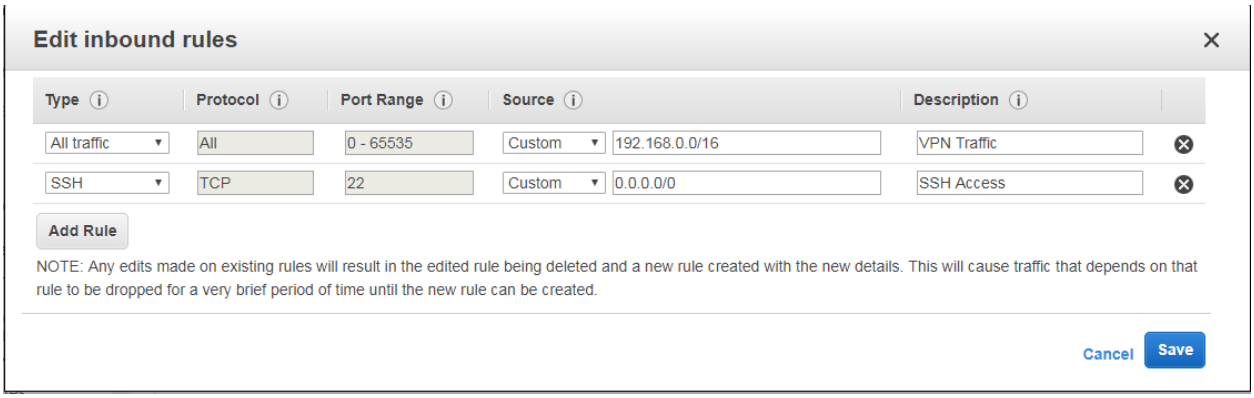
Configure VPN between Mumbai and Ohio Lab 3 of 4

Go to Security Group “Mumbai_Linux_sec_Group”.

Click “Edit “ and then click “Add Rule”.

Allow all traffic from 192.168.0.0/16 subnet.

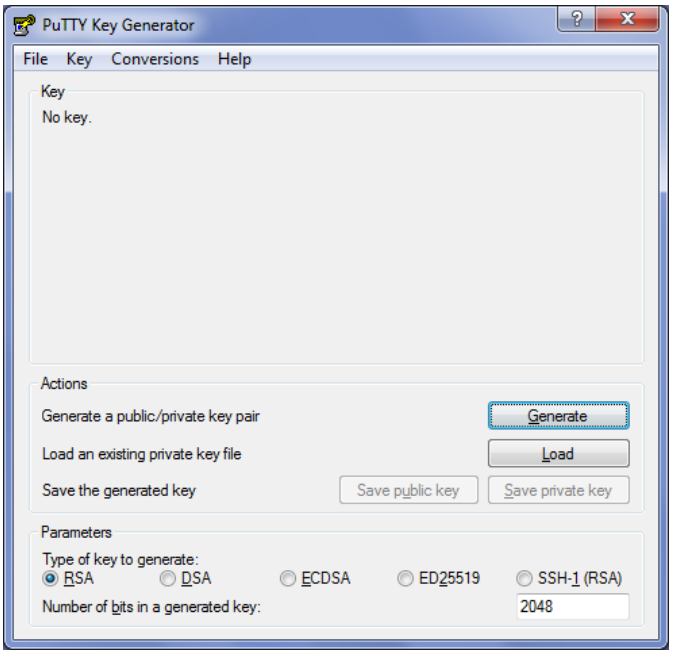


Then click save.

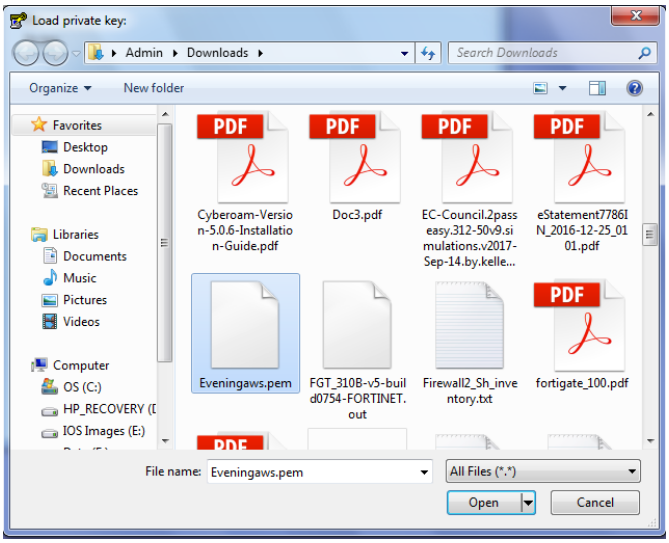
Goto Mumbai region to get public ip address of VPN Server Interface (13.127.161.231)

Launch putty key generator in your local machine,

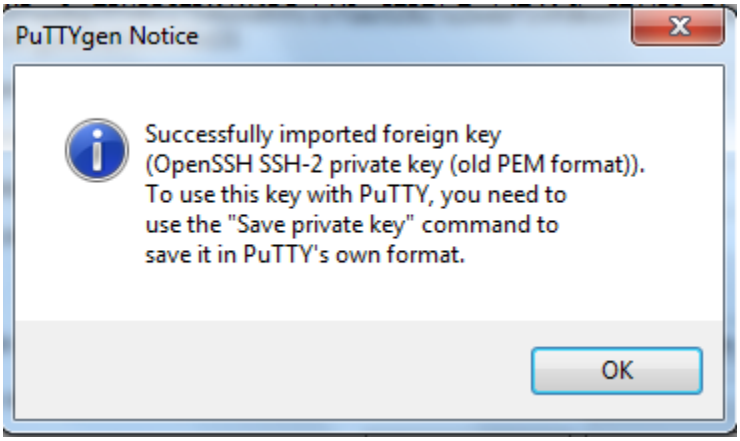
In File → Load private key



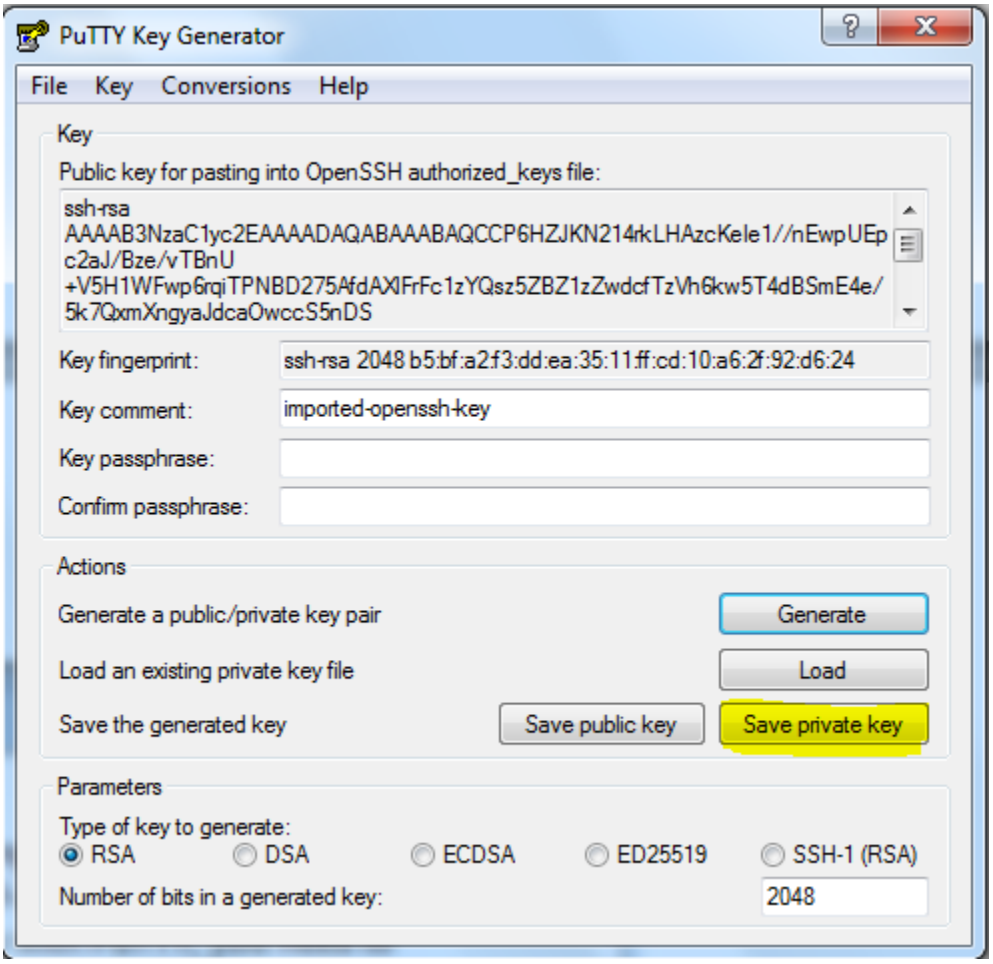
Locate the *.pem file and click “open”.



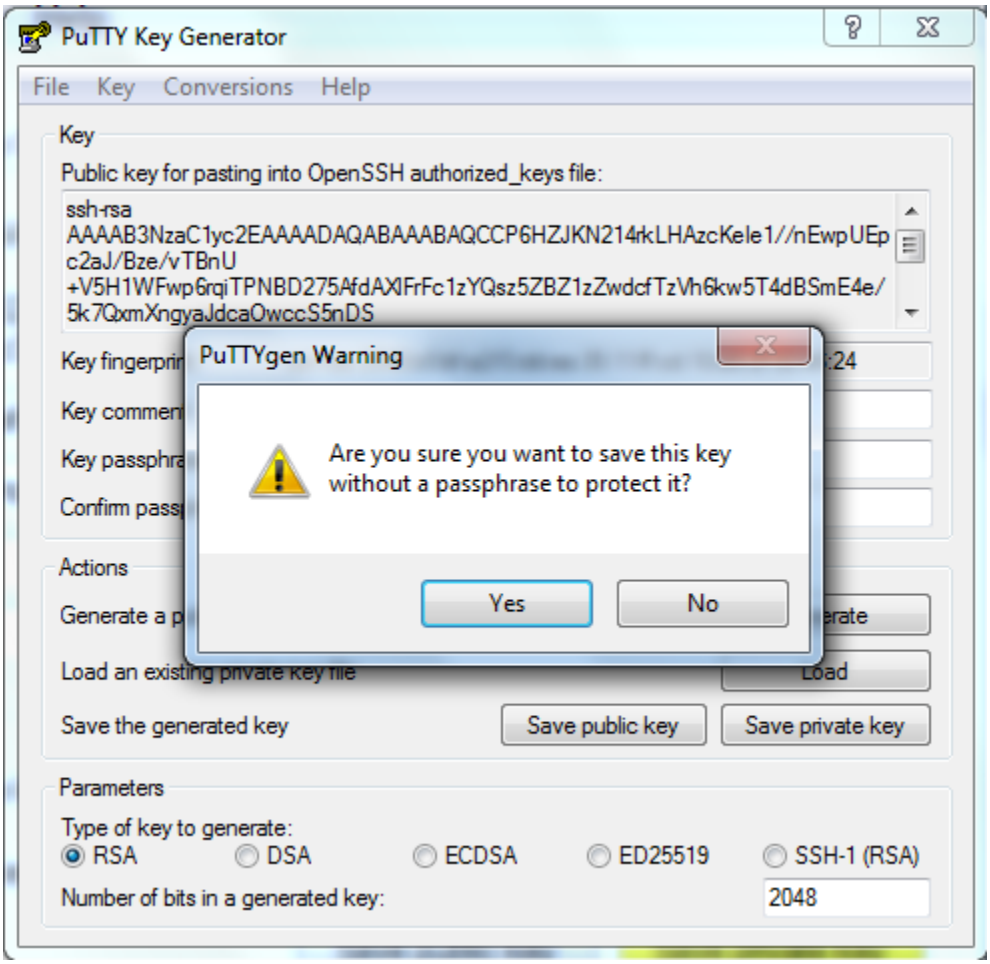
Click ”Ok:”.



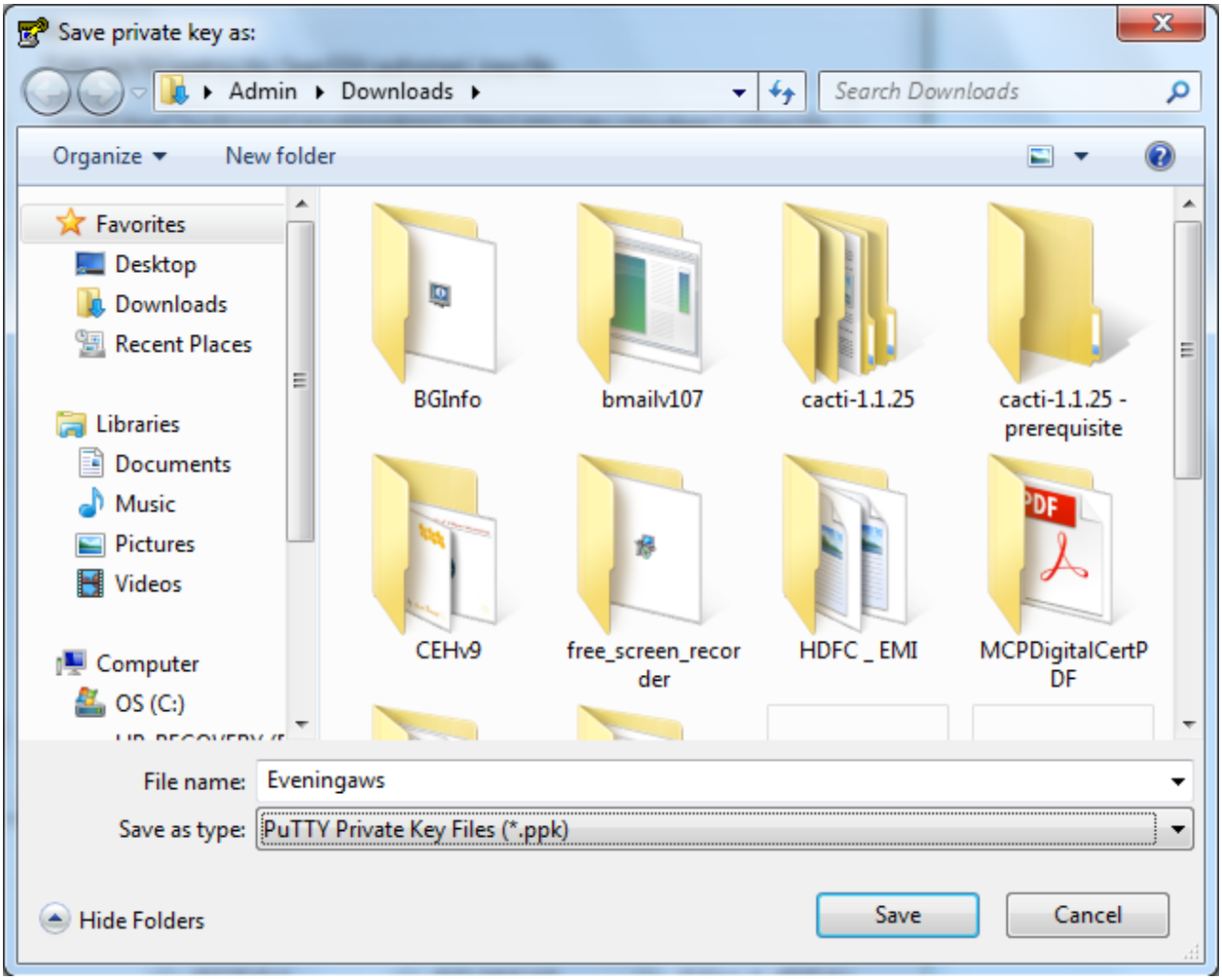
Click “save Private Key”.



