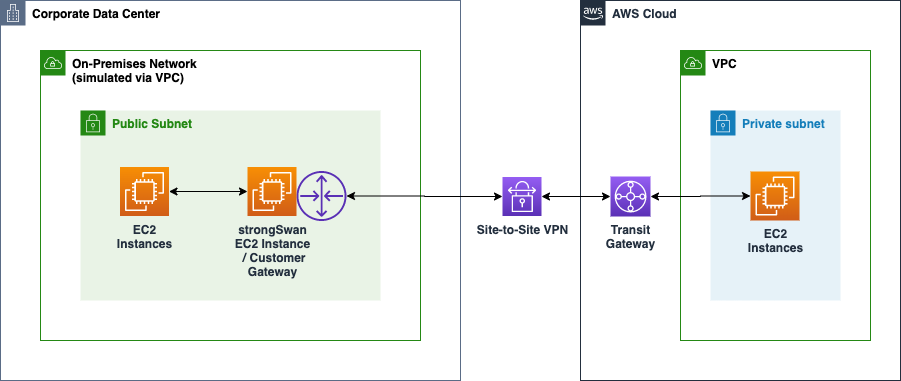
* AWS Site-to-Site VPN enables you to securely connect your on-premises network or branch office site to your Amazon Virtual Private Cloud (Amazon VPC). AWS Client VPN enables you to securely connect users to AWS or on-premises networks.



* By default, instances that you launch into an Amazon VPC can't communicate with your own (remote) network. You can enable access to your remote network from your VPC by creating an AWS Site-to-Site VPN (Site-to-Site VPN) connection, and configuring routing to pass traffic through the connection.
* Although the term *VPN connection* is a general term, in this documentation, a VPN connection refers to the connection between your VPC and your own on-premises network. Site-to-Site VPN supports Internet Protocol security (IPsec) VPN connections.
* Your Site-to-Site VPN connection is either an AWS Classic VPN or an AWS VPN. For more information, see [Site-to-Site VPN categories](https://docs.aws.amazon.com/vpn/latest/s2svpn/vpn-categories.html).

## 

## 

## **Concepts**

**The following are the key concepts for Site-to-Site VPN:**

* VPN connection: A secure connection between your on-premises equipment and your VPCs.
* VPN tunnel: An encrypted link where data can pass from the customer network to or from AWS.  
  Each VPN connection includes two VPN tunnels which you can simultaneously use for high availability.
* Customer gateway: An AWS resource which provides information to AWS about your customer gateway device.
* Customer gateway device: A physical device or software application on your side of the Site-to-Site VPN connection.
* Target gateway: A generic term for the VPN endpoint on the Amazon side of the Site-to-Site VPN connection.
* Virtual private gateway: A virtual private gateway is the VPN endpoint on the Amazon side of your Site-to-Site VPN connection that can be attached to a single VPC.
* Transit gateway: A transit hub that can be used to interconnect multiple VPCs and on-premises networks, and as a VPN endpoint for the Amazon side of the Site-to-Site VPN connection.

**Working with Site-to-Site VPN**

You can create, access, and manage your Site-to-Site VPN resources using any of the following interfaces:

* AWS Management Console— Provides a web interface that you can use to access your Site-to-Site VPN resources.
* AWS Command Line Interface (AWS CLI) — Provides commands for a broad set of AWS services, including Amazon VPC, and is supported on Windows, macOS, and Linux. For more information, see [AWS Command Line Interface](https://aws.amazon.com/cli/).
* AWS SDKs — Provide language-specific APIs and takes care of many of the connection details, such as calculating signatures, handling request retries, and error handling. For more information, see [AWS SDKs](https://aws.amazon.com/tools/#SDKs).
* Query API— Provides low-level API actions that you call using HTTPS requests. Using the Query API is the most direct way to access Amazon VPC, but it requires that your application handle low-level details such as generating the hash to sign the request, and error handling. For more information, see the [Amazon EC2 API Reference](https://docs.aws.amazon.com/AWSEC2/latest/APIReference/).

**Site-to-Site VPN limitations**

A Site-to-Site VPN connection has the following limitations.

* IPv6 traffic is not supported for VPN connections on a virtual private gateway.
* An AWS VPN connection does not support Path MTU Discovery.In addition, take the following into consideration when you use Site-to-Site VPN.
* When connecting your VPCs to a common on-premises network, we recommend that you use non-overlapping CIDR blocks for your networks.

**1. How to create aws site to site vpn and get access.**

1. Create two vpc

* Mumbai region
* Singapore (customerend)

1. Create linux machine in both the vpc take RDP of it

(security group-ssh,tcp,all icmp)

1. Go to Mumbai region service **>** vpc **>** vpn

* Create virtual private gateway.
* Create customer gateway .(configure public ip of singapore ec2 instance)
* Create site to site vpn 

1. Go to route table - route propagation

Download configuration

6) Go to singapore region take access of ec2 using Putty.

7) command

* ec2-user
* sudo su
* yum install openswan -y
* vim /etc/ipsec.conf
* vim /etc/sysctl.conf

net.ipv4.ip\_forward = 1

net.ipv4.conf.all.accept\_redirects = 0

net.ipv4.conf.all.send\_redirects = 0

* service network restart
* vim /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

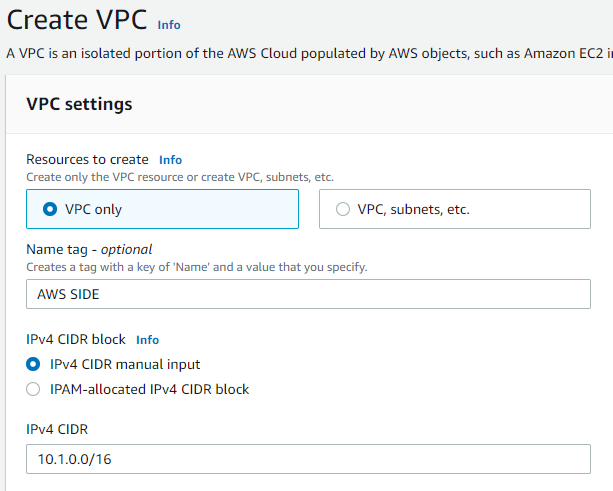
* vim /etc/ipsec.d/aws-vpn.secrets

customer\_public\_ip aws\_vgw\_public\_ip: PSK "shared secret"

