Project 2 networking project

How does the EC2 instance know its way out to the internet? (Answer this question in a text document)... Hint: Check the Route Table assigned to the subnet of the EC2 instance?

By checking the route table in our VPC. There should be a target that starts with "IGW-". This means Internet Gateway. The destination is 0.0.0.0/0 which represents the entire internet. The instances are able to communicate through the internet gateway and make their way out to the internet.

rtb-097b545314575ba2e

| Details | Routes | Subnet associations | Edge associations | Route propagation | Tags |

Routes (2)

Destination	Target	Status
0.0.0.0/0	igw-05f805f1c8a7a22df	⊘ Active
172.31.0.0/16	local	⊘ Active

| Launch an instance | EC2 | us   × | Instances | EC2 | us-east-1   × | 54.162.183.142   × | + |

← → C ⚠ Not Secure 54.162.183.142   ☆ ⫶

Hello World

Does connectivity work? If so, what do you see? Did we traverse the internet while making this request?

When I input curl <Private IP of the web-server > I see

```
●  ○  ○    📁 Desktop — ec2-user@ip-172-31-20-234:~ — ssh -i The2ndInstance.pem ec...

Last login: Mon Jul 15 08:24:38 on ttys000
[djpriya@5ce91e9213ed ~ % cd desktop
[djpriya@5ce91e9213ed desktop % chmod 400 The2ndInstance.pem
[djpriya@5ce91e9213ed desktop % ssh -i The2ndInstance.pem ec2-user@54.90.179.233
      ,      #_
      ~\_   ####_        Amazon Linux 2023
     ~~  \_#####\
     ~~      \###|
     ~~       \#/ ___    https://aws.amazon.com/linux/amazon-linux-2023
      ~~      V~' '->
       ~~~        /
        ~~._.   _/
          _/ _/
         _/m/'
Last login: Mon Jul 15 15:09:12 2024 from 15.248.6.17
[[ec2-user@ip-172-31-20-234 ~]$ curl 172.31.18.141
<h1>Hello World</h1>
```

Yes, the connectivity works because the security groups are configured to allow the necessary traffic
For the web server, we have allowed Port 80 (http) traffic from the entire internet 0.0.0.0/0 and Port 22 (ssh) from our IP which establishes a secure connection.

No, we did not traverse the internet when we curl because we used a private IP address which you can't use on the internet.

Is there any difference in response? Did we traverse the internet while making this request?

When I input curl <Public IP of the web-server > I see,

```
[[ec2-user@ip-172-31-20-234 ~]$ curl 50.19.46.223
<h1>Hello World</h1>
[ec2-user@ip-172-31-20-234 ~]$ ▯
```

Similar to when I curl into the private IP of the web server, I am able to see Hello World.

Yes, we did traverse through the internet while making this request because we are using a public IP. When we curl the public IP, it sends the internet packet to the internet gateway

Did pinging the web-server work? Why? Hint: What protocol does PING use?

When I ping into the <Public-IP of the web - server > I see,

```
[[ec2-user@ip-172-31-20-234 ~]$ ping 50.19.46.223
PING 50.19.46.223 (50.19.46.223) 56(84) bytes of data.
^C
--- 50.19.46.223 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5213ms

[ec2-user@ip-172-31-20-234 ~]$
```

Pinging the Web server did not work because the security group only allows traffic that is port 80 (http) and port 22 (ssh).

The protocol ping uses is internet control message protocol (ICMP)

What was the response? If connectivity failed, explain the possible cause.

when I try to curl into the <private-IP of client instance> I see,

```
[[ec2-user@ip-172-31-20-234 ~]$ curl 172.31.20.234
 curl: (7) Failed to connect to 172.31.20.234 port 80 after 0 ms: Couldn't connect to server
 [ec2-user@ip-172-31-20-234 ~]$
```

When creating the client instance, the security groups were configured to only allows port 22 (SSH) traffic. The securities groups restriction to only port 22 traffic is the reason for connectivity failure.
If the security groups also allowed port 80 traffic, it would fix the connectivity issue because it would allow HTTP traffic to reach the client instance.

