

# 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`).

---



Name \*

Lowercase letters, numbers, hyphens allowed

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

Subnet creation mode ?

☒ Custom

☐ Automatic

Add a subnet:

Name: `subnet-project-1`

Region: Select the region (e.g., `us-central1`).

IP Address range: `10.1.1.0/24`

^

New subnet

Name \*

subnet-project-1

?

Lowercase letters, numbers, hyphens allowed

Description

Region \*

us-central1

▼

?

IP stack type

☒ IPv4 (single-stack)

☐ IPv4 and IPv6 (dual-stack) 

?

IPv4 range \*

10.1.1.0/24

?

E.g. 10.0.0.0/24

CREATE SECONDARY IPV4 RANGE

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`).

Name \*

vpc-project-2



Lowercase letters, numbers, hyphens allowed

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

Subnet creation mode ?

☒ Custom

☐ Automatic

Add a subnet:

Name: **subnet-project-2**

Region: Select the region (e.g., **us-central1**).

IP Address range: **10.2.2.0/24**

## ^ New subnet



Name \*

subnet-project-2



Lowercase letters, numbers, hyphens allowed

Description

Region \*

us-central1



IP stack type

☒ IPv4 (single-stack)

☐ IPv4 and IPv6 (dual-stack) ?

IPv4 range \*

10.2.2.0/24



E.g. 10.0.0.0/24

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`).

The screenshot shows a configuration form for a VPN gateway. It contains three input fields, each with a label, a value, a dropdown arrow, and a help icon (question mark). The first field is labeled 'VPN gateway name \*' and contains the text 'vpn-gateway-project-1'. Below it is a note: 'Lowercase letters, numbers, hyphens allowed'. The second field is labeled 'Network \*' and contains the text 'vpc-project-1'. The third field is labeled 'Region \*' and contains the text 'us-central1 (Iowa)'. Below it is a note: 'Region is permanent'.

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`).

The screenshot shows a configuration form for a VPN gateway. It has three main sections, each with a label, a text input field, and a help icon (question mark). The first section is 'VPN gateway name \*' with the value 'vpn-gateway-project-2' and a note 'Lowercase letters, numbers, hyphens allowed'. The second section is 'Network \*' with a dropdown menu showing 'vpc-project-2'. The third section is 'Region \*' with a dropdown menu showing 'us-central1 (Iowa)' and a note 'Region is permanent'.

VPN gateway name \*  
vpn-gateway-project-2 ?  
Lowercase letters, numbers, hyphens allowed

Network \*  
vpc-project-2 ▼ ?

Region \*  
us-central1 (Iowa) ▼ ?  
Region is permanent

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`)

**Name \***  ?

Lowercase letters, numbers, hyphens allowed

**Description**

**Network \***  ▼ ?

**Region \***  ▼ ?

**Google ASN**  ?

**BGP peer keepalive interval**  seconds ?

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

## Advertised routes ?

### Routes

- ☐ Advertise all subnets visible to the Cloud Router (Default)
- ☒ Create custom routes

### Advertise all subnets

- ☒ Advertise all subnets visible to the Cloud Router

Filter <input type="text" value="Enter property name or value"/> ?	
Subnet ↑	IP ranges
subnet-project-1	IPv4 : 10.1.1.0/24

- 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**)

**Name \***  
my-cloud-router-2 ?  
Lowercase letters, numbers, hyphens allowed

Description

**Network \***  
vpc-project-2 ▼ ?

**Region \***  
us-central1 (Iowa) ▼ ?

**Google ASN**  
64530 ?

**BGP peer keepalive interval**  
30 seconds ?

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

## Advertised routes ?

### Routes

☐ Advertise all subnets visible to the Cloud Router (Default)


☒ Create custom routes

### Advertise all subnets

☒ Advertise all subnets visible to the Cloud Router

 Filter Enter property name or value



Subnet 

IP ranges

subnet-project-2

IPv4 : 10.2.2.0/24



- Click **Create**.

