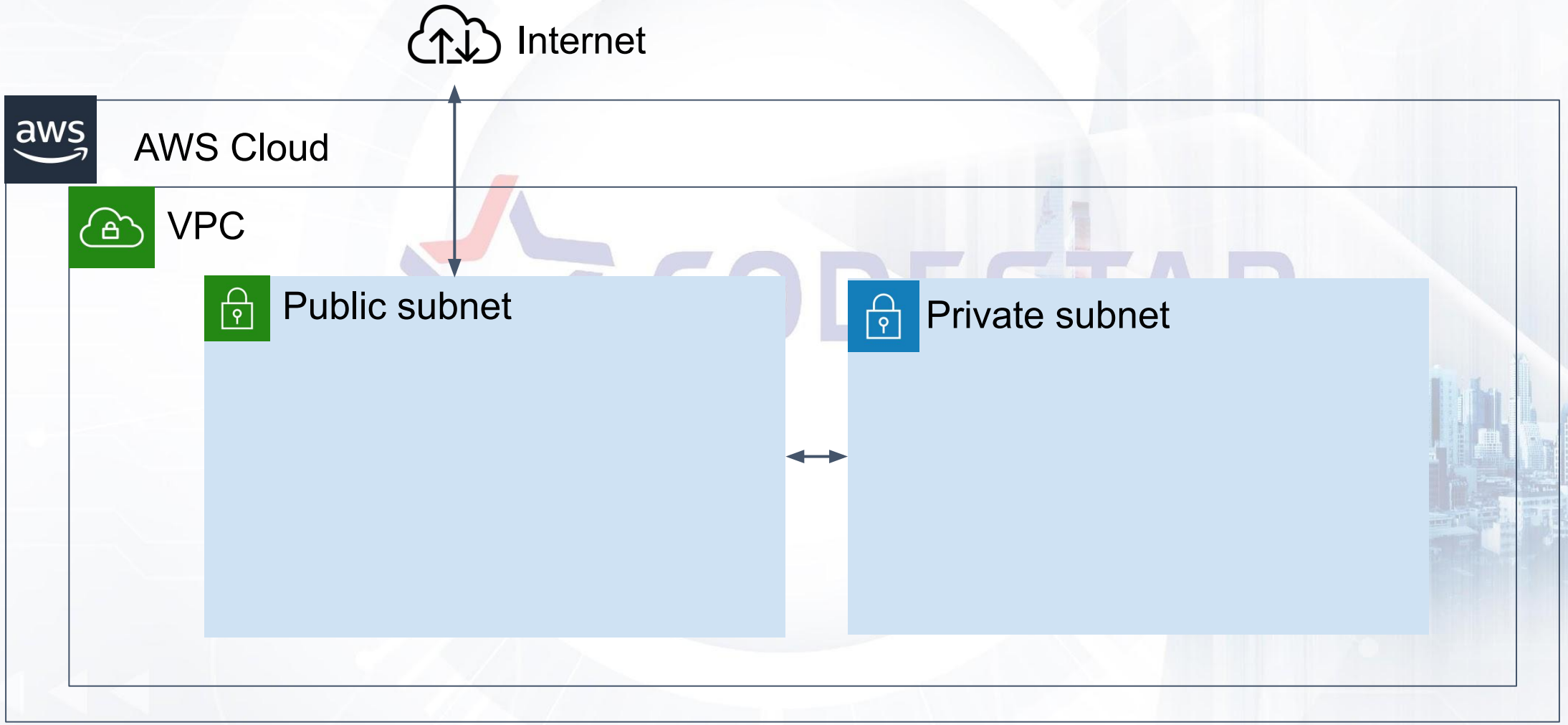
Networking

CodeStar Academy

Nội dung chính

- Các thành phần trên VPC
- Các phương án kết nối nhiều mạng VPC

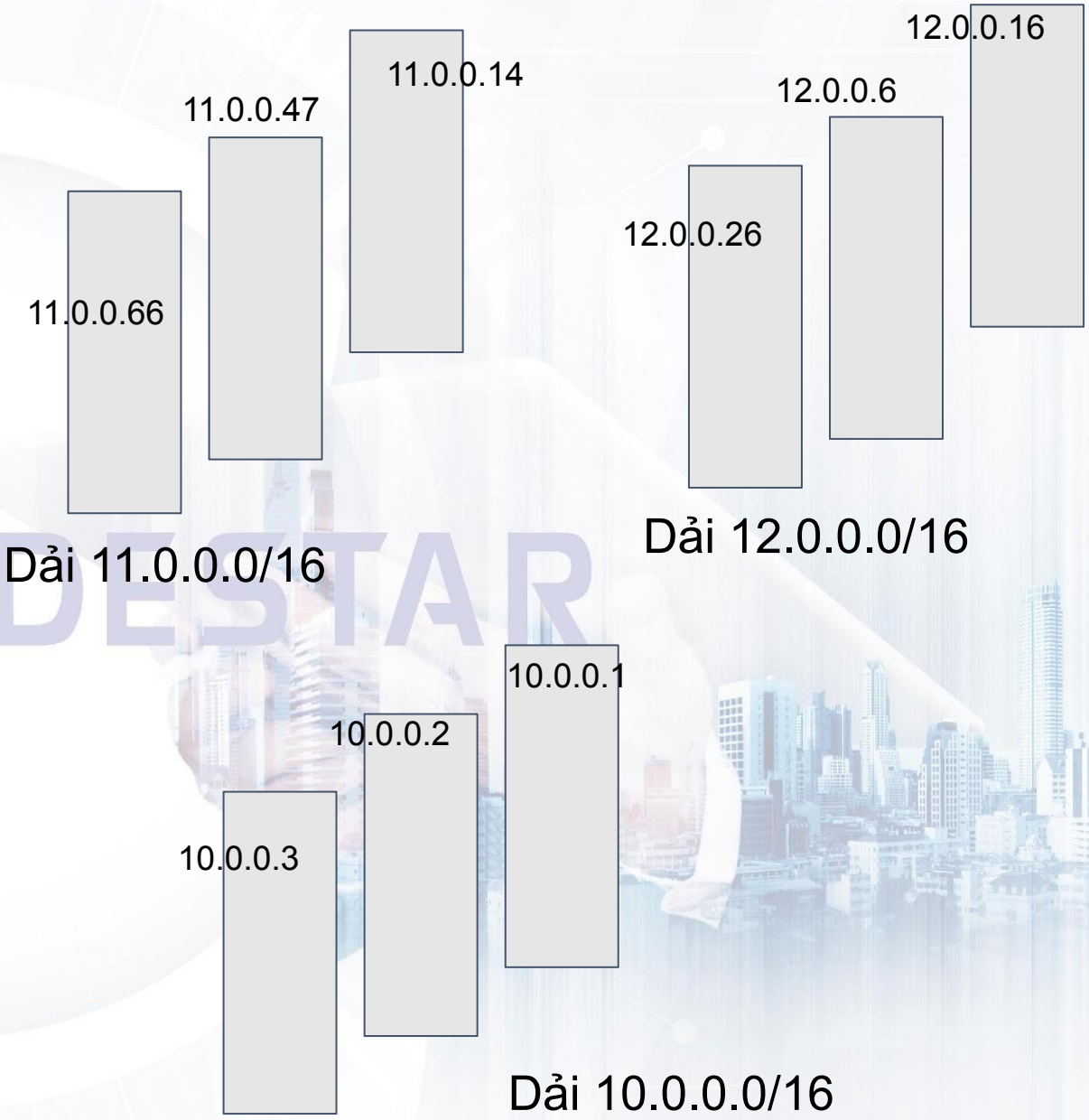
VPC



VPC

VPC là không gian lưu trữ và định vị các thành phần trong một network.

Các vị trí của các thành phần trên network được định danh bằng các địa chỉ được gọi là địa chỉ IP.



CIDR Block

IPv4

10 . 1 . 2 . 3

IPv6

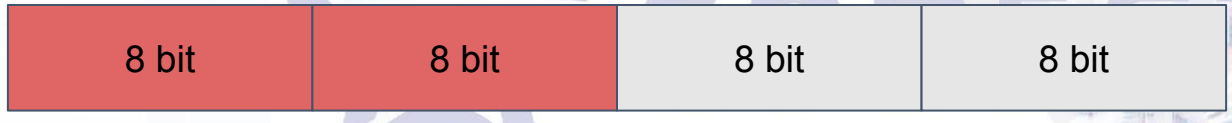
100D : ABCD : 000A : 111B : C000 : DAF4 : 0123 : 1234

CIDR Block

IPv4

10 . 1 . 2 . 3

CIDR Block



10 . 1 . 0 . 0 /16

10 . 1 . 2 . 3

10 . 1 . 20 . 34

Địa chỉ Số 607 tầng 5 tòa HSDC

?? tầng 5 tòa HSDC

Số 607 tầng 5 tòa HSDC

Số 312 tầng 5 tòa HSDC

CIDR Block

IPv4

10 . 1 . 2 . 3

CIDR Block

10 . 1 . 160 . 0 /19

10 . 1 . 162 . 3

10 . 1 . 190 . 34

~~10 . 1 . 220 . 89~~

Địa chỉ Số 607
tầng 5 tòa HSDC

số 160-191 tầng 5 tòa HSDC

Số 162 tầng 5 tòa HSDC

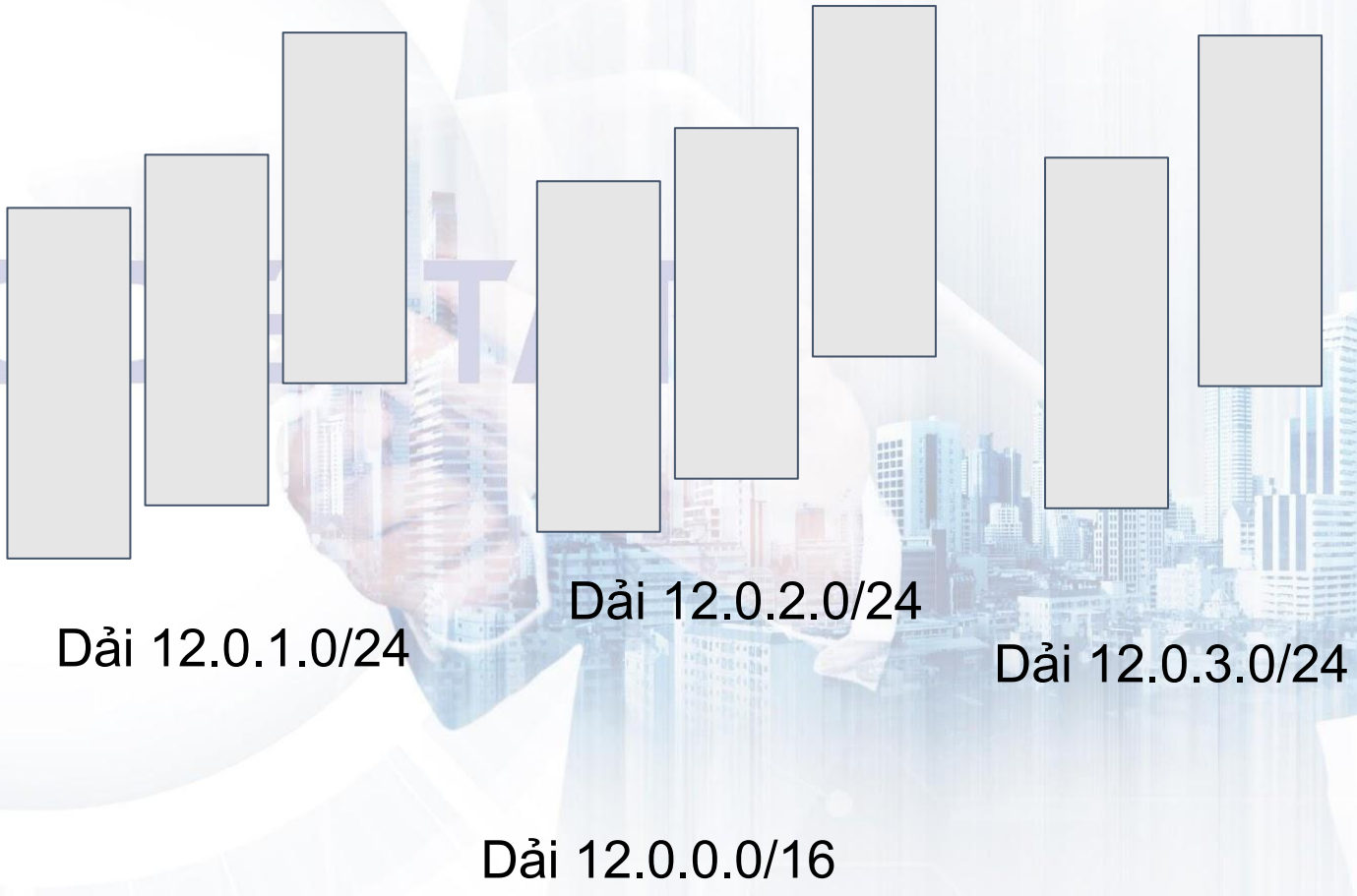
Số 190 tầng 5 tòa HSDC

Số 220 tầng 5 tòa HSDC
(không thuộc CIDR block này)

Subnet

Subnet là một network con, nằm trong phạm vi của Network, được chia nhỏ ra để dễ quản lý.

Tất cả các IP nằm trong các dải CIDR của subnet đều thỏa mãn dải CIDR của VPC.



