BATCH :	B107 AWS-DevOps
LESSON :	**AWS**
DATE :	06.03.2023
SUBJECT :	**VPC-1**

ZOOM GİRİŞLERİNİZİ LÜTFEN **LMS** SİSTEMİ ÜZERİNDEN YAPINIZ

VPC and its Components

What is VPC?

- ✔ Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined.

- ✔ Amazon VPC is a logically isolated area, isolated network in the AWS Cloud.

VPC Components

The following are the key concepts for VPCs:

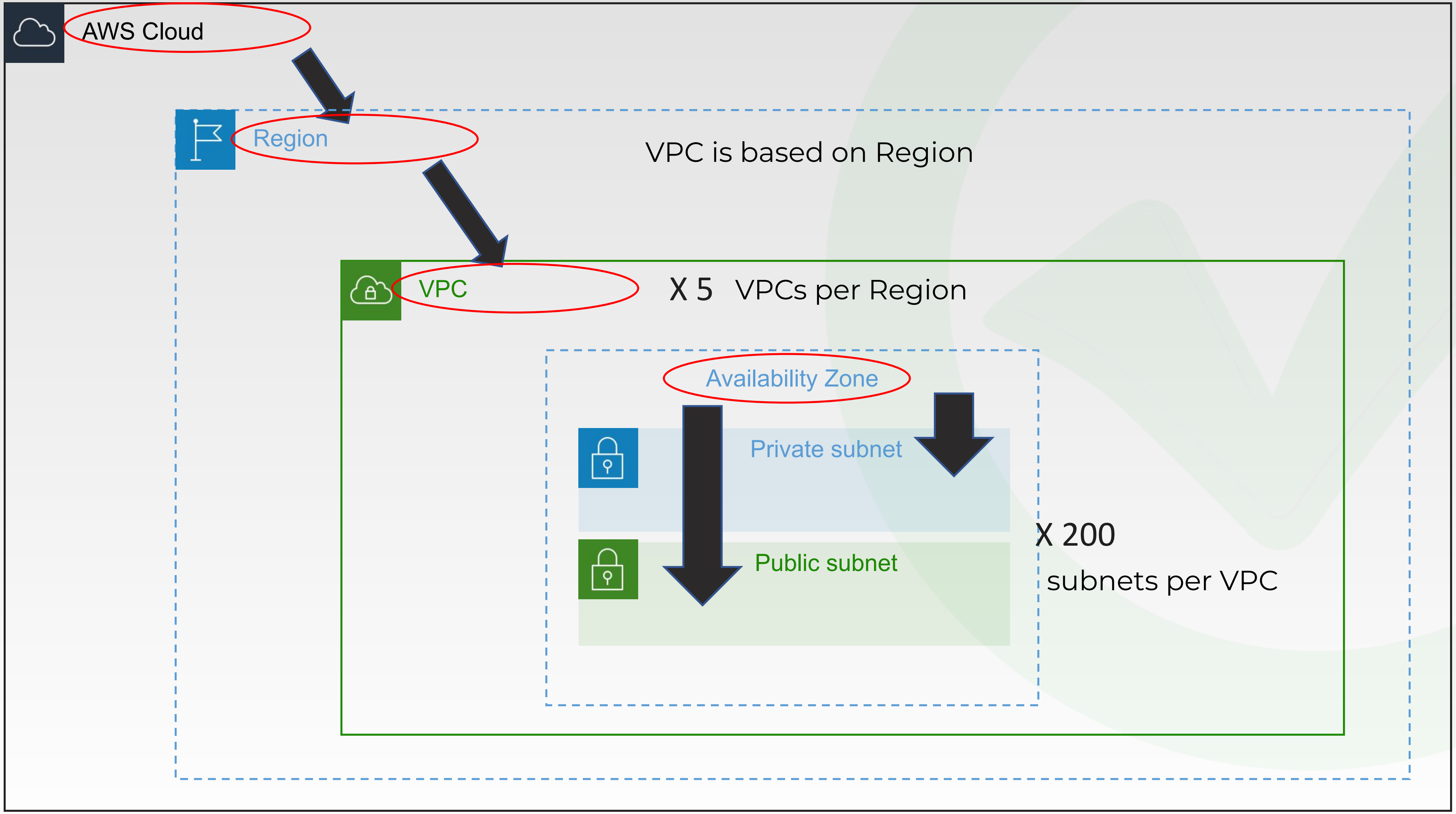
- ✔ **Virtual private cloud (VPC)** — A virtual network dedicated to your AWS account.
- ✔ **Subnet** — A segment of VPC's IP address range.
- ✔ **Route table** — A set of rules, called routes, that are used to determine where network traffic is directed.
- ✔ **Internet gateway** — A gateway that you 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 to capture and inspect network traffic in VPC.
  - ○ You route traffic to security services.
  - ○ Capture packets
  - ○ Used for troubleshooting, content inspection, threat monitoring
- ✔ **Flow Logs** — Capture information about IP traffic inside VPC
  - ○ Logs can be sent to S3 or CloudWatch
- ✔ **Network Firewall** — Layer 3 to Layer 7 managed network firewall and intrusion prevention/detection service that allows customers to filter traffic at the perimeter of their VPC.

