(1). Create a VPC with one public and two private subnets across two AZs, attach an IGW and NAT Gateway, associate route tables, and validate reachability.

1. VPC Creation

Created MyVPC with CIDR block `10.0.0.0/16`.

2. Subnets Setup

Public Subnet: `public-a` → `10.0.0.0/24` (AZ-A).

Private Subnet 1: `private-a` → `10.0.1.0/24` (AZ-A).

Private Subnet 2: `private-b` → `10.0.2.0/24` (AZ-B).

3. Internet Gateway

Created and attached `My-Internet-Gateway` to `My-VPC`.

4. Route Tables

`rtb-public`: Associated with `public-a`, route `0.0.0.0/0 → IGW`.

`rtb-private`: Associated with `private-a` and `private-b`, route `0.0.0.0/0 → NAT`.

5. NAT Gateway

Created NAT Gateway `My-NAT-Gateway` in `public-a` with Elastic IP.

Verified private subnets route through this NAT for internet egress.

6. Security Groups

`sg-1`: SSH allowed from my IP.

`sg-private`: SSH allowed only from SG,1 outbound all allowed.

7. EC2 Validation

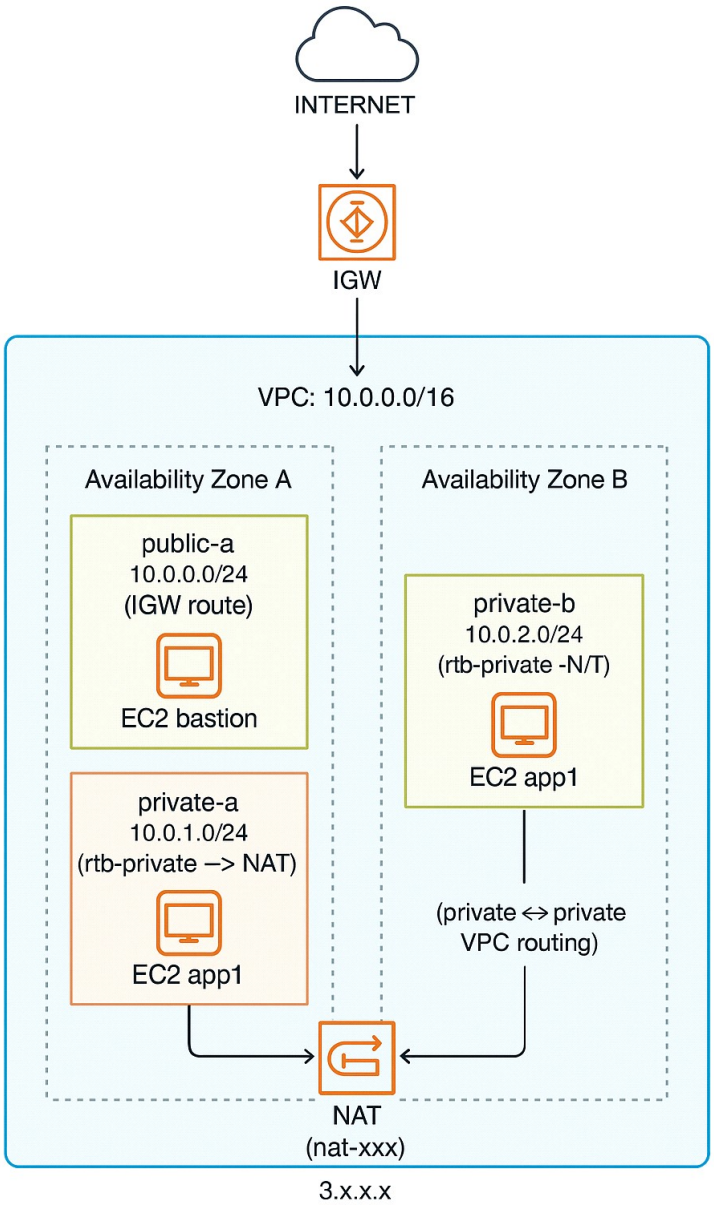
Launched Bastion Host in `public-a` with public IP.

Launched two private EC2s in `private-a` and `private-b` (no public IPs).

Successfully SSH'd into bastion → then into private instances.

Verified internet connectivity (`curl example.com`) from private EC2s via NAT Gateway.

Confirmed no direct access to private instances from internet.



(2). Implement tiered security groups for web and app hosts and verify east-west and north-south flows with simple connectivity tests.

VPC Setup

Created VPC-Tiered with CIDR 10.1.0.0/16.

Subnets:

public-web (10.1.1.0/24, AZ-A)

private-app (10.1.2.0/24, AZ-A)

Internet & Routing

Created and attached IGW-Tiered.

Configured route tables:

rtb-public → 0.0.0.0/0 → IGW (for web subnet).

rtb-private → (optional NAT if outbound required for app).

Security Groups (Tiered)

sg-web (Web Tier):

Inbound: HTTP(80), HTTPS(443) from anywhere, SSH from my IP.

Outbound: allowed traffic to sg-app.

sg-app (App Tier):

Inbound: allowed only from sg-web.

Outbound: default (all allowed).

EC2 Deployment

Launched Web Server in public-web with public IP and sg-web.

Launched App Server in private-app without public IP and sg-app.

Connectivity Tests

 SSH to Web server from laptop → Success.

 HTTP access to Web server from internet → Success.

 SSH from Web server → App server private IP → Success.

 App accessible only from Web server, not from internet → Confirmed.

 Internet to App server directly → Blocked (expected)

(3). VPC Peering

Established a VPC Peering connection between two VPCs and test connectivity

Configured Route Tables for Connection peering and launched ec2s in diffrent vpcs to test connection.