# Lab Guide for Introduce Compute Services from GCP

## CONTENTS

### Day-6 Assignments

## Contents

*Context*

This document contains assignments to be completed as part of the hands on session for the course

*Guidelines*

- The lab guide has been designed to give hands on experience to map the concepts learnt in the theory session with real life business oriented case studies/assignments.

***Day-6 Assignments***

## *Assignment 1: Create a VPC network with custom subnets*

***Highlights:***

*Virtual Private Cloud is a global resource.*

*Subnets are limited to regions*

*Routes in VPC networks are applicable within the project.*

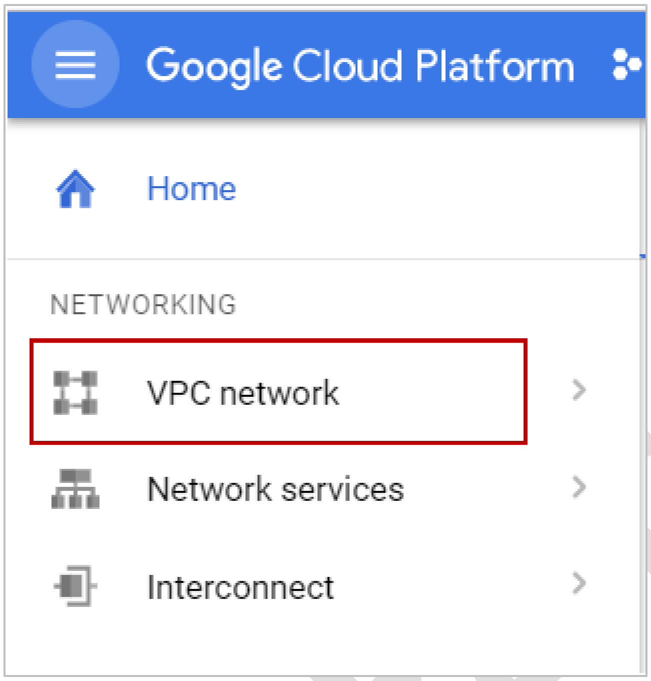
*Demo steps:*

*Panchama wants to configure network and subnet to create a private cloud topology in GCP in which instances under VPC can also access GCP products and services.*

*VPC creation using Google cloud platform console*

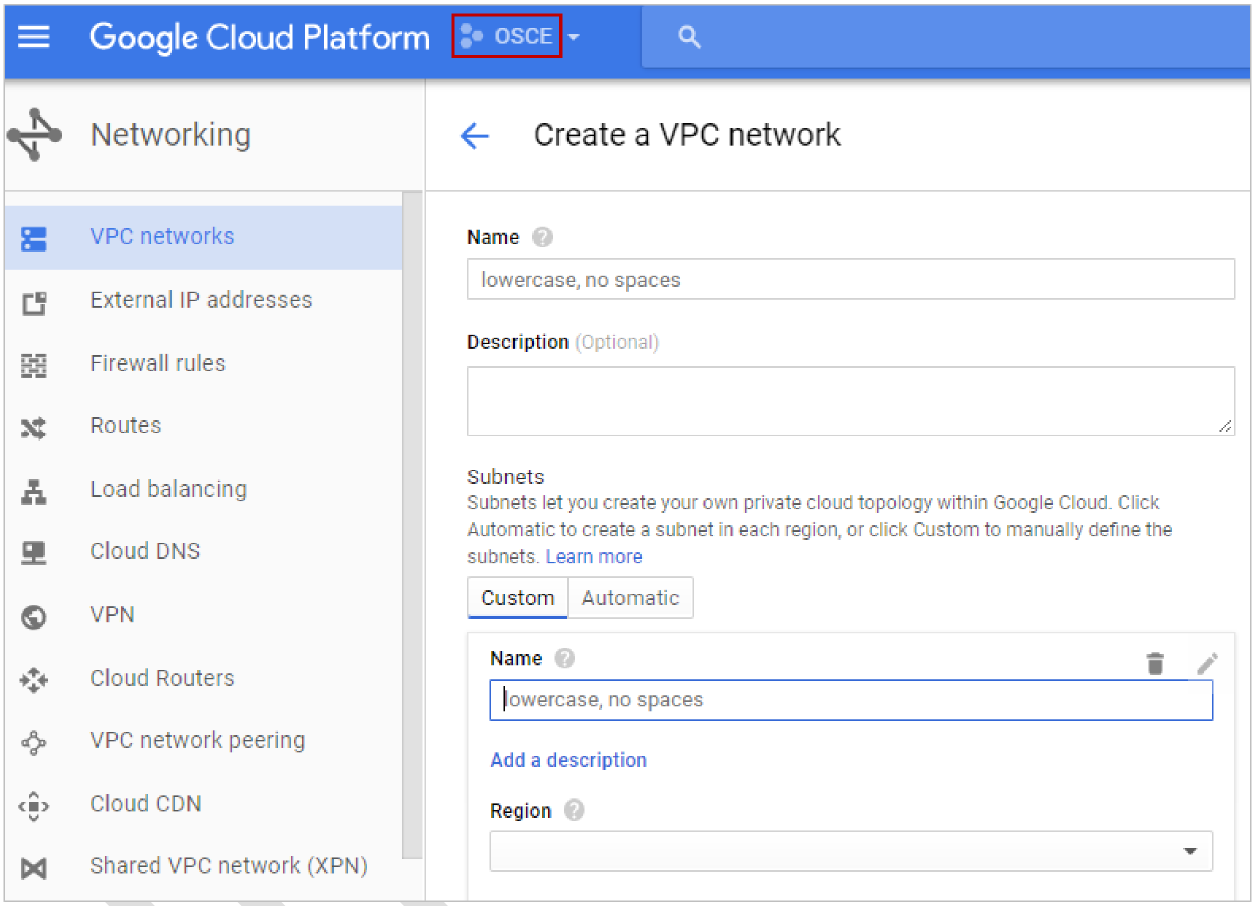
*Step 1:*

*Navigate to VPC network under Networking in google cloud platform console as shown below:*



***Step 2:***

*Select **VPC networks** of project **OSCE** as shown below.*



Create a VPC network

Name: lowercase, no spaces

Description (Optional)

Subnets

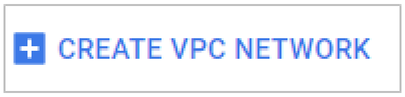
Subnets let you create your own private cloud topology within Google Cloud. Click Automatic to create a subnet in each region, or click Custom to manually define the subnets. Learn more

