



Amazon VPC





Table of Contents

-  Introduction to VPC
-  VPC Basic Components



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.
- So, VPC provides much better security control over your AWS resources.
- This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

VPC Basic Components

- VPC Region&AZ
- VPC Subnets
- VPC CIDR
- Internet Gateway
- Route Table and Router
- Security Group and Network ACL



► Region, AZ and Subnets

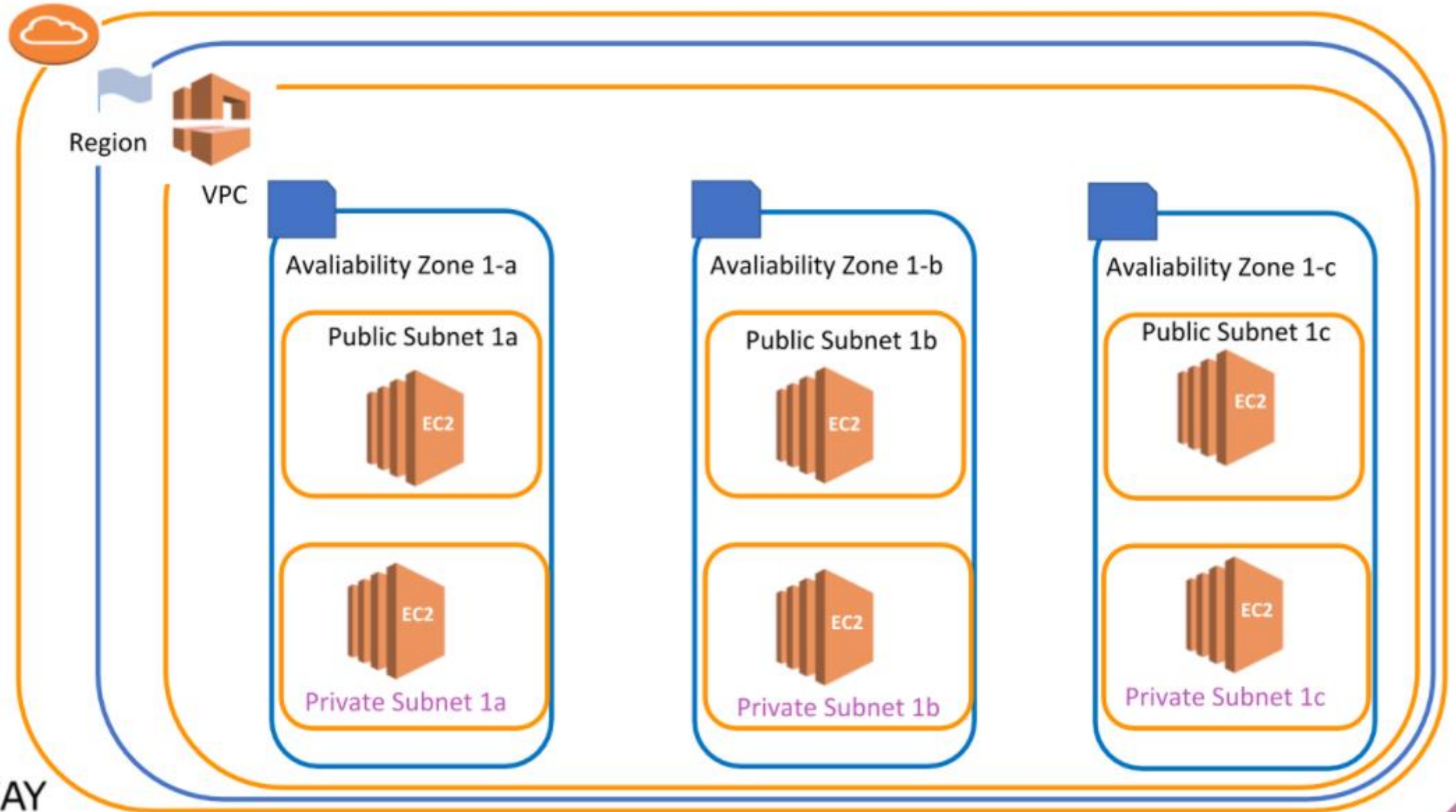


Region is a **physical location** around the world. AWS Region consists of multiple, isolated, and physically separate **AZ's where** data centers are located.

