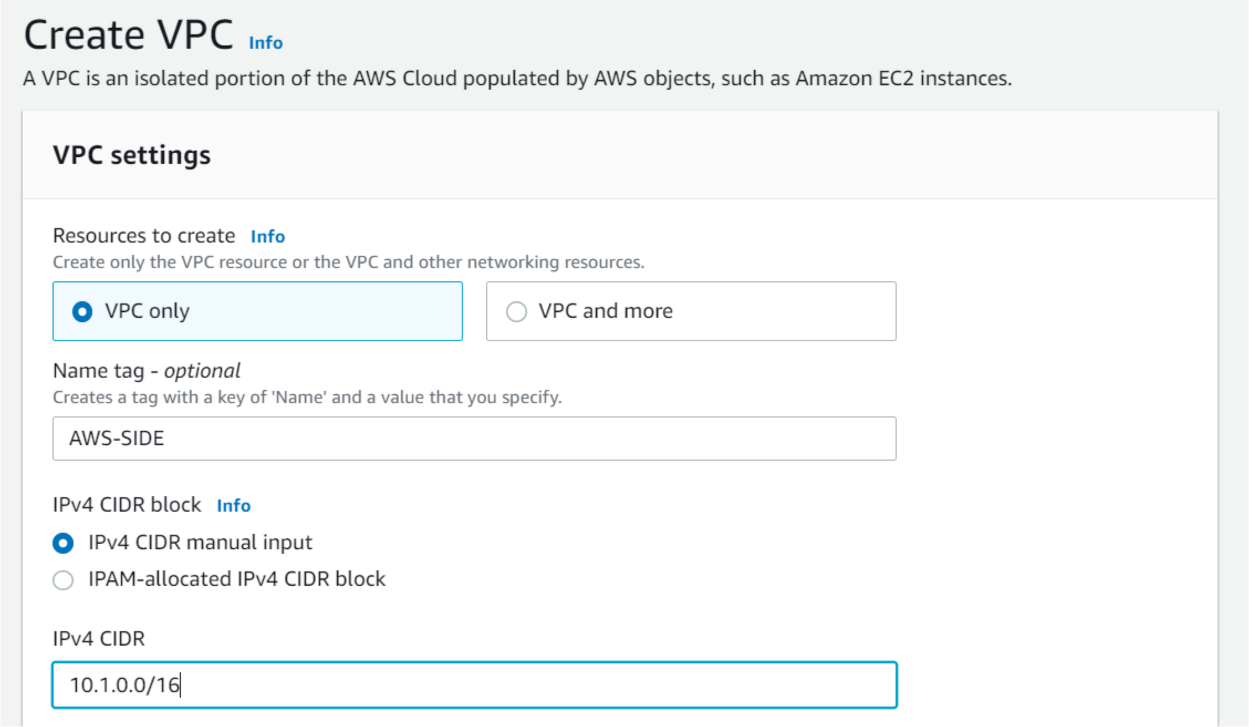
Atharv Bhogale – AWS SAA 20th August, 2022 – Batch

VPC – Site to site VPN Lab

VPC – Site to Site VPN Lab.

Let’s Start…

Creating VPC in Mumbai Region.



Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.

● VPC only ○ VPC and more

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.

AWS-SIDE

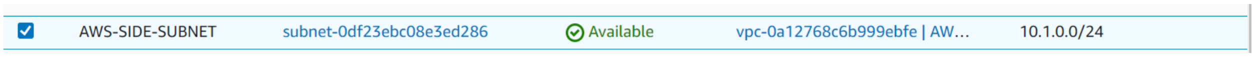
IPv4 CIDR block Info

● IPv4 CIDR manual input
○ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

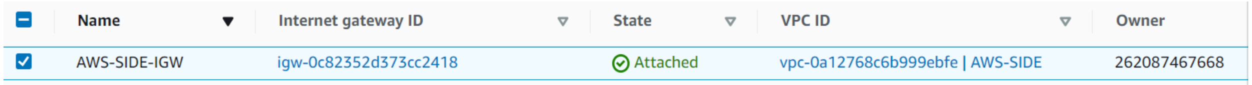
10.1.0.0/16

Subnet created



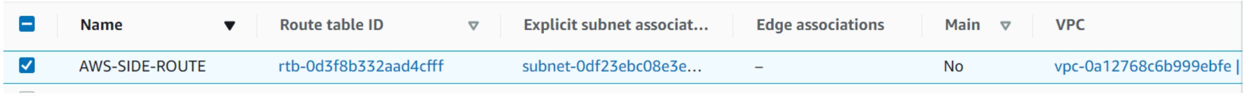
☑	AWS-SIDE-SUBNET	subnet-0df23ebc08e3ed286	✓ Available	vpc-0a12768c6b999ebfe | AW…	10.1.0.0/24

