Hybrid Cloud Setup Using VPN

1. Project Overview

Project Name: Hybrid Cloud Setup Using VPN
Services Used: AWS Site-to-Site VPN, VPC, EC2, Route Tables, Virtual Private Gateway, Customer Gateway
Goal: Securely connect an on-premises *simulated environment* (VirtualBox VM) with AWS VPC using Site-to-Site VPN.
Skills Gained: Hybrid networking, routing, VPN concepts, secure connectivity, hybrid DNS basics.

---

2. Architecture Overview (Conceptual)

- On-Premises Network (VirtualBox VM)
  - Example CIDR: 192.168.1.0/24
  - Acts as Customer Network
- AWS Cloud
  - VPC CIDR: 10.0.0.0/16
  - Public subnet with EC2 instance
  - Site-to-Site VPN tunnel connecting both networks

---

3. Prerequisites

On-Premises (Local System)

- VirtualBox installed
- Linux VM (Ubuntu preferred)
- VM Network Adapter: **Bridged** or **Host-only**
- Static private IP (example: 192.168.1.10)

AWS Account Requirements

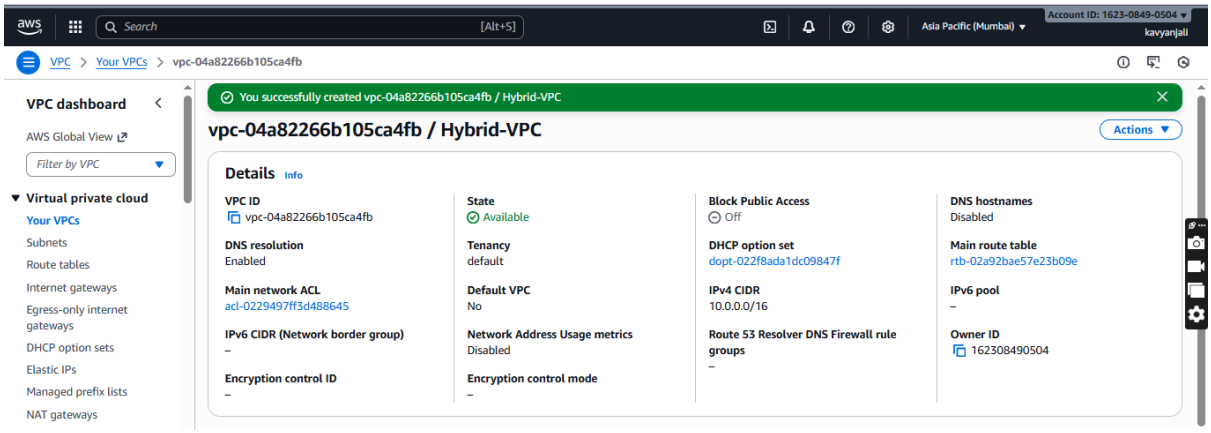
- AWS account
- IAM user with VPC full access
- Region selected (example: **ap-south-1**)

---

4. Step-by-Step AWS Console Setup

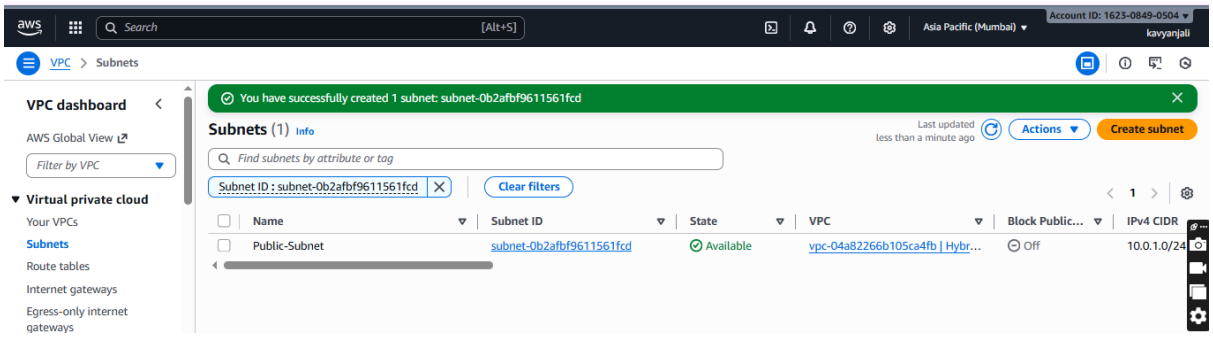
Step 1: Create a VPC

1. Go to **AWS Console → VPC**
2. Click **Create VPC**
3. Select **VPC only**
4. Configure:
   - Name: Hybrid-VPC
   - IPv4 CIDR: 10.0.0.0/16
5. Click **Create VPC**



