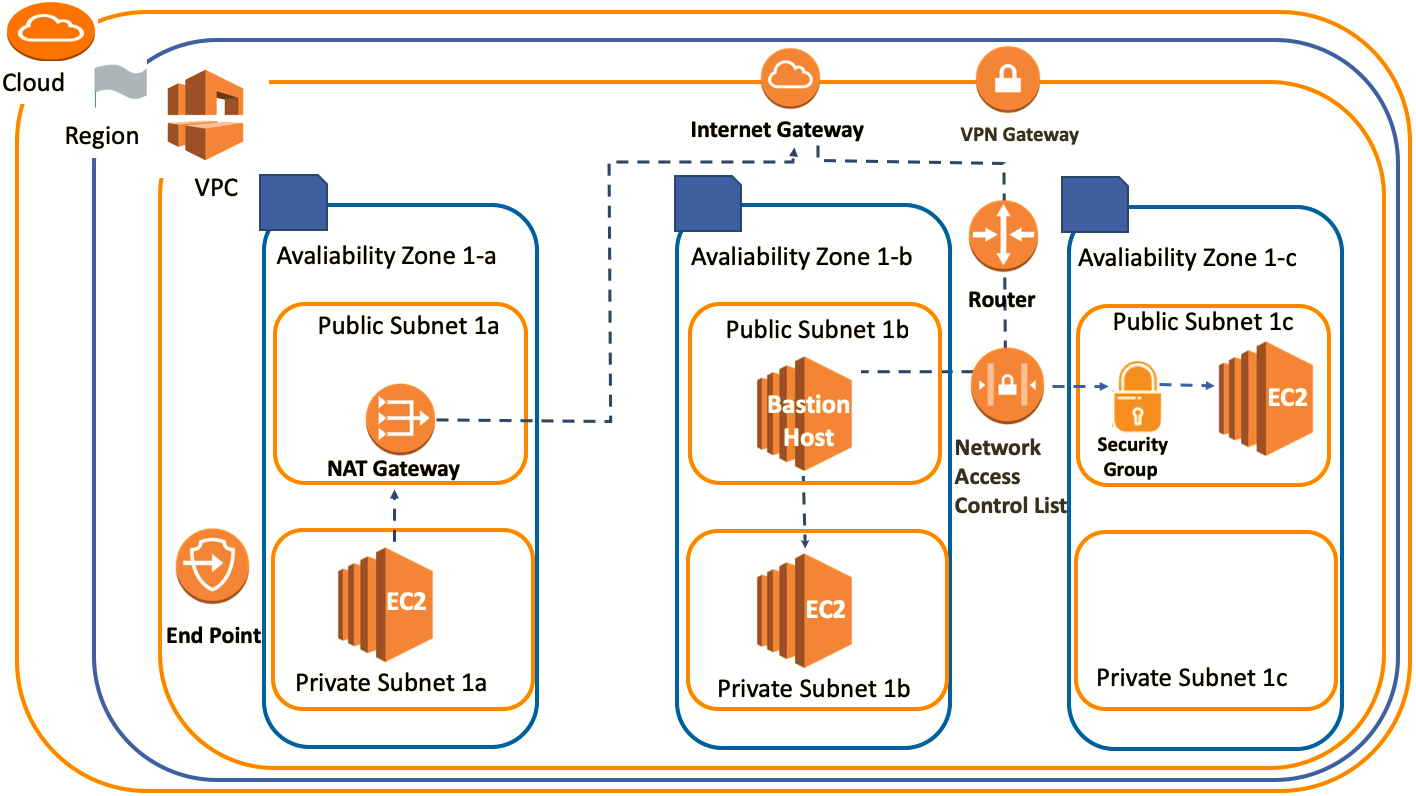
Introduction to VPC

We can provide the communication part of physical networks that we create through devices such as switches, routers, repeaters, firewalls, load balancers connected by network cables.

