**ADVANCE NETWORKING**

**1.**

**- Create 1 custom VPC network**

**- Create 2 subnets (Private subnets)**

**- Create 1 VM in each subnet. (VM should have only private IPs and no Public IPs)**

**Task:**

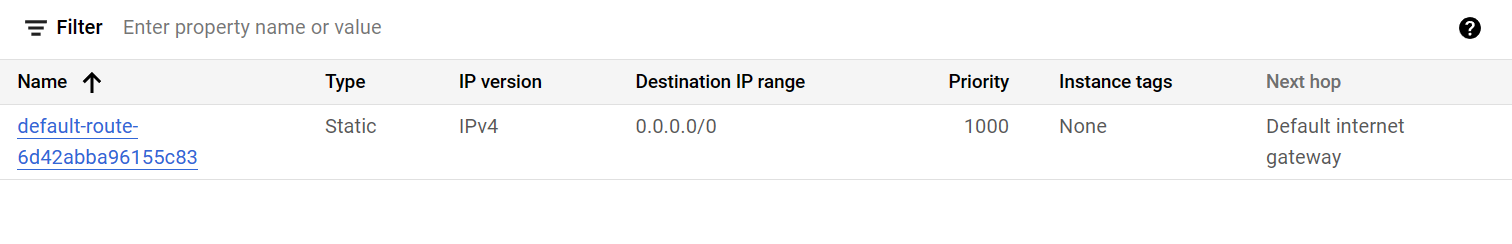
**1. Look at the VPC routes without any subnets in it.**

**2. Look at the VPC routes after subnet creation.**

**3. Look at the VPC route to internet gateway.**

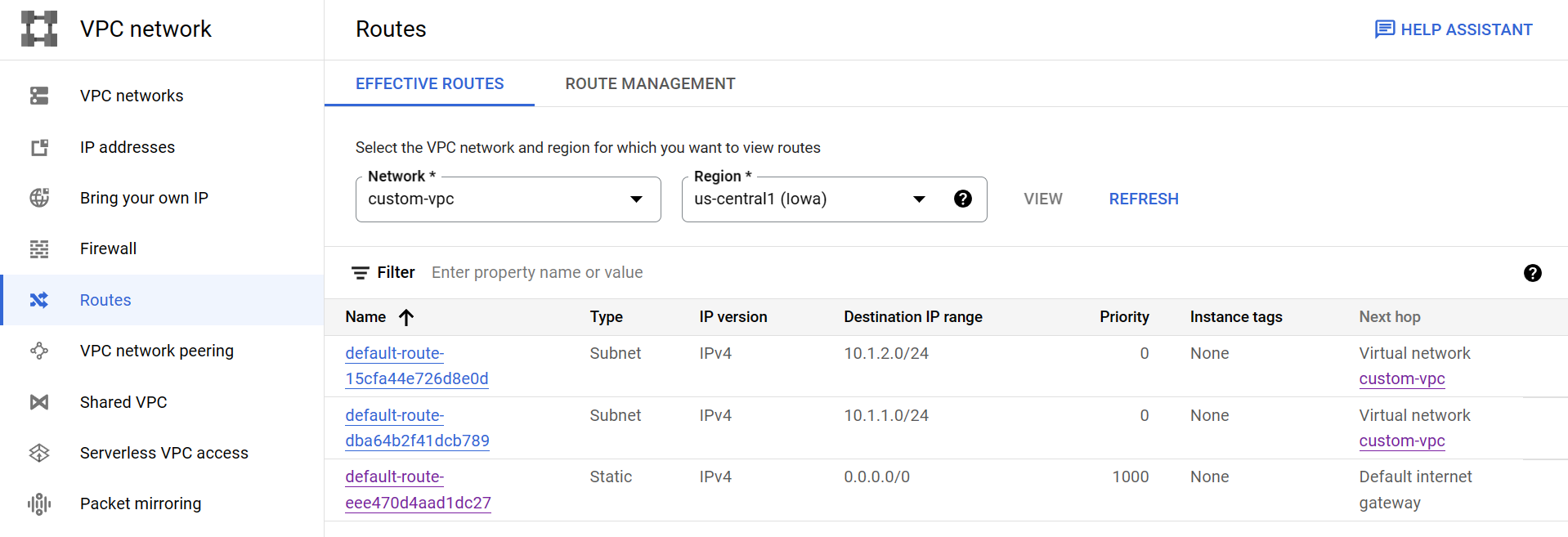
**4. Demonstrate hot to ping from VM1 to VM2, but not from VM2 to VM1**

**Task-1**  
Without subnets you won’t see name corresponding to type-subnet   
You can only view the default static route there



**Task 2-3**

After Creating the subnets the view will be like below Routes.



**VM-1 address 10.1.1.2**

**VM-2 address 10.1.2.2**

**Task 4**

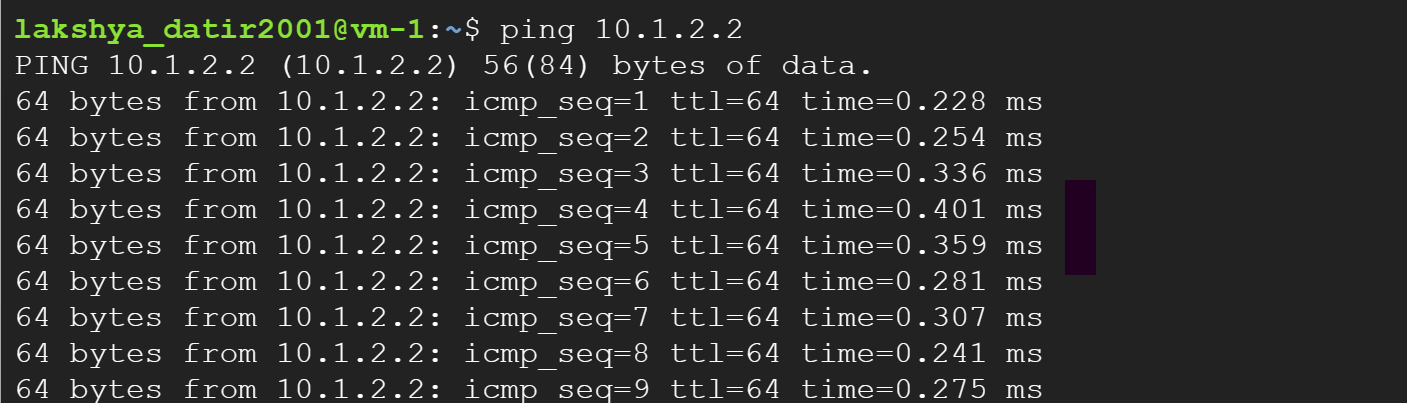
Now u have to ping VM-2 from VM-1, but not VM-1 from VM-2

By default pinging is off, so we can ignore second condition

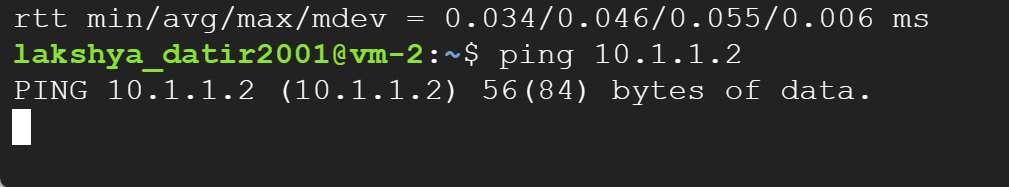
So what does the statement “ ping VM-2 from VM-1” means.  
It simply means when you ssh into VM-1 and try to access VM-2 from there you should be able to do that .

