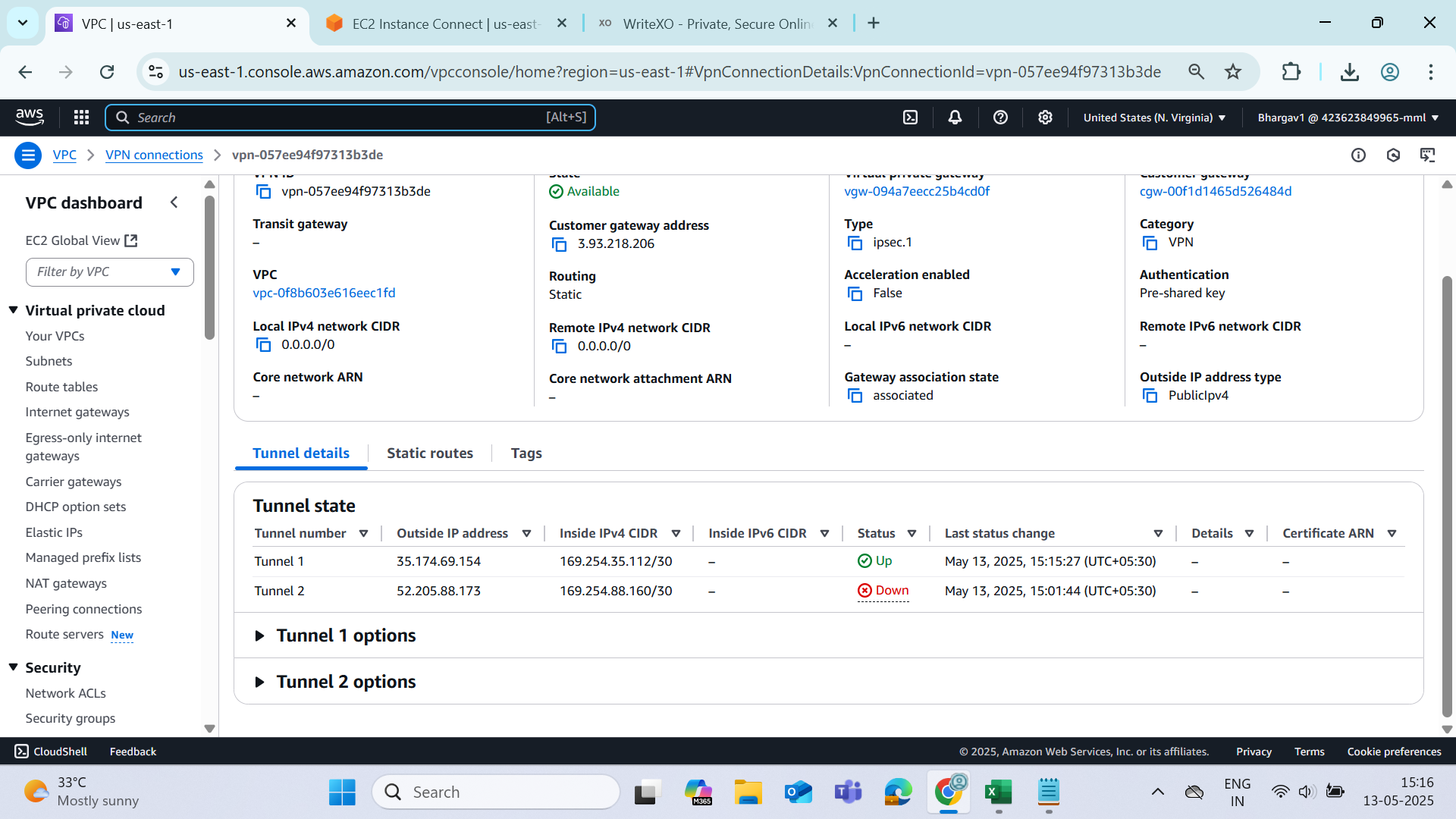
