**EX: 04 NAME: M. NIVASHINI**

**DATE: 23.07.2024 ROLL.NO.: 23MCA020**

**Virtual Private Cloud Configuration(VPC)**

**Aim:**

To develop and work with Virtual Private Cloud Configuration(VPC) using AWS.

**Theoretical Background**

**1. Create a New VPC**

1. **Log in to AWS Management Console:**
   * Navigate to the AWS Management Console and sign in.
2. **Open the VPC Dashboard:**
   * Go to the VPC service by selecting **Services** from the top menu and then **VPC**.
3. **Create a New VPC:**
   * Click **Create VPC**.
   * Select **VPC only** and click **Next: Configure VPC**.
   * Enter a **Name tag** (e.g., MyCustomVPC).
   * Define an **IPv4 CIDR block** (e.g., 10.0.0.0/16).
   * Optionally, select an **IPv6 CIDR block** if needed.
   * Choose a **Tenancy** (default or dedicated).
   * Click **Create VPC**.

**2. Create Subnets**

1. **Open the Subnets Section:**
   * In the VPC Dashboard, go to **Subnets**.
2. **Create a Public Subnet:**
   * Click **Create subnet**.
   * Enter a **Name tag** (e.g., PublicSubnet).
   * Choose the VPC created in Step 1.
   * Define the **Availability Zone** (optional but recommended for high availability).
   * Specify an **IPv4 CIDR block** within the VPC’s CIDR range (e.g., 10.0.1.0/24).
   * Click **Create subnet**.
3. **Create a Private Subnet:**
   * Repeat the process above.
   * Enter a **Name tag** (e.g., PrivateSubnet).
   * Use a different **IPv4 CIDR block** (e.g., 10.0.2.0/24).
   * Click **Create subnet**.

**3. Configure Security Groups**

1. **Open the Security Groups Section:**
   * Go to **Security Groups** in the VPC Dashboard.
2. **Create a New Security Group:**
   * Click **Create security group**.
   * Enter a **Name tag** (e.g., PublicSG).
   * Provide a **Description** (e.g., Security group for public subnet).
   * Choose the VPC created in Step 1.
   * Configure **Inbound rules** (e.g., allow HTTP and SSH from anywhere).
   * Click **Create security group**.
3. **Repeat for Private Security Group:**
   * Create another security group (e.g., PrivateSG).
   * Define inbound rules based on your application’s needs.
   * Configure outbound rules to allow necessary traffic (e.g., to the NAT gateway).

**4. Create and Configure an Internet Gateway**

1. **Open the Internet Gateways Section:**
   * Go to **Internet Gateways** in the VPC Dashboard.
2. **Create a New Internet Gateway:**
   * Click **Create internet gateway**.
   * Enter a **Name tag** (e.g., MyInternetGateway).
   * Click **Create internet gateway**.
3. **Attach the Internet Gateway to the VPC:**
   * Select the newly created internet gateway.
   * Click **Actions** > **Attach to VPC**.
   * Select the VPC created in Step 1 and click **Attach**.

**5. Create and Configure a NAT Gateway**

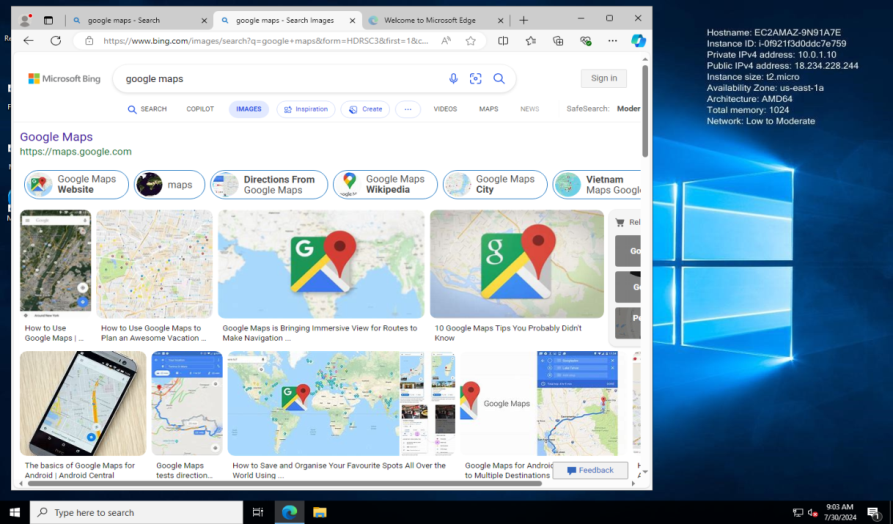
1. **Allocate an Elastic IP Address:**
   * Go to **Elastic IPs** under the **Network & Security** section.
   * Click **Allocate elastic IP address**.
   * Click **Allocate** and copy the allocated IP address.
2. **Create a NAT Gateway:**
   * Go to **NAT Gateways** in the VPC Dashboard.
   * Click **Create NAT gateway**.
   * Choose the **Public subnet** for the NAT gateway.
   * Assign the **Elastic IP address** allocated in the previous step.
   * Click **Create NAT gateway**.