VPC is a isolated **virtual network** located **in a single region**.

A subnet is a logical partition of an IP network into VPC. There are two types of subnets; **Public Subnet** and **Private Subnet**.

Region, AZ and Subnets



VPC CIDR



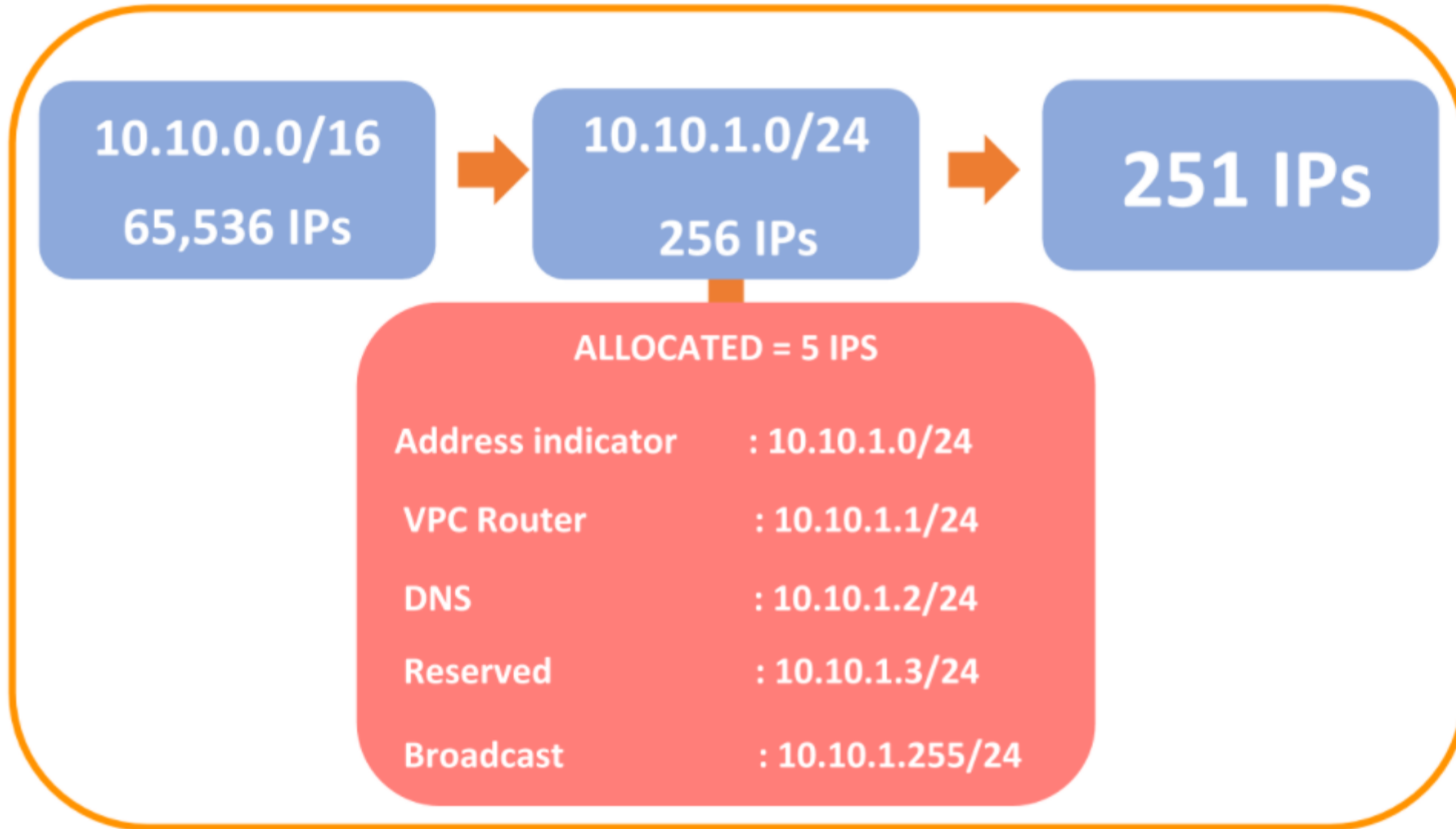
$10.0.0.0/16 = 65,536$ IPs in Range

$10.0.1.0/24 = 256$ IPs in Range

