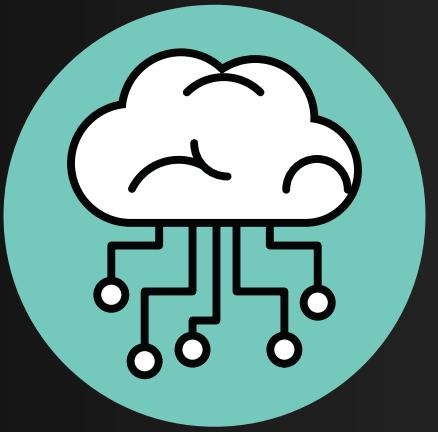


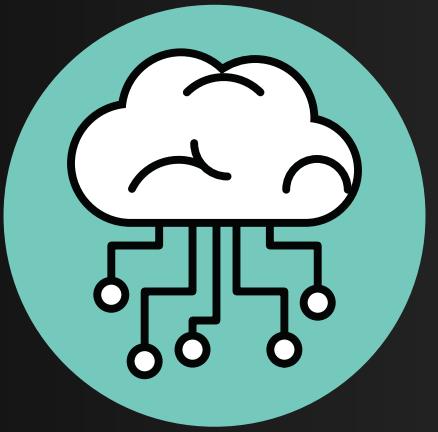
Networking

# Virtual Private Cloud (VPC)



## Virtual Private Cloud (VPC)

**A private, isolated network within the AWS cloud  
where you can launch and manage your resources  
securely.**



## Why we need VPC?

To securely isolate and control network environments.





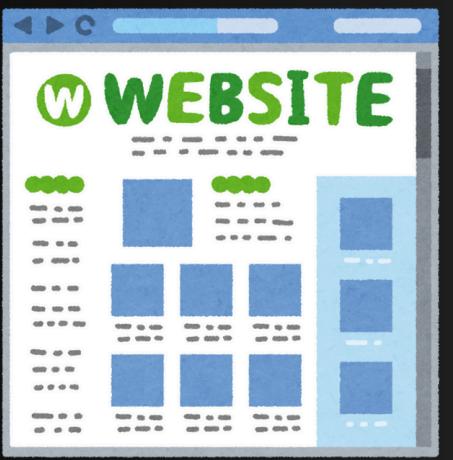
**Website is ready  
Where to deploy?**



**Website is ready  
Where to deploy?**



US



**Website is ready  
Where to deploy?**



Asia

Europe

# Website is ready

# Where to deploy?



# Asia

# North

# East

# South

# *REGION*



**Website is ready  
Where to deploy?**



**Asia**

**North**

**Singapore**

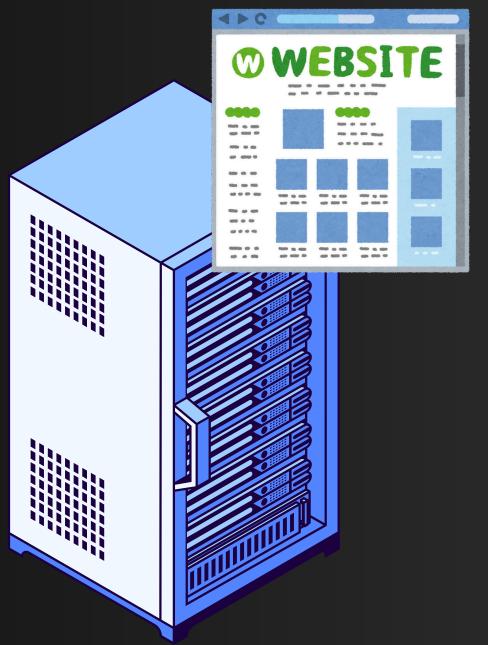
**East**

**Mumbai  
Hyderabad**

**South**

**Tokyo**

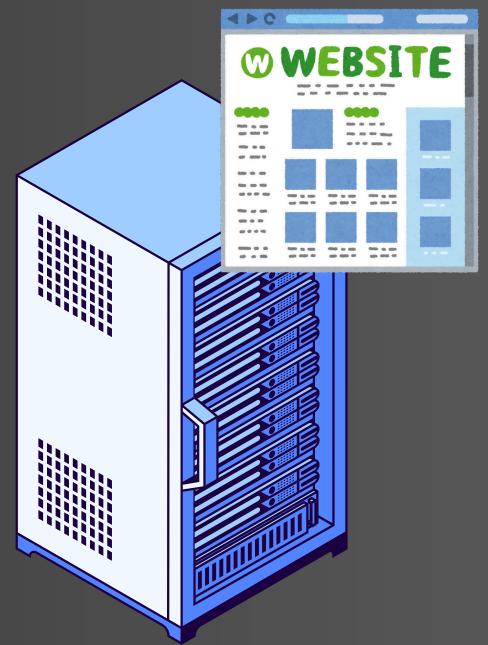
# Availability Zones



a



b



c

Mumbai

**region - mumbai**



**MY-VPC**

## VPC CIDR Block

When you create a VPC, you specify a CIDR block that defines the IP address range for the entire VPC. For example:

```
sh
```

