

AWS Cloud for beginner

Instructor: Linh Nguyen

(Engineering Consultant, AWS Cloud Solution Architect)

Level: Beginner

“Không có việc gì khó, chỉ sợ không biết làm”

Virtual Private Cloud (VPC)

“Có 2 thứ ngăn cản chúng ta trên con đường trở thành chuyên gia Cloud:

- 1. Security*
- 2. Networking” 😊*

Target

- Hiểu được VPC là gì, tại sao cần VPC?
- Các thành phần cơ bản tạo nên một VPC.
- Hiểu rõ các nguyên tắc khi thiết kế một VPC.
- Hiểu rõ các concept về Networking liên quan VPC.
- Thực hành tạo VPC theo chuẩn AWS (High Availability, Security).
- Thực hành với VPC Endpoint và VPC Peering.

Copyright@Linh Nguyen on Udemy

What is VPC

Viết tắt của **Virtual Private Cloud**

Là một service cho phép người dùng tạo một mạng ảo (virtual network) và control toàn bộ network in/out của mạng đó.

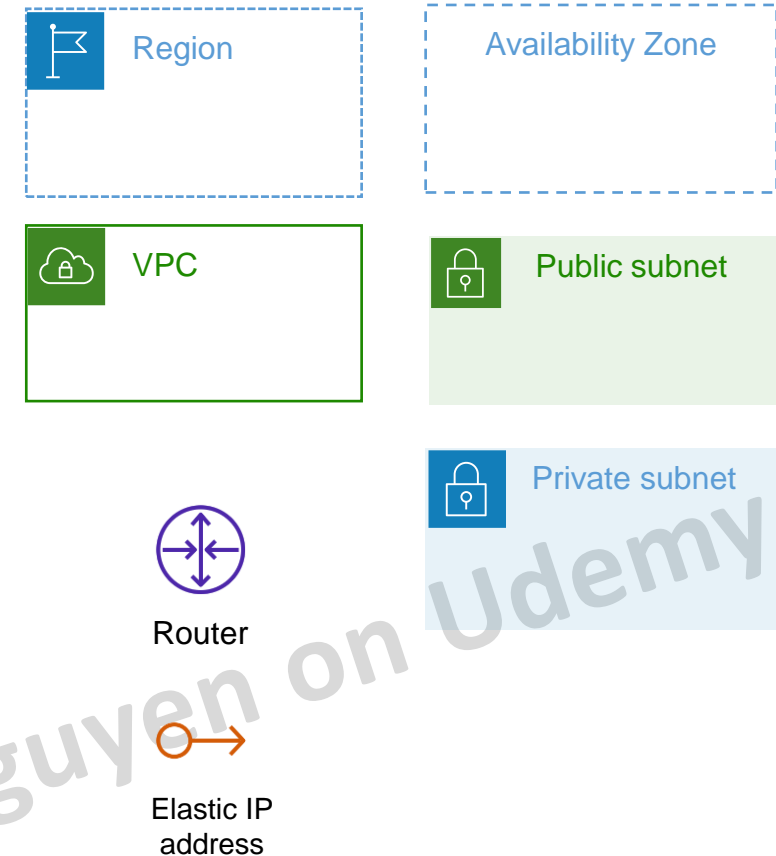
VPC tương đối giống với network ở datacenter truyền thống tuy nhiên các khái niệm đã được AWS đơn giản hoá giúp người dùng dễ tiếp cận.



Virtual Private Cloud

Các thành phần cơ bản của VPC

- VPC: Một mạng ảo được tạo ra ở cấp độ region.
- Subnet: Một dải IP được định nghĩa nằm trong VPC. Mỗi subnet phải được quyết định Availability Zone tại thời điểm tạo ra.
- IP Address: IP V4 hoặc V6 được cấp phát. Có 2 loại là Public IP và Private IP.
- Routing: xác định traffic sẽ được điều hướng đi đâu trong mạng.
- Elastic IP: IP được cấp phát riêng, có thể access từ internet (public), không bị thu hồi khi instance start -> stop.



Các thành phần cơ bản của VPC

- Security Group: Đóng vai trò như một firewall ở cấp độ instance, định nghĩa traffic được đi vào /đi ra. *Đã học ở bài EC2.
- Network Access Control List (ACL): được apply ở cấp độ subnet, tương tự như security group nhưng có rule Deny và các rule được đánh độ ưu tiên. Mặc định khi tạo VPC sẽ có 1 ACL được apply cho toàn bộ subnet trong VPC (mở all traffic không chặn gì cả).



Network access
control list

Security group

Copyright@Linh Nguyen on Udemy

Các thành phần cơ bản của VPC

- VPC Flow Log: capture các thông tin di chuyển của traffic trong network.
- VPN Connection: kết nối VPC trên AWS với hệ thống dưới On-premise.
- Elastic Network Interface: đóng vai trò như 1 card mạng ảo.



Flow logs



VPN connection



Elastic network interface

Copyright@Linh Nguyen on Udemy

Các thành phần cơ bản của VPC

- Internet Gateway: Kết nối VPC với Internet, là cổng vào từ internet tới các thành phần trong VPC.
- NAT Gateway: dịch vụ NAT của AWS cho phép các thành phần bên trong kết nối tới internet nhưng không cho bên ngoài kết nối tới.
- VPC Endpoint: kênh kết nối private giúp kết nối tới các services khác của AWS mà không thông qua internet.
- Peering connection: kênh kết nối giữa 2 VPC.
- Transit gateways: đóng vai trò như 1 hub đứng giữa các VPCs, VPN Connection, Direct Connect.



Internet gateway



Peering connection



NAT gateway



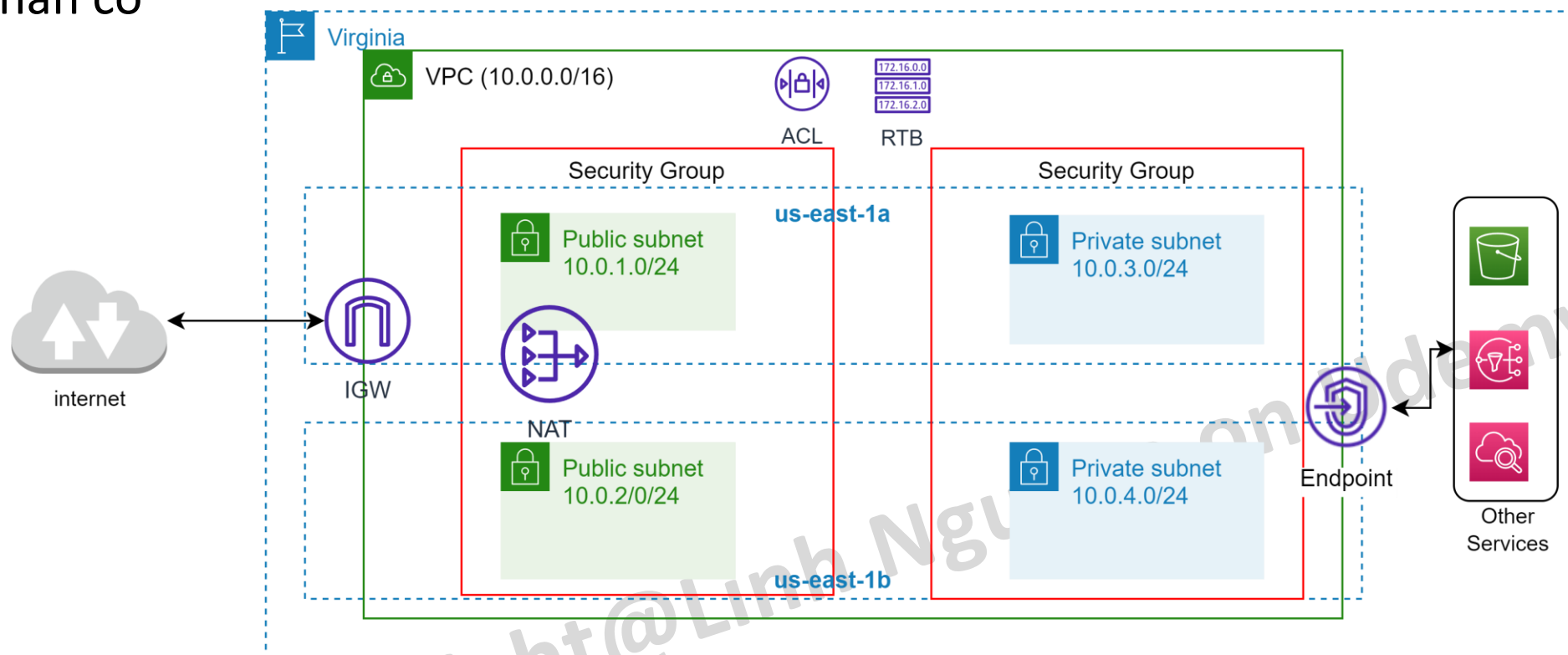
Transit Gateway



Endpoints

Common VPC Design

Ví dụ về một VPC có đầy đủ các thành phần cơ bản.



