Adding Firewall Rules To The VPC Network

Firewall Rules on Google Cloud Platform (GCP) allow or disallow communication to and from Virtual Machine (VM) instances based on a configuration you define. You select a Virtual Private Cloud (VPC) network and a collection of components that define what the rule does when you create a firewall rule.

**Two Implied Firewall Rules:**

* **Allow Egress Rule:** with its action of “allow”, allows all traffic out to the 0.0.0.0/0 destination, which basically means everywhere. The priority of the implied allow egress rule is the lowest possible, 65535.
* **Deny Ingress Rule:** with an action of “deny”, blocks all incoming connections. Like the egress rule, the priority of the ingress rule is 65535. However, instead of having a destination defined as 0.0.0.0/0, it is the source that is defined as 0.0.0.0/0.

While these implied rules cannot be removed, they can be overridden with custom rules that you create.

\*\* By default, all protocols and ports are allowed in GCP, but if firewall rules block egress, the specific destination protocol and port must be allowed.\*\*

***In this Lab Step you will create Firewall Rule. This rule will allow the HTTP traffic on port 80 and the DNS traffic on port 53. The rules have a priority that determines the order firewall rules are applied in. The highest priority rule, which corresponds to the rule with the lowest priority number, is processed first. If the rule matches the traffic, then lower priority rules are ignored. Otherwise, the next highest priority rule is checked against. Default rules with the lowest possible priority will allow outbound traffic (egress) and deny inbound traffic (ingress) if no higher priority rules match the traffic.***

* **Create a Rule to allow HTTP traffic on port 80 and the DNS on port 53.**

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.



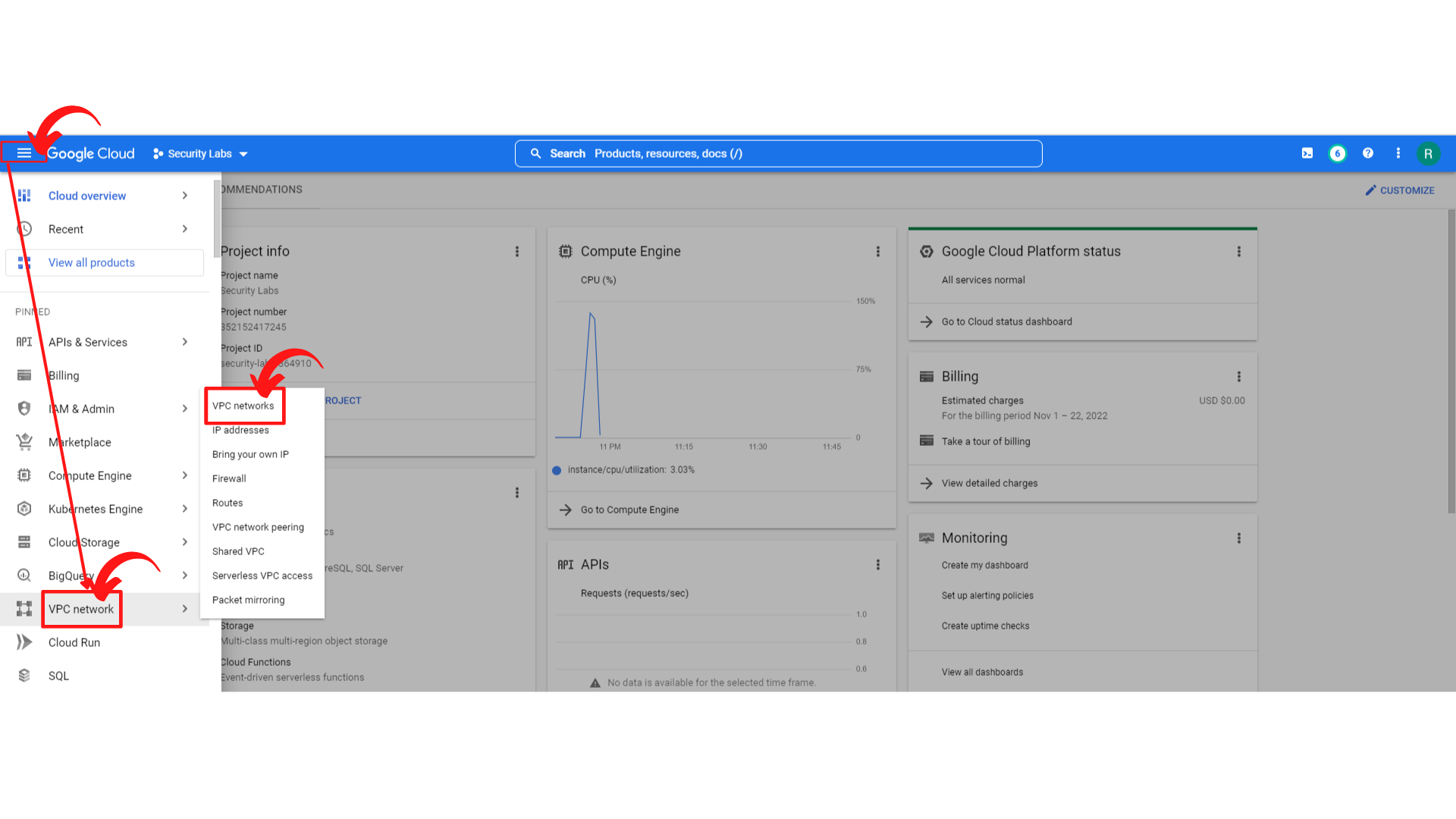
1. Since, we are doing labs on a Security Labs project, Click on *“Security Labs”*.