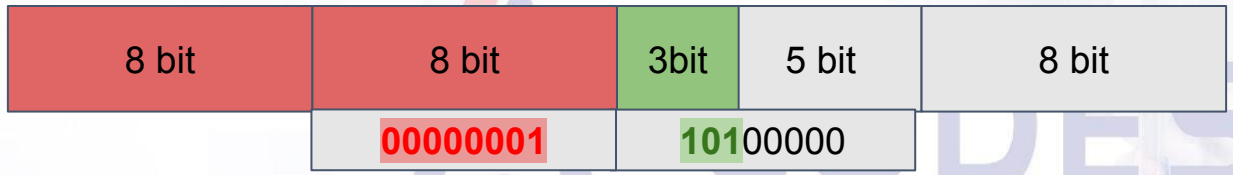
Subnet: CIDR Block

chung cư HSDC

IPv4

10 . 1 . 2 . 3

CIDR



Block

10 . 1 . 160 . 0 /19

10 . 1 . 162 . 3

10 . 1 . 190 . 34

~~10 . 1 . 220 . 89~~

Tòa 101 chung cư HSDC

Số 162 tòa 101 chung cư HSDC

Số 190 tòa 101 chung cư HSDC

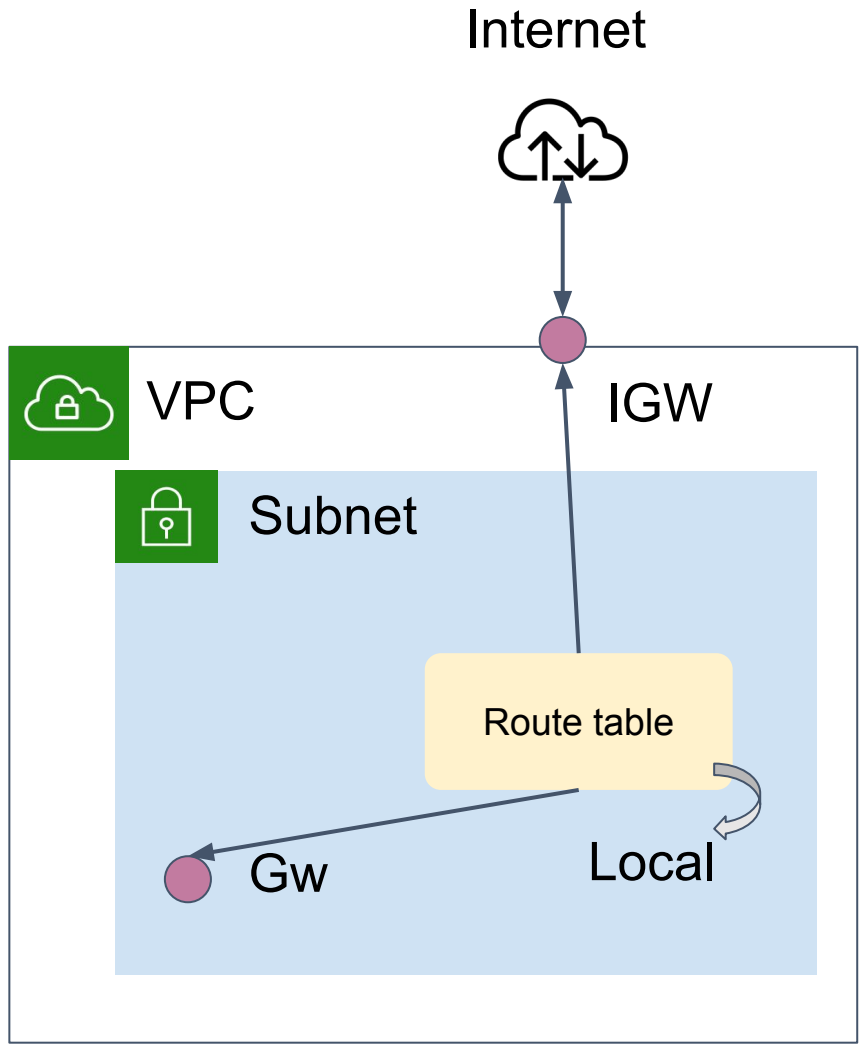
Số 220 tòa 110 chung cư HSDC
(không thuộc CIDR của subnet,
nhưng thuộc CIDR của VPC này)

Subnet: Route table

Route table : tập hợp các routes xác định traffic từ subnet hoặc gateway được chuyển đến đâu, cổng nào, và được liên kết với subnet.

Route table hoạt động giống như thiết bị Router trong network

Destination	Target
10.0.1.0/24	local
10.0.2.0/24	gw-...
0.0.0.0/0	igw

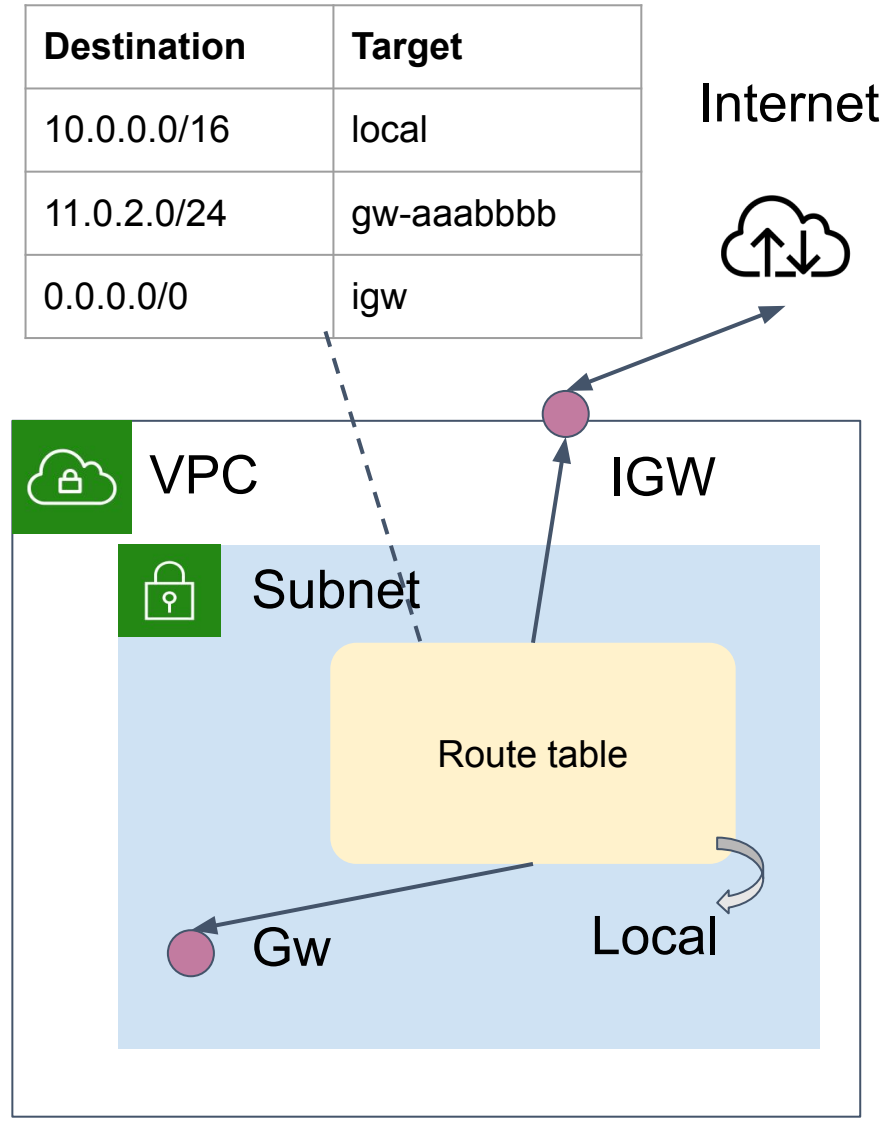


Subnet: Route table

Tại hình bên dưới, route table chỉ rõ cho chúng ta

- Nếu muốn đi tới các địa chỉ IP 11.0.2.X => đi tới gateway gw-aaabbbb
- Đi tới các địa chỉ 10.0.X.Y => đi tới local (trong VPC hiện tại)
- Đi tới các địa chỉ khác => đi tới IGW.

Lưu ý: Thứ tự trỏ sẽ ưu tiên dải địa chỉ nào chi tiết hơn (có phần / m phía sau là lớn nhất)



Subnet: Private & Public

Private Subnet

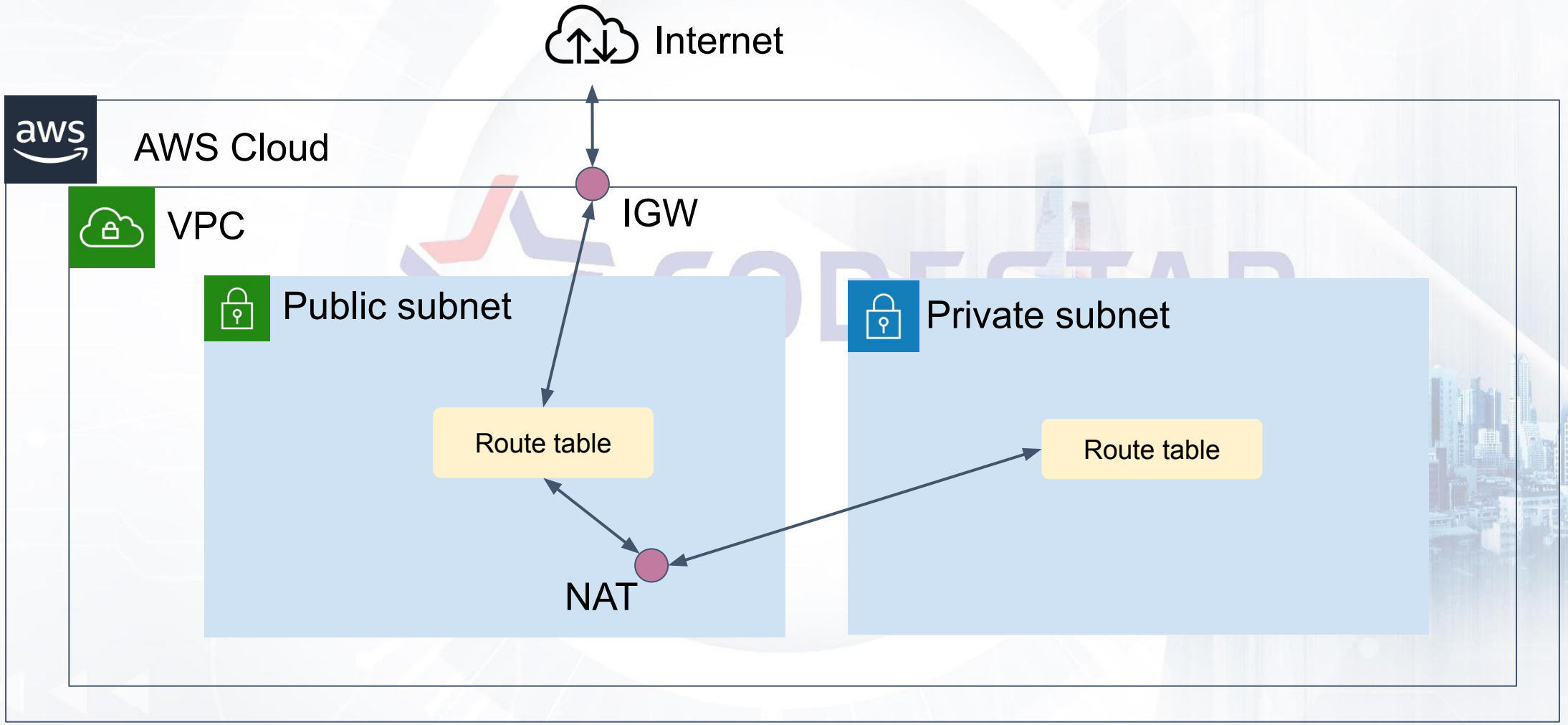
Là subnet không kết nối trực tiếp ra ngoài internet (không có Route table trỏ tới Internet GW)

Để Request đi được ra ngoài Internet, cần mượn IP của thiết bị NAT nằm trong public subnet.

Public Subnet

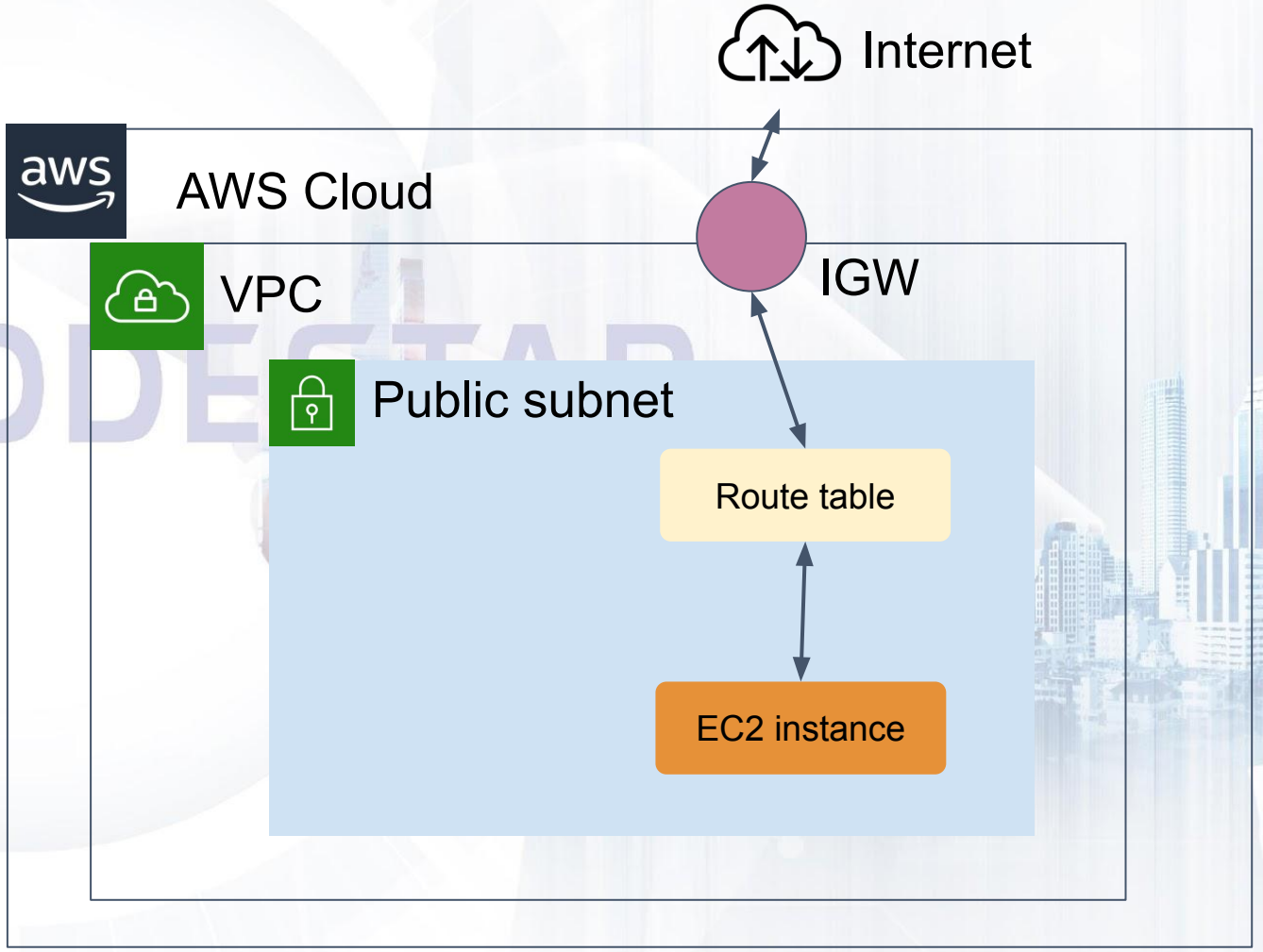
Là subnet có kết nối trực tiếp ra ngoài internet (có Route table trỏ tới Internet GW).

