AWS PROJECT

CREATE PUBLIC AND PRIVATE INSTANCES and ACCESS INTERNET FROM PRIVATE INSTANCE

FREDERIC TWAHIRWA
May 2018

TABLE OF CONTENTS

TABLE OF FIGURES

OBJECTIF

The objectif of this project is to set up a configuration within aws with a private instance addressable to internet.
To achieve this, we should have a NAT gateway configured in the public subnet and the private subnet traffic should be routed through this NAT gateway for internet access.

DIAGRAM

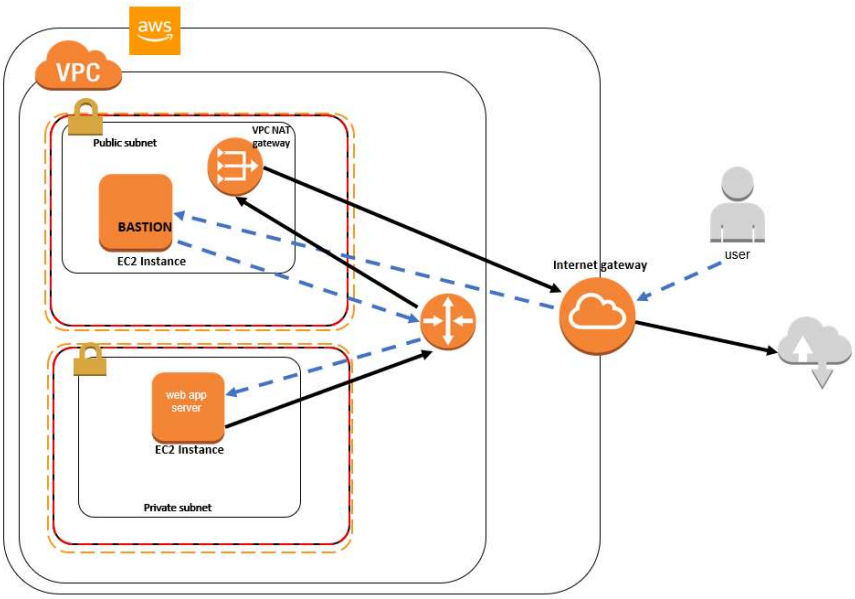

FIGURE 1: VPC WITH PUBLIC AND PRIVATE SUBNETS

CONFIGURATION

- ## CREATE A VPC AND SUBNETS

- ✓ Create a VPC
- ✓ Create a public subnet
  - Create an EC2 in the public subnet which will serves as a BASTION (this was created with a Linux t2.micro)
- ✓ Create a private subnet
  - ✓ Create an EC2 in the private subnet (this was created with a Linux t2.micro)
  - ✓

The 2 subnets were created in differents Availability Zones (eu_west_1b and eu_west_1c)

Below the screenshoots of the 2 instances

Public EC2 (with the IPv4 Public: 54.246.156.111 and Private IP: 10.0.1.113)

Filter by tags and attributes or search by keyword — 1 to 2 of 2

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarr	Public DNS (IPv4)
TWF_NAT/Bastion_PB	i-0a17f6675cba016f4	t2.micro	eu-west-1b	running	2/2 checks ...		
TWF_WEBSERVER_PV	i-0e7bb1698018a7a...	t2.micro	eu-west-1c	running	2/2 checks ...		

Instance: i-0a17f6675cba016f4 (TWF_NAT/Bastion_PB) **Public IP: 54.246.153.111**

Description | Status Checks | Monitoring | Tags

Instance ID	i-0a17f6675cba016f4	Public DNS (IPv4)	-
Instance state	running	IPv4 Public IP	54.246.153.111
Instance type	t2.micro	IPv6 IPs	-
Elastic IPs		Private DNS	ip-10-0-1-113.eu-west-1.compute.internal
Availability zone	eu-west-1b	Private IPs	10.0.1.113
Security groups	TWF_WEBSERVER_SG. view inbound rules	Secondary private IPs	
Scheduled events	No scheduled events	VPC ID	vpc-00d6a715bccbe6d17
AMI ID	amzn-ami-hvm-2018.03.0.20180508-x86_64-gp2 (ami-ca0135b3)	Subnet ID	subnet-040eadef575b8bc44
Platform	-	Network interfaces	eth0
IAM role	-	Source/dest. check	True
Key pair name	TWF_KEYPAIR_LP	T2 Unlimited	Disabled

