|  |
| --- |
|  |
| Daydreams Travel Agency Design and Configure the Virtual Network |
|  |

|  |
| --- |
| Thong Thao  Student ID: 474587265 |

**Contents**

[Section B – Configure a virtual network and peering 2](#_Toc161921111)

[Reference 13](#_Toc161921112)

# Section B – Configure a virtual network and peering

2.3 Insert screen shots to show how you have enabled the gateways and services according to the table in question 2.1. These can include dialog boxes from the AWS management console showing each activity, and/or operations taken at the command line interface. You may also show code fragments if you are using code in your development.

1. To create an Internet Gateway for DTA, I use AWS CLI to create and attach it to VPC. Using this CLI to create an Internet Gateway:

aws ec2 create-internet-gateway --tag-specifications 'ResourceType=internet-gateway,Tags=[{Key=Name,Value=dta-igw},{Key=Project,Value=DTA Project},{Key=Owner,Value=DTA}]'

A black screen with white text

Description automatically generated

Figure 1 Using AWS CLI to create Internet Gateway

2. Attach Internet Gateway to VPC by this CLI:

aws ec2 attach-internet-gateway --vpc-id vpc-04816a1356754aa8c --internet-gateway-id igw-0ea5da126f317ce86

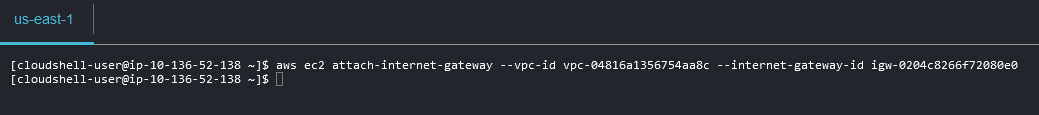


Figure 2 Attached Internet Gateway to VPC

Checking Internet Gateway is created and attached to VPC ID: vpc-04816a1356754aa8c by CLI.

A screenshot of a computer

Description automatically generated

Figure 3 The Internet Gateway is created and attached to VPC.

Checking on AWS Management Console.

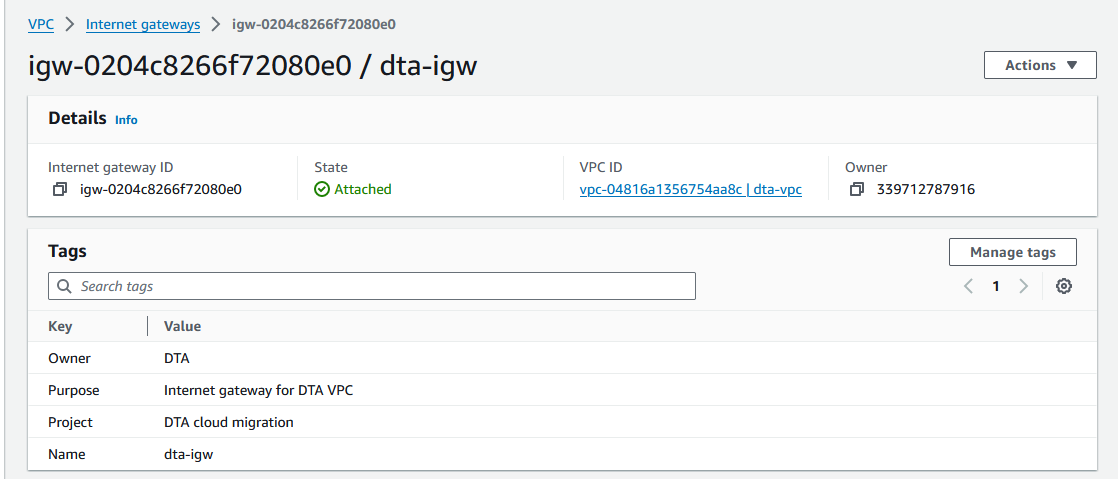


Figure 4 Internet Gateway and attached to VPC

2.4 Include screen shots to show how you have configured route tables and routing targets. This should align to the topology in question 2.1 and your subnetting scheme in question 2.2.