VPC Components (Region, VPC, AZ, Subnets)

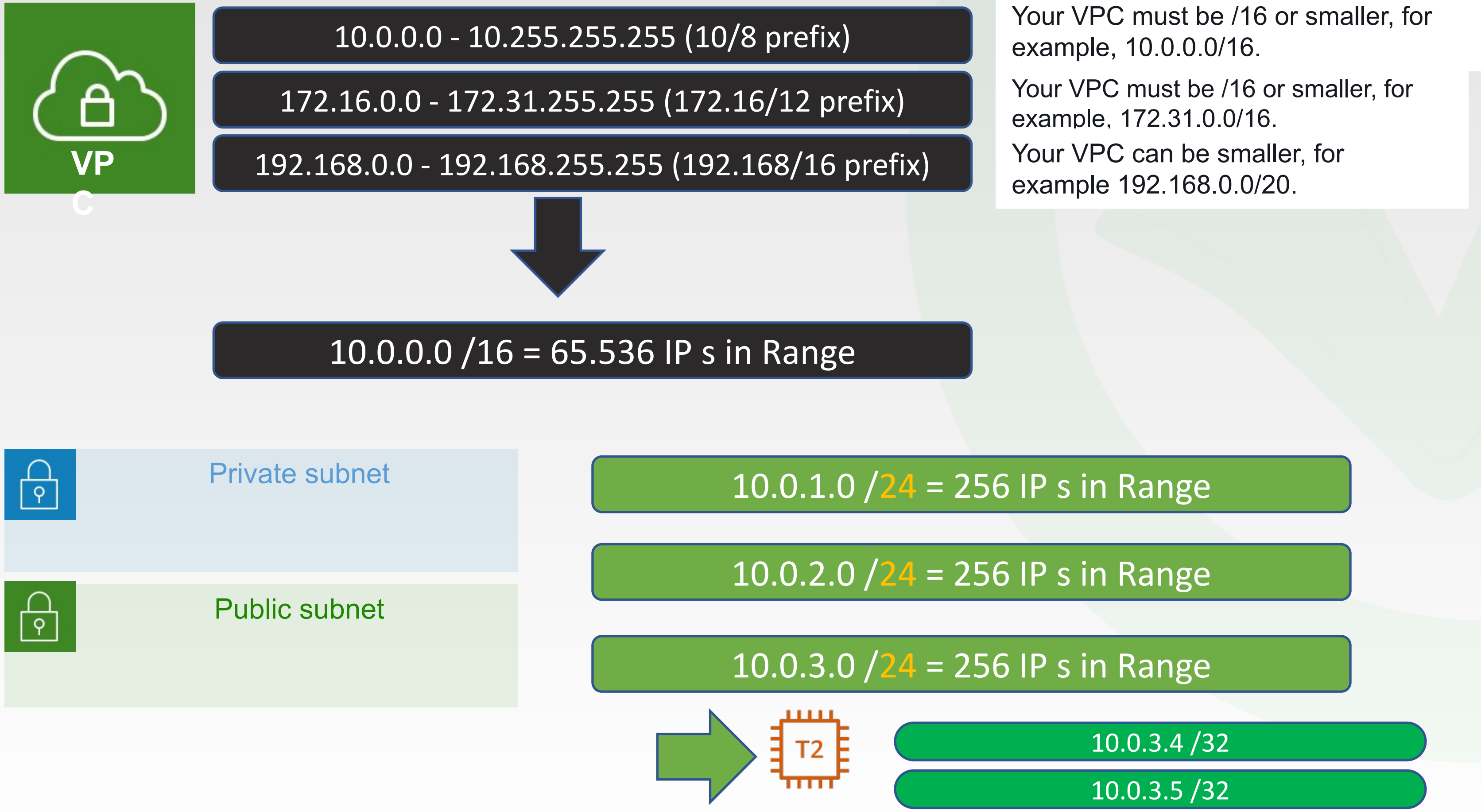


VPC Components (CIDR)

