Contents

[**Giai đoạn 2: Bảo mật VPCs** 3](#_Toc202377880)

[**Nhiệm vụ 2.1: Xem lại LabVPC và các tài nguyên liên quan** 3](#_Toc202377881)

[**Bước 1: Mở Amazon VPC Console và kiểm tra VPC** 3](#_Toc202377882)

[**Bước 2: Kiểm tra IAM Role cho VPC Flow Logs** 4](#_Toc202377883)

[**Bước 3: Mở Amazon EC2 Console và kiểm tra WebServer Instance** 5](#_Toc202377884)

[**Nhiệm vụ 2.2: Tạo một VPC Flow Log cho VPC** 8](#_Toc202377885)

[**Bước 1: Truy cập vào VPC** 8](#_Toc202377886)

[**Bước 2: Chọn VPC LabVPC** 8](#_Toc202377887)

[**Bước 3: Tạo Flow Log** 8](#_Toc202377888)

[**Bước 4: Cấu hình Flow Log** 8](#_Toc202377889)

[**Bước 5: Tạo Flow Log** 9](#_Toc202377890)

[**Nhiệm vụ 2.3: Truy cập phiên bản WebServer từ internet và xem lại nhật ký luồng VPC trong CloudWatch** 9](#_Toc202377891)

[**Bước 1: Thử truy cập WebServer bằng trình duyệt** 9](#_Toc202377892)

[**Bước 2: Kiểm tra truy cập từ Cloud9** 10](#_Toc202377893)

[**Bước 3: Xem lại VPC Flow Logs trên CloudWatch** 11](#_Toc202377894)

[**Bước 4: Lọc log theo IP của Cloud9** 12](#_Toc202377895)

[**Bước 5: Lọc log theo IP máy tính của bạn** 13](#_Toc202377896)

[**Nhiệm vụ 2.4: Cấu hình bảng định tuyến và cài đặt nhóm bảo mật** 14](#_Toc202377897)

[**Bước 1: Cấu hình Route Table** 14](#_Toc202377898)

[**Bước 2: Kiểm tra HTTP từ trình duyệt** 16](#_Toc202377899)

[**Bước 3: Chỉnh sửa Security Group** 16](#_Toc202377900)

[**Bước 4: Kiểm tra kết nối** 18](#_Toc202377901)

[**Nhiệm vụ 2.5: Bảo mật WebServerSubnet bằng ACL mạng** 19](#_Toc202377902)

[**Bước 1: Điều hướng đến Network ACL** 19](#_Toc202377903)

[**Bước 2: Chỉnh sửa Rule 100 để TỪ CHỐI port 22** 20](#_Toc202377904)

[**Bước 3: Kiểm tra bằng nc (netcat):** 20](#_Toc202377905)

[**Bước 4: Kiểm tra HTTP trên trình duyệt:** 21](#_Toc202377906)

[**Bước 5: Cho phép lại port 22 (SSH) trong rule 100** 21](#_Toc202377907)

[**Bước 6: Kiểm tra lại SSH bằng netcat** 22](#_Toc202377908)

[**Bước 7: Thêm Rule 90 để cho phép HTTP traffic** 22](#_Toc202377909)

[**Bước 8: Truy cập lại website** 22](#_Toc202377910)

[**Nhiệm vụ 2.6: Đánh giá NetworkFirewallVPC và các tài nguyên liên quan** 23](#_Toc202377911)

[**Bước 1: Kiểm tra cấu trúc NetworkFirewallVPC** 23](#_Toc202377912)

[**Bước 2: Kiểm tra cấu hình Network ACL** 23](#_Toc202377913)

[**Bước 3: Xác minh truy cập WebServer2** 24](#_Toc202377914)

[**Bước 4: Chuẩn bị sơ đồ mạng (Network Firewall Diagram) ko cần làm** 25](#_Toc202377915)

[**Bước 5: Cách routing hoạt động (giải thích) Ko cần làm** 26](#_Toc202377916)

[**Nhiệm vụ 2.7: Tạo tường lửa mạng** 26](#_Toc202377917)

[**Bước 1: Truy cập Amazon VPC Console** 26](#_Toc202377918)

[**Bước 2: Tạo Network Firewall** 27](#_Toc202377919)

[**Bước 3: Nhập thông tin firewall** 27](#_Toc202377920)

[**Bước 4: Configure advanced settings** 27](#_Toc202377921)

[**Bước 5: Associate firewall policy** 27](#_Toc202377922)

[**Bước 6: Hoàn tất** 27](#_Toc202377923)

[**Bước 7: Kiểm tra trạng thái** 27](#_Toc202377924)

[**Nhiệm vụ 2.8: Tạo bảng lộ trình** 27](#_Toc202377925)

[**Bước 1: Tạo bảng định tuyến cho Internet Gateway** 27](#_Toc202377926)

[**Bước 2: Tạo bảng định tuyến cho FirewallSubnet** 28](#_Toc202377927)

[**Bước 3: Tạo bảng định tuyến cho WebServer2Subnet** 30](#_Toc202377928)

[**Nhiệm vụ 2.9: Cấu hình ghi nhật ký cho tường lửa mạng** 31](#_Toc202377929)

[**Bước 1: Tạo CloudWatch Log Group** 31](#_Toc202377930)

[**Bước 2: Cấu hình log cho Network Firewall** 32](#_Toc202377931)

[**Bước 3: Kiểm tra cấu hình logging** 34](#_Toc202377932)

[**Bước 4: Kiểm tra log trong CloudWatch** 34](#_Toc202377933)

[**Nhiệm vụ 2.10: Cấu hình chính sách tường lửa và kiểm tra quyền truy cập** 35](#_Toc202377934)

[**Bước 1: Tạo rule group type** 35](#_Toc202377935)

[**Bước 2: Add to firewall policy** 37](#_Toc202377936)

[**Bước 3: Kiểm tra firewall** 38](#_Toc202377937)

[**Bước 4: Quan sát Log trong cloudwatch** 40](#_Toc202377938)

# **Giai đoạn 2: Bảo mật VPCs**

Sau khi bạn bảo mật dữ liệu trong Amazon S3, nhóm lãnh đạo của AnyCompany Financial muốn bạn tập trung vào việc bảo mật mạng trong AWS Cloud lưu trữ các ứng dụng quan trọng của công ty. Họ biết về các sự cố bảo mật mạng gần đây và muốn đảm bảo rằng mạng của họ được bảo vệ khỏi các cuộc tấn công và truy cập trái phép. Nhiệm vụ của bạn là bảo mật các đám mây riêng ảo (VPC) cho các máy chủ web của công ty.

Một nhân viên thiếu kinh nghiệm của AnyCompany Financial đã tạo LabVPC và phiên bản WebServer tồn tại trước trong môi trường dự án phòng thí nghiệm của bạn. Nhân viên đó đã mắc một số lỗi và kết quả là mạng không được cấu hình đúng cách. Trong các nhiệm vụ từ 2.1 đến 2.4, bạn sẽ phân tích các cấu hình hiện có và thực hiện các bản cập nhật để sửa cấu hình mạng.

Sơ đồ sau đây hiển thị các tài nguyên đã tồn tại trong môi trường phòng thí nghiệm và bạn sẽ sử dụng cho năm nhiệm vụ đầu tiên trong giai đoạn này:

## **Nhiệm vụ 2.1: Xem lại LabVPC và các tài nguyên liên quan**

### **Bước 1: Mở Amazon VPC Console và kiểm tra VPC**

**Hành động:**

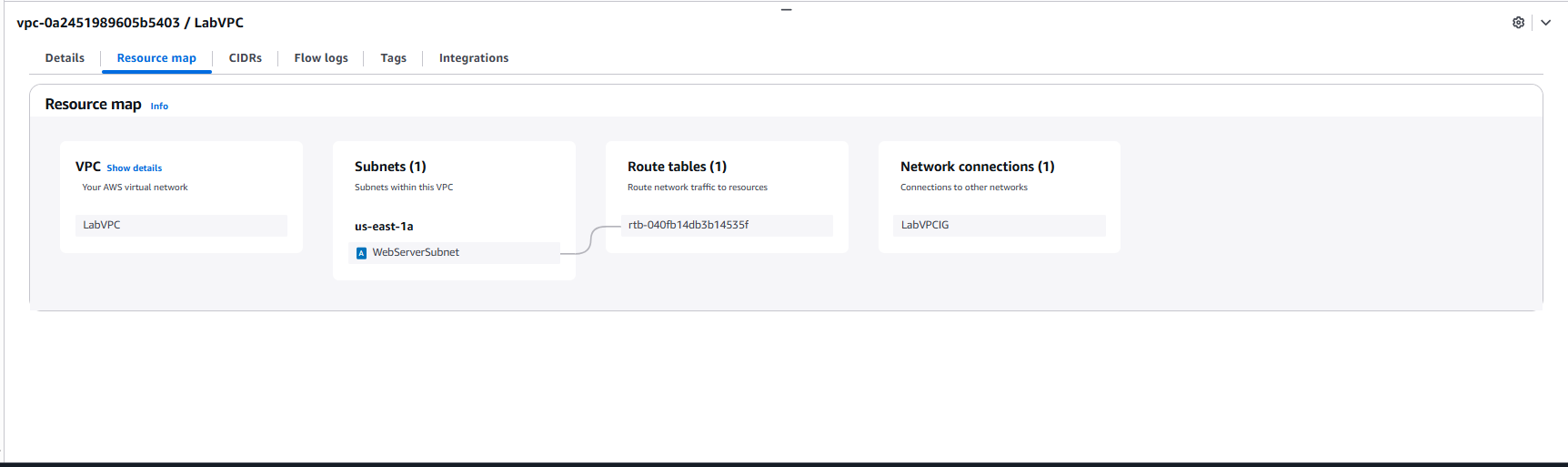
* Vào AWS Management Console > Chọn dịch vụ **VPC**
* Ở góc trên bên phải, **chọn đúng Region: us-east-1 (N. Virginia)**

**Kiểm tra:**

* Tìm VPC có tên là LabVPC
* Kiểm tra sơ đồ tài nguyên (Resource map hoặc VPC Dashboard), bạn sẽ thấy:

🧩 **Các thành phần hiện có**:

* Một subnet tên là **WebServerSubnet**
* Một **Main route table** (được tạo mặc định cùng VPC)
* Một **Internet Gateway** (được gắn vào VPC)



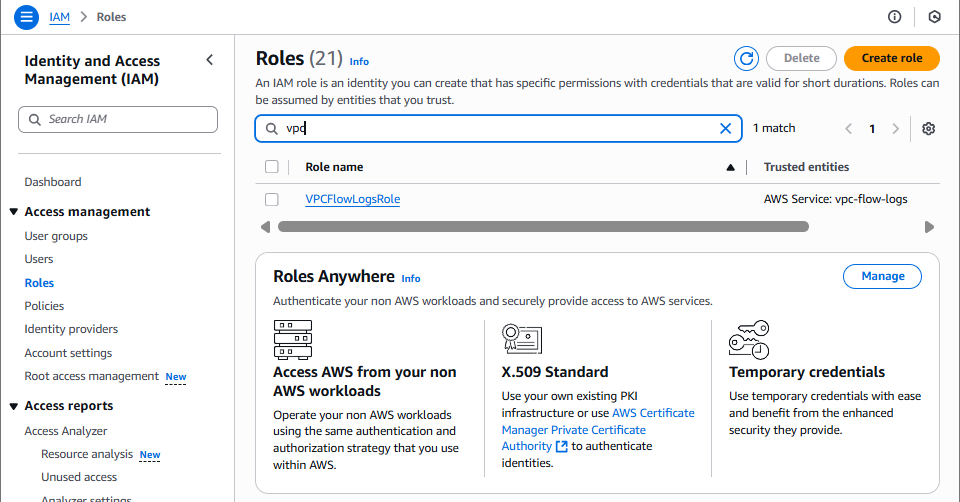
* ⚠️ **Subnet chưa được kết nối với Internet Gateway**  
  ➤ Nghĩa là: Dữ liệu từ WebServer chưa thể ra/vào internet

📌 Ghi chú: Route table của WebServerSubnet hiện **không có route đến IGW**, bạn sẽ xử lý điều này ở Task 2.2.

### **Bước 2: Kiểm tra IAM Role cho VPC Flow Logs**

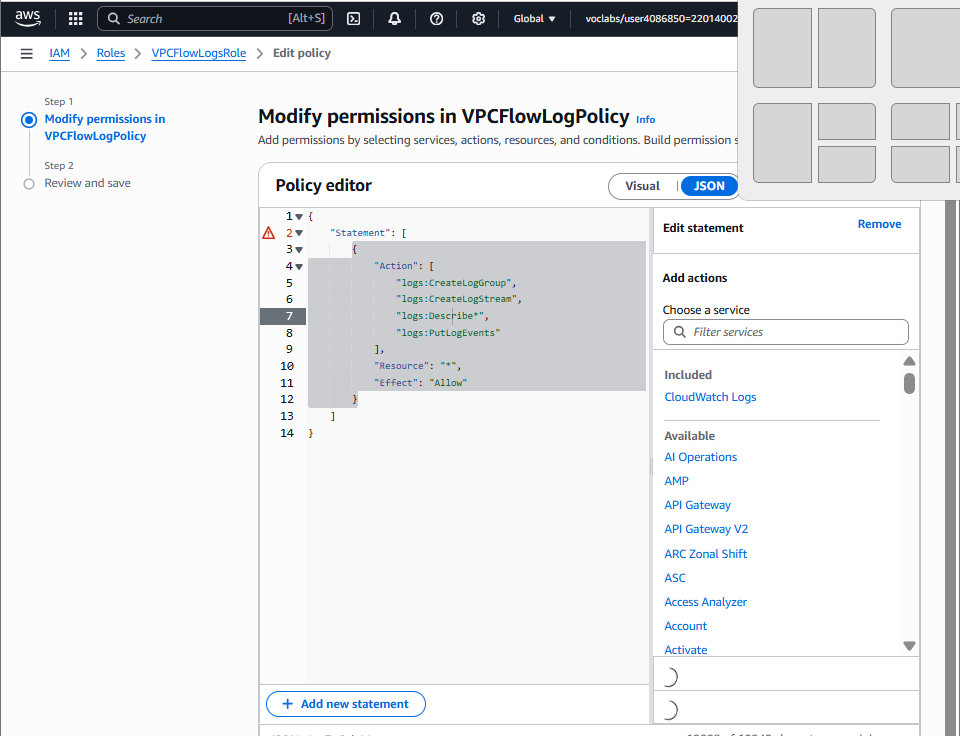
**Hành động:**

* Vào **IAM Console** (AWS Management Console > IAM)
* Tìm role có tên là **VPCFlowLogsRole**



**Kiểm tra nội dung:**

* Mở phần **Permissions** của role
* Bạn sẽ thấy policy cấp quyền cho:
  + Ghi log từ VPC Flow Logs vào **Amazon CloudWatch Logs**



🔍 **Giải thích**:  
Role này giúp dịch vụ **VPC Flow Logs** có thể ghi lại nhật ký hoạt động mạng trong VPC, ví dụ như:

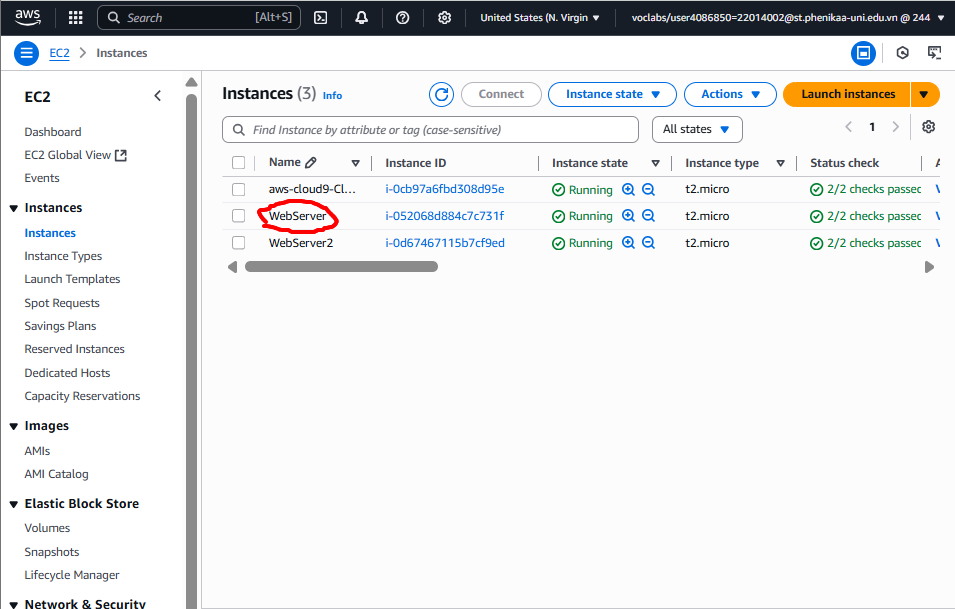
* Ai đó truy cập web server qua HTTP
* Những kết nối bị từ chối

👉 Bạn sẽ sử dụng role này để bật VPC Flow Logs ở task sau.

