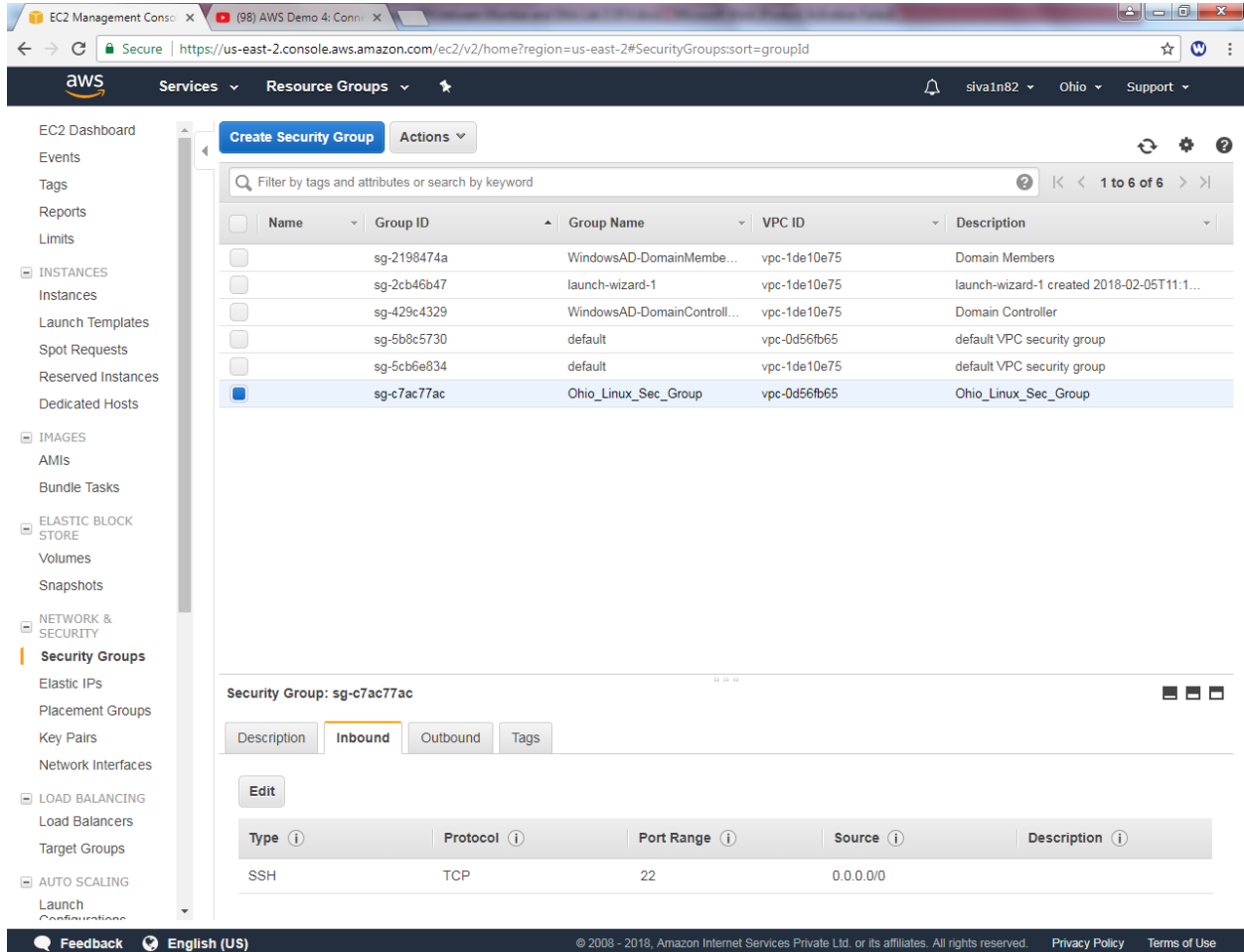


Configure VPN between Mumbai and Ohio Lab 4 of 4

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.



The screenshot shows the AWS Management Console interface for the Ohio region. The left sidebar contains navigation links for various AWS services. The main content area displays a list of Security Groups. The 'Ohio_Linux_Sec_Group' is selected, and its details are shown below. The 'Inbound' tab is active, showing a rule for SSH (TCP) on port 22 from source 0.0.0.0/0.

Name	Group ID	Group Name	VPC ID	Description
sg-2198474a	sg-2198474a	WindowsAD-DomainMembe...	vpc-1de10e75	Domain Members
sg-2cb46b47	sg-2cb46b47	launch-wizard-1	vpc-1de10e75	launch-wizard-1 created 2018-02-05T11:1...
sg-429c4329	sg-429c4329	WindowsAD-DomainControll...	vpc-1de10e75	Domain Controller
sg-5b8c5730	sg-5b8c5730	default	vpc-0d56fb65	default VPC security group
sg-5cb6e834	sg-5cb6e834	default	vpc-1de10e75	default VPC security group
sg-c7ac77ac	sg-c7ac77ac	Ohio_Linux_Sec_Group	vpc-0d56fb65	Ohio_Linux_Sec_Group

Security Group: sg-c7ac77ac

Inbound

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/0	

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

Edit inbound rules

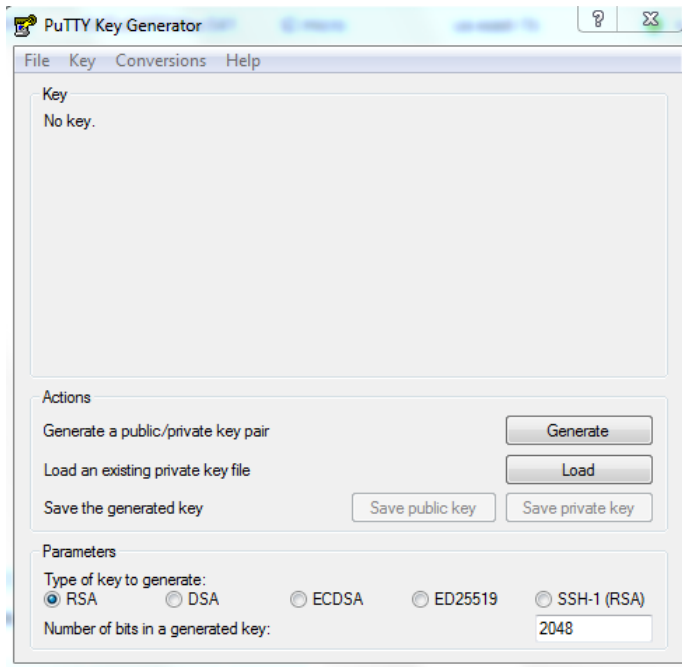
Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
All traffic	All	0 - 65535	Custom 10.0.0.0/16	e.g. SSH for Admin Desktop

Add Rule

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

Cancel
Save

Go to Putty key gen installed in your local machine.



PuTTY Key Generator

File Key Conversions Help

Key

No key.

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

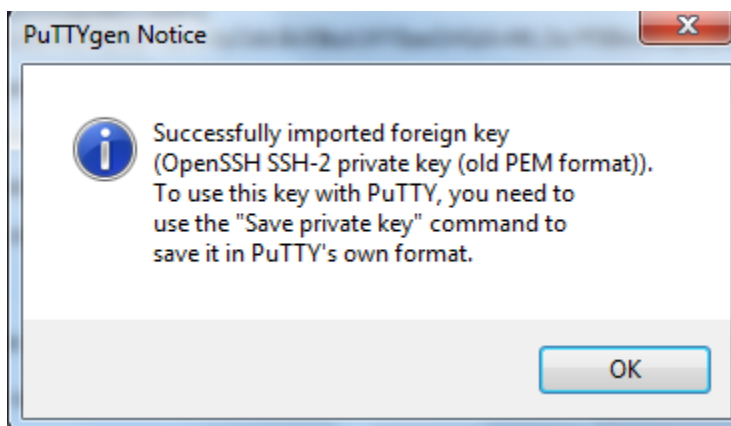
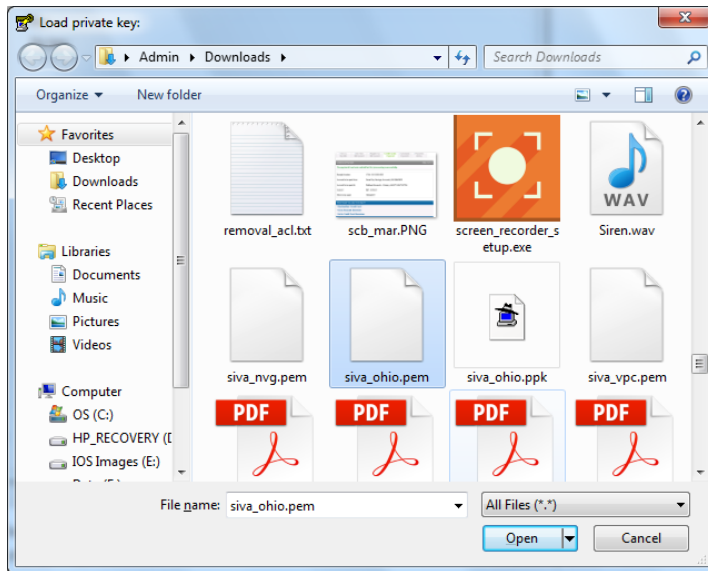
Parameters

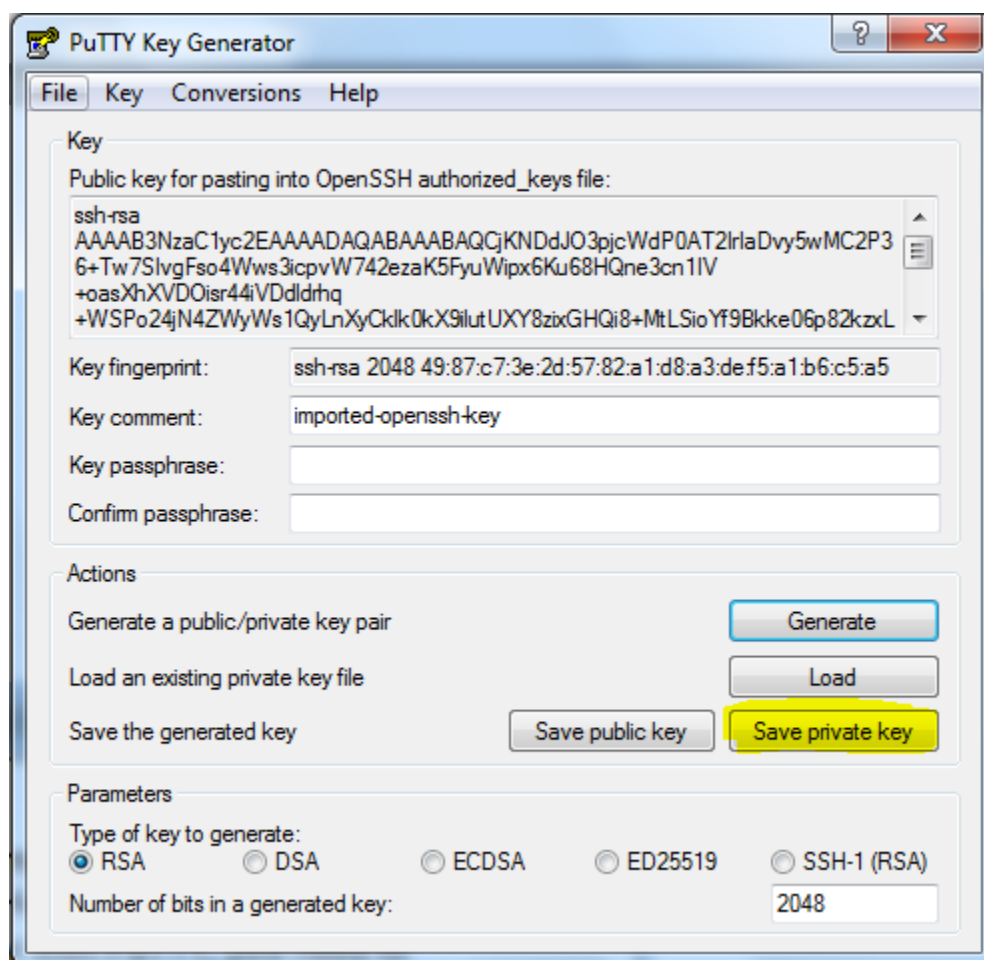
Type of key to generate:

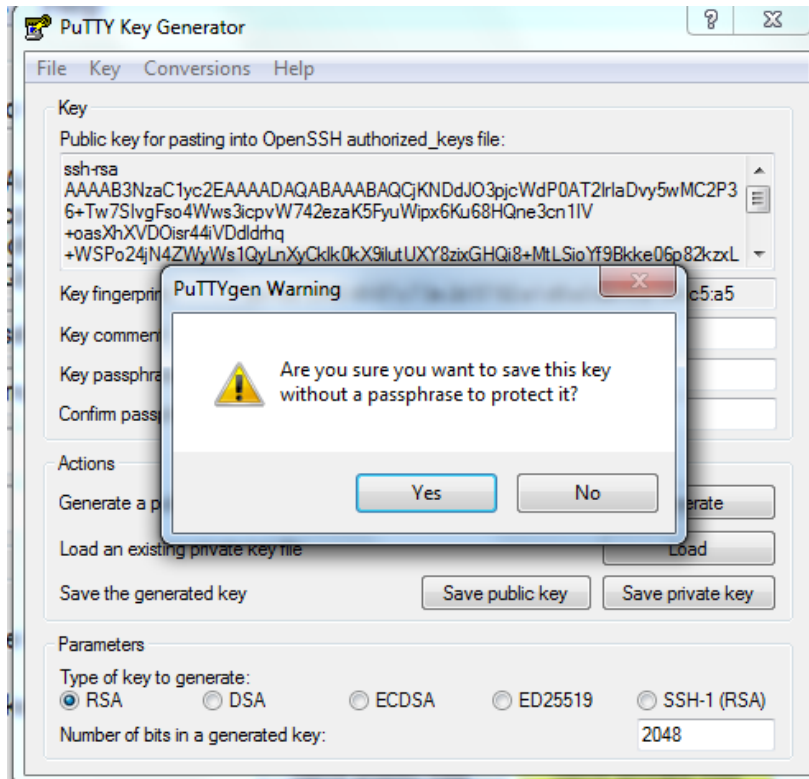
☒ RSA ☐ DSA ☐ ECDSA ☐ ED25519 ☐ SSH-1 (RSA)

Number of bits in a generated key: 2048

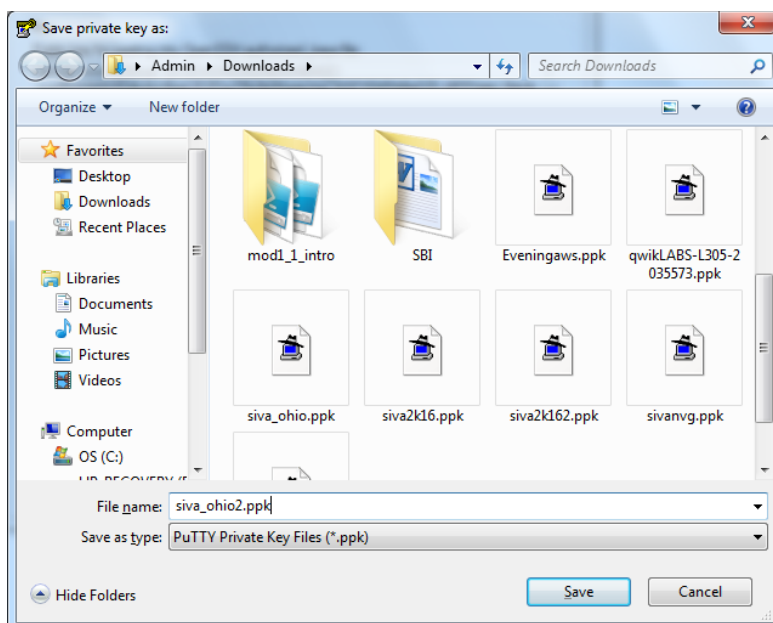
Locate the file and click "Open".

