BATCH : BATCH 85

LESSON : **AWS DAY 18**

DATE : 26.08.2022

SUBJECT : **VPC-1**

techproeducation

techproeducation

techproeducation

techproeducation

techproedu

VPC

What is VPC?

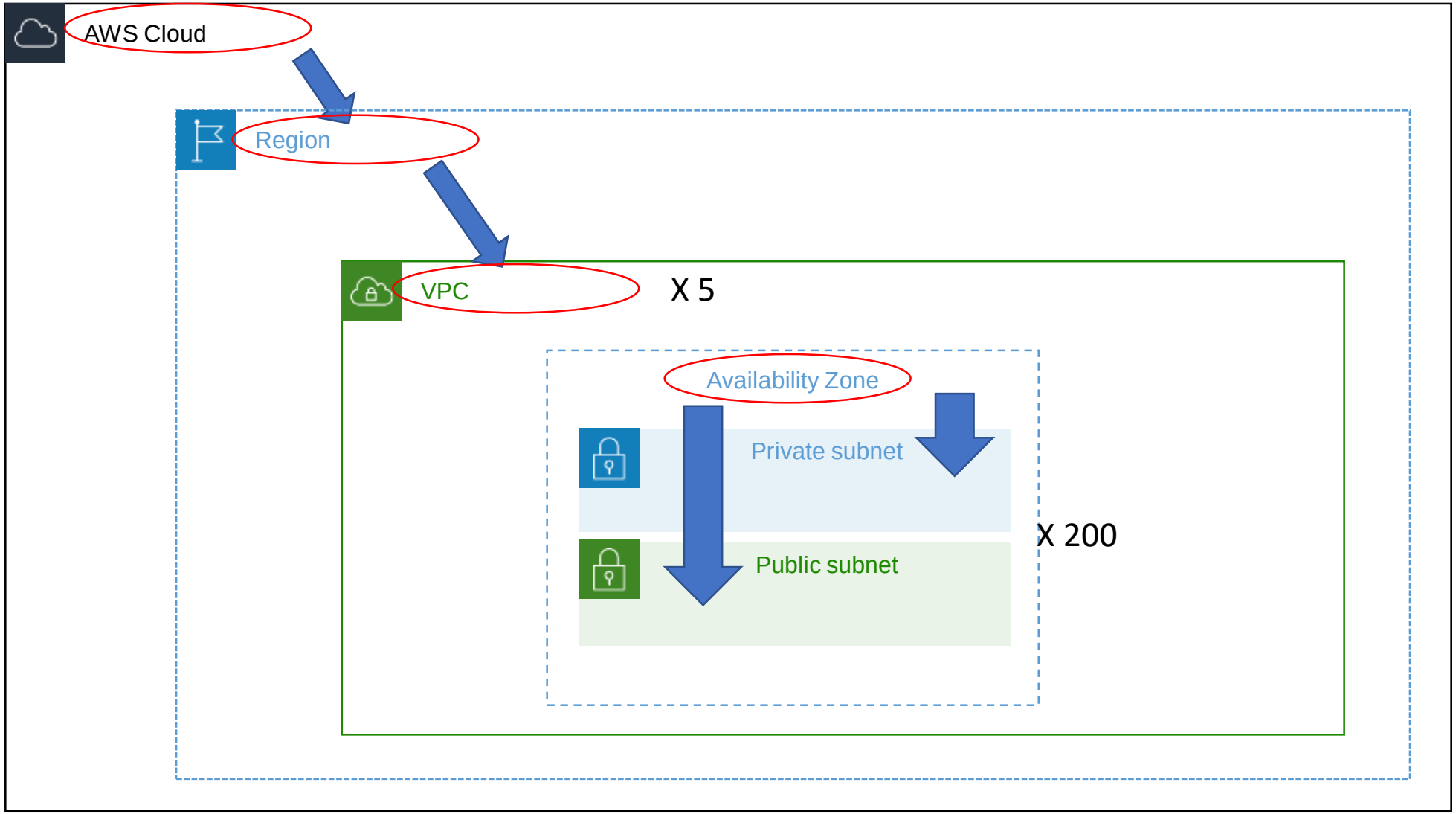
- ✓ Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined.
- ✓ Amazon VPC is a logically isolated area of the AWS Cloud.

VPC Components

The following are the key concepts for VPCs:

- ✓ **Virtual private cloud (VPC)** — A virtual network dedicated to your AWS account.
- ✓ **Subnet** — A range of IP addresses in your VPC.
- ✓ **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.
- ✓ **VPC endpoint** — Enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network. For more information, see AWS PrivateLink and VPC endpoints.
- ✓ **CIDR block** —Classless Inter-Domain Routing. An internet protocol address allocation and route aggregation methodology. For more information.

