AWS VPC

Overview & Hands-on Lab Walk Through

By: Muthuraja Ayyanar

Agenda

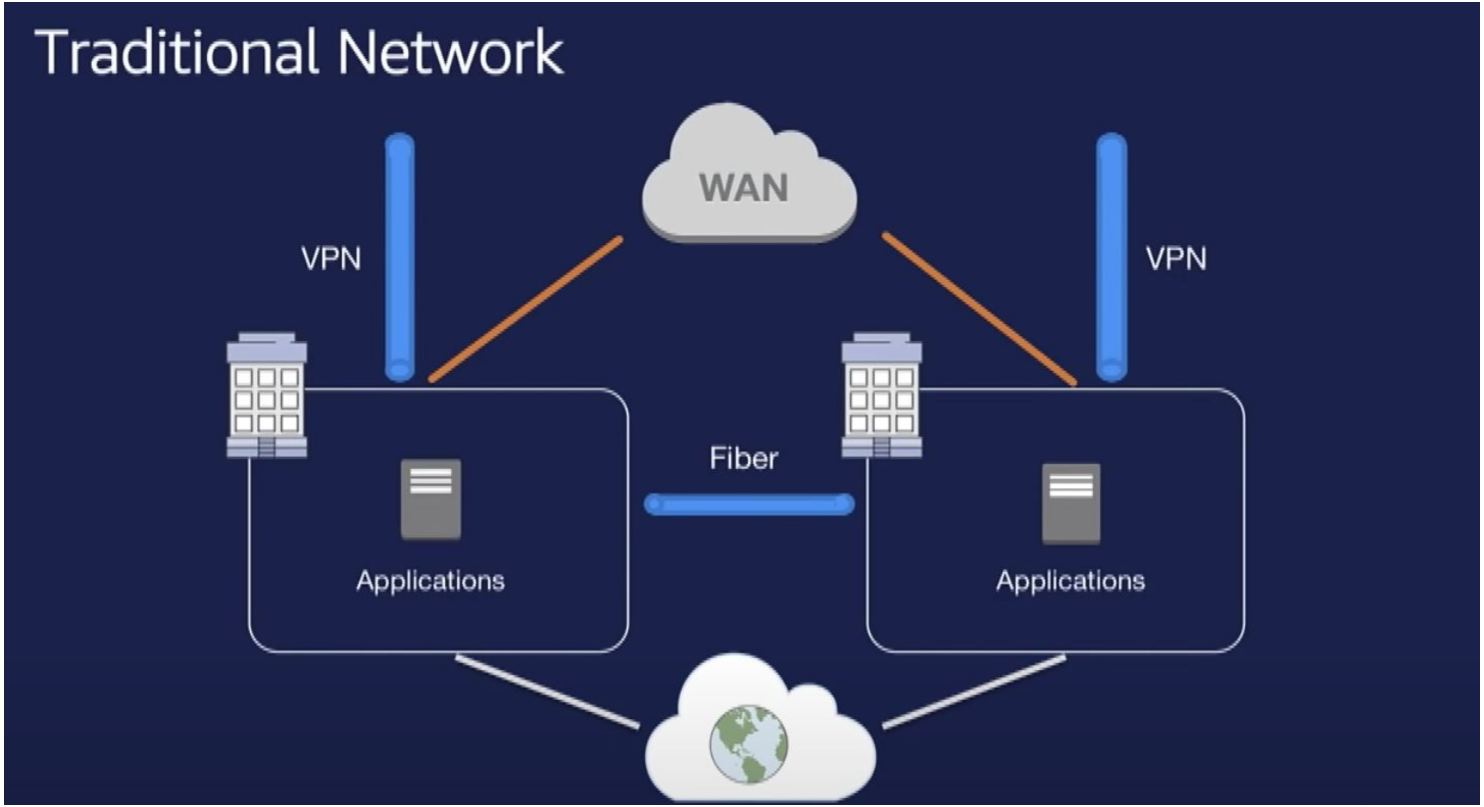
- What is VPC?
- Key VPC concepts (aka AWS Networking Fundamentals)
- AWS VPC Based services
- AWS Console walkthrough - VPC
  - VPC, Subnet Creation
  - Route Table, IGW walkthrough
  - Security (NACL, Security Group) walkthrough
- VPC Demo/Hands-on
  - Setup instance on Public Subnet & Allow Bi-dir Access to it from Externally
  - Setup instance on Private Subnet & allow Outbound access to it from VPC
  - Bastion Host use case

What is VPC Service?

Short Answer: Managed (Private) Data Center Service in Cloud

Long Answer: Virtual Private Cloud lets AWS customer create a Secure, dedicated (a logically isolated) network infrastructure with their own IP address range, subnets, route tables and security to design a Data Center in the Cloud the way they want and to deploy various services and resources to host their Application, DB infrastructure etc in a very short time

Traditional Network/On-Prem DC



Dlagram Source: From a slide :AWS London Summit 2018 - Breakout Session: VPC Design and New Capabilities for Amazon VPC

AWS Cloud DC/VPC

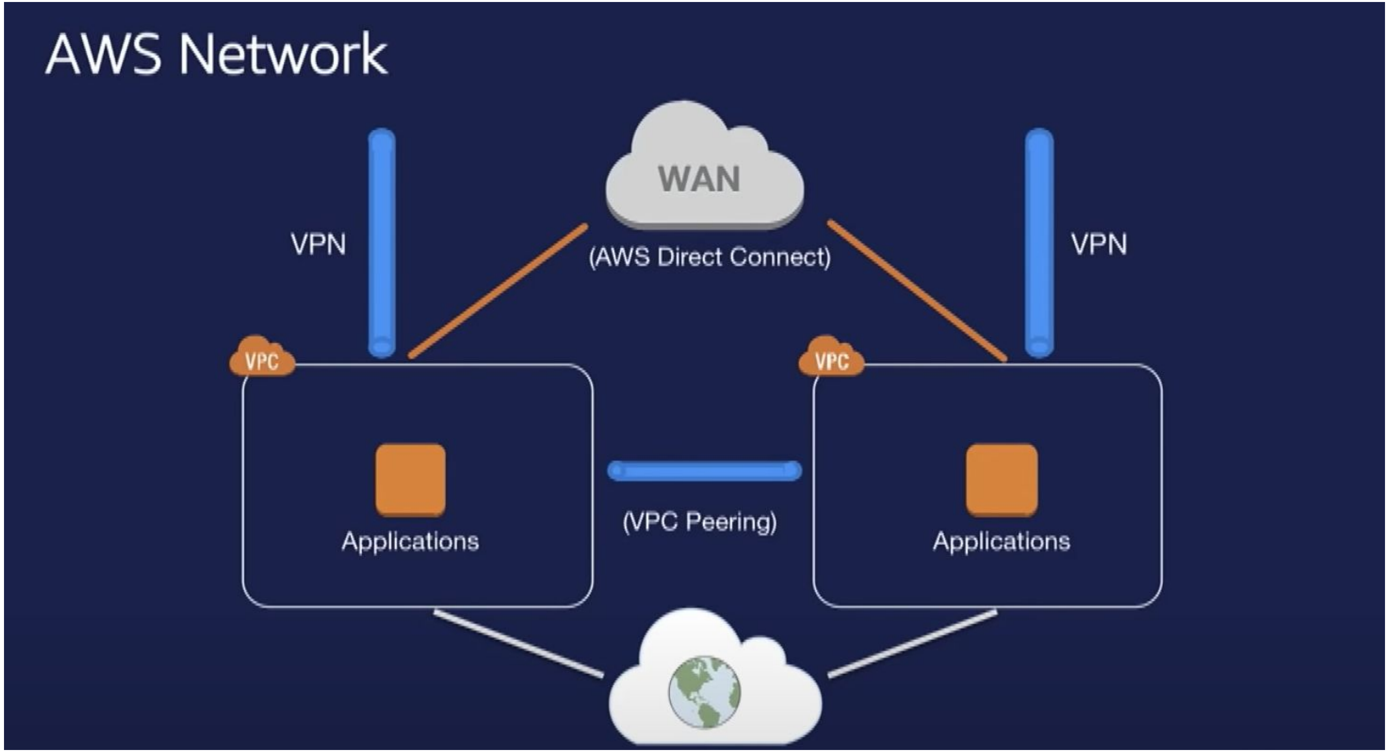
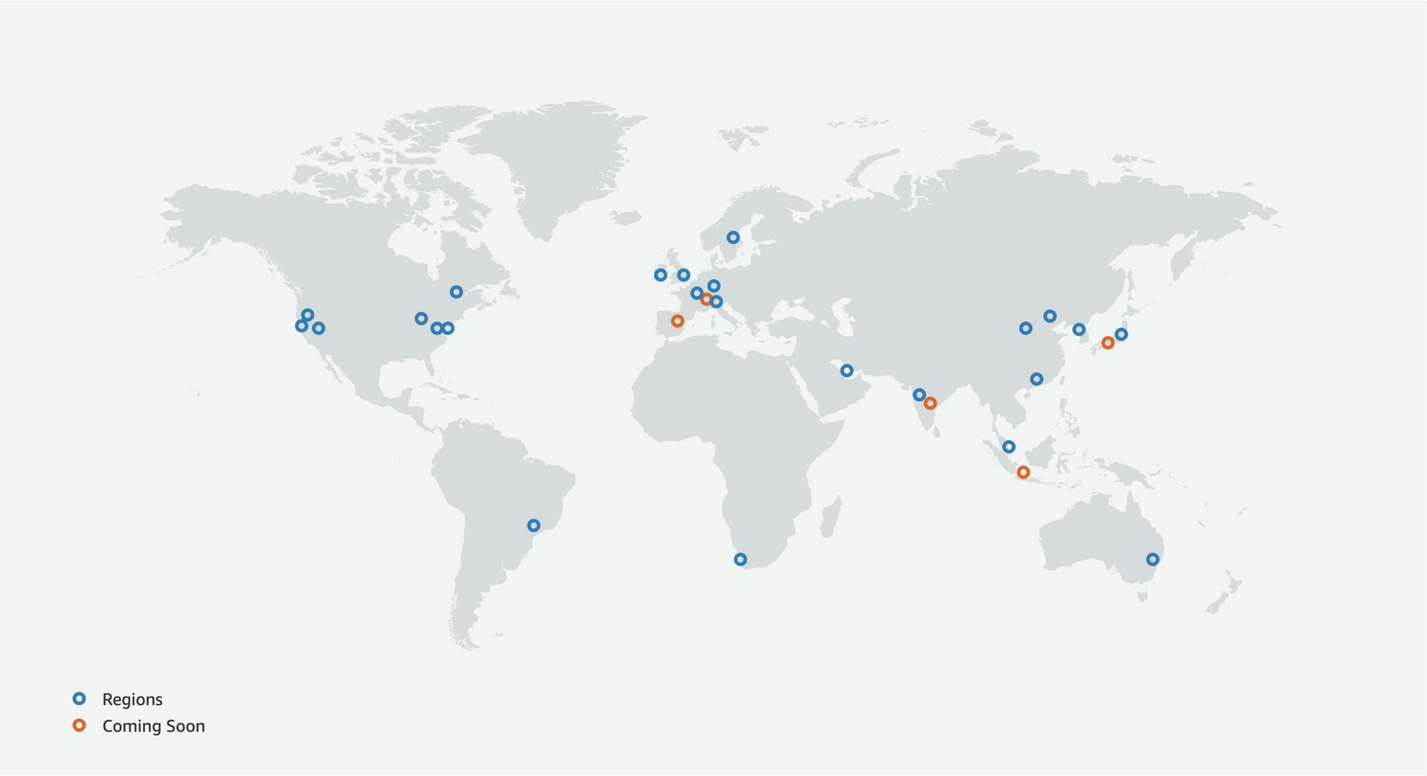


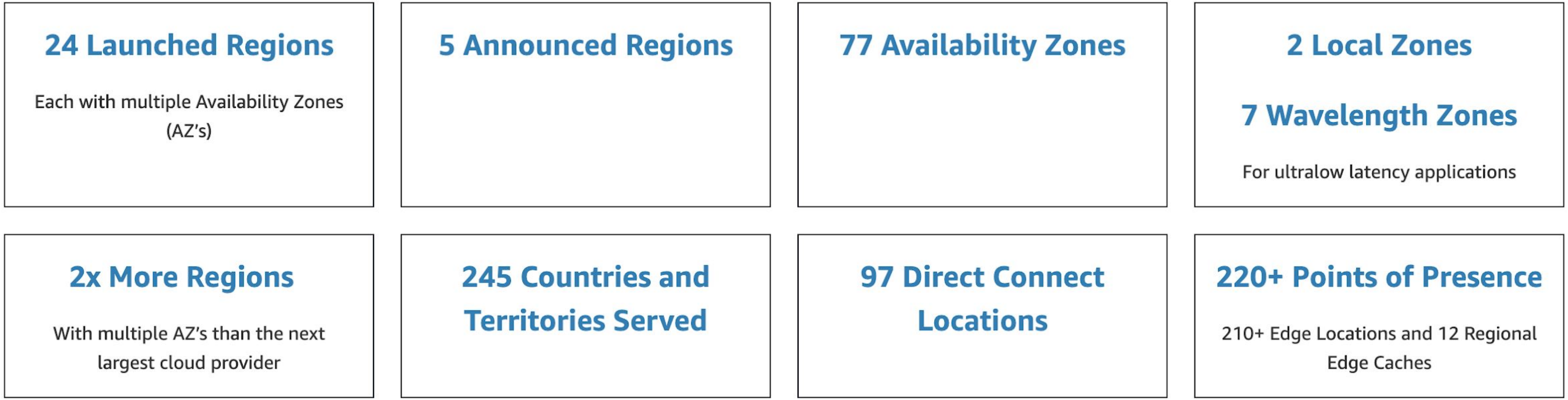
DIagram Source: From a slide :AWS London Summit 2018 - Breakout Session: VPC Design and New Capabilities for Amazon VPC

AWS Global Infrastructure



Source: https://aws.amazon.com/about-aws/global-infrastructure/

AWS Global Infrastructure



24 Launched Regions

Each with multiple Availability Zones (AZ's)

5 Announced Regions

77 Availability Zones

2 Local Zones

7 Wavelength Zones

For ultralow latency applications

2x More Regions

With multiple AZ's than the next largest cloud provider

245 Countries and Territories Served

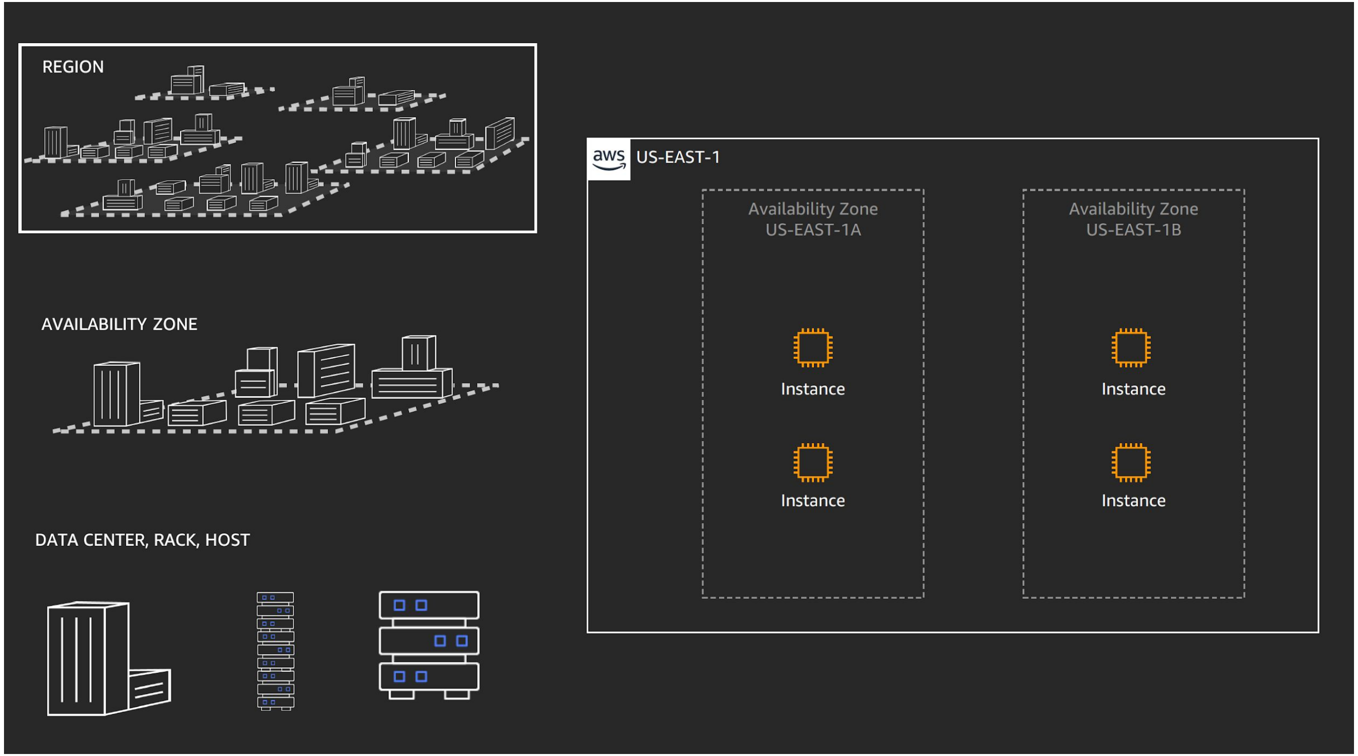
97 Direct Connect Locations

220+ Points of Presence

210+ Edge Locations and 12 Regional Edge Caches

Source: https://aws.amazon.com/about-aws/global-infrastructure/

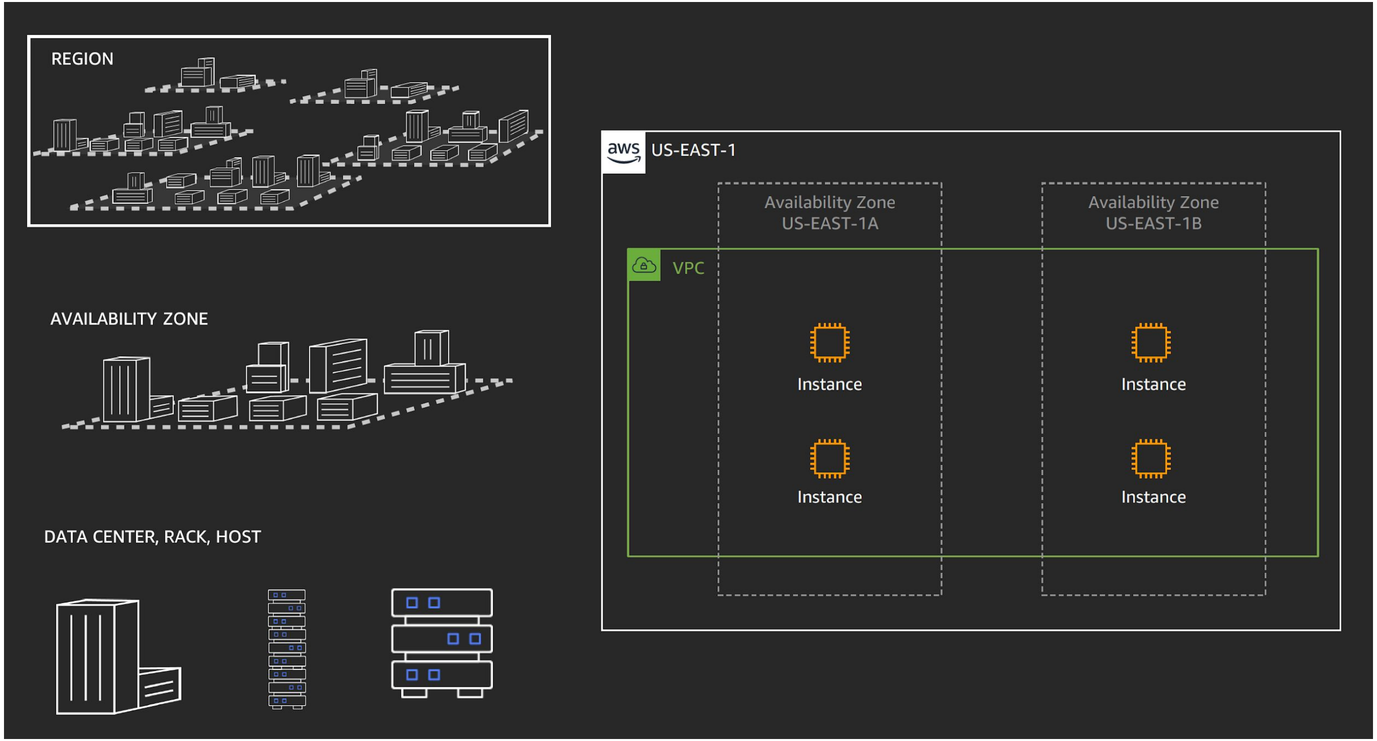
AWS Regions, AZ, VPC etc



- An AWS Region is a geographical location with a collection of availability zones (AZ) mapped to physical data centers in that region
- Each Region will have two or more Availability Zones
- An Availability Zone (AZ) is typically mapped to a DC in a given region
- While a single AZ can span multiple data centers, no two zones share a data center.
- Each AZ in a given region will have diverse/redundant/separate power, external network connectivity

Source: AWS re:Invent Slides (from NET-201 R Session)

AWS Regions, AZ, VPC etc



- VPC Spans across all AZ in a given Region
- Participating data centers in a zone are connected to each other over redundant low-latency private network links.
- All zones in a region communicate with each other over redundant private network links.
- These intra and inter-zone links are heavily used for data replication by a number of AWS services including storage and managed databases.
-

Source: AWS re:Invent Slides (from NET-201 R Session)

Core VPC Components

- CIDR
- Subnets
- Route Table
- Gateway(s)
- NACL
- Security Groups

CIDR, Subnet Overview

- CIDR - Classless Internet Domain Routing
- CIDR - Provides address space for your VPC
- More of IPv4 specific concept
- VPC CIDR typically uses addresses from RFC 1918 space
- AWS Automatically provides a single /16 ipv4 address space when a VPC is created (or for the default VPC)
- CIDR range supported in VPC : /16 (Largest) to /28 (Smallest)
- CIDR is broken down to small address space (aka subnets)
- Subnets could be Public or Private
- Subnets are typically mapped to AZ
- AWS automatically provides a /56 ipv6 address space when requested (from it's global ipv6 address space)

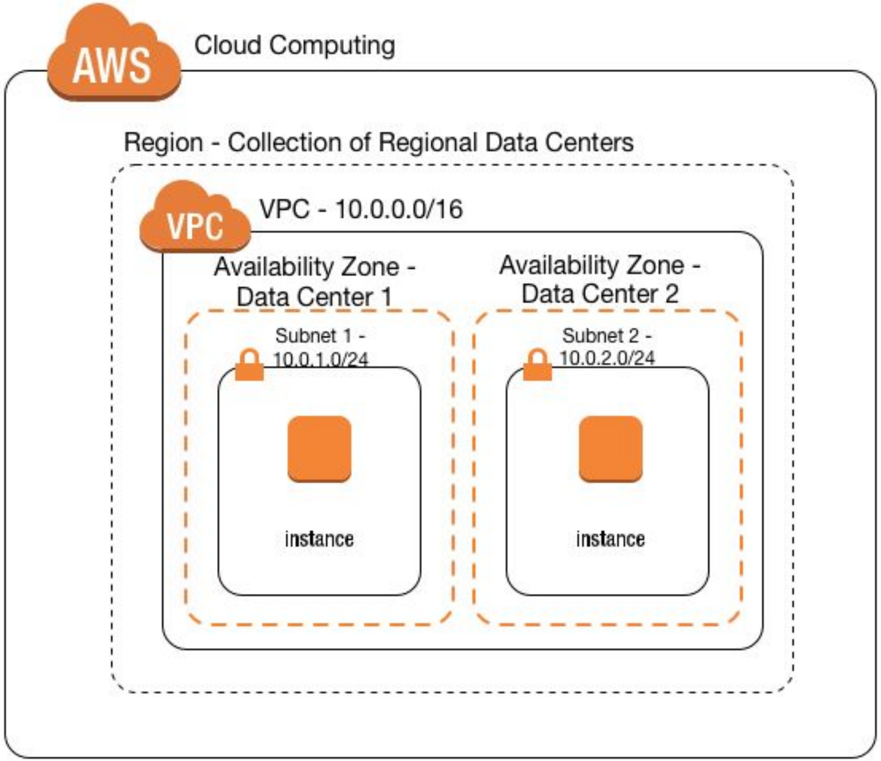
Route Table, Gateways and Endpoint Overview

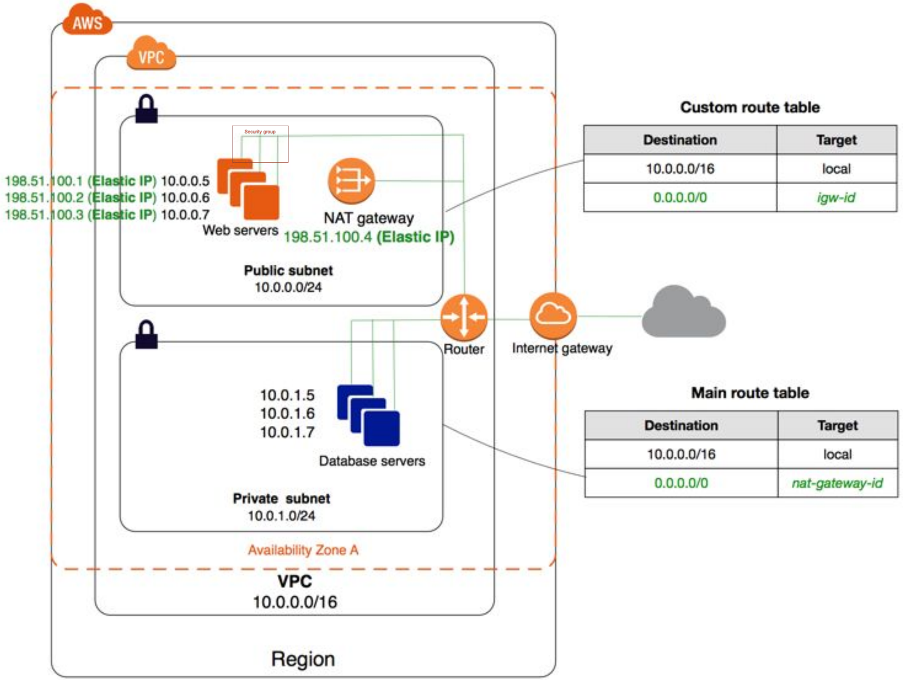
- **Route table** : A set of rules, called routes, that are used to determine where network traffic is directed.
- **Gateway** : A gateway (IGW/NAT) attaches to your VPC to enable communication between resources in your VPC and the internet.
- **VPC endpoint** : Enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink
  - With VPC Endpoint, there is no need for Internet gateway, NAT device, VPN connection, or AWS Direct Connect connection to access AWS Services or other services hosted in different VPC.
  - Instances in your VPC do not require public IP addresses to communicate with AWS resources/service.
  - Traffic between your VPC and the other service does not leave the Amazon network.

