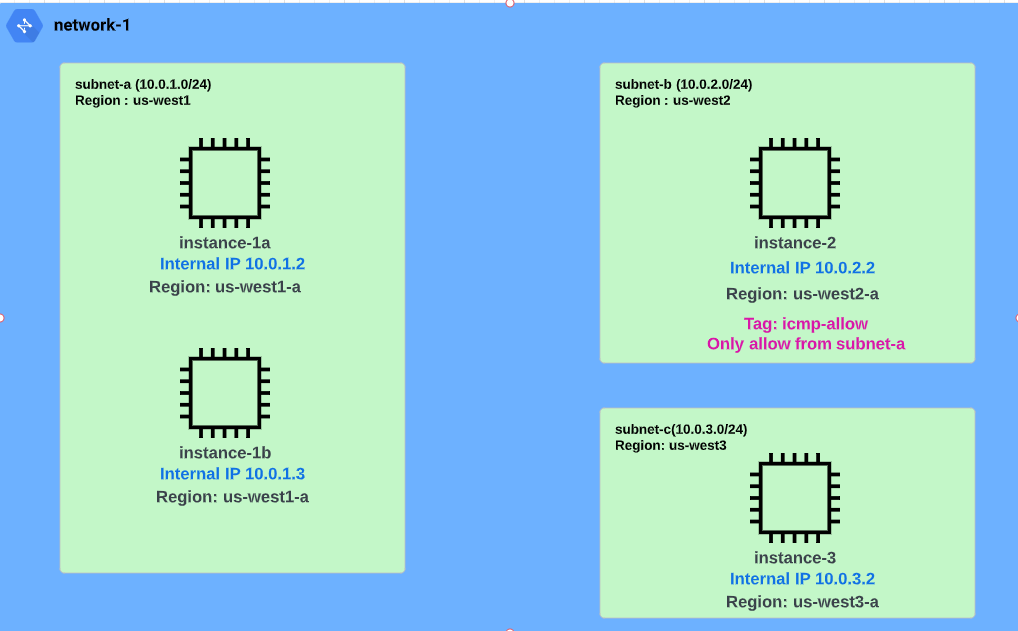
**Network security Lab-2**

**Lab: Creating Firewall Rules On Google Cloud VPC Network**

**Before doing this Lab, you have to create the following environment on the GCP.**



**\*\***

**There is a document to create VPC “network-1 with subnet-a, subnet-b and subnet-c”**

**There is a document to create “instance-1a connected to network-1(subnet-a)”**

**There is a document to create “instance-1b connected to network-1(subnet-a)”**

**There is a document to create “instance-2 connected to network-1(subnet-b)”**

**There is a document to create “instance-3 connected to network-1(subnet-c)”**

**There is a one more document to create “firewall rule for network-1” which allow port 22 tcp ( Helps you to access SSH)**

**\*\***

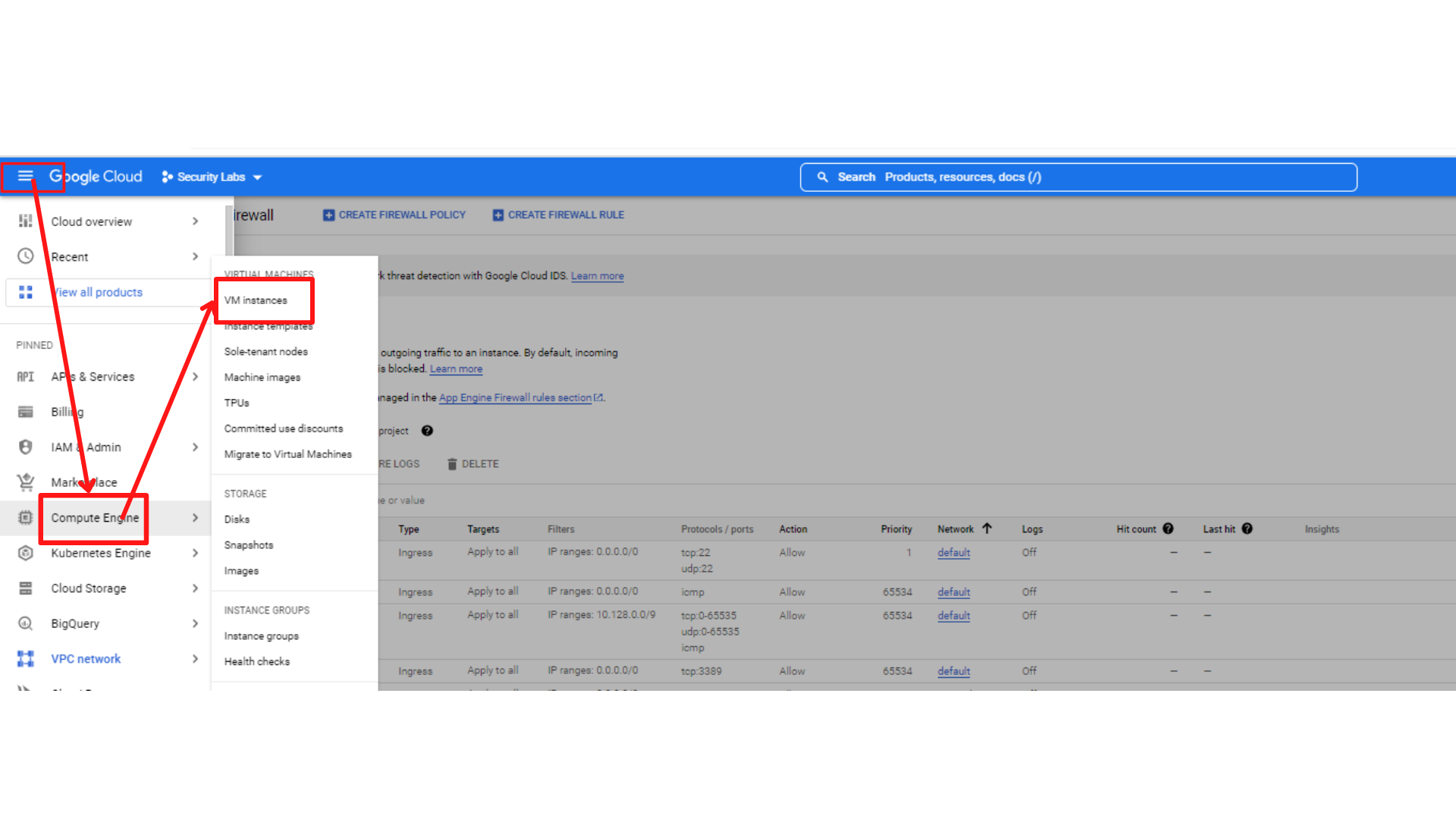
**Note: It is important to create the specific environment, if not it leads to confusion.**

**Problem:**  Your organization wants you to help them allow google cloud traffic from a particular subnet and none other. How will you do it?