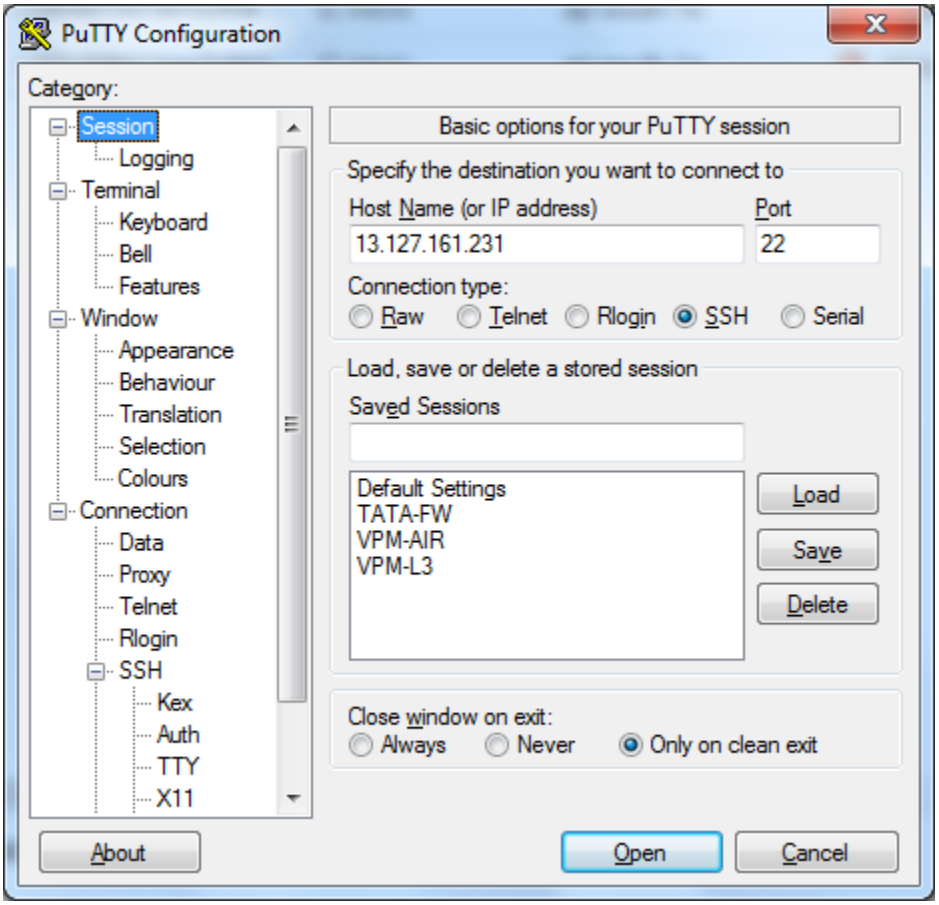
Click “Yes”.


PuTTY Key Generator
File Key Conversions Help
Key
Public key for pasting into OpenSSH authorized_keys file:
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCCP6HZJKN214rkLHAzcKele1//nEwpUEp
c2aJ/Bze/vTBnU
+V5H1WFwp6rqiTPNBD275AfdAXlFrFc1zYQsz5ZBZ1zZwdcfTzVh6kw5T4dBSmE4e/
5k7QxmXngyaJdcaOwccS5nDS
PuTTYgen Warning
Are you sure you want to save this key without a passphrase to protect it?
Yes
No
Actions
Load an existing private key file
Load
Save the generated key
Save public key
Save private key
Parameters
Type of key to generate:
RSA
DSA
ECDSA
ED25519
SSH-1 (RSA)
Number of bits in a generated key:
2048

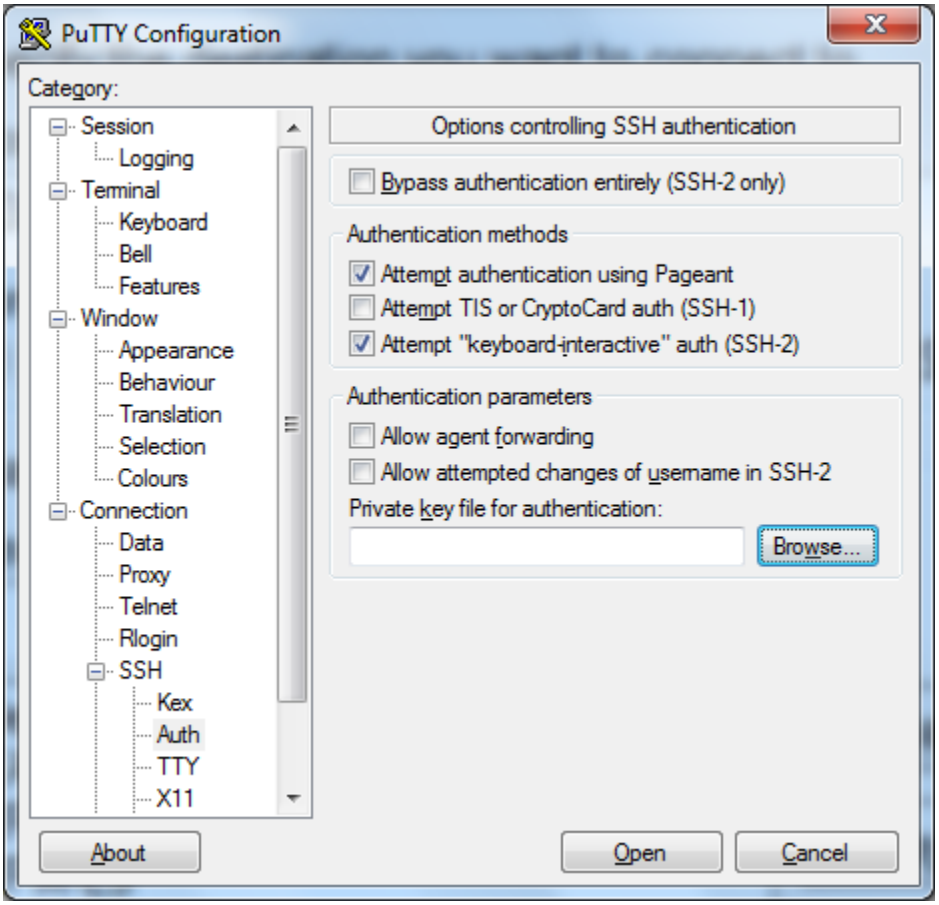
Save the private key in location.



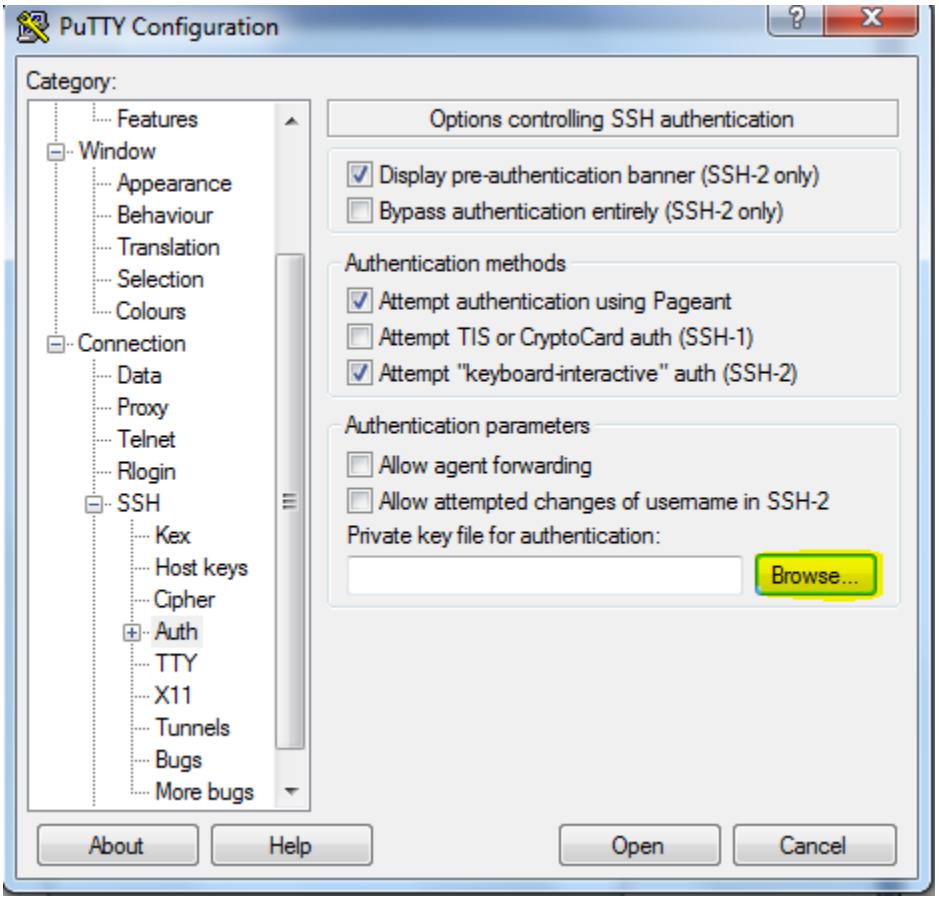
Type the ip address in putty.



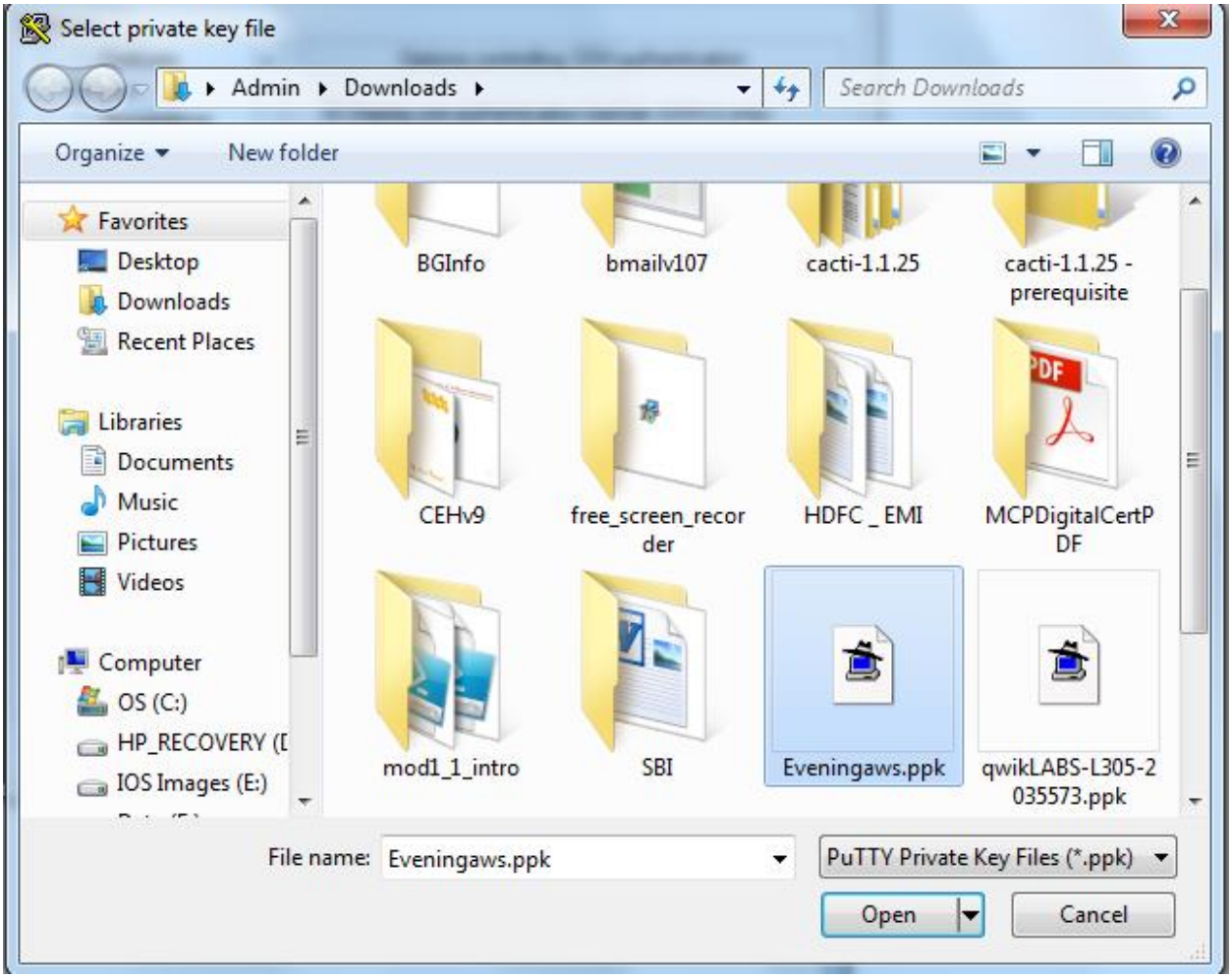
Click SSH and expand it click “Auth”.



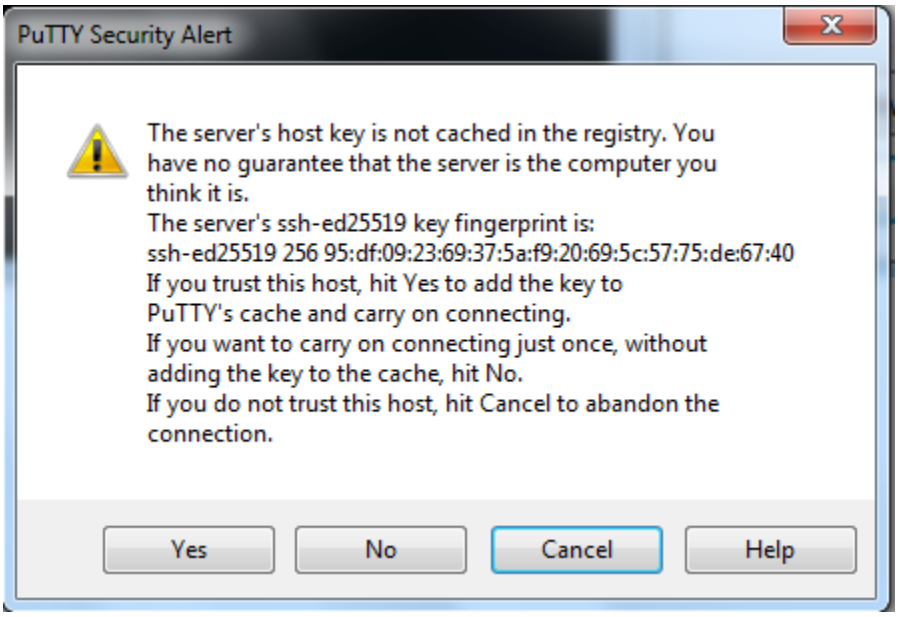
Click browse and locate the *.ppk file.