So for that what we can do that in your custom-vpc, set a firewall to ingress request from source ranges of subnet containing VM-1.

VM-1 SSH (Can access VM-2 from VM-1)



VM-2 SSH (Can’t access VM-1 from VM-2)



**2.**

**1. Create 2 vpc networks (VPC A & VPC B) and 2 subnets in it.**

**2. Create 3 VMs:**

**1 VM in each network (VM A in VPC A, VM B in VPC B)**

**1 VM (VM Router) which will serve as a router. This VM should be connected to both VPC networks, and should have IP forwarding turned on.**

**3. Configure the router VM to forward traffic between the two networks using IPTABLES or ip routes.**

**VPC A IP ranges should exit from the interface connected to VPC A and should go to the VPC A gateway (subnet gateway)**

**VPC B IP ranges should exit from the interface connected to VPC B and should go to the VPC B gateway (subnet gateway)**

**4. In VM A, add a static route for for VPC B ranges which forwards traffic to the VM Router**

**5. In VM B, add a static route for the VPC B ranges which forwards traffic to the VM router**

**6. Do connectivity tests between VM A & VM B**

**7. After this is done, delete the custom routes in VM A & VM B**

**8. Create custom route in VPC A with VPC B destination ranges and forwards it to Router VM**

**9. Create custom route in VPC B with VPC A destination ranges and forwards it to Router VM**

**10. Do connectivity tests between VM A & VM B**

**11. Make sure all firewall rules are placed correctly.**

**VPc PEERING**

**- Create 2 custom VPCs**

**- Create 1 private subnet in each VPC**

**- Create 1 VM in each subnet - Only private IPs and no Public IPs**

**- Setup VPC Peering between the 2 VPCs**

**- Figure out how to ping from VM 1 to VM 2, but not from VM 2 to VM 1**

**Tasks:**

**1. Routing in individual standalone VPCs.**

**2. Routing between two peered VPCs.**

**3. Understanding peering connections and importance 2 way connection.**

**4. Firewall rules list for the two VMs.**

**VPC Peering:**

It is mainly used for establishing connection between 2 VPC’s network

The VPC’s can be in different region, different project , or in different organization also

It is not transitive in nature ( suppose if vpc-a → vpc-b is true )

(and vpc-b → vpc-c is true )

(then vpc-a → vpc-c is not always true)

To create VPC peering one should have the IAM permission of VPC administration to perform all tasks that correspond to make it possible.

Also you would not get the access to any of the components of other VPC.

If you haven’t peered from both sides then vpn peering connection would not work with showing status as inactive in the status section.

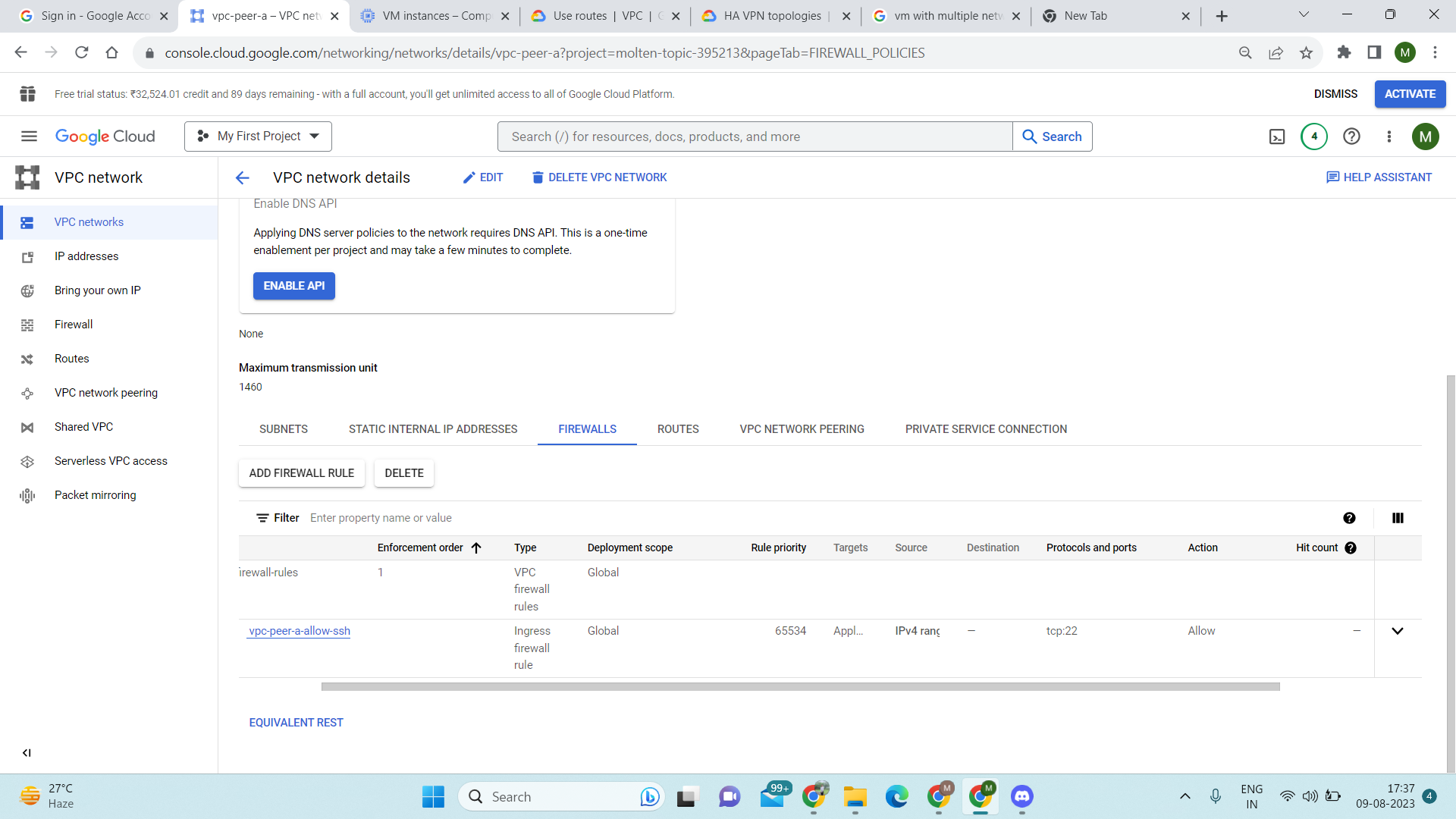
**Steps to perform task –>**

Create the vpc-a and vpc-b with the custom subnets (remember the subnets should not overlap)

