Understanding Google Cloud VPC - Network, Firewalls, and Compute Engine Creation

Google Cloud’s Virtual Private Cloud (VPC)

is a powerful solution for networking in the cloud, allowing seamless communication between Compute Engine Virtual Machines (VMs) across different zones and regions. Whether you're building a fault-tolerant system or connecting VMs within the same network, VPCs offer a robust and scalable way to manage cloud resources.

Why Use Google Cloud VPC?

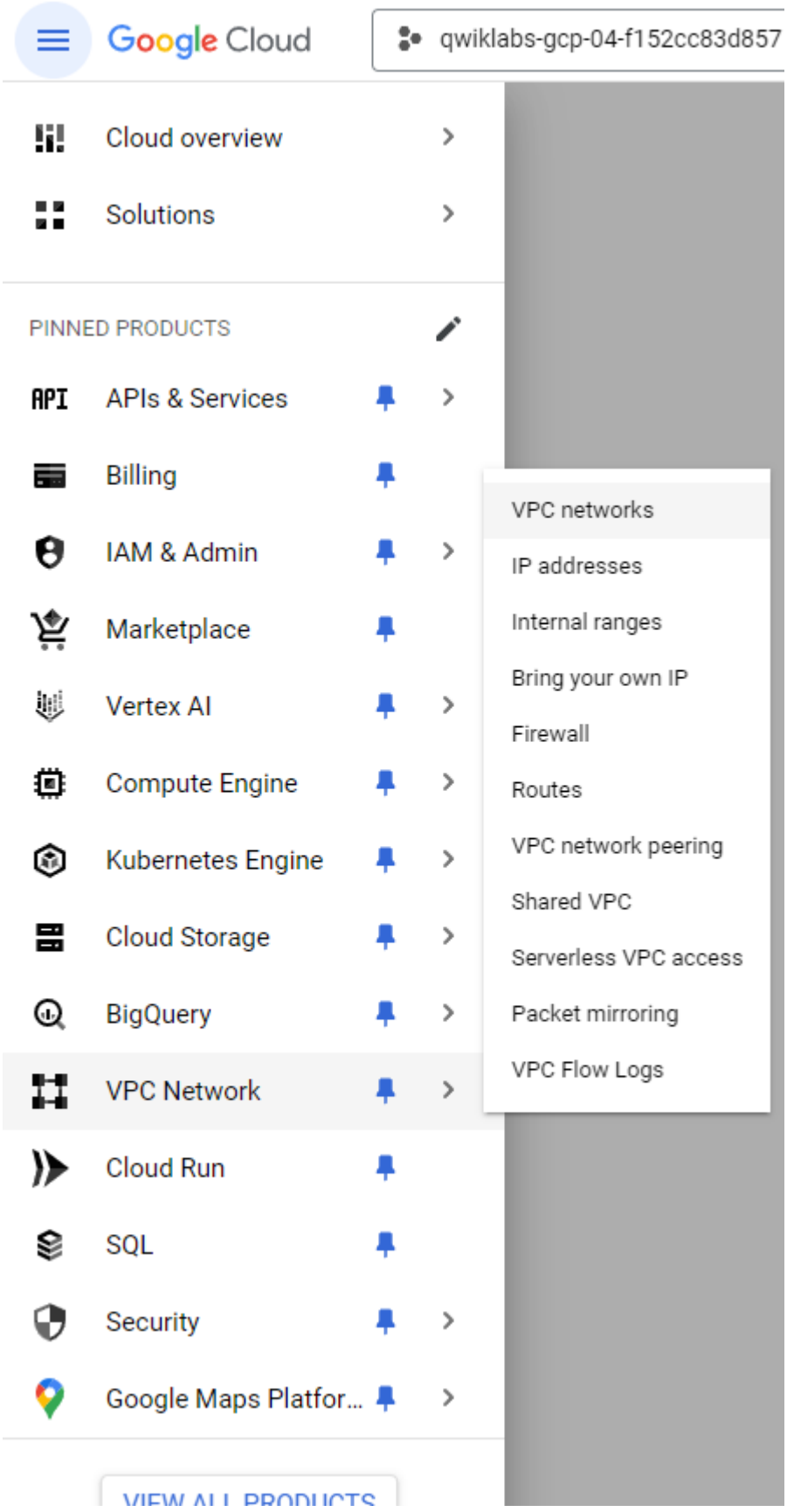
Even when VMs are in different regions or zones, Google Cloud VPC enables seamless communication across subnets, as if they were in the same physical location. Some key benefits include:

- **Unified Networking**: Despite being deployed in different zones, all VMs within a subnet are treated as part of the same network. This allows for straightforward communication between VMs in the same subnet, even if they are located in different geographical regions.
- **Fault Tolerance**: By deploying VMs across different zones, you increase fault tolerance and ensure high availability. At the same time, the VPC structure maintains a simple, unified network layout, making it easier to manage and troubleshoot.