Internet Gateway created and attached to VPC



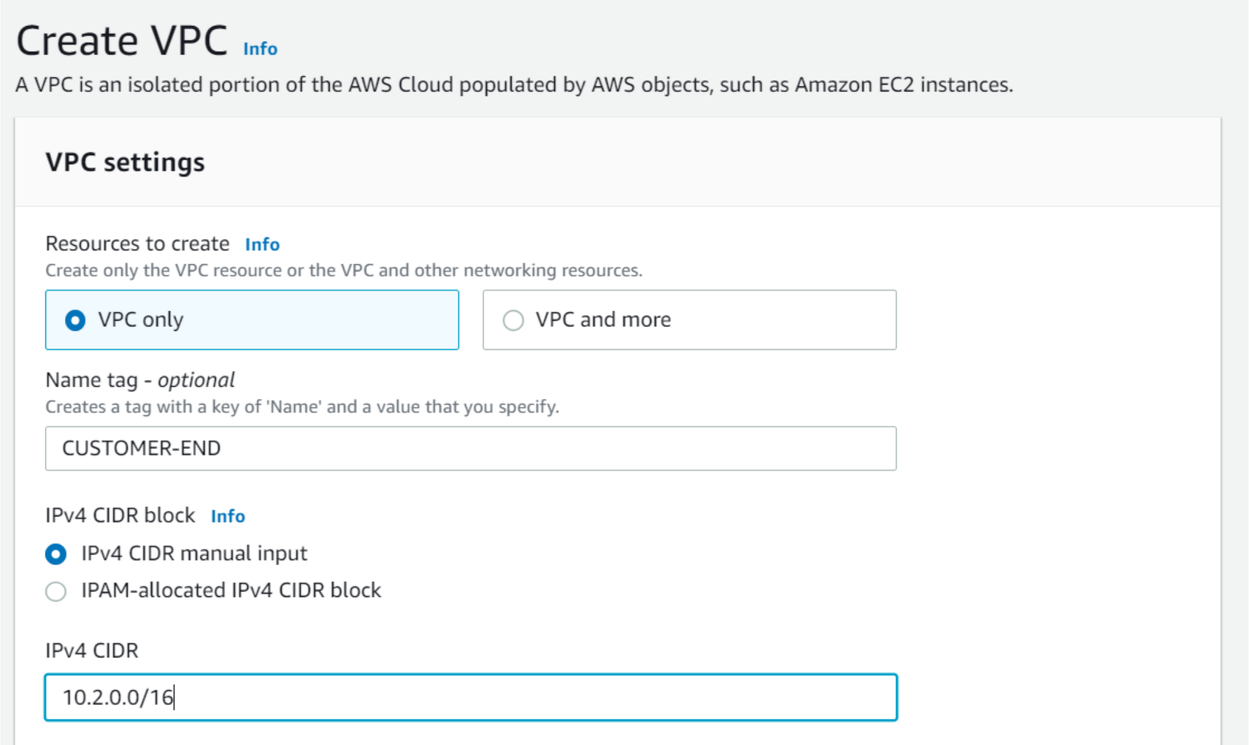
▬	Name	Internet gateway ID	State	VPC ID	Owner
☑	AWS-SIDE-IGW	igw-0c82352d373cc2418	✓ Attached	vpc-0a12768c6b999ebfe | AWS-SIDE	262087467668

Route Table created and association is done, also route is defined towards internet.



▬	Name	Route table ID	Explicit subnet associat…	Edge associations	Main	VPC
☑	AWS-SIDE-ROUTE	rtb-0d3f8b332aad4cfff	subnet-0df23ebc08e3e…	–	No	vpc-0a12768c6b999ebfe |

Now, I will create a VPC in Singapore region.



Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create Info

Create only the VPC resource or the VPC and other networking resources.

● VPC only ○ VPC and more

Name tag - *optional*

Creates a tag with a key of 'Name' and a value that you specify.