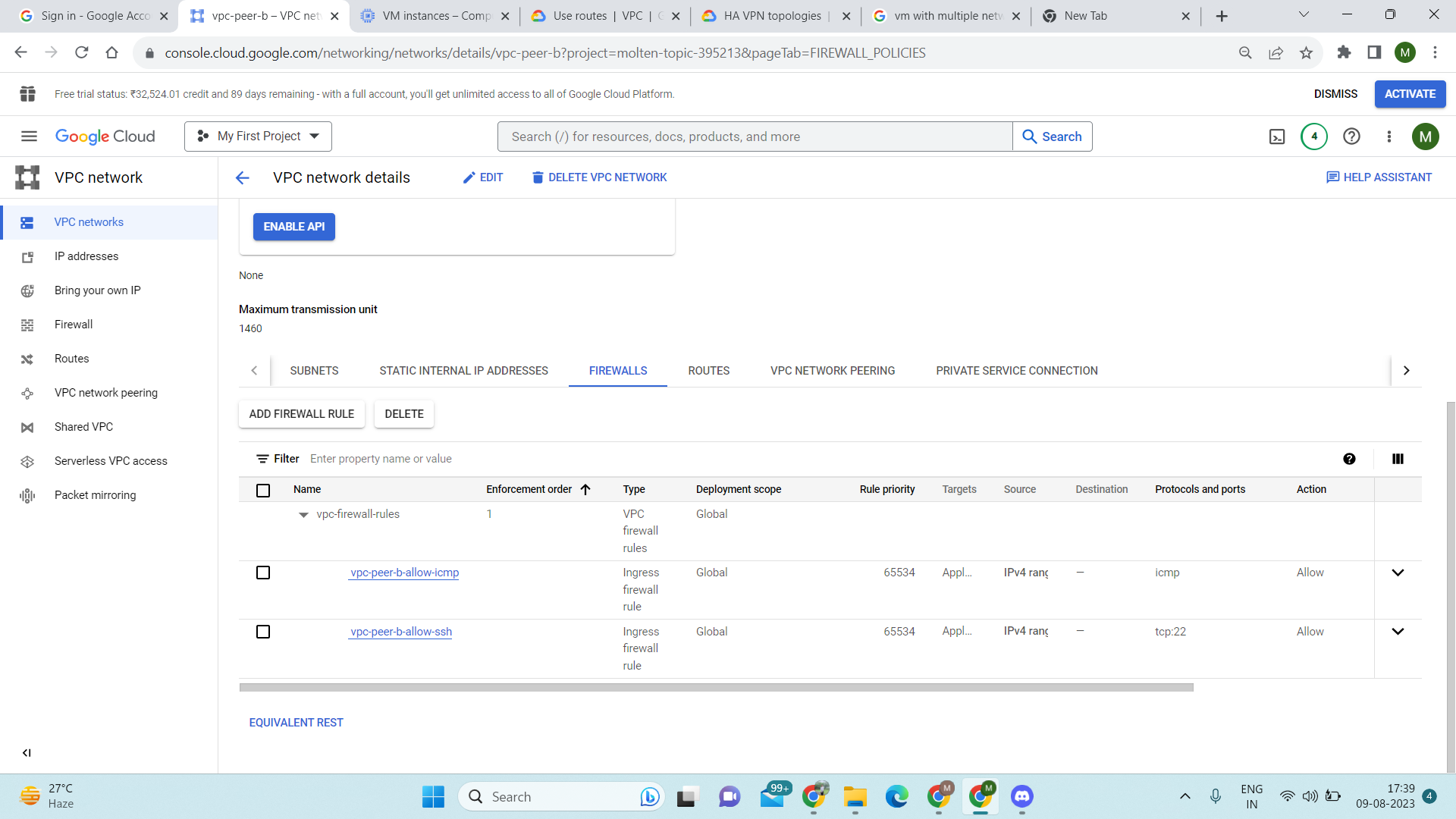
Create the Private ip only VM by providing none to Ephemeral address.

