

TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP.HCM

KHOA: CÔNG NGHỆ THÔNG TIN



**HCMUTE**

**BÁO CÁO ĐỀ TÀI**

**PRIVATE CLOUD SETUP WITH SECURITY  
BEST PRACTICES**

**MÔN HỌC: ĐIỆN TOÁN ĐÁM MÂY**

**GVHD: TS.Huỳnh Xuân Phụng**

**Mã LHP: CLCO332779\_23\_1\_07**

**Nhóm sinh viên thực hiện:**

- |                        |          |
|------------------------|----------|
| 1. Nguyễn Lê Gia Hân   | 21110432 |
| 2. Nguyễn Thùy Diễm My | 21110549 |
| 3. Nguyễn Võ Minh Luân | 21110899 |

**TP.Hồ Chí Minh, tháng 11 năm 2023**

## ĐÁNH GIÁ VÀ CHẤM ĐIỂM

STT	MSSV	Họ tên	Hoàn tất	Điểm
1	21110432	Nguyễn Lê Gia Hân	100%	
2	21110549	Nguyễn Thùy Diễm My	100%	
3	21110899	Nguyễn Võ Minh Luân	100%	

Đánh giá của Giảng viên

.....  
.....  
.....  
.....  
.....

Giảng viên ký, ghi họ tên

**Huỳnh Xuân Phùng**

## LỜI CẢM ƠN

Lời đầu tiên, nhóm chúng em xin gửi lời cảm ơn chân thành đến Trường Đại học Sư phạm Kỹ thuật Thành phố Hồ Chí Minh đã đưa môn học Điện toán đám mây vào chương trình giảng dạy cho sinh viên ngành Công nghệ thông tin. Đặc biệt, chúng em xin gửi lời cảm ơn sâu sắc đến giảng viên bộ môn – TS. Huỳnh Xuân Phụng đã dạy dỗ, truyền đạt những kiến thức quý báu cho chúng em trong suốt thời gian học tập vừa qua. Trong thời gian tham gia lớp học Điện toán đám mây của thầy, chúng em đã có thêm cho mình nhiều kiến thức bổ ích, tinh thần học tập hiệu quả, nghiêm túc. Đây chắc chắn sẽ là những kiến thức quý báu, không chỉ giúp ích cho chúng em trong việc lựa chọn chuyên ngành mà còn là hành trang để chúng em có thể vững bước sau này.

Môn học Điện toán đám mây là một môn học thú vị, bổ ích và rất thiết thực trong thời đại bùng nổ công nghệ 4.0 hiện nay, đảm bảo kiến thức đầy đủ, gắn với thực tiễn cho sinh viên. Tuy nhiên, do thiếu kinh nghiệm trong lĩnh vực này cũng như hạn chế về kiến thức, chắc chắn sẽ có một số điểm trong bài báo cáo không tránh khỏi những thiếu sót. Chúng em rất mong được sự nhận xét, góp ý, phê bình của thầy để bài báo cáo được hoàn thiện hơn.

Lời cuối cùng, chúng em xin kính chúc thầy nhiều sức khỏe, thành công và hạnh phúc. Nhóm chúng em chân thành cảm ơn!

## MỤC LỤC

<b>1. GIỚI THIỆU .....</b>	<b>5</b>
1.1. Lý do chọn đề tài .....	5
1.2. Đối tượng và phạm vi nghiên cứu .....	6
1.3. Kết quả dự kiến đạt được .....	6
<b>2. CƠ SỞ LÝ THUYẾT .....</b>	<b>6</b>
2.1. Google Cloud .....	6
2.2. Amazon Web Services .....	9
2.3. Private Cloud .....	10
2.4. Virtual Private Cloud (VPC) .....	14
2.5. Identity and Access Management (IAM) .....	18
2.6. Network Firewall .....	21
2.7. VPN .....	22
<b>3. PHƯƠNG PHÁP THỰC HIỆN .....</b>	<b>24</b>
<b>4. THIẾT KẾ VÀ CÀI ĐẶT .....</b>	<b>25</b>
<b>5. KẾT QUẢ VÀ ĐÁNH GIÁ .....</b>	<b>51</b>
<b>6. PHÂN TÍCH DỊCH VỤ VÀ CÔNG NGHỆ CLOUD .....</b>	<b>53</b>
<b>7. KẾT LUẬN .....</b>	<b>53</b>
<b>TÀI LIỆU THAM KHẢO .....</b>	<b>56</b>

# 1. GIỚI THIỆU

## 1.1. Lý do chọn đề tài

An toàn và bảo mật thông tin trong thời đại công nghệ số phát triển như hiện nay luôn là vấn đề được các cá nhân và doanh nghiệp đặt lên hàng đầu. Trong những năm gần đây, Cloud Computing đã trở thành một khía cạnh cần thiết trong hoạt động kinh doanh của bất kỳ doanh nghiệp nào bởi tính tiện lợi và khả năng bảo mật mà nó mang lại. Với nhu cầu tăng cao về dịch vụ Cloud, các công ty phải quyết định liệu họ nên chọn giải pháp Public Cloud, Hybrid Cloud hay Private Cloud. Trong số những mô hình trên, Private Cloud đặc biệt nhấn mạnh sự kiểm soát hoàn toàn của doanh nghiệp đối với môi trường lưu trữ dữ liệu và ứng dụng. Nó không chỉ cung cấp giải pháp linh hoạt mà còn giúp đổi mới với những rủi ro bảo mật, đảm bảo an toàn cho dữ liệu và tài nguyên của tổ chức. Do đó, doanh nghiệp có thể yên tâm về sự an toàn và bảo mật dữ liệu của mình một cách tốt nhất, tăng cường uy tín cũng như sự tin tưởng từ phía người dùng và đối tác. Thế nhưng, ở thị trường Việt Nam hiện nay thì việc triển khai môi trường đám mây nội bộ vẫn còn khá mới mẻ và phải đổi mới với nhiều khó khăn trong quá trình triển khai cũng như quản lý.

Từ những lý do trên, nhóm chúng em đã chọn đề tài "**PRIVATE CLOUD SETUP WITH SECURITY BEST PRACTICES**" để tiến hành nghiên cứu. Đề tài không chỉ cung cấp kiến thức vững chắc về xây dựng một đám mây nội bộ mà còn hướng dẫn cách áp dụng các phương pháp, quy trình và công nghệ bảo mật tiên tiến nhất vào trong quá trình triển khai và vận hành. Chính điều này sẽ giúp doanh nghiệp địa phương nâng cao khả năng bảo mật, giảm thiểu rủi ro và đồng thời tối ưu hóa hiệu suất hệ thống. Thị trường đang ngày càng chú trọng đến vấn đề bảo mật và uy tín cho nên việc nghiên cứu và áp dụng các best practices trong private cloud sẽ tạo ra cơ hội cạnh tranh và đáp ứng nhu cầu ngày càng cao từ phía người dùng và đối tác. Nhóm chúng em hy vọng rằng đề tài của chúng em không chỉ mang lại kiến thức hữu ích mà còn đóng góp vào sự phát triển và ứng dụng của công nghệ đám mây nội bộ trong bối cảnh kinh doanh hiện đại.

## **1.2. Đối tượng và phạm vi nghiên cứu**

- Đối tượng nghiên cứu: tìm hiểu và xây dựng VPC trên nền tảng Google Cloud Platform (GCP), tích hợp tính năng AWS nhằm tạo thành đám mây lai, thực hiện các biện pháp bảo mật và so sánh với VPC trên AWS để từ đó đưa ra nhận xét, đánh giá.
- Phạm vi nghiên cứu: Đề tài này chỉ nghiên cứu các phạm vi liên quan đến các dịch vụ và biện pháp bảo mật mà cả hai nền tảng hỗ trợ cho tài khoản sinh viên.

## **1.3. Kết quả dự kiến đạt được**

Trong phạm vi nghiên cứu của đề tài, nhóm chúng em dự kiến sẽ tạo ra được VPC trên GCP với các dịch vụ cũng như biện pháp bảo mật thường gặp, phù hợp với nhu cầu của thị trường hiện nay và so sánh với VPC ở trên AWS.

# **2. CƠ SỞ LÝ THUYẾT**

## **2.1. Google Cloud**

Google Cloud hay còn gọi là Google Cloud Platform (GCP) chính là một nền tảng của kỹ thuật điện toán đám mây cho phép các cá nhân, tổ chức, các doanh nghiệp, các cơ quan có thể xây dựng, phát triển, và hoạt động các ứng dụng của mình trên hệ thống phần mềm do google tạo ra. Các ứng dụng phổ biến hiện nay được mọi người sử dụng rất nhiều như: Trình duyệt Chrome, ứng dụng bản đồ Google Map, Google Apps, kênh Youtube... Google Cloud cung cấp tất cả các giải pháp quản lý cho doanh nghiệp, giúp doanh nghiệp có thể phát triển hệ thống công nghệ của mình một cách chính xác, hiện đại. Bên cạnh đó, GC còn giúp người dùng và doanh nghiệp giải quyết các vấn đề như: Developer (phát triển), Management (Quản lý), Computer Engine, Mobile, Storage, Big Data...

Một điểm khác biệt nữa mà GC mang lại so với các dịch vụ đám mây khác đó chính là hệ thống DataCenter luôn ổn định và có độ bảo mật dữ liệu cực cao, giúp bảo vệ

dữ liệu người dùng và khách hàng trước sự dòm ngó và xâm nhập trái phép của các hacker công nghệ.

# Google Cloud Platform

## Compute



Compute Engine



Kubernetes Engine



App Engine



Cloud Functions

## Management



Cloud Console



Stackdriver



Trace



Logging



Debugger



Monitoring

## Networking



Cloud Load Balancing



Cloud CDN



Cloud DNS



Firewall Rules



Cloud Interconnect



Cloud VPN

## Storage & Databases



Cloud Bigtable



Cloud Datastore



Cloud Spanner



Cloud SQL



Cloud Storage

## Big Data



BigQuery



Cloud Dataflow



Cloud Dataprep



Cloud Dataproc



Cloud IoT Core



Cloud Pub/Sub

## Identity & Security



Cloud IAM



Cloud Endpoints



VPC



Identity Aware Proxy



KMS



Data Loss Prevention

## Machine Learning



Cloud ML



Natural Language API



Cloud Speech API



Cloud Vision API



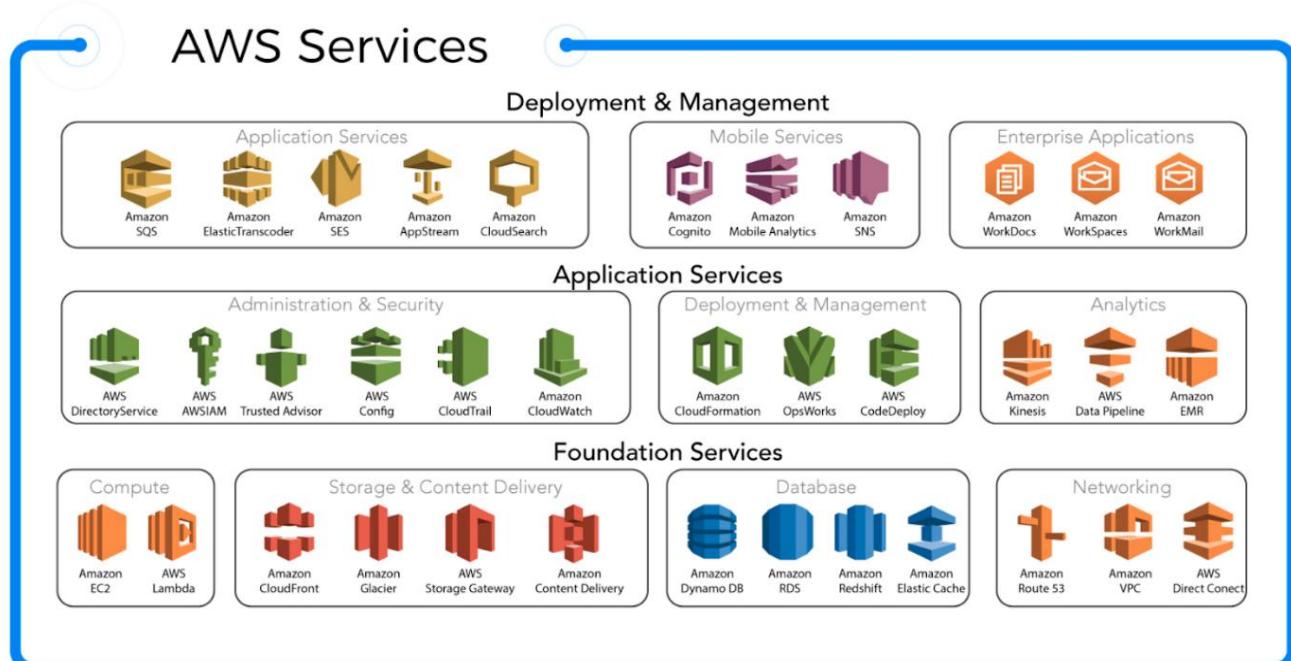
Cloud Translate API

## 2.2. Amazon Web Services

Amazon Web Services (AWS) là một dịch vụ đám mây hàng đầu của Amazon, ra mắt vào năm 2006 và nhanh chóng trở thành một trong những nhà cung cấp lớn và phổ biến nhất trên toàn cầu. AWS cung cấp nhiều dịch vụ đám mây đa dạng như máy chủ ảo, lưu trữ, cơ sở dữ liệu, tích hợp, phân tích dữ liệu, máy học, và IoT. Doanh nghiệp từ các công ty khởi nghiệp đến các tập đoàn lớn và cơ quan chính phủ đều tin tưởng sử dụng AWS để giảm chi phí, tăng tính linh hoạt và đổi mới nhanh chóng.

Mô hình dịch vụ đám mây của AWS cho phép người dùng trả tiền chỉ cho những tài nguyên họ sử dụng, mà không cần mua và duy trì cơ sở hạ tầng vật lý, giúp thu nhỏ ngân sách mà vẫn đảm bảo khả năng mở rộng. AWS được thiết kế để đảm bảo bảo mật và linh hoạt cao, với cơ sở hạ tầng xây dựng để đáp ứng các yêu cầu bảo mật cao cấp.

Với hơn 300 dịch vụ và tính năng bảo mật, AWS hỗ trợ tuân thủ và quản trị, cũng như đáp ứng 143 tiêu chuẩn bảo mật và chứng nhận. AWS cung cấp không ngừng các công nghệ mới để khuyến khích thử nghiệm và đổi mới, như việc tiên phong với AWS Lambda trong không gian điện toán không có máy chủ và dịch vụ quản lý machine learning Amazon SageMaker. Private Cloud



## 2.3. Private Cloud

### 2.3.1. Khái niệm

Private Cloud là môi trường điện toán đám mây dành riêng cho một tổ chức. Bất kỳ cơ sở hạ tầng đám mây nào cũng có các tài nguyên điện toán cơ bản như CPU và bộ lưu trữ mà bạn cung cấp theo yêu cầu thông qua cổng tự phục vụ. Trong Private Cloud, tất cả tài nguyên đều bị cô lập và nằm trong sự kiểm soát của một tổ chức. Vì vậy, Private Cloud còn được gọi là đám mây nội bộ hoặc đám mây doanh nghiệp. Thuật ngữ Private Cloud được đưa ra để phân biệt giữa các môi trường đám mây nội bộ này và các dịch vụ Public Cloud của bên thứ ba do các tổ chức như Amazon, Google cung cấp.

Ngày nay, một số công ty đã áp dụng các công nghệ và thay đổi trong hoạt động của mình để đưa ra một số khái niệm về điện toán đám mây. Một ví dụ là các công ty có thể tính phí các tài nguyên máy tính mà đơn vị kinh doanh của họ sử dụng. Tuy nhiên, phần lớn khách hàng vẫn chưa thực sự thành công trong việc triển khai Private Cloud với những lợi ích tương đương với Public Cloud.

### 2.3.2. *Ưu và nhược điểm*

#### a) *Ưu điểm của private cloud*

- Hiệu suất và khả năng đáp ứng cao: Cơ sở hạ tầng private cloud được thiết kế và triển khai để đáp ứng nhu cầu cụ thể của tổ chức. Điều này có thể giúp cải thiện hiệu suất và khả năng đáp ứng của các ứng dụng và dịch vụ.
- Bảo mật và quyền riêng tư cao: Cơ sở hạ tầng private cloud nằm trong quyền kiểm soát của tổ chức. Điều này giúp tăng cường bảo mật và quyền riêng tư cho dữ liệu và ứng dụng.
- Linh hoạt và khả năng tùy chỉnh cao: Cơ sở hạ tầng private cloud có thể được tùy chỉnh để đáp ứng nhu cầu thay đổi của tổ chức. Điều này giúp tổ chức tiết kiệm chi phí và tối ưu hóa hiệu quả hoạt động.
- Khả năng kiểm soát và quản lý cao: Tổ chức có toàn quyền kiểm soát và quản lý cơ sở hạ tầng private cloud. Điều này giúp tổ chức đảm bảo rằng cơ sở hạ tầng được sử dụng hiệu quả và an toàn.

### b) *Nhược điểm của private cloud*

- Chi phí cao: Chi phí triển khai và vận hành private cloud có thể cao hơn so với các mô hình điện toán đám mây khác.
- Yêu cầu kỹ năng và chuyên môn cao: Việc triển khai và quản lý private cloud đòi hỏi kỹ năng và chuyên môn cao.
- Giới hạn khả năng mở rộng: Khả năng mở rộng của private cloud có thể bị giới hạn bởi cơ sở hạ tầng vật lý.

Tóm lại, private cloud là một lựa chọn phù hợp cho các tổ chức cần kiểm soát cao, bảo mật và quyền riêng tư cao, hoặc yêu cầu hiệu suất và khả năng đáp ứng cao. Tuy nhiên, private cloud cũng có thể đi kèm với chi phí cao và yêu cầu kỹ năng và chuyên môn cao.

