ATTACK DEFENSE

by PentesterAcademy

Name	VPC Enumeration
URL	https://attackdefense.com/challengedetails?cid=2425
Type	AWS Cloud Security : EC2

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

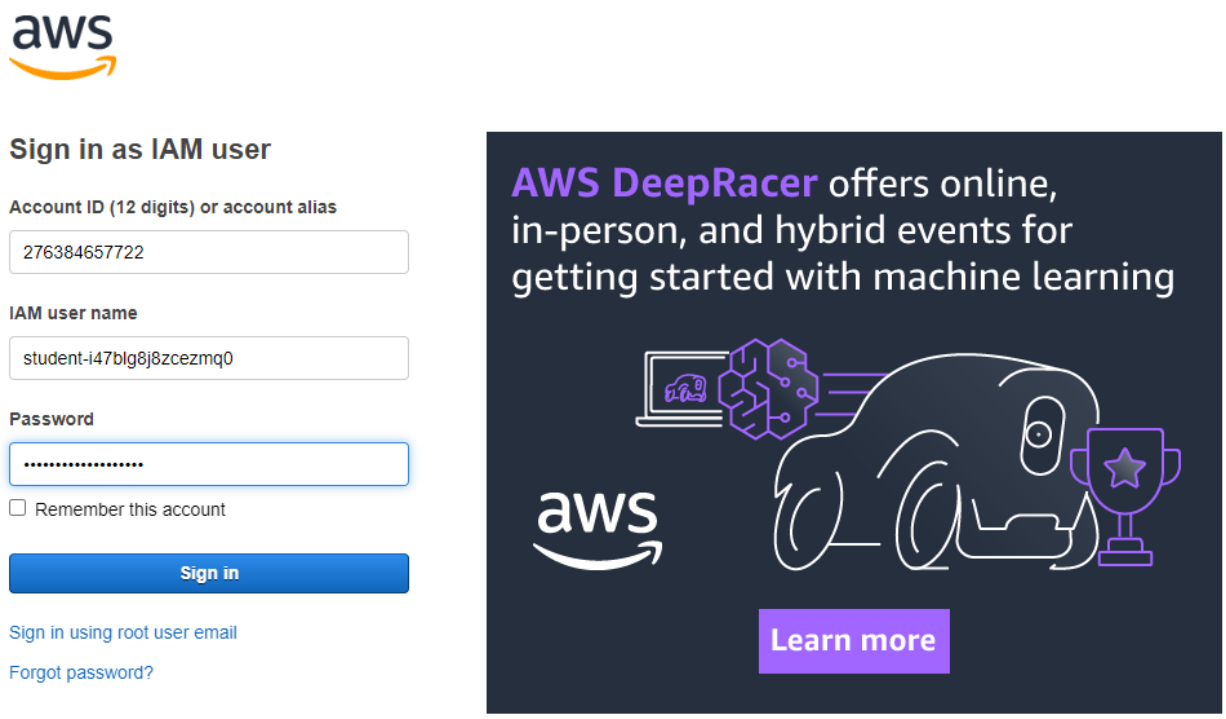
Solution:

Console Based Enumeration

Step 1: Click on the lab link button to get access to the AWS lab credentials.

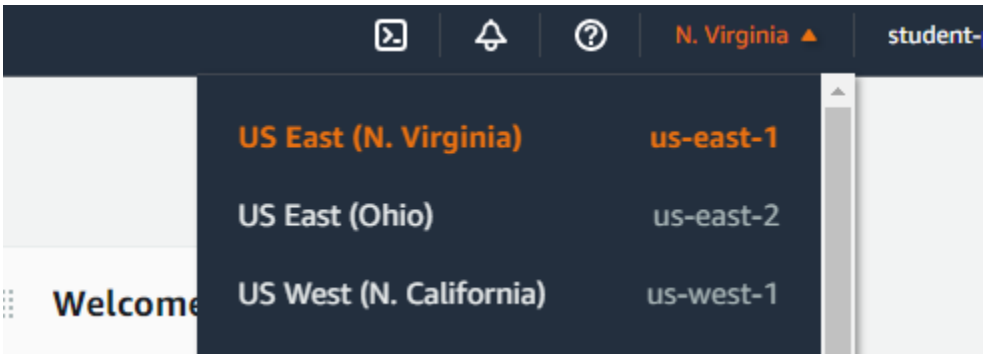
Login URL	https://276384657722.signin.aws.amazon.com/console
Region	Asia Pacific (Singapore) ap-southeast-1
Username	student-i47blg8j8zcezmq0
Password	c8PZVRx3TMjraIu61aC
Access Key ID	AKIAUAWOPGE5KDXBZHOM
Secret Access Key	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