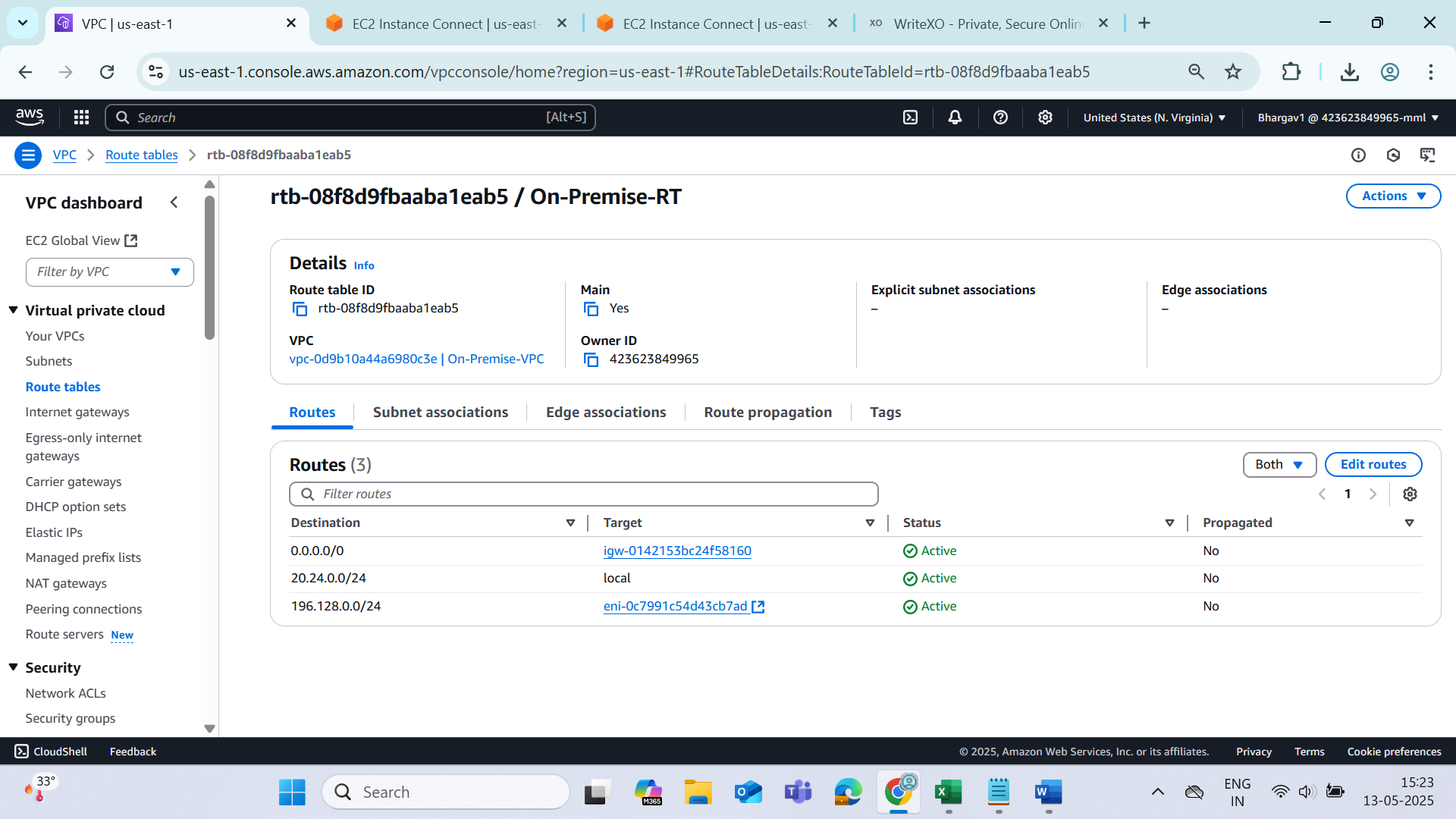
