# Table of contents

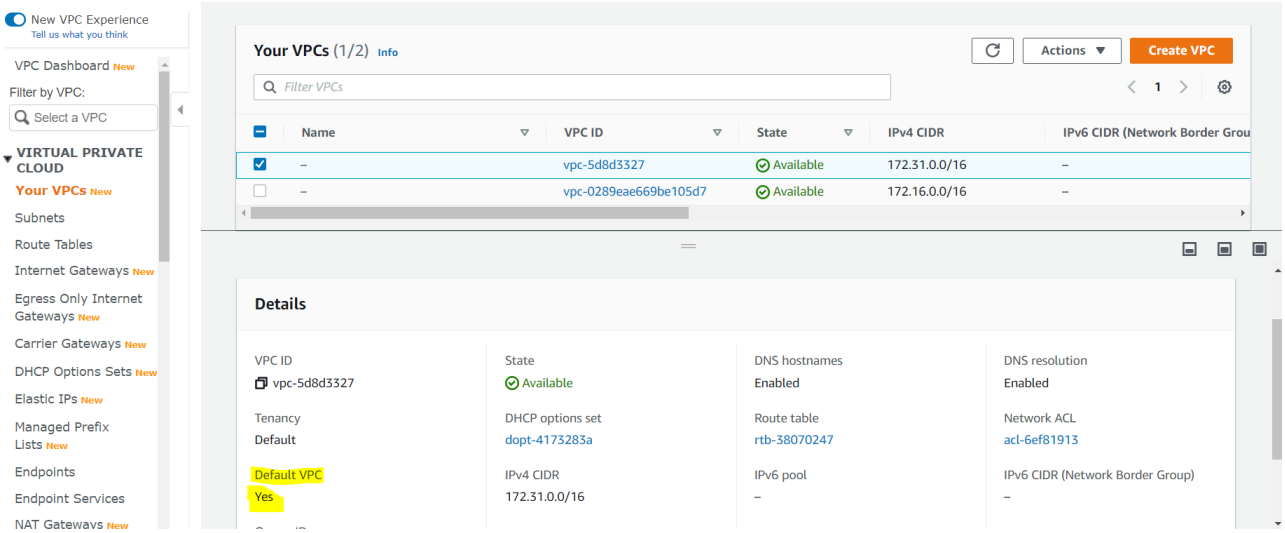


# VPC :

- 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

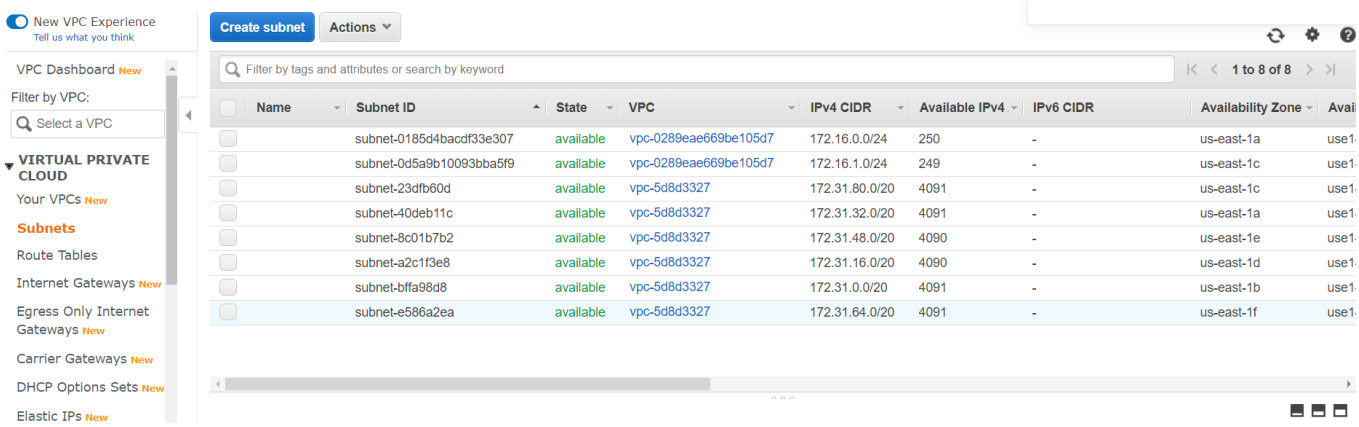
- When an AWS account is created , by aws creates 1 VPC in every region . This is to ensure ,people who have just started to explore aws shouldn't face much difficulties launching an EC2.
- Default VPC will have a description which denotes if it is a default VPC



