

**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH**

**TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN**



## **BÁO CÁO**

### **Lab 3. LAN SECURITY**

**Họ và tên: Nguyễn Hữu Thạch**

**MSSV:20120576**

**Môn học: An ninh máy tính**

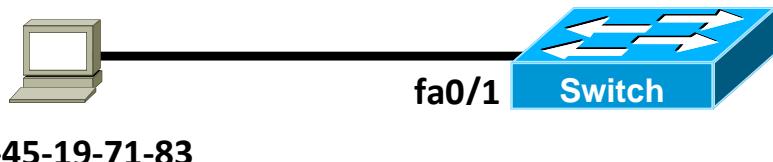
**Thành phố Hồ Chí Minh-2024**

## 1. Port Security (1,0 điểm)

Bằng cách giới hạn và kiểm soát các thiết bị gắn vào Switch có thể hạn chế nhiều tấn công trong LAN như:

- Kẻ tấn công dùng công cụ để quét lấy hết IP từ DHCP server
- Kiểm soát các thiết bị người dùng cố định, các server kết nối đến Switch (tránh sự thay đổi tự do trong quá trình vận hành hệ thống)

Topology



### Yêu cầu

1. Chỉ có client với địa chỉ MAC: 00-40-45-19-71-83 được sử dụng port fa0/1 trên Switch (tùy vào PC, SV có thể dùng địa chỉ MAC khác).
2. Các client khác gắn vào port fa0/1, port fa0/1 sẽ bị shutdown
3. port fa0/1 sẽ khôi phục lại sau 30 giây (ko lam duoc tren packet tracer).

### Cấu hình

1. Cấu hình port security. Chỉ có client với địa chỉ MAC: 00-40-45-19-71-83 được sử dụng port fa0/1 trên Switch.

```
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
(Switch(config-if)#switchport port-security mac-address 0040.4519.7183)
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address sticky
```

2. Các client khác gắn vào port fa0/1, port fa0/1 sẽ bị shutdown

```
Switch(config)#interface fa0/1
Switch(config-if)#switchport port-security violation shutdown
```

```
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#ex
Switch(config)#interface fa0/1
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#

```

3. port fa0/1 sẽ khôi phục lại sau 30 giây (các lệnh sau không hỗ trợ trên phần mềm giả lập Packet Tracer, – SV không cần làm chức năng này hoặc thử nghiệm trên GNS3)

```

Switch(config)#errdisable detect cause all
Switch(config)#errdisable recovery cause all
Switch(config)#errdisable recovery interval 30

```

Kiểm tra cấu hình

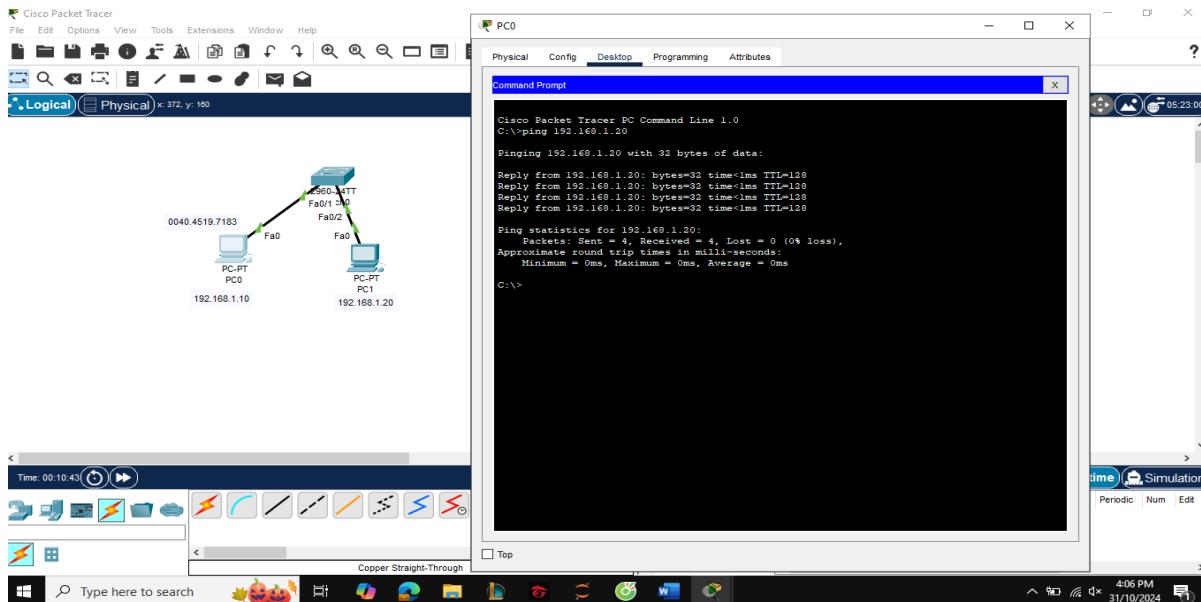
```

show interface switchport
show port-security interface

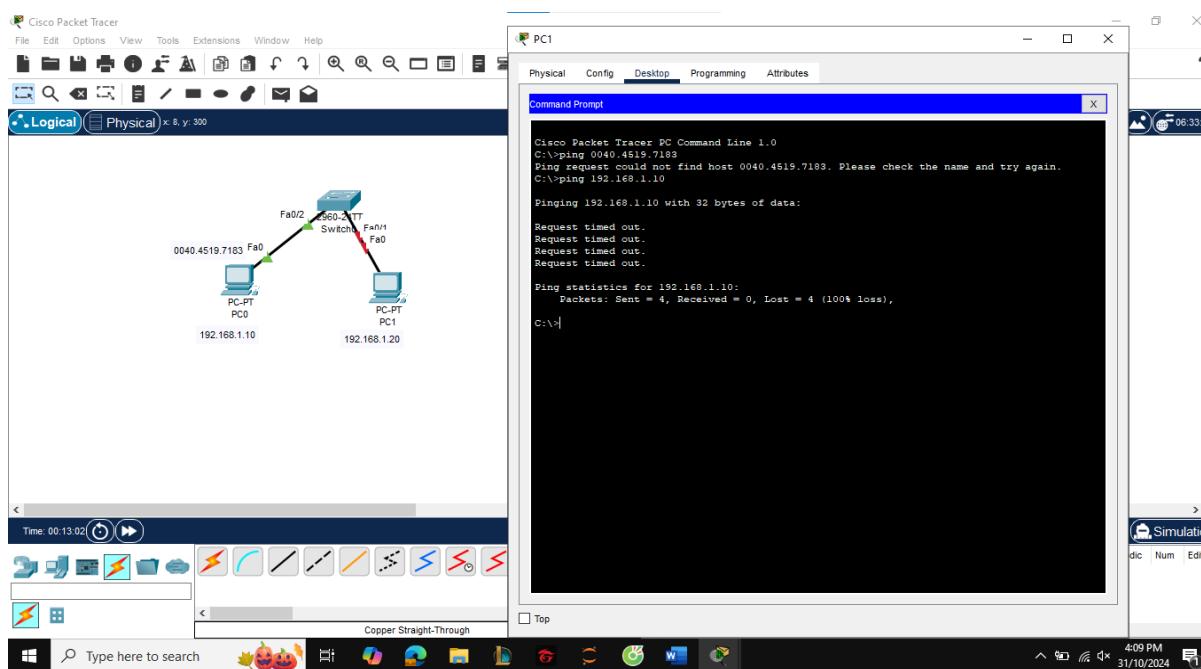
```

**Kết quả:**

**PC1 (Địa chỉ MAC: 0040.4519.7183)**

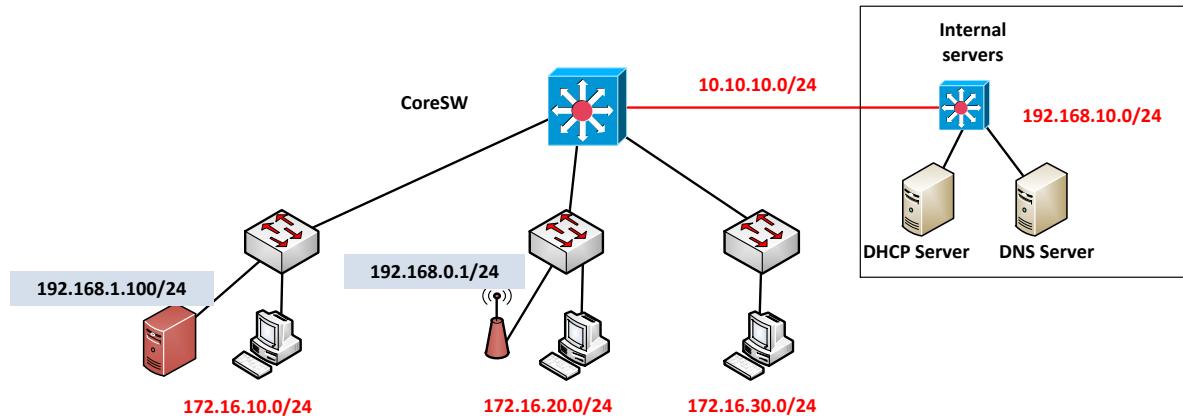


**PC2: (Địa chỉ MAC khác 0040.4519.7183)**



- ⇒ Chỉ có client với địa chỉ MAC: 00-40-45-19-71-83 được sử dụng port fa0/1 trên Switch. Các client khác gắn vào port fa0/1, port fa0/1 sẽ bị shutdown
- DHCP snooping (2,0 điểm)**

Chống giả các DHCP server trong hệ thống, chỉ cho phép các client xin IP từ DHCP Server thật (*sử dụng phần mềm giả lập Packet Tracer hoặc EVE*)

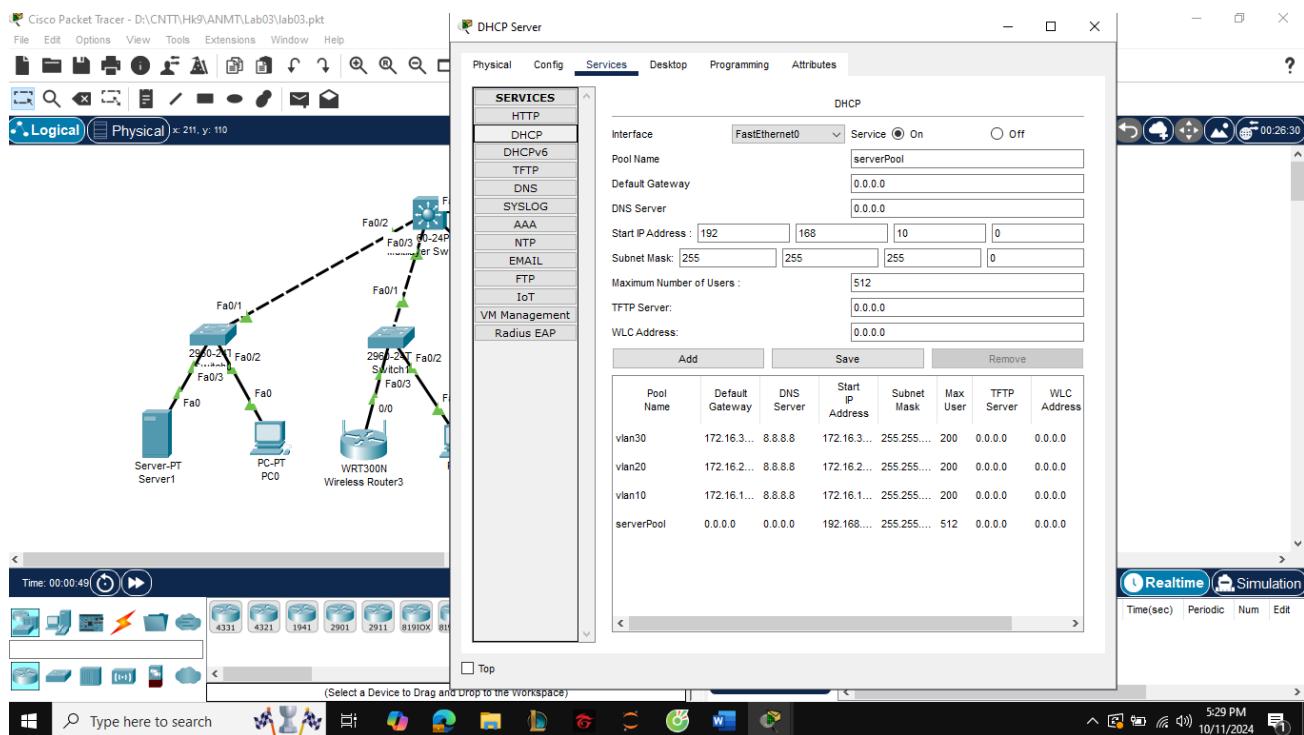


## Topology

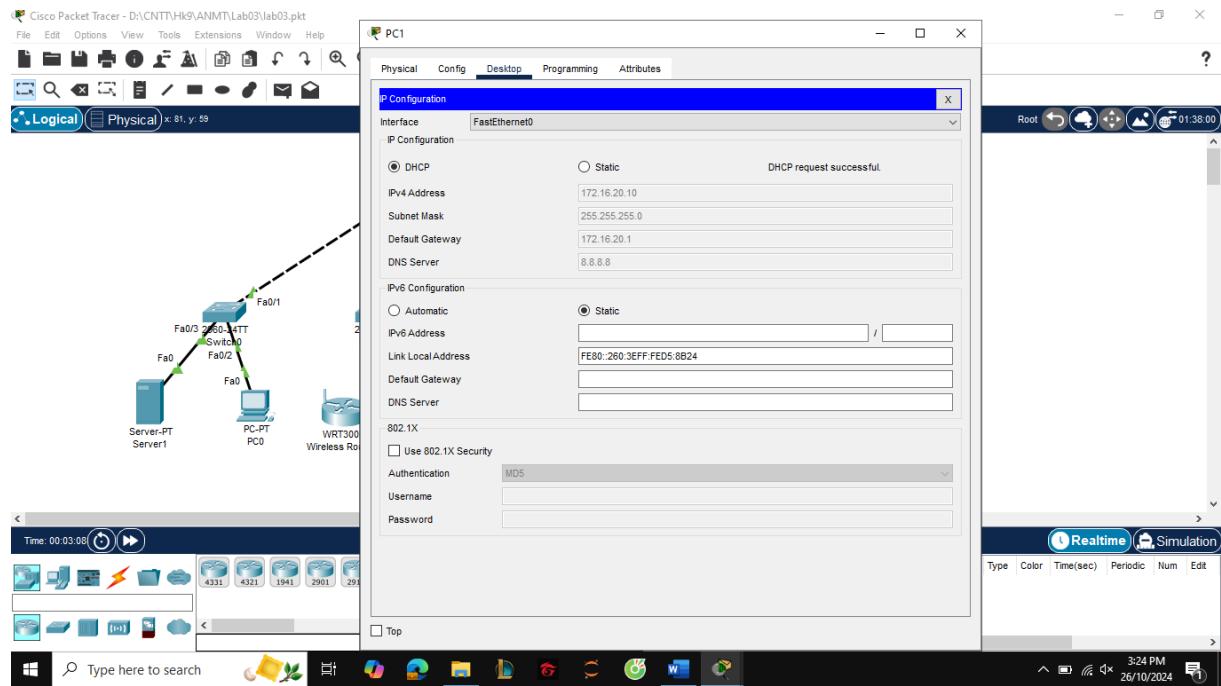
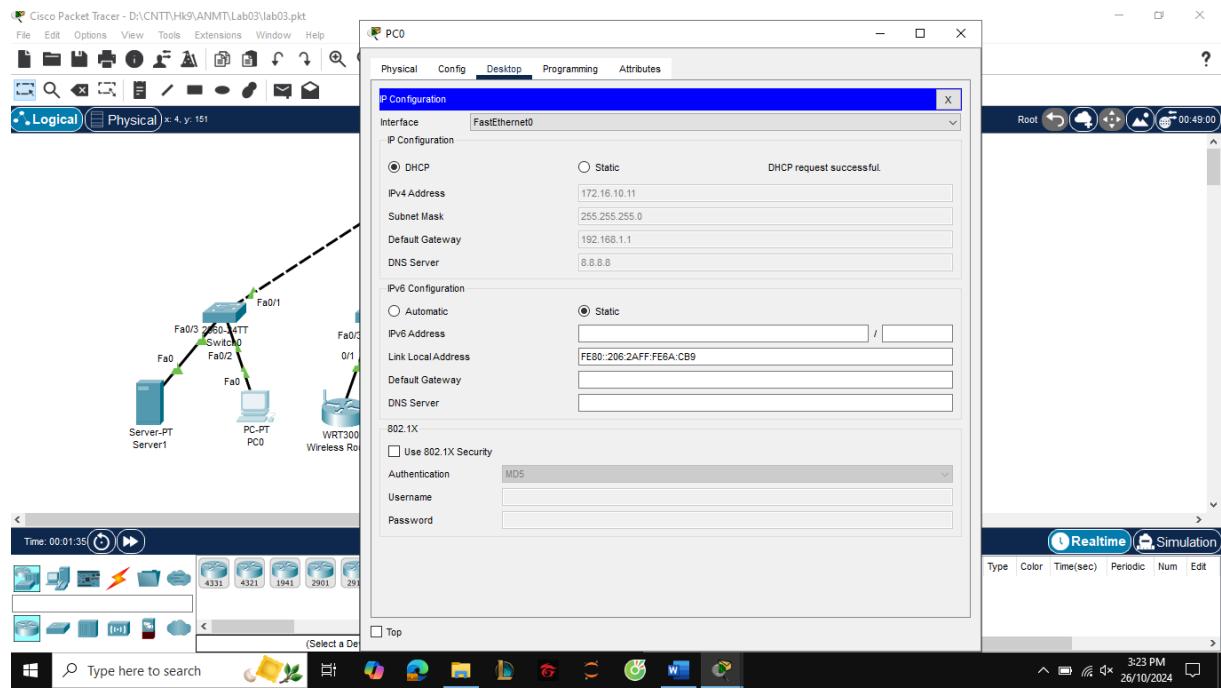
### Yêu cầu

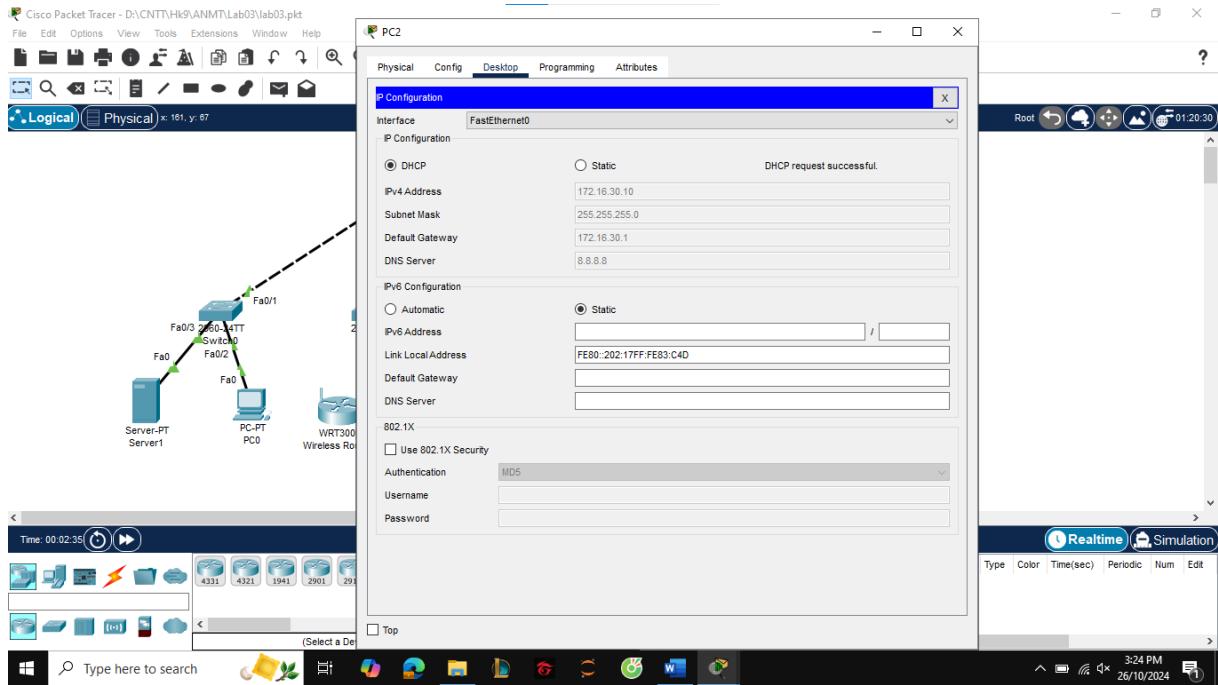
- Cáu hình theo sơ đồ mạng trên
- Cáu hình định tuyến
- Cáu hình cho DHCP server cấp phát địa chỉ IP động cho các PC ở các mạng 172.16.10.0/24, 172.16.20.0/24, 172.16.30.0/24

### Cáu hình cho DHCP server cấp phát IP động:



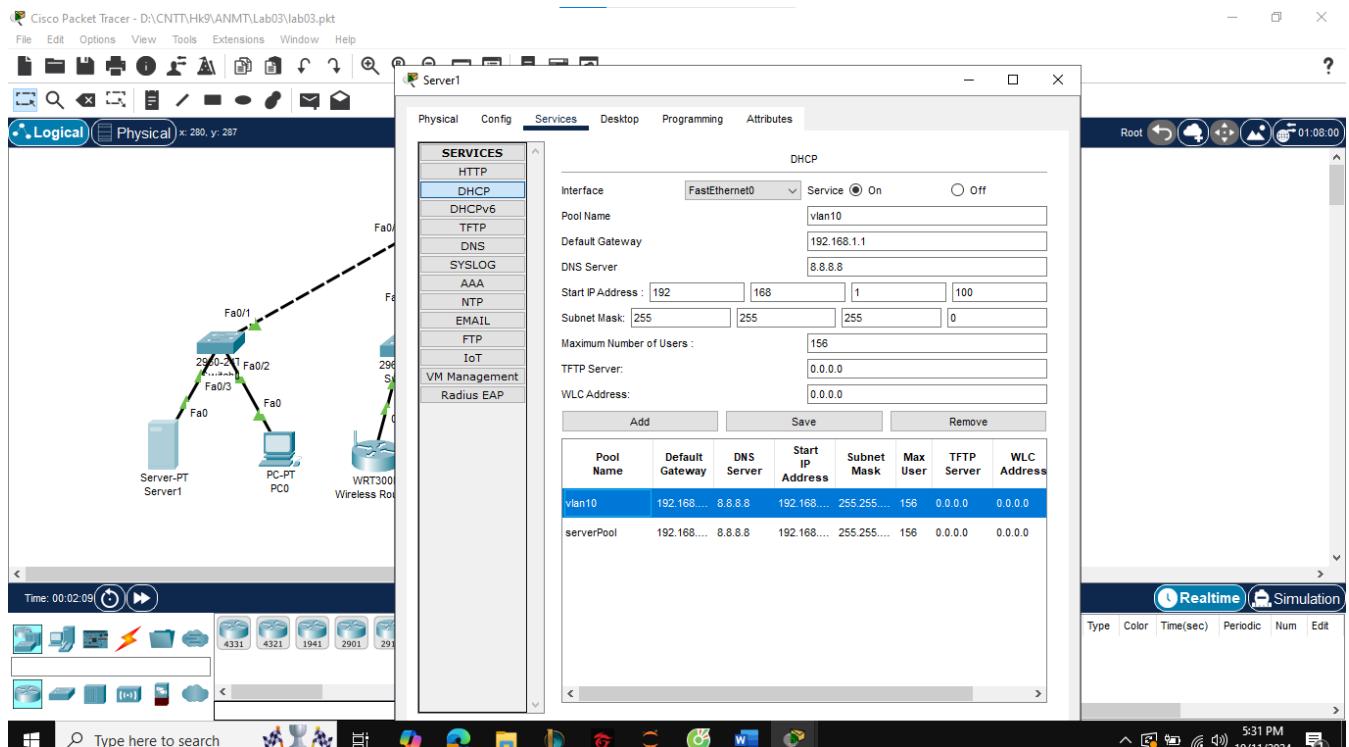
## Kết quả:

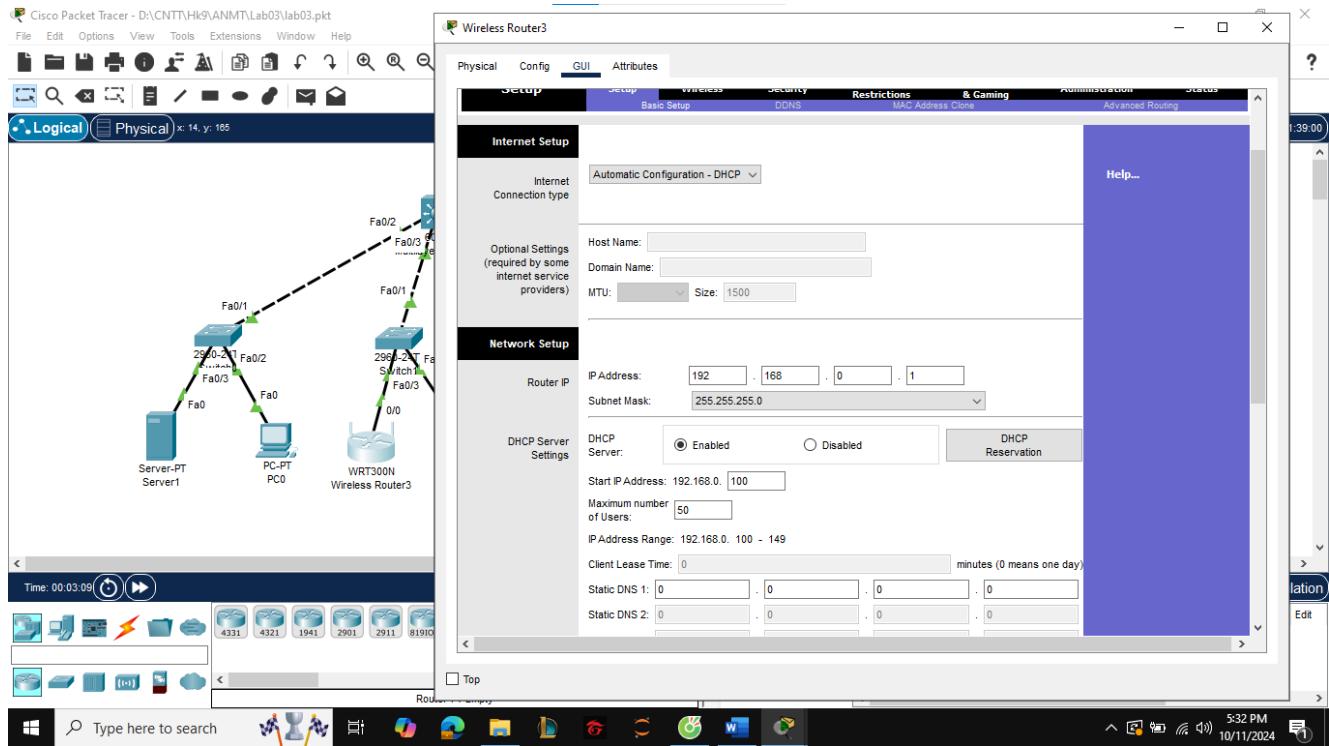




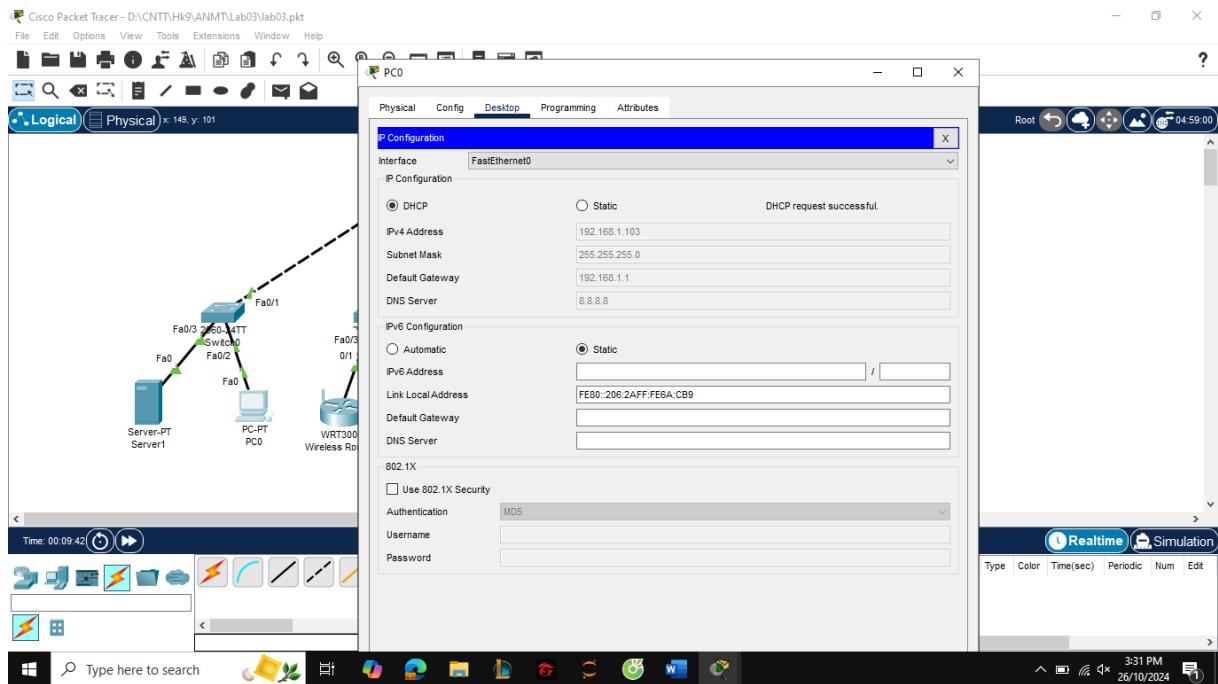
- ⇒ PC0, PC1, PC2 sẽ nhận địa chỉ IP do DHCP server cấp phát.  
 2. Thủ trưởng hợp với các DHCP server giả và AP cấp IP động

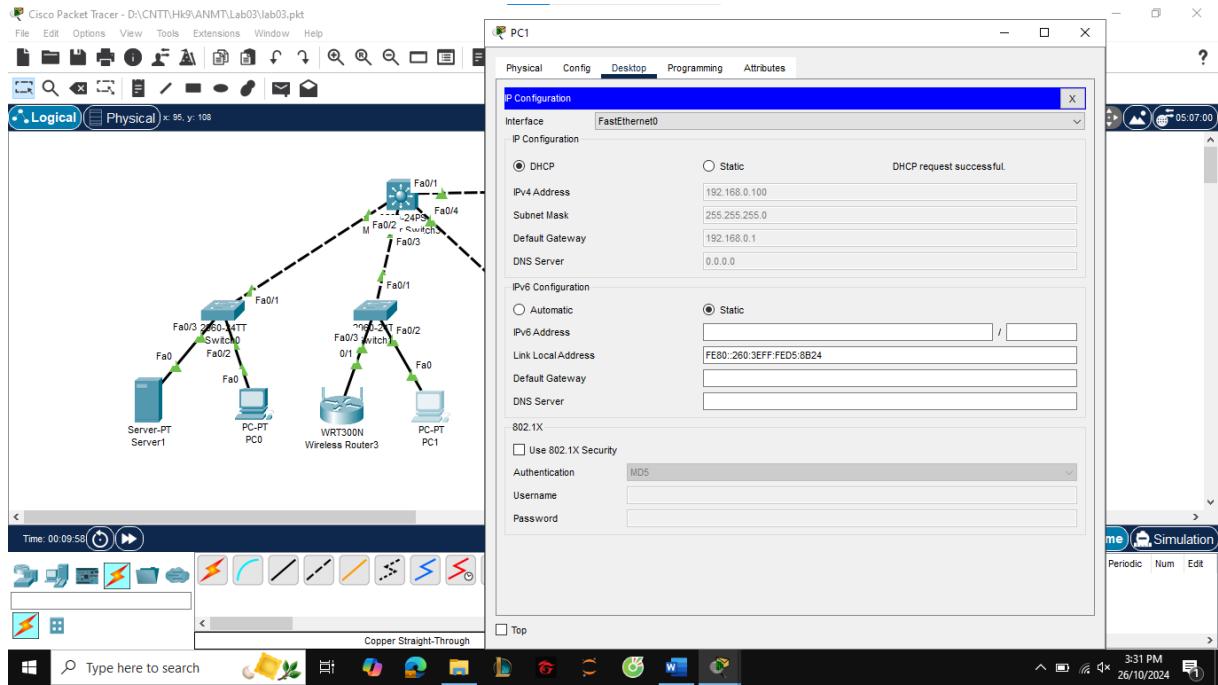
### Cấu hình cho DHCP server giả và AP cấp phát IP giả cho các PC





Kết quả:





- ⇒ PC0 sẽ nhận địa chỉ IP do DHCP server giả lập phát, PC1 sẽ nhận được địa chỉ IP do AP cấp phát.
3. Cấu hình DHCP snooping trên Switch, sao cho các client chỉ xin địa chỉ IP từ DHCP trên DHCP Server thật.

Các lệnh cấu hình:

```

Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#no ipdhcp snooping information option
Switch(config)#interface <interface> (port kết nối hoặc port hướng kết nối về DHCP thật)
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#exit

```

### Cấu hình DHCP trên Switch0

```

Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 10
Switch(config)#no ipdhcp snooping information option
%
% Invalid input detected at '^' marker.

Switch(config)#no ip dhcp snooping information option
Switch(config)#int fa0/1
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#exit

```

### Cấu hình DHCP trên Switch1

```

Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 20
Switch(config)#no ipdhcp snooping information option
%
% Invalid input detected at '^' marker.

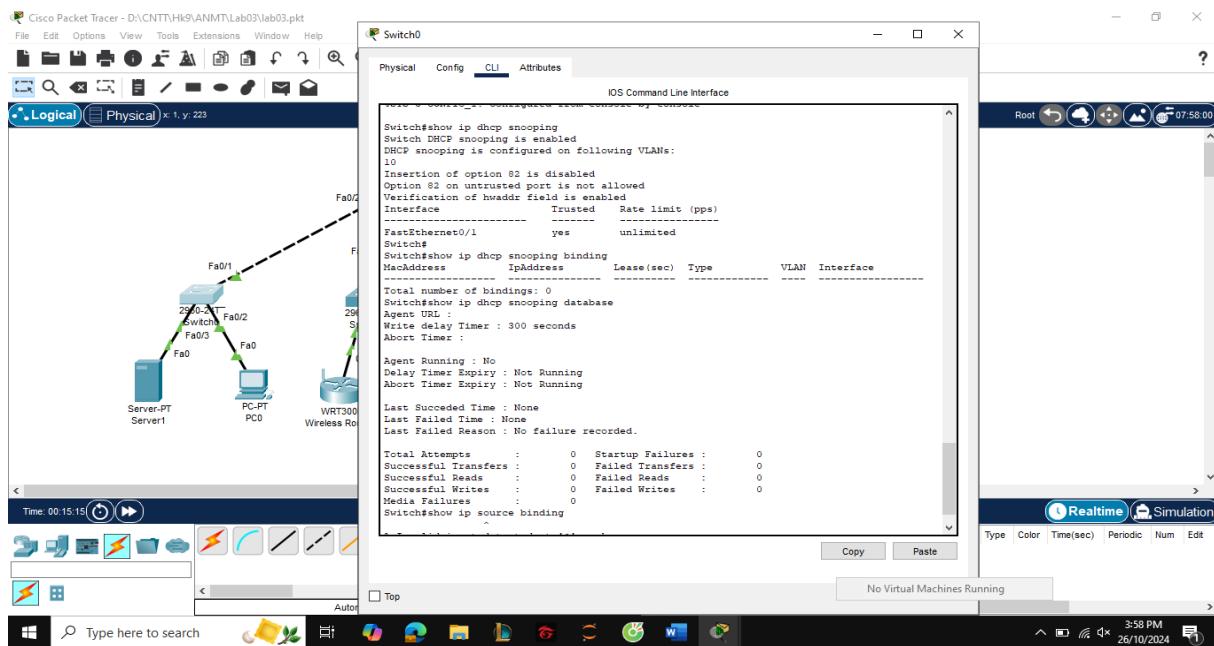
Switch(config)#no ip dhcp snooping information option
Switch(config)#int fa0/1
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#exit

```

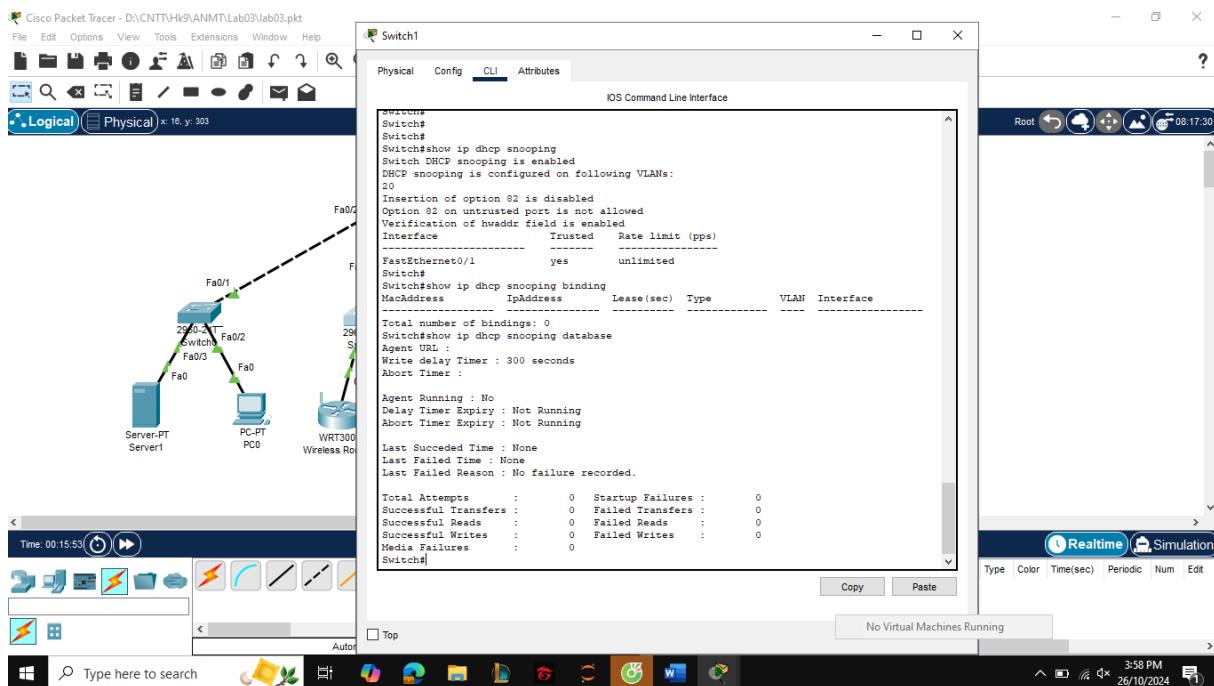
## Kiểm tra cấu hình

*show ip dhcp snooping*  
*show ip dhcp snooping binding*  
*show ip dhcp snooping database*  
*show ip source binding*

### Switch0

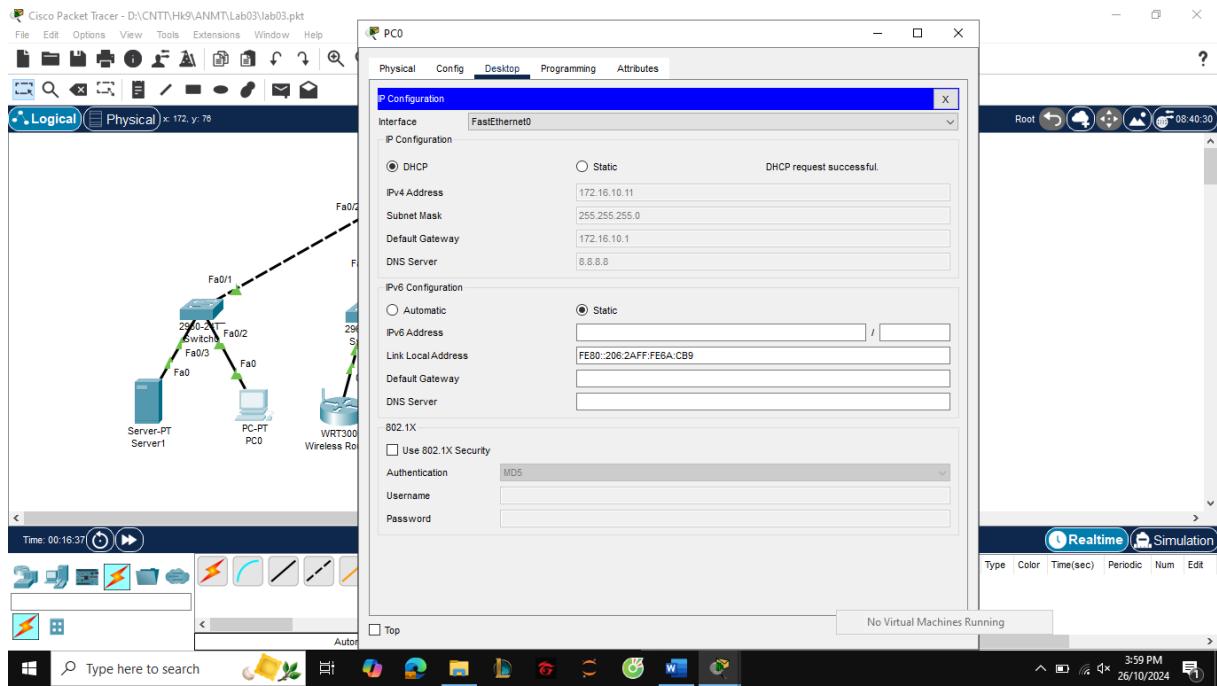


### Switch1

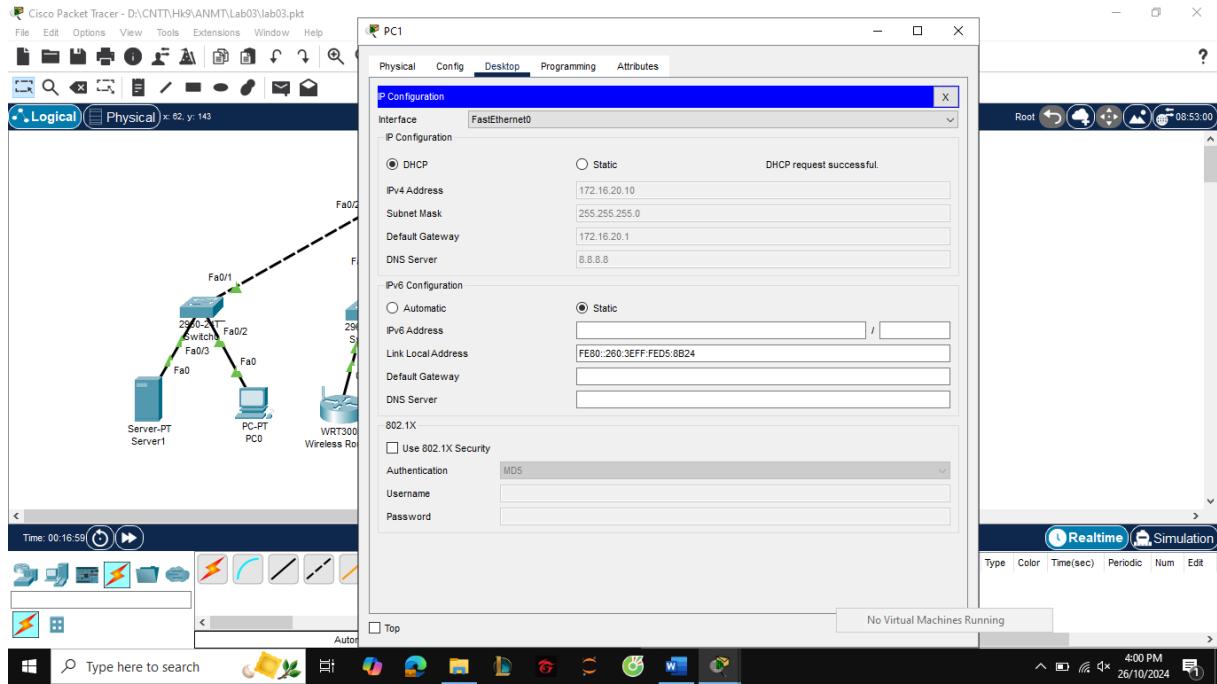


## Kết quả:

### PC0:



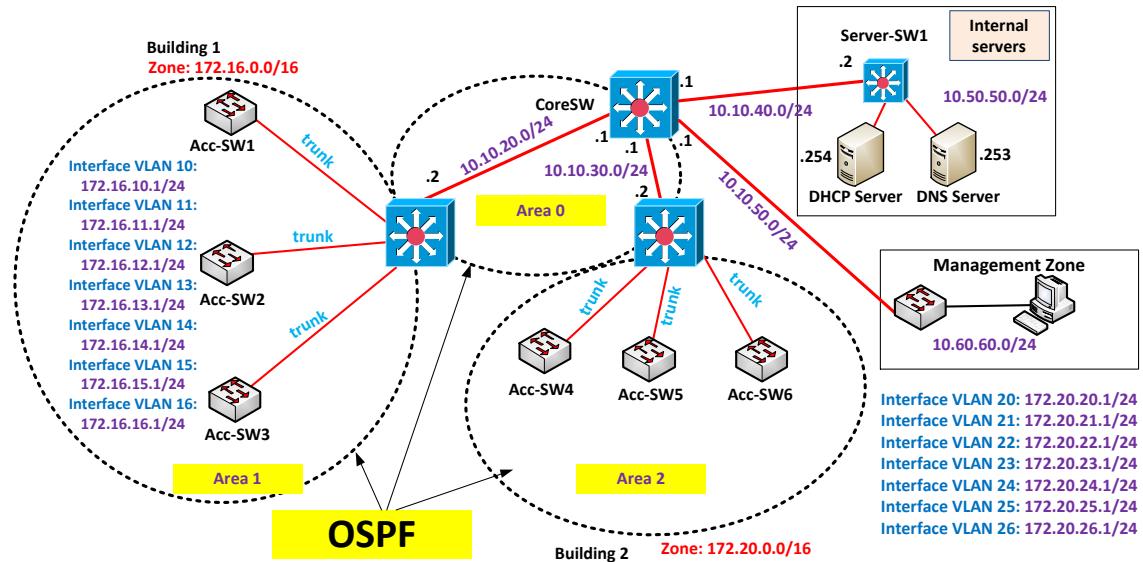
### PC1:



⇒ PC0 và PC1 đã xin đúng IP từ DHCP server thật

### 3. Access Control List (2,0 điểm)

Cho sơ đồ mạng



Sử dụng lại bài Lab 01, có bổ sung thêm khu vực quản trị (Management zone)

- a) Định tuyến cho khu vực Management Zone

Mở line telnet/SSH trên các thiết bị mạng: CoreSW, Dist-SW1, Dist-SW2, Access-SW1 → Access-SW6)

Trong đó:

- IP của các Acc-Sw1 → Acc-SW3: 172.16.1.1/24 → 172.16.1.3/24
- IP của các Acc-Sw4 → Acc-SW6: 172.16.2.4/24 → 172.16.2.6/24

- b) Cấu hình ACL:

- Cấm các PC thuộc VLAN 10 và VLAN 20 ping tới các server trong khu vực Internal Server
- Chỉ cho phép các PC trong khu vực quản trị được phép quản trị từ xa các thiết bị mạng (CoreSW, Dist-SW1, Dist-SW2, Access-SW1 → Access-SW6)

#### Các bước thực hiện:

- a) Định tuyến cho khu vực Management Zone

Mở line telnet/SSH trên các thiết bị mạng: CoreSW, Dist-SW1, Dist-SW2, Access-SW1 → Access-SW6)

Trong đó:

- IP của các Acc-Sw1 → Acc-SW3: 172.16.1.1/24 → 172.16.1.3/24

#### 1. Cấu hình và định tuyến cho khu vực Management Zone:

- Cấu hình L3 EtherChannel giữa Core-SW và Management Zone (đặt tên channel là Po 14)

#### Core-SW

1. Chuyển các cổng vật lý sang chế độ Layer 3.

```
Core-SW#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Core-SW(config)#int range fa0/8-9
Core-SW(config-if-range)#no switchport
```

2. Tạo và cấu hình Etherchannel trên cổng: (Sử dụng chế độ PAgP)

```
Core-SW(config-if-range)#channel-protocol pagp
Core-SW(config-if-range)#channel-group 14 mode desirable
Core-SW(config-if-range)#
%LINK-3-UPDOWN: Interface Port-channel14, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel14, changed state to down
Core-SW(config-if-range)#ex
```

3. Cấu hình giao diện Port-channel 14 với địa chỉ IP

```
Core-SW(config)#int port-channel 14
Core-SW(config-if)#ip address 10.10.50.1 255.255.255.0
Core-SW(config-if)#no shutdown
Core-SW(config-if)#
%LINK-5-CHANGED: Interface Port-channel14, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel14, changed state to up
Core-SW(config-if)#ex
```

## Management Zone

1. Chuyển các cổng vật lý sang chế độ Layer 3.

```
Switch(config)#int range fa0/1-2
Switch(config-if-range)#no switchport
```

2. Tạo và cấu hình Etherchannel trên cổng: (Sử dụng chế độ PAgP)

```
Switch(config-if-range)#channel-protocol pagp
Switch(config-if-range)#channel-group 14 mode desirable
Switch(config-if-range)#
%LINK-3-UPDOWN: Interface Port-channel14, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel14, changed state to down
Switch(config-if-range)#ex
```

3. Cấu hình giao diện Port-channel 14 với địa chỉ IP:

```
Switch(config)#int port-channel 14
Switch(config-if)#ip address 10.10.50.2 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#
%LINK-5-CHANGED: Interface Port-channel14, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel14, changed state to up
Switch(config-if)#ex
```

- Định tuyến cho khu vực Management Zone:

### Management Zone:

```

Switch(config)#ip routing
Switch(config)#ip route 172.16.0.0 255.255.0.0 10.10.50.1
Switch(config)#ip route 172.20.0.0 255.255.0.0 10.10.50.1
Switch(config)#ip route 0.0.0.0 0.0.0.0 10.10.50.1

```

### Core-SW:

```

Core-SW#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Core-SW(config)#ip route 10.60.60.0 255.255.255.0 10.10.50.2

