Amazon VPC-1

Table of Contents

CLARUSWAY
WAY TO REINVENT YOURSELF

1 Introduction to VPC

Introduction to VPC

What is VPC?

Cloud
Region

VPC

Auto
Scaling

EC2

ELB

RDS

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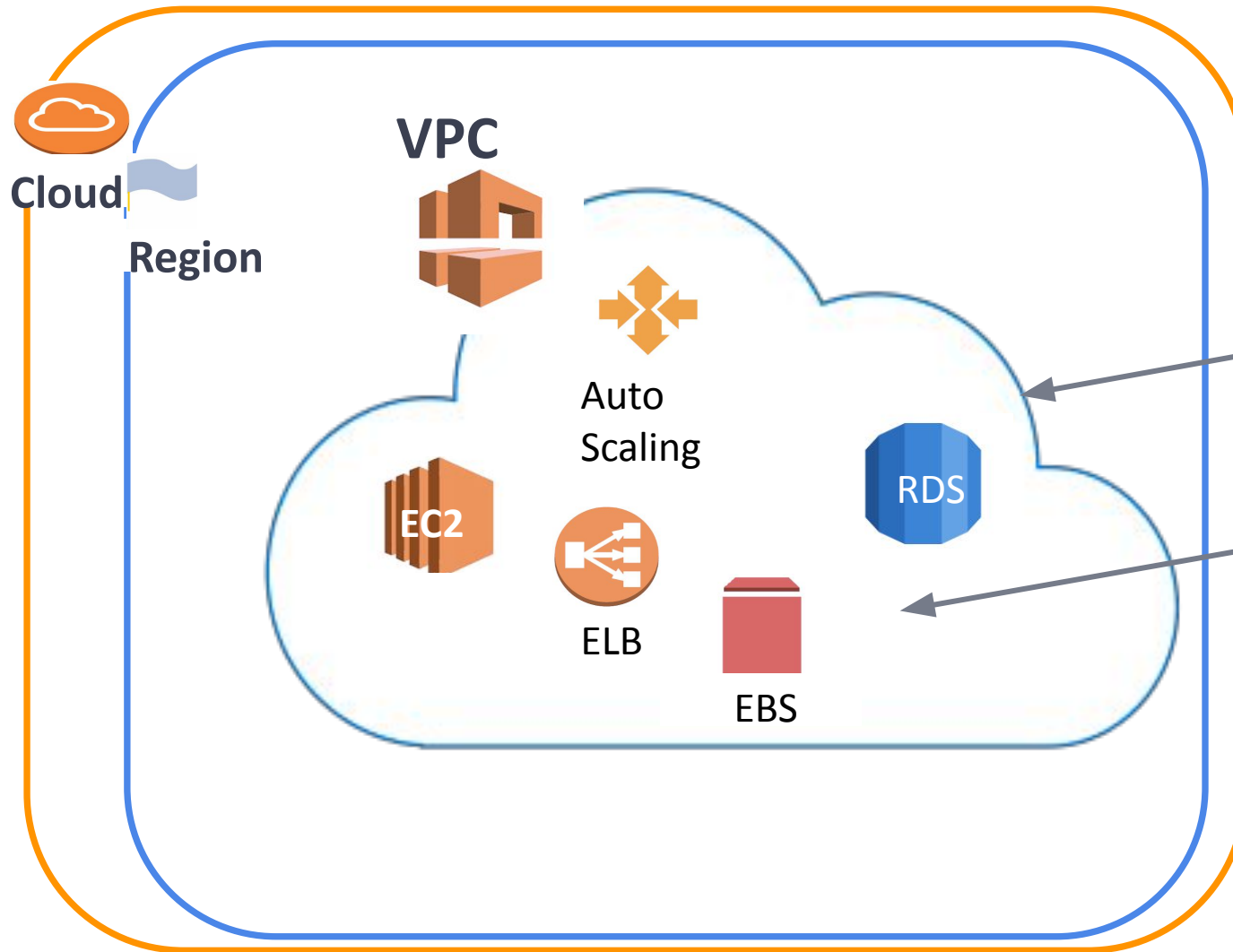
