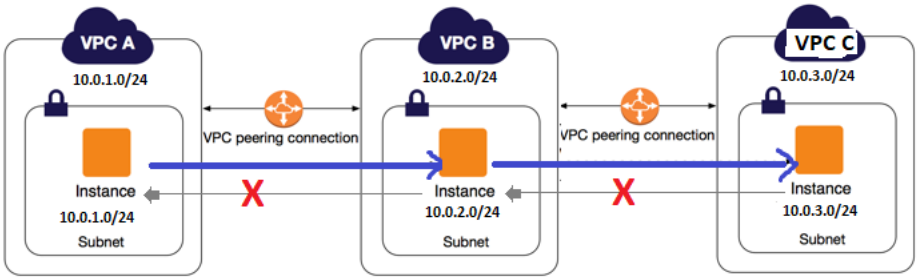
Assignment 1

Requirement:

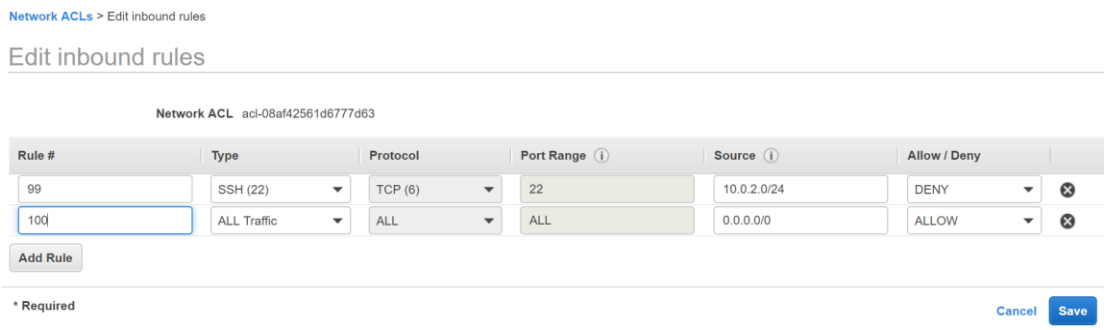
Create 3 EC2 instances (Machine A, Machine B and Machine C)in 3 different VPCs(VPC A, VPC B, VPC C). We should be able to do SSH from Machine A to Machine B and from Machine B to Machine C.

However, we should NOT be allowed to do SSH from Machine B to Machine A as well as Machine C to Machine B

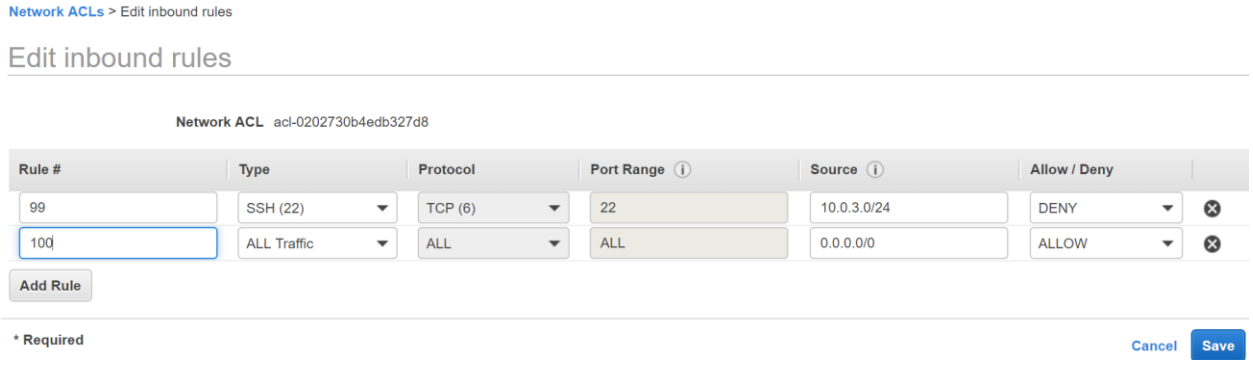


Solution:

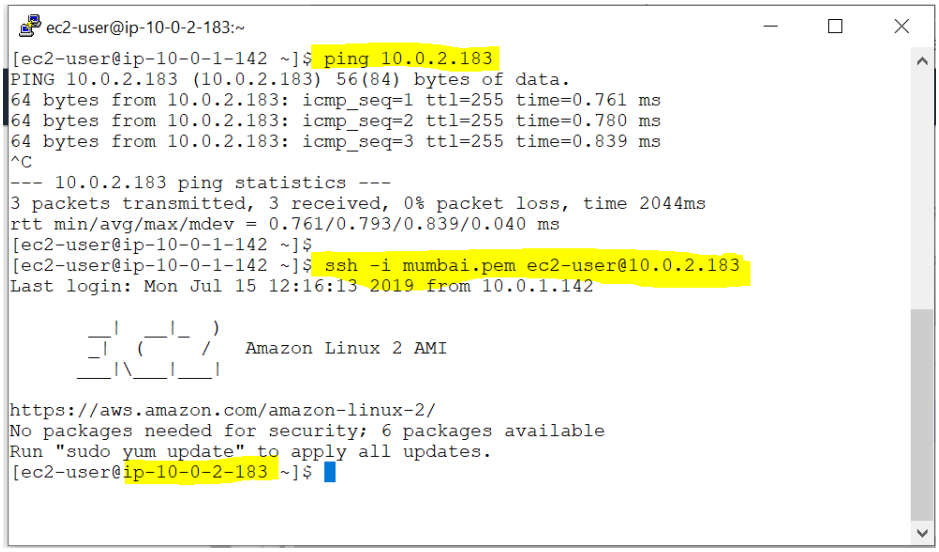
1. Create two VPC with CIDR Range 10.0.1.0/24, 10.0.2.0/24 & 10.0.3.0/24
2. Create Subnet in respective VPC with range same as VPC CIDR
3. Create two Internet Gateway and attach to respective VPC.
4. In default Route Table add the default Rule (0.0.0.0/0) and target to Internet Gateway.
5. Create Peering connections (for VPC Peering)
    a. Select the Source as VPC A and destination as VPC B
    b. Accept the Peering request
    c. Select the Source as VPC B and destination as VPC C
    d. Accept the Peering request
6. Edit Route table A and add the route to VPC B CIDR Range and target to VPC Peering
7. Edit Route table B and add the route to VPC A CIDR Range and target to VPC Peering
8. Edit Route table B and add the route to VPC C CIDR Range and target to VPC Peering
9. Edit Route table C and add the route to VPC B CIDR Range and target to VPC Peering
10. Create three EC2 instances (VM) in respective VPC.
11. Edit the default NACL of VPC A
    - Edit the inbound rule to deny login from VPC B CIDR range



