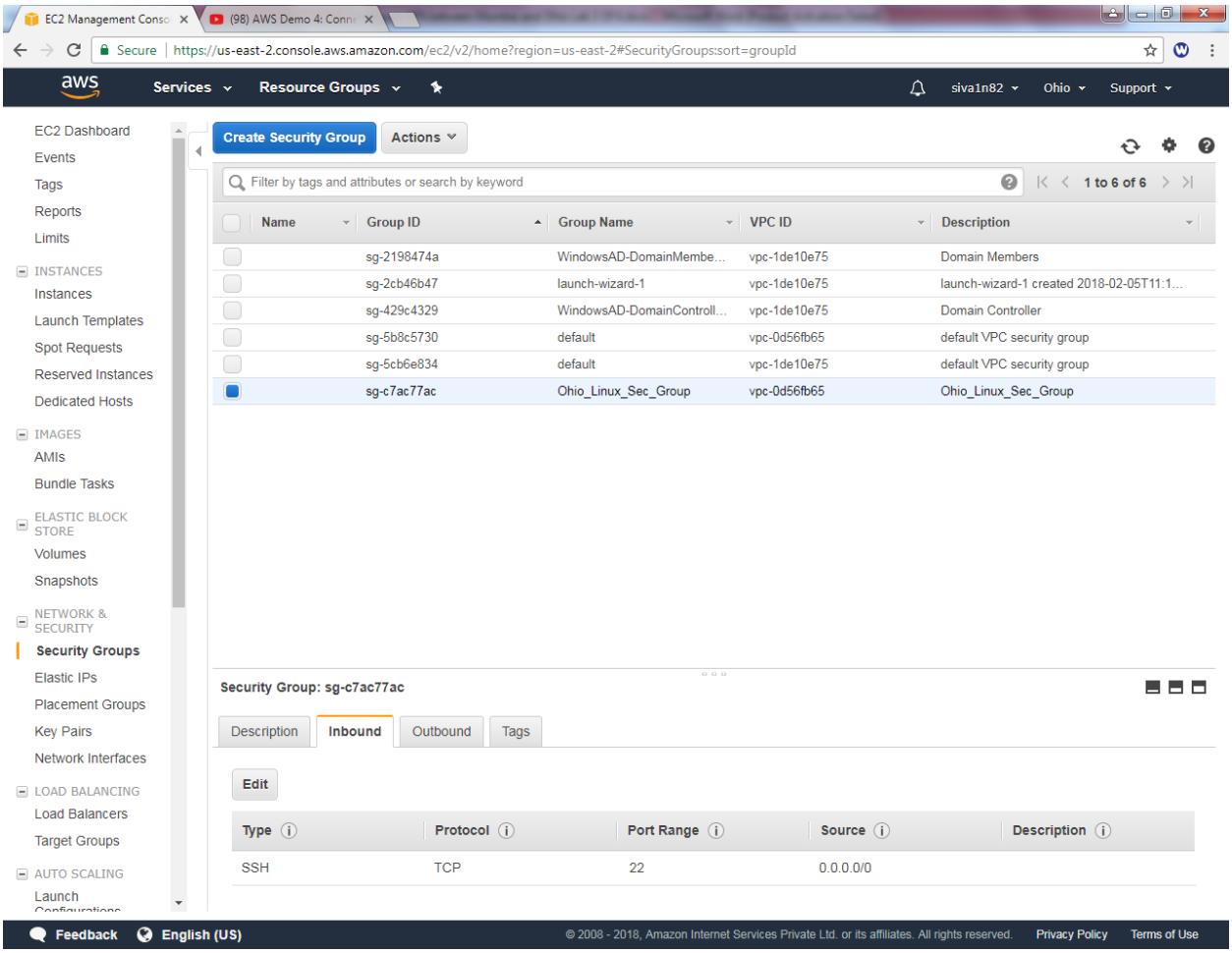
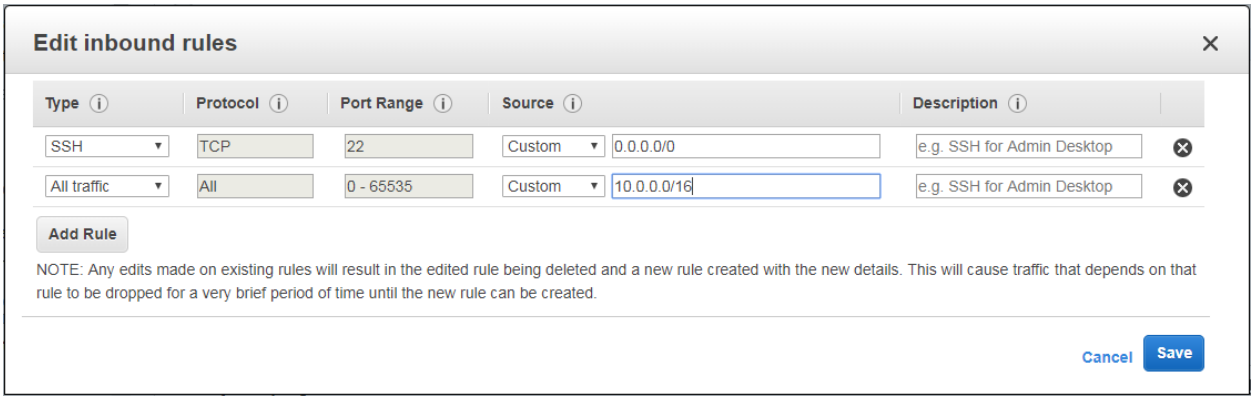
Configure VPN between Mumbai and Ohio Lab 4 of 4

Go to Ohio region, to view the public ip for the network interface (18.218.11.25)

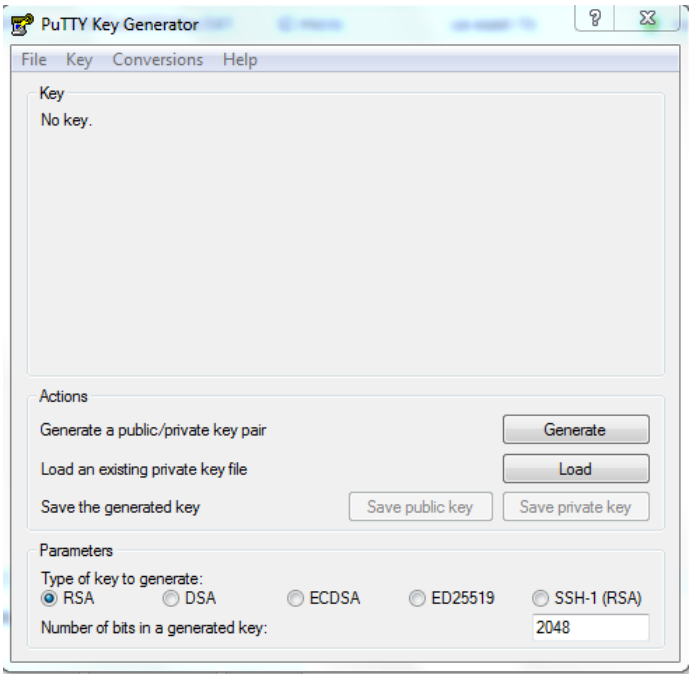
Select security group we need to allow all traffic for 10.0.0.0/16 subnet.



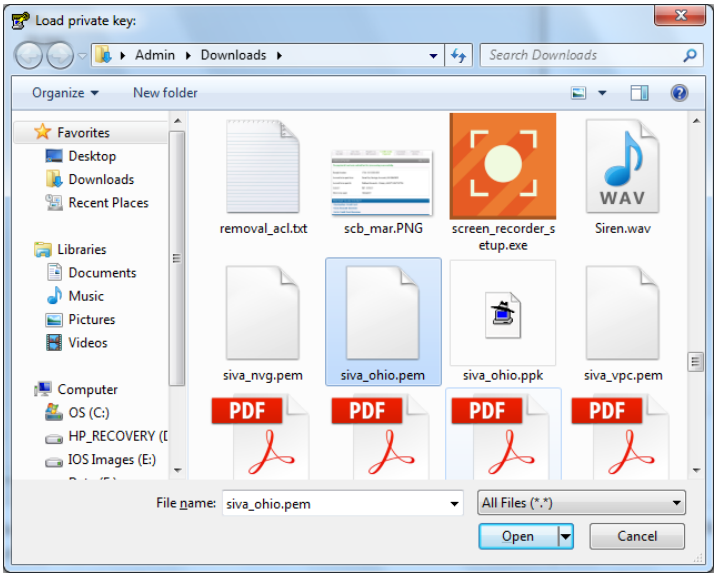
Click Add rule and allow All traffic type source as 10.0.0.0/16 subnet then click “Save”.

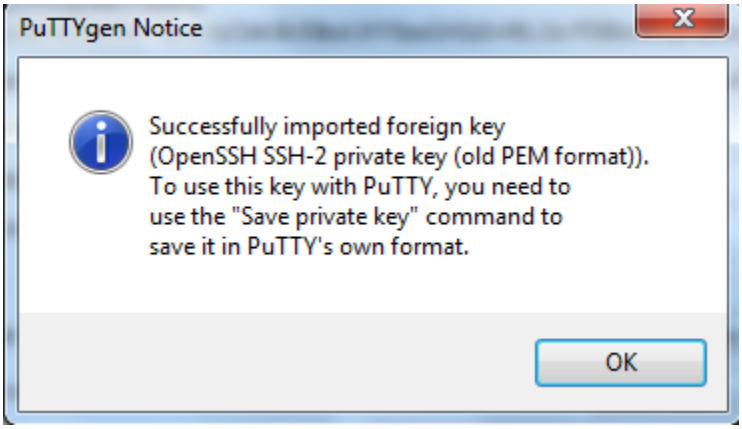


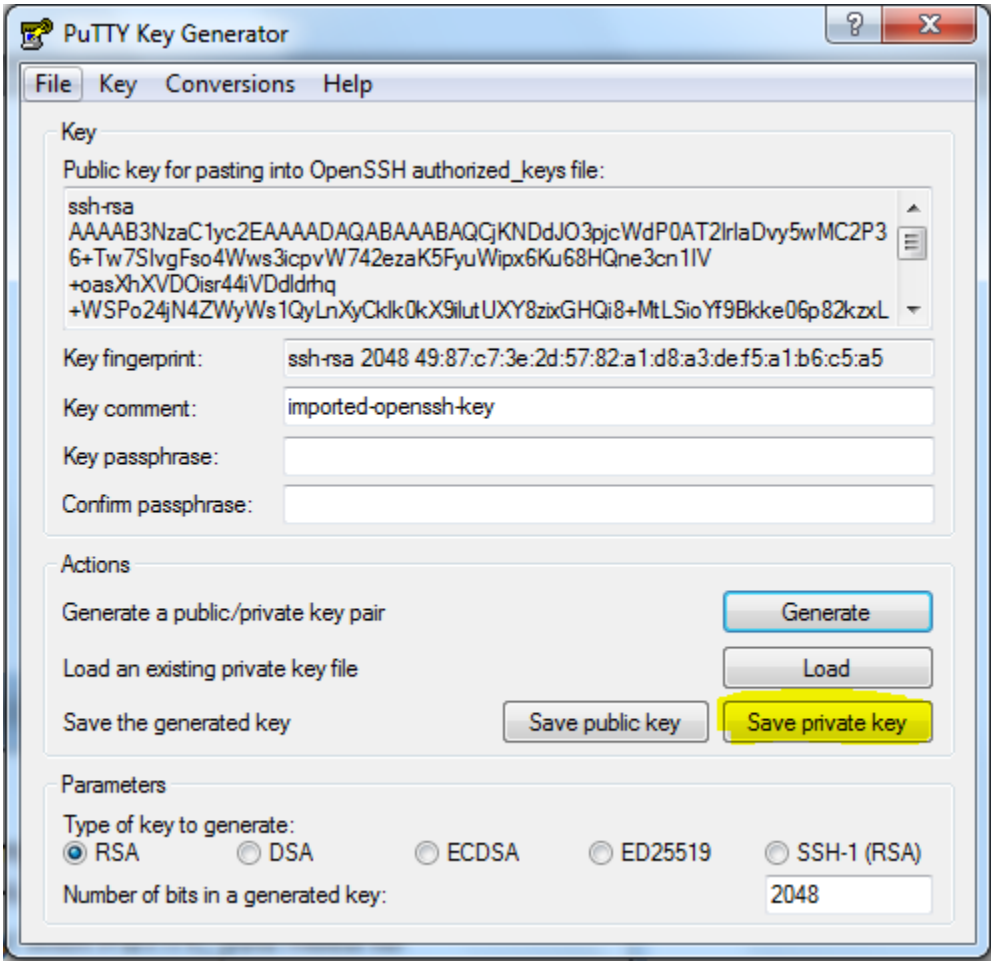
Go to Putty key gen installed in your local machine.

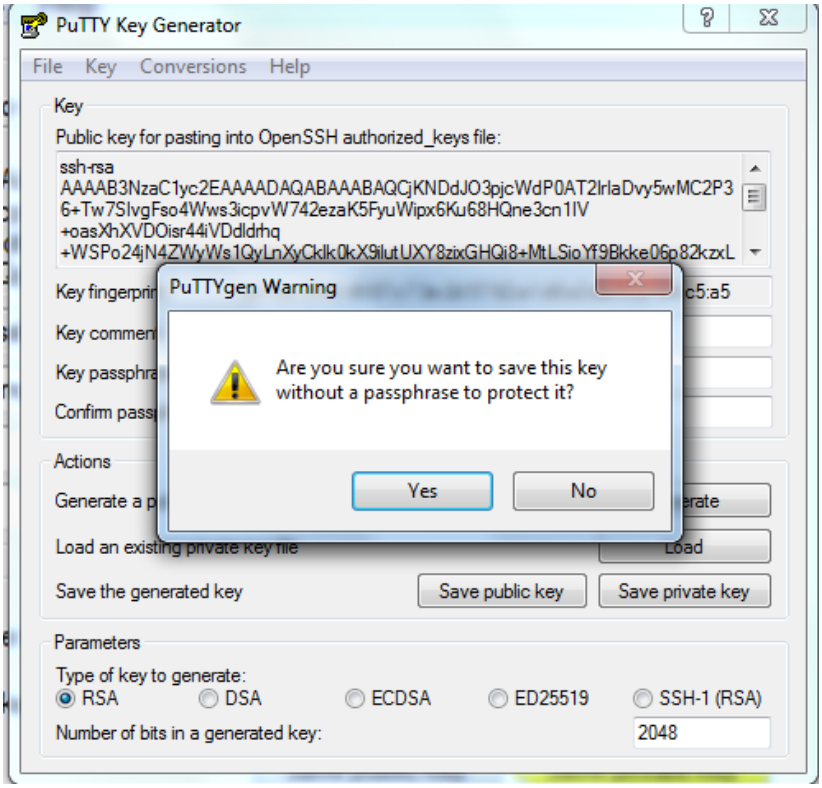


Locate the file and click “Open”.

