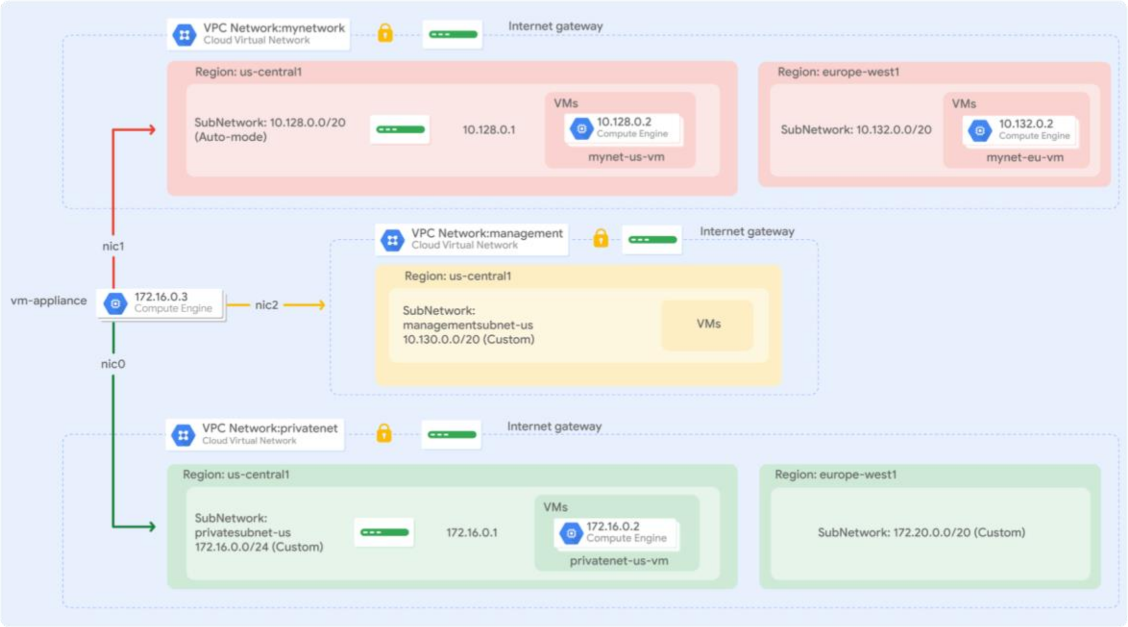
Multiple VPC Networks

Overview

Virtual Private Cloud (VPC) networks allow you to maintain isolated environments within a larger cloud structure, giving you granular control over data protection, network access, and application security.

In this lab you create several VPC networks and VM instances, then test connectivity across networks. Specifically, you create two custom mode networks (**managementnet** and **privatenet**) with firewall rules and VM instances as shown in this network diagram:



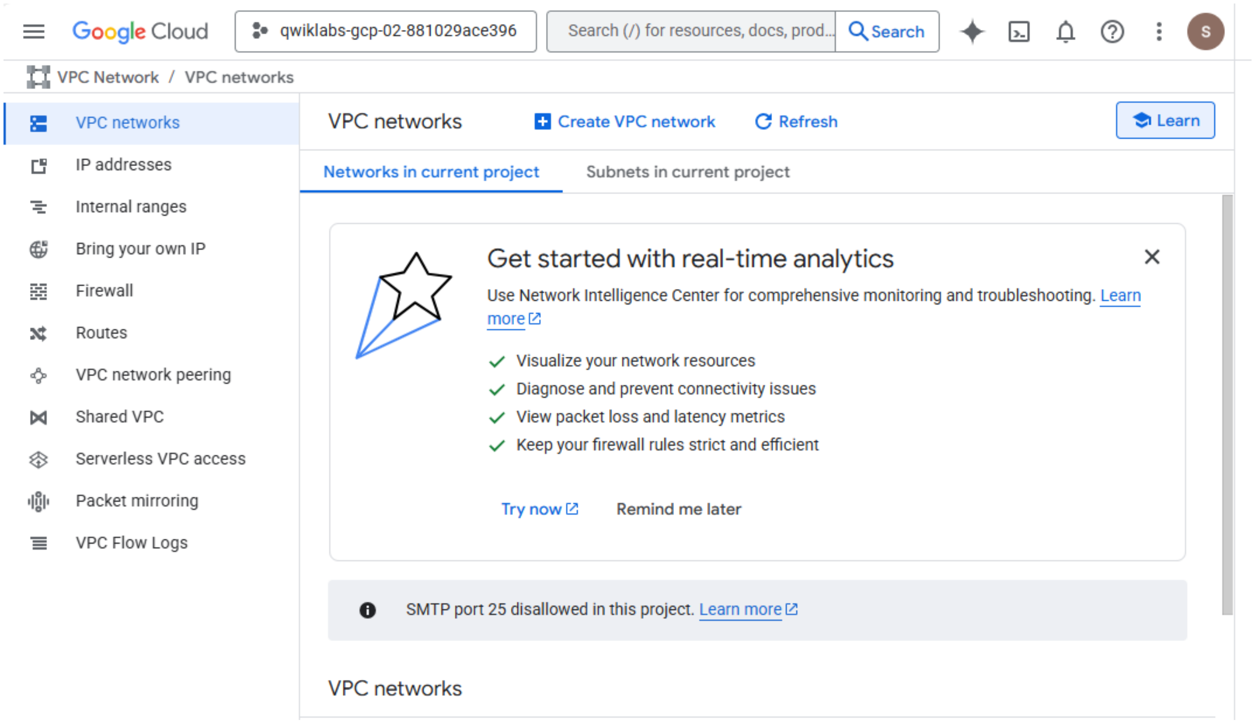
Task 1. Create custom mode VPC networks with firewall rules

Create two custom networks **managementnet** and **privatenet**, along with firewall rules to allow **SSH**, **ICMP**, and **RDP** ingress traffic.

Create the managementnet network

Create the **managementnet** network using the Cloud console.

1. In the Cloud console, navigate to **Navigation menu** (☰) > **VPC network** > **VPC networks**.



Get started with real-time analytics

Use Network Intelligence Center for comprehensive monitoring and troubleshooting. Learn more

- Visualize your network resources
- Diagnose and prevent connectivity issues
- View packet loss and latency metrics
- Keep your firewall rules strict and efficient

SMTP port 25 disallowed in this project. Learn more

2. Notice the **default** and **mynetwork** networks with their subnets.

Each Google Cloud project starts with the **default** network. In addition, the **mynetwork** network has been premade as part of your network diagram.

3. Click **Create VPC Network**.

4. Set the **Name** to managementnet.

5. For **Subnet creation mode**, click **Custom**.

6. Set the following values, leave all other values at their defaults:

Property	Value (type value or select option as specified)
Name	managementsubnet-1
Region	<Region_1>
IPv4 range	10.130.0.0/20

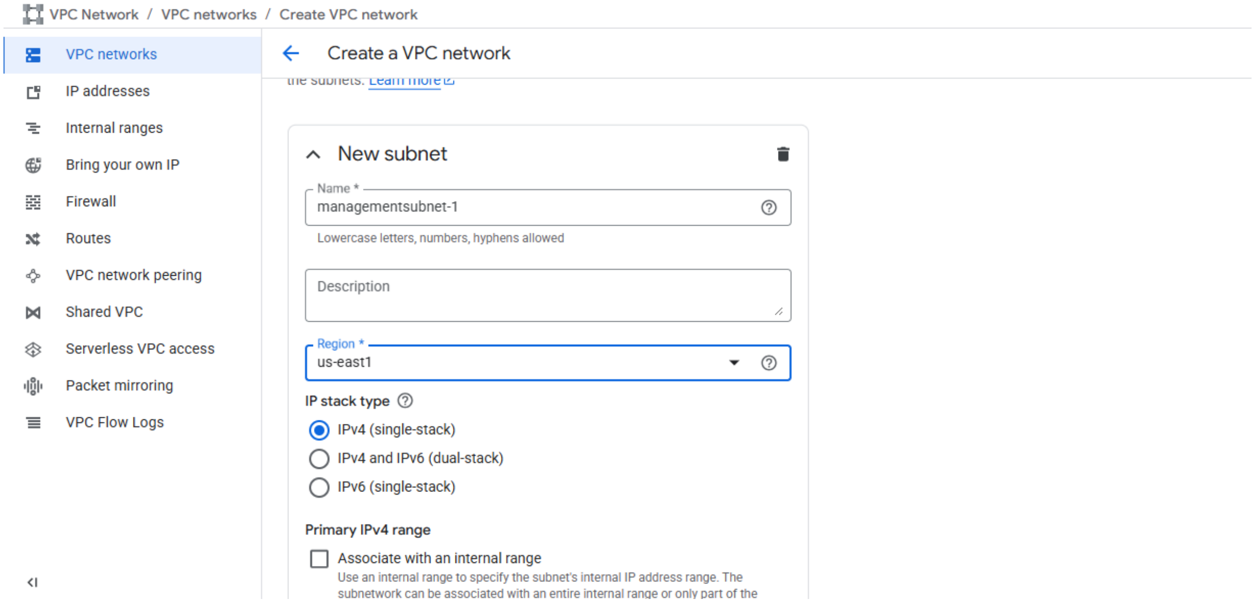
7. Click **Done**.

8. Click **EQUIVALENT COMMAND LINE**.

These commands illustrate that networks and subnets can be created using the Cloud Shell command line. You will create the **privatenet** network using these commands with similar parameters.

9. Click **Close**.

10. Click **Create**.



Create a VPC network

the subnets. Learn more

New subnet

Name * managementsubnet-1

Lowercase letters, numbers, hyphens allowed

Description

Region * us-east1

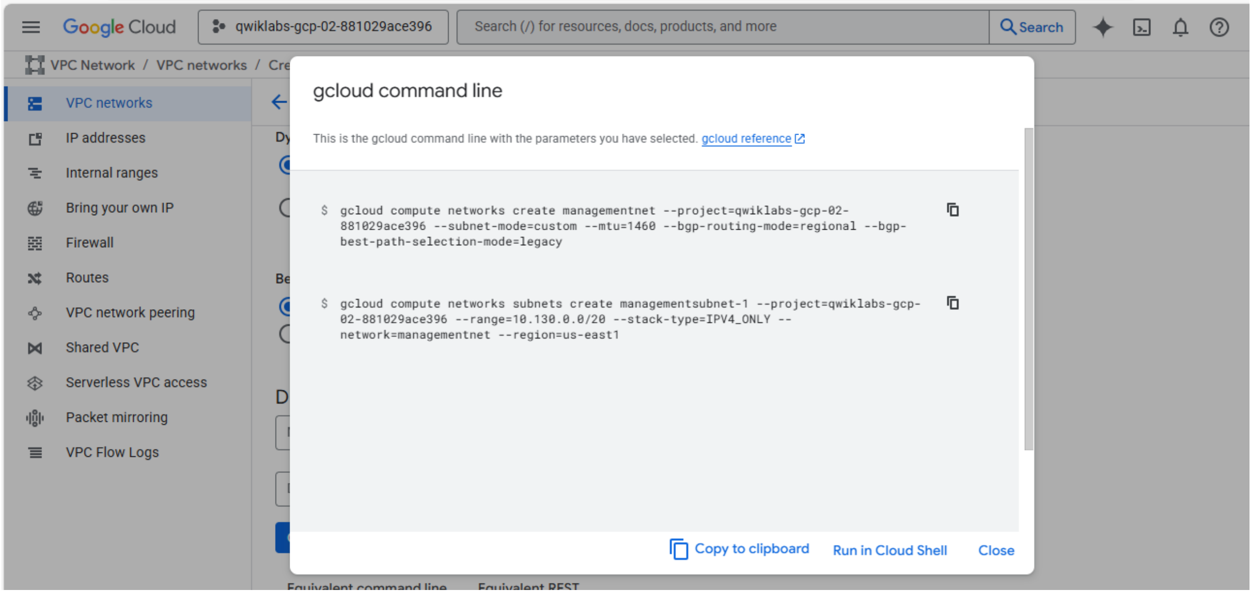
IP stack type

● IPv4 (single-stack)
○ IPv4 and IPv6 (dual-stack)
○ IPv6 (single-stack)