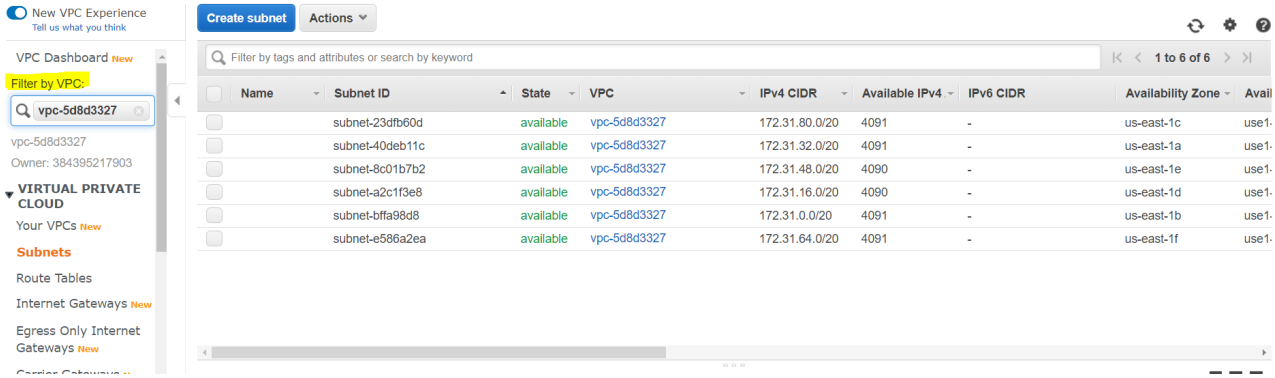

  - These default VPCs come with certain components inside them . Let us try and understand the components
  - To start with , default VPC has a CIDR associated with it . ex : 172.31.0.0/16

### 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.

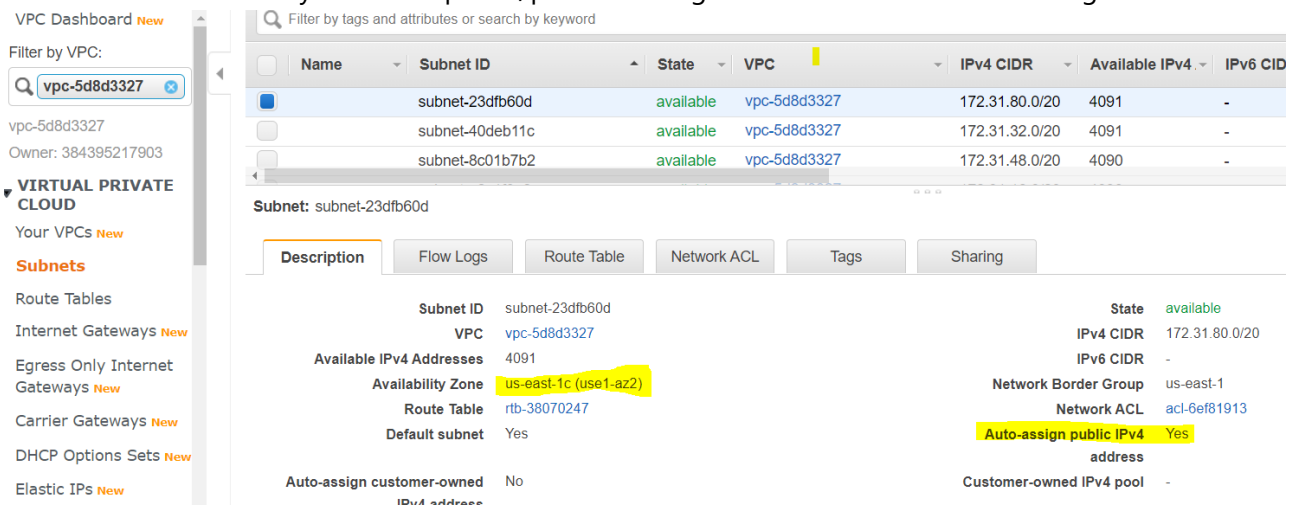



- Above screen shows all the subnets under one region . If we want to see subnets associated with only one VPC , select the VPC from the filter in the top left corner



