DATE : 19.02.2025

DT/NT : NT

LESSON : AWS

SUBJECT: VPC-1

BATCH : B 303

AWS-DEVOPS

TECHPRO EDUCATION

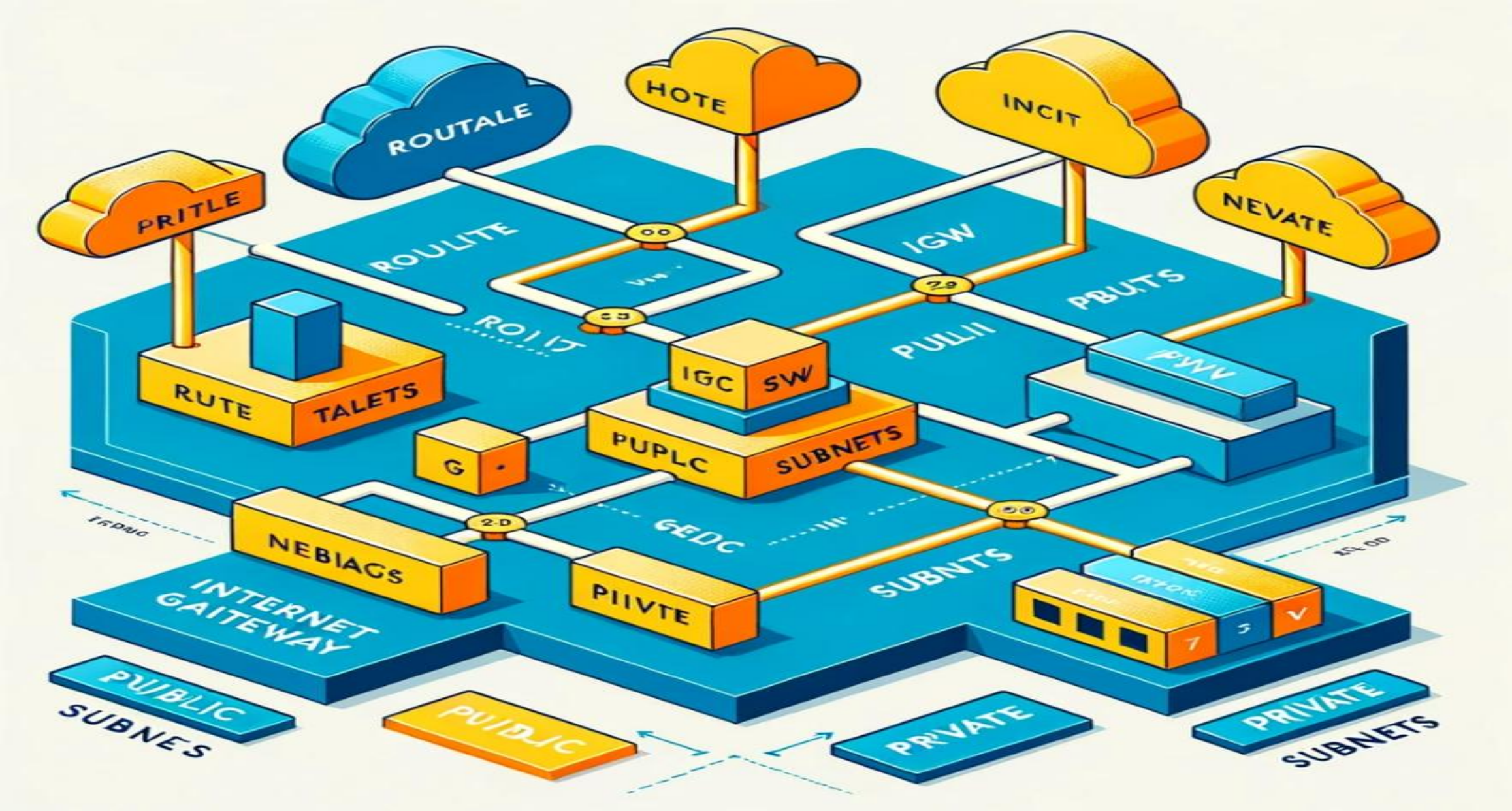
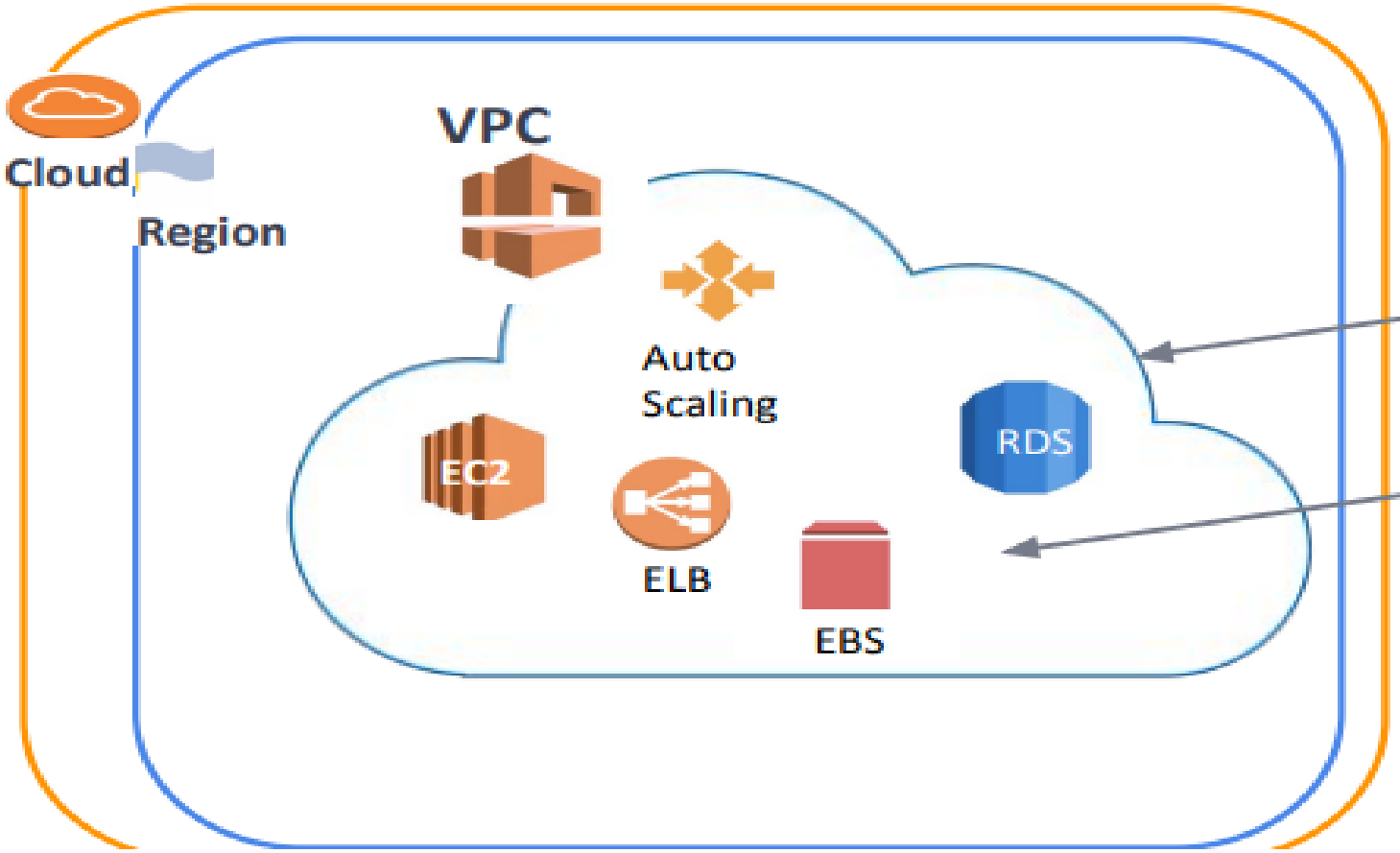

ROUTALE
HOTE
INCIT
PRITLE
NEVATE
ROULITE
IGW
PBUTS
RUTE
TALETS
IGC
SW
PUBLC
SUBNETS
PWV
NEBIAGS
INTERNET
GAITEWAY
PIIVTE
SUBNTS
PUBLIC
SUBNES
PUBLIC
PRIVATE
PRIVATE
SUBNETS

