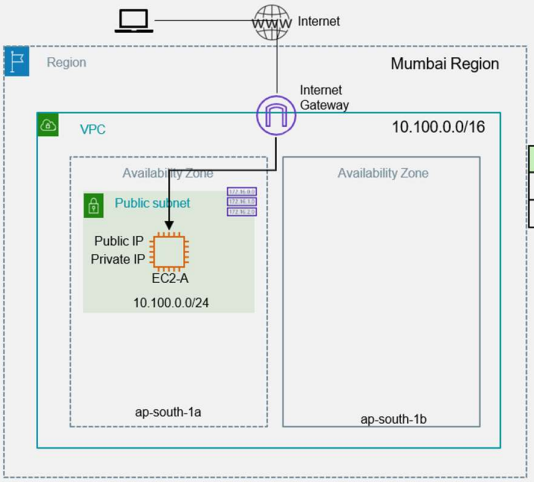
Exercise – Public Subnet



Public Subnet Route table

Destination	Target
10.100.0.0/16	Local
0.0.0.0/0	igw-xxxxxx

High level steps

1. Create a new VPC
2. Create an Internet Gateway & associate with your VPC
3. Create a Subnet in one of the availability zone. Enable Auto-assign Public IP for a subnet.
4. Create a Route table and add a route for destination (0.0.0.0/0) with target as an internet gateway
5. Associate route table with your subnet
6. Launch EC2 instance in your subnet.
7. Connect to EC2 instance over SSH using it's Public IP

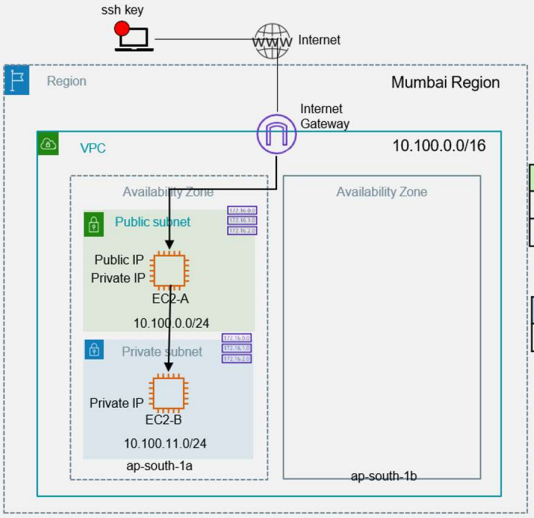
Steps

1. Create VPC
   a. AWS Console -> Go to VPC service -> Your VPCs -> Create VPC (Resources to create : VPC Only, Name tag: VPC-A, IPv4 CIDR block: Select IPv4 CIDR manual input (10.100.0.0/16) , Tenancy : Default - > Create VPC
2. Create Internet Gateway
   a. Internet Gateways -> Create internet gateway (Name tag: VPC-A-IGW) -> Create internet gateway
   b. Select Internet gateway -> Actions -> Attach to VPC -> Select your VPC (VPC-A) -> Attach Internet Gateway
3. Create Subnet
   a. Subnets -> Create subnet
   b. Select VPC ID: VPC-A
   c. Subnet 1 of 1 -> Subnet Name: VPC-A-Public, AZ: Select AZ 1, IPv4 CIDR block : 10.100.0.0/24) -> Create Subnet
   d. Select Subnet -> Actions -> Edit Subnet Settings - > Modify Auto-Assign IP Settings-> Enable -> Save
1. Create Route table
   a. Route Tables -> Create Route Table (Name: VPC-A-Public-RT, select VPC: VPC-A) -> Create route table
   b. Select Route table -> Routes -> Edit routes -> Add another route (Destination: 0.0.0.0/0, Target: Internet gateway -> igw-xxxxx) -> Save changes
5. Associate route table with the subnet
   a. Select Route table -> Subnet Associations -> Edit subnet associations -> Check the VPC-A-Public subnet -> Save associations

Steps

6. Launch EC2 instance in newly created Public Subnet
    a. Go to EC2 Service -> EC2 Dashboard -> Launch Instances
    b. Name: EC2-A
    c. Select Application and OS Images (Amazon Machine Image): Amazon Linux (default)
    d. Select instance type: t2.micro (default)
    e. Select key pair : *Your key-pair that you had created earlier in pre-requisites*
    f. Network settings -> Edit -> Select your VPC (VPC-A) and your public subnet
    g. Make sure Auto-Assign Public IP is enabled
    h. Firewall -> Create security group
        a. Name: EC2-A-SG
        b. Inbound Security group rule: Add rule (Type-> SSH, port Range-> 22, source type -> My IP
    i. Configure Storage -> 8GiB, gp3 (default)
    j. Launch Instance
7. Connect to EC2 instance with *Public IP* from your workstation using Putty or terminal with user *ec2-user*

Exercise – Private Subnet



Public Subnet Route table

Destination	Target
10.100.0.0/16	Local
0.0.0.0/0	igw-xxxxxx

Private Subnet Route table

Destination	Target
10.100.0.0/16	Local

Continuing with earlier setup

1. Create a new subnet in Availability zone 1 (as shown)
2. Create a new route tables and associate with Private subnet. (route entries as shown)
3. Launch EC2 instance (EC2-B) in the Private subnet. Make sure Security Group for EC2-B allows SSH and ICMP (ping) from VPC CIDR.
4. Connect to EC2-A over SSH. Ping to EC2-B Private IP.
5. Bring/copy SSH key onto EC2-A and change file permissions to 400
6. From EC2-A terminal SSH into EC2-B using ssh key file
7. Once logged into EC2-B, try to ping google.com or wget google.com

Steps

1. Create Private subnet
   a. Subnets -> Create subnet, Select VPC ID: VPC-A
   b. Subnet 1 of 1 -> Subnet Name: VPC-A-Private, AZ: Select AZ 1, IPv4 CIDR: 10.100.11.0/24) -> Create Subnet
2. Create a Route table for Private subnet
   a. Route Tables -> Create Route Table (Name: VPC-A-Private-RT, select VPC: VPC-A) -> Create route table
   b. Select Route table -> Subnet Associations -> Edit subnet associations -> Check the VPC-A-Private subnet -> Save associations
3. Launch EC2-B instance in the Private Subnet
   a. Go to EC2 Service -> EC2 Dashboard -> Launch Instances
   b. Name: EC2-B
   c. Select AMI: Amazon Linux (default)
   d. Select instance type: t2.micro (default)
   e. Select key pair : *Your key-pair that you had created earlier*
   f. Network settings -> Edit -> Select your VPC (VPC-A) and Private subnet (VPC-B-Private)
   g. Firewall -> Create security group
      a. Security Group Name: EC2-B-SG
      b. Inbound Security group rule: Add rule for SSH (port 22) for source type (Custom) Source as 10.100.0.0/16
      c. Add security group rule
      d. Inbound Security group rule: Add rule for ICMP IPv4 for source as 10.100.0.0/16 (Type: All ICMP –IPV4, Source type- Custom as 10.100.0.0/16
   h. Configure Storage -> 8GiB, gp3 (default)
   i. Launch Instance and wait for the instance to be in running state

Steps

4. From EC2-A instance, ping to EC2-B private IP using command:
   $ping 10.100.11.x
5. Create a key.pem on EC2-A using any editor. Paste .pem file content and save the file. Change file permissions to 400 using command:
   $chmod 400 key.pem
6. SSH to EC2-B using command:
   $ssh –i key.pem ec2-user@10.100.11.x
7. Try to access the internet using following commands:
   $ping google.com
   $wget https://google.com