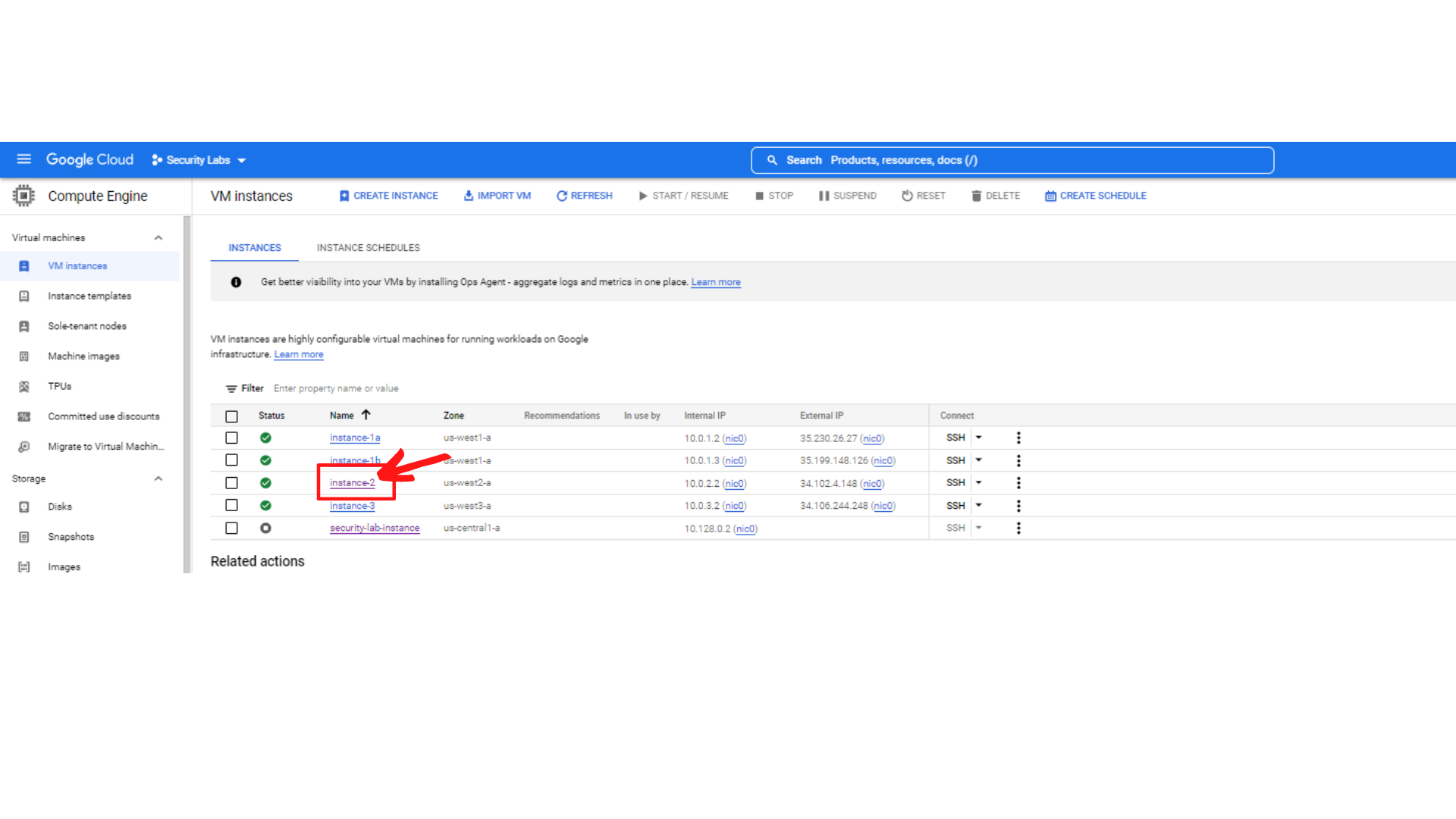
**Solution:** You can configure firewall rules accordingly. Such an option is given by GCP to its users.

***Step1:*** **Apply Network Tag to “instance-2”**

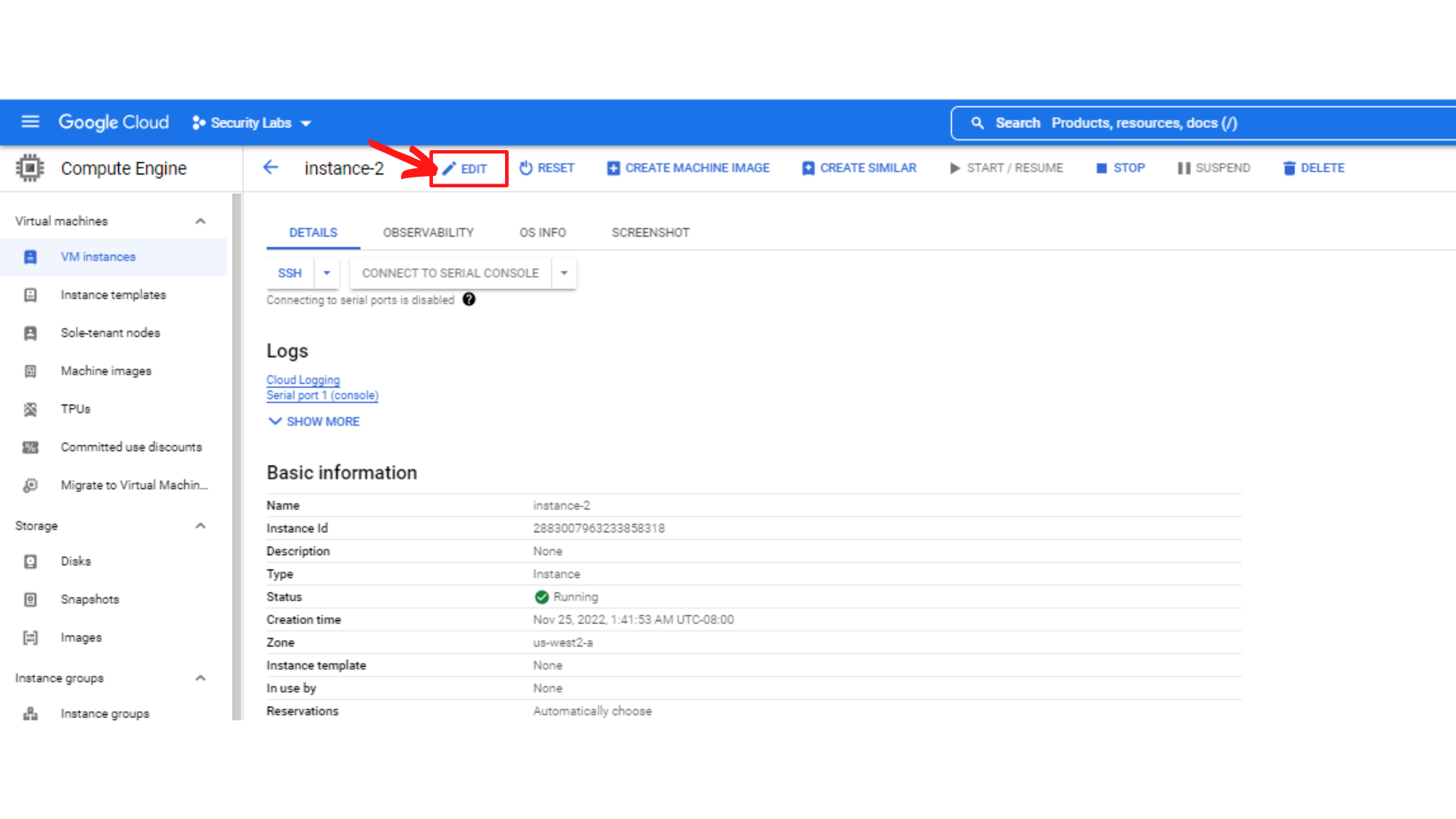
1. Click on ***“Navigation Menu”*** then ***“click → Compute Engine → VM instances”***