#### **2.3.3. Sự khác nhau giữa Private Cloud, Public Cloud và Hybrid Cloud**

Đặc điểm	Private cloud	Public cloud	Hybrid cloud
Sở hữu và quản lý	Tổ chức sở hữu và quản lý cơ sở hạ tầng đám mây	Nhà cung cấp đám mây sở hữu và quản lý cơ sở hạ tầng đám mây	Tổ chức sở hữu một phần cơ sở hạ tầng đám mây, phần còn lại được sở hữu và quản lý bởi nhà cung cấp đám mây
Vị trí	Cơ sở hạ tầng đám mây được đặt tại trung tâm dữ liệu của tổ chức	Cơ sở hạ tầng đám mây được đặt tại trung tâm dữ liệu của nhà cung cấp đám mây	Cơ sở hạ tầng đám mây có thể được đặt tại trung tâm dữ liệu của tổ chức hoặc nhà cung cấp đám mây
Khả năng mở rộng	Có thể được tùy	Có thể mở rộng	Có thể mở rộng linh

	chỉnh để đáp ứng nhu cầu cụ thể của tổ chức	nhanh chóng để đáp ứng nhu cầu thay đổi của tổ chức	hoạt để đáp ứng nhu cầu của cả tổ chức và nhà cung cấp đám mây
Bảo mật và quyền riêng tư	Cao	Trung bình	Tùy thuộc vào mô hình triển khai
Chi phí	Cao	Thấp	Trung bình
Yêu cầu kỹ năng và chuyên môn	Cao	Trung bình	Trung bình
Ví dụ	Các tổ chức có dữ liệu nhạy cảm, cần bảo mật cao hoặc yêu cầu hiệu suất và khả năng đáp ứng cao	Các tổ chức có nhu cầu về tính linh hoạt, khả năng mở rộng và chi phí thấp	Các tổ chức có nhu cầu kết hợp các ưu điểm của private cloud và public cloud

#### **2.3.4. Cách Private Cloud hoạt động**

Kiến trúc của một Private Cloud tương tự như Public Cloud và yêu cầu triển khai các công nghệ tương tự.

##### a) Virtualization (Ảo hóa)

Virtualization là công nghệ trùu tượng hóa tài nguyên CNTT từ phần cứng vật lý cơ bản của chúng. Người dùng có thể tạo các máy ảo hoặc đơn vị phần mềm và tương tác với chúng theo cách tương tự như máy vật lý. Phần mềm ảo hóa tập hợp các tài nguyên phần cứng như CPU, bộ nhớ hoặc bộ lưu trữ và phân bổ chúng cho các máy ảo theo yêu cầu.

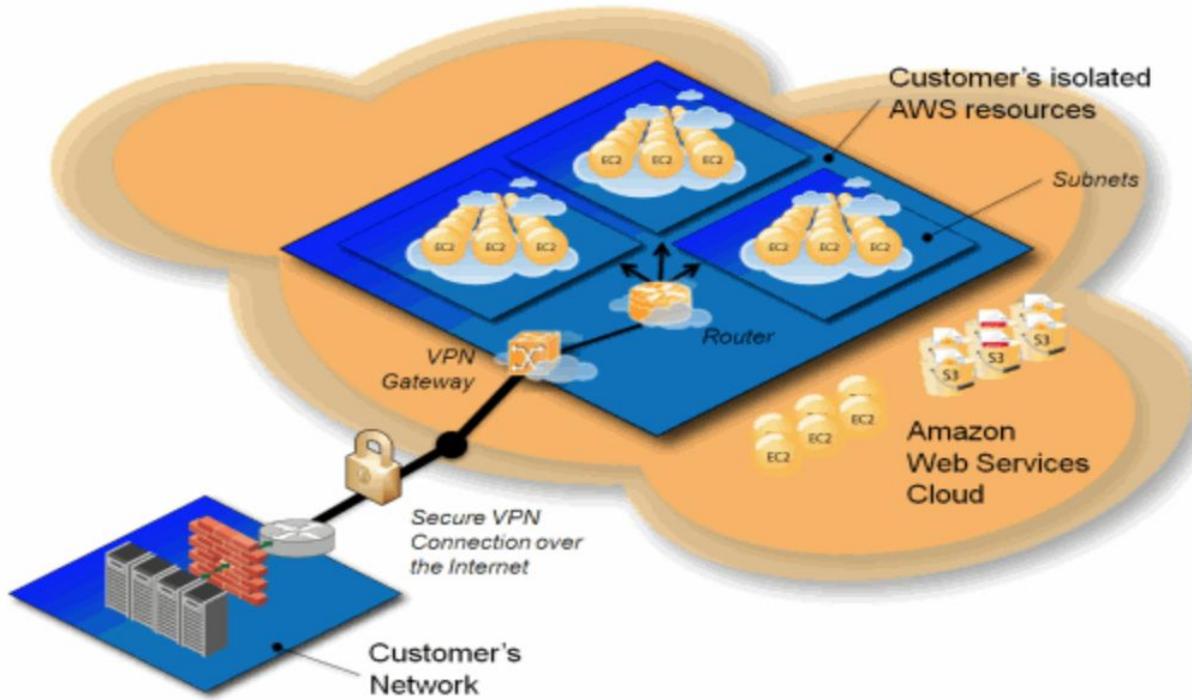
b) Management software (Phần mềm quản lý)

Quản trị viên cần phần mềm quản lý để kiểm soát và quản lý cơ sở hạ tầng CNTT của họ một cách tập trung dưới dạng đơn vị phần mềm. Họ sử dụng phần mềm này để triển khai các cấu hình nhất quán trên các máy chủ và môi trường ứng dụng, đảm bảo tuân thủ bảo mật và tối ưu hóa việc phân bổ tài nguyên.

c) Automation technologies (Công nghệ tự động hóa)

Tự động hóa tăng tốc các tác vụ như tích hợp và cung cấp máy chủ vốn tẻ nhạt và dễ xảy ra lỗi khi thực hiện thủ công. Các tổ chức muốn triển khai môi trường đám mây riêng phải cung cấp khả năng tự động hóa để quản lý cơ sở hạ tầng đám mây hiệu quả hơn.

Ngoài các công nghệ đám mây riêng, các tổ chức cũng phải thực hiện các thay đổi đối với hoạt động phát triển và triển khai của mình. Ví dụ: các hoạt động ứng dụng tập trung vào đám mây như DevOps và DevSecOps cũng như các kiến trúc như microservice và container mang lại hiệu quả và tính linh hoạt cao hơn cho môi trường private cloud.



## 2.4. Virtual Private Cloud (VPC)

### 2.4.1. Khái niệm

VPC – Virtual Private Cloud hay đám mây riêng ảo là một đám mây riêng biệt, an toàn và được lưu trữ trong môi trường Public Cloud (đám mây công cộng). Khách hàng của VPC có thể chạy mã code, lưu trữ dữ liệu, lưu trữ trang web và làm bất kỳ điều gì khác mà họ có thể làm như cách họ thường làm trong Private Cloud (đám mây riêng).

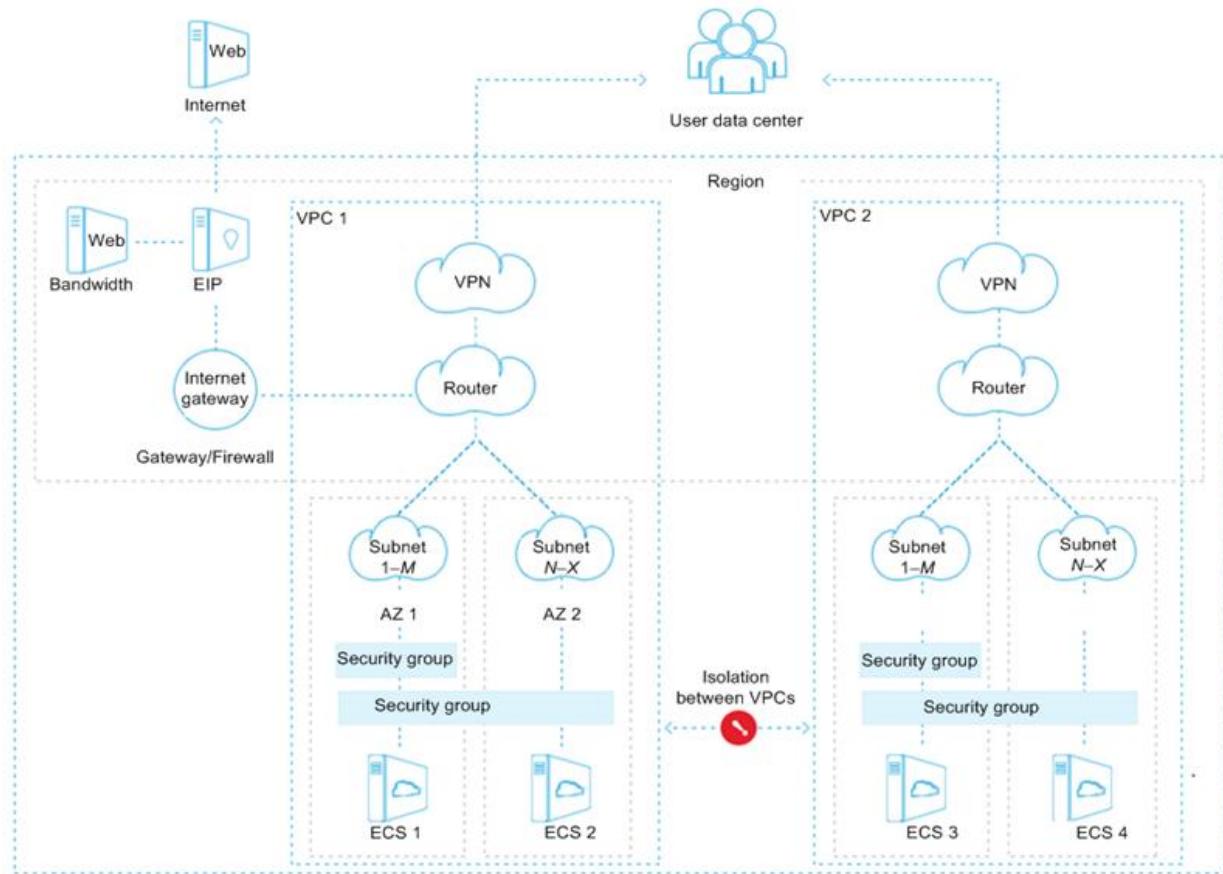
Tuy nhiên, VPC sẽ được lưu trữ từ xa bởi một nhà cung cấp đám mây công cộng (Public Cloud) trong khi không phải tất cả các đám mây riêng đều được lưu trữ theo cách này. Các đám mây riêng ảo giúp kết hợp khả năng mở rộng và sự tiện lợi của các đám mây công cộng với sự cô lập, bảo toàn dữ liệu của các đám mây riêng.

Có thể hiểu là, Private Cloud lại nói đến môi trường đám mây riêng biệt chỉ có một người thuê, đây là dạng dịch vụ được cung cấp độc quyền cho một tổ chức.

Một đám mây riêng ảo (VPC) là một đám mây riêng được đặt trong môi trường Public Cloud, sẽ không có ai chia sẻ dữ liệu trên VPC với người khác.

#### 2.4.2. VPC trong Public Cloud

##### Cloud



VPC cách ly tài nguyên máy tính với các tài nguyên điện toán khác có sẵn trong Public Cloud. Các công nghệ chính để cách ly VPC khỏi phần còn lại của đám mây công cộng có thể là:

- Subnets

Subnets hay mạng con là một dải địa chỉ IP trong mạng được dành riêng để chúng không được chia sẻ với tất cả các khách hàng sử dụng mạng, mà sẽ được chia sẻ một phần mạng riêng để sử dụng. Trong VPC, đây là những địa chỉ IP riêng không thể truy cập được

bằng Internet công cộng, chúng không giống với các địa chỉ IP thông thường và sẽ được hiển thị công khai.

#### – VLAN

Virtual Local Area Network (VLAN) là một mạng cục bộ ảo, trong đó mạng LAN (mạng cục bộ) là một nhóm các thiết bị tính toán được kết nối với nhau mà không cần sử dụng đến Internet. Giống như mạng con, VLAN là một cách phân vùng mạng, nhưng việc phân vùng sẽ được diễn ra ở lớp 3 thay vì lớp 2 trong mô hình OSI (Open Systems Interconnection – Mô hình kết nối hệ thống mở).

#### – VPN

Virtual Private Network (Mạng riêng ảo) sử dụng mã hóa để tạo ra mạng riêng qua đầu mạng công cộng. Dữ liệu của VPN đi qua cơ sở hạ tầng Internet được chia sẻ công khai qua bộ định tuyến, bộ chuyển mạch, ... nhưng sẽ bị thay đổi hoặc xáo trộn và không hiển thị cho bất cứ ai. Khách hàng của VPC sẽ kết nối VPN với máy chủ của họ, do đó, dữ liệu đi vào và ra khỏi VPC sẽ không hiển thị với những người dùng Public Cloud khác.

## Ưu điểm của VPC

-  **Khả năng mở rộng**
-  **Triển khai Hybrid Cloud dễ dàng**
-  **Nâng cao hiệu suất**
-  **Tăng cường bảo mật**

## 2.5. Identity and Access Management (IAM)

### 2.5.1. Khái niệm

Identity and Access Management (IAM) là một khái niệm chung được áp dụng trên tất cả các nền tảng đám mây, bao gồm cả Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP) và nhiều nền tảng khác. IAM quản lý và kiểm soát quyền truy cập của người dùng và các tài nguyên trong môi trường đám mây. IAM thường bao gồm các thành phần sau:

- Quản lý danh tính: Bao gồm tạo, quản lý và xóa danh tính người dùng. Danh tính có thể là cá nhân, nhóm hoặc máy.
- Kiểm soát truy cập: Bao gồm gán quyền cho danh tính để truy cập tài nguyên. Quyền có thể được cấp ở cấp cá nhân, nhóm hoặc vai trò.
- Xác thực: Bao gồm xác minh danh tính của người dùng trước khi cấp cho họ quyền truy cập vào tài nguyên. Xác thực có thể được thực hiện bằng nhiều phương pháp, chẳng hạn như mật khẩu, mã thông báo hoặc quét sinh trắc học.
- Ủy quyền: Bao gồm xác định xem người dùng đã được xác thực có quyền cần thiết để truy cập tài nguyên hay không.

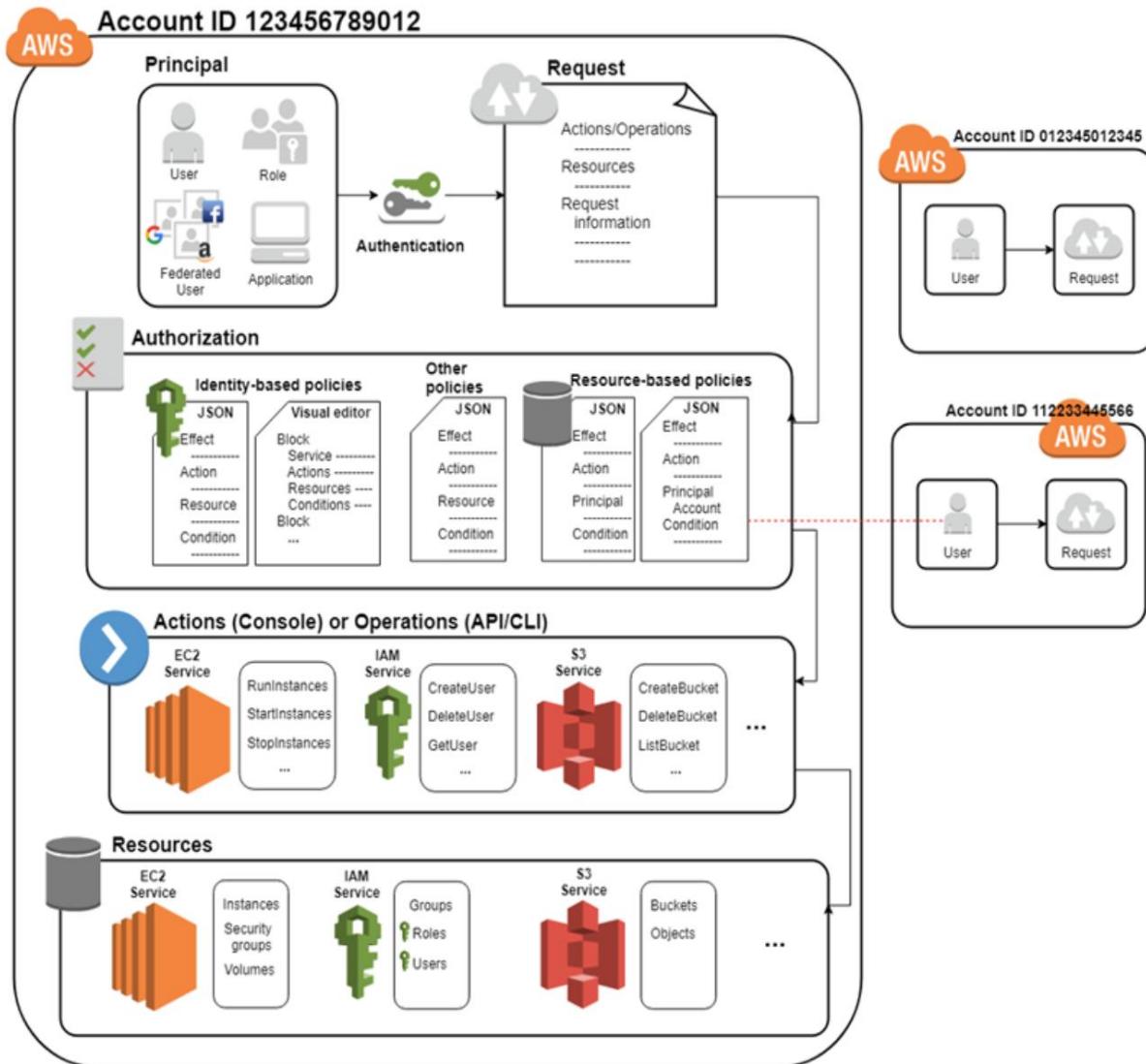
IAM có thể được triển khai bằng nhiều công cụ và công nghệ khác nhau. Có nhiều sản phẩm IAM thương mại có sẵn, cũng như các giải pháp mã nguồn mở. Giải pháp tốt nhất cho một tổ chức sẽ phụ thuộc vào nhu cầu và yêu cầu cụ thể của tổ chức đó.

