VPC - Virtual Private Cloud

Presented by Marcia Maimela

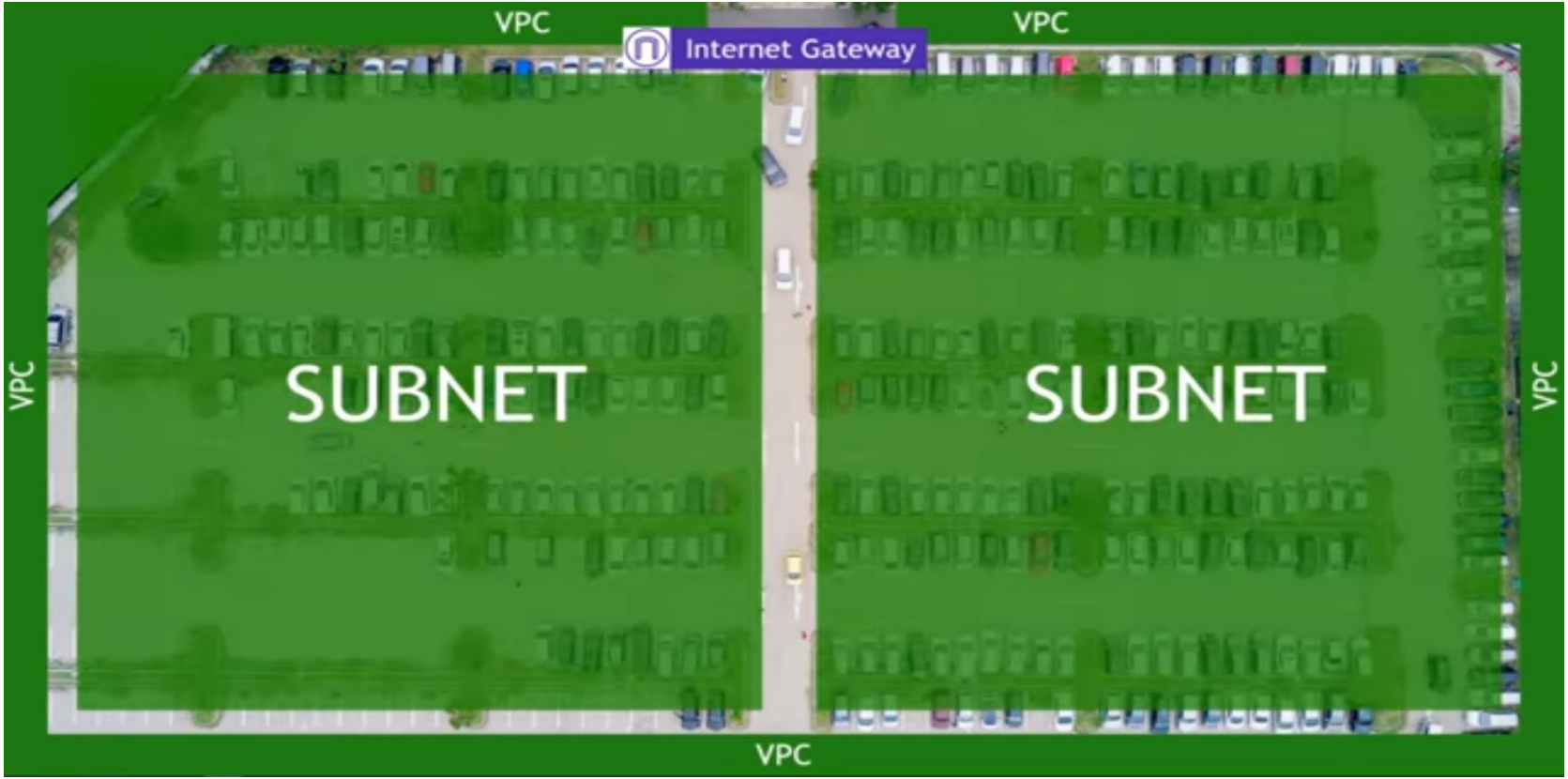
What is a VPC in simple terms

Virtual Private Cloud is your own private cloud/network within the cloud that isolates your resources from everyone else's.
Imagine a VPC as a digital parking lot for your computer resources, like servers and databases. It's like having your own private space within a huge digital parking lot.