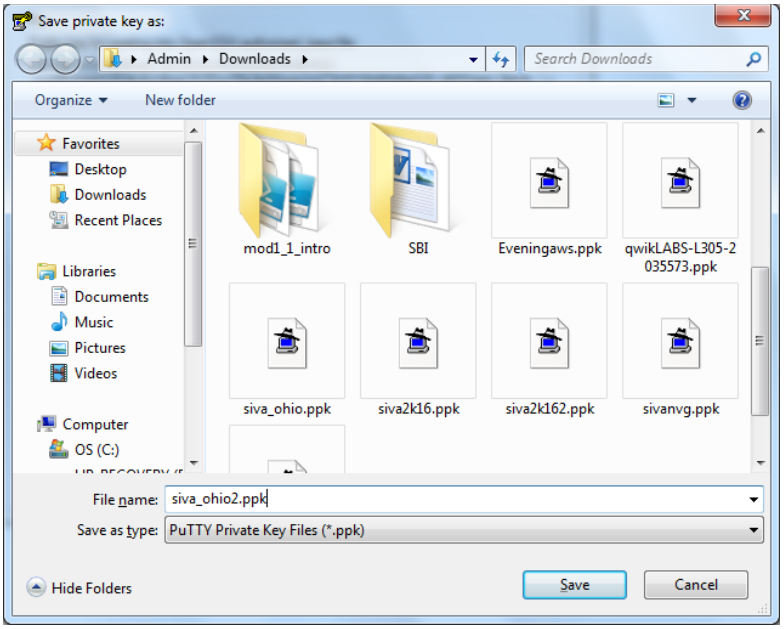

Load private key:
Admin ▸ Downloads ▸
Search Downloads
Organize
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
OS (C:)
HP_RECOVERY (D
IOS Images (E:)
removal_acl.txt
scb_mar.PNG
screen_recorder_setup.exe
Siren.wav
siva_nvg.pem
siva_ohio.pem
siva_ohio.ppk
siva_vpc.pem
File name: siva_ohio.pem
All Files (*.*)
Open
Cancel

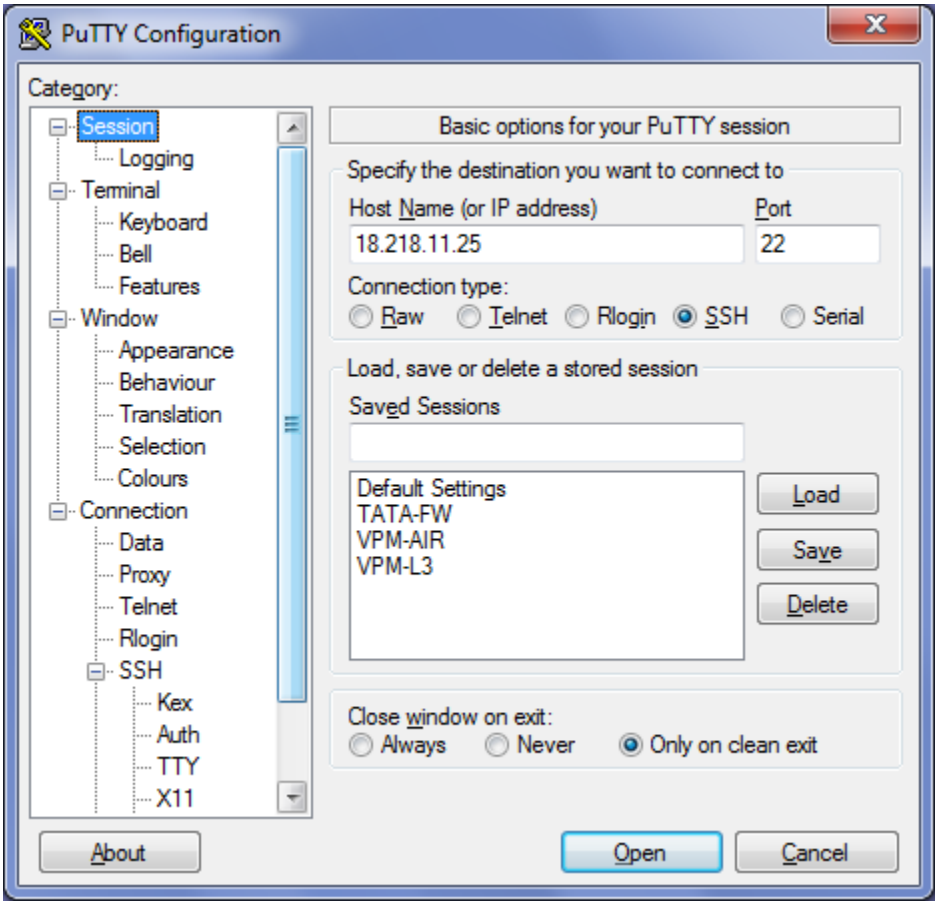

PuTTYgen Notice
Successfully imported foreign key
(OpenSSH SSH-2 private key (old PEM format)).
To use this key with PuTTY, you need to
use the "Save private key" command to
save it in PuTTY's own format.
OK


PuTTY Key Generator
File
Key
Conversions
Help
Key
Public key for pasting into OpenSSH authorized_keys file:
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCjKNDdJO3pjcWdP0AT2lrlaDvy5wMC2P3
6+Tw7SlvgFso4Wws3icpvW742ezaK5FyuWipx6Ku68HQne3cn1IV
+oasXhXVDOisr44iVDdldrhq
+WSPo24jN4ZWyWs1QyLnXyCklk0kX9ilutUXY8zixGHQi8+MtLSioYf9Bkke06p82kzxL
Key fingerprint:
ssh-rsa 2048 49:87:c7:3e:2d:57:82:a1:d8:a3:de:f5:a1:b6:c5:a5
Key comment:
imported-openssh-key
Key passphrase:
Confirm passphrase:
Actions
Generate a public/private key pair
Generate
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

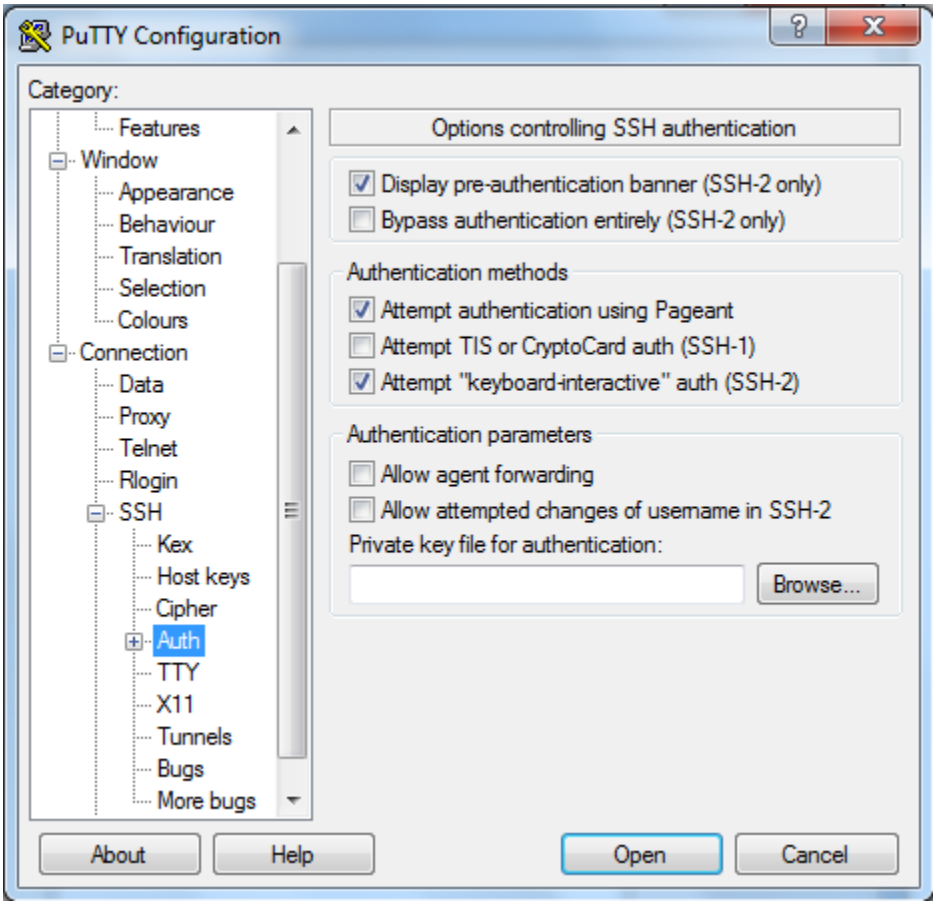


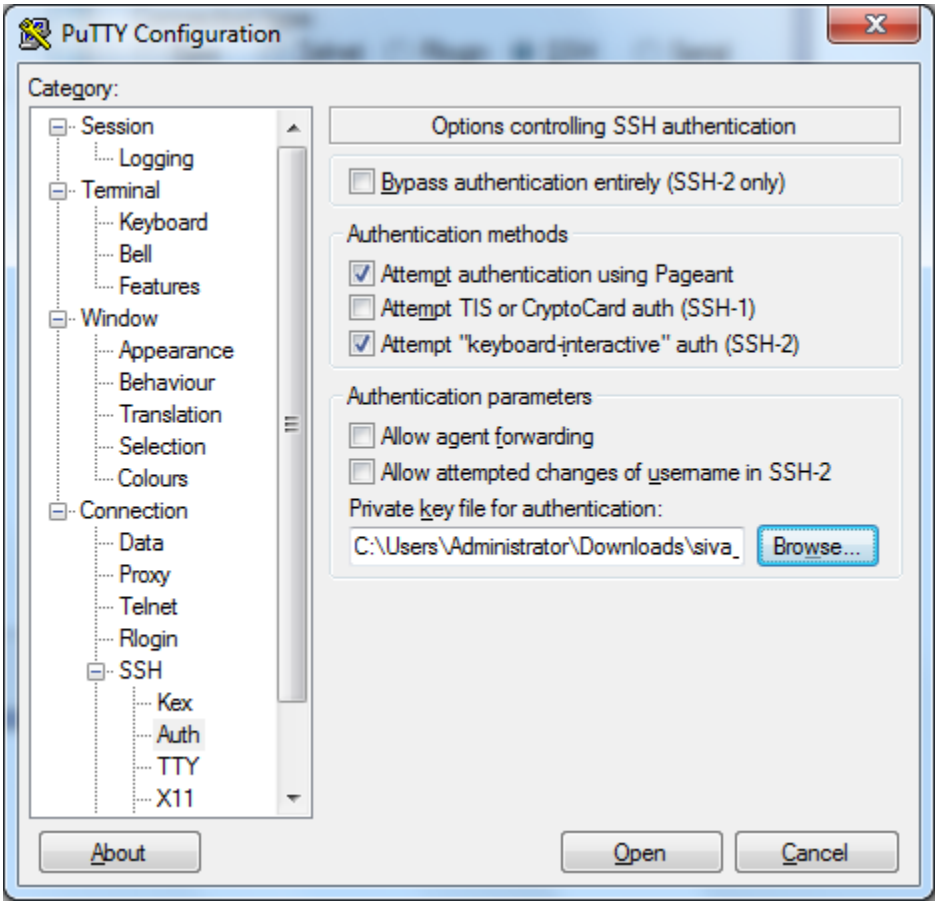
Locate the file to save.

