Cloud Architect, Cloud Network Engineer, Cloud Security Engineer, Cloud Administrator

Networking

**Lab Details**

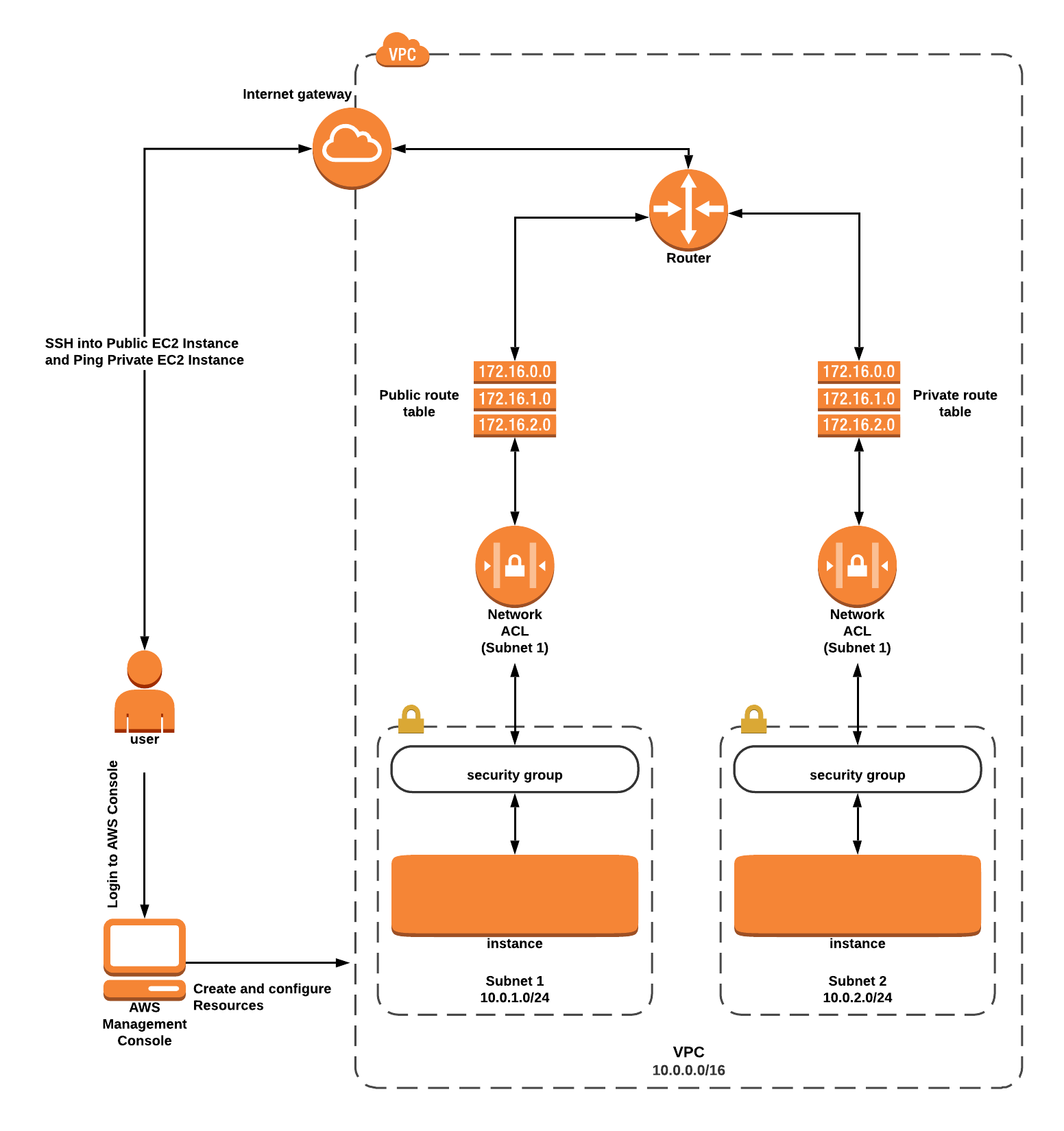
1. This lab walks you through the steps to Configure Multi-layered Security in AWS VPC and to launch 2 EC2 instances (one in a public subnet and another in a private subnet)
2. You will practice it using Amazon VPC, Amazon EC2
3. Duration: **1 Hour**
4. AWS Region: **US East (N. Virginia) us-east-1**

**Introduction**

Amazon Virtual Private Cloud

1. Amazon VPC allows us to launch **AWS resources in an isolated network** that is defined by us in a **more private and secure environment.**
2. This feature enables us to **increase the security level** of the AWS resources.
3. The AWS resources can be protected using **multilayered VPC** which includes **security groups** and **Network Access Control list**.
4. The VPC **security group** provides security at **instance level** which acts like a firewall and controls both inbound and outbound traffic.
5. The VPC **NACL** provides security at **Network Level** i.e **subnet level** which acts like a firewall for associated subnets and controls inbound and outbound traffic.

**Architecture Diagram**



**Task Details**

1. Sign in to AWS Management Console
2. Create a new VPC.
3. Create and attach an Internet Gateway.
4. Create two Subnets.
5. Create Route Tables, configure routes, and associate them with Subnets.
6. Create a Security Group.
7. Create and configure Network ACL.
8. Launch 2 EC2 Instances.
9. Test the EC2 Instances.

**Launching Lab Environment**

1. To launch the lab environment, Click on the  button.
2. Please wait until the cloud environment is provisioned. It will take less than a minute to provision.
3. Once the Lab is started, you will be provided with **IAM user name**, **Password**, **Access** **Key**, and **Secret** **Access** **Key**.

Submit Feedback