VPC Components (Region, VPC, AZ, Subnets)



VPC Components (CIDR)

- ✓ **CIDR block** —Classless Inter-Domain Routing.
- ✓ An internet protocol address allocation and route aggregation methodology.

Subnet Mask	CIDR	Binary Notation	Available Addresses Per Subnet
255.255.255.255	/32	11111111.11111111.11111111.11111111	1
255.255.255.254	/31	11111111.11111111.11111111.11111110	2
255.255.255.252	/30	11111111.11111111.11111111.11111100	4
255.255.255.248	/29	11111111.11111111.11111111.11111000	8
255.255.255.240	/28	11111111.11111111.11111111.11110000	16
255.255.255.224	/27	11111111.11111111.11111111.11100000	32
255.255.255.192	/26	11111111.11111111.11111111.11000000	64
255.255.255.128	/25	11111111.11111111.11111111.10000000	128
255.255.255.0	/24	11111111.11111111.11111111.00000000	256
255.255.254.0	/23	11111111.11111111.11111110.00000000	512
255.255.252.0	/22	11111111.11111111.11111100.00000000	1024
255.255.248.0	/21	11111111.11111111.11111000.00000000	2048
255.255.240.0	/20	11111111.11111111.11110000.00000000	4096
255.255.224.0	/19	11111111.11111111.11100000.00000000	8192
255.255.192.0	/18	11111111.11111111.11000000.00000000	16384
255.255.128.0	/17	11111111.11111111.10000000.00000000	32768
255.255.0.0	/16	11111111.11111111.00000000.00000000	65536
255.254.0.0	/15	11111111.11111110.00000000.00000000	131072
255.252.0.0	/14	11111111.11111100.00000000.00000000	262144
255.248.0.0	/13	11111111.11111000.00000000.00000000	524288
255.240.0.0	/12	11111111.11110000.00000000.00000000	1048576
255.224.0.0	/11	11111111.11100000.00000000.00000000	2097152
255.192.0.0	/10	11111111.11000000.00000000.00000000	4194304
255.128.0.0	/9	11111111.10000000.00000000.00000000	8388608
255.0.0.0	/8	11111111.00000000.00000000.00000000	16777216
254.0.0.0	/7	11111110.00000000.00000000.00000000	33554432
252.0.0.0	/6	11111100.00000000.00000000.00000000	67108864
248.0.0.0	/5	11111000.00000000.00000000.00000000	134217728
240.0.0.0	/4	11110000.00000000.00000000.00000000	268435456
224.0.0.0	/3	11100000.00000000.00000000.00000000	536870912
192.0.0.0	/2	11000000.00000000.00000000.00000000	1073741824
128.0.0.0	/1	10000000.00000000.00000000.00000000	2147483648
0.0.0.0	/0	00000000.00000000.00000000.00000000	4294967296

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)

10.0.0.0 /16 = 65.536 IP s in Range

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.