Subnet: Private & Public



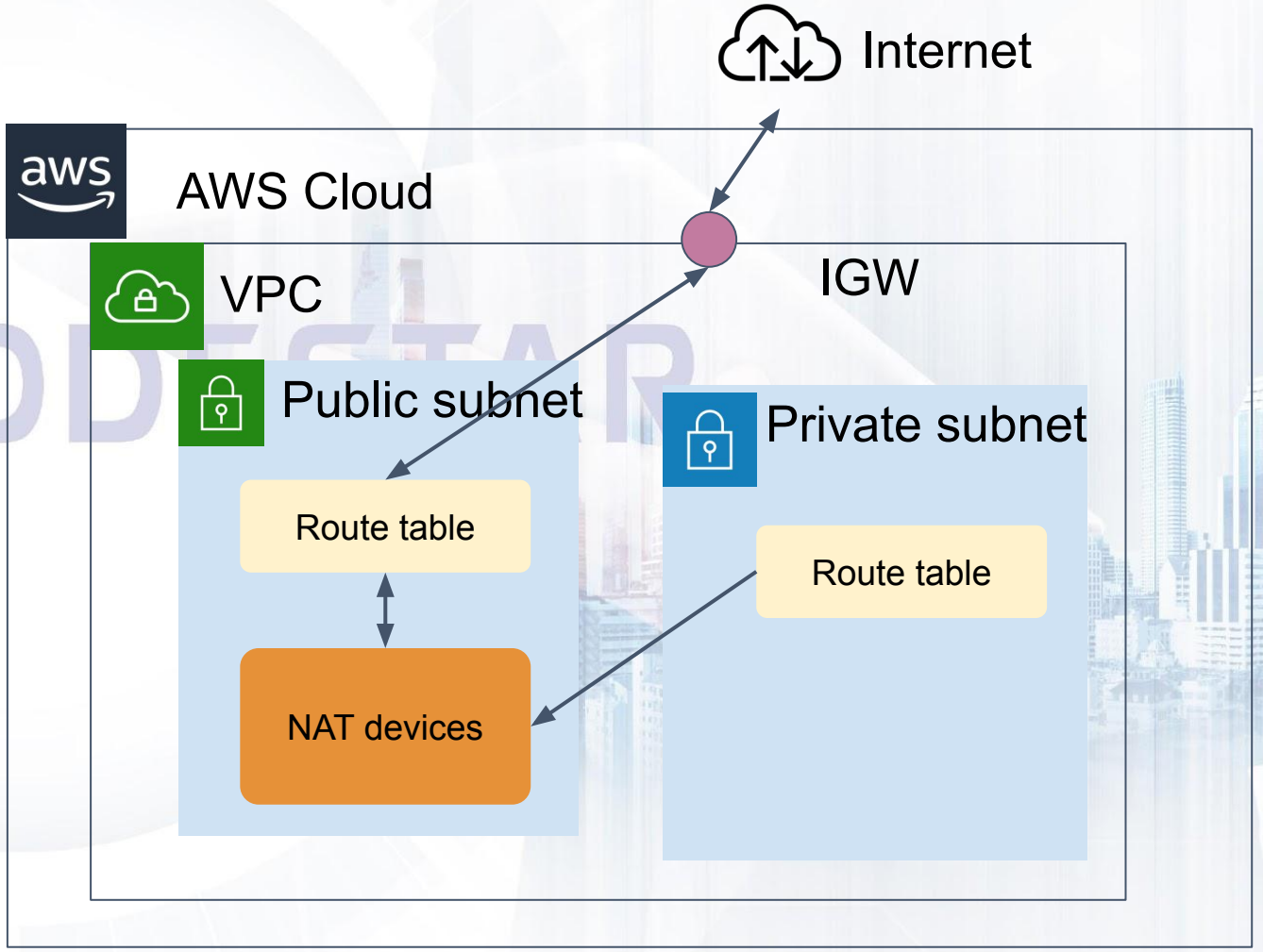
Subnet: Internet Gateway

- Internet GW là cổng kết nối đưa network của một hệ thống kết nối ra Internet.
- Để sử dụng IGW, dùng Route table của subnet đưa request tới IGW
- Subnet có sử dụng Route table mà có Route tới IGW được gọi là public subnet



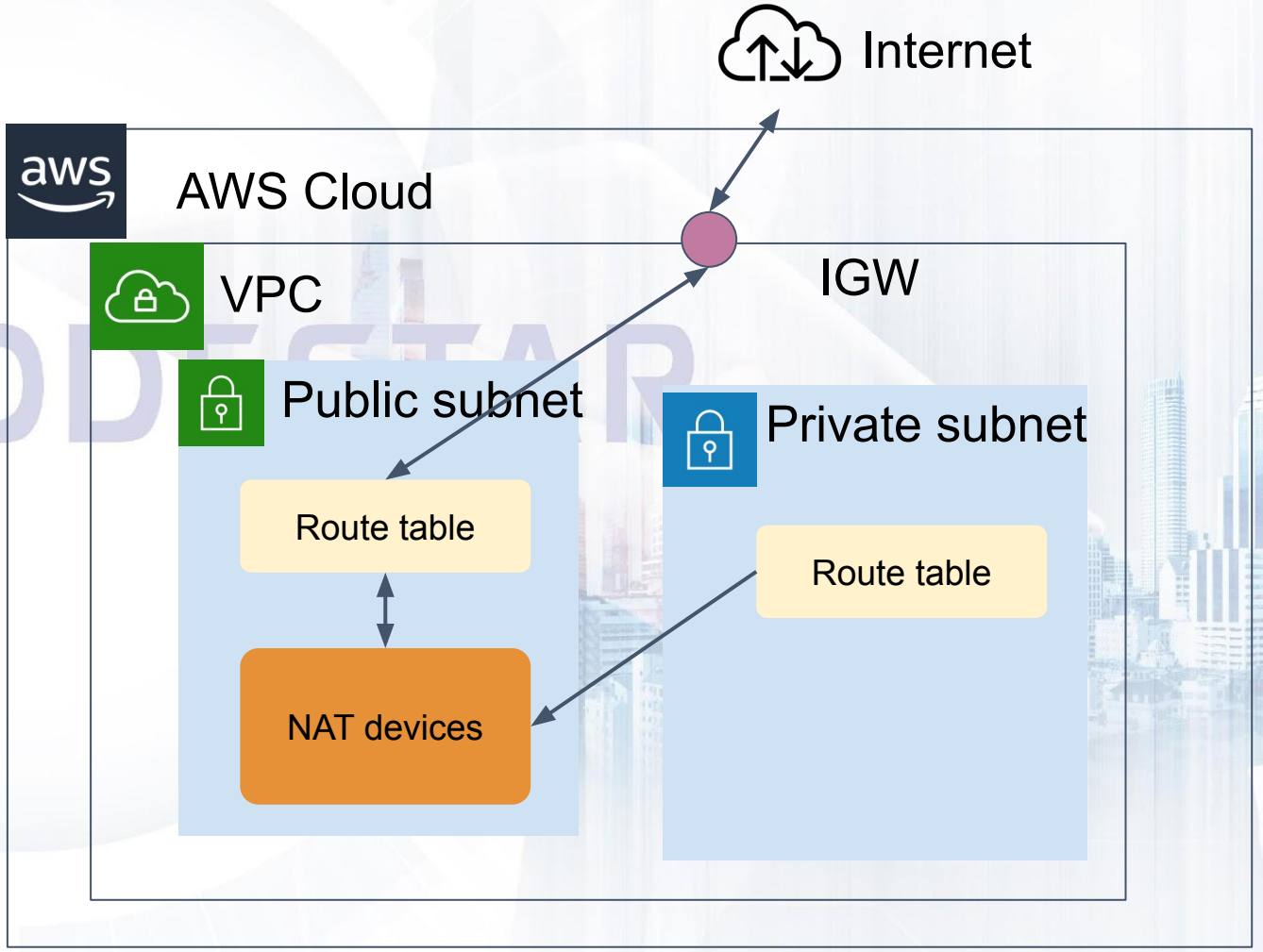
Subnet: NAT Devices

- NAT Device là thiết bị nằm trong một Public Subnet, với nhiệm vụ, cho phép các request trỏ tới nó có thể sử dụng dưới danh nghĩa là NAT devices.
- NAT devices cho phép các thành phần trong private subnet có thể đi ra ngoài internet (1 chiều chỉ đi ra)
- NAT Devices chỉ sử dụng cho IPv4



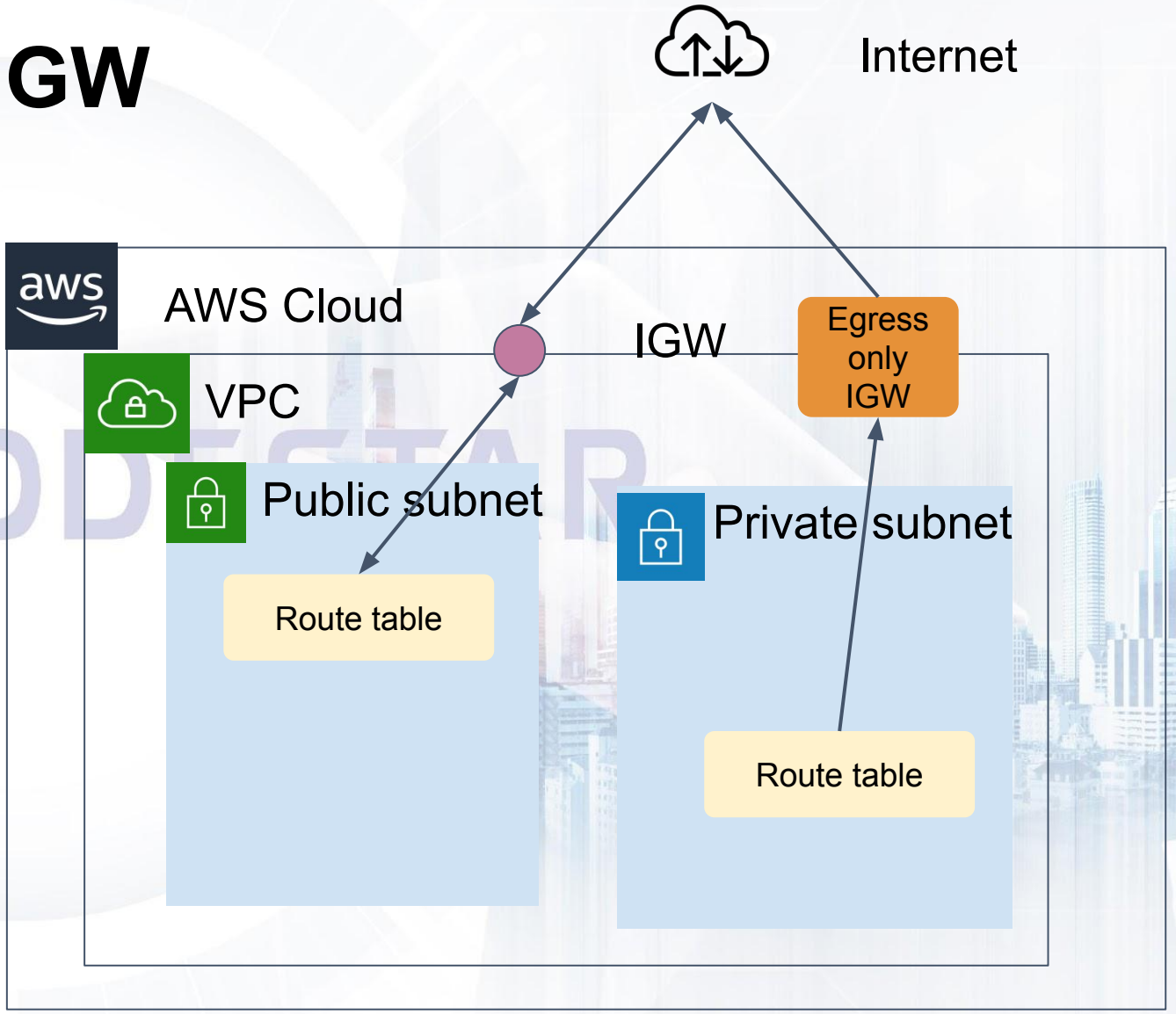
Subnet: NAT Devices

- **NAT Devices** trên AWS có 2 loại:
- **NAT Gateway** (một thành phần managed services của AWS, thực hiện công việc của 1 NAT Device)
- **NAT Instance** là một EC2 instance, được thiết lập để cho phép các request đi qua nó.



Subnet: Egress only IGW

- Đối với hệ thống sử dụng IPv6, NAT Devices sẽ không được sử dụng mà thay vào đó, chúng ta sử dụng **Egress-only Internet Gateway**



Subnet: Network ACL & Security Groups

- NACL firewall kiểm soát traffic vào/ra subnet
- Rule trong NACL xử lý theo thứ tự ưu tiên và Rule cos priority thấp nhất sẽ được xử lý trước.
- AWS khuyến nghị đánh số Rule tăng dần từ 100
- Mặc định rule cuối cùng là Deny anything
- Ví dụ:
  - Rule 100 cho phép ping từ IP 192.168.1.1/32,
  - Rule 200 chặn ping từ IP 192.168.1.1/32

Inbound Rules

Rule #	Type	Protocol	Port Range	Source	Allow/Deny
100	All IPv4 Traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 Traffic	All	All	0.0.0.0/0	DENY

Outbound Rules

Rule #	Type	Protocol	Port Range	Destination	Allow/Deny
100	All IPv4 Traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 Traffic	All	All	0.0.0.0/0	DENY

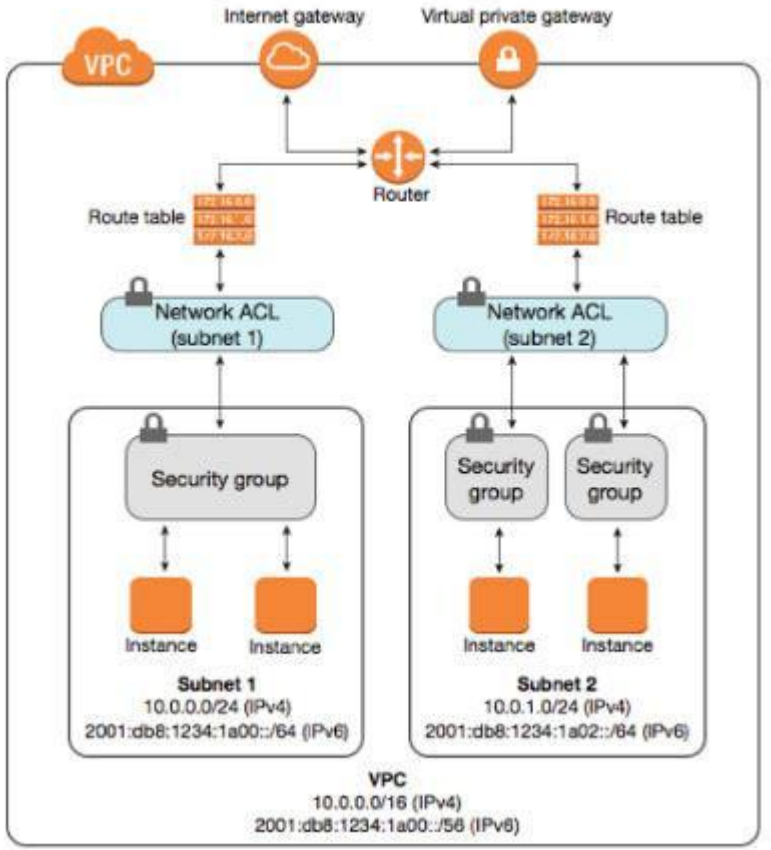
=> NACL sẽ xét Rule 100 và cho phép ping nếu có IP match với IP khai báo trong Rule