Step 1: Creating a VPC Network on Google Cloud

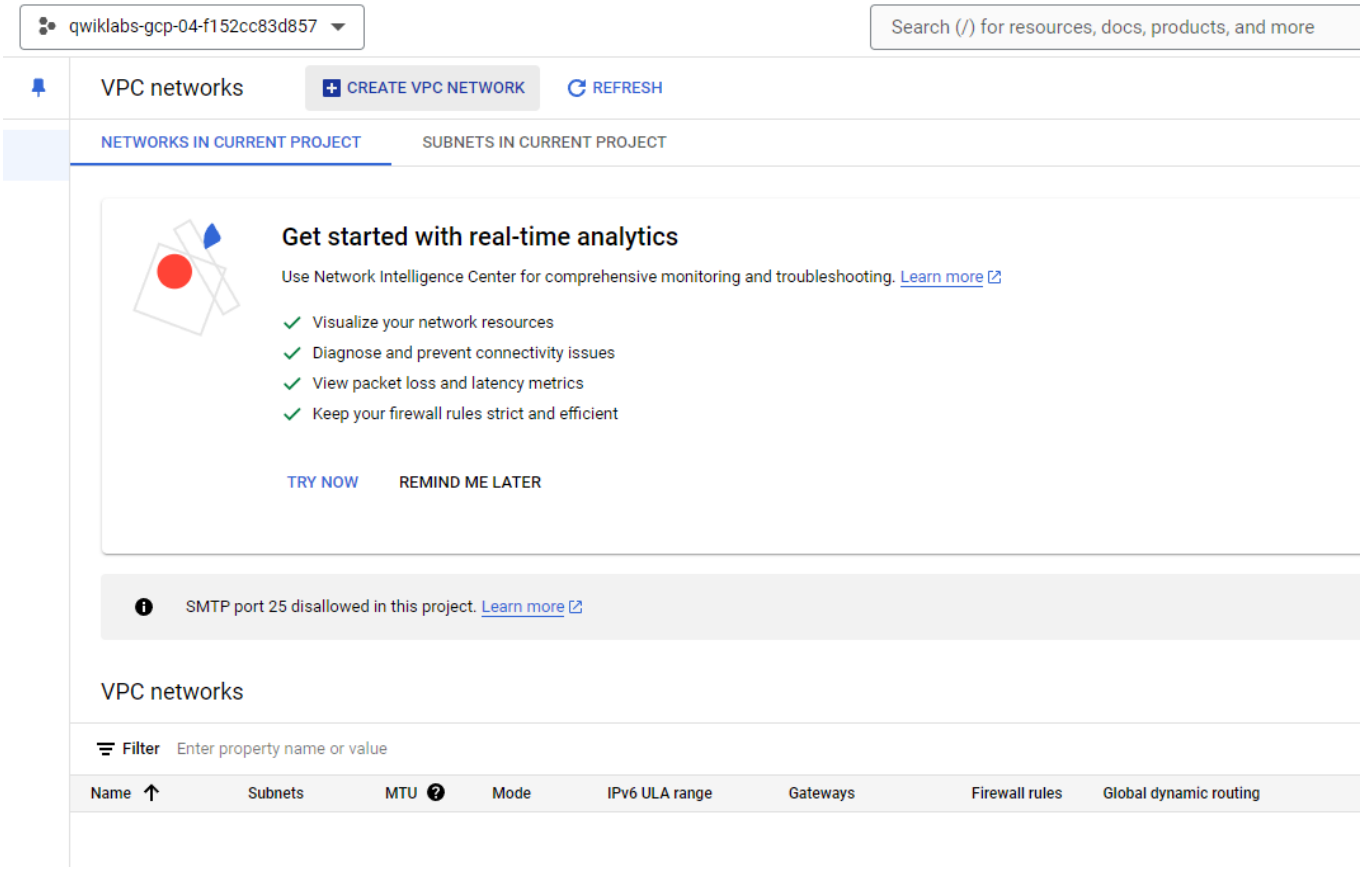
1- Navigate to the VPC Network page

In the Google Cloud Console, go to **VPC Network** > **VPC Networks**.



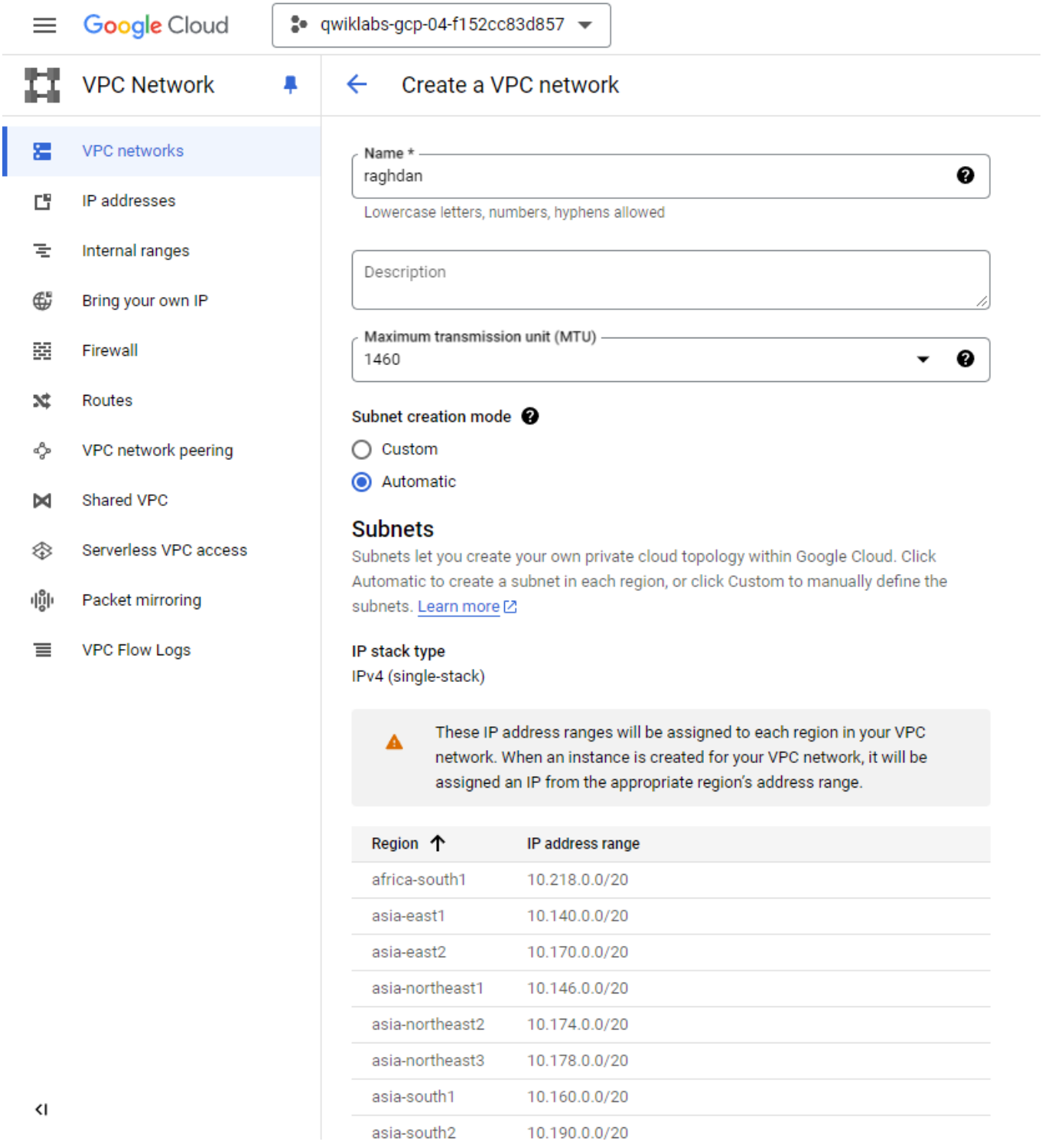
2- Create a VPC Network

Click on **Create VPC Network**.



