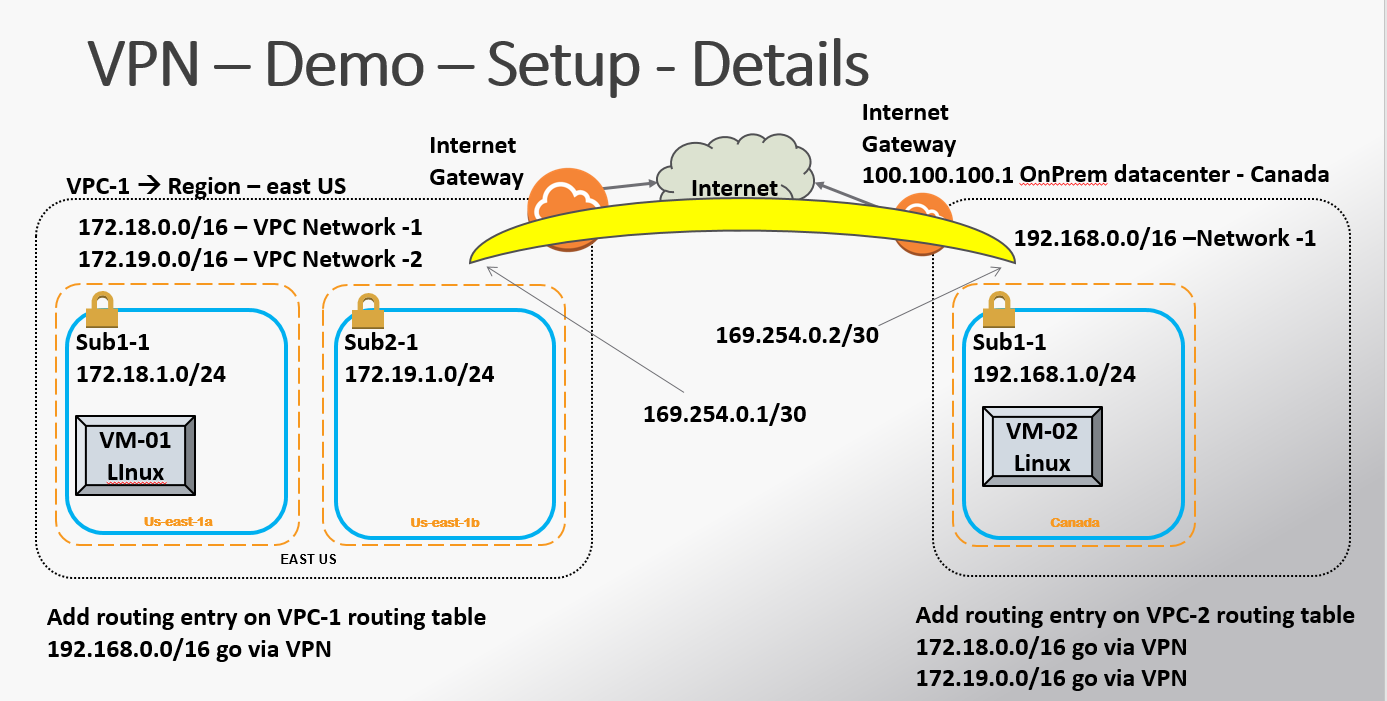
**AWS VPN use Case**

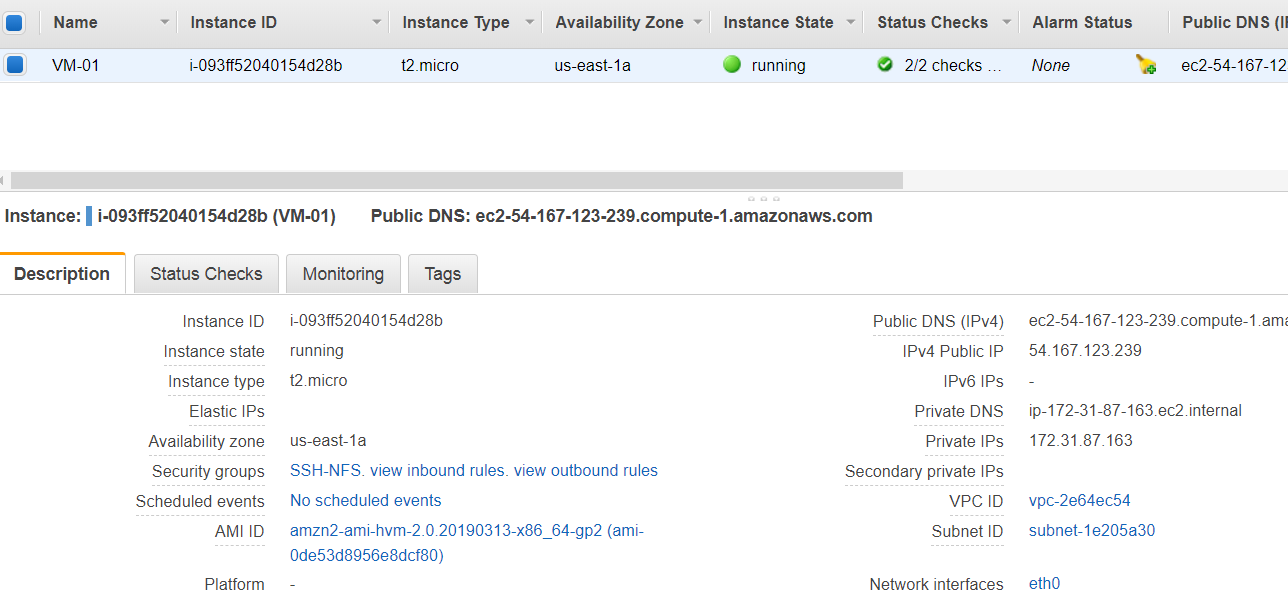


**Steps Involved.**

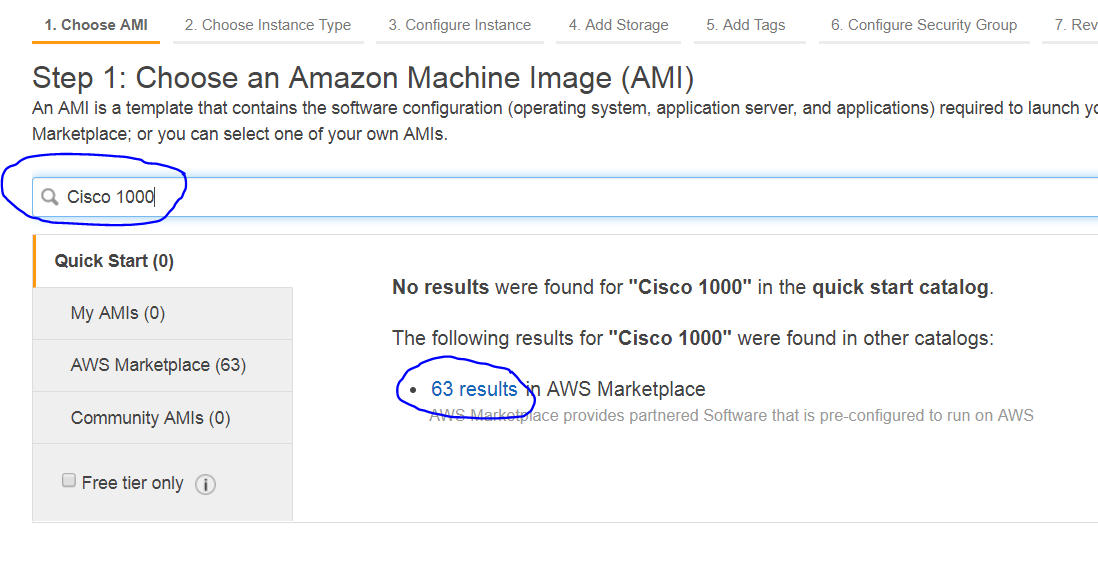
1. **Create EC2 instance in the N.Virginia**
2. **Create the VPN box on onprem/Datacenter side (in our example, in the other region – Oregon)**
3. **Configure the VPN on AWS VPC side**
4. **Configure the VPN box.**
5. **Configure the Routing Table on both the sides.**
6. **Check if the EC2 instance is able to reach the on Prem datacenter**