Subnet: Network ACL & Security Groups

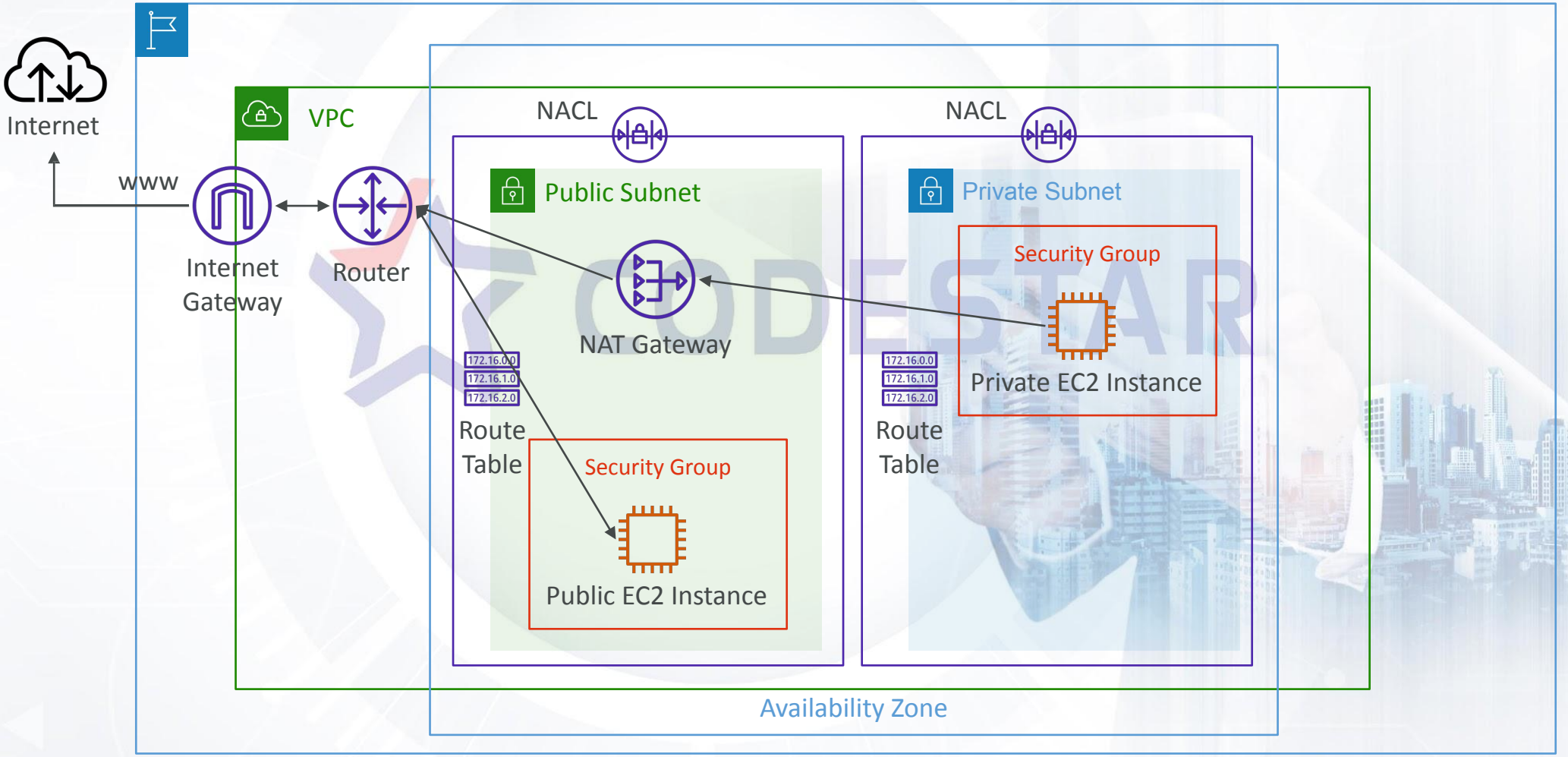
Trong một mạng network, thì Network ACL (NACLs) sẽ được kiểm tra trước, Security Group sẽ được kiểm tra sau.

NACL là **Stateless**, do vậy khi request đi ra đi vào cần kiểm tra độc lập 2 phía Inbound và Outbound.

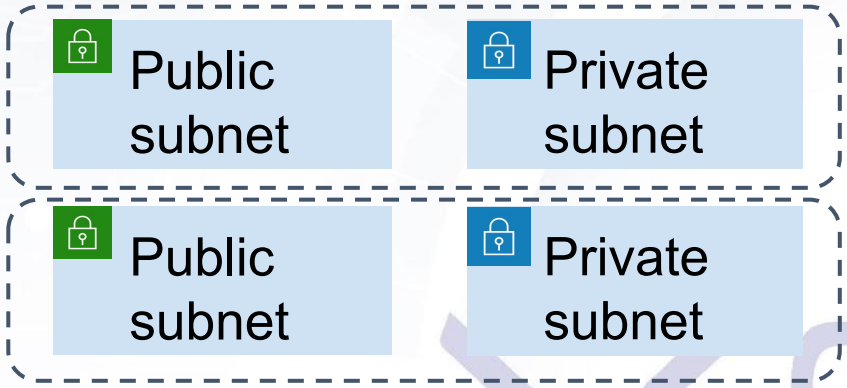
Security Group là **Stateful**, do vậy, khi request được phép đi vào khai báo Inbound thì response cho request đó mặc định được phép đi ra mà không cần khai báo trong outbound



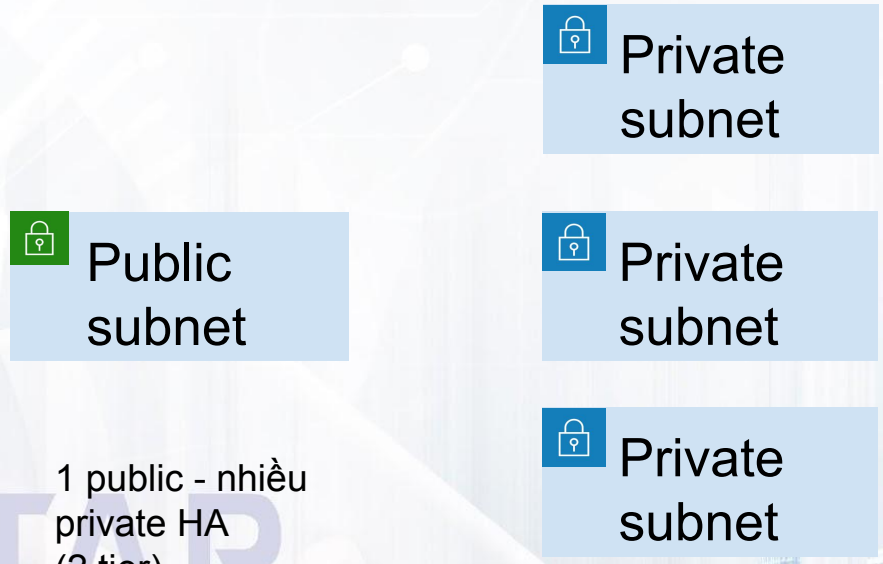
Subnet: Network ACL & Security Groups



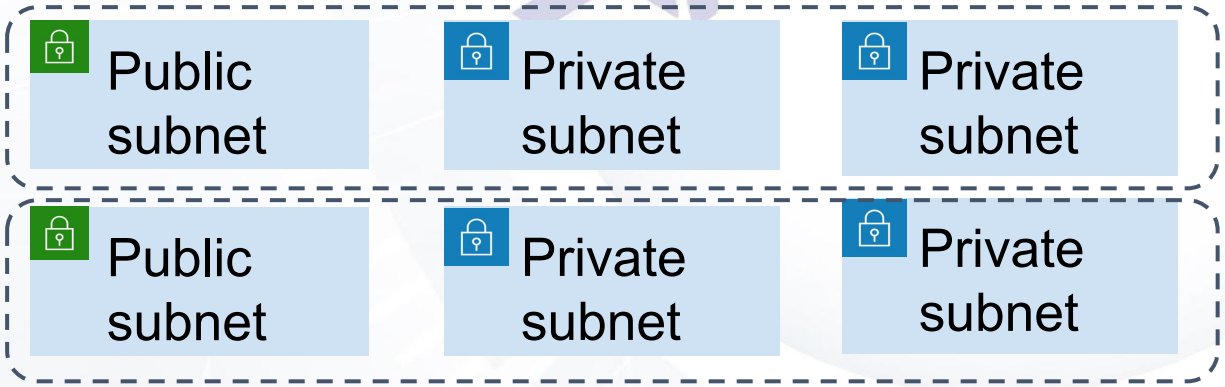
Subnet: Một số mô hình



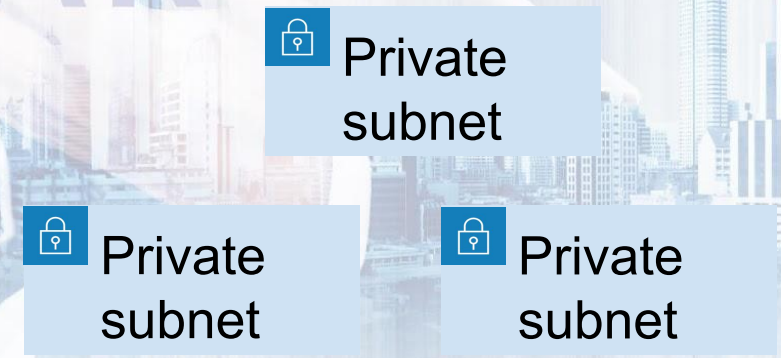
Public/private trên các AZ khác nhau



1 public - nhiều private HA (2 tier)



Mô hình 3 cấp (3 tier) 1 layer ingress, 1 layer workload private, 1 layer database

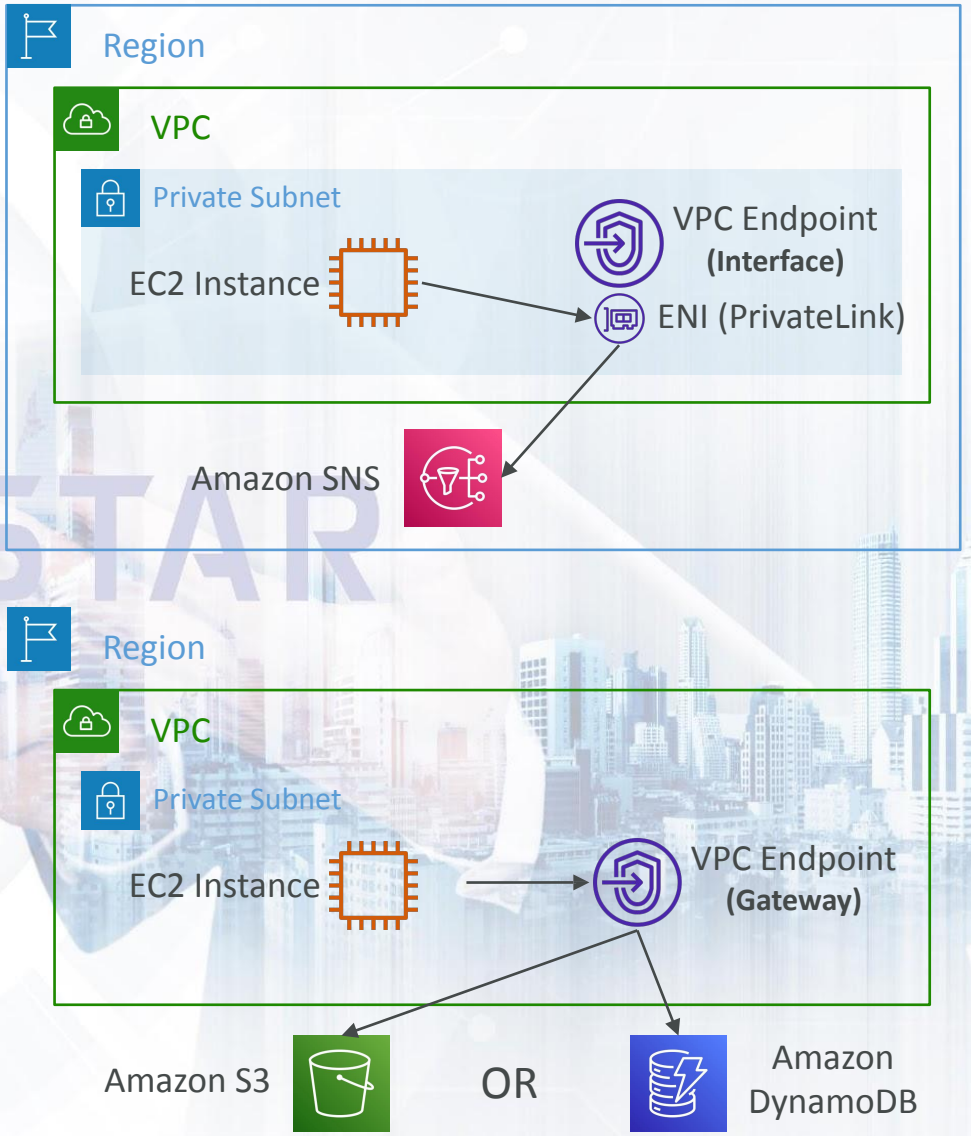


Mô hình hoạt động nội bộ, chỉ có private subnet

VPC Endpoints

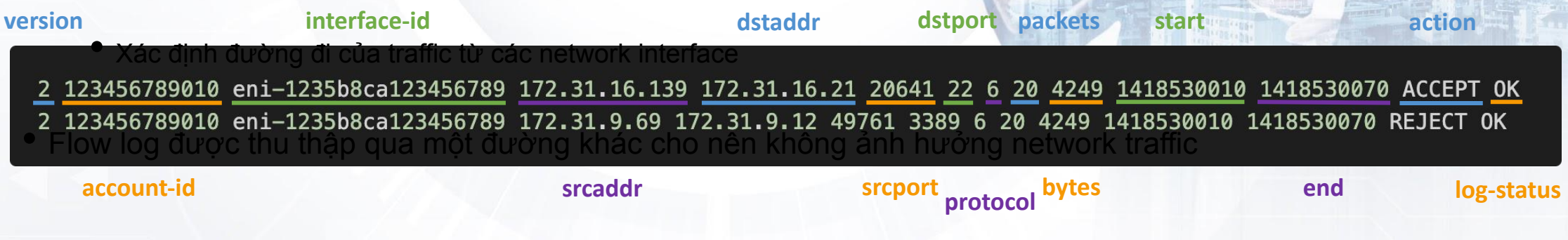
Có 2 loại VPC Endpoints

- **Interface Endpoints (PrivateLink)**: cần triển khai một ENI và IP private để kết nối các service như CloudWatch, SNS… Tính phí theo giờ và lượng data xử lý
- **Gateway Endpoints**: dùng để kết nối S3 và DynamoDB và miễn phí

