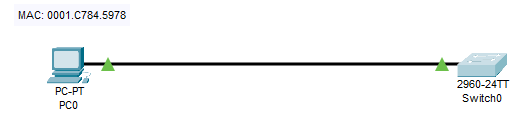
Huỳnh Nghiêm Phú Hưng

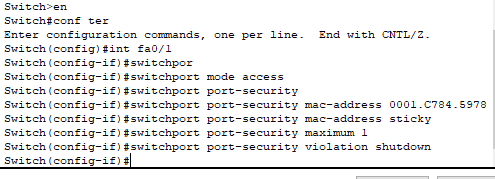
1712478

LAB 3 LAN SECURITY

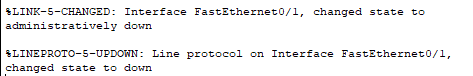
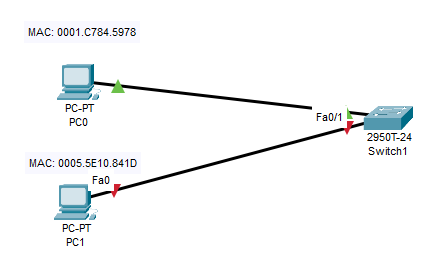
1 Port Security



Cấu hình port security. Chỉ có client với địa chỉ MAC: 0001.C784.5978 được sử dụng port fa0/1 trên Switch. Các client khác gắn vào port fa0/1, port fa0/1 sẽ bị shutdown

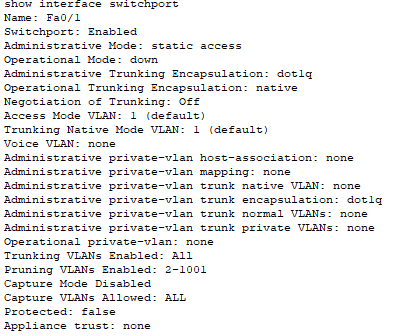


Thử cho PC có MAC 0005.5E10.841D gắn vào port fa0/1.

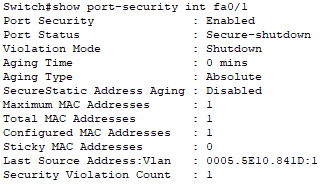


#### Kiểm tra cấu hình

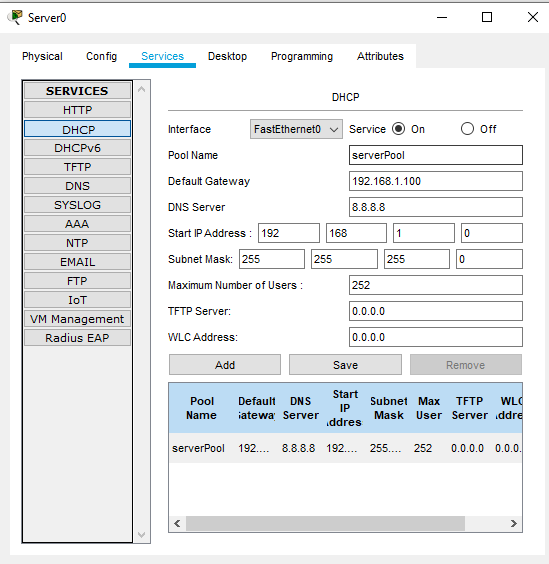
*show interface switchport*

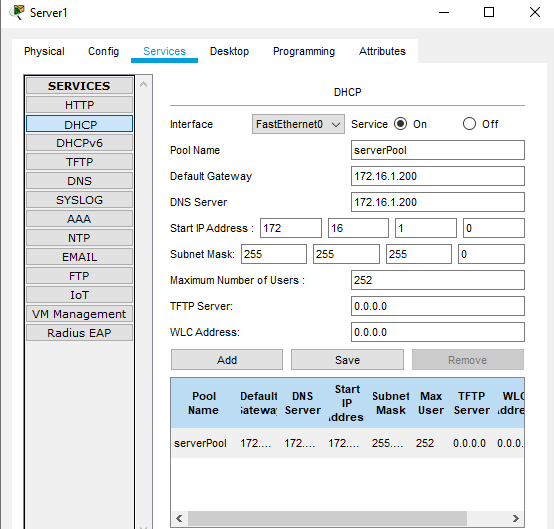


*show port-security interface fa0/1*

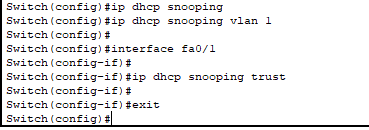


2. DHCP Snooping

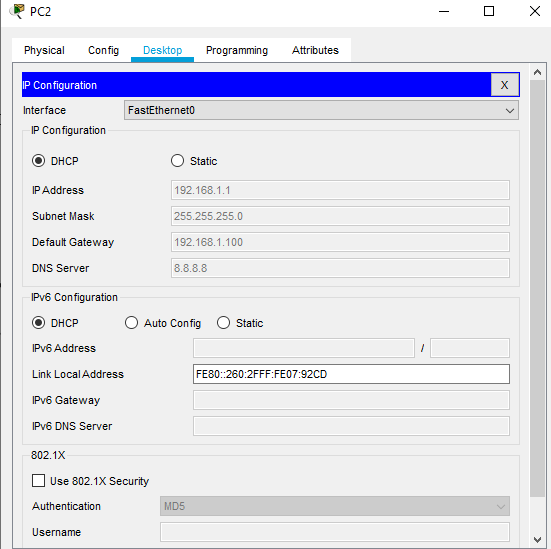




Cấu hình DHCP snooping trên Switch, sao cho các client chỉ xin địa chỉ IP từ DHCP trên DHCP Server 0.

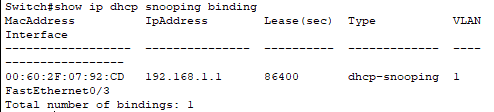


Tại PC client, cấu hình xin địa chỉ IP từ DHCP server. Kết quả, client xin được IP với các thông số do DHCP Server0 cấp.

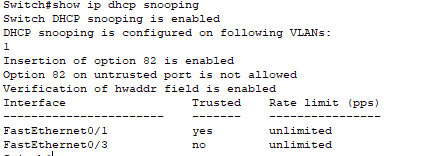


Kiểm tra cấu hình bằng các lệnh:

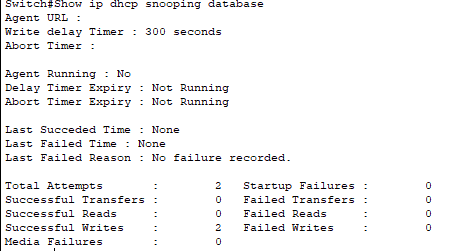
* show ip dhcp snooping binding



* show ip dhcp snooping

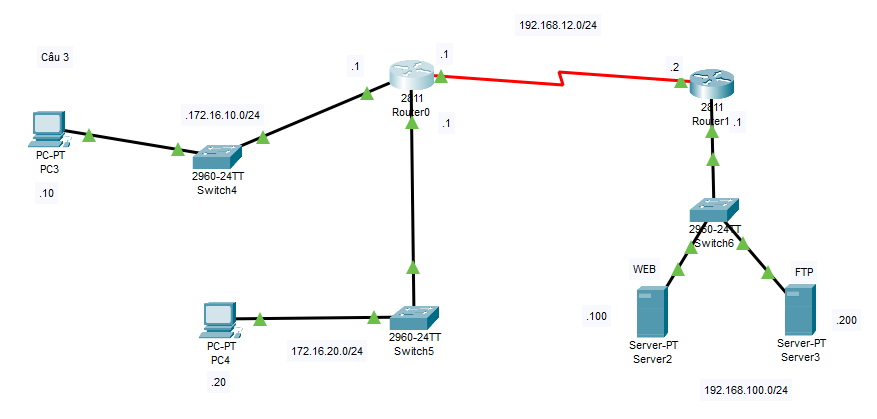


* Show ip dhcp snooping database



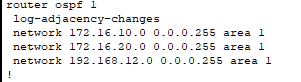
3 ACL

Topology:

