Firewall Rule For network-2

In order to connect to SSH, you need to add following firewall rule to the network-2

1. Once you first log in, your screen should look similar to this.



1. Click on the project selector drop-down menu at the top of the screen.



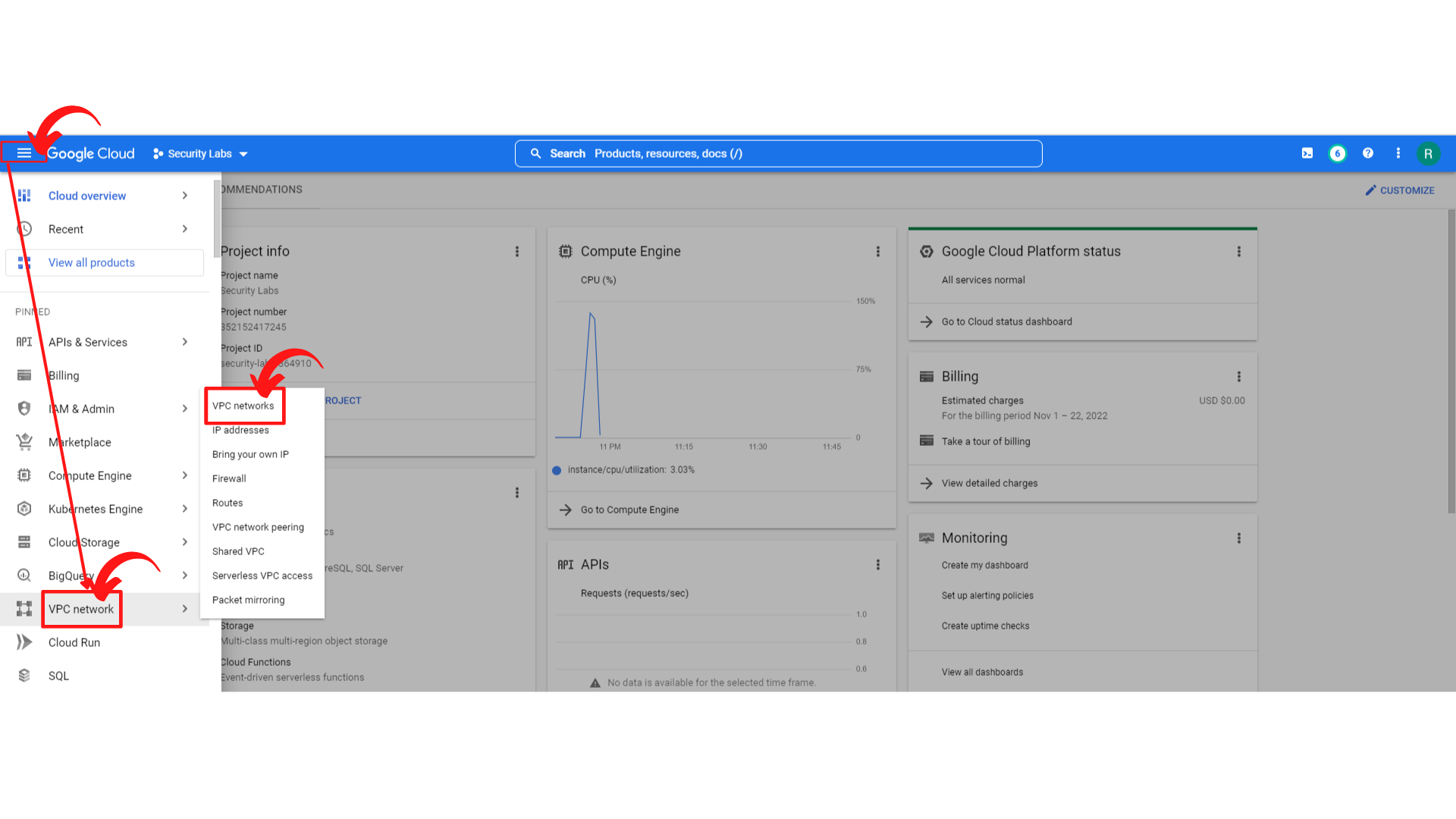
1. Since, we are doing labs on a Security Labs project, Click on *“Security Labs”*.



