

MSDS 7346

Cloud Computing

Mini Project 4 – VPC

Name: Mooyoung Lee

Virtual Private Cloud

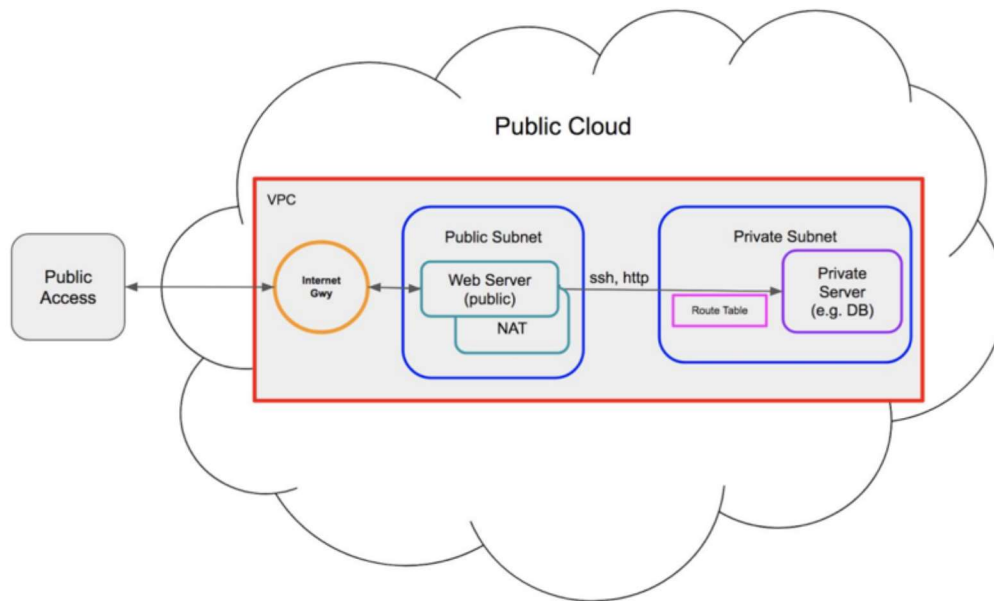
In this lab you will design a VPC with a public subnet, a private subnet, and a network address translation (NAT) instance in the public subnet. A NAT instance enables instances in the private subnet to initiate outbound traffic to the Internet. This scenario is common when you have a public-facing web 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 be 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)
- Public 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

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set	Route table
Lee	vpc-06de17cd...	available	10.0.0.0/16		dopt-13e4b37b	rtb-018b21274f...
	vpc-9fd9a7f7	available	172.31.0.0/16		dopt-13e4b37b	rtb-1492ad7c

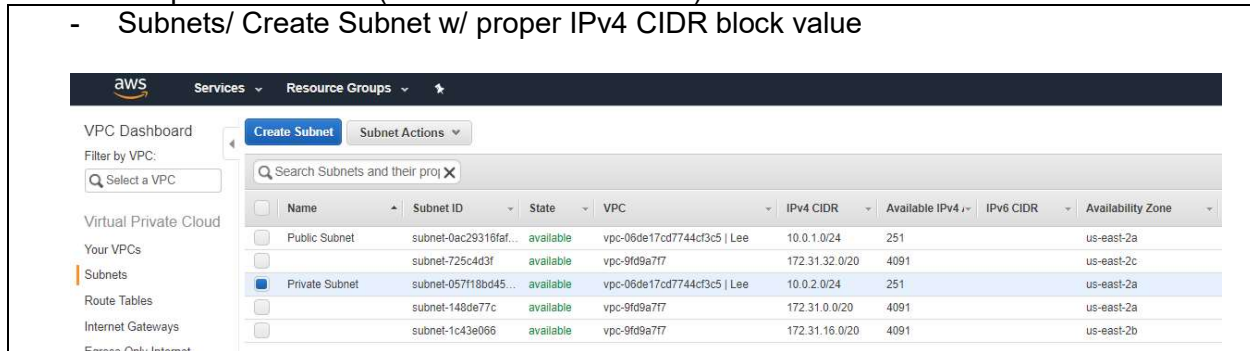
• Internet Gateway

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

Name	ID	State	VPC
gw-Lee	igw-0cee4bcf6984...	attached	vpc-06de17cd774...
	igw-75a8541d	attached	vpc-9fd9a7f7

- Public and private subnets (inbound/outbound rules)

