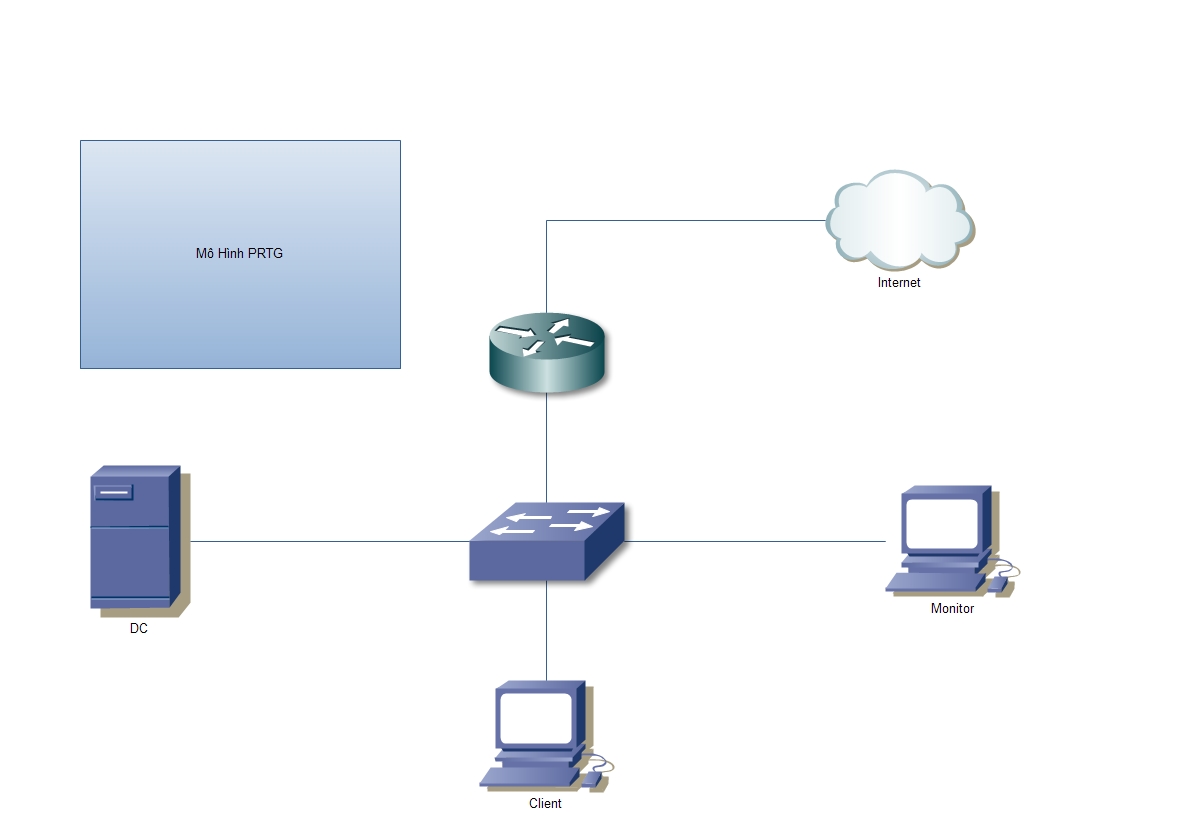
1. Mô hình thực hiện



Mô hình thực hiện gồm

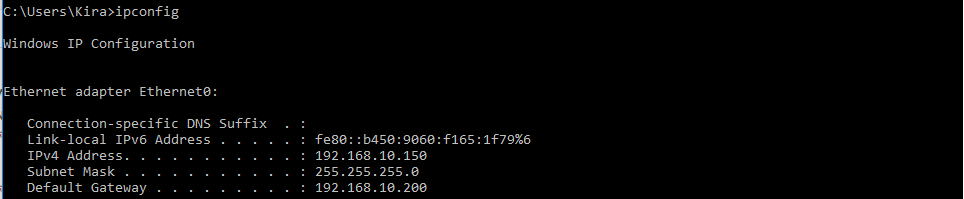
+ 1 Router định tuyến các end user và server ra internet

+ 1 Máy làm Monitor ( Win 10 )

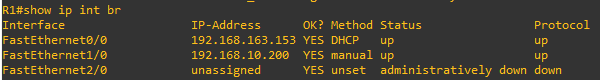
+ 1 DC ( Windows Server 2012)

+ 1 Máy Client ( Option )