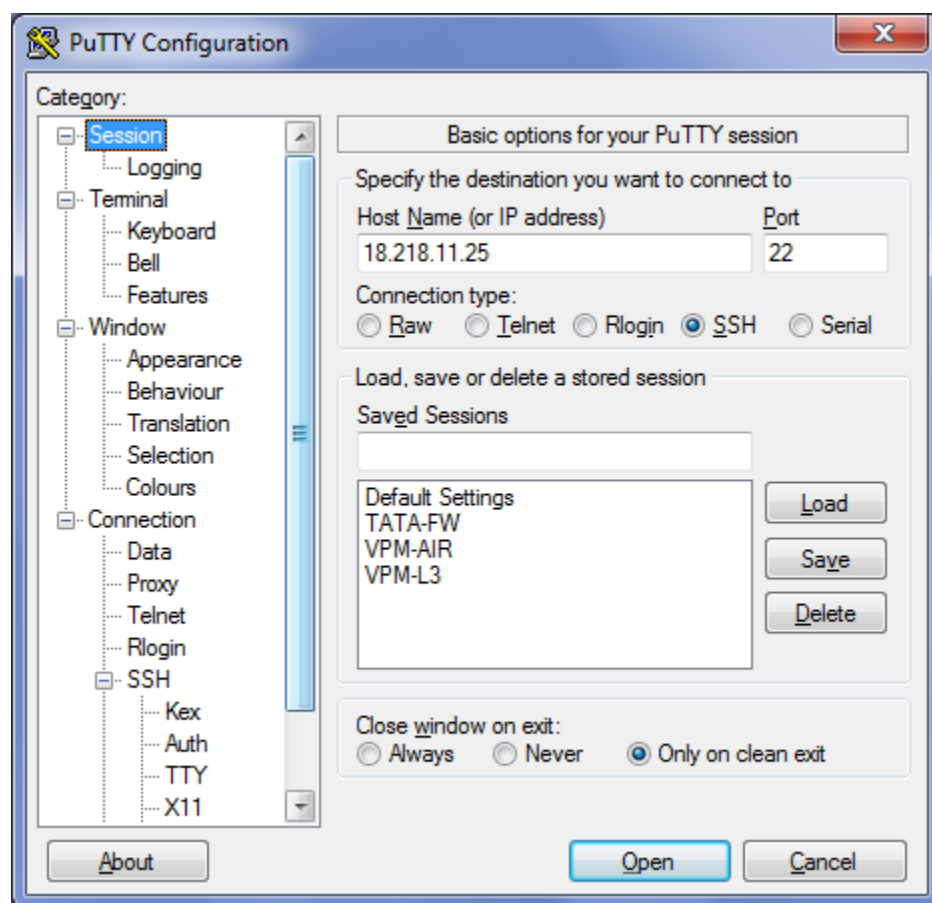




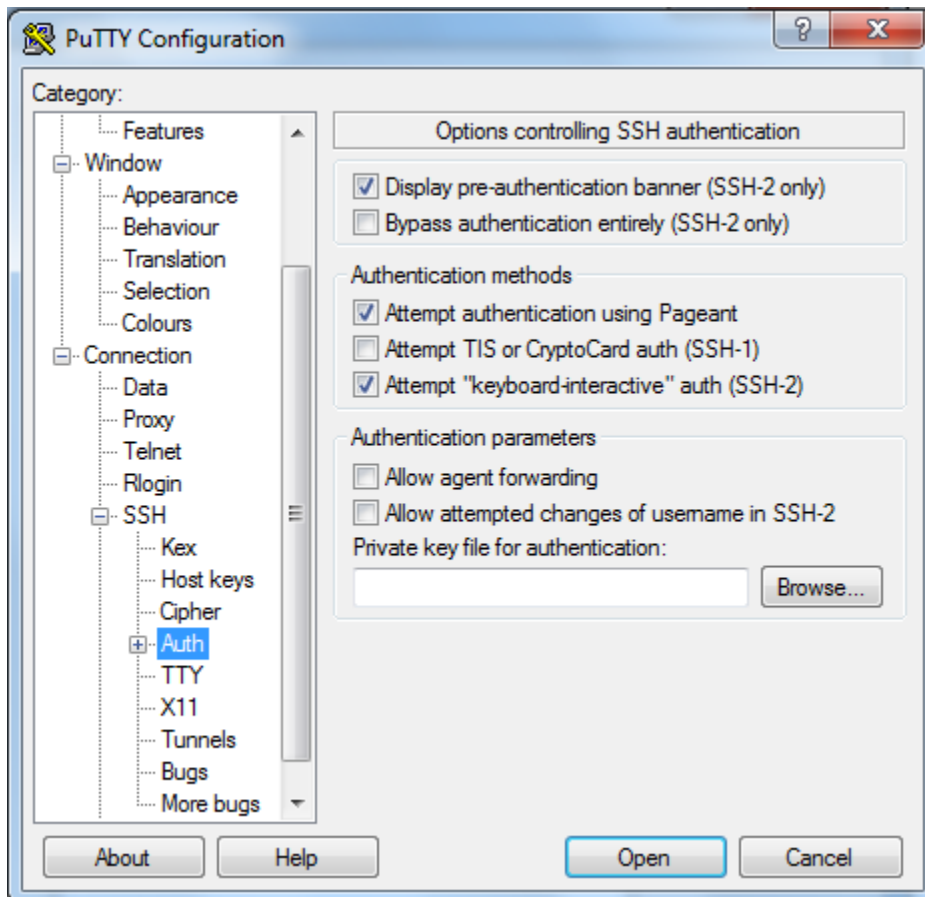


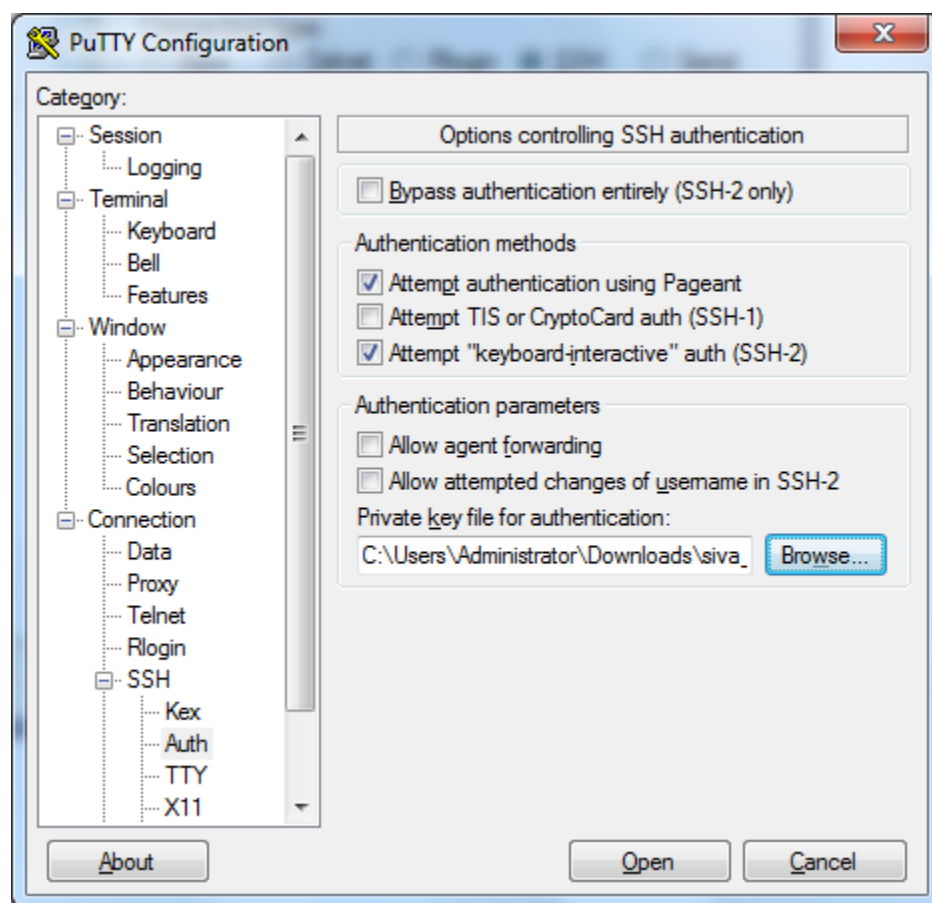
Locate the file to save.

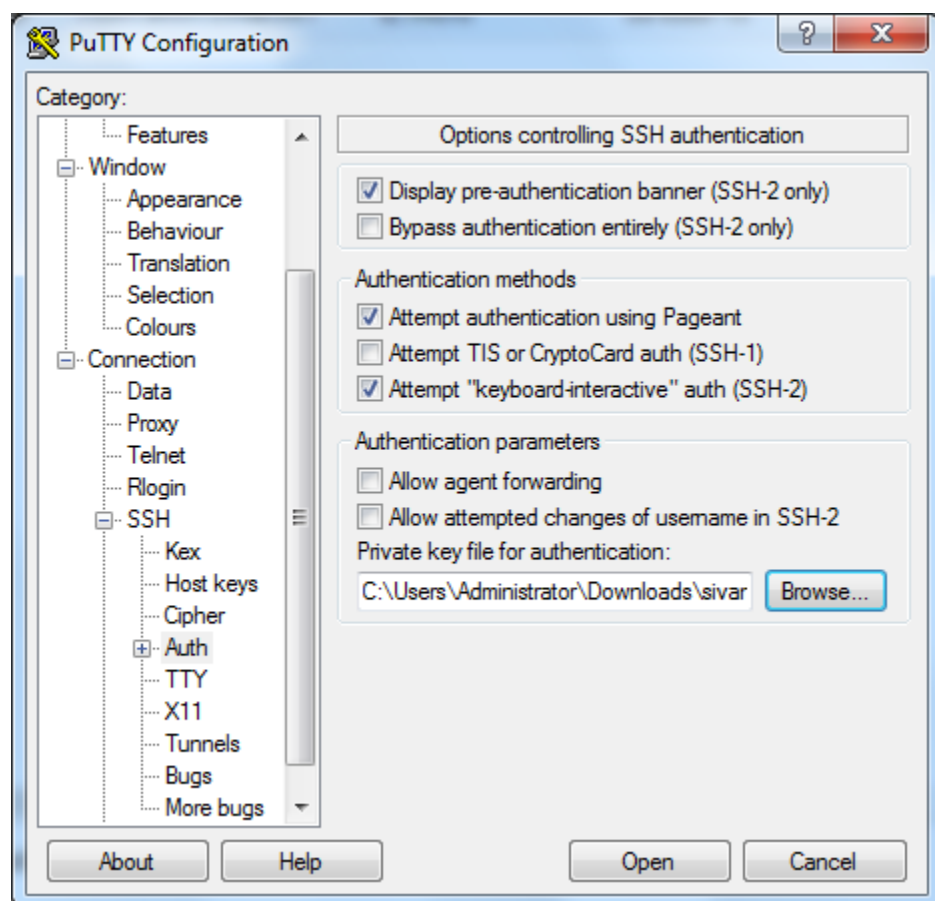


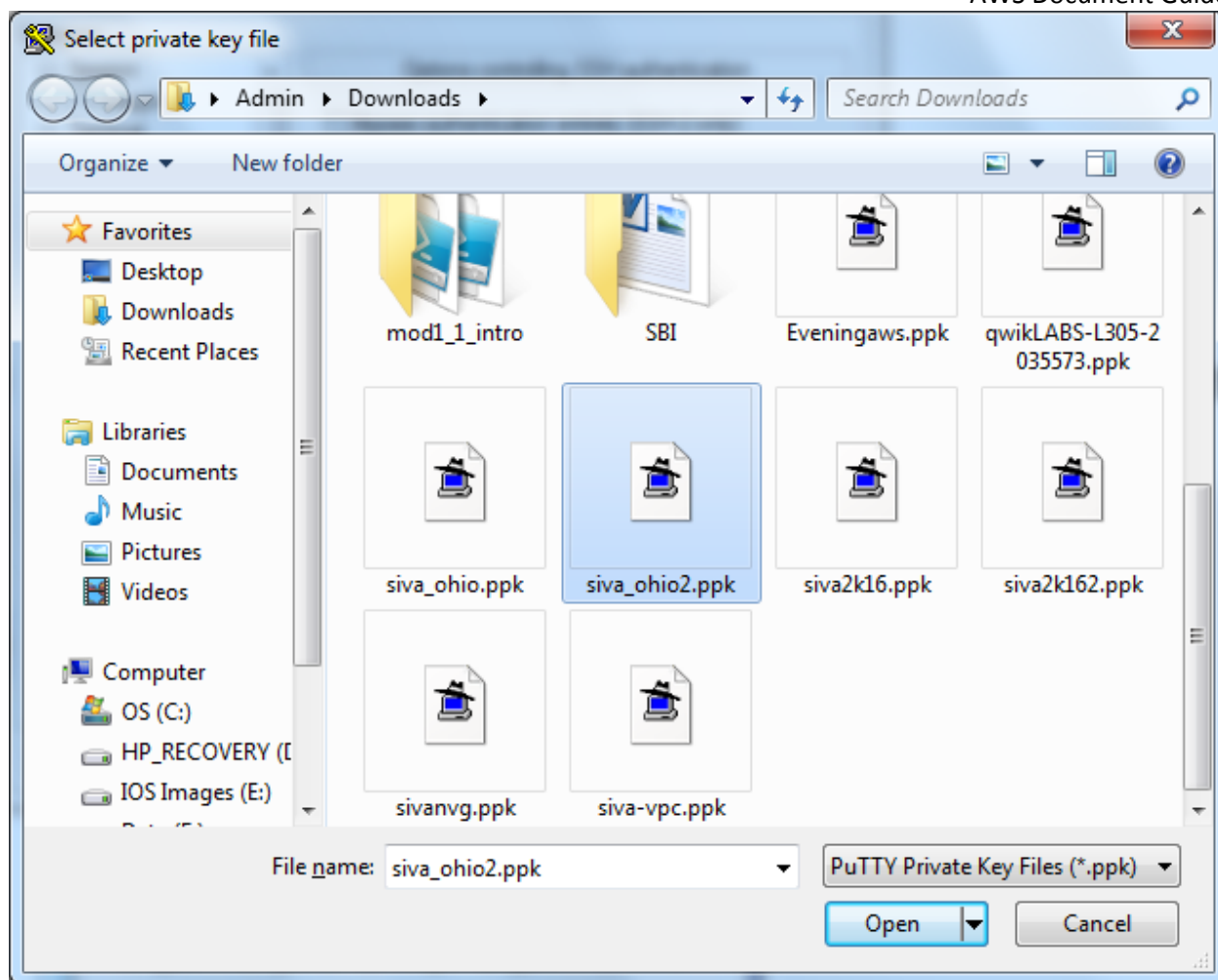


Click Browse and locate the *.ppk file.

