GCP Public and Private Subnets

Okay, let's walk through how to create public and private subnets and demonstrate connectivity using the Google Cloud Console.

1. Create a VPC Network:

- Navigate to the Google Cloud Console: https://console.cloud.google.com/
- Open the navigation menu (☰) in the top-left corner.
- Go to **VPC network**.
- Click **Create VPC network**.
- **Name:** Enter my-vpc-network.
- **Subnet creation mode:** Select **Custom**.
- Click **Create**.

2. Create the Public Subnet:

- On the VPC network details page for my-vpc-network (you'll be redirected there after creation, or you can find it in the VPC network list), click **Add subnet**.
- **Name:** Enter public-subnet.
- **Region:** Choose a region (e.g., asia-south1).
- **IP address range:** Enter 10.0.1.0/24.
- **Private Google Access:** Leave as **Off**.
- Click **Add**.

3. Create the Private Subnet:

- Again, on the VPC network details page for my-vpc-network, click **Add subnet**.
- **Name:** Enter private-subnet.
- **Region:** Ensure it's the same region as the public subnet (e.g., asia-south1).
- **IP address range:** Enter 10.0.2.0/24.
- **Private Google Access:** Set to **On**. This allows instances in this subnet to reach Google Cloud services without a public IP.
- Click **Add**.

4. Create Instances in Each Subnet:

- Open the navigation menu (☰) and go to **Compute Engine** > **VM instances**.
- Click **Create instance**.

Public Subnet Instance:

- **Name:** Enter public-instance.
- **Region:** Choose the same region as your subnets (e.g., asia-south1).
- **Zone:** Choose a zone within that region (e.g., asia-south1-a).
- **Machine configuration:** Choose a machine type (e.g., e2-medium).
- **Boot disk:** Select an image (e.g., Debian 11). Click **Change**, choose an image, and click **Select**.
- **Network interfaces:** Click on the **default** network interface to edit it.
  - **Network:** Select my-vpc-network.
  - **Subnetwork:** Select public-subnet.
  - **External IPv4 address:** Select **Ephemeral** or **Static** to assign a public IP.
  - Click **Done**.
- **Firewall:** Check **Allow HTTP traffic** and **Allow HTTPS traffic** (optional, but helpful for testing internet access later).
- Click **Create**.

Private Subnet Instance:

- Click **Create instance**.
- **Name:** Enter private-instance.
- **Region:** Choose the same region.
- **Zone:** Choose a zone within that region (it can be the same or different from the public instance's zone within the same region).
- **Machine configuration:** Choose a machine type.
- **Boot disk:** Select an image.
- **Network interfaces:** Click on the **default** network interface to edit it.
  - **Network:** Select my-vpc-network.
  - **Subnetwork:** Select private-subnet.
  - **External IPv4 address:** Select **None** to ensure it doesn't get a public IP.
  - Click **Done**.
- **Firewall:** Leave the firewall rules unchecked for now; we'll create specific rules.
- Click **Create**.

5. Configure Firewall Rules for Connectivity:

- Open the navigation menu (☰) and go to **VPC network** > **Firewall**.
- Click **Create firewall rule**.

Allow SSH to Public Instance:

- **Name:** Enter allow-ssh-public.
- **Network:** Select my-vpc-network.
- **Direction of traffic:** Select **Ingress**.
- **Action on match:** Select **Allow**.
- **Targets:** Select **Specified target tags**.
- **Target tags:** Enter public-instance. (You might need to edit the public-instance after creation to add this tag under the instance details.)
- **Source filter:** Select **IP ranges**.
- **Source IP ranges:** Enter 0.0.0.0/0 (for testing purposes; in production, restrict this to your known IP ranges).
- **Protocols and ports:** Select **Specified protocols and ports** and enter tcp:22.
- Click **Create**.

Allow ICMP (Ping) from Public to Private Instance:

- Click **Create firewall rule**.
- **Name:** Enter allow-icmp-internal.
- **Network:** Select my-vpc-network.
- **Direction of traffic:** Select **Ingress**.
- **Action on match:** Select **Allow**.
- **Targets:** Select **Specified target tags** or **All instances in the network** (for simplicity in this demonstration).
- **Source filter:** Select **IP ranges**.
- **Source IP ranges:** Enter 10.0.1.0/24 (the IP range of the public subnet).
- **Protocols and ports:** Select **Specified protocols and ports** and enter icmp.
- **Destination filter:** Select **IP ranges**.
- **Destination IP ranges:** Enter 10.0.2.0/24 (the IP range of the private subnet).
- Click **Create**.

Allow SSH from Public to Private Instance:

- Click **Create firewall rule**.
- **Name:** Enter allow-ssh-internal.
- **Network:** Select my-vpc-network.
- **Direction of traffic:** Select **Ingress**.

- **Action on match:** Select **Allow**.
- **Targets:** Select **Specified target tags** or **All instances in the network**.
- **Source filter:** Select **IP ranges**.
- **Source IP ranges:** Enter 10.0.1.0/24.
- **Protocols and ports:** Select **Specified protocols and ports** and enter tcp:22.
- **Destination filter:** Select **IP ranges**.
- **Destination IP ranges:** Enter 10.0.2.0/24.
- Click **Create**.

6. Demonstrate Connectivity:

- Go to **Compute Engine** > **VM instances**.
- Find the public-instance and note its **External IP**.
- Use a terminal or SSH client to connect to the public-instance using its external IP:

ssh <your-username>@<public-instance-external-ip>

(Replace <your-username> with your username on the instance). You might need to set up SSH keys for your project or instance if you haven't already.

- Once you are SSH'd into the public-instance, you need to find the **Internal IP** of the private-instance. Go back to the VM instances list in the console and note the "Internal IP" of the private-instance (it will be in the 10.0.2.0/24 range).
- Also, make sure that you are creating an **SSH key inside your public VM** using the command **ssh-keygen** then you need to copy the **Public Key** and paste it inside your Private VM.
- To paste the Public key inside your Private VM, you need to open it on the console and click on edit, then scroll down to SSH keys, click on add items and paste the public key there. Then click on save.

  ssh <your-username>@<private-instance-private-ip
- From the SSH session of the public instance, try to ping the internal IP of the private instance:

ping <private-instance-internal-ip>

If the allow-icmp-internal firewall rule is working, you should see successful ping replies.

- (Optional) From the public-instance, try to SSH into the private-instance using its internal IP:

ssh <your-username>@<private-instance-internal-ip>

If the allow-ssh-internal firewall rule is working and you have configured SSH access (e.g., through metadata or the same user), you should be able to connect.

- (Optional) From the public-instance, try to ping an external website (e.g., ping google.com). This should work because the public-instance has a public IP.

- (Optional) Try to ping an external website from the private-instance (you'll need to be SSH'd into it via the public-instance). This should likely fail as the private-instance doesn't have a direct public IP. To allow internet access from the private instance, you would need to configure a Cloud NAT gateway.