CUSTOMER-END

IPv4 CIDR block Info

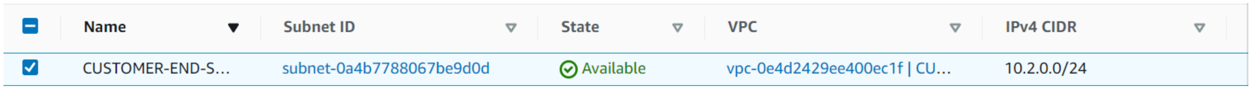
● IPv4 CIDR manual input

○ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

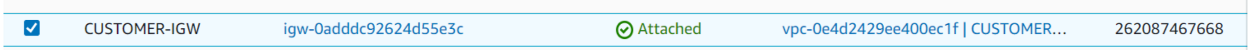
10.2.0.0/16

Subnet created



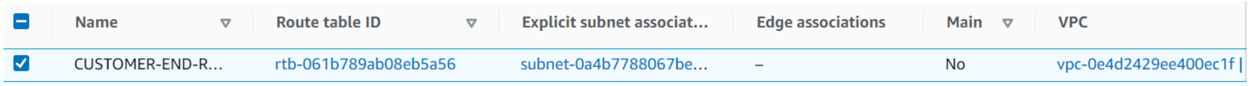
☐	Name	Subnet ID	State	VPC	IPv4 CIDR
☑	CUSTOMER-END-S…	subnet-0a4b7788067be9d0d	✓ Available	vpc-0e4d2429ee400ec1f | CU…	10.2.0.0/24

Internet Gateway created and attached to VPC



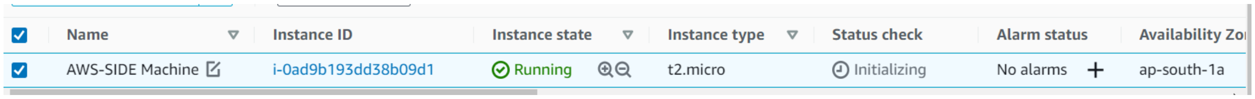
☑	CUSTOMER-IGW	igw-0adddc92624d55e3c	✓ Attached	vpc-0e4d2429ee400ec1f | CUSTOMER…	262087467668

Route Table created and association is done, also route is defined towards internet.

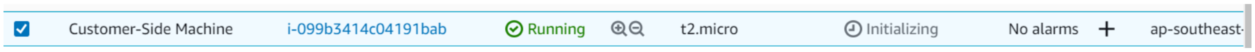


☐	Name	Route table ID	Explicit subnet associat…	Edge associations	Main	VPC
☑	CUSTOMER-END-R…	rtb-061b789ab08eb5a56	subnet-0a4b7788067be…	–	No	vpc-0e4d2429ee400ec1f |

Now, I will create linux EC2 instances in both VPCs



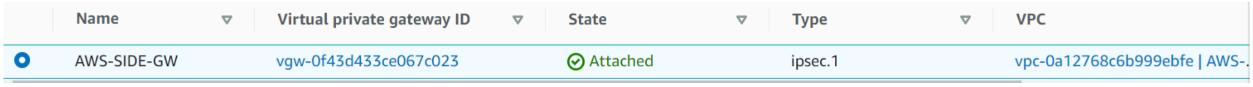
☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zo
☑	AWS-SIDE Machine	i-0ad9b193dd38b09d1	✓ Running	t2.micro	Initializing	No alarms +	ap-south-1a



☑	Customer-Side Machine	i-099b3414c04191bab	✓ Running	t2.micro	Initializing	No alarms +	ap-southeast-

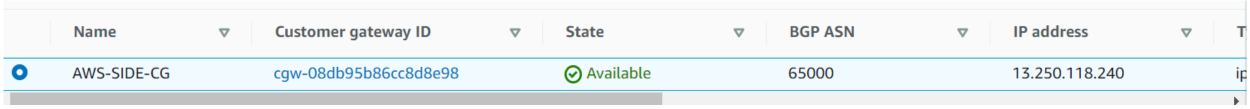
Mumbai region VPC is AWS side VPC & Singapore region VPC is customer side VPC.

Let’s create Virtual Private Gateway in Mumbai region and attach it to VPC.



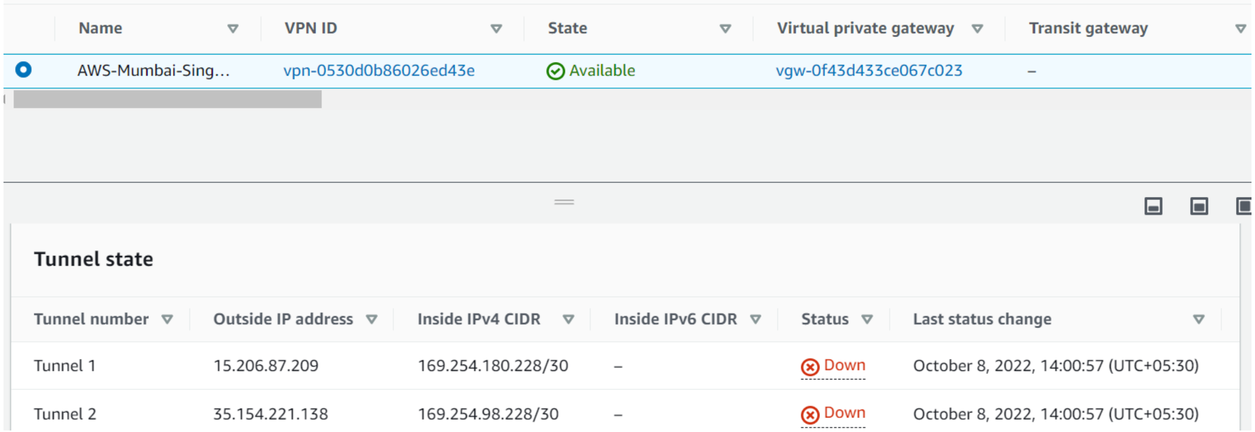
	Name	Virtual private gateway ID	State	Type	VPC
●	AWS-SIDE-GW	vgw-0f43d433ce067c023	✓ Attached	ipsec.1	vpc-0a12768c6b999ebfe | AWS-.