```

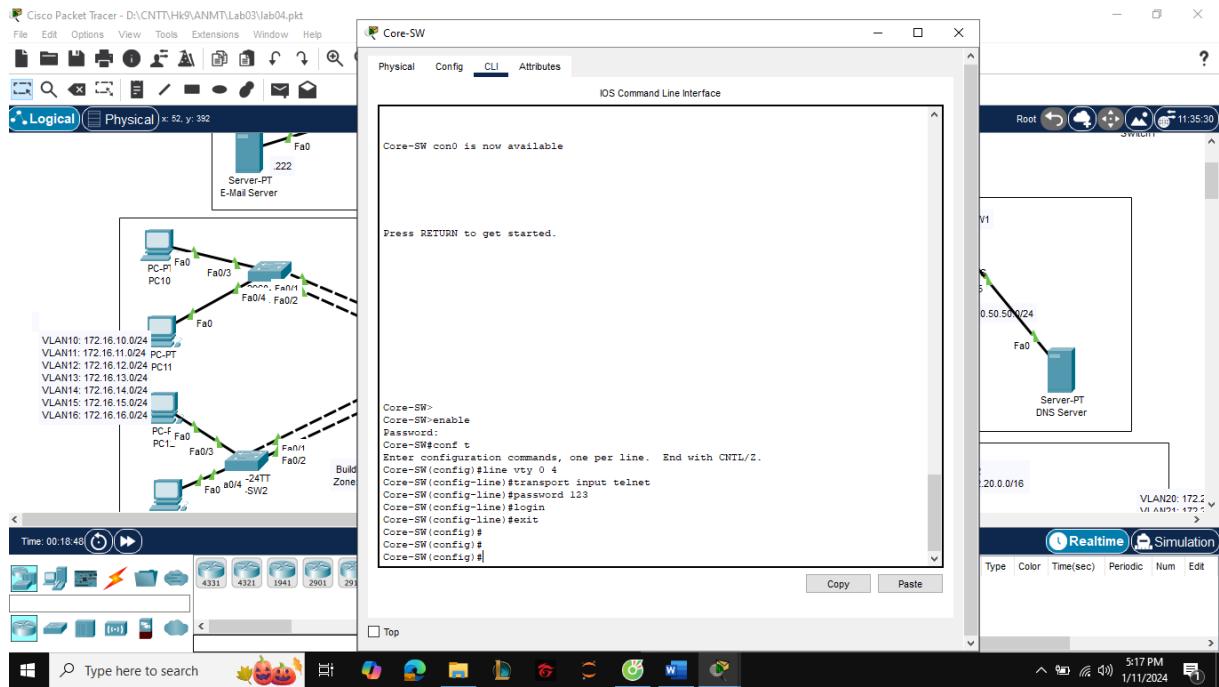
### Firewall:

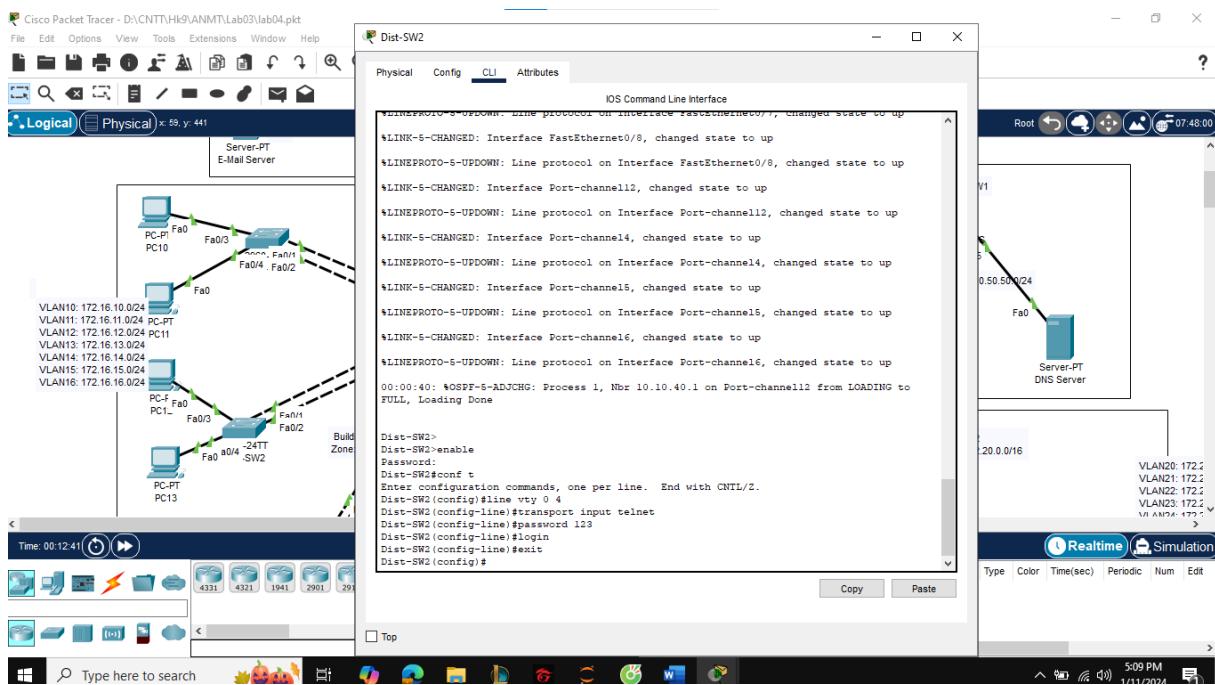
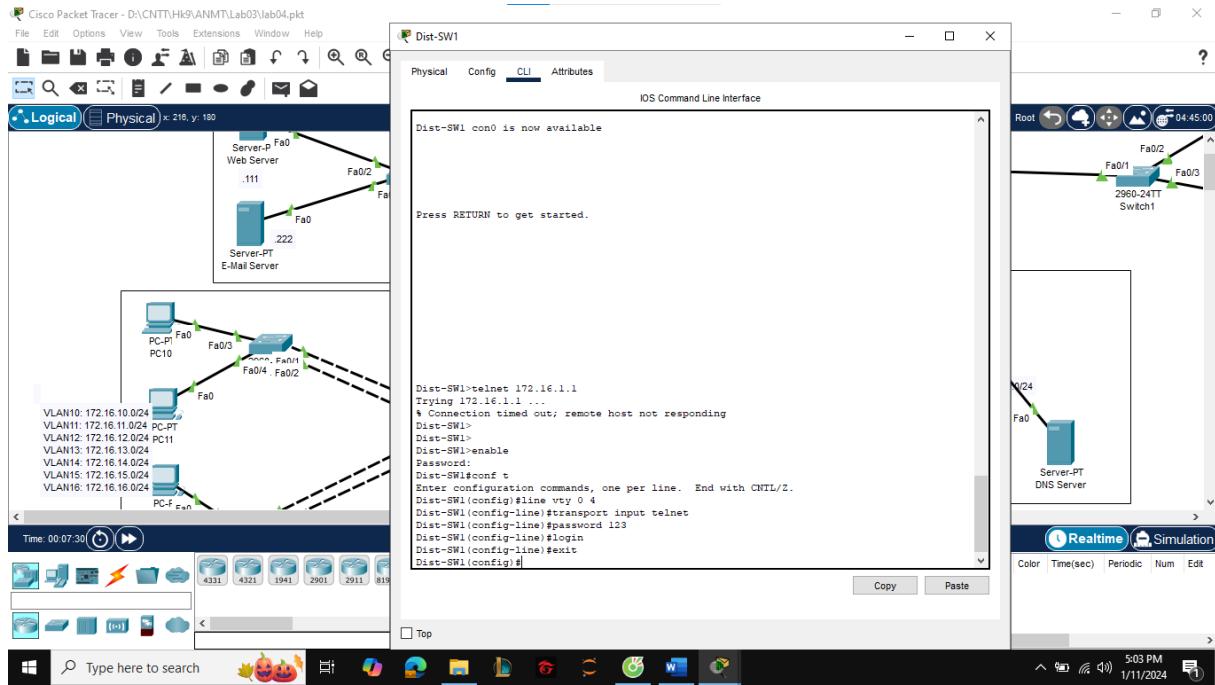
```

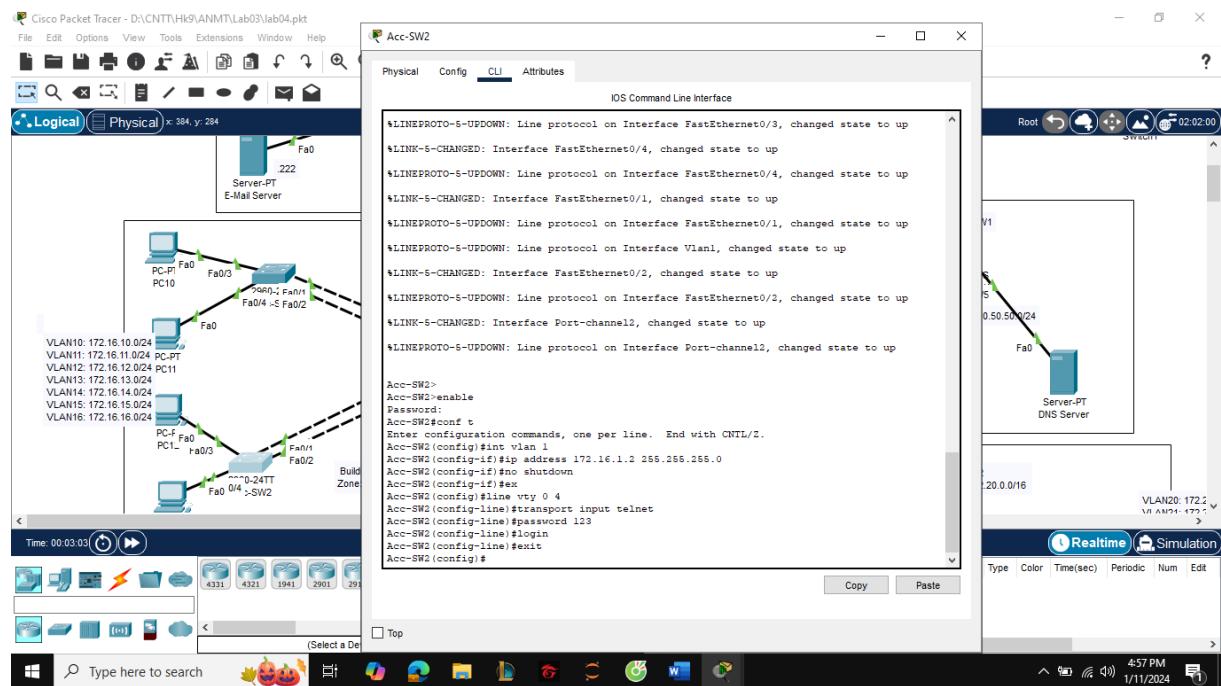
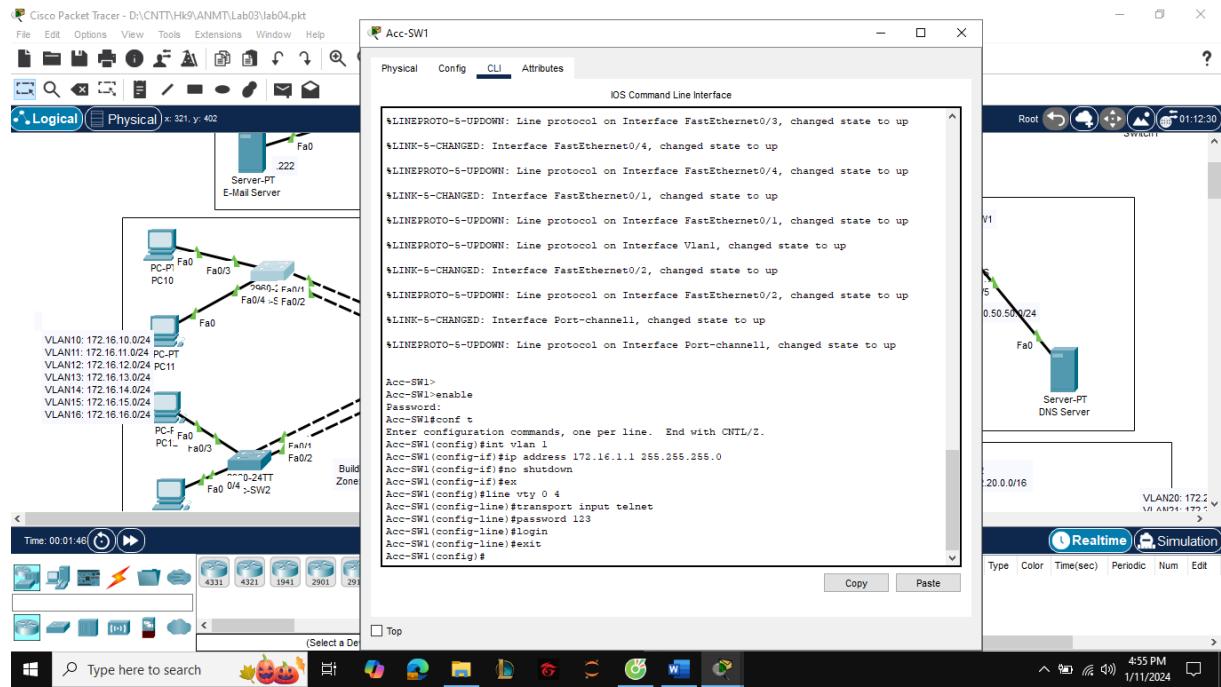
ciscoasa#conf t
ciscoasa(config)#route inside 10.60.60.0 255.255.255.0 10.10.10.2
ciscoasa(config)#
ciscoasa(config)#ex

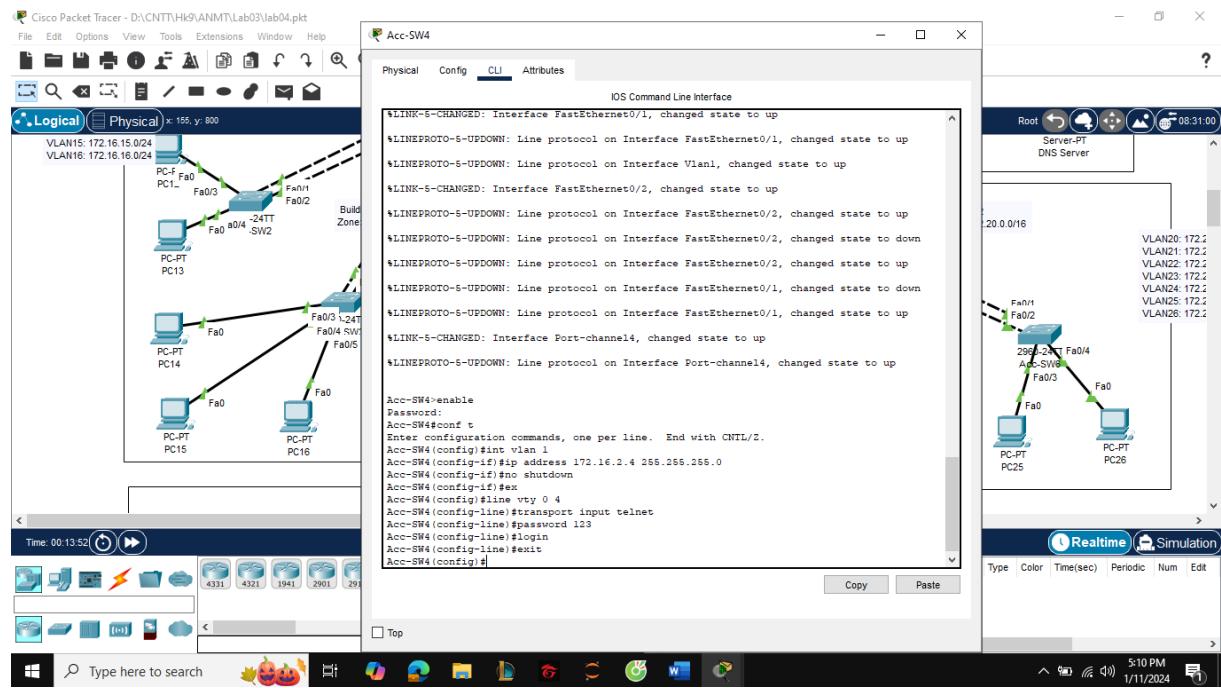
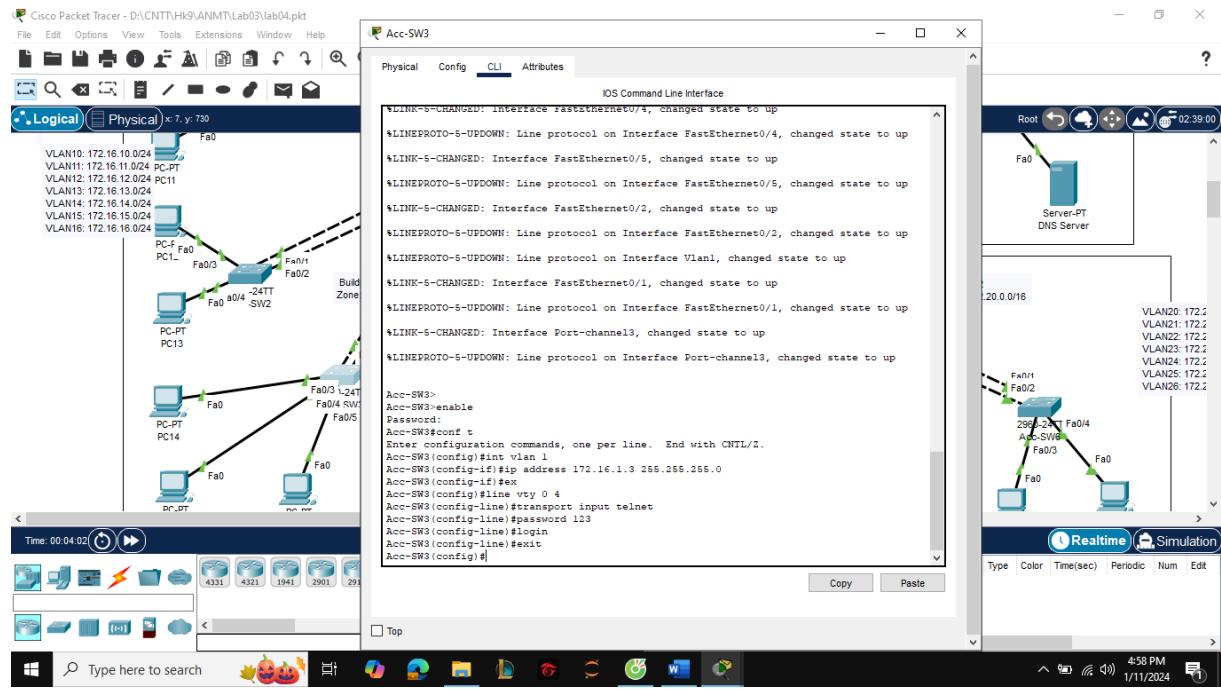
```

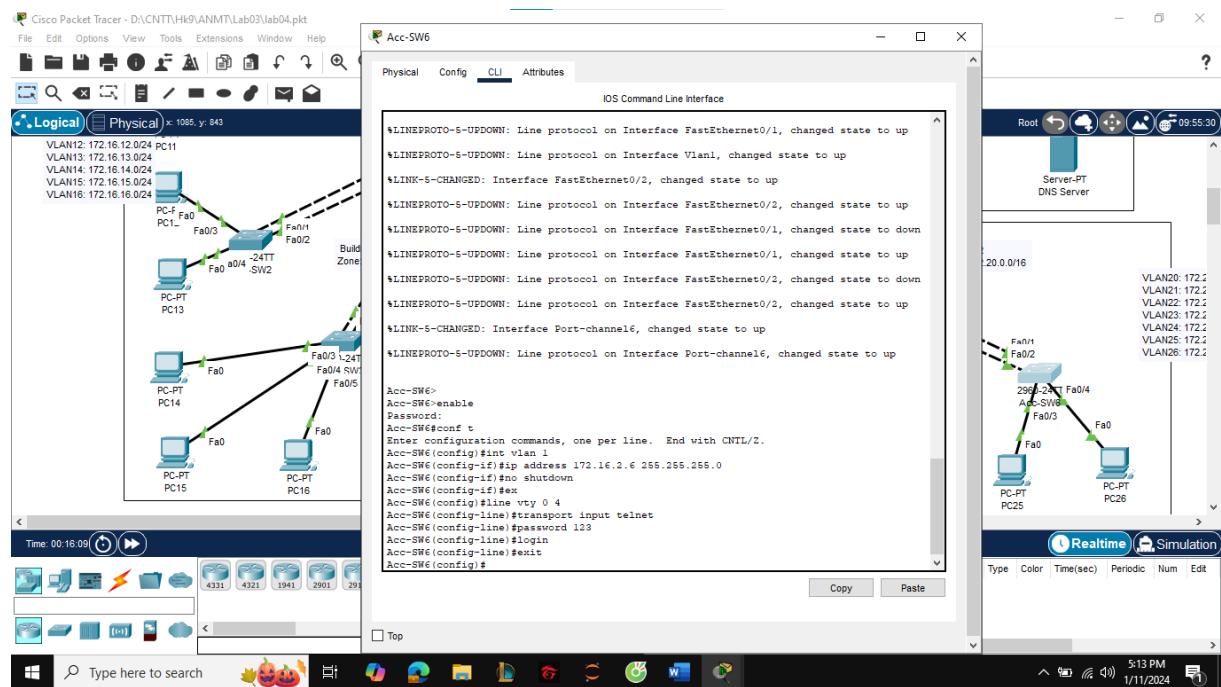
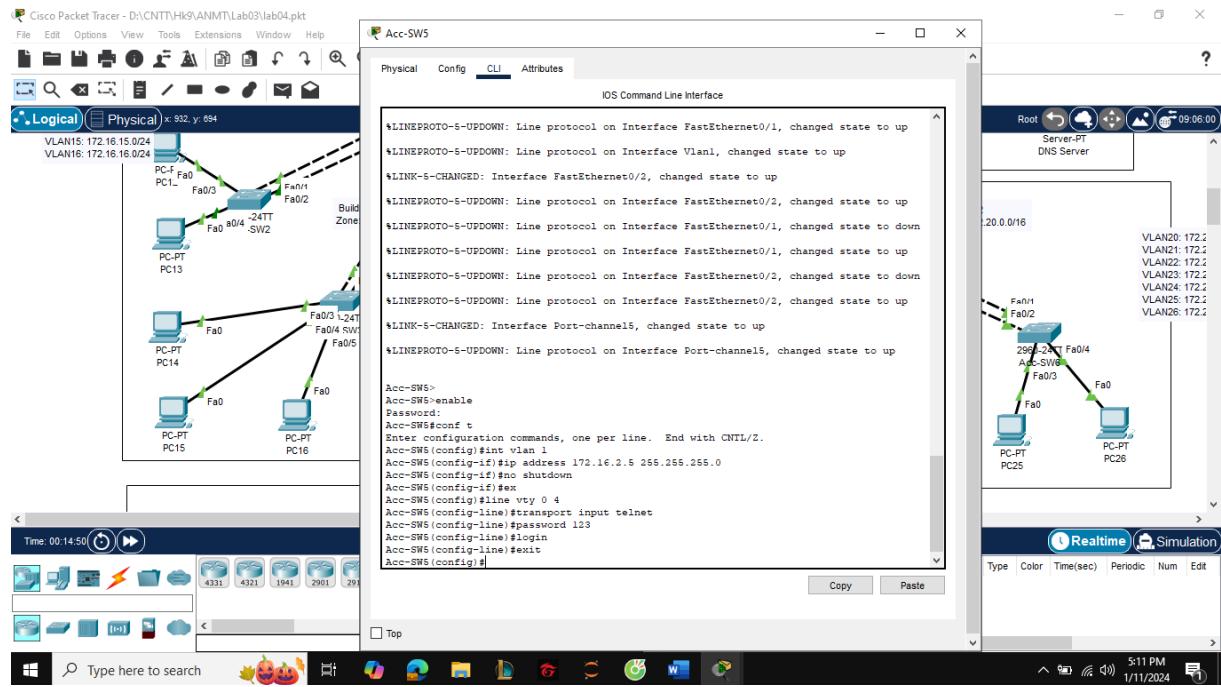
## 2. Mở line telnet trên tất cả các thiết bị mạng





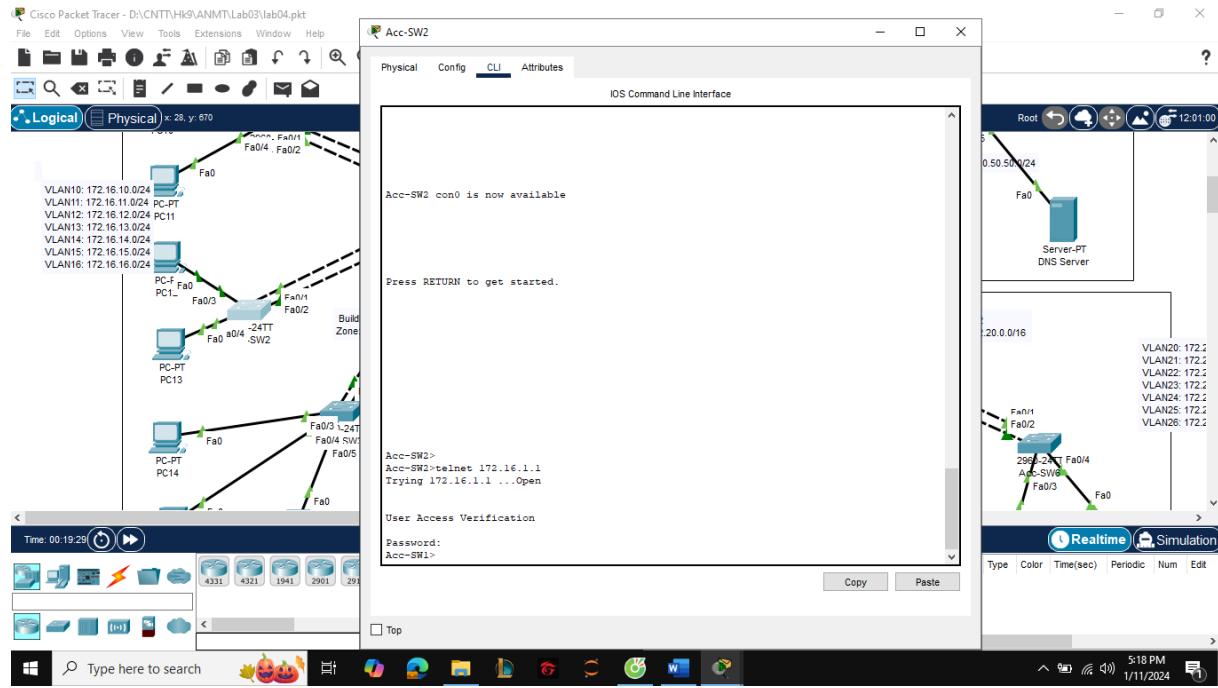




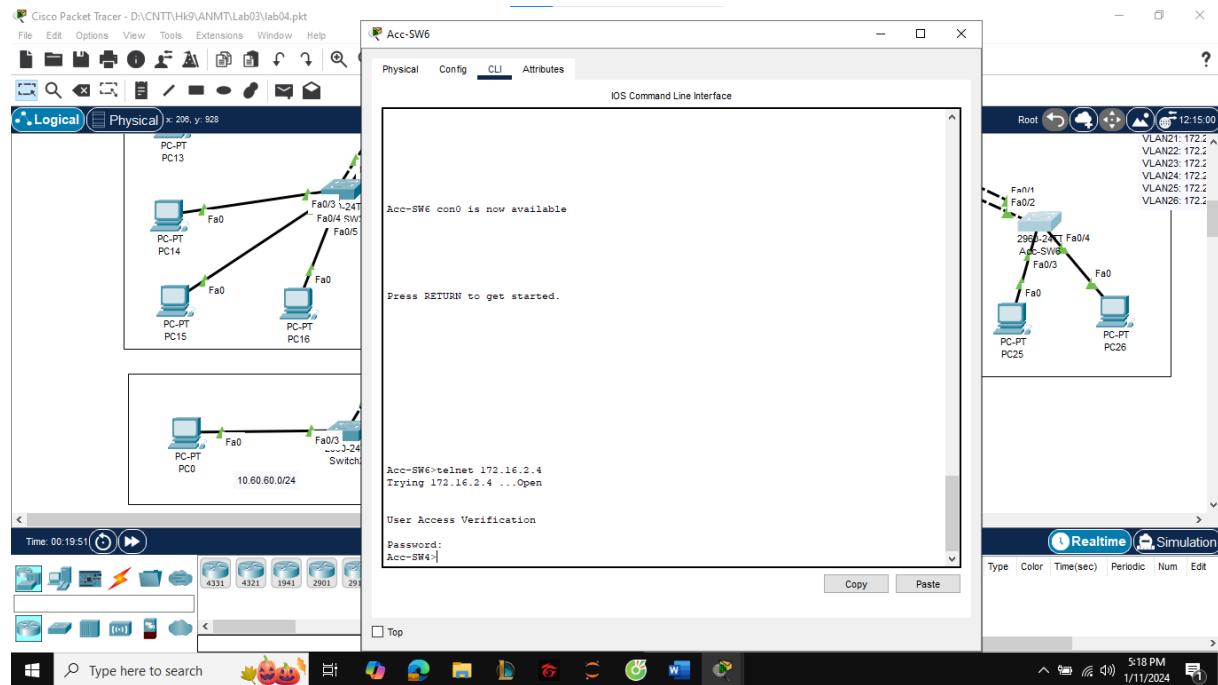


Kết quả:

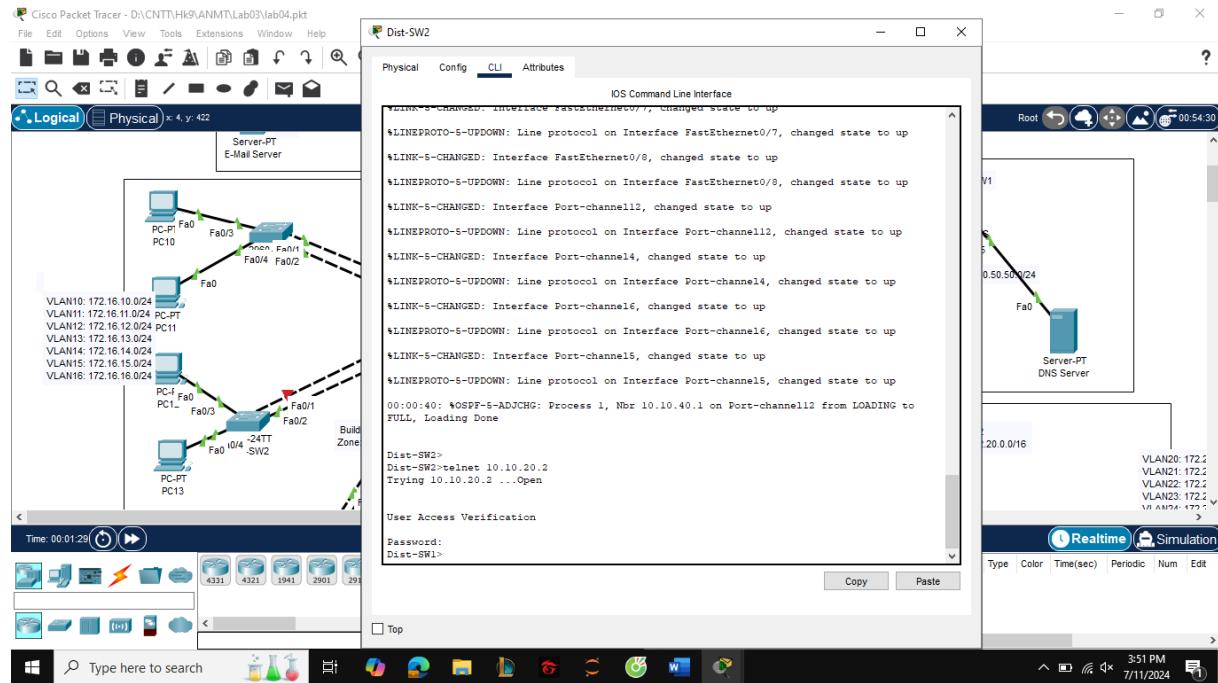
### Acc-SW2 kết nối từ xa qua telnet đến Acc-SW1



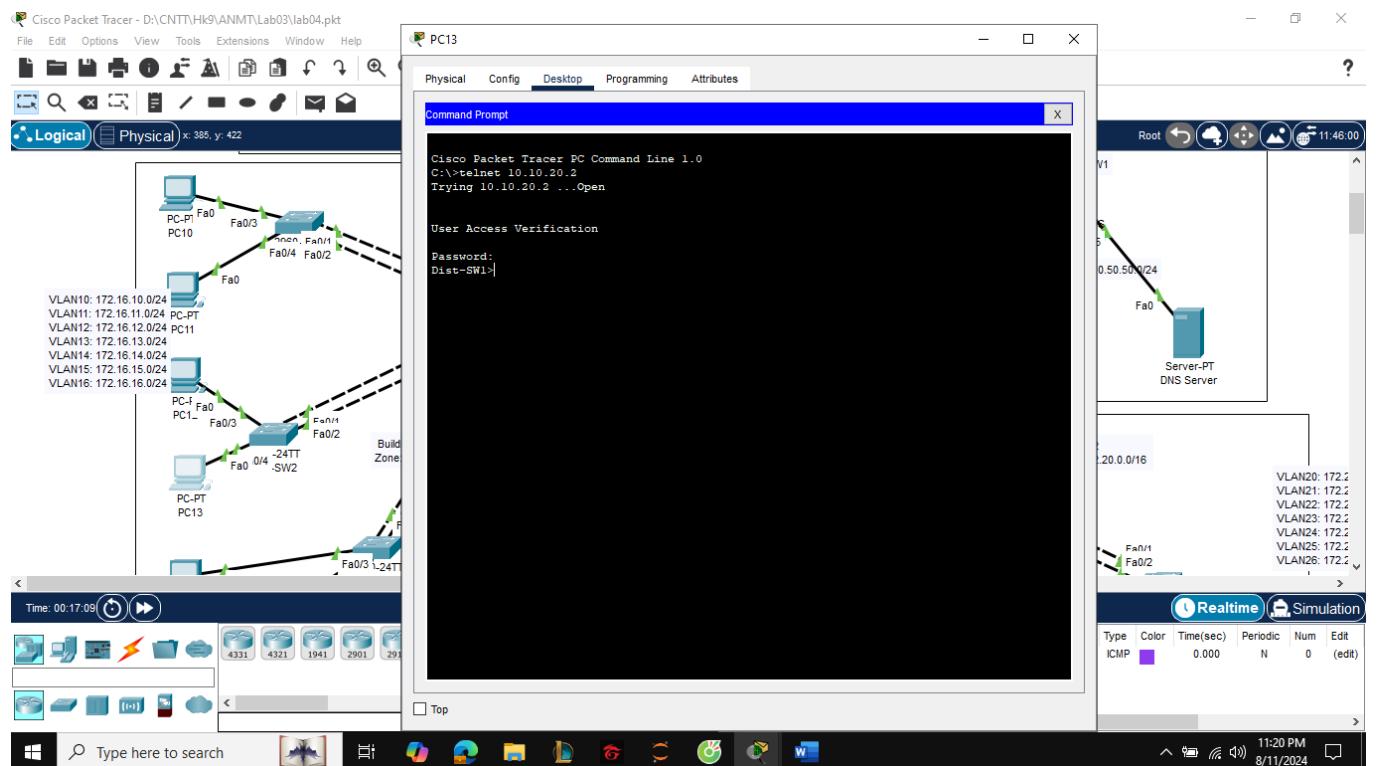
### Acc-SW6 kết nối từ xa qua telnet đến Acc-SW4

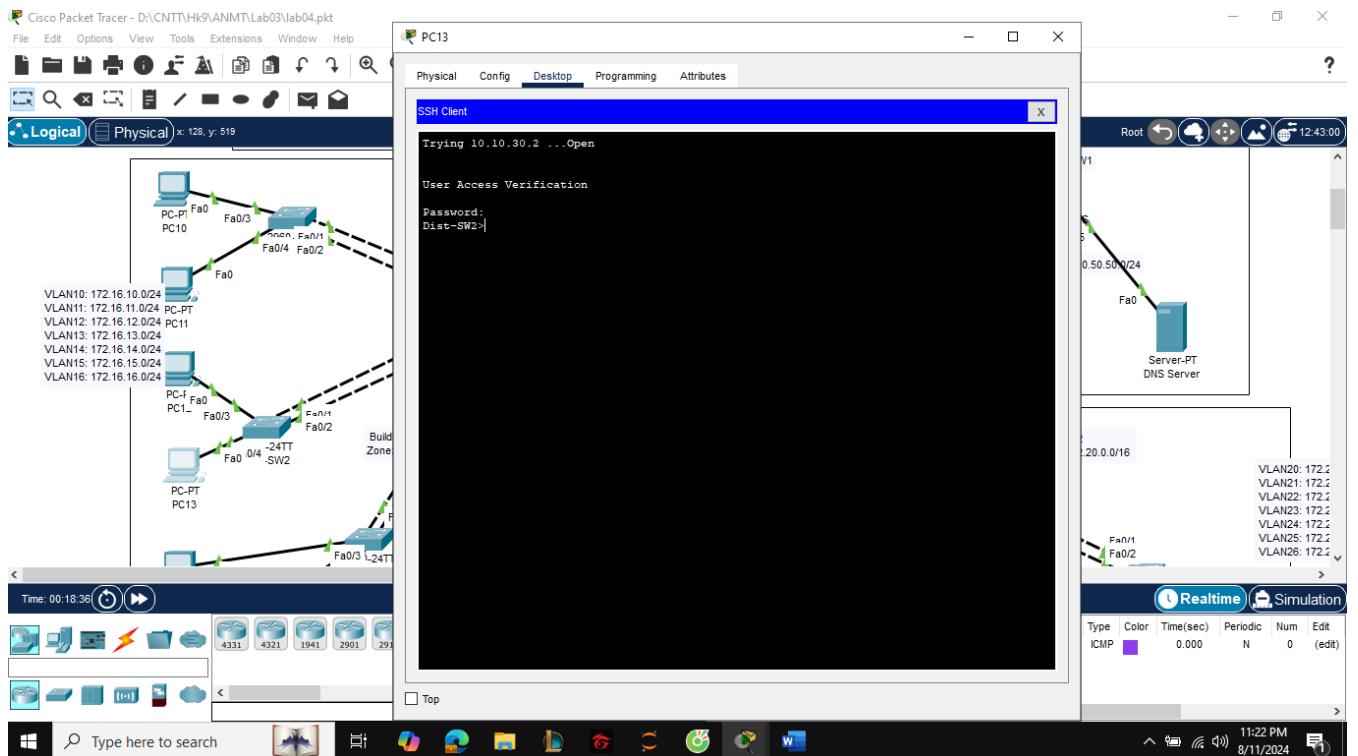
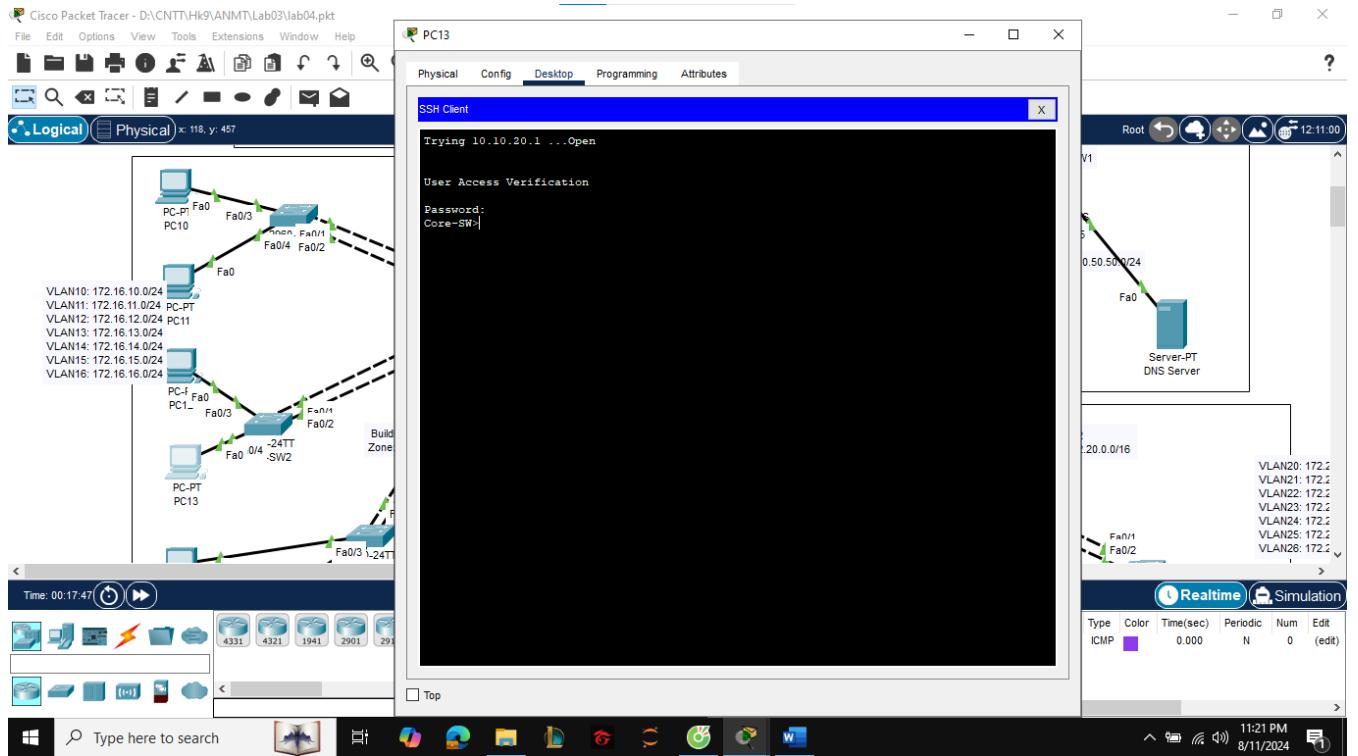


## Dist-SW2 kết nối từ xa qua telnet đến Dist-SW1



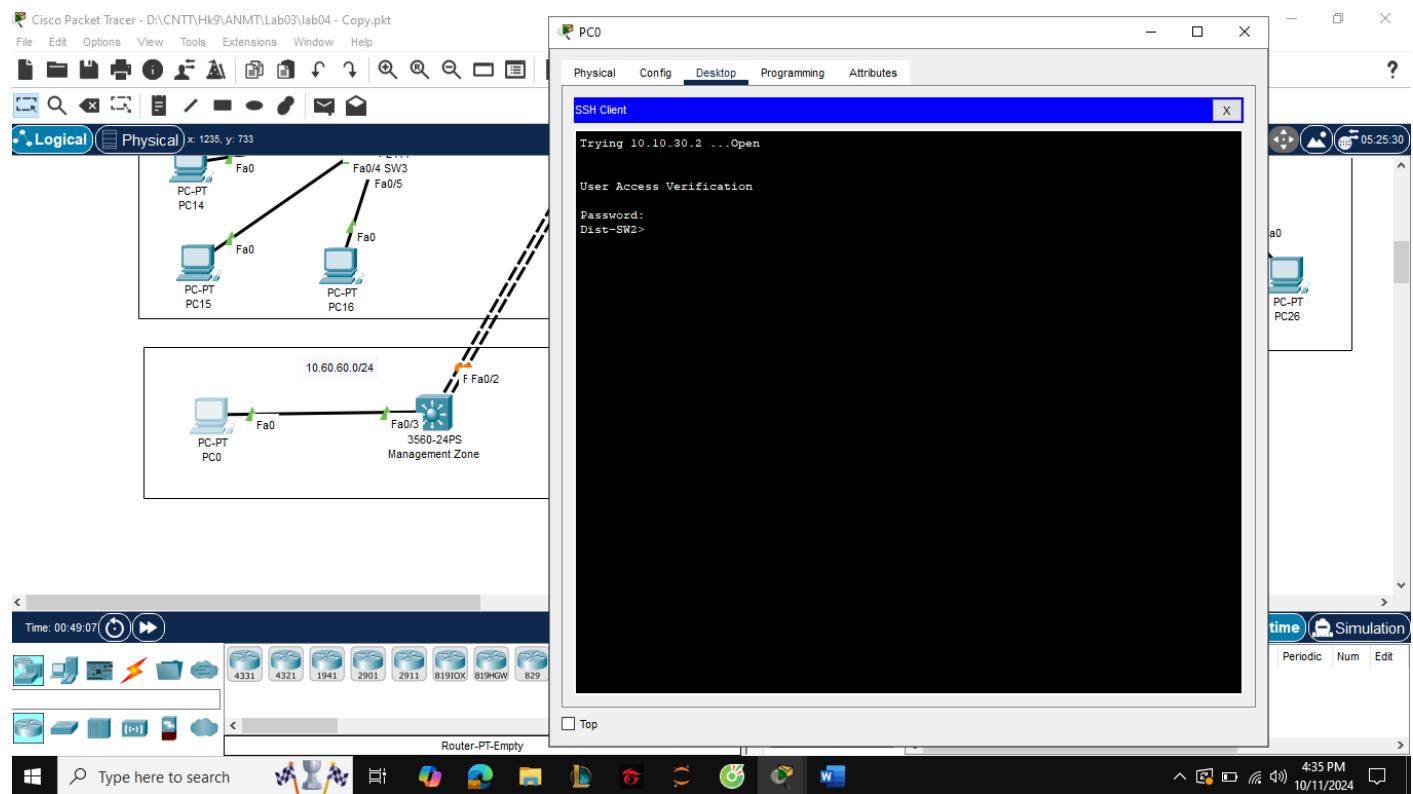
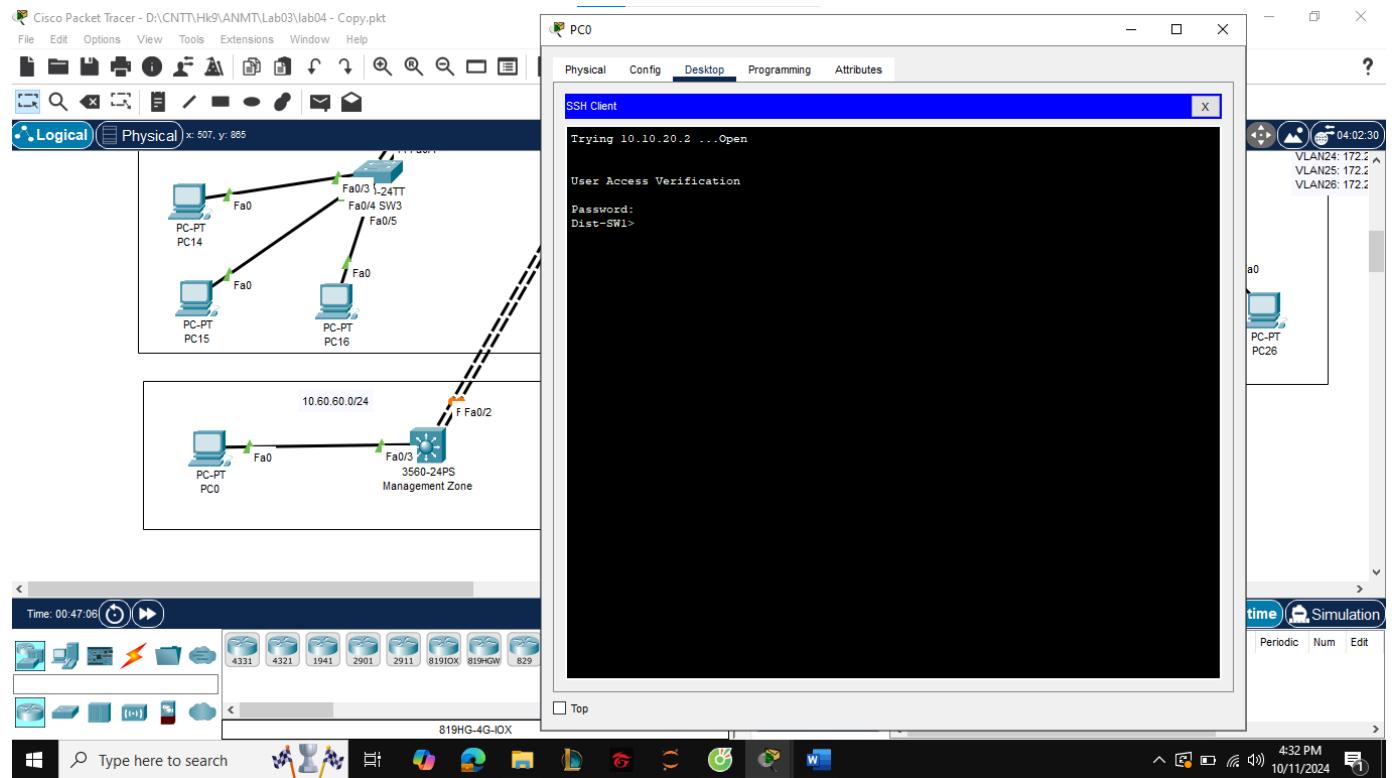
## PC13 kết nối từ xa qua telnet đến Dist-SW1, Core-SW, Dist-SW2





Tương tự các PC khác cũng thực hiện như PC13 để kết nối từ xa qua telnet đến các thiết bị mạng.