FIGURE 2: PUBLIC INSTANCE CONFIGURATION

Private EC2 (withouth an IPv4 public, the Private IP is 10.0.2.11)

Filter by tags and attributes or search by keyword — 1 to 2 of 2

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarr	Public DNS (IPv4)
TWF_NAT/Bastion_PB	i-0a17f6675cba016f4	t2.micro	eu-west-1b	running	2/2 checks ...		
TWF_WEBSERVER_PV	i-0e7bb1698018a7a...	t2.micro	eu-west-1c	running	2/2 checks ...		

Instance: i-0e7bb1698018a7a07 (TWF_WEBSERVER_PV) **Private IP: 10.0.2.11**

Description | Status Checks | Monitoring | Tags

Instance ID	i-0e7bb1698018a7a07	Public DNS (IPv4)	-
Instance state	running	IPv4 Public IP	-
Instance type	t2.micro	IPv6 IPs	-
Elastic IPs		Private DNS	ip-10-0-2-11.eu-west-1.compute.internal
Availability zone	eu-west-1c	Private IPs	10.0.2.11
Security groups	TWF_WEBSERV_UNIX_PV. view inbound rules	Secondary private IPs	
Scheduled events	No scheduled events	VPC ID	vpc-00d6a715bccbe6d17
AMI ID	amzn-ami-hvm-2018.03.0.20180508-x86_64-gp2 (ami-ca0135b3)	Subnet ID	subnet-0351a753069563a58
Platform	-	Network interfaces	eth0
IAM role	-	Source/dest. check	True
Key pair name	TWF_KEYPAIR_LP	T2 Unlimited	Disabled
		Owner	192991303082

FIGURE 3: PRIVATE INSTANCE CONFIGURATION

▪ CREATE SECURITY GROUPS

- ✓ A security group which allow HTTP, HTTPS and SSH inbound traffic (and all traffic outbound) was created, this will be used by the Bastion (the name in this project is TWF_WEBSERVERS_SG)
- ✓ Another security group which allow SSH, HTTPand HTTPS inbound traffic only from the BASTION(and all traffic outbound) was created, this will be used by the Private Instance(the name in this project is TWF_WEBSERV_LINUX_PV

Below the screenshoots of the 2 security Groups

NAT/BASTION Security Groups:

search : tw Add filter 1 to 3 of 3

Name	Group ID	Group Name	VPC ID	Description
TWF_WEBSERV_LINUX_PV	sg-0aee583ac94c05461	TWF_WEBSERV_UNIX_PV	vpc-00d6a715bccbe6d17	Web servers linux private
TWF_DBSERVER_SG	sg-0bcfcd3ef011e3b73	TWF_DBSERVER_SG	vpc-00d6a715bccbe6d17	TWF DB SERVER SECURITY GROUPS
TWF_WEBSERVER_SG	sg-0d1007a5513bf448e	TWF_WEBSERVER_SG	vpc-00d6a715bccbe6d17	TWF WEBSERVER SECURITY GROUPS

Security Group: sg-0d1007a5513bf448e

Description | Inbound | Outbound | Tags

Edit

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	
SSH	TCP	22	0.0.0.0/0	
Custom TCP Rule	TCP	443	0.0.0.0/0	

FIGURE 4: BASTION SECURITY GROUP CONFIGURATION

Security Group: sg-0d1007a5513bf448e

Description | Inbound | Outbound | Tags

Edit

Type	Protocol	Port Range	Destination	Description
All traffic	All	All	0.0.0.0/0	

FIGURE 5: BASTION SECURITY GROUP CONFIGURATION (OUTBOUND)

PRIVATE SG

search : tw Add filter 1 to 3 of 3

Name	Group ID	Group Name	VPC ID	Description
TWF_WEBSERV_LINUX_PV	sg-0aee583ac94c05461	TWF_WEBSERV_UNIX_PV	vpc-00d6a715bccbe6d17	Web servers linux private
TWF_DBSERVER_SG	sg-0bcfcd3ef011e3b73	TWF_DBSERVER_SG	vpc-00d6a715bccbe6d17	TWF DB SERVER SECURITY GROUPS
TWF_WEBSERVER_SG	sg-0d1007a5513bf448e	TWF_WEBSERVER_SG	vpc-00d6a715bccbe6d17	TWF WEBSERVER SECURITY GROUPS

