VPC Networking

View the firewall rules

Each VPC network implements a distributed virtual firewall that you can configure. Firewall rules allow you to control which packets are allowed to travel to which destinations. Every VPC network has two implied firewall rules that block all incoming connections and allow all outgoing connections.

The following command describes an individual firewall rule. Replace [FIREWALL-NAME] with the name of the firewall rule. Because firewall rule names are unique to the project, you don't have to specify a network when describing an existing one.

Notice that there are 4 **Ingress** firewall rules for the **default** network:

- default-allow-icmp
- default-allow-rdp
- default-allow-ssh
- default-allow-internal

```
gcloud compute firewall-rules describe [FIREWALL-NAME]
```

Delete the Firewall rules

The following command deletes a firewall rule. Replace [FIREWALL-NAME] with the name of the rule to be deleted.

```
gcloud compute firewall-rules delete [FIREWALL-NAME]
```

Repeat this for each of the firewall-rules listed above.

Delete the default network

To delete the default network, run:

```
gcloud compute networks delete default
```

Output:

```
The following networks will be deleted:
 - [default-network]

Do you want to continue (Y/n)?  y
```

Press enter to continue:

Try to create a VM instance

Verify that you cannot create a VM instance without a VPC network, run:

```
gcloud compute instances create [INSTANCE_NAME]
```

As expected, you cannot create a VM instance without a VPC network!

Create an auto mode VPC network with firewall rules

1.
```
gcloud compute networks create mynetwork --project=[PROJECT-
```

```
ID] subnet-mode=auto --bgp-routing-mode=regional
```

2.
```
gcloud compute firewall-rules create mynetwork-allow-icmp --
project=[PROJECT-ID]  --network=projects/[PROJECT-ID]
/global/networks/mynetwork --description=Allows\ ICMP\
connections\ from\ any\ source\ to\ any\ instance\ on\ the\
network. --direction=INGRESS --priority=65534 --source-
ranges=0.0.0.0/0 --action=ALLOW --rules=icmp
```

3.
```
gcloud compute firewall-rules create mynetwork-allow-internal
--project=[PROJECT-ID]  --network=projects/[PROJECT-ID]
/global/networks/mynetwork --description=Allows\ connections\
from\ any\ source\ in\ the\ network\ IP\ range\ to\ any\
instance\ on\ the\ network\ using\ all\ protocols. --
direction=INGRESS --priority=65534 --source-
ranges=10.128.0.0/9 --action=ALLOW --rules=all
```

4.
```
gcloud compute firewall-rules create mynetwork-allow-rdp --
project=[PROJECT-ID]  --network=projects/[PROJECT-ID]
/global/networks/mynetwork --description=Allows\ RDP\
connections\ from\ any\ source\ to\ any\ instance\ on\ the\
network\ using\ port\ 3389. --direction=INGRESS --
priority=65534 --source-ranges=0.0.0.0/0 --action=ALLOW --
rules=tcp:3389
```

5.
```
gcloud compute firewall-rules create mynetwork-allow-ssh --
project=[PROJECT-ID]  --network=projects/[PROJECT-ID]
/global/networks/mynetwork --description=Allows\ TCP\
connections\ from\ any\ source\ to\ any\ instance\ on\ the\
network\ using\ port\ 22. --direction=INGRESS --priority=65534
--source-ranges=0.0.0.0/0 --action=ALLOW --rules=tcp:22
```

Create a VM instance in us-central1

Create a VM instance in the us-central1 region. Selecting a region and zone determines the subnet and assigns the internal IP address from the subnet's IP address range.

1. Property	2. Value (type value or select option as specified)
3. Name	4. mynet-us-vm
5. Region	6. us-central1
7. Zone	8. us-central1-c
9. Machine type	10. n1-standard-1 (1 vCPU, 3.75 GB memory)

gcloud beta compute --project=[PROJECT-ID] instances create mynet-us-vm --zone=us-central1-c --machine-type=n1-standard-1 --subnet=default --network-tier=PREMIUM --maintenance-policy=MIGRATE --service-account=441967460138-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/servicecontrol,https://www.googleapis.com/auth/service.management.readonly,https://www.googleapis.com/auth/trace.append --image=debian-9-stretch-v20200902 --image-project=debian-cloud --boot-disk-size=10GB --boot-disk-type=pd-standard --boot-disk-device-name=mynet-us-vm --reservation-affinity=any

Output:

```
NAME         ZONE           MACHINE_TYPE   PREEMPTIBLE
INTERNAL_IP  EXTERNAL_IP    STATUS
mynet-us-vm  us-central1-c  n1-standard-1
10.128.0.2   34.123.171.80  RUNNING
```

