**NETWORKING BSICS**

**Diagram

Description automatically generated**

When we are working in a na office ghen the network we are in is known as a private network and in aws terms it is aws vpc(virtual private cloud)

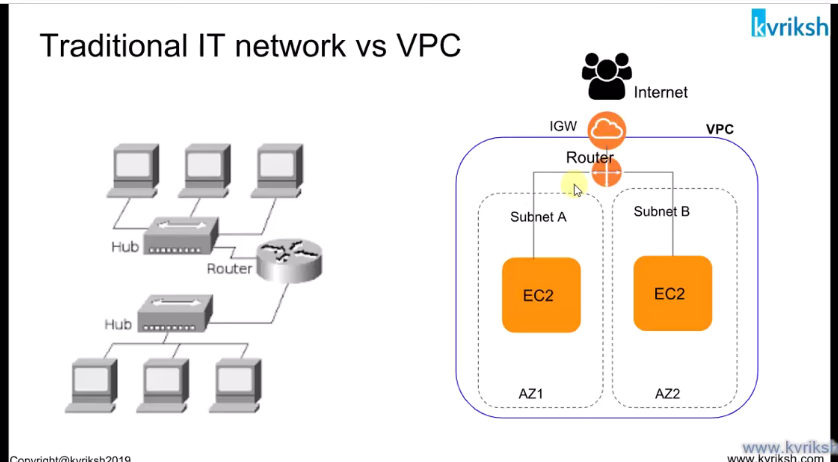
So there will be many system on a floor connected with each other ina lan and joined through the switches.so they all are considered to be a part of a network.

Now if we want our system a to communicate with system b then we will need a router which is used to establish a connection between the switches and also router on different floor.now when our system in the private netwok wants to talk to the internet then there is a gateway which contro,s the inbound an the outbound traffic.

**VIRTUAL PRIAVTE CLOUD**

Amazon virtual private cloud enables you to launch Amazon Web services resources into a virtual network that you have defined.This virtual network closely resembles a traditional network that you would operate in your own data center,with the benefits of using the scalable infrastructure of AWS.