Now, I will create customer gateway in Mumbai region and provided public IP of Singapore Instance.



	Name	Customer gateway ID	State	BGP ASN	IP address	T
●	AWS-SIDE-CG	cgw-08db95b86cc8d8e98	✓ Available	65000	13.250.118.240	ip

Now, I will create site to site VPN connection in Mumbai region. **Tunnel status is showing as down.**

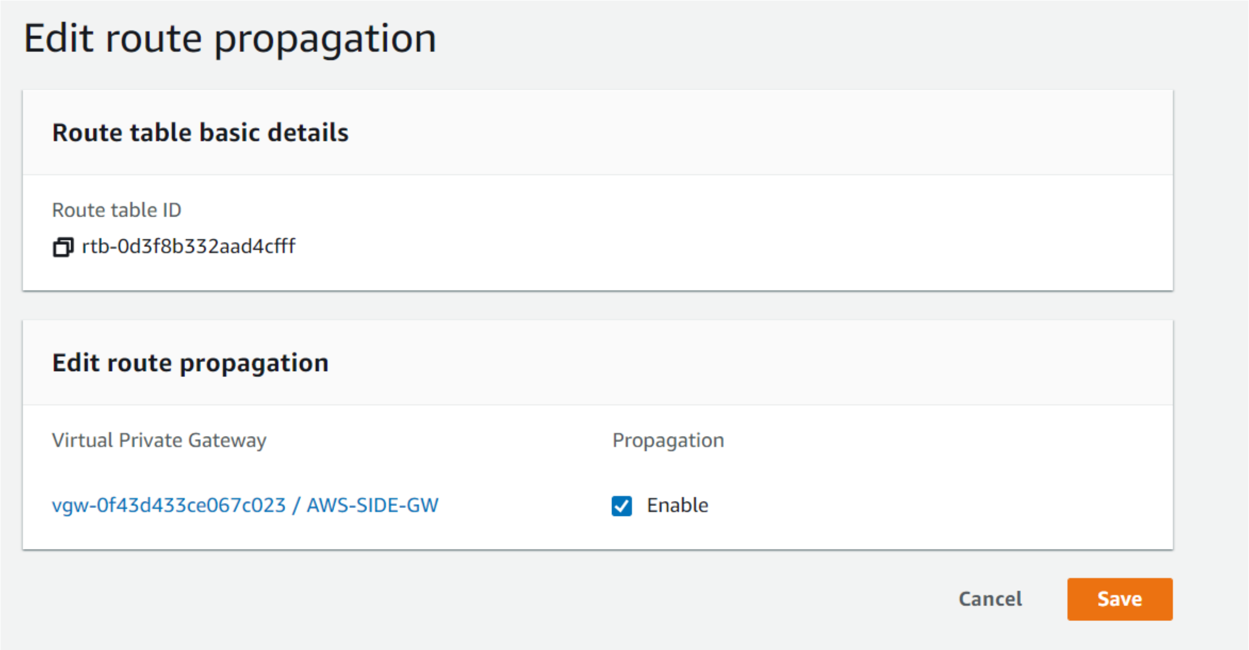


	Name	VPN ID	State	Virtual private gateway	Transit gateway
●	AWS-Mumbai-Sing…	vpn-0530d0b86026ed43e	✓ Available	vgw-0f43d433ce067c023	–

Tunnel state

Tunnel number	Outside IP address	Inside IPv4 CIDR	Inside IPv6 CIDR	Status	Last status change
Tunnel 1	15.206.87.209	169.254.180.228/30	–	☒ Down	October 8, 2022, 14:00:57 (UTC+05:30)
Tunnel 2	35.154.221.138	169.254.98.228/30	–	☒ Down	October 8, 2022, 14:00:57 (UTC+05:30)

Enabled route propagation from route table in Mumbai region.