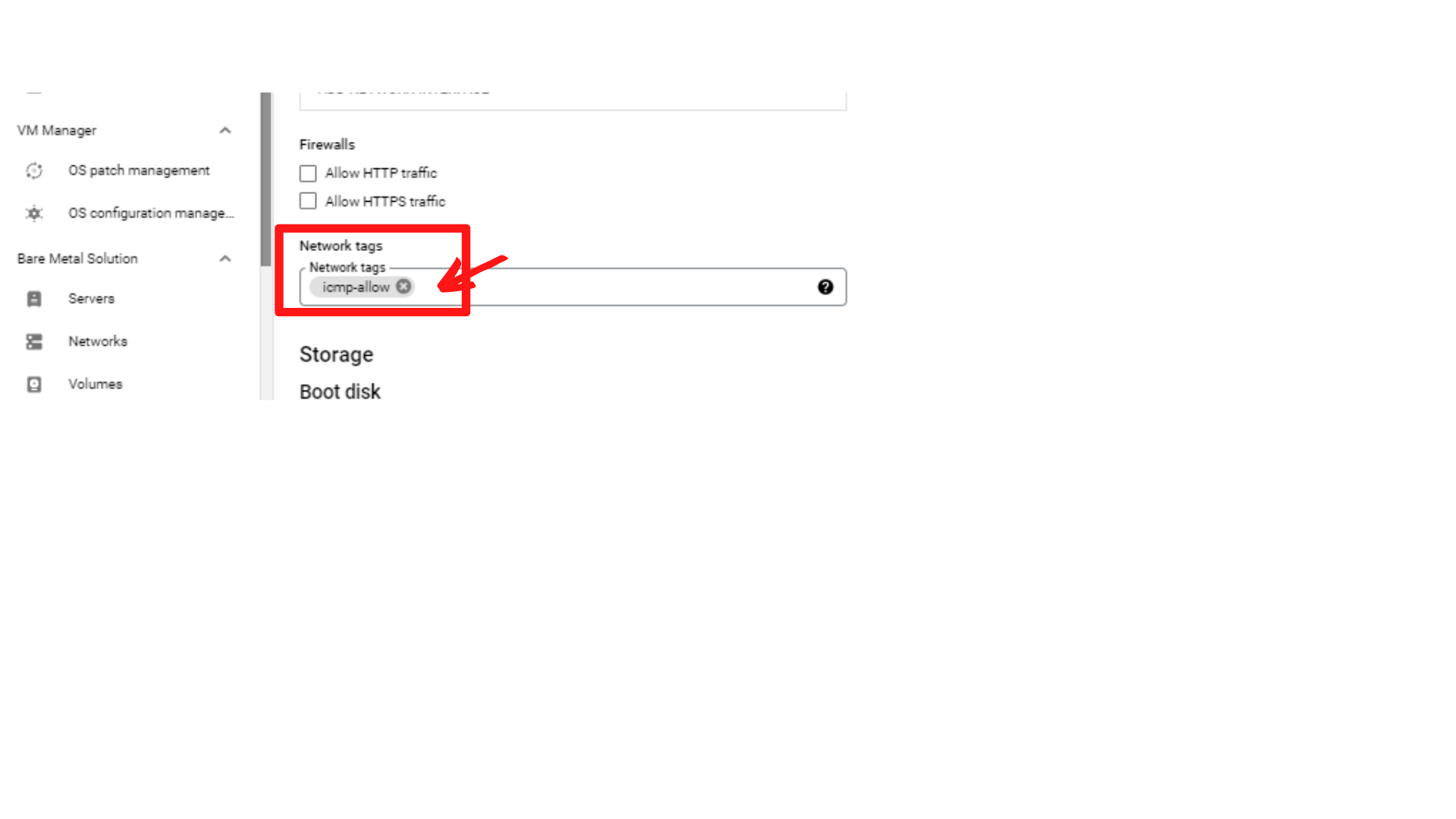
1. Your screen should look similar to this with an instances list. Then ***“Click → instance-2”***

****

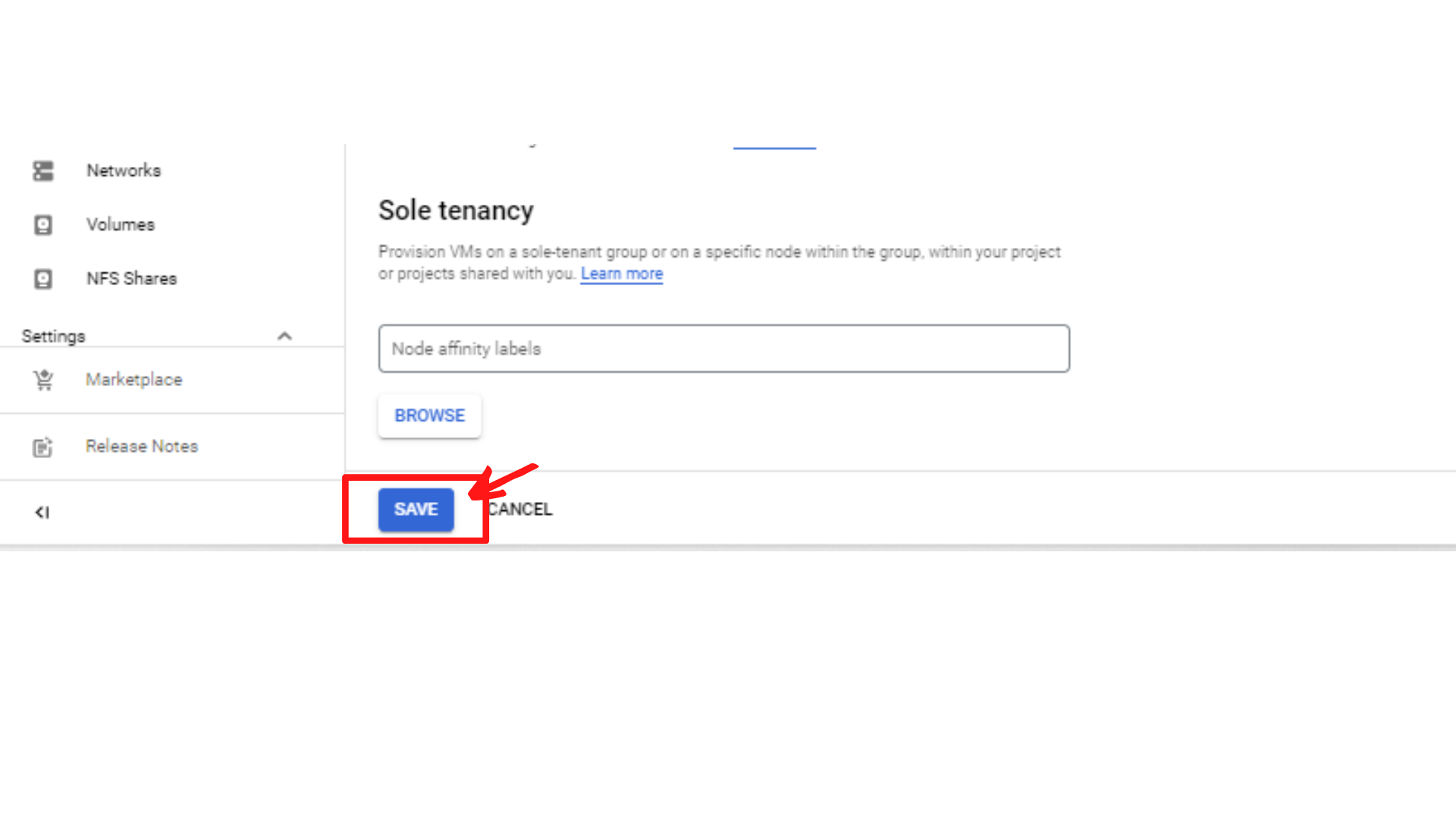
1. Your screen should look similar to this with instance-2 details. ***“Click →EDIT”*** (which is on TOP middle of the screen)



1. Now scroll down until you see the **“network tags”** field. Enter **icmp-allow** and press Enter.



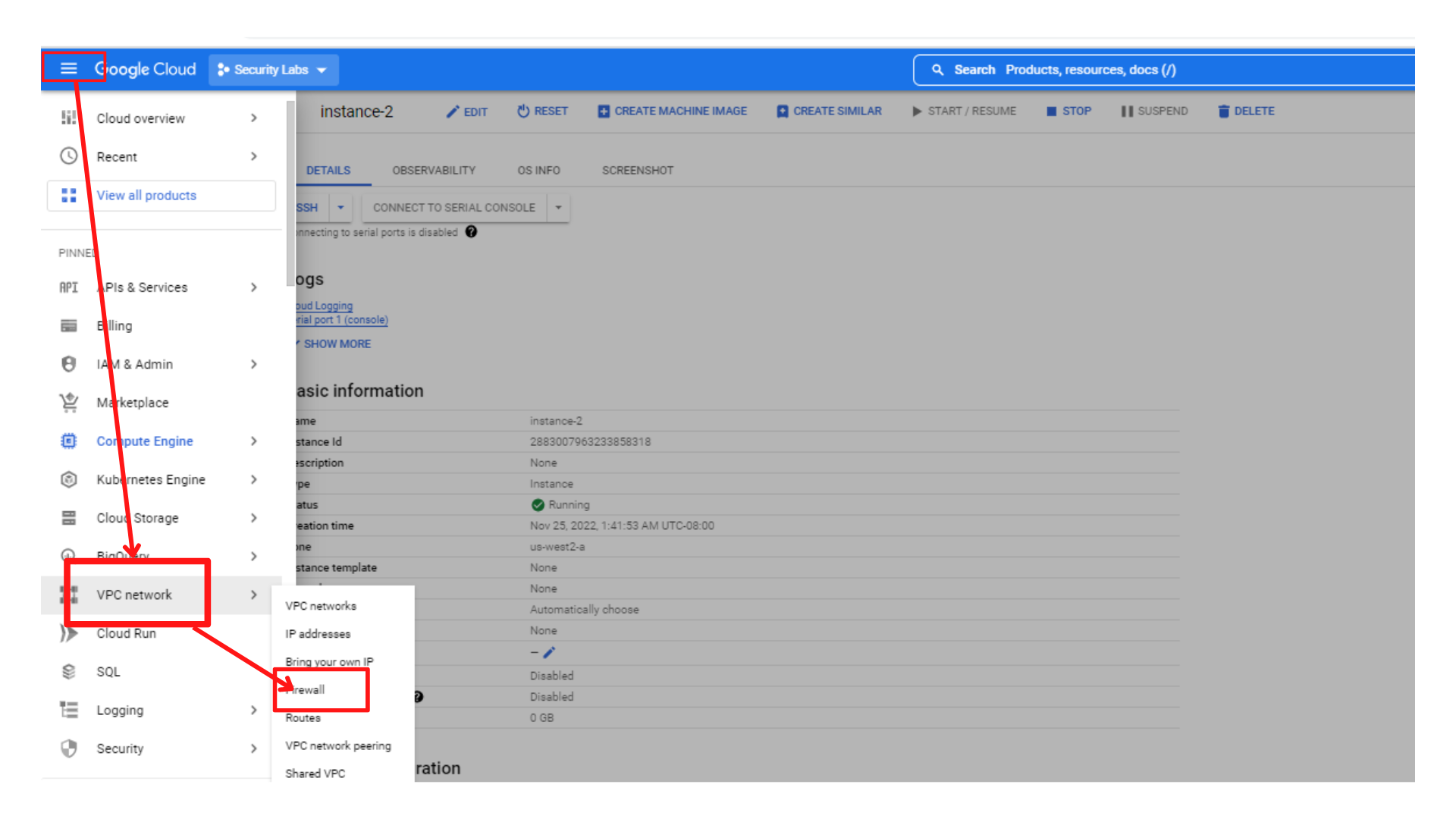
1. Now Scroll down, and ***“Click → Save”***



