Amazon Virtual Private Cloud

What is Amazon VPC?

Amazon Virtual Private Cloud

What is Amazon VPC?

VPC stands for Virtual Private Cloud.
Amazon Virtual Private Cloud (Amazon VPC) provides a logically isolated area of the AWS cloud where you can launch AWS resources in a virtual network that you define.
You have complete control over your virtual networking environment, including a selection of your IP address range, the creation of subnets, and configuration of route tables and network gateways.

Amazon Virtual Private Cloud

What is Amazon VPC?

You can easily customize the network configuration for your Amazon Virtual Private Cloud. you can create a public-facing subnet for web servers that can access to the internet and can also place your backend system such as databases or application servers to a private-facing subnet.
You can provide multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

Amazon Virtual Private Cloud

Advantages of Amazon VPC

Provide constant scalability and reliability by making the resources up and down as per your requirement.

Higher-level managed services.

It provides advanced security options and enables storing your data securely with inbound and outbound filtering, security groups, and a network access control list.

You can pay for what you use. So it requires only a minimum operating cost.

Simple and user-friendly.

Amazon Virtual Private Cloud

- A VPC is your private network within AWS. A VPC isolates your resources from everyone else's.
- Each AWS account comes with a default VPC that is pre-configured for you to start using immediately. A VPC can span multiple availability zones in a region.
- A VPC only exists in one AWS region.

Amazon Virtual Private Cloud

- IGW

Internet Gateway is a VPC component that allows communication between your VPC and the Internet.
An Internet Gateway is a logical connection between an AWS VPC and the Internet. There is no underlying physical resource.
Each VPC has only one Internet Gateway. If a VPC doesn't have an Internet Gateway, then resources cannot be accessed from the Internet.

Amazon Virtual Private Cloud

- Subnetwork or subnet

The subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting. provides two types of subnetting one is Public which allows the internet to access the machine, and another is private which is hidden from the internet.

Amazon Virtual Private Cloud

- Subnetwork or subnet

1. AWS reserve 4 IP address (first 3 and last 1 IP address) in each subnet
2. These 4 IPS are not available for use and cannot be assigned to an instance

Example: if 10.0.0.0/24, reserved IPs are:
10.0.0.0: Networks
10.0.0.1: reserved by AWS for VPC Router
10.0.0.2: reserved by AWS for mapping amazon provided DNS
10.0.0.3: reserved by AWS for future use
10.0.0.255: Network broadcast address

Amazon Virtual Private Cloud

- IP Address

IP (Internet Protocol) addresses are used to identify hardware devices on a network. The addresses allow these devices to connect to one another and transfer data on a local network or over the internet.

- Route Table

A route table contains a set of rules, called routes, that determine where network traffic from your subnet

CIDR: a collection of IP addresses

Amazon Virtual Private Cloud

- Demo
- Creating VPC
- 10.0.0.0/16
- Creating IGW
- Attach IGW to VPC
- Creating Subnet
- 10.0.1.0/24 and 10.0.2.0/24
- Enabling public ip in the subnet
- Create a public route table to IGW

	Private address range	
Class	start address	finish address
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

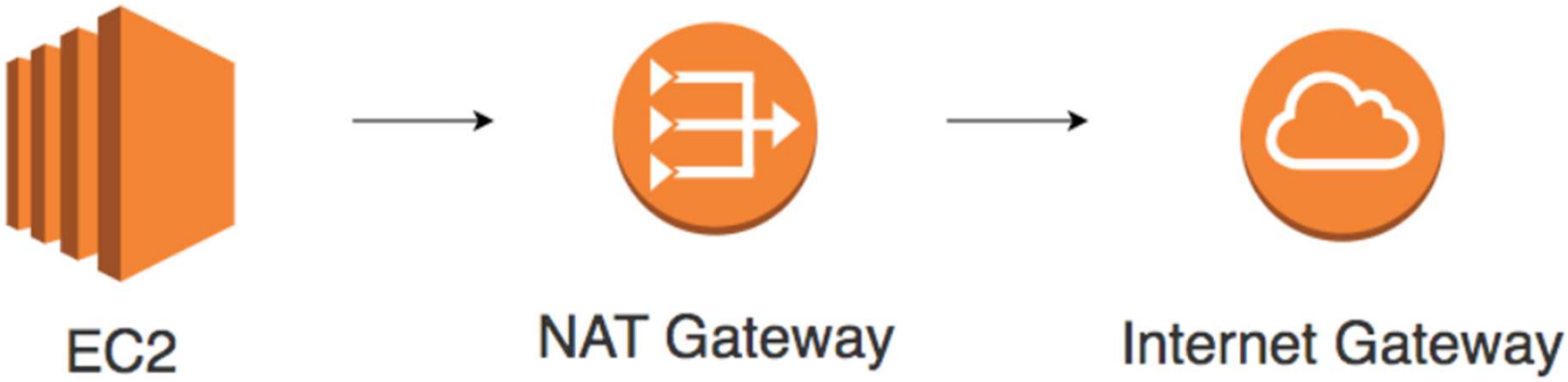
	Public address range	
Class	start address	finish address
A	0.0.0.0	126.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	223.255.255.255
D	224.0.0.0	239.255.255.255
E	240.0.0.0	254.255.255.255

Amazon Virtual Private Cloud

VPC
That means a “10.0.0.0/16” leaves the remaining 16 bits (or the last two numbers) free to use for specific addresses

Subnet
10.0.1.0/24: Includes ranges 10.0.1.1–10.0.1.254 (can assign the last number)

Amazon NAT Gateway



AWS NAT Gateway

What is AWS NAT Gateway?

NAT Gateway, also known as Network Address Translation Gateway, is used to enable instances present in a private subnet to help connect to the internet or AWS services. In addition to this, the gateway makes sure that the internet doesn’t initiate a connection with the instances. NAT Gateway service is a fully managed service by Amazon, that doesn’t require any efforts from the administrator.

AWS NAT Gateway

What is AWS NAT Gateway?

A NAT gateway in a device forwards the traffic from instances present in the private subnet to the internet and sends back the response from the server back to the instance. When the traffic moves to the internet, an IPV4 address gets replaced with the NAT's device address. Once the response is obtained, it has to be sent to the instance, and in this case, the NAT device translates the address back to the IPV4 and it is given to the IPV4 address.

AWS NAT Gateway

What is AWS NAT Gateway?

Your private network can communicate with other public networks with the help of NAT Gateways. They can be used for sending and receiving traffic from a single IP address while keeping hosts' identities private.

All the Instances within your private network are protected with the help of NAT Gateways, as it blocks incoming traffic and allows outgoing traffic.