Name: lowercase, no spaces

Region

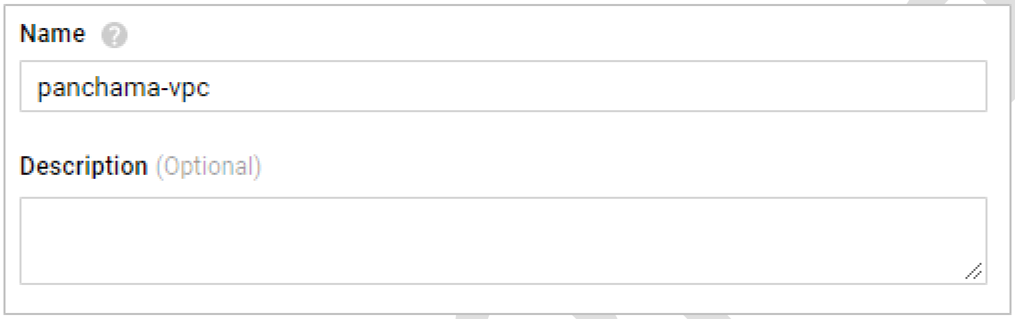
***Step 3:***

*Click on **Create VPC network** in the VPC networks dashboard.*



***Step 4: Describe network***

*Give a unique name to network as shown below.*



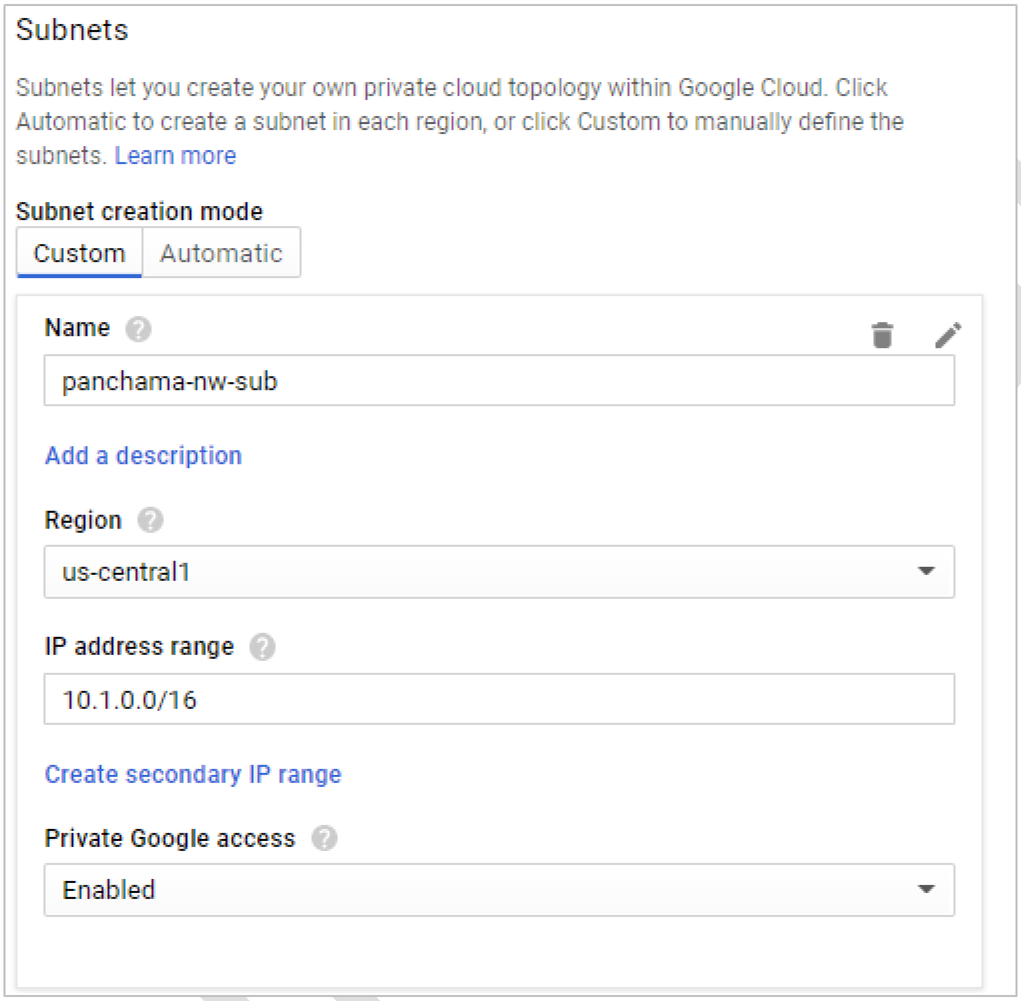
Name

panchama-vpc

Description (Optional)

***Step 5:***

*Define subnet by providing the following values as shown below.*



Subnets

Subnets let you create your own private cloud topology within Google Cloud. Click Automatic to create a subnet in each region, or click Custom to manually define the subnets. Learn more

Subnet creation mode

Name: panchama-nw-sub

Region: us-central1

IP address range: 10.1.0.0/16

Private Google access: Enabled

***Name:*** *Provide a unique name to subnet.*

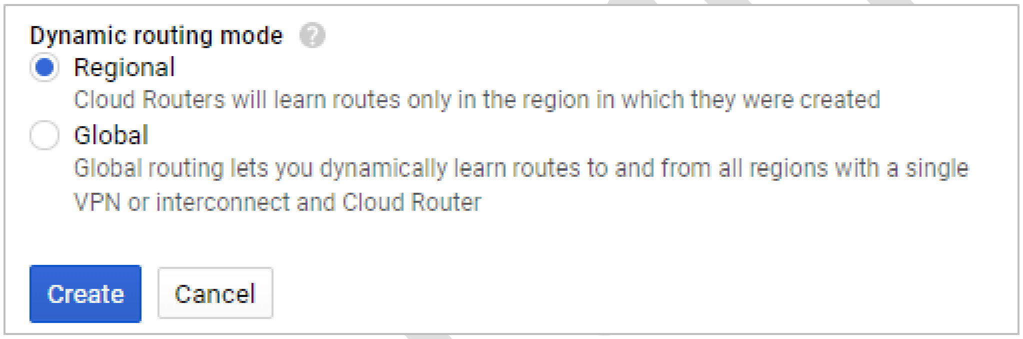
***Region:*** *Panchama has decided to deploy their application in North America as their region. Hence selected the nearest proximity region of "us-central1".*

***IP address:*** *Choose an IP address range in Classless Inter-Domain Routing(CIDR) notation.*

***Private Google Access:*** *Enabling accessibility of instance for Google services without setting external IP address.*

***Step 6:***

*Select **Dynamic Routing** mode as Regional and click create as shown below.*

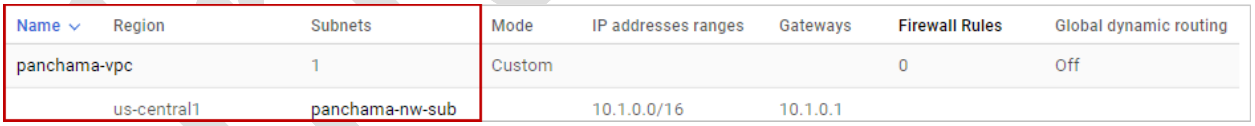


Dynamic routing mode

● Regional
Cloud Routers will learn routes only in the region in which they were created

○ Global
Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router

*You can **verify the custom network and subnet** by navigating to VPC networks page.*



| Name | Region | Subnets | Mode | IP addresses ranges | Gateways | Firewall Rules | Global dynamic routing |
|---|---|---|---|---|---|---|---|
| panchama-vpc | | 1 | Custom | | | 0 | Off |
| | us-central1 | panchama-nw-sub | | 10.1.0.0/16 | 10.1.0.1 | | |

*At this point, the network has routes to the internet and to any instances. To enable the connectivity for the resources in VPCs, appropriate firewall rules to be added.*

*In next section, you will learn how to add firewall to secure your VPC configuration.*

## *Assignment 2: Adding firewall rule and instance within the secure network*

***Highlights:***

*Firewall rules are added to dedicated network in the project*

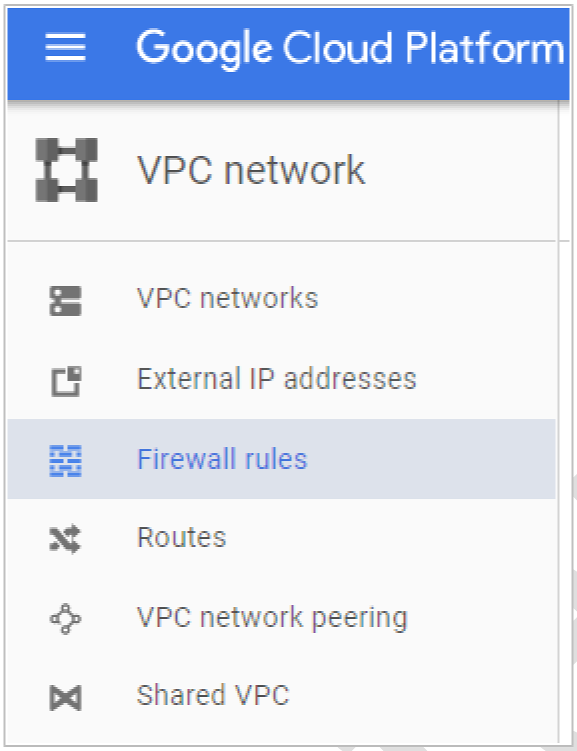
*Default rules are created for auto-type networks*

*Demo steps:*

*Firewalls let you to determine the traffic that can be allowed or denied to or from instances based on IP addresses, protocols and ports. In our demonstration, will add SSH protocol to enable connectivity for the instance inside VPC network.*

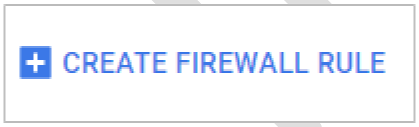
*Step 1:*

*Navigate to the VPC networks and select "firewall rules" as shown below.*



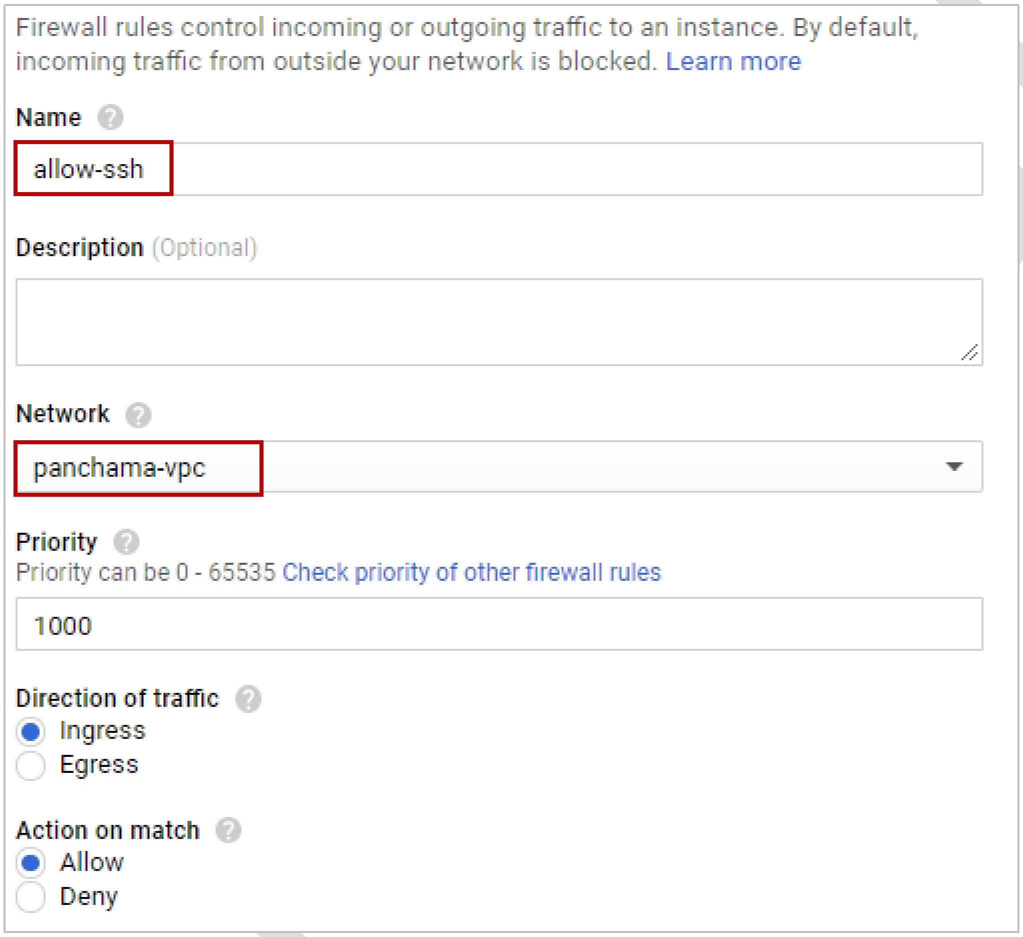
***Step 2:***

*Click on* ***create firewall rule*** *as shown*



***Step 3:***

*Provide unique name to Firewall and select Panchama's Network as mentioned below.*



Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. Learn more

Name: allow-ssh

Description (Optional)

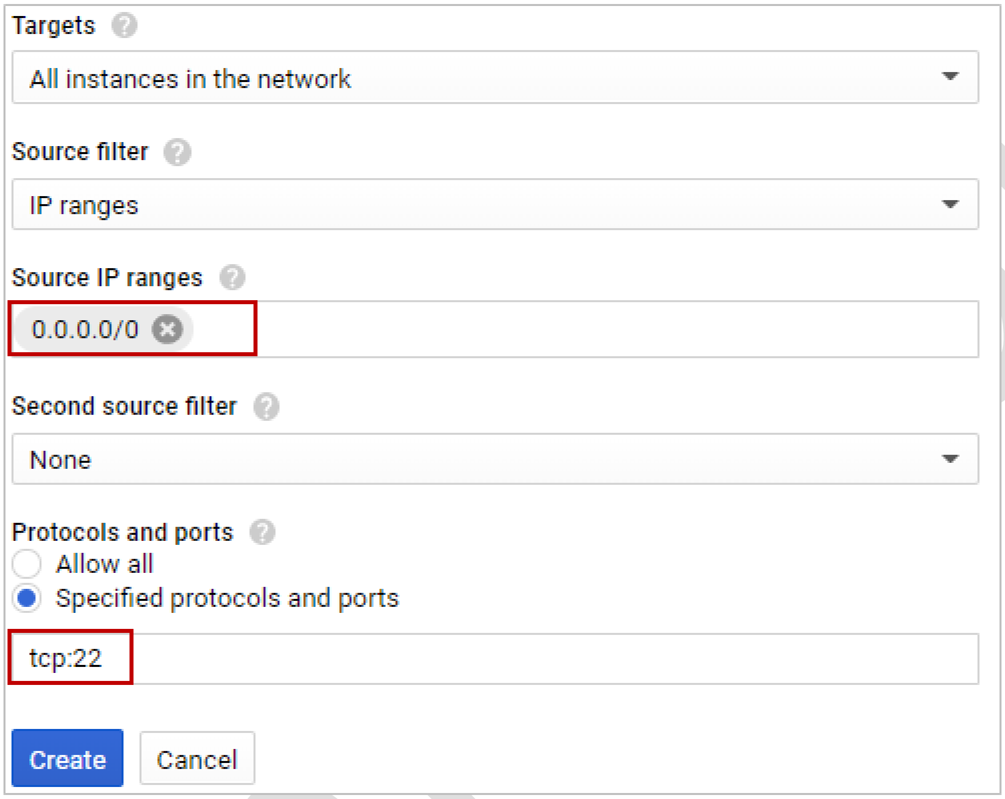
Network: panchama-vpc

Priority
Priority can be 0 - 65535 Check priority of other firewall rules

1000

Direction of traffic
● Ingress
○ Egress

Action on match
● Allow
○ Deny



Targets

All instances in the network

Source filter

IP ranges

Source IP ranges

0.0.0.0/0

Second source filter

None

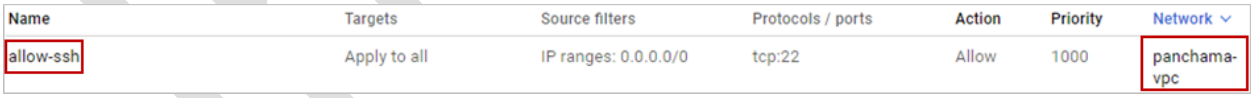
Protocols and ports

○ Allow all

● Specified protocols and ports

tcp:22

*Upon creation, you can verify the protocol in firewall rules page.*



| Name | Targets | Source filters | Protocols / ports | Action | Priority | Network |
|---|---|---|---|---|---|---|
| allow-ssh | Apply to all | IP ranges: 0.0.0.0/0 | tcp:22 | Allow | 1000 | panchama-vpc |

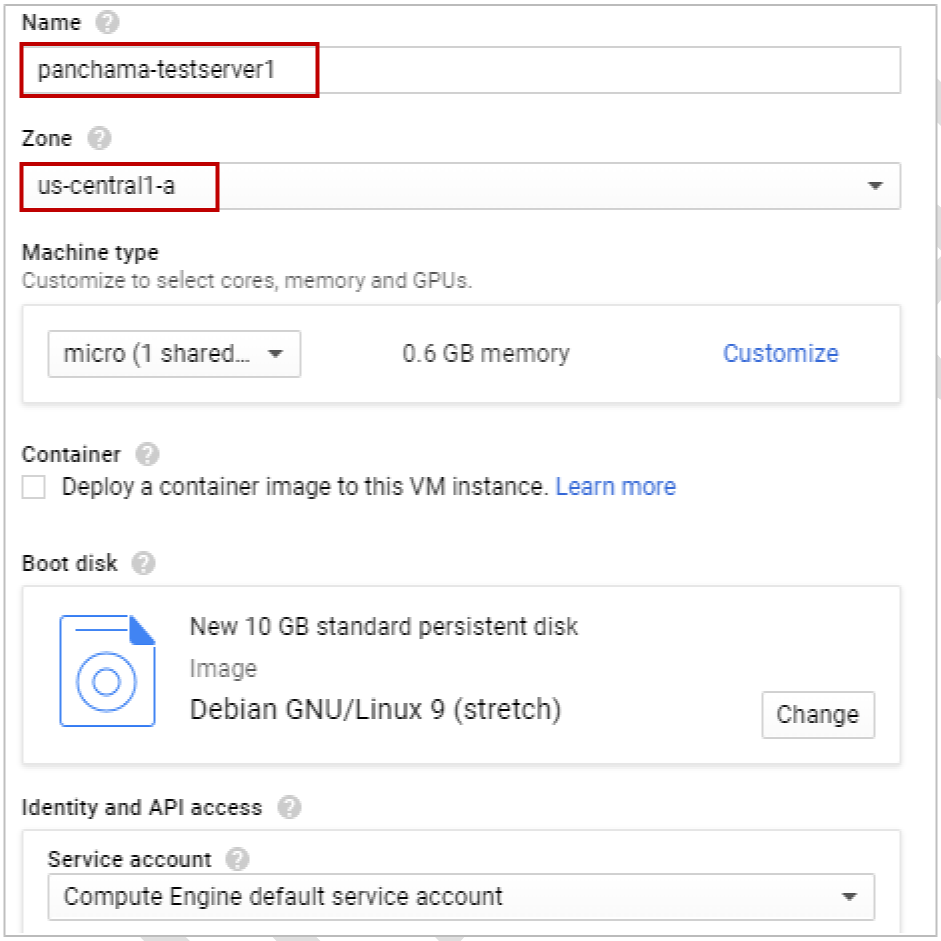
*To verify the connectivity, Panchama wants to deploy the resources inside VPC.*

***Instance** is to be created in your desired project by selecting the custom netwok under "Management, disk, Networking, access and security"*

***Step 4:***

*Navigate to **Compute Engine** and create instance by specifying below details.*

*1. Provide valid name and select the appropriate zone where your network is established*



Name

panchama-testserver1

Zone

us-central1-a

Machine type

Customize to select cores, memory and GPUs.

micro (1 shared... 0.6 GB memory Customize

Container

□ Deploy a container image to this VM instance. Learn more

Boot disk

New 10 GB standard persistent disk

Image

Debian GNU/Linux 9 (stretch)

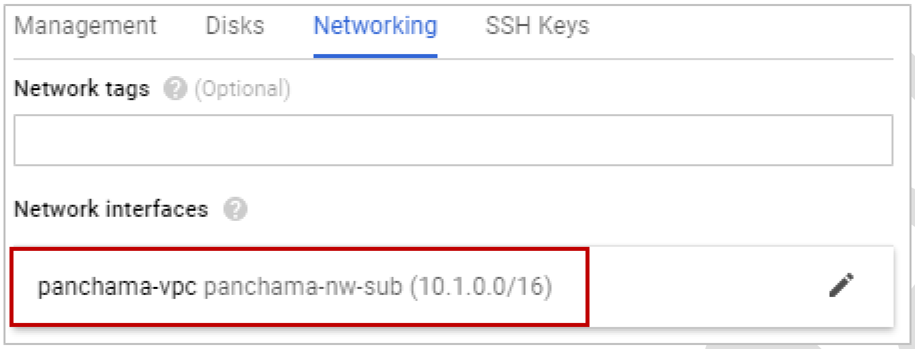
Change

Identity and API access

Service account

Compute Engine default service account

*2. Choose the network, created in the previous steps.*



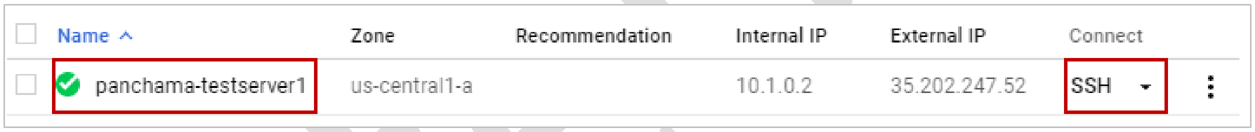
Network tags (Optional)