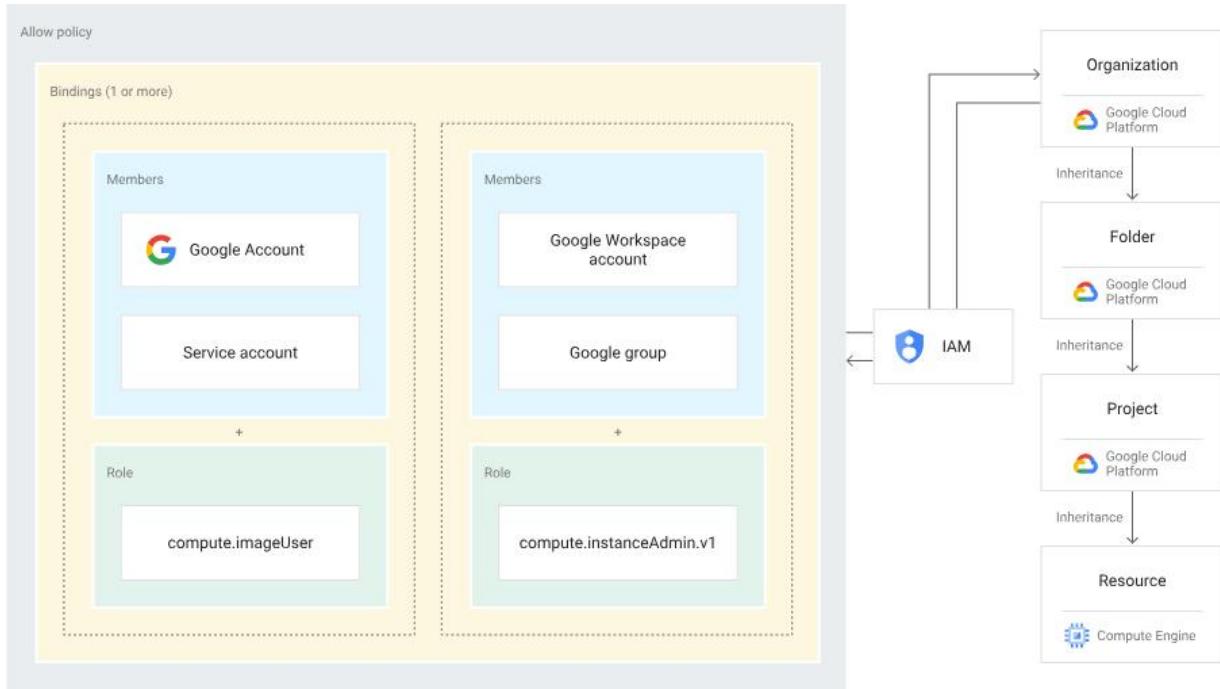
IAM là cần thiết để bảo vệ chống lại nhiều mối đe dọa bảo mật, bao gồm:

- Truy cập trái phép: Đây là loại mối đe dọa bảo mật phổ biến nhất và nó có thể xảy ra khi người dùng trái phép truy cập vào tài nguyên. IAM có thể giúp ngăn chặn truy cập trái phép bằng cách đảm bảo rằng chỉ những người dùng được ủy quyền mới có quyền truy cập vào tài nguyên.
- Vi phạm dữ liệu: Vi phạm dữ liệu có thể xảy ra khi người dùng trái phép truy cập vào dữ liệu nhạy cảm. IAM có thể giúp ngăn chặn vi phạm dữ liệu bằng cách mã hóa dữ liệu và kiểm soát quyền truy cập vào các hệ thống nhạy cảm.

## 2.5.2. Cách mà IAM hoạt động

IAM cung cấp cơ sở hạ tầng cần thiết để kiểm soát việc xác thực và ủy quyền cho tài khoản cloud của bạn. Cơ sở hạ tầng IAM được minh họa bằng các sơ đồ sau:





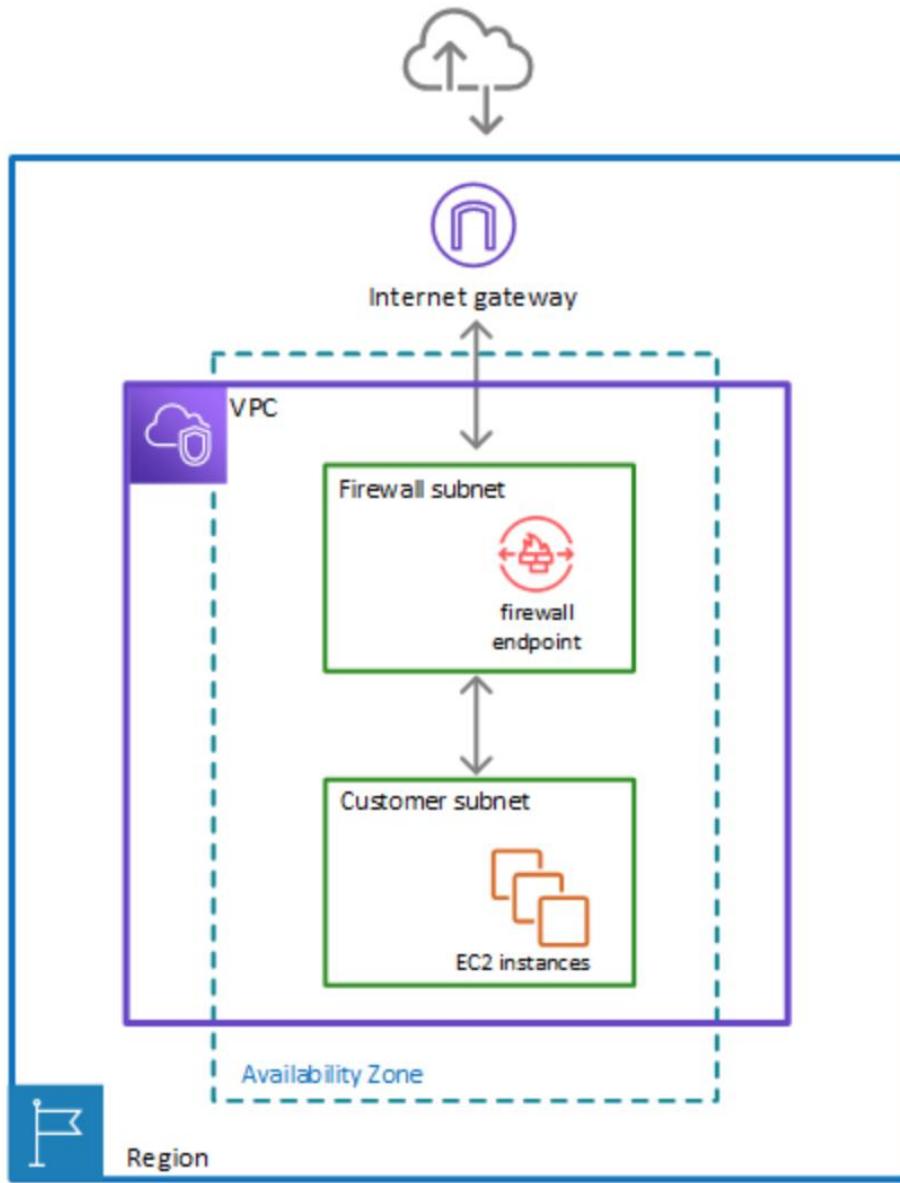
## 2.6. Network Firewall

Cloud Firewall (Tường lửa đám mây) là thiết bị mạng được triển khai trên nền tảng đám mây, dựa trên phần mềm. Cloud Firewall được xây dựng để ngăn chặn hoặc giảm thiểu truy cập không mong muốn vào mạng riêng.

Cloud Firewall mang đến nhiều lợi ích so với tường lửa truyền thống. Các ưu điểm có thể kể đến như khả năng mở rộng dễ dàng, tính khả dụng cao, và khả năng triển khai ở bất kỳ đâu. Nó cung cấp tính bảo mật với khả năng lọc lưu lượng từ nhiều nguồn khác nhau và bảo vệ danh tính. Cloud Firewall cũng hỗ trợ quản lý hiệu suất, đồng thời giúp quản lý quyền truy cập an toàn và bảo vệ chi tiết đối với các công cụ lọc. Việc tích hợp với nhà cung cấp kiểm soát truy cập cũng là một điểm đáng chú ý.

Cloud Firewall bảo vệ các mạng con trong VPC của bạn bằng cách lọc lưu lượng truy cập giữa các mạng con và các vị trí bên ngoài VPC của bạn. Hình ví dụ sau đây mô

tả vị trí của tường lửa trong một kiến trúc rất đơn



giản.

## 2.7. VPN

VPN hay Mạng riêng ảo tạo ra kết nối mạng riêng tư giữa các thiết bị thông qua Internet. VPN được sử dụng để truyền dữ liệu một cách an toàn và ẩn danh qua các mạng công cộng. VPN hoạt động bằng cách ẩn địa chỉ IP của người dùng và mã hóa dữ liệu để chỉ người được cấp quyền nhận dữ liệu mới có thể đọc được.

Công dụng của VPN bao gồm quyền riêng tư, tính ẩn danh, và bảo mật. Nó giữ bí mật thông tin cá nhân, ẩn địa chỉ IP để duyệt web ẩn danh, và bảo vệ kết nối Internet khỏi truy cập trái phép.

VPN hoạt động bằng cách chuyển hướng gói dữ liệu qua một máy chủ từ xa trước khi gửi chúng qua Internet. Các nguyên tắc chính đằng sau công nghệ VPN bao gồm:

- Giao thức đường hầm

Mạng riêng ảo về cơ bản tạo ra đường hầm dữ liệu bảo mật giữa máy cục bộ của bạn và một máy chủ VPN khác ở cách xa bạn hàng ngàn cây số. Khi bạn truy cập mạng, máy chủ VPN này trở thành nguồn chung cho tất cả dữ liệu của bạn. Nhà cung cấp dịch vụ Internet (ISP) của bạn và các bên thứ ba khác sẽ không thể xem nội dung lưu lượng Internet của bạn nữa.

- Mã hóa

Giao thức VPN như IPsec làm nhiều dữ liệu của bạn trước khi gửi chúng qua đường hầm dữ liệu. IPsec là một bộ giao thức bảo mật giao tiếp thông qua Giao thức Internet (IP) bằng cách xác thực và mã hóa mỗi gói IP của một dòng dữ liệu. Dịch vụ VPN hoạt động như một bộ lọc, khiến dữ liệu của bạn trở nên không thể đọc được ở một đầu và chỉ giải mã dữ liệu ở đầu bên kia — việc này ngăn ngừa hành vi sử dụng dữ liệu cá nhân trái phép, kể cả khi kết nối mạng của bạn bị xâm phạm. Lưu lượng mạng trở nên khó bị tấn công và kết nối Internet của bạn được bảo mật.

Trong đề tài này chúng em sử dụng giao thức đường hầm để tạo kết nối cho VPC trên GCP và AWS.

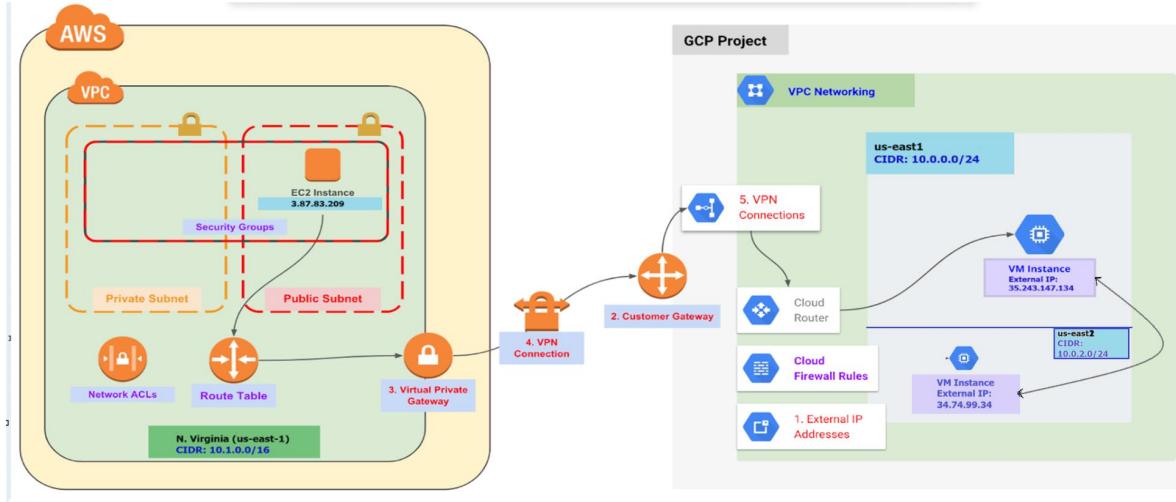
### **3. PHƯƠNG PHÁP THỰC HIỆN**

#### **3.1. Các dịch vụ đám mây và công cụ**

- Trên Google Cloud Platform (GCP) :

- VPC (Virtual Private Cloud): Tạo và quản lý mạng riêng ảo để triển khai các dịch vụ và tài nguyên trong Google Cloud.
- Cloud VPN: Dịch vụ VPN của GCP cho phép kết nối an toàn giữa mạng riêng ảo của bạn trên GCP và mạng tại chỗ của bạn.
- Cloud Router: Quản lý định tuyến giữa mạng riêng ảo và mạng tại chỗ, cung cấp tính linh hoạt và tự động hóa cho kết nối VPN.
- Cloud Identity-Aware Proxy (IAP): Cung cấp quyền truy cập an toàn dựa trên danh tính vào ứng dụng và dịch vụ trên GCP.
- Trên Amazon Web Services (AWS):
  - VPC (Virtual Private Cloud): Dịch vụ tạo mạng riêng ảo trong AWS, cho phép bạn kiểm soát môi trường mạng ảo của mình.
  - Amazon VPN (AWS Site-to-Site VPN): Cho phép kết nối an toàn giữa VPC trên AWS và mạng tại chỗ của bạn thông qua VPN.
  - Direct Connect: Dịch vụ kết nối trực tiếp giữa mạng tại chỗ của bạn và mạng AWS, cung cấp kết nối đáng tin cậy với băng thông cao.
  - AWS Identity and Access Management (IAM): Quản lý quyền truy cập và xác thực cho người dùng và tài nguyên trong AWS.
  - AWS Config: Cung cấp kiểm soát và xác minh đối với cấu hình tài nguyên, giúp duy trì tính bảo mật và tuân thủ

### 3.2. Kiến trúc



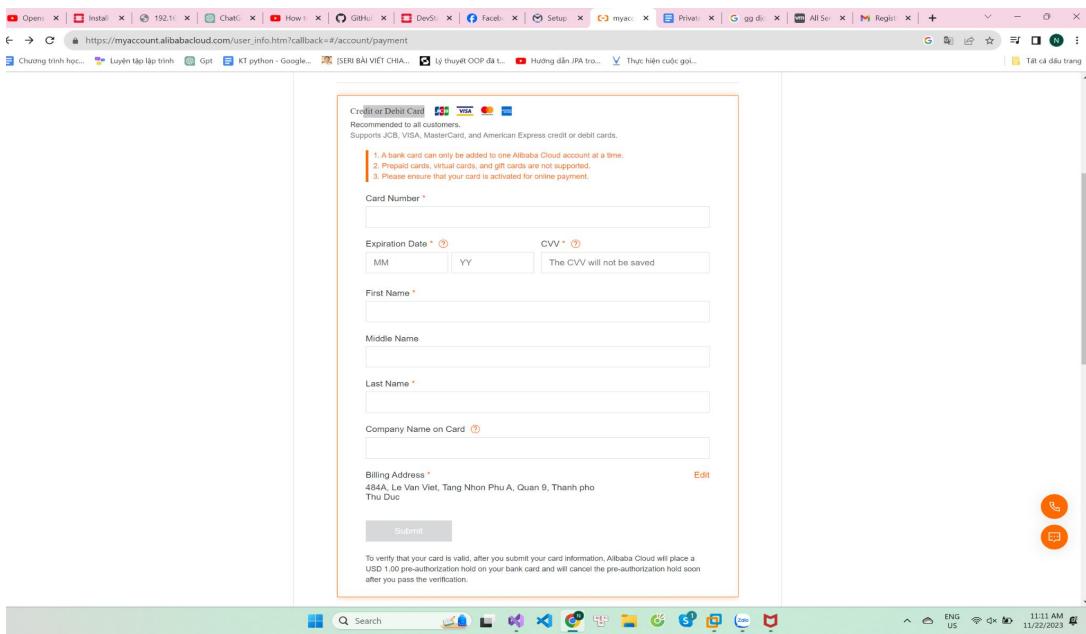
## 4. THIẾT KẾ VÀ CÀI ĐẶT

### 4.1. Xây dựng VPC trên hai nền tảng GCP và AWS thực hiện các best practices

**Bước 1: Tạo VPC trên cả hai nền tảng và cấu hình cơ bản**

**-Tạo VPC trên GCP**

**+ Tạo tài khoản**



Credit or Debit Card 

Recommended to all customers.  
Supports JCB, VISA, MasterCard, and American Express credit or debit cards.

1. A bank card can only be added to one Alibaba Cloud account at a time.  
2. Prepaid cards, virtual cards, and gift cards are not supported.  
3. Please ensure that your card is activated for online payment.

