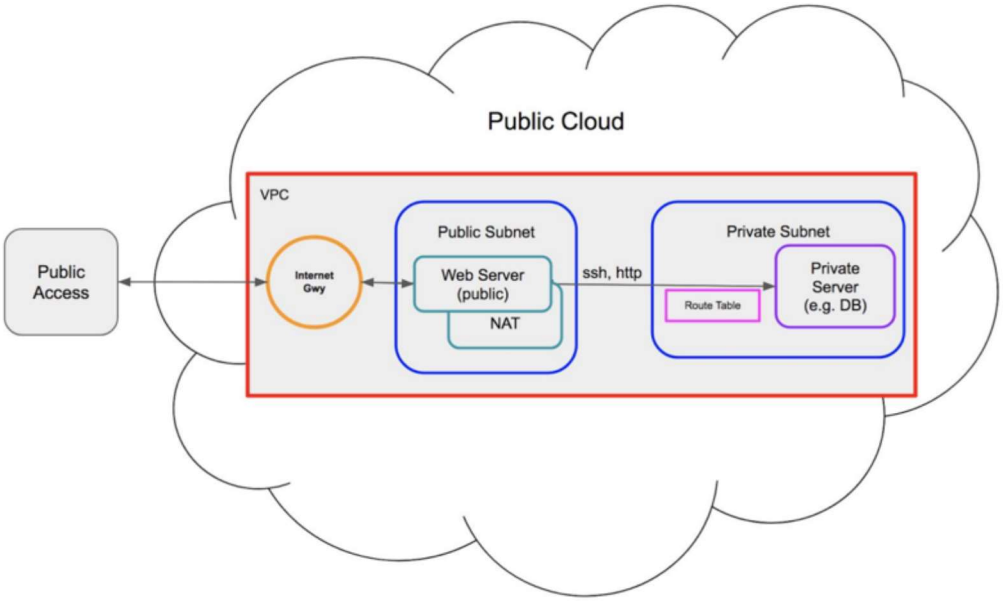
MSDS 7346
Cloud Computing
Mini Project 4 – VPC

Name: Mooyoung Lee

Virtual Private Cloud
In this lab you will design a VPC with a public subnet, a private subnet, and a network address translation (NAT) instance in the public subnet. A NAT instance enables instances in the private subnet to initiate outbound traffic to the Internet. This scenario is common when you have a public-facing web application, while maintaining back-end servers that aren't publicly accessible. A common example is a multi-tier website, with the web servers in a public subnet, and the database servers in a private subnet. You will set up security and routing allowing the web servers to communicate with the database servers. The instances in the public subnet can send outbound traffic directly to the Internet, whereas the instances in the private subnet cannot. The instances in the private subnet can access the Internet via the NAT instance in the public subnet. In a real-life situation, you can increase the network security using a network access control list (NACL), which is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet. In this mini project we will NOT by setting up NACL.
Upon completion of this mini project you will be able to create, configure and test the following:
• Virtual Private Cloud (VPC)
• Internet Gateway
• Public and private subnets (inbound/outbound rules)
• Security groups (inbound/outbound rules for multiple purposes)
• Pubic host (Web Server) or SSH access from the internet to private instances
• Network Address Translation (NAT) instance to grant access for private instances to perform operating system updates
• Route tables associated with public and private subnets

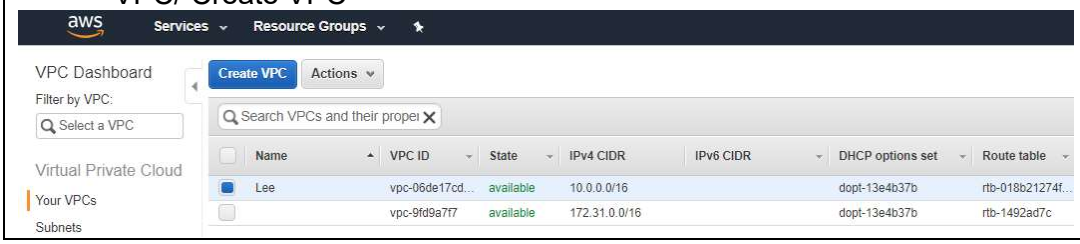
Lab Environment
The following picture represents the final configuration after you are done with your mini lab.



Submissions: Submit screenshots of each of the step.