Network interfaces

panchama-vpc panchama-nw-sub (10.1.0.0/16)

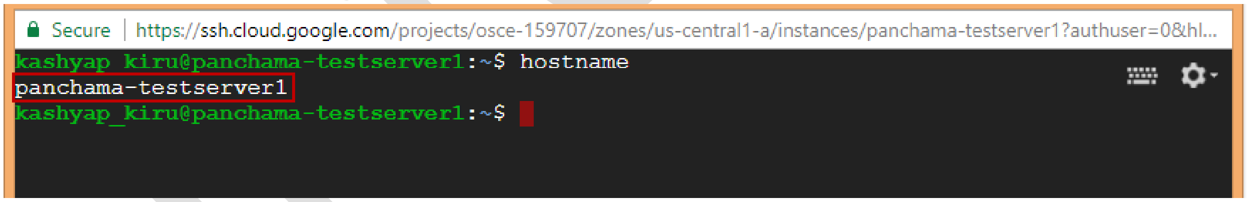
*Step 6:*

*You can verify the instance from instance page as shown below.*



| □ | Name ^ | Zone | Recommendation | Internal IP | External IP | Connect |
|---|---|---|---|---|---|---|
| □ | ✓ panchama-testserver1 | us-central1-a |  | 10.1.0.2 | 35.202.247.52 | SSH ▾ |

*You can connect using console "SSH" and verify the instance as shown below:*



Secure | https://ssh.cloud.google.com/projects/osce-159707/zones/us-central1-a/instances/panchama-testserver1?authuser=0&hl...

```
kashyap_kiru@panchama-testserver1:~$ hostname
panchama-testserver1
kashyap_kiru@panchama-testserver1:~$
```

## *Assignment 3: Creating a network peering connection between two VPCs*

*Objective: In this demonstration, you will learn to create VPC Network Peering connection between two custom mode VPCs.*

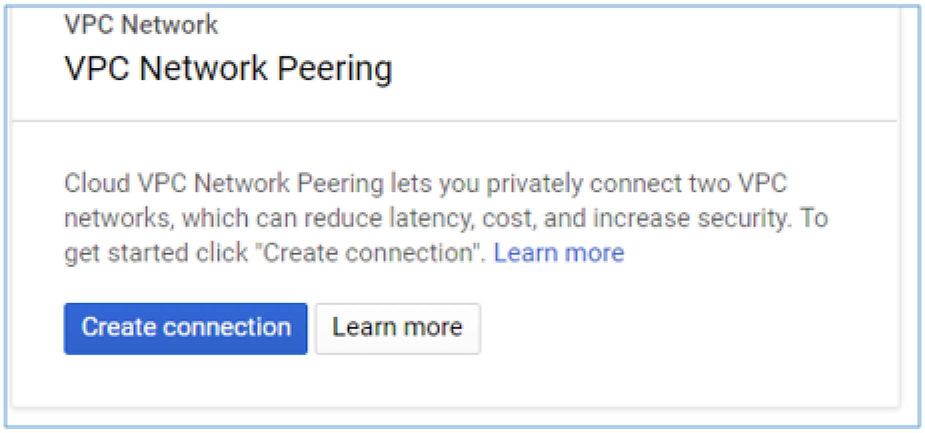
*Create a custom mode VPC with one subnet with the below parameters.*

- *Name of the network: peer-vpc-1*
- *Name of the subnet: public-subnet-1*
- *CIDR: 10.0.0.0/24*

*Create another custom mode VPC with one subnet with the below parameters.*

- *Name of the network: peer-vpc-2*
- *Name of the subnet: public-subnet-2*
- *CIDR: 192.168.0.0/24*

*Navigate to VPC Network Peering in the console and select "Create connection".*

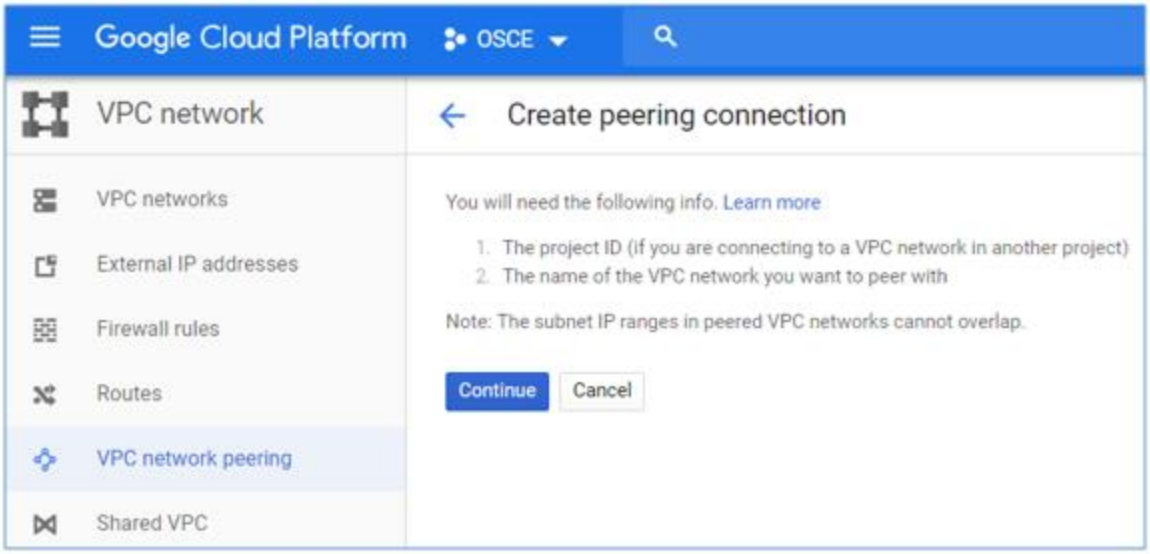


VPC Network

VPC Network Peering

Cloud VPC Network Peering lets you privately connect two VPC networks, which can reduce latency, cost, and increase security. To get started click "Create connection". Learn more

Click “continue”.



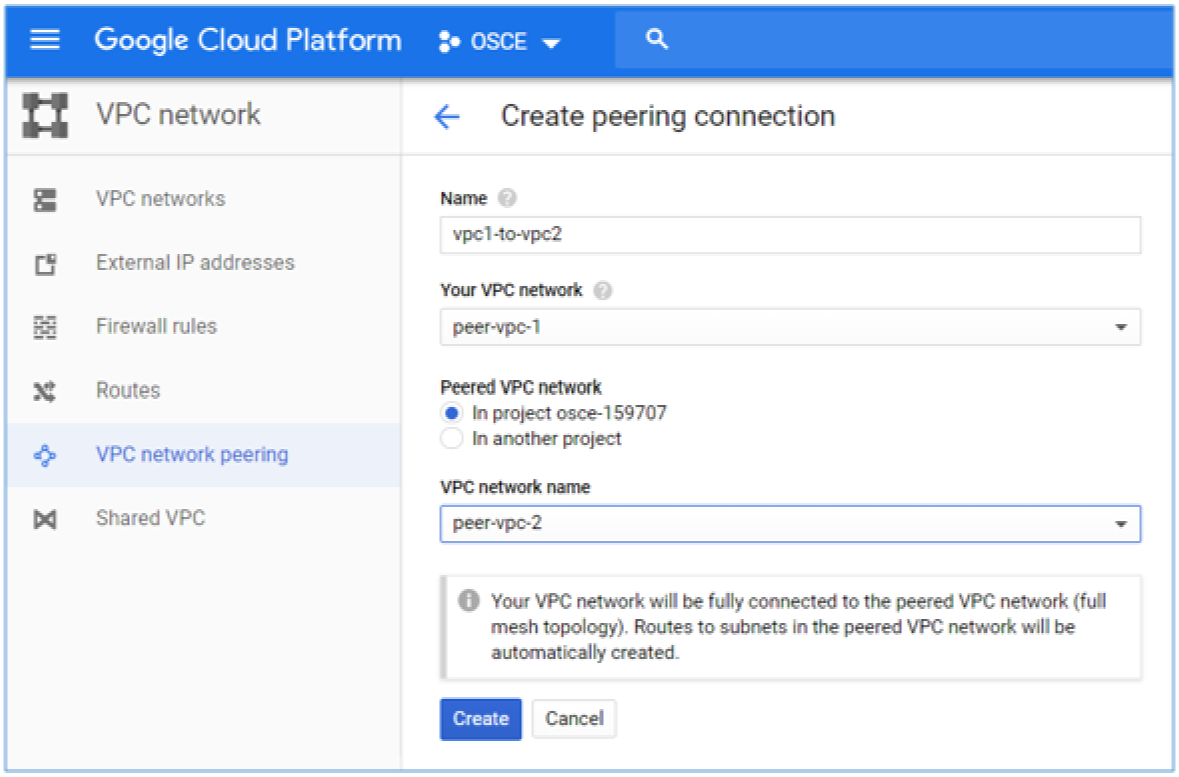
Create peering connection

You will need the following info. Learn more

1. The project ID (if you are connecting to a VPC network in another project)
2. The name of the VPC network you want to peer with

Note: The subnet IP ranges in peered VPC networks cannot overlap.