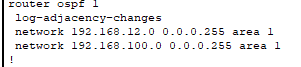


1 Cấu hình định tuyến cho hệ thống theo mô hình trên

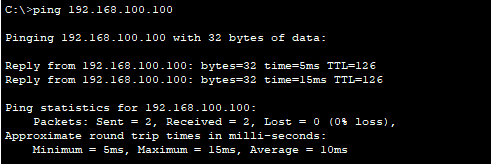
Router 0



Router 1

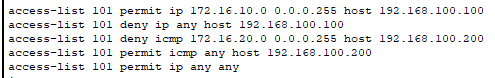


Các thiết bị mạng đã thông với nhau từ PC 3 ping tới web server



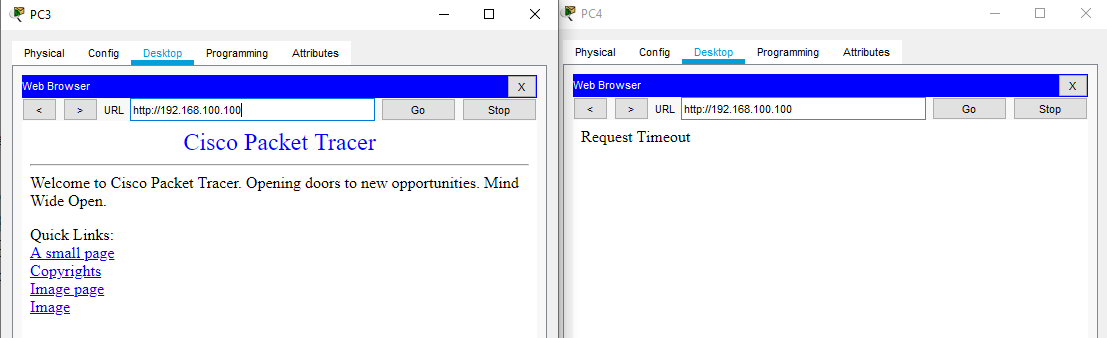
2 Cấu hình ACL

Router 1

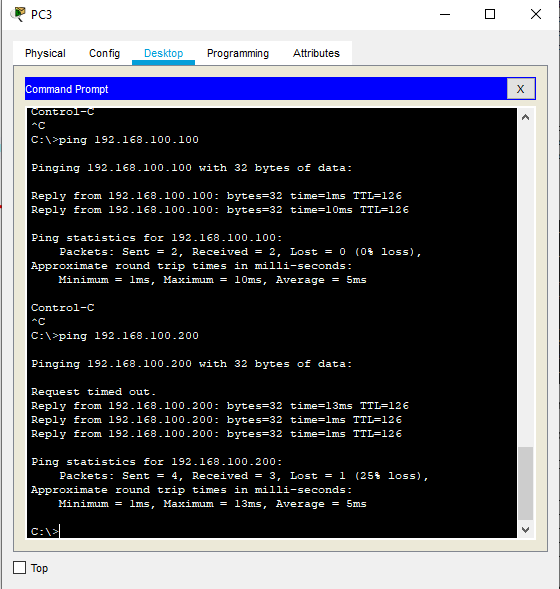


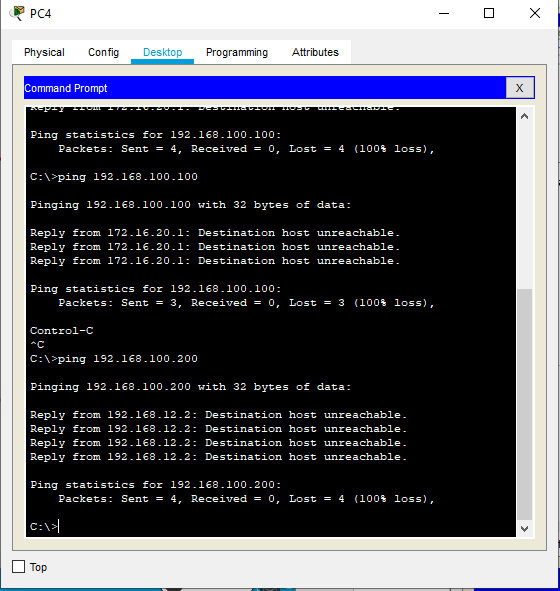
Interface f0/0

Ip access-group 101 out

A Chỉ cho phép các PC thuộc mạng 172.16.10.0/24 truy cập tới Web server bằng dịch vụ Web

B Cấm PC thuộc mạng 172.16.20.0/24 ping tới FTP server (192.168.100.200)





C Chỉ cho phép máy Admin (172.16.10.10) telnet/SSH tới các router (R1, R2) và các Switch

Router 0



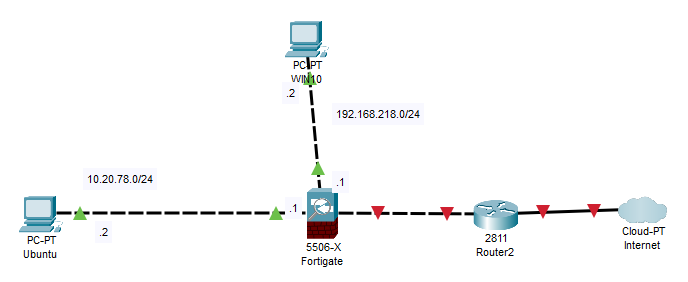


4. Firewall: Sử dụng Fortigate

Nguồn tham khảo:

<https://www.youtube.com/watch?v=hd4u6crwxAI>

- Topology



Chú thích:

Win10 là máy thật và chỉ đóng vai trò là máy cấu hình cho firewall và cầu nối đi ra inter net

