**Tên: Lê Hải Đăng**

**MSSV: 20110243**

**Lab 7. Network Infrastructure Security**

**Submission:**

You will compose a lab report that documents each step you take, including screenshots to illustrate the effects of commands you type, and describing your observations. Simply attaching code without any explanation will not receive credits

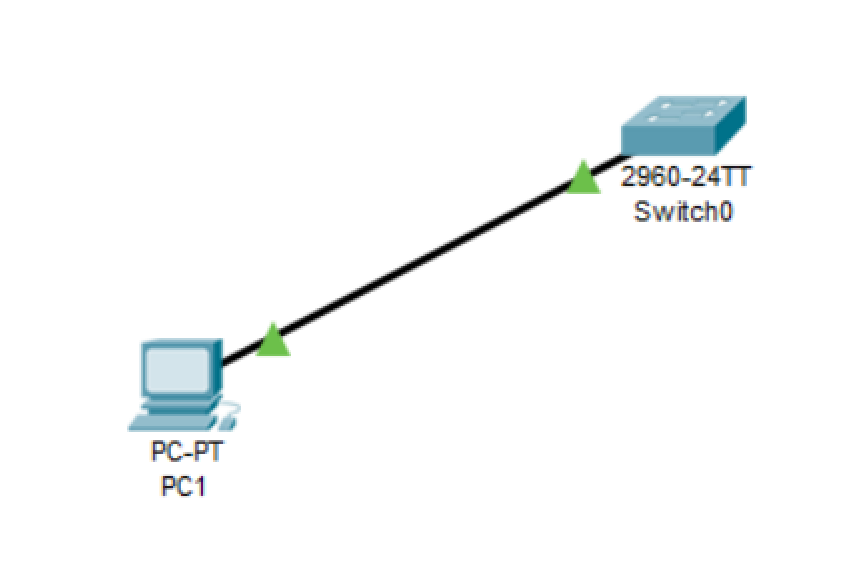
**Câu 1. Port Security**

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.

#### 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) 00E0.8FC9.256C*

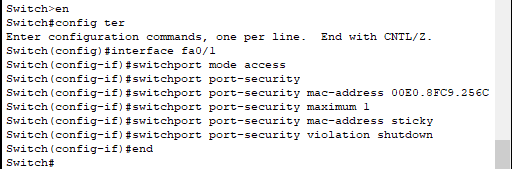
Switch(config-if)#switchport port-security maximum 1

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



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)*

Switch(config)#errdisable detect cause all

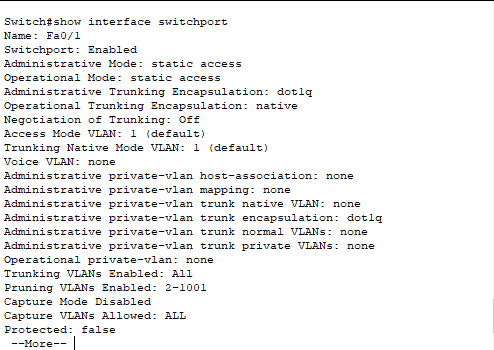
Switch(config)#errdisable recovery cause all