Primary IPv4 range

□ Associate with an internal range

Use an internal range to specify the subnet's internal IP address range. The subnetwork can be associated with an entire internal range or only part of the



gcloud command line

This is the gcloud command line with the parameters you have selected. gcloud reference

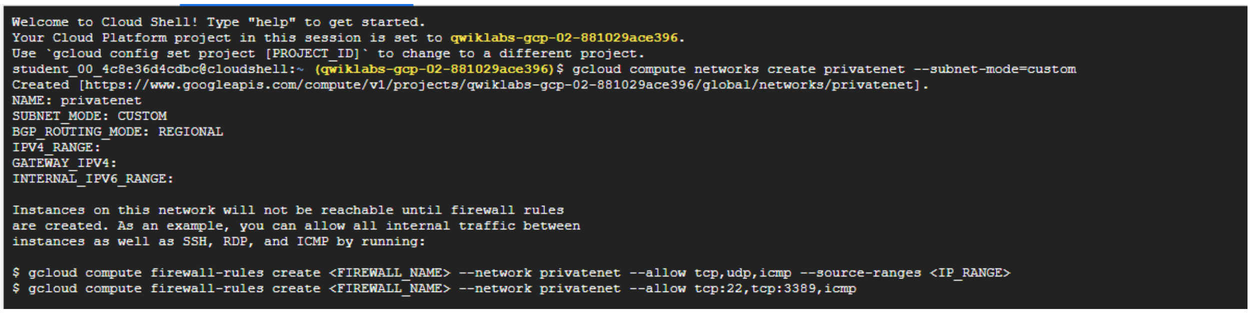
```
$ gcloud compute networks create managementnet --project=qwiklabs-gcp-02-
  881029ace396 --subnet-mode=custom --mtu=1460 --bgp-routing-mode=regional --bgp-
  best-path-selection-mode=legacy

$ gcloud compute networks subnets create managementsubnet-1 --project=qwiklabs-gcp-
  02-881029ace396 --range=10.130.0.0/20 --stack-type=IPV4_ONLY --
  network=managementnet --region=us-east1
```

Create the privatenet network

Create the **privatenet** network using the Cloud Shell command line.

1. Run the following command to create the **privatenet** network:

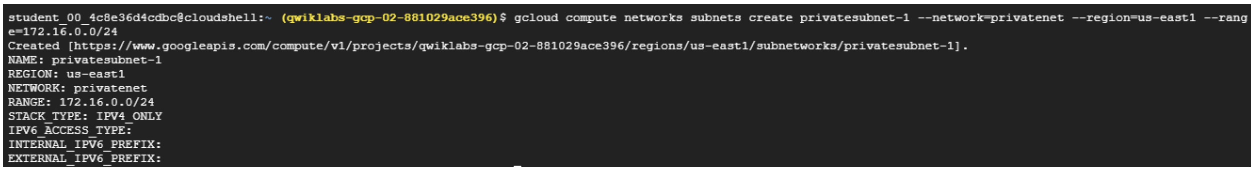
```
gcloud compute networks create privatenet --subnet-mode=custom
```



```
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to qwiklabs-gcp-02-881029ace396.
Use `gcloud config set project [PROJECT_ID]` to change to a different project.
student_00_4c8e36d4cdbc@cloudshell:~ (qwiklabs-gcp-02-881029ace396)$ gcloud compute networks create privatenet --subnet-mode=custom
Created [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-02-881029ace396/global/networks/privatenet].
NAME: privatenet
SUBNET_MODE: CUSTOM
BGP_ROUTING_MODE: REGIONAL
IPV4_RANGE:
GATEWAY_IPV4:
INTERNAL_IPV6_RANGE:

Instances on this network will not be reachable until firewall rules
are created. As an example, you can allow all internal traffic between
instances as well as SSH, RDP, and ICMP by running:

$ gcloud compute firewall-rules create <FIREWALL_NAME> --network privatenet --allow tcp,udp,icmp --source-ranges <IP_RANGE>
$ gcloud compute firewall-rules create <FIREWALL_NAME> --network privatenet --allow tcp:22,tcp:3389,icmp
```

Run the following command to create the privatesubnet-1 subnet:

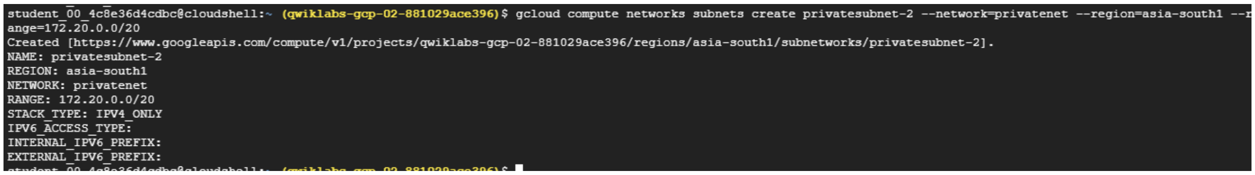
```
gcloud compute networks subnets create privatesubnet-1 --network=privatenet --region=Region_1 --range=172.16.0.0/24
```



```
student_00_4c8e36d4cdbc@cloudshell:~ (qwiklabs-gcp-02-881029ace396)$ gcloud compute networks subnets create privatesubnet-1 --network=privatenet --region=us-east1 --rang
e=172.16.0.0/24
Created [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-02-881029ace396/regions/us-east1/subnetworks/privatesubnet-1].
NAME: privatesubnet-1
REGION: us-east1
NETWORK: privatenet
RANGE: 172.16.0.0/24
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:
```

3. Run the following command to create the **privatesubnet-2** subnet:

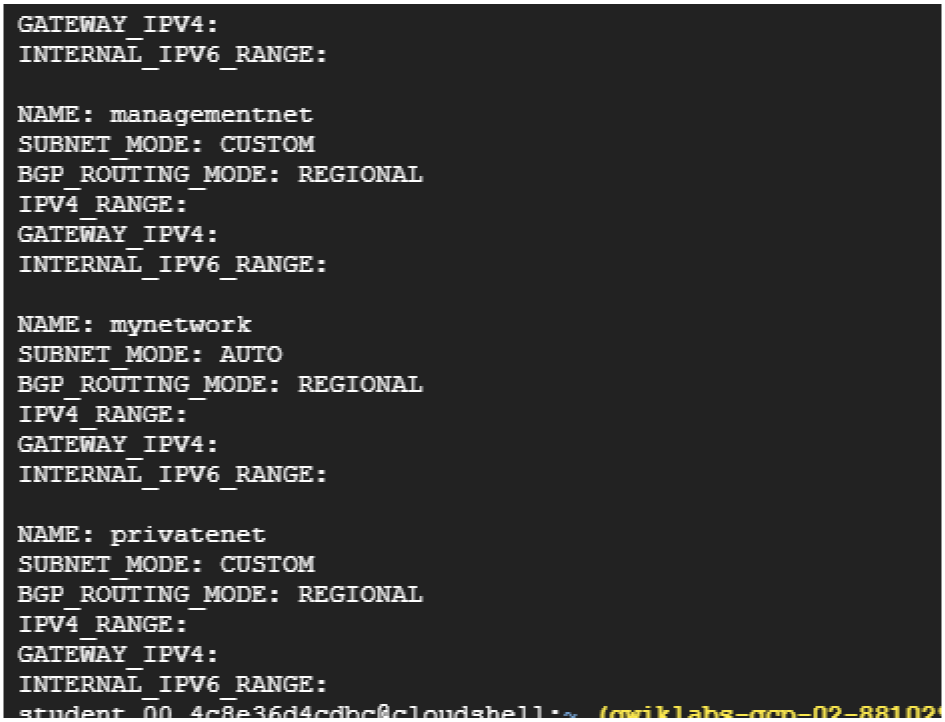
   ```
   gcloud compute networks subnets create privatesubnet-2 --network=privatenet --region=Region_2 --range=172.20.0.0/20
   ```

   ```
   student_00_4c8e36d4cdbc@cloudshell:~ (qwiklabs-gcp-02-881029ace396)$ gcloud compute networks subnets create privatesubnet-2 --network=privatenet --region=asia-south1 --r
   ange=172.20.0.0/20
   Created [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-02-881029ace396/regions/asia-south1/subnetworks/privatesubnet-2].
   NAME: privatesubnet-2
   REGION: asia-south1
   NETWORK: privatenet
   RANGE: 172.20.0.0/20
   STACK_TYPE: IPV4_ONLY
   IPV6_ACCESS_TYPE:
   INTERNAL_IPV6_PREFIX:
   EXTERNAL_IPV6_PREFIX:
   student_00_4c8e36d4cdbc@cloudshell:~ (qwiklabs-gcp-02-881029ace396)$
   ```

4. Run the following command to list the available VPC networks:

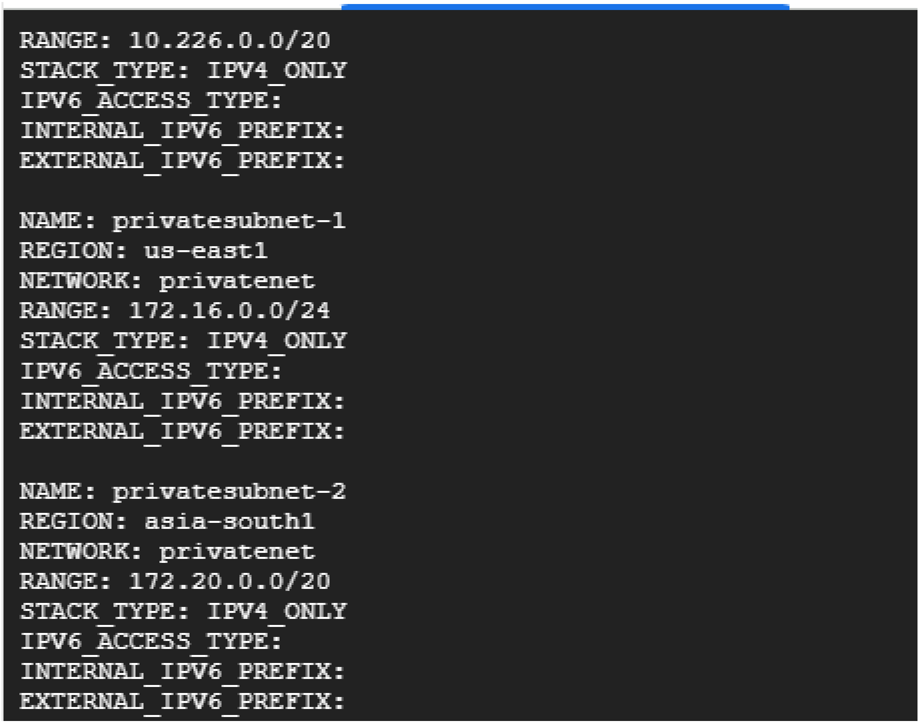
   ```
   gcloud compute networks list
   ```



```
GATEWAY_IPV4:
INTERNAL_IPV6_RANGE:

NAME: managementnet
SUBNET_MODE: CUSTOM
BGP_ROUTING_MODE: REGIONAL
IPV4_RANGE:
GATEWAY_IPV4:
INTERNAL_IPV6_RANGE:

NAME: mynetwork
SUBNET_MODE: AUTO
BGP_ROUTING_MODE: REGIONAL
IPV4_RANGE:
GATEWAY_IPV4:
INTERNAL_IPV6_RANGE:

NAME: privatenet
SUBNET_MODE: CUSTOM
BGP_ROUTING_MODE: REGIONAL
IPV4_RANGE:
GATEWAY_IPV4:
INTERNAL_IPV6_RANGE:
student_00_4c8e36d4cdbc@cloudshell:~ (qwiklabs-gcp-02-881029
```