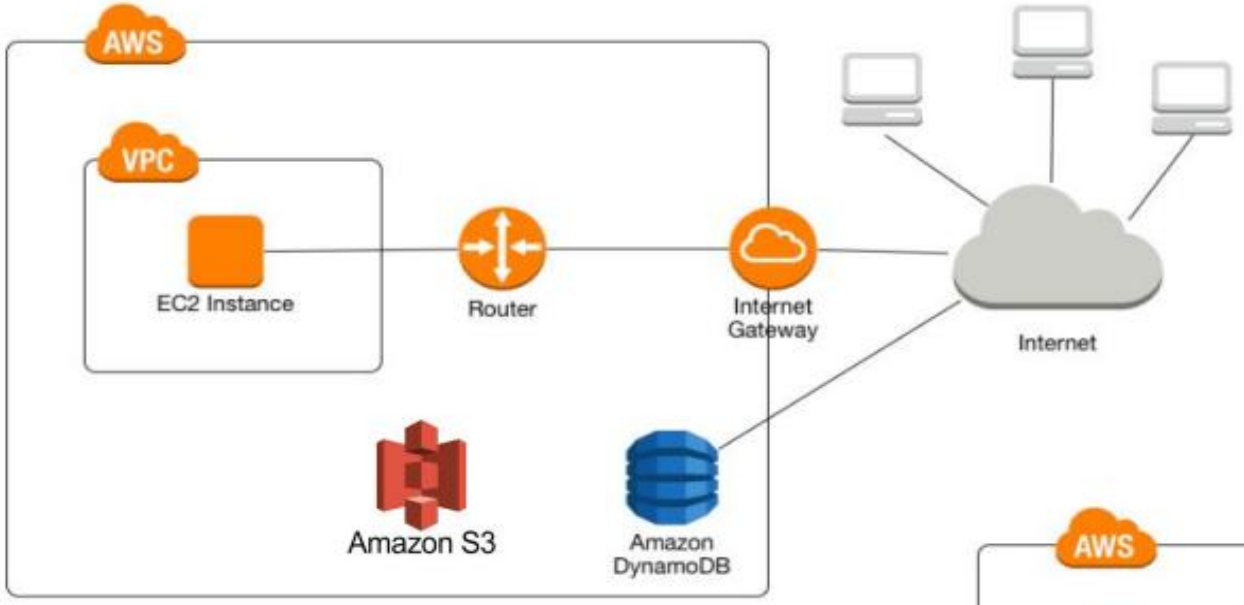
Table of Contents

Introduction to VPC

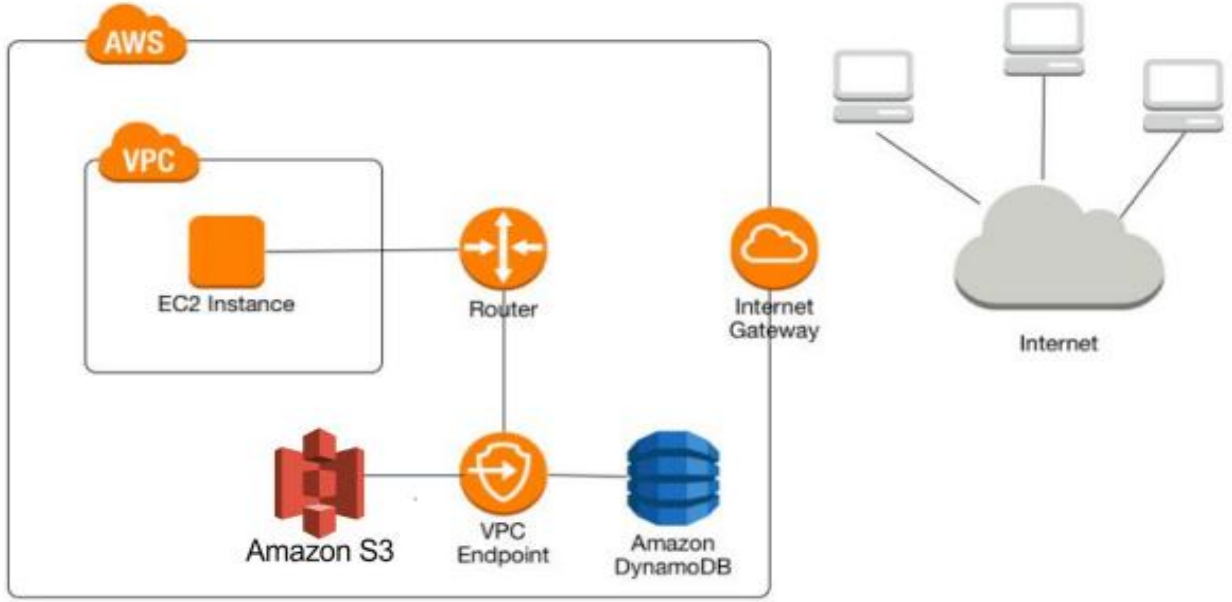
What is VPC?



Amazon Virtual Private Cloud (Amazon VPC) is a logically isolated area of the AWS cloud where you can launch AWS resources in a virtual network that you define.



services using HTTP protocol



VPC Basic Components

VPC Basic Components

- VPC Region (AZ)
- VPC Subnets
- VPC CIDR
- Internet Gateway
- Route Table
- Security Group and Network ACL

VPC COMPONENTS

The following are the key concepts for VPCs:

- ✓ **Virtual private cloud (VPC)** — A virtual network dedicated to your AWS account.
- ✓ **Subnet** — A segment of VPC's IP address range.
- ✓ **Route table** — A set of rules, called routes, that are used to determine where network traffic is directed.
- ✓ **Internet gateway** — A gateway that you attach to your VPC to enable communication between resources in your VPC and the internet.
- ✓ **Egress only Internet Gateway** — Internet Gateway for IPv6.
- ✓ **VPC endpoint** — Private connection to public AWS services.
- ✓ **Peering connection** — Direct connection between 2 VPCs.
- ✓ **CIDR block** — Classless Inter-Domain Routing. An IP address allocation and route aggregation methodology.
- ✓ **Security Group** — Instance-level firewall.
- ✓ **NACL** — Subnet-level firewall.

VPC COMPONENTS

The following are some concepts for VPCs:

✓ **Traffic Mirroring** — Allows capturing and inspecting network traffic in a VPC.

- You route traffic to security services.
- Capture packets.
- Used for troubleshooting, content inspection, and threat monitoring.

✓ **Flow Logs** — Capture information about IP traffic inside a VPC.

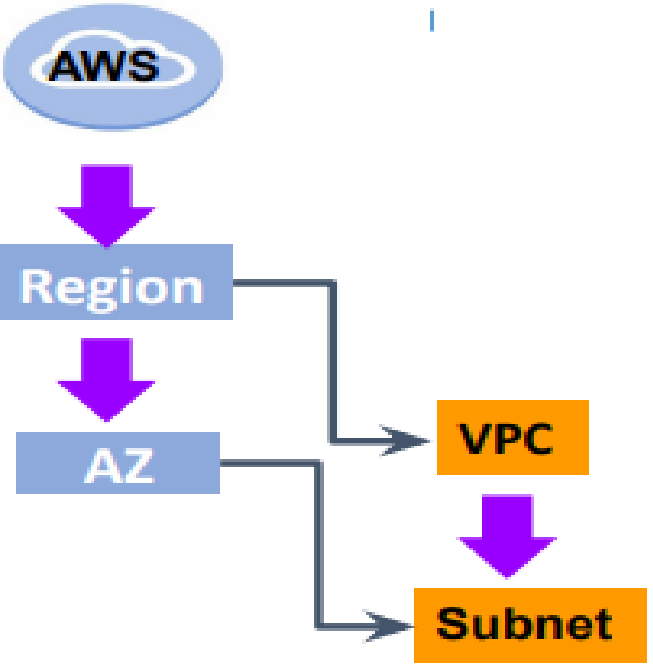
- Logs can be sent to S3 or CloudWatch.

