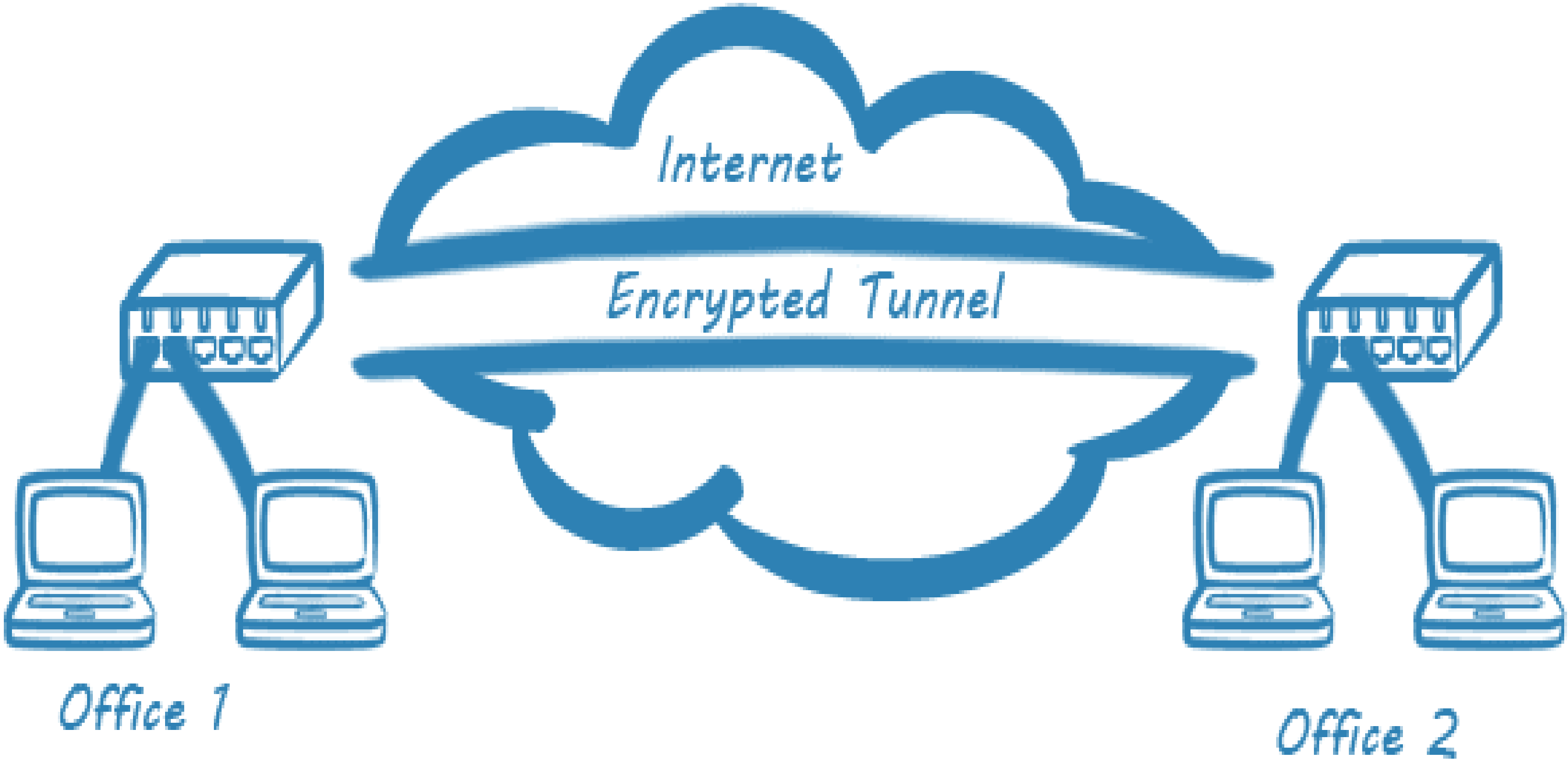

Internet
Encrypted Tunnel
Office 1
Office 2

VPN

- ✓ AWS Virtual Private Network solutions establish secure connections between your on-premises networks, remote offices, client devices, and the AWS global network. AWS VPN is comprised of two services: AWS Site-to-Site VPN and AWS Client VPN. Together, they deliver a highly-available, managed, and elastic cloud VPN solution to protect your network traffic.
- ✓ AWS Site-to-Site VPN creates encrypted tunnels between your network and your Amazon Virtual Private Clouds or AWS Transit Gateways. For managing remote access, AWS Client VPN connects your users to AWS or on-premises resources using a VPN software client.