**6. Set Up Route Tables**

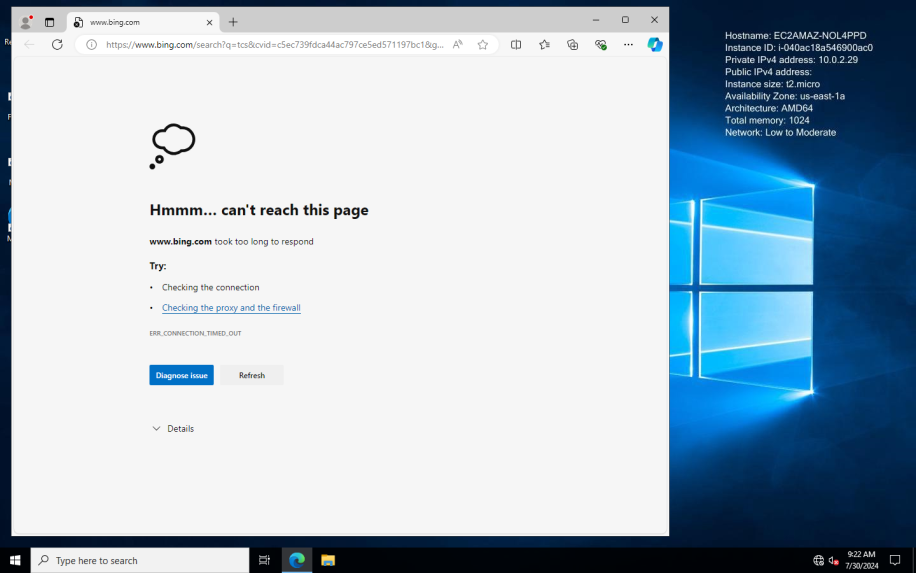
1. **Open Route Tables Section:**
   * Go to **Route Tables** in the VPC Dashboard.
2. **Create a Route Table for the Public Subnet:**
   * Click **Create route table**.
   * Enter a **Name tag** (e.g., PublicRouteTable).
   * Choose the VPC created in Step 1.
   * Click **Create route table**.
3. **Add Routes for Public Access:**
   * Select the route table.
   * Go to the **Routes** tab and click **Edit routes**.
   * Add a route:
     + Destination: 0.0.0.0/0 (for all IPv4 traffic)
     + Target: Select the **Internet Gateway** created earlier.
   * Click **Save changes**.
4. **Associate the Public Subnet:**
   * Go to the **Subnet Associations** tab.
   * Click **Edit subnet associations**.
   * Select the **Public Subnet** and click **Save**.
5. **Create a Route Table for the Private Subnet:**
   * Repeat the process above to create another route table (e.g., PrivateRouteTable).
6. **Add Routes for Private Subnet Access:**
   * Select the route table.
   * Go to the **Routes** tab and click **Edit routes**.
   * Add a route:
     + Destination: 0.0.0.0/0 (for all IPv4 traffic)
     + Target: Select the **NAT Gateway** created earlier.
   * Click **Save changes**.
7. **Associate the Private Subnet:**
   * Go to the **Subnet Associations** tab.
   * Click **Edit subnet associations**.
   * Select the **Private Subnet** and click **Save**.

**Output**

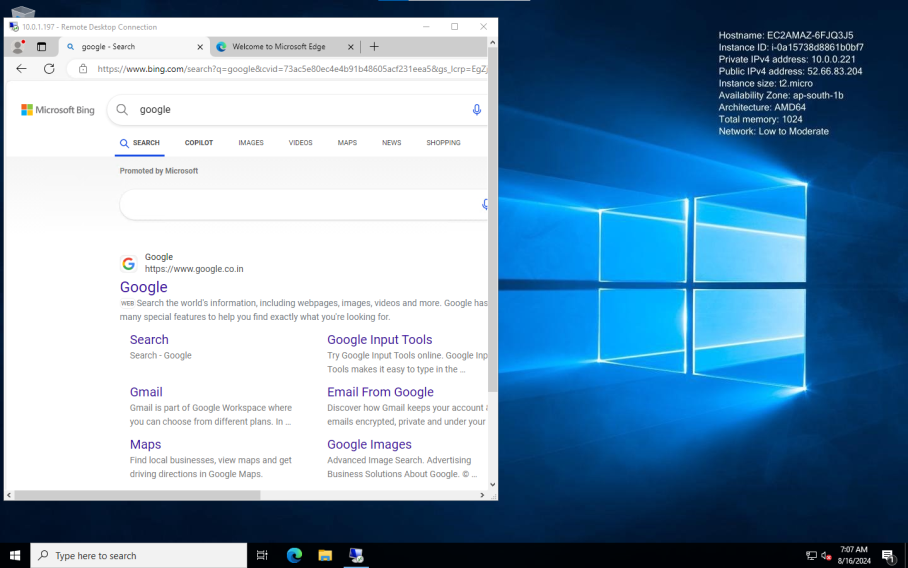
**Public**



**Private**



**After creating NAT**

****

**Conclusion**

Thus the AWS VPC with public and private subnets, ensuring the public subnet has direct internet access and the private subnet uses a NAT Gateway for internet access. Security Groups and Route Tables were set up to control traffic and access has been developed and executed successfully.