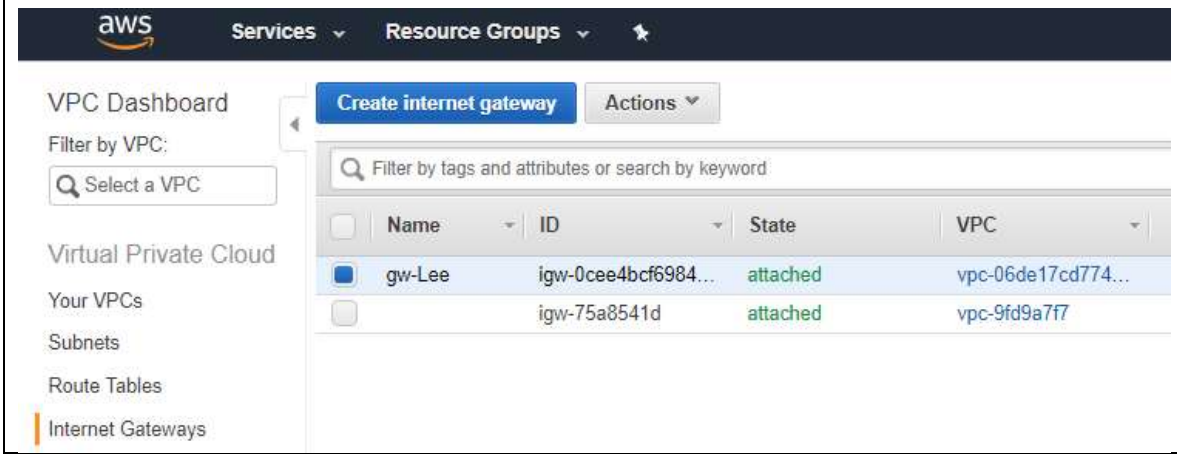
• Virtual Private Cloud (VPC)

- VPC/ Create VPC



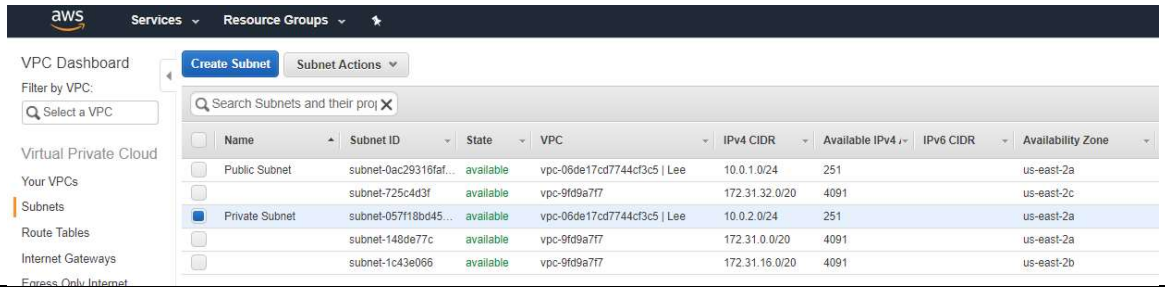
• Internet Gateway

- Internet Gateways/ Create internet gateway
- Internet Gateways/ Actions/ Attach to VPC



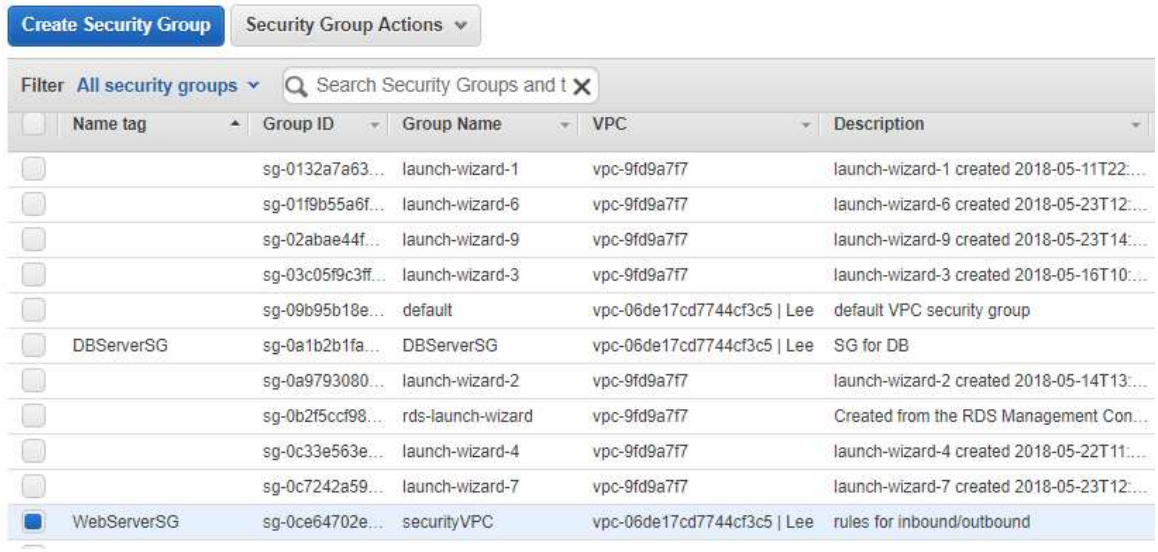
• Public and private subnets (inbound/outbound rules)