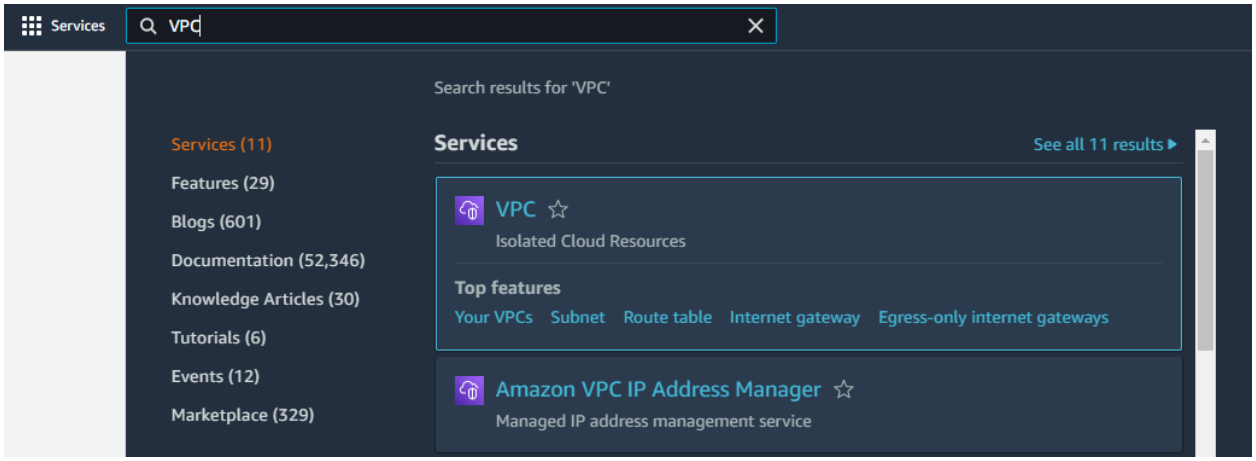
Step 2: Sign in to the AWS console.



