Virtual Private Cloud (VPC)

lamdaongc@gmail.com

Nội dung bài học

1. Network căn bản
2. VPC & Subnet Overview
3. VPC connection
4. VPC traffic management
5. VPC Pricing
6. Tổng Kết

Mục tiêu

Kết thúc bài học, sinh viên cần:

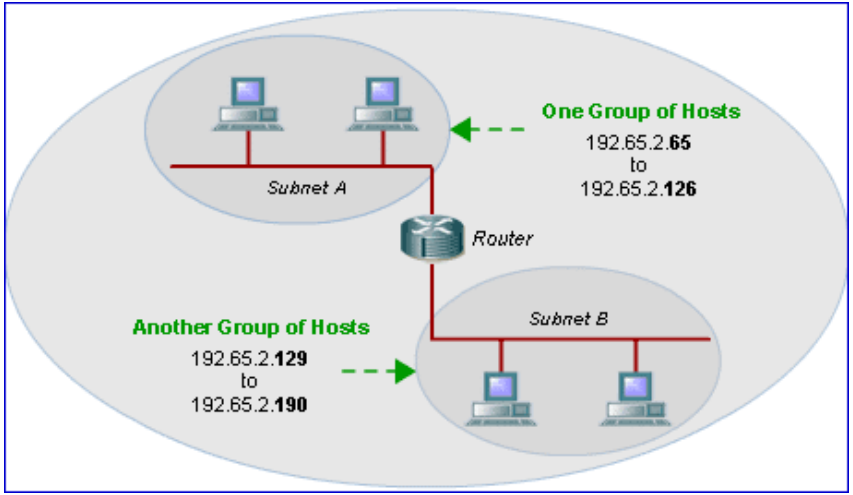
- Nắm được các kiến thức cơ bản về network
- Nắm được mô hình các dịch vụ network trên AWS (VPC)
- Có khả năng phác thảo kiến trúc của AWS VPC
- Tự thiết kế và từng bước triển khai được một VPC hoàn chỉnh
- Có khả năng triển khai tài nguyên nằm trong VPC
- Hiểu được vai trò của Security Group và Access Control List

Section 1:

Network căn bản

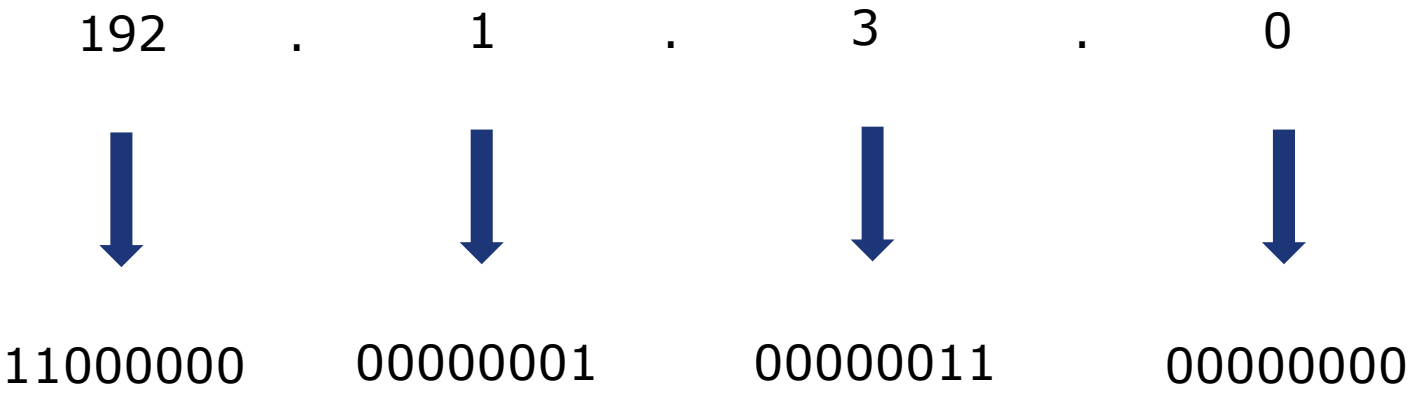
Network

- Một Network bao gồm hai hoặc nhiều thiết bị được kết nối nhằm chia sẻ tài nguyên cho nhau
- Một Network có thể được chia nhỏ thành các subnet
- Một network cần phải có thiết bị mạng (router hoặc switch) để cung cấp kết nối giữa các thiết bị

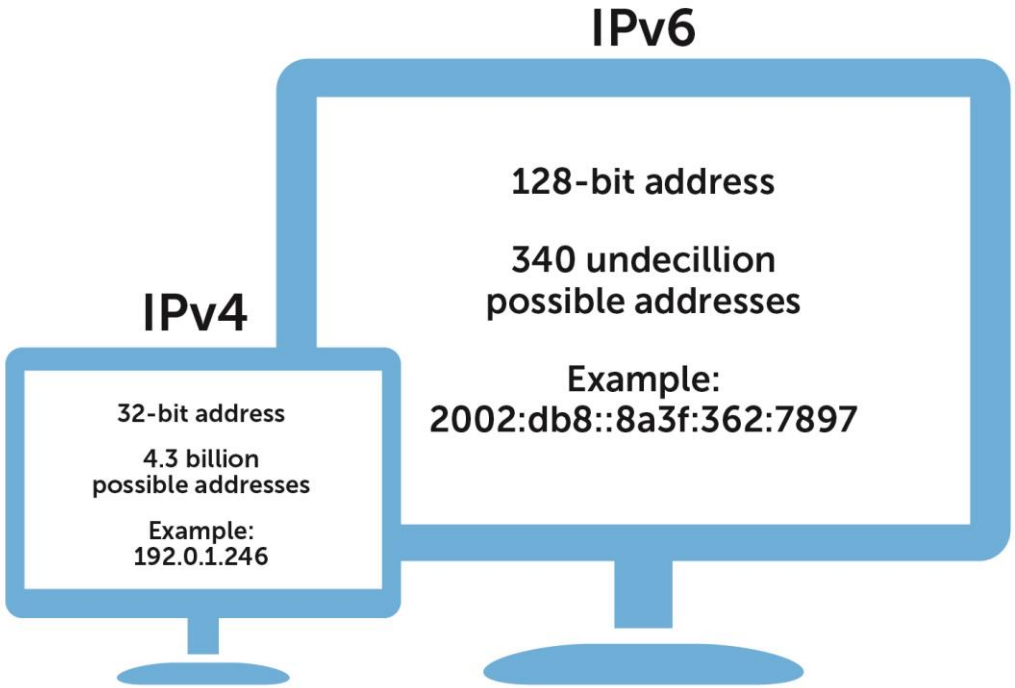


Địa Chỉ IP

- Mỗi client trong Network cần có 1 địa chỉ IP duy nhất để có thể kết nối
- Địa chỉ IP được thể hiện dưới dạng thập phân và client sẽ tự động chuyển sang dạng nhị phân khi sử dụng



IPv4 vs IPv6


IPv6
128-bit address
340 undecillion
possible addresses
Example:
2002:db8::8a3f:362:7897
IPv4
32-bit address
4.3 billion
possible addresses
Example:
192.0.1.246

Classless Inter Domain Routing (CIDR)

- Làm sao để quy hoạch một Network?
- Phải gắn địa chỉ IP như thế nào

→ Cần có quy tắc quy hoạch địa chỉ IP

Classless Inter Domain Routing (CIDR)

- Với windows, mở CMD và gõ ipconfig
- Với linux, mở terminal và gõ ifconfig

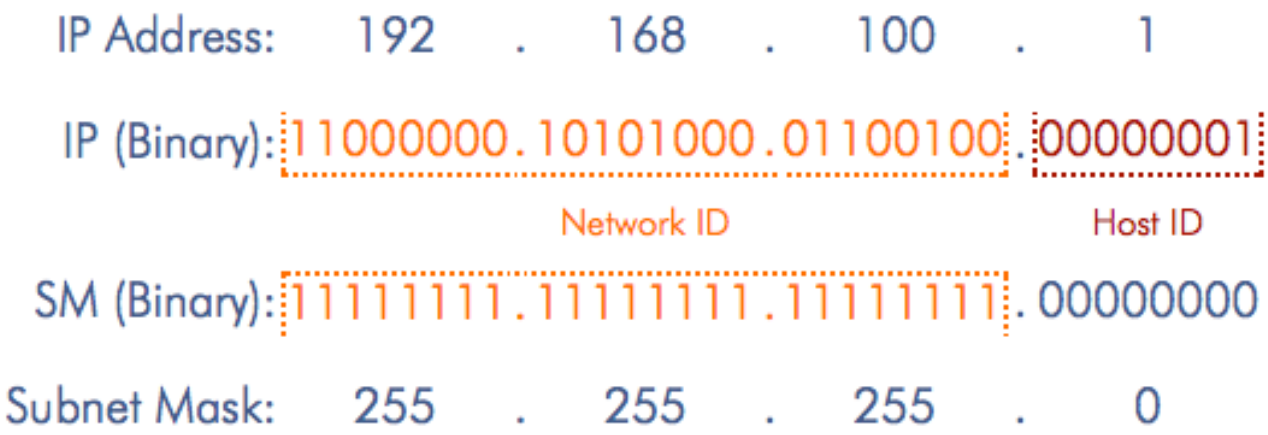
```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::eccd:40ca:e173:232d%16
   IPv4 Address. . . . . . . . . . . : 192.168.201.104
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.201.3
```