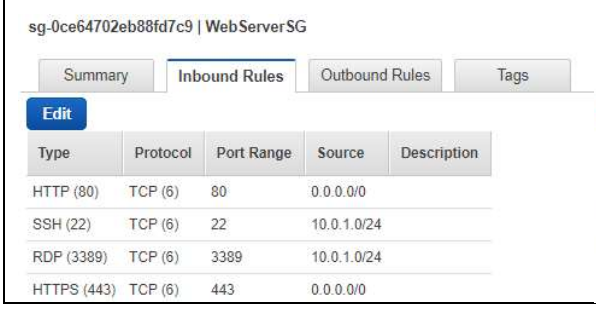
- Subnets/ Create Subnet w/ proper IPv4 CIDR block value

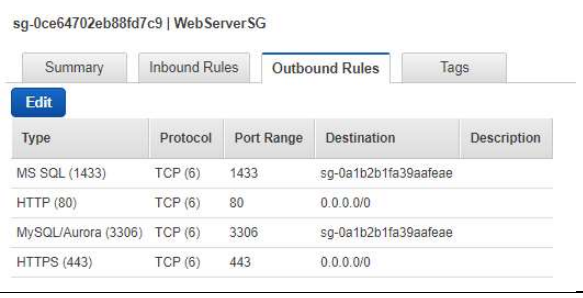


• Security groups (inbound/outbound rules for multiple purposes)

- Security Groups/ Create Security Group for Web server and DB server
- Assign proper inbound/outbound channels







• Pubic host (Web Server) or SSH access from the internet to private instances

- Ping to 'google.com' works from the public server (I used different VPC/EC2s than previous steps)

ec2-user@ip-10-0-2-132:~

```
e=31.4 ms
^C
--- google.com ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8012ms
rtt min/avg/max/mdev = 18.698/20.179/31.486/4.000 ms
[ec2-user@ip-10-0-2-132 ~]$ ping google.com
PING google.com (216.58.192.142) 56(84) bytes of data.
64 bytes from ord36s01-in-f14.1e100.net (216.58.192.142): icmp_seq=1 ttl=44 time
=31.4 ms
64 bytes from ord36s01-in-f142.1e100.net (216.58.192.142): icmp_seq=2 ttl=44 tim
e=31.5 ms
64 bytes from ord36s01-in-f14.1e100.net (216.58.192.142): icmp_seq=3 ttl=44 time
=31.4 ms
64 bytes from ord36s01-in-f142.1e100.net (216.58.192.142): icmp_seq=4 ttl=44 tim
e=31.5 ms
64 bytes from ord36s01-in-f14.1e100.net (216.58.192.142): icmp_seq=5 ttl=44 time
=31.5 ms
64 bytes from ord36s01-in-f142.1e100.net (216.58.192.142): icmp_seq=6 ttl=44 tim
e=31.4 ms
^C
--- google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 31.467/31.501/31.553/0.231 ms
[ec2-user@ip-10-0-2-132 ~]$
```

• Network Address Translation (NAT) instance to grant access for private instances to perform operating system updates

- Create NAT instance
- Associate the NAT instance w/ EC2 instance from 'EC2/ Network Interfaces'

