



ondia



Amazon VPC-1

AGENDA



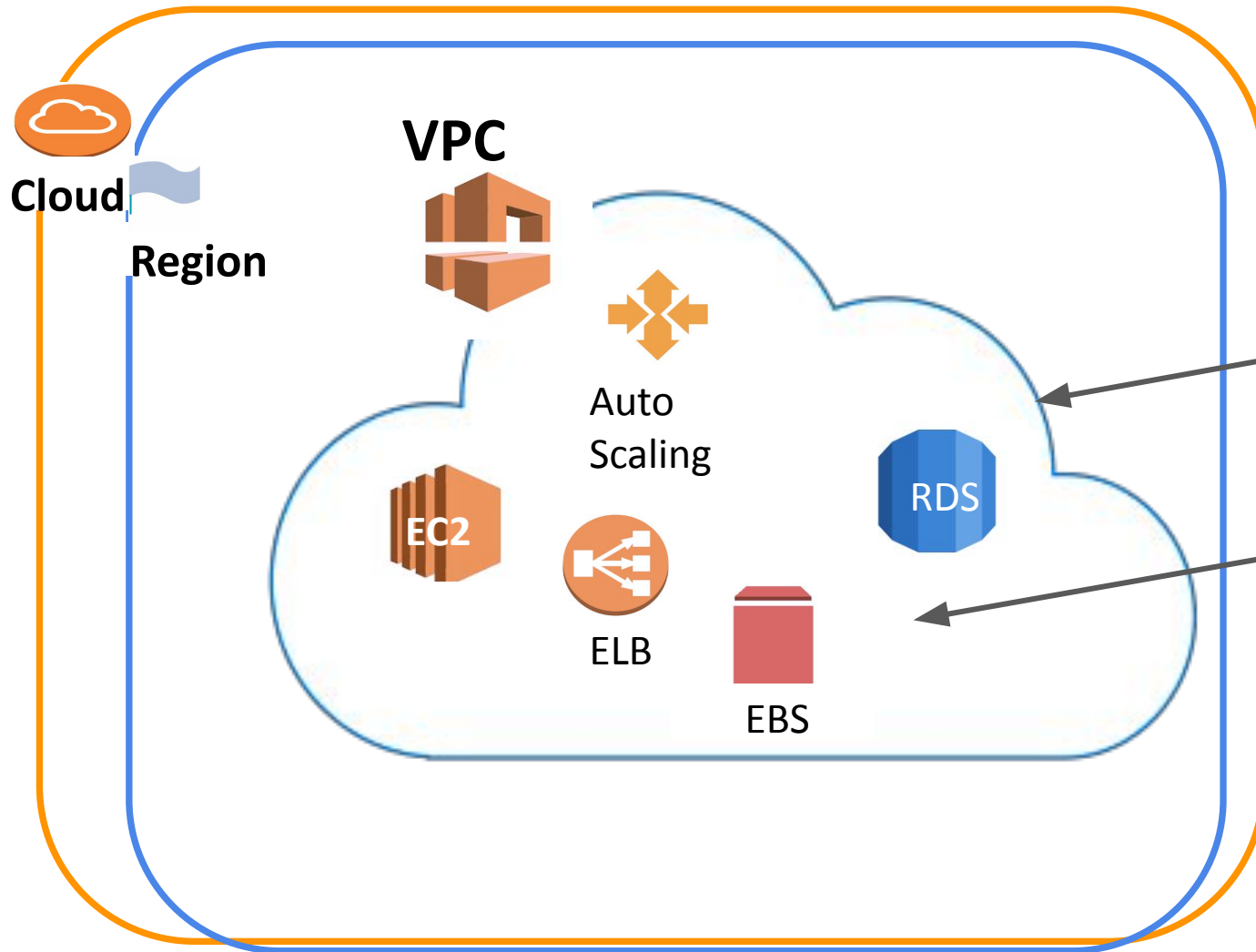
- ▶ **Introduction to VPC**
- ▶ **VPC Basic Components**




Introduction to VPC

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.



