Introduction to VPC

What is VPC?

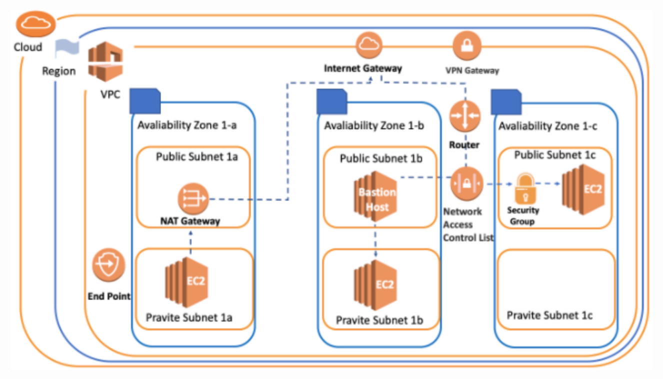
Amazon Virtual Private Cloud (Amazon VPC)

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

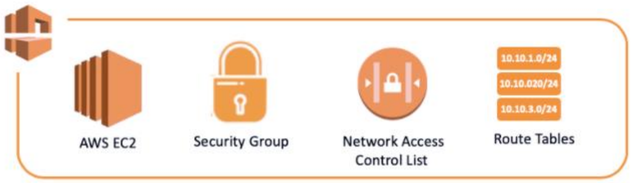


Architecture of VPC

The picture seen above shows the Architecture of VPC. In the following lessons, we'll see how to create VPC and the work methodology of its components, based on this architecture.

VPC and Components

VPC Structure

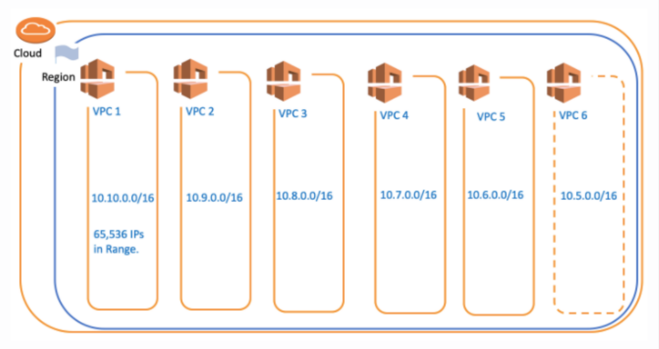


Some Unique Components of VPC

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



VPC

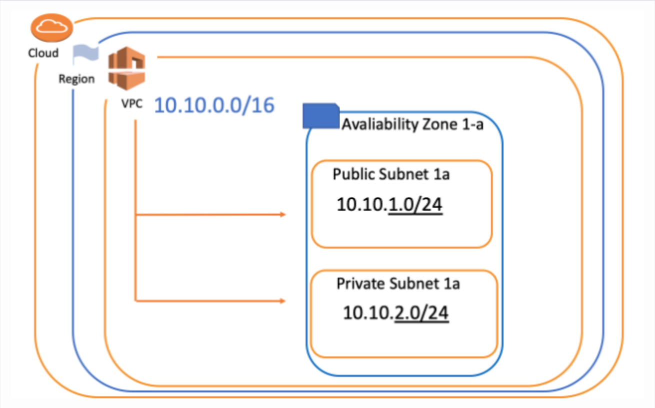
AWS has the concept of a Region, which is a physical location around the world where data centers are clustered. Each AWS Region consists of multiple, isolated, and physically separate AZ's within a geographic area as you remember in the **Getting Started with AWS** section.

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.

AWS now spans 76 Availability Zones within 24 geographic regions around the world and has announced plans for sixteen more Availability Zones and five more AWS Regions in Indonesia, Italy, Japan, South Africa, and Spain.