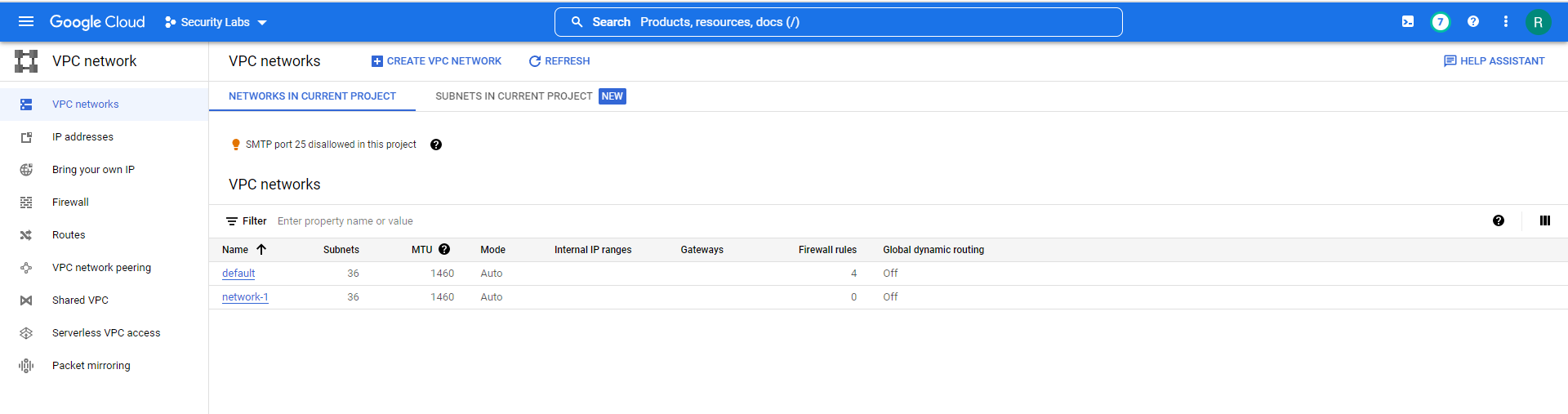
1. Your screen should look similar to this with project info changed to “*Security Labs”* project.



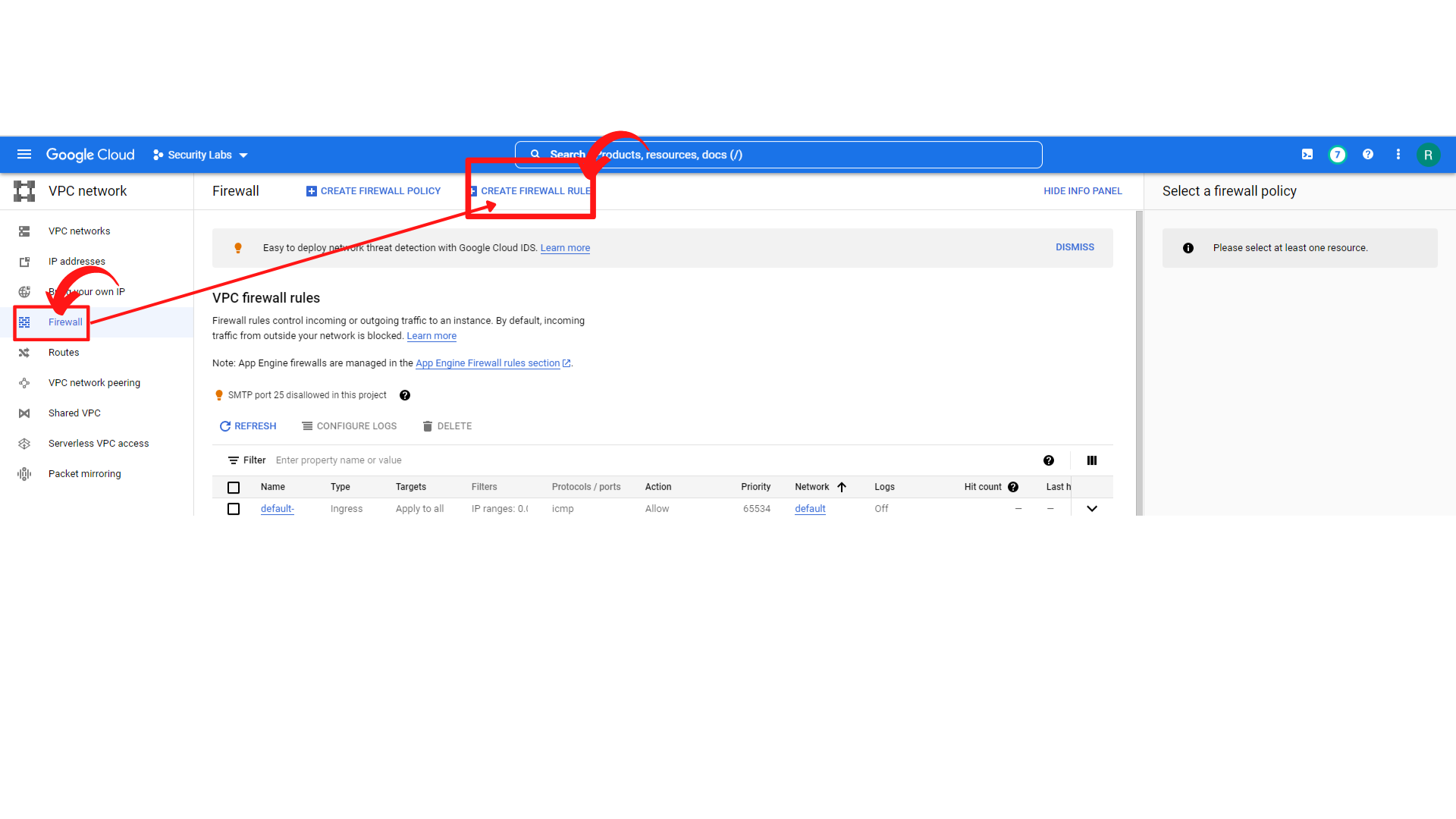
1. To create a new VPC Network, Click on *“Navigation menu”* on top left, then click on ***“VPC Network → VPC Networks”***



