amazon
web services

AWS Certified Solutions Architect Professional

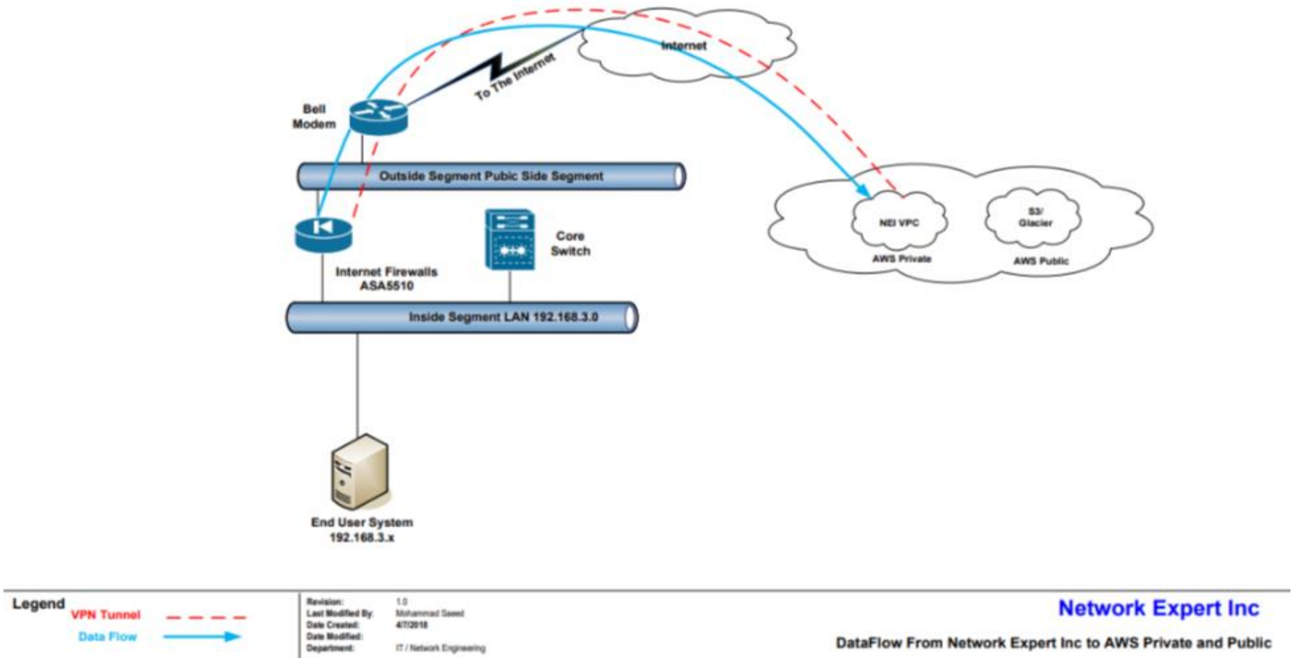
Student’s Lab Manual

Developed by: Network Expert Inc.

Table of Contents

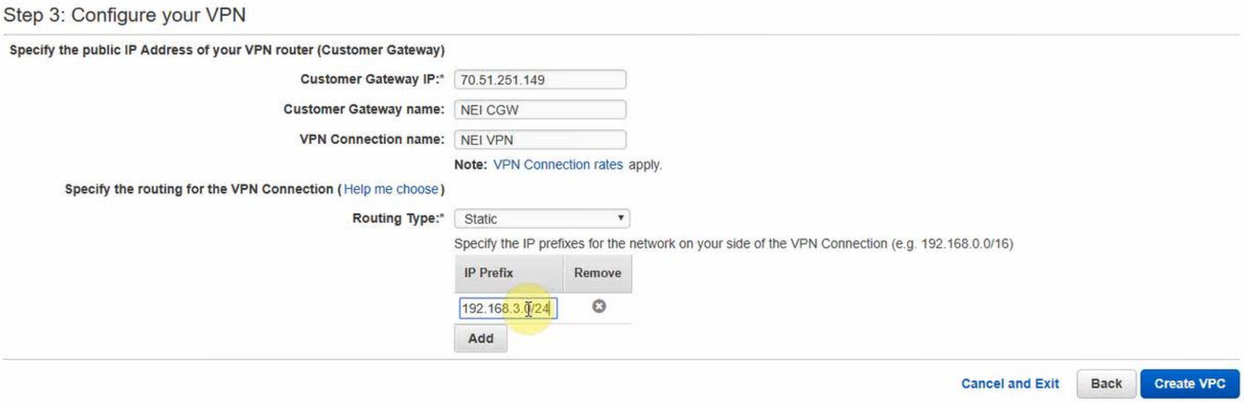
Lab 4.1: Connecting Your Data Center to VPC via VPN