Card Number \*

Expiration Date \*  MM YY  CVV \*  The CVV will not be saved

First Name \*

Middle Name

Last Name \*

Company Name on Card 

Billing Address \* 

484A, Le Van Viet, Tang Nhon Phu A, Quan 9, Thanh pho  
Thu Duc

Submit

To verify that your card is valid, after you submit your card information, Alibaba Cloud will place a USD 1.00 pre-authorization hold on your bank card and will cancel the pre-authorization hold soon after you pass the verification.

## + Tạo một VPC Network

← → C https://console.cloud.google.com/networking/networks/add?hl=vi&project=aws-gcp-vpn-hanmyluan

Chương trình học... Luyện tập lập trình Gpt KT python - Google... [SERI BÀI VIẾT CHIA... Lý thuyết OOP đã t... Tất cả dấu trang

Google Cloud aws-gcp-vpn-hanmyluan Search (/) for resources, do... Search

VPC network Create a VPC network

VPC networks Name \* vpc-aws-gcp-vpn-hanmyluan Description Using to demo connect with vpc in AWS Maximum transmission unit (MTU) 1460

IP addresses

Bring your own IP

Firewall

Routes

VPC network peering

Shared VPC

Serverless VPC access

Packet mirroring

**VPC network ULA internal IPv6 range** Enabling this feature will assign a /48 from Google defined ULA prefix fd20::/20.  Enabled  Disabled

**Subnets** Subnets let you create your own private cloud topology within Google Cloud. Click Automatic to create a subnet in each region, or click Custom to manually define the subnets. [Learn more](#)

Subnet creation mode  Custom  Automatic

New subnet

Name \* subnet-us-east-1 Description Region \* us-east1

Create a VPC network – VPC network

https://console.cloud.google.com/networking/networks/add?hl=vi&project=aws-gcp-vpn-hanmyluan

Chương trình học... Luyện tập lập trình Gpt KT python - Google... [SERI BÀI VIẾT CHIA... Lý thuyết OOP đã t... Tất cả dấu trang

Google Cloud aws-gcp-vpn-hanmyluan Search (/) for resources, do... Search

VPC network

Create a VPC network

Name \* subnet-us-east-1

Description

Region \* us-east1

IP stack type

IPv4 (single-stack)

IPv4 and IPv6 (dual-stack)

IPv4 range \* 10.0.0.0/24

E.g. 10.0.0.0/24

CREATE SECONDARY IPV4 RANGE

Private Google Access

On

Off

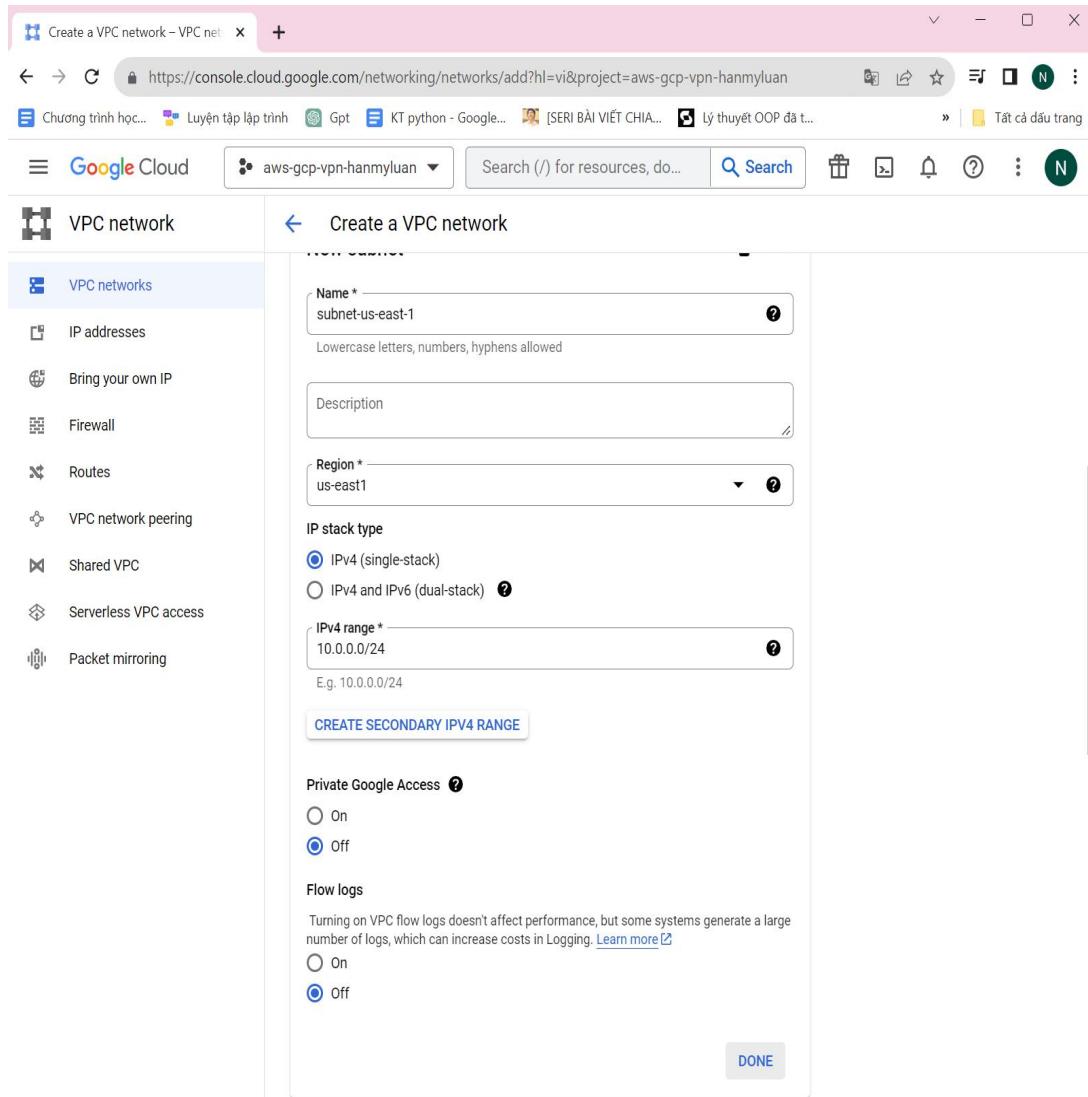
Flow logs

Turning on VPC flow logs doesn't affect performance, but some systems generate a large number of logs, which can increase costs in Logging. [Learn more](#)

On

Off

DONE



**Chọn Done**

Create a VPC network – VPC network

https://console.cloud.google.com/networking/networks/add?hl=vi&project=aws-gcp-vpn-hanmyluan

Chương trình học... Luyện tập lập trình Gpt KT python - Google... [SERI BÀI VIẾT CHIA... Lý thuyết OOP đã t... Hướng dẫn JPA tro... Tất cả dấu trang

Google Cloud aws-gcp-vpn-hanmyluan Search (/) for resources, docs, products, a... Search

VPC network

Create a VPC network

	Protocol	Port Range	Action	IP Ranges	Allow	Port Range	EDIT
<input checked="" type="checkbox"/>	vpc-aws-gcp-vpn-hanmyluan-allow-custom	Ingress	Apply to all	IP ranges: 10.0.0/24	all	Allow	65,534
<input type="checkbox"/>	vpc-aws-gcp-vpn-hanmyluan-allow-icmp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	icmp	Allow	65,534
<input type="checkbox"/>	vpc-aws-gcp-vpn-hanmyluan-allow-rdp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:3389	Allow	65,534
<input type="checkbox"/>	vpc-aws-gcp-vpn-hanmyluan-allow-ssh	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow	65,534

Dynamic routing mode [?](#)

Regional  
Cloud Routers will learn routes only in the region in which they were created

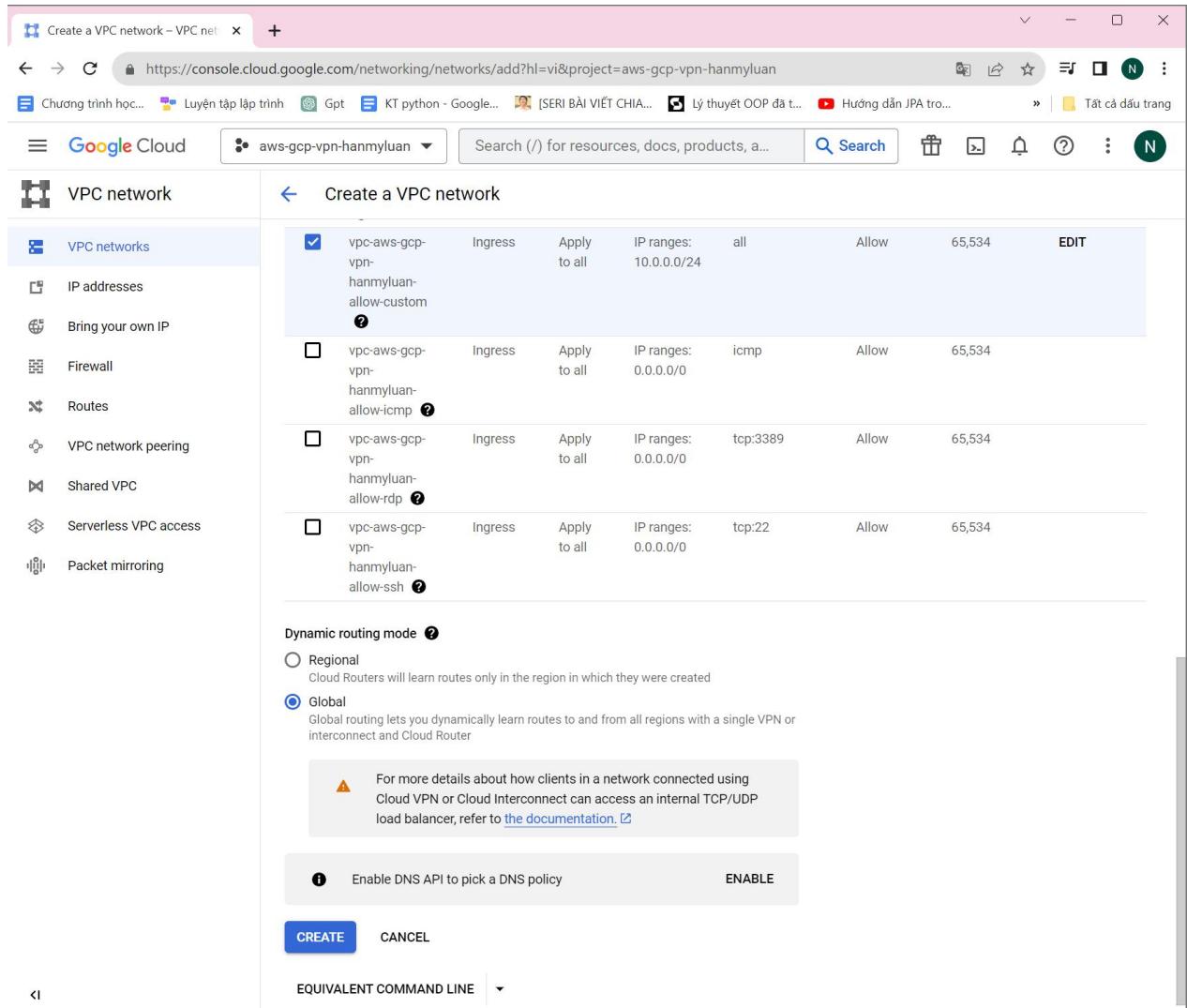
Global  
Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router

⚠ For more details about how clients in a network connected using Cloud VPN or Cloud Interconnect can access an internal TCP/UDP load balancer, refer to [the documentation](#).

Enable DNS API to pick a DNS policy [ENABLE](#)

[CREATE](#) [CANCEL](#)

EQUIVALENT COMMAND LINE



**Chọn create**

VPC networks – VPC network – +

https://console.cloud.google.com/networking/networks/list?hl=vi&project=aws-gcp-vpn-hanmyluan

Chương trình học... Luyện tập lập trình Gpt KT python - Google... [SERI BÀI VIẾT CHIA... Lý thuyết OOP đã t... Hướng dẫn JPA tro... Tất cả dấu trang

Google Cloud aws-gcp-vpn-hanmyluan Search (/) for resources, docs, products, and ... Search 2 ? N

VPC network

VPC networks + CREATE VPC NETWORK REFRESH

NETWORKS IN CURRENT PROJECT SUBNETS IN CURRENT PROJECT

SMTP port 25 disallowed in this project. Learn more

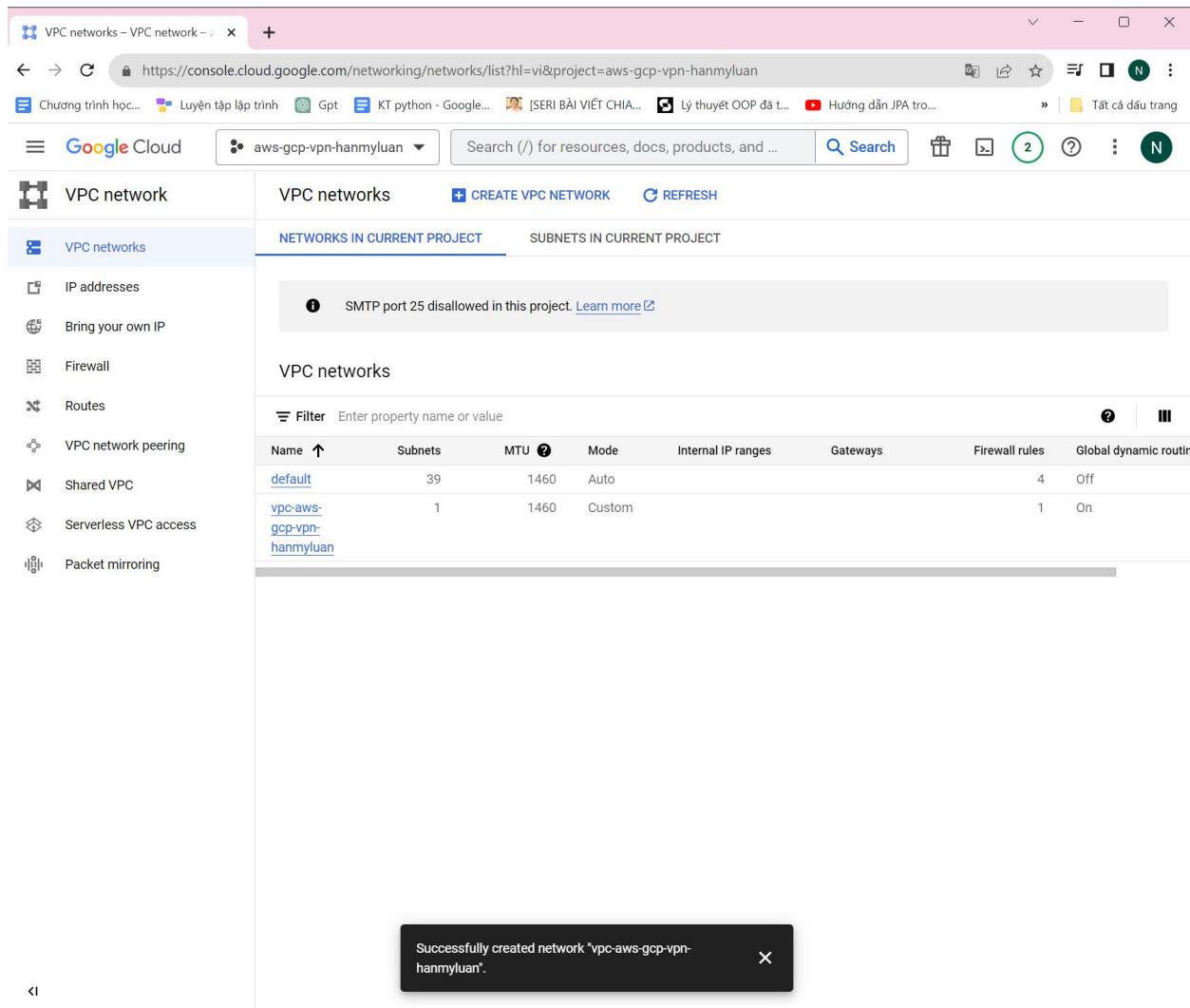
VPC networks

Filter Enter property name or value

Name	Subnets	MTU	Mode	Internal IP ranges	Gateways	Firewall rules	Global dynamic routin
default	39	1460	Auto			4	Off
vpc-aws-gcp-vpn-hanmyluan	1	1460	Custom			1	On

Successfully created network "vpc-aws-gcp-vpn-hanmyluan".