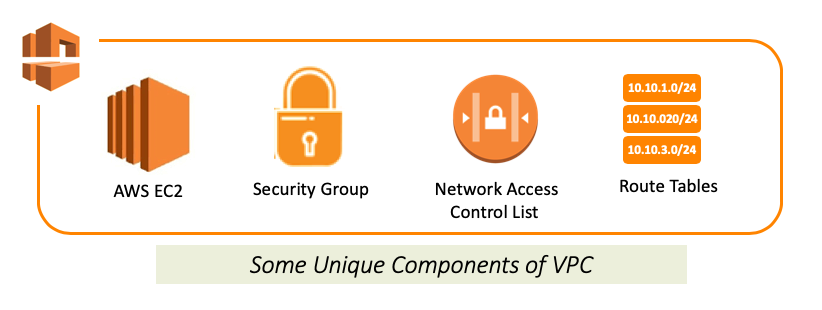
But when it comes to the cloud, there is no longer a physical network that we access and configure. There are virtual structures that simulate this physical network and allow us to build logical structures on it. In the AWS world, this is called VPC.

Briefly, Amazon Virtual Private Cloud (Amazon VPC) is a logically isolated area of the AWS cloud where you can launch AWS resources in a virtual network that you define. So, VPC provides much better security control over your AWS resources.