Edit route propagation

Route table basic details

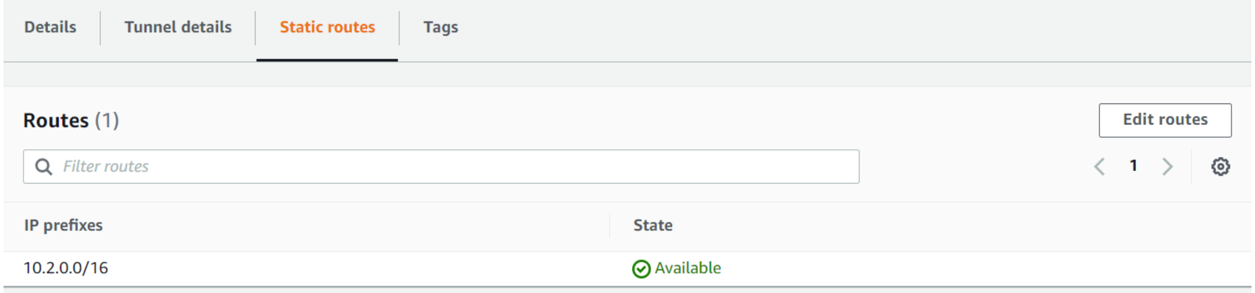
Route table ID

rtb-0d3f8b332aad4cfff

Edit route propagation

Virtual Private Gateway	Propagation
vgw-0f43d433ce067c023 / AWS-SIDE-GW	☑ Enable

Static Route of Site to Site VPN. (Subnet of Singapore's VPC)

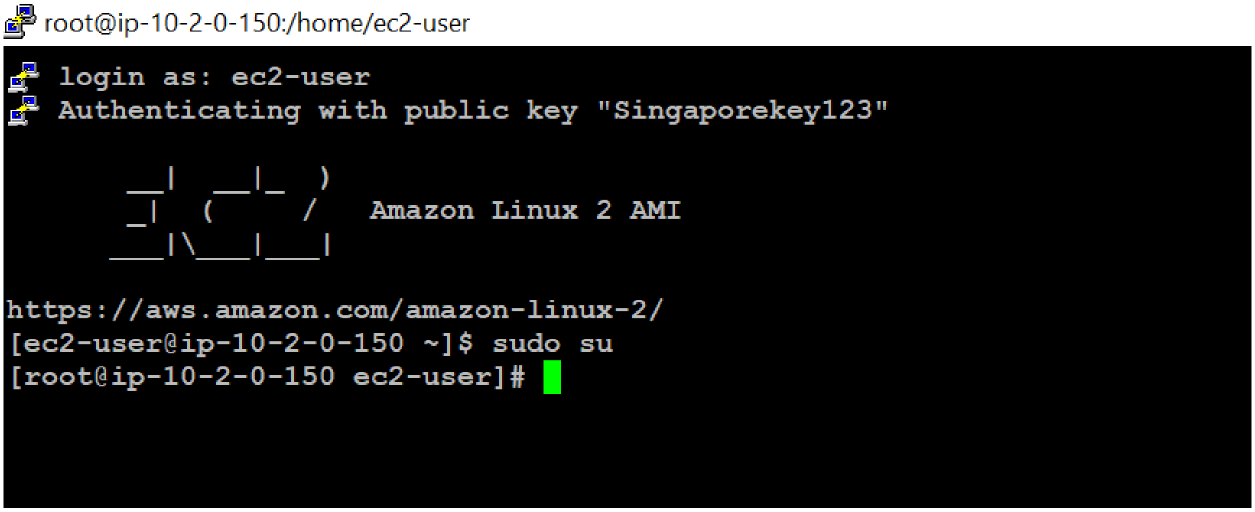


Routes (1)

IP prefixes	State
10.2.0.0/16	✓ Available

Let's download configuration from site to site VPN.

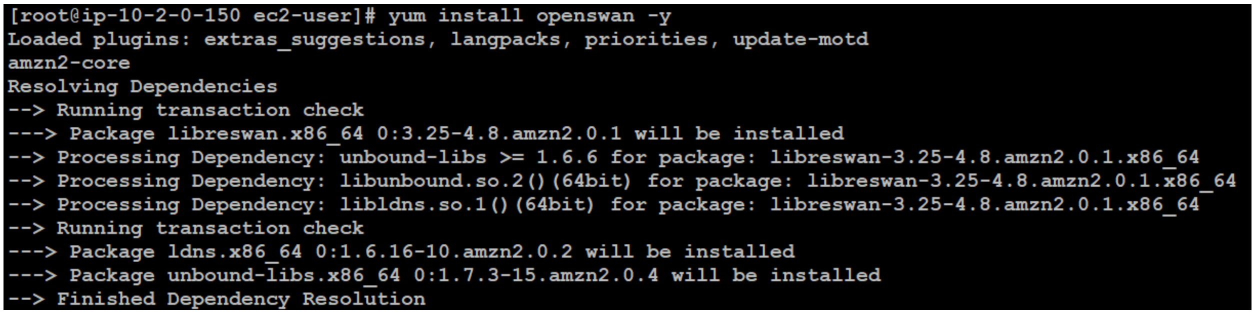
Now, I will login to EC2 instance from Singapore region.