VPN Tunnel

A VPN tunnel is an encrypted link between your device and another network.

How does a VPN tunnel work?

- A VPN tunnel works by encapsulating data in an encrypted data packet. To understand encapsulation, let us attempt a simple analogy.
- If you were a political refugee and your location was confidential for your safety but you needed to communicate with key people in your home country, how would you do it?
- Well, one way would be write the message on a postcard with the address of the final recipient and then put the postcard into an envelope and post it to a trusted friend in your home country. When your friend receives it, he opens the envelope, puts a stamp on the postcard and posts it. The final recipient of the postcard has no knowledge of where the postcard came from since the stamp is local.
- The act of putting the postcard into the envelope with its own address is equivalent to encapsulation and when you do this with data on the Internet, you create a virtual private network tunnel, commonly called 'VPN tunneling'.

VPN Tunnel protocols

Internet Protocol Security (IPSec):
Internet Protocol Security, known as IPSec, is used to secure Internet communication across an IP network. IPSec secures Internet Protocol communication by verifying the session and encrypts each data packet during the connection.

Layer 2 Tunneling Protocol (L2TP):
L2TP or Layer 2 Tunneling Protocol is a tunneling protocol that is often combined with another VPN security protocol like IPSec to establish a highly secure VPN connection. L2TP generates a tunnel between two L2TP connection points and IPSec protocol encrypts the data and maintains secure communication between the tunnel.

Point–to–Point Tunneling Protocol (PPTP):
PPTP or Point-to-Point Tunneling Protocol generates a tunnel and confines the data packet. Point-to-Point Protocol (PPP) is used to encrypt the data between the connection. PPTP is one of the most widely used VPN protocol and has been in use since the early release of Windows. PPTP is also used on Mac and Linux apart from Windows.

VPN Tunnel protocols

- ✓ **SSL and TLS:**
  SSL (Secure Sockets Layer) and TLS (Transport Layer Security) generate a VPN connection where the web browser acts as the client and user access is prohibited to specific applications instead of entire network. Online shopping websites commonly uses SSL and TLS protocol. It is easy to switch to SSL by web browsers and with almost no action required from the user as web browsers come integrated with SSL and TLS. SSL connections have “https” in the initial of the URL instead of “http”.
- ✓ **OpenVPN:**
  OpenVPN is an open source VPN that is commonly used for creating Point-to-Point and Site-to-Site connections. It uses a traditional security protocol based on SSL and TLS protocol.
- ✓ **Secure Shell (SSH):**
  Secure Shell or SSH generates the VPN tunnel through which the data transfer occurs and also ensures that the tunnel is encrypted. SSH connections are generated by a SSH client and data is transferred from a local port on to the remote server through the encrypted tunnel.

