

AWS PROJECT

CREATE PUBLIC AND PRIVATE INSTANCES and
ACCESS INTERNET FROM PRIVATE INSTANCE

FREDERIC TWAHIRWA
May 2018

TABLE OF CONTENTS

DIAGRAM	2
CONFIGURATION.....	2
▪ CREATE A VPC AND SUBNETS	2
▪ CREATE SECURITY GROUPS	4
▪ CREATE AN ELASTIC IP	5
▪ INTERNET GATEWAY AND NAT GATEWAY	6
▪ ROUTE TABLES	7
▪ SUBNETS AND ROUTE TABLES	9
RESULTS	10
CONCLUSION.....	11

TABLE OF FIGURES

FIGURE 1: VPC WITH PUBLIC AND PRIVATE SUBNETS	2
FIGURE 2: PUBLIC INSTANCE CONFIGURATION	3
FIGURE 3: PRIVATE INSTANCE CONFIGURATION	3
FIGURE 4: BASTION SECURITY GROUP CONFIGURATION	4
FIGURE 5: BASTION SECURITY GROUP CONFIGURATION (OUTBOUND)	4
FIGURE 6: PRIVATE WEBSERVER SECURITY GROUP CONFIGURATION (INBOUND)	5
FIGURE 7: PRIVATE WEBSERVER SECURITY GROUP CONFIGURATION (OUTBOUND)	5
FIGURE 8: EIP CONFIGURATION	5
FIGURE 9: KEY PAIR CONFIGURATION	6
FIGURE 10: IGW CONFIGURATION	6
FIGURE 11: NAT GATEWAY CONFIGURATION	7
FIGURE 12: ROUTE TABLE (IGW) -ROUTES CONFIGURATION	7
FIGURE 13: ROUTE TABLE (IGW) -SUBNET ASSOCIATIONS CONFIGURATION	8
FIGURE 14: ROUTE TABLE (NAT GATEWAY) -ROUTES CONFIGURATION	8
FIGURE 15: PUBLIC SUBNET CONFIGURATION -SUMMARY	9
FIGURE 16: PUBLIC SUBNET CONFIGURATION -ROUTE TABLE	9
FIGURE 17: PRIVATE SUBNET CONFIGURATION -SUMMARY	10
FIGURE 18: PRIVATE SUBNET CONFIGURATION -ROUTE TABLE	10
FIGURE 19: SSH THE PRIVATE INSTANCE	11
FIGURE 20: PING GOOGLE.COM FROM THE PRIVATE INSTANCE	11

