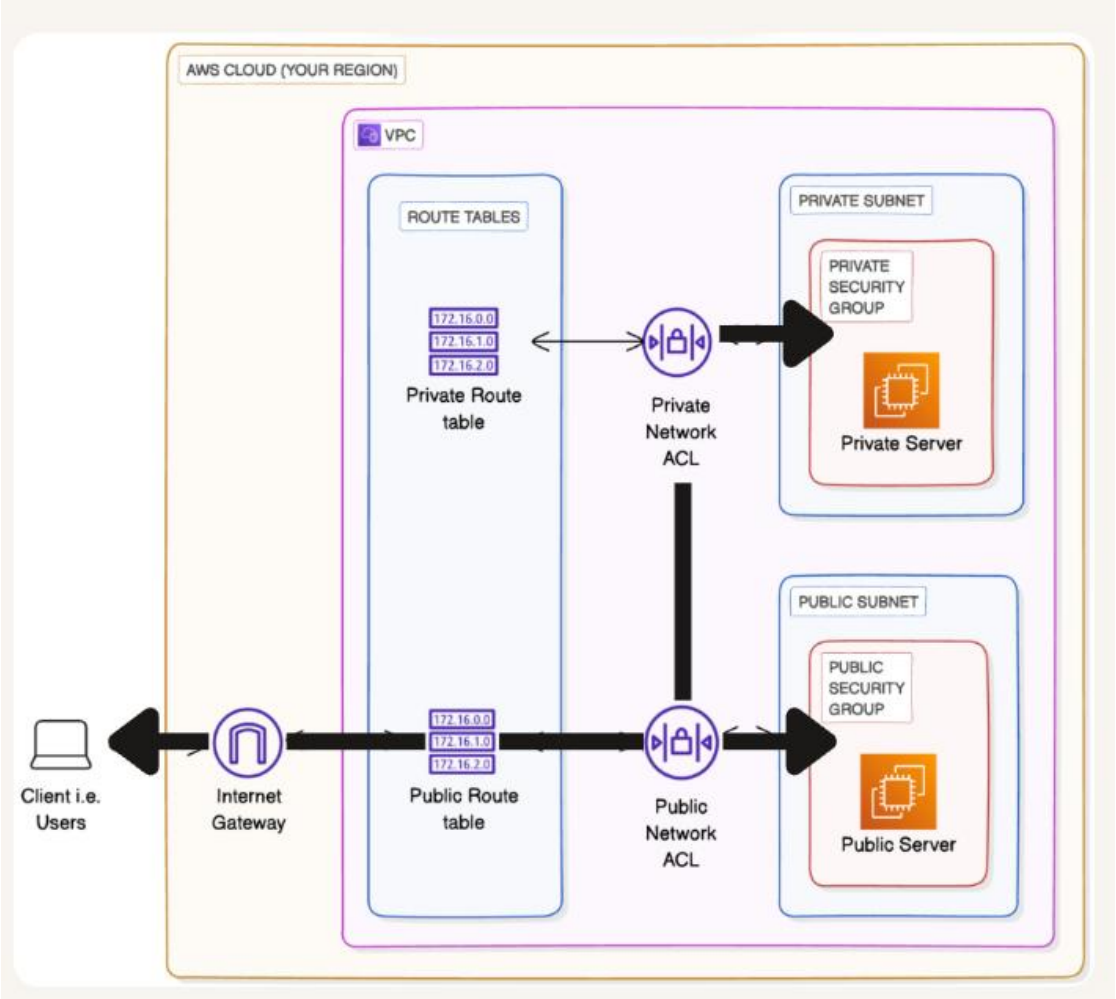
Project 1: VPC Architecture & Connectivity (Public + Private Subnets)



Objective: Build a secure VPC with public and private subnets, attach an Internet Gateway, configure route tables, NACLs, and Security Groups, launch EC2 instances, and validate connectivity.

Architecture

- VPC CIDR: 10.0.0.0/16
- Public Subnet: 10.0.0.0/24 (via Internet Gateway)
- Private Subnet: 10.0.1.0/24 (no IGW)
- Route Tables: Public RT → 0.0.0.0/0 to IGW; Private RT → local only
- Security Groups: Public SG (HTTP/SSH), Private SG (SSH from Public SG)
- Network ACLs: Public allow all; Private allow ICMP from 10.0.0.0/24
- EC2 Instances: 1 in Public Subnet (public IP), 1 in Private Subnet

Build Steps (Console)

- Create VPC (10.0.0.0/16) → "VPC and more" wizard.
- Create public subnet (10.0.0.0/24) & private subnet (10.0.1.0/24).
- Create & attach Internet Gateway to the VPC.
- Public Route Table → add route 0.0.0.0/0 → Internet Gateway; associate to Public Subnet.
- Private Route Table → associate to Private Subnet (no default 0.0.0.0/0).
- Create Security Groups:
- • Public SG: Inbound HTTP (80) + SSH (22) from 0.0.0.0/0; Outbound all.
- • Private SG: Inbound SSH (22) from Public SG; Outbound all.
- Network ACLs:
- • Public NACL: Allow inbound/outbound all.
- • Private NACL: Add inbound/outbound 'All ICMP - IPv4' from 10.0.0.0/24.
- Launch EC2
- • Public server in Public Subnet with auto-assign public IP Enabled (use EC2 Instance Connect).
- • Private server in Private Subnet without public IP.

Validate Connectivity

From the public instance (EC2 Instance Connect):

```
ping <private-ec2-private-ip>
curl example.com
```

Expectations:

- Public → Internet works via curl (IGW path).
- Public → Private ping works after NACL + SG rules.
- Private instance stays non-internet reachable (no IGW path).