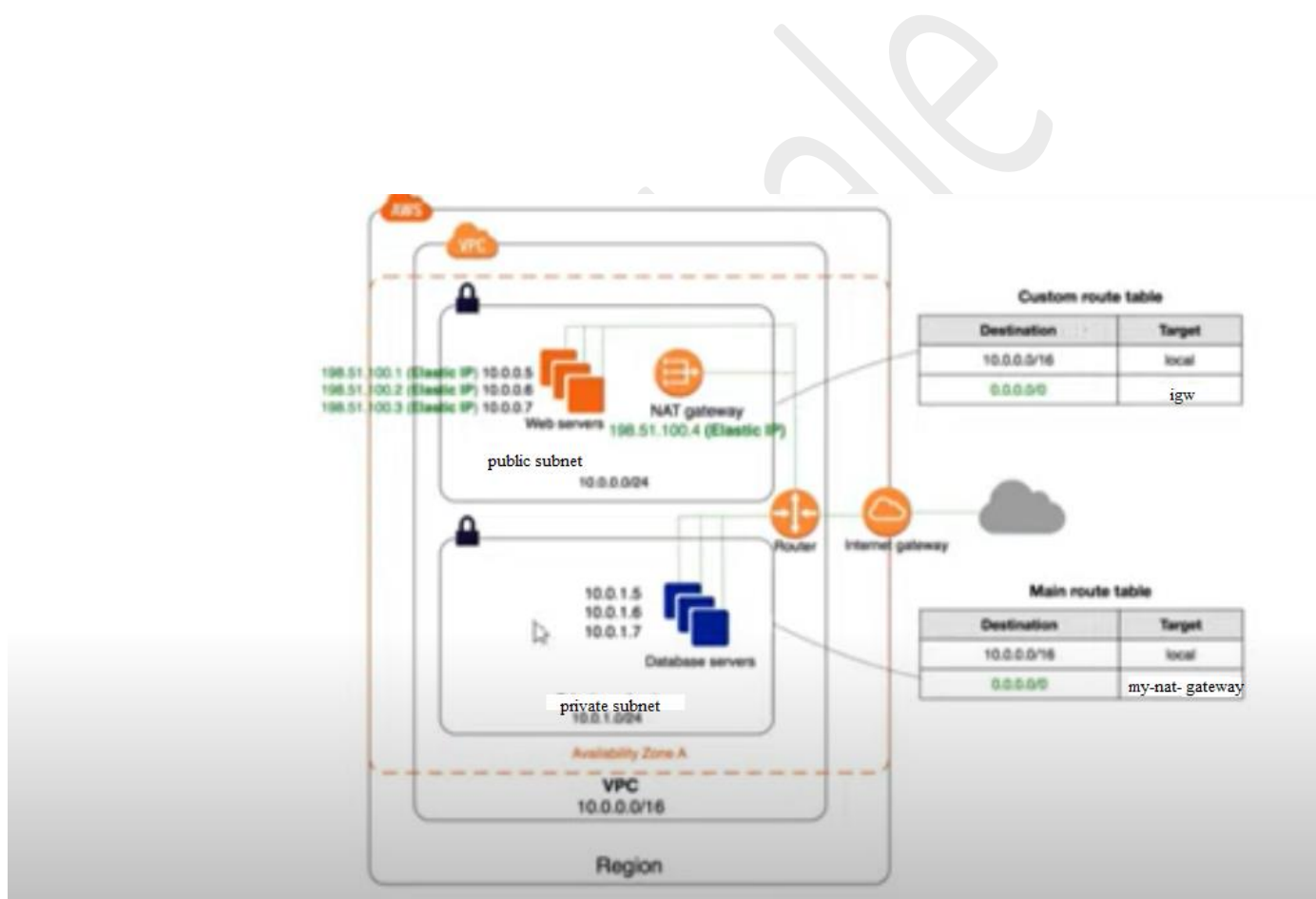


AWS VPC with public, private subnet and NAT Gateway

Create custom VPC with two subnet one as public & other as private subnet add Internet gateway to custom VPC. Create route table for each subnet and add one windows instances on each subnet and connect public subnet to internet gateway and private subnet to NAT gateway to access the internet securely.