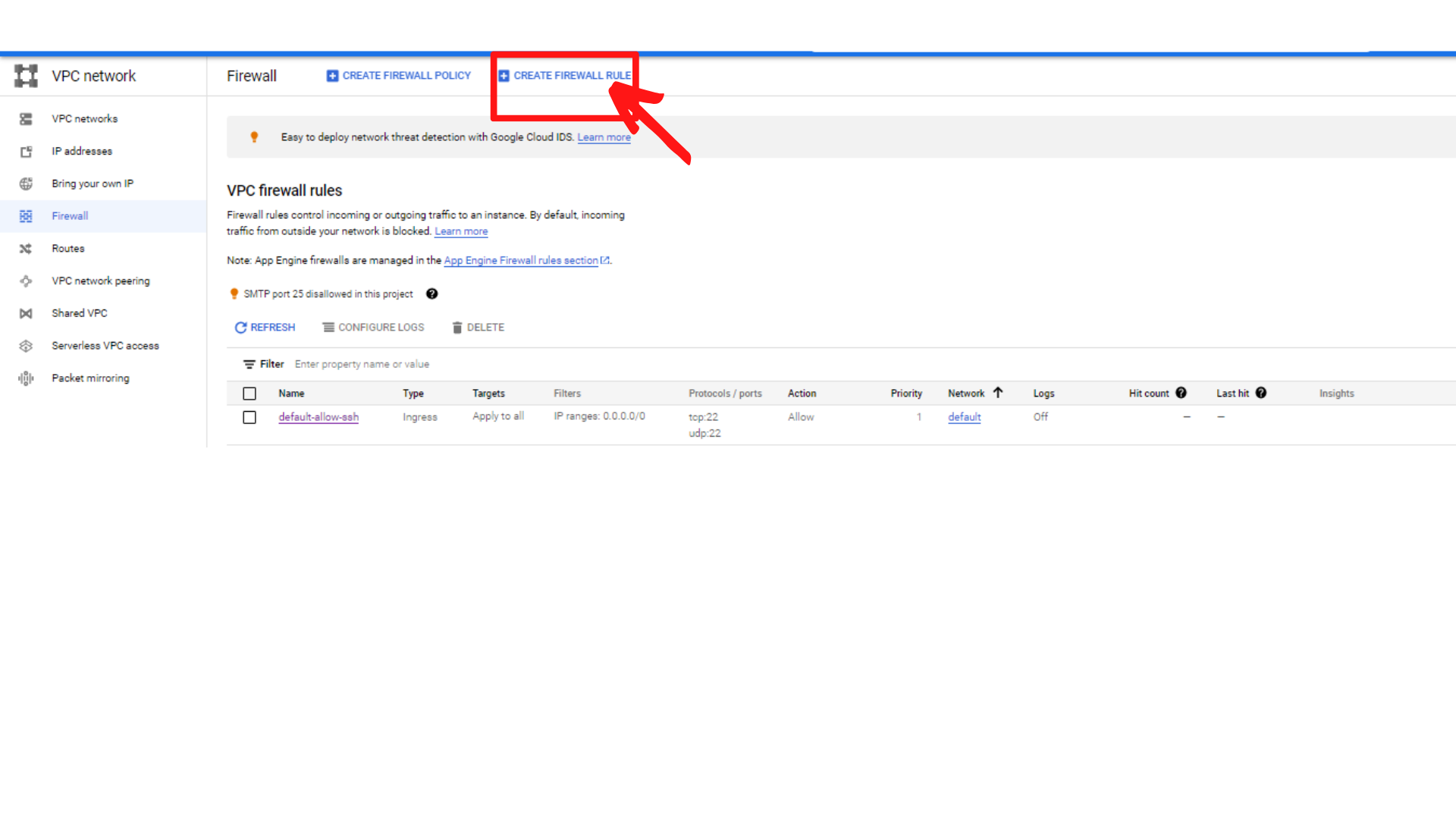
1. That’s it, you have added network tag “icmp-allow” to instance-2.