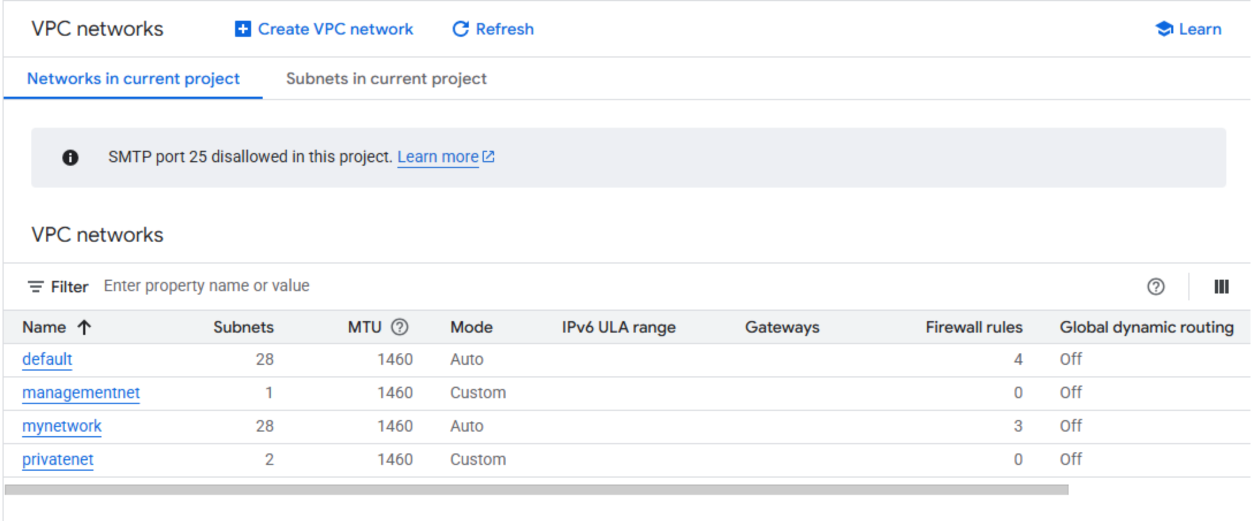
5. Run the following command to list the available VPC subnets (sorted by VPC network):

   gcloud compute networks subnets list --sort-by=NETWORK



```
RANGE: 10.226.0.0/20
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:

NAME: privatesubnet-1
REGION: us-east1
NETWORK: privatenet
RANGE: 172.16.0.0/24
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:

NAME: privatesubnet-2
REGION: asia-south1
NETWORK: privatenet
RANGE: 172.20.0.0/20
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:
```

6. In the Cloud console, navigate to **Navigation menu** > **VPC network** > **VPC networks**.
7. You see that the same networks and subnets are listed in the Cloud console.


VPC networks
Create VPC network
Refresh
Learn
Networks in current project
Subnets in current project

SMTP port 25 disallowed in this project. Learn more

VPC networks

Filter
Enter property name or value

Name	Subnets	MTU	Mode	IPv6 ULA range	Gateways	Firewall rules	Global dynamic routing
default	28	1460	Auto			4	Off
managementnet	1	1460	Custom			0	Off
mynetwork	28	1460	Auto			3	Off
privatenet	2	1460	Custom			0	Off

reate the firewall rules for managementnet

Create firewall rules to allow **SSH**, **ICMP**, and **RDP** ingress traffic to VM instances on the **managementnet** network.

1. In the Cloud console, navigate to **Navigation menu** (☰) > **VPC network** > **Firewall**.
2. Click **+ Create Firewall Rule**.
3. Set the following values, leave all other values at their defaults:

Property	**Value (type value or select option as specified)**
Name	managementnet-allow-icmp-ssh-rdp
Network	managementnet
Targets	All instances in the network

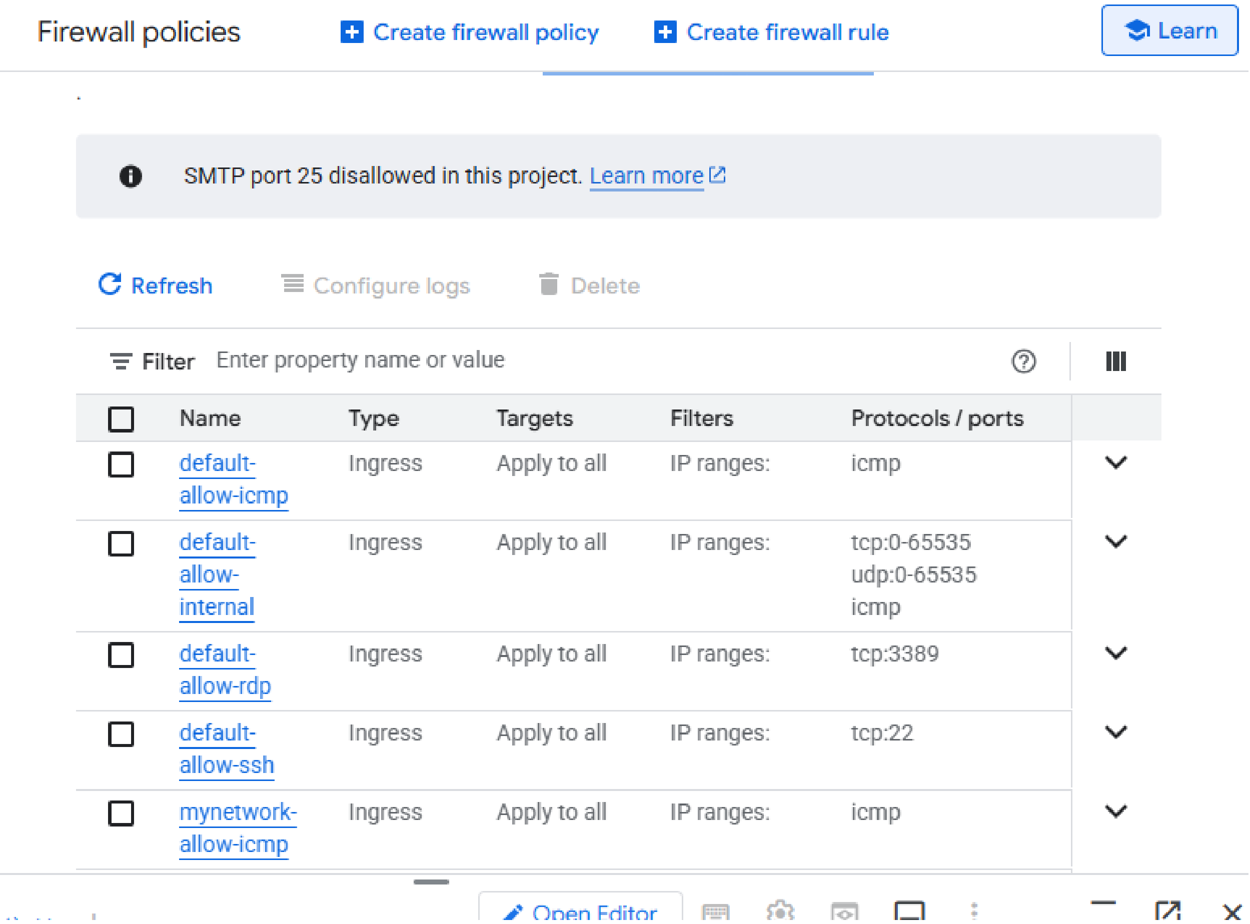
Source filter	IPv4 Ranges
Source IPv4 ranges	0.0.0.0/0
Protocols and ports	Specified protocols and ports, and then *check* tcp, *type:* 22, 3389; and *check* Other protocols, *type:* icmp.

4. Click **EQUIVALENT COMMAND LINE**.

   These commands illustrate that firewall rules can also be created using the Cloud Shell command line. You will create the **privatenet**'s firewall rules using these commands with similar parameters.

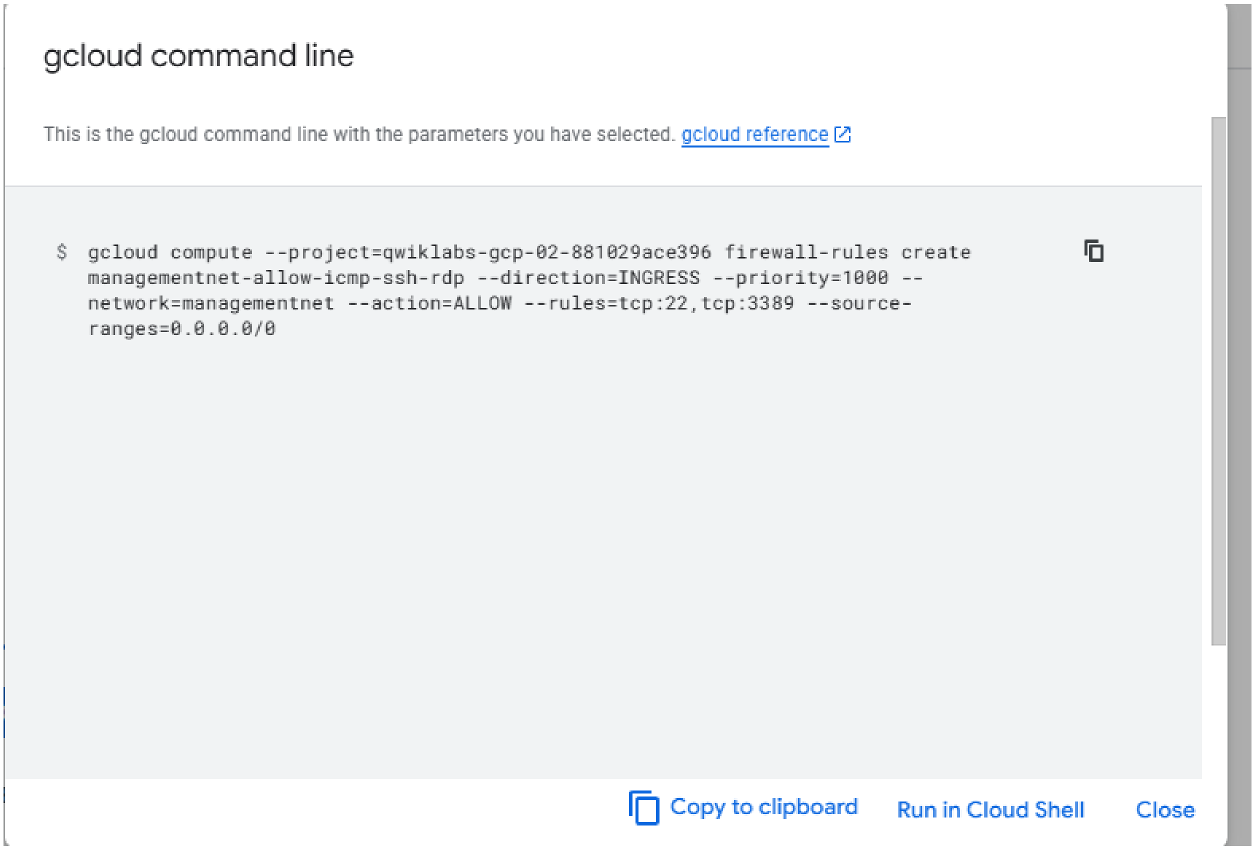
5. Click **Close**.