**TRADITIONAL IT NETWORK OVER THE VPC**

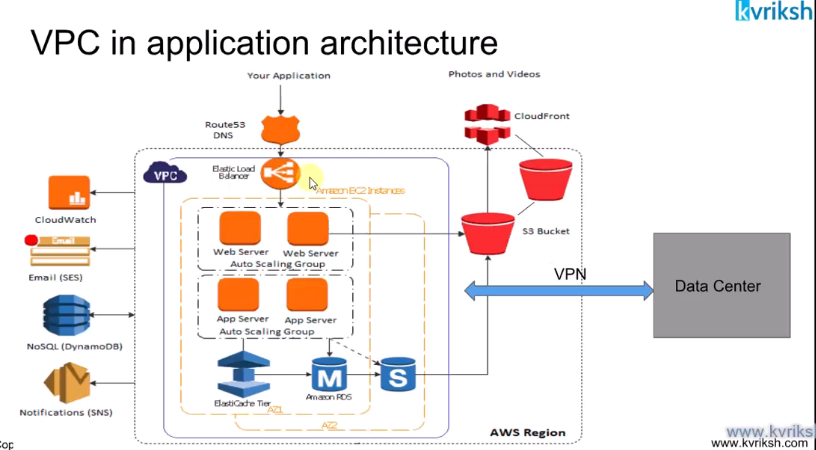
****

**SOME GLOBAL,REGIONAL AND AVAILABILITY ZONE SPECIFIC SERVICES**

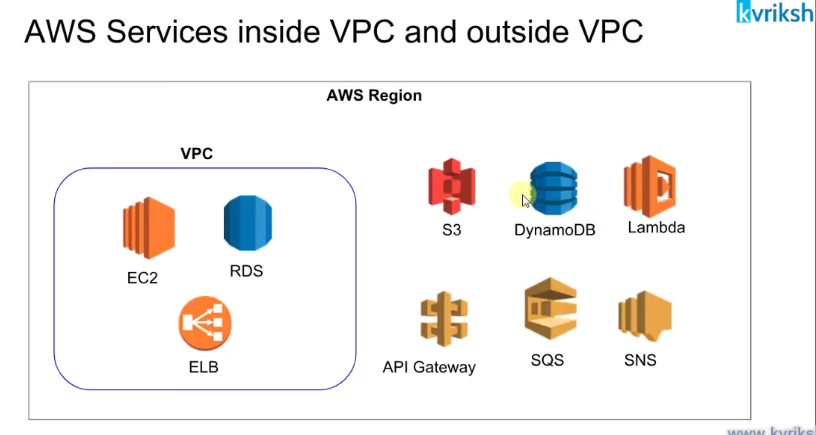
Diagram

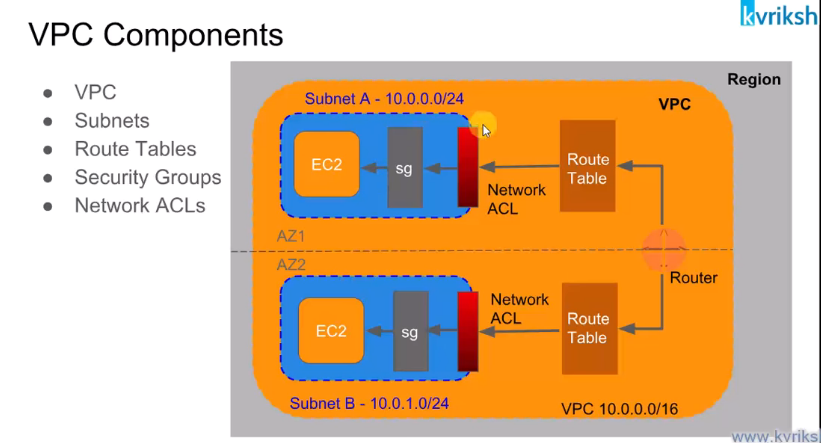
Description automatically generated

**VPC IN APPLICATION ARCHITECTUR**

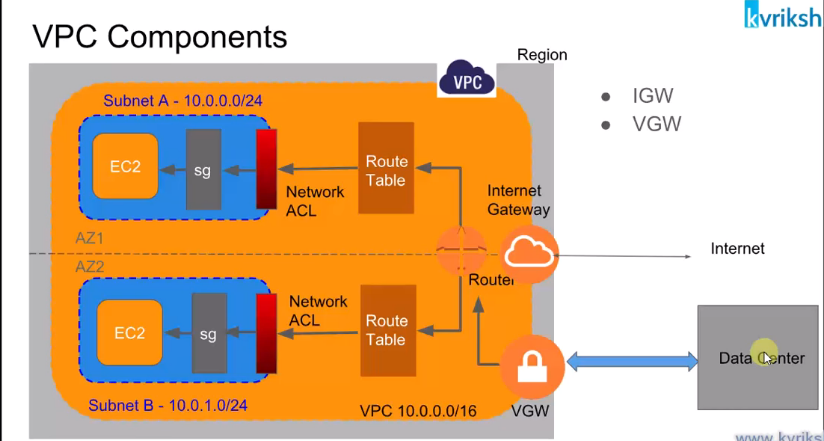
****

**SOME VPC SERVICES INSIDE VPC AND OUTSIDE VPC**

****

****

* Vpc is a big address space and vpc is bound ina aregion means.There can be a vpc in a region.In one region there can be multiple vpcs.
* Subnet is a further categorization of a vpc.
* A subnet has a one to one mapping with an az.which means we can have one subnet in one az onl;y not in two azs.An az can have many subnets in it.
* Route table:each vpc has a route table which will look on the traffic going in and out of avpc.Some rules are there in the routing table which decide whether your machine is going to be accessible to the internet or they are private.
* Firewall:two firewall in the vpc.one is the ec2 level called the security group and the network acl work at the subnet level.So what rules we apply to an nacl firewall apply to all the instances in that subnet.And security group rules are applied to only one ec2 instance.

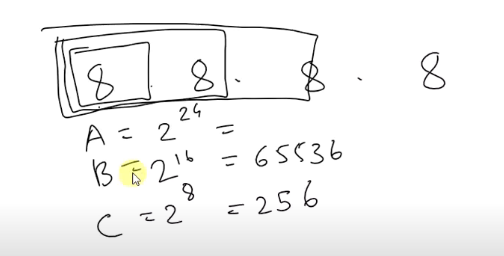


* **Internet gateway:**an internet gateway is a gateway which allows internet access to our vpc.
* **Virtual private gateway:** this allows to connect to our on premise data center to have access to the vpc.There needs to be a priavtge connection between the two and we do not want our two connections to be accessible to outside world.

**HOW AN IP ADDRESSS IS FORMED**

While forming an ip address it is said that some bits are reserved so that will form some classes.

As we can see in the diagram below if we speak of a class then first 8 bits are reserved and rest 24 will be used to form addresses.

\And oif we speak of class b then 16 will be reserveda and rest 8 used to form the ip ranges. 

In the new form we denote the address a s  **X.X.X.X/X**

So if the address is written as  **10.10.0.0/16**  means 16 bits are reserved for the host.

So we can have 2^16 adresses=65536 addresses.