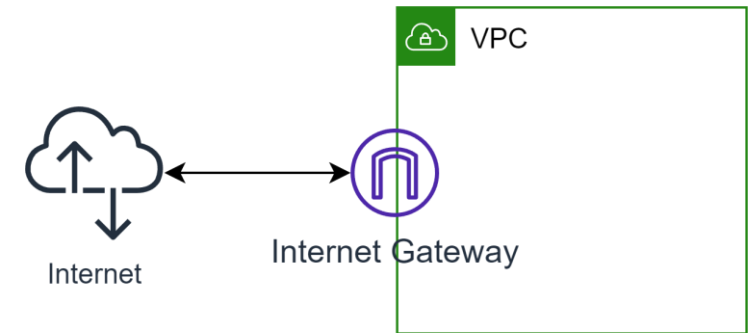
Các thành phần của VPC (detail)

Internet Gateway

Là cửa ngõ để truy cập các thành phần trong VPC.

Nếu VPC không được gắn Internet Gateway thì không thể kết nối SSH tới instance kể cả instance đó có được gắn public IP.

Mặc định default-vpc do AWS tạo sẵn đã có gắn Internet Gateway.

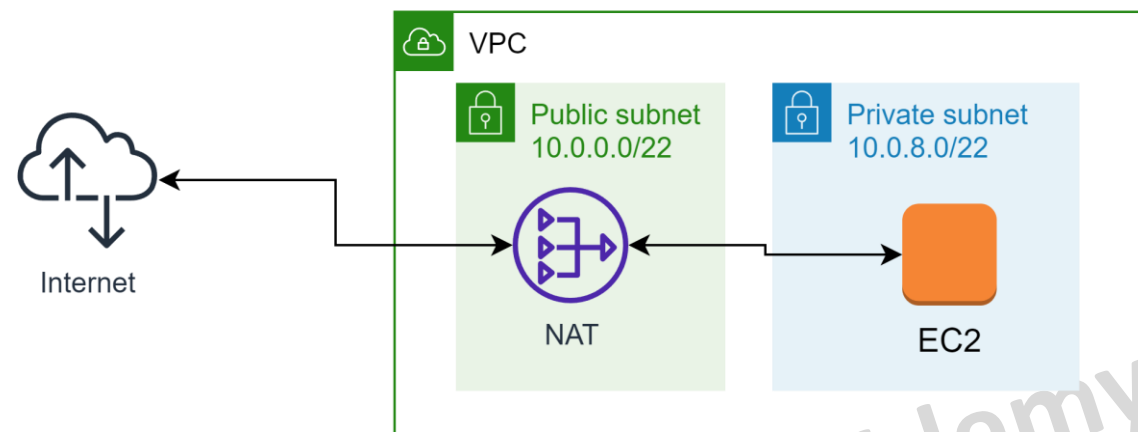


Các thành phần của VPC (detail)

NAT Gateway

Giúp cho các instance trong Private Subnet có thể đi ra internet mà không cần tới public IP.

Giúp tăng cường bảo mật cho các resource cần private (App, DB).



Các thành phần của VPC (detail)

Network Access Control List (ACL)

Control network in/out đối với subnet được associate

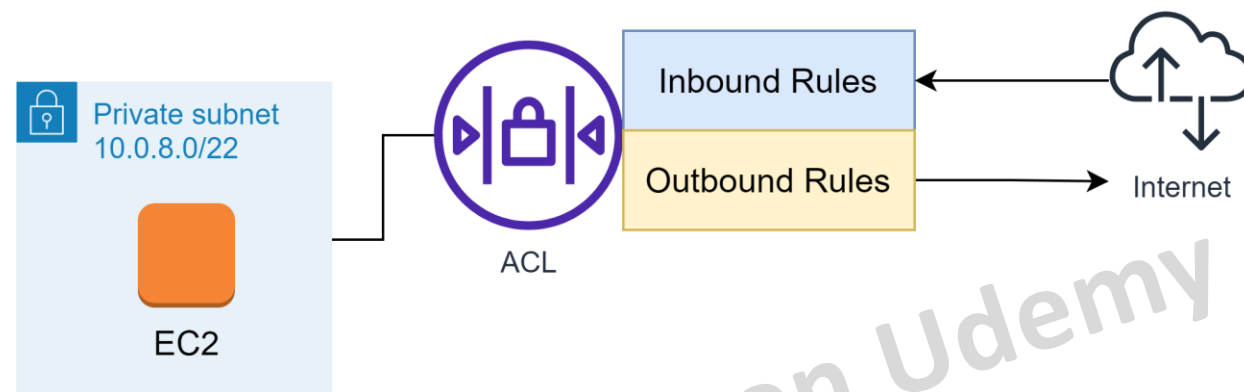
Mỗi rule sẽ có các thông số:

- Priority
- Allow/Deny
- Protocol
- Port range
- Source IP / Destination IP

Default ACL sẽ allow all.

Sử dụng quá nhiều rule của ACL sẽ làm giảm performance.

Rule của ACL là stateless.



Các thành phần của VPC (detail)

Security Group

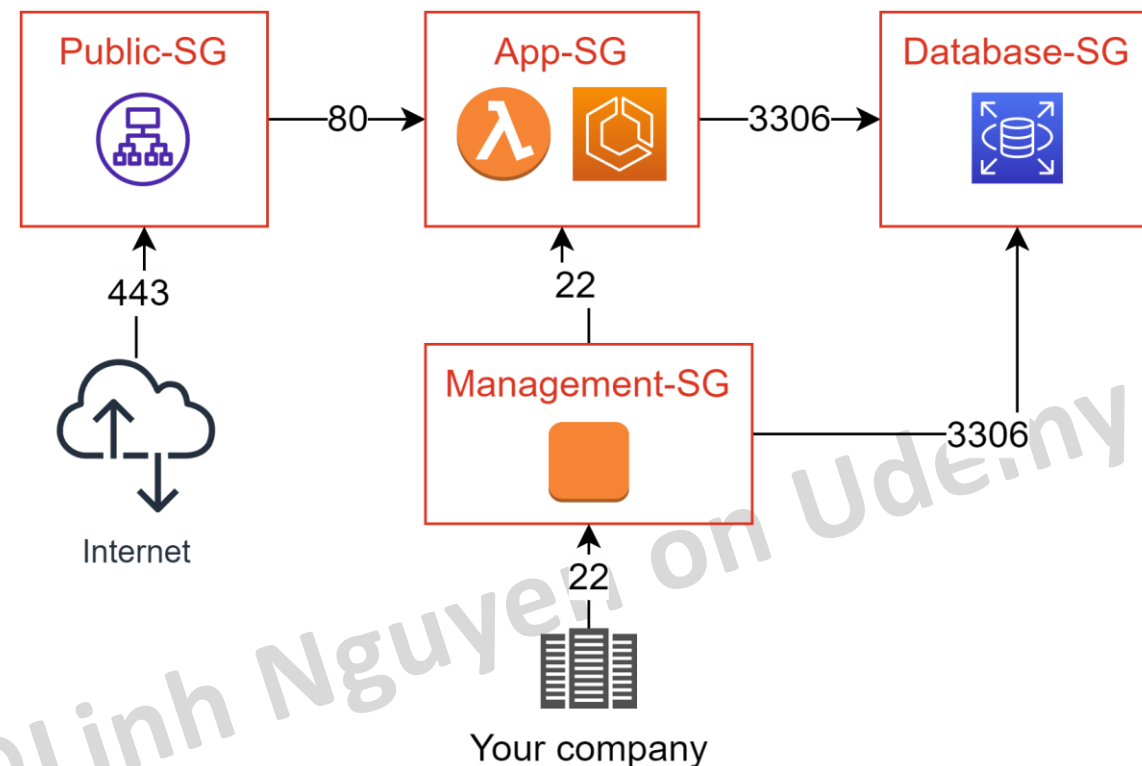
Thường được dùng để gom nhóm các resource có chung network setting (in/out, protocol, port).

Khi thiết kế cần quan tâm tới tính tái sử dụng, dễ quản lý.

Source của một Security Group có thể là CIDR hoặc id của một Security Group khác.

Rule của Security Group là stateful và không có deny rule.

*Statefull có nghĩa là nếu Inbound cho phép traffic đi vào thì khi request tới sẽ nhận được response mà không cần explicit allow Outbound. Khác với Network ACL.



