**AN NINH MÁY TÍNH**

**Lab03 – LAN Security**

Sinh viên:

**Đỗ Trọng Nghĩa - 18120477**

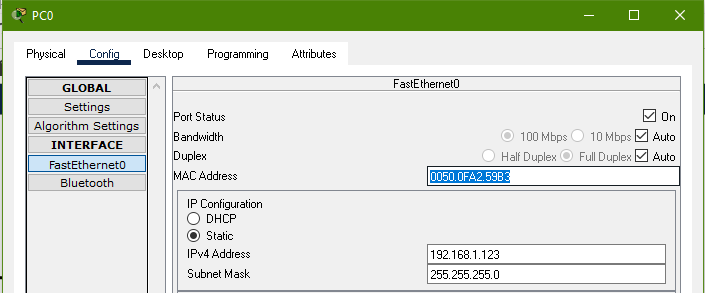
C:\Users\tdqua_000\Dropbox\SS-Slides\DeCuong-CDIO\Template CDIO v4.2\Templates\Hinh anh\LogoTruong.png

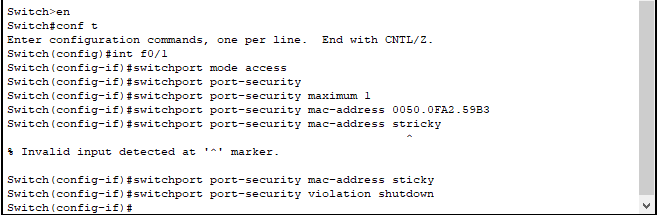
Khoa Công nghệ Thông tin

Đại học Khoa học Tự nhiên TP HCM

1. Port Security
   1. Mô hình mạng



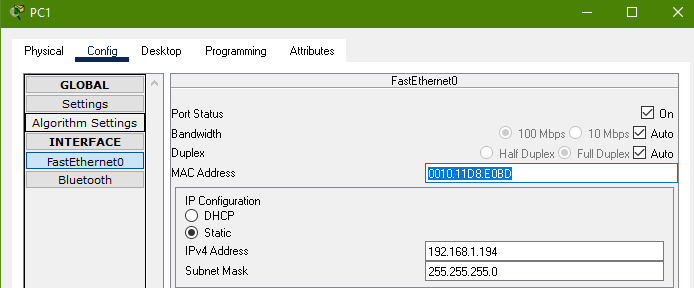
* 1. Cấu hình
* Địa chỉ MAC và IP máy PC0
* Cấu hình ở Switch với interface tương ứng làm port security

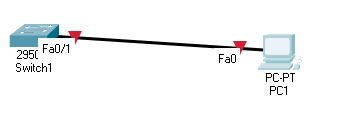


* 1. Nối dây PC
* Nối PC0 với địa chỉ MAC ứng với port security f0/1 => Thành công

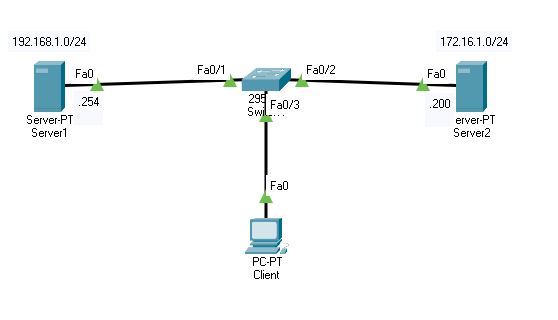


* Nối PC1 với địa chỉ MAC chưa được cài đặt trên port security => Thất bại
  + Thông tin máy PC1

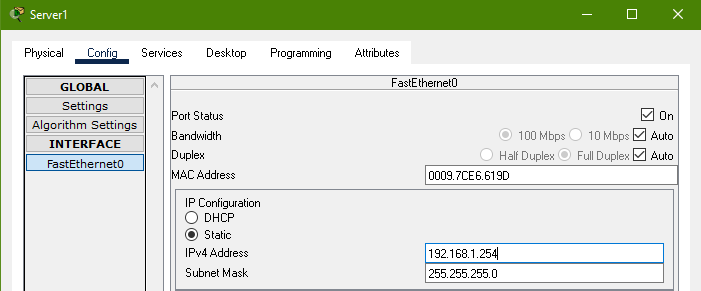


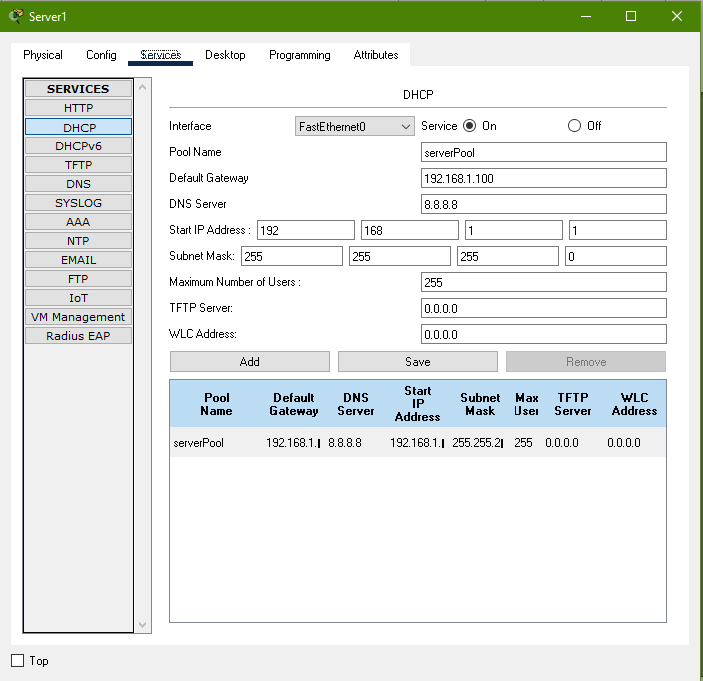


1. DHCP Snooping
   1. Mô hình mạng

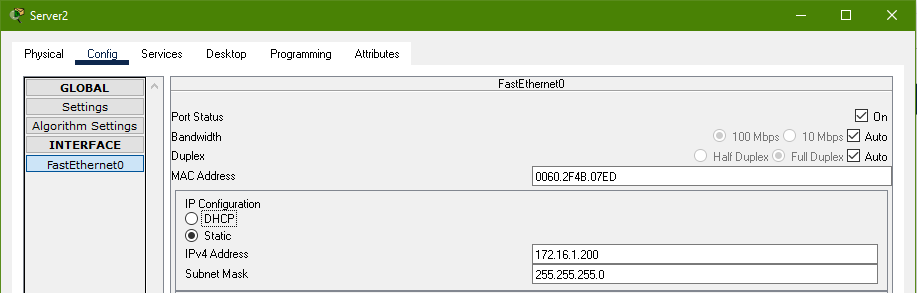


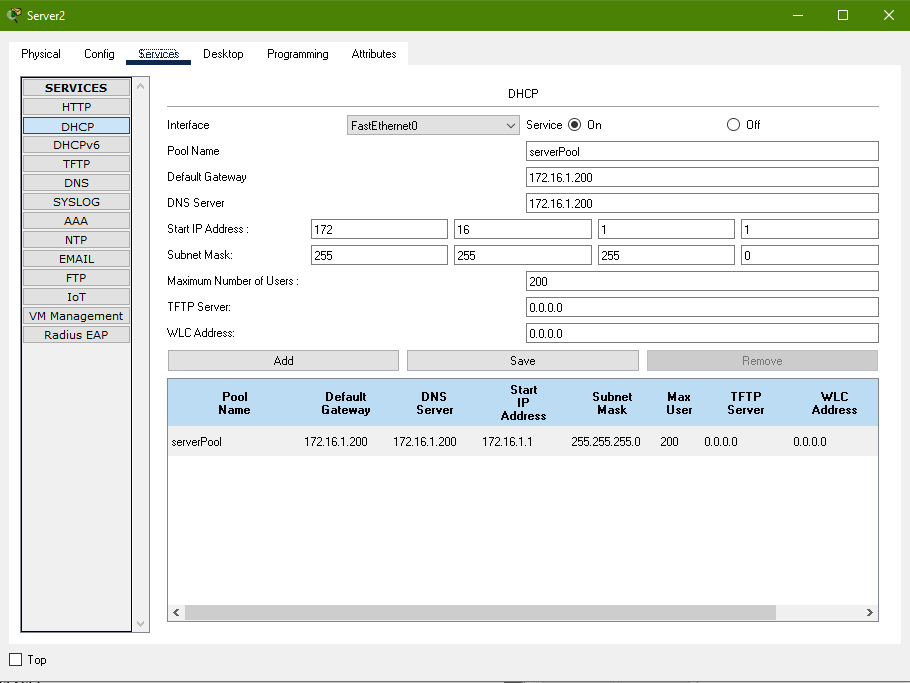
* 1. Cấu hình DHCP server
     1. DHCP Server1 (server giả)



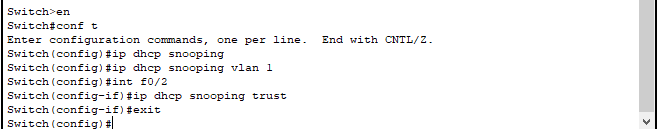


* + 1. Trên Server2 (server thật)

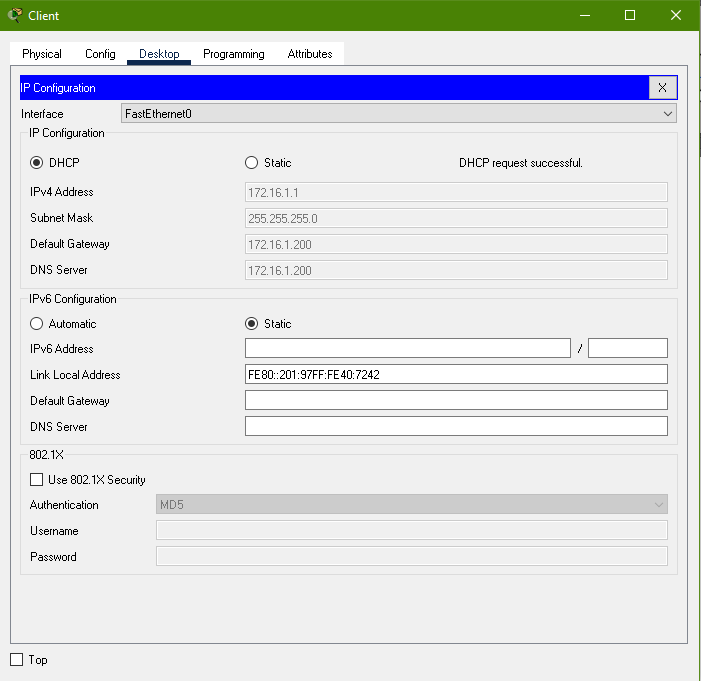




* + 1. Trên Switch



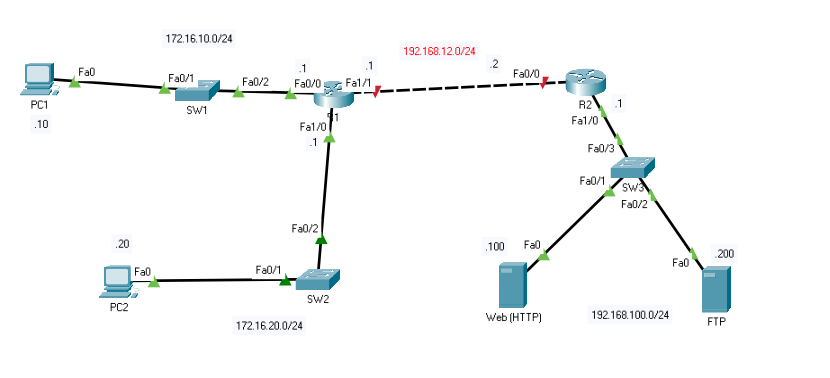
* 1. Kiểm tra
* Client request IP đến DHCP Server2 thành công (Server thật)



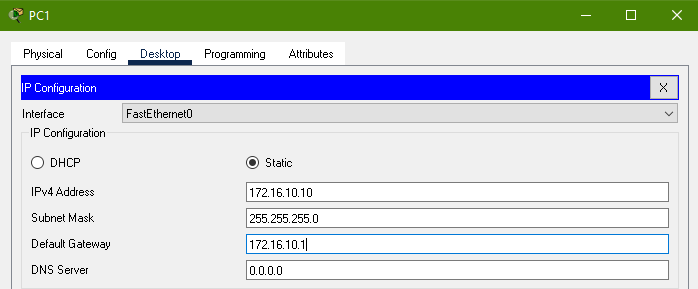
* Kiểm tra các cài đặt trên switch



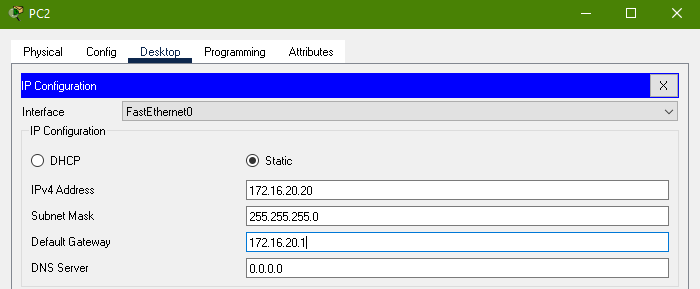
1. ACL
   1. Sơ đồ mạng



* 1. Cấu hình định tuyến theo mô hình mạng
     1. Set các địa chỉ IP tĩnh cho các PC và Server
* PC1

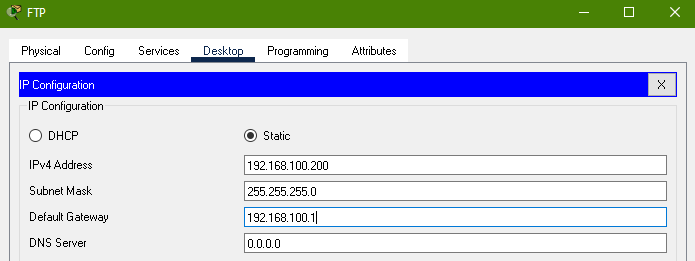


* PC2



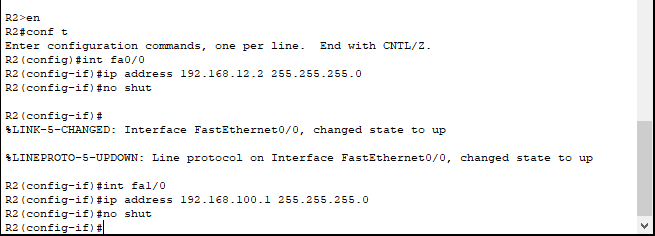
* Web (HTTP)



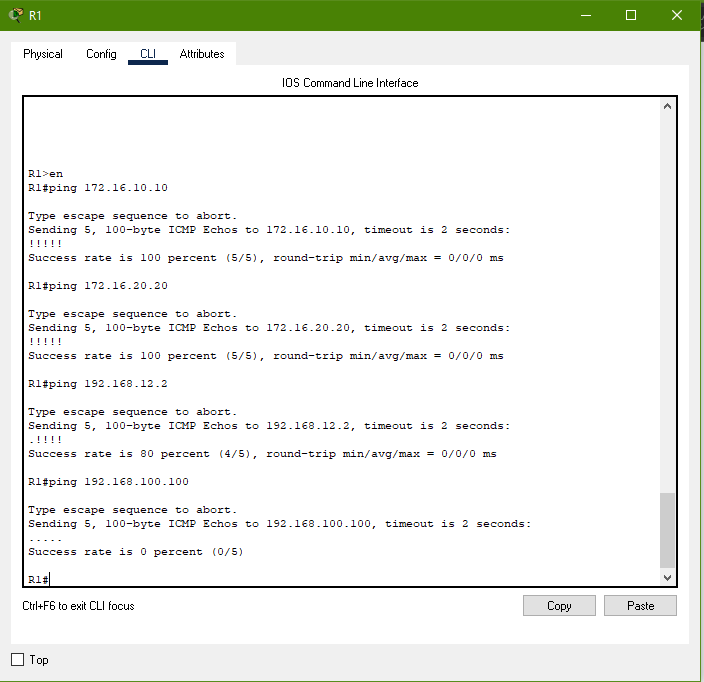
* FTP
  + 1. Cấu hình trên Router
* R1



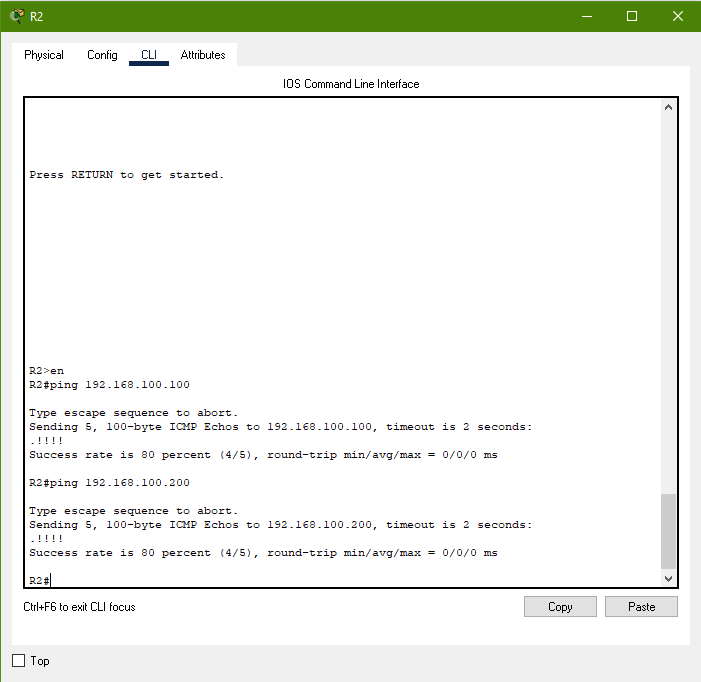
* R2



* R1 ping PC0, PC1, R2, Web (Web bị fail)



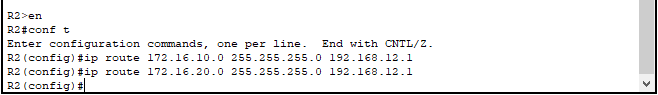
* R2 ping Web và FTP



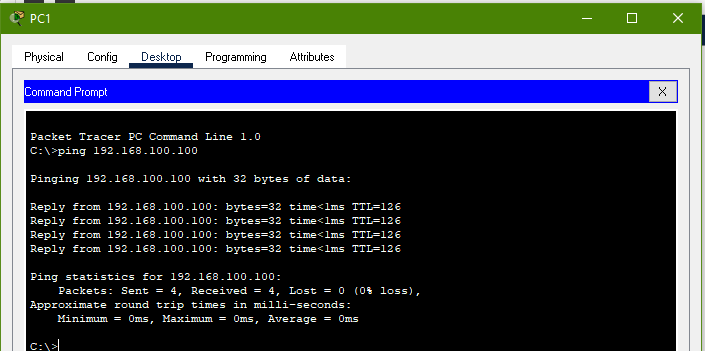
* + 1. Cấu hình định tuyến tĩnh
* Định tuyến trên R1



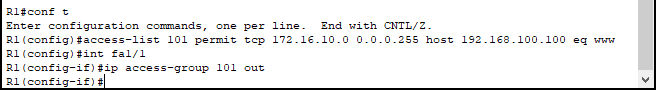
* Tương tự trên Router R2



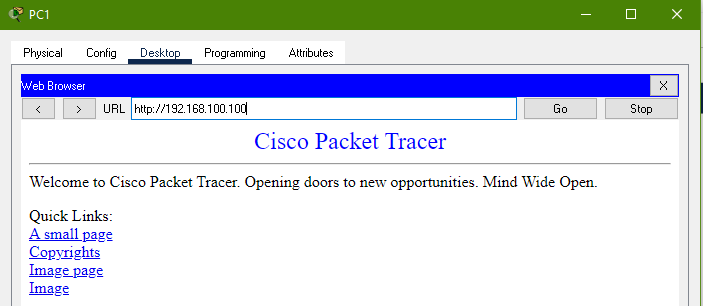
* + 1. Kiểm tra PC1 xem đã kết nối đến Web Server hay chưa
* Ping thành công => có kết nối



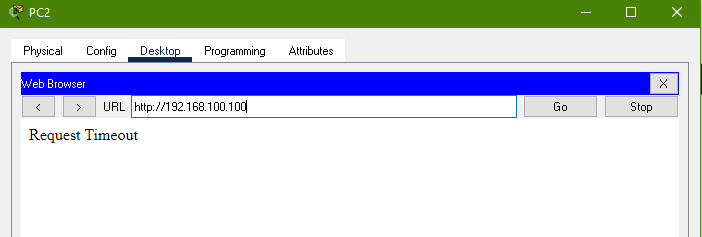
* 1. Cấu hình ACL
     1. Chỉ cho phép các PC thuộc mạng 172.16.10.0/24 truy cập tới Web server bằng dịch vụ Web (HTTP)
* Cấu hình trên R1



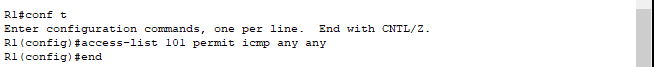
* Kiểm tra PC1 => duyệt được web



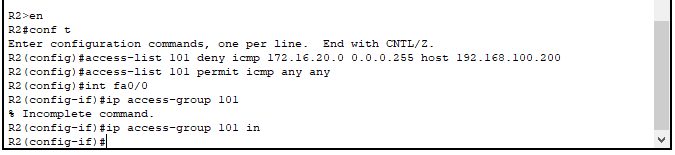
* PC2 => không duyệt được



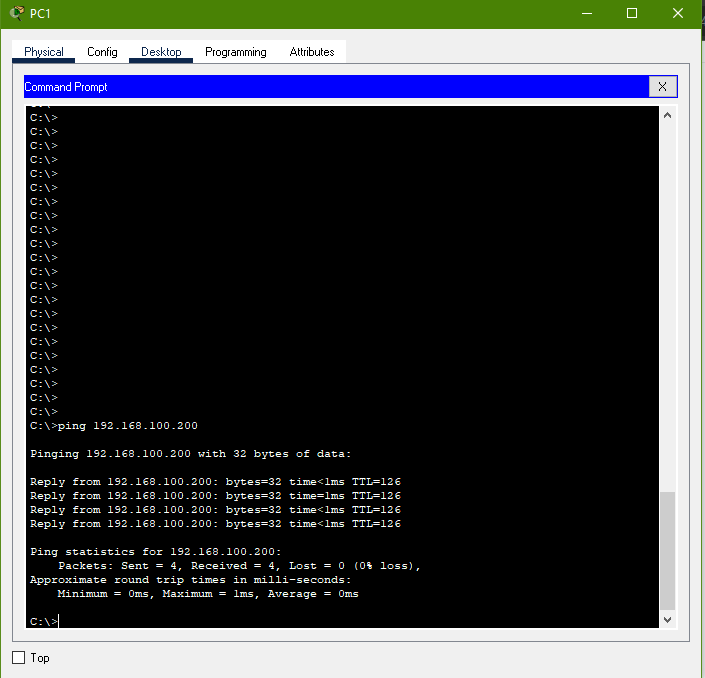
* + 1. Cấm PC ping tới FTP server (192.168.100.200)
* Cấu hình trên R1