NACL and Security Groups Overview

- **NACL**: Network Access Control List, scoped @ Subnet level constitutes one or more ACE/Access Control Entries (ACE)
- By default there is one ACE in inbound and Outbound direction that allows all traffic
- NACL provides access control in a stateless manner
- NACL can be configured with ACE to either ALLOW or DENY based on L3 protocol, L4 port along with SRC/DST IP
- ACE are numbered from 1 to 65525 and are processed/applied in an ascending order
- **Security Group** : SG is applied to an Elastic Network Interface at the Instance Level
- Default Security Group allows communication from resources in Inbound direction that are using same SG
- Default Security Group allows access to all resources in the outbound direction
- Security Group provides access control in a stateful manner
- Security Group has an implict “DENY ALL” rule, only an explicit “ALLOW Rule” can be added
- Like NACL, SG can be configured to ALLOW based on L3 protocol, L4 port along with SRC/DST IP

VPC Implementation Examples


AWS
Cloud Computing
Region - Collection of Regional Data Centers
VPC
VPC - 10.0.0.0/16
Availability Zone - Data Center 1
Availability Zone - Data Center 2
Subnet 1 - 10.0.1.0/24
Subnet 2 - 10.0.2.0/24
instance
instance



Custom route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*igw-id*

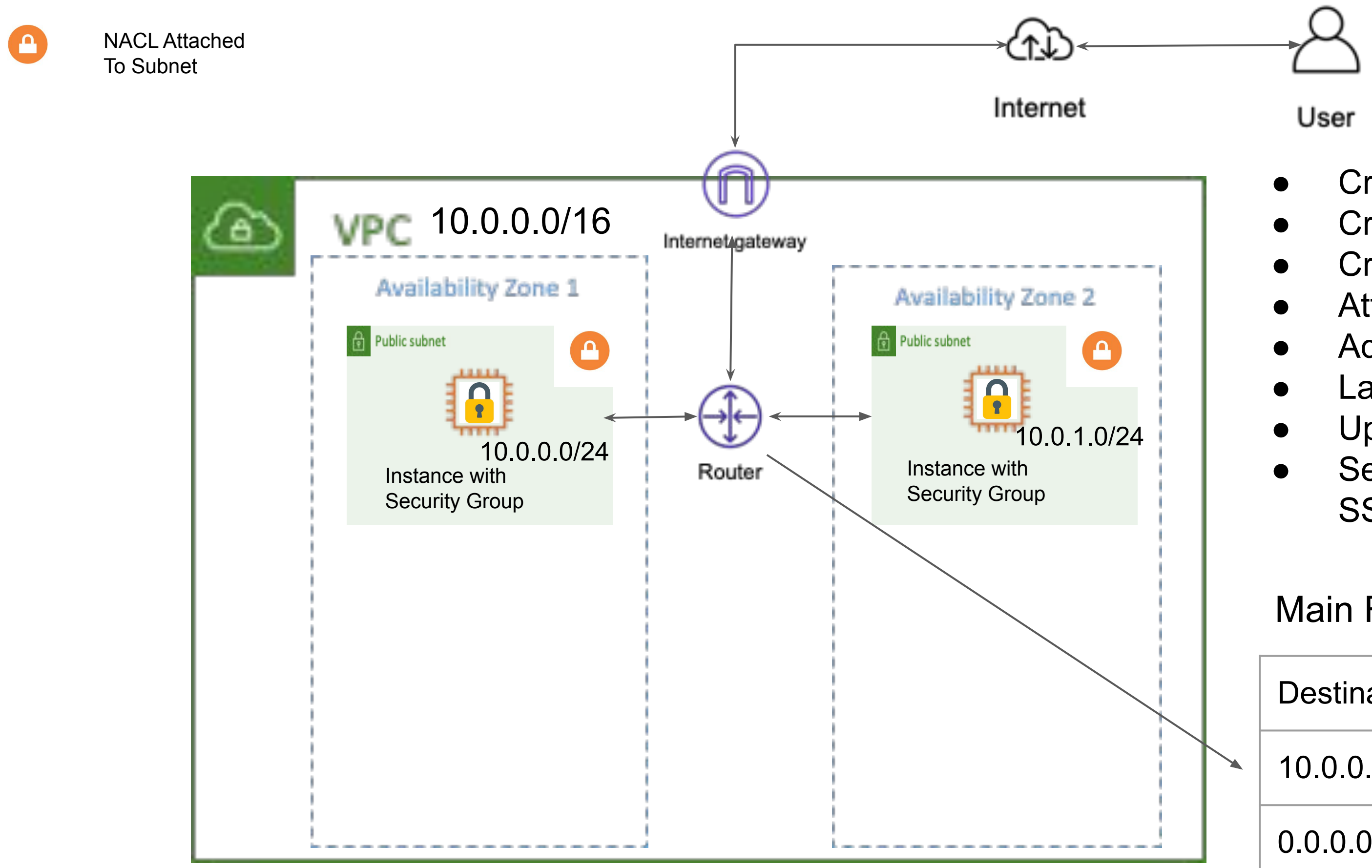
Main route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*nat-gateway-id*

VPC Services

- Internet Gateway (Covered in Hands-on)
- NAT Gateway (Covered in Hands-on)
- Egress Only Gateway (Covered in Hands-on)
- VPC Endpoint Services (Gateway/Interfaces)
- VPC Peer Gateway
- Transit Gateway
- Direct Connect
- VPN Gateway

Hands-on #1 : Access Instance from External Network



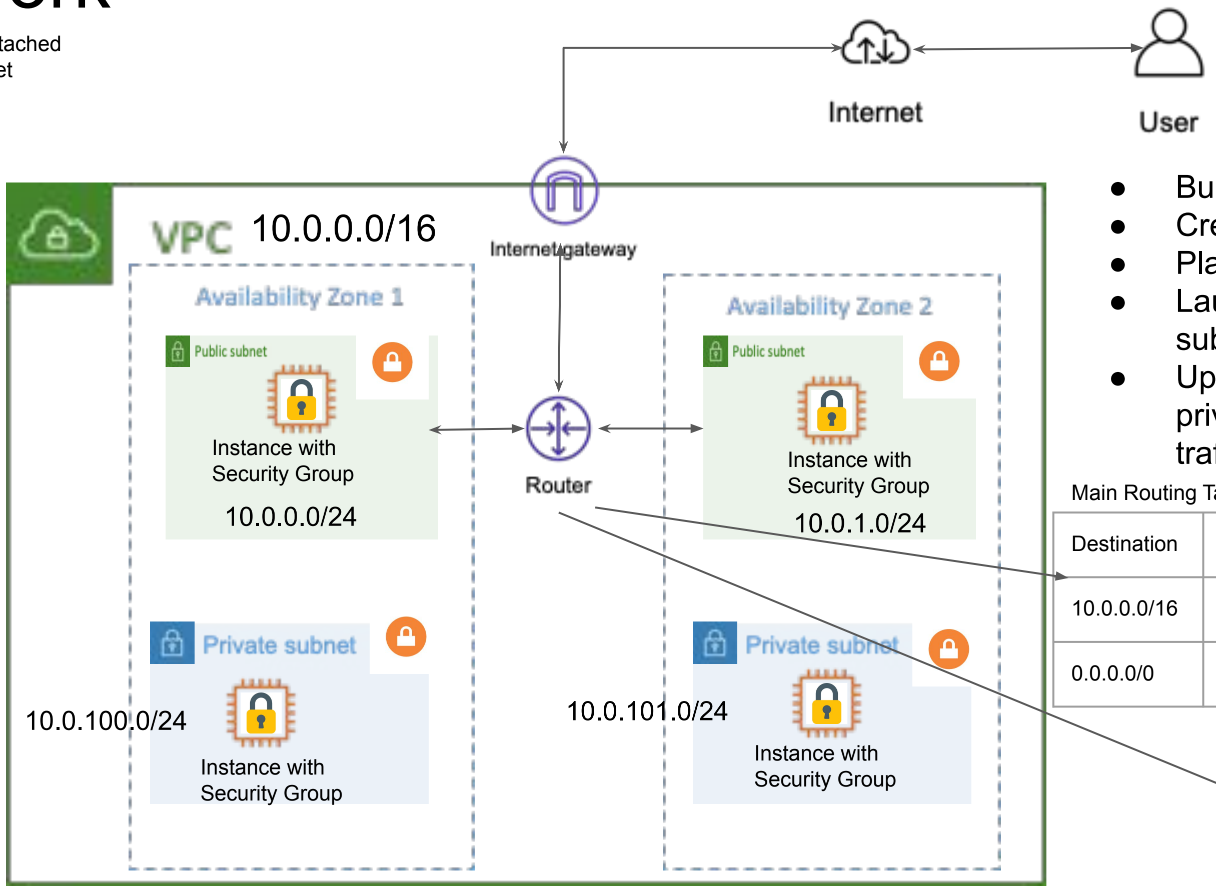
- Create VPC
- Create Subnet
- Create Internet Gateway
- Attach to VPC
- Add default route
- Launch EC2 Instance
- Update Security Group/NACL
- Security group allows ICMP, SSH from external network

Main Routing Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	IGW

Hands-on #2 : Access Private Instance from External Network

🔒 NACL Attached To Subnet



- Building on Handson #1
- Create a second Route Table
- Place private subnets in it
- Launch EC2 Instance in private subnet
- Update Security Group for private subnet instance to allow traffic from public subnet only

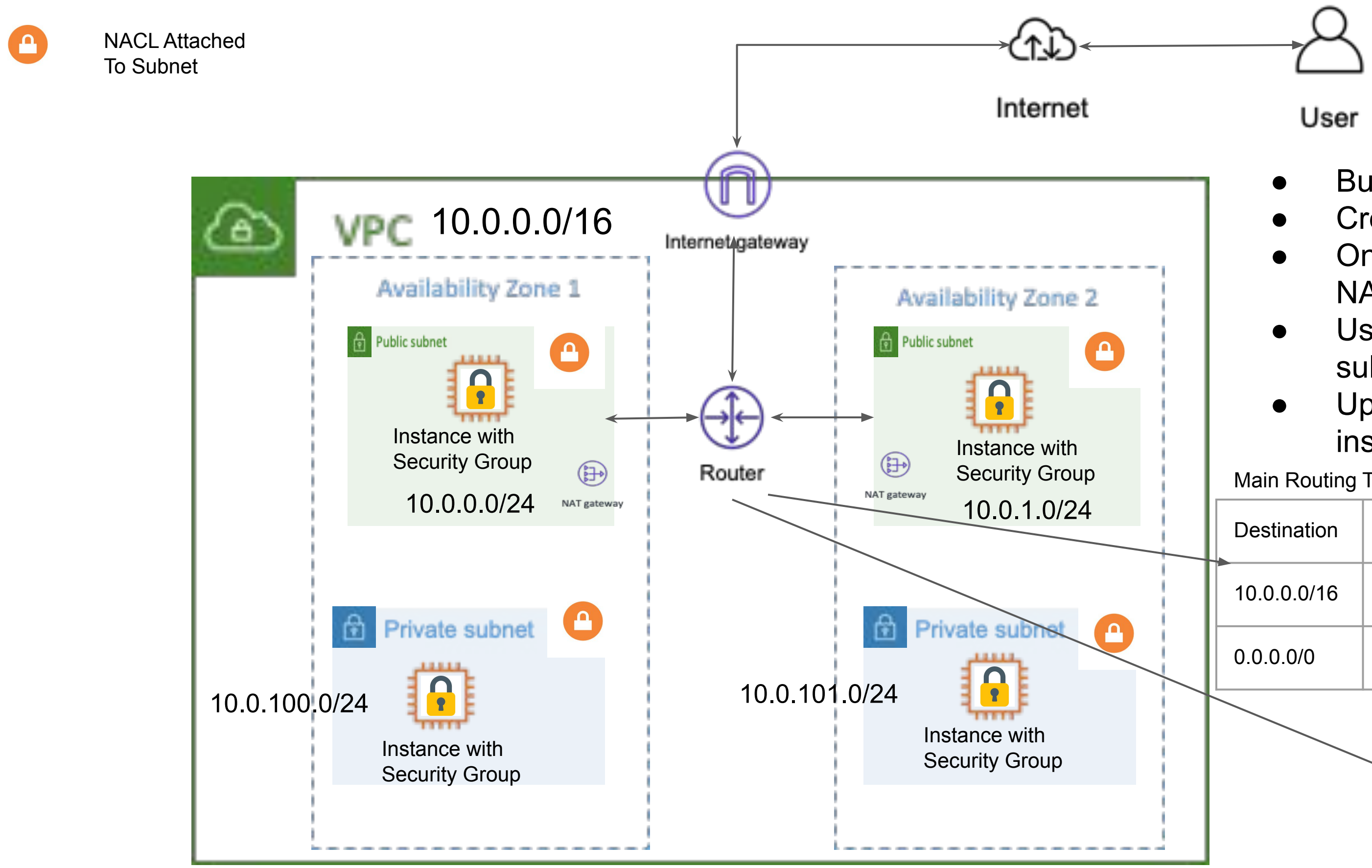
Main Routing Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	IGW

Private Routing Table

Destination	Target
10.0.0.0/16	local
10.0.100.0/024	local
10.0.101.0/24	local

Hands-on #3 : NAT Gateway for Private Instance to Access External Network



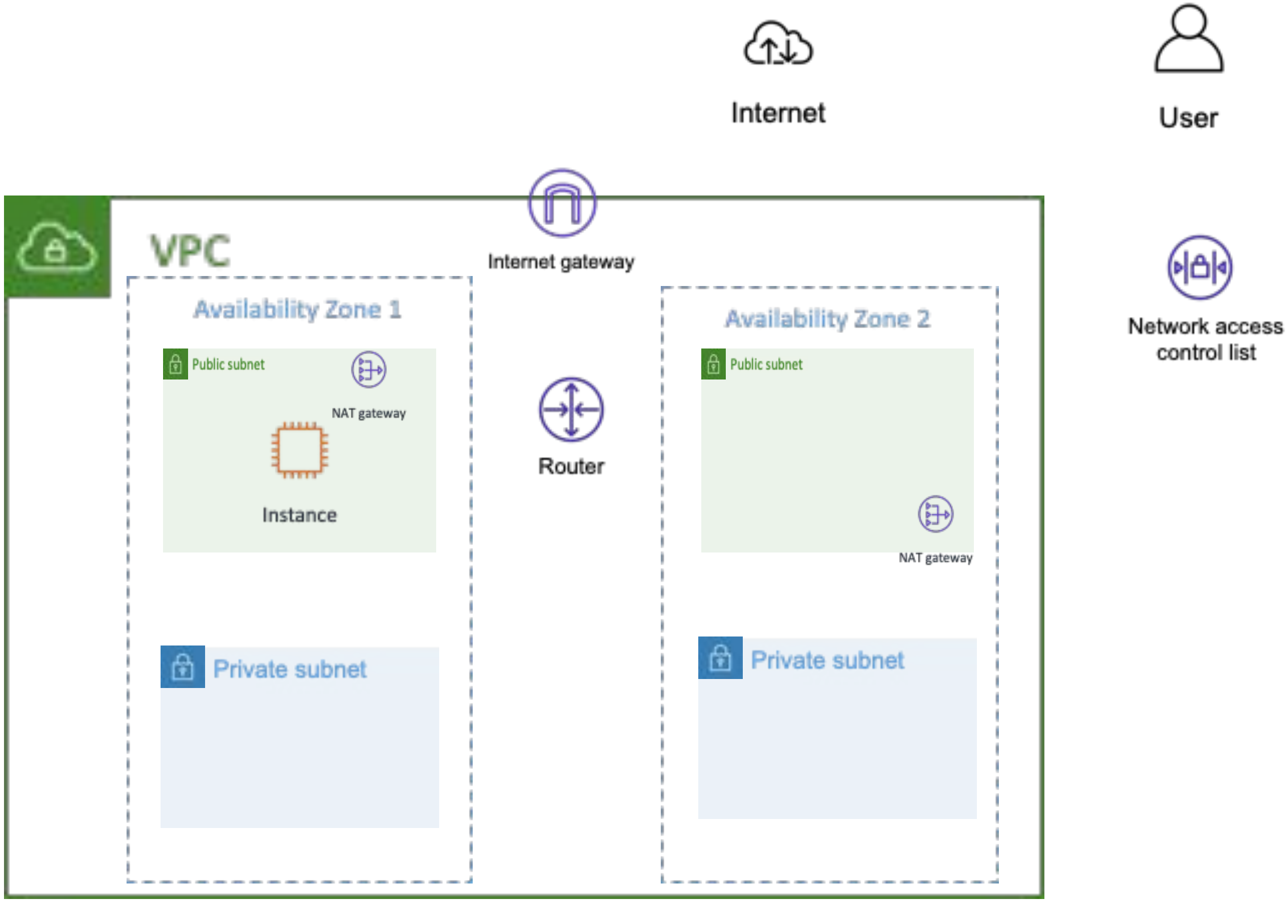
- Building on Handson #2
- Create a NAT Gateway with EIP
- On priv RT add def route with NAT GW as NH
- Use EC2 Instance in private subnet
- Update SG on Private EC2 instance to use def SG

Main Routing Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	IGW

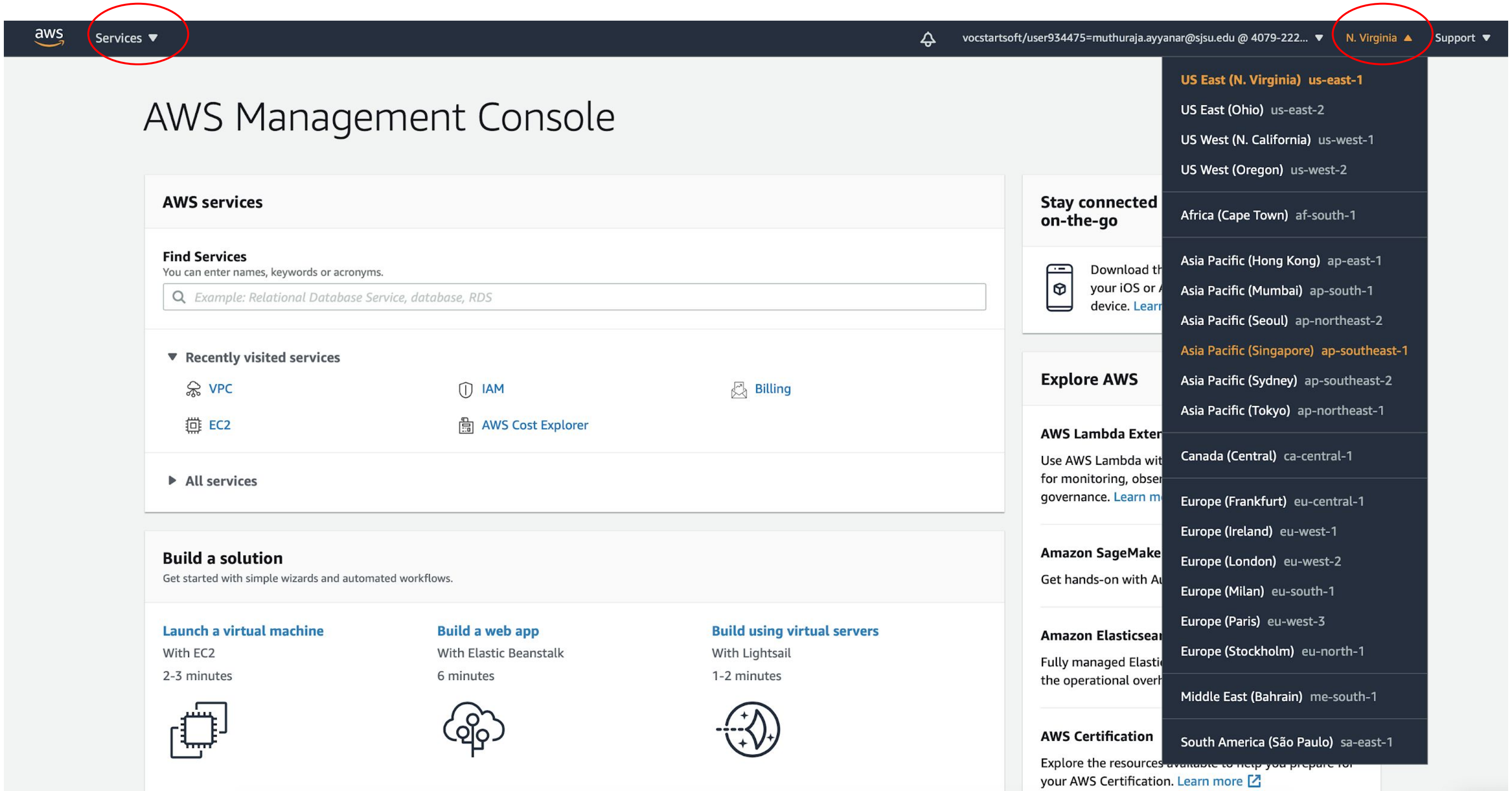
Private Routing Table

Destination	Target
10.0.0.0/16	local
10.0.100.0/024	local
10.0.101.0/24	local
0.0.0.0/0	NAT GW


Internet
User
VPC
Internet gateway
Availability Zone 1
Public subnet
NAT gateway
Instance
Private subnet
Router
Availability Zone 2
Public subnet
NAT gateway
Private subnet
Network access control list

VPC Hands-on

To deploy a VPC. First sign into the console. Select a (your) region that is closest to you.



aws
Services ▼
vocstartsoft/user934475=muthuraja.ayyanar@sjsu.edu @ 4079-222... ▼
N. Virginia ▲
Support ▼

AWS Management Console

AWS services

Find Services
You can enter names, keywords or acronyms.

Example: Relational Database Service, database, RDS

▼ Recently visited services

VPC IAM Billing
EC2 AWS Cost Explorer

▶ All services

Build a solution
Get started with simple wizards and automated workflows.

Launch a virtual machine
With EC2
2-3 minutes

Build a web app
With Elastic Beanstalk
6 minutes

Build using virtual servers
With Lightsail
1-2 minutes

Stay connected on-the-go

Download th
your iOS or
device. Learn

Explore AWS

AWS Lambda Exten
Use AWS Lambda wit
for monitoring, obse
governance. Learn m

Amazon SageMake
Get hands-on with A

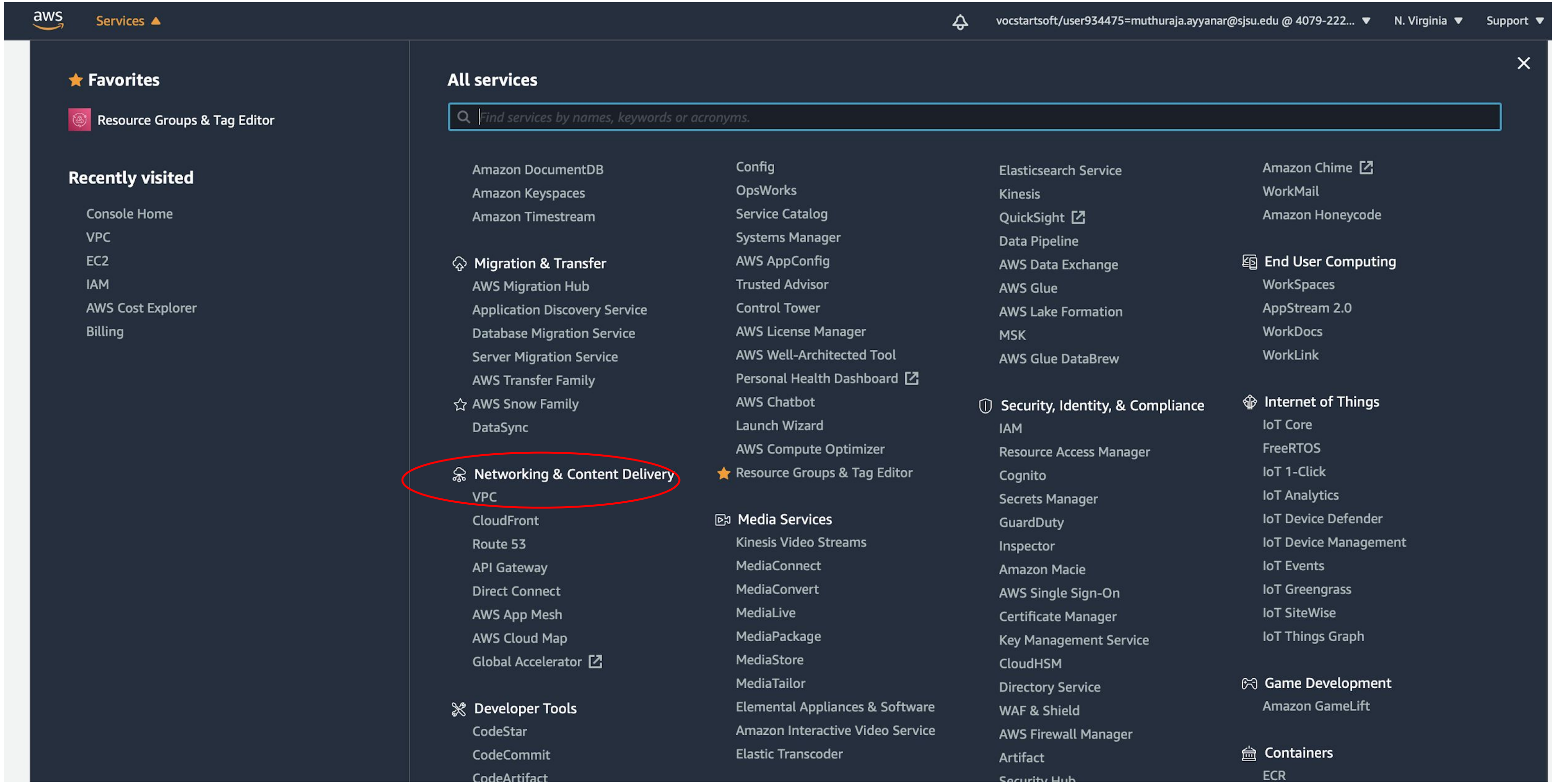
Amazon Elasticsear
Fully managed Elasti
the operational overh

AWS Certification
Explore the resources available to help you prepare for your AWS Certification. Learn more

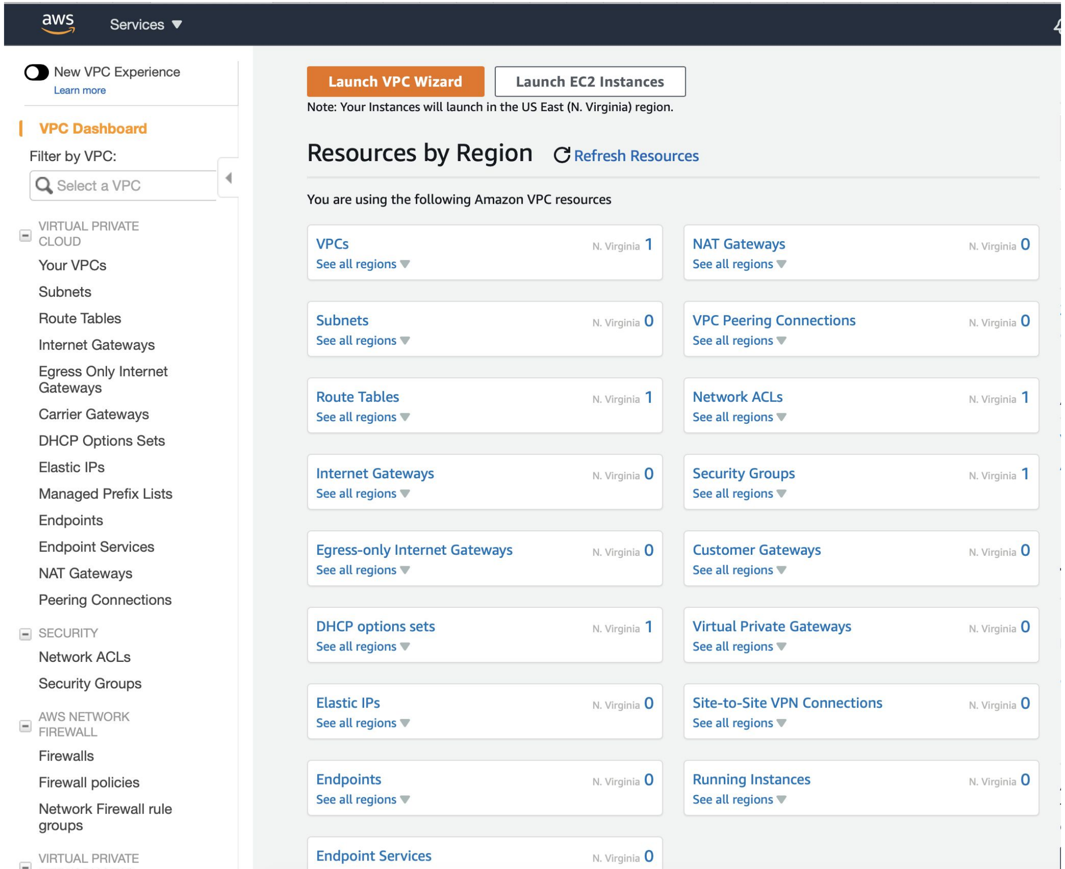
- US East (N. Virginia) us-east-1
- US East (Ohio) us-east-2
- US West (N. California) us-west-1
- US West (Oregon) us-west-2
- Africa (Cape Town) af-south-1
- Asia Pacific (Hong Kong) ap-east-1
- Asia Pacific (Mumbai) ap-south-1
- Asia Pacific (Seoul) ap-northeast-2
- Asia Pacific (Singapore) ap-southeast-1
- Asia Pacific (Sydney) ap-southeast-2
- Asia Pacific (Tokyo) ap-northeast-1
- Canada (Central) ca-central-1
- Europe (Frankfurt) eu-central-1
- Europe (Ireland) eu-west-1
- Europe (London) eu-west-2
- Europe (Milan) eu-south-1
- Europe (Paris) eu-west-3
- Europe (Stockholm) eu-north-1
- Middle East (Bahrain) me-south-1
- South America (São Paulo) sa-east-1

VPC Hands-on

Click on “All Services search box and search for VPC” or click “VPC” under “Networking and Content Delivery.”



Default VPC Resource Dashboard



Note: Your Instances will launch in the US East (N. Virginia) region.