Bonus Question:
setting up a tcp connection between the two instances.

```
[djpriya@5ce91e9213ed ~ % cd desktop
[djpriya@5ce91e9213ed desktop % chmod 400 The2ndInstance.pem
[djpriya@5ce91e9213ed desktop % ssh -i "The2ndInstance.pem" ec2-user@ec2-54-90-17]
9-233.compute-1.amazonaws.com
The authenticity of host 'ec2-54-90-179-233.compute-1.amazonaws.com (54.90.179.2
33)' can't be established.
ED25519 key fingerprint is SHA256:wKWZu8TYMc4XmRCCASOWLwEKPXGFdd7u/DxuKKqtCds.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:40: 54.90.179.233
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-54-90-179-233.compute-1.amazonaws.com' (ED25519)
 to the list of known hosts.
     ,       #_
    ~\_   ####_         Amazon Linux 2023
   ~~  \_#####\
   ~~     \###|
   ~~       \#/ ___     https://aws.amazon.com/linux/amazon-linux-2023
    ~~       V~' '->
     ~~~         /
       ~~._.   _/
          _/ _/
        _/m/'
Last login: Mon Jul 15 15:57:34 2024 from 15.248.6.1
[ec2-user@ip-172-31-20-234 ~]$ ▯
```
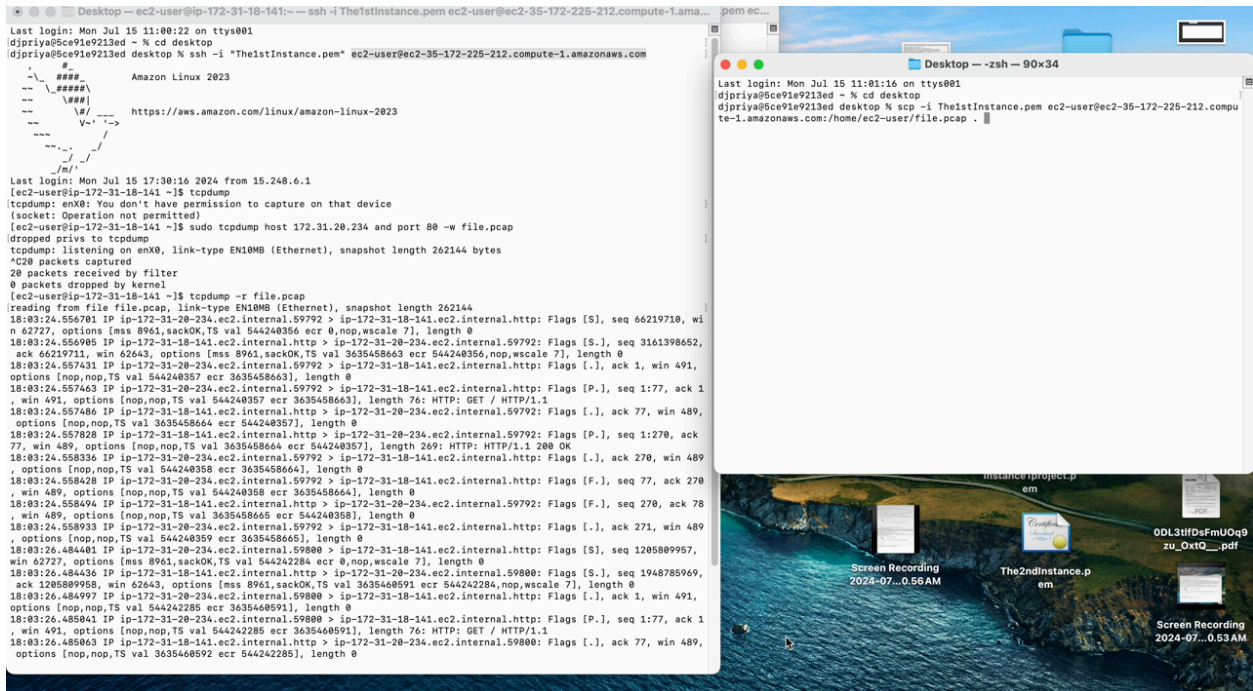
```
Last login: Mon Jul 15 09:09:01 on ttys000
[djpriya@5ce91e9213ed ~ % cd desktop
[djpriya@5ce91e9213ed desktop % chmod 400 The1stInstance.pem
[djpriya@5ce91e9213ed desktop % ssh -i "The1stInstance.pem" ec2-user@ec2-50-19-46]
-223.compute-1.amazonaws.com
     ,       #_
    ~\_   ####_         Amazon Linux 2023
   ~~  \_#####\
   ~~     \###|
   ~~       \#/ ___     https://aws.amazon.com/linux/amazon-linux-2023
    ~~       V~' '->
     ~~~         /
       ~~._.   _/
          _/ _/
        _/m/'
Last login: Mon Jul 15 16:03:35 2024 from 15.248.6.1
[ec2-user@ip-172-31-18-141 ~]$ ▮
```

```
Last login: Mon Jul 15 11:00:22 on ttys001
djpriya@5ce91e9213ed ~ % cd desktop
djpriya@5ce91e9213ed desktop % ssh -i "The1stInstance.pem" ec2-user@ec2-35-172-225-212.compute-1.amazonaws.com
   `.    #_
  ~\_  ####_         Amazon Linux 2023