3- Name your VPC and Define Subnets

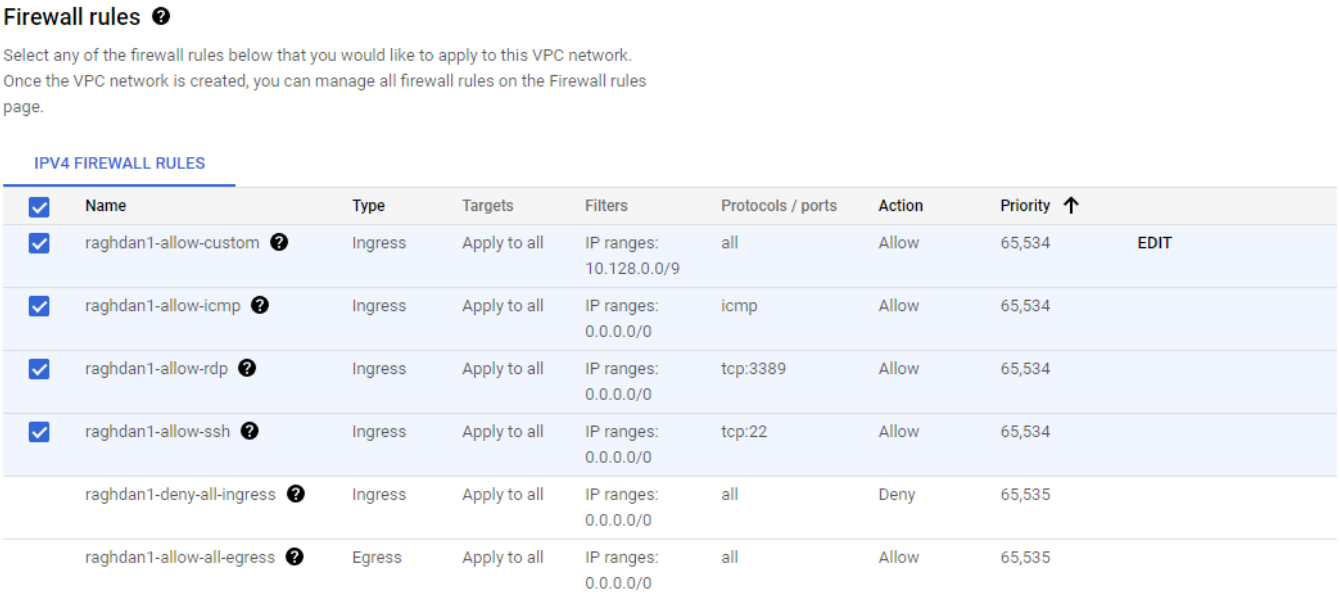
Give your VPC a name. For subnets, you can either create them manually or allow Google to automatically assign them per region.



4- Configure Firewall Rules

Basic firewall rules will be set up by default, enabling essential network traffic to pass through. It's important to note that there is an implicit deny-all rule that can't be deleted, which means

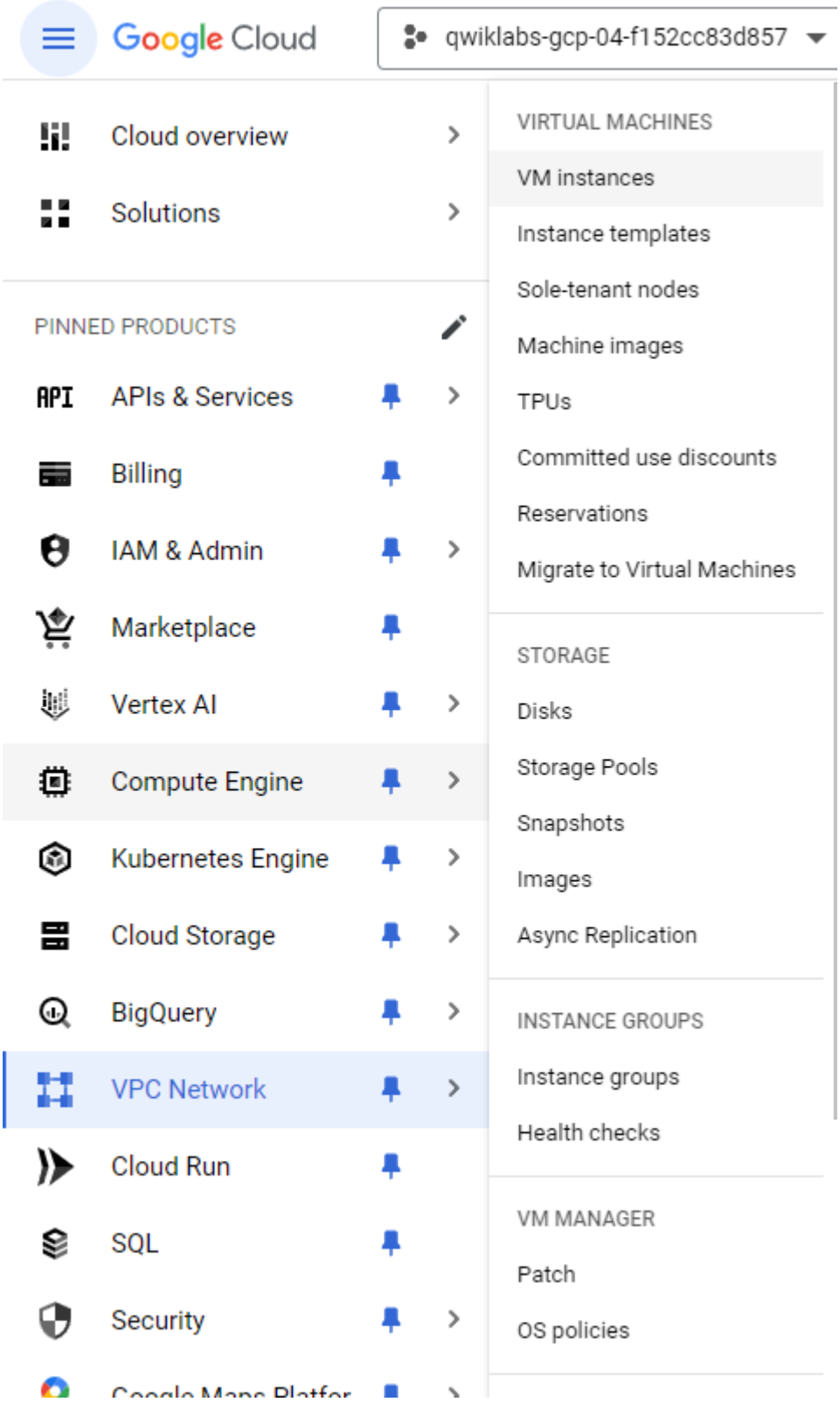
only explicitly allowed traffic will flow.