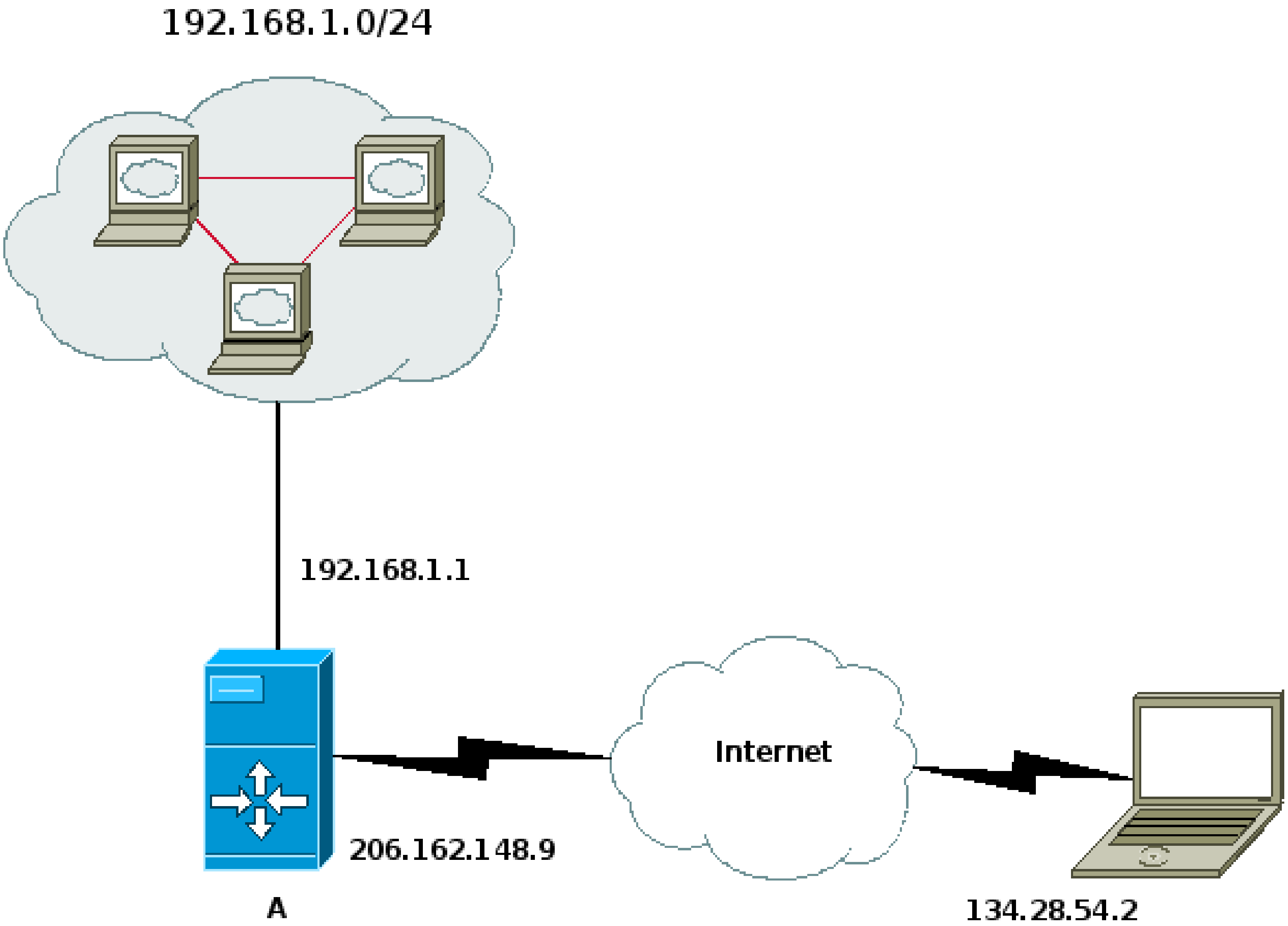
VPN Types

Remote Access VPN:

Remote Access VPN permits a user to connect to a private network and access all its services and resources remotely. The connection between the user and the private network occurs through the Internet and the connection is secure and private. Remote Access VPN is useful for home users and business users both. An employee of a company, while he/she is out of station, uses a VPN to connect to his/her company's private network and remotely access files and resources on the private network.

Site to Site VPN:

A Site-to-Site VPN is also called as Router-to-Router VPN and is commonly used in the large companies. Companies or organizations, with branch offices in different locations, use Site-to-site VPN to connect the network of one office location to the network at another office location.


192.168.1.0/24
192.168.1.1
206.162.148.9
A
Internet
134.28.54.2

VPN Client Lab Steps --openvpn

1) Create one VPC with Public and Private Subnet.

2) Create openvpn server from aws marketplace-select public subnet-next –SG-keep default ---launch