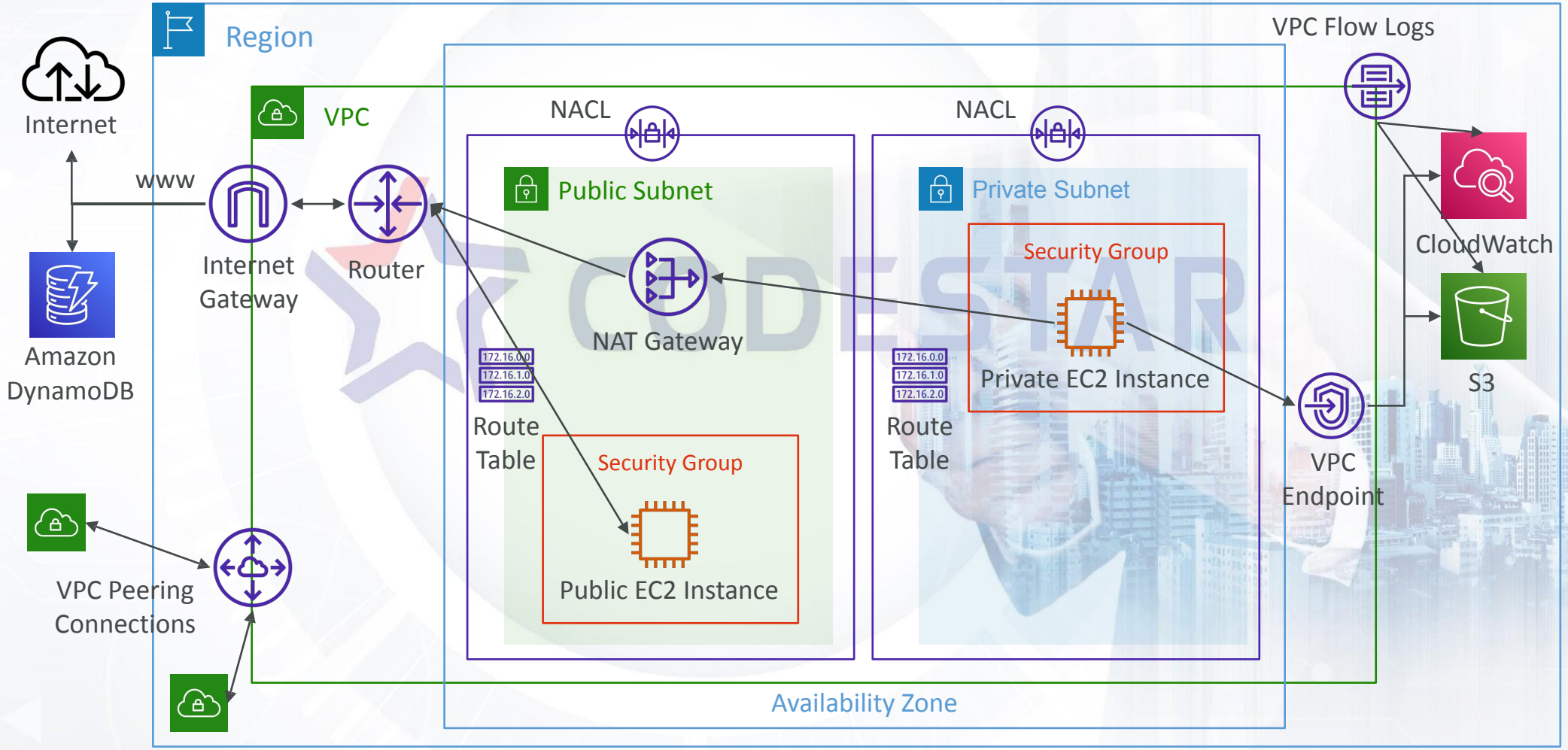


VPC Flow Logs

- VPC Flow Logs giúp capture log toàn bộ traffic đi ra/vào từ các network interface trong VPC
- Log được gửi đến CloudWatch Logs hoặc S3
- Có thể query VPC Flow Logs bằng Athena hoặc dùng CloudWatch Logs Insight
- VPC Flow Log thường dùng trong các trường hợp:
  - Giám sát traffic vào các EC2, RDS
  - Kiểm tra hoạt động của Security Groups
  - Xác định đường đi của traffic từ các network interface
- Flow log được thu thập qua một đường khác cho nên không ảnh hưởng network traffic

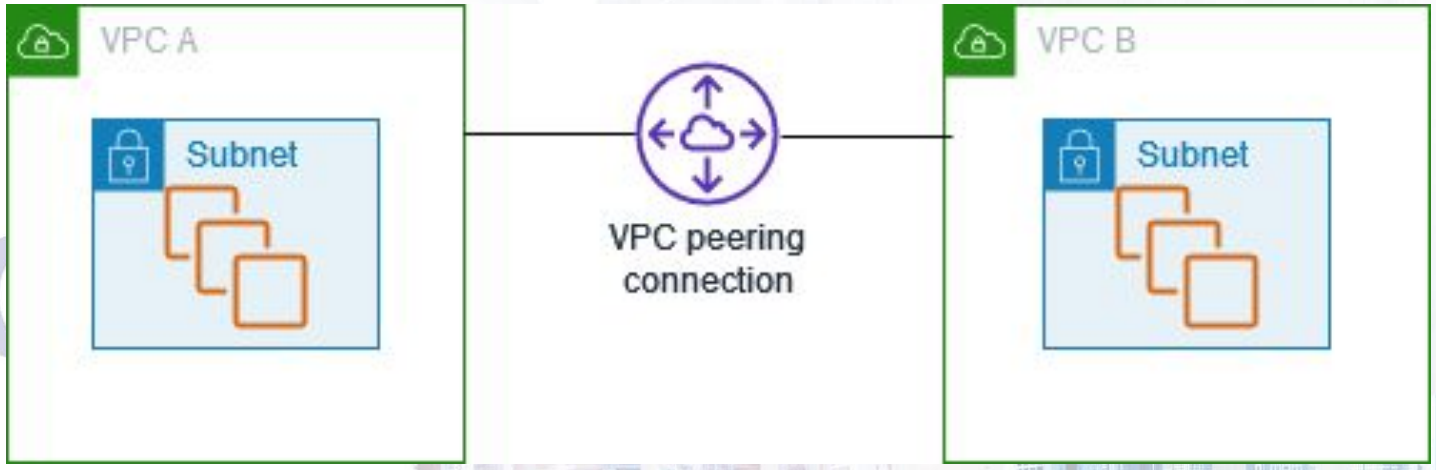


VPC Flow Logs



VPC Peering

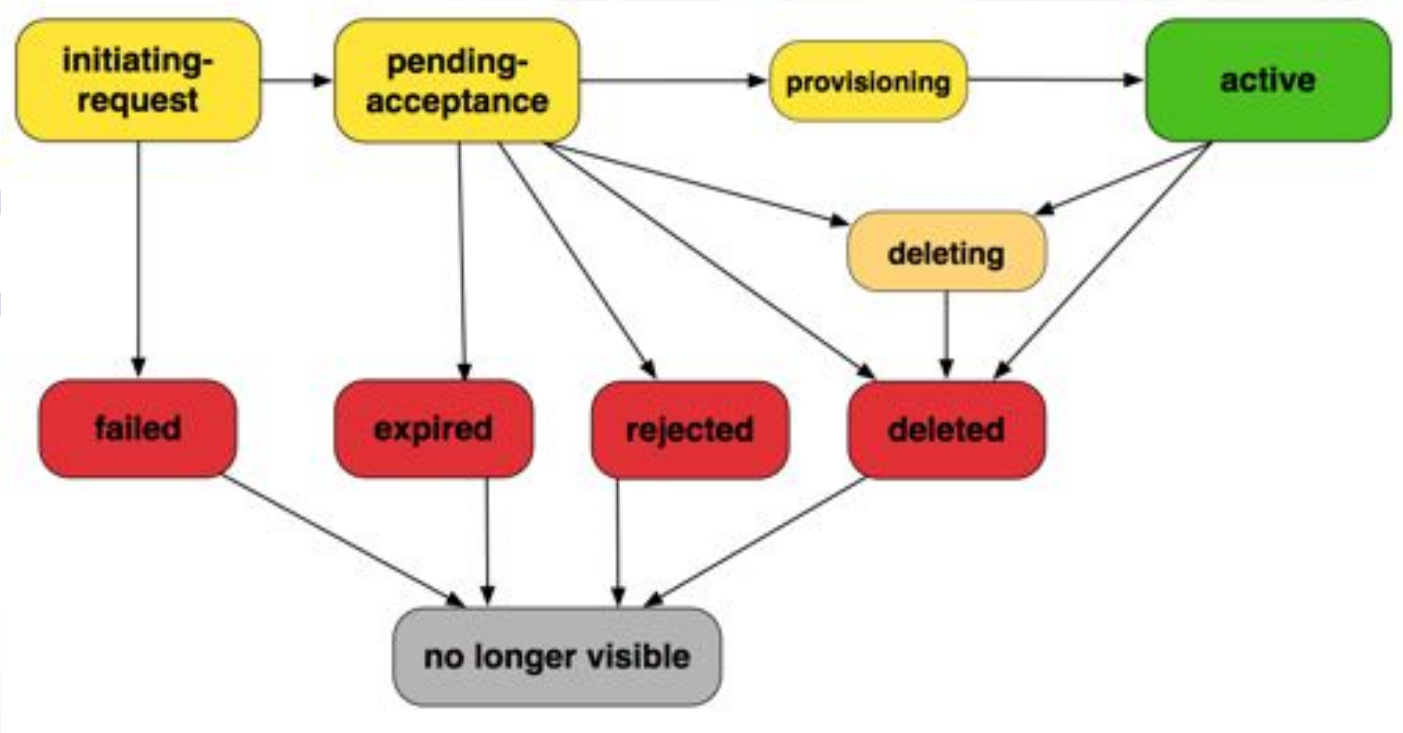
- Do VPC bị giới hạn trong chỉ 1 Account và 1 Region. Do vậy khi cần Connect nhiều Account, nhiều Region, hoặc nhiều hệ thống, chúng ta sẽ cần Connect các VPC với nhau.



- VPC Peering là phương pháp đơn giản nhất kết nối 2 VPC hoặc 1 số ít VPC với nhau.
- 2 VPC kết nối Peering với nhau không được phép trùng dải địa chỉ CIDR
- VPC Peering hiện không tính phí, chỉ tính phí Data Transfer.

VPC Peering

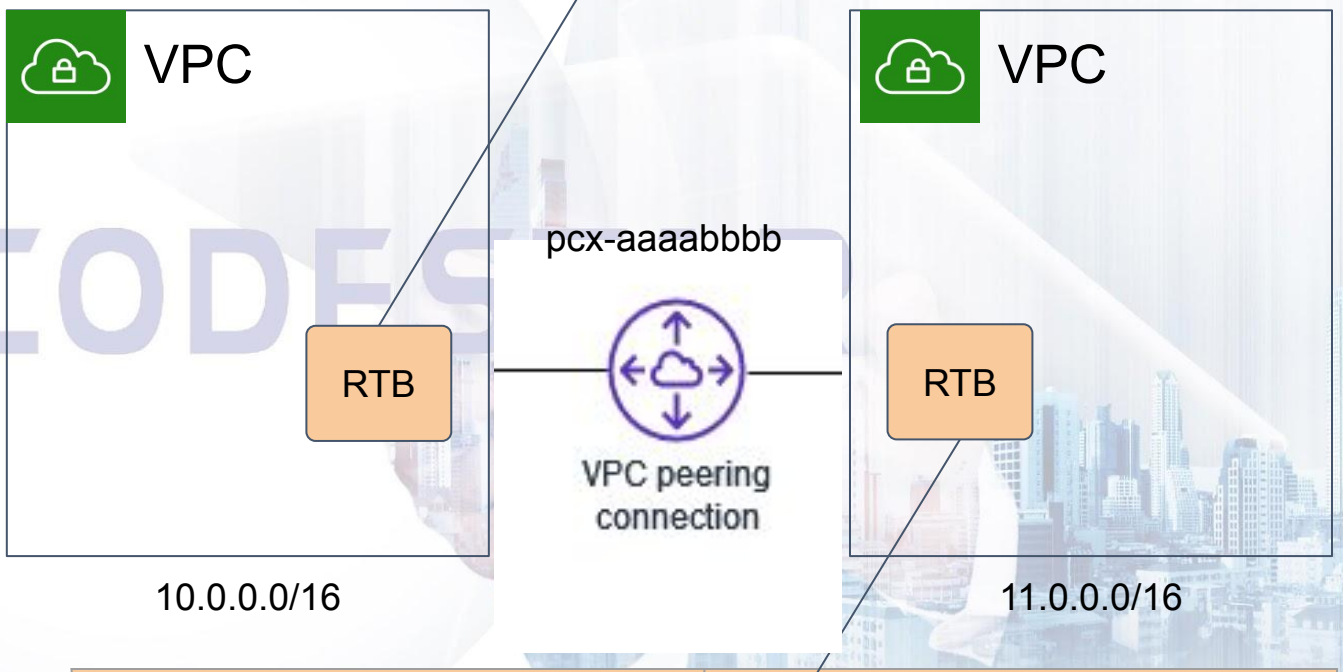
- Để kết nối VPC Peering với nhau, chúng ta cần một bên gửi yêu cầu kết nối (requester VPC) và một bên nhận request (accepter VPC)
- Sau khi requester VPC gửi yêu cầu và bên accepter đồng ý, VPC peering connection sẽ được hình thành.



VPC Peering

- Để kết nối sang VPC bên kia, chúng ta sử dụng Route Table, và trỏ tới peering connection đã được khởi tạo.
- VPC Peering tồn tại giữa 2 VPC và không thể kết nối sang một mạng kết nối khác.