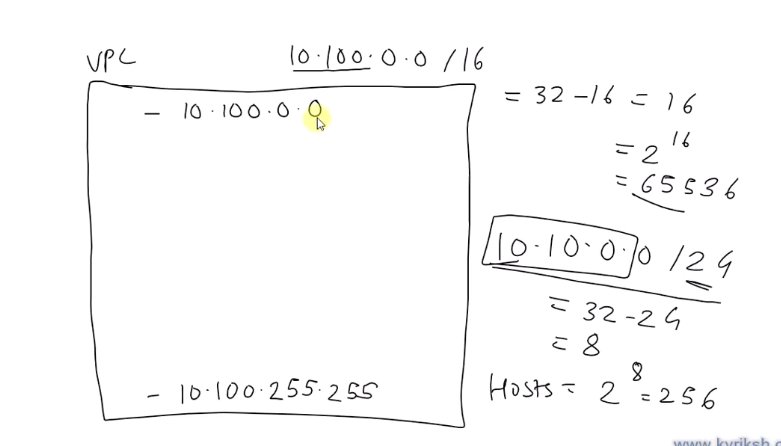
**Diagram

Description automatically generated**

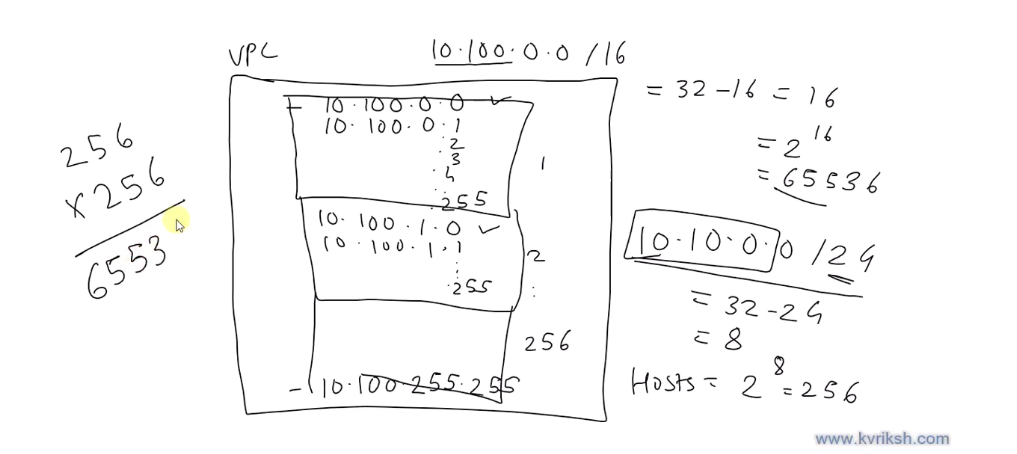
**Now we**  take the below example to understand how our vpc addresses are formed.

So for example we define a vpc with the cidr as:**10.100.0.0/16**  means the 16 bits are reserved for our host that means we are left with 16 bits to form our hosts.

Now the starting address in this vpc will be  **10.100.0.0**  and the last address will be  **10.100.255.255**

****

Now we want to  **form subnets**

****

One big vpc is divided into subnets and there can be 256 subnets and in each of those 256 subntes there will be 256 hosts in each of the subnets.

**EXAMPLE**

Now as inn our example we wanted to have 256 hosts so what we did we took the vpc ip address and the fixed one more octet for the network which is the third one so mean snow in all 24 bits are given to the subnet thus our subnet is denoted by  **10.100.0.0/24**

So in the above subnet the hosts can have address starting form  **10.100.0.0/24 to 10.100.0.255/24**

A picture containing diagram

Description automatically generated

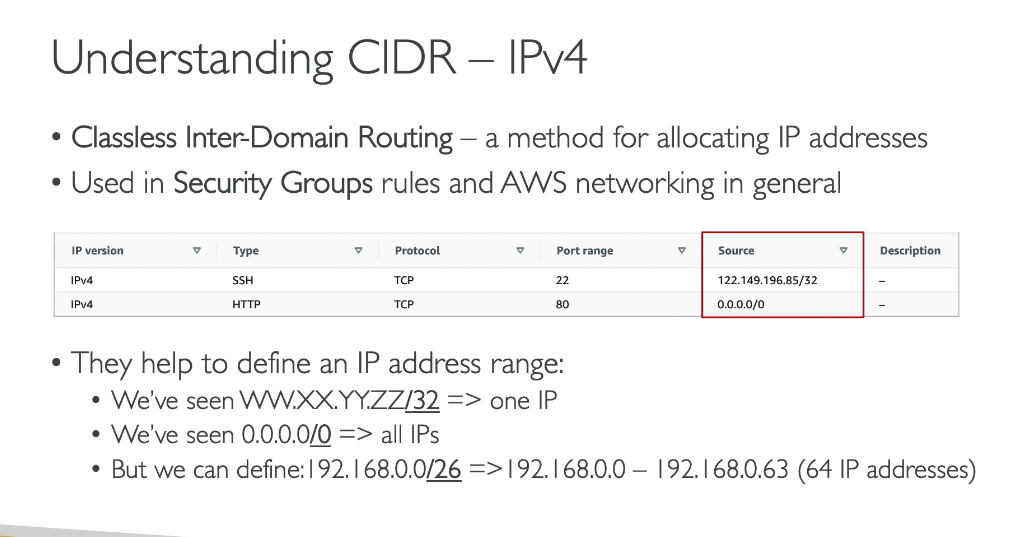
**UNDERSTANDING THE CIDER IPV4**

Cidr stands for classless inter domain routing and it is a method for allocating IP addresses.

These are used in security group rules and AWS networking in general.

They help us to define an IP address range

1.we have seen some ip addresses already in the security group so lets discuss about them.