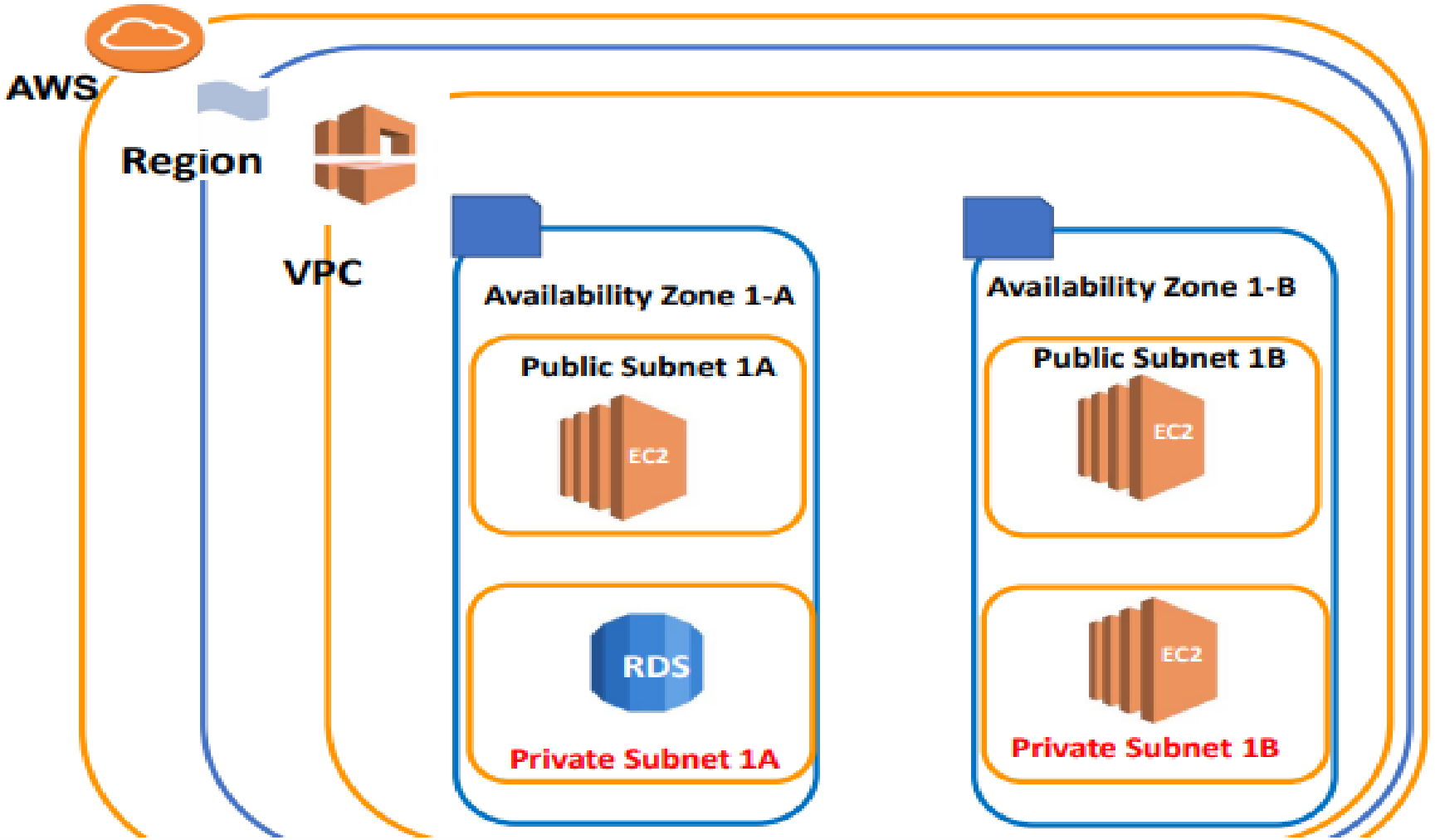
✓ **Network Firewall** — A managed network firewall and intrusion prevention/detection service (Layer 3 to Layer 7) that allows customers to filter traffic at the perimeter of their VPC.

Subnets

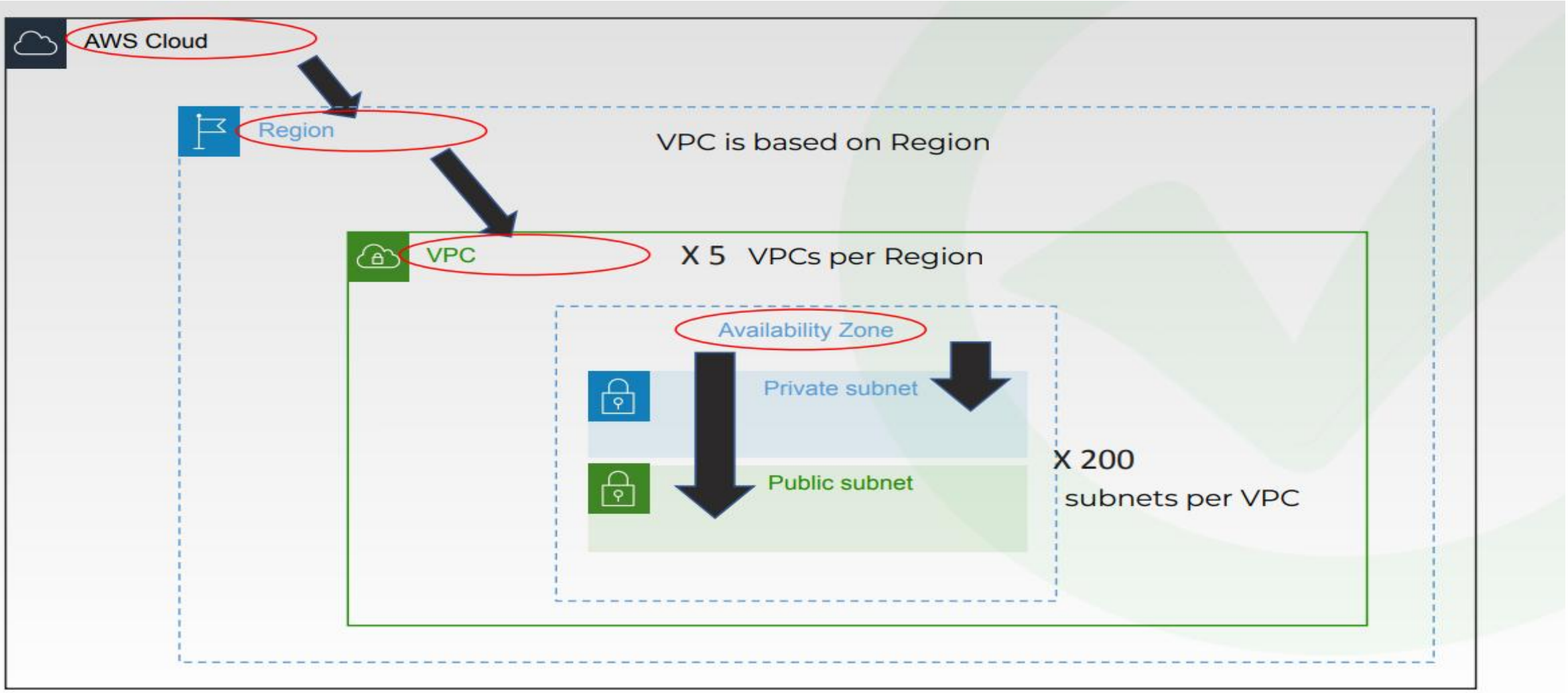
- AWS VPC (Virtual Private Cloud) contains a "Subnet" (Subnetwork), which is used to divide your VPC into smaller, more manageable sections. A subnet is a segment of a larger network (in this case, the VPC) that has a specific range of IP addresses. Each subnet within a VPC utilizes a portion of the VPC's IP address range.

Region, VPC, AZ and Subnets





VPC Components



VPC CIDR

10.0.0.0/16 Block Size

10.0.0.0/16= **65,536** IPs in Range
10.0.1.0/24= **256** IPs in Range
10.0.1.0/32= **1** IP in Range

CIDR refers to Classless Inter-Domain Routing.

It is a set of Internet protocol (IP) standards that is used to create unique identifiers for networks.

As the Size Block/Netmask (/16,24,32) increases, the number of IP located in CIDR Block decreases.