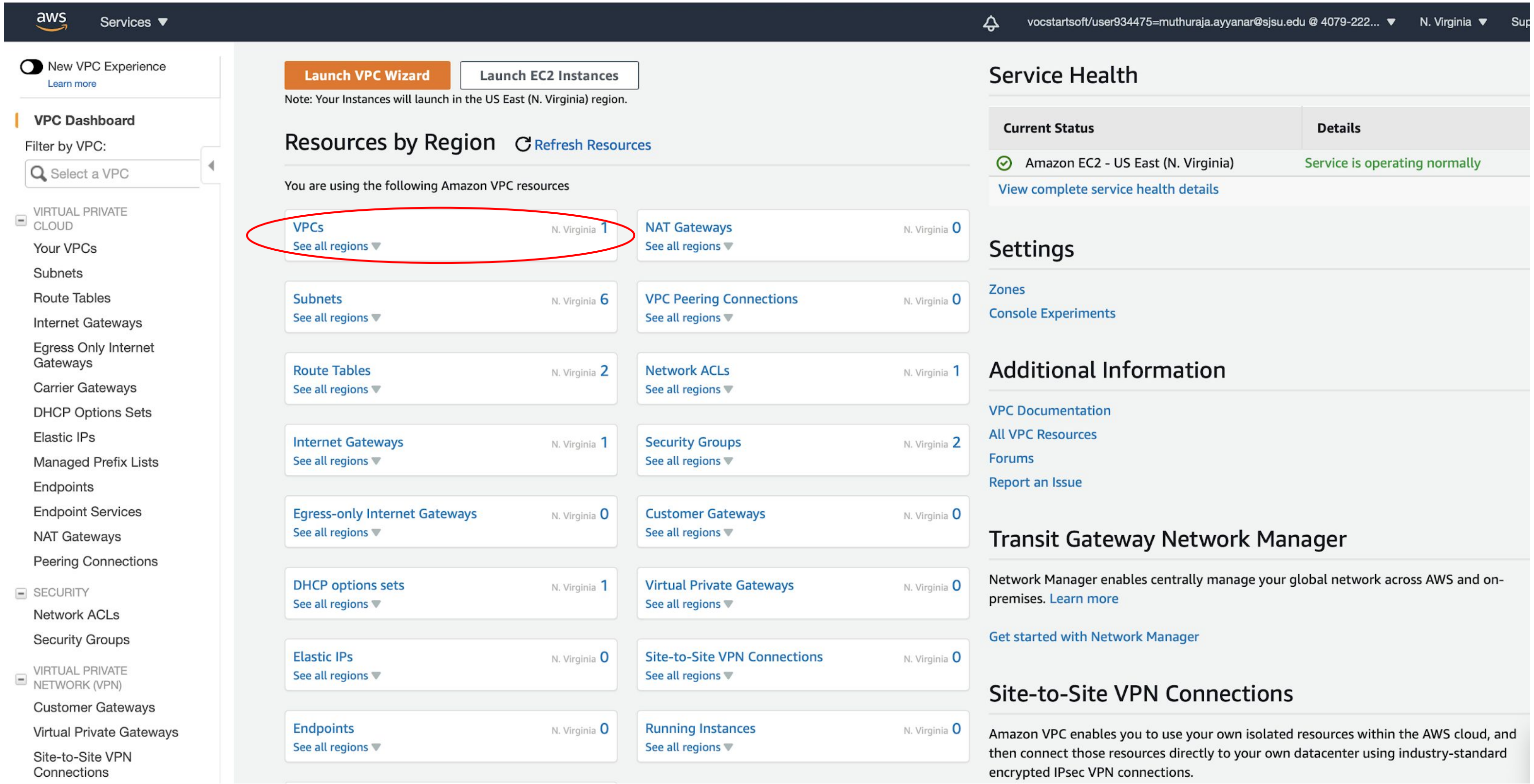
Resources by Region

You are using the following Amazon VPC resources

VPCs See all regions ▼	N. Virginia	1
NAT Gateways See all regions ▼	N. Virginia	0
Subnets See all regions ▼	N. Virginia	0
VPC Peering Connections See all regions ▼	N. Virginia	0
Route Tables See all regions ▼	N. Virginia	1
Network ACLs See all regions ▼	N. Virginia	1
Internet Gateways See all regions ▼	N. Virginia	0
Security Groups See all regions ▼	N. Virginia	1
Egress-only Internet Gateways See all regions ▼	N. Virginia	0
Customer Gateways See all regions ▼	N. Virginia	0
DHCP options sets See all regions ▼	N. Virginia	1
Virtual Private Gateways See all regions ▼	N. Virginia	0
Elastic IPs See all regions ▼	N. Virginia	0
Site-to-Site VPN Connections See all regions ▼	N. Virginia	0
Endpoints See all regions ▼	N. Virginia	0
Running Instances See all regions ▼	N. Virginia	0
Endpoint Services	N. Virginia	0

VPC Hands-on

Some Network infrastructure will be created by default ..such as a default VPC, subnets , RT etc . Either use the default VPC or delete VPC, RT, Subnets to start from scratch. Below example shows state of a non-default VPC (Where some resources were added on top of default VPC)



Note: Your Instances will launch in the US East (N. Virginia) region.

Resources by Region

You are using the following Amazon VPC resources

Resource	Region	Count	Resource	Region	Count
VPCs	N. Virginia	1	NAT Gateways	N. Virginia	0
Subnets	N. Virginia	6	VPC Peering Connections	N. Virginia	0
Route Tables	N. Virginia	2	Network ACLs	N. Virginia	1
Internet Gateways	N. Virginia	1	Security Groups	N. Virginia	2
Egress-only Internet Gateways	N. Virginia	0	Customer Gateways	N. Virginia	0
DHCP options sets	N. Virginia	1	Virtual Private Gateways	N. Virginia	0
Elastic IPs	N. Virginia	0	Site-to-Site VPN Connections	N. Virginia	0
Endpoints	N. Virginia	0	Running Instances	N. Virginia	0

Service Health

Current Status	Details
Amazon EC2 - US East (N. Virginia)	Service is operating normally

View complete service health details

Settings

Zones

Console Experiments

Additional Information

VPC Documentation

All VPC Resources

Forums

Report an Issue

Transit Gateway Network Manager

Network Manager enables centrally manage your global network across AWS and on-premises. Learn more

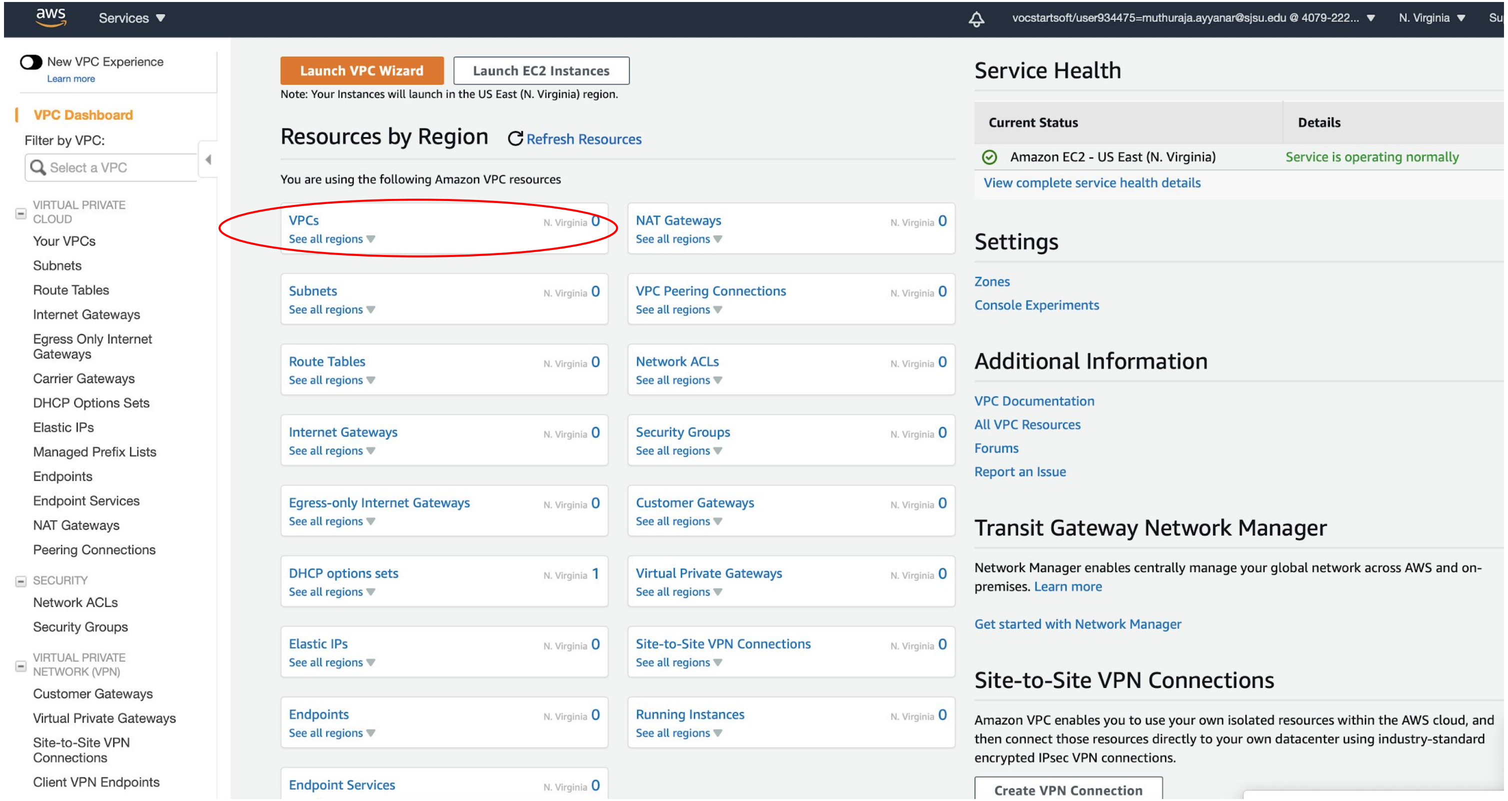
Get started with Network Manager

Site-to-Site VPN Connections

Amazon VPC enables you to use your own isolated resources within the AWS cloud, and then connect those resources directly to your own datacenter using industry-standard encrypted IPsec VPN connections.

VPC Hands-on

After deleting default VPC, there are no default VPC/networks resources



aws
Services ▼
vocstartsoft/user934475=muthuraja.ayyanar@sjsu.edu @ 4079-222... ▼
N. Virginia ▼
Su

New VPC Experience
Learn more

VPC Dashboard

Filter by VPC:

Select a VPC

VIRTUAL PRIVATE CLOUD
- Your VPCs
- Subnets
- Route Tables
- Internet Gateways
- Egress Only Internet Gateways
- Carrier Gateways
- DHCP Options Sets
- Elastic IPs
- Managed Prefix Lists
- Endpoints
- Endpoint Services
- NAT Gateways
- Peering Connections

SECURITY
- Network ACLs
- Security Groups

VIRTUAL PRIVATE NETWORK (VPN)
- Customer Gateways
- Virtual Private Gateways
- Site-to-Site VPN Connections
- Client VPN Endpoints

Launch VPC Wizard | Launch EC2 Instances

Note: Your Instances will launch in the US East (N. Virginia) region.

Resources by Region

Refresh Resources

You are using the following Amazon VPC resources

VPCs See all regions ▼	N. Virginia	0	NAT Gateways See all regions ▼	N. Virginia	0
Subnets See all regions ▼	N. Virginia	0	VPC Peering Connections See all regions ▼	N. Virginia	0
Route Tables See all regions ▼	N. Virginia	0	Network ACLs See all regions ▼	N. Virginia	0
Internet Gateways See all regions ▼	N. Virginia	0	Security Groups See all regions ▼	N. Virginia	0
Egress-only Internet Gateways See all regions ▼	N. Virginia	0	Customer Gateways See all regions ▼	N. Virginia	0
DHCP options sets See all regions ▼	N. Virginia	1	Virtual Private Gateways See all regions ▼	N. Virginia	0
Elastic IPs See all regions ▼	N. Virginia	0	Site-to-Site VPN Connections See all regions ▼	N. Virginia	0
Endpoints See all regions ▼	N. Virginia	0	Running Instances See all regions ▼	N. Virginia	0
Endpoint Services	N. Virginia	0			

Service Health

Current Status	Details
✓ Amazon EC2 - US East (N. Virginia)	Service is operating normally

View complete service health details

Settings

Zones

Console Experiments

Additional Information

VPC Documentation

All VPC Resources

Forums

Report an Issue

Transit Gateway Network Manager

Network Manager enables centrally manage your global network across AWS and on-premises. Learn more

Get started with Network Manager

Site-to-Site VPN Connections

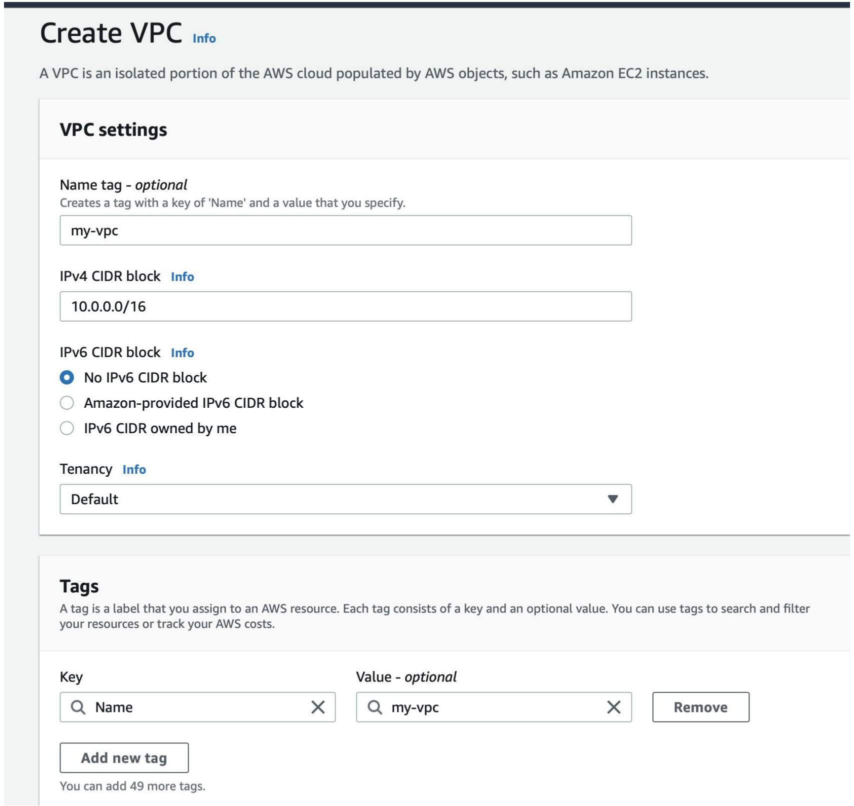
Amazon VPC enables you to use your own isolated resources within the AWS cloud, and then connect those resources directly to your own datacenter using industry-standard encrypted IPsec VPN connections.

Create VPN Connection

VPC Creation/configuration : Step by step process

- Select the “Launch VPC Wizard” from AWS VPC Dashboard or “Create VPC” button from AWS VPC Console (Under your VPCs). You will see your default VPC also.
- Now we add a name for VPC, add a CIDR block range, and click “Create.” (I choose for my CIDR block range 10.10.0.0/16 which will give you 2^16 addresses in the slides. /28 gives you the smallest range of IP addresses. You can choose whatever fits your needs best. You can also select if you want shared tenancy or dedicated. Dedicated will cost you extra.
- Create an Internet Gateway and attach it to the newly created VPC. Click on Internet Gateway located along the left side of your console.
- On this screen you will see one Internet Gateway that is already created when your default VPC was created. We are going to click “Create Internet Gateway” to create a new Internet Gateway. Then we will have to attach the newly created IGW to the newly created VPC. You can only have one IGW attached to a VPC at a time.
- Now we select our newly created VPC, click Actions, and then select Attach To VPC. You will see currently the default IGW is attached to the default VPC. Use the drop down menu to select the correct VPC and then click “Attach.” Now your IGW is attached to your VPC.
- Create your subnets. Click on Subnet on the left hand side of your console.
- Click “create subnet” to create a new subnet for our VPC, assign a name , add detail to the name so it is more easily identifiable. Use the drop down menu to pick the correct VPC, use the drop down menu to pick an availability zone, and then assign the CIDR block range. choose a network/ip range for this subnet. you must create this CIDR range to be a subset of your VPC CIDR range. You cannot have overlapping CIDR ranges. Then click “Create.” You can continue to create as many subnets as needed. We created a public subnet, but you can also create a private subnet.
- Create Route Table. Click on Route Table on the left hand side of your console.
- Select the RT and VPC you need to edit, and the click on the Routes tab below. Click “Edit” and “Add route”. I used 0.0.0.0/0 so it is open to the internet and then used the drop down menu to select my IGW.
- Associate subnets to the Route Table
- NACL - For subnets
- Security Groups - Associated with Instance ENI

Create a VPC



Create VPC Info

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.
my-vpc

IPv4 CIDR block Info
10.0.0.0/16

IPv6 CIDR block Info
● No IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block
○ IPv6 CIDR owned by me

Tenancy Info
Default ▼

Tags

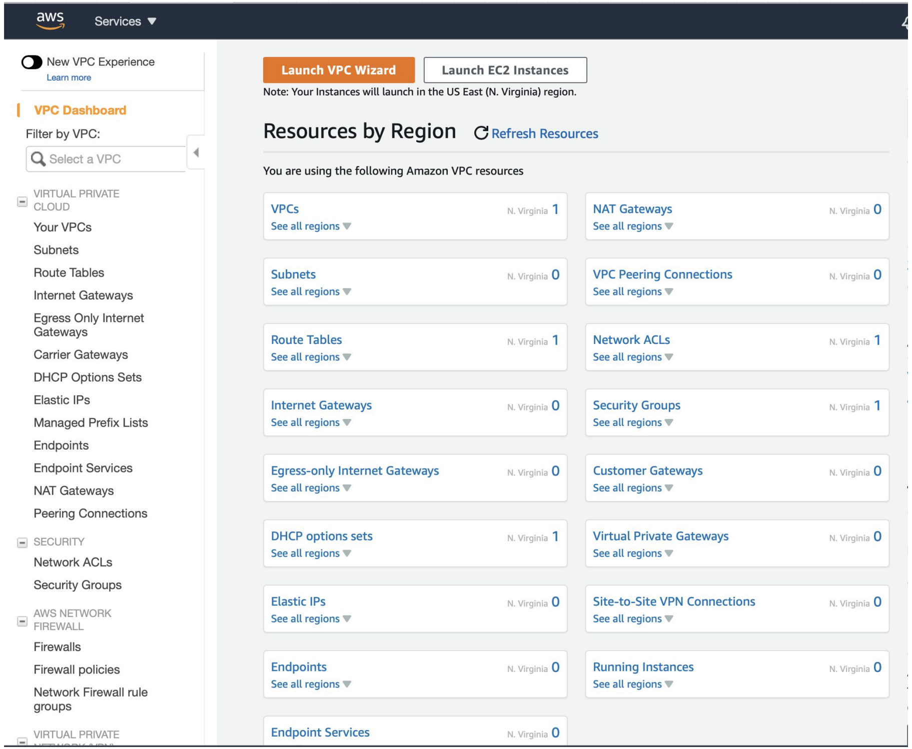
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*	
Name	my-vpc	Remove

Add new tag

You can add 49 more tags.

Default Resources



Note: Your Instances will launch in the US East (N. Virginia) region.

Resources by Region

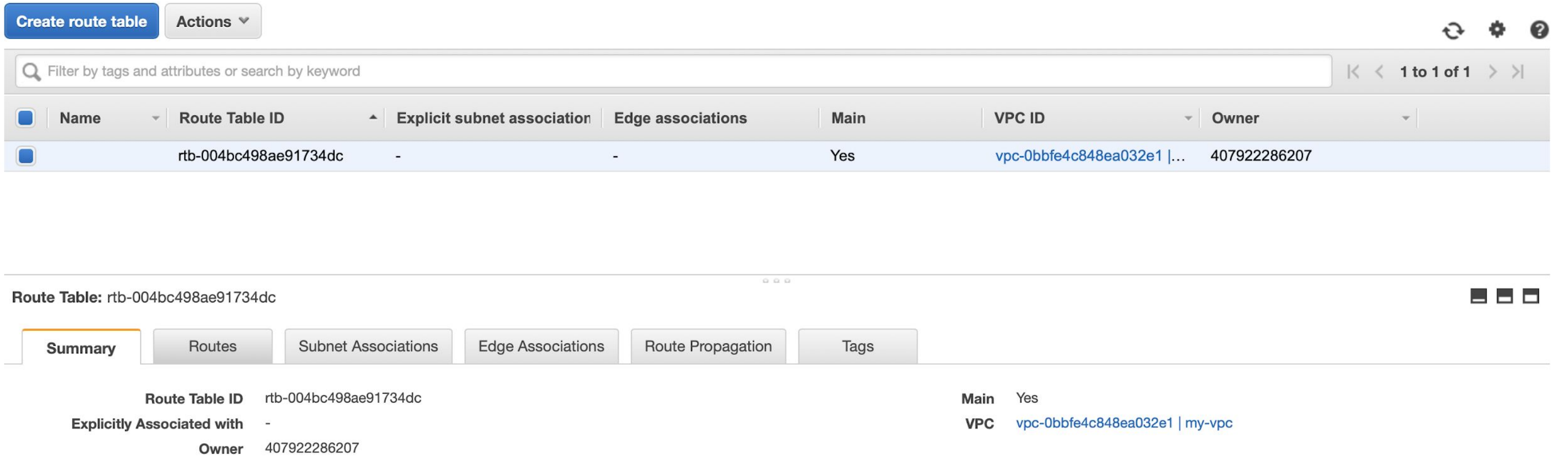
Refresh Resources

You are using the following Amazon VPC resources

Resource	Region	Count
VPCs	N. Virginia	1
NAT Gateways	N. Virginia	0
Subnets	N. Virginia	0
VPC Peering Connections	N. Virginia	0
Route Tables	N. Virginia	1
Network ACLs	N. Virginia	1
Internet Gateways	N. Virginia	0
Security Groups	N. Virginia	1
Egress-only Internet Gateways	N. Virginia	0
Customer Gateways	N. Virginia	0
DHCP options sets	N. Virginia	1
Virtual Private Gateways	N. Virginia	0
Elastic IPs	N. Virginia	0
Site-to-Site VPN Connections	N. Virginia	0
Endpoints	N. Virginia	0
Running Instances	N. Virginia	0
Endpoint Services	N. Virginia	0

See all regions ▼

Default RT



Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
	rtb-004bc498ae91734dc	-	-	Yes	vpc-0bbfe4c848ea032e1 |...	407922286207

Route Table: rtb-004bc498ae91734dc

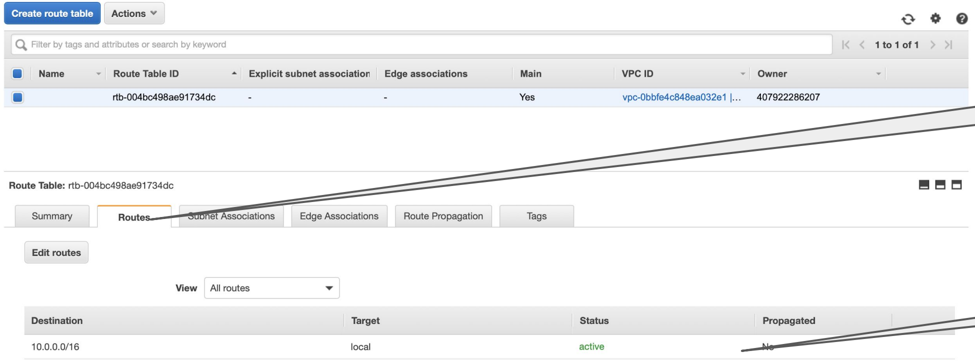
Route Table ID rtb-004bc498ae91734dc

Explicitly Associated with -

Owner 407922286207

Main Yes

VPC vpc-0bbfe4c848ea032e1 | my-vpc



Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
	rtb-004bc498ae91734dc	-	-	Yes	vpc-0bbfe4c848ea032e1 |...	407922286207

Route Table: rtb-004bc498ae91734dc

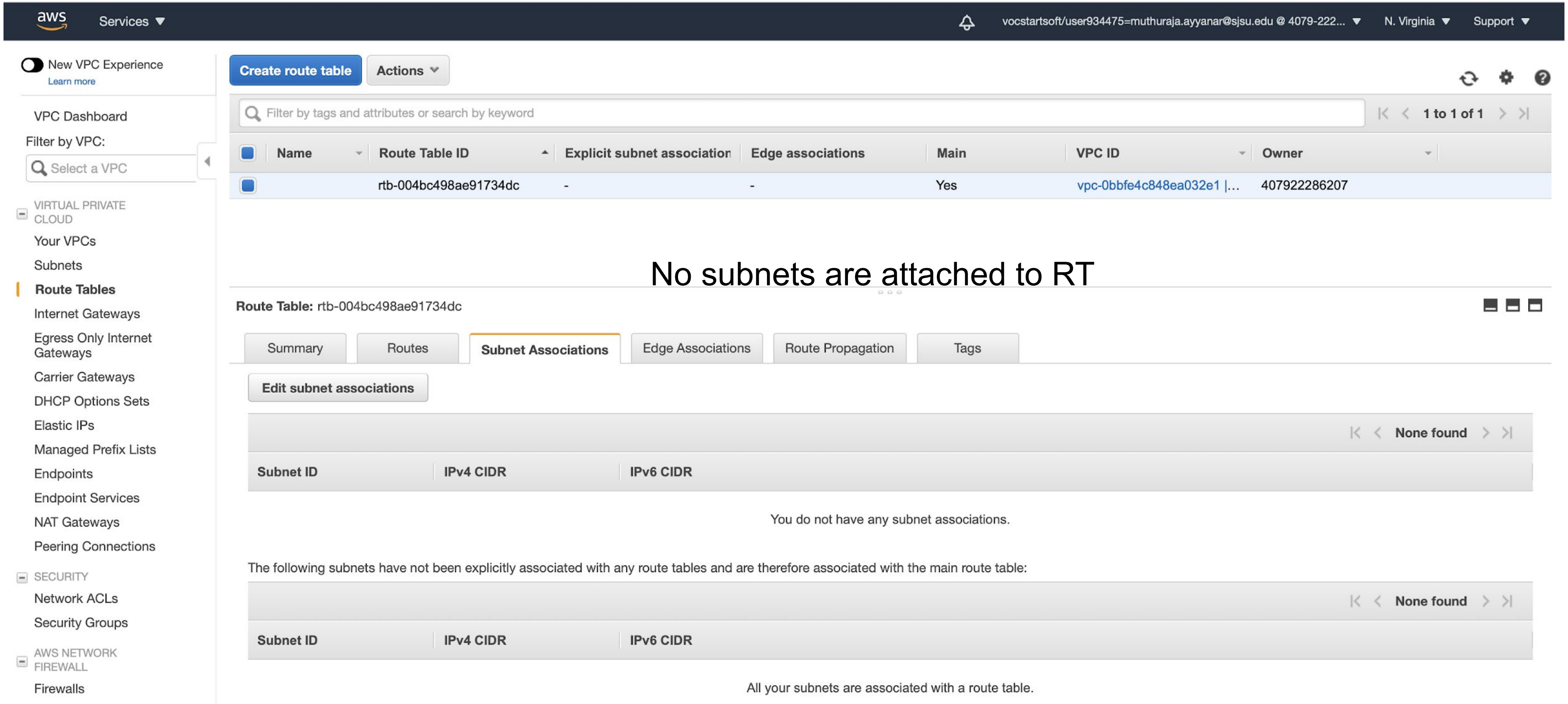
View: All routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No

Go to Routes Tab

By default RT has one “local”route for the VPC Address space

Default RT (Subnet Associations)



Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
	rtb-004bc498ae91734dc	-	-	Yes	vpc-0bbfe4c848ea032e1 |...	407922286207

No subnets are attached to RT

Route Table: rtb-004bc498ae91734dc

None found

Subnet ID	IPv4 CIDR	IPv6 CIDR

You do not have any subnet associations.

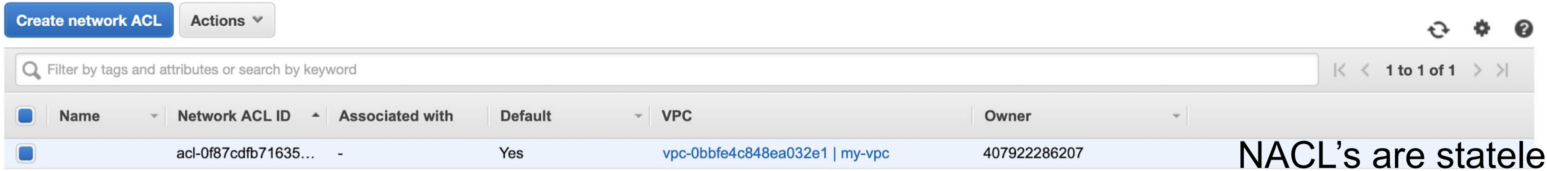
The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

None found

Subnet ID	IPv4 CIDR	IPv6 CIDR

All your subnets are associated with a route table.

