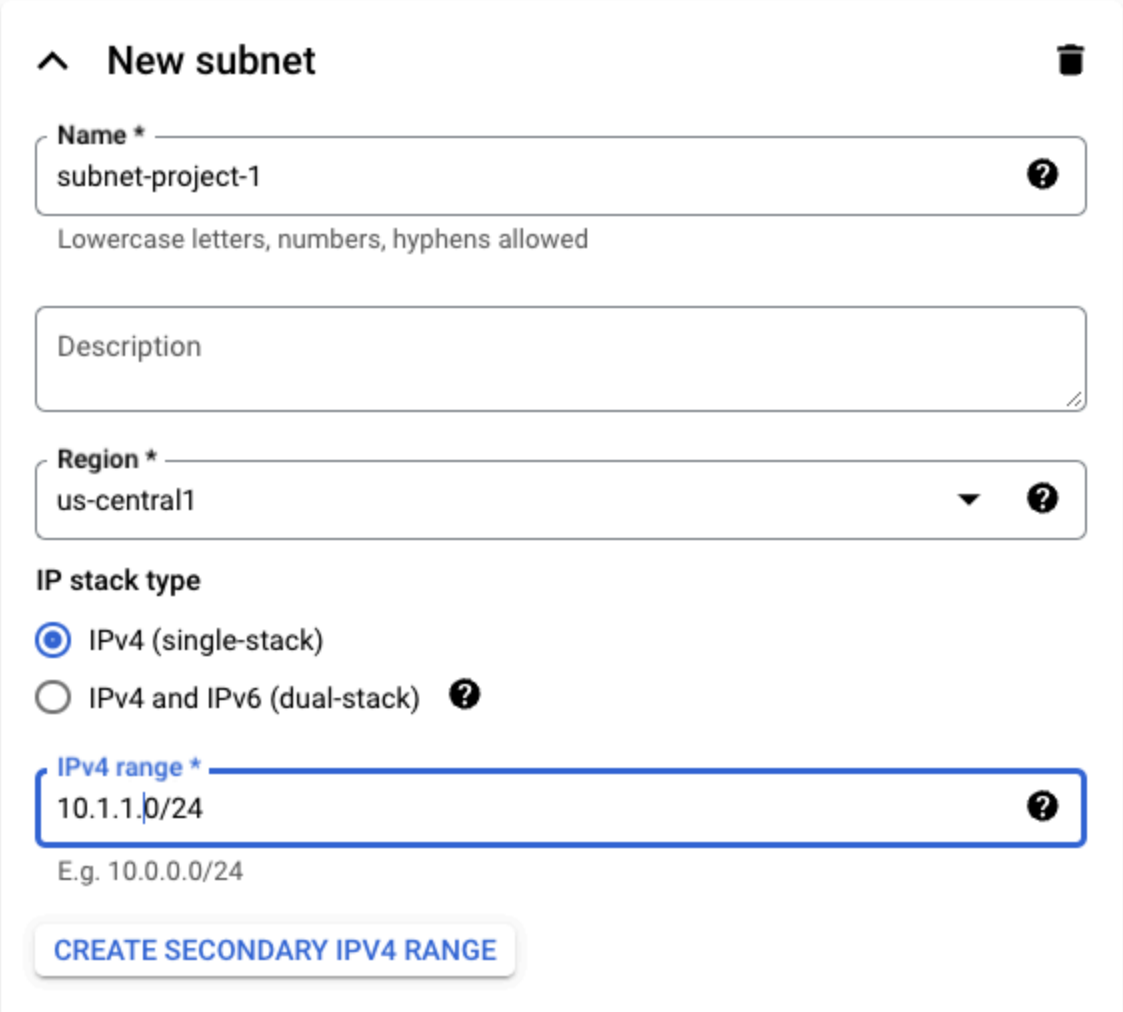
1. Setup VPC Across Projects

Select Project 1:
Switch to the first project from the project dropdown.
Create the VPC Network:
Click Create VPC network.
Enter a name for the network (e.g., `vpc-project-1`).

Set the Subnet creation mode to **Custom**.

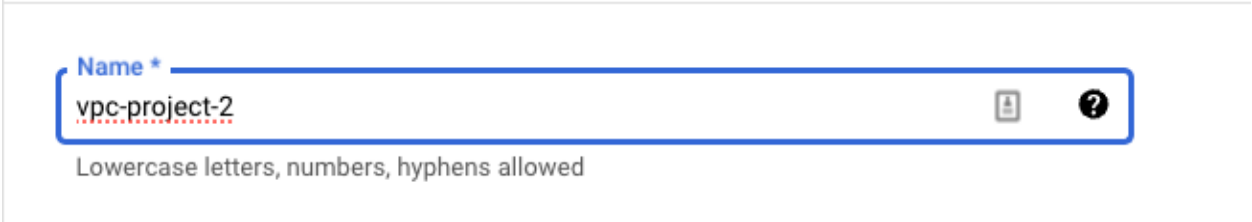


Add a subnet:
Name: `subnet-project-1`
Region: Select the region (e.g., us-central1).
IP Address range: 10.1.1.0/24

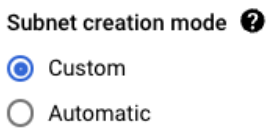


Select the default firewall rules.
Click on Create.

