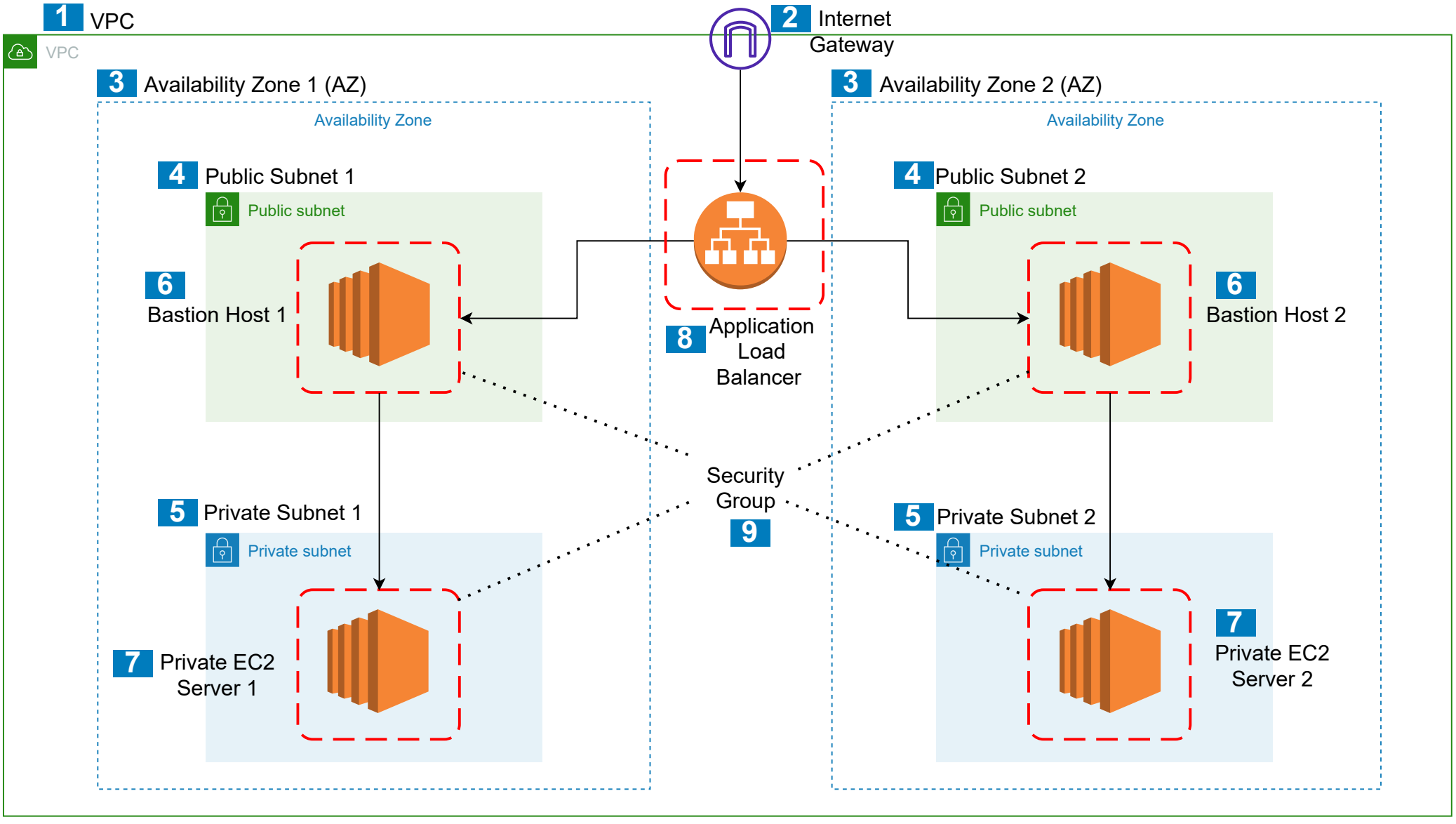
AWS Security - Cloud Computing Project

By Nikhil Amin



1. **VPC (Virtual Private Cloud):**
VPC is a virtual network where various AWS resources can be created and managed in a more secure and scalable manner. In this project, the entire infra is inside a VPC named "VPC-Nik".

2. **Internet Gateway:**
This component allows communication between the resources in the VPC and the internet.

3. **Availability Zone (AZ)**
AZs are logical data centres within a region. In this project, 2 identical set of resources are created in 2 different AZs in order to provide redundancy and isolation, in case one of the AZs fail.

4. **Public Subnet**
Public Subnets are accessible from the internet. The EC2 instance inside the public subnet called the Bastion Host can be accessed from the internet via the Application Load Balancer (ALB).

5. **Private Subnet**
Private Subnets cannot be accessed directly from the internet. The EC2 instance inside the private subnet can only be accessed by the Bastion Host (which is inside the Public Subnet) via SSH connection.

6. **Bastion Host**
The Bastion Host is actually an internet facing EC2 Instance that sits inside a Public Subnet. It is accessible from the internet via the Load Balancer.

7. **Private EC2**
Private EC2 instance is not accessible from the internet directly. This server can only be accessed by the Bastion Host via the SSH connection.

8. **Application Load Balancer (ALB)**
The ALB's primary function is to evenly distribute load among the EC2 instances. It is connected directly with the Internet Gateway. The Bastion Host inside the Public Subnet can only access traffic coming from the ALB.

9. **Security Group**
Each EC2 instance (Bastion Host & Private EC2) and also the ALB has an associated Security Group. The Security Group of the Bastion Host only allows inbound access from the Security Group of the ALB via HTTP protocol. The Security Group of the Private EC2 only allows inbound access from the Security Group of the Bastion Host via SSH.

Project Infrastructure

The Project Infrastructure was created using the CloudFormation Service via YAML code and few of the services were created via the Management console (EC2 & ALB).

Security Features

1. Subnet Bifurcation into Public and Private Subnets
The EC2 instance (Bastion Host) in the Public Subnet can be accessed from the Internet whereas the Private Subnet instances can only be accessed via SSH connection by the Bastion Host only.

2. Application Load Balancer
Usage of Application Load Balancer not only to distribute the internet traffic but also to provide availability as it connects to the EC2 instances (Bastion Hosts) in 2 different Availability Zones. Moreover, the Security Group of the ALB can be updated to provide access to only a particular IP Address from the internet.

Associated Resource Names in the AWS Console:-

VPC (Virtual Private Cloud) - VPC-Nik"

Internet Gateway - IGW_Nik

Public Subnet - PublicSubnet1_Nik & PublicSubnet2_Nik

Public Subnet - PrivateSubnet1_Nik & PrivateSubnet2_Nik

Bastion Host - BastionHost1 & BastionHost2

Private EC2 - Pvt1-EC2-Nik & Pvt2-EC2-Nik

Application Load Balancer - ALB-Nik

Security Group -
SG_BastionHost1_Nik & SG_BastionHost2_Nik : Bastion Hosts
VPC-Nik-WebServerSecurityGroup : Private EC2 Instance
ALB_SecurityGroup_Nik : ALB