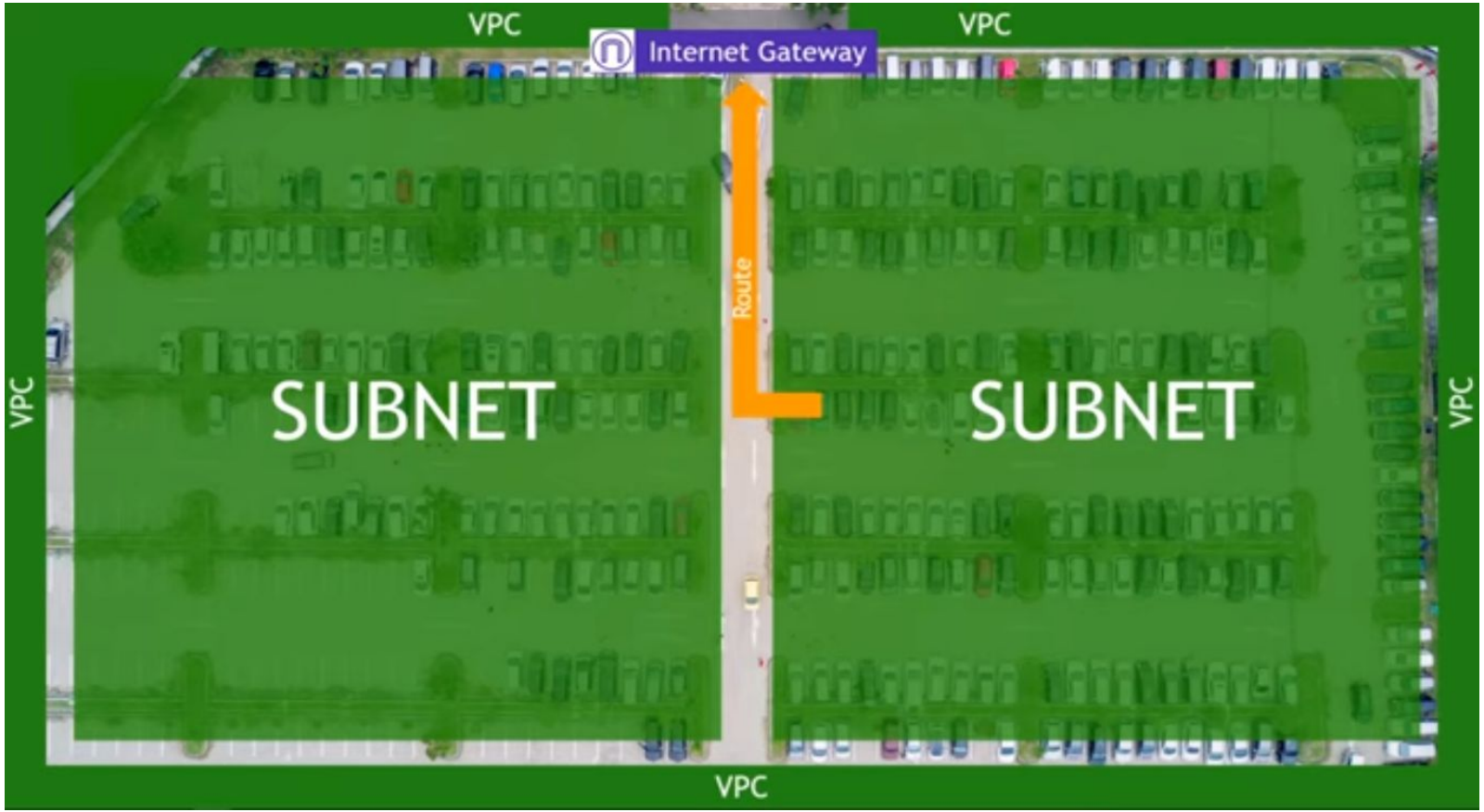
In this parking lot (VPC), you can set up your resources however you want. You can define where each resource goes, who can access them, and how they communicate with each other. It's like putting up virtual fences or boom gates to control who can come in and what they can do.

This will help in understanding the core concepts. Let's use this analogy of a parking lot, and outside the parking lot is the whole world- AWS world.

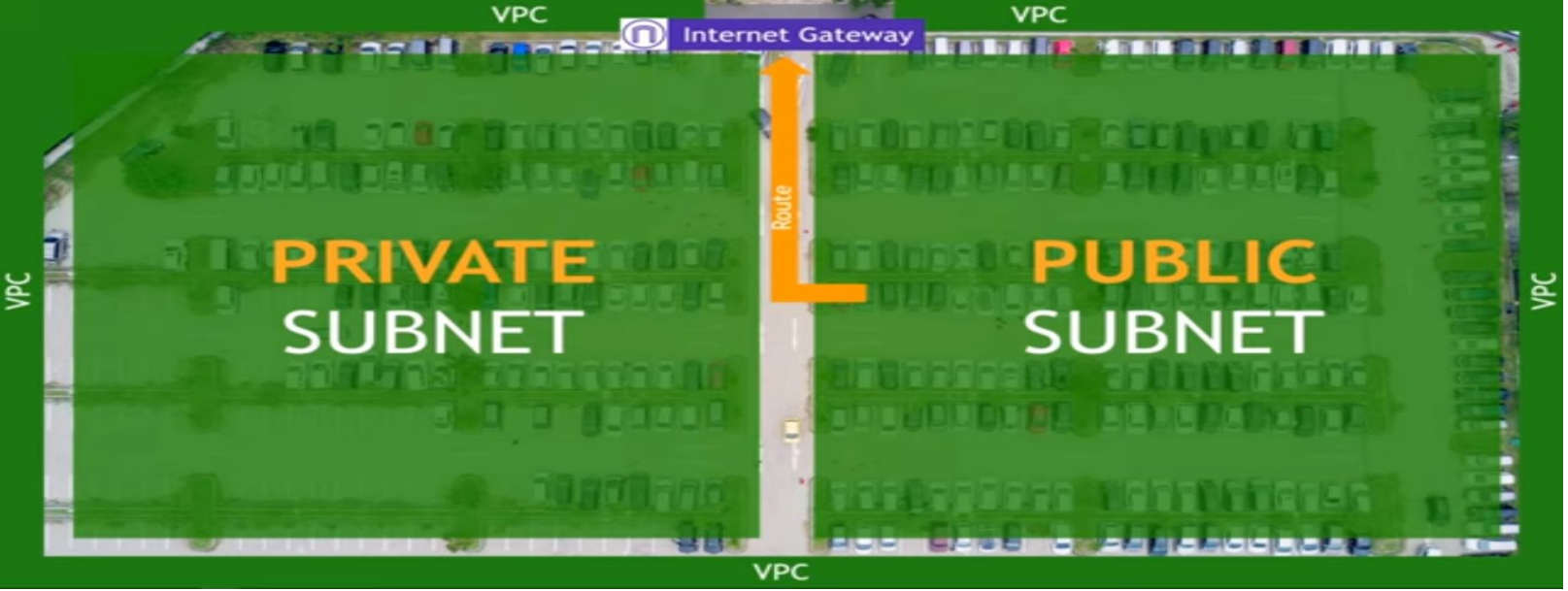
The Parking lot can be thought of as your VPC, So the fence or border around your world separates your resources from the rest of your resources. And up at the top we have traffic coming inside and outside of the world. In AWS term it is called Internet gateway, that is how your VPC talks to the internet.