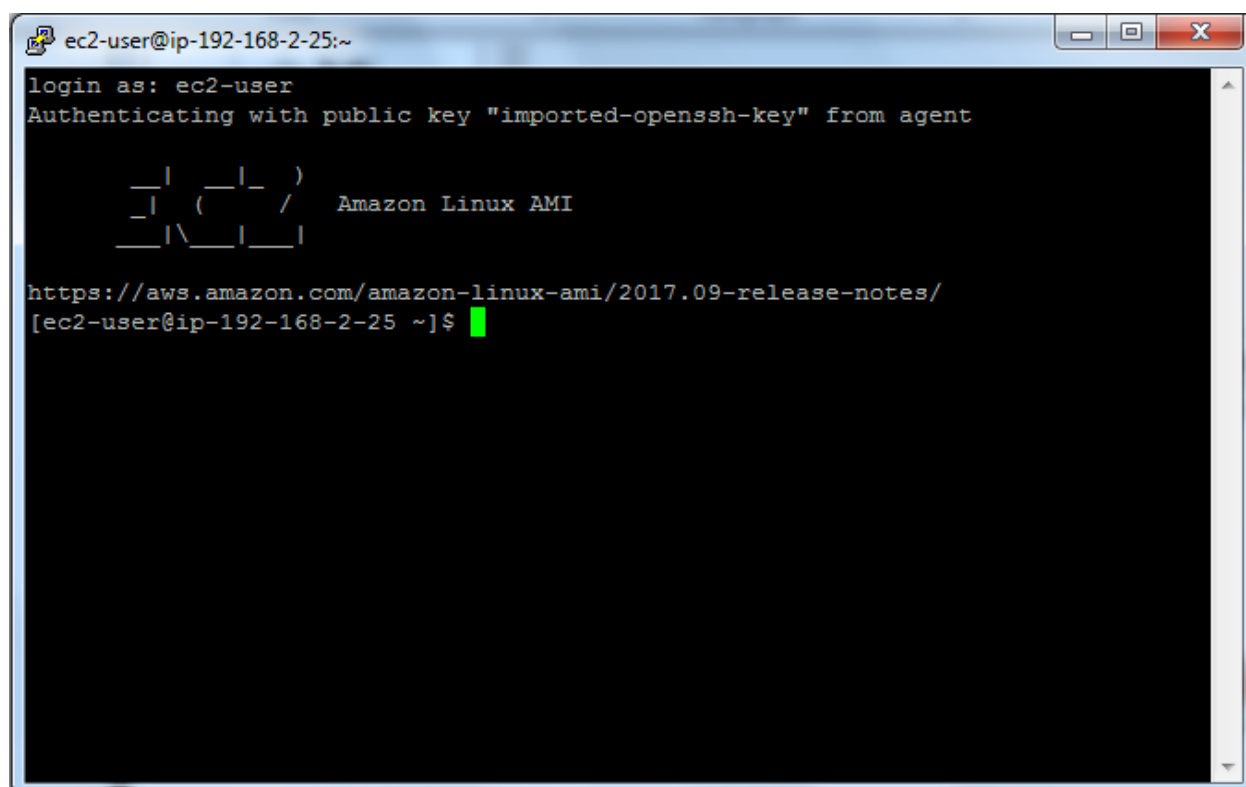
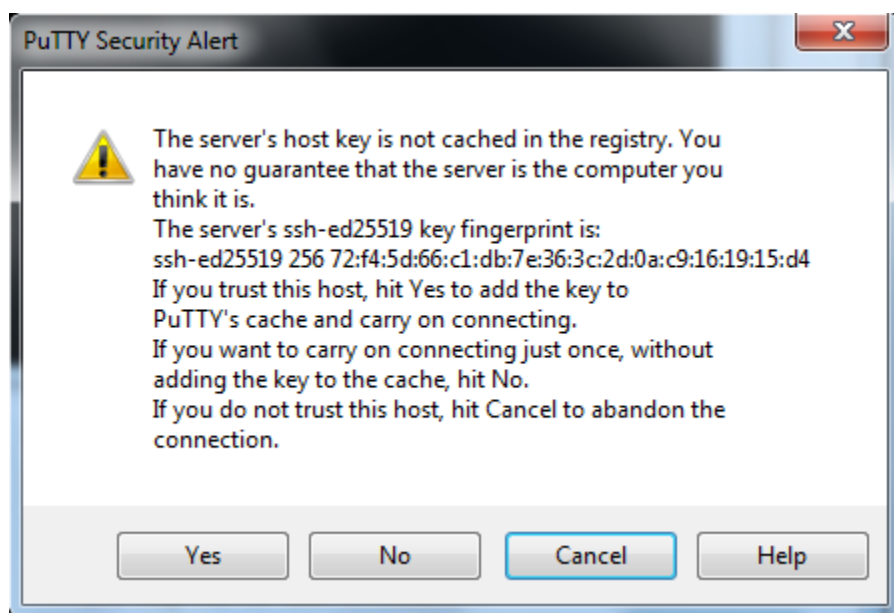






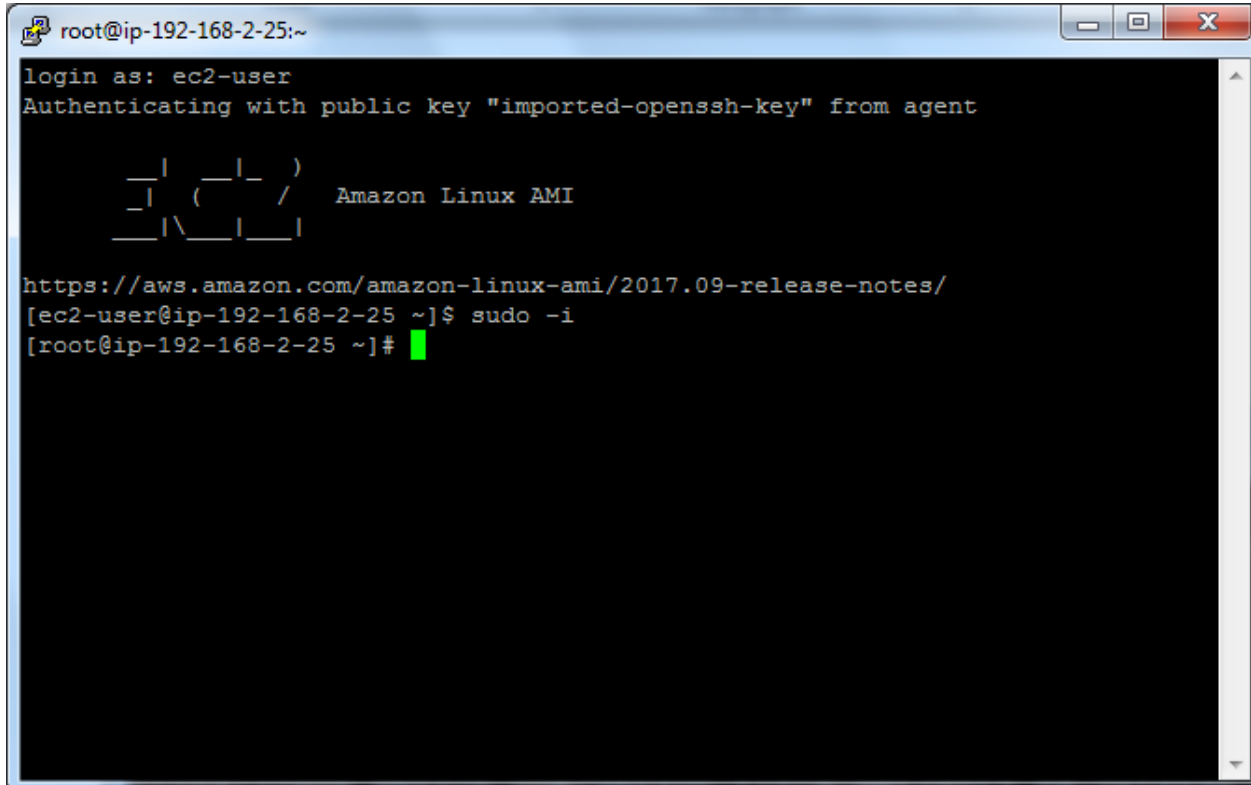


Select the file and Click “Open”.



Type

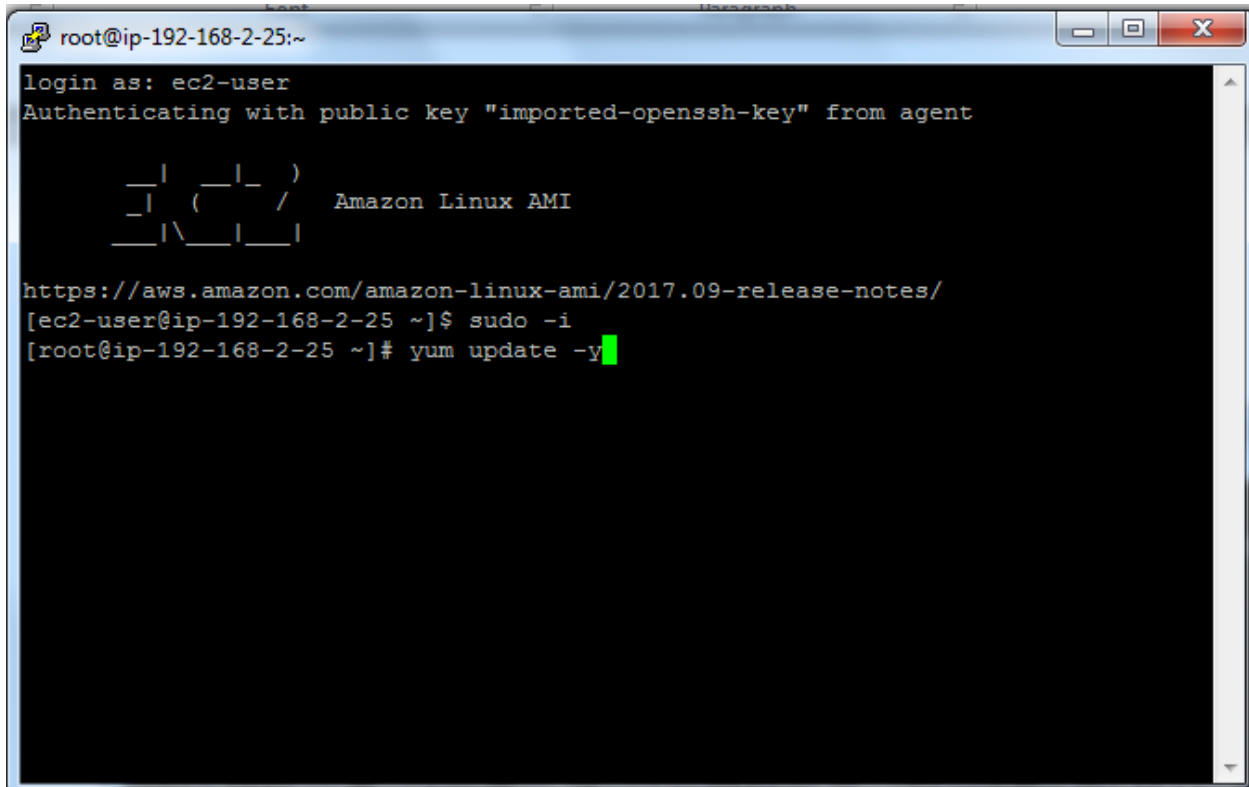
Sudo -i



```
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

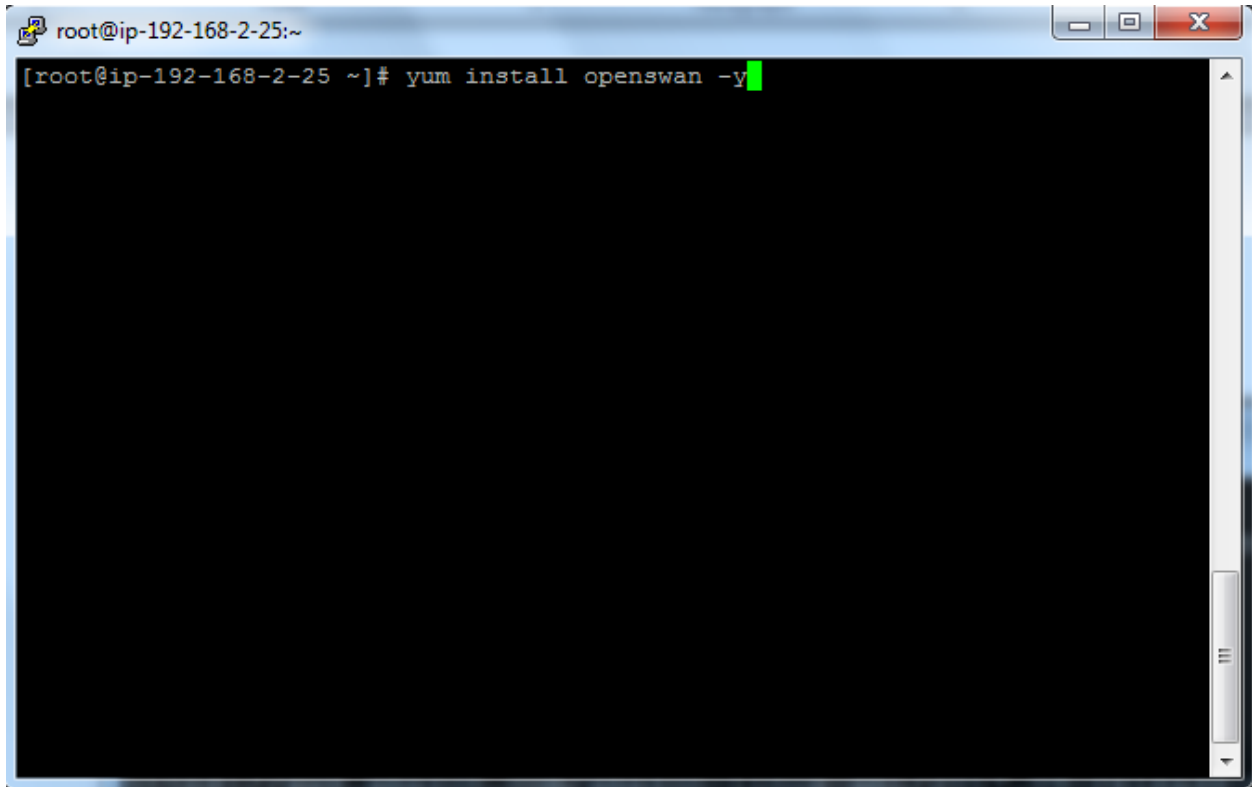
Yum update -y



```
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 ~]# yum update -y
```

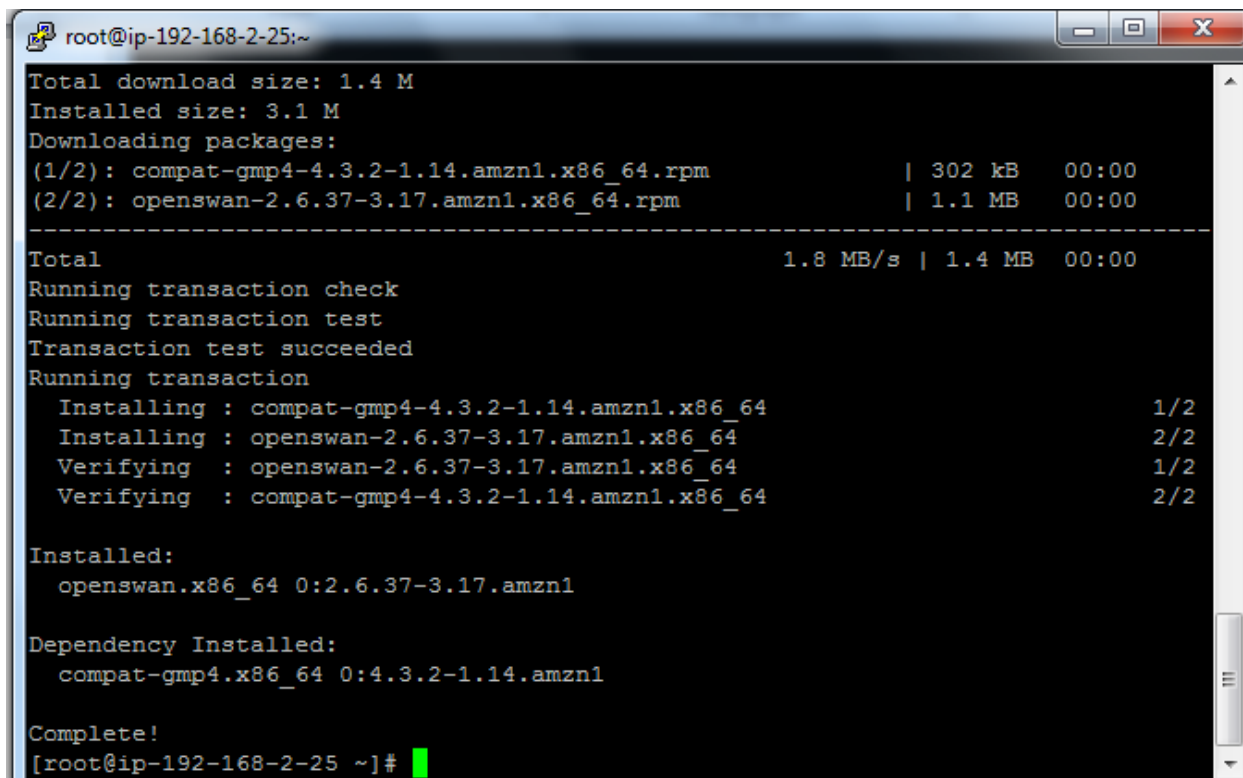
Type

Yum install openswan -y

A terminal window with a blue title bar. The title bar contains a small icon on the left and three window control buttons (minimize, maximize, close) on the right. The text in the title bar is 'root@ip-192-168-2-25:~'. The terminal area has a black background. The prompt '[root@ip-192-168-2-25 ~]#' is visible, followed by the command 'yum install openswan -y' and a green cursor at the end of the line.