Step:1 Created custom VPC *myvpc*.

vpc-0c24f95465f636441 / myvpc

Actions

DetailsInfo

VPC ID vpc-0c24f95465f636441	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP options set dopt-002d7893e45bc677d	Route table rtb-0abed1be27dba6449	Network ACL acl-03db6458dd90fb6ba
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -	IPv6 CIDR (Network border group) -
Owner ID 405170431204			

CIDRs

Flow logs

Tags

IPv4 CIDRsInfo

CIDR	Status
------	--------

Step: 2 Created two subnets as

1) Public subnet

subnet-0555dc5da18c81f78 / publicsubnet

Actions

Details

Subnet ID subnet-0555dc5da18c81f78	State Available	VPC vpc-0c24f95465f636441 myvpc	IPv4 CIDR 10.0.0.0/24
Available IPv4 addresses 249	IPv6 CIDR -	Availability Zone us-east-1e	Availability Zone ID use1-az3
Network border group us-east-1	Route table rtb-0359e376e805a65f0 publicroute	Network ACL acl-03db6458dd90fb6ba	Default subnet No
Auto-assign public IPv4 address No	Auto-assign IPv6 address No	Auto-assign customer-owned IPv4 address No	Customer-owned IPv4 pool -
Outpost ID -	Owner 405170431204	Subnet ARN arn:aws:ec2:us-east-1:405170431204:subnet/subnet-0555dc5da18c81f78	

2) Private subnet

subnet-0038e5e8cca4c50aa / privatesubnet

Actions

Details

Subnet ID subnet-0038e5e8cca4c50aa	State Available	VPC vpc-0c24f95465f636441 myvpc	IPv4 CIDR 10.0.1.0/24
Available IPv4 addresses 250	IPv6 CIDR -	Availability Zone us-east-1e	Availability Zone ID use1-az3
Network border group us-east-1	Route table rtb-038498e37db4d9779 privateroute	Network ACL acl-03db6458dd90fb6ba	Default subnet No
Auto-assign public IPv4 address No	Auto-assign IPv6 address No	Auto-assign customer-owned IPv4 address No	Customer-owned IPv4 pool -
Outpost ID -	Owner 405170431204	Subnet ARN arn:aws:ec2:us-east-1:405170431204:subnet/subnet-0038e5e8cca4c50aa	

Step: 3 Created one Internet Gateway *myigw* and connected to custom VPC *myvpc*.

VPC > Internet gateways > igw-02bbf749e49627051

igw-02bbf749e49627051 / myigw

Details Info

Internet gateway ID igw-02bbf749e49627051	State Attached	VPC ID vpc-0c24f95465f636441 myvpc	Owner 405170431204
--	-------------------	---	-----------------------

Step: 4 Created two route table and private & public subnet associated to these *privateroute* & *publicroute* route table respectively after that added route information related to internet gateway in *publicroute* table.

Create route table

Actions

Filter by tags and attributes or search by keyword

1 to 4 of 4

Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
rtb-0359e376e805a65f0	subnet-0555dc5da18c81f78	-	No	vpc-0c24f95465f636441 ...	405170431204

Route Table: rtb-0359e376e805a65f0

Summary

Routes

Subnet Associations

Edge Associations

Route Propagation

Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	igw-02bbf749e49627051	active	No

Step: 5 Launched two Microsoft windows server 2019 instances namely *public* and *private* in public and private subnet respectively.

Instances (2)