Create a VM instance in europe-west1

1. Specify the following, and leave the remaining settings as their defaults:

2. Property	3. Value (type value or select option as specified)
4. Name	5. mynet-eu-vm

6. Region	7. europe-west1
8. Zone	9. europe-west1-c
10. Machine type	11. n1-standard-1 (1 vCPU, 3.75 GB memory)

gcloud beta compute --project=[PROJECT-ID] instances create mynet-eu-vm --zone=europe-west1-c --machine-type=n1-standard-1 --subnet=mynetwork --network-tier=PREMIUM --maintenance-policy=MIGRATE --service-account=890053130700-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/servicecontrol,https://www.googleapis.com/auth/service.management.readonly,https://www.googleapis.com/auth/trace.append --image=debian-9-stretch-v20200902 --image-project=debian-cloud --boot-disk-size=10GB --boot-disk-type=pd-standard --boot-disk-device-name=mynet-eu-vm --reservation-affinity=any

Verify that the **Internal IP** for the new instance was assigned from the IP address range for the subnet in **europe-west1** (10.132.0.0/20).

The **Internal IP** should be 10.132.0.2 because 10.132.0.1 is reserved for the gateway, and you have not configured any other instances in that subnet.

Output:

```
AME          ZONE             MACHINE_TYPE    PREEMPTIBLE
INTERNAL_IP  EXTERNAL_IP    STATUS
mynet-eu-vm  europe-west1-c  n1-standard-1
10.132.0.2   34.76.82.245  RUNNING
```

Verify connectivity for the VM instances

The firewall rules that you created with **mynetwork** allow ingress SSH and ICMP

traffic from within **mynetwork** (internal IP) and outside that network (external IP).

Run the following code:

```
gcloud compute ssh [USER]@qwiklabs.
net@mynet-eu-vm
```

2. Type y and press to continue.

Leave the passphrase blank and when asked again press enter.
Your identification is saved, take note of this, it is the username needed in the next step. This should start with ‘student’

If you are asked to identify a region, type y if it is the same region you used when creating the VM, otherwise type n.

You will then be asked to match the correct zone and region. Take note of the region number followed by the zone number.

Output:

```
No zone specified. Using zone [europe-west1-c] for instance:
[mynet-eu-vm].
Warning: Permanently added 'compute.3103395765129373057'
(ECDSA) to the list of known hosts.
Linux mynet-eu-vm 4.9.0-13-amd64 #1 SMP Debian 4.9.228-1
(2020-07-05) x86_64

The programs included with the Debian GNU/Linux system are
free software;
the exact distribution terms for each program are described in
the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the
extent
permitted by applicable law.
Creating directory '/home/student-02-04dc6aaa1069'.
student-02-04dc6aaa1069@mynet-eu-vm:~$ ping -c
```

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

```
ping -c 3 <Enter mynet-eu-vm's internal IP here>
```

Output:

```
PING 34.76.82.245 (34.76.82.245) 56(84) bytes of data.
64 bytes from 34.76.82.245: icmp_seq=1 ttl=64 time=0.773 ms
64 bytes from 34.76.82.245: icmp_seq=2 ttl=64 time=0.412 ms
64 bytes from 34.76.82.245: icmp_seq=3 ttl=64 time=0.354 ms

--- 34.76.82.245 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2053ms
rtt min/avg/max/mdev = 0.354/0.513/0.773/0.185 ms
student-02-04dc6aaa1069@mynet-eu-vm:~$
```

4. Repeat the same test by running the following:

```
ping -c 3 mynet-eu-vm
```

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

```
ping -c 3 <Enter mynet-eu-vm's external IP here>
```

Convert the network to a custom mode network

Exit out of the shell. Run:

```
exit
```

The auto mode network worked great so far, but you have been asked to convert it to a custom mode network so that new subnets aren't automatically created as new regions become available. This could result in overlap with IP addresses used by manually created subnets or static routes, or could interfere with your overall network

planning.

```
gcloud compute networks update mynetwork \
    --switch-to-custom-subnet-mode
```

When prompted, type y and continue.

Specify the following, and leave the remaining settings as their defaults:

Property	Value (type value or select option as specified)
Name	managementsubnet-us
Region	us-central1
IP address range	10.130.0.0/20

Create the managementnet network

Create the **managementnet** network using the terminal.

```
gcloud compute networks create managementnet --
project=[PROJECT_ID] --subnet-mode=custom --bgp-routing-
mode=regional

gcloud compute networks subnets create managementsubnet-us --
project=[PROJECT_ID] --range=10.130.0.0/20 --
network=managementnet --region=us-central1
```

Output:

```
NAME                    REGION       NETWORK         RANGE
managementsubnet-us     us-central1  managementnet   10.130.0.0/20
```

Create the privatenet network

1.1. To create the **privatenet** network, run the following command:

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

4.2. To create the **privatesubnet-us** subnet, run the following command:

```
gcloud compute networks subnets create privatesubnet-us --
network=privatenet --region=us-central1 --range=172.16.0.0/24
```