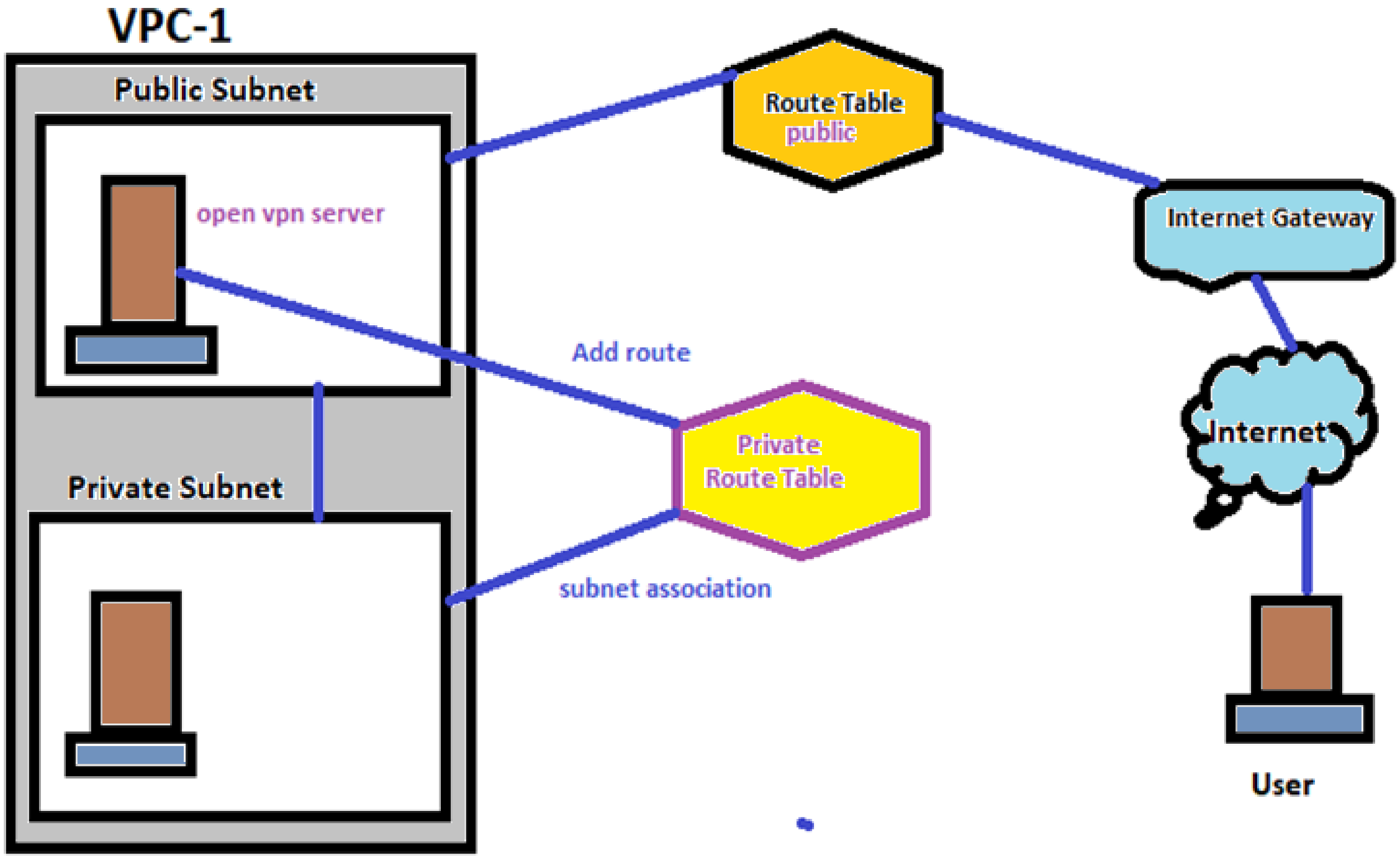
3) Open this server with user name : openvpnas

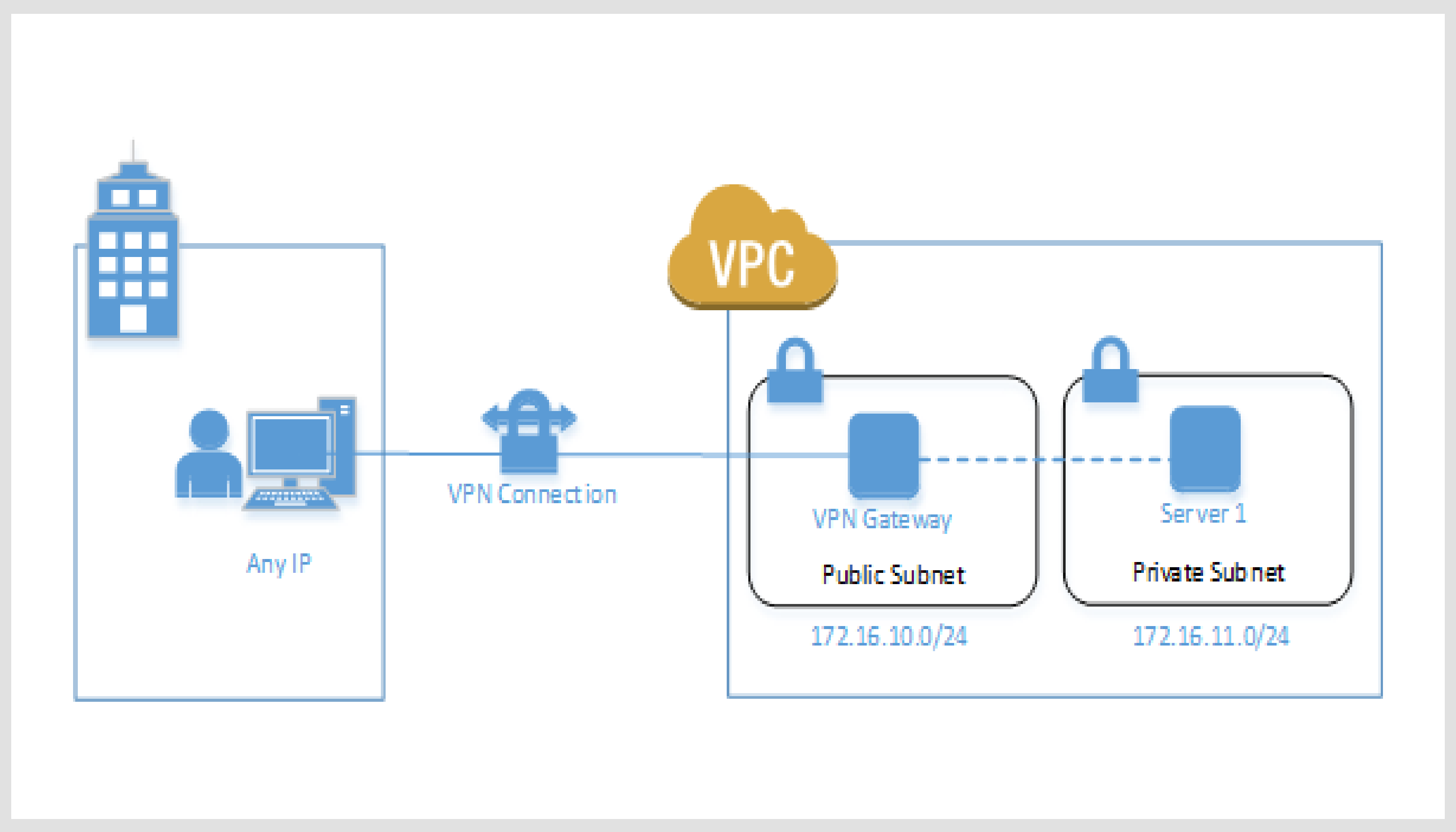
4) Follow the instruction ----yes-yes—etc ---passwd openvpn –give new password