Default NACL - Inbound Rules

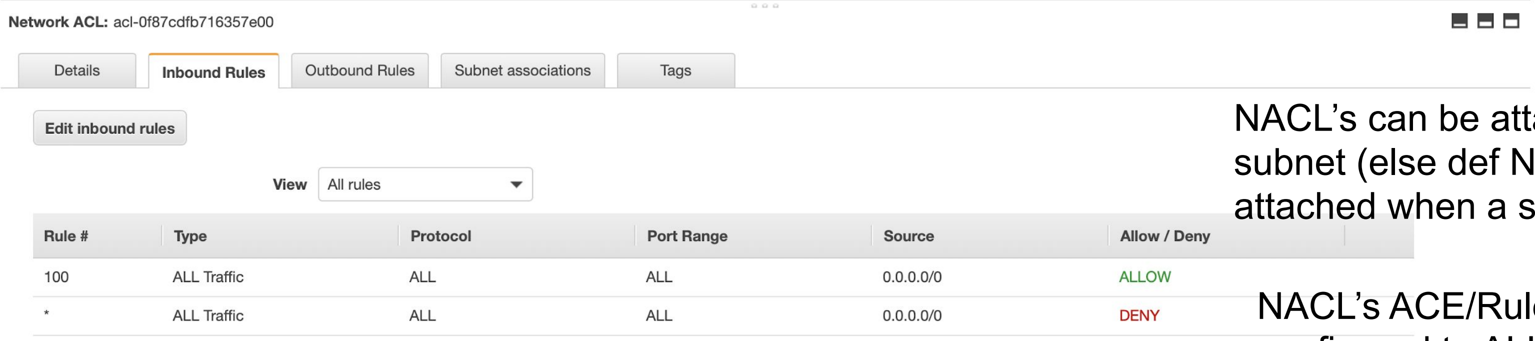


Name	Network ACL ID	Associated with	Default	VPC	Owner
	acl-0f87cdfb71635…	-	Yes	vpc-0bbfe4c848ea032e1 | my-vpc	407922286207

NACL’s are stateless, hence rules are to be defined separately in both inbound and outbound directions

By default NACL allows everything inbound (ACE 100), ACE starts from #1

ACE are processed from smallest to highest



Network ACL: acl-0f87cdfb716357e00

View All rules

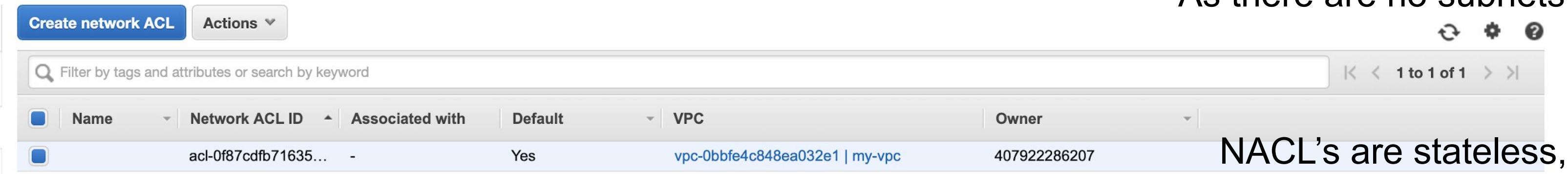
Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

NACL’s can be attached to a subnet (else def NACL will be attached when a subnet is created)

NACL’s ACE/Rules can be configured to ALLOW/DENY a flow

Default NACL - Outbound Rules

No subnets associated with NACL
As there are no subnets created yet

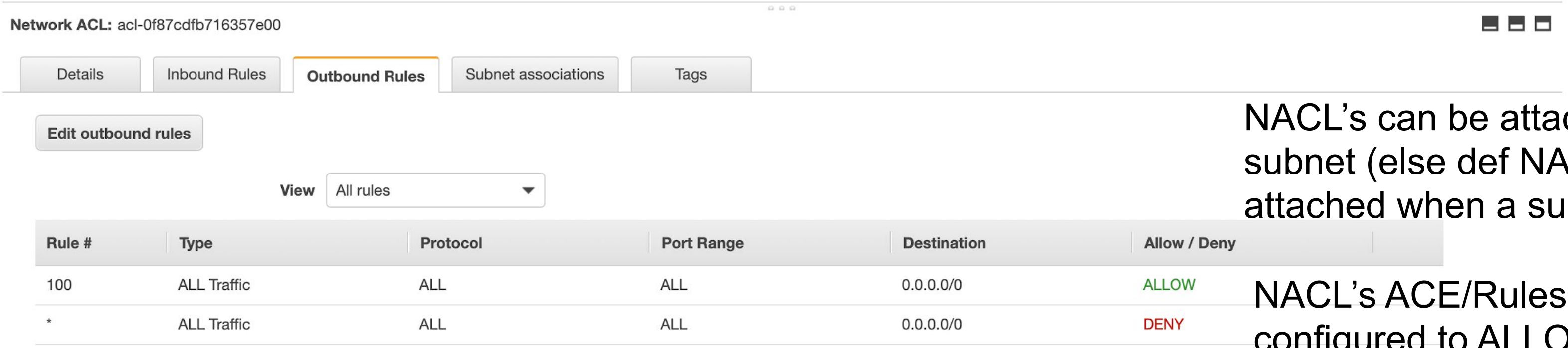


Name	Network ACL ID	Associated with	Default	VPC	Owner
	acl-0f87cdfb71635...	-	Yes	vpc-0bbfe4c848ea032e1 | my-vpc	407922286207

NACL's are stateless, hence rules are to be defined separately in both inbound and outbound directions

ACE are processed from smallest to highest

By default NACL allows everything outbound (ACE 100), ACE starts from #1



Network ACL: acl-0f87cdfb716357e00

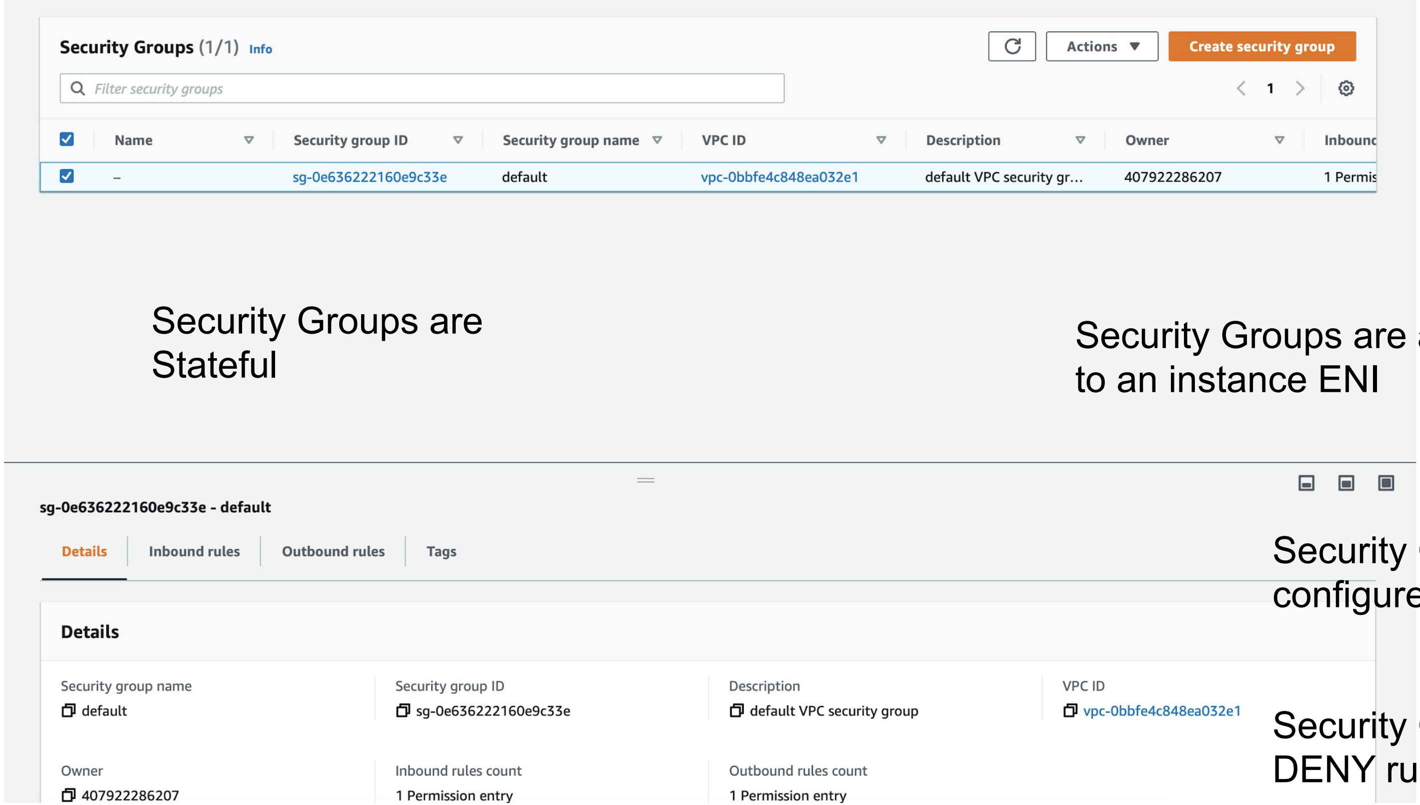
View All rules

Rule #	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

NACL's can be attached to a subnet (else def NACL will be attached when a subnet is created)

NACL's ACE/Rules can be configured to ALLOW/DENY a flow

Default Security Group



Security Groups (1/1) Info

☑	Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbounc
☑	–	sg-0e636222160e9c33e	default	vpc-0bbfe4c848ea032e1	default VPC security gr…	407922286207	1 Permis

sg-0e636222160e9c33e - default

Details

Security group name: default

Security group ID: sg-0e636222160e9c33e

Description: default VPC security group

VPC ID: vpc-0bbfe4c848ea032e1

Owner: 407922286207

Inbound rules count: 1 Permission entry

Outbound rules count: 1 Permission entry

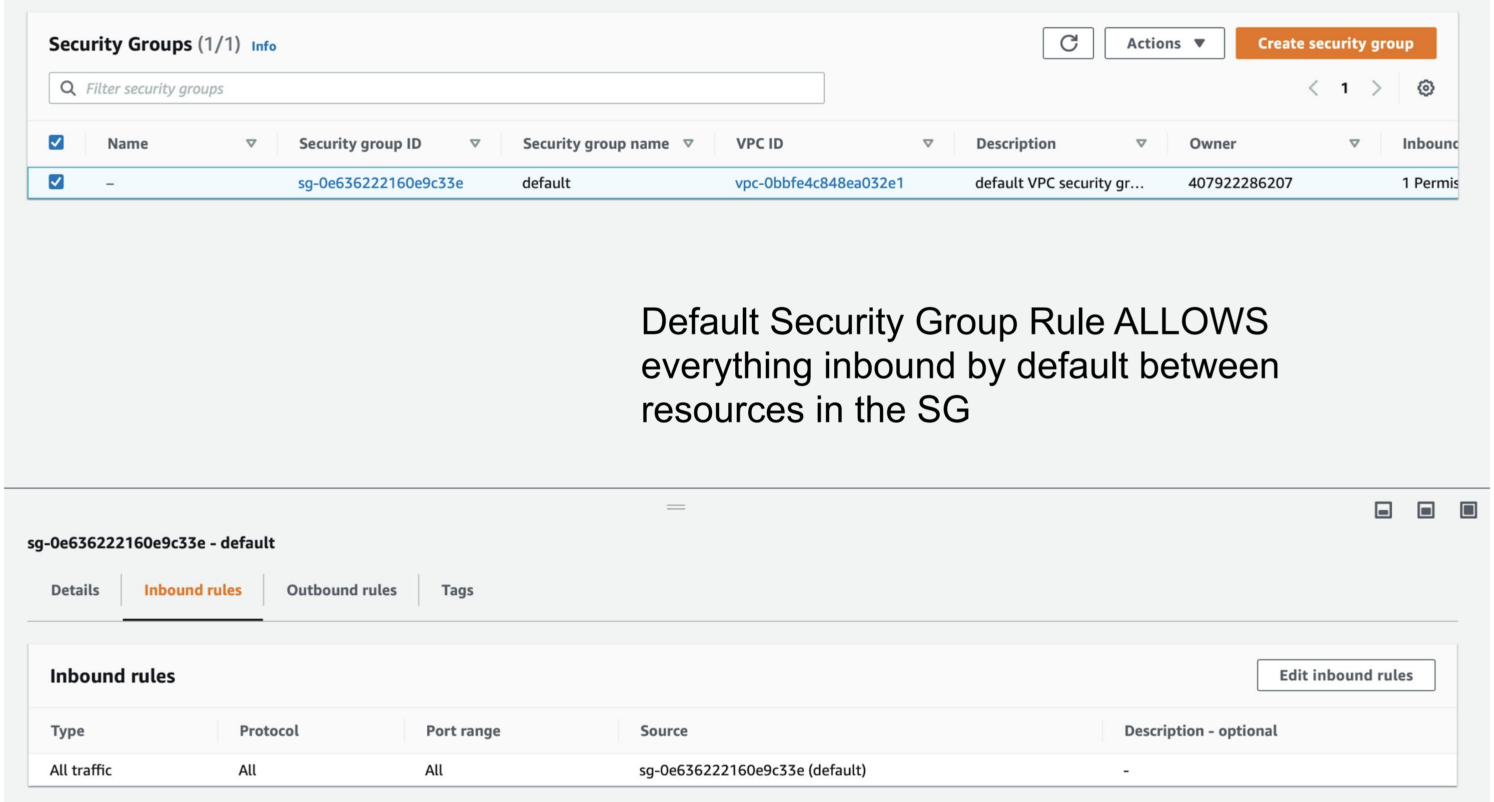
Security Groups are Stateful

Security Groups are attached to an instance ENI

Security Group Rules can be configured to only ALLOW a flow

Security Group Rules has an implicit DENY rule

Default Security Group - Inbound Rules



Security Groups (1/1)

☑	Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbounc
☑	–	sg-0e636222160e9c33e	default	vpc-0bbfe4c848ea032e1	default VPC security gr...	407922286207	1 Permis

Default Security Group Rule ALLOWS everything inbound by default between resources in the SG

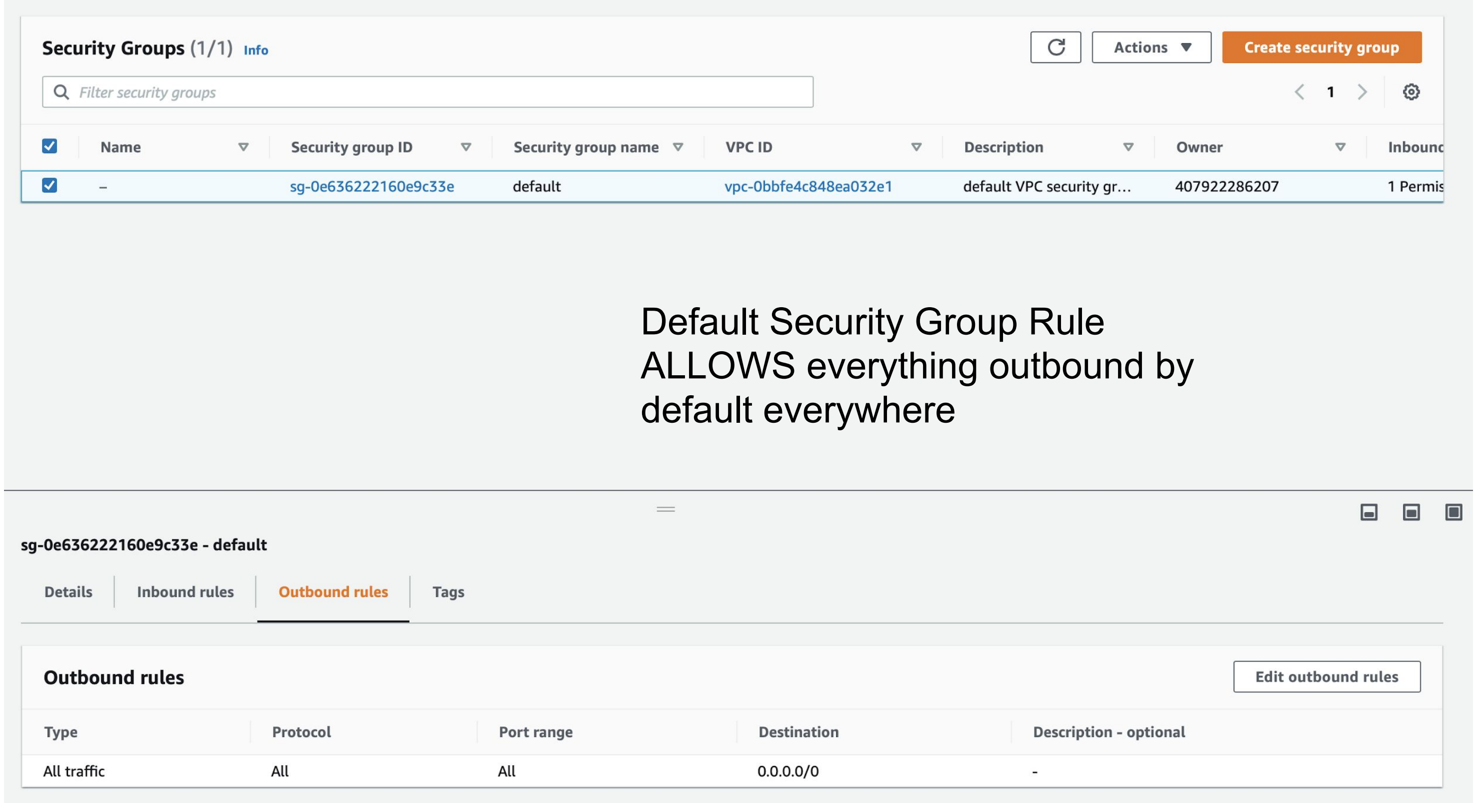
sg-0e636222160e9c33e - default

Details | Inbound rules | Outbound rules | Tags

Inbound rules

Type	Protocol	Port range	Source	Description - optional
All traffic	All	All	sg-0e636222160e9c33e (default)	-

Default Security Group - Outbound Rules



☑	Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbounc
☑	–	sg-0e636222160e9c33e	default	vpc-0bbfe4c848ea032e1	default VPC security gr...	407922286207	1 Permis

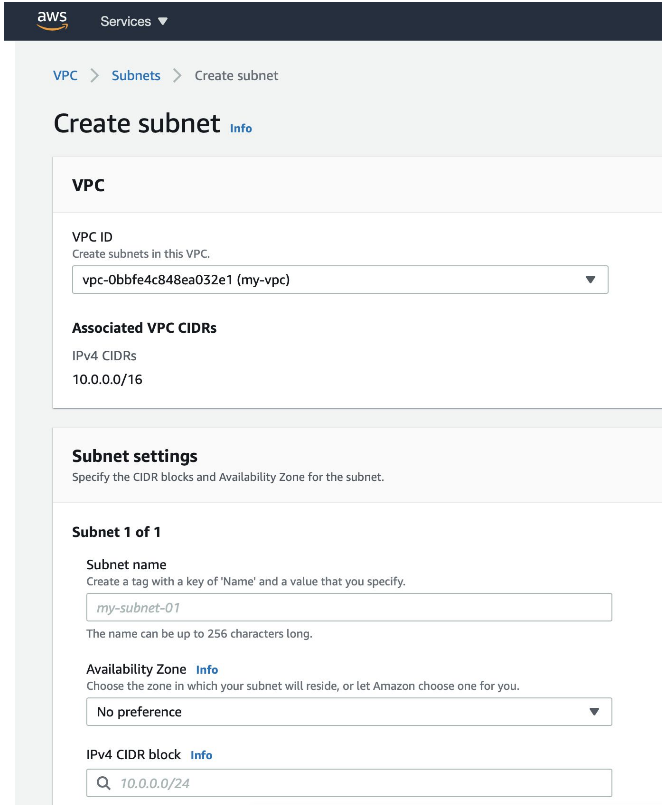
Default Security Group Rule ALLOWS everything outbound by default everywhere

sg-0e636222160e9c33e - default

Outbound rules

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	0.0.0.0/0	-

Create/Add Subnet



Create subnet Info

VPC

VPC ID
Create subnets in this VPC.
vpc-0bbfe4c848ea032e1 (my-vpc)

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

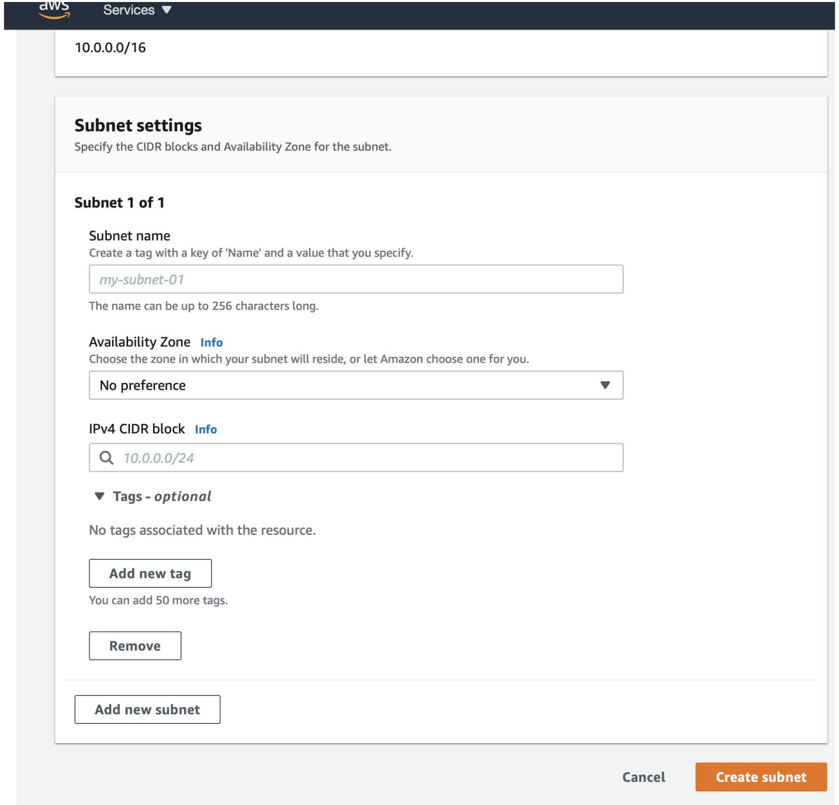
Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
my-subnet-01
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
No preference

IPv4 CIDR block Info
10.0.0.0/24



10.0.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
my-subnet-01
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
No preference

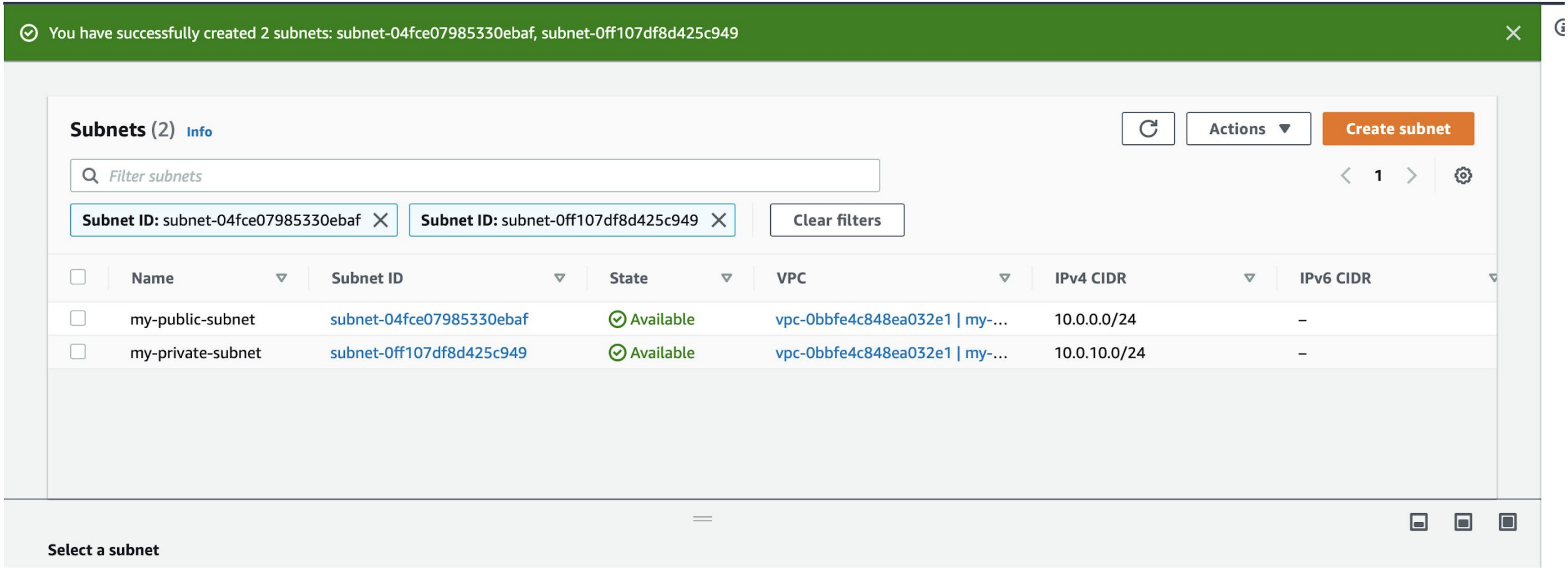
IPv4 CIDR block Info
10.0.0.0/24

▼ Tags - *optional*

No tags associated with the resource.

You can add 50 more tags.

Add Subnets



You have successfully created 2 subnets: subnet-04fce07985330ebaf, subnet-0ff107df8d425c949

Subnets (2) Info

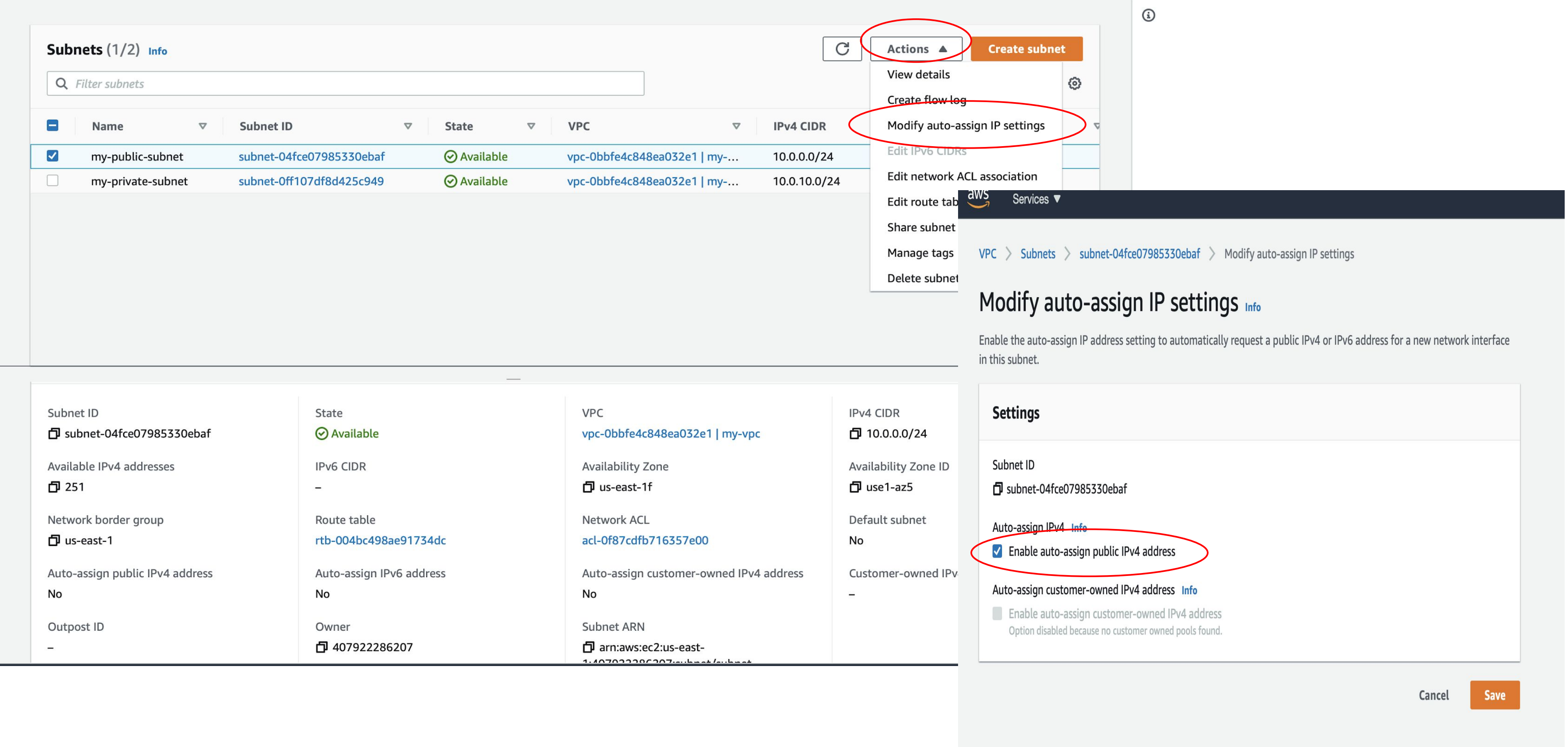
Subnet ID: subnet-04fce07985330ebaf ✕

Subnet ID: subnet-0ff107df8d425c949 ✕

□	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
□	my-public-subnet	subnet-04fce07985330ebaf	✓ Available	vpc-0bbfe4c848ea032e1 | my-…	10.0.0.0/24	–
□	my-private-subnet	subnet-0ff107df8d425c949	✓ Available	vpc-0bbfe4c848ea032e1 | my-…	10.0.10.0/24	–

Select a subnet

Change Subnet setting



Subnets (1/2) Info

Filter subnets

	Name	Subnet ID	State	VPC	IPv4 CIDR
☑	my-public-subnet	subnet-04fce07985330ebaf	✓ Available	vpc-0bbfe4c848ea032e1 | my-...	10.0.0.0/24
□	my-private-subnet	subnet-0ff107df8d425c949	✓ Available	vpc-0bbfe4c848ea032e1 | my-...	10.0.10.0/24

Subnet ID subnet-04fce07985330ebaf	State ✓ Available	VPC vpc-0bbfe4c848ea032e1 | my-vpc	IPv4 CIDR 10.0.0.0/24
Available IPv4 addresses 251	IPv6 CIDR –	Availability Zone us-east-1f	Availability Zone ID use1-az5
Network border group us-east-1	Route table rtb-004bc498ae91734dc	Network ACL acl-0f87cdfb716357e00	Default subnet No
Auto-assign public IPv4 address No	Auto-assign IPv6 address No	Auto-assign customer-owned IPv4 address No	Customer-owned IPv –
Outpost ID –	Owner 407922286207	Subnet ARN arn:aws:ec2:us-east-	

VPC > Subnets > subnet-04fce07985330ebaf > Modify auto-assign IP settings

Modify auto-assign IP settings Info

Enable the auto-assign IP address setting to automatically request a public IPv4 or IPv6 address for a new network interface in this subnet.

