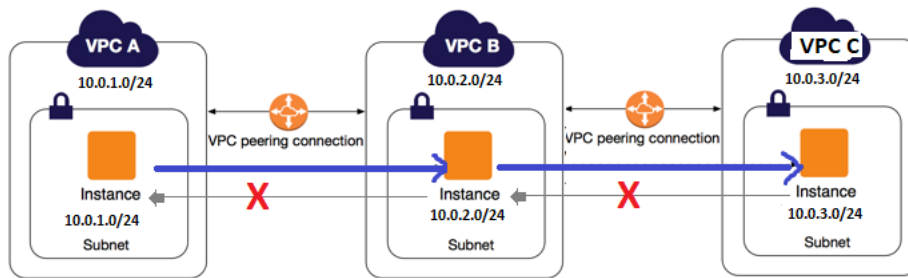


Assignment 1

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

Edit inbound rules

Network ACL acl-08af42561d6777d63

Rule #	Type	Protocol	Port Range ⓘ	Source ⓘ	Allow / Deny	
99	SSH (22) ▼	TCP (6) ▼	22	10.0.2.0/24	DENY ▼	✕
100	ALL Traffic ▼	ALL ▼	ALL	0.0.0.0/0	ALLOW ▼	✕

Add Rule

* Required

Cancel Save

12. Edit the default NACL of VPC B

- Edit the Inbound rule to deny from VPC C CIDR Range

Edit inbound rules

Network ACL acl-0202730b4edb327d8

Rule #	Type	Protocol	Port Range ⓘ	Source ⓘ	Allow / Deny	
99	SSH (22) ▼	TCP (6) ▼	22	10.0.3.0/24	DENY ▼	✕
100	ALL Traffic ▼	ALL ▼	ALL	0.0.0.0/0	ALLOW ▼	✕

Add Rule

* Required

Cancel Save

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)

```
ec2-user@ip-10-0-2-183:~  
[ec2-user@ip-10-0-1-142 ~]$ ping 10.0.2.183  
PING 10.0.2.183 (10.0.2.183) 56(84) bytes of data.  
64 bytes from 10.0.2.183: icmp_seq=1 ttl=255 time=0.761 ms  
64 bytes from 10.0.2.183: icmp_seq=2 ttl=255 time=0.780 ms  
64 bytes from 10.0.2.183: icmp_seq=3 ttl=255 time=0.839 ms  
^C  
--- 10.0.2.183 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2044ms  
rtt min/avg/max/mdev = 0.761/0.793/0.839/0.040 ms  
[ec2-user@ip-10-0-1-142 ~]$  
[ec2-user@ip-10-0-1-142 ~]$ ssh -i mumbai.pem ec2-user@10.0.2.183  
Last login: Mon Jul 15 12:16:13 2019 from 10.0.1.142  
  
 _ | _ | _ )  
 _ | ( _ | /  Amazon Linux 2 AMI  
 _ | \ _ | _ |  
  
https://aws.amazon.com/amazon-linux-2/  
No packages needed for security; 6 packages available  
Run "sudo yum update" to apply all updates.  
[ec2-user@ip-10-0-2-183 ~]$
```

b. Machine B to Machine C (Successful SSH)

```
ec2-user@ip-10-0-3-247:~  
[ec2-user@ip-10-0-2-183 ~]$ ping 10.0.3.247  
PING 10.0.3.247 (10.0.3.247) 56(84) bytes of data.  
64 bytes from 10.0.3.247: icmp_seq=1 ttl=255 time=0.409 ms  
64 bytes from 10.0.3.247: icmp_seq=2 ttl=255 time=0.524 ms  
64 bytes from 10.0.3.247: icmp_seq=3 ttl=255 time=0.443 ms  
^C  
--- 10.0.3.247 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2031ms  
rtt min/avg/max/mdev = 0.409/0.458/0.524/0.054 ms  
[ec2-user@ip-10-0-2-183 ~]$ ssh -i mumbai.pem ec2-user@10.0.3.247  
The authenticity of host '10.0.3.247 (10.0.3.247)' can't be established.  
ECDSA key fingerprint is SHA256:qL8cJmx9Q41V02MqGh2M0oo4SYDPCjQ6ZPTvKGT9n78.  
ECDSA key fingerprint is MD5:bd:42:8f:5c:ab:47:f2:5a:54:b9:60:74:ce:0b:8b:3c.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '10.0.3.247' (ECDSA) to the list of known hosts.  
Last login: Mon Jul 15 12:08:09 2019 from 27.59.115.119  
  
 _ | _ | _ )  
 _ | ( _ | /  Amazon Linux 2 AMI  
 _ | \ _ | _ |  
  
https://aws.amazon.com/amazon-linux-2/  
No packages needed for security; 6 packages available  
Run "sudo yum update" to apply all updates.  
[ec2-user@ip-10-0-3-247 ~]$
```

