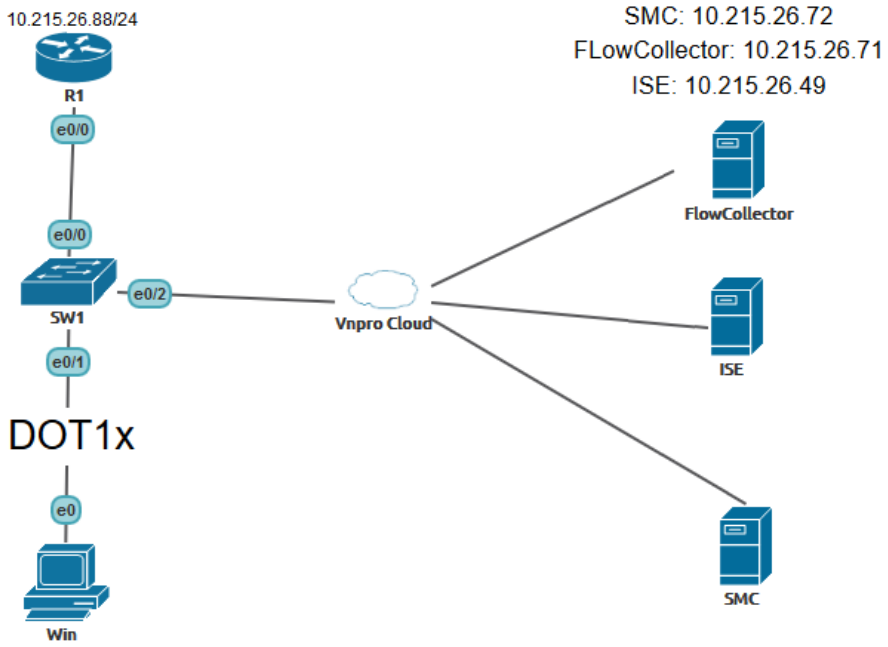
Lab – Steathwatch kết hợp Cisco ISE



Trong bài lab này, chúng ta sẽ tiến hành thực nghiệm quá trình trao đổi thông tin về người dùng giữa Cisco ISE và Stealthwatch thông qua cấu hình **Wired Dot1x** và **Flexible NetFlow.**

BƯỚC 1: Thực hiện cấu hình Dot1x trên switch để thực hiện xác thực giữa switch-client (máy tính Windows) và xác thực Radius giữa switch-Cisco ISE.
Trên các cổng của switch cấu hình đưa về mode access và đặt ip cho interface vlan 1

```
SW1(config)#int range e0/0-2
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#exit
SW1(config)#int vlan 1
SW1(config-if)#ip add 10.215.26.85 255.255.255.0
SW1(config-if)#no shut
```

```
SW1#show ip int br