Security Group: sg-0aee583ac94c05461

Description | Inbound | Outbound | Tags

Edit

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	sg-0d1007a5513bf448e (TWF_WEBSI	
SSH	TCP	22	0.0.0.0/0	
Custom TCP Rule	TCP	443	sg-0d1007a5513bf448e (TWF_WEBSI	

FIGURE 6: PRIVATE WEBSERVER SECURITY GROUP CONFIGURATION (INBOUND)

Security Group: sg-0aee583ac94c05461

Description | Inbound | Outbound | Tags

Edit

Type	Protocol	Port Range	Destination	Description
All traffic	All	All	0.0.0.0/0	

FIGURE 7: PRIVATE WEBSERVER SECURITY GROUP CONFIGURATION (OUTBOUND)

- ## CREATE AN ELASTIC IP

Create an Elastic IP address with any instance which will be associated to our VPC

Allocate new address Actions 1 to 1 of 1

Name	Elastic IP	Allocation ID	Instance	Private IP address	Scope	Association ID	Network Interface ID
	54.246.163.60	eipalloc-05532b00a...	-	10.0.1.107	vpc	eipassoc-900aa05d	eni-c17727f4

Address: 54.246.163.60

Description | Tags

Elastic IP	54.246.163.60	Allocation ID	eipalloc-05532b00aa31917a5
Instance	-	Private IP address	10.0.1.107
Scope	vpc	Association ID	eipassoc-900aa05d
Public DNS	-	Network interface ID	eni-c17727f4

FIGURE 8: EIP CONFIGURATION

- **KEY PAIR was generated**

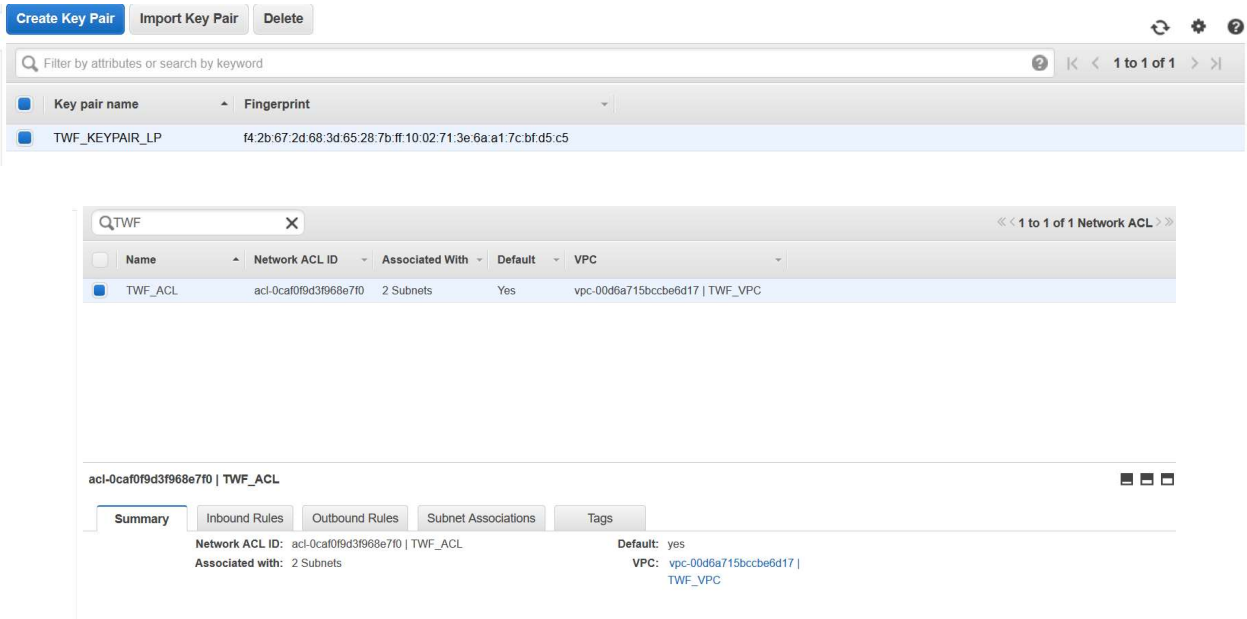

FIGURE 9: KEY PAIR CONFIGURATION

- ## INTERNET GATEWAY AND NAT GATEWAY

Internet gateway and nat gateway were created
Internet Gateway is the interface between the VPC and the internet
NAT Gateway will enable the private subnet to access the internet