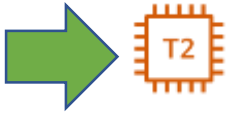
Private subnet

Public subnet

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

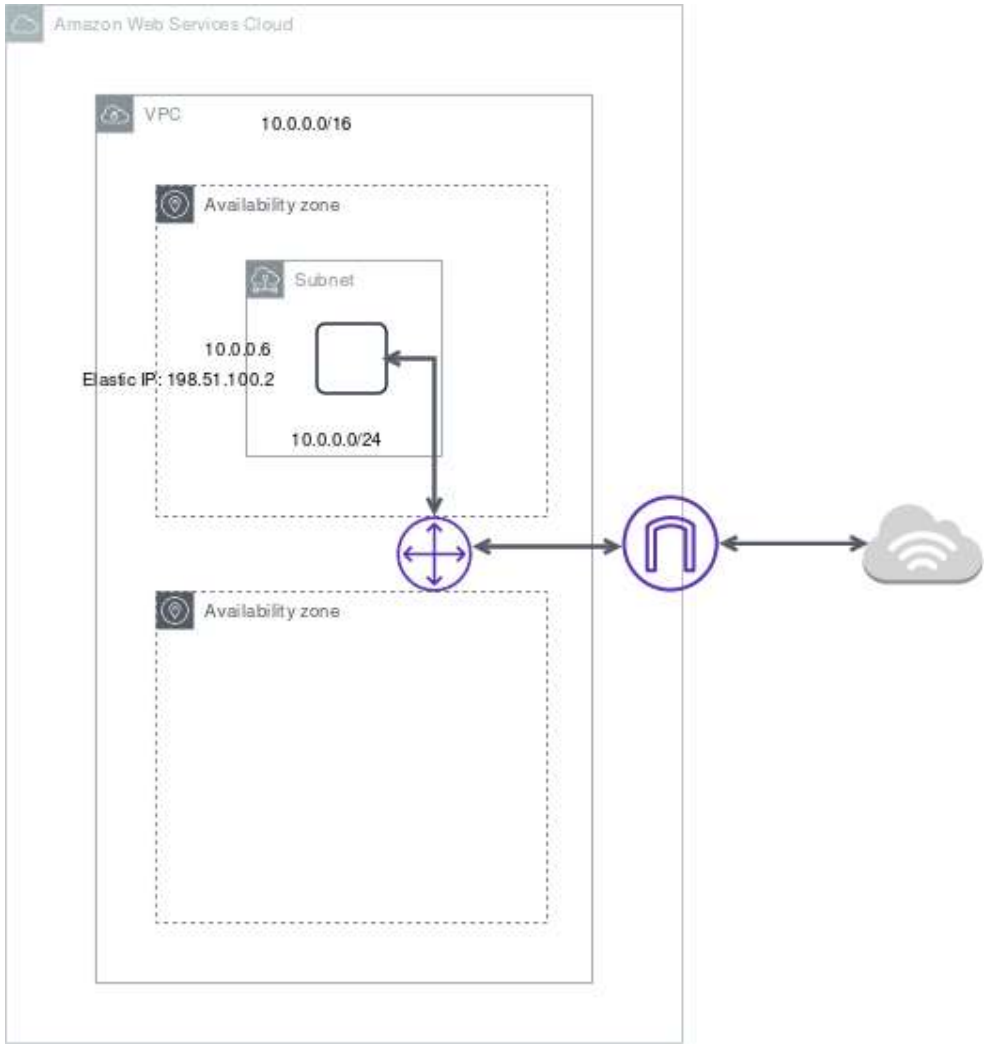
10.0.3.5 /32

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:

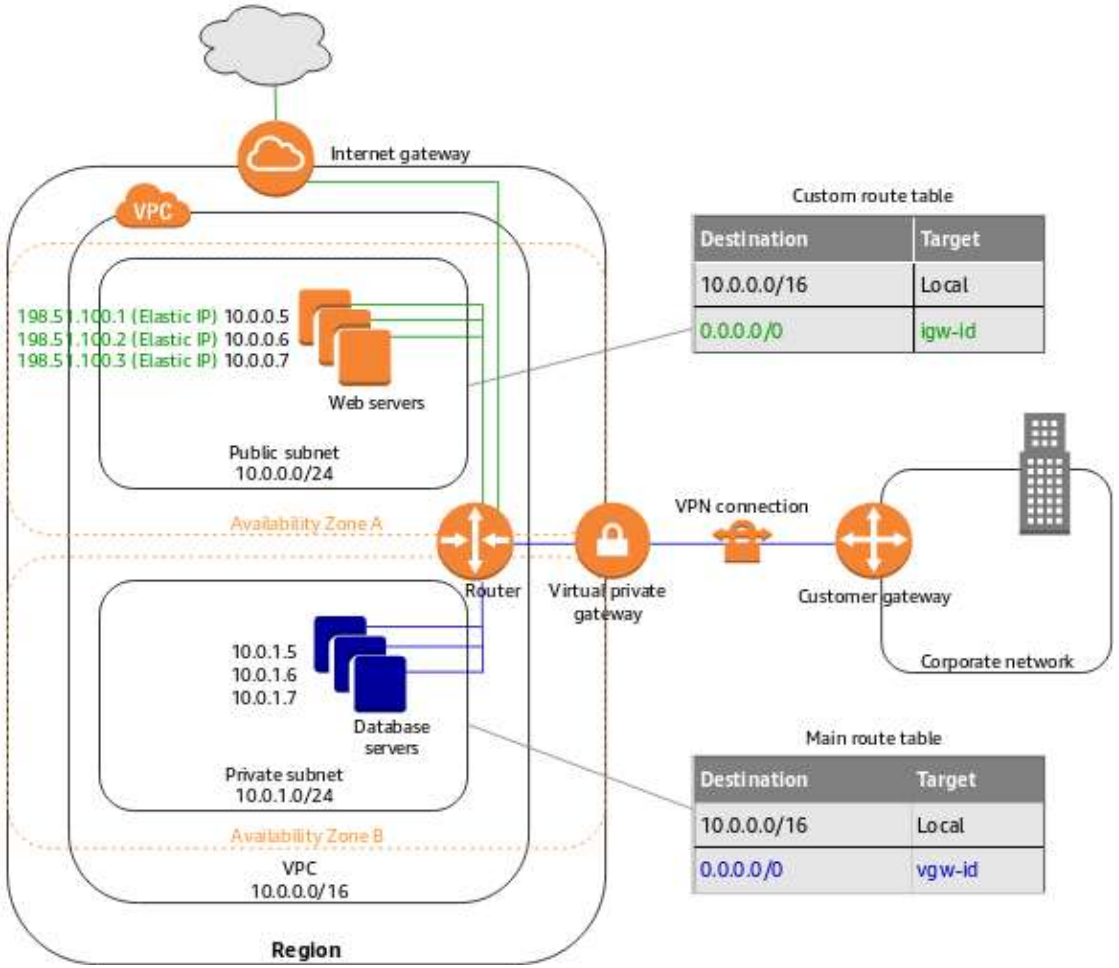
  - ❑ 10.0.0.0: Network address.
  - ❑ 10.0.0.1: Reserved by AWS for the VPC router.
  - ❑ 10.0.0.2: Reserved by AWS. The IP address of the DNS server is the base of the VPC network range plus two. For VPCs with multiple CIDR blocks, the IP address of the DNS server is located in the primary CIDR. We also reserve the base of each subnet range plus two for all CIDR blocks in the VPC. For more information, see Amazon DNS server.
  - ❑ 10.0.0.3: Reserved by AWS for future use.
  - ❑ 10.0.0.255: Network broadcast address. We do not support broadcast in a VPC, therefore we reserve this address.