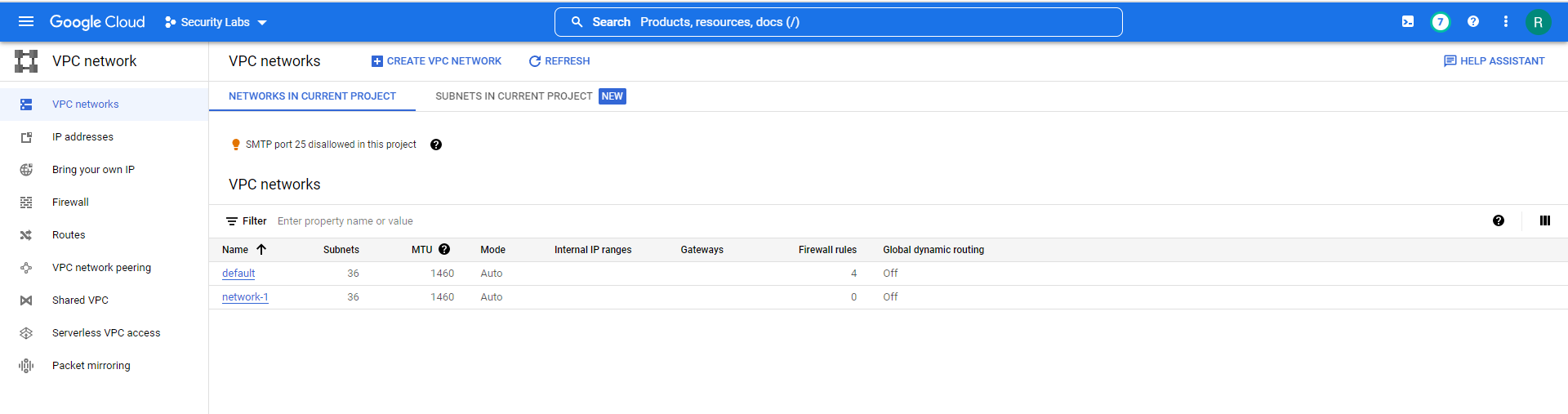
1. Your screen should look similar to this with project info changed to “*Security Labs”* project.



