

## AWS VPC

### VPC (Virtual Private Cloud):

- VPC comes under Network Engineering
- IP ranges from 0 to 255
- CIDR (Classless Inter-Domain Routing) – Representation of IP address.  
<https://www.ipaddressguide.com/cidr>
- Understand the Difference between IPv4 and IPv6 :  
[https://byjus.com/free-ias-prep/difference-between-ipv4-and-ipv6/?utm\\_source=Google&utm\\_medium=CPC&utm\\_campaign=IAS\\_Dynamic\\_Traffic\\_Chennai\\_April30&utm\\_term=&gclid=CjwKCAjw9r-DBhBxEiwA9qYUpTsn9BITHLIN5qXby5QYV-rLezM5a78stKWNrcdaTulb3Ydq-OFs6xoCjakQAvD\\_BwE](https://byjus.com/free-ias-prep/difference-between-ipv4-and-ipv6/?utm_source=Google&utm_medium=CPC&utm_campaign=IAS_Dynamic_Traffic_Chennai_April30&utm_term=&gclid=CjwKCAjw9r-DBhBxEiwA9qYUpTsn9BITHLIN5qXby5QYV-rLezM5a78stKWNrcdaTulb3Ydq-OFs6xoCjakQAvD_BwE)

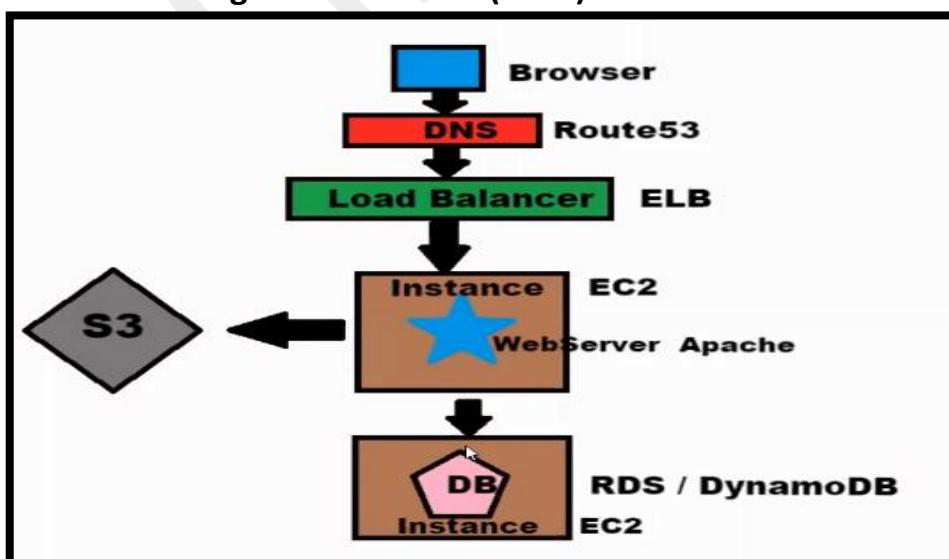
**Refer below to understand IP, CIDR, IPv4 and Need of Private IP**



### Key Concepts:

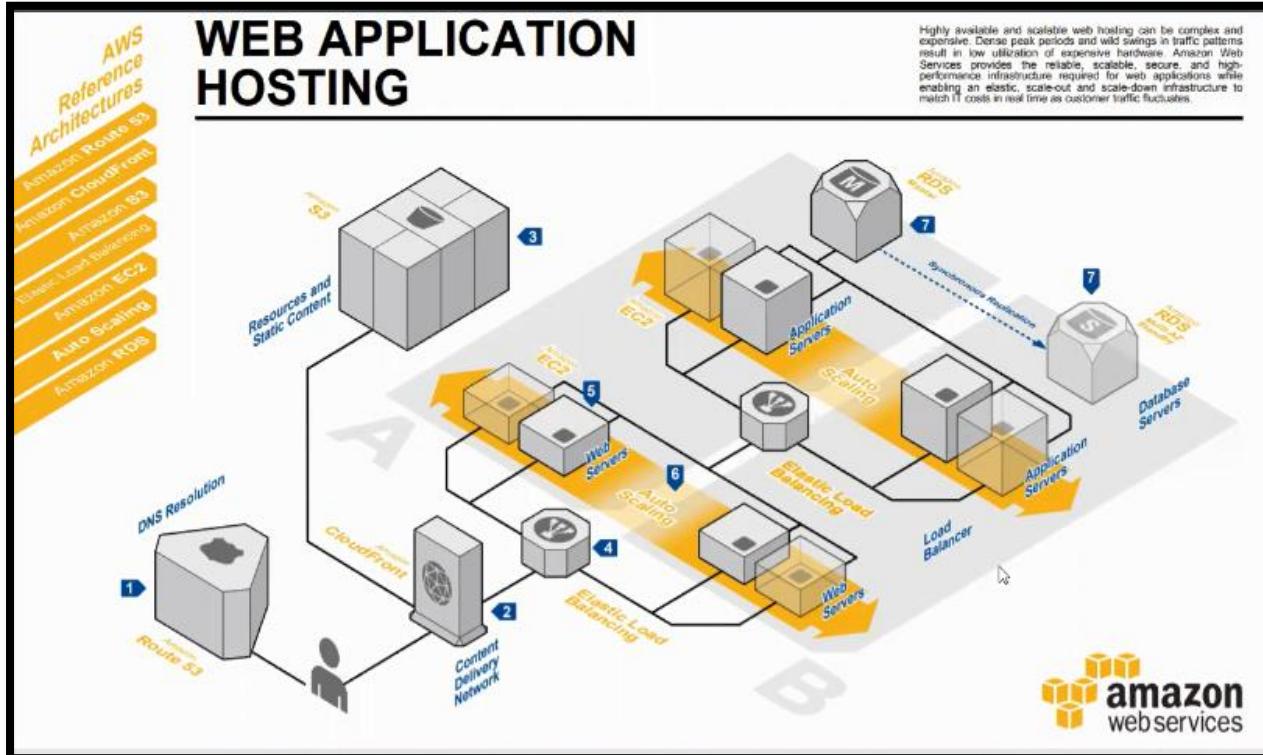
- **VPC** - a Virtual Network dedicated to AWS user on internet
- **IGW** - Enables communication between instances on your VPC over net
- **SUBNET**:  
 A logical subdivision of a Network  
 One or more sub network can be created based on business requirement  
 IP representation and range can be set using CIDR
- **CIDR**: Classless Inter-Domain Routing helps to set the range and IP addresses representation for the subnets.
- **IP**: Essential to access the Internet. Which has a set of rules
- **Public IP**: assigned from Amazon pool and able to access our instance only through this dynamic and static
- **Private IP**: Each instance will have a default network interface eth0...from here the private IP is generated for each instance static
- **Route tables**: This directs subnets and controls traffic through routes (set of rules)
- **NAT gateways**: Enables communication between instances (Public and Private)
- **Elastic IP on NAT gateways**: Static IP

### Amazon Management Console (AMC):



- Browser – Way to access the server
- DNS (Route53) – Since It is easy to remember we have to host domain to Public Ip or the server
- ELB – Balances Clients Application Request with the help of Autoscaling and ensure better server performance
- Webserver – Application server Engineering
- Database Engineering (Private and it contains confidential data's)
- Understand the differences between two-tier and three-tier architecture

## Example Architecture from AWS



- 2-tier => Client Application + Webserver + DB (Static Application)
- 3-Tier=> Client Application + Webserver+Application Server +DB (dynamic application)

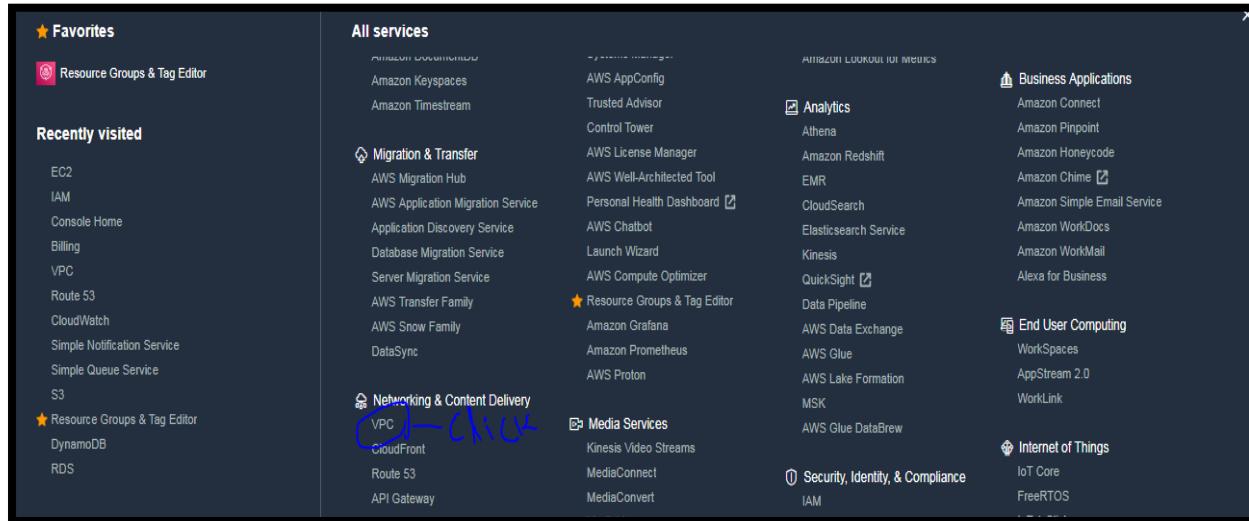
## VPC Creation:

Steps to Create and set up a VPC in AWS environment:

1. Create a own VPC.
2. Create a Public and Private subnet for different Available AZs by assigning different CIDR blocks.
3. Create Internet Gateway & attach it to the VPC.
4. Create Routing table [RT], One as Public & One as Private by associating the appropriate subnets to it.
5. Edit the Public route table's Route alone and map the IGW, not the Private and leave it as it is.
6. Create Two Security Groups - One for Public [Edit the Inbound rules with RDP, HTTP/HTTPS, SSH and map 0.0.0.0/0 in the source] & One for Private [Edit the inbound rules and map the SG of Public in the source].
7. Create Two EC2s one in public and one in private subnets with proper Security Groups.
8. Login into Public and check the internet connection.
9. Create NAT gateway with new Elastic IP for the internet connection in the Private Subnet. Map it to Private RT.
10. Now login into the Private EC2 and verify the connectivity and Internet facility.

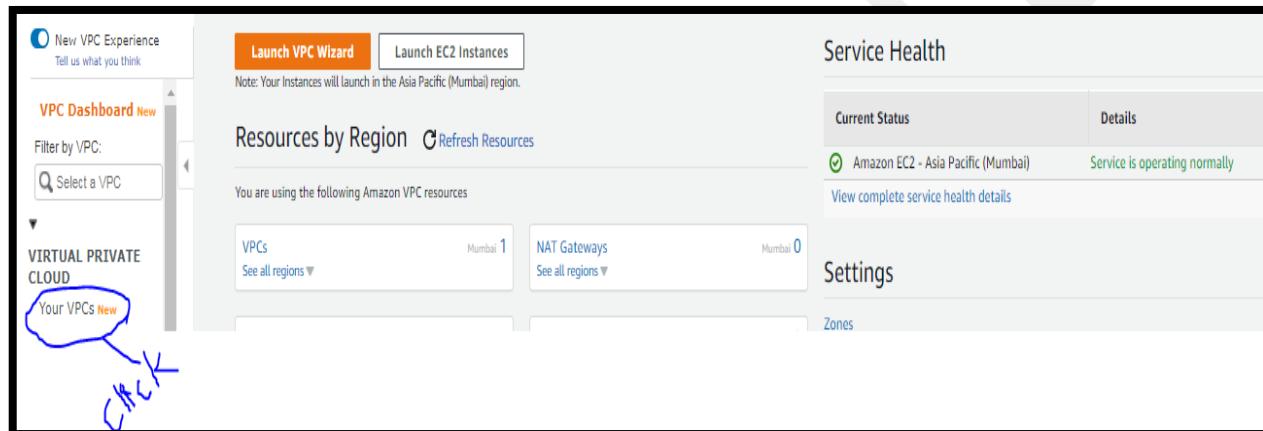
## Step1: Create a VPC

Choose the Service from AWS Console and single click→



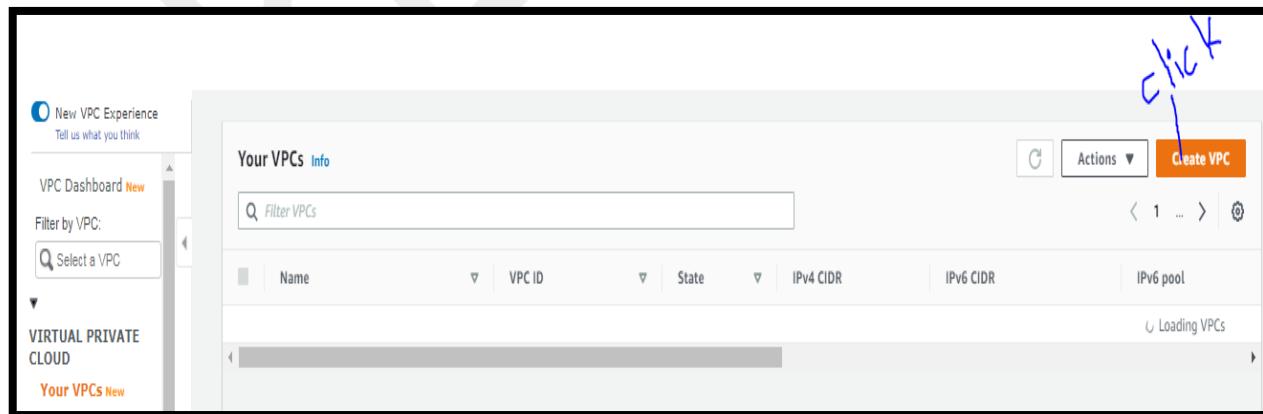
The screenshot shows the AWS navigation bar with the 'VPC' service highlighted. The 'Recently visited' section includes EC2, IAM, Console Home, Billing, VPC, Route 53, CloudWatch, Simple Notification Service, Simple Queue Service, S3, Resource Groups & Tag Editor, DynamoDB, and RDS. The 'All services' section is expanded, showing categories like Migration & Transfer, Networking & Content Delivery, Business Applications, End User Computing, Internet of Things, and others. The 'Networking & Content Delivery' category contains VPC, CloudFront, Route 53, and API Gateway. A blue circle with a hand icon is drawn over the 'VPC' link.