VPC Basic Components

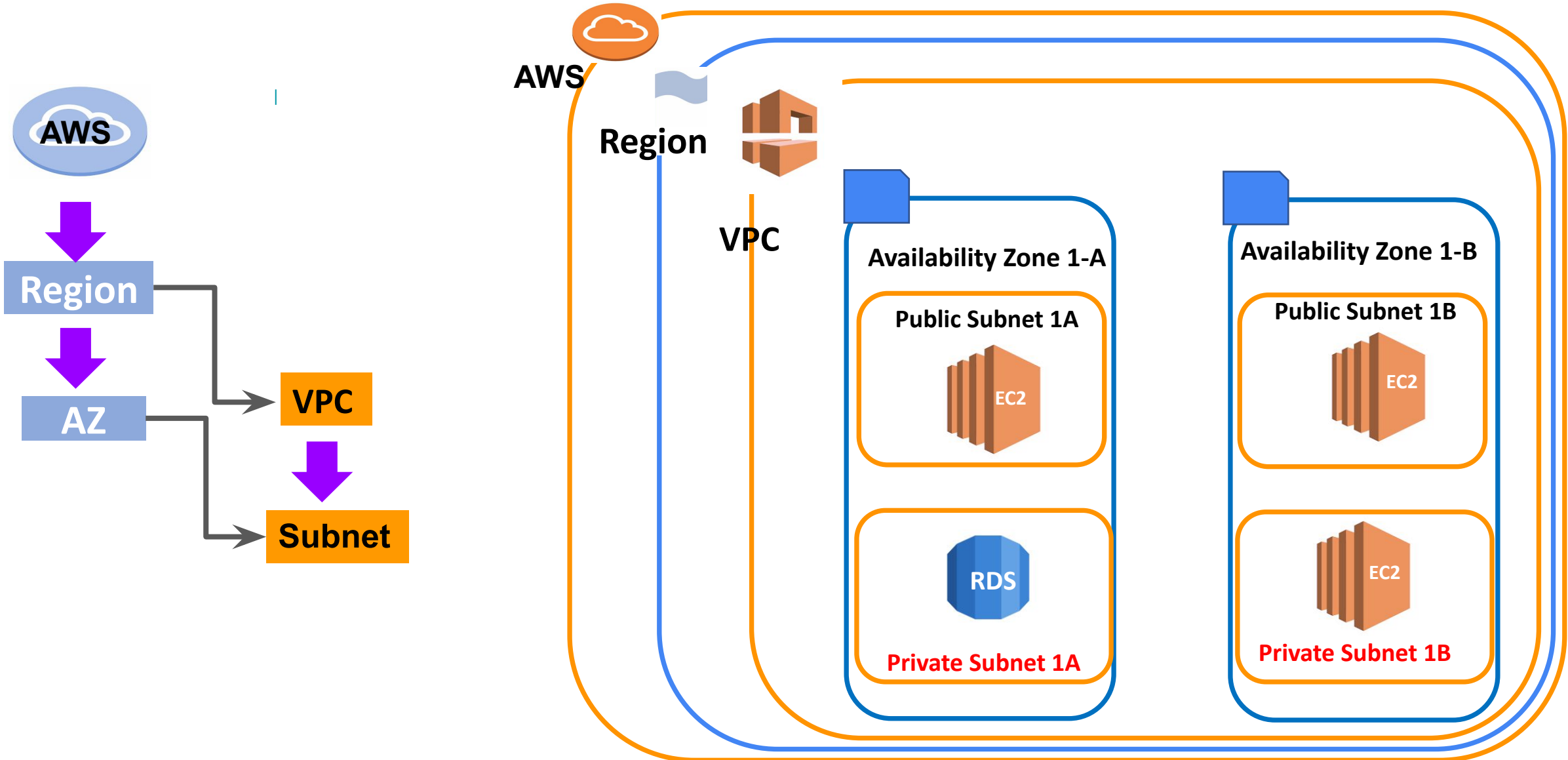
VPC Basic Components



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