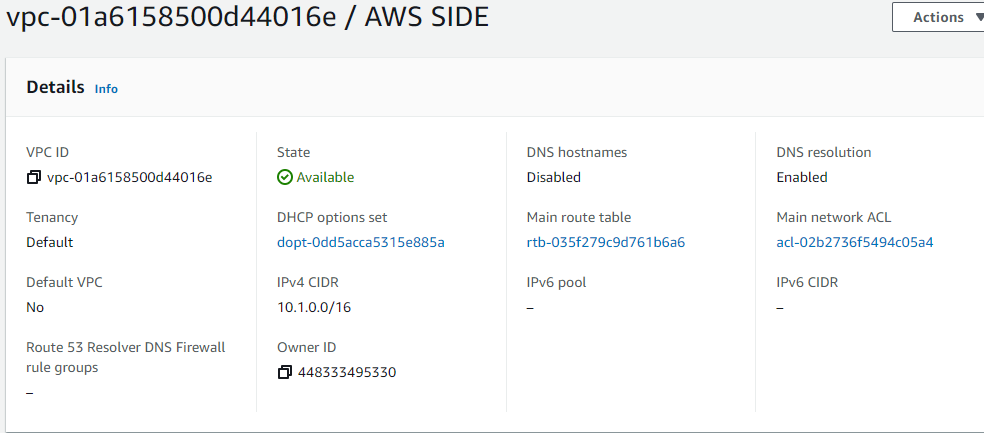
* chkconfig ipsec on
* service ipsec start
* service ipsec status
* ping 8.8.8.8