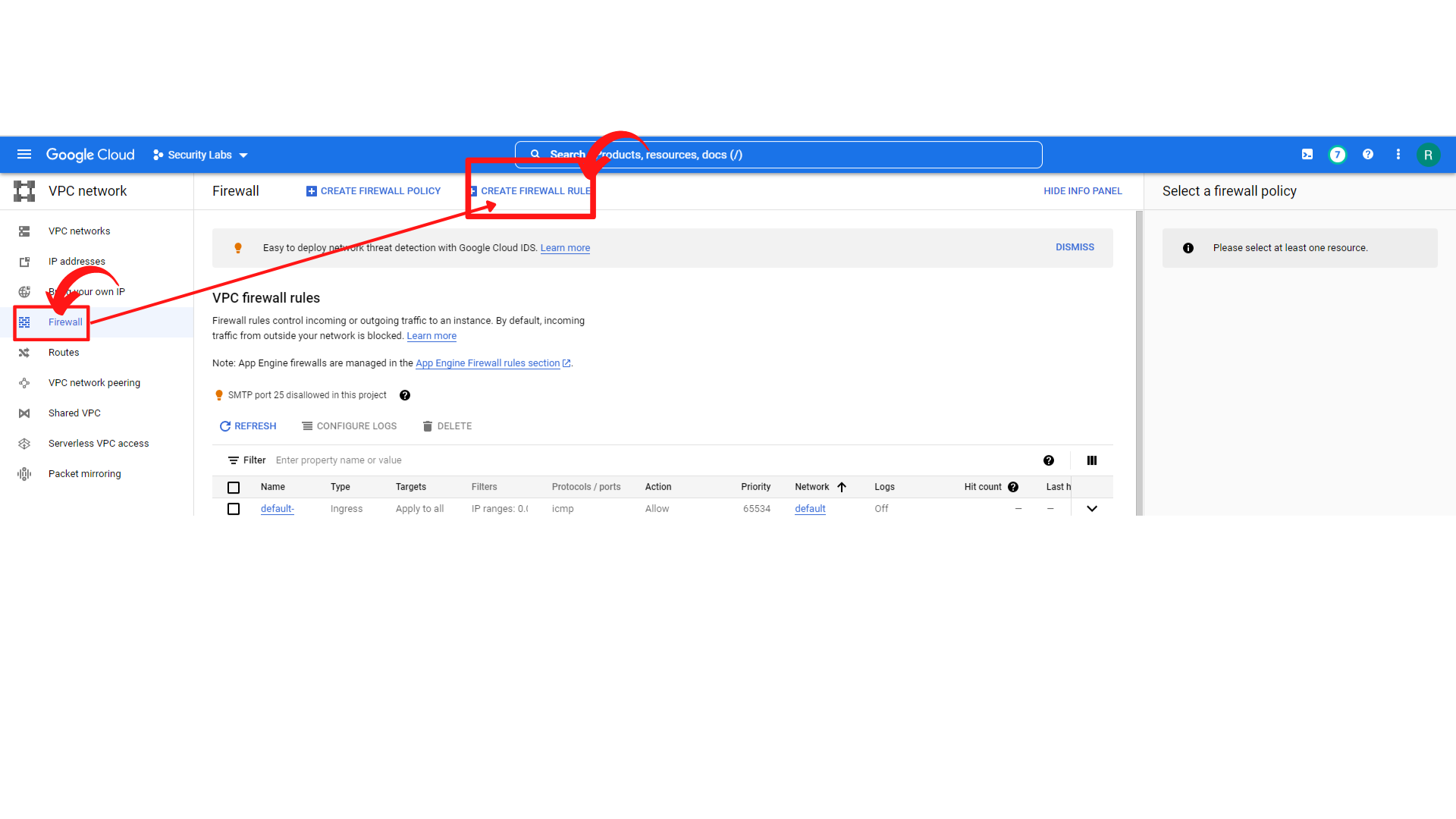
1. To create a new VPC Network, Click on *“Navigation menu”* on top left, then click on ***“VPC Network → VPC Networks”***