←



## + Tạo subnet

https://console.cloud.google.com/networking/networks/details/vpc-aws-gcp-vpn-hanmyluan?project=aws-gcp-vpn-hanmyluan&cloudshell=true&pageTab=SUBNETS

Chương trình học... Luyện tập lập trình Gpt KT python - Google... [SERI BÀI VIẾT CHIA... Lý thuyết OOP đã t... Hướng dẫn JPA tro... Thực hiện cuộc gọi... Cloud Security Best... Hướng dẫn đăng k... Tất cả dấu trang

Google Cloud aws-gcp-vpn-hanmyluan Search (/) for resources, docs, products, and more Search 5 ? N

VPC network

VPC network details EDIT DELETE VPC NETWORK SHOW INFO PANEL

Maximum transmission unit 1460

VPC network ULA internal IPv6 range Disabled

Subnet creation mode Custom subnets

Dynamic routing mode Global

DNS server policy None

SUBNETS STATIC INTERNAL IP ADDRESSES FIREWALLS FIREWALL ENDPOINTS ROUTES VPC NETWORK PEERING PRIVATE SERVICE ACCESS

Subnets ADD SUBNET FLOW LOGS

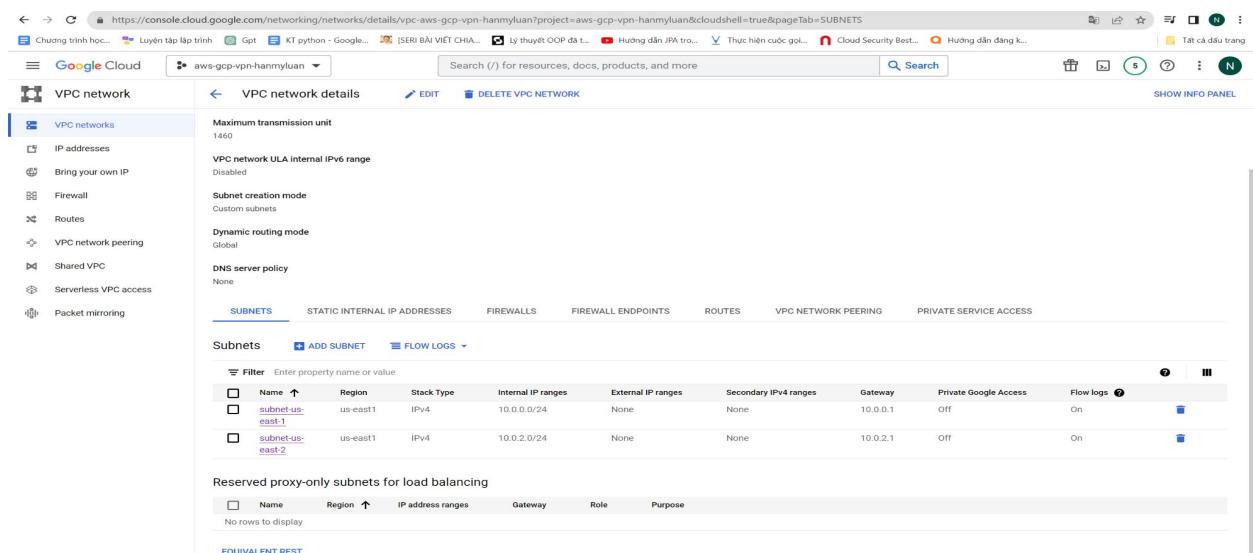
Filter Enter property name or value

Name	Region	Stack Type	Internal IP ranges	External IP ranges	Secondary IPv4 ranges	Gateway	Private Google Access	Flow logs
subnet-us-east-1	us-east1	IPv4	10.0.0.0/24	None	None	10.0.0.1	Off	On
subnet-us-east-2	us-east1	IPv4	10.0.2.0/24	None	None	10.0.2.1	Off	On

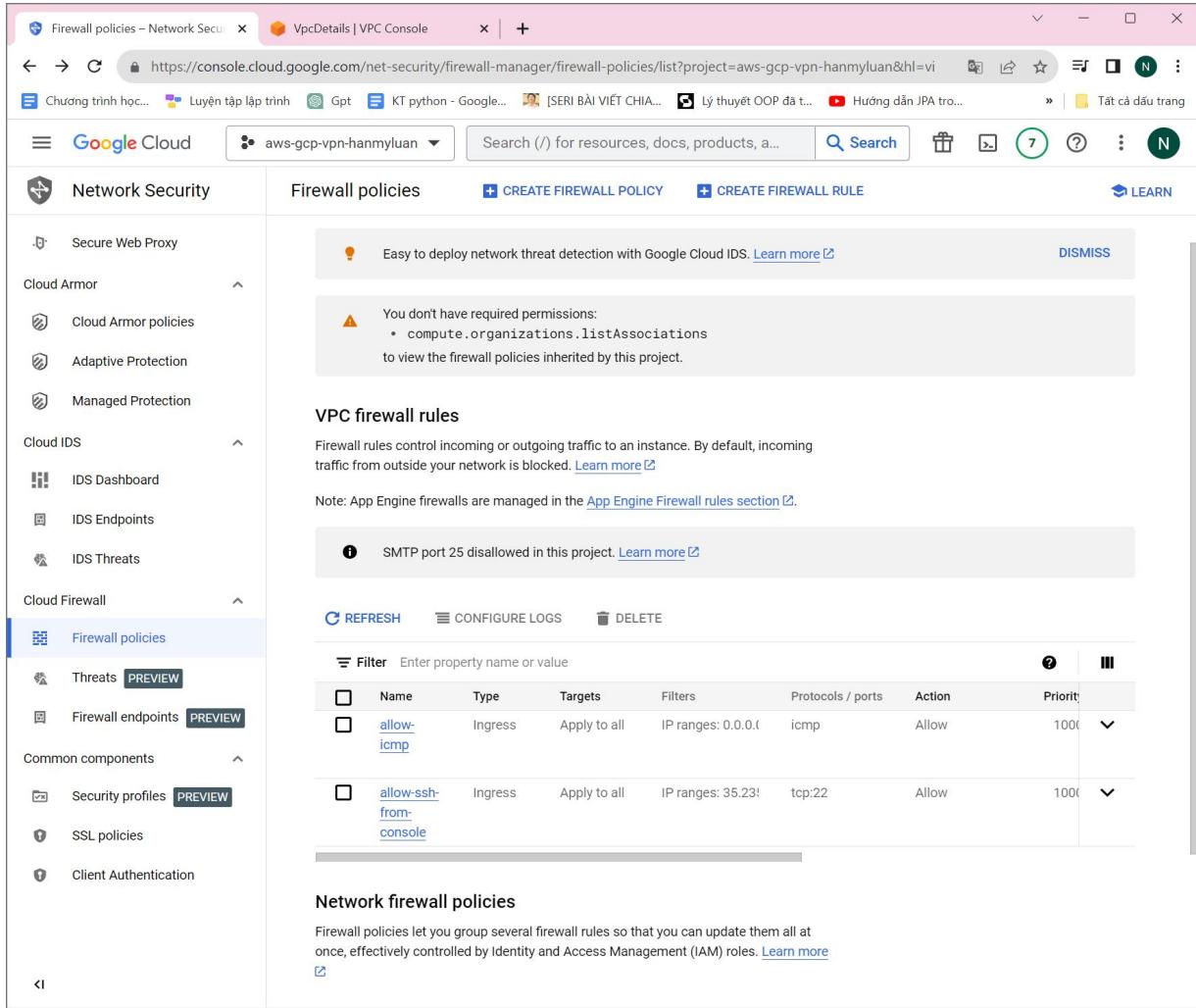
Reserved proxy-only subnets for load balancing

Name	Region	IP address ranges	Gateway	Role	Purpose
No rows to display					

EQUIVALENT REST



## + Tạo Firewall rules



The screenshot shows the Google Cloud VPC Firewall Manager interface. On the left, a sidebar lists various security components: Secure Web Proxy, Cloud Armor, Adaptive Protection, Managed Protection, Cloud IDS, IDS Dashboard, IDS Endpoints, IDS Threats, and Cloud Firewall. Under Cloud Firewall, 'Firewall policies' is selected, showing 'Threats' and 'Firewall endpoints' as previewed features. The main panel displays 'Firewall policies' with two entries:

Name	Type	Targets	Filters	Protocols / ports	Action	Priority
allow-icmp	Ingress	Apply to all	IP ranges: 0.0.0.1	icmp	Allow	1000
allow-ssh-from-console	Ingress	Apply to all	IP ranges: 35.23.1	tcp:22	Allow	1000

Below the table, a section titled 'Network firewall policies' explains that policies let you group rules for easier management. A note also mentions that App Engine firewalls are managed in a separate section.

## + Tạo Cloud Router

## -Tạo VPC trên AWS

### + Tạo tài khoản và cấu hình vpc

### + Tạo subnet

You have successfully created 1 subnet: subnet-0d2d13d328573d2ef

**Subnets (1/1) Info**

Subnet ID : subnet-0d2d13d328573d2ef

Actions Create subnet

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
subnet-us-east-1	subnet-0d2d13d328573d2ef	Available	vpc-031ae689647d125fd   vpc...	10.1.0.0/24	-

**subnet-0d2d13d328573d2ef / subnet-us-east-1**

**Details**

Subnet ID	subnet-0d2d13d328573d2ef	Subnet ARN	arn:aws:ec2:us-east-1:56875124825:subnet/subnet-0d2d13d328573d2ef	State	Available	IPv4 CIDR	10.1.0.0/24
Available IPv4 addresses	251	IPv6 CIDR	-	Availability Zone	us-east-1a	Availability Zone ID	use1-az4
Network border group	-	Network border group	-	Route table	-	Network ACL	-

## + Tạo Route tables

You have successfully updated subnet associations for rtb-0e7e1d18f3dacc21d / rt-aws-gcp-vpc-hanmyluan.

**Route tables (2) Info**

Route table ID Explicit subnet associations Edge associations Main VPC Own...

rt-aws-gcp-vpc-hanmyluan	rtb-0e7e1d18f3dacc21d	subnet-0d2d13d328573d2ef	-	Yes	vpc-031ae689647d125fd   vpc...	568751...
-	rtb-06ff3e7d81d3e68dc	-	-	Yes	vpc-05d24ea54d49981f   defa...	568751...

Select a route table

## + Tạo internet gateway

Internet gateway igw-0c216e04f2b2c6db7 successfully attached to vpc-031ae689647d125fd

igw-0c216e04f2b2c6db7 / igw-aws-gcp-vpn-hanmyluan

Details Info

Internet gateway ID: igw-0c216e04f2b2c6db7 State: Attached VPC ID: vpc-031ae689647d125fd | vpc-aws-gcp-vpn-hanmyluan Owner: 568751248425

Tags

Search tags

Key	Value
Name	igw-aws-gcp-vpn-hanmyluan

## + Bật DNS Hostname

You have successfully modified the settings for vpc-031ae689647d125fd / vpc-aws-gcp-vpn-hanmyluan.

vpc-031ae689647d125fd / vpc-aws-gcp-vpn-hanmyluan

Details Info

VPC ID: vpc-031ae689647d125fd	State: Available	DNS hostnames: Enabled	DNS resolution: Enabled
Tenancy: Default	DHCP option set: dopt-0340ab002383ba572	Main route table: rtb-0e7e1d18f3dacc21d / rt-aws-gcp-vpc-hanmyluan	Main network ACL: acl-036ea3ac9c0f17631
Default VPC: No	IPv4 CIDR: 10.1.0.0/16	IPv6 pool: -	IPv6 CIDR (Network border group): -
Network Address Usage metrics: Disabled	Route 53 Resolver DNS Firewall rule groups: -	Owner ID: 568751248425	

Resource map New | CIDRs | Flow logs | Tags | Integrations

Resource map Info

VPC Show details Subnets (1) Route tables (1) Network connections (1)

Your AWS virtual network Subnets within this VPC Route network traffic to resources Connections to other networks

vpc-aws-gcp-vpn-hanmyluan us-east-1a subnet-us-east-1 rt-aws-gcp-vpc-hanmyluan igw-aws-gcp-vpn-hanmyluar

Was the resource map helpful today? Give us feedback as often as

Updated routes for rtb-0e7e1d18f3dacc21d / rt-aws-gcp-vpc-hanmyluan successfully

rtb-0e7e1d18f3dacc21d / rt-aws-gcp-vpc-hanmyluan

Details

Route table ID: rtb-0e7e1d18f3dacc21d

Main: Yes

Owner ID: 568751248425

Explicit subnet associations: subnet-0d2d13d328573d2ef / subnet-us-east-1

Edge associations: -

Routes (2)

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0c216e04f2b2c6db7	Active	No
10.1.0.0/16	local	Active	No

## Bước 2: Kết nối VPN cho VPC của hai nền tảng

### - Tạo VPN trên GCP

Create a VPN - Network Connectivity Center

VPC | us-east-1

vpc-aws-gcp-hanmyluan - VPC

Create a VPN - Network Connectivity Center

Connectivity - aws-gcp-vpn...

console.cloud.google.com

Mức sử dụng bộ nhớ: 485 MB

ws-gcp-vpn-hanmyluan

Search (I) for resources, docs, products, and more

Network Connectivity

Network Connectivity Center

VPN

Interconnect

Cloud Routers

Create a VPN

1 Create Cloud HA VPN gateway

2 Add VPN tunnels

3 Configure BGP sessions

4 Summary and reminder

Add VPN tunnels

A VPN tunnel connects the Cloud VPN gateway to a peer gateway. Traffic sent through the tunnel is encrypted using the IPsec protocol operating in tunnel mode. [Learn more](#)

VPC network: vpc-aws-gcp-vpn-hanmyluan

Region: us-east1

VPN gateway name: vpn-gateway-aws-gcp-hanmyluan

Interfaces: 0 : 35.242.3.24 1 : 35.220.15.50

Peer VPN gateway:

On-prem or Non Google Cloud

Google Cloud

Peer VPN gateway name \*

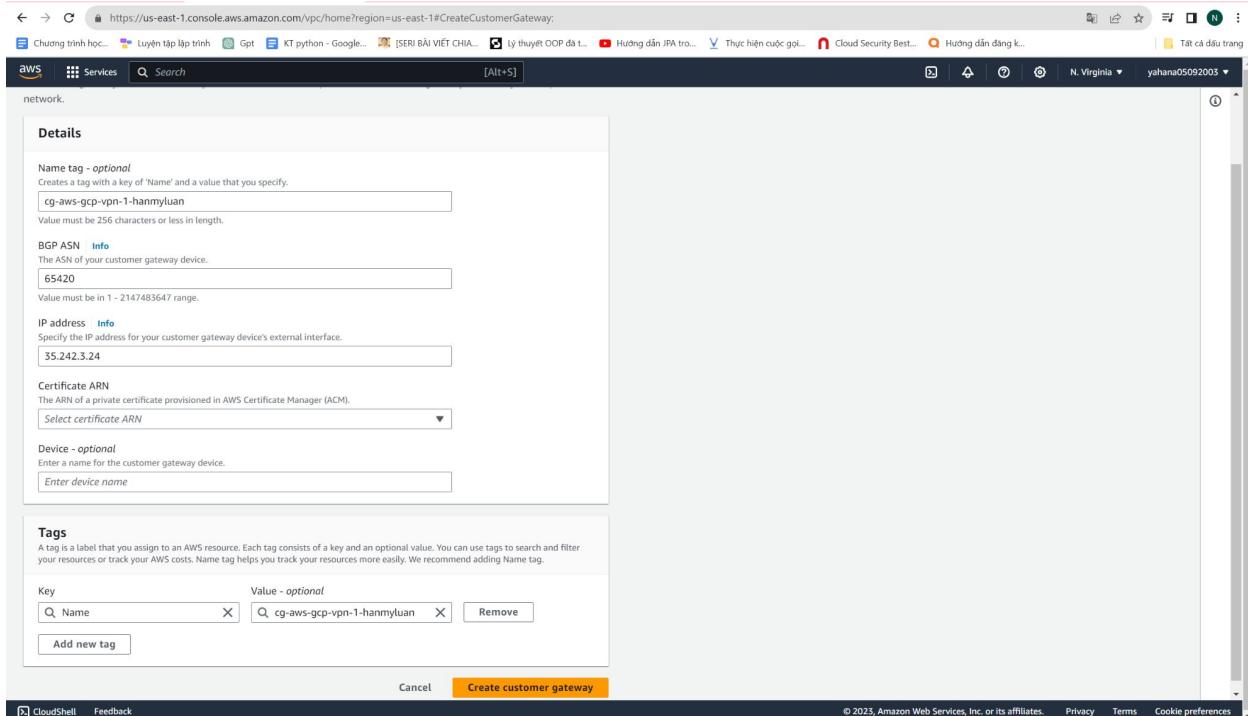
You can add more VPN tunnels to the same VPN gateway afterwards

CREATE & CONTINUE CANCEL

Created VPN gateway "vpn-gateway-aws-gcp-hanmyluan"

## - Trên AWS

### + Tạo Customer gateway



https://us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#CreateCustomerGateway

Chương trình học... Luyện tập lập trình Gpt Kt python - Google... [SERI BÀI VIẾT CHIA... Lý thuyết OOP đã t... Hướng dẫn JPA tro... Thực hiện cuộc gọi... Cloud Security Best... Hướng dẫn đăng k... Tất cả dấu trang

aws Services Search [Alt+S]

**Details**

**Name tag - optional**  
Creates a tag with a key of 'Name' and a value that you specify.  
cg-aws-gcp-vpn-1-hanmyluan

**BGP ASN** **Info**  
The ASN of your customer gateway device.  
65420

**IP address** **Info**  
Specify the IP address for your customer gateway device's external interface.  
35.242.3.24

**Certificate ARN**  
The ARN of a private certificate provisioned in AWS Certificate Manager (ACM).  
Select certificate ARN

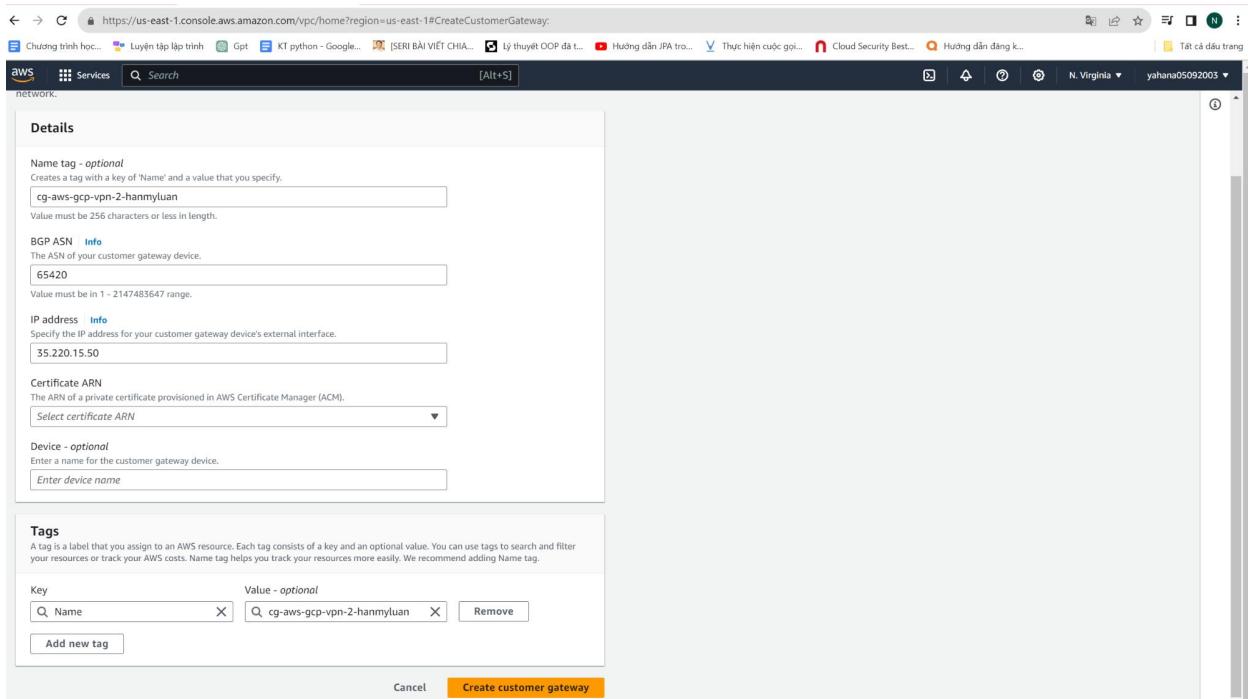
**Device - optional**  
Enter a name for the customer gateway device.  
Enter device name

**Tags**  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs. Name tag helps you track your resources more easily. We recommend adding Name tag.