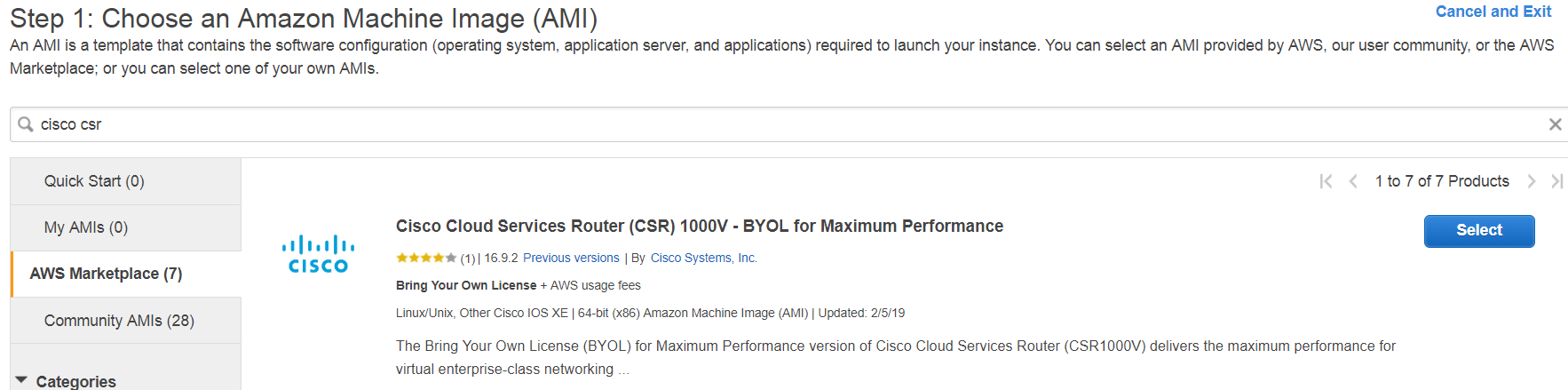
**Steps for the LAB Setup.**

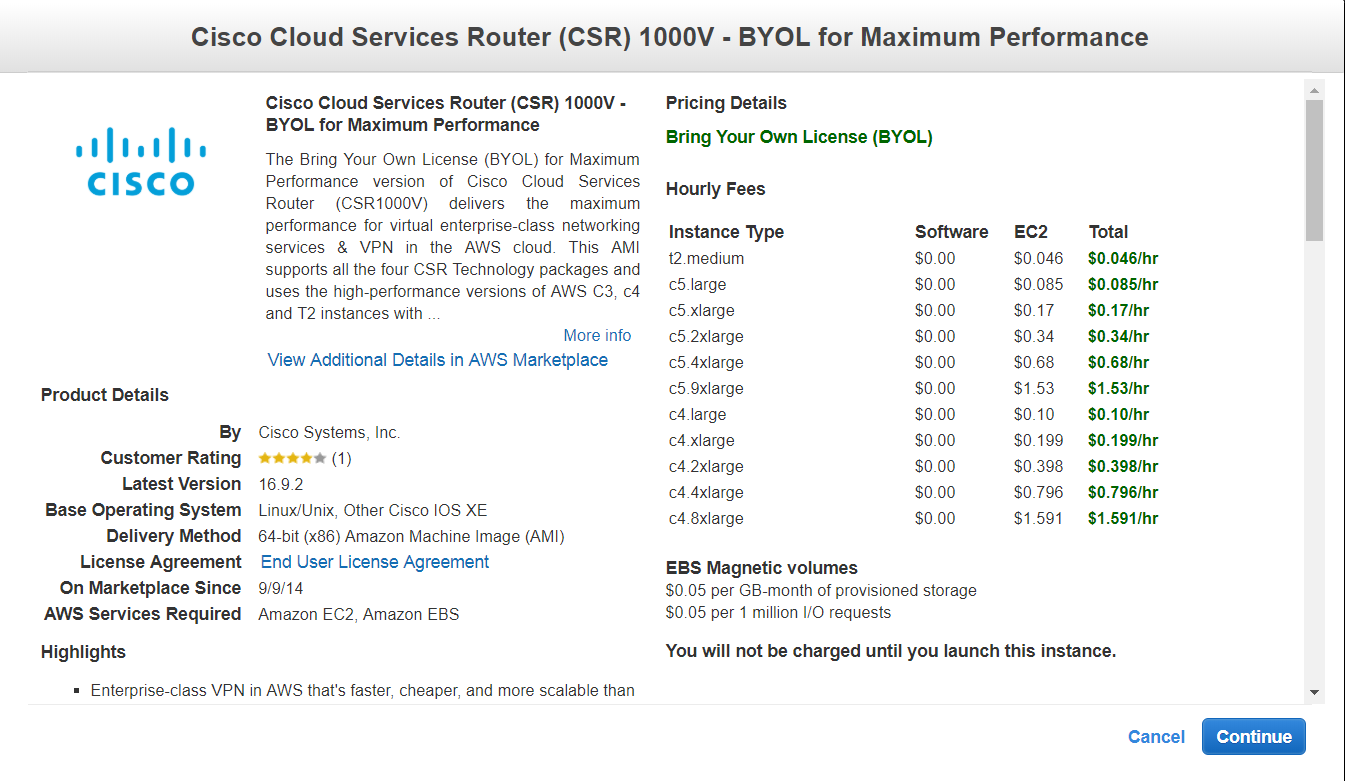
1. **Create EC2 instance in the N.Virginia**

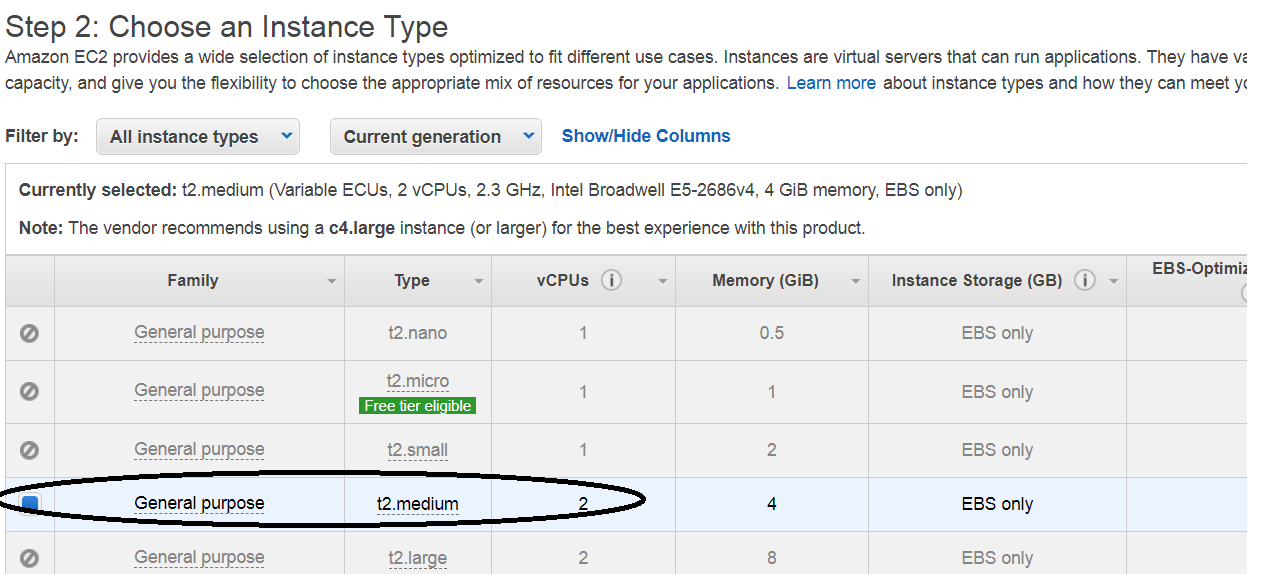


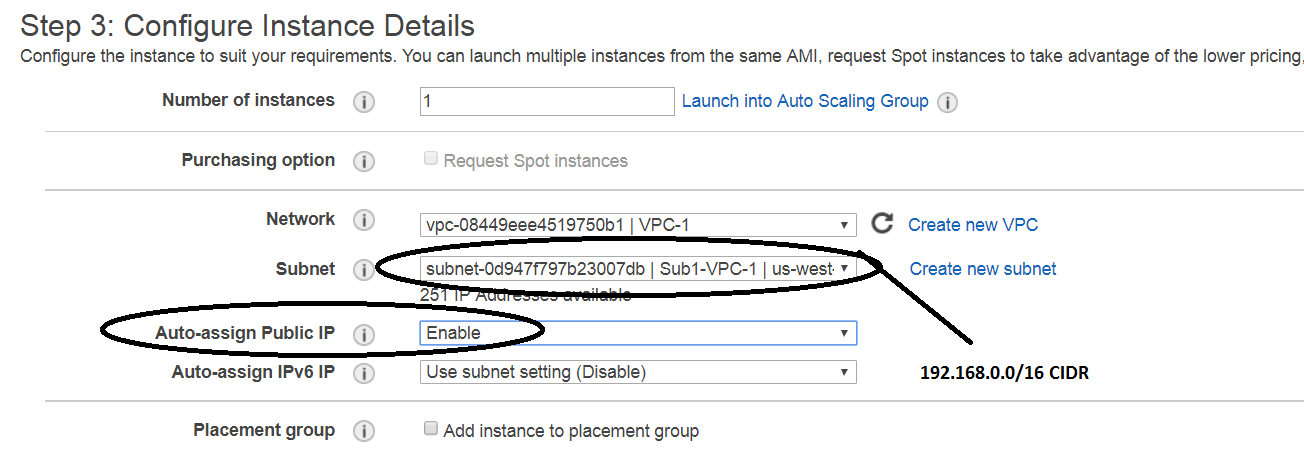
1. **Create the “Cisco CSR 1000R” EC2 instance in “Oregon” region with Public ip on it.**