 ~~  \_#####\
 ~~     \###|
 ~~      \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
  ~~       V~' '->
   ~~~         /
     ~~._.   _/
        _/ _/
      _/m/'
Last login: Mon Jul 15 17:30:16 2024 from 15.248.6.1
[ec2-user@ip-172-31-18-141 ~]$ tcpdump
tcpdump: enX0: You don't have permission to capture on that device
(socket: Operation not permitted)
[ec2-user@ip-172-31-18-141 ~]$ sudo tcpdump host 172.31.20.234 and port 80 -w file.pcap
dropped privs to tcpdump
tcpdump: listening on enX0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C20 packets captured
20 packets received by filter
0 packets dropped by kernel
[ec2-user@ip-172-31-18-141 ~]$ tcpdump -r file.pcap
reading from file file.pcap, link-type EN10MB (Ethernet), snapshot length 262144
18:03:24.556701 IP ip-172-31-20-234.ec2.internal.59792 > ip-172-31-18-141.ec2.internal.http: Flags [S], seq 66219710, win 62727, options [mss 8961,sackOK,TS val 544240356 ecr 0,nop,wscale 7], length 0
18:03:24.556905 IP ip-172-31-18-141.ec2.internal.http > ip-172-31-20-234.ec2.internal.59792: Flags [S.], seq 3161398652, ack 66219711, win 62643, options [mss 8961,sackOK,TS val 3635458663 ecr 544240356,nop,wscale 7], length 0
18:03:24.557431 IP ip-172-31-20-234.ec2.internal.59792 > ip-172-31-18-141.ec2.internal.http: Flags [.], ack 1, win 491, options [nop,nop,TS val 544240357 ecr 3635458663], length 0
18:03:24.557463 IP ip-172-31-20-234.ec2.internal.59792 > ip-172-31-18-141.ec2.internal.http: Flags [P.], seq 1:77, ack 1, win 491, options [nop,nop,TS val 544240357 ecr 3635458663], length 76: HTTP: GET / HTTP/1.1
18:03:24.557486 IP ip-172-31-18-141.ec2.internal.http > ip-172-31-20-234.ec2.internal.59792: Flags [.], ack 77, win 489, options [nop,nop,TS val 3635458664 ecr 544240357], length 0