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

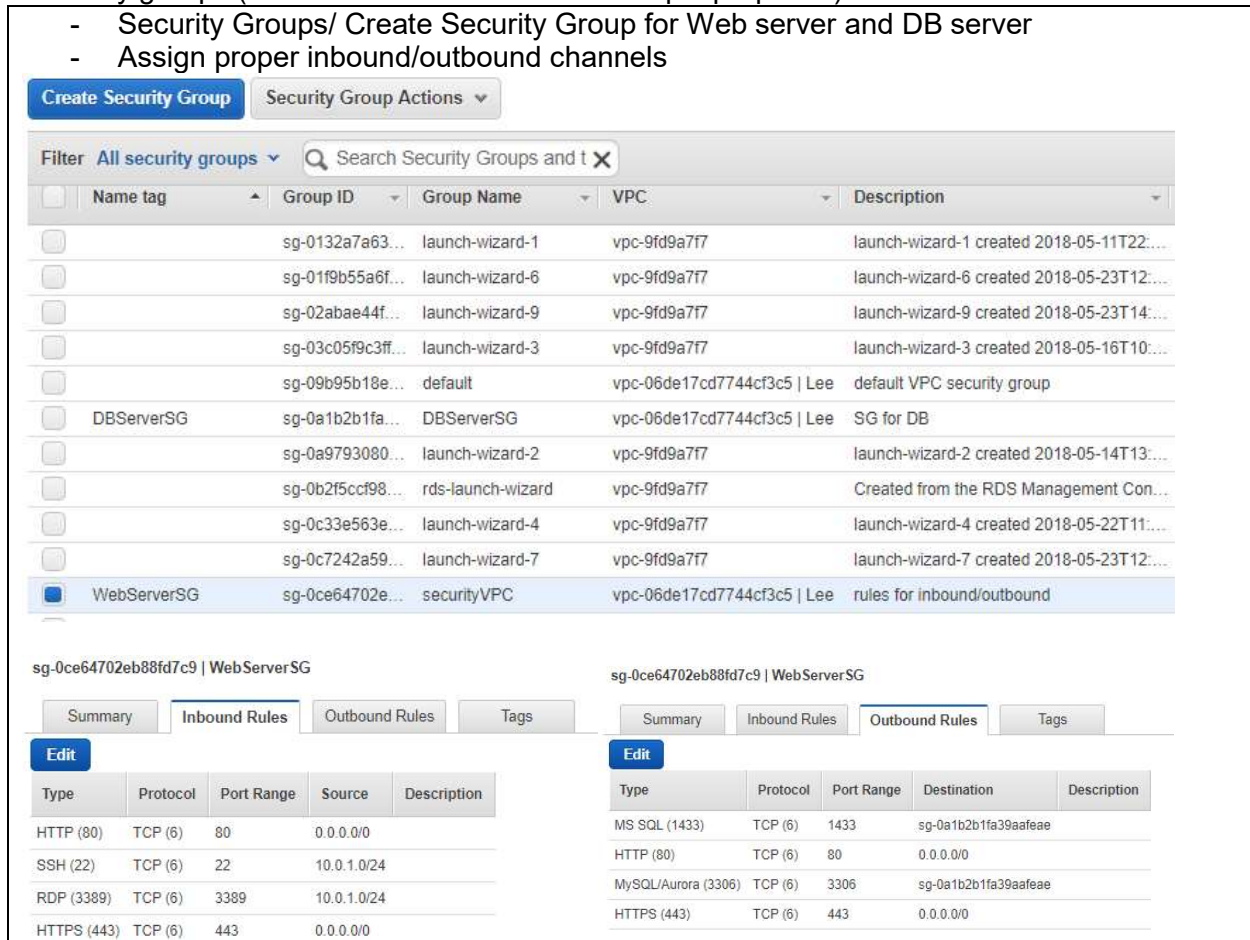


The screenshot shows the AWS VPC console. On the left, there's a sidebar with 'VPC Dashboard' and 'Virtual Private Cloud' sections. The main area displays a table of subnets. The table has columns: Name, Subnet ID, State, VPC, IPv4 CIDR, Available IPv4, IPv6 CIDR, and Availability Zone. One subnet is selected: 'Private Subnet' with ID 'subnet-057118bd45...', state 'available', VPC 'vpc-06de17cd7744cf3c5 | Lee', IPv4 CIDR '10.0.2.0/24', and Availability Zone 'us-east-2a'.