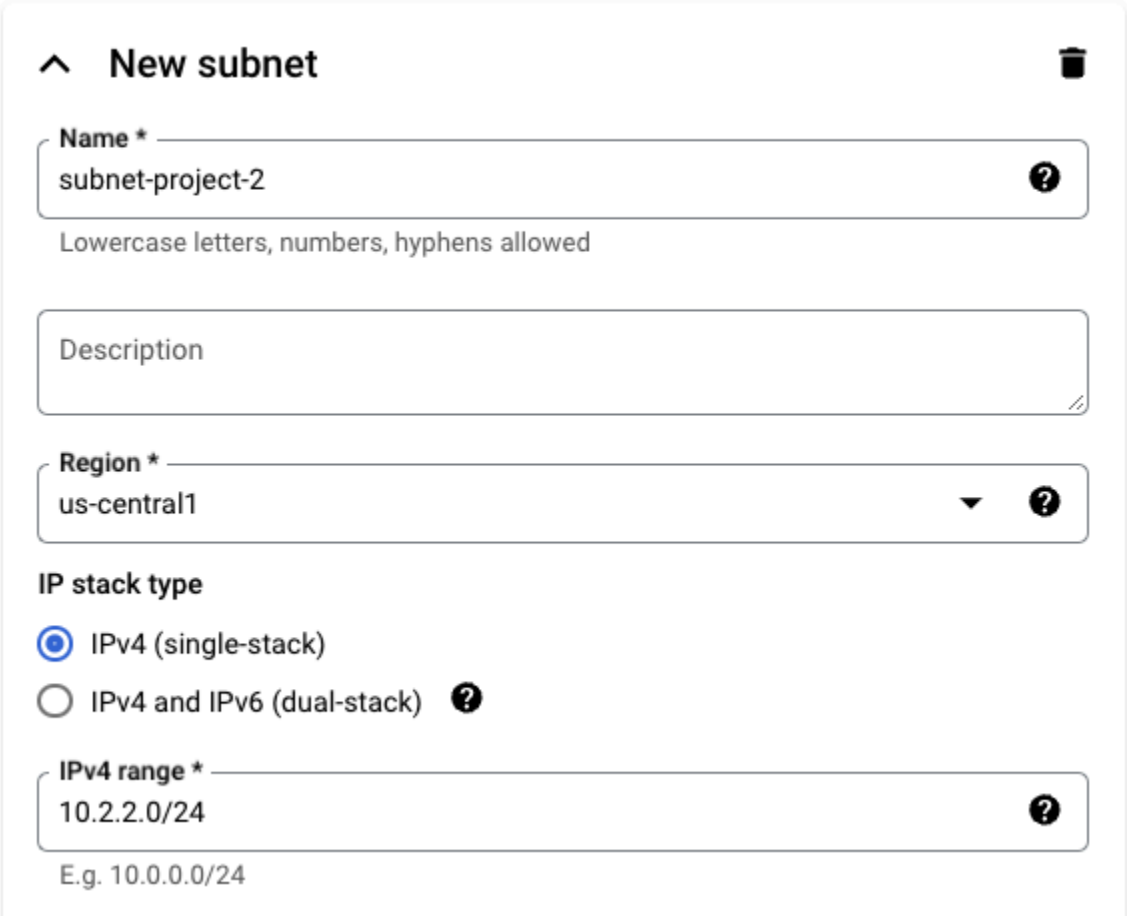
Project 2:
Select Project 2:
Switch to the second project from the project dropdown.
Create the VPC Network:
Click Create VPC network.
Enter a name for the network (e.g., `vpc-project-2`).



Set the Subnet creation mode to **Custom**.



Add a subnet:
Name: `subnet-project-2`
Region: Select the region (e.g., us-central1).
IP Address range: 10.2.2.0/24



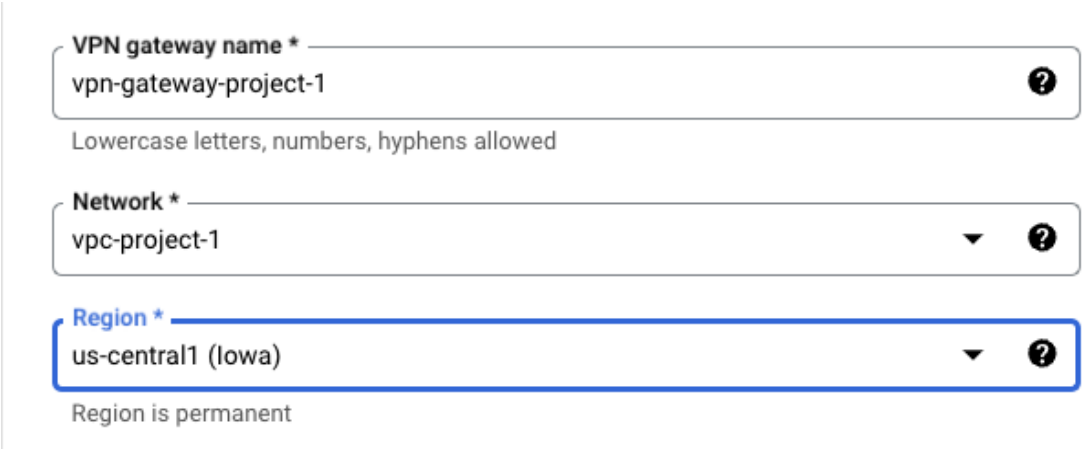
Select the default firewall rules.
Click on Create.

