

Table of contents

- [Table of contents](#)
- [VPC :](#)
 - [Default VPC](#)
 - [Subnet](#)
 - [Route tables](#)
 - [Internet gateway](#)
 - [NACL](#)
 - [Understanding architecture diagram](#)
 - [Analogy to remember](#)

VPC :

- VPC stands for virtual private cloud and is a way to define and secure your network perimeter in aws .
- Getting to know VPC is essential to understand how networking works in AWS or cloud in general

Default VPC

- When an AWS account is created , by aws creates 1 VPC in every region . This is to ensure ,people who have just started to explore aws shouldn't face much difficulties launching an EC2.
- Default VPC will have a description which denotes if it is a default VPC

The screenshot displays the AWS Management Console interface for VPCs. On the left, a sidebar shows navigation options like 'VPC Dashboard', 'Subnets', 'Route Tables', and 'Internet Gateways'. The main content area is titled 'Your VPCs (1/2)' and contains a table with the following data:

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR (Network Border Group)
-	vpc-5d8d3327	Available	172.31.0.0/16	-
-	vpc-0289eae669be105d7	Available	172.16.0.0/16	-

Below the table, the 'Details' section for the selected VPC 'vpc-5d8d3327' is expanded, showing the following information:

- VPC ID:** vpc-5d8d3327
- State:** Available
- DNS hostnames:** Enabled
- DNS resolution:** Enabled
- Tenancy:** Default
- DHCP options set:** dopt-4173283a
- Route table:** rtb-38070247
- Network ACL:** acl-6ef81913
- IPv4 CIDR:** 172.31.0.0/16
- IPv6 pool:** -
- IPv6 CIDR (Network Border Group):** -

- These default VPCs come with certain components inside them . Let us try and understand the components
- To start with , default VPC has a CIDR associated with it . ex : 172.31.0.0/16

Subnet

- Subnets are a subset of a VPC .
- These are AZ specific .
- Vpcs are split into smaller subnets to have smaller network groups which can be controlled easily.

Filter by tags and attributes or search by keyword

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Avail
	subnet-0185d4bacdf33e307	available	vpc-0289eae669be105d7	172.16.0.0/24	250	-	us-east-1a	use1
	subnet-0d5a9b10093bba5f9	available	vpc-0289eae669be105d7	172.16.1.0/24	249	-	us-east-1c	use1
	subnet-23dfb60d	available	vpc-5d8d3327	172.31.80.0/20	4091	-	us-east-1c	use1
	subnet-40deb11c	available	vpc-5d8d3327	172.31.32.0/20	4091	-	us-east-1a	use1
	subnet-8c01b7b2	available	vpc-5d8d3327	172.31.48.0/20	4090	-	us-east-1e	use1
	subnet-a2c1f3e8	available	vpc-5d8d3327	172.31.16.0/20	4090	-	us-east-1d	use1
	subnet-bffa98d8	available	vpc-5d8d3327	172.31.0.0/20	4091	-	us-east-1b	use1
	subnet-e586a2ea	available	vpc-5d8d3327	172.31.64.0/20	4091	-	us-east-1f	use1

- Above screen shows all the subnets under one region . If we want to see subnets associated with only one VPC , select the VPC from the filter in the top left corner

Filter by tags and attributes or search by keyword

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Avail
	subnet-23dfb60d	available	vpc-5d8d3327	172.31.80.0/20	4091	-	us-east-1c	use1
	subnet-40deb11c	available	vpc-5d8d3327	172.31.32.0/20	4091	-	us-east-1a	use1
	subnet-8c01b7b2	available	vpc-5d8d3327	172.31.48.0/20	4090	-	us-east-1e	use1
	subnet-a2c1f3e8	available	vpc-5d8d3327	172.31.16.0/20	4090	-	us-east-1d	use1
	subnet-bffa98d8	available	vpc-5d8d3327	172.31.0.0/20	4091	-	us-east-1b	use1
	subnet-e586a2ea	available	vpc-5d8d3327	172.31.64.0/20	4091	-	us-east-1f	use1