 Copy code

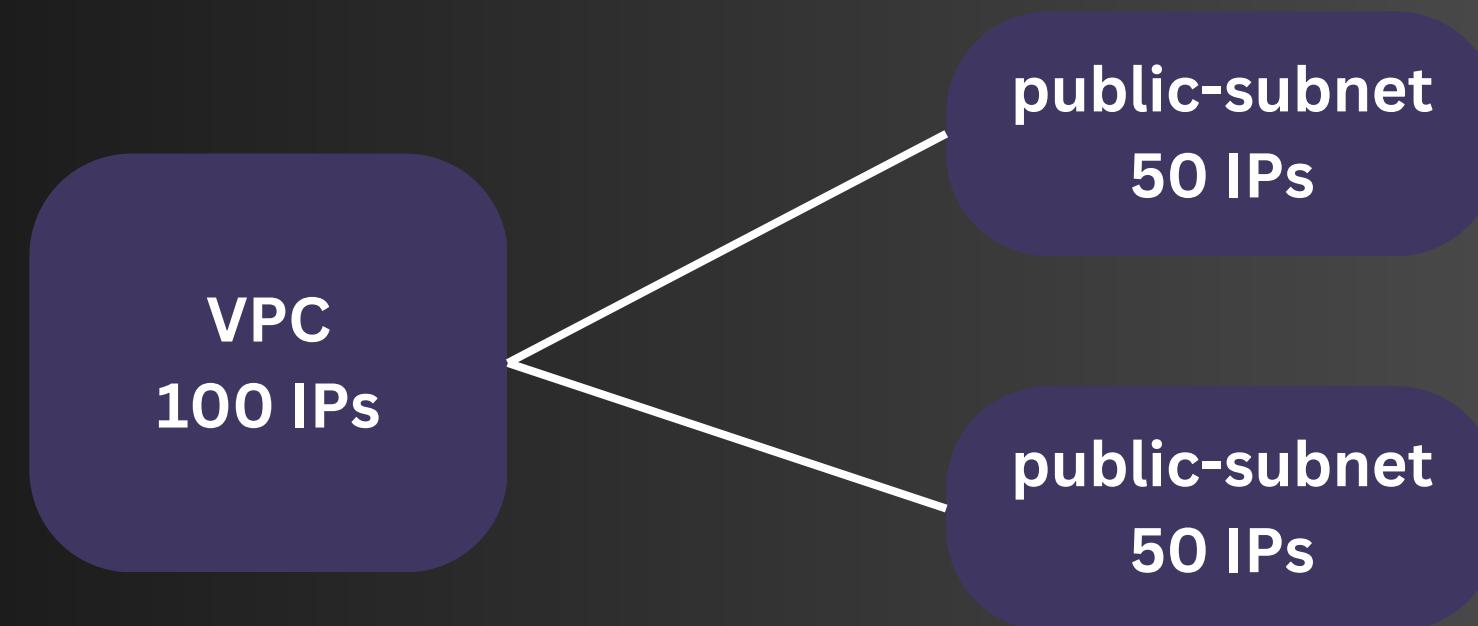
```
10.0.0.0/16
```

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

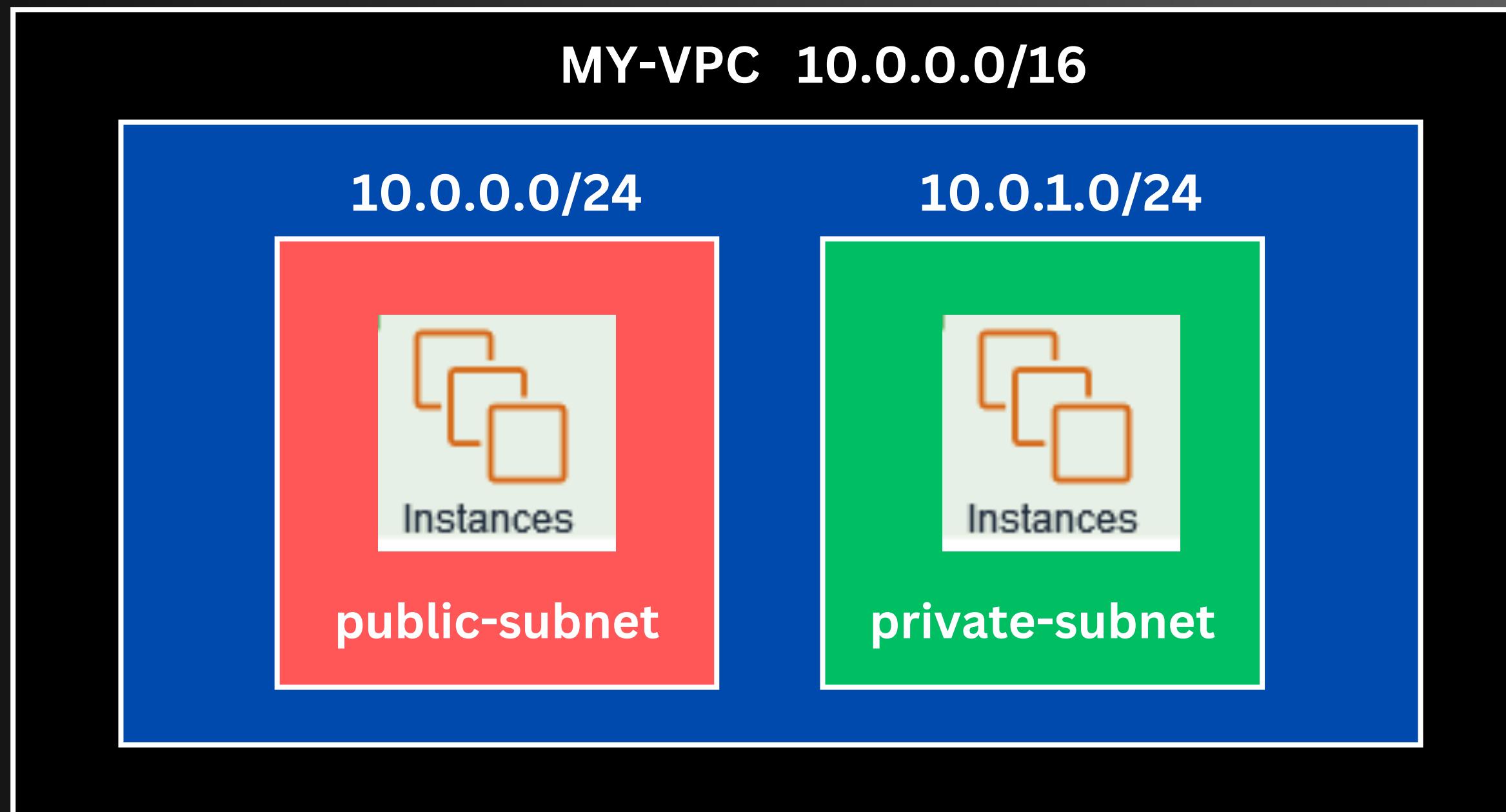
**CIDR (Classless Inter-Domain Routing) is a method for allocating IP addresses and routing Internet Protocol (IP) packets.**

