AWS
Virtual Private Cloud (VPC)

Virtual private cloud a private, isolated network within the AWS cloud where you can launch and manage your resources. Securely.

→ where you can define your own virtual network.

→ In VPC you control:
- IP address
- Subnets
- Route tables
- Network gateways
- Security

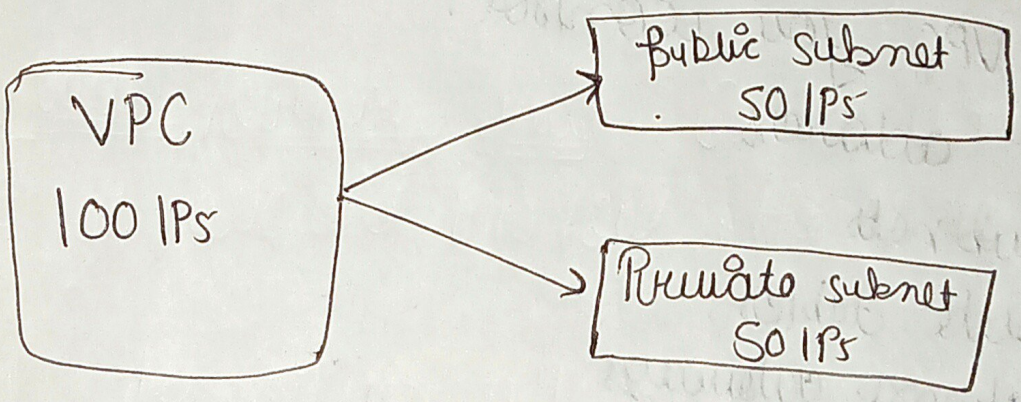
Key Components

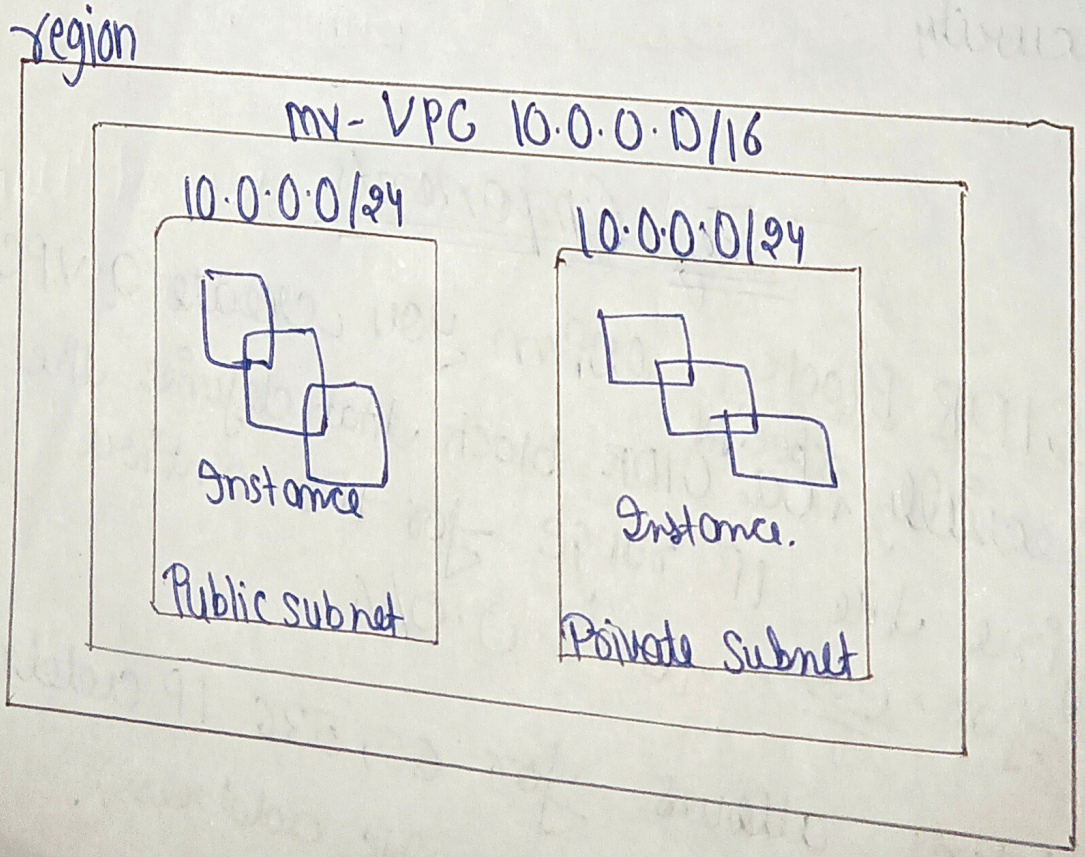
1. VPC CIDR Block :- when you create a VPC, you specially specify a CIDR block that defines the the define the IP range for the entire VPC for ex 10.0.0.0/16

This block allows for 65,536 IP address (but in reality, 65,531 usable address).