### **Bước 3: Mở Amazon EC2 Console và kiểm tra WebServer Instance**

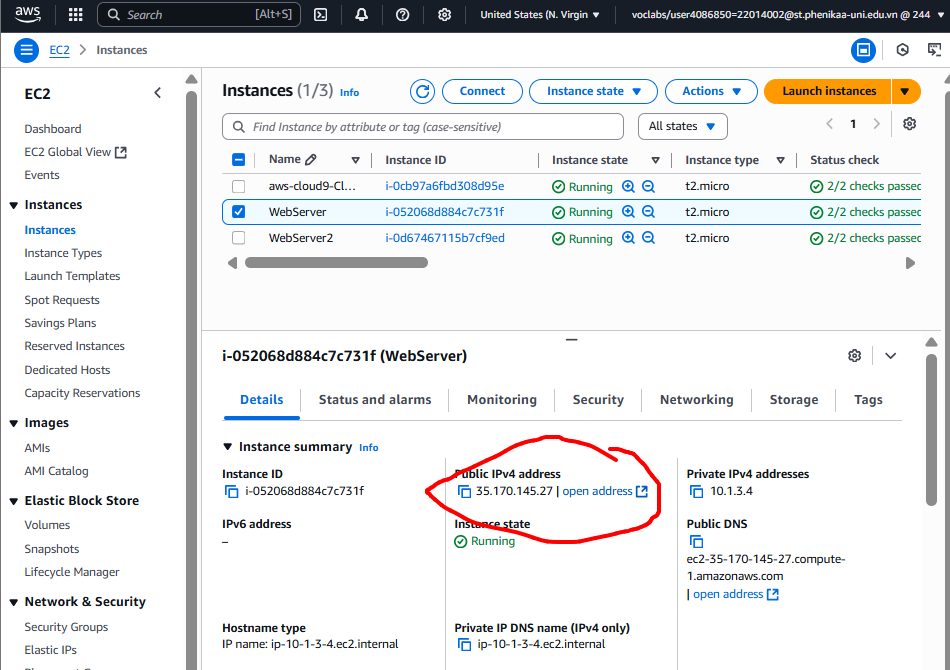
**Hành động:**

* Vào **EC2 Console**
* Chọn **Instances** từ menu bên trái
* Chọn instance tên là **WebServer** hoặc instance đang dùng subnet WebServerSubnet

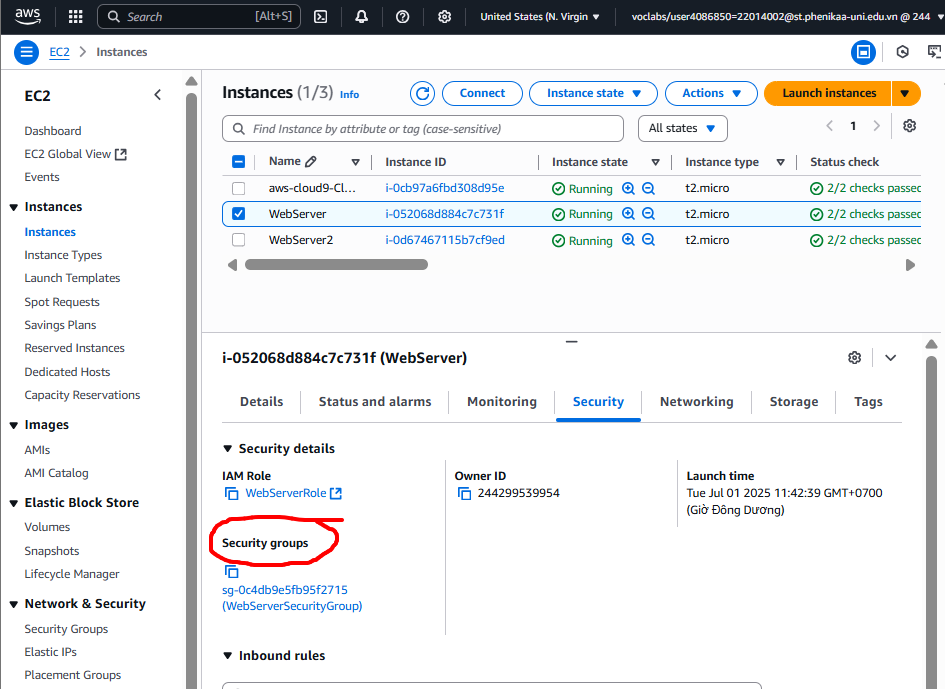


**Kiểm tra các thông tin sau:**

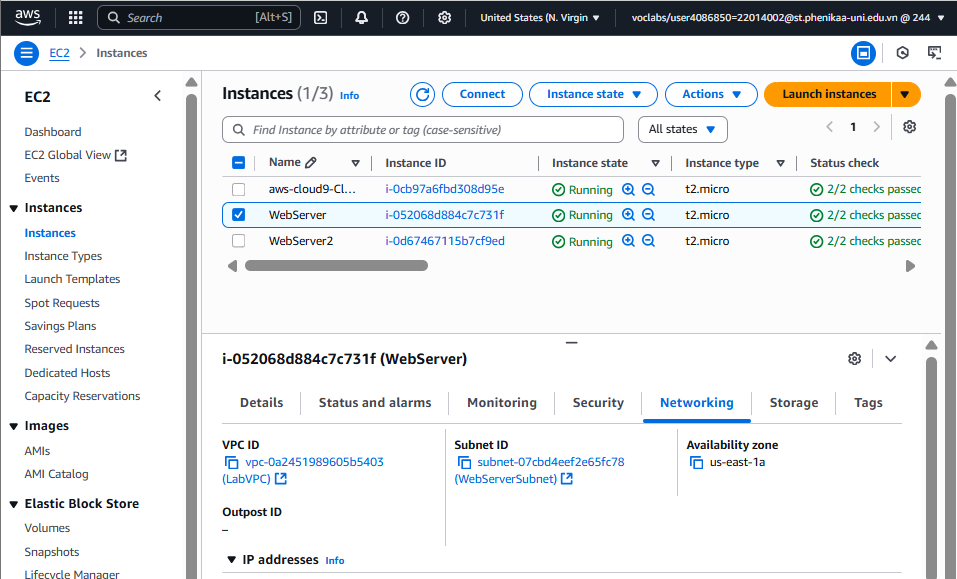
* ✅ Có **Public IPv4 address** → Cho phép truy cập từ internet



* ✅ Được gán **IAM Role** → Cho phép instance sử dụng dịch vụ AWS khác (nếu được cấp quyền)
* ✅ Gắn với **Security Group tên là Webserver Security Group**



* ✅ Đặt trong **subnet WebServerSubnet**, thuộc **LabVPC**



## **Nhiệm vụ 2.2: Tạo một VPC Flow Log cho VPC**

### **Bước 1: Truy cập vào VPC**

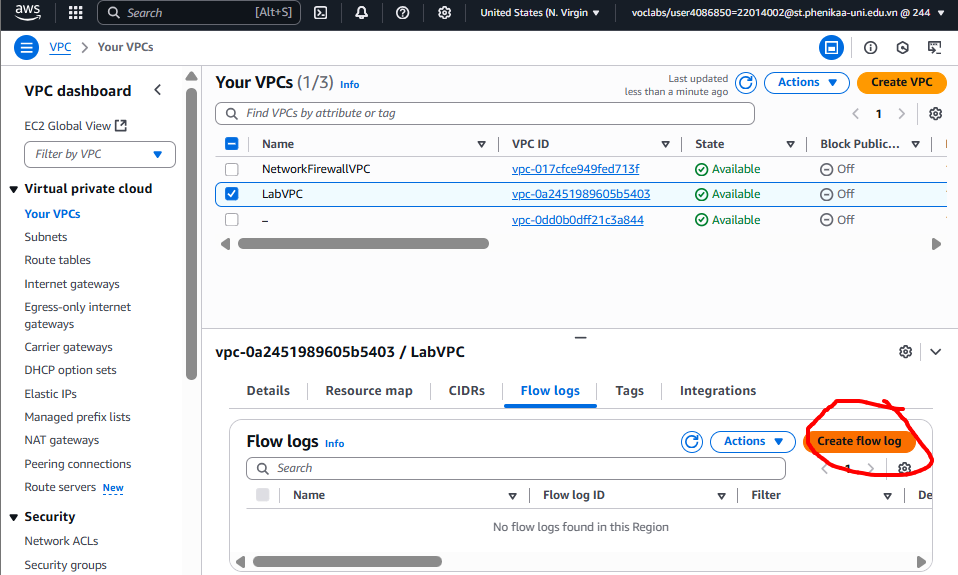
* Vào **AWS Console**.
* Chọn **VPC**.
* Đảm bảo bạn đang ở **Region us-east-1** (xác nhận ở góc trên bên phải).

### **Bước 2: Chọn VPC LabVPC**

* Trong menu bên trái, chọn **Your VPCs**.
* Nhấn chọn VPC có tên LabVPC.

### **Bước 3: Tạo Flow Log**

* Trong phần chi tiết của LabVPC, kéo xuống và chọn tab **Flow Logs**.
* Nhấn **Create flow log**.



### **Bước 4: Cấu hình Flow Log**

* **Name tag**: LabVPCFlowLogs.
* **Filter**: chọn All (để ghi lại tất cả lưu lượng).
* **Maximum aggregation interval**: chọn 1 minute.
* **Destination**: chọn Send to CloudWatch Logs.
* **Destination log group**: nhấn **Create new log group**, nhập LabVPCFlowLogs.
* **IAM Role**: chọn **IAM Role** đã được sử dụng trong task trước (ví dụ: LabFlowLogsRole hoặc tương tự, bạn đã thấy nó trước đó).

### **Bước 5: Tạo Flow Log**

* Nhấn **Create flow log**.

**Sau khi hoàn tất:**

* Bạn sẽ thấy dòng LabVPCFlowLogs trong danh sách Flow Logs của LabVPC.



* Log sẽ bắt đầu ghi trong **CloudWatch Logs** → mục **Log groups** → LabVPCFlowLogs.

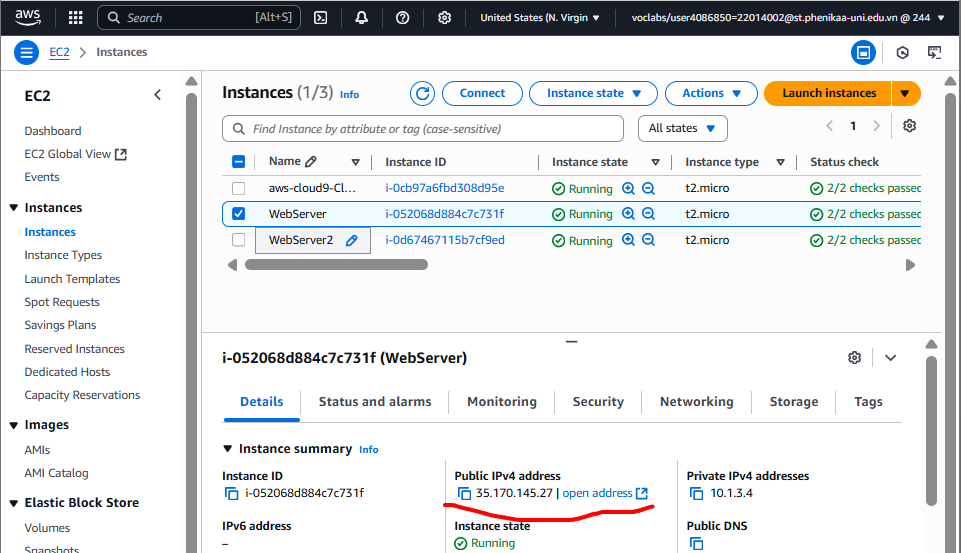
Nếu bạn chưa biết IAM Role nào dùng trong task trước, hãy:

* Vào **IAM** > **Roles**.
* Tìm role được gán quyền AmazonVPCFlowLogs và CloudWatchLogs.
* Chọn đúng role đó khi tạo log.

## **Nhiệm vụ 2.3: Truy cập phiên bản WebServer từ internet và xem lại nhật ký luồng VPC trong CloudWatch**

### **Bước 1: Thử truy cập WebServer bằng trình duyệt**

1. Vào EC2 Console ➝ tìm WebServer instance.
2. Ghi lại Public IPv4 address.



1. Mở trình duyệt web và truy cập:

cpp

Sao chépChỉnh sửa

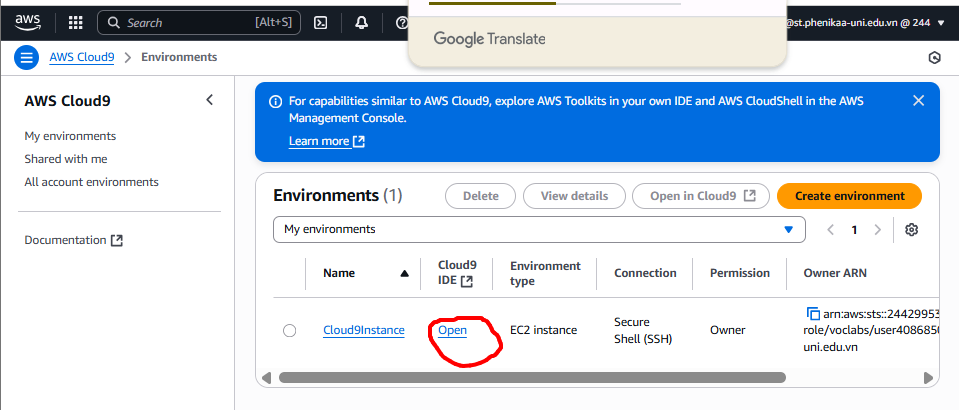
http://<WebServer-public-IP>

➡️ Kết quả: Trang không tải được ❌ — điều này bình thường, vì VPC chưa cấu hình đúng.