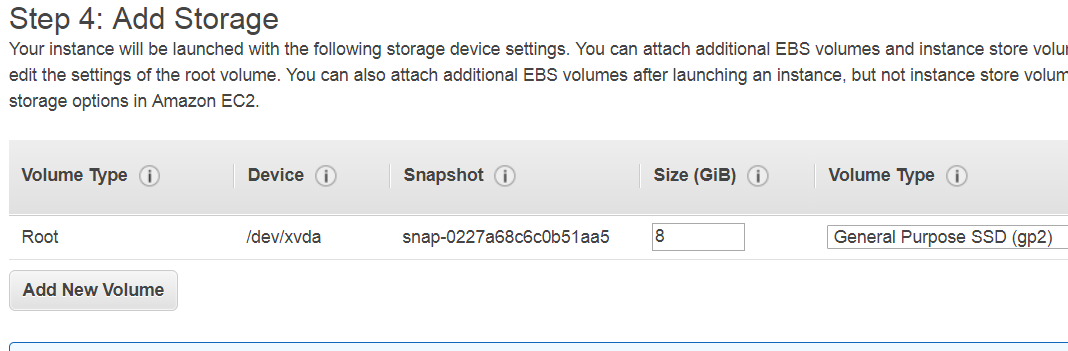


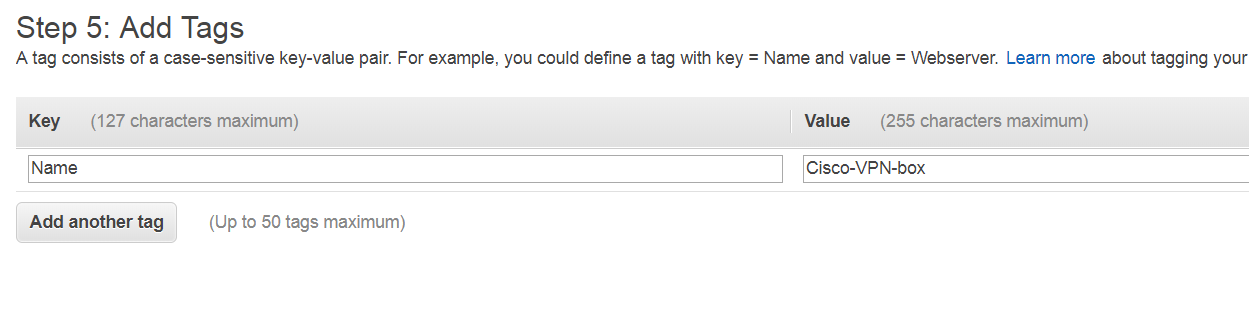


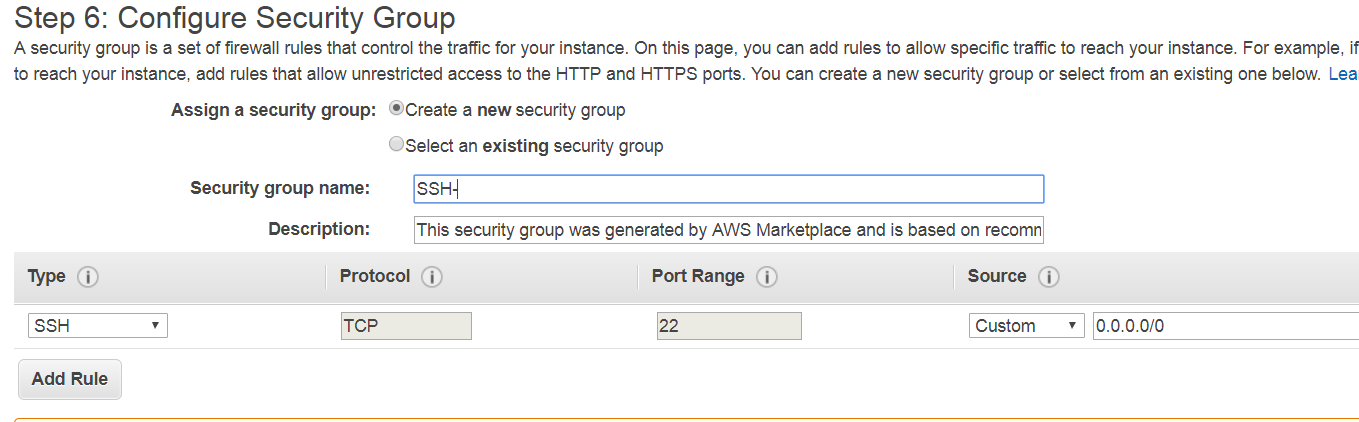


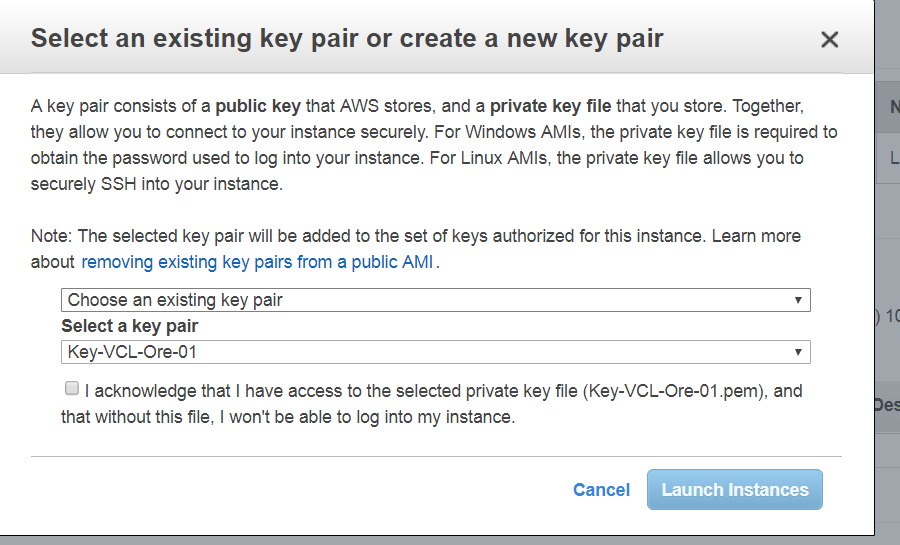
****

****

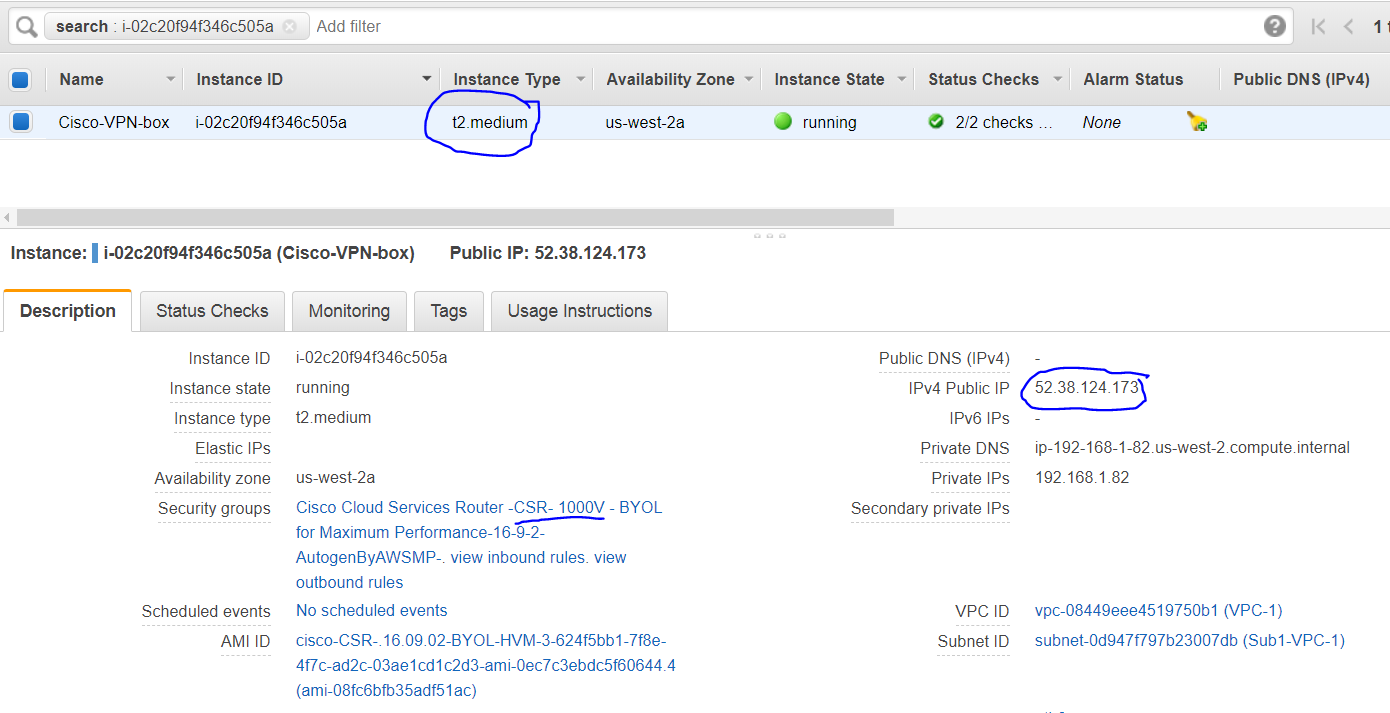








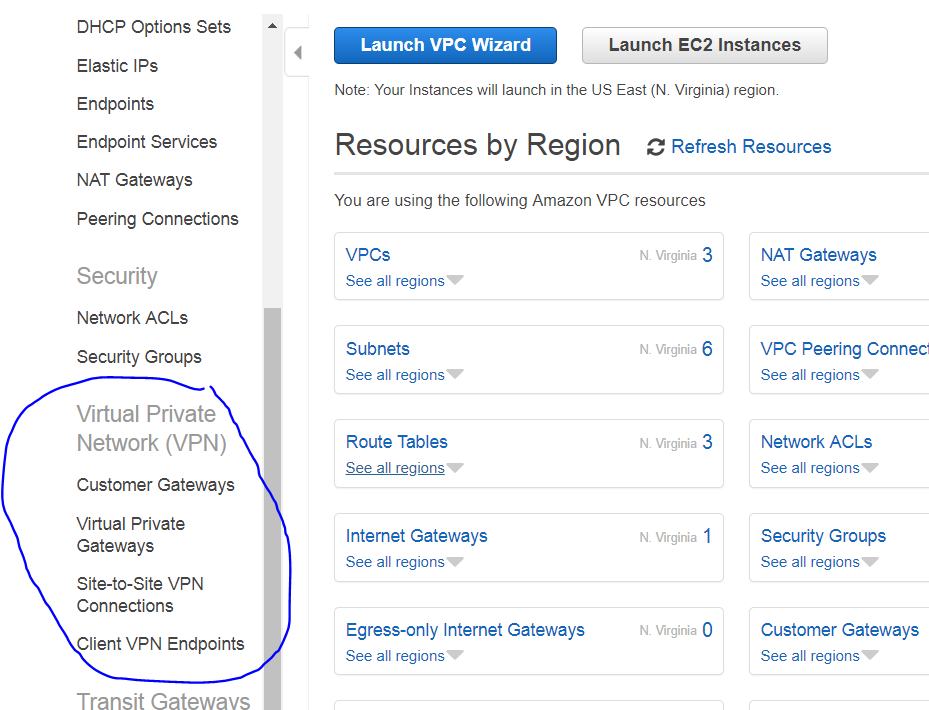
**Output:**



1. **Configure the VPN on AWS VPC Side**

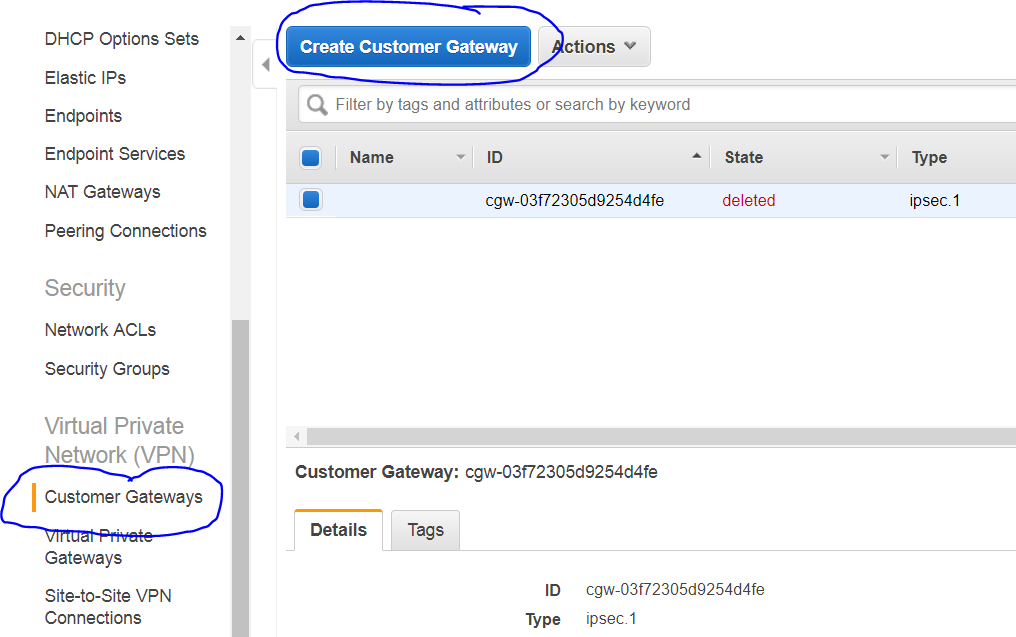
**There are 3 steps**

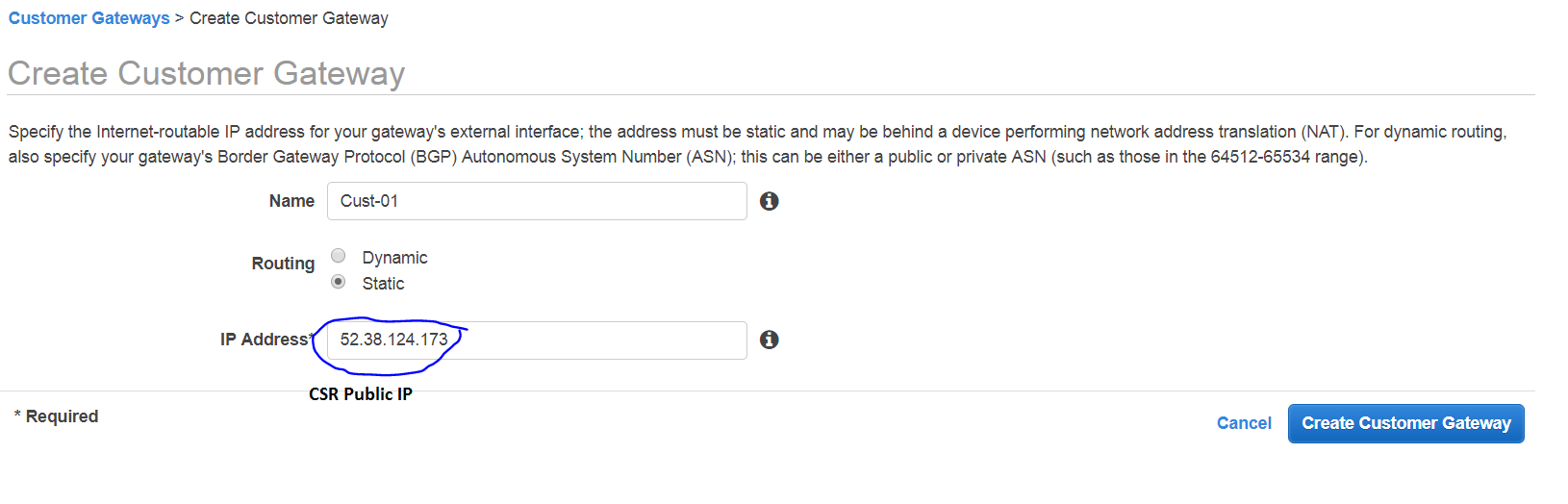
* 1. **Customer Gateway**
  2. **Virtual private Gateway**
  3. **Site-to-Site VPN**

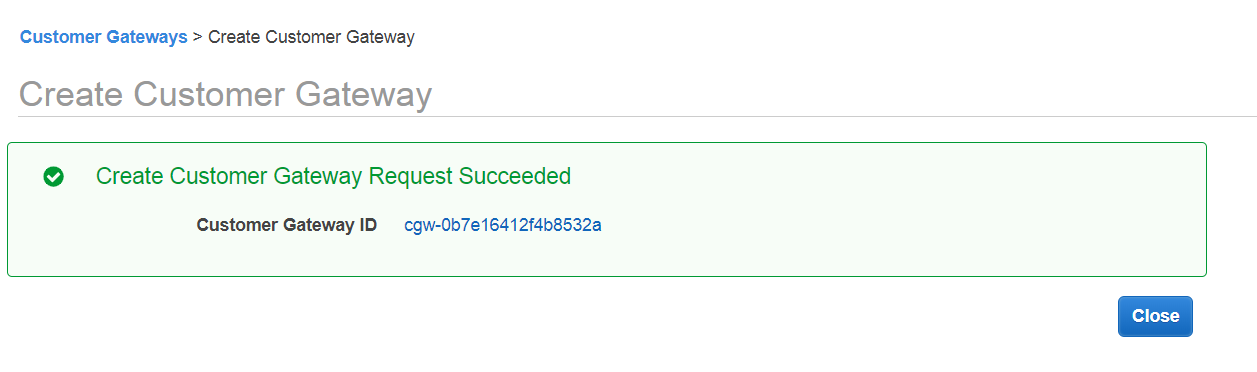


1. **Customer Gateway**

We would need to create this in the N.Virginia.