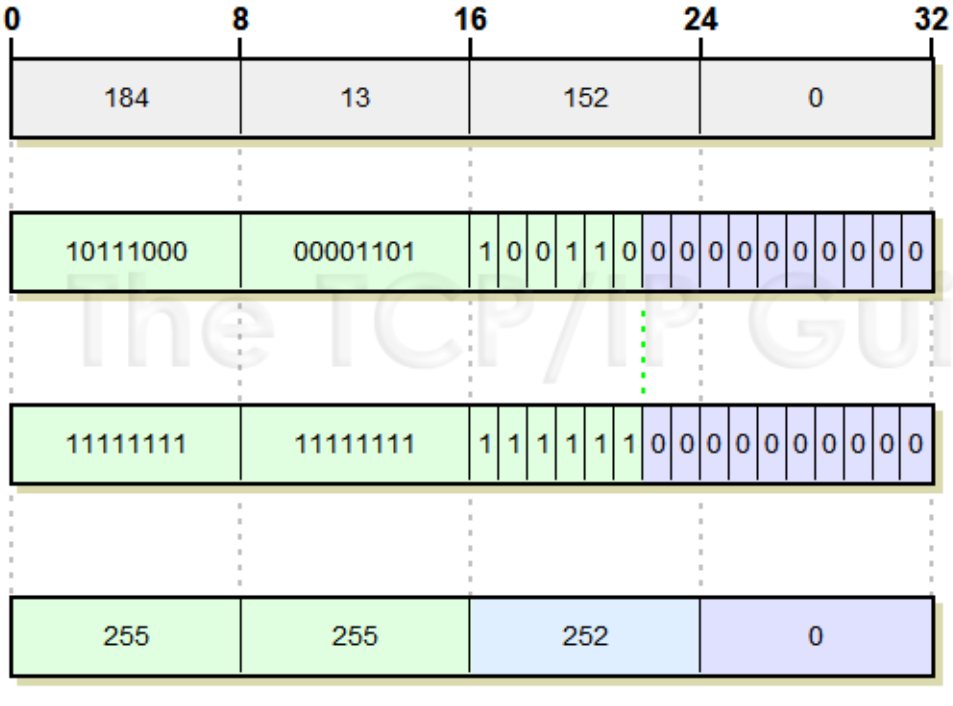
- Ngoài Ipv4 Address, còn có Subnet Mark và Default Gateway

Classless Inter Domain Routing (CIDR)

Subnet Mark: đánh dấu các bit không thay đổi của các địa chỉ trong cùng subnet, network



Classless Inter Domain Routing (CIDR)



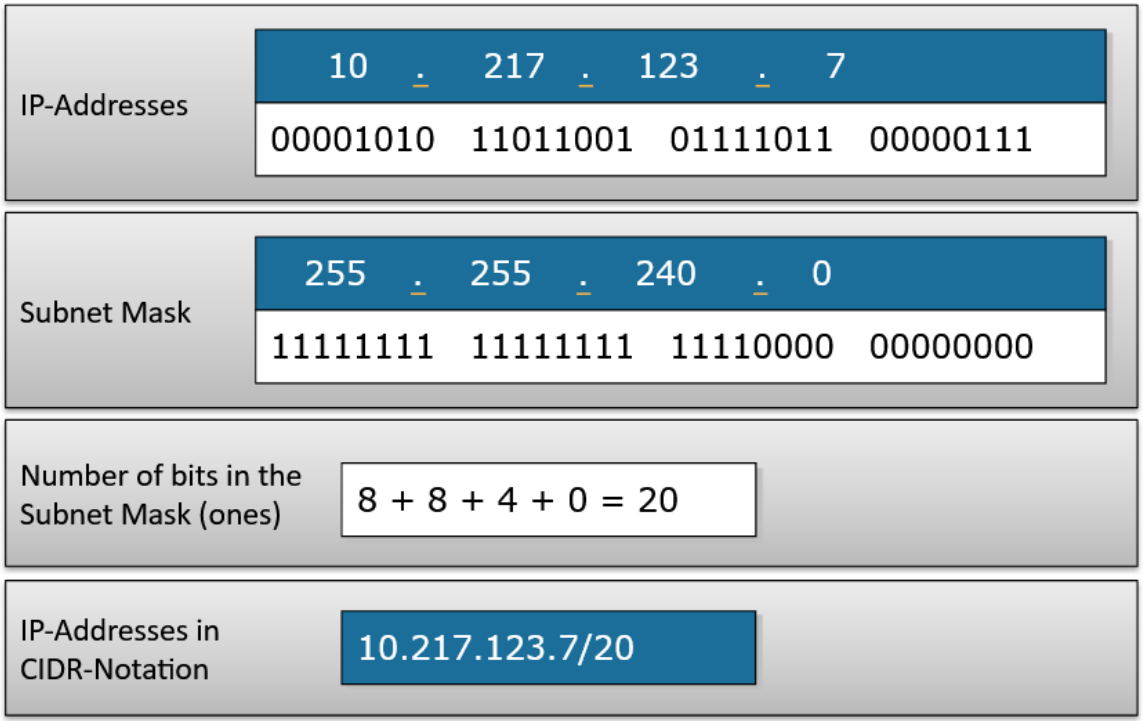
Classless Network 184.13.152.0/22

22 Bits for Prefix (Network ID) and 10 Bits for Host ID

Binary Subnet Mask for /22 Network

Binary Subnet Mask Converted to Dotted Decimal (255.255.252.0)

Exercise: CIDR Hand-on



Section 2:

VPC Overview

Khái Niệm VPC

AWS VPC

- VPC cung cấp một logical network độc lập trên AWS cloud, tạo môi trường kết nối mạng cho các máy chủ
- VPC có khả năng quản lý tài nguyên mạng bao gồm:
  - Thiết lập dải địa chỉ IP
  - Tạo các subnet
  - Cấu hình các quy tắc định tuyến và gateway
- VPC cho phép người quản trị có thể tùy chỉnh các cài đặt về Network
- VPC cung cấp nhiều lớp bảo mật

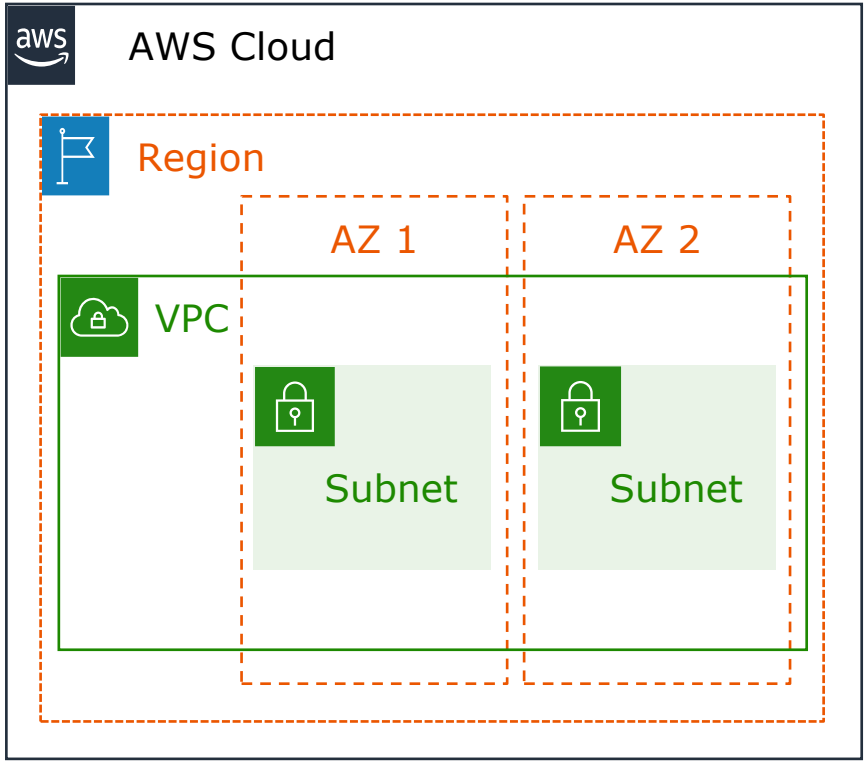
VPC & Subnet

VPC:

- Mỗi VPC là **độc lập** về mặt **logic**
- VPC nằm trên một **Region**
- VPC thuộc về một **account ID** duy nhất

Subnet:

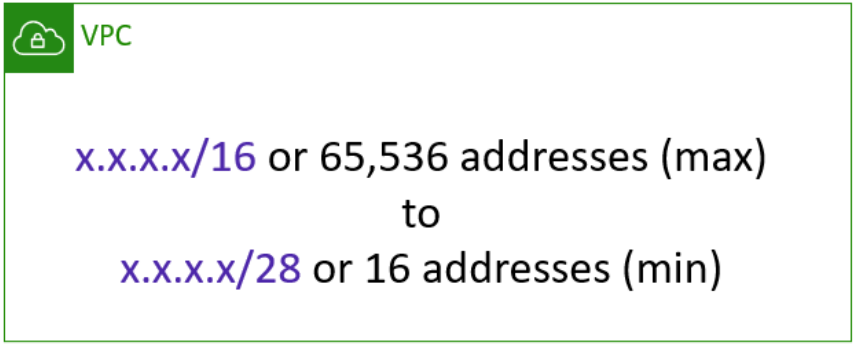
- Mỗi Subnet đều thuộc 1 VPC nào đó
- **Dải IP** của Subnet phải nằm trong dải IP của VPC
- Subnet nằm trên một **AZ**
- 2 loại subnet: **public** và **private**



Cấu Hình Địa Chỉ IP

Cấu hình đ/c IP cho VPC & Subnet:

- VPC cần được cài đặt dải địa chỉ IP khi khởi tạo. Dải địa chỉ này là không thể thay đổi
- Các subnet trên cùng VPC phải được cấu hình dải địa chỉ IP độc lập, không được overlap
- Giới hạn dải IP trong VPC là từ /16 tới /28
    - /16: 65,536 địa chỉ IP
    - /28: 16 địa chỉ IP
- VPC có hỗ trợ IPv6 trên một số instance type



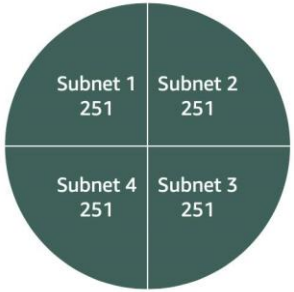
VPC IP Addessing

Một Số Địa Chỉ IP Cố Định

Các địa chỉ IP cố định:

- Địa chỉ đầu tiên: subnet ID
- Địa chỉ thứ 2: local route (default gw)
- Địa chỉ thứ 3: DNS server
- Địa chỉ thứ 4: dự phòng cho tính năng mới trong tương lai
- Địa chỉ cuối cùng: broadcast address