### **Bước 2: Kiểm tra truy cập từ Cloud9**

🔹 Truy cập Cloud9 IDE

1. Vào AWS Console ➝ Cloud9 ➝ mở Cloud9Instance.



Chạy lệnh *sudo yum install -y nc* để cài **nc(netcat)**

🔹 Chạy lệnh nc kiểm tra port 80

*nc -vz <WebServer-public-IP> 80*

➡️ Sau một lúc: Kết nối timeout hoặc failed.



Nhấn Ctrl+C nếu muốn dừng sớm.

🔹 Chạy lệnh nc kiểm tra port 22 (SSH)

nc -vz <WebServer-public-IP> 22

➡️ Tương tự: Kết nối thất bại.



### **Bước 3: Xem lại VPC Flow Logs trên CloudWatch**

🔹 Đi tới CloudWatch Logs

1. Vào CloudWatch Console ➝ Logs ➝ tìm log group:

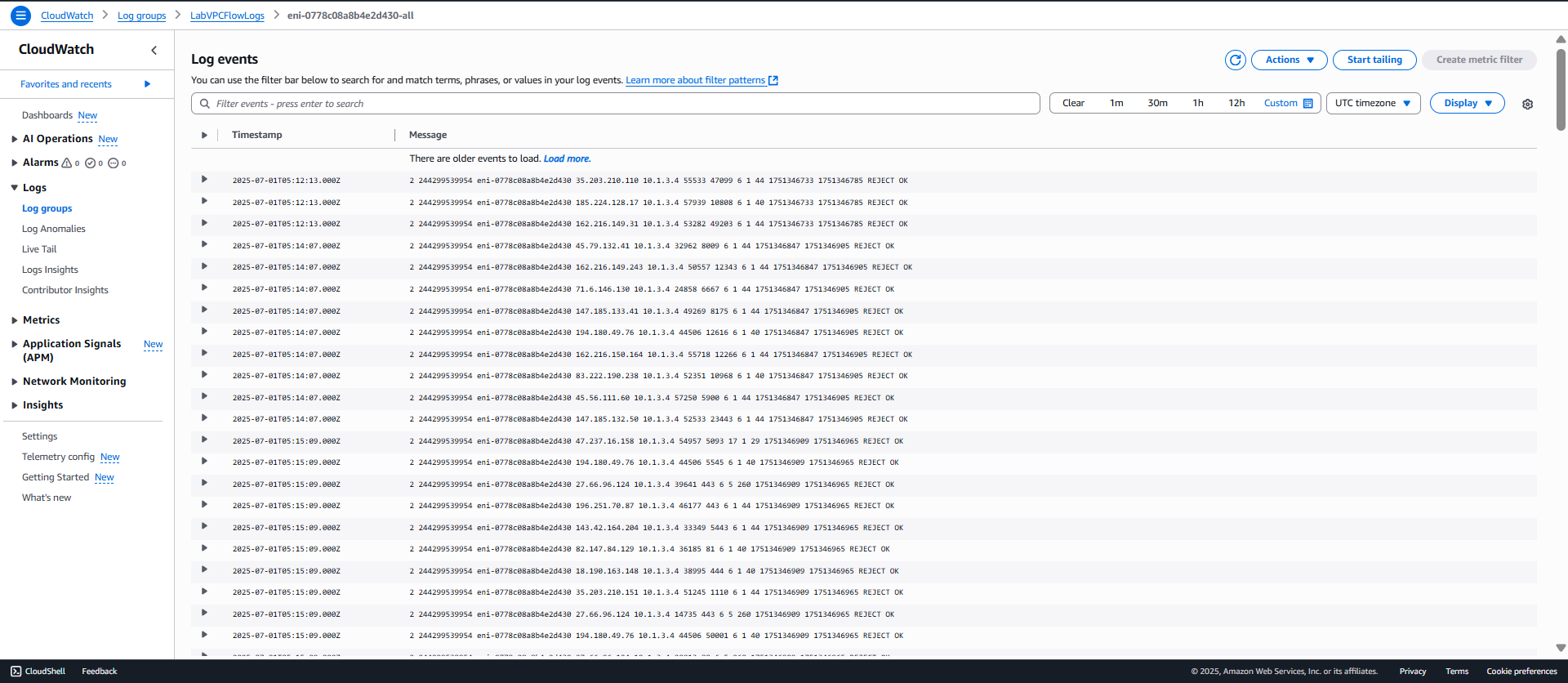


LabVPCFlowLogs

1. Mở log stream gần nhất.

🔹 Kiểm tra các bản ghi log

* Trong cột Message, bạn sẽ thấy các dòng có REJECT.
* Chúng biểu thị các kết nối bị từ chối (inbound traffic đến port 80, 22).

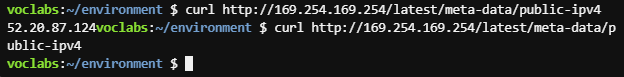


### **Bước 4: Lọc log theo IP của Cloud9**

🔹 Lấy Public IP của Cloud9

Trong terminal của Cloud9, chạy:

*curl http://169.254.169.254/latest/meta-data/public-ipv4*



🔹 Lọc trong CloudWatch

Chọn **Logs** từ thanh điều hướng bên trái.

Tìm log group có tên: **LabVPCFlowLogs**

Nhấn vào log group này để xem danh sách các Log streams.

Chọn Log stream mới nhất (có timestamp gần thời gian bạn thực hiện lệnh nc).

🔹 Tìm kiếm bằng địa chỉ IP **52.20.87.12**

Trong trang hiển thị log stream, tìm hộp "Search log stream" hoặc "Filter events".

Dán địa chỉ IP Cloud9 của bạn vào: **52.20.87.12**

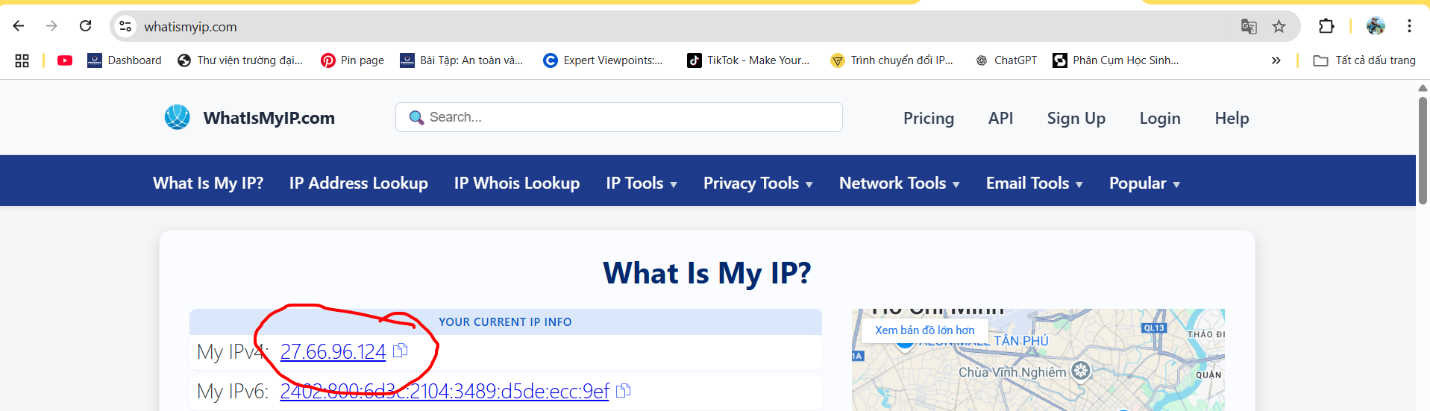
🔹 **Giải thích chi tiết dòng log**



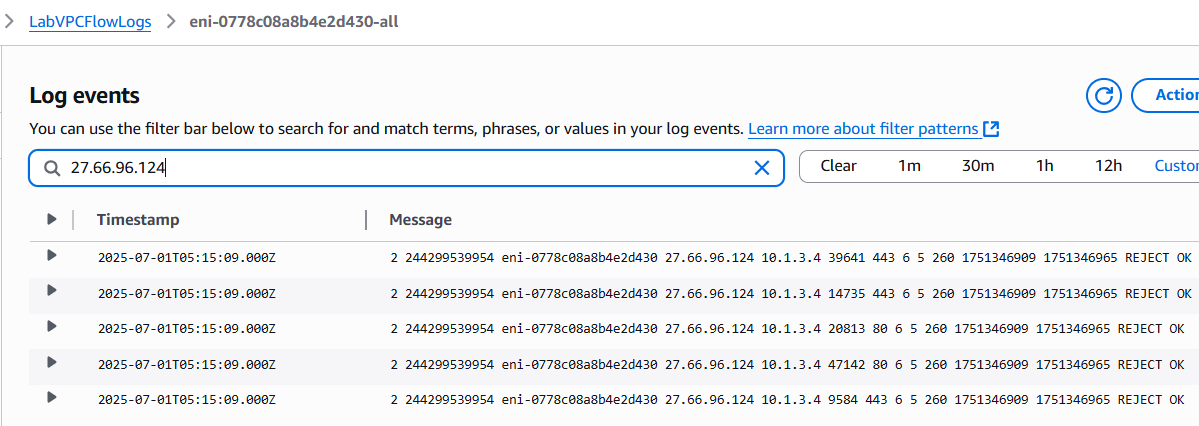
| **Trường** | **Giá trị** | **Ý nghĩa** |
| --- | --- | --- |
| account-id | 244299539954 | ID của tài khoản AWS đang dùng |
| interface-id | eni-0778c08a8b4e2d430 | Elastic Network Interface của WebServer |
| srcaddr | 52.20.87.124 | IP nguồn – đây là Cloud9Instance của bạn |
| dstaddr | 10.1.3.4 | IP đích – đây là Private IP của WebServer |
| srcport | 57558 | Port tạm thời từ Cloud9 |
| dstport | 80 | Cổng HTTP – bạn đã kiểm tra bằng nc |
| protocol | 6 | Giao thức TCP (mã số 6 theo IANA) |
| packets | 4 | Số lượng gói tin đã gửi |
| bytes | 240 | Tổng số byte dữ liệu |
| start / end time | 1751347391 ➝ 1751347446 | Thời gian bắt đầu và kết thúc log (đơn vị: epoch time) |
| action | REJECT | ❌ Kết nối bị từ chối (khớp với yêu cầu bài lab) |
| log-status | OK | Ghi log thành công |

### **Bước 5: Lọc log theo IP máy tính của bạn**

1. Vào trang: <https://www.whatismyip.com> ➝ Lấy địa chỉ IP.



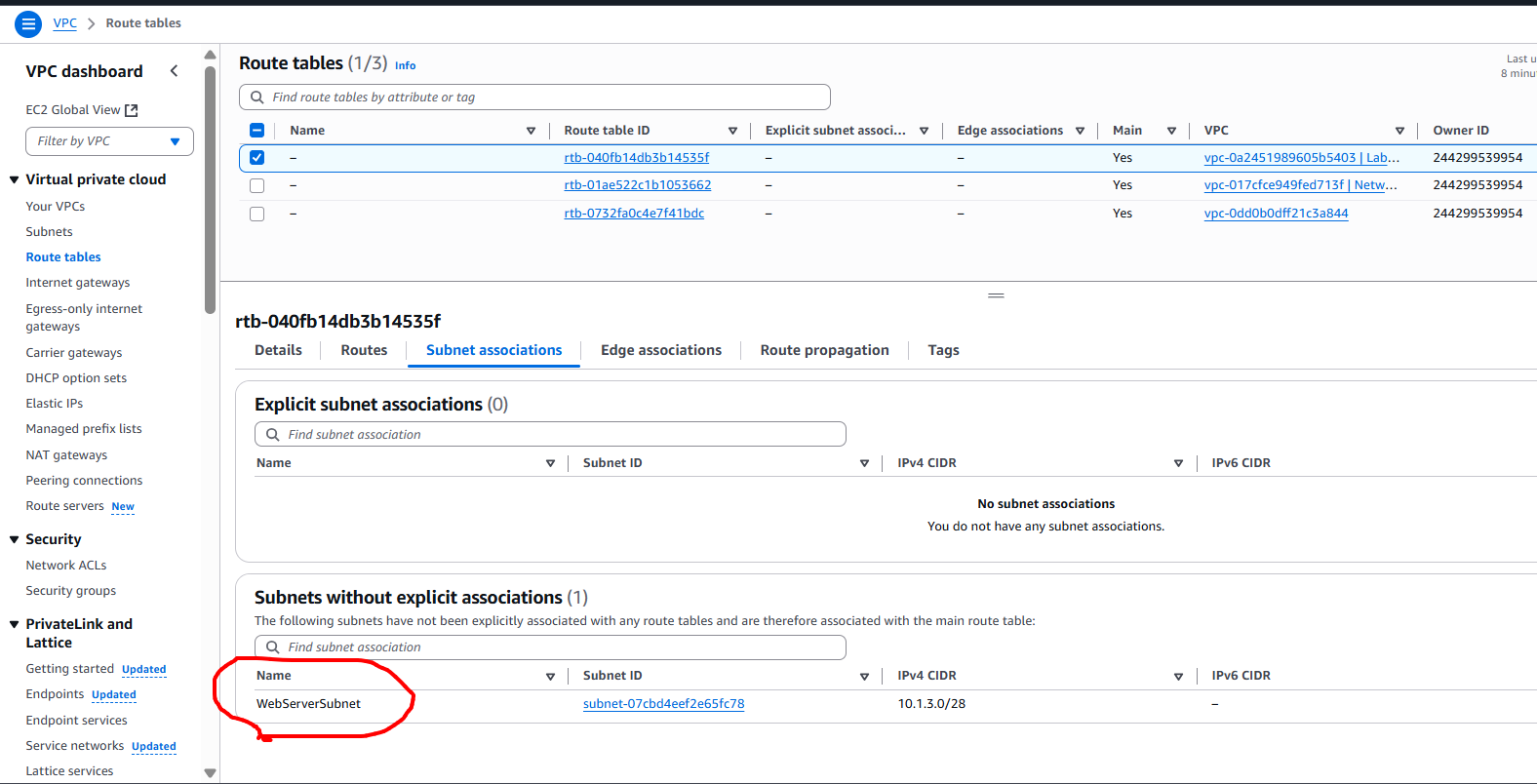
1. Lọc tương tự trong CloudWatch Log Stream theo IP đó.