6. Click **Create**.



SMTP port 25 disallowed in this project. Learn more

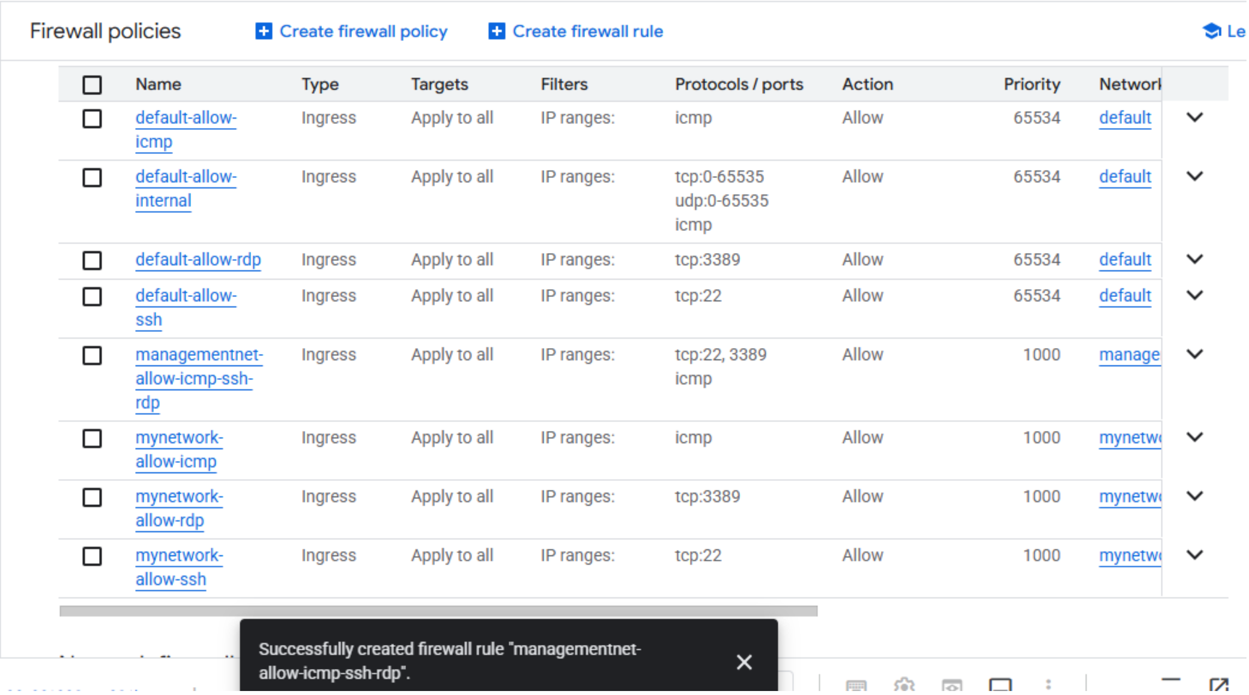
☐	Name	Type	Targets	Filters	Protocols / ports
☐	default-allow-icmp	Ingress	Apply to all	IP ranges:	icmp
☐	default-allow-internal	Ingress	Apply to all	IP ranges:	tcp:0-65535 udp:0-65535 icmp
☐	default-allow-rdp	Ingress	Apply to all	IP ranges:	tcp:3389
☐	default-allow-ssh	Ingress	Apply to all	IP ranges:	tcp:22
☐	mynetwork-allow-icmp	Ingress	Apply to all	IP ranges:	icmp



gcloud command line

This is the gcloud command line with the parameters you have selected. gcloud reference

```
$ gcloud compute --project=qwiklabs-gcp-02-881029ace396 firewall-rules create
  managementnet-allow-icmp-ssh-rdp --direction=INGRESS --priority=1000 --
  network=managementnet --action=ALLOW --rules=tcp:22,tcp:3389 --source-
  ranges=0.0.0.0/0
```



Firewall policies

☐	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Networ
☐	default-allow-icmp	Ingress	Apply to all	IP ranges:	icmp	Allow	65534	default
☐	default-allow-internal	Ingress	Apply to all	IP ranges:	tcp:0-65535 udp:0-65535 icmp	Allow	65534	default
☐	default-allow-rdp	Ingress	Apply to all	IP ranges:	tcp:3389	Allow	65534	default
☐	default-allow-ssh	Ingress	Apply to all	IP ranges:	tcp:22	Allow	65534	default
☐	managementnet-allow-icmp-ssh-rdp	Ingress	Apply to all	IP ranges:	tcp:22, 3389 icmp	Allow	1000	manage
☐	mynetwork-allow-icmp	Ingress	Apply to all	IP ranges:	icmp	Allow	1000	mynetw
☐	mynetwork-allow-rdp	Ingress	Apply to all	IP ranges:	tcp:3389	Allow	1000	mynetw
☐	mynetwork-allow-ssh	Ingress	Apply to all	IP ranges:	tcp:22	Allow	1000	mynetw

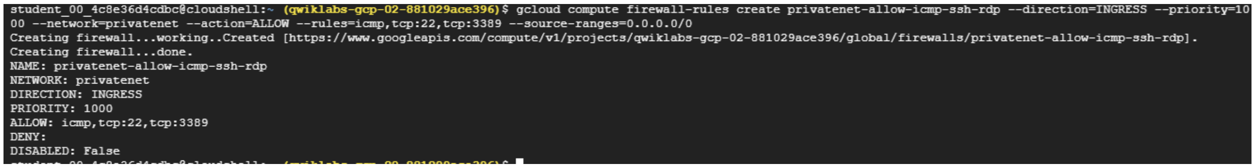
Successfully created firewall rule "managementnet-allow-icmp-ssh-rdp".

Create the firewall rules for privatenet

Create the firewall rules for **privatenet** network using the Cloud Shell command line.

1. In Cloud Shell, run the following command to create the **privatenet-allow-icmp-ssh-rdp** firewall rule:

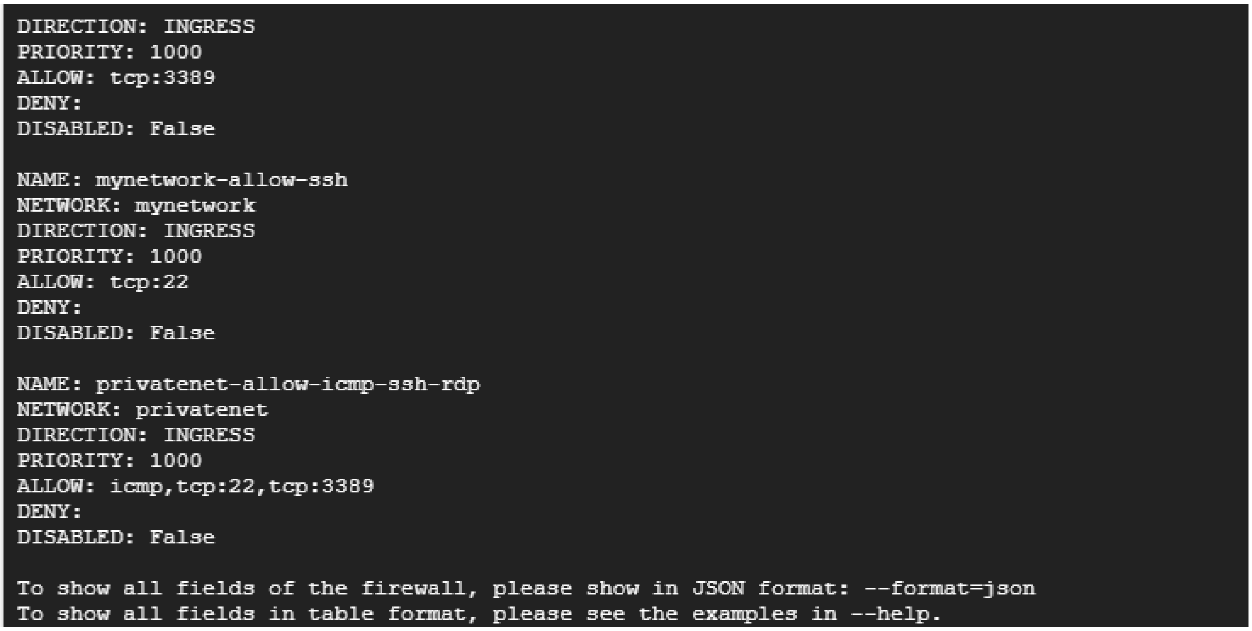
gcloud compute firewall-rules create privatenet-allow-icmp-ssh-rdp --direction=INGRESS --priority=1000 --network=privatenet --action=ALLOW --rules=icmp,tcp:22,tcp:3389 --source-ranges=0.0.0.0/0



```
student_00_4c8e36d4cdbc@cloudshell:~ (qwiklabs-gcp-02-881029ace396)$ gcloud compute firewall-rules create privatenet-allow-icmp-ssh-rdp --direction=INGRESS --priority=10
00 --network=privatenet --action=ALLOW --rules=icmp,tcp:22,tcp:3389 --source-ranges=0.0.0.0/0
Creating firewall...working..Created [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-02-881029ace396/global/firewalls/privatenet-allow-icmp-ssh-rdp].
Creating firewall...done.
NAME: privatenet-allow-icmp-ssh-rdp
NETWORK: privatenet
DIRECTION: INGRESS
PRIORITY: 1000
ALLOW: icmp,tcp:22,tcp:3389
DENY:
DISABLED: False
```

2. Run the following command to list all the firewall rules (sorted by VPC network):

gcloud compute firewall-rules list --sort-by=NETWORK



```
DIRECTION: INGRESS
PRIORITY: 1000
ALLOW: tcp:3389
DENY:
DISABLED: False

NAME: mynetwork-allow-ssh
NETWORK: mynetwork
DIRECTION: INGRESS
PRIORITY: 1000
ALLOW: tcp:22
DENY:
DISABLED: False

NAME: privatenet-allow-icmp-ssh-rdp
NETWORK: privatenet
DIRECTION: INGRESS
PRIORITY: 1000
ALLOW: icmp,tcp:22,tcp:3389
DENY:
DISABLED: False

To show all fields of the firewall, please show in JSON format: --format=json
To show all fields in table format, please see the examples in --help.
```

The firewall rules for **mynetwork** network have been created for you. You can define multiple protocols and ports in one firewall rule (**privatenet** and **managementnet**), or spread them across multiple rules (**default** and **mynetwork**).

3. In the Cloud console, navigate to **Navigation menu** > **VPC network** > **Firewall**.

4. You see that the same firewall rules are listed in the Cloud console.

ask 2. Create VM instances

Create two VM instances:

- **managementnet-vm-1** in **managementsubnet-1**
- **privatenet-vm-1** in **privatesubnet-1**

Create the managementnet-vm-1 instance

Create the **managementnet-vm-1** instance using the Cloud console.

1. In the Cloud console, navigate to **Navigation menu** > **Compute Engine** > **VM instances**.

The **mynet-vm-2** and **mynet-vm-1** has been created for you, as part of your network diagram.