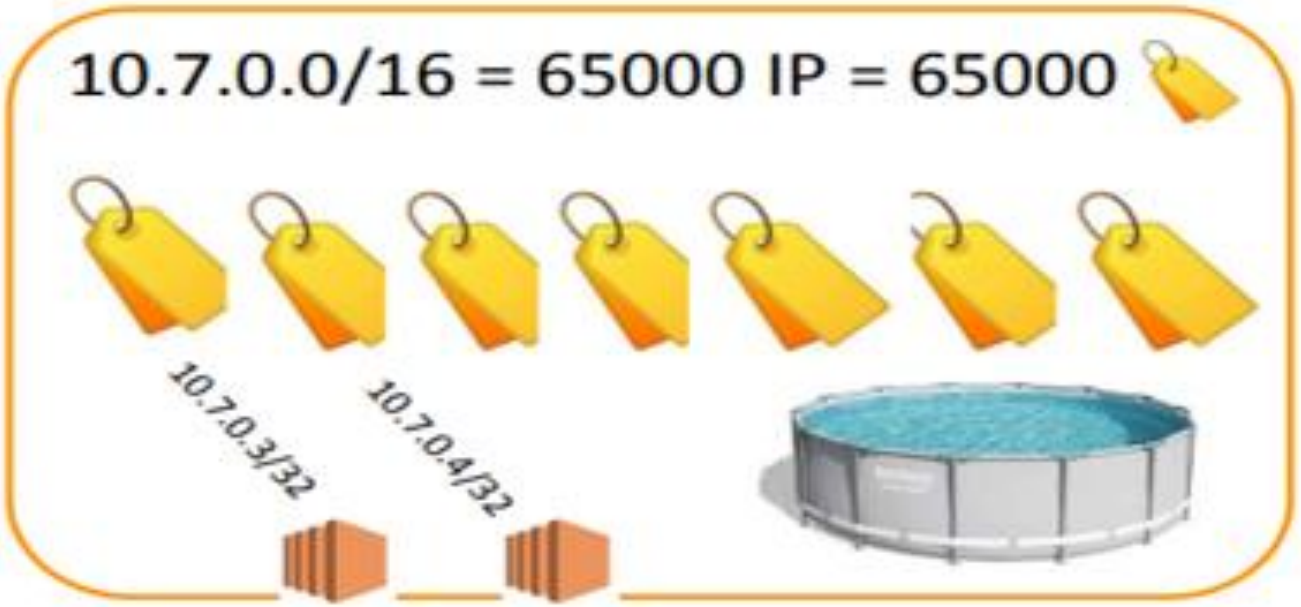
VPC CIDR

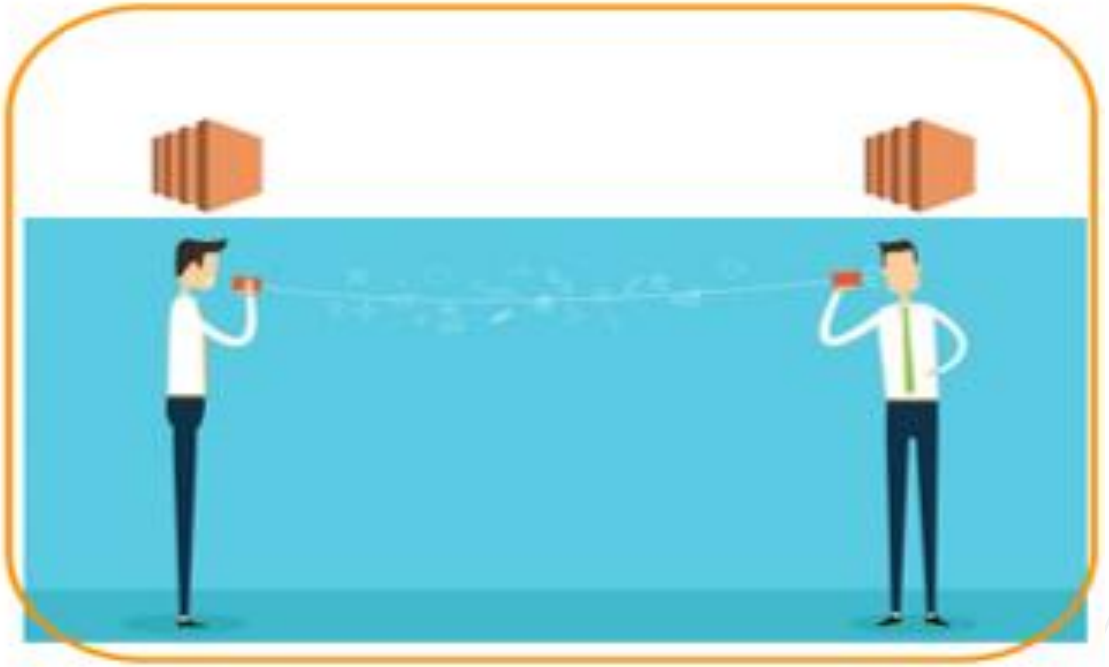
In AWS VPC (Virtual Private Cloud), the "CIDR Block" (Classless Inter-Domain Routing Block) is a method used to define a range of IP addresses. CIDR defines an IP network using a specific network address and a 'mask' associated with that address. This mask determines the size of the network (i.e., how many IP addresses it contains). Using a CIDR block in a VPC defines the IP address range that all subnets and resources within the VPC can use.

VPC CIDR Bock

Labeling

Internal Communication





How is it possible to use the same CIDR block for all of us?

