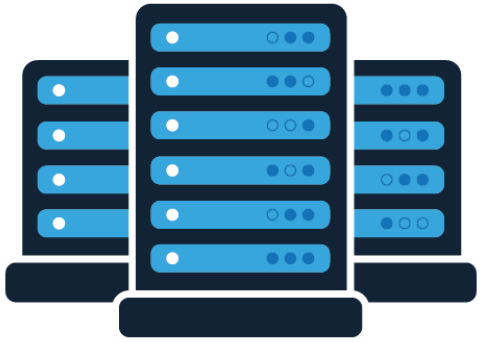
Contents

- VPC Introduction
- Networking CIDR
- Subnet Introduction
- IGW, Route Table
- NACL vs Security Groups
- NAT Introduction

VPC introduction

VPC

- VPC stands for **V**irtual **P**rivate **C**loud.
- Think as Datacenter in the cloud.



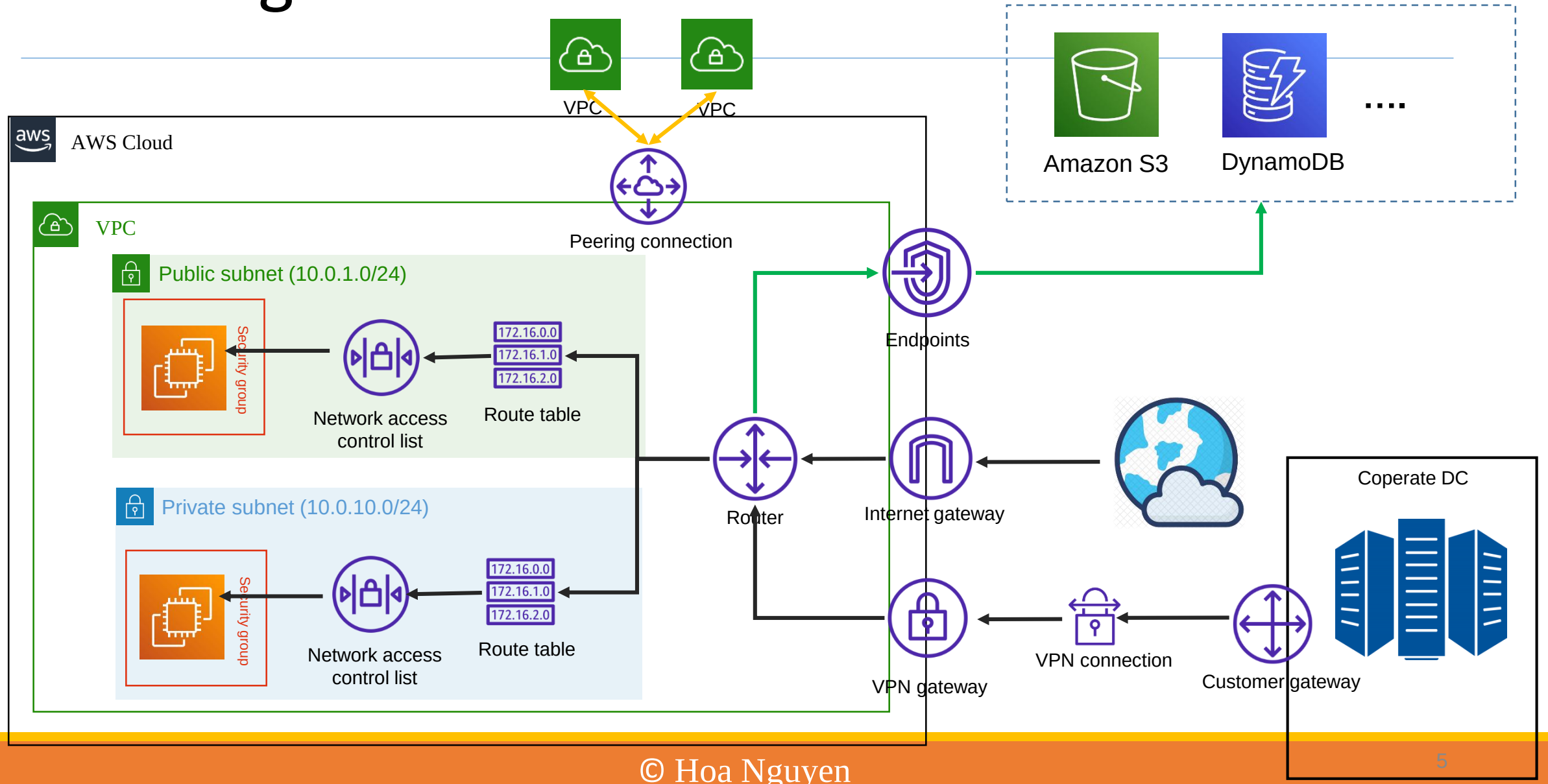
On-premise datacenter

Datacenter in Cloud

VPC features

- IP Addressing, setting up CIDR.
- Create sub networks, routing
- Security
  - Firewall (Security Groups, NACL)