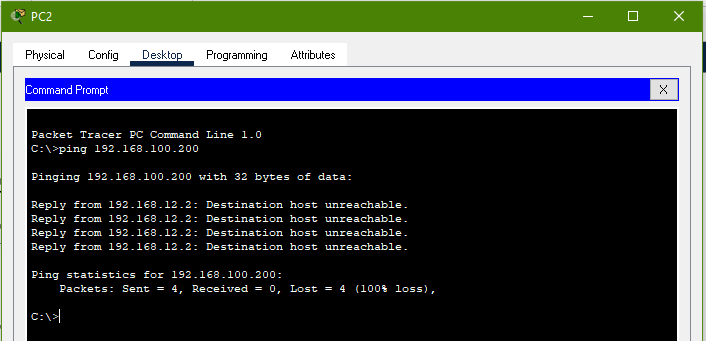
* Cấu hình trên R2



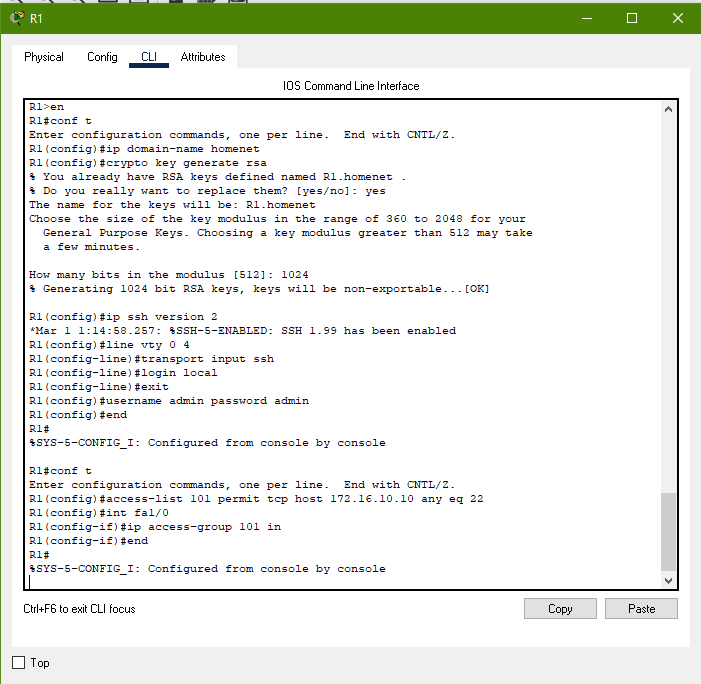
* PC1 (172.16.10.10) có thể ping được ftp server (192.168.100.200)



* PC2 (192.168.11.20) không ping được ftp server (192.168.100.200)
* PC2 không ping được (Destination host unreachable)



* + 1. Chỉ cho phép máy Admin (172.16.10.10) telnet/SSH tới các router (R1, R2) và các Switch
* Cấu hình SSH trên **R1**

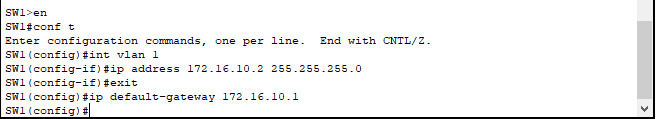


* Theo file hướng dẫn thì chỉ cần tới đây là đủ, các phần cấu hình SSH cho các thiết bị khác là em làm thêm
* Tương tự trên **R2**

Graphical user interface, text, application, email

Description automatically generated

* Đối với Switch cần set IP management và default gateway đối với IP management
* **SW1**: 172.16.10.2, default gateway: 172.16.10.1

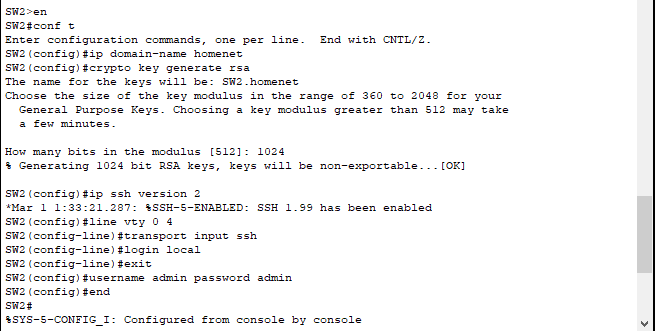


Graphical user interface, text, application, email

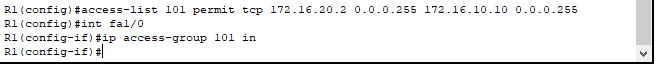
Description automatically generated

* **SW2**:172.16.20.2, default gateway: 172.16.20.1

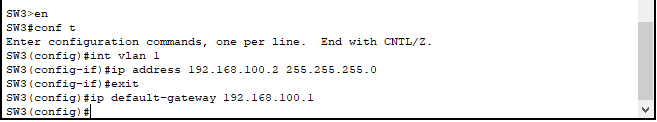


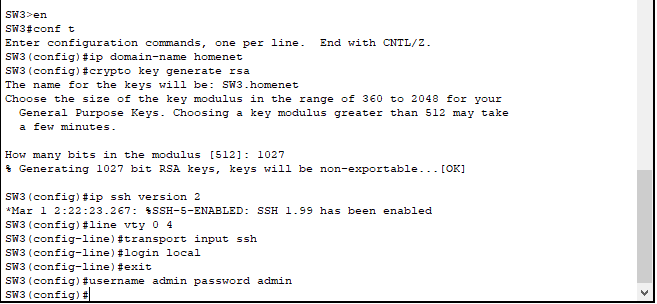


* Tại R1, ta cho phép địa chỉ IP management của SW2 được kết nối với giao thức là TCP với máy admin

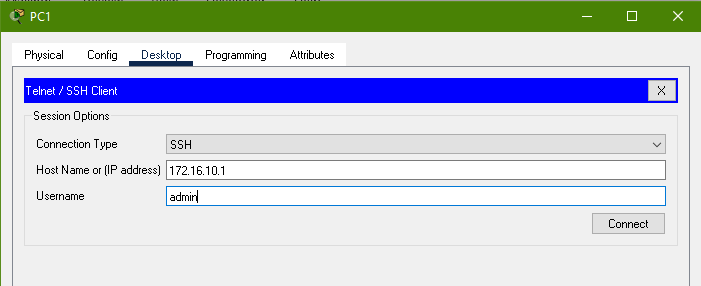


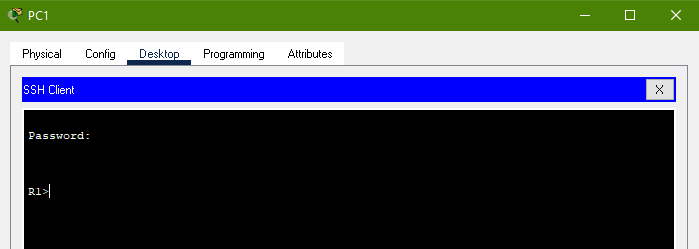
* **SW3**: 192.168.100.2, default gateway: 192.168.100.1



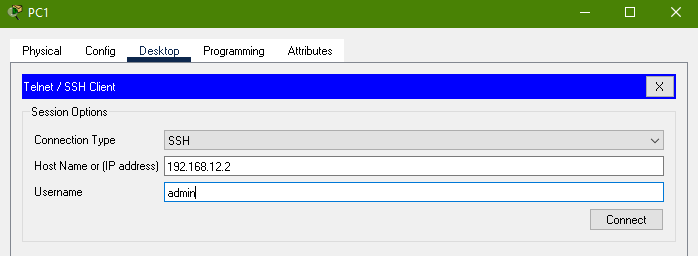


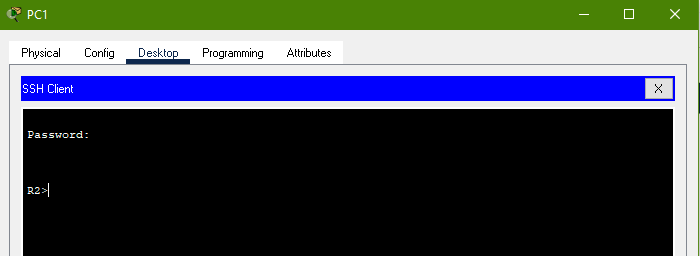
* + 1. Kiểm tra SSH đối với PC1
* Kiểm tra trên PC1 (172.16.10.10) đã có thể SSH tới R1



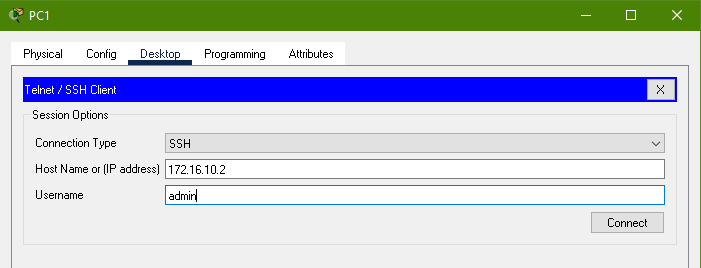


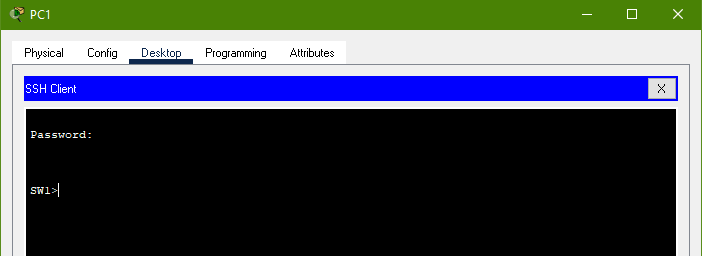
* Kiểm tra PC1 cũng SSH được dến R2



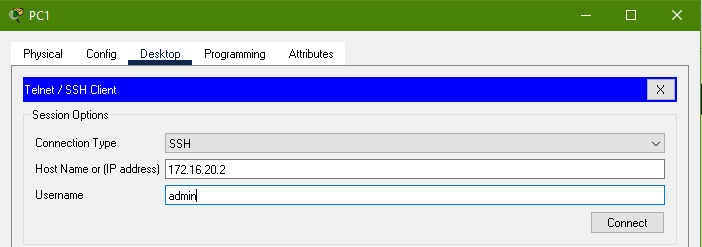


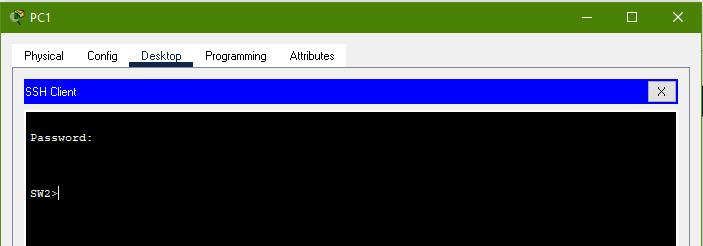
* Kiểm tra PC1 SSH được tới SW1



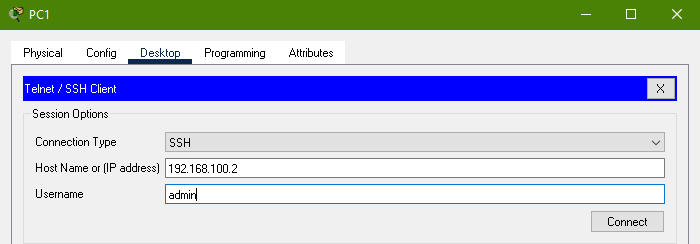


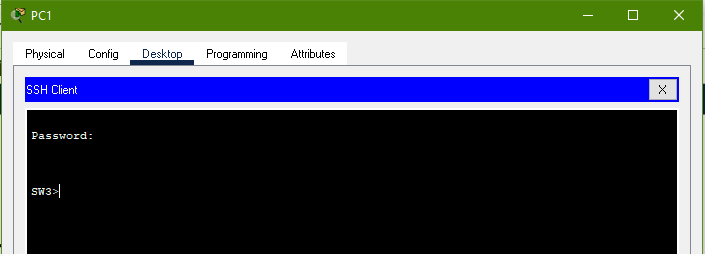
* PC1 SSH được đến SW2



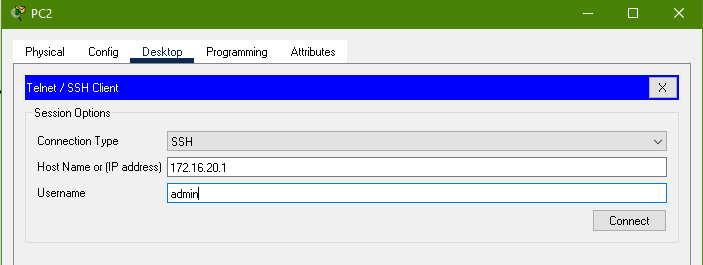


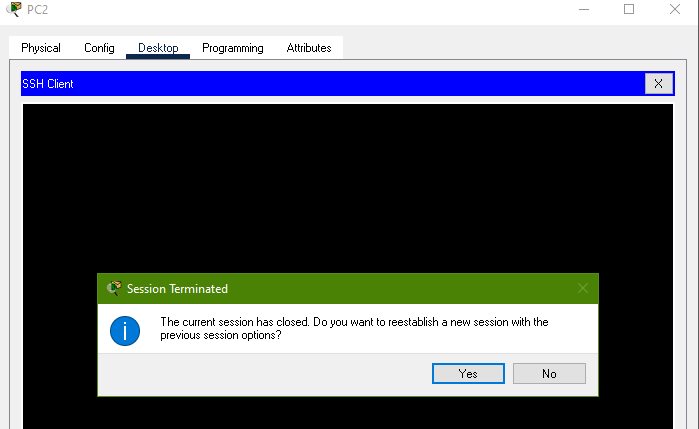
* PC1 SSH được đến SW3



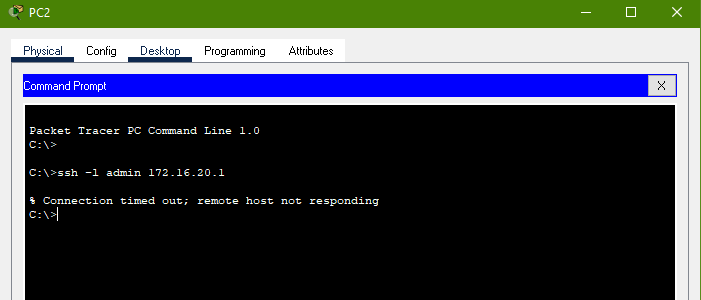


* + 1. Kiểm tra SSH đối với PC2
* Kiểm tra trên PC2 (172.16.20.20) không thể SSH tới R1

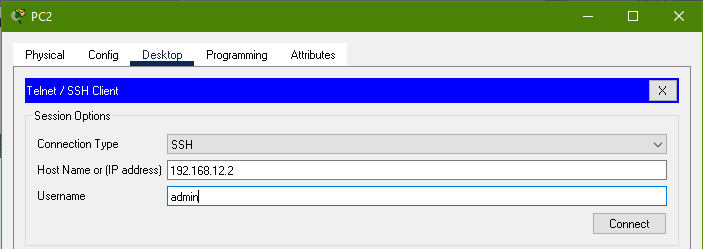


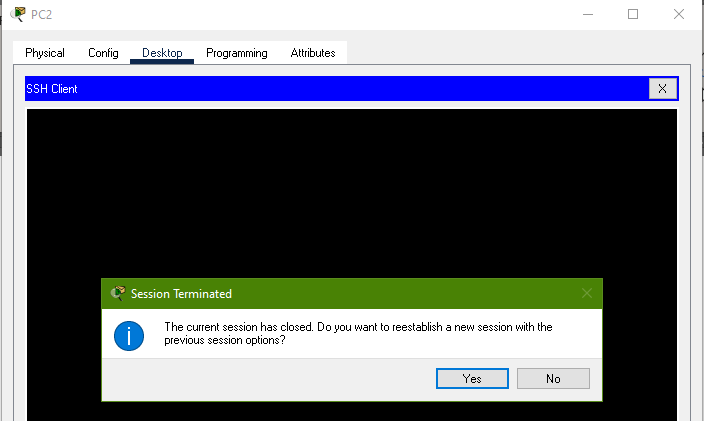


* Dùng Terminal để SSH cũng không được

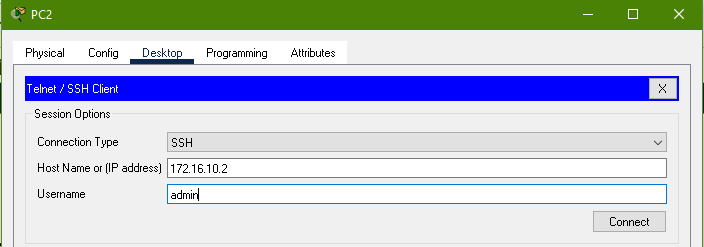


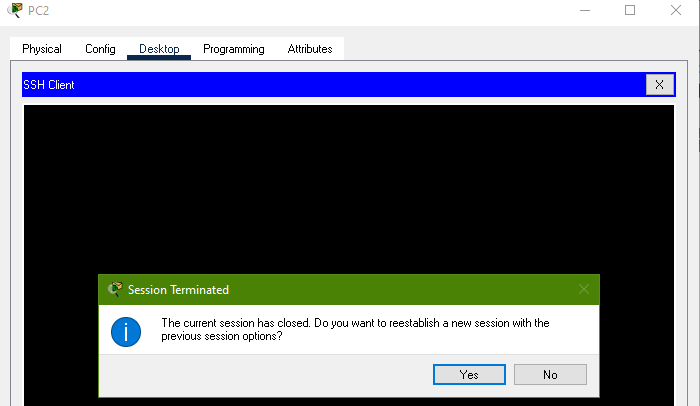
* Kiểm tra PC2 cũng không SSH được tới R2





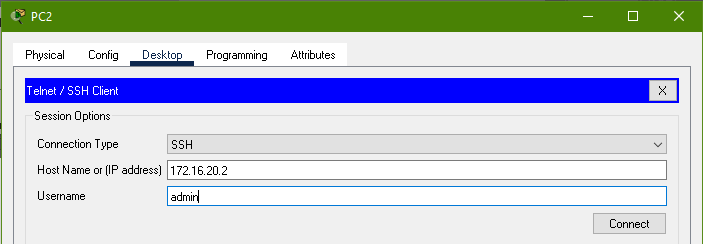
* Kiểm tra PC2 không thể SSH đến SW1





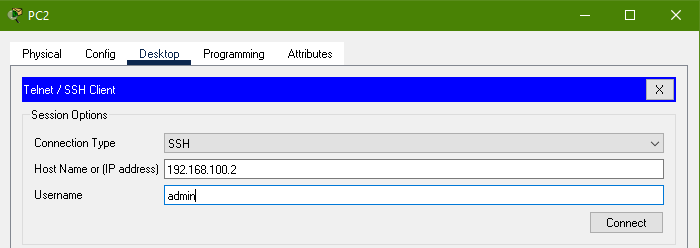
* PC2 SSH được đến SW2

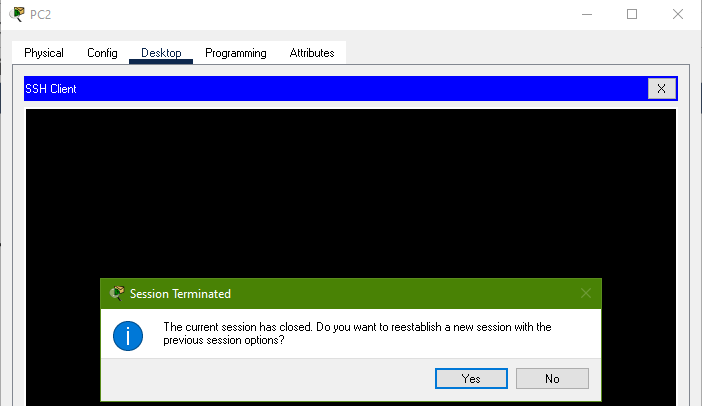
*Vì đề bài cho dùng Switch (Layer 2) nên không thể thao tác với địa chỉ IP và protocol (Layer 3) (tạo access-list rồi bind vào cổng interface bằng phương thức access-group) nên rất khó để chặn phương thức và địa chỉ của PC2 (172.16.20.20), PC2 cũng SSH được đến SW2. Ta có thể dùng phương thức port security như trong câu 1 nhưng như vậy thì coi như PC2 không vào mạng Internet được nên em cảm thấy không hợp lý. Theo như em tìm hiểu thêm trên mạng thì tạo mac access-list nhưng phải đổi các thiết bị khác. Em thầy giải đáp giúp em phần này ạ. Em xin cảm ơn ạ.*





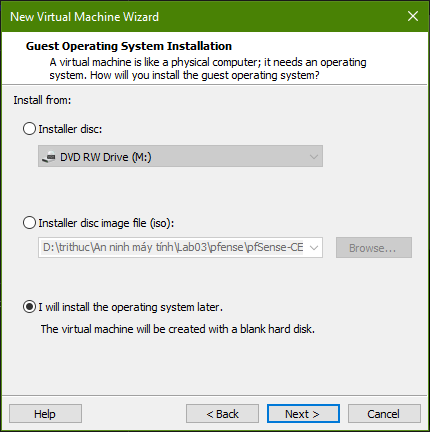
* PC2 không SSH được tới SW3



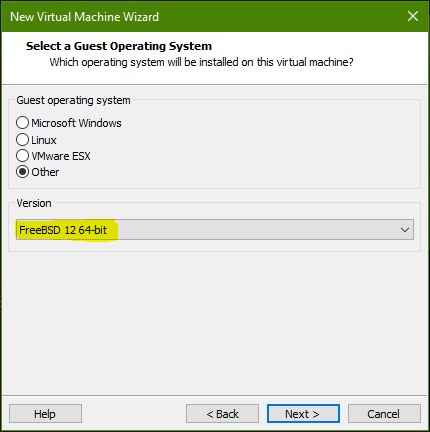


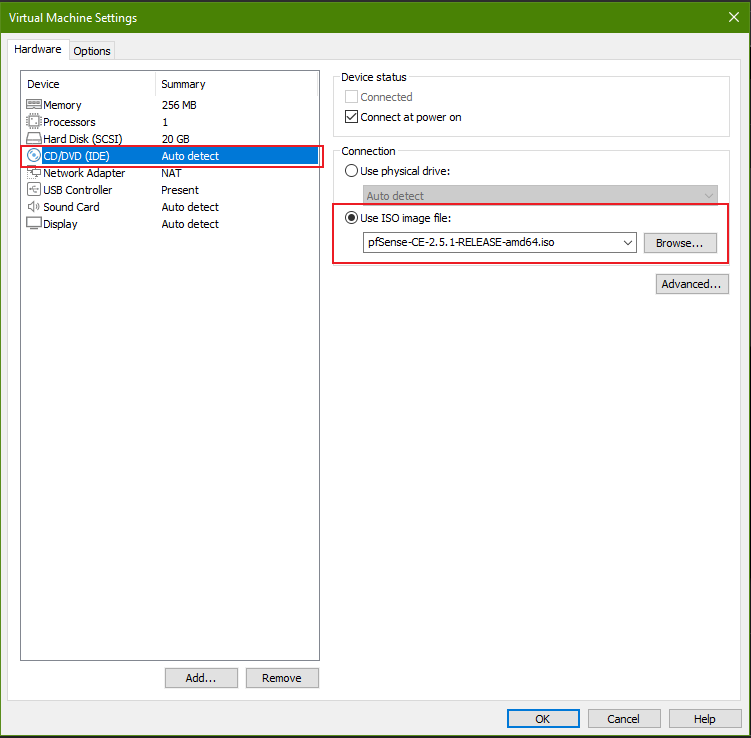
1. Firewall

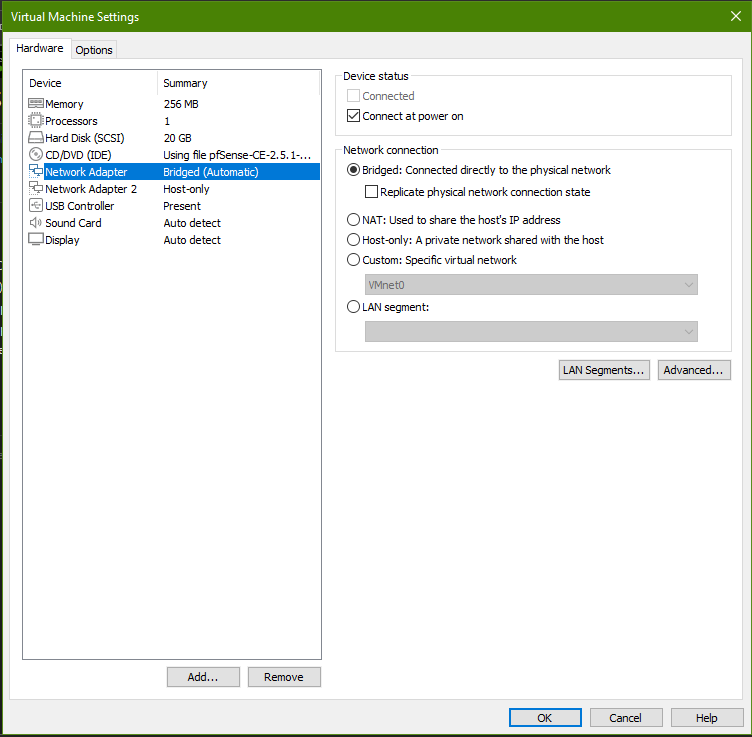
* Chọn Firewall dạng Vmware là pfSense
  1. Cài đặt
     1. Máy cài đặt pfSense
* Tạo một máy ảo mới trên Vmware, chưa cần thêm file .iso