root@ip-10-2-0-150:/home/ec2-user

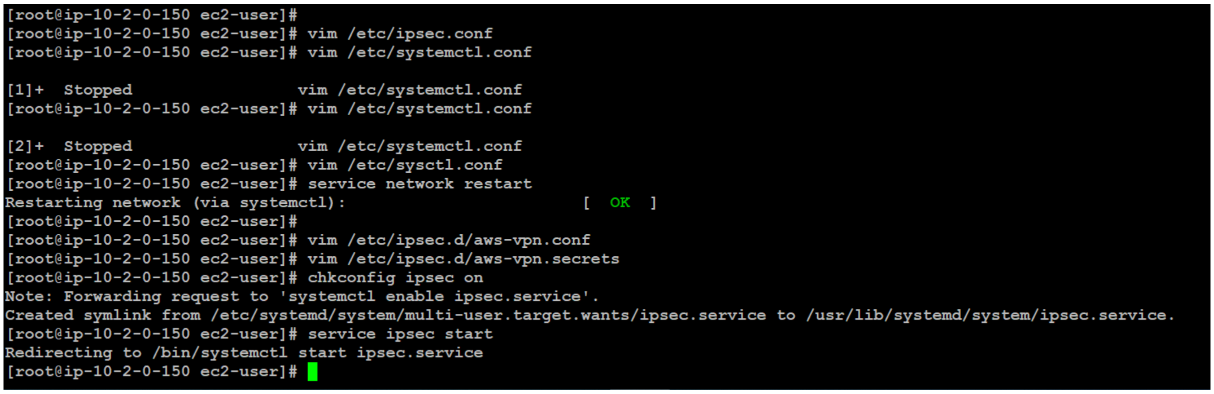
```
 login as: ec2-user
 Authenticating with public key "Singaporekey123"

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-2-0-150 ~]$ sudo su
[root@ip-10-2-0-150 ec2-user]#
```

I will do configuration on EC2 instance. First, I will install openswan package.



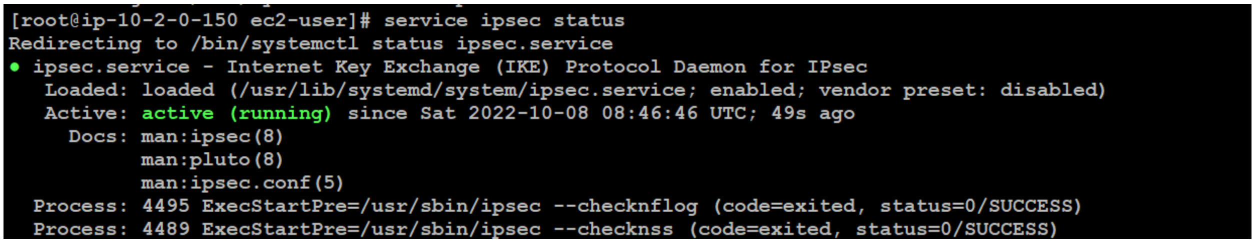
```
[root@ip-10-2-0-150 ec2-user]# yum install openswan -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core
Resolving Dependencies
--> Running transaction check
---> Package libreswan.x86_64 0:3.25-4.8.amzn2.0.1 will be installed
--> Processing Dependency: unbound-libs >= 1.6.6 for package: libreswan-3.25-4.8.amzn2.0.1.x86_64
--> Processing Dependency: libunbound.so.2()(64bit) for package: libreswan-3.25-4.8.amzn2.0.1.x86_64
--> Processing Dependency: libldns.so.1()(64bit) for package: libreswan-3.25-4.8.amzn2.0.1.x86_64
--> Running transaction check
---> Package ldns.x86_64 0:1.6.16-10.amzn2.0.2 will be installed
---> Package unbound-libs.x86_64 0:1.7.3-15.amzn2.0.4 will be installed
--> Finished Dependency Resolution
```