Step 2: Creating VMs on Google Compute Engine

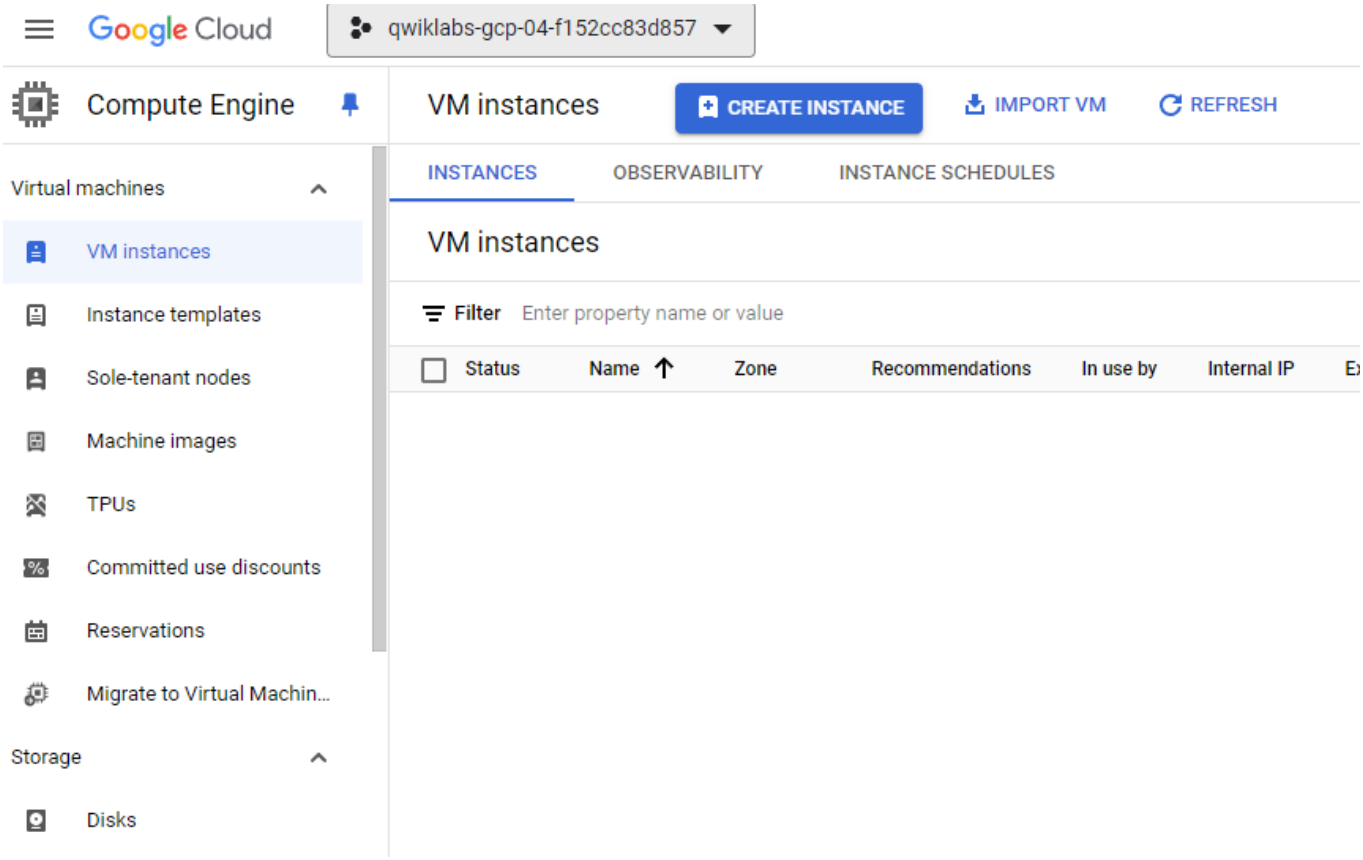
1- Navigate to VM Instances

Go to **Compute Engine** > **VM Instances**.



2- Create a New VM Instance

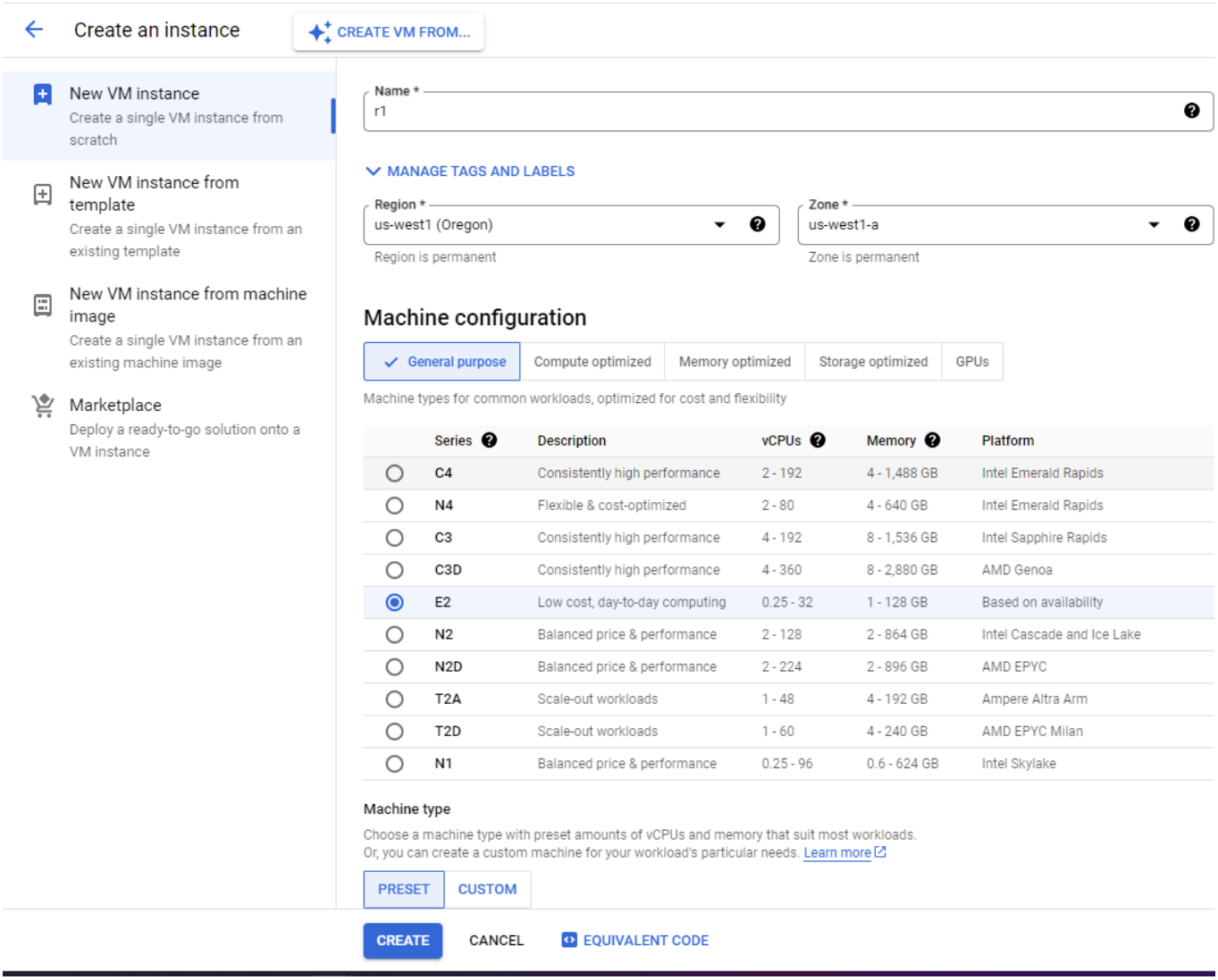
Click on **Create Instance** at the top of the screen.