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)

```
[ec2-user@ip-10-0-2-183 ~]$ ssh -i mumbai.pem ec2-user@10.0.1.142
ssh: connect to host 10.0.1.142 port 22: Connection timed out
[ec2-user@ip-10-0-2-183 ~]$ ping 10.0.1.142
PING 10.0.1.142 (10.0.1.142) 56(84) bytes of data.
64 bytes from 10.0.1.142: icmp_seq=1 ttl=255 time=0.816 ms
64 bytes from 10.0.1.142: icmp_seq=2 ttl=255 time=0.794 ms
64 bytes from 10.0.1.142: icmp_seq=3 ttl=255 time=0.827 ms
64 bytes from 10.0.1.142: icmp_seq=4 ttl=255 time=0.789 ms
^C
--- 10.0.1.142 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3067ms
rtt min/avg/max/mdev = 0.789/0.806/0.827/0.032 ms
[ec2-user@ip-10-0-2-183 ~]$
```

b. Machine C to Machine B (Unsuccessful SSH)

```
[ec2-user@ip-10-0-3-247 ~]$ ping 10.0.2.183
PING 10.0.2.183 (10.0.2.183) 56(84) bytes of data.
64 bytes from 10.0.2.183: icmp_seq=1 ttl=255 time=0.335 ms
64 bytes from 10.0.2.183: icmp_seq=2 ttl=255 time=0.947 ms
64 bytes from 10.0.2.183: icmp_seq=3 ttl=255 time=0.442 ms
^C
--- 10.0.2.183 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2021ms
rtt min/avg/max/mdev = 0.335/0.574/0.947/0.268 ms
[ec2-user@ip-10-0-3-247 ~]$ ssh -i mumbai.pem ec2-user@10.0.2.183
ssh: connect to host 10.0.2.183 port 22: Connection timed out
[ec2-user@ip-10-0-3-247 ~]$
```

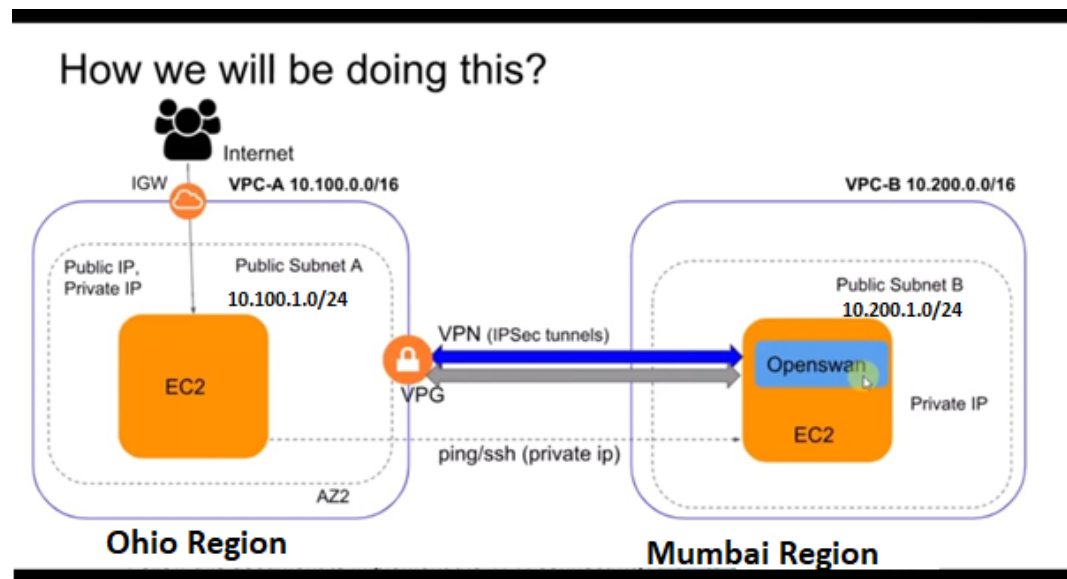
Assignment 2

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

Virtual Private Gateways > Create Virtual Private Gateway

Create Virtual Private Gateway

A virtual private gateway is the router on the Amazon side of the VPN tunnel.