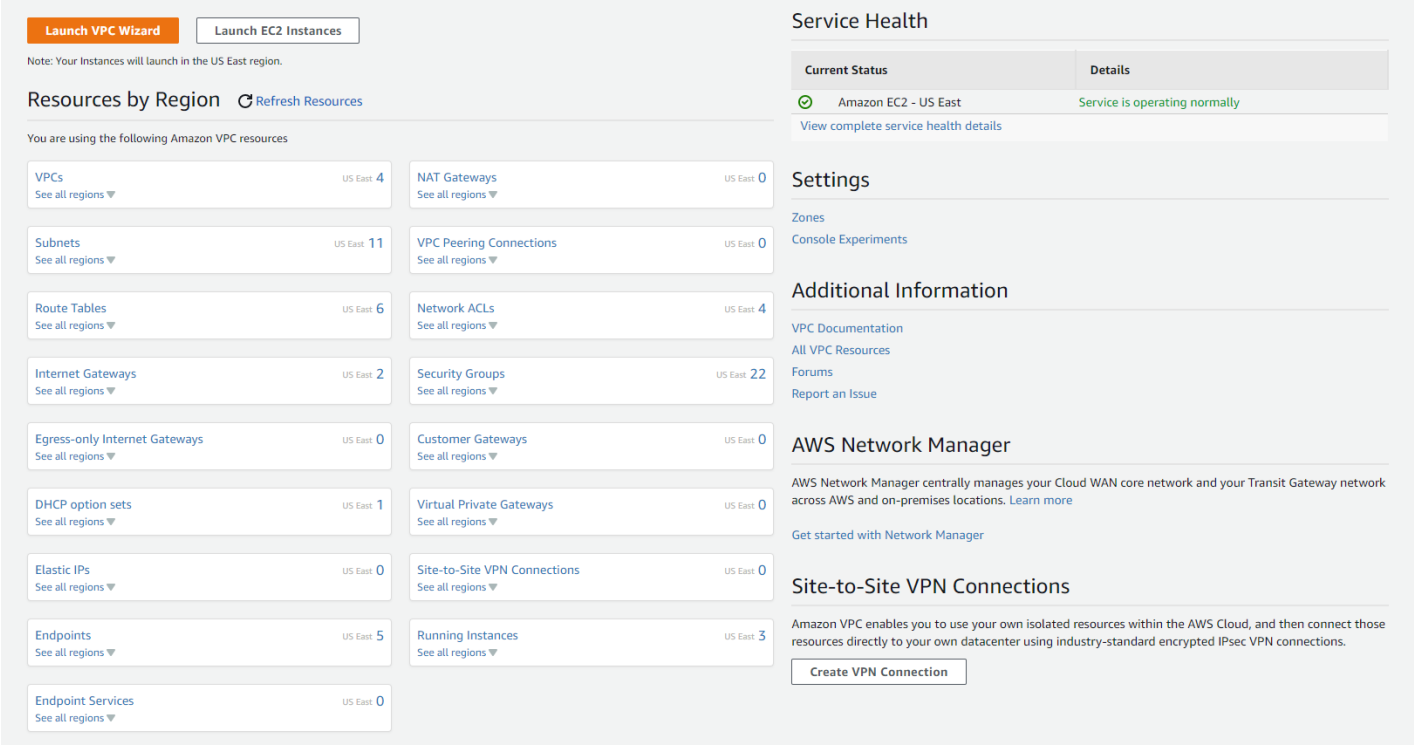
Step 3: Search for the VPC Dashboard and navigate to it.

Note: Change the region to “us-east-1”, if it is not selected by default.



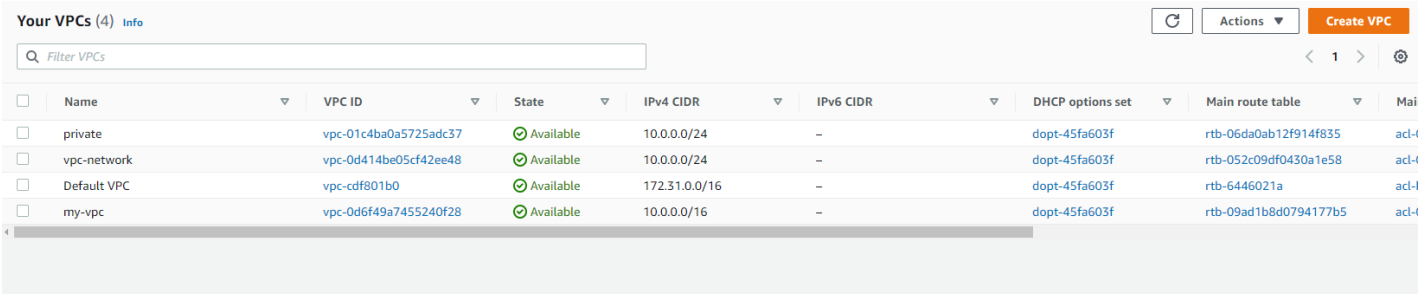


Step 4: Navigate to the VPC from the dashboard by clicking “VPCs” under the resources by region.