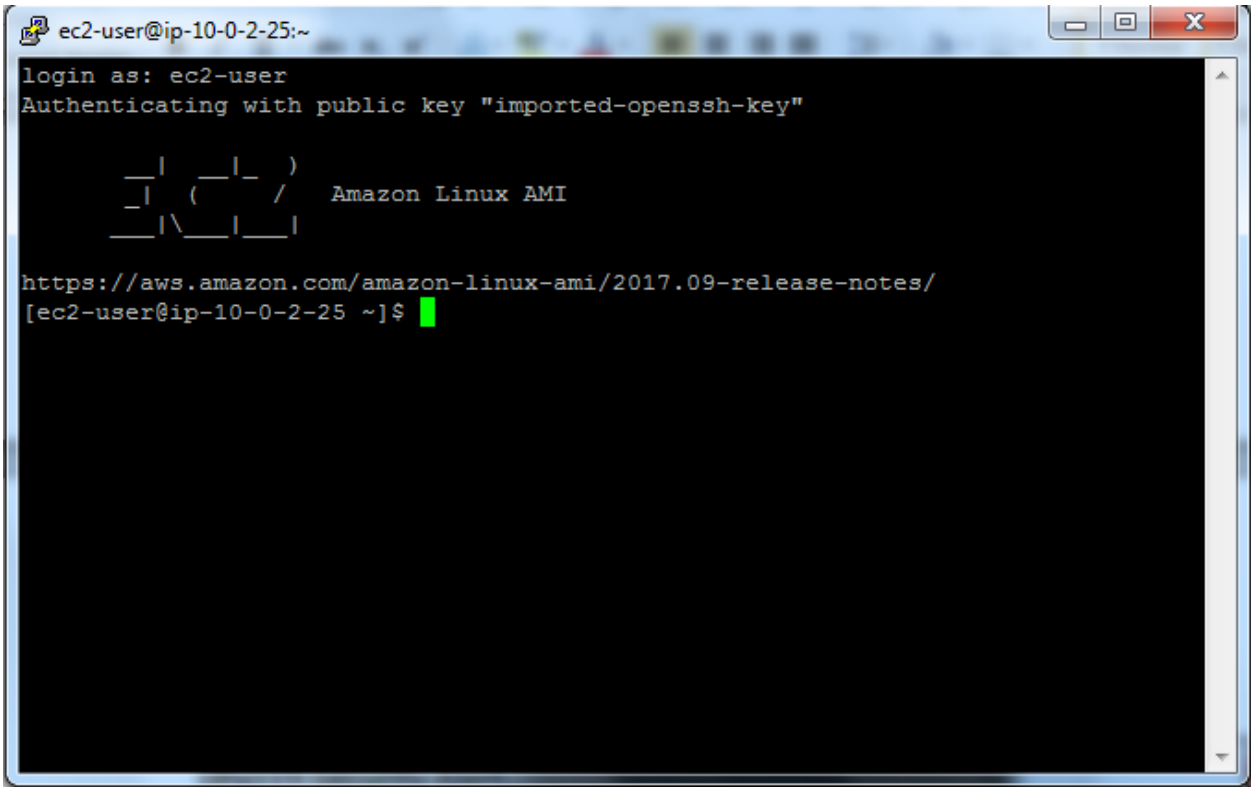


Locate the file and click “Open”.



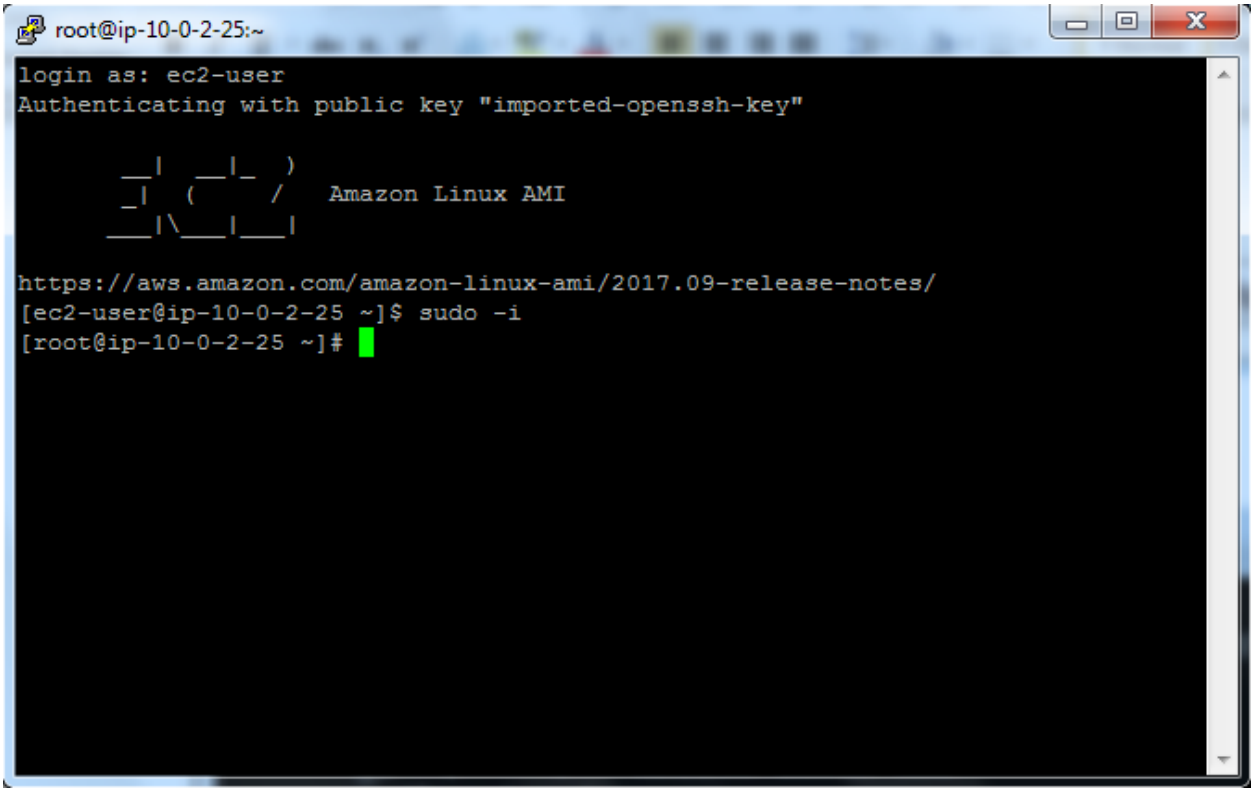
Click “Yes”.


PuTTY Security Alert
The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 256 95:df:09:23:69:37:5a:f9:20:69:5c:57:75:de:67:40
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.
Yes
No
Cancel
Help


ec2-user@ip-10-0-2-25:~
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Amazon Linux AMI
https://aws.amazon.com/amazon-linux-ami/2017.09-release-notes/
[ec2-user@ip-10-0-2-25 ~]$

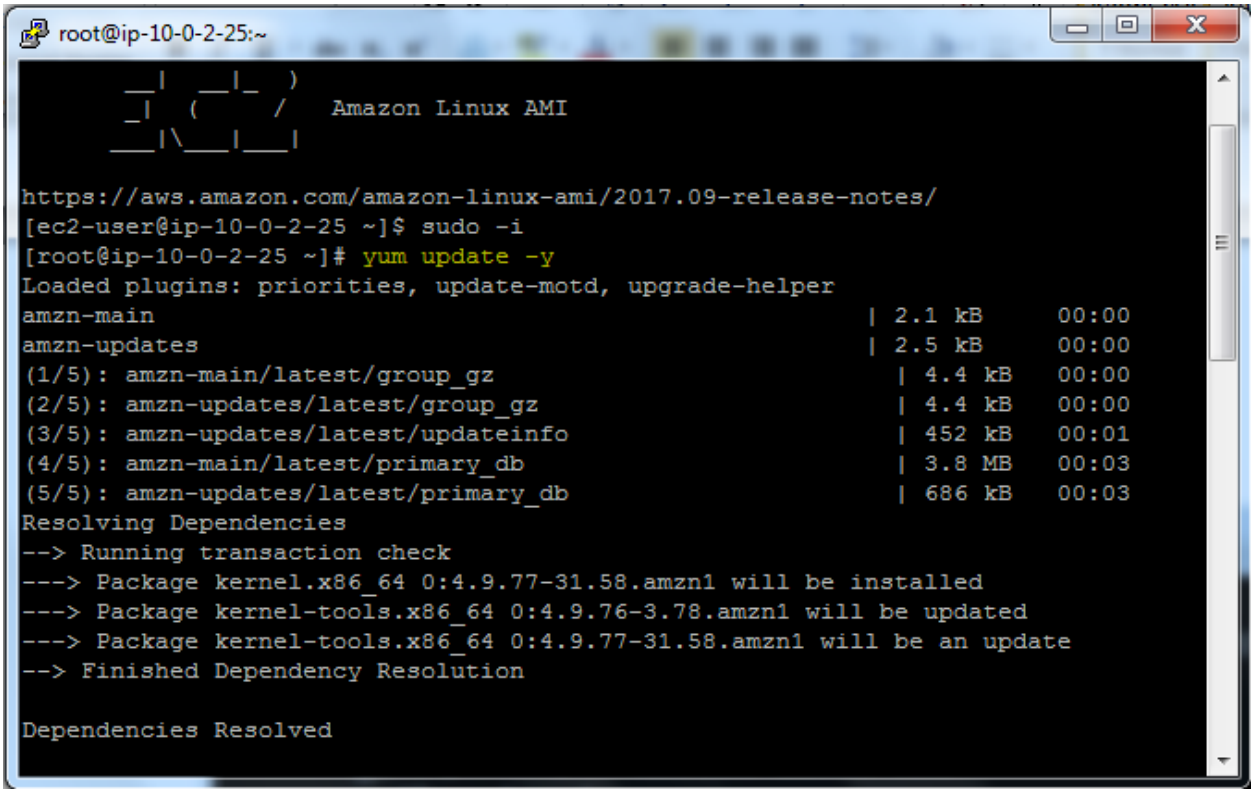
Type

sudo-i


root@ip-10-0-2-25:~
login as: ec2-user
Authenticating with public key "imported-openssh-key"
__| __|_)
_| (/ Amazon Linux AMI
___|___|___|
https://aws.amazon.com/amazon-linux-ami/2017.09-release-notes/
[ec2-user@ip-10-0-2-25 ~]$ sudo -i
[root@ip-10-0-2-25 ~]#

Type

Yum update -y



Type

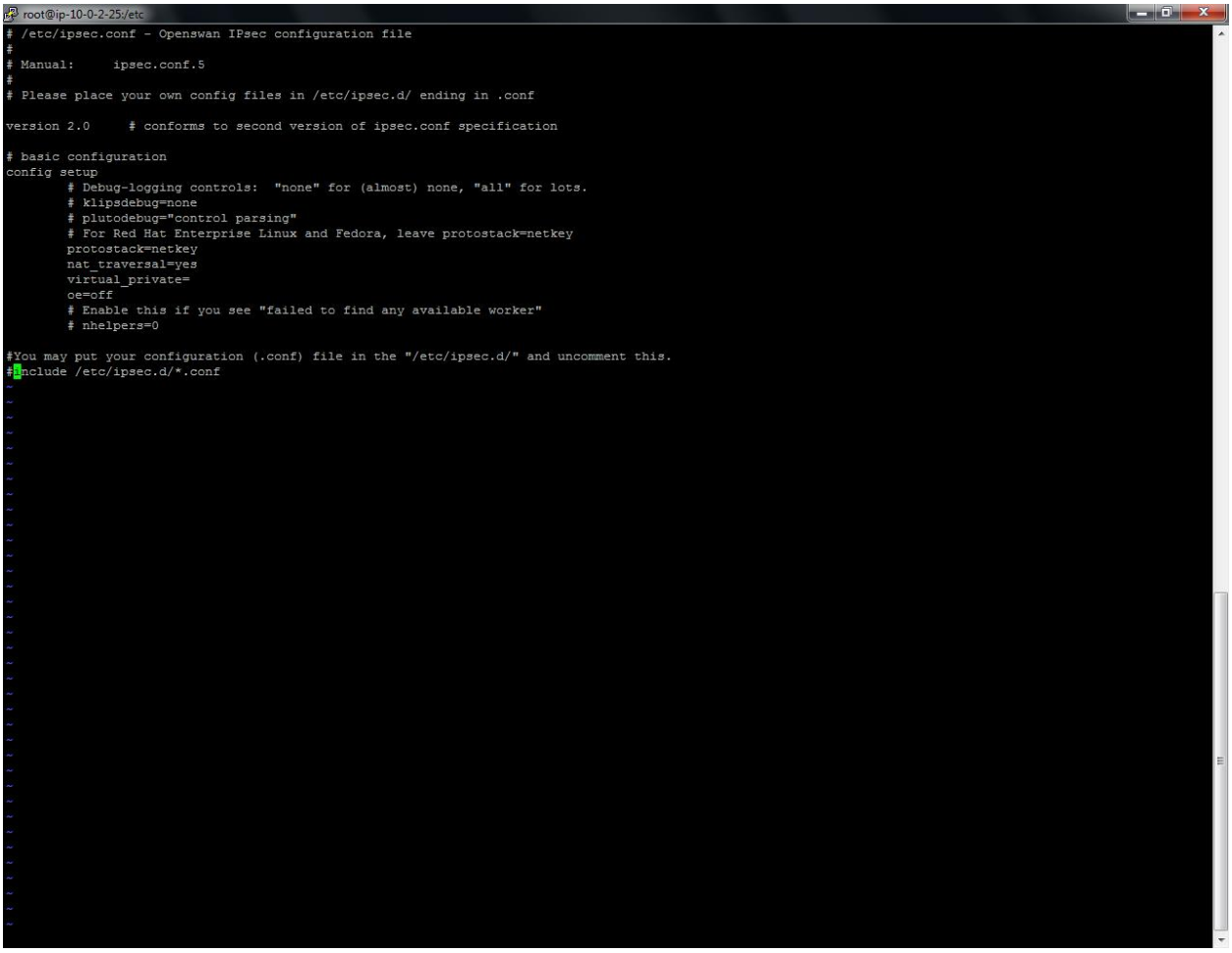
Yum install openswan -y

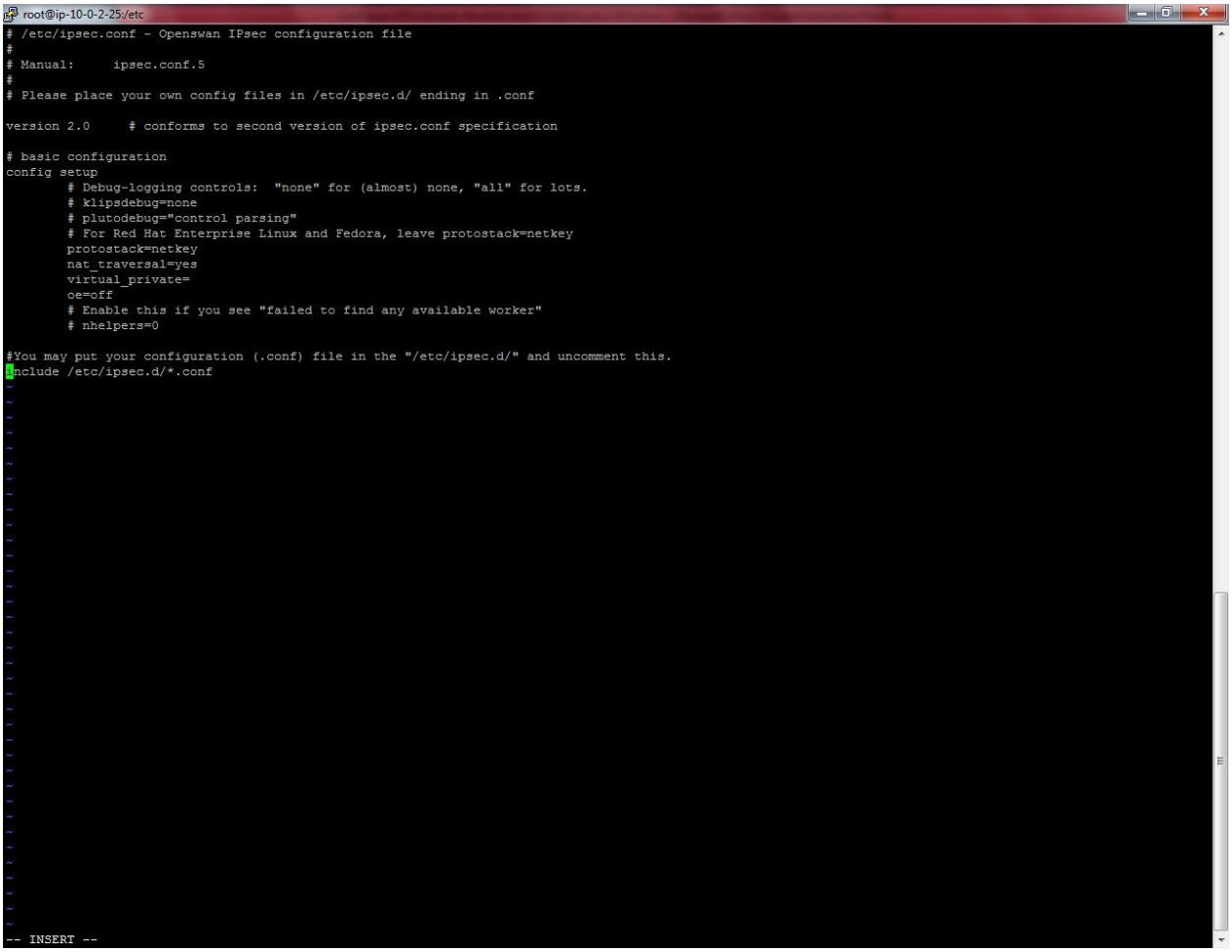
```
root@ip-10-0-2-25:~
[root@ip-10-0-2-25 ~]# yum install openswan -y
Loaded plugins: priorities, update-motd, upgrade-helper
Resolving Dependencies
--> Running transaction check
---> Package openswan.x86_64 0:2.6.37-3.17.amzn1 will be installed
--> Processing Dependency: libgmp.so.3()(64bit) for package: openswan-2.6.37-3.1
7.amzn1.x86_64
--> Running transaction check
---> Package compat-gmp4.x86_64 0:4.3.2-1.14.amzn1 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package           Arch         Version                   Repository       Size
================================================================================
Installing:
 openswan          x86_64       2.6.37-3.17.amzn1         amzn-main       1.1 M
Installing for dependencies:
 compat-gmp4       x86_64       4.3.2-1.14.amzn1          amzn-main       302 k

Transaction Summary
================================================================================
Install  1 Package (+1 Dependent package)
```