Create 2 vpc (vpc-peer-a and vpc-peer-b) with firewall rule as

Firewall Rules

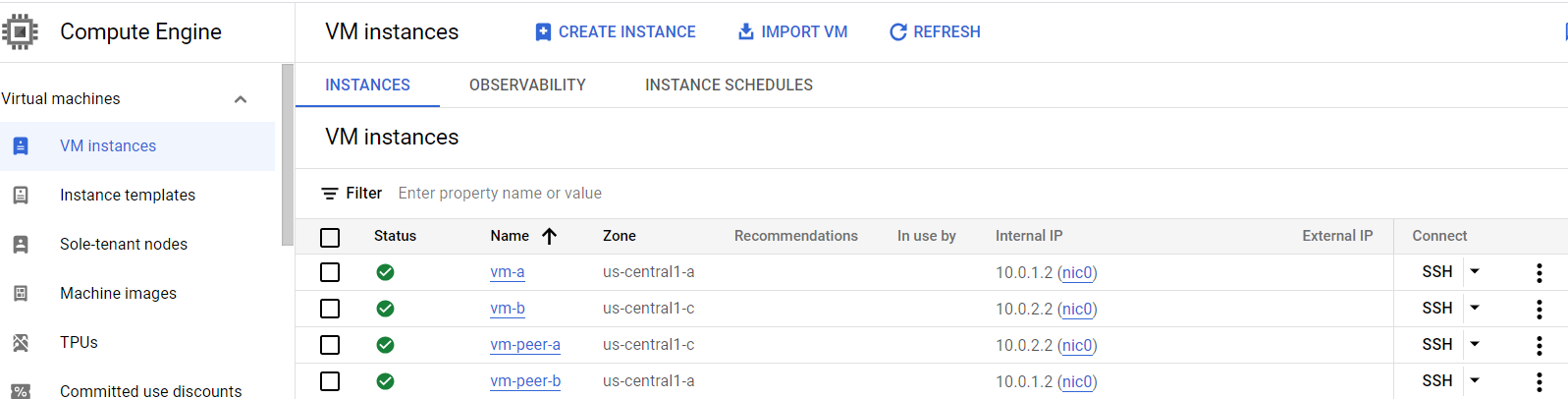
vpc-peer-a

Vpc-peer-b



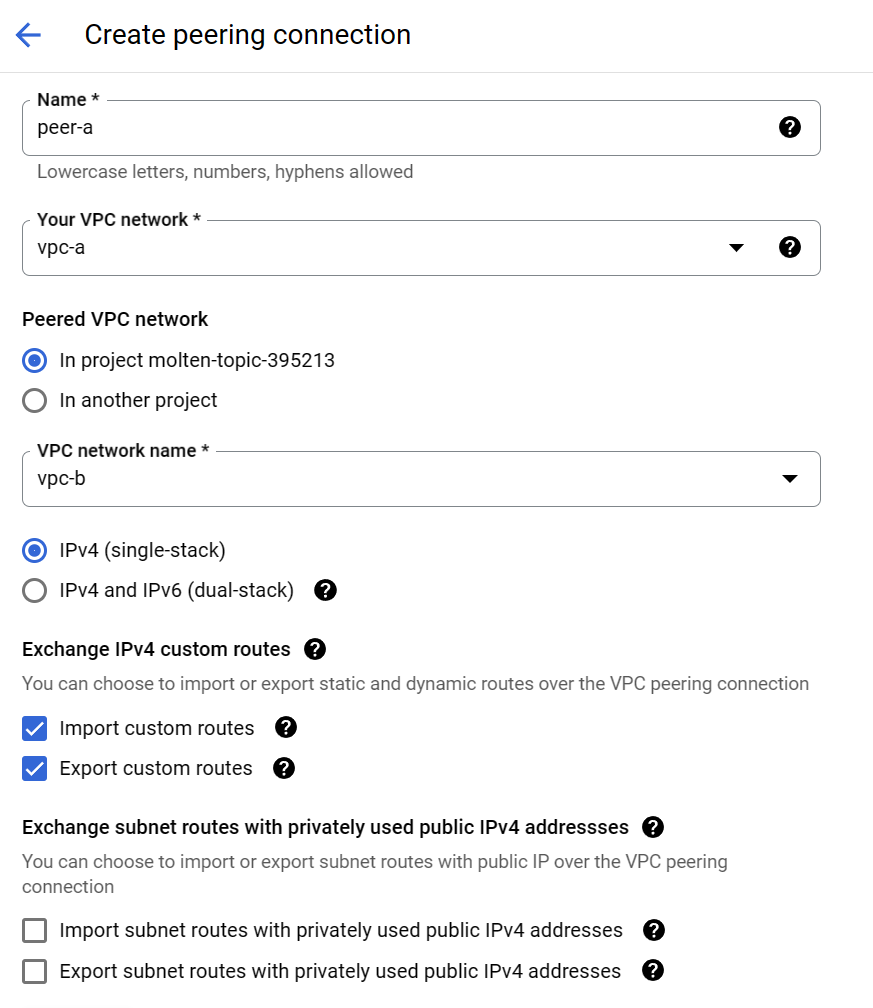
Create 2 VMs

vm-peer-a and vm-peer-b



Go to vpc peering inside the vpc networks

And create peering connection (peer-a & peer-b) →



Name → provide name to vpc peering

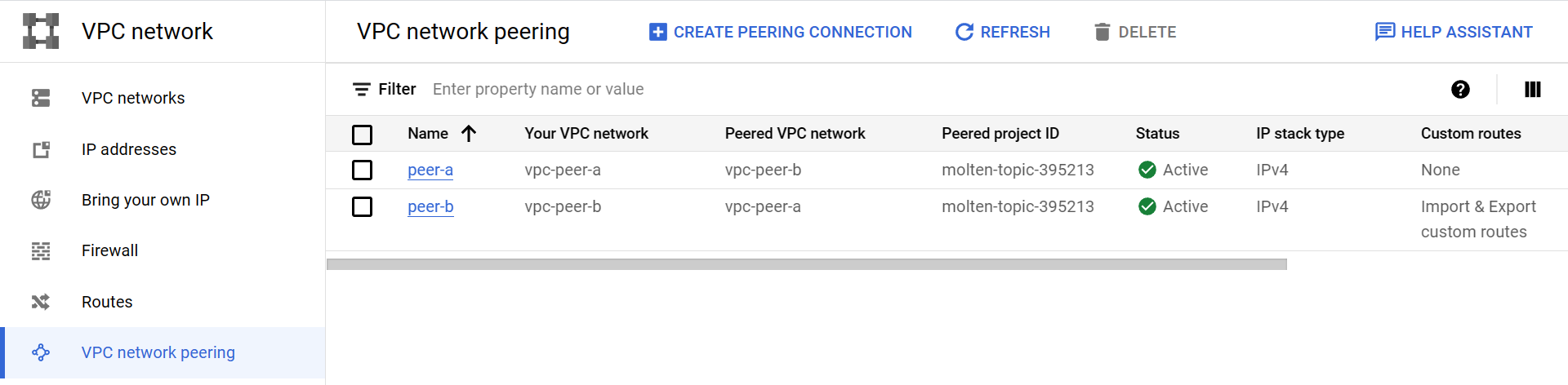
Your VPC network → the vpc to which we want peering to establish.

Preferred VPC network → can select name of any other project whose VPC you want to use

VPC network name → the name of the other vpc.

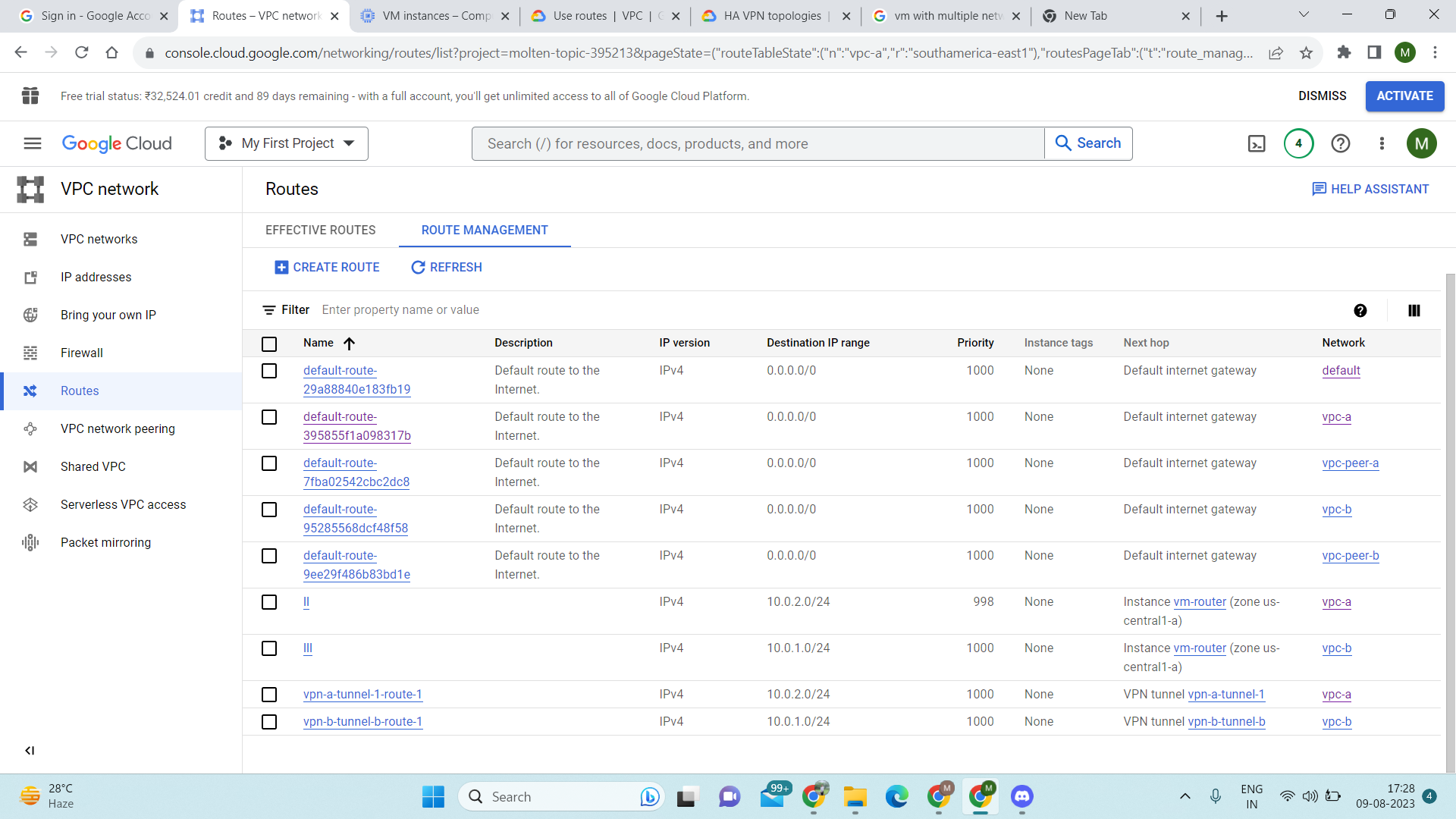
*By default-> static routes are exported and imported and you can’t change them.*