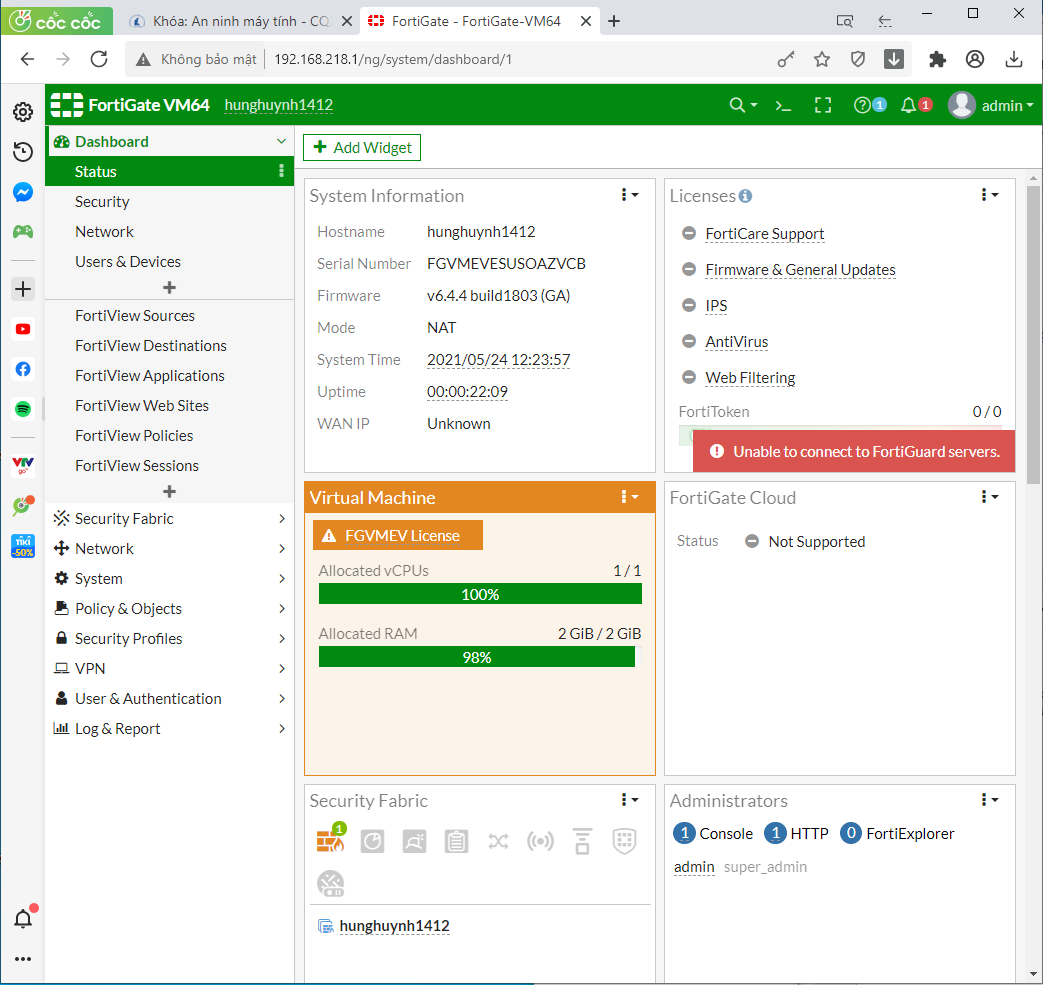
Ubuntu sẽ là máy ảo và bị giới hạn bởi rule của firewall fortigate

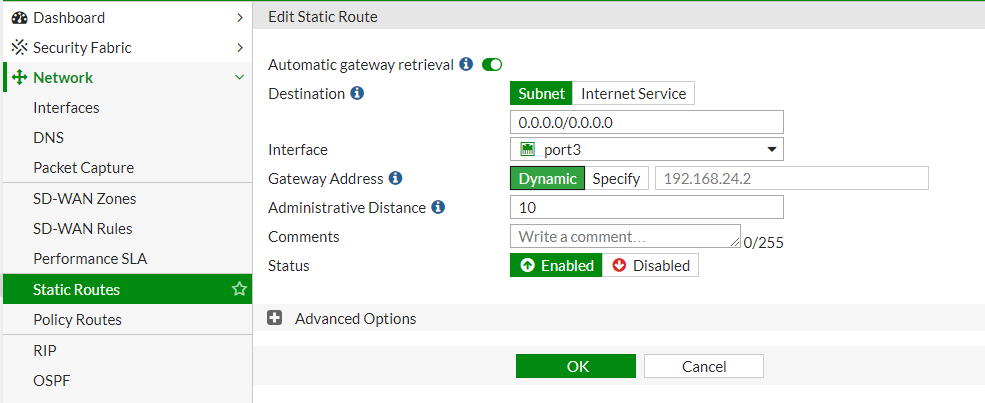
Port 1: Kết nối đến Window 10 (Host Only)

Port 2: Kết nối đến Ubuntu (Host Only)

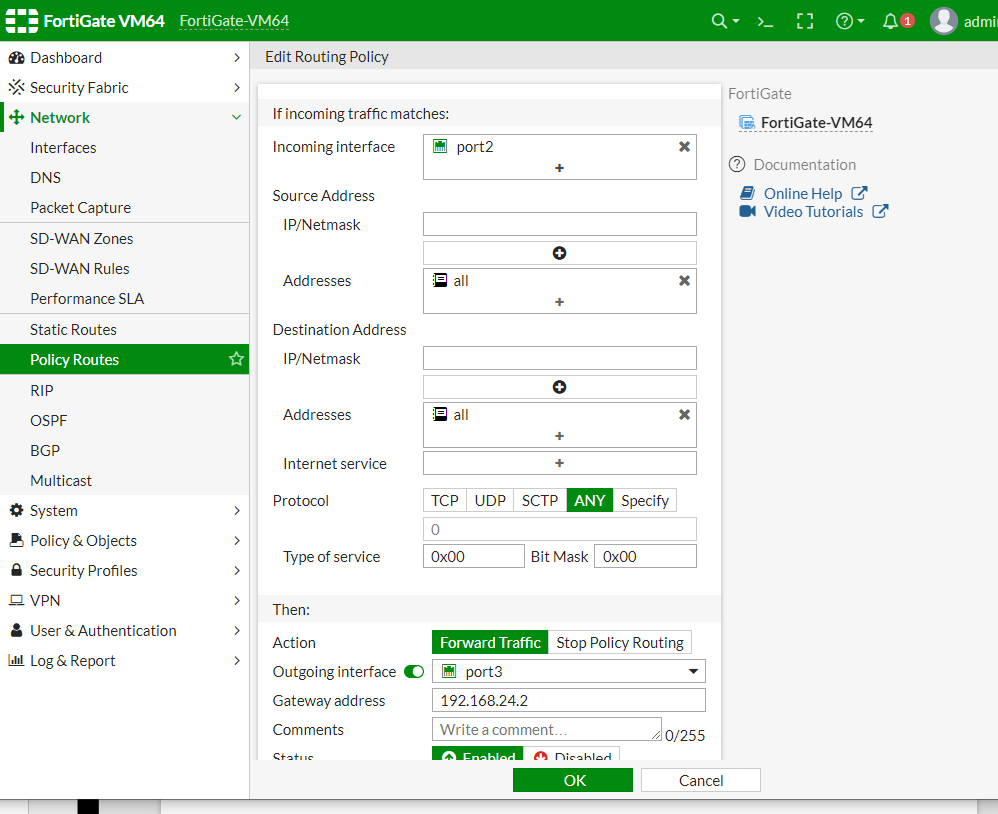
Port 3: Đi ra ngoài mạng (NAT)

Sau khi thiết lập các thông số như mô hình trên và cài đặt Fortigate VM, tại win 10 sẽ thực hiện kết nối tới Fortigate qua giao diện trên Web browser để cấu hình.