**1.1 create vpc,subnet,internet gateway,route table in mumbai region.**

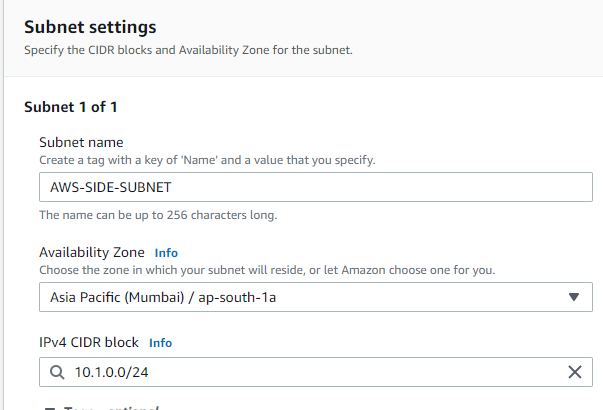
1. Vpc



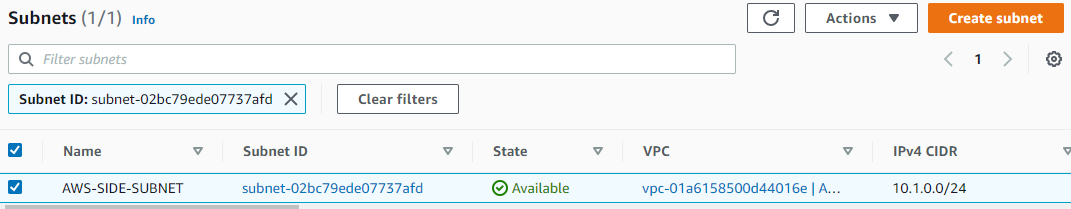




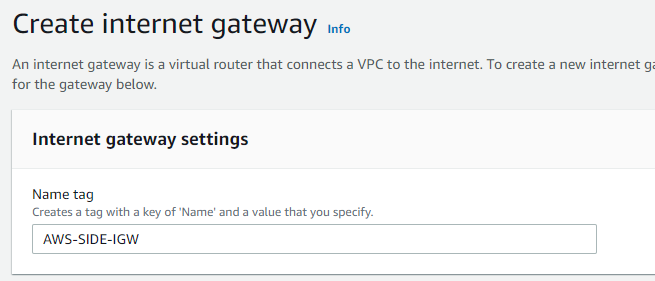
1. Subnet



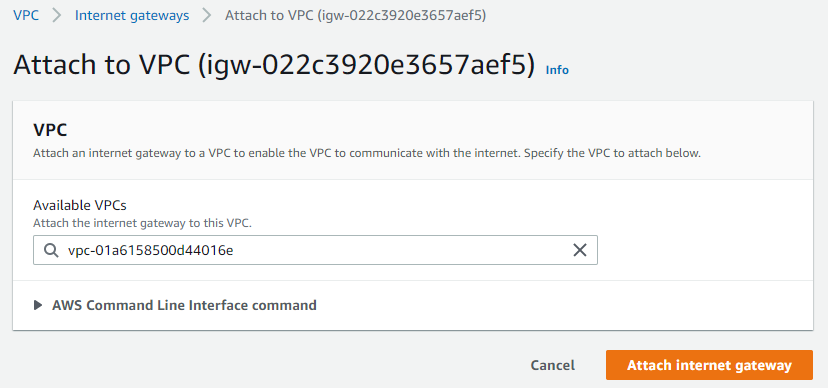




1. Internet gateway.



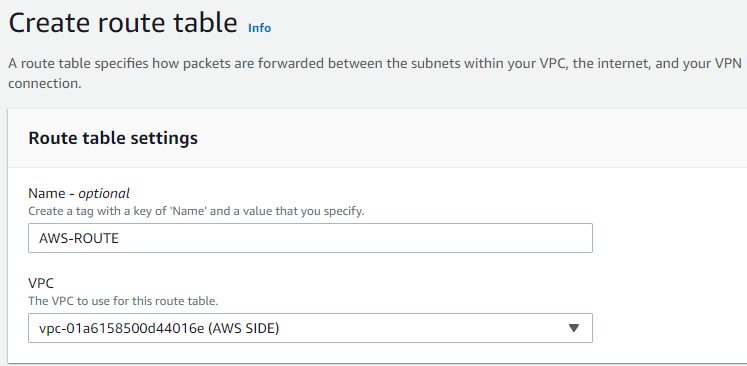




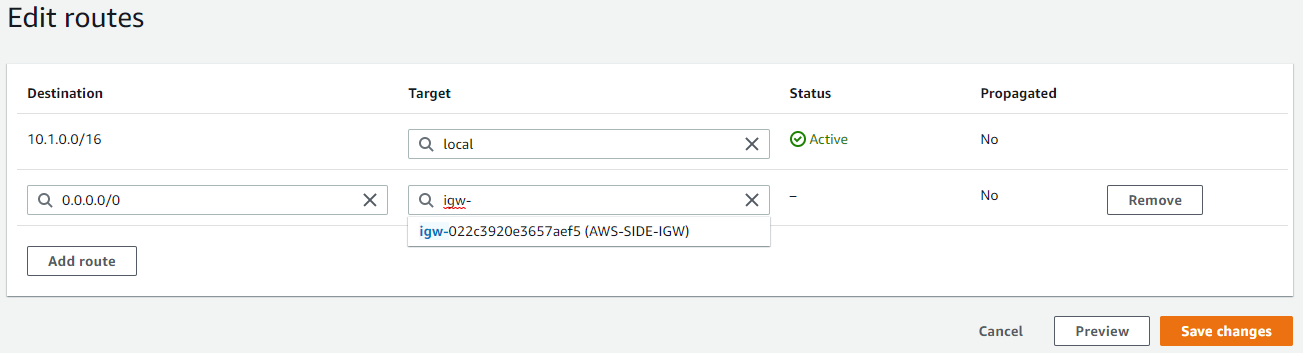




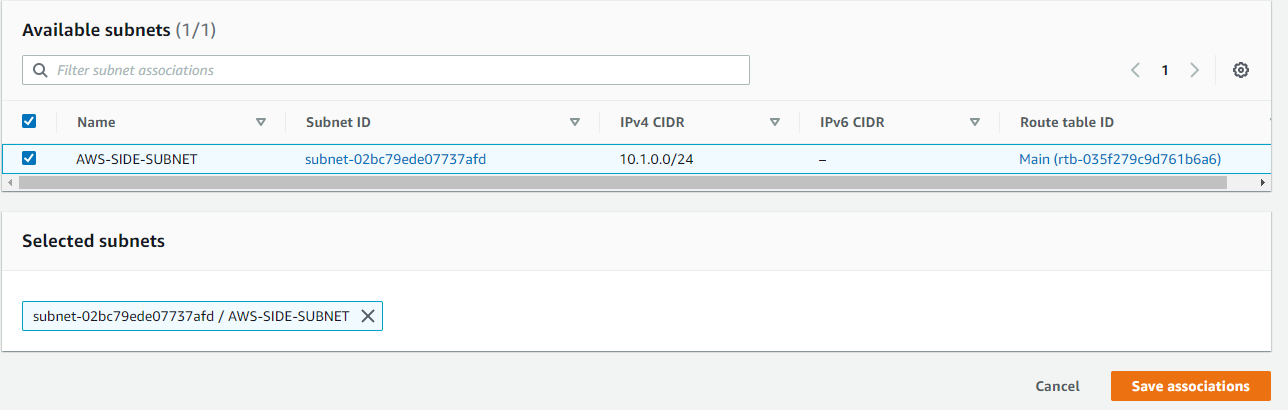
1. Route table





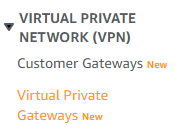






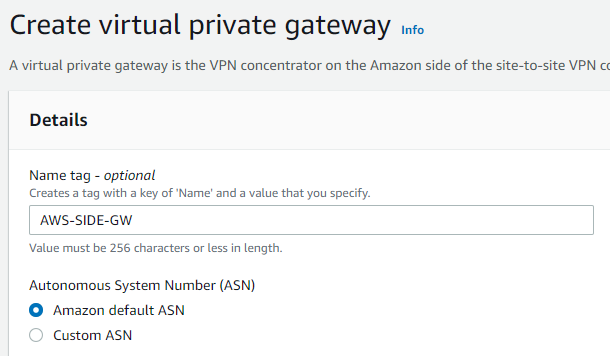
**1.2 create virtual private network (vpn)** aws console management **>** service **>** vpc

**>** virtual private network.

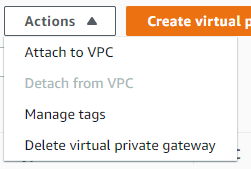
1. 



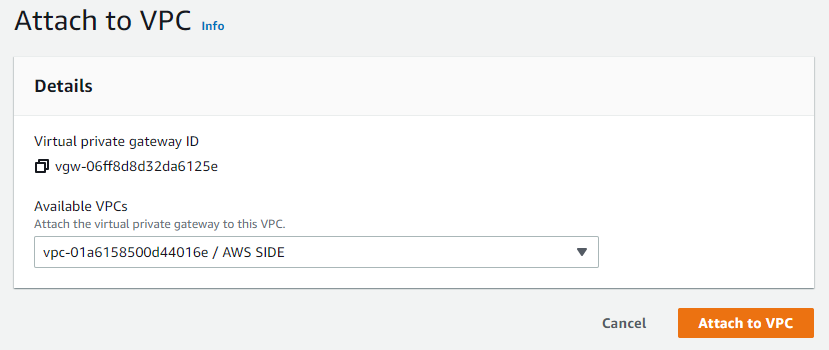






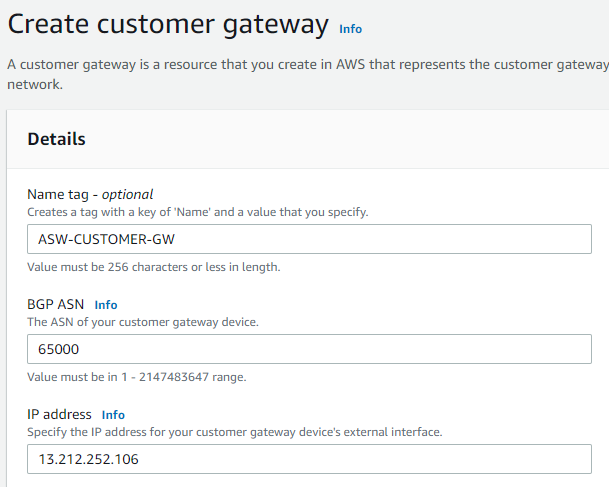


1. Attach to the vpc .

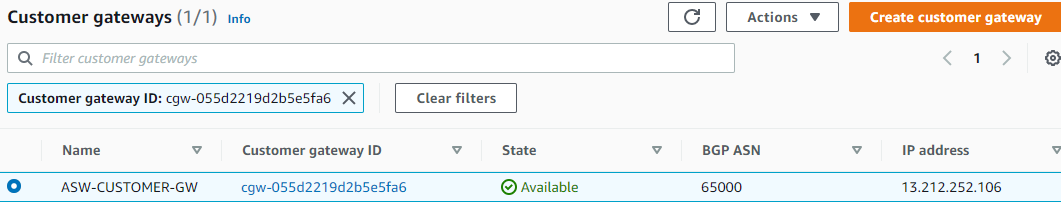


**1.3 create customer gateway .**

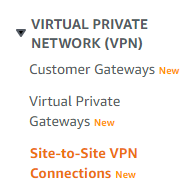
1. 