```
root@ip-192-168-2-25:~  
[root@ip-192-168-2-25 ~]# yum install openswan -y
```

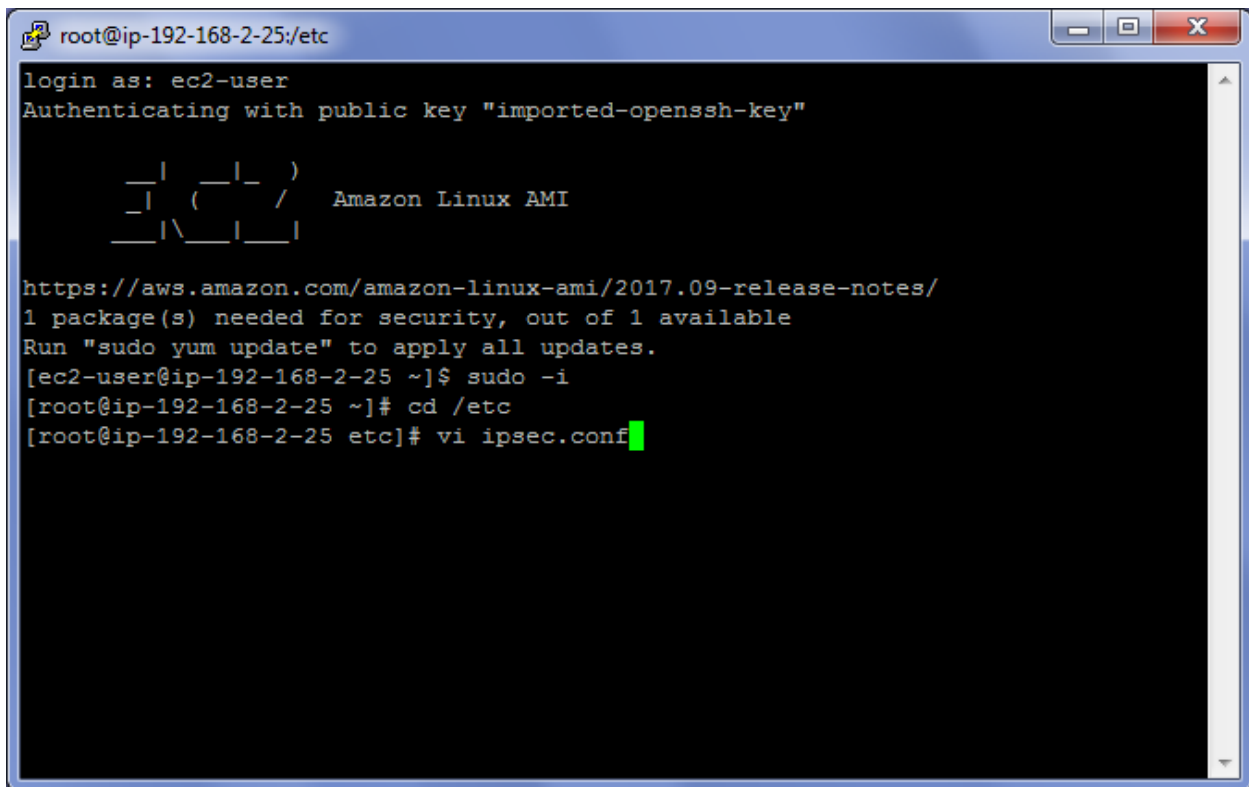
Open swan has been successfully installed.



```
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



```
root@ip-192-168-2-25:/etc
login as: ec2-user
Authenticating with public key "imported-openssh-key"

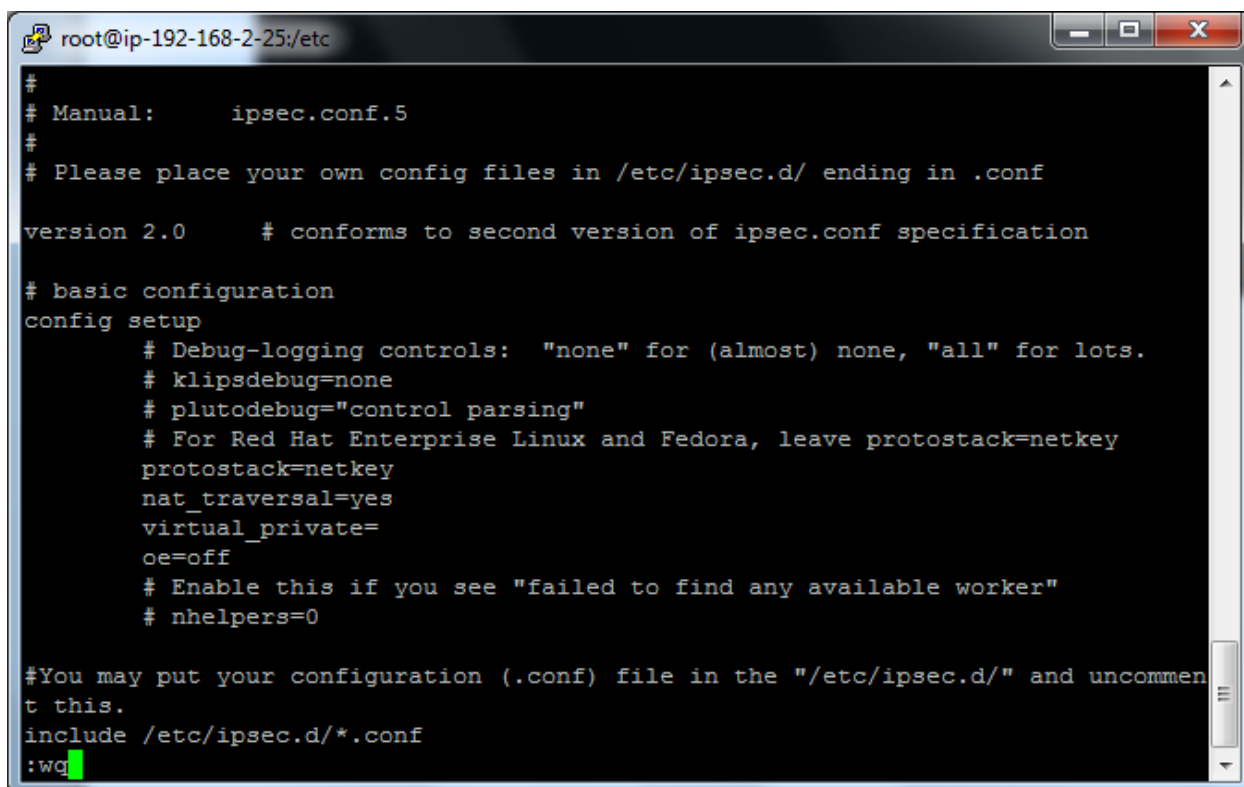
  ____|__|_ )
  _| ( _|_ /   Amazon Linux AMI
  __| \__|__|

https://aws.amazon.com/amazon-linux-ami/2017.09-release-notes/
1 package(s) needed for security, out of 1 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-192-168-2-25 ~]$ sudo -i
[root@ip-192-168-2-25 ~]# cd /etc
[root@ip-192-168-2-25 etc]# vi ipsec.conf
```


[illegible]

Press escape and type

:wq



```
root@ip-192-168-2-25:/etc
#
# Manual:      ipsec.conf.5
#
# Please place your own config files in /etc/ipsec.d/ ending in .conf

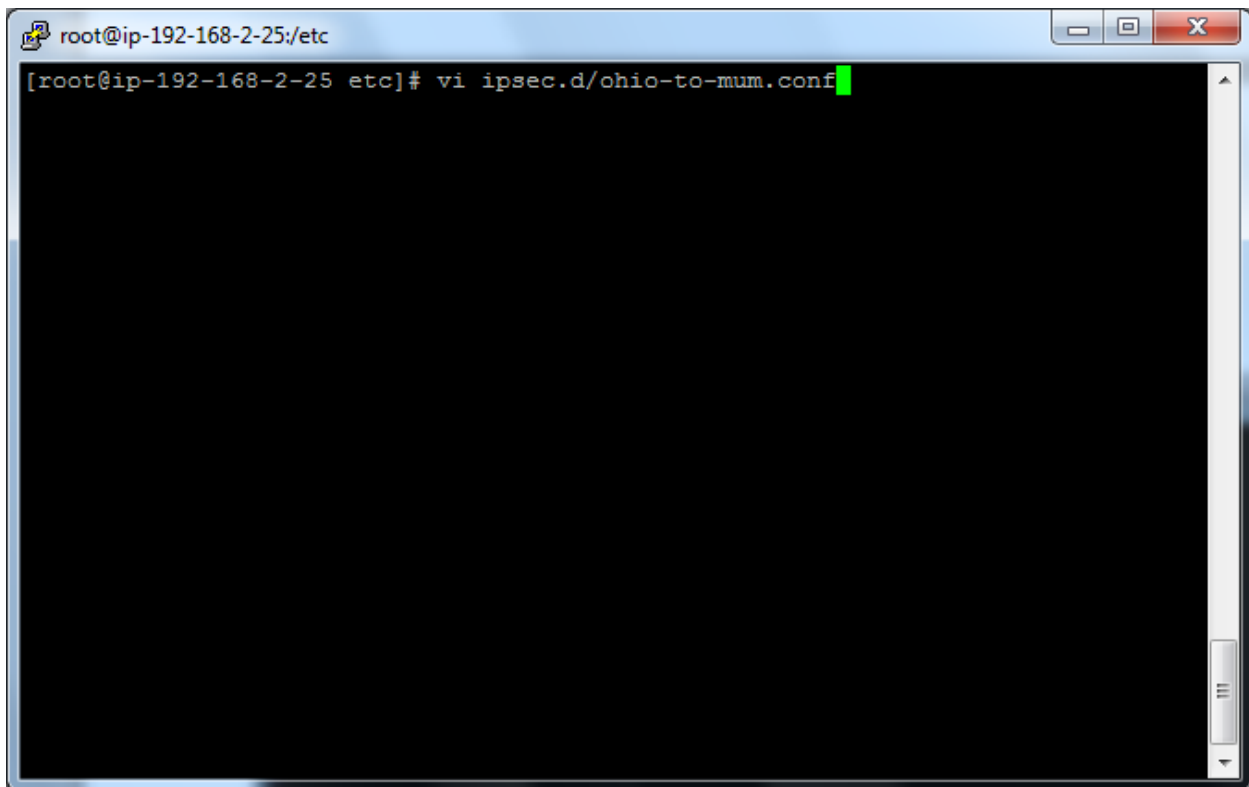
version 2.0      # conforms to second version of ipsec.conf specification

# 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 uncommen
t this.
include /etc/ipsec.d/*.conf
:wq
```

Type

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



```
root@ip-192-168-2-25:/etc
[root@ip-192-168-2-25 etc]# 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

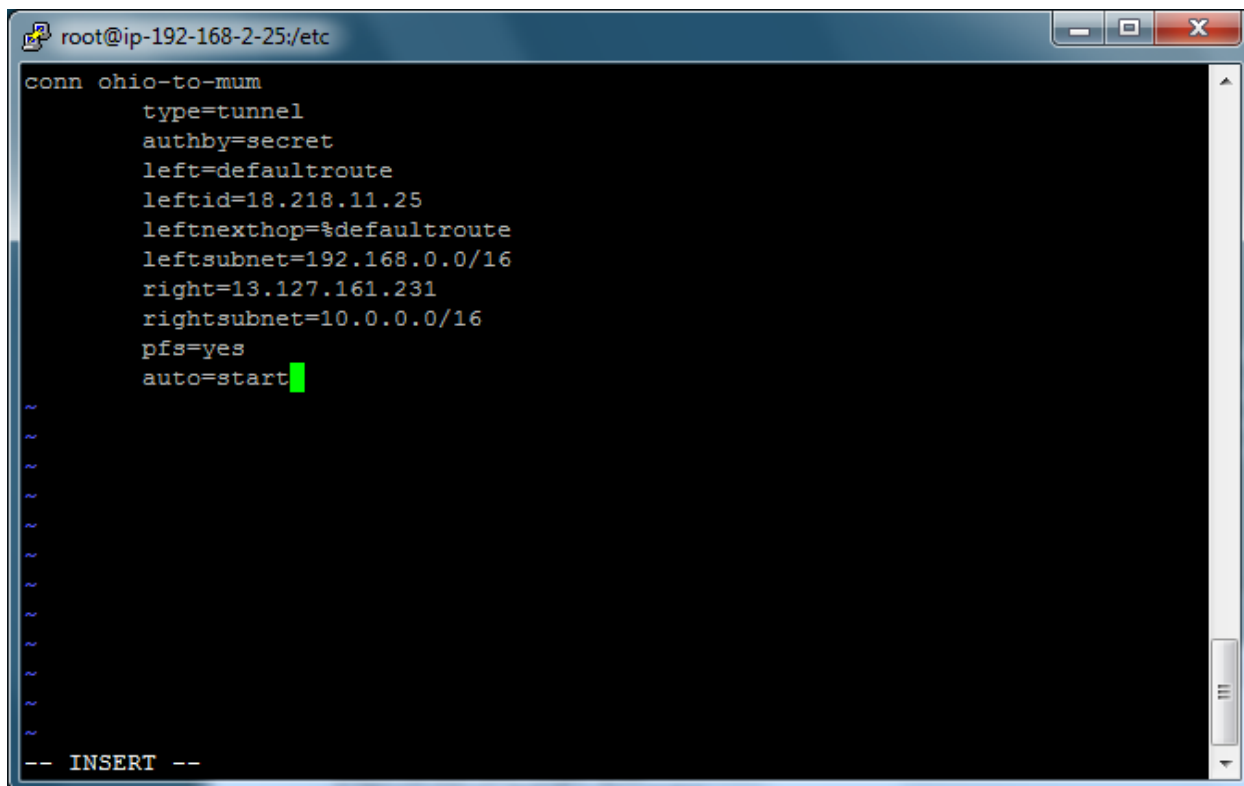
leftsubnet=192.168.0.0/16

right=13.127.161.231

rightsubnet=10.0.0.0/16

pfs=yes

auto=start



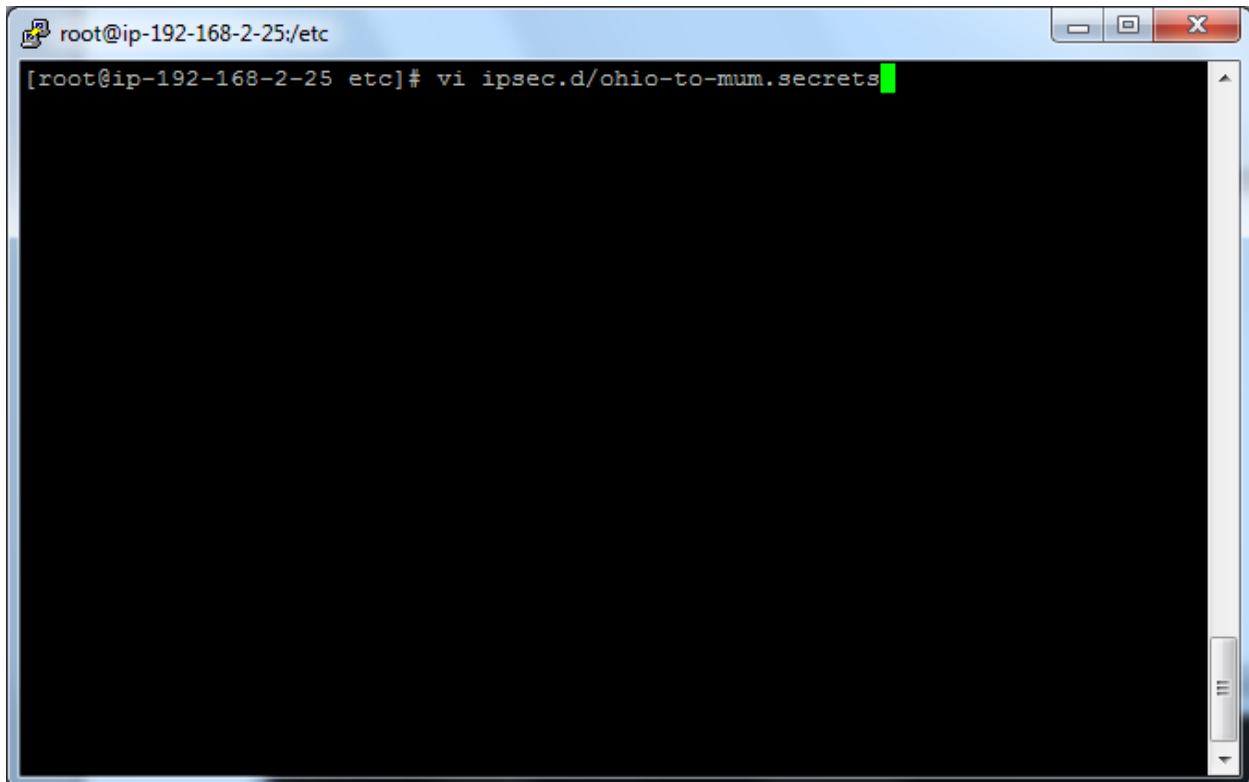
```
root@ip-192-168-2-25:/etc
conn ohio-to-mum
    type=tunnel
    authby=secret
    left=defaultroute
    leftid=18.218.11.25
    leftnexthop=%defaultroute
    leftsubnet=192.168.0.0/16
    right=13.127.161.231
    rightsubnet=10.0.0.0/16
    pfs=yes
    auto=start
~
~
~
~
~
~
~
~
~
~
-- INSERT --
```

Press escape and type

:wq

Type

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