**Step2:** **Create a Narrow-Scope Firewall Rule for instance-2.**

1. Click on ***“Navigation Menu”*** then ***“click → VPC Network → Firewall”***

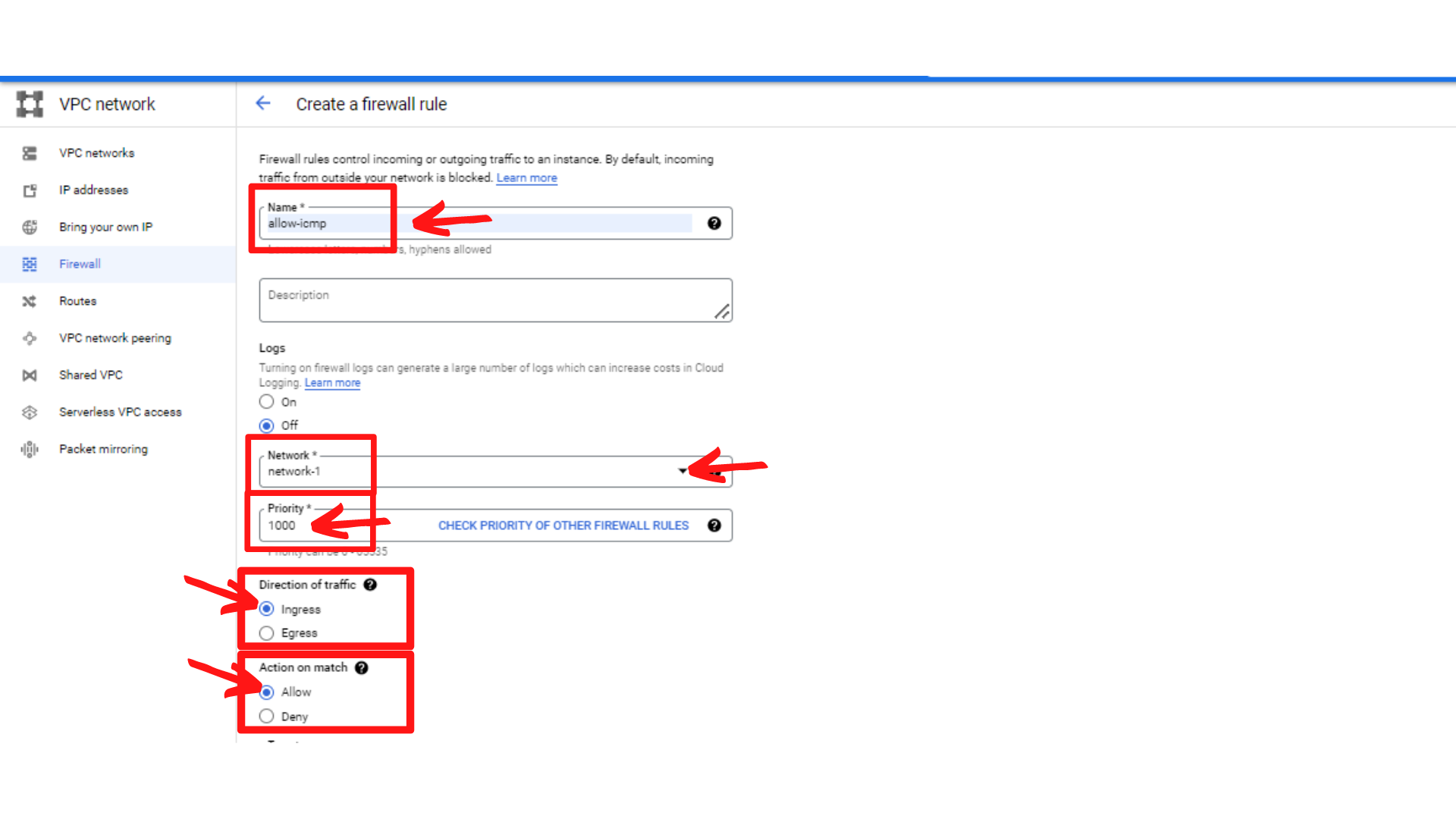


1. Your screen should look similar to this with the firewall rules list. ***“Click → Create Firewall Rule”***



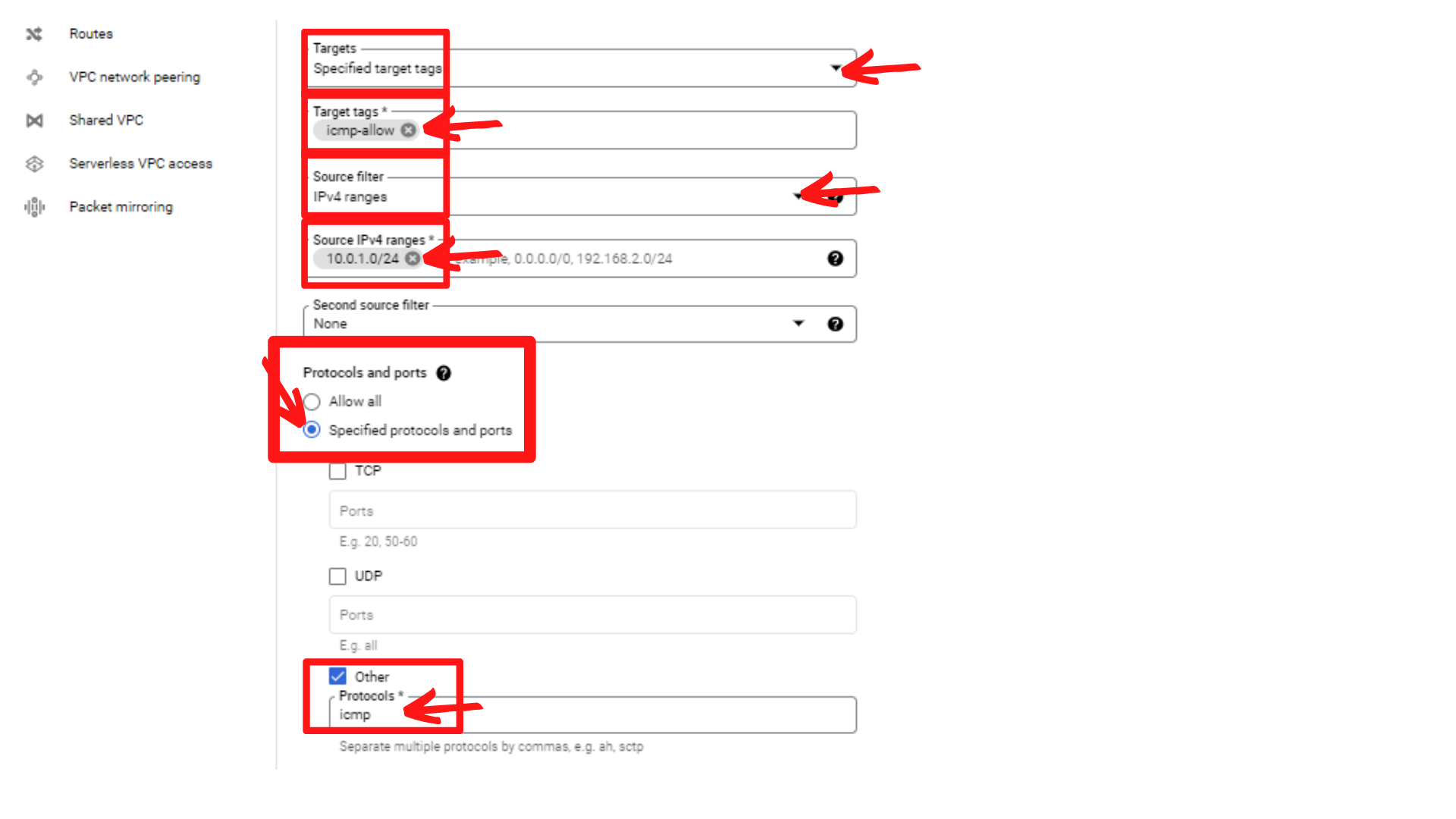
1. Now you will see **Create a firewall rule Form**. Enter the following information.

* **Name : allow-icmp**
* **Network :** select **“network-1”** since we are creating rule for network-1
* **Priority: 1000**
* **Direction of traffic :** **Ingress (since we are creating traffic for incoming traffic)**
* **Action on match : Allow**