Destination	Target
10.0.0.0/16	local
11.0.0.0/16	pcx-aaaabbbb
0.0.0.0/0	igw

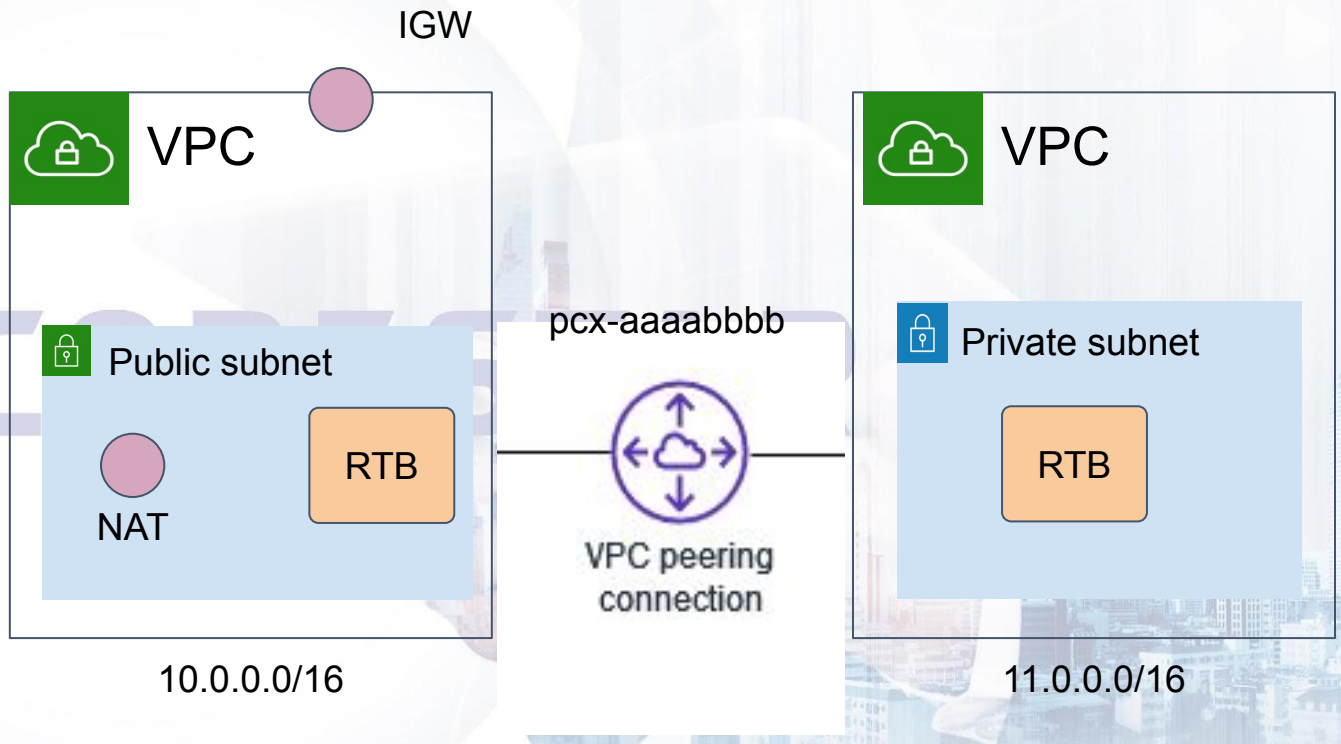


Destination	Target
11.0.0.0/16	local
10.0.10.0/24	pcx-aaaabbbb

VPC Peering

- VPC Peering không thể kết nối chuyển tiếp.

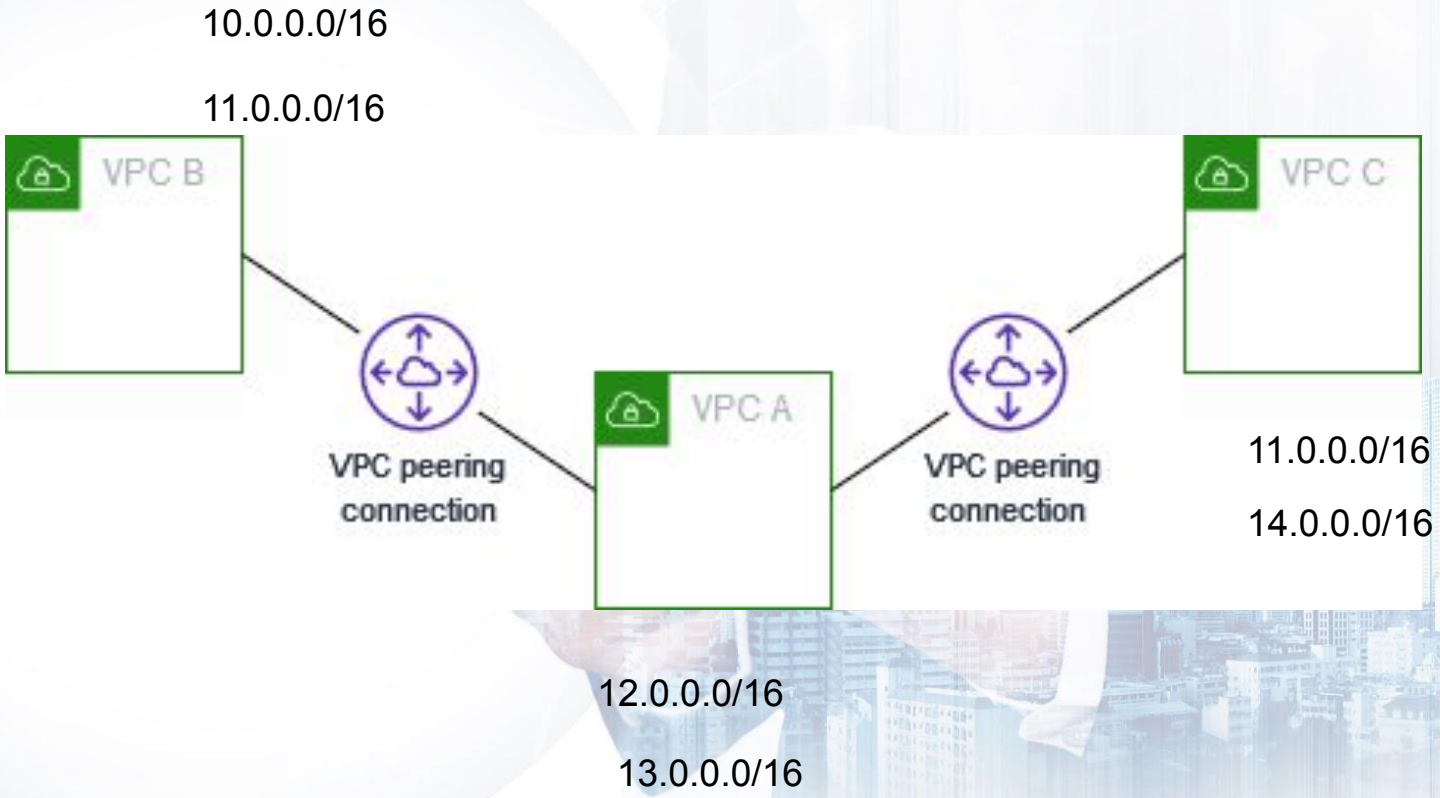
  Như hình bên, subnet trong VPC bên phải không thể kết nối ra ngoài internet nhờ sử dụng NAT gateway/instance của VPC bên trái. Tính chất này áp dụng với tất cả các thành phần khác như IGW, VPN, Direct Connect



VPC Peering

- VPC Peering không có tính chất bắc cầu.

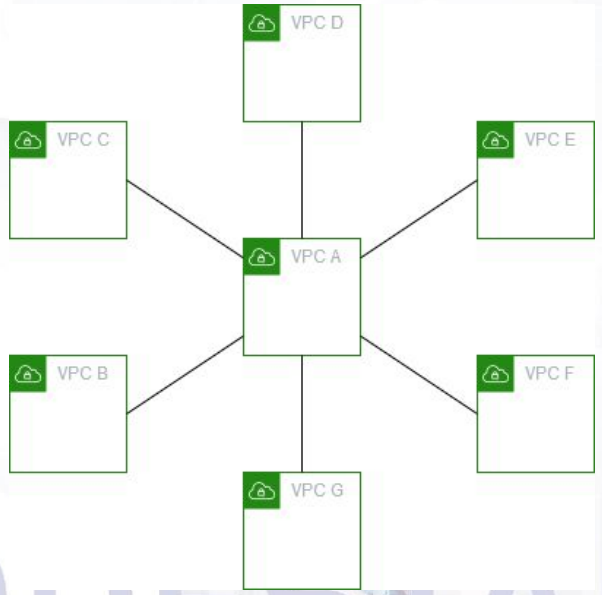
  Ở hình bên phải, VPC A và B kết nối với nhau. VPC A và C kết nối với nhau. Nhưng VPC B và C không được kết nối với nhau. Các VPC ***có kết nối*** *Peering với nhau không được phép có dải địa chỉ CIDR trùng.*