Key Value - optional  
Name cg-aws-gcp-vpn-1-hanmyluan Remove

Add new tag

Cancel **Create customer gateway**



https://us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#CreateCustomerGateway

Chương trình học... Luyện tập lập trình Gpt Kt python - Google... [SERI BÀI VIẾT CHIA... Lý thuyết OOP đã t... Hướng dẫn JPA tro... Thực hiện cuộc gọi... Cloud Security Best... Hướng dẫn đăng k... Tất cả dấu trang

aws Services Search [Alt+S]

**Details**

**Name tag - optional**  
Creates a tag with a key of 'Name' and a value that you specify.  
cg-aws-gcp-vpn-2-hanmyluan

**BGP ASN** **Info**  
The ASN of your customer gateway device.  
65420

**IP address** **Info**  
Specify the IP address for your customer gateway device's external interface.  
35.22.0.15.50

**Certificate ARN**  
The ARN of a private certificate provisioned in AWS Certificate Manager (ACM).  
Select certificate ARN

**Device - optional**  
Enter a name for the customer gateway device.  
Enter device name

**Tags**  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs. Name tag helps you track your resources more easily. We recommend adding Name tag.

Key Value - optional  
Name cg-aws-gcp-vpn-2-hanmyluan Remove

Add new tag

Cancel **Create customer gateway**

### + Tạo Virtual private gateways

Virtual private gateways (1/1) info

Name	Virtual private gateway ID	State	Type	VPC	Amazon ASN
vgw-aws-gcp-hanmyluan...	vgw-0b4b30d3dbd8c7885	Attached	ipsec.1	vpc-031ae689647d125fd   vpc-a...	64512

Virtual private gateway vgw-0b4b30d3dbd8c7885 / vpg-aws-gcp-hanmyluan

Details Tags

Details

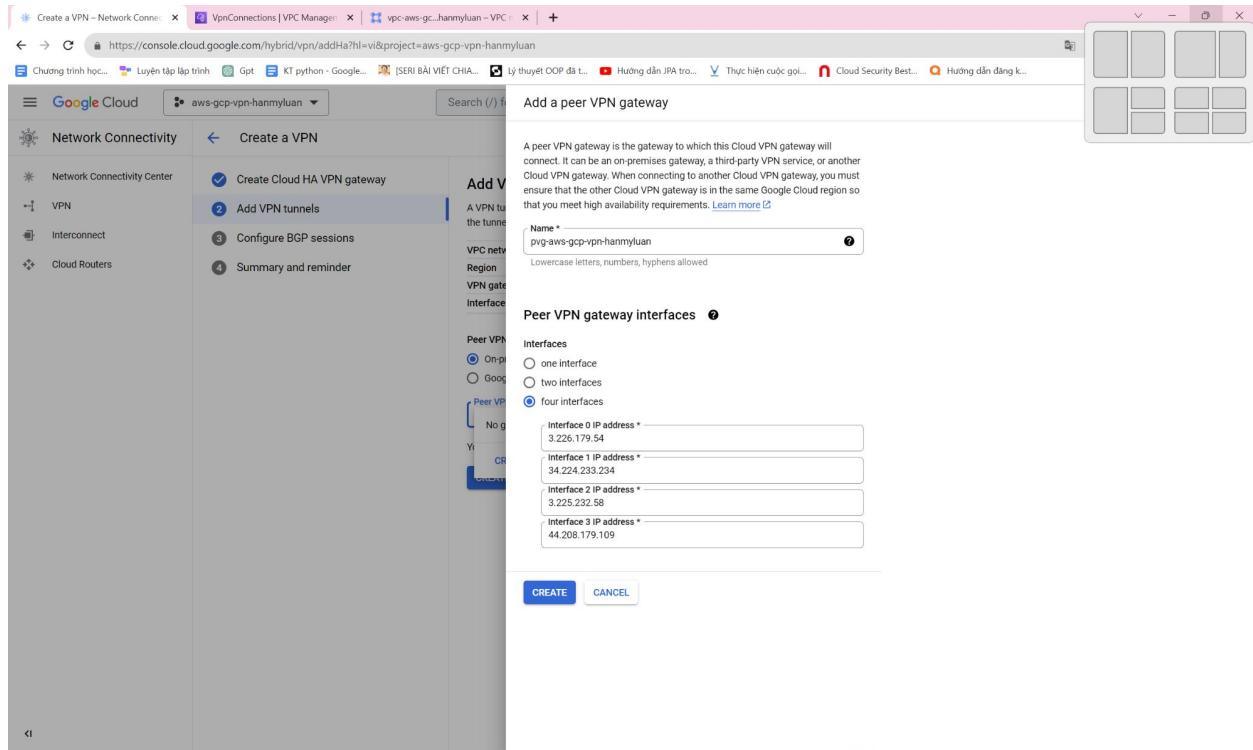
Virtual private gateway ID vgw-0b4b30d3dbd8c7885	State Attached	Type ipsec.1	VPC vpc-031ae689647d125fd   vpc-aws-gcp-vpn-hanmyluan
Amazon ASN 64512			

## + Tạo VPN Connection

VPN connections (2) info

Name	VPN ID	State	Virtual private gateway	Transit gateway	Customer gateway	Custom
vpn-aws-gcp-1-han...	vpn-0a78dafa3d276d4e1	Available	vgw-0b4b30d3dbd8c7885	-	cgw-0cd9104ef02873942	35.242.0.0/24
vpn-aws-gcp-2-han...	vpn-0640579735548978e	Available	vgw-0b4b30d3dbd8c7885	-	cgw-00c0a1b54045bd1df	35.220.0.0/24

Select a VPN connection



## + Lần lượt edit các tunnel dựa trên VPN Connection Configuration của AWS

- Link của 1-vpn-0a78daf3d276d4e1: [config\\_1](#)
- Link của 2-vpn-0640579735548978e: [config\\_2](#)

## Edit VPN tunnel



Associated Cloud VPN gateway interface

0 : 35.242.3.24

Associated peer VPN gateway interface \*

0 : 3.226.179.54



Name \*

vpm-tunnel-1-1



Lowercase letters, numbers, hyphens allowed

Description



IKE version

IKEv2



IKE pre-shared key \*

1\_aGHT6MxZAw6tbYmoVtdekCWFsv5.qT

[GENERATE AND COPY](#)

Enter your own key or generate one automatically



Make sure you record the pre-shared key in a secure location. The key can't be retrieved after this form is closed. [Learn more](#)

[DONE](#)

## Edit VPN tunnel



Associated Cloud VPN gateway interface

0 : 35.242.3.24

Associated peer VPN gateway interface \* —

1 : 34.224.233.234



Name \*

vpm-tunnel-1-2



Lowercase letters, numbers, hyphens allowed

Description



IKE version

IKEv2



IKE pre-shared key \*

DPrDhCWsTRxZMih\_7M4O\_chfOtE2WIRK

[GENERATE AND COPY](#)

Enter your own key or generate one automatically



Make sure you record the pre-shared key in a secure location. The key can't be retrieved after this form is closed. [Learn more](#)

[DONE](#)

## Edit VPN tunnel



Associated Cloud VPN gateway interface

1 : 35.220.15.50

Associated peer VPN gateway interface \*

2 : 3.225.232.58



Name \*

vpm-tunnel-2-1



Lowercase letters, numbers, hyphens allowed

Description



IKE version

IKEv2



IKE pre-shared key \*

FdH6dkE2fQTTQXIWvKpMdncBnCL53GxJ

[GENERATE AND COPY](#)

Enter your own key or generate one automatically



Make sure you record the pre-shared key in a secure location. The key can't be retrieved after this form is closed. [Learn more](#)

[DONE](#)

## Edit VPN tunnel



Associated Cloud VPN gateway interface

1 : 35.220.15.50

Associated peer VPN gateway interface \*

3 : 44.208.179.109



Name \*

vpm-tunnel-2-2



Lowercase letters, numbers, hyphens allowed

Description



IKE version

IKEv2



IKE pre-shared key \*

TsQVdKThwtOi2O6nQ4Fd8bErBf0AK2rr

[GENERATE AND COPY](#)

Enter your own key or generate one automatically



Make sure you record the pre-shared key in a secure location. The key can't be retrieved after this form is closed. [Learn more](#)

[DONE](#)

Name	Cloud VPN gateway (IP)	Peer VPN gateway (IP)	Cloud Router BGP IP address	Peer BGP IP address	VPN tunnel status	BGP session status	VPC network	Region
vpm-tunnel-1-1	vpn-gateway-aws-gcp-hanmyluan.35.242.3.24	pvg-aws-gcp-vpn-hanmyluan.3.226.179.54	169.254.68.118	169.254.68.117	Established	BGP established	vpc-aws-gcp-vpn-hanmyluan	us-east1
vpm-tunnel-1-2	vpn-gateway-aws-gcp-hanmyluan.35.242.3.24	pvg-aws-gcp-vpn-hanmyluan.34.224.233.234	169.254.37.206	169.254.37.205	Established	BGP established	vpc-aws-gcp-vpn-hanmyluan	us-east1
vpm-tunnel-2-1	vpn-gateway-aws-gcp-hanmyluan.35.220.15.50	pvg-aws-gcp-vpn-hanmyluan.3.225.232.58	169.254.169.174	169.254.169.173	Established	BGP established	vpc-aws-gcp-vpn-hanmyluan	us-east1
vpm-tunnel-2-2	vpn-gateway-aws-gcp-hanmyluan.35.220.15.50	pvg-aws-gcp-vpn-hanmyluan.44.208.179.109	169.254.56.158	169.254.56.157	Established	BGP established	vpc-aws-gcp-vpn-hanmyluan	us-east1

## + Kết quả kết nối VPN

Name	VPN ID	State	Virtual private gateway	Transit gateway	Customer gateway	Customer gateway
vpn-aws-gcp-1-han...	vpn-0a78dafa3d276d4e1	Available	vgw-0b4b30d3dbd8c7885	-	cgw-0cd9104ef02873942	35.242.3.24
vpn-aws-gcp-2-han...	vpn-0640579735548978e	Available	vgw-0b4b30d3dbd8c7885	-	cgw-00c0a1b54045bd1df	35.220.15.50

Tunnel number	Outside IP address	Inside IPv4 CIDR	Inside IPv6 CIDR	Status	Last status change	Details	Certificate ARN
Tunnel 1	3.226.179.54	169.254.68.116/30	-	Up	November 24, 2023, 13:00:15 (UTC+07:00)	1 BGP ROUTES	-
Tunnel 2	34.224.233.234	169.254.37.204/30	-	Up	November 24, 2023, 13:01:54 (UTC+07:00)	1 BGP ROUTES	-

The screenshot shows the AWS VPC console with the following details:

- VPN connections (1/2) info:**

Name	VPN ID	State	Virtual private gateway	Transit gateway	Customer gateway	Customer gateway
vpn-aws-gcp-1-han...	vpn-0a78dafa3d276d4e1	Available	vgw-0b4b30d3dbd8c7885	-	cgw-0cd9104ef02873942	35.242.3.24
vpn-aws-gcp-2-han...	vpn-0640579735548978e	Available	vgw-0b4b30d3dbd8c7885	-	cgw-00c0a1b54045bd1df	35.220.15.50
- VPN connection vpn-0640579735548978e / vpn-aws-gcp-2-hanmyluan:**
  - Tunnel state:**

Tunnel number	Outside IP Address	Inside IPv4 CIDR	Inside IPv6 CIDR	Status	Last status change	Details	Certificate ARN
Tunnel 1	3.225.232.58	169.254.169.172/30	-	Up	November 24, 2023, 13:00:20 (UTC+07:00)	0 BGP ROUTES	-
Tunnel 2	44.208.179.109	169.254.56.156/30	-	Up	November 24, 2023, 13:05:15 (UTC+07:00)	1 BGP ROUTES	-
  - Tunnel 1 options:** Info
  - Tunnel 2 options:** Info

## Bước 3: Test kết nối giữa 2 VPC

- Tạo instances trên hai nền tảng
- + Tạo instance test-vpn-connection trên AWS

The screenshot shows the AWS EC2 console with the following details:

- Instances (1/2) info:**

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
HanMyLuan	i-04f80bfs19ea5897b	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	ec2-107-20-49-242.co...	107.20.49.242	-
test-vpn-conn...	i-093fd6b13c0e1c469	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	ec2-3-87-83-209.comp...	3.87.83.209	-
- Instance: i-093fd6b13c0e1c469 (test-vpn-connection):**
  - Details:** Status and alarms New, Monitoring, Security, Networking, Storage, Tags
  - Instance summary:**
    - Instance ID: i-093fd6b13c0e1c469 (test-vpn-connection)
    - Public IPv4 address: 3.87.83.209 [open address]
    - Private IPv4 address: 10.1.213.125
    - Instance state: Running
    - Private IP DNS name (IPv4 only): ip-10-1-0-213.ec2.internal
    - Instance type: t2.micro
    - VPC ID: vpc-031ae689647d125fd (vpc-aws-gcp-vpn-hanmyluan)
    - Subnet ID: subnet-0d2d13d528573d2ef (subnet-us-east-1)

## + Tạo instance test-vpn-connection trên GG Cloud

## + Test kết nối

VM instances – Compute Engine | Network interfaces | EC2 | us-east-1 | Instance details | EC2 | us-east-1 | vpc-aws-g...-hammyluan – VPC | Create key pairs - Amazon Elasti... | ChatGPT | ← → ⌂ https://console.cloud.google.com/compute/instances?onCreate=true&h=vi&project=aws-gcp-vpn-hammyluan

Chương trình học... Luyện tập lập trình Gpt KT python - Google... [SERI BÀI VIẾT CHA... Lý thuyết OOP đ... Hướng dẫn JPA tro... Thực hiện cuộc gọi... Cloud Security Best... Hướng dẫn đăng k... Tất cả dấu trang

Google Cloud aws-gcp-vpn-hammyluan Search ( / ) for resources, docs, products, and more 15 N

Compute Engine VM instances CREATE INSTANCE IMPORT VM REFRESH

Virtual machines VM instances Instance templates Sole-tenant nodes Machine images TPUs Committed use discounts Reservations Migrate to Virtual Machin...

Storage Disks Snapshots Images Async Replication

Instance groups Instance groups Marketplace Release Notes

INSTANCES OBSERVABILITY INSTANCE SCHEDULES

VM instances

Filter Enter property name or value

Status	Name	Zone	Recommendations	In use by	Internal IP	External IP	Connect
Green	test-vpn-connection	us-east1-b			10.0.0.2 (nic0)	35.243.147.134 (nic0)	SSH

Related a Command Prompt

```

Ping statistics for 3.87.83.209:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 295ms, Maximum = 380ms, Average = 342ms

C:\Users\GIA HAN>ping 10.1.0.213

Pinging 10.1.0.213 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.1.0.213:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 276ms, Maximum = 380ms, Average = 342ms

C:\Users\GIA HAN>ping 35.243.147.134

Pinging 35.243.147.134 with 32 bytes of data:
Reply from 35.243.147.134: bytes=32 time=312ms TTL=56
Reply from 35.243.147.134: bytes=32 time=330ms TTL=56
Reply from 35.243.147.134: bytes=32 time=276ms TTL=56
Reply from 35.243.147.134: bytes=32 time=338ms TTL=56

Ping statistics for 35.243.147.134:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 276ms, Maximum = 338ms, Average = 314ms
  
```

## + Test kết nối giữa các subnet

VM instances

Filter Enter property name or value

Status	Name	Zone	Recommendations	In use by	Internal IP	External IP	Connect
Green	instance-1	us-east1-c			10.0.2.2 (nic0)	34.74.99.34 (nic0)	SSH
Green	test-vpn-connection	us-east1-b	Save \$6 / mo		10.0.0.2 (nic0)	35.243.147.134 (nic0)	SSH

Linux instance-1 5.10.0-26-cloud-amd64 #1 SMP Debian 5.10.197-1 (2023-09-29) x86\_64

The programs included with the Debian GNU/Linux system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/\*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.

g21110432@instance-1:~\$ ping 10.0.0.2

```

PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=1.39 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.394 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=0.419 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=0.329 ms
64 bytes from 10.0.0.2: icmp_seq=5 ttl=64 time=0.403 ms
^C
--- 10.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4059ms
rtt min/avg/max/mdev = 0.329/0.587/1.393/0.403 ms
g21110432@instance-1:~$ 
```

## -Test kết nối từ GCP đến AWS

Instance summary for i-093fd6b13c0e1c469 (test-vpn-connection)

Updated less than a minute ago

Instance ID: i-093fd6b13c0e1c469 (test-vpn-connection)

IPv6 address: -

Hostname type: IP name: ip-10-1-0-213.ec2.internal

Answer private resource DNS name: -

Auto-assigned IP address: 3.87.83.209 [Public IP]

IAM Role: -

IMDSv2: Optional

EC2 recommends setting IMDSv2 to required | Learn more

Details | Status and alarms New | Monitoring | Security | Networking | Storage

Instance details info

Platform: Amazon Linux (Inferred)

Platform details: Linux/UNIX

Stop protection: Disabled

AMI ID: ami-0230bd60a...