SSN:01-A-2345-4563

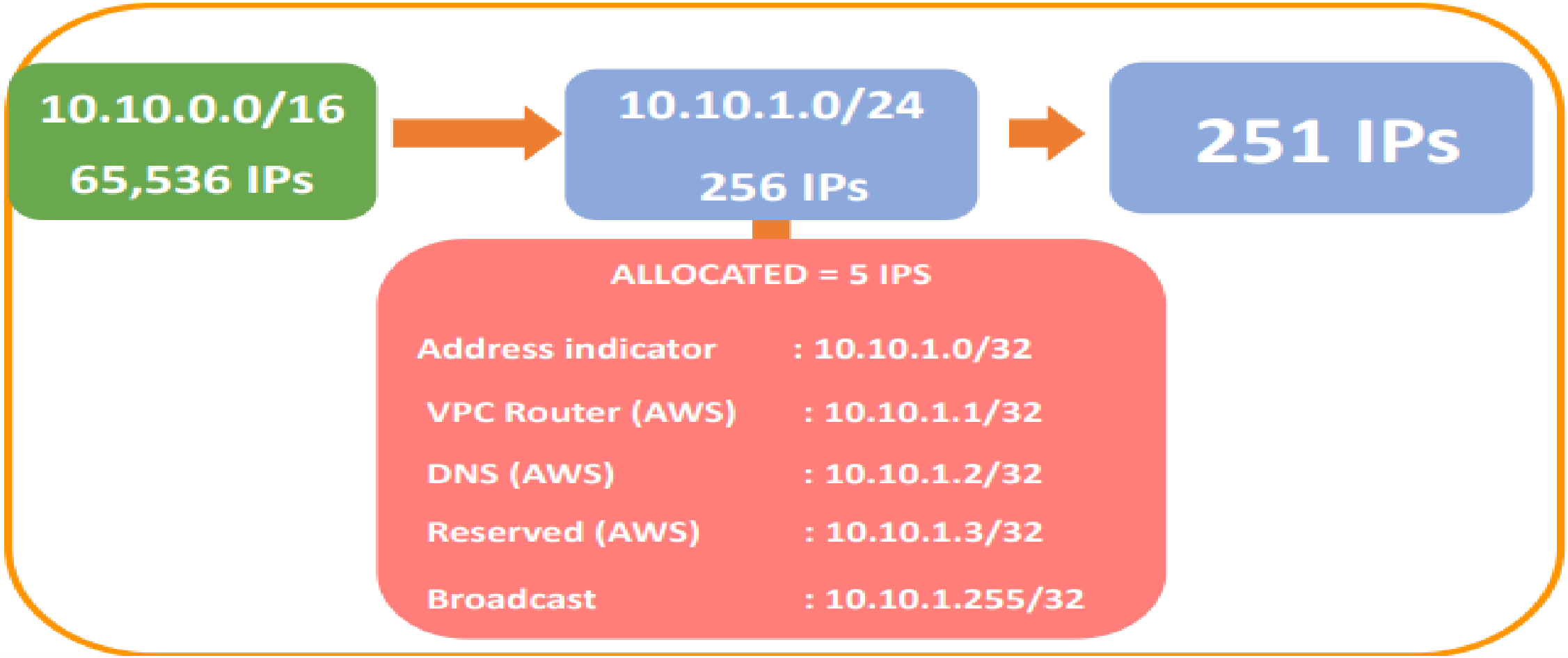
SSN:02-C-98756H64

VPC 1=House 1

VPC 2=House 2

TECHPRO EDUCATION

VPC CIDR



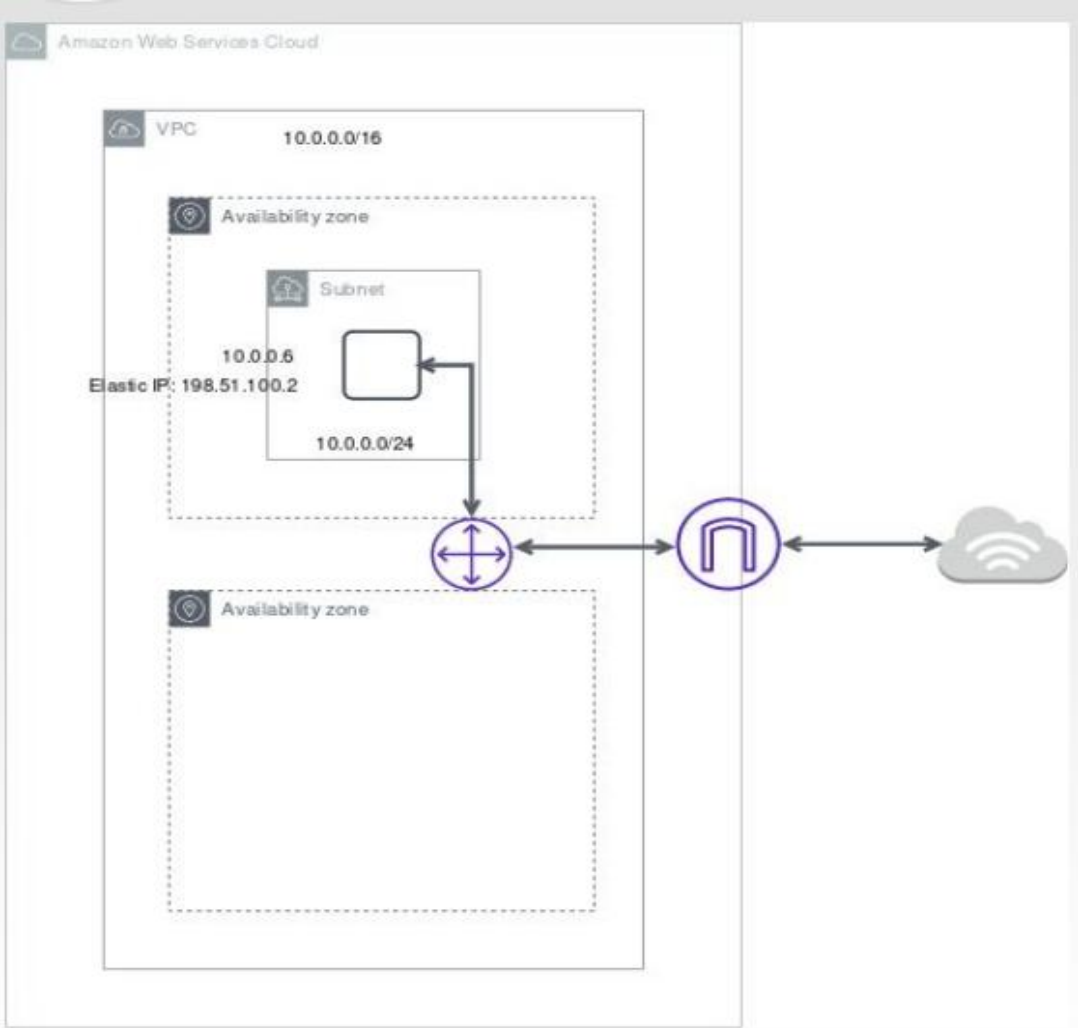
Internet Gateway

- Internet Gateway is a VPC component that provides communication between resources in your VPC and the internet.

Internet Gateway

- The Internet Gateway is our gateway to the outside, meaning the internet. Think of it like an external terminal. It is the gateway through which the VPC connects to the outside world. It provides bidirectional access from inside to outside and from outside to inside. However, just because we open a gateway does not mean the VPC is completely open to the outside; we will later define who can use that gateway.
- Let's select **Internet Gateways** from the left console. By default, there was one, but we will create a new one by selecting **Create Internet Gateway**.

Internet Gateway

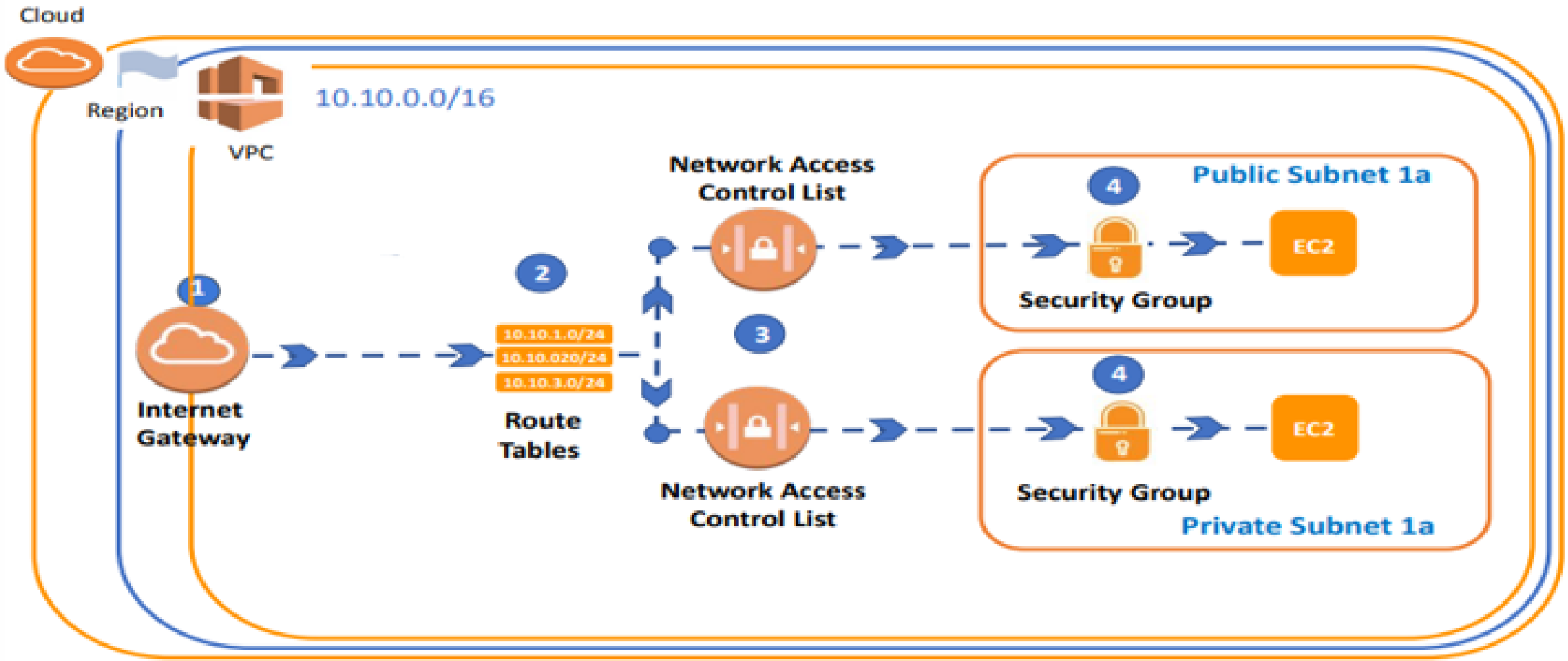


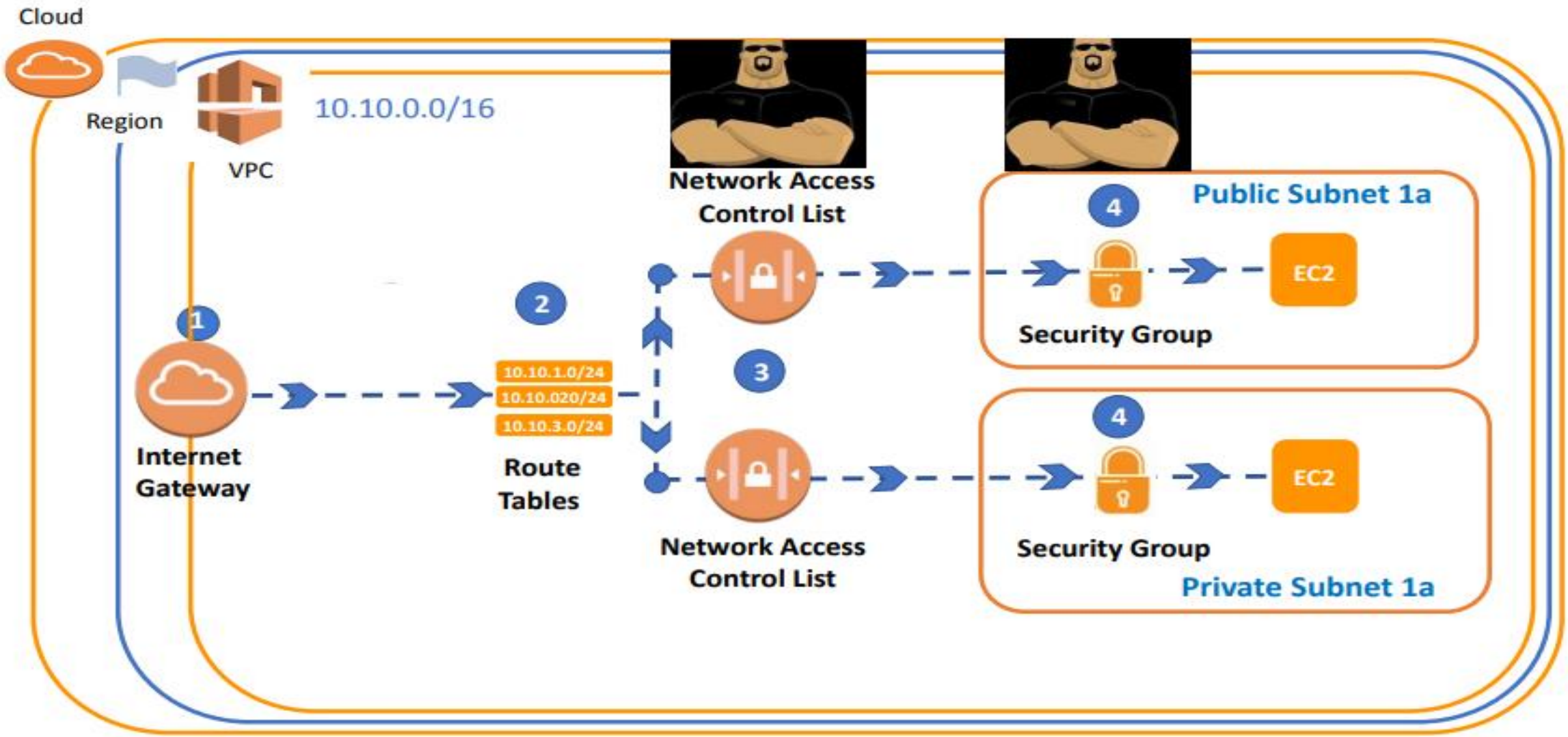
✓ **An internet gateway** is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet.