1. Create Route Table by using AWS CLI:

aws ec2 create-route-table --vpc-id vpc-04816a1356754aa8c --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=dta-rt-public},{Key=Project,Value=DTA Project},{Key=Owner,Value=DTA}]'

A black background with white lines

Description automatically generated

Figure 5 Creating Route Table

2. Create Route Destination of DTA to 0.0.0.0/0 using the CLI:

aws ec2 create-route --route-table-id rtb-05d9ccca313e2fb81 --destination-cidr-block 0.0.0.0/0 --gateway-id igw-0204c8266f72080e0

A screen shot of a computer

Description automatically generated

Figure 6 Create Route Table Destination of DTA to 0.0.0.0/0

Checking on AWS Management Console the Route Table is created, and route completed.

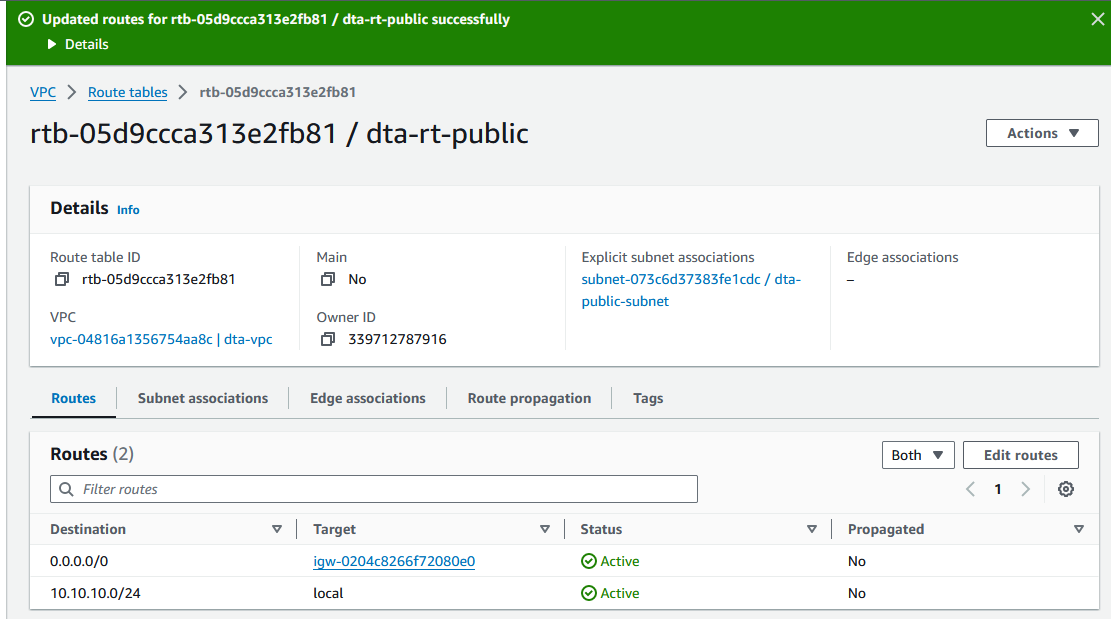


Figure 7 Route Table and Route of DTA Created.

2.5 Include screen shots to show how you have configured security controls to support your virtual network. The configuration should align to the security controls that you listed in the table in question 1.3.

1. Create Security Group of DTA by using AWS CLI:

aws ec2 create-security-group \

--group-name dta-sg \

--description "DTA Security Group" \

--tag-specifications 'ResourceType=security-group,Tags=[{Key=Name,Value=dta-sg},{Key=Project,Value=DTA Project},{Key=Owner,Value=DTA}]'

