Nội dung

CloudNut
Learn Clouds in a Nutshell

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

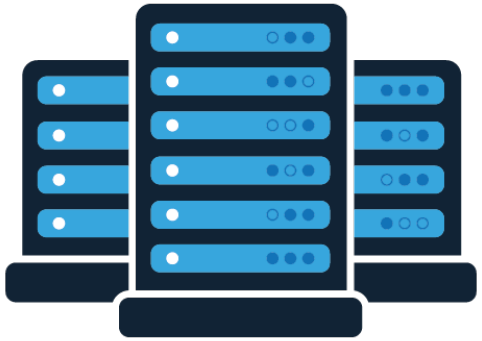
CloudNut
Learn Clouds in a Nutshell

VPC introduction

VPC

CloudNut
Learn Clouds in a Nutshell

- VPC viết tắt của **V**irtual **P**rivate **C**loud.
- VPC giống như một Data Center trên Cloud



On-premise datacenter

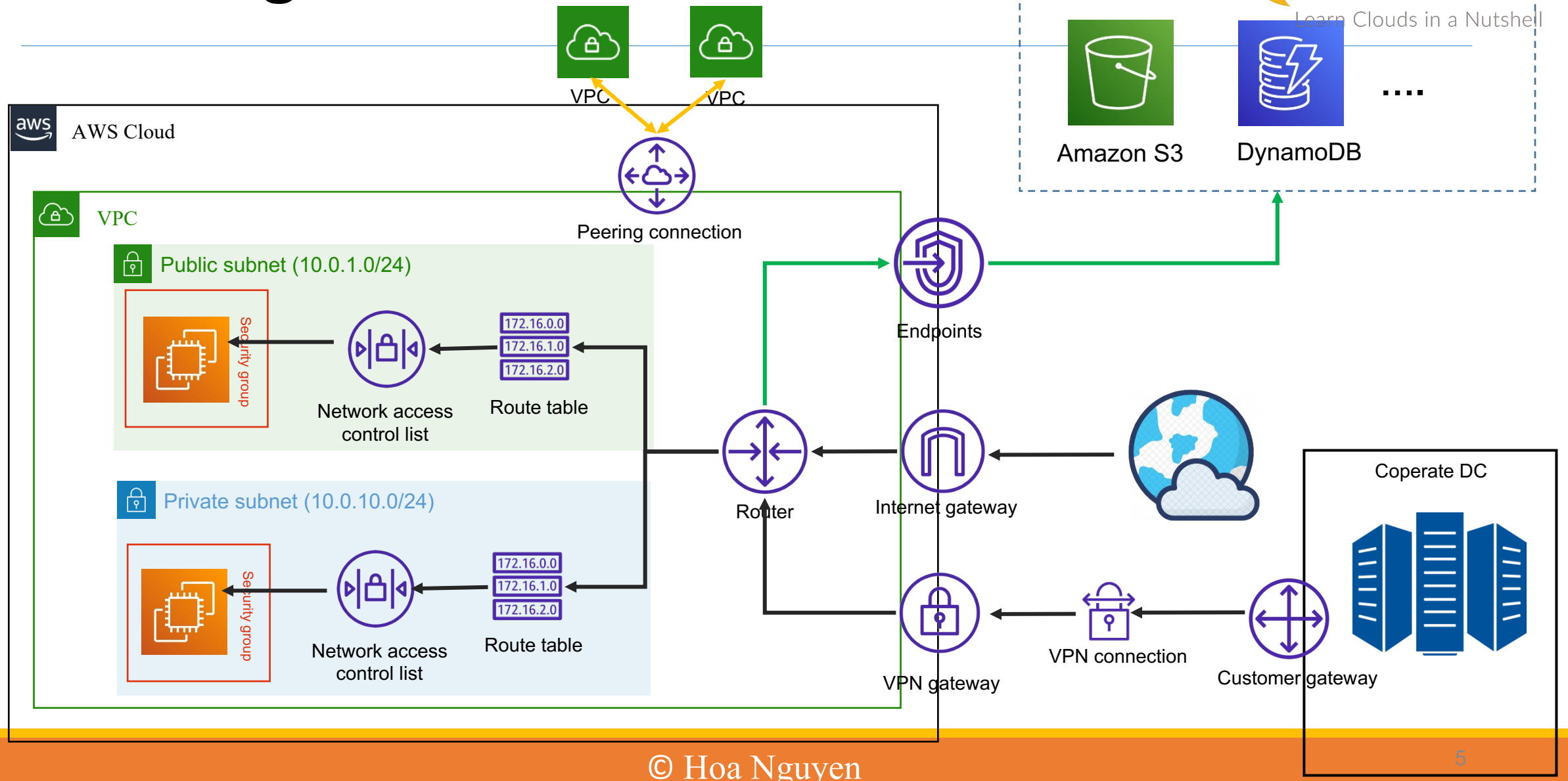
Datacenter in Cloud

Các tính năng của VPC

CloudNut
Learn Clouds in a Nutshell

- Quản lý, cấp phát dải địa chỉ IP. Cấu hình CIDR (Classless Inter-Domain Routing)
- Tạo mạng con (Subnets), định tuyến (Routing)
- Security
  - Firewall (Security Groups, NACL)
  - Lưu lại thông tin các traffic in/out (VPC Flow logs)

VPC diagram


CloudNut
Learn Clouds in a Nutshell
VPC
VPC
AWS Cloud
Amazon S3
DynamoDB
....
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