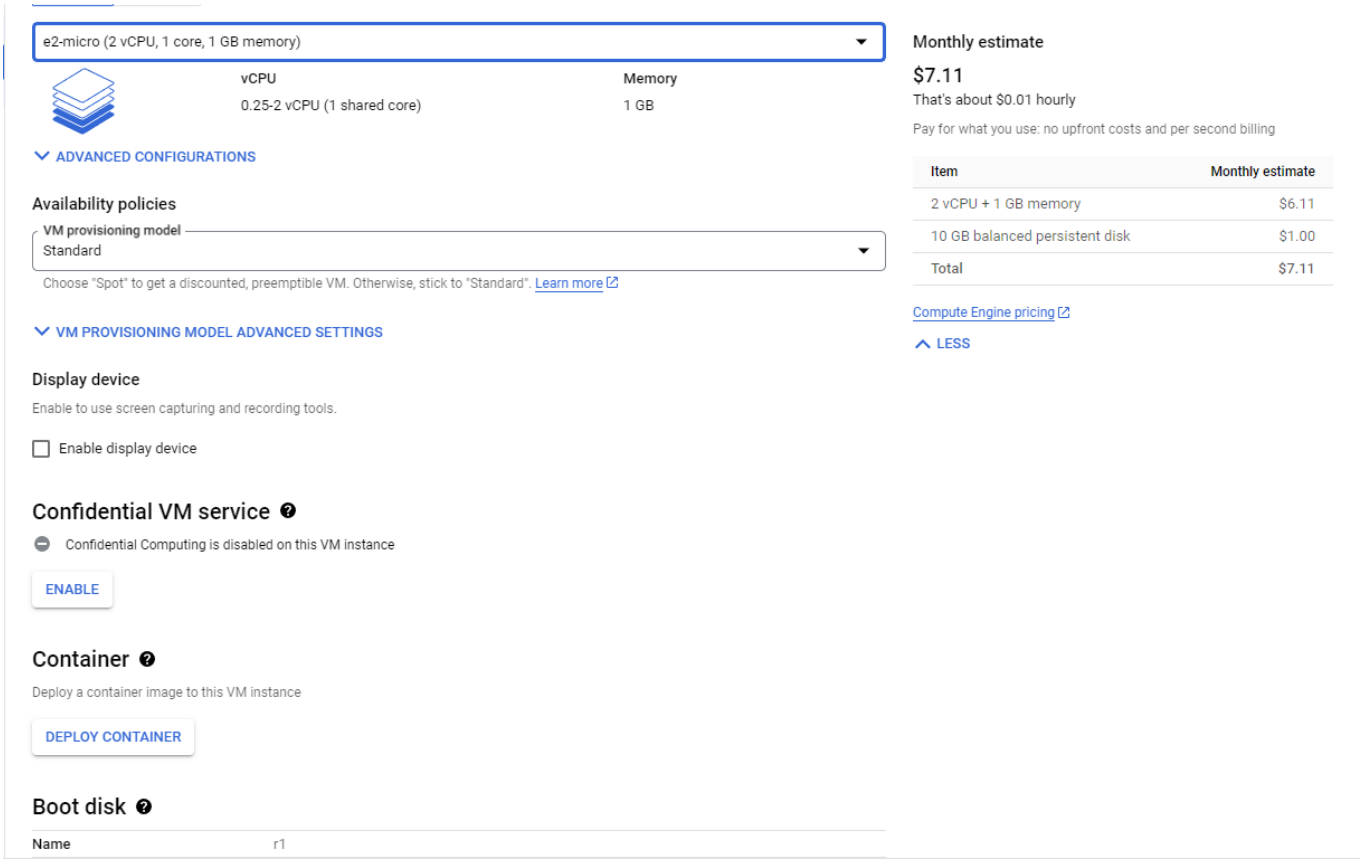


3- Configure Your VM

Name your VM and select the VM type. For this Lab, we'll use an `e2-micro` instance, which is a cost-effective option for testing purposes. The estimated monthly cost will be displayed on the

right.


Create an instance
CREATE VM FROM...
New VM instance
Create a single VM instance from scratch
New VM instance from template
Create a single VM instance from an existing template
New VM instance from machine image
Create a single VM instance from an existing machine image
Marketplace
Deploy a ready-to-go solution onto a VM instance
Name *
r1
MANAGE TAGS AND LABELS
Region *
us-west1 (Oregon)
Region is permanent
Zone *
us-west1-a
Zone is permanent
Machine configuration
General purpose
Compute optimized
Memory optimized
Storage optimized
GPUs
Machine types for common workloads, optimized for cost and flexibility
Series
Description
vCPUs
Memory
Platform
C4 Consistently high performance 2 - 192 4 - 1,488 GB Intel Emerald Rapids
N4 Flexible & cost-optimized 2 - 80 4 - 640 GB Intel Emerald Rapids
C3 Consistently high performance 4 - 192 8 - 1,536 GB Intel Sapphire Rapids
C3D Consistently high performance 4 - 360 8 - 2,880 GB AMD Genoa
E2 Low cost, day-to-day computing 0.25 - 32 1 - 128 GB Based on availability
N2 Balanced price & performance 2 - 128 2 - 864 GB Intel Cascade and Ice Lake
N2D Balanced price & performance 2 - 224 2 - 896 GB AMD EPYC
T2A Scale-out workloads 1 - 48 4 - 192 GB Ampere Altra Arm
T2D Scale-out workloads 1 - 60 4 - 240 GB AMD EPYC Milan
N1 Balanced price & performance 0.25 - 96 0.6 - 624 GB Intel Skylake
Machine type
Choose a machine type with preset amounts of vCPUs and memory that suit most workloads.
Or, you can create a custom machine for your workload's particular needs. Learn more
PRESET
CUSTOM
CREATE
CANCEL
EQUIVALENT CODE



NOTE Review Firewall Rules

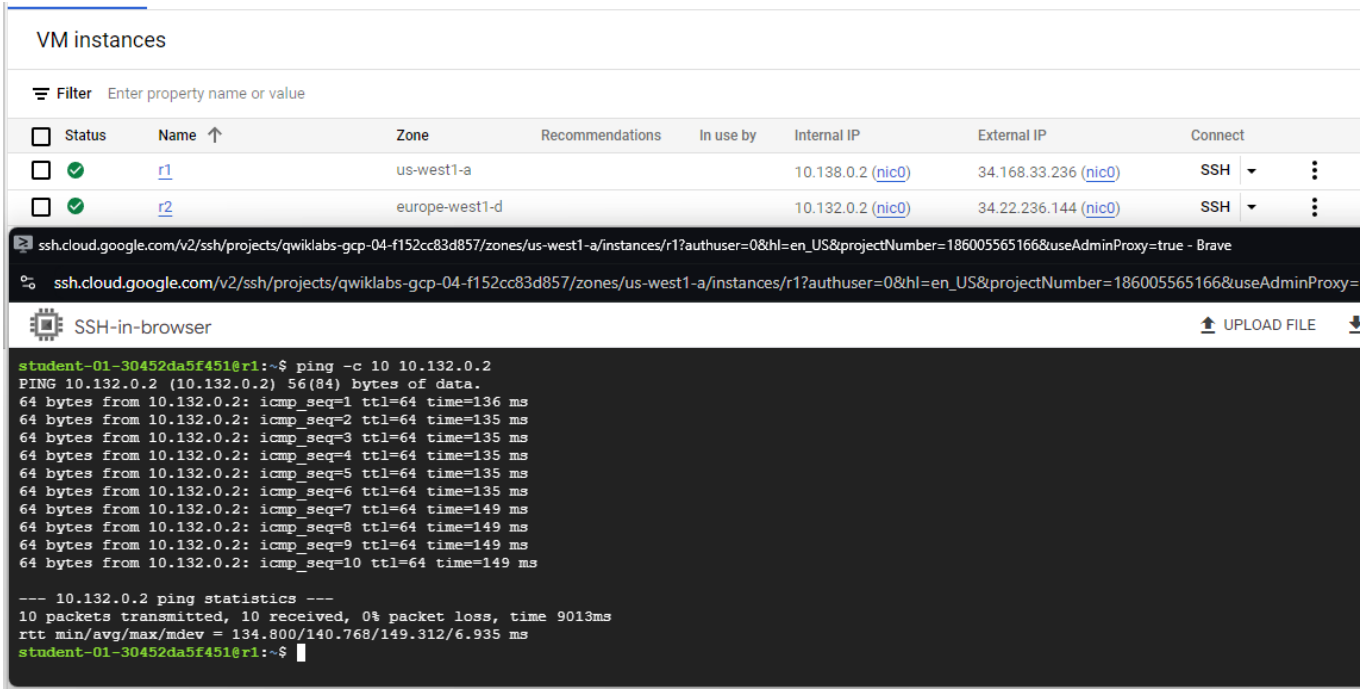
If necessary, you can review and modify firewall settings by navigating to **VPC Network** > **Firewall**. This is where you can manage rules for inbound and outbound traffic.