2. Click **Create Instance**.
3. In the **Machine configuration**:

Set the following values, leave all other values at their defaults:

Property	**Value (type value or select option as specified)**
Name	managementnet-vm-1
Region	US_Region
Zone	US_Zone
Series	E2
Machine Type	e2-micro

4. Click **Networking**.

For **Network interfaces**, click the dropdown to edit. Set the following values, leave all other values at their defaults:

Property	**Value (type value or select option as specified)**

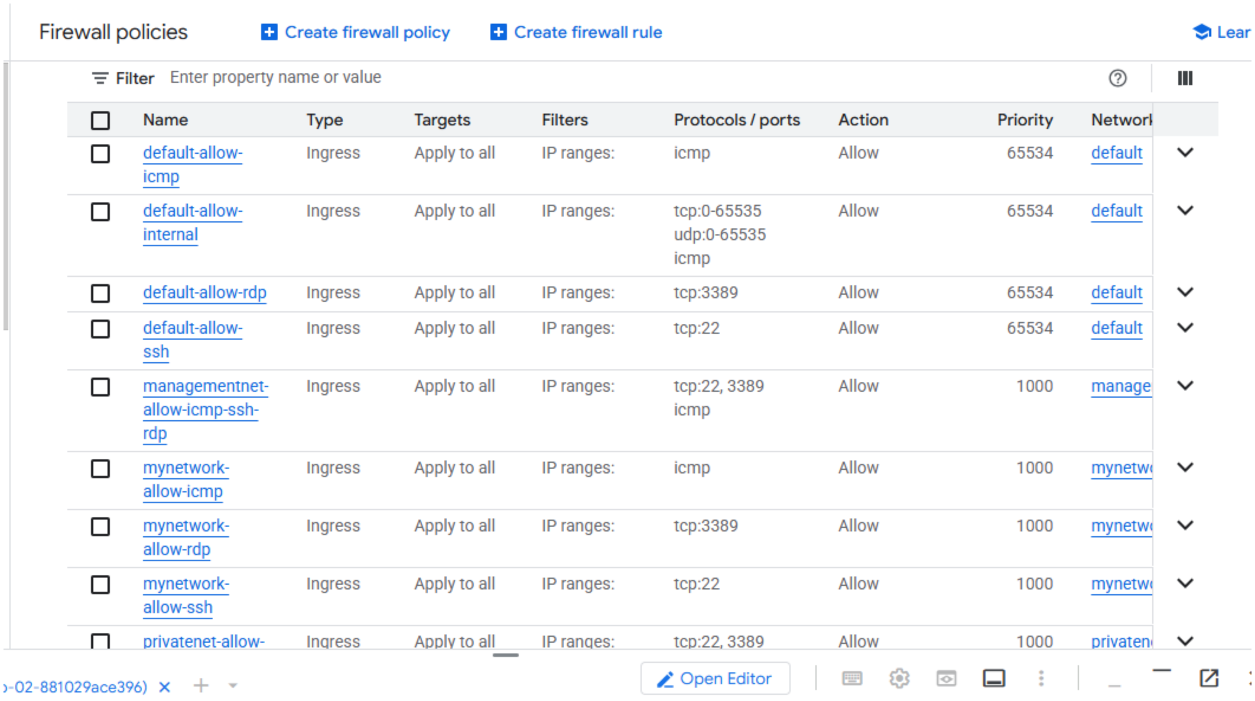
Network	managementnet
Subnetwork	managementsubnet-1

5. Click **Done**.

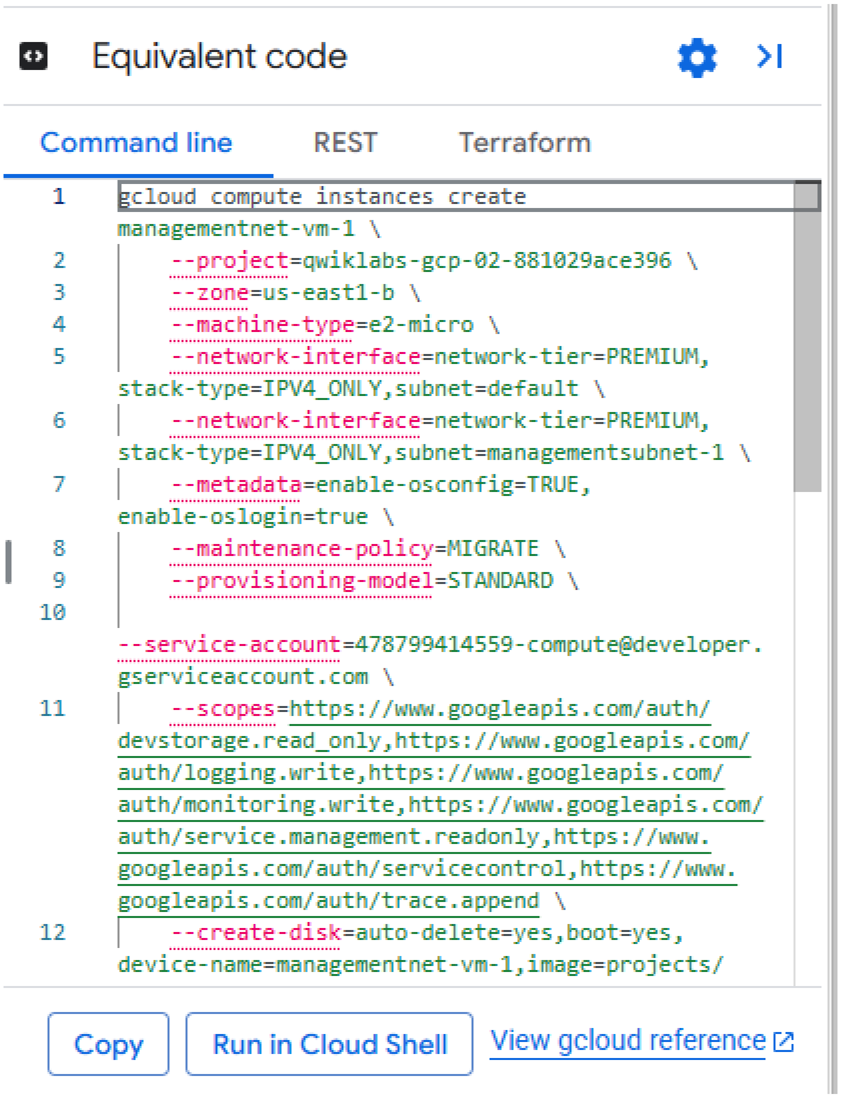
6. Click **EQUIVALENT CODE**.

This illustrate that VM instances can also be created using the Cloud Shell command line. You will create the **privatenet-vm-1** instance using these commands with similar parameters.

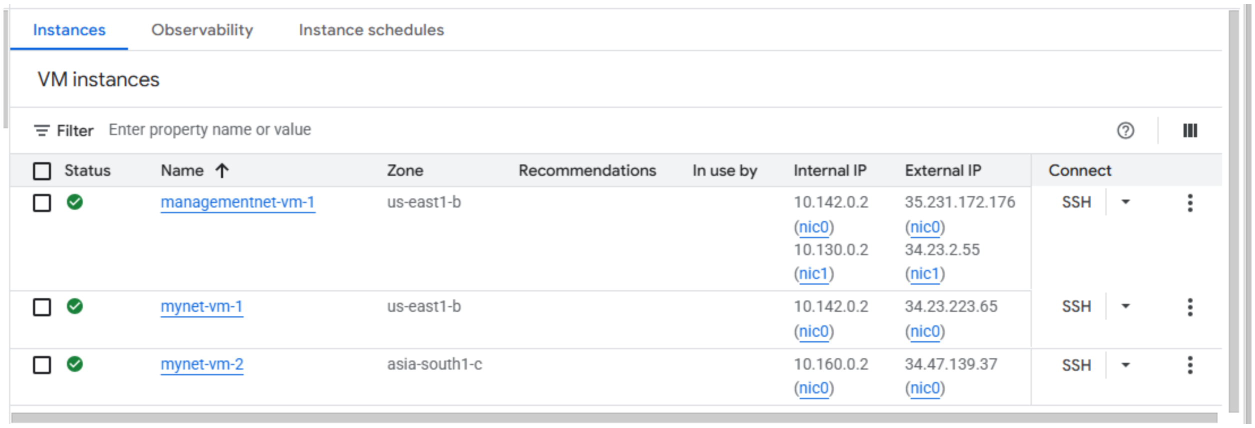
7. Click **Create**.



Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Networ
default-allow-icmp	Ingress	Apply to all	IP ranges:	icmp	Allow	65534	default
default-allow-internal	Ingress	Apply to all	IP ranges:	tcp:0-65535 udp:0-65535 icmp	Allow	65534	default
default-allow-rdp	Ingress	Apply to all	IP ranges:	tcp:3389	Allow	65534	default
default-allow-ssh	Ingress	Apply to all	IP ranges:	tcp:22	Allow	65534	default
managementnet-allow-icmp-ssh-rdp	Ingress	Apply to all	IP ranges:	tcp:22, 3389 icmp	Allow	1000	manage
mynetwork-allow-icmp	Ingress	Apply to all	IP ranges:	icmp	Allow	1000	mynetw
mynetwork-allow-rdp	Ingress	Apply to all	IP ranges:	tcp:3389	Allow	1000	mynetw
mynetwork-allow-ssh	Ingress	Apply to all	IP ranges:	tcp:22	Allow	1000	mynetw
privatenet-allow-	Ingress	Apply to all	IP ranges:	tcp:22, 3389	Allow	1000	privaten



```
gcloud compute instances create managementnet-vm-1 \
    --project=qwiklabs-gcp-02-881029ace396 \
    --zone=us-east1-b \
    --machine-type=e2-micro \
    --network-interface=network-tier=PREMIUM,stack-type=IPV4_ONLY,subnet=default \
    --network-interface=network-tier=PREMIUM,stack-type=IPV4_ONLY,subnet=managementsubnet-1 \
    --metadata=enable-osconfig=TRUE,enable-oslogin=true \
    --maintenance-policy=MIGRATE \
    --provisioning-model=STANDARD \
    --service-account=478799414559-compute@developer.gserviceaccount.com \
    --scopes=https://www.googleapis.com/auth/devstorage.read_only,https://www.googleapis.com/auth/logging.write,https://www.googleapis.com/auth/monitoring.write,https://www.googleapis.com/auth/service.management.readonly,https://www.googleapis.com/auth/servicecontrol,https://www.googleapis.com/auth/trace.append \
    --create-disk=auto-delete=yes,boot=yes,device-name=managementnet-vm-1,image=projects/
```



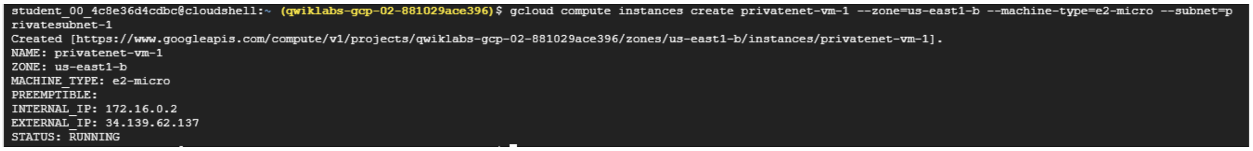
□	Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External IP	Connect
□	✓	managementnet-vm-1	us-east1-b			10.142.0.2 (nic0) 10.130.0.2 (nic1)	35.231.172.176 (nic0) 34.23.2.55 (nic1)	SSH
□	✓	mynet-vm-1	us-east1-b			10.142.0.2 (nic0)	34.23.223.65 (nic0)	SSH
□	✓	mynet-vm-2	asia-south1-c			10.160.0.2 (nic0)	34.47.139.37 (nic0)	SSH

Create the privatenet-vm-1 instance

Create the **privatenet-vm-1** instance using the Cloud Shell command line.