→ Các địa chỉ trên trong Subnet được sử dụng cho mục đích riêng, và sẽ không được cấp phát cho các tài nguyên



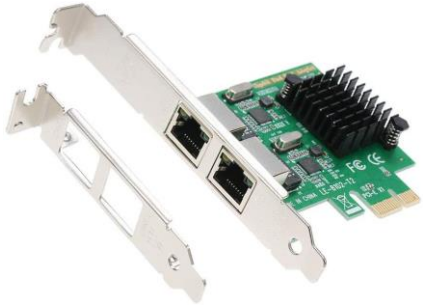
IP address	Reserved for
10.0.0.0	Network address
10.0.0.1	VPC local router
10.0.0.2	DNS server
10.0.0.3	Future use
10.0.3.255	Network broadcast address

Mẫu ví dụ về VPC với network 10.0.0.0/16 mỗi subnet được phân dải subnet /24 với 256 địa chỉ IP và 251 địa chỉ khả dụng để gắn cho tài nguyên

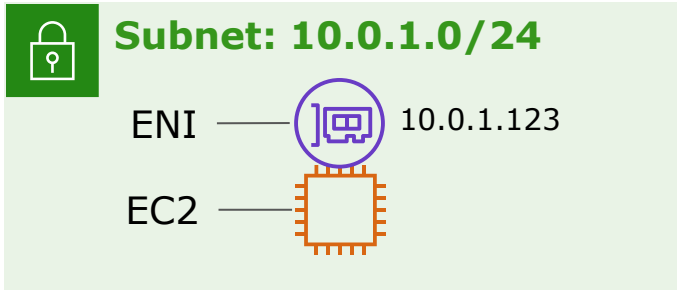
Elastic Network Interface

Elastic Network Interface:

- ENI là một **Virtual Network Interface** được sử dụng như một card mạng cho các Instance
- Có thể detach ENI khỏi instance và attach ENI đó sang instance khác
- Mặc định, mỗi instance khi được tạo ra đã có một ENI mặc định với địa chỉ IP private nằm trong dải IP của VPC



Network Interface Card

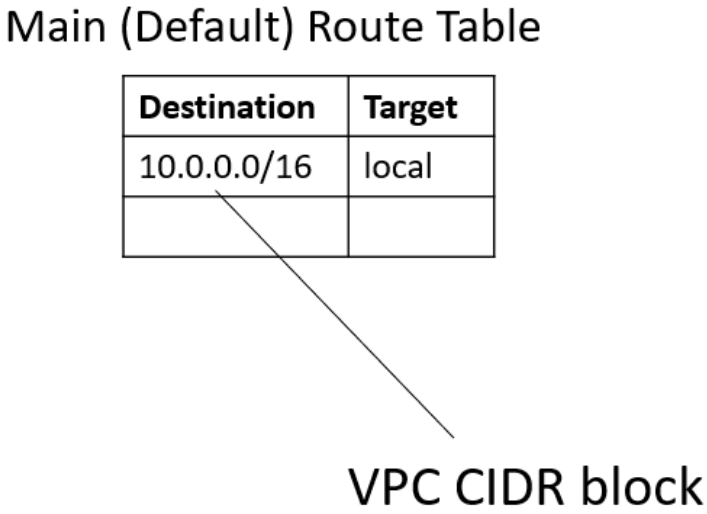


Virtual Network Interface

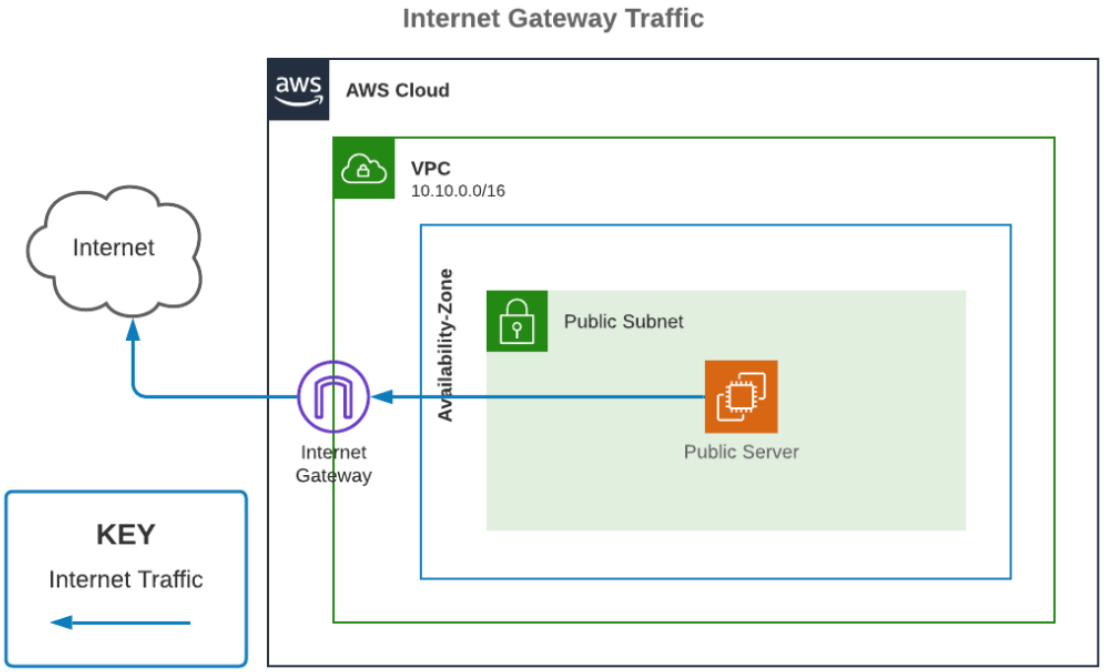
Route Table

Route table:

- Route table là một bảng lưu trữ danh sách các quy tắc giúp định tuyến traffic đi từ subnet
- Mỗi một quy tắc mô tả 2 phần: Destination và Target
- Mặc định, các Subnet cùng nằm trong một VPC có thể kết nối tới nhau dựa trên local route
- Mỗi Subnet chỉ được gắn với 1 route table
- Subnet không được gắn với route table nào sẽ tự động được gắn với main route table



Internet Gateway

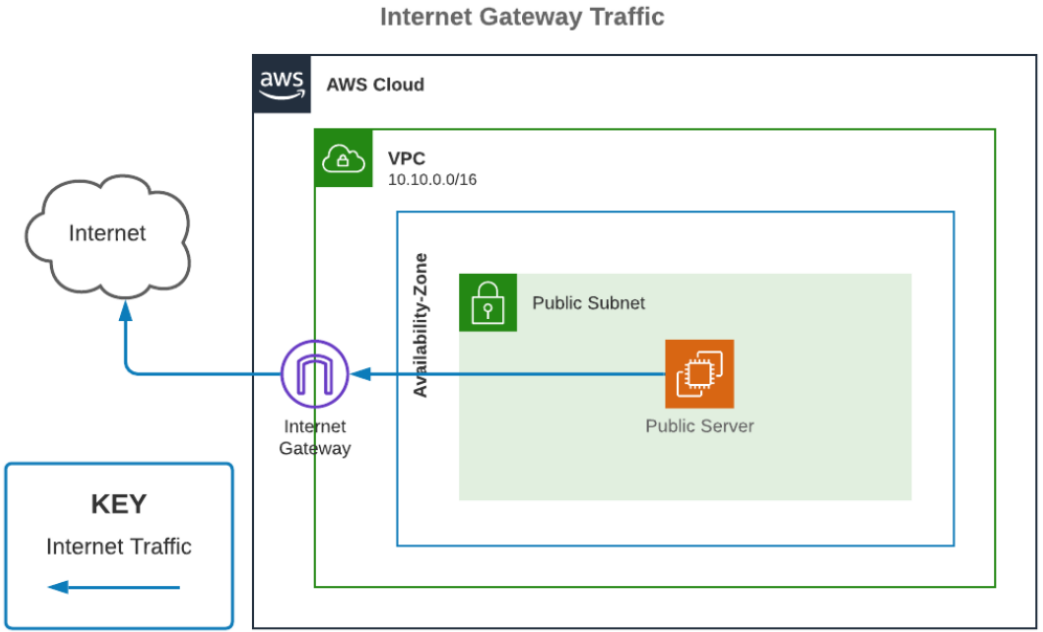


Public Subnet Route Table

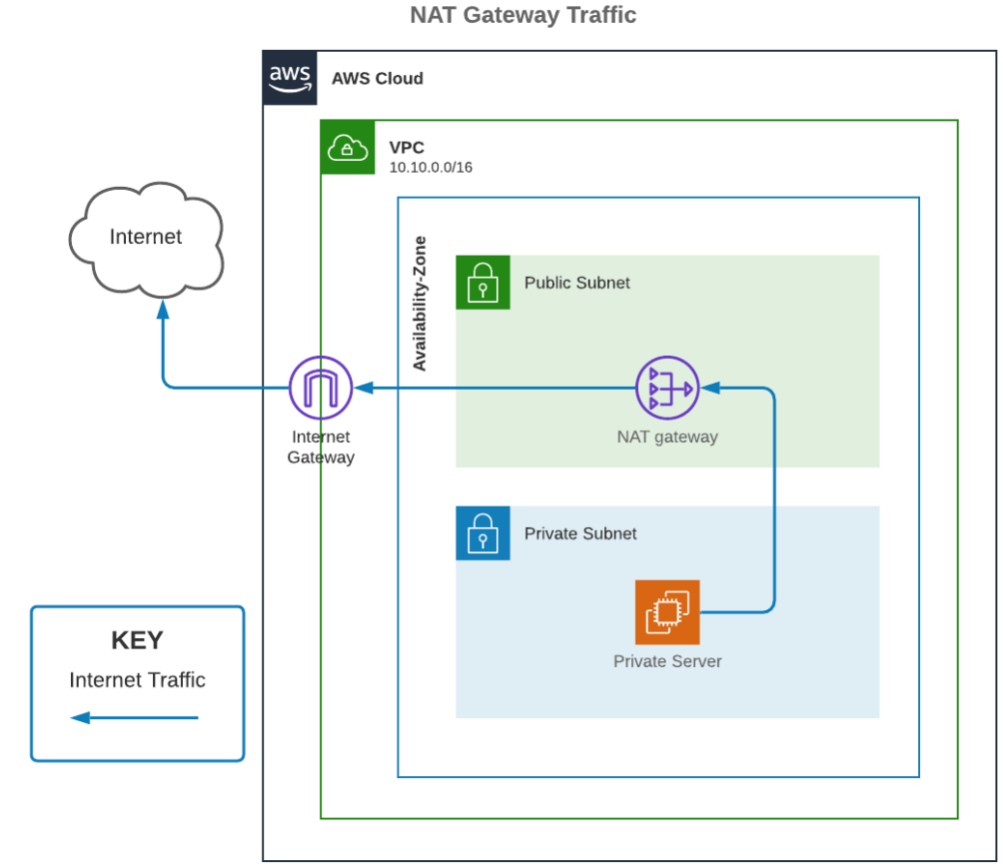
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-id