Các thành phần của VPC (detail)

Route Table

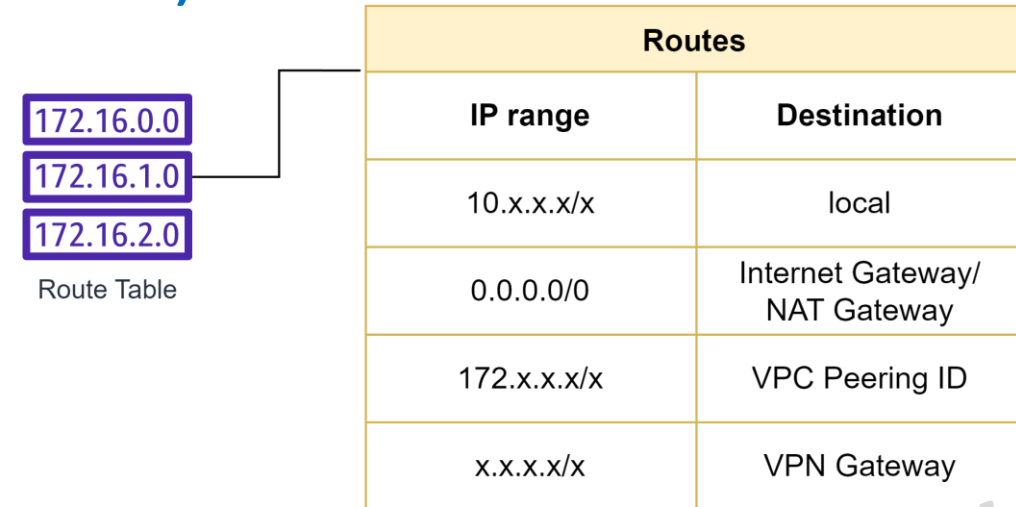
Định tuyến traffic trong subnet hoặc gateway sẽ được điều hướng đi đâu

Route Table sẽ quyết định một subnet sẽ là **Private** hay **Public**.

Subnet được gọi là Public khi có route đi tới **Internet Gateway** và ngược lại.

Một Subnet chỉ có thể associate 1 route table.

Default VPC do AWS tạo sẵn sẽ có 1 main route table associate với toàn bộ subnet.



| Routes | |
|-------------|----------------------------------|
| IP range | Destination |
| 10.x.x.x/x | local |
| 0.0.0.0/0 | Internet Gateway/ NAT Gateway |
| 172.x.x.x/x | VPC Peering ID |
| x.x.x.x/x | VPN Gateway |

| Destination | Target |
|-------------------------|-----------------------|
| 10.0.0.0/16 | Local |
| 2001:db8:1234:1a00::/56 | Local |
| 172.31.0.0/16 | pcx-11223344556677889 |
| 0.0.0.0/0 | igw-12345678901234567 |
| ::/0 | eigw-aabbccdde1122334 |

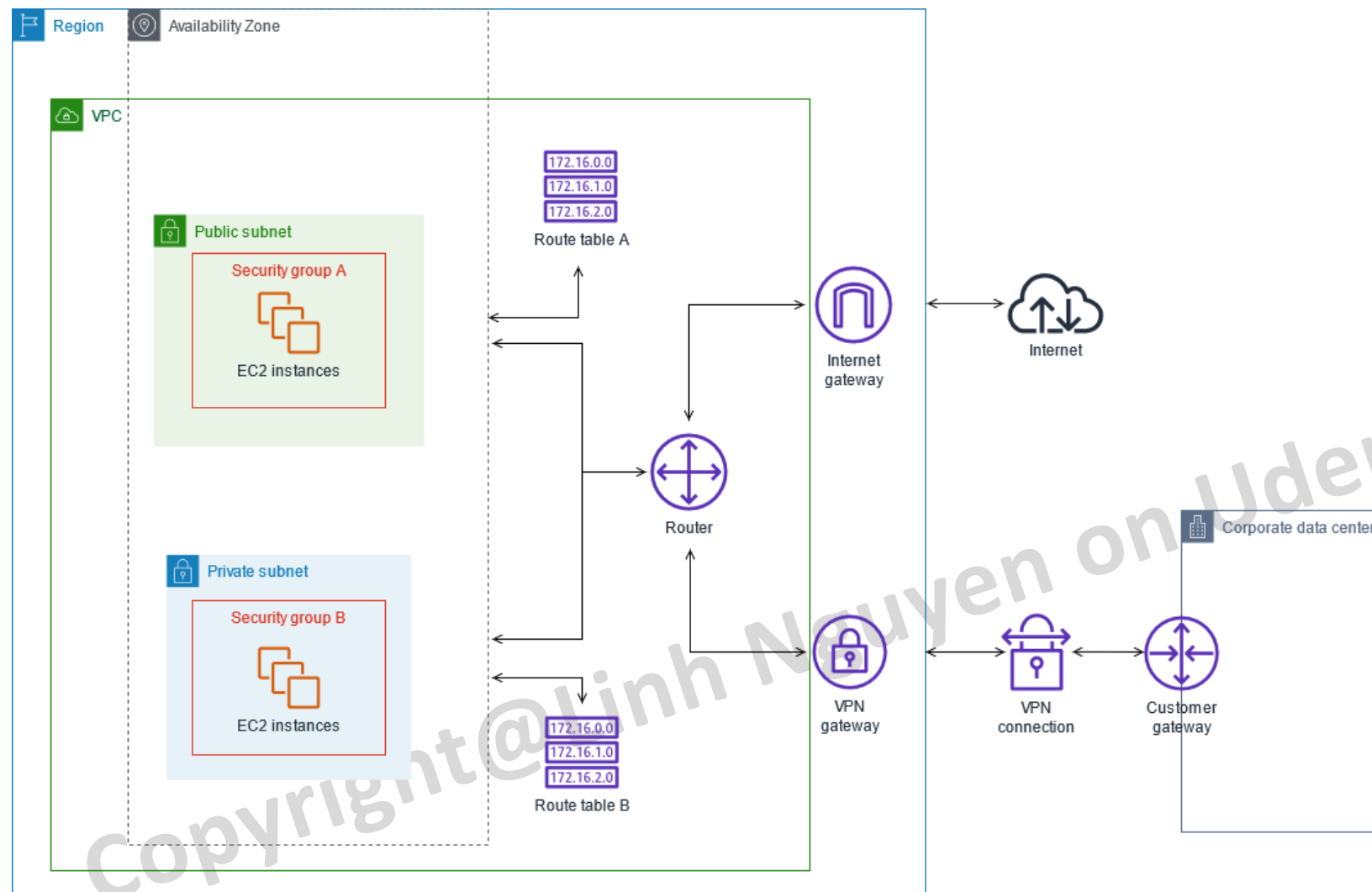
Example of route table

Các thành phần của VPC (detail)

Route

Table

Example



Các thành phần của VPC (detail)

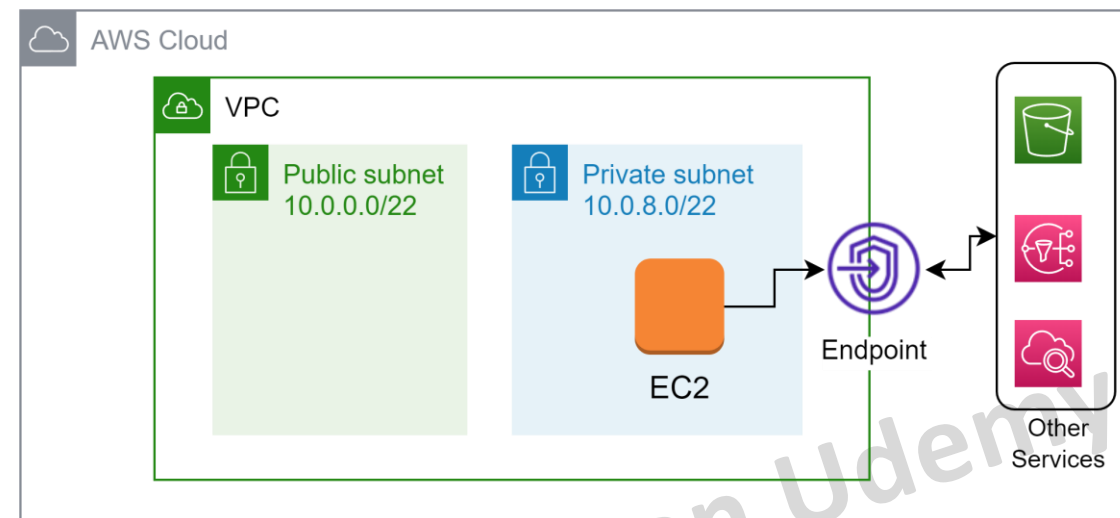
VPC Endpoint

Giúp các resource trong VPC có thể kết nối tới các dịch vụ khác của AWS thông qua private connection.

Công dụng: secure, tăng tốc độ.

Có 2 loại endpoint là Gateway Endpoint (S3, Dynamodb) và Interface Endpoint (SQS, CloudWatch,...)

Endpoint có thể được cấu hình Security Group để hạn chế truy cập.



Làm sao định nghĩa một VPC?

VPC được định nghĩa bằng 1 dải CIDR.

AWS cho recommend chọn 1 trong 3 dải CIDR sau (theo chuẩn RFC-1918)

- 192.168.0.0 – 192.168.255.255. Ex: **192.168.0.0/20**
- 10.0.0.0 – 10.255.255.255. Ex: **10.0.0.0/16**
- 172.16.0.0 – 172.31.255.255. Ex: **172.31.0.0/16**

Việc định nghĩa CIDR của IP cần tuân thủ một số tiêu chí sau:

- Cover được số lượng IP private cần cấp phát trong tương lai.
- Tránh overlap với các hệ thống sẵn có (kể cả on-premise) nếu không sẽ không thể peering.