CloudNut
Learn Clouds in a Nutshell

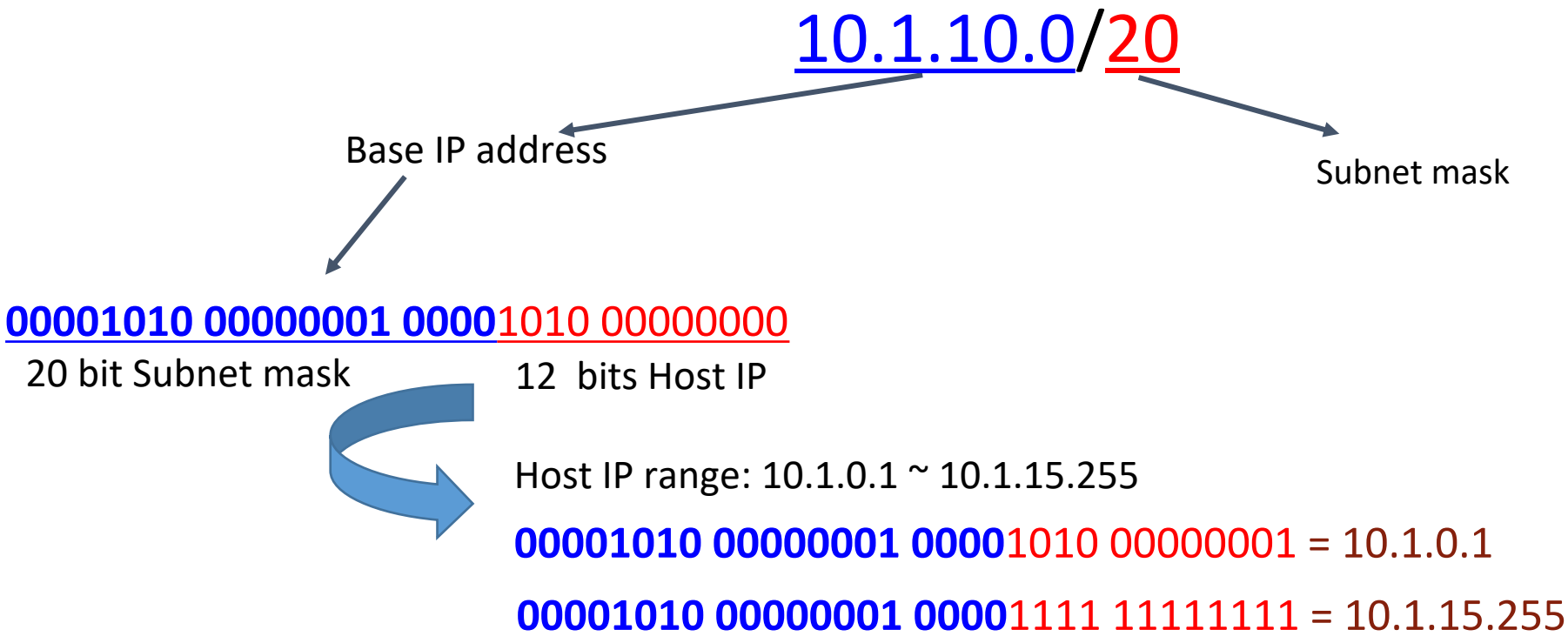
Networking CIDR

Giới thiệu CIDR

CloudNut
Learn Clouds in a Nutshell

- CIDR viết tắt của **C**lassless **I**nter-**D**omain **R**outing
- CIDR giúp định nghĩa một dải địa chỉ IP (IP Address Range)
  - 10.10.0.8/32 => Một địa chỉ IP
  - 0.0.0.0/0 => Tất cả địa chỉ IP
  - 10.0.0.0/20 => Một dải IP (IP Address Range) 10.0.0.1 ~ 10.0.15.255 ~ 4096 IPs

Ký hiệu CIDR (CIDR notation)



Ref: https://cidr.xyz

Dải địa chỉ Private vs Public IP

CloudNut
Learn Clouds in a Nutshell

- Dải địa chỉ Private IP tuân theo chuẩn **RFC1918** bao gồm những dải sau
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
- Những dải IP khác những dải trên thì sẽ là dải Public IP

Private, Public, Elastic IP

CloudNut
Learn Clouds in a Nutshell

	Private IP	Public IP	Elastic IP
Truy cập được từ Internet	Không Dành cho giao tiếp trong nội bộ VPC	Có Dành cho giao tiếp với Internet	Có Dành cho giao tiếp với Internet
Bị thay đổi khi Stop/Start Instance	Không	Có	Không

Exercise

CloudNut
Learn Clouds in a Nutshell

1. Tìm dải địa chỉ IP của CIDR sau: 10.1.10.0/24