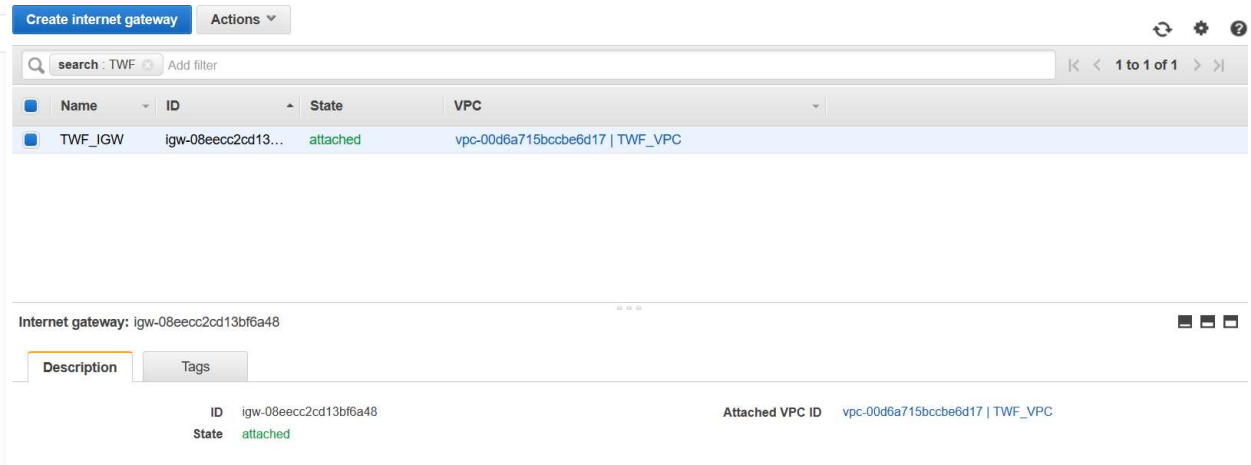

FIGURE 10: IGW CONFIGURATION

NAT GATEWAY

Create NAT Gateway | Actions

Filter by tags and attributes or search by keyword — 1 to 1 of 1

Name	NAT Gateway ID	Status	Status Message	Elastic IP Address	Private IP Address	Network Interface	VPC	Subnet
	nat-0a2865b8196...	available	-	54.246.163.60	10.0.1.107	eni-c17727f4	vpc-00d6a715bcc...	subnet-040e

NAT Gateway: nat-0a2865b81963af8b1

Details | Monitoring | Tags

NAT Gateway ID	nat-0a2865b81963af8b1	Status	available
Status Message	-	Elastic IP Address	54.246.163.60
Private IP Address	10.0.1.107	Network Interface ID	eni-c17727f4
VPC	vpc-00d6a715bccbe6d17 | TWF_VPC	Subnet	subnet-040eadef575b8bc44 | 10.0.1.0_EU_WEST_1B_TWF_PUB
Created	May 26, 2018 at 5:14:01 PM UTC+2	Deleted	-

FIGURE 11: NAT GATEWAY CONFIGURATION

- ## ROUTE TABLES

Set up rules (Routes) that will direct network traffic flowing in and out the subnet
2 Routes tables were created, one with target the internet gateway and the second one with target the NAT
The public subnet will through Internet gateway
The public subnet will access internet through NAT
Below the screenshoots of the route tables and theirs routes and subnet associations

Route table to Internet gateway

TWF — 1 to 2 of 2 Route Tables

Name	Route Table ID	Explicitly Associat	Main	VPC
TWF_RTB	rtb-0daaf2325c3da07ac	1 Subnet	No	vpc-00d6a715bccbe6d17 | TWF_VPC
TWF_RTB_Main	rtb-0dd7fcdfcf084b04c	0 Subnets	Yes	vpc-00d6a715bccbe6d17 | TWF_VPC

rtb-0daaf2325c3da07ac | TWF_RTB

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-08eecc2cd13bf6a48	Active	No