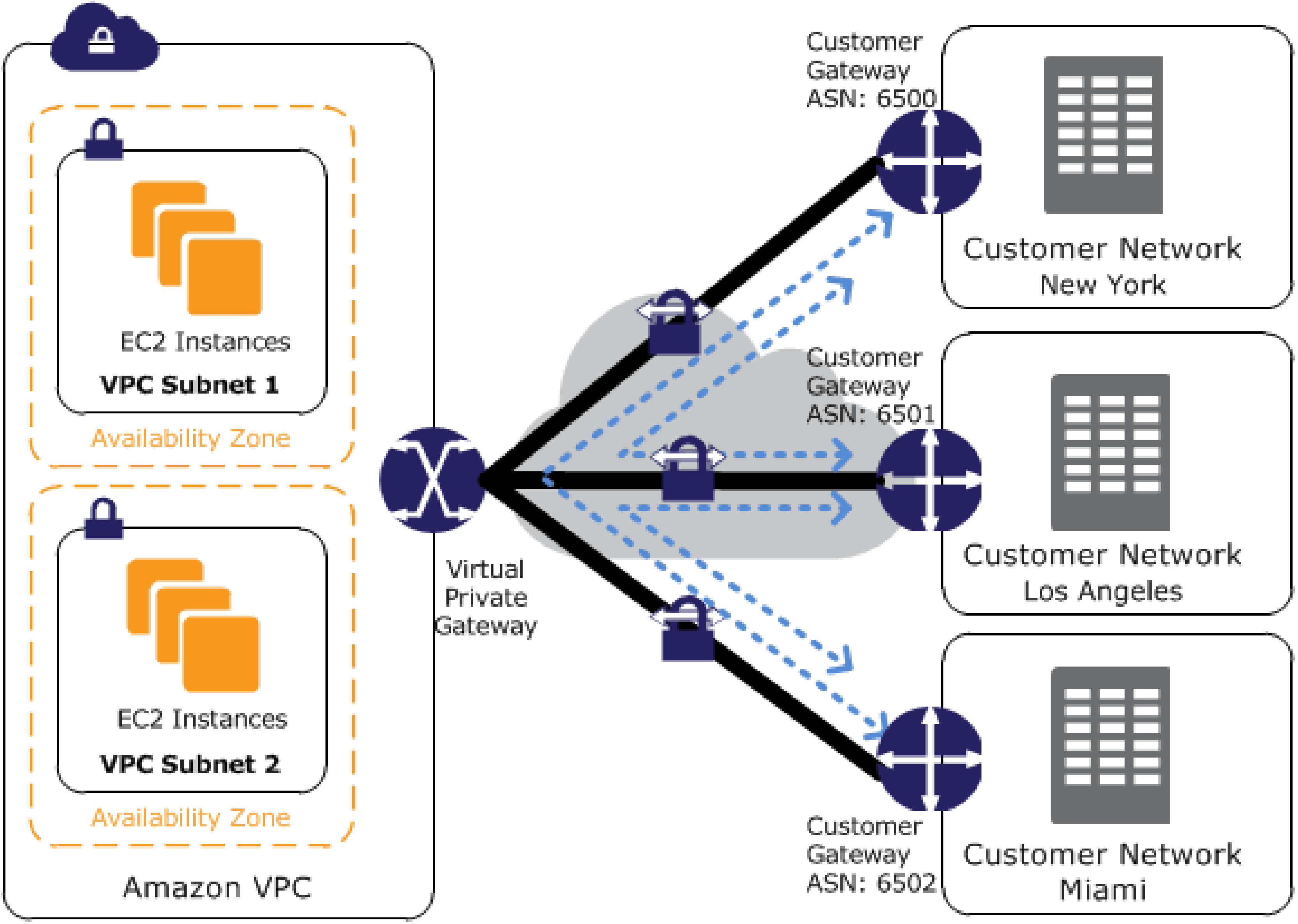
Now copy –admin UI and Client UI and paste in browser