2. Tìm CIDR chứa 2 địa chỉ IP sau: 10.0.0.10 và 10.0.127.250

CloudNut
Learn Clouds in a Nutshell

Subnet Introduction

Subnet

CloudNut
Learn Clouds in a Nutshell

- Mỗi Subnet sẽ gắn với một Avalibility Zone (Mapping 1-1)
- Có 2 loại Subnet
  - **Public subnet:**
    - Cho phép các thực thể bên ngoài Internet có thể tiếp cận
    - Có một luật trong **Route Table** được định tuyến tới **Internet Gateway**
  - **Private subnet:**
    - Dành cho giao tiếp nội bộ VPC. Các thực thể bên ngoài Internet không thể truy cập được
    - Không có luật trong **Route Table** được định tuyến tới **Internet Gateway**

Dải địa chỉ IPv4 của Subnet

CloudNut
Learn Clouds in a Nutshell

- AWS bảo lưu (Reserved) 5 IP Address (4 IP đầu tiên và 1 IP cuối cùng) trong mỗi Subnet cho mục đích riêng của AWS
- 5 IP này sẽ không được cấp phát cho EC2 Instances
- Ví dụ: Subnet với CIDR block: 10.10.0.0/24
  - 10.10.0.0: Network address
  - 10.10.0.1: Dành VPC router
  - 10.10.0.2: Dành cho Amazon-provided DNS
  - 10.10.0.3: Dành cho mục đích trong tương lai
  - 10.10.0.255: Địa chỉ Network broadcast