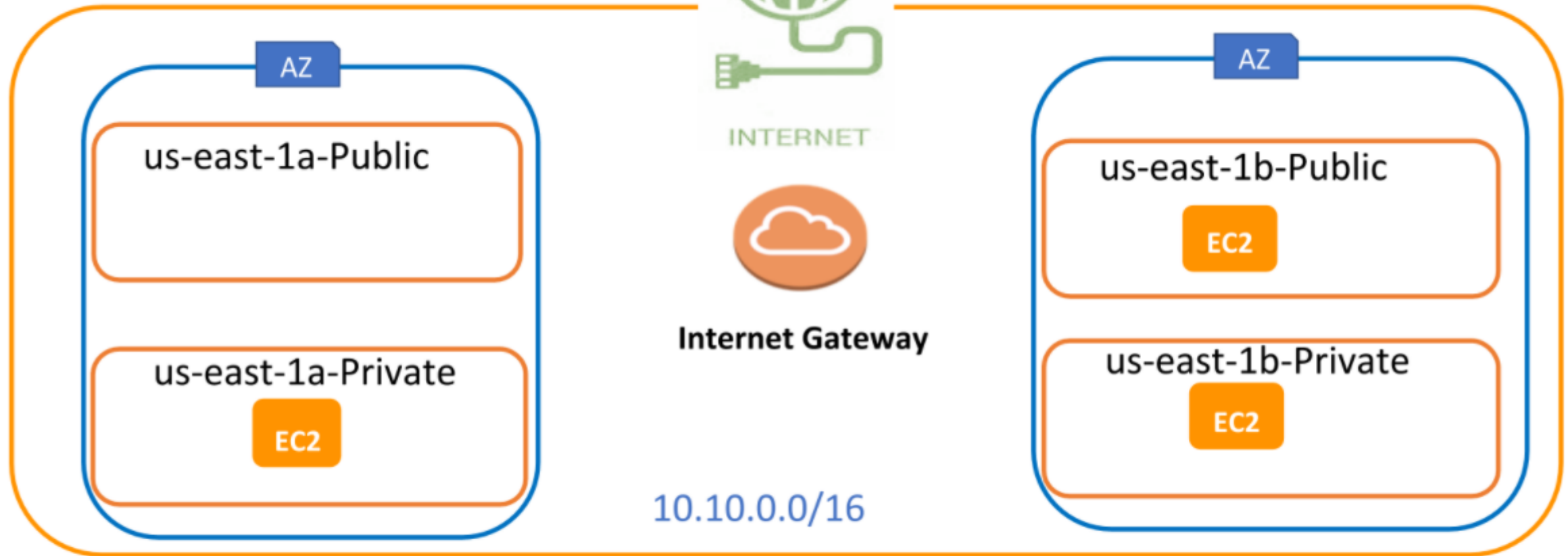
$10.0.1.0/32 = 1$ IP in Range

- 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.
- When you create a VPC, you must specify a range of IPv4 addresses for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block.
- As the Size Block (/16,24,32) increases, the number of IP located in CIDR Block decreases.