VPC Subnets



Subnet

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

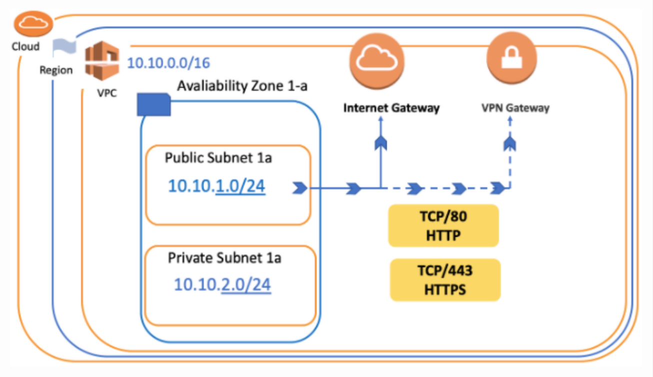
We divide the main IP block that we define in VPC into sub-logical networks called a subnet. In this way, we can easily cluster the components with the same properties.

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



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.

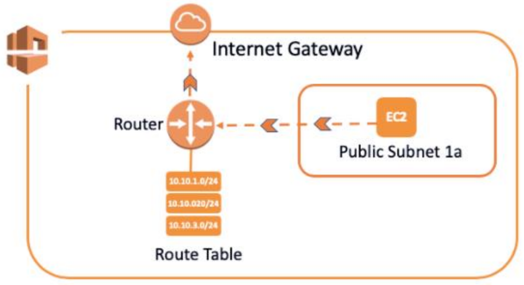
An **Internet Gateway** is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet.

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 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.

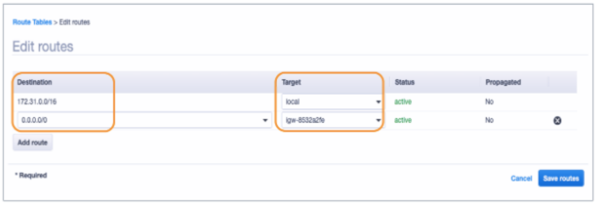
Route Table is roughly configuration files that explain how to go from destination X to destination Y or to the internet and which way to use.

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.



Route Tables > Edit routes

Edit routes

Destination	Target	Status	Propagated
172.31.0.0/16	local	active	No
0.0.0.0/0	igw-8532a2fe	active	No

Route Table

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 Access Control List

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.

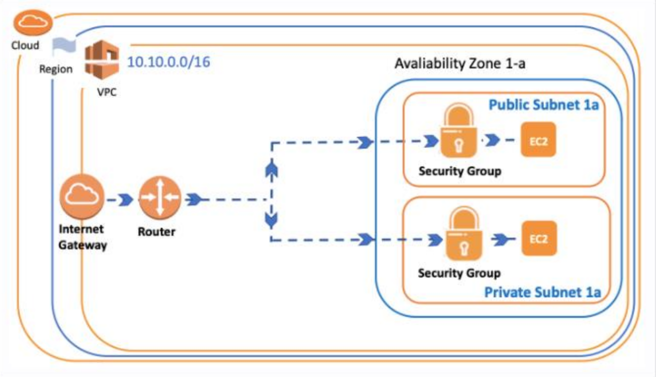
⚠Avoid ! :

- 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



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.

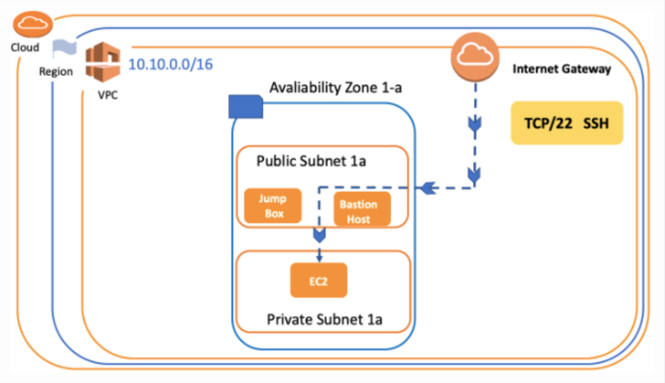
In other words, a Security Group is a virtual **Firewall of Instance**.