Amazon Virtual Private Cloud (Amazon VPC) is a logically isolated area of the AWS cloud where you can launch AWS resources in a virtual network that you define.
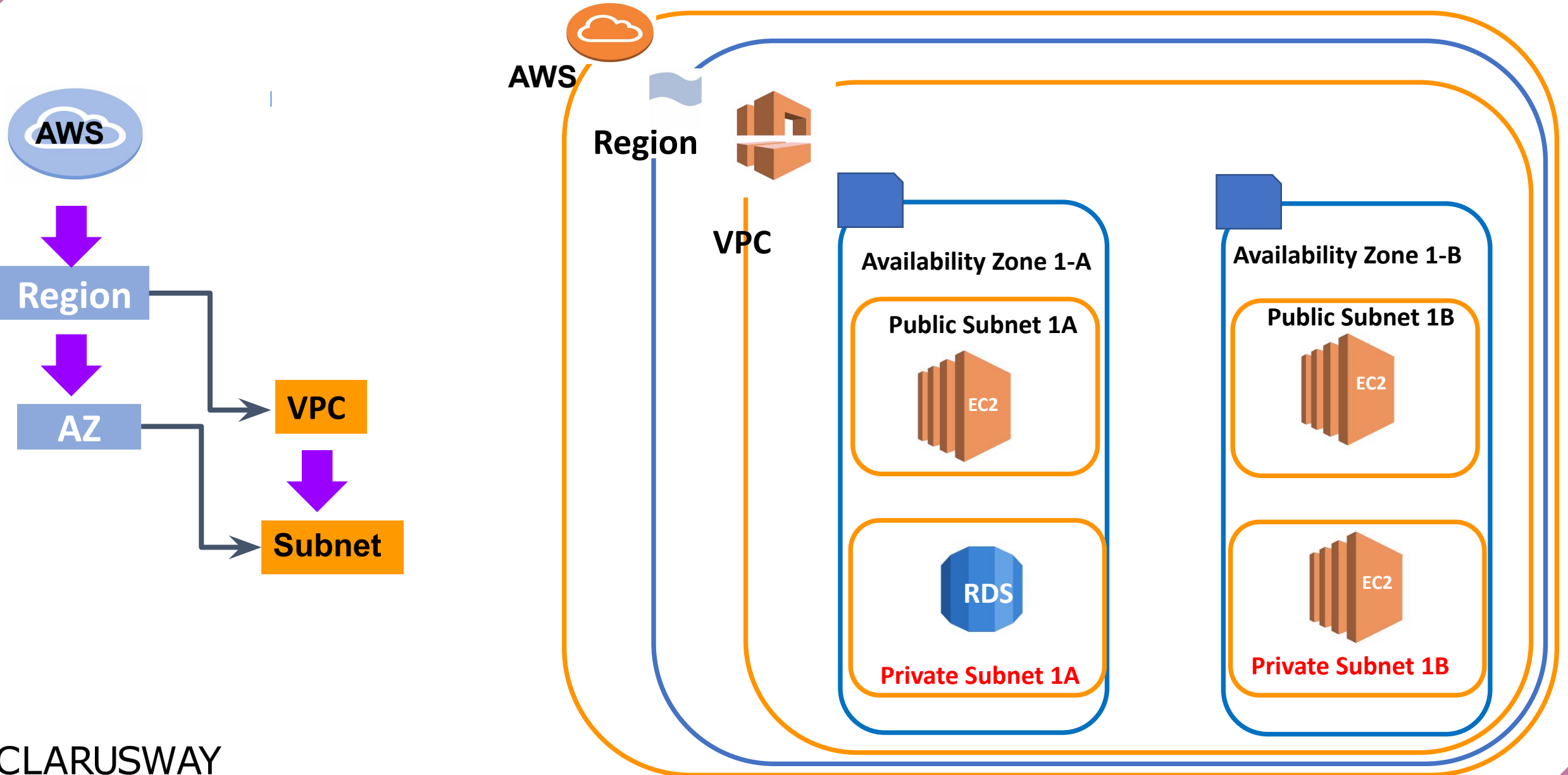
CLARUSWAY
WAY TO REINVENT YOURSELF