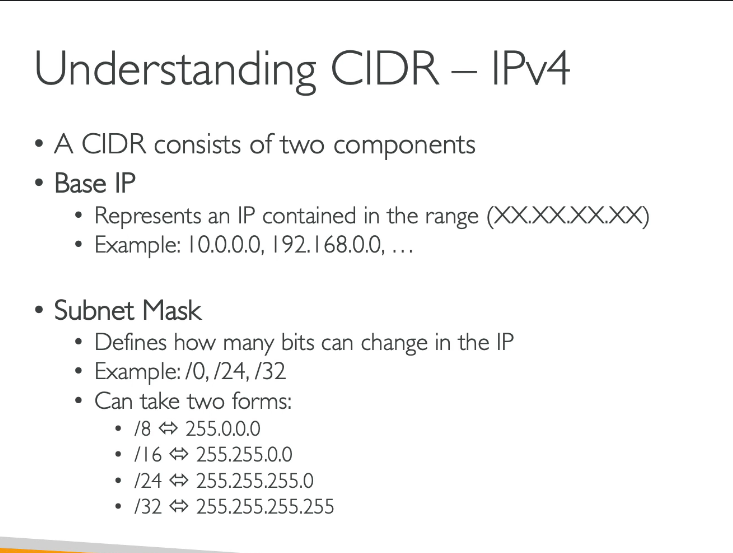


A cidr consists of two components:

1.base ip2.subnet mask

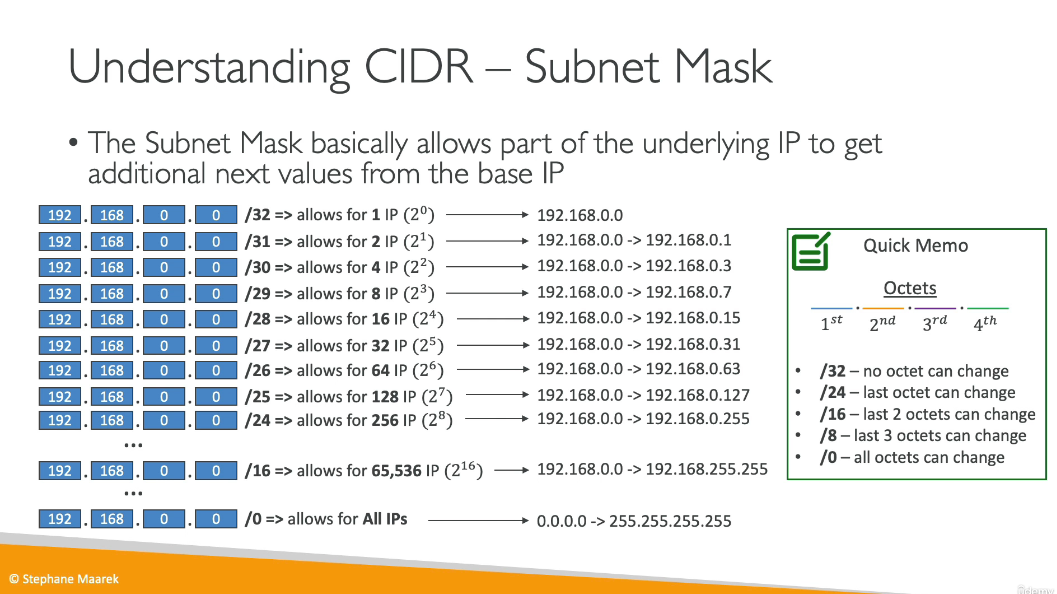
A base ip represents an ip contained in the range.

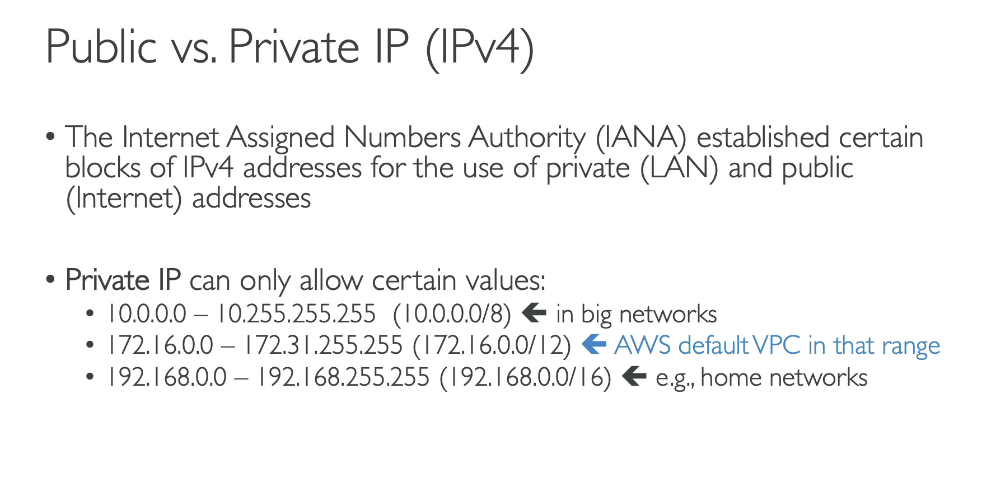
Subnet mask defines how many bits can change in the ip.



**UNDERSTANDING CIDR SUBNET MASK**

The subnet mask basically allows part of the underlying ip to get additional next values from the base ip.