```
root@ip-192-168-2-25/etc
[root@ip-192-168-2-25 etc]# vi ipsec.d/ohio-to-mum.secrets
```

Preshared key is “Sansbound”

[illegible]

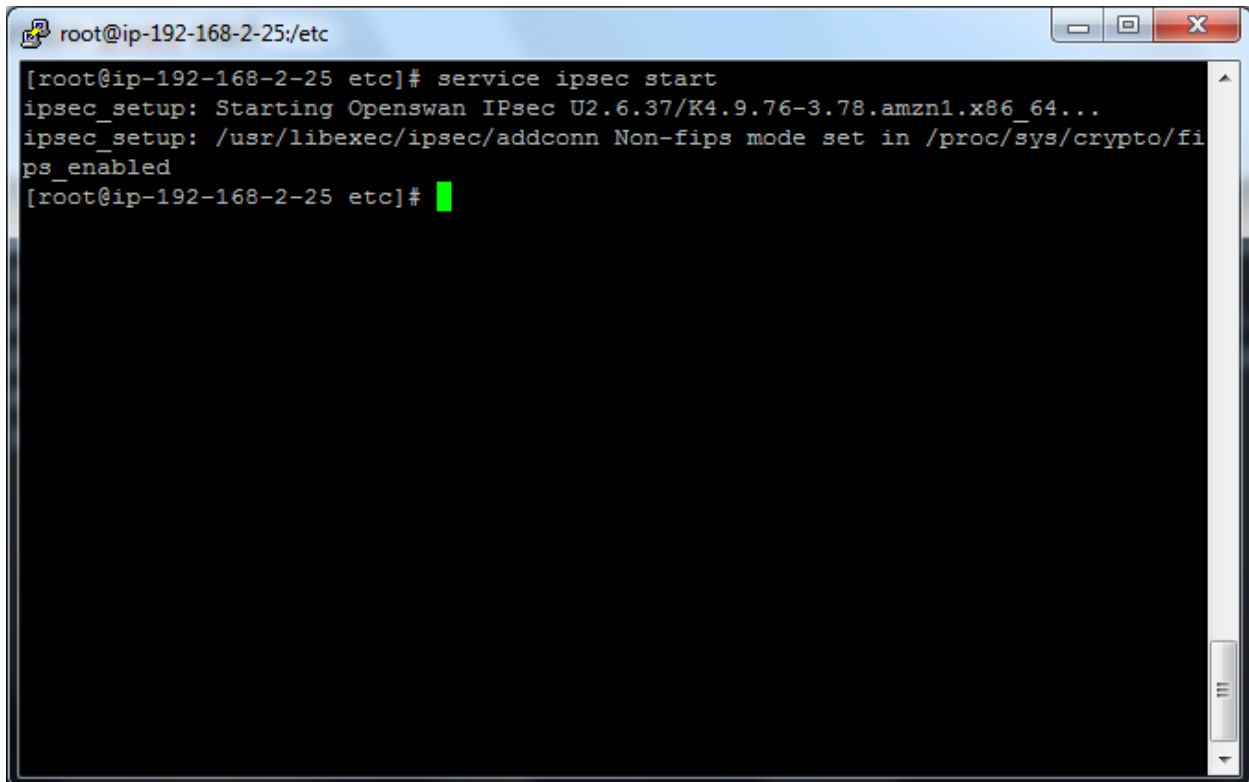
Press escape and type

:wq

[illegible]

Type

service ipsec start



```
root@ip-192-168-2-25/etc  
[root@ip-192-168-2-25 etc]# service ipsec start  
ipsec_setup: Starting Openswan IPsec U2.6.37/K4.9.76-3.78.amzn1.x86_64...  
ipsec_setup: /usr/libexec/ipsec/addconn Non-fips mode set in /proc/sys/crypto/fips_enabled  
[root@ip-192-168-2-25 etc]#
```

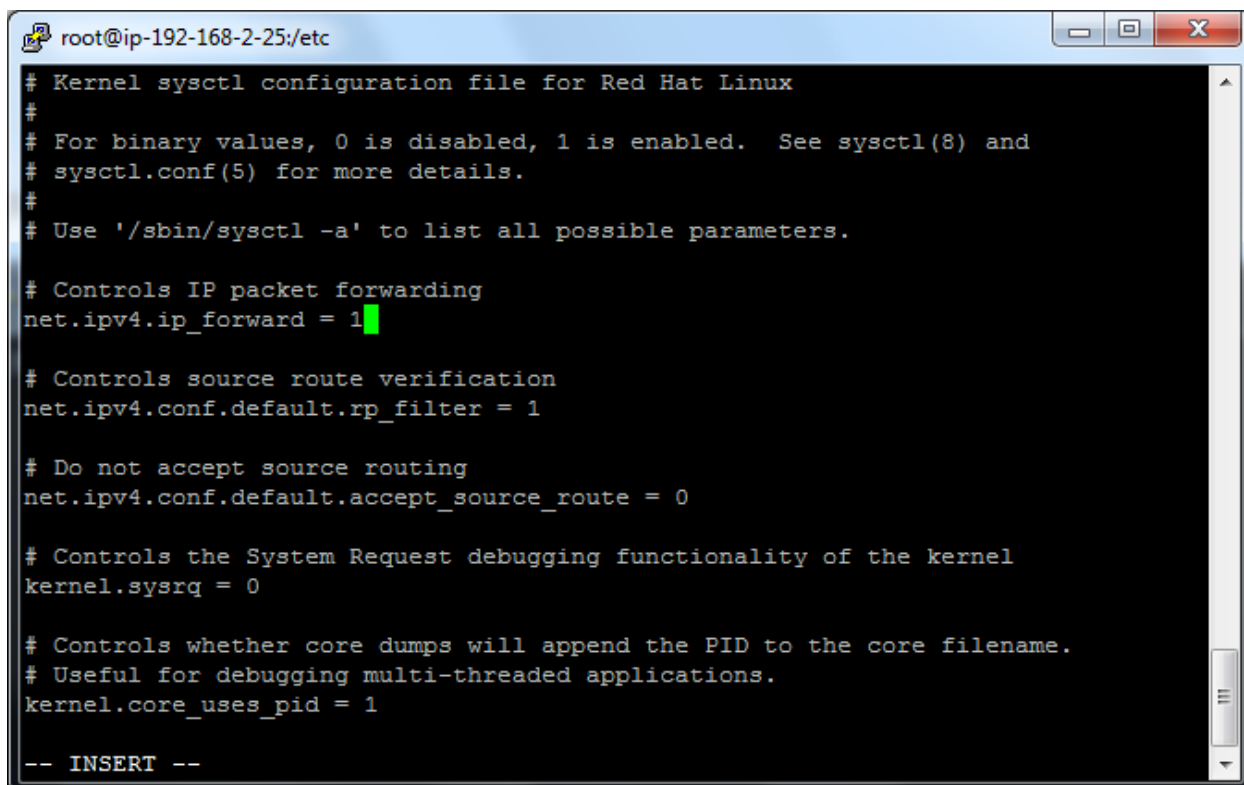

Type

Vi sysctl.conf

A terminal window with a blue title bar. The title bar text is "root@ip-192-168-2-25:/etc". The terminal content shows the command "[root@ip-192-168-2-25 etc]# vi sysctl.conf" followed by a green cursor. The terminal background is black, and the text is white. The window has standard Linux window controls (minimize, maximize, close) in the top right corner.

```
root@ip-192-168-2-25:/etc
[root@ip-192-168-2-25 etc]# vi sysctl.conf
```

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



```
root@ip-192-168-2-25:/etc
# Kernel sysctl configuration file for Red Hat Linux
#
# For binary values, 0 is disabled, 1 is enabled.  See sysctl(8) and
# sysctl.conf(5) for more details.
#
# Use '/sbin/sysctl -a' to list all possible parameters.

# Controls IP packet forwarding
net.ipv4.ip_forward = 1

# Controls source route verification
net.ipv4.conf.default.rp_filter = 1

# Do not accept source routing
net.ipv4.conf.default.accept_source_route = 0

# Controls the System Request debugging functionality of the kernel
kernel.sysrq = 0

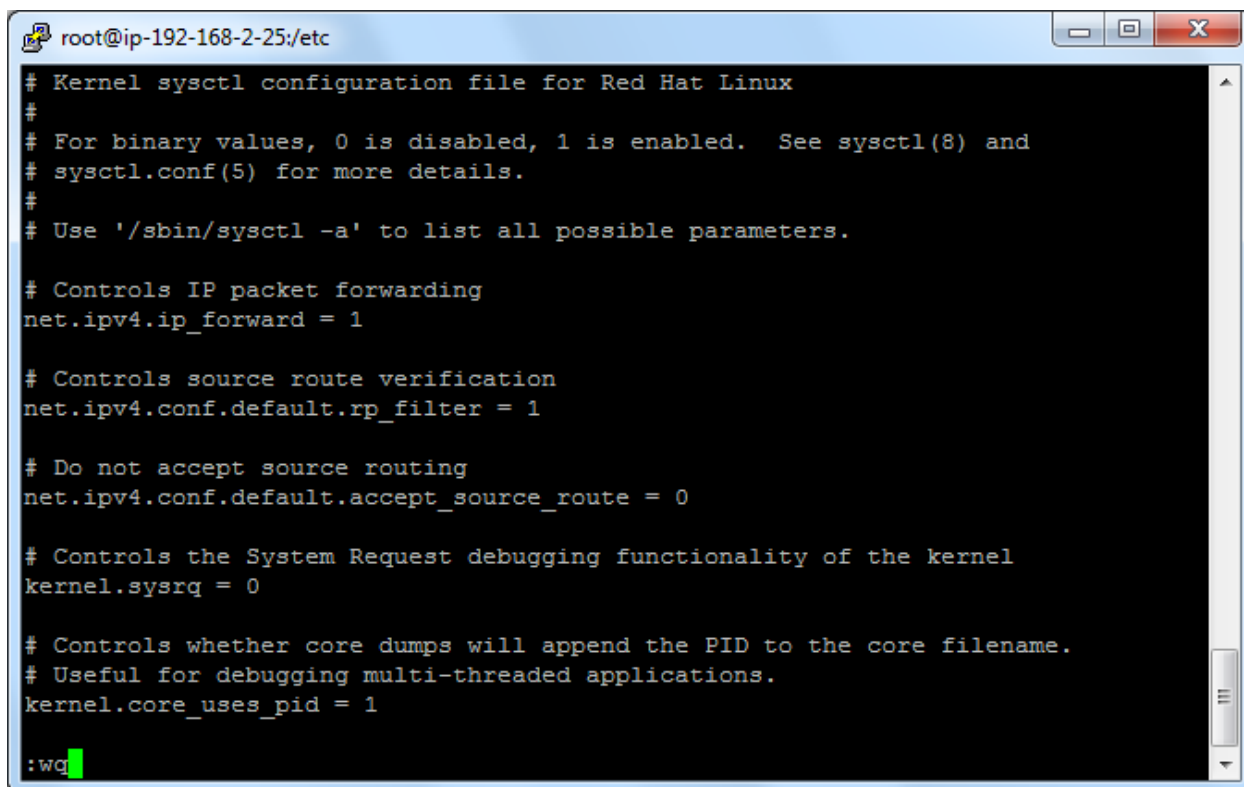
# Controls whether core dumps will append the PID to the core filename.
# Useful for debugging multi-threaded applications.
kernel.core_uses_pid = 1

-- INSERT --
```

Press escape key.

Type

:wq

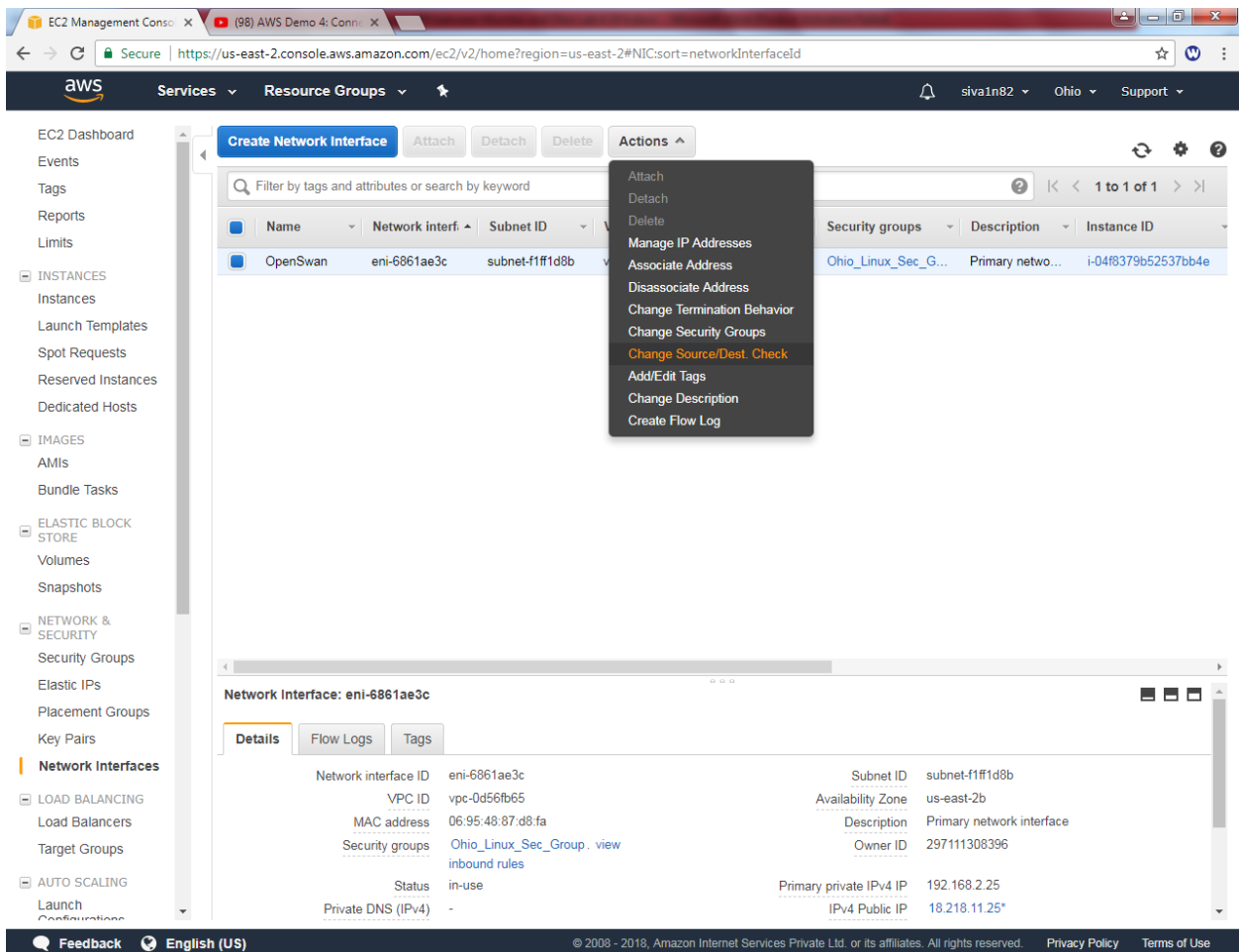