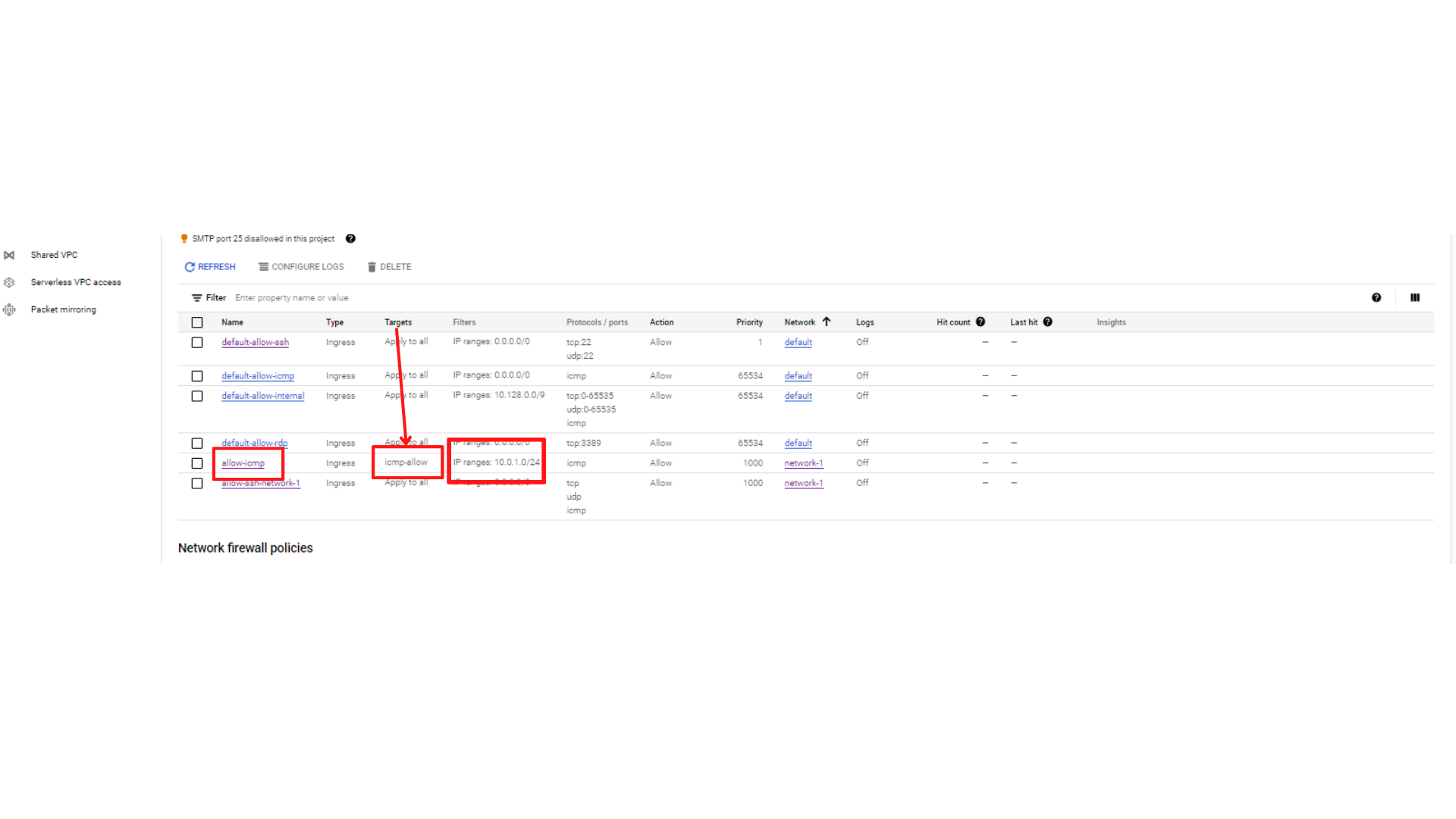
****

1. Now scroll down and enter the following information.

* **Targets : select “Specified target tags”**
* **Target Tags :** Enter **icmp-allow** since we are targeting this tag (instance-2)
* **Source filter : IPv4 ranges**
* **Source IPv4 Ranges : IP range of subnet-a i.e (10.0.1.0/24)**
* **Protocols and ports : select Specified protocols and ports → tick “other” and enter icmp in the field**



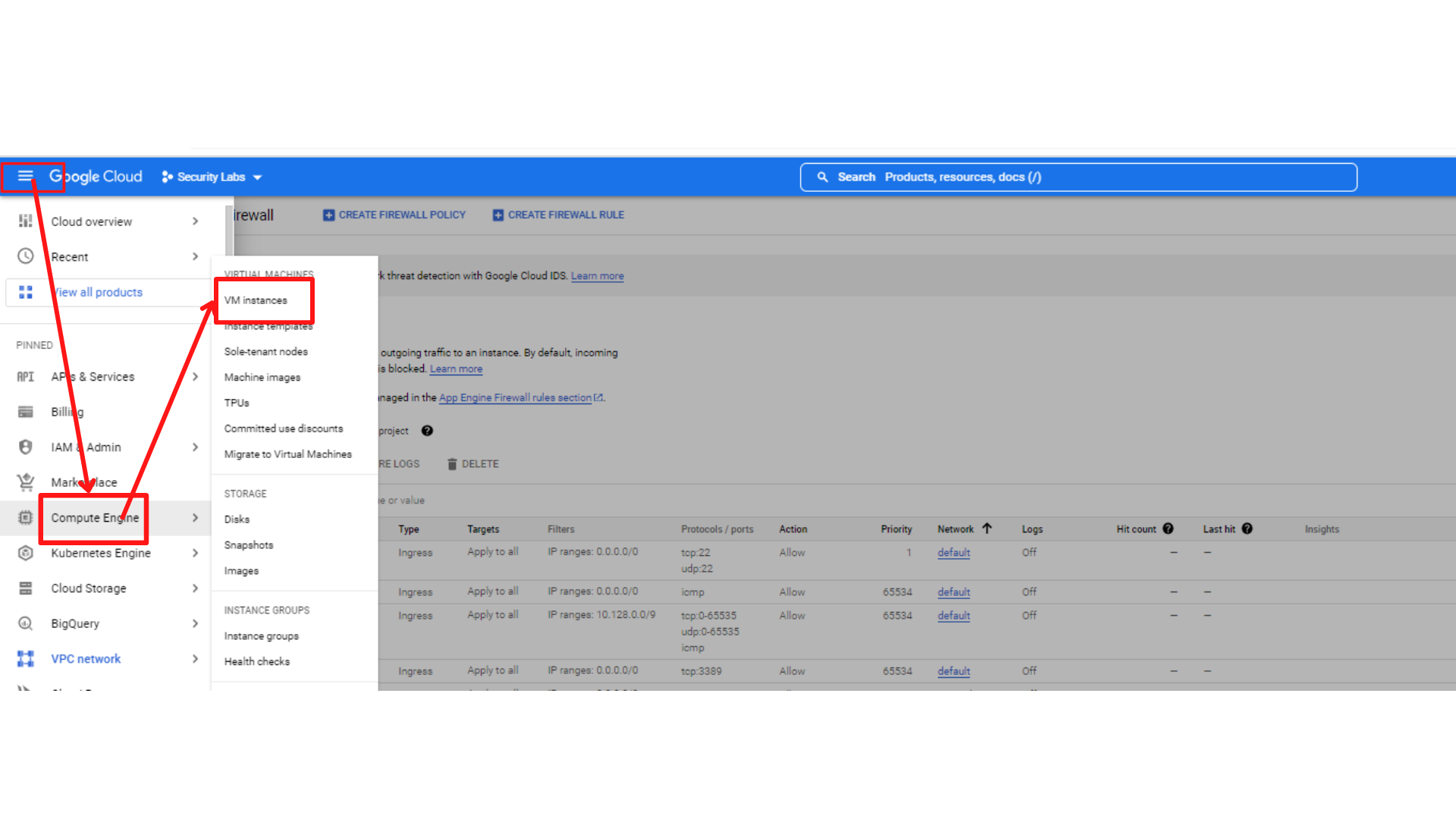
1. Now **“click → Create”**
2. Now your screen should look similar to this with the firewall rule added.



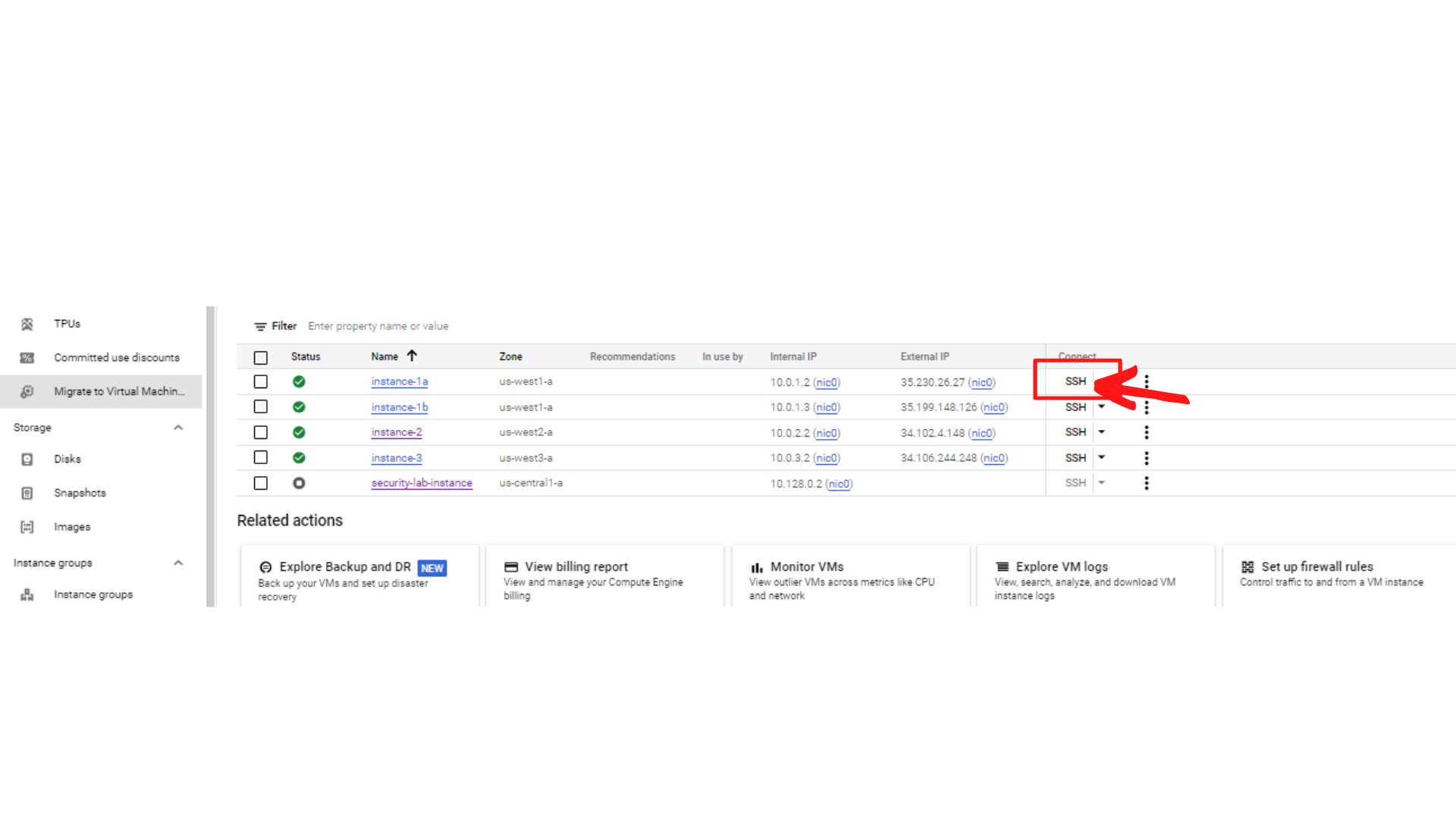
**That’s it, you have created a firewall rule to access instance-2 from subnet-a**