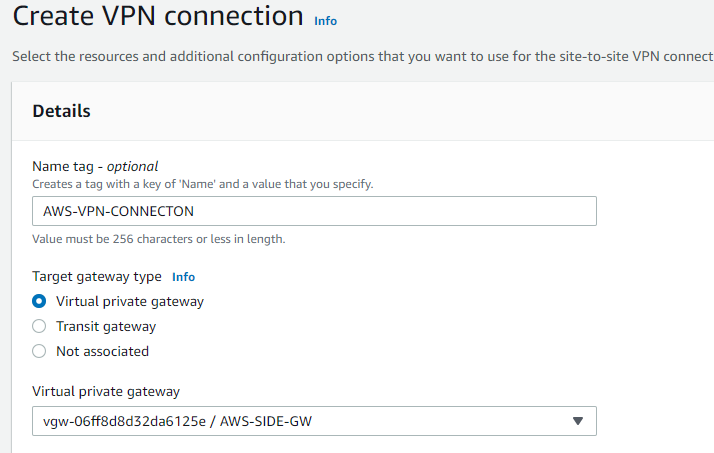




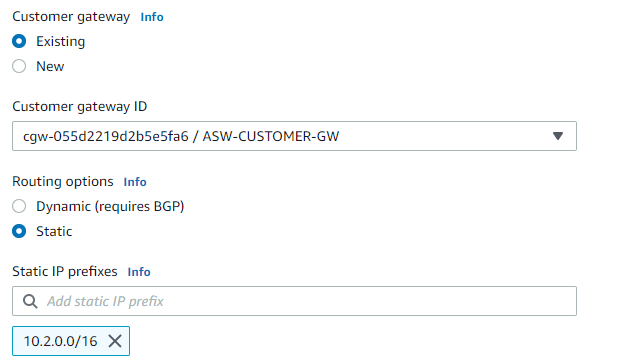
**1.4 create site to site connection:**

1. 

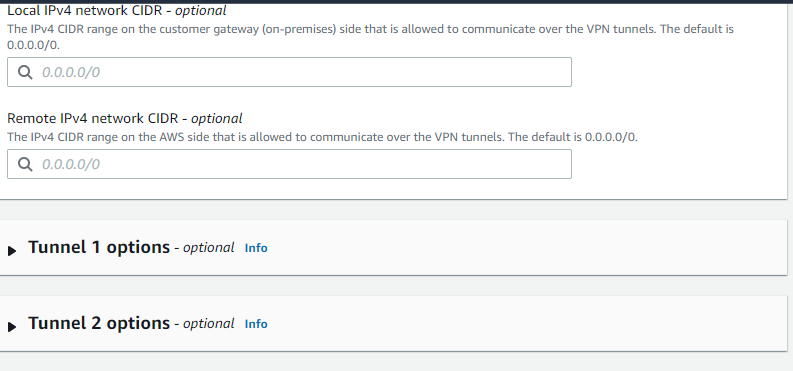




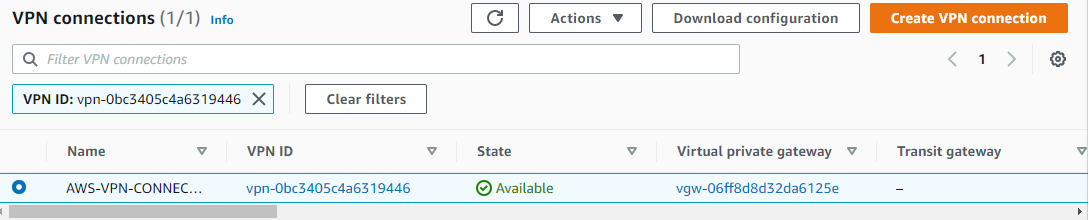




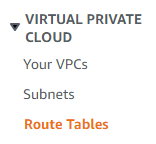


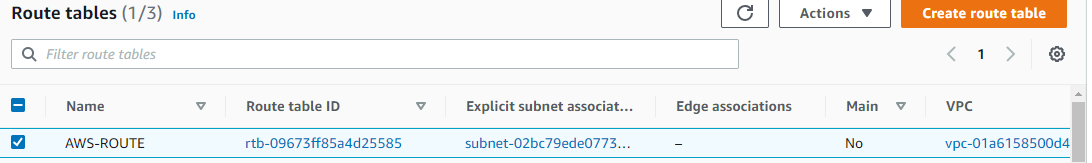


1. After creation of site to site connection **download configuration file.**

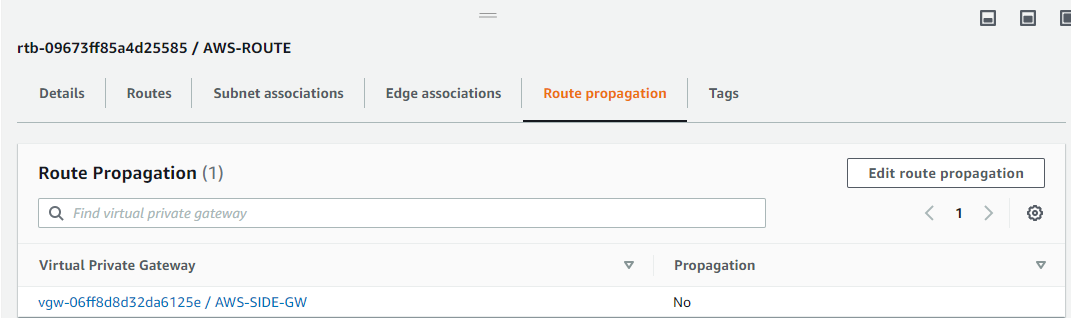


**1.5 Go to route table > route propagation**

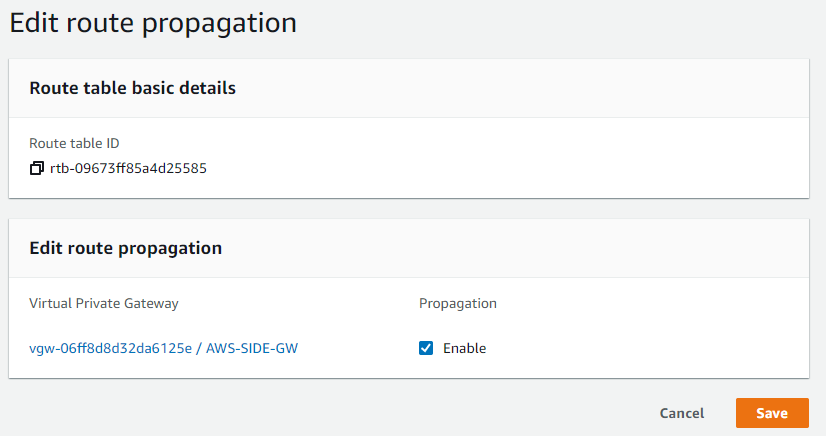
1. 