Cd /etc

Vi ipsec.conf

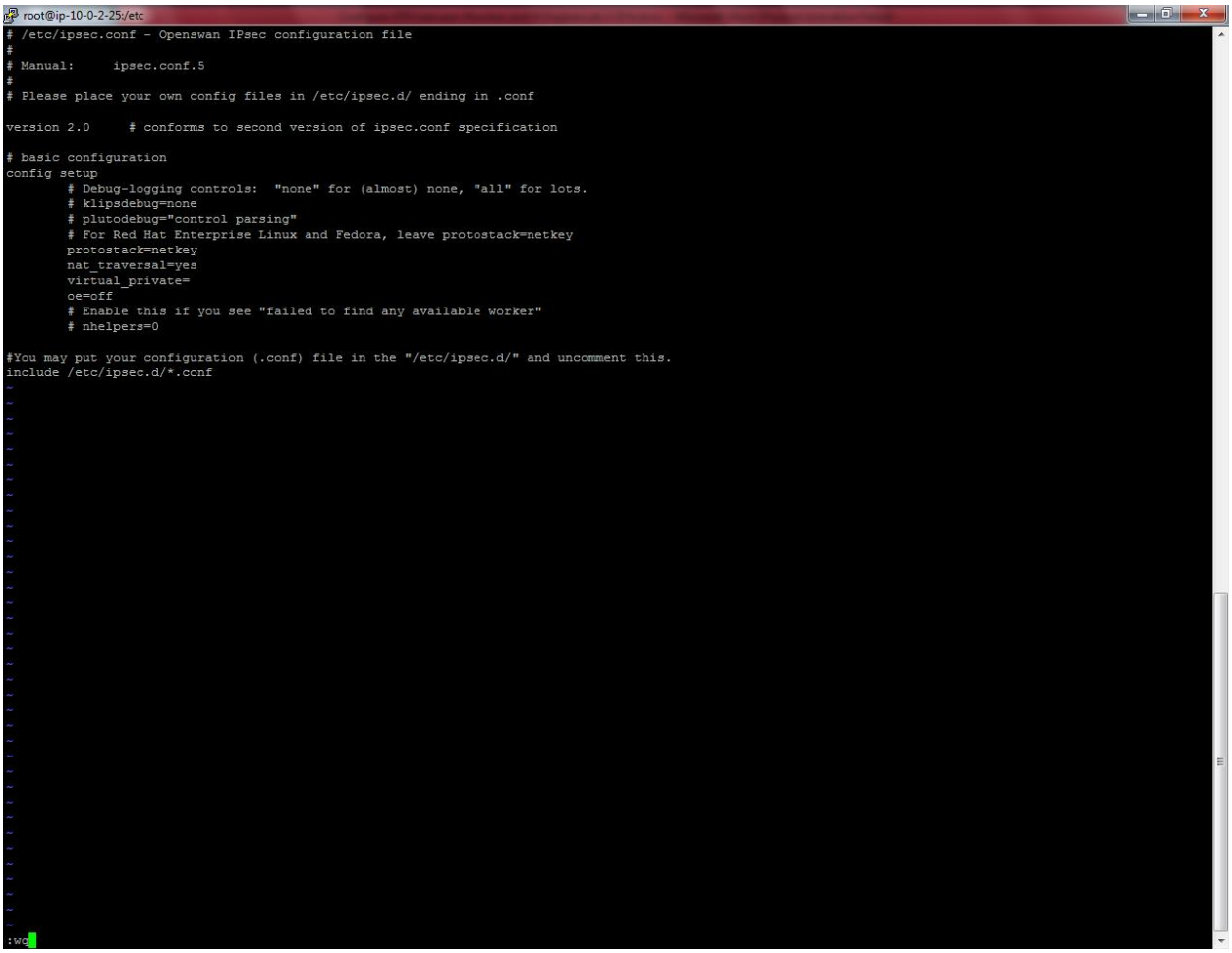
In ipsec.conf file we need to **remove # from** #include /etc/ipsec.d/*.conf line





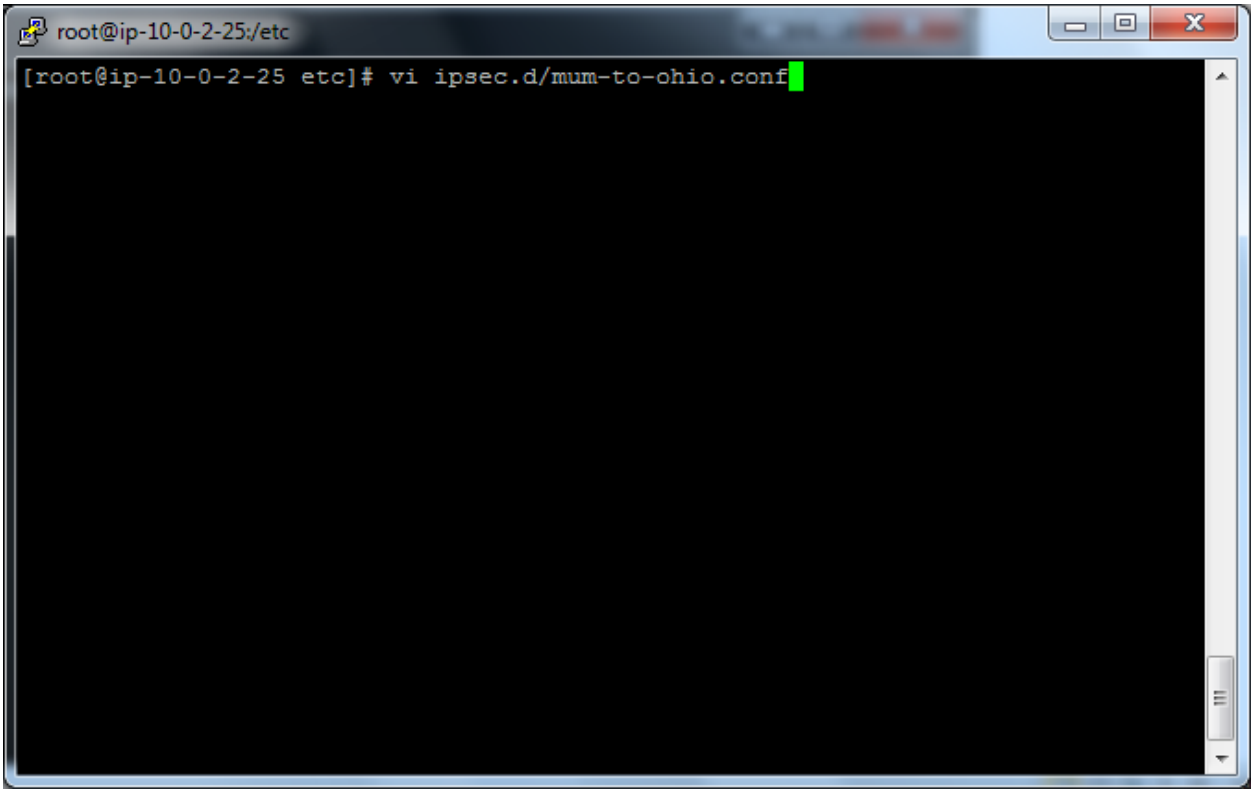
Press Escape key

Type :wq


root@ip-10-0-2-25:/etc
/etc/ipsec.conf - Openswan IPsec configuration file
#
Manual: ipsec.conf.5
#
Please place your own config files in /etc/ipsec.d/ ending in .conf
version 2.0   # conforms to second version of ipsec.conf specification
basic configuration
config setup
        # Debug-logging controls: "none" for (almost) none, "all" for lots.
        # klipsdebug=none
        # plutodebug="control parsing"
        # For Red Hat Enterprise Linux and Fedora, leave protostack=netkey
        protostack=netkey
        nat_traversal=yes
        virtual_private=
        oe=off
        # Enable this if you see "failed to find any available worker"
        # nhelpers=0
#You may put your configuration (.conf) file in the "/etc/ipsec.d/" and uncomment this.
include /etc/ipsec.d/*.conf
:wq

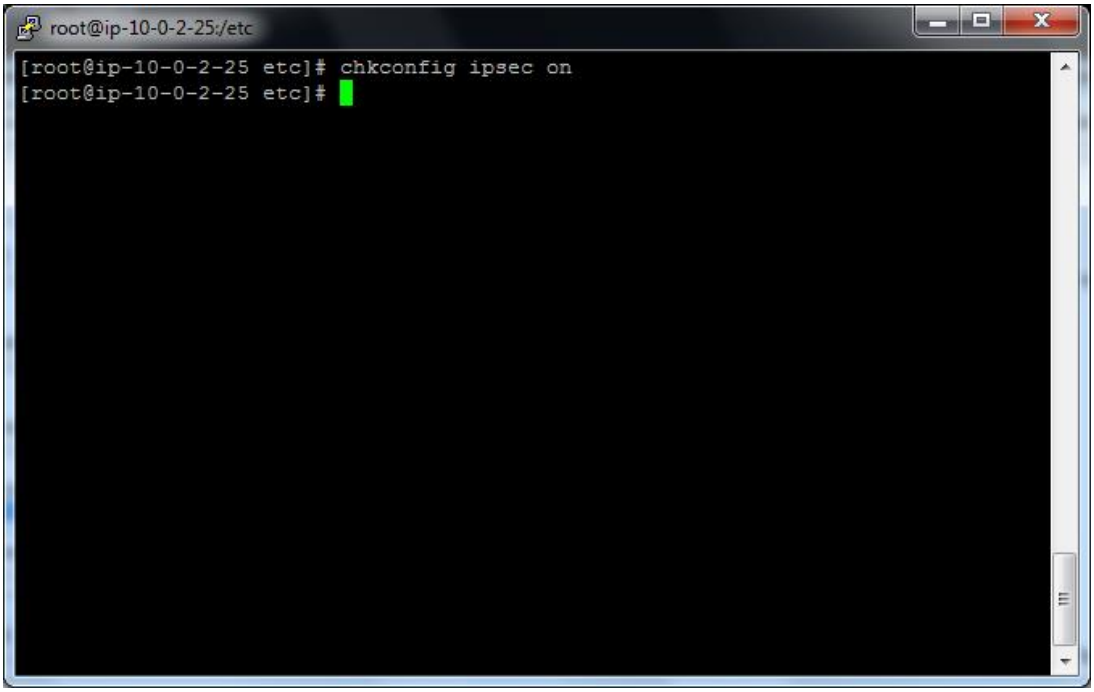
Type

Vi ipsec.d/mum-to-ohio.conf



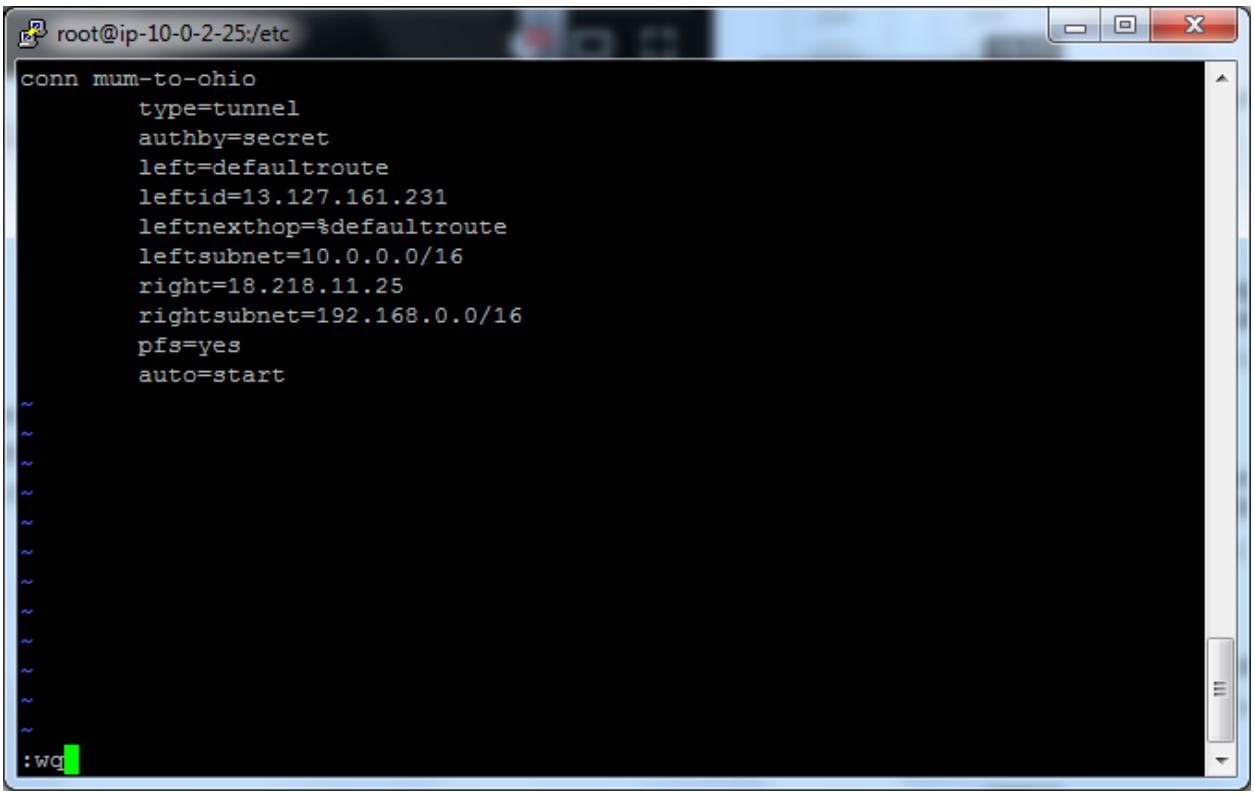
Type

Chkconfig ipsec on



Copy the command to below editor.