1. Your screen should look similar to this with the VPC networks list.

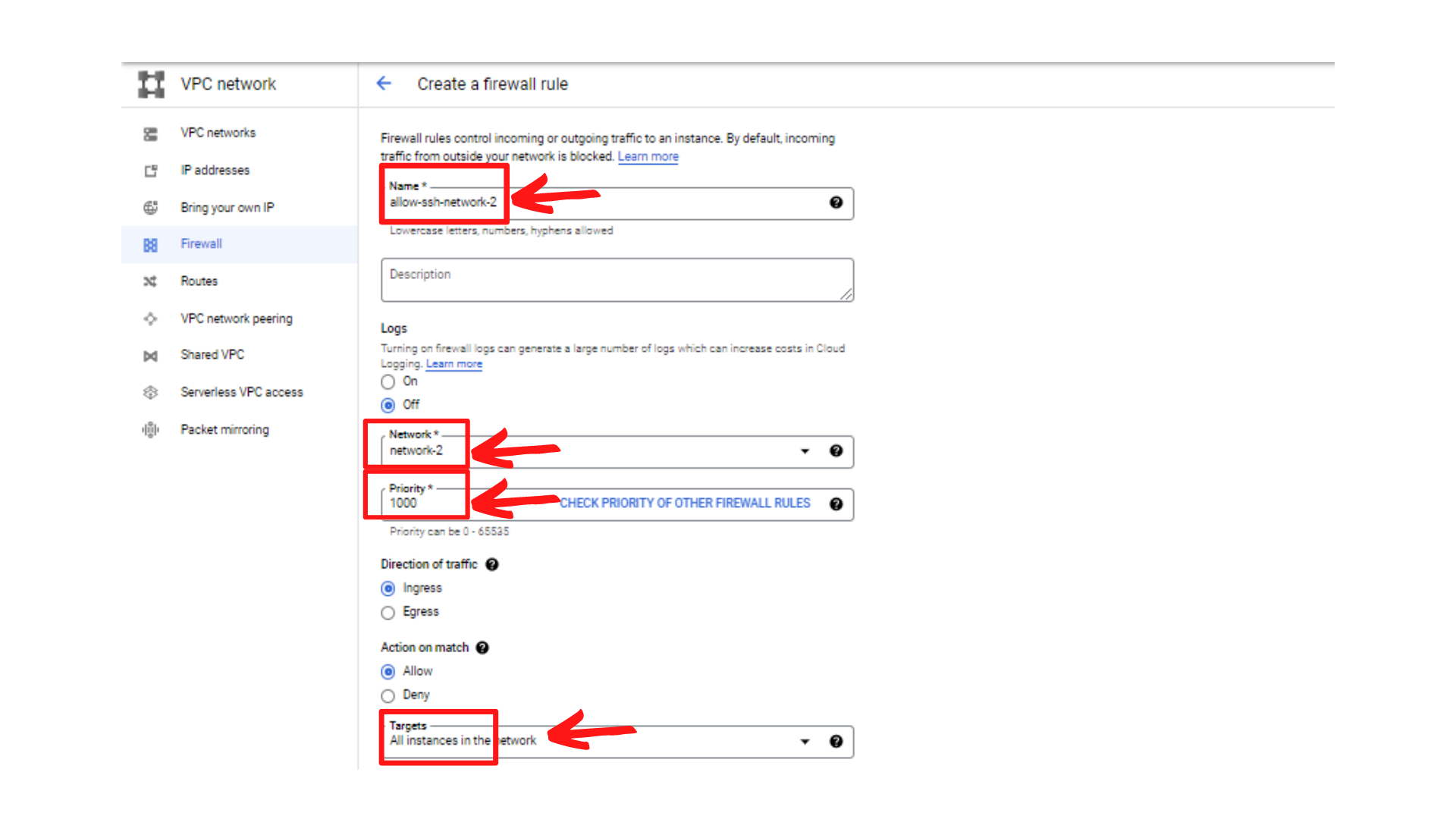