## Click on Your VPC



The screenshot shows the VPC Dashboard. It features a 'New VPC Experience' section with a 'Launch VPC Wizard' button. Below it is a 'VPC Dashboard' with a 'Select a VPC' dropdown. The main area is titled 'Resources by Region' with a 'Refresh Resources' button. It shows 'VPCs' (Mumbai 1) and 'NAT Gateways' (Mumbai 0). On the right, there's a 'Service Health' table with one entry: 'Amazon EC2 - Asia Pacific (Mumbai)' with status 'Service is operating normally'. A blue speech bubble with a hand icon points to the 'Your VPCs New' link.

## Click on Create VPC



The screenshot shows the VPC Dashboard again. It has the same layout as the previous screenshot, but with a blue arrow and a large blue 'click' annotation pointing to the 'Create VPC' button located at the top right of the 'Your VPCs' table.

## Name the VPC / Set CIDR as 10.0.0.0/16 (65536 Hosts created)

VPC > Your VPCs > Create 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.

MyVPC

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
<input type="text" value="Name"/>	<input type="text" value="MyVPC"/>

Add new tag

You can add 49 more tags.

Cancel Create VPC

Click

You successfully created [vpc-021cfbe8e114df0a1 / MyVPC](#)

VPC Dashboard [New](#)  
Filter by VPC:

**VIRTUAL PRIVATE CLOUD**

Your VPCs [New](#)  
 Subnets [New](#)  
 Route Tables  
 Internet Gateways [New](#)  
 Egress Only Internet Gateways [New](#)  
 DHCP Options Sets [New](#)  
 Elastic IPs [New](#)  
 Managed Prefix Lists [New](#)  
 Endpoints  
 Endpoint Services  
 NAT Gateways [New](#)  
 Peering Connections

**SECURITY**

Network ACLs [New](#)  
 Security Groups [New](#)

**REACHABILITY**

Reachability Analyzer

**Details** [Info](#)

VPC ID <a href="#">vpc-021cfbe8e114df0a1</a>	State <span style="color: green;">Available</span>	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP options set <a href="#">dept:c81cfea3</a>	Main route table <a href="#">rtb-00582c53e788b0b37</a>	Main network ACL <a href="#">acl-02818ab59497fccc5</a>
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -	IPv6 CIDR -
Route 53 Resolver DNS Firewall rule groups -	Owner ID <a href="#">773611265713</a>		

CIDRs Flow logs Tags

**IPv4 CIDRs** [Info](#)

CIDR	Status
<a href="#">10.0.0.0/16</a>	<span style="color: green;">Associated</span>

**IPv6 CIDRs** [Info](#)

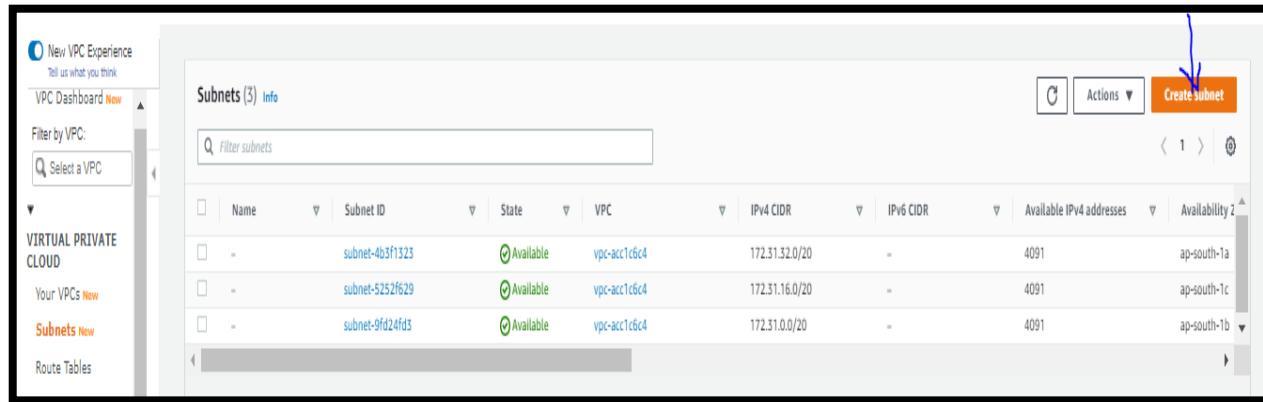
CIDR	Pool	Status
------	------	--------

## VPC Created

VPC	ID	Status	CIDR	RTB	Dept
<input checked="" type="checkbox"/> MyVPC	vpc-021cfbe8e114df0a1	<span style="color: green;">Available</span>	10.0.0.0/16	-	dept:c81cfea3

## Step2: Create a Public and Private Subnets in different AZ's

### Create a Public Subnet:

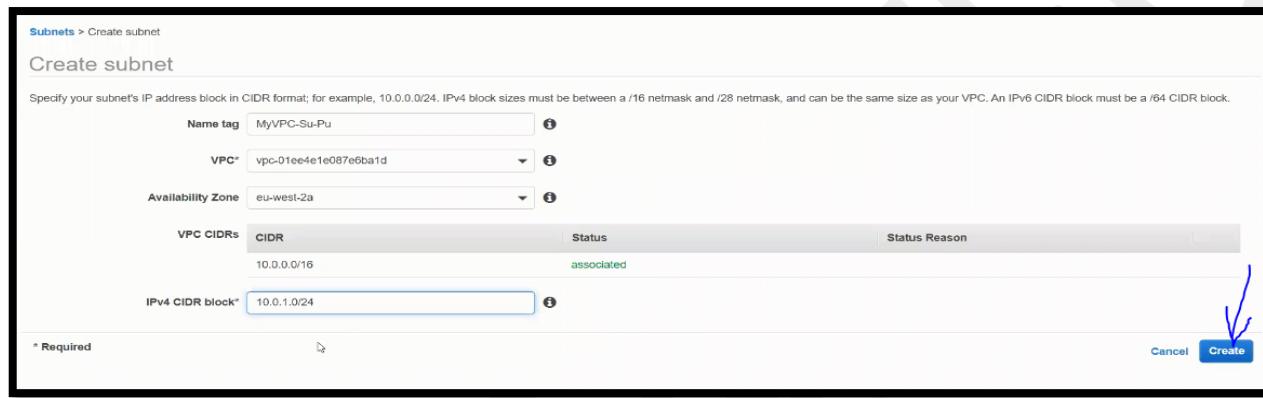


New VPC Experience  
Tell us what you think  
VPC Dashboard New  
Filter by VPC:  
Select a VPC  
Your VPCs New  
Subnets New  
Route Tables

**Subnets (3) Info**

Filter subnets

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	Availability Z.
subnet-4b3f1323	Available	vpc-acc1c6c4	172.31.32.0/20	=	4091	ap-south-1a	
subnet-5252f629	Available	vpc-acc1c6c4	172.31.16.0/20	=	4091	ap-south-1c	
subnet-9fd24fd3	Available	vpc-acc1c6c4	172.31.0.0/20	=	4091	ap-south-1b	



Subnets > Create subnet

Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag: MyVPC-Su-Pu

VPC\*: vpc-01ee4e1e087e6ba1d

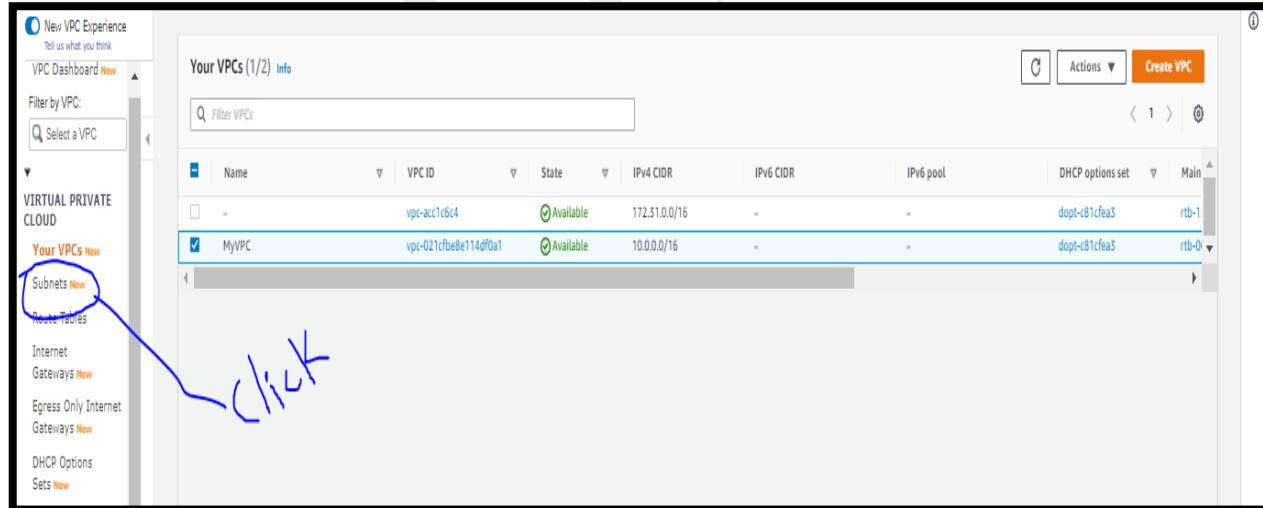
Availability Zone: eu-west-2a

VPC CIDRs	CIDR	Status	Status Reason
10.0.0.0/16		associated	

IPv4 CIDR block\*: 10.0.1.0/24

\* Required

Cancel **Create**



New VPC Experience  
Tell us what you think  
VPC Dashboard New  
Filter by VPC:  
Select a VPC  
Your VPCs New  
Subnets New  
Route Tables

**Your VPCs (1/2) Info**

Filter VPCs

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	IPv6 pool	DHCP options set	Main
vpc-acc1c6c4	Available	172.31.0.0/16	=	=	dopt-c81cfea3	rtb-1	
<b>MyVPC</b>	Available	10.0.0.0/16	=	=	dopt-c81cfea3	rtb-0	

## Create a Private Subnet:

Subnets > Create subnet

### Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag	MyVPC-Su-Pvt	<small>i</small>	
VPC*	vpc-01ee4e1e087e6ba1d	<small>i</small>	
Availability Zone	eu-west-2b	<small>i</small>	
VPC CIDRs	CIDR	Status	Status Reason
	10.0.0.0/16	associated	
IPv4 CIDR block*	10.0.2.0/24	<small>i</small>	

\* Required

Cancel Create

## Step3: Create an IGW & attach to VPC (IGW supplies n/w to VPC)

New VPC Experience  
Tell us what you think.

VPC Dashboard New

Filter by VPC:  
 Select a VPC

**VIRTUAL PRIVATE CLOUD**

- Your VPCs New
- Subnets
- Route Tables
- Internet Gateways New** 

Internet gateways (1/1) Info

<input checked="" type="checkbox"/>	Name	Internet gateway ID	State	VPC ID	Owner
<input checked="" type="checkbox"/>	-	igw-1433c07c	Attached	vpc-e7531b8f	172676947635

C Actions Create Internet gateway

New VPC Experience  
Tell us what you think.

VPC Dashboard New

Filter by VPC:  
 Select a VPC

**VIRTUAL PRIVATE CLOUD**

- Your VPCs New
- Subnets
- Route Tables
- Internet Gateways New** 

Internet gateways (1/1) Info

<input checked="" type="checkbox"/>	Name	Internet gateway ID	State	VPC ID	Owner
<input checked="" type="checkbox"/>	-	igw-1433c07c	Attached	vpc-e7531b8f	172676947635

C Actions Create Internet gateway

VPC > Internet gateways > Create internet gateway

### 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.  
 MyVPC-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
<input type="text"/> Name	<input type="text"/> MyVPC-IGW
<small>Add new tag</small>	

You can add 49 more tags.

Cancel Create Internet gateway

## Attach the IGW to MyVPC – Click attach to a VPC

The following internet gateway was created: igw-08ba1562c3a10c3c8 . You can now attach to a VPC to enable the VPC to communicate with the Internet.