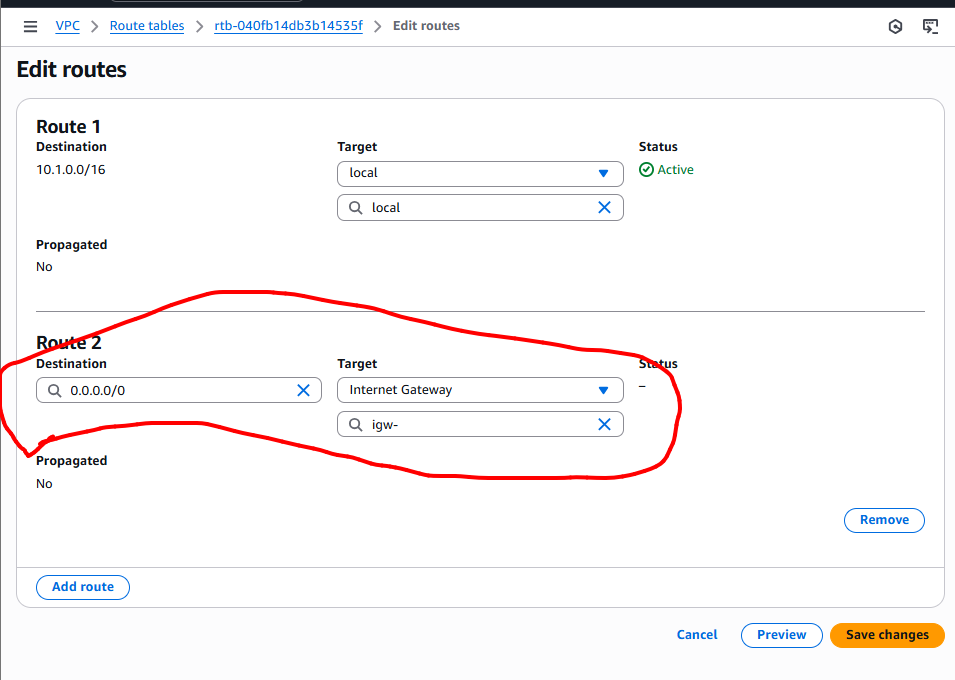
## **Nhiệm vụ 2.4: Cấu hình bảng định tuyến và cài đặt nhóm bảo mật**

### **Bước 1: Cấu hình Route Table**

1. Mở **Amazon VPC console**.
2. Tìm đến Route Table gắn với **WebServerSubnet**.

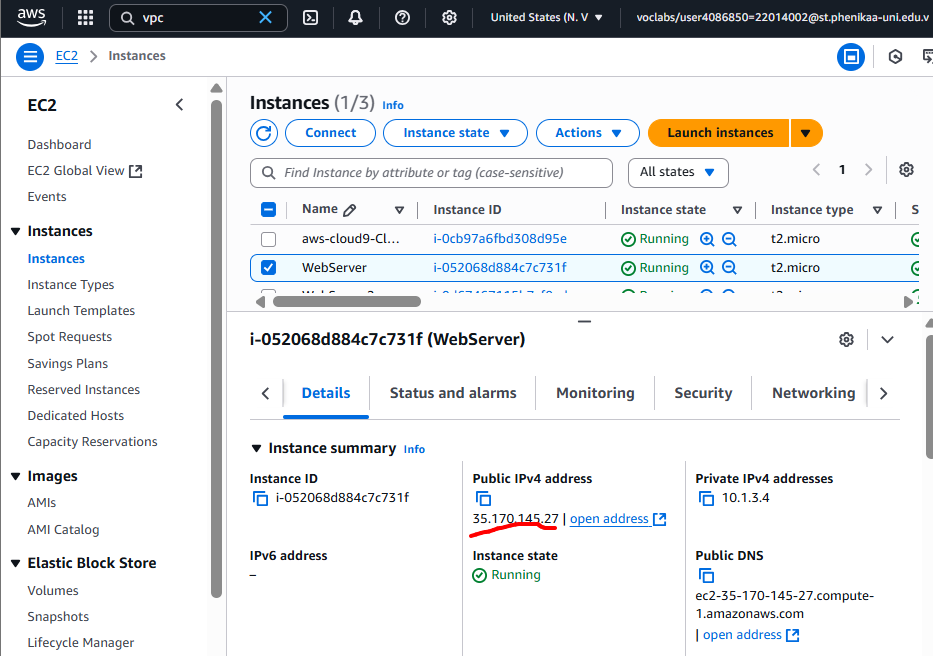


1. Thêm **route mới**:
   * **Destination**: 0.0.0.0/0
   * **Target**: Chọn **Internet Gateway (LabVPCIG)** đã được tạo sẵn.



📌 Mục đích: Cho phép tất cả lưu lượng đi ra ngoài Internet.

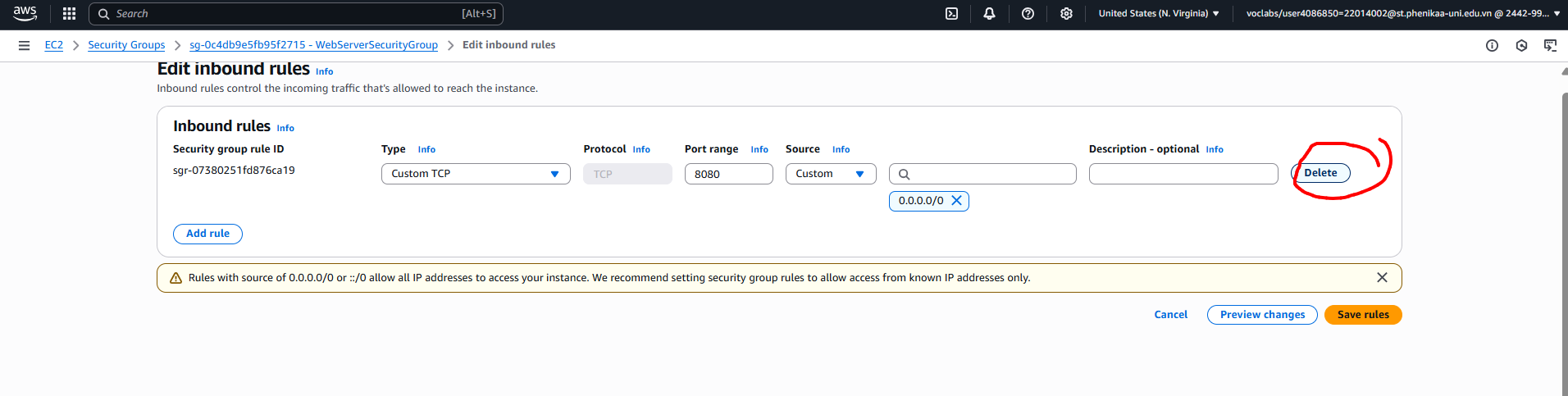
### **Bước 2: Kiểm tra HTTP từ trình duyệt**

****

* Truy cập: http://<WebServer-public-IP>  
  → Nếu bị **timeout hoặc fail**, **KHÔNG SAO** – vì Security Group **chưa cho phép** lưu lượng đến port 80.

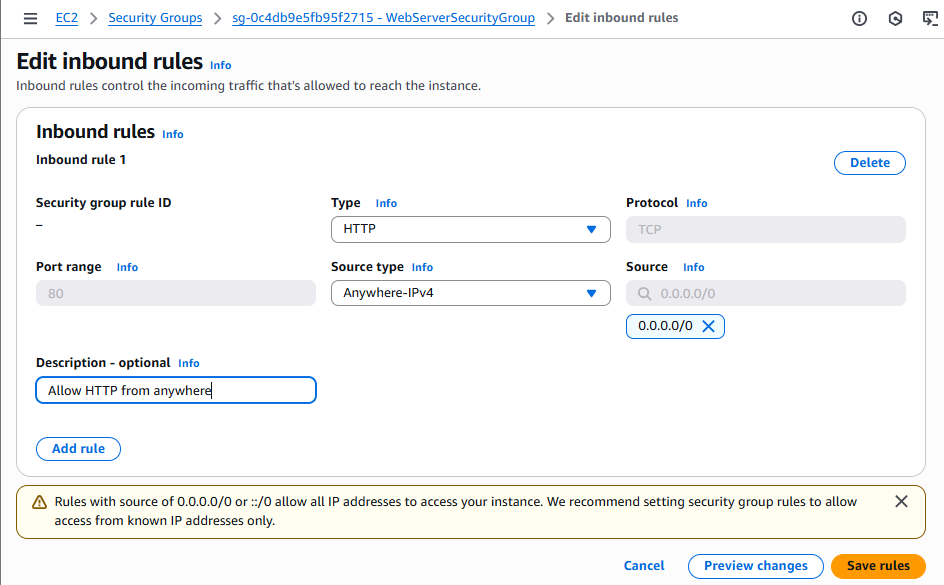
### **Bước 3: Chỉnh sửa Security Group**

1. Mở **EC2 Console** → Chọn **Security Groups** liên kết với WebServer.
2. **Xóa các inbound rule** hiện tại **trừ** khi là port 22 hoặc 80.



1. **Thêm 3 rule mới**:

**🟢 Rule 1:**

****

**🟢 Rule 2: Cho phép SSH từ Cloud9**

* Mở terminal trong AWS Cloud9, chạy:

*curl https://checkip.amazonaws.com*

→ Lấy IP công khai Cloud9



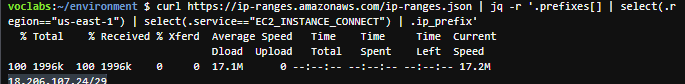
* Thêm rule:
  + **Type**: SSH
  + **Port**: 22
  + **Source**: 52.20.87.124/32  
    → Chỉ cho phép SSH từ **một địa chỉ IP** cụ thể.
  + **Description** | Allow SSH from Cloud9

**🟢 Rule 3: Cho phép SSH từ EC2 Instance Connect**

* Chạy trong Cloud9:

*sudo yum install -y jq*

*curl https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] | select(.region=="us-east-1") | select(.service=="EC2\_INSTANCE\_CONNECT") | .ip\_prefix'*

******

→ Copy dải IP trả về (18.206.107.24/29)

* Thêm rule:
  + **Type**: SSH
  + **Port**: 22
  + **Source**: dải IP đó  
    → Đảm bảo bạn có thể sử dụng **EC2 Instance Connect** để SSH vào máy chủ.
  + **Description** | Allow EC2 Instance Connect

### **Bước 4: Kiểm tra kết nối**

**✅ Kiểm tra SSH (port 22)**

Trong Cloud9:

*nc -zv <WebServer-public-IP> 22*

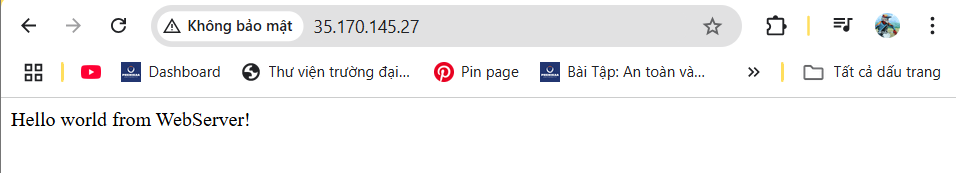
*nc -zv 35.170.145.27 22*

→ Nếu thấy succeeded, kết nối thành công.



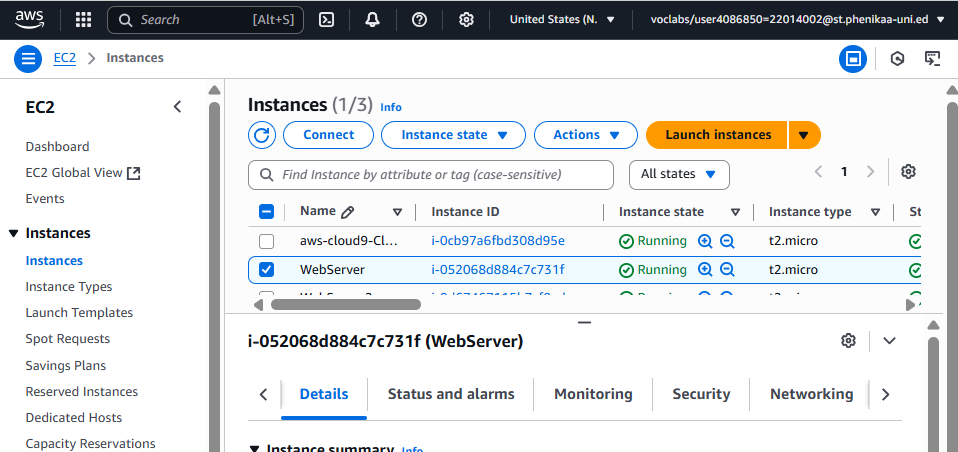
**✅ Kiểm tra HTTP (port 80)**

* Truy cập http://<WebServer-public-IP> trong trình duyệt  
  → Nếu thấy: **“Hello world from WebServer!”**, đã thành công!



**✅ SSH bằng EC2 Instance Connect**

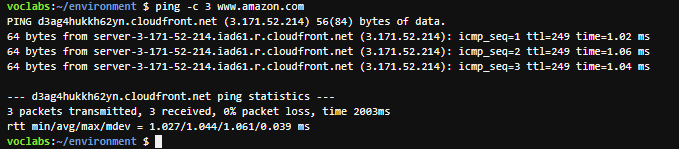
1. EC2 Console → Chọn WebServer → Chọn "Connect" → EC2 Instance Connect



1. Sau khi kết nối:

ping -c 3 www.amazon.com

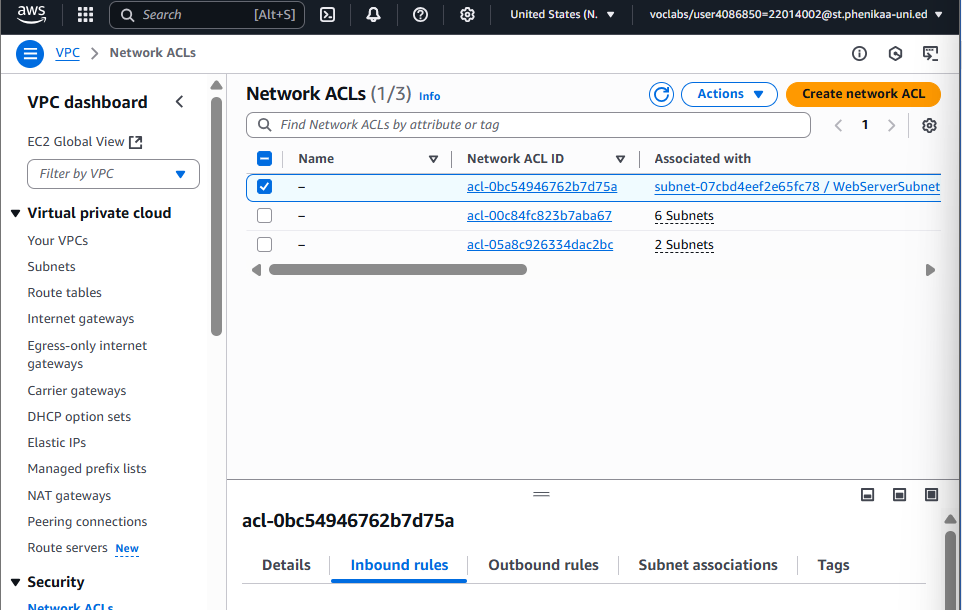
→ Nếu thấy phản hồi 64 bytes, instance đã truy cập được Internet.



