



NACL

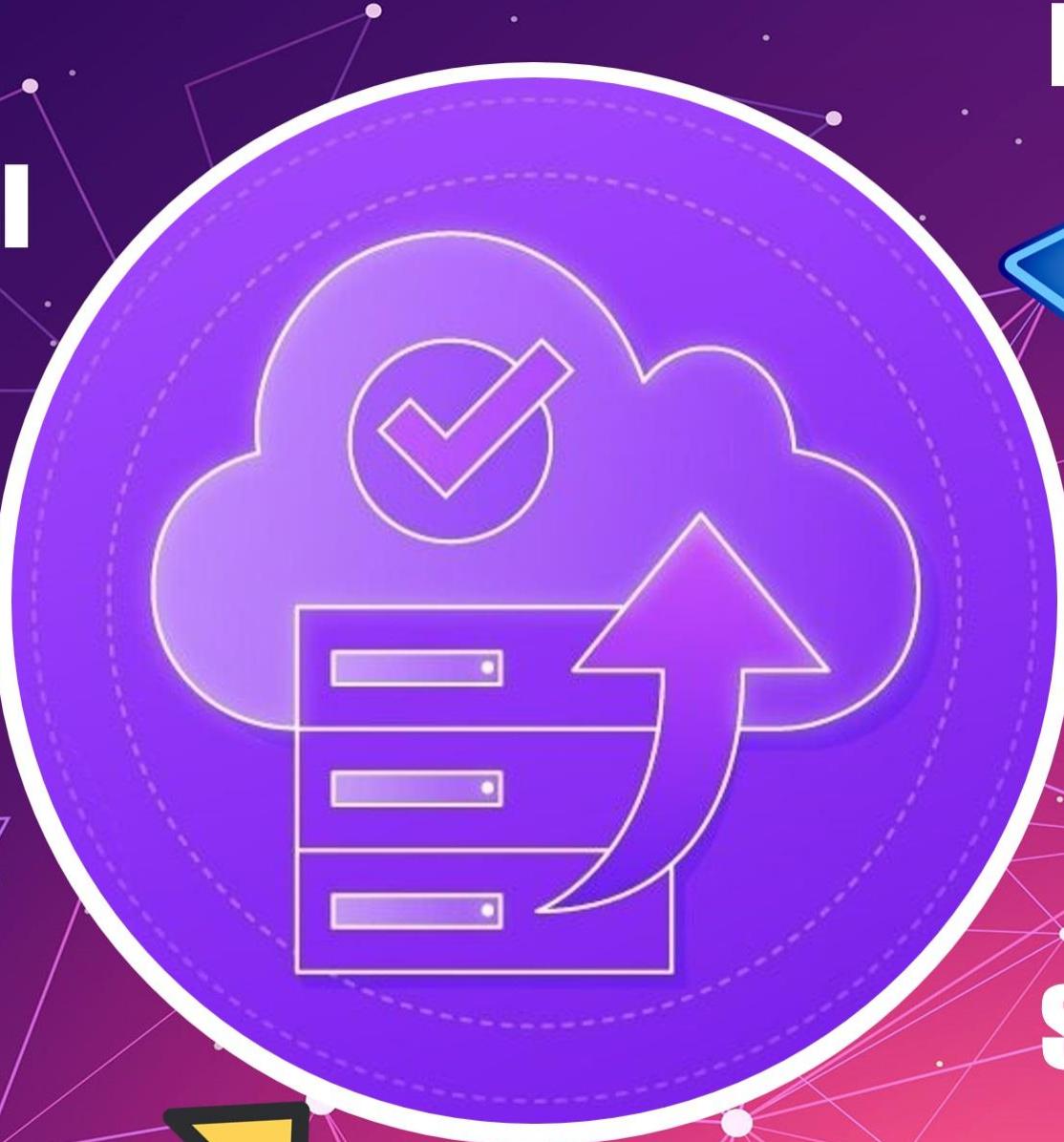
# Custom VPC

Networking

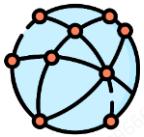
Fire Wall

Security

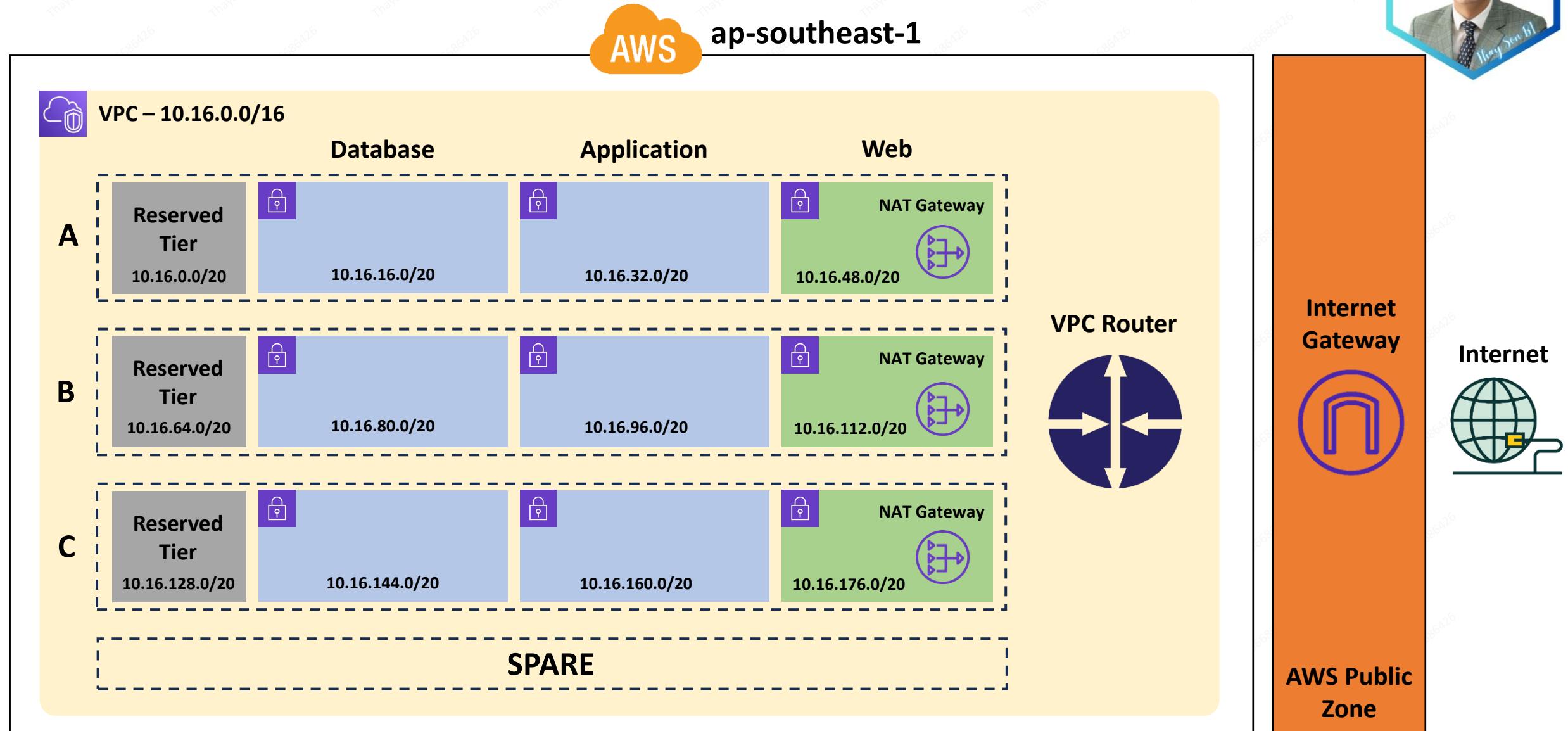
SG

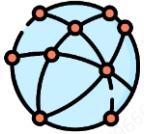


Amazon Web Service - Training



# TARGET ARCHITECTURE





## Regional Service – Toàn bộ AZs trong Region

Là mạng **độc lập** (local network)

