

Networking - Amazon VPC

Học tập cho AWS Certified Developer / Solutions Architect

📅 2025-10-17



Cloud



Networking



VPC



Certified

Nội dung trình bày

Danh sách các phần chính sẽ được trình bày trong bài về Amazon VPC

1. Tổng quan về Networking & Amazon VPC



Giới thiệu, các thành phần chính

2. CIDR và Subnet Mask



Lựa chọn dải IP cho VPC

3. Default VPC



VPC mặc định trong AWS

4. Subnets và IP Allocation



Sơ đồ VPC cơ bản

5. Internet Gateway & Route Table



Kết nối ra Internet

6. Bastion Host



SSH an toàn vào Private Subnet

7. NAT Gateway



Private Subnet truy cập Internet

8. Network ACL vs Security Group



So sánh SG và NACL

9. VPC Peering



Kết nối giữa các VPC

10. VPC Endpoints



Gateway vs. Interface Endpoints

11. VPC Flow Logs



Giám sát lưu lượng mạng

12. Site-to-Site VPN và Direct Connect



Kết nối Hybrid Cloud

13. Tổng kết phần VPC



Lời khuyên ôn thi

1. Tổng quan về Networking & Amazon VPC

Amazon VPC là gì?

Amazon VPC (Virtual Private Cloud) là một dịch vụ cho phép bạn triển khai các tài nguyên AWS trong một mạng ảo được cài đặt logic trong đám mây AWS.

Bạn có toàn quyền kiểm soát môi trường mạng ảo này, bao gồm:



Lựa chọn dải địa chỉ IP (CIDR Block)

Định nghĩa không gian địa chỉ IP cho VPC của bạn



Tạo các Subnet

Chia nhỏ dải IP thành các phân đoạn mạng con



Cấu hình Bảng định tuyến (Route Tables)

Kiểm soát cách lưu lượng mạng được định tuyến



Cấu hình Cổng mạng (Gateways)

Cho phép kết nối với Internet, các VPC khác hoặc mạng On-premises

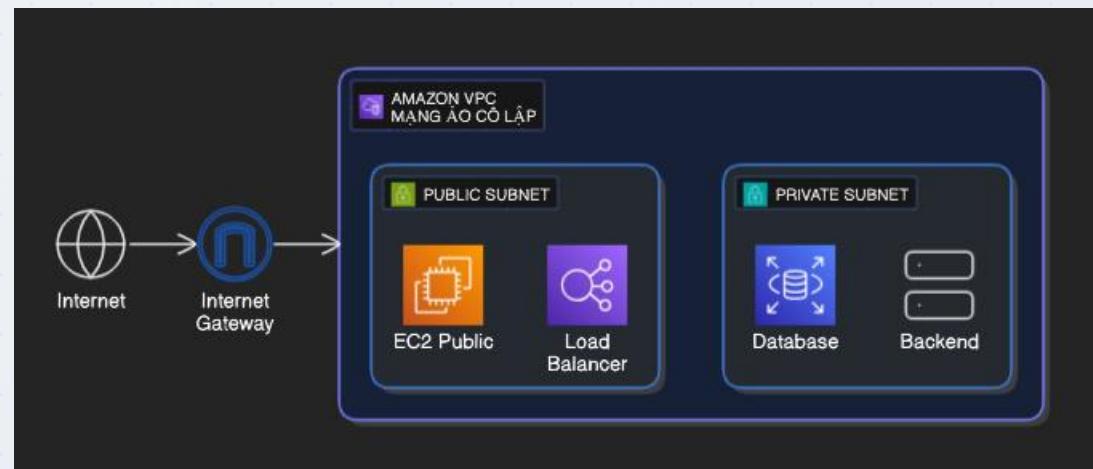


Thiết lập các lớp bảo mật

Sử dụng Security Groups và Network ACLs để kiểm soát truy cập



Vai trò của VPC trong kiến trúc mạng AWS

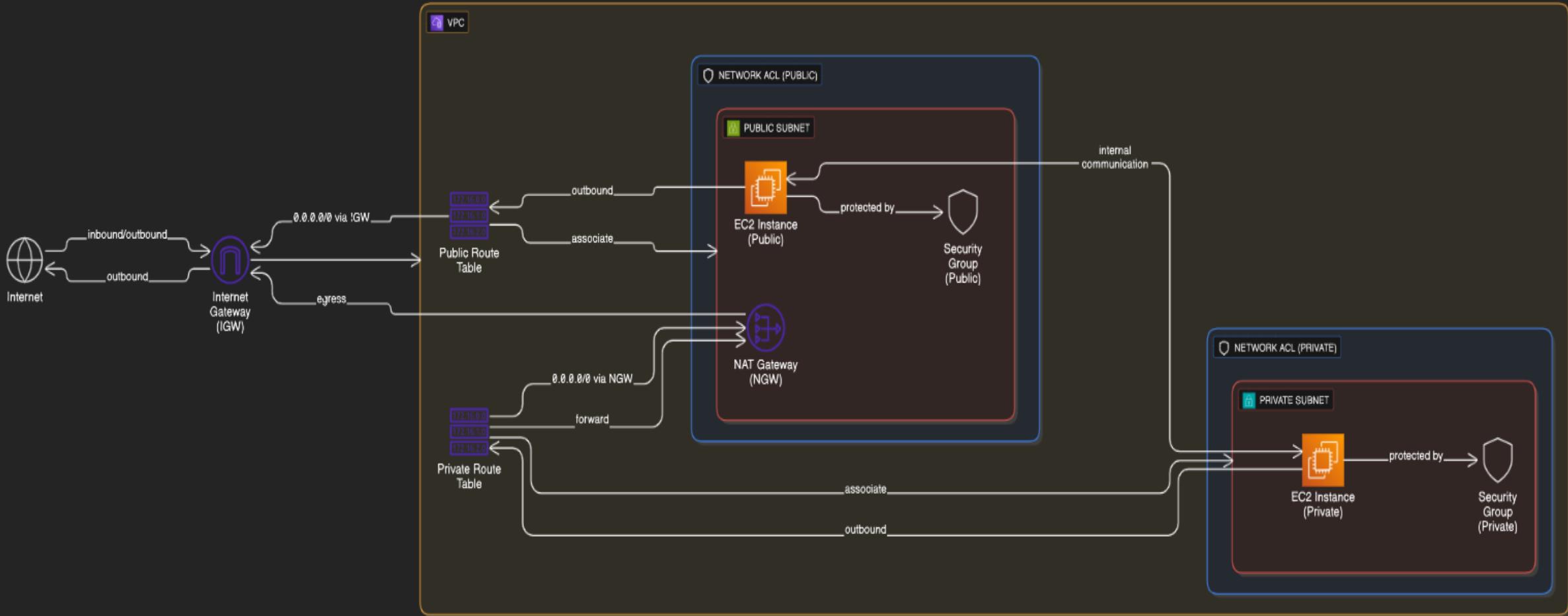


Lợi ích của VPC

VPC cung cấp cho bạn khả năng xây dựng một mạng ảo riêng biệt trên nền tảng đám mây AWS, mang lại sự kiểm soát và bảo mật cao cho các tài nguyên của bạn.