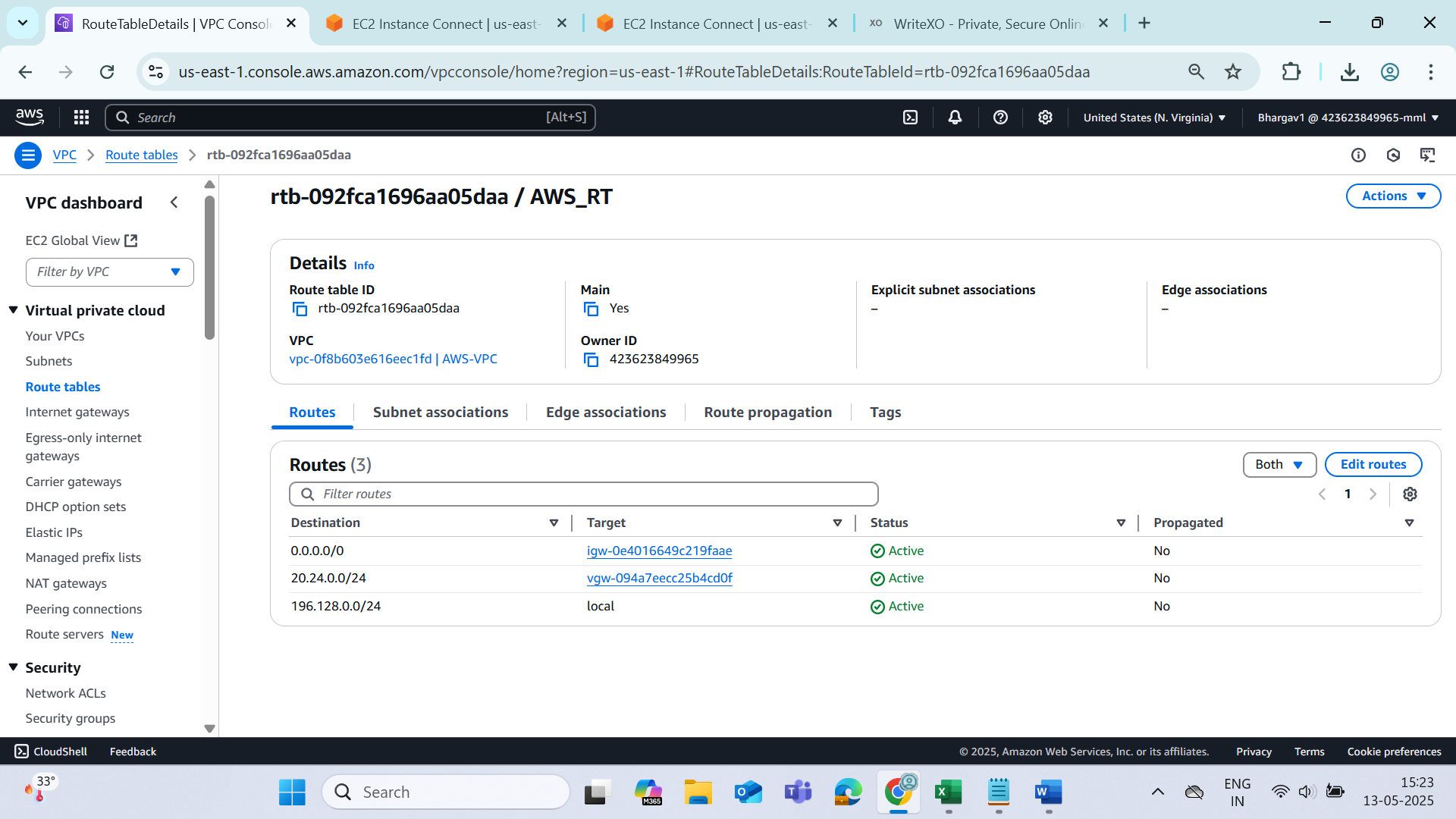
Site-to-site-vpn