Info

Refresh

Connect

Instance state

Actions

Launch instances

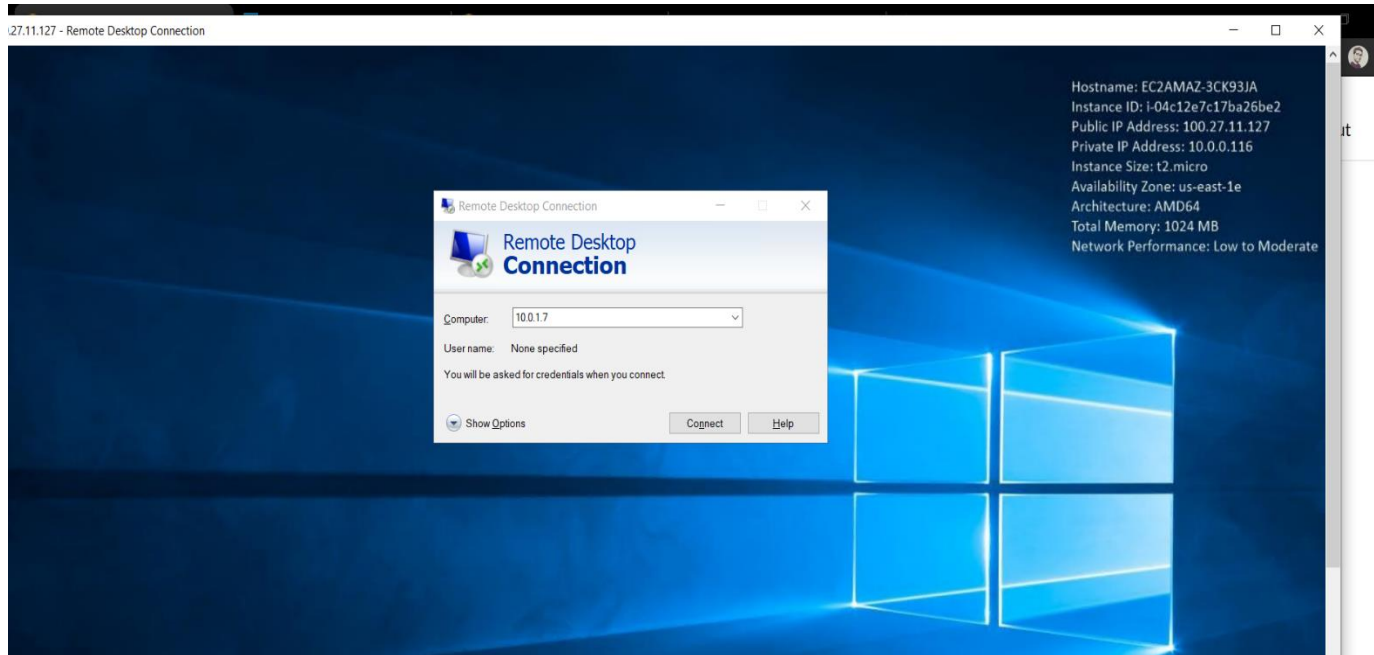
Filter instances

1

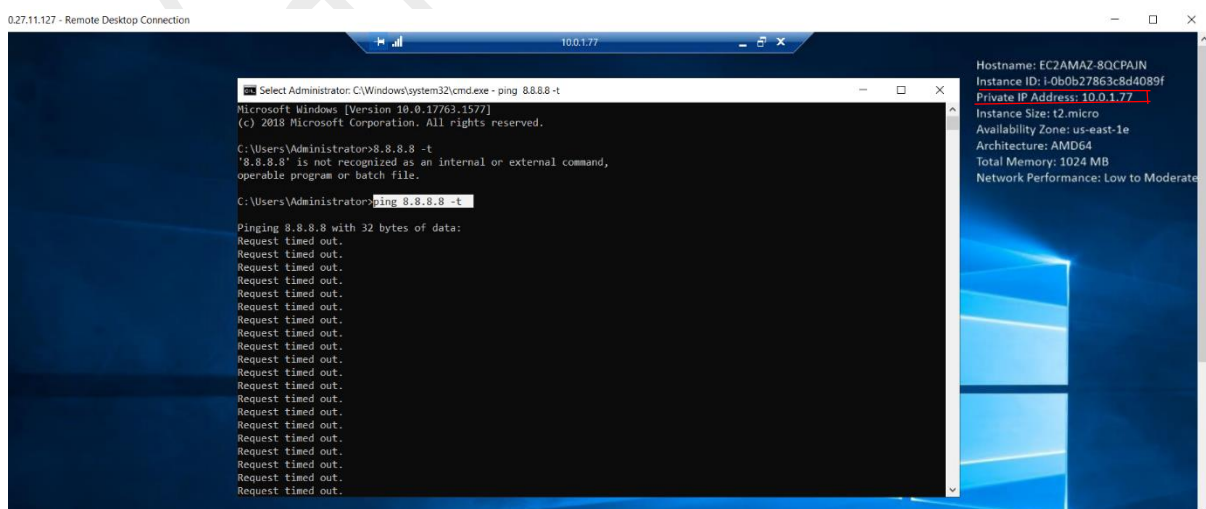
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input type="checkbox"/>	public	i-04c12e7c17ba26be2	Running	t2.micro	2/2 checks ...	No alarms	us-east-1e
<input type="checkbox"/>	private	i-0b0b27863c8d4089f	Running	t2.micro	2/2 checks ...	No alarms	us-east-1e