  - Capture traffic routing in/out (VPC flow logs)

VPC diagram

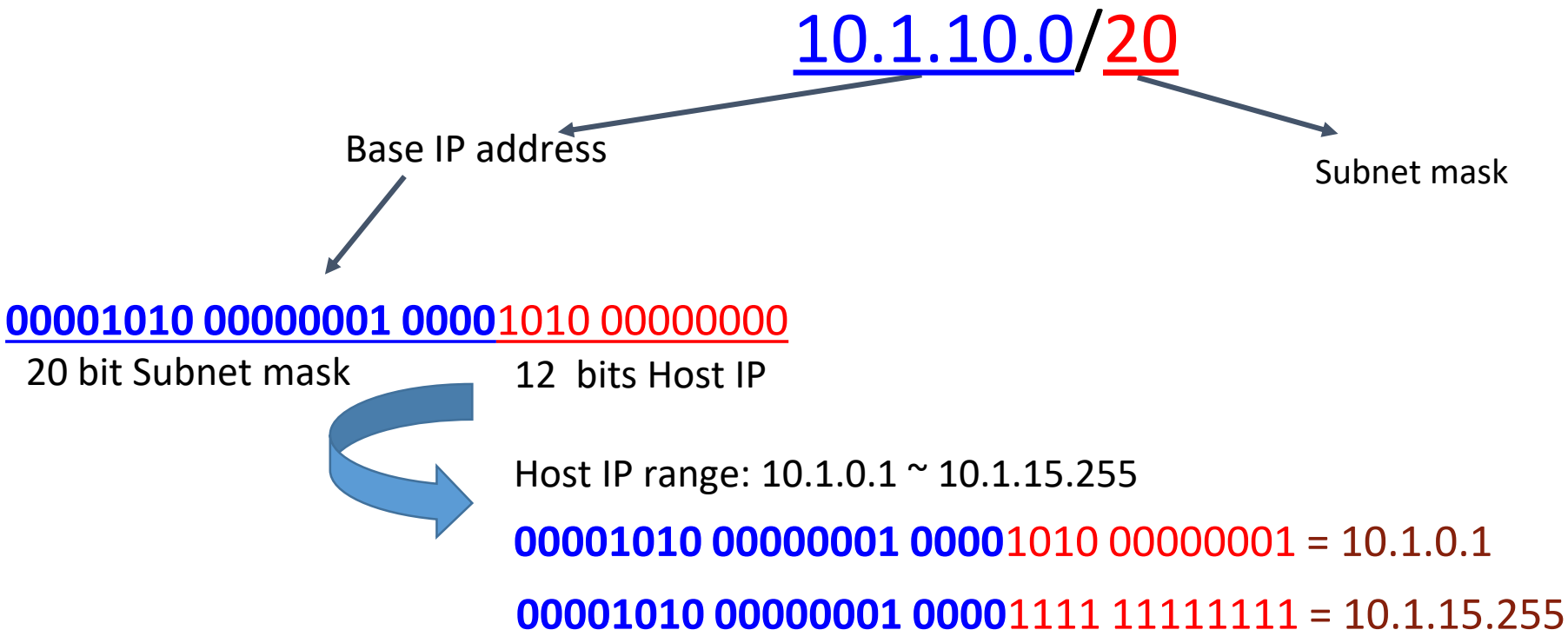

VPC
VPC
Amazon S3
DynamoDB
....
AWS Cloud
Peering connection
VPC
Public subnet (10.0.1.0/24)
Security group
Network access control list
172.16.0.0
172.16.1.0
172.16.2.0
Route table
Endpoints
Router
Internet gateway
Private subnet (10.0.10.0/24)
Security group
Network access control list
172.16.0.0
172.16.1.0
172.16.2.0
Route table
VPN gateway
VPN connection
Customer gateway
Coperate DC