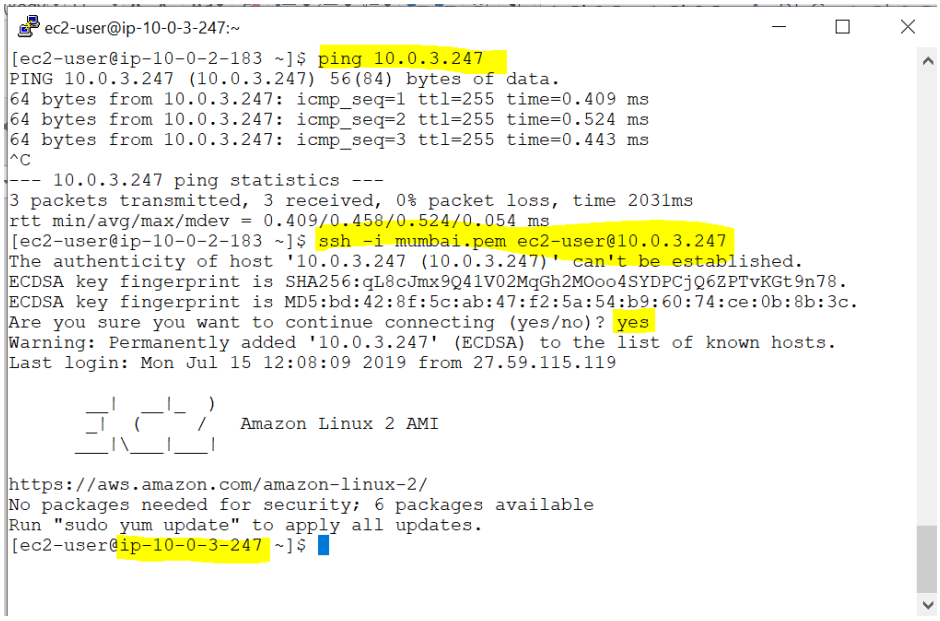
12. Edit the default NACL of VPC B
    - Edit the Inbound rule to deny from VPC C CIDR Range



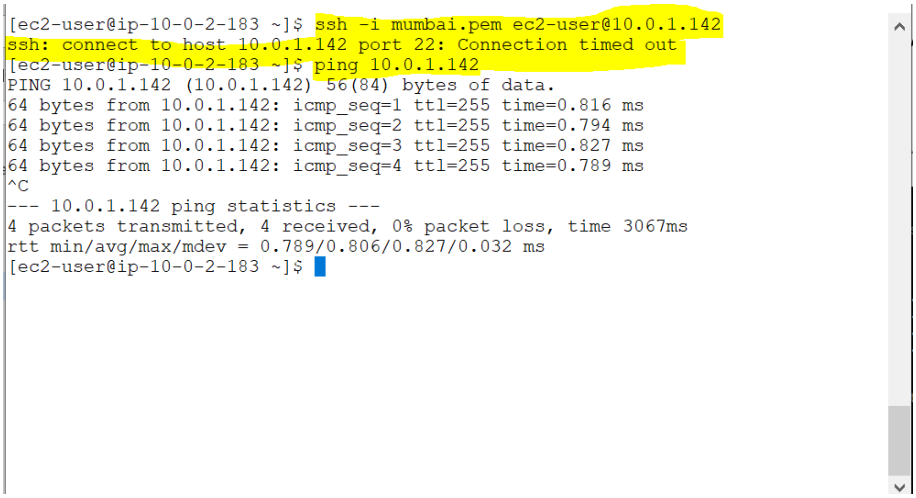
13. Login to Machine A and check if you should be able to ssh to Machine B. And Machine B to machine C.
    a. Machine A to Machine B (Successful SSH)



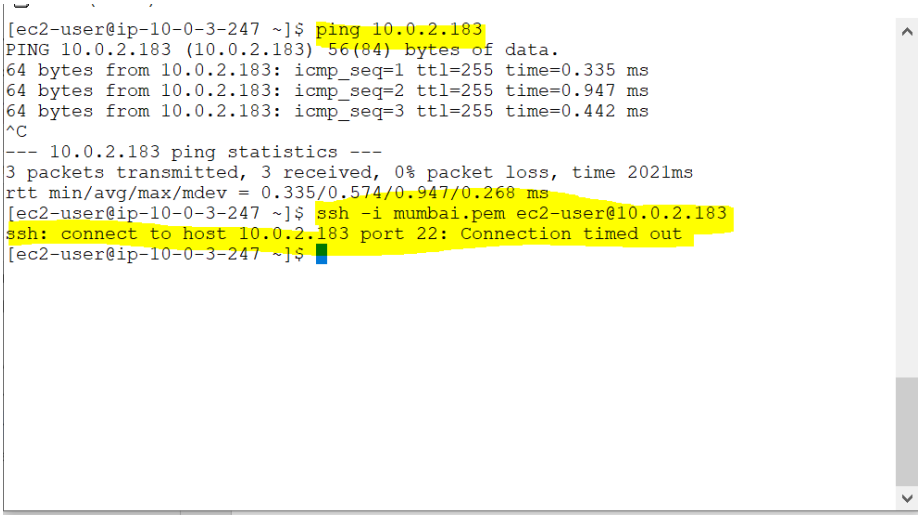
    b. Machine B to Machine C (Successful SSH)



14. SSH should not be possible from Machine B to Machine A and Machine C to machine B
    a. Machine B to Machine A (Unsuccessful SSH)



    b. Machine C to Machine B (Unsuccessful SSH)