Step:6

- I. Public instance is accessible due to public IP so take RDP of public instance. Both instances present in one VPC so they can communicate with each other using IP.
- II. Take access of private instance using its private IP by public instance.



Step: 7 Check whether private instance able to access an internet or not.



Step:8 Add NAT gateway.

Private instance is not able to access internet due to private IP. Using NAT gateway private instance in private subnet can access internet securely. Here NAT gateway created in public subnet and connected to private subnet throw route table.

nat-0a8b0c1cc6ad5e120 / my-nat-gateway

Delete

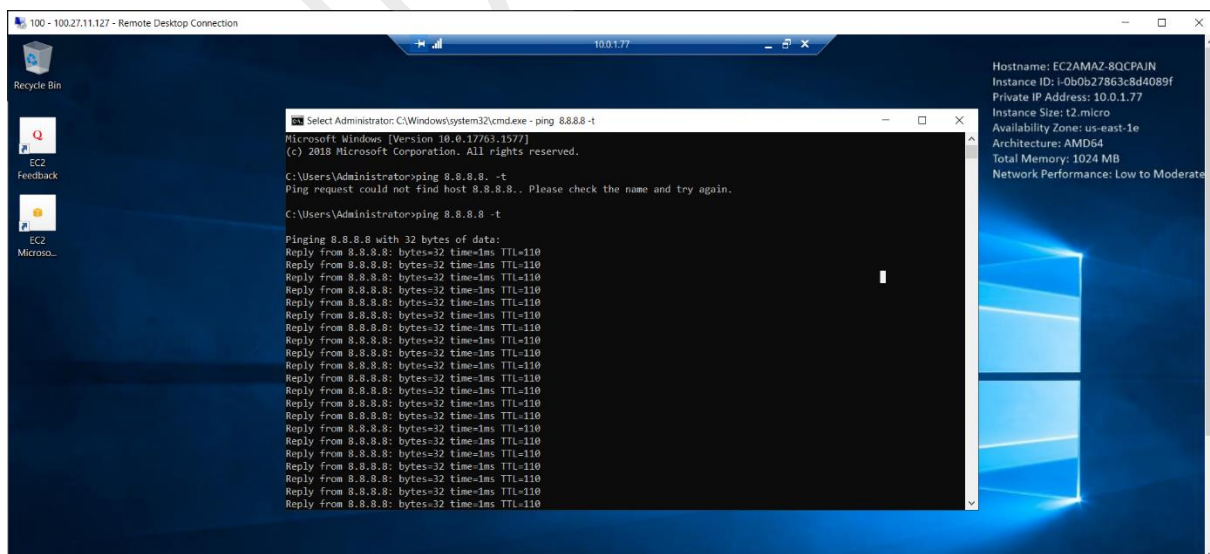
Details [Info](#)

NAT gateway ID	State	State message Info	Elastic IP address
nat-0a8b0c1cc6ad5e120	Available	-	54.163.227.164
Private IP address	Network interface ID	VPC	Subnet
10.0.0.98	eni-0647567d6c2d36a65	vpc-0c24f95465f636441 / myvpc	subnet-0555dc5da18c81f78 / publicsubnet
Created	Deleted		
2020/12/12 14:24 GMT+5:30	-		

Monitoring

Tags

In this picture you can see after adding NAT gateway private instance able to ping internet.



THANK YOU