- ✔ **CIDR block** —Classless Inter-Domain Routing

An internet protocol address allocation and route aggregation methodology.

- ✔ Use IP address guide to work around. https://www.ipaddressguide.com/cidr



10.0.0.0 - 10.255.255.255 (10/8 prefix)

172.16.0.0 - 172.31.255.255 (172.16/12 prefix)

192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

Your VPC must be /16 or smaller, for example, 10.0.0.0/16.

Your VPC must be /16 or smaller, for example, 172.31.0.0/16.

Your VPC can be smaller, for example 192.168.0.0/20.

10.0.0.0 /16 = 65.536 IP s in Range

10.0.1.0 /24 = 256 IP s in Range

10.0.2.0 /24 = 256 IP s in Range

10.0.3.0 /24 = 256 IP s in Range

10.0.3.4 /32

10.0.3.5 /32

VPC Components (CIDR)

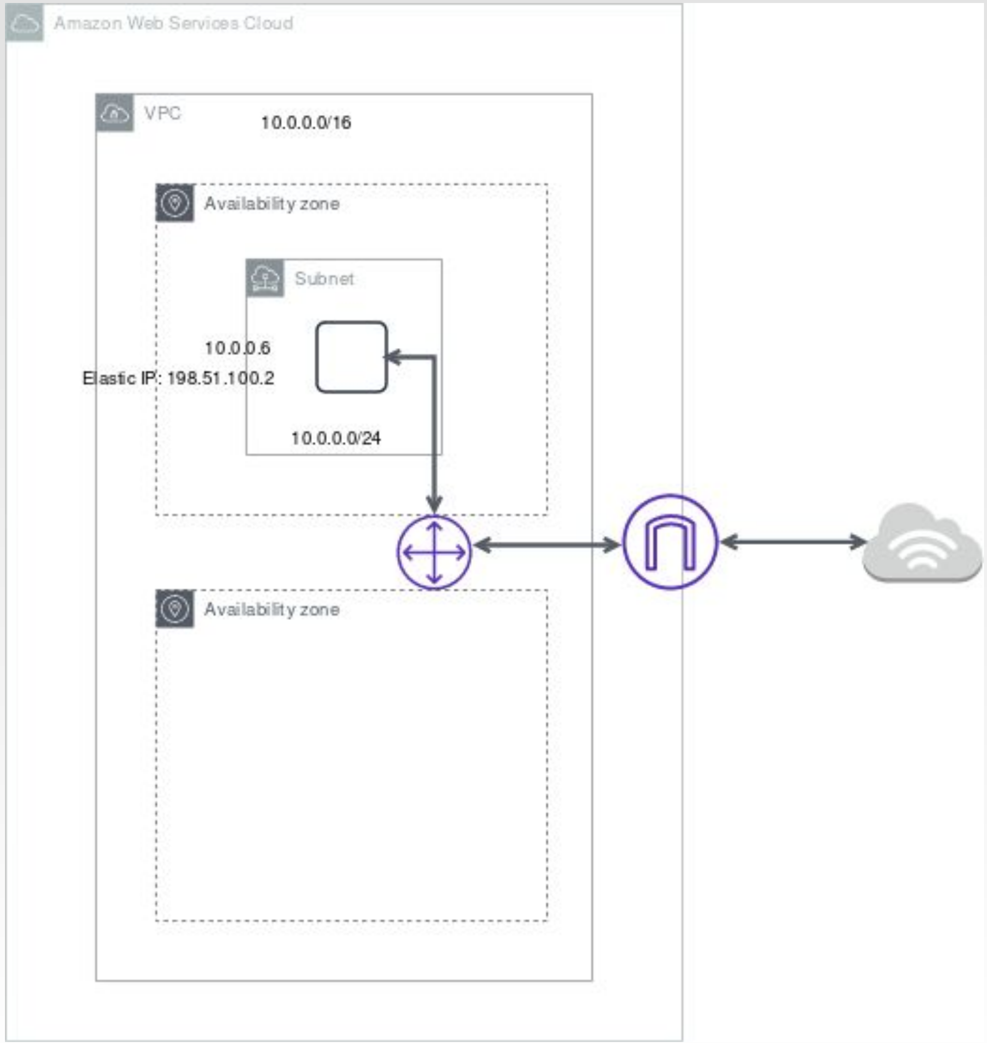
✔ The first four IP addresses and the last IP address in each subnet CIDR block are not available for you to use, and cannot be assigned to an instance. For example, in a subnet with CIDR block 10.0.0.0/24, the following five IP addresses are reserved:

- ❑ 10.0.0.0: Network address.
- ❑ 10.0.0.1: Reserved by AWS for the VPC router.
- ❑ 10.0.0.2: Reserved by AWS.
- ❑ 10.0.0.3: Reserved by AWS for future use.
- ❑ 10.0.0.255: Network broadcast address. AWS does not support broadcast in a VPC, therefore this address is reserved.

CIDR Best Practices

- Plan VPC first
- Bigger CIDR blocks are better (more flexible)
- Smaller subnets are fine for most use cases
- Deploy application tiers per subnet
- Avoid overlapping CIDR blocks
- Split your HA resources across subnets in different AZs

VPC Components (Internet Gateway)



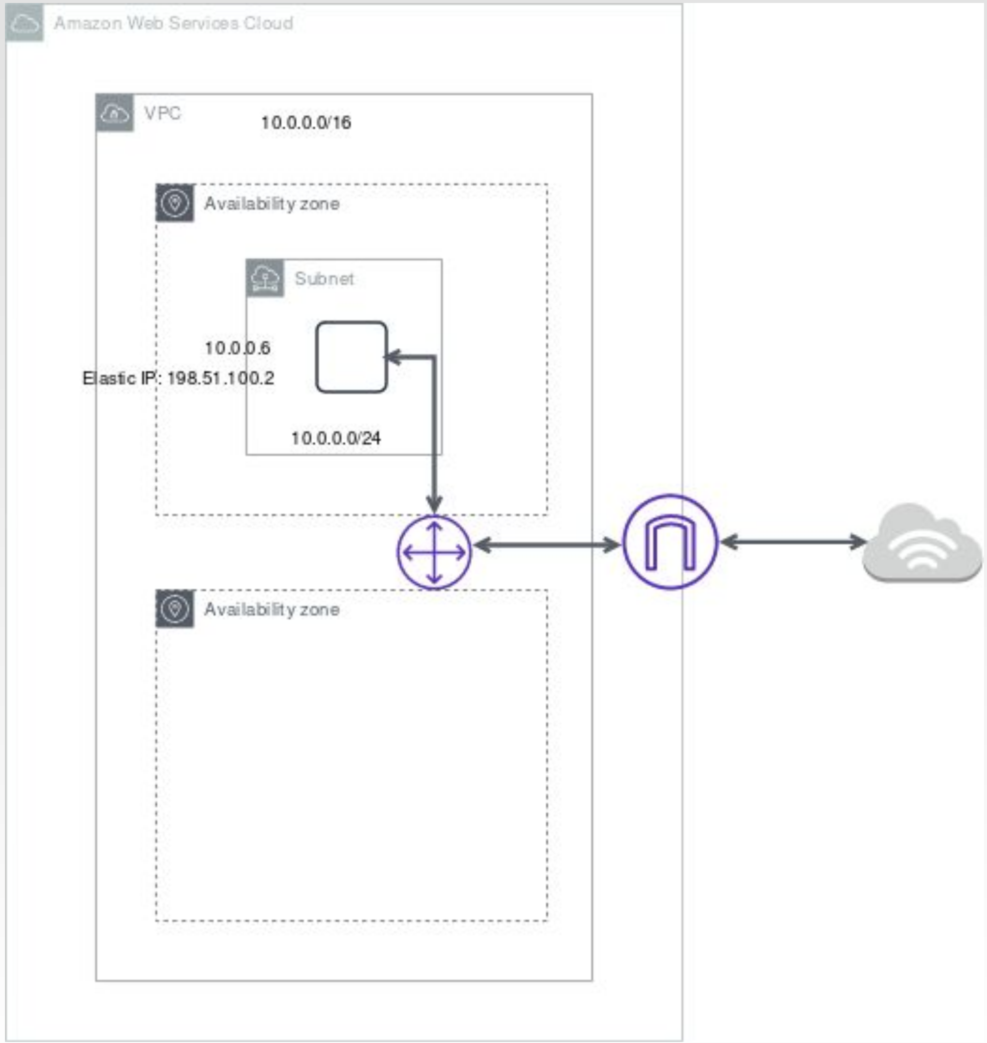
✔ An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet.