Switch(config)#errdisable recovery interval 30

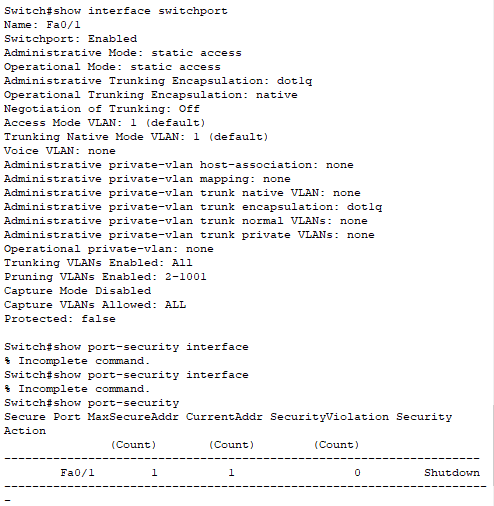


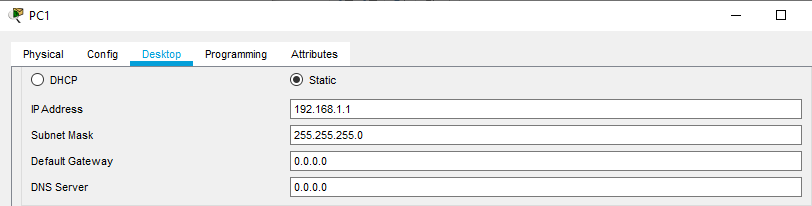
#### Kiểm tra cấu hình

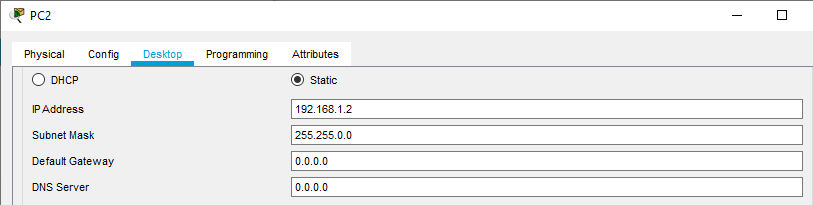
*show interface switchport*

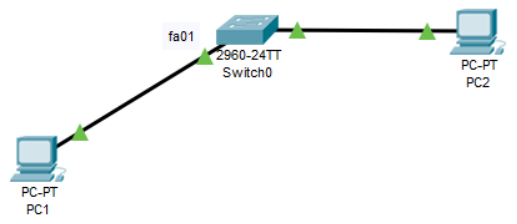
**

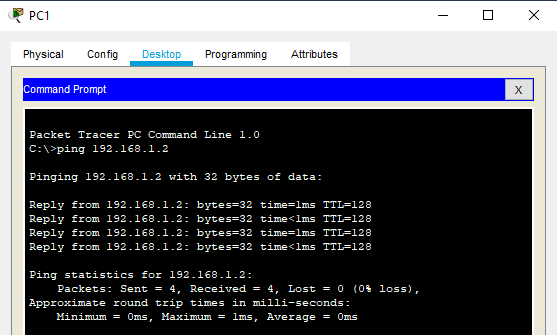
*show port-security interface*

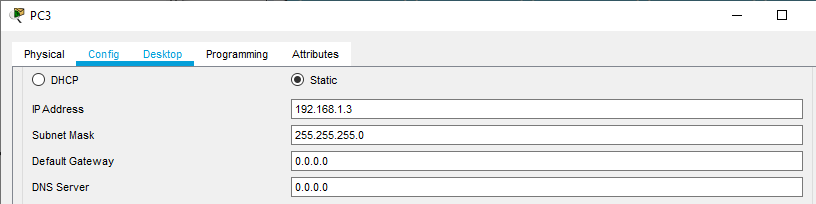


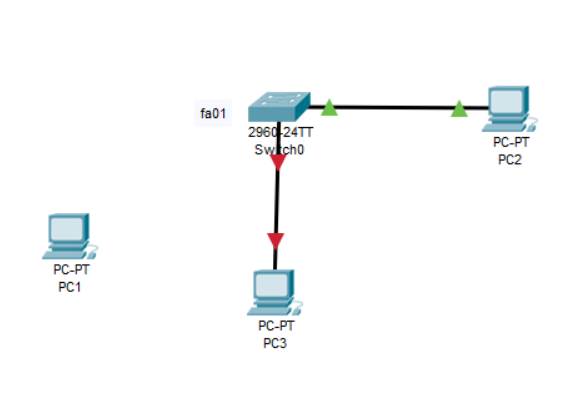


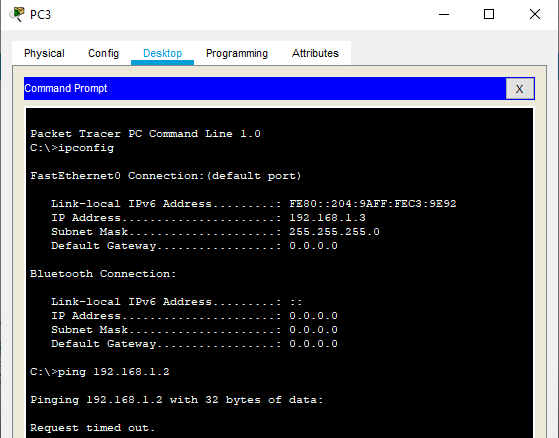


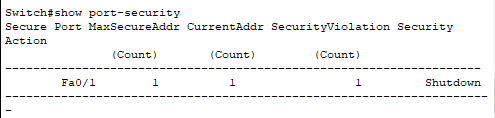


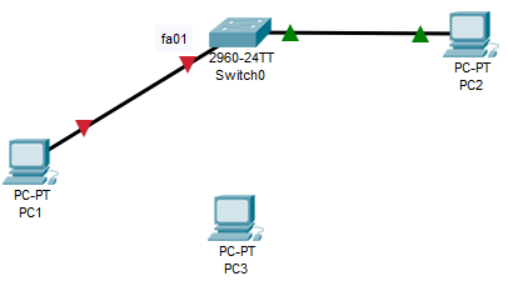


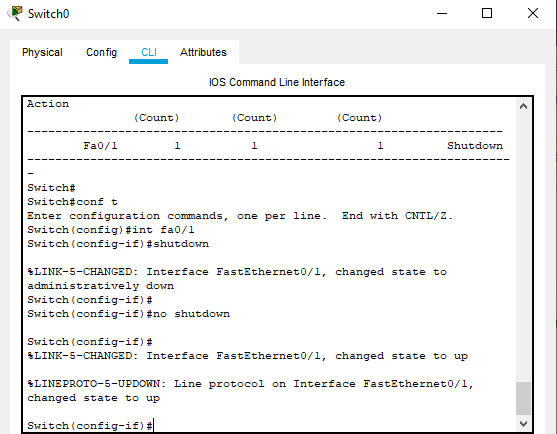


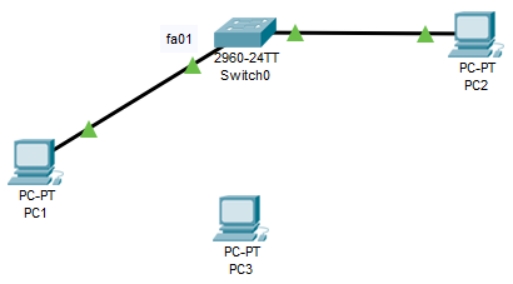




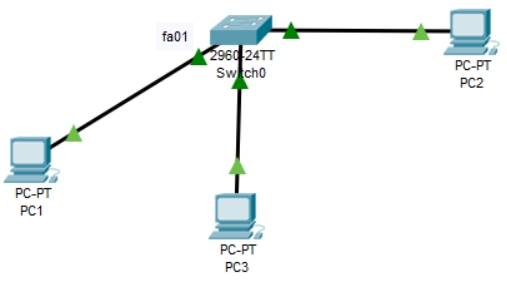












**Câu 2. DHCP snooping**

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

1. Cấu hình DHCP Server.

DHCP Server1: Cấp dãy địa chỉ IP : 192.168.1.0/24

Defaul Gateway : 192.168.1.100

DNS: 8.8.8.8

DHCP Server2: Cấp dãy địa chỉ IP : 172.16.1.0/24

Defaul Gateway : 172.16.1.200

DNS: 172.16.1.200

2. Cấu hình DHCP snooping trên Switch, so cho các client chỉ xin địa chỉ IP từ DHCP trên DHCP Server1.

Cấu hình DHCP snooping trên Switch, so cho các client chỉ xin địa chỉ IP từ DHCP trên DHCP Server 1.

Switch(config)#ip dhcp snooping

Switch(config)#ip dhcp snooping vlan 1

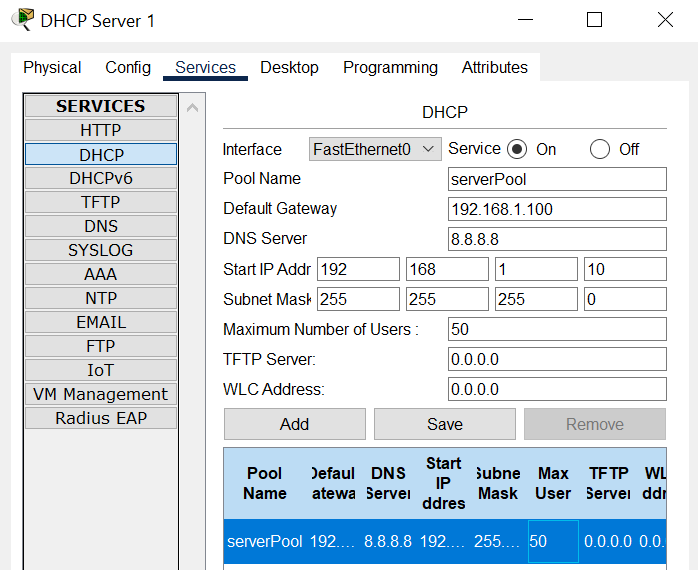
Switch(config)#interface fa0/2 (nối với DHCP thật)

Switch(config-if)#ip dhcp snooping trust

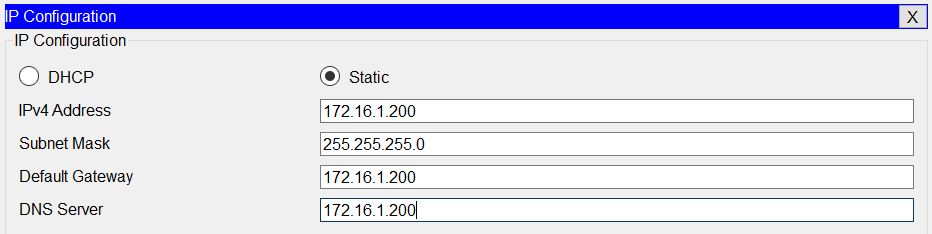
Switch(config-if)#exit

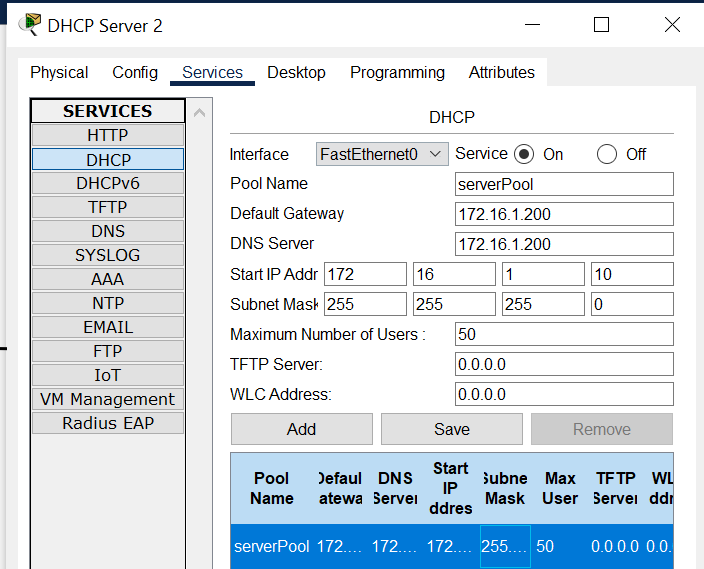
* Cấu hình DHCP Server 1



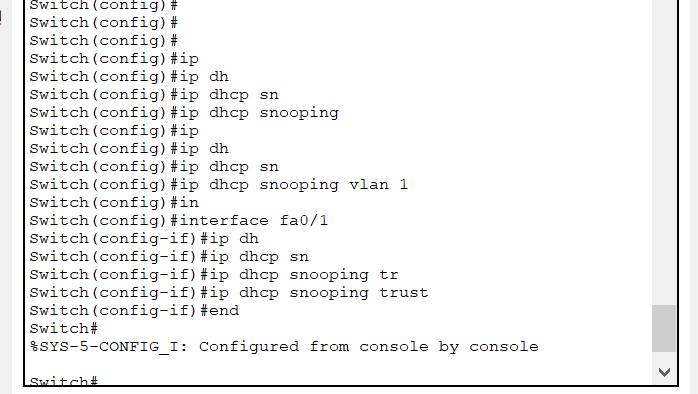
****

* Cấu hình DHCP Server 2

****

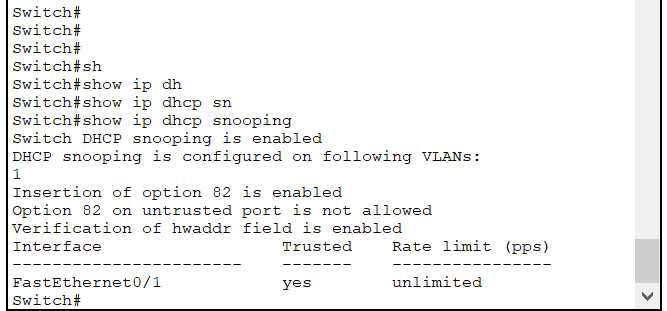
****

* Cấu hình DHCP snooping trên Switch, sao cho các client chỉ xin địa chỉ IP từ DHCP trên DHCP Server1.