VPC > Internet gateways > igw-08ba1562c3a10c3c8

igw-08ba1562c3a10c3c8 / MyVPC-IGW

Details Info

Internet gateway ID: igw-08ba1562c3a10c3c8 State: Detached

VPC ID: - Owner: 172676947635

Tags

Key	Value
Name	MyVPC-IGW

Actions ▾

*(Handwritten note: "attach to myVPC" is written next to the "State: Detached" section)*

## Choose MyVPC and attach

VPC > Internet gateways > Attach to VPC (igw-08ba1562c3a10c3c8)

Attach to VPC (igw-08ba1562c3a10c3c8) [Info](#)

**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-01ee4e1e087e6ba1d

AWS Command Line Interface command

Cancel **Attach internet gateway**

## Attachment Completed

Internet gateway igw-08ba1562c3a10c3c8 successfully attached to vpc-01ee4e1e087e6ba1d

VPC > Internet gateways > igw-08ba1562c3a10c3c8

igw-08ba1562c3a10c3c8 / MyVPC-IGW

Details Info

Internet gateway ID: igw-08ba1562c3a10c3c8 State: Attached

VPC ID: vpc-01ee4e1e087e6ba1d | MyVPC Owner: 172676947635

Tags

Key	Value
Name	MyVPC-IGW

## Step4: Create a Public & private Route Tables & associate with appropriate Subnets.

*Public RT*

Route Tables > Create route table

### Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Name tag	MyVPC-RT-Pu	<small>i</small>
VPC*	vpc-01ee4e1e087e6ba1d	<small>C i</small>
Key (128 characters maximum)		Value (256 characters maximum)
<small>This resource currently has no tags</small>		
Add Tag	50 remaining (Up to 50 tags maximum)	
* Required		<small>Cancel</small> <small>Create</small> 

*Private RT*

Route Tables > Create route table

### Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Name tag	MyVPC-RT-Pvt	<small>i</small>
VPC*	vpc-01ee4e1e087e6ba1d	<small>C i</small>
Key (128 characters maximum)		Value (256 characters maximum)
<small>This resource currently has no tags</small>		
Add Tag	50 remaining (Up to 50 tags maximum)	
* Required		<small>Cancel</small> <small>Create</small> 

## Ensure to Two Route Tables Created

New VPC Experience  
Tell us what you think

VPC Dashboard New

Filter by VPC:  
 Select a VPC

**VIRTUAL PRIVATE CLOUD**

Your VPCs New

Subnets

**Route Tables** 

Internet Gateways New

Egress Only Internet Gateways New

DHCP Options Sets New

Elastic IPs New

Managed Prefix Lists New

Endpoints

Endpoint Services

NAT Gateways New

Peering Connections

**Create route table** Actions v

Filter by tags and attributes or search by keyword

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
MyVPC-RT-Pu	rtb-02a2a56e582f49929	-	-	No	vpc-01ee4e1e087e6ba1d   MyVPC	17267
	rtb-05788af7dcf2a2efb	-	-	Yes	vpc-01ee4e1e087e6ba1d   MyVPC	17267
MyVPC-RT-Pvt	rtb-0a7f16a007d002140	-	-	No	vpc-01ee4e1e087e6ba1d   MyVPC	17267
	rtb-69eaef01	-	-	Yes	vpc-e7531b6f	17267

Route Table: rtb-02a2a56e582f49929

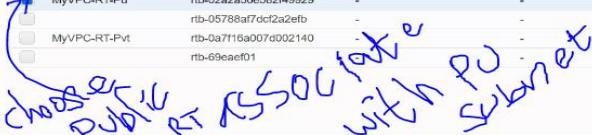
Summary Routes Subnet Associations Edge Associations Route Propagation Tags

**Edit subnet associations**

Subnet ID	IPv4 CIDR	IPv6 CIDR
-----------	-----------	-----------

## Associate Public RT with Public Subnet

### Click Subnet Associations



New VPC Experience  
Tell us what you think

VPC Dashboard [New](#)

Filter by VPC: [Select a VPC](#)

**VIRTUAL PRIVATE CLOUD**

- Your VPCs [New](#)
- Subnets
- Route Tables**
- Internet Gateways [New](#)
- Egress Only Internet Gateways [New](#)
- DHCP Options Sets [New](#)
- Elastic IPs [New](#)
- Managed Prefix Lists [New](#)
- Endpoints
- Endpoint Services

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
MyVPC-RT-Pu	rtb-02a2a56e582f49929	-	-	No	vpc-01ee4e1e087e6ba1d   MyVPC	17267t
MyVPC-RT-Pvt	rtb-05788af7dcf2a2efb	-	-	Yes	vpc-01ee4e1e087e6ba1d   MyVPC	17267t
	rtb-0a7f16a007d002140	-	-	No	vpc-01ee4e1e087e6ba1d   MyVPC	17267t
	rtb-69eaef01	-	-	Yes	vpc-e7531b8f	17267t

Route Table: rtb-02a2a56e582f49929

Summary Routes Subnet Associations Edge Associations Route Propagation Tags

Route Table ID: rtb-02a2a56e582f49929  
Explicitly Associated with: -  
Owner: 172676947635

Main: No  
VPC: vpc-01ee4e1e087e6ba1d | MyVPC

### Click Edit Subnet Associations



New VPC Experience  
Tell us what you think

VPC Dashboard [New](#)

Filter by VPC: [Select a VPC](#)

**VIRTUAL PRIVATE CLOUD**

- Your VPCs [New](#)
- Subnets
- Route Tables**
- Internet Gateways [New](#)
- Egress Only Internet Gateways [New](#)
- DHCP Options Sets [New](#)
- Elastic IPs [New](#)
- Managed Prefix Lists [New](#)
- Endpoints
- Endpoint Services
- NAT Gateways [New](#)
- Peering Connections

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
MyVPC-RT-Pu	rtb-02a2a56e582f49929	-	-	No	vpc-01ee4e1e087e6ba1d   MyVPC	17267t
	rtb-05788af7dcf2a2efb	-	-	Yes	vpc-01ee4e1e087e6ba1d   MyVPC	17267t
MyVPC-RT-Pvt	rtb-0a7f16a007d002140	-	-	No	vpc-01ee4e1e087e6ba1d   MyVPC	17267t
	rtb-69eaef01	-	-	Yes	vpc-e7531b8f	17267t

Route Table: rtb-02a2a56e582f49929

Summary Routes Subnet Associations Edge Associations Route Propagation Tags

Edit subnet associations

Subnet ID IPv4 CIDR IPv6 CIDR

### Select Public Subnet and save



Route Tables > Edit subnet associations

Edit subnet associations

Route table: rtb-02a2a56e582f49929 (MyVPC-RT-Pu)

Associated subnets: [subnet-0bb0c3dba5af5dcff](#)

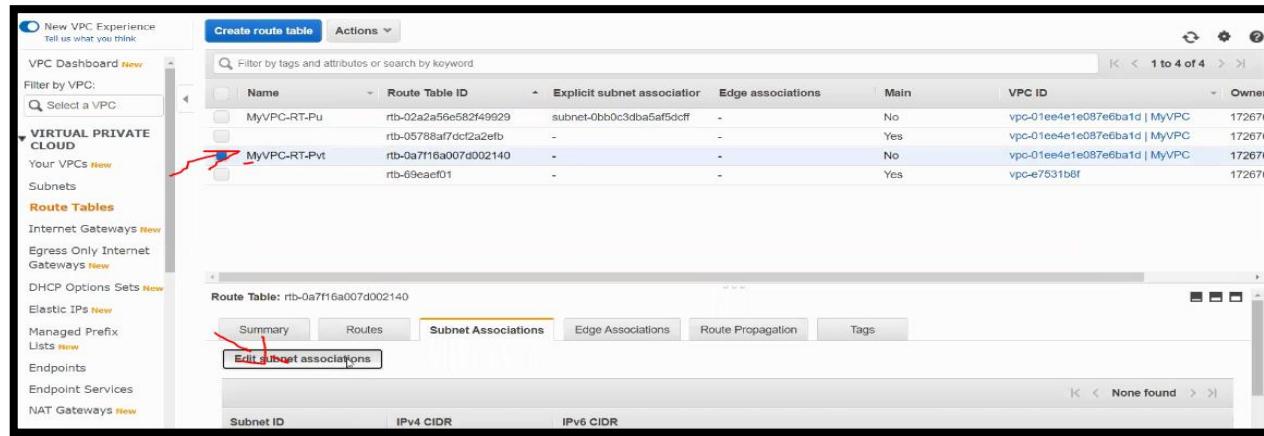
Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
subnet-0bb0c3dba5af5dcff   MyVPC...	10.0.1.0/24	-	Main
subnet-013a2878e0d608ab5   MyVPC...	10.0.2.0/24	-	Main

\* Required

Cancel Save

## Associate Private RT with Private Subnet

### Click Subnet Associations



New VPC Experience  
Tell us what you think

VPC Dashboard [New](#)

Filter by VPC:  
 Select a VPC

**VIRTUAL PRIVATE CLOUD**  
Your VPCs [New](#)

Subnets

**Route Tables**

Internet Gateways [New](#)  
Egress Only Internet Gateways [New](#)  
DHCP Options Sets [New](#)  
Elastic IPs [New](#)  
Managed Prefix Lists [New](#)  
Endpoints  
Endpoint Services  
NAT Gateways [New](#)

Create route table Actions ▾

Filter by tags and attributes or search by keyword

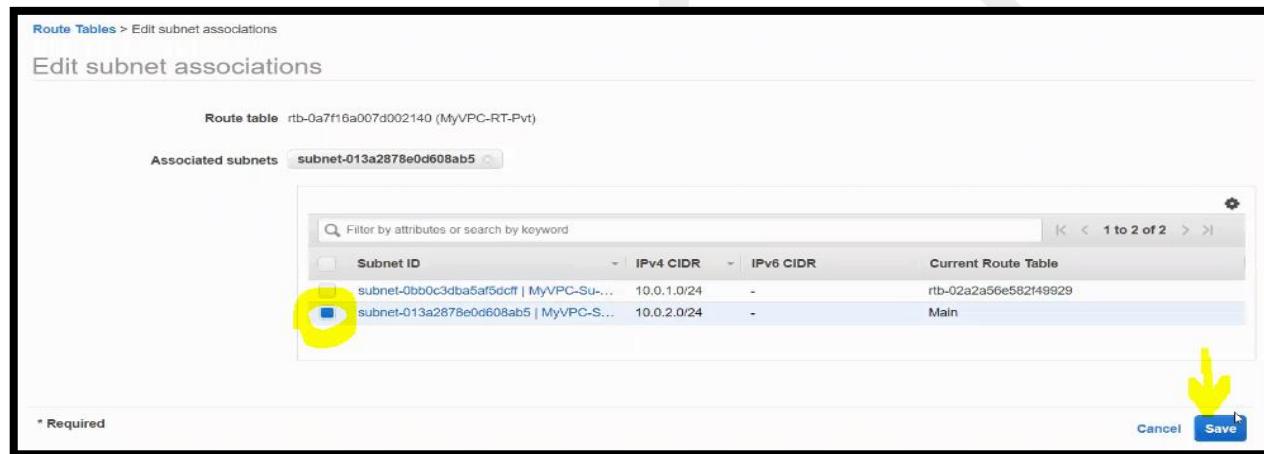
Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
MyVPC-RT-Pu	rtb-02a2a56e582f49929	subnet-0bb0c3dba5af5dcff	-	No	vpc-01ee4e1e087e6ba1d   MyVPC	17267
MyVPC-RT-Pvt	rtb-0a7f16a007d002140	-	-	Yes	vpc-01ee4e1e087e6ba1d   MyVPC	17267
	rtb-69eaef01	-	-	No	vpc-01ee4e1e087e6ba1d   MyVPC	17267
	rtb-69eaef01	-	-	Yes	vpc-e7531b8f	17267

Route Table: rtb-0a7f16a007d002140 (MyVPC-RT-Pvt)

Summary Routes Subnet Associations Edge Associations Route Propagation Tags

Edit subnet associations

None found



Route Tables > Edit subnet associations

Route table rtb-0a7f16a007d002140 (MyVPC-RT-Pvt)

Associated subnets [subnet-013a2878e0d608ab5](#)

Filter by attributes or search by keyword

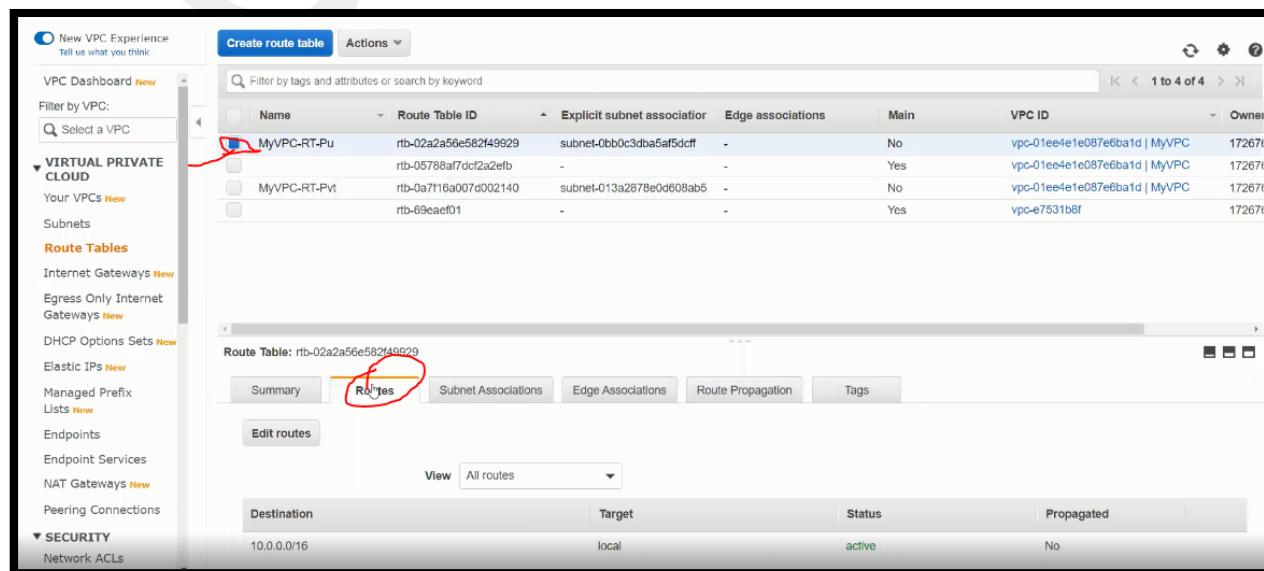
Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
subnet-0bb0c3dba5af5dcff   MyVPC-Su...	10.0.1.0/24	-	rtb-02a2a56e582f49929
subnet-013a2878e0d608ab5   MyVPC-S...	10.0.2.0/24	-	Main