Name tag

ASN ☒ Amazon default ASN ☐ Custom ASN

* Required

Cancel **Create Virtual Private Gateway**

Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints

Create Virtual Private Gateway Actions

Filter by tags and attributes or search by keyword

	Name	ID	State	Type	VPC	ASN (Amazon s
<input checked="" type="checkbox"/>	VPG-A	vgw-0b11cab753efa74cc	detached	ipsec.1	-	64512
<input type="checkbox"/>		vgw-0eff0517add1906e7	deleted	ipsec.1	-	64512

- 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.

Customer Gateways > Create Customer Gateway

Create Customer Gateway

Specify the Internet-routable IP address for your gateway's external interface; the address must be static and may be behind a device performing network address translation (NAT). For dynamic routing, also specify your gateway's Border Gateway Protocol (BGP) Autonomous System Number (ASN); this can be either a public or private ASN (such as those in the 64512-65534 range).

Name

Routing ☐ Dynamic ☒ Static

IP Address

* Required

Cancel **Create Customer Gateway**

- 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.

aws Services Resource Groups

VPN Connections > Create VPN Connection

Create VPN Connection

Select the virtual private gateway and customer gateway that you would like to connect via a VPN connection. You must have entered the virtual private gateway and your customer gateway information already.

Name tag: A2B VPN conn

Virtual Private Gateway: vgw-0b11cab753efa74cc

Customer Gateway: Existing

Customer Gateway ID: cgw-079c476d3c62faf2a

Routing Options: Static

Static IP Prefixes:

IP Prefixes	Source	State
10.200.0.0/16	-	-

Add Another Rule

Tunnel Options

Customize tunnel inside CIDR and pre-shared keys for your VPN tunnels. Unspecified tunnel options will be randomly generated by Amazon.

Inside IP CIDR for Tunnel 1: Generated by Amazon

Pre-Shared Key for Tunnel 1: Generated by Amazon

Inside IP CIDR for Tunnel 2: Generated by Amazon

Pre-shared key for Tunnel 2: Generated by Amazon

VPN connection charges apply once this step is complete. [View Rates](#)

* Required

Cancel Create VPN Connection

Create VPN Connection Download Configuration Actions

Filter by tags and attributes or search by keyword

Name	VPN ID	State	Virtual Private Gateway	Transit Gateway	Customer Gateway
A2B VPN conn	vpn-0051b5207855eab79	pending	vgw-0b11cab753efa74cc VPG-A	-	cgw-079c476d3c62faf2a C

VPN Connection: vpn-0051b5207855eab79

Details Tunnel Details Static Routes Tags

Outside IP Address	Inside IP CIDR	Status	Status Last Changed	Details
3.13.170.32	169.254.57.192/30	DOWN	July 17, 2019 at 12:39:30 PM UTC+5...	-
52.15.227.214	169.254.57.44/30	DOWN	July 17, 2019 at 12:39:30 PM UTC+5...	-

- 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.

Create route table **Actions** ↻ ⚙ ?

Filter by tags and attributes or search by keyword 1 to 2 of 2

<input type="checkbox"/>	Name	Route Table ID	Explicitly Associated with	Main	VPC ID	Owner
<input checked="" type="checkbox"/>	RTable-A	rtb-002258ceb7b7908d7	-	Yes	vpc-0531774610ae7faea VPC-A	756123794335
<input type="checkbox"/>		rtb-2a298441	-	Yes	vpc-59ed0932	756123794335

Route Table: rtb-002258ceb7b7908d7 📄 📄 📄

Summary **Routes** **Subnet Associations** **Route Propagation** **Tags**

Edit route propagation

Virtual Private Gateway	Propagate
vgw-0b11cab753efa74cc VPG-A	No

[Route Tables](#) > Edit route propagation

Edit route propagation

Route table rtb-002258ceb7b7908d7

Route propagation

Virtual Private Gateway	Propagate
vgw-0b11cab753efa74cc VPG-A	<input checked="" type="checkbox"/>

* Required Cancel Save

Create route table **Actions** ↻ ⚙ ?