CloudNut
Learn Clouds in a Nutshell

IGW, Route Table

Internet Gateway (IGW)

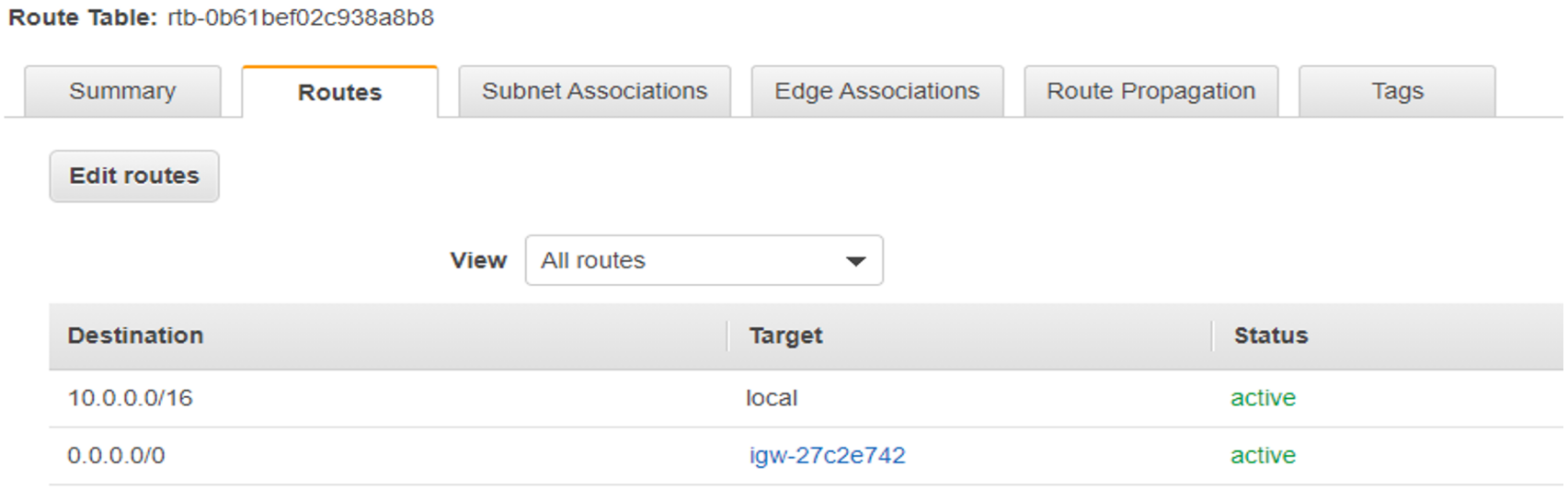
CloudNut
Learn Clouds in a Nutshell

- IGW cho phép các Instances trong VPC nói chuyện với Internet và ngược lại
- IGW có khả năng mở rộng tốt (Scalability), High Availibility
- Mỗi VPC có thể gắn duy nhất 1 IGW và ngược lại