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

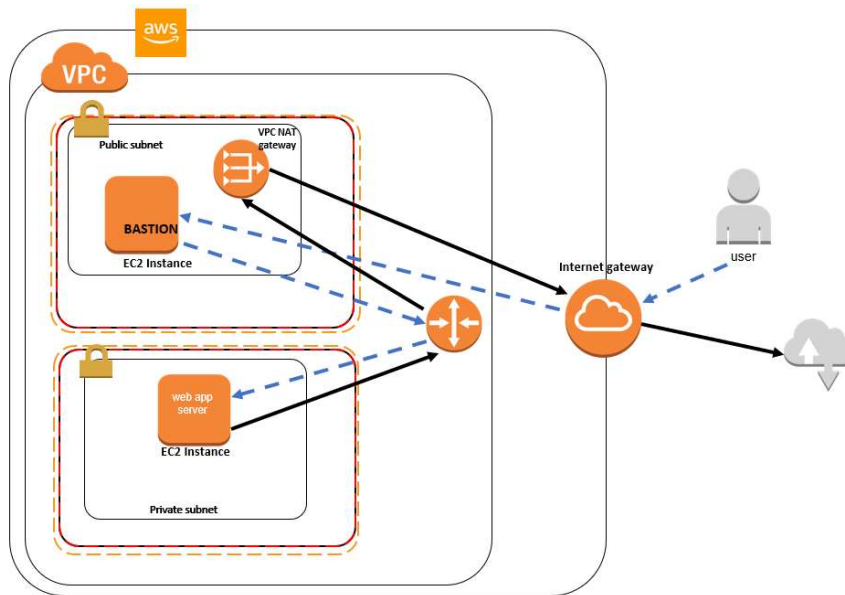


FIGURE 1: VPC WITH PUBLIC AND PRIVATE SUBNETS

CONFIGURATION

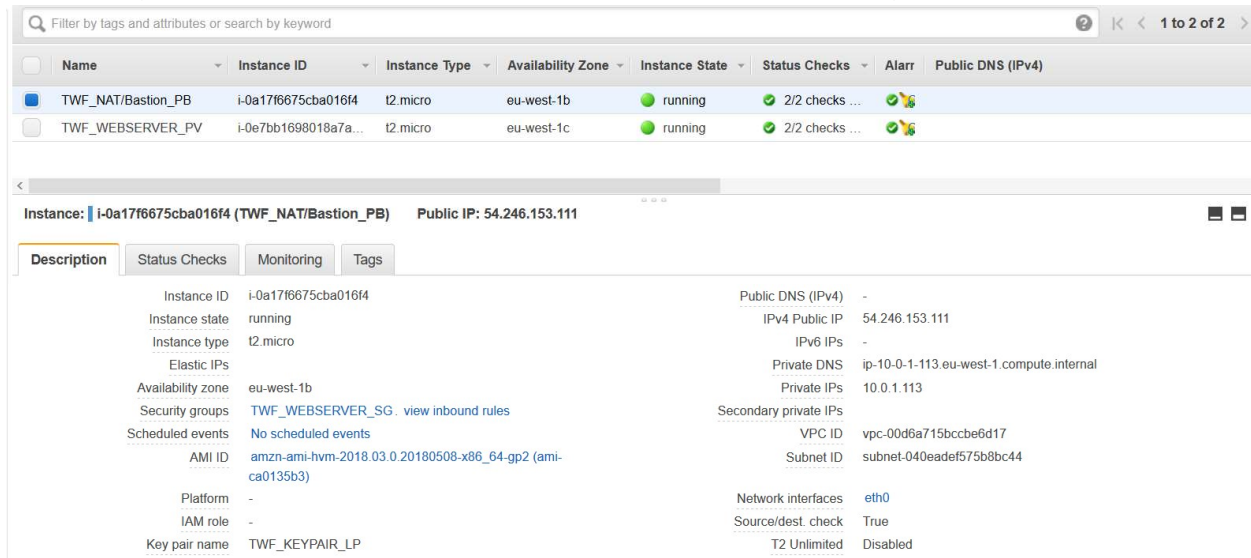
■ CREATE A VPC AND SUBNETS

- ✓ Create a VPC
- ✓ Create a public subnet
 - Create an EC2 in the public subnet which will serve 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 different Availability Zones (eu-west-1b and eu-west-1c)

Below the screenshots of the 2 instances

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



The screenshot displays the AWS Management Console interface for a Public EC2 instance. At the top, a table lists two instances: TWF_NAT/Bastion_PB (Instance ID: i-0a17f6675cba016f4, t2.micro, eu-west-1b) and TWF_WEBSERVER_PV (Instance ID: i-0e7bb1698018a7a07, t2.micro, eu-west-1c). Both are in a 'running' state. Below the table, the configuration details for the selected instance (TWF_NAT/Bastion_PB) are shown. The instance has a Public IP of 54.246.153.111. The configuration details are organized into two columns: Description and Monitoring. The Description column includes Instance ID, Instance state, Instance type, Elastic IPs, Availability zone, Security groups, Scheduled events, AMI ID, Platform, IAM role, and Key pair name. The Monitoring column includes Public DNS (IPv4), IPv4 Public IP, IPv6 IPs, Private DNS, Private IPs, Secondary private IPs, VPC ID, Subnet ID, Network interfaces, Source/dest. check, T2 Unlimited, and Owner.