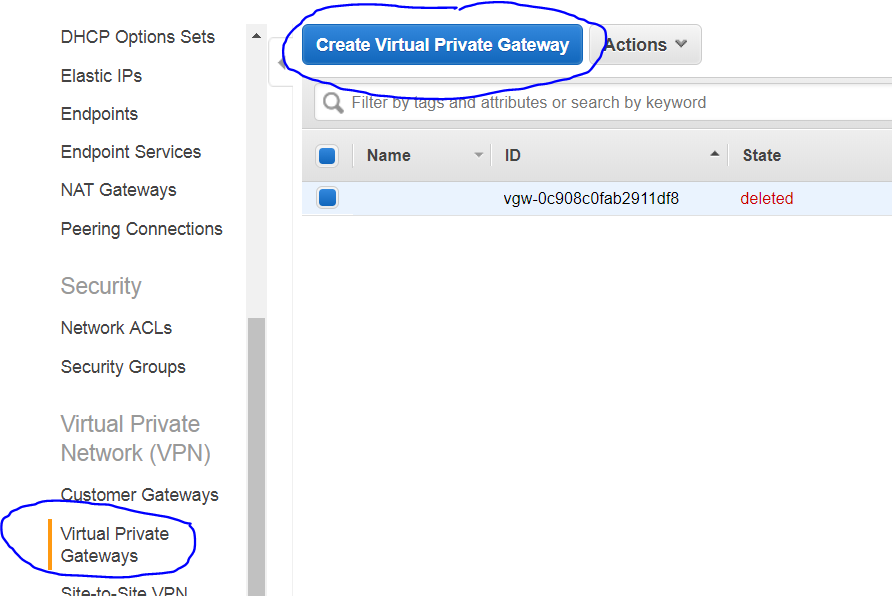


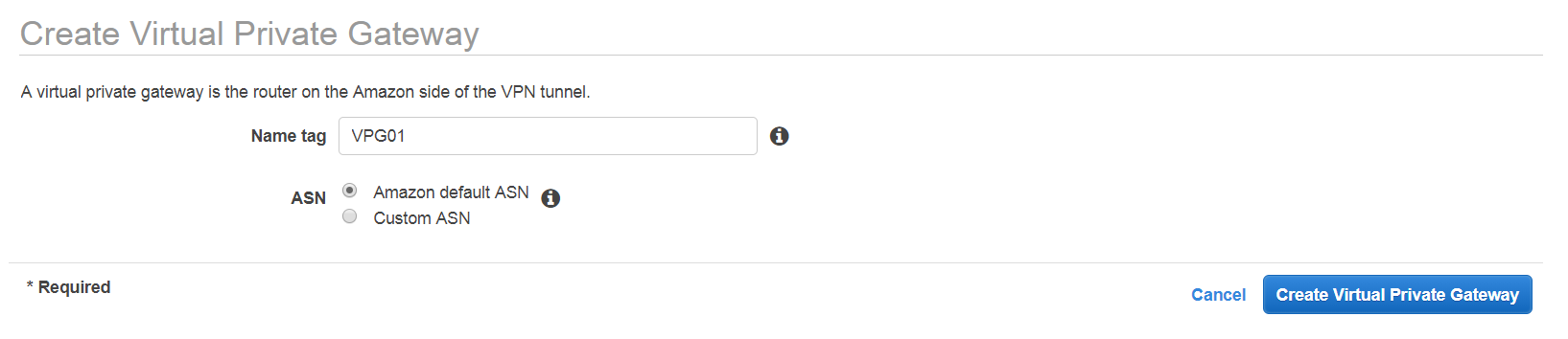


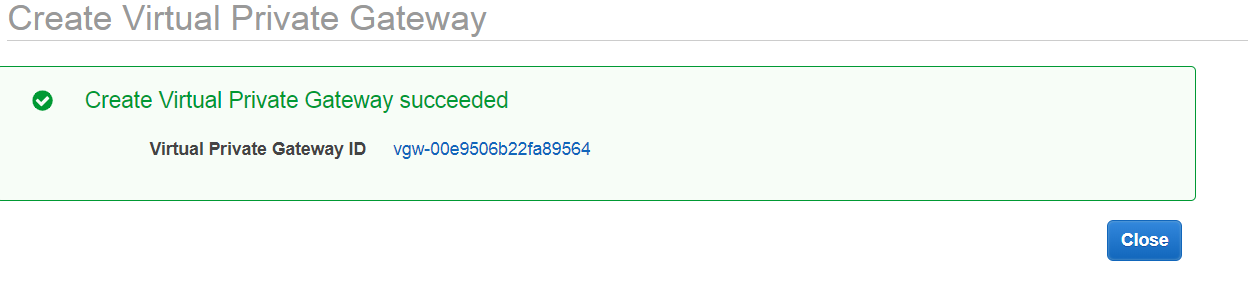


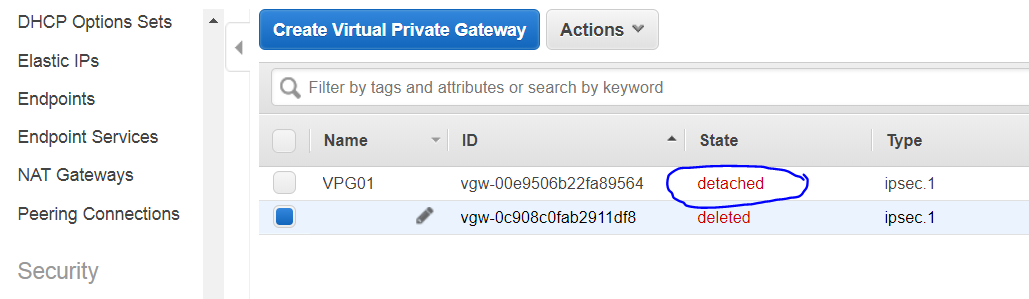
1. **Virtual private Gateway**

This will intimate the AWS that the VPC is going to have a VPN connection

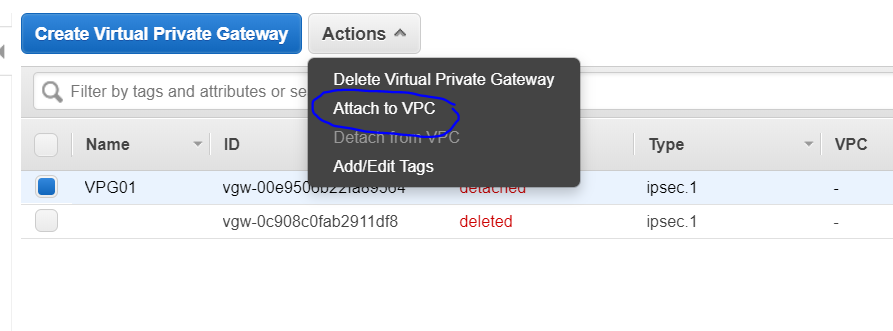




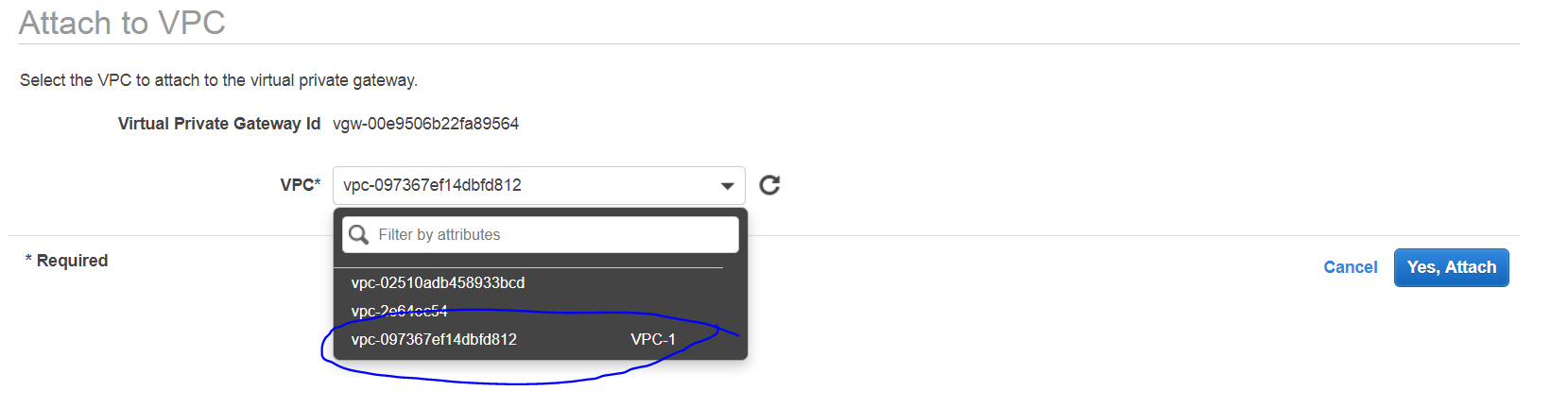


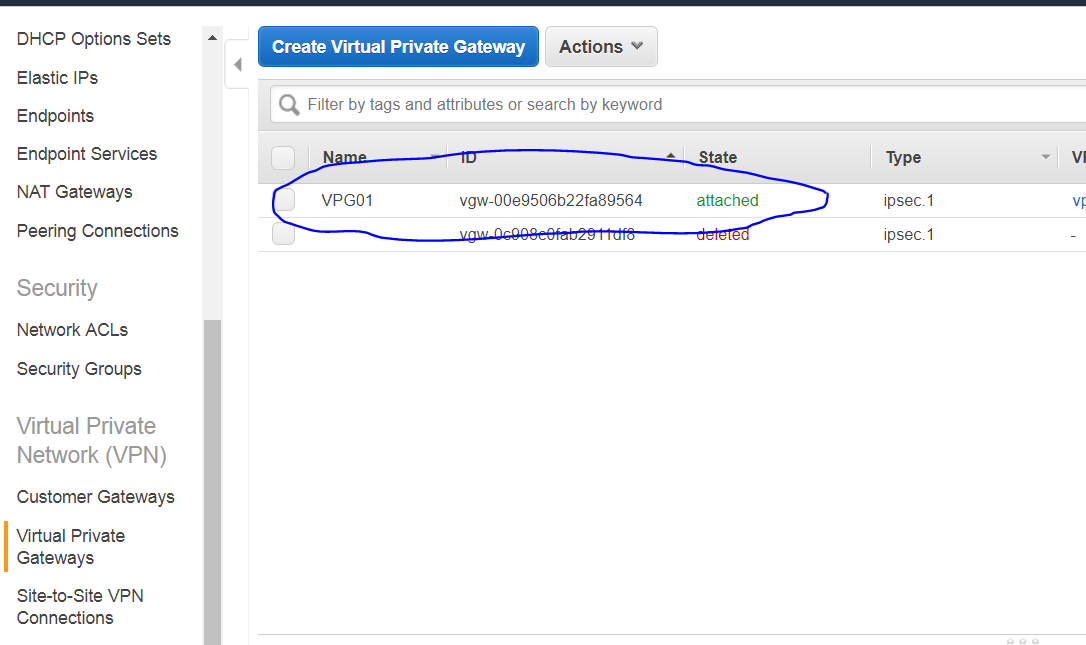


The Above screen say, it is “detached” , and we need to attach it to an VPC.