2 VPC Basic Components

VPC Basic Components

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

CLARUSWAY
WAY TO REINVENT YOURSELF

Region, VPC, AZ and Subnets

AWS → Region → VPC → Subnet

AWS → Region
Region → VPC
AZ → Subnet

AWS

Region

VPC

Availability Zone 1-A

Public Subnet 1A

EC2

Private Subnet 1A

RDS

Availability Zone 1-B

Public Subnet 1B

EC2

Private Subnet 1B

EC2

CLARUSWAY
WAY TO REINVENT YOURSELF

VPC CIDR

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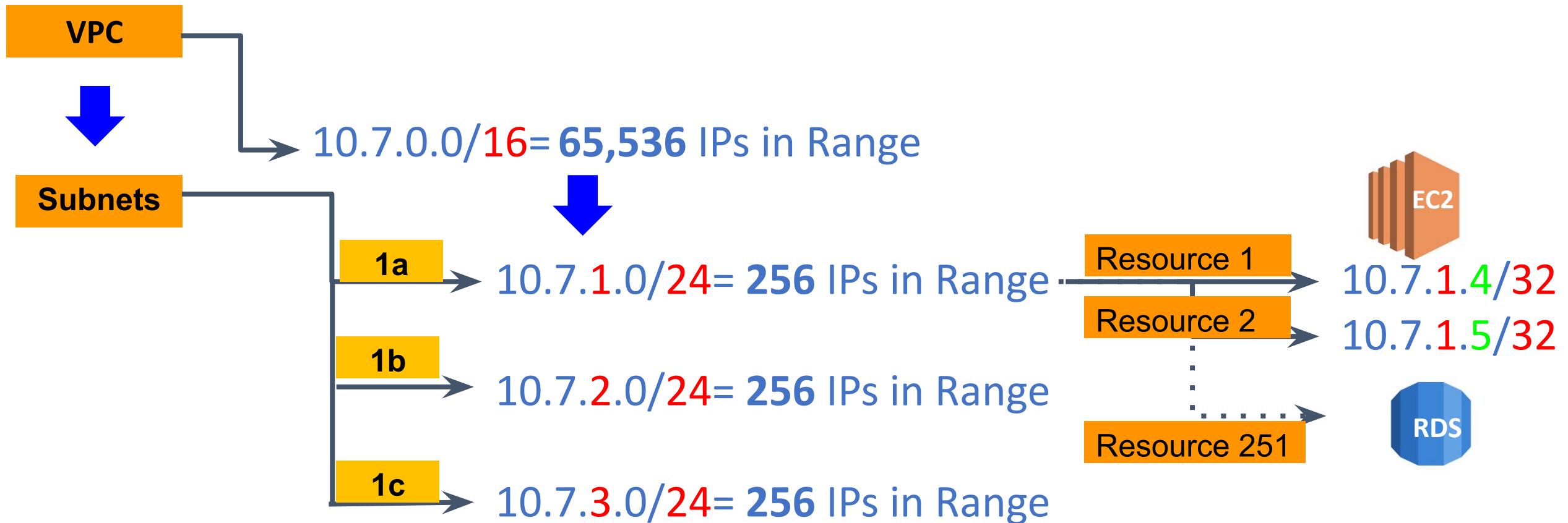10.0.1.0/24 = **256** IPs in Range
10.0.1.0/32 = **1** IP in Range