Create NAT Gateway | Actions

Filter by tags and attributes or search by keyword

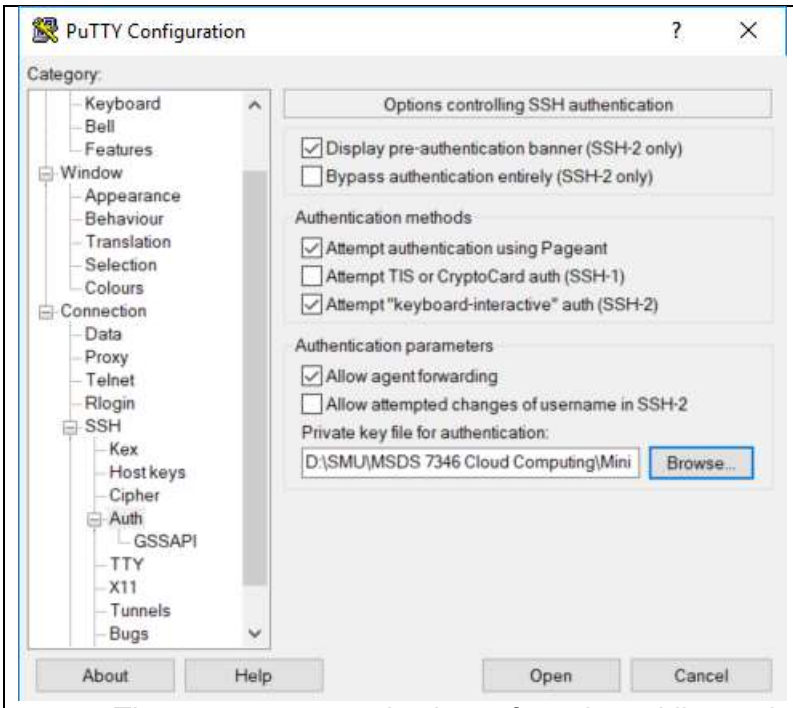
Name	NAT Gateway ID	Status	Status Message	Elastic IP Address	Private IP Address	Network Interface	VPC
nyNATGW	nat-02342e480e0...	available	-	18.221.154.34	10.0.2.238	eni-1e180c4f	vpc-03eec0cf4af0...

Create Network Interface | Attach | Detach | Delete | Actions

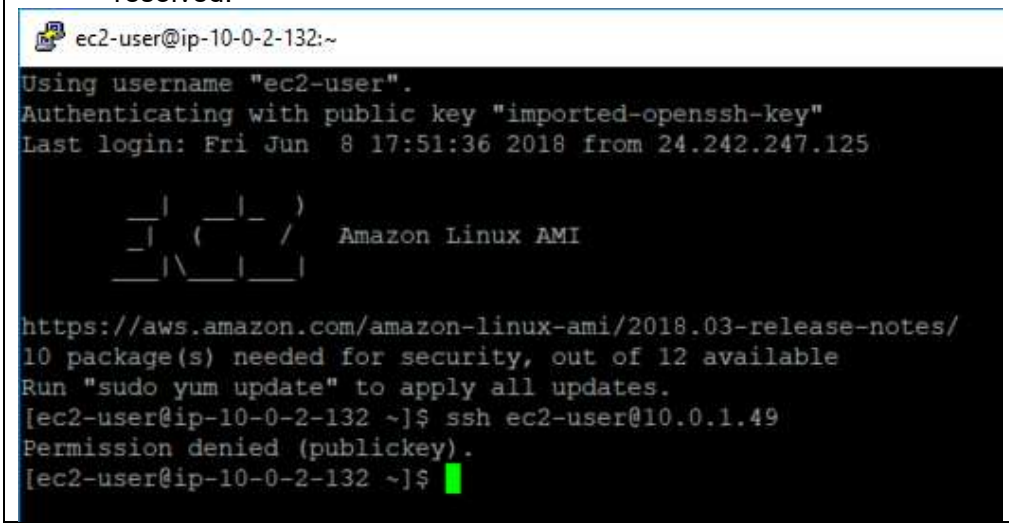
Filter by tags and attributes or search by keyword

Name	Network interfa	Subnet ID	VPC ID	Zone	Security groups
	eni-01b2f557e...	subnet-057f18...	vpc-06de17cd...	us-east-2a	launch-wizard-12
	eni-0a21c8426...	subnet-0ac293...	vpc-06de17cd...	us-east-2a	NATSG

- Select 'Allow agent forwarding' from Putty/ SSH/ Auth option in order to connect to private server from a public server.