5) Open client UI –download openvpn for windows –install it-and connect to openvpn server –user: openvpn, password –new

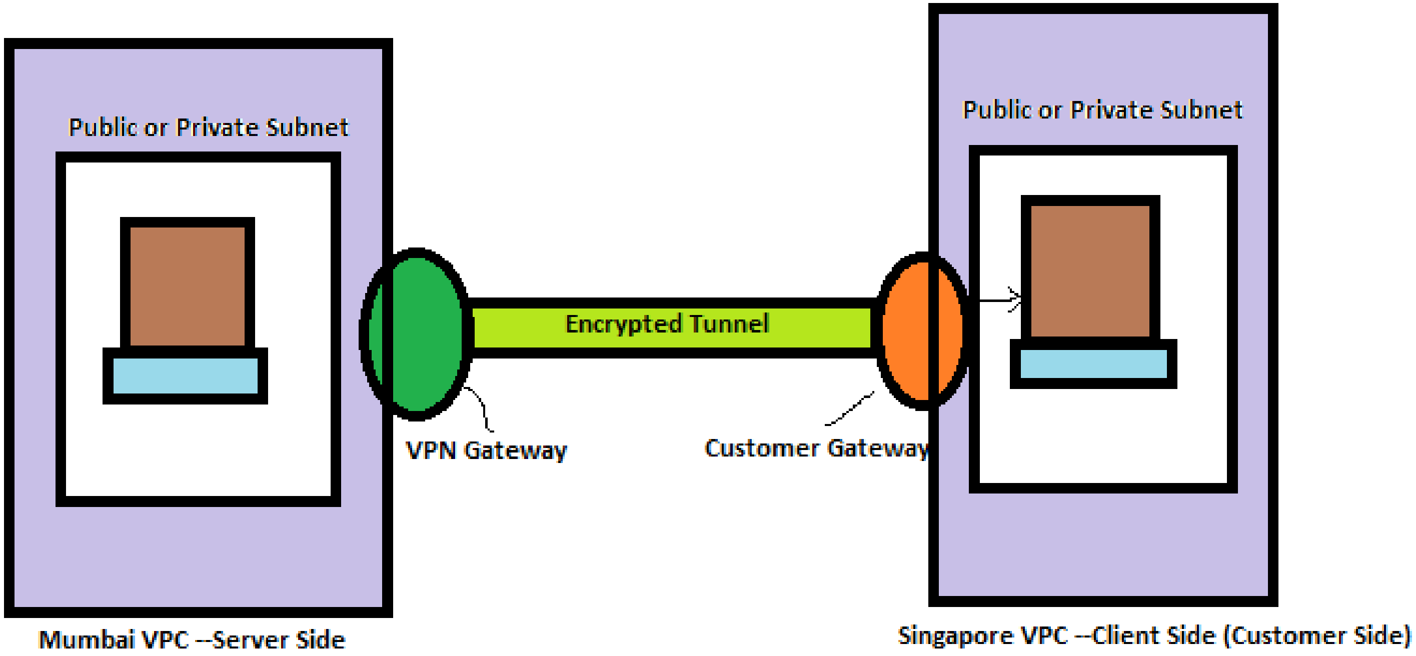
6) Now connect to your DB server directly using private IP


VPC-1
Public Subnet
open vpn server
Private Subnet
Route Table
public
Add route
Private
Route Table
subnet association
Internet Gateway
Internet
User