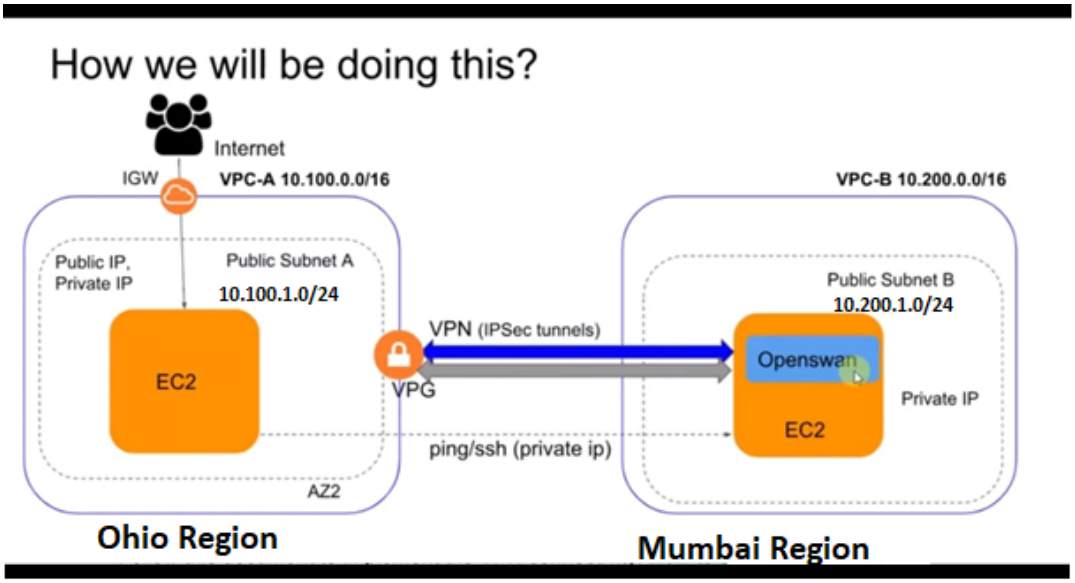
Assignment 2

Requirement:

Establish the VPN Tunneling between two data center.

Solution:

We are creating IPSec Tunneling between two VPC in different account in different region as we don't have our own data center.

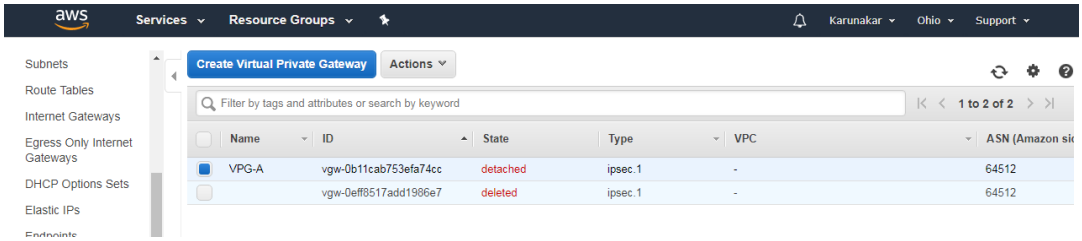


Steps to achieve this.

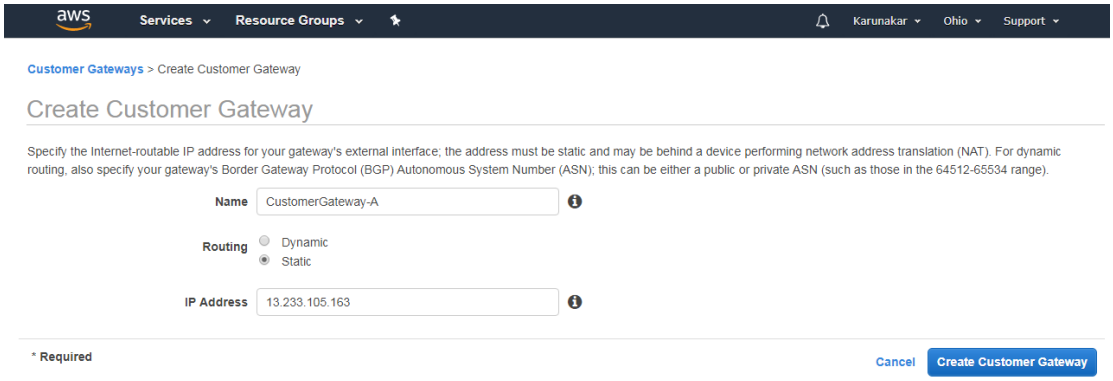
1. Create VPC A with CIDR Range 10.100.0.0/16 in First account.
2. Create Subnet A in VPC A with range 10.100.1.0/24
3. Create Internet Gateway and attach to VPC A.
4. Add the Route (0.0.0.0/0) in default Route Table and target to Internet Gateway.
5. Create VPC B with CIDR Range 10.200.0.0/16 in Second account.
6. Create Subnet B in VPC B with range 10.200.1.0/24
7. Create Internet Gateway and attach to VPC B.
8. Add the Route (0.0.0.0/0) in default Route Table and target to Internet Gateway.
9. Below steps to be executed at VPC B
    a. Launch the EC2 instance in VPC B with only Public IP enabled.
    b. Login to EC2 instance created for OpenSwan software and install as below