Ngăn chặn tất cả các truy cập **IN** hoặc **OUT** không rõ ràng

Cho phép cấu hình **linh hoạt**

Hybrid Networking - **Cloud** khác hoặc **On-premise**

Hai dạng: **Default** hoặc **Dedicated tenancy**



# VPC Subnet



Networking

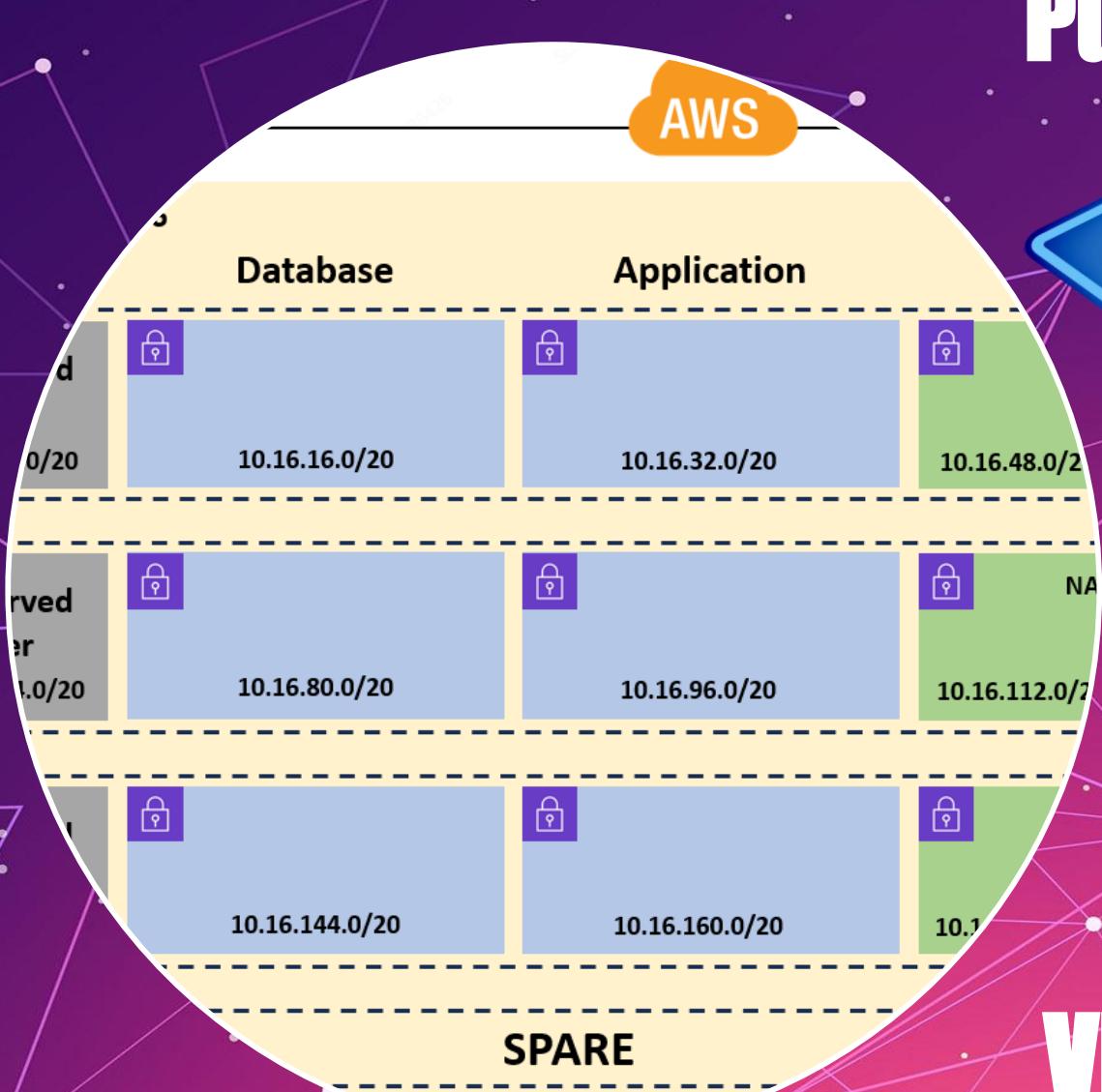
Private

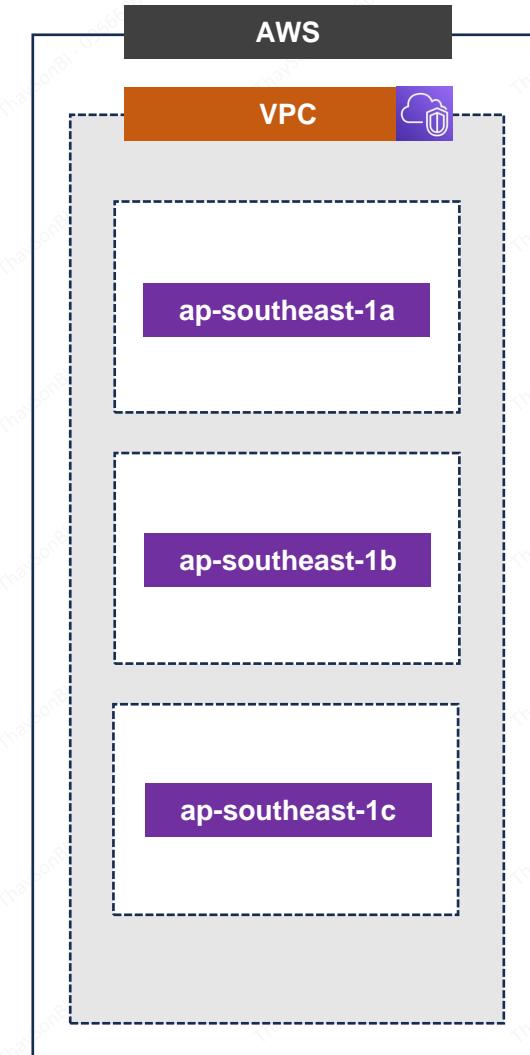
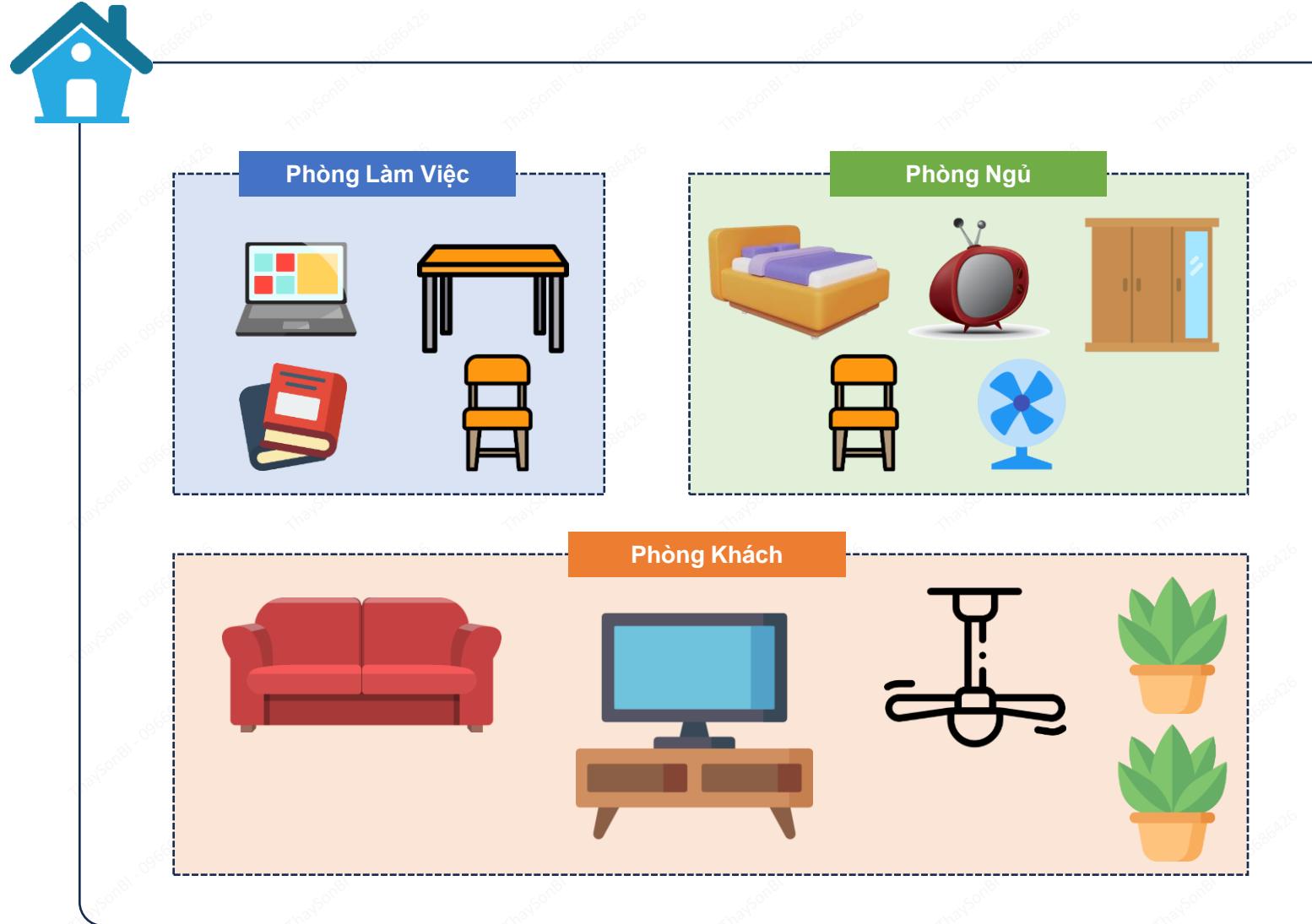
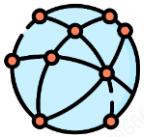
CIDR Block