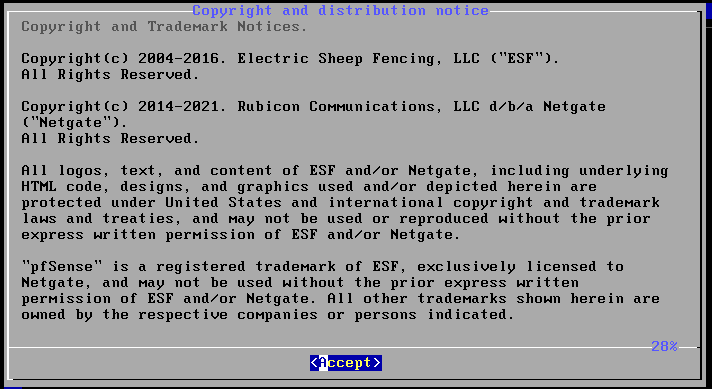
* Chọn version là FreeBSD 64-bit

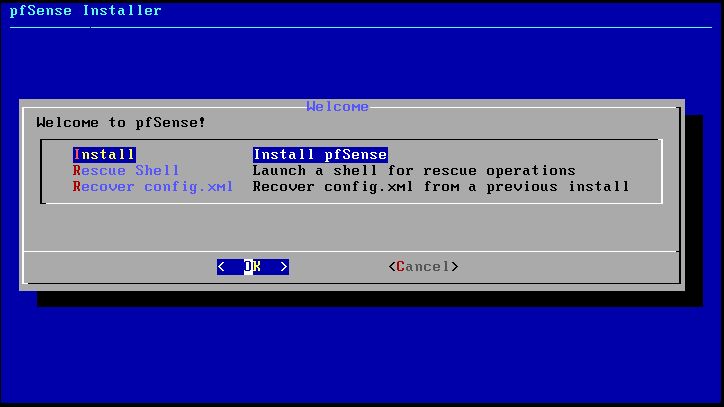


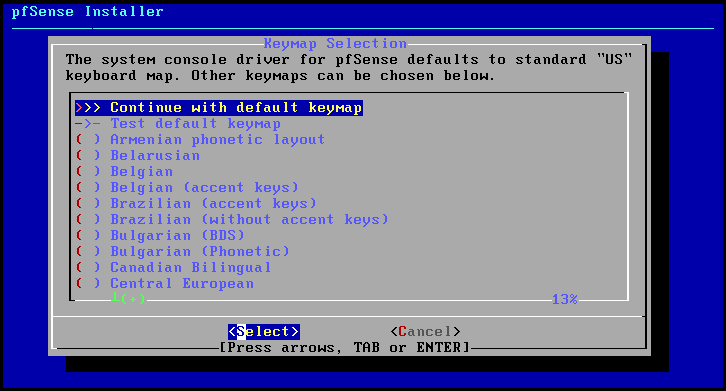
* Sau đó tiến hành cài đặt mặc định máy ảo
* Khi cải đặt xong, chọn **Edit virutal machine settings** và thêm file .iso cài đặt vào
* Thêm một card mạng mới với các chế độ là **Bridged** và **Host-only**, đối với Vmnet1 (Host-only thì không cần kết nối với máy host, chì cần để các máy ảo kết nối với nhau)

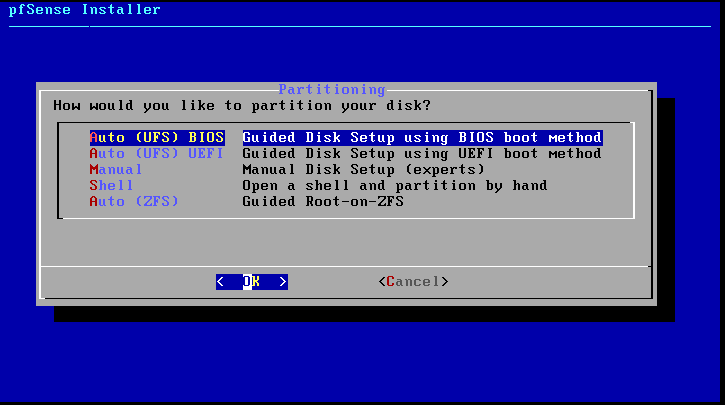


* Tiến hành cài đặt mặc định pfSense

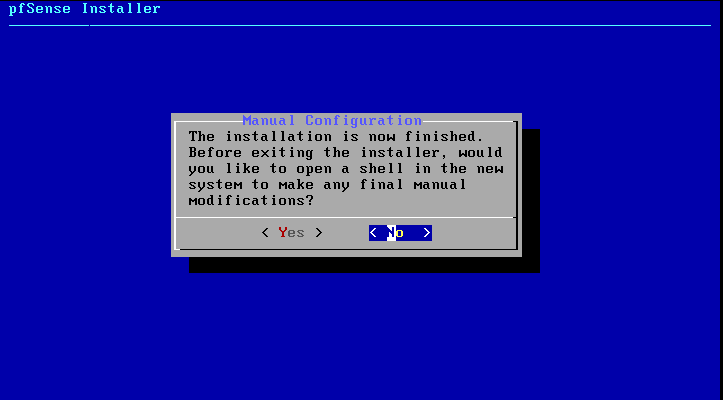




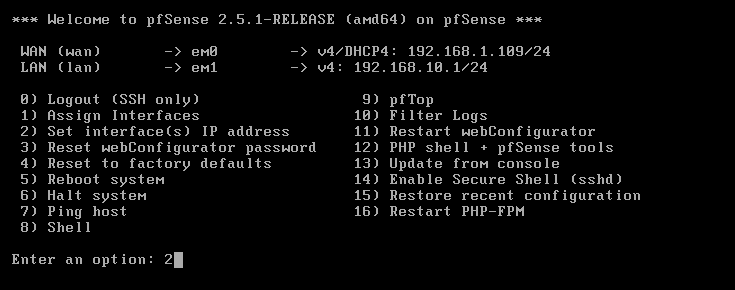




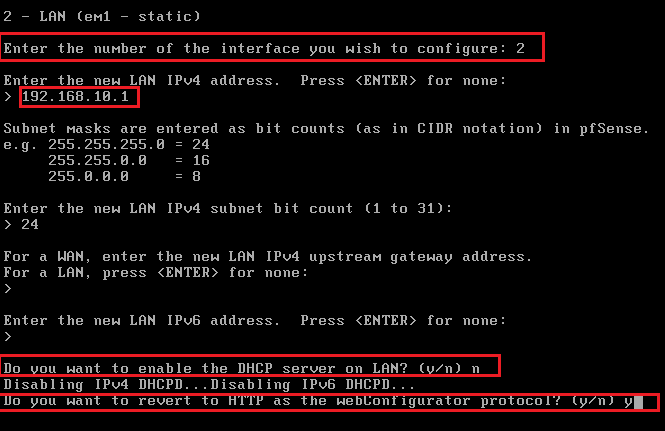
* Chọn **No** và tiến hành Reboot



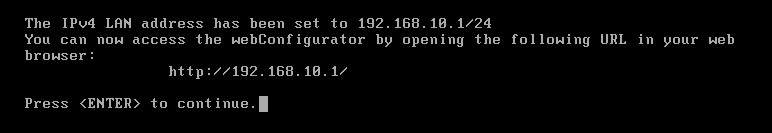
* Chọn 2 để cấu hình cho card mạng Host-only



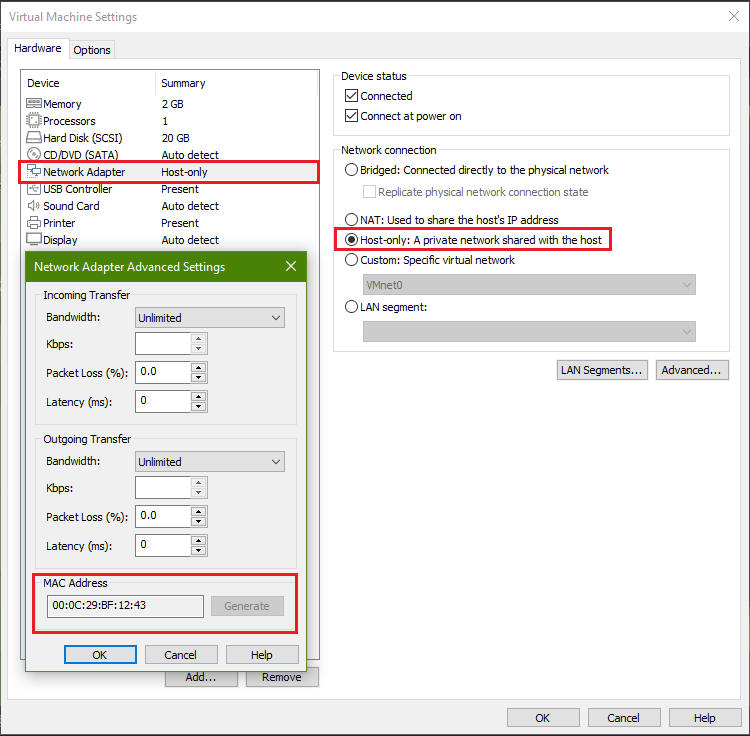
* Nhập địa chỉ IP là 192.168.10.0 (cho Host-only network)



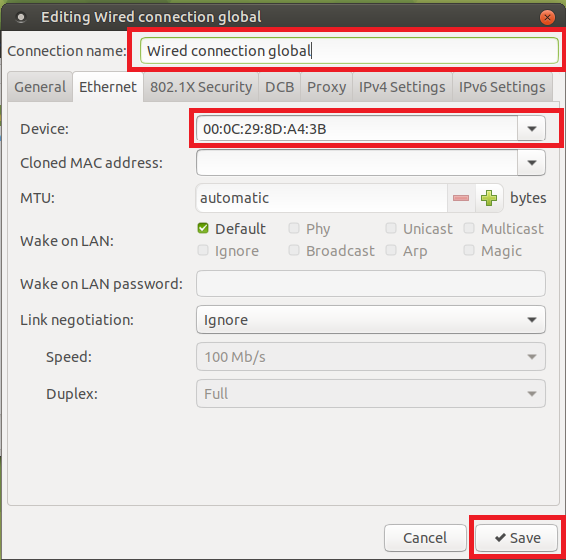
* Địa chỉa IP cho card mạng Host-only đã được set

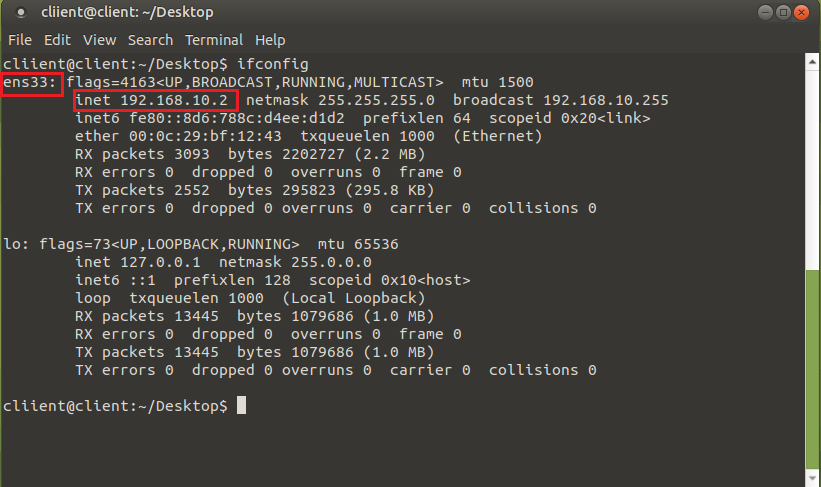


* + 1. Cài đặt cho máy client (Ubuntu mate – 18.04)
* Chỉ cần một card mạng với chế độ kết nối là Host-only.

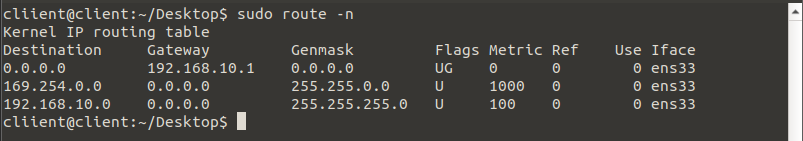


* Chọn card và set địa chỉ IP là 192.168.10.2 trong mạng Host-only

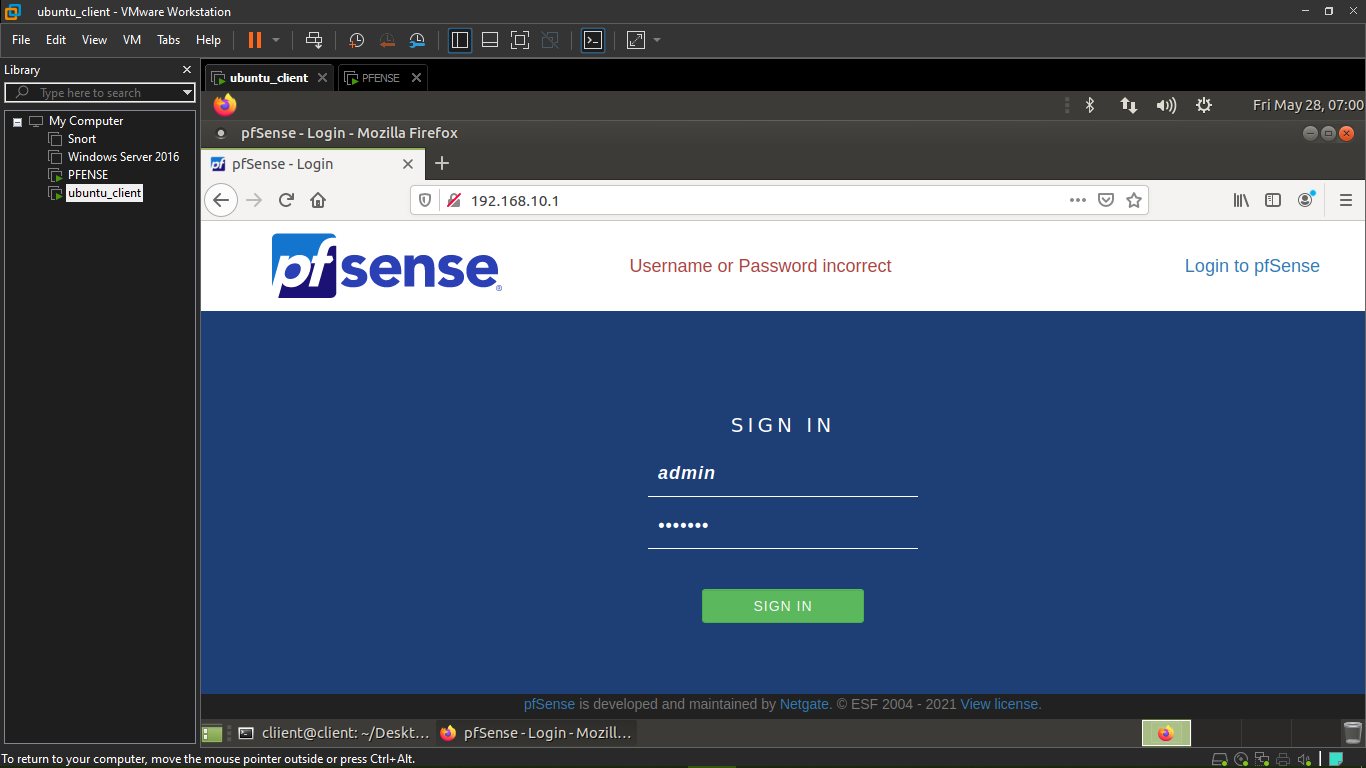


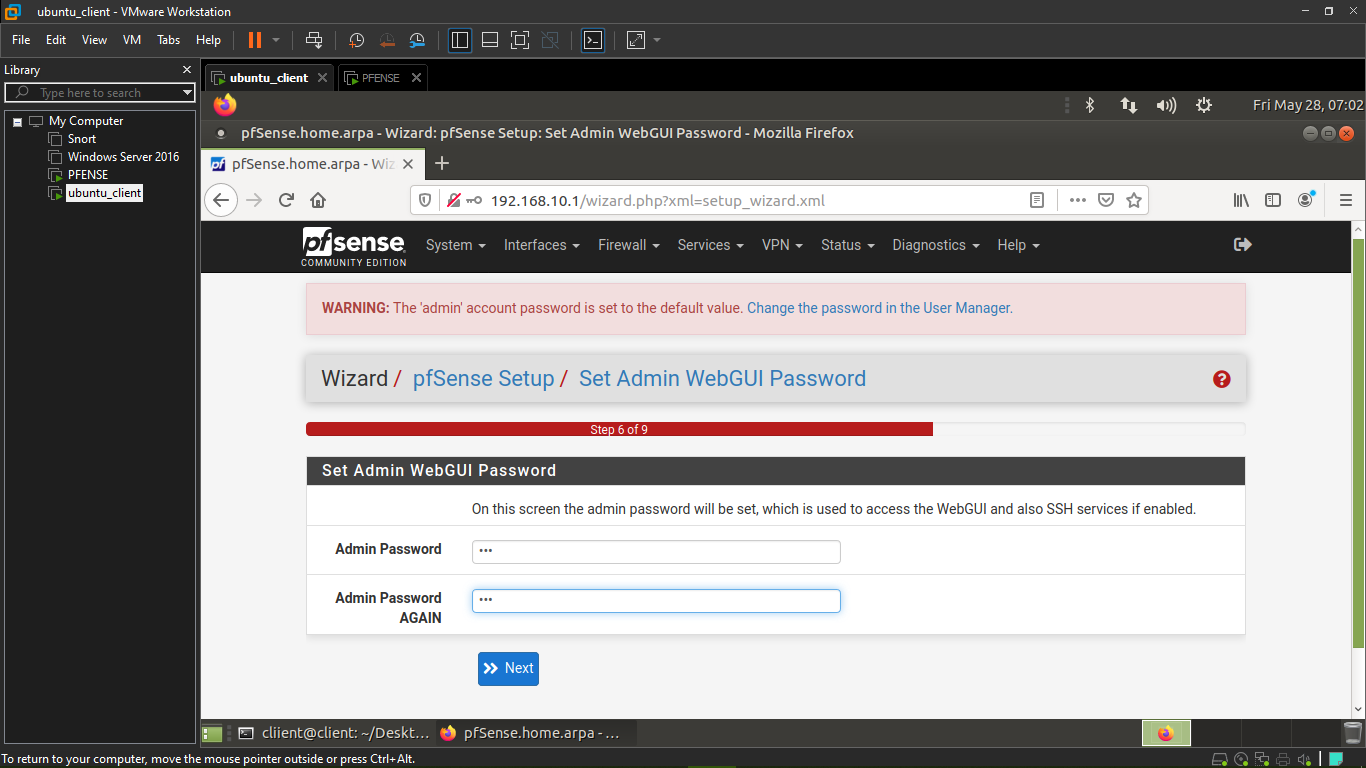


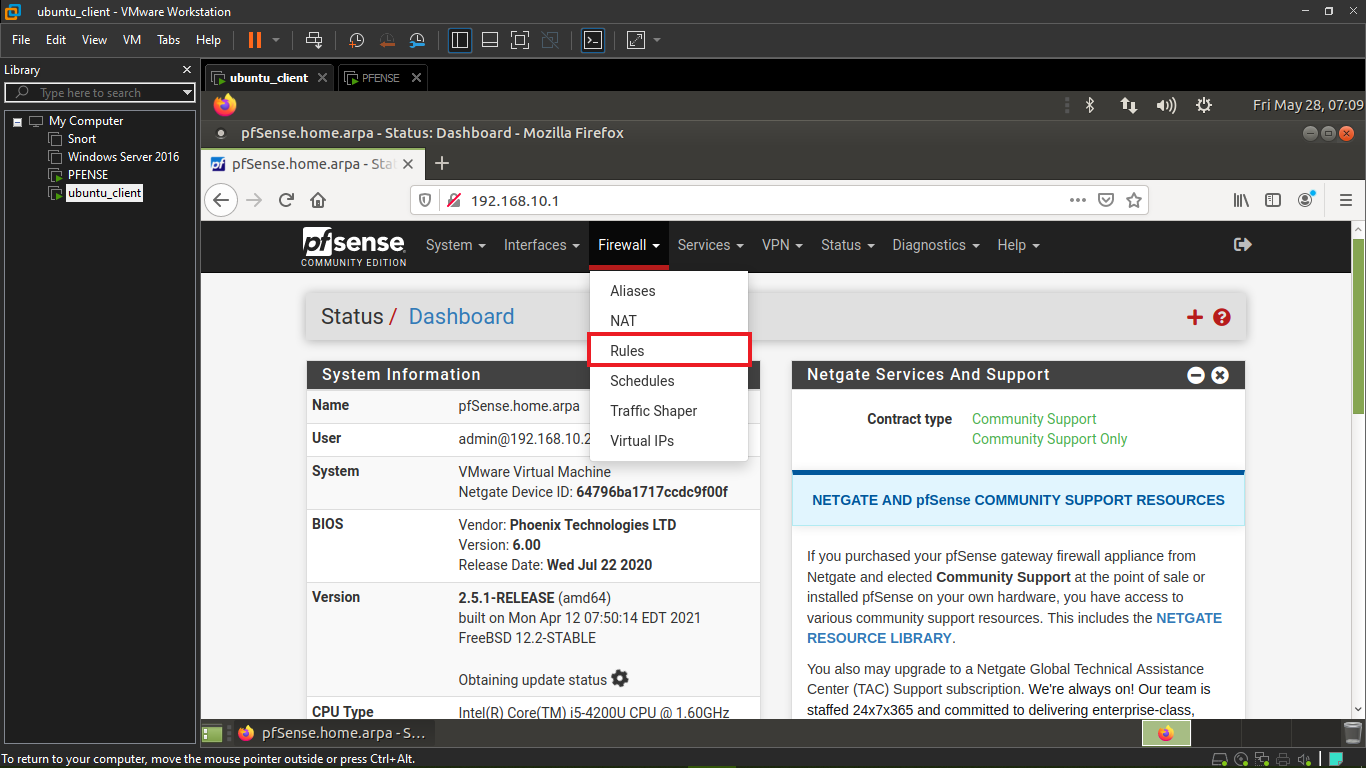
* Route cho default gateway là địa chỉ IP của máy pfSense trong đường mạng Host-only