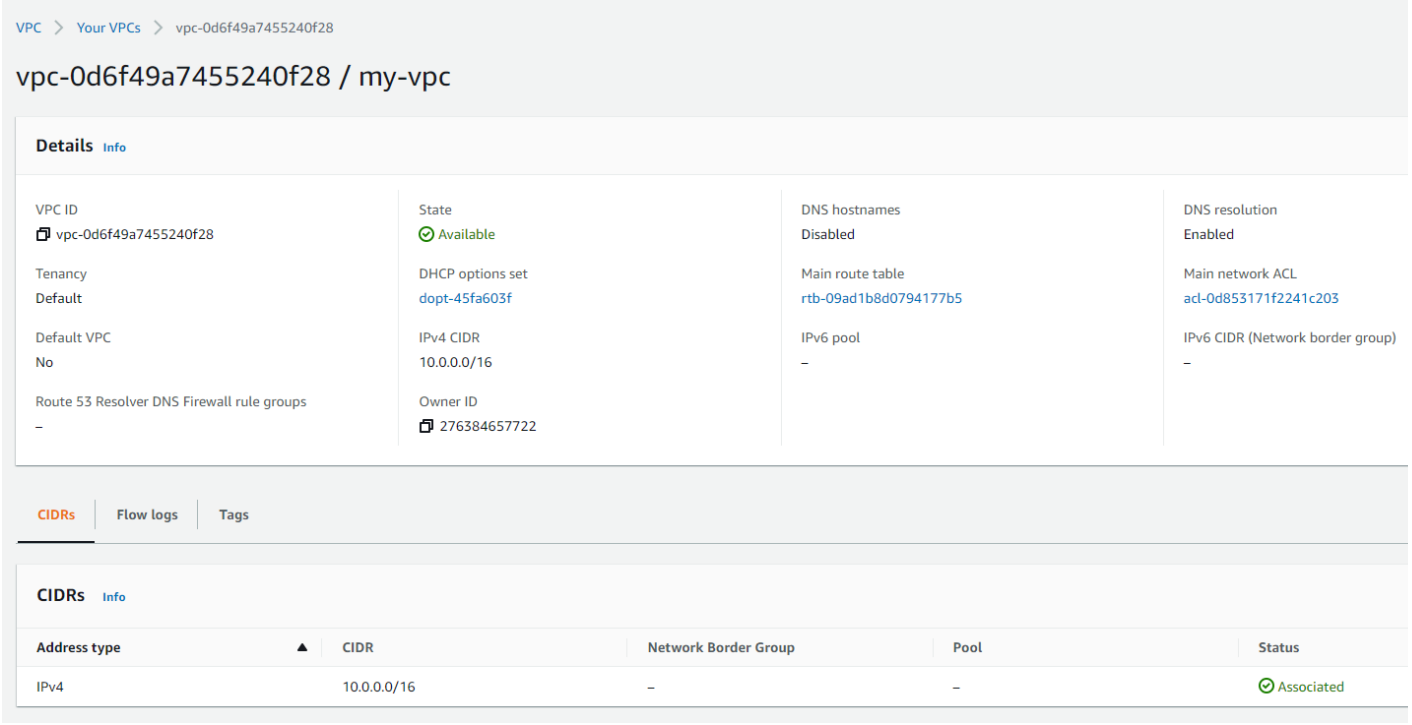


Step 5: Under VPC is a list of the VPCs deployed in the account. Click on VPC id with the name “my-vpc”.

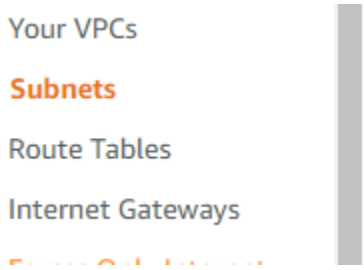
A virtual private cloud (VPC) is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS Cloud. You can launch your AWS resources, such as Amazon EC2 instances, into your VPC. You can specify an IP address range for the VPC, add subnets, associate security groups, and configure route tables.



The details of the VPC deployed are mentioned here.



Step 6: Click on subnets to see the list of available subnets in this account.



A subnet is a range of IP addresses in your VPC. You can launch AWS resources, such as EC2 instances, into a specific subnet. When you create a subnet, you specify the IPv4 CIDR block for the subnet, which is a subset of the VPC CIDR block. Each subnet must reside entirely within one Availability Zone and cannot span zones. By launching instances in separate Availability Zones, you can protect your applications from the failure of a single zone.