Step 3: Connectivity Test Between VM Instances

1- Ping Between Internal IPs

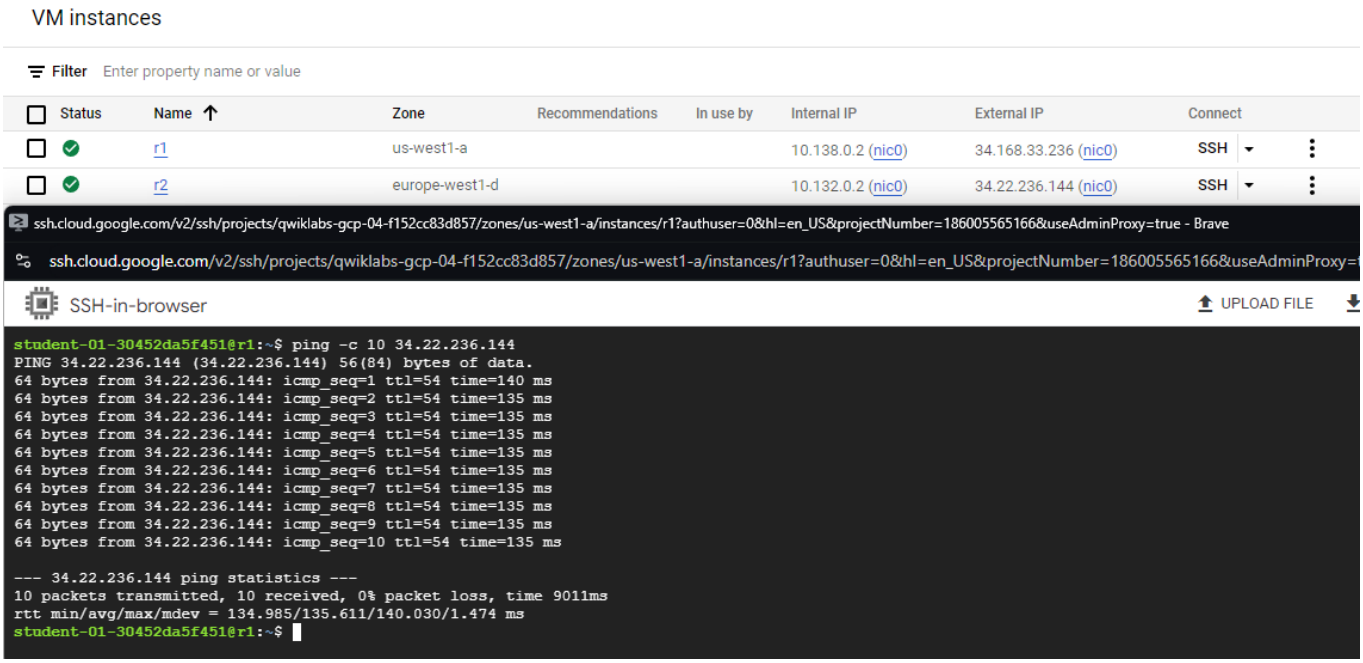
Each VM is assigned both an internal and external IP address. You should be able to successfully ping between the internal IP addresses of VMs, thanks to the default firewall rules

that allow ICMP (ping) traffic and the VPC's default routing between subnet regions.



2- Ping Between External IPs

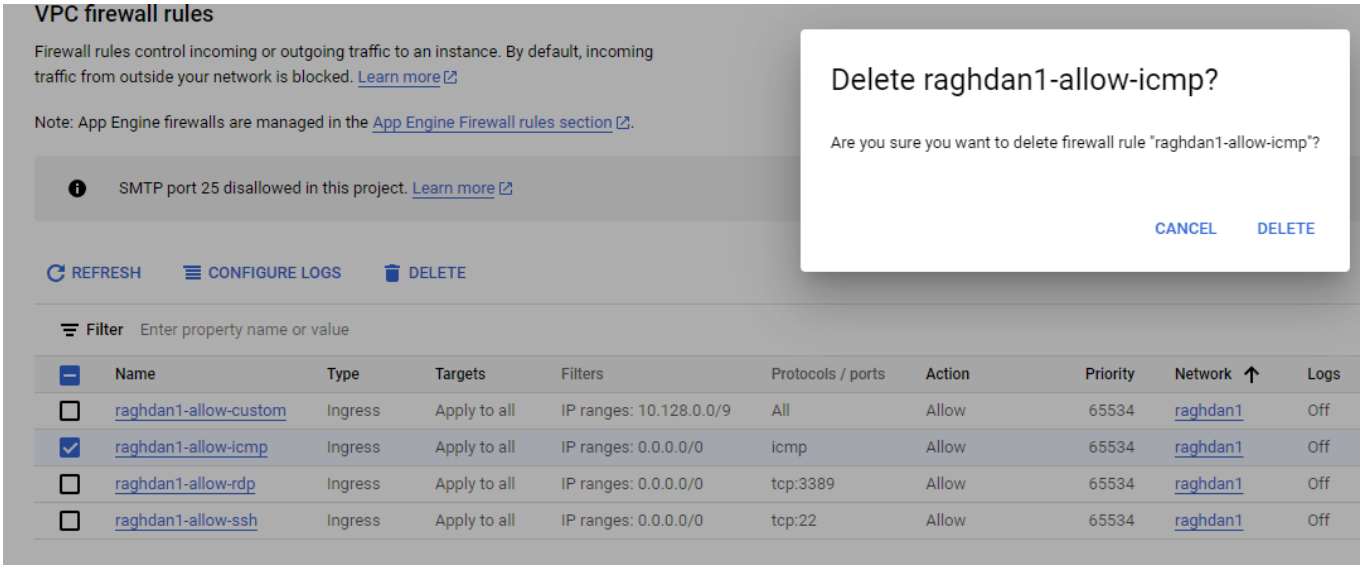
Similarly, VMs should be able to ping each other over their external IP addresses unless specific firewall rules are blocking external ICMP traffic.