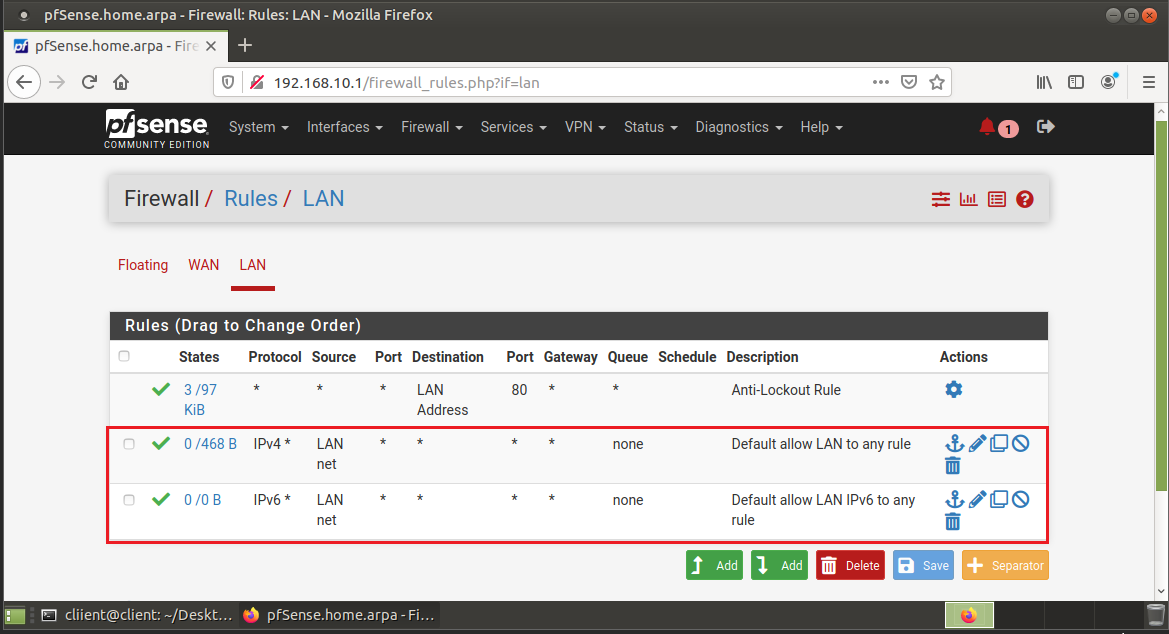


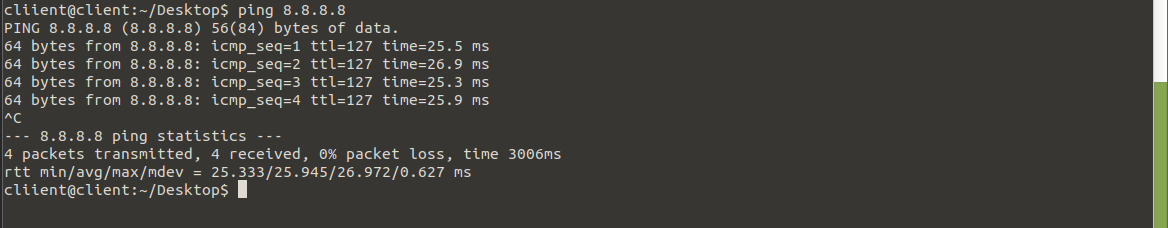
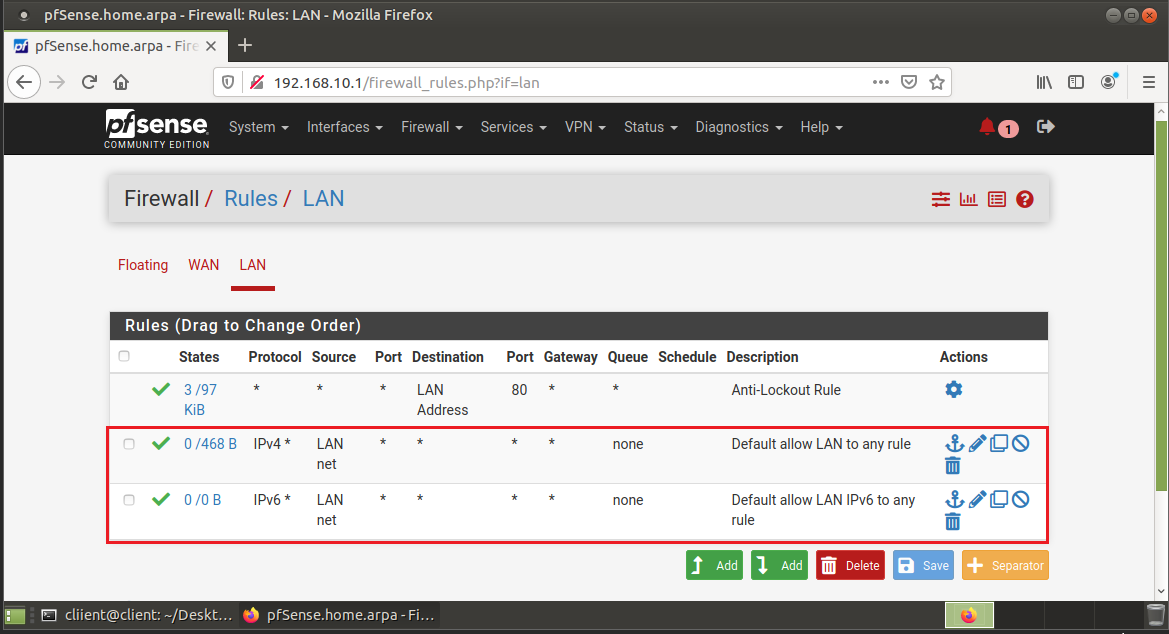
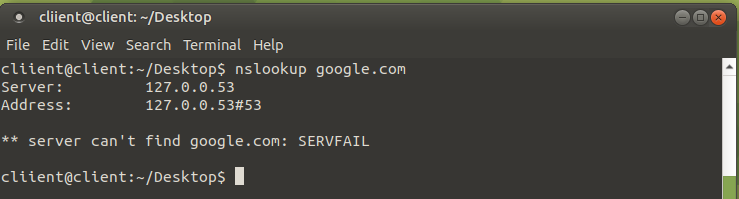
* 1. Thực hiện các rule (đều ở trên máy Client)
* Vào trình duyệt và truy cập 192.168.10.1 (địa chỉ IP của máy pfSense trong đường mạng Host-only). Username: admin, Password: pfSense

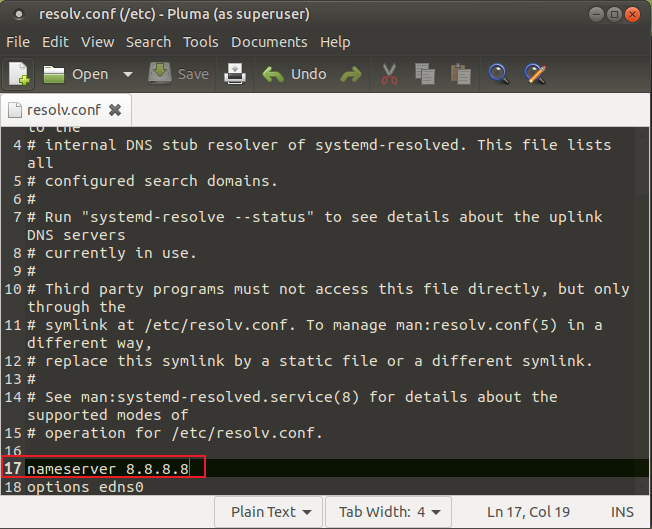


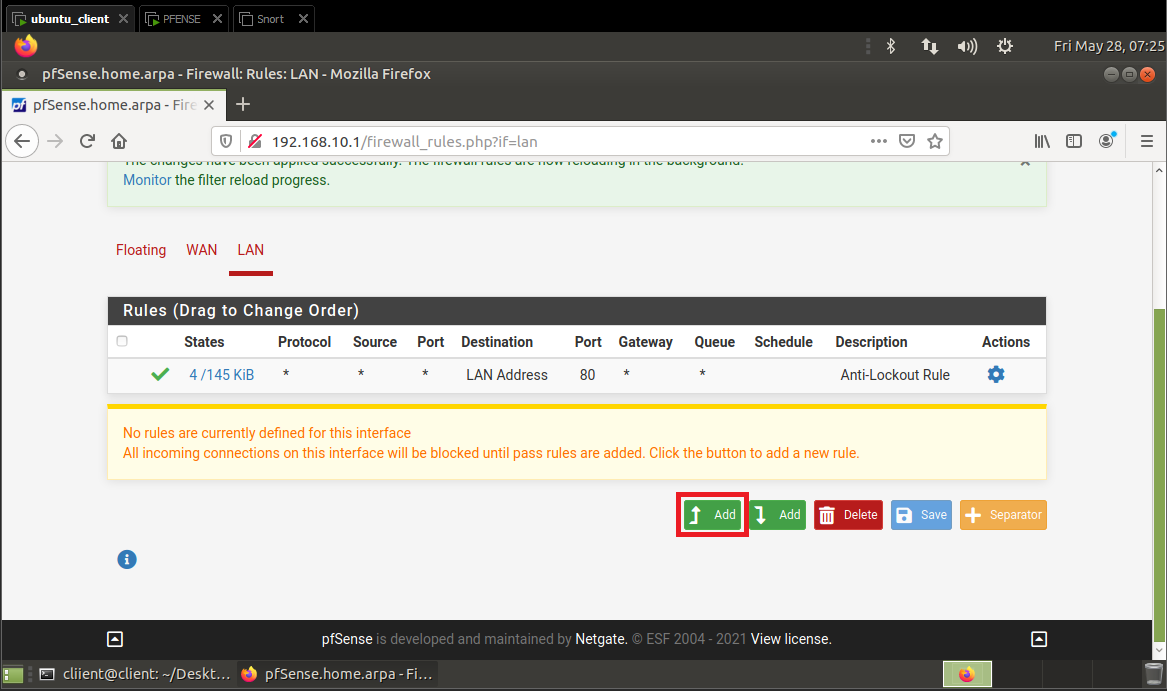
* Sau đó tiến hành các setup mặc định, có thể đổi mật khẩu đăng nhập nếu cần thiết
  + 1. Cho phép máy kết nối với Internet
* Đây cũng là rule mặc định của pfSense

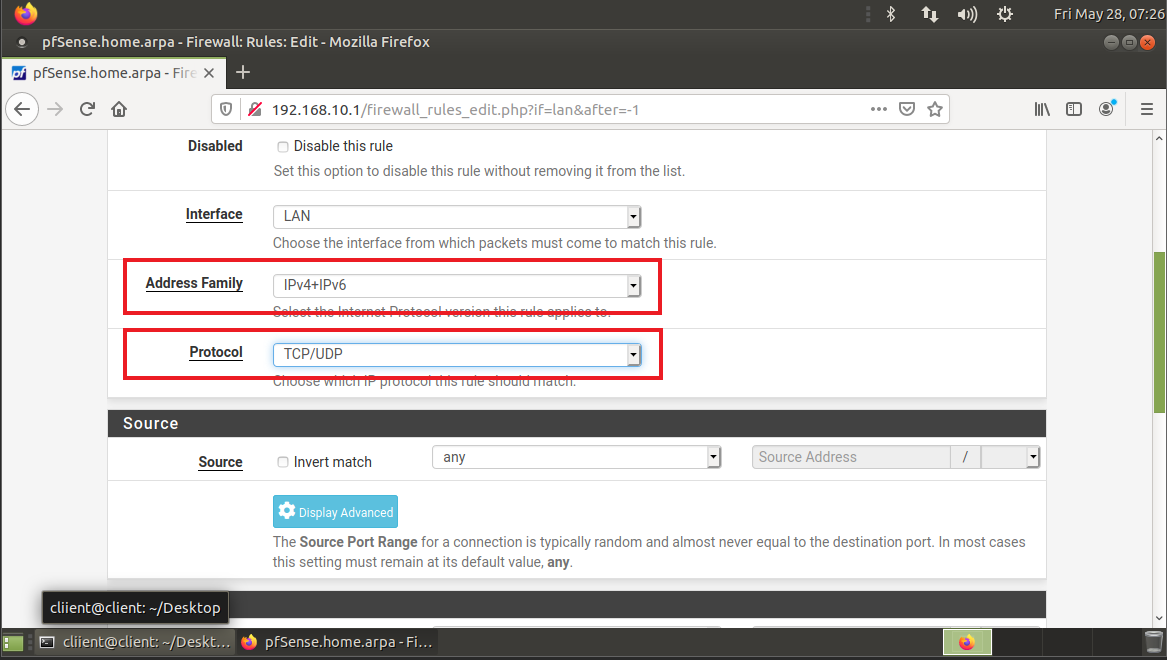




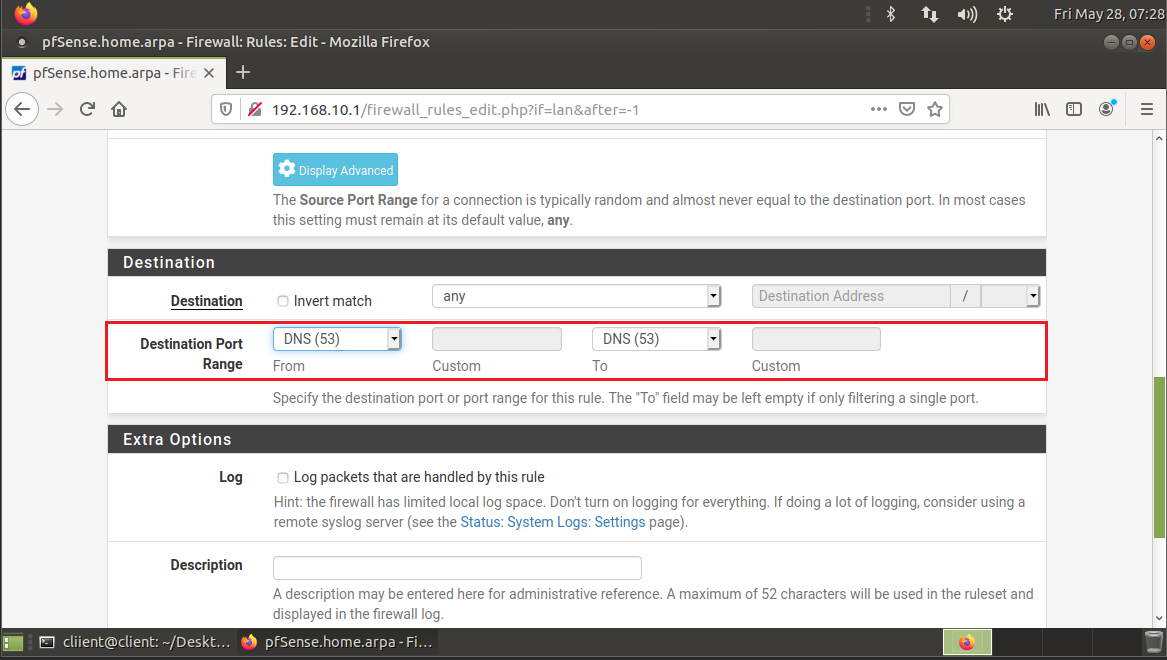
* Kiểm tra
  + 1. Thêm các rule mới
* Vào lại phần rule và xóa 2 rule mặc định
* Kiểm tra bằng cách nslookup google.com thì không tìm thấy
  + 1. Allow DNS
* Sửa nameserver trong file resolv.conf thành
* Sửa 127.0.0.53 => 8.8.8.8

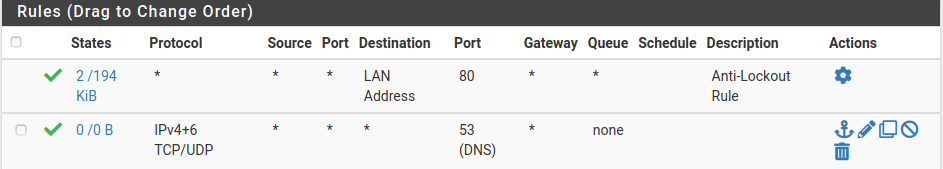
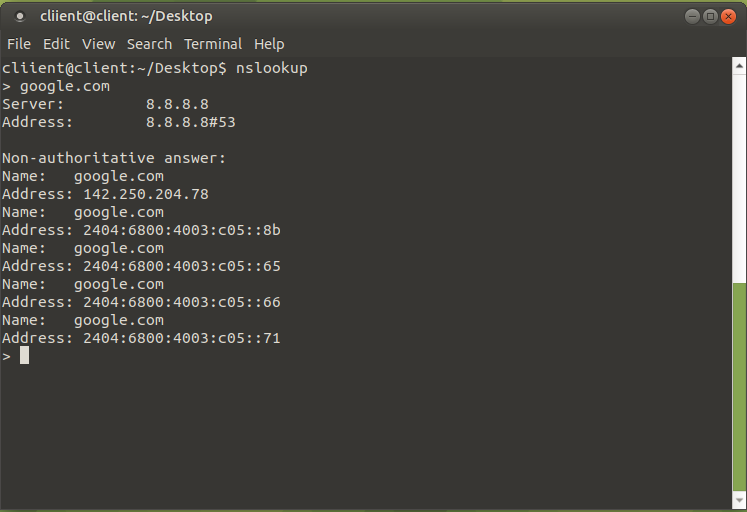


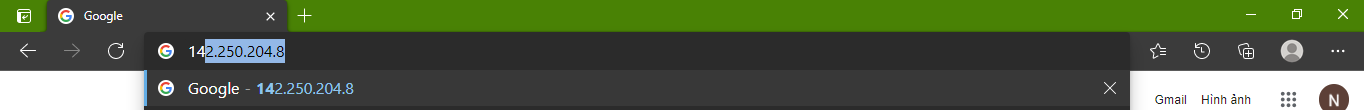
* Sau đó ta tạo rule mới, quay lại phần rule LAN lúc nãy
* Để Action là Pass và cài đặt như sau



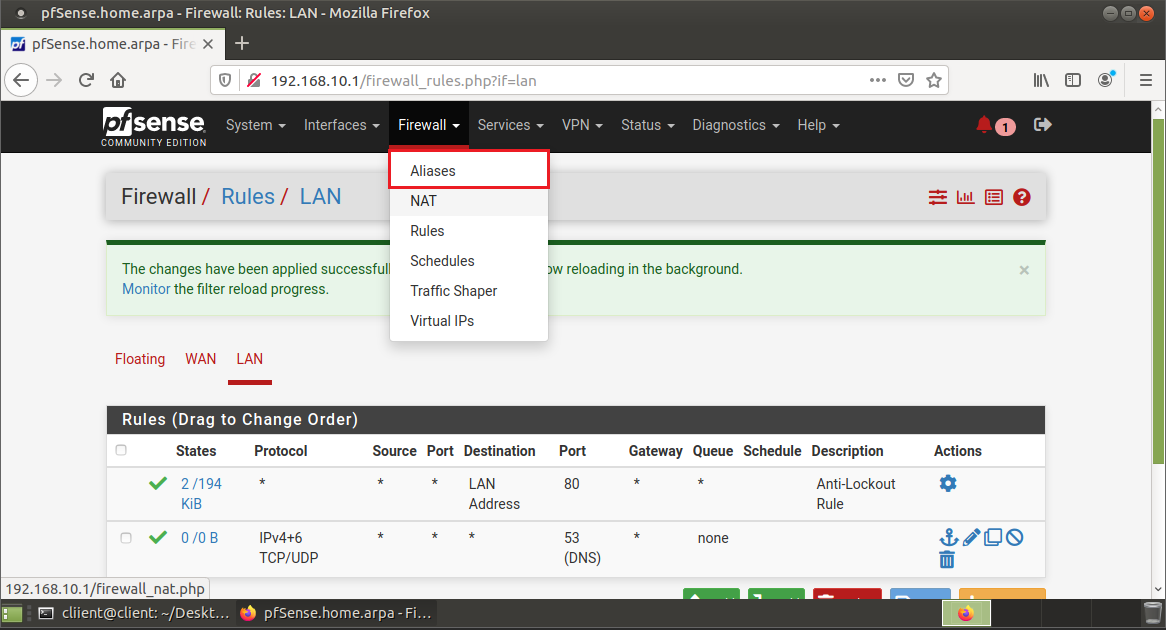
* Chọn Port là 53

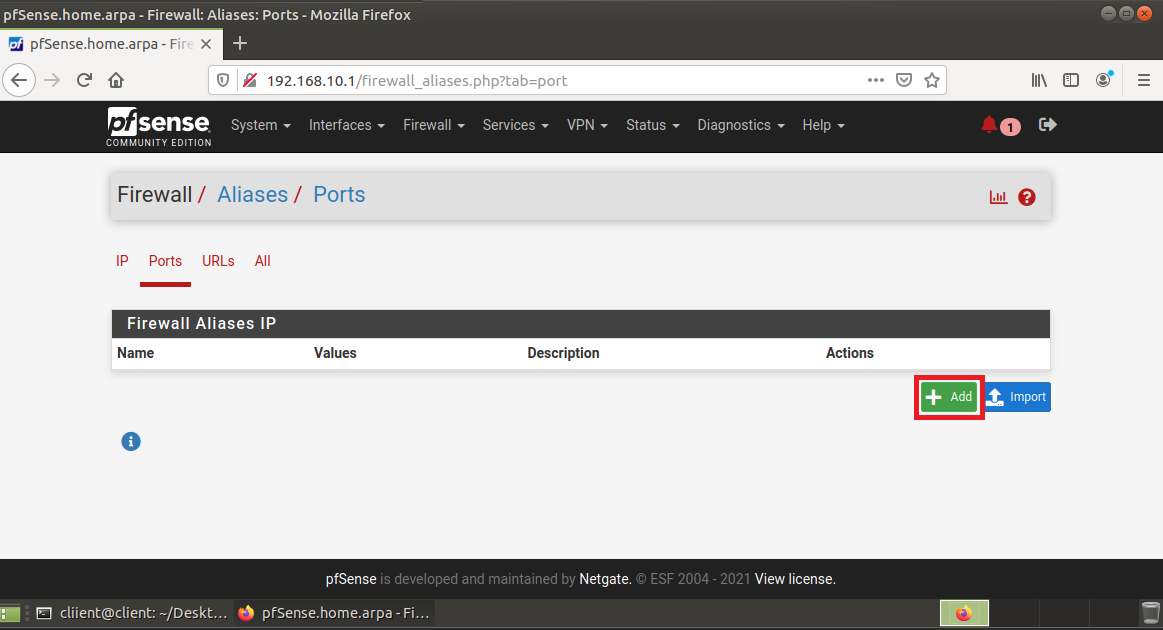


* Thêm thành công
* Kiểm tra

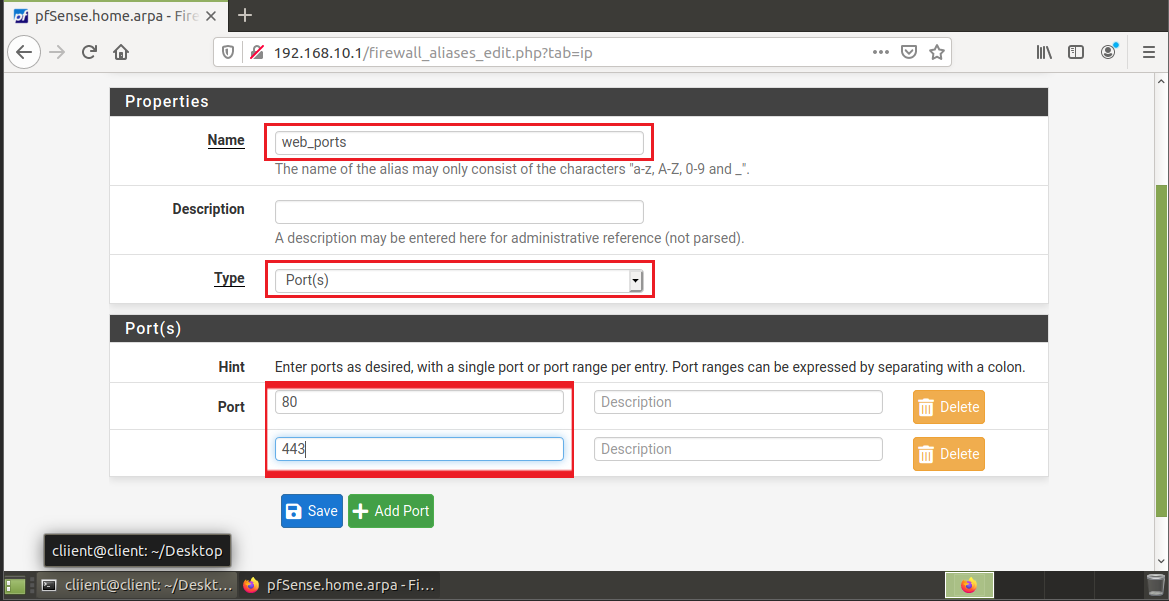


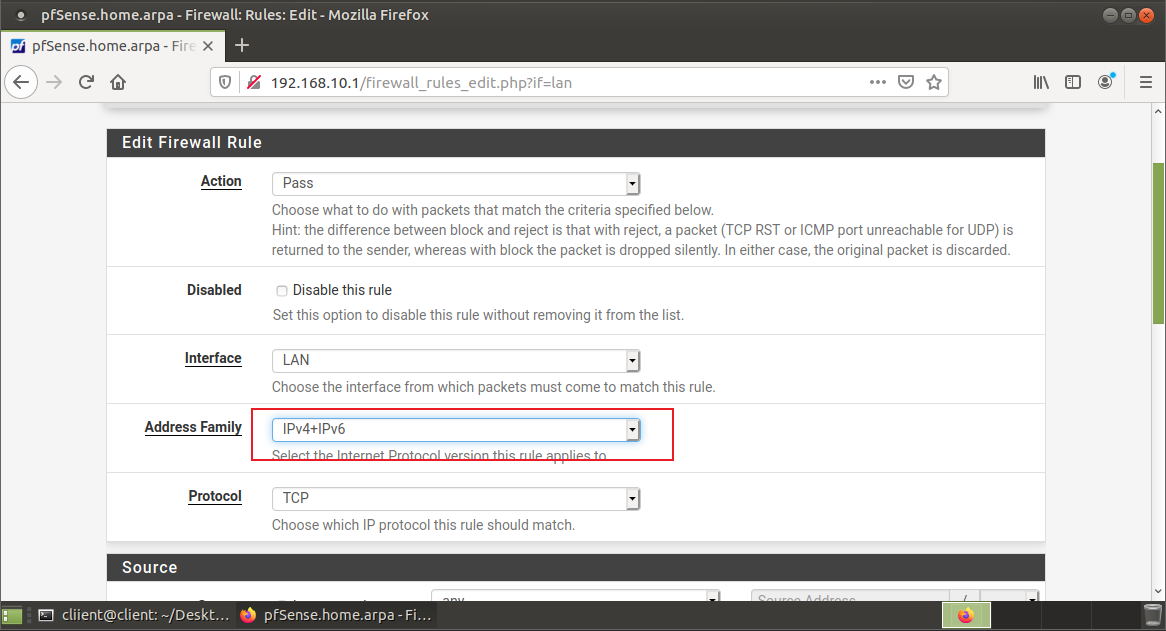
* + 1. Cho phép truy cập web
* Tạo alias cho ports web