Subnets (11) Info

Filter subnets

Name	Subnet ID	State	VPC	IPv4 CIDR
My-Subnet-1	subnet-0db023f3337e57d0a	Available	vpc-0d6f49a7455240f28 | my...	10.0.1.0/24
–	subnet-8ca454bd	Available	vpc-cdf801b0 | Default VPC	172.31.48.0/20
–	subnet-bb18b09a	Available	vpc-cdf801b0 | Default VPC	172.31.80.0/20
private-2	subnet-0680e03de6c635bf1	Available	vpc-01c4ba0a5725adc37 | pri...	10.0.0.128/26
–	subnet-e3ea97ae	Available	vpc-cdf801b0 | Default VPC	172.31.16.0/20
–	subnet-c3b11ca5	Available	vpc-cdf801b0 | Default VPC	172.31.0.0/20
–	subnet-2c59f773	Available	vpc-cdf801b0 | Default VPC	172.31.32.0/20
private	subnet-08ca6afa10392c0d9	Available	vpc-01c4ba0a5725adc37 | pri...	10.0.0.0/26
My-Subnet-2	subnet-0117c0dfb9c3e60d4	Available	vpc-0d6f49a7455240f28 | my...	10.0.2.0/24
subnet	subnet-0f8eb1c3c34d6e36b	Available	vpc-0d414be05cf42ee48 | vpc...	10.0.0.128/25
–	subnet-658dea6b	Available	vpc-cdf801b0 | Default VPC	172.31.64.0/20

Step 7: Click on subnet id with the name “My-Subnet-1”.

The details of the subnet deployed are mentioned here.

VPC > Subnets > subnet-0db023f3337e57d0a

subnet-0db023f3337e57d0a / My-Subnet-1

Details

Subnet ID subnet-0db023f3337e57d0a	Subnet ARN arn:aws:ec2:us-east-1:276384657722:subnet/subnet-0db023f3337e57d0a	State Available	IPv4 CIDR 10.0.1.0/24
Available IPv4 addresses 251	IPv6 CIDR –	Availability Zone us-east-1a	Availability Zone ID use1-az4
Network border group us-east-1	VPC vpc-0d6f49a7455240f28 | my-vpc	Route table rtb-0f482764c0f62290f | My-Public-Routing-Table	Network ACL acl-0d853171f2241c203
Default subnet No	Auto-assign public IPv4 address Yes	Auto-assign IPv6 address No	Auto-assign customer-owned IPv4 address No
Customer-owned IPv4 pool –	Outpost ID –	IPv4 CIDR reservations –	IPv6 CIDR reservations –
IPv6-only No	Hostname type IP name	Resource name DNS A record Disabled	Resource name DNS AAAA record Disabled
DNS64 Disabled	Owner 276384657722		

Step 8: Click on Network ACL and check the network access control list.

It is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

Flow logs | Route table | Network ACL | CIDR reservations | Sharing | Tags

Network ACL: acl-0d853171f2241c203 — Edit network ACL association

Inbound rules (2)

Filter inbound rules

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

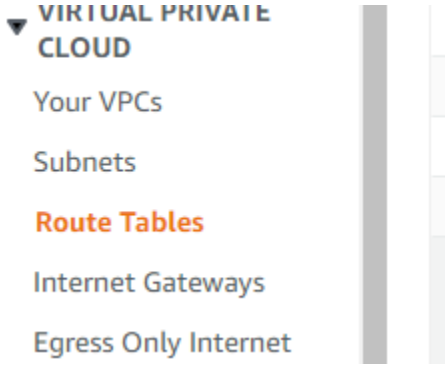
Outbound rules (2)