And then inside the VPC we have logically separated areas, for example we have the left and the right of the parking lot. These are called your Subnets in AWS networking terms and generally they are gonna be used for different purposes.



Now the one subnet has a route to get out of the internet,



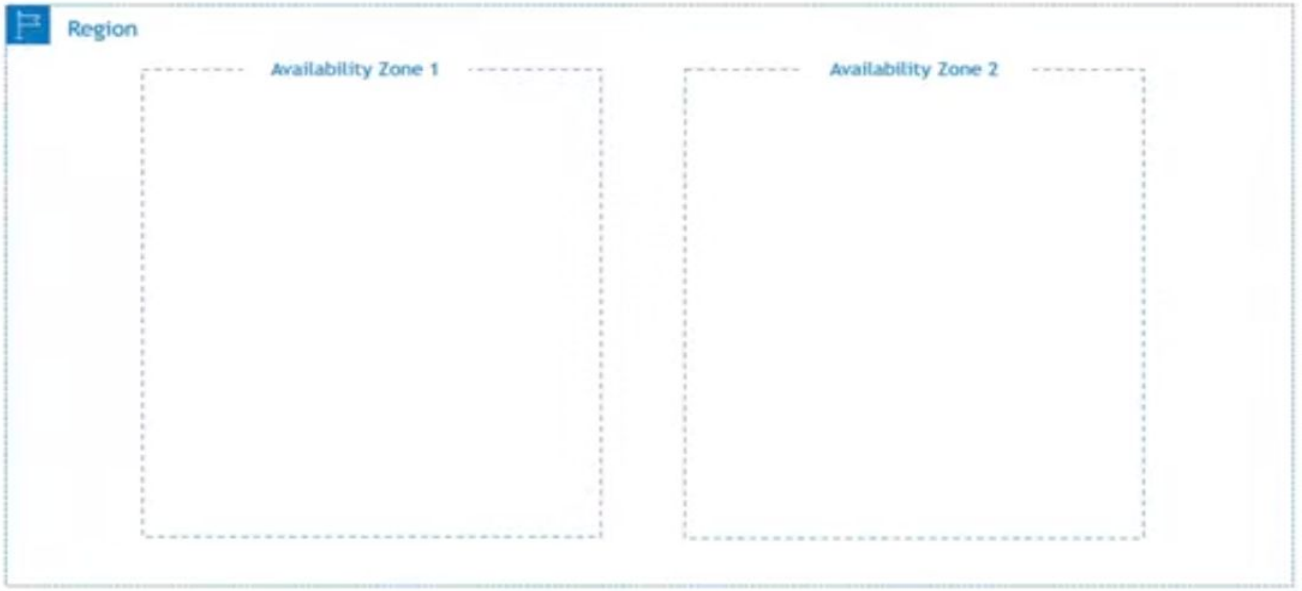
If that is the case, this is a public subnet and the other side the subnet doesn't have the route to the internet and that is a private subnet and that is the main distinction.

On the public subnet you put servers that would host, public-facing web pages and in the private subnet you would put your databases there.