```
root@ip-192-168-2-25:/etc
# Kernel sysctl configuration file for Red Hat Linux
#
# For binary values, 0 is disabled, 1 is enabled.  See sysctl(8) and
# sysctl.conf(5) for more details.
#
# Use '/sbin/sysctl -a' to list all possible parameters.
#
# Controls IP packet forwarding
net.ipv4.ip_forward = 1
#
# Controls source route verification
net.ipv4.conf.default.rp_filter = 1
#
# Do not accept source routing
net.ipv4.conf.default.accept_source_route = 0
#
# Controls the System Request debugging functionality of the kernel
kernel.sysrq = 0
#
# Controls whether core dumps will append the PID to the core filename.
# Useful for debugging multi-threaded applications.
kernel.core_uses_pid = 1
:wq
```

Go to Ec2 Dashboard

Click “Network interface” and then select “OpenSwan”

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



The screenshot shows the AWS Management Console for the EC2 service. The left sidebar contains navigation links for various AWS services. The main content area displays a list of Network Interfaces. The 'OpenSwan' interface is selected, and the 'Actions' menu is open, showing options like 'Attach', 'Detach', 'Delete', 'Manage IP Addresses', 'Associate Address', 'Disassociate Address', 'Change Termination Behavior', 'Change Security Groups', 'Change Source/Dest. Check' (highlighted), 'Add/Edit Tags', 'Change Description', and 'Create Flow Log'.

Name	Network interf.	Subnet ID	Security groups	Description	Instance ID
OpenSwan	eni-6861ae3c	subnet-f1f1d8b	Ohio_Linux_Sec_G...	Primary netwo...	i-04f8379b52537bb4e

Network Interface: eni-6861ae3c

Details | Flow Logs | Tags

Network interface ID	eni-6861ae3c	Subnet ID	subnet-f1f1d8b
VPC ID	vpc-0d56fb65	Availability Zone	us-east-2b
MAC address	06:95:48:87:d8:fa	Description	Primary network interface
Security groups	Ohio_Linux_Sec_Group · view inbound rules	Owner ID	297111308396
Status	in-use	Primary private IPv4 IP	192.168.2.25
Private DNS (IPv4)	-	IPv4 Public IP	18.218.11.25*

Set as “Disabled” and click “save”.

Change Source/Dest. Check ×

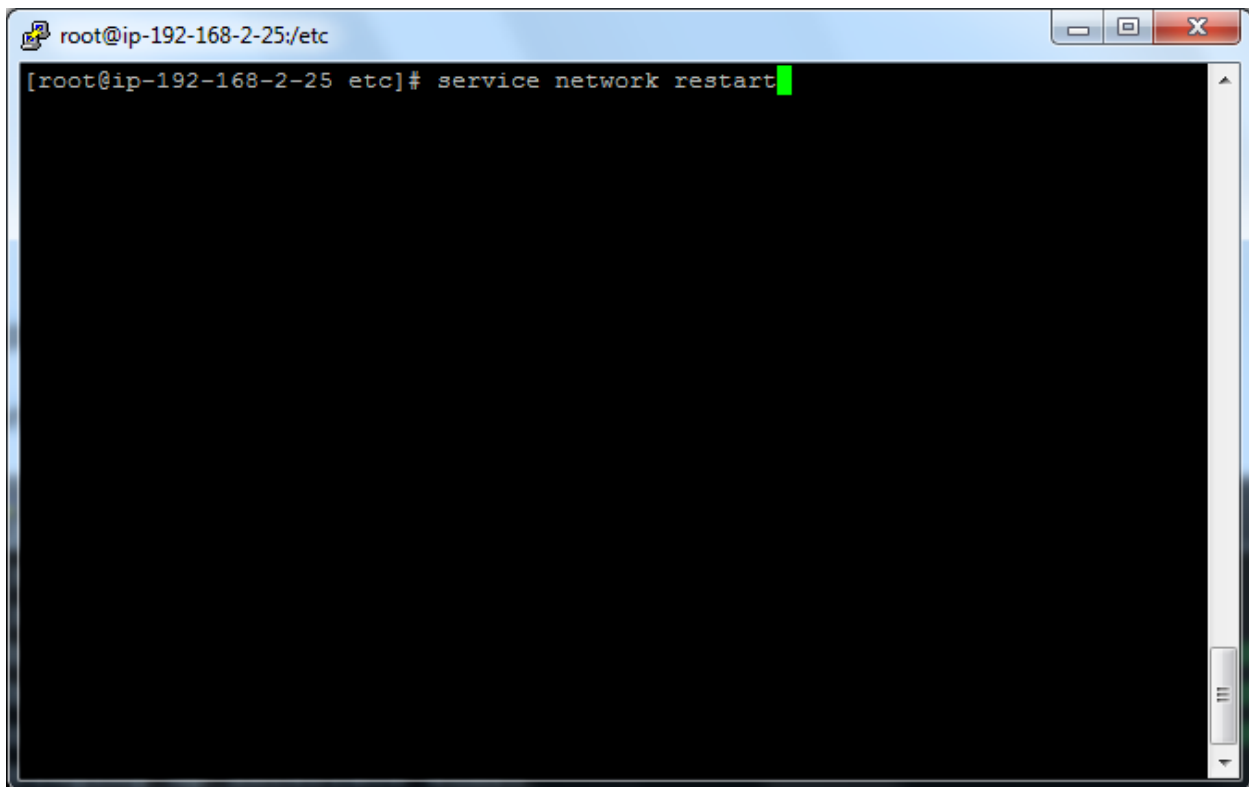
Network Interface eni-6861ae3c

Source/dest. check ☐ Enabled
☒ Disabled

Cancel Save

Type

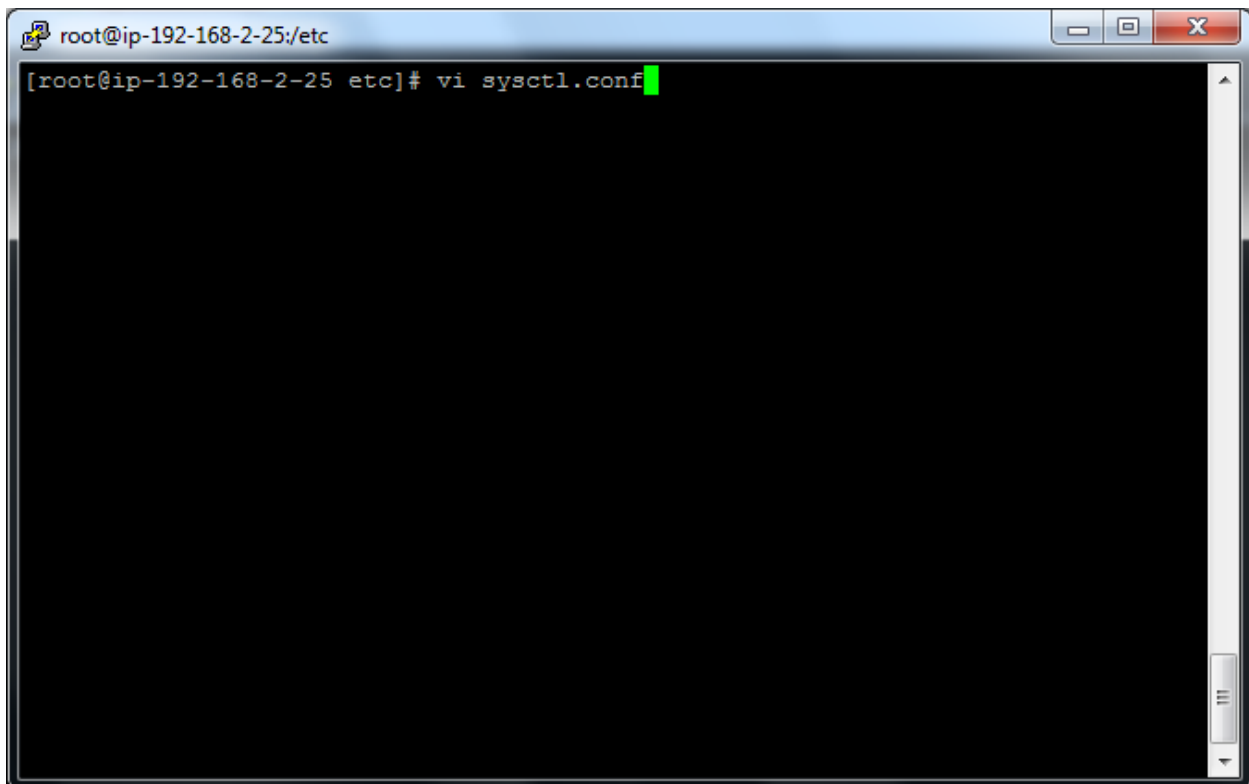
Service network restart



```
root@ip-192-168-2-25:/etc
[root@ip-192-168-2-25 etc]# service network restart
```

Type

Vi sysctl.conf

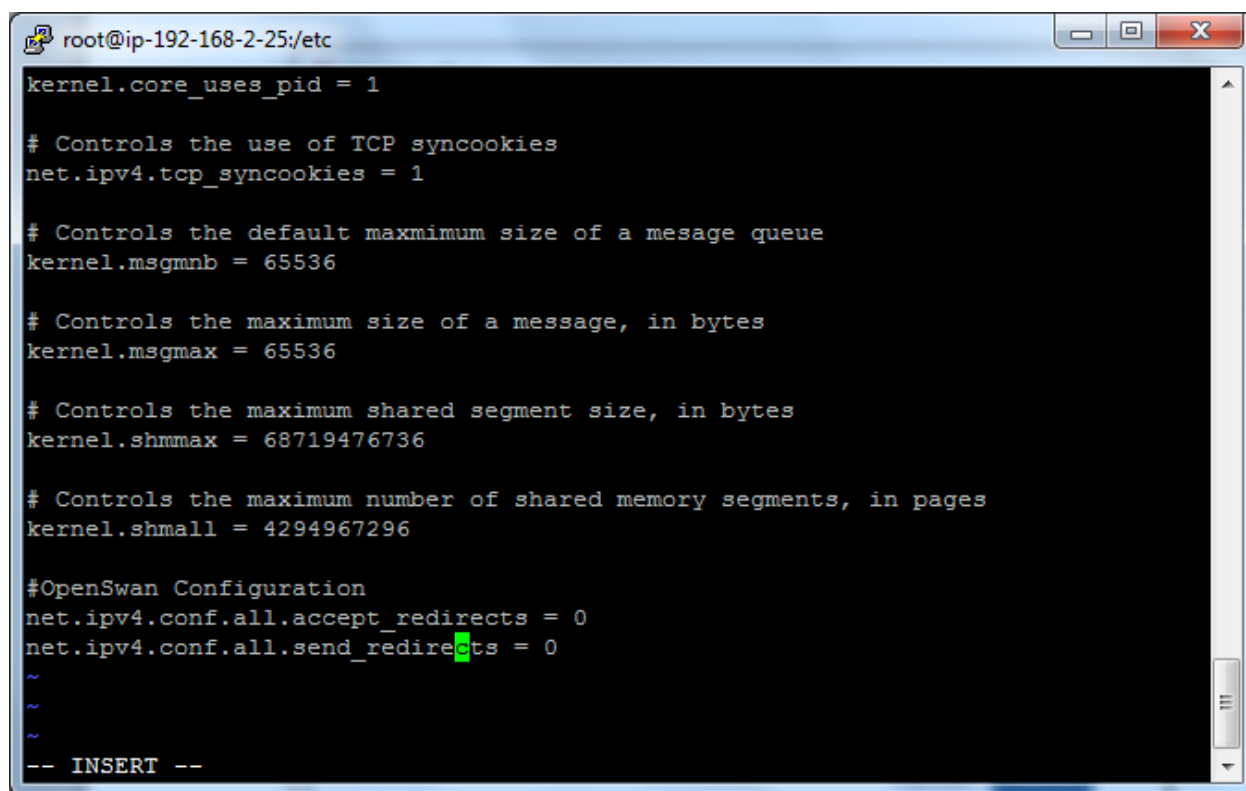


```
root@ip-192-168-2-25/etc  
[root@ip-192-168-2-25 etc]# vi sysctl.conf
```

Press insert key

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

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

A terminal window titled 'root@ip-192-168-2-25:/etc' with standard window controls. The terminal displays a configuration file with various kernel and network settings. The settings include: 'kernel.core_uses_pid = 1', a comment about TCP syncookies followed by 'net.ipv4.tcp_syncookies = 1', a comment about message queue size followed by 'kernel.msgmnb = 65536', a comment about message size followed by 'kernel.msgmax = 65536', a comment about shared segment size followed by 'kernel.shmmax = 68719476736', and a comment about shared memory segments followed by 'kernel.shmall = 4294967296'. Under the section '#OpenSwan Configuration', it shows 'net.ipv4.conf.all.accept_redirects = 0' and 'net.ipv4.conf.all.send_redirects = 0'. The cursor is positioned at the end of the second line. At the bottom, there are tilde characters and a '-- INSERT --' prompt.