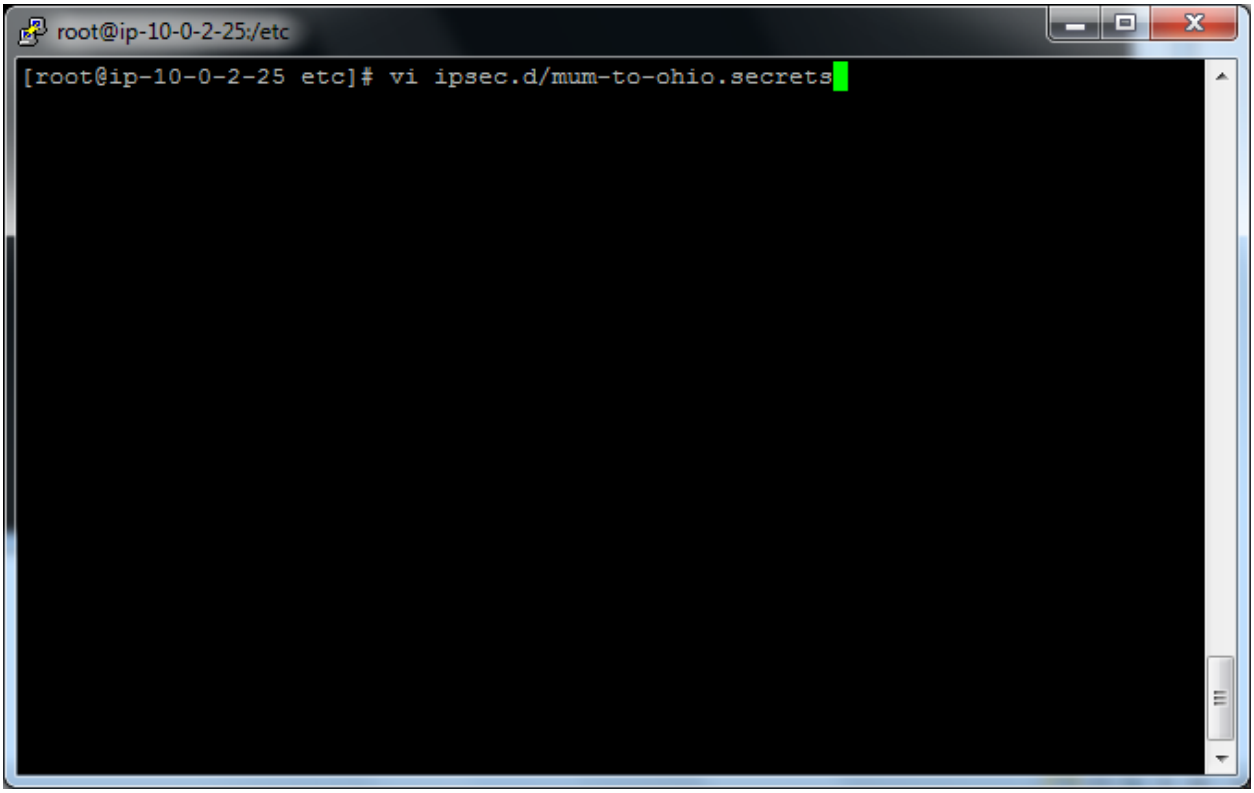
```
conn mum-to-ohio
        type=tunnel
        authby=secret
        left=defaultroute
        leftid=13.127.161.231
        leftnexthop=%defaultroute
        leftsubnet=10.0.0.0/16
        right=18.218.11.25
        rightsubnet=192.168.0.0/16
        pfs=yes
        auto=start
```



Press escape and type :wq

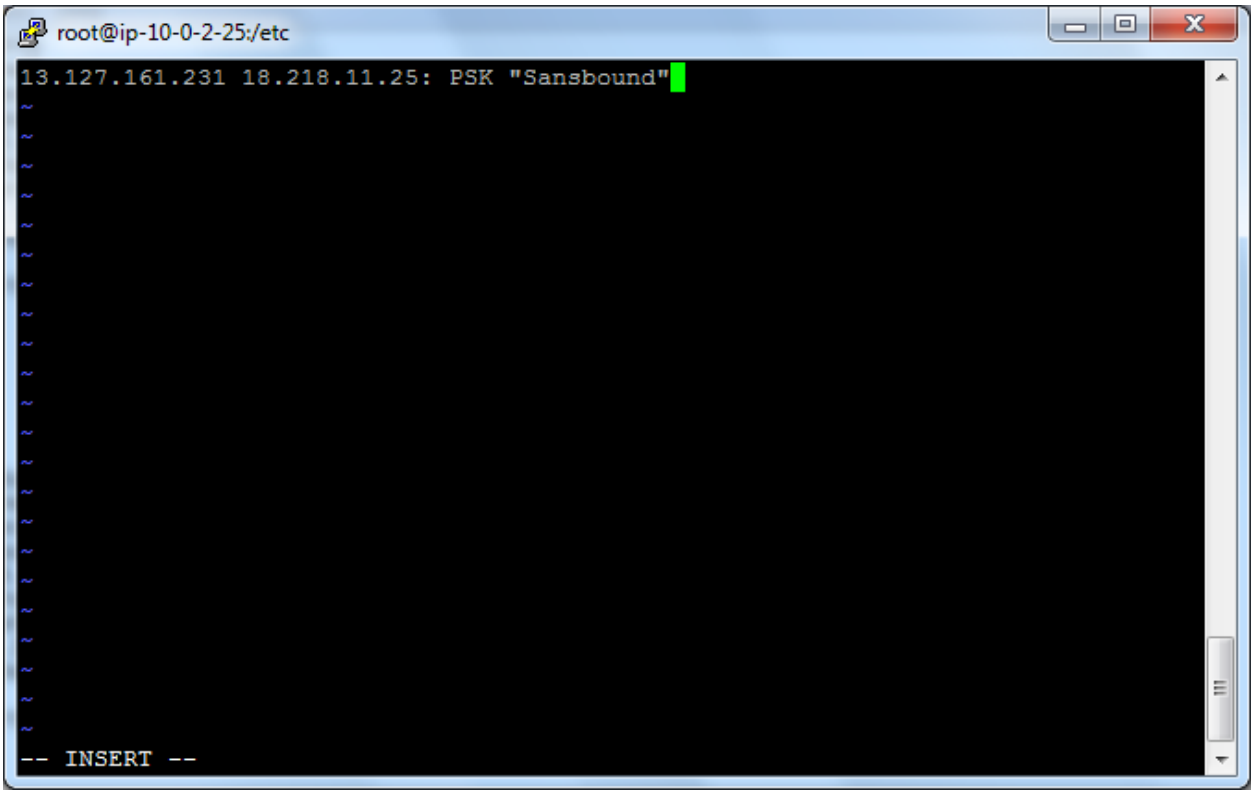
Type

Vi ipsec.d/mum-to-ohio.secrets



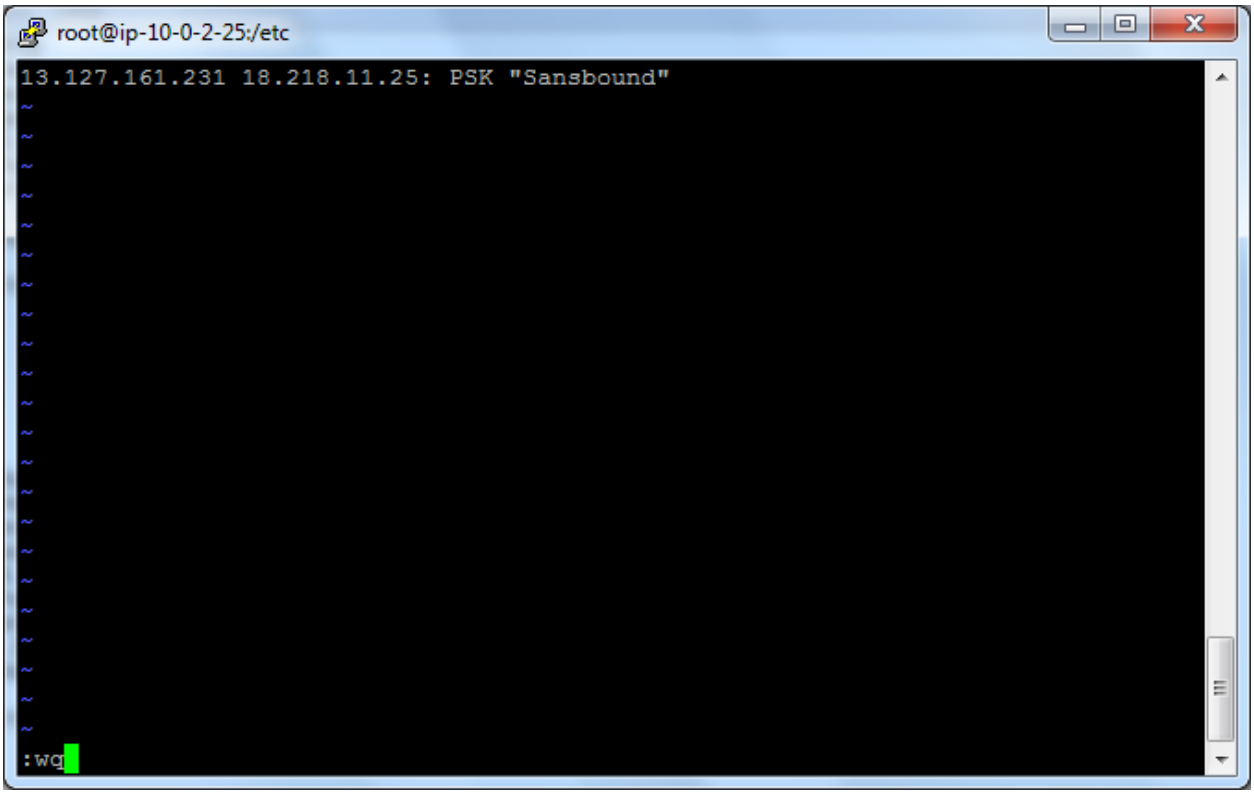
TYPE EIP1 (Mumbai EIP) and type EIP2 (Ohio EIP) then type : PSK “Preshared key of the tunnel”.

Our Tunnel Preshared key is “Sansbound”