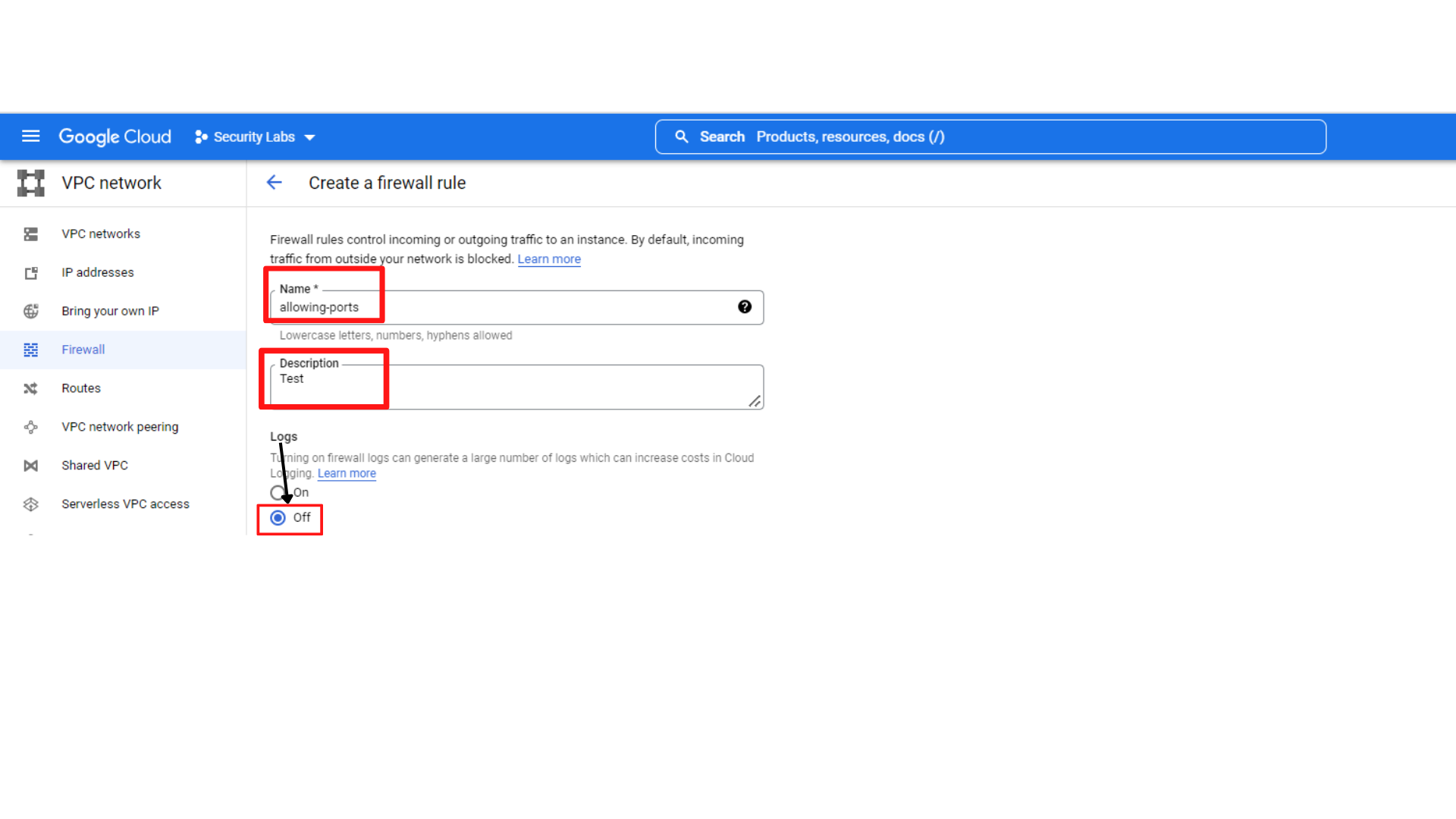
1. Your screen should look similar to this with the VPC networks list.