```
root@ip-192-168-2-25:/etc
kernel.core_uses_pid = 1

# Controls the use of TCP syncookies
net.ipv4.tcp_syncookies = 1

# Controls the default maximum size of a message queue
kernel.msgmnb = 65536

# Controls the maximum size of a message, in bytes
kernel.msgmax = 65536

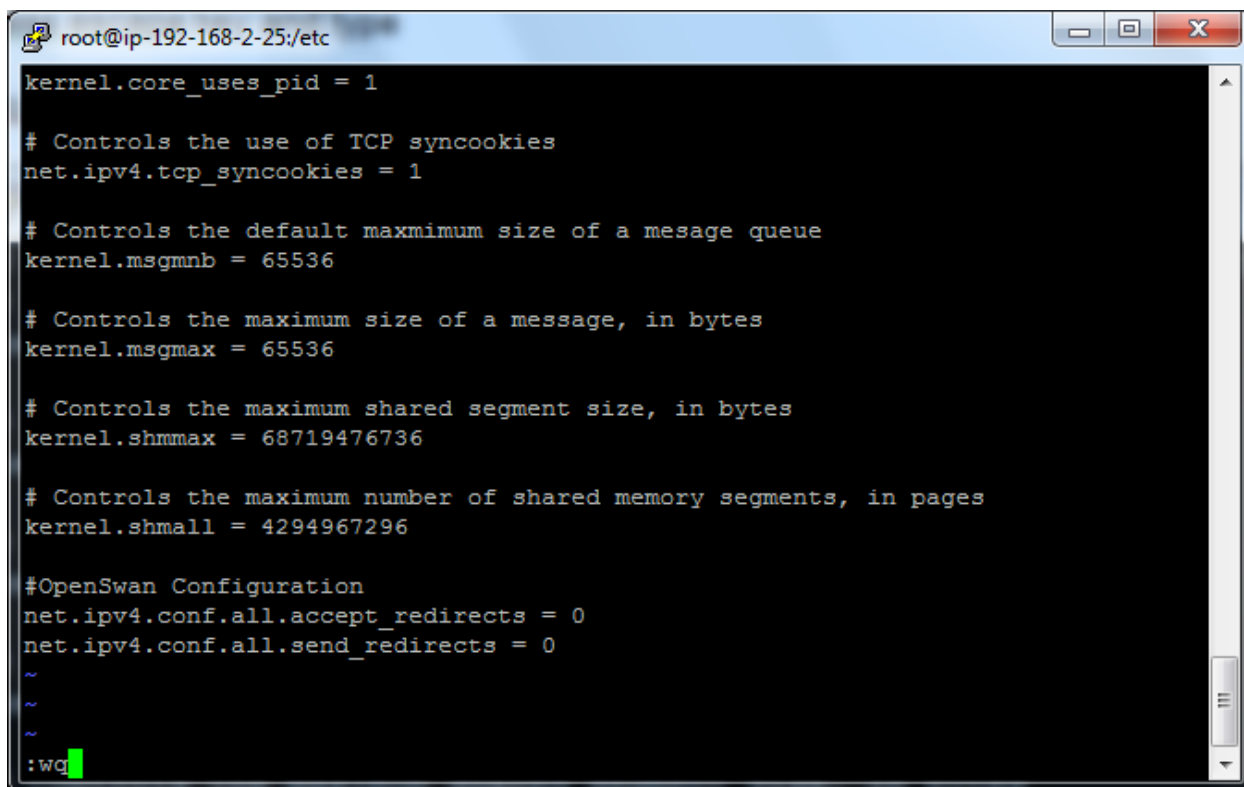
# Controls the maximum shared segment size, in bytes
kernel.shmmax = 68719476736

# Controls the maximum number of shared memory segments, in pages
kernel.shmall = 4294967296

#OpenSwan Configuration
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
~
~
~
-- INSERT --
```


Press escape key and then type

:wq

A terminal window titled 'root@ip-192-168-2-25:/etc' with standard window controls. The terminal displays a configuration file with various kernel and network settings. At the bottom, the user has entered ':wq' to save and exit the editor, with a green cursor at the end of the command.

```
root@ip-192-168-2-25:/etc
kernel.core_uses_pid = 1

# Controls the use of TCP syncookies
net.ipv4.tcp_syncookies = 1

# Controls the default maximum size of a message queue
kernel.msgmnb = 65536

# Controls the maximum size of a message, in bytes
kernel.msgmax = 65536

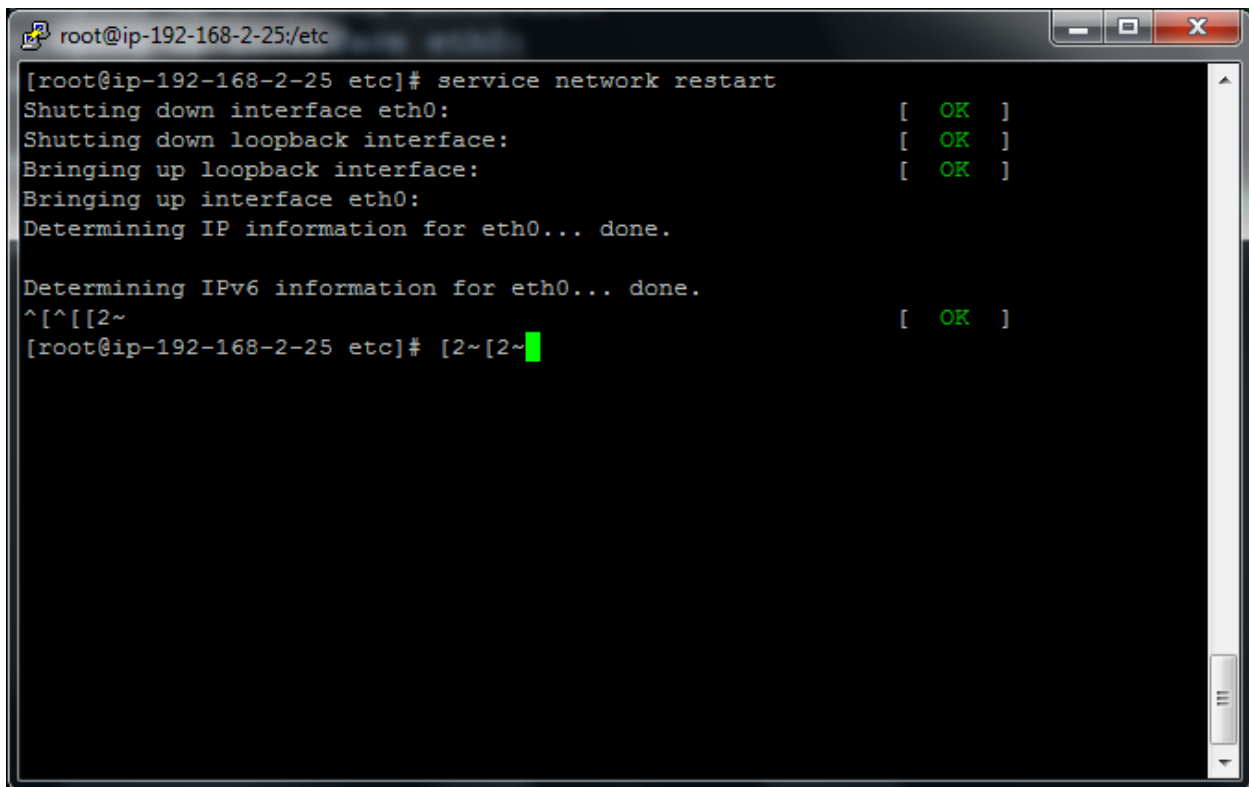
# Controls the maximum shared segment size, in bytes
kernel.shmmax = 68719476736

# Controls the maximum number of shared memory segments, in pages
kernel.shmall = 4294967296

#OpenSwan Configuration
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
~
~
~
:wq
```

Type

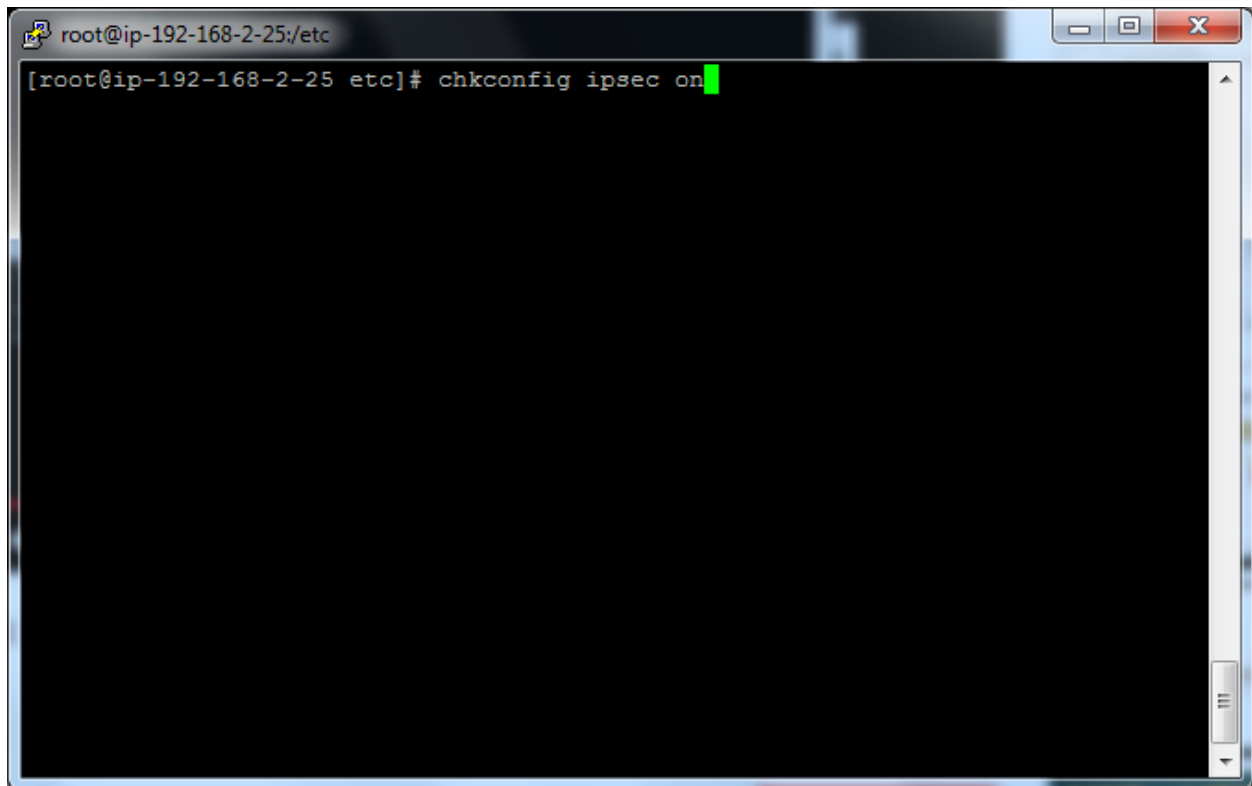
Service network restart



```
root@ip-192-168-2-25:/etc
[root@ip-192-168-2-25 etc]# service network restart
Shutting down interface eth0:           [ OK ]
Shutting down loopback interface:       [ OK ]
Bringing up loopback interface:         [ OK ]
Bringing up interface eth0:
Determining IP information for eth0... done.

Determining IPv6 information for eth0... done.
^[^[2~                                   [ OK ]
[root@ip-192-168-2-25 etc]# [2~[2~
```

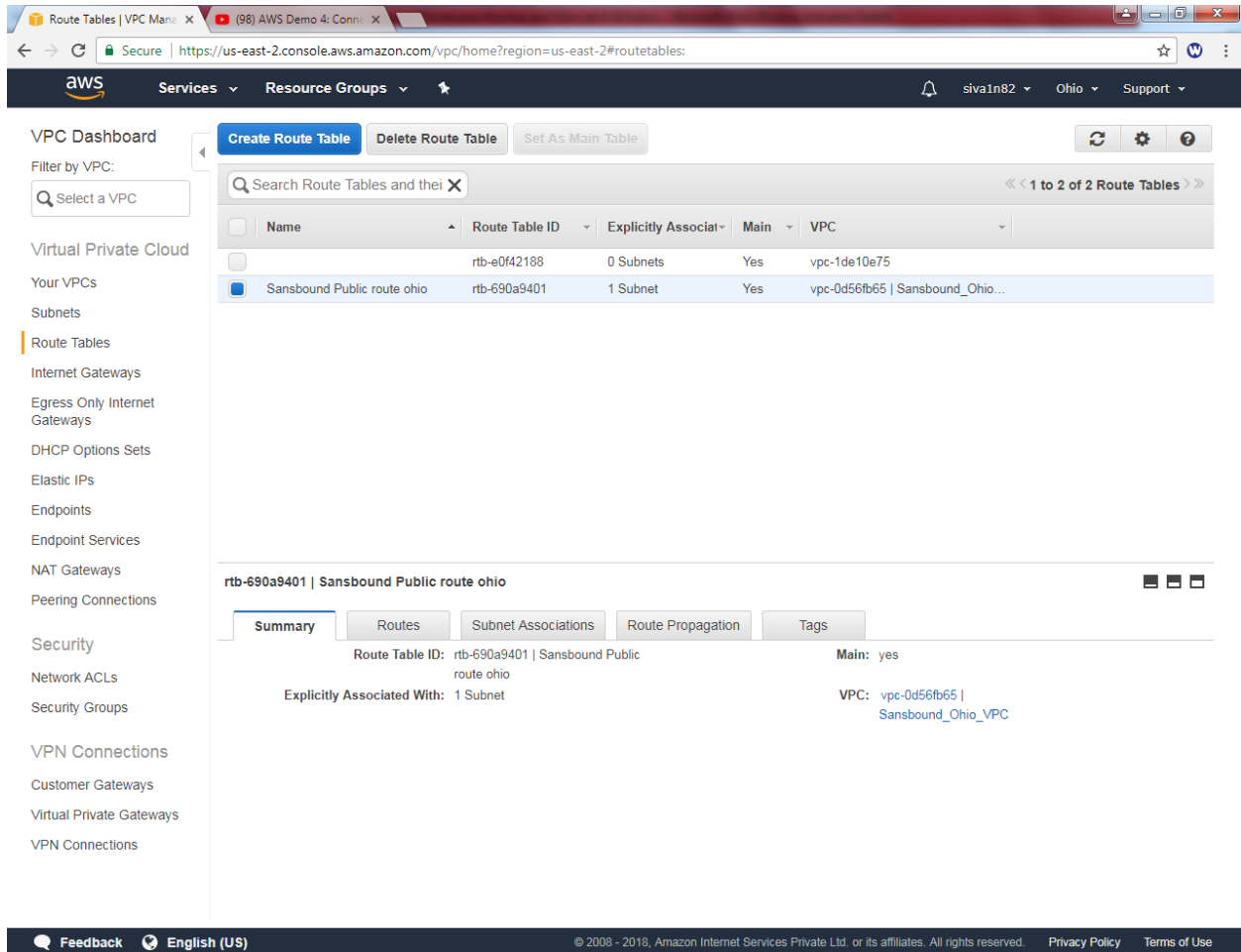
Type `chkconfig ipsec on`



