
Cloud Network & Access Control Architecture for Internal Application

Role: Cloud Network & Security Intern
Cloud Provider: AWS
Region: ap-south-1 (Mumbai)

---

1. Objective

The goal of this project is to design a **secure cloud network architecture** that allows employees to access an internal application while protecting it from external threats.
The solution must:

- Restrict public exposure
- Enforce network segmentation
- Allow access only through defined ports
- Use basic firewall and security group rules (no IDS/IPS)

---

2. High-Level Architecture Overview

Architecture Pattern Used:
Public Subnet + Bastion Host + Private Application Subnet

Access Flow:

User Laptop

↓ (SSH)

Bastion Host (Public Subnet)

↓ (SSH / App Port)

Application Server (Private Subnet)

This ensures:

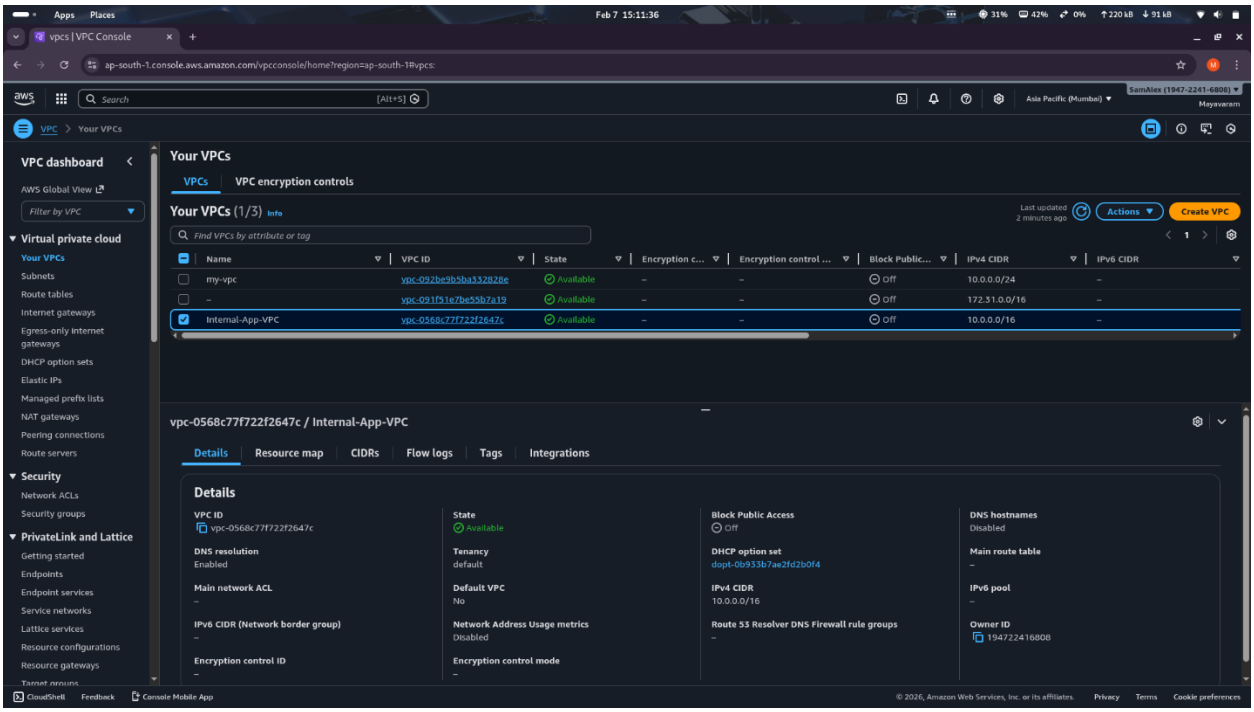
- No direct public access to the application server
- A single controlled administrative access path
- Least-privilege network access

3. VPC Design

3.1 Virtual Private Cloud (VPC)

- **VPC Name:** Internal-App-VPC
- **CIDR Block:** 10.0.0.0/16
- **DNS Resolution:** Enabled
- **DNS Hostnames:** Enabled

Purpose:
Provides isolated networking for the internal application and administrative resources.