AMI name: al2023-ami-2023.2.20231113.0-kernel-6.1-x86\_64

AMI location: amazon/al2023-ami-2023.2.20231113.0-kernel-6.1-x86\_64

Termination protection: Disabled

AMI location: amazon/al2023-ami-2023.2.20231113.0-kernel-6.1-x86\_64

```
g21110432@test-vpn-connection:~$ ping 10.1.0.213
PING 10.1.0.213 (10.1.0.213) 56(84) bytes of data.
64 bytes from 10.1.0.213: icmp_seq=1 ttl=126 time=24.6 ms
64 bytes from 10.1.0.213: icmp_seq=2 ttl=126 time=18.2 ms
64 bytes from 10.1.0.213: icmp_seq=3 ttl=126 time=18.0 ms
64 bytes from 10.1.0.213: icmp_seq=4 ttl=126 time=13.0 ms
64 bytes from 10.1.0.213: icmp_seq=5 ttl=126 time=13.9 ms
64 bytes from 10.1.0.213: icmp_seq=6 ttl=126 time=19.3 ms
64 bytes from 10.1.0.213: icmp_seq=7 ttl=126 time=14.4 ms
64 bytes from 10.1.0.213: icmp_seq=8 ttl=126 time=13.8 ms
64 bytes from 10.1.0.213: icmp_seq=9 ttl=126 time=13.9 ms
64 bytes from 10.1.0.213: icmp_seq=10 ttl=126 time=13.7 ms
64 bytes from 10.1.0.213: icmp_seq=11 ttl=126 time=15.2 ms
64 bytes from 10.1.0.213: icmp_seq=12 ttl=126 time=13.6 ms
64 bytes from 10.1.0.213: icmp_seq=13 ttl=126 time=13.6 ms
64 bytes from 10.1.0.213: icmp_seq=14 ttl=126 time=14.1 ms
...

```

Instance summary for i-093fd6b13c0e1c469 (test-vpn-connection)

Updated less than a minute ago

Instance ID: i-093fd6b13c0e1c469 (test-vpn-connection)

IPv6 address: -

Hostname type: IP name: ip-10-1-0-213.ec2.internal

Answer private resource DNS name: -

Auto-assigned IP address: 3.87.83.209 [Public IP]

IAM Role: -

IMDSv2: Optional

EC2 recommends setting IMDSv2 to required | Learn more

Details | Status and alarms New | Monitoring | Security | Networking | Storage

Instance details info

Platform: Amazon Linux (Inferred)

Platform details: Linux/UNIX

Stop protection: Disabled

AMI ID: ami-0230bd60a...

AMI name: al2023-ami-2023.2.20231113.0-kernel-6.1-x86\_64

AMI location: amazon/al2023-ami-2023.2.20231113.0-kernel-6.1-x86\_64

Termination protection: Disabled

AMI location: amazon/al2023-ami-2023.2.20231113.0-kernel-6.1-x86\_64

```
g21110432@test-vpn-connection:~$ ping 10.1.0.213
PING 10.1.0.213 (10.1.0.213) 56(84) bytes of data.
64 bytes from 10.1.0.213: icmp_seq=1 ttl=126 time=24.6 ms
64 bytes from 10.1.0.213: icmp_seq=2 ttl=126 time=18.2 ms
64 bytes from 10.1.0.213: icmp_seq=3 ttl=126 time=18.0 ms
64 bytes from 10.1.0.213: icmp_seq=4 ttl=126 time=13.0 ms
64 bytes from 10.1.0.213: icmp_seq=5 ttl=126 time=13.9 ms
64 bytes from 10.1.0.213: icmp_seq=6 ttl=126 time=19.3 ms
64 bytes from 10.1.0.213: icmp_seq=7 ttl=126 time=14.4 ms
64 bytes from 10.1.0.213: icmp_seq=8 ttl=126 time=13.8 ms
64 bytes from 10.1.0.213: icmp_seq=9 ttl=126 time=13.9 ms
64 bytes from 10.1.0.213: icmp_seq=10 ttl=126 time=13.7 ms
64 bytes from 10.1.0.213: icmp_seq=11 ttl=126 time=15.2 ms
64 bytes from 10.1.0.213: icmp_seq=12 ttl=126 time=13.6 ms
64 bytes from 10.1.0.213: icmp_seq=13 ttl=126 time=13.6 ms
64 bytes from 10.1.0.213: icmp_seq=14 ttl=126 time=14.1 ms
...

```

## -Bước 4: Chuyển file từ S3 của AWS sang GCP

+Tạo bucket trên AWS

+ Tạo Transfer job để nhận tài nguyên được chuyển phát

← → 🔍 https://console.cloud.google.com/transfer/create?hl=vi&project=aws-gcp-vpn-hanmyluan

Chương trình học... Luyện tập lập trình Gpt KT python - Google... [SERI BÀI VIẾT CHIA... Lý thuyết OOP đ... Hướng dẫn JPA tro... Thực hiện cuộc gọi... Cloud Security Best... Hướng dẫn đăng k... Tất cả dấu trang

☰ Google Cloud aws-gcp-vpn-hanmyluan Search (/) for resources, docs, products, and more

Storage Transfer Create a transfer job

Get started Amazon S3 to Google Cloud Storage

Choose a source aws-gcp-hanmyluan Some form fields are incorrect

Choose a destination

Choose when to run job Batch - Run job once - Starting now

Choose settings Never delete files

CREATE CANCEL

Choose a source

Specify your source details. You'll need read access.

Bucket or folder \* aws-gcp-hanmyluan

Ex: mybucket/path/to/myfolder/

CloudFront domain (optional)

Specify an Amazon CloudFront distribution as your egress path. Learn more. Ex: https://ab1c2d3e4f56.cloudfront.net

Credentials

Authentication options

Access key (selected)

AWS IAM role for identity federation

Secret resource

AWS Management Console instructions: Navigate to Your Security Credentials and open the Access keys section. Click Create New Access Key. In the dialog that appears, click Show Access Keys to see your new access key ID and secret access key.

SHOW MORE

Access Key ID \* AKIAV13BXKQU5GGJHJD

Secret access key \*

Choose which data to transfer

Filter by prefix

Filter by last modified time

NEXT STEP

## +Kết quả

← → 🔍 https://console.cloud.google.com/transfer/jobs?jobType=ALL&page=1&hl=vi&project=aws-gcp-vpn-hanmyluan

Chương trình học... Luyện tập lập trình Gpt KT python - Google... [SERI BÀI VIẾT CHIA... Lý thuyết OOP đ... Hướng dẫn JPA tro... Thực hiện cuộc gọi... Cloud Security Best... Hướng dẫn đăng k... Tất cả dấu trang

☰ Google Cloud aws-gcp-vpn-hanmyluan Search (/) for resources, docs, products, and more

Storage Transfer Transfer jobs CREATE TRANSFER JOB

Transfer jobs Agent pools

Quickly and securely transfer data to, from, and between cloud and on-premises storage systems. Sources include Google Cloud Storage, Amazon S3, Azure Storage, filesystems, and more. [Learn more](#)

ALL	CLOUD-TO-CLOUD	TO/FROM FILESYSTEMS						
<input type="checkbox"/> Job ID	Description	Source type	Source	Destination type	Destination	Scheduling mode	Latest operation started	Latest operation status
<input type="checkbox"/> 2339490620279435525		Amazon S3	aws-gcp-hanmyluan	Google Cloud Storage	saves3	Batch (not recurring)	Nov 24, 2023, 3:15:21 PM	Success

"transferJobs/2339490620279435525..." has been created successfully! ×

https://console.cloud.google.com/transfer/jobs/transferJobs%2F233949062027943552/runs?hl=vi&project=aws-gcp-vpn-hanmyluan

Chương trình học... Luyện tập lập trình Gpt KT python - Google... [SERI BÀI VIẾT CHIA... Lý thuyết OOP đã t... Hướng dẫn JPA tro... Thực hiện cuộc gọi... Cloud Security Best... Hướng dẫn đăng k... Tất cả dấu trang

Google Cloud aws-gcp-vpn-hanmyluan Search (i) for resources, docs, products, and more

Storage Transfer Job details START A RUN DELETE JOB COPY JOB DISABLE JOB

Transfer jobs Agent pools

233949062027943552

Job information

Full resource name transferJobs/233949062027943552  
Description —  
Scheduling mode Batch (not recurring)

Source

Type Amazon S3  
Name aws-gcp-vpn-hanmyluan  
Folder path —

Destination

Type Google Cloud Storage  
Name saves3  
Folder path —

MONITORING OPERATIONS CONFIGURATION

Latest run of 'transferJobs/233949062027943552'

Status Success  
Start time November 24, 2023 at 3:15:21 PM UTC+7  
End time November 24, 2023 at 3:15:42 PM UTC+7  
Duration 20 sec

Progress 100% Data transferred 78.6 KB of 78.6 KB 1 of 1 file Errors 0 Data skipped 0 B 0 files Average speed estimate 3.88 KB/s Estimated based on data transferred and duration

Changes made after start time may not be discovered until the next transfer

Run history

Start time	Status	Percent successful	Data transferred	Data size	Errors	Duration	End time
November 24, 2023 at 3:15:21 PM UTC+7	Success	100%	78.6 KB	78.6 KB	—	20 sec	November 24, 2023 at 3:15:42 PM UTC+7

https://console.cloud.google.com/storage/browser/\_details/saves3/z4831303858093\_b895e075627c7165ec23b2542767af08.jpg;tab=live\_object?hl=vi&project=aws-gcp-vpn-hanmyluan

Chương trình học... Luyện tập lập trình Gpt KT python - Google... [SERI BÀI VIẾT CHIA... Lý thuyết OOP đã t... Hướng dẫn JPA tro... Thực hiện cuộc gọi... Cloud Security Best... Hướng dẫn đăng k... Tất cả dấu trang

Google Cloud aws-gcp-vpn-hanmyluan Search (i) for resources, docs, products, and more

Cloud Storage Object details

Buckets > saves3 > z4831303858093\_b895e075627c7165ec23b2542767af08.jpg

Overview

Type image/jpeg  
Size 78.6 KB  
Created Nov 24, 2023, 3:15:33 PM  
Last modified Nov 24, 2023, 3:15:33 PM  
Storage class Standard  
Custom time —  
Public URL Not applicable  
Authenticated URL [https://storage.cloud.google.com/saves3/z4831303858093\\_b895e075627c7165ec23b2542767af08.jpg](https://storage.cloud.google.com/saves3/z4831303858093_b895e075627c7165ec23b2542767af08.jpg)  
gsutil URI gs://saves3/z4831303858093\_b895e075627c7165ec23b2542767af08.jpg

Permissions

Public access Not public

Protection

Version history —  
Retention policy None  
Hold status None  
Encryption type Google-managed



-Các best practices security đã dùng

+ Tạo Nhiều Subnet:

Subnets									
SUBNETS		STATIC INTERNAL IP ADDRESSES		FIREWALLS		FIREWALL ENDPOINTS		ROUTES	
Subnets		+ ADD SUBNET		FLOW LOGS					
<input type="checkbox"/>	Name <span>↑</span>	Region	Stack Type	Internal IP ranges	External IP ranges	Secondary IPv4 ranges	Gateway	Private Google Access	Flow logs <span>?</span>
<input type="checkbox"/>	subnet-us-east-1	us-east1	IPv4	10.0.0.0/24	None	None	10.0.0.1	Off	On <span>trash</span>
<input type="checkbox"/>	subnet-us-east-2	us-east1	IPv4	10.0.2.0/24	None	None	10.0.2.1	Off	On <span>trash</span>

## + Cấu hình firewall rules

Firewalls													
ADD FIREWALL RULE		DELETE		Filter Enter property name or value									
<input type="checkbox"/>	Name	Enforcement order <span>↑</span>	Type	Deployment scope	Rule priority	Targets	Source	Destination	Protocols and ports	Action	Security profile group	TLS inspection	Hit count <span>?</span>
<input type="checkbox"/>	vpc-firewall-rules	1	VPC firewall rules	Global									

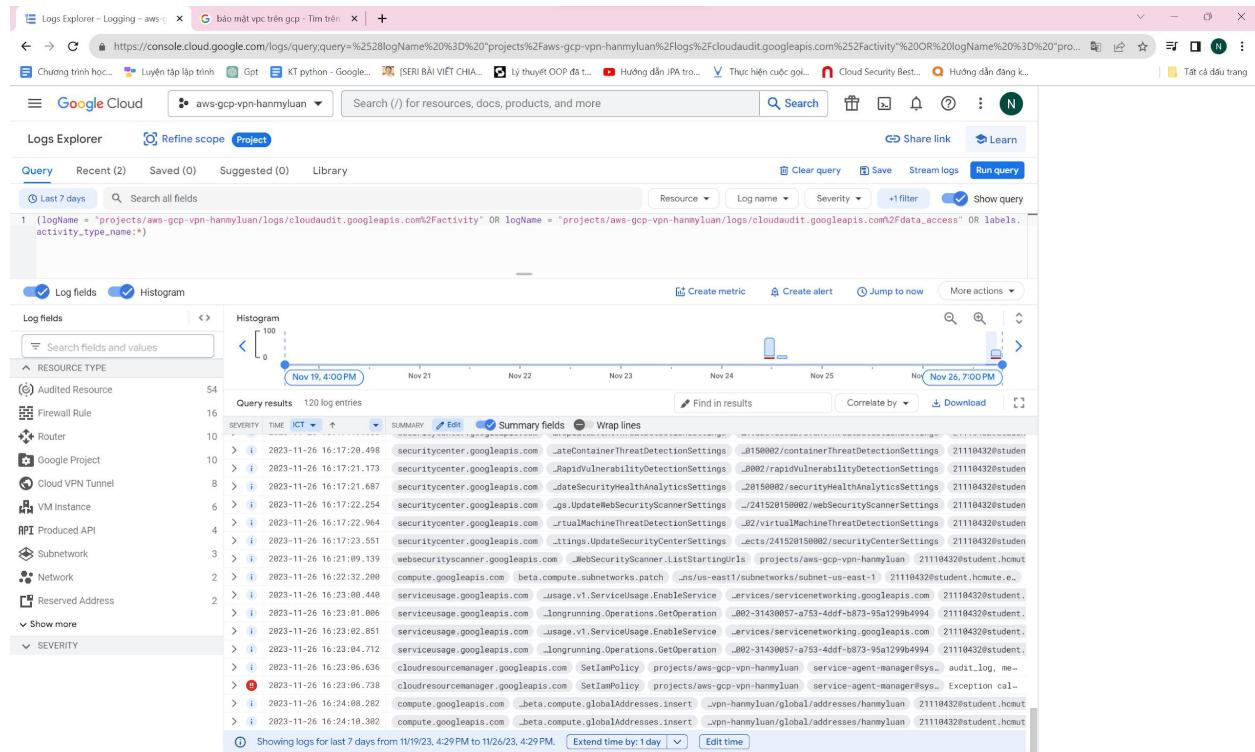
## + Cấu hình private service access

PRIVATE SERVICE ACCESS																	
ALLOCATED IP RANGES FOR SERVICES		PRIVATE CONNECTIONS TO SERVICES															
Internal IP address ranges that are allocated for services private connection <a href="#">Learn more</a>																	
Use Private Service Access to connect to specific Google and third-party services without assigning external IP addresses to your Google Cloud and Google or third-party resources <a href="#">Learn more</a>																	
Private services access requires you to first allocate an internal IPv4 address range and then create a private connection <a href="#">Learn more</a>																	
<a href="#">ALLOCATED IP RANGE</a> <a href="#">RELEASE</a>																	
<input type="checkbox"/> Name <span>↑</span> Internal IP range Service producer Connection name																	
<input type="checkbox"/> hanmyluan 10.178.204.0/24 - -																	
<a href="#">EQUIVALENT REST</a>																	

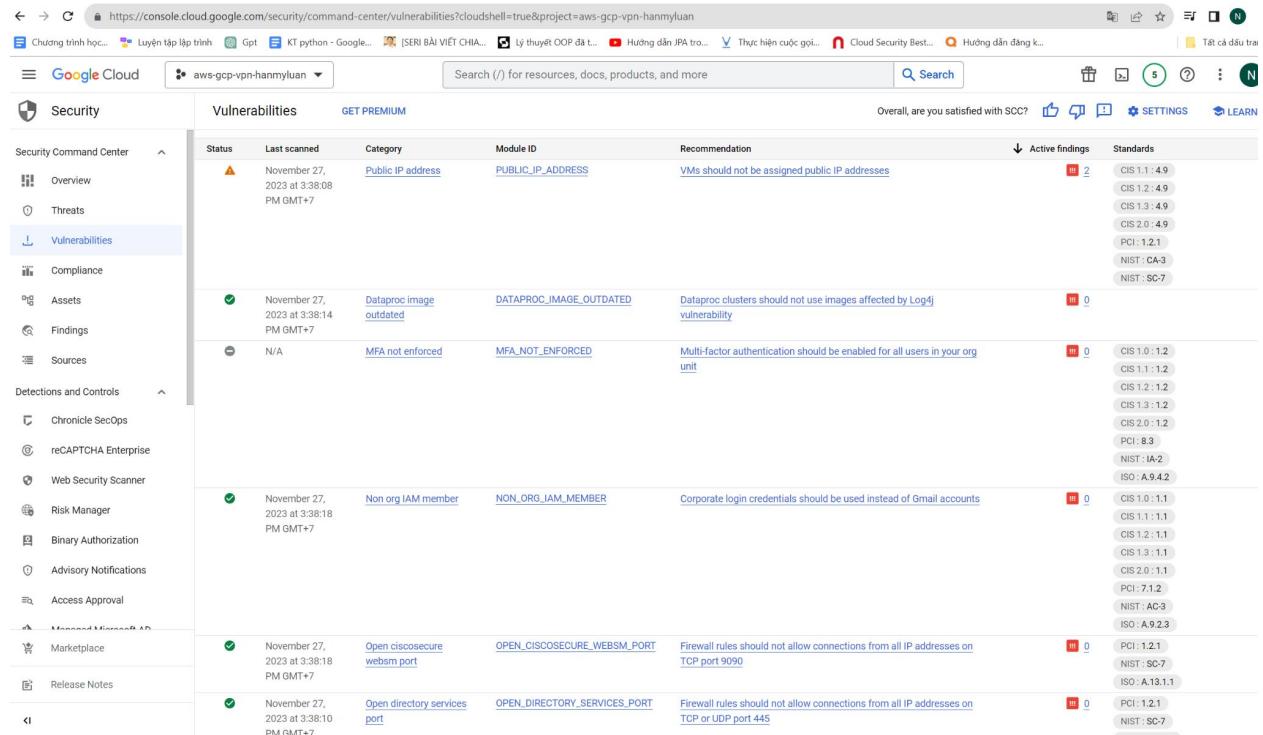
## + Phân quyền trong IAM & Admin

The screenshot shows the Google Cloud IAM & Admin interface. The left sidebar has 'IAM & Admin' selected. The main area shows 'Permissions for project "aws-gcp-vpn-hanmyluan"'. It lists two principals: '2110432@student.hcmute.edu.vn' (Owner) and '241520150002-compute@developer.gserviceaccount.com' (Editor). The 'VIEW BY PRINCIPALS' tab is selected. A 'GRANT ACCESS' button is visible. A 'Filter' input field is at the bottom. A checkbox for 'Include Google-provided role grants' is present.