### **Architecture of VPC**



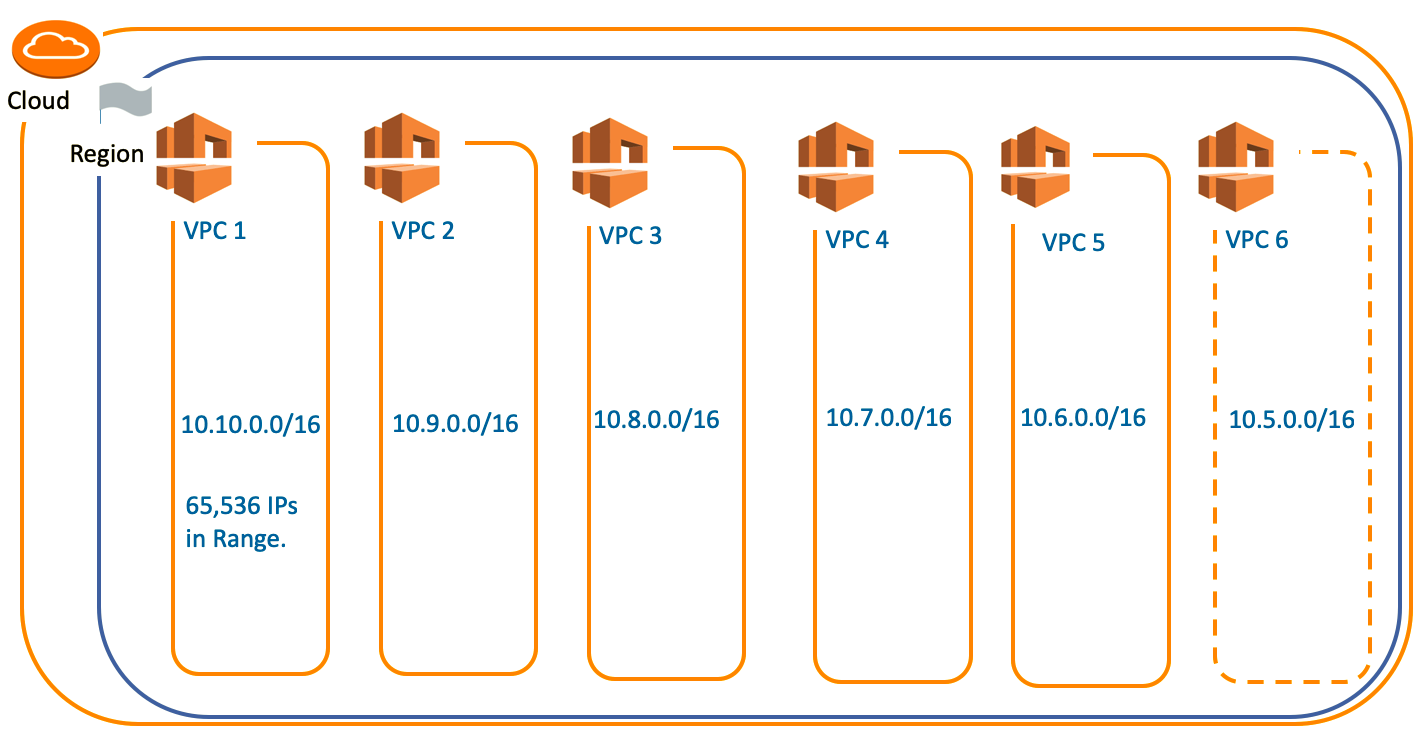
### **VPC Structure**



VPC is a layer of a virtual network where we can create our own private network structure, run our resources and logically isolated. Thus, VPC allows full control over your virtual network environment, including choosing your own IP address range, creating subnets, configuring route tables and gateways.

VPC is a unique area. So when you create or set something associated with VPC, it means these things can only work harmoniously in this environment.

### **VPC Region&AZ**



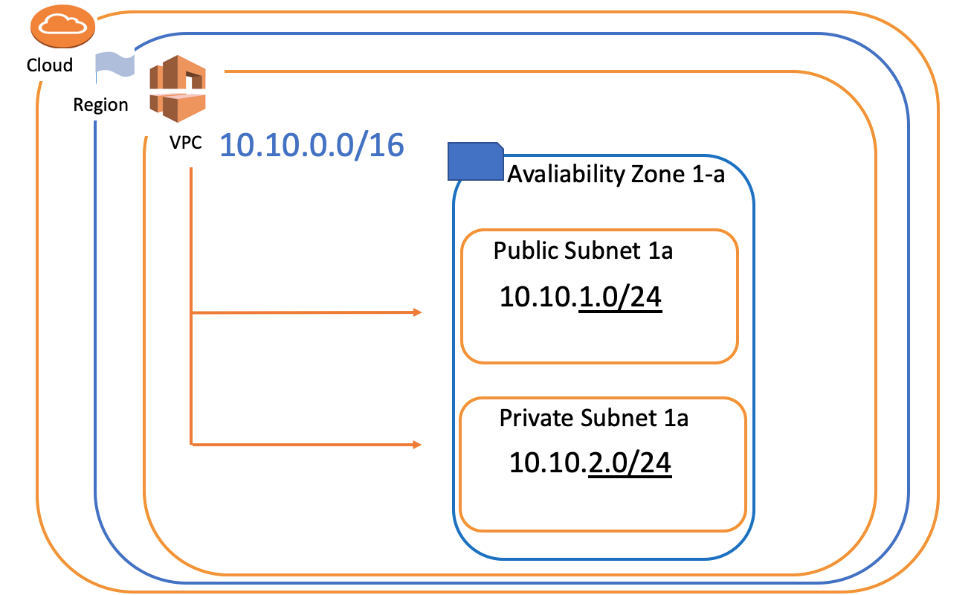
AWS has the concept of a Region, which is a physical location around the world where data centers are clustered. Each AWS Region consists of multiple, isolated, and physically separate AZ's within a geographic area as you remember in the **Getting Started with AWS** section.

Each region; it comes with one default VPC and we can also create 5 more VPCs for each region. This is a soft limit of 5 and if we need more than 5 VPCs, we can request it from AWS.

VPCs are associated with a single region. You cannot span a VPC across regions.

### **VPC Subnets**

A subnet is a range of IP addresses in your VPC.