Filter by tags and attributes or search by keyword 1 to 2 of 2

<input type="checkbox"/>	Name	Route Table ID	Explicitly Associated with	Main	VPC ID	Owner
<input checked="" type="checkbox"/>	RTable-A	rtb-002258ceb7b7908d7	-	Yes	vpc-0531774610ae7faea VPC-A	756123794335
<input type="checkbox"/>		rtb-2a298441	-	Yes	vpc-59ed0932	756123794335

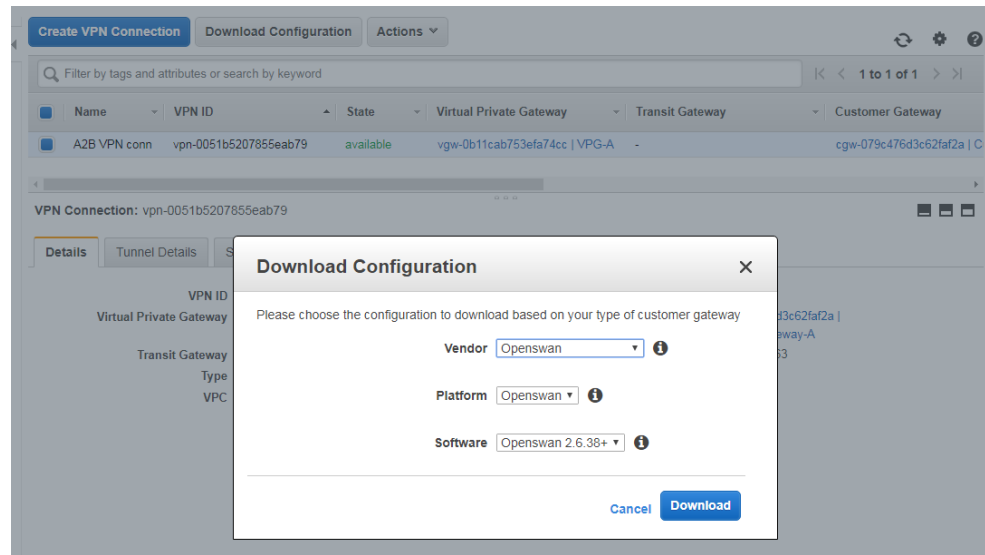
Route Table: rtb-002258ceb7b7908d7 📄 📄 📄

Summary **Routes** **Subnet Associations** **Route Propagation** **Tags**

Edit route propagation

Virtual Private Gateway	Propagate
vgw-0b11cab753efa74cc VPG-A	Yes

- 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):
[root@ip-10-200-1-88 ~]# [ OK ]
```

```
root@ip-10-200-1-88:/home/ec2-user
[root@ip-10-200-1-88 ec2-user]# 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).
ipv4.ip_forward = 1
net.ipv4.conf.default.rp_filter = 0
net.ipv4.conf.default.accept_source_route = 0

[root@ip-10-200-1-88 ec2-user]# service network restart
Restarting network (via systemctl): [ OK ]
[root@ip-10-200-1-88 ec2-user]#
```

- 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 --checknflag (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**.

VPN Connection: vpn-0051b5207855eab79

Details | **Tunnel Details** | Static Routes | Tags

Outside IP Address	Inside IP CIDR	Status	Status Last Changed	Details
3.13.170.32	169.254.57.192/30	UP	July 17, 2019 at 2:06:44 PM UTC+5:30	-
52.15.227.214	169.254.57.44/30	DOWN	July 17, 2019 at 12:42:08 PM UTC+5:30	-

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

```
ec2-user@ip-10-100-1-53:~  
[ec2-user@ip-10-200-1-88 ~]$ ping 10.100.1.53  
PING 10.100.1.53 (10.100.1.53) 56(84) bytes of data.  
64 bytes from 10.100.1.53: icmp_seq=1 ttl=254 time=192 ms  
64 bytes from 10.100.1.53: icmp_seq=2 ttl=254 time=192 ms  
64 bytes from 10.100.1.53: icmp_seq=3 ttl=254 time=192 ms  
64 bytes from 10.100.1.53: icmp_seq=4 ttl=254 time=192 ms  
^C  
--- 10.100.1.53 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3004ms  
rtt min/avg/max/mdev = 192.363/192.481/192.720/0.461 ms  
[ec2-user@ip-10-200-1-88 ~]$  
[ec2-user@ip-10-200-1-88 ~]$ vi ohio.pem  
[ec2-user@ip-10-200-1-88 ~]$  
[ec2-user@ip-10-200-1-88 ~]$ chmod 400 ohio.pem  
[ec2-user@ip-10-200-1-88 ~]$  
[ec2-user@ip-10-200-1-88 ~]$ ssh -i ohio.pem ec2-user@10.100.1.53  
  