1. In Cloud Shell, run the following command to create the **privatenet-vm-1** instance:

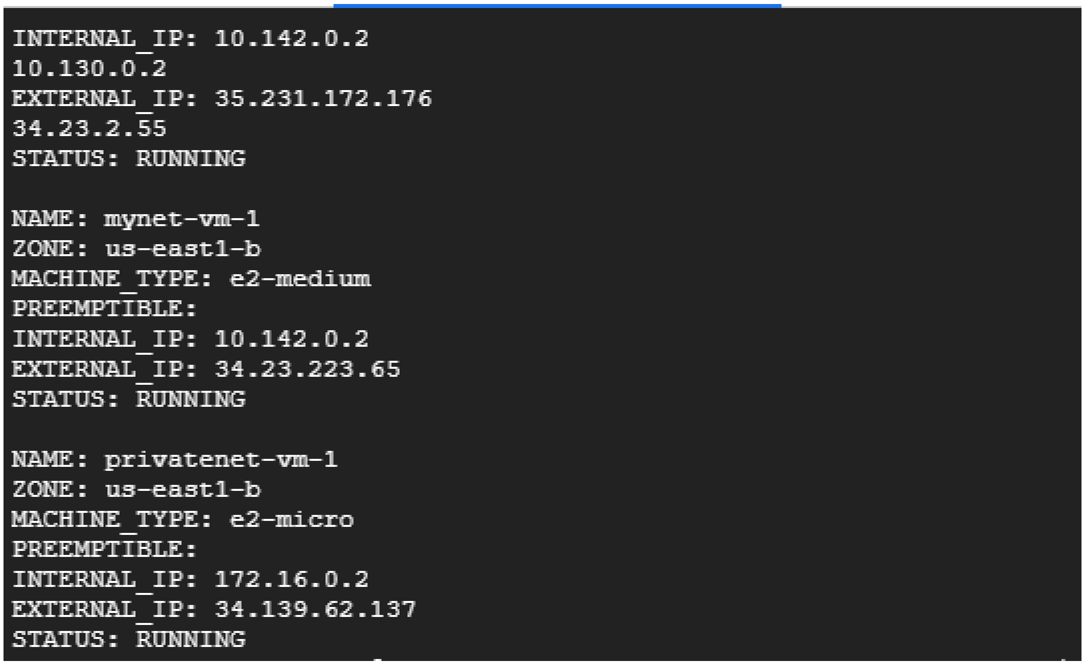
gcloud compute instances create privatenet-vm-1 --zone= --machine-type=e2-micro --subnet=privatesubnet-1



```
student_00_4c8e36d4cdbc@cloudshell:~ (qwiklabs-gcp-02-881029ace396)$ gcloud compute instances create privatenet-vm-1 --zone=us-east1-b --machine-type=e2-micro --subnet=p
rivatesubnet-1
Created [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-02-881029ace396/zones/us-east1-b/instances/privatenet-vm-1].
NAME: privatenet-vm-1
ZONE: us-east1-b
MACHINE_TYPE: e2-micro
PREEMPTIBLE:
INTERNAL_IP: 172.16.0.2
EXTERNAL_IP: 34.139.62.137
STATUS: RUNNING
```

2. Run the following command to list all the VM instances (sorted by zone):

gcloud compute instances list --sort-by=ZONE



```
INTERNAL_IP: 10.142.0.2
10.130.0.2
EXTERNAL_IP: 35.231.172.176
34.23.2.55
STATUS: RUNNING

NAME: mynet-vm-1
ZONE: us-east1-b
MACHINE_TYPE: e2-medium
PREEMPTIBLE:
INTERNAL_IP: 10.142.0.2
EXTERNAL_IP: 34.23.223.65
STATUS: RUNNING

NAME: privatenet-vm-1
ZONE: us-east1-b
MACHINE_TYPE: e2-micro
PREEMPTIBLE:
INTERNAL_IP: 172.16.0.2
EXTERNAL_IP: 34.139.62.137
STATUS: RUNNING
```

3. In the Cloud console, navigate to **Navigation menu** (☰) > **Compute Engine** > **VM instances**.

4. You see that the VM instances are listed in the Cloud console.

5. Click on **Column display options**, then select **Network**. Click **Ok**.

There are three instances in **Region_1** and one instance in **Region_2**. However, these instances are spread across three VPC networks (**managementnet**, **mynetwork** and **privatenet**), with no instance in the same zone and network as another. In the next section, you explore the effect this has on internal connectivity.

Task 3. Explore the connectivity between VM instances

Explore the connectivity between the VM instances. Specifically, determine the effect of having VM instances in the same zone versus having instances in the same VPC network.

Ping the external IP addresses

Ping the external IP addresses of the VM instances to determine if you can reach the instances from the public internet.

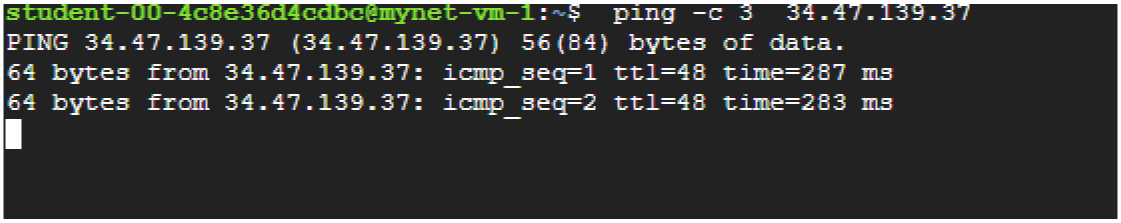
1. In the Cloud console, navigate to Navigation menu > Compute Engine > VM instances.

2. Note the external IP addresses for mynet-vm-2, managementnet-vm-1, and privatenet-vm-1.

3. For mynet-vm-1, click SSH to launch a terminal and connect.

4. To test connectivity to mynet-vm-2's external IP, run the following command, replacing mynet-vm-2's external IP:

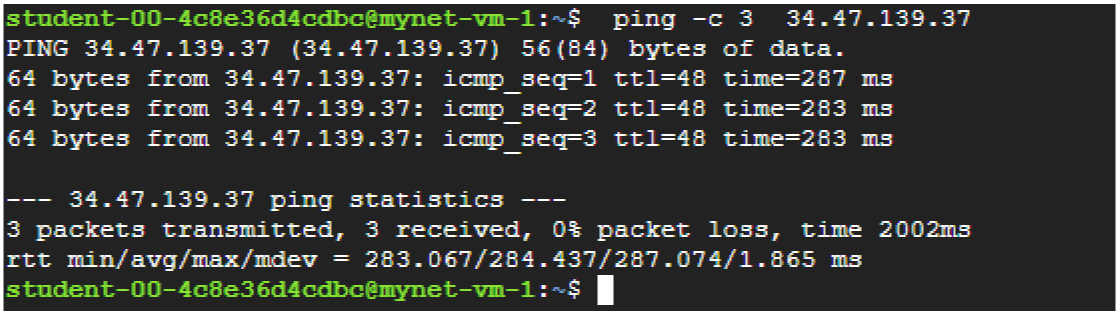
   ping -c 3 'Enter mynet-vm-2 external IP here'



```
student-00-4c8e36d4cdbc@mynet-vm-1:~$  ping -c 3  34.47.139.37
PING 34.47.139.37 (34.47.139.37) 56(84) bytes of data.
64 bytes from 34.47.139.37: icmp_seq=1 ttl=48 time=287 ms
64 bytes from 34.47.139.37: icmp_seq=2 ttl=48 time=283 ms
```

5. To test connectivity to **managementnet-vm-1**'s external IP, run the following command, replacing **managementnet-vm-1**'s external IP:

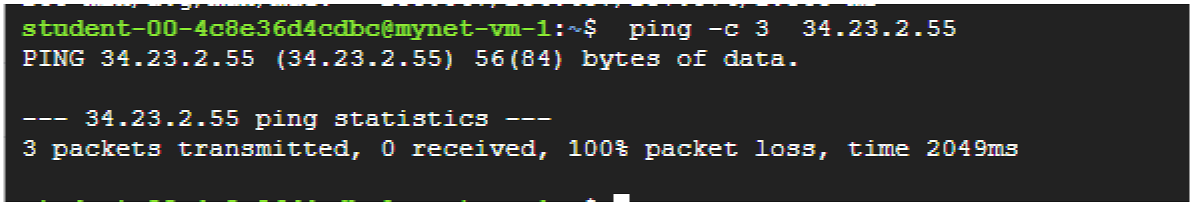
   ping -c 3 'Enter managementnet-vm-1 external IP here'



```
student-00-4c8e36d4cdbc@mynet-vm-1:~$  ping -c 3  34.47.139.37
PING 34.47.139.37 (34.47.139.37) 56(84) bytes of data.
64 bytes from 34.47.139.37: icmp_seq=1 ttl=48 time=287 ms
64 bytes from 34.47.139.37: icmp_seq=2 ttl=48 time=283 ms
64 bytes from 34.47.139.37: icmp_seq=3 ttl=48 time=283 ms

--- 34.47.139.37 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 283.067/284.437/287.074/1.865 ms
student-00-4c8e36d4cdbc@mynet-vm-1:~$
```

6. To test connectivity to **privatenet-vm-1**'s external IP, run the following command, replacing **privatenet-vm-1**'s external IP:

   ping -c 3 'Enter privatenet-vm-1 external IP here'



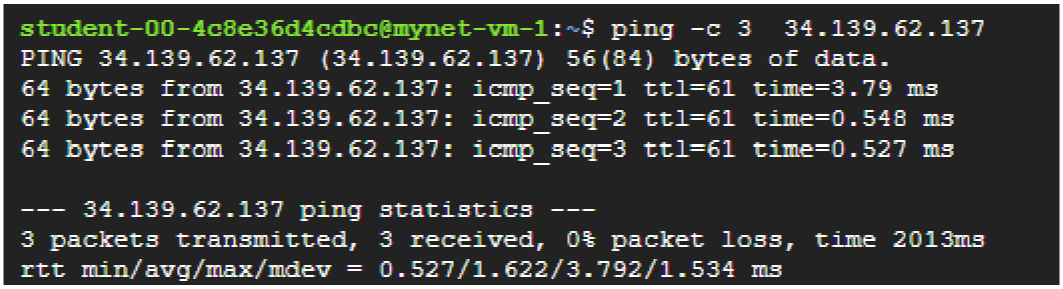
```
student-00-4c8e36d4cdbc@mynet-vm-1:~$  ping -c 3  34.23.2.55
PING 34.23.2.55 (34.23.2.55) 56(84) bytes of data.

--- 34.23.2.55 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2049ms
```

Ping the internal IP addresses

Ping the internal IP addresses of the VM instances to determine if you can reach the instances from within a VPC network.

1. In the Cloud console, navigate to **Navigation menu** > **Compute Engine** > **VM instances**.
2. Note the internal IP addresses for **mynet-vm-2**, **managementnet-vm-1**, and **privatenet-vm-1**.
3. Return to the **SSH** terminal for **mynet-vm-1**.
4. To test connectivity to **mynet-vm-2**'s internal IP, run the following command, replacing **mynet-vm-2**'s internal IP:

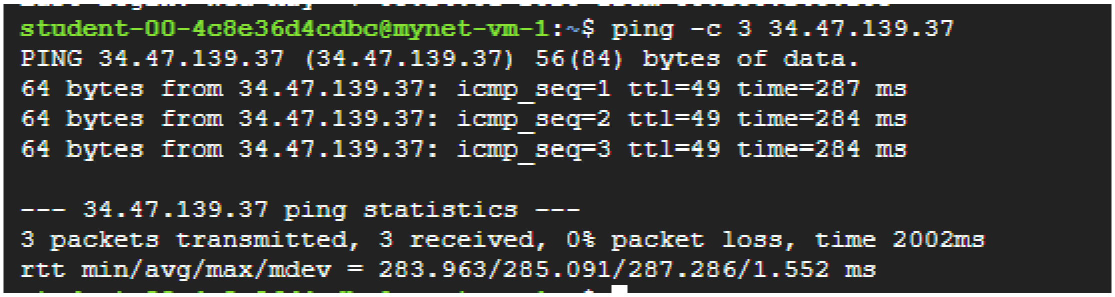
   ping -c 3 'Enter mynet-vm-2 internal IP here'



```
student-00-4c8e36d4cdbc@mynet-vm-1:~$ ping -c 3  34.139.62.137
PING 34.139.62.137 (34.139.62.137) 56(84) bytes of data.
64 bytes from 34.139.62.137: icmp_seq=1 ttl=61 time=3.79 ms
64 bytes from 34.139.62.137: icmp_seq=2 ttl=61 time=0.548 ms
64 bytes from 34.139.62.137: icmp_seq=3 ttl=61 time=0.527 ms

--- 34.139.62.137 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2013ms
rtt min/avg/max/mdev = 0.527/1.622/3.792/1.534 ms
```

5. To test connectivity to **managementnet-vm-1**'s internal IP, run the following command, replacing **managementnet-vm-1**'s internal IP:

   ping -c 3 'Enter managementnet-vm-1 internal IP here'



```
student-00-4c8e36d4cdbc@mynet-vm-1:~$ ping -c 3 34.47.139.37
PING 34.47.139.37 (34.47.139.37) 56(84) bytes of data.
64 bytes from 34.47.139.37: icmp_seq=1 ttl=49 time=287 ms
64 bytes from 34.47.139.37: icmp_seq=2 ttl=49 time=284 ms
64 bytes from 34.47.139.37: icmp_seq=3 ttl=49 time=284 ms

--- 34.47.139.37 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 283.963/285.091/287.286/1.552 ms
```

6. To test connectivity to **privatenet-vm-1**'s internal IP, run the following command, replacing **privatenet-vm-1**'s internal IP:

   ping -c 3 'Enter privatenet-vm-1 internal IP here'

   VPC networks are by default isolated private networking domains. However, no internal IP address communication is allowed between networks, unless you set up mechanisms such as VPC peering or VPN.