VPC
Any IP
VPN Connection
VPN Gateway
Public Subnet
172.16.10.0/24
Server 1
Private Subnet
172.16.11.0/24


Customer
Gateway
ASN: 6500
Customer Network
New York
EC2 Instances
VPC Subnet 1
Availability Zone
Customer
Gateway
ASN: 6501
Customer Network
Los Angeles
Virtual
Private
Gateway
EC2 Instances
VPC Subnet 2
Availability Zone
Customer
Gateway
ASN: 6502
Customer Network
Miami
Amazon VPC

Site to Site VPN



VPN Site to Site Lab Steps

1)Create two VPC –One in Mumbai and other in Singapore.

2) Create one-one Linux system in Mumbai and Singapore

Security Group –SSH, All TCP, ALL ICMP allowed

3) Go to Mumbai region and

→create Virtual Private Gateway

→create customer gateway –enter public ip of singapore ec2 instance

→create site to site vpn connection –add subnet of customer end

→go to route table----+ --route propagation

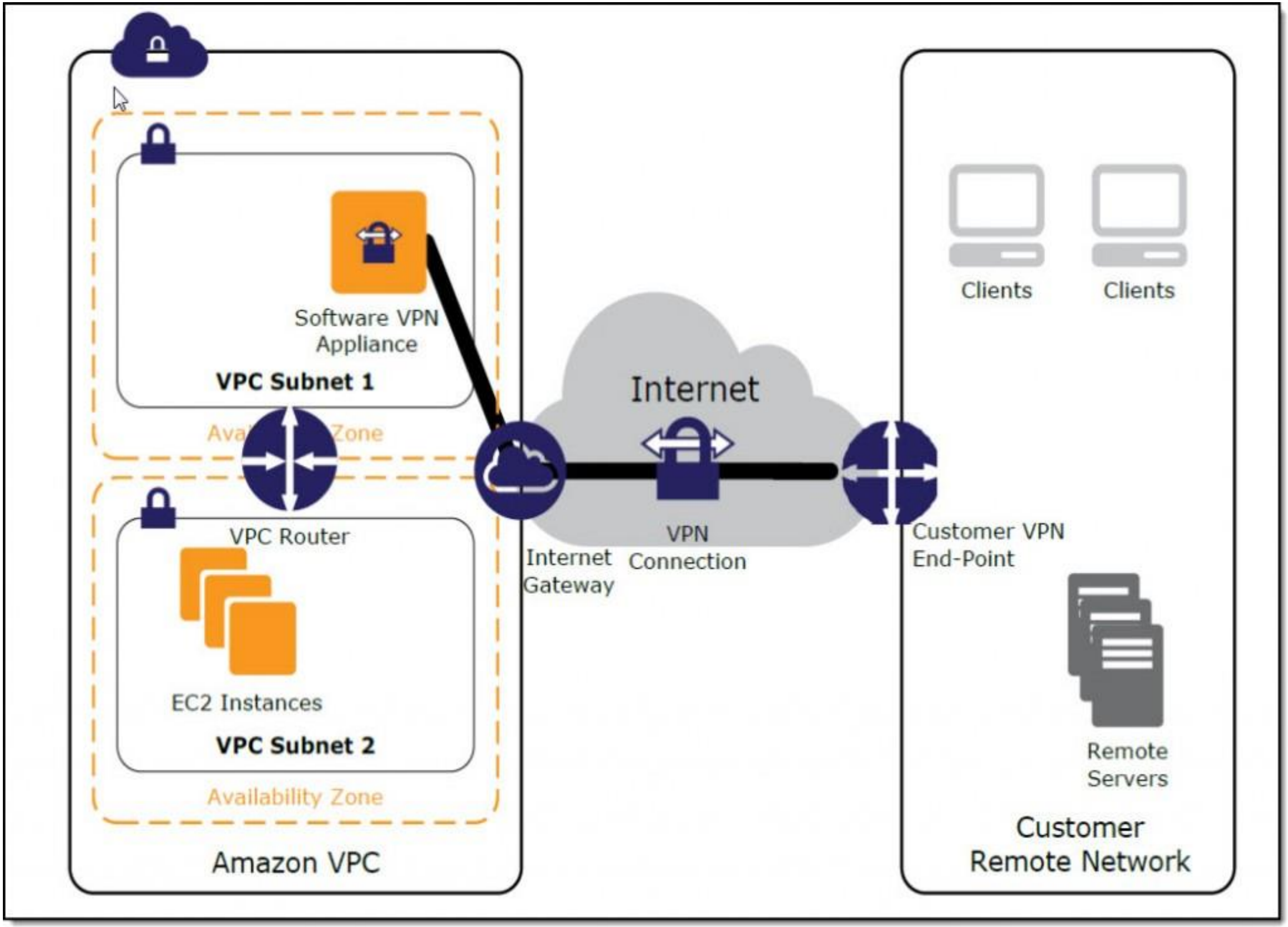
→site to site vpn –download configuration