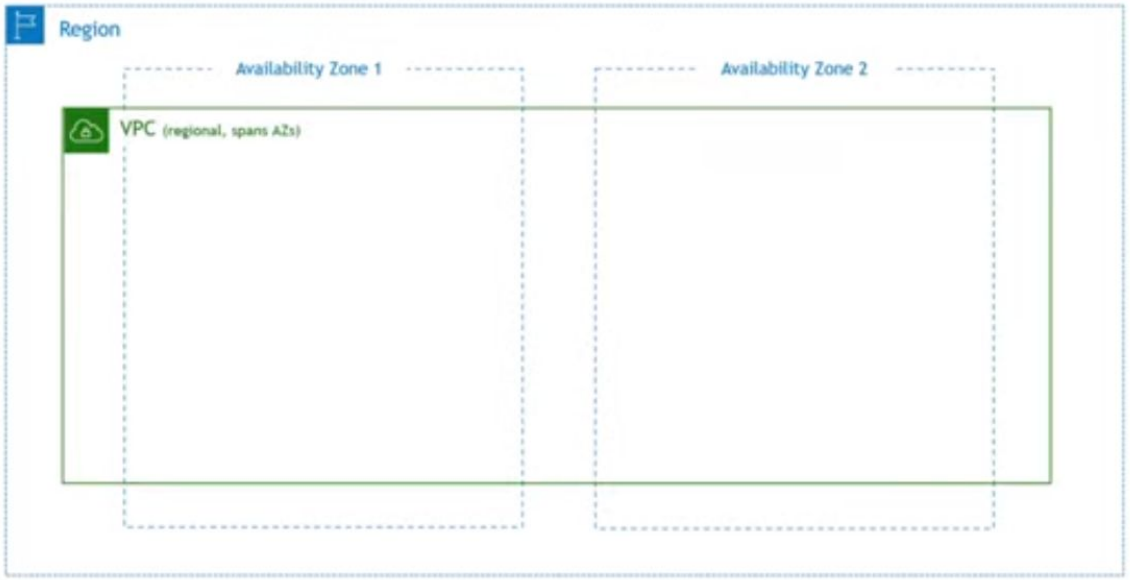
So there is that extra layer of security protecting from the outside world.

Hope this was helpful in understanding the concept of a VPC

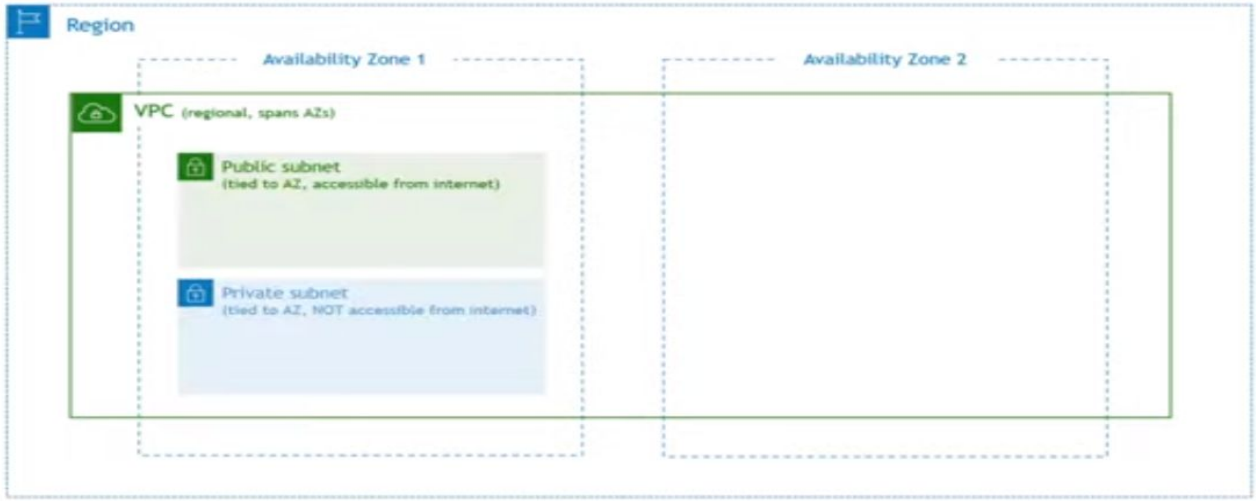
This represents the region for example US West one or EU West 2,



And within that we have availability zone, these are basically data centers within that region or two or more per region, something like US East 2a ,2b and 2c and so on.



Your VPC is tied into a single Region and it spans two or more availability zones



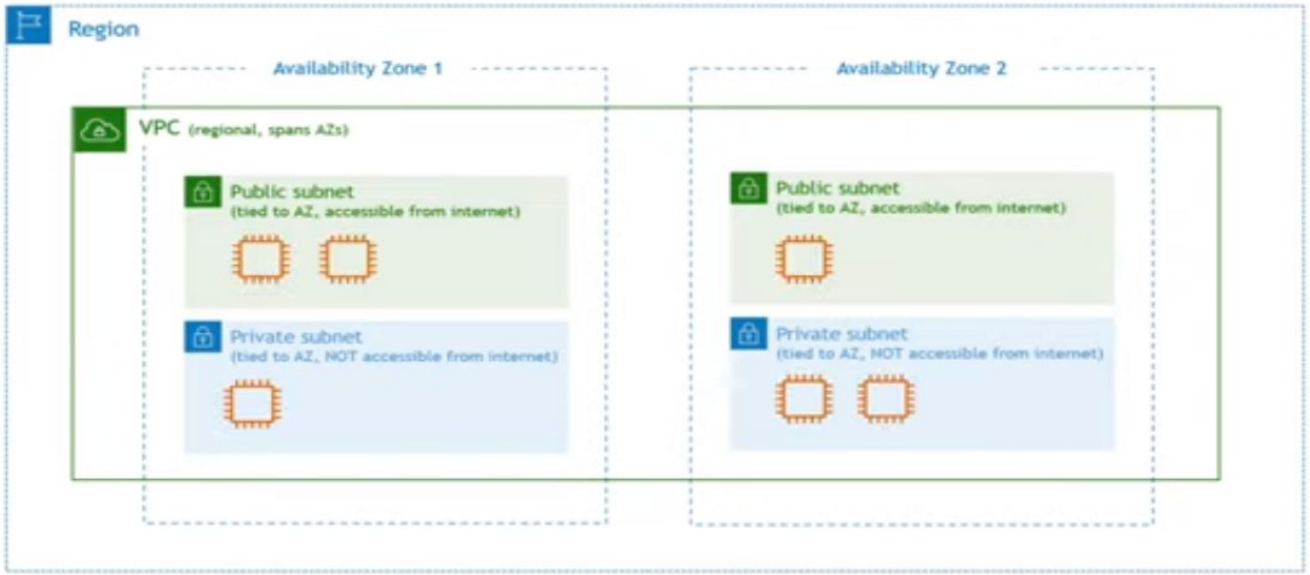
Then going down one more level.