\* Required

Cancel Save

## Step5: Set the Routes to the Public Subnet

### Select Public Subnet and click on routes



New VPC Experience  
Tell us what you think

VPC Dashboard [New](#)

Filter by VPC:  
 Select a VPC

**VIRTUAL PRIVATE CLOUD**  
Your VPCs [New](#)

Subnets

**Route Tables**

Internet Gateways [New](#)  
Egress Only Internet Gateways [New](#)  
DHCP Options Sets [New](#)  
Elastic IPs [New](#)  
Managed Prefix Lists [New](#)  
Endpoints  
Endpoint Services  
NAT Gateways [New](#)  
Peering Connections  
SECURITY  
Network ACLs

Create route table Actions ▾

Filter by tags and attributes or search by keyword

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
MyVPC-RT-Pu	rtb-02a2a56e582f49929	subnet-0bb0c3dba5af5dcff	-	No	vpc-01ee4e1e087e6ba1d   MyVPC	17267
MyVPC-RT-Pvt	rtb-0a7f16a007d002140	subnet-013a2878e0d608ab5	-	No	vpc-01ee4e1e087e6ba1d   MyVPC	17267
	rtb-69eaef01	-	-	Yes	vpc-e7531b8f	17267

Route Table: rtb-02a2a56e582f49929

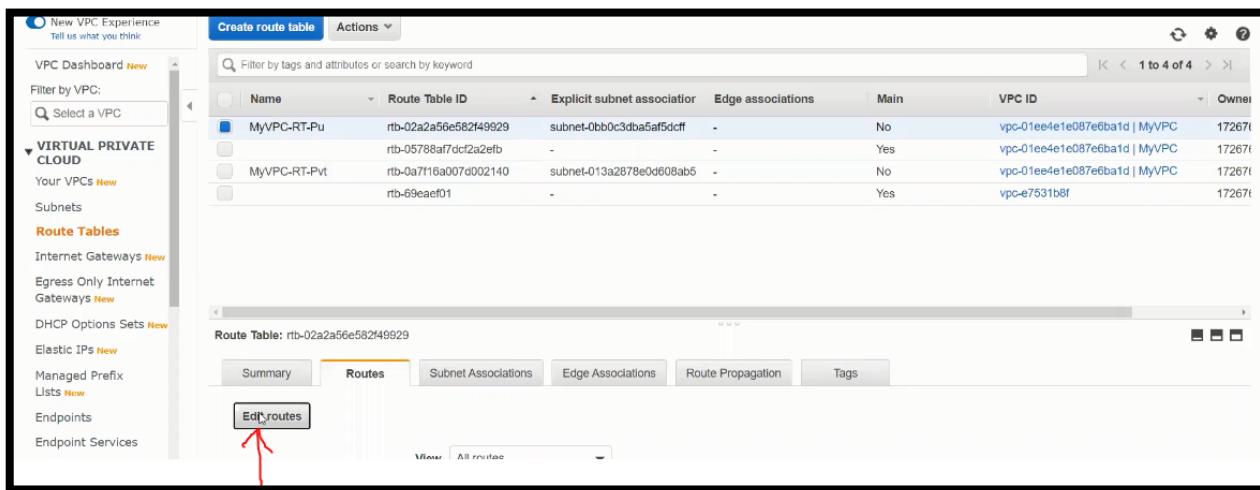
Summary Routes Subnet Associations Edge Associations Route Propagation Tags

Edit routes

View All routes

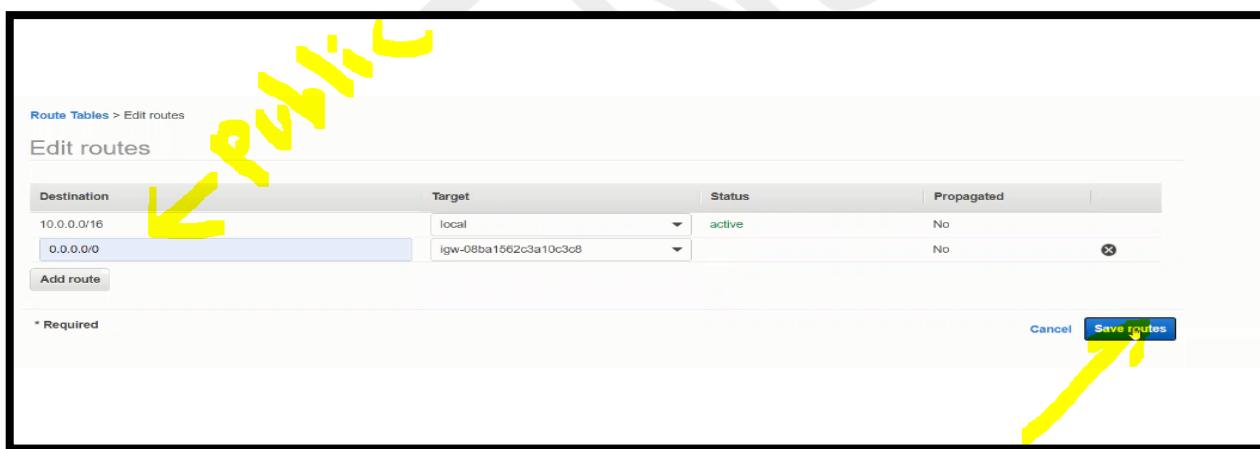
Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No

## Click Edit Routes



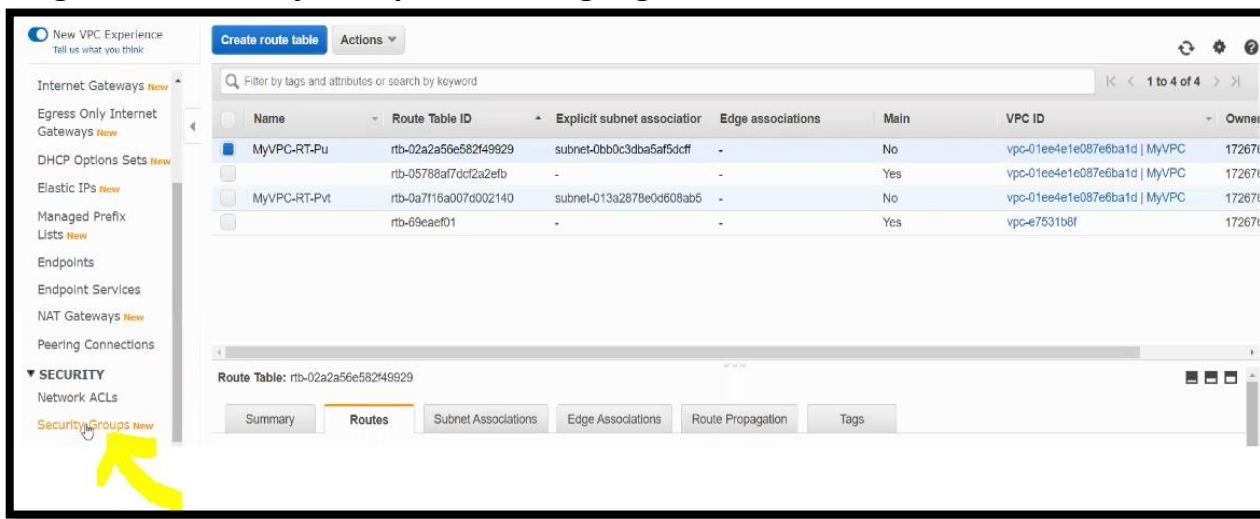
The screenshot shows the AWS VPC Route Tables page. On the left sidebar, under 'Route Tables', the 'Routes' tab is selected. In the main content area, a table lists route tables. The first row, 'MyVPC-RT-Pu', has its 'Edit routes' button highlighted with a red arrow.

**Destination 0.0.0.0/0 indicates can access from anywhere – Public Target – IGW needs to be selected because we are using our own VPC  
Then click Save routes**



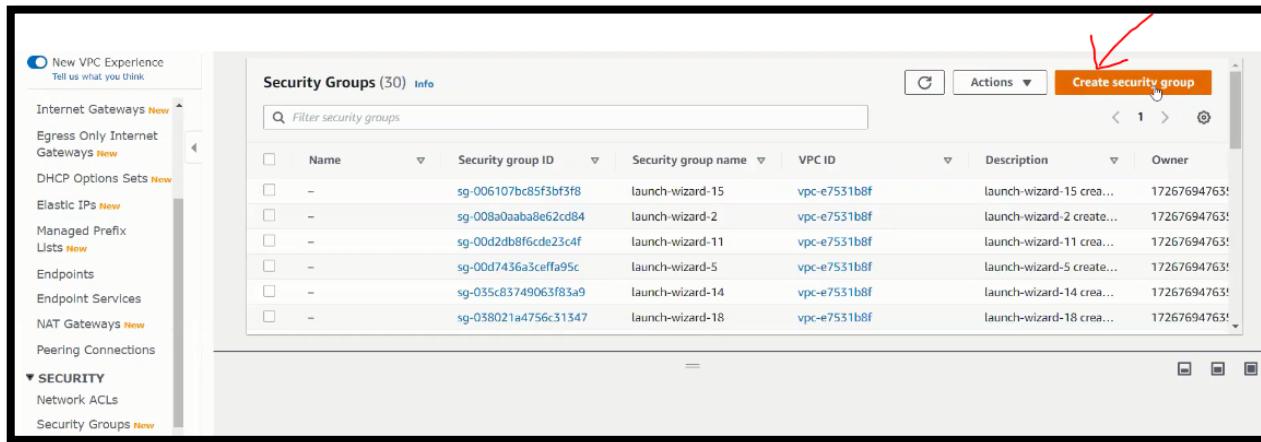
The screenshot shows the 'Edit routes' dialog box. It contains a table with two rows. The first row has 'Destination' as '10.0.0.0/16' and 'Target' as 'local'. The second row has 'Destination' as '0.0.0.0/0' and 'Target' as 'igw-08ba1562c3a10c3c8'. A yellow arrow points to the 'Target' dropdown for the second row. Another yellow arrow points to the 'Save routes' button at the bottom right of the dialog.

**Step6: Create an Public and Private Security Groups  
Single click Security Group module highlighted in Yellow mark**



The screenshot shows the AWS VPC Route Tables page. On the left sidebar, under 'SECURITY', the 'Network ACLs' and 'Security Groups' links are visible. The 'Security Groups' link is highlighted with a yellow arrow. In the main content area, the 'Routes' tab is selected, showing the same route table list as the previous screenshot.

## Click Create Security Group



New VPC Experience Tell us what you think

Internet Gateways New

Egress Only Internet Gateways New

DHCP Options Sets New

Elastic IPs New

Managed Prefix Lists New

Endpoints

Endpoint Services

NAT Gateways New

Peering Connections

**SECURITY**

Network ACLs

Security Groups New

**Security Groups (30) Info**

Filter security groups

Name	Security group ID	Security group name	VPC ID	Description	Owner
-	sg-006107bc85f3bf3fb	launch-wizard-15	vpc-e7531b8f	launch-wizard-15 crea...	17267694763!
-	sg-008a0aabaae62cd84	launch-wizard-2	vpc-e7531b8f	launch-wizard-2 create...	17267694763!
-	sg-00d2db8f6cde23c4f	launch-wizard-11	vpc-e7531b8f	launch-wizard-11 crea...	17267694763!
-	sg-00d7436a3ceffa95c	launch-wizard-5	vpc-e7531b8f	launch-wizard-5 create...	17267694763!
-	sg-035c83749063f83a9	launch-wizard-14	vpc-e7531b8f	launch-wizard-14 crea...	17267694763!
-	sg-038021a4756c31347	launch-wizard-18	vpc-e7531b8f	launch-wizard-18 crea...	17267694763!

## Create Public Security Group:

Tag Understandable Public SG name, keep the same in Description

Choose our own VPC

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  
MyVPC-SG-Pu  
Name cannot be edited after creation.

Description Info  
MyVPC-SG-Pu

VPC Info  
vpc-01ee4e1e087e6ba1d (MyVPC)

**Inbound rules** Info

This security group has no inbound rules.