# What is Subnets?

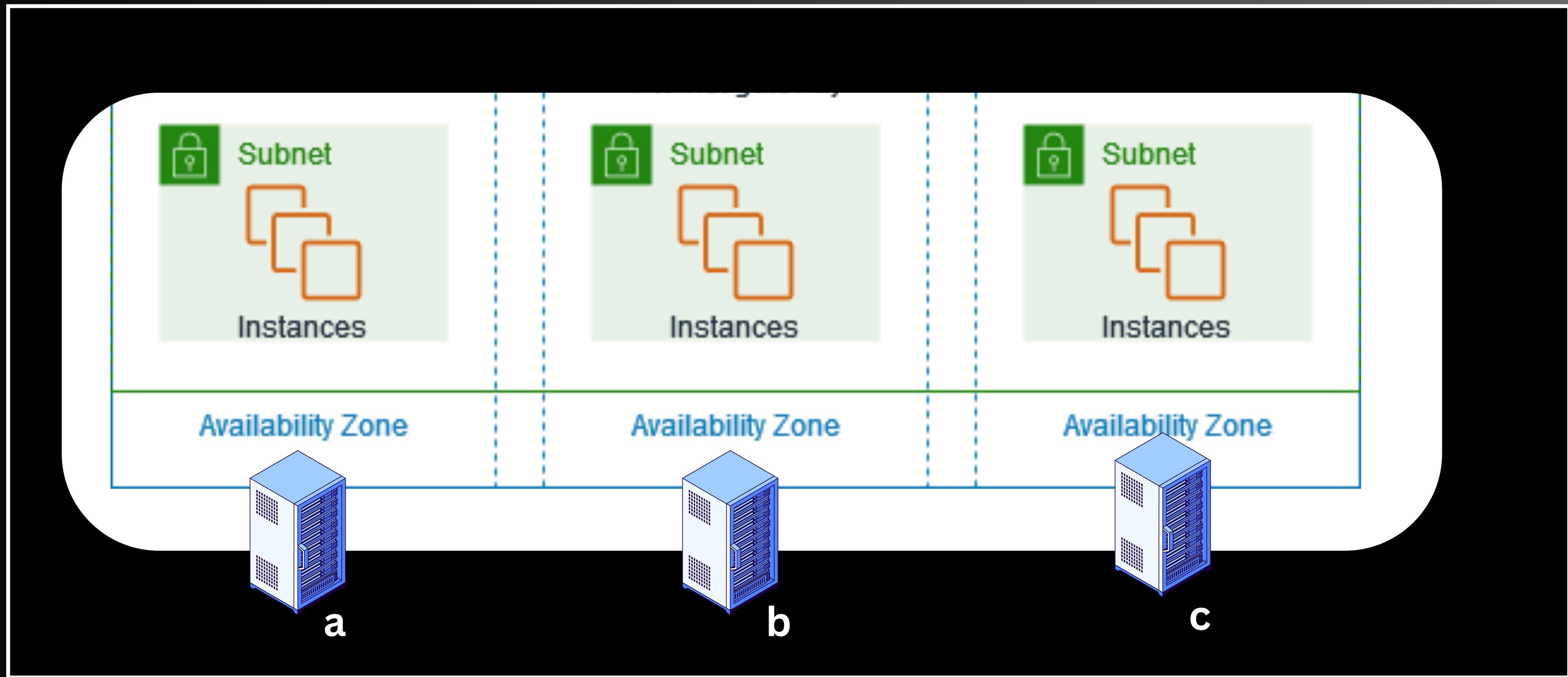
A subnet is a smaller, segmented part of a larger network that isolates and organizes devices within a specific IP address range.



region



region



# What happens when creating subnet?

## CIDR Block Allocation:

You specify a range of IP addresses (CIDR block) within the VPC's IP address range for the subnet.