Các thành phần chính của VPC

Giới thiệu các thành phần cốt lõi của Amazon VPC và vai trò của chúng



Exam Tip: VPC là nền tảng cơ sở cho tất cả các dịch vụ mạng AWS. Mỗi tài khoản AWS được tạo ra với một VPC mặc định.

2. CIDR và Subnet Mask

Phân chia không gian địa chỉ IP trong VPC

i CIDR là gì?

CIDR (Classless Inter-Domain Routing) là một phương pháp biểu diễn dải địa chỉ IP, giúp phân bổ địa chỉ IP hiệu quả hơn.

↙ Ký hiệu CIDR

Địa chỉ IP / Độ dài tiền tố

Ví dụ: 10.0.0.0/16

呂 Địa chỉ IP

Phần đầu tiên xác định địa chỉ mạng

📘 Độ dài tiền tố

Số bit đầu tiên dùng để xác định mạng

💻 Ý nghĩa trong VPC

VPC CIDR

Xác định toàn bộ không gian địa chỉ IP cho VPC

Subnet CIDR

Là một phần nhỏ hơn của VPC CIDR

Ví dụ về CIDR

Nếu VPC có CIDR 10.0.0.0/24 (256 địa chỉ IP), bạn có thể chia thành hai Subnet /25:

Subnet 1:

10.0.0.0/25

128 địa chỉ IP (10.0.0.0-127)

Subnet 2:

10.0.0.128/25

128 địa chỉ IP (128-255)

田 Độ dài tiền tố (Prefix Length)

/16

65.536 địa chỉ

/24

256 địa chỉ

/28

16 địa chỉ

⚠ Lưu ý quan trọng

Trong AWS, một số dải IP được sử dụng bởi các dịch vụ cụ thể. Ví dụ, AWS Cloud9 sử dụng dải 172.17.0.0/16. Nên tránh sử dụng dải IP này.

Lựa chọn dải IP cho VPC

Hướng dẫn lựa chọn dải địa chỉ IP phù hợp cho VPC

💡 Nguyên tắc thiết kế không gian địa chỉ

✓ Sử dụng dải IP riêng tư (RFC 1918)

AWS khuyến nghị sử dụng các dải địa chỉ IPv4 riêng tư để tránh xung đột với các địa chỉ IP công cộng

✓ Kích thước VPC CIDR

Khi tạo VPC, chỉ định một khối CIDR IPv4 chính với kích thước từ /16 (65.536 địa chỉ) đến /28 (16 địa chỉ)

✗ Khối CIDR bị hạn chế

Không thể sử dụng các dải như 0.0.0.0/8, 127.0.0.0/8, 169.254.0.0/16, 224.0.0.0/4

⚠ Tránh xung đột dịch vụ

Một số dịch vụ AWS (ví dụ: AWS Cloud9, Amazon SageMaker AI) sử dụng dải 172.17.0.0/16. Nên tránh dải này

+ Khối CIDR phụ (Secondary CIDR blocks)

Bạn có thể thêm các khối CIDR phụ vào VPC nếu cần mở rộng không gian địa chỉ

Exam Tip: Khi chuẩn bị cho kỳ thi, hãy nhớ rằng việc lựa chọn dải IP là một quyết định quan trọng ảnh hưởng đến khả năng mở rộng và kết nối.

🌐 Dải RFC 1918 được khuyến nghị

Dải RFC 1918

10.0.0.0 - 10.255.255.255 (10/8)

Ví dụ khối CIDR

10.0.0.0/16

172.16.0.0 - 172.31.255.255 (172.16/12)

172.31.0.0/16

192.168.0.0 - 192.168.255.255 (192.168/16)

192.168.0.0/20

Cách phân bổ dải IP trong VPC



3. Default VPC

Mô tả Default VPC, các đặc điểm và cấu hình mặc định

Giới thiệu về Default VPC



Tự động tạo: Khi bạn tạo tài khoản AWS mới, một VPC mặc định (Default VPC) được tự động tạo ra trong mỗi khu vực (Region).



Cấu hình sẵn: Đã được cấu hình với các thành phần cơ bản như Internet Gateway, Route Table mặc định, và các Subnet trong mỗi Zone khả dụng.



Nhanh chóng bắt đầu: Cho phép bạn bắt đầu sử dụng dịch vụ AWS Networking mà không cần phải cấu hình từ đầu.