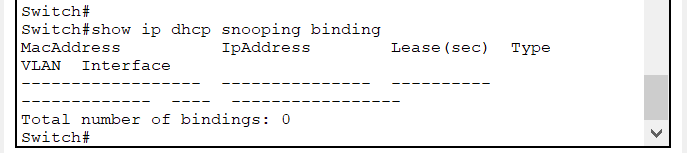
****

#### Kiểm tra cấu hình

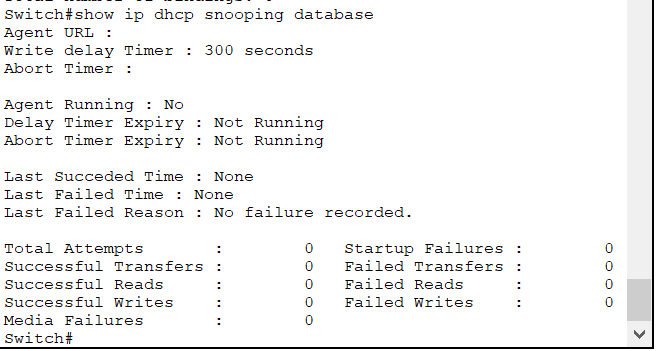
* Dùng lệnh *show ip dhcp snooping*



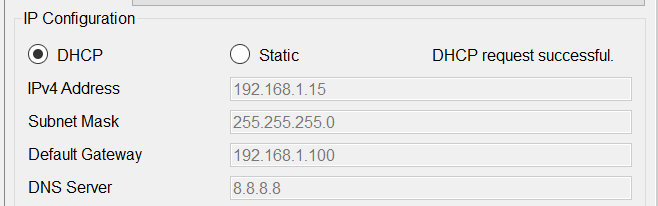
* Gõ lệnh *show ip dhcp snooping binding*

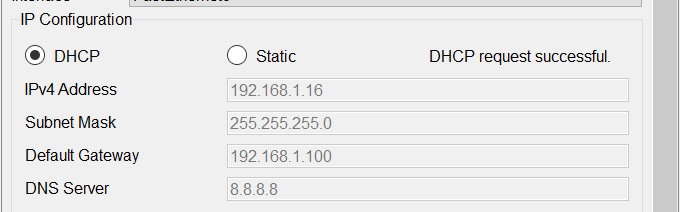


* Gõ lệnh *show ip dhcp snooping database*

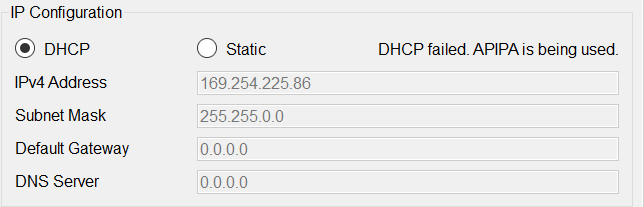


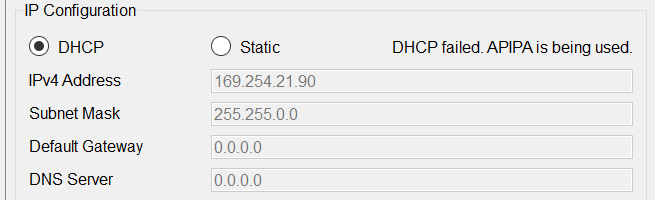
* Ta thấy cả 2 PC đều được cấp IP address từ DHCP Server 1

**

**

* Khi ta bỏ đường kết nối giữa switch và DHCP Server 1 thì PC xin cấp IP sẽ thất bại

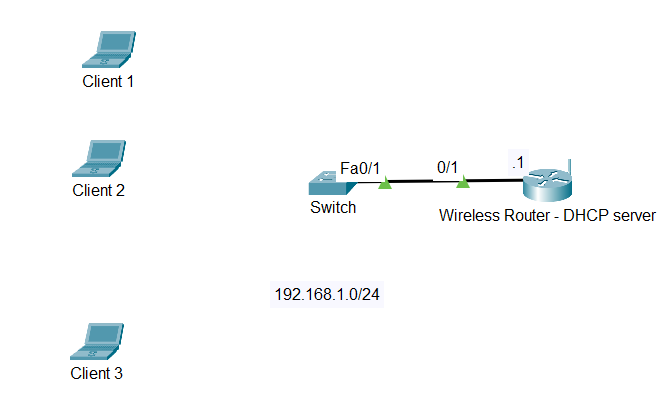
**

**

**Câu 3. Wifi Security**

1. **Cấu hình WiFi cơ bản**

* MAC filtering
* WPA2 – Personal

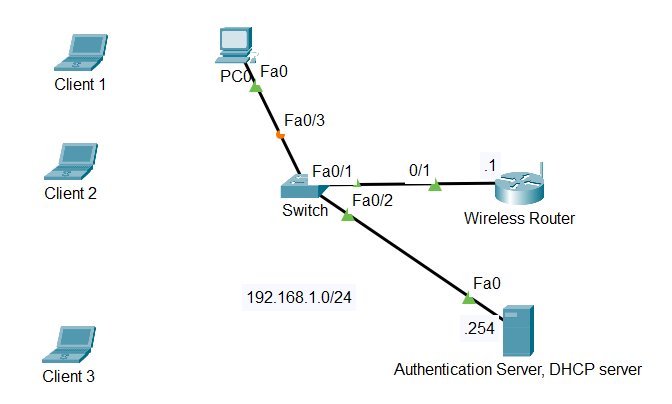


* AP có IP 192.168.1.1/24
* Mạng nội bộ được hoạch định với IP: 192.168.1.0/24

**Yêu cầu:**

* Cấu hình AP – tên SSID SV tự cho
* Cấu hình AP làm DHCP server, các thông số IP cấp phát
  + Network: 192.168.1.0/24
  + IP range 192.168.1.10 – 192.168.1.200
  + Default gateway: 192.168.1.1
  + DNS: 8.8.8.8
* Cấu hình AP chỉ cho phép máy Client 1 và Client 2 sử dụng mạng WiFi (MAC filtering)
* Cấu hình WPA2-personal (password SV tự cho)

1. **Cấu hình chứng thực người dùng WiFi dùng Radius Server**



* AP có IP 192.168.1.1/24
* Mạng nội bộ được hoạch định với IP: 192.168.1.0/24

**Yêu cầu:**

* Cấu hình AP – tên SSID SV tự cho
* Cấu hình Authentication Server (Radius server), tạo account để chứng thực người dùng Wifi
* AP đóng vai trò là Authenticator (dùng WPA2-Enterprise)
* Authentication Server cũng đóng vai trò là DHCP server cấp pháp IP động cho các client trong mạng. Các thông số IP cấp phát như sau:
  + Network: 192.168.1.0/24
  + IP range 192.168.1.10 – 192.168.1.200
  + Default gateway: 192.168.1.1
  + DNS: 8.8.8.8

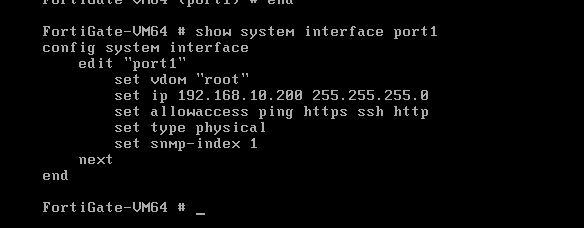
**Câu 3. Firewall**

Sử dụng Firewall dạng VMWare (Fortigate) thực hiện các rule bao gồm:

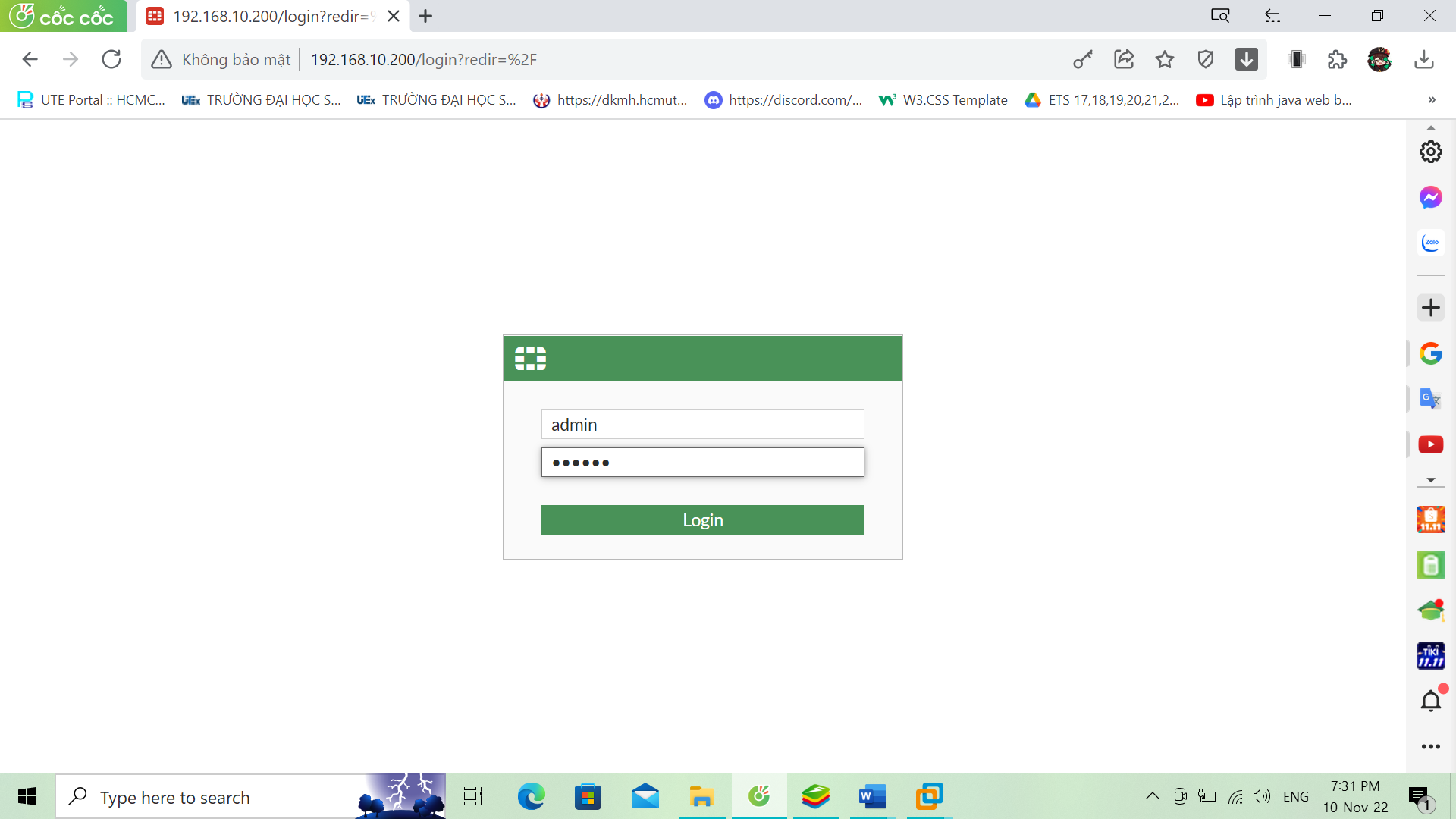
* Cho phép các PC bên trong mạng nội bộ ra ngoài Internet.
* Kiểm soát truy cập Web.
* Kiểm soát port truy cập.
* Kiểm soát ứng dụng truy cập.
* Thực hiện các phương thức khác.