## **Nhiệm vụ 2.5: Bảo mật WebServerSubnet bằng ACL mạng**

### **Bước 1: Điều hướng đến Network ACL**

* Mở **Amazon VPC Console**.
* Trong thanh điều hướng, chọn **Network ACLs**.
* Tìm **Network ACL** gắn với **WebServerSubnet** trong **LabVPC**.
* Nhấp vào để vào trang chi tiết của nó.



### **Bước 2: Chỉnh sửa Rule 100 để TỪ CHỐI port 22**

* Tìm **Inbound Rule số 100** (mặc định là ALLOW all traffic).
* Nhấn **Edit inbound rules**.
* Chỉnh sửa rule số **100**:
  + **Type**: All Traffic
  + **Protocol**: All
  + **Port Range**: ALL
  + **Source**: 0.0.0.0/0
  + **Action**: ❌ **DENY**
* **Save changes**.

### **Bước 3: Kiểm tra bằng nc (netcat):**

* Dùng lệnh netcat để kiểm tra cổng 22:

*nc -zv <WebServer-public-IP> 22*

*nc -zv 35.170.145.27 22*

* ❌ Kết nối sẽ **thất bại hoặc bị timeout** (chặn bởi ACL).
* Điều này xác nhận rằng: **Network ACL có thể chặn truy cập mạng dù Security Group vẫn cho phép**.

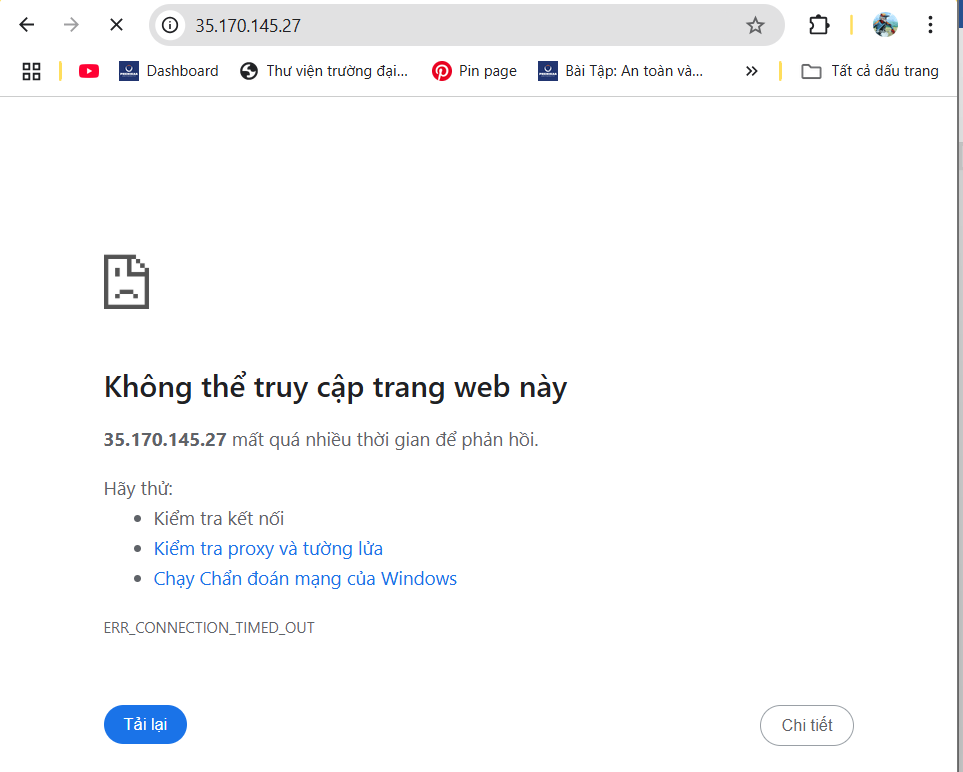


### **Bước 4: Kiểm tra HTTP trên trình duyệt:**

* Truy cập địa chỉ:

http://<WebServer-public-IP>

* ❌ Trang sẽ không tải được — bị chặn vì Rule 100 hiện đang DENY mọi traffic.



### **Bước 5: Cho phép lại port 22 (SSH) trong rule 100**

* Chỉnh sửa lại **Rule 100**:
  + **Type**: SSH
  + **Protocol**: TCP (6)
  + **Port Range**: 22
  + **Source**: 0.0.0.0/0
  + **Action**: ✅ **ALLOW**
* **Save changes**.

### **Bước 6: Kiểm tra lại SSH bằng netcat**

nc -zv <WebServer-public-IP> 22

* ✅ Lần này kết nối **thành công** → ACL đã cho phép SSH.

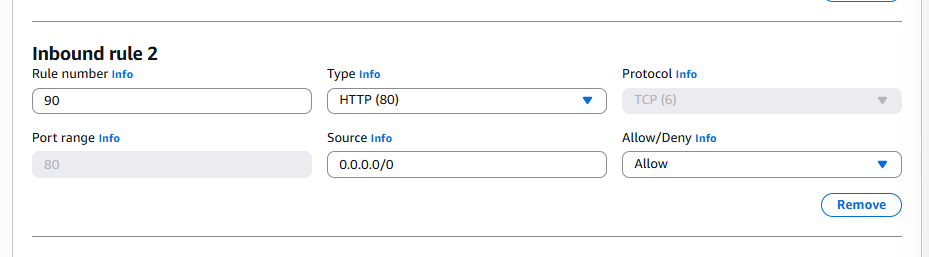


### **Bước 7: Thêm Rule 90 để cho phép HTTP traffic**

* Nhấn **Edit inbound rules**.
* Thêm một **rule mới**:
  + **Rule number**: 90 *(ưu tiên cao hơn số 100)*
  + **Type**: HTTP
  + **Protocol**: TCP (6)
  + **Port Range**: 80
  + **Source**: 0.0.0.0/0
  + **Action**: ✅ **ALLOW**

⚠️ **Quan trọng:** ACL được xử lý theo thứ tự từ số nhỏ đến lớn → Rule 90 sẽ được xử lý trước rule 100.

* **Save changes**.



### **Bước 8: Truy cập lại website**

* Mở trình duyệt và vào:

http://<WebServer-public-IP>

http://35.170.145.27/

* Bạn sẽ thấy nội dung:

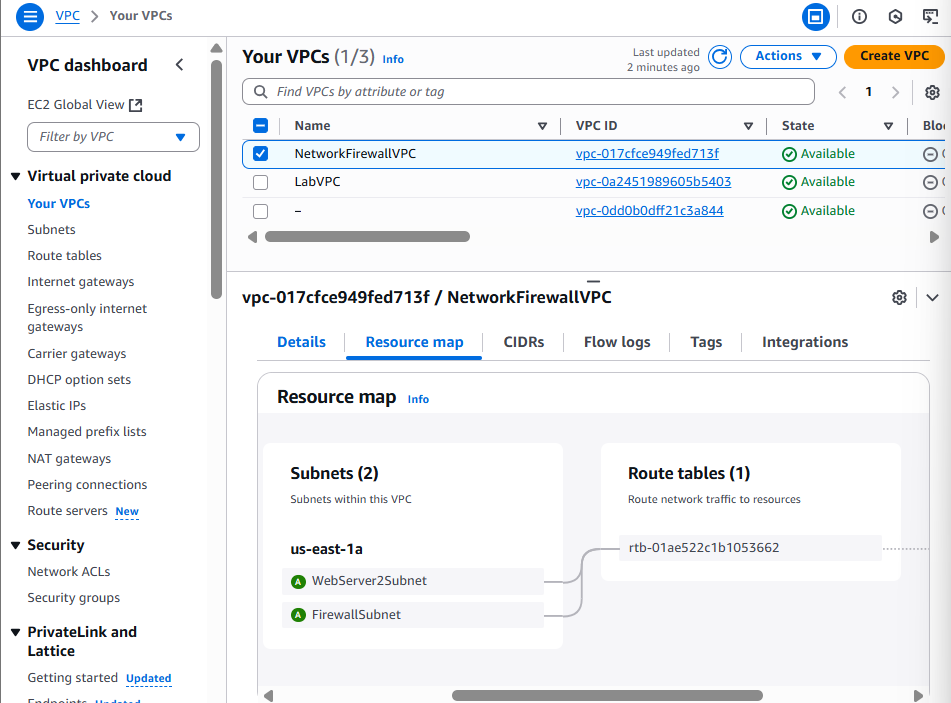
***Hello world from WebServer!***

## **Nhiệm vụ 2.6: Đánh giá NetworkFirewallVPC và các tài nguyên liên quan**

### **Bước 1: Kiểm tra cấu trúc NetworkFirewallVPC**

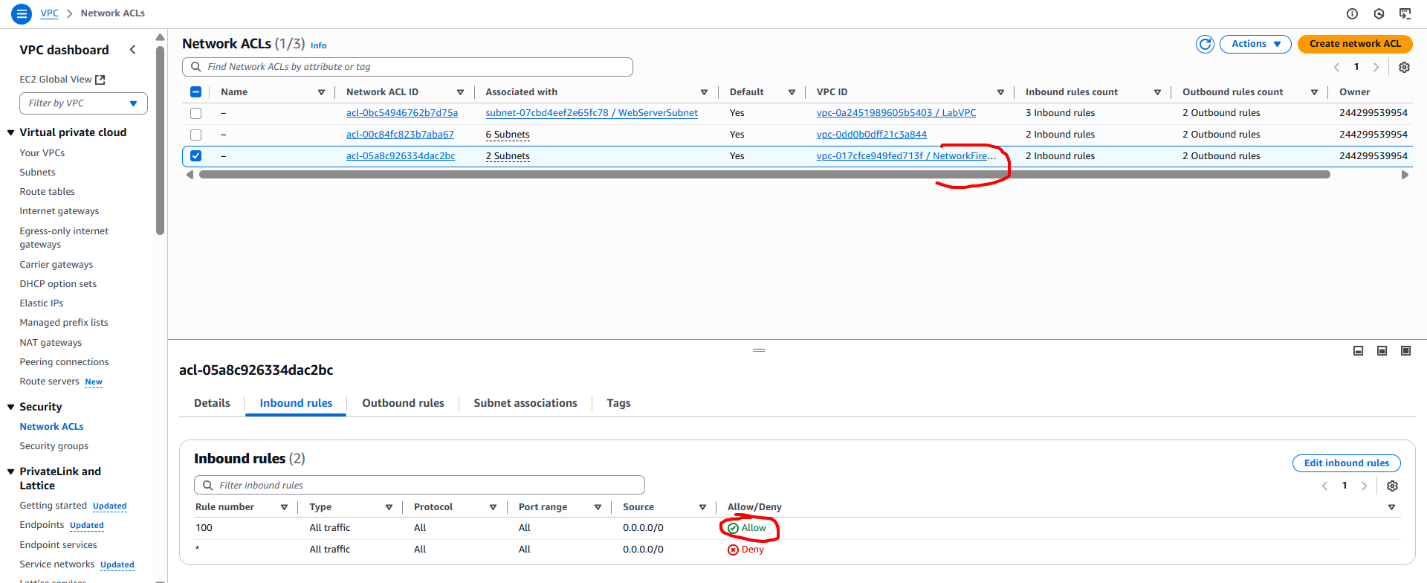
Trên **AWS VPC Console**, chọn VPC tên NetworkFirewallVPC, chuyển sang tab **Resource map**, bạn sẽ thấy:

| **Thành phần** | **Mô tả** |
| --- | --- |
| WebServer2Subnet | Chứa EC2 tên WebServer2 |
| FirewallSubnet | Chứa Firewall Endpoint (bạn sẽ tạo ở Task 2.7) |
| Internet Gateway | Đã gắn (NetworkFirewallIG) và route table mặc định đã cấu hình |



### **Bước 2: Kiểm tra cấu hình Network ACL**

* Vào VPC Console → **Network ACLs** → Chọn ACL gắn với WebServer2Subnet.
* Kiểm tra các rule **inbound**:
  + Rule 100: ALLOW ALL (0.0.0.0/0, all traffic).

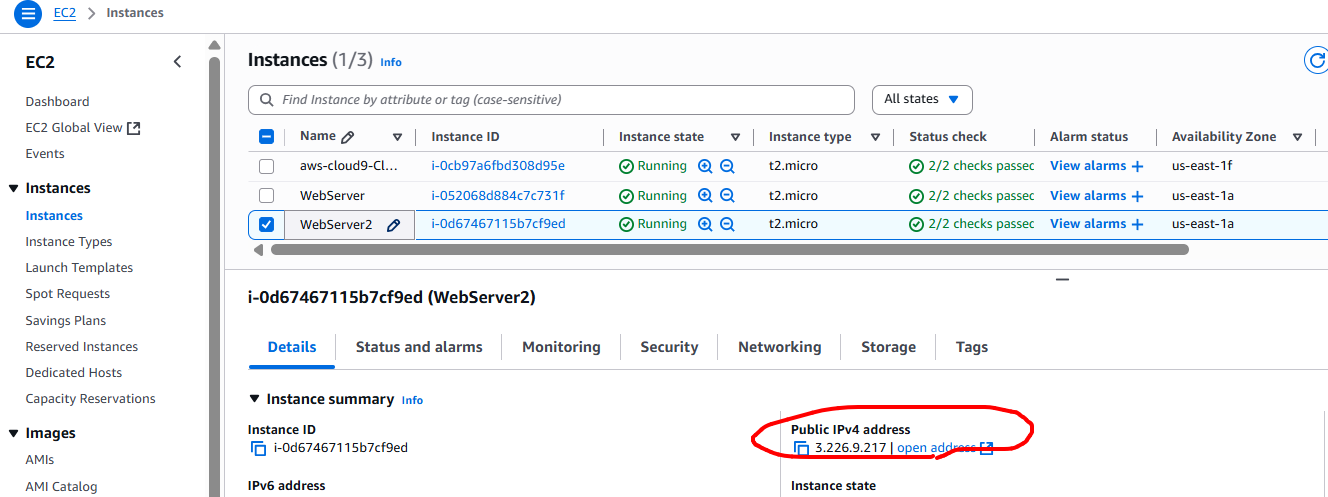


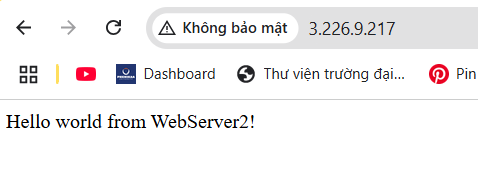
* + Tạm thời cho phép, nhưng bạn sẽ **cấu hình tường lửa để kiểm soát chặt hơn** ở các bước sau.