Copyright@Linh Nguyen on Udemy

Phân chia subnet như thế nào?

Subnet được coi như một thành phần con của VPC.

Một VPC có thể chứa nhiều subnet không overlap nhau.

Khi tạo subnet phải chọn Availability Zone.

Chọn CIDR cho subnet cần lưu ý:

- Số lượng IP cho các resource cần cấp phát (EC2, Container, Lambda,...)

VD: bạn tạo 1 subnet 10.0.1.0/24 sẽ chứa được 256 IP trừ đi 5 reserve ip của AWS
-> 251 IP khả dụng.

- Số lượng subnet dự tính sẽ tạo trong tương lai.
- Đặt số sao cho dễ quản lý.

Copyright@Linh Nguyen on Udemy

Sử dụng tool để chia VPC và Subnet

<https://www.ipaddressguide.com/cidr>

VD: một dải ip 10.0.0.0/16 sẽ có thể chứa tổng cộng 65536 IPs.
 $2^{(32-16)} = 65536$

CIDR to IP Range

Result

| | |
|--------------------|--------------|
| CIDR Range | 10.0.0.0/16 |
| Netmask | 255.255.0.0 |
| Wildcard Bits | 0.0.255.255 |
| First IP | 10.0.0.0 |
| First IP (Decimal) | 167772160 |
| Last IP | 10.0.255.255 |
| Last IP (Decimal) | 167837695 |
| Total Host | 65,536 |

CIDR

10.0.0.0/16

Calculate

Sử dụng tool để chia VPC và Subnet

<https://www.ipaddressguide.com/cidr>

VD: một dải ip 10.0.0.0/22 sẽ có thể chứa tổng cộng 1024 IPs.

$$2^{(32-22)} = 1024$$

⇒ Số lượng subnet của một VPC =
 Tổng IP / Số IP của mỗi Subnet.
 = 65536/1024 = 64 subnet

Lưu ý: Các subnet trong một VPC không nhất thiết phải có số lượng IP giống nhau.

CIDR to IP Range

Result

| | |
|--------------------|---------------|
| CIDR Range | 10.0.0.0/22 |
| Netmask | 255.255.252.0 |
| Wildcard Bits | 0.0.3.255 |
| First IP | 10.0.0.0 |
| First IP (Decimal) | 167772160 |
| Last IP | 10.0.3.255 |
| Last IP (Decimal) | 167773183 |
| Total Host | 1,024 |

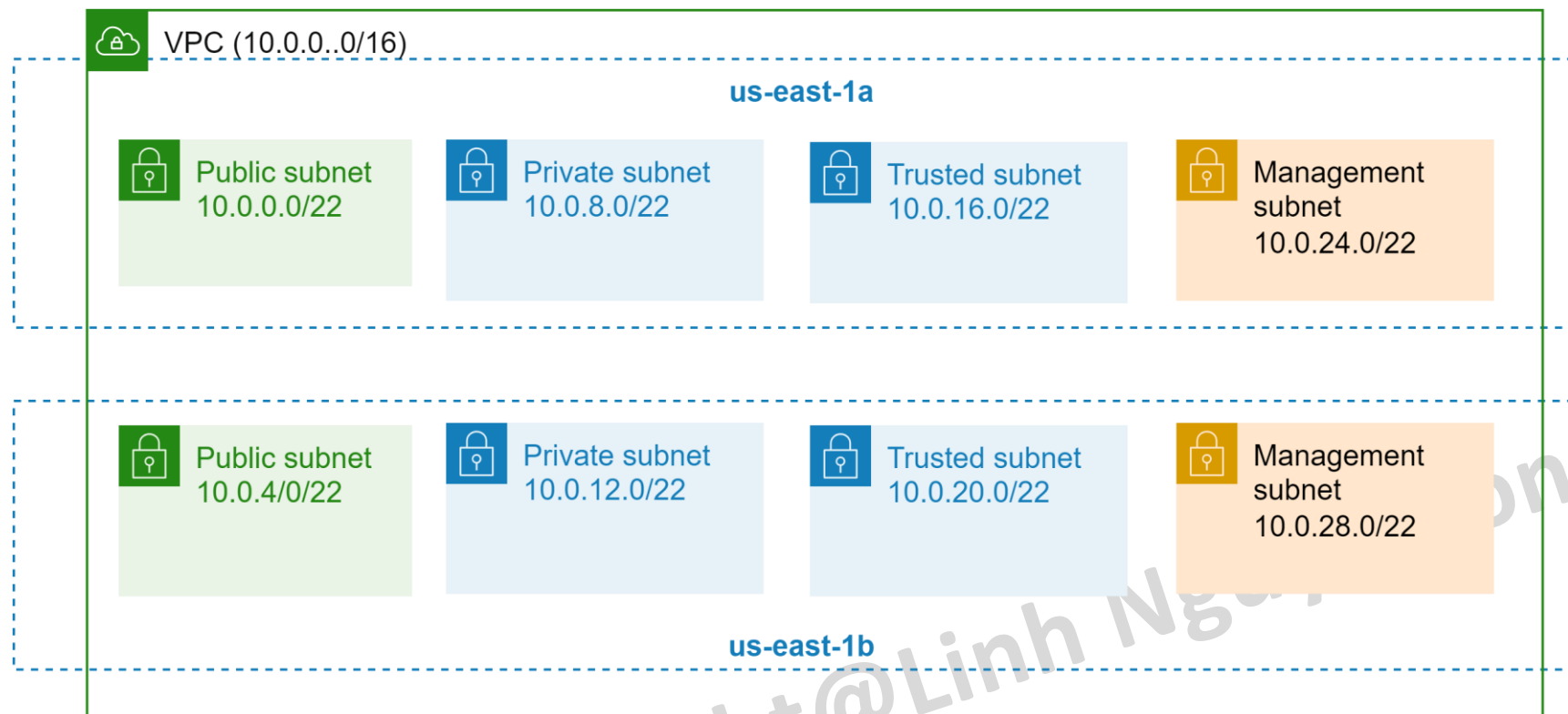
CIDR

10.0.0.0/22

Calculate

Sử dụng tool để chia VPC và Subnet

Giả sử VPC sử dụng CIDR /16 và Subnet sử dụng CIDR /22 ta sẽ có sơ đồ sau.



- *Việc phân chia bao nhiêu loại subnet phụ thuộc vào yêu cầu về độc lập network cho các component
- *Các subnet không sử dụng hết IP của VPC nên trong tương lai vẫn có thể mở rộng tạo thêm subnet nếu cần

Pricing of VPC

VPC là một dịch vụ miễn phí tuy nhiên user phải trả phí cho các resource liên quan

- NAT Gateway: tính tiền theo giờ, ~\$45/month/Gateway.
- VPC Endpoint: Tính tiền theo giờ và lưu lượng traffic.
- VPN Connection: tính tiền theo giờ.
- Elastic IP: Tính tiền theo giờ x số IP.
- Traffic: data đi ra ngoài internet.
- ...and more

Copyright@Linh Nguyen on Udemy

Lab 1 – Thiết kế VPC Đơn giản

Thiết kế một VPC như sau (sử dụng drawio hoặc Powerpoint)