Create a connection from vpc1-to-vpc2.



Name
vpc1-to-vpc2

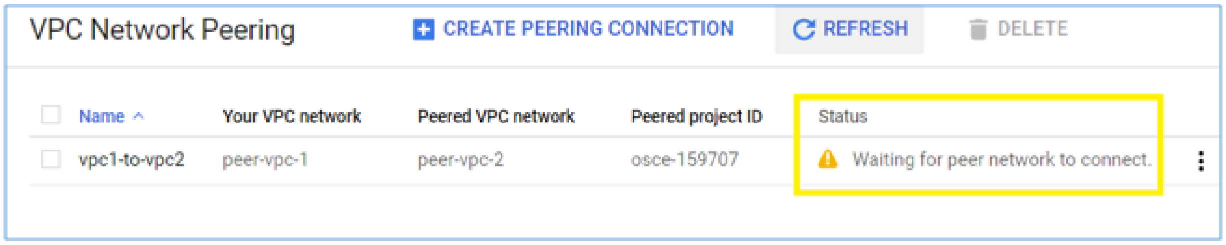
Your VPC network
peer-vpc-1

Peered VPC network
● In project osce-159707
○ In another project

VPC network name
peer-vpc-2

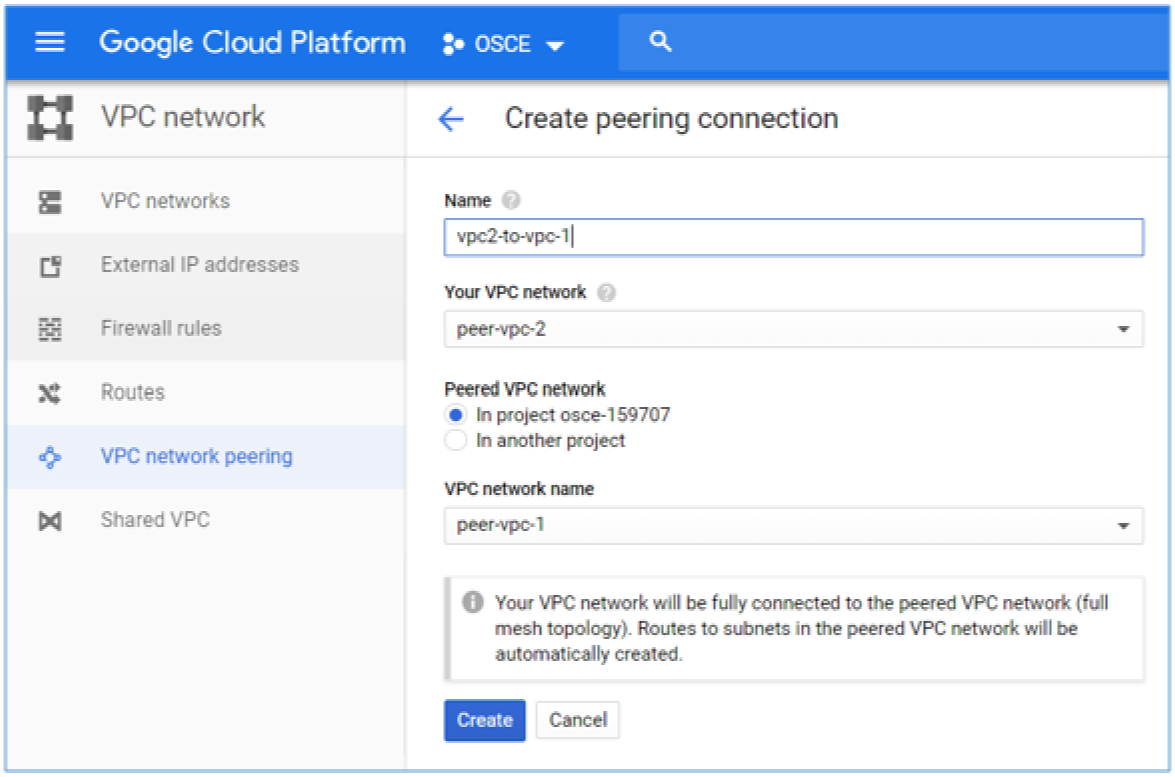
Your VPC network will be fully connected to the peered VPC network (full mesh topology). Routes to subnets in the peered VPC network will be automatically created.

Observer the status of the network peering connection.



| □ | Name ^ | Your VPC network | Peered VPC network | Peered project ID | Status |
|---|---|---|---|---|---|
| □ | vpc1-to-vpc2 | peer-vpc-1 | peer-vpc-2 | osce-159707 | ⚠ Waiting for peer network to connect. |

*Create the peering connection from vpc2-to-vpc1*



Create peering connection

Name: vpc2-to-vpc-1

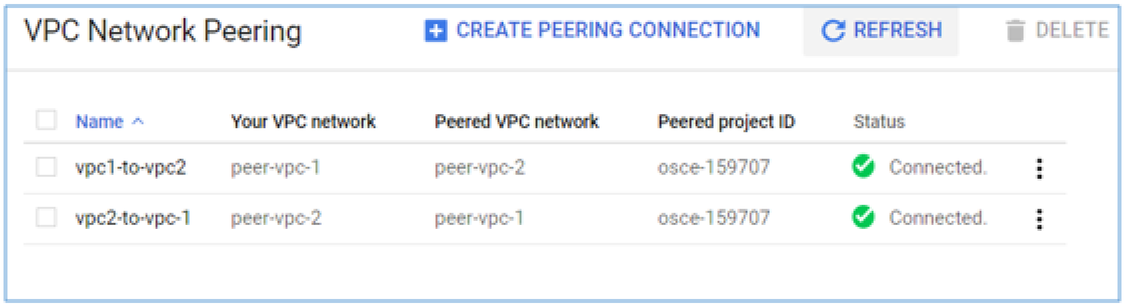
Your VPC network: peer-vpc-2

Peered VPC network
● In project osce-159707
○ In another project

VPC network name: peer-vpc-1

Your VPC network will be fully connected to the peered VPC network (full mesh topology). Routes to subnets in the peered VPC network will be automatically created.

*Now. the connection is complete and successful.*



| □ | Name ^ | Your VPC network | Peered VPC network | Peered project ID | Status | |
|---|---|---|---|---|---|---|
| □ | vpc1-to-vpc2 | peer-vpc-1 | peer-vpc-2 | osce-159707 | ✓ Connected. | ⋮ |
| □ | vpc2-to-vpc-1 | peer-vpc-2 | peer-vpc-1 | osce-159707 | ✓ Connected. | ⋮ |

*Now, the services can be shared between the VPCs.*

*Note: If connection is removed from either side, peering will be disconnected*

***Summary***

*Learnt to establish VPC network peering connection between two VPCs to share the services between them.*

# *Assignment 4: Creating a Google Cloud Virtual Private Network(VPN)*

***Objective:*** *Creating a VPN gateway and a tunnel using static routes in Google Cloud*

***Background: Google Cloud VPN***

*Google Cloud VPN connects your existing network to Google's Network through an IPsec VPN connection which is secure. Traffic between the two networks will be encrypted by one gateway and decrypted by the other VPN which helps your data more protected when it travels over the Internet.*

*With the help of VPN Cloud, connect two different GCP networks or regions.*

***Problem Description:***

*Before you can start coding your first client application, there are a few things you need to do, if you haven't done them already. Using VPN, securely connect your existing network to Compute Engine network over IPsec. It's important to become familiar with Compute Engine basics before you continue here.*

***Estimated time: 15 minutes***

***Solution:***

***Select the GCP network configuration to setup a VPN:***

- ➢ *Based on your GCP network and the number of regions you want to connect, choose from the below options* *i. Simple setup*

*ii. Auto Subnet network using gateway subnet alone*

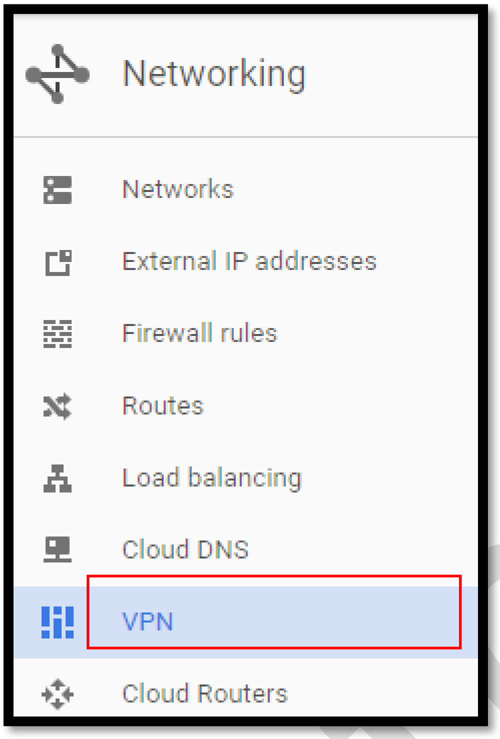
*iii. Auto Subnet network with multiple subnets*