### **Bước 3: Xác minh truy cập WebServer2**

**🔹 A. Truy cập HTTP qua trình duyệt:**

* Lấy địa chỉ **Public IPv4** của WebServer2 trong **EC2 Console**.
* Truy cập:  
  http://<Public-IP> → hiển thị: **Hello world from WebServer2!**





**🔹 B. Truy cập SSH qua lệnh nc (netcat):**

Trong **Cloud9 Terminal**, gõ:

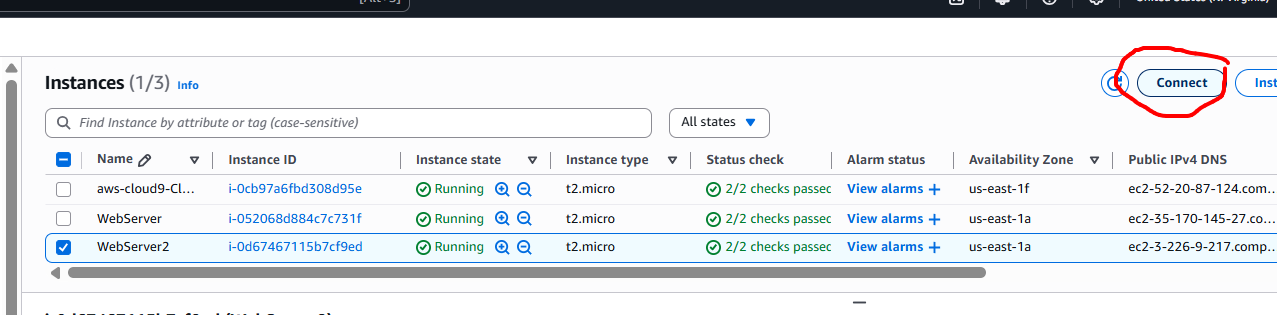
*nc -zv <Public-IP> 22*

*nc -zv 3.226.9.217 22*

→ Kết nối thành công.

**🔹 C. Khởi chạy dịch vụ HTTP trên port 8080:**

* Kết nối EC2 Instance qua **EC2 Instance Connect**.

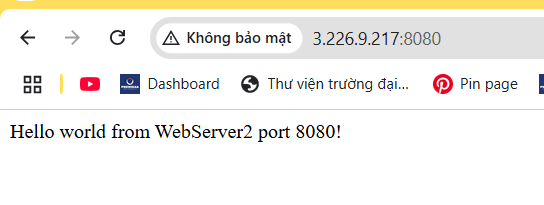


* Gõ lệnh:

python3 -m http.server 8080 &

* Truy cập trình duyệt:  
  http://<Public-IP>:8080 → hiển thị: **Hello world from WebServer2 port 8080!**

http://3.226.9.217:8080/



### **Bước 4: Chuẩn bị sơ đồ mạng (Network Firewall Diagram) ko cần làm**

Bạn sẽ điền các chi tiết vào 4 bảng **Routing Tables** và **CIDR block của các subnet**, gồm:

**🟦 1. WebServer2Subnet CIDR block:**

**🟦 2. FirewallSubnet CIDR block:**

**📘 3. Route table: WebServer2Subnet RT**

| **Destination** | **Target** |
| --- | --- |
| 0.0.0.0/0 | Firewall Endpoint (ENI) |

→ Tất cả outbound traffic đi qua Firewall.

**📘 4. Route table: FirewallSubnet RT**

| **Destination** | **Target** |
| --- | --- |
| 0.0.0.0/0 | Internet Gateway (NetworkFirewallIG) |

→ Firewall xử lý xong thì gửi ra internet.

**📘 5. Route table: Internet-bound RT (for return traffic)**

| **Destination** | **Target** |
| --- | --- |
| 10.0.1.0/24 | Firewall Endpoint |

→ Trả lại traffic về WebServer2Subnet.

### **Bước 5: Cách routing hoạt động (giải thích) Ko cần làm**

**➤ Traffic từ internet đến WebServer2:**

1. Truy cập HTTP/SSH đến WebServer2 public IP.
2. Route từ internet qua **Internet Gateway → Firewall Endpoint**.
3. Tường lửa kiểm tra, nếu rule cho phép → forward đến WebServer2Subnet.
4. WebServer2 nhận traffic.

**➤ Traffic từ WebServer2 ra internet:**

1. WebServer2 gửi traffic → đi qua **Firewall Endpoint** (route table).
2. Firewall xử lý và **forward đến Internet Gateway**.
3. Internet trả lại phản hồi → quay về Firewall → WebServer2.

## **Nhiệm vụ 2.7: Tạo tường lửa mạng**

### **Bước 1: Truy cập Amazon VPC Console**

* Truy cập <https://console.aws.amazon.com/vpc>
* Đảm bảo bạn đang ở **Region: us-east-1**

### **Bước 2: Tạo Network Firewall**

1. Trong menu bên trái, chọn **Network Firewall** > **Firewalls**.
2. Nhấn **Create firewall**.

### **Bước 3: Nhập thông tin firewall**

* **Firewall name**: NetworkFirewall
* **VPC**: Chọn NetworkFirewallVPC
* **Availability Zone**: us-east-1a
* **Subnet**: Chọn FirewallSubnet thuộc us-east-1a
* **IP address type**: Chọn IPv4

### **Bước 4: Configure advanced settings**

* **Delete protection**: Bỏ chọn **Enable**
* **Subnet change protection:** Bỏ chọn **Enable**

### **Bước 5: Associate firewall policy**

* New firewall policy name : FirewallPolicy
* Description – optional : Bỏ trống
* Phần còn lại giữ nguyên

### **Bước 6: Hoàn tất**

* Nhấn **Create firewall**

### **Bước 7: Kiểm tra trạng thái**

* Quay lại trang **Firewalls**
* Kiểm tra cột **Status**, đợi đến khi hiện trạng thái **Ready**
  + *Mất khoảng 3 phút*
  + Bạn có thể nhấn **Refresh** định kỳ để cập nhật trạng thái nhanh hơn

## **Nhiệm vụ 2.8: Tạo bảng lộ trình**

### **Bước 1: Tạo bảng định tuyến cho Internet Gateway**

**Tên: IGW-Ingress-Route-Table**

1. Vào **Amazon VPC Console**.
2. Chọn **Route Tables** → Nhấn **Create route table**.
   * **Name tag**: IGW-Ingress-Route-Table
   * **VPC**: Chọn NetworkFirewallVPC
   * Nhấn **Create**

**➕ Thêm Route:**

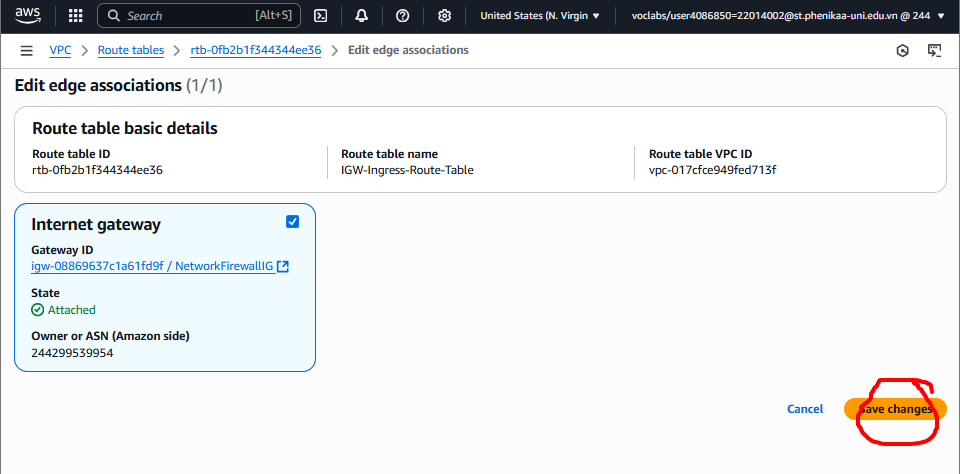
1. Chọn IGW-Ingress-Route-Table → Chọn tab **Routes** → **Edit routes**
   * **Destination**: CIDR block của **WebServer2Subnet** (**IPv4 CIDR**

10.1.3.0/28)

* + **Target**: Chọn **Gateway Load Balancer Endpoint** duy nhất đang có.
  + Nhấn **Save routes**

**🔗 Tạo liên kết Edge (Edge Association):**

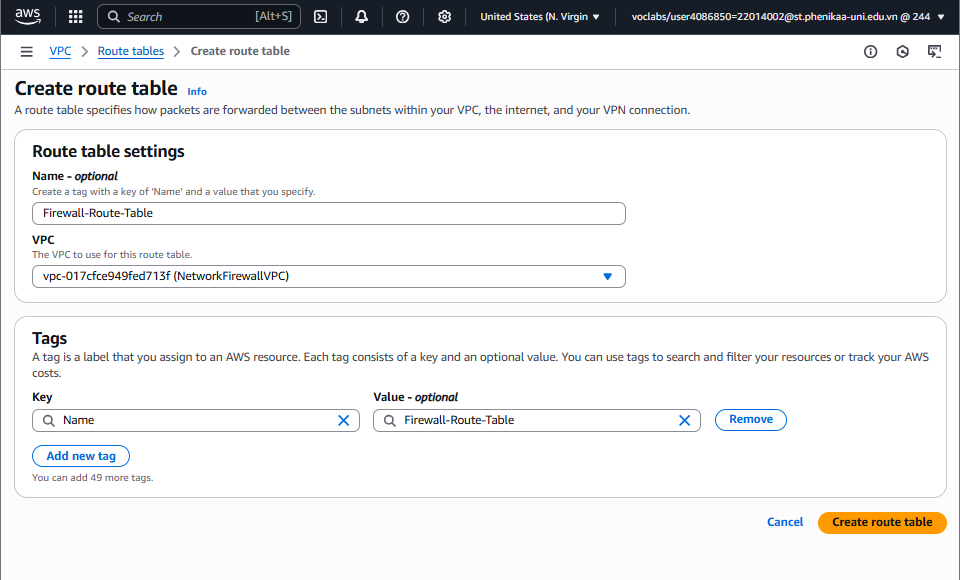
1. Vào tab **Edge associations** → Nhấn **edit asociations**



### **Bước 2: Tạo bảng định tuyến cho FirewallSubnet**

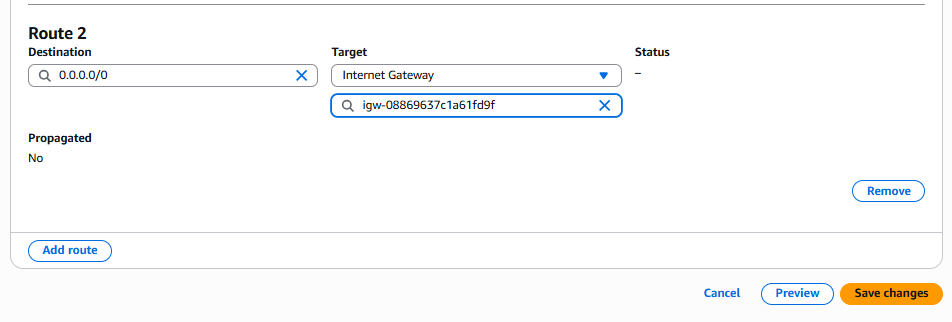
**📌 Tên: Firewall-Route-Table**

1. Quay lại **Route Tables** → Nhấn **Create route table**
   * **Name tag**: Firewall-Route-Table
   * **VPC**: Chọn NetworkFirewallVPC
   * Nhấn **Create**



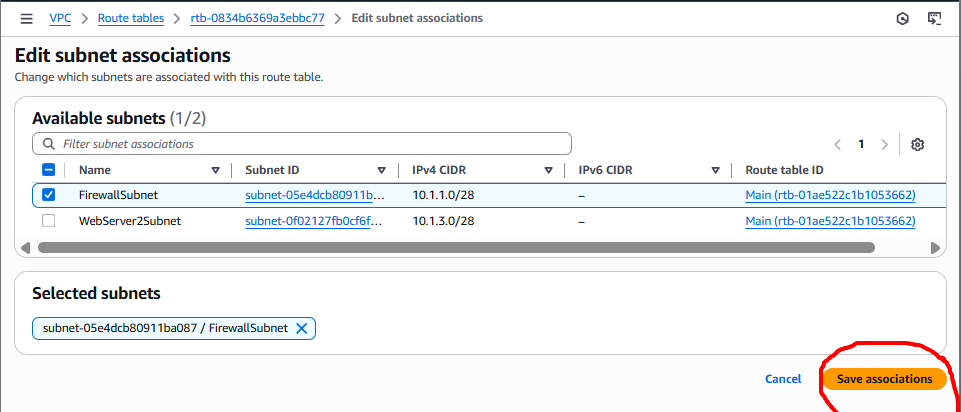
**➕ Thêm Route:**

1. Chọn bảng Firewall-Route-Table → Tab **Routes** → **Edit routes**
   * **Destination**: 0.0.0.0/0 (tức là tất cả lưu lượng internet)
   * **Target**: chọn **NetworkFirewallIG** (Internet Gateway)
   * Nhấn **Save routes**



**🔗 Liên kết với Subnet:**

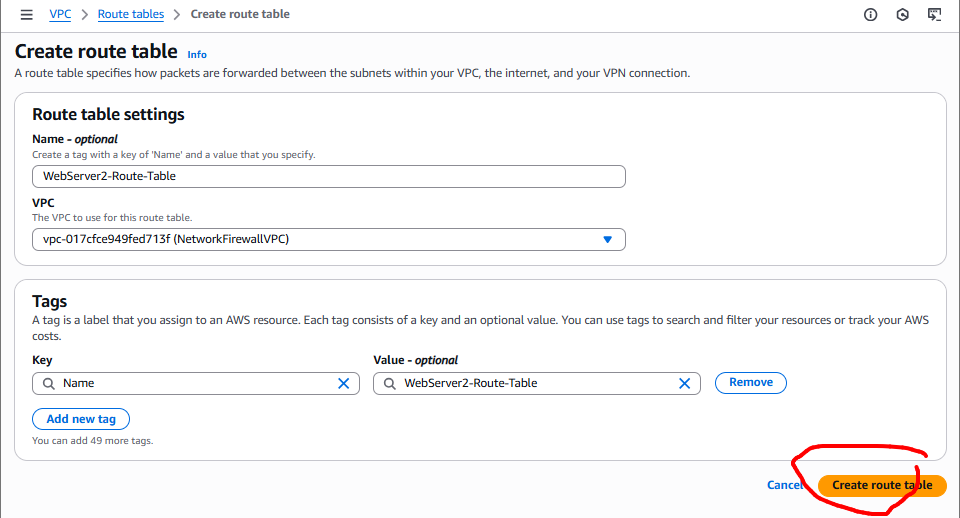
1. Tab **Subnet associations** → Nhấn **Edit subnet associations**
   * Chọn **FirewallSubnet**
   * Nhấn **Save associations**