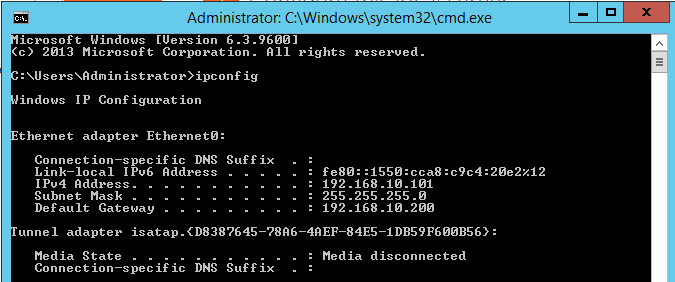
Địa chỉ máy Monitor



Địa chỉ IP Router Cisco



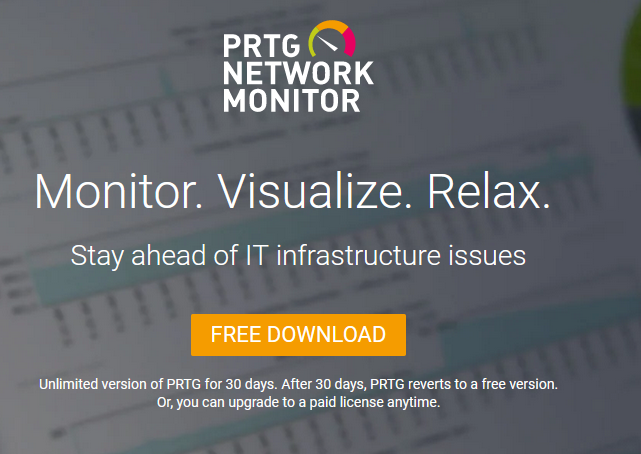
Địa chỉ IP Máy Chủ DC



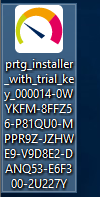
1. Tiến hành bài lab

**Bước 1: tải và cài đặt PRTG**

**https://www.paessler.com/prtg**

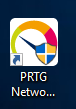


Ta tiến hành bấm vào Free Download để tải 1 bản try dùng 30 day

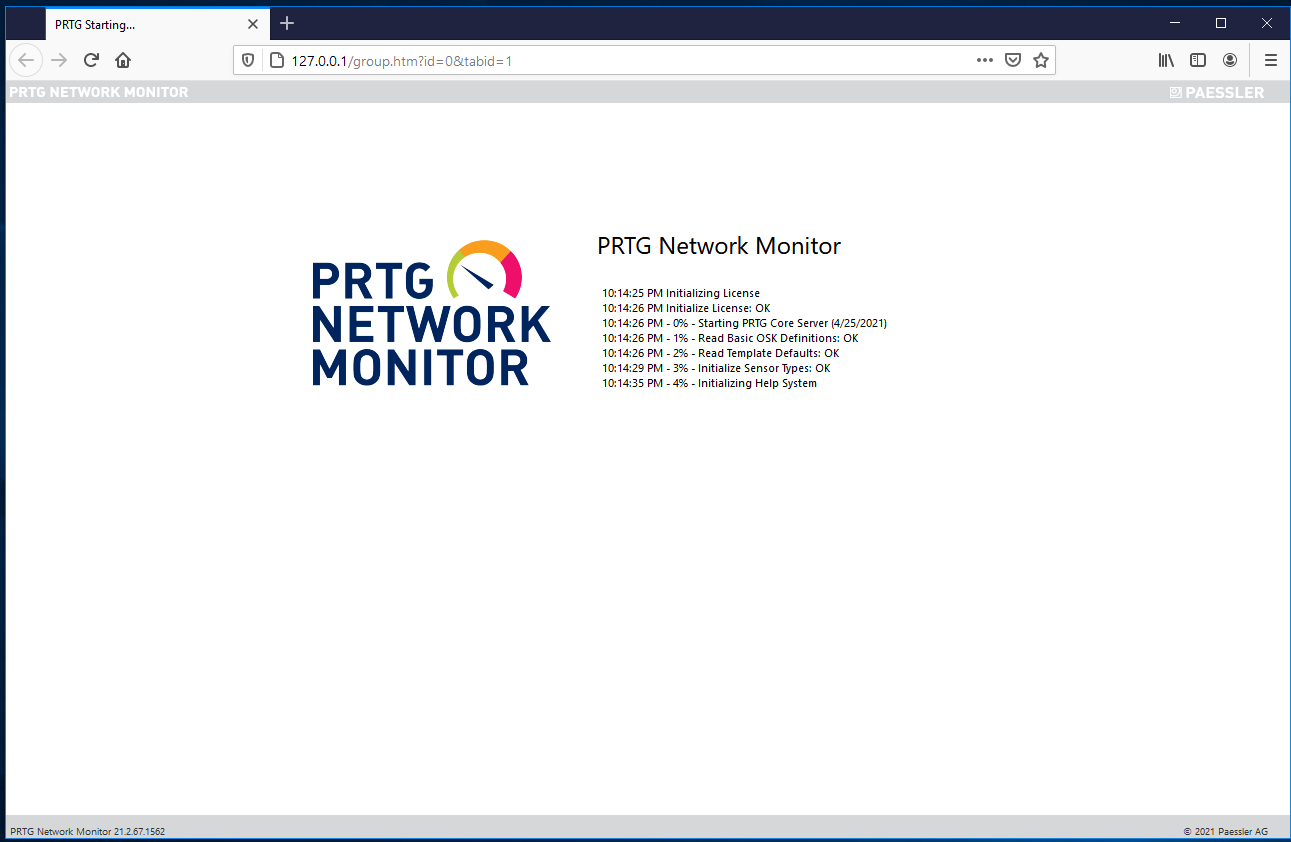


Sau khi tải xong ta sẽ được file exe như thế này đã bao gồm cả key try trong đó

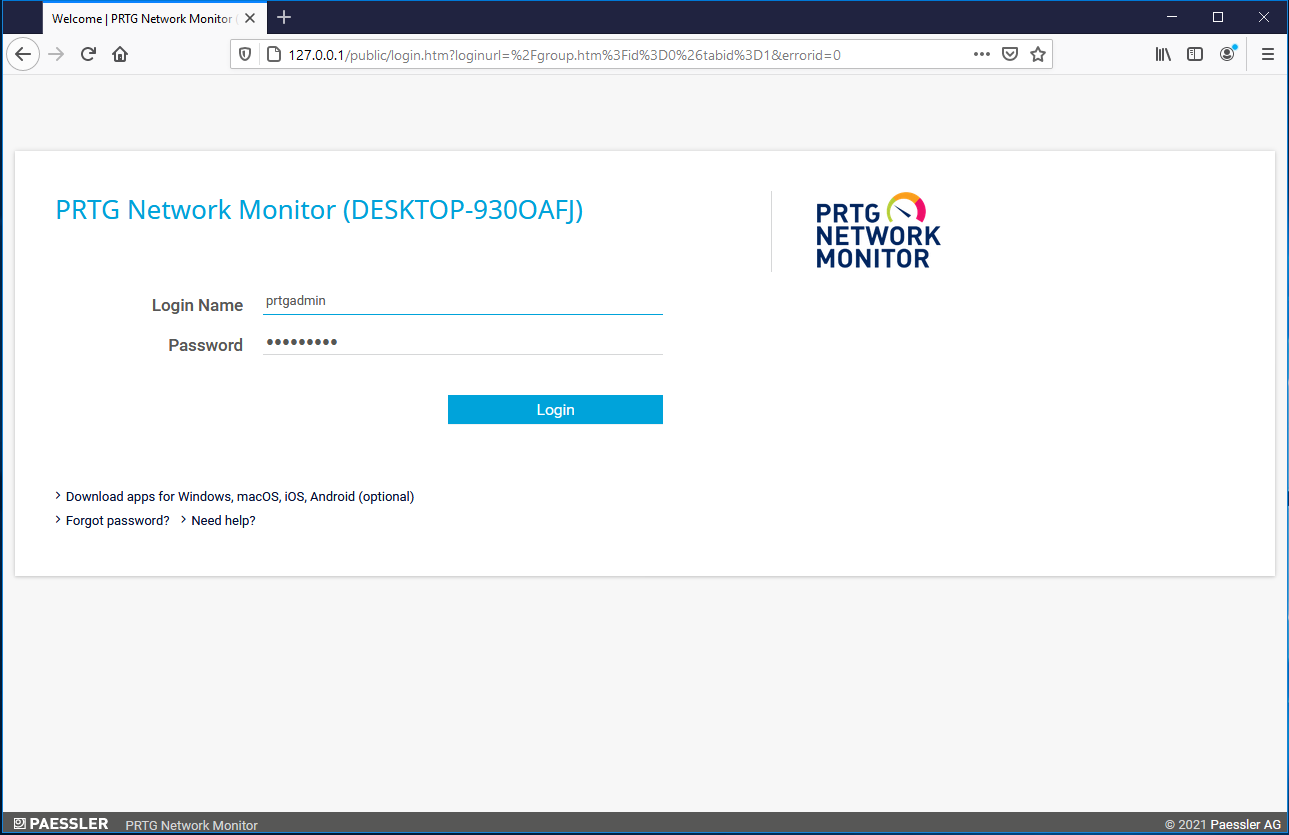
Tiến hành cài PRTG chỉ cần bấm next next liên tục và đảm bảo máy cài đặt phải có mạng



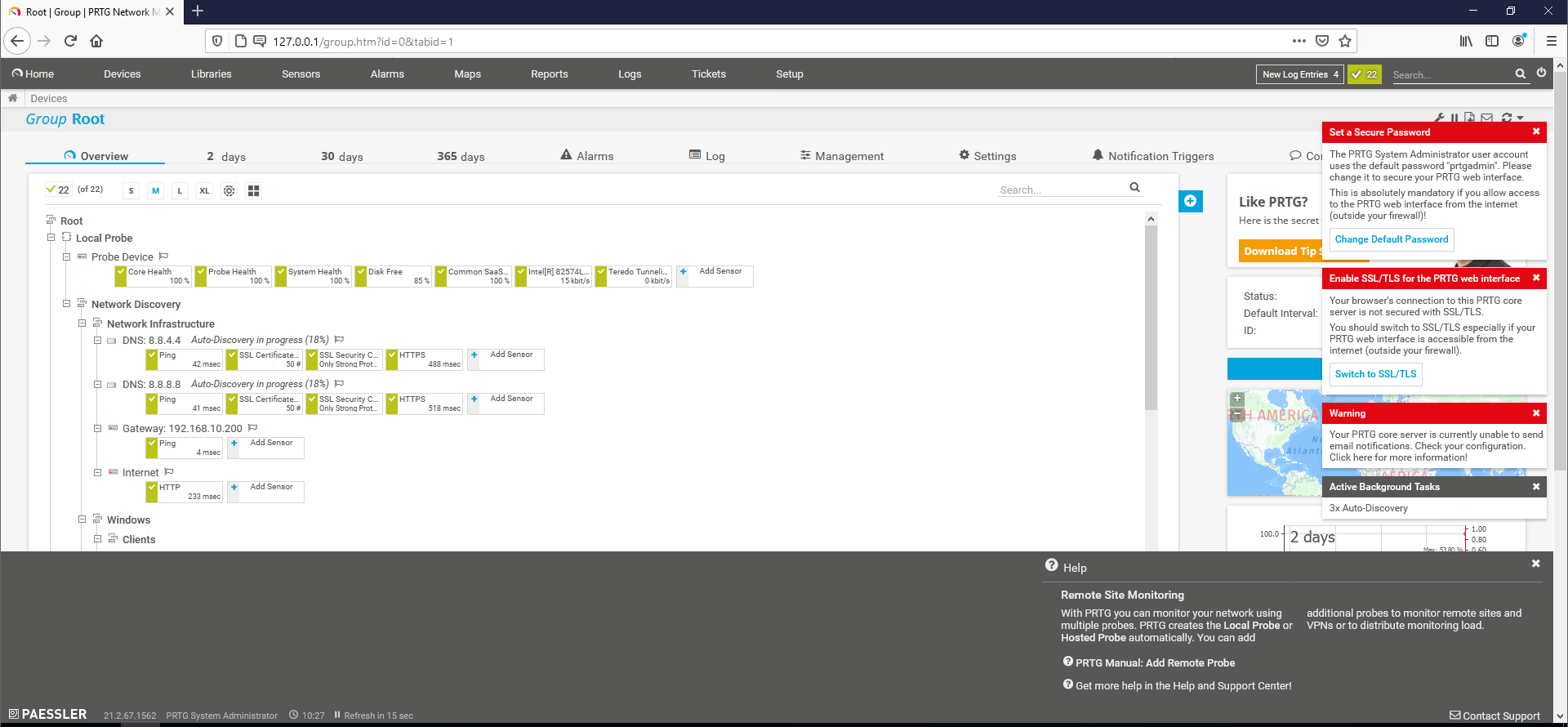
Sau khi cài xong ta sẽ có được icon như thế này . Tiến hành mở PRTG bằng cách nhấp đúp vào



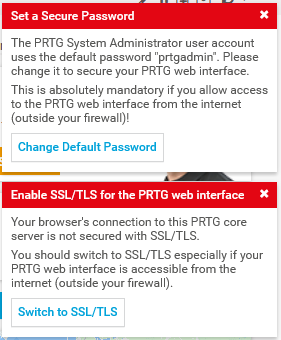
1 Giao diện web sẽ hiện ra ta đợi load để đăng nhập PRTG quản lí bằng giao diện web



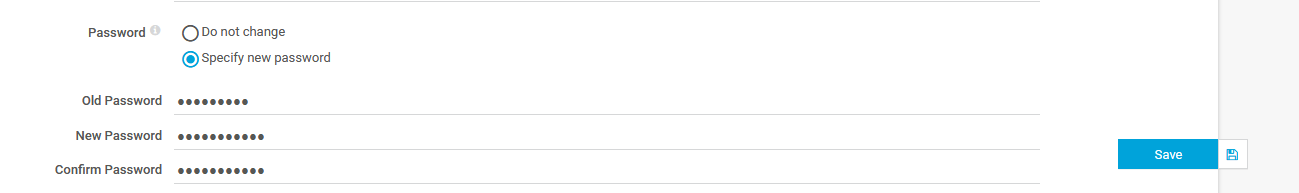
Lúc này ta có Username là **prtgadmin** password **prtgadmin** ta nên tiến hành thay đổi password khi login thành công



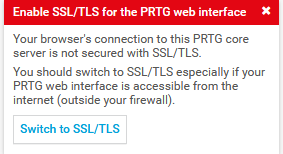
Ta sẽ được giao diện quản lí như thế này để ý bên góc phải



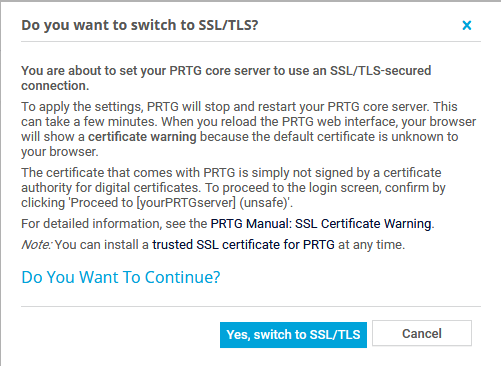
Nhấp vào Change Default Password để thay đổi password



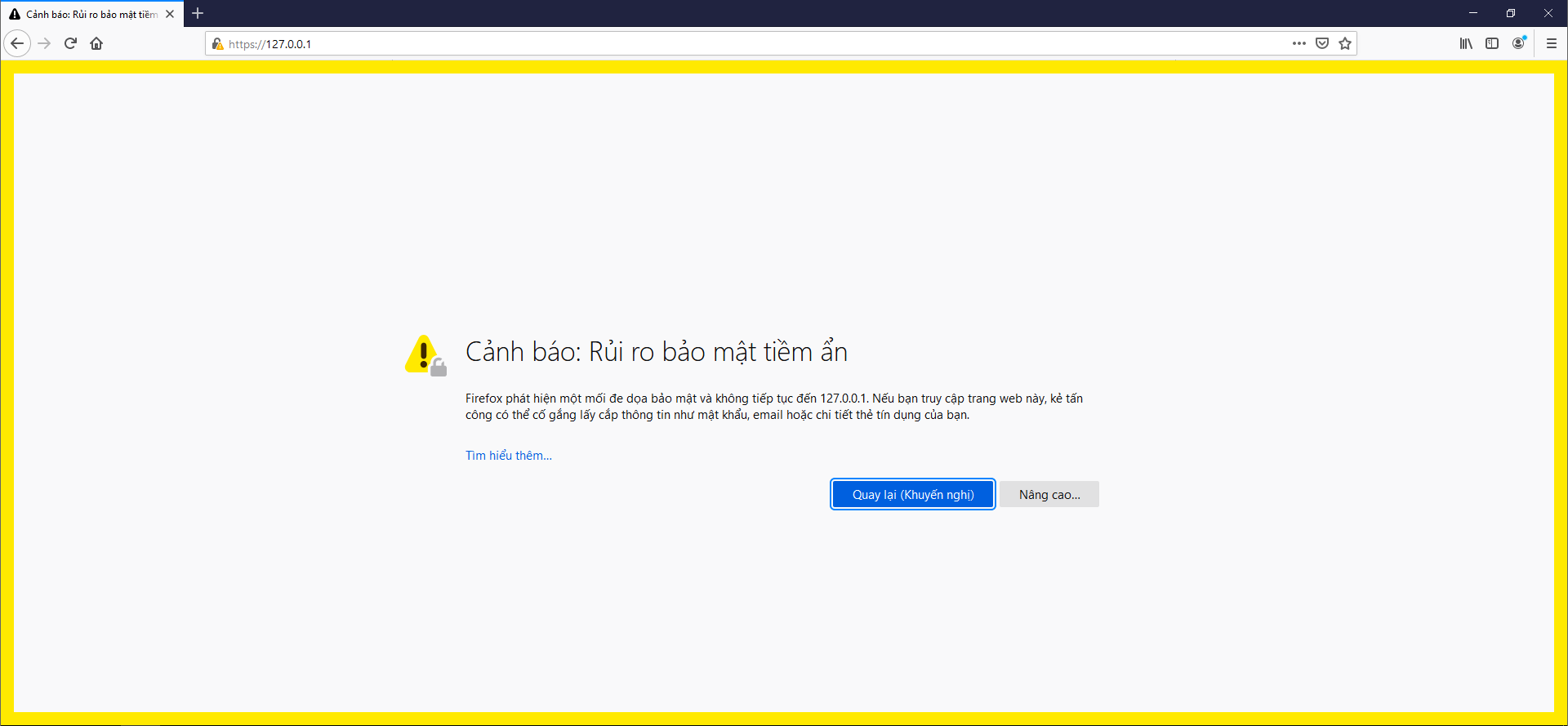
Chọn như hình nhập mật khẩu mặc định và mật khẩu ta muốn đổi và Save lại