Filter outbound rules

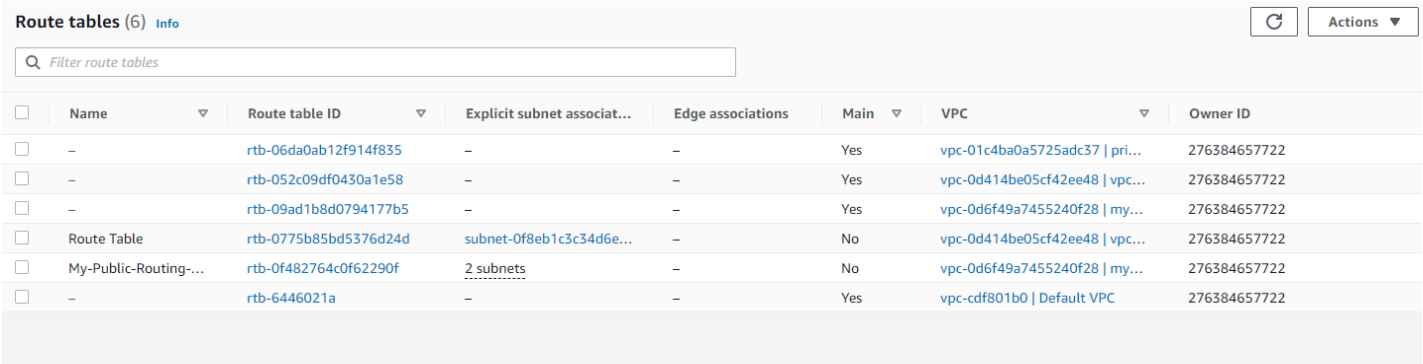
Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Step 9: Click on Route Tables to see the list of route tables available in the account.

.



A route table contains a set of rules, called routes, that determine where network traffic from your subnet or gateway is directed. Each subnet in your VPC must be associated with a route table, which controls the routing for the subnet (subnet route table). You can explicitly associate a subnet with a particular route table. Otherwise, the subnet is implicitly associated with the main route table. A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same subnet route table.



Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID
–	rtb-06da0ab12f914f835	–	–	Yes	vpc-01c4ba0a5725adc37 | pri...	276384657722
–	rtb-052c09df0430a1e58	–	–	Yes	vpc-0d414be05cf42ee48 | vpc...	276384657722
–	rtb-09ad1b8d0794177b5	–	–	Yes	vpc-0d6f49a7455240f28 | my...	276384657722
Route Table	rtb-0775b85bd5376d24d	subnet-0f8eb1c3c34d6e...	–	No	vpc-0d414be05cf42ee48 | vpc...	276384657722
My-Public-Routing-...	rtb-0f482764c0f62290f	2 subnets	–	No	vpc-0d6f49a7455240f28 | my...	276384657722
–	rtb-6446021a	–	–	Yes	vpc-cdf801b0 | Default VPC	276384657722

Step 10: Click on route table id with the name “My-Public-Routing-Table”.

Two routes are in this route table where one route has a target of local and the other one is associated with an internet gateway.

VPC > Route tables > rtb-0f482764c0f62290f

rtb-0f482764c0f62290f / My-Public-Routing-Table

You can now check network connectivity with Reachability Analyzer

Details Info

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-0f482764c0f62290f	No	2 subnets	–
VPC	**Owner ID**		
vpc-0d6f49a7455240f28 | my-vpc	276384657722		

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

Routes (2)

Filter routes | Both

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-07afdebebfb65c829	Active	No

Step 11: Click on Subnet associations to get the explicit subnet associations.

Here we have two subnet associations in this route table.

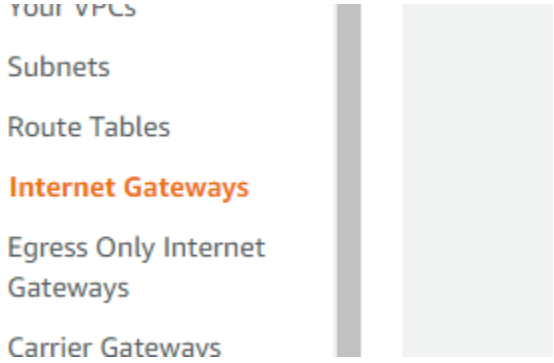
Routes | Subnet associations | Edge associations | Route propagation | Tags

Explicit subnet associations (2)