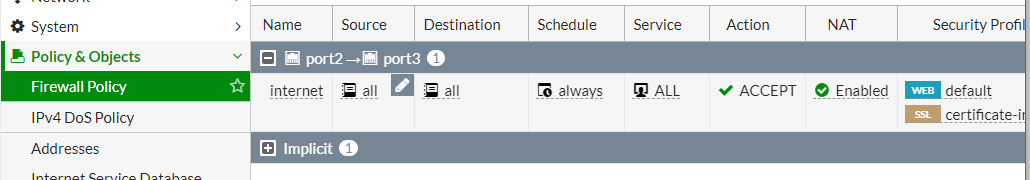


Để cho phép thiết bị trong LAN kết nối ra Internet, đầu tiên cần tạo Static Route hướng traffic đến Router. 

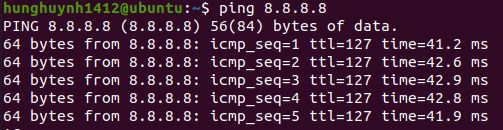
Tiếp theo là Forward Traffic từ LAN sang port hướng ra Router trong phần Policy Routes



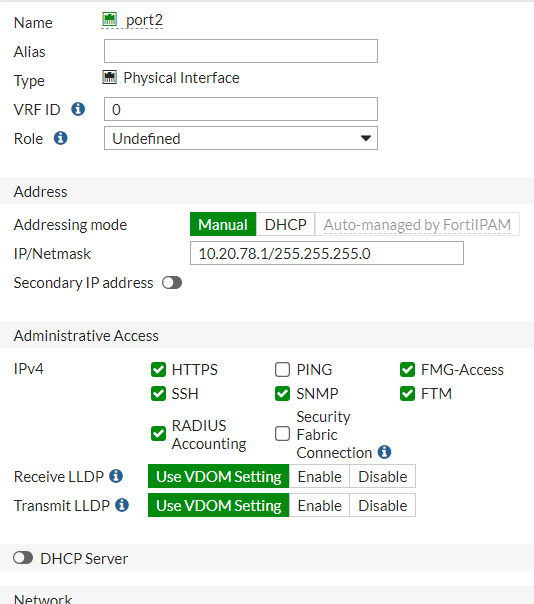
Cuối cùng là Rule cho phép traffic trong Lan có thể ra ngoài Internet ở mục Firewall Policy.



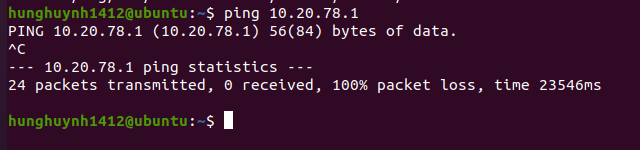
Kiểm tra kết nối Internet tại Ubuntu



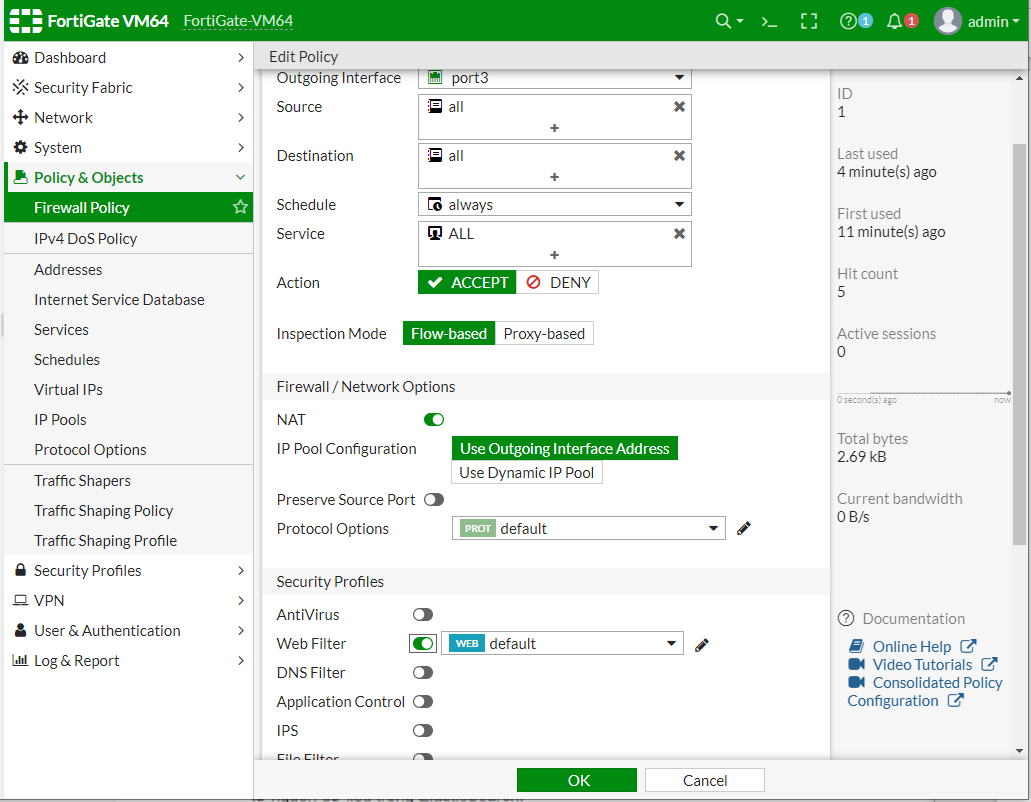
Có thể kiểm soát các giao thức trên port LAN bằng cách tùy chỉnh trong phần Interface. Ở đây bỏ chọn PING.



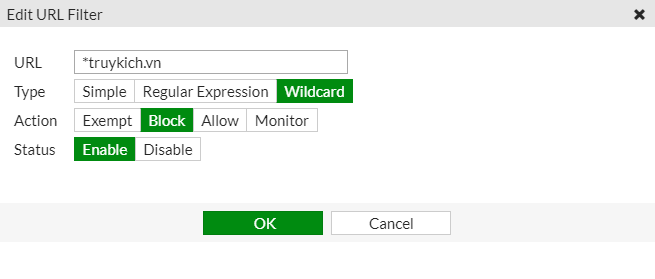
Kiểm tra Ping tại Ubuntu.

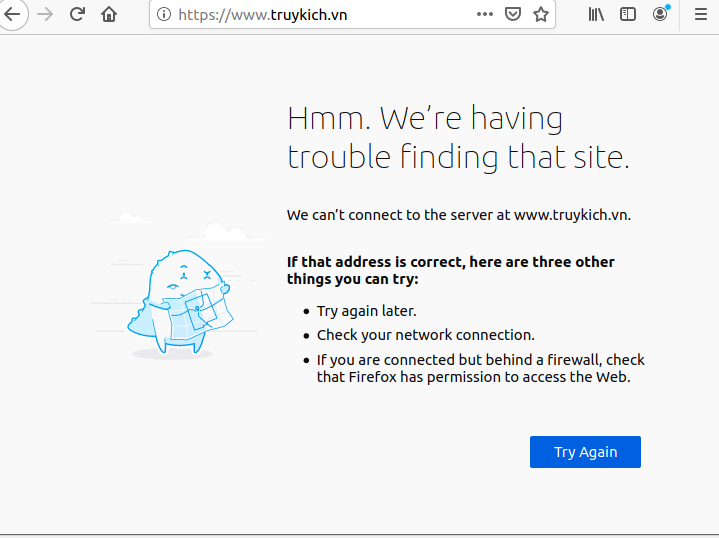


Có thể block các Website bằng Web Filter. Tùy chỉnh trong Policy forward internet vừa được tạo trong Firewall Policy, chọn Edit (hình cây viết)