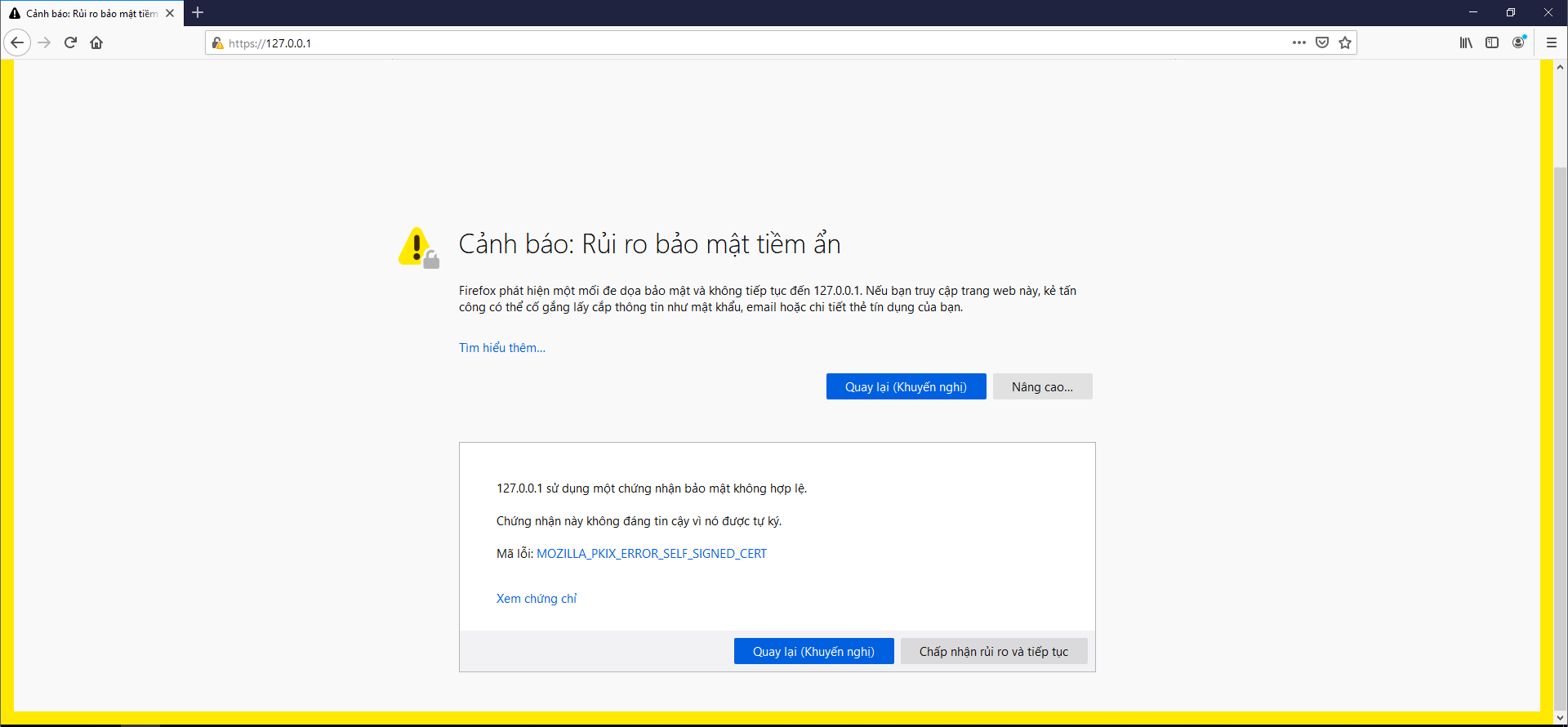
Sử dụng SSL để mã hoá các thông tin dư liệu lúc này trang web hiện tại là http sẽ chuyển sang https



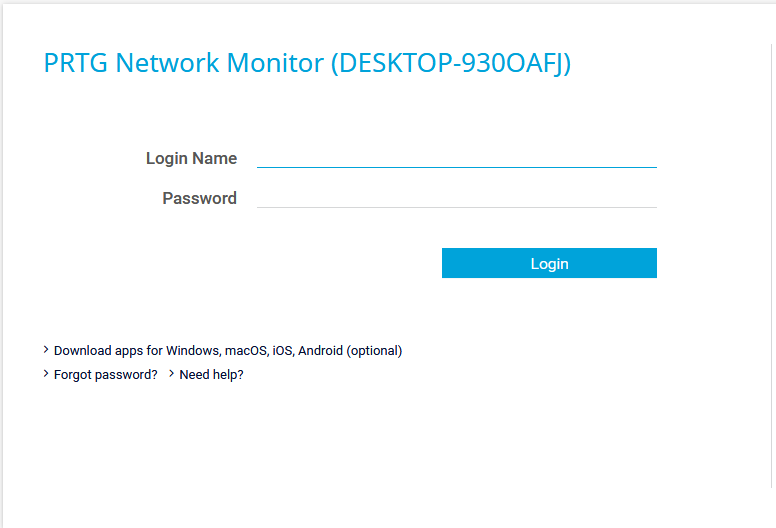
Chọn Yes



Lúc này ta thấy đường dẫn ta đã là https

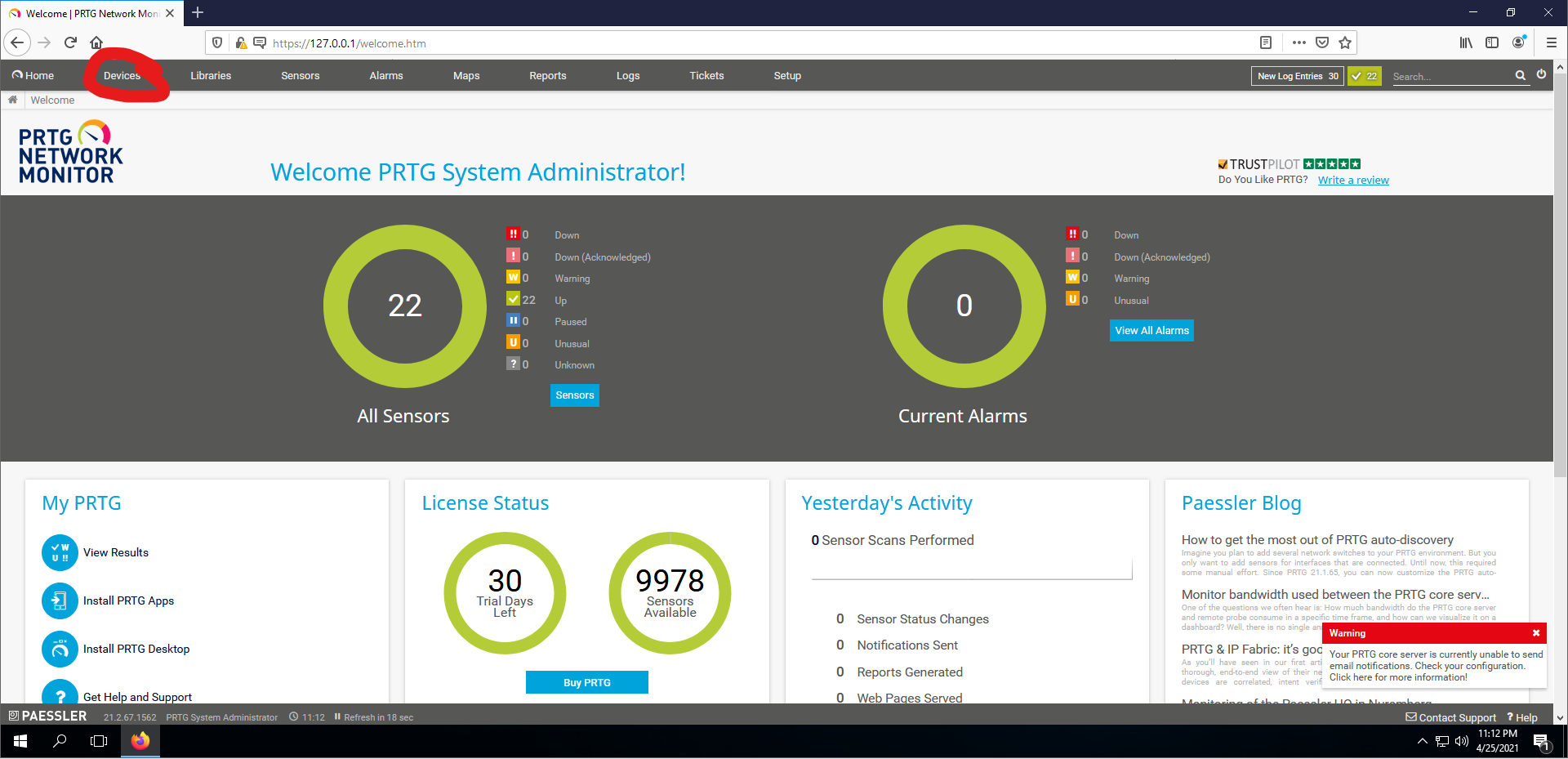


Chọn vào Nâng cao và bấm vào chấp nhận rủi ro và tiếp tục vì ta chưa có 1 Server để cấp chứng thực nên sẽ hiện thông báo như thế này