Graphical user interface, text, application, email

Description automatically generated

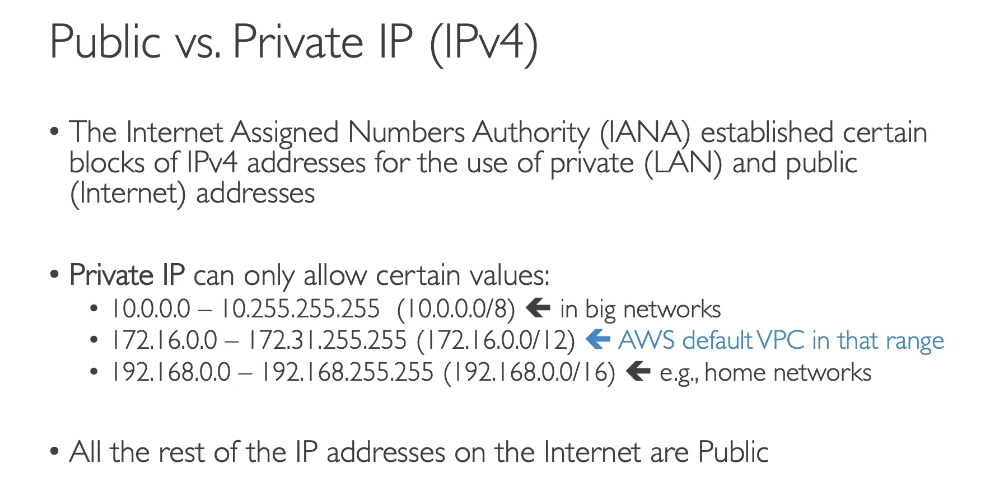
Table

Description automatically generated

If it is written 10.0.0./8 means 8 bits have been reserved and you can use the rest of it.

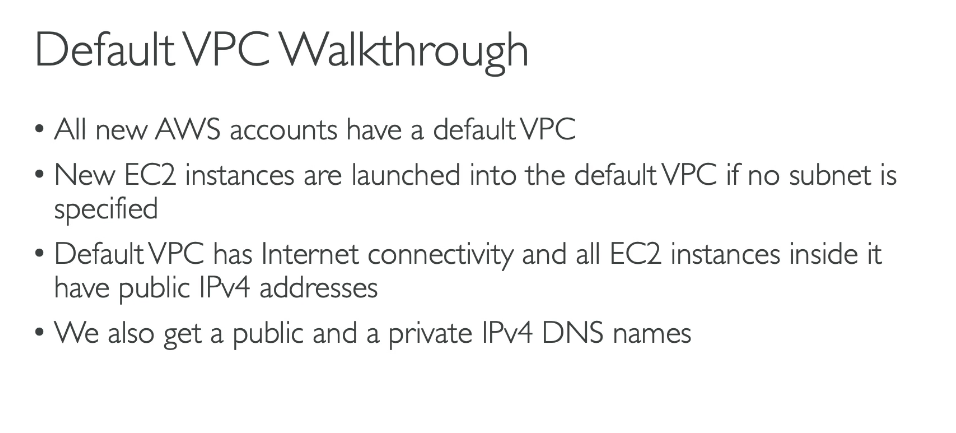
The total number of bits in an ip address are:32

So if 8 are reserved so we can use 32-8=24 bit that means 2^24 addresses will be there.



**DEFAULT VPC OVERVIEW**

This is the default vpc which si created with our account when we create anew aws account.