Route Table

CloudNut
Learn Clouds in a Nutshell

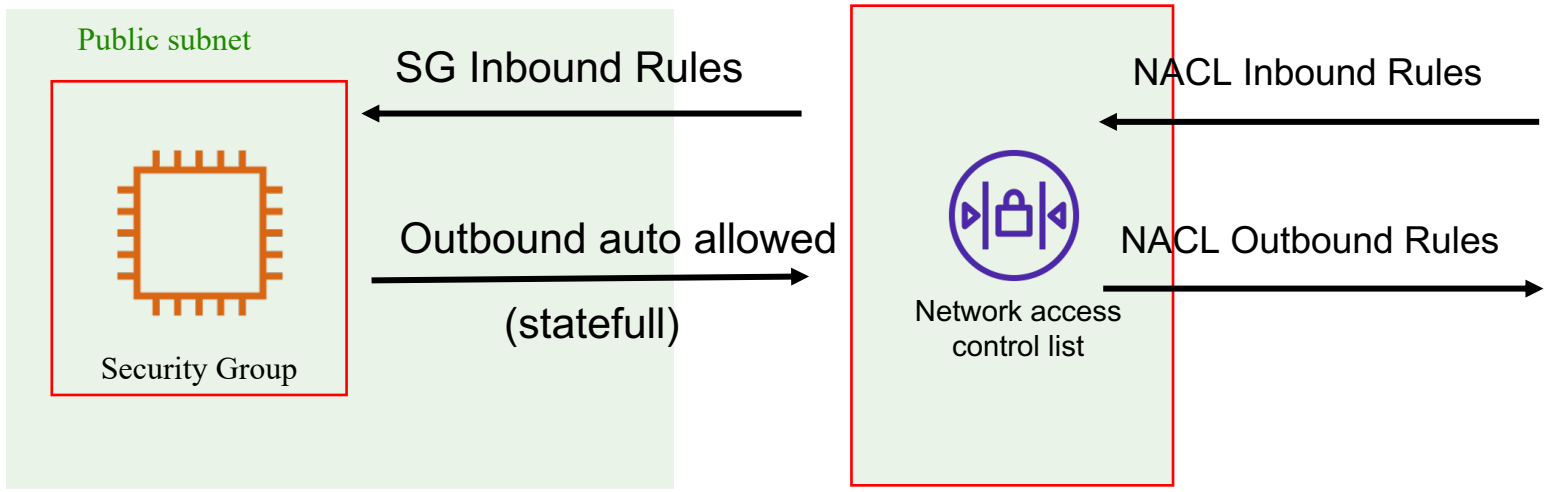
- Sử dụng như bảng định tuyến để điều hướng Traffic In/Out trong một Subnet
- Mỗi Subnet chỉ có thể gắn 1 Route Table
- Mỗi Route Table có thể gắn vào nhiều Subnets khác nhau



CloudNut
Learn Clouds in a Nutshell

NACL and SG

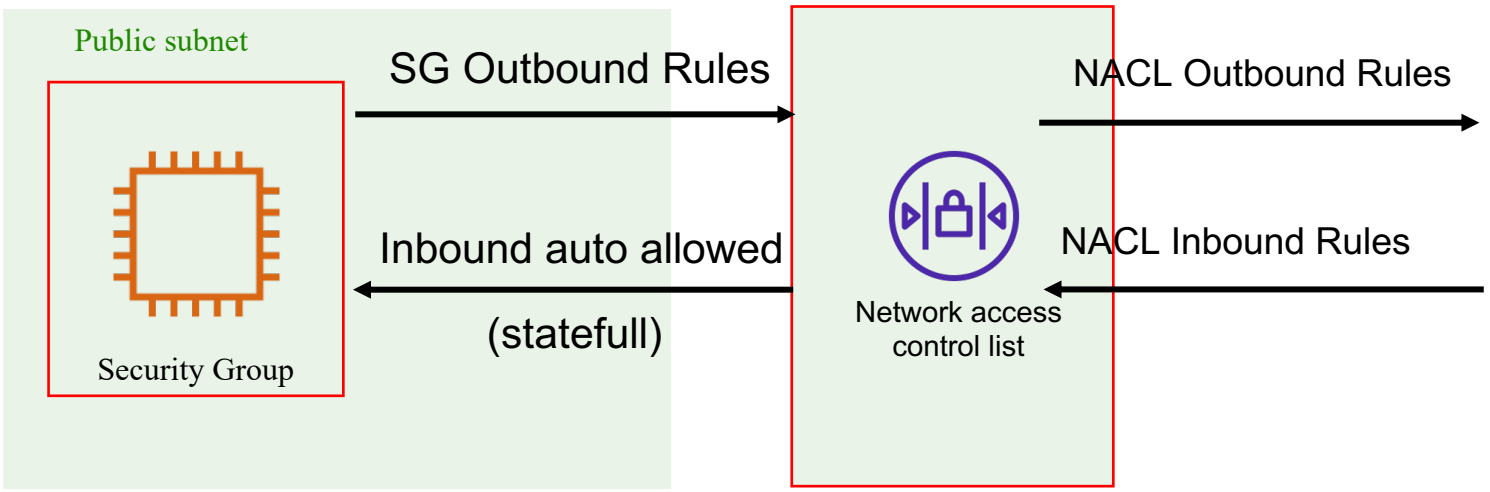
Cách Incoming Request vào EC2?