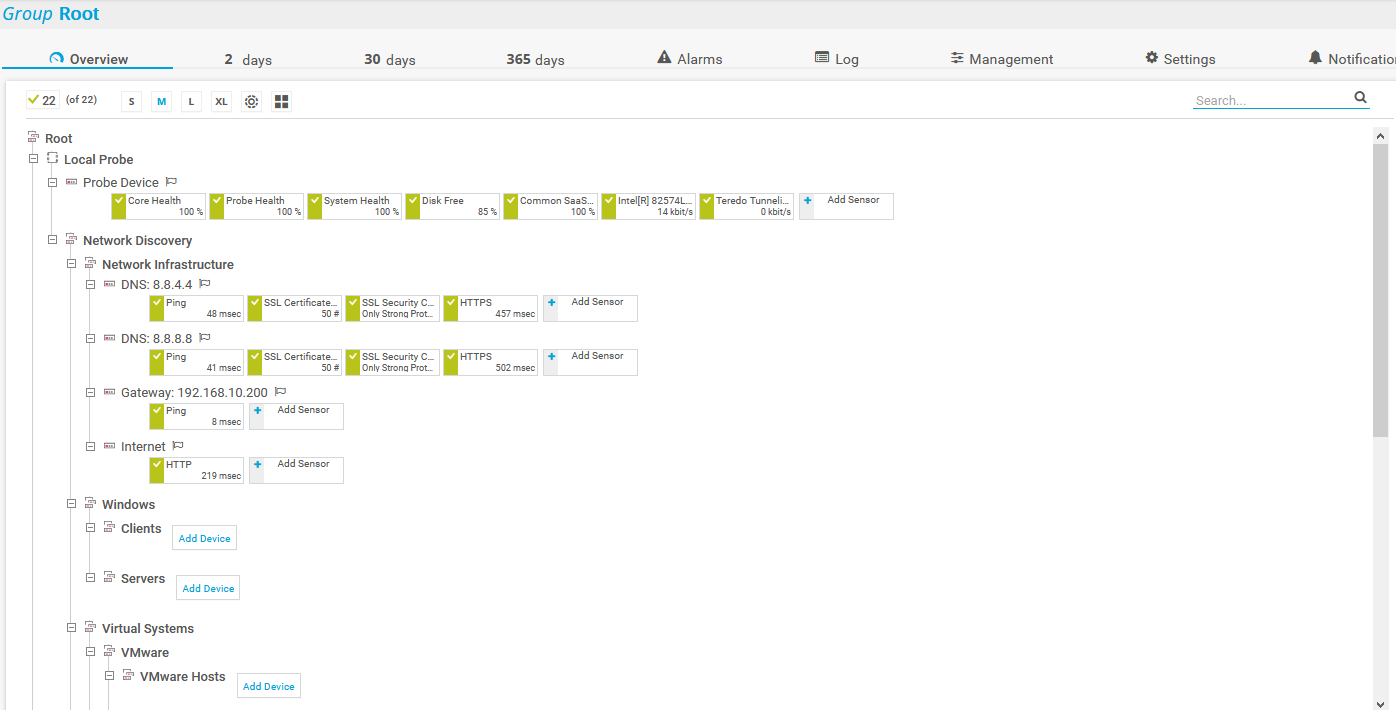


Tiến hành đăng nhập lại UserName: **prtgadmin** và Password: ( Password ta vừa đặt )

**Bước 2: Thêm các thiết bị cần giám sát vào PRTG**



Tiến hành chọn Device để xem các thiết bị ta đang giám sát

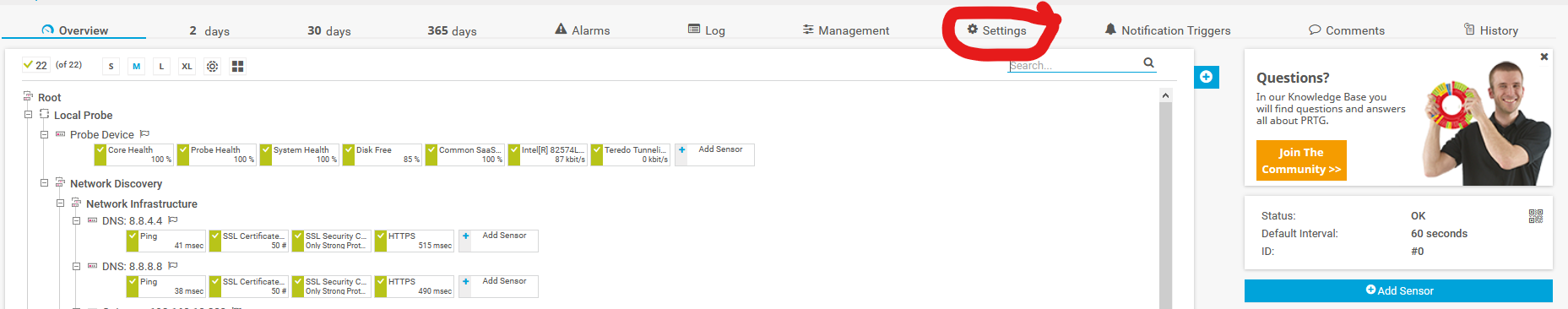


Ta sẽ thấy được rất nhiều thông số . Đây là những thông số trên local của ta

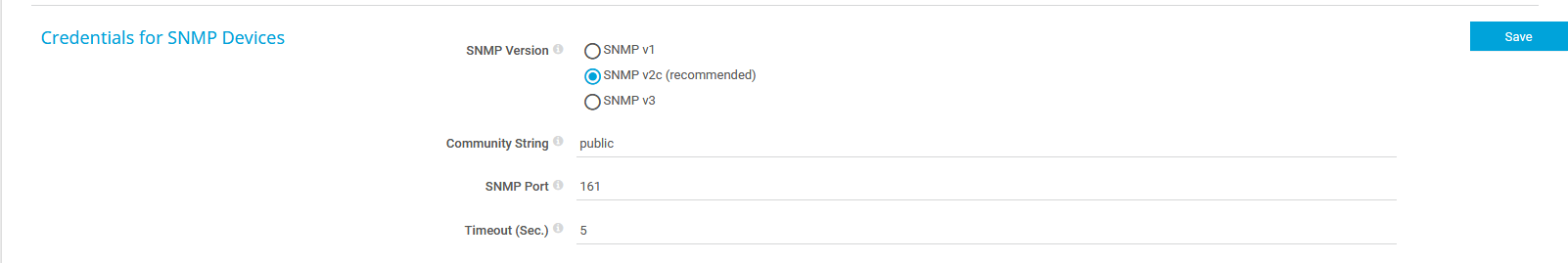
Như sức khoẻ của máy Monitor này ra sao Disk có ổn không Card mạng đang hoạt động không . Nếu toàn màu xanh thì hệ thống vẫn đang rất Oke

Ta tiến hành cấu hình SNMP trên các thiết bị muốn giám sát . Ở bài lab này mình muốn giám sát Máy chủ DC và Router Cisco

Thực hiện các cấu hình như sau



Ở giao diện này ta chọn Setting

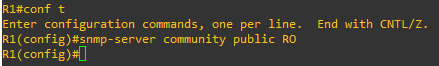
Kéo xuống dưới ta sẽ thấy dòng cấu hình SNMP ở đây có dòng Community String . Ta xem nó như là 1 mật khẩu thì cái Community String này mặc định là public ta có thể thay đổi nó để đảm bảo an toàn . Ở bài lab này mình giữ nguyên do dễ :v

Trên Router Cisco ta cần cấu hình SNMP

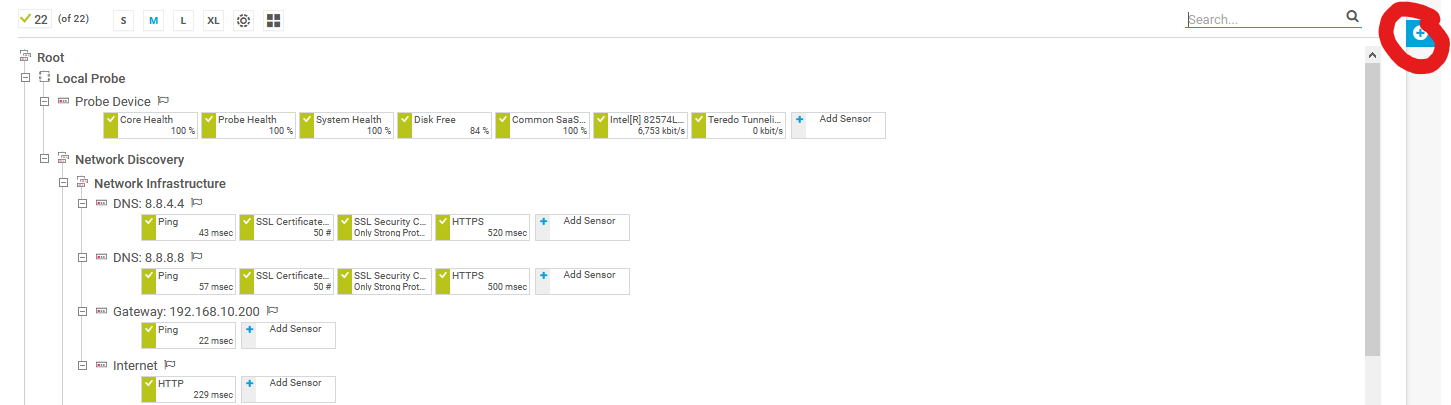
Sử dụng câu lệnh sau

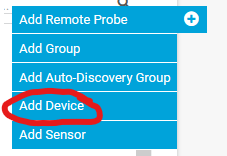
**snmp-server community public RO**

Với community là chuỗi mình đã đặt trên Máy Monitor

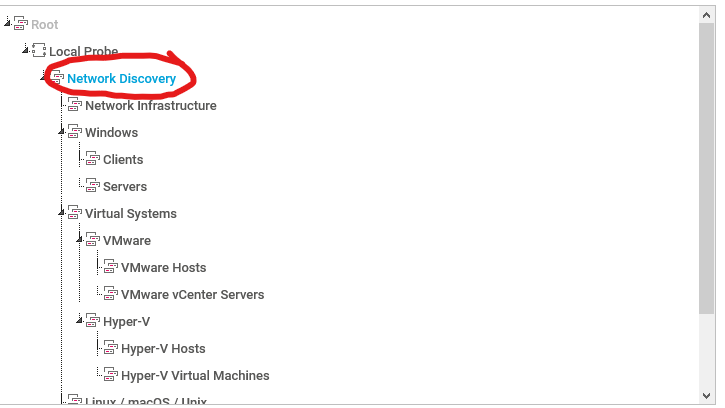


Sau đó tiền hành qua máy monitor ta thực hiện thêm thiết bị Router Cisco vào để giám sát