18:03:24.557828 IP ip-172-31-18-141.ec2.internal.http > ip-172-31-20-234.ec2.internal.59792: Flags [P.], seq 1:270, ack 77, win 489, options [nop,nop,TS val 3635458664 ecr 544240357], length 269: HTTP: HTTP/1.1 200 OK
18:03:24.558336 IP ip-172-31-20-234.ec2.internal.59792 > ip-172-31-18-141.ec2.internal.http: Flags [.], ack 270, win 489, options [nop,nop,TS val 544240358 ecr 3635458664], length 0
18:03:24.558428 IP ip-172-31-20-234.ec2.internal.59792 > ip-172-31-18-141.ec2.internal.http: Flags [F.], seq 77, ack 270, win 489, options [nop,nop,TS val 544240358 ecr 3635458664], length 0
18:03:24.558494 IP ip-172-31-18-141.ec2.internal.http > ip-172-31-20-234.ec2.internal.59792: Flags [F.], seq 270, ack 78, win 489, options [nop,nop,TS val 3635458665 ecr 544240358], length 0
18:03:24.558933 IP ip-172-31-20-234.ec2.internal.59792 > ip-172-31-18-141.ec2.internal.http: Flags [.], ack 271, win 489, options [nop,nop,TS val 544240359 ecr 3635458665], length 0
18:03:26.484401 IP ip-172-31-20-234.ec2.internal.59800 > ip-172-31-18-141.ec2.internal.http: Flags [S], seq 1205809957, win 62727, options [mss 8961,sackOK,TS val 544242284 ecr 0,nop,wscale 7], length 0
18:03:26.484436 IP ip-172-31-18-141.ec2.internal.http > ip-172-31-20-234.ec2.internal.59800: Flags [S.], seq 1948785969, ack 1205809958, win 62643, options [mss 8961,sackOK,TS val 3635460591 ecr 544242284,nop,wscale 7], length 0
18:03:26.484997 IP ip-172-31-20-234.ec2.internal.59800 > ip-172-31-18-141.ec2.internal.http: Flags [.], ack 1, win 491, options [nop,nop,TS val 544242285 ecr 3635460591], length 0
18:03:26.485041 IP ip-172-31-20-234.ec2.internal.59800 > ip-172-31-18-141.ec2.internal.http: Flags [P.], seq 1:77, ack 1, win 491, options [nop,nop,TS val 544242285 ecr 3635460591], length 76: HTTP: GET / HTTP/1.1
18:03:26.485063 IP ip-172-31-18-141.ec2.internal.http > ip-172-31-20-234.ec2.internal.59800: Flags [.], ack 77, win 489, options [nop,nop,TS val 3635460592 ecr 544242285], length 0
```