1. Go to aws.amazon.com/console/. Login to AWS Management console.
2. Choose any AWS region from the top right of the console.
3. In this exercise we will be creating a VPN tunnel from out Data Center to AWS.


Internet
To The Internet
Bell Modem
Outside Segment Pubic Side Segment
Internet Firewalls ASA5510
Core Switch
Inside Segment LAN 192.168.3.0
End User System 192.168.3.x
NEI VPC
AWS Private
S3/ Glacier
AWS Public
Legend
VPN Tunnel
Data Flow
Revision: 1.0
Last Modified By: Mohammad Saeed
Date Created: 4/7/2018
Date Modified:
Department: IT / Network Engineering
Network Expert Inc
DataFlow From Network Expert Inc to AWS Private and Public

4. Look under AWS services, under network and content delivery, choose **VPC**.
5. While at the VPC dashboard, click **create VPC**.
6. For VPC configuration, select the VPC with Public and Private Subnets and Hardware VPN Access.
7. For the top level IPv4 CIDR block you can give **172.20.0.0/16** and give an appropriate VPC name.
8. For the public subnet’s IPv4 CIDR block, give **172.20.1.0/24** and for the private subnet’s IPv4 CIDR block you can give **172.20.2.0/24**.
9. Leave all other settings and preferences as is. Click **next**.
10. You will be asked for your Customer Gateway IP. This is the IP of your VPN terminating device in your data center. In our case it was the CISCO ASA firewall. Go ahead and check the public IP of your device and paste it here.

11. Give an appropriate Customer Gateway name and VPN Connection name.
12. Change the routing type to static. Under IP prefix give the private subnet of your datacenter.



Step 3: Configure your VPN

Specify the public IP Address of your VPN router (Customer Gateway)

Customer Gateway IP:* 70.51.251.149

Customer Gateway name: NEI CGW

VPN Connection name: NEI VPN

Note: VPN Connection rates apply.

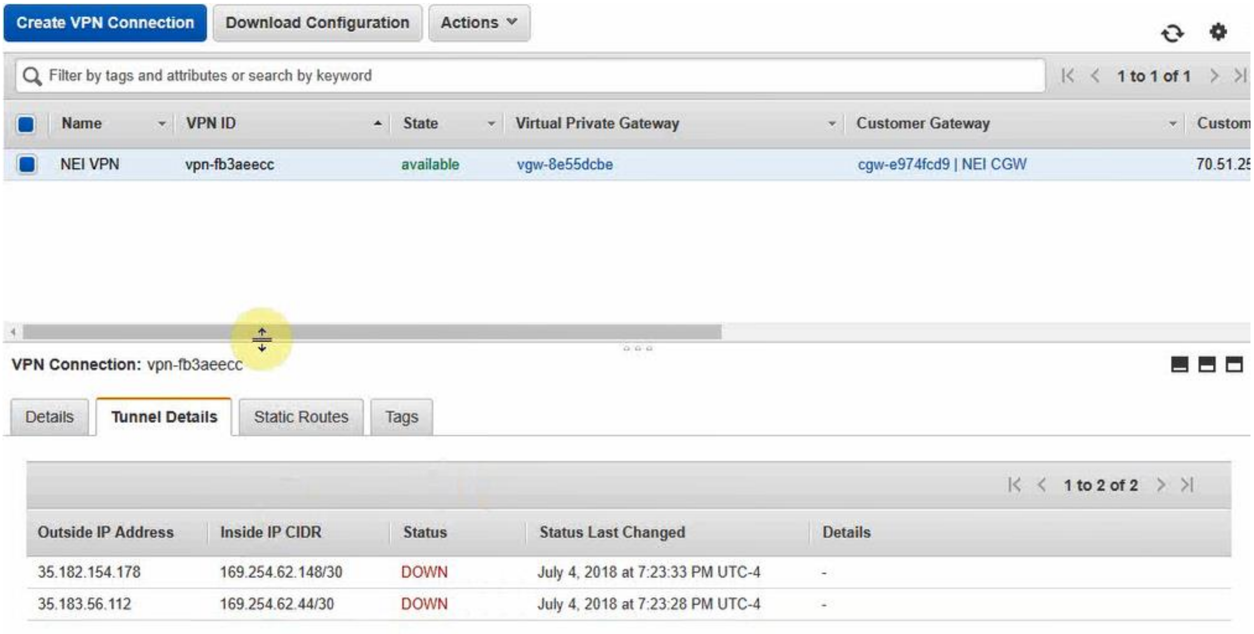
Specify the routing for the VPN Connection (Help me choose)