Configuration on linux done



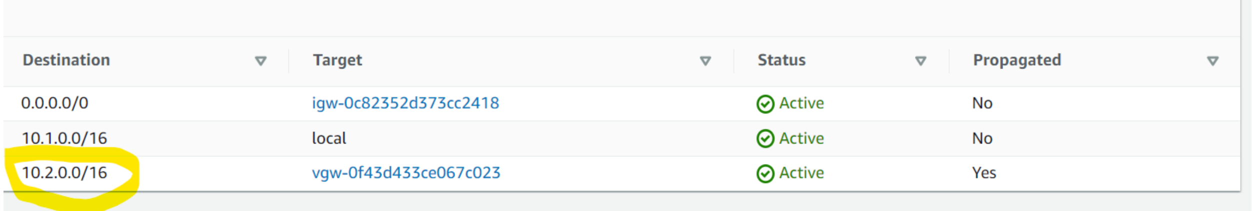
```
[root@ip-10-2-0-150 ec2-user]#
[root@ip-10-2-0-150 ec2-user]# vim /etc/ipsec.conf
[root@ip-10-2-0-150 ec2-user]# vim /etc/systemctl.conf

[1]+  Stopped                 vim /etc/systemctl.conf
[root@ip-10-2-0-150 ec2-user]# vim /etc/systemctl.conf

[2]+  Stopped                 vim /etc/systemctl.conf
[root@ip-10-2-0-150 ec2-user]# vim /etc/sysctl.conf
[root@ip-10-2-0-150 ec2-user]# service network restart
Restarting network (via systemctl):                        [  OK  ]
[root@ip-10-2-0-150 ec2-user]#
[root@ip-10-2-0-150 ec2-user]# vim /etc/ipsec.d/aws-vpn.conf
[root@ip-10-2-0-150 ec2-user]# vim /etc/ipsec.d/aws-vpn.secrets
[root@ip-10-2-0-150 ec2-user]# chkconfig ipsec on
Note: Forwarding request to 'systemctl enable ipsec.service'.
Created symlink from /etc/systemd/system/multi-user.target.wants/ipsec.service to /usr/lib/systemd/system/ipsec.service.
[root@ip-10-2-0-150 ec2-user]# service ipsec start
Redirecting to /bin/systemctl start ipsec.service
[root@ip-10-2-0-150 ec2-user]#
```

Status is active.



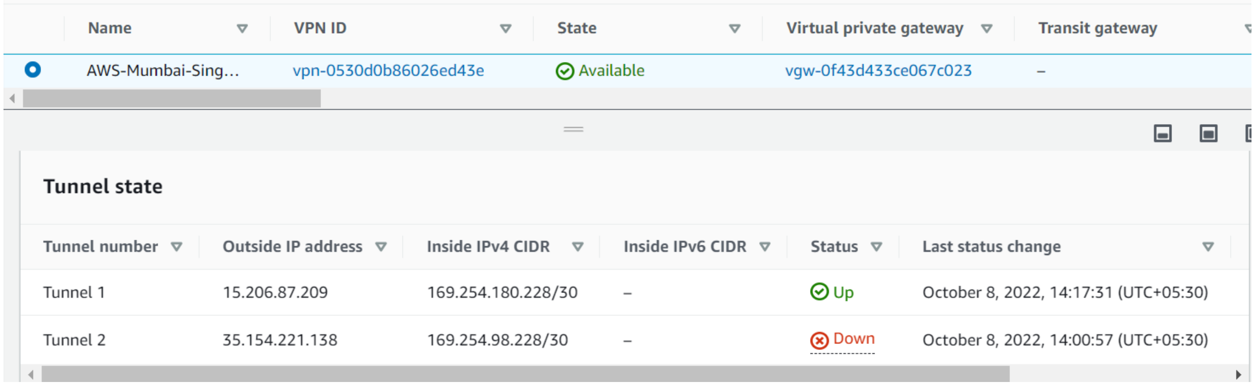
```
[root@ip-10-2-0-150 ec2-user]# service ipsec status
Redirecting to /bin/systemctl status ipsec.service
● ipsec.service - Internet Key Exchange (IKE) Protocol Daemon for IPsec
   Loaded: loaded (/usr/lib/systemd/system/ipsec.service; enabled; vendor preset: disabled)
   Active: active (running) since Sat 2022-10-08 08:46:46 UTC; 49s ago
     Docs: man:ipsec(8)
           man:pluto(8)
           man:ipsec.conf(5)
  Process: 4495 ExecStartPre=/usr/sbin/ipsec --checknflog (code=exited, status=0/SUCCESS)
  Process: 4489 ExecStartPre=/usr/sbin/ipsec --checknss (code=exited, status=0/SUCCESS)
```

You can see Singapore's subnet is reflecting under Mumbai region's subnet. (Highlighted is Singapore region subnet)



Destination	Target	Status	Propagated
0.0.0.0/0	igw-0c82352d373cc2418	✓ Active	No
10.1.0.0/16	local	✓ Active	No
10.2.0.0/16	vgw-0f43d433ce067c023	✓ Active	Yes

Also, in site to site VPN, you can see Tunnel 1 is up, previously it was down.

