Steps for VPN Project

1. **Create VPC (VPC & More)**

   Name – On-Prem

   IPv4 CIDR – 172.16.0.0/16

   Available Zone - 1

   Public Subnet - 1

   Private Subnet - 0

   Nat Gateway – none

   Create VPC

2. **Create an Instance in On-Prem**

   Name – On-Premises

   AMI – Ubuntu

   Key pair – Existing

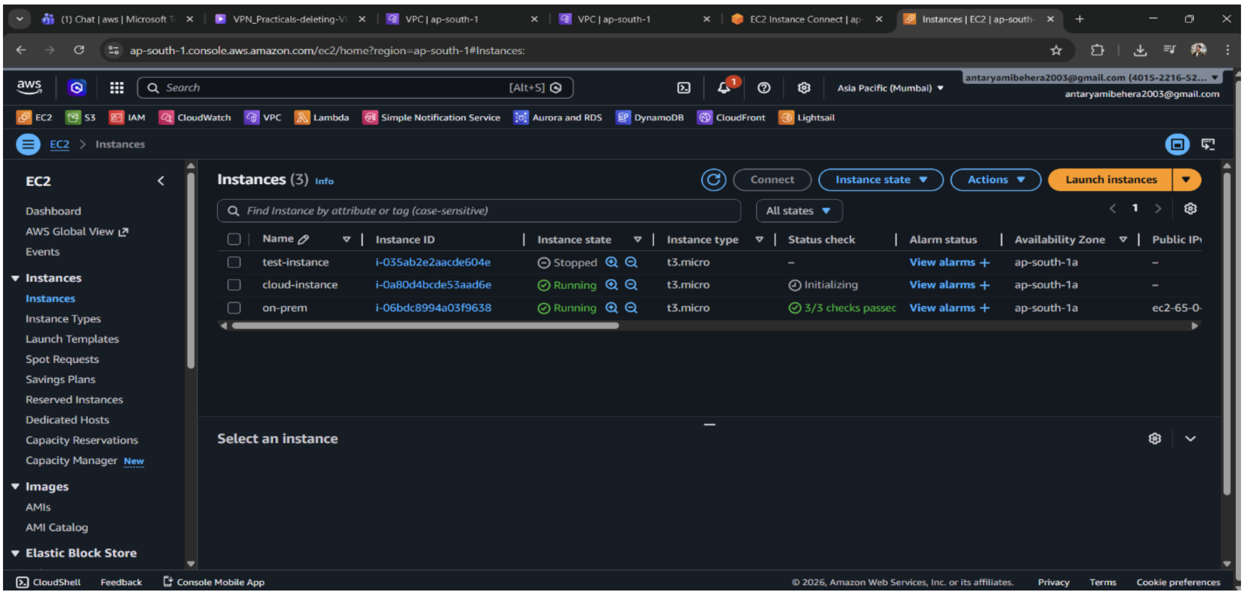
   Network settings edits

   - VPC – On-Prem
   - Public subnet
   - Auto assign public IP – Enable

   Security Group

   - SSH
   - ICMP all (custom) (172.16.0.0/16)
   - Custom UDP (custom) (172.16.0.0/16) - [500]
   - Custom UDP (custom) (172.16.0.0/16) - [4500]

   Launch Instance



ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Instances:

Instances (3) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
test-instance	i-035ab2e2aacde604e	Stopped	t3.micro	–	View alarms +	ap-south-1a	–
cloud-instance	i-0a80d4bcde53aad6e	Running	t3.micro	Initializing	View alarms +	ap-south-1a	–
on-prem	i-06bdc8994a03f9638	Running	t3.micro	3/3 checks passec	View alarms +	ap-south-1a	ec2-65-0-