Region, VPC, AZ and Subnets



VPC CIDR



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

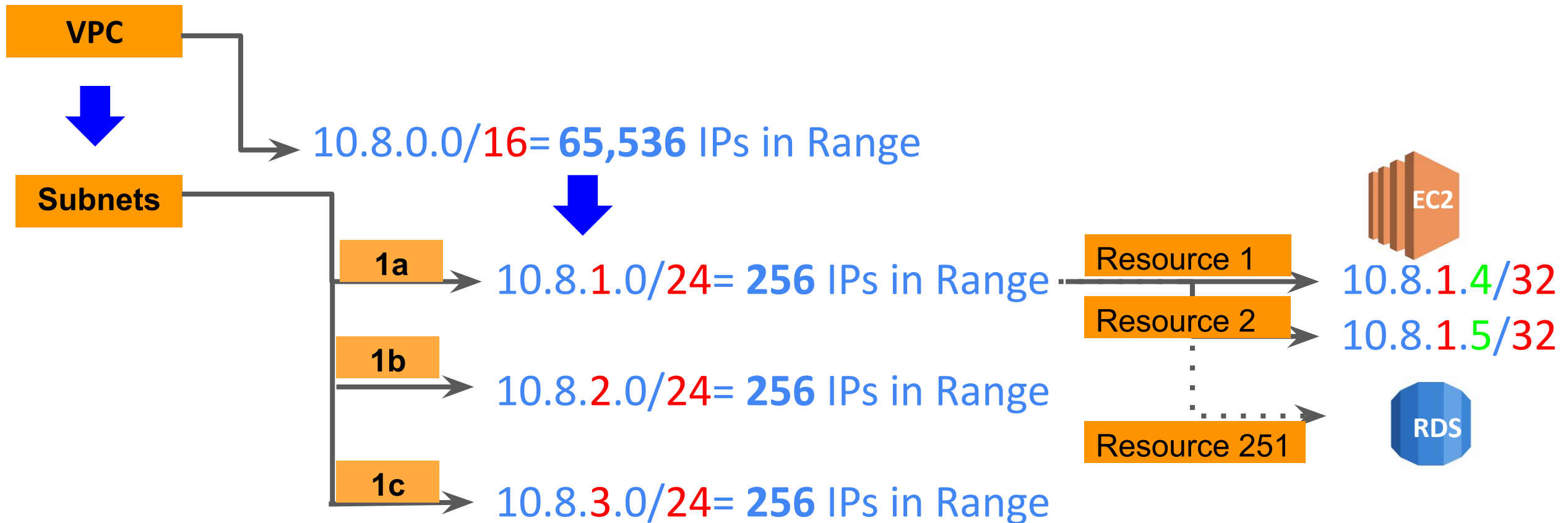
$10.0.1.0/24 = 256$ IPs in Range