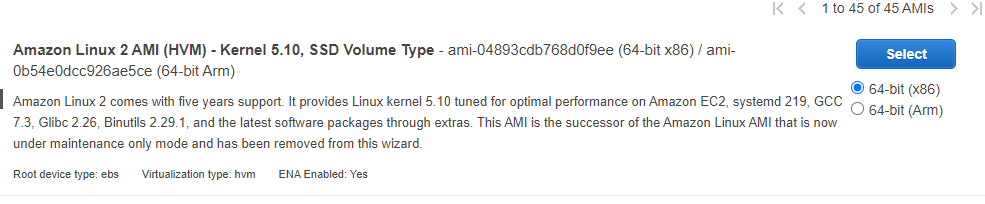


1. Enable route-propagation



**1.6 Create linux machine in Mumbai region**

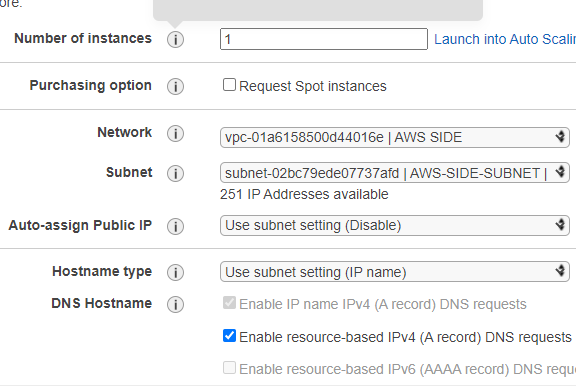
1. 