✓ **An internet gateway serves two purposes:**

- To provide a target in your VPC route tables for **internet-routable traffic**.
- To perform **network address translation (NAT)** for instances that have been assigned **IPv4** addresses.
  (For IPv6, NAT is not needed as they are all public.)

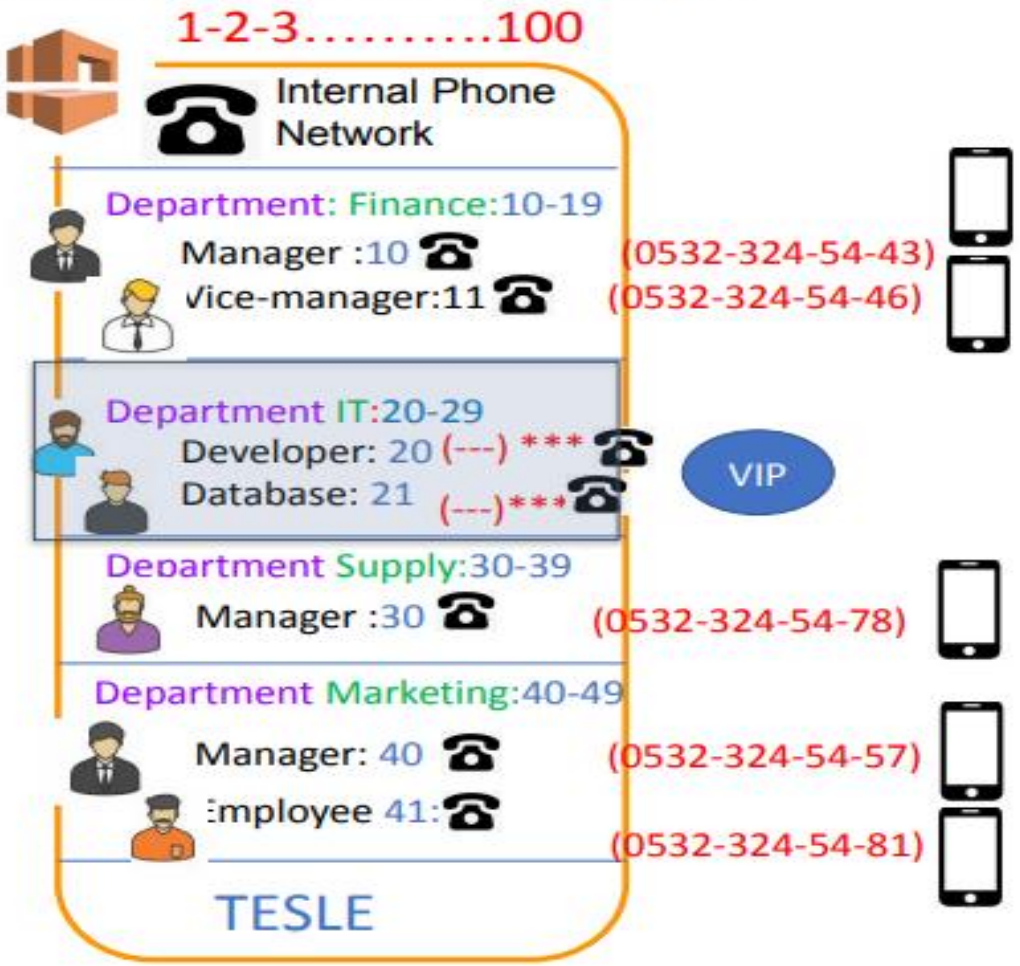
Security Group - Network Access Control List



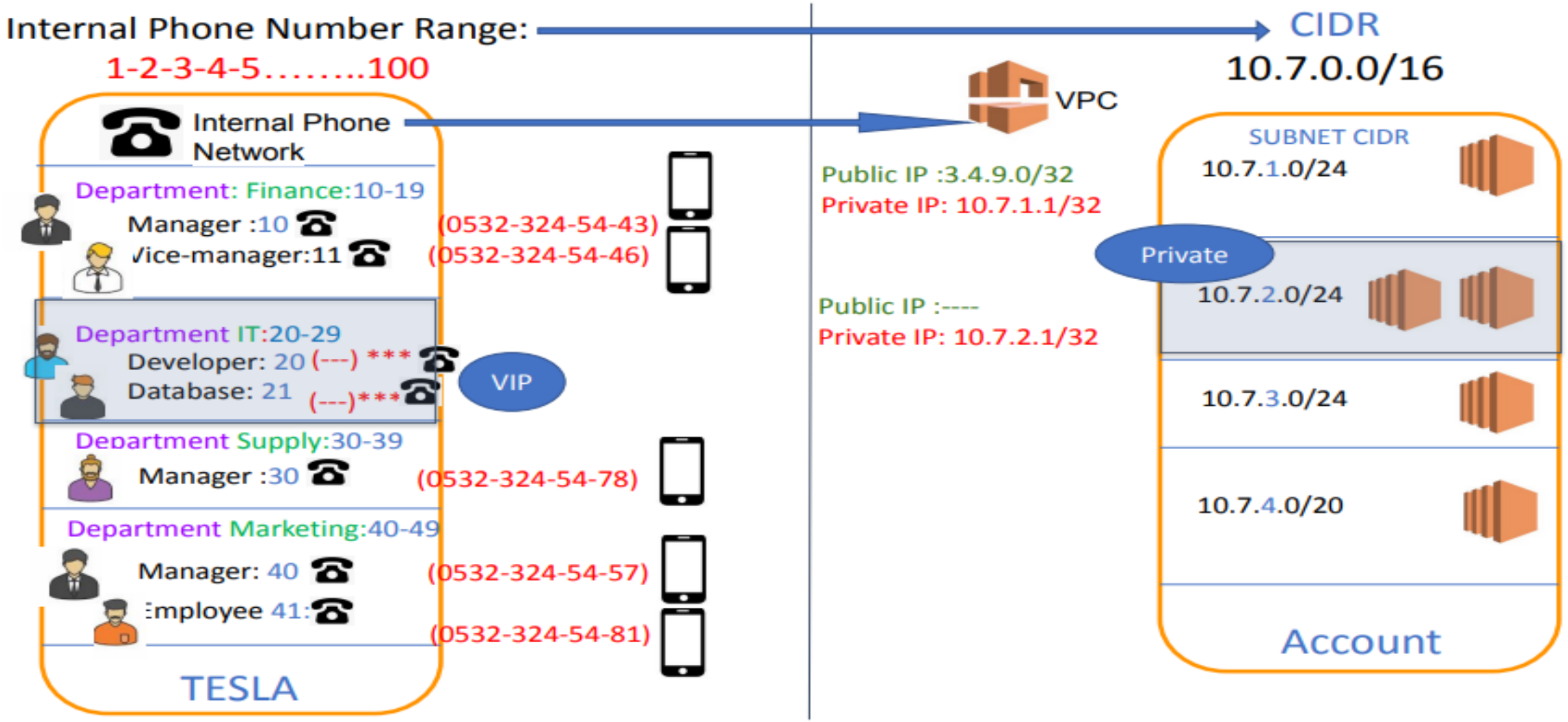

Cloud
Region
VPC
10.10.0.0/16
Network Access
Control List
Public Subnet 1a
4
EC2
Security Group
1
2
3
10.10.1.0/24
10.10.020/24
10.10.3.0/24
Internet
Gateway
Route
Tables
Network Access
Control List
4
EC2
Security Group
Private Subnet 1a