2. Create two fully configured HA VPN gateways that connect to each other

1. Create VPN Gateways

Project 1:

1. **Create a VPN Gateway**: Navigate to Network **Connectivity** > **VPN**.
2. Select **High Availability (HA) VPN**
   HA VPN is an advanced VPN solution designed to provide higher reliability, availability, and performance compared to standard VPN setups. Its features, such as redundancy, automatic failover, and load balancing, make it an ideal choice for enterprises and applications that require continuous, high-quality connectivity and enhanced fault tolerance.
3. Enter a **Name** for the VPN (e.g., `vpn-gateway-project-1`).
4. **Network**: Select the VPC network you have created in the previous step (e.g., `vpc-project-1`).
5. **Region**: Choose the region where your VPC is located (e.g., `us-central1`).



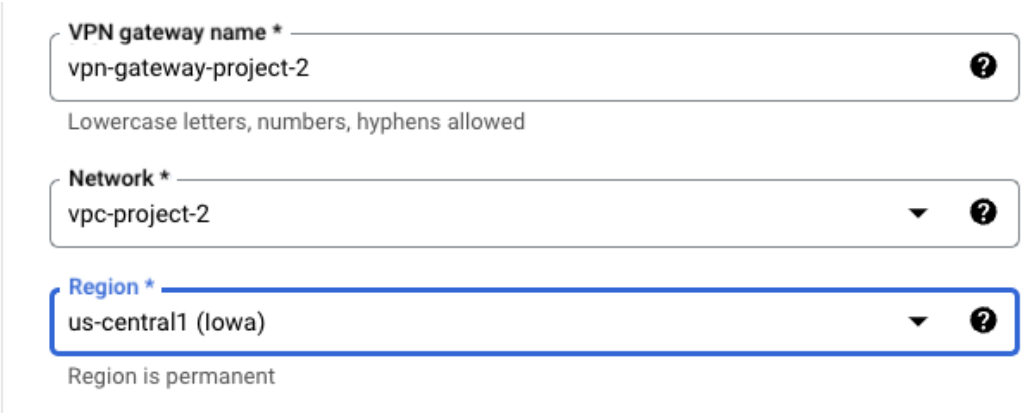
6. Click **Create**.

Project 2:

1. **Select Project 2:** Switch to the second project from the project dropdown.
2. Select **High Availability (HA) VPN**
   HA VPN is an advanced VPN solution designed to provide higher reliability, availability, and performance compared to standard VPN setups. Its features, such as redundancy,

automatic failover, and load balancing, make it an ideal choice for enterprises and applications that require continuous, high-quality connectivity and enhanced fault tolerance.

3. Enter a **Name** for the VPN (e.g., `vpn-gateway-project-2`).
4. **Network**: Select the VPC network you have created in the previous step (e.g., `vpc-project-2`).
5. **Region**: Choose the region where your VPC is located (e.g., us-central1).