## PC thuộc khu vực Management Zone kết nối từ xa qua telnet đến các thiết bị mạng:



b) Cấu hình ACL:

- Cấm các PC thuộc VLAN 10 và VLAN 20 ping tới các server trong khu vực Internal Server

Các bước thực hiện:

Dist-SW1:

```
Dist-SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Dist-SW1(config)#ip access-list extended BLOCK_VLAN10
Dist-SW1(config-ext-nacl)#deny icmp 172.16.10.0 0.0.0.255 10.50.50.0 0.0.0.255
Dist-SW1(config-ext-nacl)#permit ip any any
Dist-SW1(config-ext-nacl)#exit
Dist-SW1(config)#interface vlan 10
Dist-SW1(config-if)#ip access-group BLOCK_VLAN10 in
Dist-SW1(config-if)#ex
```

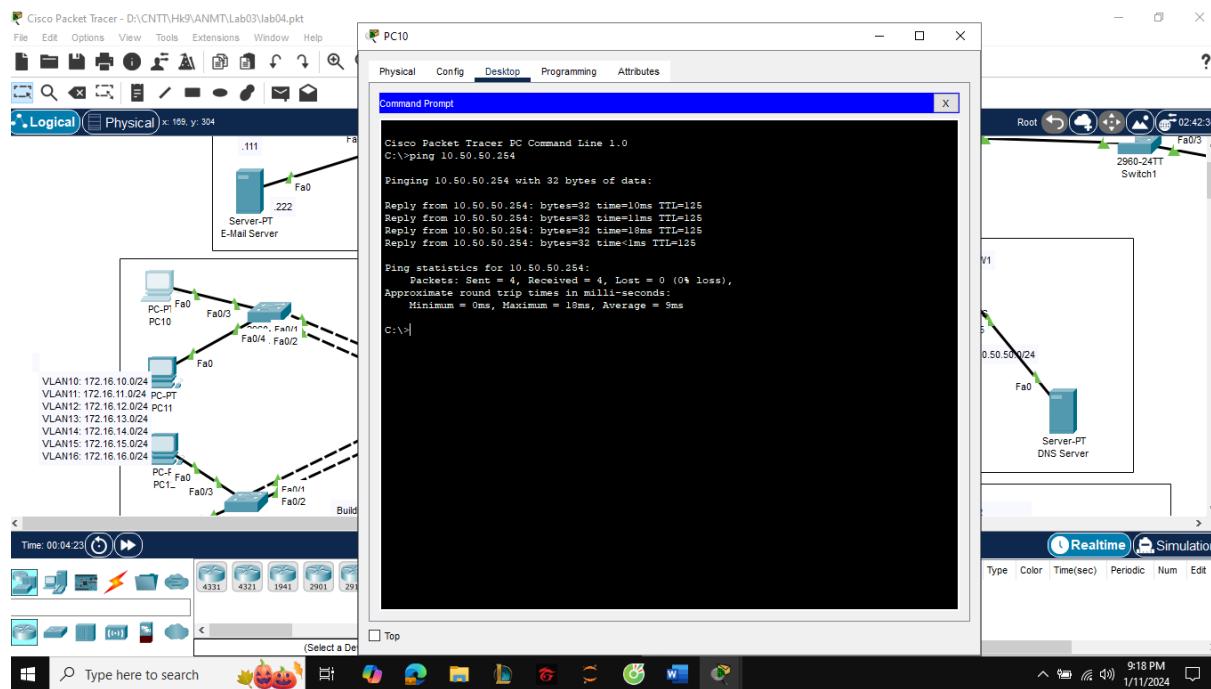
Dist-SW2:

```
Dist-SW2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Dist-SW2(config)#ip access-list extended BLOCK_VLAN20
Dist-SW2(config-ext-nacl)#deny icmp 172.20.20.0 0.0.0.255 10.50.50.0 0.0.0.255
Dist-SW2(config-ext-nacl)#permit ip any any
Dist-SW2(config-ext-nacl)#exit
Dist-SW2(config)#interface vlan 20
Dist-SW2(config-if)#ip access-group BLOCK_VLAN20 in
Dist-SW2(config-if)#exit
```

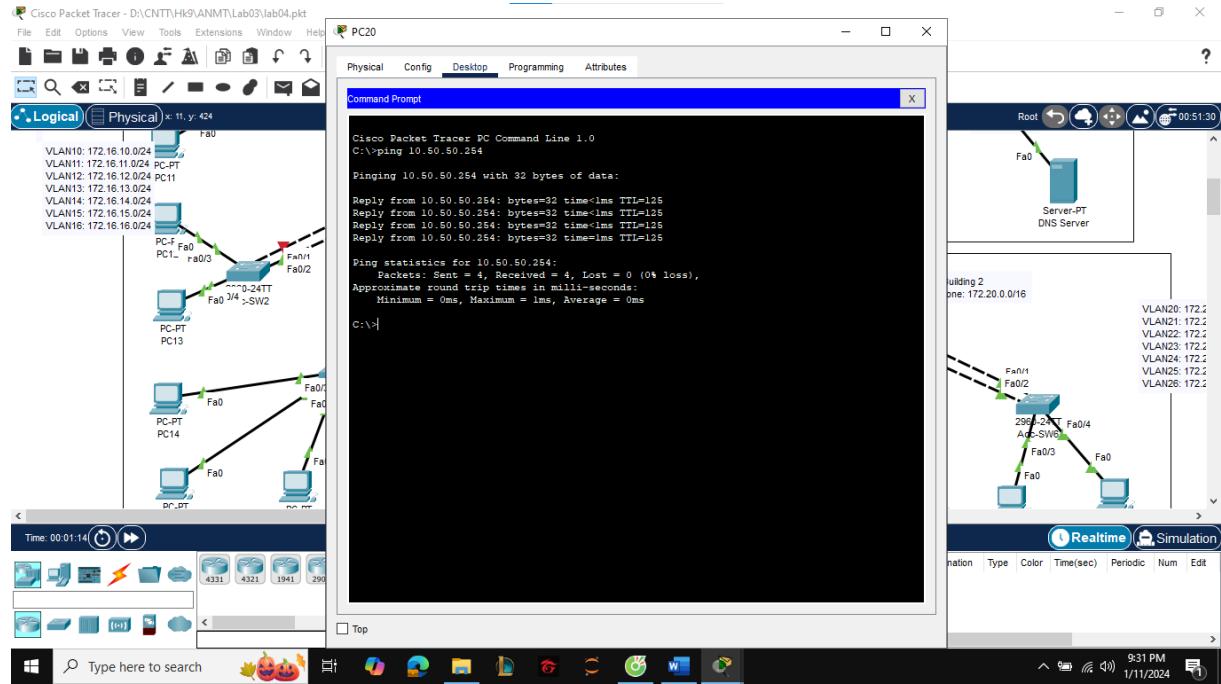
Kết quả:

Trước khi cấu hình ACL:

PC thuộc VLAN10:

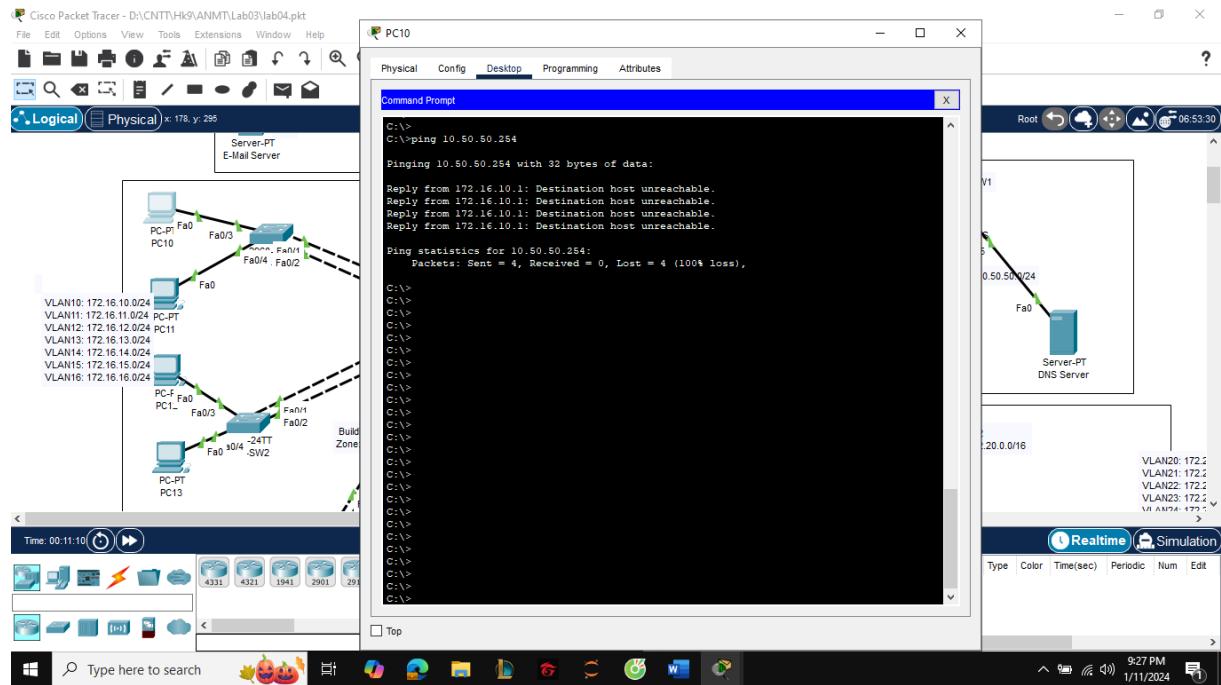


## PC thuộc VLAN20:

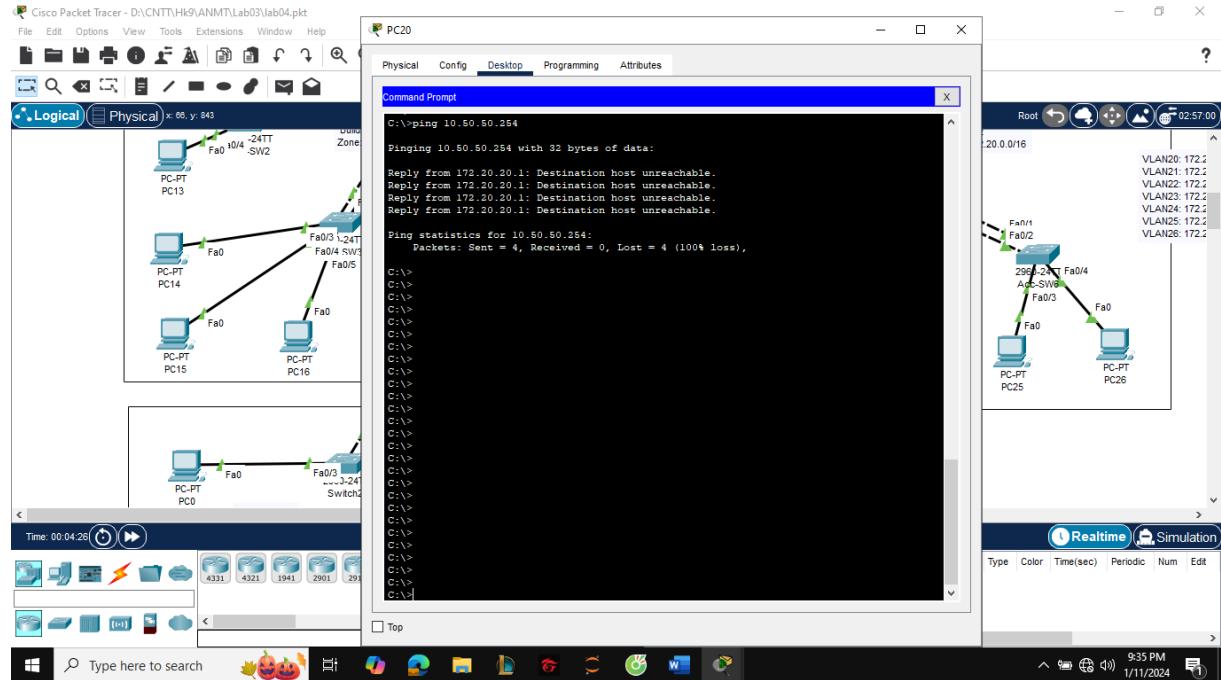


## Sau khi cấu hình ACL:

### PC thuộc VLAN10:



## PC thuộc VLAN20:



- Chỉ cho phép các PC trong khu vực quản trị được phép quản trị từ xa các thiết bị mạng (CoreSW, Dist-SW1, Dist-SW2, Access-SW1 → Access-SW6)

### Các bước thực hiện:

Cấu hình ACL trên các thiết bị mạng sau đó áp dụng vào line vty mở ở câu a:

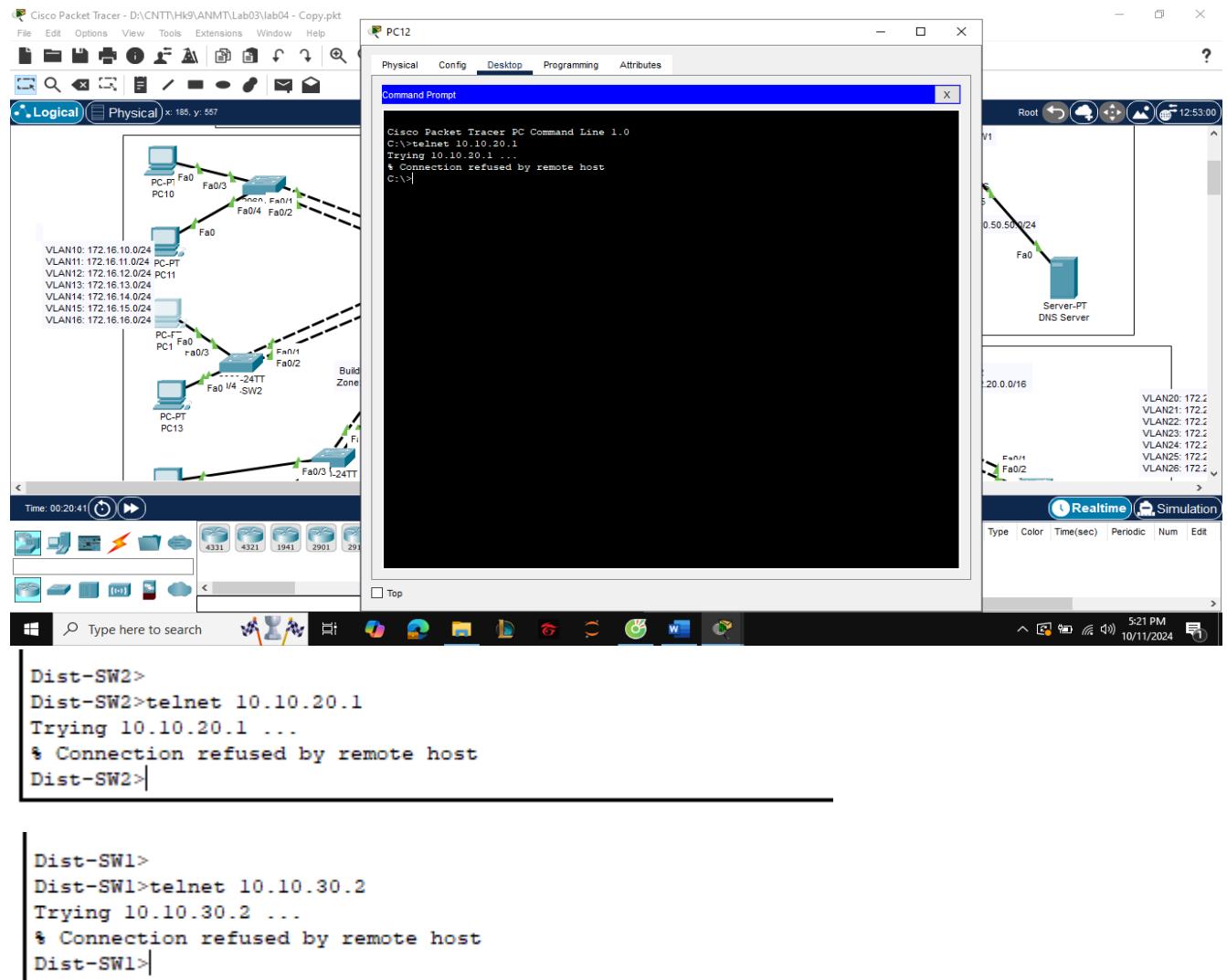
```
Core-SW#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Core-SW(config)#access-list 1 permit 10.60.60.0 0.0.0.255
Core-SW(config)#access-list 1 deny any
Core-SW(config)#line vty 0 4
Core-SW(config-line)#access-class 1 in
Core-SW(config-line)#end
```

```
Dist-SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Dist-SW1(config)#access-list 1 permit 10.60.60.0 0.0.0.255
Dist-SW1(config)#access-list 1 deny any
Dist-SW1(config)#line vty 0 4
Dist-SW1(config-line)#access-class 1 in
Dist-SW1(config-line)#end
```

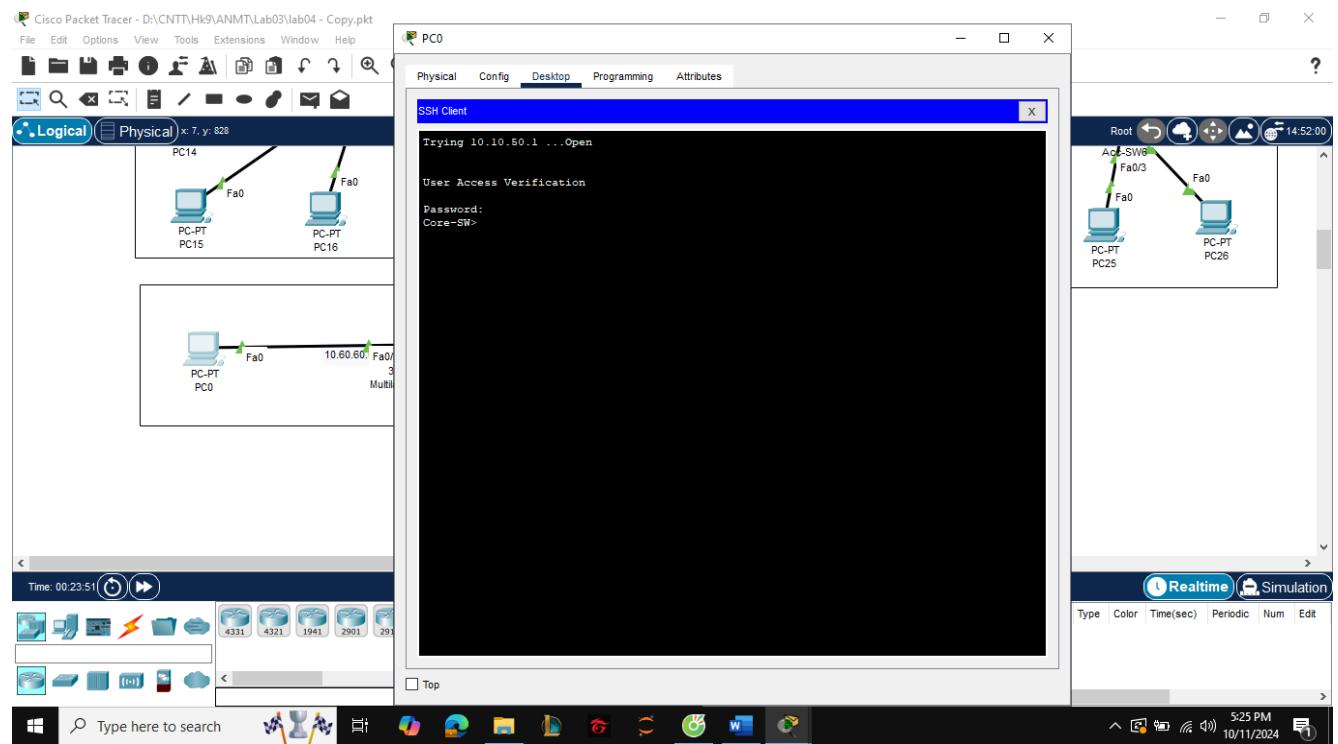
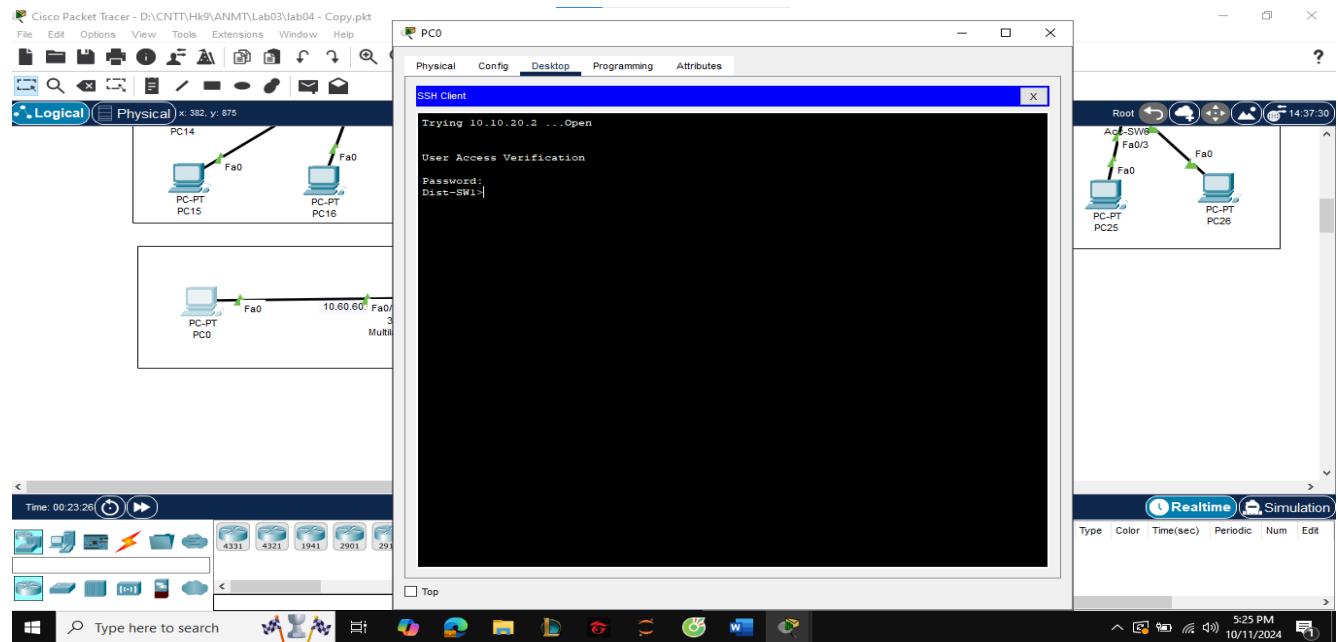
Tương tự cấu hình ACL như trên với các thiết bị mạng còn lại

## Kết quả sau khi cấu hình ACL trên:

Các PC hay thiết bị mạng không thuộc khu vực Management Zone thì sẽ không kết nối từ xa qua telnet được



## PC thuộc khu vực Management Zone :



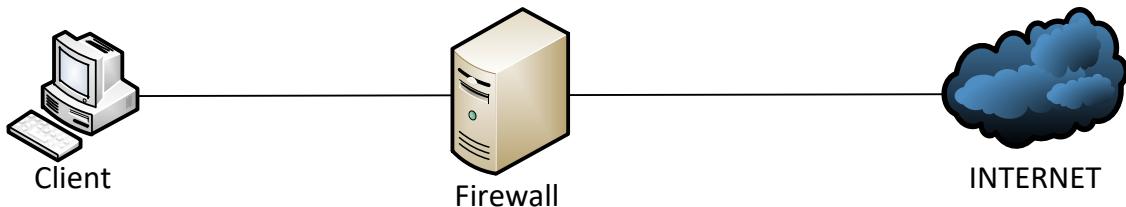
#### 4. Firewall (2,0 điểm)

##### c) ASA

a. Firewall rule: inside → outside

d) Sinh viên tự chọn một Firewall dạng VMWare để thử nghiệm (Fortigate, Checkpoint,...)

Topology



Thực hiện các rule:

- Cho phép các PC bên trong mạng nội bộ ra ngoài Internet
- Kiểm soát truy cập Web
- Kiểm soát port truy cập
- Kiểm soát ứng dụng truy cập
- Thực hiện các phương thức khác

SV có thể sử dụng các FW dạng VMWare: Fortigate, Checkpoint,...

Các bước thực hiện:

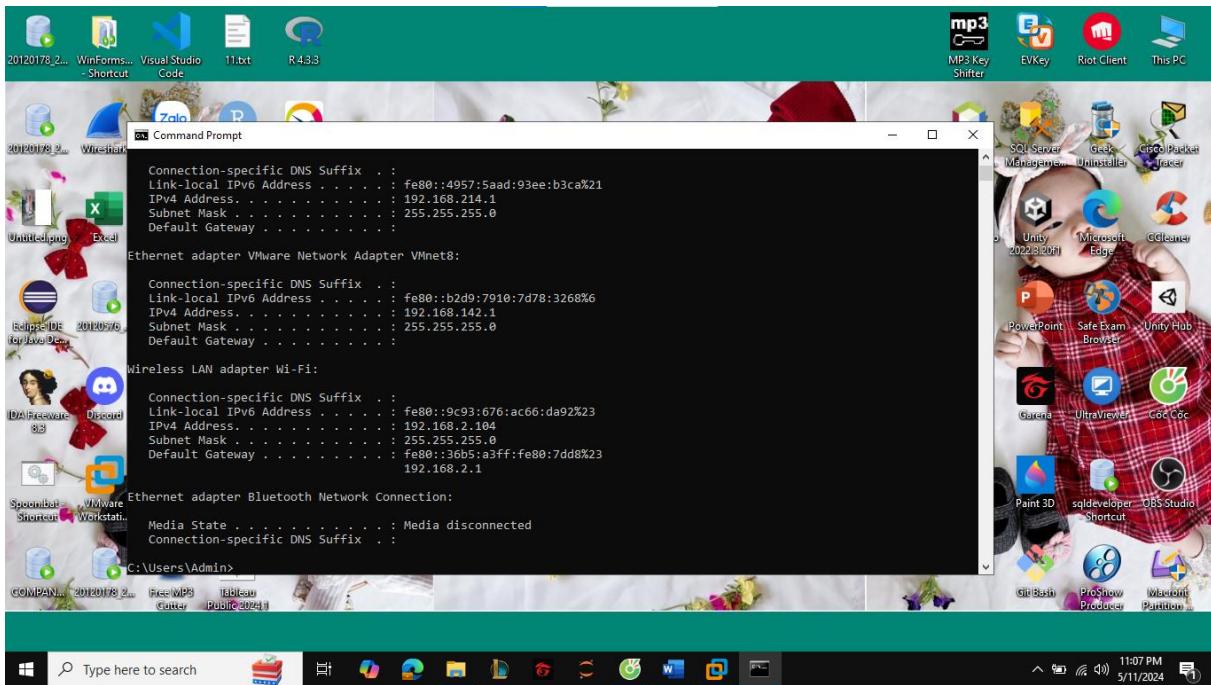
Cấu hình Fortigate:

```
Serial number is FGUMEEUJ0IUUSLDF
FGUMEEUJ0IUUSLDF login: admin
Password:
Welcome!

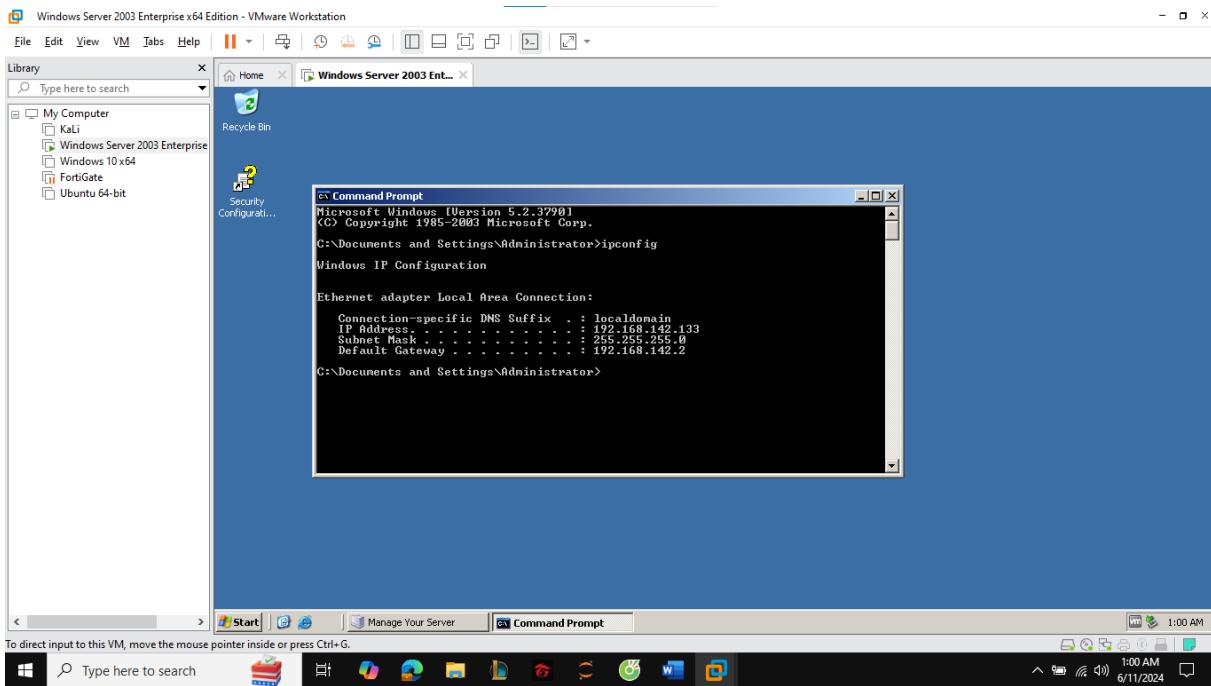
FGUMEEUJ0IUUSLDF # system config interface
Unknown action 0

FGUMEEUJ0IUUSLDF # config system interface
FGUMEEUJ0IUUSLDF (interface) # edit port1
FGUMEEUJ0IUUSLDF (port1) # show
config system interface
edit "port1"
    set vdom "root"
    set ip 192.168.2.200 255.255.255.0
    set allowaccess ping https ssh http
    set type physical
    set snmp-index 1
next
end
FGUMEEUJ0IUUSLDF (port1) # _
```