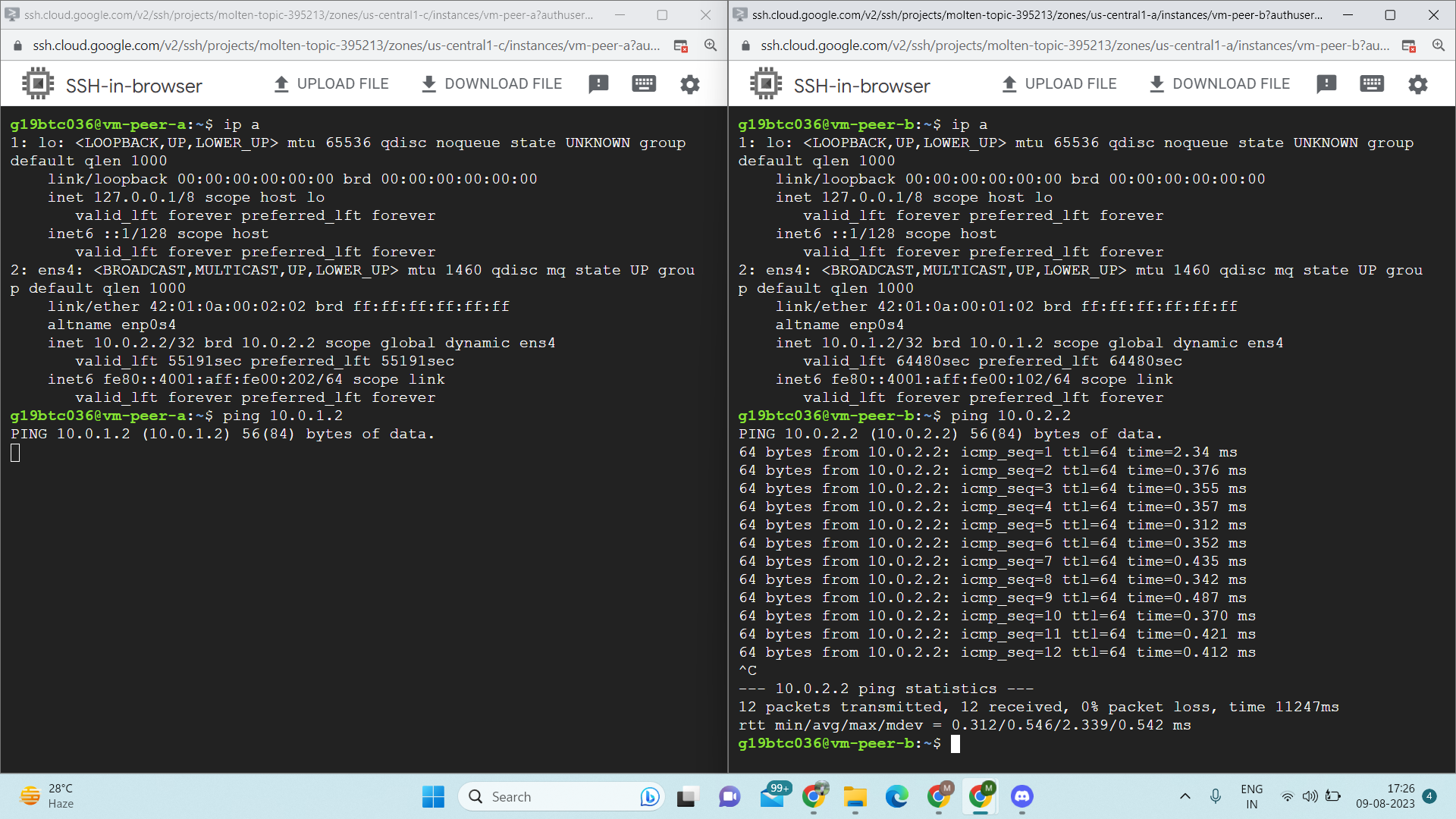
You can exchange the custom routes that you had made or not if you want to.



Routes

When we create vpc network peering we get a default route to internet gateway





**3.**

**- Create 2 custom VPC networks**

**- Create 2 subnets in 1st VPC network and 1 subnet in 2nd VPC network.**

**- Create 1 VM in each subnet**

**- Setup Classic route based VPN between the 2 VPCs**

**- 2nd subnet in 1st VPC should not be routable from the 2nd VPC**

**- Ping from VM in 2nd VPC to VM in 1st subnet of 1st VPC**

There are two VPN Gateway connectivity available -

CLASSICAL & HA(high availability)

* In HA VPN you can only provide static routes.
* In classical VPN you can configure only *1 tunnel*

while in HA you can provide *multiple tunnels* hence we get high availability.

* For classical VPN you have to *reserve static IP address* for the Gateway

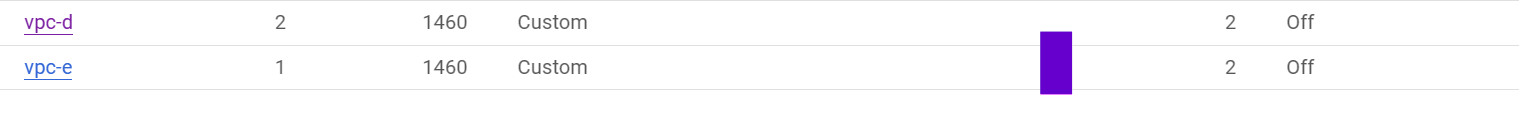
For HA VPN you need to create a *cloud router* which would handle the dynamic routing on its own.

In Google Cloud Platform (GCP), dynamic routing and route-based routing are two different concepts. [Dynamic routing refers to the automatic advertisement of subnets and propagation of learned routes in a Virtual Private Cloud (VPC) network using Cloud Router1](https://cloud.google.com/network-connectivity/docs/router/how-to/configuring-routing-mode). [The dynamic routing mode of a VPC network can be set to either regional or global, and all Cloud Routers in the network use the dynamic routing mode of that network1](https://cloud.google.com/network-connectivity/docs/router/how-to/configuring-routing-mode).

[On the other hand, route-based routing refers to the use of custom routes to define the paths that network traffic takes from a virtual machine (VM) instance to other destinations2](https://cloud.google.com/vpc/docs/routes). [These destinations can be inside or outside the VPC network2](https://cloud.google.com/vpc/docs/routes). Custom routes can be either static or dynamic. [Static routes are manually created, while dynamic routes are automatically maintained by Cloud Routers3](https://cloudacademy.com/course/implementing-a-gcp-virtual-private-cloud-1224/routing-in-gcp/).