10.0.0.0/16   Block Size
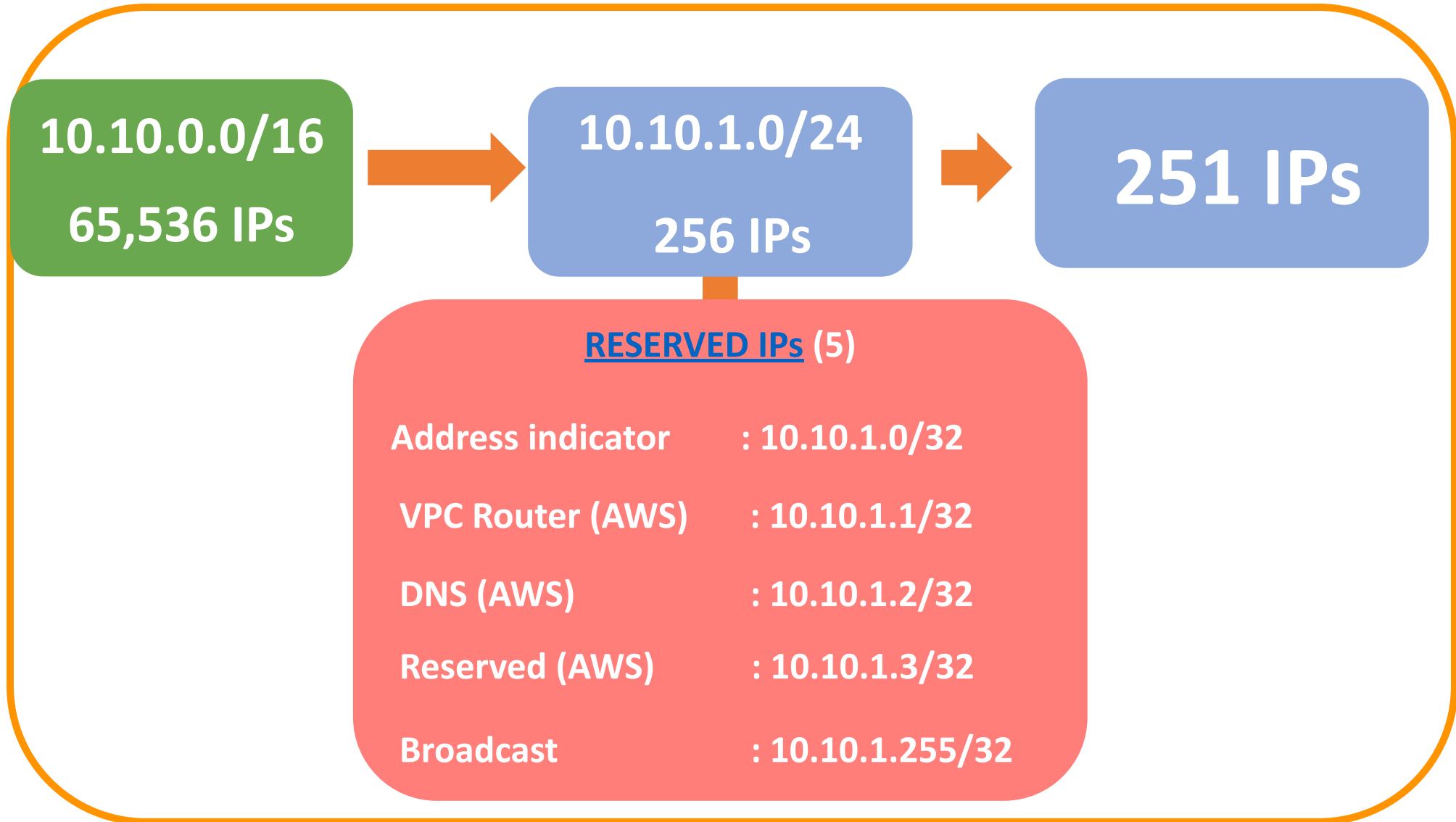
- CIDR refers to Classless Inter-Domain Routing.
- It is a set of Internet protocol (IP) standards that is used to create unique identifiers for networks.