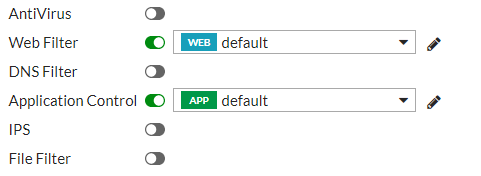


Thêm vào URL muốn block. Ở đây sẽ block website truykich.vn

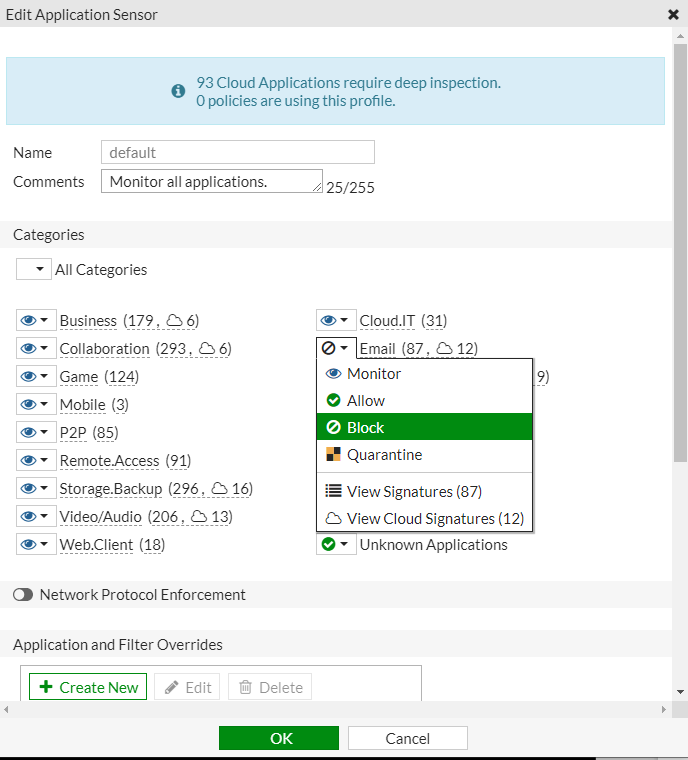




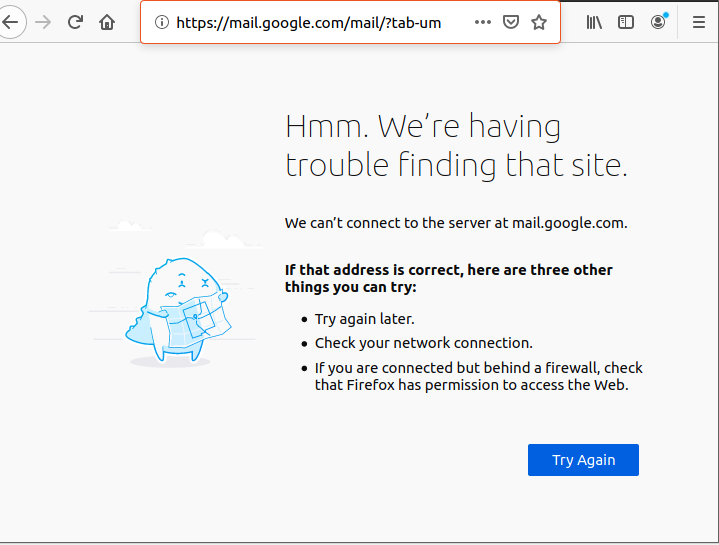
Có thể kiểm soát các ứng dụng bằng cách bật Application Control trong Policy forward internet và chọn Edit.



Tủy chỉnh ứng dụng muốn kiểm soát. Ở đây sẽ chọn hành động chặn những truy cập liên quan đến Email. Có thể xem trong phần View Signatures để xem những ứng dụng liên quan hoặc có thể tự thêm ứng dụng vào mục này

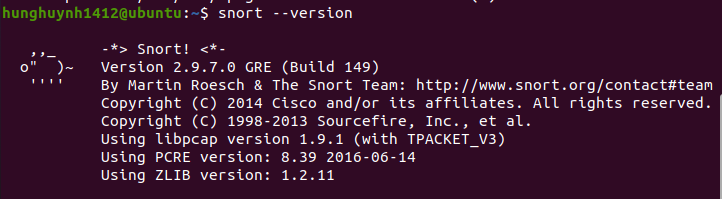


Truy cập gmail tại Ubuntu sẽ bị firewall từ chối, kết quả hiển thị Time out



5. Snort-IDS

- Cài đặt Snort trên Ubuntu, bằng lệnh: apt-get install snort (ở quyền sudo hoặc root). Kiểm tra cài đặt thành công bằng lệnh: snort –version

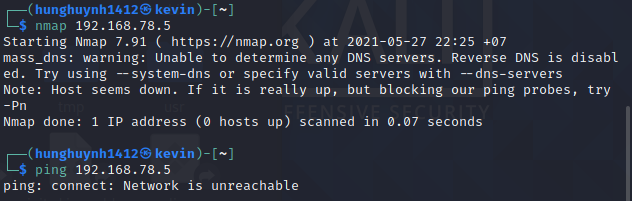


- Sử dụng Nmap trên Kali (IP 192.168.78.4) để làm công cụ tấn công, nhập: nmap 192.168.78.5 (IP của Ubuntu).

- Tại Ubuntu, sử dụng Snort để theo dõi trên interface ens33 (IP 192.168.78.5), nhập lệnh: snort -A console -q -c /etc/snort/snort.conf -i ens33

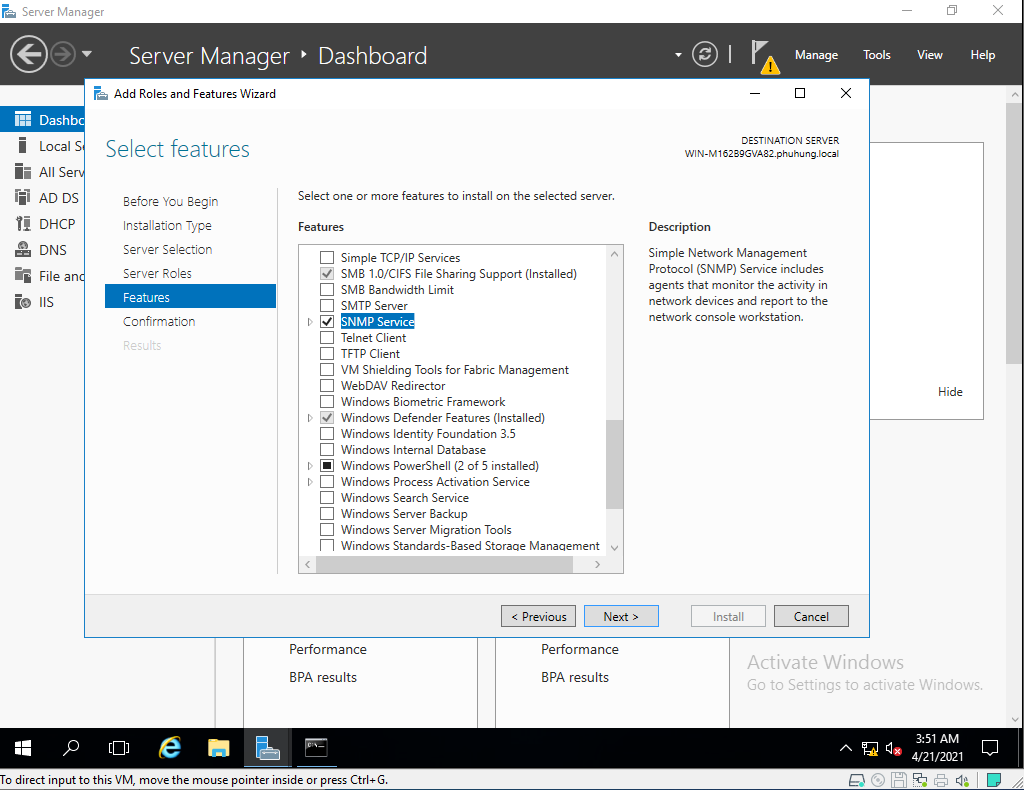
- Snort phát hiện SNMP request từ 192.168.78.4 (IP của máy Kali), phân loại là Attemted Information Leak.