	Security Group 	Network Access Control List 
Rules	It supports only **Allow Rules**	It supports **both Allow and Deny** rules
Default by AWS	By default, **inbound** rules are **Denied, outbound** rules are **Allow**	By default, all the rules are **Allowed**
* **Newly Created by User**	By default, **inbound** rules are **Denied, outbound** rules are **Allow**	By default, all the rules are **Denied*** until you add rules.
Add Rule	You need to add the rule which you'll **Allow**	You need to add the rule which you can **either Allow or Deny it**.
Stateful/Stateless	It is a **Stateful** means that any changes made in the inbound rule will be automatically reflected in the outbound rule	It is a **Stateless** means that any changes made in the inbound rule will not reflect the outbound rule
Association	1. It is **instance-based** 2. Instances can associate with **more than one** Security Groups	1. It is **subnet-based** 2. Subnets can **associate with only one** Network ACL

Internal Phone Number Range:



Internal Phone Number Range:


Internal Phone Number Range:
1-2-3-4-5.....100
CIDR
10.7.0.0/16
VPC
Internal Phone Network
Department: Finance:10-19
Manager :10
Vice-manager:11
(0532-324-54-43)
(0532-324-54-46)
Public IP :3.4.9.0/32
Private IP: 10.7.1.1/32
SUBNET CIDR
10.7.1.0/24
Private
Department IT:20-29
Developer: 20 (---) ***
Database: 21 (---)***
VIP
Public IP :----
Private IP: 10.7.2.1/32
10.7.2.0/24
10.7.3.0/24
Department Supply:30-39
Manager :30
(0532-324-54-78)
10.7.4.0/20
Department Marketing:40-49
Manager: 40
(0532-324-54-57)
Employee 41:
(0532-324-54-81)
TESLA
Account

Launching an Instance

Create in Public Subnet

Private IP

VPC CIDR Pool

+

Public IP

(Auto Assign IP)

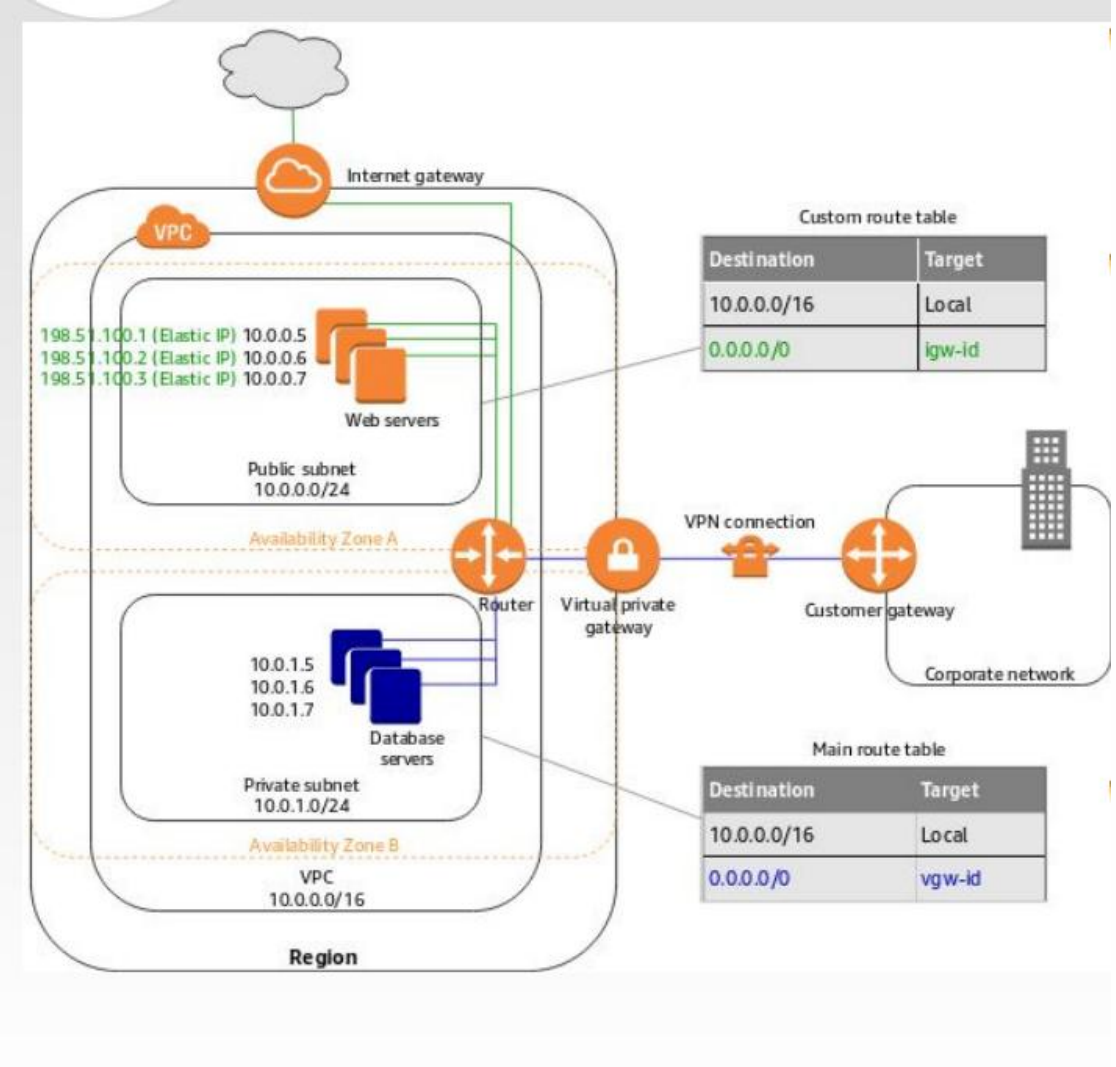
AWS IP POOL

Create in Private Subnet

Private IP

VPC CIDR Pool

Route Table

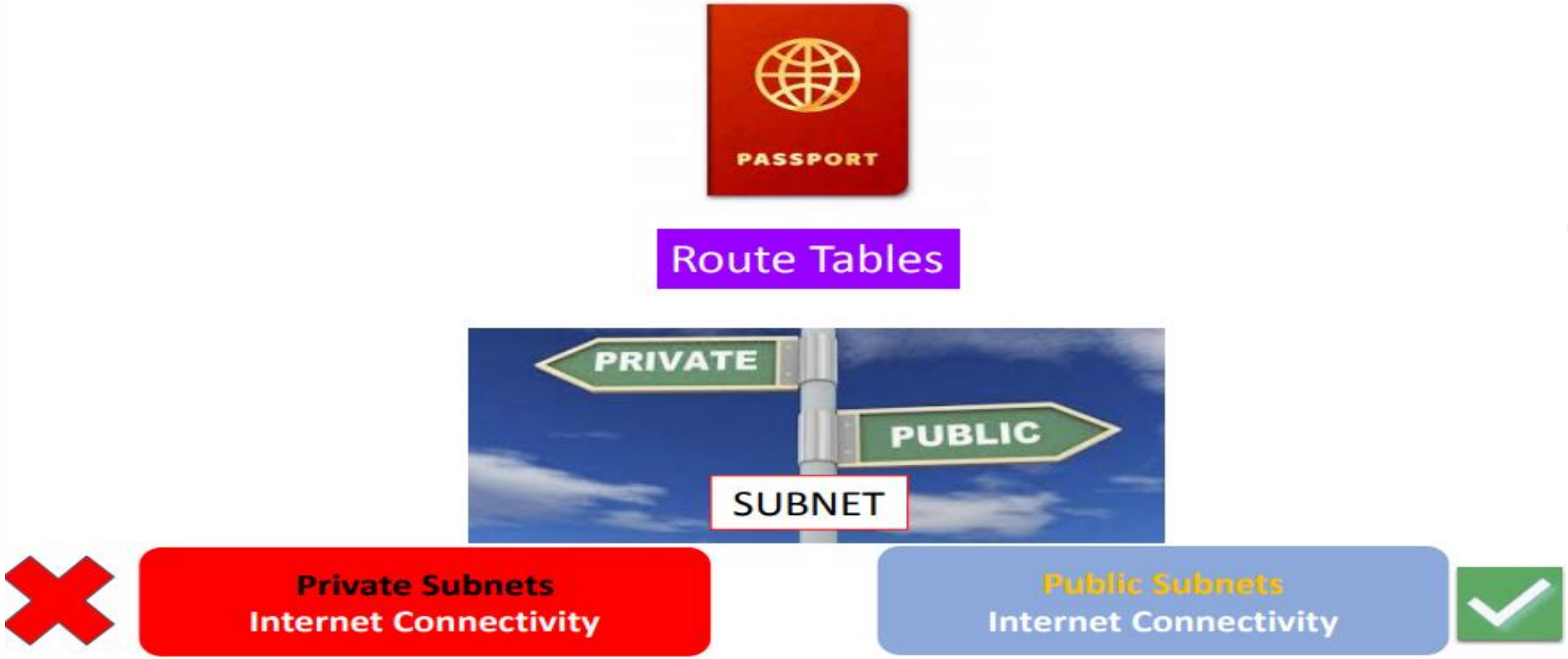


✓ **Your VPC has an implicit router**, and you use route tables to control where network traffic is directed.