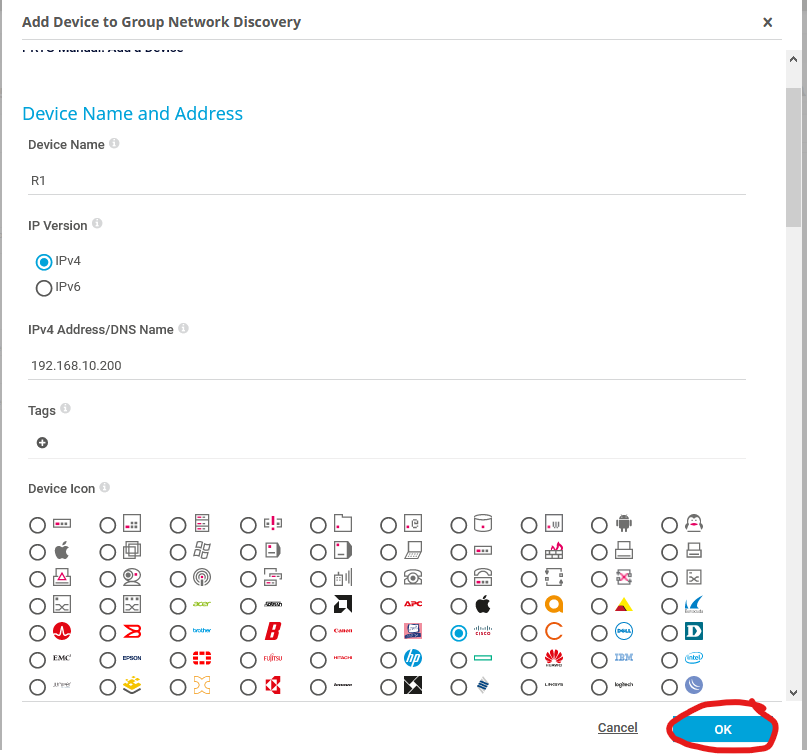




Chọn Add Device



Chọn Vị trí bạn muốn nó hiện thị ở đó sau đó bấm Ok



Đặt tên cho thiếu bị muốn giám sát chọn kiểu IP và nhập địa chỉ IP của Router mình muốn giám sát . Chọn Icon cho dễ quản lí và bấm OK



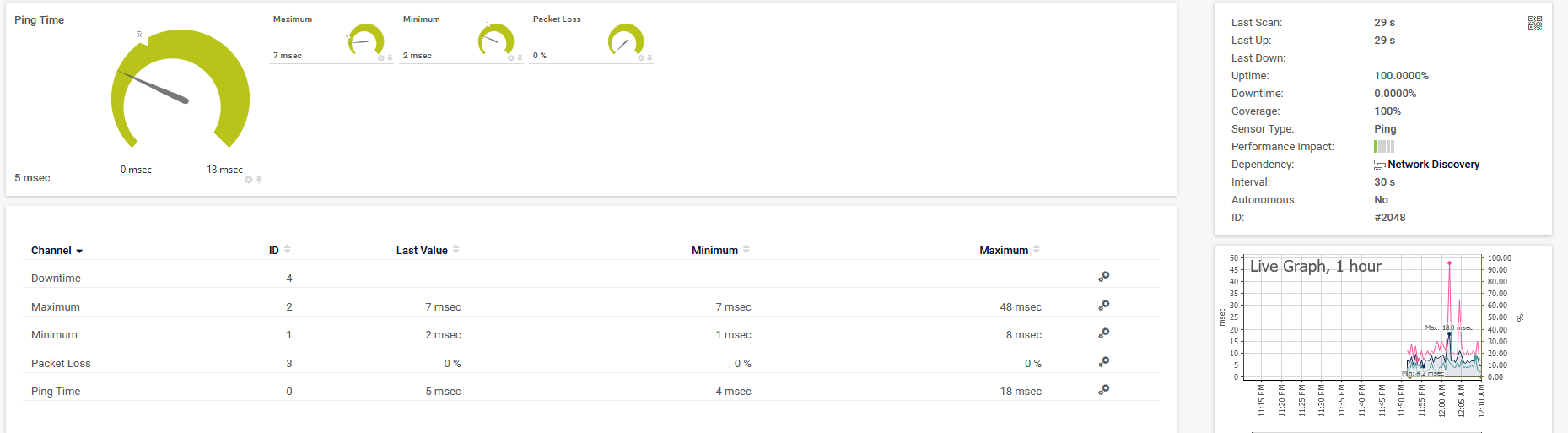
Sau khi thêm xong ta sẽ có được như thế này bấm vào Run Auto-Discovery để khám phá các thông tin từ Router Cisco mình giám sát



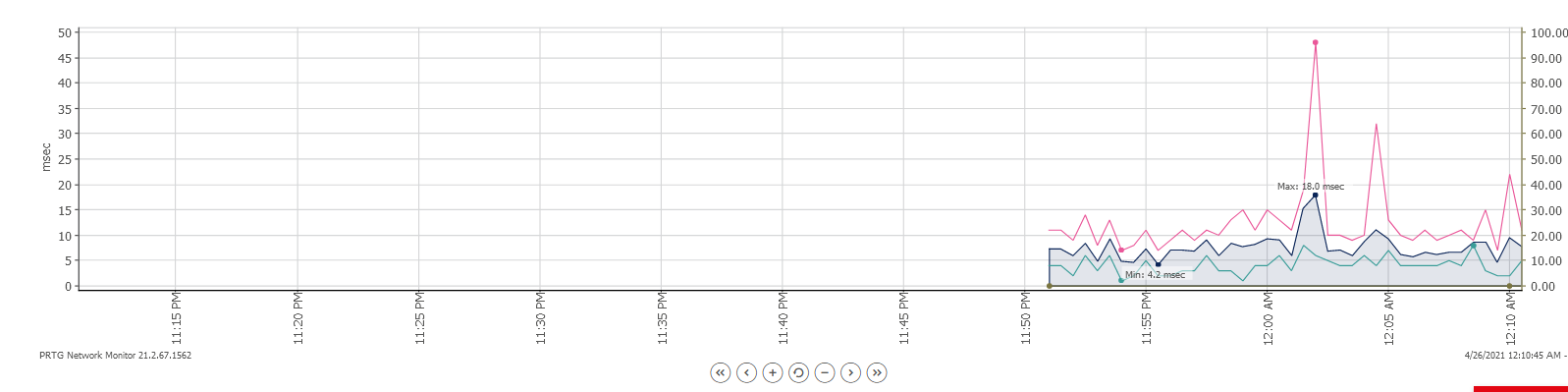
Đợi quá trình tìm kiếm thành công ta sẽ có những thông tin chi tiết từ Router Cisco



Sau khi quá trình tìm kiếm đã diễn ra thành công ta sẽ thấy được rất nhiều thông số thử bấm vào 1 Sensor xem như thế nào

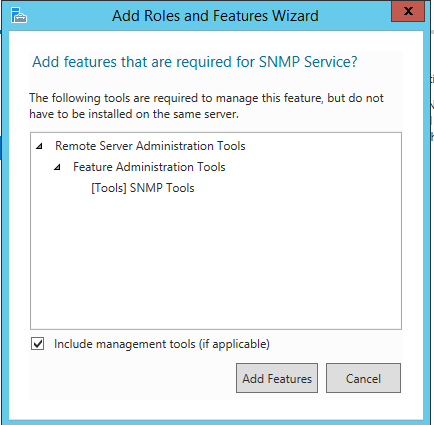


Ta sẽ thấy được rất nhiều thông số chi tiết



Có cả biểu đồ chi tiết

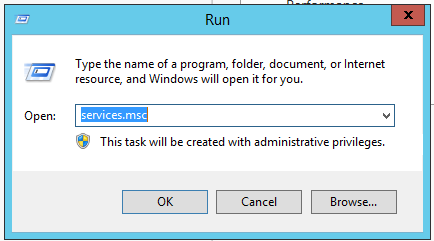
Tiến hành Add thêm máy chủ DC vào để tiến hành giám sát



Tiến hành cài đặt SNMP-Service trên máy chủ DC

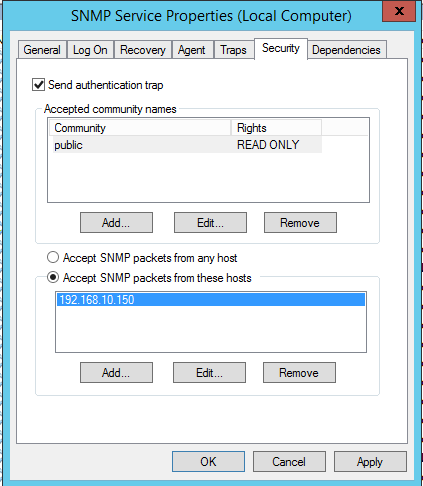


Sau khi cài đặt xong tiến hành vào run và gõ như sau

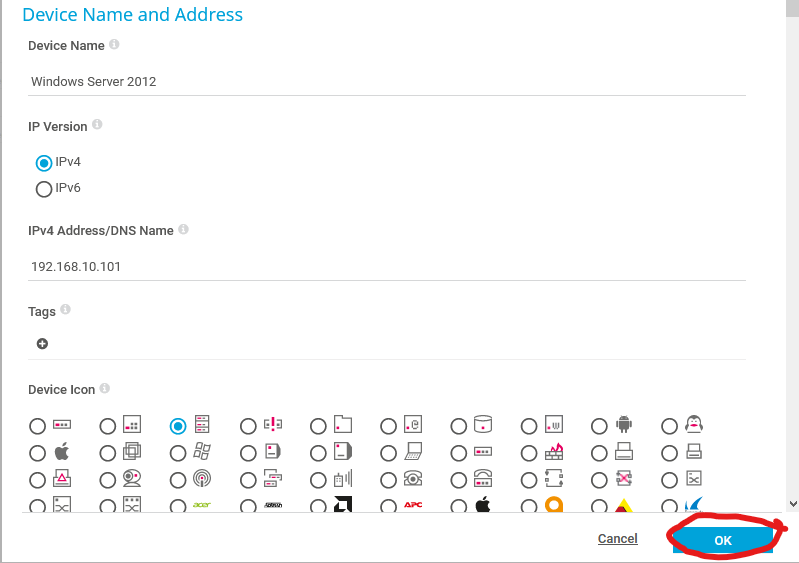




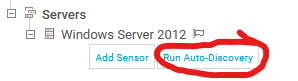
Chọn SNMP Service



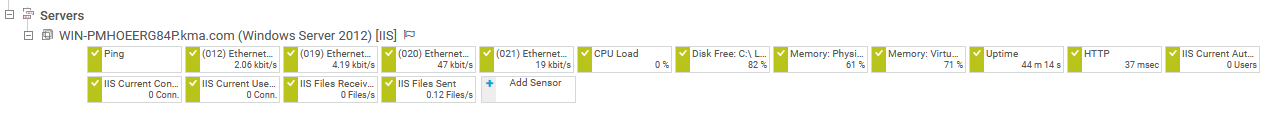
Thêm chuỗi Community và ADD địa chỉ Máy Monitor cho phép nhận thông tin của DC



Tiến hành thêm Máy chủ DC vào để giám sát



Tiến hành các bước như thêm Router Cisco



Ta đã thấy 1 số thông số đã hiện ra

**Bước 3: Cài đặt NetFlow trên router Cisco và giám sát lưu lượng đó**

Dữ liệu NetFlow data cung cấp thông tin sử dụng băng thông chi tiết có thể được phân đoạn theo nhiều cách, bao gồm theo người dùng “user”, hệ thống máy khách “client”, thời gian “time” và ứng dụng “application”. Dữ liệu đến bộ thu thập dữ liệu NetFlow Collector gần như theo thời gian thực, cho phép theo dõi chi tiết cụ thể và tổng hợp dữ liệu để nhìn ra bức tranh tổng thể như nó đang diễn ra.