```
root@ip-192-168-2-25:/etc
[root@ip-192-168-2-25 etc]# chkconfig ipsec on
```

Go to VPC,

Click Route table and select sansbound public route table.



The screenshot shows the AWS Management Console interface. The top navigation bar includes the AWS logo, a search bar, and navigation links for Services, Resource Groups, and a user profile. The left sidebar displays the VPC Dashboard with a search filter and a list of VPC resources. The main content area shows a table of Route Tables. The selected route table, 'Sansbound Public route ohio', is highlighted. Below the table, the details for this route table are displayed, including its ID, name, and associated VPC.

VPC Dashboard

Filter by 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

Route Tables

Search Route Tables and their associated VPCs

Name	Route Table ID	Explicitly Associated	Main	VPC
	rtb-e0f42188	0 Subnets	Yes	vpc-1de10e75
<input checked="" type="checkbox"/> 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

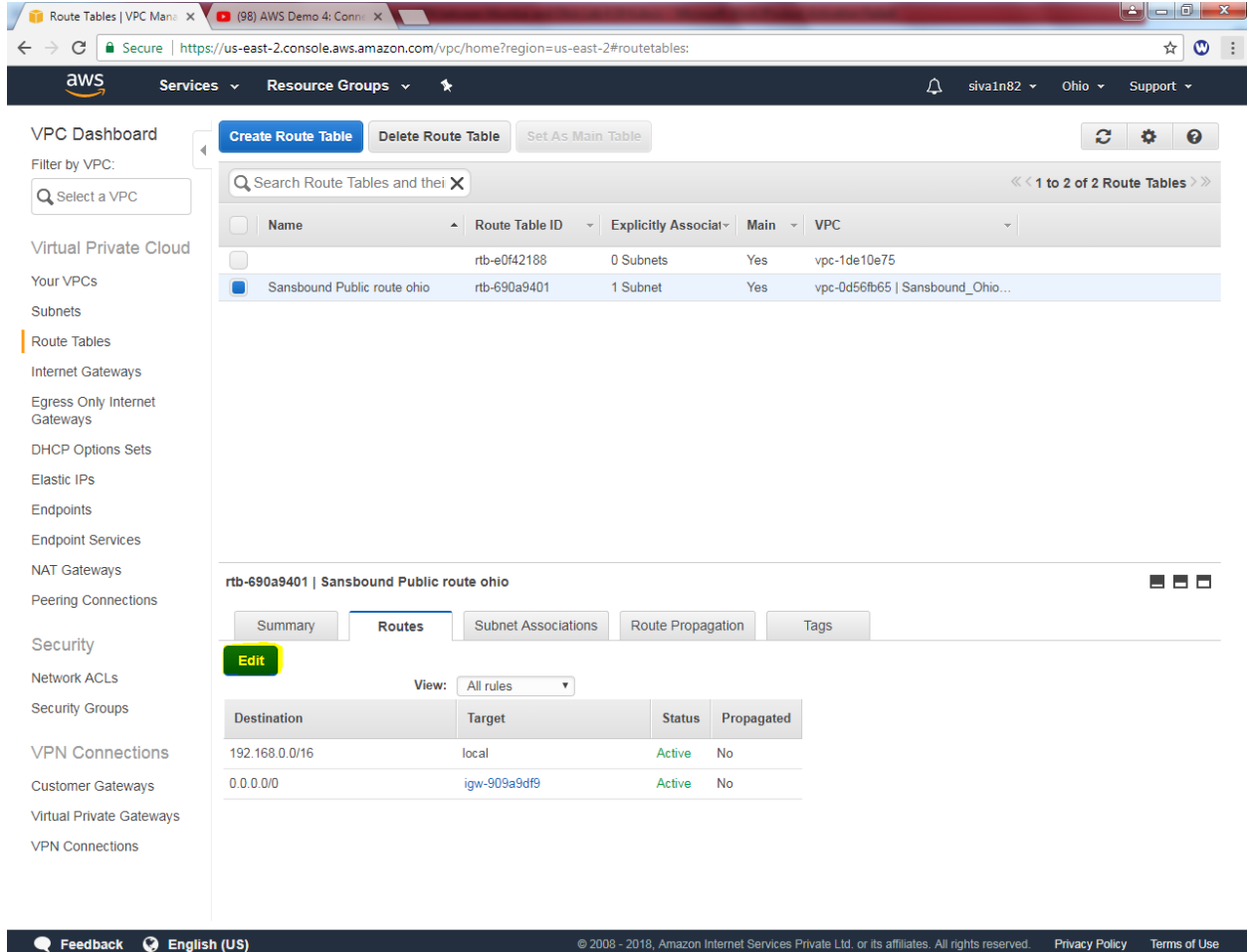
Route Table ID: rtb-690a9401 | Sansbound Public route ohio

Main: yes

Explicitly Associated With: 1 Subnet

VPC: vpc-0d56fb65 | Sansbound_Ohio_VPC

Click “Edit”.

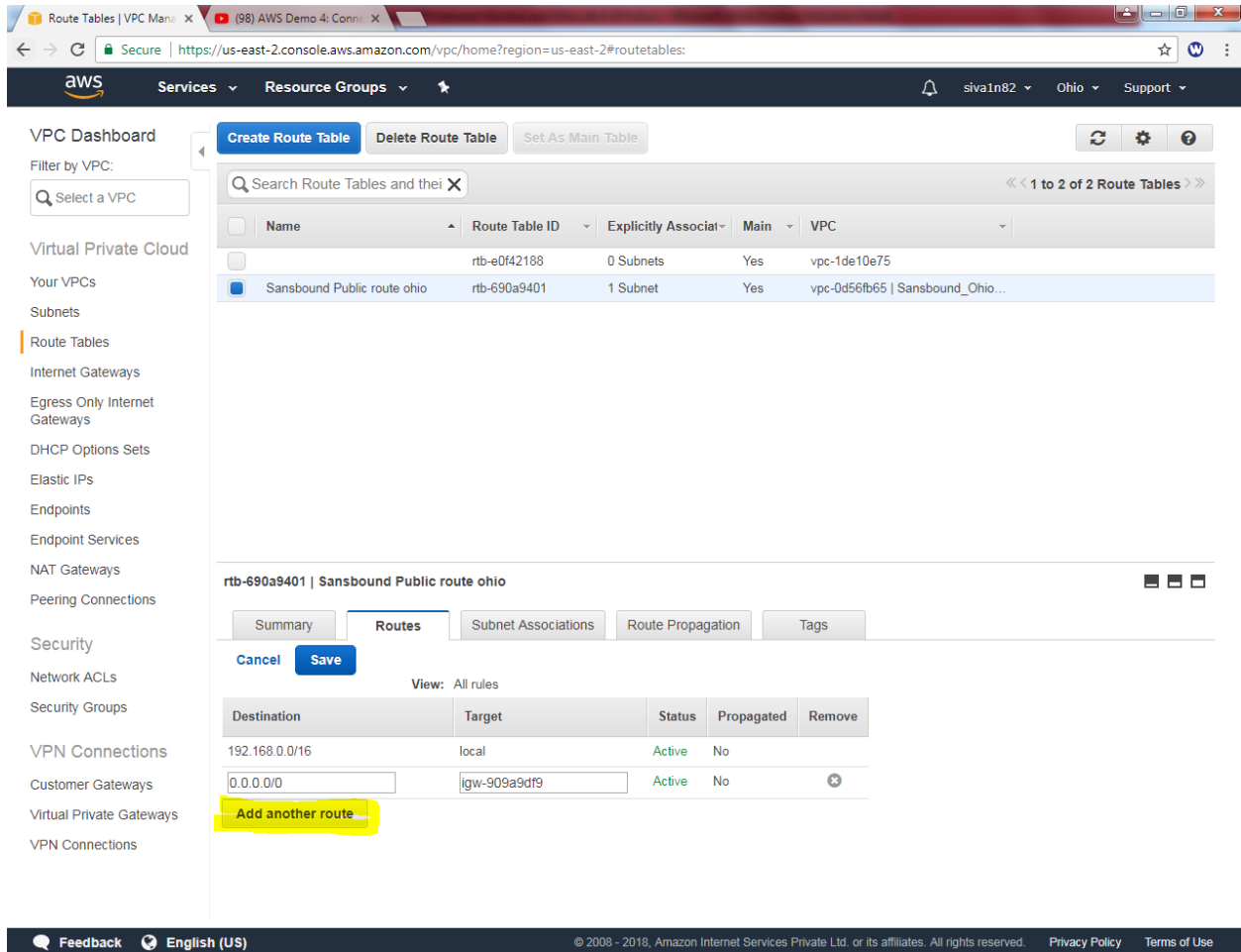


The screenshot shows the AWS Management Console interface. The left sidebar contains the VPC Dashboard menu with options like Virtual Private Cloud, Your VPCs, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, Endpoint Services, NAT Gateways, Peering Connections, Security, Network ACLs, Security Groups, VPN Connections, Customer Gateways, Virtual Private Gateways, and VPN Connections. The main content area displays the 'Sansbound Public route ohio' route table (rtb-690a9401) with 1 Subnet. The 'Routes' tab is selected, showing a table of routes:

Destination	Target	Status	Propagated
192.168.0.0/16	local	Active	No
0.0.0.0/0	igw-909a9df9	Active	No

An 'Edit' button is visible in the top left of the route table details section.

Click “add another route”.

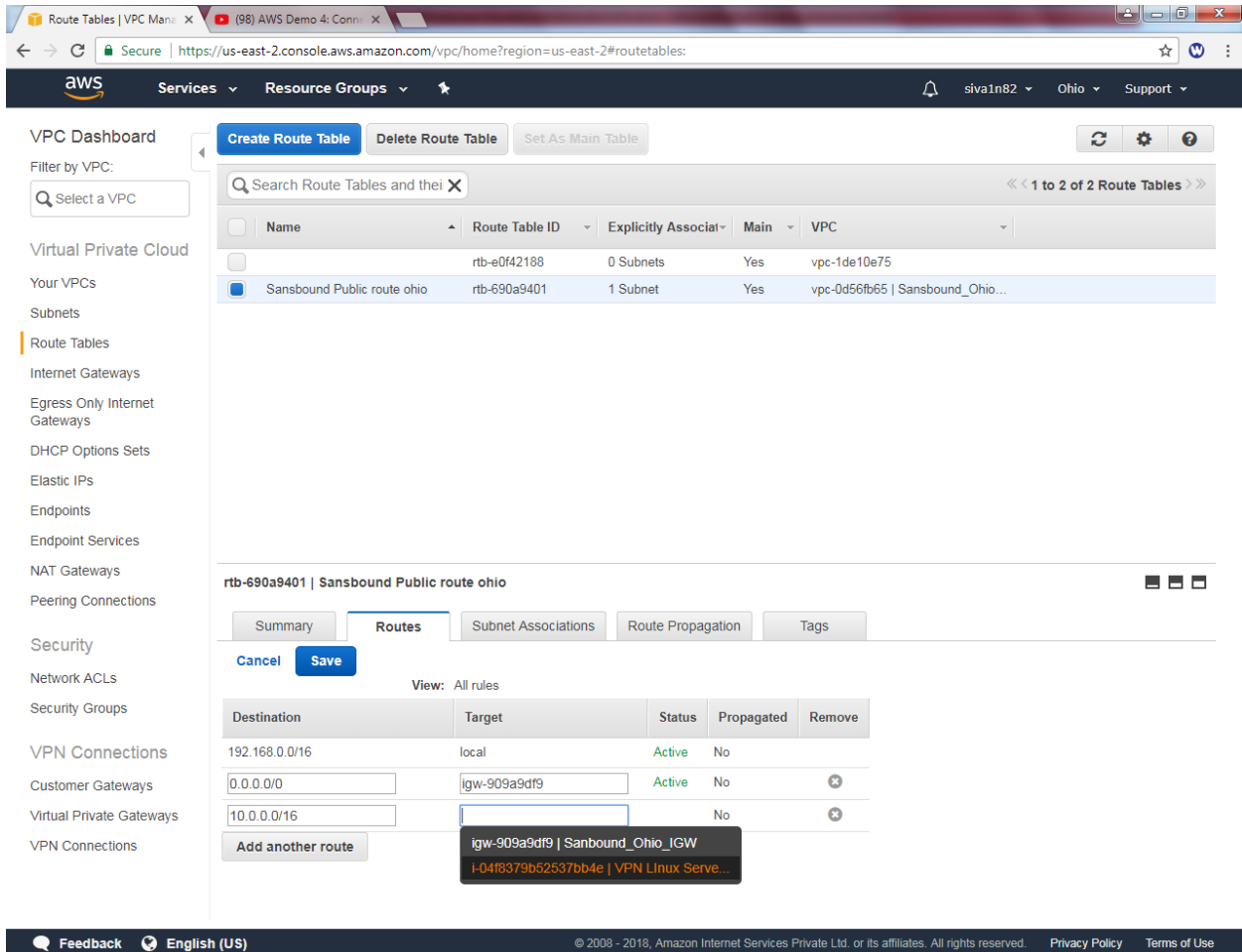


The screenshot shows the AWS Management Console interface for the VPC Dashboard. The left sidebar contains a navigation menu with categories like VPC, Security, VPN, and Customer Gateways. The main content area displays a list of route tables. The 'Sansbound Public route ohio' route table is selected, and the 'Routes' tab is active. Below the tabs, there is a table of routes with columns for Destination, Target, Status, Propagated, and Remove. The first route is for destination 192.168.0.0/16 with target 'local'. The second route is for destination 0.0.0.0/0 with target 'igw-909a9df9'. A yellow box highlights the 'Add another route' button at the bottom of the route table.

Destination	Target	Status	Propagated	Remove
192.168.0.0/16	local	Active	No	
0.0.0.0/0	igw-909a9df9	Active	No	

[Add another route](#)

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



Route Tables | VPC Manage | (98) AWS Demo 4: Conn... X

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 their VPCs << 1 to 2 of 2 Route Tables >>

Name	Route Table ID	Explicitly Associated	Main	VPC
	rtb-e0f42188	0 Subnets	Yes	vpc-1de10e75
<input checked="" type="checkbox"/> 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

Cancel Save

View: All rules

Destination	Target	Status	Propagated	Remove
192.168.0.0/16	local	Active	No	
0.0.0.0/0	igw-909a9df9	Active	No	
10.0.0.0/16	igw-909a9df9	No	No	

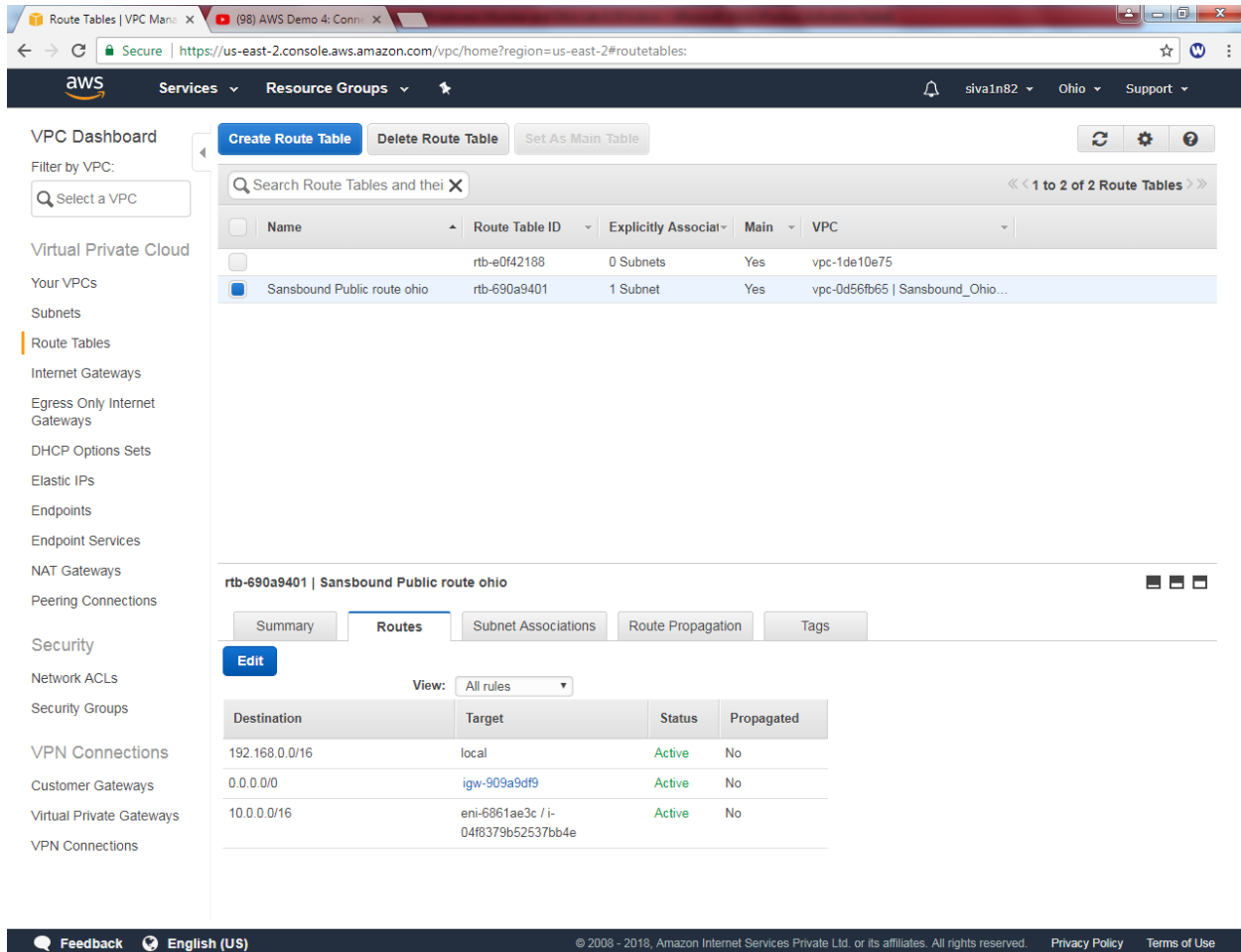
Add another route

igw-909a9df9 | Sanbound_Ohio_IGW
i-04f8379b52537bb4e | VPN Linux Serve...

Feedback English (US) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Click “save”.

Click To view detailed information of routing table as below.



The screenshot displays the AWS Management Console interface. On the left is the VPC Dashboard sidebar with various navigation links. The main content area shows a list of Route Tables. The selected route table, 'rtb-690a9401 | Sansbound Public route ohio', is highlighted. Below the list, the 'Routes' tab is active, showing a table of routing rules.

Destination	Target	Status	Propagated
192.168.0.0/16	local	Active	No
0.0.0.0/0	igw-909a9df9	Active	No
10.0.0.0/16	eni-6861ae3c / i-04f8379b52537bb4e	Active	No