✓ **Each subnet in your VPC must be associated with a route table**, which controls the routing for the subnet (subnet route table).

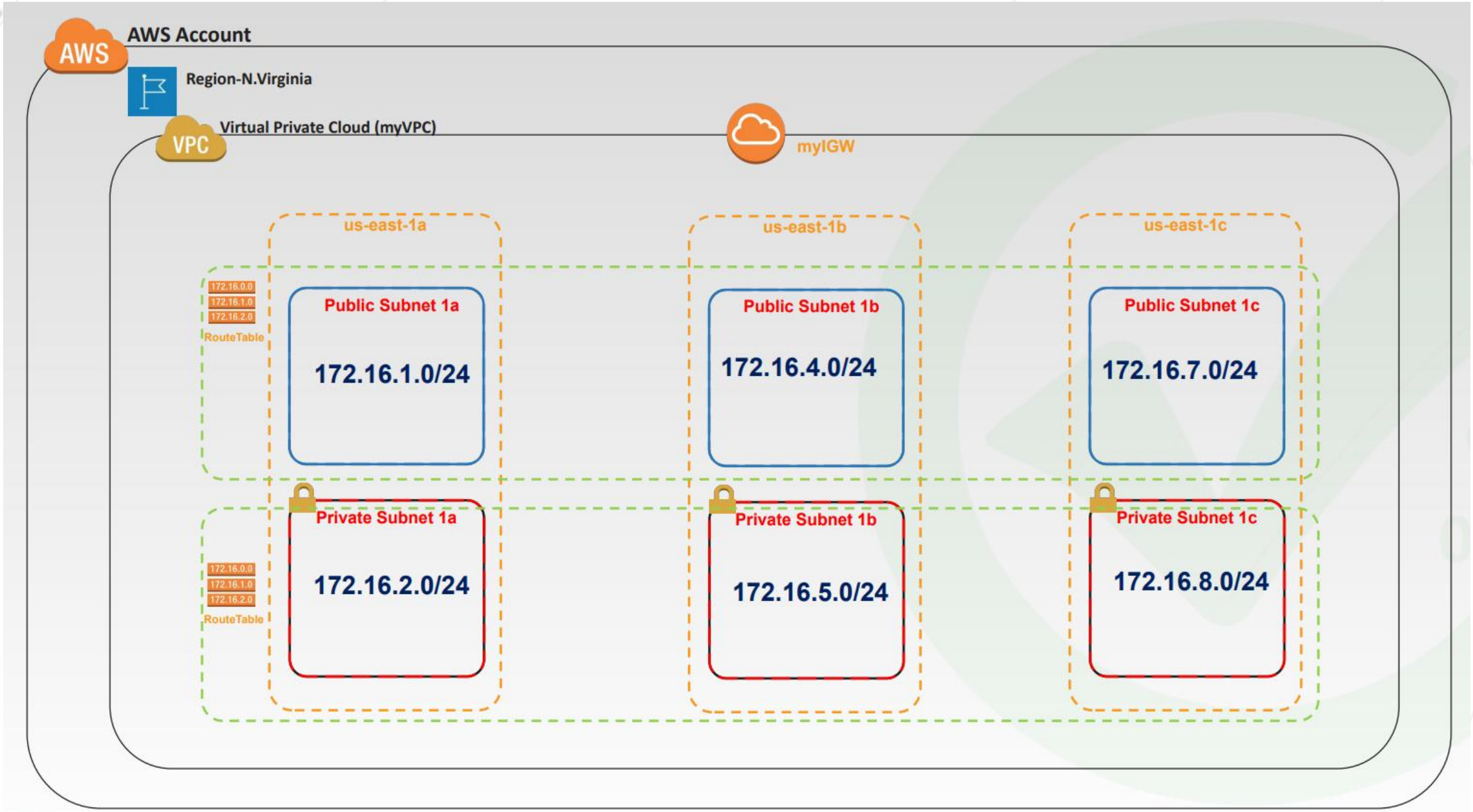
- You can explicitly associate a subnet with a particular route table.
- Otherwise, the subnet is implicitly associated with the main route table.

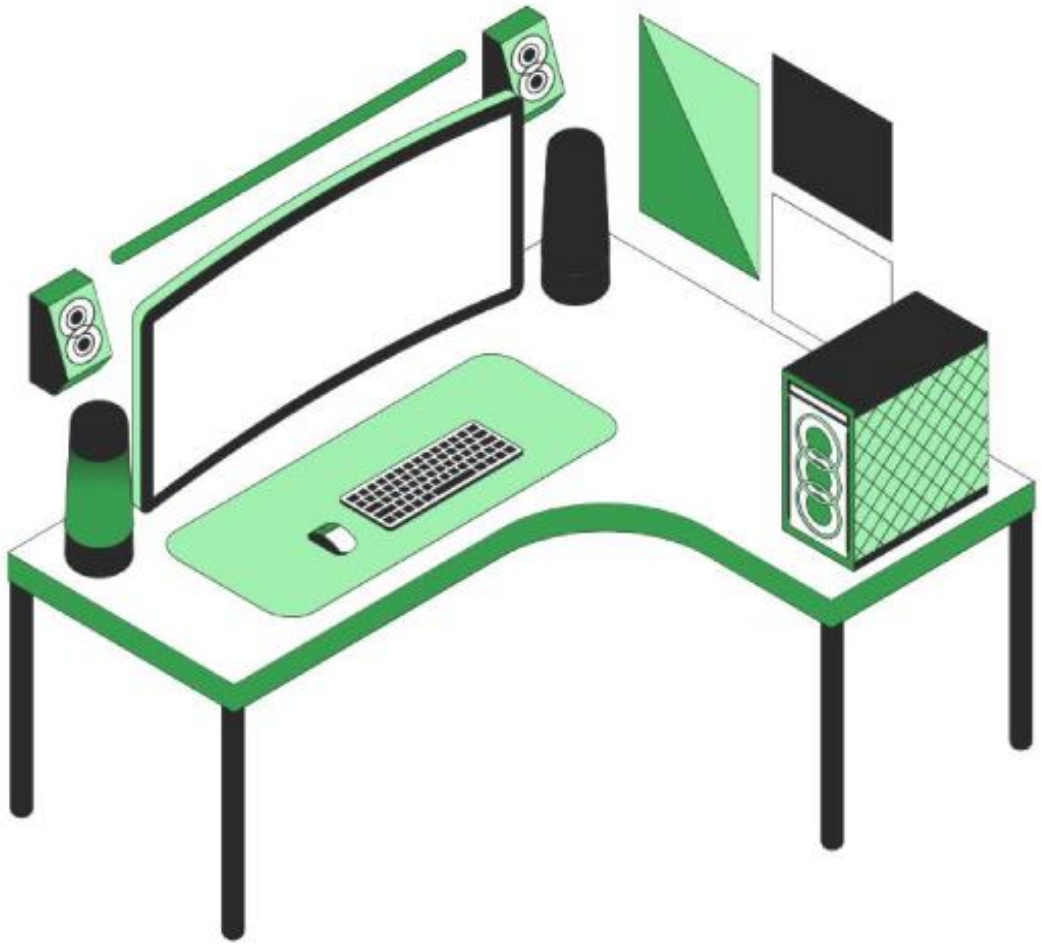
✓ **A subnet can only be associated with one route table at a time**, but you can associate multiple subnets with the same subnet route table.



"Route Tables" in AWS VPC (Virtual Private Cloud) are a collection of rules that determine how network traffic is directed. Each subnet within a VPC must be associated with one or more route tables, which define where the network traffic should be routed.


Cloud
VPC
Region
10.10.0.0/16
Local
İç Hatlar Giden Yolcu
Domestic Departures
2
10.10.1.0/24
10.10.020/24
10.10.3.0/24
Internet Gateway
Route Tables
PASSPORT
DIŞ HATLAR / INTERNATIONAL


AWS Account
Region-N.Virginia
Virtual Private Cloud (myVPC)
VPC
myIGW
us-east-1a
us-east-1b
us-east-1c
172.16.0.0
172.16.1.0
172.16.2.0
RouteTable
Public Subnet 1a
172.16.1.0/24
Public Subnet 1b
172.16.4.0/24
Public Subnet 1c
172.16.7.0/24
Private Subnet 1a
172.16.2.0/24
Private Subnet 1b
172.16.5.0/24
Private Subnet 1c
172.16.8.0/24



Do you have any questions?

Send it to us! We hope you learned something new.