***Cấu hình các lệnh sau trên router cisco***

(config)#interface FastEthernet 1/0

(config-if)#ip route-cache flow

(config-if)#exit

(config)#ip flow-export destination 192.168.10.150 9995

(config)#ip flow-export source FastEthernet 1/0

(config)#ip flow-export version 5

(config)#ip flow-cache timeout active 1

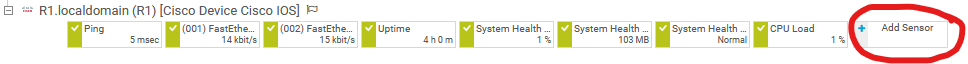
(config)#ip flow-cache timeout inactive 15

(config)#snmp-server ifindex persist

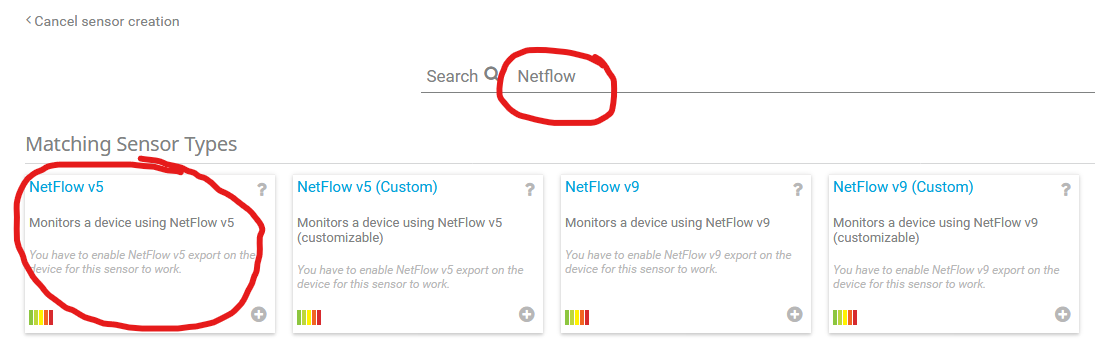
#show ip flow export

#show ip cache flow

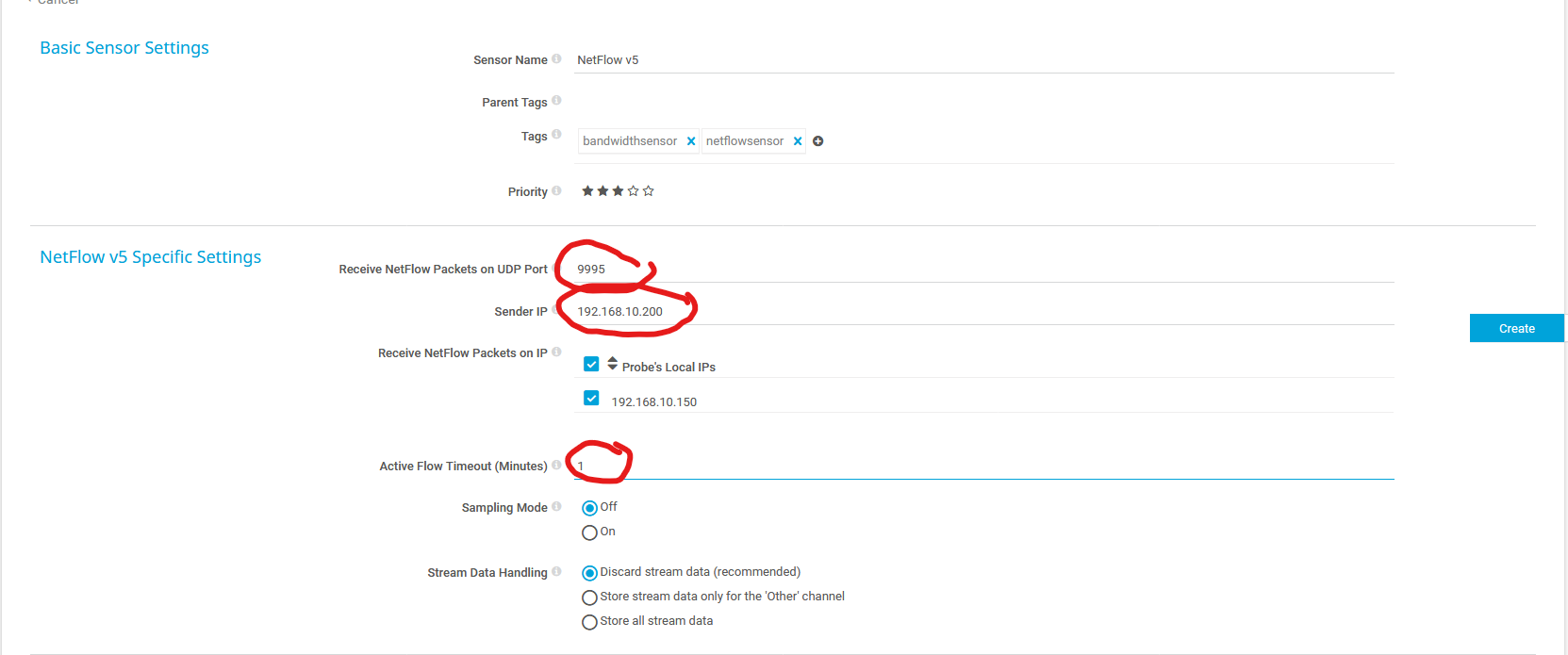
***Trên máy Monitor tiến hành thêm giám sát lưu lượng Netflow***



Tiến hành thêm 1 Sensor mới



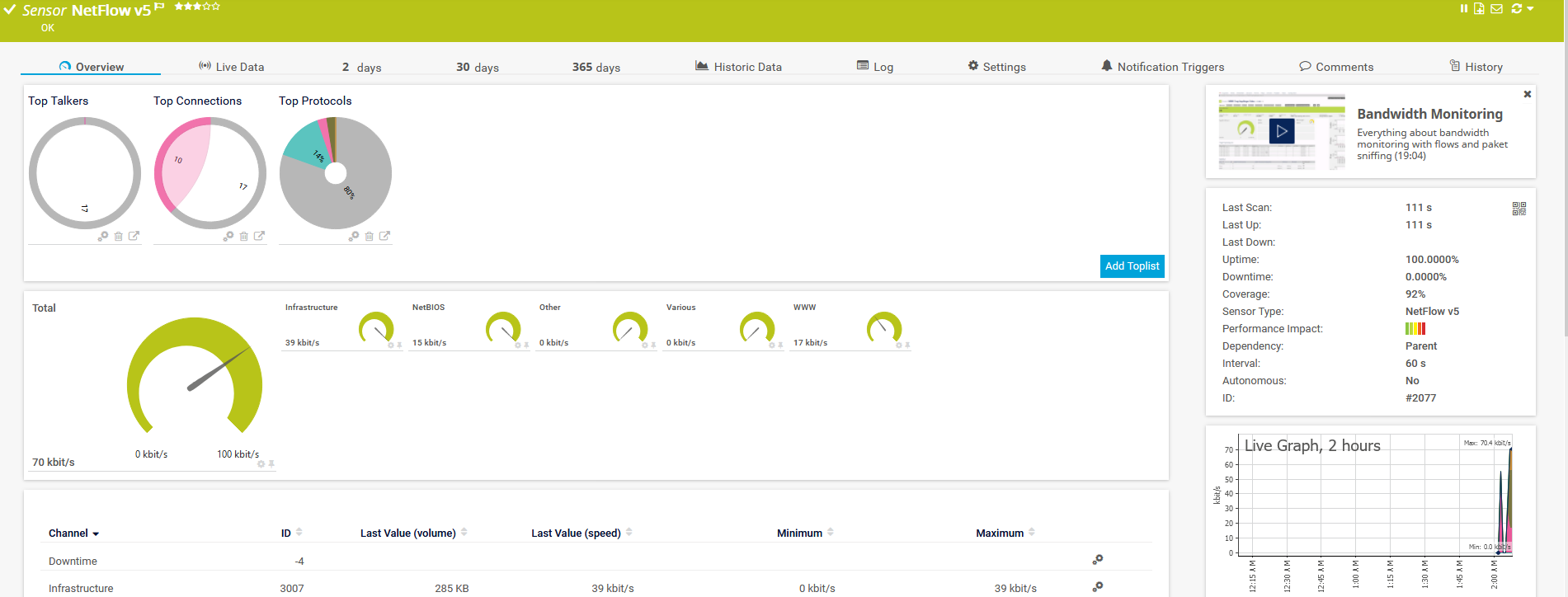
Nhập vào Netfow và chọn Netflow Version 5



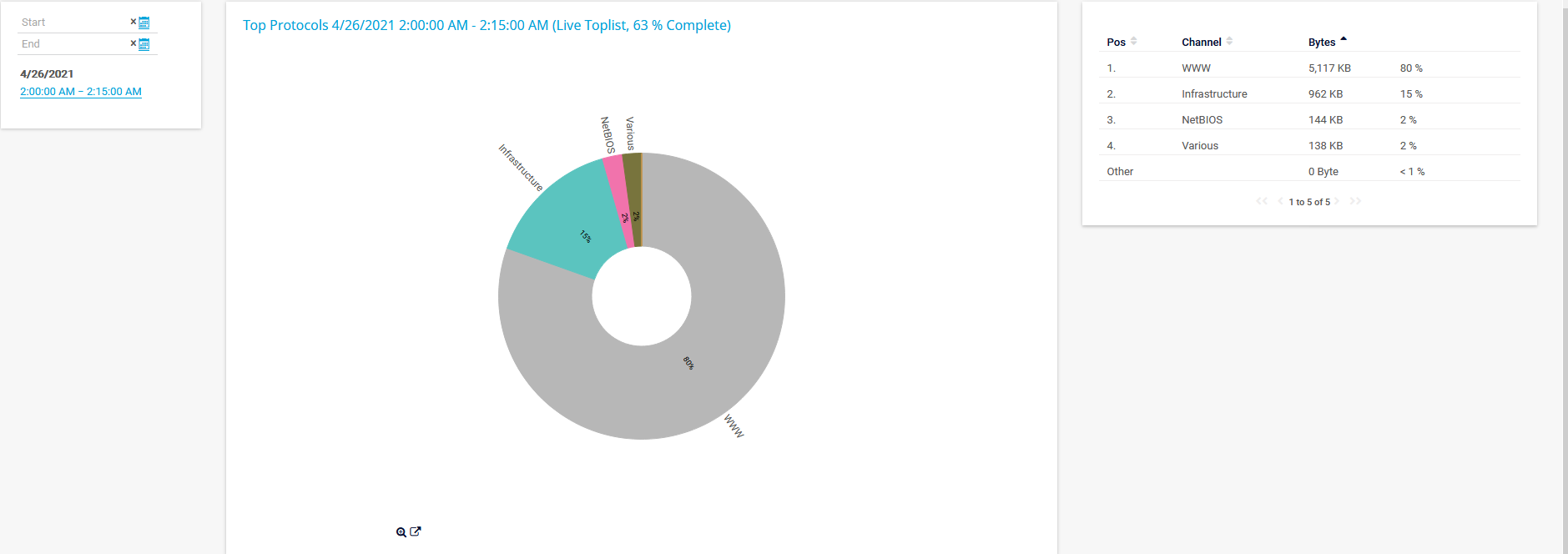
Điền Port ta đã cấu hình trên Router Cisco và nhập địa chỉ của cổng mà cổng đó dùng để truyền lưu lượng netflow về monitor nhập thời gian chờ hoạt động của netflow là 1 phút sau đó bấm Create bên phải