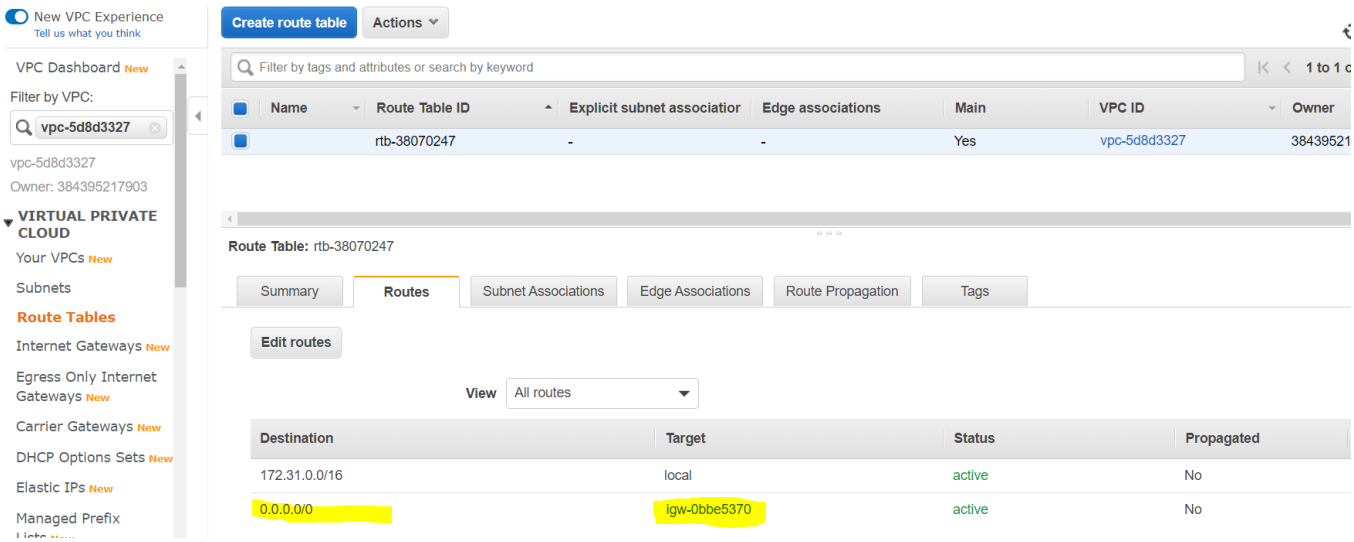

- Whenever we are making any changes to any of the components under VPC , it is important that we use this filter to make sure appropriate resources are selected .
- The CIDR of the subnets will be subsets of the larger VPC CIDR . for ex
    - VPC CIDR : 172.31.0.0/16
        - Subnet A : 172.31.0.0/20
        - 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.