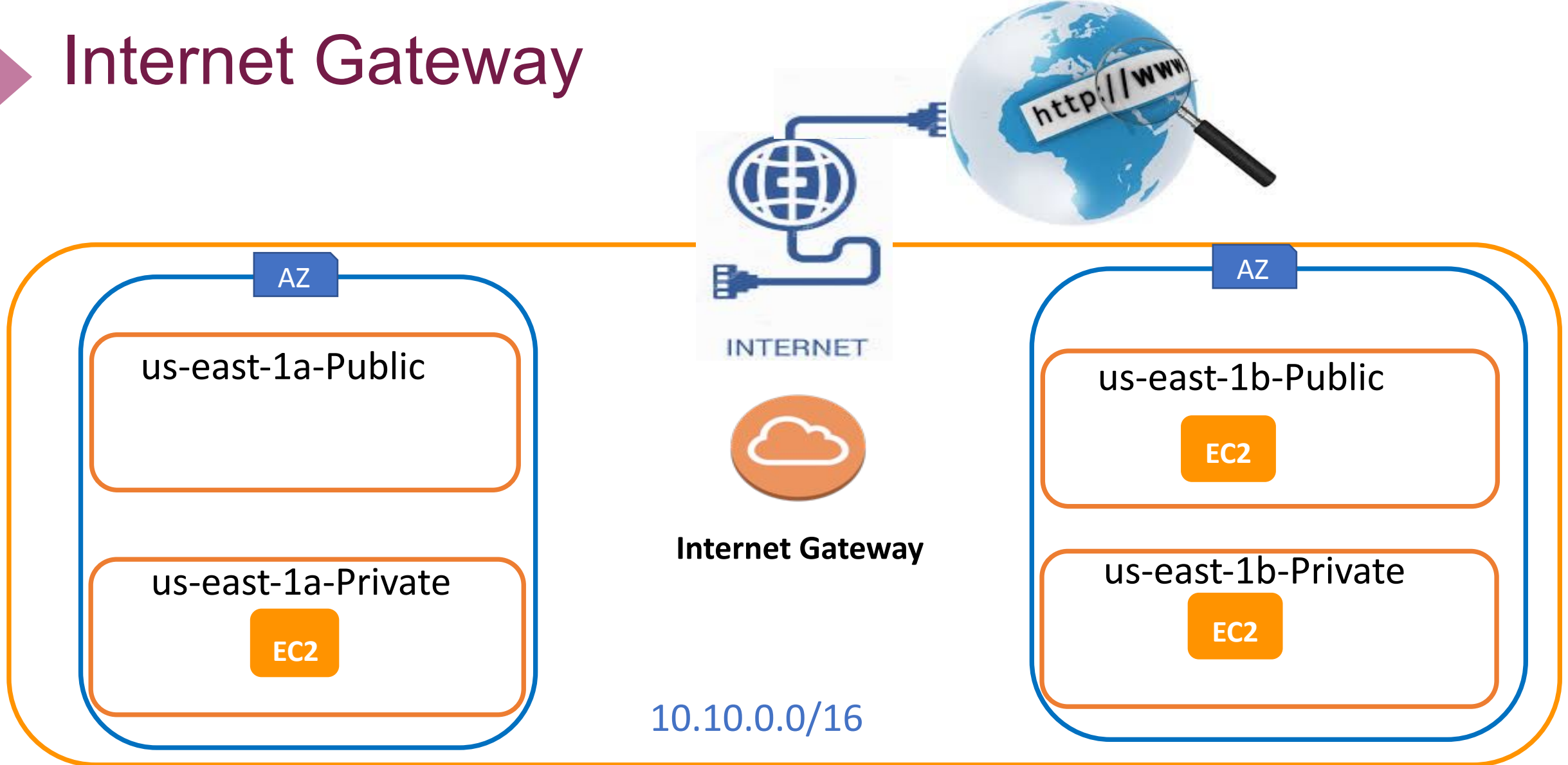- As the Size Block/Netmask (/16,24,32) increases, the number of IP located in CIDR Block decreases.

CLARUSWAY
WAY TO REINVENT YOURSELF

VPC CIDR

VPC

10.7.0.0/16= **65,536** IPs in Range

Subnets

1a

10.7.1.0/24= **256** IPs in Range

EC2

Resource 1

10.7.1.4/32

Resource 2

10.7.1.5/32

1b

10.7.2.0/24= **256** IPs in Range

Resource 251

RDS

1c

10.7.3.0/24= **256** IPs in Range

CLARUSWAY
WAY TO REINVENT YOURSELF

VPC CIDR

10.10.0.0/16

65,536 IPs

→

10.10.1.0/24

256 IPs

→

251 IPs

RESERVED IPs (5)