A screenshot of a computer

Description automatically generated

Figure 8 Create Security Group for DTA

2. Create inbound rules by CLI:

aws ec2 authorize-security-group-ingress \

--group-id sg-08eac28165bf25ba7 \

--protocol tcp \

--port 443 \

--cidr 0.0.0.0/0

aws ec2 authorize-security-group-ingress \

--group-id sg-08eac28165bf25ba7 \

--protocol icmp \

--port -1 \

--cidr 0.0.0.0/0

aws ec2 authorize-security-group-ingress \

--group-id sg-08eac28165bf25ba7 \

--protocol tcp \

--port 80 \

--cidr 0.0.0.0/0

aws ec2 authorize-security-group-ingress \

--group-id sg-08eac28165bf25ba7 \

--protocol tcp \

--port 3389 \

--cidr 0.0.0.0/0

aws ec2 authorize-security-group-ingress \

--group-id sg-08eac28165bf25ba7 \

--protocol tcp \

--port 22 \

--cidr 0.0.0.0/0

3. Checking the Security Group is created on AWS Management Console.

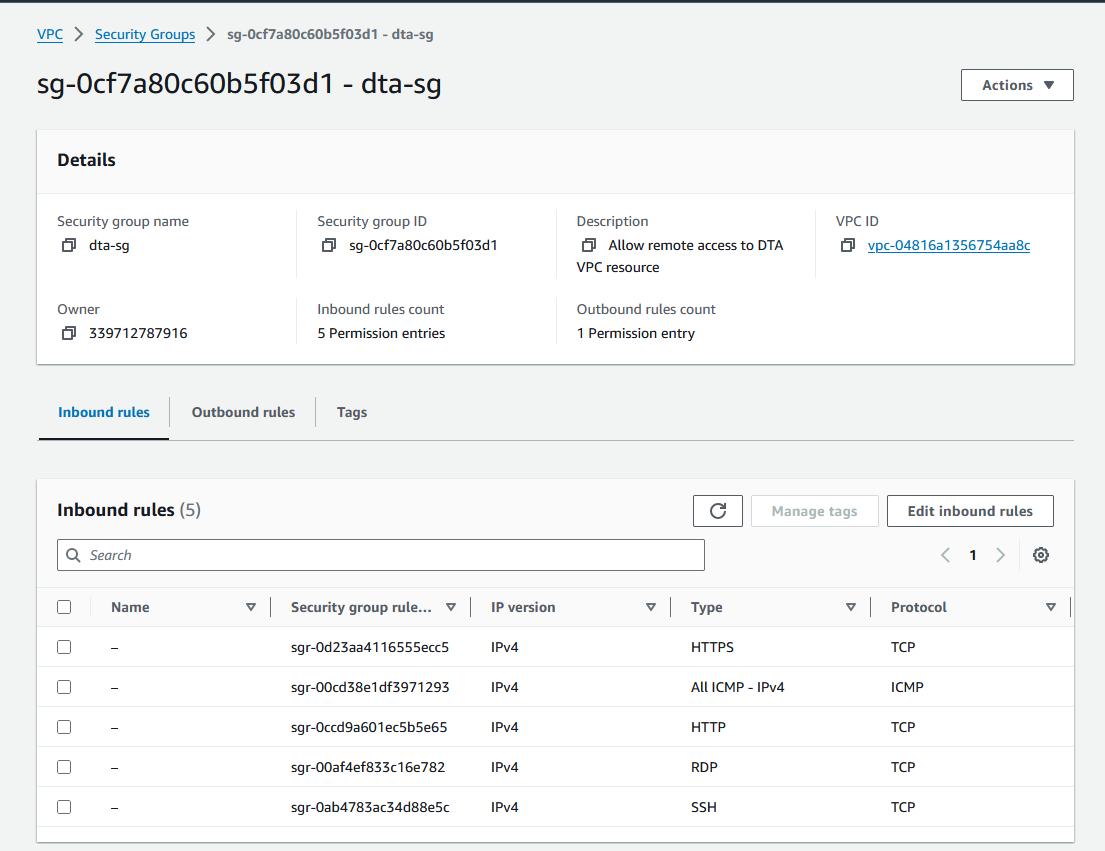


Figure 9 Security Group for DTA is created.