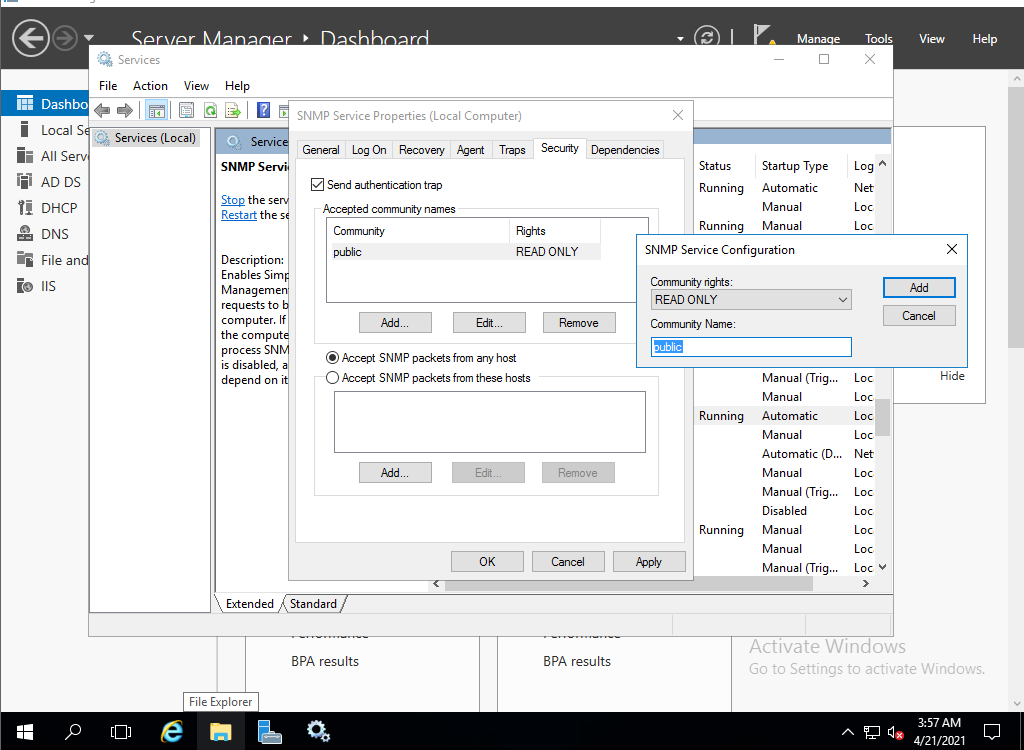


6. Network Monitorign System

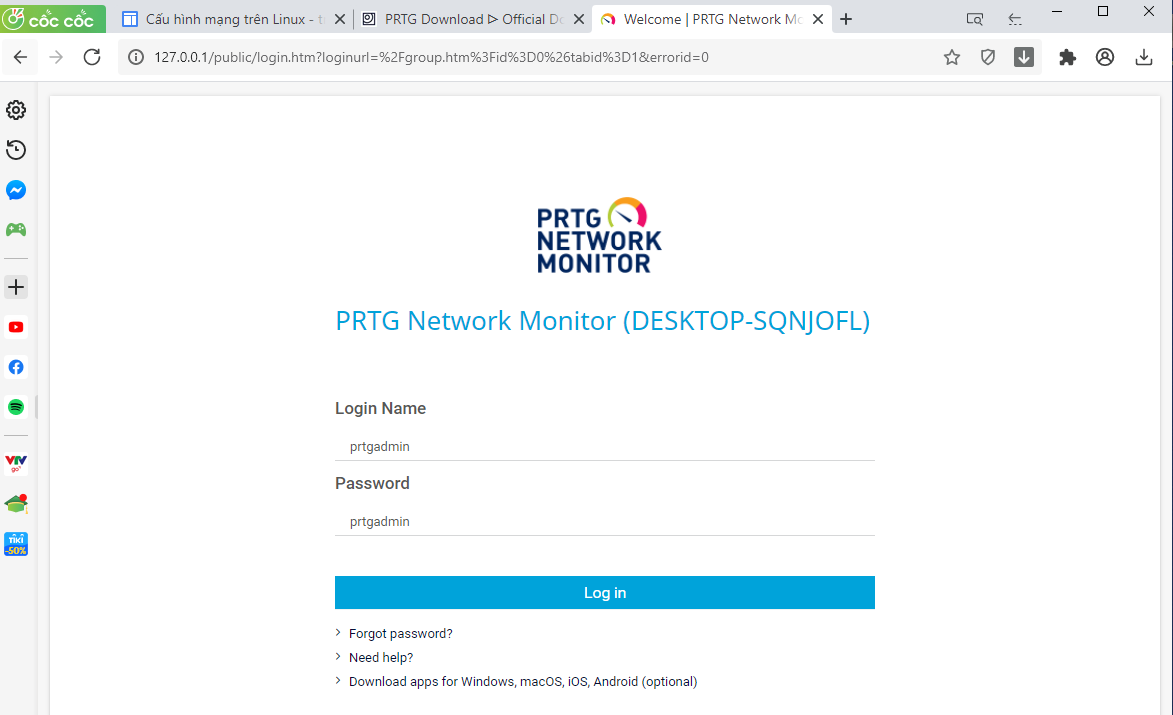
- Tại Window Server 2016, cài đặt SNMP service.