We have our subnets and those different partitions of your VPC.

These are tied to the availability zone, so you have subnets for the first availability zone

And more subnets for the second availability zone. There are public and private subnets.

Public subnets are accessible from the internet and the private subnets aren’t.

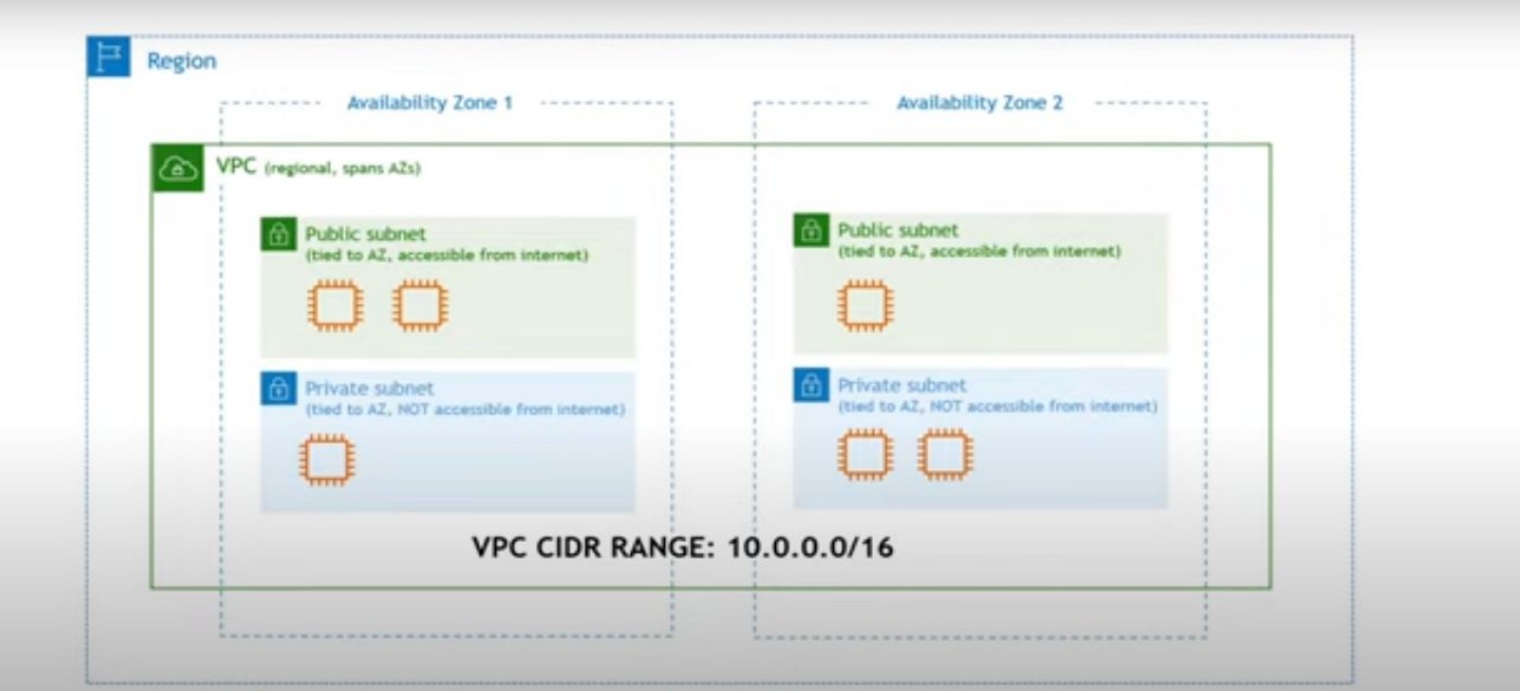


And then within the subnets that is where your actual resources live such as your EC2 and so on

Now let's jump into CIDR - CIDR is a Classless Internet-Domain Routing, now this is a notation for describing blocks of IP addresses.