2.6 Include screen shots to show how you have confirmed the expected flow of traffic through the virtual network.

2.6.1 Confirm network traffic is permitted to enter into the virtual network

Pig my PC to the IP of EC2 (dta-web)

A screenshot of a computer

Description automatically generated

Figure 10 Ping from External Network to EC2

2.6.2 Confirm network traffic is permitted to travel through the virtual network

Ping the same network from dta-web2 to dta-web

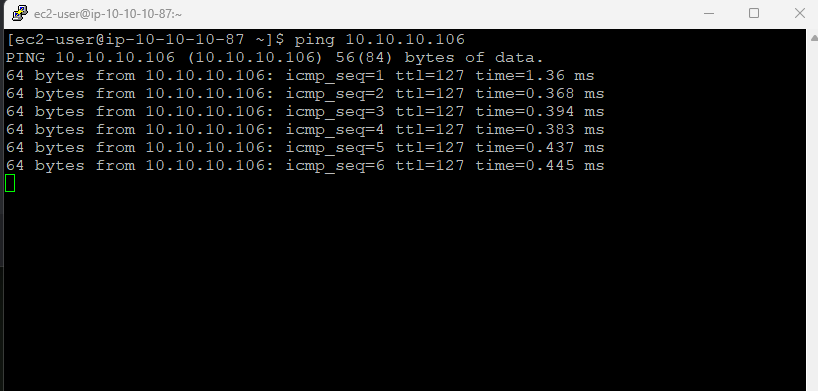


Figure 11 Ping to other IPs within the same network

2.6.3 Confirm network traffic is permitted to travel out of the virtual network

The dta-web can ping Google DNS 8.8.8.8 which means the virtual network can travel out to the external network.

A screen shot of a computer

Description automatically generated

Figure 12 EC2 can ping to public IP.

2.7 Include screen shots to show how you collected and monitored network traffic logs and other metrics. This can focus on collection and monitoring tasks using the AWS Cloudwatch tools that are available to you in the learning environment.

* Setup a CloudWatch alarm for CPU utilisation for DTA-Web Server

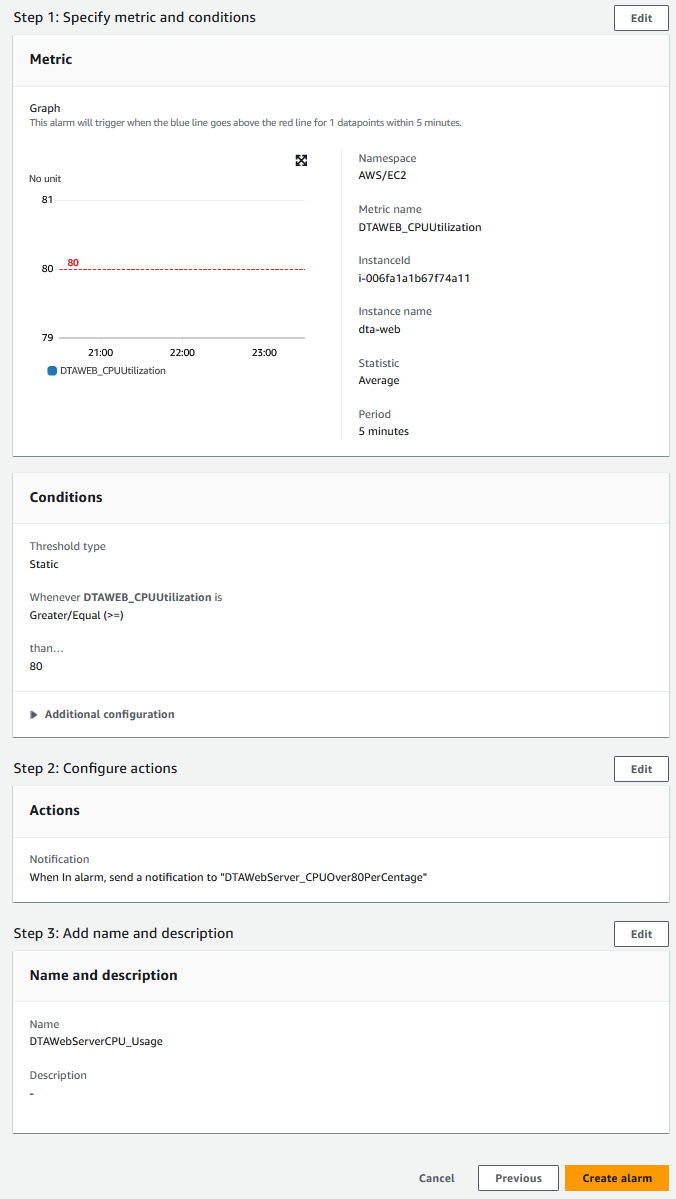


Figure 13 The metrics and conditions of dta-web CPUUtilisation.