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone
Public Subnet	subnet-0ac29316faf...	available	vpc-06de17cd7744cf3c5 Lee	10.0.1.0/24	251		us-east-2a
	subnet-725c4d3f	available	vpc-9fd9a7f7	172.31.32.0/20	4091		us-east-2c
Private Subnet	subnet-057118bd45...	available	vpc-06de17cd7744cf3c5 Lee	10.0.2.0/24	251		us-east-2a
	subnet-148de77c	available	vpc-9fd9a7f7	172.31.0.0/20	4091		us-east-2a
	subnet-1c43e066	available	vpc-9fd9a7f7	172.31.16.0/20	4091		us-east-2b

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

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



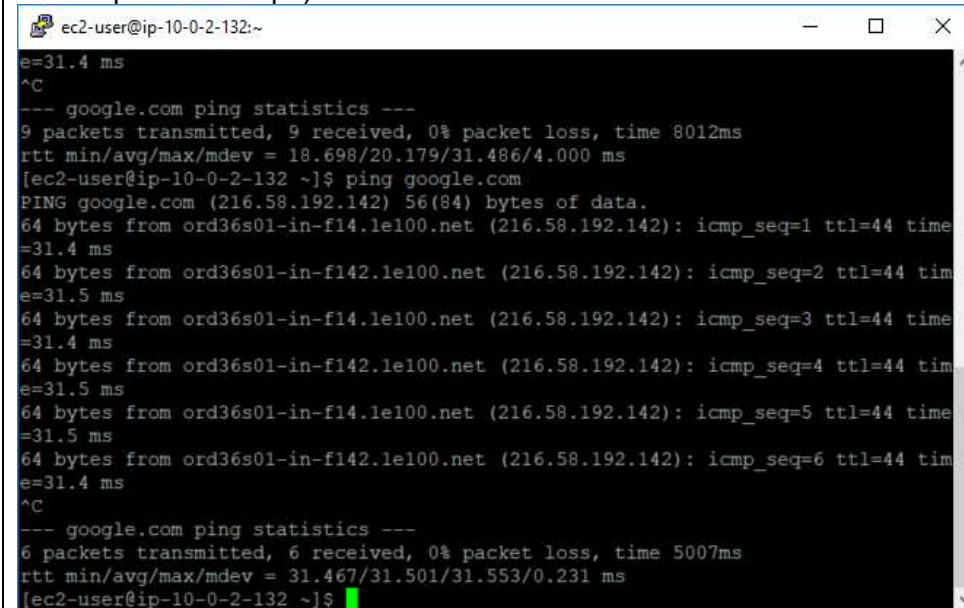
The screenshot shows the AWS Security Groups console. The top section lists security groups with columns: Name tag, Group ID, Group Name, VPC, and Description. 'WebServerSG' is selected. Below, the 'Inbound Rules' tab is active, showing a table of rules. The rules table has columns: Type, Protocol, Port Range, Source, and Description. The rules are for HTTP (80), SSH (22), RDP (3389), and HTTPS (443), all with source '0.0.0.0/0'.

Name tag	Group ID	Group Name	VPC	Description
	sg-0132a7a63...	launch-wizard-1	vpc-9fd9a7f7	launch-wizard-1 created 2018-05-11T22:...
	sg-01f9b55a6f...	launch-wizard-6	vpc-9fd9a7f7	launch-wizard-6 created 2018-05-23T12:...
	sg-02abae44f...	launch-wizard-9	vpc-9fd9a7f7	launch-wizard-9 created 2018-05-23T14:...
	sg-03c05f9c3ff...	launch-wizard-3	vpc-9fd9a7f7	launch-wizard-3 created 2018-05-16T10:...
	sg-09b95b18e...	default	vpc-06de17cd7744cf3c5 Lee	default VPC security group
DBServerSG	sg-0a1b2b1fa...	DBServerSG	vpc-06de17cd7744cf3c5 Lee	SG for DB
	sg-0a9793080...	launch-wizard-2	vpc-9fd9a7f7	launch-wizard-2 created 2018-05-14T13:...
	sg-0b2f5ccf98...	rds-launch-wizard	vpc-9fd9a7f7	Created from the RDS Management Con...
	sg-0c33e563e...	launch-wizard-4	vpc-9fd9a7f7	launch-wizard-4 created 2018-05-22T11:...
	sg-0c7242a59...	launch-wizard-7	vpc-9fd9a7f7	launch-wizard-7 created 2018-05-23T12:...
WebServerSG	sg-0ce64702e...	securityVPC	vpc-06de17cd7744cf3c5 Lee	rules for inbound/outbound

Type	Protocol	Port Range	Source	Description
HTTP (80)	TCP (6)	80	0.0.0.0/0	
SSH (22)	TCP (6)	22	10.0.1.0/24	
RDP (3389)	TCP (6)	3389	10.0.1.0/24	
HTTPS (443)	TCP (6)	443	0.0.0.0/0	