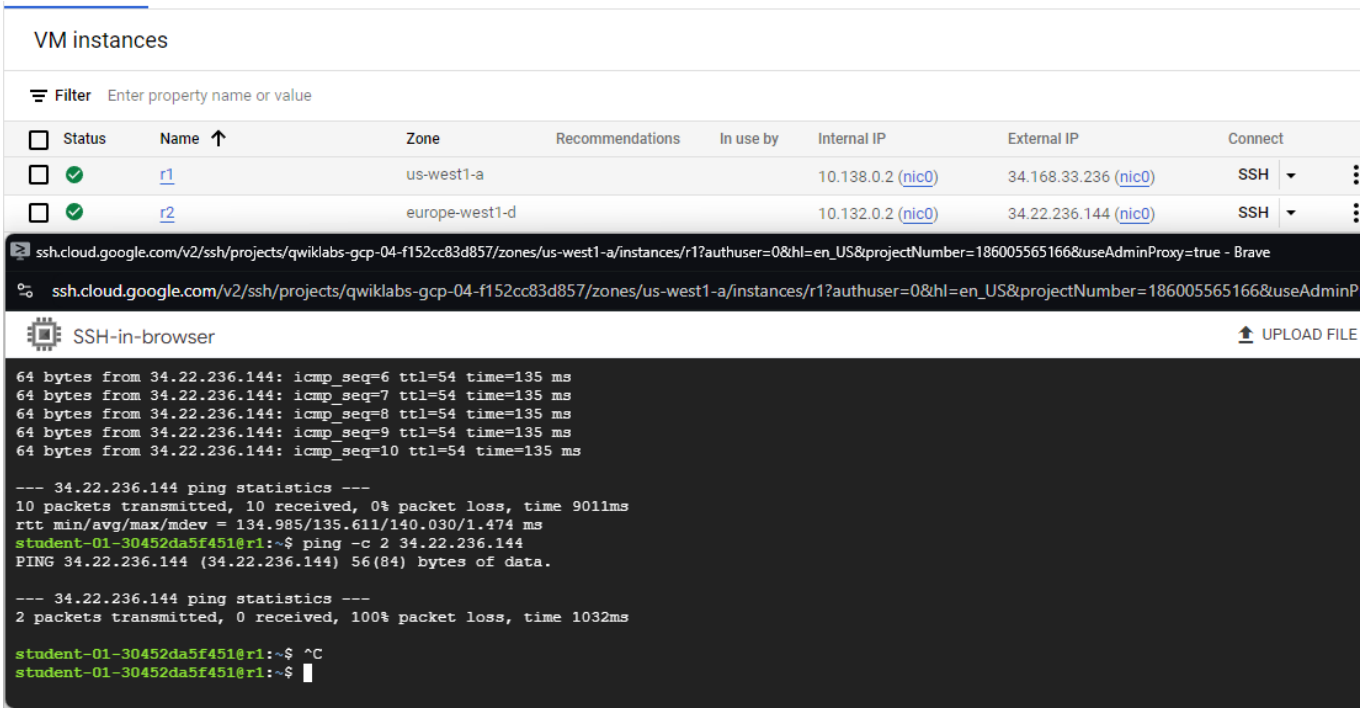


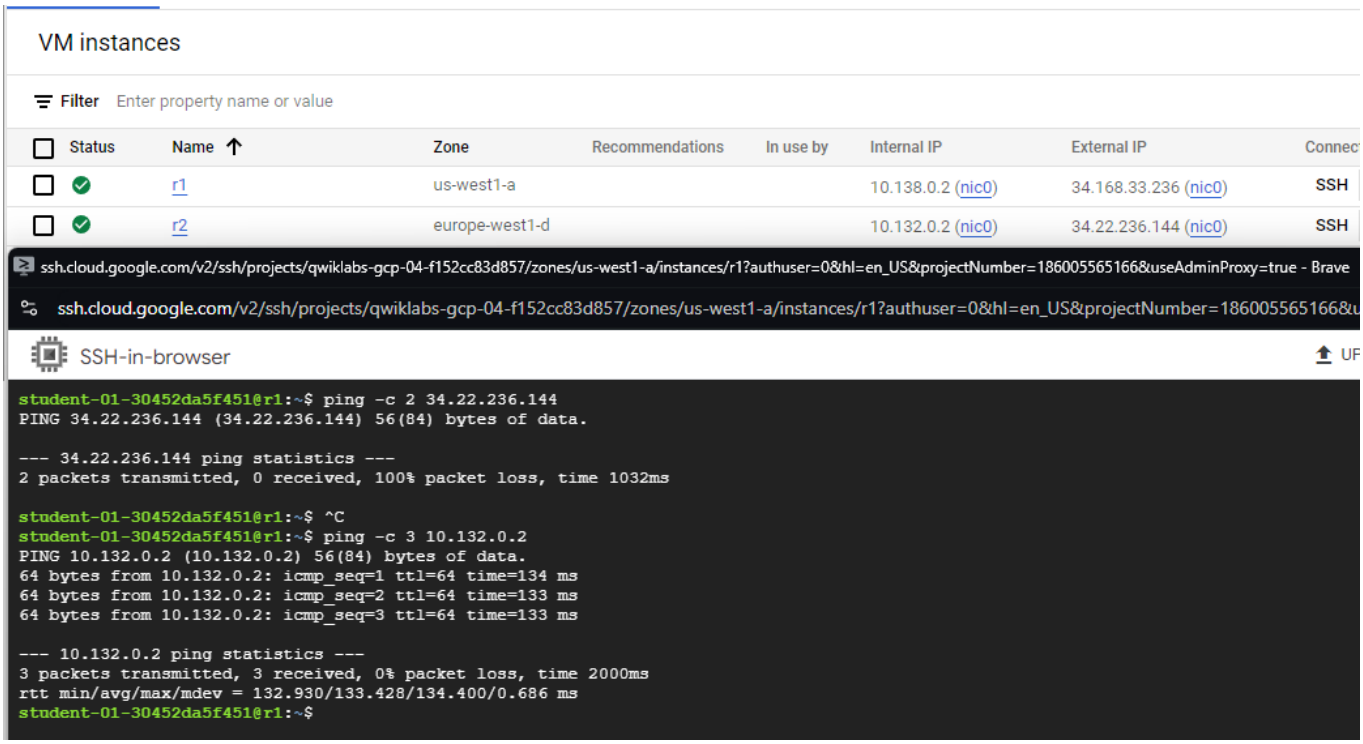
Step 4: Modifying Firewall Rules

1- Deleting the ICMP Firewall Rule

When you delete the rule that allows ICMP traffic, you will see a 100% packet loss when attempting to ping external IP addresses. However, internal connectivity remains unaffected due to the default custom firewall rule that allows internal traffic.