* Monitoring EC2 instance (dta-web)

A screenshot of a computer

Description automatically generated

Figure 14 Monitoring dta-web instance.

* Monitoring EC2 instance (dta-web2)

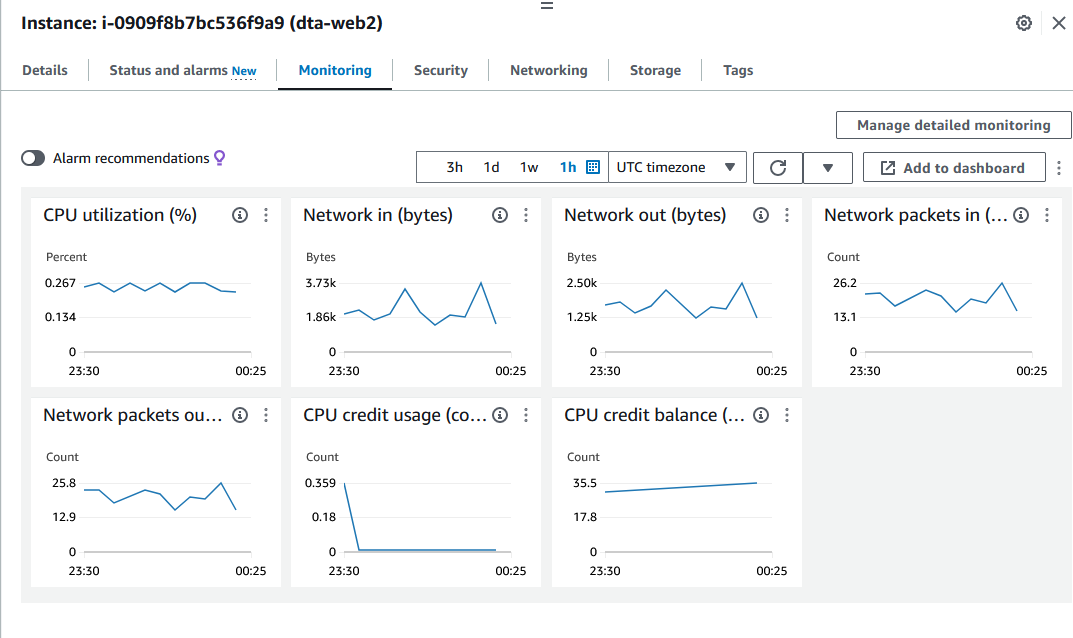


Figure 15 Monitoring dta-web2 instance.

2.8 Referring to your findings in question 2.6: explain how the testing that you completed has confirmed external connectivity to resources within the virtual network, and how only permitted traffic was able to access that resource.

The testing completed as per the document confirmed external connectivity to resources within the virtual network by verifying that network traffic was permitted to enter into, travel through, and travel out of the virtual network. This validation ensures that only permitted traffic can access the resources within the virtual network, enhancing security and control over network access.

2.9 Referring again to question 2.6:

a) Describe one of the major problems that you encountered.

I am unable to ping the IP address 10.10.10.106, and the reason is pinpointed to a security group configuration.

A screenshot of a computer

Description automatically generated

b) Describe the process you used to solve that problem.

1. Identify the Problem:

* Clearly define the communication issue (e.g., "Unable to ping 10.10.10.106").
* Analyse any error messages or diagnostics ("security group does not allow inbound access port ICMP-IPv4").

2. Access Cloud Console:

* Login to the AWS Management Console.