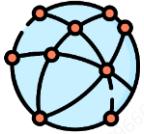
Public

VPC

SPARE







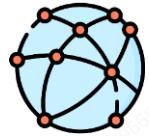
Subnet được triển khai trên **AZ**

**1 subnet** → 1 AZ, 1AZ → **0+** subnet

Không thể khai báo **chồng chéo** các IP giữa những Subnet

Có thể khai báo thêm **IPv6 CIDR** cho subnet

Các subnet **trong 1 VPC** có thể **giao tiếp với nhau**



**10.16.16.0/20** (10.16.16.0 → 10.16.31.255)

**Network Address** (10.16.16.0)

**Network + 1** (10.16.16.1) – **VPC Router**

**Network + 2** (10.16.16.2) – Reserved (**DNS**)

**Network + 3** (10.16.16.3) – Reserved (**Future**)

**Broadcast address** 10.16.31.255 (**Last IP in Subnet**)



Easily

Step by Step

Hands On

# Create VPC & Subnet

Explain

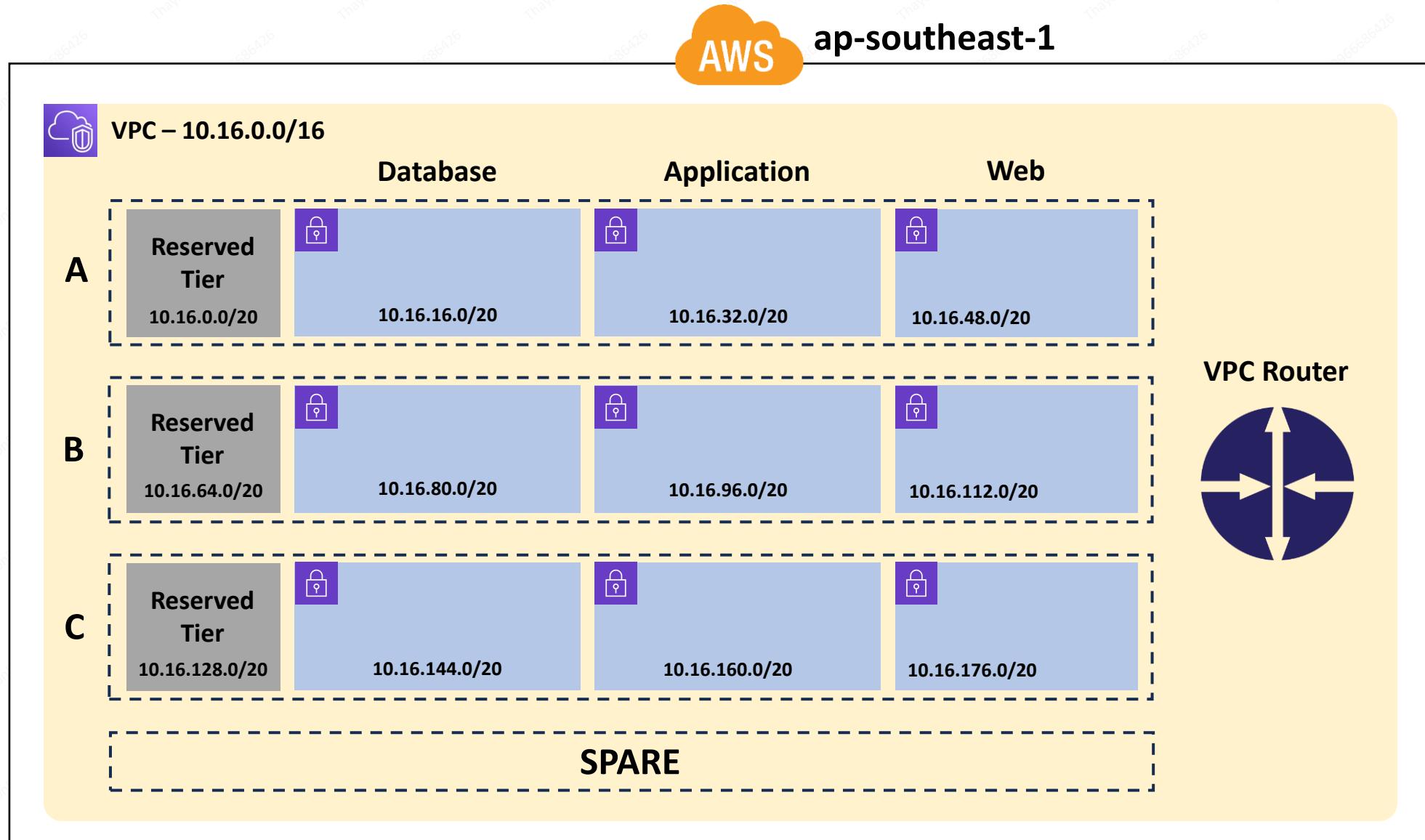
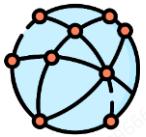
ĐỀ MÔ



Practice

Amazon Web Service - Training







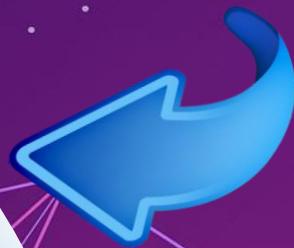
# DHCP Server

Networking

Manage

Grant

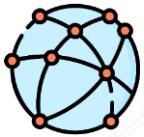
Option Set



Automatic

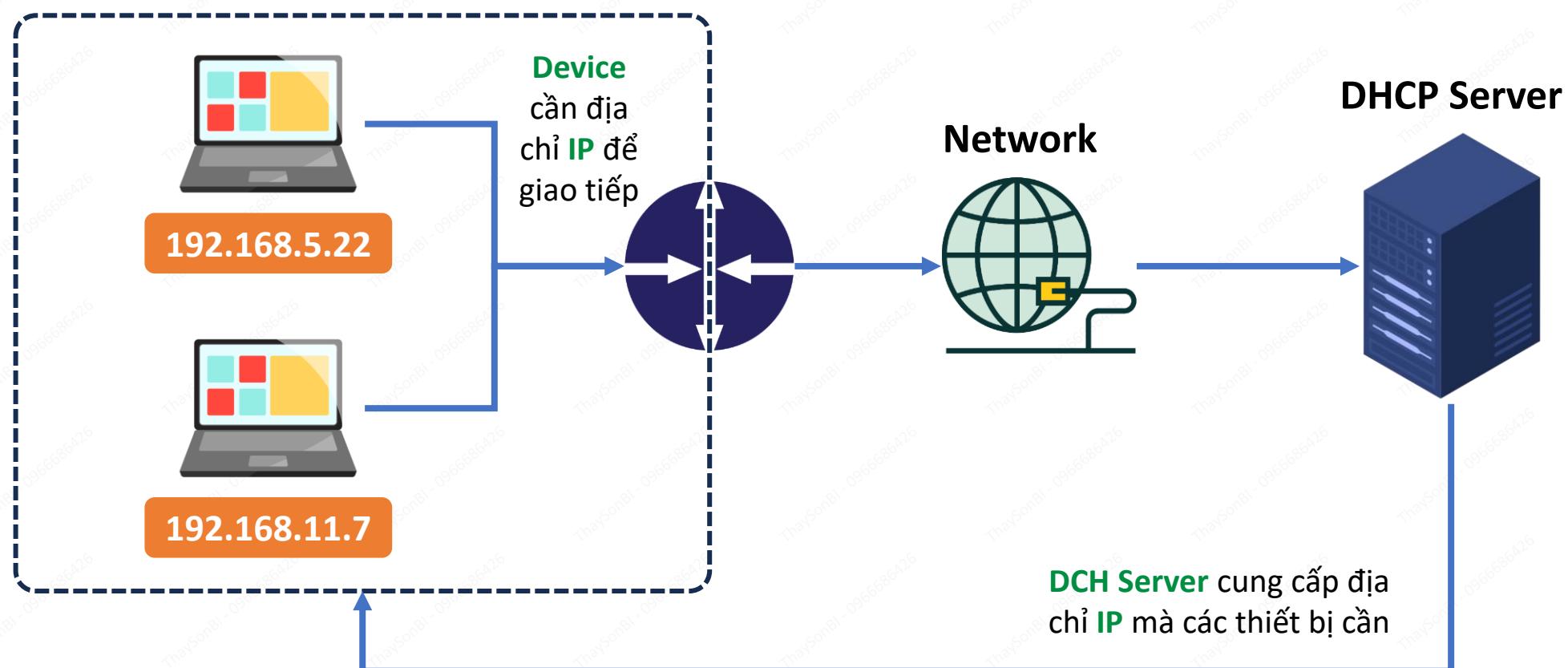
Amazon Web Service - Training

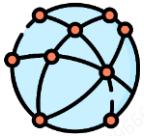




**DHCP – Dynamic Host Configuration Protocol** là một giao thức quản trị mạng được sử dụng trên Internet Protocol (IP) networks.