NACL = Network Access Control List

Cách Outgoint Request đi ra từ EC2?

CloudNut
Learn Clouds in a Nutshell

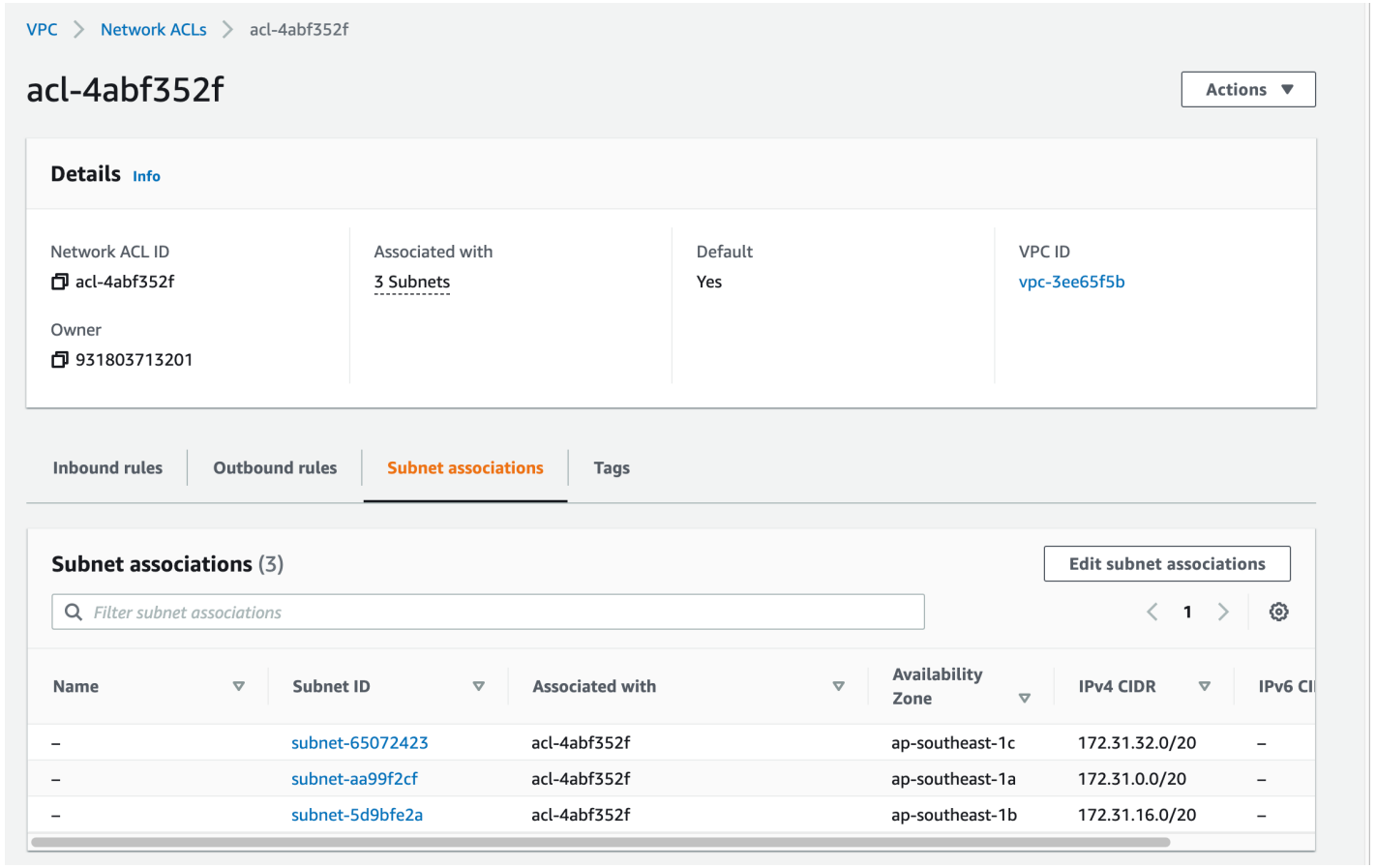


NACL = Network Access Control List

Network ACL (NACL)

CloudNut
Learn Clouds in a Nutshell

- Hoạt động như một Firewall của Subnet
- Mỗi Subnet có thể gắn một NACL và một NACL có thể gắn vào nhiều Subnet



Network ACL (NACL)

CloudNut
Learn Clouds in a Nutshell

- Mặc định NACL là AnyOpen (Cho phép tất cả Traffic In/Outbound Subnet)
- Các Rules được đánh thứ tự ưu tiên. Số càng nhỏ, càng có mức độ ưu tiên cao hơn

  (Smaller Number, Higher Predence)

Inbound rules (3)

Edit inbound rules

Filter inbound rules

1

Rule number	Type	Protocol	Port range	Source	Allow/Deny
90	All TCP	TCP (6)	0	0.0.0.0/0	Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Network ACL vs Security Groups

CloudNut
Learn Clouds in a Nutshell

Security Groups	Network ACL
Firewall ở Instance Level, ENI	Firewall ở Subnet Level
Chỉ hỗ trợ Allow Rule	Hỗ trợ Allow và Deny Rule
Stateful (Lưu trạng thái): Traffic Out sẽ tự động được cho phép nếu như Traffic In được cho phép và ngược lại	Stateless (Không trạng thái): Traffic Out cần được tường minh khai báo cho phép (Allow), không phụ thuộc vào việc Traffic In được cho phép
Đánh giá tất cả các Rules để quyết định	Xử lý theo thứ tự các số ưu tiên để đưa ra quyết định
Có hiệu lực cho tất cả các EC2 Instances được gắn với Security Group	Có hiệu lực cho tất cả các EC2 Instance nằm trong Subnet

CloudNut
Learn Clouds in a Nutshell

NAT Introduction

NAT là gì?

CloudNut
Learn Clouds in a Nutshell

- NAT viết tắt của **N**etwork **A**ddress **T**ranslation
- NAT cho phép các **EC2 Instances** trong **Private Subnet** có thể kết nối với Internet
- Có 2 loại NAT trong AWS
  - NAT Instance
  - NAT Gateway