- Public 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)

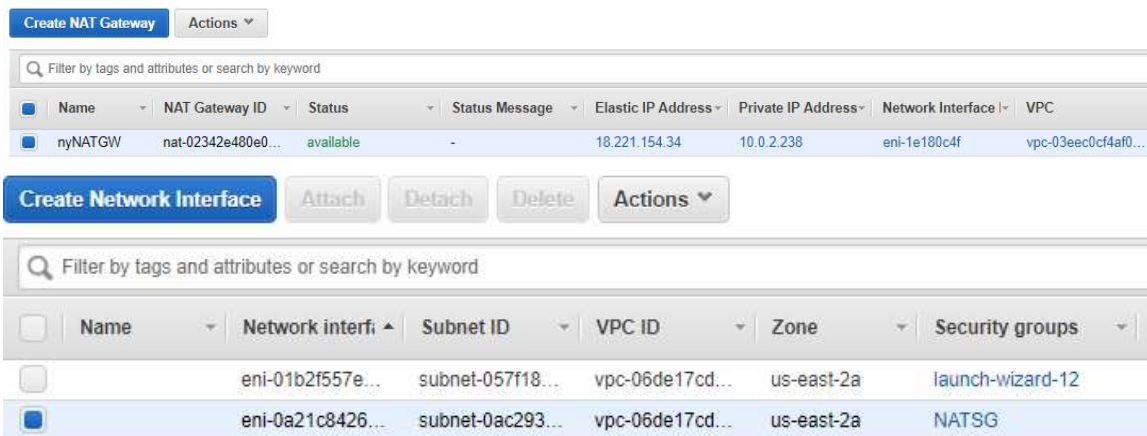


```

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'

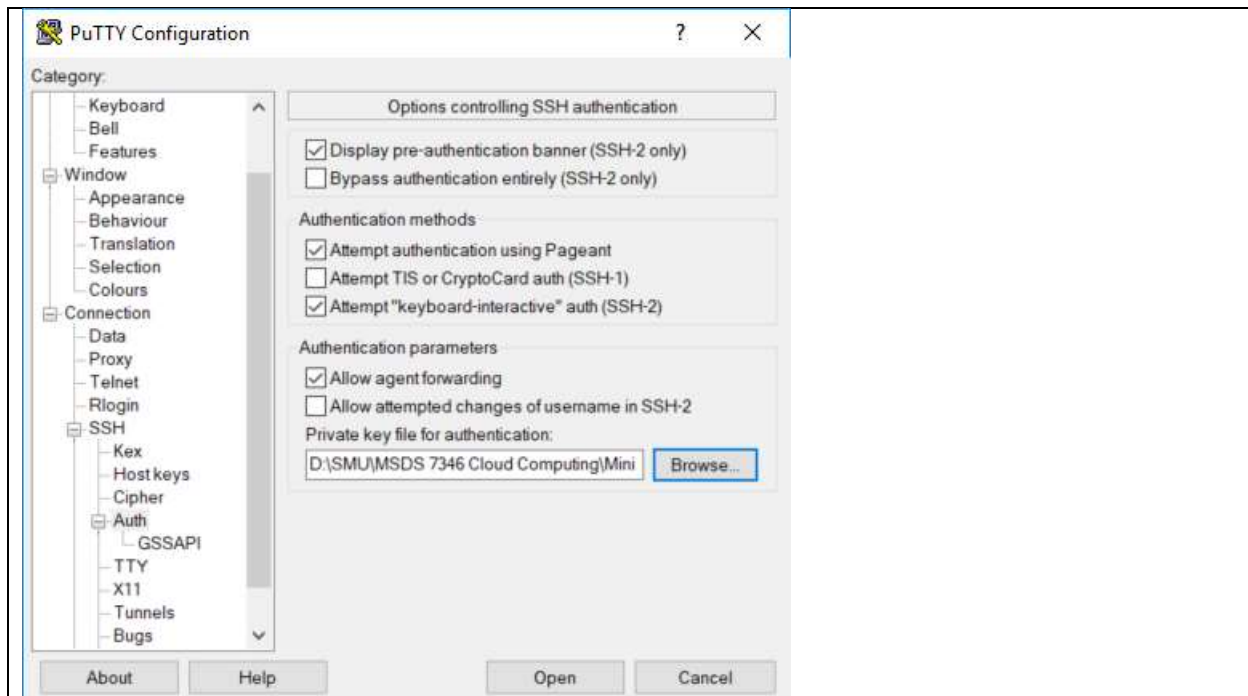


The first screenshot shows the 'Create NAT Gateway' page in the AWS Management Console. It displays a table with one NAT Gateway named 'nyNATGW' with ID 'nat-02342e480e...', status 'available', and associated Elastic IP '18.221.154.34' and Private IP '10.0.2.238'. The second screenshot shows the 'Create Network Interface' page, displaying a table with two network interfaces. The first is 'eni-01b2f557e...' associated with 'launch-wizard-12'. The second is 'eni-0a21c8426...' associated with 'NATSG'.

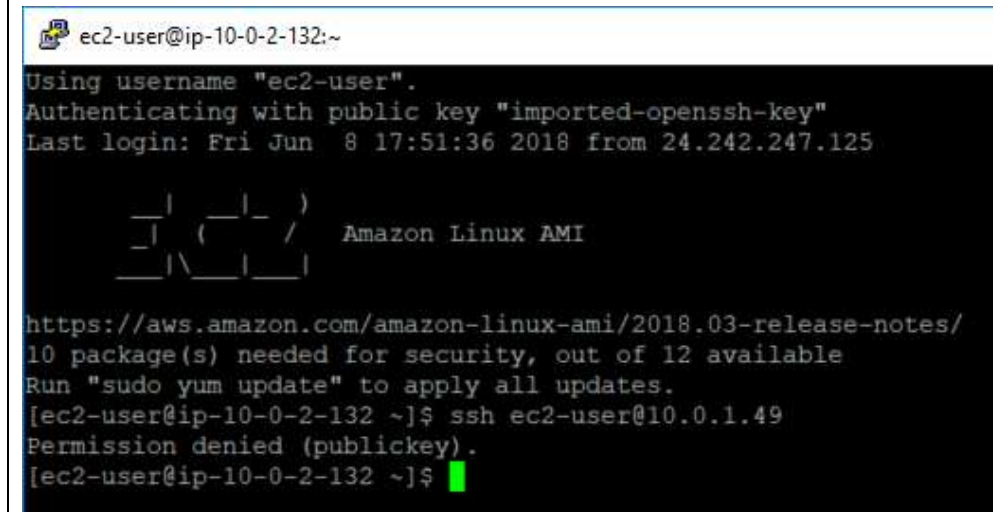
Name	NAT Gateway ID	Status	Status Message	Elastic IP Address	Private IP Address	Network Interface	VPC
nyNATGW	nat-02342e480e...	available	-	18.221.154.34	10.0.2.238	eni-1e180c4f	vpc-03eec0cf4af0...

Name	Network interface	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

VPC Dashboard

Filter by VPC:

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

Security

Network ACLs

Security Groups

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their VPCs

Name	Route Table ID	Explicitly Associated	Main	VPC
private-RT	rtb-043382ce0f2aa...	0 Subnets	No	vpc-06de17cd7744cf3c5 Lee