3. **Create Another VPC (VPC & More)**

   Name – Aws Cloud

   CIDR – 10.0.0.0/16

   Available zone – 1

   Public subnet – 0

   Private subnet – 1

   NAT Gateway – none

   Create VPC

4. **In VPC left-side menu – VPN**

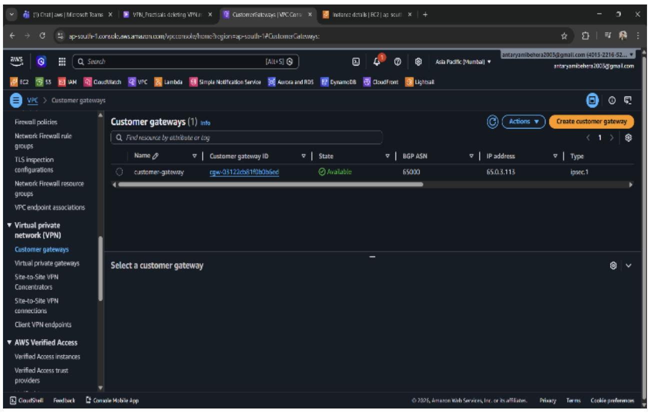
   ❖ Customer gateway – Create

   Name – customer-gateway

   BGD ASN – Bydefault

   IP Address – Give the public IP of On-prem (Which Instance have the Customer gate way)

   Create Customer gateway



Customer gateways (1)

Name	Customer gateway ID	State	BGP ASN	IP address	Type
customer-gateway	cgw-03122cb81f0b0b6ed	Available	65000	65.0.3.113	ipsec.1

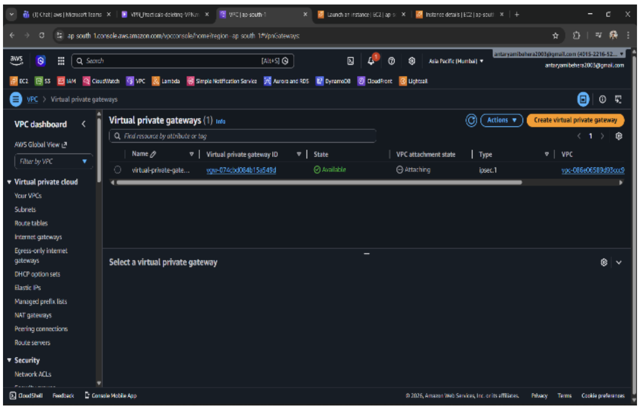
❖ **Virtual Private Gateway**

Name – Virtual-Private-gateway

ASN – Amazon default ASN

Create Virtual Gateway

After available select that GW then in Action – Attach – AWS Cloud VPC



Virtual private gateways (1)

Name	Virtual private gateway ID	State	VPC attachment state	Type	VPC
virtual-private-gate...	vgw-074cbd084b15a549d	Available	Attaching	ipsec.1	vpc-086e06589d93cc9