Add rule

**Outbound rules** Info

Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Destination <small>Info</small>	Description - optional <small>Info</small>
All traffic	All	All	Custom	0.0.0.0/0

Add rule

**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.

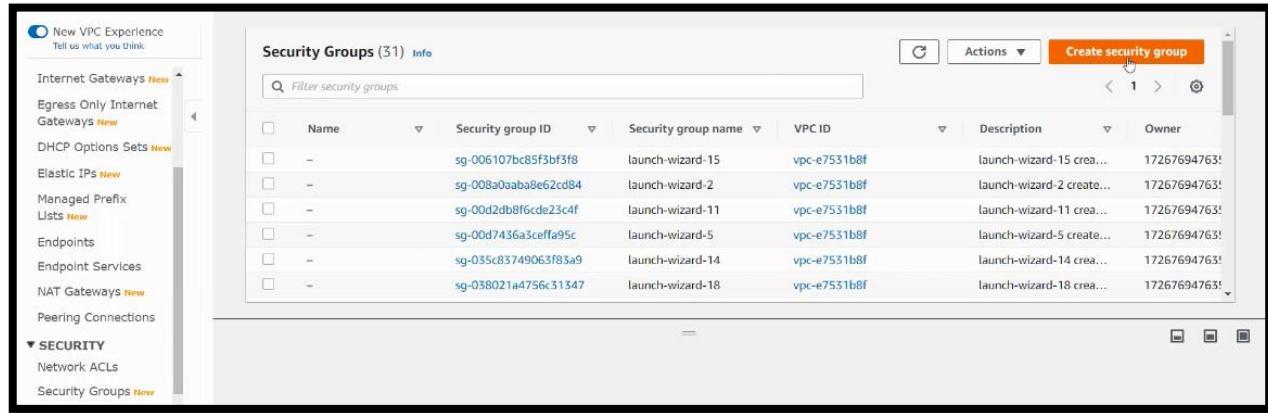
Add new tag

You can add up to 50 more tag

Cancel **Create security group**

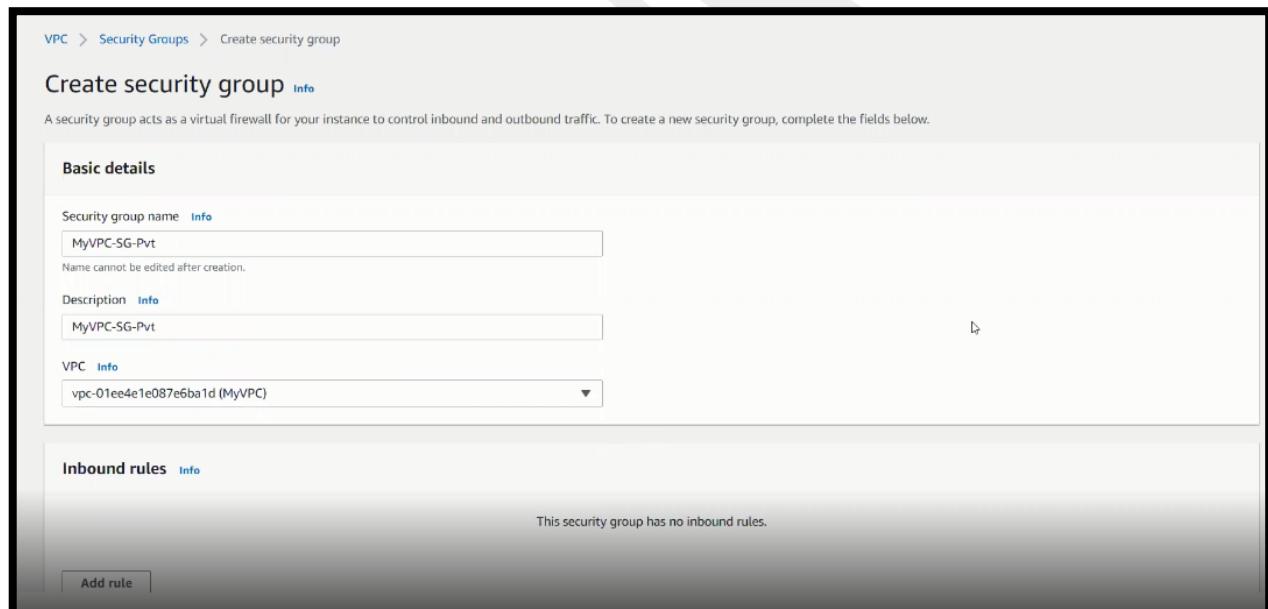
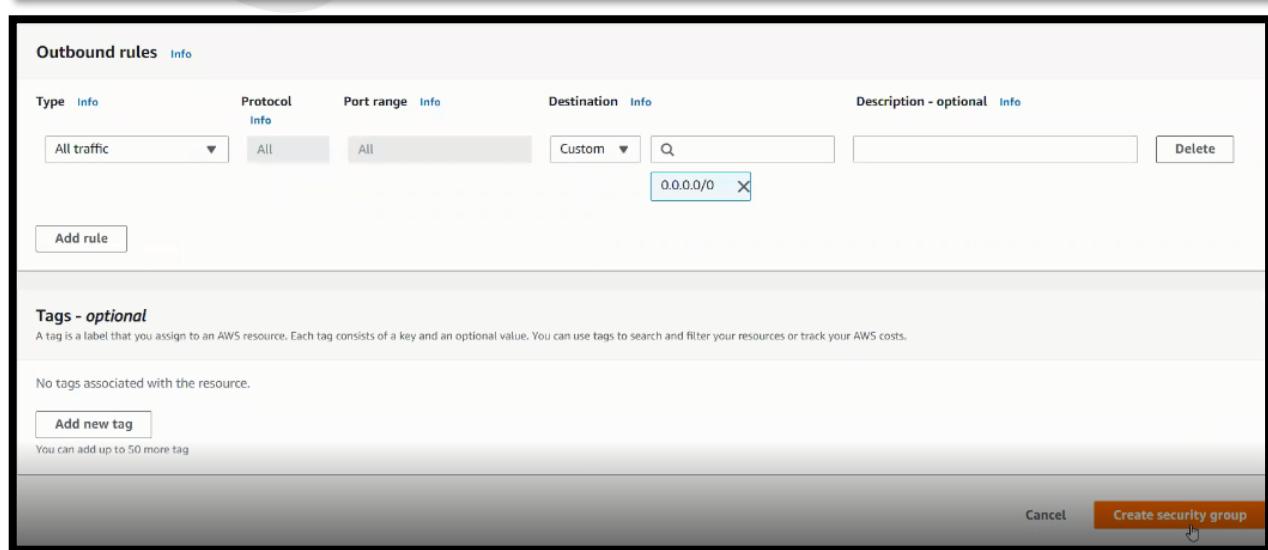
**Note: Once Click on Create Security Group, Public SG will be created**

## Create a Private Security Group



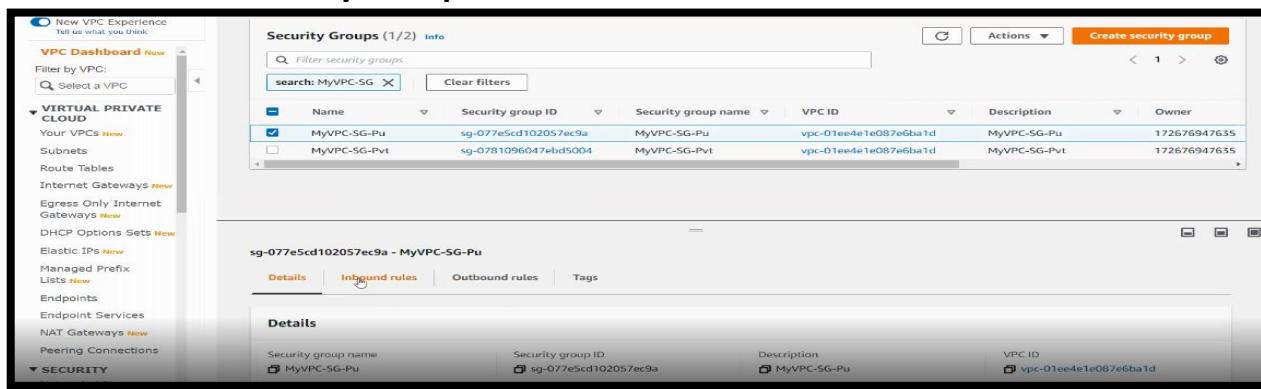
**Name the Understandable Private SG name, keep the same in Description**

**Choose our own VPC**

**Note: Once Click on Create Security Group, Private SG will be created**

## Choose Public Security Group and Edit Inbound Rules



**Security Groups (1/2) Info**

Name	Security group ID	Security group name	VPC ID	Description	Owner
<input checked="" type="checkbox"/> MyVPC-SG-Pu	sg-077e5cd102057ec9a	MyVPC-SG-Pu	vpc-01ee4e1e087e6ba1d	MyVPC-SG-Pu	172676947635
<input type="checkbox"/> MyVPC-SG-Pvt	sg-0781096047ebd5004	MyVPC-SG-Pvt	vpc-01ee4e1e087e6ba1d	MyVPC-SG-Pvt	172676947635

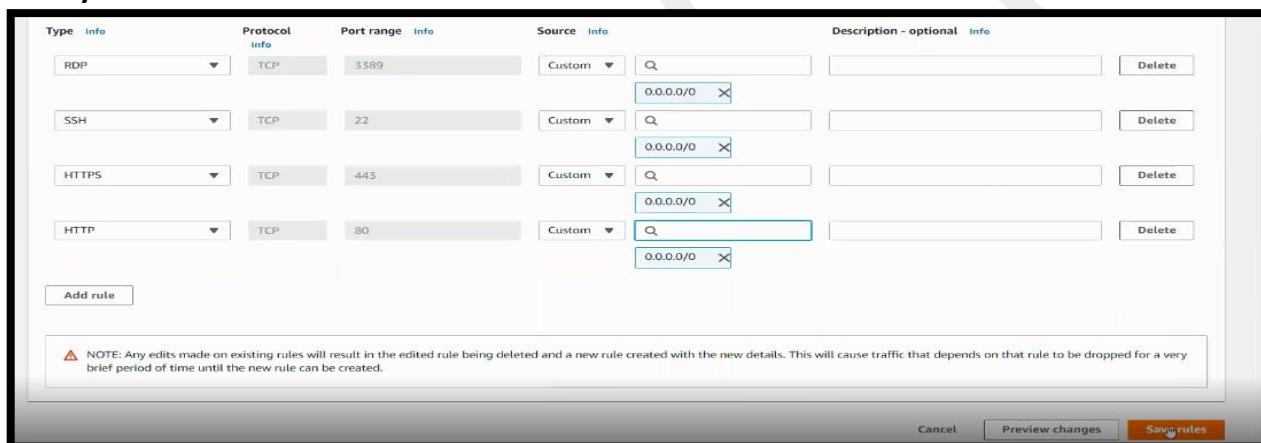
**sg-077e5cd102057ec9a - MyVPC-SG-Pu**

**Inbound rules**

Type	Protocol	Port range	Source	Description - optional
RDP	TCP	5389	Custom	0.0.0.0/0
SSH	TCP	22	Custom	0.0.0.0/0
HTTPS	TCP	443	Custom	0.0.0.0/0
HTTP	TCP	80	Custom	0.0.0.0/0

Add Firewalls RDP, SSH, HTTP and HTTPS; Source can be Public hence choose 0.0.0.0/0

Finally click on save rules



**Inbound security group rules successfully modified on security group (sg-077e5cd102057ec9a | MyVPC-SG-Pu)**

**Details**

**sg-077e5cd102057ec9a - MyVPC-SG-Pu**

**Inbound rules**

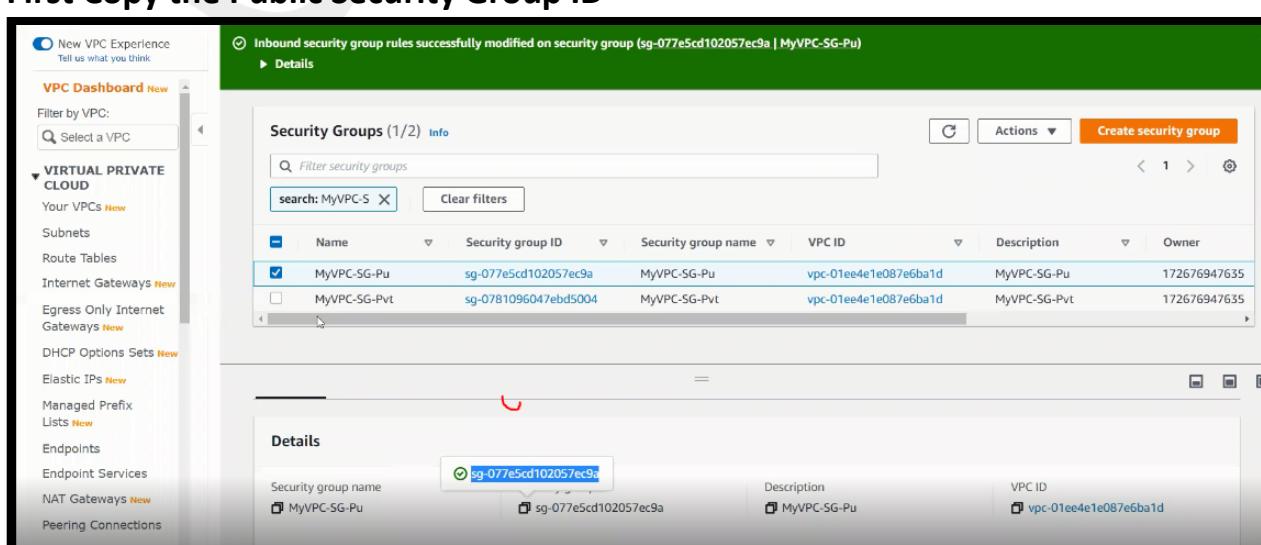
Type	Protocol	Port range	Source	Description - optional
RDP	TCP	5389	Custom	0.0.0.0/0
SSH	TCP	22	Custom	0.0.0.0/0
HTTPS	TCP	443	Custom	0.0.0.0/0
HTTP	TCP	80	Custom	0.0.0.0/0