$10.0.1.0/32 = 1$ IP in Range

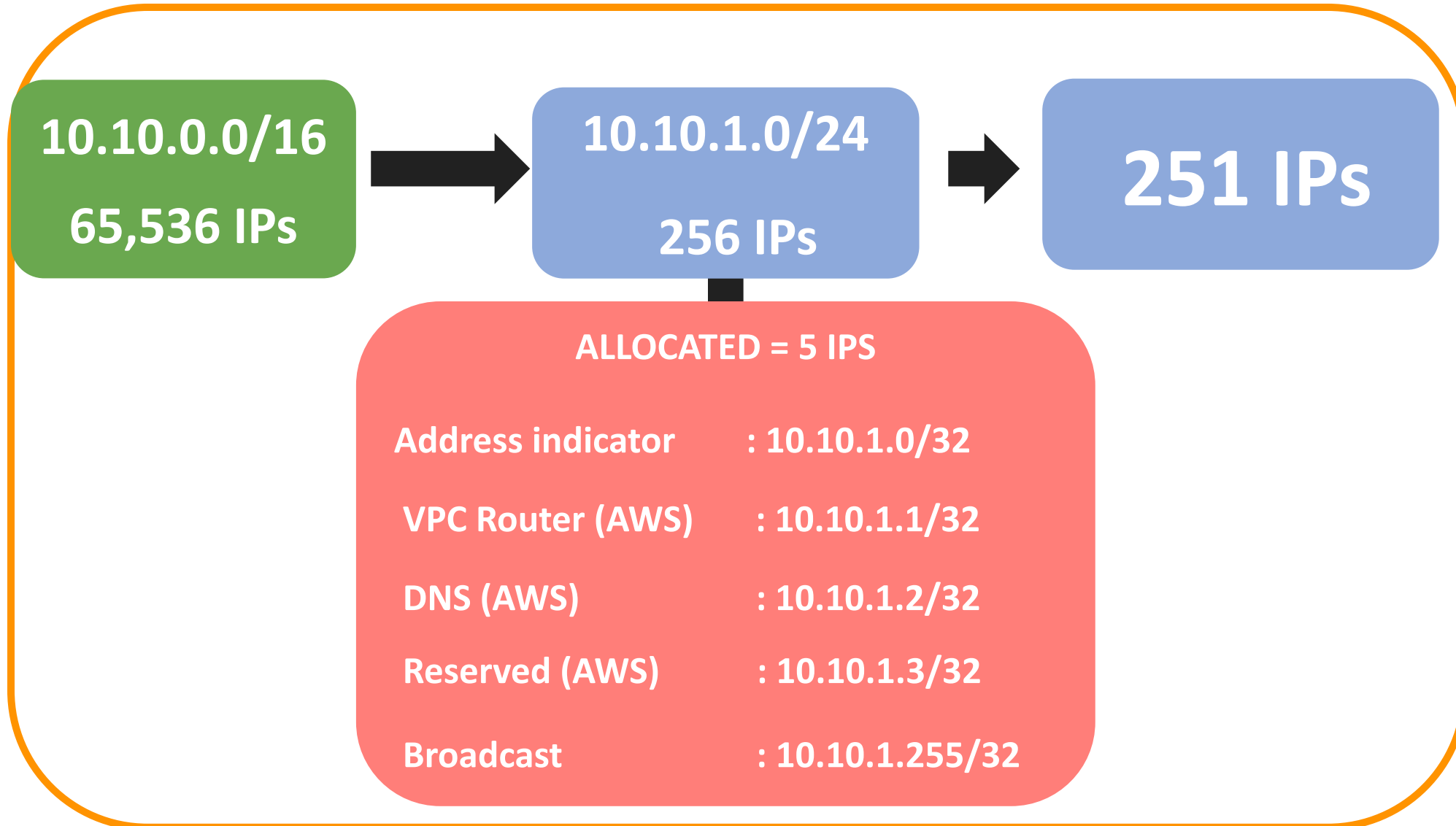
$10.0.0.0/16$ Block Size

- 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.