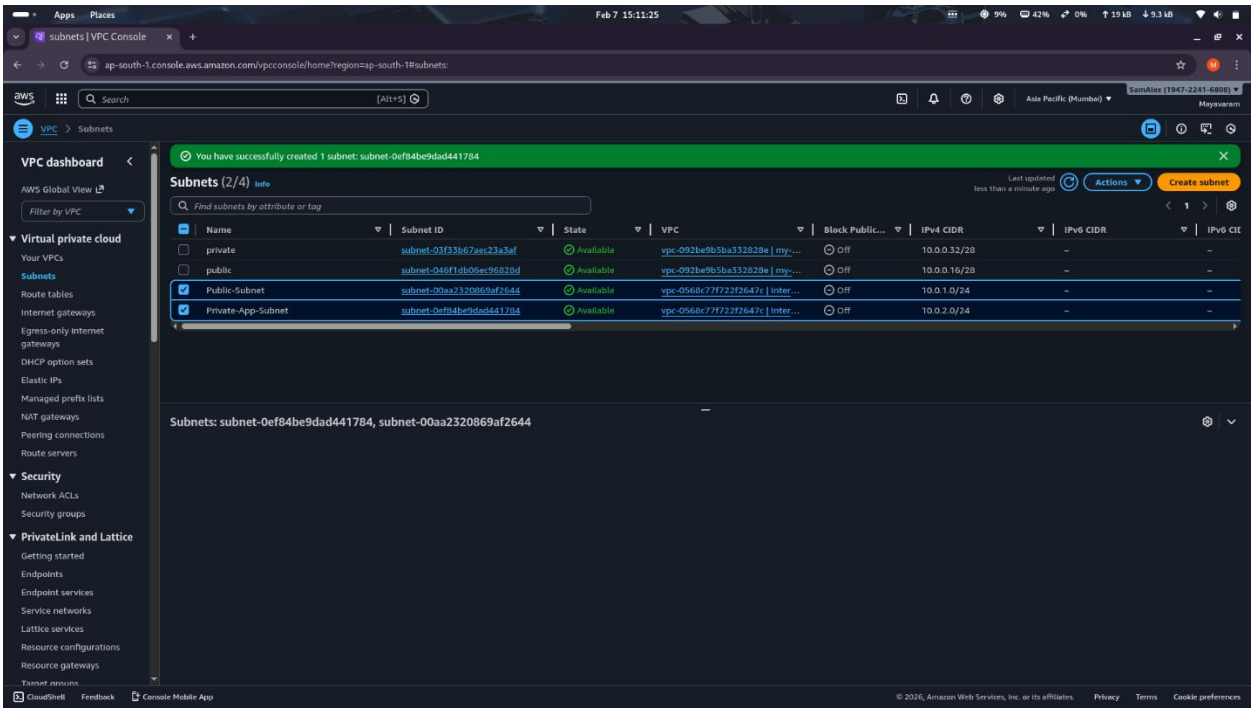
4. Subnet Design & Segmentation

4.1 Public Subnet

- **Subnet Name:** Public-Subnet
- **CIDR:** 10.0.1.0/24
- **Purpose:** Hosts the Bastion Host
- **Internet Access:** Yes (via Internet Gateway)

4.2 Private Application Subnet

- **Subnet Name:** Private-App-Subnet
- **CIDR:** 10.0.2.0/24
- **Purpose:** Hosts internal application server
- **Internet Access:** No direct internet access



✓ This satisfies **network segmentation** and **internal-only application hosting**.