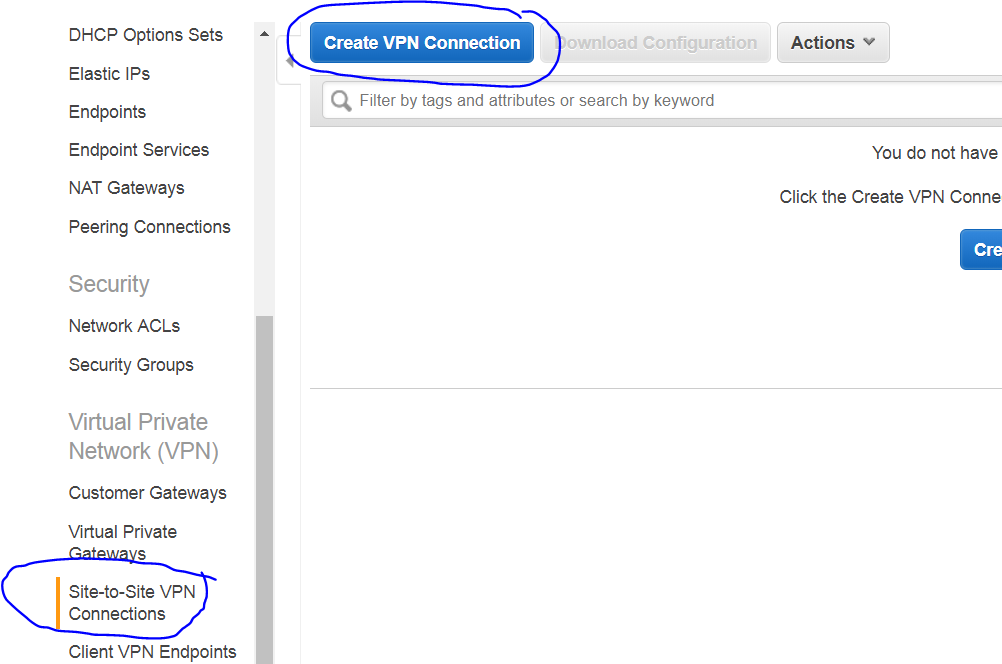
Select Actions 🡪 click on “attach to VPC”



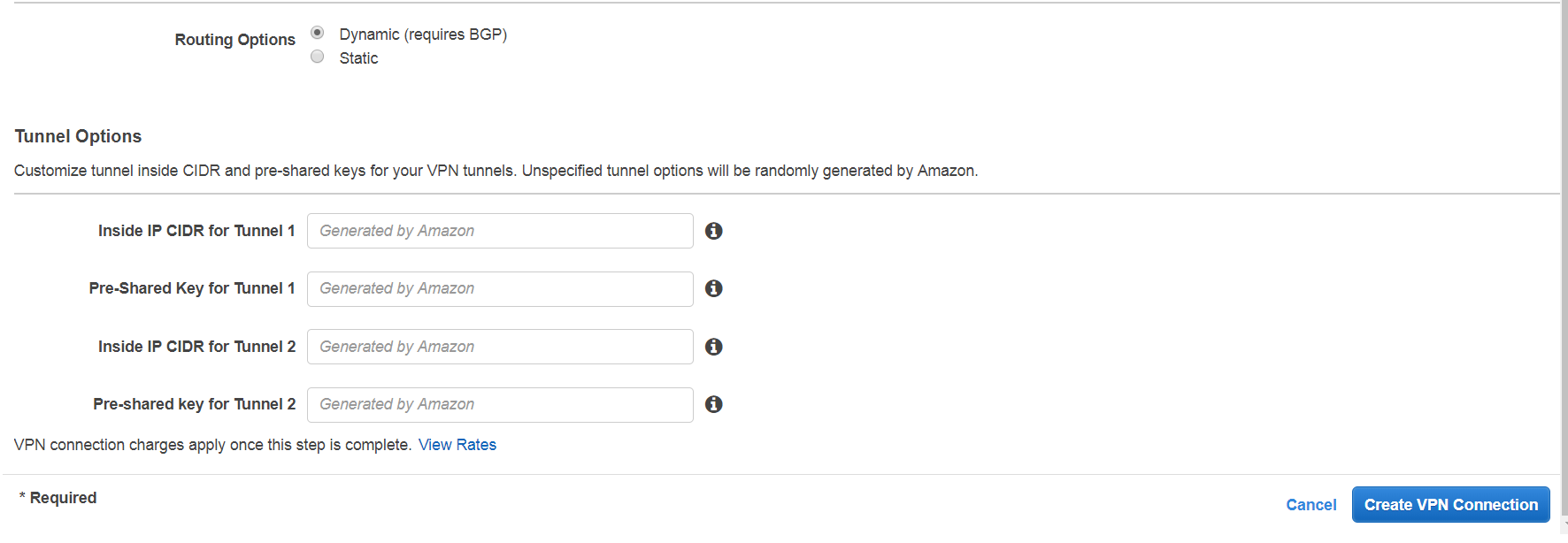


1. **Site to Site VPN Connections**

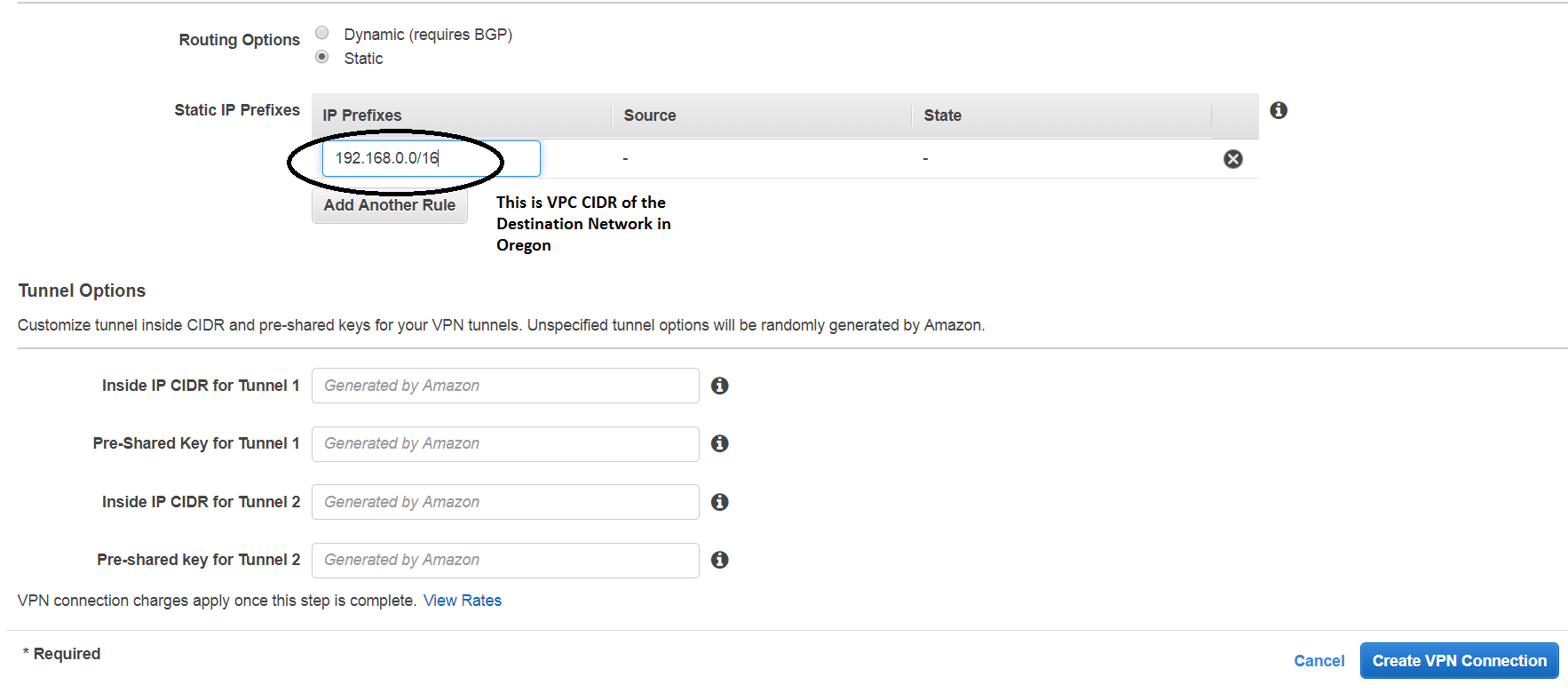
This would connect the Customer side and VPC side.