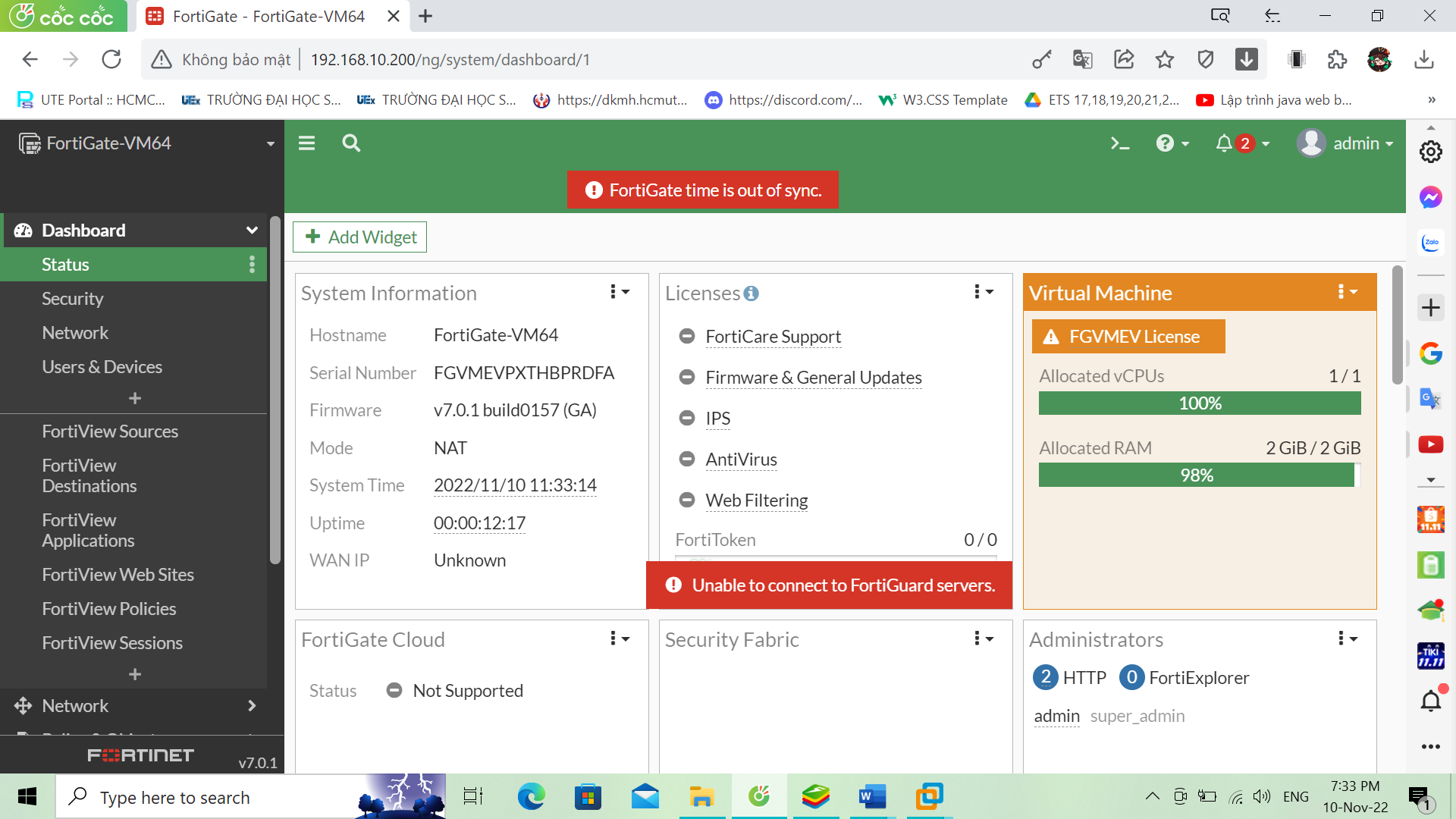
***Các bước thực hiện:***

* Thiết đặt fortigate

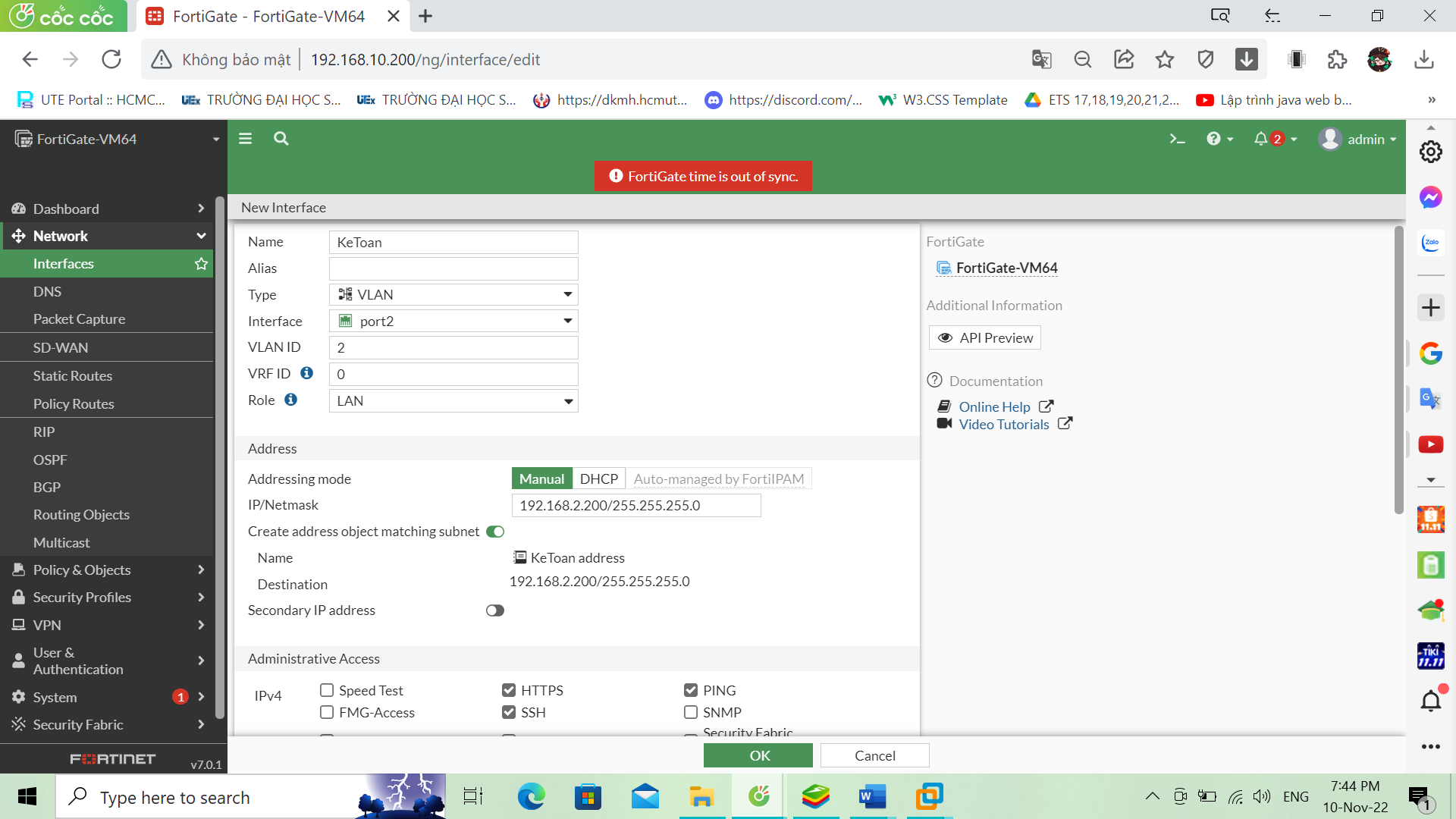


* Truy cập vào trang fortigate và tiến hành đăng nhập



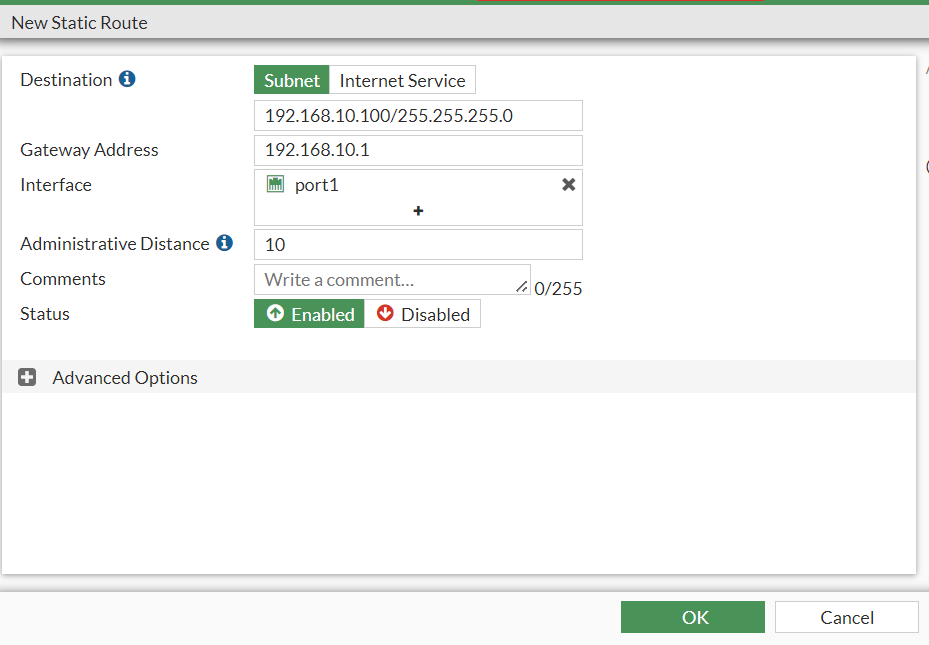


* Cấu hình tạo một interface

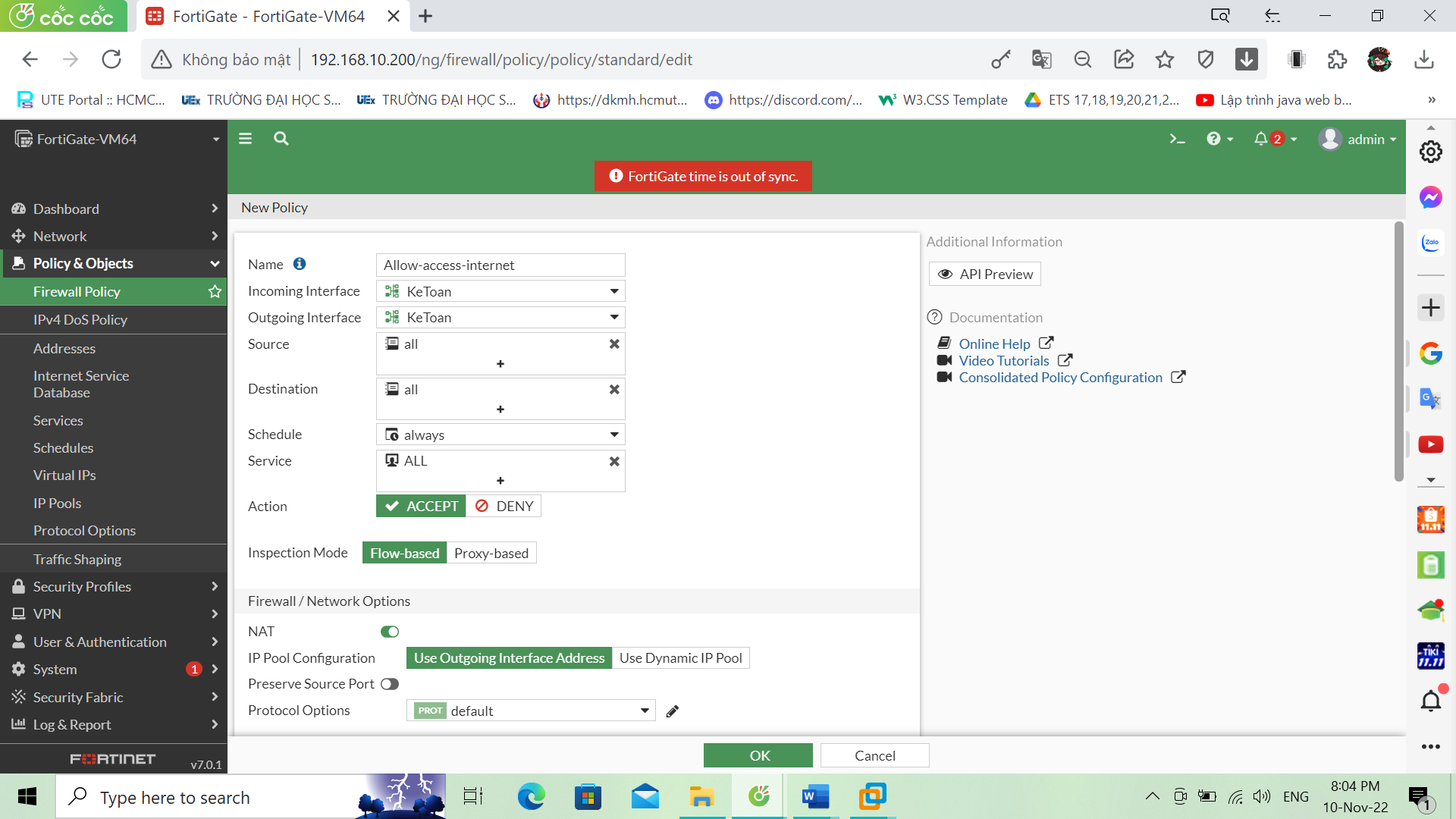


Cấu hình trên tạo ra Interface có tên là **KeToan** và được gán vào **port2**, type là **VLAN** với địa chỉ ip là **192.168.2.100** subnet mask **255.255.255.0**, chỉ cho phép truy cập các giao thức **HTTPS, PING, SSH**. Lúc này phòng **KeToan** chịu sự quản lý của **port2** nằm trong **VLAN ID 2.**