Networking CIDR

CIDR

- CIDR stands for **C**lassless **I**nter-**D**omain **R**outing
- CIDR help to define an IP address range
  - 10.10.0.8/32 => an IP
  - 0.0.0.0/0 => all IPs
  - 10.0.0.0/20 => an IP address range (10.0.0.1 ~ 10.0.15.255) ~ 4096 IPs

CIDR notation



Ref: https://cidr.xyz

Private vs Public IP Allow ranges

- Private IP ranges followed by **RFC1918** standard includes these following CIDRs
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
- The rest of IP are public IPs

Private, Public, Elastic IP

	Private IP	Public IP	Elastic IP
Reachable from internet	Not. For communication between instances in same VPC	Reachable from the internet. For communication between instances and internet	Reachable from the internet. For communication between instances and internet
Change when instances stop/start	No	Yes	No After EIP is allocated, it is yours until you release it

Exercise

1. Find IP range of CIDR (10.1.10.0/24)

2. Find CIDR that contains 2 IP addresses 10.0.0.10 and 10.0.127.250

Subnet Introduction

Subnet

- A subnet tight with an Availability Zone
- 2 type of subnets
  - **Public subnet:**
    - Allow entities in the internet can be able to connect to
    - There is a route to Internet Gateway in attached route table
  - **Private subnet:**
    - For private resources, not expose to the internet
    - There is no route to Internet Gateway in attached route table

Subnet sizing for IPv4

- AWS reserved 5 IP addresses (first 4 and last 1 IP address) in each Subnet
- Those 5 IP addresses cannot be assigned to an instance
- Ex: subnet with CIDR block: 10.10.0.0/24
  - 10.10.0.0: Network address
  - 10.10.0.1: Reserved by AWS for VPC router
  - 10.10.0.2: Reserved by AWS for mapping to Amazon-provided DNS
  - 10.10.0.3: For future use
  - 10.10.0.255: Network broadcast address