Interface              IP-Address      OK? Method Status        Protocol
Ethernet0/0            unassigned      YES unset  up            up
Ethernet0/1            unassigned      YES unset  up            up
Ethernet0/2            unassigned      YES unset  up            up
Ethernet0/3            unassigned      YES unset  up            up
Vlan1                  10.215.26.85    YES manual up            up

SW1#show vlan br
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
```

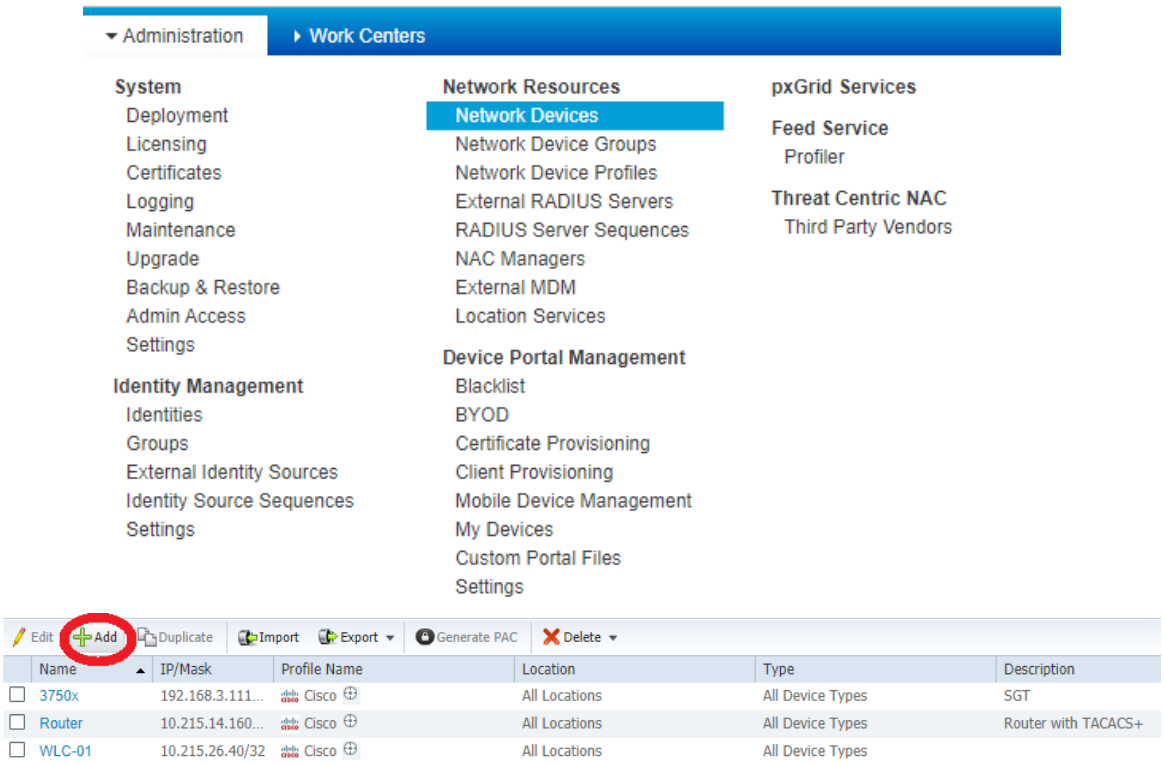
```
1    default                          active    Et0/0, Et0/1, Et0/2,
Et0/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

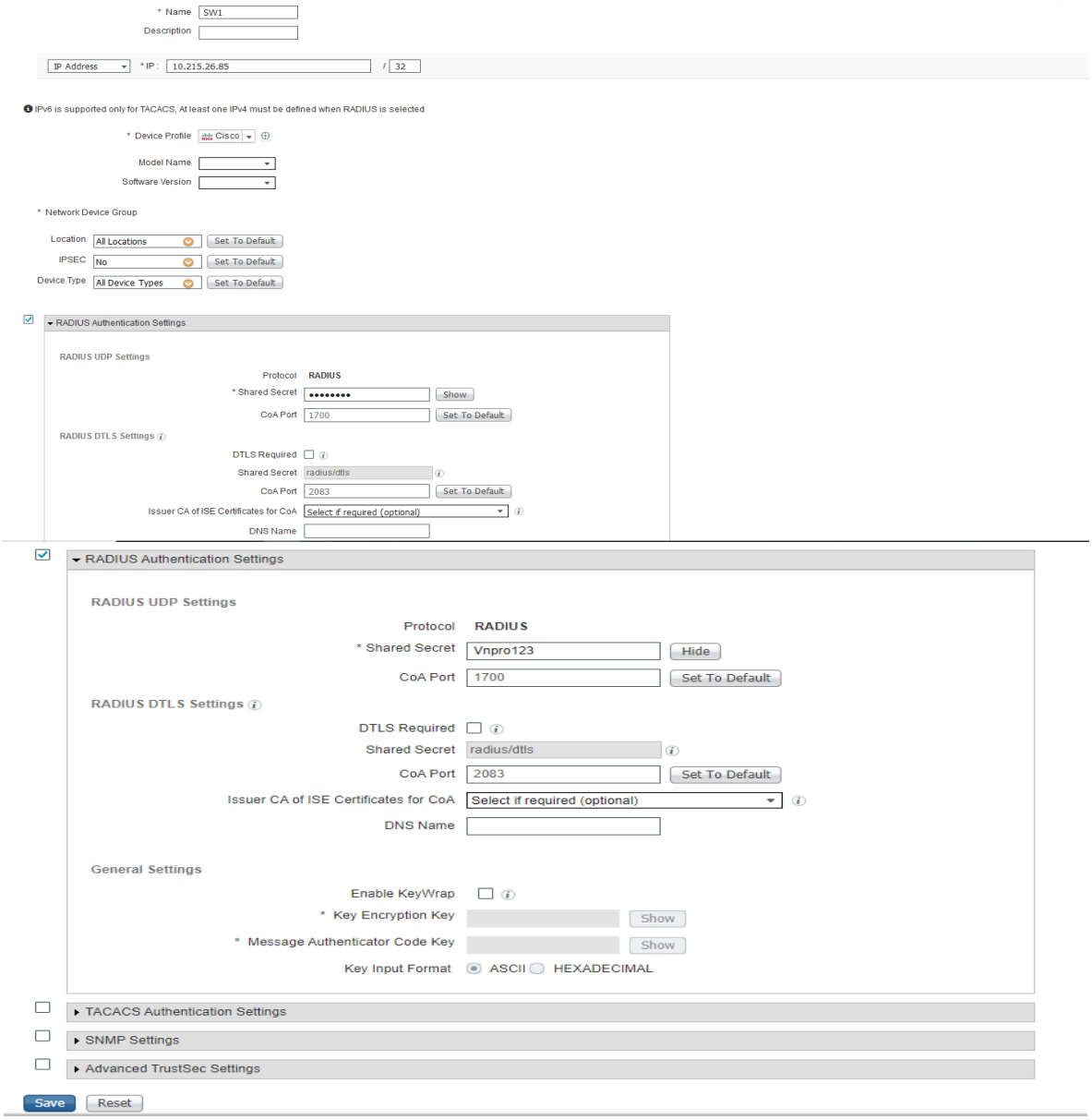
```
SW1(config)#aaa new-model