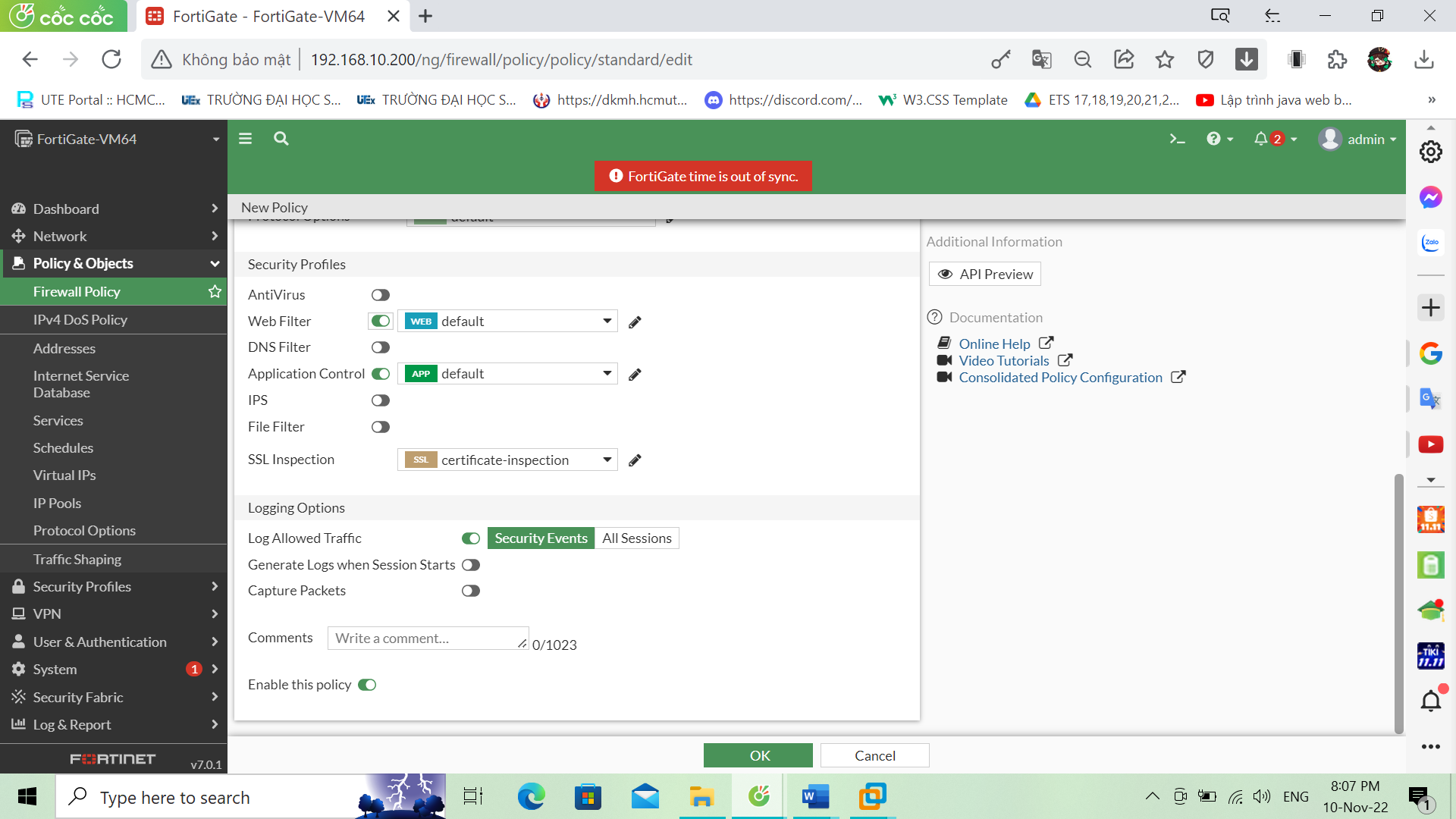
* Cấu hình tạo static route



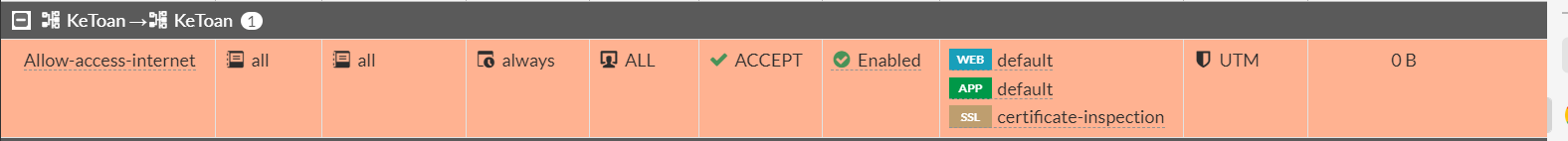
* Cấu hình firewall policy
  + Cho phép mạng LAN ra Internet



* + Ở phần **Application Control**, *rule default* được tạo sẵn với tác dụng kiểm soát toàn bộ truy cập ứng dụng
  + Ở phần **Web Filter**, rule *monitor-all* có sẵn với tác dụng kiểm soát tất cả URL truy cập, flow-based…