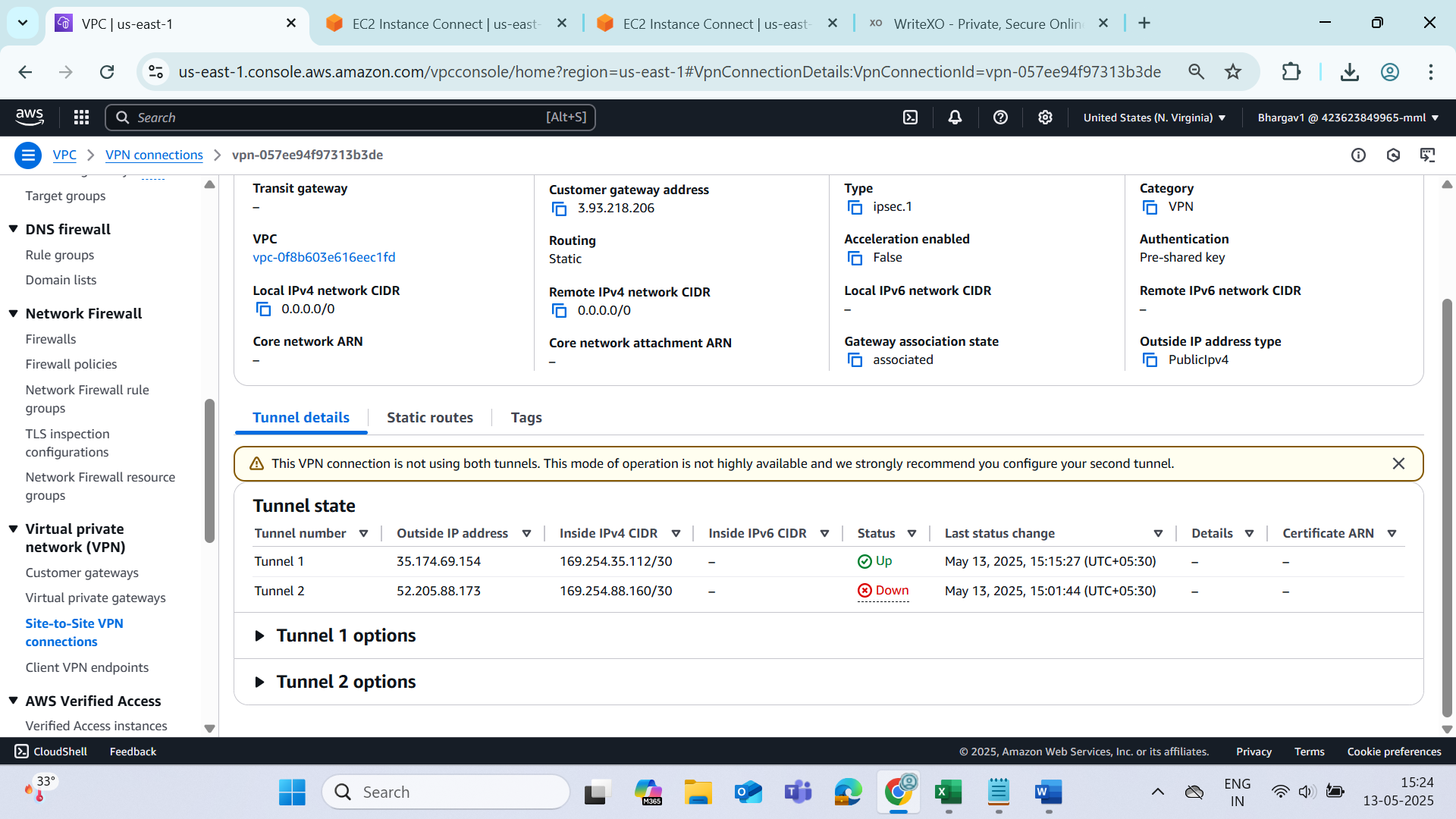


On-Premise Instance



AWS virtual gateway





Site to Site VPN connection

**Created 2 VPC**

AWS-VPC : 196.128.0.0/24

On-Prim-VPC : 20.24.0.0/24

**Create Subnets**

AWS-VPC-Subnet

196.128.0.0/25

On-Prim-VPC-Subnet

20.24.0.0/25

Created EC2 On Prim

Simulating as Local machine

Public IP : 3.110.143.247

Install Strongswan in On premises EC2

>>sudo apt update

>>sudo apt install strongswan -y

Created a EC2 on AWS-VPC

Public IP:

Private IP

**Create Customer Gateway**

By giving the On premises Public IPv4 address

**Create Virtual Private Gateway**

1.Create by passing the Name

2. Attach it to the AWS-VPC

**Create a VPN connection**

Attach the Customer Gateway

Attach the Virtual Private Gateway

Select static under the Routing Options

Pass the On-Premises VPC Public Subnet cidr where the On-Prim EC2 is created

**Download the VPN configuration**

Select the strongswan in the provider section and click on download

**Connect to On-Prim EC2 instance**

Enable Packet Forwarding

1) Open /etc/sysctl.conf and uncomment the following line to enable IP packet forwarding:

  net.ipv4.ip\_forward = 1

>>vi /etc/sysctl.conf

2) Apply the changes in step 1 by executing the command 'sudo sysctl -p'

>> 'sudo sysctl -p'

3) Create a new file at /etc/ipsec.conf if doesn't already exist, and then open it. Uncomment the line "uniqueids=no" under the 'config setup' section.