## Internet

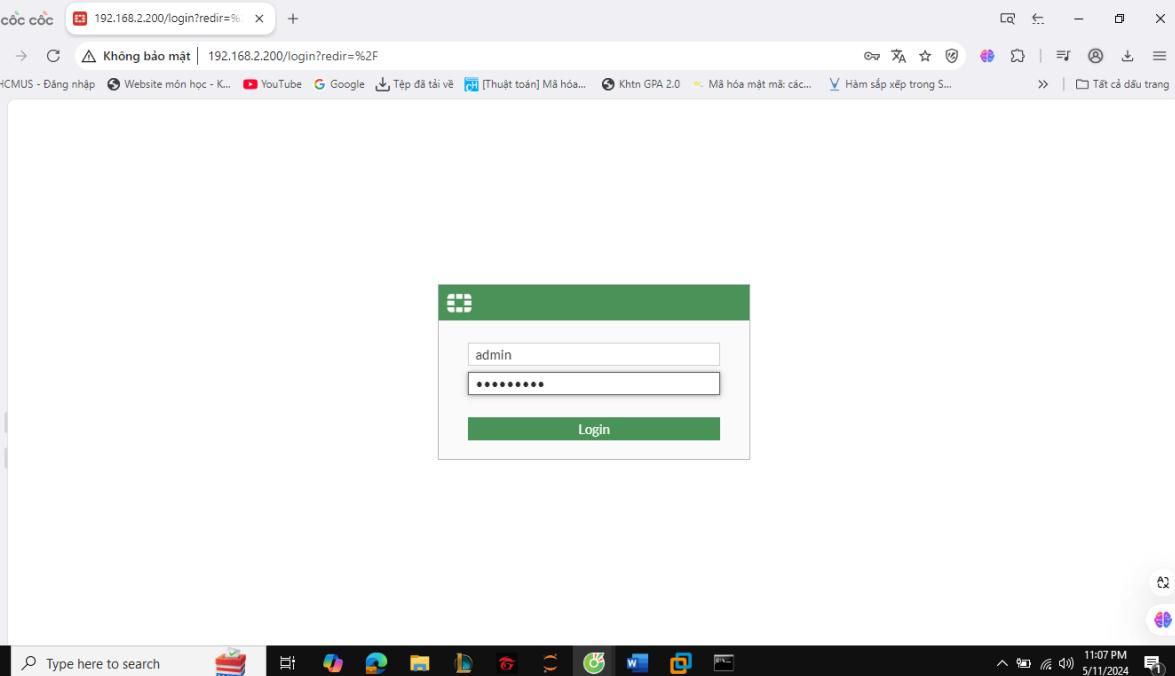


## Máy client



## Đầu tiên cấu hình Network:

### B1: Đăng nhập fortigate trên máy internet

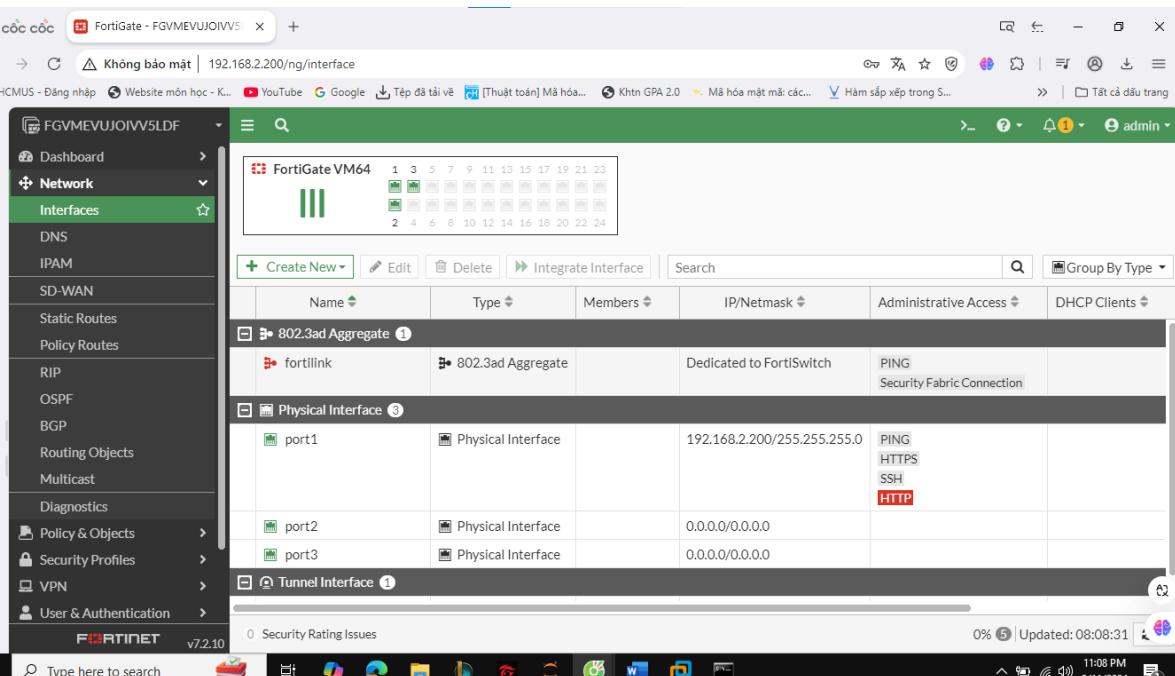


192.168.2.200/login?redir=%2F

admin

\*\*\*\*\*

Login

FortiGate VM64

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients
fortilink	802.3ad Aggregate			PING Security Fabric Connection	
port1	Physical Interface		192.168.2.200/255.255.255.0	PING HTTPS SSH HTTP	
port2	Physical Interface		0.0.0.0/0.0.0.0		
port3	Physical Interface		0.0.0.0/0.0.0.0		

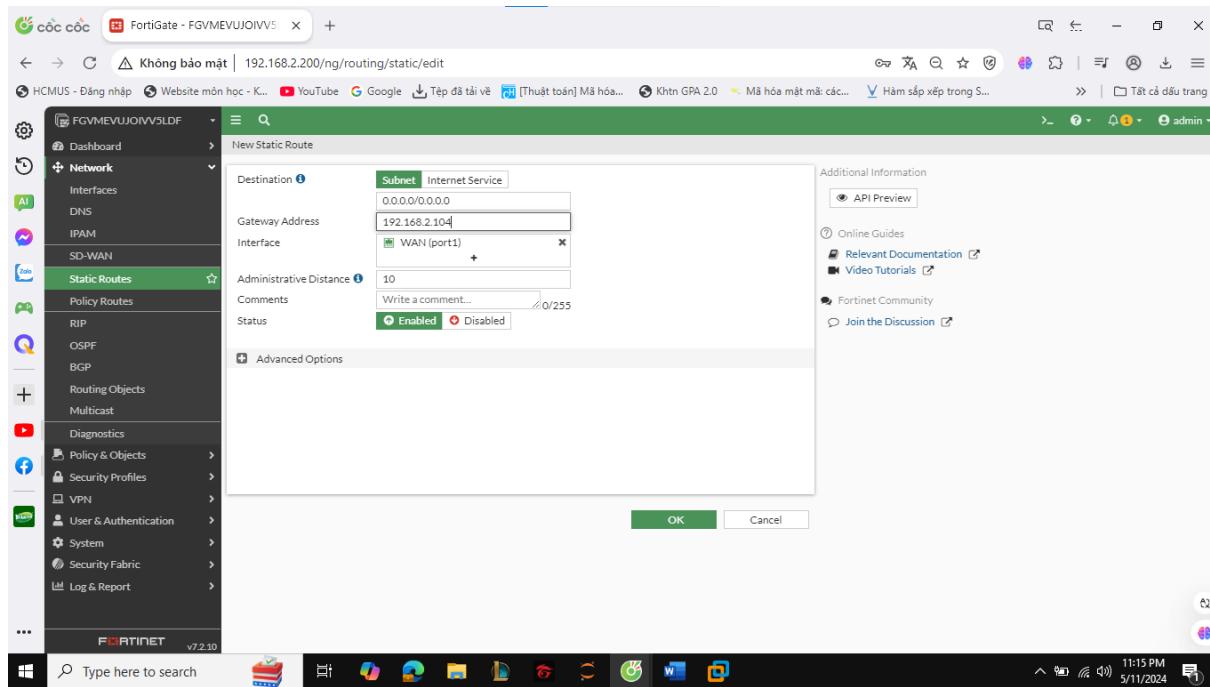
## B2: Edit port1 như bên dưới. Rồi nhấn OK

The screenshot shows the 'Edit Interface' page for 'port1'. The 'Name' field is set to 'port1' and 'Alias' to 'WAN'. The 'Type' is 'Physical Interface'. 'VRF ID' is set to 0 and 'Role' to 'WAN'. Under 'Address', 'Addressing mode' is 'Manual' with IP/Netmask '192.168.2.200/255.255.255.0'. In the 'Administrative Access' section, 'IPv4' checkboxes include HTTPS, PING, SSH, and RADIUS Accounting. Below this, 'Receive LLDP' and 'Transmit LLDP' options are shown. On the right side of the interface, there's a summary of the FortiGate status: 'Status Up', 'MAC address 00:0c:29:dc:9c:e2', and a 'Speed Test' button.

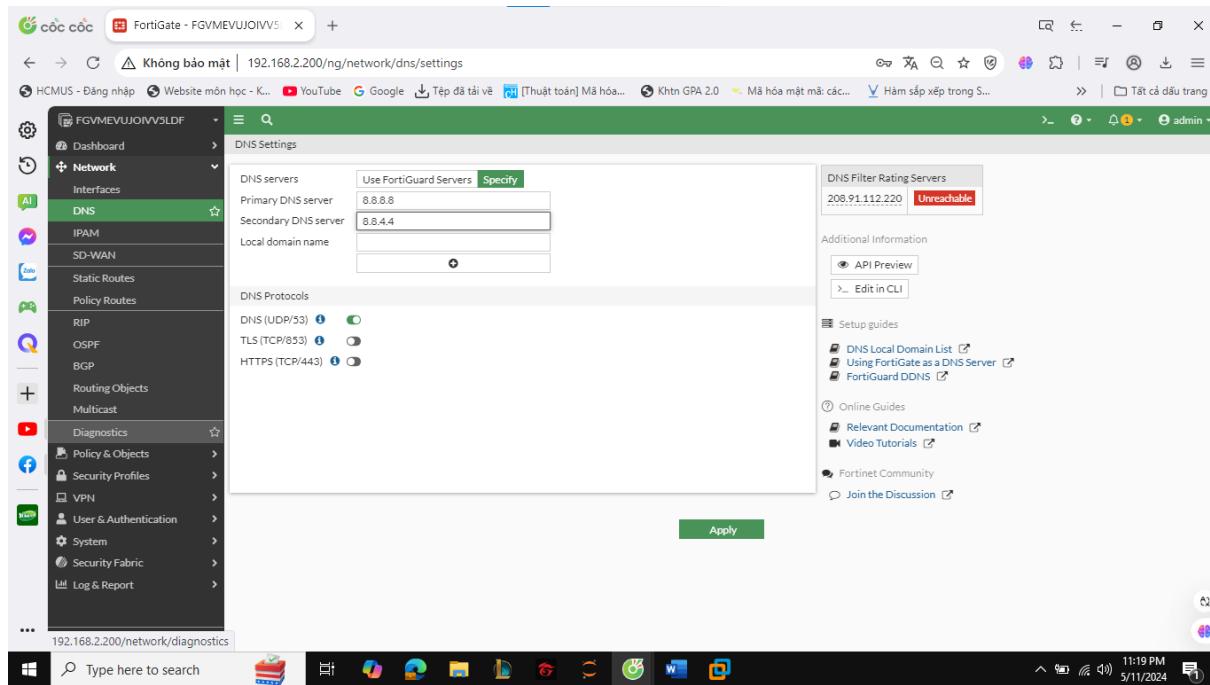
## B3: Edit port2 như dưới . Rồi nhấn OK

The screenshot shows the 'Edit Interface' page for 'port2'. The 'Name' field is set to 'LAN (port2)' and 'Alias' to 'LAN'. The 'Type' is 'Physical Interface'. 'VRF ID' is set to 0 and 'Role' to 'LAN'. Under 'Address', 'Addressing mode' is 'Manual' with IP/Netmask '192.168.142.1/255.255.255.0'. In the 'Administrative Access' section, 'IPv4' checkboxes include PING, SSH, and RADIUS Accounting. Below this, 'Receive LLDP' and 'Transmit LLDP' options are shown. On the right side of the interface, there's a summary of the FortiGate status: 'Status Up', 'MAC address 00:0c:29:dc:9c:e2', and a 'Speed Test' button.

#### B4: Cấu hình Static Routes như dưới . Rồi nhấn OK



#### B5: Cấu hình DNS. Rồi nhấn Apply



## Thực hiện các rule:

- Cho phép các PC bên trong mạng nội bộ ra ngoài Internet

### B1: Chọn Firewall Policy. Rồi nhấn chọn Create New

The screenshot shows the FortiGate management interface with the title bar "cốc cốc FortiGate - FGVMEMUJOIVV5LDF". The left sidebar menu is expanded, showing "Policy & Objects" selected, and "Firewall Policy" is highlighted. The main content area displays a table titled "Firewall Policy" with one row labeled "Implicit". The table columns include Name, Source, Destination, Schedule, Service, Action, NAT, Security Profiles, Log, Bytes, and Type. At the top of the table, there are buttons for "+ Create New", "Edit", "Edit in CLI", "Delete", "Policy lookup", "Search", "Export", "Interface Pair View", and "By Sequence". The status bar at the bottom right shows "Updated: 08:23:39", "11:23 PM", and "5/11/2024".

### B2: Điền và chọn các thông tin như bên dưới. Rồi nhấn OK

The screenshot shows the FortiGate management interface with the title bar "cốc cốc FortiGate - FGVMEMUJOIVV5LDF". The left sidebar menu is expanded, showing "Policy & Objects" selected, and "Firewall Policy" is highlighted. The main content area shows a "New Policy" dialog box. In the "Name" field, "Allow Lan to Internet" is entered. Under "Incoming Interface", "LAN (port2)" is selected. Under "Outgoing Interface", "WAN (port1)" is selected. The "Source" and "Destination" fields both have "all" selected. Under "Schedule", "always" is selected. Under "Service", "ALL" is selected. The "Action" button has "ACCEPT" checked. On the right side of the dialog, there is an "Additional Information" panel with sections for "API Preview", "Online Guides" (including "Relevant Documentation", "Video Tutorials", and "Consolidated Policy Configuration"), and "Fortinet Community" (with a "Join the Discussion" link). At the bottom of the dialog are "OK" and "Cancel" buttons. The status bar at the bottom right shows "11:26 PM", "11:26 PM", and "5/11/2024".

- Kiểm soát truy cập Web

## B1: Tạo Web Filter Profile

New Web Filter Profile

URL	Type	Action	Status
facebook.com	Wildcard	Block	Enable

## B2: Tạo policy để kiểm soát truy cập Web. Bật Web Filter và chọn Web Filter Profile vừa tạo . Sau đó nhấn OK

Edit Policy

Outgoing Interface: WAN (port1)	Last used: 51 minute(s) ago
Source: all	First used: 54 minute(s) ago
Destination: all	Active sessions: 0
Schedule: always	Hit count: 2
Service: ALL	Total bytes: 720 B
Action: ACCEPT	Current bandwidth: 0 bps

- Kiểm soát port truy cập

Trong phần Service, chọn port mà bạn muốn kiểm soát. Sau đó nhấn OK

The screenshot shows the FortiGate interface under 'Policy & Objects' > 'Firewall Policy'. A policy named 'Allow Lan to Internet' is selected. In the 'Service' section, 'HTTP' is chosen from the dropdown. A 'Select Entries' dialog is open, showing a list of services including 'ALL', 'ALL\_ICMP', 'ALL\_TCP', 'ALL\_UDP', and 'HTTP'. To the right, a 'Statistics (since last reset)' table provides details like 'Last used' (1 hour ago), 'First used' (1 hour ago), and 'Hit count' (2). Below the table is a chart showing traffic over the last 7 days.

- Kiểm soát ứng dụng truy cập

## B1: Tạo Application Control Profile

Đặt tên cho profile

Trong profile, bạn có thể chọn các ứng dụng hoặc nhóm ứng dụng để **Allow** (cho phép), **Monitor** (giám sát), hoặc **Block** (chặn).

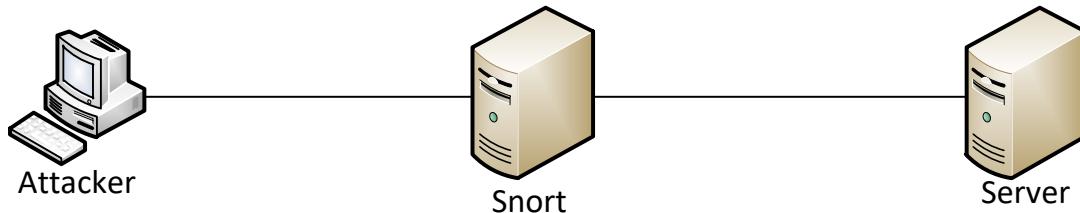
Sau đó nhấn OK

The screenshot shows the FortiGate interface under 'Policy & Objects' > 'Security Profiles'. A new profile is being created with the name 'Business'. The 'Categories' section lists various application categories like Business, Collaboration, Game, etc. On the right side, there are sections for 'Firmware & General Updates License' (Not Supported), 'Application Control Signatures Package' (Version 6.00741), 'Application Signatures' (View Application Signatures), and 'Additional Information' (API Preview, Online Guides, Relevant Documentation, Video Tutorials, Fortinet Community, Join the Discussion).

B2: Tạo policy để kiểm soát ứng dụng truy cập. Bật Application Control và chọn Application Control Profile vừa tạo. Sau đó nhấn OK

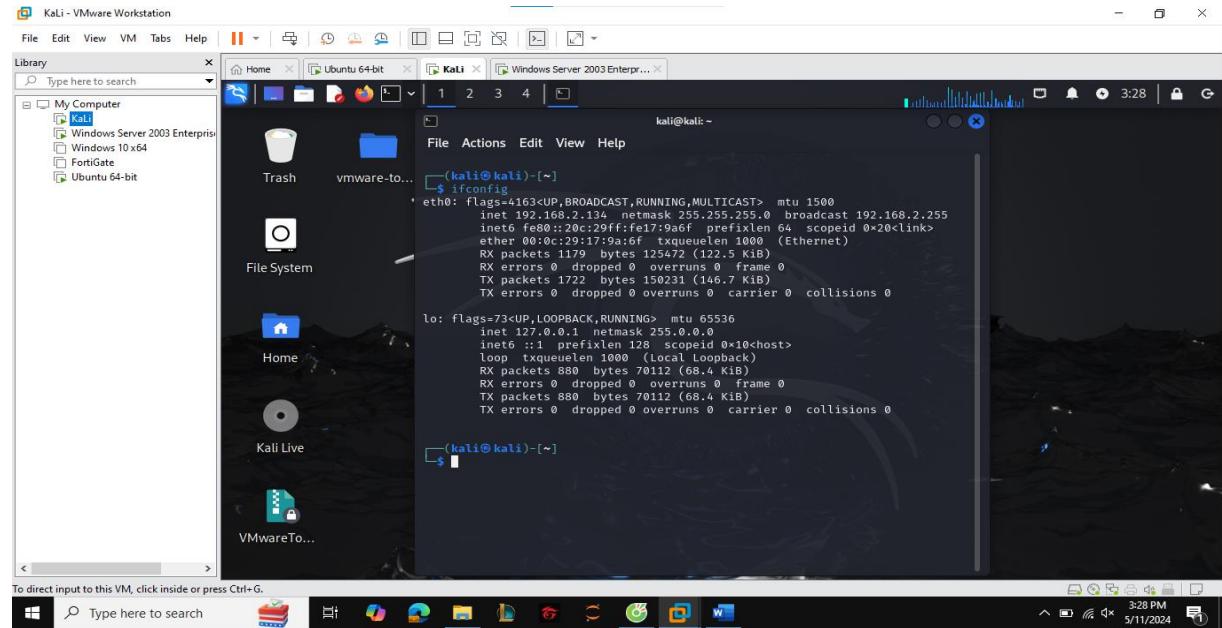
The screenshot shows the FortiGate management interface for editing a firewall policy. The left sidebar is titled 'Policy & Objects' and lists various security profiles like AntiVirus, Web Filter, DNS Filter, and Application Control. Under Application Control, a profile named 'block-high-risk' is selected. The main panel displays traffic statistics for the last 7 days, including bytes transferred by SPU, Software, and Hardware. Below the stats is an 'Additional Information' section with links to API Preview, Edit in CLI, Online Guides, Relevant Documentation, Video Tutorials, and Join the Discussion.

## 5. Snort-IDS (2,0 điểm)

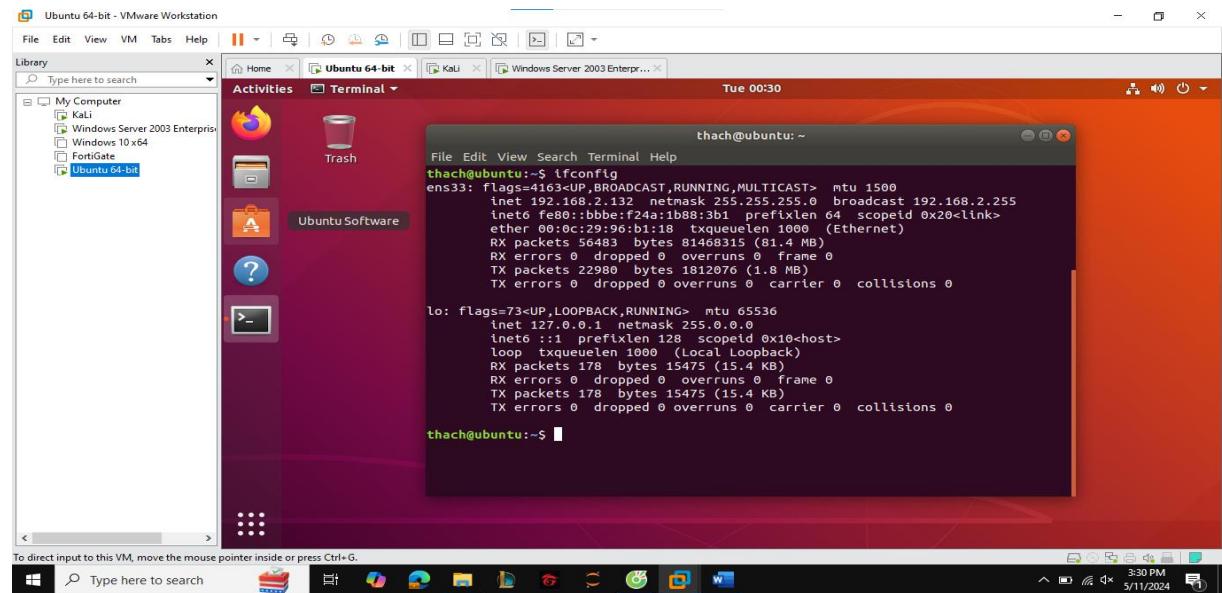


- Cài đặt Snort
- Dùng một số công cụ tấn công và mô tả kết quả xử lý trên Snort

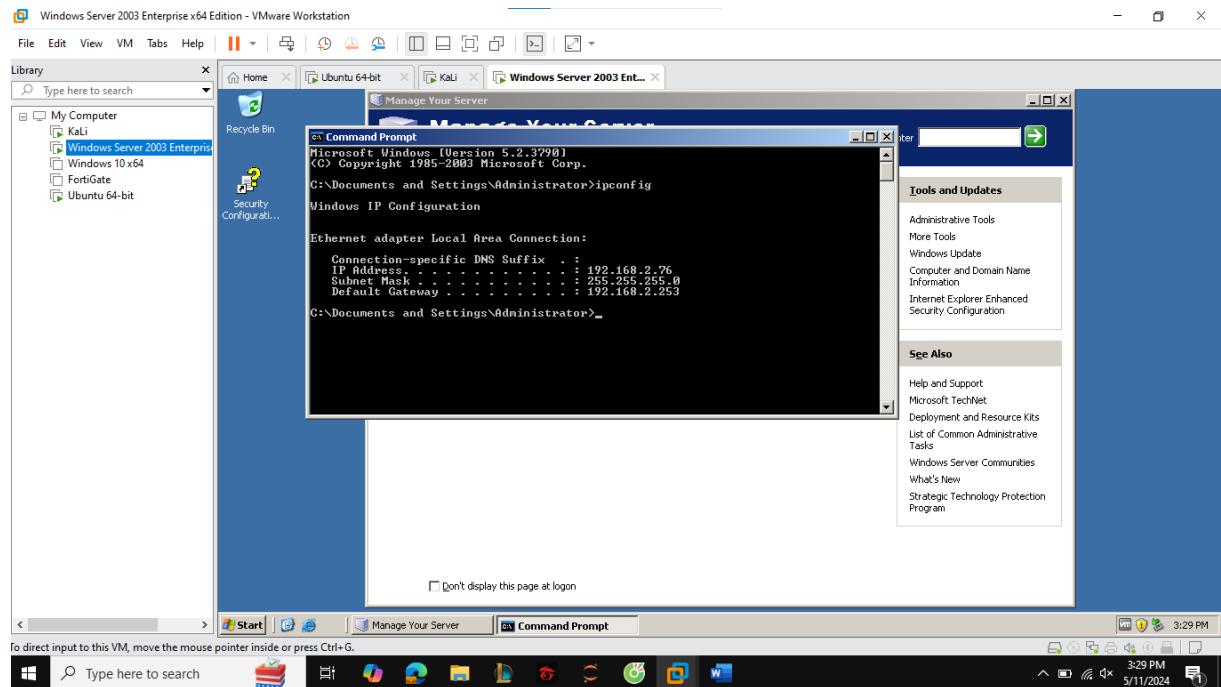
## Máy Attack ( Hệ điều hành Kali-linux)