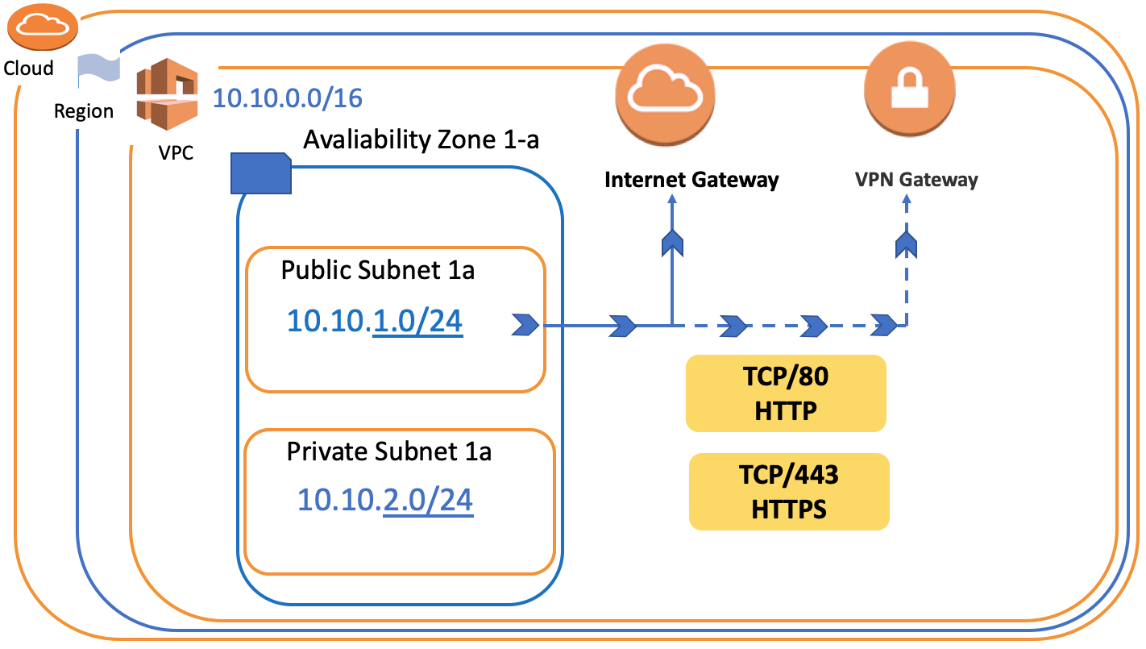
We divide the main IP block that we define in VPC into sub-logical networks called a subnet. In this way, we can easily cluster the components with the same properties.

Subnets can be 2 types: **Public Subnet** and **Private Subnet**.

* When we say Public Subnet, the virtual machines that we place in the subnets can be accessed from the outside of the VPC (Public internet).
* The machines we place in the subnets called Private have the opportunity to communicate only through VPC. In this way, we protect our resources against unauthorized access and ensure network security.

In addition, each subnet can be created only in a specific AZ (Availability Zone). A subnet cannot be associated with more than one AZ.

**Internet Gateway & VPN Gateway**

****

Let's say we created our VPC and subnets. But how do we get them to connect to the internet? The answer is Internet Gateway or VPN Gateway.

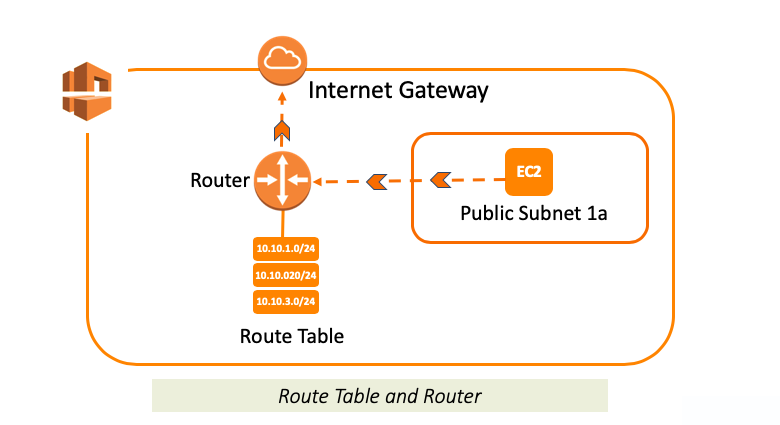
An **Internet Gateway** is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet.

We can think of internet gateways as basic internet providers with our ADSL or fiber routers that allow us to access the internet in our home.

Besides, this internet connection can be made as a direct connection between its own company network infrastructure and this VPC. This system is also called a **VPN Gateway**.