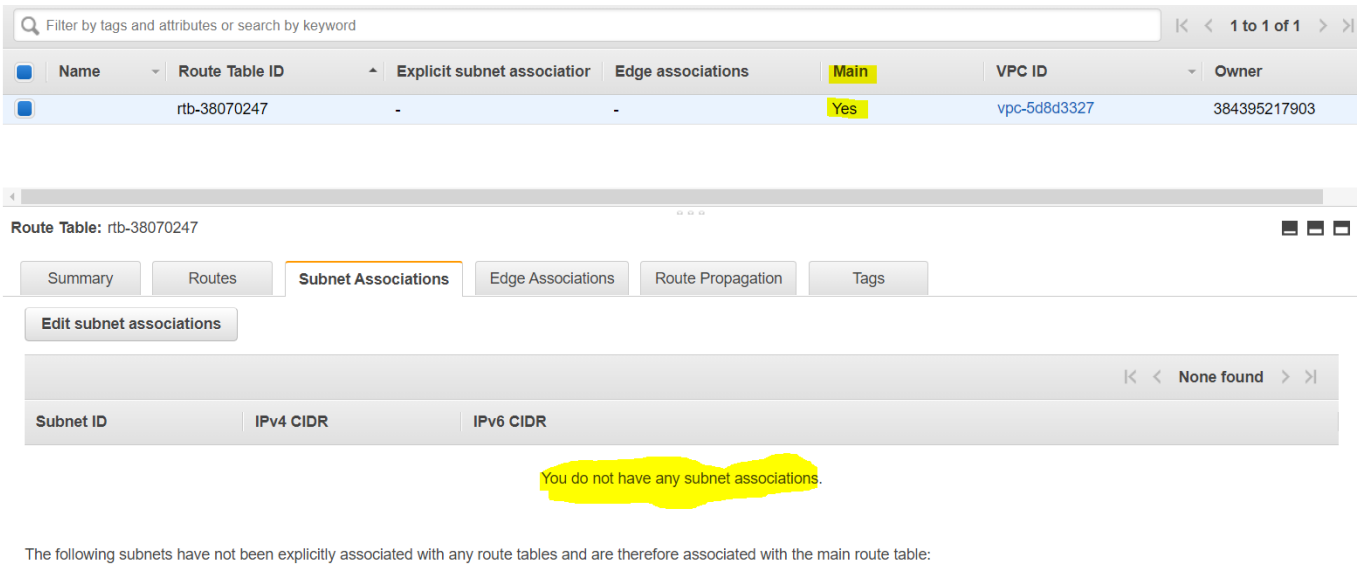



## Route tables

- 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



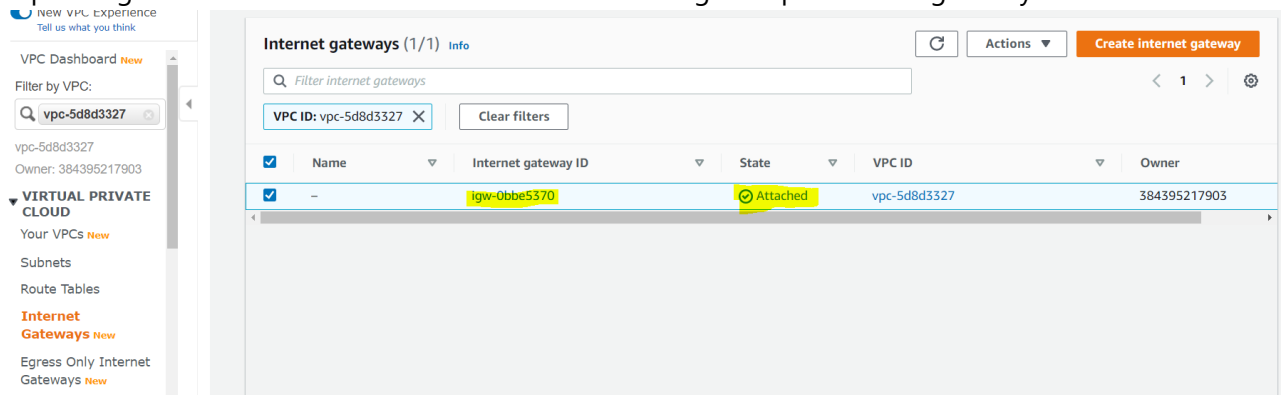

- Notice that there are 2 entries inside the routes under route table .
- First entry is done by default whenever a new route table is created . Which basically states that the subnet can communicate anywhere within the VPC .
- Second entry allows traffic to go to the internet .
- There are other entries which can control traffic to move to other networks as well, which we will see in upcmoning 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