FIGURE 12: ROUTE TABLE (IGW) -ROUTES CONFIGURATION

rtb-0daaf2325c3da07ac | TWF_RTB

Summary | Routes | **Subnet Associations** | Route Propagation | Tags

Edit

Subnet	IPv4 CIDR	IPv6 CIDR
subnet-040eadef575b8bc44 | 10.0.1.0_EU_WEST_1B_TWF_PUB	10.0.1.0/24	-

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Subnet	IPv4 CIDR	IPv6 CIDR
subnet-0351a753069563a58 | 10.0.2.0_EU_WEST_1C_TWF_PRV	10.0.2.0/24	-

FIGURE 13: ROUTE TABLE (IGW) -SUBNET ASSOCIATIONS CONFIGURATION

Route table to NAT (wich will be used by the private instance)

Create Route Table | Delete Route Table | Set As Main Table

TWF

Name	Route Table ID	Explicitly Associat	Main	VPC
TWF_RTB	rtb-0daaf2325c3da07ac	1 Subnet	No	vpc-00d6a715bccbe6d17 | TWF_VPC
TWF_RTB_Main	rtb-0dd7fcdfcf084b04c	0 Subnets	Yes	vpc-00d6a715bccbe6d17 | TWF_VPC

rtb-0dd7fcdfcf084b04c | TWF_RTB_Main

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-0a2865b81963af8b1	Active	No

