

Table of contents

- [Table of contents](#)
- [Introduction to Public subnet and Private subnet :](#)
 - [How to differentiate between a public subnet and private subnet](#)
 - [Public Subnet](#)
 - [Private subnet](#)
 - [Creating private subnet](#)
 - [How to access instances in private subnet i.e. which only have a private ip address](#)
 - [NAT gateway](#)
 - [Creating and using a NAT gateway](#)
 - [Points to consider](#)

Introduction to Public subnet and Private subnet :

- Now that we can create VPC,subnets ,route tables ,IGW and NACL, we'll see how do we differentiate between public subnet and private subnet .
- Agenda for today we'll be understanding the subnet , NAT and VPC endpoint

How to differentiate between a public subnet and private subnet

Public Subnet

- The Public subnet hosts EC2 instances having public ip addresses .
- Since the instances are expected to have public ip ,generally the "**auto-assign public ip**" will be marked as **Yes**
- Also in order to reach the instances having public ip , we need IGW . This basically translates to having a route table attached to the subnet which must have a route to IGW.
- So 2 properties using which we can identify a public subnet is
 - "Auto assign public ip " setting to be turned to Yes
 - Subnet should have a route table assigned which should have a route to IGW
 - Now we can conclude , all the default subnets created under default VPC are public subnets.

Private subnet

- Private subnet hosts instances which will only have private ip address .
- Naturally the "**auto assign public ip**" setting is kept as **No**
- Since the instances do not have public ip , they cannot utilize the IGW anyways . Hence a subnet has to have a separate route table which does not have IGW associated with it.
- 2 properties which define a private subnet
 - "Auto assign public ip " setting to be turned to No
 - Subnet should have a separate route table assigned which does not have a route to IGW

Creating private subnet

- We have already seen how to create a public subnet when we were replicating the default subnet under default VPC .

- Let us now create a private subnet
- Create a VPC create a subnet under the same
- Once created , click on subnet , go to actions and click on "modify auto-assign IP settings "

[Subnets](#) > Modify auto-assign IP settings

Modify auto-assign IP settings

Enable the auto-assign IP address setting to automatically request a public IPv4 or IPv6 address for an instance launched in this subnet. You can override the auto-assign IP settings for an instance at launch time.

Subnet ID subnet-0390ad276de3e544c

Auto-assign IPv4 ☐ Enable auto-assign public IPv4 address ⓘ

Auto-assign Co-IP ☐ Enable auto-assign customer-owned IPv4 address ⓘ

* Required

[Cancel](#) [Save](#)

- Make sure the "Enable auto-assign public IPv4 address" is unticked like above .
- Now that we have enabled the 1st setting let us move to the 2nd criteria
- We need to create a separate route table which needs to be associated with the subnet
- Navigate to route table and click on create route table

[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 private-RT ⓘ

VPC* vpc-0a0152fbfb1aaecc7 ⓘ

Key (128 characters maximum)

Value (256 characters maximum)

This resource currently has no tags

[Add Tag](#) 50 remaining (Up to 50 tags maximum)

* Required

[Cancel](#) [Create](#)

- Provide a name for Route table and select the VPC as above and click on create route table .
- Once the route table is created , click on the created route table and navigate to subnet associations

☒ New VPC Experience
Tell us what you think

[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
private-RT	rtb-0acda69fea5072d27	-	-	No	vpc-0a0152fbfb1aaecc7 ...	384395217903

Route Table: rtb-0acda69fea5072d27

[Summary](#) [Routes](#) [Subnet Associations](#) [Edge Associations](#) [Route Propagation](#) [Tags](#)

[Edit subnet associations](#)

Subnet ID	IPv4 CIDR	IPv6 CIDR
None found		

You do not have any subnet associations.

- click on edit subnet associations , check the private subnet and click on save .

The screenshot shows the AWS Management Console interface for a Route Table. At the top, there's a search bar and navigation links. Below, a table lists route tables. The 'private-RT' is selected, showing its details. The 'Subnet Associations' tab is active, displaying a table with one association to 'subnet-07de0a69061ab2dd9' with an IPv4 CIDR of '10.0.0.16/28'.

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
private-RT	rtb-0acda69fea5072d27	subnet-07de0a69061ab2dd9	-	No	vpc-0a0152fbfb1aaecc7 ...	384395217903

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-07de0a69061ab2d...	10.0.0.16/28	-

- Since this route table by default does not have an IGW attached , and is attached to our subnet . This fulfills our second criteria of private subnet .
- All the instances launched in this subnet will not have a public ip as well as they will not have internet access from and to the instances.