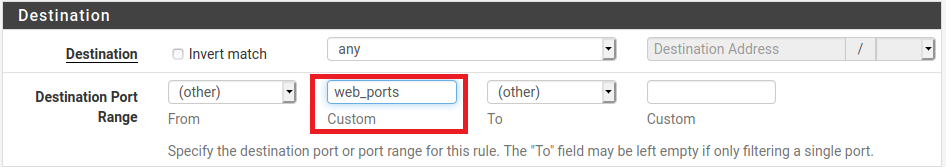




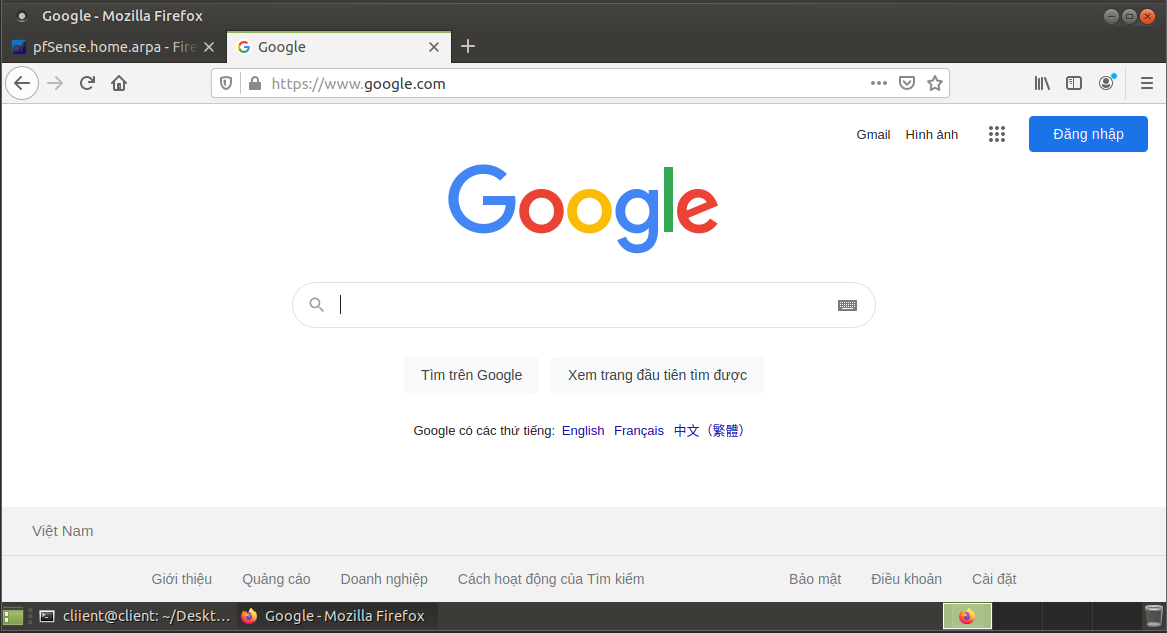
* 2 ports là 80 và 443 được sử dụng



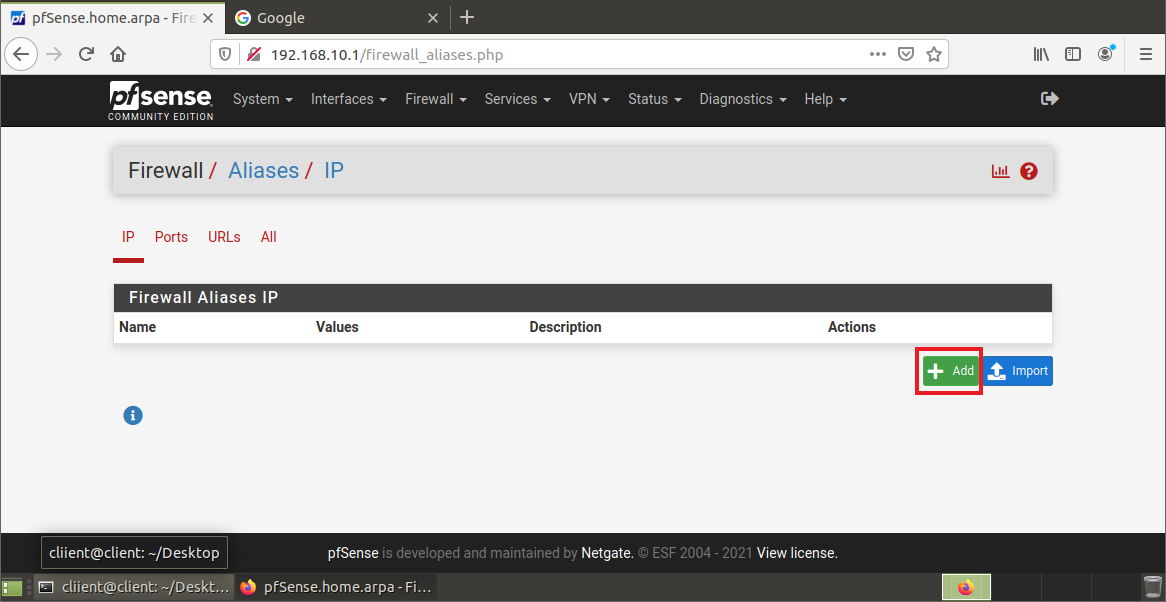
* Sau đó tạo rule mới
* Phần Destination của rule thì thêm port với alias vừa tạo (cho port 80 và 443)



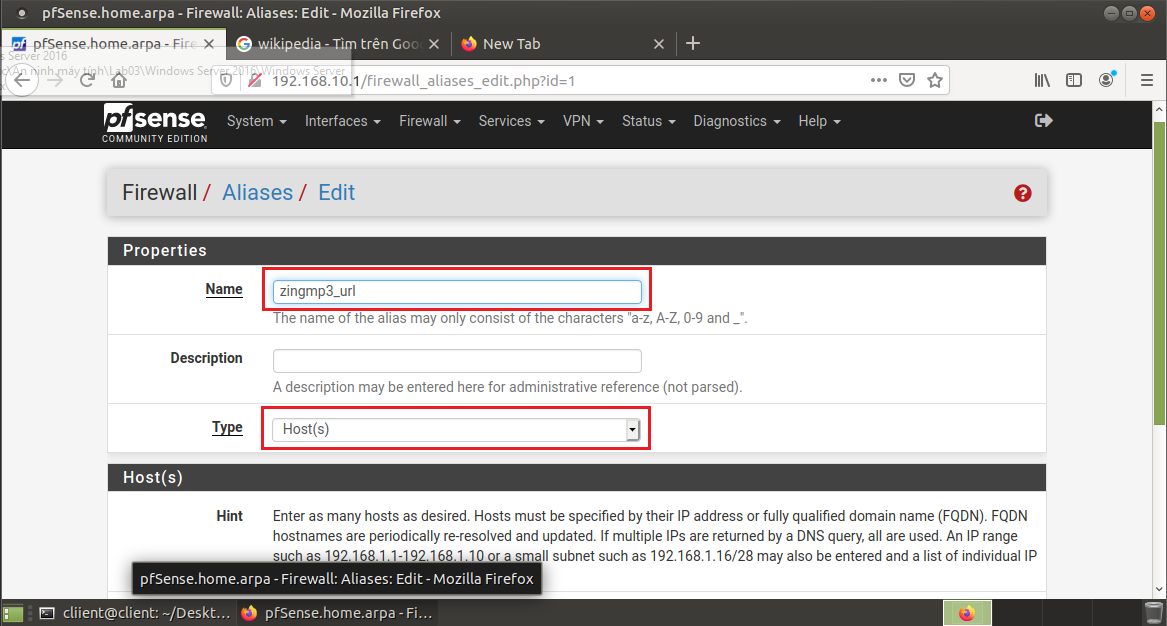
* Kiểm tra bằng cách truy cập google

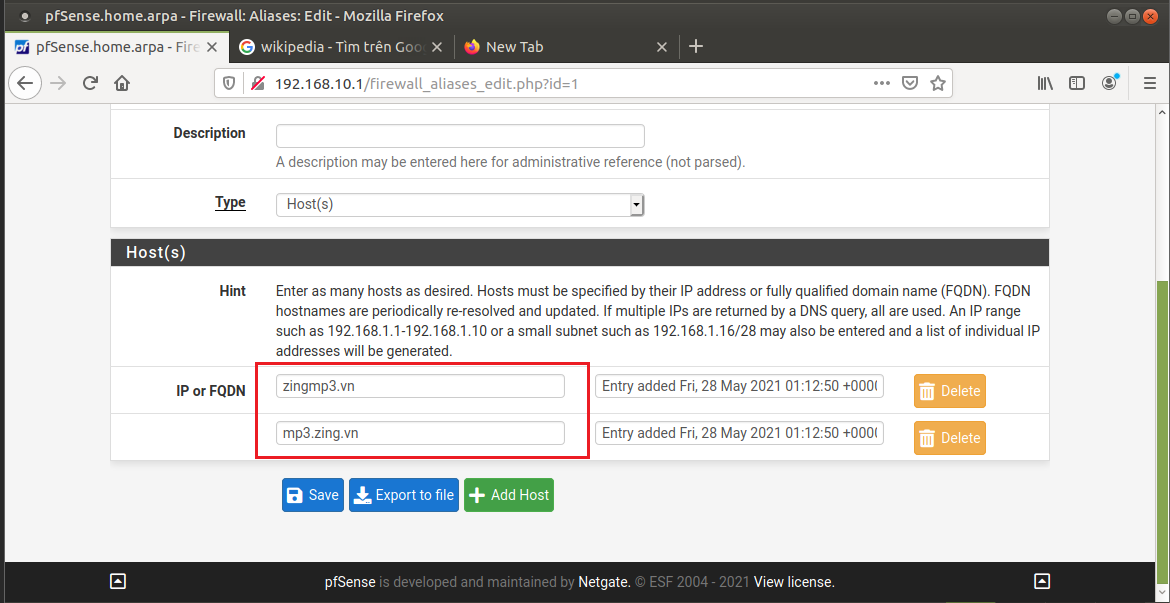


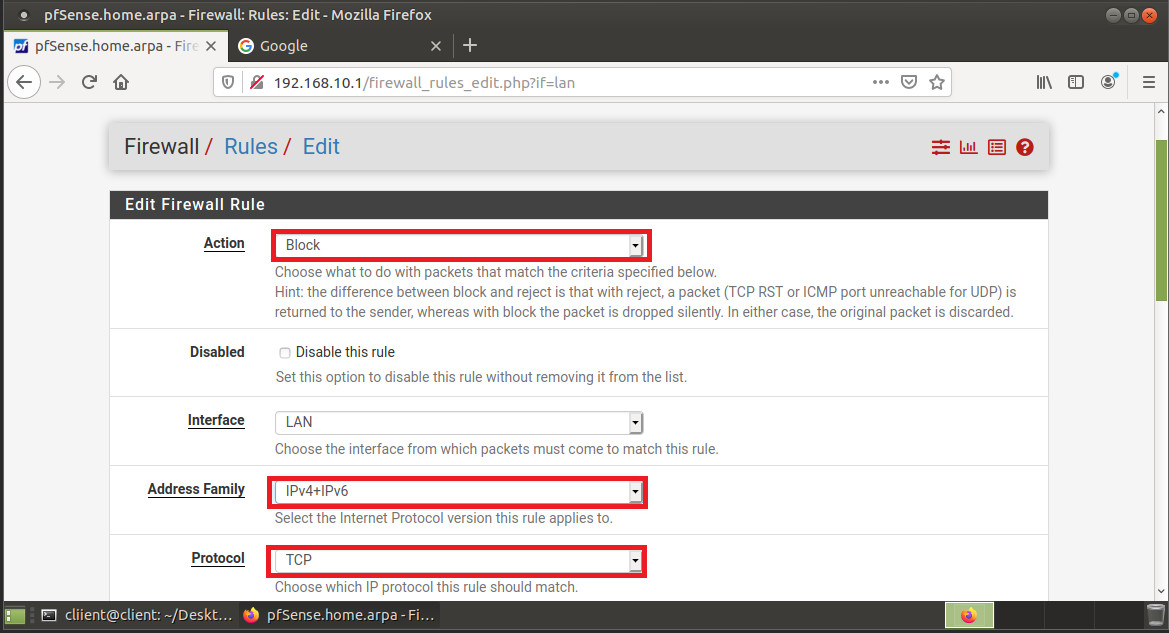
* + 1. Chặn một trang web (cụ thể là zingmp3)
* Tạo alias cho web url của zingmp3

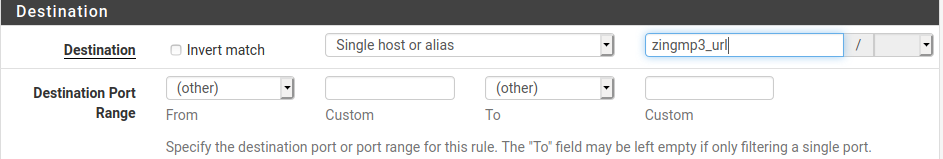


* Thêm 2 tên miền của web zingmp3 này vào, Type là Host(s)

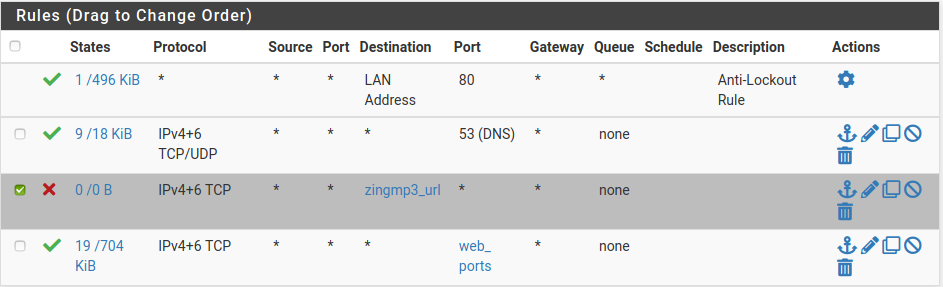


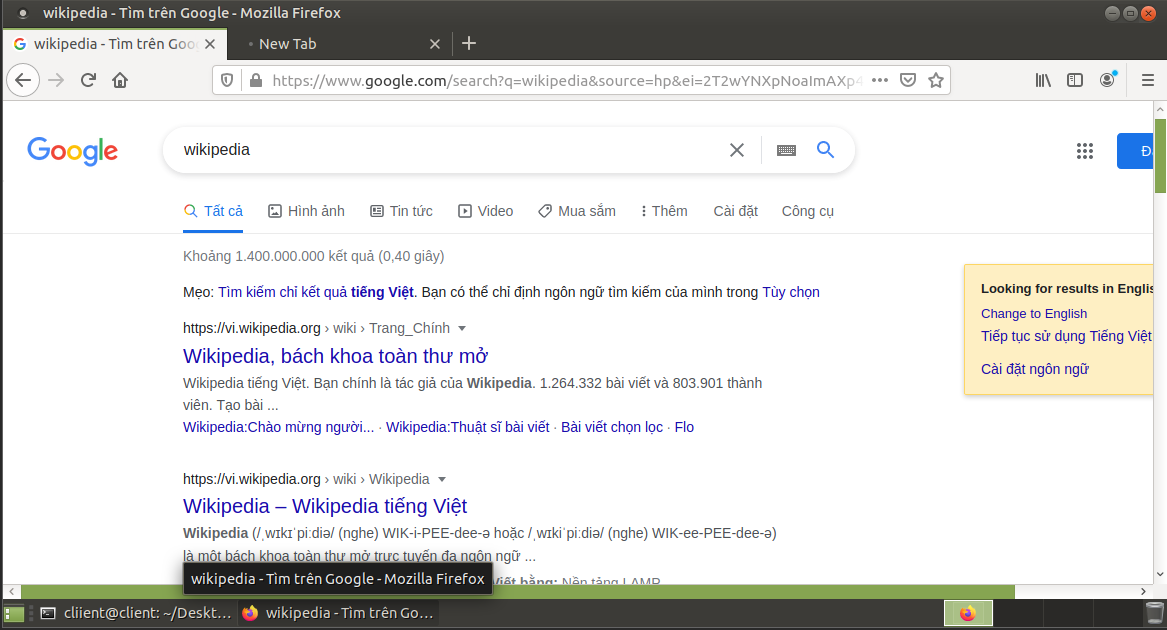


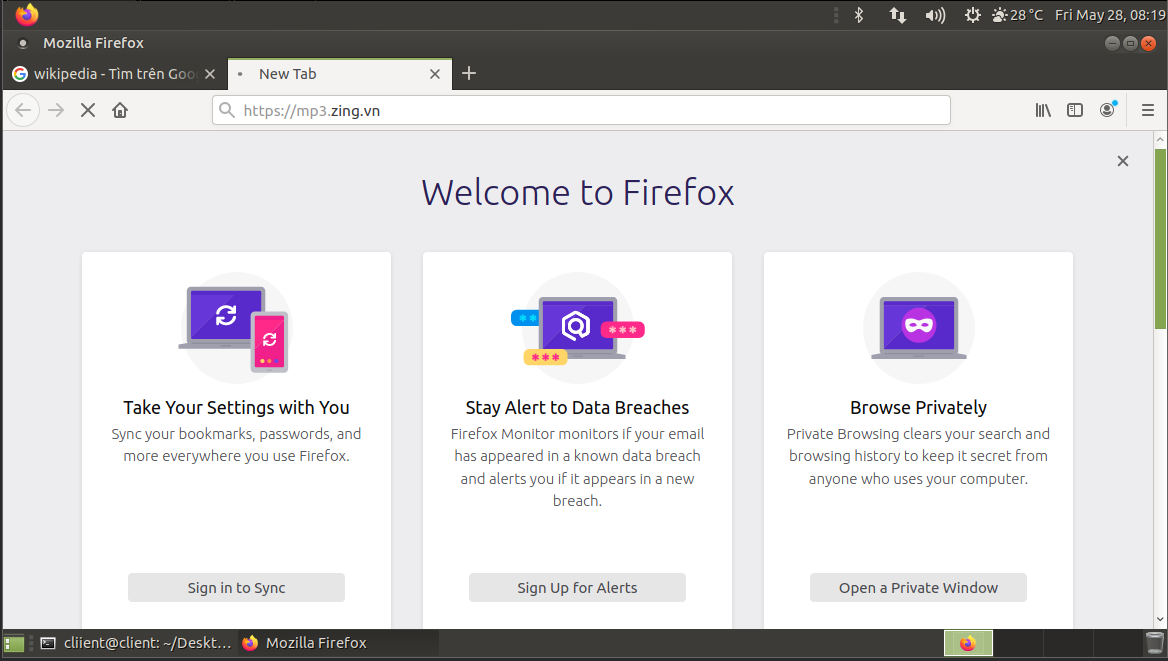
* Sau đó ta tạo rule mới trong LAN để thao tác đặc biệt với trang web này (Block)
* Phần Destination của rule ta nhập alias ứng với url zingmp3 vừa tạo



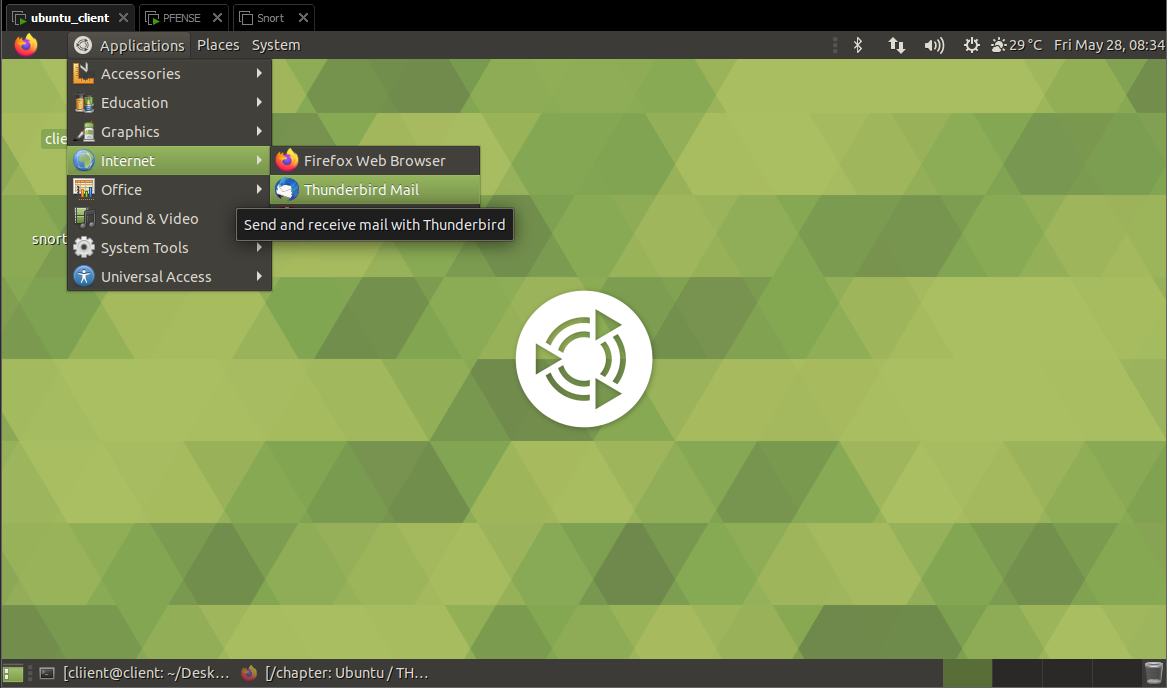
* Chọn save để tạo rule
* Sau đó để rule này lên trên rule cho phép truy cập DNS trong bản mức độ ưu tiên