✔ 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.

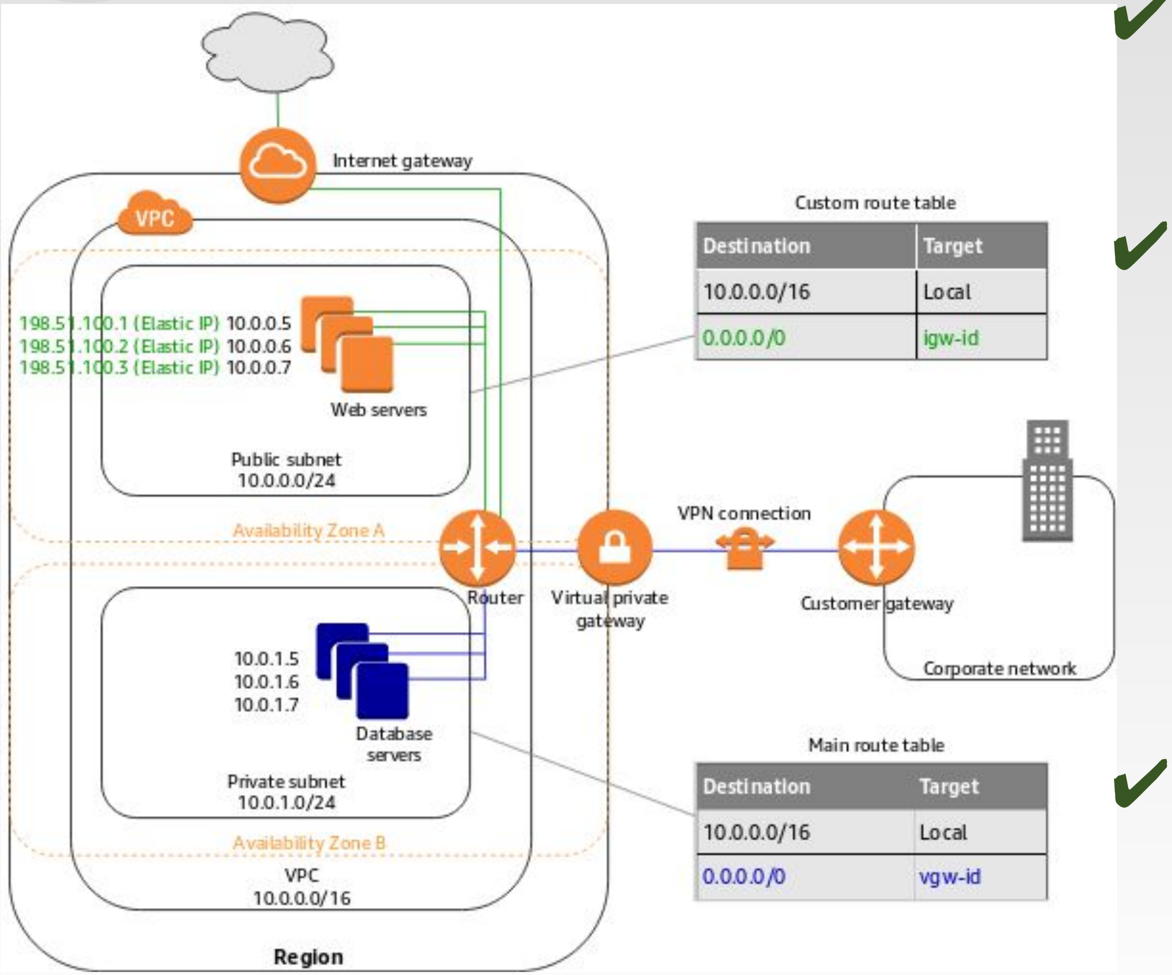
(for IPv6, NAT is not needed as they are all public.)

