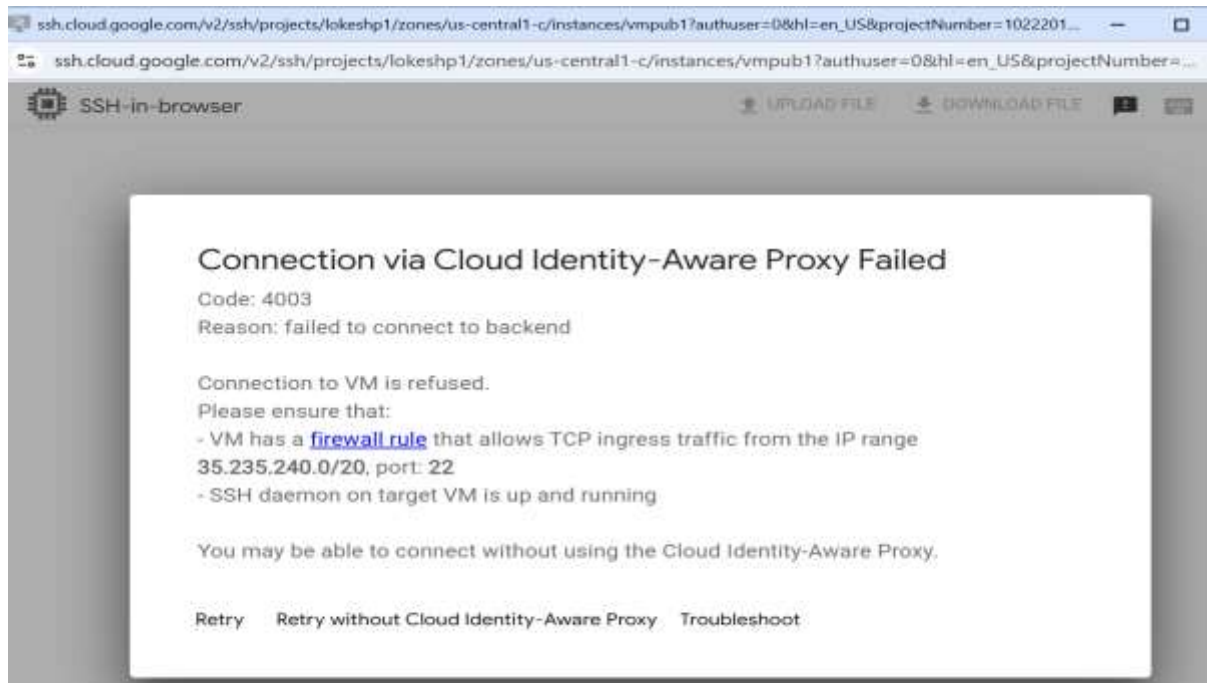
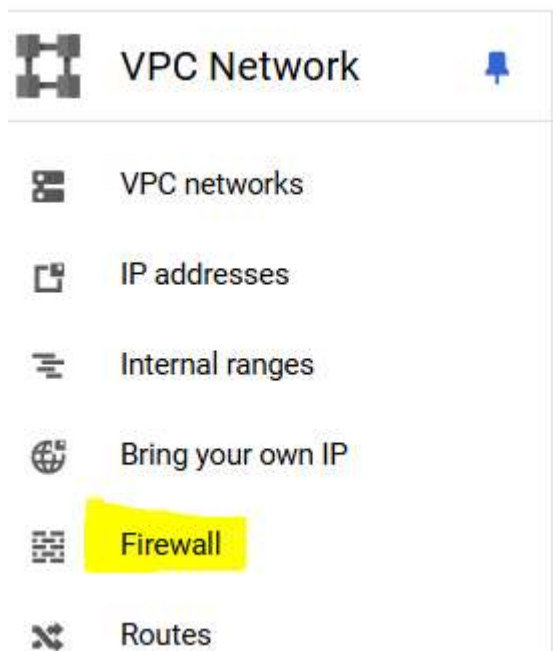