    [root@ip-10-200-1-88 ~]# yum install openswan -y

10. Below steps to be executed at VPC A
    a. Create the **Virtual Private Gateway** and then attach to VPC A

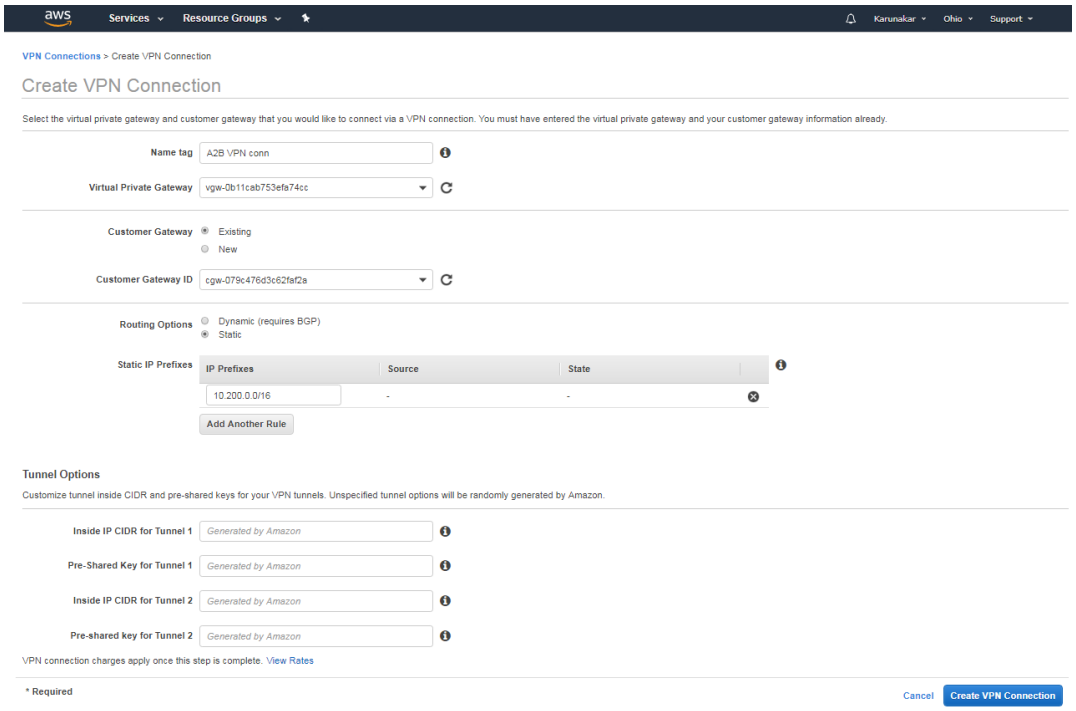


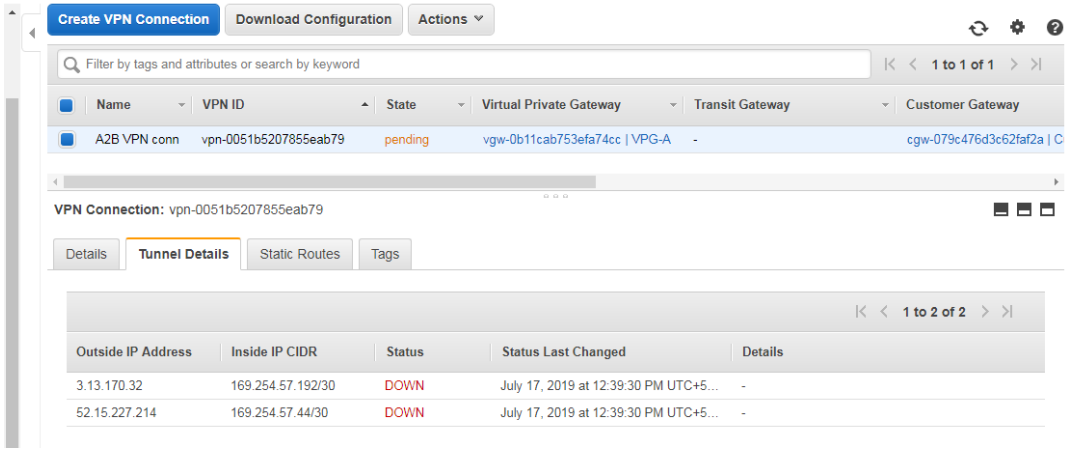
    b. Create **Customer Gateway**, Enter the Name and select Static Routing Radio button. Then Enter the Public IP address of OpenSwan Server created in VPC B.



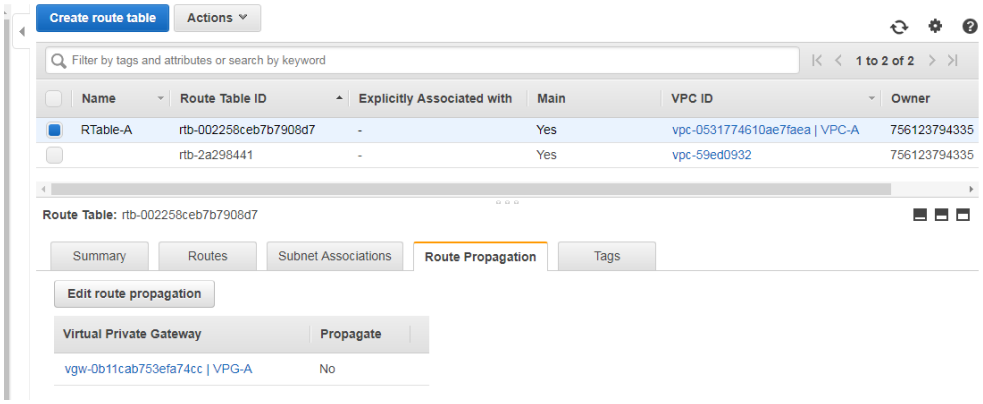
    c. Create **Site-to-Site VPN Connection**
        i. Enter Name Tag
        ii. Select Virtual Private Gateway from the dropdown
        iii. Select Customer Gateway from the drop down
        iv. Select Routing option as Static and enter the CIDR range of VPC B
        v. Keep rest of the values default and Click on **Create VPC Connection** button

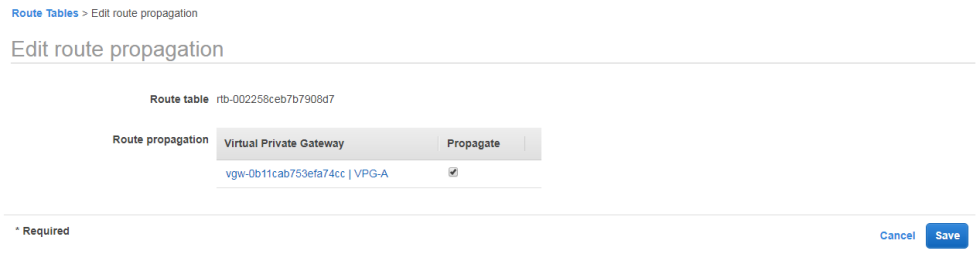
    Note: This will take few min to be active.