This determines the pool of IP addresses available for instances in the subnet.

## Subnet CIDR Blocks

Within the VPC, you can create subnets by allocating smaller CIDR blocks from the VPC's range.

For example:

- Public Subnet: `10.0.1.0/24`
- Private Subnet: `10.0.2.0/24`

Each of these subnets has 256 IP addresses (251 usable).

# Explanation of 10.0.1.0/24

- An IPv4 address is 32 bits long.
- Example in binary: `10.0.1.0` -> `00001010.00000000.00000001.00000000`
- The **/24 indicates that the first 24 bits are the network portion of the address.**
- The remaining 8 bits are available for host addresses within the network.

**10.0.1.0 to 10.0.1.255 is the full range.**

# Route Table

## What is a Route Table?

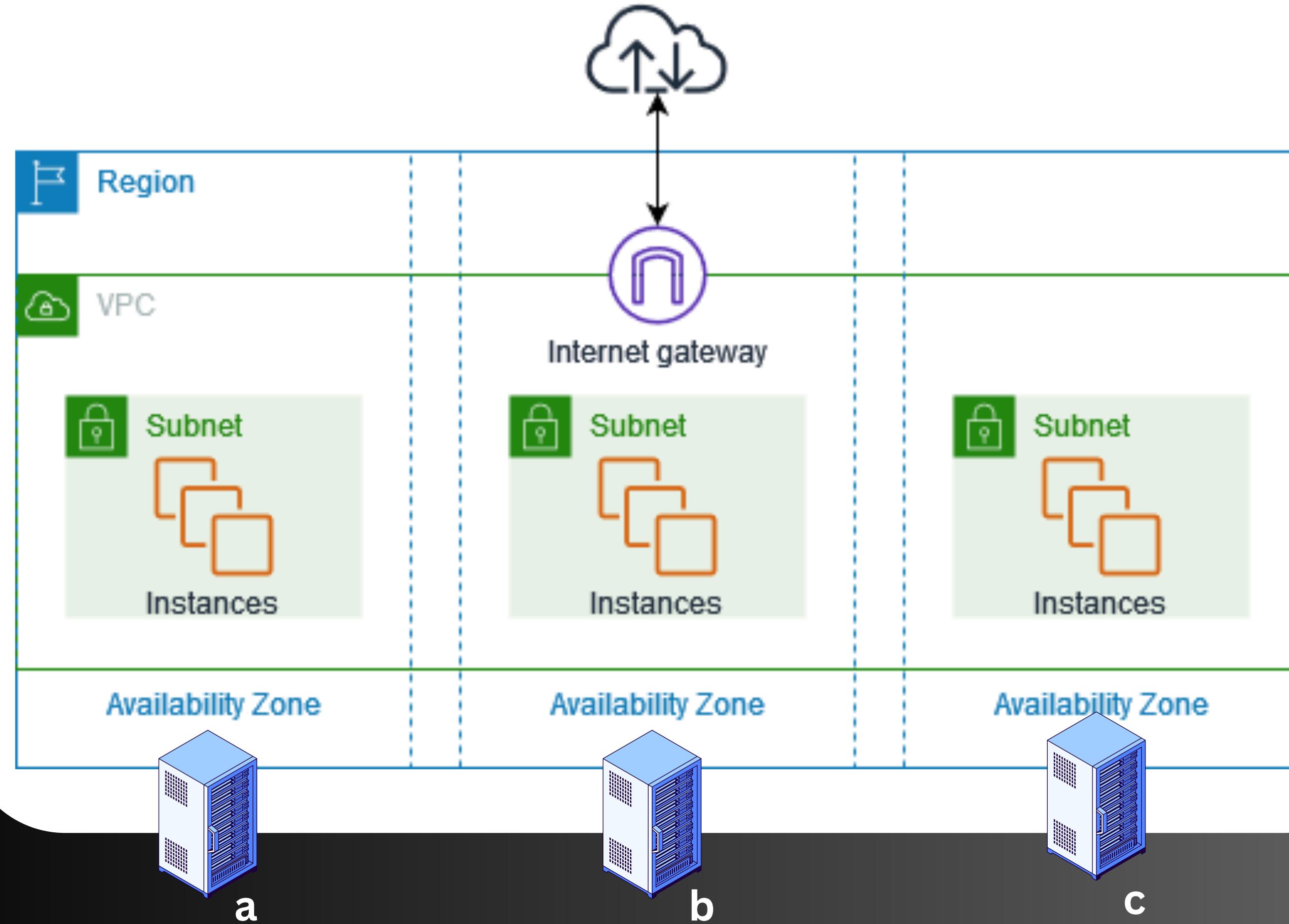
A route table is a set of rules, called routes, that are used to determine where network traffic from your subnets or gateway is directed. Each subnet in your VPC must be associated with a route table, which controls the routing for that subnet.

Routes (2)	
<input type="text"/> Filter routes	
Destination	Target
0.0.0.0/0	<a href="#">igw-0bc1bb62e4e4f3c3c</a>
172.31.0.0/16	local

# Internet Gateway

An Internet Gateway is a component that allows communication between instances in your VPC and the internet.