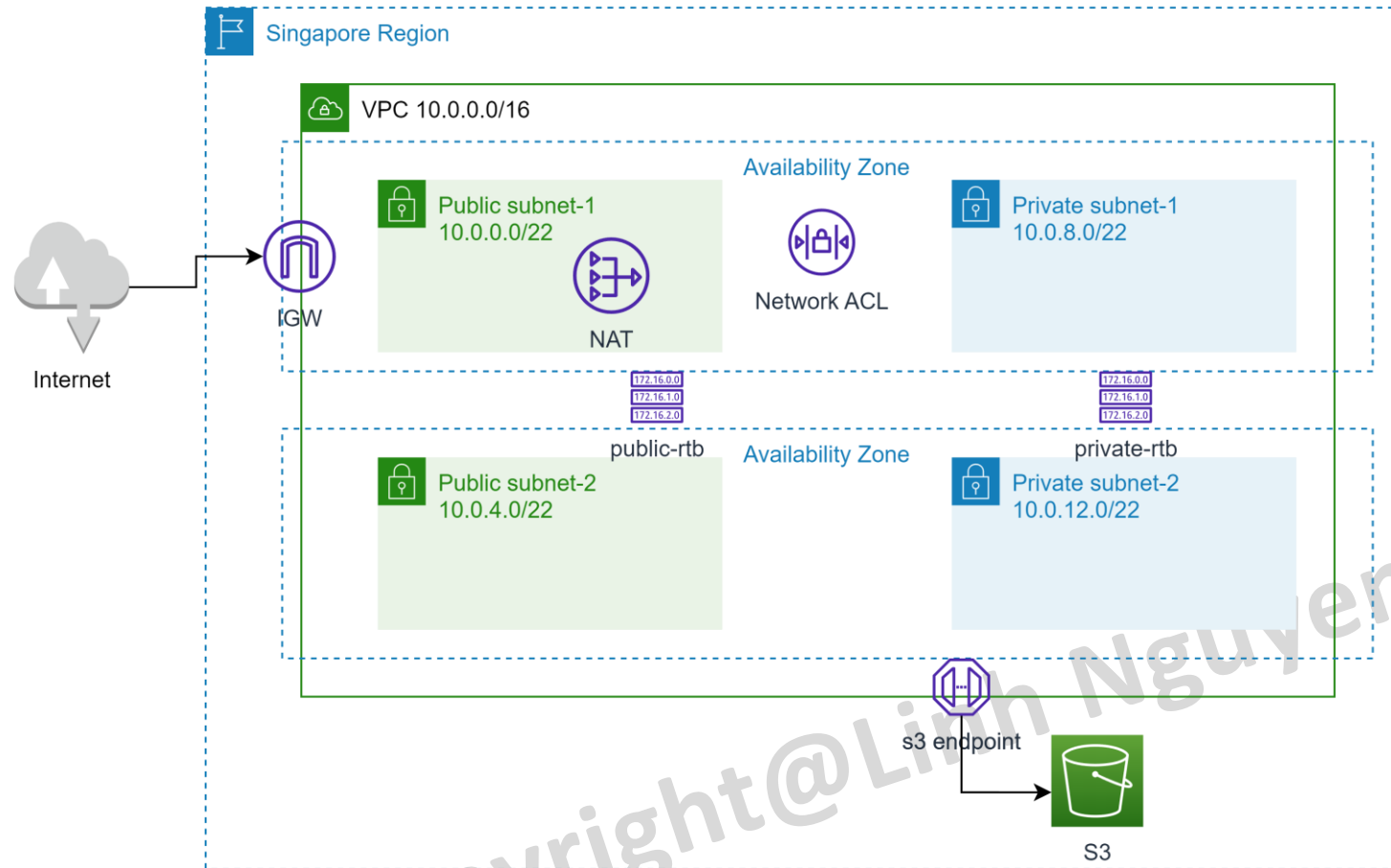
- VPC CIDR: 10.0.0.0/16
- Có 2 loại subnet Public, Private. Mỗi subnet chứa ít nhất **1000** IPs.
- Mỗi loại subnets nằm ở ít nhất 2 AZ.
- Có 1 Internet Gateway, cấu hình route table tới Internet Gateway.
- Có 1 NAT Gateway, cấu hình route table tới NAT Gateway.

Thiết kế security group cho 4 nhóm đối tượng:

- Application Load Balancer (ALB): expose port HTTPS 443.
- App Server cho phép port 80 từ ALB, 22 từ Bastion server.
- Database Server sử dụng MySQL sd port: 3306. Elastic Search sd port: 9200.
- Bastion Server: SSH port 22 từ IP công ty.
- Thiết kế VPC Endpoint cho S3 service.

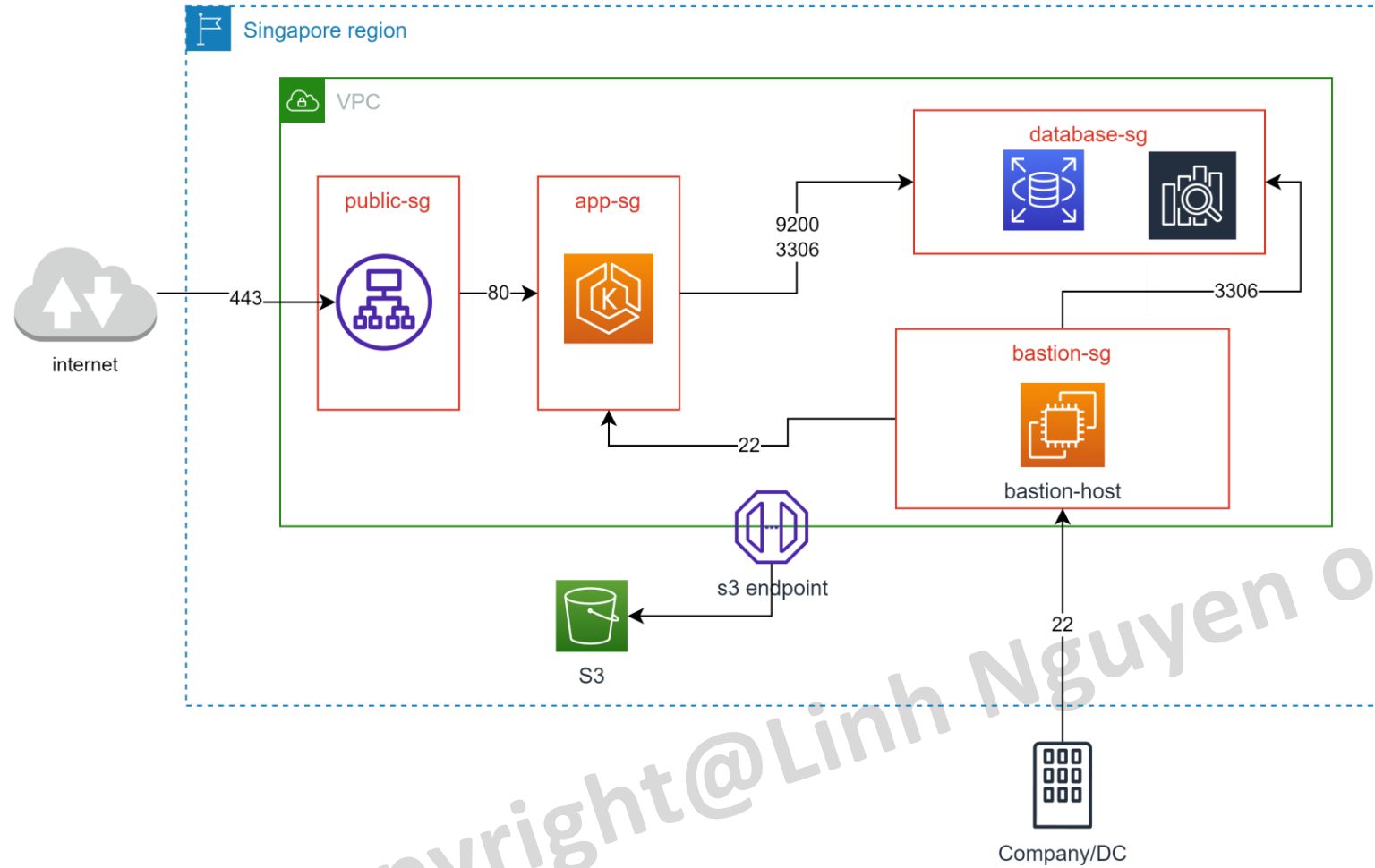
Lab 1 – Thiết kế VPC Đơn giản

Đáp án



Lab 1 – Thiết kế VPC Đơn giản

Đáp án



Lab 2 – Tạo VPC và các thành phần

Yêu cầu: Sử dụng AWS Console để tạo các resource đã thiết kế trong bài Lab 1

**Lưu ý, trong bài lab này sẽ làm step-by-step để các bạn nắm lý thuyết.*

Thứ tự tạo resources:

1. VPC
2. Subnets
3. IGW
4. NAT GW
5. RouteTables (Public and Private). Attach vào subnets tương ứng.
6. VPC Endpoint for S3, Cấu hình route table private đi ra S3 End Point.
7. Security Groups.

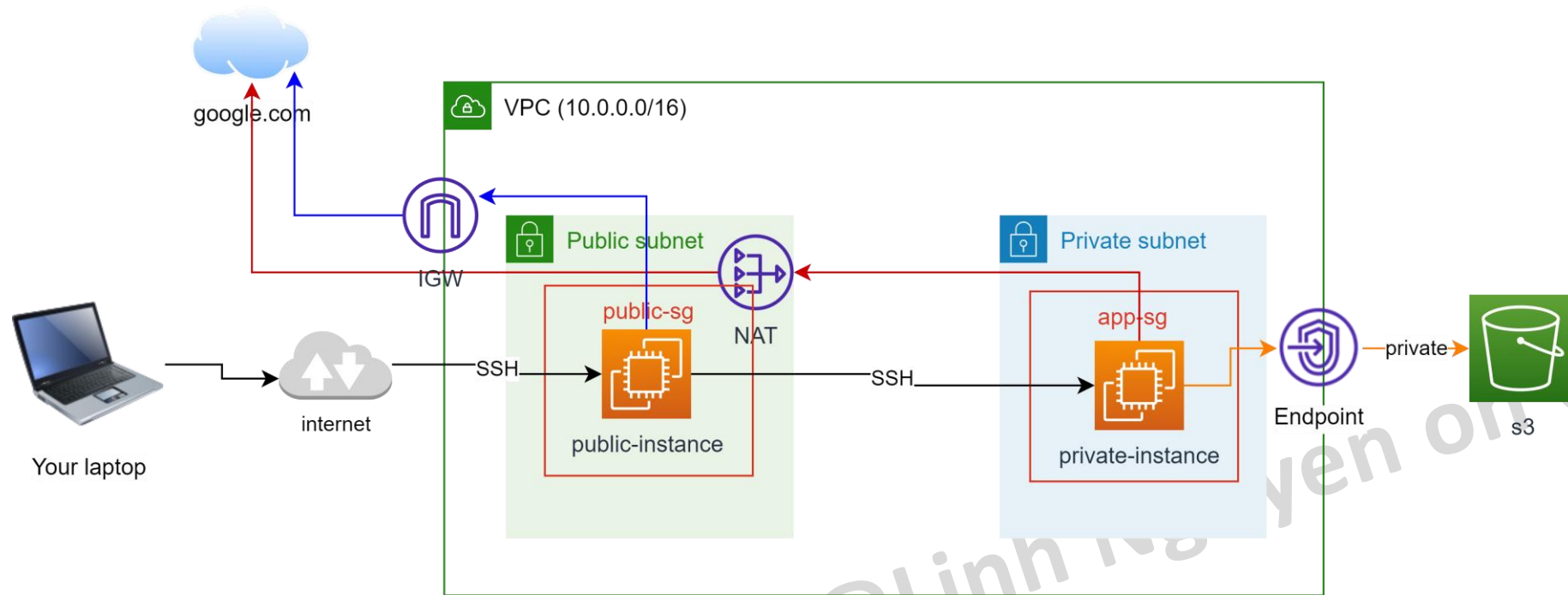
Lab 3 – Test connection trên VPC vừa tạo