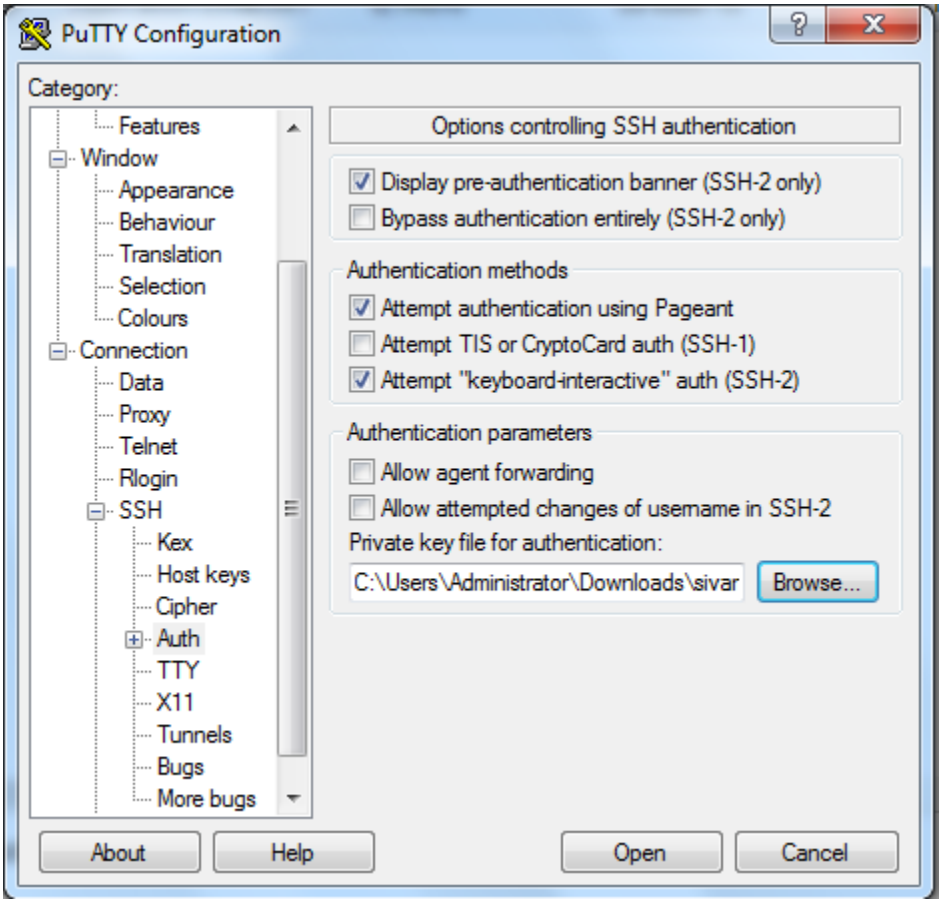


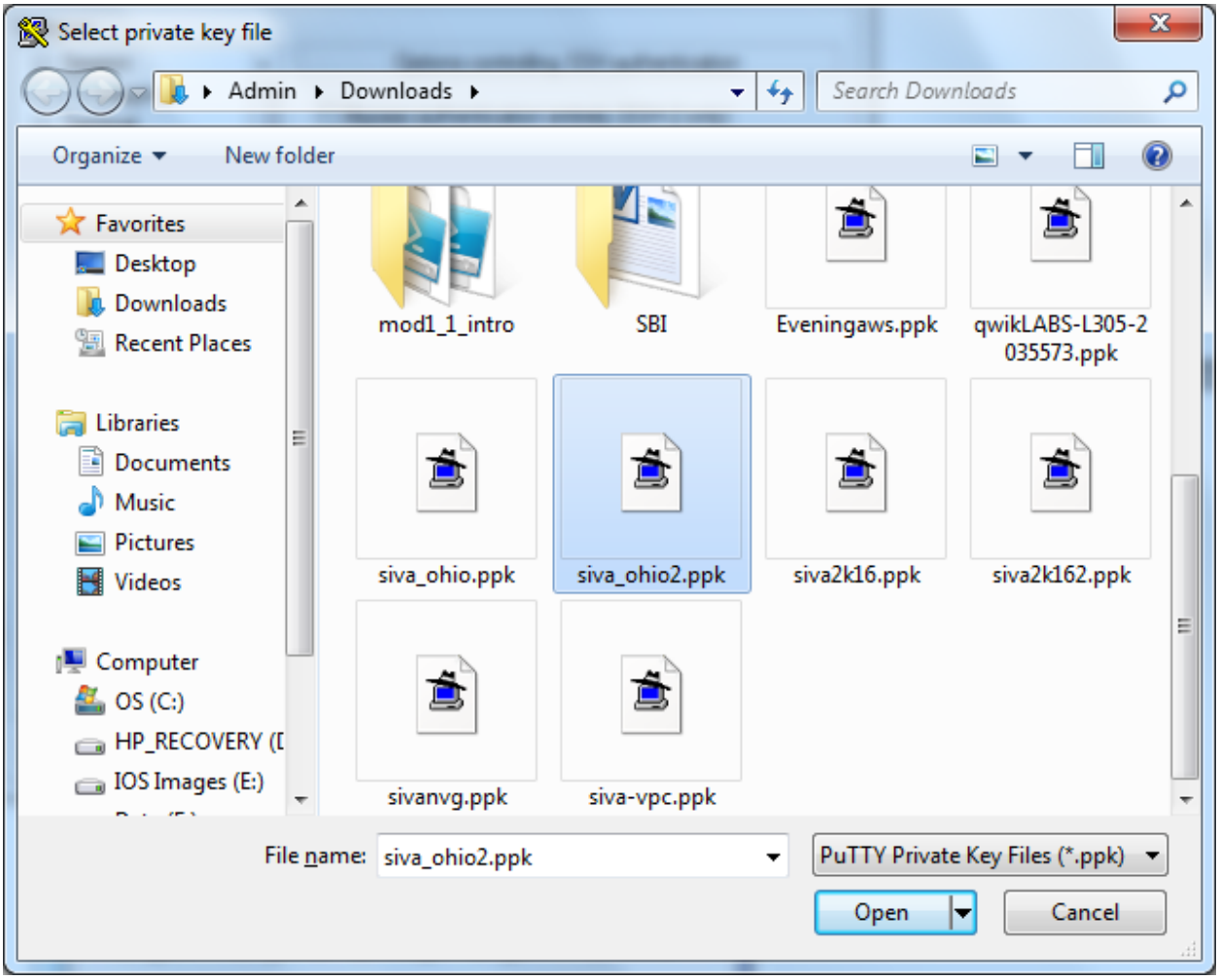

PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Auth
TTY
X11
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
18.218.11.25
22
Connection type:
Raw
Telnet
Rlogin
SSH
Serial
Load, save or delete a stored session
Saved Sessions
Default Settings
TATA-FW
VPM-AIR
VPM-L3
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Open
Cancel

Click Browse and locate the *.ppk file.

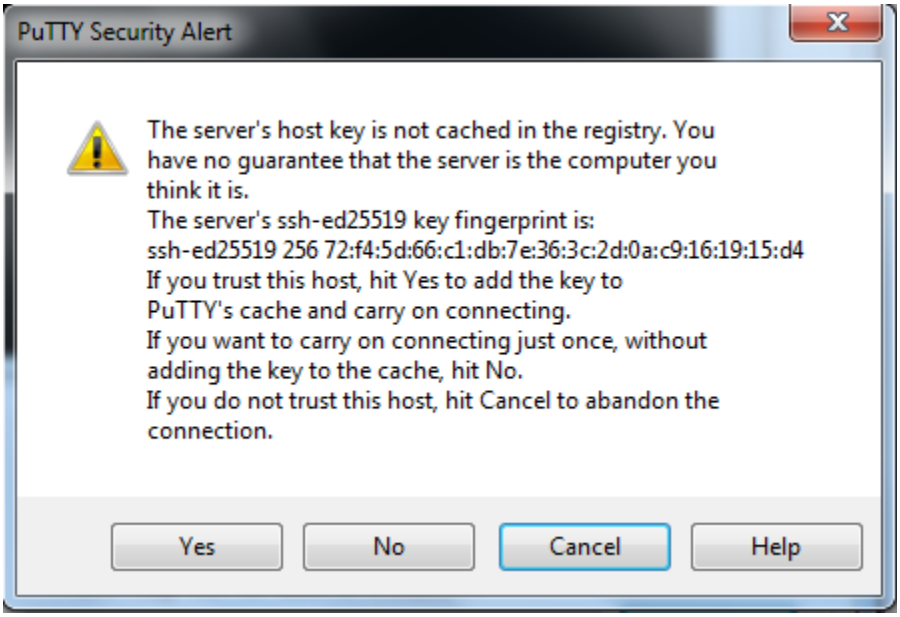


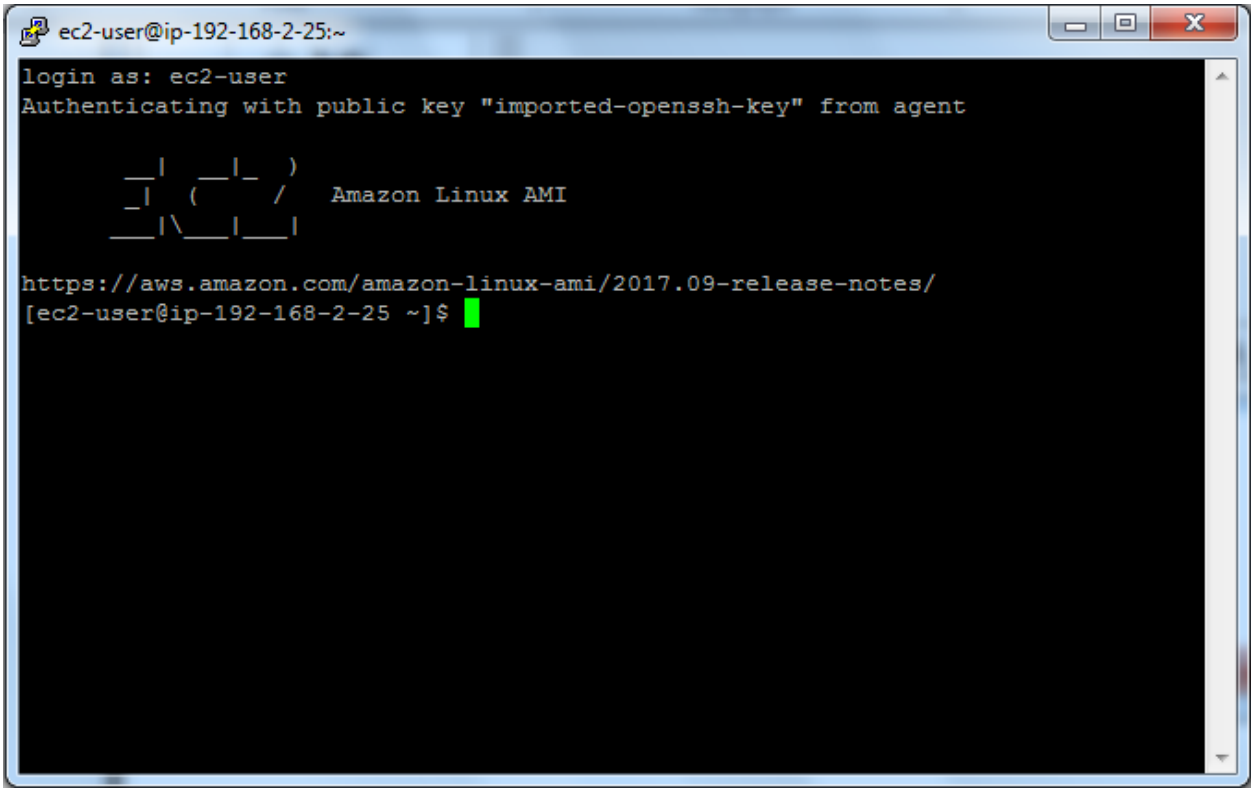

PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Auth
TTY
X11
Options controlling SSH authentication
Bypass authentication entirely (SSH-2 only)
Authentication methods
Attempt authentication using Pageant
Attempt TIS or CryptoCard auth (SSH-1)
Attempt "keyboard-interactive" auth (SSH-2)
Authentication parameters
Allow agent forwarding
Allow attempted changes of username in SSH-2
Private key file for authentication:
C:\Users\Administrator\Downloads\siva_
Browse...
About
Open
Cancel


PuTTY Configuration
Category:
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Host keys
Cipher
Auth
TTY
X11
Tunnels
Bugs
More bugs
Options controlling SSH authentication
Display pre-authentication banner (SSH-2 only)
Bypass authentication entirely (SSH-2 only)
Authentication methods
Attempt authentication using Pageant
Attempt TIS or CryptoCard auth (SSH-1)
Attempt "keyboard-interactive" auth (SSH-2)
Authentication parameters
Allow agent forwarding
Allow attempted changes of username in SSH-2
Private key file for authentication:
C:\Users\Administrator\Downloads\sivar
Browse...
About
Help
Open
Cancel



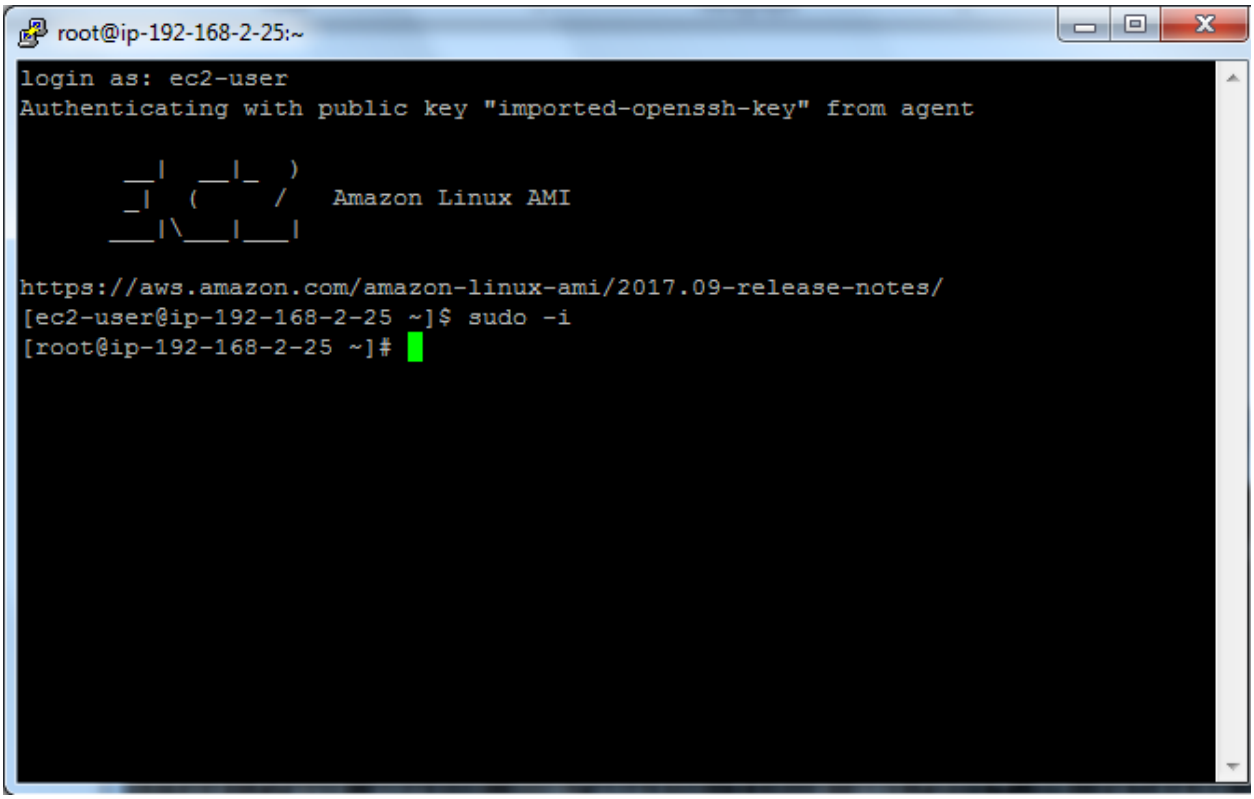
Select the file and Click “Open”.


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 72:f4:5d:66:c1:db:7e:36:3c:2d:0a:c9:16:19:15:d4
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-192-168-2-25:~
login as: ec2-user
Authenticating with public key "imported-openssh-key" from agent
__| __|_)
_| (/ Amazon Linux AMI
___|___|___|
https://aws.amazon.com/amazon-linux-ami/2017.09-release-notes/
[ec2-user@ip-192-168-2-25 ~]$

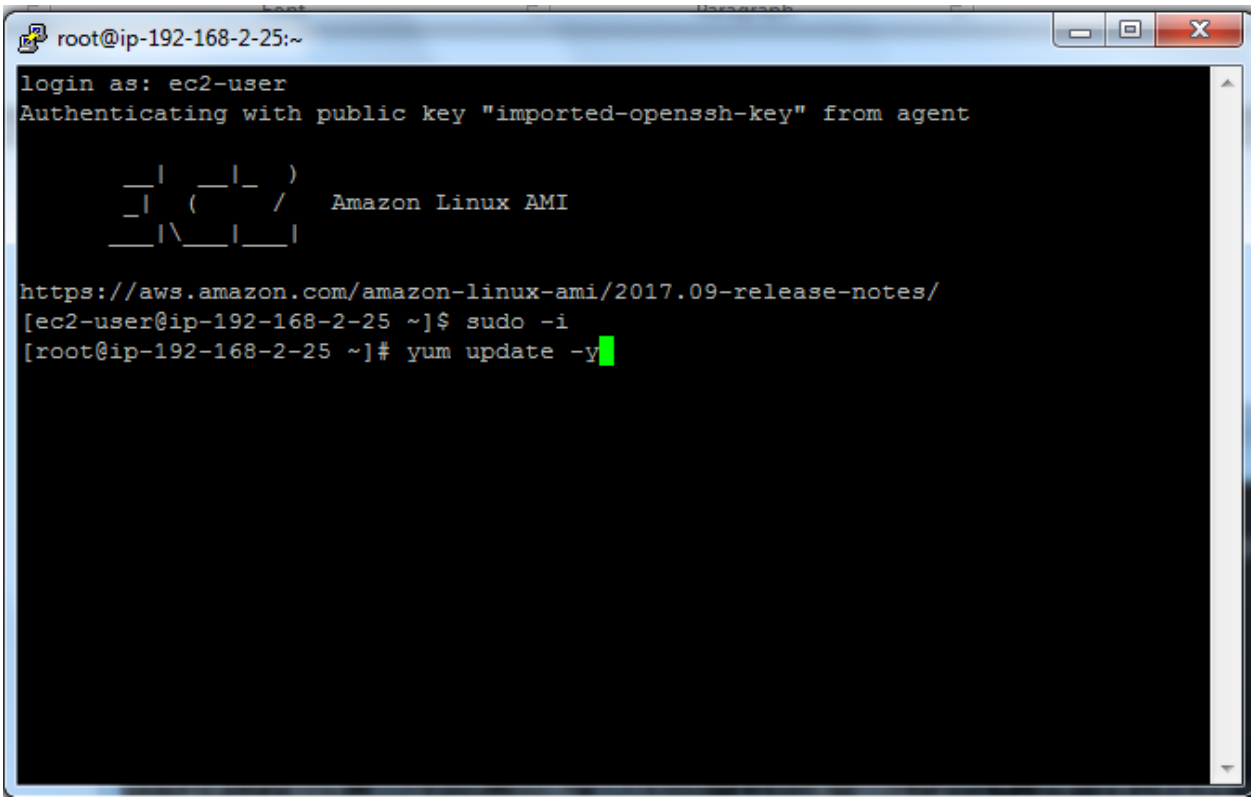
Type

Sudo -i


root@ip-192-168-2-25:~
login as: ec2-user
Authenticating with public key "imported-openssh-key" from agent
__| __|_)
_| (/ Amazon Linux AMI
___|___|___|
https://aws.amazon.com/amazon-linux-ami/2017.09-release-notes/
[ec2-user@ip-192-168-2-25 ~]$ sudo -i
[root@ip-192-168-2-25 ~]#