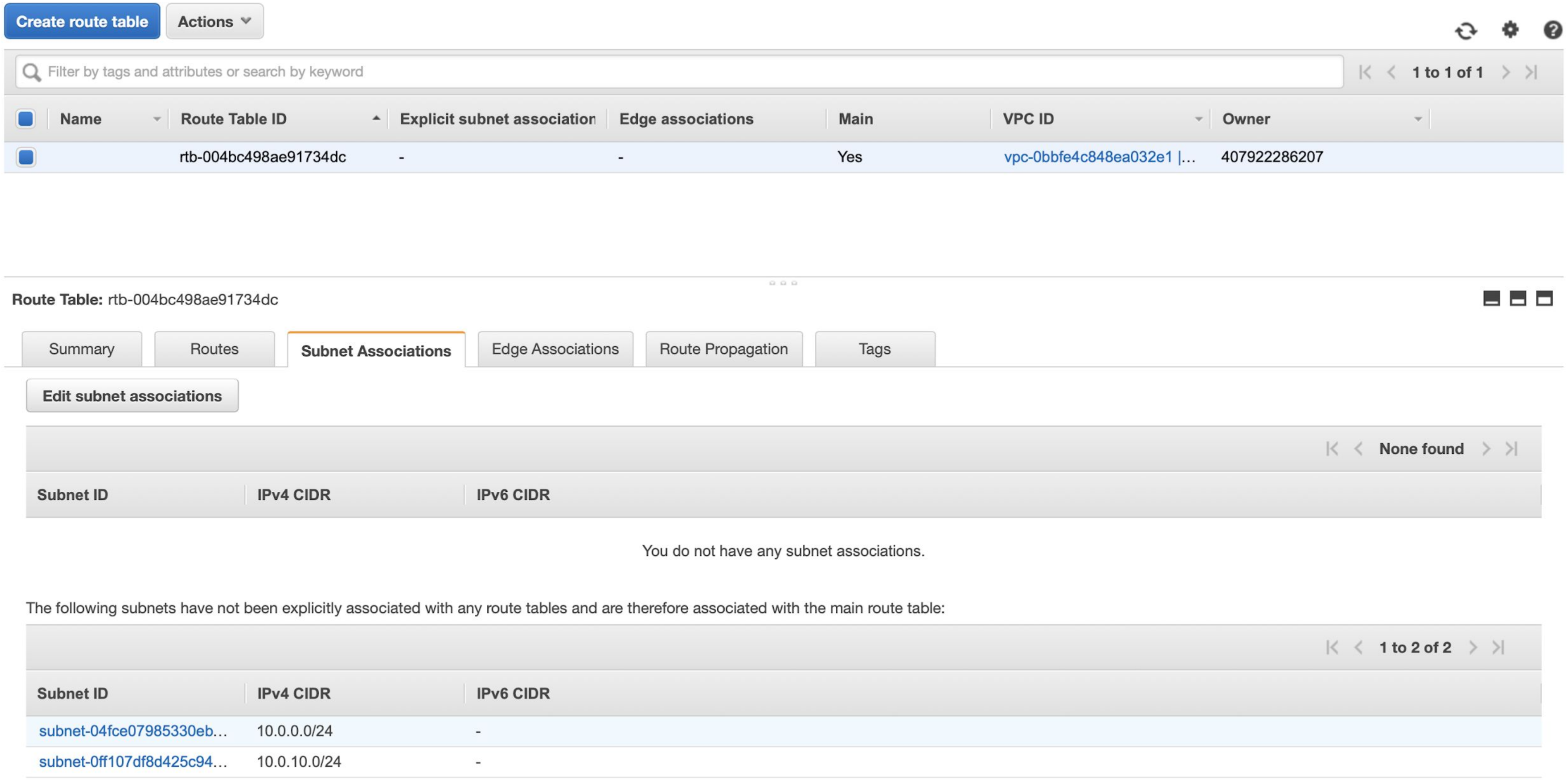
Settings

Subnet ID
subnet-04fce07985330ebaf

Auto-assign IPv4 Info
☑ Enable auto-assign public IPv4 address

Auto-assign customer-owned IPv4 address Info
□ Enable auto-assign customer-owned IPv4 address
Option disabled because no customer owned pools found.

Default RT after adding subnets



☐	Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
☐		rtb-004bc498ae91734dc	-	-	Yes	vpc-0bbfe4c848ea032e1 |...	407922286207

Route Table: rtb-004bc498ae91734dc

None found

Subnet ID	IPv4 CIDR	IPv6 CIDR

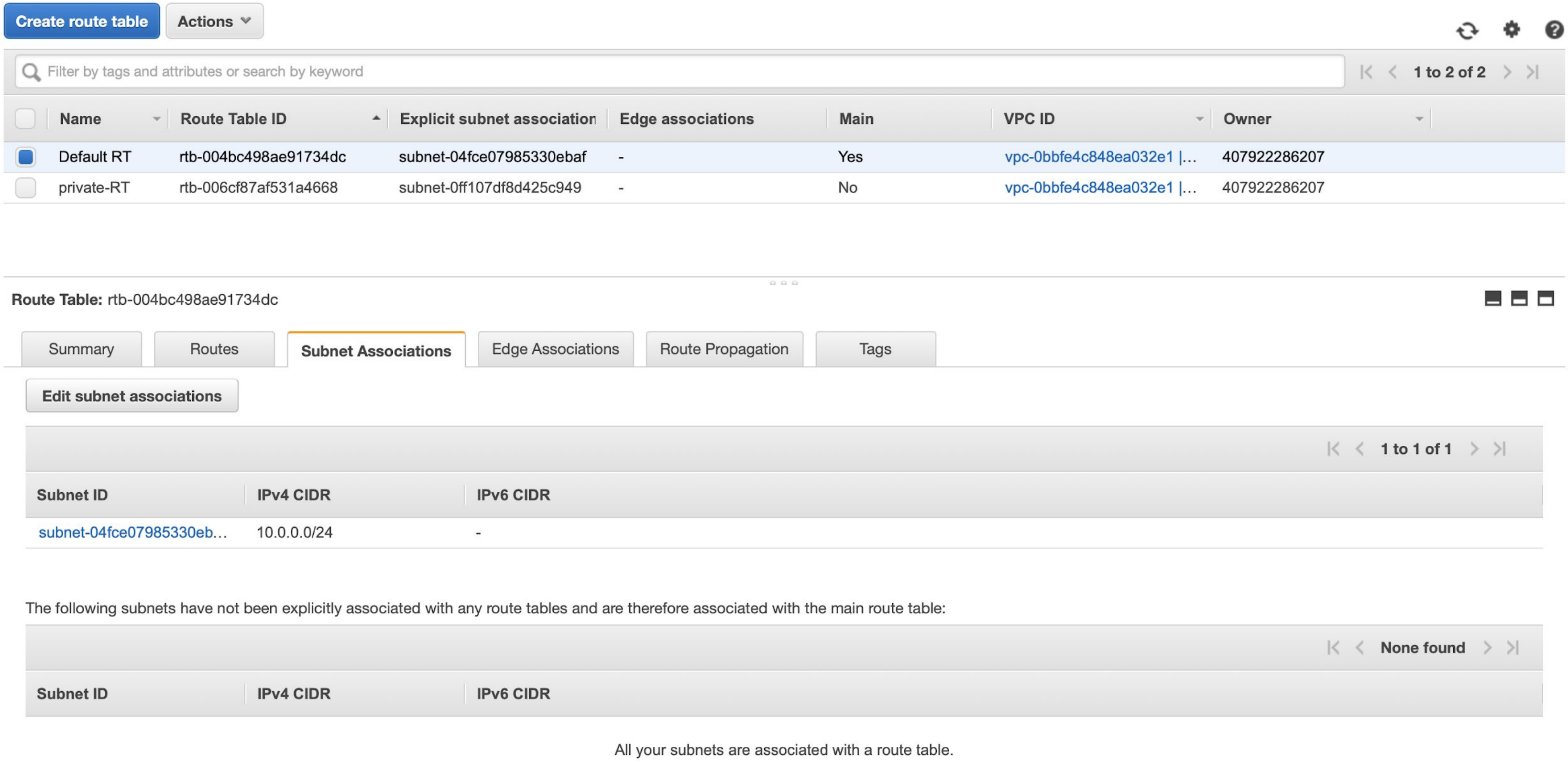
You do not have any subnet associations.

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

1 to 2 of 2

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-04fce07985330eb...	10.0.0.0/24	-
subnet-0ff107df8d425c94...	10.0.10.0/24	-

Default RT after Associating Public subnet



☐	Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
☑	Default RT	rtb-004bc498ae91734dc	subnet-04fce07985330ebaf	-	Yes	vpc-0bbfe4c848ea032e1 |...	407922286207
☐	private-RT	rtb-006cf87af531a4668	subnet-0ff107df8d425c949	-	No	vpc-0bbfe4c848ea032e1 |...	407922286207

Route Table: rtb-004bc498ae91734dc

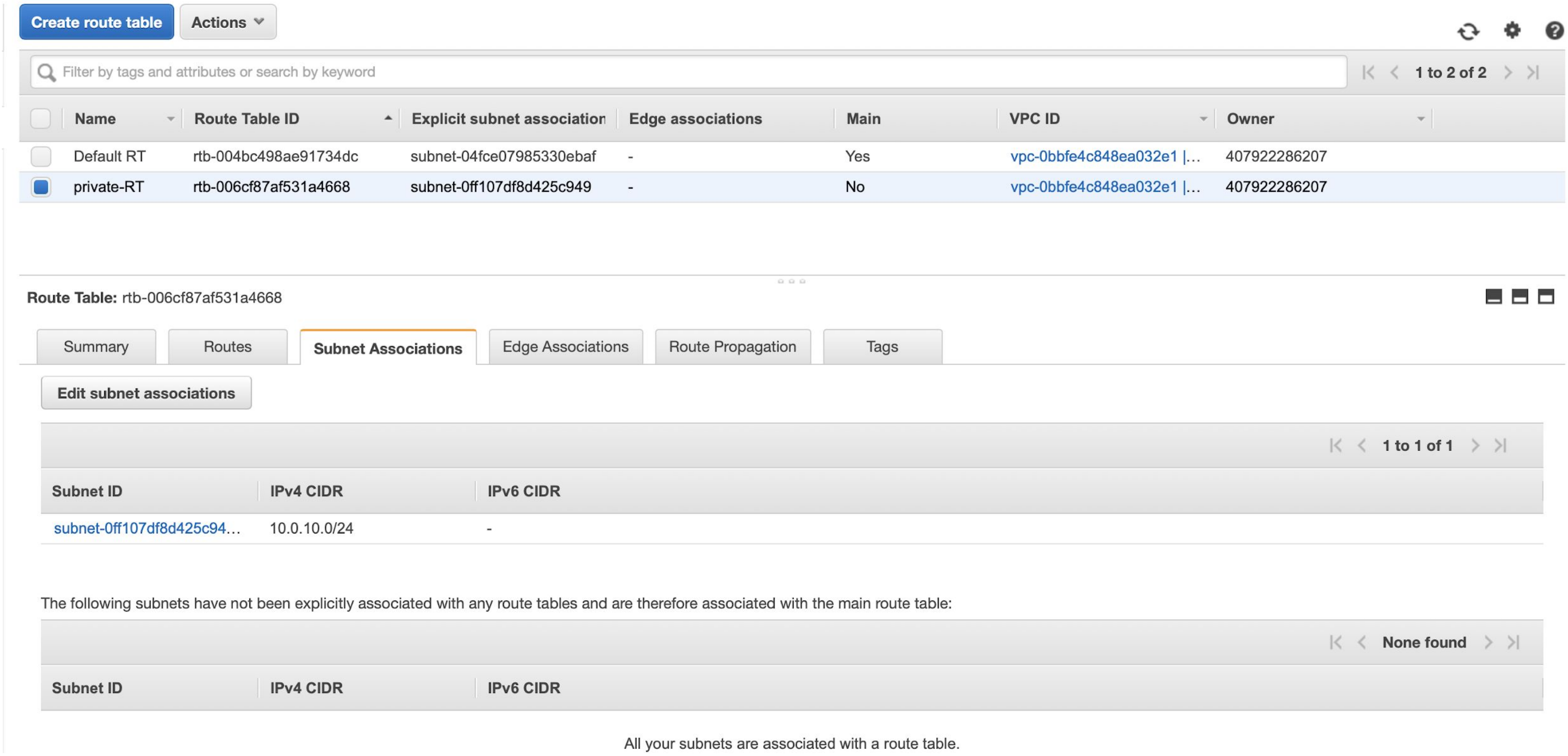
Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-04fce07985330eb...	10.0.0.0/24	-

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

Subnet ID	IPv4 CIDR	IPv6 CIDR

All your subnets are associated with a route table.

Private RT after Associating Private subnet



☐	Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
☐	Default RT	rtb-004bc498ae91734dc	subnet-04fce07985330ebaf	-	Yes	vpc-0bbfe4c848ea032e1 |...	407922286207
☑	private-RT	rtb-006cf87af531a4668	subnet-0ff107df8d425c949	-	No	vpc-0bbfe4c848ea032e1 |...	407922286207

Route Table: rtb-006cf87af531a4668

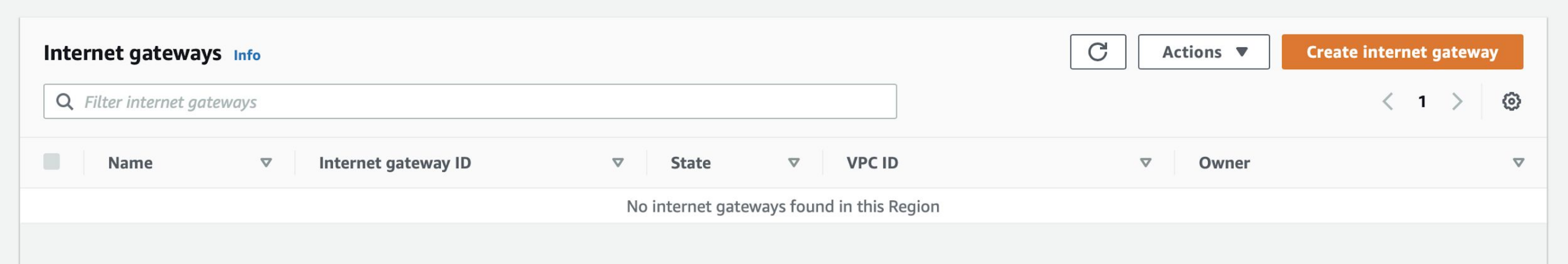
Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-0ff107df8d425c94...	10.0.10.0/24	-

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

Subnet ID	IPv4 CIDR	IPv6 CIDR

All your subnets are associated with a route table.

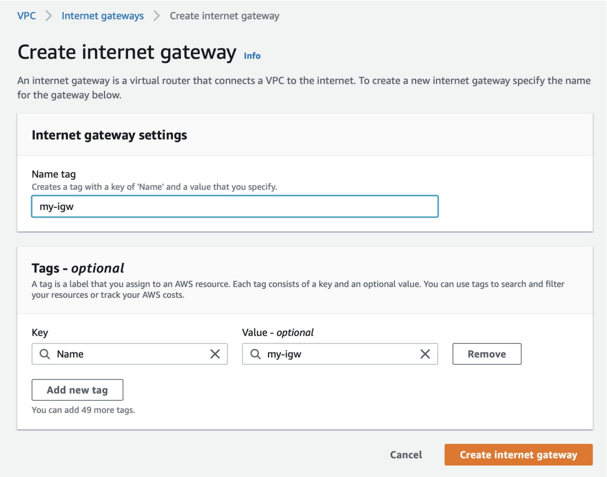
Internet Gateway (By default IGW is not created)



Internet gateways Info

☐	Name	Internet gateway ID	State	VPC ID	Owner

No internet gateways found in this Region



Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

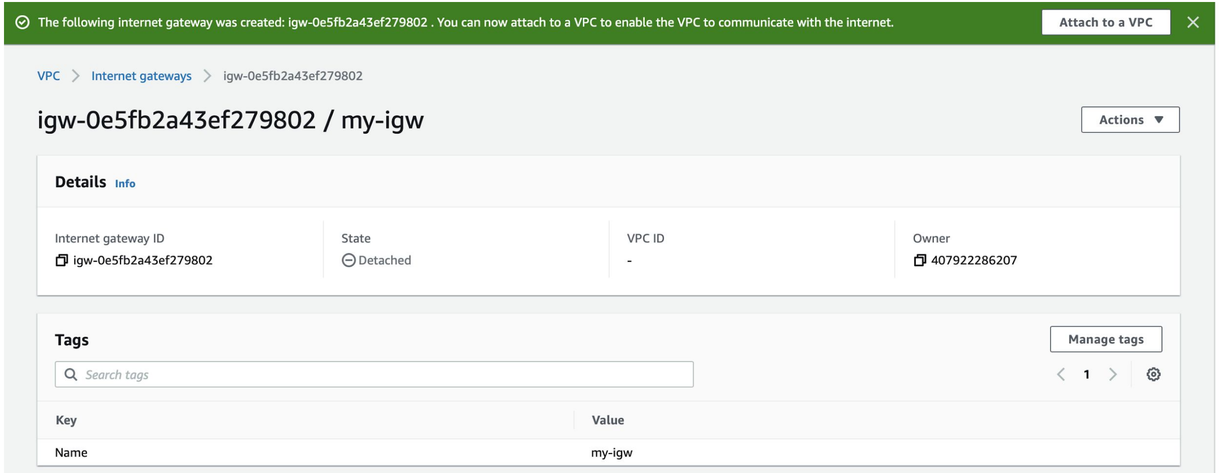
Name tag
Creates a tag with a key of 'Name' and a value that you specify.
my-igw

Tags - *optional*

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*
Name	my-igw

You can add 49 more tags.



The following internet gateway was created: igw-0e5fb2a43ef279802 . You can now attach to a VPC to enable the VPC to communicate with the internet.

igw-0e5fb2a43ef279802 / my-igw

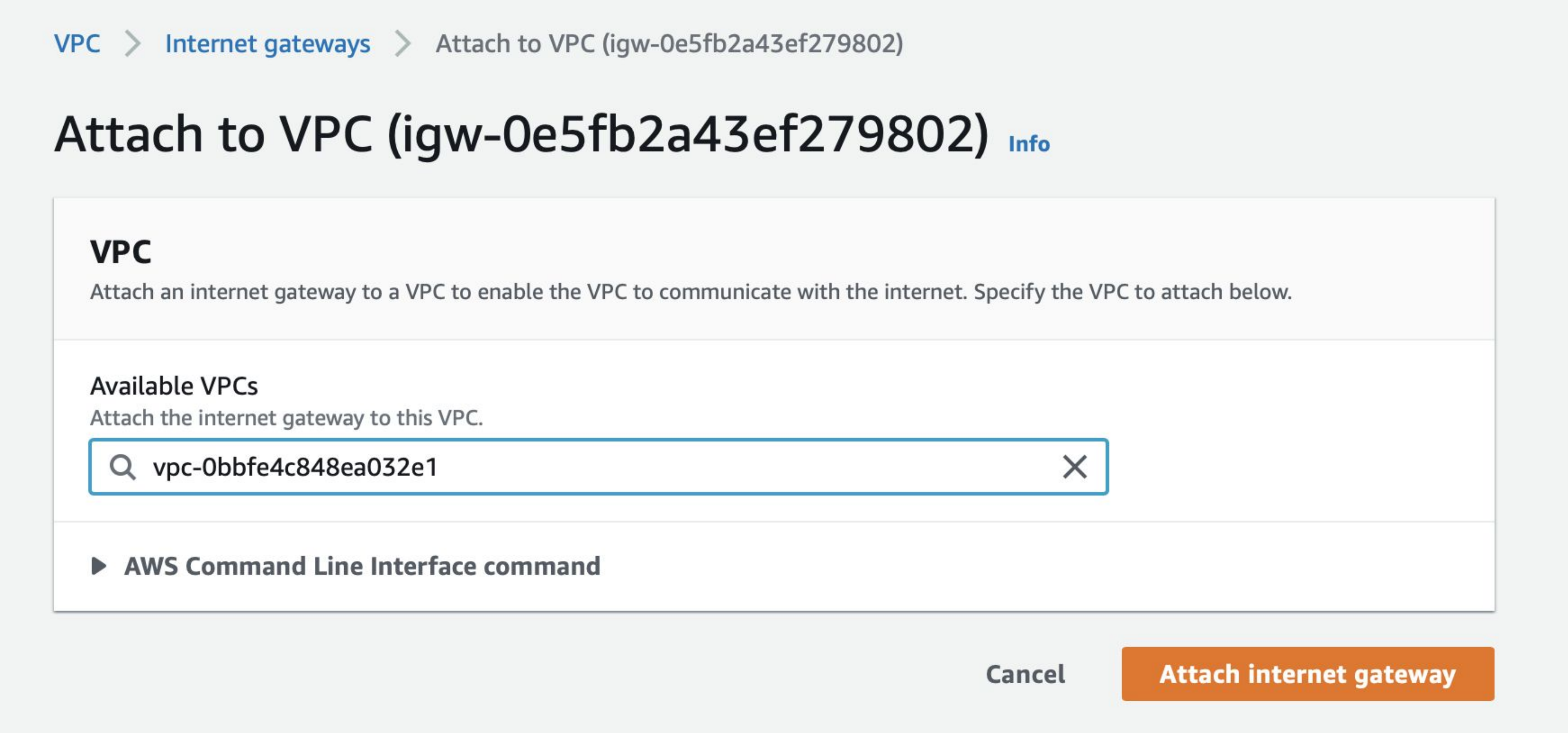
Details Info

Internet gateway ID	State	VPC ID	Owner
igw-0e5fb2a43ef279802	Detached	-	407922286207

Tags

Key	Value
Name	my-igw

Internet Gateway (Attach IGW to a VPC)



VPC > Internet gateways > Attach to VPC (igw-0e5fb2a43ef279802)

Attach to VPC (igw-0e5fb2a43ef279802)

VPC

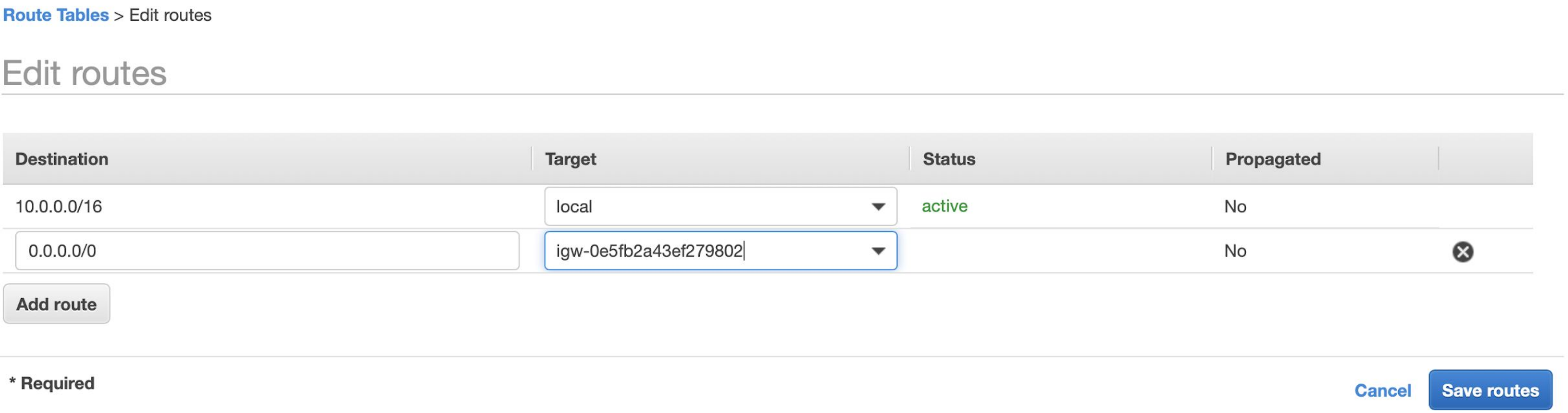
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

vpc-0bbfe4c848ea032e1

Add Def Route with Internet Gateway as NH (Def RT)

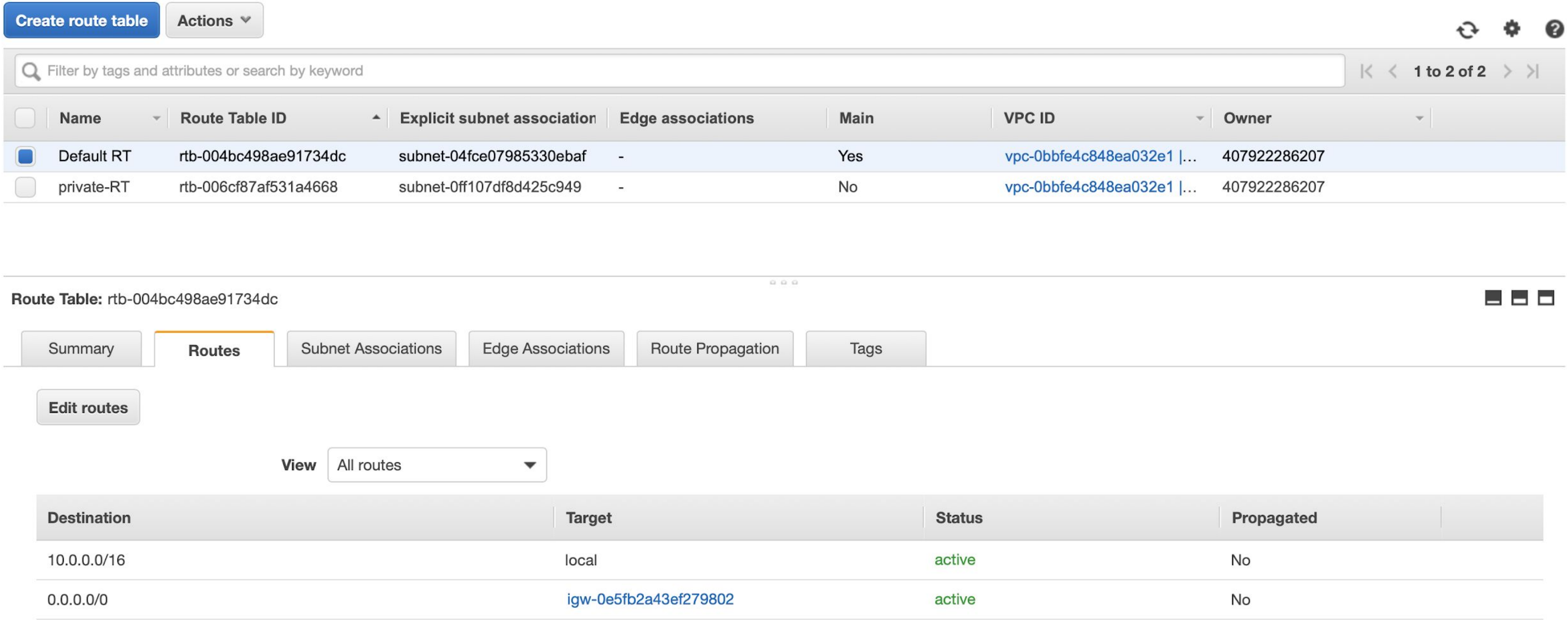


Route Tables > Edit routes

Edit routes

Destination	Target	Status	Propagated	
10.0.0.0/16	local	active	No	
0.0.0.0/0	igw-0e5fb2a43ef279802		No	⊗

Add Def Route with Internet Gateway as NH (Def RT)



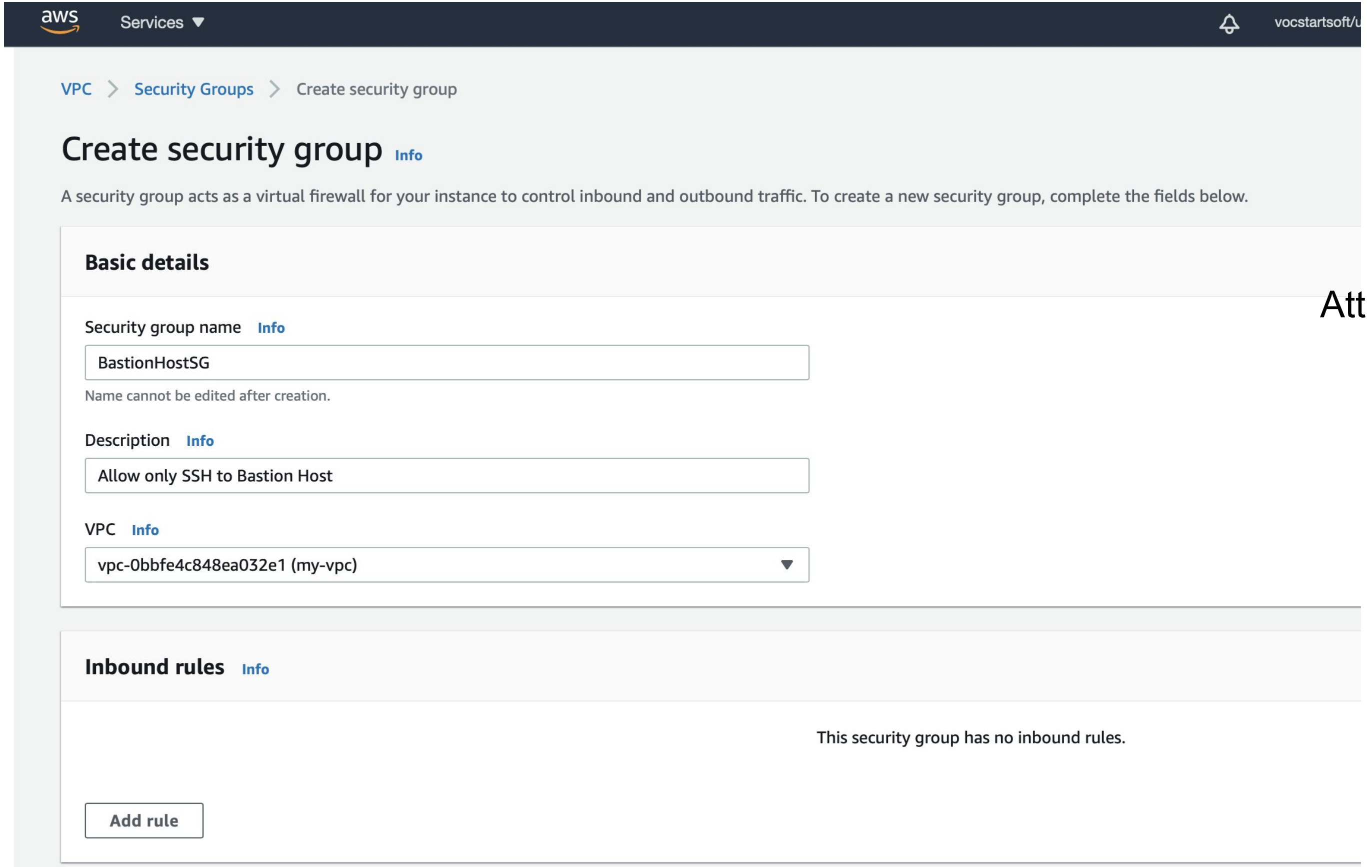
□	Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
☑	Default RT	rtb-004bc498ae91734dc	subnet-04fce07985330ebaf	-	Yes	vpc-0bbfe4c848ea032e1 |...	407922286207
□	private-RT	rtb-006cf87af531a4668	subnet-0ff107df8d425c949	-	No	vpc-0bbfe4c848ea032e1 |...	407922286207

Route Table: rtb-004bc498ae91734dc

View All routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	igw-0e5fb2a43ef279802	active	No

Create a New SG (non-def)



VPC > Security Groups > Create security group

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info

BastionHostSG

Name cannot be edited after creation.