VPC CIDR



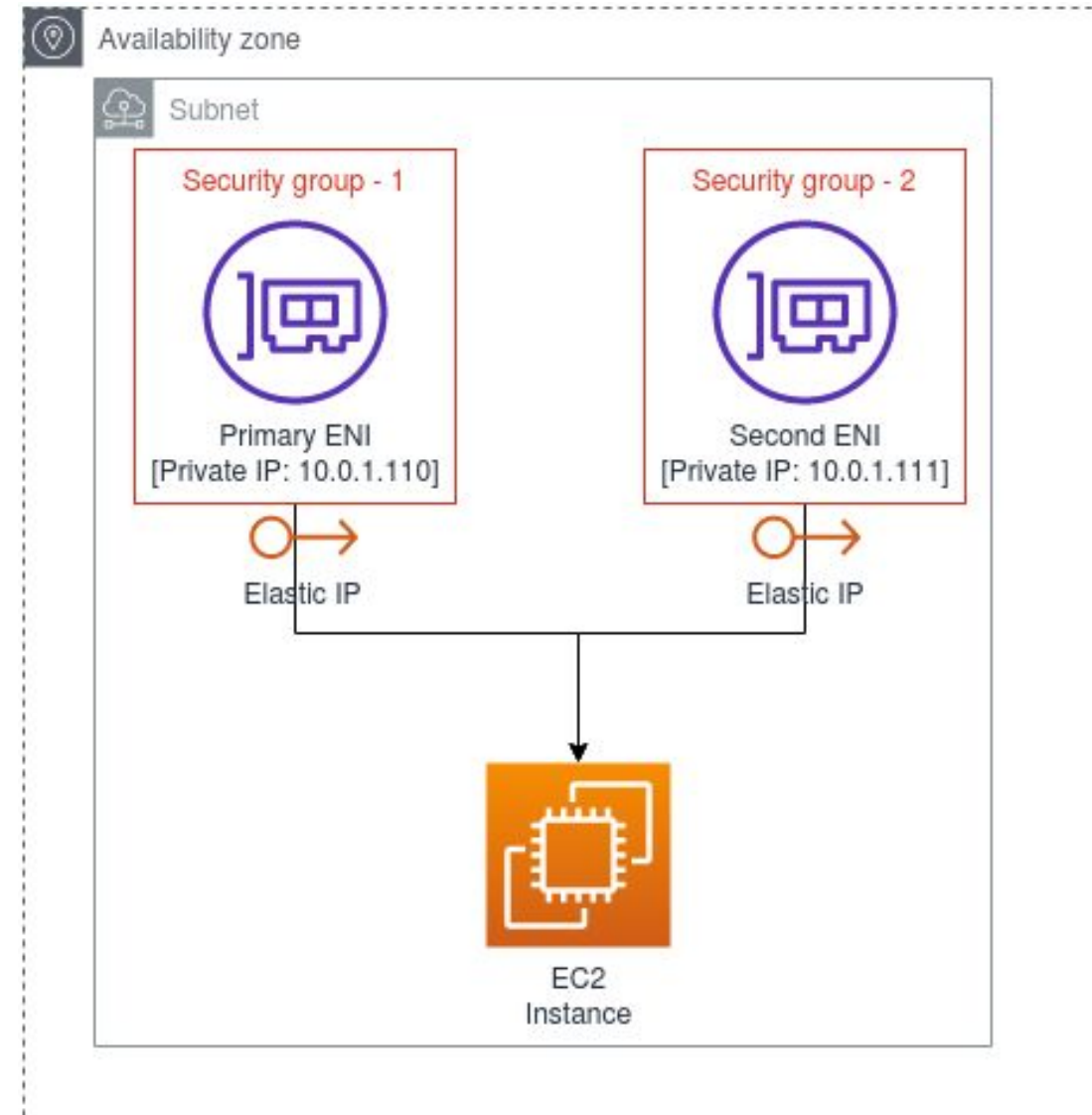
VPC CIDR



Elastic Network Interface



- An elastic network interface is a **logical networking component** in a VPC that represents a **virtual network card**. It corresponds to an **ethernet card** in a conventional computer.
- It provides to direct internet traffic to EC2 instance. Each EC2 instance has a default Elastic Network Interface (ENI). But you can add more ENI's to an instance depending on the instance type.