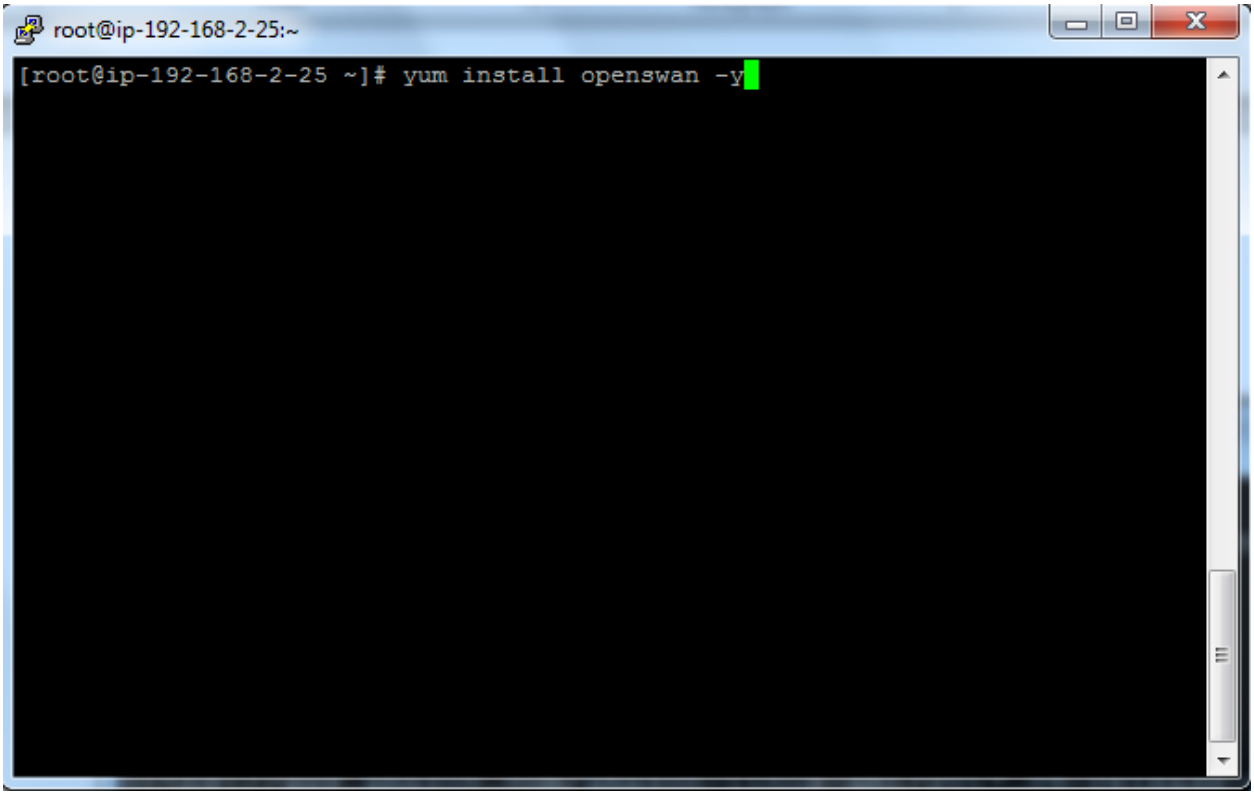
Type

Yum update –y



Type

Yum install openswan -y

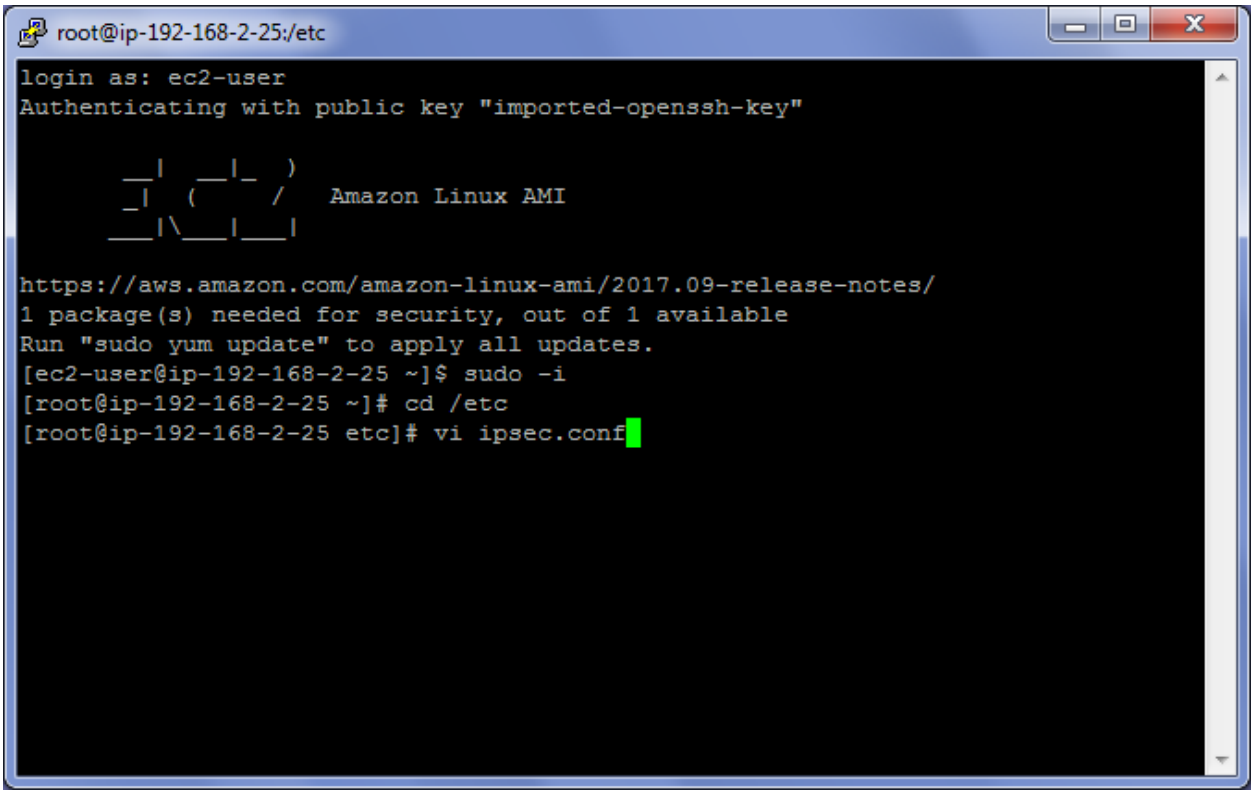


Open swan has been successfully installed.

```
root@ip-192-168-2-25:~
Total download size: 1.4 M
Installed size: 3.1 M
Downloading packages:
(1/2): compat-gmp4-4.3.2-1.14.amzn1.x86_64.rpm            | 302 kB   00:00
(2/2): openswan-2.6.37-3.17.amzn1.x86_64.rpm              | 1.1 MB   00:00
--------------------------------------------------------------------------------
Total                                              1.8 MB/s | 1.4 MB  00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : compat-gmp4-4.3.2-1.14.amzn1.x86_64                         1/2
  Installing : openswan-2.6.37-3.17.amzn1.x86_64                           2/2
  Verifying  : openswan-2.6.37-3.17.amzn1.x86_64                           1/2
  Verifying  : compat-gmp4-4.3.2-1.14.amzn1.x86_64                         2/2

Installed:
  openswan.x86_64 0:2.6.37-3.17.amzn1

Dependency Installed:
  compat-gmp4.x86_64 0:4.3.2-1.14.amzn1

Complete!
[root@ip-192-168-2-25 ~]#
```

Type

Vi ipsec.conf

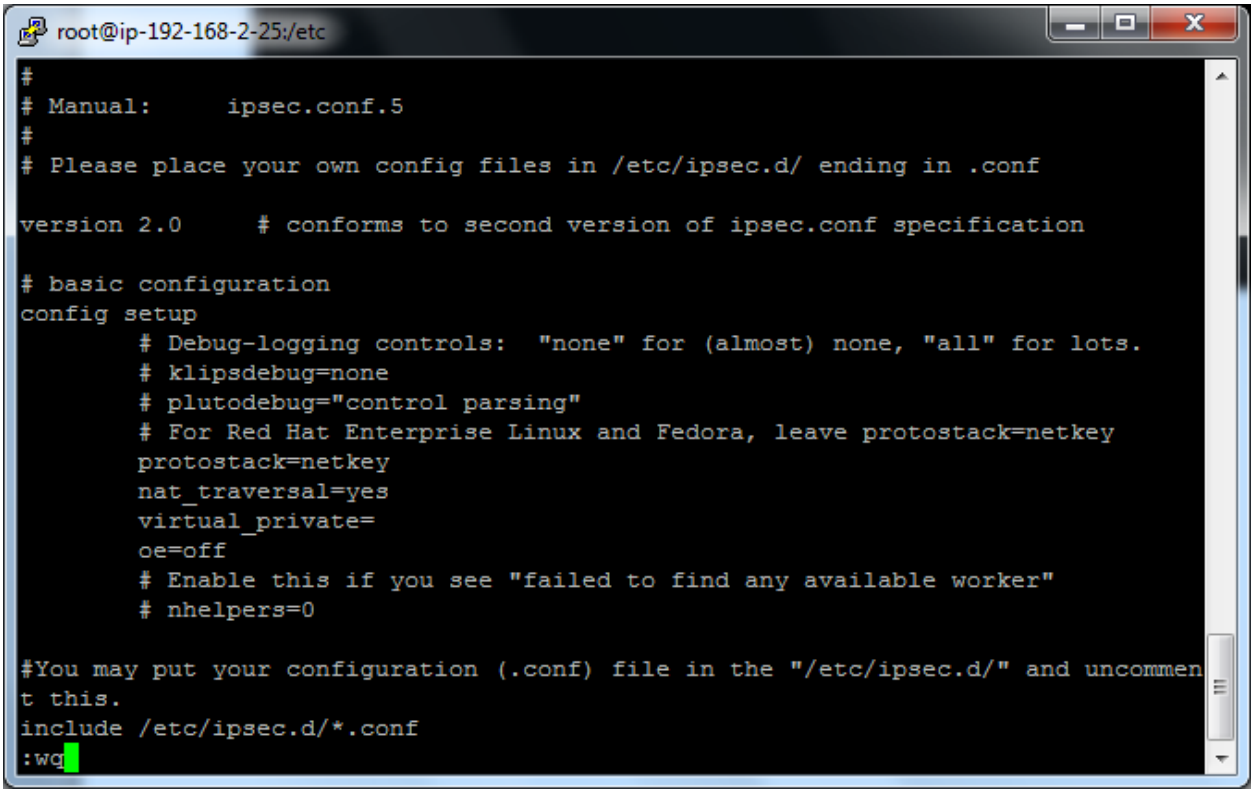


Press insert and remove # from #include /etc/

```
root@ip-192-168-2-25:/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
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"ipsec.conf" 24L, 784C
```