```
Last login: Mon Jul 15 11:01:16 on ttys001
djpriya@5ce91e9213ed ~ % cd desktop
djpriya@5ce91e9213ed desktop % scp -i The1stInstance.pem ec2-user@ec2-35-172-225-212.compute-1.amazonaws.com:/home/ec2-user/file.pcap .
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.31.20.234	172.31.18.141	TCP	74	59792 → 80 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM TSval=544240356 TSecr=0 WS=128
2	0.000204	172.31.18.141	172.31.20.234	TCP	74	80 → 59792 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=3635458663 TSecr=544240356 WS=128
3	0.000730	172.31.20.234	172.31.18.141	TCP	66	59792 → 80 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=544240357 TSecr=3635458663
4	0.000762	172.31.20.234	172.31.18.141	HTTP	142	GET / HTTP/1.1
5	0.000785	172.31.18.141	172.31.20.234	TCP	66	80 → 59792 [ACK] Seq=1 Ack=77 Win=62592 Len=0 TSval=3635458664 TSecr=544240357
6	0.001127	172.31.18.141	172.31.20.234	HTTP	335	HTTP/1.1 200 OK (text/html)
7	0.001635	172.31.20.234	172.31.18.141	TCP	66	59792 → 80 [ACK] Seq=77 Ack=270 Win=62592 Len=0 TSval=544240358 TSecr=3635458664
8	0.001727	172.31.20.234	172.31.18.141	TCP	66	59792 → 80 [FIN, ACK] Seq=77 Ack=270 Win=62592 Len=0 TSval=544240358 TSecr=3635458664
9	0.001793	172.31.18.141	172.31.20.234	TCP	66	80 → 59792 [FIN, ACK] Seq=270 Ack=78 Win=62592 Len=0 TSval=3635458665 TSecr=544240358
10	0.002232	172.31.20.234	172.31.18.141	TCP	66	59792 → 80 [ACK] Seq=78 Ack=271 Win=62592 Len=0 TSval=544240359 TSecr=3635458665
11	1.927700	172.31.20.234	172.31.18.141	TCP	74	59800 → 80 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM TSval=544242284 TSecr=0 WS=128
12	1.927735	172.31.18.141	172.31.20.234	TCP	74	80 → 59800 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=3635460591 TSecr=544242284 WS=128
13	1.928296	172.31.20.234	172.31.18.141	TCP	66	59800 → 80 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=544242285 TSecr=3635460591
14	1.928340	172.31.20.234	172.31.18.141	HTTP	142	GET / HTTP/1.1
15	1.928362	172.31.18.141	172.31.20.234	TCP	66	80 → 59800 [ACK] Seq=1 Ack=77 Win=62592 Len=0 TSval=3635460592 TSecr=544242285
16	1.928688	172.31.18.141	172.31.20.234	HTTP	335	HTTP/1.1 200 OK (text/html)
17	1.929494	172.31.20.234	172.31.18.141	TCP	66	59800 → 80 [ACK] Seq=77 Ack=270 Win=62592 Len=0 TSval=544242286 TSecr=3635460592
18	1.929642	172.31.20.234	172.31.18.141	TCP	66	59800 → 80 [FIN, ACK] Seq=77 Ack=270 Win=62592 Len=0 TSval=544242286 TSecr=3635460592
19	1.929712	172.31.18.141	172.31.20.234	TCP	66	80 → 59800 [FIN, ACK] Seq=270 Ack=78 Win=62592 Len=0 TSval=3635460593 TSecr=544242286
20	1.930167	172.31.20.234	172.31.18.141	TCP	66	59800 → 80 [ACK] Seq=78 Ack=271 Win=62592 Len=0 TSval=544242287 TSecr=3635460593

```
> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: 0a:ff:f6:bc:47:af (0a:ff:f6:bc:47:af), Dst: 0a:ff:e8:46:ac:79 (0a:ff:e8:46:...
> Internet Protocol Version 4, Src: 172.31.20.234, Dst: 172.31.18.141
  Transmission Control Protocol, Src Port: 59792, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  0a ff e8 46 ac 79 0a ff  f6 bc 47 af 08 00 45 00   ···F·y·· ··G···E·
0010  00 3c a8 5d 40 00 7f 06  d3 a8 ac 1f 14 ea ac 1f   ·<·]@··· ········
0020  12 8d e9 90 00 50 03 f2  6e 6e 00 00 00 00 a0 02   ·····P·· n·······
0030  f5 07 c6 0f 00 00 02 04  23 01 04 02 08 0a 20 70   ········ #····· p
0040  72 e4 00 00 00 00 01 03  03 07                     r········ ··
```

file.pcap   Packets: 20 · Displayed: 20 (100.0%)

○ *Who initiates the TCP three-way handshake?*

```
18:03:24.556701 IP ip-172-31-20-234.ec2.internal.59792 > ip-172-31-18-141.ec2.internal.http: Flags [S], seq 66219710, win 62727, options [mss 8961,sackOK,TS val 544240356 ecr 0,nop,wscale 7], length 0
18:03:24.556905 IP ip-172-31-18-141.ec2.internal.http > ip-172-31-20-234.ec2.internal.59792: Flags [S.], seq 3161398652, ack 66219711, win 62643, options [mss 8961,sackOK,TS val 3635458663 ecr 544240356,nop,wscale 7], length 0
```

Private IP of the client instance

The private IP of the client server initiated the three-way handshake

- *What is the HTTP request method?*

request methods to indicate the desired action to be performed for a given resource
The method is the Get /HTTP/ 1.1 method to obtain the webpage

- *How is the connection closed between the two peers? (What TCP flags do you see?)*

The client sends a fin which stands for finish connection.