Lab 1: Tạo VPC Với Public Subnet

- Default VPC overview
- Tạo VPC
- Tạo subnet trong VPC
- Tạo Internet gateway
- Cấu hình Route table
- Tạo EC2 instance
- Kết nối EC2 tới internet



NAT Gateway



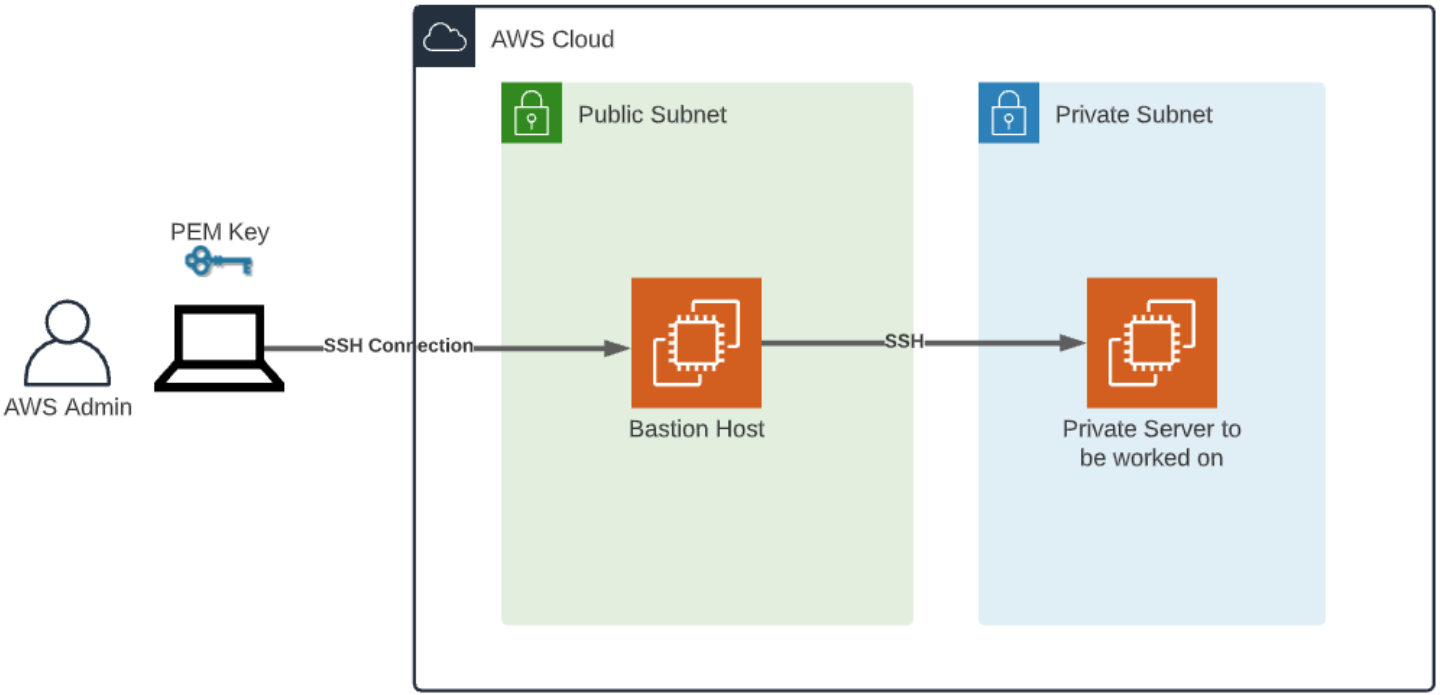
Public Subnet Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-id

Private Subnet Route Table

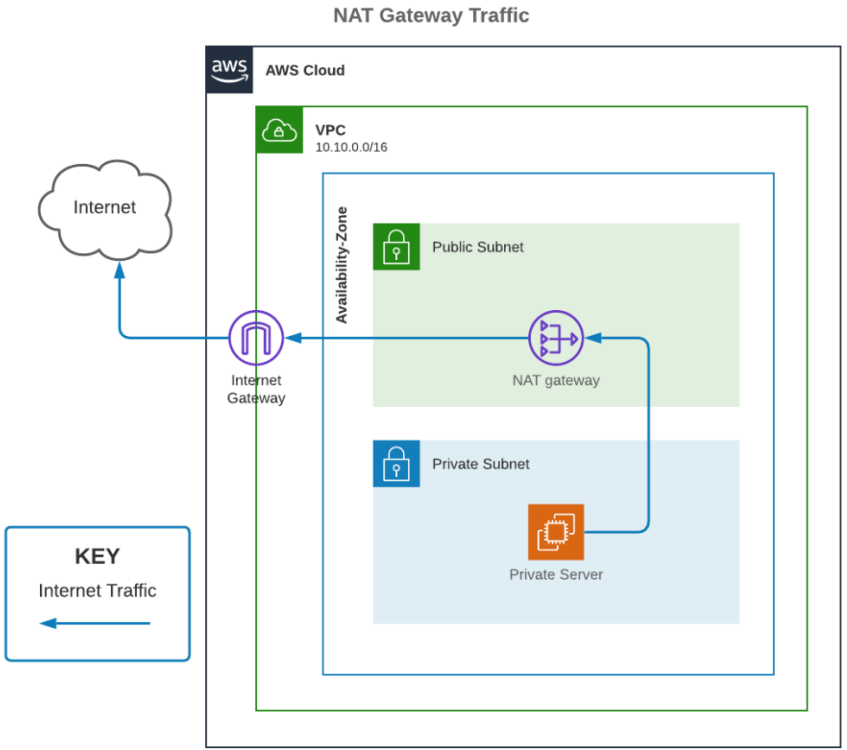
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	nat-gw-id

Bastion Host



Lab 2: Tạo VPC Với Private Subnet

- Thực hiện Lab 1
- Tạo private subnet trong VPC
- Tạo NAT gateway
- Cấu hình Route table
- Tạo EC2 instance
- Kết nối EC2 tới internet

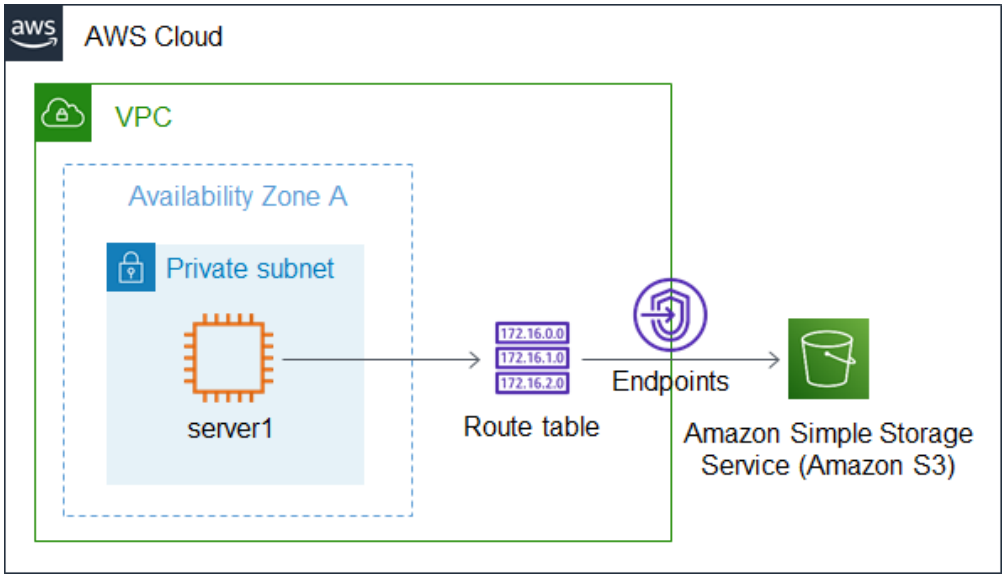


VPC Endpoint

VPC Endpoint:

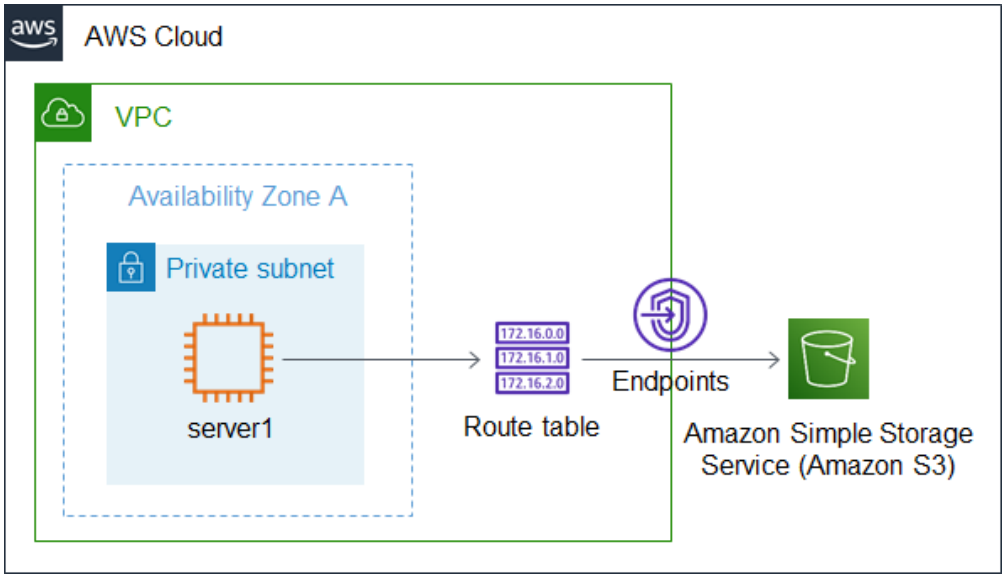
- Cung cấp một endpoint tới các dịch vụ khác của AWS