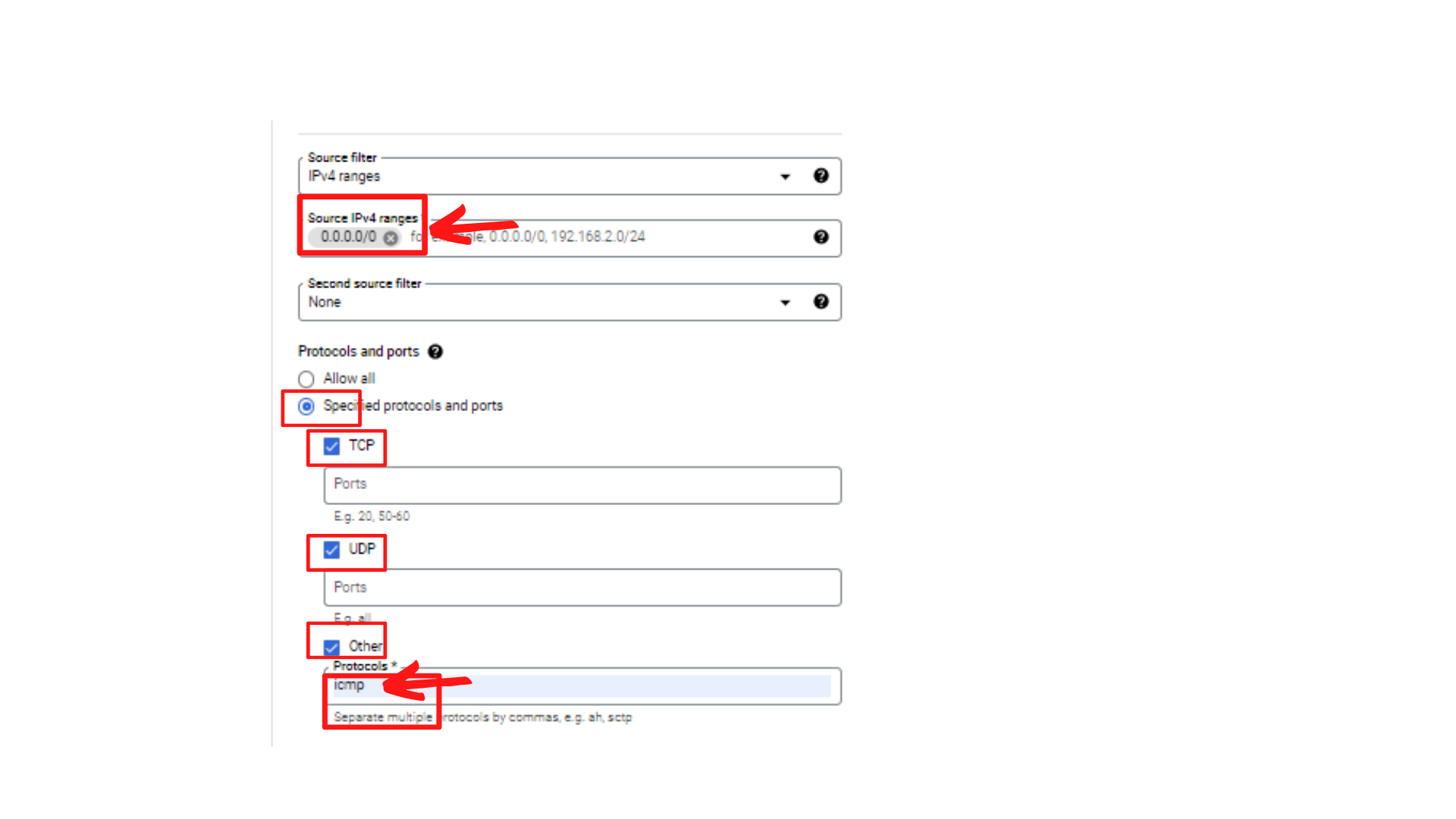
1. Now click on the **“Firewall → Create Firewall Rule.**”