Routing Type:* Static

Specify the IP prefixes for the network on your side of the VPN Connection (e.g. 192.168.0.0/16)

IP Prefix	Remove
192.168.3.0/24	⊗

13. Click **create VPC**. This will take a few minutes.
14. Once your VPC has been successfully created, you can go ahead and scroll down from the navigation panel on the left, navigate to Customer Gateways, Virtual Private Gateways, and VPN connections and see that all these resources have been created for you.
15. Head over to VPN connections from the navigation panel, choose your VPN go to **tunnel details** and you will see that 2 tunnels have been created which are both down.



Name	VPN ID	State	Virtual Private Gateway	Customer Gateway	Custom
NEI VPN	vpn-fb3aeecc	available	vgw-8e55dcbe	cgw-e974fcd9 | NEI CGW	70.51.25

VPN Connection: vpn-fb3aeecc

Outside IP Address	Inside IP CIDR	Status	Status Last Changed	Details
35.182.154.178	169.254.62.148/30	DOWN	July 4, 2018 at 7:23:33 PM UTC-4	-
35.183.56.112	169.254.62.44/30	DOWN	July 4, 2018 at 7:23:28 PM UTC-4	-

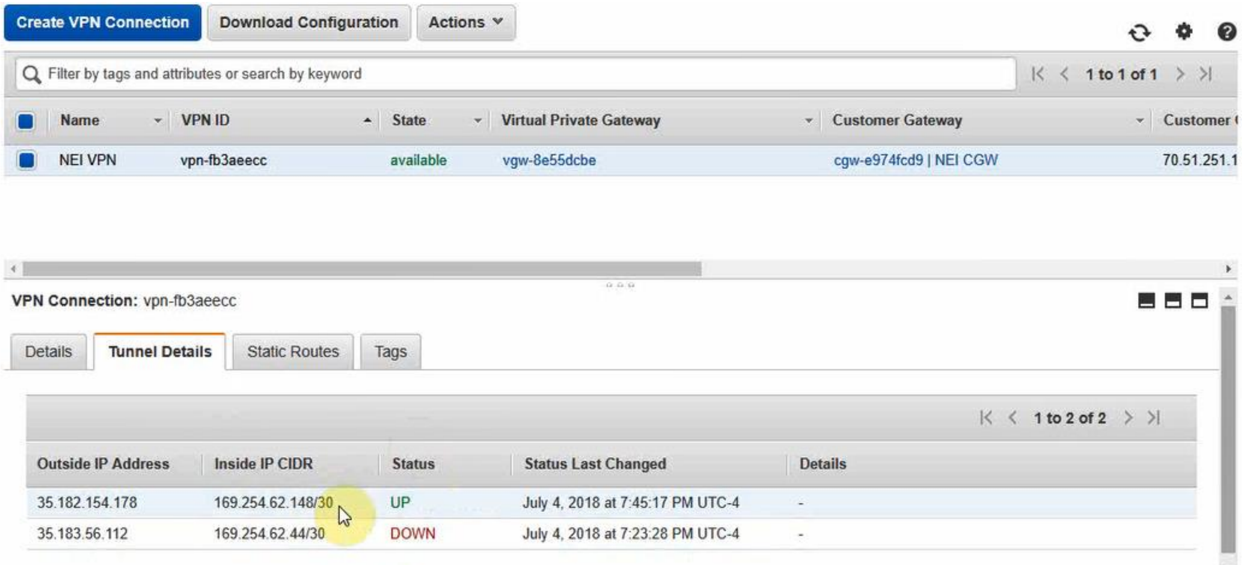
16. Now go ahead and click **download configuration**.
17. This is the configuration that you need to implement on your VPN terminating device so ensure you choose the appropriate Vendor, Platform and Software.
18. In our case our VPN terminating device was a CISCO Systems ASA 5500 series firewall. Once you have chosen the appropriate settings, click **download** and open the configuration with wordpad or microsoft word.
19. The configuration is lengthy as it has lots of extra information, you can read through the configuration copy the necessary parts into a text document and make the necessary edits. Below is a sample shortened and edited configuration for CISCO ASA firewall.

```
!ACL defining interesting traffic
!
access-list acl-amzn extended permit ip any4 172.20.0.0 255.255.0.0
!
access-list outside-in extended permit ip host 52.60.119.167 host 174.95.68.142
access-list outside-in extended permit ip host 52.60.237.251 host 174.95.68.142
!
!NAT Exempt
!
object network obj-SrcNet
subnet 0.0.0.0 0.0.0.0
object network obj-amzn
subnet 172.20.0.0 255.255.0.0
nat (inside,outside) 1 source static obj-SrcNet obj-SrcNet destination static obj-amzn obj-amzn
!
!VPN Related Config defining Phase 1 and 2 parameters
!
crypto isakmp identity address
crypto ikev1 enable outside
crypto ikev1 policy 201
  encryption aes
  authentication pre-share
  group 2
  lifetime 28800