How to access instances in private subnet i.e. which only have a private ip address

- We have seen till now that private ip addresses can only be accessed from within a network
- Since our VPC is a network , this can provide us a way to connect to our instances .
- In order to achieve this , we need to have a VPC with one public subnet and one private subnet .
- Launch 1 EC2 instance in each subnet so that we will have 2 instances in total. Make sure you use different security group for each.
- We will refer the instance launched in public subnet as public instance and similarly instance launched in the private subnet will be termed as private instance.
- The pem key which we have assigned to our private instance need to be copied on the public instance
 - Note : You can upload the key in any S3 bucket , use an IAM role to copy the file on the public instance
- Now the goal here is to access the private instance using public instance
- Login to public instance and use below command

```
ssh -i keyname.pem ec2-user@private-ip-address-of-private-instance
```

- If you receive **bad permissions** error then perform below command and try again

```
sudo chmod 400 keyname.pem
```

- There will be a connection timed out error now. in order to resolve it , it the security group of private instance , add a rule granting ssh access from private ip of public instance .
- Once this is setup try again and it should work .

NAT gateway

- Once we are connected to the private instance, let us check if we have internet connectivity from the instance

```
ping www.google.com
```

- Since we do not have a route table which has an IGW , we will not be having internet connectivity and above command will fail
- NAT gateway stands for Network Address Translation , it is basically used for bringing internet to instances which do not have public ip address .

Creating and using a NAT gateway

- Navigate to "NAT gateways" in VPC
- Click on "Create NAT gateway"
- Name the NAT gateway
- In the subnet tab select the ****Public subnet****
- Reason for selecting public subnet is , NAT gateway relies on IGW to bring internet . Since public subnet has access to IGW , we need to create NAT in public subnet
- Click on allocate Elastic Ip . This creates a elastic ip which will be associated to our NAT . We need a static public IP because without a public IP IGW cannot get us internet . Hence we require a EIP

aws Services krupal

✓ Elastic IP address 34.226.15.17 (eipalloc-0070f897173eaa69d) allocated.

VPC > NAT gateways > Create NAT gateway

Create NAT gateway [Info](#)

Create a NAT gateway and assign it an Elastic IP address.

NAT gateway settings

Name - optional
Create a tag with a key of 'Name' and a value that you specify.

my-NAT

The name can be up to 256 characters long.

Subnet
Select a public subnet in which to create the NAT gateway.

subnet-0390ad276de3e544c (subnet-A)

Elastic IP allocation ID
Assign an Elastic IP address to the NAT gateway.

eipalloc-0070f897173eaa69d

[Allocate Elastic IP](#)

Tags

- Click on create NAT gateway
- Wait for the NAT gateway to become available

NAT gateways (1/1) [Info](#)

Filter NAT gateways

VPC: vpc-0a0152fbfb1aaecc7 [Clear filters](#)

Name	NAT gateway ID	State	State message	Elastic IP address	Private IP address
my-NAT	nat-0cd8021b1b52be819	Available	-	34.226.15.17	10.0.0.5

nat-0cd8021b1b52be819 / my-NAT

[Details](#) [Monitoring](#) [Tags](#)

Details

NAT gateway ID	State	State message	Elastic IP address
nat-0cd8021b1b52be819	Available	-	34.226.15.17
Private IP address	Network interface ID	VPC	Subnet

- Once this NAT is created, similar to IGW, in order to use it we must add a route to internet using route table
- We had created a dedicated route table for our private subnet. Let us add an entry in the route table like below

[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
private-RT	rtb-0acda69fea5072d27	subnet-07de0a69061ab2dd9	-	No	vpc-0a0152fbfb1aaecc7 ...	384395217903

Route Table: rtb-0acda69fea5072d27

[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
0.0.0.0/0	nat-0cd8021b1b52be819	active	No

- In order to add the above entry, select our private route table. Click on add route
- In destination add 0.0.0.0/0
- In target select "NAT gateway" and select the newly created nat gateway id.
- Click on save.
- Once this is done, login to the private instance again and try the below command again

```
ping www.google.com
```

Points to consider

- Post practice make sure to delete the components inside the VPC , i.e. igw ,NACL,NAT.elastic ip etc before deleting the VPC. Without that VPC will not be deleted
- Public instance used for jumping to private instances is termed as jump host or bastian host
- While whitelisting traffic for within a VPC , always use private ip address
- Always remember , NAT gateway is created in public subnet but is used by a private subnet