Lab 3

1. **Create a Private subnet**
   a. Create subnet (Name: MyVPC-Private, VPC: MyVPC, AZ: Select different AZ (ap-southeast-2b), CIDR:10.100.1.0/24)
2. **Create Private route table**
   a. Route Tables => Create Route Table (Name: MyVPC-Private, VPC: MyVPC)
3. **Associate Route table with Subnet to make it Private subnet**
   a. Select Route table => Subnet Associations => Edit => Check the MyVPC-Private subnet => Save
4. **Launch another EC2 instance in the same VPC but in the newly created Private subnet.**
   a. Tag this instance with Name=EC2-DataBase
   b. New security group
      i. Add rule RDP for CIDR of Public Subnet source CIDR
      ii. Add rule All-ICMP IPv4 for Public Subnet source CIDR
5. **Note down EC2-DataBase instance private IP address**
6. **Try to ping EC2-B Private IP from EC2-A instance => Should work**
7. **Try to ping google.com from EC2-B instance**
   a. ping google.com (You should not be able to ping. Why?)
8. **Create a NAT Gateway in your VPC (when you finish the Lab delete this Gateway to avoid any cost.)**
   a. VPC => NAT Gateways => Create NAT Gateway
      i. Subnet: MyVPC-Public (Must select Public Subnet)
      ii. EIP: Create New EIP
      iii. Create NAT Gateway
      iv. It takes 5-10 minutes for NAT Gateway to be Active
9. **Add a route in Private subnet for internet traffic and route through NAT Gateway**
   a. Route Tables => Select MyVPC-Private route table
   b. Routes => Edit => Add another route
      i. Destination: 0.0.0.0/0
      ii. Target: nat-gateway
      iii. Save
10. **Now again try to ping google.com from EC2-B**
11. **ping google.com**

steps to create an inbound rule for ICMP traffic in Windows Firewall:

1. Open the Windows Firewall with Advanced Security management console by typing "wf.msc" into the Start menu or Run dialog box.
2. In the console, click on "Inbound Rules" in the left-hand pane.
3. Click on "New Rule" in the right-hand pane to create a new inbound rule.
4. In the "New Inbound Rule Wizard," select "Custom" as the rule type, and click "Next."
5. Select "All Programs" as the protocol type, and click "Next."
6. In the "Scope" section, select "Any IP address" for the remote IP address, and click "Next."
7. In the "Protocol and Ports" section, select "ICMPv4" as the protocol type, and click "Next."
8. In the "Action" section, select "Allow the connection," and click "Next."
9. In the "Profile" section, select the appropriate profile(s) for the rule, and click "Next."
10. In the "Name" section, enter a name for the rule (e.g., "Allow ICMP"), and click "Finish.