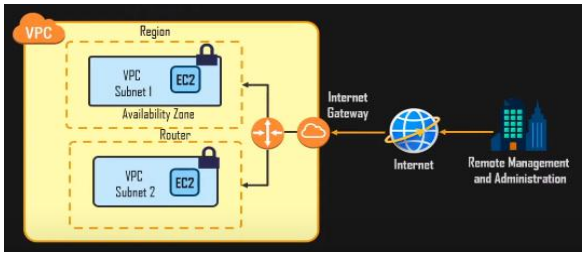
# Amazon Virtual Private Cloud

## 1. Introduction

Amazon Virtual Private Cloud (VPC) is a service that provides a private environment where we can define our own network and use AWS services that are relevant to us. Amazon VPC lets us provision a logically isolated section of the AWS Cloud where we can launch AWS resources in a virtual network that we define. This virtual network resembles a traditional network that we'd operate in our own data center, with the benefits of using the scalable infrastructure of AWS. VPC can be spread in all the availability zones within a region. VPC, generally being a large network is divided into smaller chunks which is known as subnets. We can select the IP address range, create subnets, configure root tables, set up network gateways, define security settings using security groups, and network access control lists. (Amazon, 2021)




In this picture, it is shown that the VPC is spread among the two availability zones.

## 2. Benefits of using a VPC in general

As VPC provides an extra layer of security where people can define their own networks, it has its own perks. Major perks are explained below:

i. Privacy.

ii. Security.

iii. Prevention of loss of proprietary data.

iv. Very simple to set-up and implement.

v. Customizable virtual network.

3. **Advantages of using a VPC instead of a Private Cloud**
    i. Scalability: Public cloud provide hosts a VPC due to which it would be very easier for customers to add more computing resources on demand.
    ii. Better Performance: Cloud-hosted websites and applications often tend to perform better than those that are hosted in local premises.
    iii. Better Security: This can either be an advantage or a disadvantage. It is an advantage especially for small and mid-market businesses because the cloud providers that offer VPCs have more resources for updating and maintaining the infrastructure. It could also be a disadvantage for such companies the face extremely tight data security regulations. (Cloudflare, 2021)

4. **Use Cases of VPC**

1. A simple public website can be hosted in no time.
2. Multi-tier web applications can be hosted.
3. Backup and recover the data in case of a disaster.
4. Extending a corporate network into the cloud.

5. **Key Components of VPC**

**Internet Gateway and NAT**: It logically enables routing of traffic in the public network. It helps the VPC connect to the internet.

**DNS**: It is a standard which resolve names used over the Internet into IP address.

**Elastic IP**: It is a static IP that never changes. (Only supports IPv4).

**VPC Endpoints**: Private connection between the created VPC and AWS services without using the internet.

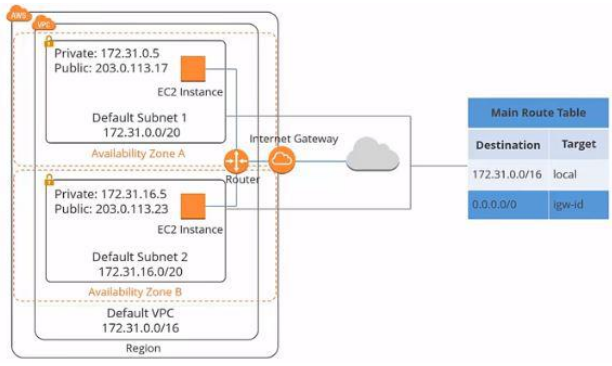
**Network Interface**: It is a point of connection between a public and a private network.

6. **Types of VPC**

### 1. Default Amazon VPC

Each Amazon account comes with a default VPC that is pre-configured for us to start using immediately. A VPC can span multiple availability zones in a region. In the first section, there is a default Amazon VPC. The CIDR block for the default VPC is always a 16-subnet mask; in this example, it's 172.31.0.0/16. It means this VPC can provide up to 65,536 IP addresses.