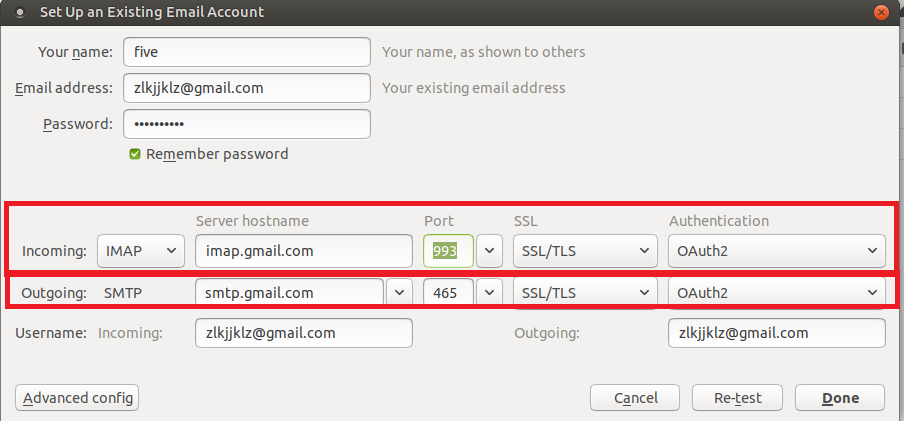
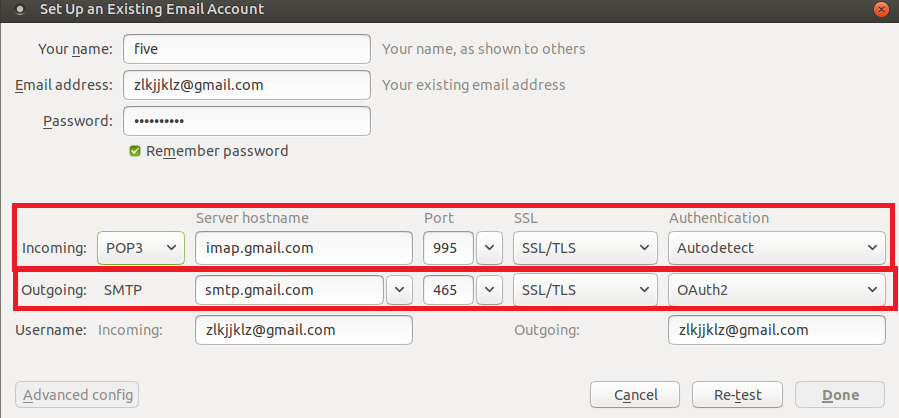


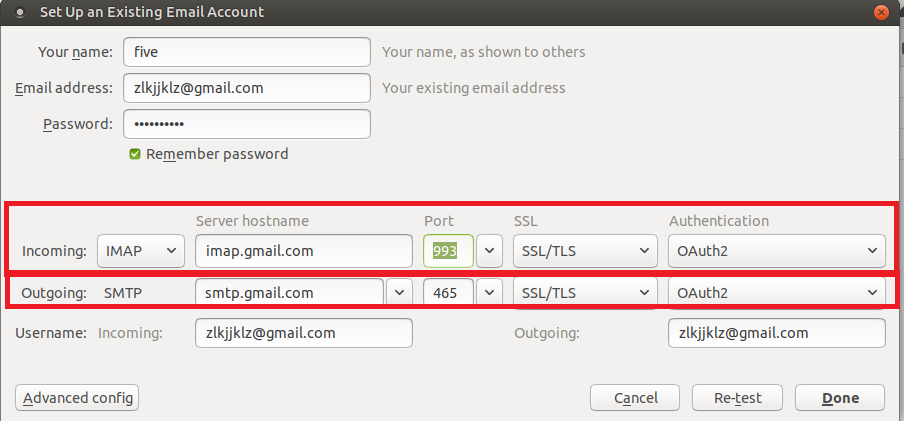
* Kiểm tra bằng cách truy cập mạng bình thường nhưng khi truy cập zingmp3 thì không phản hồi

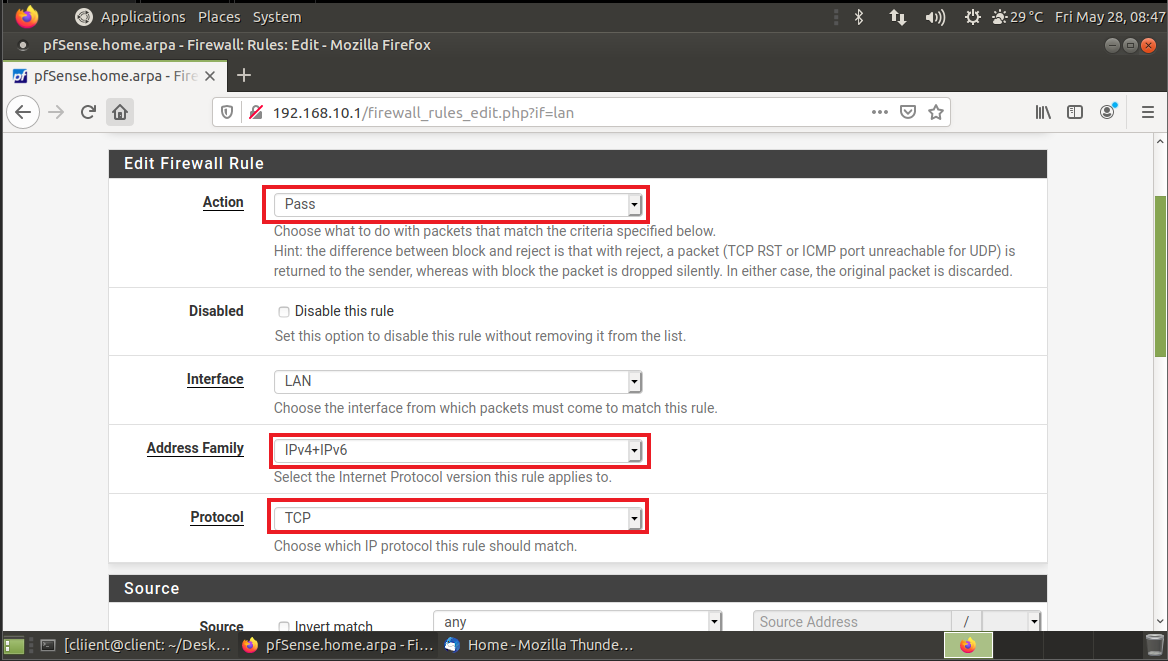


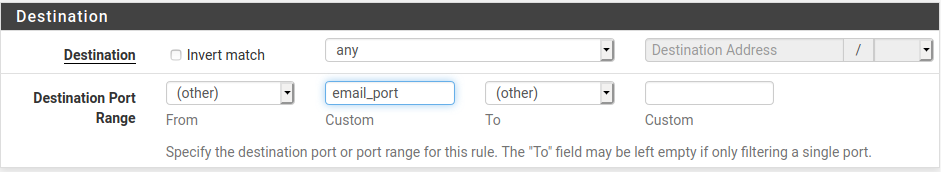
* + 1. Cho phép ứng dụng mail (cụ thể là thunderbird)
* Mở thunderbird và xem các port được sử dụng trong ứng dụng







* Ta thấy có 3 port được sử dụng là 995, 465 và 993. Ta tạo alias tương ứng cho 3 port này
* Tạo rule mới để cho phép ứng dụng
* Phần Destination của rule, nhập alias vừa tạo ứng với các port mà ứng dụng sử dụng

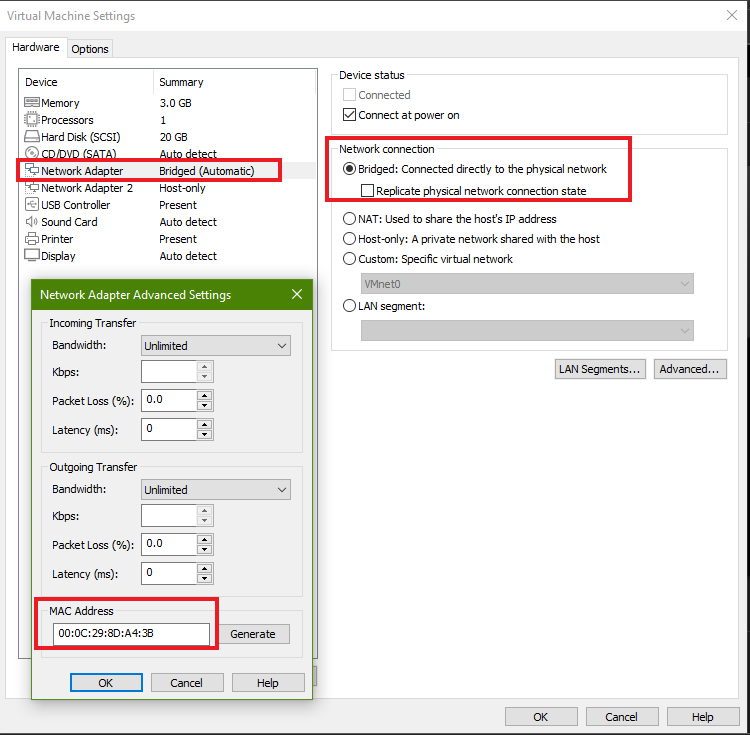


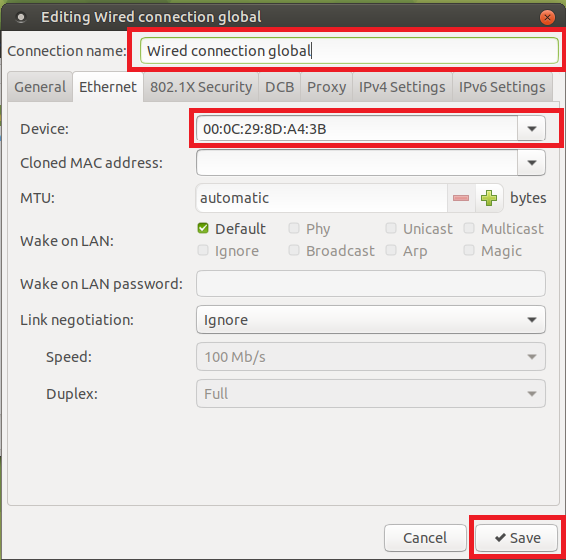
* Sau đó chọn save để tạo rule
* Sau đó vào lại thunderbird để kiểm tra



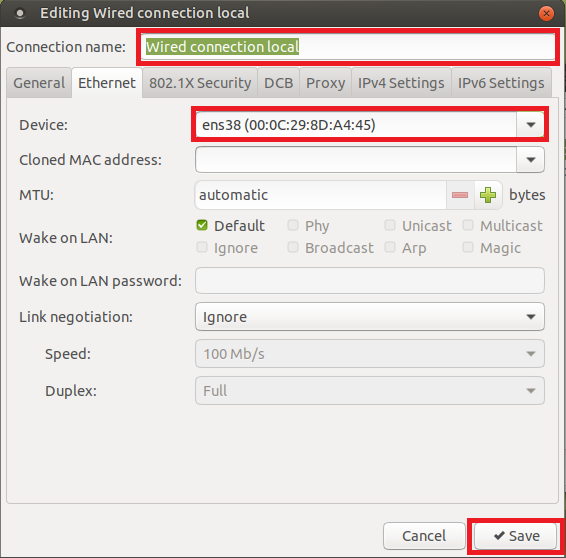
1. Snort – IDS
   1. Cài đặt Snort
      1. Máy cài Snort

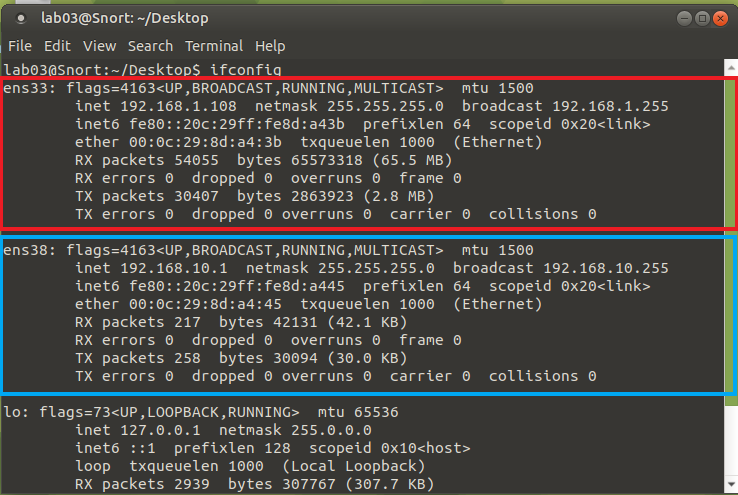
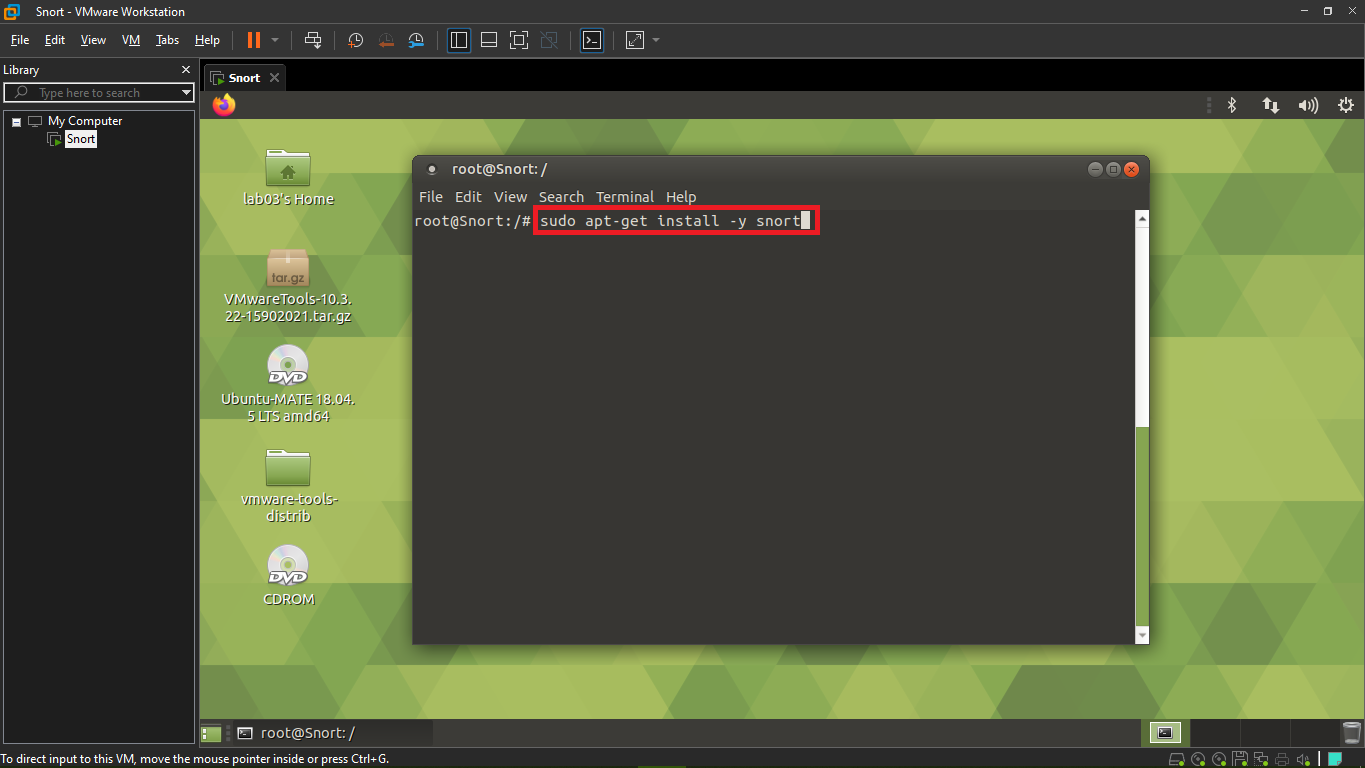
* Thiết lập 2 card mạng, một card mạng sử dụng chế độ Bridge vớ máy Attacker, máy còn lại kết nối với máy Client trong mạng (Host-only)

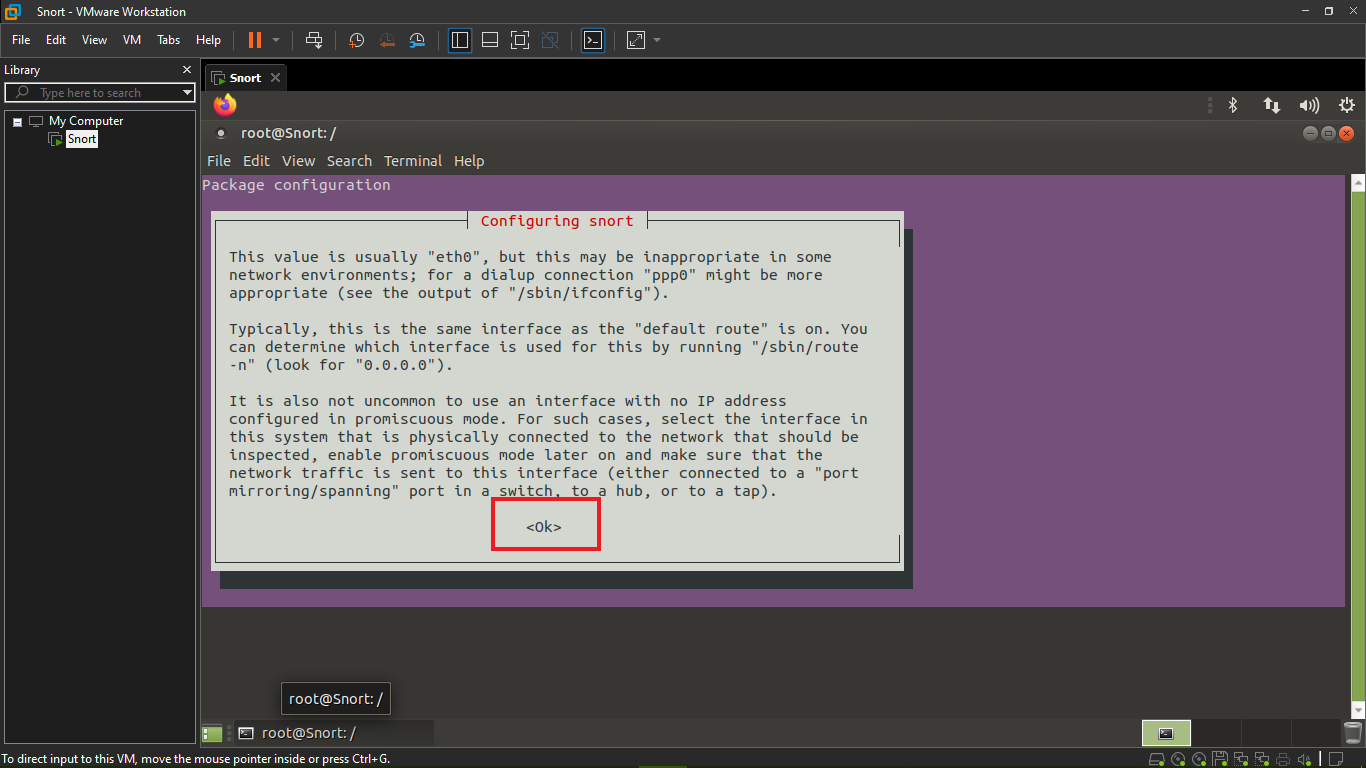


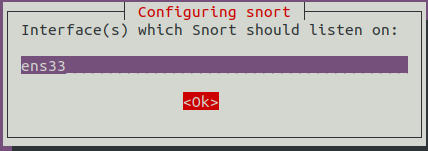
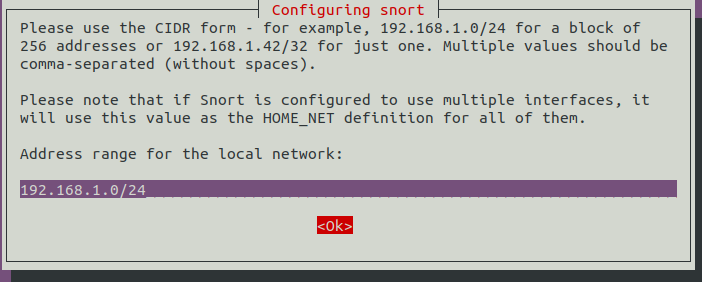


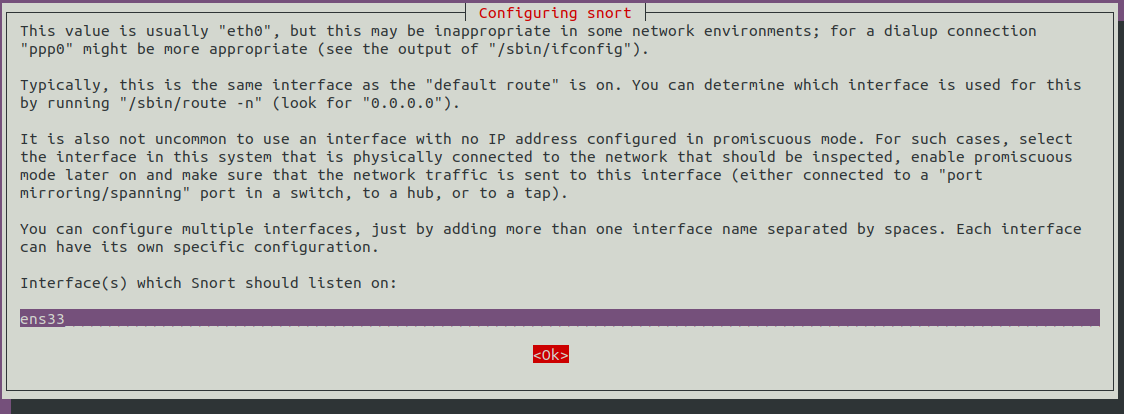


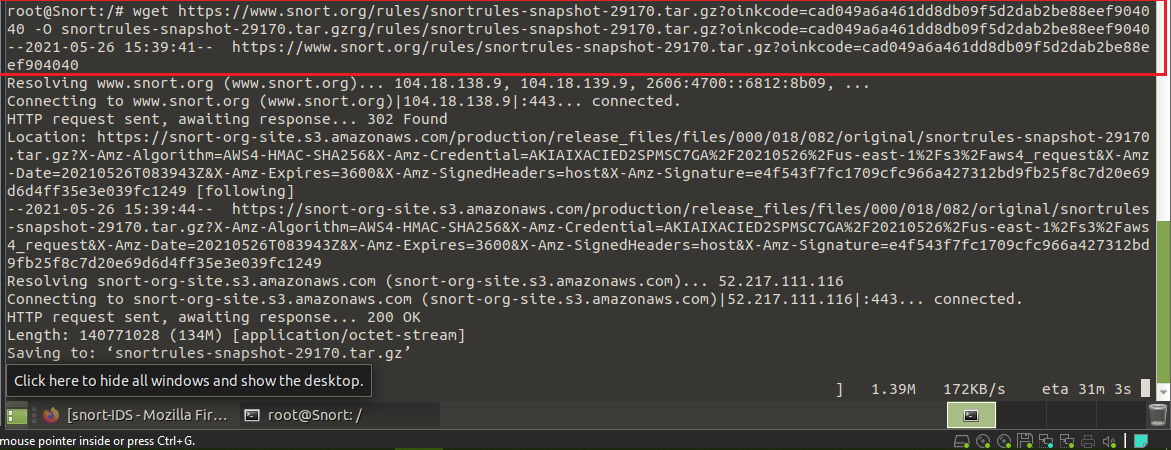


* Kiểm tra địa chỉ IP ứng với các card mạng Local (Host – Only) và Global (Bridge)
* Tiến hành cài Snort