---

5. Internet Gateway & Routing

5.1 Internet Gateway (IGW)

- Attached to **Internal-App-VPC**
- Used only by the public subnet

5.2 Route Tables

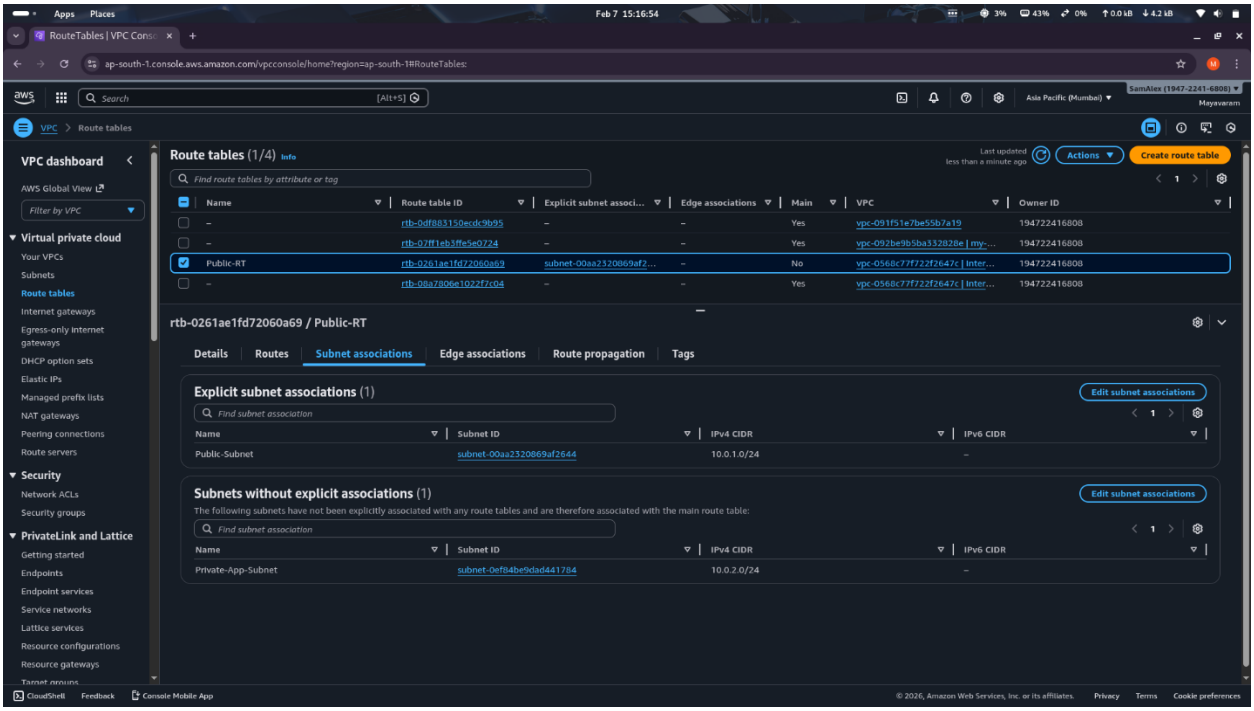
Public Route Table (Public-RT)

- 10.0.0.0/16 → local

- 0.0.0.0/0 → Internet Gateway
- Associated with **Public-Subnet**

Private Route Table (Private-RT)

- 10.0.0.0/16 → local
- **No route to Internet Gateway**
- Associated with **Private-App-Subnet**



✓ This ensures **private subnet isolation**.

