VPC with Public and Private Subnets on AWS

Description

This project demonstrates how to create a custom Virtual Private Cloud (VPC) with public and private subnets. The setup includes Internet Gateway, NAT Gateway, and route tables for secure and controlled network traffic flow.

AWS Services Used

- Amazon VPC
- Subnets (Public & Private)
- Internet Gateway
- NAT Gateway
- Route Tables
- Elastic IP
- Security Groups

Instructions

1. Create a VPC

- CIDR block: 10.0.0.0/16

2. Create Subnets

- Public Subnet: 10.0.1.0/24 (AZ-a)
- Private Subnet: 10.0.2.0/24 (AZ-a)

3. Create and Attach an Internet Gateway

- Attach the IGW to the VPC

4. Create Route Tables

- Public Route Table: Add route to 0.0.0.0/0 via IGW
- Associate with Public Subnet

5. NAT Gateway

- Allocate Elastic IP
- Create NAT Gateway in Public Subnet
- Create Private Route Table: Add route to 0.0.0.0/0 via NAT Gateway
- Associate with Private Subnet

6. Launch EC2 Instances

- Public EC2 in public subnet (e.g., for bastion or web server)
- Private EC2 in private subnet (e.g., for database or app backend)
- Use Security Groups to restrict access

Diagram

See architecture diagram included in this project.

Author

Ebenezer Gbormittah

Architecture Diagram