Ta thấy Netflow v5 đã được thêm vào



Ta thấy được rất nhiều thông số biểu đồ 1 cách chi tiết thử bấm vào Top Protocols để xem top các giao thức

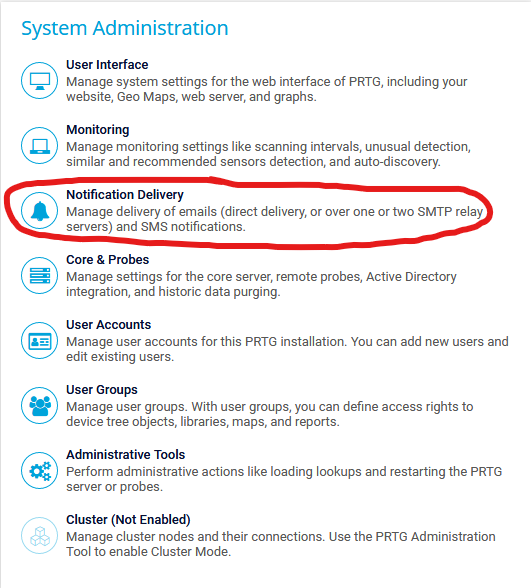


Ta có thể thấy thời gian của biểu đồ là từ 2 giờ đến 2 giờ 15 đây là thời gian thu thập của mỗi biểu đồ mỗi 15p sẽ cập nhập 1 biểu đồ mới . Ở giữa là 1 biểu đồ trực quan về lưu lượng . Bên trái là giao thức như www, v.vv.

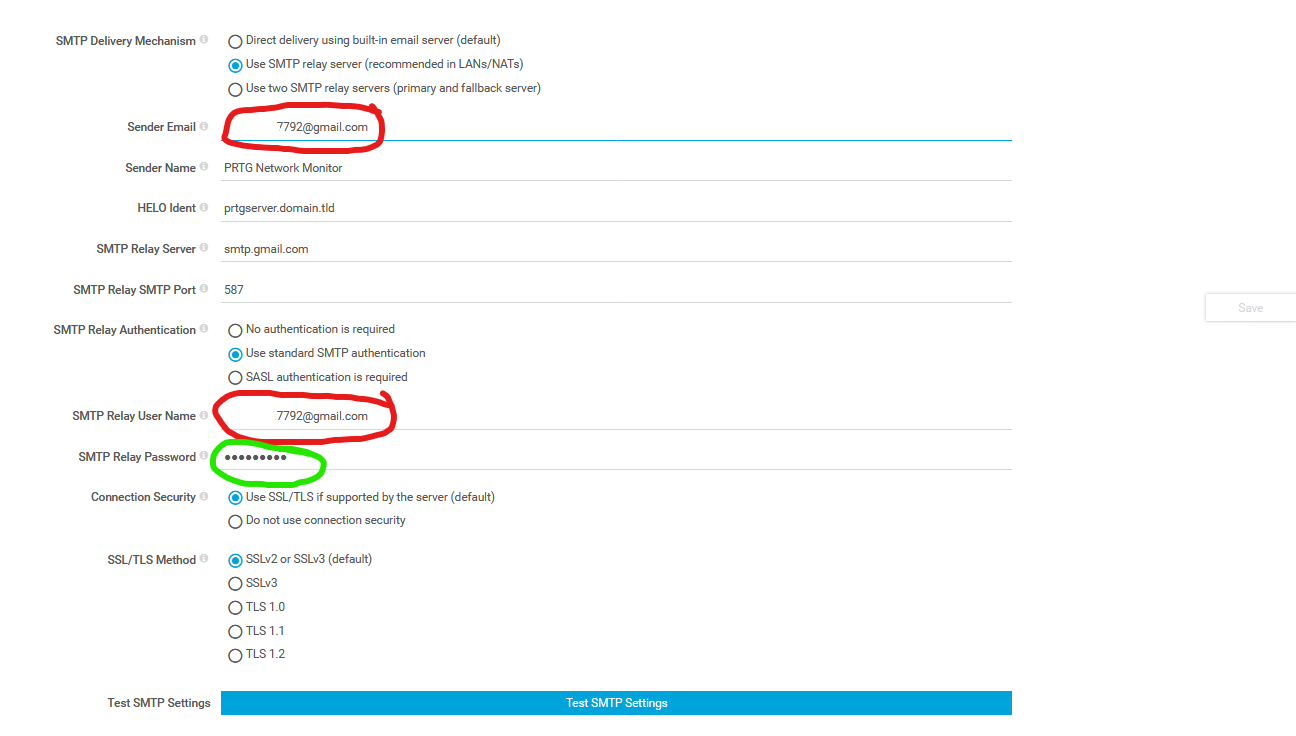
**Bước 4 : Tiến hành cấu hình thông báo bằng email nếu có sự cố bất thường diễn ra**

****

Chọn Setup

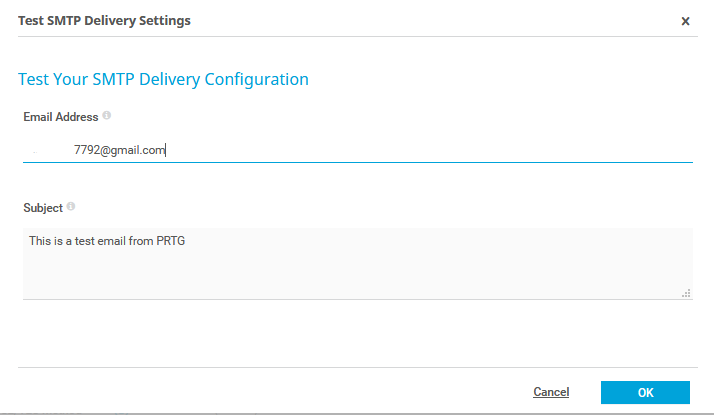


Chọn Notification Delivery



Ta nhập các thông số như hình những ô màu đỏ ta nhập gmail của người gửi và ô màu xanh ta nhập password gmail của người gửi

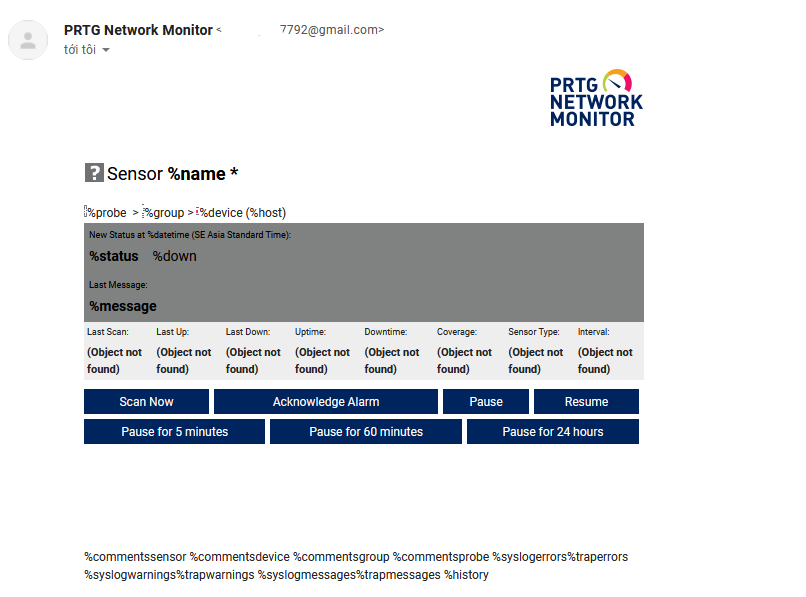
Ta thử tiến hành bấm Test SMTP Setting xem đã oke chưa



Ở đây ta nhập mail của người được nhận và bấm Oke

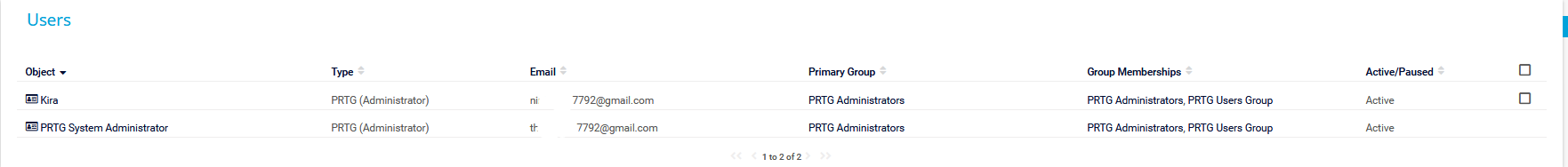


Ta sẽ nhận được 1 Gmail như thế này

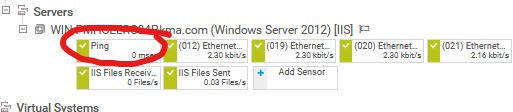


Ta sẽ được 1 thư test như thế này

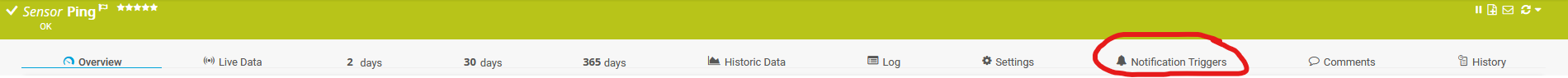
Tiếp theo ta tiến hành cài đặt cảnh báo nếu 1 Sensor nào đó bị xảy ra vấn đề sẽ gửi cảnh báo về mail