---

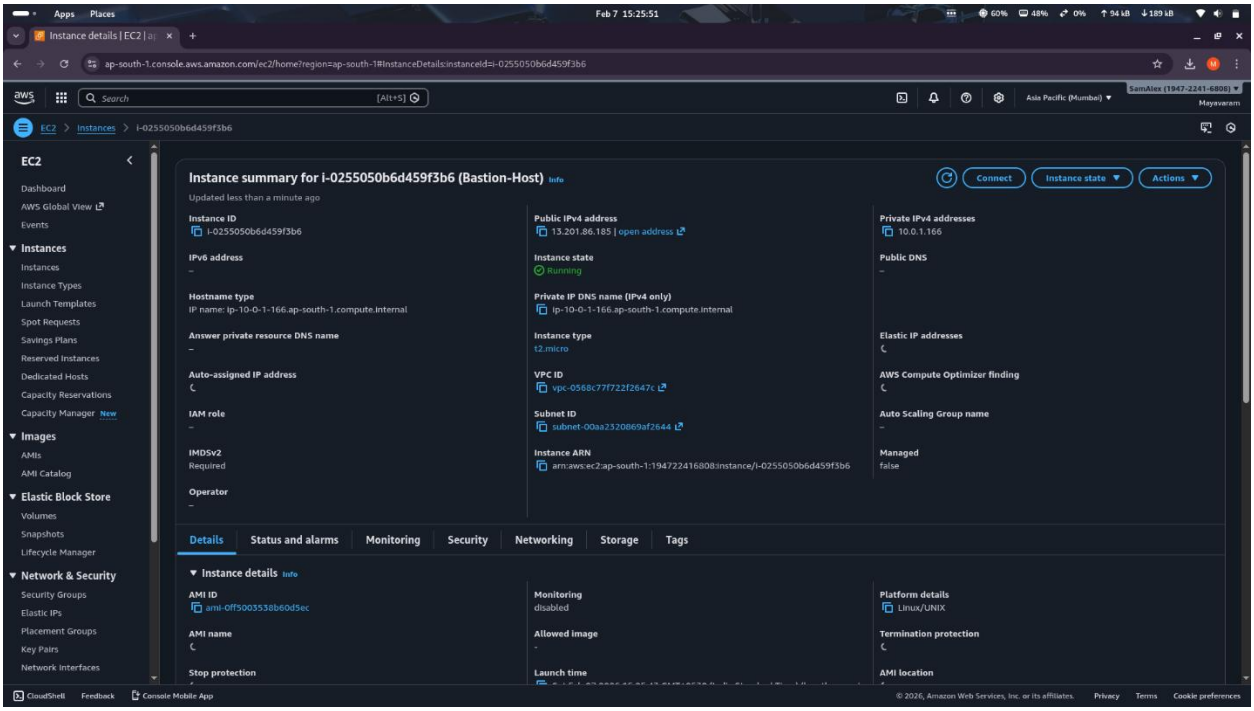
6. EC2 Instances

6.1 Bastion Host

- **Subnet:** Public-Subnet
- **Public IP:** Assigned
- **Private IP:** 10.0.1.166
- **OS:** Amazon Linux 2023

Purpose:

Acts as the **only administrative entry point** into the private network.



6.2 Application Server

- **Subnet:** Private-App-Subnet
- **Public IP:** None
- **Private IP:** 10.0.2.10

Purpose:

Hosts the internal application and is **not directly accessible from the internet**.

---

7. Security Groups (Firewall Rules)

7.1 Bastion Host Security Group

Inbound Rules:

- SSH (22) → Allowed from **Admin Public IP only**

Outbound Rules:

- All traffic allowed (default)

Security Benefit:

Prevents open SSH access from the internet.

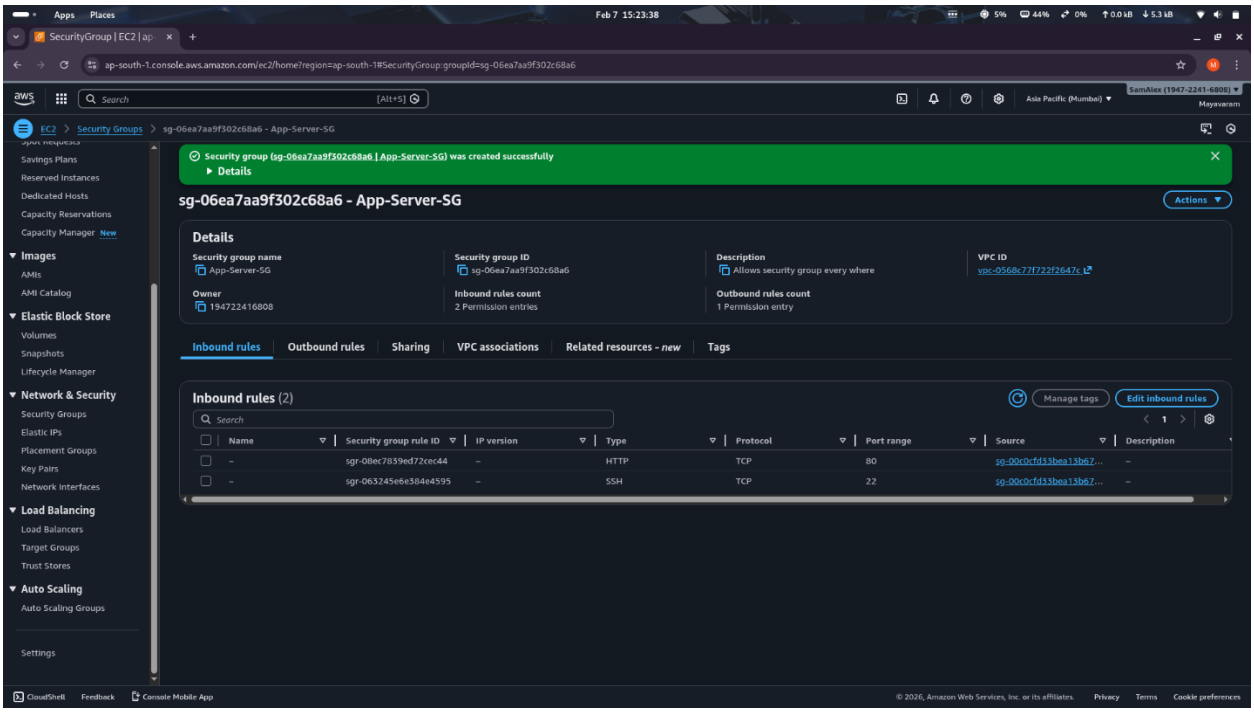
7.2 Application Server Security Group (App-Server-SG)