Trong đó, **DHCP Server** cấp phát một địa chỉ IP và những thông số cần thiết cho **mỗi một thiết bị trong mạng** để có thể giao tiếp với **những IP network khác**





# DHCP – Dynamic Host Configuration Protocol

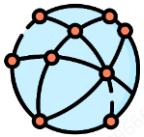
**DHCP Server** có sẵn trong Windows hoặc phần cứng

...tự động cấp phát tài nguyên cho các thiết bị trong mạng

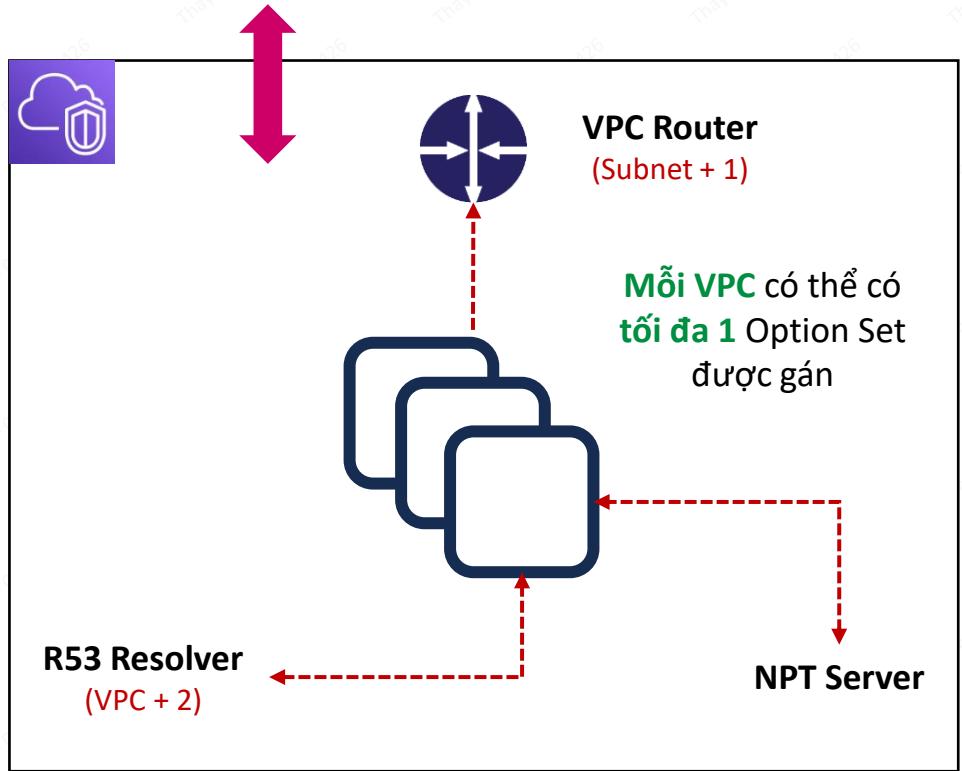
IP Address, Subnet Mask và Default Gateway

DNS Servers và Domain name, NTP Server...

**AmazonProvidedDNS** và **Custom DNS Domain**



Việc cấp phát Option sets mới là **ngay lập tức** nhưng việc thay đổi yêu cầu **DHCP Renew** khá tốn thời gian



Mỗi VPC có thể có  
tối đa 1 Option Set  
được gán

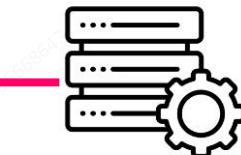
R53 Resolver  
(VPC + 2)

AWS cung cấp **public** và **private** DNS names. Để sử dụng **custom domains** bạn cũng cần sử dụng **custom DNS servers**