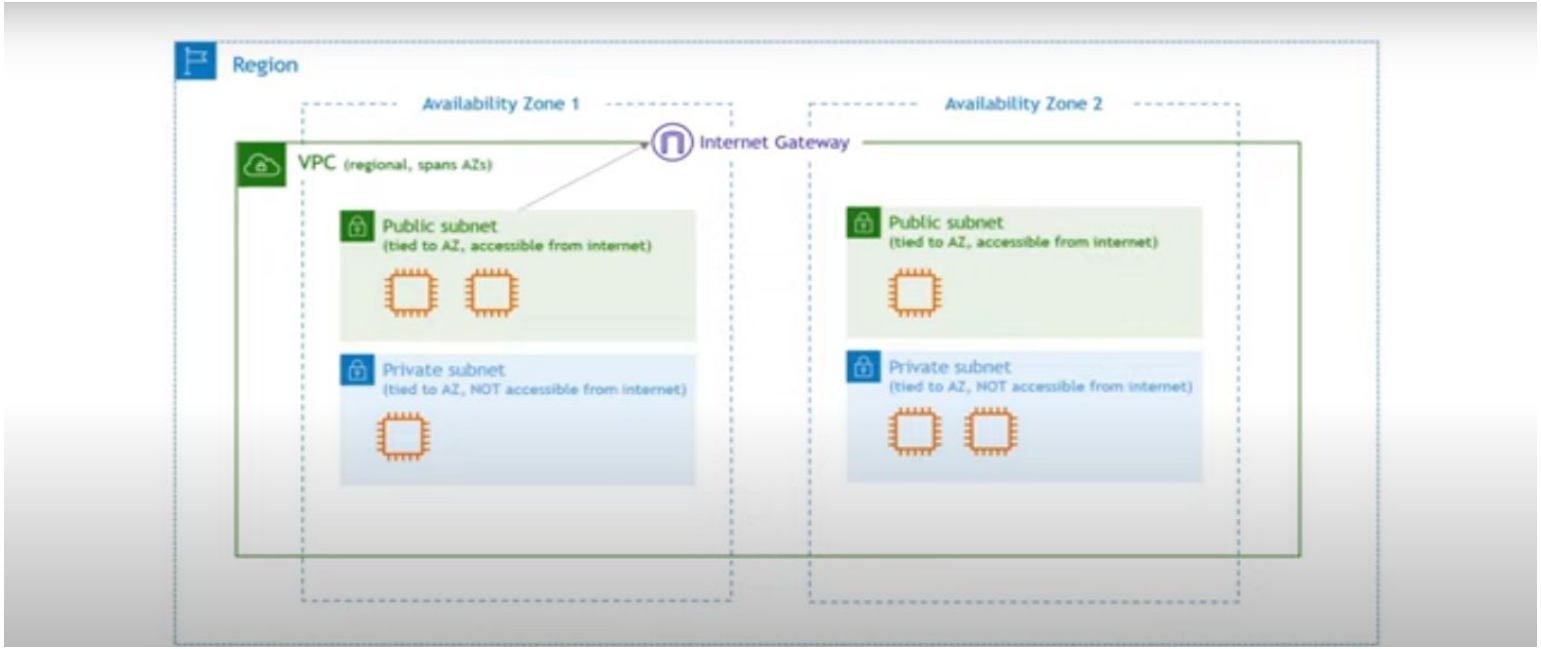
An IP address is like your home address but for a computer.

It tells the world where to find you.



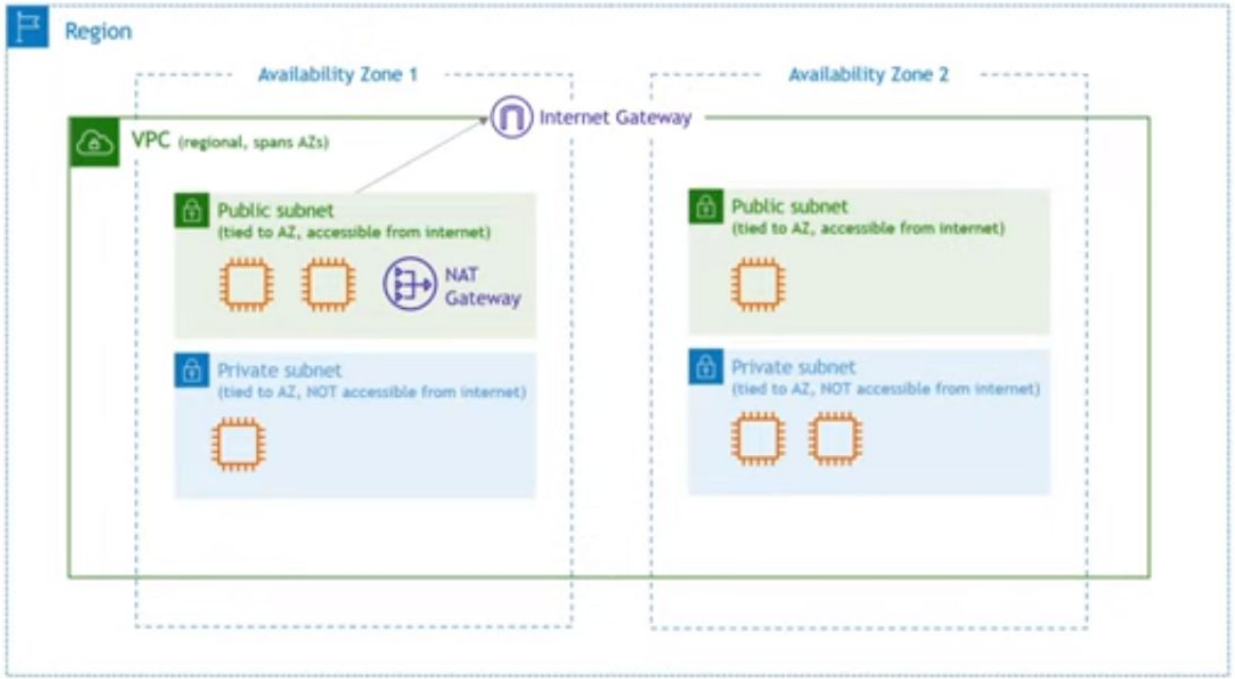
This IP address comes from CIDR block which is assigned at the VPC level. The CIDR range is assigned to the VPC level and this tells us how many IP addresses we can assign to thighs within that range.