**Step3: Check success if firewall rule is working.**

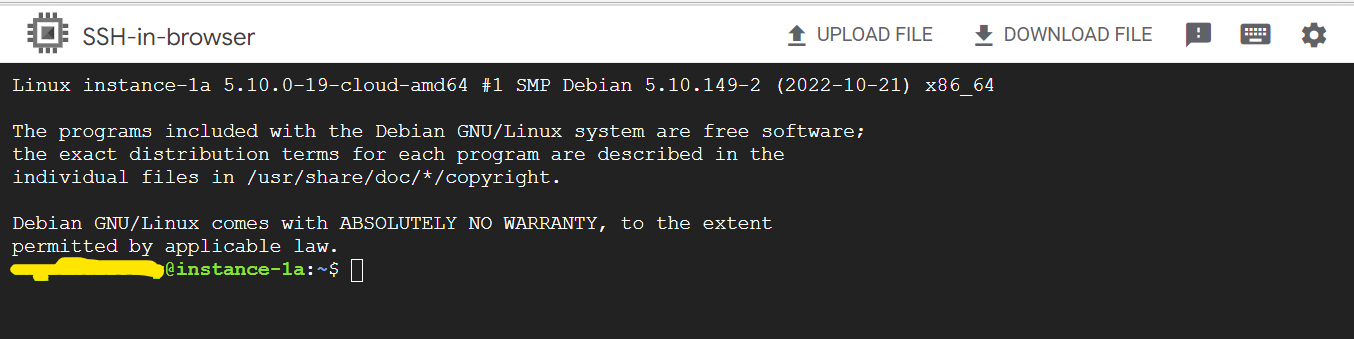
1. Click on ***“Navigation Menu”*** then ***“click → Compute Engine → VM instances”***



1. Your screen should look similar to this with an instances list. ***“Click on instance-1a → SSH”*** this will open a new browser window with SSH-in-browser.

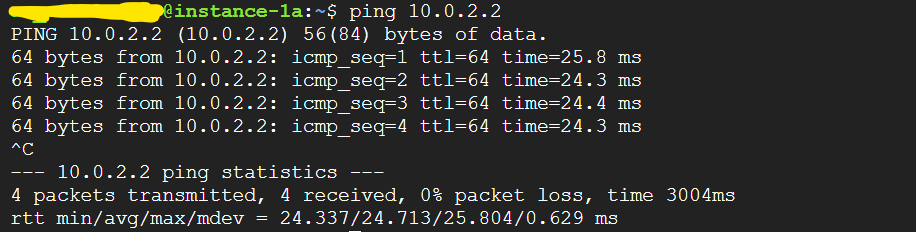


1. Your screen should look similar to this.



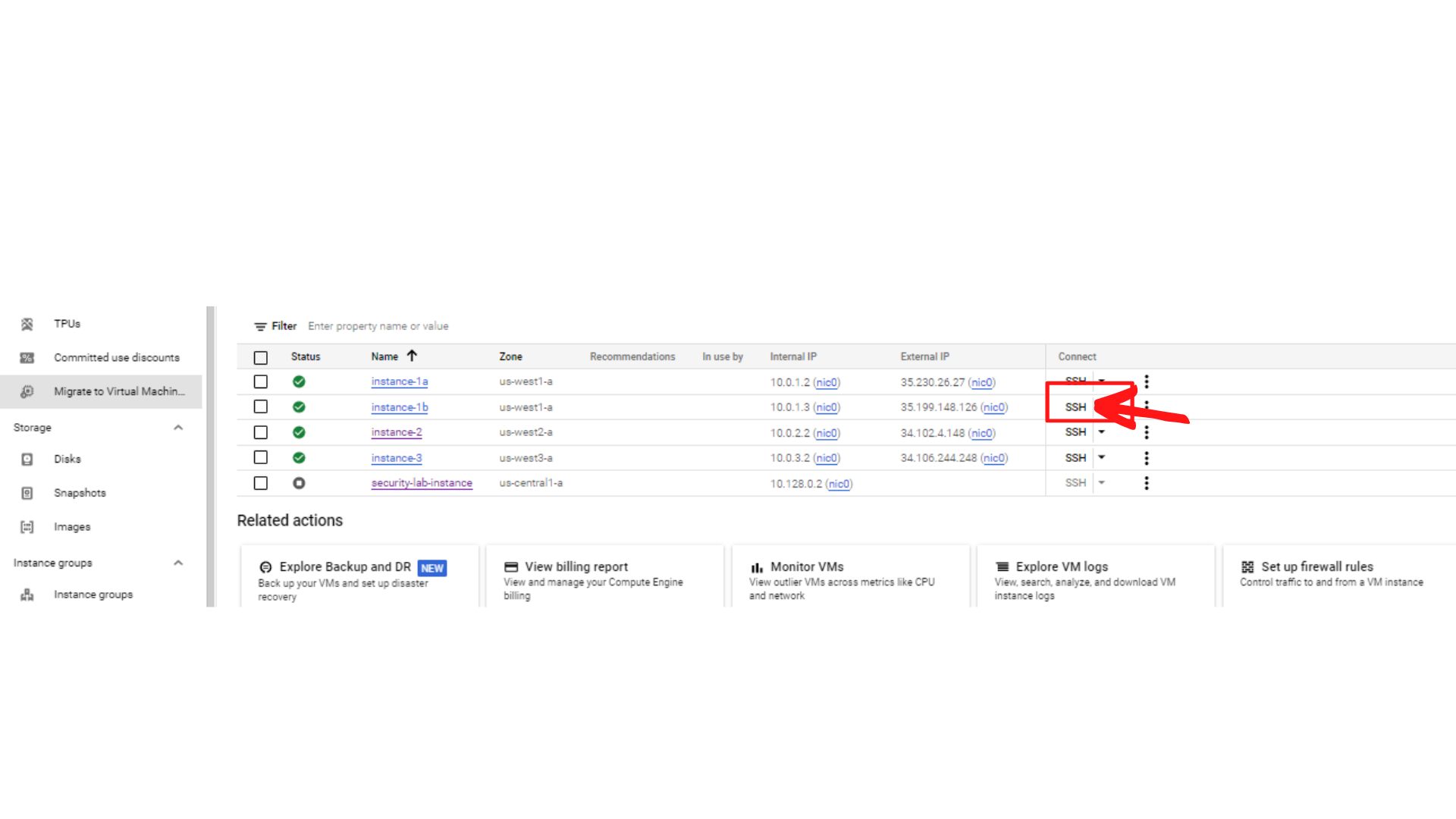
1. Now attempt to ping instance-2 internal IP address using the following command. **“ping <ip address>”**

ping 10.0.2.2

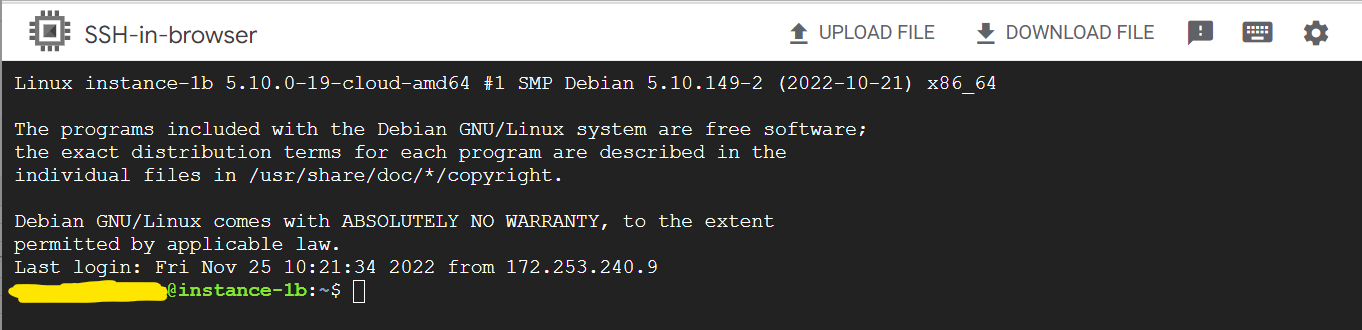


**You received a response from instance-2, that means you are able to access instance-2 from subnet-a since we have allowed subnet-a for target tags “icmp-allow”**

1. Now check from instance-1b. ***“Click on instance-1b → SSH”*** this will open a new browser window with SSH-in-browser.