## + Sử dụng Flowlog



## +Sử dụng tính năng Security Health Analytics



## 4.2. Các khó khăn và giải pháp

### a. Khó Khăn: Không Thể Kết Nối Các Dịch Vụ AWS

Giải Pháp: Sử Dụng Kết Nối HA VPN:

- Sử dụng kết nối HA VPN giữa GCP và AWS để thiết lập một đường ống an toàn và chịu lỗi cho việc truyền dữ liệu giữa hai môi trường.
- Đảm bảo rằng cấu hình VPN được thực hiện đúng đắn và tuân thủ các yêu cầu bảo mật.

### b. Khó Khăn: Không Biết Cấu Hình Bảo Mật

Giải Pháp: Sử Dụng Dịch Vụ Bảo Mật Của GCP:

- Tận dụng các dịch vụ bảo mật của GCP như Security Health Analytics để kiểm tra và đánh giá mức độ bảo mật của hạ tầng.
- Xem xét và cấu hình các tùy chọn bảo mật trong GCP Console, bao gồm các luật tường lửa, IAM Roles, và các tùy chọn mật khẩu.

### c. Khó Khăn: Chia IP Range Không Hợp Lý Dẫn Đến Xung Đột

Giải Pháp: Xác Định CIDR Đúng Đắn Cho Subnet:

- Xác định CIDR range cho các subnet một cách cẩn thận để tránh xung đột.
- Sử dụng công cụ quản lý IP và CIDR như CIDR Calculator để hỗ trợ việc xác định IP range hợp lý.

### d. Khó Khăn: Thiếu Kinh Nghiệm và Trải Nghiệm Thực Tế

Giải Pháp: Tra Cứu và Học Từ Tài Liệu Chính Thống:

- Tìm hiểu từ tài liệu chính thống và hướng dẫn của cả GCP và AWS để hiểu rõ hơn về các quy trình và quy định cấu hình.
- Tham gia các khóa học trực tuyến và tìm kiếm thông tin từ cộng đồng để nâng cao kỹ năng và kiến thức như Youtube, StackOverflow...

### e. Khó Khăn: Tích Hợp Các Dịch Vụ An Ninh của GCP

Giải Pháp: Tích Hợp Security Health Analytics:

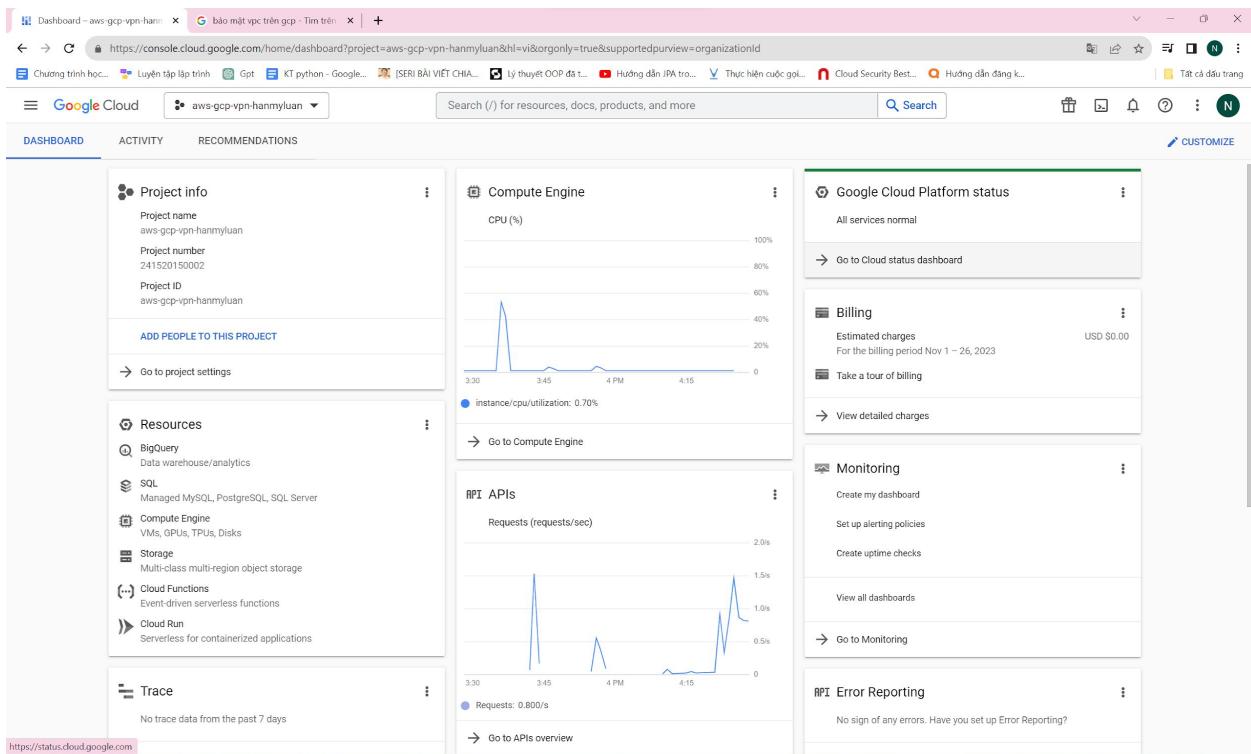
- Sử dụng dịch vụ như Security Health Analytics của GCP để tự động phát hiện và cảnh báo về các vấn đề bảo mật.
  - Cấu hình cảnh báo để nhận thông báo ngay khi có vấn đề liên quan đến bảo mật.
- f. *Khó Khăn: Kiểm Soát Bảo Mật trong Cả Hai Môi Trường*

Giải Pháp: Tạo Các Luật Tường Lửa và IAM Roles Thống Nhất:

- Tạo các luật tường lửa và IAM Roles có thể sử dụng chung giữa GCP và AWS để đảm bảo sự đồng nhất trong quản lý bảo mật.
- Thực hiện kiểm tra định kỳ để đảm bảo rằng quy định và cấu hình bảo mật không bị phá vỡ.

## 5. KẾT QUẢ VÀ ĐÁNH GIÁ

- Các subnet trong VPC có thể kết nối được với nhau một cách dễ dàng.
- Các quy tắc về tường lửa được cấu hình đúng, kết nối được với AWS trên cổng cho phép và chặn các kết nối còn lại.
- Phân quyền truy cập đã được cung cấp đúng theo quy tắc của tối thiểu quyền cần thiết.
- Flow Logs trả về được các thông tin chi tiết và chính xác về lưu lượng mạng, đồng thời cảnh báo khi xảy ra lỗi.



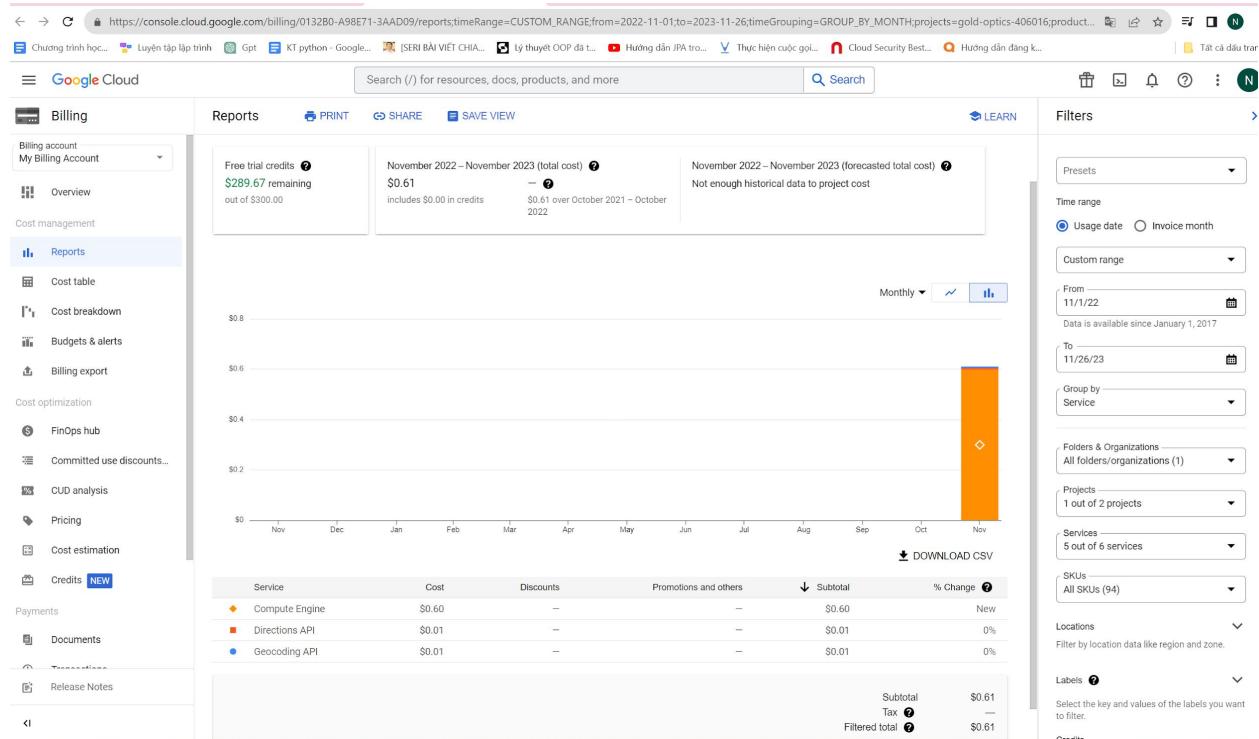
### - Ưu điểm:

- + Tạo được VPC trên nền tảng GCP để lưu trữ dữ liệu và thực hiện chuyển đổi được dữ liệu với VPC trên AWS.
- + Thực hiện được một số biện pháp bảo mật cho đám mây riêng nhằm tránh sự tấn công hay mất dữ liệu

### - Nhược điểm:

- + Chưa khai thác được nhiều các dịch vụ mà GCP cung cấp.
- + Các biện pháp bảo mật còn ít, chưa linh hoạt. Nhiều dịch vụ bảo mật yêu cầu chi phí cao nhưng tài chính không đủ để trải nghiệm.

## 6. PHÂN TÍCH DỊCH VỤ VÀ CÔNG NGHỆ CLOUD



Do sử dụng free trial nên những chi phí phát sinh sẽ tự động trừ vào 300\$ được cấp miễn phí

## 7. KẾT LUẬN

### 7.1. Tổng kết

Trong quá trình triển khai và kết nối VPN giữa Google Cloud và AWS để tạo Virtual Private Cloud (VPC), chúng em đã thành công trong việc xây dựng một môi trường mạng linh hoạt và an toàn, kết nối hai nền tảng đám mây hàng đầu một cách hiệu quả.

Việc tạo VPC trên Google Cloud Platform (GCP) đã được thực hiện một cách suôn sẻ, đặt nền móng cho việc triển khai và quản lý tài nguyên mạng. Quá trình này bao gồm cấu hình subnet, firewall rules, và sử dụng các tính năng như Private Service Access để giữ cho môi trường mạng nội bộ và an toàn.

Việc kết nối VPN giữa GCP và AWS đã được thực hiện thành công, tạo ra một cầu nối an toàn và hiệu quả giữa hai môi trường đám mây khác nhau. Điều này giúp

chúng em tận dụng sự linh hoạt của cả hai nền tảng để triển khai ứng dụng và dịch vụ một cách toàn diện.

Đối với biện pháp bảo mật, chúng em đã thường xuyên thực hiện kiểm tra và cập nhật các quy tắc tường lửa (Firewall Rules) để đảm bảo rằng chỉ có lưu lượng cần thiết được chấp nhận. Các chiến lược IAM & Admin Permissions được áp dụng để tối thiểu hóa quyền truy cập và giữ cho quản lý hệ thống được kiểm soát chặt chẽ. Đồng thời, việc sử dụng Flow Logs đã hỗ trợ chúng em trong việc giám sát và phân tích lưu lượng mạng, đặt nền tảng cho khả năng theo dõi và giải quyết sự cố mạng.

Tóm lại, thông qua việc tạo VPC, kết nối VPN giữa GCP và AWS, cùng với việc thực hiện các biện pháp bảo mật đều đặn, chúng em đã xây dựng một môi trường đám mây an toàn, linh hoạt và có khả năng mở rộng, giúp ứng dụng và dịch vụ của chúng em hoạt động mạnh mẽ và ổn định.

## 7.2. Đề xuất hướng phát triển

Từ đê tài đã triển khai và kết quả đạt được, nhóm chúng em có một số đề xuất phát triển như sau:

- **Tối Ưu Hóa Tài Nguyên Mạng:**
  - Tiếp tục theo dõi và tối ưu hóa cấu hình mạng, đảm bảo rằng subnet, địa chỉ IP, và băng thông đều được sử dụng hiệu quả.
  - Xem xét việc triển khai CDN (Content Delivery Network) để cải thiện hiệu suất truy cập từ các vị trí khác nhau trên thế giới.
- **Mở Rộng Kết Nối và Tích Hợp Dịch vụ Khác:**
  - Nghiên cứu và triển khai các dịch vụ mở rộng khác của cả GCP và AWS để đáp ứng nhu cầu kinh doanh cụ thể.
  - Xem xét việc tích hợp các dịch vụ quản lý và giám sát để đơn giản hóa quá trình quản lý.
- **Tăng Cường Bảo Mật và Theo Dõi:**

- Thực hiện các biện pháp bảo mật tiên tiến như Encryption at Rest cho các dữ liệu quan trọng.
- Tăng cường quá trình giám sát và báo cáo bằng cách tích hợp các giải pháp tự động hóa và phân tích dữ liệu.
- Thăm Dò Công Nghệ Mới:
  - Duy trì một quá trình liên tục để thăm dò và đánh giá các công nghệ mới có thể tối ưu hóa hoặc cải thiện môi trường đám mây.
  - Xem xét việc triển khai các dịch vụ mới như serverless computing để tối ưu hóa chi phí và tăng cường hiệu suất.

Bằng cách thực hiện những hướng phát triển này, chúng em tin rằng môi trường đám mây sẽ ngày càng trở nên mạnh mẽ, linh hoạt và đáp ứng được các thách thức và cơ hội trong tương lai.

## TÀI LIỆU THAM KHẢO

1. “What is a Private Cloud? - Private Cloud Explained.” AWS, <https://aws.amazon.com/what-is/private-cloud/>. Accessed 23 November 2023.
2. “AWS là gì.” AWS, <https://aws.amazon.com/vi/what-is-aws/>. Accessed 23 November 2023.
3. “Tìm hiểu về AWS phần 1: VPC - Virtual Private Cloud.” Viblo, <https://viblo.asia/p/tim-hieu-ve-aws-phan-1-vpc-virtual-private-cloud-924lJGv05PM>. Accessed 24 November 2023.
4. “Tổng quan về Cloud Firewall (Tường lửa đám mây)” ViettelIDC, <https://www.viettelidc.com.vn/tin-tuc/tong-quan-ve-cloud-firewall-tuong-lua-dam-may>. Accessed 26 November 2023.
5. “What is identity and access management? Guide to IAM” TechTarget, <https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system>. Accessed 26 November 2023.
6. “What is a virtual private cloud (VPC)?” Cloudflare, <https://www.cloudflare.com/learning/cloud/what-is-a-virtual-private-cloud/>. Accessed 26 November 2023.
7. “Google Cloud Platform là gì? Những dịch vụ Google Cloud Platform” BKNS, <https://www.bkns.vn/google-cloud-platform-la-gi.html>. Accessed 26 November 2023.