  hash sha
exit
!
tunnel-group 52.60.119.167 type ipsec-l2l
tunnel-group 52.60.119.167 ipsec-attributes
   ikev1 pre-shared-key WnTS3Euig_Ho.keNAyXfcEpZWb28c3D5
isakmp keepalive threshold 10 retry 10
exit
```

```
!
tunnel-group 52.60.237.251 type ipsec-l2l
tunnel-group 52.60.237.251 ipsec-attributes
   ikev1 pre-shared-key jtON9cwZIqPLn9e9CogCblIx86yr_u7H
!
isakmp keepalive threshold 10 retry 10
exit
!
crypto ipsec ikev1 transform-set transform-amzn esp-aes esp-sha-hmac
!
!Below is Crypto map thats using acl-amzn ACL to detect traffic going to AWS VPC and enrcypt and send it through tunnel
!
crypto map amzn_vpn_map 1 match address acl-amzn
crypto map amzn_vpn_map 1 set pfs group2
crypto map amzn_vpn_map 1 set peer  52.60.119.167 52.60.237.251
crypto map amzn_vpn_map 1 set ikev1 transform-set transform-amzn
crypto map amzn_vpn_map 1 set security-association lifetime seconds 3600
!
!Applying Crypto Map to outside interface
!
crypto map amzn_vpn_map interface outside
!
! there are few more IPsec related parameters that we need to setup
!
crypto ipsec df-bit clear-df outside
!
crypto ipsec security-association replay window-size 128
!
crypto ipsec fragmentation before-encryption outside
!
sysopt connection tcpmss 1379
!
!
! To send contant traffic to AWS side to ensure that tunnel stays up, we will setup IP SLA Monitor that will send PING packets
! AWS Side
sla monitor 1
   type echo protocol ipIcmpEcho 52.60.119.167 interface outside
   frequency 5
exit
sla monitor schedule 1 life forever start-time now
!
icmp permit any outside
!
!The VPN Filter will restrict traffic that is permitted through the tunnels. By default all traffic is denied.
!
access-list amzn-filter extended permit ip 172.20.0.0 255.255.0.0 192.168.3.0 255.255.255.0
```

```
access-list amzn-filter extended deny ip any any
group-policy filter internal
group-policy filter attributes
vpn-filter value amzn-filter
tunnel-group 52.60.119.167 general-attributes
default-group-policy filter
exit
tunnel-group 52.60.237.251 general-attributes
default-group-policy filter
Exit
```

21. Once you have edited the configuration go ahead and implement it on your VPN device. Once the configuration has been successfully implemented check the status of the tunnels. At least one tunnel should be up. You may also check the status of tunnels using the AWS console by navigating to the VPC console and then navigating to VPN connections. Choose your VPN and go to **tunnel details**.