- 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

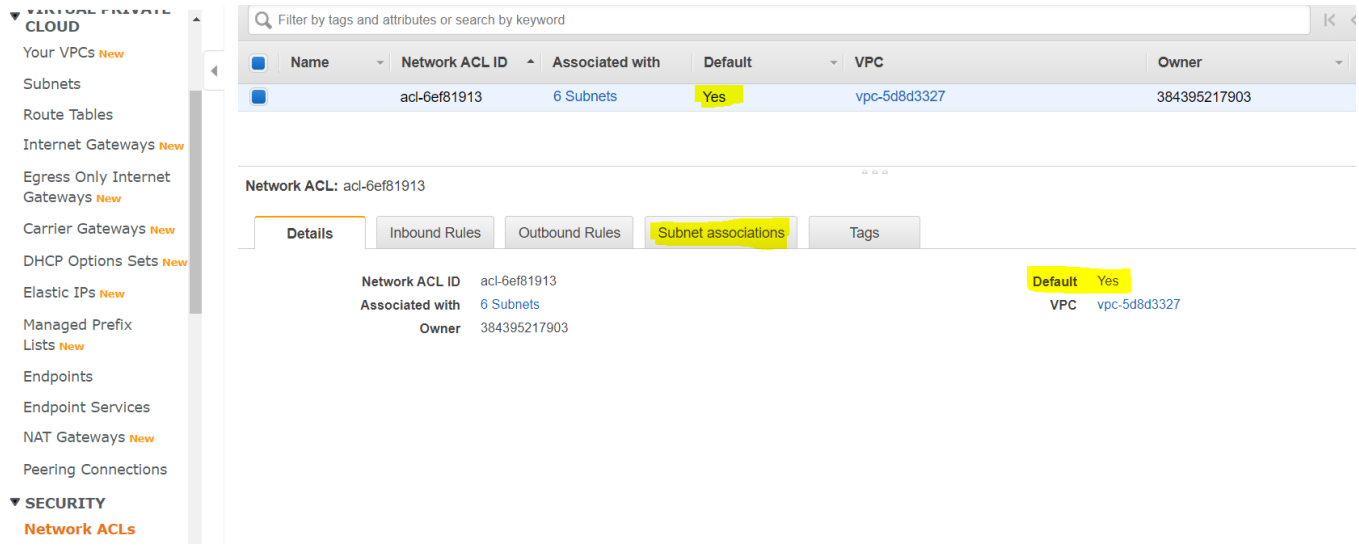
## Internet gateway

- 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 .

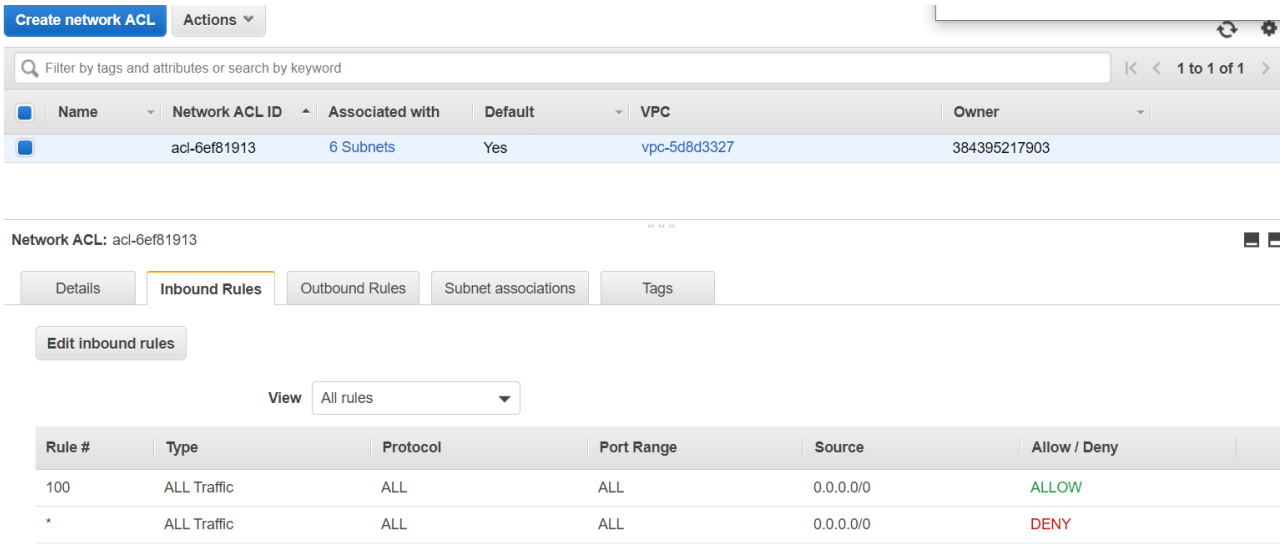



### NACL

- 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 explicitely .