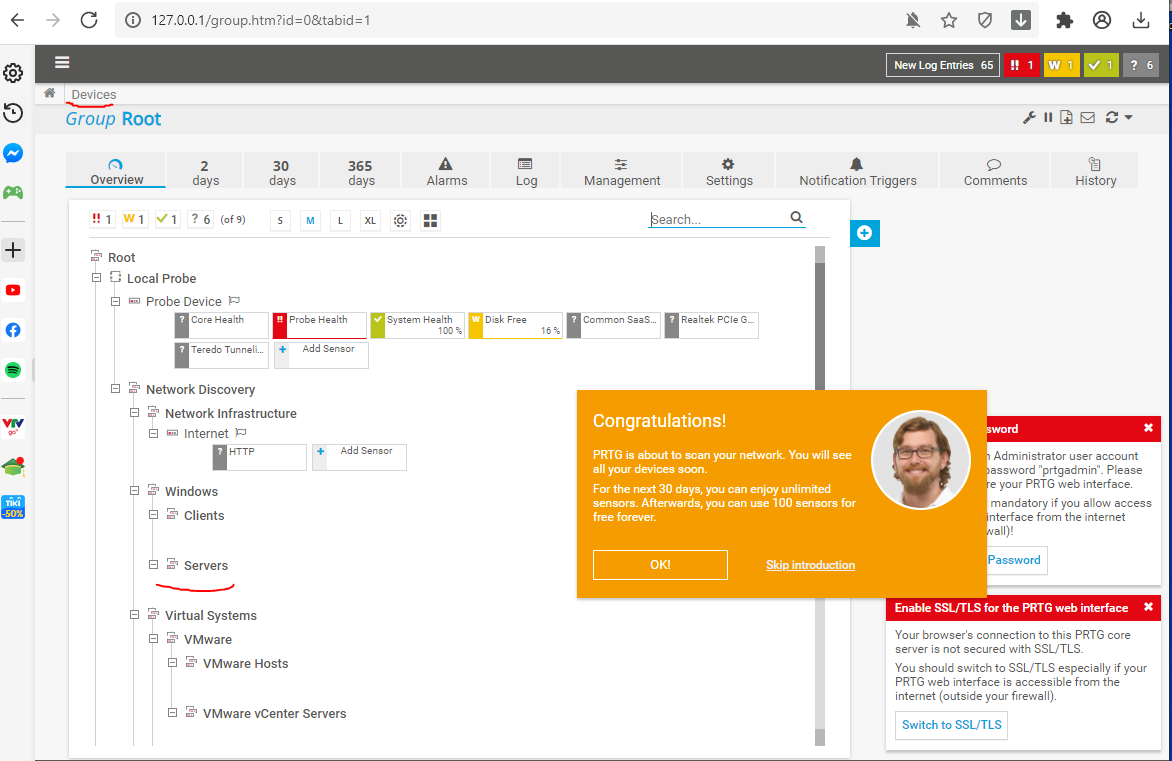
Sau khi cài đặt, vào thiết lập trong SNMP service, thiết lập community string là public và tích chọn Accept SNMP packet from any host



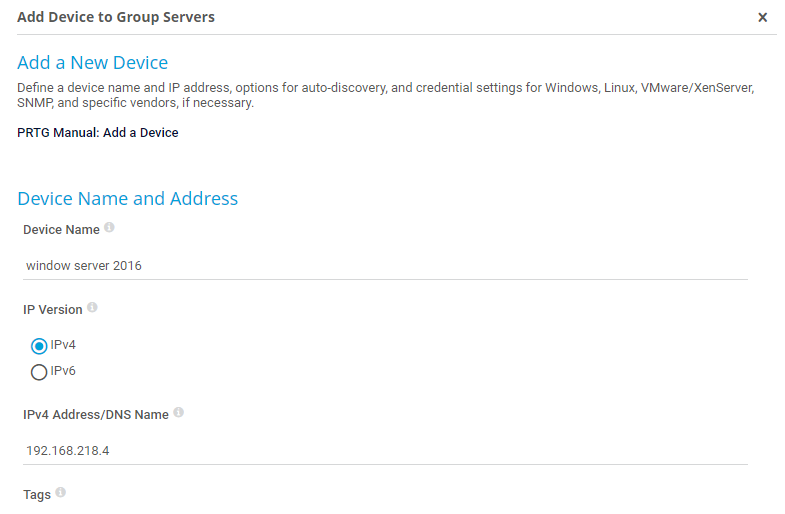
- Tải và cài đặt PRTG trên máy thật (Win 10 Home SL). Cài đặt thành công khi khởi chạy sẽ có giao diện sau trên Web Browser



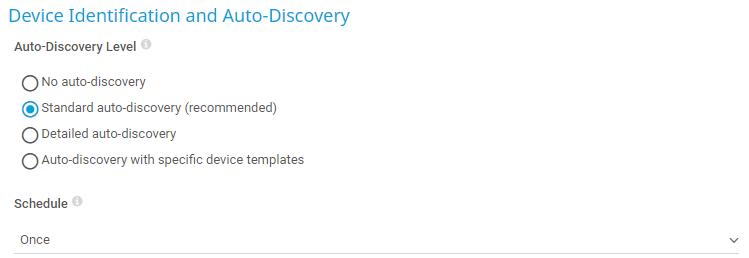
Login. Sau đó thực hiện thêm thiết bị cần giám sát tại tab Devices. Nhấp chuột phải trên mục Servers, chọn Add Device.



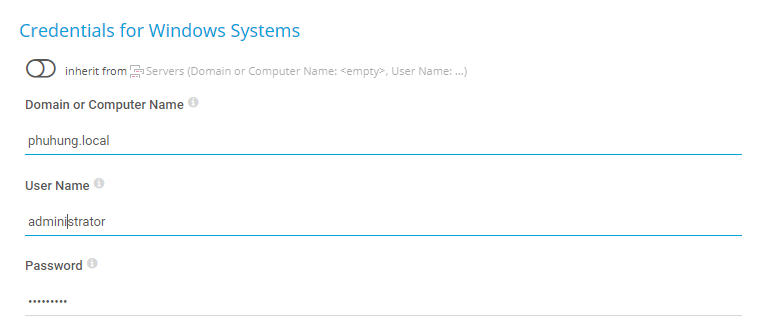
- Nhập vào IP của Window server 2016



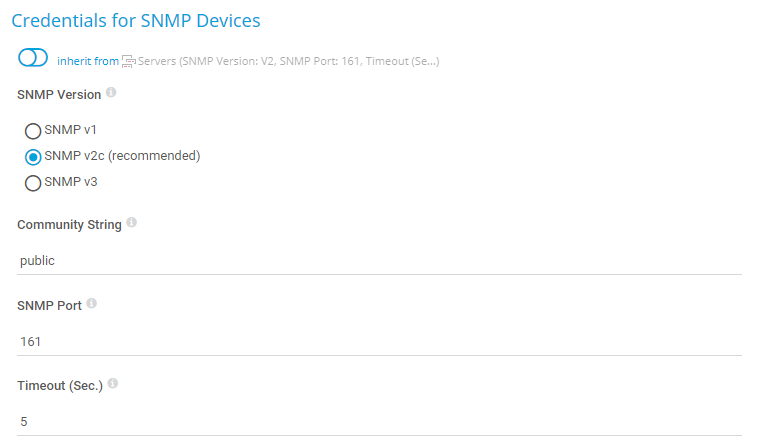
Chọn Standard auto-Discovery tại mục Device Identification and Auto-Discovery



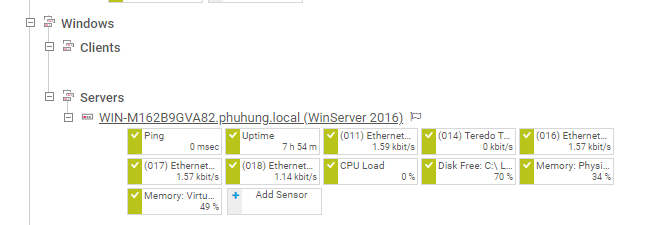
- Điền tên domain, tài khoản và mật khẩu của window server 2016