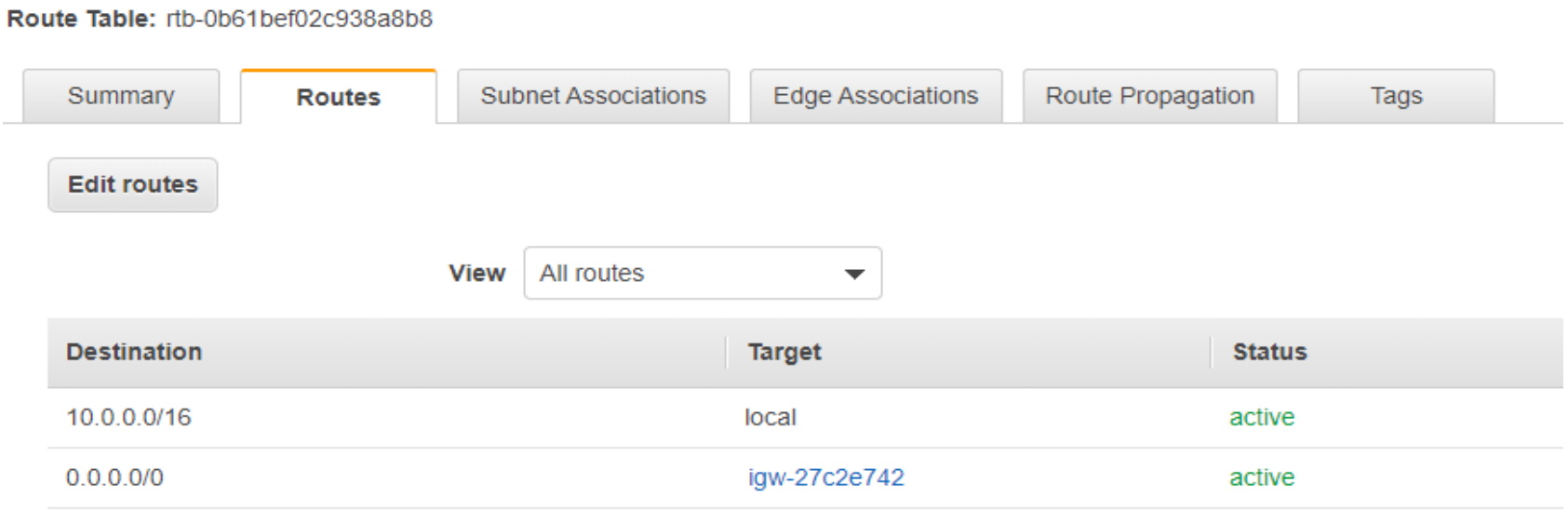
IGW, Route Table

Internet Gateway (IGW)

- IGW helps instances in VPC connect to the internet
- Providing one-to-one NAT for instances in VPC
- It horizontally scaled, redundant, and highly available
- Only one IGW can attach to a VPC and vice versa

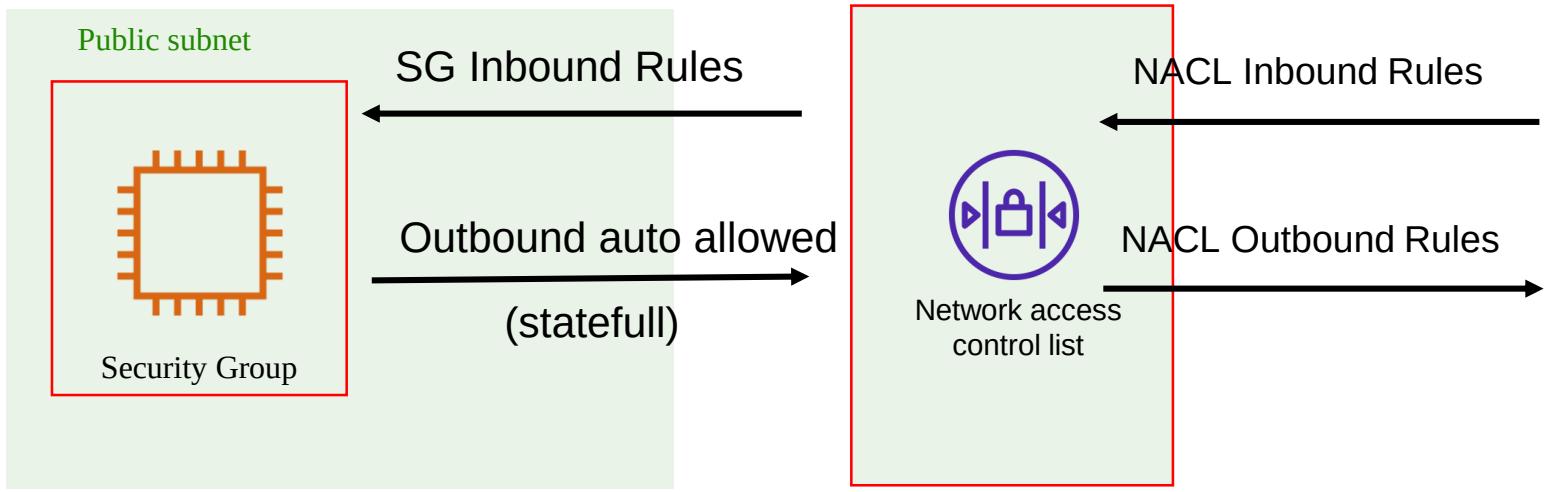
Route Table

- Use to control where network traffic is directed in subnet or gateway
- Each subnet can only attach one Route Table
- Each Route Table can attach to as many as subnets