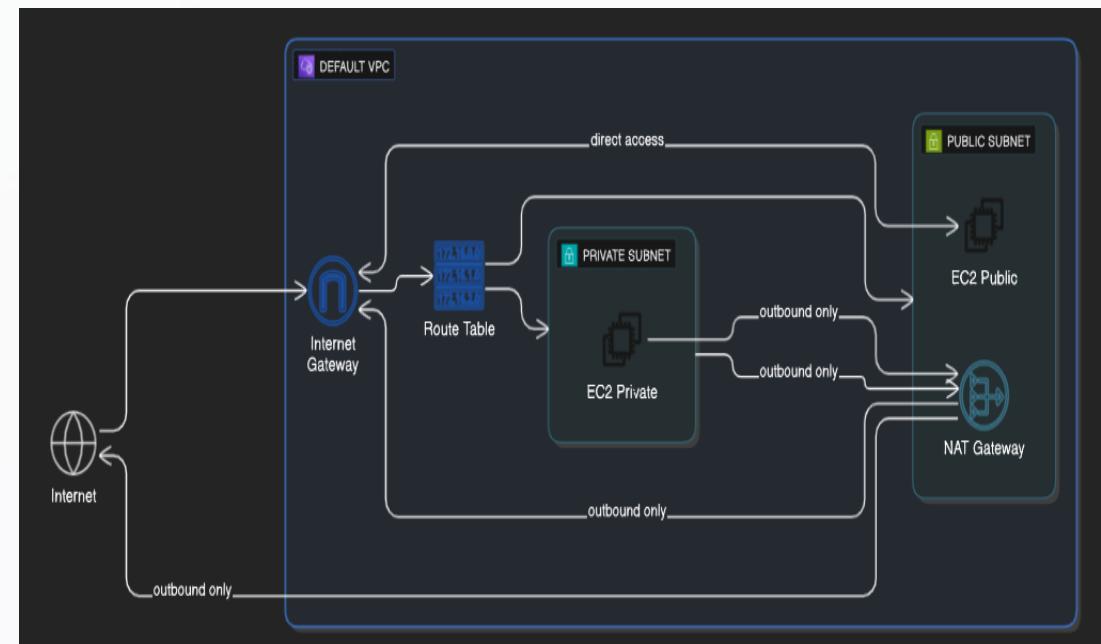


Giới hạn: Mặc dù dễ dàng sử dụng, nhưng Default VPC có thể không phù hợp cho các triển khai phức tạp hoặc yêu cầu bảo mật cao.



Bảo mật: Sử dụng Security Groups và Network ACLs mặc định để kiểm soát truy cập vào các tài nguyên của bạn.

Cấu trúc Default VPC



Default VPC được tạo tự động khi bạn đăng ký tài khoản AWS mới

4. Subnets và IP Allocation

Phân chia VPC thành các subnet và quản lý địa chỉ IP

Giới thiệu về Subnet

Subnet là một dải địa chỉ IP trong VPC, được triển khai trong một Availability Zone cụ thể. Subnet cho phép bạn phân đoạn mạng VPC để tổ chức tài nguyên và áp dụng các quy tắc bảo mật khác nhau.

Loại Subnet

Public Subnet

- Chứa tài nguyên cần truy cập trực tiếp từ Internet
- Yêu cầu Route Table trỏ đến Internet Gateway
- Các instance thường được gán Public IP

Private Subnet

- Chứa tài nguyên không cần truy cập trực tiếp từ Internet
- Truy cập Internet thông qua NAT Gateway
- Các instance chỉ có Private IP

Địa chỉ IP trong Subnet

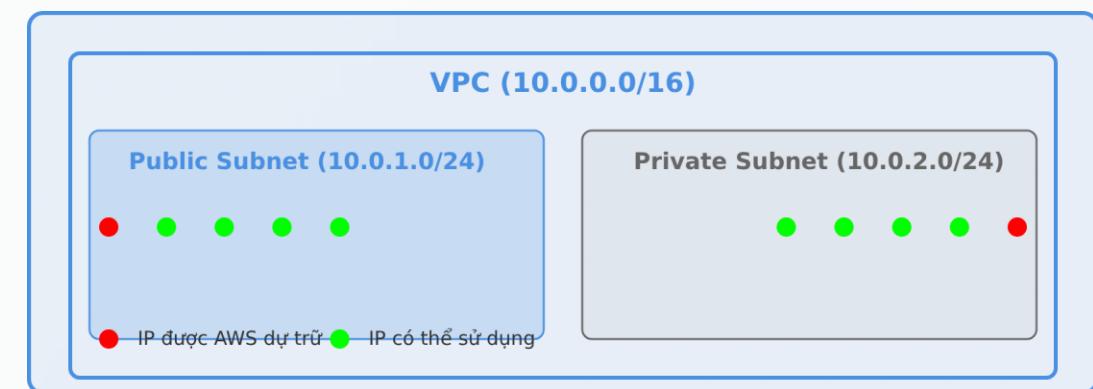
Trong mỗi khối CIDR của subnet, 5 địa chỉ IP đầu tiên và cuối cùng được AWS dự trữ và không thể gán cho tài nguyên:



- .0: Địa chỉ mạng

1: Địa chỉ广播 (Broadcast)