Yêu cầu sử dụng lại VPC của bài lab 2

1. Tạo 1 instance trong Public subnet, gán **bastion-sg**, thử kết nối.
2. Gán Elastic IP cho Instance, thử kết nối qua Elastic IP.
3. Tạo 1 instance trong Private subnet, gán **app-sg**, thử kết nối từ bastion.
4. Ping từ private instance ra internet (vd [google.com](https://www.google.com)).
5. Thử gỡ bỏ route đi ra NAT từ private subnet, thử thao tác với S3 từ private instance để check xem S3 Endpoint có hoạt động không. **Chú ý gán Role cho EC2 instance.*

Lab 3 – Test connection trên VPC vừa tạo

*Sơ đồ cho bài lab (lưu ý sơ đồ đã loại bỏ các yếu tố Multi AZ cho đỡ rối)



- kết nối thông qua NAT
- kết nối thông qua Internet Gateway
- kết nối thông qua Endpoint

Trouble shoot lỗi connect

Khi các bạn bị lỗi không kết nối được tới EC2, có thể trouble shoot theo các step sau:

1. Check xem VPC có **Internet Gateway** chưa?
2. Check xem **Security Group** gán với instance có mở cho SSH từ ip của mình vô chưa?
3. Check xem **Route Table** gán vô subnet chứa EC2 có rule đi ra Internet Gateway chưa?
4. Check xem EC2 có **Public IP** hoặc **Elastic IP** chưa?
5. Check xem **Network ACL** gán với subnet chứa EC2 có allow cả 2 chiều Inbound/Outbound chưa?
6. Nếu check hết các issue trên vẫn OK có thể do OS treo -> **Restart EC2**.

Nhắc các bạn học viên clear resource!!! 😊

Nếu các bạn làm tới đây mà bạn chưa thể follow tiếp thì hãy xoá các resource để tránh mất phí (hôm sau tạo lại).

1. Terminate instance (nếu có)
2. Xoá VPC
3. Xoá Elastic IP (nếu còn lại)
4. Xoá NAT Gateway (nếu còn lại)
5. Xoá snapshot (nếu còn lại)
6. Xoá volume (nếu còn lại)

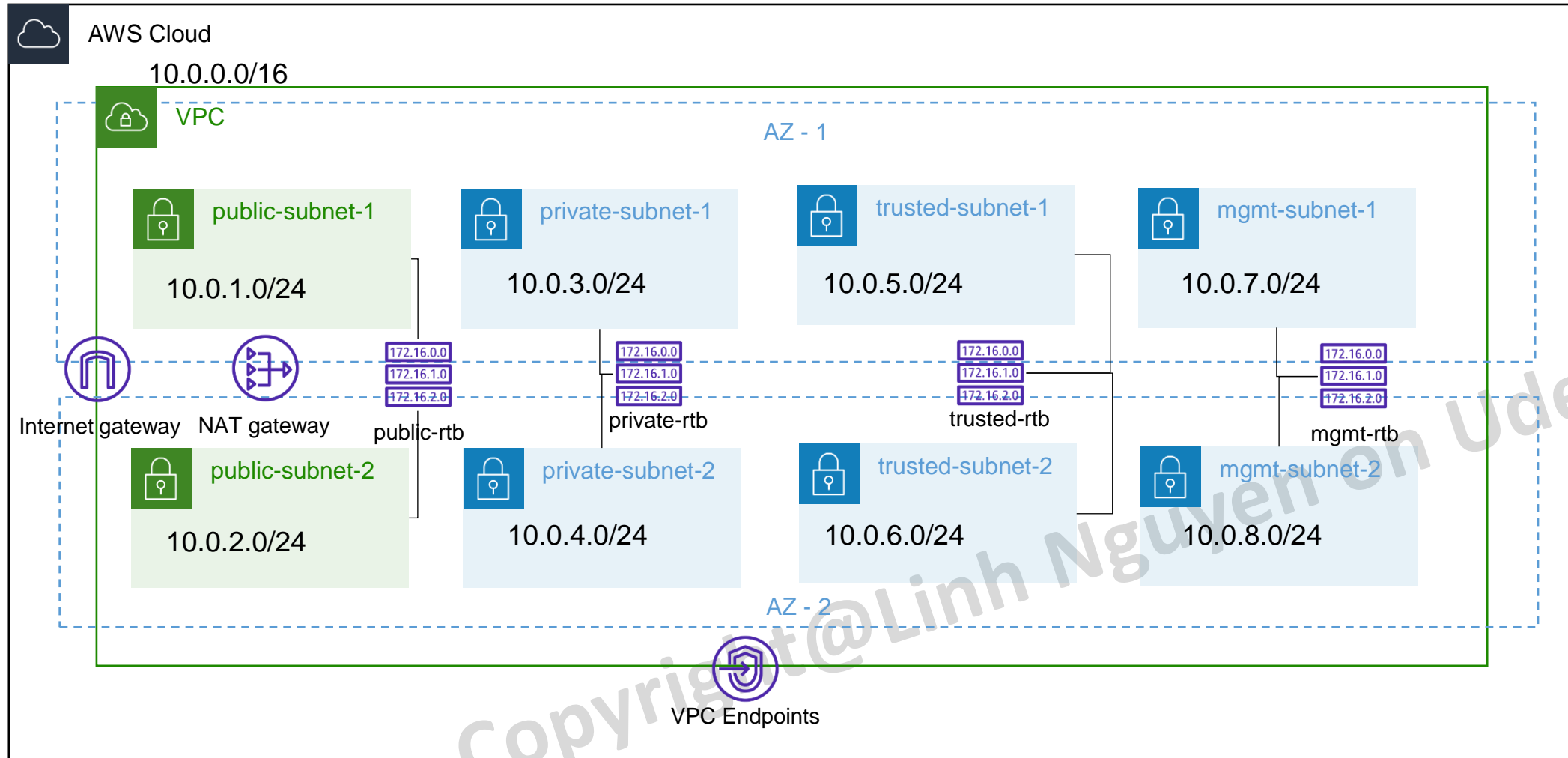
Copyright@Linh Nguyen on Udemy

Lab 2 – Bonus: Tạo VPC all-in-one-step.