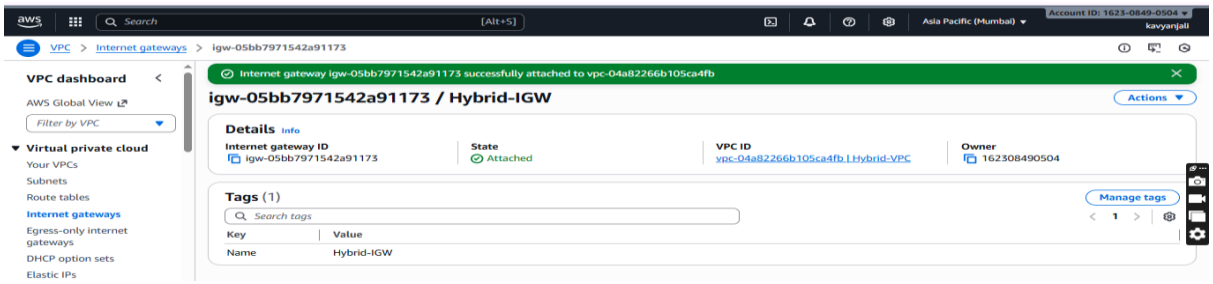
Step 2: Create a Public Subnet

1. VPC Dashboard → **Subnets** → Create subnet
2. Select VPC: Hybrid-VPC
3. Configure:
    - Subnet name: Public-Subnet
    - Availability Zone: ap-south-1a
    - CIDR: 10.0.1.0/24
4. Click **Create subnet**



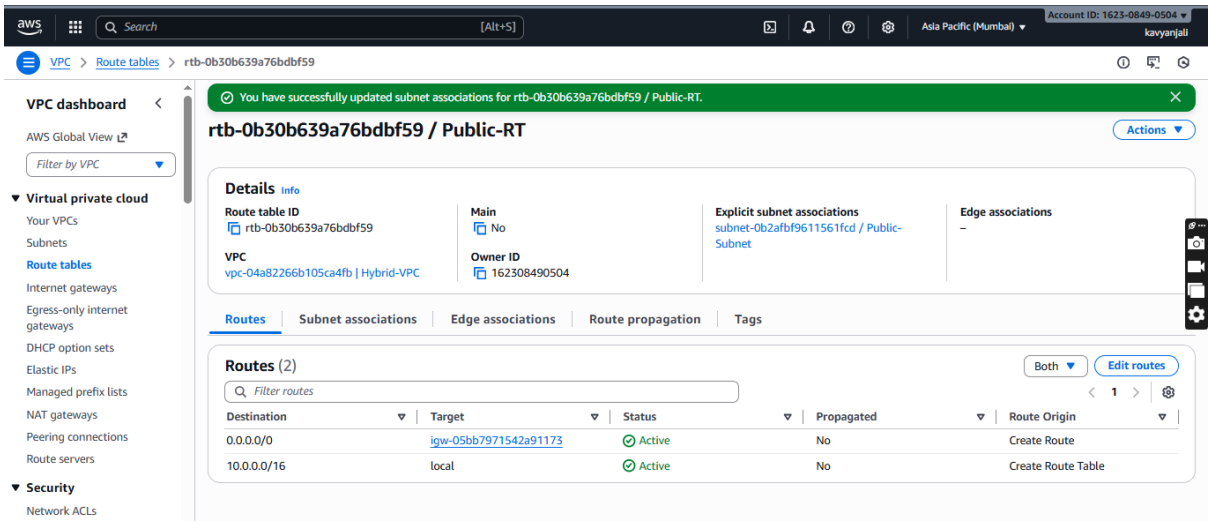
Step 3: Create Internet Gateway

1. VPC → **Internet Gateways** → Create
2. Name: Hybrid-IGW
3. Click **Create internet gateway**
4. Attach to VPC:
    - Actions → Attach → Select Hybrid-VPC