3. Modify Security Group Rules:

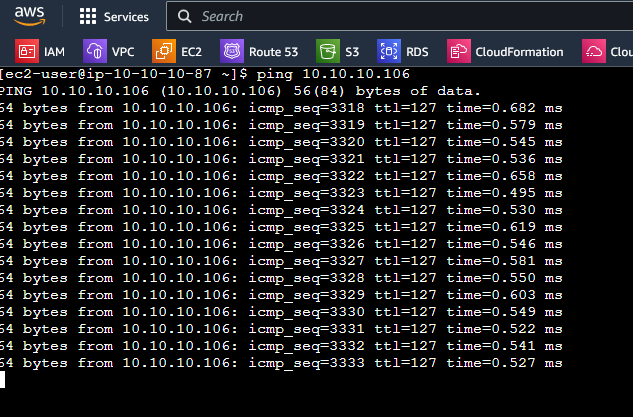
* Searching Security Groups in the search box.
* Click Security Groups

4. Edit Inbound Rules and Save Change:

* Choose dta-sg Security Group
* Inbound Rules -> Edit inbound rules
* Add rule all ICMP-IPv4 -> Source Custom 0.0.0.0/0
* Save the Rules

5. Test Connectivity:

* Ping from dta-web to dta-web2 the IP address: 10.10.10.106



c) What tools did you use?

1. AWS Management Console: The primary interface for managing the virtual network resources, including security groups. The AWS Management Console is accessed through a web browser.

2. Security Group Configuration Interface: Within the AWS Management Console, we can use the Security Group console to view and modify inbound and outbound access rules.

3. Ping Command Line Tool: The 'ping' command is a standard networking utility used to test the reachability of a host on an Internet Protocol (IP) network. It sends ICMP echo request packets to the target IP address and waits for ICMP echo reply packets. In this case, the 'ping' command would be used to test connectivity to the IP address 10.10.10.106 before and after making changes to the security group.

d) What was the step-by step-procedure that you followed (option to use a flow-chart)?

A diagram of a security group

Description automatically generated

e) What did you learn from that problem solving experience?

From this problem-solving experience, I learned the importance of thorough understanding and meticulous management of security controls in cloud environments. It highlighted the critical role that security groups play in regulating network traffic and ensuring the security of resources. By encountering and resolving the issue of restricted inbound access to the ICMP-IPv4 port, I gained a deeper understanding of how seemingly minor configuration settings can have significant implications for connectivity and accessibility.

Furthermore, this experience underscored the value of systematic troubleshooting and step-by-step analysis in resolving technical issues. By methodically identifying the problem, reviewing existing configurations, making targeted adjustments, and testing the solution, I reinforced the importance of a structured approach to problem-solving in complex IT environments. Overall, this experience enhanced my skills in managing cloud infrastructure, troubleshooting network issues, and implementing effective security measures.

# Reference

docs.aws.amazon.com. (n.d.). *create-internet-gateway — AWS CLI 1.32.67 Command Reference*. [online] Available at: https://docs.aws.amazon.com/cli/latest/reference/ec2/create-internet-gateway.html [Accessed 19 Mar. 2024].

‌docs.aws.amazon.com. (n.d.). *attach-internet-gateway — AWS CLI 1.32.67 Command Reference*. [online] Available at: https://docs.aws.amazon.com/cli/latest/reference/ec2/attach-internet-gateway.html [Accessed 19 Mar. 2024].

‌docs.aws.amazon.com. (n.d.). *create-route-table — AWS CLI 1.32.67 Command Reference*. [online] Available at: https://docs.aws.amazon.com/cli/latest/reference/ec2/create-route-table.html [Accessed 21 Mar. 2024].

‌docs.aws.amazon.com. (n.d.). *create-route — AWS CLI 1.32.67 Command Reference*. [online] Available at: https://docs.aws.amazon.com/cli/latest/reference/ec2/create-route.html [Accessed 19 Mar. 2024].

‌docs.aws.amazon.com. (n.d.). *create-security-group — AWS CLI 1.27.109 Command Reference*. [online] Available at: https://docs.aws.amazon.com/cli/latest/reference/ec2/create-security-group.html.

‌docs.aws.amazon.com. (n.d.). *Step 4: Configure security group inbound rules using the AWS CLI - Amazon DynamoDB*. [online] Available at: https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DAX.create-cluster.cli.configure-inbound-rules.html [Accessed 19 Mar. 2024].

‌