**Security Groups:** Network firewall rules that control inbound and outbound traffic for instances.



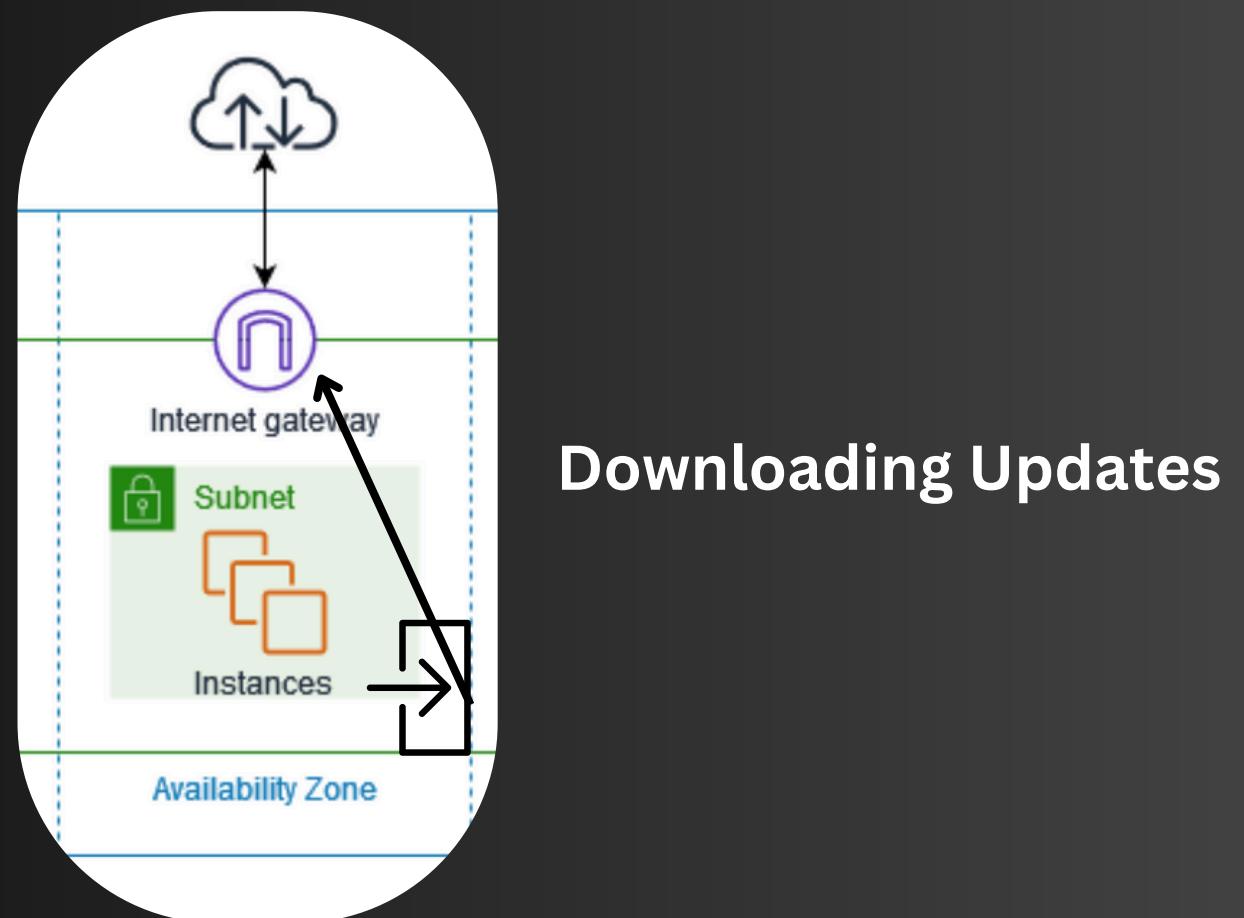
## **Network ACLs (Access Control Lists):**