*iv. Custom subnet Network*

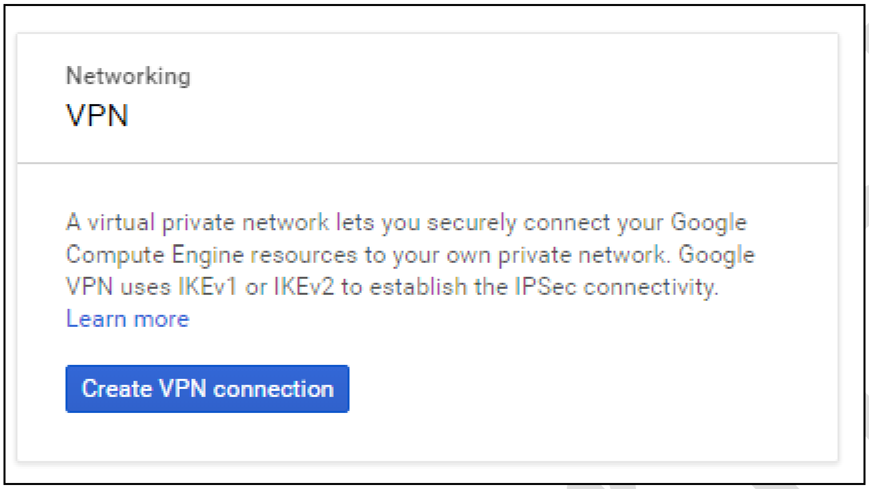
*v. Legacy Network*

*For Demonstration purpose, we are selecting option two and proceeding with the setup*

*Step **1**: Login to the Google Cloud Platform console and select "**VPN**" from the left panel of "**Networking**".*



*Step 2. Click* ***Create VPN connection*** *as below.*



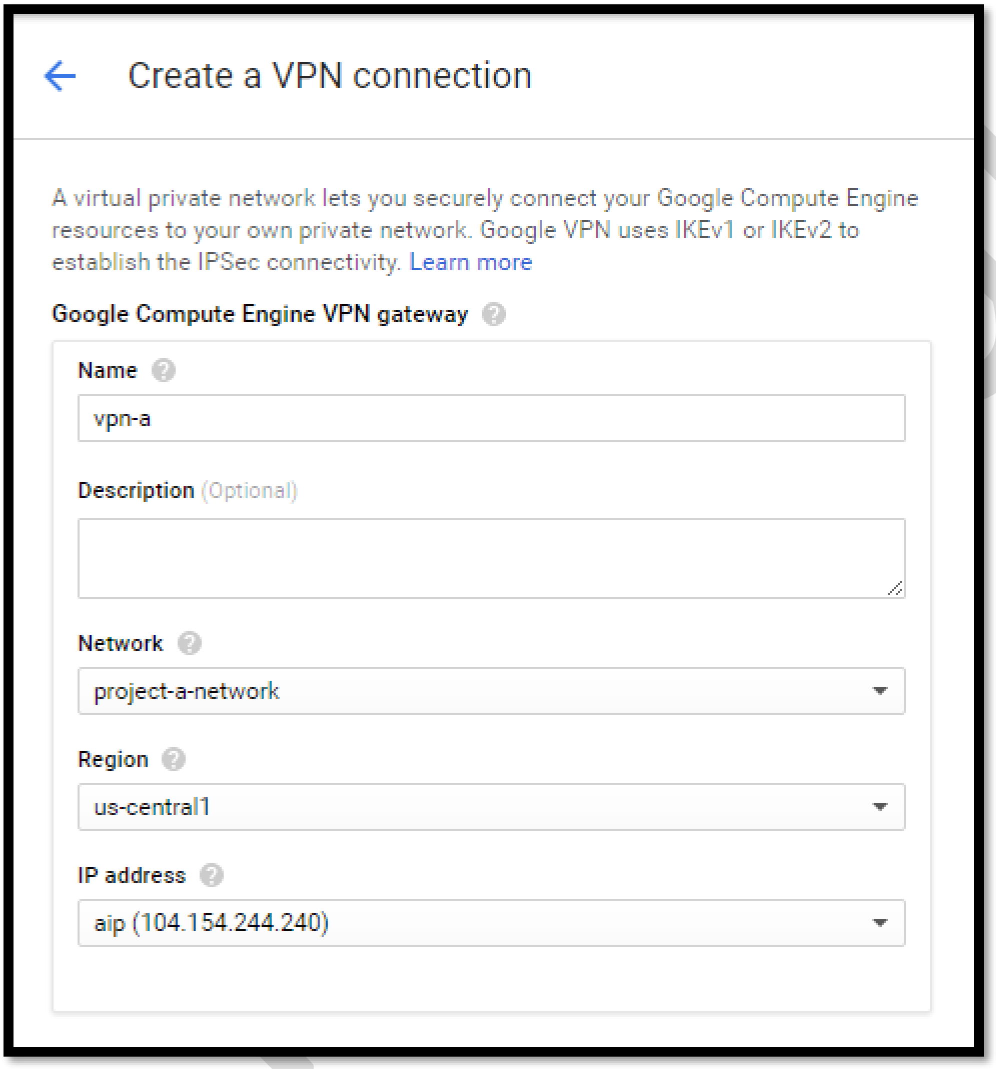
Networking

VPN

A virtual private network lets you securely connect your Google Compute Engine resources to your own private network. Google VPN uses IKEv1 or IKEv2 to establish the IPSec connectivity.

*Step 3: fill the subsequent fields for the gateway.*

- ***Name –*** *VPN Gateway Name which will be showed in the console.*
- ***Network –*** *VPN Gateway will serve based on the* ***Network you have selected*** *which contains the instances*
- ***Region –*** *provide a region to locate your VPN*
- ***IP address –*** *choose* ***New static IP address.***



Create a VPN connection

A virtual private network lets you securely connect your Google Compute Engine resources to your own private network. Google VPN uses IKEv1 or IKEv2 to establish the IPSec connectivity. Learn more

Google Compute Engine VPN gateway

Name: vpn-a

Description (Optional)

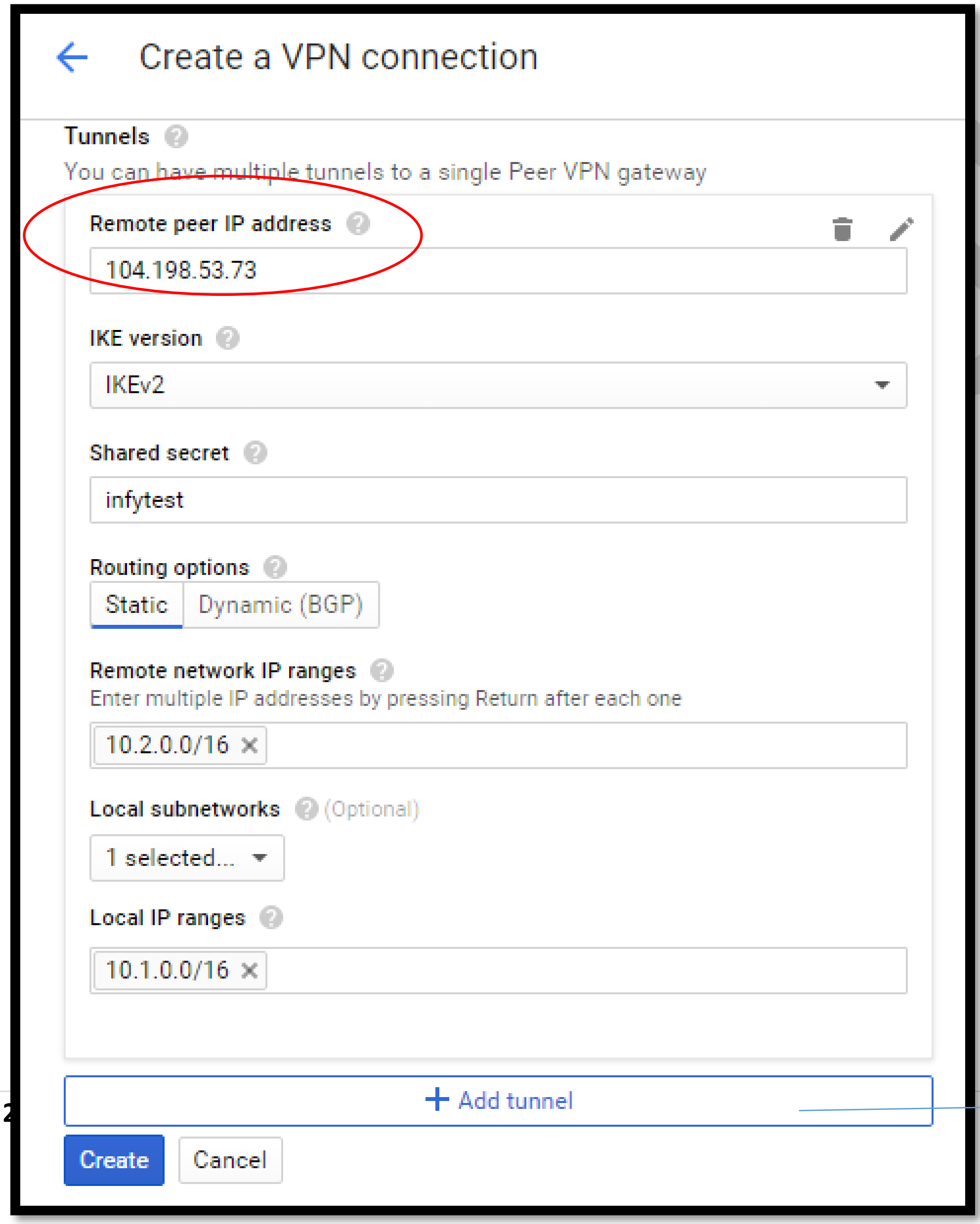
Network: project-a-network

Region: us-central1

IP address: aip (104.154.244.240)