>>vi  /etc/ipsec.conf

Append the following configuration to the end of the file:

Open the VPN-Configuration file copy the following tunnel information and append to above ippesc.conf

**conn Tunnel1**

**auto=start**

**left=%defaultroute**

**leftid=3.110.143.247**

**right=13.235.120.220**

**type=tunnel**

**leftauth=psk**

**rightauth=psk**

**keyexchange=ikev1**

**ike=aes128-sha1-modp1024**

**ikelifetime=8h**

**esp=aes128-sha1-modp1024**

**lifetime=1h**

**keyingtries=%forever**

**leftsubnet=20.24.0.0/25 #(Note: This is On Prim Subnet Cidr where EC2(On Prim) resides)**

**rightsubnet=196.128.0.0/25 #(Note: This is AWS-VPC Subnet Cidr where EC2(AWS-VPC) resides)**

**dpddelay=10s**

**dpdtimeout=30s**

**dpdaction=restart**

4) Create a new file at /etc/ipsec.secrets if it doesn't already exist, and append this line to the file (be mindful of the spacing!). This value authenticates the tunnel endpoints(you can find in the downloaded Configuration file:

3.110.143.247 13.235.120.220 : PSK "ln6HWQeItFnqKONKM33.oluoG5cdDplb"

>>vi /etc/ipsec.secrets

**Restart IPsec using the following command**

ipsec restart

ipsec up <Tunnel1>(name of the connection given in the ipsec.conf

Site to Site VPN connection

Created 2 VPC

AWS-VPC : 196.128.0.0/24

On-Prim-VPC : 20.24.0.0/24

Create Subnets

AWS-VPC-Subnet

196.128.0.0/25

On-Prim-VPC-Subnet

20.24.0.0/25

Created EC2 On Prim

Simulating as Local machine

Public IP : 3.110.143.247

Install Strongswan in On premises EC2

sudo apt update

sudo apt install strongswan -y

Created a EC2 on AWS-VPC

Public IP:

Private IP

Create Customer Gateway

By giving the On premises Public IPv4 address

Create Virtual Private Gateway

1.Create by passing the Name

2. Attach it to the AWS-VPC

Create a VPN connection

Attach the Customer Gateway

Attach the Virtual Private Gateway

Select static under the Routing Options

Pass the On-Premises VPC Public Subnet cidr where the On-Prim EC2 is created

Download the VPN configuration

Select the strongswan in the provider section and click on download

Connect to On-Prim EC2 instance

Enable Packet Forwarding

1) Open /etc/sysctl.conf and uncomment the following line to enable IP packet forwarding:

  net.ipv4.ip\_forward = 1

2) Apply the changes in step 1 by executing the command 'sudo sysctl -p'

3) Create a new file at /etc/ipsec.conf if doesn't already exist, and then open it. Uncomment the line "uniqueids=no" under the 'config setup' section.

Append the following configuration to the end of the file:

Open the VPN-Configuration file

conn Tunnel1

 auto=start

 left=%defaultroute

 leftid=3.110.143.247

 right=13.235.120.220

 type=tunnel

 leftauth=psk

 rightauth=psk

 keyexchange=ikev1

 ike=aes128-sha1-modp1024

 ikelifetime=8h

 esp=aes128-sha1-modp1024

 lifetime=1h

 keyingtries=%forever

 leftsubnet=20.24.0.0/25 #(Note: This is On Prim Subnet Cidr where EC2(On Prim) resides)

 rightsubnet=196.128.0.0/25 #(Note: This is AWS-VPC Subnet Cidr where EC2(AWS-VPC) resides)

 dpddelay=10s

 dpdtimeout=30s

 dpdaction=restart

4) Create a new file at /etc/ipsec.secrets if it doesn't already exist, and append this line to the file (be mindful of the spacing!). This value authenticates the tunnel endpoints:

3.110.143.247 13.235.120.220 : PSK "ln6HWQeItFnqKONKM33.oluoG5cdDplb"

Restart IPsec using the following command

ipsec restart

ipsec up <Tunnel1>(name of the connection given in the ipsec.conf