public-RT	rtb-018b21274faf6e...	1 Subnet	Yes	vpc-06de17cd7744cf3c5 Lee
public-RTa	rtb-0664f8ddc7806f7ff	1 Subnet	Yes	vpc-03eec0cf4af0ea138 myVPC
private-RTa	rtb-1492ad7c	0 Subnets	Yes	vpc-9fd9a7f7
private-RTa	rtb-08b812479af82...	1 Subnet	No	vpc-03eec0cf4af0ea138 myVPC

rtb-08b812479af82788d | private-RTa

Summary Routes Subnet Associations Route Propagation Tags

Edit

View: All rules

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	nat-02342e480e0894373	Active	No

Public Route Table

VPC Dashboard

Filter by VPC:

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

Security

Network ACLs

Security Groups

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their VPCs

Name	Route Table ID	Explicitly Associated	Main	VPC
private-RT	rtb-043382ce0f2aa...	0 Subnets	No	vpc-06de17cd7744cf3c5 Lee
public-RT	rtb-018b21274faf6e...	1 Subnet	Yes	vpc-06de17cd7744cf3c5 Lee
public-RTa	rtb-0664f8ddc7806f7ff	1 Subnet	Yes	vpc-03eec0cf4af0ea138 myVPC
private-RTa	rtb-1492ad7c	0 Subnets	Yes	vpc-9fd9a7f7
private-RTa	rtb-08b812479af82...	1 Subnet	No	vpc-03eec0cf4af0ea138 myVPC

rtb-0664f8ddc7806f7ff | public-RTa

Summary Routes Subnet Associations Route Propagation Tags

Edit

View: All rules

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-01d65d17e4086bc89	Active	No

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=tD9vDv0uyl8>>