**VPC-B**      **VPC-C**



**DCH Option Sets**  
có thể liên kết  
với 0 hoặc **nhiều**  
VPC



**DHCP Option Sets**

**DCH Option Sets** không thể bị chỉnh sửa,  
khi đã tạo ra thì chúng sẽ không thay đổi



# VPC Router

Networking

## Route Table

Route

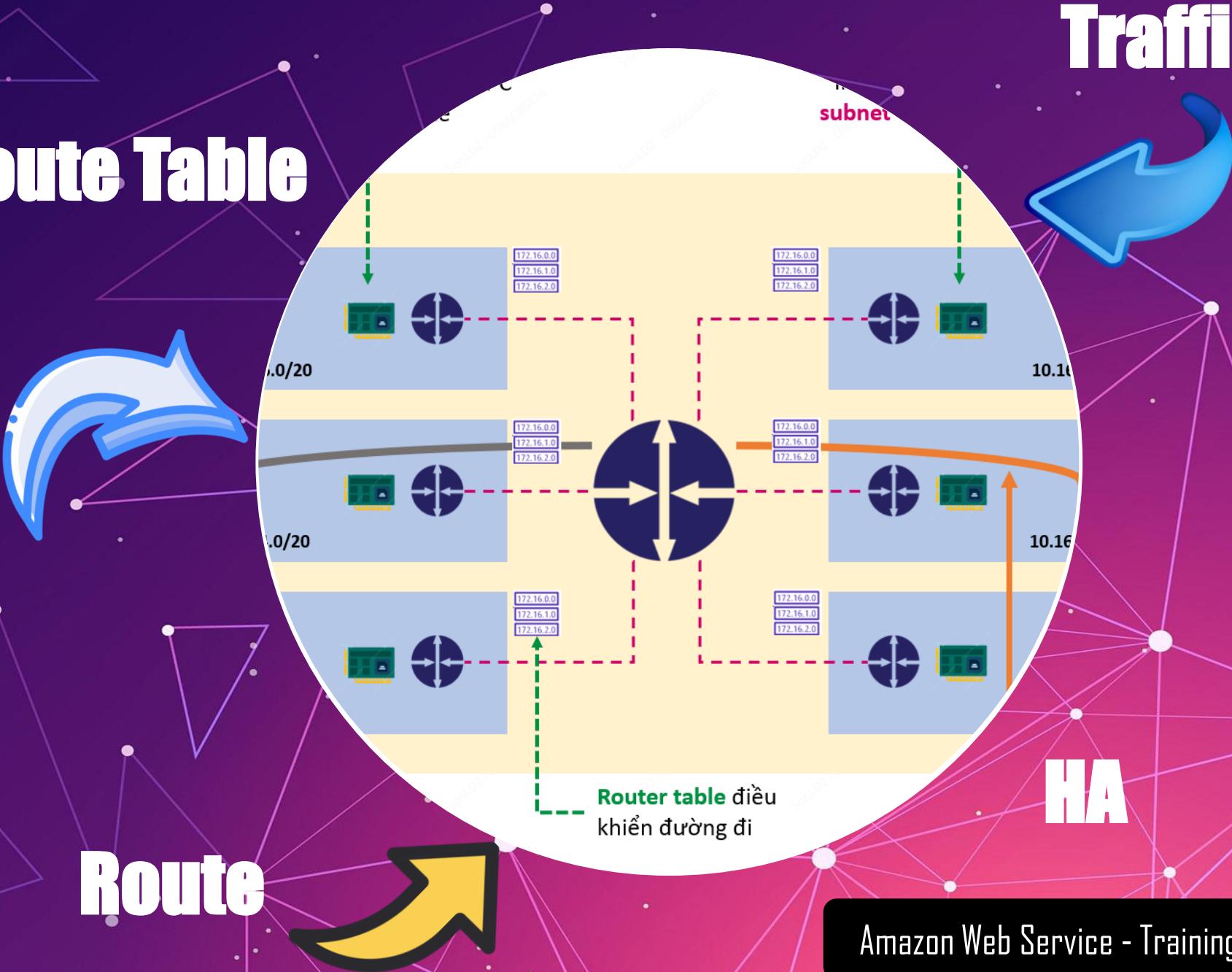


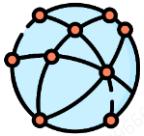
Traffic

HA

Router table điều  
khiển đường đi

Amazon Web Service - Training





**Virtual Router** nằm bên trong VPC

**Luôn sẵn sàng** – Có **trên toàn bộ AZ** của Region đó

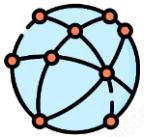
**Scalable** – không cần phải quản trị hiệu suất

**Routes** là con đường giữa các **Subnet**

...hoặc từ **External vào VPC** cũng như từ **VPC ra External**

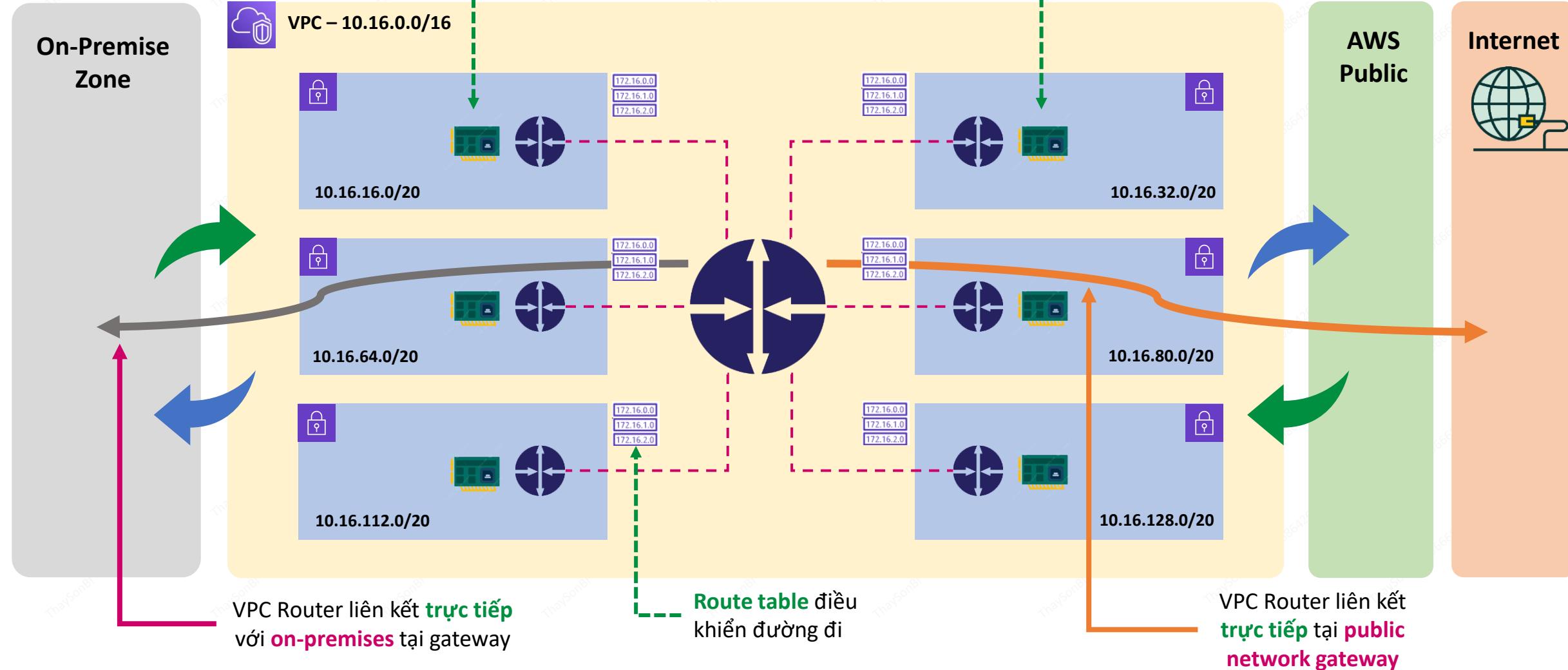
**Interface** có trên mọi subnet “**subnet + 1**”

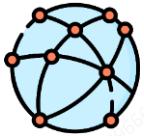
Được quản lý và điều khiển bởi **route table**



Mỗi subnet đều có một VPC  
Router Interface

Interface sử dụng địa chỉ  
subnet + 1 (VD: 10.16.32.1)





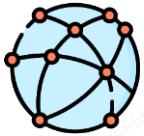
Mỗi **VPC** được tạo ra có 1 **Main route table** (RT)

Các **custom route table** có thể được tạo với Subnet

...nhưng sẽ **xóa route trước đó khỏi MAIN RT**

**Subnet** được gắn với **ONE RT** (Main hoặc Custom)

**Route table** chứa các tuyến đường sẽ truyền gói tin



rtb-01736d035bb06c5b2

You can now check network connectivity with Reachability Analyzer

Details Info

Route table ID  
[rtb-01736d035bb06c5b2](#)

VPC  
[vpc-04152b1b86063a6ba](#)

Main  
 Yes

Owner ID  
[464019668072](#)

Explicit subnet associations  
-

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (2)