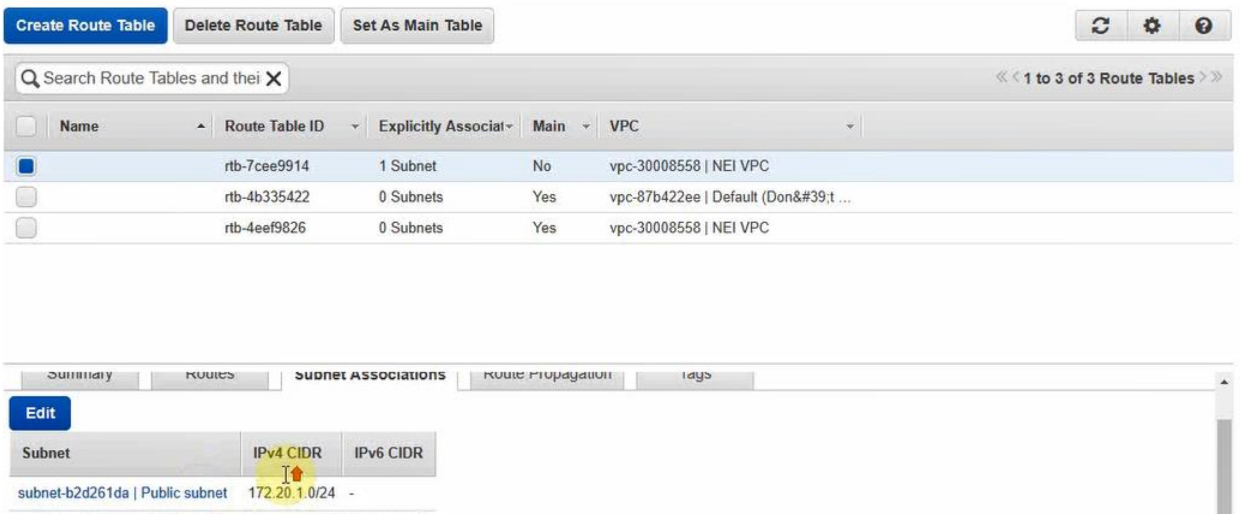


Name	VPN ID	State	Virtual Private Gateway	Customer Gateway	Customer
NEI VPN	vpn-fb3aeecc	available	vgw-8e55dcbe	cgw-e974fcd9 | NEI CGW	70.51.251.1

VPN Connection: vpn-fb3aeecc

Outside IP Address	Inside IP CIDR	Status	Status Last Changed	Details
35.182.154.178	169.254.62.148/30	UP	July 4, 2018 at 7:45:17 PM UTC-4	-
35.183.56.112	169.254.62.44/30	DOWN	July 4, 2018 at 7:23:28 PM UTC-4	-

22. Once you have confirmed that at least one tunnel is up, navigate to route tables from the left navigation panel. Choose the route table that is associated with your VPC and is **not the main route table**. Go to **subnet association** and ensure this route table is associated with the public subnet. Go to routes and ensure that the the default route is pointing to the igw (internet gateway). Click **edit**, click **add another rule**. For destination put in the private subnet of your datacenter and for the target choose your vgw. Click **save**. Click on the name blank and name it **Public Subnet RT**.



☐	Name	Route Table ID	Explicitly Associat	Main	VPC
■		rtb-7cee9914	1 Subnet	No	vpc-30008558 | NEI VPC
☐		rtb-4b335422	0 Subnets	Yes	vpc-87b422ee | Default (Don&#39;t ...
☐		rtb-4eef9826	0 Subnets	Yes	vpc-30008558 | NEI VPC