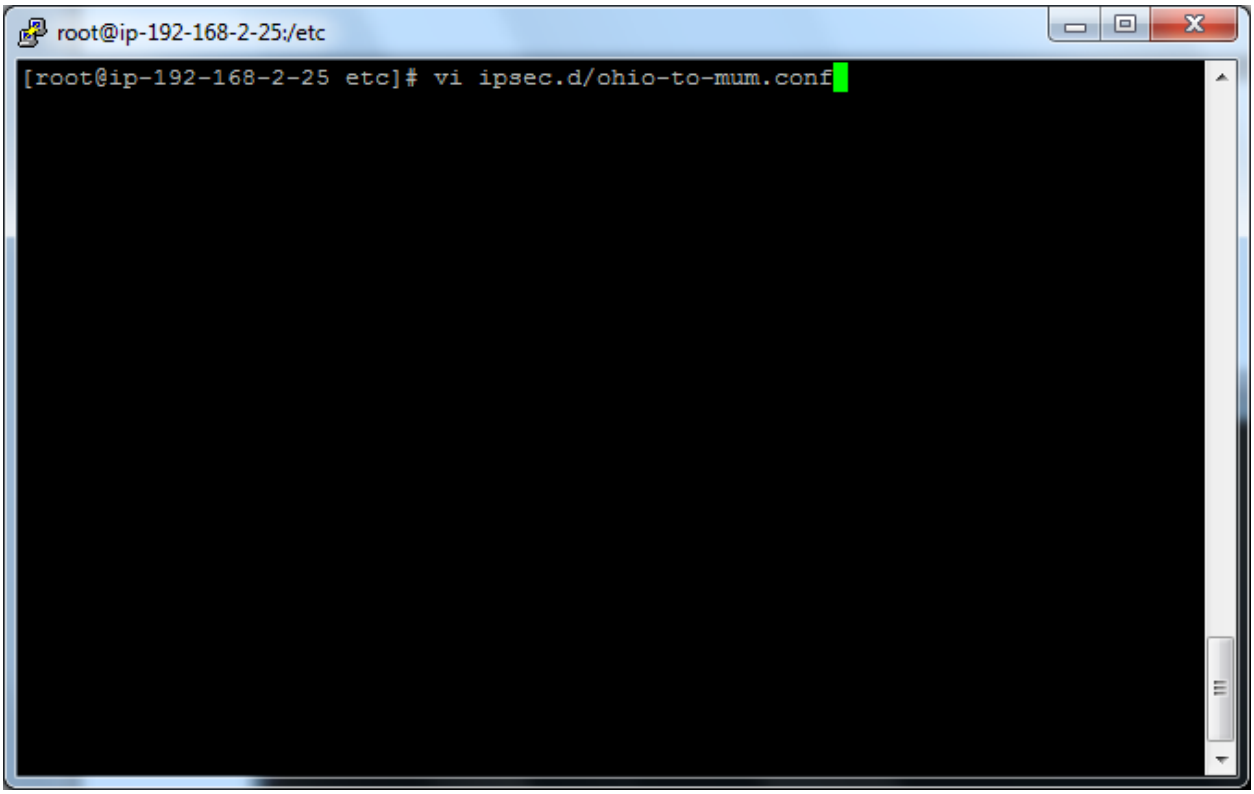
Press ecape and type

:wq



Type

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



Press Insert key and type the command in vi editor

conn ohio-to-mum

type=tunnel

authby=secret

left=defaultroute

leftid=18.218.11.25

leftnexthop=%defaultroute

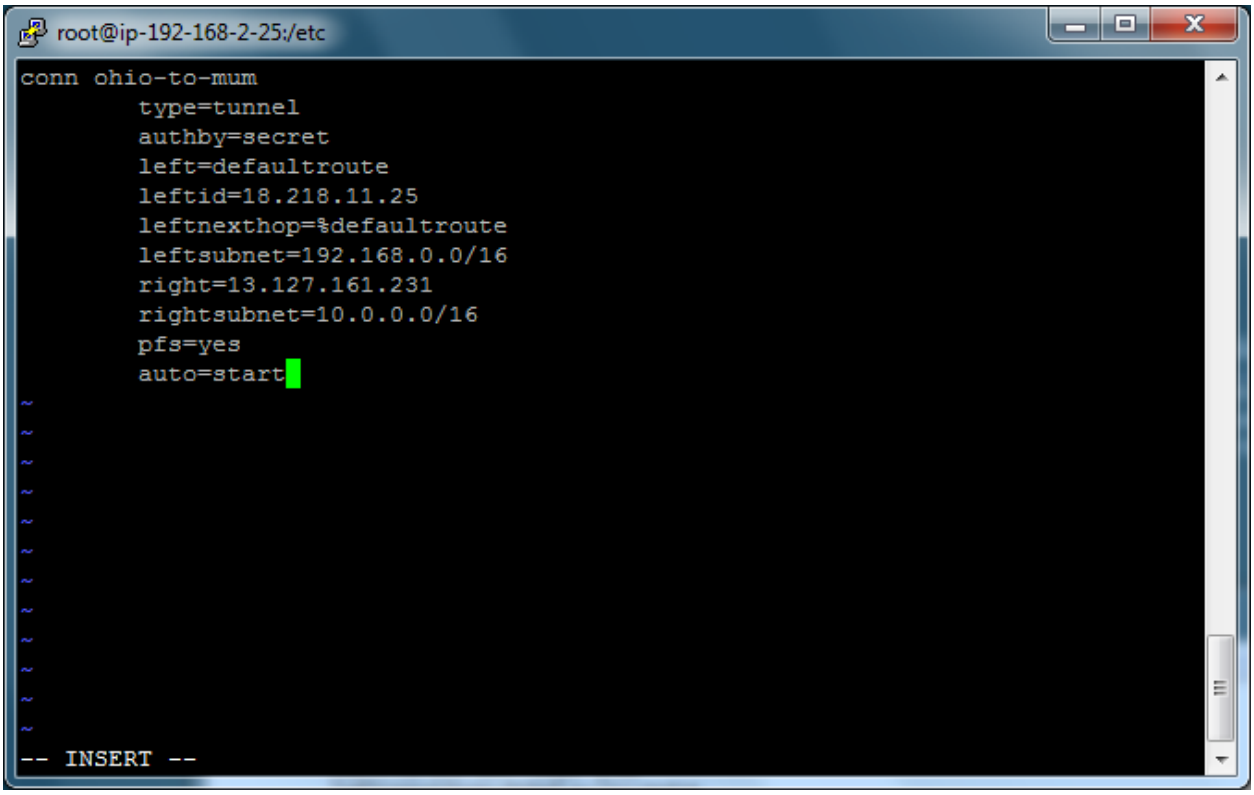
leftsubnet=192.168.0.0/16

right=13.127.161.231

rightsubnet=10.0.0.0/16

pfs=yes

auto=start

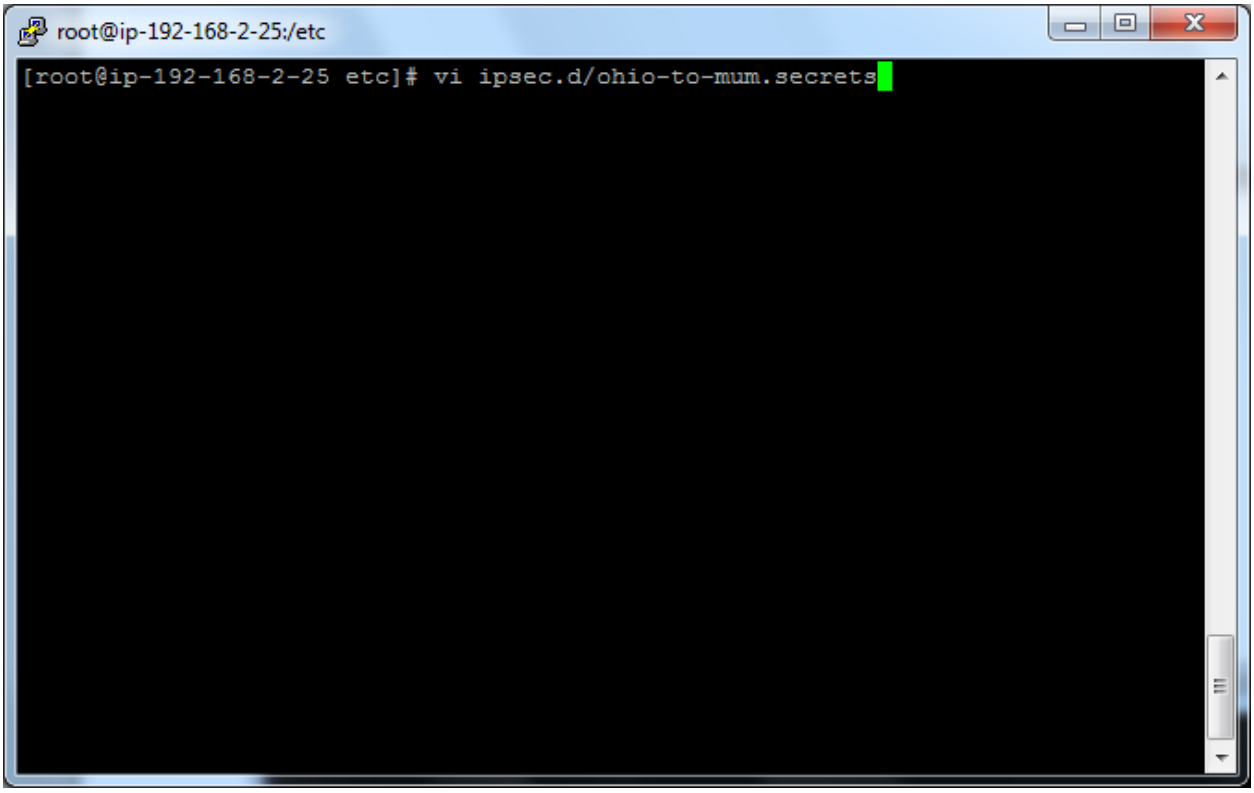


Press escape and type

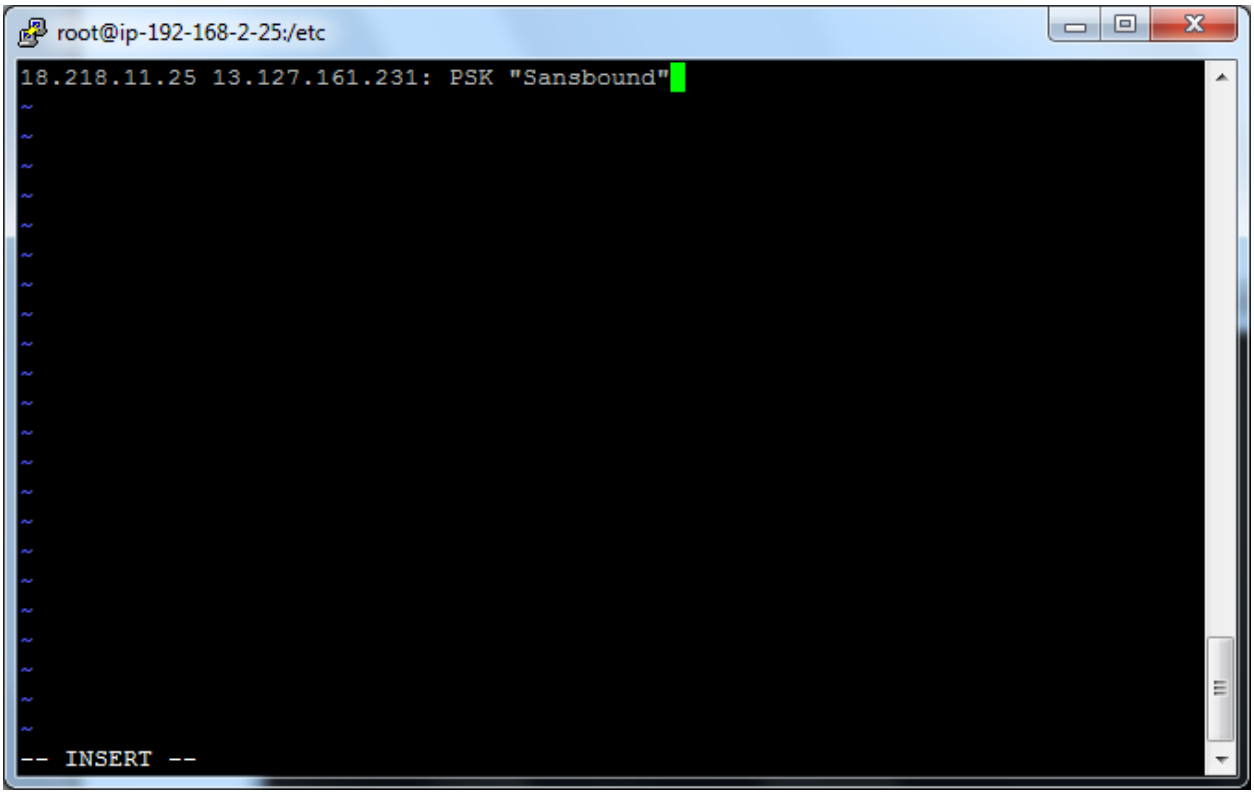
:wq

Type

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

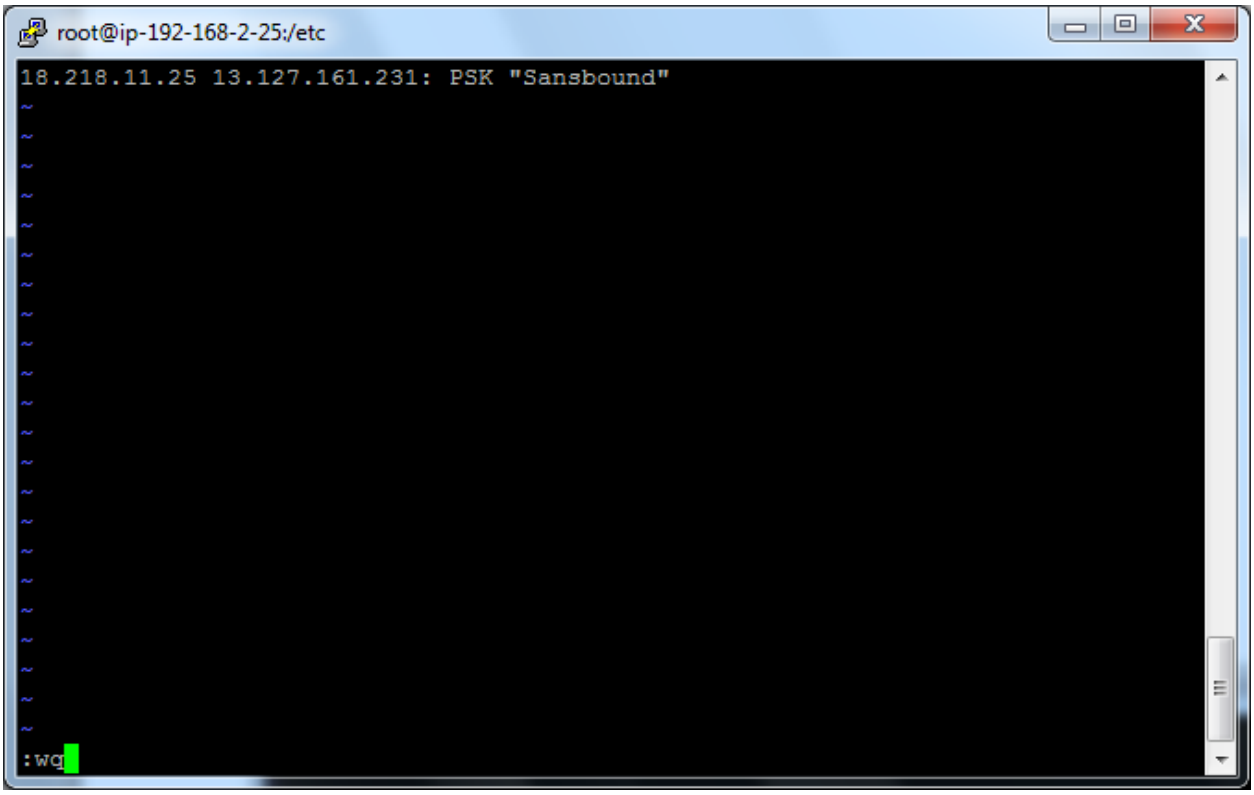


Preshared key is “Sansbound”