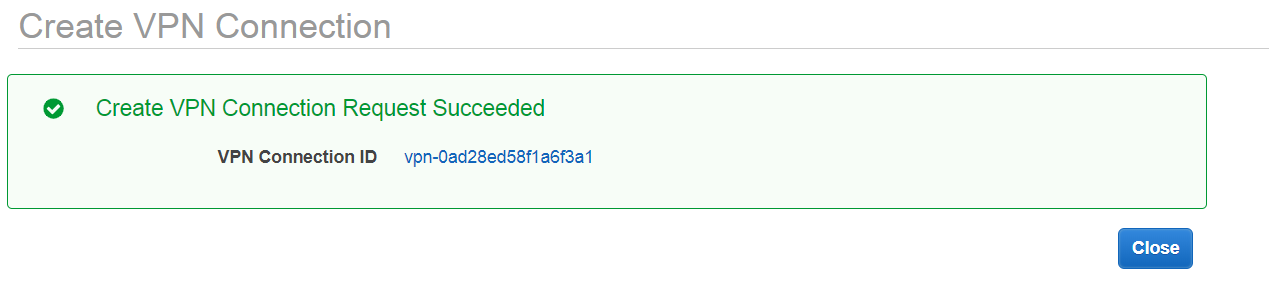


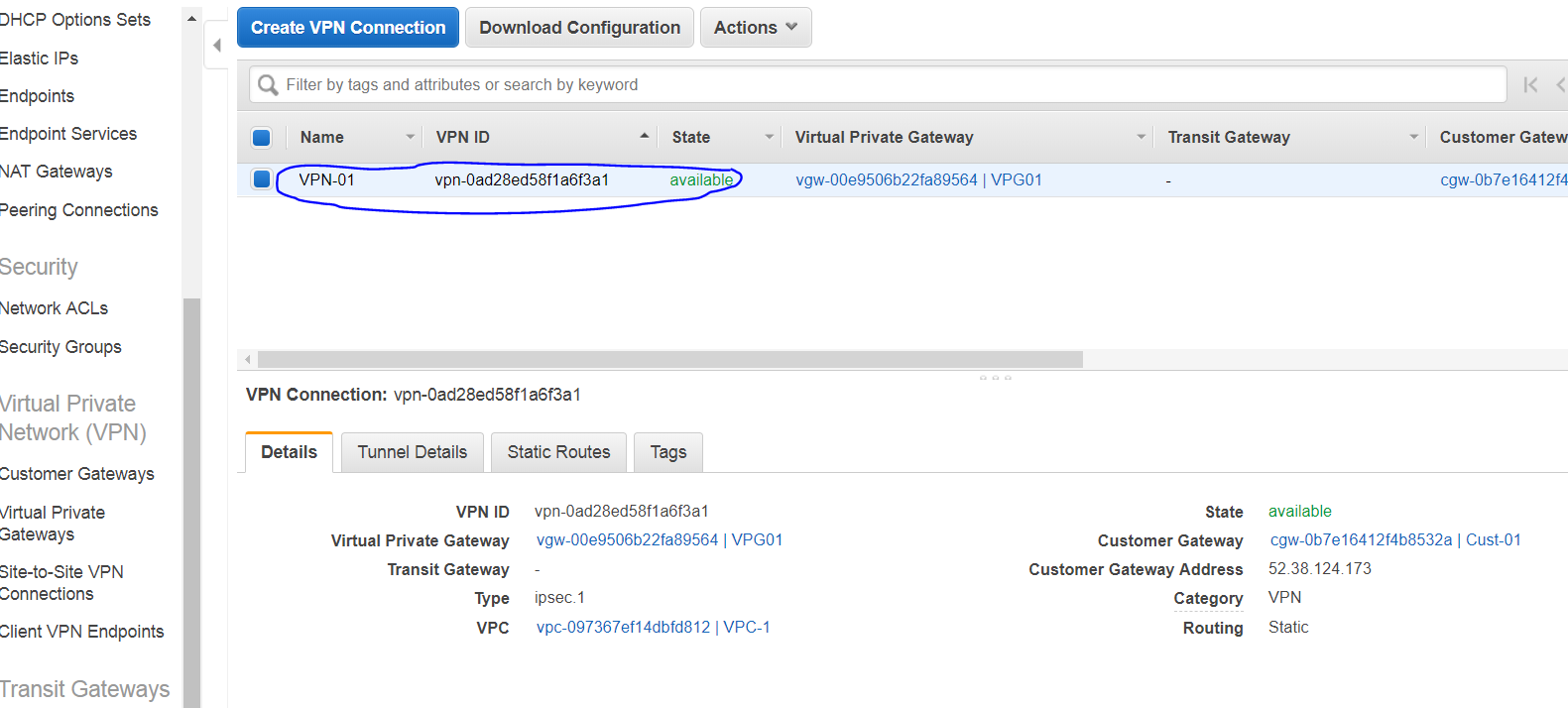




In the above diagram, change the “Routing Options to “**static**” entry.



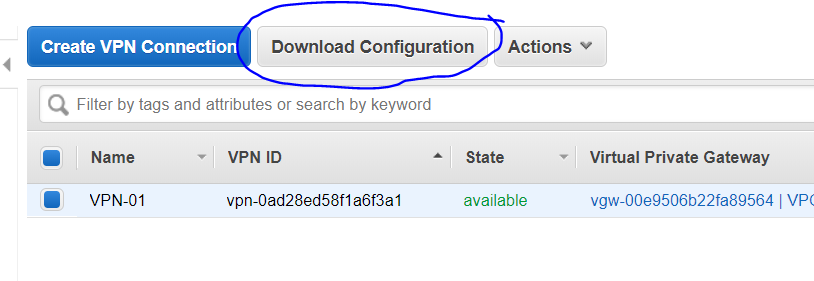


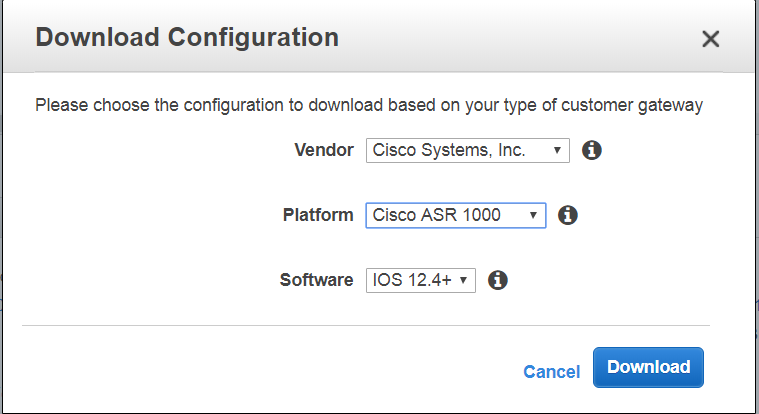


This would take around 10 to 15 min for the VPN to go **“available”.**

1. **Configure the Cisco VPN box created in Oregon**

**Download the configuration for the Cisco VPN box from the VPN configuration page in “n.Virginia”**



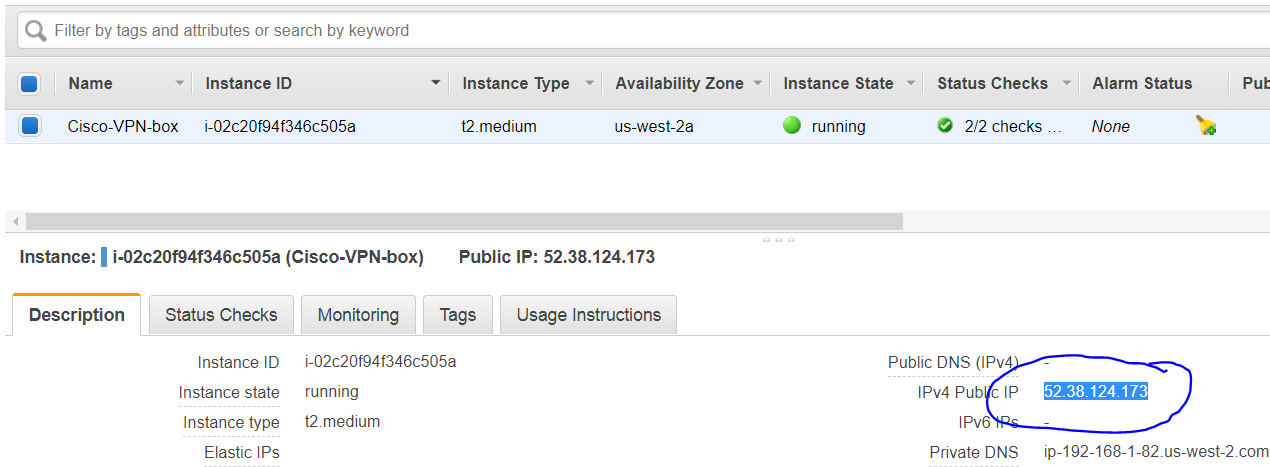


Select the appropriate device, “Vendor” , “Platform” and “Software”.

In our case it would be as above. And Click on “**Download**”

**The file that is downloaded is the configuration details that need to be configured on the Cisco CSR 1000.**

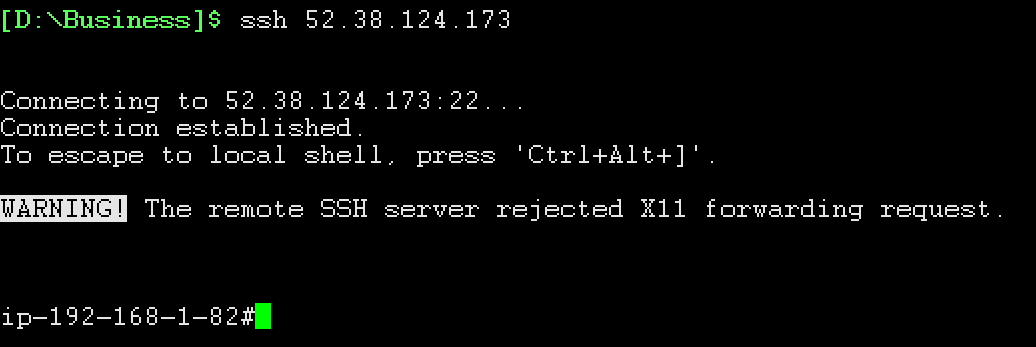
1. **Configure the Cisco 1000 VPN box instance**



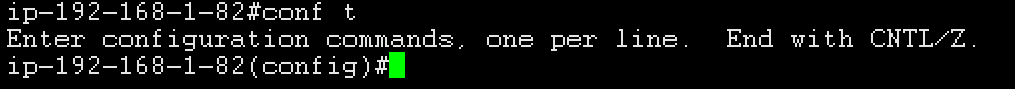
Login to the cisco 1000 VPN box.

Use the Public ip of the Cisco 1000 VPN box and

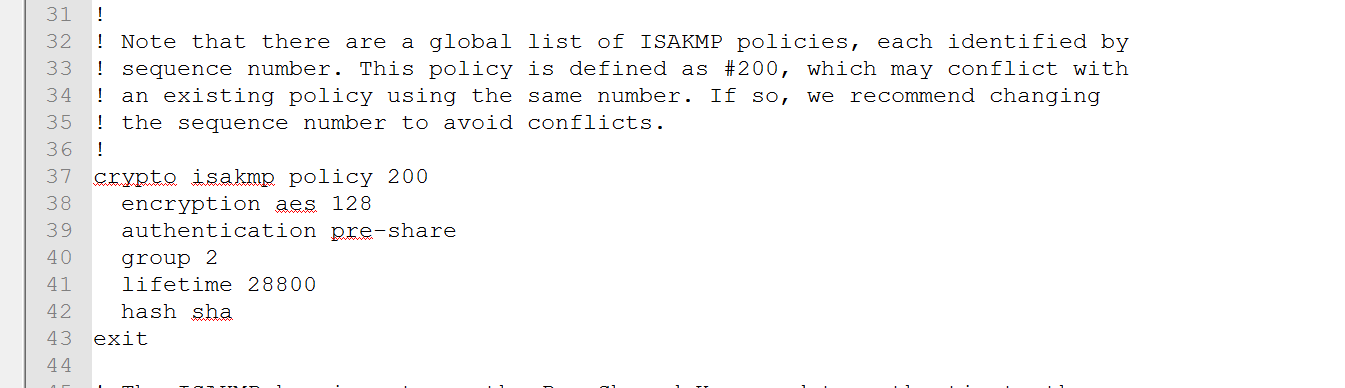
**Usr: ec2-user, pwd: the pem file.**

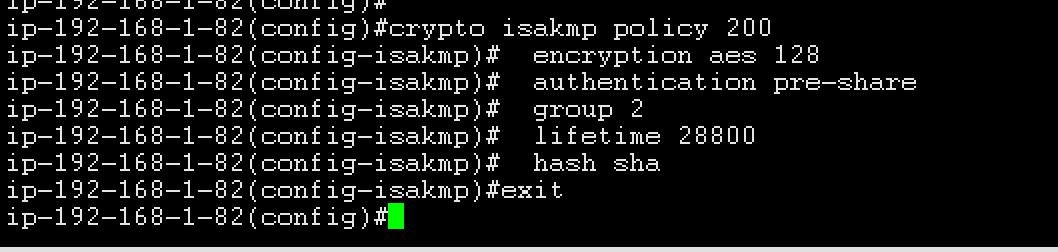


1. Now, go to the “config” mode.

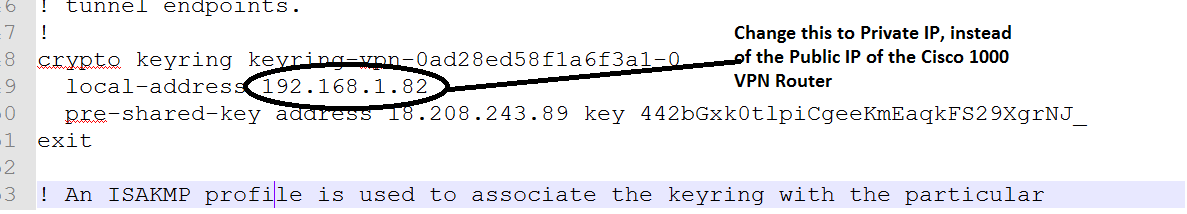


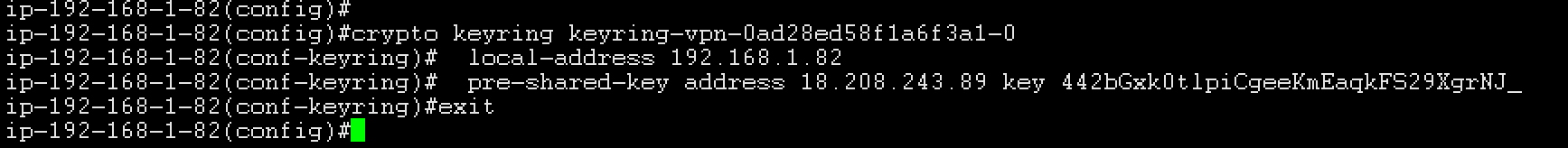
Now, lets configure the cisco VPN router with the configuration file that was downloaded