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

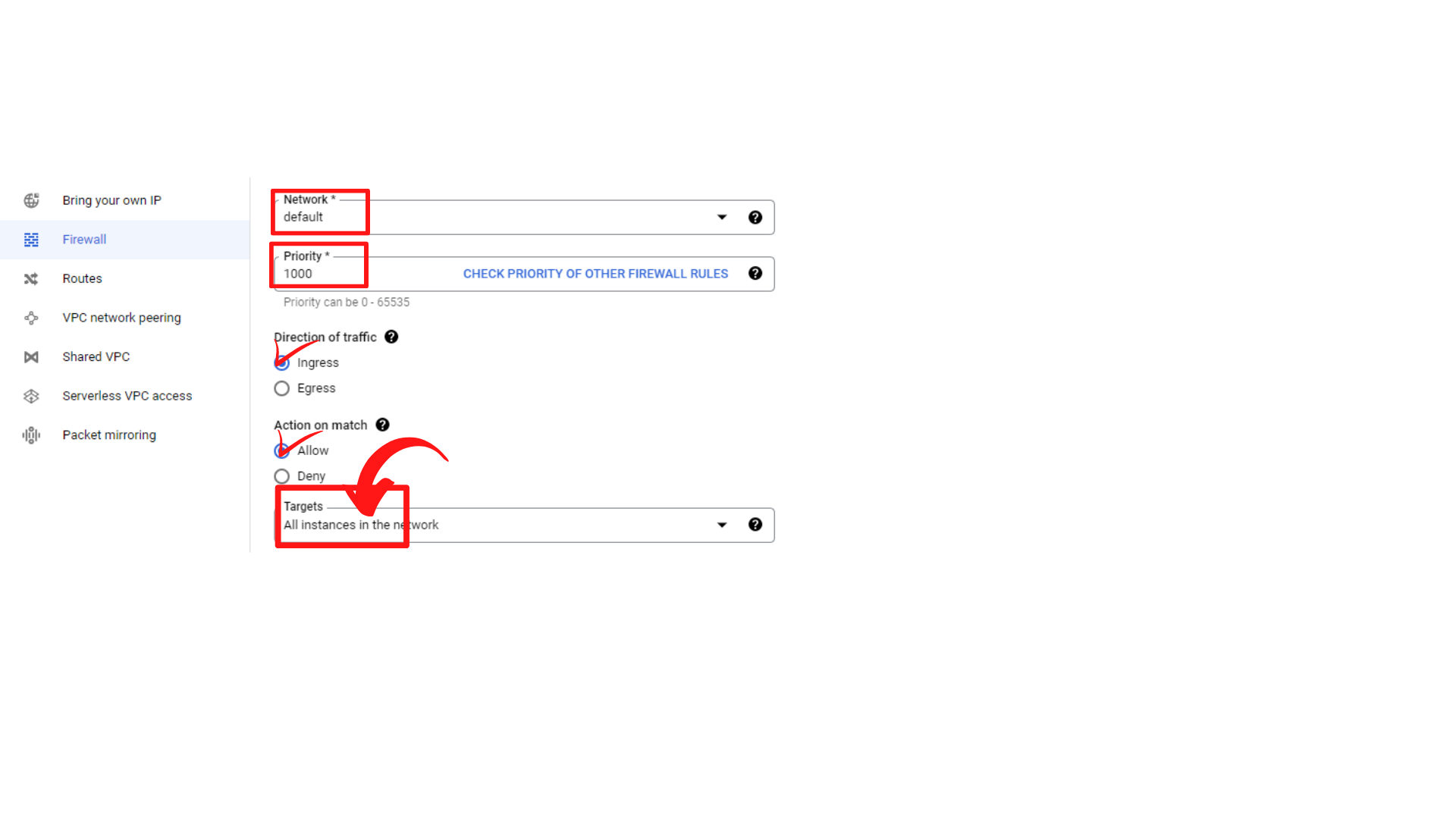


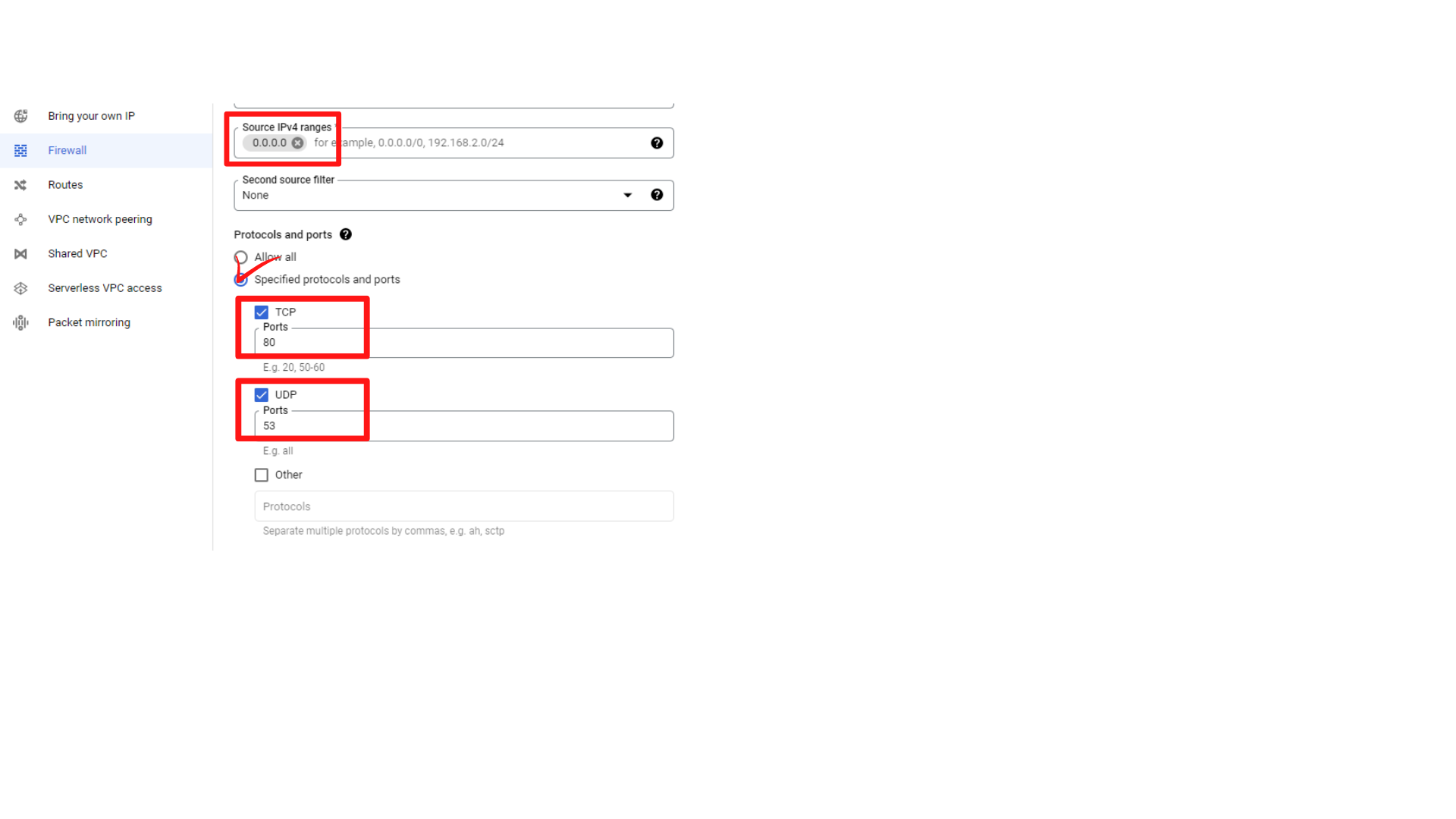
1. Now you will see the Create a firewall rule form. Enter the Name and description and you can turn on the logs if required. Here you do not need logs so turn off the Logs.



