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

Delete the Firewall rules

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

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

Delete the default network

To delete the default network, run:

Output:

Press enter to continue:

Try to create a VM instance

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

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

Create an auto mode VPC network with firewall rules

1.

2.

3.

4.

5.

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.googl
eapis.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:

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.googl
eapis.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:

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:

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:

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

Output:

4. Repeat the same test by running the following:

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

Convert the network to a custom mode network

Exit out of the shell. Run:

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.

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.

Output:

Create the privatenet network

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

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

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

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

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

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

Output:

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

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

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:

Output:

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

Output:

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

Create the privatenet-us-vm instance

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

Output:

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

Output:

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:

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:

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:

Output example:

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

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

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:

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

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

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

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:

6. To exit out of the shell environment type:

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

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

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

6. To exit out of the shell environment type:

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

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