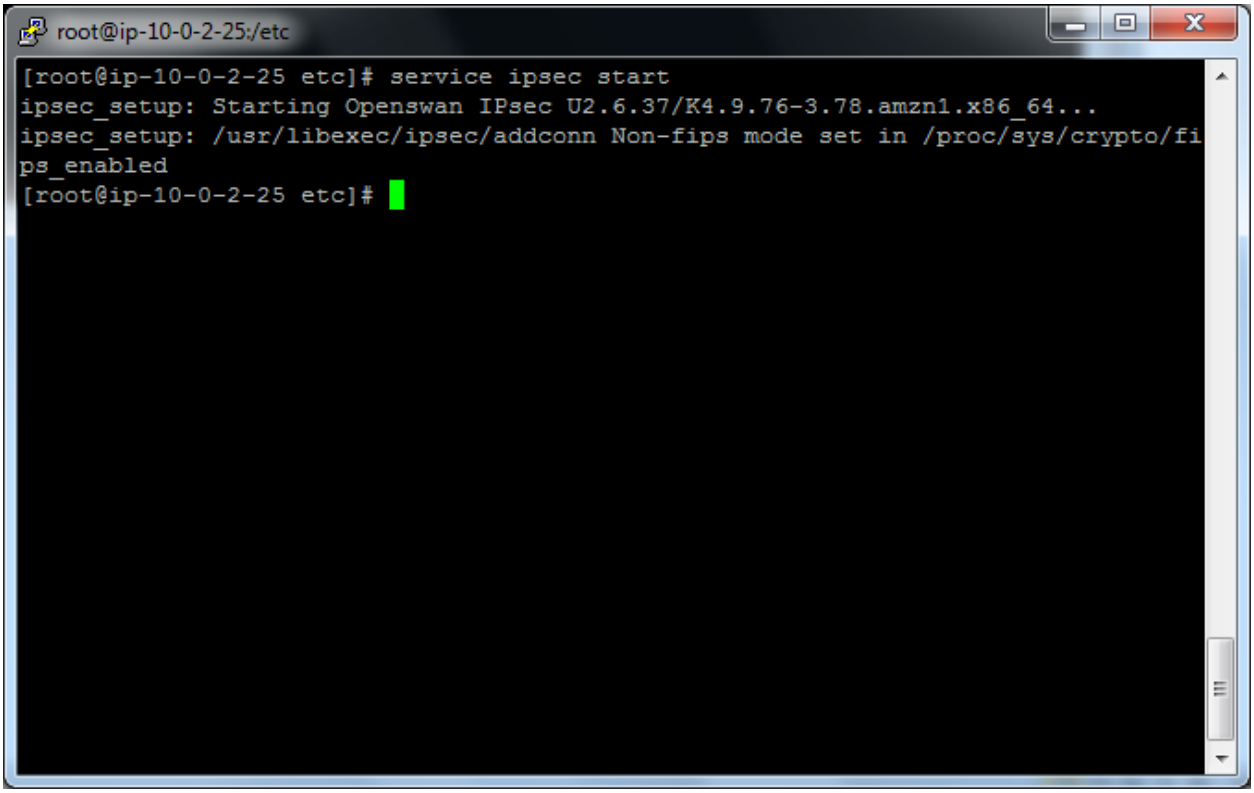


Press escape key

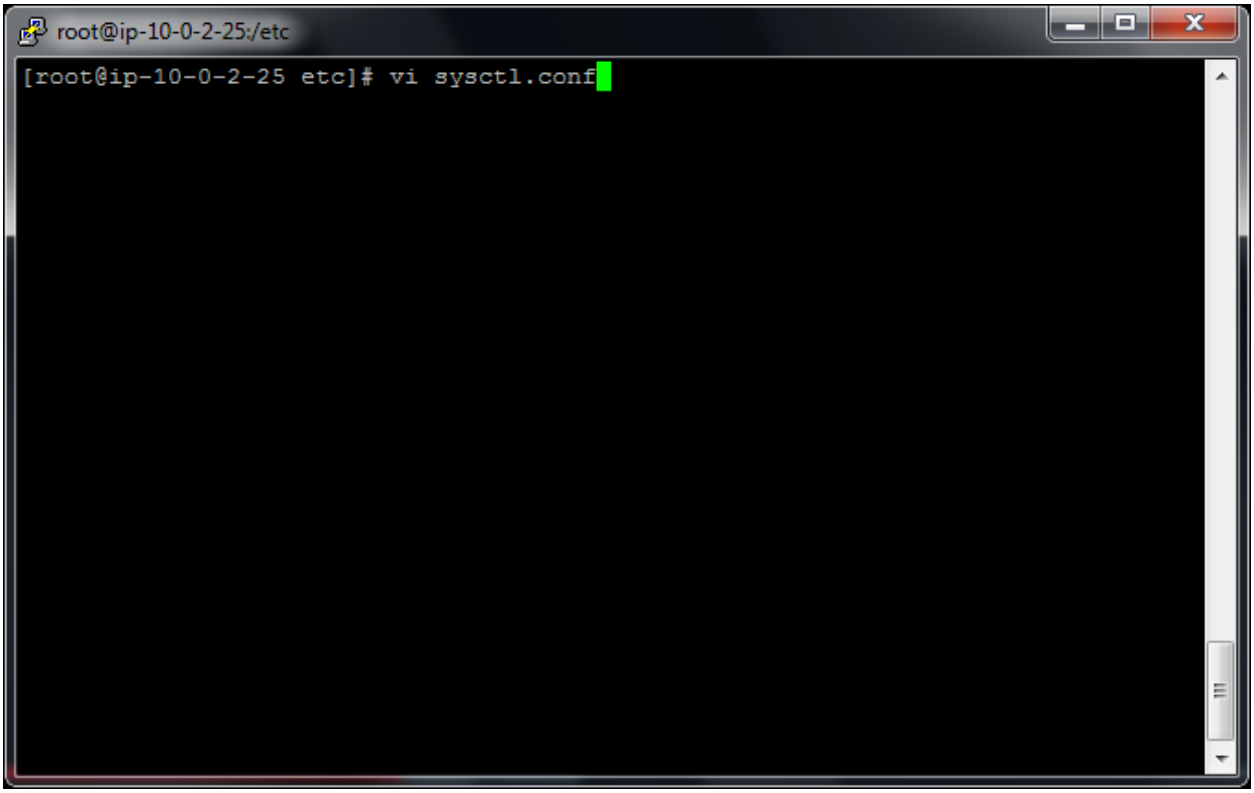
Type :wq



Service ipsec start



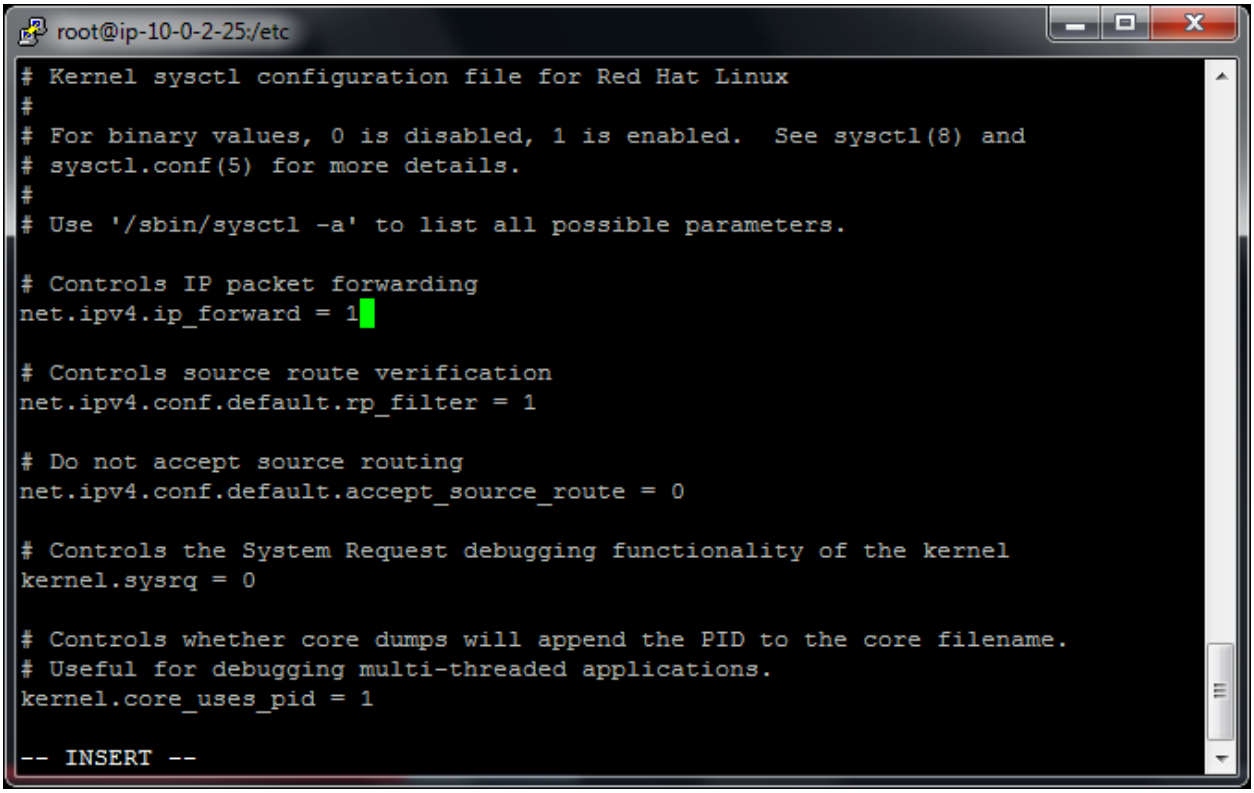
Type sysctl.conf



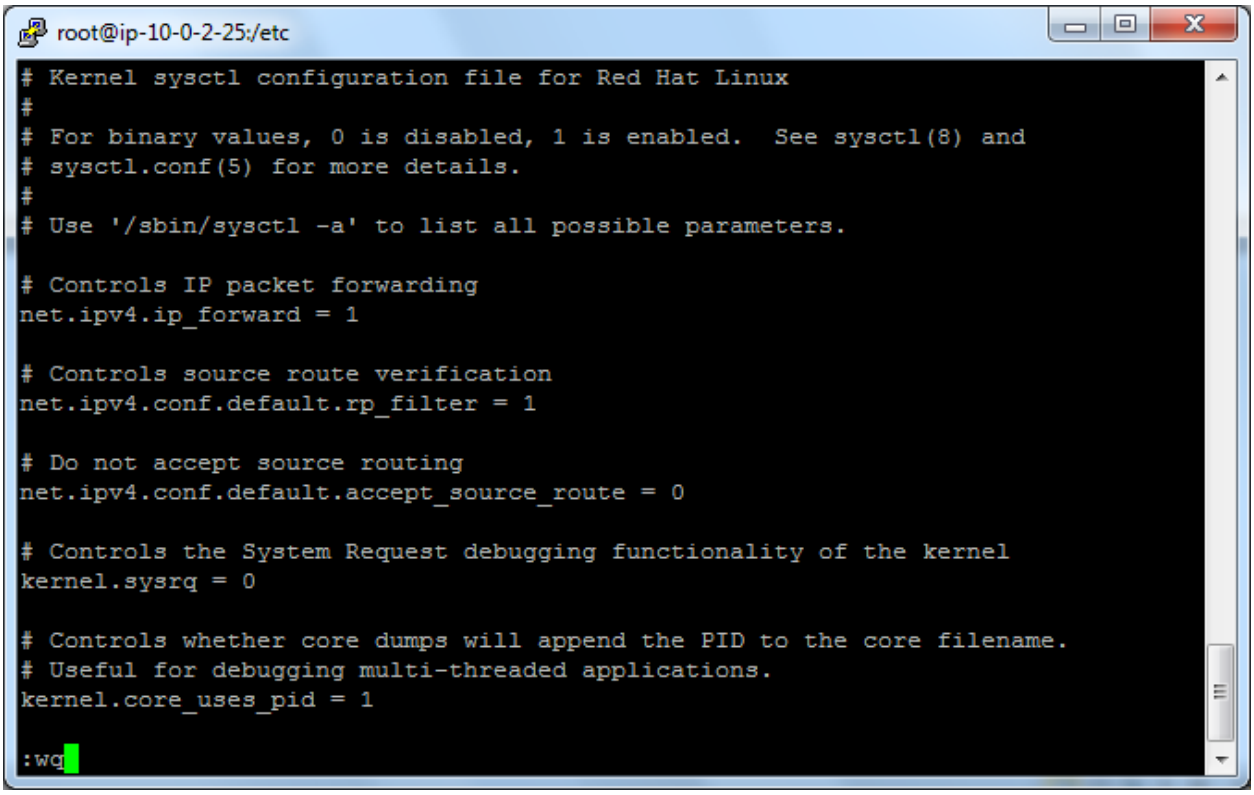
Press insert and then change the value as below.

Change

net.ipv4.ip_forward = 1



Press “Escape” key



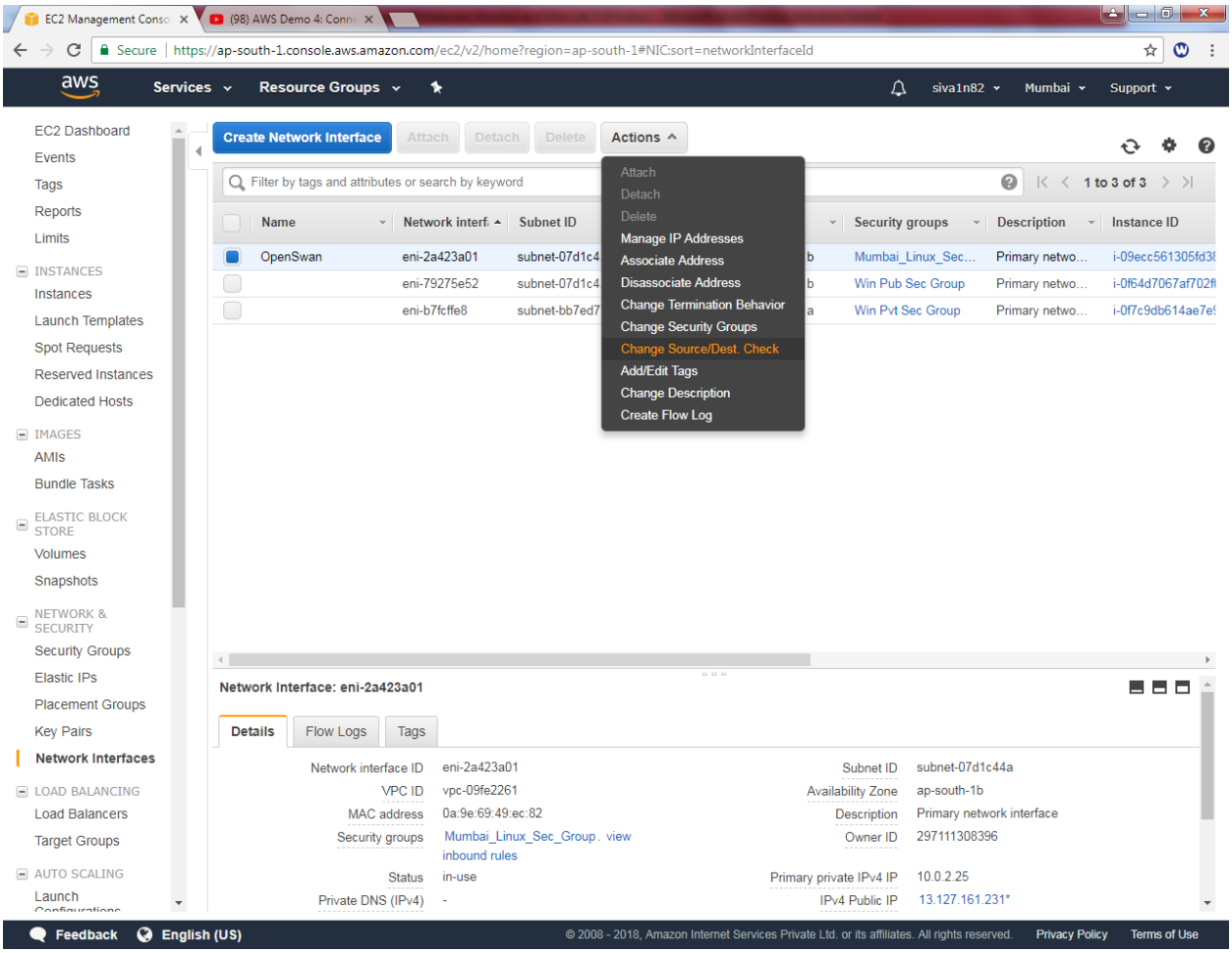
and then type

:wq

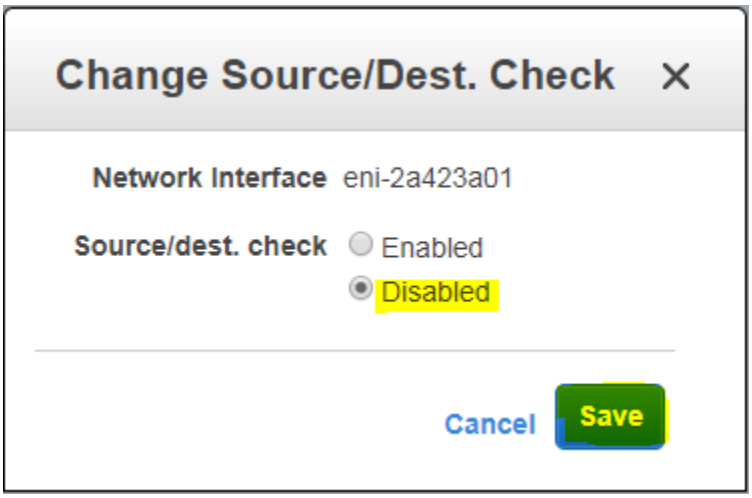
Go to Ec2 Dashboard

Click “Network interface” and then select “OpenSwan”

Click “Actions” → Click “Change source/destination check”

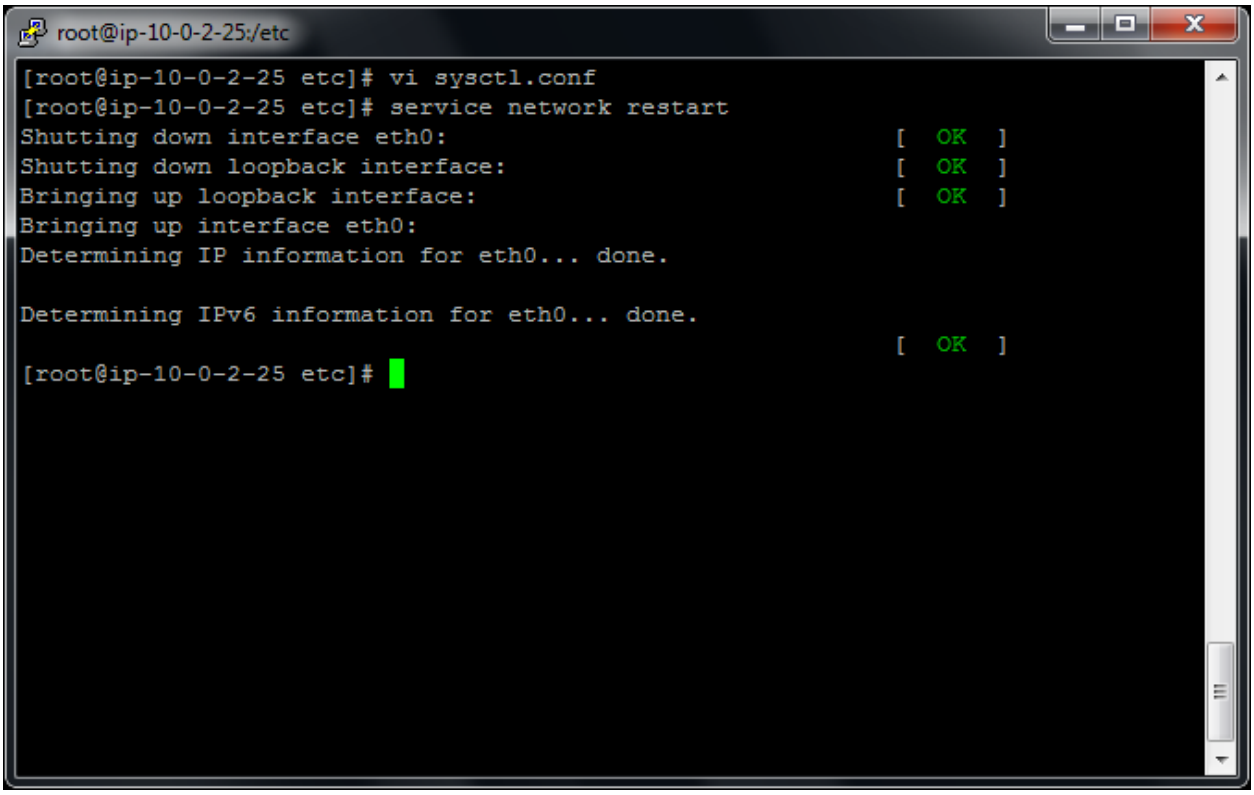


Set it as “Disabled”and click “save”.