- Whenever we are making any changes to any of the components under VPC , it is important that we use this filter to make sure appropriate resources are selected .
- The CIDR of the subnets will be subsets of the larger VPC CIDR . for ex
 - VPC CIDR : 172.31.0.0/16
 - Subnet A : 172.31.0.0/20
 - Subnet B : 172.31.16.0/20
 - Subnet C : 172.31.32.0/20
 - Subnet D : 172.31.48.0/20
 - Subnet E : 172.31.48.0/20
 - Subnet F : 172.31.80.0/20
- Note that the subnets will always be within the VPC CIDR limit and never beyond that
- A subnet decides the ip as well as the AZ in which the instance or any resource using that subnet will be deployed.

- The network connectivity as well as public/private settings could also be controlled using subnets.

VPC Dashboard **New**

Filter by VPC:

Q vpc-5d8d3327

vpc-5d8d3327
Owner: 384395217903

VIRTUAL PRIVATE CLOUD

Your VPCs **New**

Subnets

Route Tables

Internet Gateways **New**

Egress Only Internet Gateways **New**

Carrier Gateways **New**

DHCP Options Sets **New**

Elastic IPs **New**

Filter by tags and attributes or search by keyword

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR
	subnet-23dfb60d	available	vpc-5d8d3327	172.31.80.0/20	4091	-
	subnet-40deb11c	available	vpc-5d8d3327	172.31.32.0/20	4091	-
	subnet-8c01b7b2	available	vpc-5d8d3327	172.31.48.0/20	4090	-

Subnet: subnet-23dfb60d

Description | Flow Logs | Route Table | Network ACL | Tags | Sharing

Subnet ID	subnet-23dfb60d	State	available
VPC	vpc-5d8d3327	IPv4 CIDR	172.31.80.0/20
Available IPv4 Addresses	4091	IPv6 CIDR	-
Availability Zone	us-east-1c (use1-az2)	Network Border Group	us-east-1
Route Table	rtb-38070247	Network ACL	acl-6ef81913
Default subnet	Yes	Auto-assign public IPv4 address	Yes
Auto-assign customer-owned IPv4 address	No	Customer-owned IPv4 pool	-

Route tables

- Route tables are associated with subnets. And are used to control traffic going out from the subnet
- For ex . If your instance which is inside a subnet , has to connect to outside internet . There has to be a route table associated with the subnet which will allow the connectivity

New VPC Experience
Tell us what you think

VPC Dashboard **New**

Filter by VPC:

Q vpc-5d8d3327

vpc-5d8d3327
Owner: 384395217903

VIRTUAL PRIVATE CLOUD

Your VPCs **New**

Subnets

Route Tables

Internet Gateways **New**

Egress Only Internet Gateways **New**

Carrier Gateways **New**

DHCP Options Sets **New**

Elastic IPs **New**

Managed Prefix

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
	rtb-38070247	-	-	Yes	vpc-5d8d3327	38439521

Route Table: rtb-38070247

Summary | **Routes** | Subnet Associations | Edge Associations | Route Propagation | Tags

Edit routes

View: All routes

Destination	Target	Status	Propagated
172.31.0.0/16	local	active	No
0.0.0.0/0	igw-0bbe5370	active	No

- Notice that there are 2 entries inside the routes under route table .
- First entry is done by default whenever a new route table is created . Which basically states that the subnet can communicate anywhere within the VPC .
- Second entry allows traffic to go to the internet .
- There are other entries which can control traffic to move to other networks as well, which we will see in upcoming sessions
- With every VPC that is created , there is one route table that is created . Which is termed as Main route table
- If we do not associate any route table to any subnet , by default those subnets will use the Main route table

Filter by tags and attributes or search by keyword

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
	rtb-38070247	-	-	Yes	vpc-5d8d3327	384395217903

Route Table: rtb-38070247

Summary Routes Subnet Associations Edge Associations Route Propagation Tags

Edit subnet associations

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:

- Notice that there are no subnets associated with the route table . yet all the subnets in the default VPC will use this route table as there is no explicit association made with any other route table

Internet gateway

- In route table we observed that when we are defining the route to the internet , in target there is an entity like "igw-xxxx"
- This is an id of the internet gateway .
- As the name suggests , the internet gateway is responsible for granting access to the internet and back .
- In order to use internet gateway , instance should have public ip . If there is no internet gateway attached , instance cannot access internet and neither can the traffic from internet access the instance .
- There are other ways to access internet without public ip , but we will be seeing it in the upcoming sessions .
- There can be only one 1 internet gateway can be attached to a VPC at a time . Internet gateway scales depending on the traffic hence there is no need of having multiple internet gateways .

new vpc experience
Tell us what you think

VPC Dashboard New

Filter by VPC:
vpc-5d8d3327

vpc-5d8d3327
Owner: 384395217903

VIRTUAL PRIVATE CLOUD

Your VPCs New

Subnets

Route Tables

Internet Gateways New

Egress Only Internet Gateways New

Internet gateways (1/1) Info

Filter internet gateways

VPC ID: vpc-5d8d3327 Clear filters

	Name	Internet gateway ID	State	VPC ID	Owner
<input checked="" type="checkbox"/>	--	igw-0bbe5370	Attached	vpc-5d8d3327	384395217903

Create internet gateway

NACL

- NACL stands for network access control list
- Think of NACL as security group for the subnets .
- With default VPC you will be able to see one NACL . Just like rout tables , these have to be associated with a subnet explicitly .

Filter by tags and attributes or search by keyword

Name	Network ACL ID	Associated with	Default	VPC	Owner
	acl-6ef81913	6 Subnets	Yes	vpc-5d8d3327	384395217903

Network ACL: acl-6ef81913

Details Inbound Rules Outbound Rules **Subnet associations** Tags

Network ACL ID: acl-6ef81913
 Associated with: 6 Subnets
 Owner: 384395217903

Default: Yes
 VPC: vpc-5d8d3327

- NACL acts as firewall for your subnets

Create network ACL Actions

Filter by tags and attributes or search by keyword

Name	Network ACL ID	Associated with	Default	VPC	Owner
	acl-6ef81913	6 Subnets	Yes	vpc-5d8d3327	384395217903