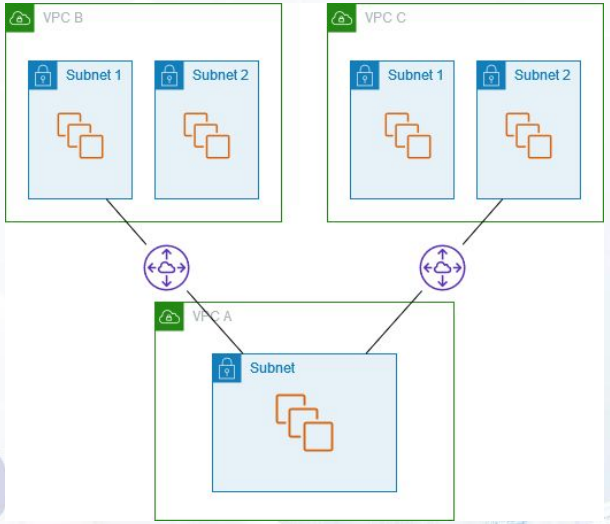


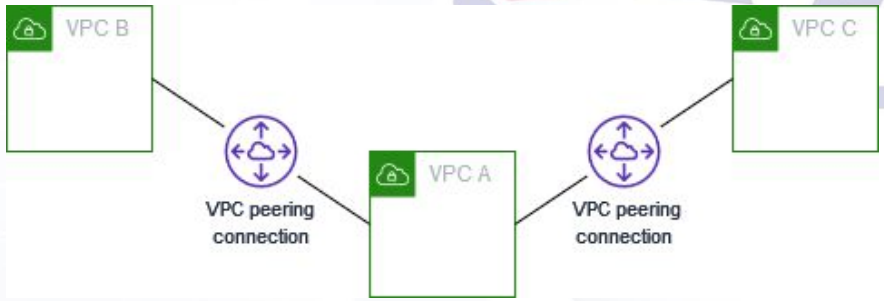
VPC Peering

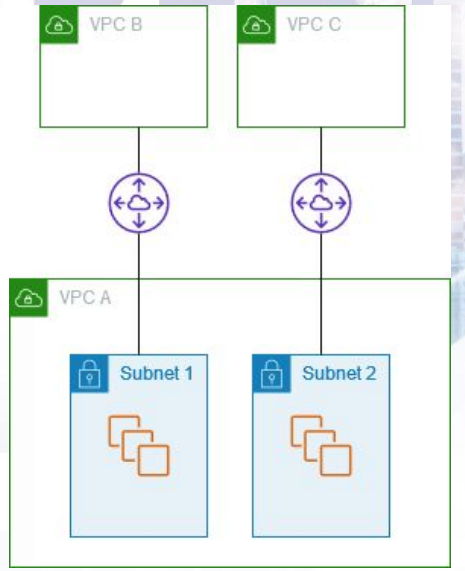
Một số mô hình connect với

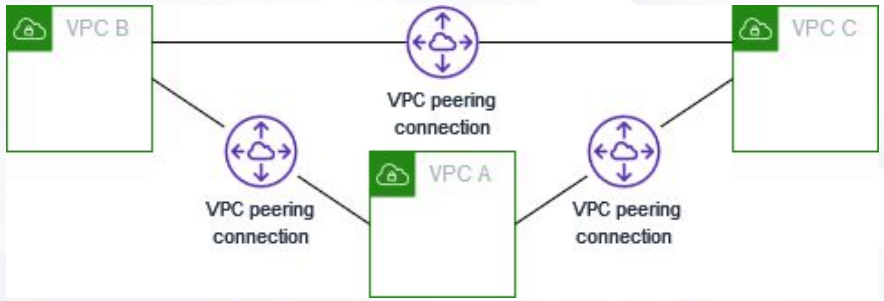
VPC Peering

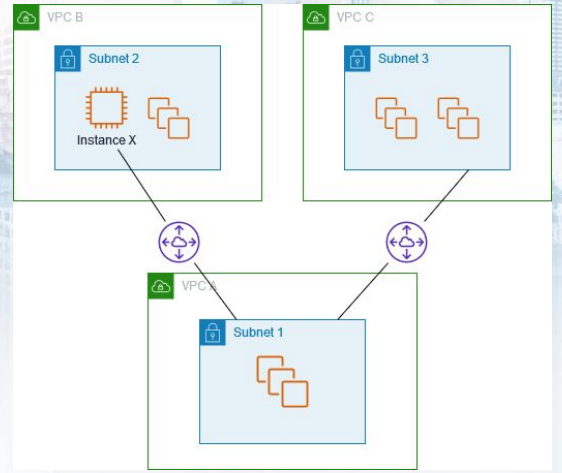






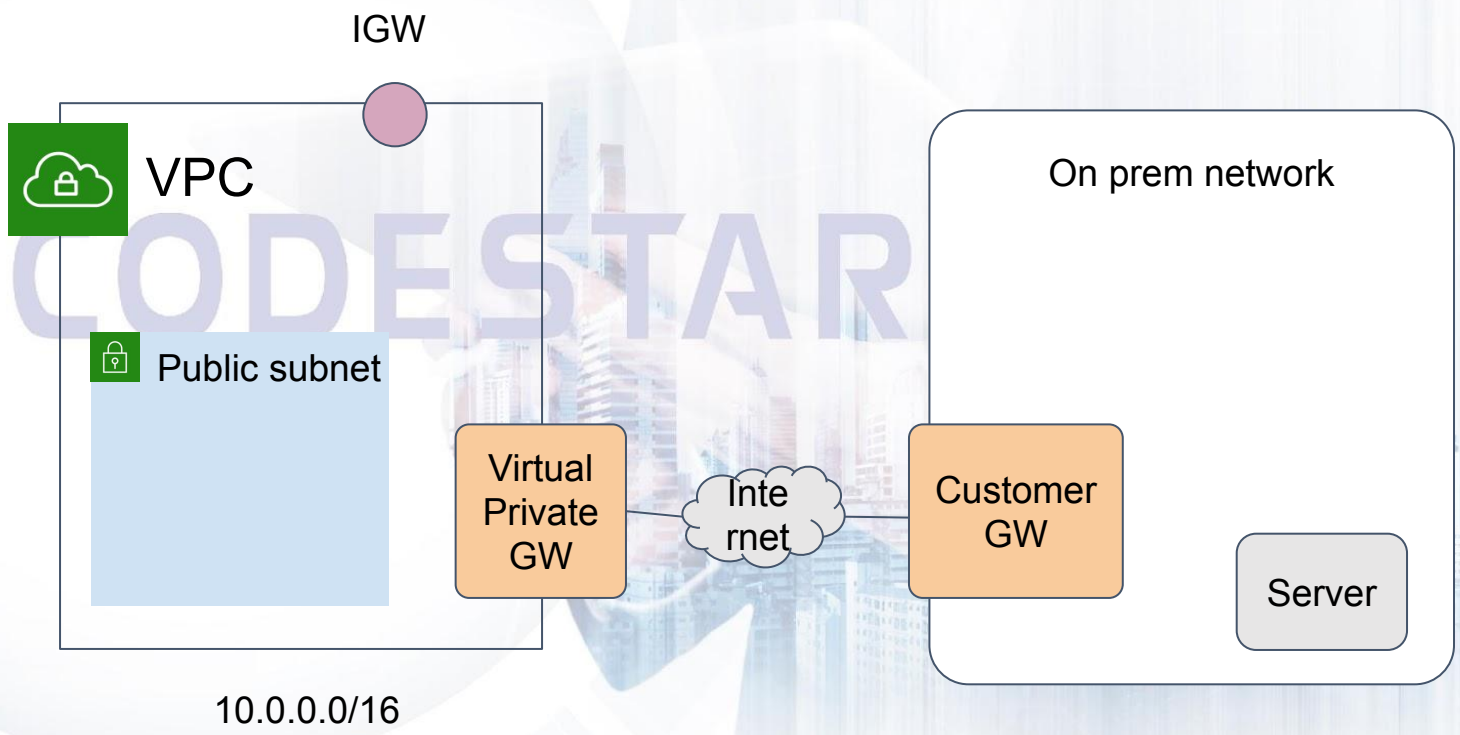






VPN Site-to-Site

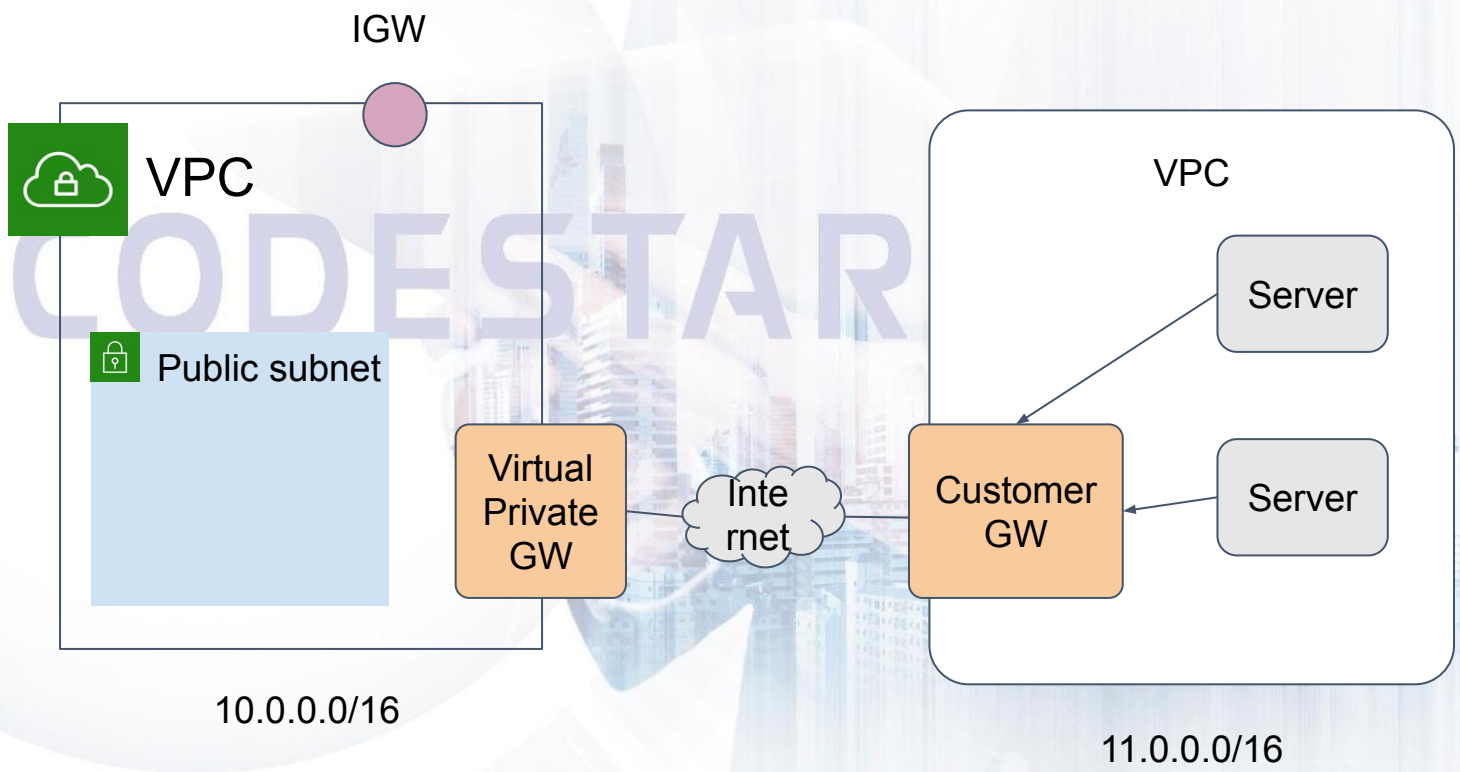
- VPN Site-to-Site là một phương thức dùng để kết nối 2 mạng với nhau.
- Kết nối giữa 2 target là một Tunnel, được mã hóa thông qua Internet



VPN Site-to-Site

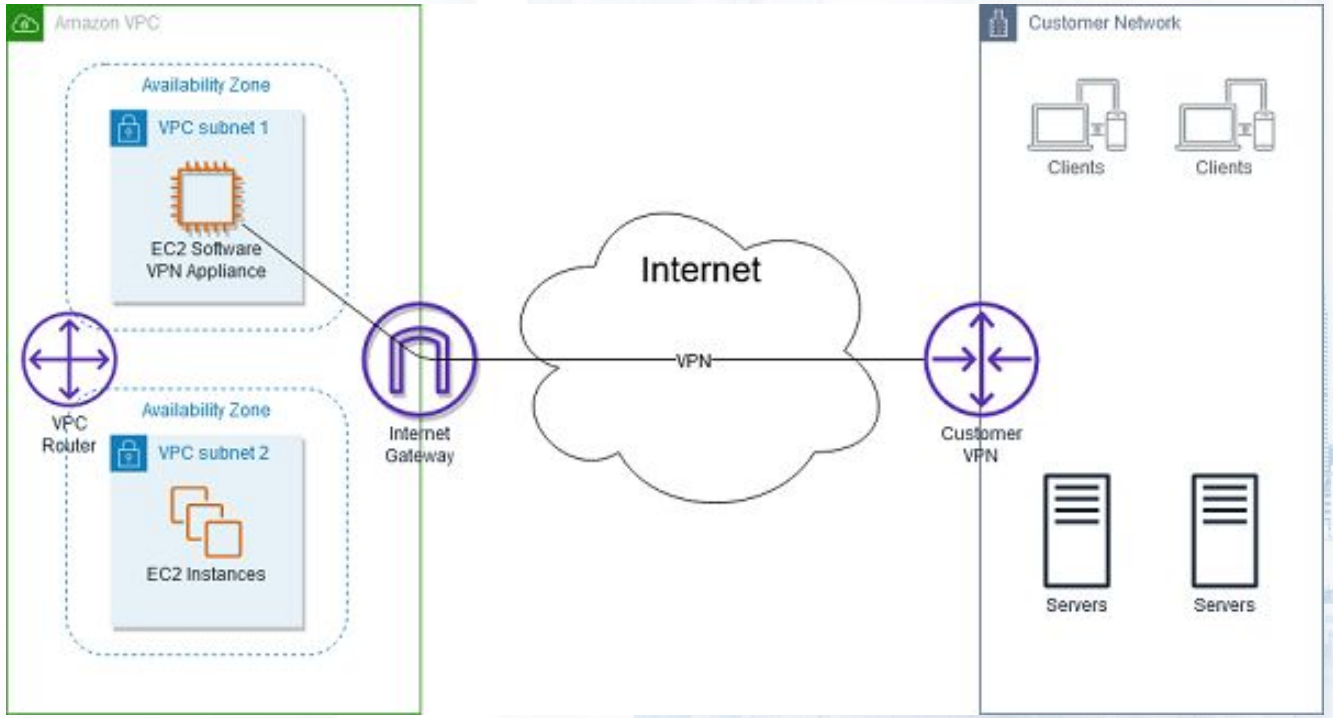
Destination	Target
10.0.0.0/16	customerGW
11.0.0.0/16	local
0.0.0.0/0	igw

- **Virtual Private Gateway** là một cổng vật lý, đại diện cho mạng khác kết nối vào.
- **Customer GW** thực chất là một máy chủ (hoặc 1 thiết bị phần cứng/Router) được cài đặt 1 số phần mềm đặc biệt để kết nối hình thành S2S Connection



VPN Site-to-Site

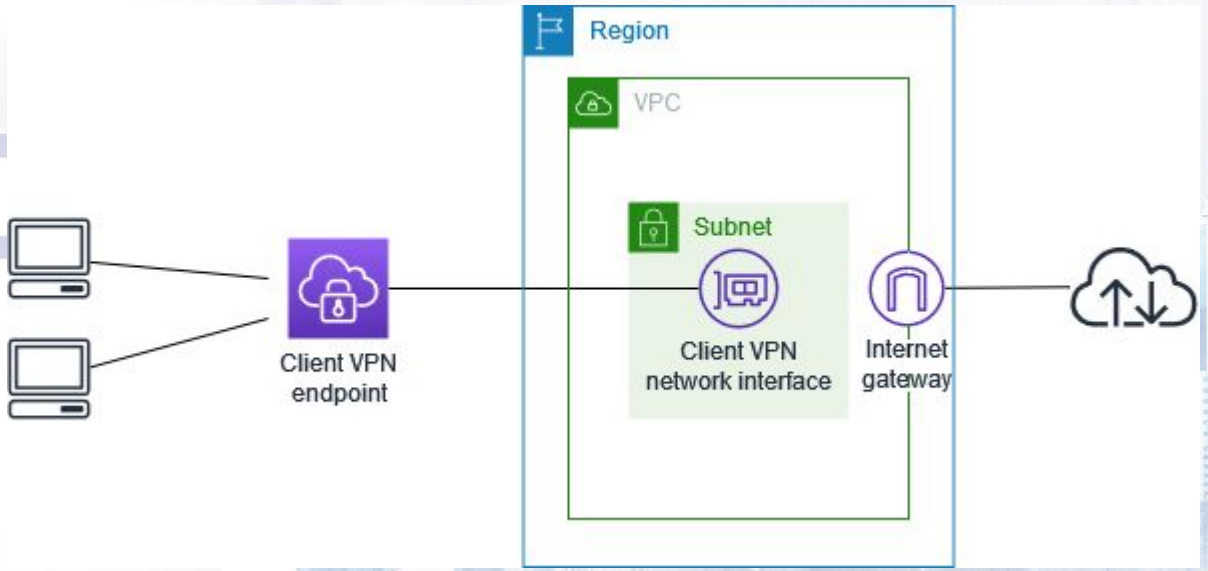
- Để kết nối từ hệ thống trên VPC sang một hệ thống dưới On prem, chúng ta sẽ cần sử dụng thêm VPN Appliance. Cài đặt VPN Appliance giúp chúng ta có thể truy cập được tới hệ thống đã kết nối.



VPN Site-to-Site

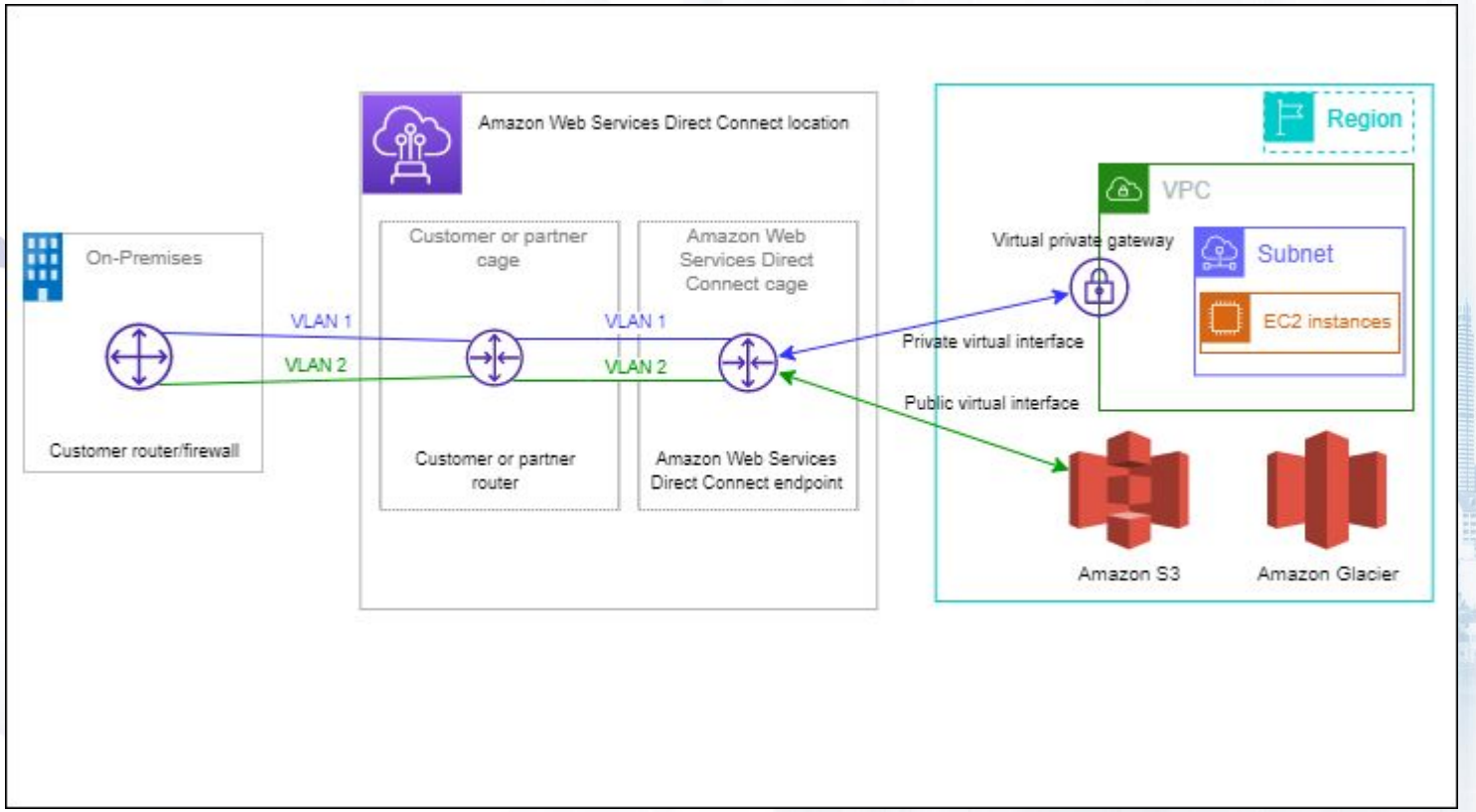
- AWS Client VPN là phần mềm cài đặt trên máy tính, hỗ trợ connect tới VPC thông qua Client VPN Network Interface.