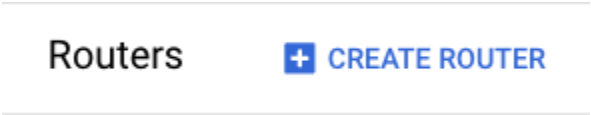


6. Click **Create**.

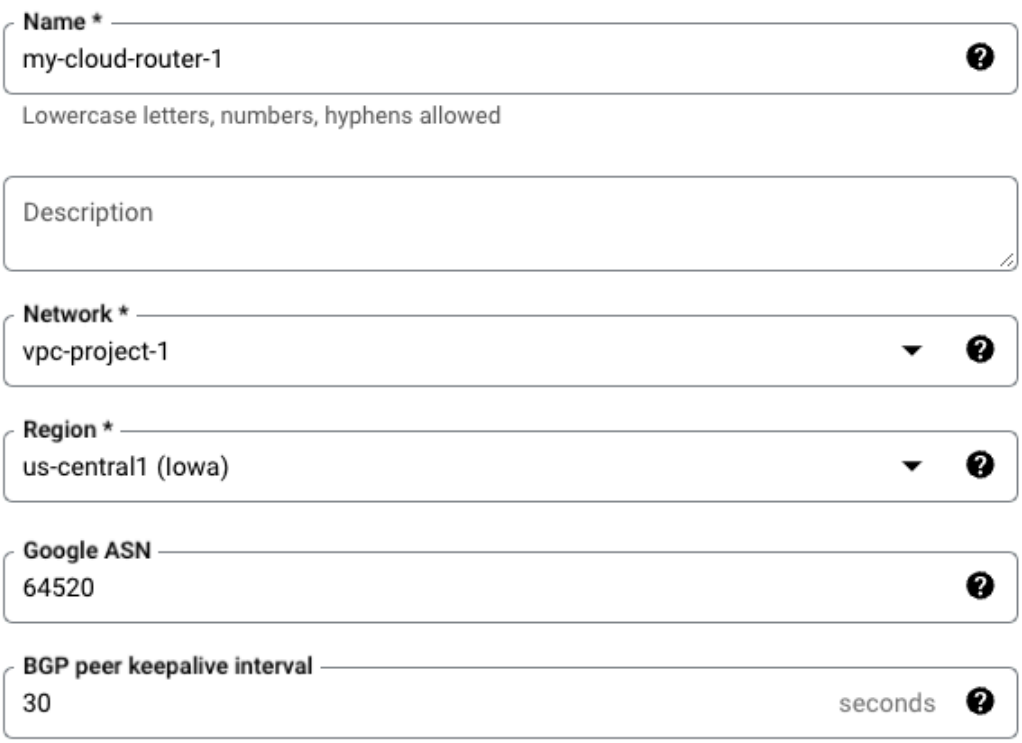
Create Cloud Routers:

Project 1:

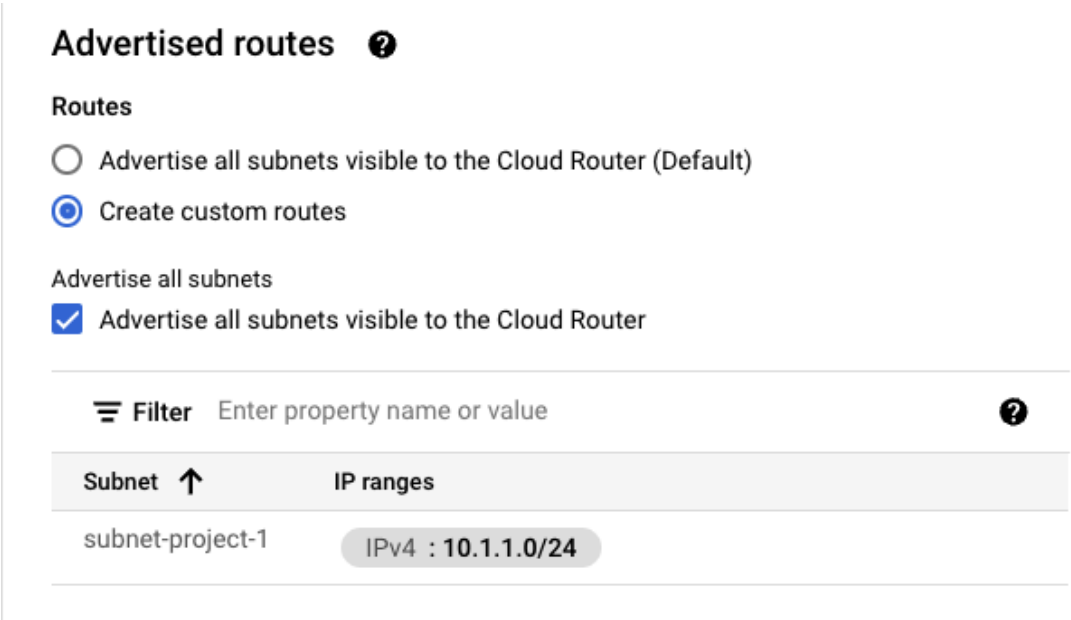
Under **Cloud Router**, click on create cloud router.



- Name: Enter a name for your Cloud Router (e.g., my-cloud-router-1).
- Network: Select the VPC network where the router will be associated (e.g., vpc-project-1).
- Region: Choose the region where you want the Cloud Router to be located (e.g., us-central1).
- A **Google ASN** for the new router (e.g., 64520)



- Under advertised routes, create custom routes and select to advertise all subnets.