### **Bước 3: Tạo bảng định tuyến cho WebServer2Subnet**

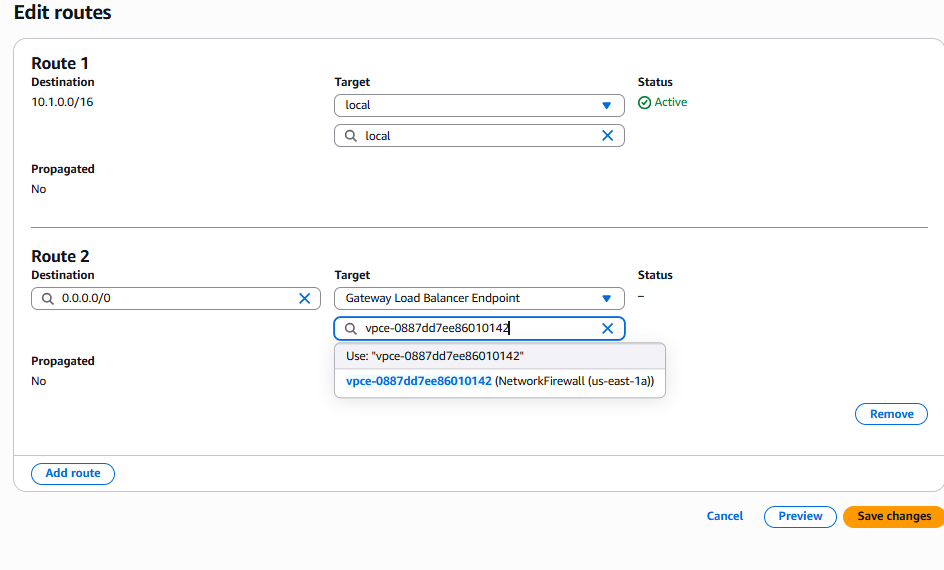
**📌 Tên: WebServer2-Route-Table**

1. Vào lại **Route Tables** → Nhấn **Create route table**
   * **Name tag**: WebServer2-Route-Table
   * **VPC**: chọn NetworkFirewallVPC
   * Nhấn **Create**



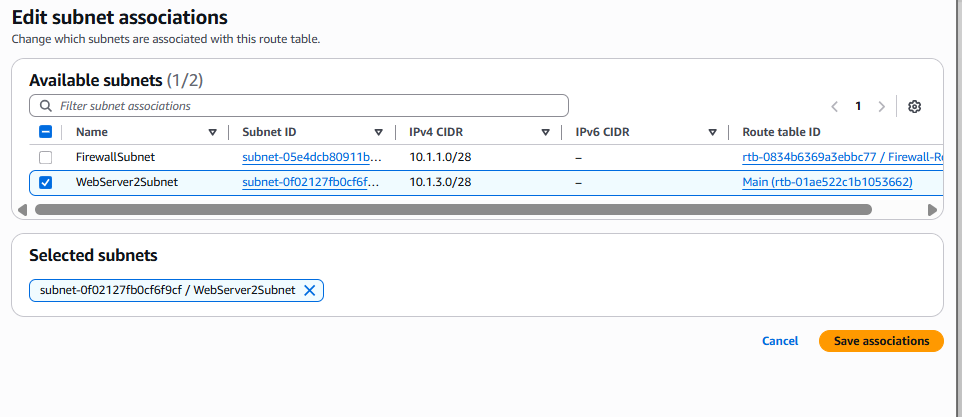
**➕ Thêm Route:**

1. Chọn WebServer2-Route-Table → Tab **Routes** → **Edit routes**
   * **Destination**: 0.0.0.0/0
   * **Target**: chọn **Gateway Load Balancer Endpoint**
   * Nhấn **Save routes**



**🔗 Liên kết với Subnet:**

1. Vào tab **Subnet associations** → **Edit subnet associations**
   * Chọn **WebServer2Subnet**
   * Nhấn **Save associations**



## **Nhiệm vụ 2.9: Cấu hình ghi nhật ký cho tường lửa mạng**

### **Bước 1: Tạo CloudWatch Log Group**

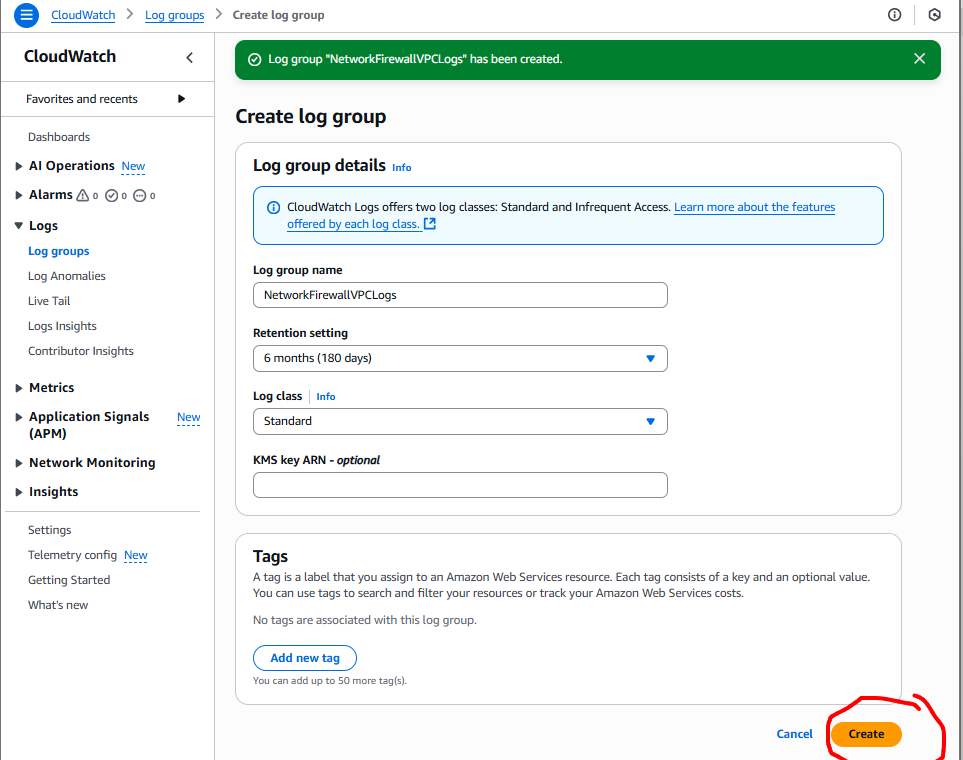
1. Truy cập **AWS Console**.
2. Mở dịch vụ **CloudWatch**.
3. Ở menu bên trái, chọn **Log groups**.
4. Nhấn nút **Create log group**.
5. Nhập tên log group là:

***NetworkFirewallVPCLogs***

1. Trong phần **Retention settings**, chọn:

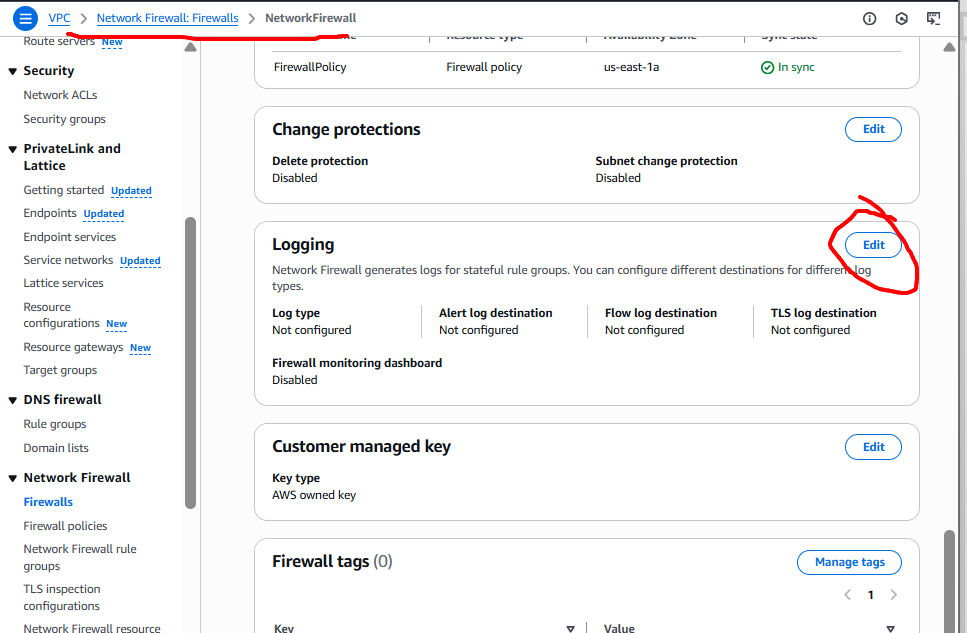
***6 months (6 tháng)***

1. Nhấn **Create** để hoàn tất.

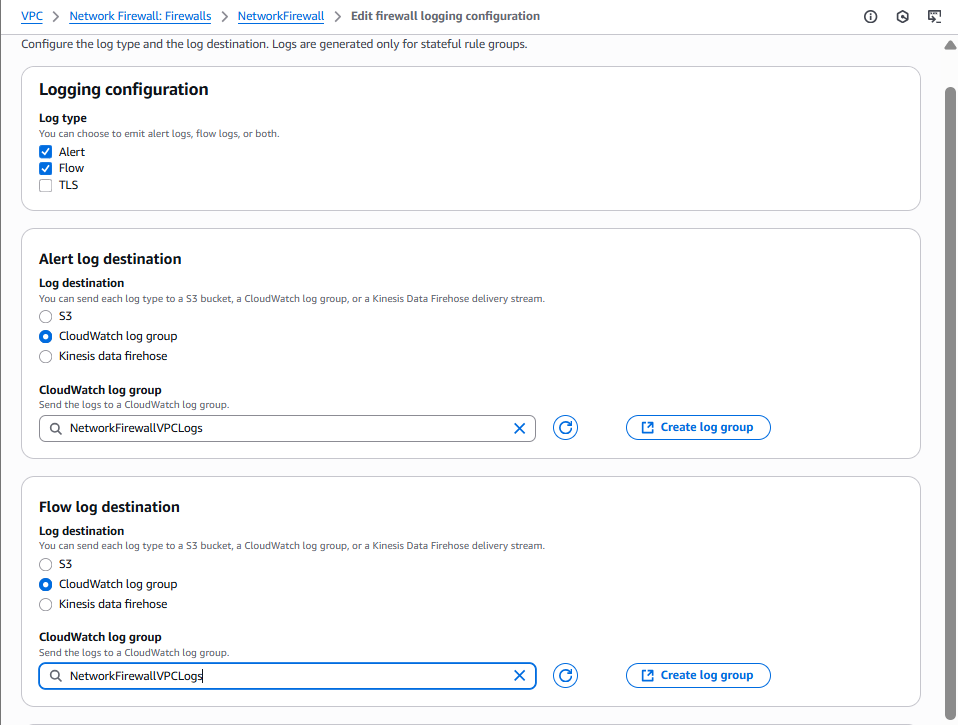


### **Bước 2: Cấu hình log cho Network Firewall**

1. Mở dịch vụ **VPC** từ AWS Console.
2. Ở menu bên trái, chọn **Network Firewall** > **Firewalls**.
3. Chọn firewall bạn đã tạo ở Task 2.7 (tên thường là NetworkFirewall).
4. Trong phần **Firewall details**, cuộn xuống **Logging configuration**.
5. Nhấn **Edit** hoặc **Add logging**.



1. Cấu hình như sau:
   * **Log types**: Chọn cả hai loại:
     + ✅ Flow logs
     + ✅ Alert logs
   * **Log destination type**: Chọn CloudWatch log group.
   * **CloudWatch log group**: Chọn NetworkFirewallVPCLogs.



1. Nhấn **Save** để lưu cấu hình logging.

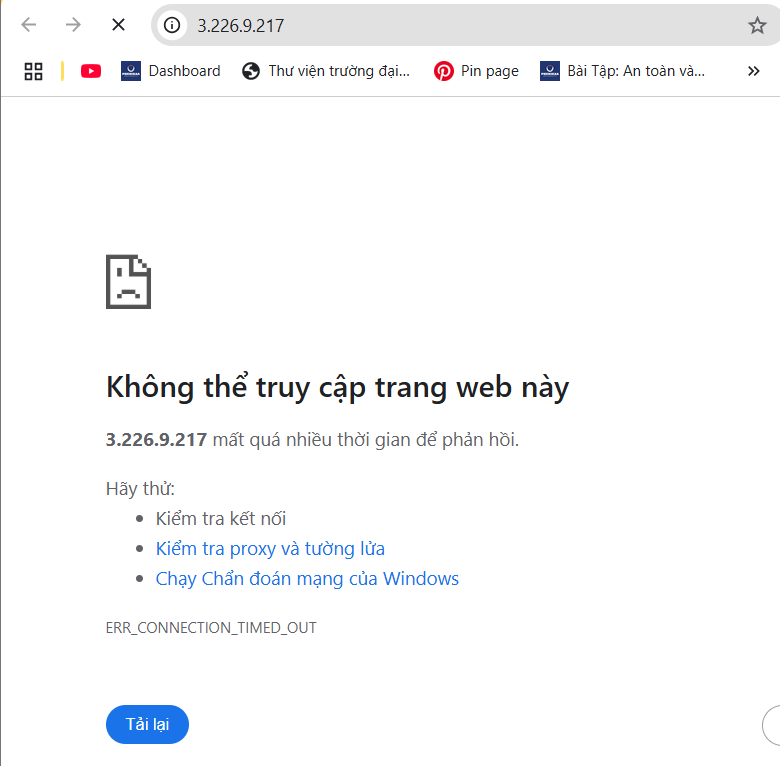
### **Bước 3: Kiểm tra cấu hình logging**

1. Mở một **tab trình duyệt mới**.
2. Truy cập địa chỉ **IPv4 Public** của **WebServer2 instance**, sử dụng **port 80 (HTTP)**, ví dụ:

http://<public-ip-of-WebServer2>

1. Trình duyệt sẽ **không load được website** và sẽ **timeout** (không sao cả, điều này là bình thường).

🔒 Vì firewall chưa cho phép HTTP traffic qua port 80, nên bị chặn.