Filter routes

Both

Destination  
0.0.0.0/0  
172.31.0.0/16

Target  
igw-008d9534af0bae055  
local

Status	Propagated
Active	No
Active	No

Các traffic được cho phép truy cập

Nơi traffic được truyền đến

Gán subnet vào route table

Các route của router



Easily

Step by Step

Hands On

# Route Table Main & Custom

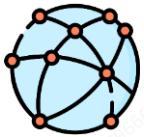
Explain

ĐỀ MÔ

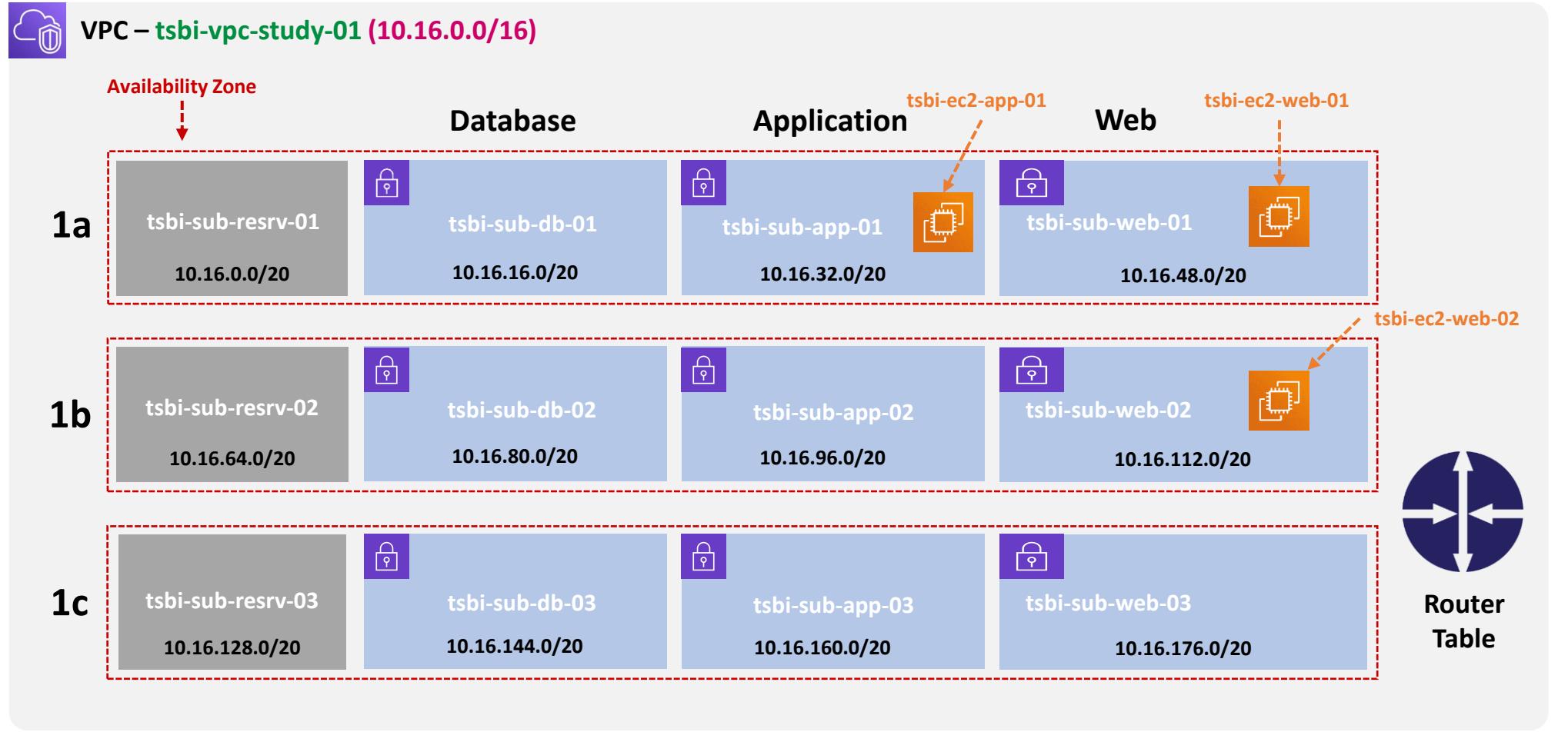
Practice



Amazon Web Service - Training



AWS ap-southeast-1





# Internet Gateway

Networking

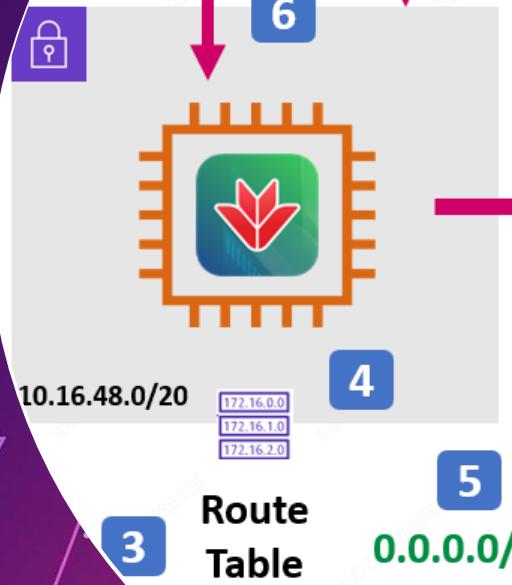
VPC

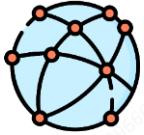
Internet

Route

Gateway

Cấp phát địa chỉ public IPv4





Giúp **VPC** kết nối ra **AWS public service** hoặc **public internet**

**Có thể** tạo và gắn vào **VPC** theo mối quan hệ **1-1**

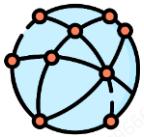
**Dịch** giao thức (**IP, TCP, SSH, Telnet...**) giữa các mạng với nhau