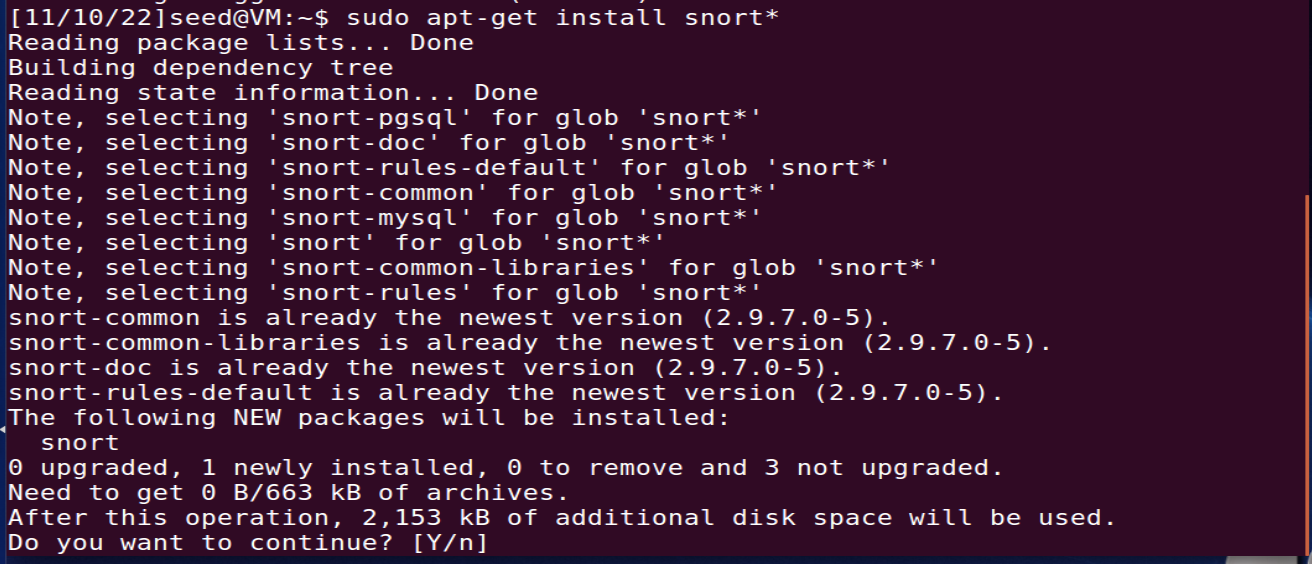


* Kết quả sau khi tạo

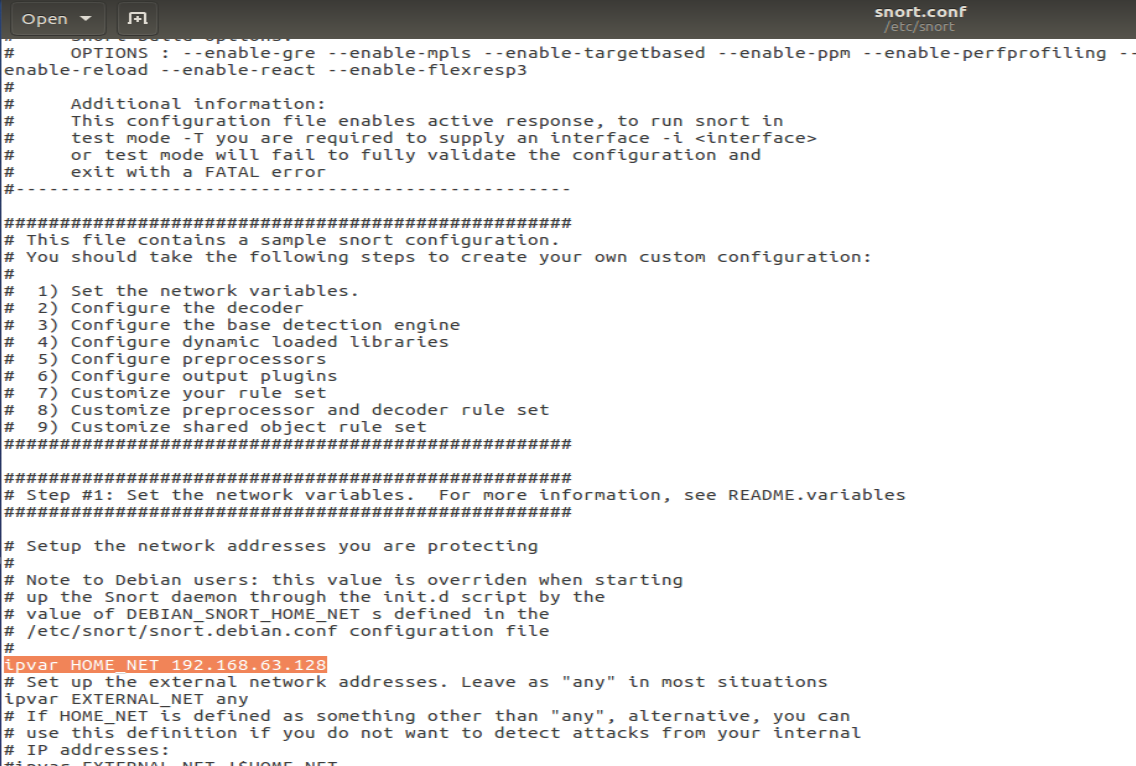


1. **Snort IDS**

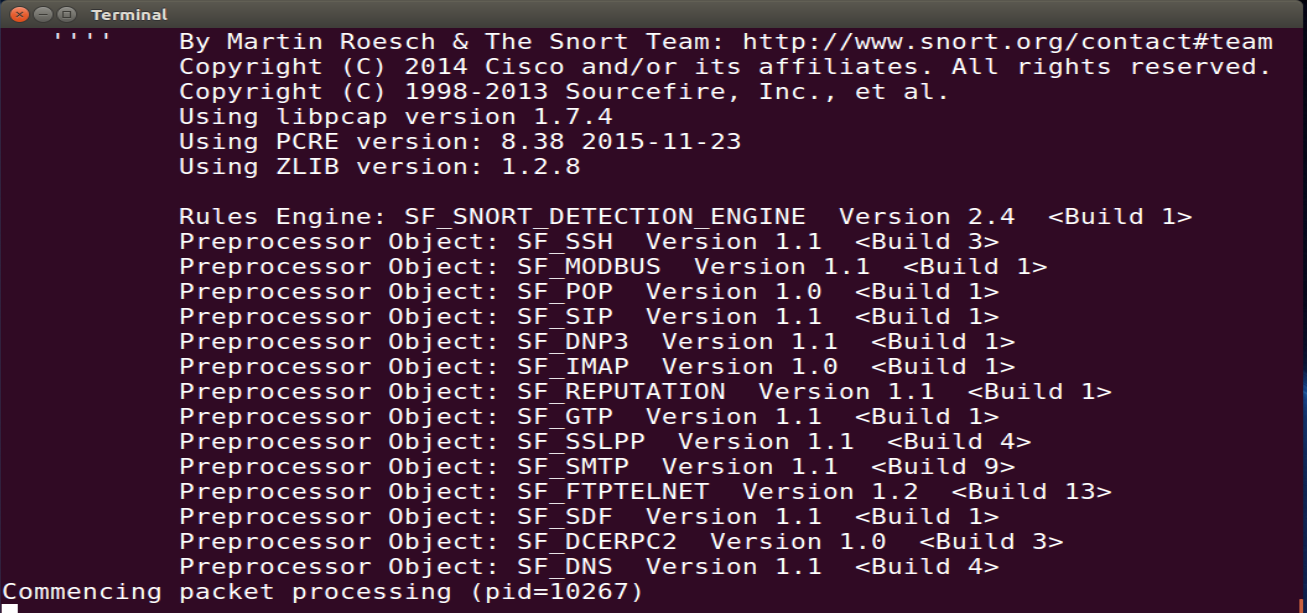
***Bước 1. Cài đặt snort***



***Bước 2. Tiến hành cấu hình cho snort ở file snort.conf. Sử dụng IP của máy ubuntu.***

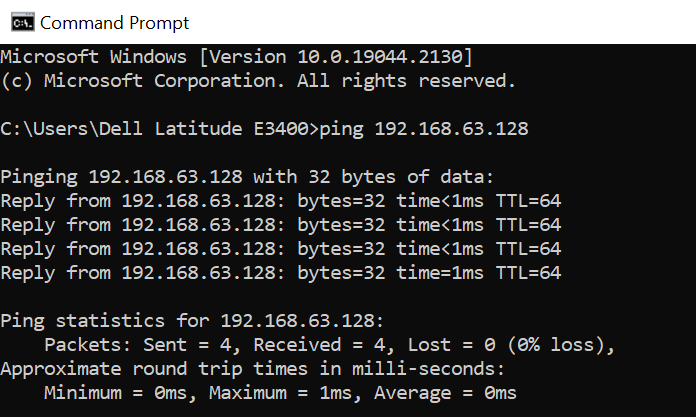


***Bước 3. Bật mode IDS bằng lệnh sudo snort -A console -i ens33 -c /etc/snort/snort.conf***

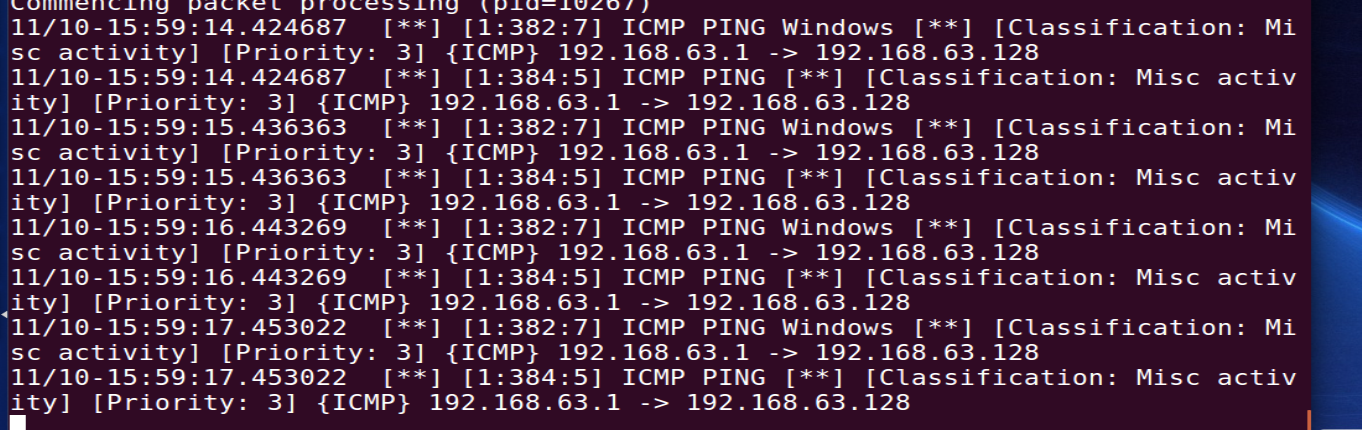