In this lab, we will explore connecting options for the VM we created in myvpc in the previous lab. We will also create firewall rules regarding this

First, go to the public VM and log in to it (This will not connect and give an error)



Now go to the VPC page and go to the Firewall



Here you will see, all rules are related to the “default” VPC only

<input type="checkbox"/>	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network ↑	Logs	
<input type="checkbox"/>	default-allow-http	Ingress	http-server	IP ranges:	tcp:8080	Allow	1000	default	Off	▼
<input type="checkbox"/>	default-allow-https	Ingress	https-	IP ranges:	tcp:443	Allow	1000	default	Off	▼
<input type="checkbox"/>	default-allow-icmp	Ingress	Apply to all	IP ranges:	icmp	Allow	65534	default	Off	▼
<input type="checkbox"/>	default-allow-internal	Ingress	Apply to all	IP ranges:	tcp:0-65535 udp:0-65535 icmp	Allow	65534	default	Off	▼
<input type="checkbox"/>	default-allow-rdp	Ingress	Apply to all	IP ranges:	tcp:3389	Allow	65534	default	Off	▼
<input type="checkbox"/>	default-allow-ssh	Ingress	Apply to all	IP ranges:	tcp:22	Allow	65534	default	Off	▼

So, we will create a new rule for myvpc, click Create firewall rule

Firewall policies

[+ CREATE FIREWALL POLICY](#)

[+ CREATE FIREWALL RULE](#)

i SMTP port 25 disallowed in this project. [Learn more](#)

[REFRESH](#)

[CONFIGURE LOGS](#)

[DELETE](#)

Give rule a name and select myvpc

[←](#)

Create a firewall rule

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

Name *

pubsubssh

Lowercase letters, numbers, hyphens allowed

Description

Logs

Turning on firewall logs can generate a large number of logs which can increase costs in Logging. [Learn more](#)

☐ On
 ☒ Off

Network *

myvpc

Priority *

1000

Priority can be 0 - 65535

[COMPARE](#)

Select for all instances in the network option (Also, there is an option for tags, this will apply the rule for the VM with specific tags)

Targets ?

- All instances in the network
- Specified target tags**
- Specified service account

Source filter

IPv4 ranges ▼ ?

Source IPv4 ranges * ?

Second source filter

None ▼ ?

Enter 0.0.0.0/0 for source IP and port number as 22, then click create

Source filter

IPv4 ranges ▼ ?

Source IPv4 ranges *

0.0.0.0/0 × ?

Second source filter

None ▼ ?

Destination filter

None ▼ ?

Protocols and ports ?

☐ Allow all

☒ Specified protocols and ports

☒ TCP

Ports

22

E.g. 20, 50-60

☐ UDP


Check the Firewall rules list again, now it should show the rule that we created above


<input type="checkbox"/>	default-allow-ssh	Ingress	Apply to all	IP ranges:	tcp:22	Allow	65534	default	Off	▼
<input type="checkbox"/>	pubsubssh	Ingress	Apply to all	IP ranges:	tcp:22	Allow	1000	myvpc	Off	▼


Network firewall policies

Firewall policies let you group several firewall rules so that you can update them all at

Now try connecting to pubvm, and this should connect this time


ssh.cloud.google.com/v2/ssh/projects/lokeshp1/zones/us-central1-c/instances/vmpub1?authuser=0&hl=en


ssh.cloud.google.com/v2/ssh/projects/lokeshp1/zones/us-central1-c/instances/vmpub1?authuser=0&hl=en


SSH-in-browser
UPLOA

```

lokeshdrall1111@vmpub1:~$ hostname
vmpub1
lokeshdrall1111@vmpub1:~$

```

Now try connecting to prvvm (VM which we created in private subnet) and you will see that both the VM can connect via SSH.