Task 4. Create a VM instance with multiple network interfaces

Every instance in a VPC network has a default network interface. You can create additional network interfaces attached to your VMs. Multiple network interfaces enable you to create configurations in which an instance connects directly to several VPC networks (up to 8 interfaces, depending on the instance's type).

Create the VM instance with multiple network interfaces

Create the **vm-appliance** instance with network interfaces in **privatesubnet-1**, **managementsubnet-1** and **mynetwork**. The CIDR ranges of these subnets do not overlap, which is a requirement for creating a VM with multiple network interface controllers (NICs).

1. In the Cloud console, navigate to **Navigation menu** > **Compute Engine** > **VM instances**.
2. Click **Create Instance**.
3. In the **Machine configuration**:

   Set the following values, leave all other values at their defaults:

Property	Value (type value or select option as specified)
Name	vm-appliance
Region	`US_Region`
Zone	`US_Zone`

Series	E2
Machine Type	`e2-standard-4`

4. Click **Networking**.

   For **Network interfaces**, click the dropdown to edit. Set the following values, leave all other values at their defaults:

Property	**Value (type value or select option as specified)**
Network	privatenet
Subnetwork	privatesubnet-1

   Click **Done**.

   Click **Add a network interface**.

   Set the following values, leave all other values at their defaults:

Property	**Value (type value or select option as specified)**
Network	managementnet
Subnetwork	managementsubnet-1

   Click **Done**.

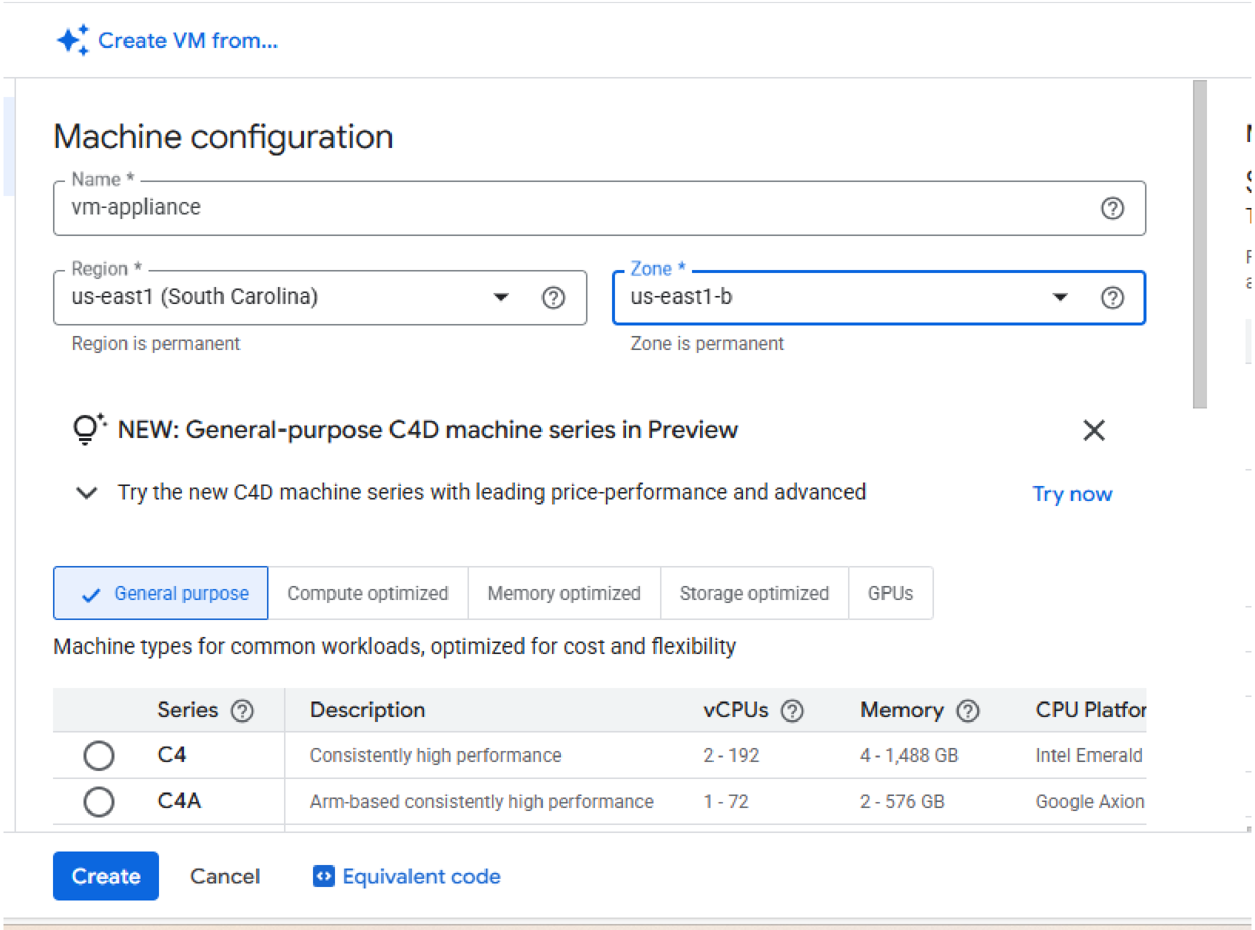
   Click **Add a network interface**.

   Set the following values, leave all other values at their defaults:

Property	Value (type value or select option as specified)
Network	mynetwork
Subnetwork	mynetwork

5. Click **Done**.

6. Click **Create**.



Create VM from...

Machine configuration

Name * vm-appliance

Region * us-east1 (South Carolina)

Region is permanent

Zone * us-east1-b

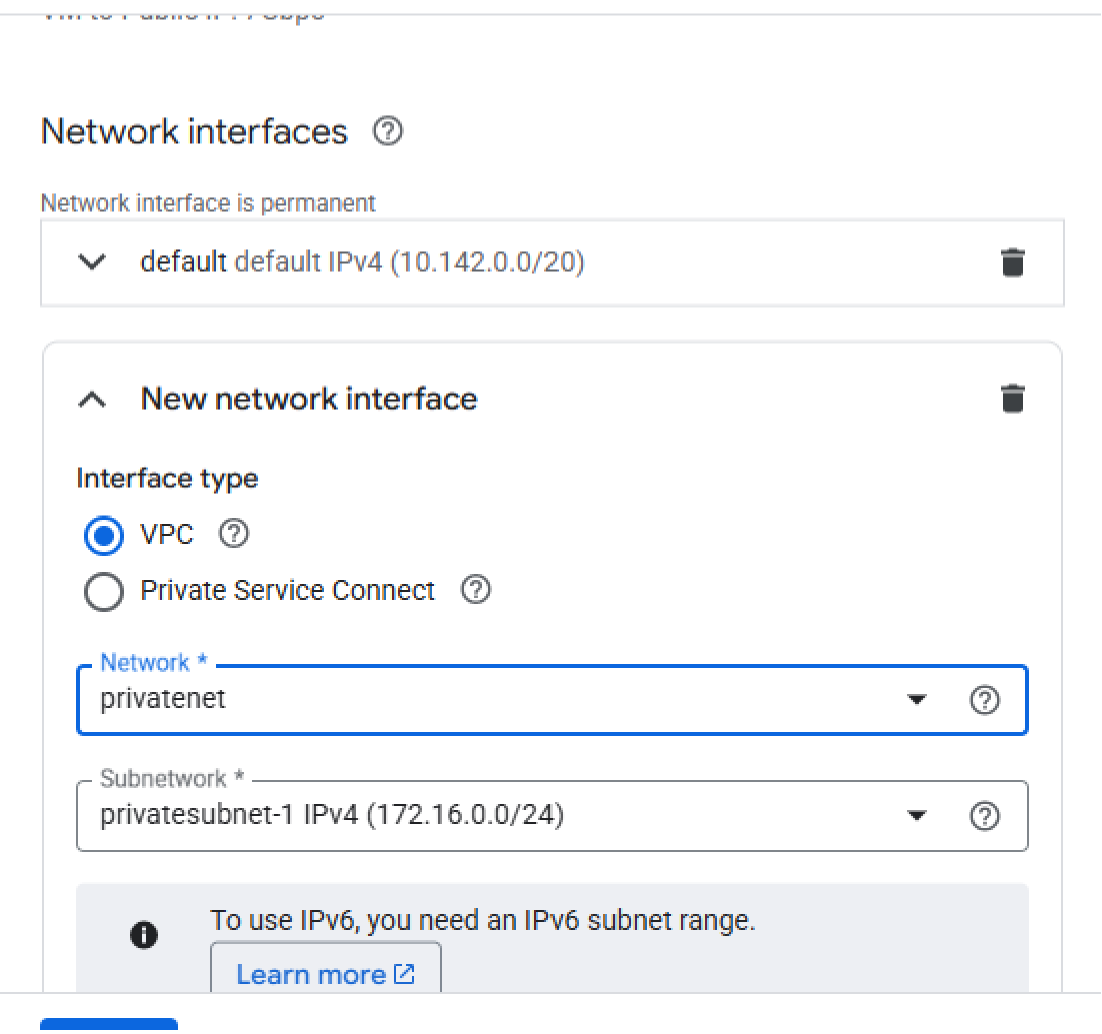
Zone is permanent

NEW: General-purpose C4D machine series in Preview

Try the new C4D machine series with leading price-performance and advanced

Machine types for common workloads, optimized for cost and flexibility

	Series	Description	vCPUs	Memory	CPU Platfor
○	C4	Consistently high performance	2 - 192	4 - 1,488 GB	Intel Emerald
○	C4A	Arm-based consistently high performance	1 - 72	2 - 576 GB	Google Axion



Network interfaces

Network interface is permanent

default default IPv4 (10.142.0.0/20)

New network interface

Interface type

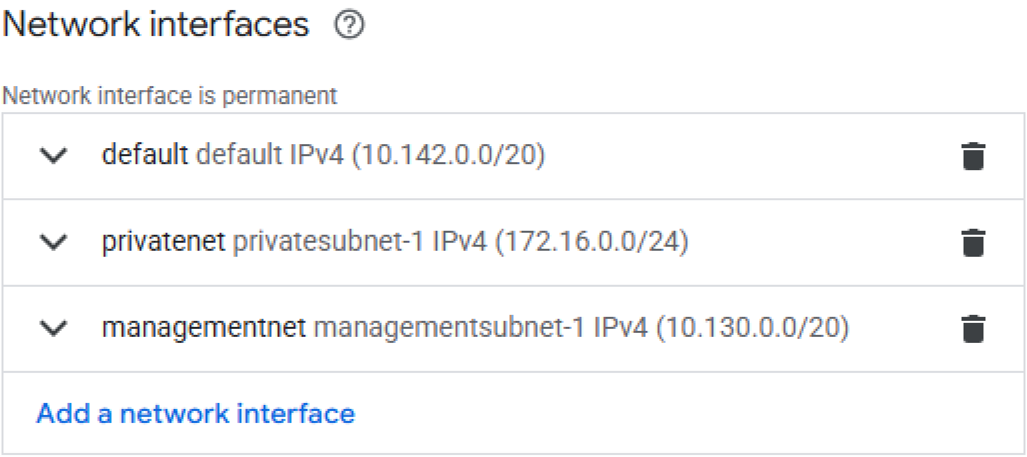
● VPC

○ Private Service Connect

Network *: privatenet

Subnetwork *: privatesubnet-1 IPv4 (172.16.0.0/24)

To use IPv6, you need an IPv6 subnet range.