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.

Bastion Host/Jump Boxes



Bastion Host/Jump Boxes

As the name suggests, Private Subnet is closed to Public internet. But, sometimes we need to access the instance located in Private Subnet. So we use a proxy server/instance, Bastion Host, for this job.

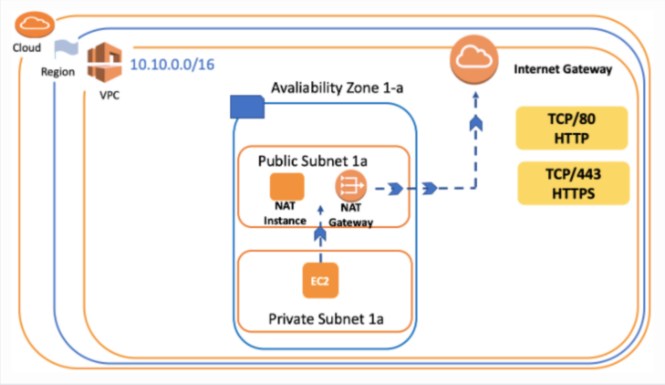
A Bastion Host is a server/instance that is used to ensure access to a Private subnet from the Internet.

Bastion Host is launched in **Public Subnets** and acts as a proxy for the instances in a **Private Subnet**. It provides security by reducing the attacks on your infrastructure.

A Bastion Host is used to administer EC2 instances using SSH or RDP securely. It is also known as **Jump Box**.

Bastion Host/Jump Boxes are used for **Inbound** traffic to the instance in Private Subnet.

VPC NAT Gateway & NAT Instance



NAT Gateway & NAT Instance

NAT stands for Network Address Translation in AWS.

You can't directly connect the internet if your instance is in a Private Subnet. Because of the security precaution, your private subnet blocks the outbound internet connectivity.

But, we can use **NAT Gateways** or **NAT Instance** which created in the Public Subnet as a proxy to tackle this problem.

So if you want to connect from EC2 instance in the private subnet to the internet, you need to create NAT Gateways or NAT Instance in Public Subnet. Then you'll obtain connectivity to your EC2 Instance via these components.

But it is important that a NAT instance and NAT Gateways allow your private instances to **outbound internet connectivity** while **blocking internet inbound** traffic.

NAT Instance:

NAT Gateways or NAT Instance are pretty much similar things and they provide the same functionality, however, a NAT Gateway is an AWS managed NAT service but NAT Instance is specified and managed by the customer.

In fact, NAT Gateways are widely used in real-time than NAT instances, and NAT Gateways are highly accessible across multiple availability zones.

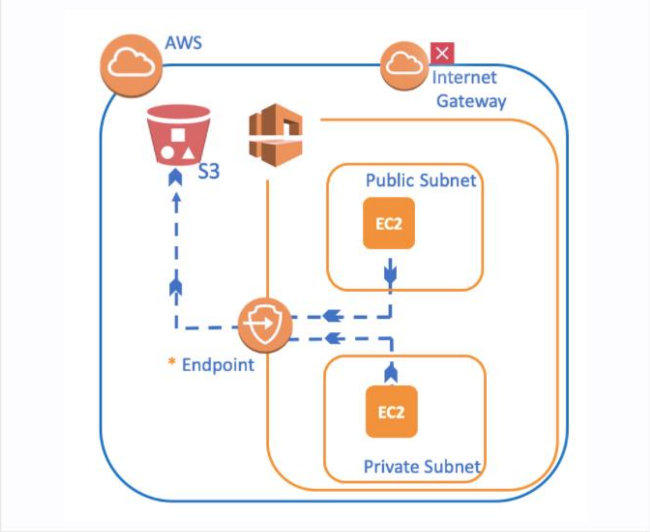
⚠Avoid ! :

- You cannot use NAT Gateway as a Bastion host. If you connect with SSH or RDP to an instance in a private subnet, you need to configure a Bastion Host. You cannot use NAT Gateway.