Actions
Create virtual private gateway
Select a virtual private gateway

❖ **Site-to-site Connection**

Name – VPN

TGT – Virtual private gateway

Virtual private gateway (Choose) – Virtual-private-gateway

Customer gateway (Choose) – That you created for On-prem

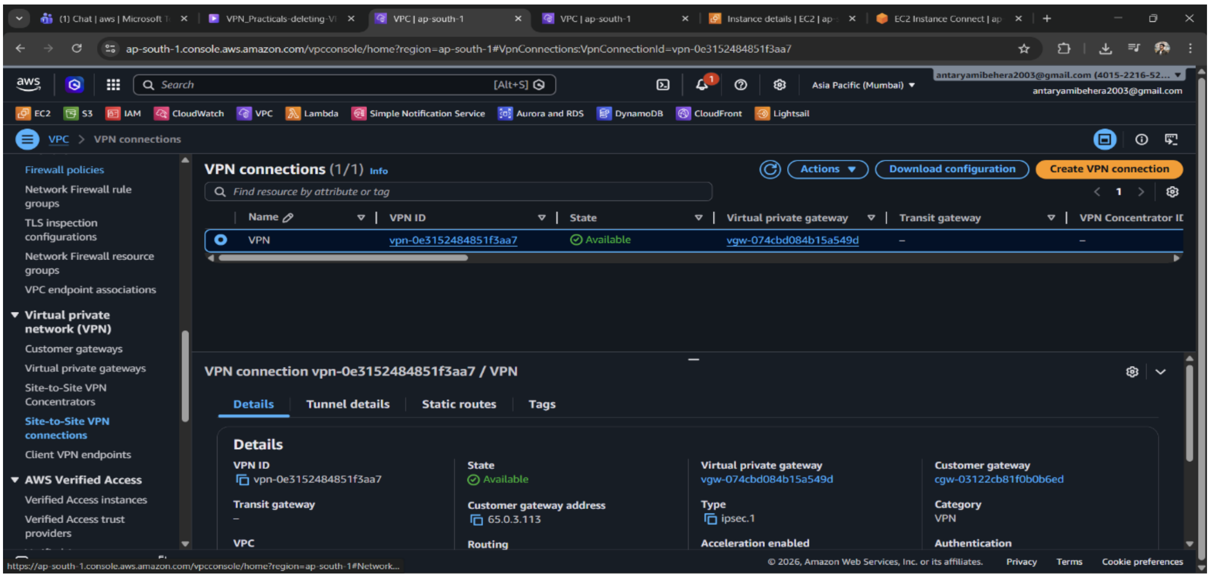
Routing Option – static

Static IP Prefixes – (On-Prem-Network) That IPv4 CIDR [In VPC you will get]

Pre-Share-key – Standard

Create VPN connection

Download configuration: - Vendor – Strongswan
Remain same – Download


(1) Chat | aws | Microsoft
VPN_Practicals-deleting-V
VPC | ap-south-1
VPC | ap-south-1
Instance details | EC2 | ap
EC2 Instance Connect | ap
aws
Search [Alt+S]
Asia Pacific (Mumbai)
EC2 S3 IAM CloudWatch VPC Lambda Simple Notification Service Aurora and RDS DynamoDB CloudFront Lightsail
VPC > VPN connections
Firewall policies
Network Firewall rule groups
TLS inspection configurations
Network Firewall resource groups
VPC endpoint associations
Virtual private network (VPN)
Customer gateways
Virtual private gateways
Site-to-Site VPN Concentrators
Site-to-Site VPN connections
Client VPN endpoints
AWS Verified Access
Verified Access instances
Verified Access trust providers
Actions
Download configuration
Create VPN connection
Find resource by attribute or tag
Details
Tunnel details
Static routes
Tags
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#VpnConnections:VpnConnectionId=vpn-0e3152484851f3aa7

antaryamibehera2003@gmail.com (4015-2216-52...

antaryamibehera2003@gmail.com

VPN connections (1/1) Info

Name	VPN ID	State	Virtual private gateway	Transit gateway	VPN Concentrator ID
VPN	vpn-0e3152484851f3aa7	Available	vgw-074cbd084b15a549d	–	–

VPN connection vpn-0e3152484851f3aa7 / VPN

Details

VPN ID: vpn-0e3152484851f3aa7

State: Available

Virtual private gateway: vgw-074cbd084b15a549d

Customer gateway: cgw-03122cb81f0b0b6ed

Transit gateway: –

Customer gateway address: 65.0.3.113

Type: ipsec.1

Category: VPN

VPC

Routing

Acceleration enabled

Authentication

https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#Network...

5. In Instance – Connect (On-Prem)

- Sudo apt update
- Sudo apt install strongswan -y
- Ipsec version
- Sudo ipsec status
- Sudo ipsec statusall
- Sudo nano /etc/sysctl.conf

  Uncomment – net.ipv4.ip_forward-1 (From configuration document)

  [Save & Exit]
- Sudo sysctl -p
- Sudo nano /etc/ipsec.conf

  Uncomment – uniqueids = no

  {Paste the “conn Tunnel1”}

  Uncomment the CIDR line (last line) Paste CIDR of AWS Cloud VPC

  [Save & Exit]
- Sudo nano /etc/ipsec.secrets

  pre-shared-key (PSK)