→ giúp instance kết nối tới các dịch vụ thông qua mạng nội bộ (bên trong VPC) mà không cần đi ra internet



Lab 3: tạo VPC endpoint cho S3

- Tạo VPC Endpoint cho s3 bucket
- Kết nối từ ec2 instance thông qua endpoint và qua internet



Section 3:

VPC Connection

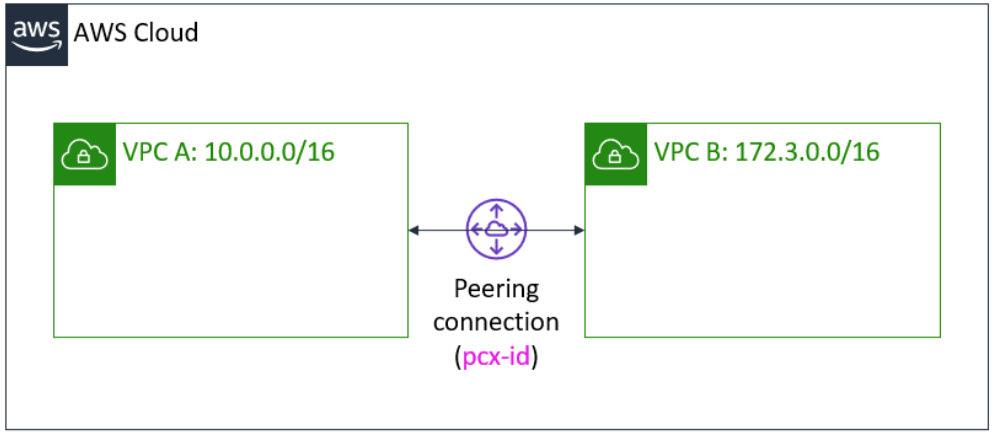
VPC Peering

VPC Peering:

- Giúp tạo kết nối giữa 2 VPC bất kể 2 VPC không nằm trên cùng một AWS Account hay Region

Lưu ý khi tạo VPC Peering

- Địa chỉ IP của 2 VPC không được overlap
- VPC peering không hỗ trợ bắc cầu
- Giữa 2 VPC chỉ có thể tạo được 1 kết nối peering



Route Table for VPC A

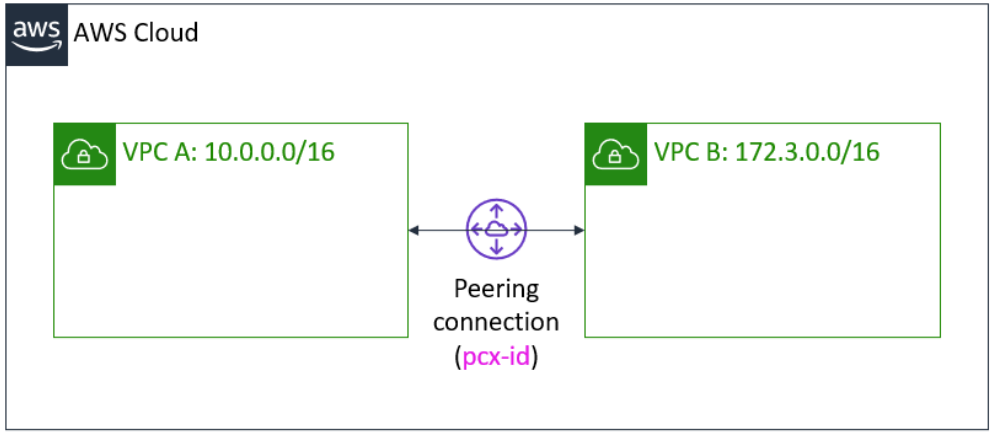
Destination	Target
10.0.0.0/16	local
172.3.0.0/16	pcx-id

Route Table for VPC B

Destination	Target
172.3.0.0/16	local
10.0.0.0/16	pcx-id

Lab 4: Tạo VPC Peering

- Tạo VPC peering giữa 2 VPC
- Kết nối giữa các instance nằm trong 2 VPC thông qua private IP



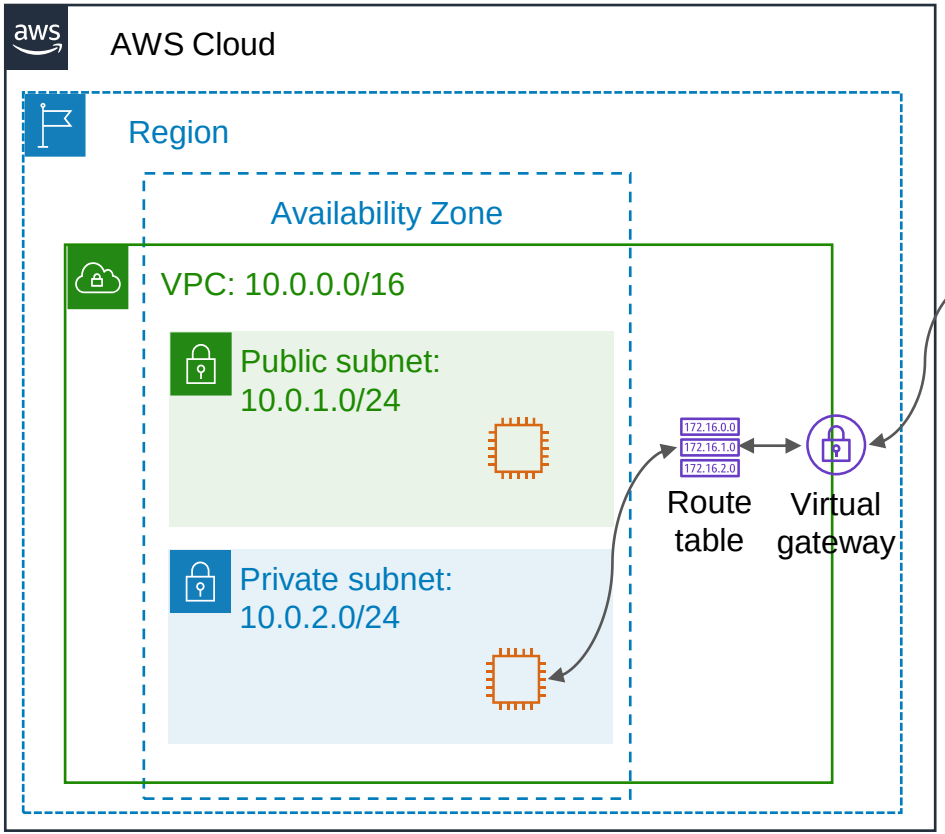
Route Table for VPC A

Destination	Target
10.0.0.0/16	local
172.3.0.0/16	pcx-id

Route Table for VPC B

Destination	Target
172.3.0.0/16	local
10.0.0.0/16	pcx-id

Site-to-Site VPN



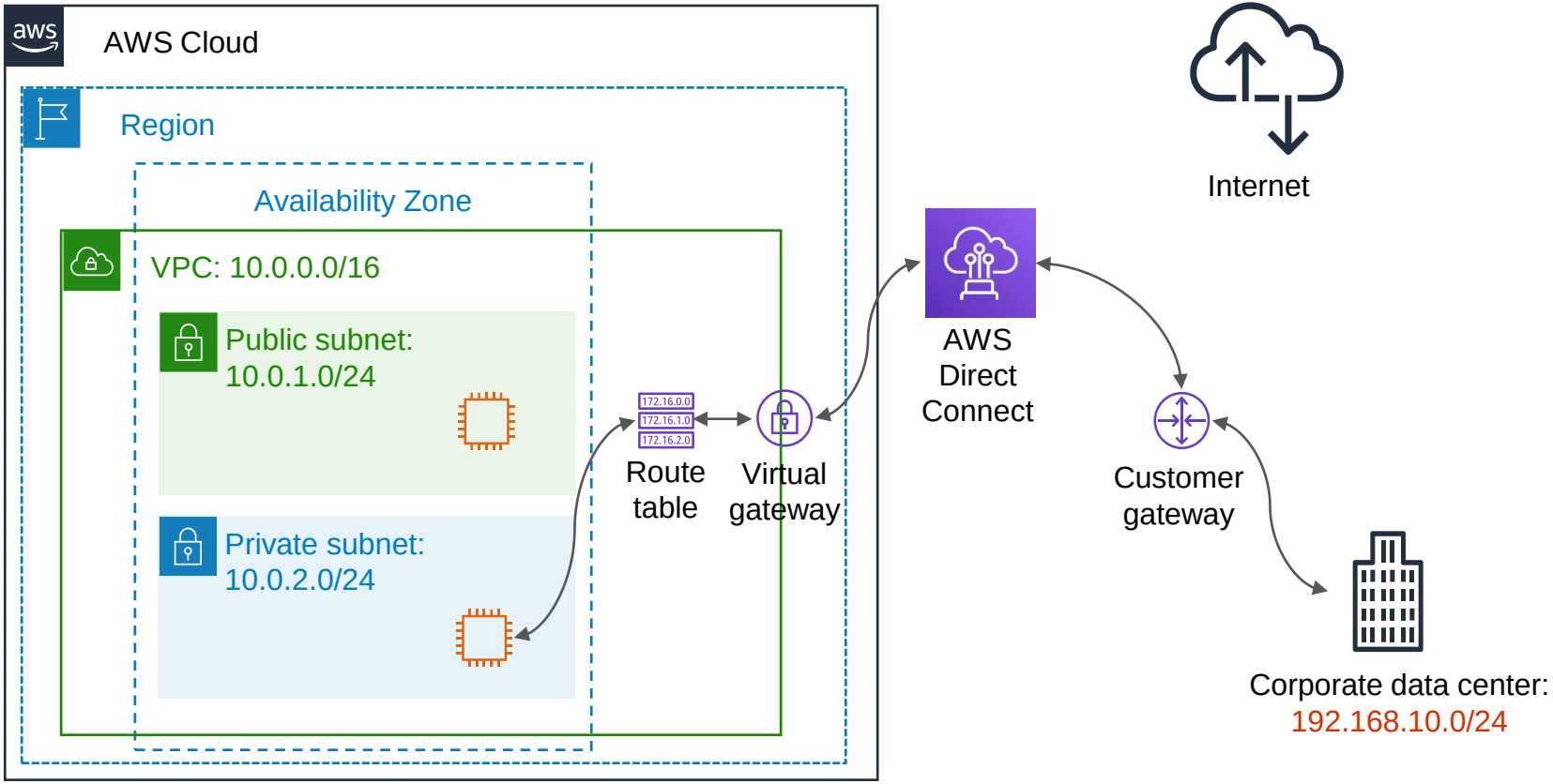
Public subnet route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-id