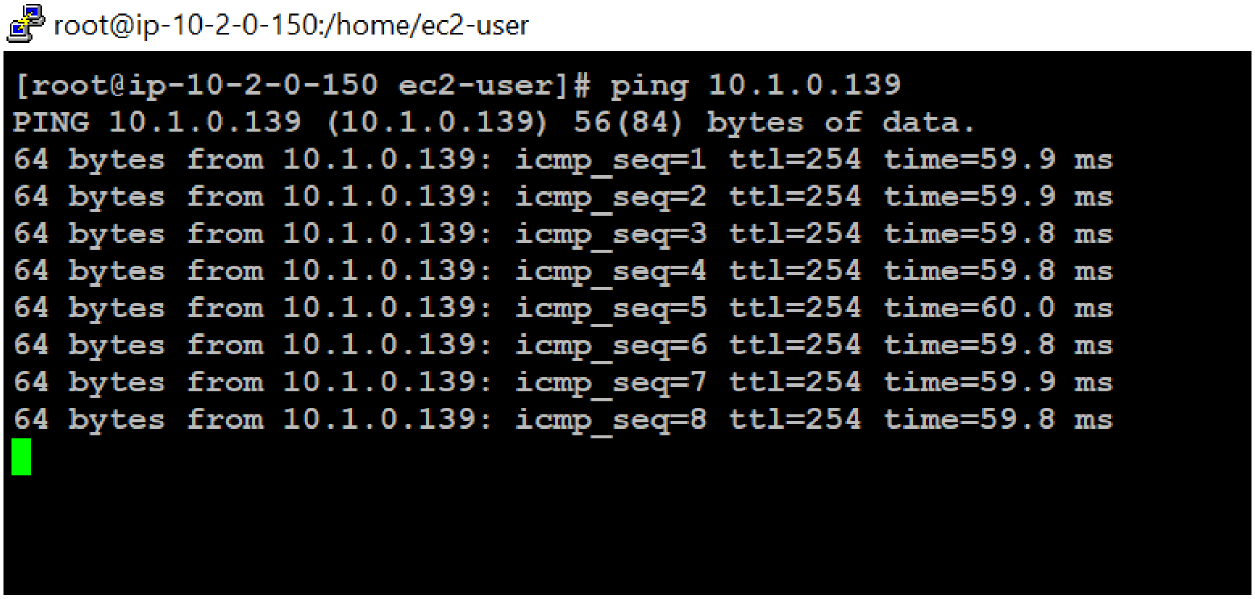


	Name	VPN ID	State	Virtual private gateway	Transit gateway
●	AWS-Mumbai-Sing…	vpn-0530d0b86026ed43e	✓ Available	vgw-0f43d433ce067c023	–

Tunnel state

Tunnel number	Outside IP address	Inside IPv4 CIDR	Inside IPv6 CIDR	Status	Last status change
Tunnel 1	15.206.87.209	169.254.180.228/30	–	✓ Up	October 8, 2022, 14:17:31 (UTC+05:30)
Tunnel 2	35.154.221.138	169.254.98.228/30	–	⊗ Down	October 8, 2022, 14:00:57 (UTC+05:30)

Now connectivity is successful, let’s ping Mumbai machine from Singapore Machine using private IP address. (10.1.0.139 – Mumbai machine private IP address).



```
[root@ip-10-2-0-150 ec2-user]# ping 10.1.0.139
PING 10.1.0.139 (10.1.0.139) 56(84) bytes of data.
64 bytes from 10.1.0.139: icmp_seq=1 ttl=254 time=59.9 ms
64 bytes from 10.1.0.139: icmp_seq=2 ttl=254 time=59.9 ms
64 bytes from 10.1.0.139: icmp_seq=3 ttl=254 time=59.8 ms
64 bytes from 10.1.0.139: icmp_seq=4 ttl=254 time=59.8 ms
64 bytes from 10.1.0.139: icmp_seq=5 ttl=254 time=60.0 ms
64 bytes from 10.1.0.139: icmp_seq=6 ttl=254 time=59.8 ms
64 bytes from 10.1.0.139: icmp_seq=7 ttl=254 time=59.9 ms
64 bytes from 10.1.0.139: icmp_seq=8 ttl=254 time=59.8 ms
```