Network interfaces

Network interface is permanent

default default IPv4 (10.142.0.0/20)

privatenet privatesubnet-1 IPv4 (172.16.0.0/24)

managementnet managementsubnet-1 IPv4 (10.130.0.0/20)

Explore the network interface details

Explore the network interface details of vm-appliance within the Cloud console and within the VM's terminal.

1. In the Cloud console, navigate to Navigation menu (☰) > Compute Engine > VM instances.
2. Click nic0 within the Internal IP address of vm-appliance to open the Network interface details page.
3. Verify that nic0 is attached to privatesubnet-1, is assigned an internal IP address within that subnet (172.16.0.0/24), and has applicable firewall rules.
4. Click nic0 and select nic1.
5. Verify that nic1 is attached to managementsubnet-1, is assigned an internal IP address within that subnet (10.130.0.0/20), and has applicable firewall rules.
6. Click nic1 and select nic2.
7. Verify that nic2 is attached to mynetwork, is assigned an internal IP address withinIn the Cloud console, navigate to **Navigation menu** > **Compute Engine** > **VM instances**.
8. For **vm-appliance**, click **SSH** to launch a terminal and connect.
9. Run the following, to list the network interfaces within the VM instance:
10. that subnet (10.128.0.0/20), and has applicable firewall rules.

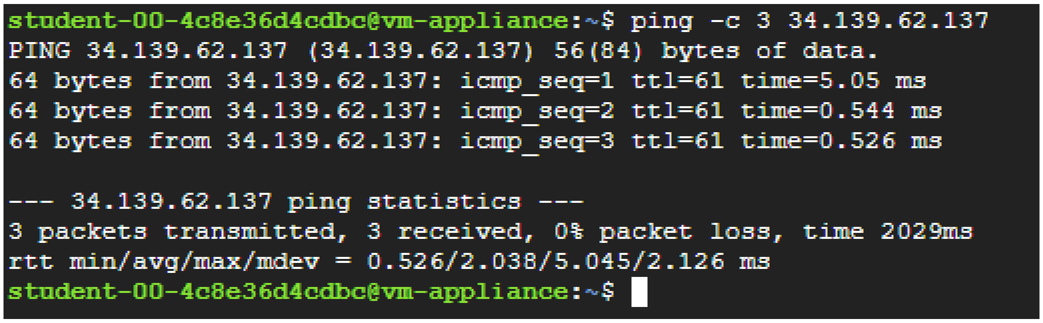
```
sudo ifconfig
```

Explore the network interface connectivity

Demonstrate that the **vm-appliance** instance is connected to **privatesubnet-1**, **managementsubnet-1** and **mynetwork** by pinging VM instances on those subnets.

1. In the Cloud console, navigate to **Navigation menu** > **Compute Engine** > **VM instances**.
2. Note the internal IP addresses for **privatenet-vm-1**, **managementnet-vm-1**, **mynet-vm-1**, and **mynet-vm-2**.
3. Return to the **SSH** terminal for **vm-appliance**.
4. To test connectivity to **privatenet-vm-1**'s internal IP, run the following command, replacing **privatenet-vm-1**'s internal IP:

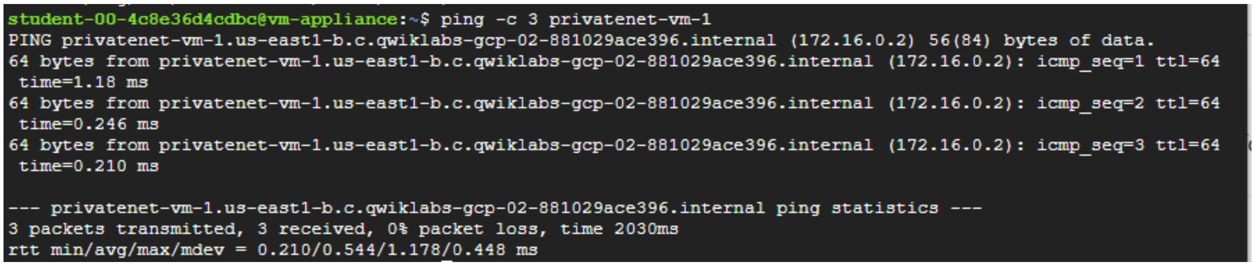
ping -c 3 'Enter privatenet-vm-1's internal IP here'



```
student-00-4c8e36d4cdbc@vm-appliance:~$ ping -c 3 34.139.62.137
PING 34.139.62.137 (34.139.62.137) 56(84) bytes of data.
64 bytes from 34.139.62.137: icmp_seq=1 ttl=61 time=5.05 ms
64 bytes from 34.139.62.137: icmp_seq=2 ttl=61 time=0.544 ms
64 bytes from 34.139.62.137: icmp_seq=3 ttl=61 time=0.526 ms

--- 34.139.62.137 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2029ms
rtt min/avg/max/mdev = 0.526/2.038/5.045/2.126 ms
student-00-4c8e36d4cdbc@vm-appliance:~$
```

5. Repeat the same test by running the following:

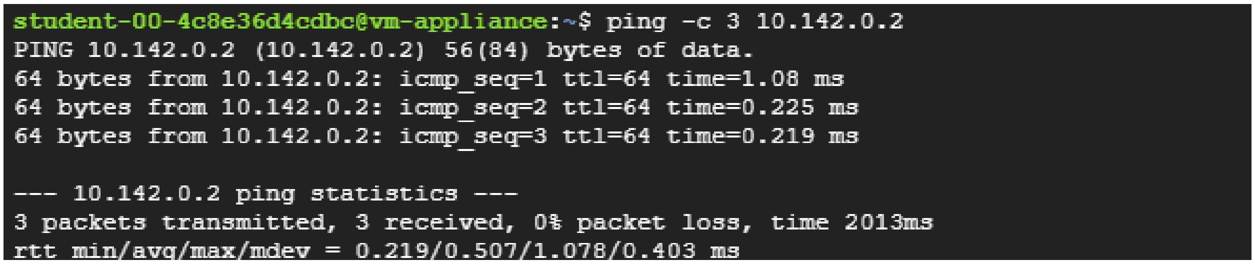
   ping -c 3 privatenet-vm-1



```
student-00-4c8e36d4cdbc@vm-appliance:~$ ping -c 3 privatenet-vm-1
PING privatenet-vm-1.us-east1-b.c.qwiklabs-gcp-02-881029ace396.internal (172.16.0.2) 56(84) bytes of data.
64 bytes from privatenet-vm-1.us-east1-b.c.qwiklabs-gcp-02-881029ace396.internal (172.16.0.2): icmp_seq=1 ttl=64
 time=1.18 ms
64 bytes from privatenet-vm-1.us-east1-b.c.qwiklabs-gcp-02-881029ace396.internal (172.16.0.2): icmp_seq=2 ttl=64
 time=0.246 ms
64 bytes from privatenet-vm-1.us-east1-b.c.qwiklabs-gcp-02-881029ace396.internal (172.16.0.2): icmp_seq=3 ttl=64
 time=0.210 ms

--- privatenet-vm-1.us-east1-b.c.qwiklabs-gcp-02-881029ace396.internal ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2030ms
rtt min/avg/max/mdev = 0.210/0.544/1.178/0.448 ms
```

6. To test connectivity to **managementnet-vm-1**'s internal IP, run the following command, replacing **managementnet-vm-1**'s internal IP:

   ping -c 3 'Enter managementnet-vm-1's internal IP here'



```
student-00-4c8e36d4cdbc@vm-appliance:~$ ping -c 3 10.142.0.2
PING 10.142.0.2 (10.142.0.2) 56(84) bytes of data.
64 bytes from 10.142.0.2: icmp_seq=1 ttl=64 time=1.08 ms
64 bytes from 10.142.0.2: icmp_seq=2 ttl=64 time=0.225 ms
64 bytes from 10.142.0.2: icmp_seq=3 ttl=64 time=0.219 ms

--- 10.142.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2013ms
rtt min/avg/max/mdev = 0.219/0.507/1.078/0.403 ms
```

7. To test connectivity to **mynet-vm-1**'s internal IP, run the following command, replacing **mynet-vm-1**'s internal IP:

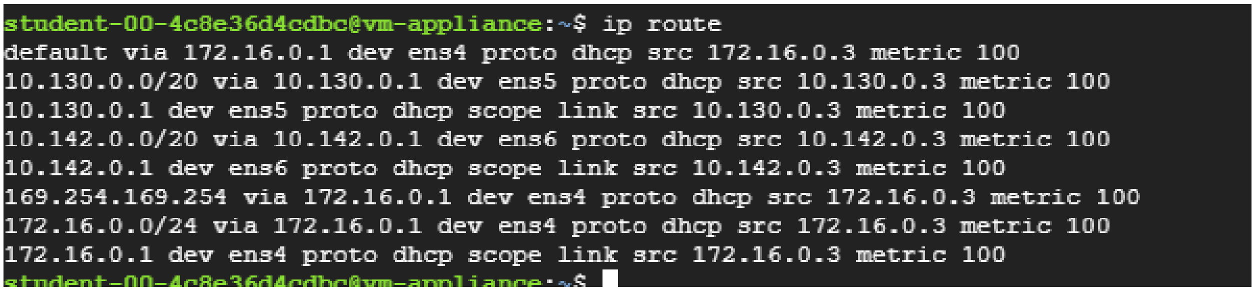
   ping -c 3 'Enter mynet-vm-1's internal IP here'

8. To test connectivity to **mynet-vm-2**'s internal IP, run the following command, replacing **mynet-vm-2**'s internal IP:

   ping -c 3 'Enter mynet-vm-2's internal IP here'

9. To list the routes for **vm-appliance** instance, run the following command:

ip route



```
student-00-4c8e36d4cdbc@vm-appliance:~$ ip route
default via 172.16.0.1 dev ens4 proto dhcp src 172.16.0.3 metric 100
10.130.0.0/20 via 10.130.0.1 dev ens5 proto dhcp src 10.130.0.3 metric 100
10.130.0.1 dev ens5 proto dhcp scope link src 10.130.0.3 metric 100
10.142.0.0/20 via 10.142.0.1 dev ens6 proto dhcp src 10.142.0.3 metric 100
10.142.0.1 dev ens6 proto dhcp scope link src 10.142.0.3 metric 100
169.254.169.254 via 172.16.0.1 dev ens4 proto dhcp src 172.16.0.3 metric 100
172.16.0.0/24 via 172.16.0.1 dev ens4 proto dhcp src 172.16.0.3 metric 100
172.16.0.1 dev ens4 proto dhcp scope link src 172.16.0.3 metric 100
student-00-4c8e36d4cdbc@vm-appliance:~$
```