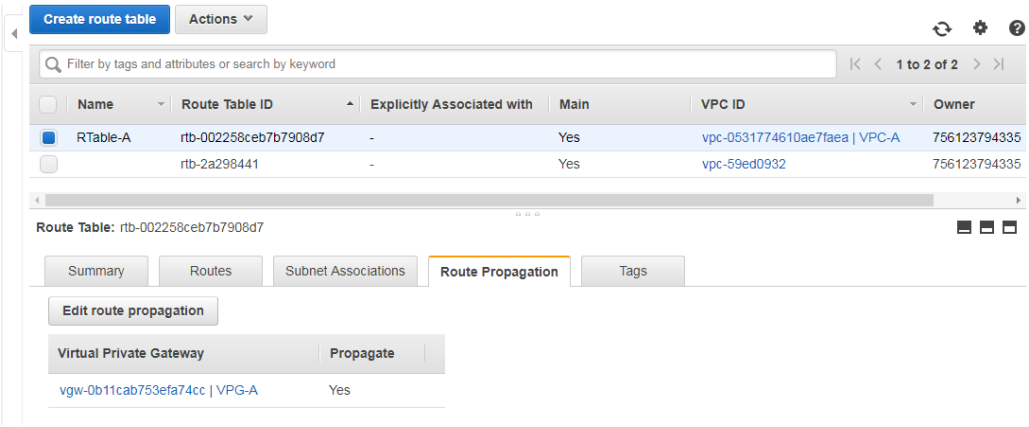




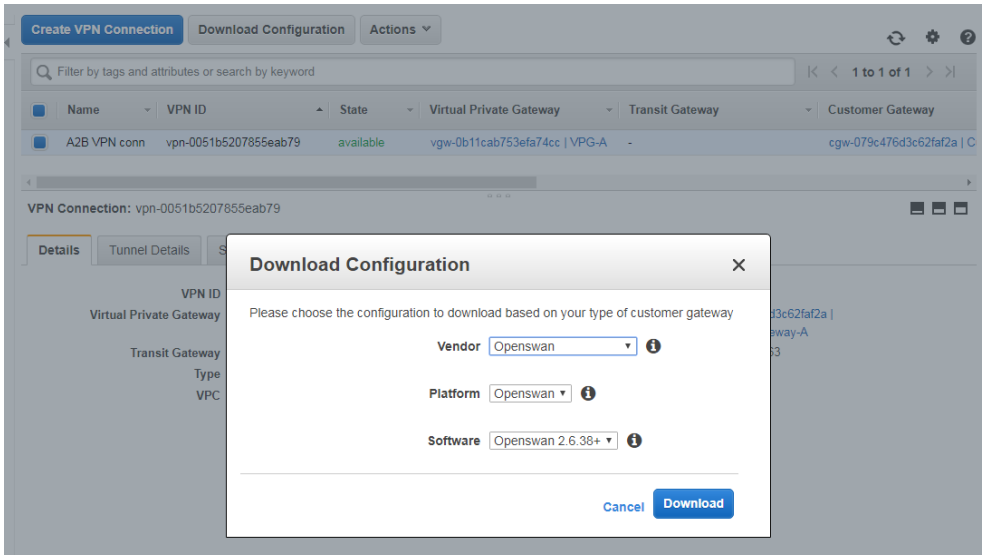
d. Go to Route table and click on Route Propagation tab
    i. Edit Route propagation button
    ii. Select the check box under Propagate and click on Save button.







e. Go back to Site to Site VPN Connection and Ensure status is available for the VPN Connection created already.
f. Select the VPN connection created and click on Download Configuration button
    i. Select Vendor as OpenSwan then click on Download button. This will download a text file into your desktop.



11. IPSec Tunnel 1 steps in the downloaded text file to be followed in OpenSwan server in VPC B
    a. Open the file /etc/sysctl.conf in edit more and add below lines then save & close the file.

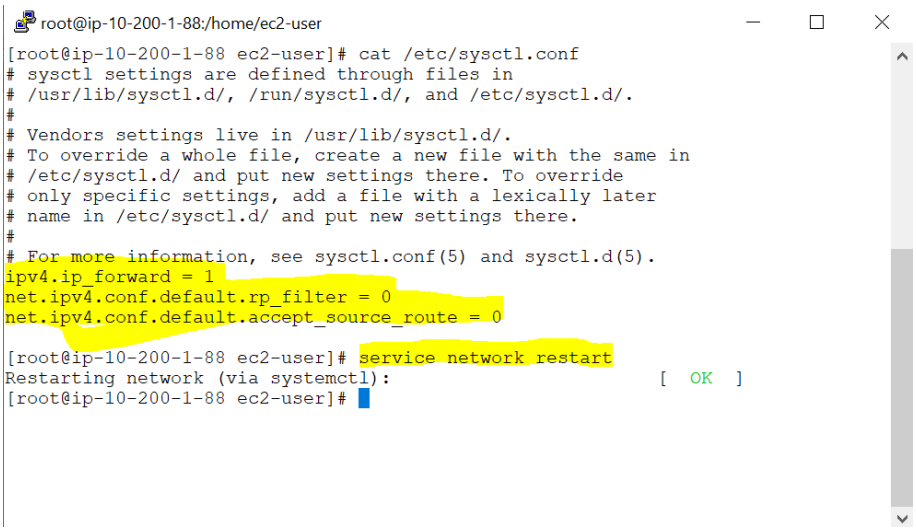
       net.ipv4.ip_forward = 1
       net.ipv4.conf.default.rp_filter = 0
       net.ipv4.conf.default.accept_source_route = 0

    b. Restart the network service as below

       service network restart

```
[root@ip-10-200-1-88 ~]# cat /etc/sysctl.conf
# sysctl settings are defined through files in
# /usr/lib/sysctl.d/, /run/sysctl.d/, and /etc/sysctl.d/.
#
# Vendors settings live in /usr/lib/sysctl.d/.
# To override a whole file, create a new file with the same in
# /etc/sysctl.d/ and put new settings there. To override
# only specific settings, add a file with a lexically later
# name in /etc/sysctl.d/ and put new settings there.
#
# For more information, see sysctl.conf(5) and sysctl.d(5).

net.ipv4.ip_forward=1
net.ipv4.conf.all.accept_redirects=0
net.ipv4.conf.all.send_redirects=0
[root@ip-10-200-1-88 ~]# service network restart
Restarting network (via systemctl):                        [  OK  ]
[root@ip-10-200-1-88 ~]#
```



c. Edit the file /etc/ipsec.conf and ensure below line is uncommented. Uncomment if not already to read the configuration files that will be created in subsequent steps.

include /etc/ipsec.d/.conf*

d. Create a new file at /etc/ipsec.d/aws.conf if doesn't already exist, and then open it. Append the following configuration to the end in the file:

#leftsubnet= is the local network behind your openswan server, and you will need to replace the <LOCAL NETWORK> below with this value (don't include the brackets). If you have multiple subnets, you can use 0.0.0.0/0 instead.