In short, VPC can connect to the outside world in two basic ways, either VPN Gateway or Internet Gateway.

**Route Table and Router**

****

**Route Table** is a set of rules, that is used to determine where network traffic is directed. It provides all traffic routing under VPC.

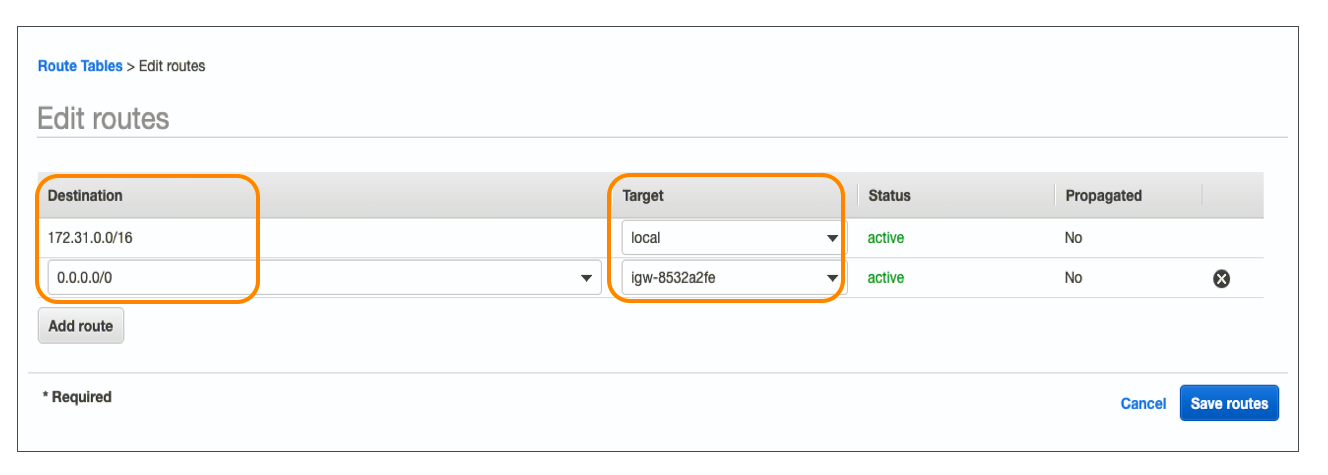
Route Table is roughly configuration files that explain how to go from destination X to destination Y or to the internet and which way to use.

**Routers** are components that manage the Route Tables and they act as “intersections” within the network.

Each AWS VPC has a VPC router.

Briefly, if we consider Route Table as a set of rules, then Router is executive of these rules.

Here, the example of the Route Table seen below.



If you want to reach somewhere in Destination Column you'll be directed to the value in Target Column

For example, You can reach **0.0.0.0/0 (Anywhere in Internet)** by using **igw-8532a2fe (Internet Gateway)** thanks to this route table.

### **Network ACLs**



Network ACL stands for Network Access Control Lists. It is a security component for your VPC that controls the traffic in and out of subnets. In other words, Subnet Network ACLs are **firewall of subnets**

Network ACLs are **subnet-based** security components.