***Bước 4. Kiểm tra hoạt động của Snort***

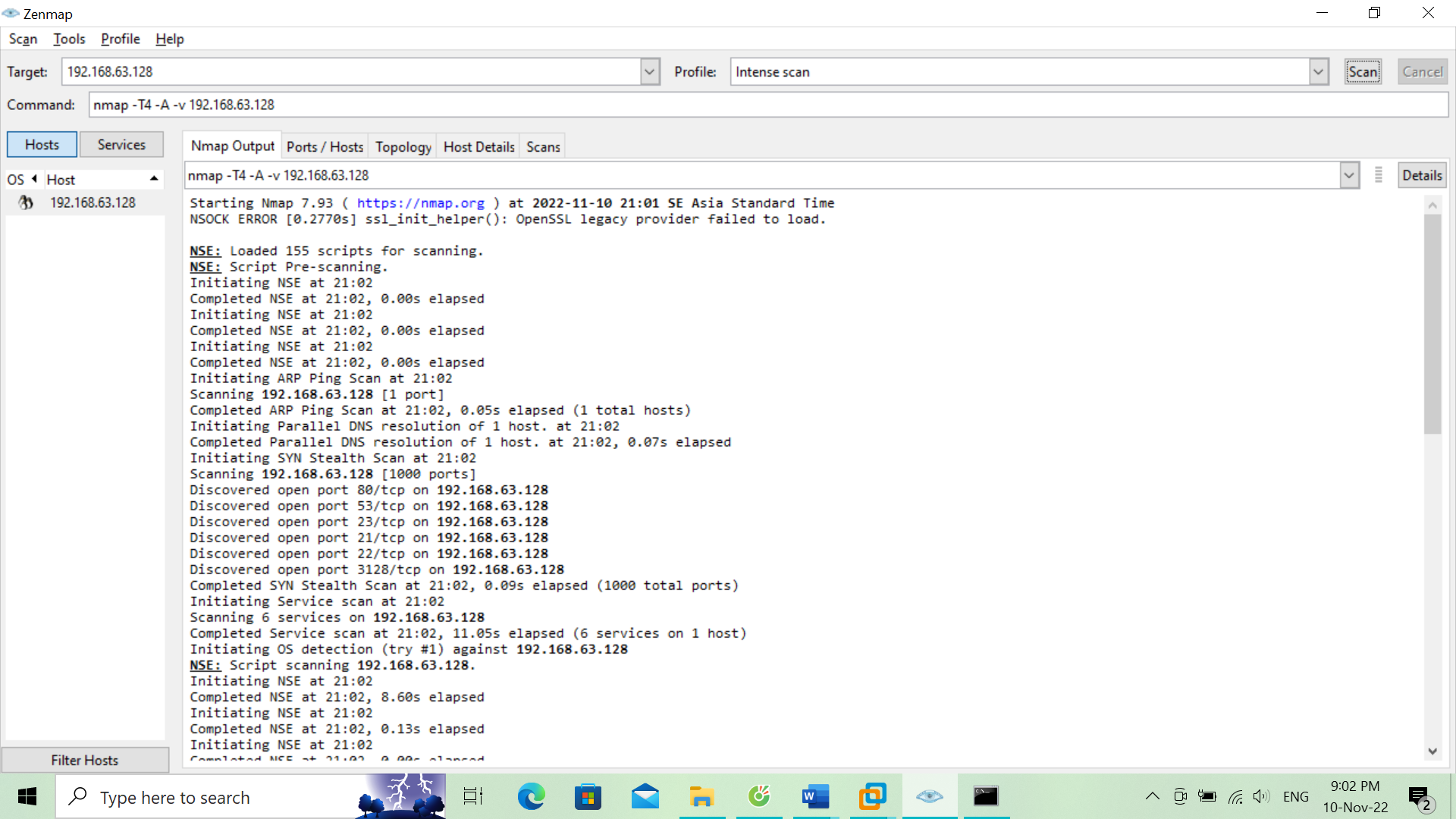
* Ta tiến hành ping từ máy thực sang máy ảo ubuntu.



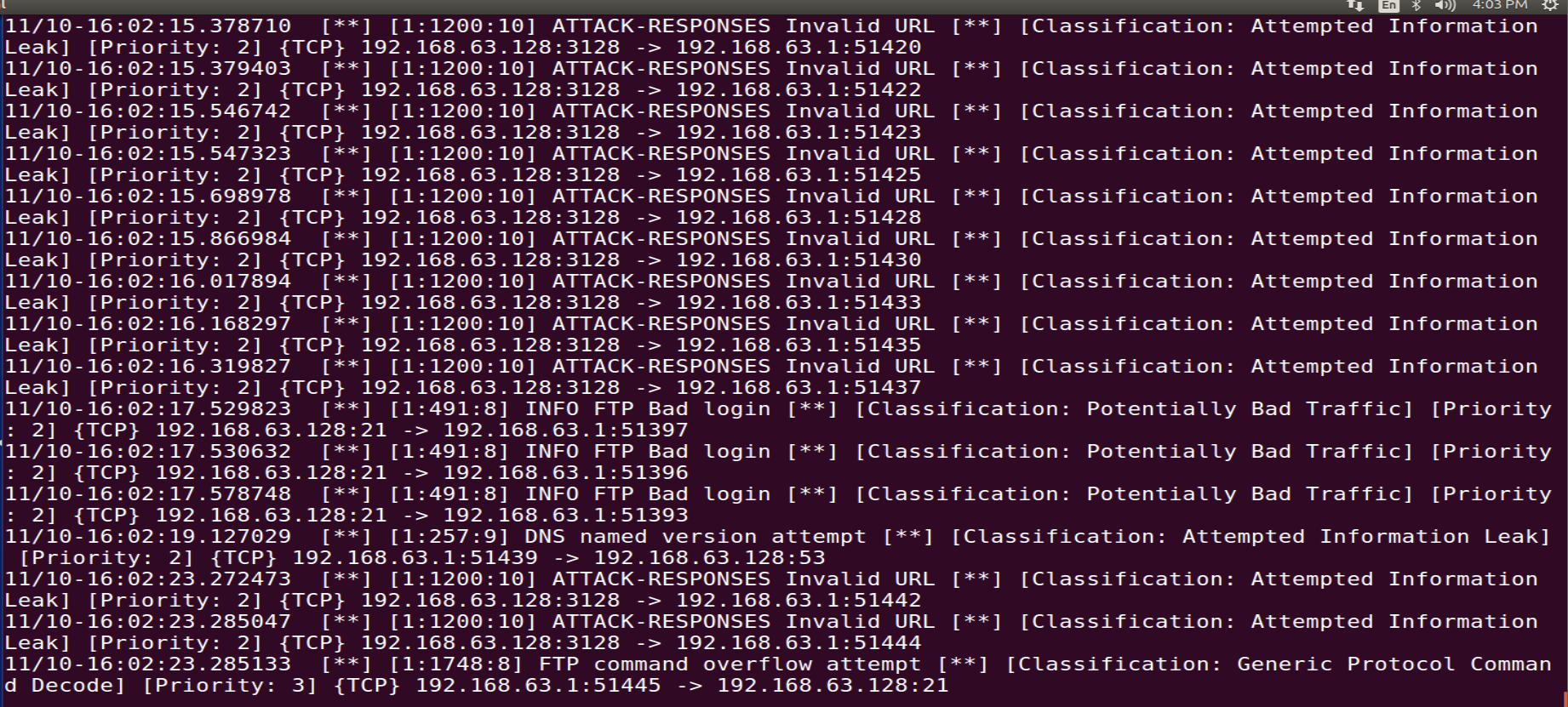
* Kết quả là snort phát hiện ra được lệnh ping



* Tiến hành scan ubuntu bằng nmap



* Kết quả là snort phát hiện ra việc scan



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