CIDR (Classless Inter-domain Routing) is a method for allocating IP address & routing Internet protocol (IP) packets)

#Subnet:- A subnet is a smaller, segmented part of a larger network that isolated and organise device within a specific IP address range.

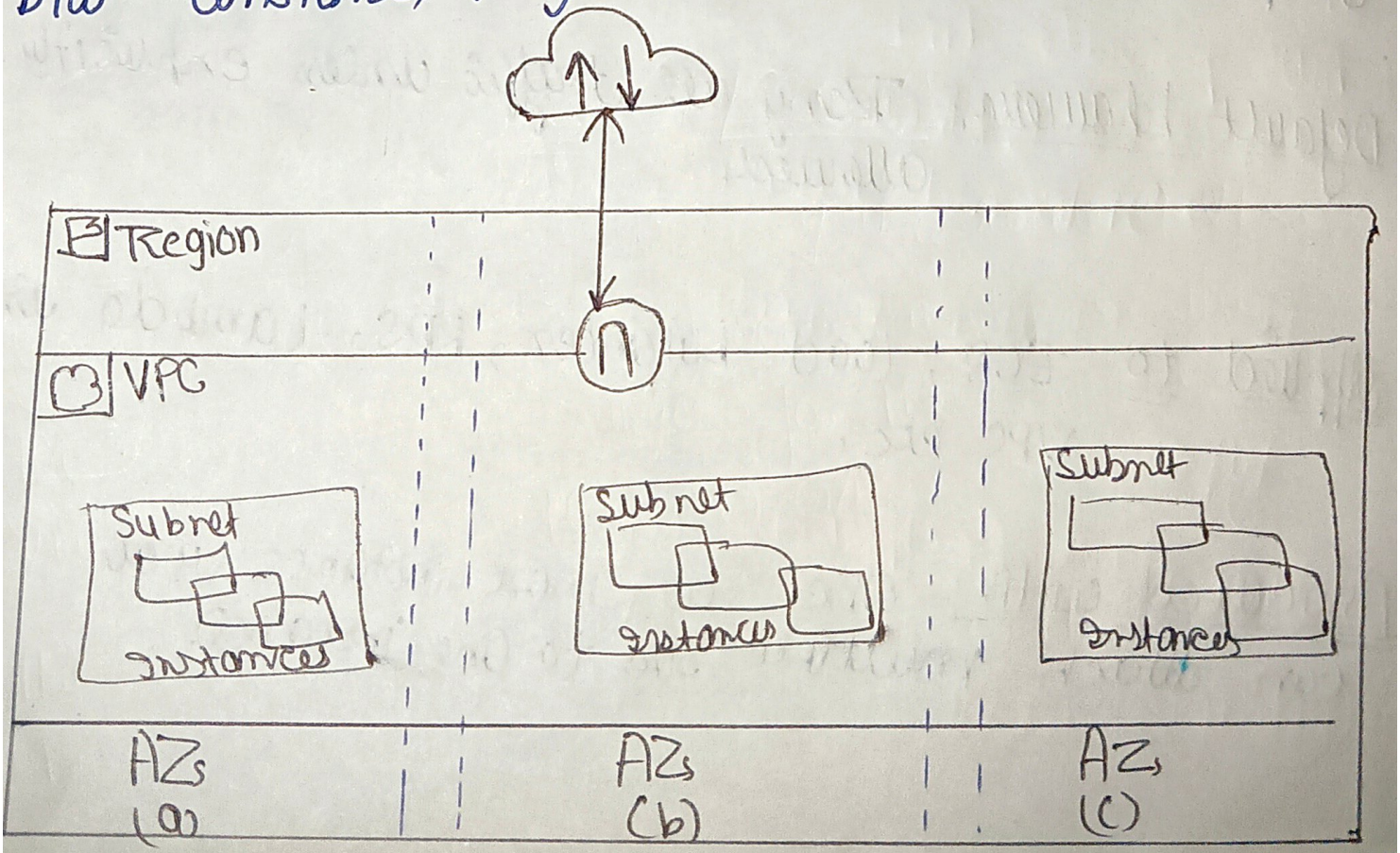




Note:- Subnet are distributes across availability Zone Because if one AZ goes down, the resources in other AZ s (other Subnets) will keep running.

#Route Table:- A route table is a set of rules, called routes, that are used to determine where network traffic from your subnets or gateway is directed. Each subnet in your VPC must be associated with a route table., which controls the routing for the subnet.

#Internet Gateway :→ An Internet Gateway is a Component that allows communication b/w instances in your VPC and the Internet.



Security Groups :- A Security Group (SG) in AWS acts like a virtual firewall that controlls inbound and outbound traffic for your EC2 instances (and other services like RDS, Lambda in a VPC).

Key Points

Scope :- Works at the instance level (not subnet or VPC).

Inbound rule / Outbound rule :- Control what traffic is allowed into / out the instance.