**OVERVIEW OF VPC**

Graphical user interface, text, application

Description automatically generated

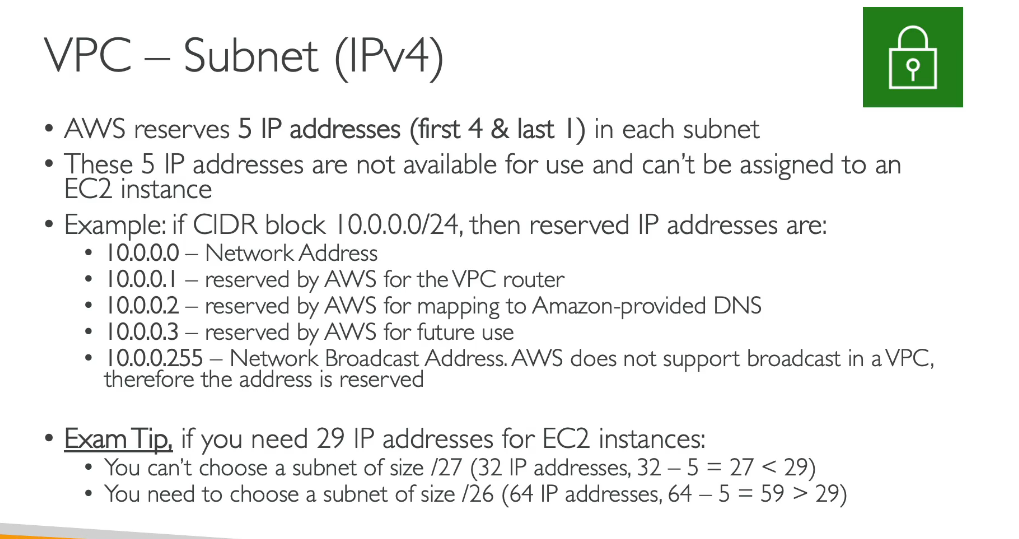
**VPC SUBNETS**

**Chart, waterfall chart

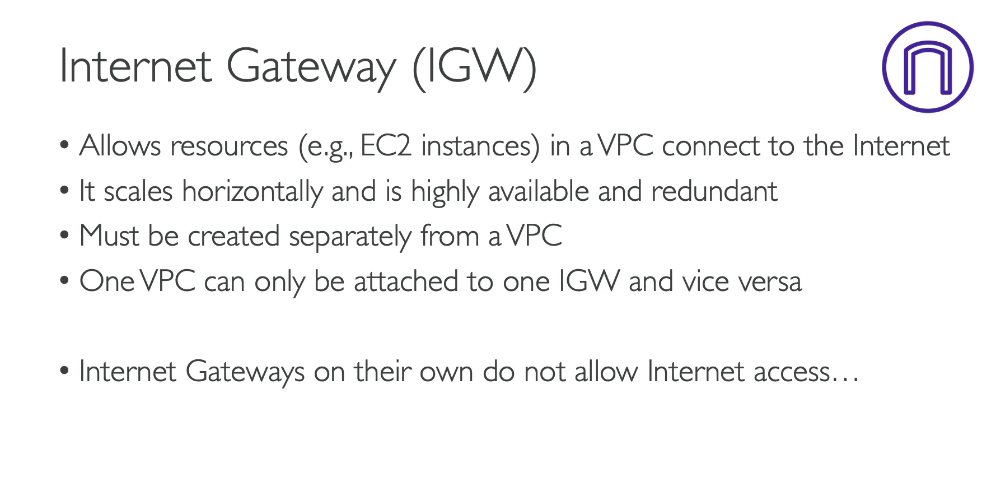
Description automatically generated**

A subnet is a set of ip ranges within our vpc which can either foram a private or a public subnet.

**AWS**  by default reserves 5 ip addresses in each subnet as can be seen below:



**INTERNET GATEWAY**

****

HOW DOES AN  **INETRNET GATEWAY WORKS**

**Graphical user interface

Description automatically generated with medium confidence**

BASTION HOSTS

Graphical user interface, application

Description automatically generated

**NAT**

**Graphical user interface, text, application

Description automatically generated**

Nat is an instance launched in a public subnet so that our instances in the private subnet can connect to the outside world.

Graphical user interface, application

Description automatically generated

Text

Description automatically generated

**NAT GATEWAY**

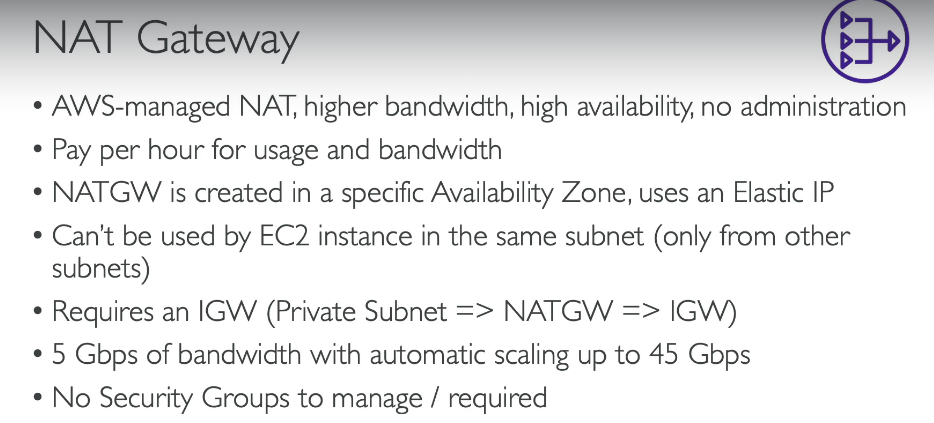
Nat gateway is working on behalf of the nat instances.

It is aws managed,higher bandwidth,high availability and no administration is needed.

Nat gateway is created in a specific az and it uses and elastic ip.

It cannot be used by an ec2 instance in the same subnet it can only be used from other subnets.

What path is generally followed is:private subnet to natgateway and the to the internet gateway.