#rightsubnet= is the remote network on the other side of your VPN tunnel that you wish to have connectivity with, and you will need to replace <REMOTE NETWORK> with this value (don't include brackets).

```
conn Tunnel1
        authby=secret
        auto=start
        left=%defaultroute
        leftid=13.233.105.163
        right=3.13.170.32
        type=tunnel
        ikelifetime=8h
        keylife=1h
        phase2alg=aes128-sha1;modp1024
        ike=aes128-sha1;modp1024
        auth=esp
        keyingtries=%forever
        keyexchange=ike
        leftsubnet=10.200.0.0/16
        rightsubnet=10.100.0.0/16
        dpddelay=10
        dpdtimeout=30
        dpdaction=restart_by_peer
```

Note: Ensure you remove the line auth=esp line

Note 2: This is the IP of Customer Gateway created in VPC A. And this should not be edited as its auto populated in text file downloaded

e. Create a new file at /etc/ipsec.d/aws.secrets if it doesn't already exist, and append this line to the file (be mindful of the spacing!):
13.233.105.163 3.13.170.32: PSK "qQ0Sws_uA4VVyCVbNi6MeNsNqrFrsNo9"

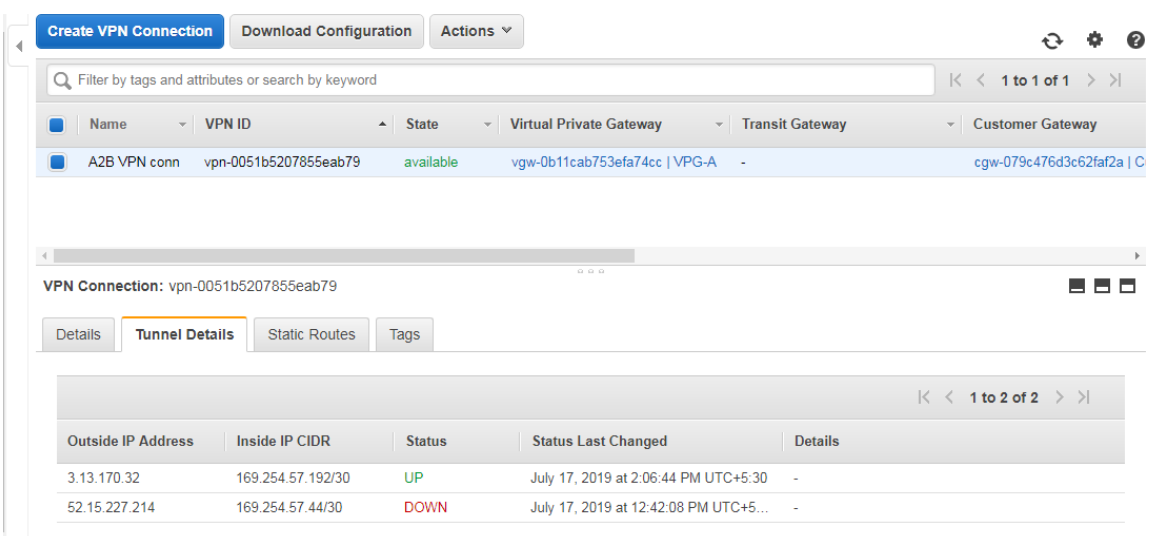
f. Restart the ipsec service

service ipsec restart

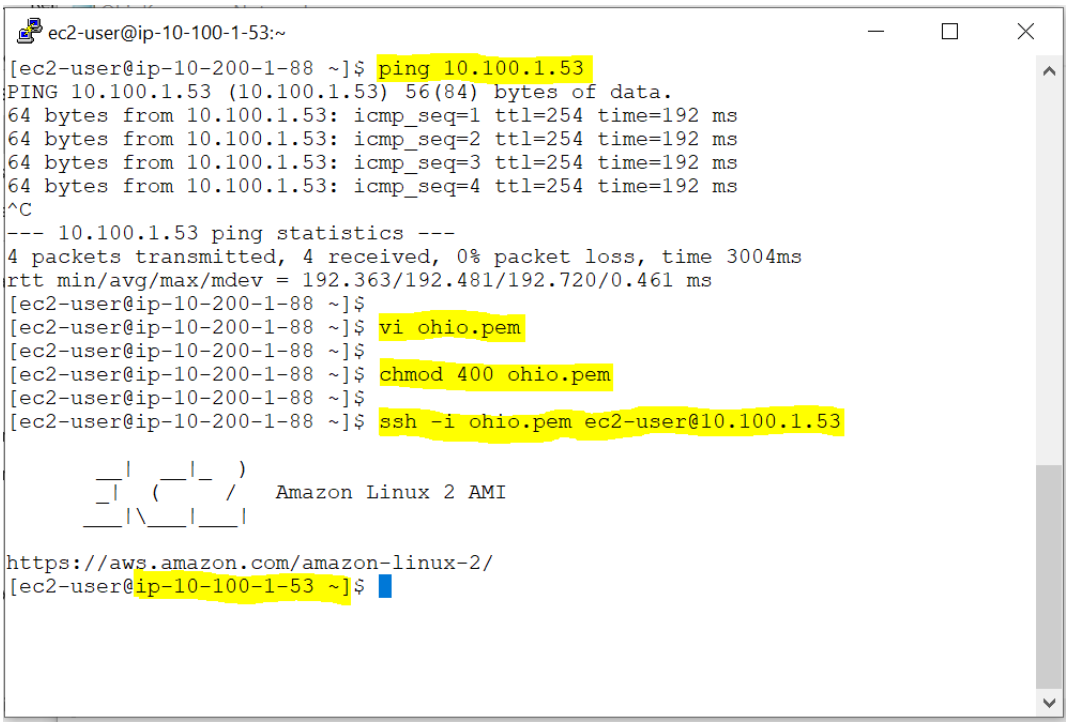
```
root@ip-10-200-1-88:/etc/ipsec.d
Redirecting to /bin/systemctl restart ipsec.service
[root@ip-10-200-1-88 ipsec.d]# service ipsec status
Redirecting to /bin/systemctl status ipsec.service
● ipsec.service - Internet Key Exchange (IKE) Protocol Daemon for IPsec
   Loaded: loaded (/usr/lib/systemd/system/ipsec.service; disabled; vendor prese
t: disabled)
   Active: active (running) since Wed 2019-07-17 08:36:11 UTC; 2min 21s ago
     Docs: man:ipsec(8)
           man:pluto(8)
           man:ipsec.conf(5)
  Process: 4687 ExecStartPre=/usr/sbin/ipsec --checknflog (code=exited, status=0
/SUCCESS)
  Process: 4681 ExecStartPre=/usr/sbin/ipsec --checknss (code=exited, status=0/S
UCCESS)
  Process: 4065 ExecStartPre=/usr/libexec/ipsec/_stackmanager start (code=exited
, status=0/SUCCESS)
  Process: 4063 ExecStartPre=/usr/libexec/ipsec/addconn --config /etc/ipsec.conf
 --checkconfig (code=exited, status=0/SUCCESS)
 Main PID: 4702 (pluto)
   Status: "Startup completed."
   CGroup: /system.slice/ipsec.service
           └─4702 /usr/libexec/ipsec/pluto --leak-detective --config /etc/ips...

Jul 17 08:36:12 ip-10-200-1-88.ap-south-1.compute.internal pluto[4702]: | set...
Jul 17 08:36:12 ip-10-200-1-88.ap-south-1.compute.internal pluto[4702]: loadi...
Jul 17 08:36:12 ip-10-200-1-88.ap-south-1.compute.internal pluto[4702]: loadi...
Jul 17 08:36:12 ip-10-200-1-88.ap-south-1.compute.internal pluto[4702]: "Tunn...
Jul 17 08:36:12 ip-10-200-1-88.ap-south-1.compute.internal pluto[4702]: "Tunn...
Jul 17 08:36:12 ip-10-200-1-88.ap-south-1.compute.internal pluto[4702]: "Tunn...
Jul 17 08:36:12 ip-10-200-1-88.ap-south-1.compute.internal pluto[4702]: "Tunn...
Jul 17 08:36:12 ip-10-200-1-88.ap-south-1.compute.internal pluto[4702]: "Tunn...
Jul 17 08:36:12 ip-10-200-1-88.ap-south-1.compute.internal pluto[4702]: "Tunn...
Jul 17 08:36:13 ip-10-200-1-88.ap-south-1.compute.internal pluto[4702]: "Tunn...
Hint: Some lines were ellipsized, use -l to show in full.
```

