VIRTUAL PRIVATE CLOUD

VPC

AWS Vpc (virtual private cloud) that allows you to create virtual private network in the cloud.it gives you full access over your networking environment allowing you to define your IP range also to create subnet and manage routing table. With vpc you can surely connect your resources to the internet or keep them isolated from the external traffic depending on your needs.it is like building your private data center within AWS

Regions

- Region in AWS is the physical location in the world (eg. Mumbai and Hyderabad Region)
- It contains multiple Availability zones

```
+------------------------------+
|          AWS Region          |
|  (e.g., ap-south-1 Mumbai)    |
|                              |
|  +------------------------+  |
|  |    Availability Zone   |  |
|  |       (e.g., AZ-a)     |  |
|  |                        |  |
|  |  +------------------+  |  |
|  |  |  Public Subnet   |  |  |
|  |  |  (10.0.1.0/24)   |  |  |
|  |  +-------------------+  |  |
|  |                  |  |
|  |  +-------------------+  |  |
|  |  |   Private Subnet  |  |  |
|  |  | (10.0.2.0/24)    |  |  |
|  |  +-------------------+  |  |
|  +------------------------+  |
|                         |
+------------------------------+
```

Availability Zones

AZ is a collection of data centers there are two or three data centers in one availability zone.

In Mumbai Region there are three availability zones

- ap-south-1a
- ap-south-1b
- ap-south-1c

If one zone completely shuts down than all the requests are diverted to the other AZ. all these zones are far away from each other within few kilometers but are connected to each other through the fiber optic cable

Subnets

Subnets in AWS is the smaller segmented portion of vpc that divides your network into smaller IP ranges to manages, organize and secure resources more efficiently.

- Subnets are created within the vpc.
- It has own IP address range.
- Each subnet exist one AZ.

Public subnet

Public subnet is a subnet where resources like ec2 instances can directly communicate with internet. This subnet has route table to inertnetgateway attached to vpc. Resources like web server and load balancer are placed in public subnet because they need access from the internet

Private Subnet

This subnet typically contains resources which cannot be directly exposed to the internet. If these resources needs internet this can be done through the Nat gateway in a public subnet which acts as a proxy server for internet traffic.

CIDR

Classless Inter-Domain Routing it defines the range to IP address using the combination if ip address and fixed length

Sub netting with cidr divides larger network into the smaller subnets

Route Table

Route Table in AWS is a navigation map that tells your vpc how to direct traffic to your subnet, internet and other network.

Key Reason to use route table

1. Traffic Direction

Route table defines how traffic enters and leaves subnet

For example: ec2 instance subnet wants to send data to internet the route table must have route to the internet-gateway.

2. Control Over Connectivity

- Subnets
- Internet gateway
- Nat gateway

- VPC Peering

Jump Server

Jump server is typically placed in public subnet. And it allows you to connect to the resources in private subnet that does not have direct internet access.

Internet gateway

Internet gateway in AWS allows your vpc to connect to internet. To enable internet access for a subnet, its associated route table must have a route pointing to the internet gateway.

How does Igw works?

1. Attach internet gateway to vpc for internet access.
2. EC2 instance must have public or elastic ip to be reachable to the internet
3. Security group NACL you need to allow traffic (ssh and http) through your security group and NACL.
4. When someone tries to access ec2 public instance the request must come from igw. Igw forwards request via vpc to network the instances responds back through igw to the user.

DHCP

Dynamic host control protocol it is used to assign automatically ip address and other network configuration to device on a network.

How it works?

1. DHCP Discover

Client sends broadcast message to locate DHCP server.

2. DHCP Offer

DHCP responds with available ip address and other configuration.

3. DHCP Request

Client requests to accept available ip address.

4. DHCP Acknowledge

Server confirms and assign available ips to the client

This is known as DORA process.

Why it is useful?

- Automatic ip management.
- Prevents ip conflict.
- Makes device network easy and usable.

- Used in home network enterprises LAN and Cloud environment.

Nat gateway

Nat gateway is AWS allows resources in a private subnet to connect to the internet but prevent internet connecting back to those resources. Nat gateway acts as a communication link between public and private subnet.

How does it work?

We assign Nat gateway to the public subnet. Resources in private subnet needs internet access once the request is sent to public subnet through the Nat gateway it prevent the internet connecting back to resources.

NACL

Network Access Control List.one such security feature provided by AWS is NACL. It is defined by default for your vpc, however you can create custom NACL according to the requirement. NACL defines inbound and outbound rule for the subnet present in vpc.

However these have same functions such as security group only difference is NACL is at subnet level and security group is at ec2 instances.

How does it work?

Suppose you have created vpc and two subnets. Subnet one and subnet two now you have to give permission to work with subnet two this can be only done with NACL. Only permitted users will have access to subnet two after verifying IP address.

Difference between security group and NACL.

1. Security Group

- It works at instance level.
- Supports allow rule.
- It is state full return traffic is allowed regardless of any rule.

2. NACL

- It works at subnet level.
- Supports allow and deny rules.

- It is stateless return traffic must be explicitly allowed by the rules.