Elastic Network Interface

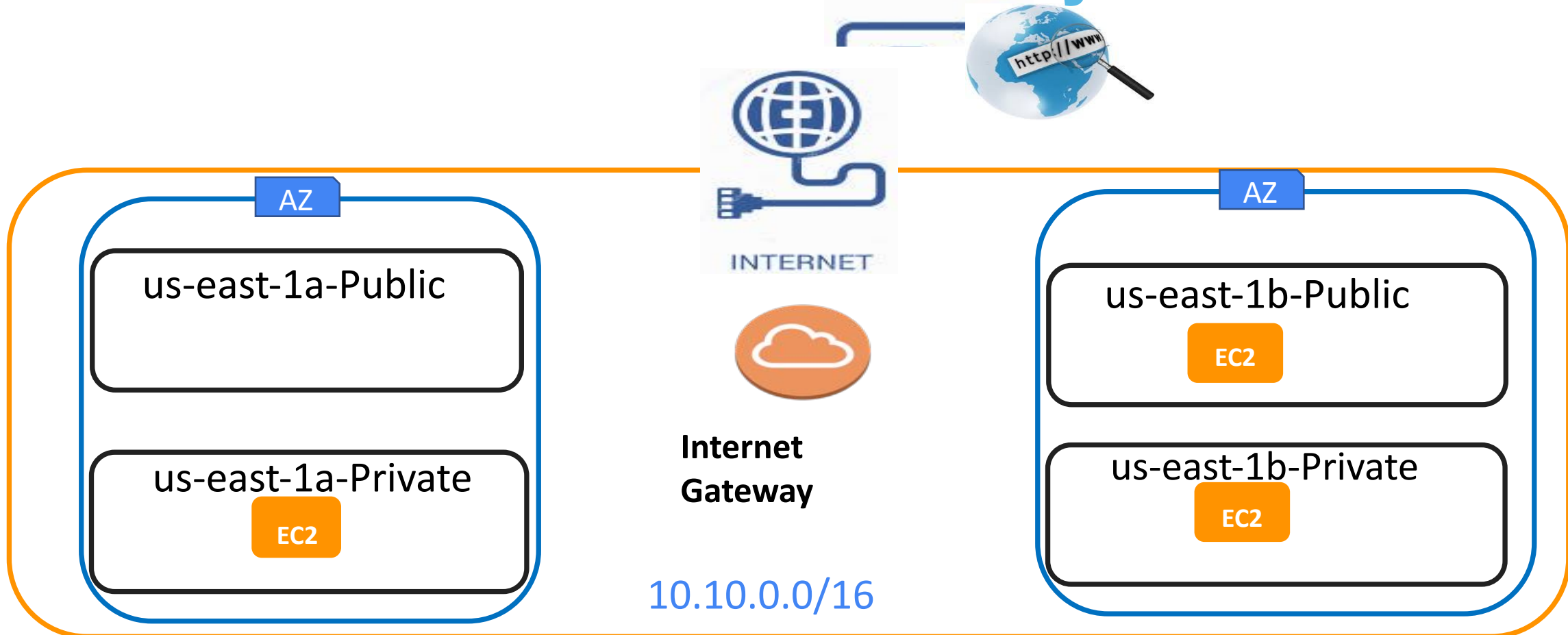


- Upto 10 GBPS
- VMDq
- TCP/IP
- Multiple ENI/instance
- Traffic can traverse across subnets
- VPC Networking, General purpose

- Upto 25 GBPS
- SR-IOV
- TCP/IP
- Single setting/per instance
- Traffic can traverses across subnets
- Low latency apps

- Upto 100 GBPS
- OS-Bypass
- SRD
- One EFA per instance
- OS Bypass traffic is limited to single subnet and is not routable
- HPC and ML Apps