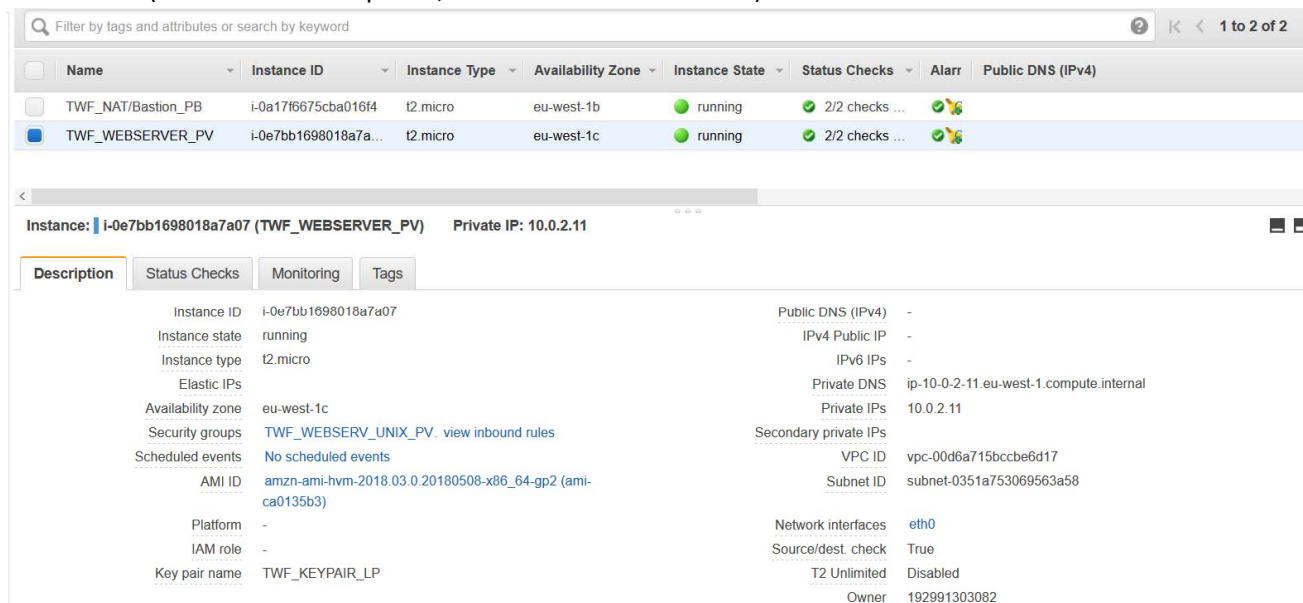
Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm	Public DNS (IPv4)
TWF_NAT/Bastion_PB	i-0a17f6675cba016f4	t2.micro	eu-west-1b	running	2/2 checks ...		
TWF_WEBSERVER_PV	i-0e7bb1698018a7a...	t2.micro	eu-west-1c	running	2/2 checks ...		

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

Description	Monitoring
Instance ID	Public DNS (IPv4)
Instance state	IPv4 Public IP
Instance type	IPv6 IPs
Elastic IPs	Private DNS
Availability zone	Private IPs
Security groups	Secondary private IPs
Scheduled events	VPC ID
AMI ID	Subnet ID
Platform	Network interfaces
IAM role	Source/dest. check
Key pair name	T2 Unlimited
	Owner

FIGURE 2: PUBLIC INSTANCE CONFIGURATION

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



The screenshot displays the AWS Management Console interface for a Private EC2 instance. At the top, a table lists two instances: TWF_NAT/Bastion_PB (Instance ID: i-0a17f6675cba016f4, t2.micro, eu-west-1b) and TWF_WEBSERVER_PV (Instance ID: i-0e7bb1698018a7a07, t2.micro, eu-west-1c). Both are in a 'running' state. Below the table, the configuration details for the selected instance (TWF_WEBSERVER_PV) are shown. The instance has a Private IP of 10.0.2.11. The configuration details are organized into two columns: Description and Monitoring. The Description column includes Instance ID, Instance state, Instance type, Elastic IPs, Availability zone, Security groups, Scheduled events, AMI ID, Platform, IAM role, and Key pair name. The Monitoring column includes Public DNS (IPv4), IPv4 Public IP, IPv6 IPs, Private DNS, Private IPs, Secondary private IPs, VPC ID, Subnet ID, Network interfaces, Source/dest. check, T2 Unlimited, and Owner.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm	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	Monitoring
Instance ID	Public DNS (IPv4)
Instance state	IPv4 Public IP
Instance type	IPv6 IPs
Elastic IPs	Private DNS
Availability zone	Private IPs
Security groups	Secondary private IPs
Scheduled events	VPC ID
AMI ID	Subnet ID
Platform	Network interfaces
IAM role	Source/dest. check
Key pair name	T2 Unlimited
	Owner

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, HTTP and 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_WEBSESV_LINUX_PV

Below the screenshots of the 2 security Groups

NAT/BASTION Security Groups:

Name	Group ID	Group Name	VPC ID	Description
<input type="checkbox"/> TWF_WEBSESV_LINUX_PV	sg-0ae583ac94c05461	TWF_WEBSESV_UNIX_PV	vpc-00d6a715bccbe6d17	Web servers linux private
<input type="checkbox"/> TWF_DBSESV_SERVER_SG	sg-0bcfcd3ef011e3b73	TWF_DBSESV_SERVER_SG	vpc-00d6a715bccbe6d17	TWF DB SERVER SECURITY GROUPS
<input checked="" type="checkbox"/> TWF_WEBSESV_SERVER_SG	sg-0d1007a5513bf448e	TWF_WEBSESV_SERVER_SG	vpc-00d6a715bccbe6d17	TWF WEBSESV_SERVER 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

Name	Group ID	Group Name	VPC ID	Description
<input checked="" type="checkbox"/> TWF_WEBSERV_LINUX_PV	sg-0aee583ac94c05461	TWF_WEBSERV_UNIX_PV	vpc-00d6a715bccbe6d17	Web servers linux private
<input type="checkbox"/> TWF_DBSERVER_SG	sg-0bcfd3ef011e3b73	TWF_DBSERVER_SG	vpc-00d6a715bccbe6d17	TWF DB SERVER SECURITY GROUPS
<input type="checkbox"/> 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 WEBSEVER 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 WEBSEVER 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

Filter by tags and attributes or search by keyword

Name	Elastic IP	Allocation ID	Instance	Private IP address	Scope	Association ID	Network Interface ID
<input checked="" type="checkbox"/>	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-05532b00a31917a5
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

The screenshot displays two AWS console interfaces. The top interface is the 'Create Key Pair' page, showing a table with one entry: 'TWF_KEYPAIR_LP' with a fingerprint. The bottom interface is the 'Network ACL' configuration page for 'TWF_ACL', showing its association with 'TWF_VPC' and a summary of its rules and associations.

Key pair name	Fingerprint
TWF_KEYPAIR_LP	f4:2b:67:2d:68:3d:65:28:7b:ff:10:02:71:3e:6a:a1:7c:bf:d5:c5

Name	Network ACL ID	Associated With	Default	VPC
TWF_ACL	acl-0caf0f9d3f968e7f0	2 Subnets	Yes	vpc-00d6a715bccbe6d17 TWF_VPC

aci-0caf0f9d3f968e7f0 | TWF_ACL

Summary | Inbound Rules | Outbound Rules | Subnet Associations | Tags

Network ACL ID: aci-0caf0f9d3f968e7f0 | TWF_ACL
Associated with: 2 Subnets
Default: yes
VPC: vpc-00d6a715bccbe6d17 | TWF_VPC

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

The screenshot shows the 'Create internet gateway' page in the AWS VPC console. It displays a table with one entry: 'TWF_IGW' with ID 'igw-08eecd2cd13bf6a48' and state 'attached'. Below the table, the 'Internet gateway' details are shown, including its ID and the VPC it is attached to.

Name	ID	State	VPC
TWF_IGW	igw-08eecd2cd13bf6a48	attached	vpc-00d6a715bccbe6d17 TWF_VPC

Internet gateway: igw-08eecd2cd13bf6a48

Description | Tags

ID: igw-08eecd2cd13bf6a48
State: attached
Attached VPC ID: vpc-00d6a715bccbe6d17 | TWF_VPC

FIGURE 10: IGW CONFIGURATION

NAT GATEWAY

The screenshot displays the AWS Management Console interface for a NAT Gateway. At the top, there's a search bar and a table listing NAT Gateways. The table has columns: Name, NAT Gateway ID, Status, Status Message, Elastic IP Address, Private IP Address, Network Interface, VPC, and Subnet. One gateway is listed with ID nat-0a2865b81963af8b1, status available, and associated with VPC vpc-00d6a715bccb6d17 and Subnet subnet-040eade575b8bc44.

Below the table, the details for the selected NAT Gateway are shown. The details are organized into two columns:

Property	Value
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
Subnet	subnet-040eade575b8bc44 10.0.1.0_EU_WEST_1B_TWF_PUB
VPC	vpc-00d6a715bccb6d17 TWF_VPC
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 Route 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 screenshots of the route tables and theirs routes and subnet associations

Route table to Internet gateway

The screenshot displays the AWS Management Console interface for a Route Table. At the top, there's a search bar and a table listing Route Tables. The table has columns: Name, Route Table ID, Explicitly Associated, Main, and VPC. Two route tables are listed: TWF_RTB (ID: rtb-0daaf2325c3da07ac) and TWF_RTB_Main (ID: rtb-0dd7fcdcf084b04c).