Subnet	IPv4 CIDR	IPv6 CIDR
subnet-b2d261da | Public subnet	172.20.1.0/24	-

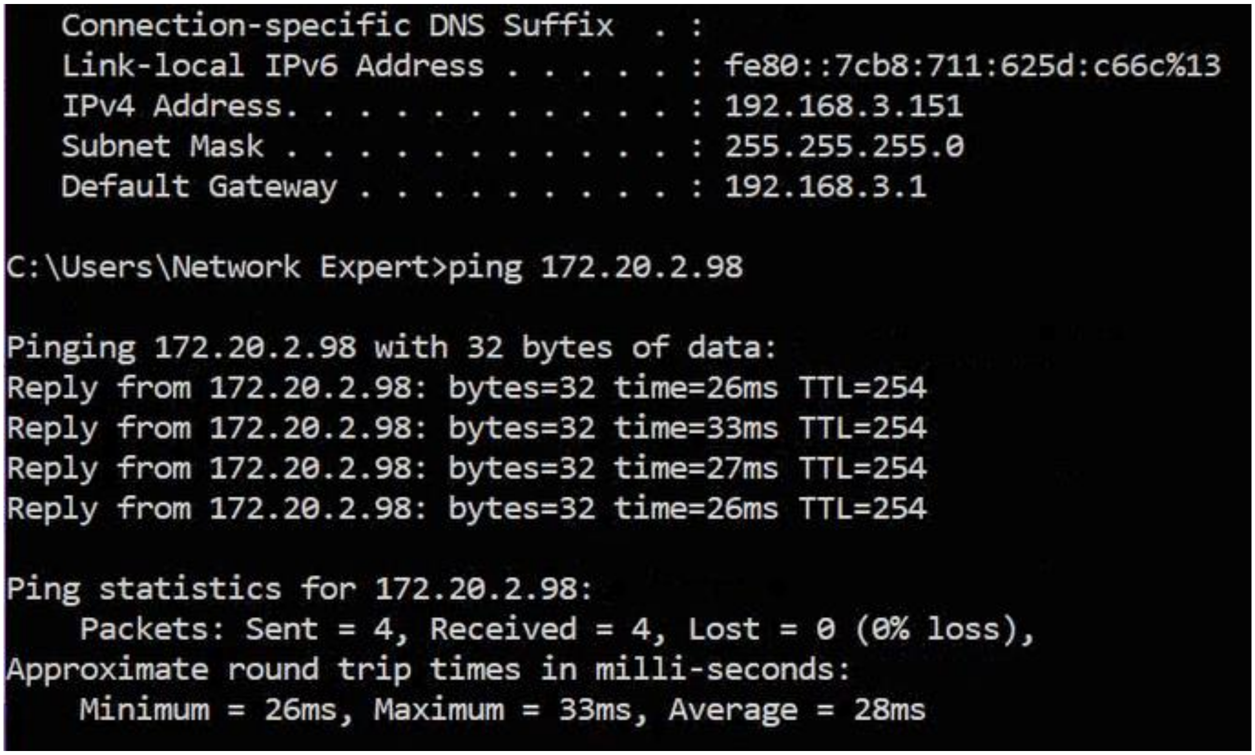
23. Click create new route table and name it **Private Subnet RT** and ensure you choose the right VPC.

24. Once the table has been created, choose it and go to subnet associations from the tabs at the bottom of the page. Click **edit** and choose your private subnet and then click **save**. Navigate to the routes tab and click **edit**, click **add another rule**. For destination put in the private subnet of your datacenter and for the target choose your vgw. Click **save**.

25. Launch a linux instance in the private subnet of your VPC. Ensure you allow all traffic to the instance when assigning it a security group so you don’t encounter any problems.

26. Once the instance has launched, copy it’s private IP address and ping it using command prompt. Make sure your private IP address is within the

private subnet of your data center.



```
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::7cb8:711:625d:c66c%13
   IPv4 Address. . . . . . . . . . . : 192.168.3.151
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.3.1

C:\Users\Network Expert>ping 172.20.2.98

Pinging 172.20.2.98 with 32 bytes of data:
Reply from 172.20.2.98: bytes=32 time=26ms TTL=254
Reply from 172.20.2.98: bytes=32 time=33ms TTL=254
Reply from 172.20.2.98: bytes=32 time=27ms TTL=254
Reply from 172.20.2.98: bytes=32 time=26ms TTL=254

Ping statistics for 172.20.2.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 26ms, Maximum = 33ms, Average = 28ms
```

27. A successful ping means you are successfully able to reach AWS over your VPN tunnel.
28. Go ahead and connect to your instance using putty. Once again you have connected to your private AWS infrastructure over your VPN tunnel.
29. Head back to the VPC console, head to VPN connections and make sure that your tunnel is up. You have successfully set up a VPN connection between your on prem data center and AWS.