Internet Gateway

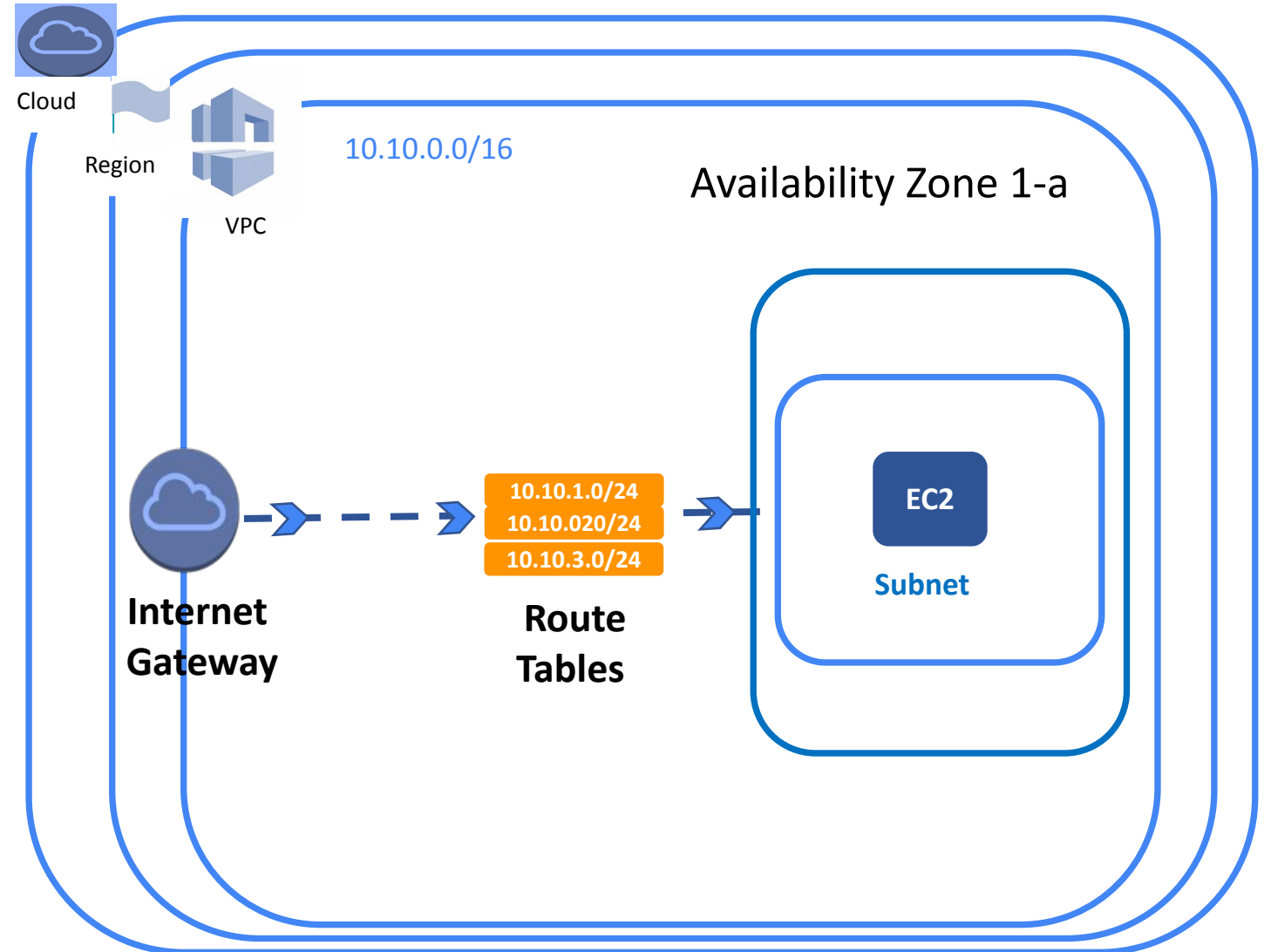


- **Internet Gateway** is a VPC component that provides communication between resources in your VPC and the internet.