Address indicator   : 10.10.1.0/32

VPC Router (AWS)   : 10.10.1.1/32

DNS (AWS)   : 10.10.1.2/32

Reserved (AWS)   : 10.10.1.3/32

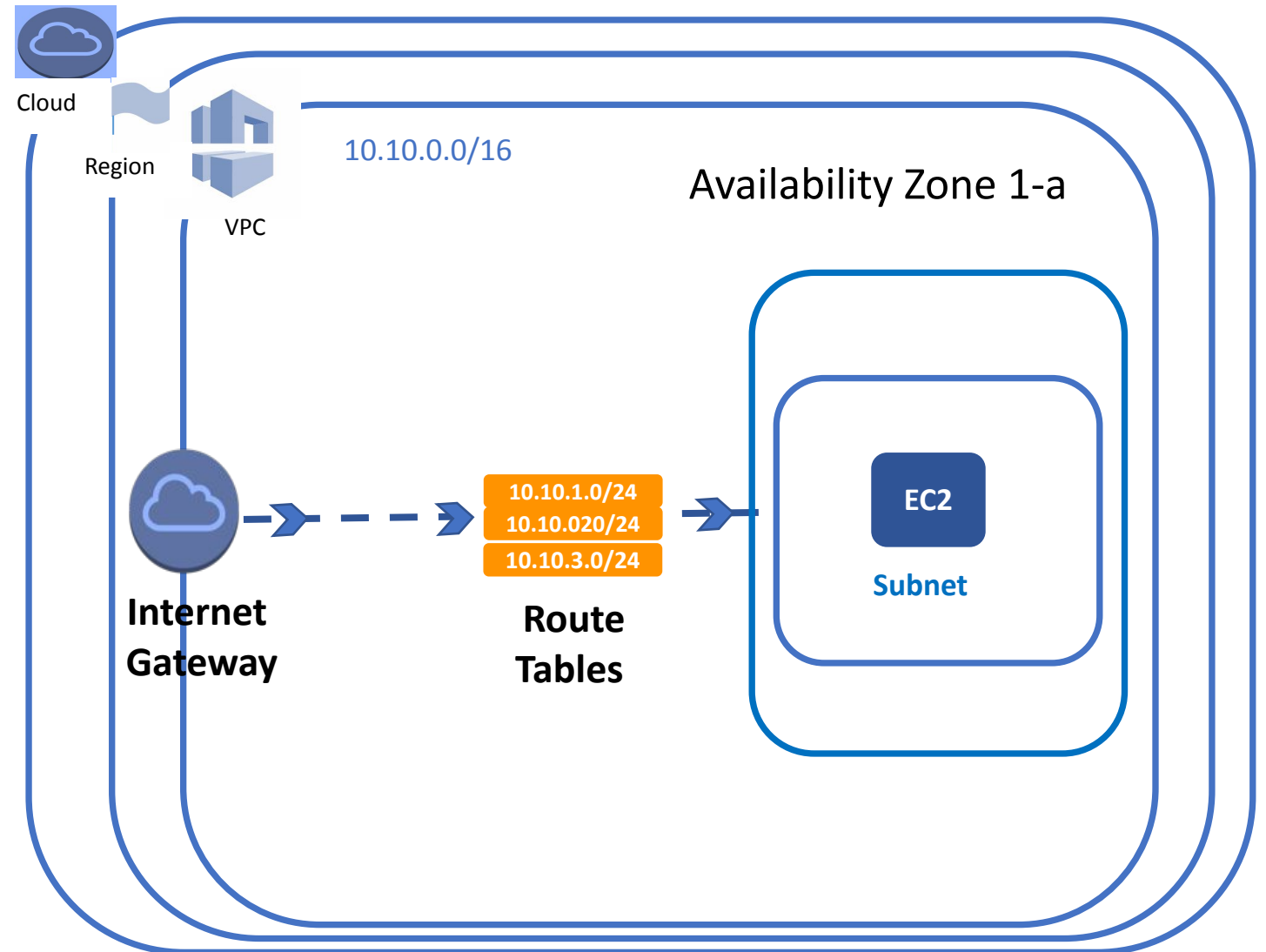Broadcast   : 10.10.1.255/32
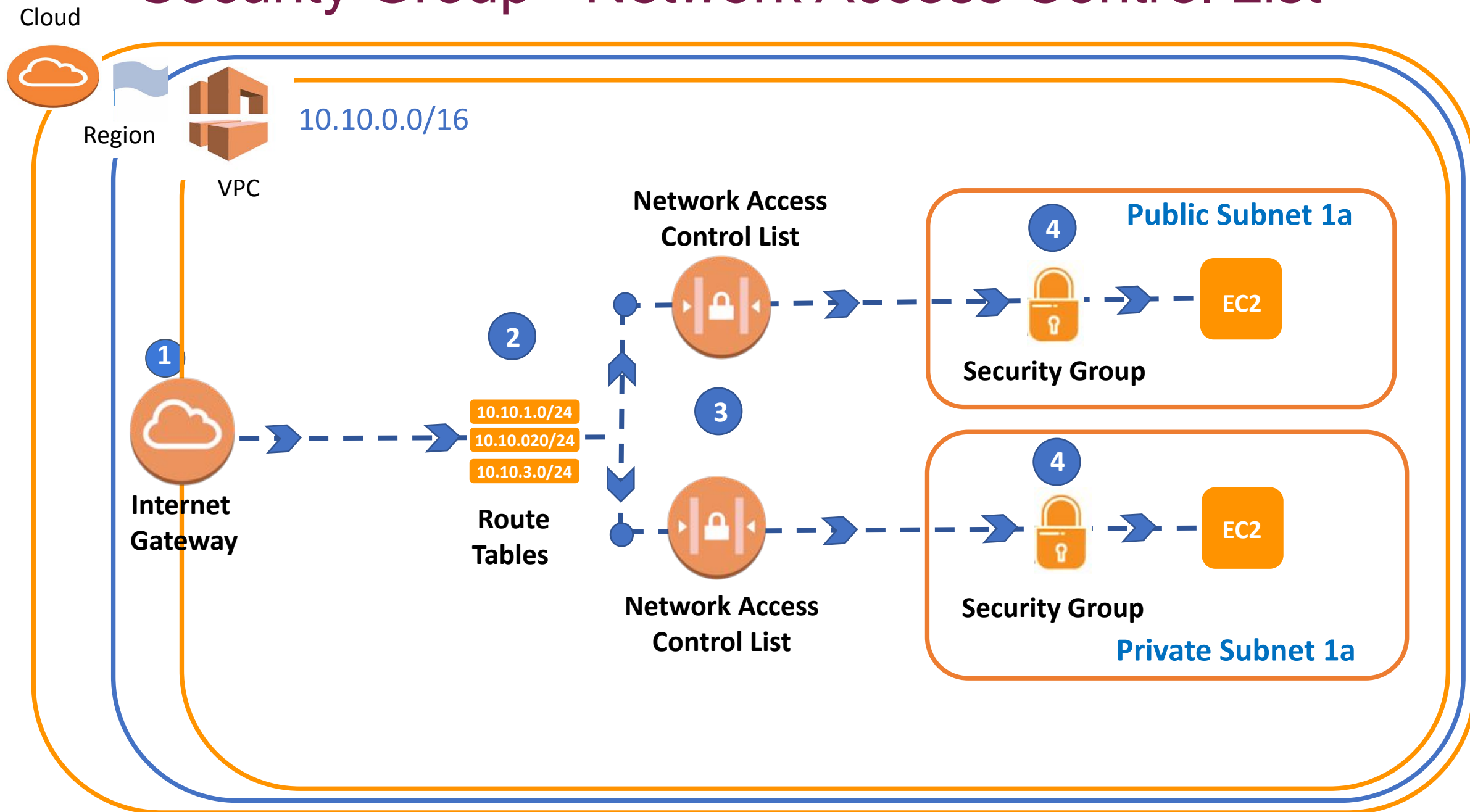
Internet Gateway

Internet Gateway

10.10.0.0/16

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

Route Table

- Route Table is a set of rules, that is used to determine where VPC traffic is directed.

Security Group - Network Access Control List

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**
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

THANKS!

Any questions?