Private subnet route table

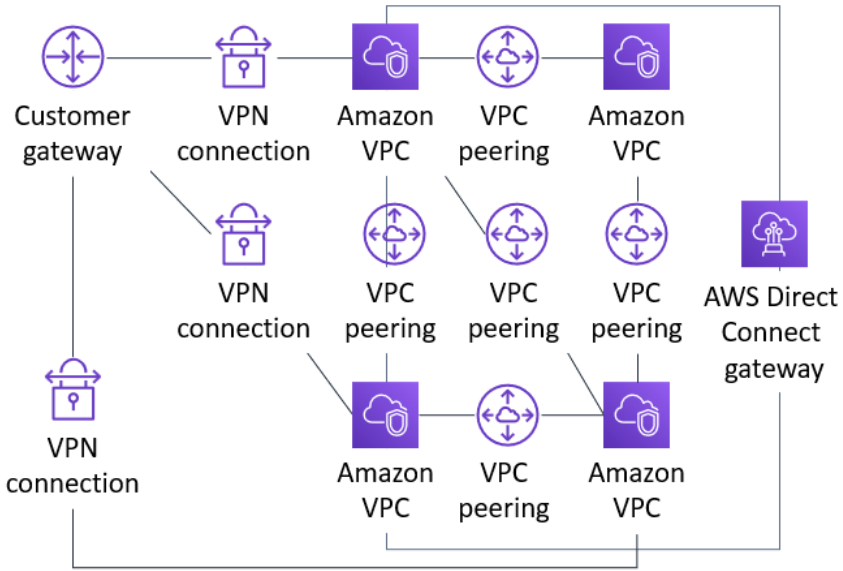
Destination	Target
10.0.0.0/16	local
192.168.10.0/24	vgw-id

AWS Direct Connect

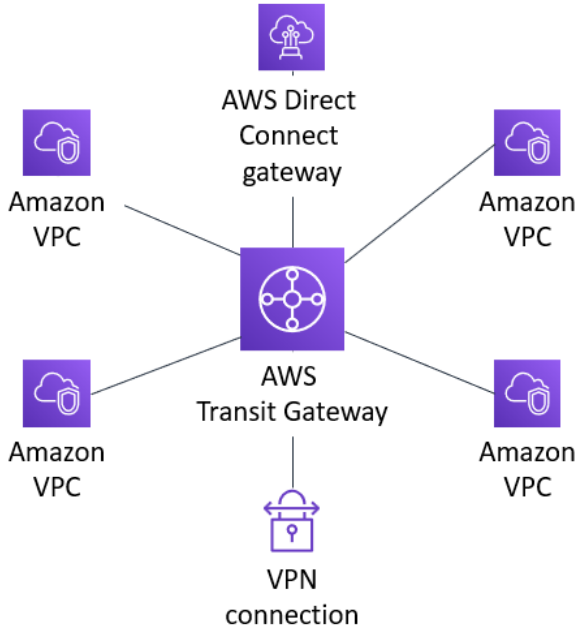


AWS Transit Gateway

From this…

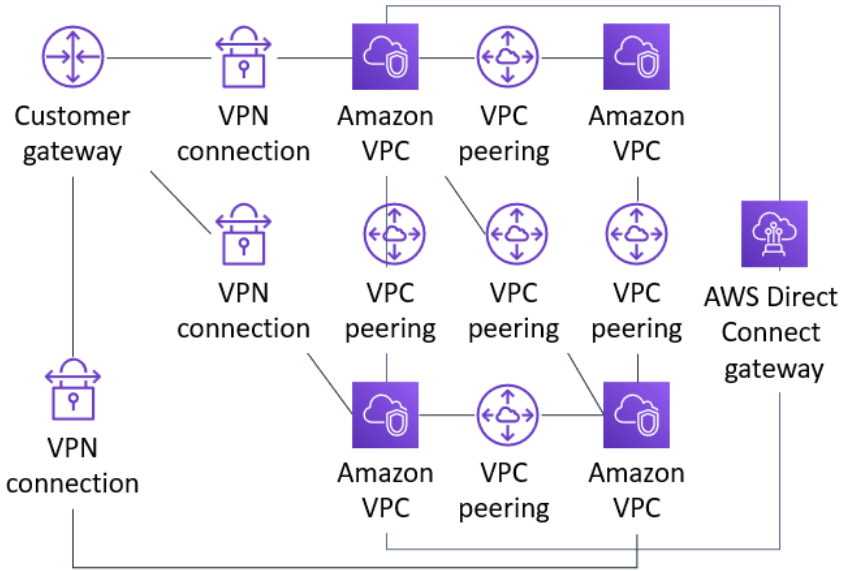


To this…

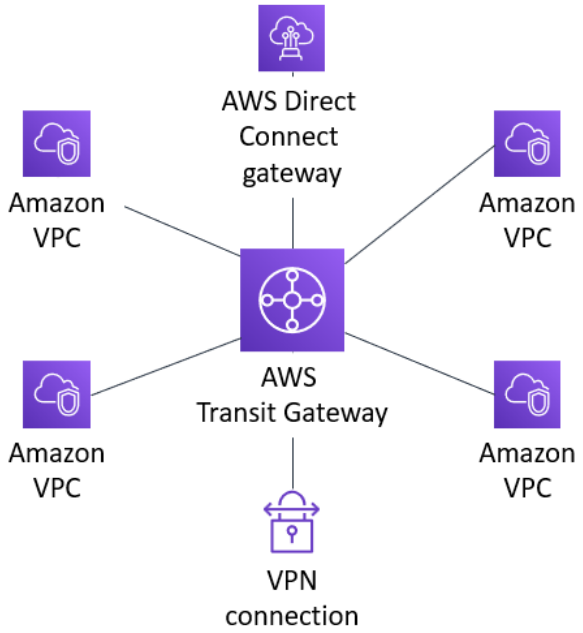


Lab 5: AWS Transit Gateway

From this...



To this...

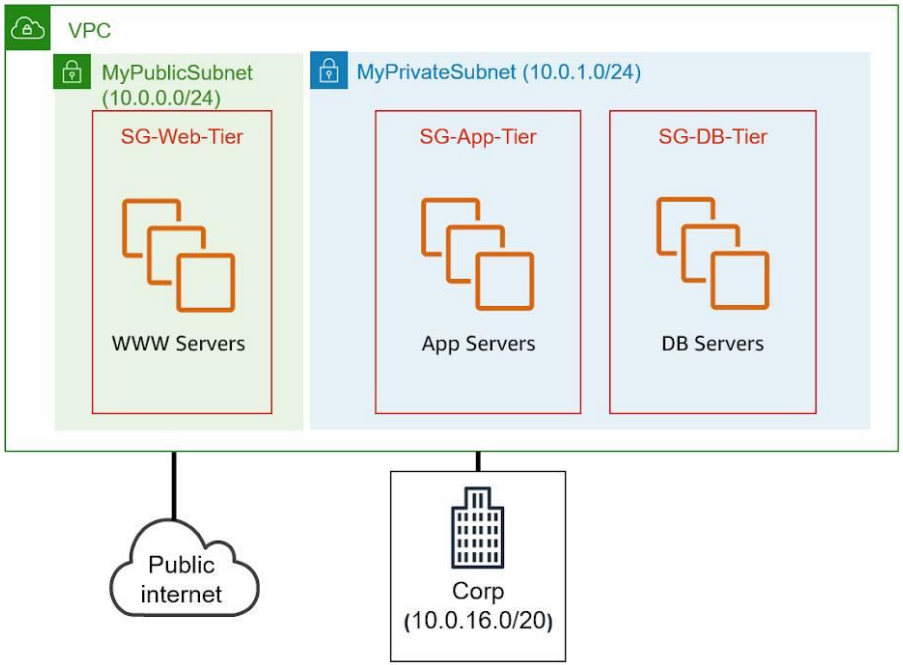


Section 4:

VPC Traffic Management

Security Group

Hoạt động như một lớp bảo mật ở mức Instance



SG-Web-Tier

Inbound		
Source	Protocol	Port Range
0.0.0.0/0	TCP	80
0.0.0.0/0	TCP	443
10.0.16.0/20	TCP	22

