Lab description

In this lab, you will design a VPC with a **public subnet, a private subnet**, and a Network Address Translation (NAT) device in the public subnet.

A **NAT device** enables instances in the private subnet to initiate outbound traffic to the Internet. This scenario is common when you have a public-facing web application while maintaining back-end servers that aren't publicly accessible.

A common example is a multi-tier website, with the web servers in a public subnet, and the database servers in a private subnet. You can set up security and routing allowing the web servers to communicate with the database servers. The instances in the public subnet can send outbound traffic directly to the Internet, whereas the instances in the private subnet cannot. The instances in the private subnet can access the Internet via the NAT Gateway in the public subnet. In this Lab, you will also increase the network security using a network access control list (NACL), which is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet. After completing this Lab, you might consider setting up network ACLs with rules similar to your security groups, in order to add an additional layer of security to your VPC.

Learning Objectives

Upon completion of this lab you will be able to create, configure and test the following:

- Virtual Private Cloud (VPC)
- Internet Gateway
- Public and private subnets (inbound/outbound rules)
- Security groups (inbound/outbound rules for multiple purposes)
- Network access control lists (NACLs) for additional security on a private subnet
- Bastion host for SSH access from the internet to private instances
- Network Address Translation (NAT) Gateway to provide private instances access to the public internet to perform operating system updates
- Route tables associated with public and private subnets

Intended Audience

- Candidates for the AWS Cloud Practitioner Exam

- Candidates for the AWS Solutions Architect Associate Exam

Prerequisites

You should be familiar with:

- Elastic Cloud Compute (EC2) basics
- Conceptual understanding of Virtual Private Clouds (VPCs), subnets, network route tables, firewalls, private and public IP addresses
- Some Linux shell/command level understanding is helpful, but not required