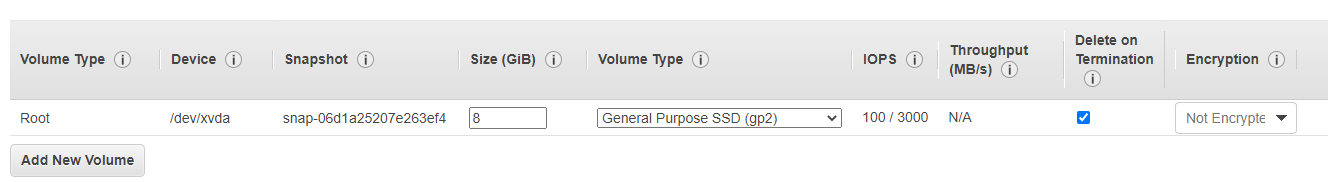




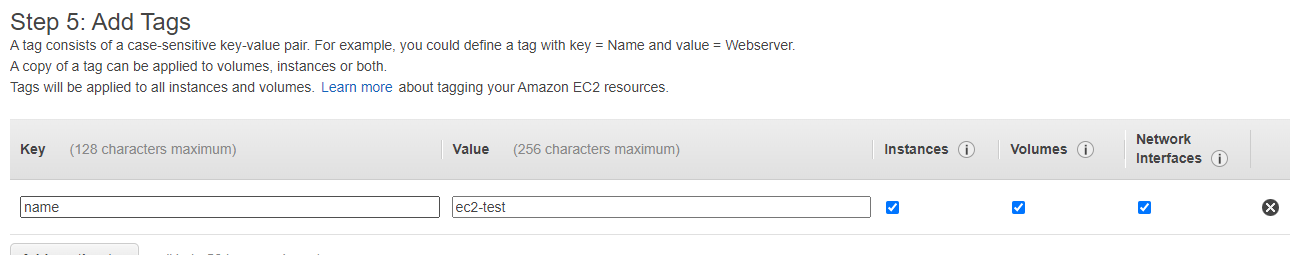




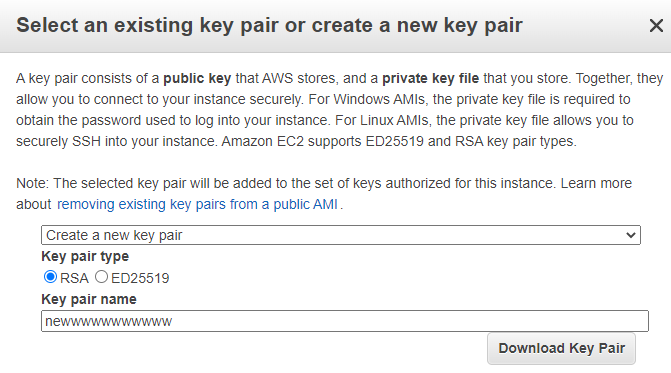




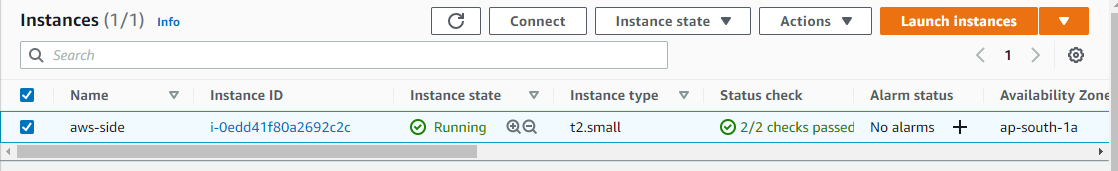




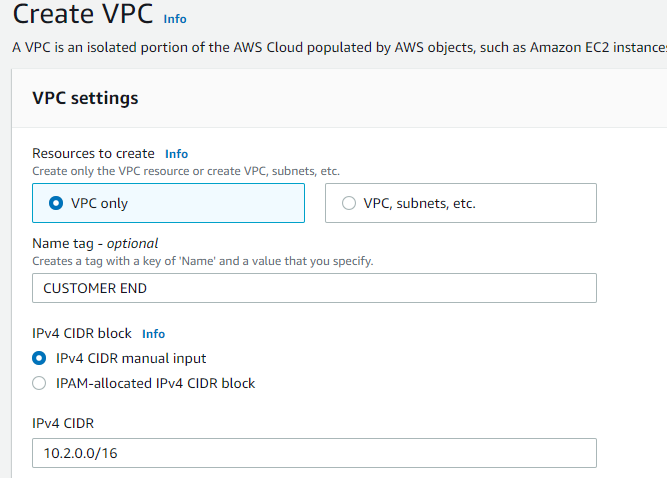


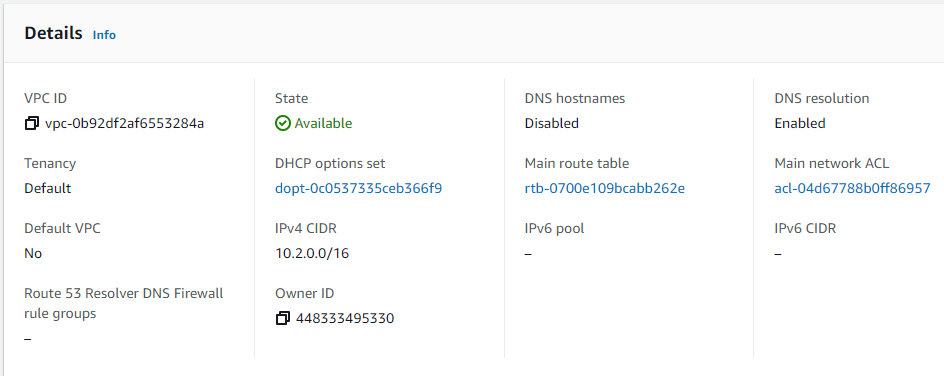




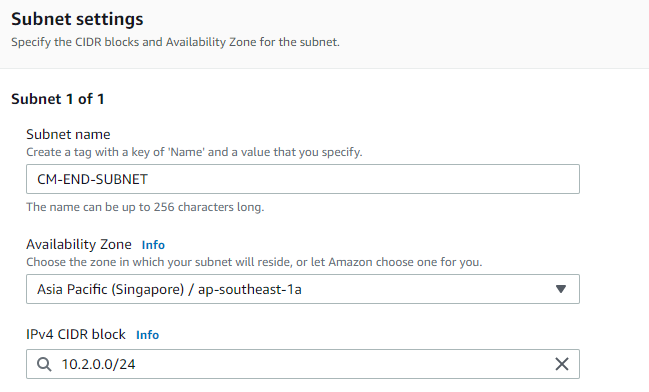


**1.7 Create vpc,subnet,internet gateway,route table.**

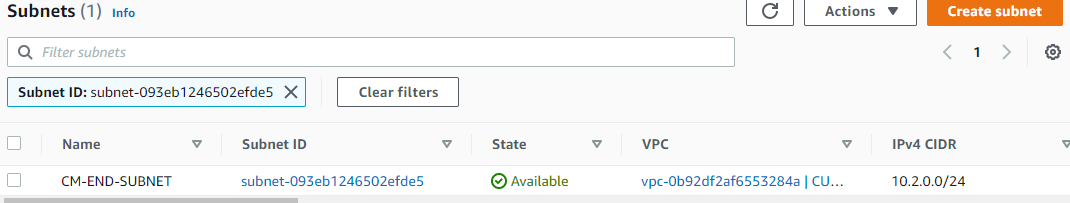
1. **Vpc** 



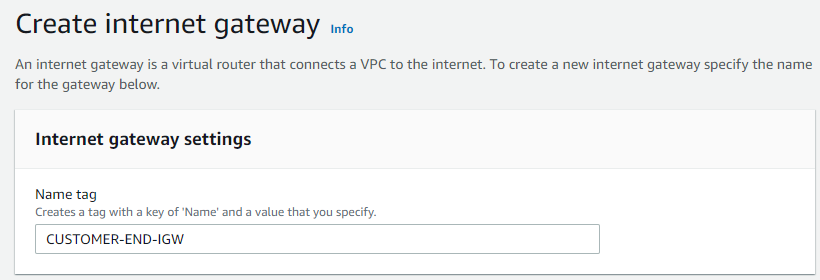
1. Subnet