**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.

**Sav**

Choose private Security Group and Edit Inbound Rules

First Copy the Public Security Group ID



**Security Groups (1/2) Info**

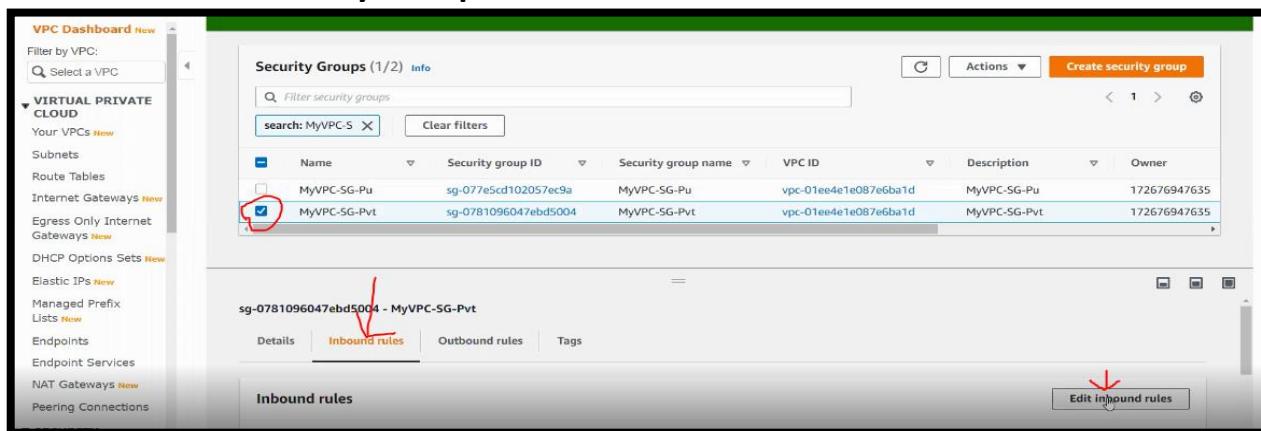
Name	Security group ID	Security group name	VPC ID	Description	Owner
<input checked="" type="checkbox"/> MyVPC-SG-Pu	sg-077e5cd102057ec9a	MyVPC-SG-Pu	vpc-01ee4e1e087e6ba1d	MyVPC-SG-Pu	172676947635
<input type="checkbox"/> MyVPC-SG-Pvt	sg-0781096047ebd5004	MyVPC-SG-Pvt	vpc-01ee4e1e087e6ba1d	MyVPC-SG-Pvt	172676947635

**sg-077e5cd102057ec9a - MyVPC-SG-Pu**

**Inbound rules**

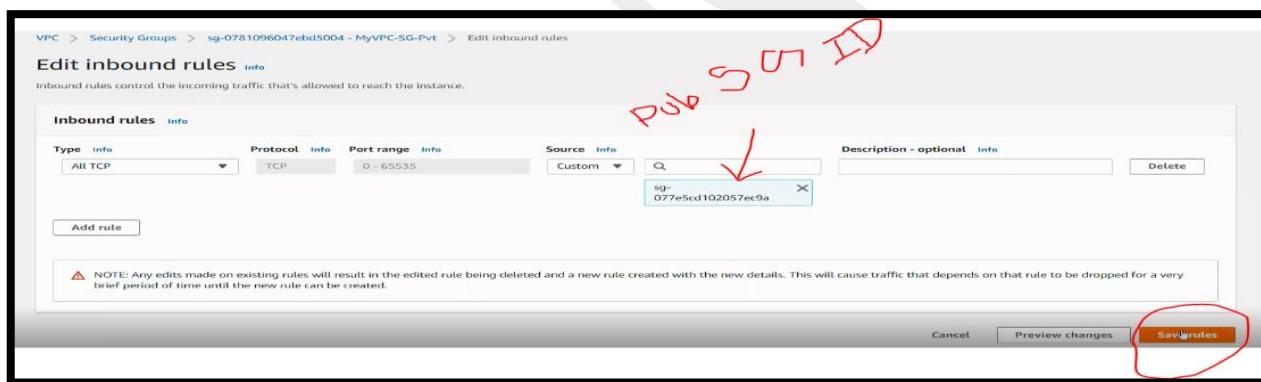
Type	Protocol	Port range	Source	Description - optional
RDP	TCP	5389	Custom	0.0.0.0/0
SSH	TCP	22	Custom	0.0.0.0/0
HTTPS	TCP	443	Custom	0.0.0.0/0
HTTP	TCP	80	Custom	0.0.0.0/0

## Choose Private Security Group and Edit Inbound Rules



The screenshot shows the AWS VPC Dashboard with the 'Security Groups' section open. Two security groups are listed: 'MyVPC-SG-Pu' and 'MyVPC-SG-Pvt'. The 'MyVPC-SG-Pvt' group is selected, indicated by a checked checkbox. Below the table, there are tabs for 'Details', 'Inbound rules' (which is highlighted with a red arrow), 'Outbound rules', and 'Tags'. At the bottom right of the 'Inbound rules' section, there is a prominent 'Edit inbound rules' button.

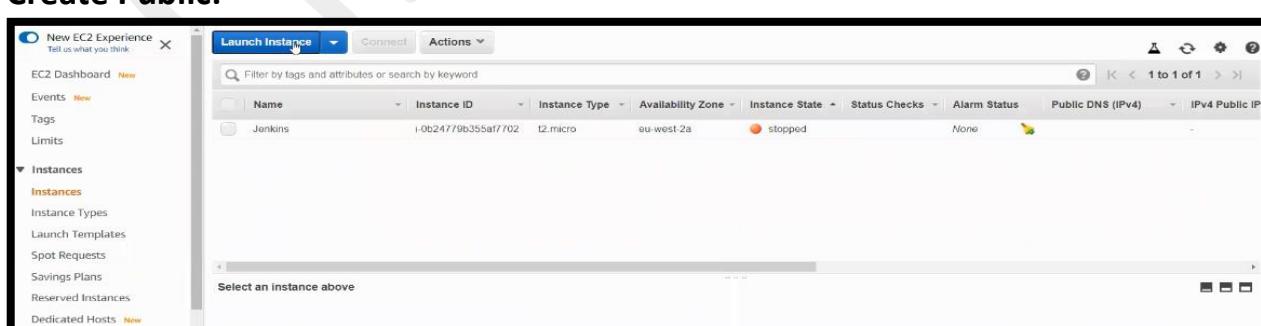
## Choose All TCP (0-65535) ports; Paste Public Security Group ID in Source then Save Rules



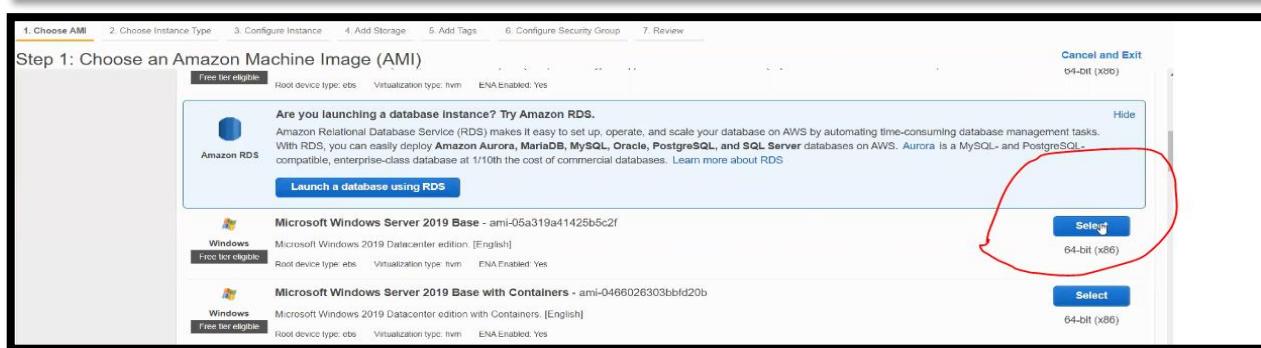
This screenshot shows the 'Edit inbound rules' interface for the 'MyVPC-SG-Pvt' security group. In the 'Source' dropdown, the public security group ID 'sg-077e5cd102057ec9a' is selected. A red arrow points from the text above to this dropdown. At the bottom right of the screen, there is a large red circle around the 'Save rules' button.

## Step7: Create an Public and Private Windows Instances

### Create Public:



The screenshot shows the AWS EC2 Dashboard with the 'Launch Instance' button highlighted. Below the button, a table lists existing instances, including one named 'Jenkins'.



This screenshot shows the 'Step 1: Choose an Amazon Machine Image (AMI)' screen. It lists several AMI options, including 'Microsoft Windows Server 2019 Base' and 'Microsoft Windows Server 2019 Base with Containers'. For each option, there is a 'Select' button and a '64-bit (x86)' link. A large red circle highlights the 'Select' button for the first option.

**Step 2: Choose an Instance Type**

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by: All instance types Current generation Show/Hide Columns

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
General purpose	<b>t2.micro</b> <small>(Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)</small>	<b>1</b>	<b>1</b>	<b>EBS only</b>	<b>-</b>	<b>Low to Moderate</b>	<b>Yes</b>
General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
General purpose	t3a.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

## Select Own VPC, Public Subnet and Enable Auto-assign Public Ip

**Step 3: Configure Instance Details**

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot Instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of Instances	1	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot Instances	
Network	vpc-01ee4e1e087e6ba1d   MyVPC	<input checked="" type="radio"/> Create new VPC
Subnet	subnet-0bb0c3ba5af5ddff   MyVPC-Su-Pu   eu-west-1	<input type="radio"/> Create new subnet 251 IP Addresses available
Auto-assign Public IP	Enable	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	Open	
Domain join directory	No directory	<input checked="" type="radio"/> Create new directory
IAM role	None	<input checked="" type="radio"/> Create new IAM role
Shutdown behavior	Stop	
Stop - Hibernate behavior	<input type="checkbox"/> Enable hibernation as an additional stop behavior	
Enable termination protection	<input type="checkbox"/> Protect against accidental termination	

Cancel Previous Review and Launch Next: Add Storage

**Step 4: Add Storage**

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (Mbps)	Delete on Termination	Encryption
Root	/dev/sda1	anap-02f4ab8b021f34725	30	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

Cancel Previous Review and Launch Next: Add Tags

**Step 5: Add Tags**

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key	Value	Instances	Volumes
Name	EC2Pub	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add another tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group

## Select existing Public Security Group

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group **7. Review**

**Step 6: Configure Security Group**  
A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group:  Create a new security group  Select an existing security group

Security Group ID	Name	Description	Actions
sg-0d593abf24d48c11	default	default VPC security group	<a href="#">Copy to new</a>
sg-077e5cd102057ec9a	MyVPC-SG-Pu	MyVPC-SG-Pu	<a href="#">Copy to new</a>
sg-0781096047ebd5004	MyVPC-SG-Pvt	MyVPC-SG-Pvt	<a href="#">Copy to new</a>

Inbound rules for sg-077e5cd102057ec9a (Selected security groups: sg-077e5cd102057ec9a)

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	
SSH	TCP	22	0.0.0.0/0	
RDP	TCP	3389	0.0.0.0/0	
HTTPS	TCP	443	0.0.0.0/0	

[Cancel](#) [Previous](#) [Review and Launch](#)

## Create a pem file – Encrypted Private Key file in .pem format

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group **7. Review**

**Step 7: Review Instance Launch**  
Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

**Select an existing key pair or create a new key pair**

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Create a new key pair  
Key pair name: Myvpc077d  
[Download Key Pair](#)

You have to download the **private key file** (\*.pem file) before you can continue. [Store it in a secure and accessible location](#). You will not be able to download the file again after it's created.

[Cancel](#) [Launch Instances](#)

## Instance Creation started

**Launch Status**

Get notified of estimated charges  
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances  
Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.  
Click [View Instances](#) to monitor your instances' status. Once your instances are in the **running** state, you can [connect](#) to them from the instances screen. Find out how to connect to your instances.