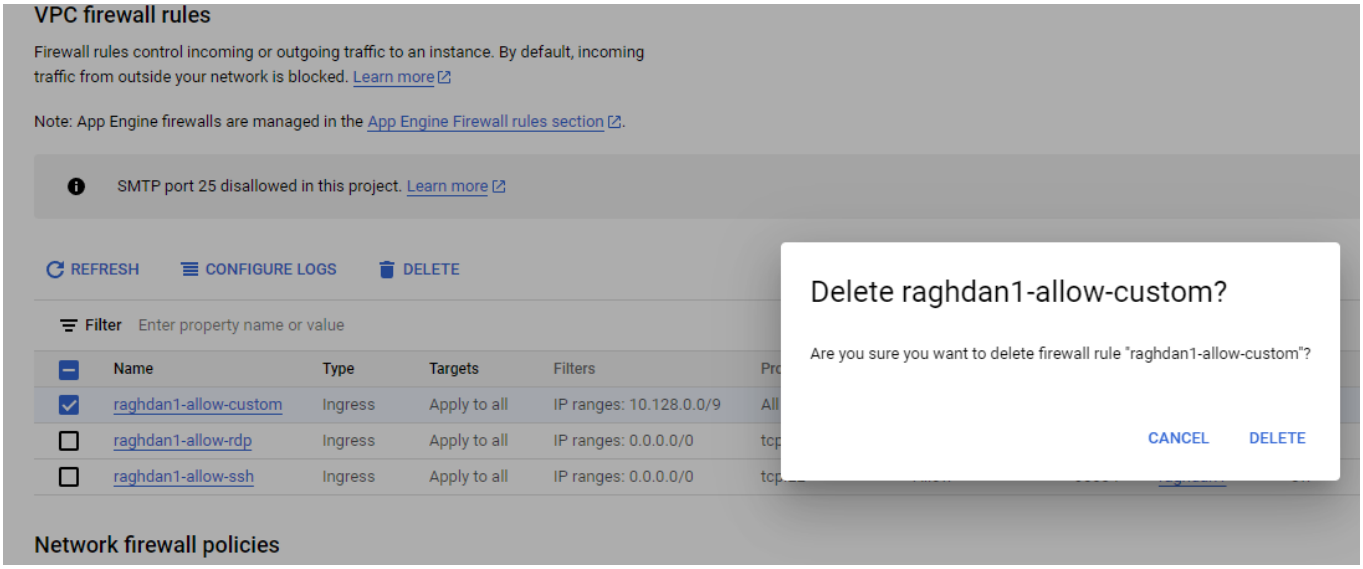




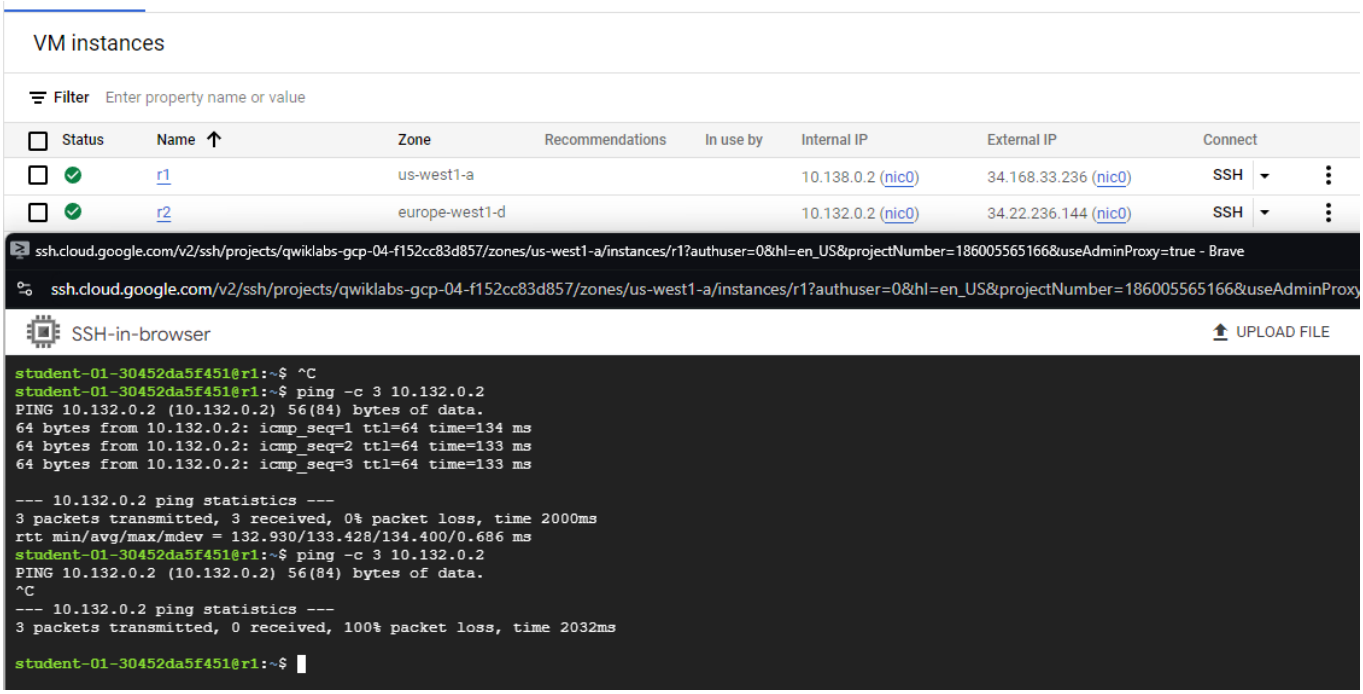


2- Delete the Custom Firewall Rule

Once you delete the custom firewall rule that allows internal communication, the internal IP address will no longer be reachable either, demonstrating the importance of proper firewall rule configuration.



Now the Internal IP is not reachable anymore.



Summary

Google Cloud VPC offers a robust and flexible networking solution for Compute Engine instances, allowing seamless communication across regions and zones. By leveraging VPC's default routing and configurable firewall rules, users can efficiently manage cloud networks while ensuring high availability and fault tolerance.\

Key Takeaways

1. **Unified Networking Across Regions**: VPC allows VMs in different zones to communicate as though they are on the same subnet, simplifying network management.
2. **High Availability**: Distributing VMs across different zones increases fault tolerance without complicating network layout.
3. **Firewall Rules Management**: Firewall rules, particularly the default deny-all policy, are crucial in controlling access. Ensure that both external and internal traffic is properly configured for your needs.
4. **Connectivity Testing**: Internal connectivity between VMs is preserved even when external access is restricted, thanks to custom firewall rules.

By following these steps, you can set up a VPC, configure firewall rules, and test connectivity to ensure that your cloud infrastructure is secure and fully functional.