Description Info

Allow only SSH to Bastion Host

VPC Info

vpc-0bbfe4c848ea032e1 (my-vpc) ▼

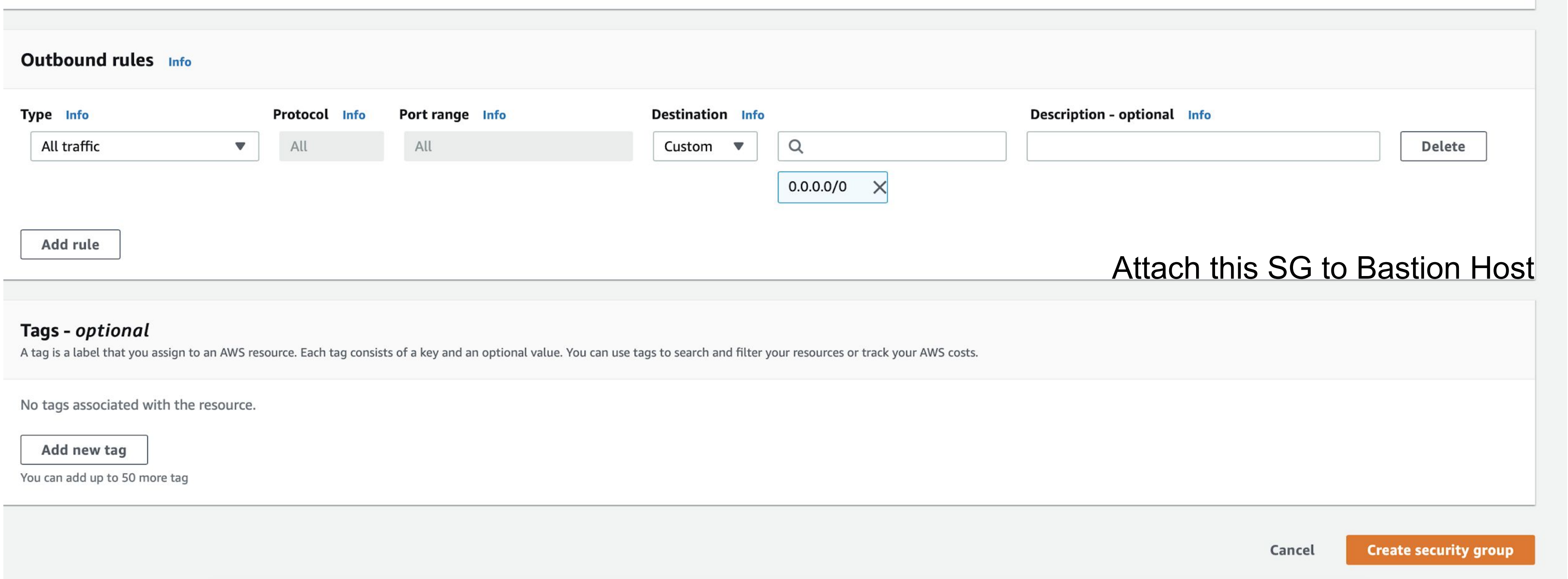
Inbound rules Info

This security group has no inbound rules.

Add rule

Attach this SG to Bastion Host

Create a New SG (non-def)



Outbound rules

Type	Protocol	Port range	Destination		Description - optional
All traffic	All	All	Custom	0.0.0.0/0	

Tags - *optional*

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

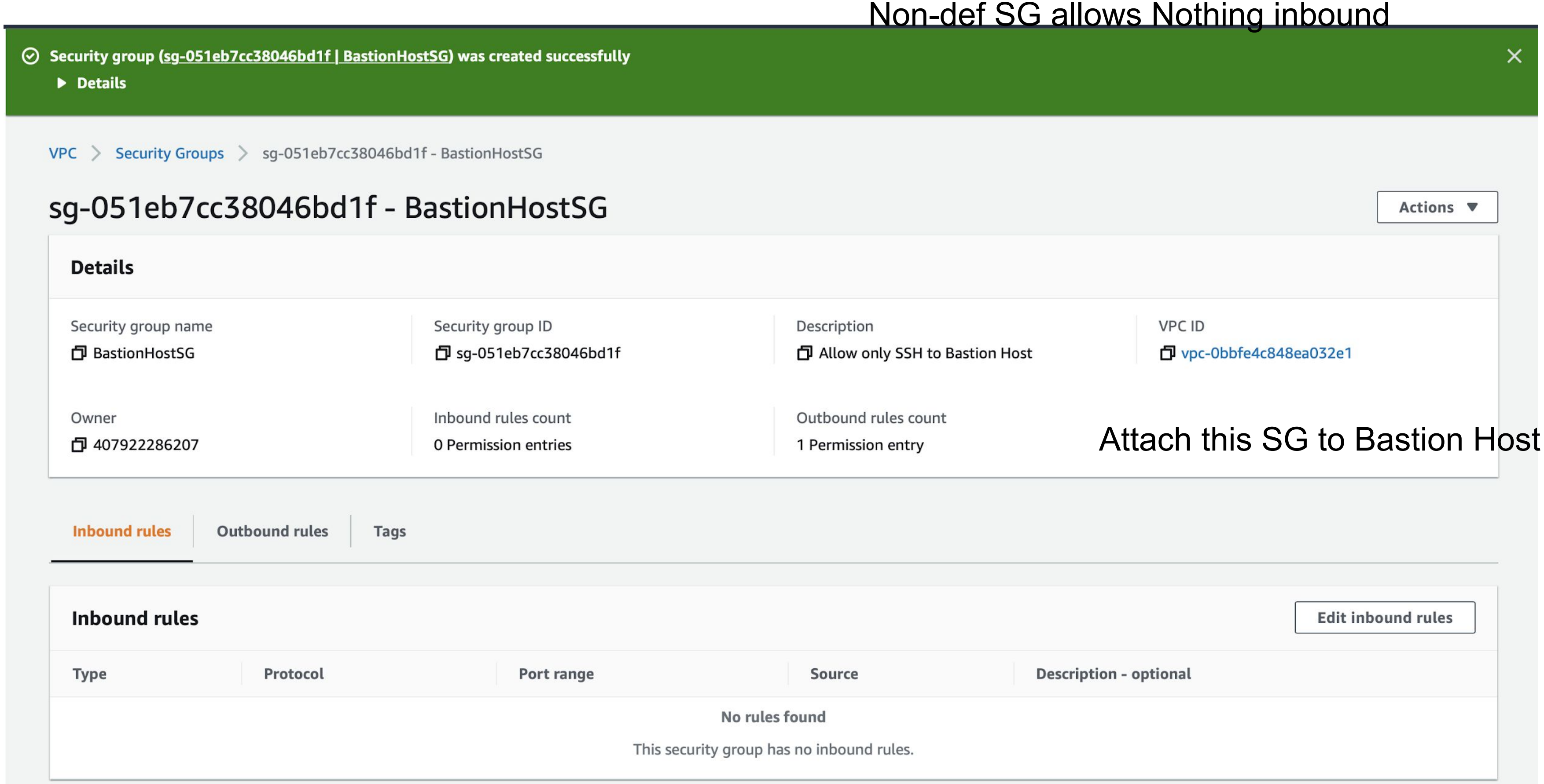
No tags associated with the resource.

You can add up to 50 more tag

Attach this SG to Bastion Host

After Creating a New SG (non-def)

Non-def SG allows Nothing inbound



Security group (sg-051eb7cc38046bd1f | BastionHostSG) was created successfully

▶ Details

VPC > Security Groups > sg-051eb7cc38046bd1f - BastionHostSG

sg-051eb7cc38046bd1f - BastionHostSG

Details

Security group name	Security group ID	Description	VPC ID
BastionHostSG	sg-051eb7cc38046bd1f	Allow only SSH to Bastion Host	vpc-0bbfe4c848ea032e1
Owner	**Inbound rules count**	**Outbound rules count**	
407922286207	0 Permission entries	1 Permission entry	

Attach this SG to Bastion Host

Inbound rules

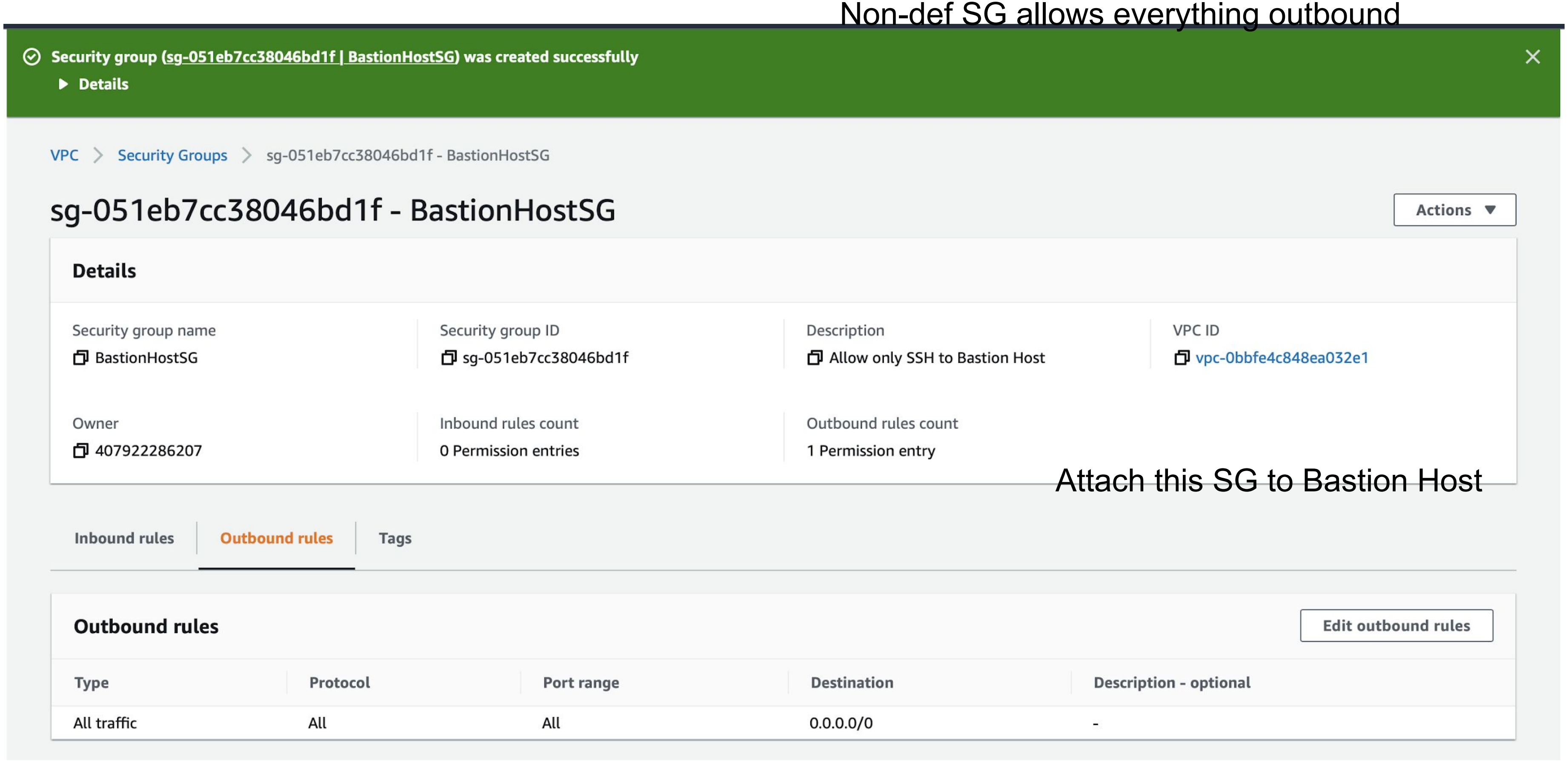
Type	Protocol	Port range	Source	Description - optional

No rules found

This security group has no inbound rules.

After Creating a New SG (non-def)

Non-def SG allows everything outbound



Security group (sg-051eb7cc38046bd1f | BastionHostSG) was created successfully

▶ Details

VPC > Security Groups > sg-051eb7cc38046bd1f - BastionHostSG

sg-051eb7cc38046bd1f - BastionHostSG

Details

Security group name: BastionHostSG

Security group ID: sg-051eb7cc38046bd1f

Description: Allow only SSH to Bastion Host

VPC ID: vpc-0bbfe4c848ea032e1

Owner: 407922286207

Inbound rules count: 0 Permission entries

Outbound rules count: 1 Permission entry

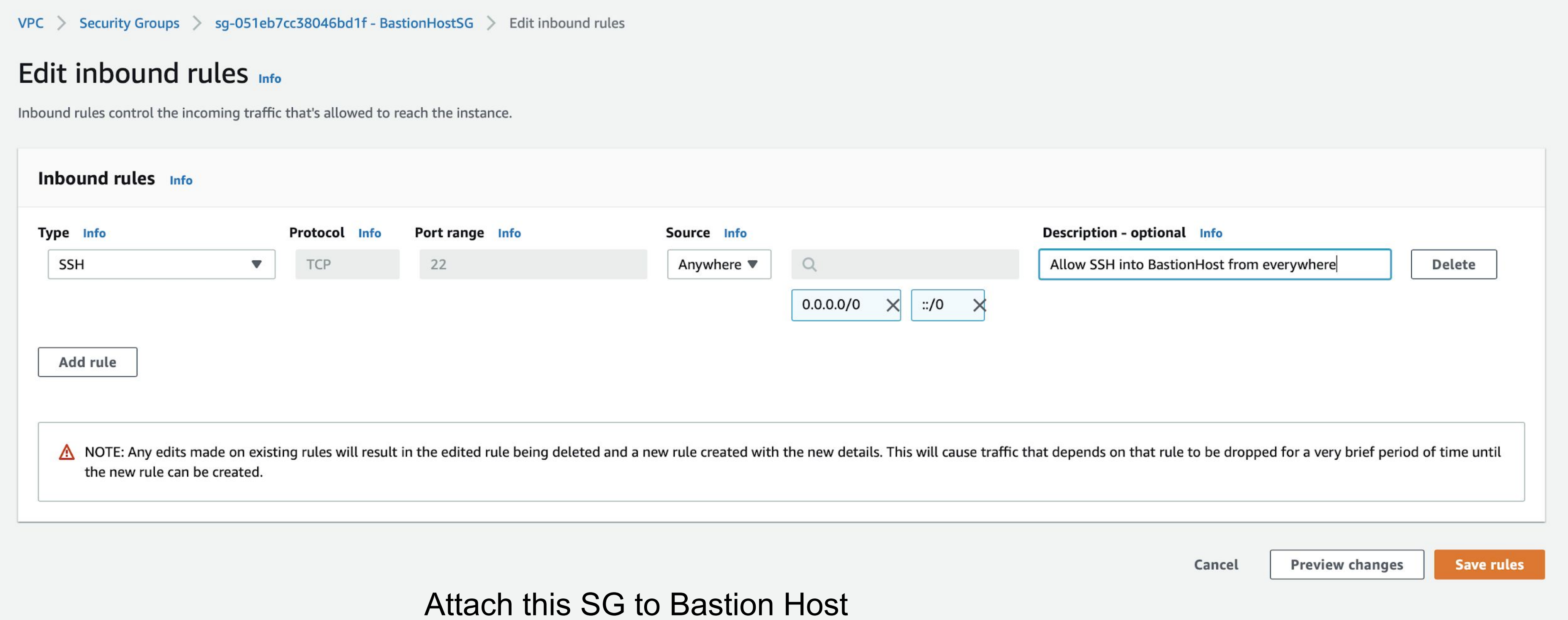
Attach this SG to Bastion Host

Outbound rules

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	0.0.0.0/0	-

After Creating a New SG (non-def)

Non-def SG - Add rule to allow SSH inbound from everywhere



VPC > Security Groups > sg-051eb7cc38046bd1f - BastionHostSG > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
SSH ▼	TCP	22	Anywhere ▼	0.0.0.0/0 ✕ ::/0 ✕	Allow SSH into BastionHost from everywhere	Delete

Add rule

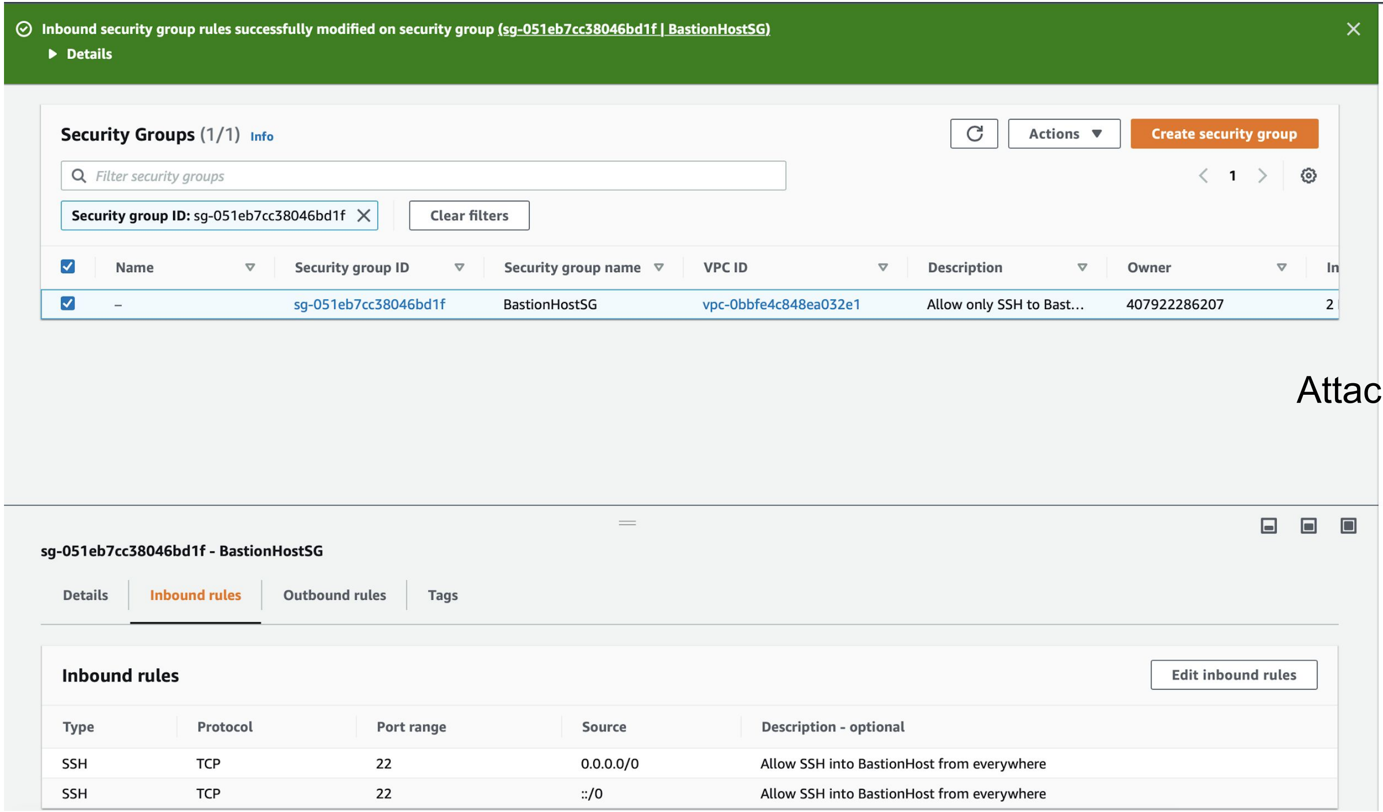
⚠ NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

Cancel | Preview changes | Save rules

Attach this SG to Bastion Host

After Creating a New SG (non-def)

Non-def SG - Add rule to allow SSH inbound from everywhere



Inbound security group rules successfully modified on security group (sg-051eb7cc38046bd1f | BastionHostSG)

▶ Details

Security Groups (1/1) Info

Security group ID: sg-051eb7cc38046bd1f ✕

☑	Name	Security group ID	Security group name	VPC ID	Description	Owner	In
☑	–	sg-051eb7cc38046bd1f	BastionHostSG	vpc-0bbfe4c848ea032e1	Allow only SSH to Bast…	407922286207	2

sg-051eb7cc38046bd1f - BastionHostSG

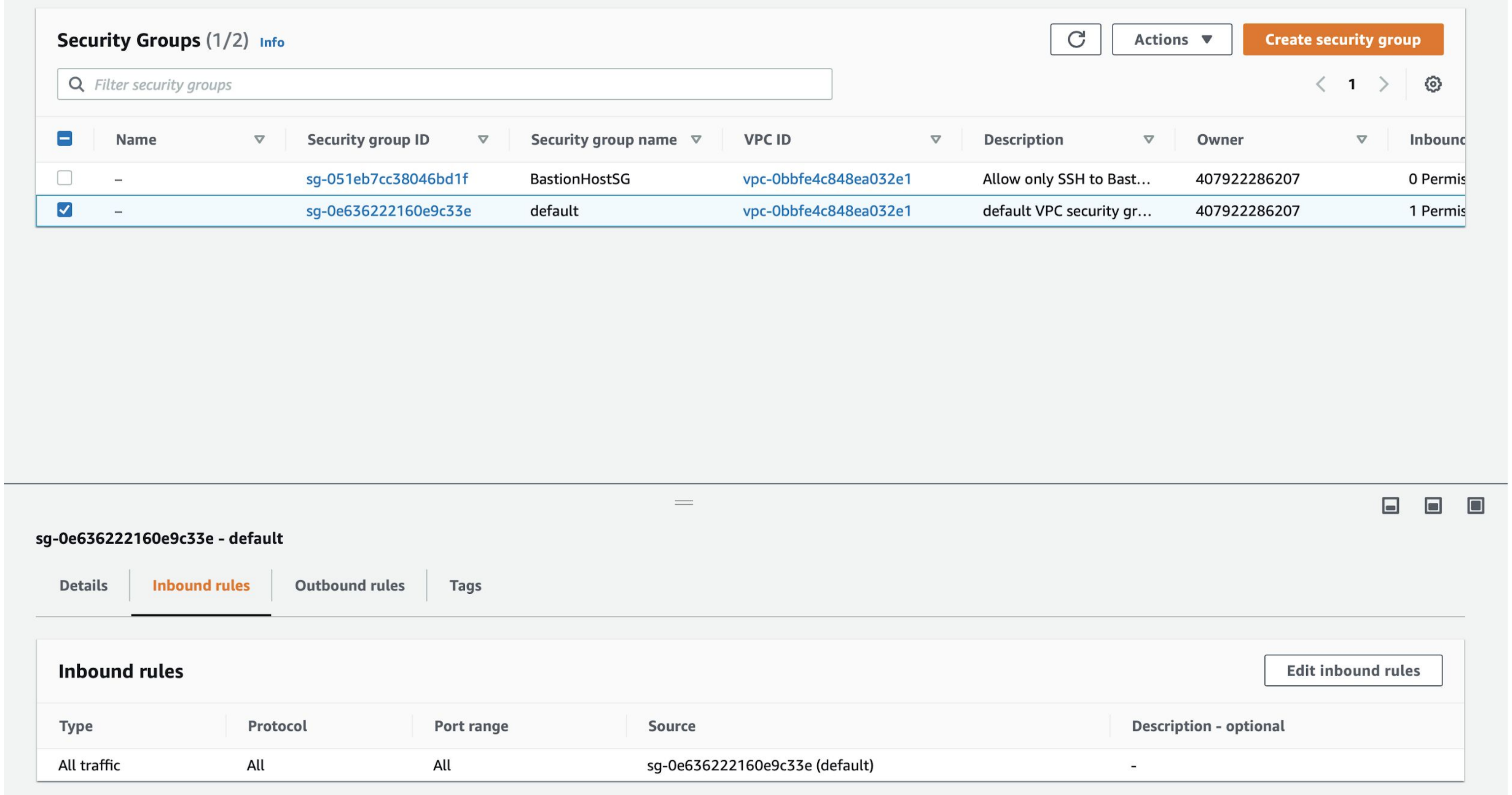
Inbound rules

Type	Protocol	Port range	Source	Description - optional
SSH	TCP	22	0.0.0.0/0	Allow SSH into BastionHost from everywhere
SSH	TCP	22	::/0	Allow SSH into BastionHost from everywhere

Attach this SG to Bastion Host

Default SG

Def SG allows everything inbound & outbound



Security Groups (1/2)

⊟	Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbounc
☐	–	sg-051eb7cc38046bd1f	BastionHostSG	vpc-0bbfe4c848ea032e1	Allow only SSH to Bast…	407922286207	0 Permis
☑	–	sg-0e636222160e9c33e	default	vpc-0bbfe4c848ea032e1	default VPC security gr…	407922286207	1 Permis

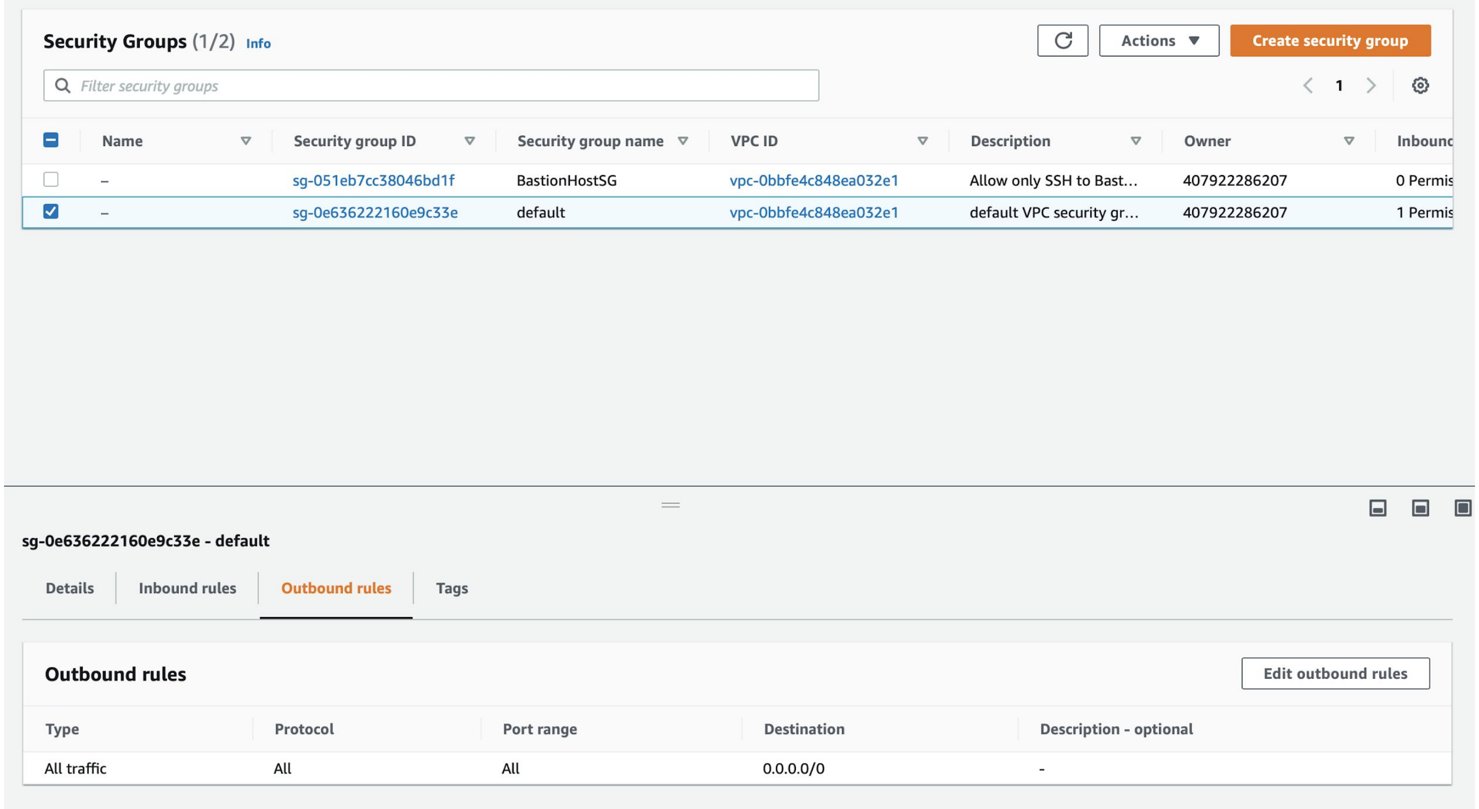
sg-0e636222160e9c33e - default

Inbound rules

Type	Protocol	Port range	Source	Description - optional
All traffic	All	All	sg-0e636222160e9c33e (default)	-

