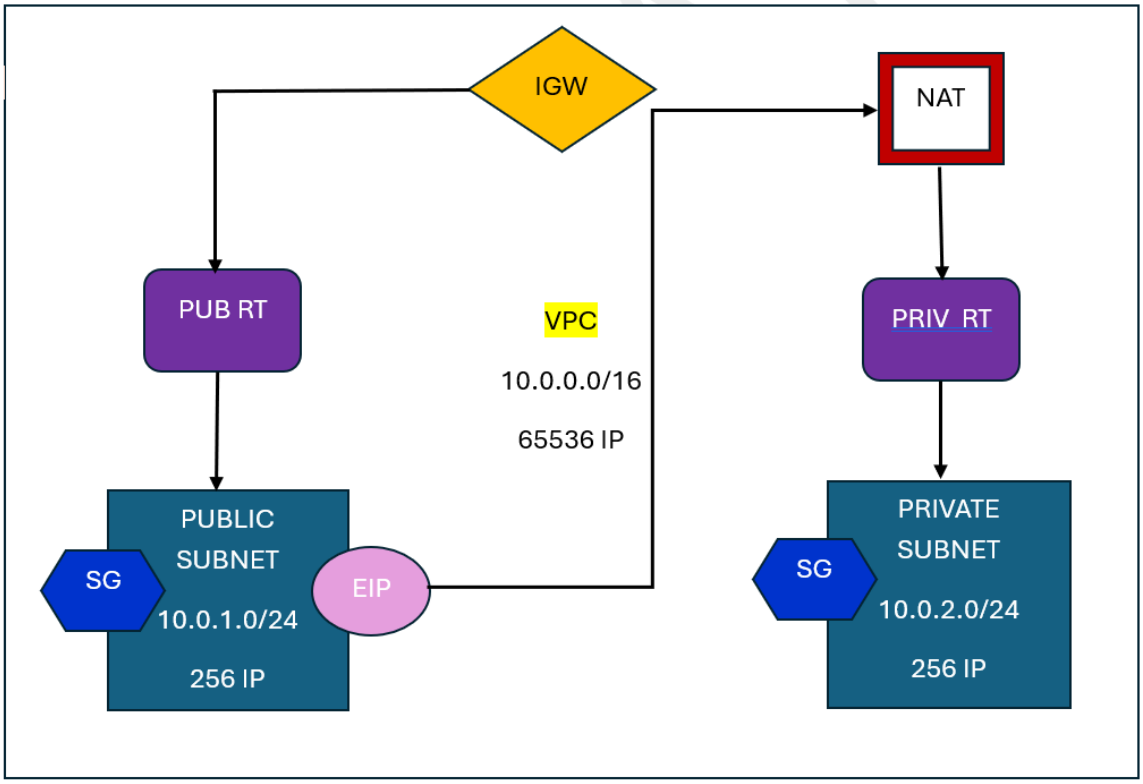
CUSTOM AWS VPC SETUP WITH PUBLIC AND PRIVATE SUBNETS FOR SECURE INFRASTRUCTURE

Project Summary:

This project demonstrates the setup of a custom Virtual Private Cloud (VPC) architecture in AWS, designed to support a scalable, secure network infrastructure for a retail-based application. The scenario assumes a retail company launching a new e-commerce platform that requires both internet-facing services (such as a web front end) and backend systems (like inventory management) hosted in a private environment.

To meet these requirements, I created a VPC with a /16 CIDR block, subdivided into a public and a private subnet, each with 256 IPs. The public subnet is configured with an Internet Gateway to enable external access, while the private subnet is secured and connected via a NAT Gateway for controlled outbound internet access. Route tables and security groups were configured accordingly. I deployed EC2 instances in both subnets and enabled secure access to the private instance using AWS Systems Manager (SSM), ensuring a fully functional and secure environment for the retail application's infrastructure.

Note: The project replicates a real-world VPC setup delivered for a retail client. While the configuration mirrors the original environment, sensitive client details have been omitted in this portfolio for privacy reasons.



Step-by-Step Implementation

1. **VPC Creation**

- Navigate to AWS Console → VPC → Create VPC
- Choose VPC only
- Name: Project-A
- IPv4 CIDR Block: 10.0.0.0/16
- Tenancy: Default
- Click Create VPC

2. **Subnets**

- **Public Subnet:**
  - Name: Public-Subnet-Project-A
  - CIDR: 10.0.1.0/24
  - Availability Zone: ap-south-1a

- **Private Subnet:**

    - Name: Private-Subnet-Project-A
    - CIDR: 10.0.2.0/24
    - Availability Zone: ap-south-1b

3. **Internet Gateway**

- Go to VPC → Internet Gateway → Create
- Name: IGW-Project-A
- Attach to the VPC Project-A

4. **Route Tables**

- **Public Route Table:**
    - Name: Public-RT-Project-A
    - Associate with Public Subnet
    - Add route: 0.0.0.0/0 → IGW-Project-A
- **Private Route Table:**
    - Name: Private-RT-Project-A
    - Associate with Private Subnet
    - Will be configured with NAT in later steps

5. **Security Groups**

- **Public SG:**
    - Name: Public-SG-Project-A
    - Inbound: Allow SSH (22), HTTP (80), HTTPS (443), RDP (3389)
    - Outbound: Allow All Traffic
- **Private SG:**
    - Name: Private-SG-Project-A
    - Inbound: Allow All TCP from Public SG
    - Outbound: Allow All Traffic

6. **Launch EC2 Instances**

- **Public EC2:**
    - AMI: Amazon Linux 2

- Network: Project-A
- Subnet: Public Subnet
- Auto-assign Public IP: Enabled
- Security Group: Public-SG-Project-A

- **Private EC2:**
  - AMI: Amazon Linux 2
  - Network: Project-A
  - Subnet: Private Subnet
  - Auto-assign Public IP: Disabled
  - Security Group: Private-SG-Project-A

7. **Configure NAT Gateway**

- Go to NAT Gateway → Create
- Name: NAT-Project-A
- Subnet: Public Subnet
- Elastic IP: Allocate and associate
- Update Private Route Table:
- Add route 0.0.0.0/0 → NAT Gateway

8. **Secure Access to Private EC2 (via SSM):**

1. **Create IAM Role for SSM**
   - Go to IAM → Roles → Create Role
   - Trusted entity: EC2
   - Attach policy: AmazonSSMManagedInstanceCore
   - Role Name: SSM-Access-Role
2. **Attach Role to Private EC2**
   - Go to EC2 → Select Instance → Actions → Security → Modify IAM Role
   - Attach SSM-Access-Role
   - SSM Session via CLI
   - Ensure Session Manager Plugin is installed:
   - Session Manager Plugin Documentation

3. **Configure AWS CLI:**

   aws configure

   aws ssm start-session --target <Instance-ID> --region ap-south-1

Closing Summary:

This **AWS VPC setup** with public and private subnets was successfully implemented to meet the needs of a growing insurance project. The project demonstrates my ability to design secure, scalable cloud infrastructure using **AWS services** like **VPC**, **IGW**, **NAT Gateway**, and **EC2**. The setup ensures that the infrastructure is ready for future expansion while keeping security and performance a top priority.