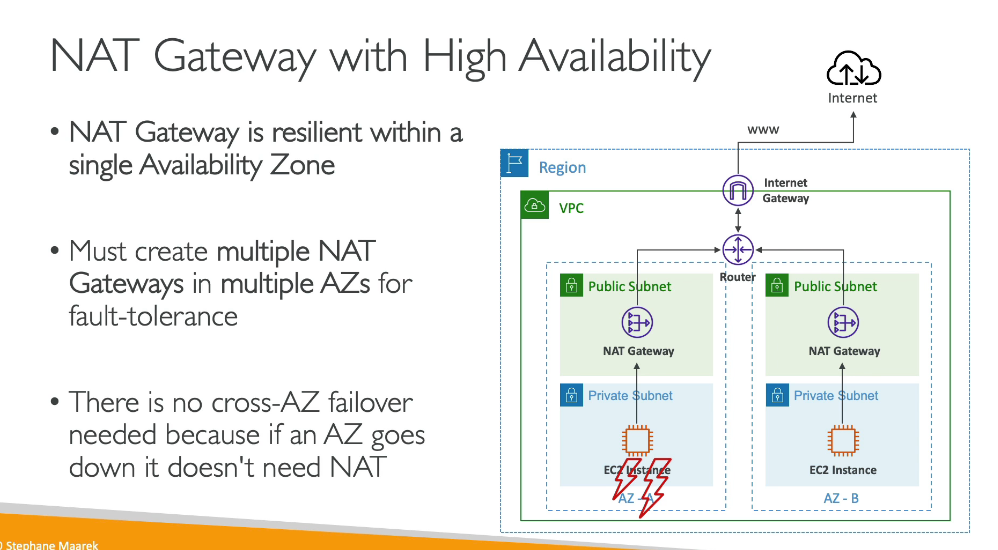


Diagram

Description automatically generated with medium confidence

**Nat**  getway is resilient(flexible ) within a single availability zone only.

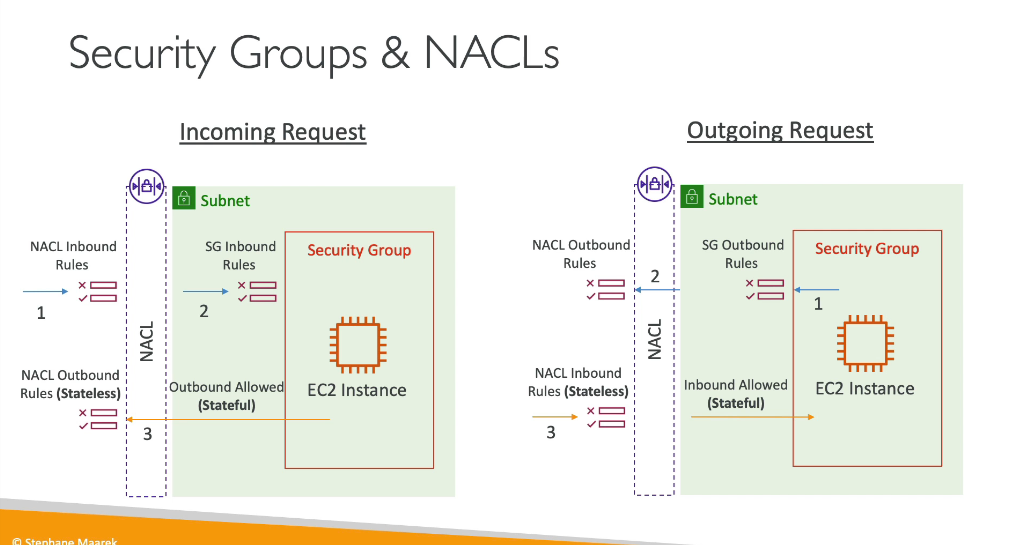
We need to create multiple nat gateways in multiple azs for fault tolerance and we do not need cross az failover because if an az goes down its ec2 instances are also down so we do not need any nat there.



Table

Description automatically generated

**NACL**

****

**INCOMING REQUEST**

The incoming request is working as below:

1.first some traffic from outside world need sto come and reach the nacl and then it will be allowed or not allowed by the nacl inbound rules.

Now if it passes it will be checked by the security group inbound rules before reaching our ec2 insgtance.

2.now when our ec2 instance has allowed a request to come in then it will be automatically allowed to be moved out from the security group but if we talk about the nacl the outgoing request will have to be chaceked by the nacl outboiund rules.