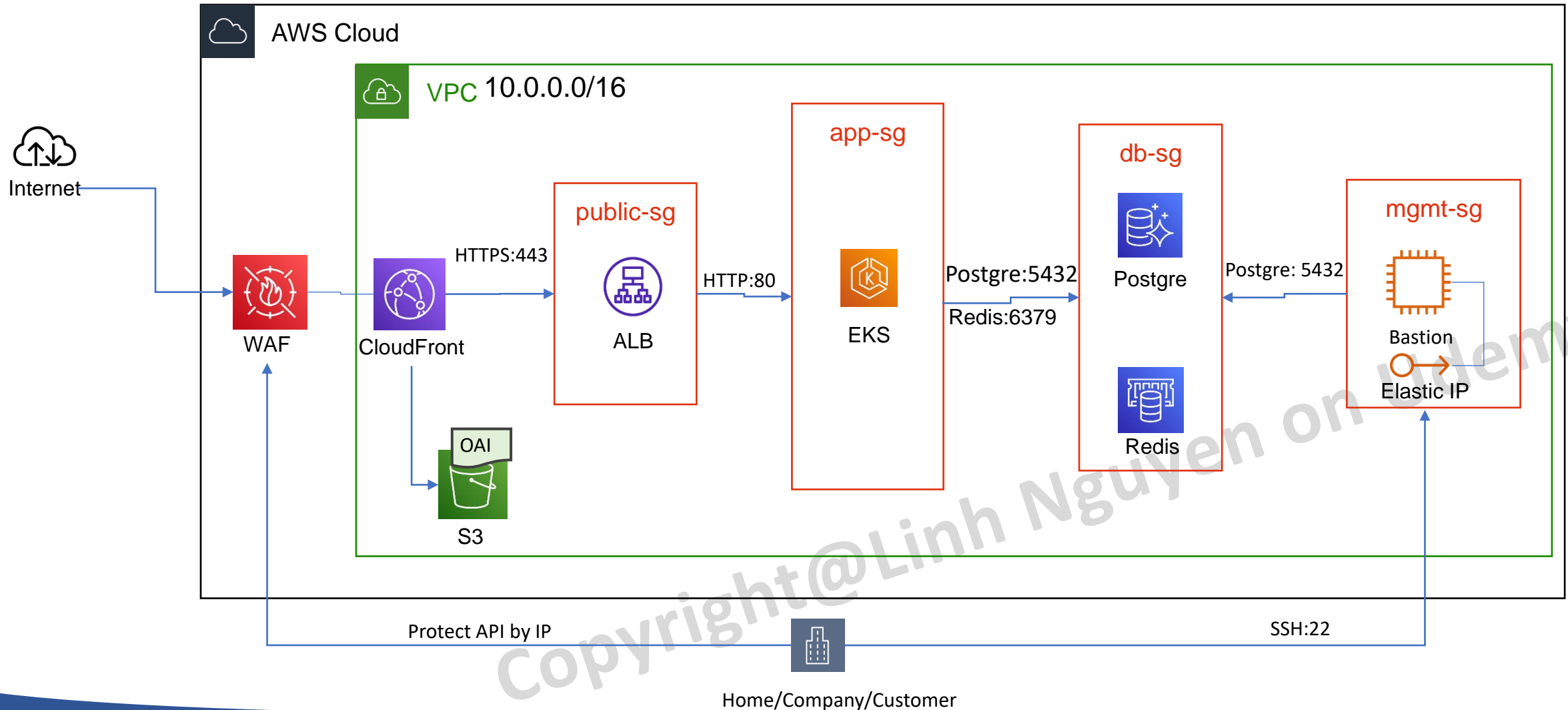
Yêu cầu:

1. Tạo VPC và các resource liên quan bằng cách sử dụng giao diện VPC mới của AWS.
2. Số lượng public subnet: 2
3. Số lượng private subnet: 4
4. Có gắn NAT, số lượng NAT: 1
5. Có gắn VPC Endpoint cho S3.
6. Riêng security group các bạn phải tự tạo (*tương tự bài lap trước nên không cần thực hiện lại*).
7. Confirm các resource được tạo ra.
8. Xoá VPC đã tạo để tránh phát sinh chi phí.

Sample VPC with 4 types of subnet



Sample Security Group setting



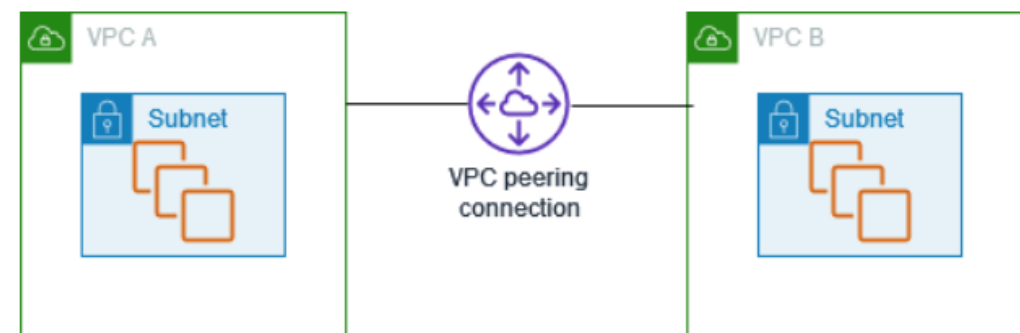
VPC Advanced section

VPC Peering

Là hình thức đơn giản nhất để kết nối 2 VPC trên AWS. 2 VPC có thể cùng account hoặc khác account.

Để thiết lập, một phía sẽ phải đưa ra peering request (requester) và bên còn lại sẽ accept request (accepter).

Sau khi đã thiết lập quan hệ peering, cần cấu hình lại **Route Table** (thêm route đi ra peering connection) và setting **Security Group** thích hợp để resource ở 2 VPC có thể connect lẫn nhau thông qua private IP (không đi ra internet).



**Lưu ý:*

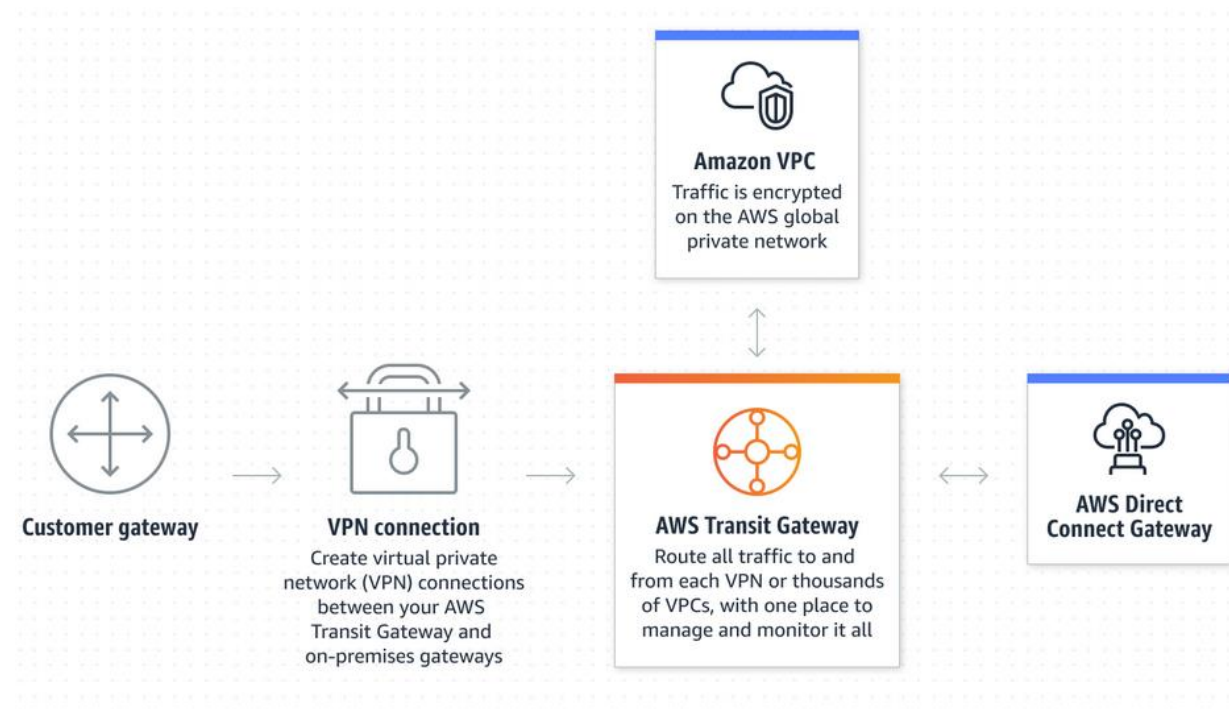
- VPC Peering không có tính chất bắc cầu. VD VPC-A peer VPC-B, VPC-B peer VPC-C không có nghĩa là VPC-A cũng peer với VPC-C.
- Hai VPC muốn peering được với nhau phải có dải IP CIDR không overlap.

VPC Advanced section

Transit Gateway

Đóng vai trò như 1 hub trung chuyển giữa On-Premise và AWS Cloud hoặc giữa nhiều VPC trên Cloud.

Thường sử dụng kết hợp với **Site-to-Site VPN** hoặc **Direct Connect**.



Nguồn: <https://aws.amazon.com/transit-gateway>

VPC Advanced section

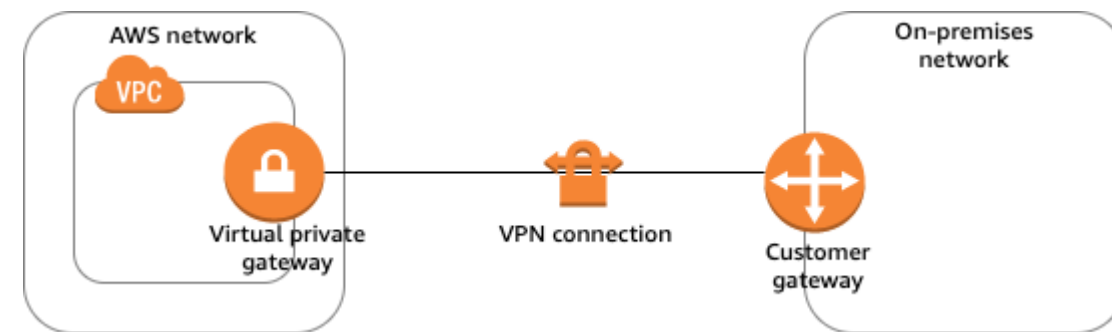
Site to Site VPN

Là hình thức kết nối network **Onpremise** với network trên **AWS Cloud**.

Customer Gateway: thiết bị vật lý hoặc virtual appliance ở phía On-Premise có nhiệm vụ điều hướng traffic.