VPC Components



- ✔ IP addresses are given by AWS from an Address Pool.
- ✔ If the IP addresses finish within the CIDR block, the instances can not get IP addresses.
- ✔ To solve it you should define additional CIDR block for the VPC.

VPC Components (Route Table)



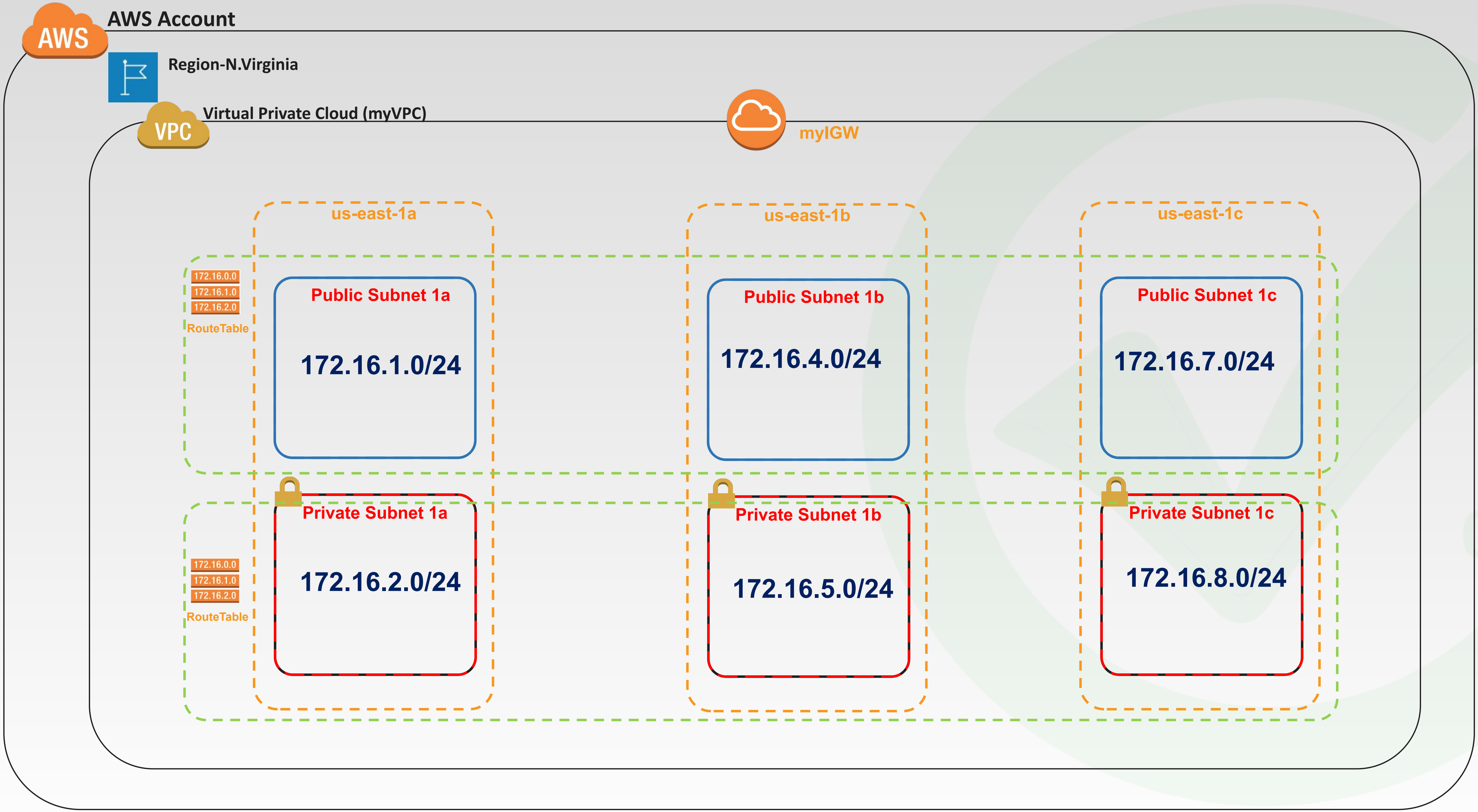
Custom route table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	igw-id

Main route table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	vgw-id

- ✔ 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.



