Project Report: Bastion Host-Based Connectivity to Private EC2 Instance on AWS

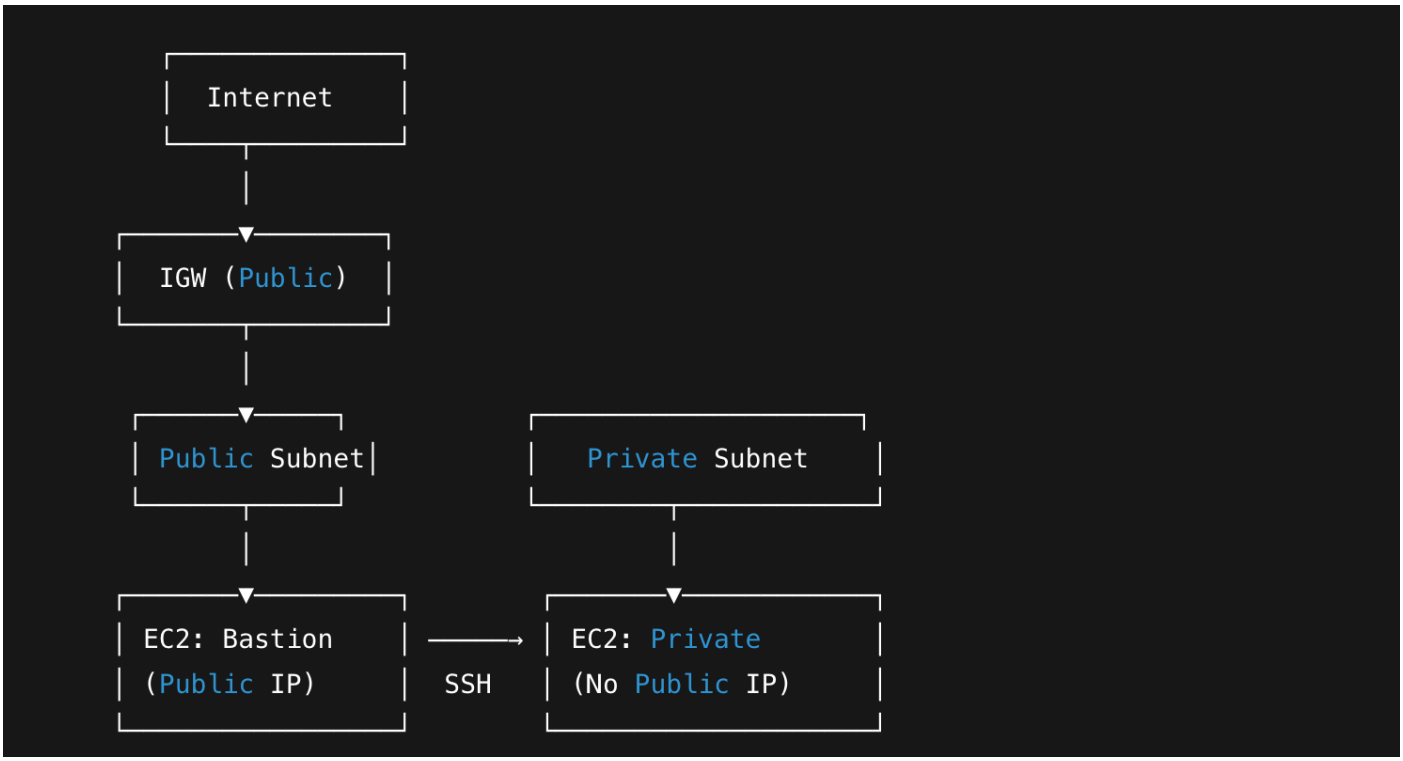
Objective

To enable SSH access to a private EC2 instance (deployed in a private subnet) using a public EC2 instance (Bastion Host), ensuring secure network design using AWS networking components.

Key Concepts & Services Used

- **Amazon VPC (Virtual Private Cloud)**
- **Subnets (Public and Private)**
- **Internet Gateway (IGW)**
- **NAT Gateway**
- **Route Tables**
- **EC2 Instances (Bastion + Private)**
- **Security Groups**
- **SSH Key Management**

Architecture Overview



Steps Implemented

1. VPC Setup

- **Created a custom VPC with a CIDR block 10.0.0.0/16.**

2. Subnets

- **Public Subnet: 10.0.1.0/24 for the Bastion Host.**
- **Private Subnet: 10.0.2.0/24 for the private EC2 instance.**

3. Internet Gateway (IGW)

- **Attached to the VPC to provide internet access to the public subnet.**

4. NAT Gateway

- **Created in the public subnet to allow outbound internet access from the private subnet.**

5. Route Tables

- **Public Route Table:**
  - **Subnet association: Public Subnet**
  - **Route: 0.0.0.0/0 → IGW**
- **Private Route Table:**
  - **Subnet association: Private Subnet**
  - **Route: 0.0.0.0/0 → NAT Gateway**

6. EC2 Instances

- **Bastion Host:**
  - **Launched in Public Subnet with a public IP.**
  - **Inbound SSH access allowed (Port 22).**
- **Private EC2:**
  - **Launched in Private Subnet without a public IP.**
  - **Inbound SSH allowed only from the Bastion Host's security group.**

7. Security Groups

- **Bastion Host SG:**
  - **Inbound: Port 22 from your IP**
- **Private EC2 SG:**
  - **Inbound: Port 22 from Bastion Host SG**

SSH Access Procedure

1. **SSH into the Bastion Host using:**

   ssh -i "key.pem" ec2-user@<bastion-public-ip>

2. **From inside the Bastion:**

   ssh -i "key.pem" ec2-user@<private-ec2-private-ip>