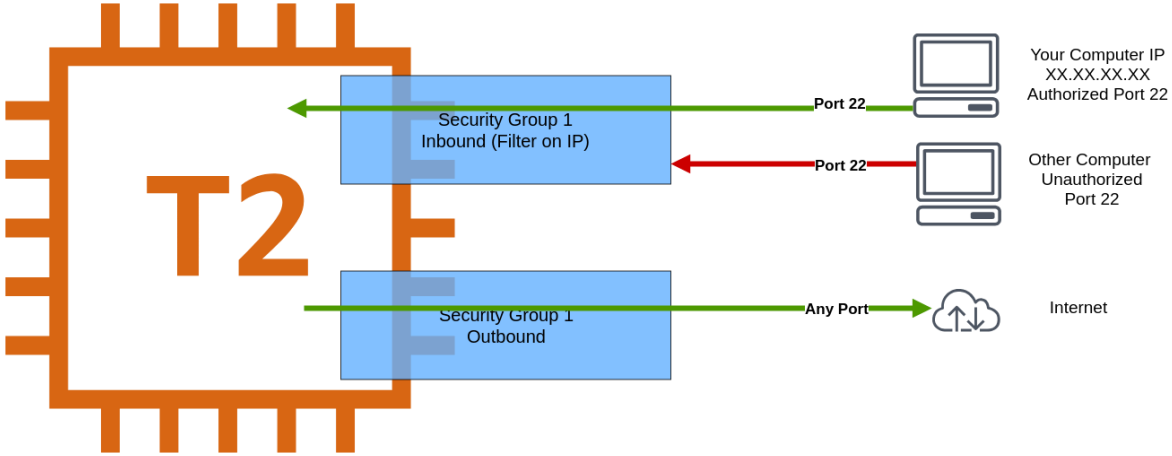
SG-App-Tier

Inbound		
Source	Protocol	Port Range
ID of SG-Web-Tier	TCP	6455
10.0.16.0/20	TCP	22

SG-DB-Tier

Inbound		
Source	Protocol	Port Range
ID of SG-App-Tier	TCP	3306
10.0.16.0/20	TCP	22

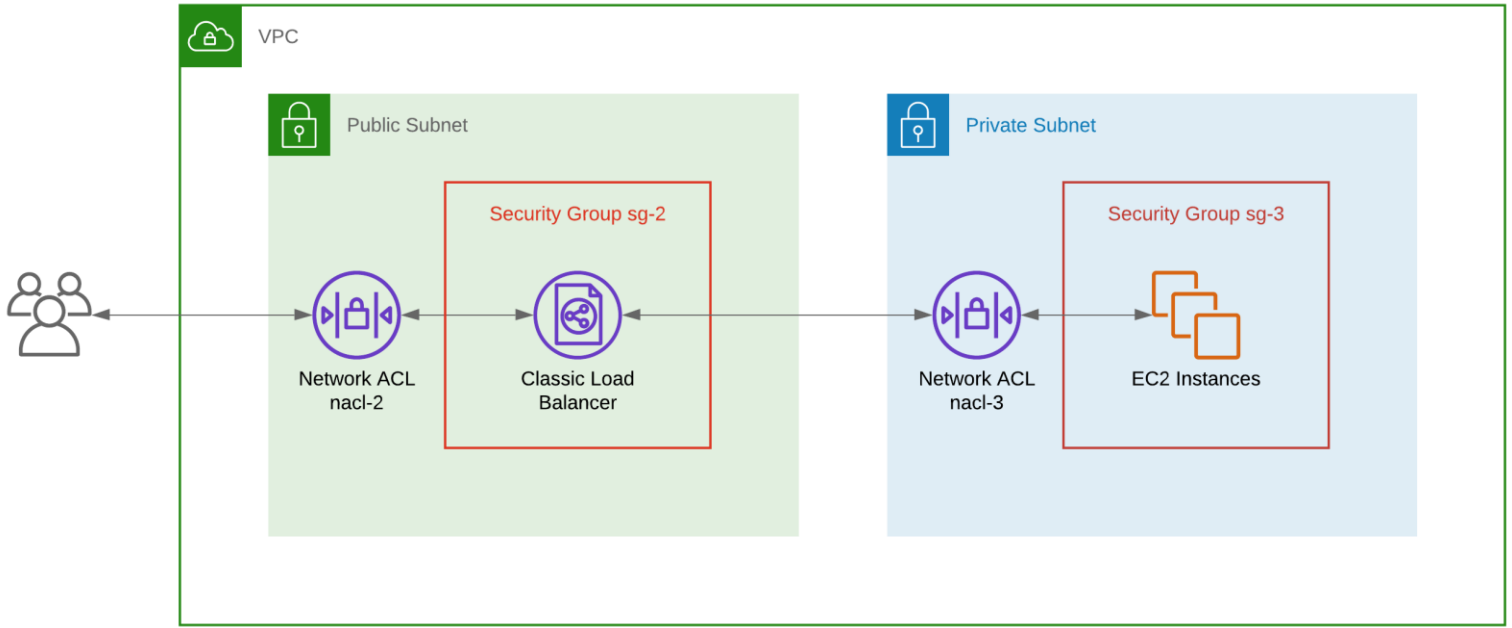
Security Group



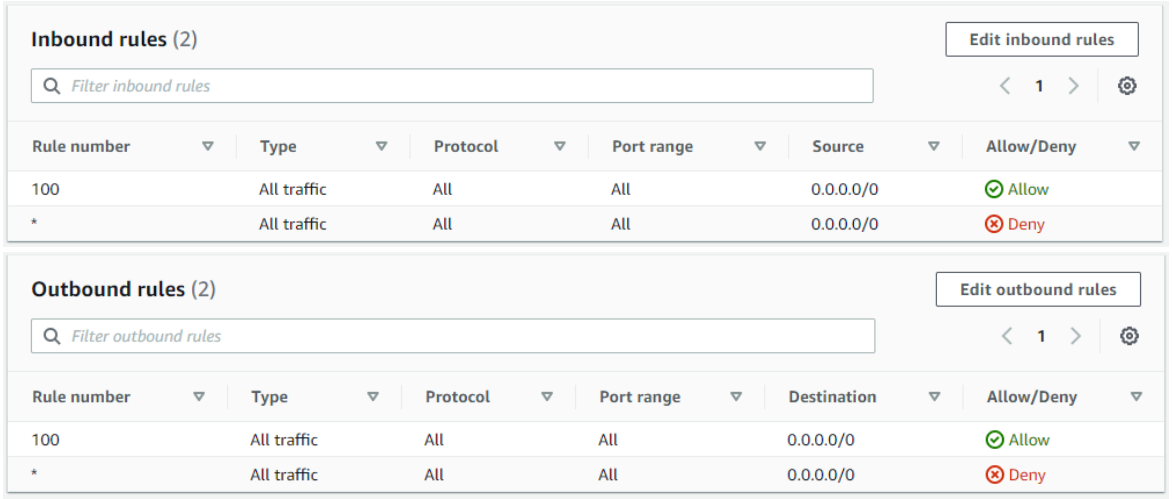
- Security Group bao gồm Inbound và Outbound rule
- Mặc định, SG denied toàn bộ Inbound và allow toàn bộ Outbound
- SG là stateful, tức nếu traffic được allow Inbound thì sẽ được allow Outbound
- SG chỉ có allow rule mà không có denied rule. Các rule không được định nghĩa sẽ được coi như là denied

Network Access Control List (ACL)

Hoạt động như một lớp bảo mật ở mức Subnet



Network Access Control List (ACL)



Inbound rules (2)

Edit inbound rules

Filter inbound rules

1

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Outbound rules (2)

Edit outbound rules

Filter outbound rules

1

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

- Security Group bao gồm Inbound và Outbound rule
- Mặc định, SG denied toàn bộ Inbound và allow toàn bộ Outbound
- ACL là stateless, tức muốn allow network cần allow trên cả Inbound và Inbound rule
- ACL có thể cấu hình cả allow rule và deny rule

Lab 6: Security Group vs ACL

Comparison of Security Groups and Network ACLs

The following table summarizes the basic differences between security groups and network ACLs.

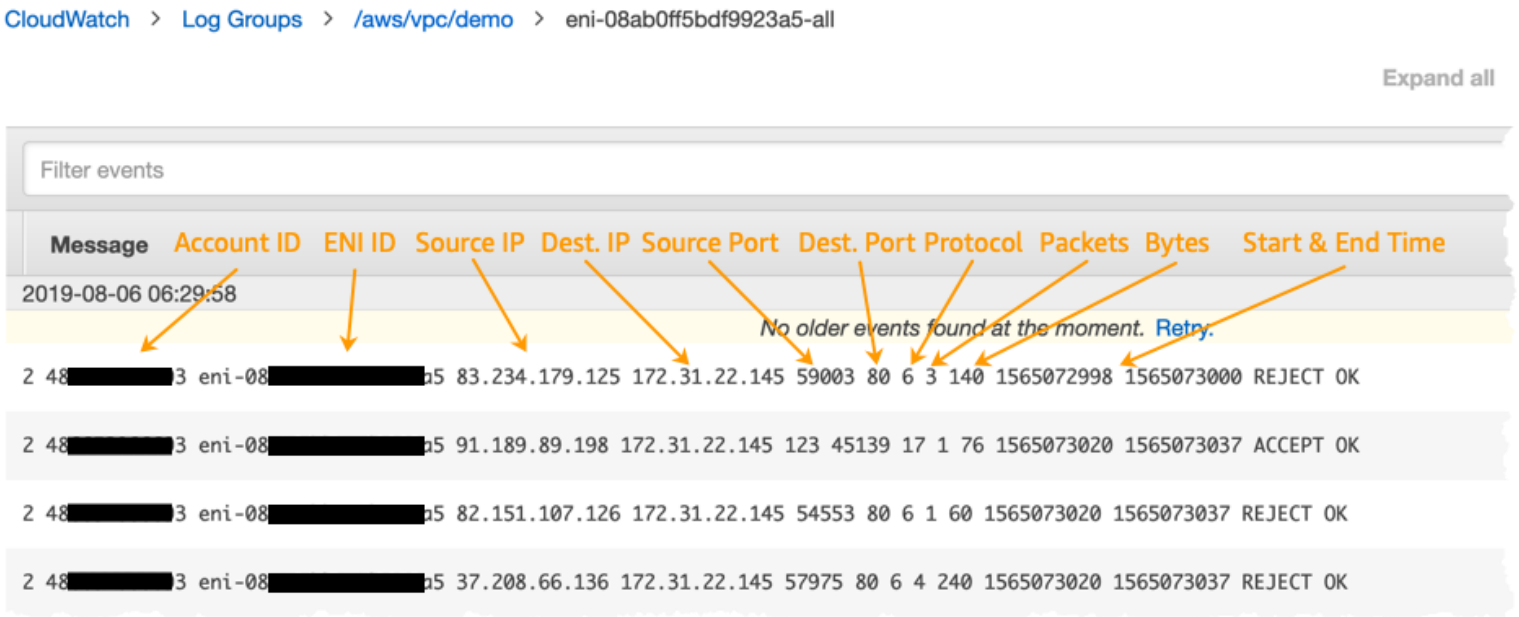
Security Group	Network ACL
Operates at the instance level (first layer of defense)	Operates at the subnet level (second layer of defense)
Supports allow rules only	Supports allow rules and deny rules
Is stateful: Return traffic is automatically allowed, regardless of any rules	Is stateless: Return traffic must be explicitly allowed by rules
We evaluate all rules before deciding whether to allow traffic	We process rules in number order when deciding whether to allow traffic
Applies to an instance only if someone specifies the security group when launching the instance, or associates the security group with the instance later on	Automatically applies to all instances in the subnets it's associated with (backup layer of defense, so you don't have to rely on someone specifying the security group)