Inbound Rules:

- SSH (22) → Allowed **only from Bastion Host Security Group**
- HTTP (80) → Allowed **only from Bastion Host Security Group**

Outbound Rules:

- All traffic allowed (default)



✓ This enforces **defined ports only** and **restricted access paths**.

---

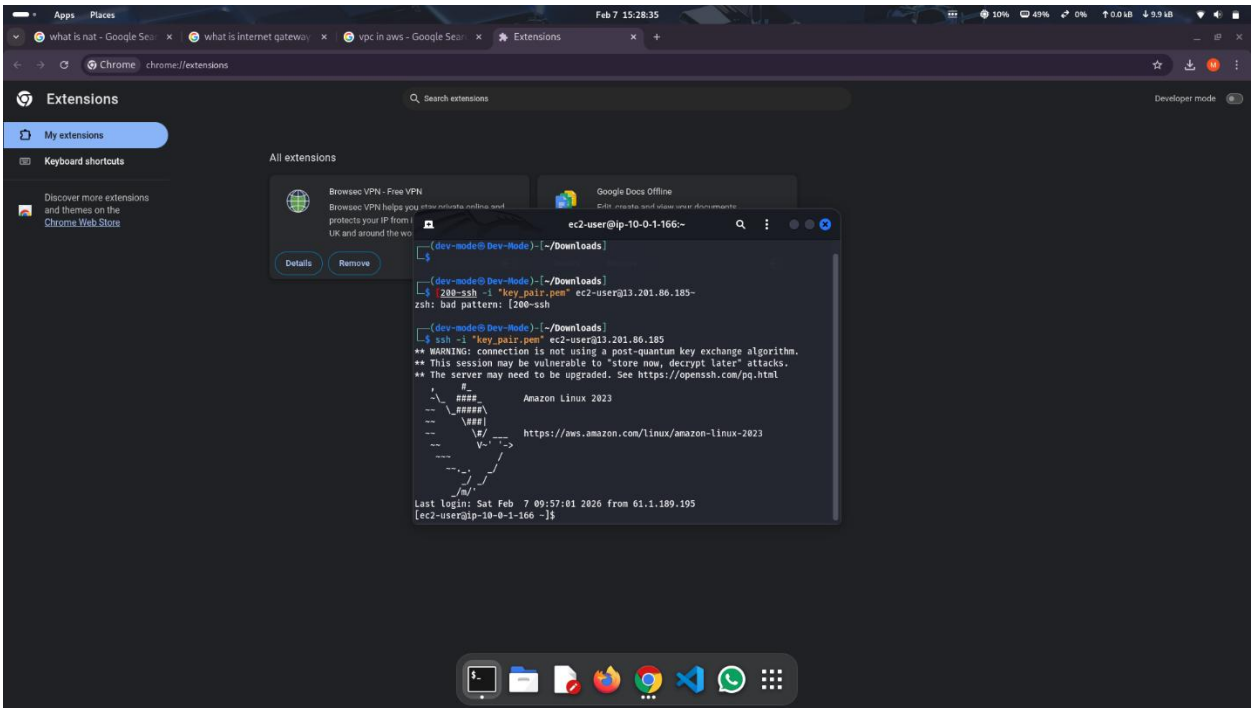
8. Access Method (Important for Submission)

Step 1: SSH to Bastion Host

ssh -i "key_pair.pem" ec2-user@<Bastion_Public_IP>

Step 2: From Bastion → Application Server

ssh ec2-user@10.0.2.10



✓ Confirms **one administrative access path**.