Thông tin truyền đi giữa On-Premise và AWS Cloud được mã hoá.

Bandwidth khoảng ~4Gbps.



trường hợp 1 VPC



trường hợp nhiều VPC

Nguồn: https://docs.aws.amazon.com/vpn/latest/s2svpn/how_it_works.html

VPC Advanced section

Direct Connect

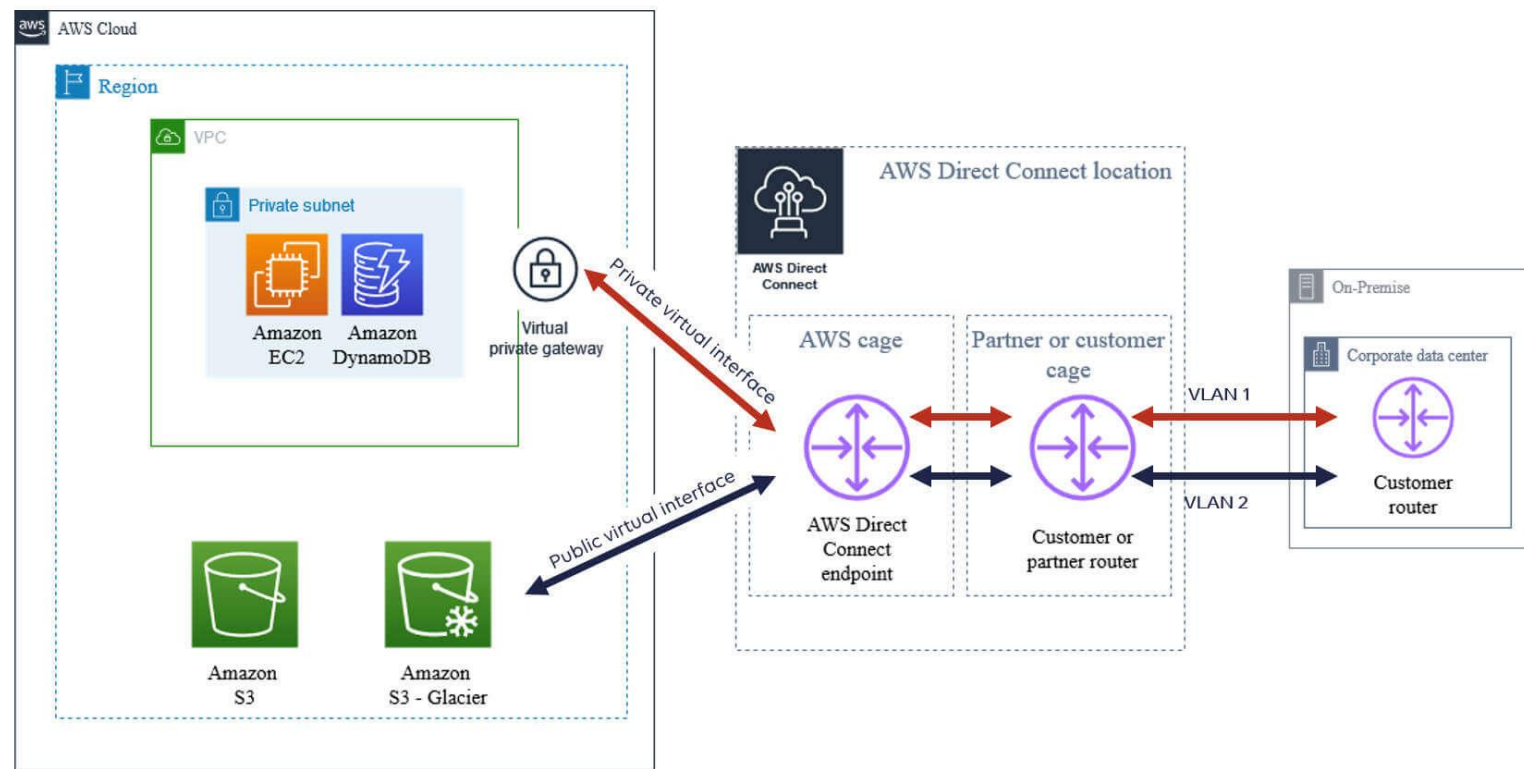
Hình thức kết nối từ On-Premise lên AWS Cloud thông qua một kênh connect low latency, high speed.

Connection được duy trì thông qua một đường truyền chuyên dụng không qua public internet.

Thông tin truyền đi giữa On-Premise và AWS Cloud **không** được mã hoá by default.

Bandwidth dao động từ 50Mbps-100Gbps.

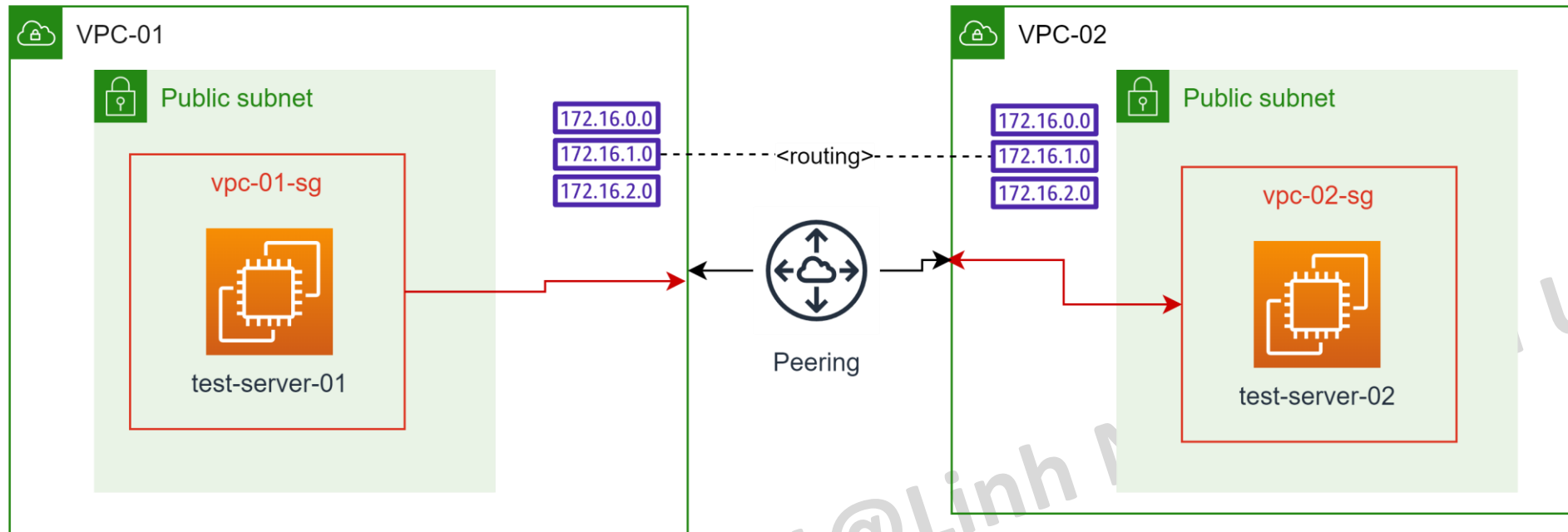
Khó setup hơn so với VPN, cần làm việc với nhà cung cấp Direct Connect.



Source: <https://www.stormit.cloud/blog/comparison-aws-direct-connect-vs-vpn/>

Lab 4 – VPC Peering

Yêu cầu: Thực hành VPC Peering.



Lab 3 – VPC Peering

Steps:

1. Tạo nhanh 2 VPC có CIDR không overlap (vd 10.0.0.0/16 và 10.1.0.0/16). Không cần tạo Nat Gateway. Mỗi VPC có 2 subnet public. **hai VPC có thể khác account.*
2. Tạo 2 security group đơn giản vd: vpc-01-sg, vpc-02-sg
3. Tạo và accept VPC Peering cho 2 VPC.
4. Modify route table cho cả 2 VPC để nhận biết CIDR của nhau.
5. Modify security group của VPC-02, allow traffic từ CIDR của VPC-01
6. Tạo 2 EC2 instance nằm trong 2 VPCs, thử ping từ Instance trong VPC-01 sang instance trong VPC-02 bằng private IP.
7. Clear các resource đã tạo để tránh phát sinh chi phí.

Tổng kết

1. Hiểu rõ VPC là gì và các concept liên quan VPC.
2. Biết cách thiết kế một VPC đúng chuẩn.
3. Biết cách tạo một VPC theo thiết kế, setting Security Group.
4. Biết cách trouble shoot nếu gặp sự cố network.
5. Làm quen với VPC Peering
6. Tìm hiểu Transit gateway, Site to Site VPN, Direct Connect ở mức độ cơ bản.

Copyright@Linh Nguyen on Udemy

Clear resources

1. Login to AWS console
2. Terminate instances (nếu có)
3. Xoá VPC
4. Xoá Elastic IP (nếu còn lại)
5. Xoá NAT Gateway (nếu còn lại)
6. Xoá snapshot (nếu còn lại)
7. Xoá volume (nếu còn lại)

Copyright@Linh Nguyen on Udemy