 _ _ | _ _ | _ _ )  
 _ | ( _ _ | / Amazon Linux 2 AMI  
 _ | \ _ _ | _ _ |  
  
https://aws.amazon.com/amazon-linux-2/  
[ec2-user@ip-10-100-1-53 ~]$
```

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

Network ACLs > Create network ACL

Create network ACL

A network ACL is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet.

Name tag ⓘ

VPC* ↕ ⓘ

* Required

Cancel Create

15. Click on Edit Subnet Association and select the SubNetB

[Create network ACL](#) [Actions](#)

1 to 3 of 3

<input type="checkbox"/>	Name	Network ACL ID	Associated with	Default	VPC	Owner
<input checked="" type="checkbox"/>	custom NACL	acl-018f64117fc04...	-	No	vpc-0531774610ae7faea VPC-A	756123794335
<input type="checkbox"/>		acl-0d6e14f805ac...	subnet-025a2a07c...	Yes	vpc-0531774610ae7faea VPC-A	756123794335
<input type="checkbox"/>		acl-2003c04b	3 Subnets	Yes	vpc-59ed0932	756123794335

Network ACL: acl-018f64117fc0459a4

[Details](#) [Inbound Rules](#) [Outbound Rules](#) [Subnet associations](#) [Tags](#)

[Edit subnet associations](#)

None found

Subnet ID	IPv4 CIDR	IPv6 CIDR
-----------	-----------	-----------

You do not have any subnets directly associated to this Network ACL

Network ACLs > Edit subnet associations

Edit subnet associations

Network ACL ID: aci-018f64117fc0459a4 (custom NACL)

Subnets: subnet-025a2a07c4a680515 ⓘ

Filter by attributes or search by keyword				< < 1 to 1 of 1 > >	
<input type="checkbox"/> Subnet ID	IPV4 CIDR	IPV6 CIDR	Associated with		
<input checked="" type="checkbox"/> subnet-025a2a07c4a680515 SubNet-A	10.100.1.0/24	-	aci-0d6e14f805ac45919		

* Required

Cancel Edit

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

Create network ACL Actions

Filter by tags and attributes or search by keyword < < 1 to 3 of 3 > >

<input type="checkbox"/>	Name	Network ACL ID	Associated with	Default	VPC	Owner
<input checked="" type="checkbox"/>	custom NACL	aci-018f64117fc04...	subnet-025a2a07c...	No	vpc-0531774610ae7faea VPC-A	756123794335
<input type="checkbox"/>		aci-0d6e14f805ac...	-	Yes	vpc-0531774610ae7faea VPC-A	756123794335
<input type="checkbox"/>		aci-2003c04b	3 Subnets	Yes	vpc-59ed0932	756123794335

Network ACL: aci-018f64117fc0459a4

Details Inbound Rules Outbound Rules Subnet associations Tags

Edit inbound rules

View All rules

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Network ACLs > Edit inbound rules

Edit inbound rules

Network ACL: aci-018f64117fc0459a4

Rule #	Type	Protocol	Port Range ①	Source ①	Allow / Deny
100	SSH (22)	TCP (6)	22	10.200.0.0/16	ALLOW
101	All ICMP - IPv4	ICMP (1)	ALL	10.200.0.0/16	ALLOW

Add Rule

* Required

Cancel Save

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

Create network ACL Actions

Filter by tags and attributes or search by keyword

Name	Network ACL ID	Associated with	Default	VPC	Owner
custom NACL	acl-018f64117fc04...	subnet-025a2a07c...	No	vpc-0531774610ae7faea VPC-A	756123794335
	acl-0d6e14f805ac...	-	Yes	vpc-0531774610ae7faea VPC-A	756123794335
	acl-2003c04b	3 Subnets	Yes	vpc-59ed0932	756123794335

Network ACL: acl-018f64117fc0459a4

Details Inbound Rules Outbound Rules Subnet associations Tags

Edit outbound rules

View All rules

Rule #	Type	Protocol	Port Range	Destination	Allow / Deny
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Create network ACL Actions

Filter by tags and attributes or search by keyword

Name	Network ACL ID	Associated with	Default	VPC	Owner
custom NACL	acl-018f64117fc04...	subnet-025a2a07c...	No	vpc-0531774610ae7faea VPC-A	756123794335
	acl-0d6e14f805ac...	-	Yes	vpc-0531774610ae7faea VPC-A	756123794335
	acl-2003c04b	3 Subnets	Yes	vpc-59ed0932	756123794335

Network ACL: acl-018f64117fc0459a4

Details Inbound Rules Outbound Rules Subnet associations Tags

Edit outbound rules

View All rules

Rule #	Type	Protocol	Port Range	Destination	Allow / Deny
100	ALL Traffic	ALL	ALL	10.200.0.0/16	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

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