***Step 4**: provide values for few fields at least for one tunnel:*

- ***Peer IP address** —this is the Public IP address of the other end of the tunnel, not the one you are currently configuring. (this is a physical device on your premises)*
- ***IKE version** — IKEv2 is ideal one to choose, however IKEv1 is supported only if all the peer gateway can manage*
- ***Shared secret** — you should provide the same shared secret into both VPN gateways for establishing encryption with that tunnel. If the other side of the tunnel doesn't generate one automatically, you can create one up.*
- ***Remote network IP range** — it is the peer network IP ranges. Remote network is on the other side of the tunnel from the Cloud VPN gateway*
- ***Local subnetworks** — States which IP ranges will be routed through the tunnel. Once the tunnel is created, you cannot change this value since it is used in IKE handshake.*
    - *Choose the gateway's entire subnet in the pull-down menu, or you can leave it empty since the local subnet is default one*
    - *Leave **Local IP ranges** empty apart from the gateway's subnet.*
- *Select **Create tab** to create Gateway and initiate all tunnels*



Create a VPN connection

**Tunnels**

You can have multiple tunnels to a single Peer VPN gateway

Remote peer IP address: 104.198.53.73

IKE version: IKEv2

Shared secret: infytest

Routing options: Static | Dynamic (BGP)

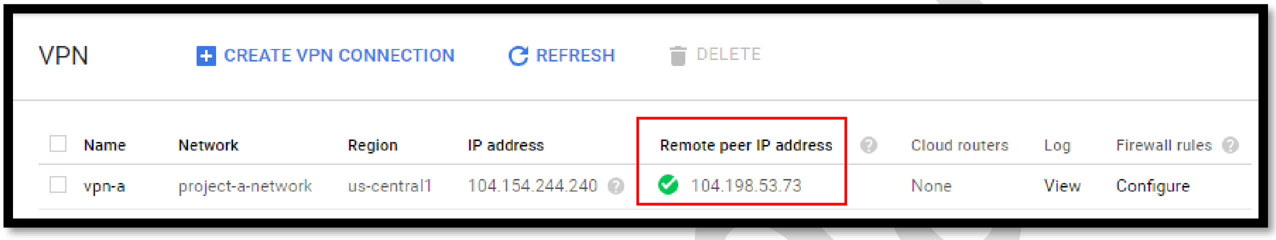
Remote network IP ranges
Enter multiple IP addresses by pressing Return after each one
10.2.0.0/16 ×

Local subnetworks (Optional): 1 selected...

Local IP ranges: 10.1.0.0/16 ×

Select **Add tunnel** only if you need to add extra

*Green checkmark for your VPN denotes that the setup is completed successfully.*



VPN | ➕ CREATE VPN CONNECTION | ⟳ REFRESH | DELETE

| □ | Name | Network | Region | IP address | Remote peer IP address | Cloud routers | Log | Firewall rules |
|---|---|---|---|---|---|---|---|---|
| □ | vpn-a | project-a-network | us-central1 | 104.154.244.240 | ✓ 104.198.53.73 | None | View | Configure |

**Note:** You need to configure Firewall rules so that tunnel will get connected

***Summary of this assignment:*** *In this assignment, you have understood about the creation of VPN connection with a gateway and a tunnel.*

***Assignment 7b: Creating a Google Cloud Virtual Private Network(VPN)***

***Objective:*** *Creating a VPN gateway and a tunnel using static routes in Google Cloud*

***Background: Google Cloud VPN***

*Google Cloud VPN connects your existing network to Google's Network through an IPsec VPN connection which is secure. Traffic between the two networks will be encrypted by one gateway and decrypted by the other VPN which helps your data more protected when it travels over the Internet.*

*With the help of VPN Cloud, connect two different GCP networks or regions.*

***Problem Description:***

*Before you can start coding your first client application, there are a few things you need to do, if you haven't done them already. Using VPN, securely connect your existing network to Compute Engine network over IPsec. It's important to become familiar with Compute Engine basics before you continue here.*

***Estimated time: 15 minutes***

***Solution:***

***Select the GCP network configuration to setup a VPN:***

- *Based on your GCP network and the number of regions you want to connect, choose from the below options*

  vi. *Simple setup*

  vii. *Auto Subnet network using gateway subnet alone*

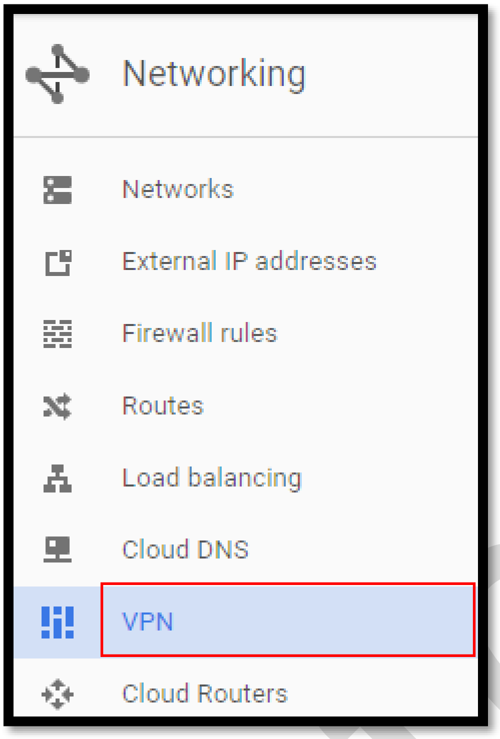
  viii. *Auto Subnet network with multiple subnets*

ix. *Custom subnet Network*

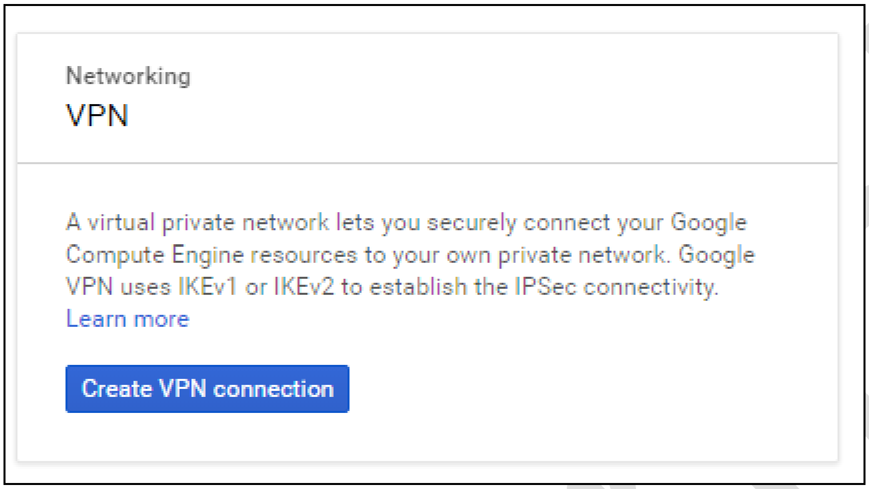
x. *Legacy Network*

*For Demonstration purpose, we are selecting option two and proceeding with the setup*

*Step **1**: Login to the Google Cloud Platform console and select "**VPN**" from the left panel of "**Networking**".*