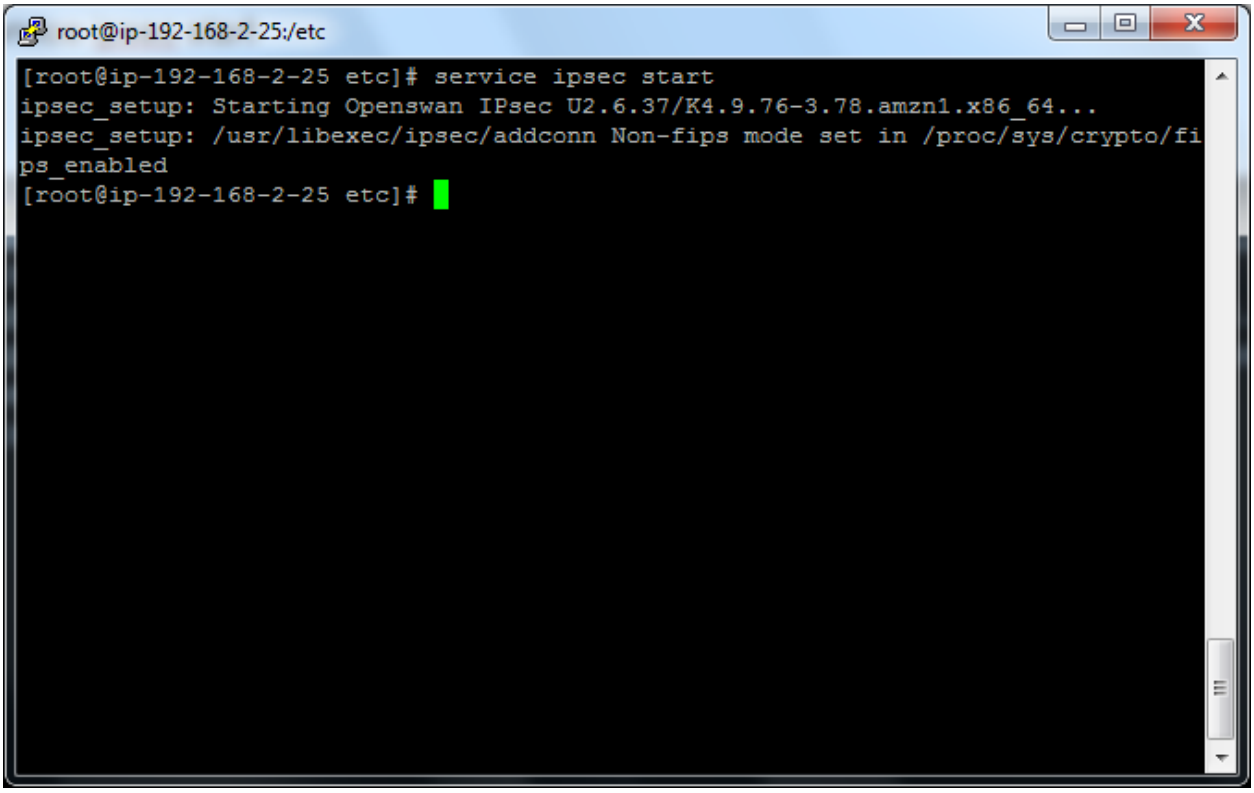
Press escape and type

:wq



Type

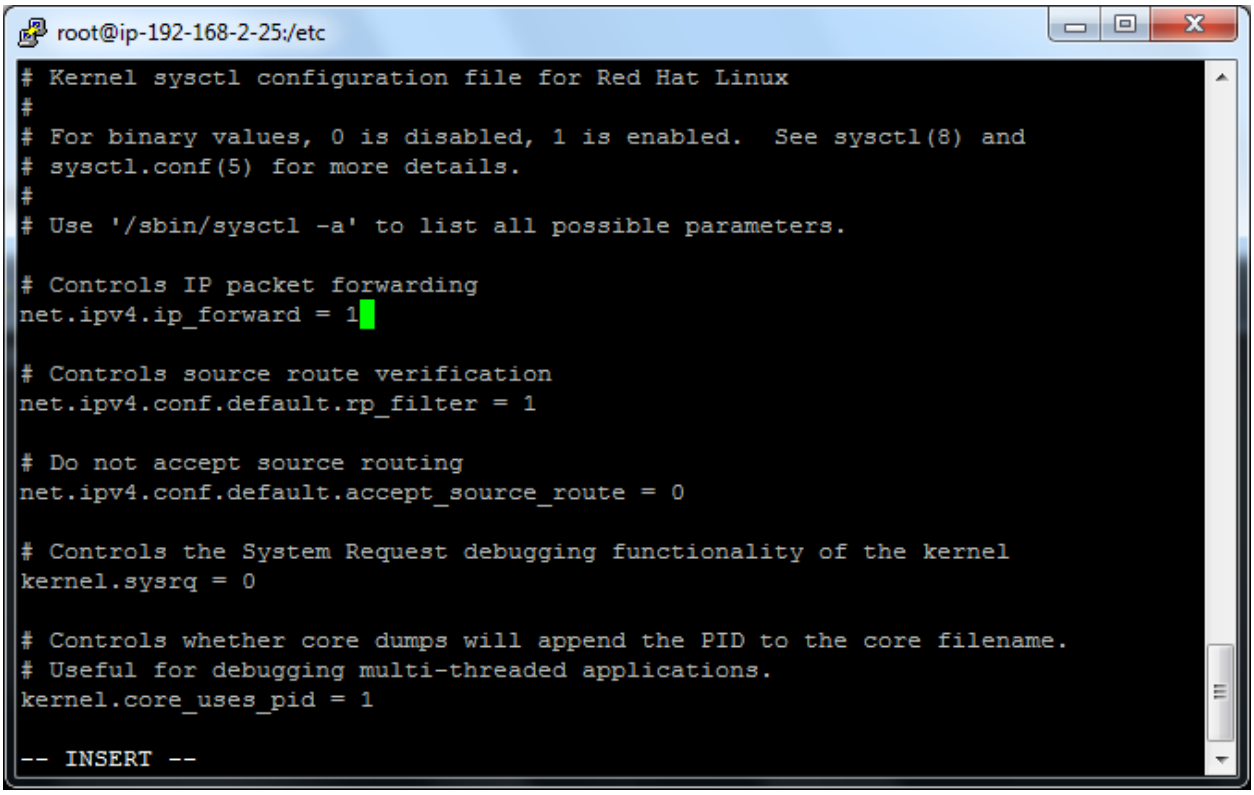
service ipsec start



Type

Vi sysctl.conf

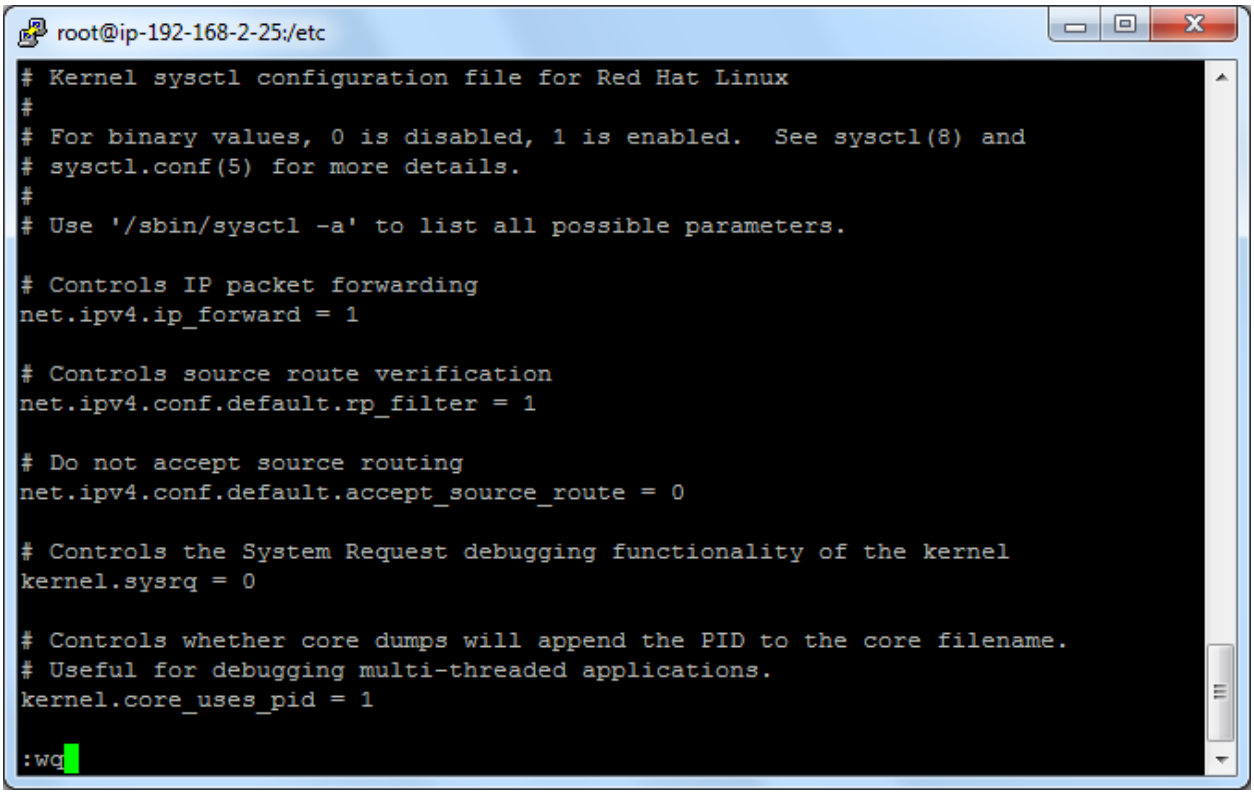
Press insert key and rename the net.ipv4.ip_forward = 1.



Press escape key.

Type

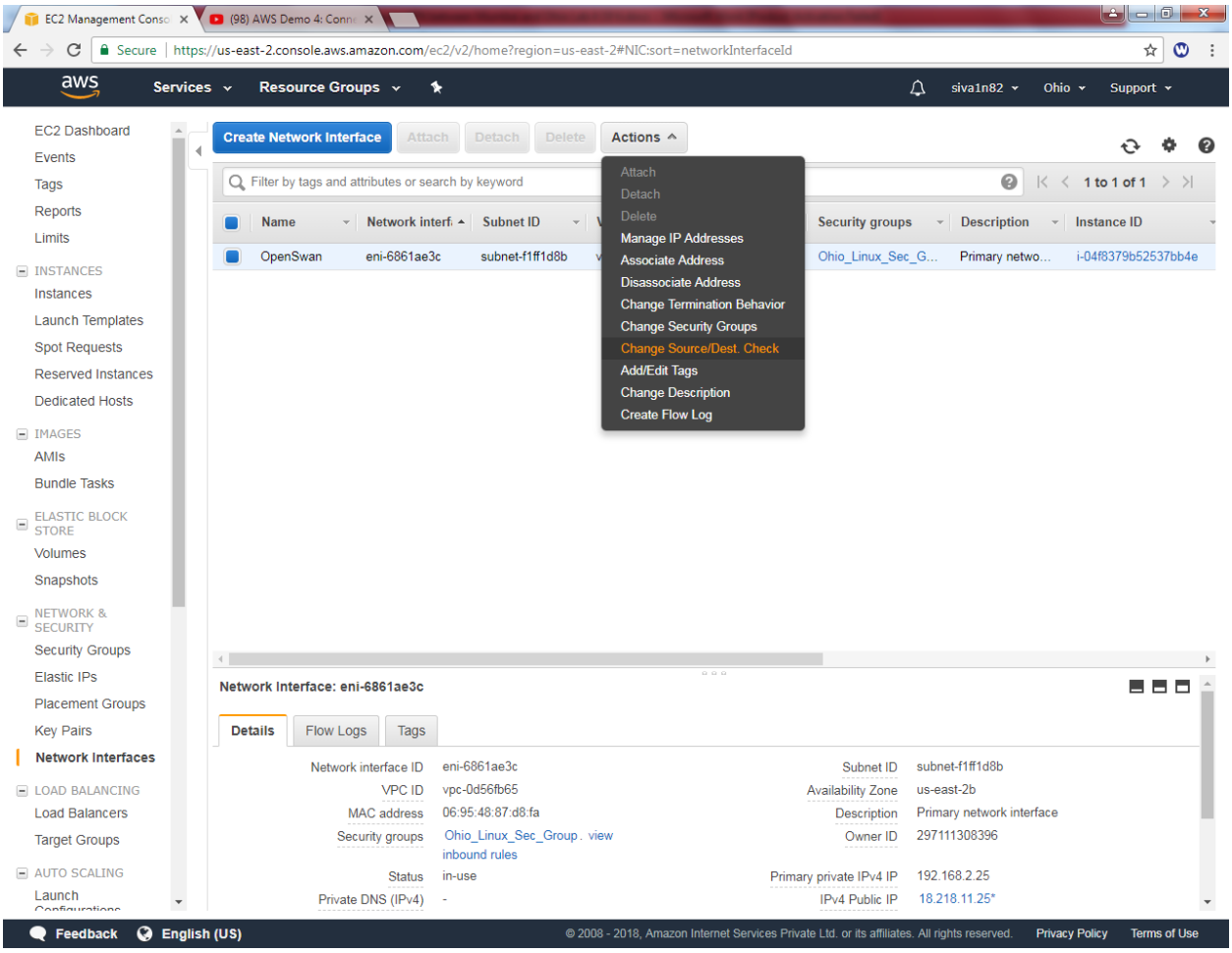
:wq



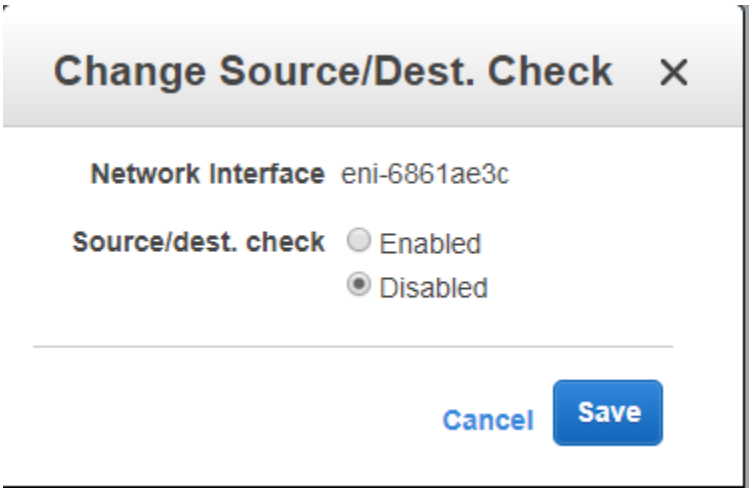
Go to Ec2 Dashboard

Click “Network interface” and then select “OpenSwan”

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

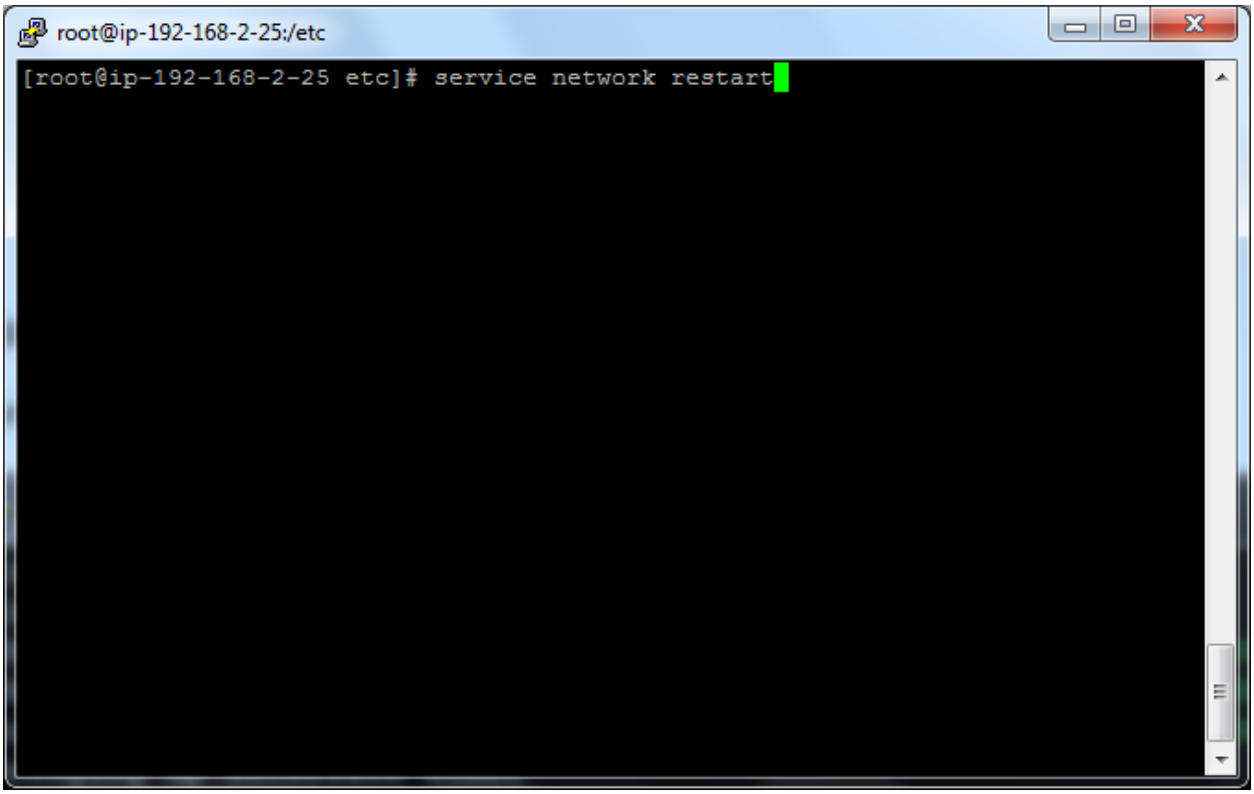


Set as “Disabled”and click “save”.