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

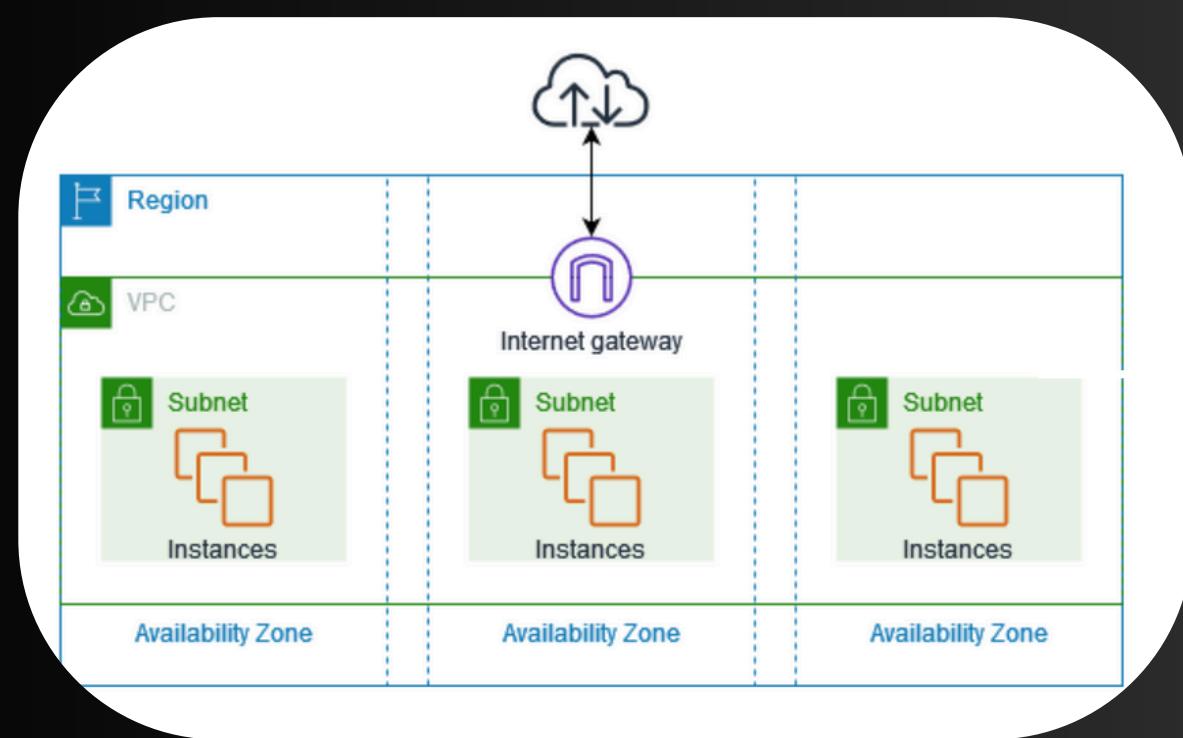
**Allow or Deny Rule.**

# NAT (Network Address Translation) Gateway:

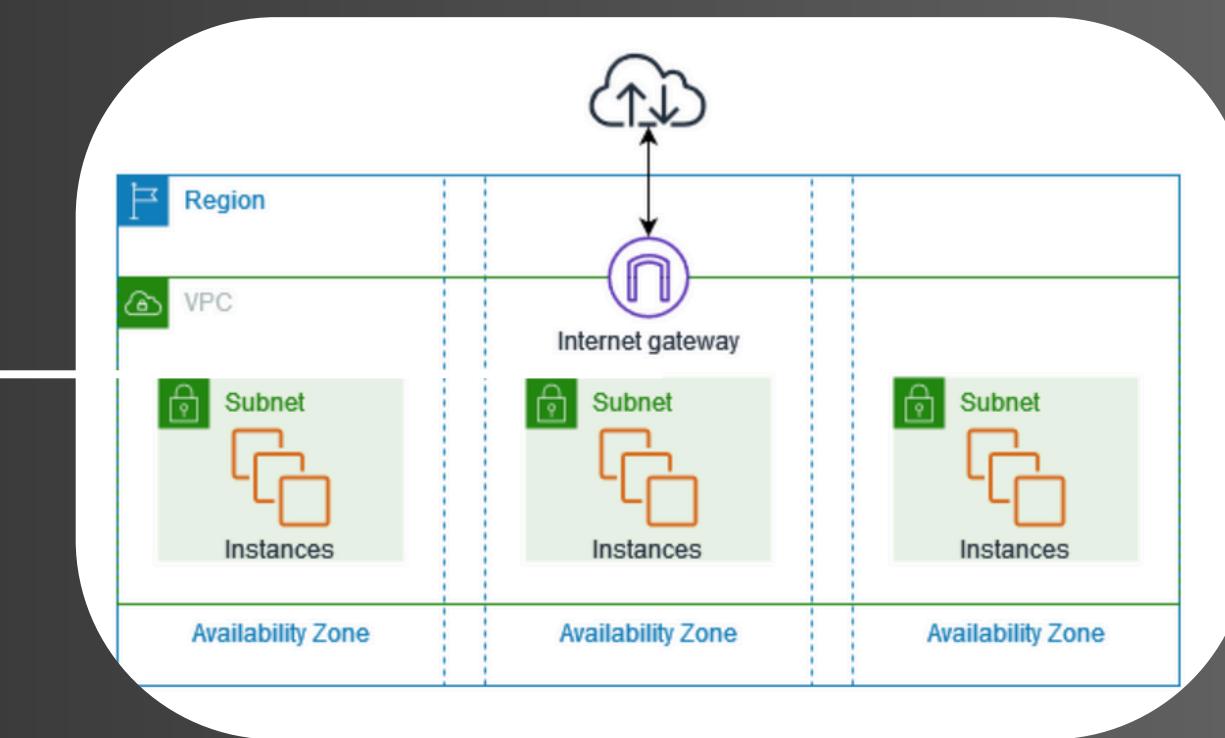
**Enables instances in a private subnet to connect to the internet or other AWS services, but prevents the internet from initiating connections to those instances.**