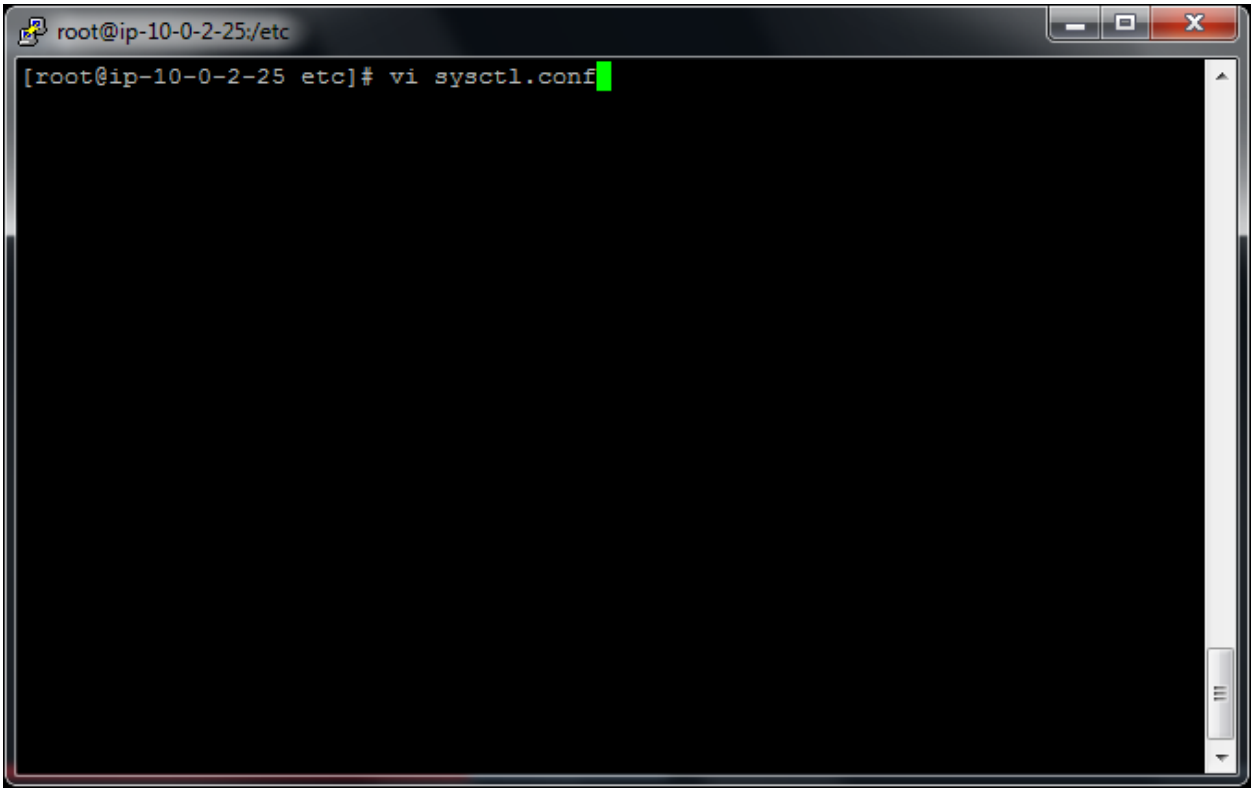


Type

Service network restart



Type vi sysctl.conf

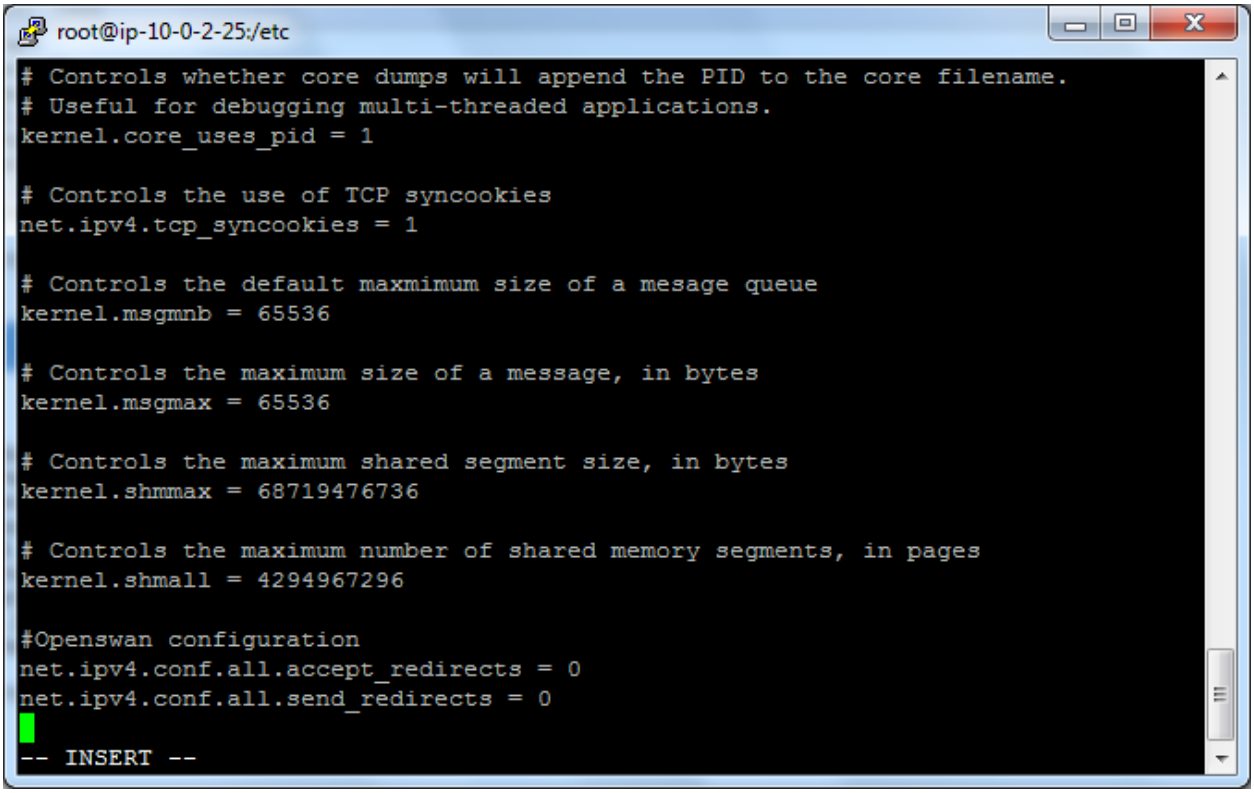


Press insert key

Type

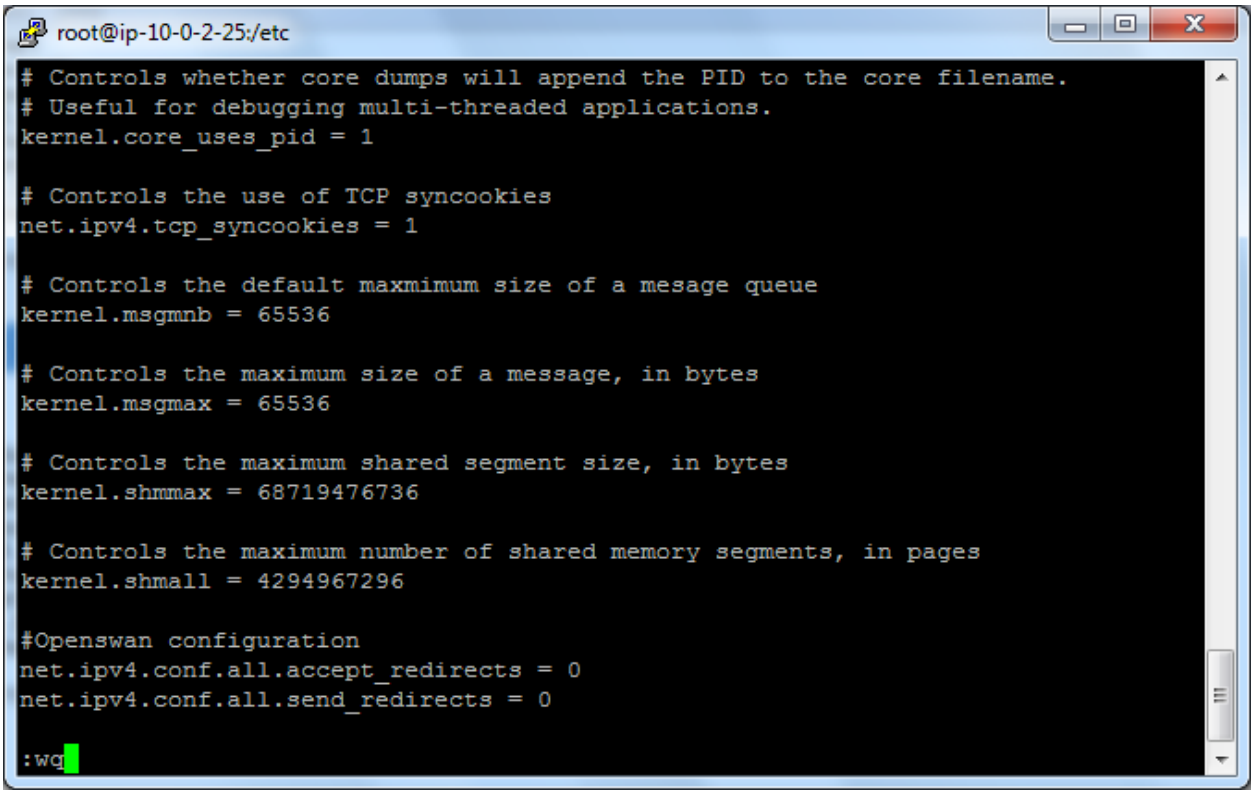
net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.all.send_redirects = 0