Default SG

Def SG allows everything inbound & outbound



Security Groups (1/2) Info

☑	Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbounc
□	–	sg-051eb7cc38046bd1f	BastionHostSG	vpc-0bbfe4c848ea032e1	Allow only SSH to Bast…	407922286207	0 Permis
☑	–	sg-0e636222160e9c33e	default	vpc-0bbfe4c848ea032e1	default VPC security gr…	407922286207	1 Permis

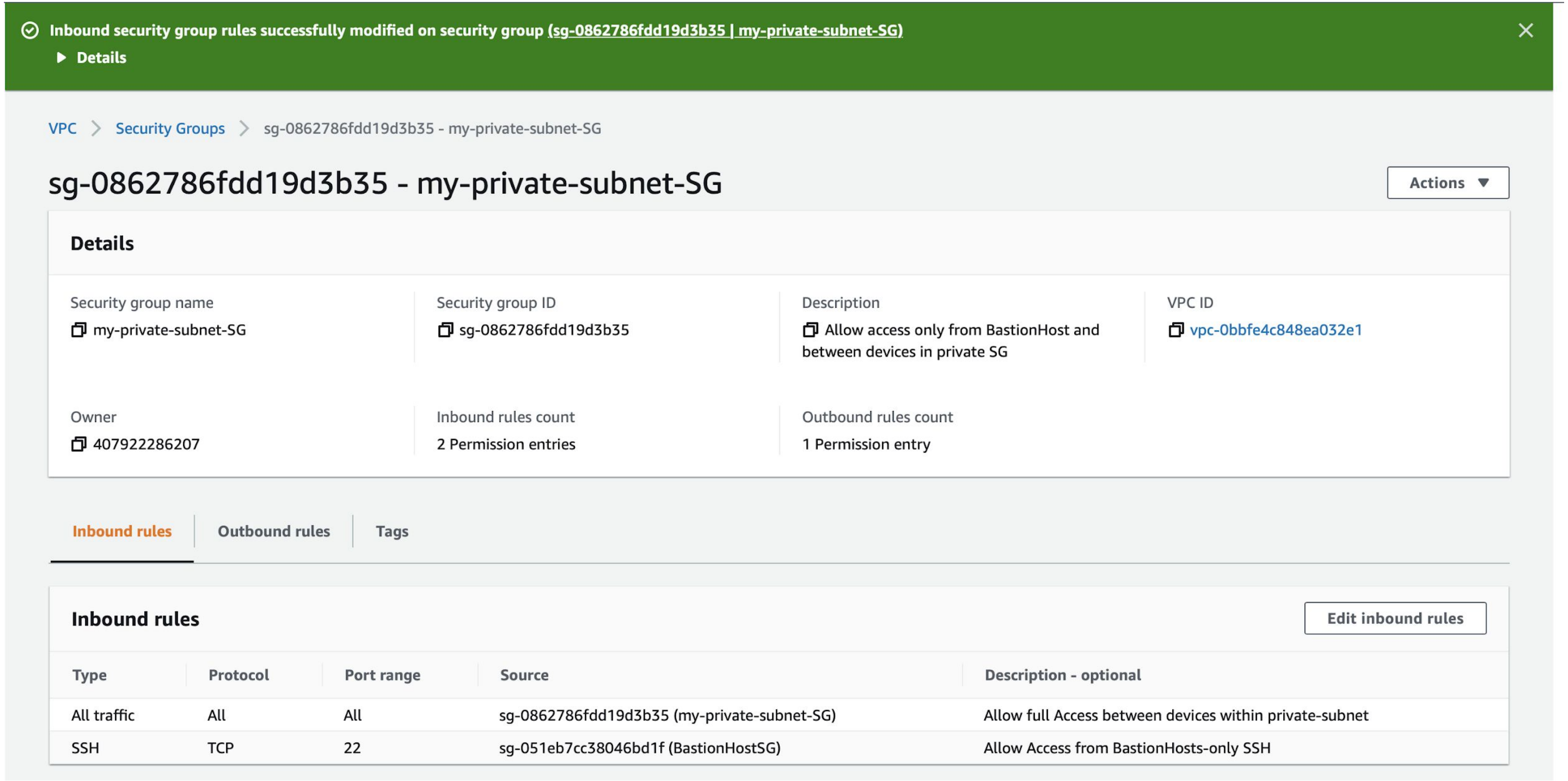
sg-0e636222160e9c33e - default

Outbound rules

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	0.0.0.0/0	-

Private-subnet-SG

Attach this SG to Private instances



Details
VPC > Security Groups > sg-0862786fdd19d3b35 - my-private-subnet-SG
Actions ▼
Inbound rules
Outbound rules
Tags
Edit inbound rules

Inbound security group rules successfully modified on security group (sg-0862786fdd19d3b35 | my-private-subnet-SG)

sg-0862786fdd19d3b35 - my-private-subnet-SG

Details

Security group name: my-private-subnet-SG

Security group ID: sg-0862786fdd19d3b35

Description: Allow access only from BastionHost and between devices in private SG

VPC ID: vpc-0bbfe4c848ea032e1

Owner: 407922286207

Inbound rules count: 2 Permission entries

Outbound rules count: 1 Permission entry

Inbound rules

Type	Protocol	Port range	Source	Description - optional
All traffic	All	All	sg-0862786fdd19d3b35 (my-private-subnet-SG)	Allow full Access between devices within private-subnet
SSH	TCP	22	sg-051eb7cc38046bd1f (BastionHostSG)	Allow Access from BastionHosts-only SSH

EC2 Instance in Public Subnet

- Setup an EC2 Instance, attach it to a Public subnet
- Use Default Security group & NACL
- Connect to EC2 Instance from External Network

Bastion Host

- From external network, laptop use the below method to access the private instance via Bastion host
- From my laptop, add the private key to the ssh agent using below command
- Ssh-add <ec2 private key)
- Ssh-add -L ; command to check that key is added
- Use below command to access Bastion host (with -A option and ip add of Bastion host, below example 3.230.155.152 is Bastion host public IP)
- ssh -A ec2-user@3.230.155.152
- From the Bastion host, use below command to access private instance
- Ssh ec2-user@private-instance-private ip

Bastion Host SG Notes

- On the Bastion host, apply a SG (non-def) with following rules
  - Inbound - allow ssh from everywhere, ICMP from only private-SG
  - Outbound - Use default rule (allow everything to everywhere)
- On the Private host, apply a SG (non-def) with following rules
  - Inbound - allow ssh only from BastionHostSG
  - Inbound - allow everythingfrom same privateSG (to allow instances in private subnet to talk to each other) only from BastionHostSG
  - Outbound - ICMP ipv4 to allow ping only from BastionHostSG

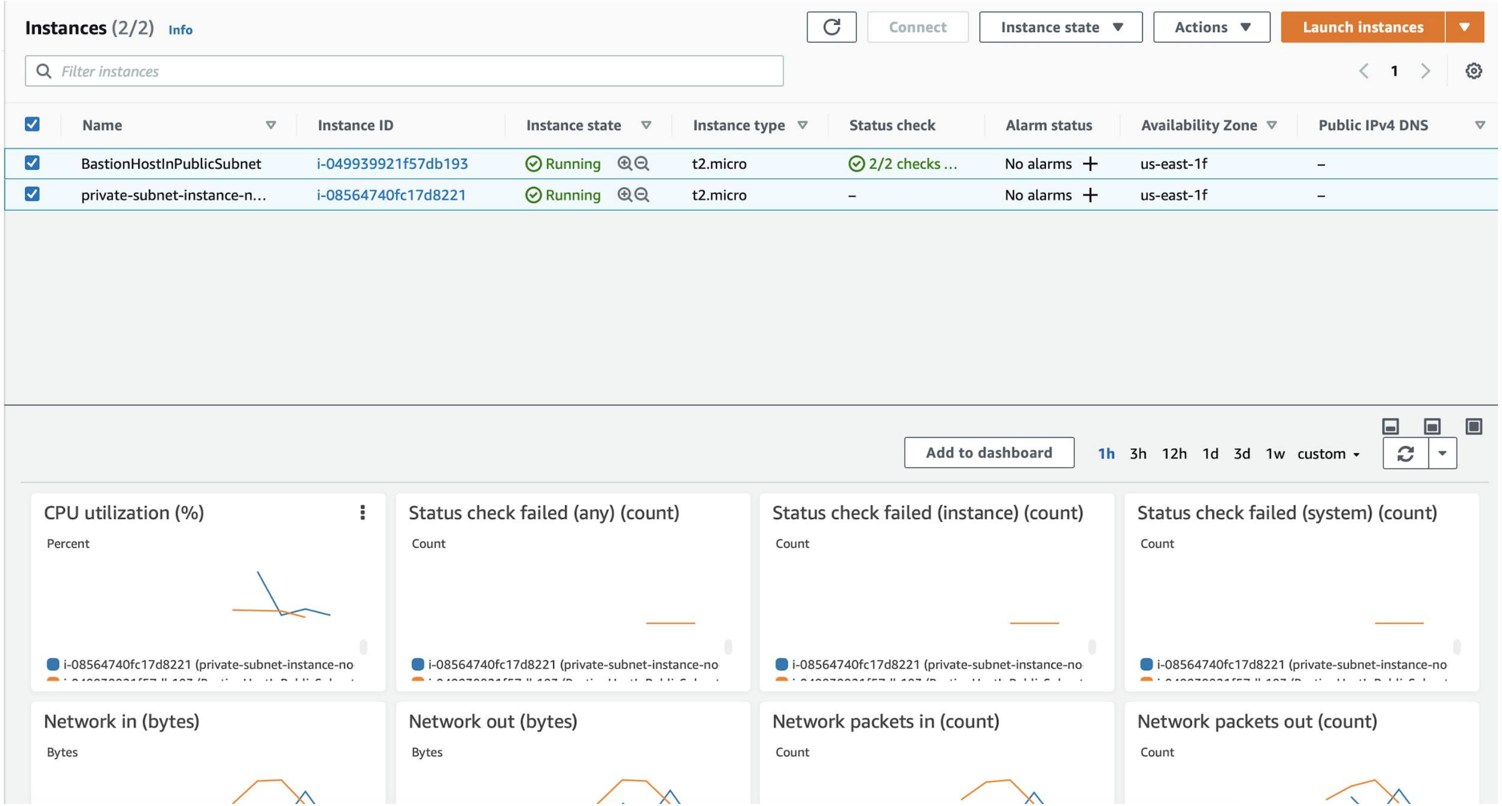
EC2 Instance in Private Subnet

- Setup an EC2 Instance, attach it to a Private subnet
- Use Default Security group & NACL
- Connect to EC2 instance in Private subnet through a publicly accessible EC2 Instance
- EC2 Instance in Private subnet will not be able to go out to Internet / External Network
- Create a NAT Gateway , add default route to Private RT with NAT GW as Nexthop
- Demonstrate how EC2 Instance in Private subnet can go out to Internet

VPC Endpoint Services

- Some Org don't want to be connected to Public Network/Internet
- Yet they have to access AWS Services/resources in Publicly available area
- An AWS VPC Endpoint allows access to AWS Services that are in public zone
- VPC Endpoint services are suited for VPC without connected to the public internet (VPC’s with only private subnets)
- AWS VPC Endpoints services are offered using two different endpoints/options to choose from:
- AWS Gateway Endpoints and AWS Interface Endpoints.
-

Launch two Instances



Instances (2/2) Info

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
☑	BastionHostInPublicSubnet	i-049939921f57db193	✓ Running	t2.micro	✓ 2/2 checks ...	No alarms +	us-east-1f	–
☑	private-subnet-instance-n...	i-08564740fc17d8221	✓ Running	t2.micro	–	No alarms +	us-east-1f	–

Connect
Instance state ▼
Actions ▼
Launch instances ▼
Filter instances
1
Add to dashboard
1h
3h
12h
1d
3d
1w
custom
CPU utilization (%)
Percent
Status check failed (any) (count)
Count
Status check failed (instance) (count)
Count
Status check failed (system) (count)
Count
i-08564740fc17d8221 (private-subnet-instance-no
Network in (bytes)
Bytes
Network out (bytes)
Bytes
Network packets in (count)
Count
Network packets out (count)
Count

EC2 User Data

For Ubuntu EC2 Instance

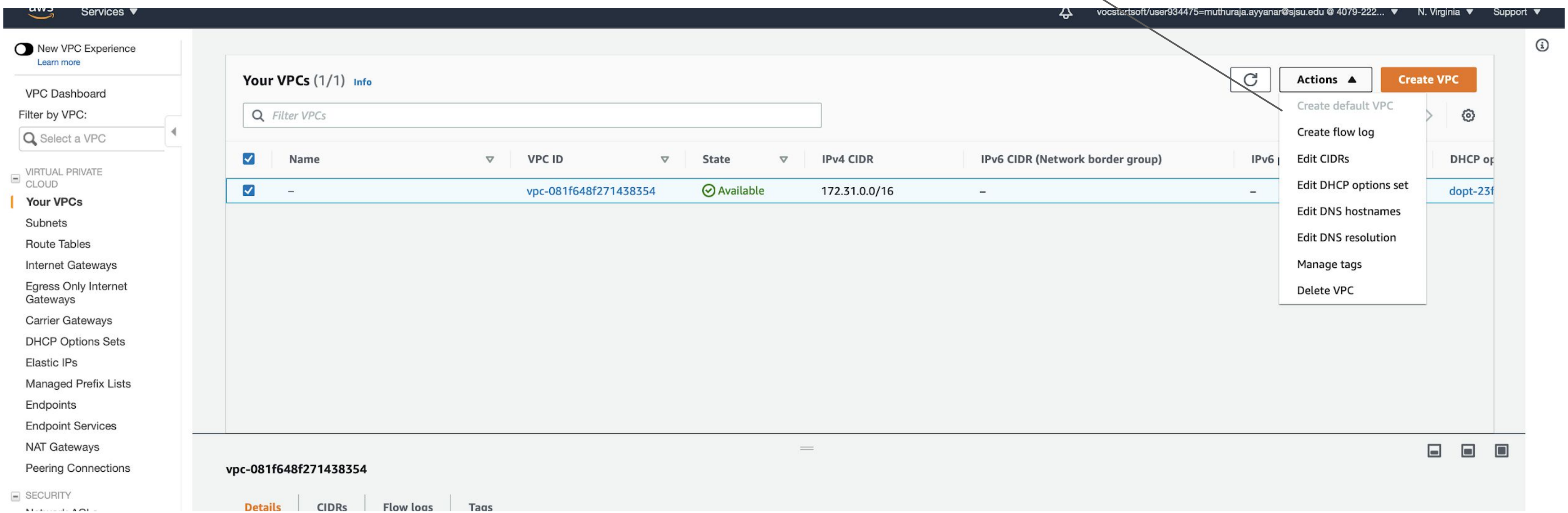
```
#!/bin/bash
#Install Apache/httpd Web Server
apt-get update -y
apt-get install apache2 -y
mv /var/www/html/index.html /var/www/html/index.html.orig
echo “Web Server is running on $(hostname -f)” >
/var/www/html/index.html
service apache2 start
```

For Amazon Linux v2 AMI EC2 Instance

```
#!/bin/bash
#Install Apache/httpd Web Server
yum update -y
yum install -y httpd.x86_64
systemctl start httpd.service
systemctl enable httpd.service
echo “Web Server is running on $(hostname -f)” >
/var/www/html/index.html
```

Create Default VPC

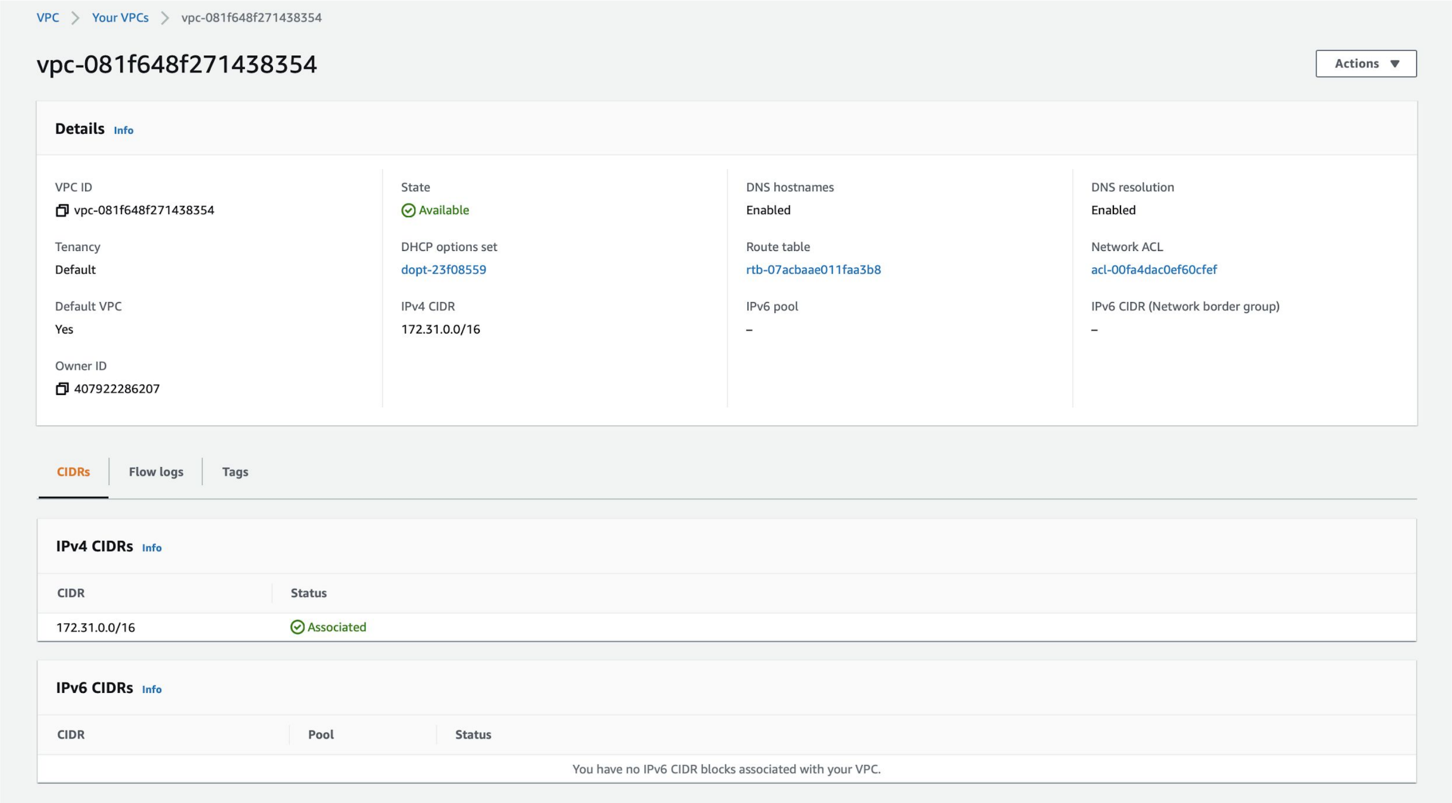
When the default VPC is deleted, we can use “Create default VPC” option from “Actions” in the Your VPCs option from VPC COnsole to create default VPC (In the below screen the option is grayed since we already have a default VPC”



☑	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR (Network border group)	IPv6	DHCP op
☑	–	vpc-081f648f271438354	✓ Available	172.31.0.0/16	–	–	dopt-23f

vpc-081f648f271438354

Create Default VPC



VPC > Your VPCs > vpc-081f648f271438354

vpc-081f648f271438354

Details Info

VPC ID vpc-081f648f271438354	State ✓ Available	DNS hostnames Enabled	DNS resolution Enabled
Tenancy Default	DHCP options set dopt-23f08559	Route table rtb-07acbaae011faa3b8	Network ACL acl-00fa4dac0ef60cfef
Default VPC Yes	IPv4 CIDR 172.31.0.0/16	IPv6 pool –	IPv6 CIDR (Network border group) –
Owner ID 407922286207			

IPv4 CIDRs Info

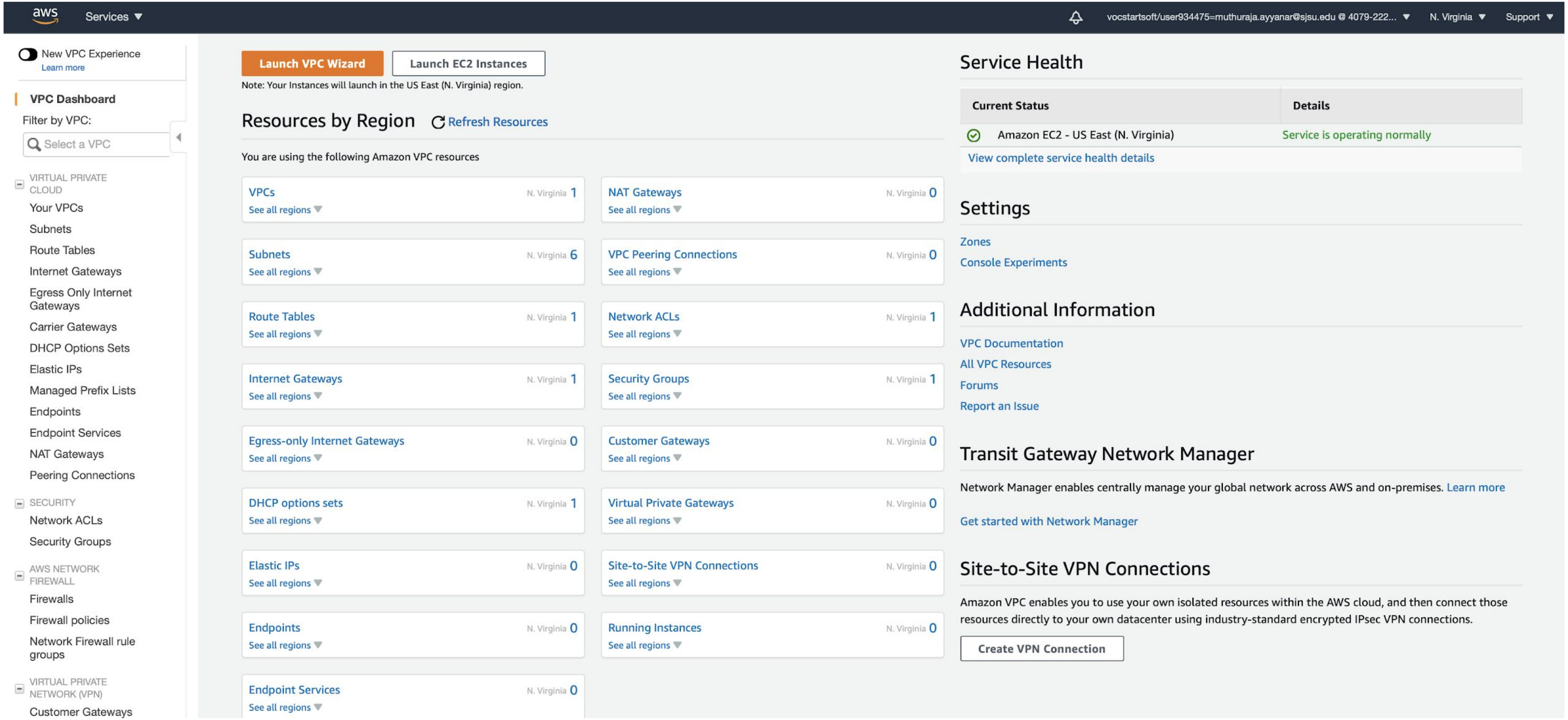
CIDR	Status
172.31.0.0/16	✓ Associated

IPv6 CIDRs Info

CIDR	Pool	Status

You have no IPv6 CIDR blocks associated with your VPC.

Default VPC Resources with new Default VPC



Note: Your Instances will launch in the US East (N. Virginia) region.

Resources by Region

Refresh Resources

You are using the following Amazon VPC resources

Resource	Region	Count
VPCs	N. Virginia	1
NAT Gateways	N. Virginia	0
Subnets	N. Virginia	6
VPC Peering Connections	N. Virginia	0
Route Tables	N. Virginia	1
Network ACLs	N. Virginia	1
Internet Gateways	N. Virginia	1
Security Groups	N. Virginia	1
Egress-only Internet Gateways	N. Virginia	0
Customer Gateways	N. Virginia	0
DHCP options sets	N. Virginia	1
Virtual Private Gateways	N. Virginia	0
Elastic IPs	N. Virginia	0
Site-to-Site VPN Connections	N. Virginia	0
Endpoints	N. Virginia	0
Running Instances	N. Virginia	0
Endpoint Services	N. Virginia	0

Service Health

Current Status	Details
✓ Amazon EC2 - US East (N. Virginia)	Service is operating normally

View complete service health details

Settings

Zones

Console Experiments

Additional Information

VPC Documentation

All VPC Resources

Forums

Report an Issue

Transit Gateway Network Manager

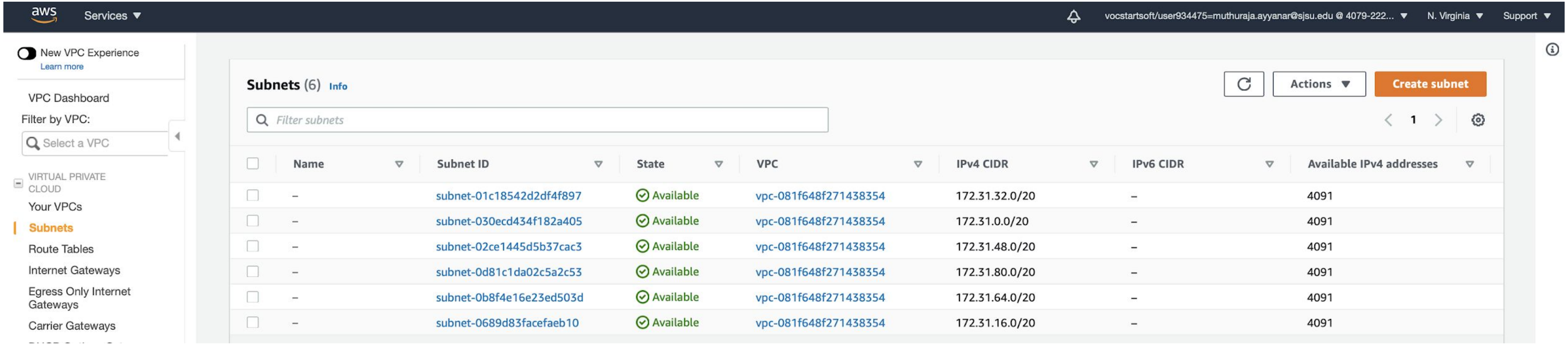
Network Manager enables centrally manage your global network across AWS and on-premises. Learn more

Get started with Network Manager

Site-to-Site VPN Connections

Amazon VPC enables you to use your own isolated resources within the AWS cloud, and then connect those resources directly to your own datacenter using industry-standard encrypted IPsec VPN connections.