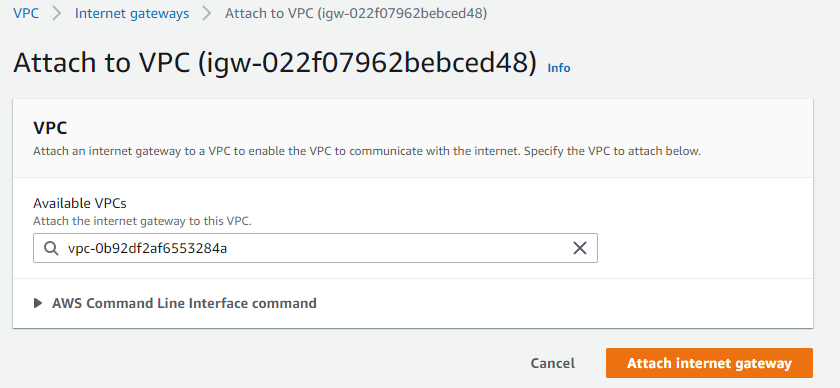




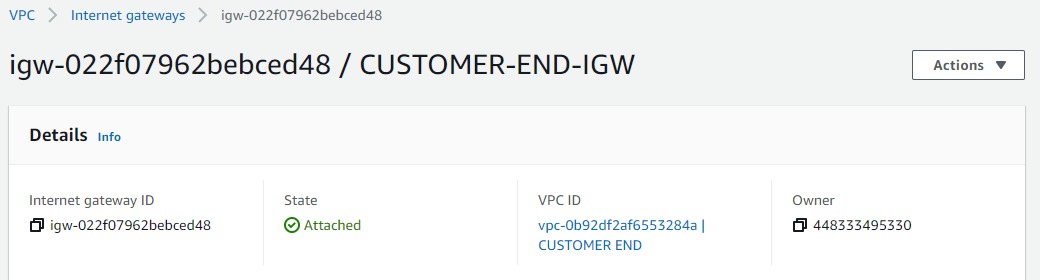
1. Internet gateway



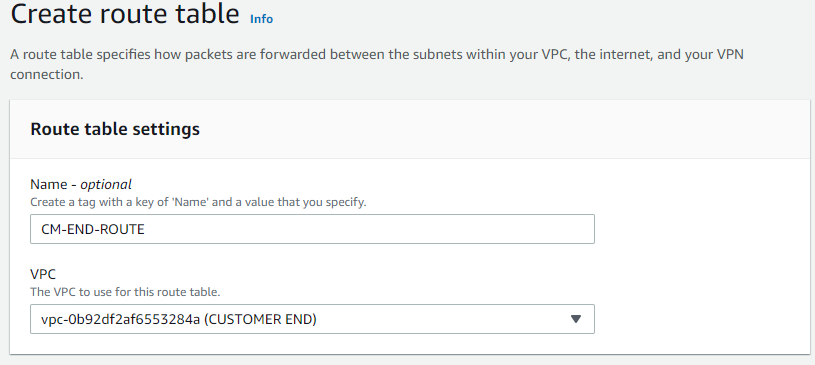




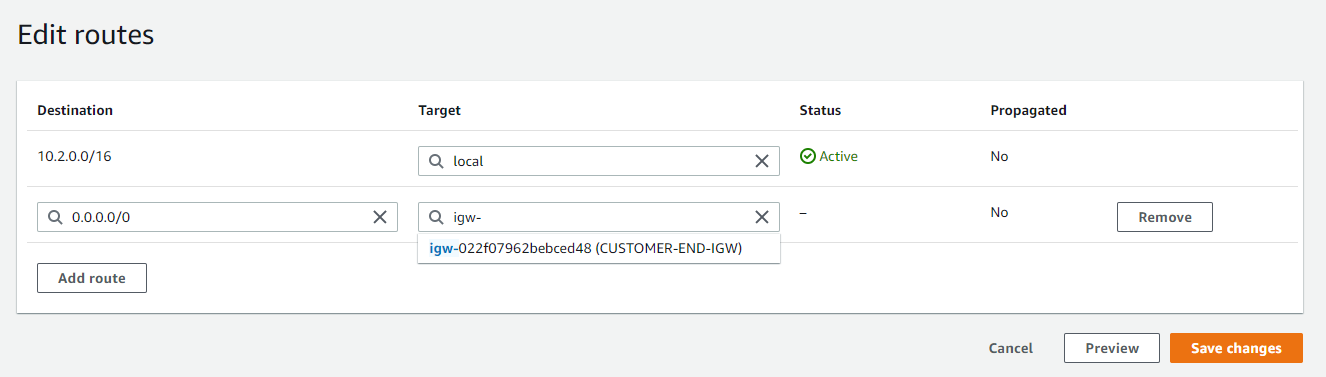




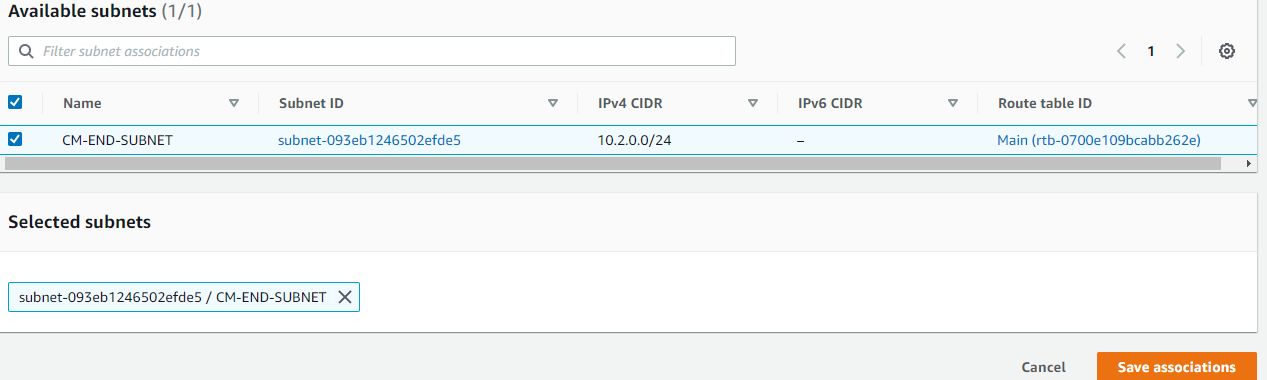
1. Route table



1. Route to internet gateway



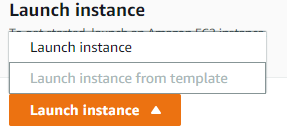
1. Associate the subnet to the route.



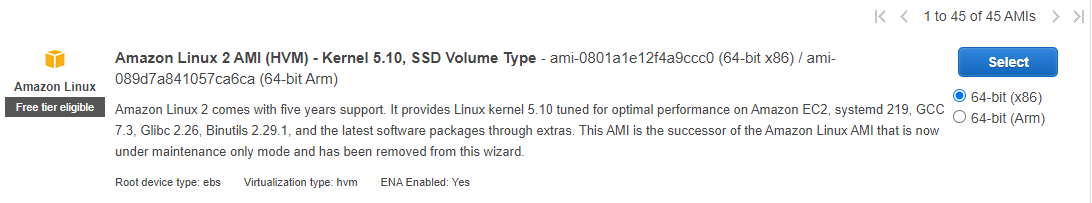
1. Successfully created of vpc in singapore region.