In this particular diagram we have six EC2 instances which would take up six IP addresses and if we added some database instances those would need IP addresses. We want to make sure that we have enough addresses for all the resources in the VPC.

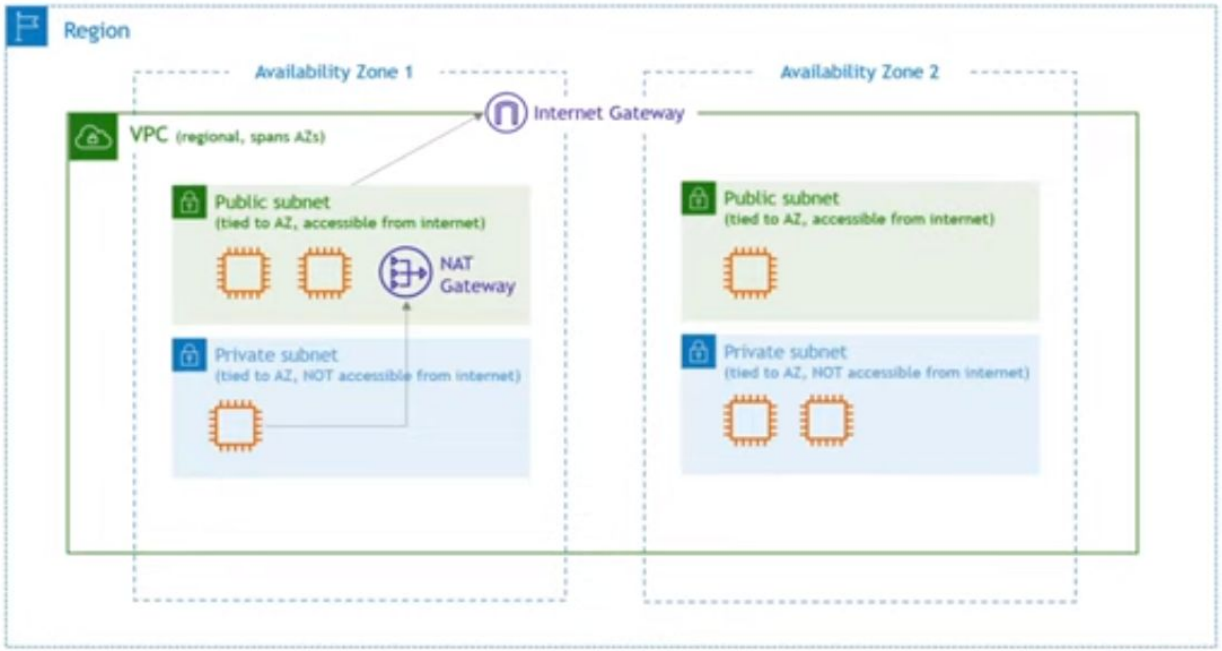


The internet Gateway that is at the VPC level and the fact that the public subnet has a route to it which is what makes it public,it is accessible to and from the internet. The private subnet doesn't have that route, you cannot get to it from the internet and you can’t get out to the internet.

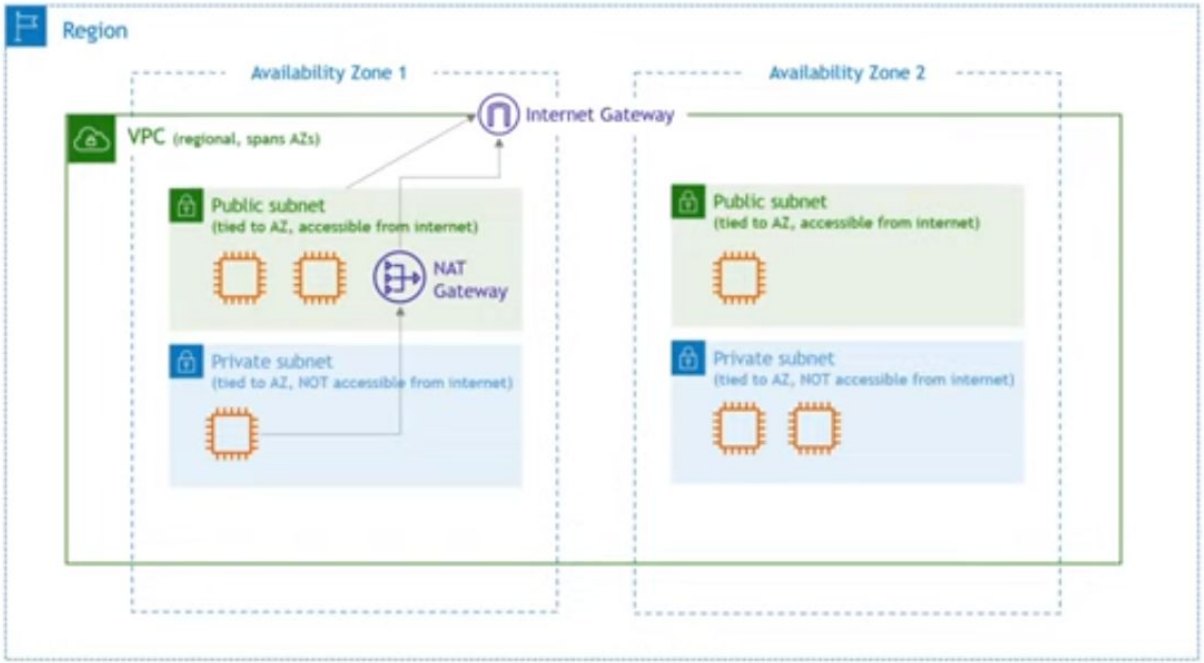
But what if you do need to get to the internet for something, maybe to do updates or downloading files, you still do not want the outside world getting in but you need to get out of certain things