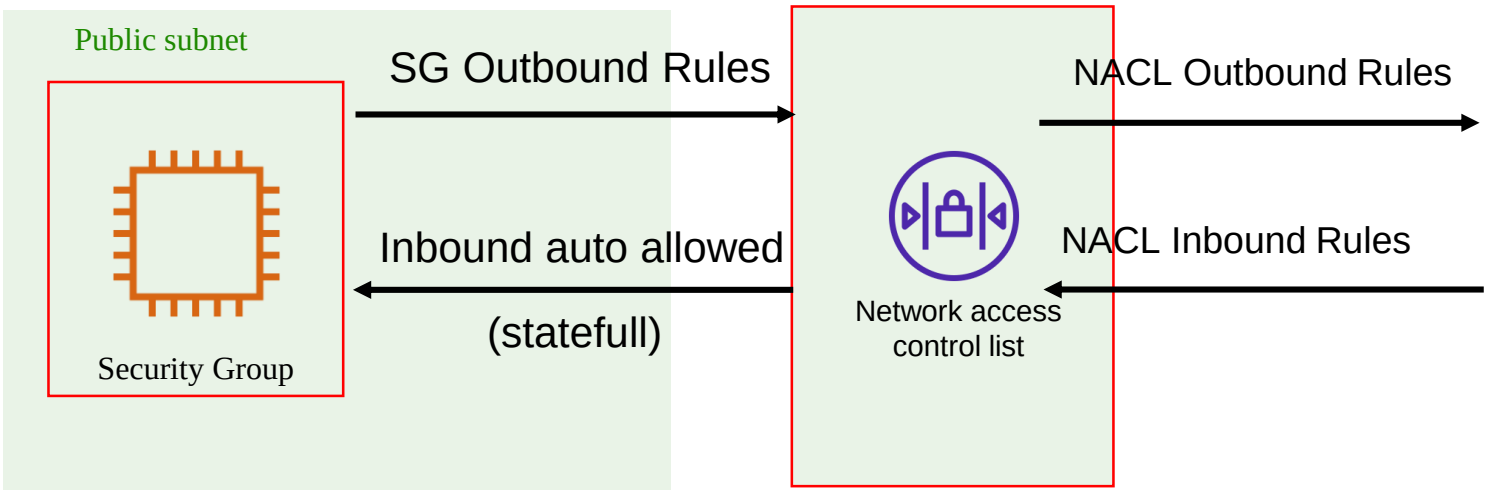
NACL and SG

How incoming requests get into EC2?



NACL = Network Access Control List

How outgoing requests get out from EC2?



NACL = Network Access Control List

Network ACL (NACL)

- Work as firewall at Subnet level
- One subnet can attach only one NACL and one NACL can attach multiple subnets
- Default NACL is anyopen traffic (Allow all In/Outbound)
- Rules are set with number. Smaller number, Higher precedence
- Newly NACL will deny everything

Network ACL and Security Groups

Security Groups	Network ACL
Operates at the instance level	Operates at the subnet level
Support only Allow rules	Support Allow vs Deny rules
Stateful: Return traffic is automatically allowed regardless on any rules	Stateless: Return traffic must be explicitly allowed by rules
Evaluate all rules before making decission	Process in number order to make decision
Applies to the instances that are explicitly attached with Security Group	Applies to all instances inside of Subnet that attached NACL

NAT Introduction

What is NAT

- NAT stands for **N**etwork **A**ddress **T**ranslation
- Allow instances in Private Subnet connect to the internet
- There are 2 types of NAT
  - NAT instance
  - NAT Gateway