  {Paste the PSK line – tunnel 1 & tunnel 2}

  [Save & Exit]
- Sudo nano /etc/ipsec.d/aws-updown.sh

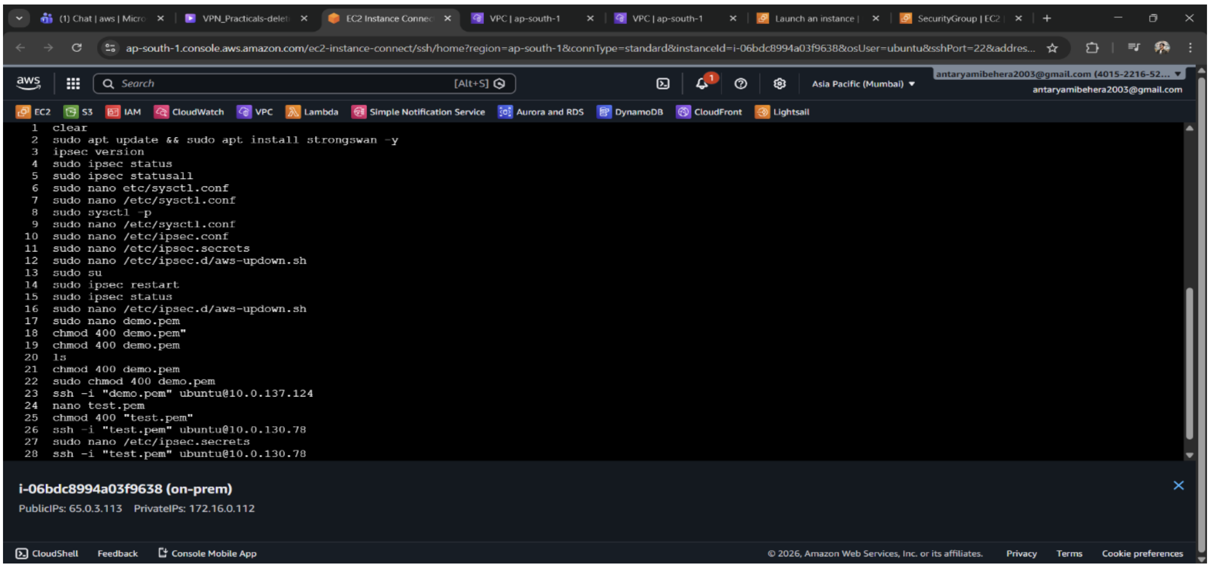
  (Copy the script of document and paste it)

  and give 744 persmission

  (In add_route line paste – src {private IP (on-prem)})

  [Save & Exit]
- Sudo su

- echo 1 > /proc/sys/net/ipv4/ip_forword
  [Save & Exit]
- Sudo ipsec restart
- Sudo ipsec status



```
  1  clear
  2  sudo apt update && sudo apt install strongswan -y
  3  ipsec version
  4  sudo ipsec status
  5  sudo ipsec statusall
  6  sudo nano etc/sysctl.conf
  7  sudo nano /etc/sysctl.conf
  8  sudo sysctl -p
  9  sudo nano /etc/sysctl.conf
 10  sudo nano /etc/ipsec.conf
 11  sudo nano /etc/ipsec.secrets
 12  sudo nano /etc/ipsec.d/aws-updown.sh
 13  sudo su
 14  sudo ipsec restart
 15  sudo ipsec status
 16  sudo nano /etc/ipsec.d/aws-updown.sh
 17  sudo nano demo.pem
 18  chmod 400 demo.pem"
 19  chmod 400 demo.pem
 20  ls
 21  chmod 400 demo.pem
 22  sudo chmod 400 demo.pem
 23  ssh -i "demo.pem" ubuntu@10.0.137.124
 24  nano test.pem
 25  chmod 400 "test.pem"
 26  ssh -i "test.pem" ubuntu@10.0.130.78
 27  sudo nano /etc/ipsec.secrets
 28  ssh -i "test.pem" ubuntu@10.0.130.78
```

i-06bdc8994a03f9638 (on-prem)