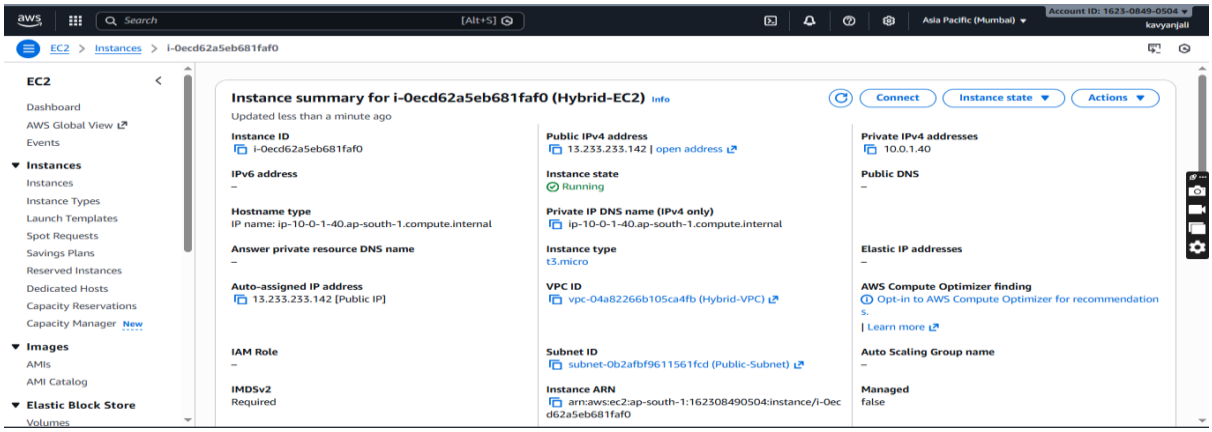
Step 4: Create Route Table

1. VPC → **Route Tables** → Create
2. Name: Public-RT
3. VPC: Hybrid-VPC
4. Edit Routes:
    - Destination: 0.0.0.0/0
    - Target: Internet Gateway (Hybrid-IGW)
5. Associate with Public-Subnet



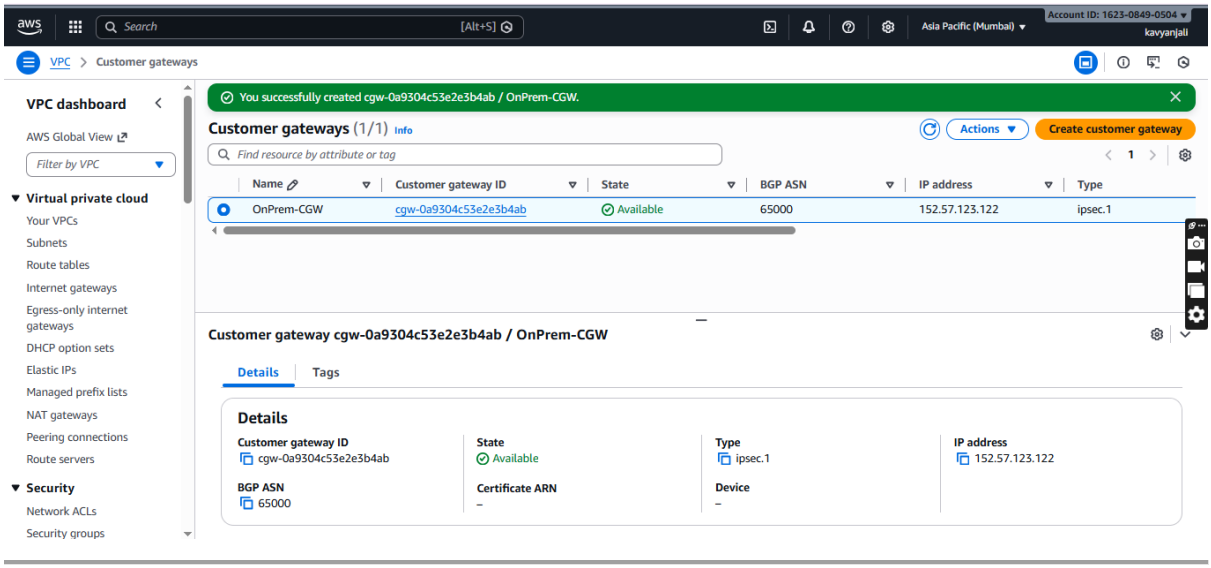
Step 5: Launch EC2 Instance (AWS Side)