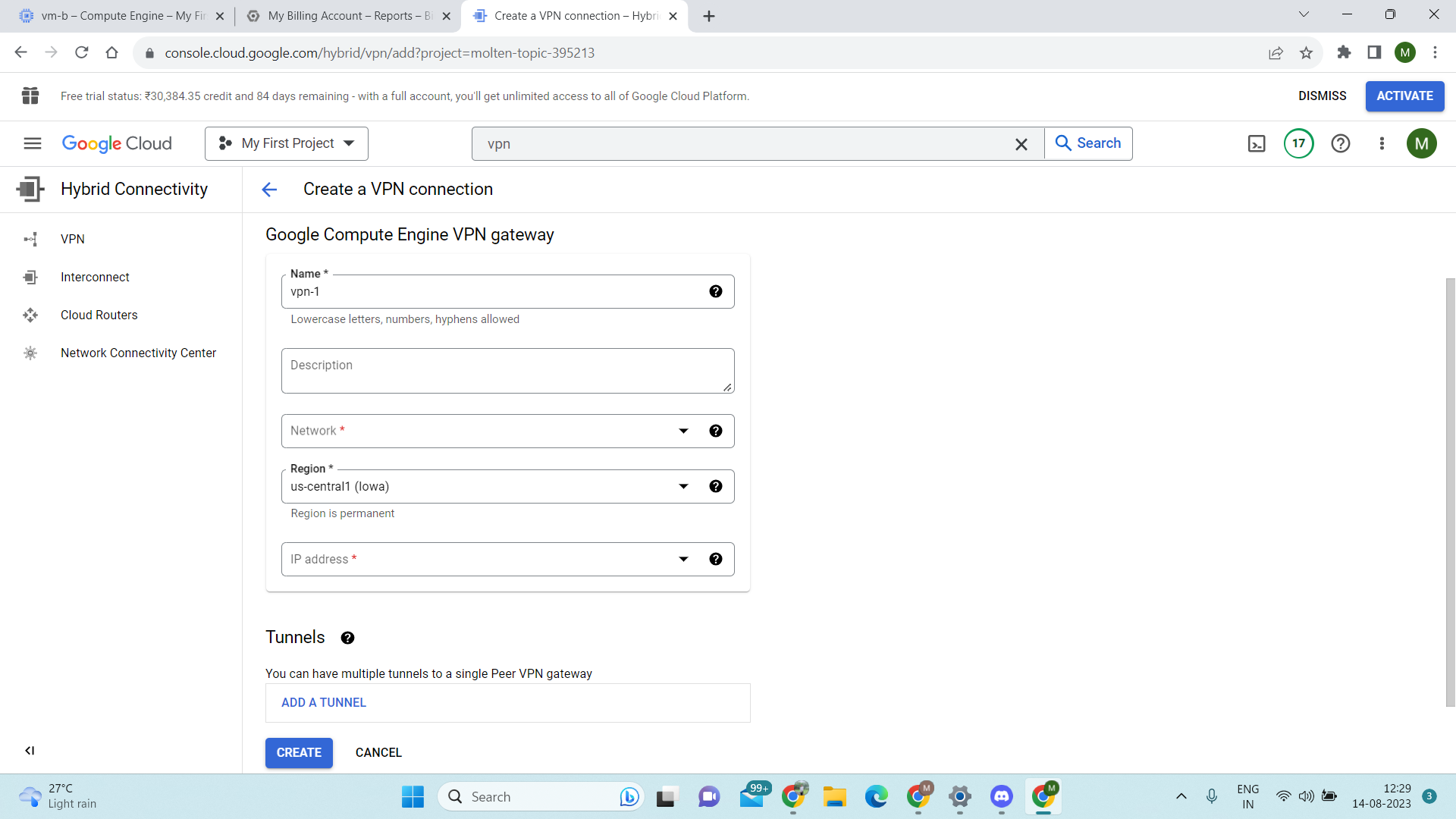
In summary, dynamic routing is a feature of Cloud Router that allows for automatic route advertisement and propagation, while route-based routing refers to the use of custom routes to direct network traffic

Created two vpc here i.e, vpc-d(two subnets) , vpc-e



—-------------------------------------------------------------------------------------------------------------------------------------------------------------------

Remembering the fact that we have to create Classical VPN gateway

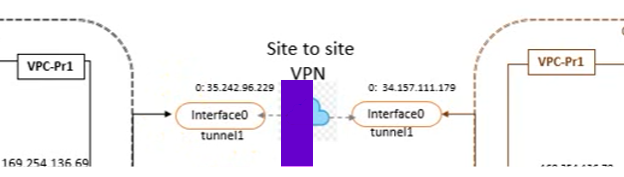


→Select type of VPN as Classical

→Provide it with a proper name

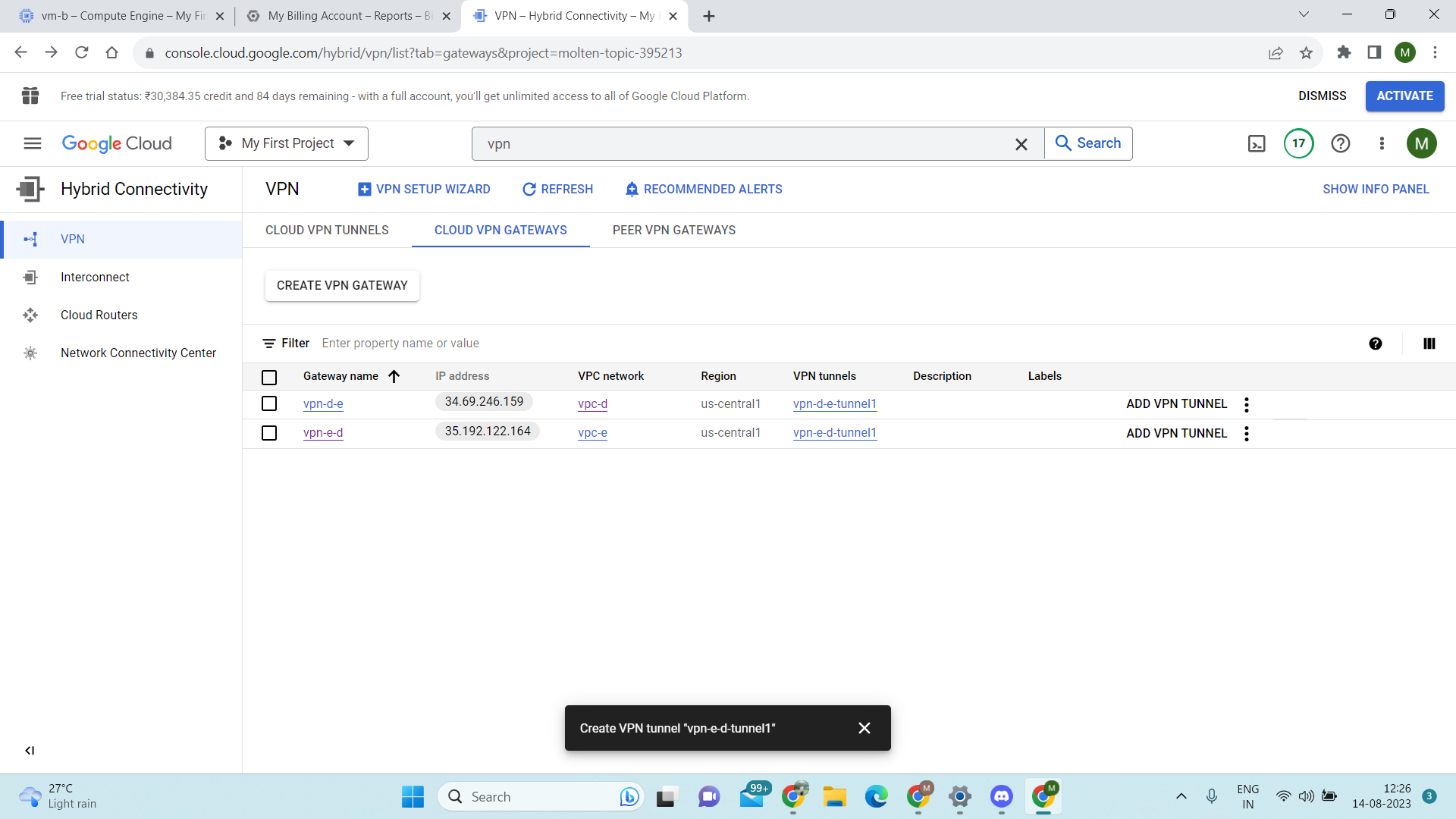
→In Network, we have to give the name of vpc on which we have to provide connection from