Stateful :- Yes, if you allow inbound, the response is automatically allowed.

Default behaviour :- Deny all traffic unless explicitly allowed.

Applied to :- EC2, load balancers, RDS, Lambda in VPC etc.

Associated with :- One or more instance (you can attach multiple SGs to one instance).

Network ACLs (Access Control list):

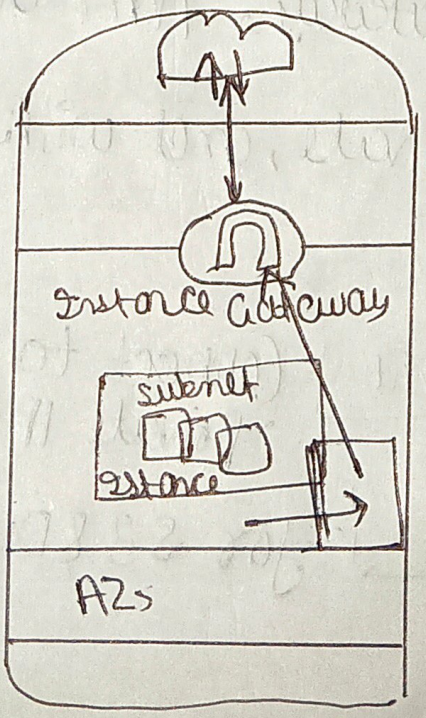
Optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnet.

→ Subnet-level scope (unlike security group which are instance level).

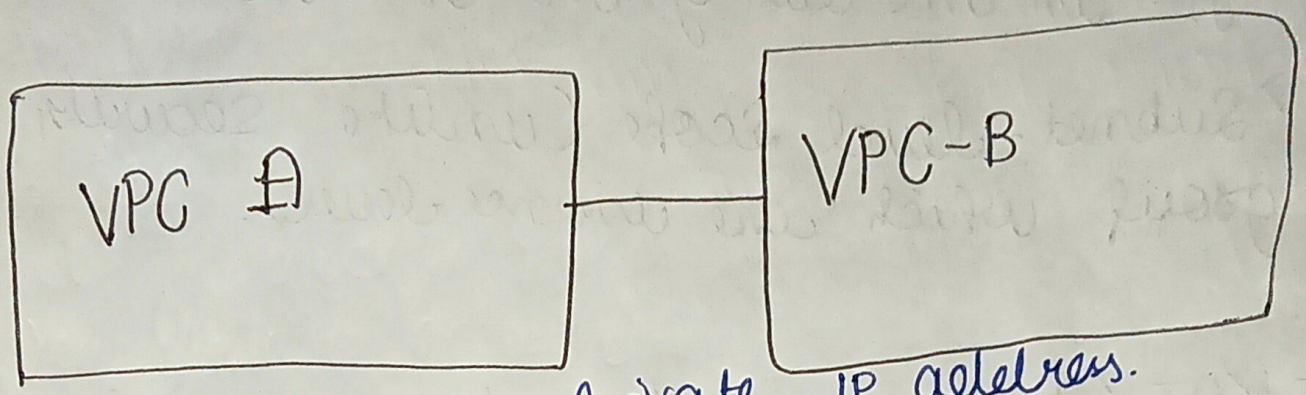
NAT (Network Address translation) Gateway:

Enables instances in a private subnet to connect to the internet or other AWS services, but prevents the internet from initiating connections to those instances.

→ One-way communication (means while preventing unsolicited inbound connections from the internet or other VPCs)



VPC Peering :- A networking connection b/w two VPCs that enable you to route traffic b/w them privately.



→ It allows over private IP address.
→ without using → internet
→ VPN
→ NAT Gateway.

VPC Endpoint :- Allow you to privately connect your VPC to supported AWS service and VPC endpoint services powered by AWS private Link. (like S3, DynamoDB) :

→ Without using :-
→ Internet Gateway, NAT Gateway, Public IPs

It's secure, private, and within the AWS network

Types :-

Interface Endpoint :- Connect to Service using a private IP (Lambda, SSM, SNS) etc

Gateway Endpoint :- for S3 & DynamodB only.

Easy way to Remember

- VPC :- Your Cloud Wife network.
- Subnet :- Room in your house.
- IGW :- Your wifi Router.
- NAT Gateway :- Download manager for secure rooms.
- Security Group :- Door lock for people
- NACL :- Rules for each room.

Key Best practice

- Use multiple AZs for high availability.
- Keep database in private subnet.
- Use NAT Gateway for secure outbound Internet from private subnet.
- Enable flow logs for monitoring.
- Use VPC Peering or Transit Gateway for multi-VPC Communication.

Bastion Host :- A special purpose instance that provides secure access across to your instances in private subnets.

Real World Scenario

You have :-

- EC2 instance in private subnet (no internet access)
- You want to access them securely via SSH.

Instead of giving public IPs to each instance (bad practice), you create one bastion host in a public subnet.