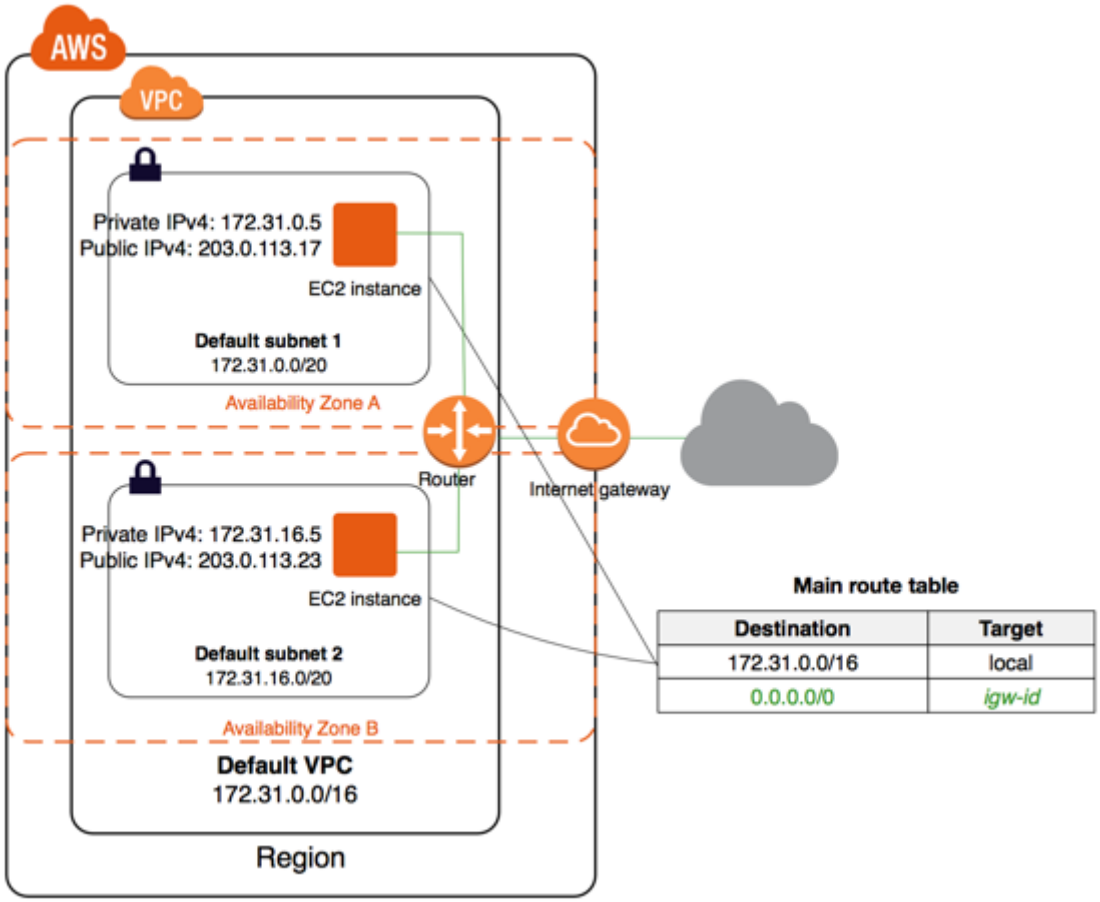

- NACL acts as firewall for your subnets




- 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 recomends using multiples of 100 .
    - type, protocol, port range , source : This is similar to security group network traffic type
    - Allow/Deny : This feature us unique to NACL. We can explicitely define if the traffic needs to be blocked or allowed .
- As you can oberve , 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 dny 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 corelate 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