💡Tips:

- While Bastion Host/Jump Boxes are used for Inbound traffic, NAT Gateway/NAT Instances are used for Outbound traffic.

VPC Endpoint



VPC Endpoint

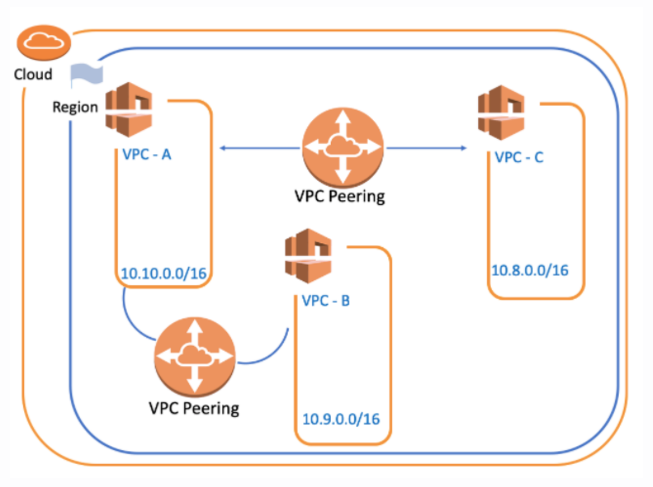
The VPC Endpoint is a component that allows you to privately connect your VPC to supported AWS services such as S3.

In fact, traffic between your VPC and the other service does not leave the Amazon network. So in this virtual environment, AWS offers us such a shortcut.

VPC Endpoint is a horizontally scaled, redundant and highly available VPC component. Thus it allows communication between instances in your VPC and services without imposing availability risks or bandwidth constraints on your network traffic.

Thanks to VPC Endpoint, Instances in your VPC do not require public addresses to communicate with the resources in the service. Because, VPC Endpoint services powered by PrivateLink without requiring an internet gateway, VPN Connection, etc.

VPC Peering



VPC Peering

A VPC peering is a networking connection between two VPCs.

It enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in different VPC can communicate with each other as if they are within the same network.

Peering between the two VPC is peculiar to them. Let's evaluate the picture seen above to understand what it means.

Suppose that you have already had VPC Peering between VPC-A and VPC-B. If you create new VPC peering between VPC-A and VPC-C, connectivity between VPC-B and VPC-C does not occur automatically. You need to create another VPC peering between VPC-B and VPC-C for their connectivity.

Elastic IP

Elastic IP

An Elastic IP address is a **Static IPv4 Address** designed for dynamic cloud computing. In short, Elastic IP is a permanent IP for your instance.

Public IP addresses are dynamic. If you stop/start your instance you get reassigned a new public IP. But, Elastic IPs get allocated to your account and stay the same.

Elastic IPs are dynamically re-mappable IP addresses so it's up to you to attach them to another instance or not.

But, why do we need Elastic IP?

We use Elastic IPs for various reasons, especially because of its advantages or situations where it is compulsory to use.

For example;

- We may prefer to assign a license to Elastic IP address,
- It may be a legal requirement for some applications to use static IP.
- Some AWS components such as NAT Gateway and Route 53 may need Elastic IP while the process of creating, operating or setting up.

But for now, the part that interests us will be **NAT Gateways** and we'll see this in the following lessons in detail.

⚠Avoid ! :

- Elastic IPs are totally free as long as they are being used by an instance. However, Amazon will charge you $0.01/hr for each EIP that you reserve and do not use. So don't forget to terminate the Elastic IP or associated component such as NAT Gateway if you'll not use anymore in the short term.

Complementary Lesson about VPC