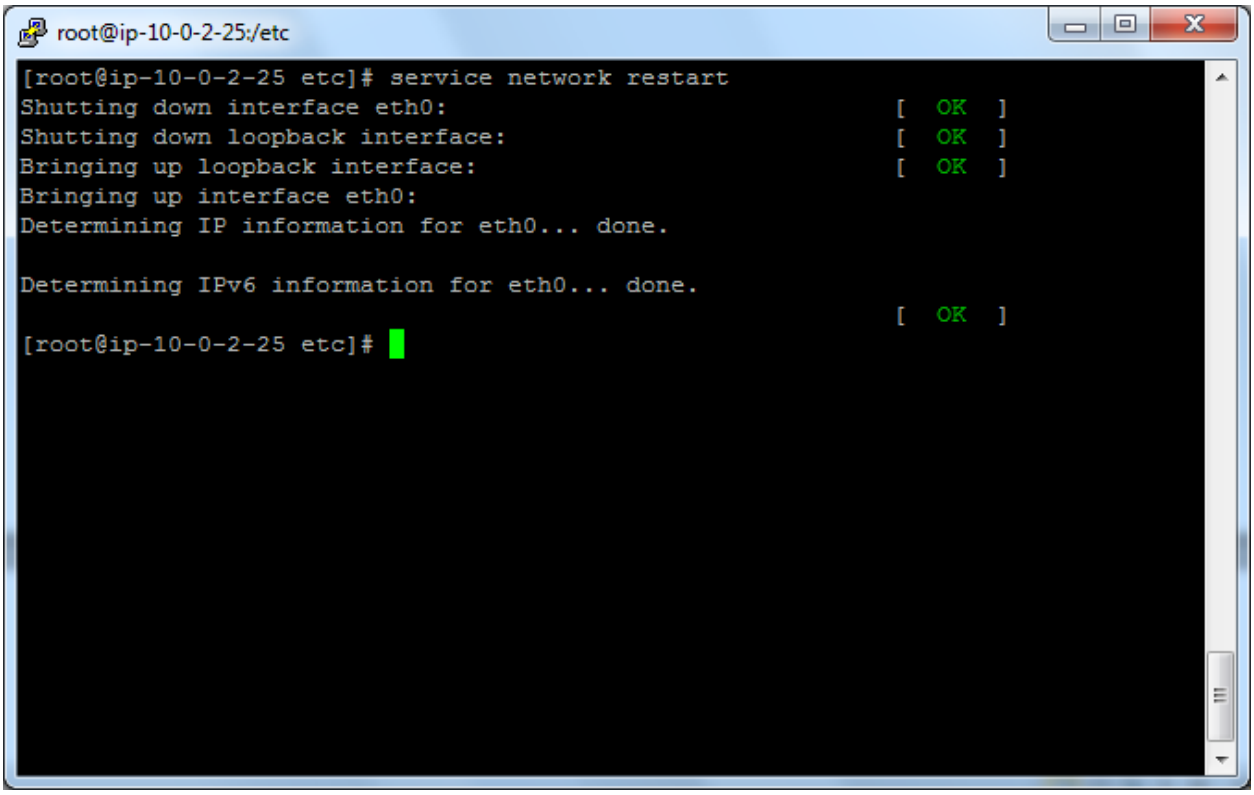
Press escape key and type

:wq



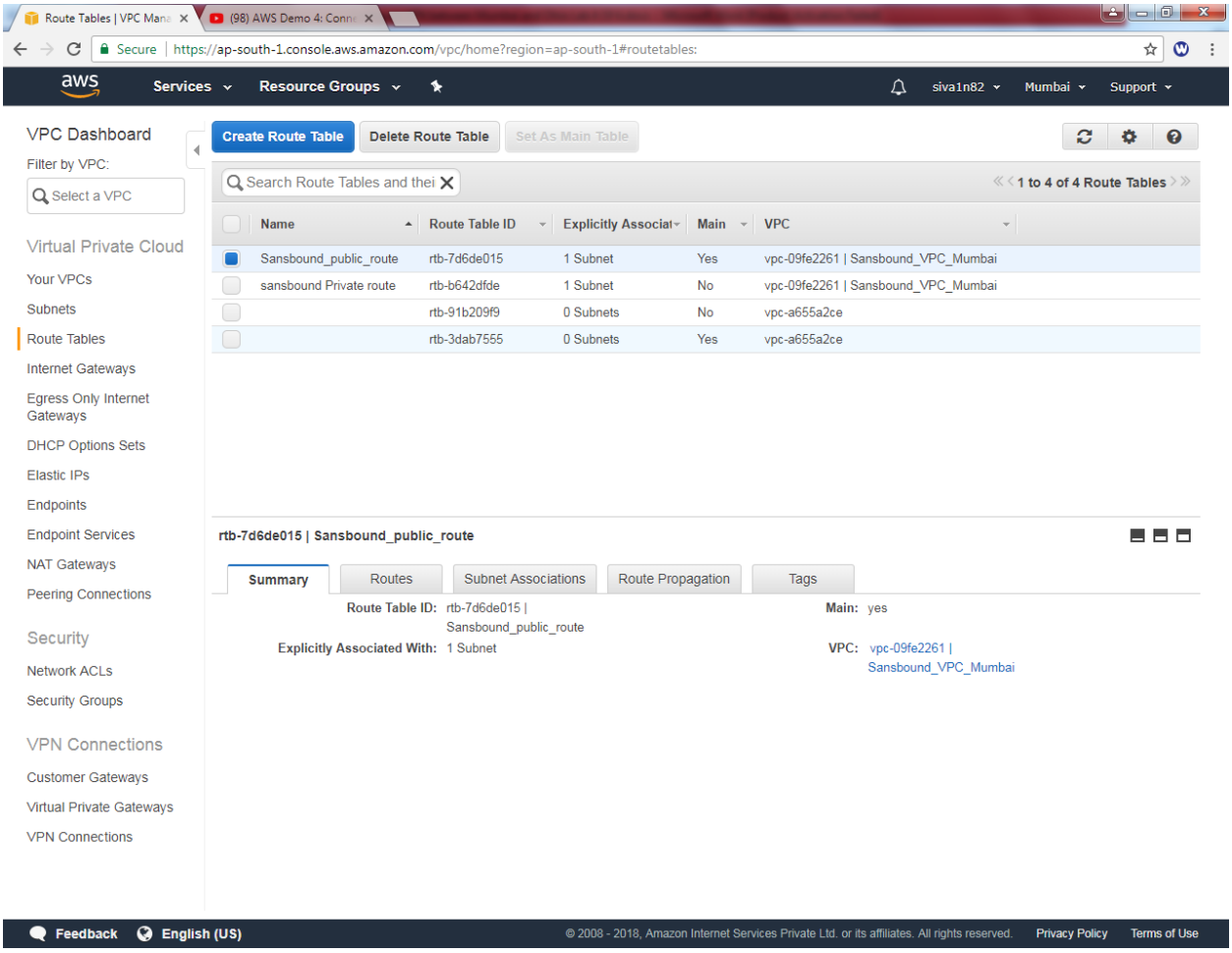
Type

Service network restart

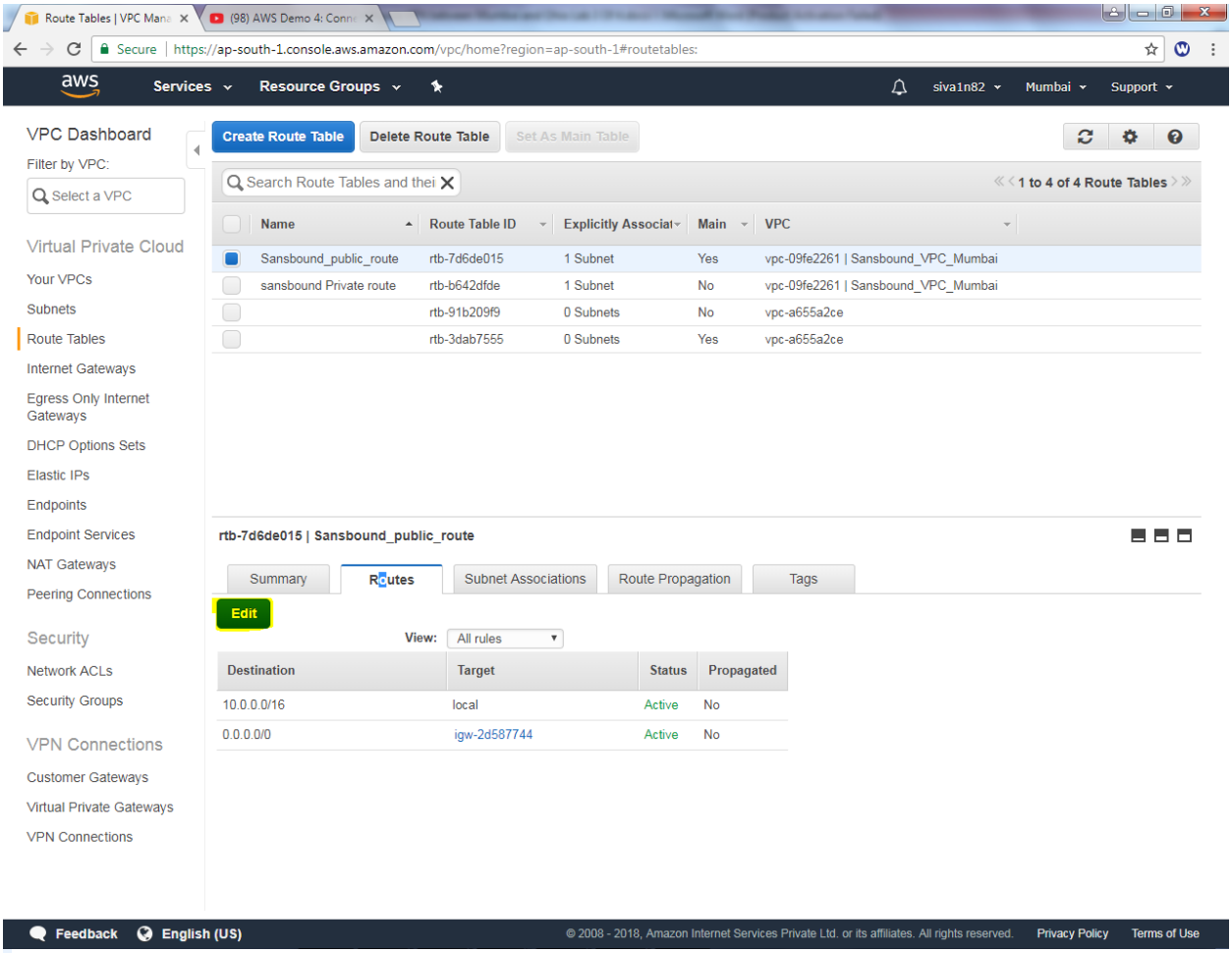


Go to VPC dashboard,

Click Route table, select sansbound public route table,

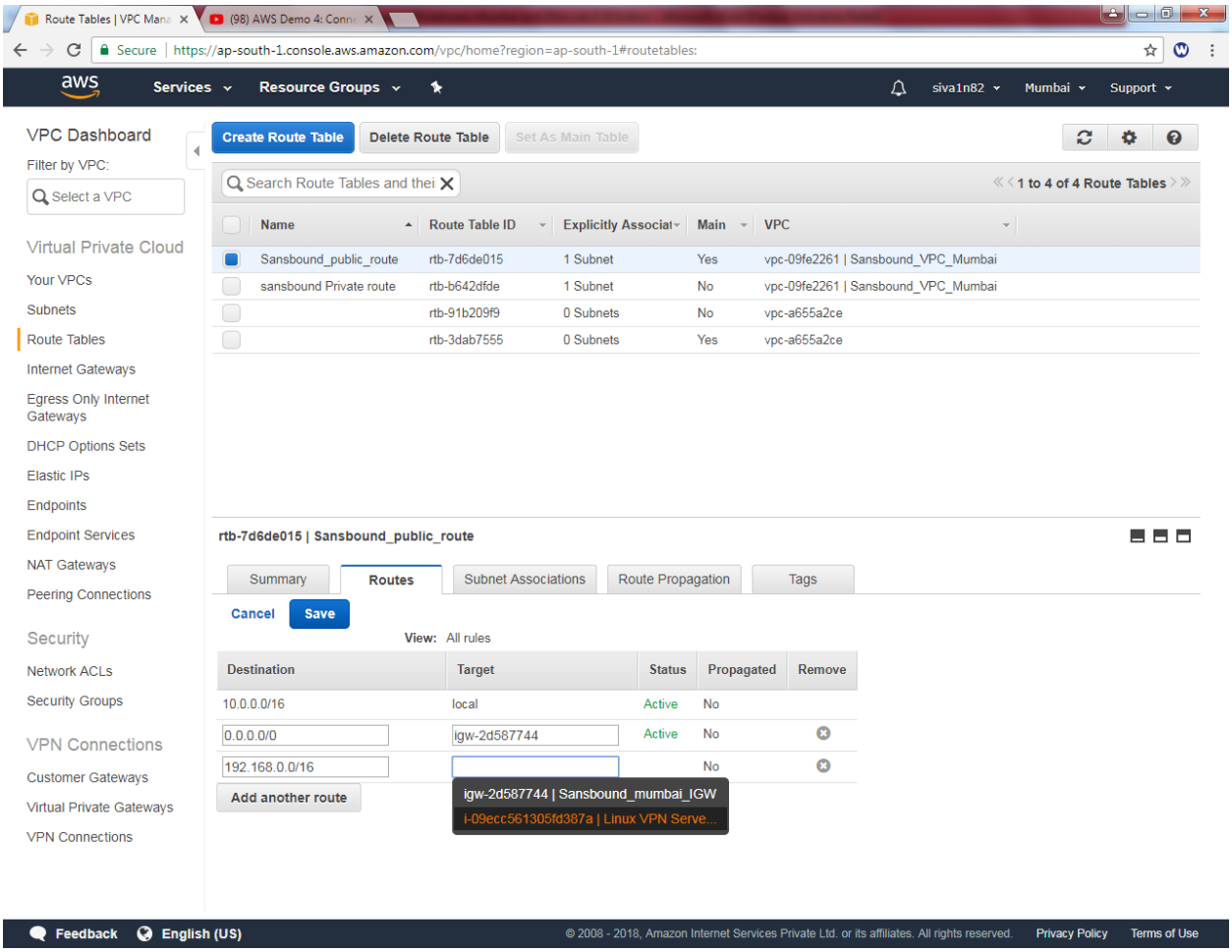


Click “Edit

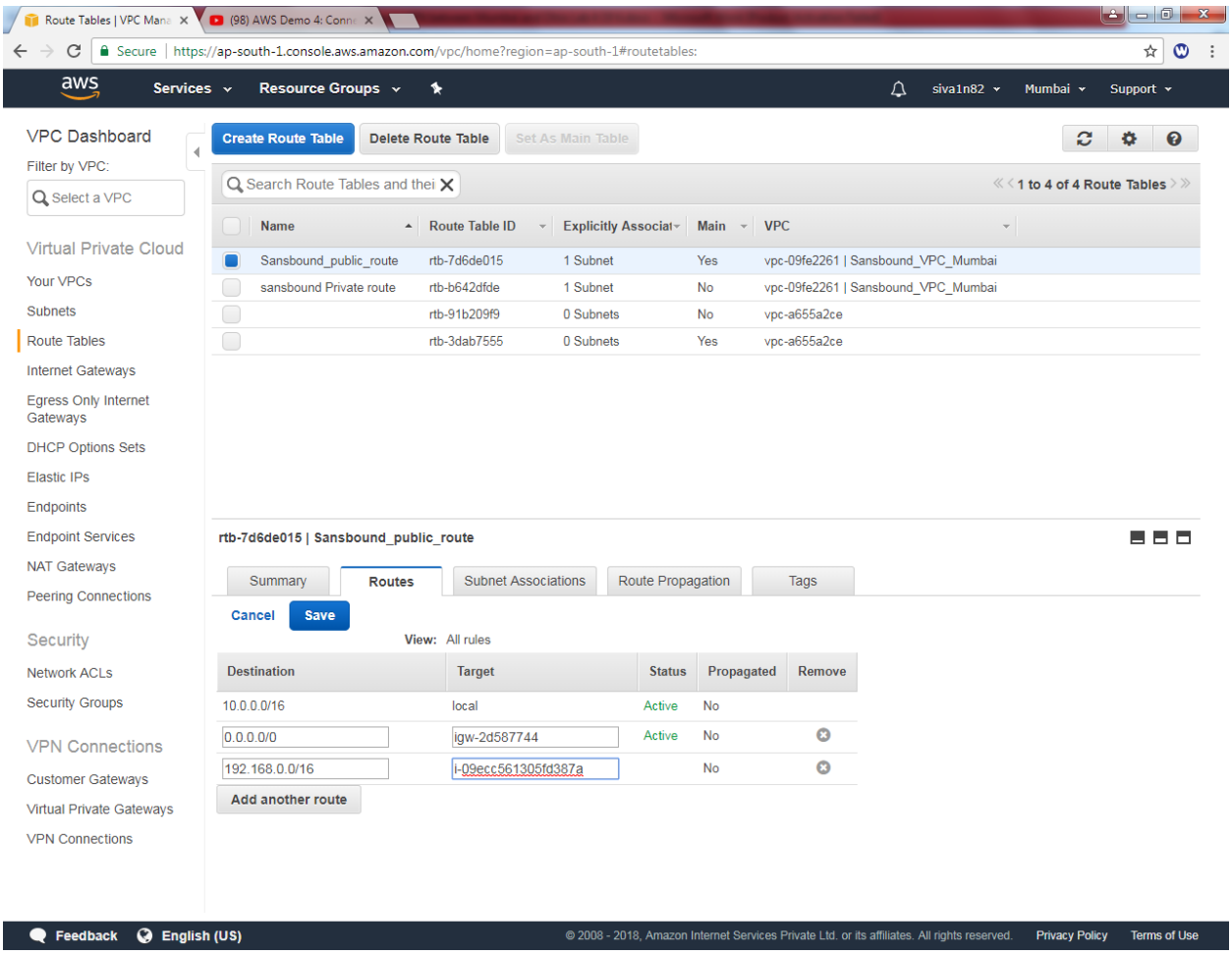

Route Tables | VPC Mana
(98) AWS Demo 4: Conne
Secure | https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#routetables:
aws
Services
Resource Groups
siva1n82
Mumbai
Support
VPC Dashboard
Filter by VPC:
Select a VPC
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
Endpoint Services
NAT Gateways
Peering Connections
Security
Network ACLs
Security Groups
VPN Connections
Customer Gateways
Virtual Private Gateways
VPN Connections
Create Route Table
Delete Route Table
Set As Main Table
Search Route Tables and thei
1 to 4 of 4 Route Tables
Name
Route Table ID
Explicitly Associat
Main
VPC
Sansbound_public_route
rtb-7d6de015
1 Subnet
Yes
vpc-09fe2261 | Sansbound_VPC_Mumbai
sansbound Private route
rtb-b642dfde
1 Subnet
No
vpc-09fe2261 | Sansbound_VPC_Mumbai
rtb-91b209f9
0 Subnets
No
vpc-a655a2ce
rtb-3dab7555
0 Subnets
Yes
vpc-a655a2ce
rtb-7d6de015 | Sansbound_public_route
Summary
Routes
Subnet Associations
Route Propagation
Tags
Edit
View:
All rules
Destination
Target
Status
Propagated
10.0.0.0/16
local
Active
No
0.0.0.0/0
igw-2d587744
Active
No
Feedback
English (US)
© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

”

Click “add another route” and then type 192.168.0.0/16 as destination and select “Linux VPN Server” as target.



Click “save”.


Route Tables | VPC Mana
(98) AWS Demo 4: Conne
Secure | https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#routetables:
aws
Services
Resource Groups
sivain82
Mumbai
Support
VPC Dashboard
Filter by VPC:
Select a VPC
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
Endpoint Services
NAT Gateways
Peering Connections
Security
Network ACLs
Security Groups
VPN Connections
Customer Gateways
Virtual Private Gateways
VPN Connections
Create Route Table
Delete Route Table
Set As Main Table
Search Route Tables and thei
1 to 4 of 4 Route Tables
Name
Route Table ID
Explicitly Associat
Main
VPC
Sansbound_public_route
rtb-7d6de015
1 Subnet
Yes
vpc-09fe2261 | Sansbound_VPC_Mumbai
sansbound Private route
rtb-b642dfde
1 Subnet
No
vpc-09fe2261 | Sansbound_VPC_Mumbai
rtb-91b209f9
0 Subnets
No
vpc-a655a2ce
rtb-3dab7555
0 Subnets
Yes
vpc-a655a2ce
rtb-7d6de015 | Sansbound_public_route
Summary
Routes
Subnet Associations
Route Propagation
Tags
Cancel
Save
View: All rules
Destination
Target
Status
Propagated
Remove
10.0.0.0/16
local
Active
No
0.0.0.0/0
igw-2d587744
Active
No
192.168.0.0/16
i-09ecc561305fd387a
No
Add another route
Feedback
English (US)
© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

Detailed information of route table.