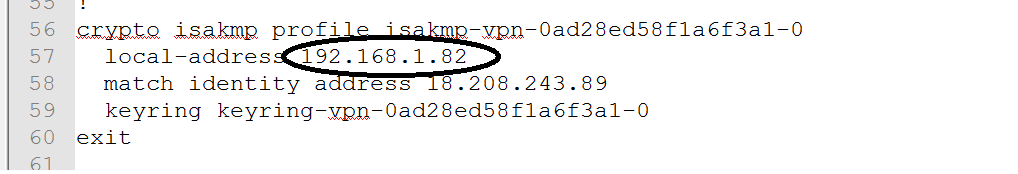


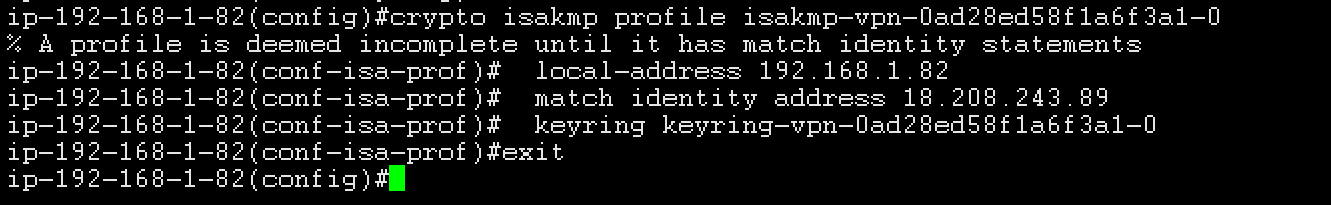
1. Crypto keyring config, change the local-address to the private ip of the cisco 1000 EC2 instance.