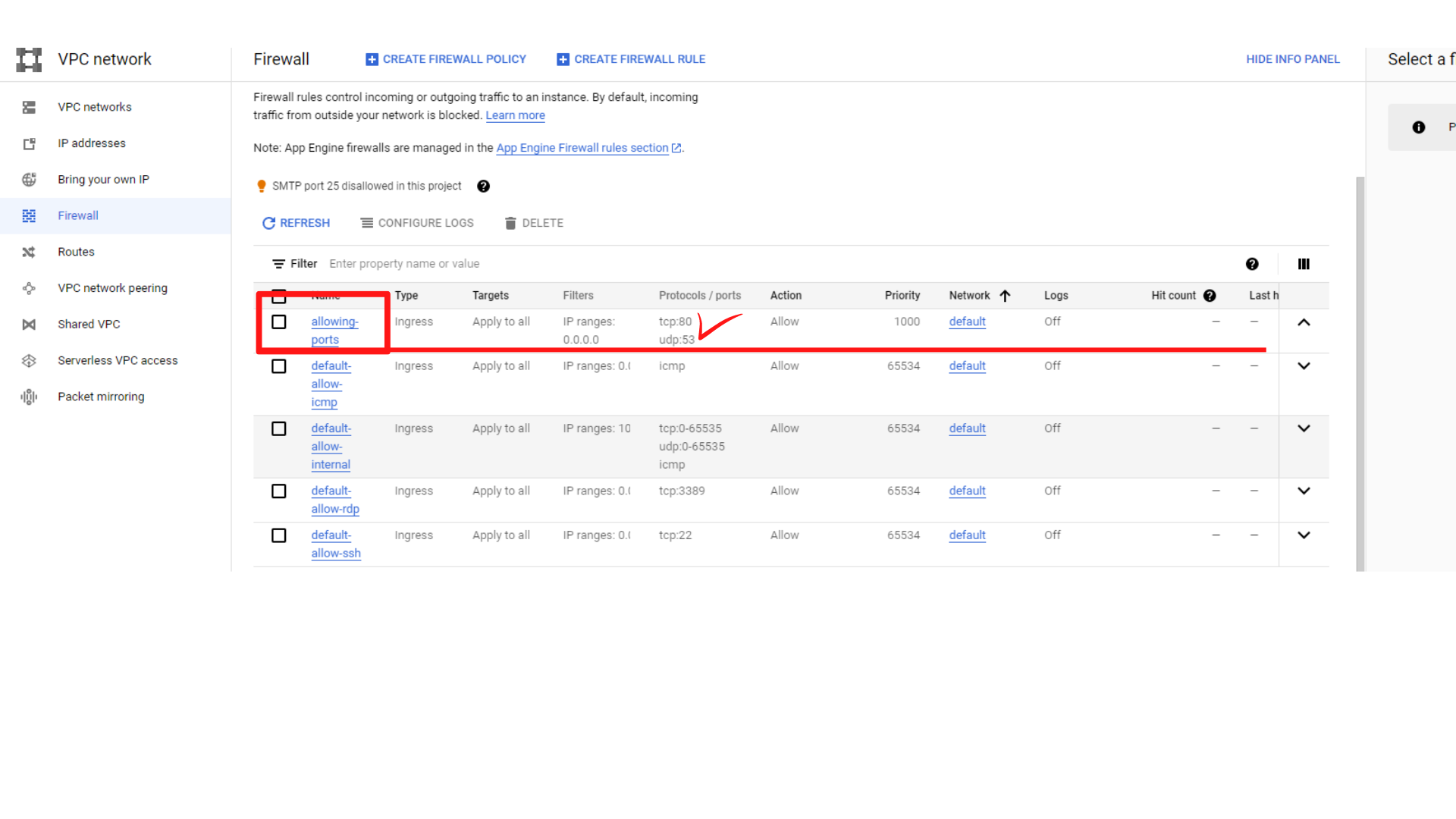
1. Fill the Firewall Rule:

* **Network :** Default ( You can choose any VPC as per your requirement)
* **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:**
* **tcp:**   ( Click the checkbox next to tcp and provide the port as 80)
* **udp:** ( Click the checkbox next to udp and provider the port as 53)





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



1. That’s it, you have successfully created a firewall rule that allows the HTTP traffic on port 80 and the DNS traffic on port 53.