**Steps to create VPN :-**

**Client side :- (it is a public)**

1. Create VPC
2. Create subnet
3. Create internet gateway
4. Create entry in route table (entry of internet gateway and enable subnet association)

**Server side:- (it is a private)**

1. Create VPC
2. Create subnet
3. Create internet gateway
4. Create entry in route table of (internet gateway and enable subnet association)
5. Create customer gateway :-

* Give name
* Routing :- static
* Ip address :- give the ip of your public ip of your public instance
* Click on customer gateway

1. Create virtual private gateway

* Name of private gateway
* ASN :- amazon default ASN
* Create virtual private gateway

1. Attach virtual private gateway to VPC
2. Create VPN connection

* Name
* Target gateway type :- virtual private gateway
* Virtual private gateway :- select the virtual private gateway that you had created
* Customer gateway :- existing and select the customer gateway
* Customer gateway ID :- select the customer ID
* Routing options :- static (static IP prefix :- give the CIDR of your server/private subnet (it means you creating VPN that side subnet CIDR))
* Create VPN connection

1. Download the configuration file
2. Enable the subnet propagation from rout table

**Client/public side :-**

1. Get the ssh of instance
2. Sudo su (login with root)
3. Install openswan (yum install openswan –y)
4. Systemctl start ipsec
5. Then open the VPN connection downloaded file
6. Open file :- (vim /etc/sysctl.conf)

* net.ipv4.ip\_forward = 1
* net.ipv4.conf.default.rp\_filter = 0
* net.ipv4.conf.default.accept\_source\_route = 0

1. Open file :-

* Vim /etc/ipsec.conf ( uncomment the last line #include /etc/ipsec.d/\*.conf)

1. Create file :- vim /etc/ipsec.d/aws.conf

* Paste the options :-

conn Tunnel1

authby=secret

auto=start

left=%defaultroute

leftid=3.82.198.78

right=35.82.67.75

type=tunnel

ikelifetime=8h

keylife=1h

phase2alg=aes128-sha1;modp1024

ike=aes128-sha1;modp1024

auth=esp **(remove this line)**

keyingtries=%forever

keyexchange=ike

leftsubnet=<LOCAL NETWORK> **(paste the CIDR of client/public )**

rightsubnet=<REMOTE NETWORK>**( paste the CIDR of server/private)**

dpddelay=10

dpdtimeout=30

dpdaction=restart\_by\_peer

* Save the file (esc :wq)

1. Create a file :- vim /etc/ipsec.d/aws.secrets

* Paste the secret key here (3.82.198.78 52.41.53.248: PSK "1M6mq3.BPSUxtraott4aZbZwaJVgoNHI")

1. Ping or get the ssh of private/server by its private ip (ssh –I /home/ec2-user/key\_name.pem ec2-user@public\_ip\_of\_server)