*Step 2. Click* ***Create VPN connection*** *as below.*



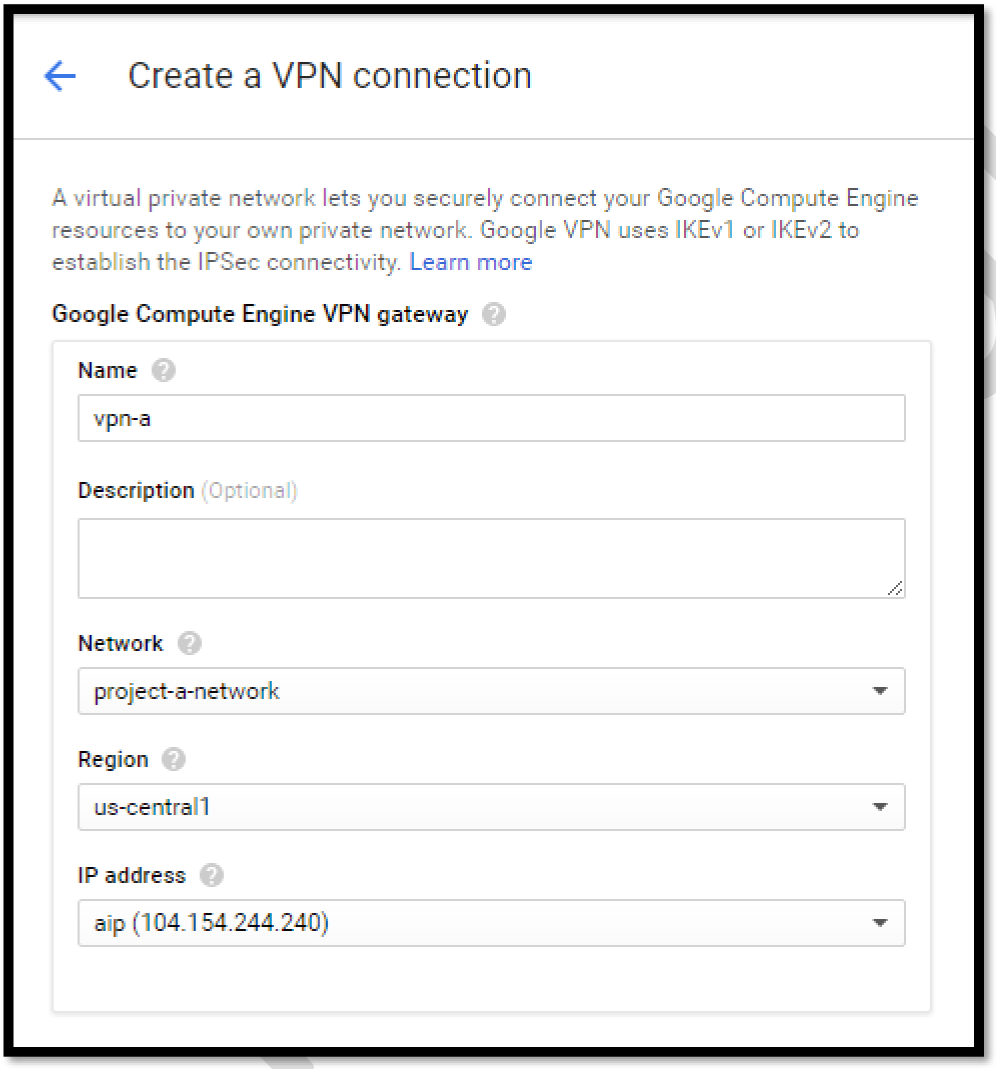
Networking

VPN

A virtual private network lets you securely connect your Google Compute Engine resources to your own private network. Google VPN uses IKEv1 or IKEv2 to establish the IPSec connectivity.
Learn more

*Step 3: fill the subsequent fields for the gateway.*

- ***Name –*** *VPN Gateway Name which will be showed in the console.*
- ***Network –*** *VPN Gateway will serve based on the* ***Network you have selected*** *which contains the instances*
- ***Region –*** *provide a region to locate your VPN*
- ***IP address –*** *choose* ***New static IP address.***



Create a VPN connection

A virtual private network lets you securely connect your Google Compute Engine resources to your own private network. Google VPN uses IKEv1 or IKEv2 to establish the IPSec connectivity. Learn more

Google Compute Engine VPN gateway

Name: vpn-a

Description (Optional)

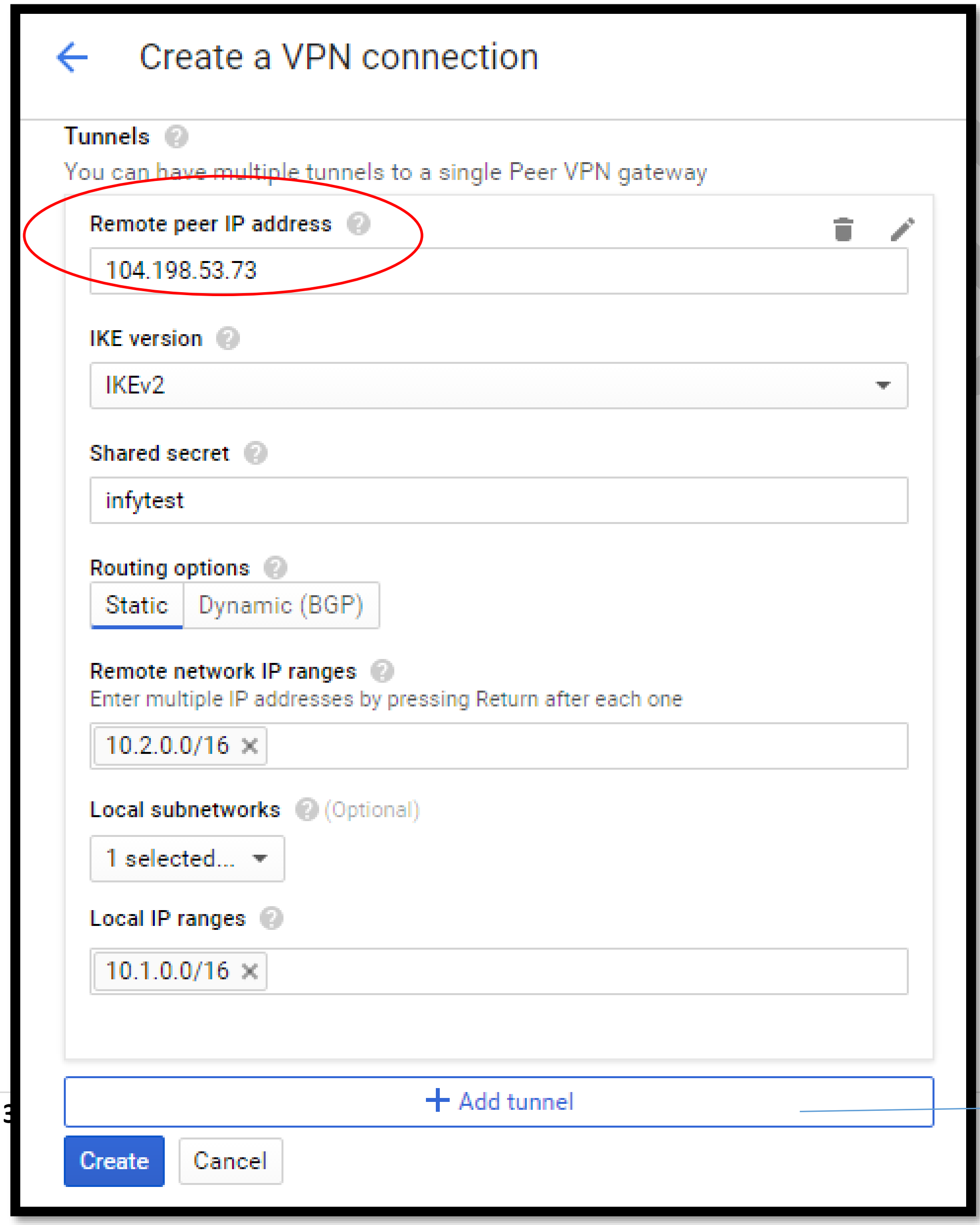
Network: project-a-network

Region: us-central1

IP address: aip (104.154.244.240)

***Step 4**: provide values for few fields at least for one tunnel:*

- ***Peer IP address** —this is the Public IP address of the other end of the tunnel, not the one you are currently configuring. (this is a physical device on your premises)*
- ***IKE version** — IKEv2 is ideal one to choose, however IKEv1 is supported only if all the peer gateway can manage*
- ***Shared secret** — you should provide the same shared secret into both VPN gateways for establishing encryption with that tunnel. If the other side of the tunnel doesn't generate one automatically, you can create one up.*
- ***Remote network IP range** — it is the peer network IP ranges. Remote network is on the other side of the tunnel from the Cloud VPN gateway*
- ***Local subnetworks** — States which IP ranges will be routed through the tunnel. Once the tunnel is created, you cannot change this value since it is used in IKE handshake.*
  - *Choose the gateway's entire subnet in the pull-down menu, or you can leave it empty since the local subnet is default one*
  - *Leave **Local IP ranges** empty apart from the gateway's subnet.*
- *Select **Create tab** to create Gateway and initiate all tunnels*



Create a VPN connection

Tunnels

You can have multiple tunnels to a single Peer VPN gateway

Remote peer IP address: 104.198.53.73

IKE version: IKEv2

Shared secret: infytest

Routing options: [✓ Static] Dynamic (BGP)

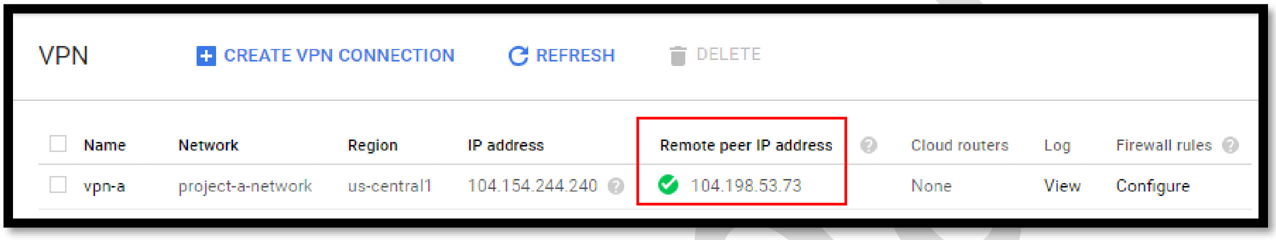
Remote network IP ranges
Enter multiple IP addresses by pressing Return after each one
10.2.0.0/16 ×

Local subnetworks (Optional): 1 selected...

Local IP ranges: 10.1.0.0/16 ×

Select **Add tunnel** only if you need to add extra

*Green checkmark for your VPN denotes that the setup is completed successfully.*



|  | Name | Network | Region | IP address | Remote peer IP address | Cloud routers | Log | Firewall rules |
|---|---|---|---|---|---|---|---|---|
| □ | vpn-a | project-a-network | us-central1 | 104.154.244.240 | ✓ 104.198.53.73 | None | View | Configure |

**Note:** You need to configure Firewall rules so that tunnel will get connected

***Summary of this assignment:*** *In this assignment, you have understood about the creation of VPN connection with a gateway and a tunnel.*