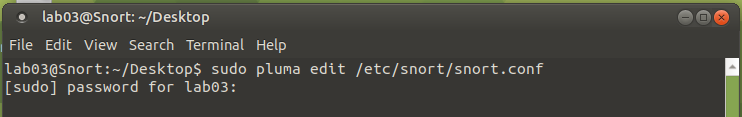
* Chọn tương ứng với card mạng được kết nối ra bên ngoài
* Địa chỉ đường mạng tương ứng

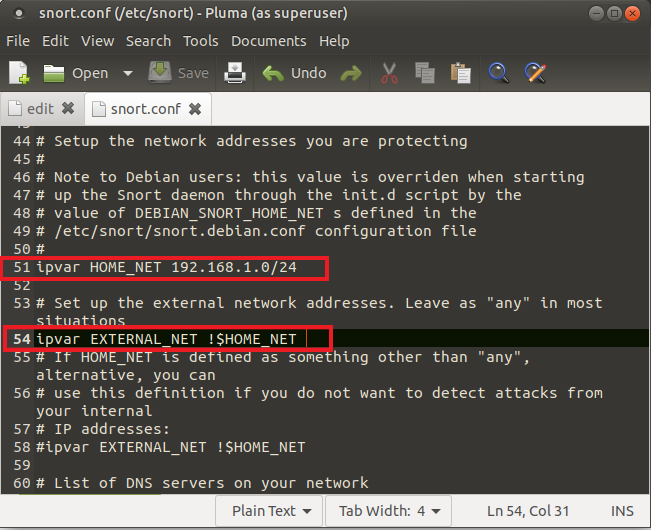


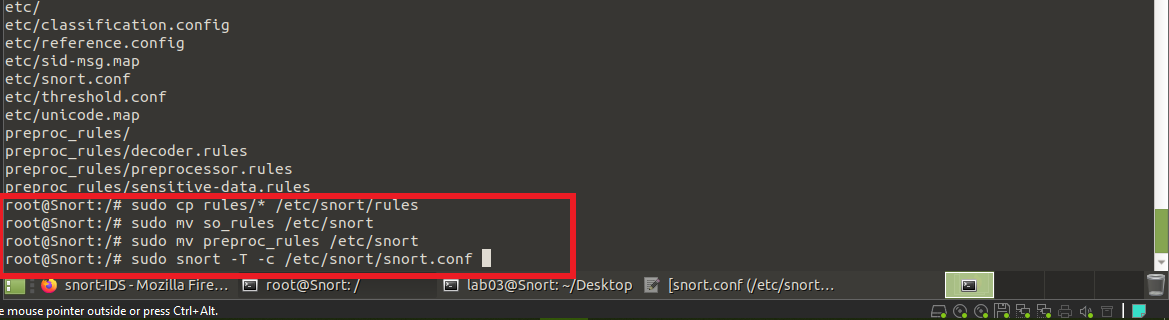
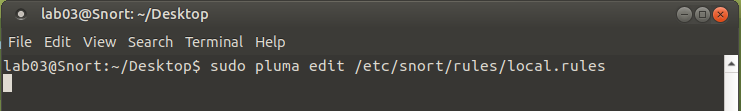
* Tiếp tục cài đặt

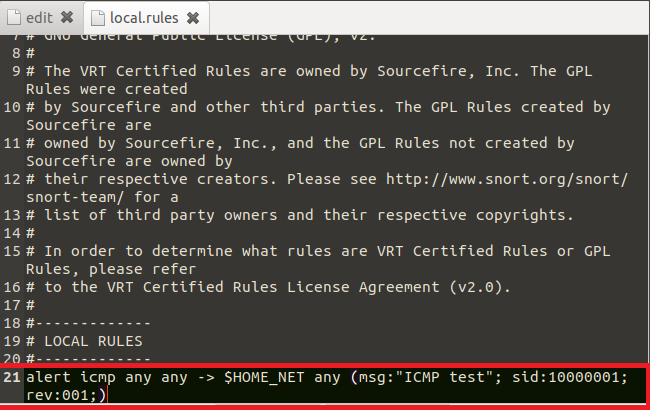


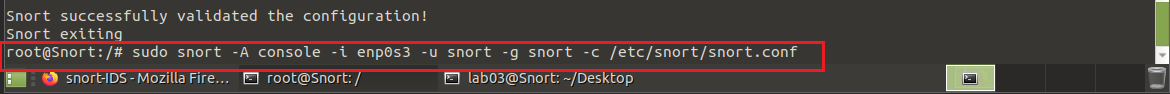
* Configure đường mạng HOME\_NET (kết nối Bridge với Attacker)

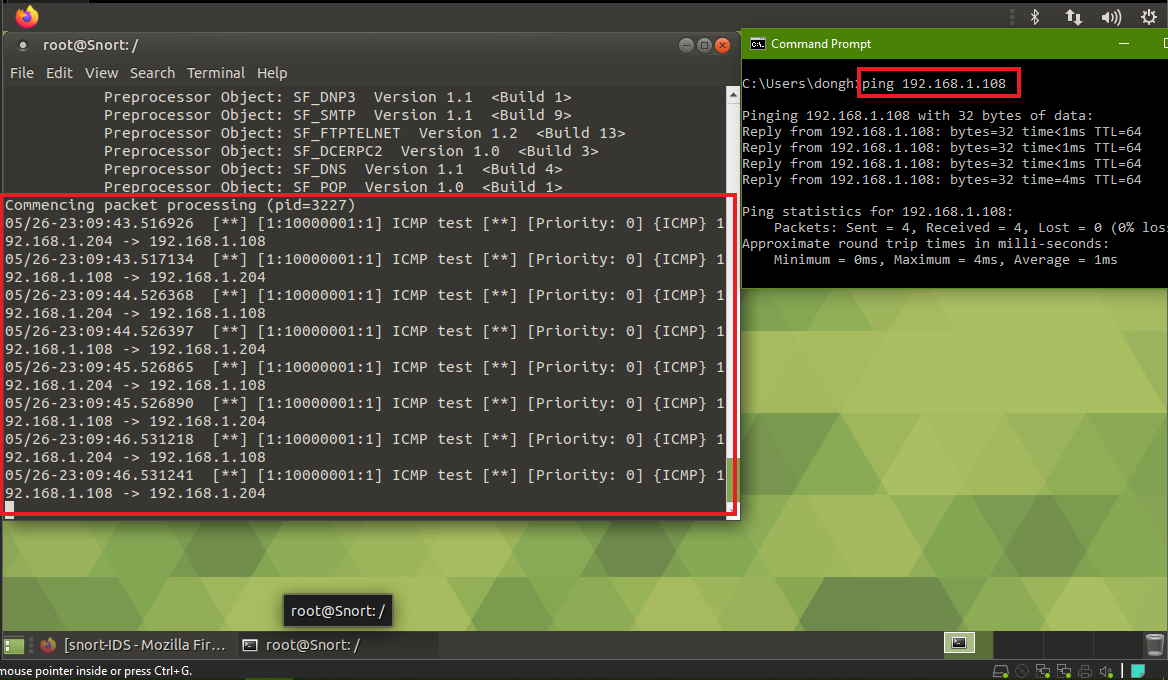


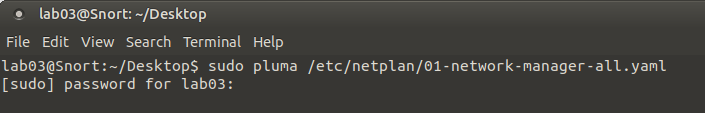


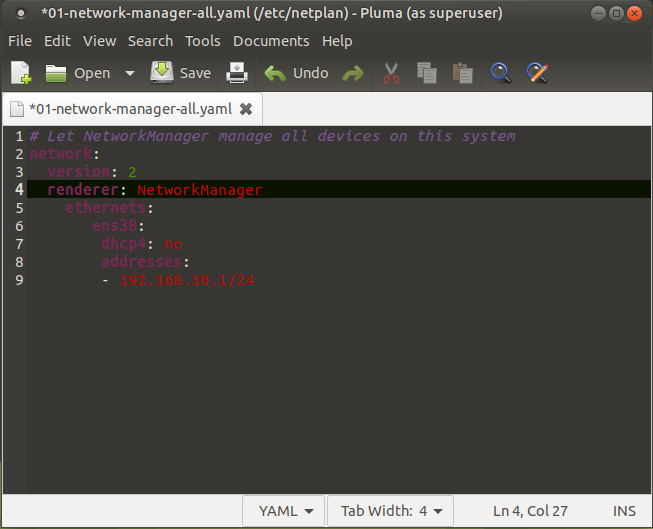
* Tiếp tục cài đặt
* Thiết lập cảnh báo

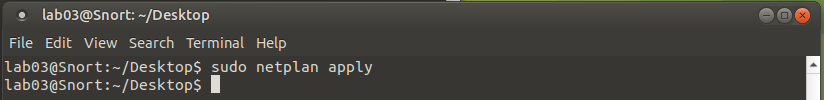


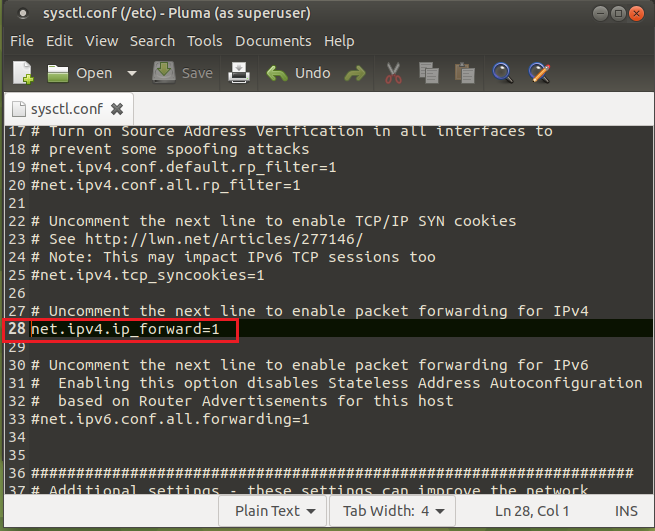
* Chạy thử và kiểm tra Snort bằng cách Ping từ máy Attacker và máy Snort

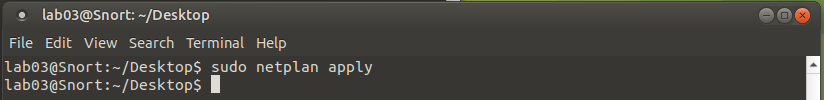


* Thiết lập cho card mạng kết nối với Client (Host-only)

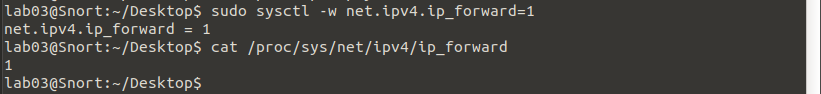




* Sau đó truy cập file /etc/sysctl.conf và bỏ comment dòng 28

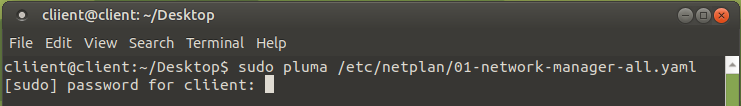


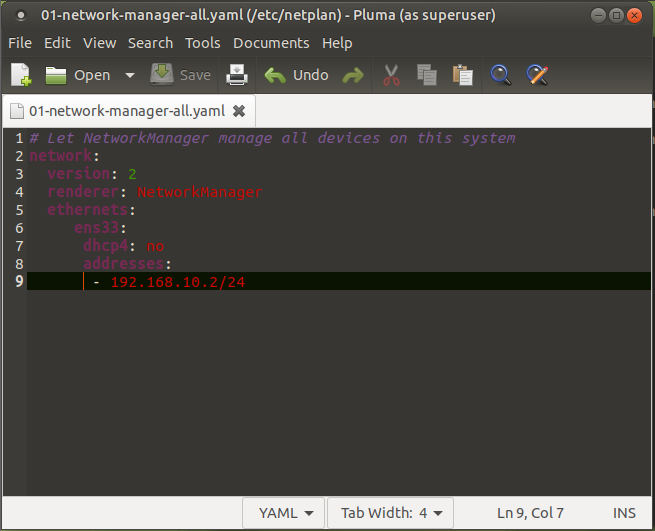
* Set ip\_forward của ipv4 = 4



* + 1. Máy Client

(Do máy của em khá yếu, không chạy nổi máy Server và Client cùng lúc nên thay máy Server bằng Client)

* Các card mạng Vmware sử dụng lại máy Client của câu 4
* Setup lại card mạng và các kết nối cho kết nối Host-only với máy Snort

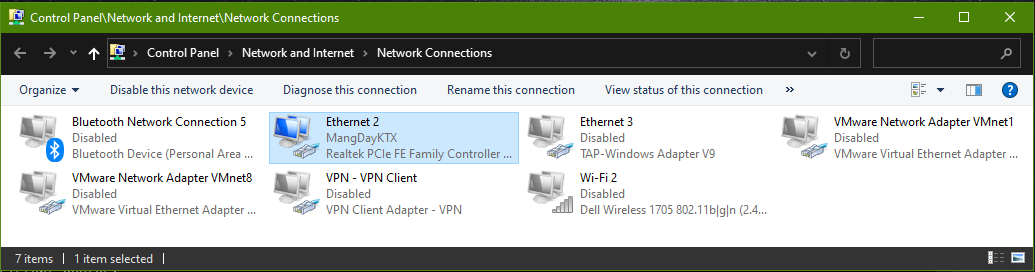




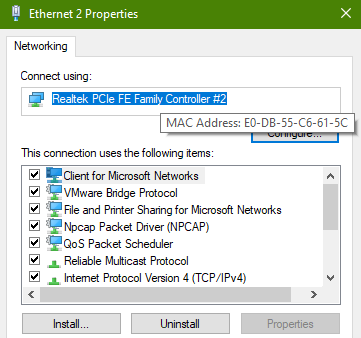
* Route default Gateway đến địa chỉ IP của Intefaces máy Snort trong đường mạng

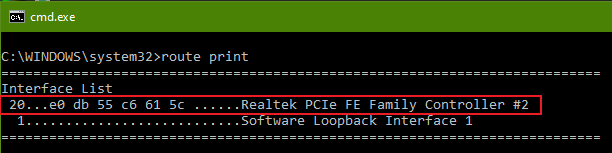


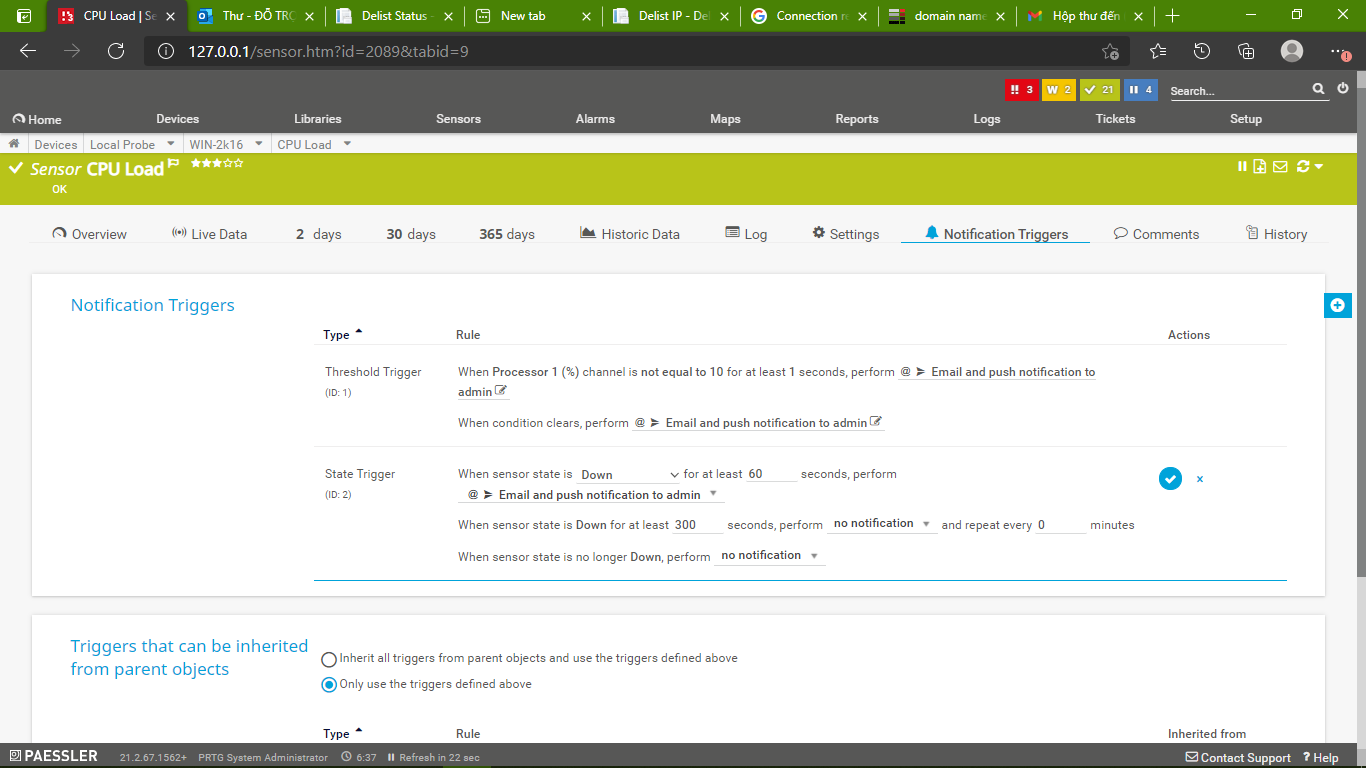
* + 1. Máy Attacker (máy thật)
* Disable các card mạng trừ card mạng đang sử dụng (kể cả Vmnet1 để máy Snort và máy Client chỉ kết nối với nhau