5.3. To create the **privatesubnet-eu** subnet, run the following command:

```
gcloud compute networks subnets create privatesubnet-eu --
network=privatenet --region=europe-west1 --range=172.20.0.0/20
```

6.4. To list the available VPC networks, run the following command:

```
gcloud compute networks list
```

5. The output should look like this (**do not copy; this is example output**):

```
NAME           SUBNET_MODE  BGP_ROUTING_MODE  IPV4_RANGE
GATEWAY_IPV4
managementnet  CUSTOM       REGIONAL
mynetwork      CUSTOM       REGIONAL
privatenet     CUSTOM       REGIONAL
```

7.6. To list the available VPC subnets (sorted by VPC network), run the following command:

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

Output:

```
NAME                REGION                  NETWORK
RANGE
managementsubnet-us us-central1             managementnet
10.130.0.0/20
mynetwork           asia-northeast1         mynetwork
10.146.0.0/20
mynetwork           us-west1                mynetwork
10.138.0.0/20
mynetwork           southamerica-east1      mynetwork
10.158.0.0/20
mynetwork           europe-west4            mynetwork
10.164.0.0/20
mynetwork           asia-east1              mynetwork
10.140.0.0/20
mynetwork           europe-north1           mynetwork
10.166.0.0/20
mynetwork           asia-southeast1         mynetwork
10.148.0.0/20
mynetwork           us-east4                mynetwork
```

```
10.150.0.0/20
mynetwork           europe-west1             mynetwork
10.132.0.0/20
mynetwork           europe-west2             mynetwork
10.154.0.0/20
mynetwork           europe-west3             mynetwork
10.156.0.0/20
mynetwork           australia-southeast1     mynetwork
10.152.0.0/20
mynetwork           asia-south1              mynetwork
10.160.0.0/20
mynetwork           us-east1                 mynetwork
10.142.0.0/20
mynetwork           us-central1              mynetwork
10.128.0.0/20
mynetwork           northamerica-northeast1  mynetwork
10.162.0.0/20
privatesubnet-eu    europe-west1             privatenet
172.20.0.0/20
privatesubnet-us    us-central1              privatenet
172.16.0.0/24
```

7. Verify that the same networks and subnets are listed in the Cloud Console.

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

Create the firewall rules for managementnet

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

1. Specify the following, and leave the remaining settings as their defaults:

2. Property	3. Value (type value or select option as specified)
4. Name	5. managementnet-allow-icmp-ssh-rdp
6. Network	7. managementnet
8. Targets	9. All instances in the network
10. Source filter	11. IP Ranges
12. Source IP ranges	13. 0.0.0.0/0
14. Protocols and ports	15. Specified protocols and ports

```
gcloud compute --project=[PROJECT-ID] firewall-rules create
managementnet-allow-icmp-ssh-rdp --direction=INGRESS --
priority=1000 --network=managementnet --action=ALLOW --
rules=tcp:22,tcp:3389,icmp --source-ranges=0.0.0.0/0
```

Create the firewall rules for privatenet

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

1. To create the **privatenet-allow-icmp-ssh-rdp** firewall rule, run the following command:

```
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
```

Output:

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

3.2. To list all the firewall rules (sorted by VPC network), run the following command:

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

Output:

```
NAME                                    NETWORK        DIRECTION
PRIORITY  ALLOW
managementnet-allow-icmp-ssh-rdp  managementnet  INGRESS
1000      icmp,tcp:22,tcp:3389
mynetwork-allow-icmp              mynetwork      INGRESS
1000      icmp
mynetwork-allow-internal          mynetwork      INGRESS
65534     all
mynetwork-allow-rdp               mynetwork      INGRESS
1000      tcp:3389
mynetwork-allow-ssh               mynetwork      INGRESS
1000      tcp:22
privatenet-allow-icmp-ssh-rdp     privatenet     INGRESS
1000      icmp,tcp:22,tcp:3389
```

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

Create two VM instances:

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

Create the managementnet-us-vm instance

1. Specify the following, and leave the remaining settings as their defaults:

Property	Value (type value or select option as specified)
Name	managementnet-us-vm
Region	us-central1
Zone	us-central1-c
Machine type	f1-micro (1 vCPU, 614 MB memory)

Specify the following, and leave the remaining settings as their defaults:

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

```
gcloud beta compute --project=[PROJECT-ID]  instances create
managementnet-us-vm --zone=us-central1-c --machine-type=f1-
micro --subnet=managementsubnet-us --network-tier=PREMIUM --
maintenance-policy=MIGRATE --service-account=441967460138-
compute@developer.gserviceaccount.com --
scopes=https://www.googleapis.com/auth/devstorage.read_only,ht
tps://www.googleapis.com/auth/logging.write,https://www.google
apis.com/auth/monitoring.write,https://www.googleapis.com/auth
/servicecontrol,https://www.googleapis.com/auth/service.manage
ment.readonly,https://www.googleapis.com/auth/trace.append --
image=debian-9-stretch-v20200902 --image-project=debian-cloud
--boot-disk-size=10GB --boot-disk-type=pd-standard --boot-
disk-device-name=managementnet-us-vm --reservation-
affinity=any
```