Below the table, the details for the selected Route Table (TWF_RTB) are shown. The details are organized into tabs: Summary, Routes, Subnet Associations, Route Propagation, and Tags. The Routes tab is selected, showing a list of routes.

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-08eccc2cd13bf6a48	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-040eade575b8bc44 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

Q TWF X

<input type="checkbox"/>	Name	Route Table ID	Explicitly Associat	Main	VPC
<input type="checkbox"/>	TWF_RTB	rtb-0daaf2325c3da07ac	1 Subnet	No	vpc-00d6a715bccbe6d17 TWF_VPC
<input checked="" type="checkbox"/>	TWF_RTB_Main	rtb-0dd7fcdcf084b04c	0 Subnets	Yes	vpc-00d6a715bccbe6d17 TWF_VPC

rtb-0dd7fcdcf084b04c | 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

Create SubnetSubnet Actions

Q TWF

<< 1 to 2 of 2 Subnets >>

	Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR
<input checked="" type="checkbox"/>	10.0.1.0_EU_WEST_1B_TWF_PUB	subnet-040eade575b8bc44	available	vpc-00d6a715bccbe6d17 TWF_VPC	10.0.1.0/24	249	
<input type="checkbox"/>	10.0.2.0_EU_WEST_1C_TWF_PRIV	subnet-0351a753069563a58	available	vpc-00d6a715bccbe6d17 TWF_VPC	10.0.2.0/24	250	

subnet-040eade575b8bc44 | 10.0.1.0_EU_WEST_1B_TWF_PUB

Summary

Route Table

Network ACL

Flow Logs

Tags

Subnet ID: subnet-040eade575b8bc44 | 10.0.1.0_EU_WEST_1B_TWF_PUB

Availability Zone: eu-west-1b

IPv4 CIDR: 10.0.1.0/24

Route table: rtb-0daaf2325c3da07ac | TWF_RTb

IPv6 CIDR:

Network ACL: acl-0ca0f9d3f968e7f0 | TWF_ACL

State: available

Default subnet: no

VPC: vpc-00d6a715bccbe6d17 | TWF_VPC

Auto-assign Public IP: no

Available IPs: 249

Auto-assign IPv6 address: no

FIGURE 15: PUBLIC SUBNET CONFIGURATION -SUMMARY

subnet-040eade575b8bc44 | 10.0.1.0_EU_WEST_1B_TWF_PUB

Summary

Route Table

Network ACL

Flow Logs

Tags

Edit

Route Table: rtb-0daaf2325c3da07ac | TWF_RTb

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-08eccc2cd13bf6a48

FIGURE 16: PUBLIC SUBNET CONFIGURATION -ROUTE TABLE

PRIVATE Subnet

Create Subnet Subnet Actions

Q TWF X << 1 to 2 of 2 Subnets >>

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR
10.0.1.0_EU_WEST_1B_TWF_PUB	subnet-040eade575b8bc44	available	vpc-00d6a715bccbe6d17 TWF_VPC	10.0.1.0/24	249	
10.0.2.0_EU_WEST_1C_TWF_PRIV	subnet-0351a753069563a58	available	vpc-00d6a715bccbe6d17 TWF_VPC	10.0.2.0/24	250	

subnet-0351a753069563a58 | 10.0.2.0_EU_WEST_1C_TWF_PRIV

Summary Route Table Network ACL Flow Logs Tags

Subnet ID: subnet-0351a753069563a58 | 10.0.2.0_EU_WEST_1C_TWF_PRIV
IPv4 CIDR: 10.0.2.0/24
IPv6 CIDR:
State: available
VPC: vpc-00d6a715bccbe6d17 | TWF_VPC
Available IPs: 250

Availability Zone: eu-west-1c
Route table: rtb-0dd7fcdcf084b04c | TWF_RTb_Main
Network ACL: acl-0ca0f9d3f968e7f0 | TWF_ACL
Default subnet: no
Auto-assign Public IP: no
Auto-assign IPv6 address: no

FIGURE 17: PRIVATE SUBNET CONFIGURATION -SUMMARY

subnet-0351a753069563a58 | 10.0.2.0_EU_WEST_1C_TWF_PRIV

Summary Route Table Network ACL Flow Logs Tags

Edit

Route Table: rtb-0dd7fcdcf084b04c | TWF_RTb_Main

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	nat-0a2865b81963af8b1

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:VwjQQZLFgBdlhxiOq8iDJijaHINsA/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