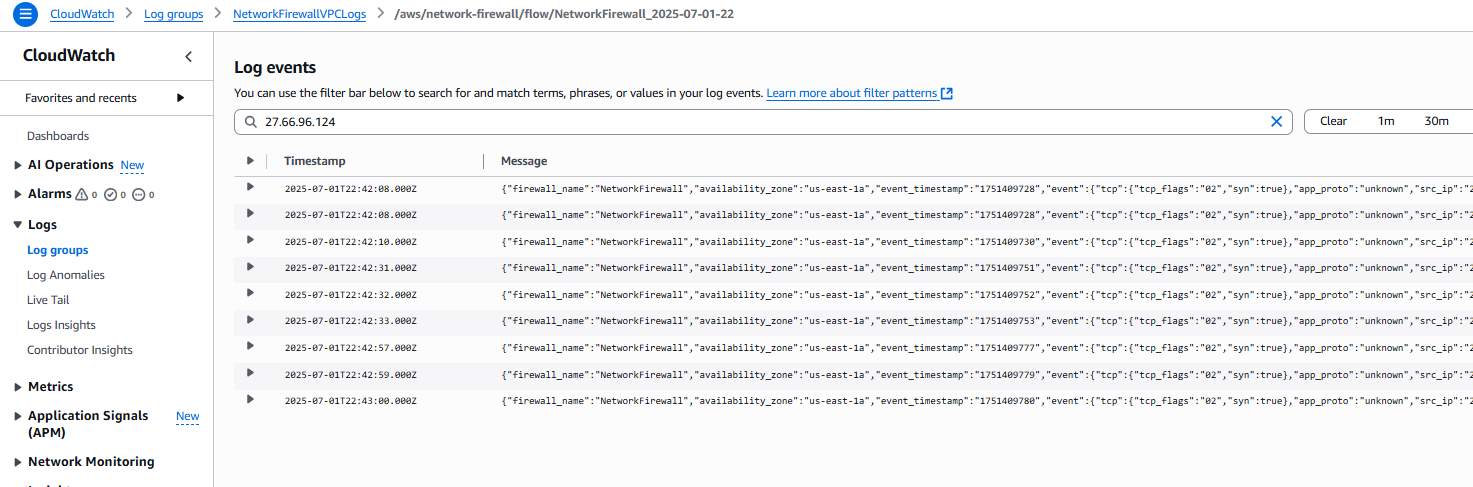


**IPv4**

### **Bước 4: Kiểm tra log trong CloudWatch**

1. Quay lại **AWS Console**, mở dịch vụ **CloudWatch**.
2. Vào **Log groups** > chọn log group tên **NetworkFirewallVPCLogs**.
3. Chọn **Log stream** mới nhất.
4. Dùng tính năng **filter (lọc)** theo địa chỉ **IP Public của bạn**:
   * Để tìm IP của bạn, truy cập <https://www.whatismyip.com>
5. Kiểm tra các log entry:
   * Log sẽ có trường src\_ip hoặc dest\_ip là IP của bạn.
   * Log inbound sẽ có dest\_port = 80.
   * Log outbound sẽ có src\_port = 80.

🕒 **Lưu ý:** Có thể mất khoảng **3–6 phút** để log được ghi vào CloudWatch.



## **Nhiệm vụ 2.10: Cấu hình chính sách tường lửa và kiểm tra quyền truy cập**

### **Bước 1: Tạo rule group type**

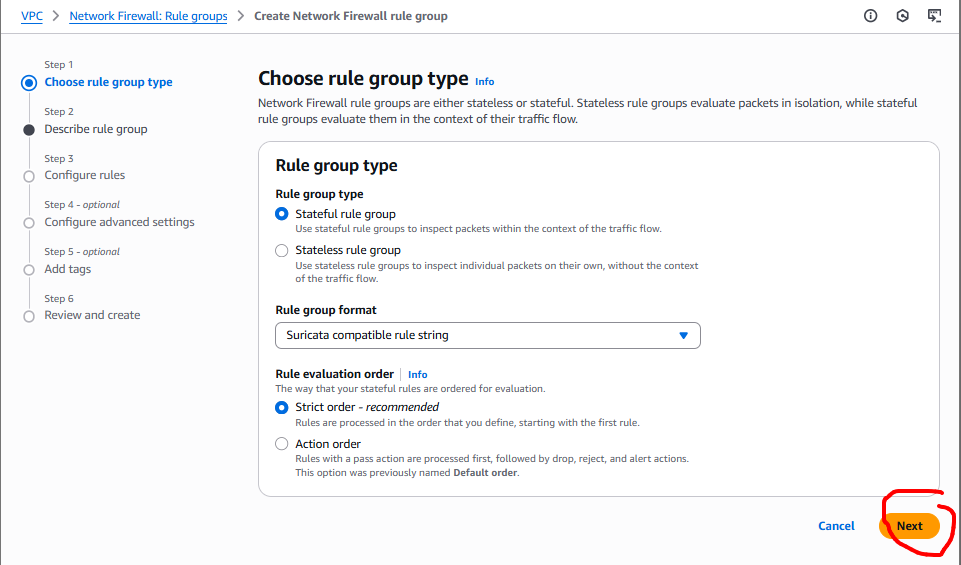
- **VPC > Network Firewall rule groups > Create rule group**

**1: Choose rule group type**

• Rule group type : Stateful rule group

• Rule group format : Suricata compatible IPS rules

• Rule evaluation order : Strict order – recommended

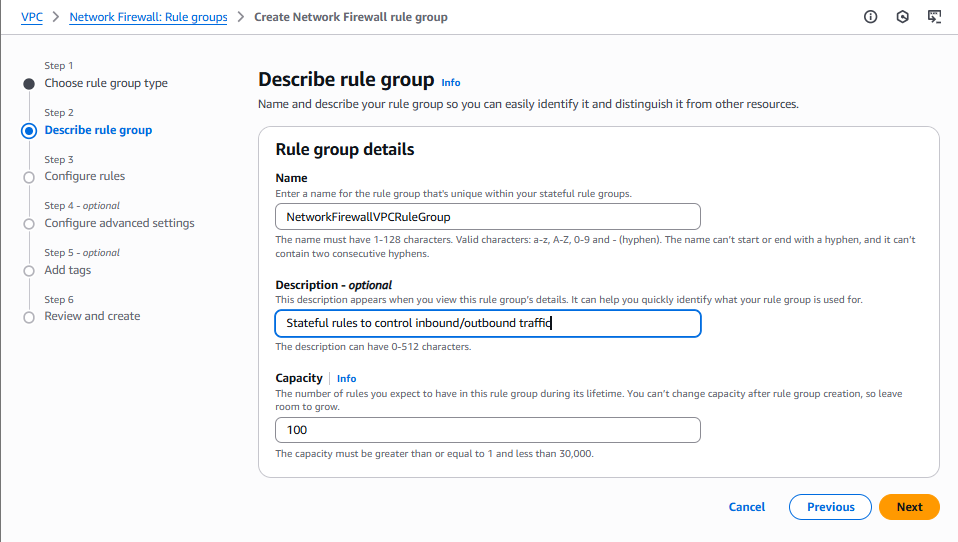


**2: Describe rule group**

• Name: NetworkFirewallVPCRuleGroup

• Capacity: 100 (hoặc giữ nguyên mặc định)

• Description: (tuỳ chọn) Stateful rules to control inbound/outbound traffic



**3: Configure rules**

***Remove tất cả các value của IP set và Port và IP set references***

• Nhập lệnh vào phần Suricata :

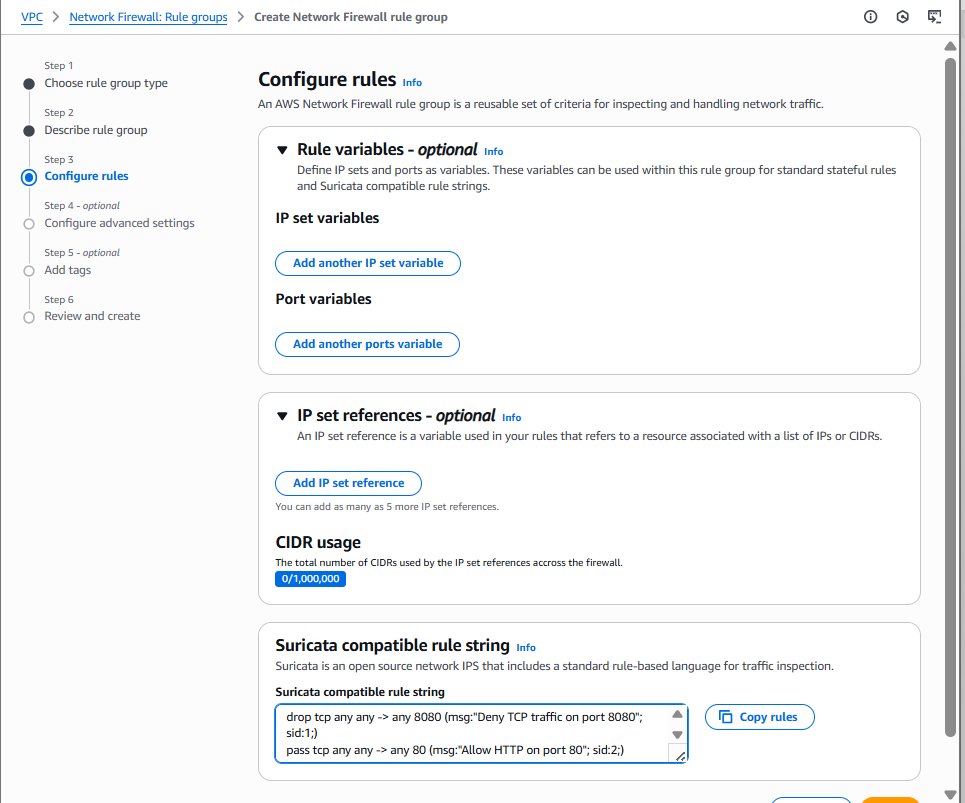
***drop tcp any any -> any 8080 (msg:"Deny TCP traffic on port 8080"; sid:1;)***

***pass tcp any any -> any 80 (msg:"Allow HTTP on port 80"; sid:2;)***

***pass tcp any any -> any 22 (msg:"Allow SSH on port 22"; sid:3;)***

***pass tcp any any -> any 443 (msg:"Allow HTTPS on port 443"; sid:4;)***

***pass icmp any any -> any any (msg:"Allow ICMP ping"; sid:5;)***

******

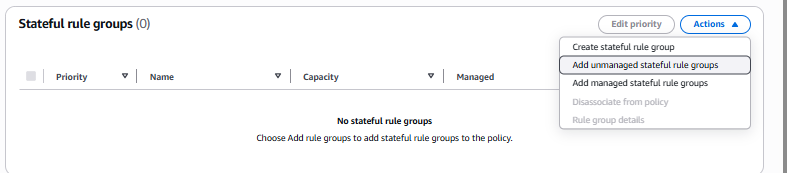
**4 : Configure advanced settings** -> bỏ qua

**5: Add tags** -> bỏ qua

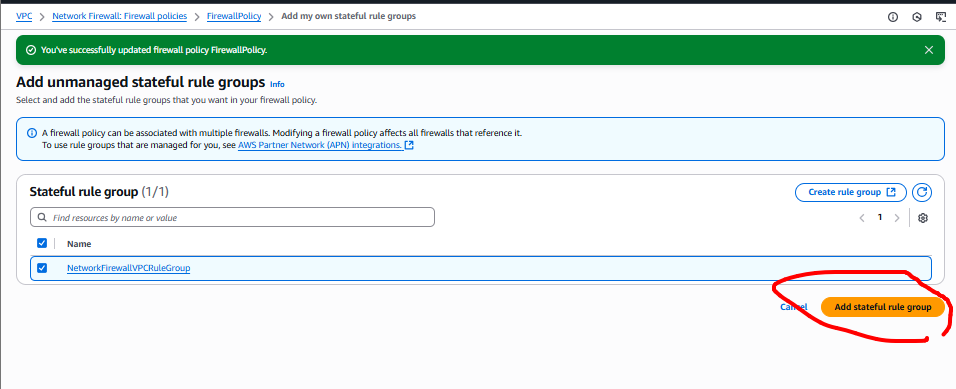
**Ấn Create**

### **Bước 2: Add to firewall policy**

Ở phần Stareful rule groups





****

### **Bước 3: Kiểm tra firewall**

Kiểm tra HTTP (port 80)

1. Mở trình duyệt
2. Truy cập vào http://<WebServer2-public-IP> **(Nếu máy chủ chỉ mở cổng 80 (HTTP) mà bạn lại dùng HTTPS (443) thì sẽ không truy cập được.)**

http://3.226.9.217/

1. ✅ Trang web hiển thị thành công vì port 80 đã được cho phép

Kiểm tra SSH (port 22) bằng Cloud9

1. Mở Cloud9 IDE
2. Chạy lệnh:

nc -zv <WebServer2-public-IP> 22

nc -zv 3.226.9.217 22



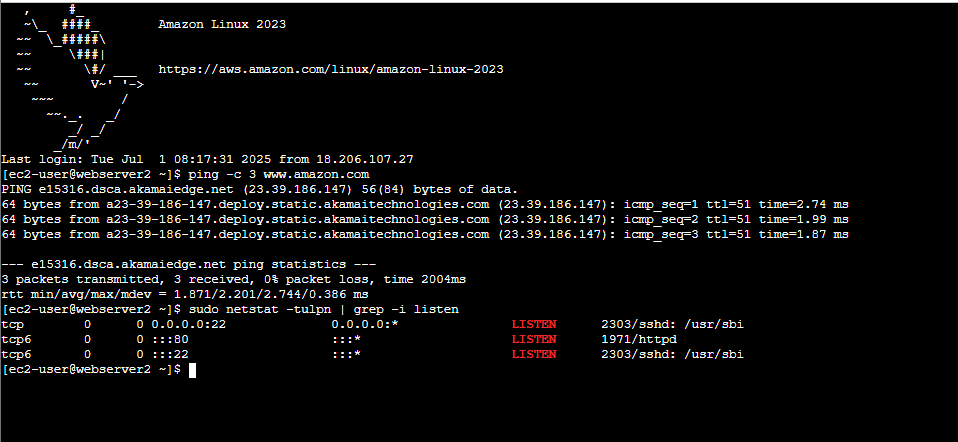
Nếu thấy succeeded, nghĩa là thành công

✅ Dùng EC2 Instance Connect để SSH vào WebServer2

1. Mở EC2 > chọn WebServer2 > nhấn Connect
2. Vào phiên làm việc, chạy:

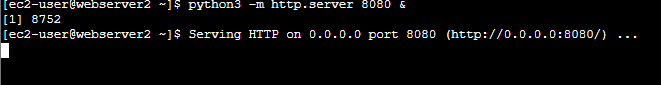
***ping -c 3 www.amazon.com***

***sudo netstat -tulpn | grep -i listen***

******

✅ Kết quả mong muốn:

* + ping hoạt động (nhờ ICMP rule)
  + netstat hiển thị các port:
    - sshd: 22
    - httpd: 80
    - python3: 8080 (nếu không thấy thì chạy python3 -m http.server 8080 &)



❌ Kiểm tra chặn truy cập port 8080

1. Truy cập: http://<WebServer2-public-IP>:8080
2. ❌ Trình duyệt báo lỗi vì port 8080 đã bị chặn bởi rule đầu tiên

🔁 Nếu muốn thử truy cập được, bạn có thể tạm đổi rule Drop sang Pass cho port 8080 → kiểm tra → đổi lại Drop.

### **Bước 4: Quan sát Log trong cloudwatch**

Quan sát log trong CloudWatch

* Mở **CloudWatch > Log groups > NetworkFirewallVPCLogs**
* Chọn **log stream mới nhất**
* Lọc theo IP máy bạn (dùng trang <https://www.whatismyip.com/>)
* Kiểm tra các dòng log:
  + Truy cập port 80: dest\_port=80, action=pass
  + Truy cập port 8080: dest\_port=8080, action=drop