Phân chia VPC thành Subnets



Best Practice

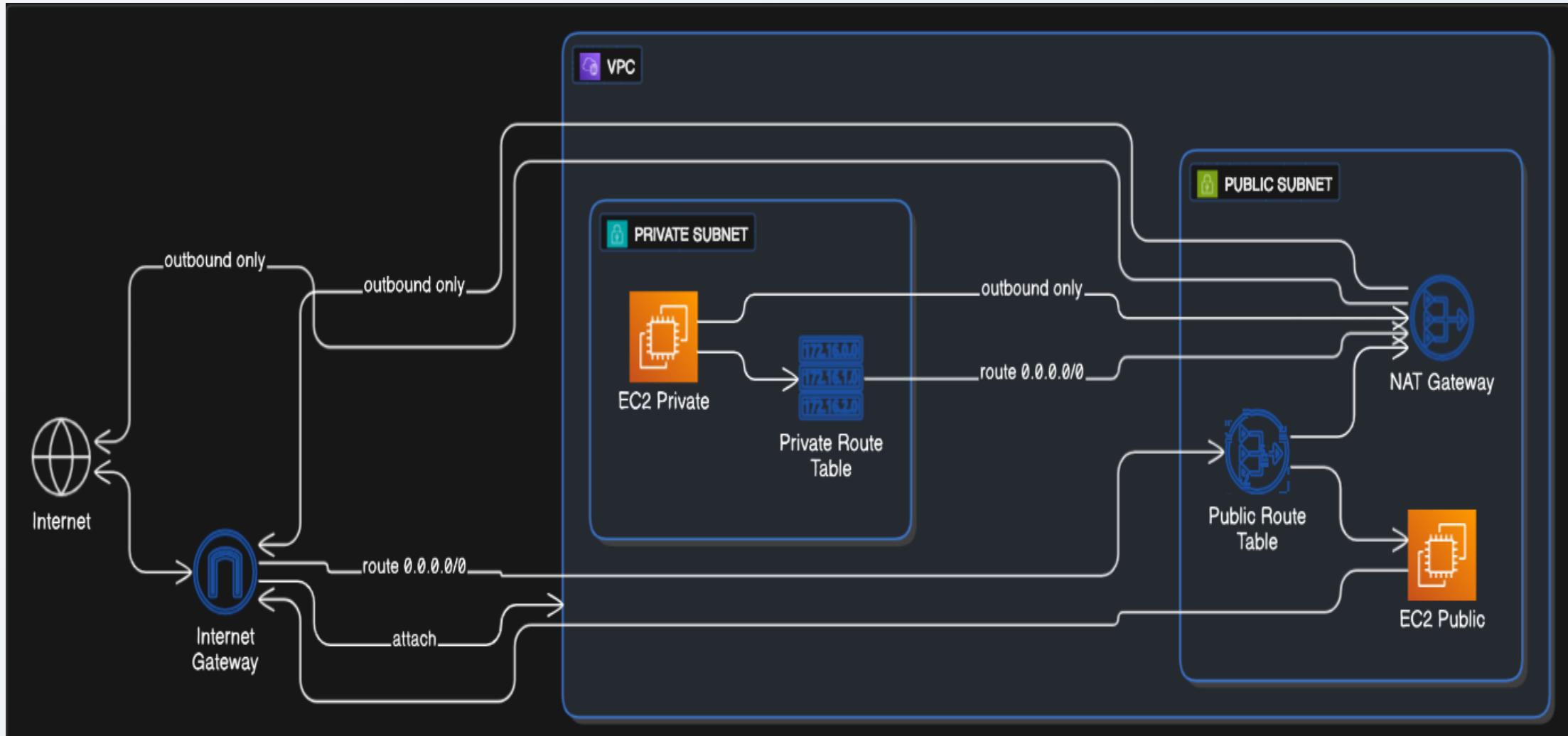


- Phân chia VPC thành Public và Private Subnet
- Public Subnet: chứa các tài nguyên cần truy cập từ Internet
- Private Subnet: chứa các tài nguyên không cần truy cập từ Internet
- Sử dụng NAT Gateway để cho phép Private Subnet truy cập Internet
- Áp dụng các quy tắc bảo mật khác nhau cho các subnet

Exam Tip: Khi tạo subnet, bạn phải chỉ định một khối CIDR IPv4 chính. Kích thước subnet CIDR phải nhỏ hơn hoặc bằng kích thước VPC CIDR.

Sơ đồ VPC cơ bản

Mô hình cấu trúc VPC điển hình với Public và Private Subnet



5. Internet Gateway & Route Table

Kết nối VPC với Internet



Internet Gateway

Cổng mạng cho phép giao tiếp giữa VPC và Internet

Chức năng chính:

- Cung cấp đích đến cho lưu lượng truy cập có thể định tuyến công khai
- Thực hiện Network Address Translation (NAT) cho các instance có địa chỉ IP công cộng

Cấu hình:

- Tạo Internet Gateway trong console
- Liên kết với VPC thông qua bảng định tuyến



Route Table

Chứa các quy tắc xác định hướng đi của lưu lượng mạng

Cấu trúc:

- Mỗi mục chứa một quy tắc định tuyến
- Bao gồm mạng đích (destination) và cổng đích (target)

Ví dụ cấu hình:

- Public Subnet: 0.0.0.0/0 → IGW
- Private Subnet: 0.0.0.0/0 → NAT Gateway

Exam Tip: Internet Gateway là một dịch vụ được quản lý hoàn toàn bởi AWS, có khả năng mở rộng theo chiều ngang và tính sẵn sàng cao

6. Bastion Host

Truy cập an toàn vào Private Subnet

Định nghĩa

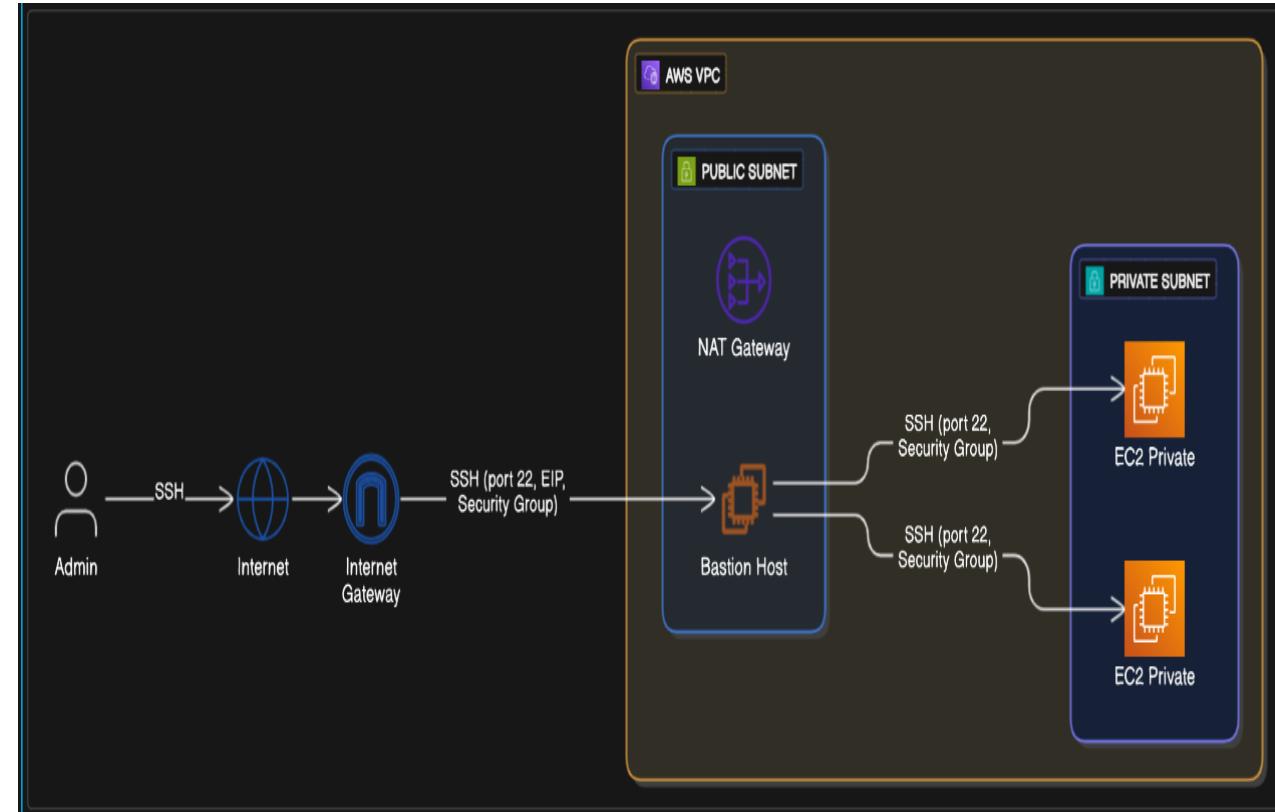
EC2 instance được đặt trong Public Subnet, đóng vai trò là điểm truy cập duy nhất để quản trị viên có thể kết nối SSH (hoặc RDP) một cách an toàn đến các instance trong Private Subnet.