1. Go to **EC2 → Launch Instance**
2. Choose AMI: Amazon Linux 2
3. Instance type: t2.micro
4. Network:
    - VPC: Hybrid-VPC
    - Subnet: Public-Subnet
    - Auto-assign public IP: Enabled
5. Security Group:
    - Allow SSH (22)
    - Allow ICMP (Ping)
6. Launch instance



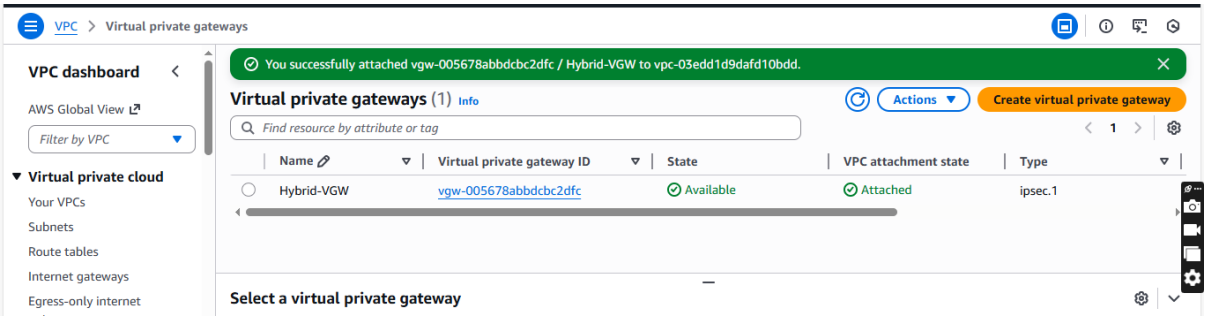
Step 6: Create Customer Gateway (On-Prem Representation)

1. VPC → **Customer Gateways** → Create
2. Configure:
    - Name: OnPrem-CGW
    - Routing: Static
    - IP Address: **Public IP of your local internet (ISP)**
3. Click **Create customer gateway**



Step 7: Create Virtual Private Gateway

1. VPC → **Virtual Private Gateways** → Create
2. Name: Hybrid-VGW
3. ASN: Default
4. Create and Attach:
    - Attach to Hybrid-VPC