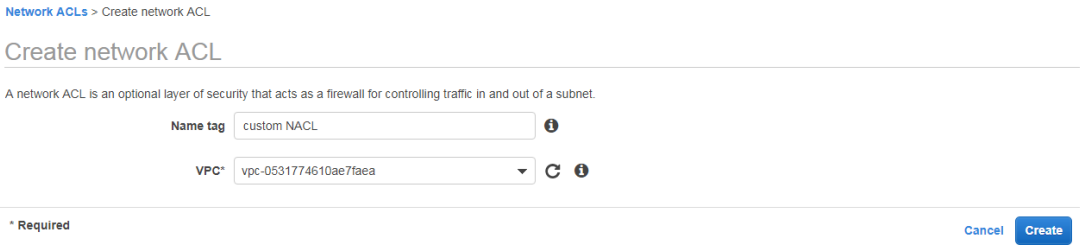
12. Navigate to **Site-to-Site VPN Connection** in VPC A and check the status under **Tunnel Details**.



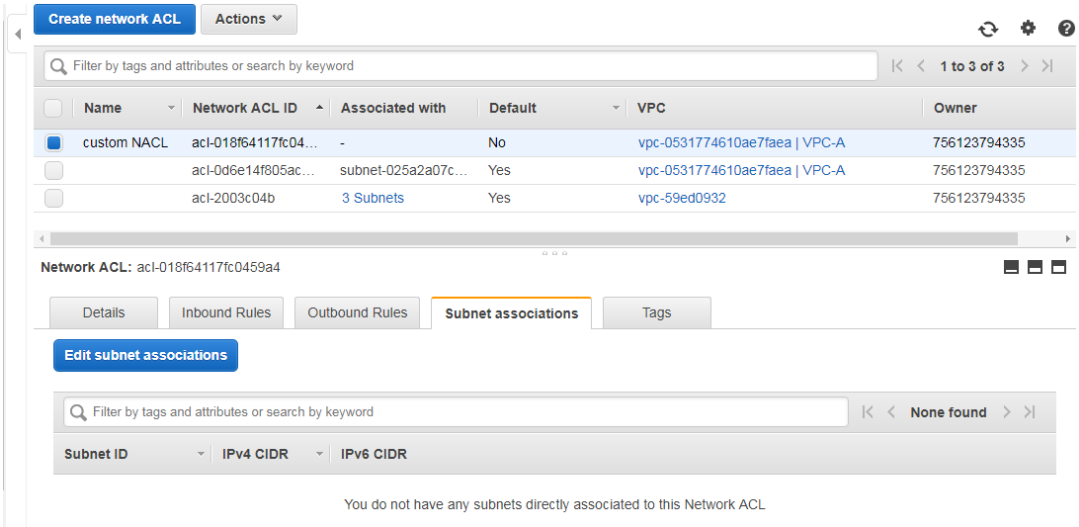
13. Login to OpenSwan Server and ping the Private IP of EC2 instance in VPC A