**Mặc định** luôn luôn **sẵn sàng** và tự động **scale**

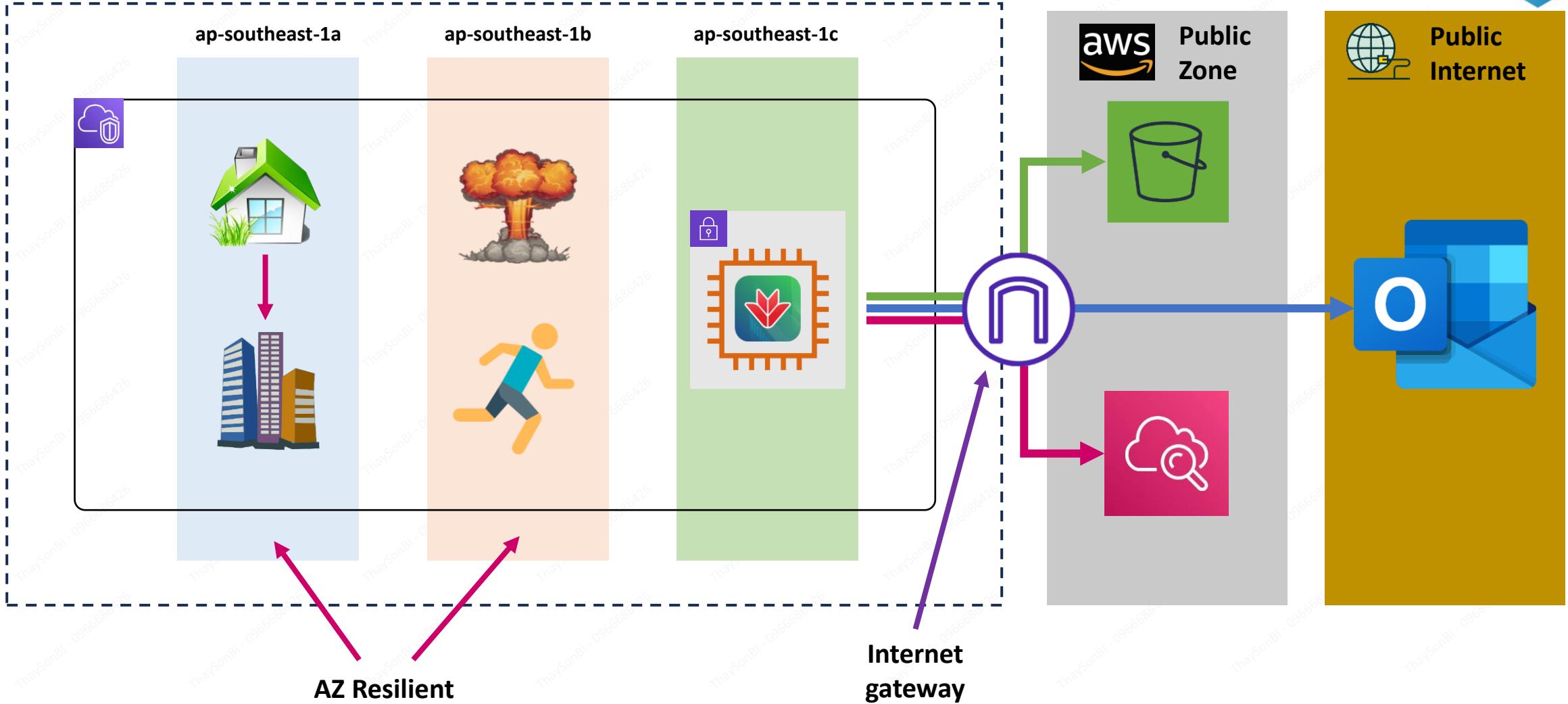
Hỗ trợ **IPv4** và **IPv6** - **IN** và **OUT**

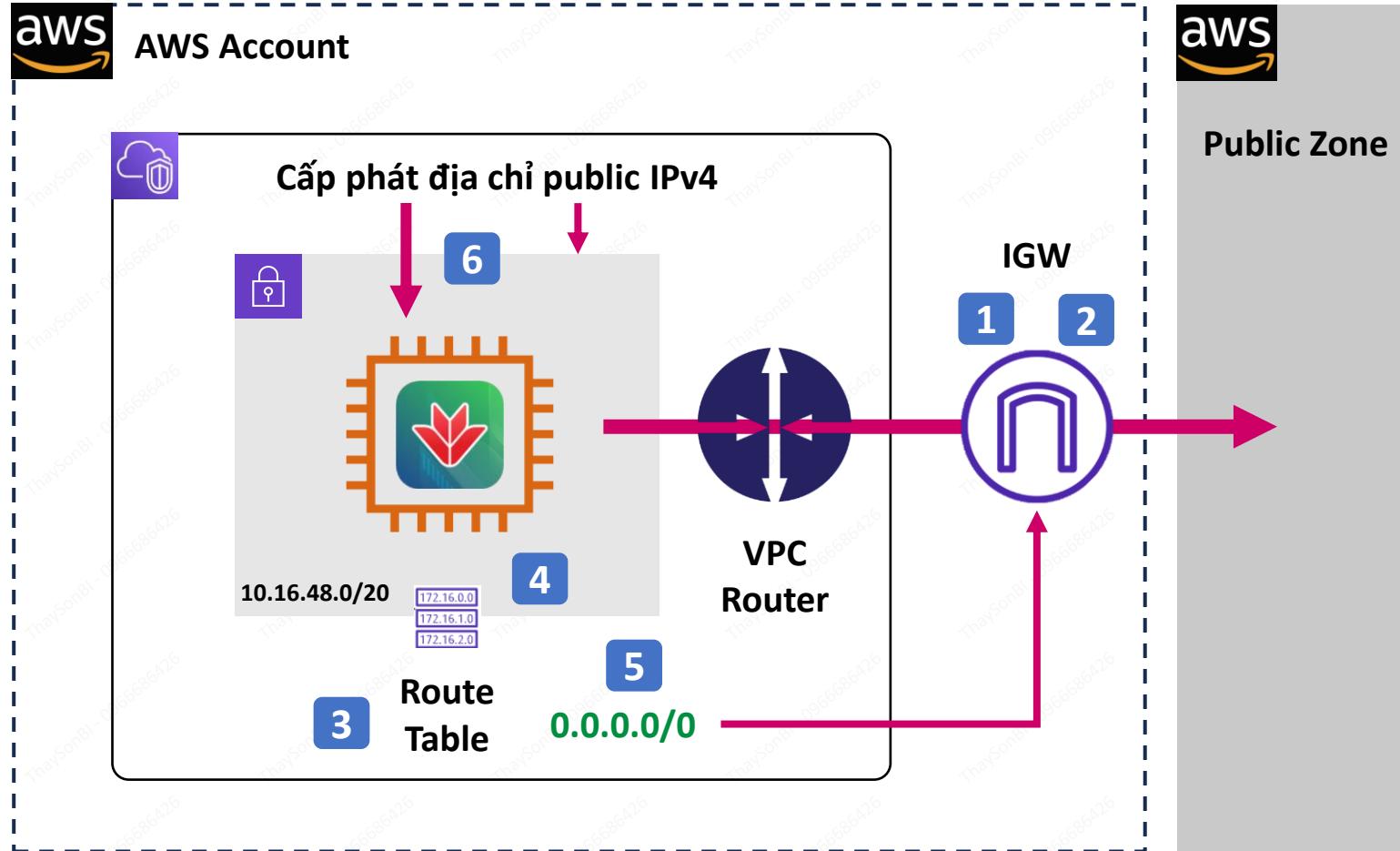
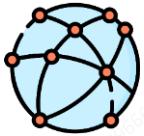
Là phần mềm **logic** không có thiết bị phần cứng tương ứng

Thực hiện **NAT** – **Private IP** to **Public IP**



## AWS Account





- 1. Create IGW**
- 2. Attach IGW to VPC**
- 3. Create custom RT**
- 4. Associate RT**
- 5. Default routes → IGW**
- 6. Subnet allocate Public IPv4**



Easily

Step by Step

Hands On

# Setup Route Table & IGW

Explain

ĐỀ MÔ



Practice



Amazon Web Service - Training