Here are some helpful resources to get you started

- How to connect to your Windows instance
- Learn about AWS Free Usage Tier
- Amazon EC2: User Guide
- Amazon EC2: Microsoft Windows Guide
- Amazon EC2: Discussion Forum

While your instances are launching you can also

- Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)
- Create and attach additional EBS volumes. (Additional charges may apply)
- Manage security groups

[View Instances](#)

New EC2 Experience Tell us what you think

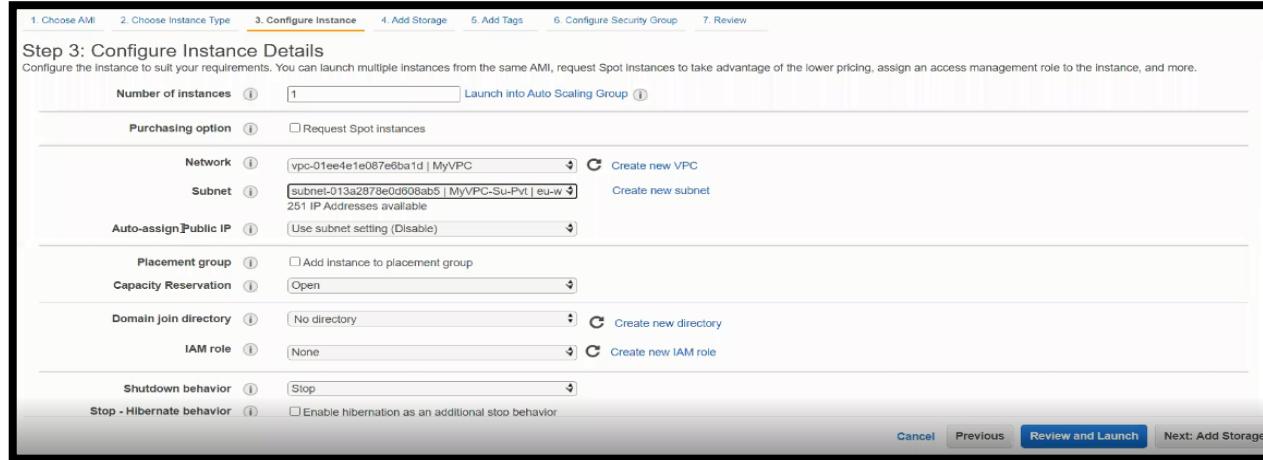
Launch Instance Connect Actions

Filter by tags and attributes or search by keyword

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
ECPub	i-0163770b1bb629011	t2.micro	eu-west-2a	pending	Initializing	None	3.10.234.197	-
Jenkins	i-0b24779b35af7702	t2.micro	eu-west-2a	stopped	None	-	-	-

Select an instance above

**Except Step3, 4 and 6 rest all are similar where we created the Public instance  
Select Own VPC, Private Subnet but Auto-assign Public IP should be disabled  
Then only we can give rights to access Private Machine only through Public**



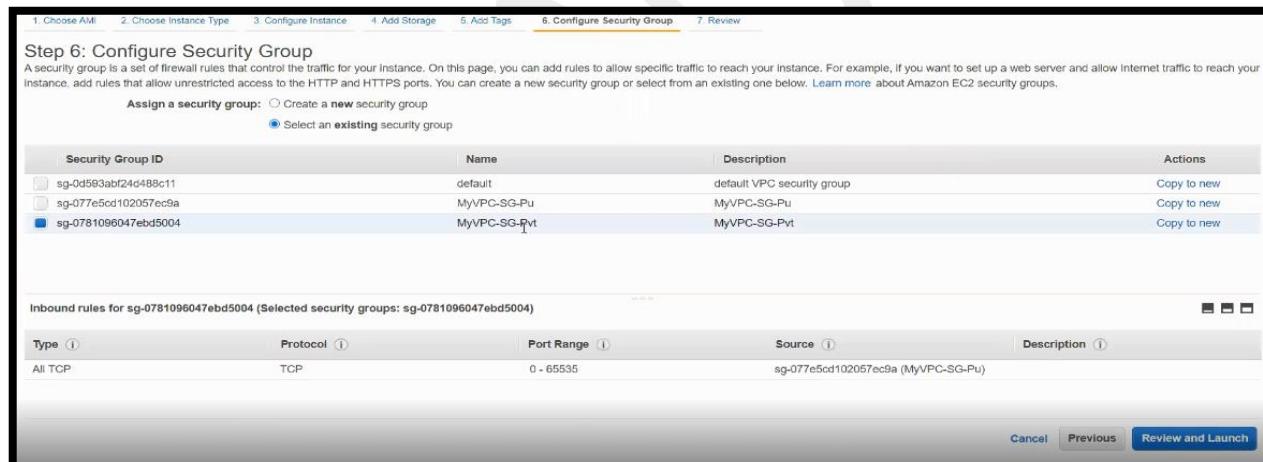
The screenshot shows the 'Configure Instance Details' step of the AWS EC2 instance creation wizard. Key settings include:

- Number of instances:** 1
- Purchasing option:** Request Spot Instances
- Network:** vpc-01ee4e1e087e6ba1d | MyVPC
- Subnet:** subnet-013a2878e0d608ab5 | MyVPC-Su-Pvt | eu-west-1
- Auto-assign Public IP:** Use subnet setting (Disable)
- Placement group:** None
- Capacity Reservation:** Open
- Domain join directory:** No directory
- IAM role:** None
- Shutdown behavior:** Stop
- Stop - Hibernate behavior:** None

Buttons at the bottom include: Cancel, Previous, Review and Launch, and Next: Add Storage.

## Step4 Tag Name could be different

### Select Private Security Group and create instance with existing pem



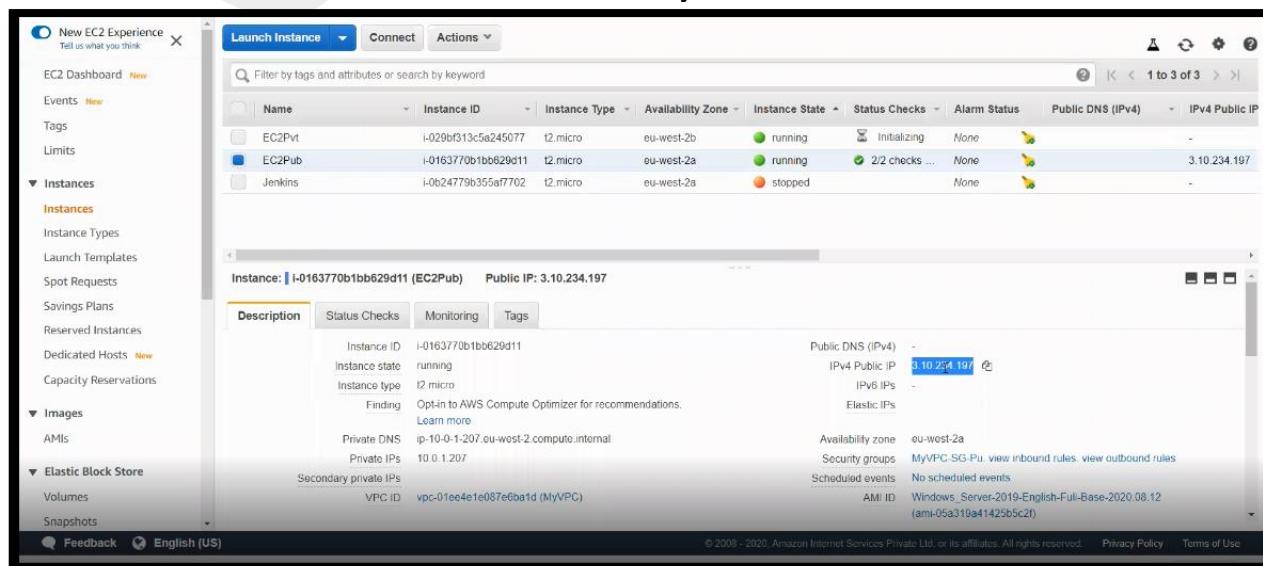
The screenshot shows the 'Configure Security Group' step of the AWS EC2 instance creation wizard. Key settings include:

- Assign a security group:** Select an existing security group (MyVPC-SG-Pvt is selected)
- Security Group ID:** sg-0781096047ebd5004
- Inbound rules for sg-0781096047ebd5004 (Selected security groups: sg-0781096047ebd5004):**

Type	Protocol	Port Range	Source	Description
All TCP	TCP	0 - 65535	sg-077e5cd102057ec9a (MyVPC-SG-Pu)	

Buttons at the bottom include: Cancel, Previous, Review and Launch.

## Two instances has been created successfully



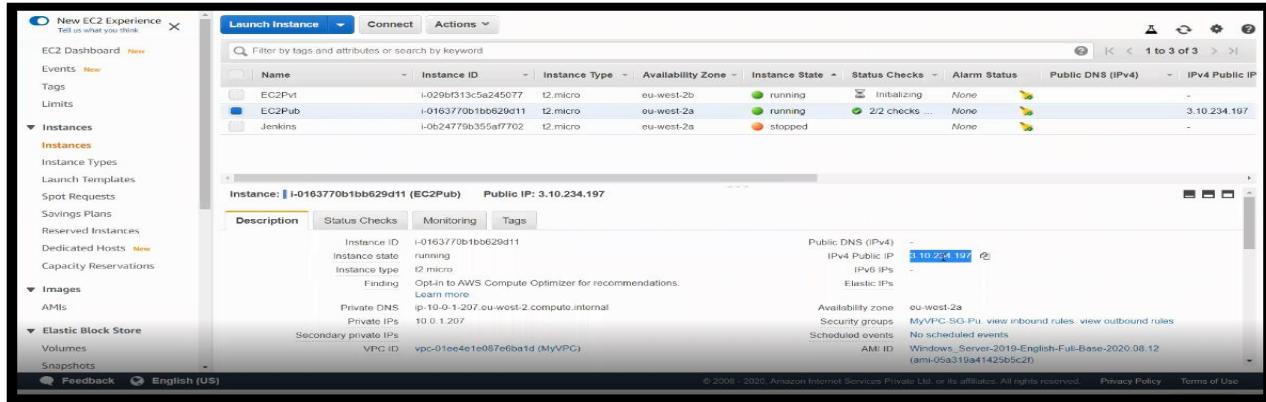
The screenshot shows the AWS EC2 Instances page. Two instances are listed:

- EC2Pub:** Instance ID: i-0163770b1bb629d11, Public IP: 3.10.234.197, Status: running, Instance Type: t2.micro, Availability Zone: eu-west-2a
- Jenkins:** Instance ID: i-0b24779b355a7702, Public IP: -, Status: stopped, Instance Type: t2.micro, Availability Zone: eu-west-2a

Details for EC2Pub:

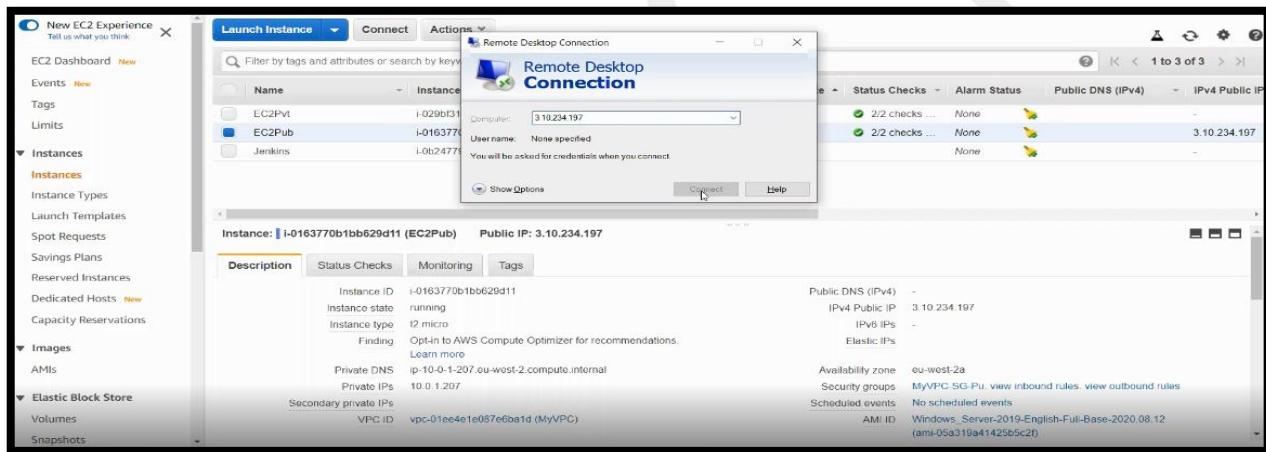
Description	Value
Instance ID	i-0163770b1bb629d11
Instance state	running
Instance type	t2.micro
Finding	Opt-in to AWS Compute Optimizer for recommendations.
Private DNS	ip-10-0-1-207.eu-west-2.compute.internal
Private IPs	10.0.1.207
Secondary private IPs	vpc-01ee4e1e087e6ba1d (MyVPC)
Public DNS (IPv4)	-
IPv4 Public IP	3.10.234.197
IPv6 IPs	-
Elastic IPs	-
Availability zone	eu-west-2a
Security groups	MyVPC-SG-Pu, view inbound rules, view outbound rules
Scheduled events	No scheduled events
AMI ID	Windows_Server-2019-English-Full-Base-2020.08.12 (ami-05a319841425b5c2f)

## Login Public Machine and Test Internet Availability Get the Public Ip



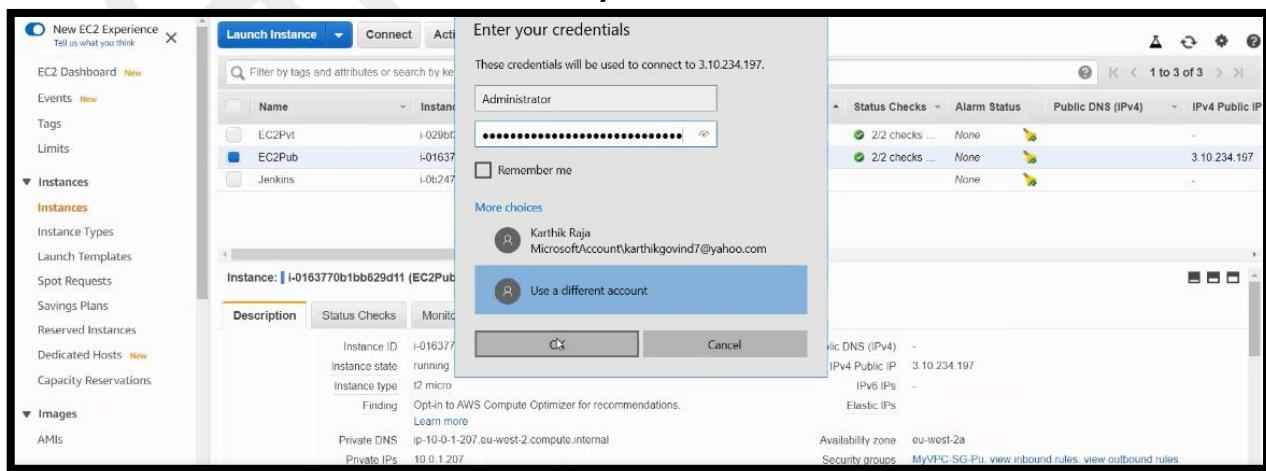
The screenshot shows the AWS EC2 Instances page. It lists two instances: EC2Pvt and EC2Pub. EC2Pub is selected. Its details are shown in the center pane, including its Public IP (3.10.234.197). The status bar at the bottom right indicates the Public DNS (IPv4) is 3.10.234.197.