NAT Instance

CloudNut
Learn Clouds in a Nutshell

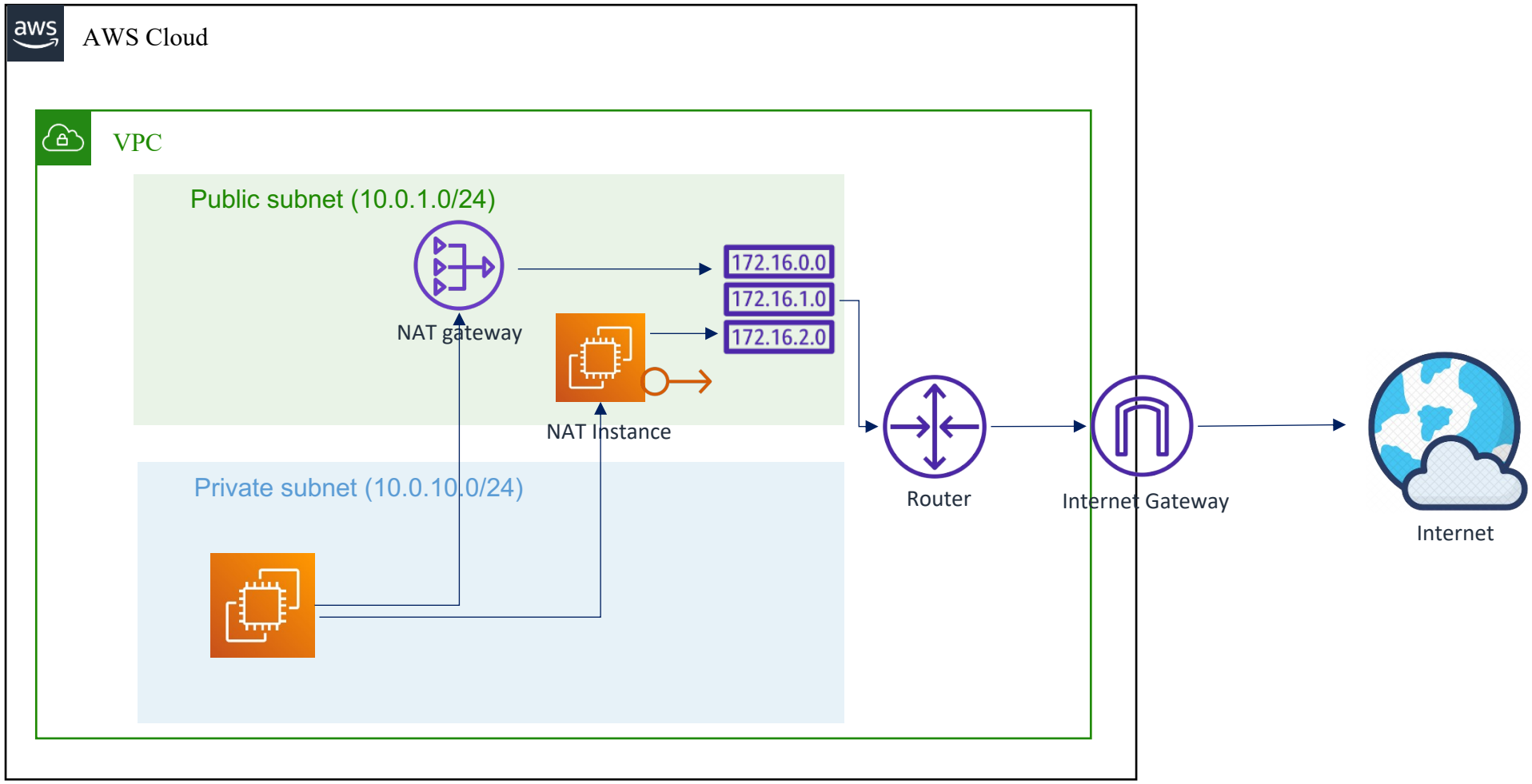
- Một máy EC2 Instance được cài đặt chức năng làm NAT
- EC2 Instance này được đặt ở Public Subnet
- EC2 Instance này cần phải có Public/Elastic IP
- Phải disable cờ **Source/Destination** check
- Route Table của Private Subnet cần phải được định tuyến tới **NAT Instance (EC2 Instance)** cho các Traffic đi ra Internet

NAT Gateway

CloudNut
Learn Clouds in a Nutshell

- NAT được cung cấp dưới dạng dịch vụ, do AWS quản lý (AWS managed service)
- High Availability, Scalability

Cách NAT hoạt động?



Exam Tips

CloudNut
Learn Clouds in a Nutshell

- NAT Instance
  - EC2 đóng vai trò làm NAT Instance cần được đặt trong Public Subnet
  - Phải disable cờ Source/Destination check
  - Bandwith phụ thuộc vào EC2 Instance Type
  - Phải quản lý SGs và Rule gắn vào NAT
  - Sử dụng ASG để quản lý NAT Instance

Labs

CloudNut
Learn Clouds in a Nutshell

1. VPC Lab