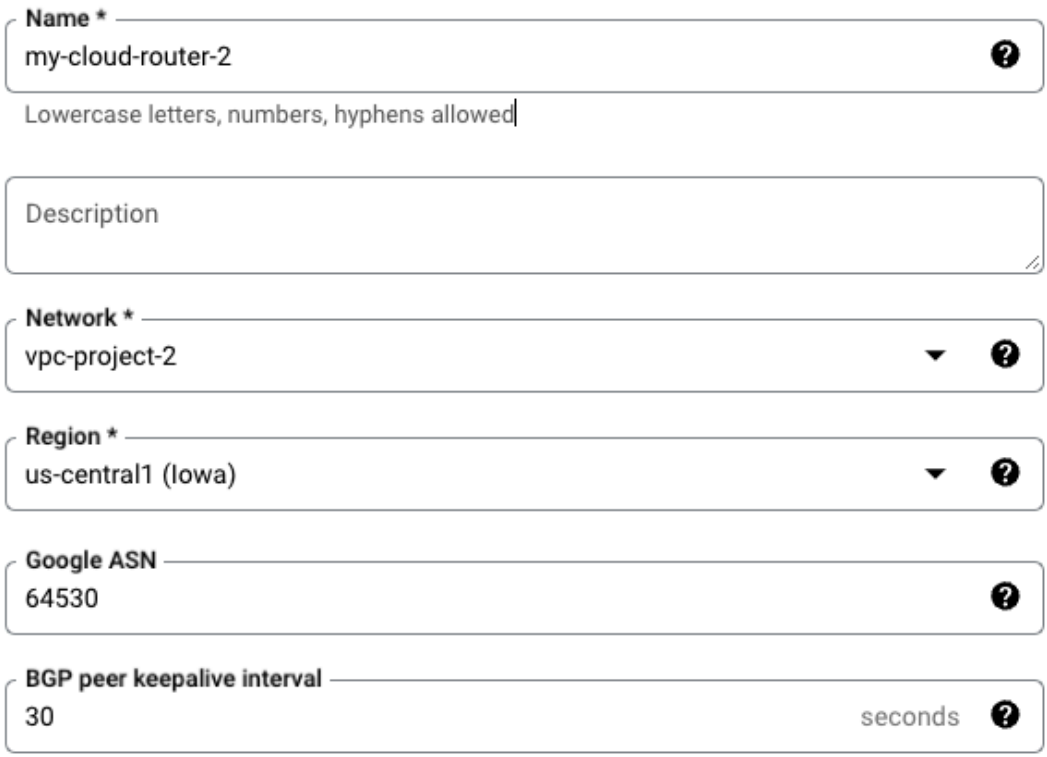


- Click **Create**.

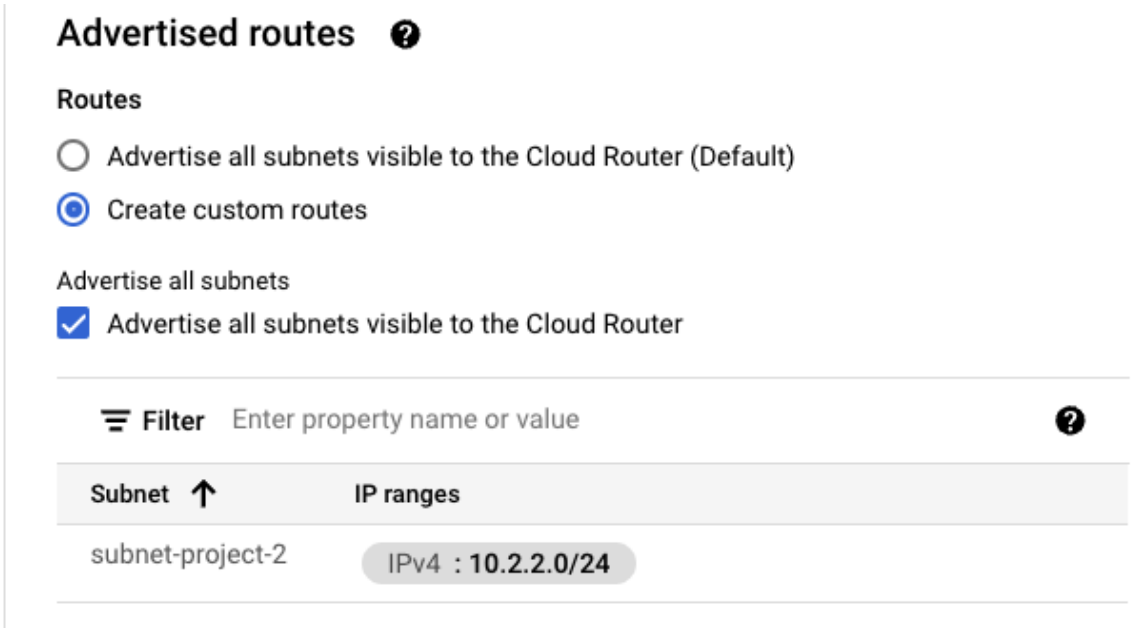
Project 2:

Under **Cloud Router**, click on create cloud router.

- Name: Enter a name for your Cloud Router (e.g., my-cloud-router-2).
- Network: Select the VPC network where the router will be associated (e.g., vpc-project-2).
- Region: Choose the region where you want the Cloud Router to be located (e.g., us-central1).
- A **Google ASN** for the new router (e.g., 64530)



- Under advertised routes, create custom routes and select to advertise all subnets.

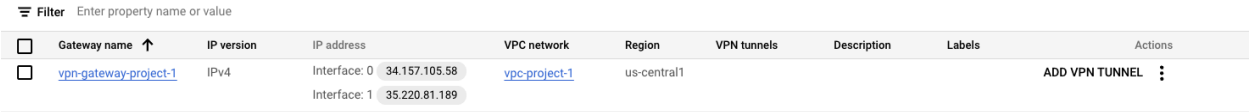


- Click **Create**.