Find subnet association

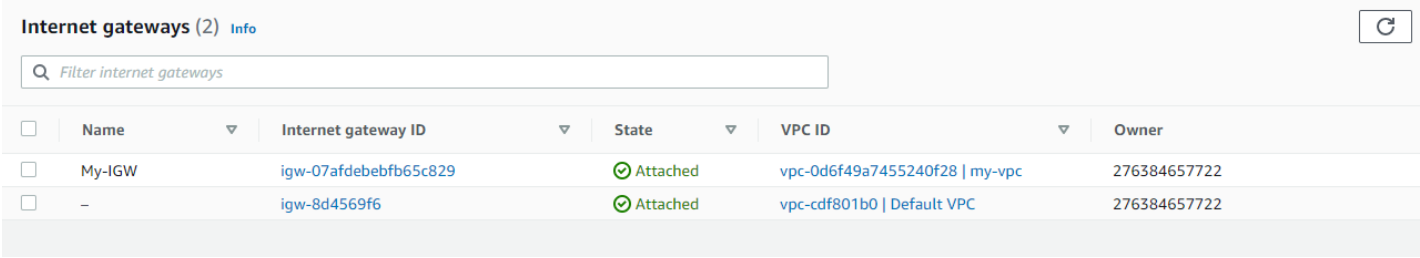
Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-0db023f3337e57d0a / My-Subnet-1	10.0.1.0/24	–
subnet-0117c0dfb9c3e60d4 / My-Subnet-2	10.0.2.0/24	–

Step 12: Click on Internet Gateways from the side panel.



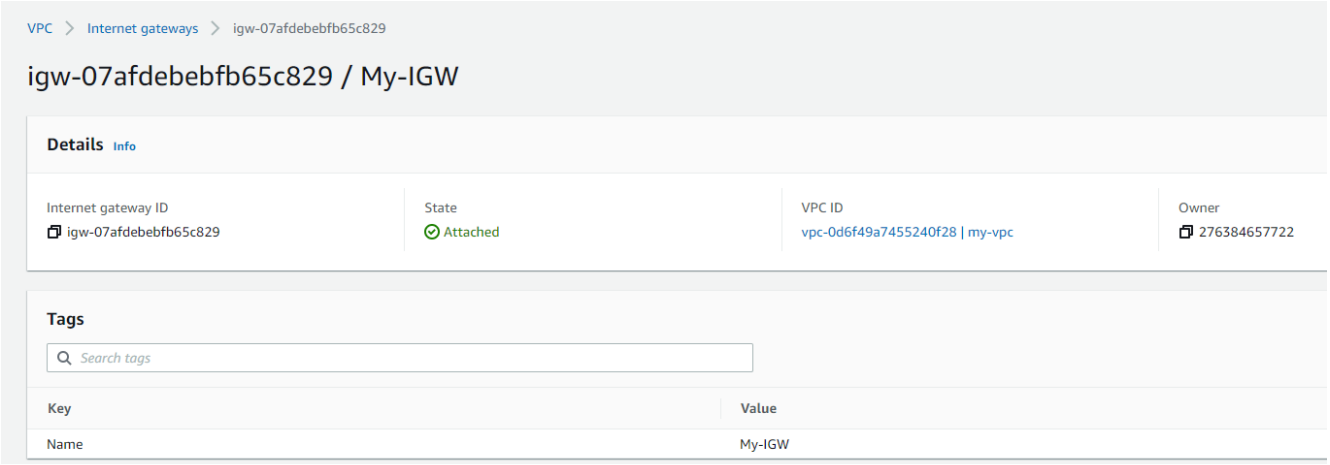
An internet gateway enables resources (like EC2 instances) in your public subnets to connect to the internet if the resource has a public IPv4 address or an IPv6 address. Similarly, resources on the internet can initiate a connection to resources in your subnet using the public IPv4 address or IPv6 address.

It will list the available internet gateways in the account here.



Step 13: Click on the internet gateway id with the name “My-IGW”.

The details associated with this internet gateway will be available here.



References:

1. AWS VPC documentation (https://docs.aws.amazon.com/vpc/latest/userguide)