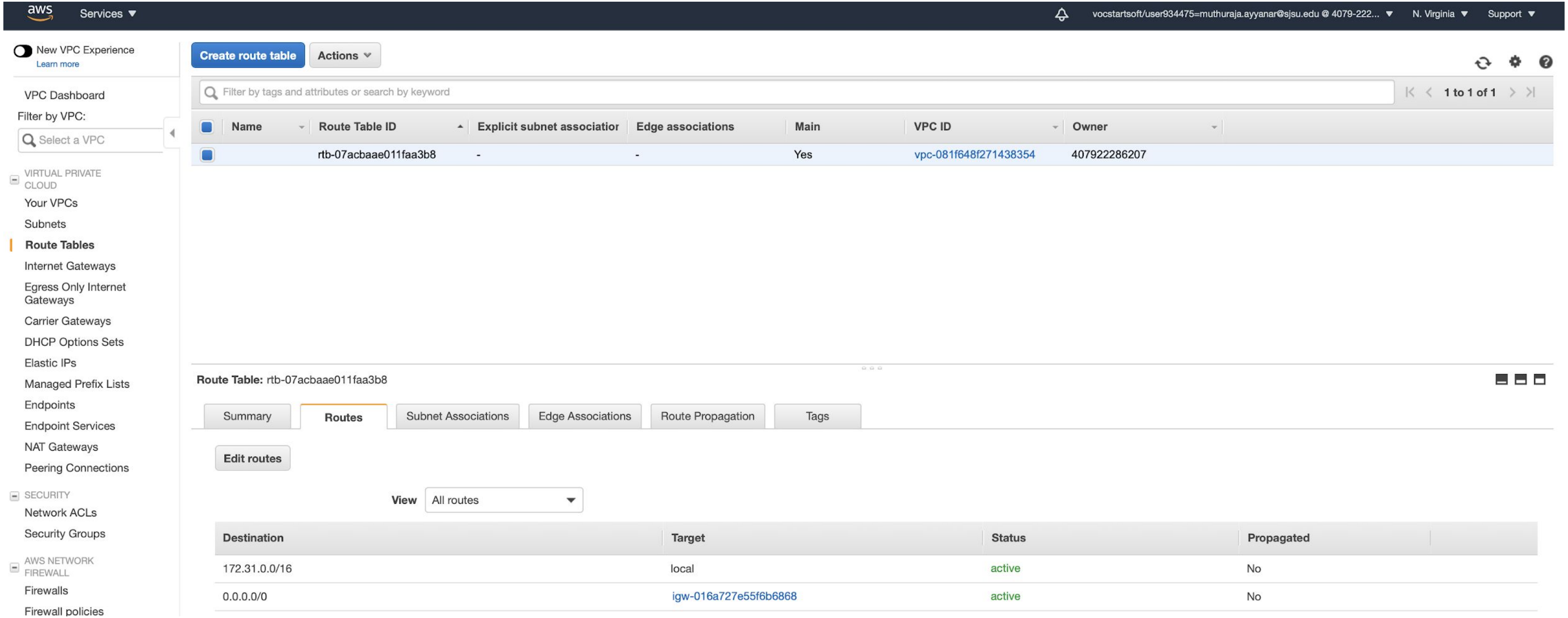
Default Subnet Resources with new Default VPC



Subnets (6) Info

□	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses
□	–	subnet-01c18542d2df4f897	✓ Available	vpc-081f648f271438354	172.31.32.0/20	–	4091
□	–	subnet-030ecd434f182a405	✓ Available	vpc-081f648f271438354	172.31.0.0/20	–	4091
□	–	subnet-02ce1445d5b37cac3	✓ Available	vpc-081f648f271438354	172.31.48.0/20	–	4091
□	–	subnet-0d81c1da02c5a2c53	✓ Available	vpc-081f648f271438354	172.31.80.0/20	–	4091
□	–	subnet-0b8f4e16e23ed503d	✓ Available	vpc-081f648f271438354	172.31.64.0/20	–	4091
□	–	subnet-0689d83facefaeb10	✓ Available	vpc-081f648f271438354	172.31.16.0/20	–	4091

Default RT Resources with new Default VPC



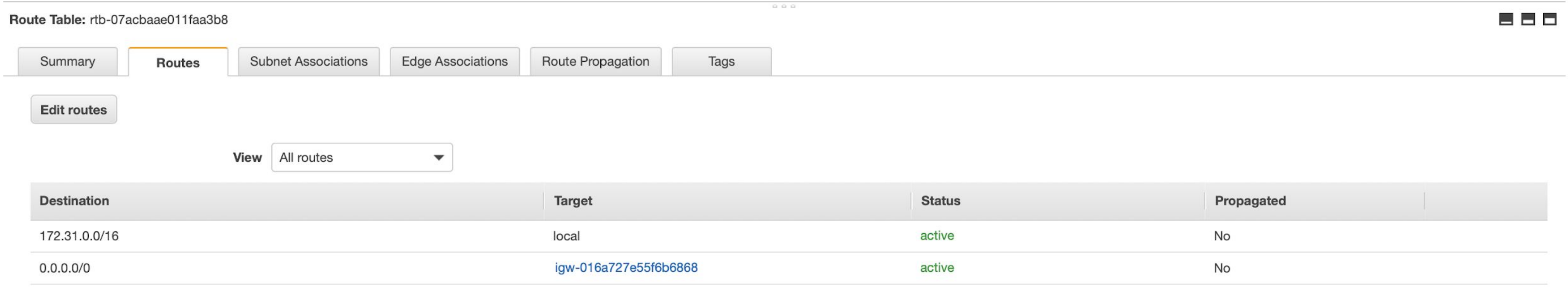
Name	Route Table ID	Explicit subnet associatior	Edge associations	Main	VPC ID	Owner
	rtb-07acbaae011faa3b8	-	-	Yes	vpc-081f648f271438354	407922286207

Route Table: rtb-07acbaae011faa3b8

View: All routes

Destination	Target	Status	Propagated
172.31.0.0/16	local	active	No
0.0.0.0/0	igw-016a727e55f6b6868	active	No

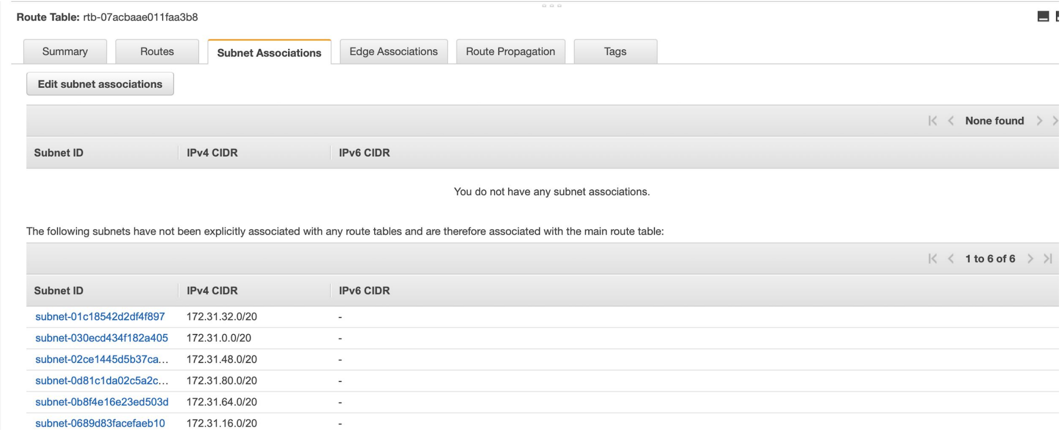
Default RT Resources with new Default VPC



Route Table: rtb-07acbaae011faa3b8

View All routes

Destination	Target	Status	Propagated
172.31.0.0/16	local	active	No
0.0.0.0/0	igw-016a727e55f6b6868	active	No



Route Table: rtb-07acbaae011faa3b8

None found

Subnet ID	IPv4 CIDR	IPv6 CIDR

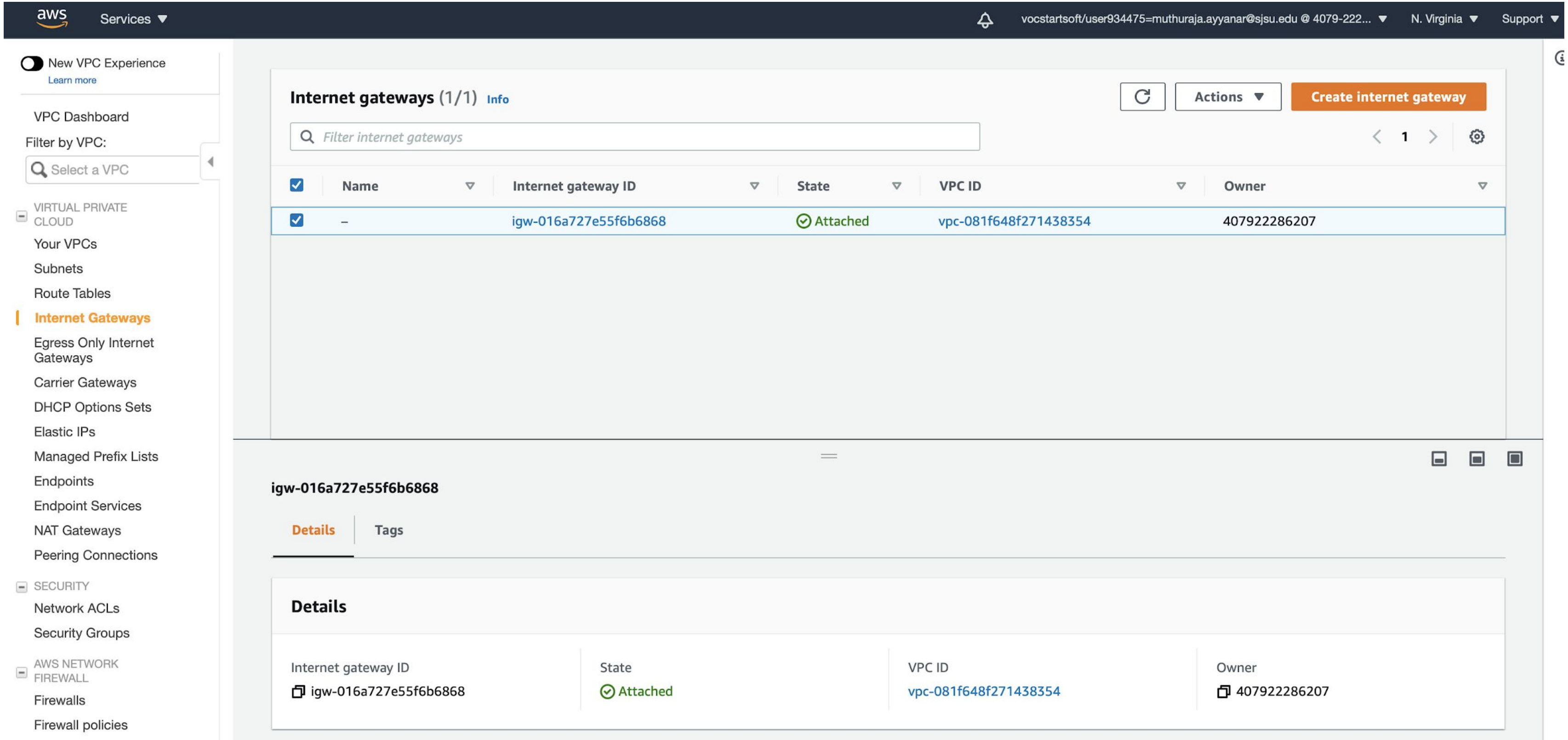
You do not have any subnet associations.

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

1 to 6 of 6

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-01c18542d2df4f897	172.31.32.0/20	-
subnet-030ecd434f182a405	172.31.0.0/20	-
subnet-02ce1445d5b37ca...	172.31.48.0/20	-
subnet-0d81c1da02c5a2c...	172.31.80.0/20	-
subnet-0b8f4e16e23ed503d	172.31.64.0/20	-
subnet-0689d83facefaeb10	172.31.16.0/20	-

Default IGW Resources with new Default VPC



Internet gateways (1/1) Info

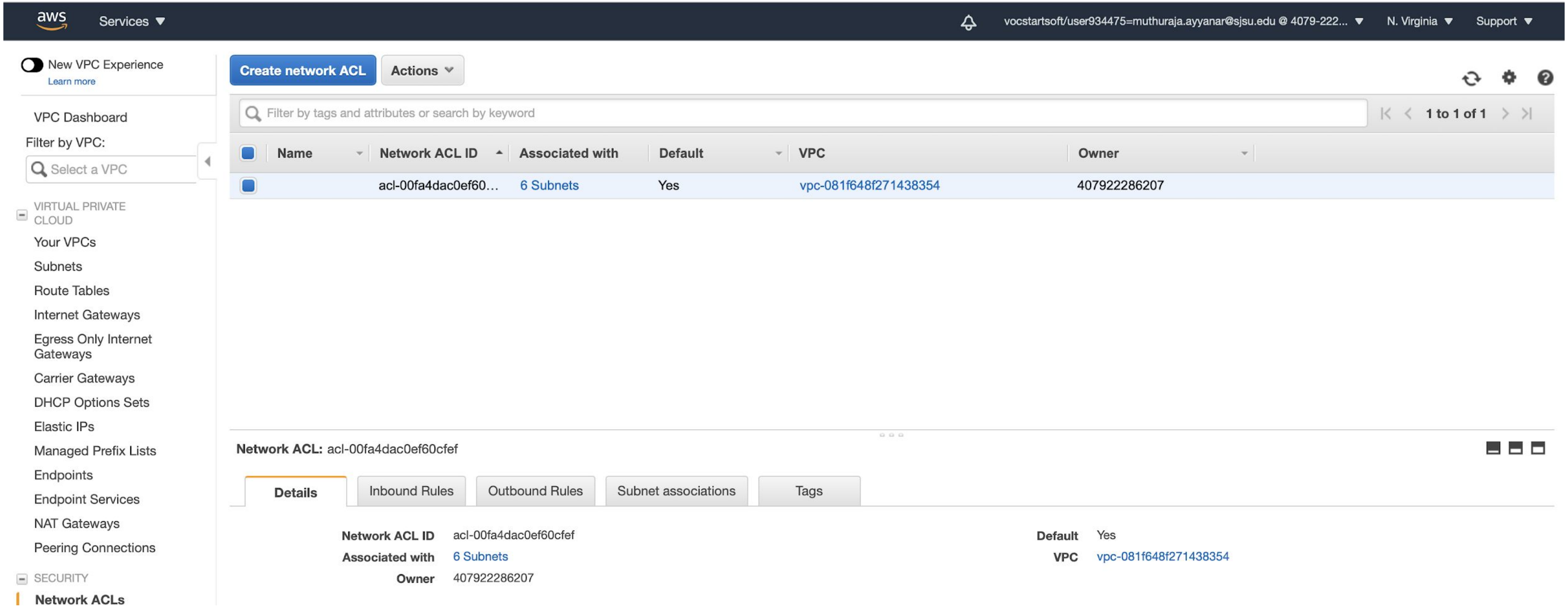
☑	Name	Internet gateway ID	State	VPC ID	Owner
☑	–	igw-016a727e55f6b6868	✓ Attached	vpc-081f648f271438354	407922286207

igw-016a727e55f6b6868

Details

Internet gateway ID	State	VPC ID	Owner
igw-016a727e55f6b6868	✓ Attached	vpc-081f648f271438354	407922286207

Default NACL Resources with new Default VPC

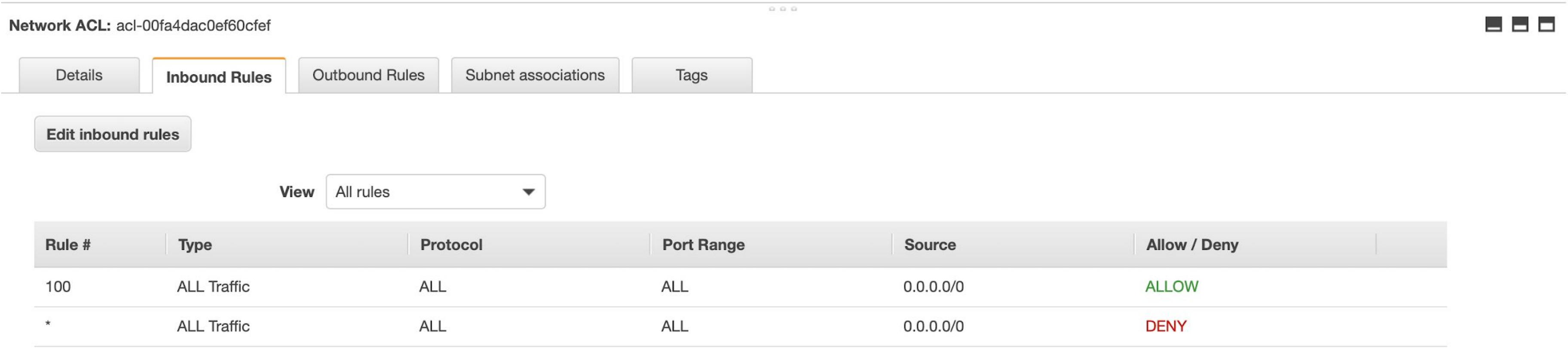


Name	Network ACL ID	Associated with	Default	VPC	Owner
	acl-00fa4dac0ef60…	6 Subnets	Yes	vpc-081f648f271438354	407922286207

Network ACL: acl-00fa4dac0ef60cfef

Network ACL ID	acl-00fa4dac0ef60cfef	**Default**	Yes
Associated with	6 Subnets	**VPC**	vpc-081f648f271438354
Owner	407922286207		

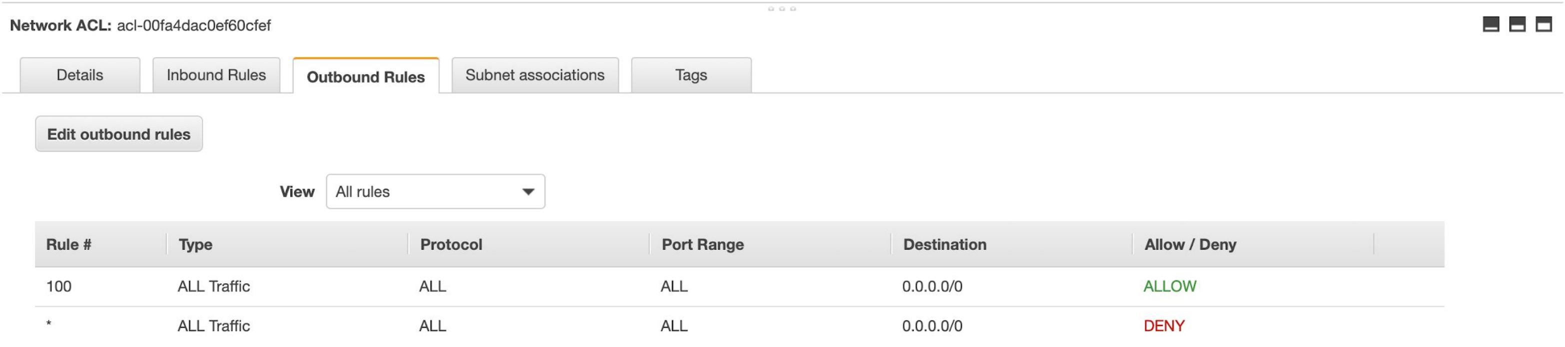
Default NACL Resources with new Default VPC



Network ACL: acl-00fa4dac0ef60cfef

View All rules

Rule #	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

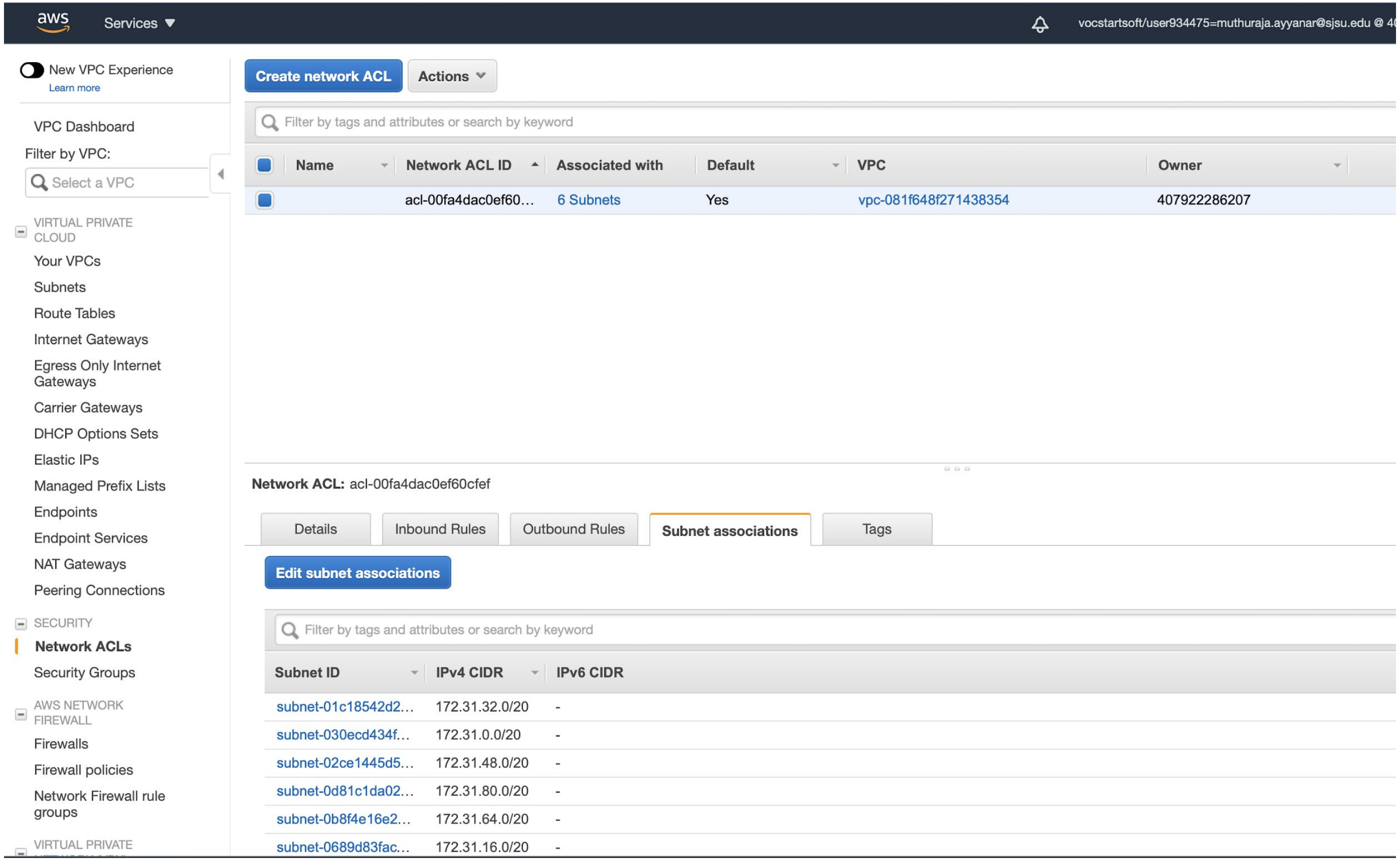


Network ACL: acl-00fa4dac0ef60cfef

View All rules

Rule #	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

Default NACL Resources with new Default VPC

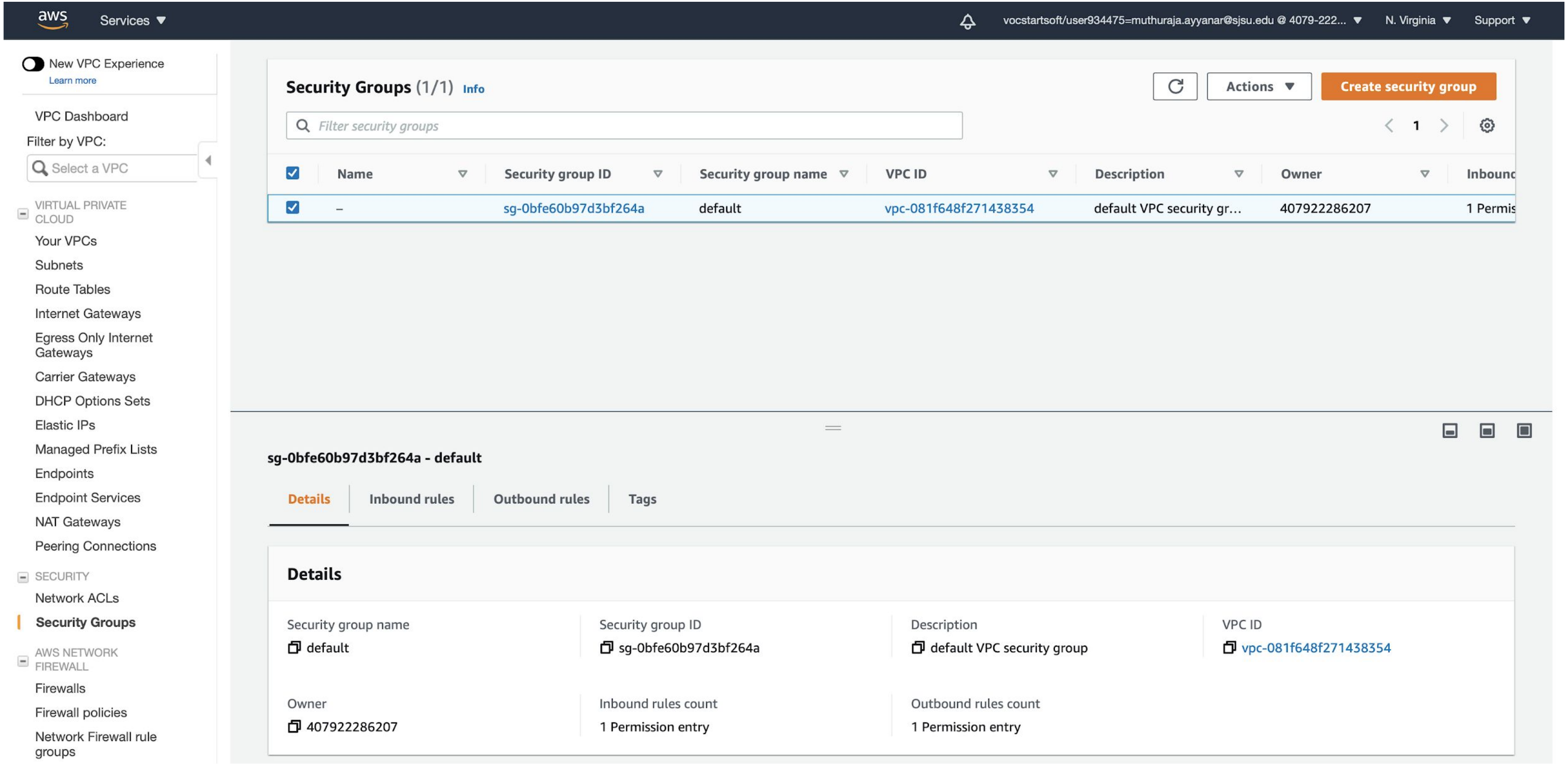


Name	Network ACL ID	Associated with	Default	VPC	Owner
	acl-00fa4dac0ef60…	6 Subnets	Yes	vpc-081f648f271438354	407922286207

Network ACL: acl-00fa4dac0efc60cfef

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-01c18542d2…	172.31.32.0/20	-
subnet-030ecd434f…	172.31.0.0/20	-
subnet-02ce1445d5…	172.31.48.0/20	-
subnet-0d81c1da02…	172.31.80.0/20	-
subnet-0b8f4e16e2…	172.31.64.0/20	-
subnet-0689d83fac…	172.31.16.0/20	-

Default SG Resources with new Default VPC



Security Groups (1/1) Info

☑	Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbounc
☑	–	sg-0bfe60b97d3bf264a	default	vpc-081f648f271438354	default VPC security gr...	407922286207	1 Permis

sg-0bfe60b97d3bf264a - default

Details

Security group name: default

Security group ID: sg-0bfe60b97d3bf264a

Description: default VPC security group

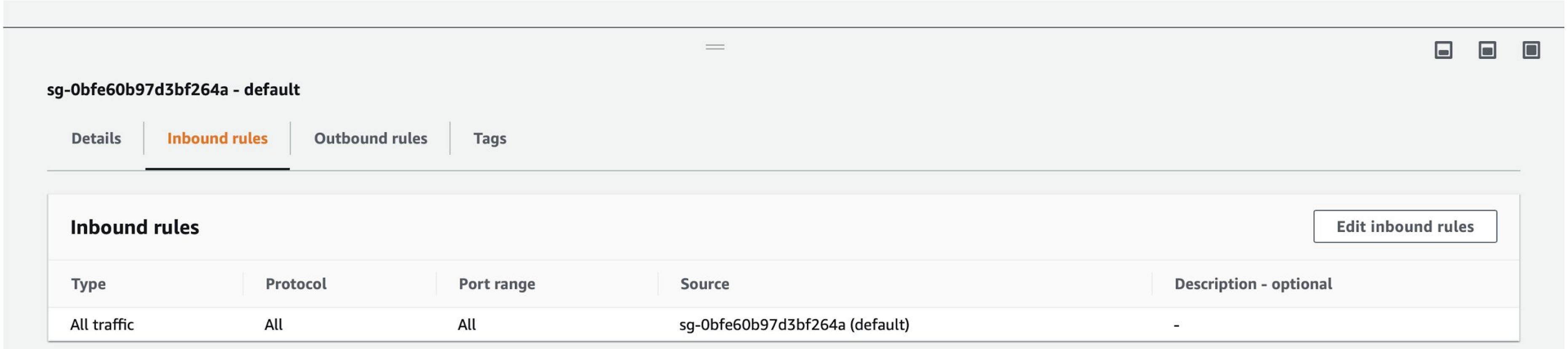
VPC ID: vpc-081f648f271438354

Owner: 407922286207

Inbound rules count: 1 Permission entry

Outbound rules count: 1 Permission entry

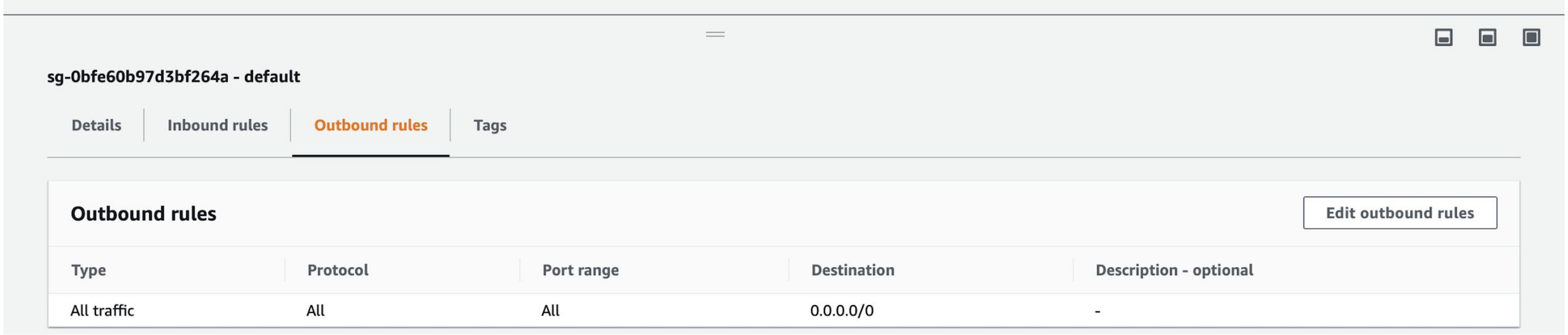
Default SG Resources with new Default VPC



sg-0bfe60b97d3bf264a - default

Inbound rules

Type	Protocol	Port range	Source	Description - optional
All traffic	All	All	sg-0bfe60b97d3bf264a (default)	-



sg-0bfe60b97d3bf264a - default

Outbound rules

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	0.0.0.0/0	-