VPC CIDR



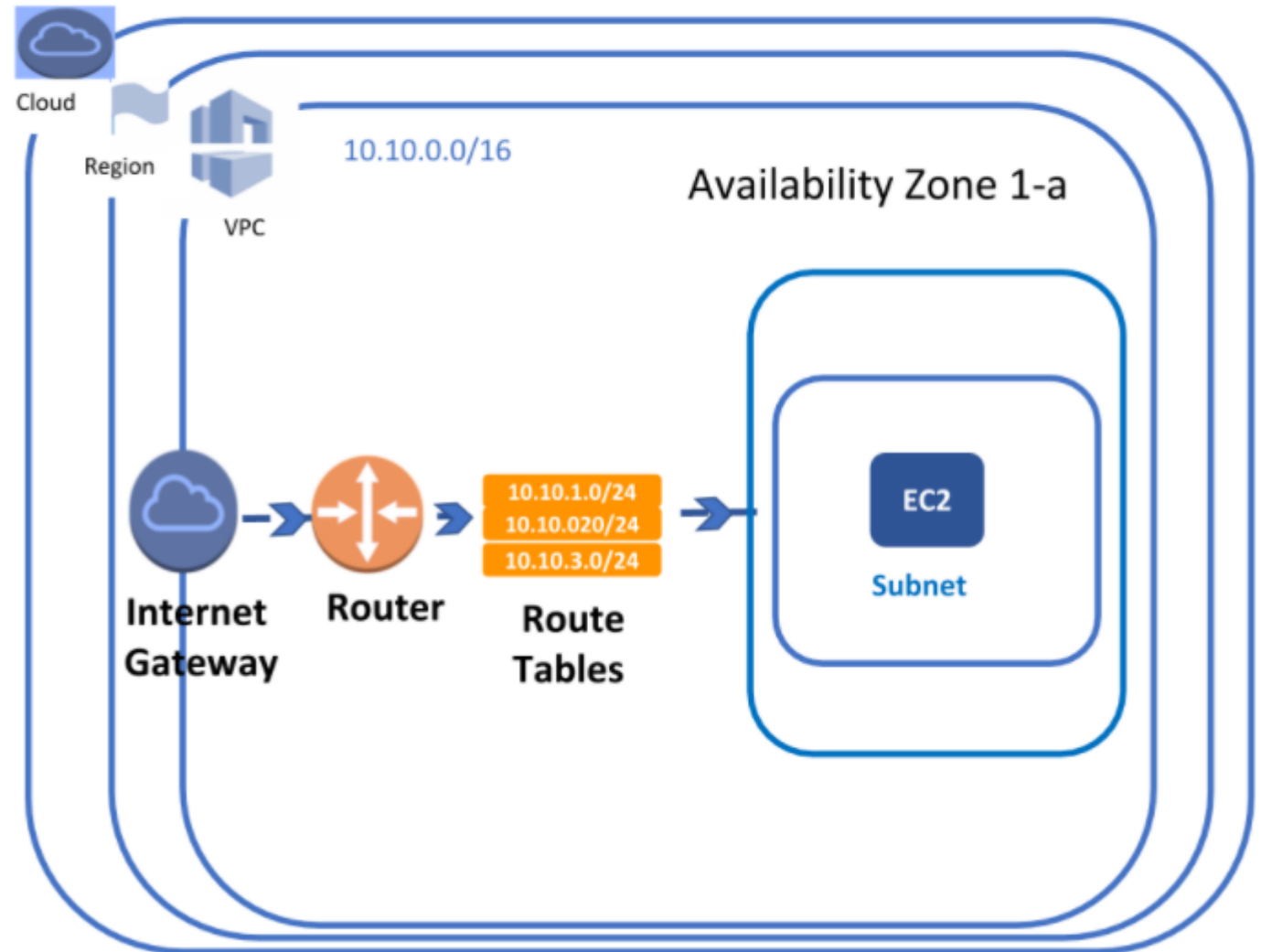
Internet Gateway



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

Route Table and Router

- **Route Table** is a **set of rules**, that is used to determine where VPC traffic is directed.
- **Routers** are components that **manage the Route Tables** and they act as “intersections” within the network.