Create the privatenet-us-vm instance

1. To create the **privatenet-us-vm** instance, run the following command:

```
gcloud compute instances create privatenet-us-vm --zone=us-
central1-c --machine-type=f1-micro --subnet=privatesubnet-us
```

Output:

```
Created
[https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-
00-c3c7336ff7b3/zones/us-central1-c/instances/privat
enet-us-vm].
NAME              ZONE           MACHINE_TYPE  PREEMPTIBLE
INTERNAL_IP  EXTERNAL_IP    STATUS
privatenet-us-vm  us-central1-c  f1-micro
172.16.0.2   34.122.161.88  RUNNING
```

To list all the VM instances (sorted by zone), run the following command:

```
gcloud compute instances list --sort-by=ZONE
```

Output:

```
NAME                  ZONE            MACHINE_TYPE  PREEMPTIBLE
INTERNAL_IP  EXTERNAL_IP    STATUS
mynet-eu-vm           europe-west1-c  n1-standard-1
10.132.0.2   34.76.115.41   RUNNING
managementnet-us-vm   us-central1-c   f1-micro
10.130.0.2   35.239.68.123  RUNNING
mynet-us-vm           us-central1-c   n1-standard-1
10.128.0.2   35.202.101.52  RUNNING
privatenet-us-vm      us-central1-c   f1-micro
172.16.0.2   34.66.197.202  RUNNING
```

Task 4. Explore the connectivity across networks

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

1.1. Enter the ssh terminal inside the shell

Run the following code:

```
gcloud compute ssh [USER]@qwiklabs.net@mynet-eu-vm
```

2. Type y and press to continue.

Once you have verified the zone you used to create the VM instance, this is an example of the output:

```
The programs included with the Debian GNU/Linux system are
free software;
the exact distribution terms for each program are described in
the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the
extent
permitted by applicable law.
Creating directory '/home/student-00-7cb7c3c22531'.
student-00-7cb7c3c22531@managementnet-us-vm:~$
```

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

1. run the following command, replacing **mynet-eu-vm**'s external IP:

```
ping -c 3 <Enter mynet-eu-vm's external IP here>
```

Output example:

```
PING 35.193.4.182 (35.193.4.182) 56(84) bytes of data.
64 bytes from 35.193.4.182: icmp_seq=1 ttl=64 time=1.07 ms
64 bytes from 35.193.4.182: icmp_seq=2 ttl=64 time=0.444 ms
64 bytes from 35.193.4.182: icmp_seq=3 ttl=64 time=0.419 ms

--- 35.193.4.182 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2011ms
rtt min/avg/max/mdev = 0.419/0.646/1.077/0.305 ms
```

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

```
ping -c 3 <Enter managementnet-us-vm's external IP here>
```

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

```
ping -c 3 <Enter privatenet-us-vm's external IP here>
```

You can ping the external IP address of all VM instances, even though they are in either a different zone or VPC network. This confirms that public access to those instances is only controlled by the **ICMP** firewall rules that you established earlier.

6. Ping the internal IP addresses

7. To exit out of the shell environment type:

```
8.  exit
```

9. To list the available VPC networks, run the following command and note the internal IP addresses of the VM instances:

```
gcloud compute networks list
```

Enter the ssh terminal again for the **mynet-us-vm**:

```
gcloud compute ssh [USER]@qwiklabs.net@mynet-eu-vm
```

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

```
ping -c 3 <Enter mynet-eu-vm's internal IP here>
```

You can ping the internal IP address of **mynet-eu-vm** because it is on the same VPC network as the source of the ping (**mynet-us-vm**), even though both VM instances are in separate zones, regions, and continents!

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

```
ping -c 3 <Enter managementnet-us-vm's internal IP here>
```

6. To exit out of the shell environment type:

```
7.  exit
```

Enter the ssh terminal again for the **managementnet-us-vm**'s:

```
gcloud compute ssh [USER]@qwiklabs.net@managementnet-us-vm
```

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

```
ping -c 3 <Enter managementnet-us-vm's internal IP here>
```

This should not work, as indicated by a 100% packet loss!

6. To exit out of the shell environment type:

7. exit

Enter the ssh terminal again for the **mynet-us-vm**:

```
gcloud compute ssh [USER]@qwiklabs.net@managementnet-us-vm
```

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

```
ping -c 3 <Enter managementnet-us-vm's internal IP here>
```

This should not work, as indicated by a 100% packet loss!