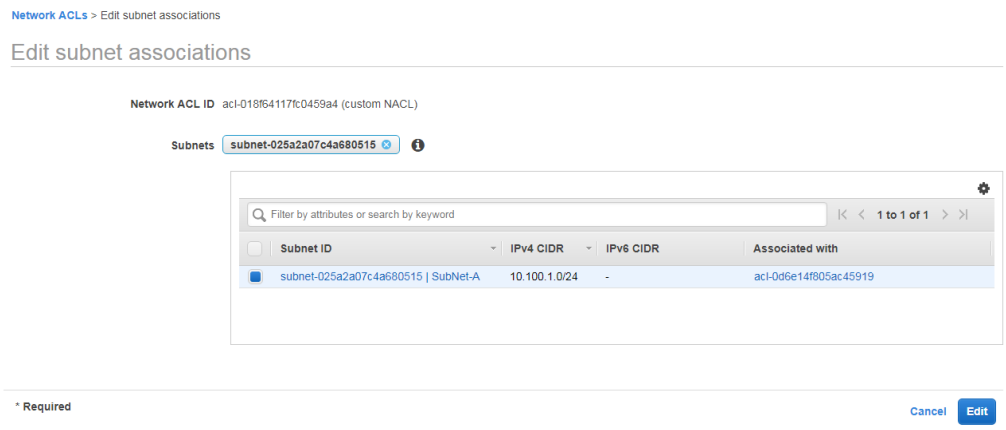


14. Create Custom NACL in VPC A and Navigate to Subnet association tab

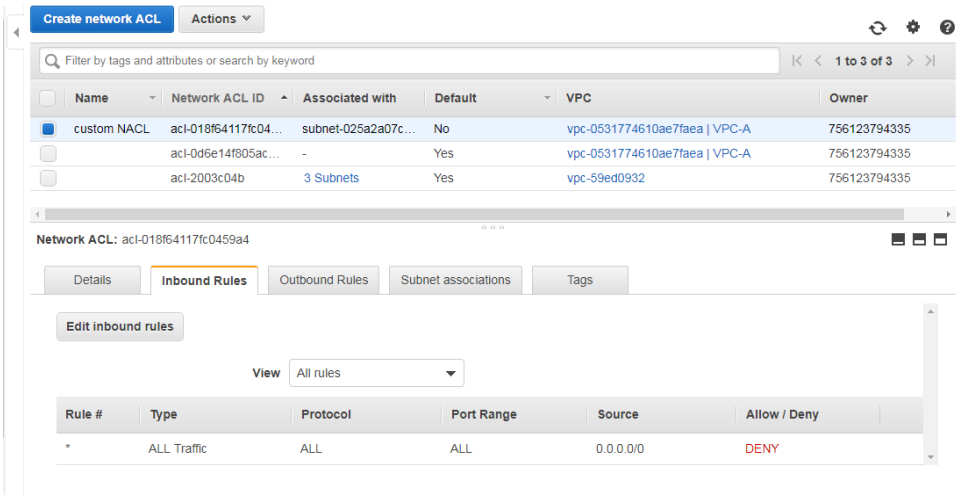


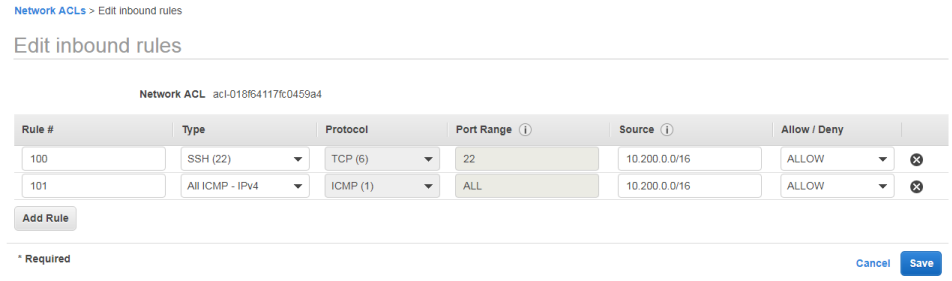
15. Click on Edit Subnet Association and select the SubNetB



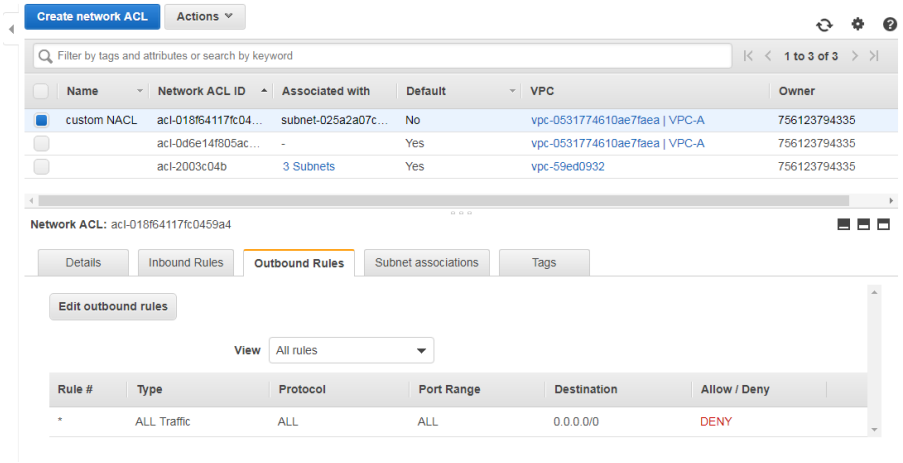


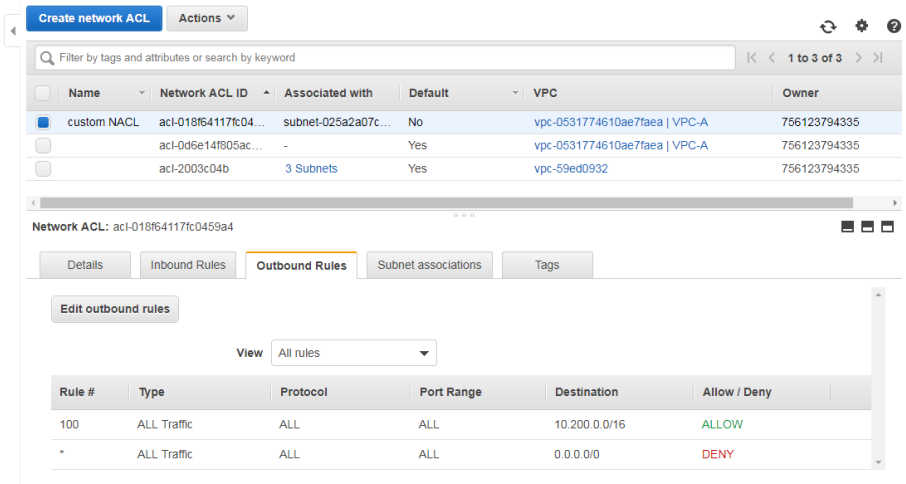
16. Add the Inbound rules to allow ssh and ping from VPC B CIDR Range.





17. Add the Outbound Rules to allow ALL IP range.





Note 1: Default or Custom NACL can have multiple SubNet. However, Subnet can be mapped only one NACL. Default its mapped to Default NACL. You will have to associate required subnet to Custom NACL.

Note 2: By default, everything is blocked in Custom NACL. We must add the rule either to Allow or Deny

Note 3: Lower the Rule Number higher the precedence.

i.e Rule # 99 will take the precedence over Rule # 100