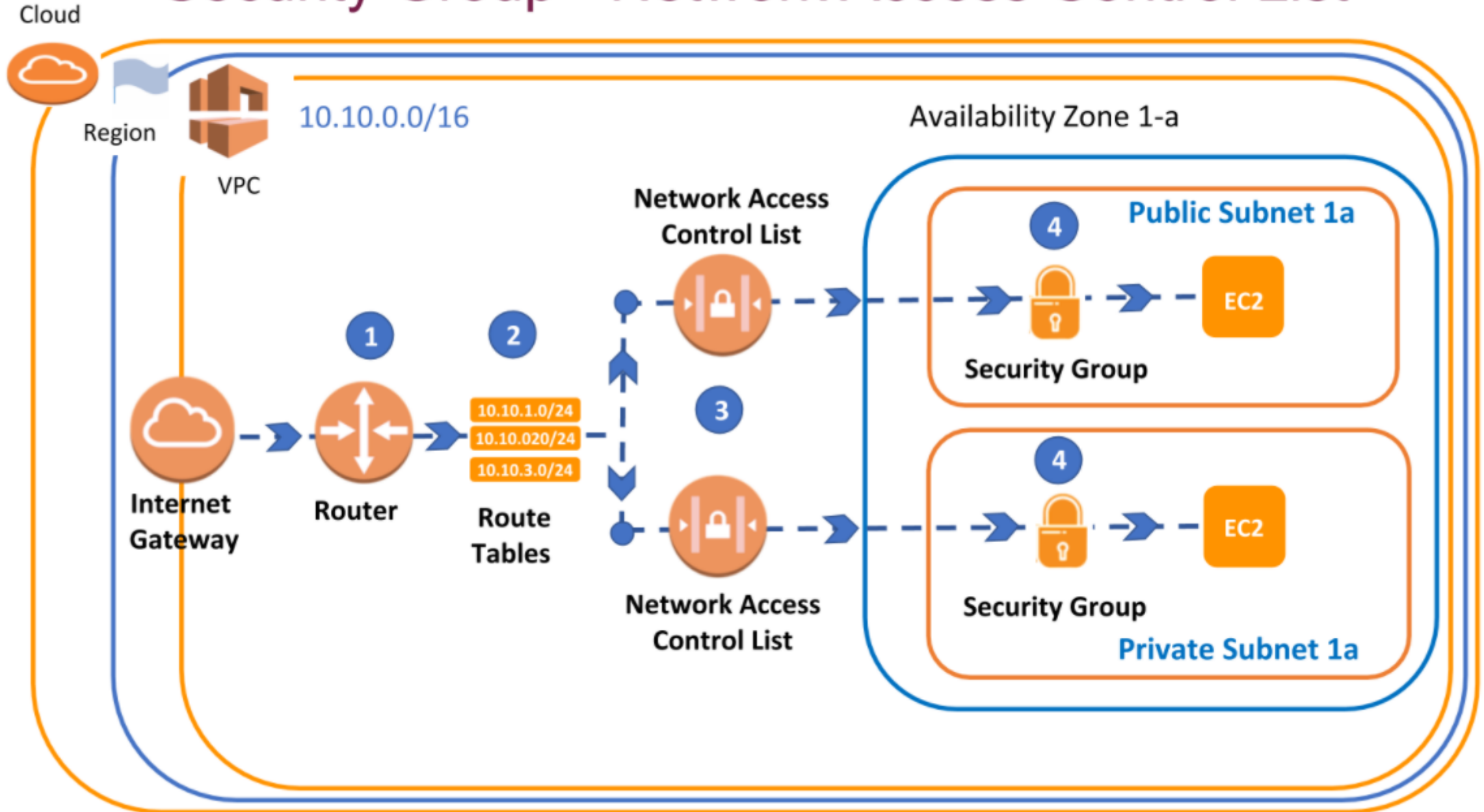




Network ACLs & Security Groups



- Network ACLs are subnet-based security components.
 - It controls the traffic in and out of subnets.
- Security Groups are instance-based security components,
 - They are used for determining which traffic will access the instance.
- Instance in subnet is affected by rules of both Security Groups and Network ACLs

Security Group - Network Access Control List



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	<ol style="list-style-type: none"> 1. It is instance-based 2. Instances can associate with more than one Security Groups 	<ol style="list-style-type: none"> 1. It is subnet-based 2. Subnets can associate with only one Network ACL

Network Access Control List