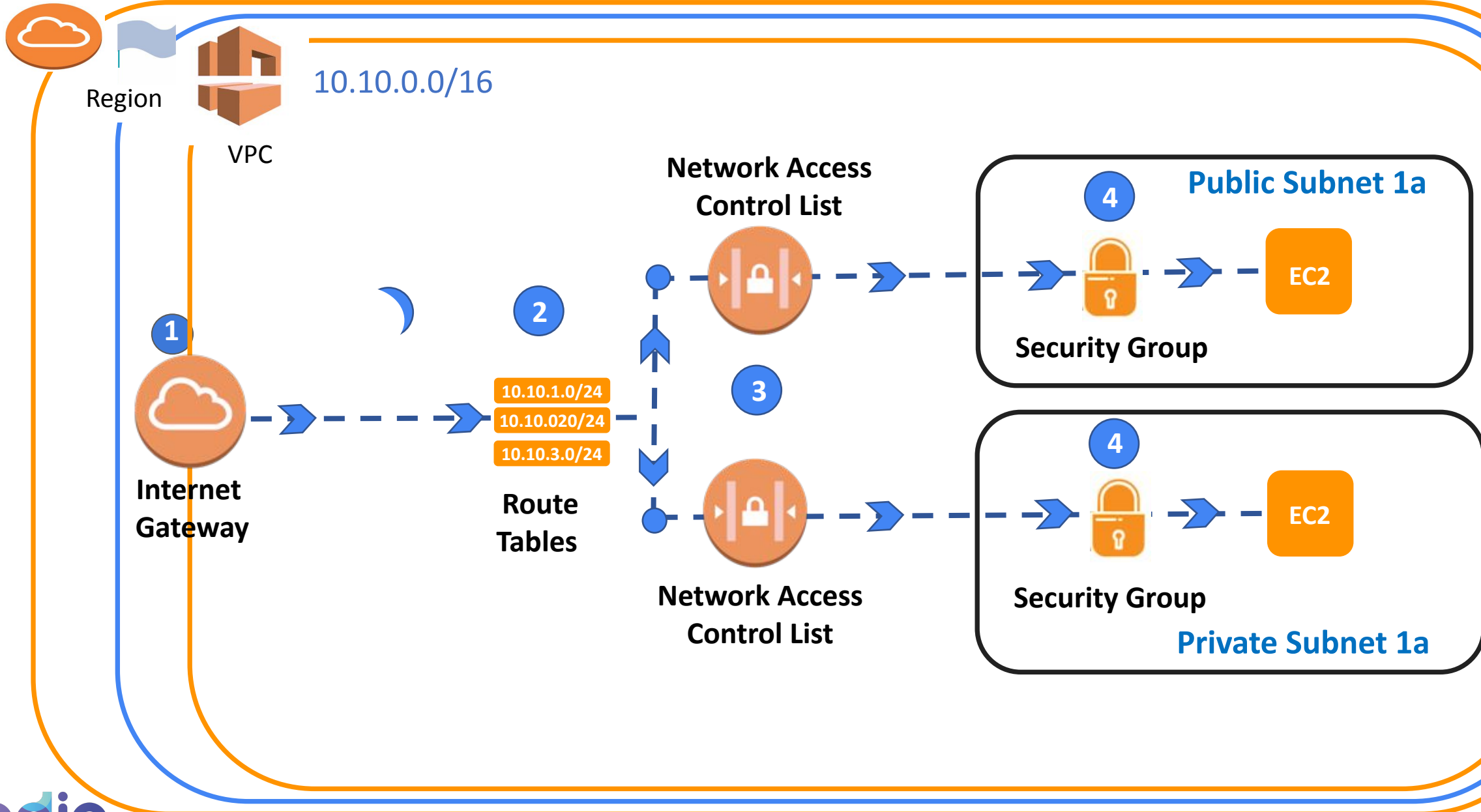
Route Table



- **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	<ol style="list-style-type: none">1. It is instance-based2. Instances can associate with more than one Security Groups	<ol style="list-style-type: none">1. It is subnet-based2. Subnets can associate with only one Network ACL



THANKS!

Any questions?