PublicIPs: 65.0.3.113 PrivateIPs: 172.16.0.112

ap-south-1.console.aws.amazon.com/ec2-instance-connect/ssh/home?region=ap-south-1&connType=standard&instanceId=i-06bdc8994a03f9638&osUser=ubuntu&sshPort=22&addres...
EC2
S3
IAM
CloudWatch
VPC
Lambda
Simple Notification Service
Aurora and RDS
DynamoDB
CloudFront
Lightsail
Asia Pacific (Mumbai)
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

6. In Rout Table

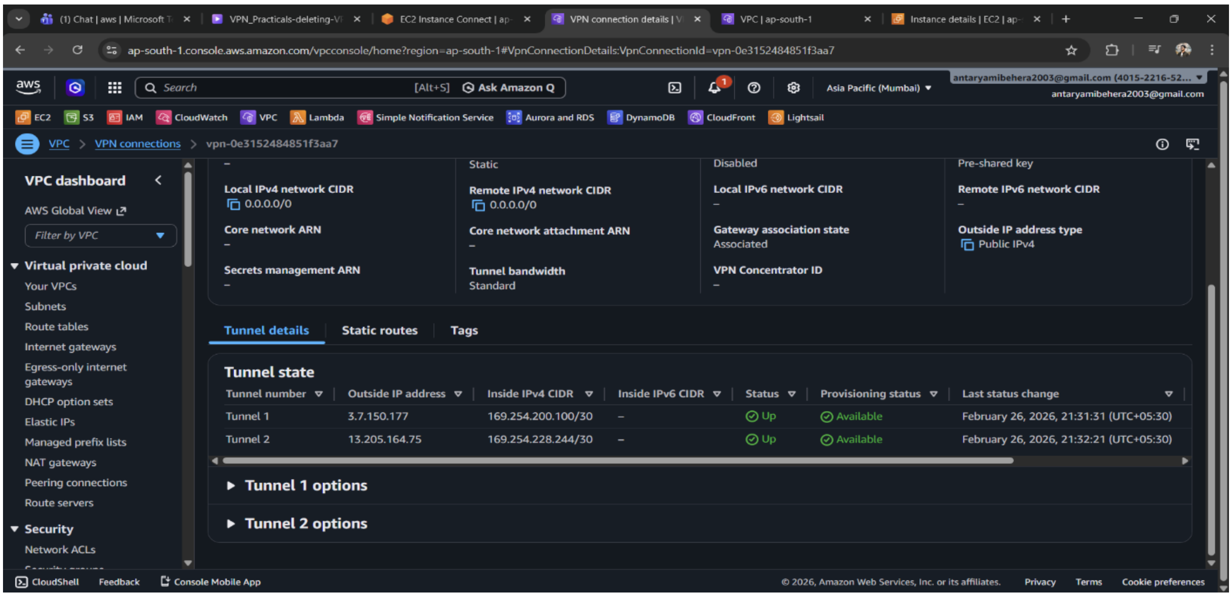
Private RT – add Inbound rule (172.16.0.0/16) – Private-virtual-gateway

[Save]

7. Create a private instance in AWS Cloud VPC

Only add – SSH – 172.16.0.0/16

– custom ICMP – Ipv4 – 172.16.0.0/16



VPC > VPN connections > vpn-0e3152484851f3aa7

–	Static	Disabled	Pre-shared key
Local IPv4 network CIDR 0.0.0.0/0	Remote IPv4 network CIDR 0.0.0.0/0	Local IPv6 network CIDR –	Remote IPv6 network CIDR –
Core network ARN –	Core network attachment ARN –	Gateway association state Associated	Outside IP address type Public IPv4
Secrets management ARN –	Tunnel bandwidth Standard	VPN Concentrator ID –	

Tunnel state

Tunnel number	Outside IP address	Inside IPv4 CIDR	Inside IPv6 CIDR	Status	Provisioning status	Last status change
Tunnel 1	3.7.150.177	169.254.200.100/30	–	Up	Available	February 26, 2026, 21:31:31 (UTC+05:30)
Tunnel 2	13.205.164.75	169.254.228.244/30	–	Up	Available	February 26, 2026, 21:32:21 (UTC+05:30)