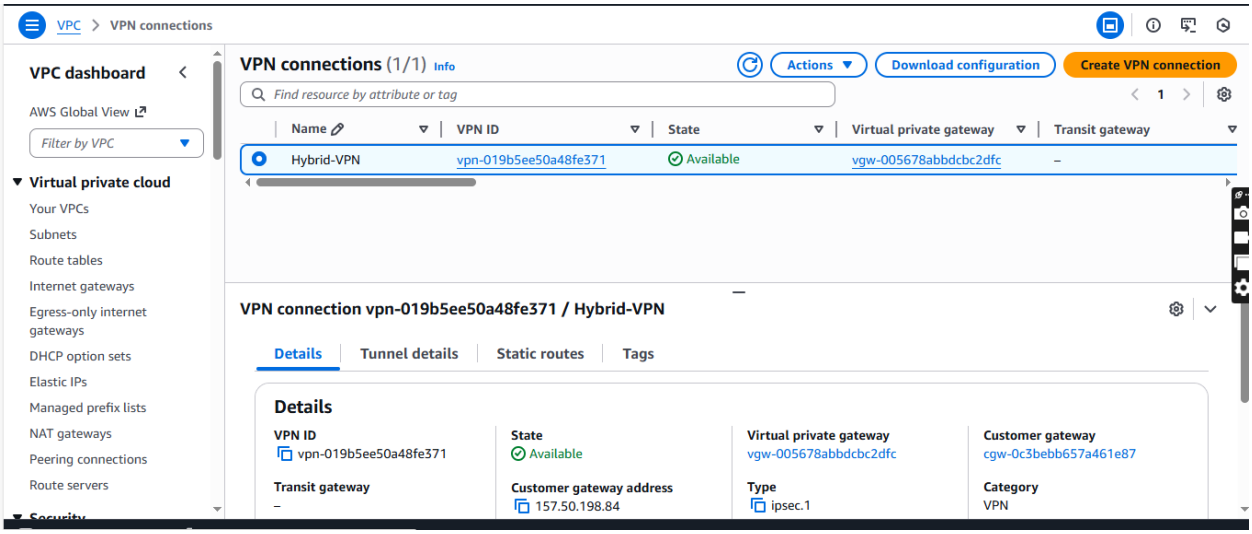


Step 8: Create Site-to-Site VPN Connection

1. VPC → **Site-to-Site VPN Connections** → Create
2. Configure:
    - Name: Hybrid-VPN
    - Target Gateway Type: Virtual Private Gateway
    - Virtual Private Gateway: Hybrid-VGW
    - Customer Gateway: Existing (OnPrem-CGW)
    - Routing Options: Static