Type

Service network restart



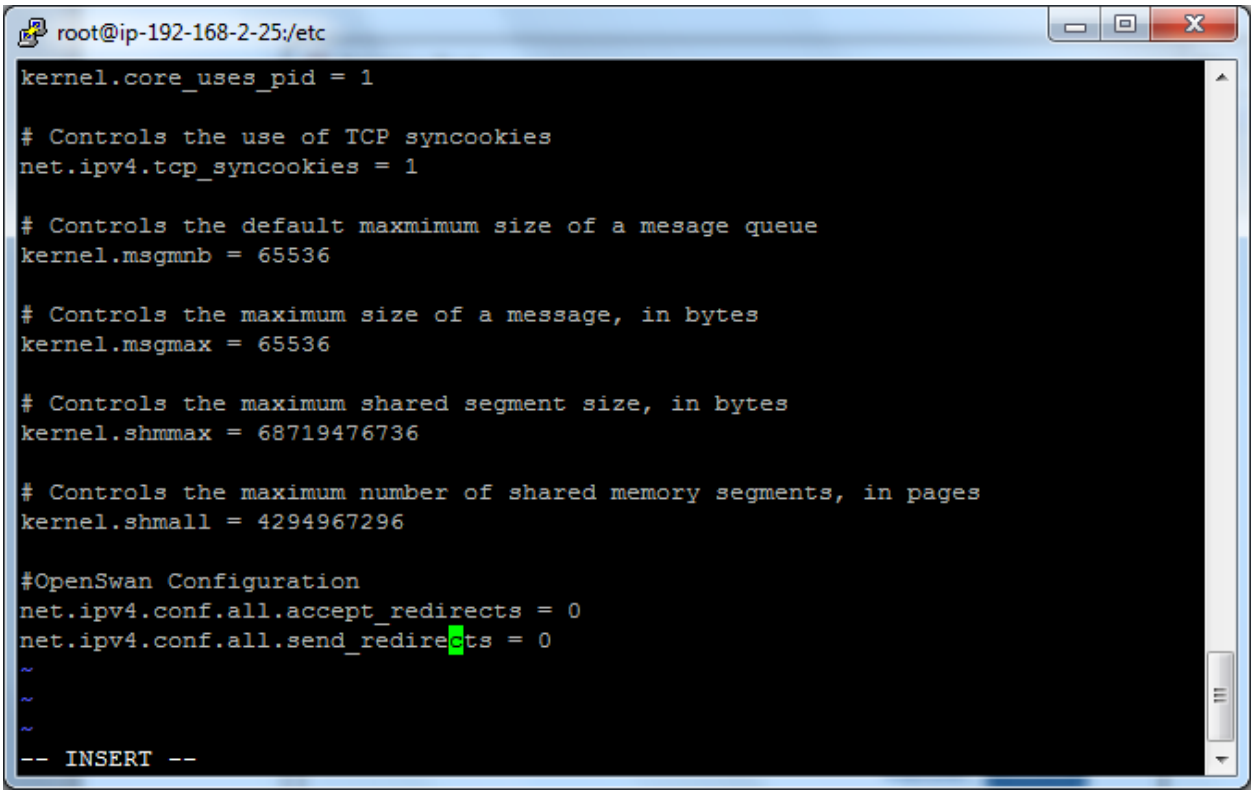
Type

Vi sysctl.conf

Press insert key

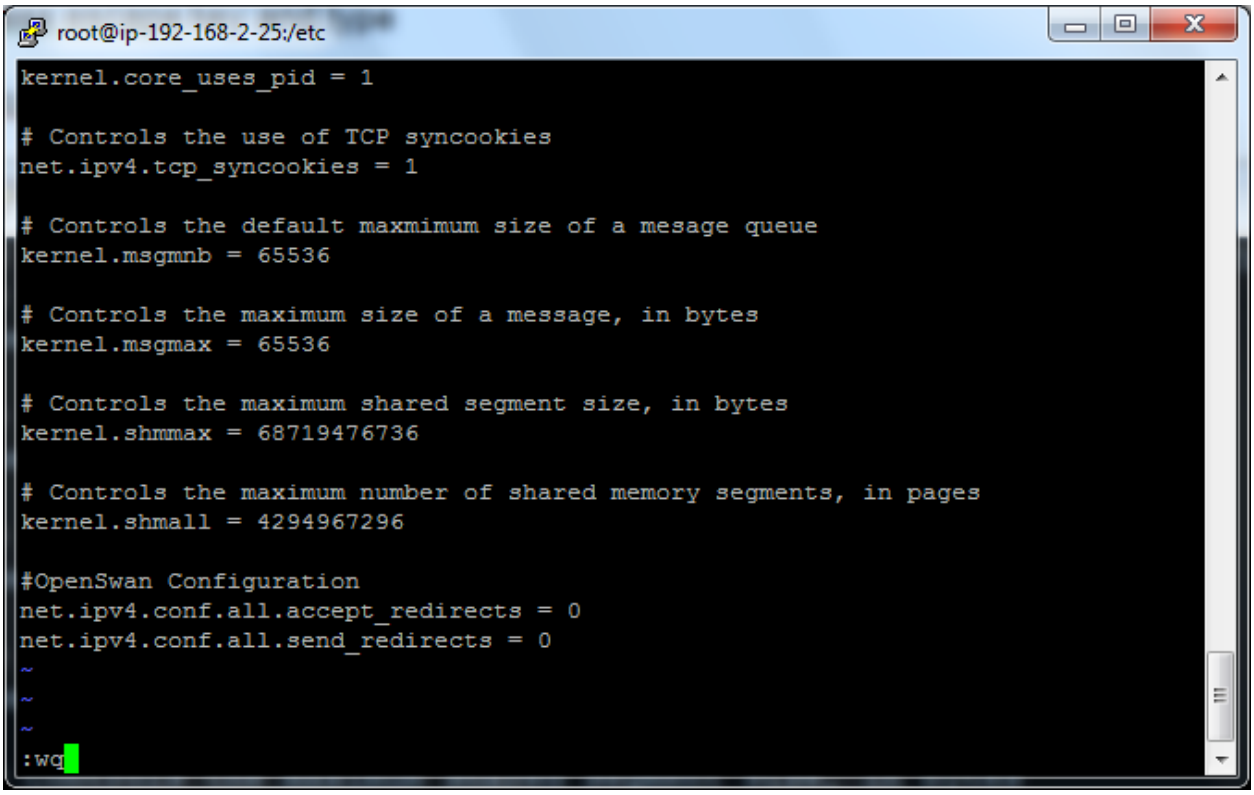
net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.all.send_redirects = 0