FIGURE 14: ROUTE TABLE (NAT GATEWAY) -ROUTES CONFIGURATION

- SUBNETS AND ROUTE TABLES

PUBLIC subnet

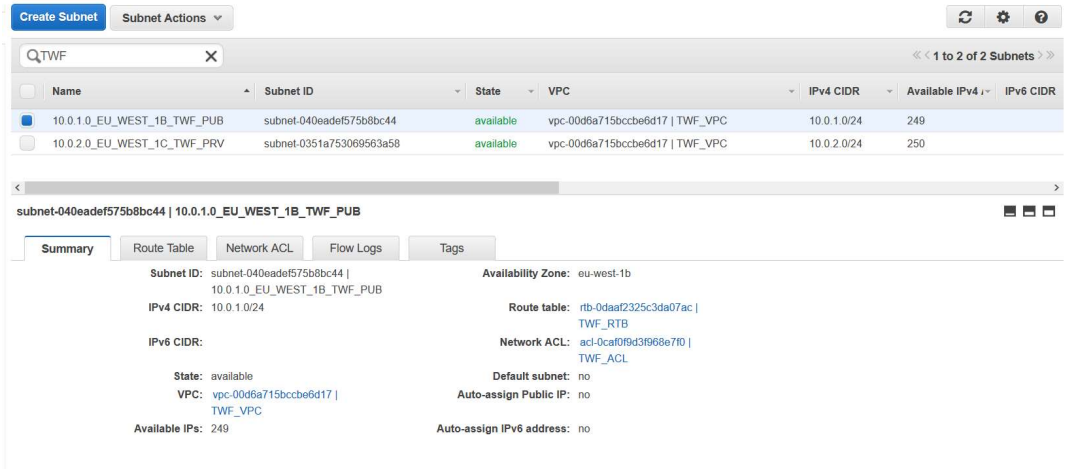

FIGURE 15: PUBLIC SUBNET CONFIGURATION -SUMMARY

FIGURE 16: PUBLIC SUBNET CONFIGURATION -ROUTE TABLE

PRIVATE Subnet

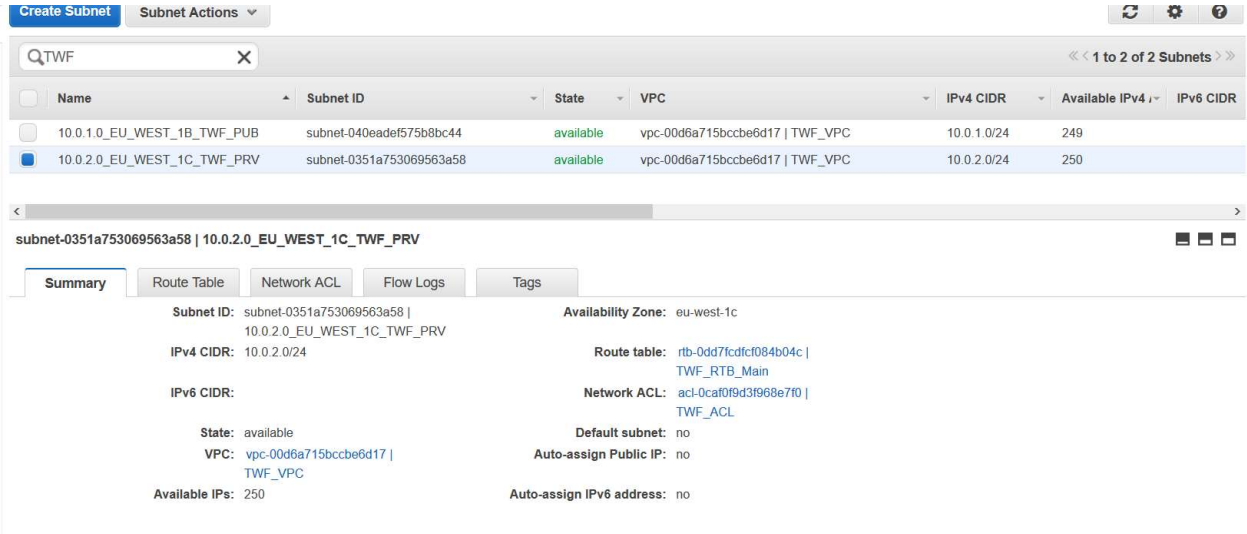

FIGURE 17: PRIVATE SUBNET CONFIGURATION -SUMMARY

FIGURE 18: PRIVATE SUBNET CONFIGURATION -ROUTE TABLE

RESULTS

Now we ssh the machine's residing on private subnet by using an instance from public subnet, which we can connect using internet

- ✓ Putty was used to ssh the public machine (the bastion)
- ✓ We ssh the private machine by the command **$ ssh** ec2-user@10.0.2.11
- ✓ On Private machine ping google.com

CONNECT SSH THROUGH

```
[ec2-user@ip-10-0-1-113 ~]$ ssh ec2-user@10.0.2.11
The authenticity of host '10.0.2.11 (10.0.2.11)' can't be established.
ECDSA key fingerprint is SHA256:VwjQQZLFgBd1hxiOq8iDJijaHINsA/toOKvTJ9LmwgA.
ECDSA key fingerprint is MD5:c7:d4:ad:c7:1c:50:7b:e6:cf:b1:02:a5:0a:3c:b5:73.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '10.0.2.11' (ECDSA) to the list of known hosts.

       __|  __|_  )
       _|  (     /   Amazon Linux AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
6 package(s) needed for security, out of 7 available
Run "sudo yum update" to apply all updates.
```

FIGURE 19: SSH THE PRIVATE INSTANCE

```
[ec2-user@ip-10-0-2-11 ~]$ ping google.com
PING google.com (216.58.198.78) 56(84) bytes of data.
64 bytes from dub08s02-in-f78.1e100.net (216.58.198.78): icmp_seq=1 ttl=48 time=
1.65 ms
64 bytes from dub08s02-in-f14.1e100.net (216.58.198.78): icmp_seq=2 ttl=48 time=
1.28 ms
64 bytes from dub08s02-in-f78.1e100.net (216.58.198.78): icmp_seq=3 ttl=48 time=
1.33 ms
64 bytes from dub08s02-in-f14.1e100.net (216.58.198.78): icmp_seq=4 ttl=48 time=
1.31 ms
64 bytes from dub08s02-in-f78.1e100.net (216.58.198.78): icmp_seq=5 ttl=48 time=
1.31 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.284/1.379/1.653/0.143 ms
[ec2-user@ip-10-0-2-11 ~]$
```

FIGURE 20: PING GOOGLE.COM FROM THE PRIVATE INSTANCE

CONCLUSION

This project has highlighted how to:

- ✓ set up a VPC and subnets in different availability zones
- ✓ Create the Linux instances in both subnets (private and public subnet)
- ✓ Create and configure the internet gateways and security groups
- ✓ Configure putty to access public and private machine