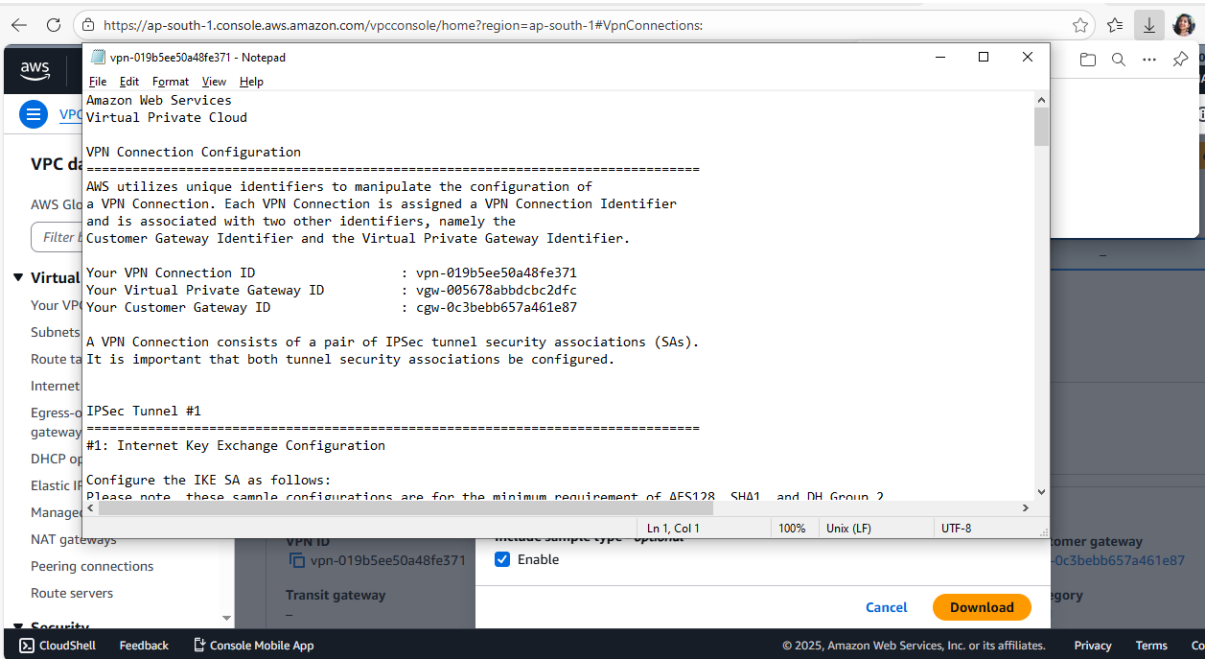
- Static IP Prefix: 192.168.1.0/24

3. Create VPN Connection



Step 9: Download VPN Configuration

1. Select VPN connection
2. Click **Download configuration**
3. Vendor: Generic
4. Save the configuration file

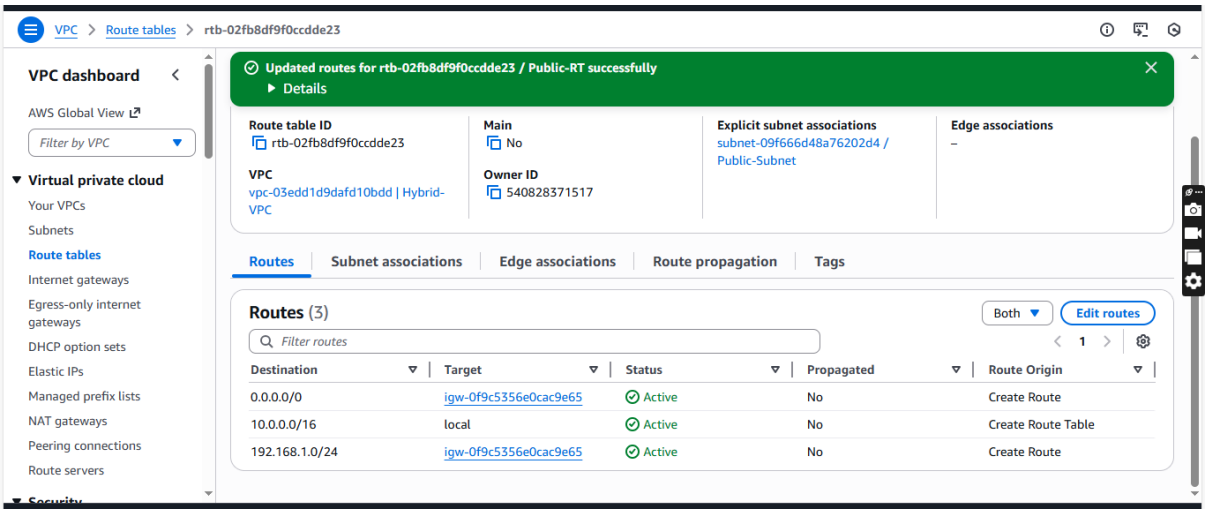


Step 10: Update VPC Route Table for VPN

1. VPC → Route Tables → Select Public-RT
2. Edit routes:

- Destination: 192.168.1.0/24
- Target: Virtual Private Gateway (Hybrid-VGW)

3. Save routes



Step 11: Verify VPN Status

Purpose

To check whether the **Site-to-Site VPN tunnel** between AWS and on-premises network is **established and working**.

Console Steps

1. Login to **AWS Management Console**
2. Go to **Services → VPC**
3. In the left menu, click **Site-to-Site VPN Connections**
4. Select the VPN connection named **Hybrid-VPN**
5. Scroll down to the **Tunnel details** section

What You Will See

AWS creates **2 VPN tunnels** for high availability:

Tunnel	Status
Tunnel 1	UP / DOWN
Tunnel 2	UP / DOWN

Status Meaning

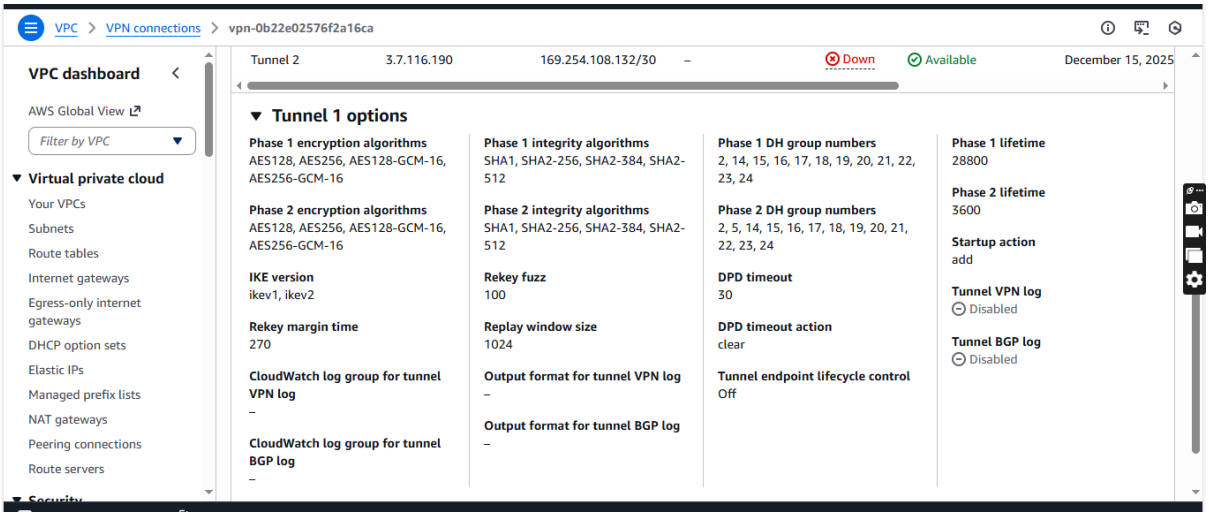
✅UP

- VPN tunnel is successfully established
- AWS can reach the on-premises gateway
- Routing and encryption are working

- Hybrid connectivity is **active**

✕DOWN

- VPN tunnel is **not established**
- AWS cannot reach the on-premises VPN device
- Common reasons:
    - On-prem VPN software not configured
    - Wrong public IP in Customer Gateway
    - ISP blocks IPsec traffic
    - Tunnel not initiated yet



---

12. Verification & Testing

From On-Prem VM

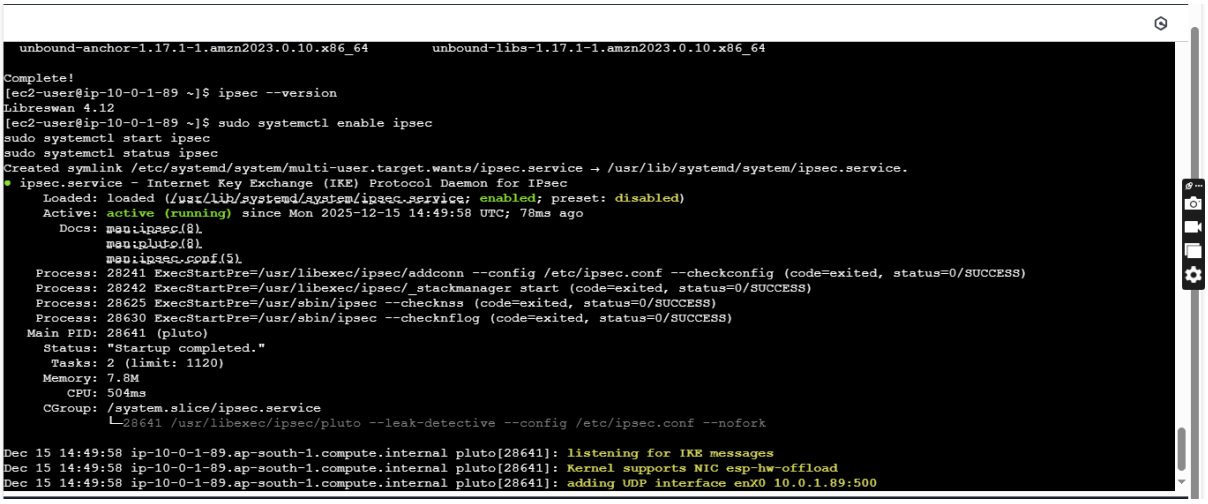
ping 10.0.0.10

ssh ec2-user@10.0.0.10

From EC2 Instance

ping 192.168.1.10

Successful ping confirms hybrid connectivity.



---

13. Hybrid DNS

- On-prem DNS resolves local names
- AWS Route 53 (optional) resolves cloud resources
- Use conditional forwarding for hybrid DNS

---

14. Security Best Practices

- Restrict Security Group rules
- Use strong VPN pre-shared keys
- Enable CloudWatch logs for VPN
- Rotate keys periodically

---

15. Project Outcome

✔ Secure hybrid connectivity established
✔ On-prem and AWS networks communicate privately
✔ Real-world enterprise hybrid cloud setup simulated

---

16. Conclusion

This project demonstrates a **real-world Hybrid Cloud architecture** using AWS Site-to-Site VPN. It is widely used in enterprises to extend on-prem infrastructure securely into AWS without exposing services to the public internet.