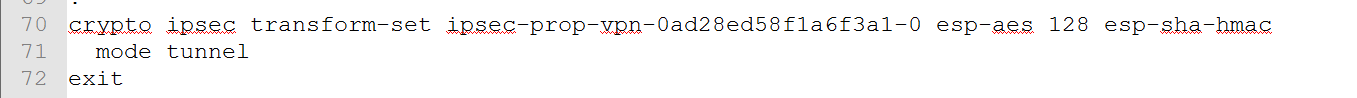


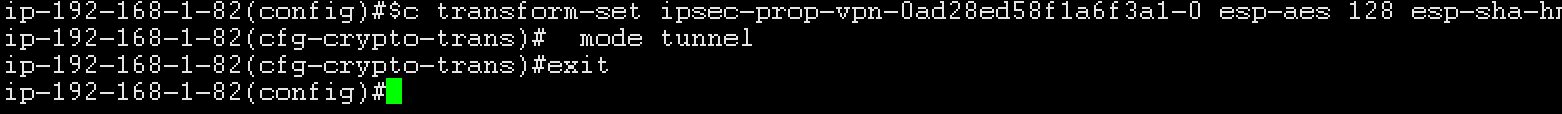
1. Configure Crypto isakmp

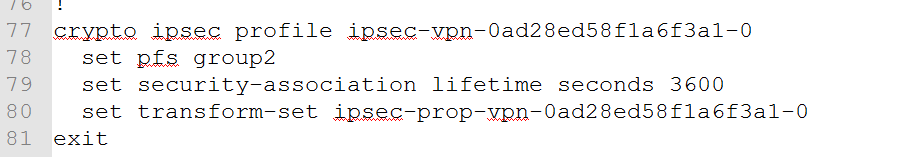


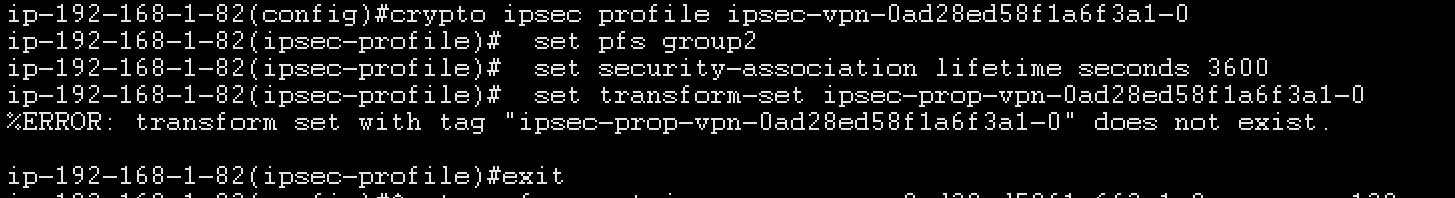


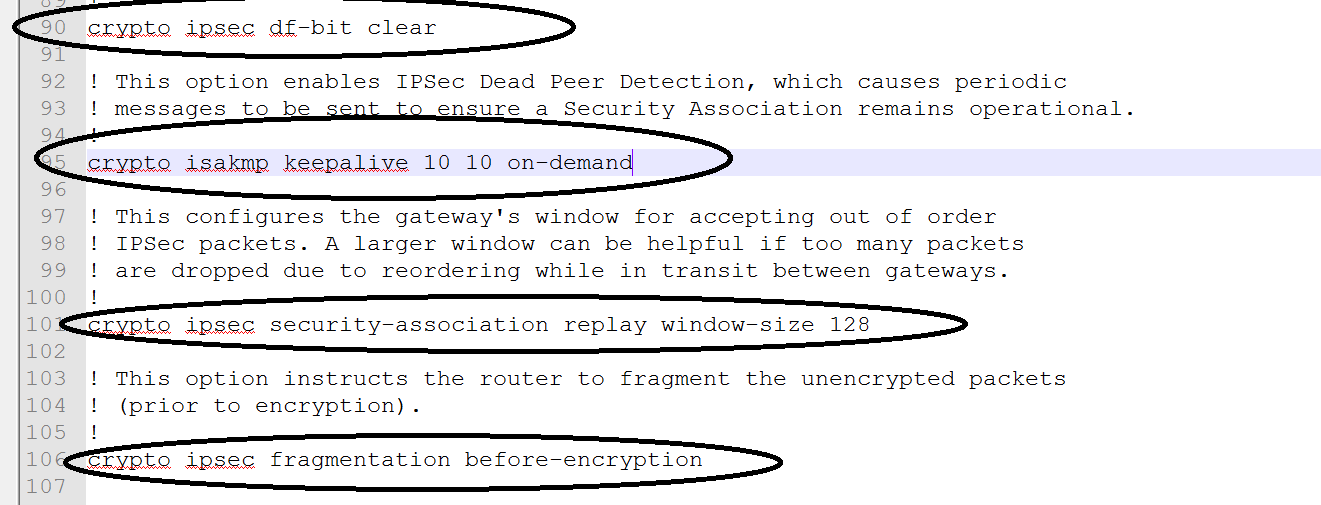
1. IPSec Configuration

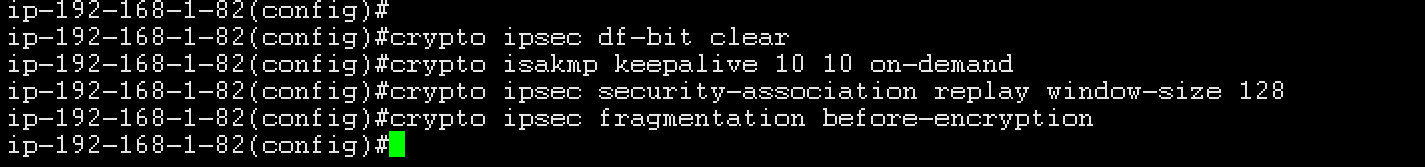




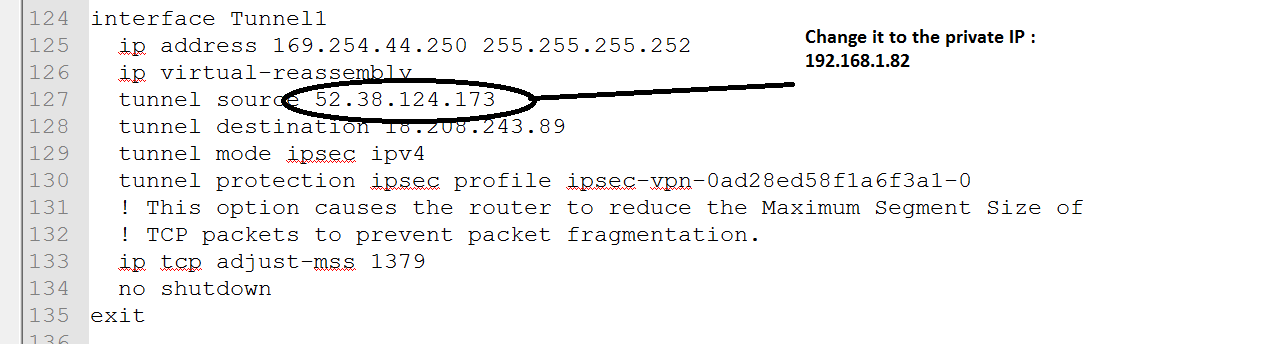


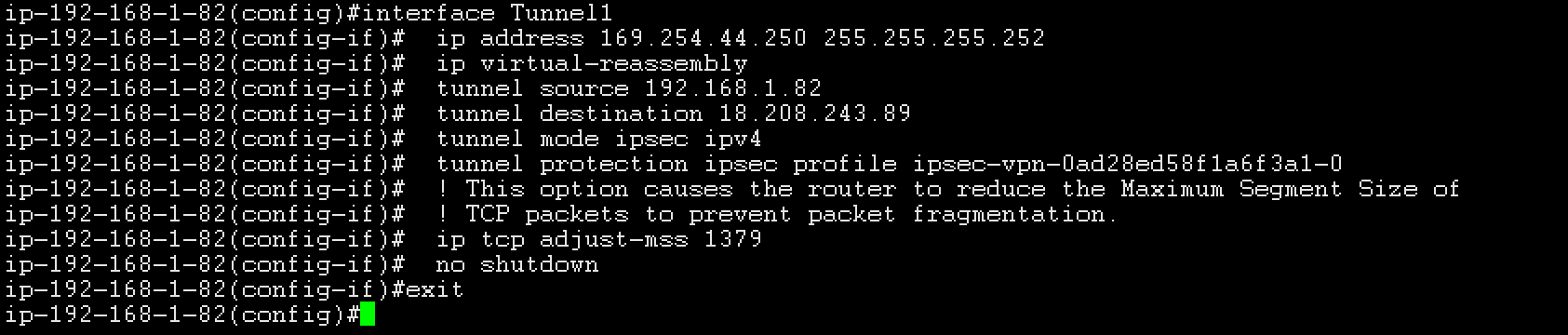




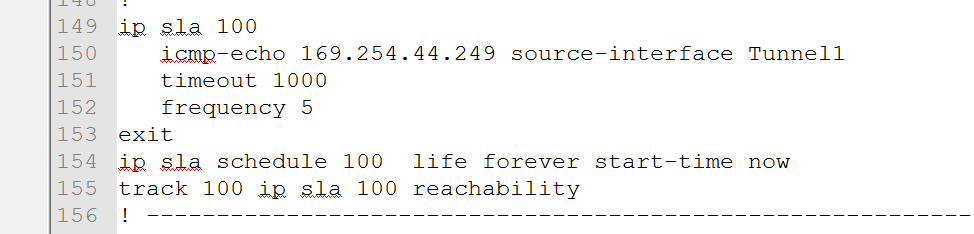


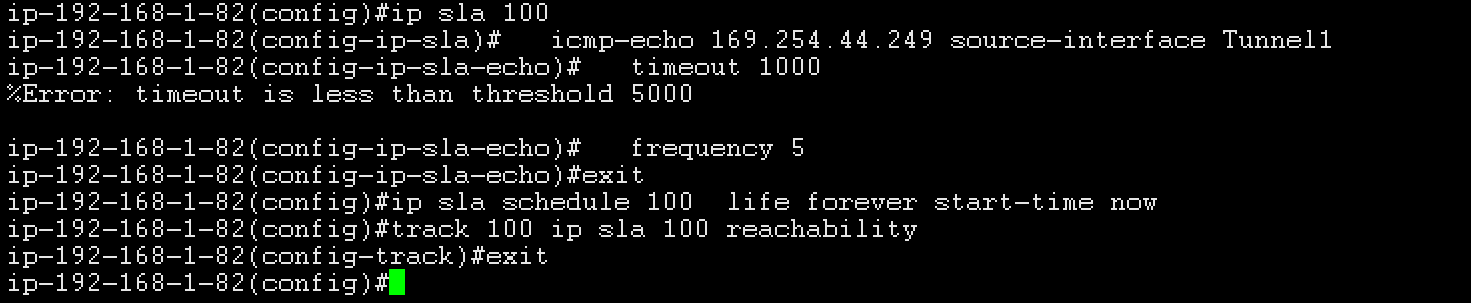
1. Tunnel Interface Configuration



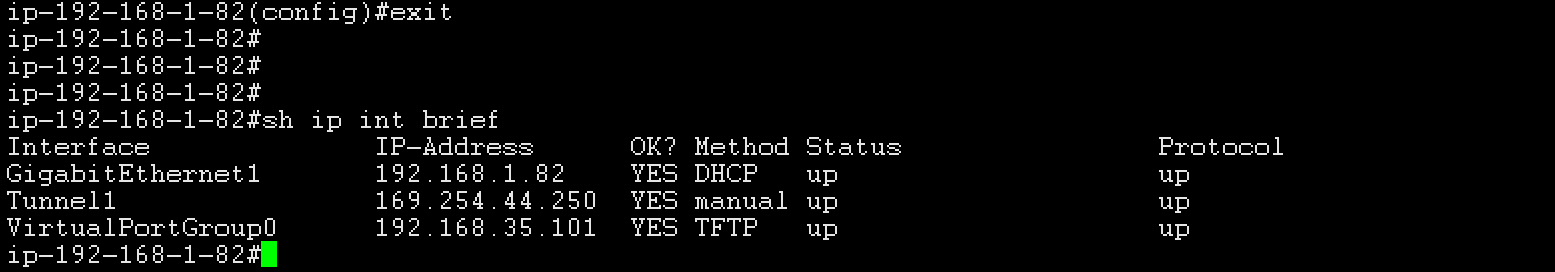


1. Static Route Configuration

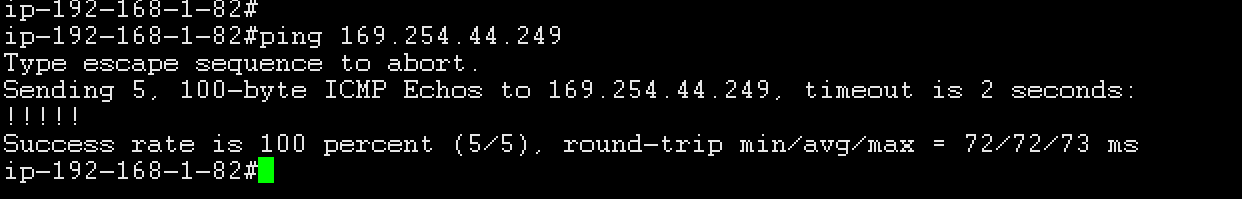




1. Check output of the Cisco VPN Router



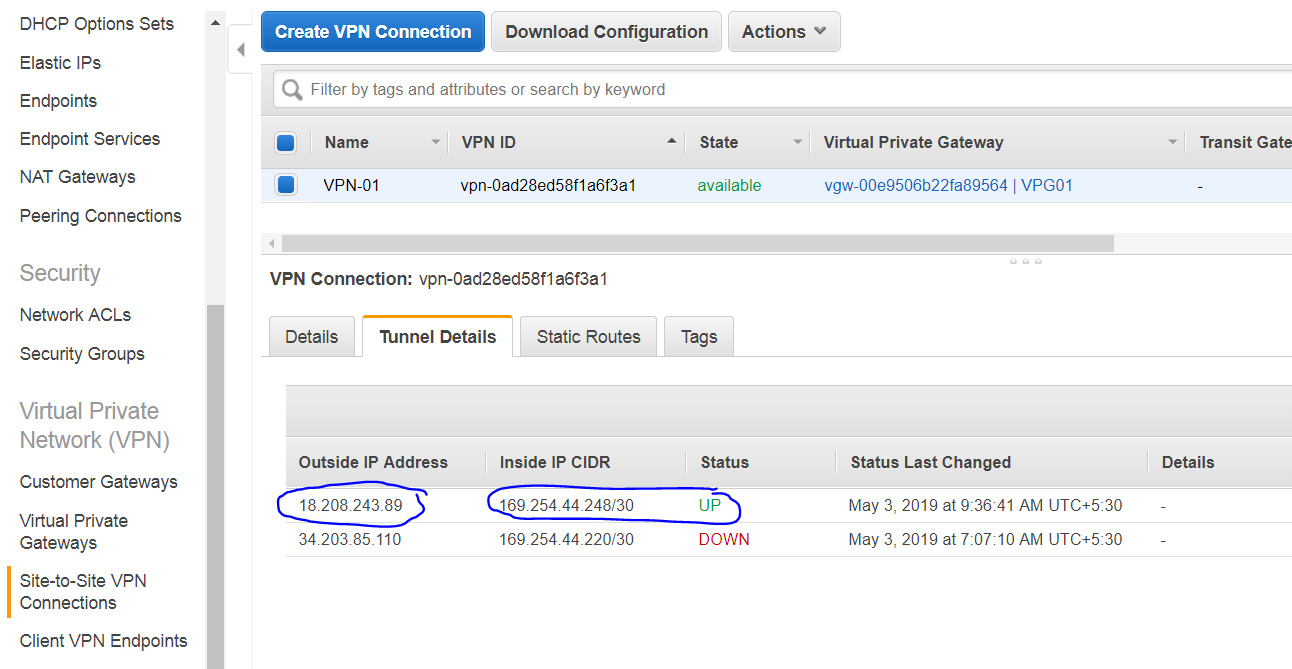
This shows that the Tunnel is up and fine.



Ping the Inside IP on the VPC side, and it should reply as the above screen.

The below screen shows the Tunnel is up on the VPC end as well.

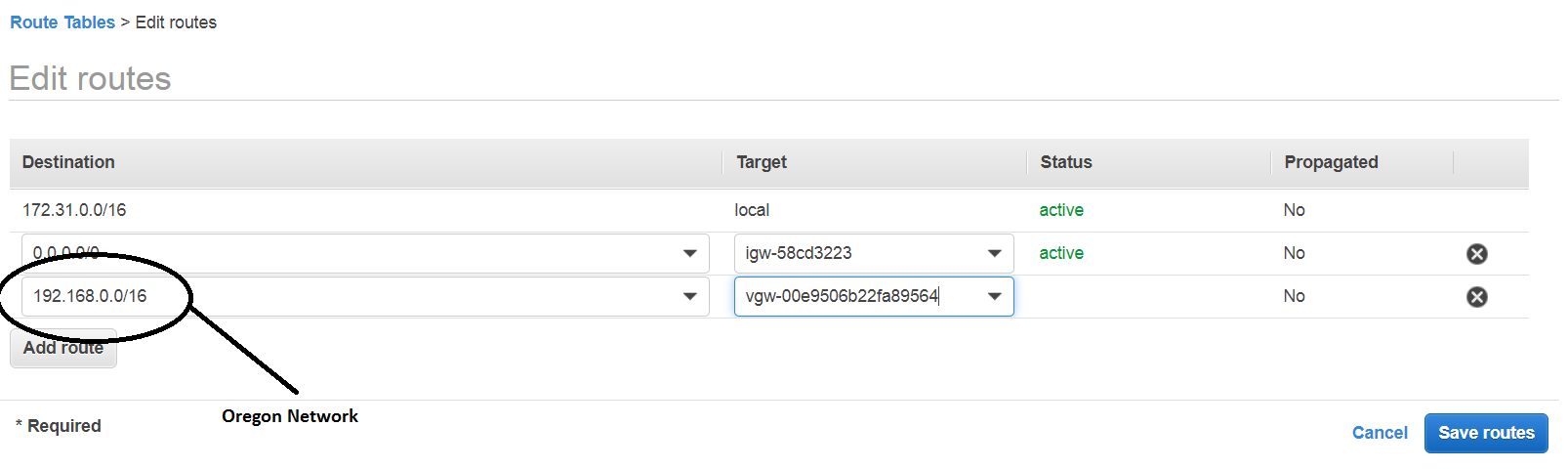
There is an “inside IP CIDR”.



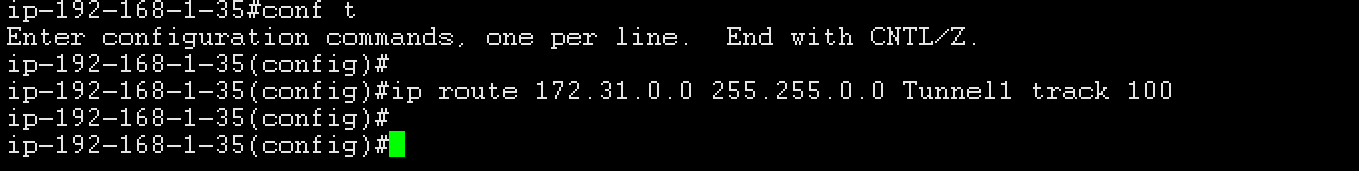
NOW, similarly configure the Tunnel 2 as well on the Cisco 1000 VPN box instance.

AWS provides 2 Tunnel for redundancy.

1. **Configure the Routing Table on both the sides.**
2. Configure the Routing table on the AWS VPC.

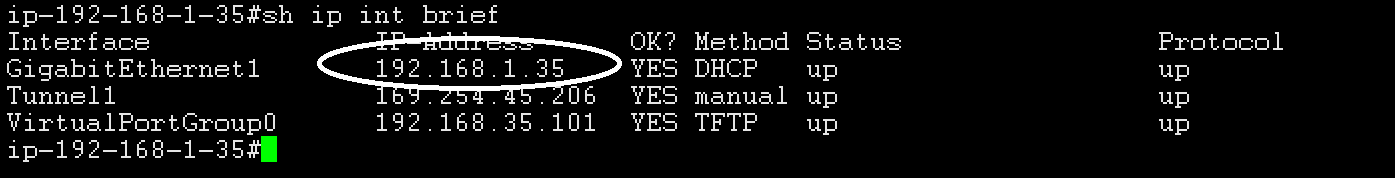


1. Configure the Routing on the Cisco VPN router.



**$ ip route 172.31.0.0 255.255.0.0 Tunnel1 track 100**

1. **Check if the EC2 instance is able to reach the on Prem datacenter**

****

**If the EC2 instance in the N.Virginia is able to Internal interface of the Cisco VPN Router, (ping to “192.168.1.35” from EC2 instance) then the setup is working fine.**