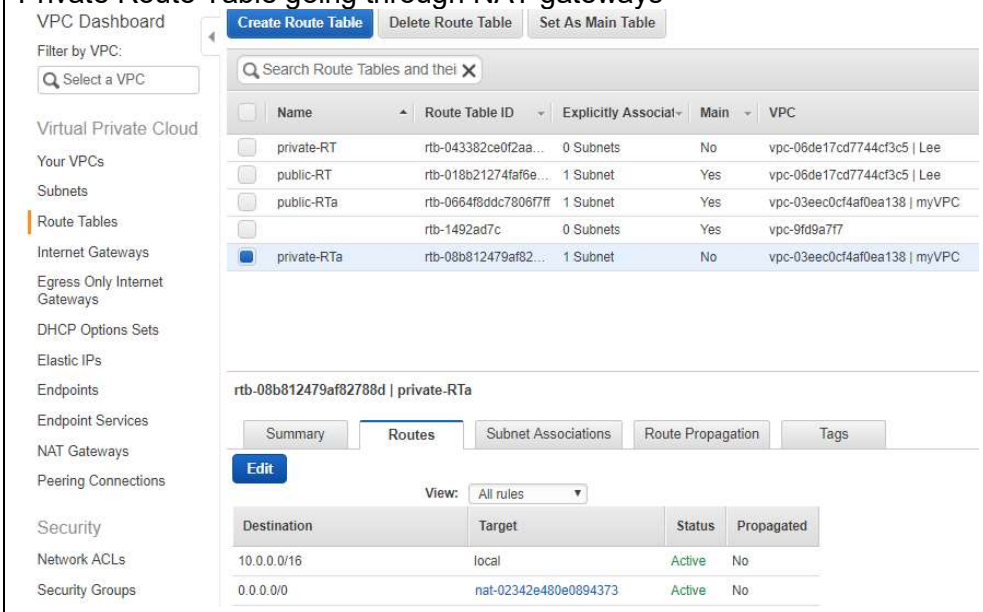


- There was a connection issue from the public to private server that cannot be resolved.

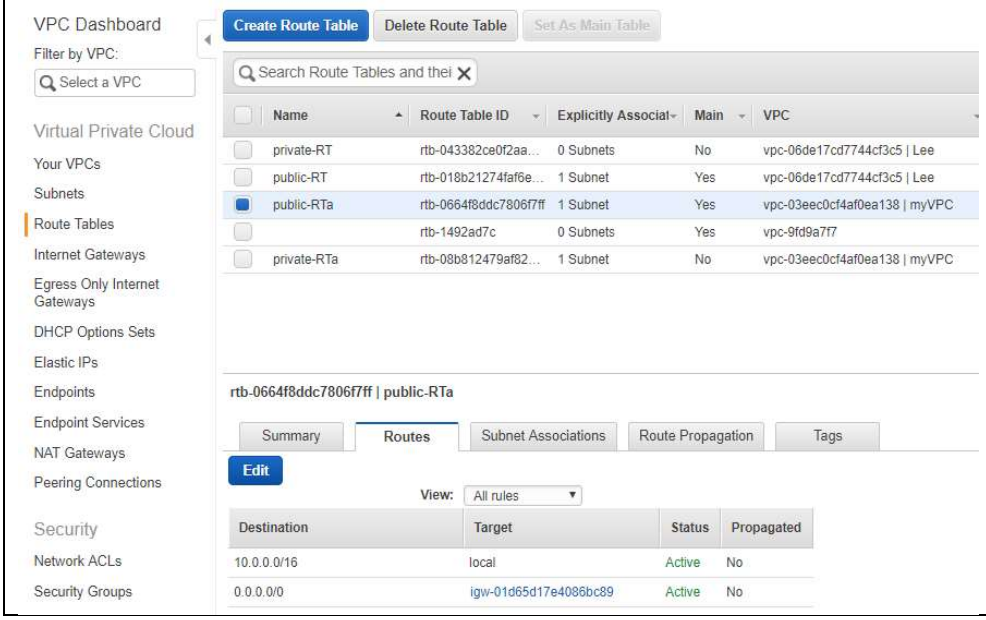


• Route tables associated with public and private subnets

Private Route Table going through NAT gateways



Public Route Table



Collaborators: None

Resources:

AWS documentation/ Scenario 2: VPC with Public and Private Subnets (NAT)

< https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html>

AWS- VPC Demo video

<https://www.youtube.com/watch?v=tD9vDv0uyI8>