Vai trò chính

- Cung cấp một điểm vào được bảo mật và kiểm soát cho các tài nguyên trong mạng riêng
- Giảm thiểu bèle tấn công bằng cách không mở trực tiếp các cổng quản trị (SSH/RDP) cho các instance riêng tư ra Internet
- Cho phép ghi nhật ký và kiểm toán các phiên truy cập quản trị

Best Practice

- Cấu hình Security Group của Bastion Host cực kỳ hạn chế, chỉ cho phép inbound SSH/RDP từ các dải IP nguồn cụ thể
- Cấu hình Security Group của các instance trong Private Subnet chỉ cho phép inbound SSH/RDP từ Security Group của Bastion Host



- 1. Quản trị viên kết nối SSH/RDP đến Bastion Host (có Public IP) từ máy tính cục bộ
- 2. Từ Bastion Host, quản trị viên khởi tạo kết nối SSH/RDP đến instance trong Private Subnet
- 3. Lưu lượng giữa Bastion Host và các instance riêng tư diễn ra hoàn toàn trong

7. NAT Gateway

Kết nối ra Internet từ Private Subnet

Định nghĩa

NAT Gateway (Network Address Translation Gateway) là một dịch vụ được quản lý hoàn toàn bởi AWS, cho phép các instance trong Private Subnet kết nối ra Internet hoặc các dịch vụ AWS khác, nhưng ngăn chặn các kết nối đến không mong muốn từ Internet.

Chức năng

Translation

Dịch địa chỉ IP riêng tư thành địa chỉ Elastic IP công cộng

Stateless

Không trạng thái, xử lý mỗi gói riêng biệt

Bảo mật

Ngăn chặn inbound traffic từ Internet

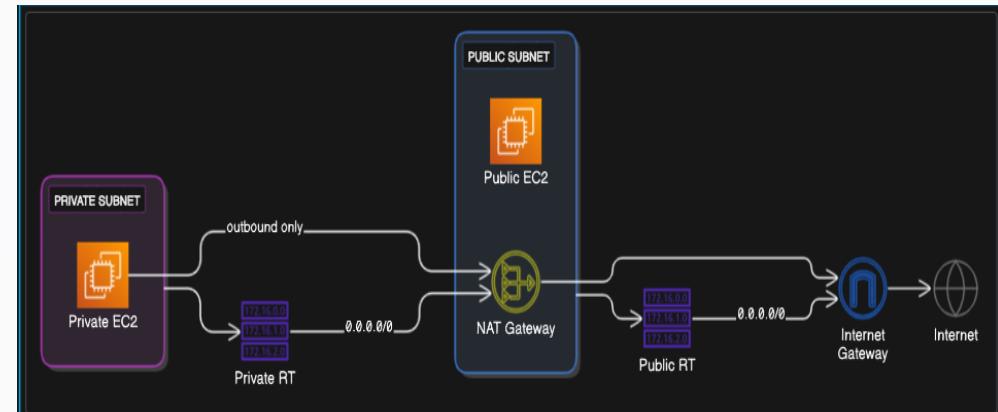
Dual stack

Hỗ trợ IPv4 và IPv6 (DNS64 và NAT64)

Trường hợp sử dụng

-  Cập nhật hệ điều hành hoặc phần mềm trên các instance trong Private Subnet
-  Tải xuống các gói phần mềm hoặc thư viện từ Internet
-  Gọi các API của các dịch vụ bên ngoài AWS

Sơ đồ NAT Gateway



 Lưu ý: NAT Gateway phải được triển khai trong một Public Subnet và yêu cầu một Elastic IP address được gán khi tạo.

Luồng hoạt động NAT Gateway

Quy trình chuyển tiếp lưu lượng từ Private Subnet ra Internet

1. Lưu lượng ra Internet

Bước 1: Instance trong Private Subnet khởi tạo kết nối



ví dụ: ping google.com

Bước 2: Lưu lượng được định tuyến đến NAT Gateway



dựa trên Route Table của Private Subnet

Bước 3: NAT Gateway dịch địa chỉ IP riêng tư thành địa chỉ Elastic IP công cộng của NAT Gateway



Bước 4: NAT Gateway gửi lưu lượng đến Internet Gateway
Internet Gateway chuyển tiếp ra Internet



2. Lưu lượng về Private Subnet

Bước 8: NAT Gateway dịch địa chỉ Elastic IP
trở lại địa chỉ IP riêng tư ban đầu của instance



Bước 7: NAT Gateway gửi lưu lượng phản hồi
đến instance trong Private Subnet



Bước 6: Internet Gateway chuyển tiếp về NAT Gateway
lưu lượng phản hồi từ Internet



Bước 5: Internet gửi phản hồi về Internet Gateway
hoàn thành kết nối



8. Network ACL vs Security Group

So sánh hai lớp bảo mật quan trọng trong VPC



Network ACL (NACL)

Tường lửa ảo ở cấp độ subnet, kiểm soát lưu lượng vào và ra cho toàn bộ subnet.

- 🕒 **Cấp độ áp dụng:** Subnet level (áp dụng cho toàn bộ subnet)
- ☒ **Statefulness:** Stateless (không trạng thái)
- ✓ **Quy tắc:** Có cả quy tắc Allow và Deny
- ↑ **Thứ tự đánh giá:** Từ thấp đến cao, dừng lại khi có quy tắc khớp

Ví dụ: Để chặn một dải IP độc hại cụ thể truy cập vào subnet của bạn, bạn có thể tạo quy tắc DENY trước.



Security Group (SG)

Tường lửa ảo ở cấp độ instance, kiểm soát lưu lượng vào và ra cho một hoặc nhiều Elastic Network Interface.