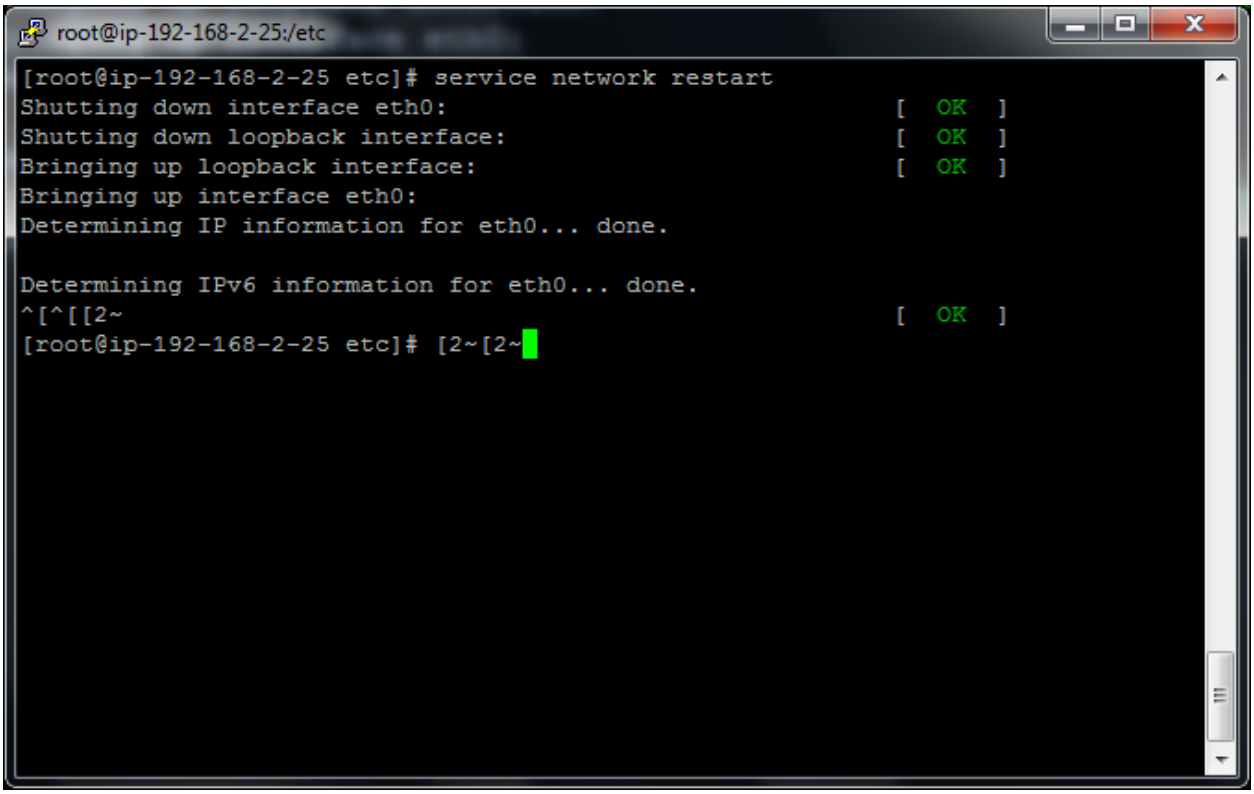
Press escape key and then type

:wq

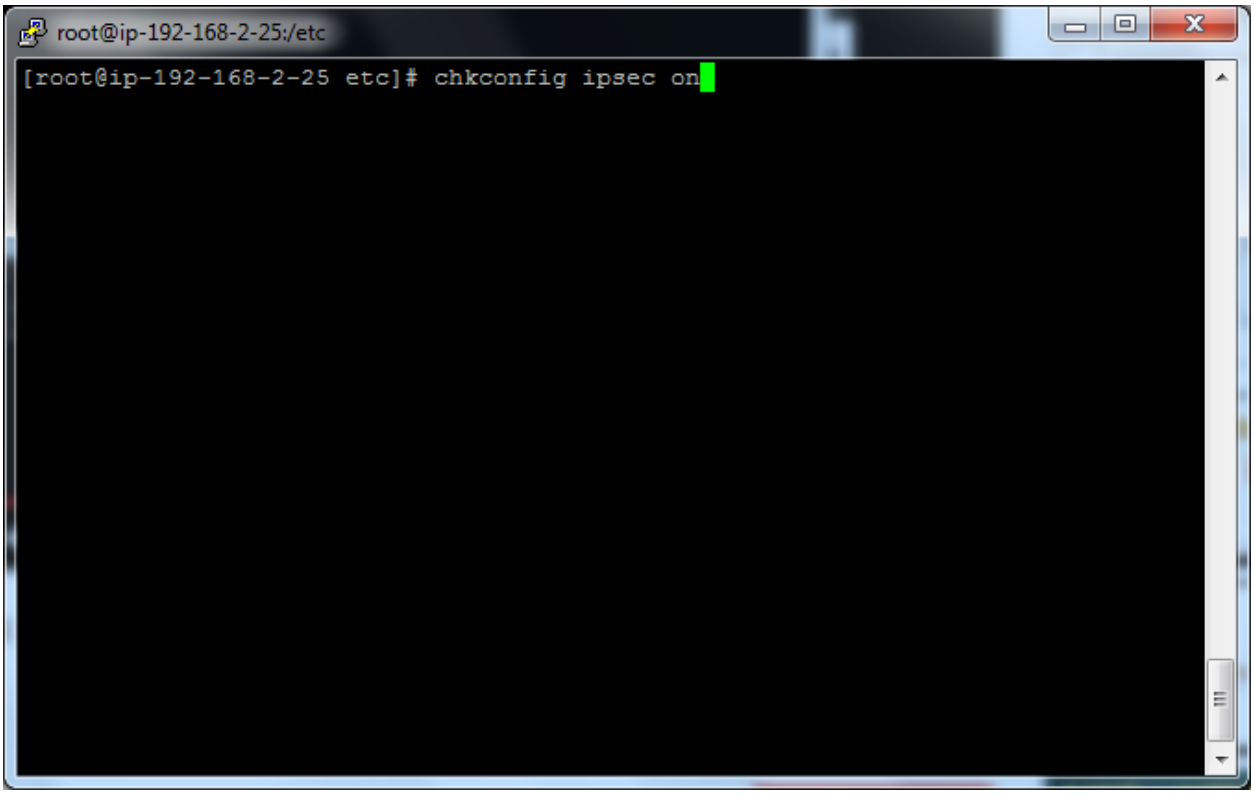


Type

Service network restart

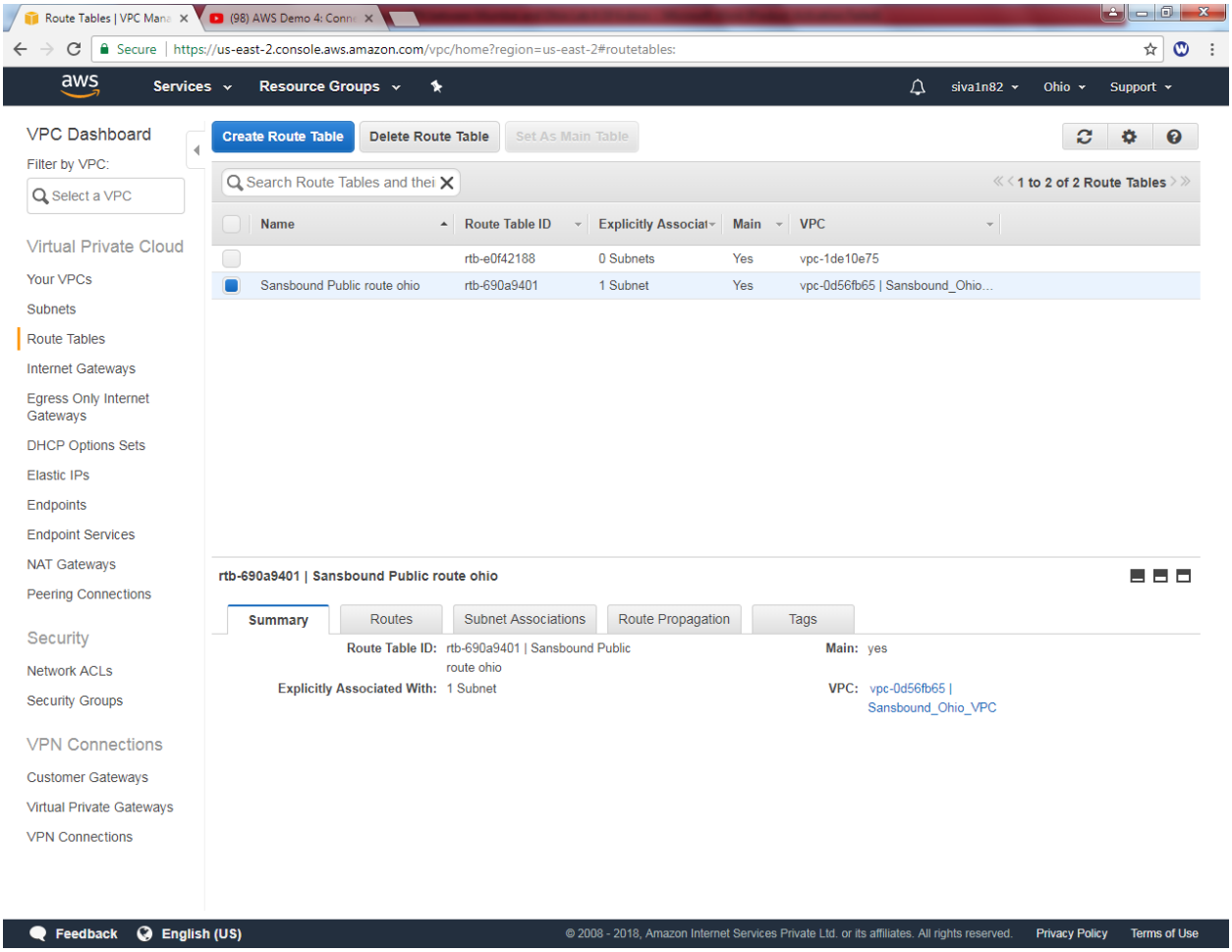


Type chkconfig ipsec on

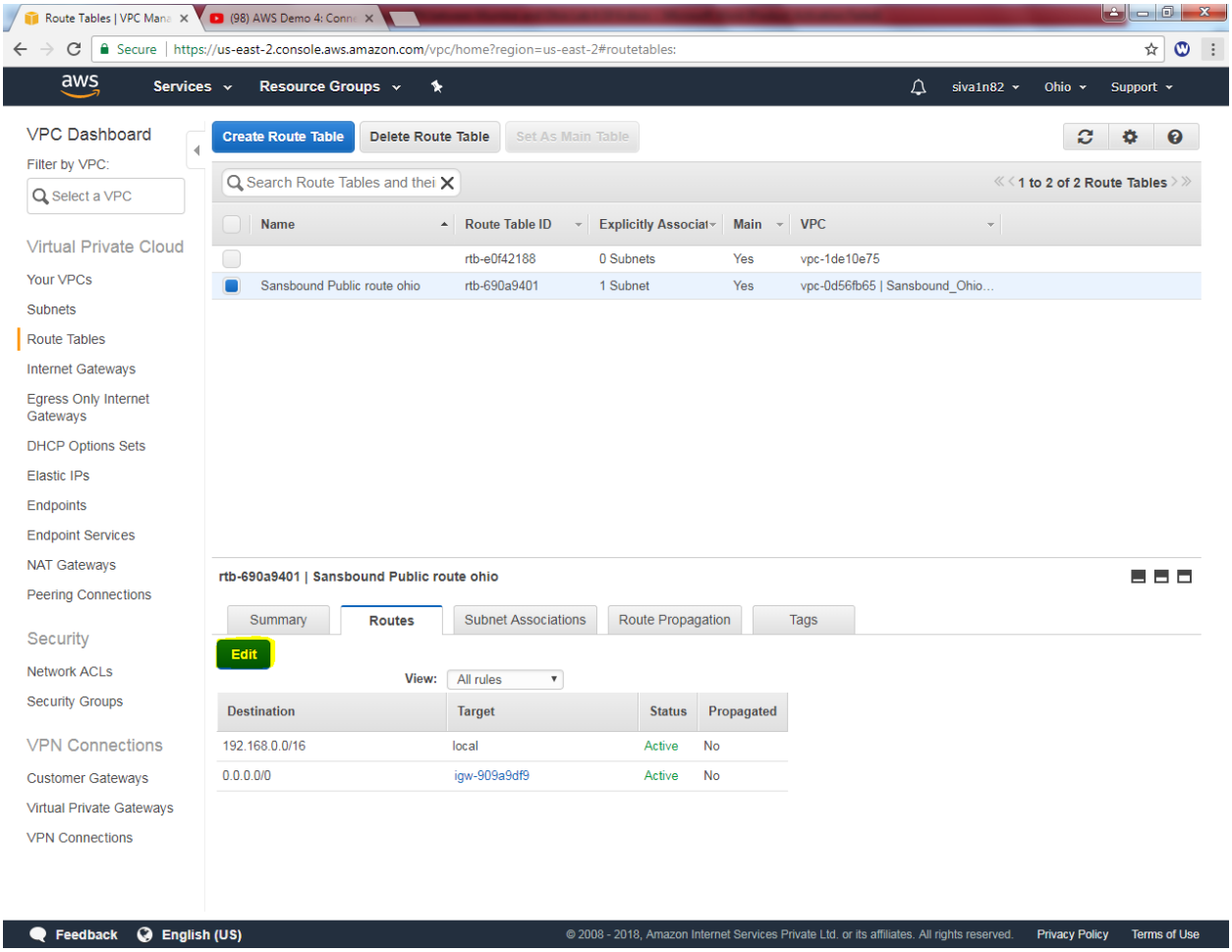


Go to VPC,

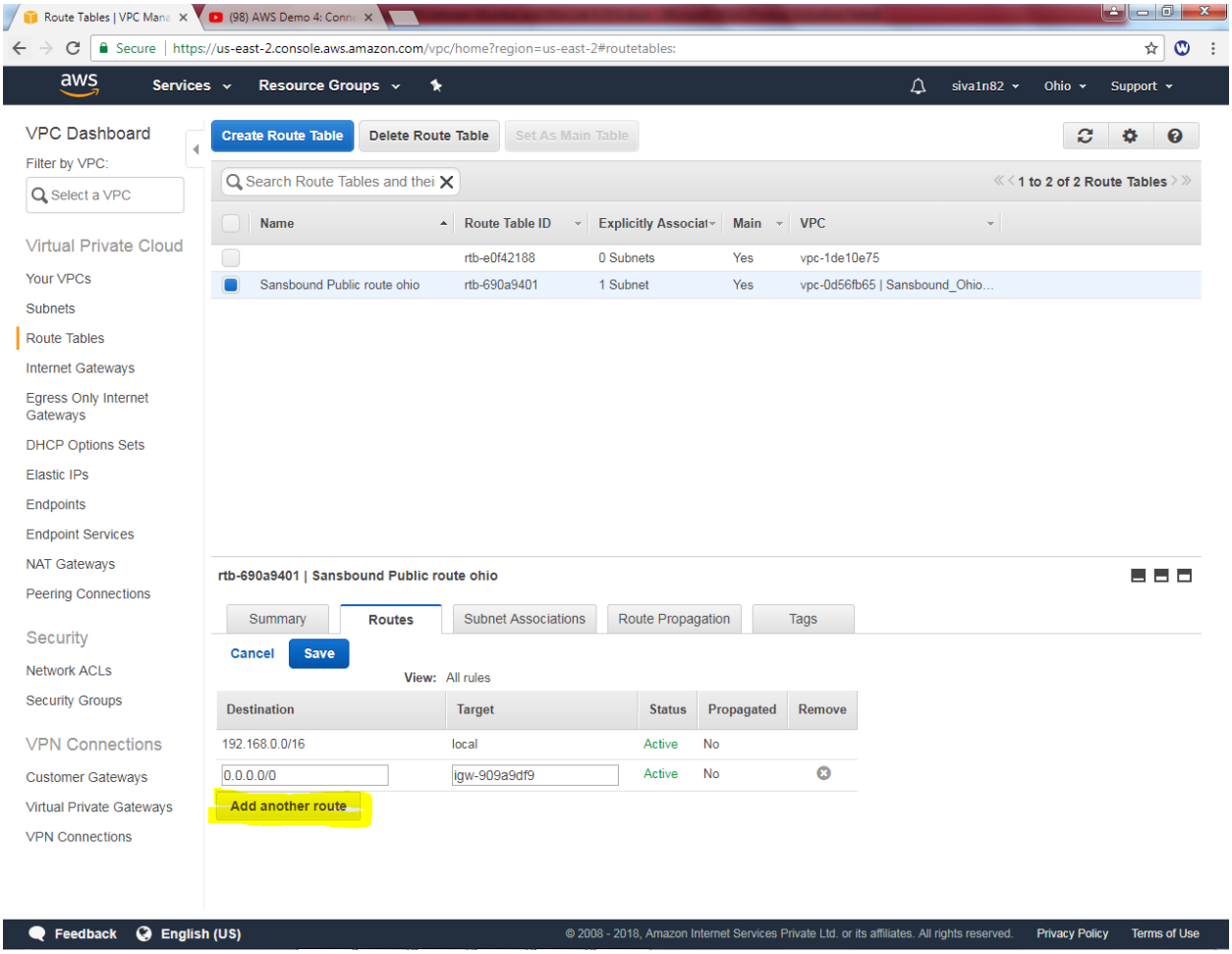
Click Route table and select sansbound public route table.



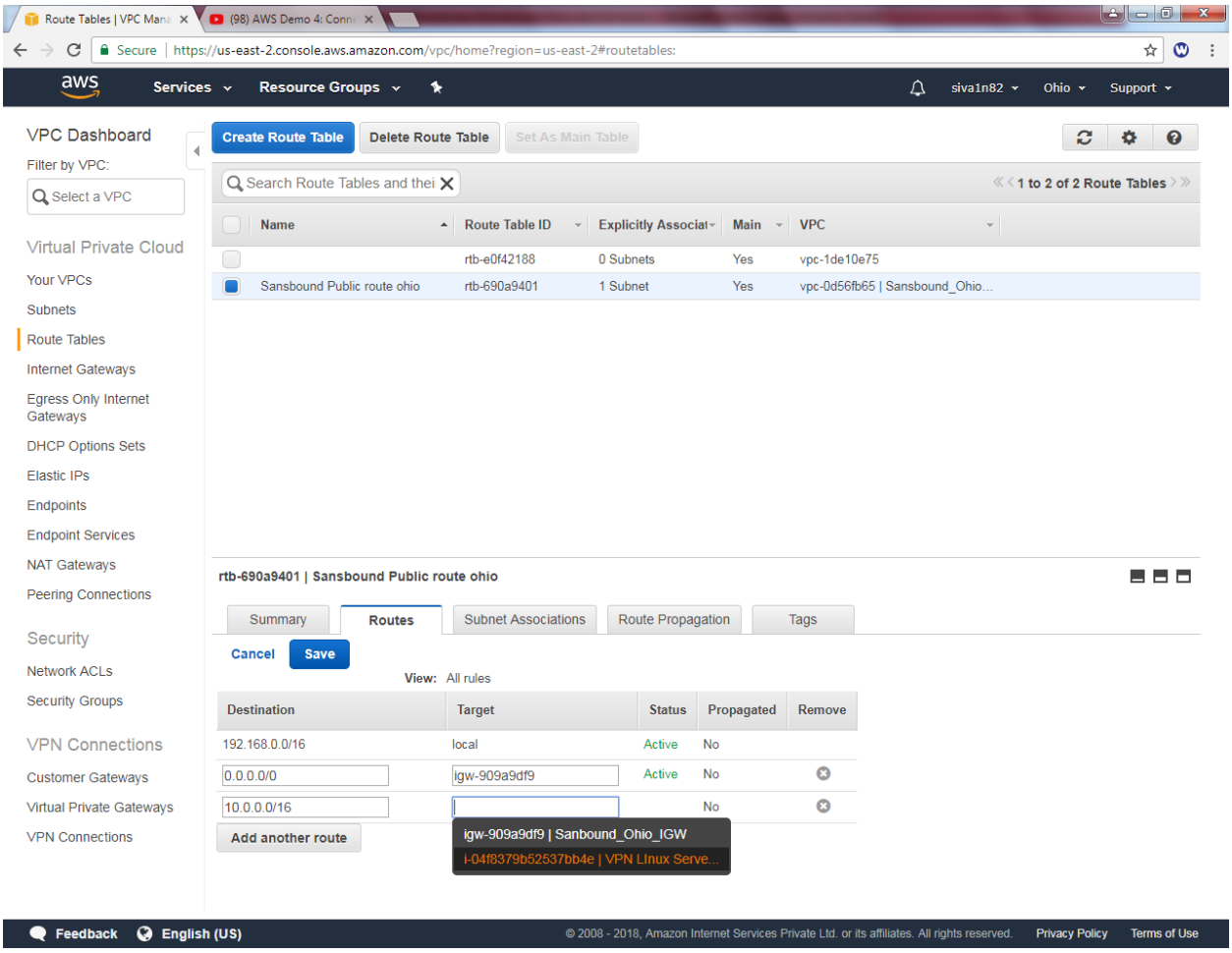
Click “Edit”.


Route Tables | VPC Mana
(98) AWS Demo 4: Conne
Secure | https://us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#routetables:
aws
Services
Resource Groups
siva1n82
Ohio
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 2 of 2 Route Tables
Name
Route Table ID
Explicitly Associat
Main
VPC
rtb-e0f42188
0 Subnets
Yes
vpc-1de10e75
Sansbound Public route ohio
rtb-690a9401
1 Subnet
Yes
vpc-0d56fb65 | Sansbound_Ohio...
rtb-690a9401 | Sansbound Public route ohio
Summary
Routes
Subnet Associations
Route Propagation
Tags
Edit
View:
All rules
Destination
Target
Status
Propagated
192.168.0.0/16
local
Active
No
0.0.0.0/0
igw-909a9df9
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”.



Type 10.0.0.0/16 subnet as destination and select “VPN Linux Server” as target.



Click “save”.

Click To view detailed information of routing table as below.