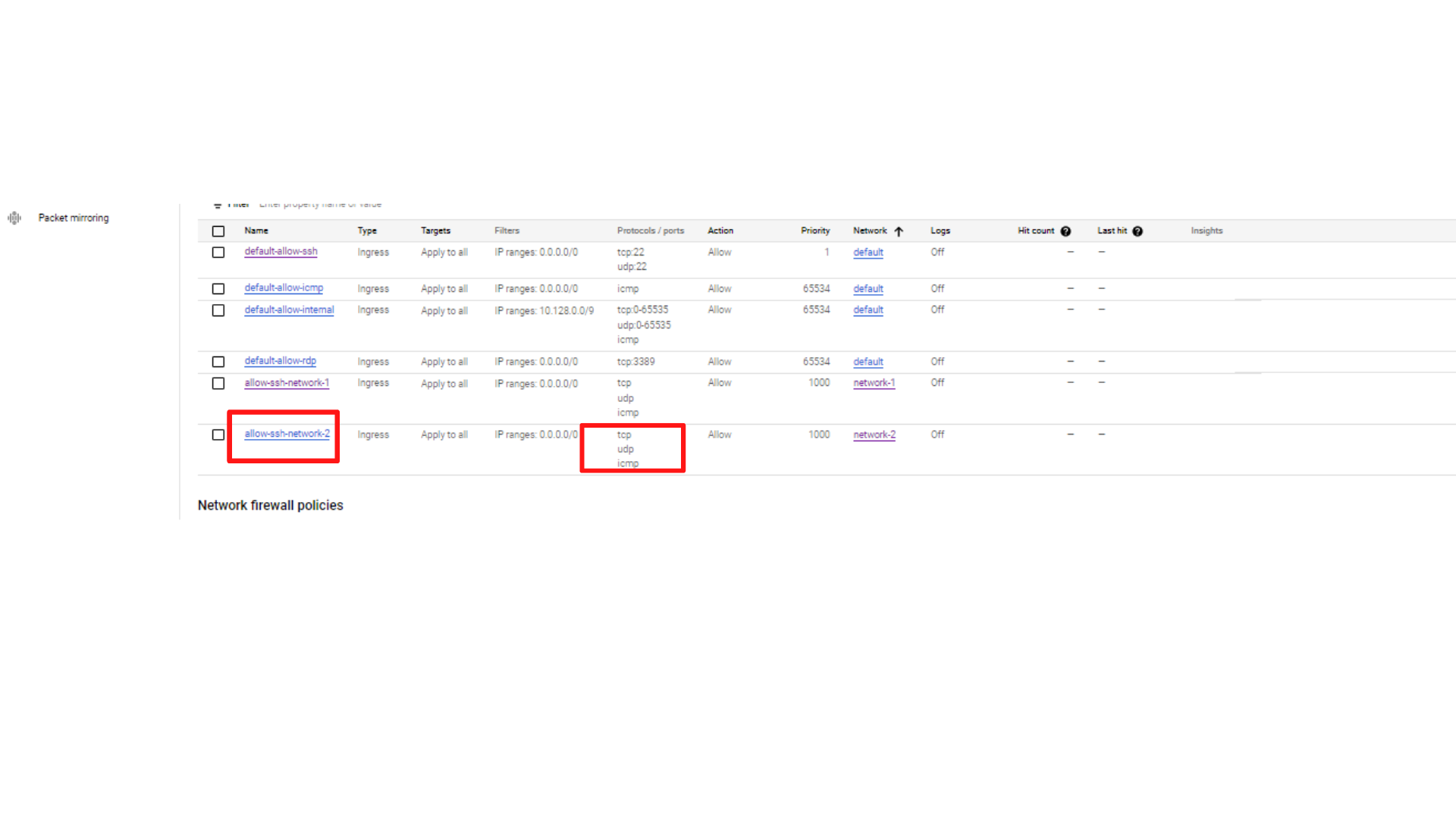
1. Now you will see the Create a firewall rule form. Enter the following information.

* **Name : allow-ssh-network-2**
* **Network :** select **“network-2”** since we are creating rule for network-2
* **Priority: 1000**
* **Direction of traffic :** **Ingress**
* **Action on match : Allow**
* **Targets:** **All instances in the network**
* **Source IP ranges:** ***0.0.0.0/0***
* **Protocols and ports: Select tcp and udp.**
* **Other protocols: Enter “icmp”**

****



1. After the filling the Firewall rules, then **“click → create”**
2. Now your screen should look similar to this with a new rule added to the list.



1. That’s it, you have successfully created a firewall rule to network-2 that allows you to connect to SSH for instance-2.