- 🕒 **Cấp độ áp dụng:** Instance level (áp dụng cho ENI của instance)
- ⟳ **Statefulness:** Stateful (có trạng thái)
- ✓ **Quy tắc:** Chỉ có quy tắc Allow (ngầm định từ chối tất cả những gì không được phép)
- 🔍 **Thứ tự đánh giá:** Đánh giá tất cả các quy tắc để xác định cho phép hay không

Ví dụ: Web Server SG cho phép HTTP/HTTPS inbound traffic từ mọi nơi và SSH từ IP quản trị viên.

VS

Exam Tip: Network ACL và Security Group hoạt động cùng nhau để tạo ra một chiến lược bảo mật đa lớp (defense-in-depth).

Bảng so sánh SG và NACL

So sánh chi tiết giữa Security Group và Network ACL



Security Group (SG)

Tường lửa ảo cấp instance



Network ACL (NACL)

Tường lửa ảo cấp subnet

Đặc điểm	Security Group (SG)	Network ACL (NACL)
Cấp độ áp dụng	Instance level áp dụng cho Elastic Network Interface của instance	Subnet level áp dụng cho toàn bộ subnet
Statefulness	Stateful có trạng thái, lưu giữ thông tin phiên	Stateless không trạng thái, đánh giá mỗi gói riêng
Quy tắc	Chỉ có quy tắc Allow ngầm định từ chối tất cả những gì không được phép	Có cả quy tắc Allow và Deny phải cấu hình cả inbound và outbound riêng biệt
Thứ tự đánh giá	Đánh giá tất cả các quy tắc để xác định cho phép hay không	Đánh giá theo thứ tự số thứ tự từ thấp đến cao, dừng lại khi có quy tắc khớp
Mặc định	Mặc định cho phép outbound traffic inbound cần được cấu hình cụ thể	Mặc định từ chối tất cả traffic phải cấu hình rõ ràng cả inbound và outbound

9. VPC Peering

Kết nối giữa các VPC để giao tiếp qua mạng riêng của AWS

i VPC Peering là gì?

VPC Peering là một kết nối mạng giữa hai VPC, cho phép chúng giao tiếp với nhau bằng địa chỉ IP riêng tư như thể chúng nằm trong cùng một mạng.

Exam Tip

Luôn nhớ rằng VPC Peering là "non-transitive". Nếu VPC A kết nối với VPC B, và VPC B kết nối với VPC C, thì VPC A không thể giao tiếp với VPC C thông qua VPC B.

✓ Điều kiện thiết kế

- Không trùng lặp các khối CIDR của hai VPC
- Có thể kết nối VPC trong cùng tài khoản hoặc giữa các tài khoản khác nhau
- Hoặc giữa các vùng AWS khác nhau (Inter-Region VPC Peering)

⚙️ Đặc điểm chính



Kết nối riêng tư

Lưu lượng không đi qua Internet công cộng, mà sử dụng mạng backbone của AWS



Không bắc cầu

Cần kết nối trực tiếp giữa các VPC nếu muốn chúng giao tiếp



Không chồng chéo CIDR

Các khối CIDR của hai VPC được peering không được phép trùng lặp



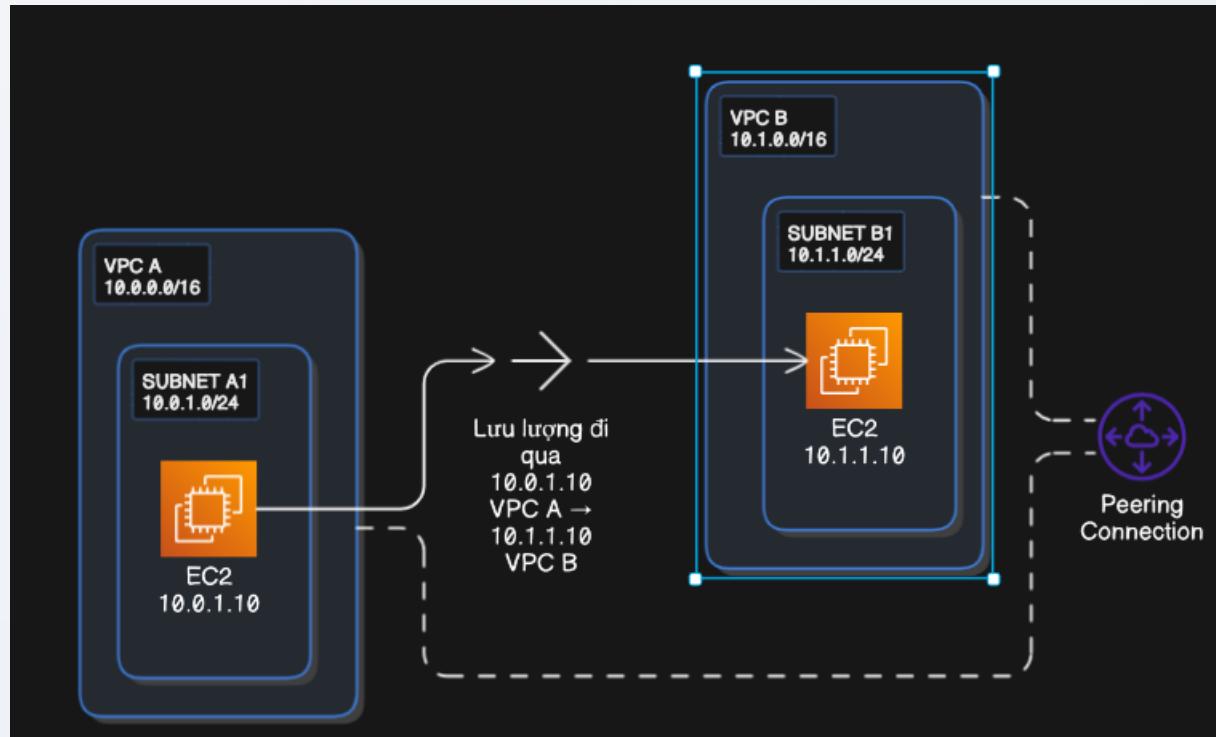
Hỗ trợ đa tài khoản/đa vùng

Có thể kết nối giữa các tài khoản khác nhau hoặc giữa các vùng AWS khác nhau



Sơ đồ VPC Peering

Kết nối giữa các VPC để giao tiếp bằng địa chỉ IP riêng tư



Đặc điểm chính của VPC Peering:

Không bắc cầu: VPC A không thể giao tiếp với VPC C thông qua VPC B

Kết nối riêng tư: Lưu lượng không đi qua Internet, sử dụng mạng backbone của AWS

Không chồng chéo CIDR: Các khối CIDR của hai VPC không được phép trùng lặp

Hỗ trợ đa tài khoản/đa vùng: Có thể kết nối giữa các tài khoản khác nhau hoặc giữa các vùng AWS khác nhau

10. VPC Endpoints

Kết nối riêng tư đến các dịch vụ AWS mà không cần qua Internet

Giới thiệu

VPC Endpoints cho phép bạn kết nối riêng tư VPC của mình với các dịch vụ AWS được hỗ trợ và các dịch vụ được cung cấp bởi AWS PrivateLink mà không cần đi qua Internet. Điều này giúp tăng cường bảo mật và giảm độ phức tạp của mạng.