VPN Lab Steps

4) Go to Singapore region and access your ec2 instance

Log on as : ec2-user

```
$ sudo su

# yum install openswan  -y

# nano /etc/ipsec.conf

# nano /etc/sysctl.conf

# service network restart

# nano /etc/ipsec.d/aws-vpn.conf

# nano /etc/ipsec.d/aws-vpn.secrets

#chkconfig ipsec  on

#service ipsec start
```


Software VPN
Appliance
VPC Subnet 1
Availability Zone
VPC Router
EC2 Instances
VPC Subnet 2
Availability Zone
Amazon VPC
Internet
Internet
Gateway
VPN
Connection
Clients
Clients
Customer VPN
End-Point
Remote
Servers
Customer
Remote Network

VPN Lab Steps

1)Create two VPC –One in Mumbai and other in Singapore

Term	VPC1	VPC2
VPC	Mumbaivpc(Server)	Singaporevpc(Client)
VPC-ID	172.16.0.0./16	172.17.0.0/16
Subnet1	Project1publicsubnet (172.16.1.0/24)	Project2publicsubnet (172.17.1.0/24)
Subnet2(optional)	Project1privatesubnet (172.16.2.0/24)	Project2privatesubnet (172.17.2.0/24)
Route Table	Mumbai-public-rt	Singapore-public-rt
Internet gateway	Internet gatewaymumbai	Internet gatewaysingapore

VPN Lab Steps

2) Create one-one Linux system in Mumbai and Singapore

Security Group –SSH, All TCP, ALL ICMP allowed

3) Go to Mumbai region and create Virtual Private Gateway

VPC—VPN --Virtual Private Gateway—name—Mumbai-VPG—create

Action –Attach to VPC –select mumbai-vpc—attach

4) Customer gateway –create Customer gateway –Name—Mumbai-CG –Routing-Static—IP address –paste singapore instance public ip ---create

5) Site to Site VPN—create VPN connection –Name: mumbai-singapore –Target gateway type: Virtual Private Gateway—select created VPG –Customer gateway –existing– select created customer gateway—Routing option –static –static IP prefix– singapore vpc-ip -- create VPN connection

Wait for 10 min for vpn connection completing

6) Route table –select mumbai-RT- Route Propagation—Edit—select propagate—save

7) Site to Site VPN – download configuration –Vendor-openswan--download

VPN Lab Steps-In singapore

4) Go to Singapore region and access your ec2 instance

Log on as : ec2-user

```
$ sudo su
```

```
# yum install openswan  -y
```

```
# nano /etc/ipsec.conf
```

Make sure the last line should not have comment --/etc/ipsec.d/*.conf

```
#nano /etc/sysctl.conf   ---update these lines at the end
```

```
net.ipv4.ip_forward = 1

net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.all.send_redirects = 0
```

VPN Lab Steps-In singapore

```
#service network restart
#nano  /etc/ipsec.d/aws-vpn.conf
conn Tunnel1
        authby=secret
        auto=start
        left=%defaultroute
        leftid=Customer end Gateway VPN public IP
        right=AWS Virtual private gateway ID- public IP
        type=tunnel
        ikelifetime=8h
        keylife=1h
        phase2alg=aes128-sha1;modp1024
        ike=aes128-sha1;modp1024
        keyingtries=%forever
        keyexchange=ike
        leftsubnet=Customer end VPN CIDR
        rightsubnet=AWS end VPN CIDR
        dpddelay=10
        dpdtimeout=30
        dpdaction=restart_by_peer
```

VPN Lab Steps-In singapore

```
#nano /etc/ipsec.d/aws-vpn.secrets
customer_public_ip aws_vgw_public_ip: PSK "shared secret“
18.141.196.10  13.127.199.95: PSK "Qyf3xrZpMOZTUHX7bEGv0b308IXgUr1d“
#systemctl start ipsec
#systemctl  enable ipsec
# systemctl status ipsec
```

Now tunnel is created

How to check

In mumbai –VPC---Site to Site VPN—Tunnel detail—we are getting one tunnel is UP

Go to singapore ec2 instance and ping the mumbai ec2 instanc eby using its private IP