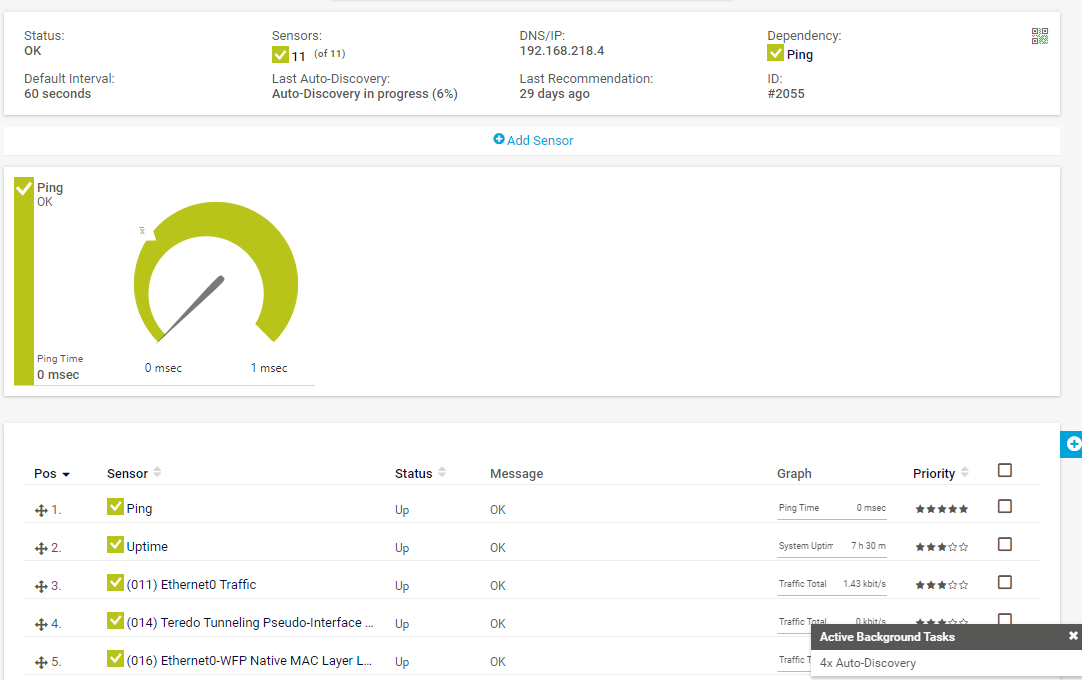


- Đảm bảo SNMP với community string là public, giống với đã thiết lập ở trên

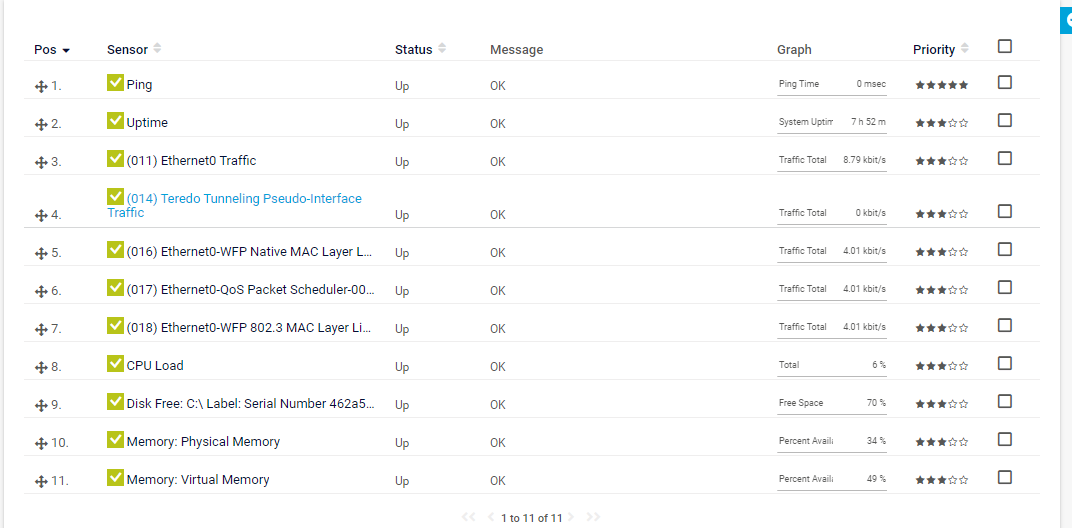


Sau 1 khoảng thời gian để Discovery, kết quả giám sát window server sẽ được hiển thị ở mục Server, nhấp chuột vào để hiển thị giao diện chi tiết.

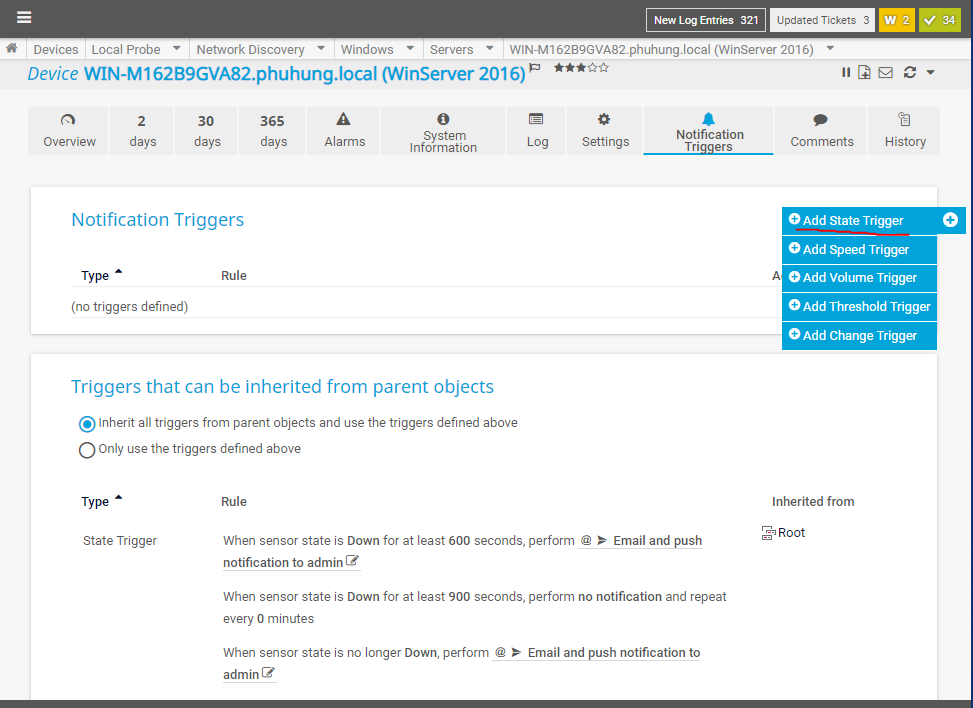




Giám sát tình trạng CPU của server hiện đang là 6%, Free Disk là 70%, Memery 34%, ... v.v



Để thiết lập ngưỡng cảnh báo. Chuyển qua tab Notification Trigger.Ở đây, thực hiện cảnh báo khi có sự thay đổi trạng thái trên window server



Tùy chỉnh các thông số, hành động khi vượt ngưỡng.