**1.8 launch linux ec2 instance in singapore region with created vpc**



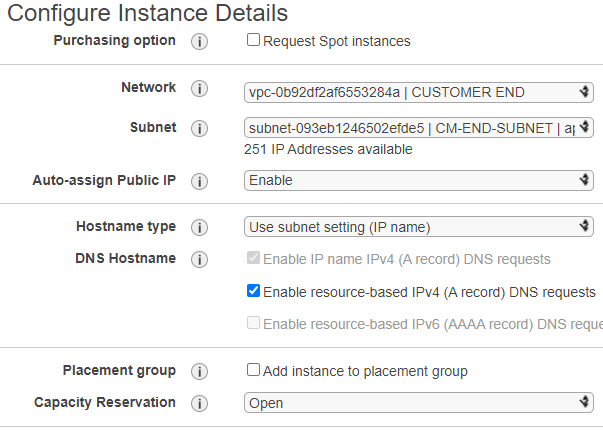




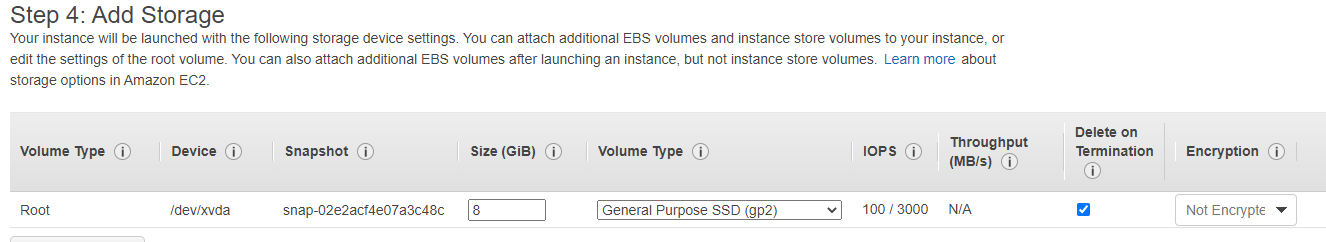




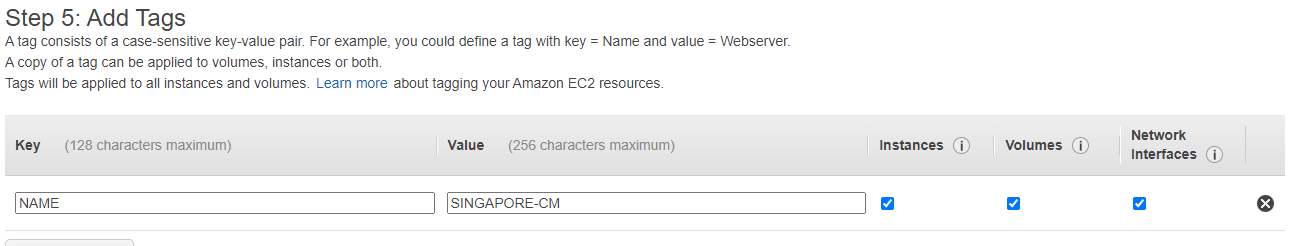




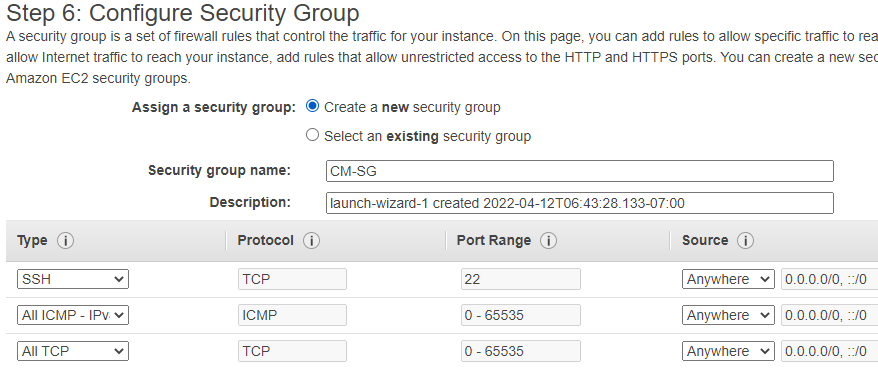




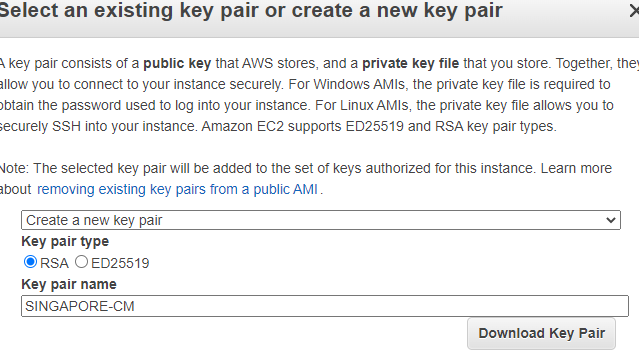




1. Configure security group - SSH, ALL ICMP,ALL TCP



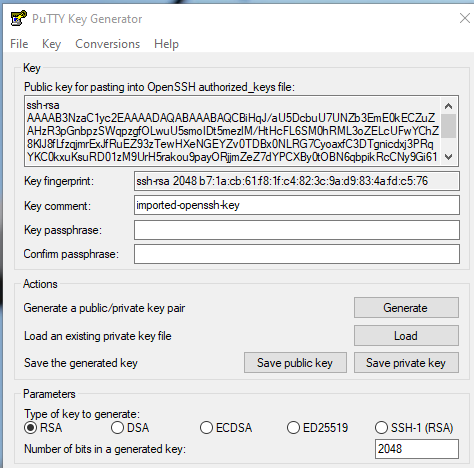
1. Download key pair



1. Get access of the linux machine.

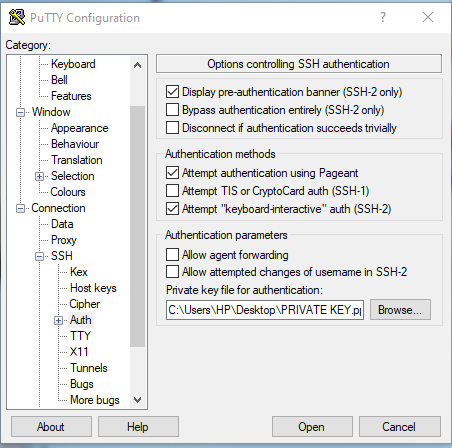




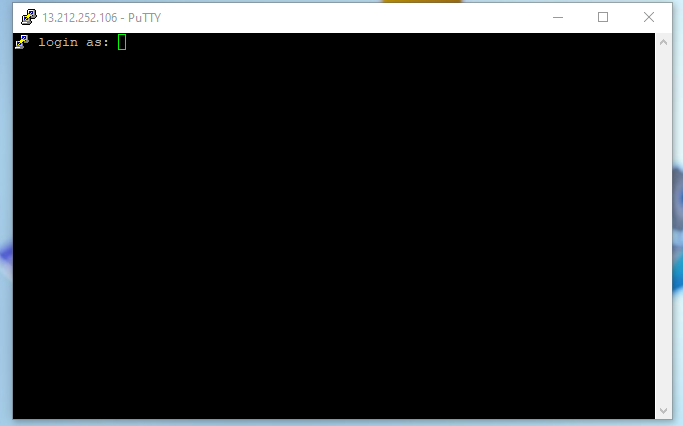




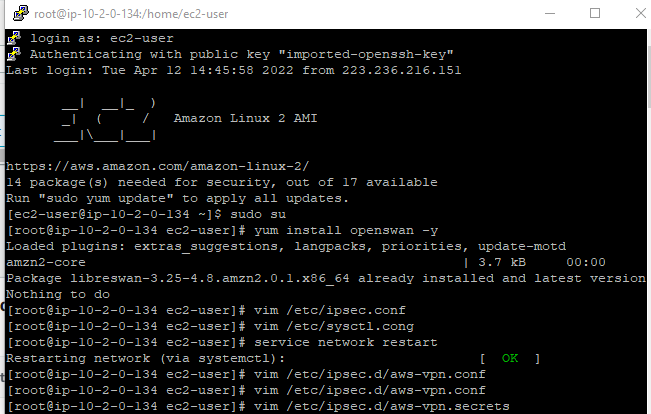




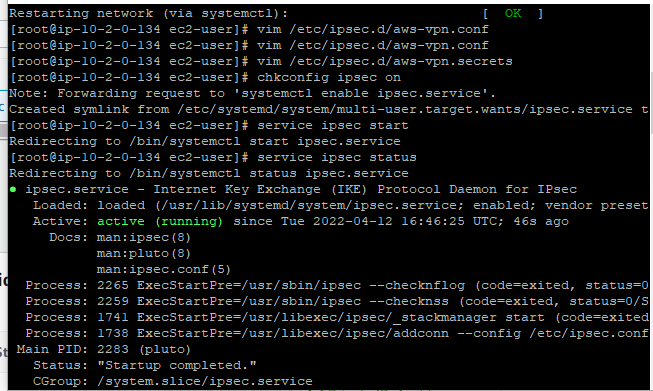




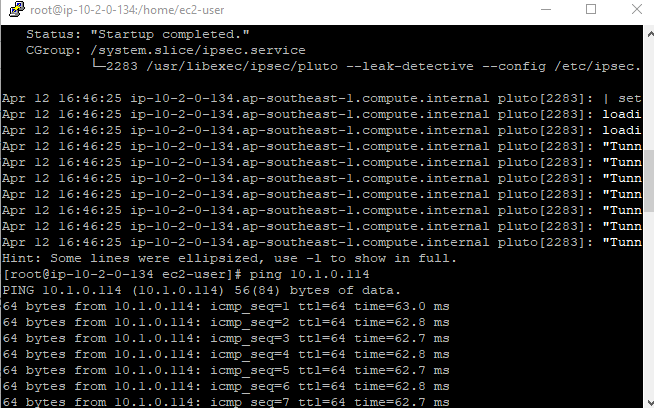




1. Vpn status is shown active running



1. Ping From singapore region to mumbai region , it respond .



**Thank you**