Add VPN Tunnel:

Project 1:

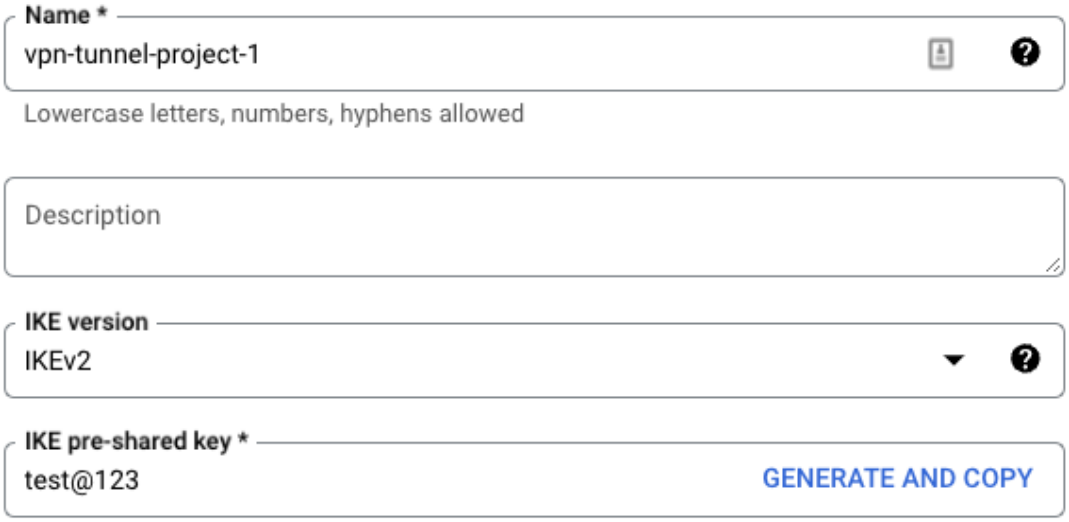
- Go to VPN Gateway and select add VPN Tunnel



- Under peer VPN gateway, select the option Google Cloud VPN Gateway.
- Select the Peer Project, Network Region and the VPC

- Select the router created in project 1 (my-cloud-router-1)

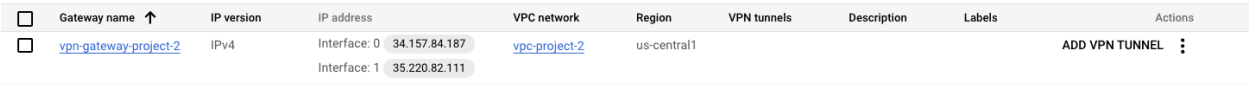
- Name: Enter a name for the tunnel (e.g., vpn-tunnel-project-1).
- IKE Version: Choose IKEv2
- Shared Secret: Enter a shared secret (e.g., test@123).



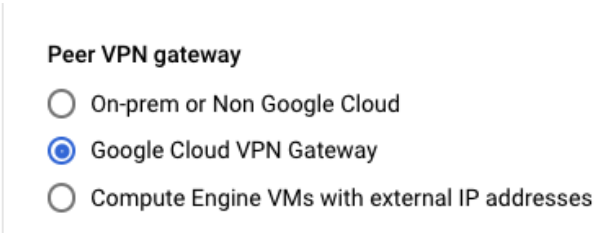
- Click on Create

Project 2:

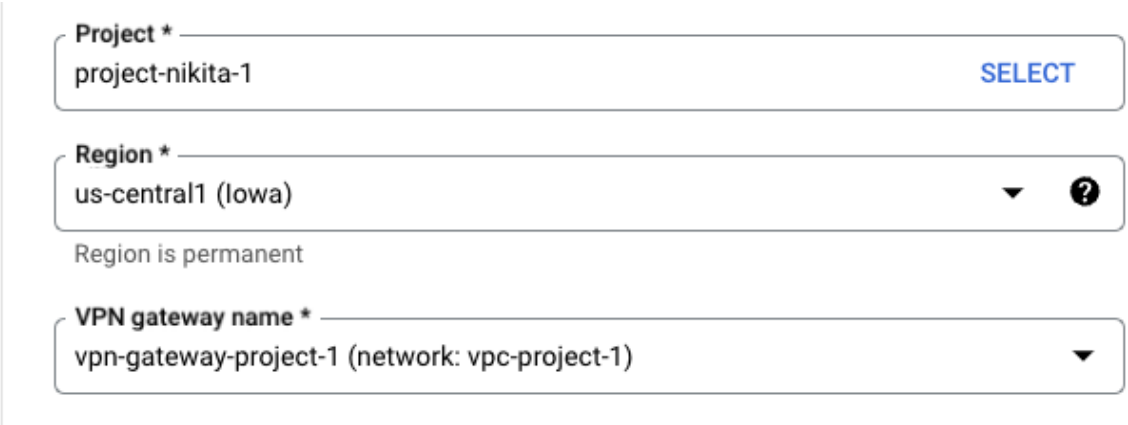
- Go to VPN Gateway and select add VPN Tunnel