In that case you need to use NAT Gateway and that stands for Network Address Translation. You create a NAT Gateway in your public subnet



And then you add a route from your private instance to it.



Then you add a route from the NAT Gateway to the Internet Gateway.

That is how you enable internet access for your resources in your private subnet

Now let's look at the network ACL and Security groups

ACL means Access Control Lists

Security Groups - acts as a virtual firewall for your EC2 instances to control incoming and outgoing traffic. Both inbound and outbound rules control the flow of traffic to and traffic from your instance, respectively.

These are similar and they both protect your AWS resources but there is some key differences.

Network ACL is a firewall that is attached at the subnet level

You will see on the following diagram

Network ACLs and Security Groups

NETWORK ACLs

Firewall that controls traffic in/out of a ***subnet***

Rules for ***Allow*** and ***Deny***

Rules include IP addresses (only)

This is how we secure everything

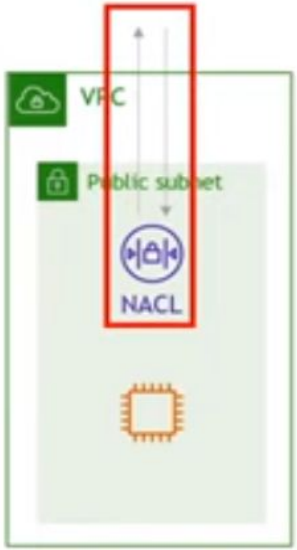
Network ACLs and Security Groups

NETWORK ACLs

Firewall that controls traffic in/out of a ***subnet***

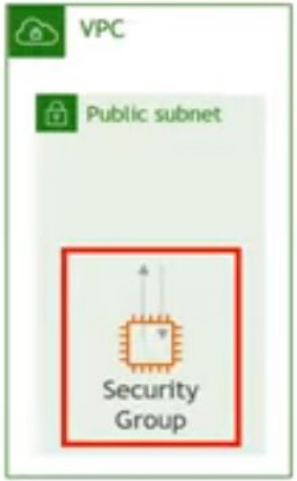
Rules for ***Allow*** and ***Deny***

Rules include IP addresses (only)



SECURITY GROUPS

Firewall that controls traffic in/out of an ***EC2 instance***



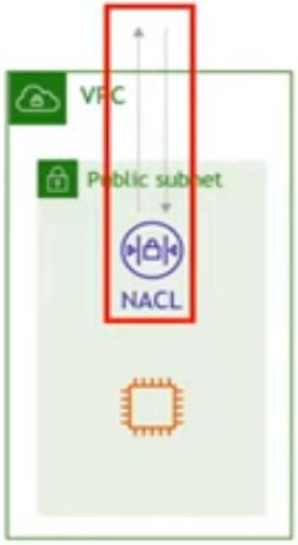
Network ACLs and Security Groups

NETWORK ACLs

Firewall that controls traffic in/out of a ***subnet***

Rules for ***Allow*** and ***Deny***

Rules include IP addresses (only)



SECURITY GROUPS

Firewall that controls traffic in/out of an ***EC2 instance***

Rules for ***Allow*** (only)

Network ACLs and Security Groups

NETWORK ACLs

Firewall that controls traffic in/out of a ***subnet***

Rules for ***Allow*** and ***Deny***

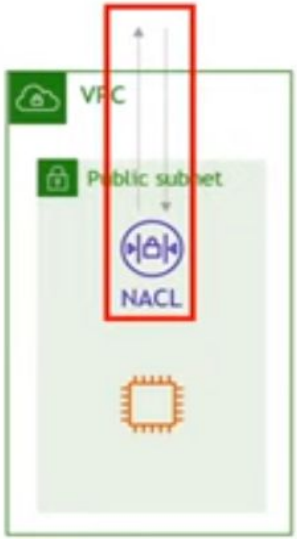
Rules include IP addresses (only)

SECURITY GROUPS

Firewall that controls traffic in/out of an ***EC2 instance***

Rules for ***Allow*** (only)

Rules include IP addresses ***AND*** other security groups



VPC can offer many benefits for organizations looking to improve their infrastructure. These benefits include improved security, greater flexibility, and scalability. However, VPC is not without its drawbacks, including cost, complexity, and dependence on the Internet.

THANK YOU

END