Secure Web App in Private Subnet – Access via Admin EC2

Objective

Deploy a **private web application** on an EC2 instance in a **private subnet**, which is **not accessible from the internet**, and access it **securely via a bastion (admin) EC2** in a **public subnet**.

Architecture Overview

- **VPC:** 10.0.0.0/16
- **Admin Subnet (Public):** 10.0.1.0/24
- **Private Subnet:** 10.0.2.0/24
- **Admin EC2 (Public):** Can SSH from the internet
- **Private EC2:** No public IP, can only be accessed from Admin EC2
- **Security Groups:**
    - Admin SG: Allows inbound SSH from anywhere
    - Private SG: Allows SSH & HTTP from Admin SG only
- **Apache Web Server:** Installed on Private EC2

Tools Used

- **AWS CloudFormation**
- **Amazon EC2**
- **Security Groups**
- **VPC & Subnets**
- **Apache Web Server**
- **SSH Port Forwarding**

1.Steps Performed

Launch Infrastructure via CloudFormation

- Used CloudFormation template to:
    - Create VPC, subnets, route tables, IGW
    - Launch Admin EC2 (public subnet) & Private EC2 (private subnet)
    - Set security groups for controlled access

Template included UserData to auto-install Apache on the private EC2.

2. SSH into Admin EC2

ssh -i "real.pem" ubuntu@<Admin_EC2_Public_IP>

Success: Accessed admin instance in public subnet.

3. SSH into Private EC2 from Admin EC2

ssh ubuntu@<Private_EC2_IP>

Success: Accessed private instance via internal IP.

4. Access Private Web App in Browser using SSH Port Forwarding

ssh -i "real.pem" -L 8080:<Private_EC2_IP>:80 ubuntu@<Admin_EC2_Public_IP>

In browser:

http://localhost:8080

Output: HTML page from private EC2 shown in browser via SSH tunnel.

Security Considerations

- Private EC2 has **no public IP**
- Only Admin EC2 can access private EC2 via SSH or HTTP
- Public SSH access is **restricted to Admin EC2 only**
- Apache runs internally, not exposed to the world

Outputs from CloudFormation

- Admin EC2 Public IP
- Private EC2 Instance ID