- Under peer VPN gateway, select the option Google Cloud VPN Gateway.
- Select the Peer Project, Network Region and the VPC

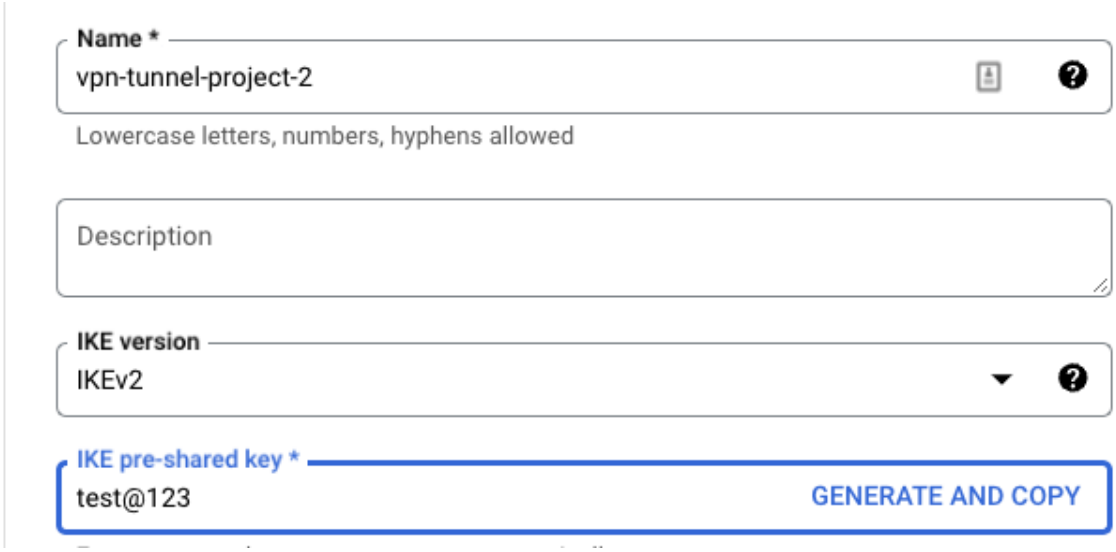


- Select the Peer Project, Network Region and the VPC



- Select the router created in project 2 (my-cloud-router-2)

- Name: Enter a name for the tunnel (e.g., vpn-tunnel-project-2).
- IKE Version: Choose IKEv2
- Shared Secret: Enter a shared secret (e.g., test@123).



- Click on Create.

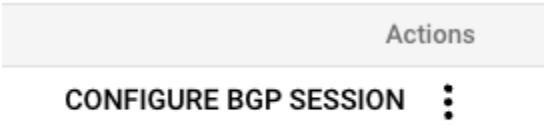
Verify if Tunnel Connection is established in both projects:

Name	Cloud VPN gateway (IP)	Peer VPN gateway (IP)	Cloud Router BGP IP address	Peer BGP IP address	VPN tunnel status
vpn-tunnel-project-1	vpn-gateway-project-1 34.157.105.58	vpn-gateway-project-2 (project: project-nikita-2) 34.157.84.187	--	--	Established

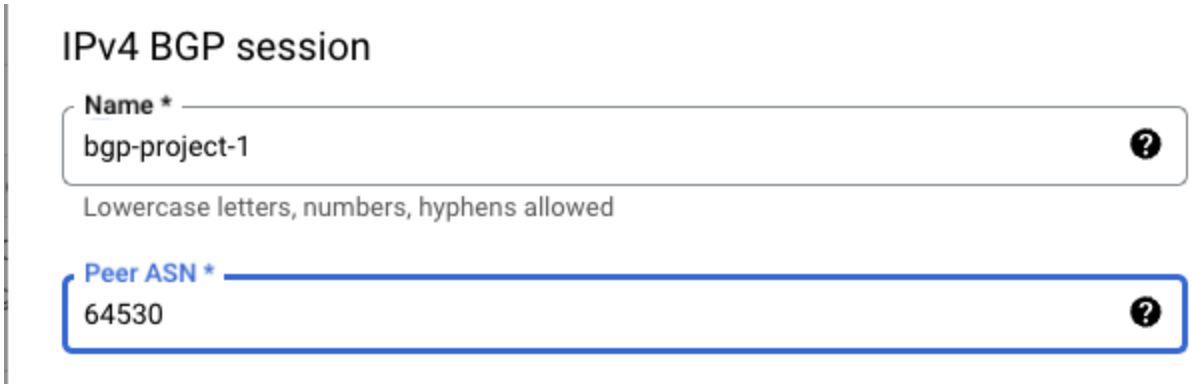
Name	Cloud VPN gateway (IP)	Peer VPN gateway (IP)	Cloud Router BGP IP address	Peer BGP IP address	VPN tunnel status
vpn-tunnel-project-2	vpn-gateway-project-2 34.157.84.187	vpn-gateway-project-1 (project: project-nikita-1) 34.157.105.58	--	--	Established