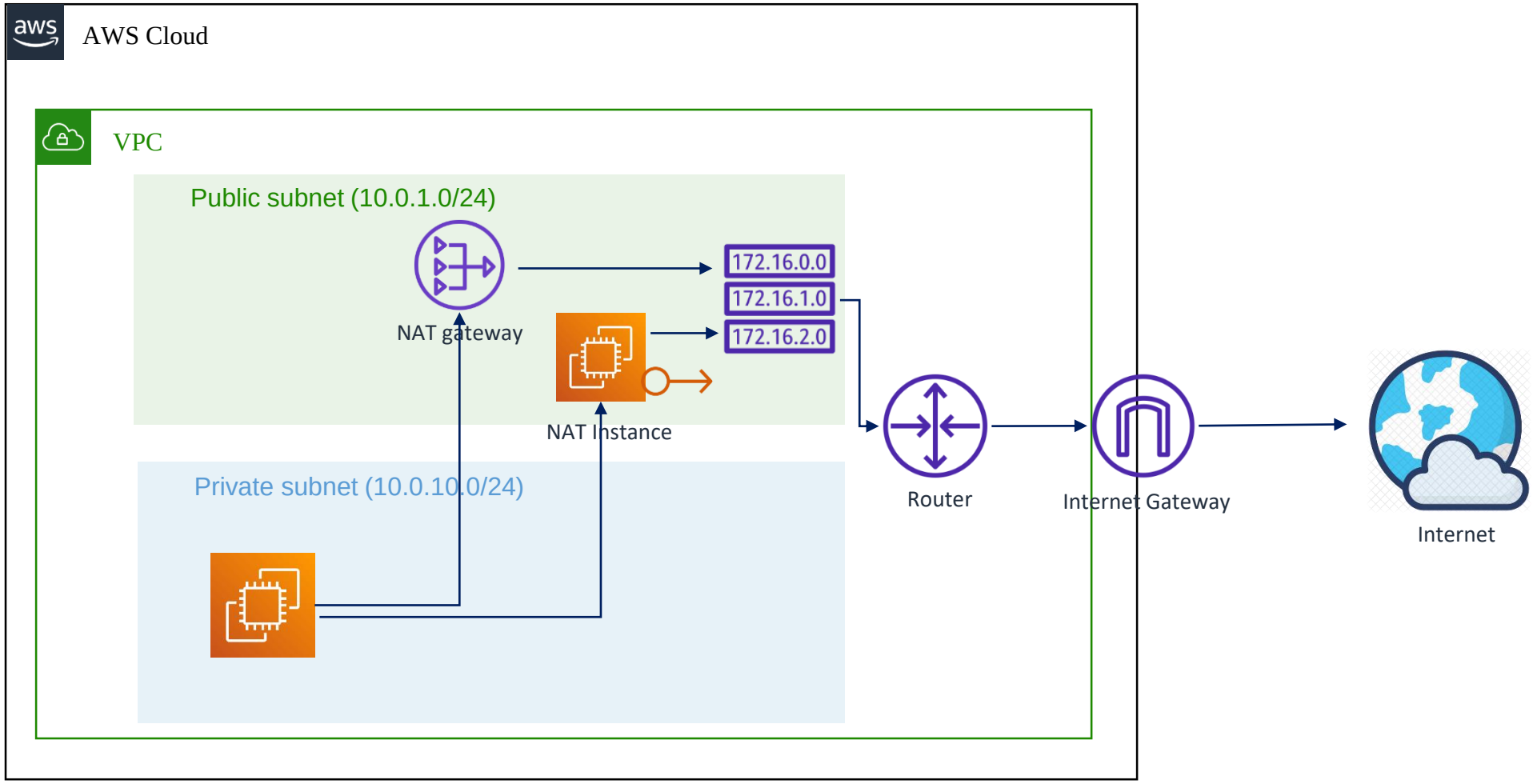
NAT instances

- A single EC2 instance that is setup, config as NAT function
- Placed in Public Subnet
- Need to have Elastic IP
- Must be disable **Source/Destination** check
- Route Table of Private Subnet must be configure to target to NAT instance

NAT Gateway

- AWS managed NAT service
- High Availability, Scalability

How NAT work?


AWS Cloud
VPC
Public subnet (10.0.1.0/24)
NAT gateway
172.16.0.0
172.16.1.0
172.16.2.0
NAT Instance
Private subnet (10.0.10.0/24)
Router
Internet Gateway
Internet

Exam Tips

- NAT instance
  - Must be in public subnet, must have ElasticIP
  - Must disable Source/Destination check
  - Traffic bandwith depends on instance type
  - Must manage SGs and rule
  - Using ASG to deploy NAT instances in multiple Azs and using script to failover

Labs

1. VPC Lab