Cloud Challenge Details

In this lab challenge, your Amazon VPC and Amazon EC2 skills are put to the test. You'll be given a requirement and you must reach it using your knowledge of Amazon VPC and other AWS services. The Lab Challenge helps you understand the real-time scenarios.

A company ABC launches two EC2 Instances, one to deploy a web application in Public subnet and the other to host another application in Private subnet. As a part of the infrastructure, they need internet access to Private Instance but secured. Now you are a Security Engineer, and your challenge is to build the entire Infrastructure from scratch so, that the dev team can host their application in both EC2 Instances.

Follow the below instructions to complete this challenge.

1. Create an Amazon VPC named **MyVPC** with IPv4 CIDR: **10.17.0.0/16** and **No** IPv6 CIDR.
2. Create Public and Private Subnets in MyVPC with IPv4 CIDR **10.17.0.0/24** and **10.17.1.0/24** Respectively.
3. Enable auto-assign public IPv4 address to Public subnet.
4. Create an Internet gateway named **MyIGW** and attach it to **MyVPC**
5. Create a **Public Route table** in MyVPC and add **Internet Gateway** public route in it.
6. Associate the Public Subnet to the Public route Table.
7. Launch an **MyPublicEC2Server Instance** in **Public Subnet** with the following configuration:
    0. Select Amazon Linux 2 AMI
    1. Select t2.micro instance type
    2. Create 8GB gp2 EBS Volume.
    3. Select MyVPC and MYPublicSubnet and Enable Auto-assign Public IP
    4. Create a new security group MyEC2Server_SG and add SSH port with source Anywhere.
    5. Create a new Key Pair for the Public EC2 Instance.

8. Launch an **MyPrivateEC2Server Instance** in **Private Subnet** with the following configuration:
    0. Select Amazon Linux 2 AMI
    1. Select t2.micro instance type
    2. Create 8GB gp2 EBS Volume.
    3. Select MyVPC and MYPrivateSubnet and Disable Auto-assign Public IP
    4. Select the Security Group created for first instance.
    5. Create a new Key Pair for the Private EC2 Instance.
9. SSH into **Public EC2 Instance** and test Internet Connectivity.
10. To Perform SSH operation
    - Windows Users use **Putty Software**.
    - Linux/Mac Users use **Terminal**.
11. First SSH into **Public EC2 Instance.**
12. Next SSH into **Private EC2 Instance** from **Public EC2 Instance** and run the following Linux commands in **Private EC2 Instance**. (Since no internet access is provided for Private EC2 instances, you will not be able to run the bellow)
    0. **yum -y update**
    1. **yum install httpd -y**
13. Create a **MyNATGateway *in* Public** Subnet of VPC **MyVPC** to provide Internet access to the private instance.
14. Update the **Main** Route table (which is different from one created by you) and Add **NAT Gateway** public Route.
15. Now again **SSH** into **Public EC2** Instance and then SSH into **Private EC2** instance from Public EC2 instance.
16. ***MyNATGateway***Run the below Linux commands in the **Private EC2 Instance**.
    0. **yum -y update**
    1. **yum install httpd -y**
17. If You can install httpd in Private Instance, you have completed this Challenge.