## Snort ( Hệ điều hành Ubuntu)



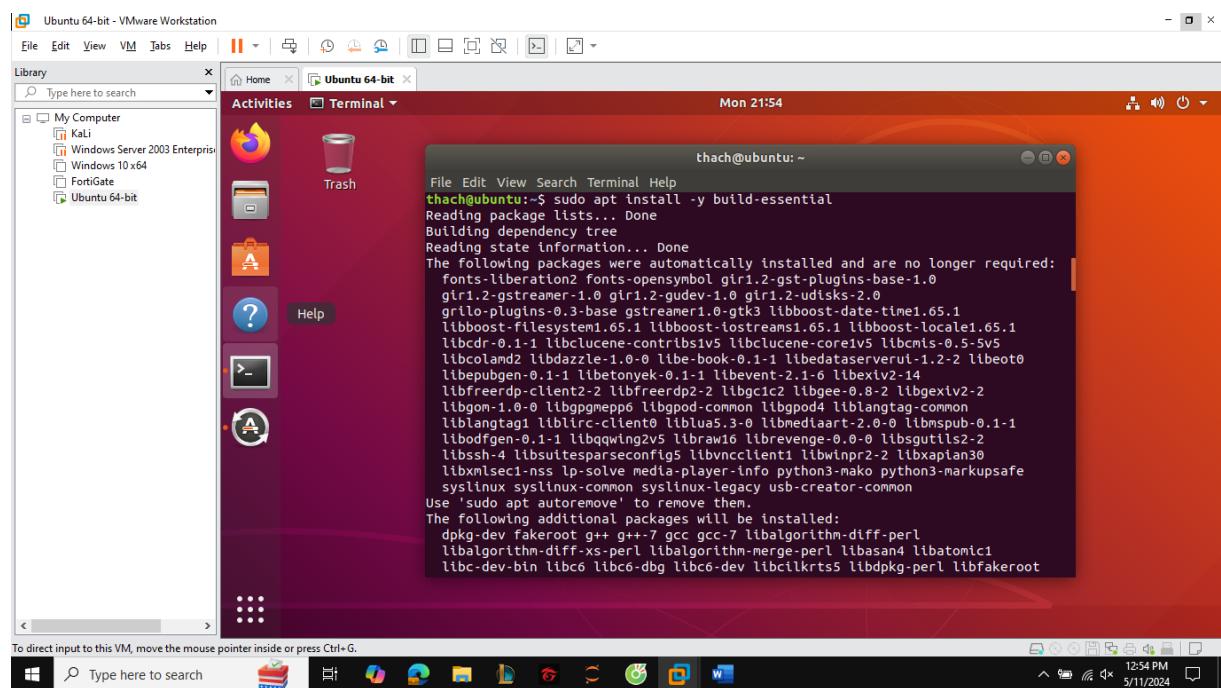
## Server ( Hệ điều hành Window Server 2003)



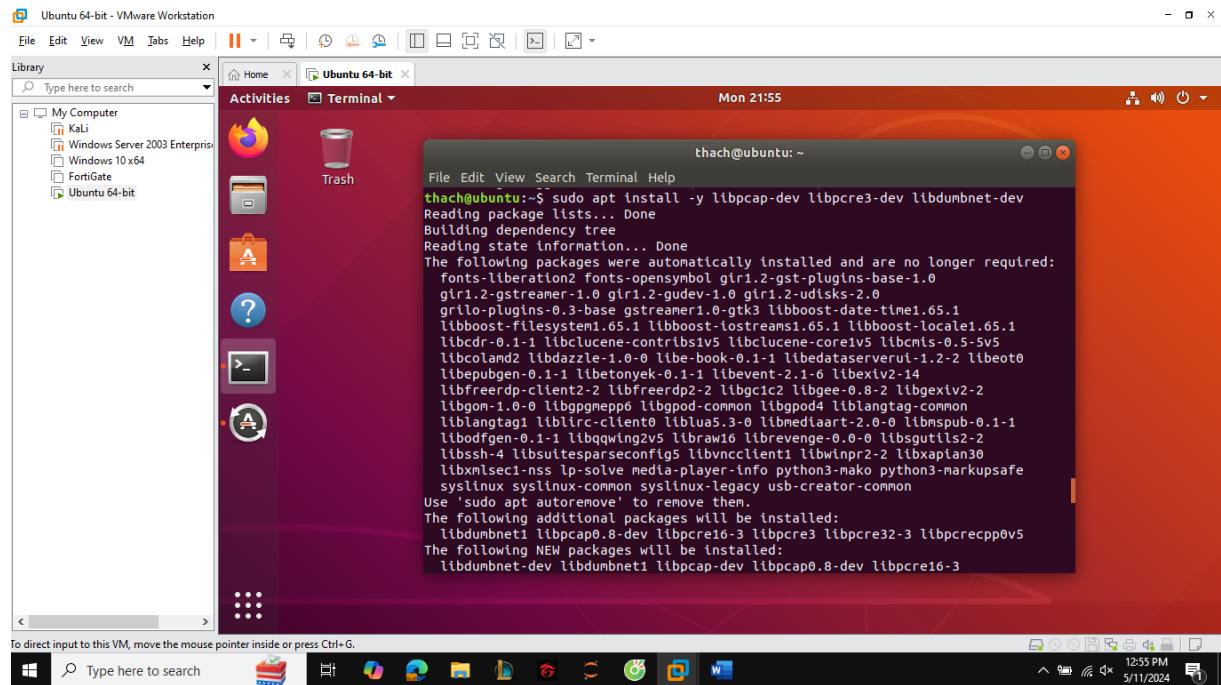
### 1. Cài đặt Snort:

#### B1:Cài đặt các gói phần mềm hỗ trợ: Pcap, PCRE, libdnet, DAQ, lib

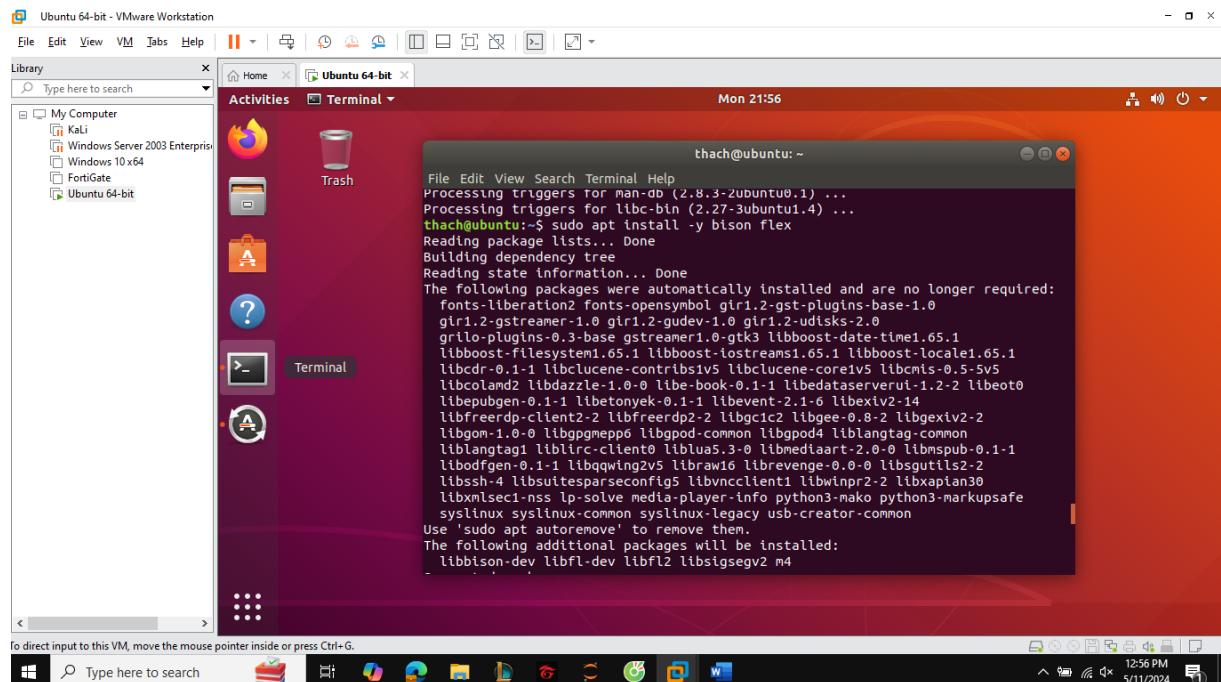
Sudo apt install -y build-essential



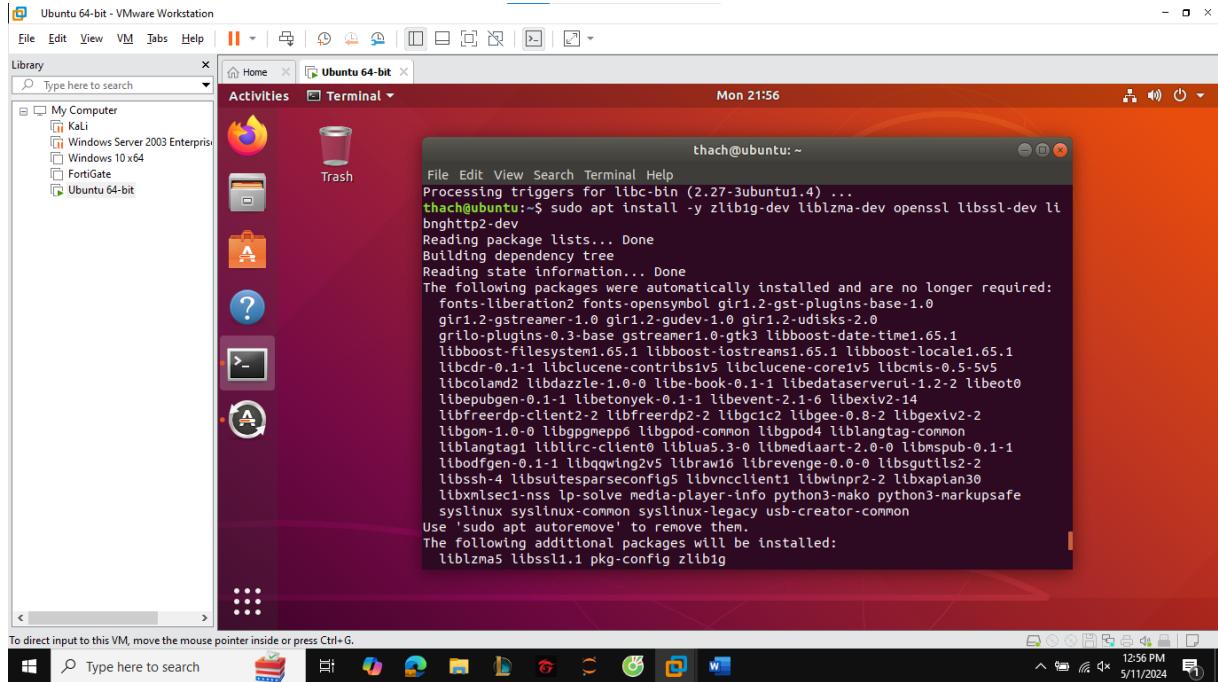
```
sudo apt install -y libpcap-dev libpcre3-dev libdumbnet-dev
```



```
sudo apt install -y bison flex
```



```
sudo apt install -y zlib1g-dev liblzma-dev openssl libssl-dev libnnghttp2-dev
```



## B2:Tạo thư mục chứa mã nguồn Snort và cài đặt Snort:

### Tạo thư mục chứa mã nguồn Snort:

```
mkdir -p ~/snort_src
```

```
cd ~/snort_src
```

### Cài đặt gói DAQ

```
sudo wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz
```

```
sudo tar -xvzf daq-2.0.7.tar.gz
```

```
cd daq-2.0.7
```

```
sudo ./configure
```

```
sudo make
```

```
sudo make install
```

```
Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help ▾
Library Type here to search
My Computer
Kali
Windows Server 2003 Enterprise
Windows 10 x64
FortiGate
Ubuntu 64-bit

Activities Terminal Mon 22:00
thach@ubuntu: ~/snort_src

thach@ubuntu:~$ clear
thach@ubuntu:~/snort_src$ sudo wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz
--2024-11-04 22:00:04-- https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz
Resolving www.snort.org (www.snort.org)... 104.19.222.12, 104.19.221.12, 2606:4700::6813:de0c, ...
Connecting to www.snort.org (www.snort.org)|104.19.222.12|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/025/695/original/daq-2.0.7.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAUT7AKS1TMM0XB2W5%2F20241105%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20241105T060009Z&X-Amz-Expires=3600X&X-Amz-SignedHeaders=host&X-Amz-Signature=031521a7df9af873f5f557d920a1b703a2c26e01ca0dd1464e0e64be15923d24 [following]
--2024-11-04 22:00:09-- https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/025/695/original/daq-2.0.7.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAUT7AKS1TMM0XB2W5%2F20241105%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20241105T060009Z&X-Amz-Expires=3600X&X-Amz-SignedHeaders=host&X-Amz-Signature=031521a7df9af873f5f557d920a1b703a2c26e01ca0dd1464e0e64be15923d24 [following]
Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)|52.216.51.153|:443... connected.
Connecting to snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)|52.216.51.153|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 515154 (503K) [binary/octet-stream]
Saving to: 'daq-2.0.7.tar.gz'

daq-2.0.7.tar.gz    100%[=====] 503.08K   133KB/s   in 3.8s

2024-11-04 22:00:14 (133 KB/s) - 'daq-2.0.7.tar.gz' saved [515154/515154]

thach@ubuntu:~/snort_src$
```

```
Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help ▾
Library Type here to search
My Computer
Kali
Windows Server 2003 Enterprise
Windows 10 x64
FortiGate
Ubuntu 64-bit

Activities Terminal Mon 22:01
thach@ubuntu: ~/snort_src

thach@ubuntu:~/snort_src$ sudo tar -xvf daq-2.0.7.tar.gz
daq-2.0.7/
daq-2.0.7/config.h.in
daq-2.0.7/config.guess
daq-2.0.7/apt/
daq-2.0.7/apt/daq.h
daq-2.0.7/apt/Makefile.am
daq-2.0.7/apt/daq_common.h
daq-2.0.7/apt/daq_base.c
daq-2.0.7/apt/daq_api.h
daq-2.0.7/apt/daq_mod_ops.c
daq-2.0.7/apt/Makefile.in
daq-2.0.7/config_sub
daq-2.0.7/lmain.sh
daq-2.0.7/os-daq-modules/
daq-2.0.7/os-daq-modules/daq_modules-config.in
daq-2.0.7/os-daq-modules/Makefile.c
daq-2.0.7/os-daq-modules/Makefile.am
daq-2.0.7/os-daq-modules/daq_static_modules.h
daq-2.0.7/os-daq-modules/daq_dump.c
daq-2.0.7/os-daq-modules/daq_ipq.c
daq-2.0.7/os-daq-modules/daq_static_modules.c
daq-2.0.7/os-daq-modules/daq_pcap.c
daq-2.0.7/os-daq-modules/daq_nfq.c
daq-2.0.7/os-daq-modules/daq_netmap.c
daq-2.0.7/os-daq-modules/daq_afpacket.c
daq-2.0.7/os-daq-modules/Makefile.in
daq-2.0.7/compile
daq-2.0.7/install-sh
daq-2.0.7/m4cissin
```

```
Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help | < > | X
Library Type here to search
Activities Terminal Mon 22:01
thach@ubuntu: ~/snort_src/daq-2.0.7
File Edit View Search Terminal Help
daq-2.0.7/decomp
thach@ubuntu:~/snort_src/daq-2.0.7$ sudo ./configure
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk... no
checking for mawk...
checking whether make sets $(MAKE)... yes
c_Help whether make supports nested variables... yes
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking for style of include used by make... GNU
checking dependency style of gcc... gcc
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking how to print strings... printf
checking for a sed that does not truncate output... /bin/sed
checking for grep that handles long lines and -e... /bin/grep
checking for egrep... /bin/grep -E
checking for fgrep... /bin/grep -F
checking for ld used by gcc... /usr/bin/ld
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
Activities Terminal 10:01 PM 5/11/2024
```

```
Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help | < > | X
Library Type here to search
Activities Terminal Mon 22:02
thach@ubuntu: ~/snort_src/daq-2.0.7
File Edit View Search Terminal Help
Build netmap DAQ module.... : no
thach@ubuntu:~/snort_src/daq-2.0.7$ sudo make
make all-recurse
make[1]: Entering directory '/home/thach/snort_src/daq-2.0.7'
make all in api
make[2]: Entering directory '/home/thach/snort_src/daq-2.0.7/api'
/bin/bash ./libtool --tag=CC --mode=compile gcc -DHAVE_CONFIG_H -I. -I.. -I/usr/include -g -O2 -fvisibility=hidden -Wall -Wwrite-strings -Wsign-compare -Wcast-align -Wextra -Wformat -Wformat-security -Wno-unused-parameter -fno-strict-aliasing -fdiagnostics-show-option -pedantic -std=c99 -D_GNU_SOURCE -MT daq_base.lo -MD -MP -MF .deps/daq_base.Tpo -o daq_base.c
libtool: compile: gcc -DHAVE_CONFIG_H -I. -I.. -I/usr/include -g -O2 -fvisibility=hidden -Wall -Wwrite-strings -Wsign-compare -Wcast-align -Wextra -Wformat -Wformat-security -Wno-unused-parameter -fno-strict-aliasing -fdiagnostics-show-option -pedantic -std=c99 -D_GNU_SOURCE -MT daq_base.lo -MD -MP -MF .deps/daq_base.Tpo -c daq_base.c -fPIC -DPIC -o .libs/daq_base.o
daq_base.c: In function 'daq_config_set_value':
d_SoftwareUpdate: warning: ISO C does not support '__FUNCTION__' predefined identifier [-Wpedantic]
              __FUNCTION__, (unsigned long) sizeof(struct _daq_dict_entry));
                                         ^
daq_base.c:542:21: warning: ISO C does not support '__FUNCTION__' predefined identifier [-Wpedantic]
              __FUNCTION__, (unsigned long) (strlen(key) + 1));
                                         ^
daq_base.c:555:21: warning: ISO C does not support '__FUNCTION__' predefined identifier [-Wpedantic]
              __FUNCTION__, (unsigned long) (strlen(value) + 1));
                                         ^
libtool: compile: gcc -DHAVE_CONFIG_H -I. -I.. -I/usr/include -g -O2 -fvisibility=hidden -Wall -Wwrite-strings -Wsign-compare -Wcast-align -Wextra -Wformat -Wformat-security -Wno-unused-parameter -fno-strict-aliasing -fdiagnostics-show-option -pedantic -std=c99 -D_GNU_SOURCE -MT daq_base.lo -MD -MP -MF .deps/daq_base.Tpo -c daq_base.c -o daq_base.o
e.o >/dev/null 2>&1
mv -f daq_base.Tpo daq_base.o
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
Activities Terminal 10:02 PM 5/11/2024
```

```

File Edit View Search Terminal Help
make[1]: Leaving directory '/home/thach/snort_src/daq-2.0.7'
thach@ubuntu:~/snort_src/daq-2.0.7$ sudo make install
make[1]: Entering directory '/home/thach/snort_src/daq-2.0.7/api'
make[2]: Entering directory '/home/thach/snort_src/daq-2.0.7/api'
/bin/mkdir -p '/usr/local/lib'
/bin/bash ./libtool --mode=install /usr/bin/install -c libdaq.la libdaq_static.la '/usr/local/lib'
libtool: install: /usr/bin/install -c .libs/libdaq.so.2.0.4 /usr/local/lib/libdaq.so.2.0.4
libtool: install: (cd /usr/local/lib && ( ln -s -f libdaq.so.2.0.4 libdaq.so.2 || { rm -f libdaq.so.2 && ln -s libda
q.so.2.0.4 libdaq.so; } ))
libtool: install: (cd /usr/local/lib && { ln -s -f libdaq.so.2.0.4 libdaq.so || { rm -f libdaq.so && ln -s libdaq.so
2.0.4 libdaq.so; } })
libtool: install: /usr/bin/install -c .libs/libdaq.lai /usr/local/lib/libdaq.la
libtool: install: /usr/bin/install -c .libs/libdaq_static.lai /usr/local/lib/libdaq_static.la
libtool: install: /usr/bin/install -c .libs/libdaq.a /usr/local/lib/libdaq.a
libtool: install: chmod 644 /usr/local/lib/libdaq.a
libtool: install: ranlib /usr/local/lib/libdaq.a
libtool: install: /usr/bin/install -c .libs/libdaq_static.a /usr/local/lib/libdaq_static.a
libtool: install: chmod 644 /usr/local/lib/libdaq_static.a
libtool: install: ranlib /usr/local/lib/libdaq_static.a
libtool: finish: PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/bin:/snap/bin:/sbin" ldconfig -n /us
r/local/lib
-----
Libraries have been installed in:
/usr/local/lib

If you ever happen to link against installed libraries
in a given directory, LIBDIR, you must either use libtool, and
specify the full pathname of the library, or use the '-LLIBDIR'
flag during linking and do at least one of the following:

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Type here to search

1:03 PM 5/11/2024

## Cài đặt Snort:

```
sudo wget https://www.snort.org/downloads/snort/snort-2.9.20.tar.gz
```

```
sudo tar -zxf snort-2.9.20.tar.gz
```

```
cd snort-2.9.20
```

```
sudo ./configure --enable-sourcefire --disable-open-appid
```

```
sudo apt install libntirpc-dev
```

```
sudo make CFLAGS=-I/usr/include/ntirpc
```

```
sudo make install
```

```

File Edit View VM Tabs Help
Library Type here to search
Activities Terminal
thach@ubuntu:~/snort_src$ cd ..
thach@ubuntu:~/snort_src$ sudo wget https://www.snort.org/downloads/snort/snort-2.9.20.tar.gz
--2024-11-04 22:04:23-- https://www.snort.org/... 104.19.222.12, 104.19.221.12, 2666:4700::6813:de0c, ...
Connecting to www.snort.org (www.snort.org)|104.19.222.12|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/025/687/original/snort-2.9.20.t
ar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AKS1TMMQGB2W5%2F20241105%2Fus-east-1%2F53%2Faws4_requ
estX-Amz-Date=20241105T0600Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=821863dd4d670383c77dac4
c65407179c4d@7dafe2b87496995df7800246 [following]
--2024-11-04 22:04:36-- https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/025/687/original
/snort-2.9.20.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AKS1TMMQGB2W5%2F20241105%2Fus-east-1%2
F53%2Faws4_requ...7dac4c05407179c4d@7dafe2b87496995df7800246
Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)|52.216.237.3, 3.5.27.233, 3.5.29.82,
...
Connecting to snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)|52.216.237.3|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7009894 (6.7M) [binary/octet-stream]
Saving to: 'snort-2.9.20.tar.gz'

snort-2.9.20.tar.gz      100%[=====] 6.68M 129KB/s in 42s

2024-11-04 22:05:13 (164 KB/s) - 'snort-2.9.20.tar.gz' saved [7009894/7009894]