  Use case: Kết nối từ 1 máy tính cụ thể tới một VPC hoặc ra ngoài Internet với IP của Network Interface.



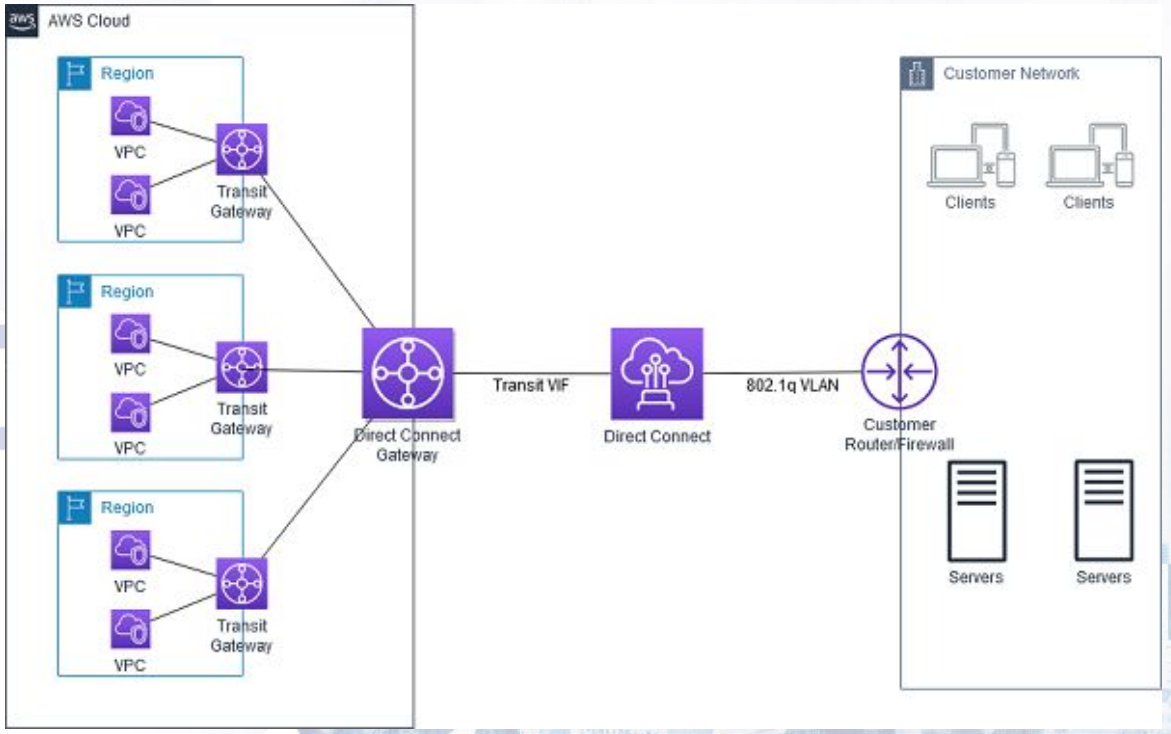
Direct Connect

- Direct Connect, dịch vụ cho phép khởi tạo và quản lý connection tới VPC trên cloud bằng một đường kết nối riêng biệt.



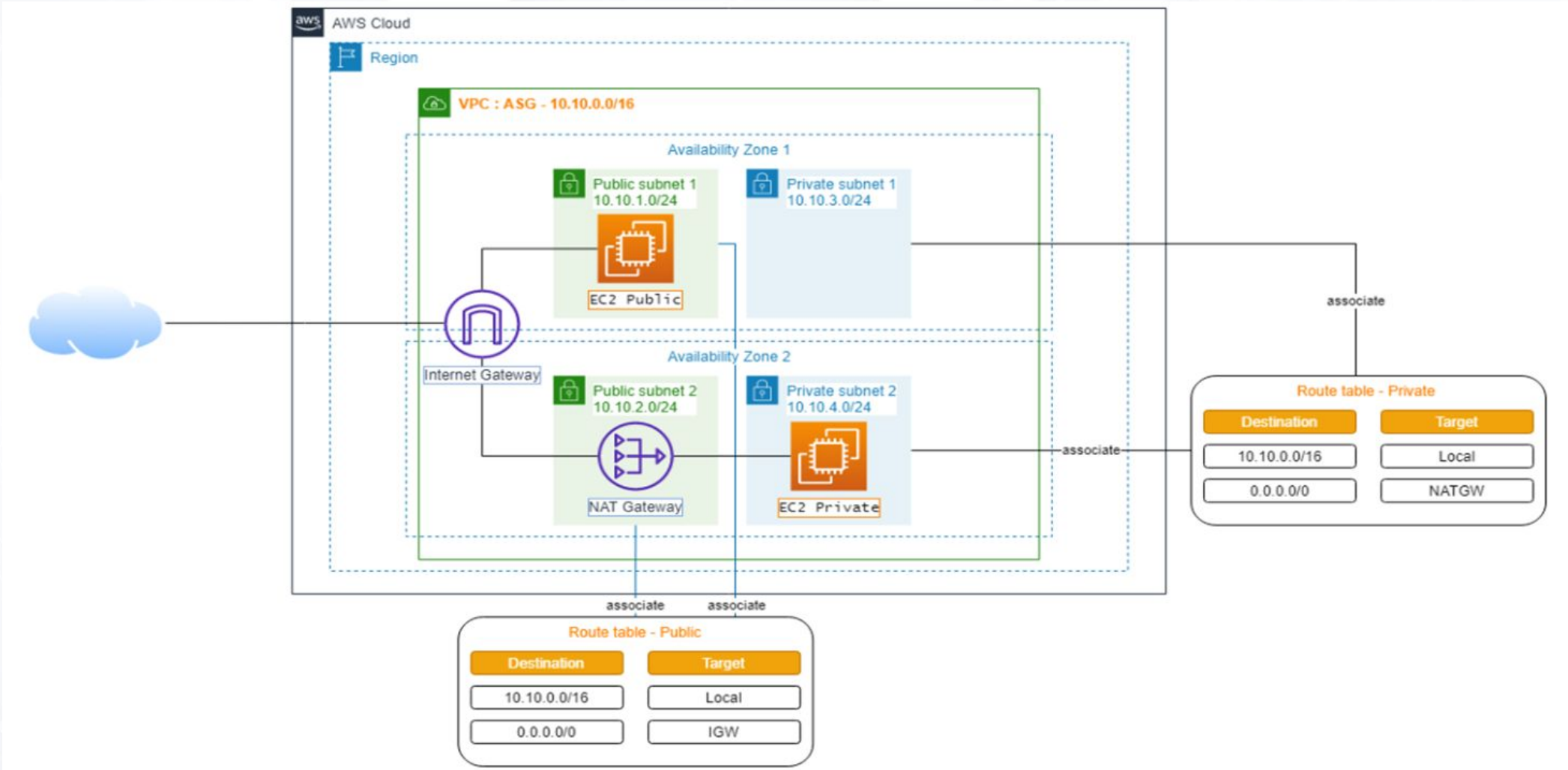
Transit Gateway

- Transit GW có thể kết nối nhiều VPC, và cả các Local Network.
- Transit GW có thể sử dụng DX, hoặc VPN.



Lab

Triển khai EC2 trong Private subnet và cấu hình sao cho EC2 này có thể truy cập Internet



Tài liệu tham khảo

1. https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html
2. https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html
3. https://aws.amazon.com/blogs/architecture/overview-of-data-transfer-costs-for-common-architectures/
4. https://medium.com/awesome-cloud/aws-difference-between-security-groups-and-network-acls-adc632ea29ae
5. https://docs.aws.amazon.com/cur/latest/userguide/cur-data-transfers-charges.html
6. https://repost.aws/questions/QUaVpck0FWTTqcZIqE0szZIg/how-to-reduce-data-transfer-cost-in-aws

CODESTAR

THANK YOU


CODESTAR

Câu 1

Công ty A có một số EC2 instance trong VPC và cần kết nối endpoint của dịch vụ SaaS mà công ty đang đăng ký sử dụng. Giải pháp SaaS này expose Giải pháp nào phù hợp để kết nối VPC đến dịch vụ SaaS đó?

A. Sử dụng AWS PrivateLink

B. Sử dụng Internet Gateway

C. Sử VPC Peering

D. Sử dụng VPN Site to Site

Câu 2

Công ty A có một số EC2 instance trong VPC và phát hiện thấy các EC2 đang bị tấn công bởi một loạt các IP như 100.1.1.1, 100.1.1.2, 100.1.1.10. Giải pháp nào sau đây sẽ giúp chặn được các tấn công từ các IP này?

A. Cấu hình SG inbound rule block range IP của các IP tấn công

B. Cấu hình NACL inbound rule block range IP của các IP tấn công

C. Cấu hình Route table block range IP của các IP tấn công

D. Cấu hình NACL outbound rule block range IP của các IP tấn công

Câu 3

Công ty A có một ứng dụng ERP SAP B1 triển khai trên VPC. Giải pháp nào sau đây cho phép nhân viên có thể truy cập ứng dụng ERP trên VPC từ nhà, văn phòng thông qua thiết bị di động, laptop?

A. Sử dụng VPN Site to Site

B. Sử dụng Client VPN

C. Sử dụng VPC Peering

D. Sử dụng Transit Gateway

Câu 4

Giải pháp nào sau đây giúp ngân hàng có thể kết nối DC ở on-premise lên các resource trên AWS thông qua kênh truyền riêng?

A. Sử dụng VPN Site to Site

B. Sử dụng AWS Direct Connect

C. Sử dụng Internet

D. Sử dụng SD-WAN

Câu 5

Khi kiểm tra việc thiết lập kết nối VPN Site to Site từ AWS đến firewall trên On-premise.

Làm thế nào để biết được VGW trên AWS đã gửi packet xuống on-premise?

A. Kiểm tra CloudTrail

B. Kiểm tra CloudWatch Alarms

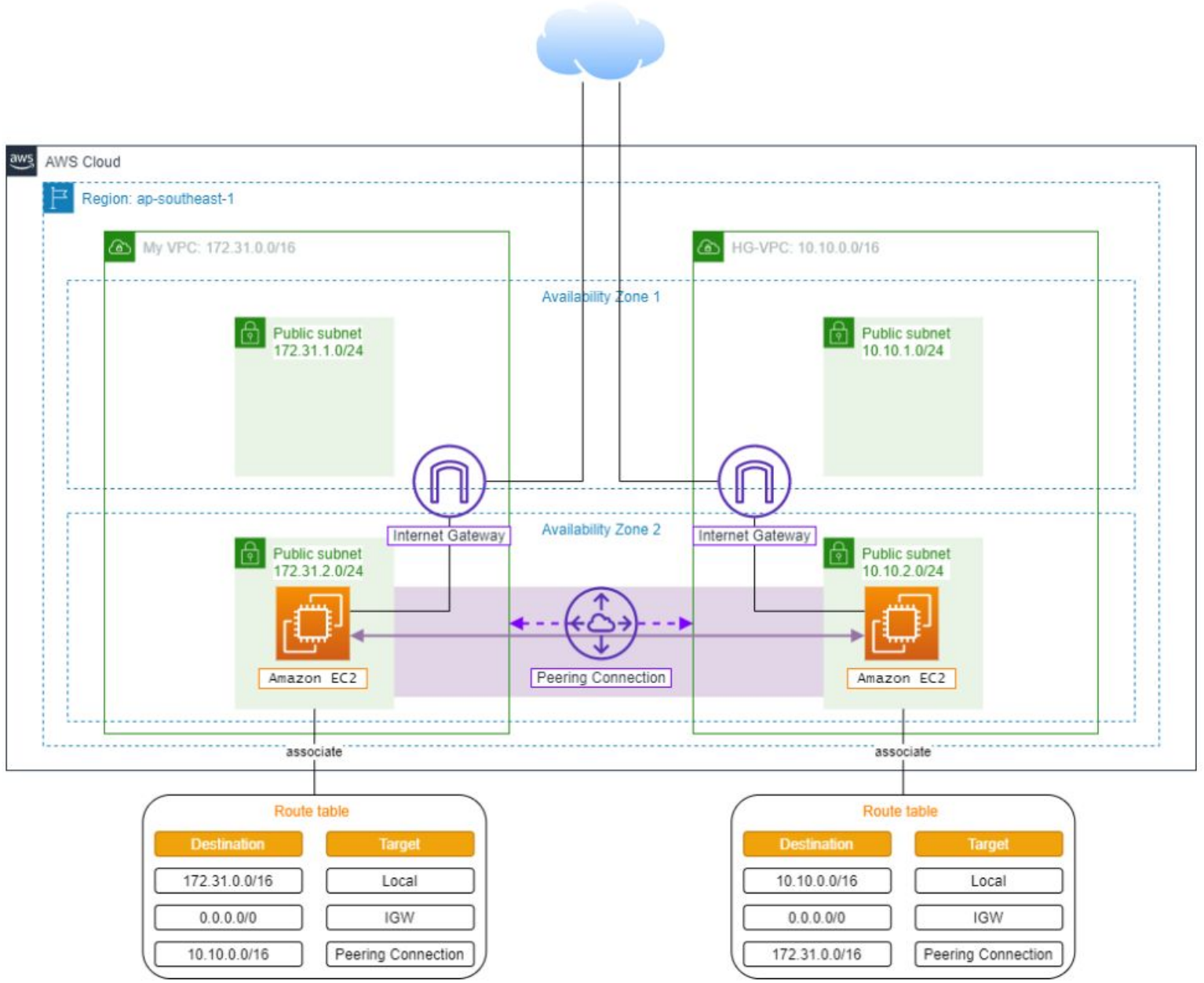
C. Kiểm tra VPC Flow Logs

D. Tất cả đều đúng


CODESTAR
Framework

Homework

Cấu hình EC2 trên 2 VPC sao cho 2 EC2 instance này có thể ping được nhau thông qua VPC Peering



CODESTAR

THANK YOU