**VPC Peering:** A networking connection between two VPCs that enables you to route traffic between them privately.

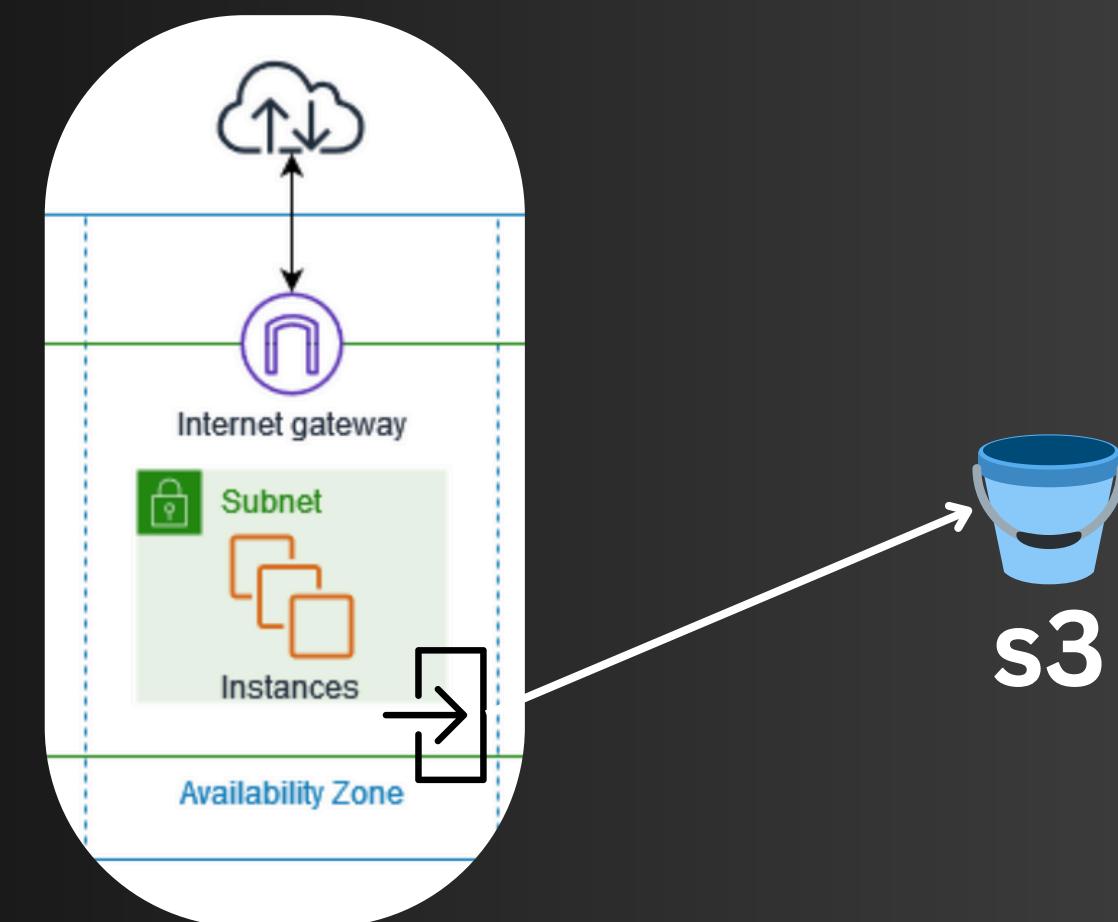


VPC A

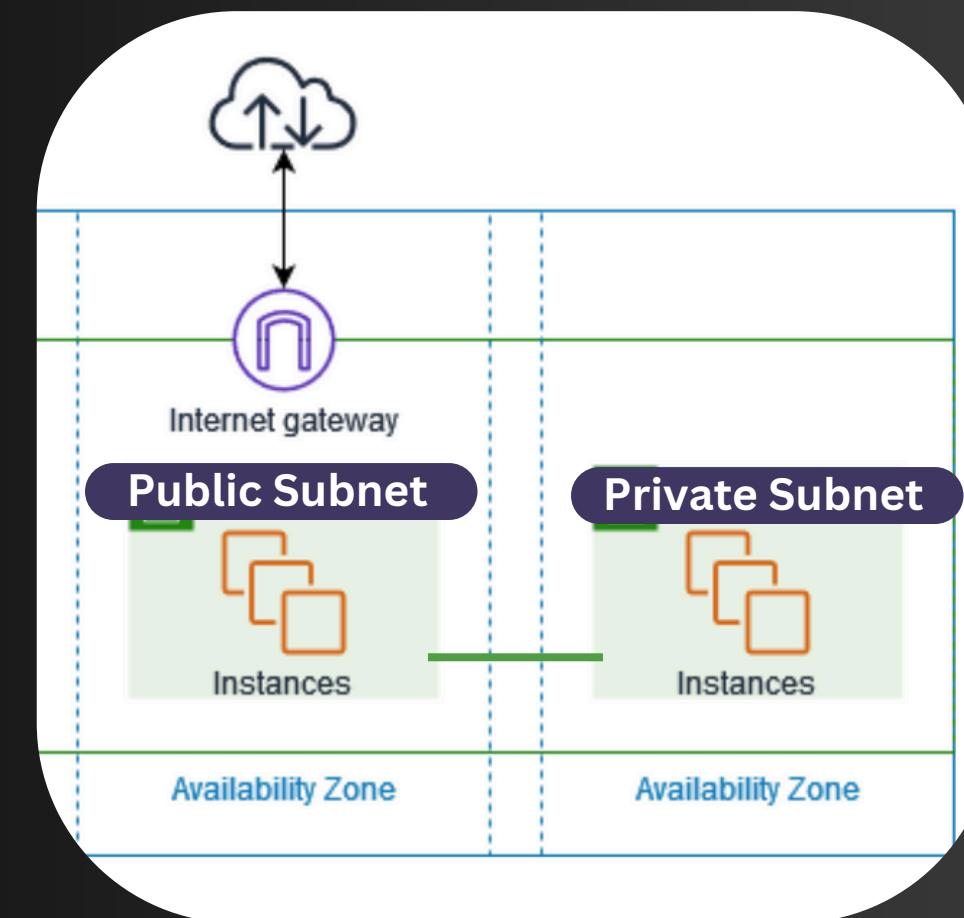


VPC B

**VPC Endpoints:** Allows you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink.



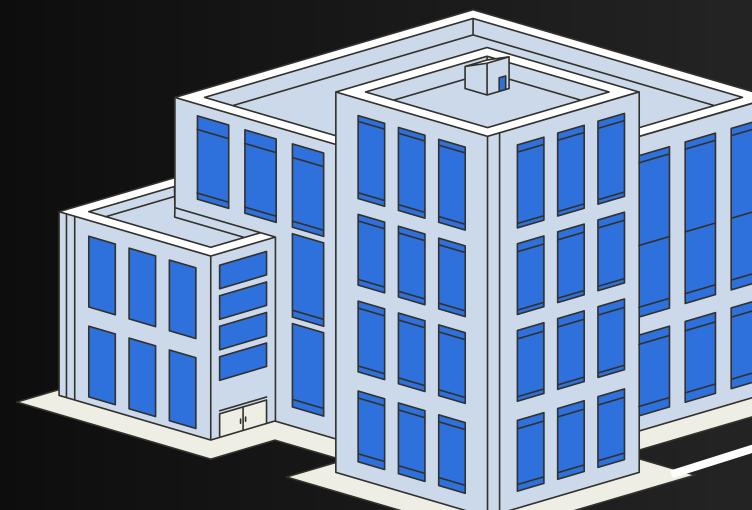
**Bastion Host:** A special-purpose instance that provides secure access to your instances in private subnets.



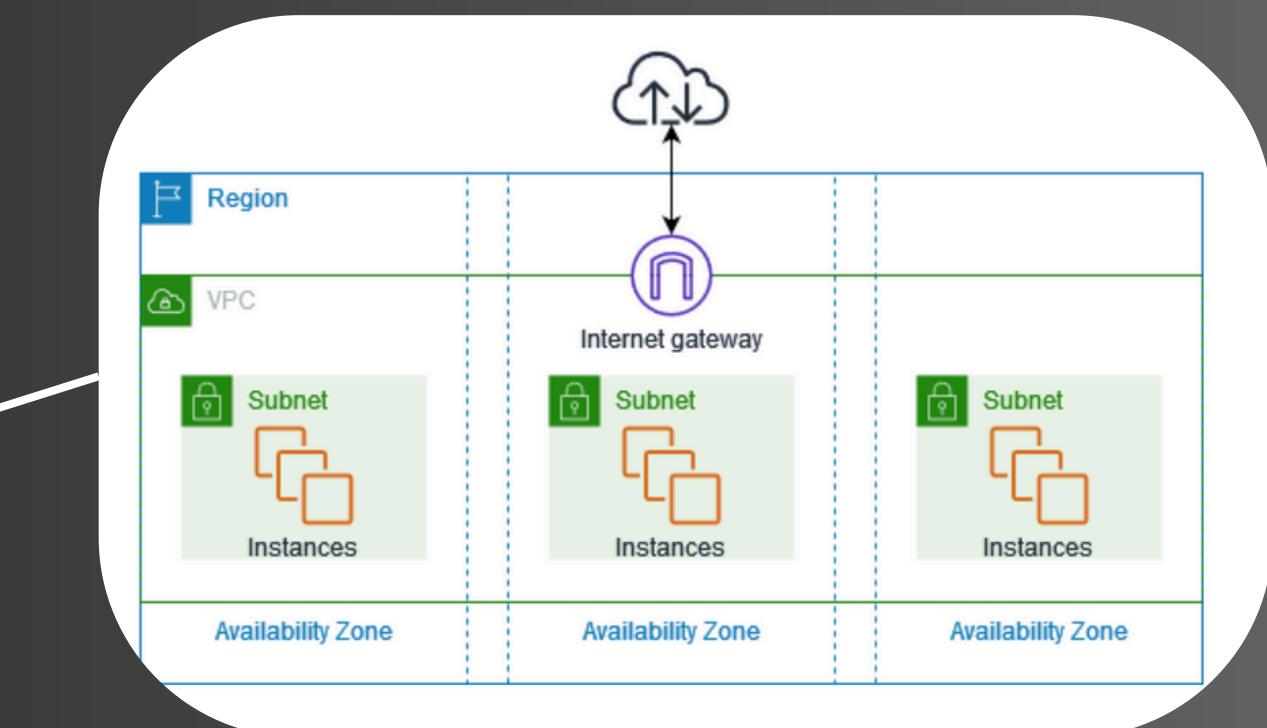
**Elastic IP Addresses:** Static IP addresses  
designed for dynamic cloud computing.

**VPC Flow Logs:** Capture information about the IP traffic going to and from network interfaces in your VPC.

# **Direct Connect: Establishes a dedicated network connection from your premises to AWS.**



Office



**Transit Gateway:** A network transit hub that you can use to interconnect your VPCs and on-premises networks.

**AWS Client VPN:** Managed VPN service that enables secure remote access to AWS resources and on-premises networks using OpenVPN-based clients.