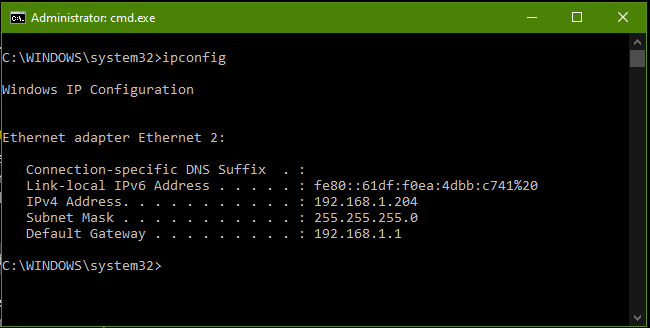


* Route đường mạng Host-only đến địa chỉ IP mà máy Snort kết nối Bridge tới

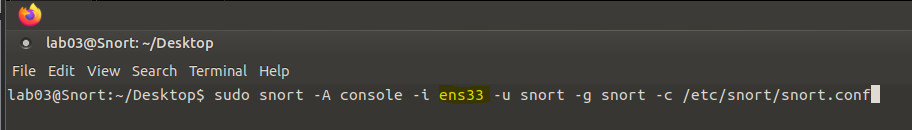


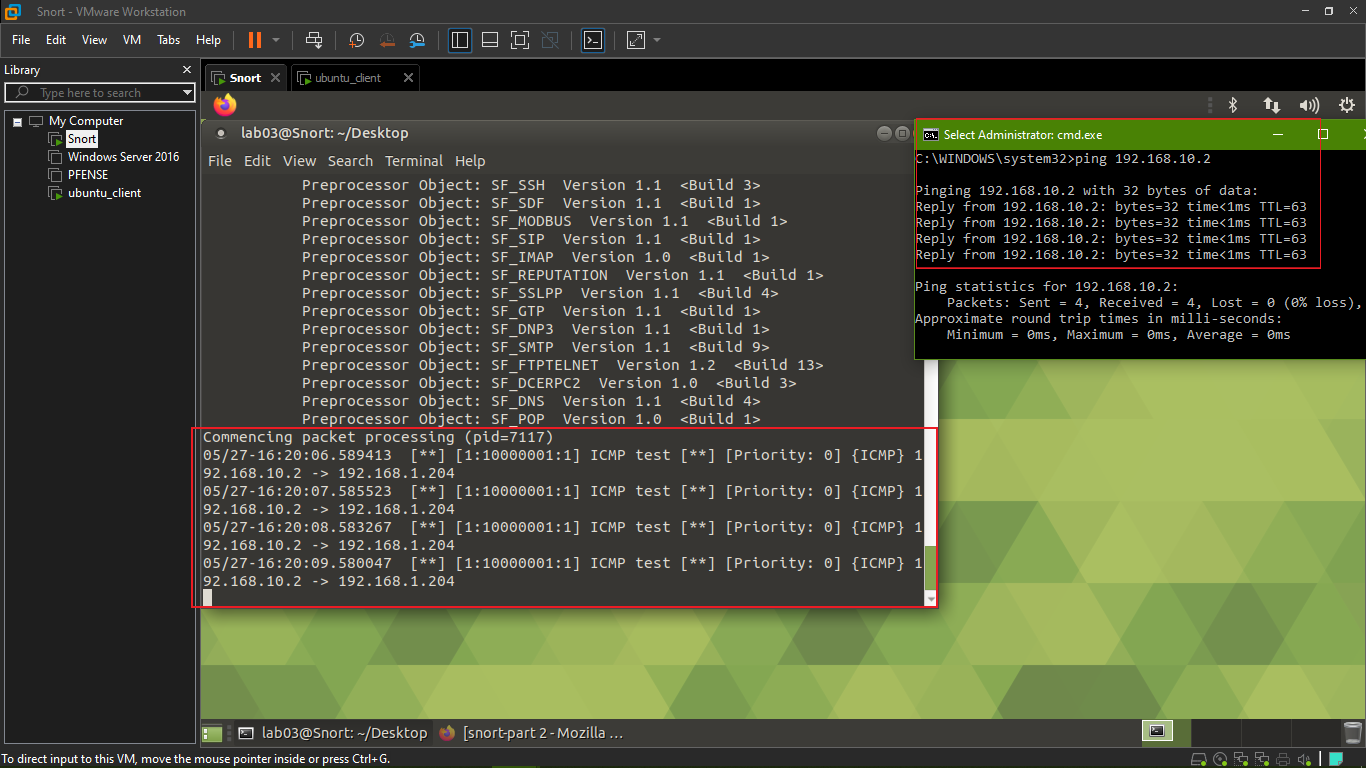


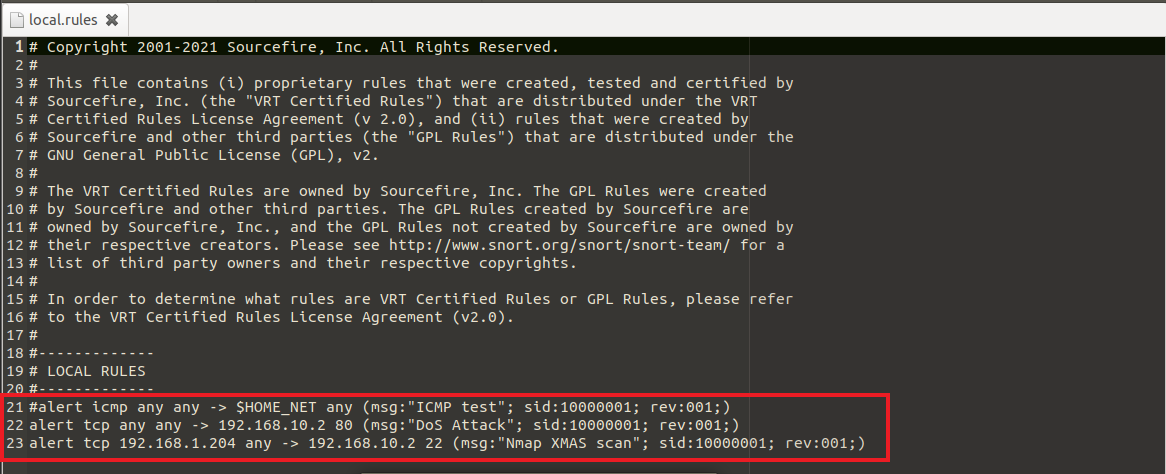


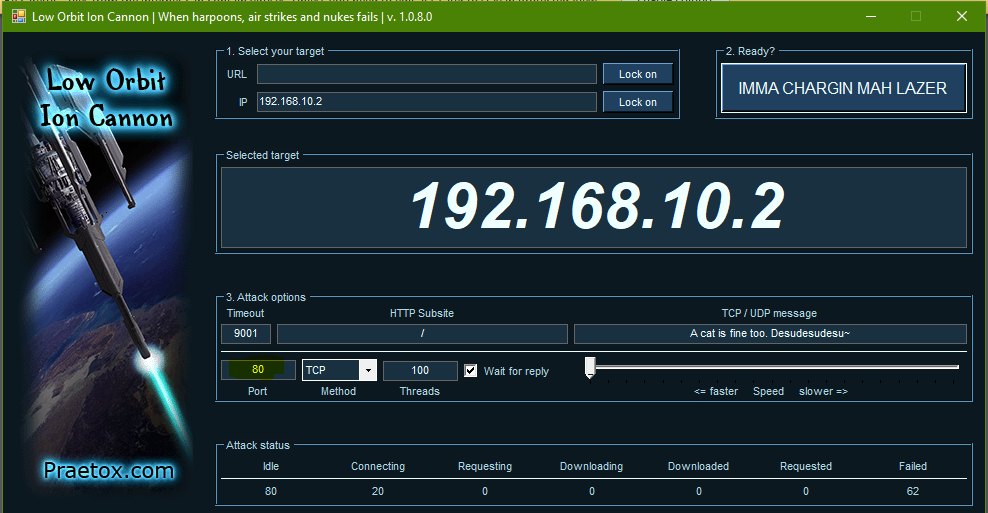
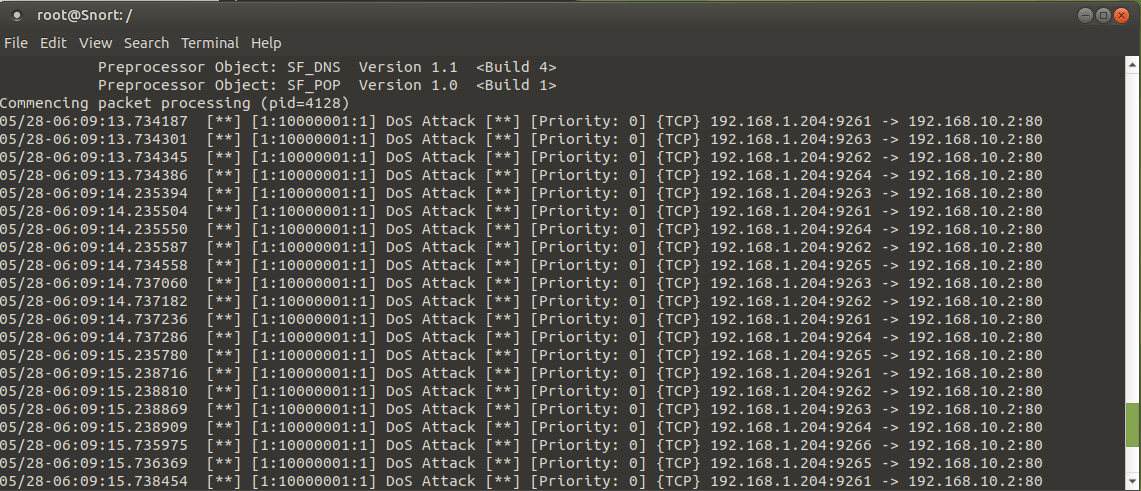


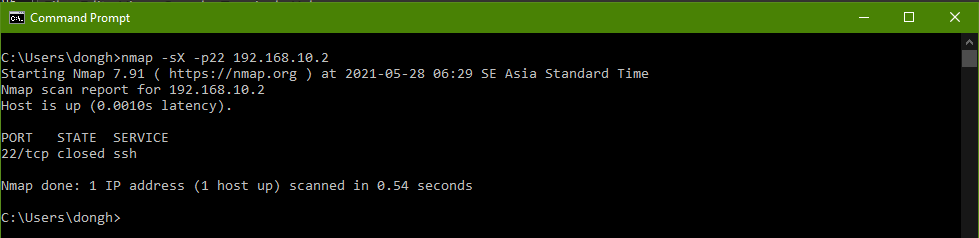
* + 1. Kiểm tra Snort
* Ở máy Snort tiến hành chạy Snort



* Máy Attacker tiến hành ping vào máy Client bên trong (Host – only). Kiểm tra ờ máy Snort ta thấy có kết quả
  1. Mô phỏng tấn công
     1. Thiết lập
* Ở máy Snort ta thiết lập các rule và cảnh báo trong **/etc/snort/rules/local.rules**
* Tạm thời comment dòng 21. Ở dòng 22 là cảnh báo khi máy Attacker tấn công DoS (port 80) và dòng 23 là cảnh báo Nmap scan từ máy Attacker (IP cụ thể, scan port 22). Tất cả đều là phương thức tcp, sau đó chạy Snort



* + 1. Tiến hành và kết quả
* Máy Attacker dùng tool LOIC tiến hành tấn công DoS bằng phương thức tcp, port 80
* Kết quả cảnh báo từ máy Snort
* Máy Attacker thực hiện scan port 22 của máy Client (tiếc là đã bị đóng)



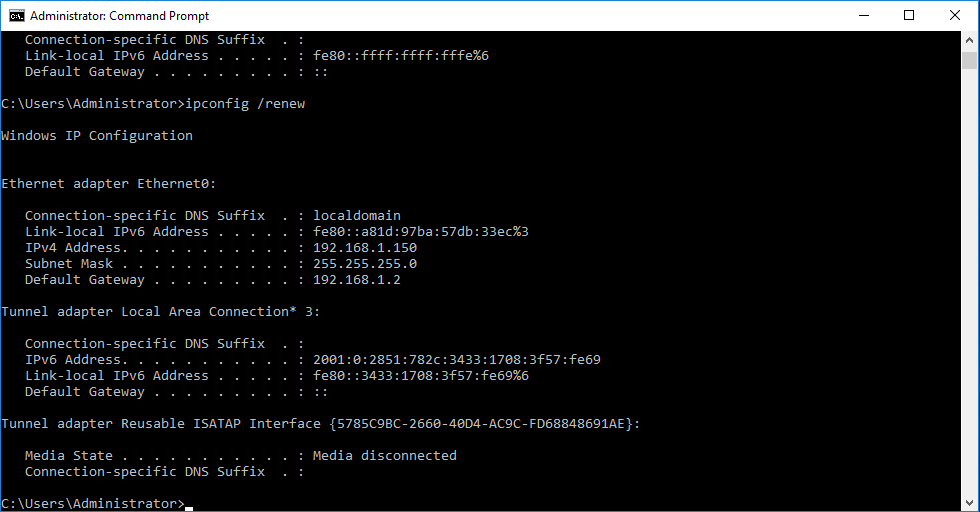
* Kết quả trên máy Snort



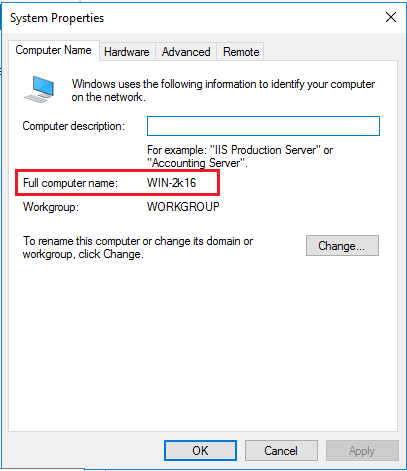
* + 1. Đánh giá
* Với các thiết lâp hiện tại, Snort giống như một công cụ theo dõi đường mang. Các công việc cụ thể khi xử lý khi bị tấn công dành cho người giám sát đường mạng. Tùy váo các loại tấn công mà có thể sử dụng thêm các tool (vd: iptables) để có thể tự động xử lý.

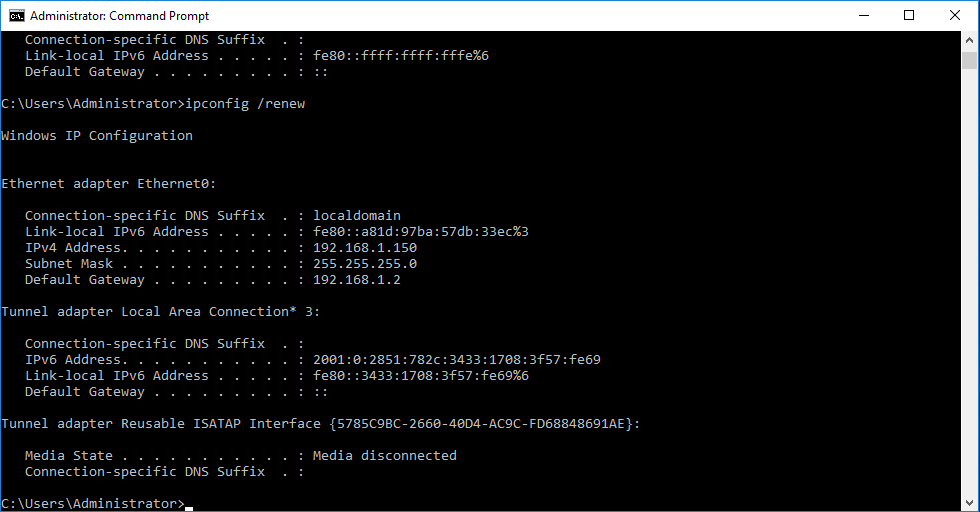
1. Network Monitoring System
   1. Thiết lập

* Máy giám sát: cài đặt PRTG
* Có địa chỉ IP là: 192.168.1.204

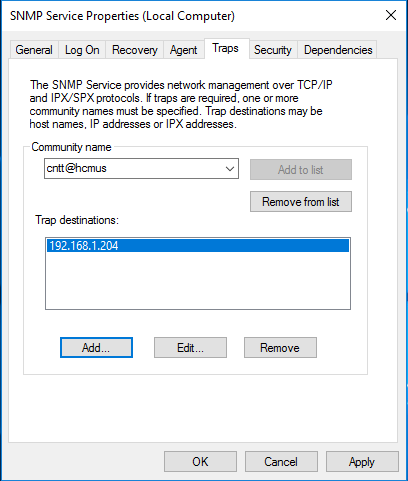


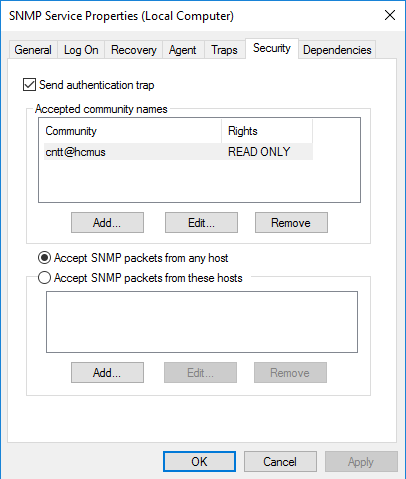
* Máy cần giám sát: Windows Server 2016 – Computer name: Win-2k16
* Các thông tin cơ bản (tên, địa chỉ IP) máy như sau:

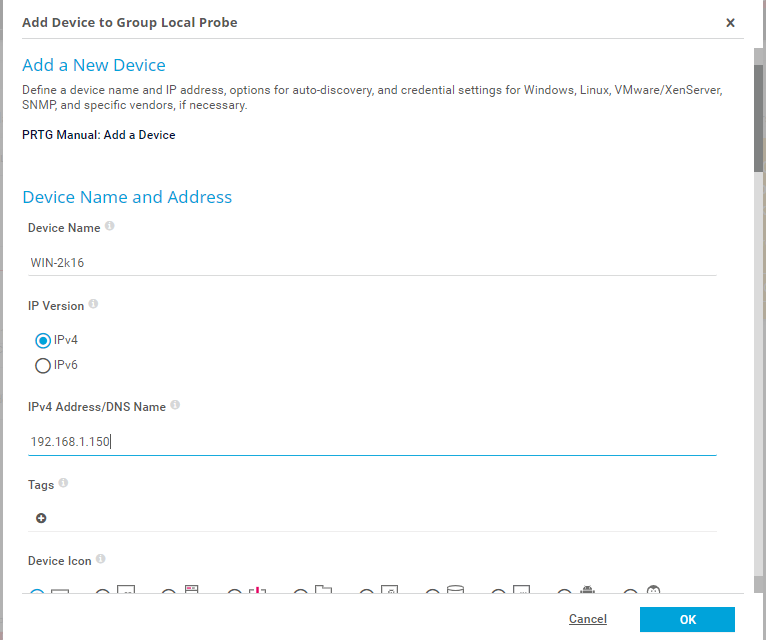


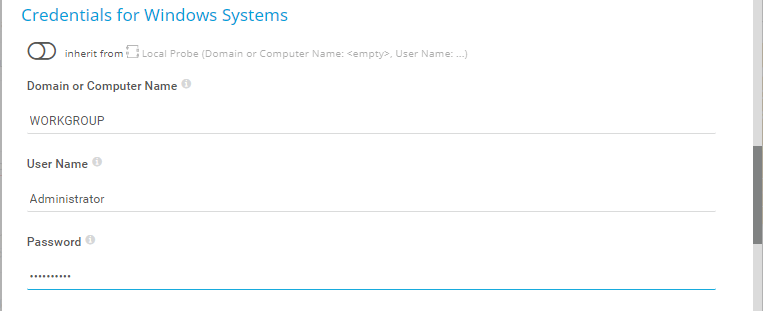


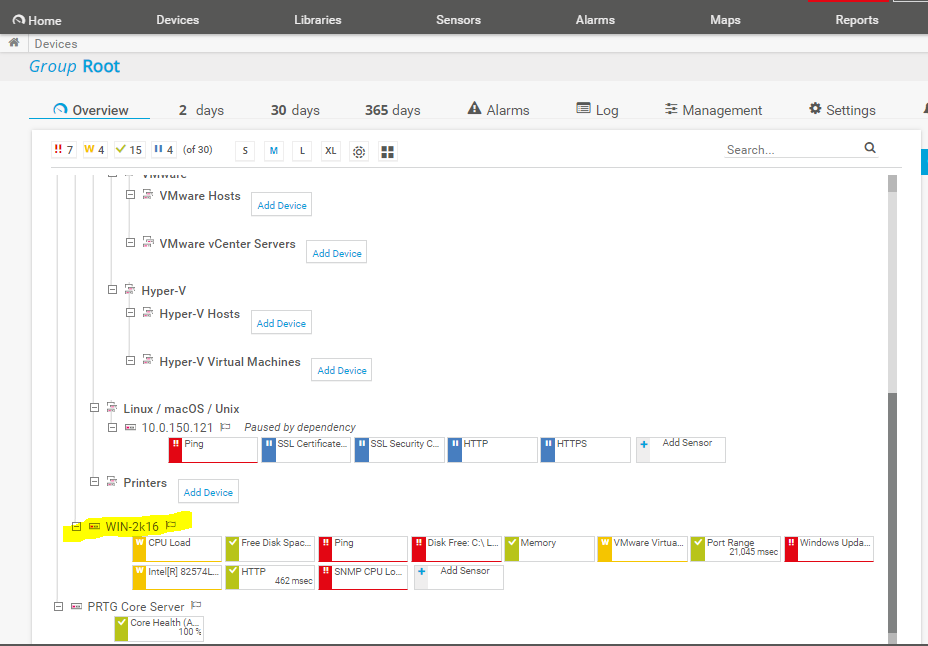
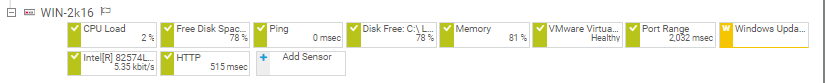
* Trong SNMP Services thiết lập trap destination (có địa chỉ IP là máy giám sát)

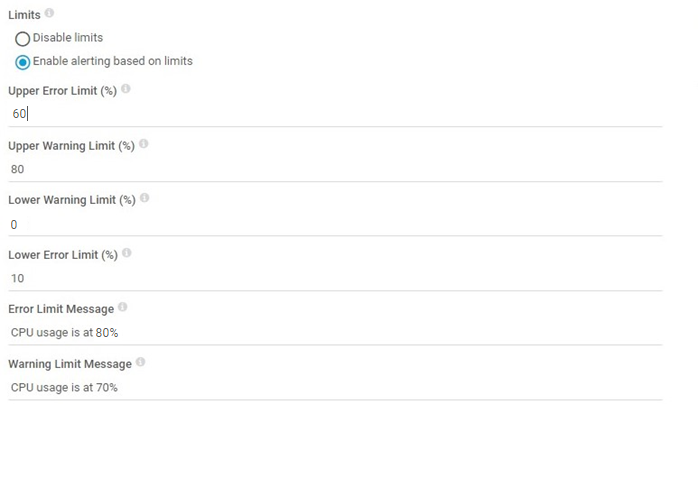


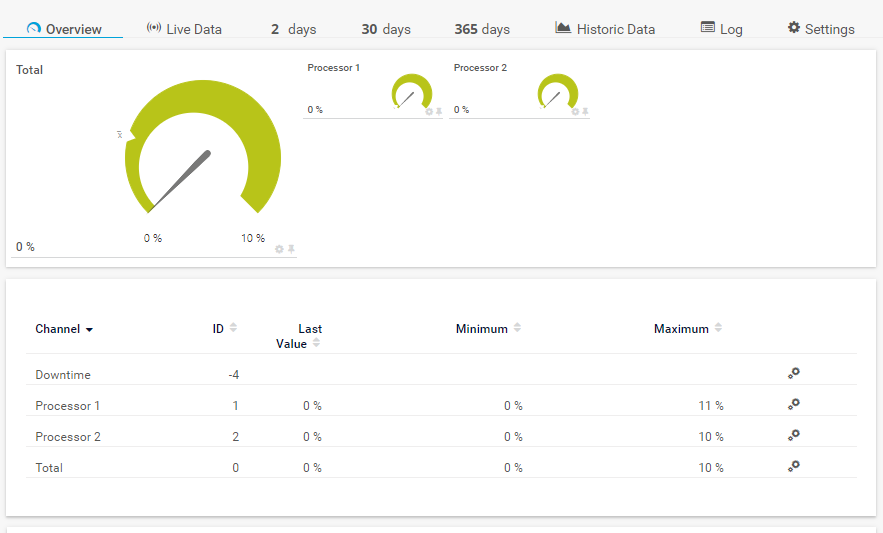


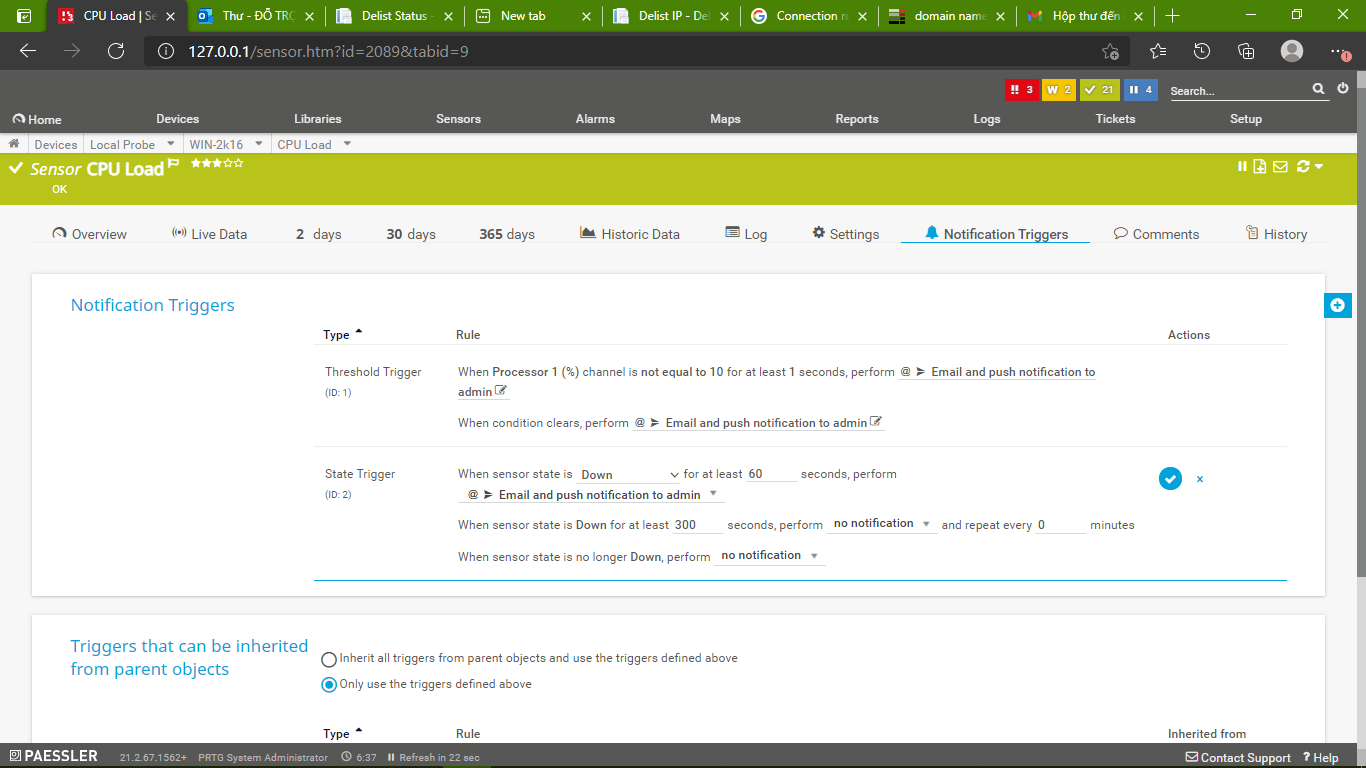
* 1. Tiến hành giám sát (các thao tác được tiến hành trên máy giám sát)
* Chọn add device để thêm thiết bị cần scan
* Vì máy cần được giám sát có tài khoản và mật khẩu nên ta cần thêm nó vào ở mục **Credential**



* Sau đó vào mục Devices và tìm thiết bị cần giám sát
* Khởi động lại máy được giám sát (Windows Server 2016), ta được kết quả giám sát như hình dưới. Ngoài ra có thề thêm các chức năng cần được giám sát ở mục **Add Sensor**
  1. Thiết lập ngưỡng cảnh báo
* Thiết lập ngưỡng cảnh báo với hiệu suất CPU



* Ngoài ra, các kết quả giám sát thường có các biểu đổ, thông số (state). Ta có thể thiết lập các cảnh báo đó sẽ được gửi qua email.
* Trong phần Notifications Trigger ta chọn add state trigger hoặc threshold trigger tùy vào mục đích



* Nhận được email cảnh báo, do máy được giám sát là máy ảo nên có đính kèm theo thông tin của máy thật (tên máy thật: **DESKTOP-2VP3D1S**)