VPC Components (Internet Gateway)

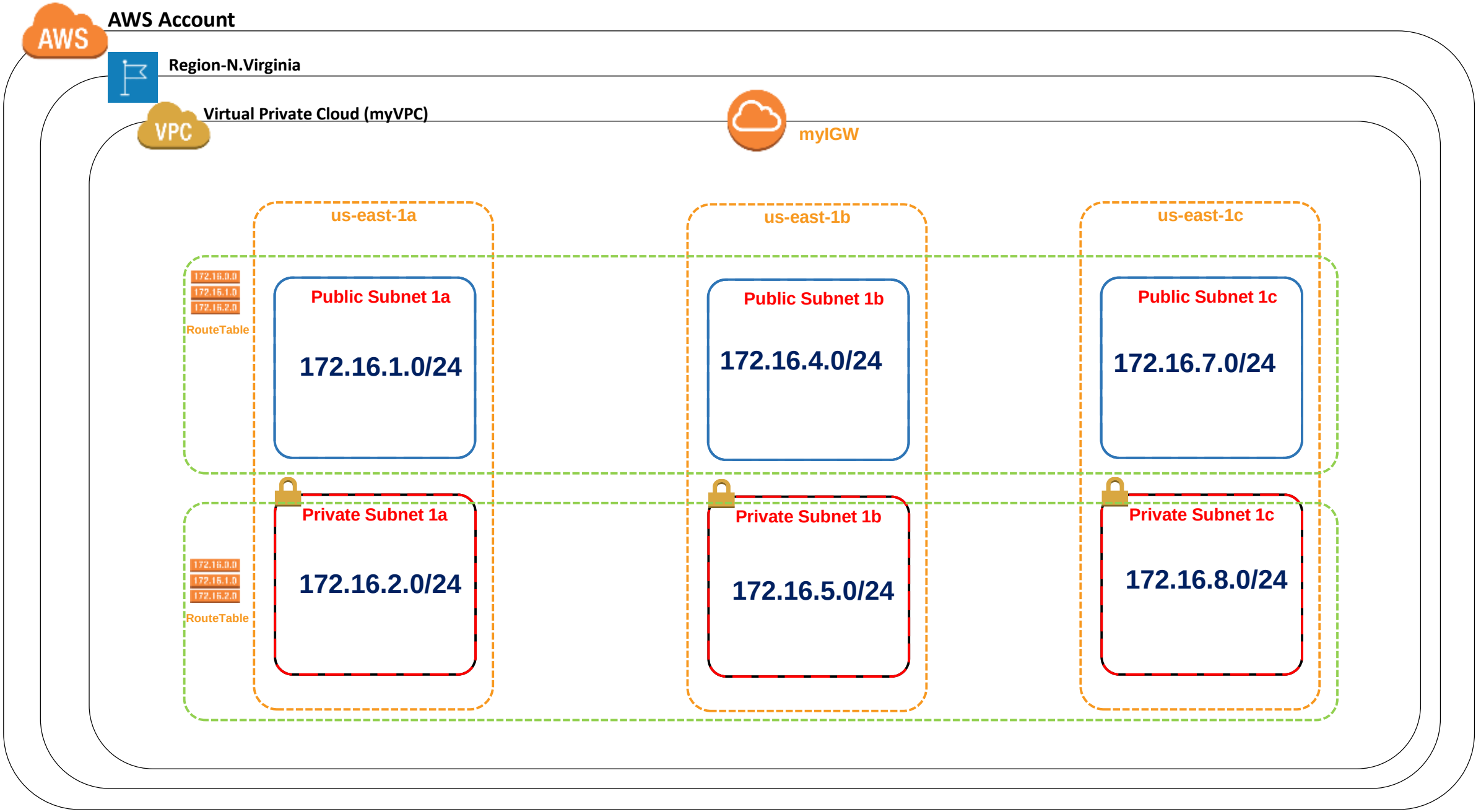


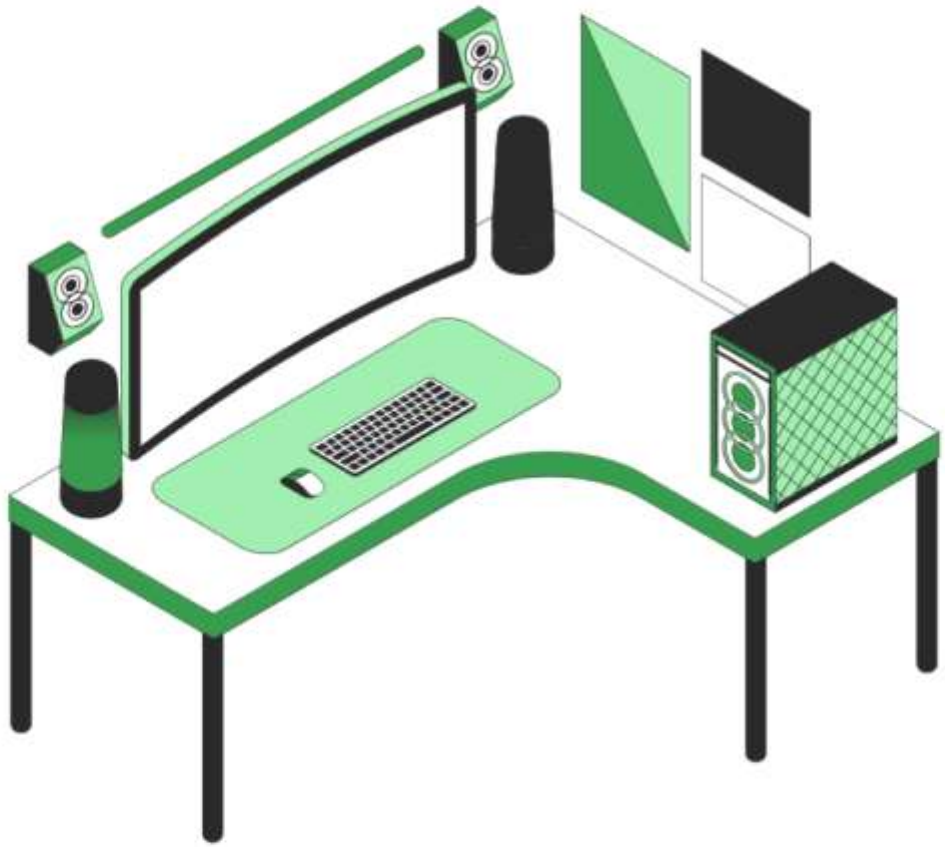
- ✓ An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet.
- ✓ An internet gateway serves two purposes:
  - ➢ to provide a target in your VPC route tables for ***internet-routable traffic,***
  - ➢ to perform ***network address translation (NAT)*** for instances that have been assigned ***public IPv4*** addresses. For more information, see Enable internet access.

VPC Components (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.


AWS Account
Region-N.Virginia
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
Private Subnet 1a
172.16.2.0/24
Private Subnet 1b
172.16.5.0/24
Private Subnet 1c
172.16.8.0/24
RouteTable



Do you have any questions?

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