thach@ubuntu:~/snort_src$ 

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Type here to search

1:06 PM 5/11/2024

```
Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library Type here to search
Activities Terminal Mon 22:08
thach@ubuntu: ~/snort_src/snort-2.9.20
thach@ubuntu:~/snort_src$ sudo tar -zxf snort-2.9.20.tar.gz
thach@ubuntu:~/snort_src$ cd snort-2.9.20
thach@ubuntu:~/snort_src/snort-2.9.20$ sudo ./configure --enable-sourcefire --disable-open-appid
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk... no
checking for mawk...
checking whether make sets $MAKE... yes
checking whether make supports nested variables... yes
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking dependency style of gcc... gcc3
checking for gcc option to accept ISO C99... none needed
checking for gcc option to accept ISO Standard C... (cached) none needed
checking for gcc... (cached) gcc
checking whether we are using the GNU C compiler... (cached) yes
checking whether gcc accepts -g... (cached) yes
checking for gcc option to accept ISO C89... (cached) none needed
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
Activities Terminal 1:08 PM 5/11/2024
```

```
Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library Type here to search
Activities Terminal Mon 22:09
thach@ubuntu: ~/snort_src/snort-2.9.20
thach@ubuntu:~/snort_src$ sudo apt install libntirpc-dev
Reading package lists... done
Building dependency tree
Reading state information... done
The following packages were automatically installed and are no longer required:
  fonts-liberation2 fonts-opensymbol gir1.2-gst-plugins-base-1.0 gir1.2-gstreamer-1.0
  gir1.2-udisks-2.0 grilo-plugins-0.3-base gstreamer1.0-gtk3 libboost-filesystem1.65.1
  libboost-iostreams1.65.1 libboost-locale1.65.1 libcdio-0.1.1 libclucene-contribs1.5 libclucene-core1.5
  libcmis-0.5.5v5 libcolam0 libdazzle-1.0 libedata-book-0.1.1 libedataserver-1.2.2 libebook libepubgen-0.1.1
  libetonyek-0.1.1 libevent-2.1.6 libexiv2-14 libfreerdp-client-2.2 libfreerdp2-2 libgc1c2 libgee-0.8.2 libgexiv2-2
  libgsm-1.0.0 libggpmepg6 libgpod-common libgpod4 liblangtag-common liblangtag1 liblirc-client0 libluas5.3-0
  libmediaart-2.0.0 libmspub-0.1.1 libodfgen-0.1.1 libqwing2v5 libraw16 librevenge-0.0.0 libsgutils2-2 libssh-4
  libsubprocessconfig5 libvncclient libvlnpr2-2 libxapian30 libxmlsec1-nss lp-solve media-player-info
  python3-nak0 python3-markupsafe syslinux syslinux-common syslinux-legacy usb-creator-common
python3-nak0 python3-markupsafe syslinux syslinux-common syslinux-legacy usb-creator-common
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libntirpc1.6
The following NEW packages will be installed:
  libntirpc-dev libntirpc1.6
0 upgraded, 2 newly installed, 0 to remove and 282 not upgraded.
Need to get 178 kB of archives.
After this operation, 758 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 libntirpc1.6 amd64 1.6.1-1 [106 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 libntirpc-dev amd64 1.6.1-1 [71.6 kB]
Fetched 178 kB in 2s (47.9 kB/s)
Selecting previously unselected package libntirpc1.6:amd64.
(Reading database ... 156960 files and directories currently installed.)
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
Activities Terminal 1:09 PM 5/11/2024
```

```
File Edit View VM Tabs Help Activities Terminal Mon 22:10
thach@ubuntu:~/snort_src/snort-2.9.20$ sudo make CFLAGS=-I/usr/include/ntirpc
make all-recursive
make[1]: Entering directory '/home/thach/snort_src/snort-2.9.20'
make[2]: Entering directory '/home/thach/snort_src/snort-2.9.20/src'
make[3]: Entering directory '/home/thach/snort_src/snort-2.9.20/src/sfutil'
gcc -DHAVE_CONFIG_H -I. -I../../src/sfutil -I/usr/include/pcap -I../../src/output-plugin
s -I../../src/detection-plugins -I../../src/dynamic-plugins -I../../src preprocessors -I../../src preprocessors/port
scan -I../../src preprocessors/HttpInspect/include -I../../src preprocessors/Session -I../../src preprocessors/Strea
m -I../../src target-based -I../../src control -I../../src file-process -I../../src file-process/libs -I../../src/s
ide-channel -I../../src side-channel/plugins -I../../src/reload-adjust -DLZMA -DGRE -DMPLS -DPPM_MGR -DNDEBUG -DSOU
RCEFI -DPMM_MGR -DENABLE_REACT -DENABLE_RESPOND -DENABLE_RESPONSE3 -DSF_WCHAR -DTARGET_BASED -DPERF_PROFILING -DPE
RF_PROFILING -DSNORT_RELOAD -DNO_NON_ETHER_DECODER -DNORMALIZER -DACTIVE_RESPONSE -I/usr/include/ntirpc -c -o sfha
sh.o sfhashcn.c
gcc -DHAVE_CONFIG_H -I. -I../../src/sfutil -I/usr/include/pcap -I../../src/output-plugin
s -I../../src/detection-plugins -I../../src/dynamic-plugins -I../../src preprocessors -I../../src preprocessors/port
scan -I../../src preprocessors/HttpInspect/include -I../../src preprocessors/Session -I../../src preprocessors/Strea
m -I../../src target-based -I../../src control -I../../src file-process -I../../src file-process/libs -I../../src/s
ide-channel -I../../src side-channel/plugins -I../../src/reload-adjust -DLZMA -DGRE -DMPLS -DPPM_MGR -DNDEBUG -DSOU
RCEFI -DPMM_MGR -DENABLE_REACT -DENABLE_RESPOND -DENABLE_RESPONSE3 -DSF_WCHAR -DTARGET_BASED -DPERF_PROFILING -DPE
RF_PROFILING -DSNORT_RELOAD -DNO_NON_ETHER_DECODER -DNORMALIZER -DACTIVE_RESPONSE -I/usr/include/ntirpc -c -o sfhs
hfcn.o sfhashfn.c
gcc -DHAVE_CONFIG_H -I. -I../../src/sfutil -I/usr/include/pcap -I../../src/output-plugin
s -I../../src/detection-plugins -I../../src/dynamic-plugins -I../../src preprocessors -I../../src preprocessors/port
scan -I../../src preprocessors/HttpInspect/include -I../../src preprocessors/Session -I../../src preprocessors/Strea
m -I../../src target-based -I../../src control -I../../src file-process -I../../src file-process/libs -I../../src/s
ide-channel -I../../src side-channel/plugins -I../../src/reload-adjust -DLZMA -DGRE -DMPLS -DPPM_MGR -DNDEBUG -DSOU
RCEFI -DPMM_MGR -DENABLE_REACT -DENABLE_RESPOND -DENABLE_RESPONSE3 -DSF_WCHAR -DTARGET_BASED -DPERF_PROFILING -DPE
RF_PROFILING -DSNORT_RELOAD -DNO_NON_ETHER_DECODER -DNORMALIZER -DACTIVE_RESPONSE -I/usr/include/ntirpc -c -o sfhs
hfcn.o sfhashfn.c
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

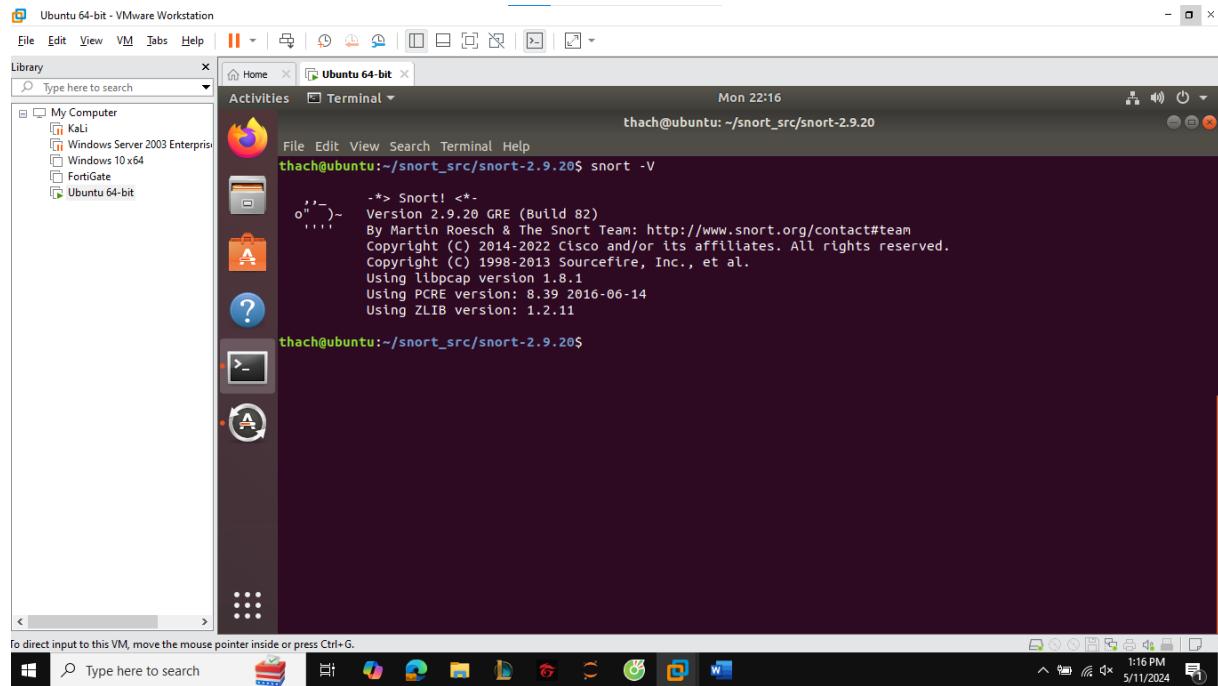
```
File Edit View VM Tabs Help Activities Terminal Mon 22:16
thach@ubuntu:~/snort_src/snort-2.9.20$ sudo make install
Making install in src
make[1]: Entering directory '/home/thach/snort_src/snort-2.9.20/src'
make[2]: Entering directory '/home/thach/snort_src/snort-2.9.20/src/sfutil'
make[3]: Entering directory '/home/thach/snort_src/snort-2.9.20/src/sfutil'
make[3]: Nothing to be done for 'install-data-am'.
make[3]: Nothing to be done for 'install-exec-am'.
make[2]: Leaving directory '/home/thach/snort_src/snort-2.9.20/src/sfutil'
make[2]: Leaving directory '/home/thach/snort_src/snort-2.9.20/src'
Making install in win32
make[2]: Entering directory '/home/thach/snort_src/snort-2.9.20/src/win32'
make[3]: Entering directory '/home/thach/snort_src/snort-2.9.20/src/win32'
make[3]: Nothing to be done for 'install-data-am'.
make[3]: Nothing to be done for 'install-exec-am'.
make[2]: Leaving directory '/home/thach/snort_src/snort-2.9.20/src/win32'
make[2]: Leaving directory '/home/thach/snort_src/snort-2.9.20/src'
Making install in output-plugins
make[2]: Entering directory '/home/thach/snort_src/snort-2.9.20/src/output-plugins'
make[3]: Entering directory '/home/thach/snort_src/snort-2.9.20/src/output-plugins'
make[3]: Nothing to be done for 'install-data-am'.
make[3]: Nothing to be done for 'install-exec-am'.
make[2]: Leaving directory '/home/thach/snort_src/snort-2.9.20/src/output-plugins'
make[2]: Leaving directory '/home/thach/snort_src/snort-2.9.20/src'
Making install in detection-plugins
make[2]: Entering directory '/home/thach/snort_src/snort-2.9.20/src/detection-plugins'
make[3]: Entering directory '/home/thach/snort_src/snort-2.9.20/src/detection-plugins'
make[4]: Entering directory '/home/thach/snort_src/snort-2.9.20/src/detection-plugins'
make[4]: Nothing to be done for 'install-data-am'.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

## Cập nhật thư viện

sudo ldconfig

sudo ln /usr/local/bin/snort /usr/sbin/snort

## Kết quả sau khi cài đặt Snort:



## B3:Cấu hình Snort:

### a) Tạo các thư mục Snort và các thư mục chứa các bộ rule

```
sudo mkdir /etc/snort
```

```
sudo mkdir /etc/snort/rules
```

```
sudo mkdir /etc/snort/rules/iplists
```

```
sudo mkdir /etc/snort/preproc_rules
```

```
sudo mkdir /usr/local/lib/snort_dynamicrules
```

```
sudo mkdir /etc/snort/so_rules
```

### b) Tạo file để lưu trữ rule và danh sách IP

```
sudo touch /etc/snort/rules/iplists/black_list.rules
```

```
sudo touch /etc/snort/rules/iplists/white_list.rules
```

```
sudo touch /etc/snort/rules/local.rules
```

```
sudo touch /etc/snort/sid-msg.map
```

### c) Tạo thư mục lưu trữ log

```
sudo mkdir /var/log/snort
```

```
sudo mkdir /var/log/snort/archived_logs
```

#### d) Sử dụng cấu hình có sẵn copy vào thư mục /etc/snort

```
cd snort_src/snort-2.9.20/etc
```

```
sudo cp *.conf* /etc/snort
```

```
sudo cp *.map /etc/snort
```

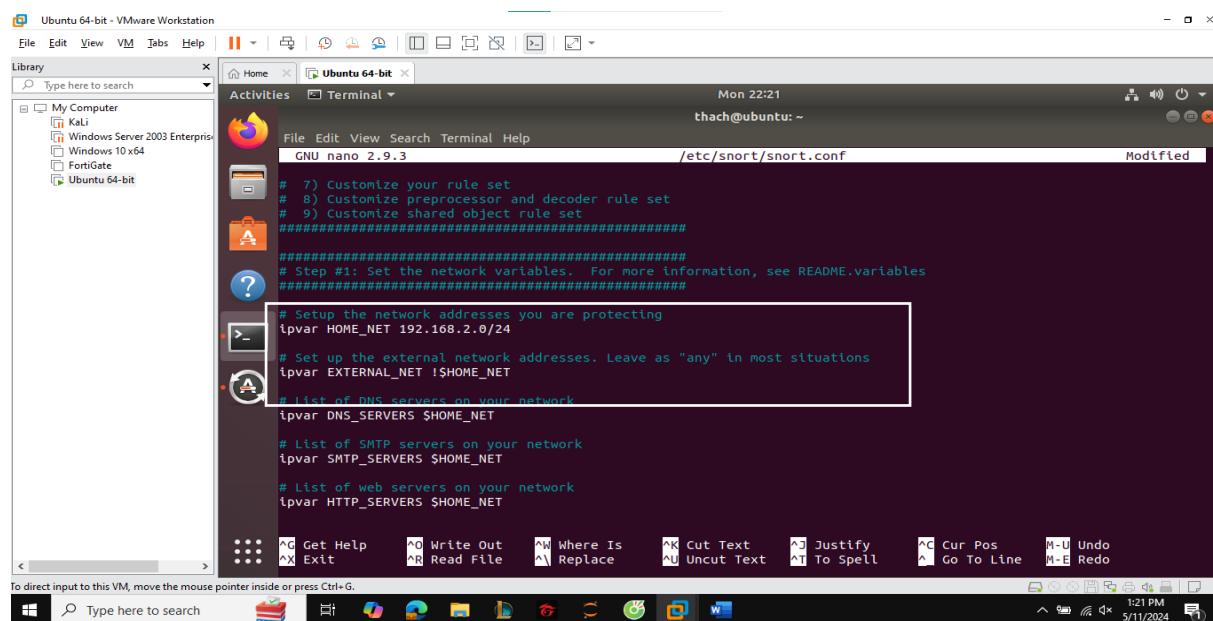
```
sudo cp *.dtd /etc/snort
```

```
cd snort_src/snort-2.9.20/src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor/
```

```
sudo cp * /usr/local/lib/snort_dynamicpreprocessor/
```

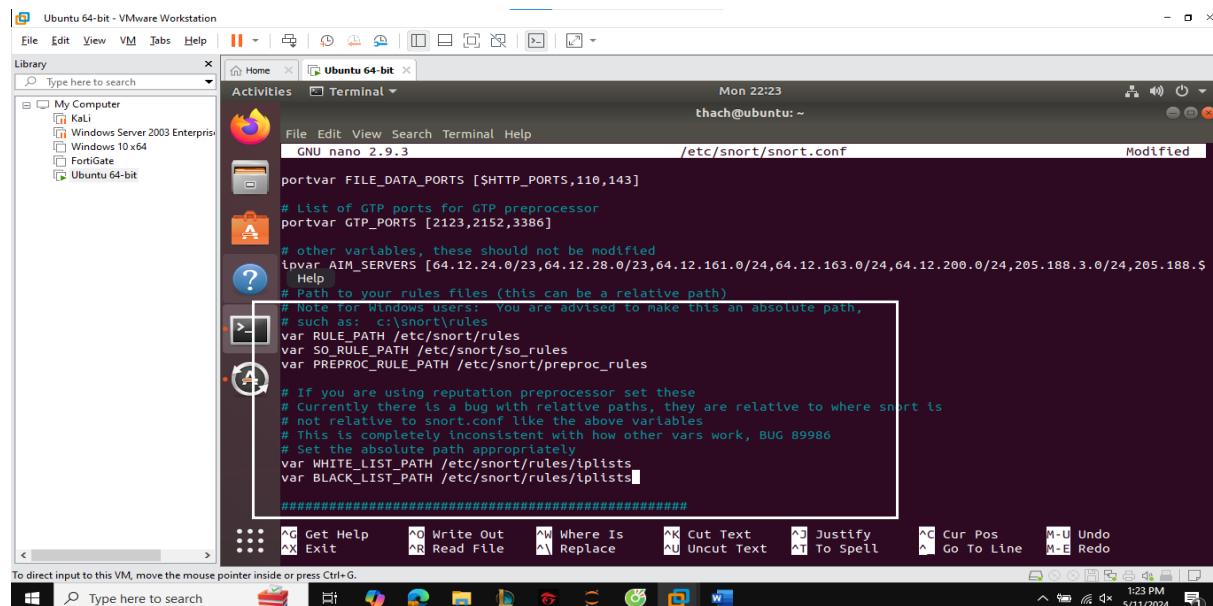
#### e) Chỉnh sửa các cấu hình cơ bản trong snort.conf

```
sudo nano /etc/snort/snort.conf
```



```
# 7) Customize your rule set
# 8) Customize preprocessor and decoder rule set
# 9) Customize shared object rule set
#####
##### Step #1: Set the network variables. For more information, see README.variables
#####

# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.2.0/24
# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET !$HOME_NET
# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET
# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET
# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET
```



```
portvar FILE_DATA_PORTS [$HTTP_PORTS,110,143]
# List of GTP ports for GTP preprocessor
portvar GTP_PORTS [2123,2152,3386]
# other variables, these should not be modified
lnvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.3.0/24,205.188.5.0/24,205.188.6.0/24]
# Path to your rules files (this can be a relative path)
# Note for Windows users: You are advised to make this an absolute path,
# such as: c:/snort/rules
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/snort.rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules
# If you are using reputation preprocessor set these
# Currently there is a bug with relative paths, they are relative to where snort is
# not relative to snort.conf like the above variables
# This is completely inconsistent with how other vars work, BUG 89986
# Set the absolute path appropriately
var WHITE_LIST_PATH /etc/snort/rules/iplists
var BLACK_LIST_PATH /etc/snort/rules/iplists
#####
#####
```

```

# site specific rules
include $RULE_PATH/local.rules

#include $RULE_PATH/app-detect.rules
#include $RULE_PATH/attack-responses.rules
#include $RULE_PATH/backdoor.rules
#include $RULE_PATH/bad-traffic.rules
#include $RULE_PATH/blacklist.rules
#include $RULE_PATH/botnet-cnc.rules
#include $RULE_PATH/browser-chrome.rules
#include $RULE_PATH/browser-firefox.rules
#include $RULE_PATH/browser-ie.rules
#include $RULE_PATH/browser-other.rules
#include $RULE_PATH/browser-plugins.rules
#include $RULE_PATH/browser-webkit.rules
#include $RULE_PATH/chat.rules
#include $RULE_PATH/content-replace.rules
#include $RULE_PATH/ddos.rules
#include $RULE_PATH/dns.rules
#include $RULE_PATH/dos.rules
#include $RULE_PATH/experimental.rules
#include $RULE_PATH/exploit-kit.rules
#include $RULE_PATH/exploit.rules
#include $RULE_PATH/file-executable.rules

```

#### B4: Kiểm tra sự hoạt động của Snort:

sudo snort -i ens33 -c /etc/snort/snort.conf -T

```

Version 2.9.20 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.8.1
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

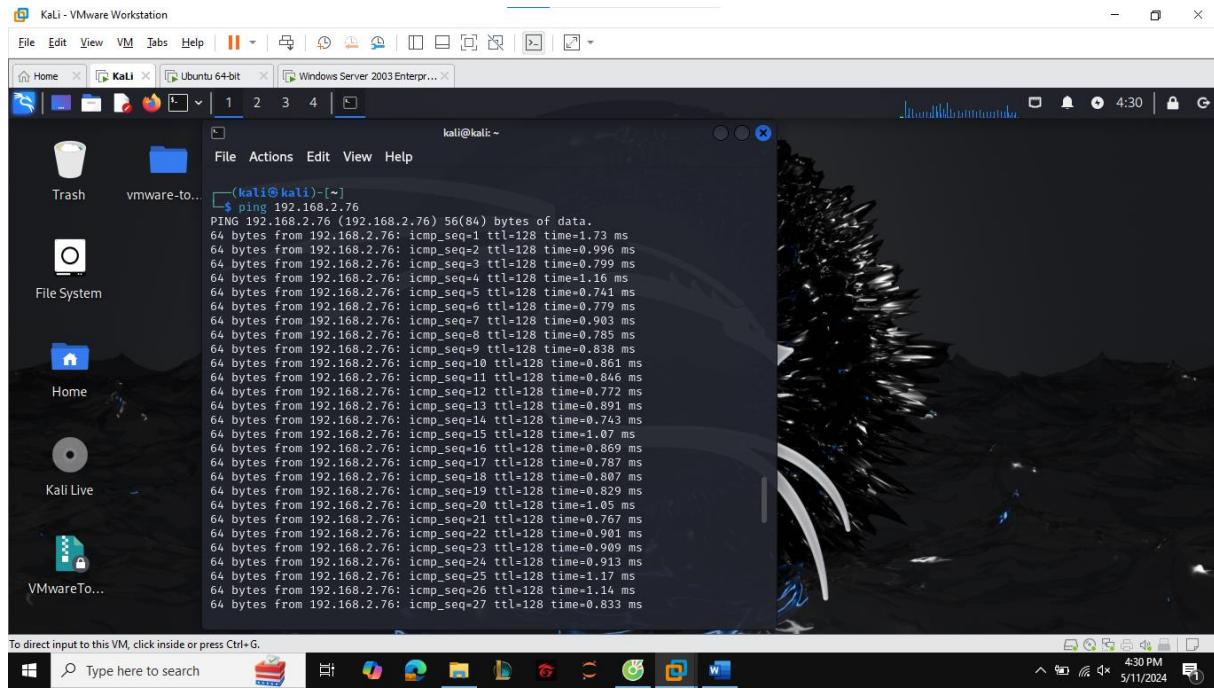
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SCOMMPPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>

Total snort Fixed Memory Cost - MaxRss:45824
Snort successfully validated the configuration!
Snort exiting

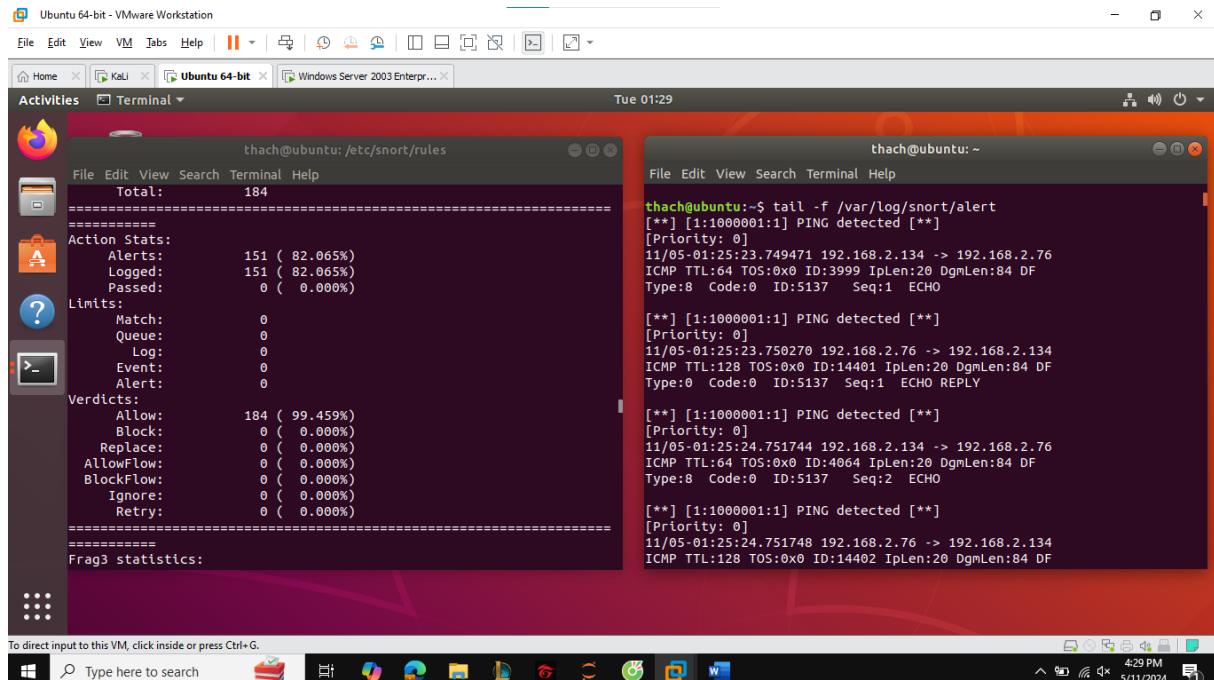
```

## 2. Dùng một số công cụ tấn công và mô tả kết quả xử lý trên Snort :

### Tấn công dò quét (Ping)



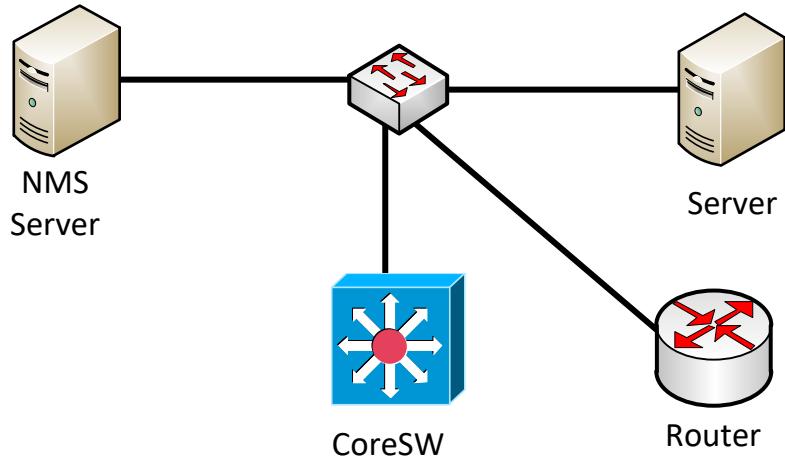
### Kết quả xử lý trên snort:



- **Terminal bên trái** hiển thị số liệu thống kê của Snort, cho biết trong số 184 gói tin, có 151 cảnh báo được kích hoạt liên quan đến phát hiện ping ICMP.
- **Terminal bên phải** đang hiển thị cảnh báo ping thời gian thực, trong đó Snort phát hiện các yêu cầu phản hồi ICMP lặp lại và ghi lại từng yêu cầu.

## 6. Network Monitoring System (1,0 điểm)

- Thực hiện giám sát mạng với phần mềm PRTG
- Cấu hình chức năng giám sát performance (RAM, CPU), giám sát một số dịch vụ mạng (DHCP, Web,...), giám sát dung lượng đĩa trên Server
- Thiết lập ngưỡng cảnh báo



### Các bước thực hiện:

- Thực hiện giám sát mạng với phần mềm PRTG