Network ACL: acl-6ef81913

Details **Inbound Rules** Outbound Rules Subnet associations Tags

Edit inbound rules

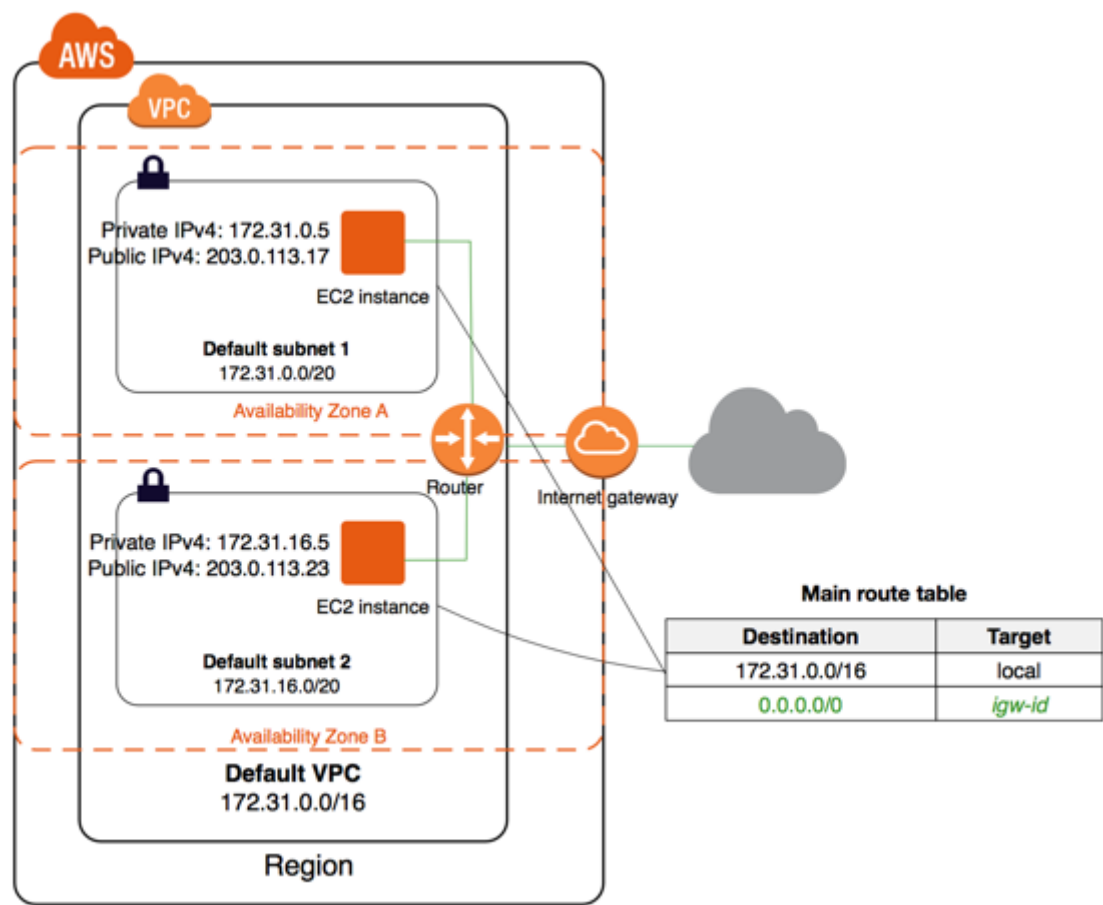
View: All rules

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

- Notice under inbound rules , there are 2 rules defined .
 - Rule # : This defines the priority of the rule . The lower the number , the higher the priority . By default AWS recommends using multiples of 100 .
 - type, protocol, port range , source : This is similar to security group network traffic type
 - Allow/Deny : This feature is unique to NACL. We can explicitly define if the traffic needs to be blocked or allowed .
- As you can observe , by default traffic is open for all
- In rule # , we can see "*" defined . This is a wildcard . In case any request comes and that does not fit in any of the rules defined , then * will be applicable . By default it is a deny action for all
- One of the most common questions asked in an interview is difference between NACL and security group .

Security Group	Network ACL
Operates at the instance level	Operates at the subnet level
Supports allow rules only	Supports allow rules and deny rules
Is stateful: Return traffic is automatically allowed, regardless of any rules	Is stateless: Return traffic must be explicitly allowed by rules
We evaluate all rules before deciding whether to allow traffic	We process rules in number order when deciding whether to allow traffic
Applies to an instance only if someone specifies the security group when launching the instance, or associates the security group with the instance later on	Automatically applies to all instances in the subnets it's associated with (therefore, you don't have to rely on users to specify the security group)

Understanding architecture diagram



- Above diagram explains how the default VPC would appear in a architectural diagram. See if we can identify and correlate all the components we discussed

Analogy to remember

- As we discussed , let us remember the components using an analogy
 - VPC - city
 - Subnet - Postal code /area within the city
 - route table - Roads for the postal code
 - internet gateway - Highway
 - NACL - security checks for the postal code
 - instance - building
 - security group - guard of the building
- To sum up , VPC is a city in which the network will reside. Subnets/postal code are subset of the VPC/city. Route table/roads control traffic going out from the postal code/subnet . Internet gateway/highway allows the subnet/postal code to connect to the internet via route table/roads .
- NACL are the security checks on the road which control the traffic coming or going from the postal codes.
 - **Points to consider**
- Default VPC has been created by AWS just for ease of getting started. It should not be used in production
- Generally companies do not use it for deployments , however we should be careful before deleting any object
- Any change to be made inside a VPC should always go through proper approvals
- Whenever there is connection timed out or connection refused error , VPC configurations is one of the prime things we should check while troubleshooting