Once done, configure BGP session for the VPN tunnel as below:

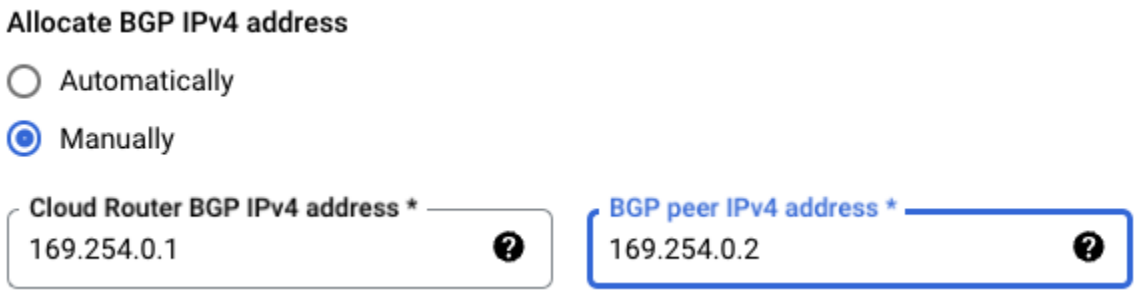
Project 1:
Select Project 1
Navigate to VPN gateway
Click on configure BGP session



Enter the BGP name (bgp-project-1)
Update the Peer ASN

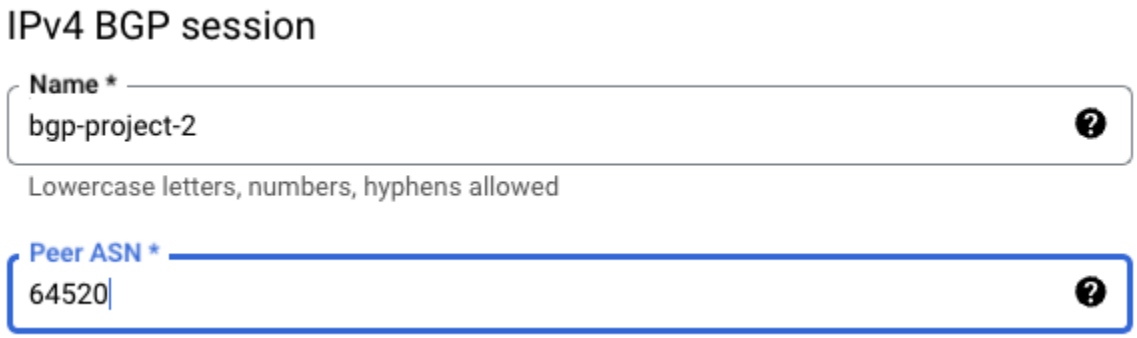


Under Allocate BGP IPv4 address, select the manual option and update the IP address.



Click on save.

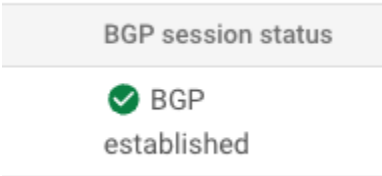
Project 2:
Select Project 2
Navigate to VPN gateway
Click on configure BGP session
Enter the BGP name (bgp-project-2)
Update the Peer ASN



Under Allocate BGP IPv4 address, select the manual option and update the IP address.

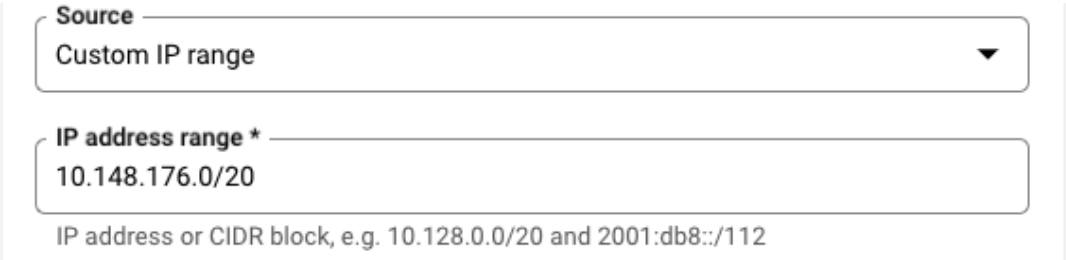
Click on save.

Refresh the page and verify that the BGP session is established in both projects:



NOTE:

- Ensure that you update the correct source and target ASN values in the BGP for the connection to establish.
- Ensure that you update the BGP custom route with MYSQL private IP range - this is to route the traffic to the MYSQL instance - We have to explicitly mention the IP range. Go to the VPC network peering tab in VPC Network



- To export the custom route, navigate to VPC network peering → Check the Export Route option → and click save. This is to initiate the route