---

9. Simulated Common Mistakes & Corrections

Mistake 1: Opening SSH (22) to 0.0.0.0/0

❌ Risk: Anyone on the internet could attempt access

✓ Fix: Restricted SSH to admin IP and Bastion SG only

Mistake 2: Public IP on Application Server

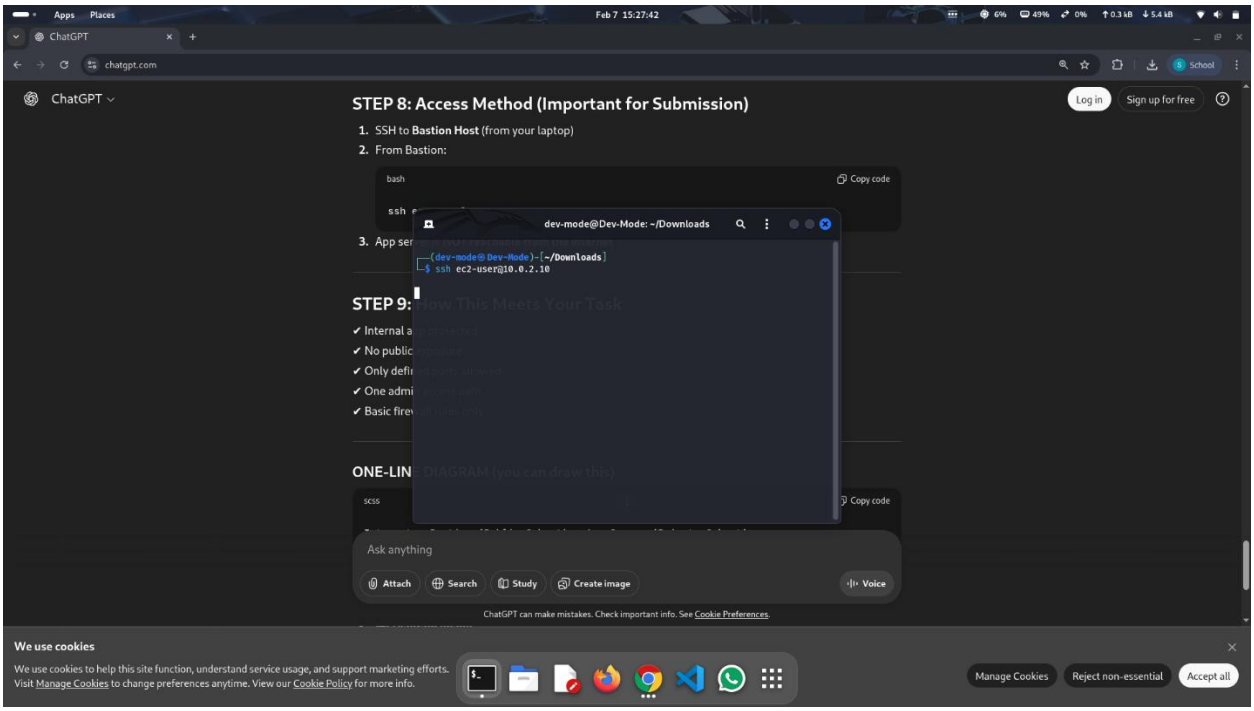
❌ Risk: Direct external exposure

✓ Fix: Removed public IP and placed instance in private subnet

Mistake 3: Internet Gateway Route on Private Subnet

❌ Risk: Unnecessary internet exposure

✓ Fix: Used separate private route table without IGW



---

10. How This Meets Task Requirements

✓ Internal application protected

✓ No direct public exposure

✓ Network segmentation using subnets

✓ Only defined ports allowed

✓ One administrative access path (Bastion Host)

✓ Basic firewall & security group rules only

✓ Fully documented and diagrammable

11. Final Architecture Diagram (Textual)

Internet

|

[Internet Gateway]

|

[Public Subnet]

|

[Bastion Host]

|

[Private App Subnet]

|

[Application Server]