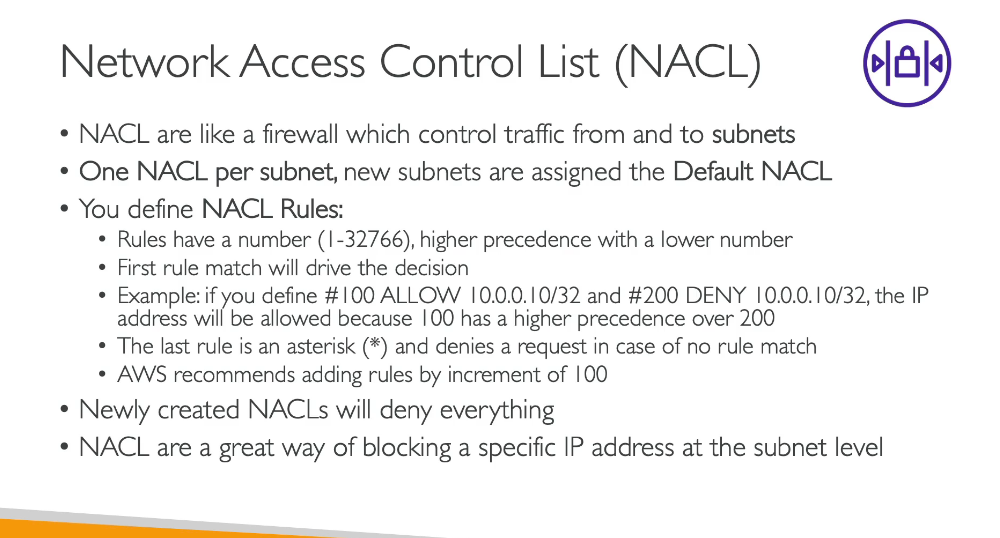
**Point to be noted:**

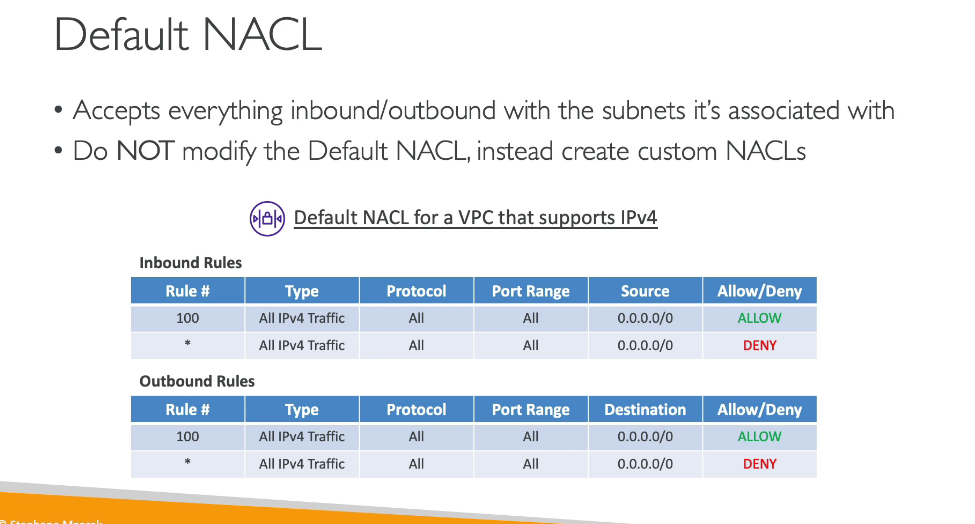
**1.nacl is a stateless:** since all the inbound na doutbound requests will be tested before coming in and out of the nacl.

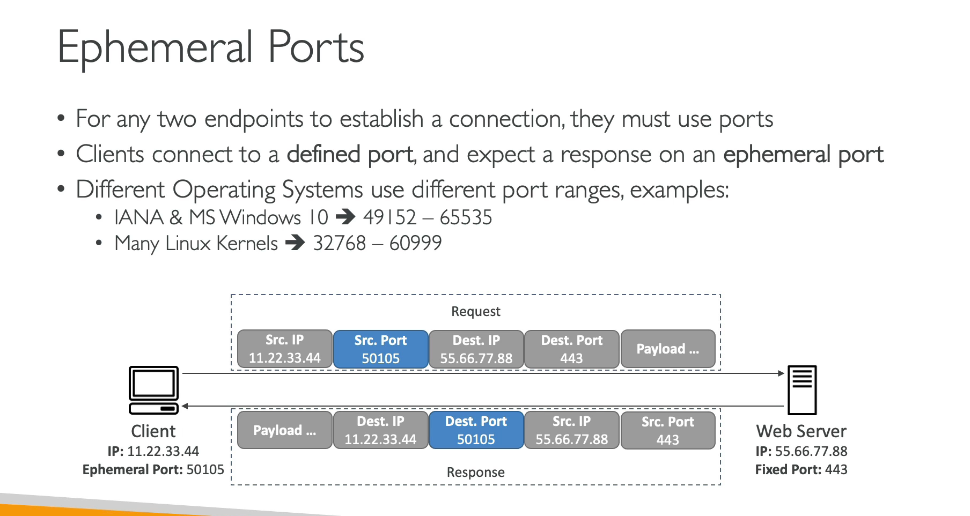
2.**security gateway is stateful:**

Since it keeps the state as when an address is allowed to come in then its state will be remembered and it will be allowed togo out.

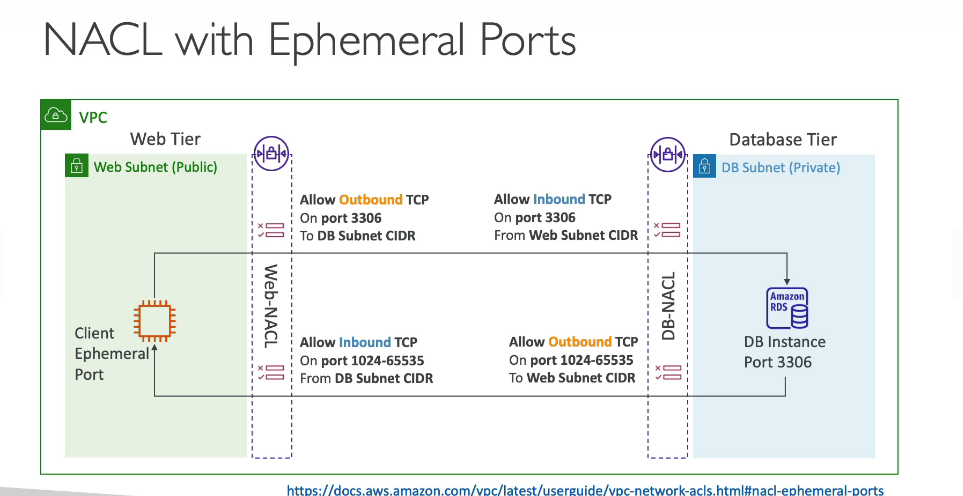
Graphical user interface, diagram, application

Description automatically generated



****

A client when send a request to a server it sends on a specific port and in return it wants the server to respond back on its ephemeral port.The name is ephemeral because it is a port opened by the client on its machine for a short term or for a particular request only.



Chart, line chart

Description automatically generated

Table

Description automatically generated with low confidence