Lợi ích chính



Tăng cường bảo mật

Lưu lượng không đi qua Internet công cộng, giảm thiểu rủi ro bảo mật



Tăng tốc độ

Tránh độ trễ của Internet, kết nối trực tiếp với dịch vụ AWS



Giảm độ phức tạp

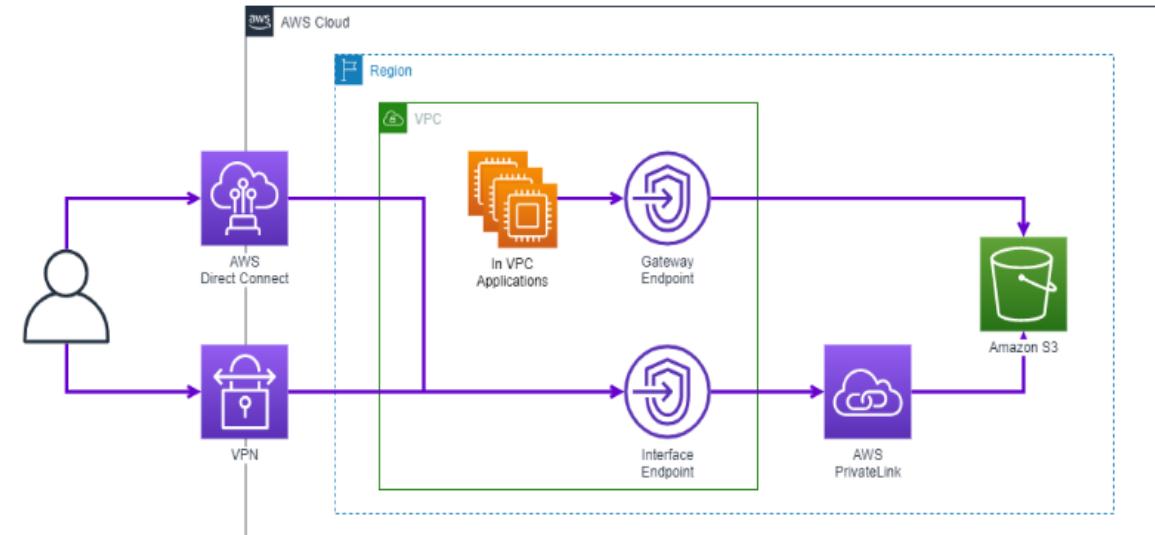
Không cần NAT Gateway, Bastion Host hoặc VPN cho kết nối này



Tiết kiệm chi phí

Tránh chi phí kết nối qua Internet, đặc biệt là cho lưu lượng lớn

Cách hoạt động



Exam Tip: VPC Endpoints sử dụng mạng backbone riêng của AWS, không đi qua Internet công cộng, giúp tăng cường bảo mật và hiệu suất cho các kết nối đến dịch vụ AWS.

Gateway vs. Interface Endpoints

So sánh hai loại VPC Endpoints, đặc điểm và trường hợp sử dụng

S3 Gateway Endpoints	S3 Interface Endpoints
Network traffic remains on the AWS network.	Network traffic remains on the AWS network.
Uses Amazon S3 public IP addresses	Uses private IP addresses from the VPC to access Amazon S3
Does not allow access from on-premises	Allow access from on-premises
Does not allow access from another AWS Region	Allow access from a VPC in another AWS Region using VPC peering or AWS Transit Gateway
Not billed	Billed

11. VPC Flow Logs

Ghi lại thông tin lưu lượng IP trong VPC

Giới thiệu

VPC Flow Logs là tính năng quan trọng cho phép ghi lại thông tin chi tiết về lưu lượng IP đi vào và ra khỏi các giao diện mạng (Elastic Network Interfaces - ENI) trong VPC.

Chức năng chính

- ✓ Ghi lại các bản ghi về lưu lượng IP (nguồn, đích, cổng, giao thức, hành động ACCEPT/REJECT)
- ✓ Giúp chẩn đoán các quy tắc Security Group hoặc Network ACL quá hạn chế hoặc quá lỏng lẻo
- ✓ Theo dõi lưu lượng truy cập đến các instance của bạn
- ✓ Xác định hướng của lưu lượng đến và đi từ các giao diện mạng

Exam Tip: Flow Logs được thu thập bên ngoài đường dẫn lưu lượng mạng, do đó không ảnh hưởng đến thông lượng hoặc độ trễ mạng.

Nơi lưu trữ Logs



CloudWatch Logs

Phân tích và giám sát theo thời gian thực



Amazon S3

Lưu trữ lâu dài và phân tích bằng các công cụ khác

Ứng dụng



Bảo mật

Xác định các kết nối không mong muốn, phân tích các cuộc tấn công



Khắc phục sự cố

Chẩn đoán vấn đề mạng, xác định nguyên nhân của kết nối bị từ chối



Phân tích lưu lượng

Theo dõi lượng truy cập, phân tích mô hình sử dụng



Hóa đơn

Xác minh sử dụng dịch vụ, phân tích chi phí

Sơ đồ Pipeline VPC Flow Logs

Luồng dữ liệu từ Network Interface đến các điểm lưu trữ



Network Interface

EC2 Instance, ELB



VPC Flow Logs

Ghi lại lưu lượng IP



CloudWatch Logs / S3

Lưu trữ & Phân tích

Mô tả luồng hoạt động:

1. Network Interface

Lưu lượng IP đi vào và ra khỏi các giao diện mạng (EC2, ELB) được giám sát

2. VPC Flow Logs

Thu thập thông tin về lưu lượng (nguồn, đích, cổng, giao thức, ACCEPT/REJECT)

3. Storage & Analysis

Dữ liệu được xuất bản đến Amazon CloudWatch Logs (giám sát thực thời) hoặc Amazon S3 (lưu trữ dài hạn)



Exam Tip: Flow Logs được thu thập bên ngoài đường dẫn lưu lượng mạng, do đó không ảnh hưởng đến thông lượng hoặc độ trễ mạng.