AWS

AWS Account

Region-N.Virginia

VPC

Virtual Private Cloud (myVPC)

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

172.16.0.0
172.16.1.0
172.16.2.0
RouteTable

Private Subnet 1a

172.16.2.0/24

Private Subnet 1b

172.16.5.0/24

Private Subnet 1c

172.16.8.0/24

Solution Architect Cases

1 How can you capture information about IP traffic inside your VPCs?

Enable VPC Flow Logs

2 You have a VPC in your AWS account that runs in a dual-stack mode. You are continuously trying to launch an EC2 instance, but it fails. After further investigation, you have found that you no longer have IPv4 addresses available. What should you do?

Add an additional IPv4 CIDR to your VPC

3 We need an AWS service that allows us to protect and control traffic in our VPC from layer 3 to layer 7. What is your advice?

Network Firewall

4 A web application is hosted on a fleet of EC2 instances managed by an Auto Scaling Group. You are exposing this application through an Application Load Balancer. Both the EC2 instances and the ALB are deployed on a VPC with the following CIDR 192.168.0.0/18. How do you configure the EC2 instances' security group to ensure only the ALB can access them on port 80?

Add an Inbound Rule with port 80 and ALB's Security Group as the source

Solution Architect Cases

5 What is the scope of a VPC?

Region AZ Subnet

6 What level do you attach an Internet Gateway?

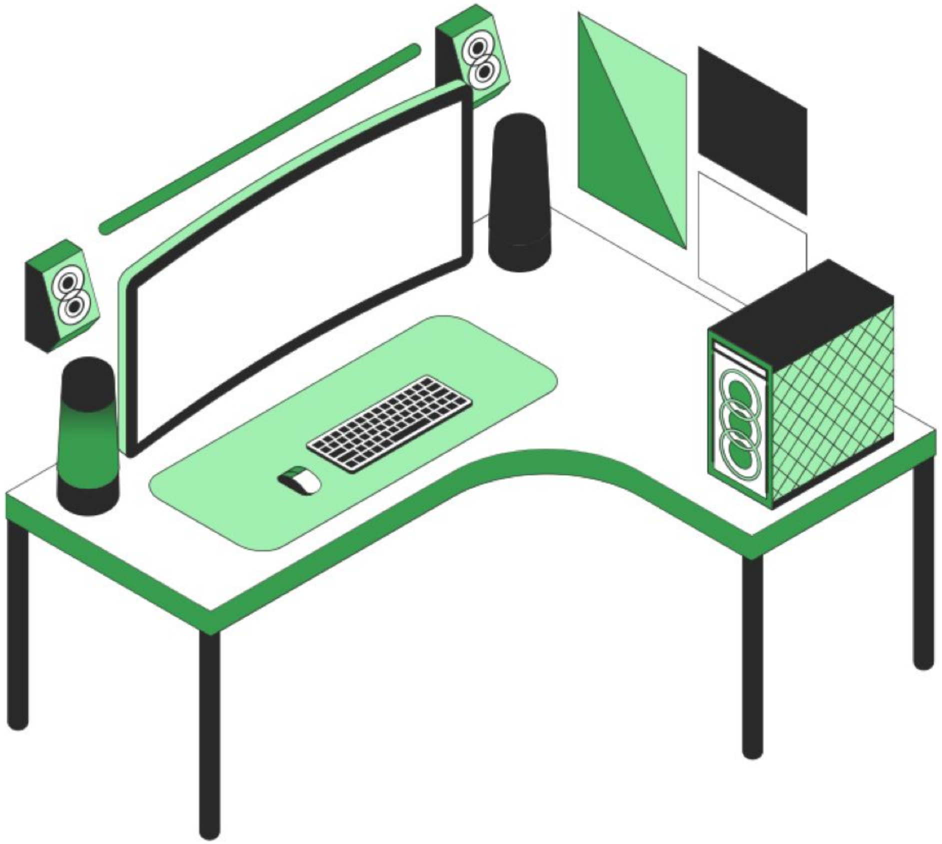
Public Subnet Private Subnet AZ VPC

7 You plan on creating a subnet and want it to have at least capacity for 28 EC2 instances. What's the minimum size you need to have for your subnet?

/28 /27 /26 /25

8 You need to apply a firewall to a group of EC2 instances launched in multiple subnets. Which option should be used?

Security Group NACL Network Firewall



Do you have any questions?

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