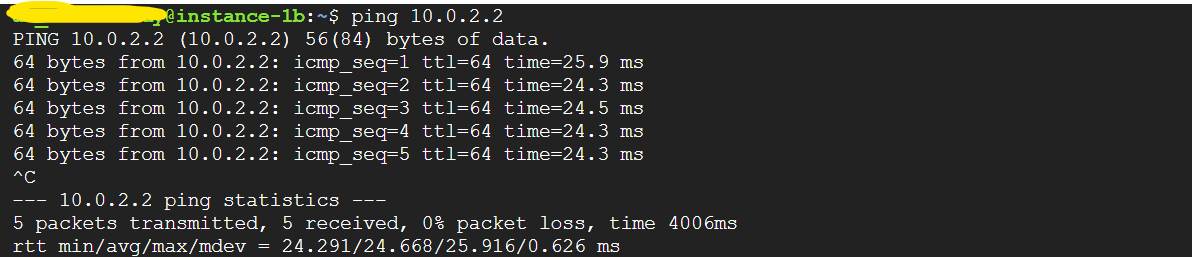


1. Your screen should look similar to this.



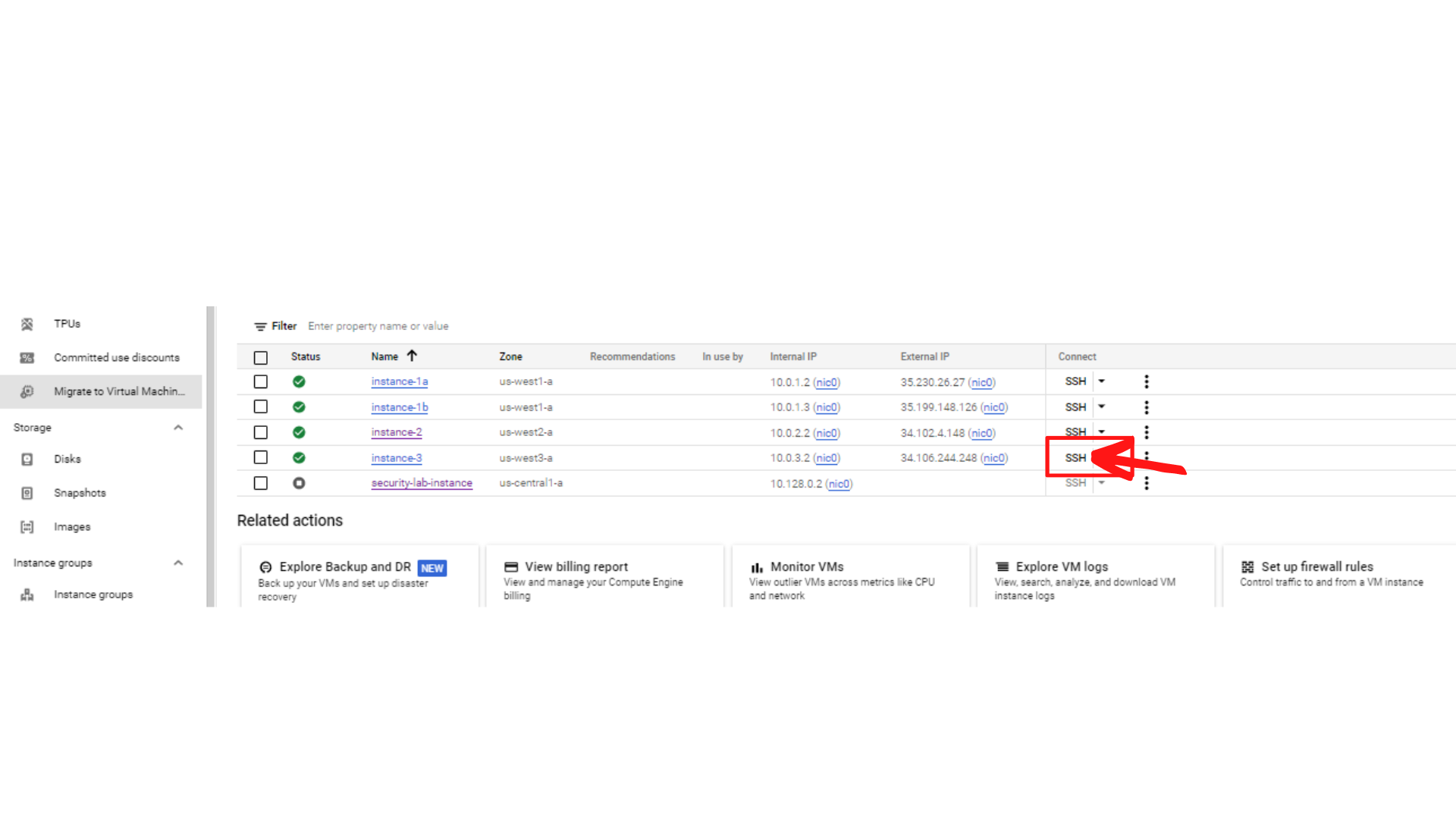
1. Now attempt to ping instance-2 internal IP address using the following command. **“ping <ip address>”**

ping 10.0.2.2

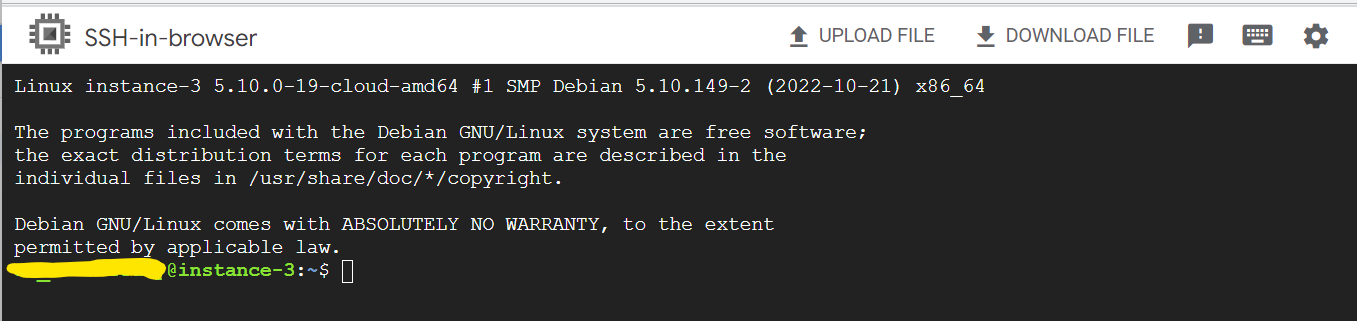


**You received a response from instance-2, that means you are able to access instance-2 from subnet-a since we have allowed subnet-a for target tags “icmp-allow”**

1. Now check from instance-3. ***“Click on instance-3 → SSH”*** this will open a new browser window with SSH-in-browser.

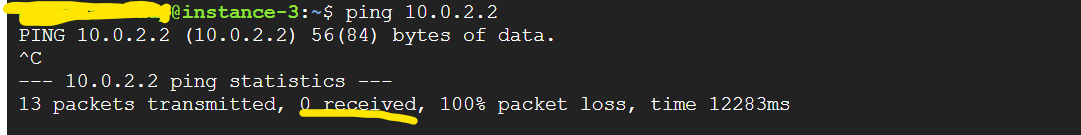


1. Your screen should look similar to this.



1. Now attempt to ping instance-2 internal IP address using the following command. **“ping <ip address>”**

ping 10.0.2.2



**You have not received response from instance-2, that means you are not able to access instance-2 from subnet-c since we have not allowed subnet-c for target tags “icmp-allow”**