→Select the appropriate region

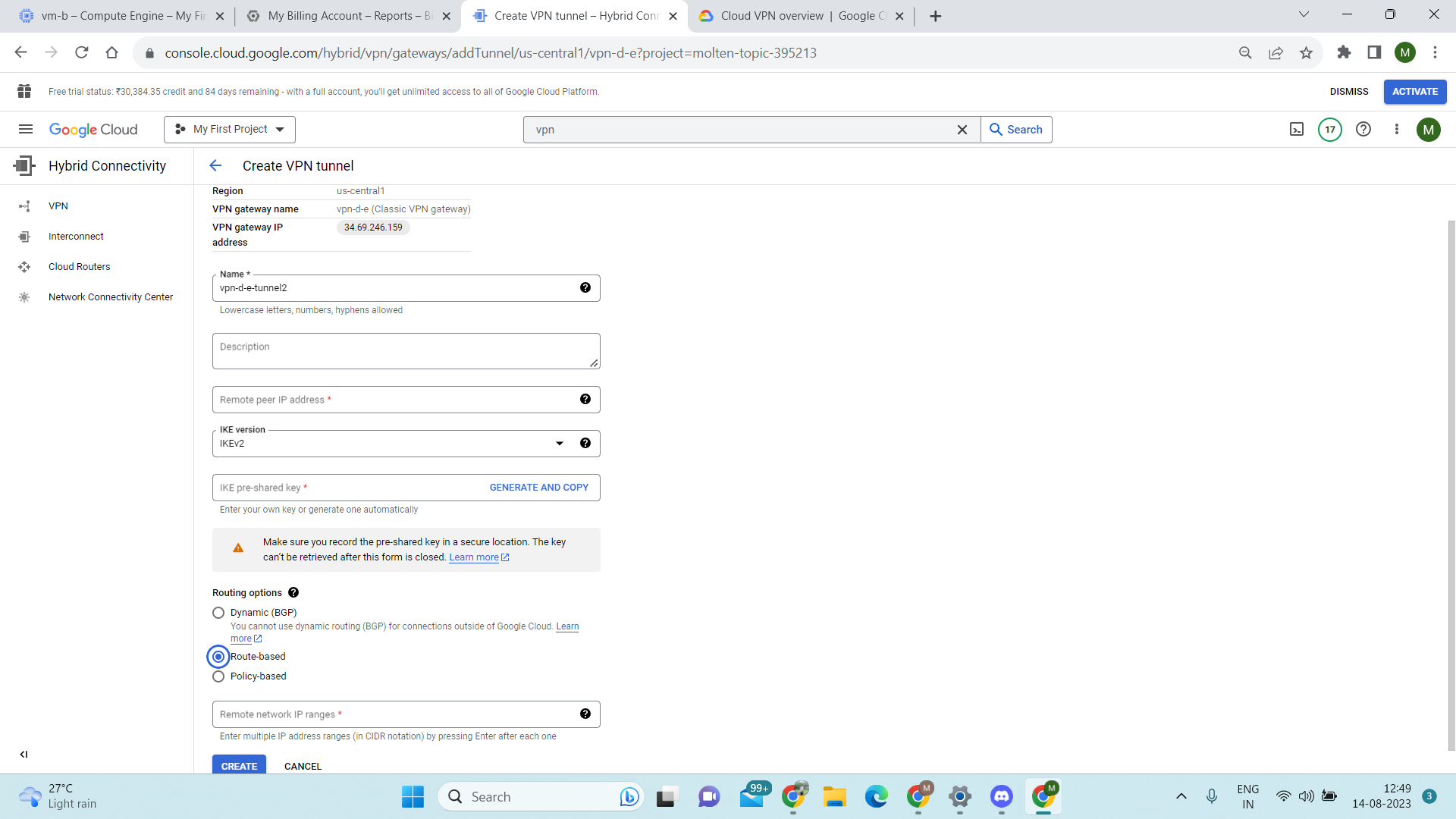
→In ip address– we have to provide a static reserved ip address to it which later on given to tunnel of other side vpc to setup a tunnel connection(ignore the 0 before ip address,get it later)

→Create the VPN-we will add tunnel afterwards

→Create the VPN for vpc-e also.



Now after creating both the VPN we will create the tunnels



Create tunnel:

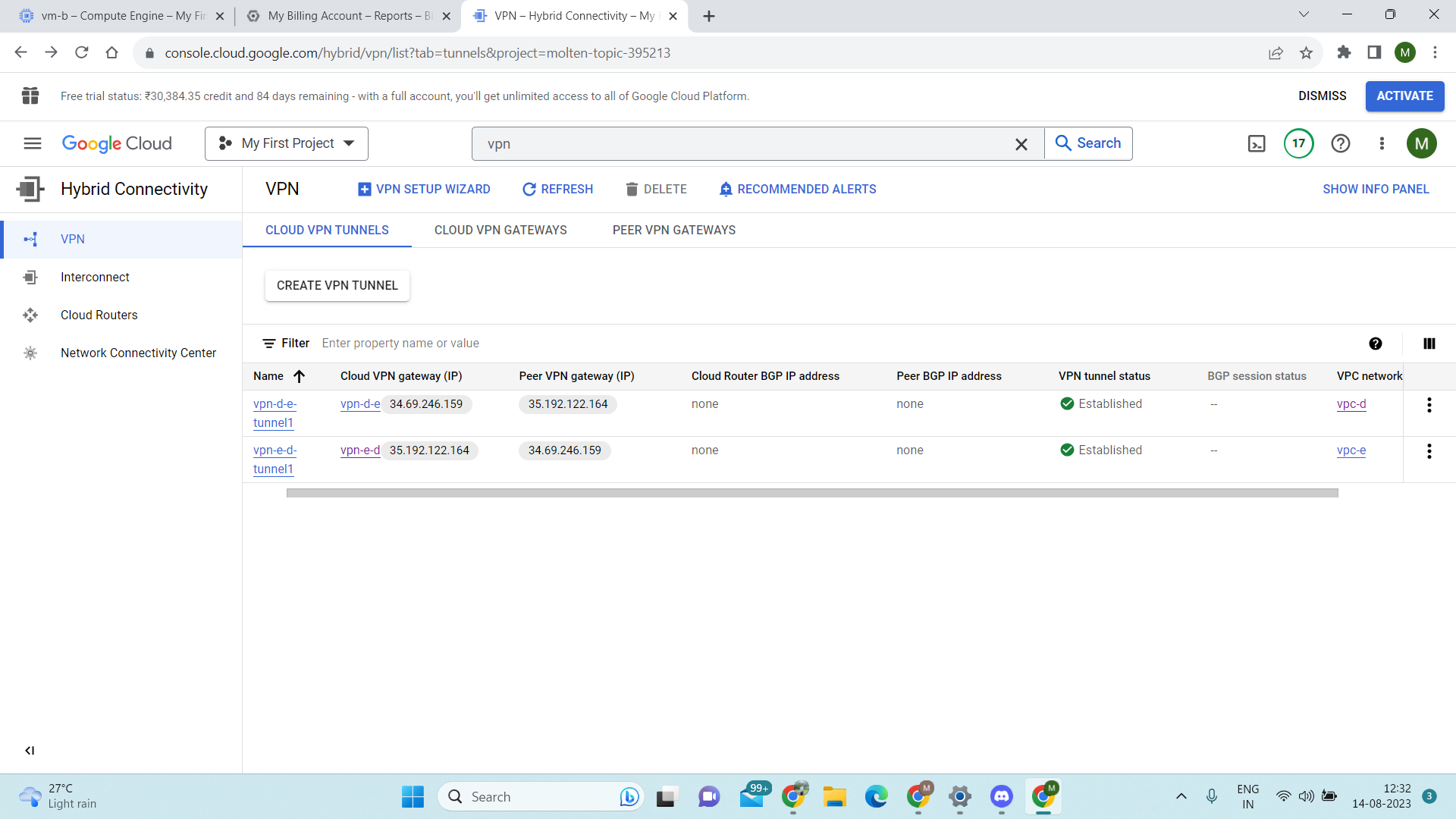
Provide a proper name to it.

In remote peer ip address you have to write the ip address that you had created earlier i.e, the static ip reserve address

Shared key is something you need to remember as it is gonna to be same for both the end of the tunnels.

Select route based routing .

And then it a remote network ip ranges i.e, the ip ranges of the subnet of other vpc that u want to connect to.



After you done that you can navigate to the tunnel section and will be able to see the status as healthy in VPN tunnel status.

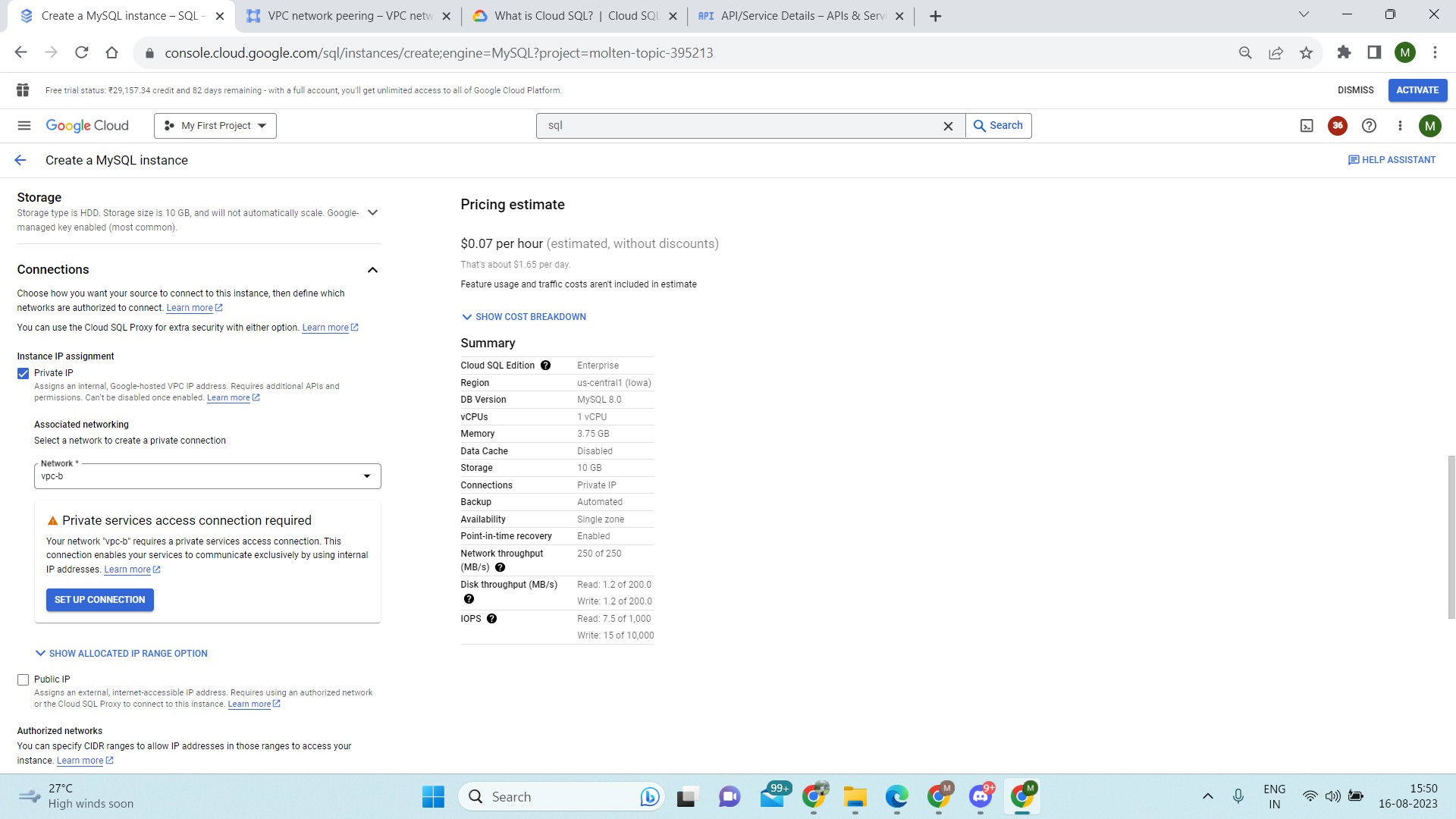
SQL

- Setup 2 VPCs

- Setup Private Service Access in VPC-1

- Setup Cloud SQL in VPC-1

- Connect to cloud SQL from VPC-2



Set up connection for private service access-