VPC Flow Logs

- Capture lại thông tin traffic tới network interface ở nhiều level:
  - VPC flowlog
  - Subnet flowlog
  - ENI flowlog
- Giúp giám sát và khắc phục sự cố liên quan tới kết nối:
  - Subnet tới Internet
  - Subnet tới Subnet
  - Internet tới Subnet
- Các dịch vụ có sử dụng Network Interface đều có thể được capture lại log
- Dữ liệu log được capture có thể đẩy vào S3 hoặc CloudWatch

Lab 7: Demo VPC Flow Logs

- Ví dụ về VPC flow logs



Section 5:

VPC Pricing

VPC Service Pricing

NAT Gateway

Region: Asia Pacific (Singapore)

Price per NAT gateway ($/hour)	Price per GB data processed ($)
$0.059	$0.059

Traffic mgmt

Region: Asia Pacific (Singapore)

Hourly Price per ENI:	$0.018

IPAM

(New launch)

Region: Asia Pacific (Singapore)

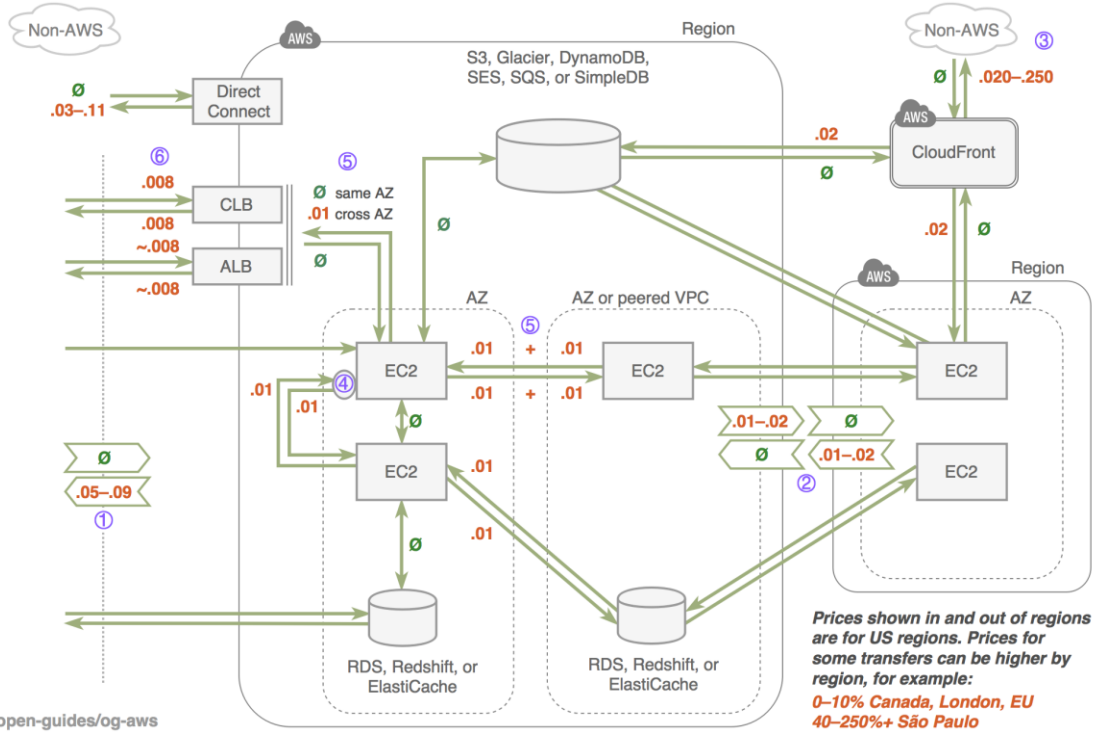
Hourly Price per active IP address managed by IPAM:	$0.00027

Data Transfer Pricing

AWS DATA TRANSFER COSTS

Numbers are data transfer in $/GB. Transaction and hourly prices are not shown. See notes.

- Ø Free. Inbound traffic is mostly free—you pay on the way out. Some but not all internal traffic is free.
- ① Direct outbound data starts at $.09/GB for <10TB, and discounts with volume. First 1GB free.
- ② Region-to-region traffic is $.02/GB when it exits a region for indicated services except between us-east-1 and us-east-2, where it's $.01/GB.
- ③ Outbound CloudFront prices are highly variable by geography and regional edge cache and start at $.085/GB in US/Canada.
- ④ Internal traffic via public or elastic IPs incurs additional fees in both directions.
- ⑤ Cross-AZ EC2 traffic within a region costs as much as region-to-region! ELB-EC2 traffic is free except outbound crossing AZs.
- ⑥ Elastic Load Balancing: Classic LB is priced per GB. Application LB costs are in LCUs, not $/GB.

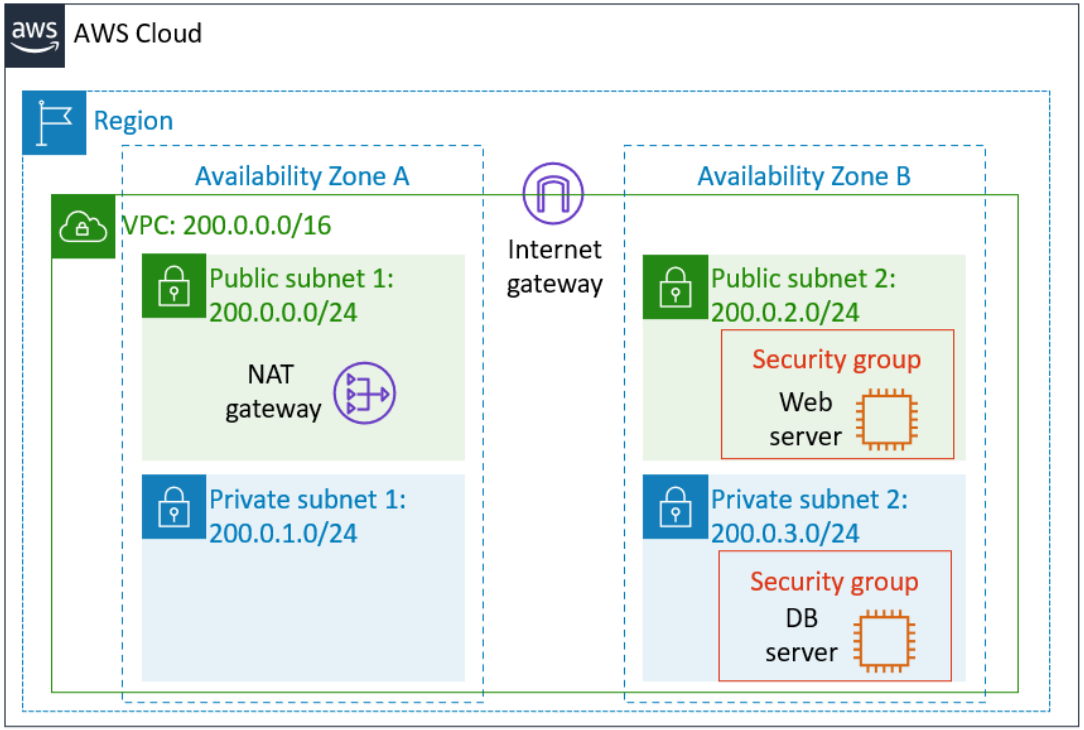


Credits and latest version: **github.com/open-guides/og-aws**
Last update: 2017-08-14

Section 6:

Tổng kết

Final Product



Public Route Table

Destination	Target
200.0.0.0/16	Local
0.0.0.0/0	Internet gateway

Private Route Table

Destination	Target
200.0.0.0/16	Local
0.0.0.0/0	NAT gateway

Tổng kết

Kết thúc bài học, sinh viên cần:

- Nắm được các kiến thức cơ bản về network
- Nắm được mô hình các dịch vụ network trên AWS (VPC)
- Có khả năng phác thảo kiến trúc của AWS VPC
- Tự thiết kế và từng bước triển khai được một VPC hoàn chỉnh
- Có khả năng triển khai tài nguyên nằm trong VPC
- Hiểu được vai trò của Security Group và Access Control List

Tài liệu tham khảo

- Amazon VPC User Guide
  https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html
- One to Many: Evolving VPC Design
  https://aws.amazon.com/vi/blogs/architecture/one-to-many-evolving-vpc-design/
- Building a Scalable and Secure Multi-VPC AWS Network Infrastructure
  https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure
- Best Practices for VPCs and Networking in Amazon WorkSpaces Deployments
  https://d1.awsstatic.com/whitepapers/best-practices-vpcs-networking-amazon-workspaces-deployments.pdf
- IPAM Re:invent 2021 (New launch)
  https://www.youtube.com/watch?v=xtLJgJfhPLg

Thank you