## In the Window start, Select Remote Desktop Connection Pass on Public IP as a Parameter



The screenshot shows the AWS EC2 Instances page with the Remote Desktop Connection window overlaid. The Public IP 3.10.234.197 is entered in the 'Computer' field of the RDP window. The status bar at the bottom right indicates the Public DNS (IPv4) is 3.10.234.197.

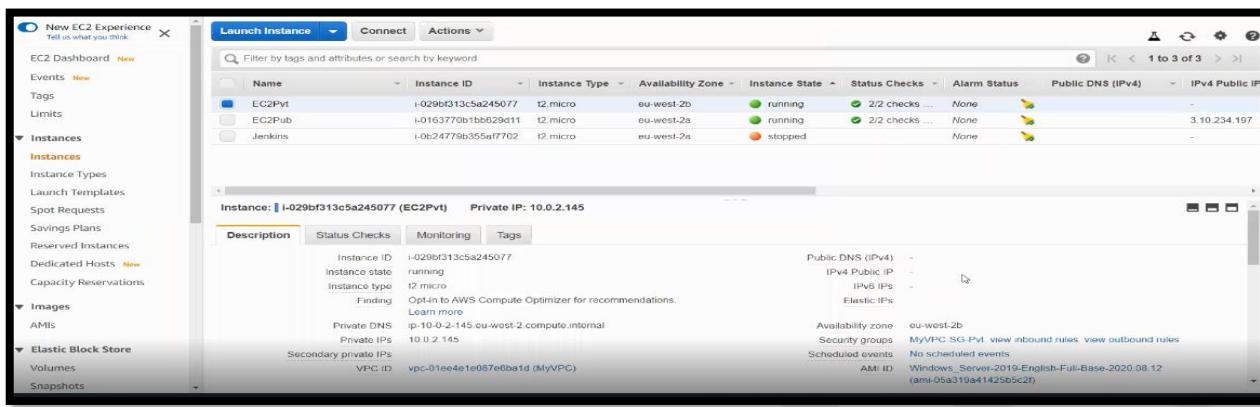
## Get the User name and Password and pass like below



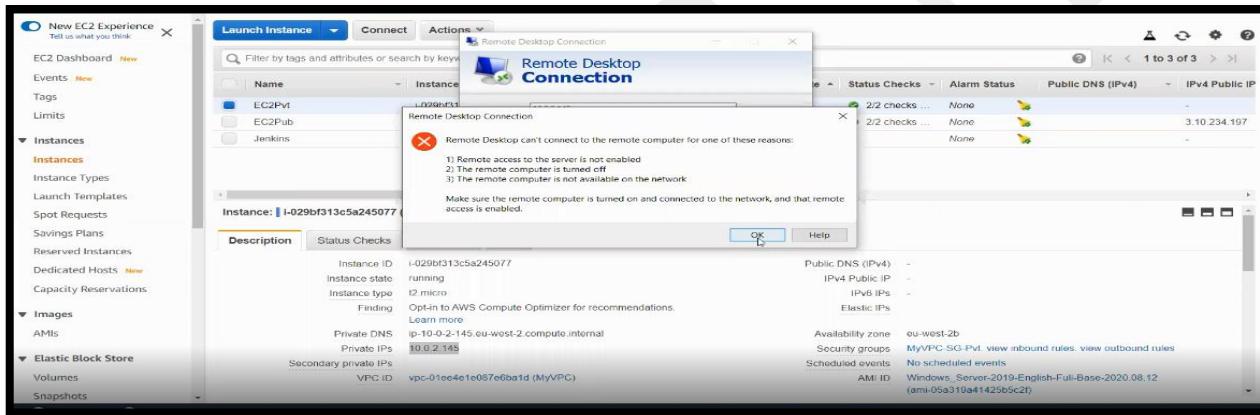
The screenshot shows the AWS EC2 Instances page with the 'Enter your credentials' dialog open. The 'Administrator' user is selected, and the password is masked. The status bar at the bottom right indicates the Public DNS (IPv4) is 3.10.234.197.

Once VM loaded check the Internet availability at the right bottom corner

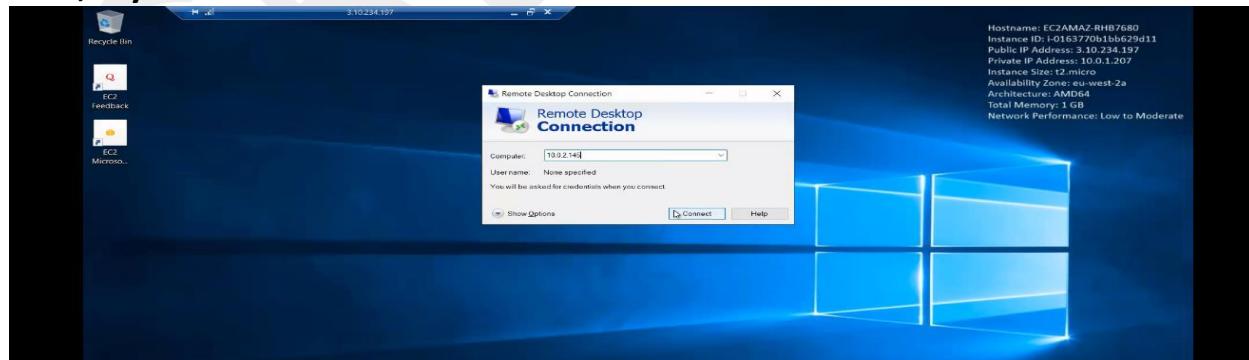
## Private machine Doesn't have Public IP



## Try to connect Private Machine from Local PC



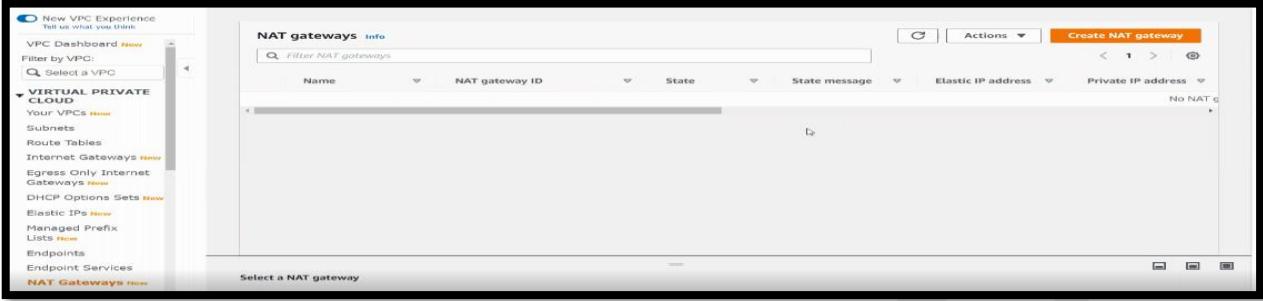
## Now, Try to connect same Private Machine via Public Machine



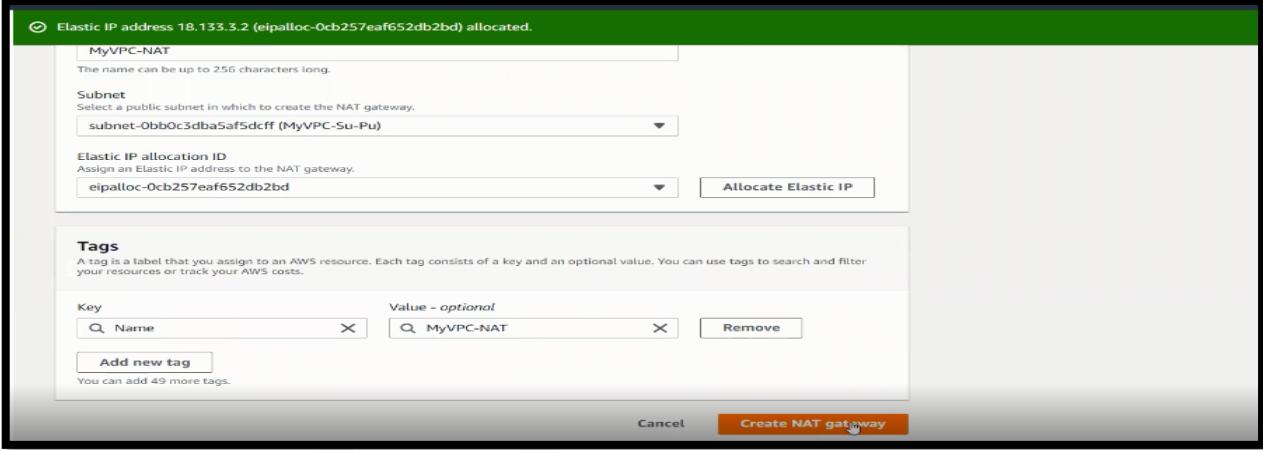

**Note:** In the Private Machine Internet will not be available

**Solution:** Need to Create NAT Gateways, Connect to Public Subnet also connect with RT

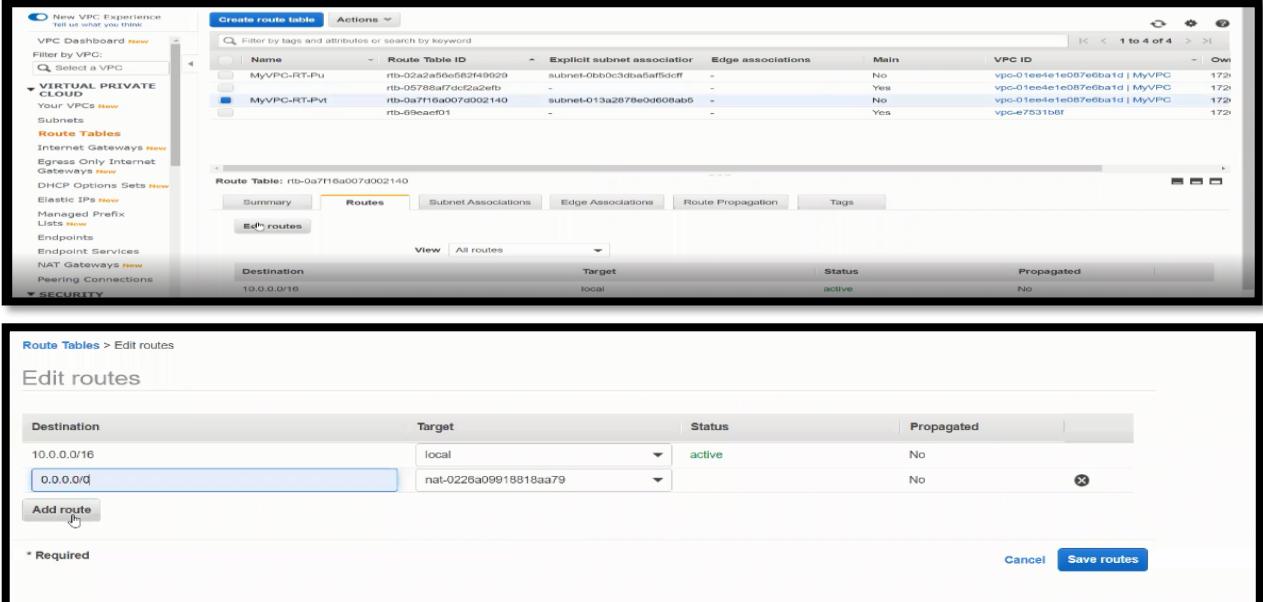
## Create an NAT Gateway



## Pass all parameters properly, Create Static ip



## In Private RT, associate with NAT Gateways



**NOTE: Private machine now has Internet facility.**

**Demolish:**

- >Delete EC2 Machines
- Delete NAT Gateway
- Delete VPC
- Delete Elastic IP

**Assignment:** Create an Amazon Linux instances and check the same.