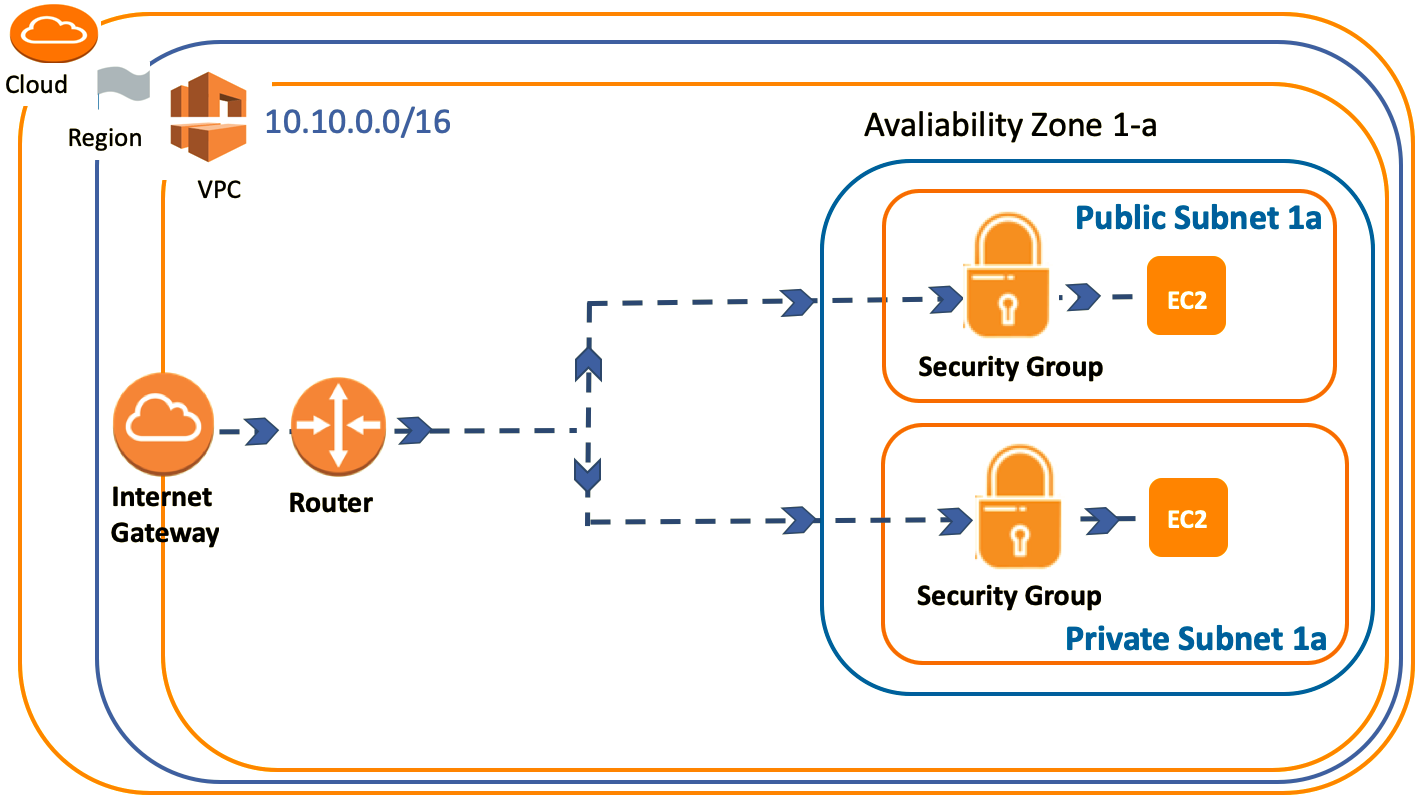
Your VPC automatically comes with a modifiable default Network ACL. **By default**, it **allows** all inbound and outbound IPv4 traffic.

* Unlike default Network ACL, If you want to create a new one, it denies all the inbound and outbound traffic until you add rules

Each subnet in your VPC must be associated with a Network ACL. If you don't explicitly associate a subnet with a Network ACL, the subnet is automatically associated with the default Network ACL.

You can associate multiple subnets with a Network ACLs. However, a subnet can be associated with the single Network ACL.

### **Security Groups**



In addition to the Network ACLs, we can also create Security Groups in VPC for security precautions.

Security Groups, also mentioned in the EC2 section, are used for determining which traffic will access the instance.

In other words, a Security Group is a virtual **Firewall of Instance**.

Security Groups are **instance-based** components, while Network ACLs are the subnet-based. So, you need to consider both Security Groups and Network ACLs about the inbound and outbound traffic for instance in any subnet.

Each instance in a subnet in your VPC can be assigned to a different set of security groups. When you launch an instance in a VPC, you can associate with **five** security groups to one instance.

We will see more details and implementation of Network ACL and Security Groups in the following lessons. So that's enough for now.