12. Site-to-Site VPN và Direct Connect

Hai phương pháp kết nối hybrid cloud giữa on-premises và AWS

Site-to-Site VPN

Kết nối mạng an toàn giữa mạng on-premises và VPC qua Internet

Đặc điểm:

- 🛡️ Sử dụng giao thức IPsec để mã hóa lưu lượng
- 🌐 Lưu lượng đi qua Internet công cộng
- 🕒 Thiết lập nhanh chóng, chi phí thấp

Thành phần:

- 💻 Virtual Private Gateway (VGW): Cổng VPN phía AWS
- 💻 Customer Gateway (CGW): Thiết bị VPN on-premises

Trường hợp sử dụng:

- 🏠 Ứng dụng không yêu cầu băng thông cao
- ⌚ Khi cần giải pháp nhanh chóng, tiết kiệm chi phí



AWS Direct Connect

Kết nối vật lý riêng, chuyên dụng từ trung tâm dữ liệu đến AWS

Đặc điểm:

- 🔒 Lưu lượng không đi qua Internet công cộng
- 📶 Băng thông ổn định (50 Mbps đến 100 Gbps)
- ⚡ Độ trễ mạng thấp hơn

Thành phần:

- 📍 Direct Connect Location: Điểm kết nối vật lý
- 🔌 Direct Connect Connection: Kết nối vật lý

Trường hợp sử dụng:

- YSQL Ứng dụng yêu cầu bảo mật cao
- ⚡ Khi cần băng thông ổn định và độ trễ thấp



On-premises



Internet



AWS

So sánh Site-to-Site VPN và Direct Connect

Các khác biệt về cơ chế kết nối, hiệu suất và chi phí

Site-to-Site VPN



Direct Connect

So sánh	Site-to-Site VPN	Direct Connect	Ưu điểm	Hạn chế
➡ Cơ chế kết nối	IPsec qua Internet	Kết nối vật lý riêng	VPN là dịch vụ được quản lý	VPN có thể bị ảnh hưởng bởi mạng internet
🛡️ Tính bảo mật	IPsec mã hóa lưu lượng	Kết nối riêng tư hơn	VPN đủ bảo mật cho nhiều trường hợp	VPN qua Internet có rủi ro trung gian
⚡ Hiệu suất	Băng thông phụ thuộc mạng internet	50 Mbps đến 100 Gbps	Direct Connect có độ trễ thấp hơn	VPN qua internet có độ trễ cao hơn
฿ Chi phí	Chi phí thấp hơn	Chi phí cao hơn	VPN tiết kiệm chi phí	Direct Connect có chi phí cố định hàng tháng
✖ Độ phức tạp	Dễ triển khai	Thời gian triển khai lâu hơn	VPN thiết lập nhanh chóng	Direct Connect cần thời gian và nguồn lực hơn

💡 Exam Tip: Hãy nhớ rằng Site-to-Site VPN sử dụng IPsec qua internet, trong khi Direct Connect tạo kết nối vật lý riêng với băng thông nhất quán.

13. Tổng kết phần VPC

Tổng hợp các khái niệm chính về Amazon VPC và các thành phần mạng

VPC Foundation

Amazon VPC

Mạng ảo được cài đặt logic trong AWS Cloud, cho phép bạn kiểm soát môi trường mạng

CIDR & Subnet

Xác định dải IP cho VPC và phân đoạn mạng con trong từng Availability Zone

Subnet Types

Public Subnet (có IGW) và Private Subnet (truy cập Internet thông NAT Gateway)

Route Table

Chứa các quy tắc định tuyến lưu lượng mạng trong VPC

Connectivity

Internet Gateway

Cổng mạng cho phép giao tiếp giữa VPC và Internet

NAT Gateway

Cho phép Private Subnet truy cập Internet (một chiều)

VPC Peering

Kết nối giữa các VPC bằng IP riêng tư (non-transitive)

VPC Endpoints

Kết nối riêng tư đến dịch vụ AWS (Gateway hoặc Interface)

Security

Security Group

Tường lửa cấp instance (stateful), chỉ có quy tắc Allow

Network ACL

Tường lửa cấp subnet (stateless), có Allow/Deny

Advanced Networking

VPC Flow Logs

Ghi lại thông tin lưu lượng IP vào/ra các giao diện mạng

Hybrid Cloud

Site-to-Site VPN (qua Internet) và Direct Connect (kết nối vật lý)



Exam Tip: Luôn nhớ sự khác biệt giữa Security Group (stateful, instance-level) và Network ACL (stateless, subnet-level).

Bastion Host

Lời khuyên ôn thi

Các điểm cần tập trung khi chuẩn bị cho kỳ thi chứng chỉ AWS



Nắm vững sự khác biệt

Đặc biệt giữa Security Group (stateful, instance-level) và Network ACL (stateless, subnet-level).



Khi nào dùng NAT Gateway

Hiểu rõ vai trò của NAT Gateway trong việc cho phép Private Subnet truy cập Internet.



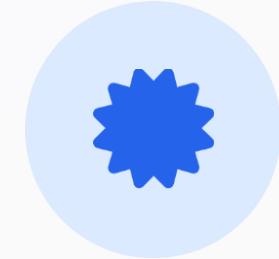
VPC Peering vs. VPC Endpoints

Phân biệt trường hợp sử dụng của từng loại kết nối riêng tư này.



Thực hành

Tạo và cấu hình các thành phần VPC trên AWS Console để củng cố kiến thức.



Chuẩn bị cho kỳ thi

Sử dụng sơ đồ và ví dụ thực tế để hiểu rõ các khái niệm

Các điểm khác cần chú ý:

- ✓ CIDR block allocation và subnetting
- ✓ Route Table và định tuyến mạng
- ✓ Bảo mật mạng: Security Groups vs NACLs
- ✓ Kết nối Hybrid Cloud: VPN vs Direct Connect



Exam Tip:

VPC Peering là "non-transitive". Nếu VPC A peering với VPC B, và VPC B peering với VPC C, thì VPC A không thể giao tiếp với VPC C.

Chúc bạn thành công trong kỳ thi AWS Certified!