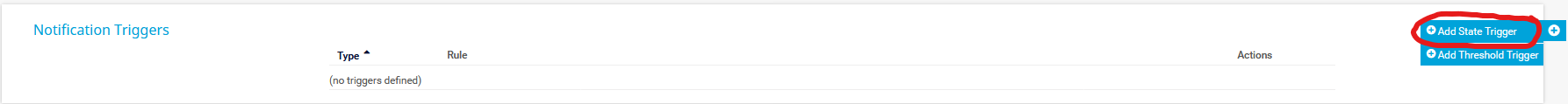
Ta sẽ tạo thêm 1 User nữa ở bài lab này với 1 địa chỉ gmail khác để test xem liệu user này có nhận được gmail cảnh báo hay không. Ở đây mình đưa user kira và User Admin về cùng 1 Group cho dễ quản lí



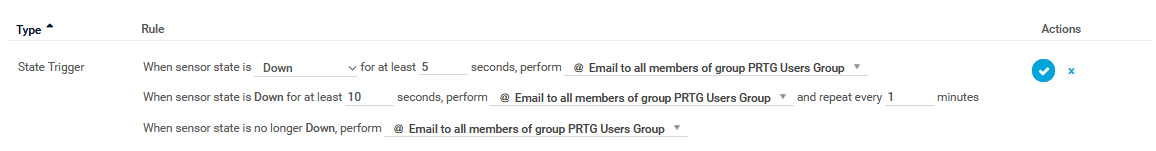
Ở đây mình sẽ chọn Sensor Ping mình sẽ đặt 1 Trigger Notifications lên Sensor này để nhận thông báo



Chọn như ảnh trên

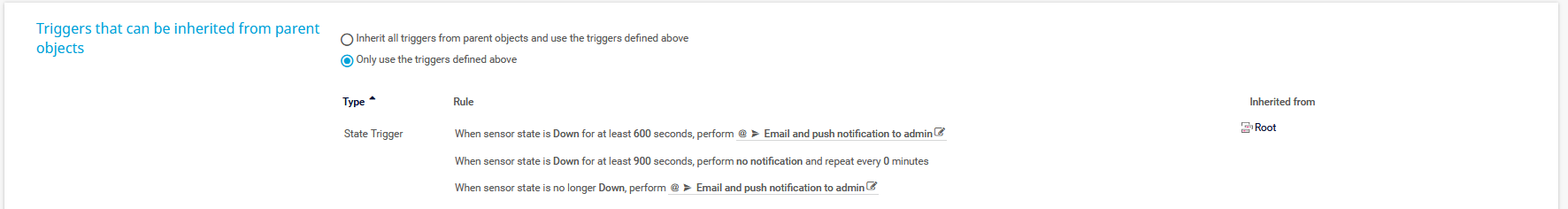


Chọn như ảnh trên

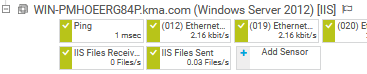


Điền các thông số như trên hình nếu cổng down quá 5 giây sẽ gửi thông báo đến mail của tất cả các thành viên trong group. Dòng thứ 2 nếu mà down hơn 10s thì sẽ gửi mail đến tất cả các thành viên trong group với định kì là 1 phút gửi 1 lần . Và nếu trạng thái không còn Down nữa cũng gửi 1 mail cảnh báo đến toàn bộ thành viên trong group

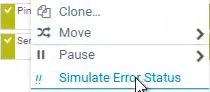
Sau đó tiến hành lưu lại bằng đấu tính bên phải



Dòng ở dưới ta chọn như ảnh

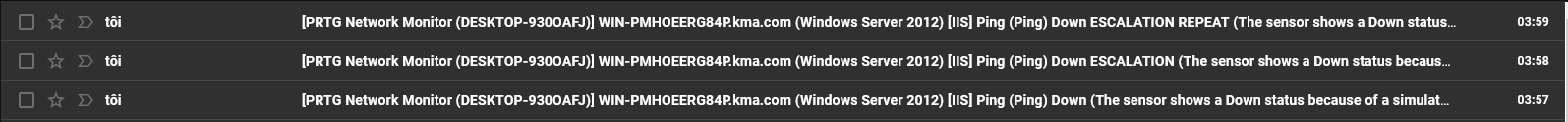


Chuột phải vào Ping

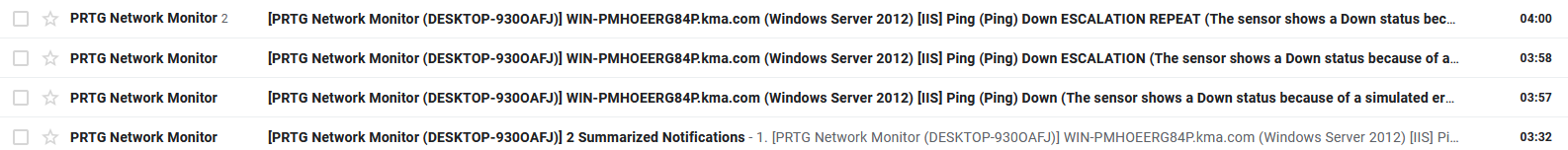


Chọn như hình để tạo ra 1 hình huống lỗi

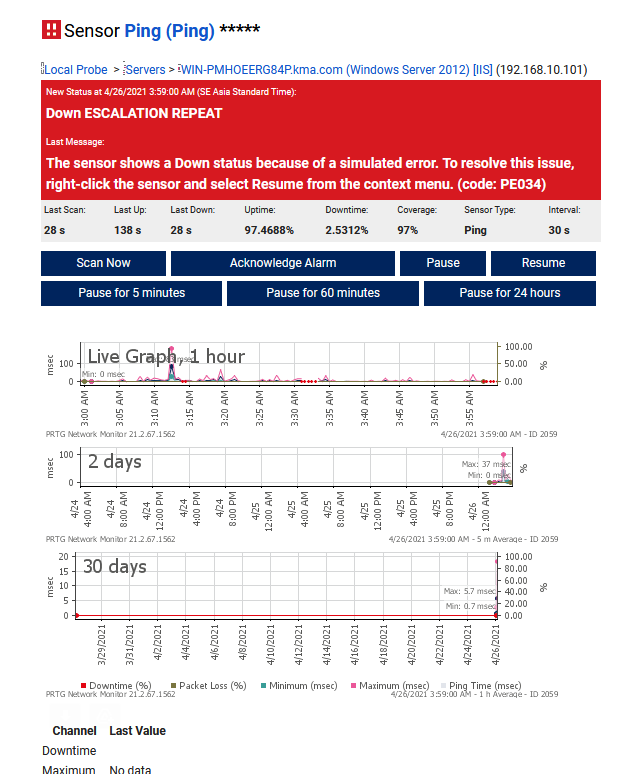
Lúc này ta tiến hành qua 2 gmail của 2 user để kiểm tra thử



Đây là gmail của user admin và ta đã thấy thông báo lỗi đã được hiện ra và mỗi 1 phút trôi qua nếu trạng thái down vẫn tiếp tục trong 10 giây ta sẽ nhận liên tiếp các thông báo

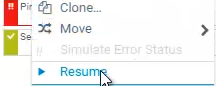


Bên phía user Kira còn lại cũng thế

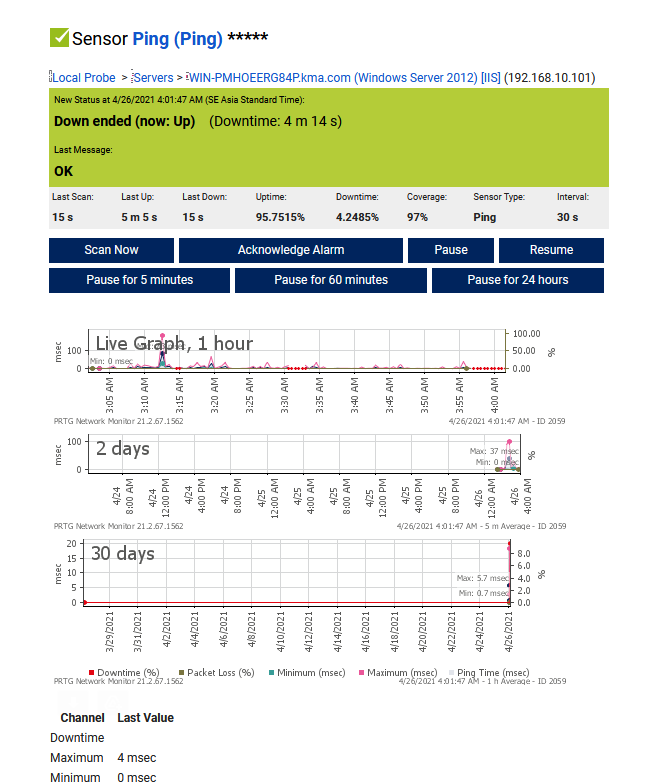


Đây trạng thái của thông báo lỗi được hiển thị về

Ta tiến hành mở lại trạng thái cho cổng ping xem có nhận được thông báo không

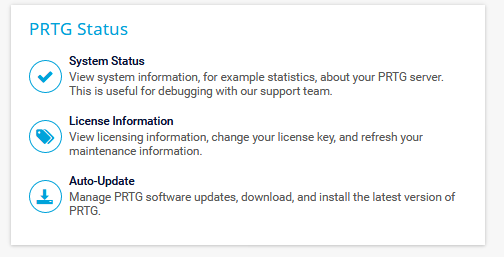


Chuột phải vào Ping chọn Resume

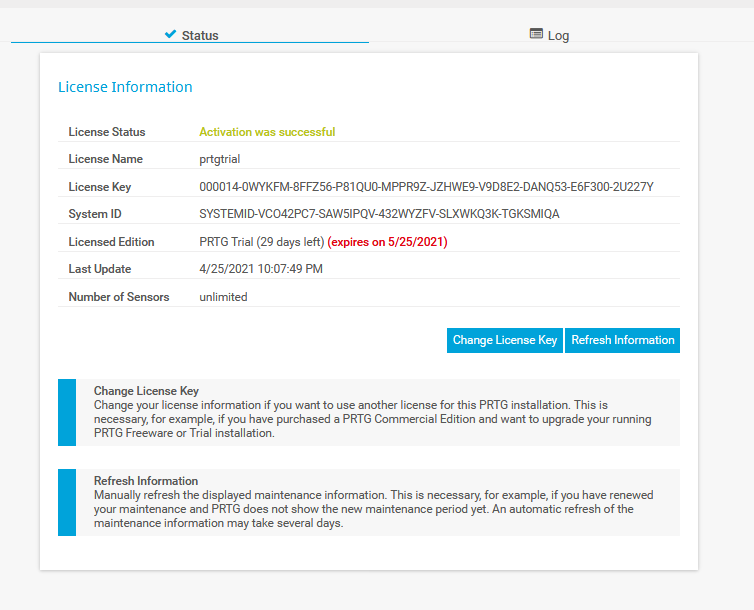


Quay trở lại mail ta thấy rằng thông báo up đã hiển thị

**Bước 5: Cách nhập License Key**



Chọn License Information



Bạn chỉ cần Change License Key và nhập vào Key bạn đã mua là sẽ active thành công