## Add VPN Tunnel:

### Project 1:

- Go to VPN Gateway and select add VPN Tunnel

 Filter Enter property name or value

<input type="checkbox"/>	Gateway name 	IP version	IP address	VPC network	Region	VPN tunnels	Description	Labels	Actions
<input type="checkbox"/>	<a href="#">vpn-gateway-project-1</a>	IPv4	Interface: 0 34.157.105.58 Interface: 1 35.220.81.189	<a href="#">vpc-project-1</a>	us-central1				ADD VPN TUNNEL 

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



### Peer VPN gateway

- ☐ On-prem or Non Google Cloud
- ☒ Google Cloud VPN Gateway
- ☐ Compute Engine VMs with external IP addresses



Make sure you created a VPN gateway in the Google Cloud project that you want to connect.

Project \*

project-nikita-2

SELECT

Region \*

us-central1 (Iowa)



Region is permanent

VPN gateway name \*

vpn-gateway-project-2 (network: vpc-project-2)



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

Cloud Router \*

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**).

Name \*

vpn-tunnel-project-1



Lowercase letters, numbers, hyphens allowed

Description

IKE version

IKEv2



IKE pre-shared key \*

test@123

GENERATE AND COPY

- Click on Create

## Project 2:

- Go to VPN Gateway and select add VPN Tunnel

<input type="checkbox"/>	Gateway name ↑	IP version	IP address	VPC network	Region	VPN tunnels	Description	Labels	Actions
<input type="checkbox"/>	<a href="#">vpn-gateway-project-2</a>	IPv4	Interface: 0 34.157.84.187 Interface: 1 35.220.82.111	<a href="#">vpc-project-2</a>	us-central1				ADD VPN TUNNEL ⋮

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

### Peer VPN gateway

- ☐ On-prem or Non Google Cloud  
☒ Google Cloud VPN Gateway  
☐ Compute Engine VMs with external IP addresses

- Select the Peer Project, Network Region and the VPC

**Project \***  
 project-nikita-1 SELECT

**Region \***  
 us-central1 (Iowa) ▼ ?  
 Region is permanent

**VPN gateway name \***  
 vpn-gateway-project-1 (network: vpc-project-1) ▼



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

**Cloud Router \***  
 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](#)).

Name \*

vpn-tunnel-project-2






Lowercase letters, numbers, hyphens allowed

Description

IKE version

IKEv2

IKE pre-shared key \*

test@123

GENERATE AND COPY

- Click on Create.

Verify if Tunnel Connection is established in both projects:

<input type="checkbox"/>	Name ↑	Cloud VPN gateway (IP)	Peer VPN gateway (IP)	Cloud Router BGP IP address	Peer BGP IP address	VPN tunnel status
<input type="checkbox"/>	<a href="#">vpn-tunnel-project-1</a>	<a href="#">vpn-gateway-project-1</a> 34.157.105.58	vpn-gateway-project-2 (project: project-nikita-2) 34.157.84.187	--	--	Established

<input type="checkbox"/>	Name ↑	Cloud VPN gateway (IP)	Peer VPN gateway (IP)	Cloud Router BGP IP address	Peer BGP IP address	VPN tunnel status
<input type="checkbox"/>	<a href="#">vpn-tunnel-project-2</a>	<a href="#">vpn-gateway-project-2</a> 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

Actions

CONFIGURE BGP SESSION

Enter the BGP name (bgp-project-1)

Update the Peer ASN

## IPv4 BGP session

Name \*

bgp-project-1



Lowercase letters, numbers, hyphens allowed

Peer ASN \*

64530



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

### Allocate BGP IPv4 address

☐ Automatically

☒ Manually

Cloud Router BGP IPv4 address \*

169.254.0.1



BGP peer IPv4 address \*

169.254.0.2



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

## IPv4 BGP session

Name \*

bgp-project-2



Lowercase letters, numbers, hyphens allowed

Peer ASN \*

64520



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

☒ Manually

Cloud Router BGP IPv4 address \*

169.254.0.2



BGP peer IPv4 address \*

169.254.0.1



Click on save.

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

#### BGP session status



BGP  
established

#### 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

Source

Custom IP range



IP address range \*

10.148.176.0/20

IP address or CIDR block, e.g. 10.128.0.0/20 and 2001:db8::/112

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

#### Exchange IPv4 custom routes

You can choose to import or export static and dynamic routes over the VPC peering connection



Import custom routes



Export custom routes