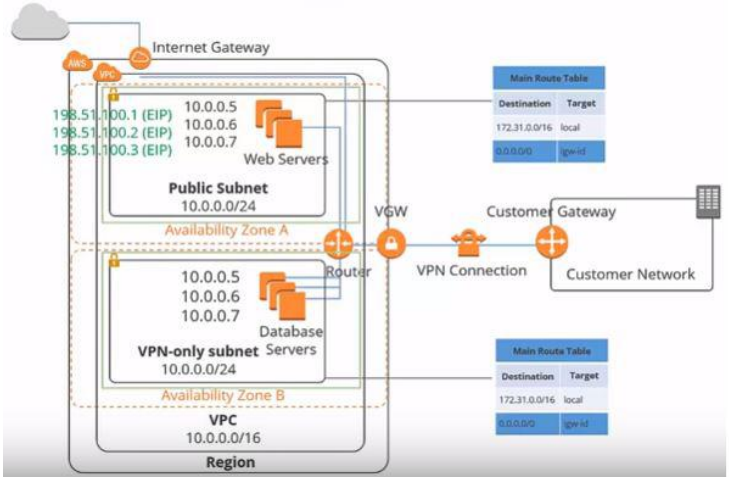
This is the diagram of a default VPC:




### 2. Custom Amazon VPC

The default VPC is suitable for launching new instances when we are testing AWS, but creating a custom VPC allows us to:

- Make things more secure
- Customize your virtual network, as we can define your own our IP address range
- Create your subnets that are both private and public
- Tighten security settings




## 7. Creation Process

A Public-Private VPC can be created and deployed with AWS Elastic Beanstalk. An Amazon VPC can contain both public and private subnets. The instances in the public subnet can send outbound traffic directly to the Internet, whereas the instances in the private subnet can't. The public subnet contains an Amazon EC2 instance that performs network address translation (NAT) to enable instances in the private subnet to communicate with the public internet. The two subnets must reside in the same Availability Zone (AZ).

## 8. Connection to the Amazon VPC

VPC endpoints enables users to privately connect their VPC to services hosted on AWS without requiring an Internet gateway, a NAT device, VPN, or firewall proxies. Endpoints are horizontally scalable and highly available virtual devices that allow communication between instances in their VPC and AWS services. Amazon VPC offers two different types of endpoints: gateway type endpoints and interface type endpoints.

Gateway type endpoints are available only for AWS services including S3 and DynamoDB. These endpoints will add an entry to their route table they selected and route the traffic to the supported services through Amazon's private network.

Interface type endpoints provide private connectivity to services powered by PrivateLink, being AWS services, their own services or SaaS solutions, and supports connectivity over Direct Connect.

The other connectivity options for the Amazon VPC are as follows:

a. The internet (via an internet gateway)
b. A corporate data center using an AWS Site-to-Site VPN connection (via the virtual private gateway)
c. Both the internet and the corporate data center (utilizing both an internet gateway and a virtual private gateway)
d. Other AWS services (via internet gateway, NAT, virtual private gateway, or VPC endpoints)
e. Other Amazon VPCs (via VPC peering connections)

Since, the instances without the public IP addresses can also access the internet, here is how it is made possible:

a. Instances without public IP addresses can route their traffic through a NAT gateway or a NAT instance to access the Internet. These instances use the public IP address of the NAT gateway or NAT instance to traverse the Internet. The NAT gateway or NAT instance allows outbound communication but doesn't allow machines on the Internet to initiate a connection to the privately addressed instances.

b. For VPCs with a hardware VPN connection or Direct Connect connection, instances can route their Internet traffic down the virtual private gateway to your existing datacenter. From there, it can access the Internet via your existing egress points and network security/monitoring devices.

## References

Amazon, 2021. *Amazon Virtual Private Cloud.* [Online]
Available at: https://aws.amazon.com/vpc/?vpc-blogs.sort-

by=item.additionalFields.createdDate&vpc-blogs.sort-order=desc
[Accessed 12 03 2021].

Cloudflare, 2021. *What is a Virtual Private Cloud.* [Online]
Available at: https://www.cloudflare.com/learning/cloud/what-is-a-virtual-private-cloud/
[Accessed 18 March 2021].