SW1(config)#aaa authentication dot1x default group radius
SW1(config)#dot1x system-auth-control
SW1(config)#int e0/1
SW1(config-if)#dot1x port-control auto
SW1(config-if)#dot1x pae authenticator
SW1(config-if)#authentication host-mode multi-auth
SW1(config)#radius-server host 10.215.26.49
SW1(config)#radius-server key Vnpro123
```

Cấu hình địa chỉ ip cho cổng e0/0 của R1 và trỏ default route về đám mây của VnPro.

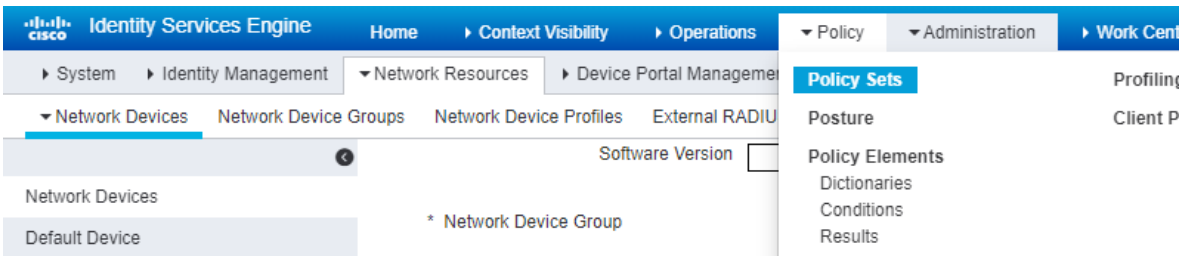
```
R1(config)#int e0/0
R1(config-if)#ip address 10.215.26.88 255.255.255.0
R1(config)#ip route 0.0.0.0 0.0.0.0 10.215.26.1
```

Tiếp theo, chúng ta tiếp tục thực hiện tạo policy và chỉ định Switch cho cisco ISE chứng thực. Chúng ta tiến hình thực hiện cấu hình Cisco ISE theo dãy hình bên dưới.

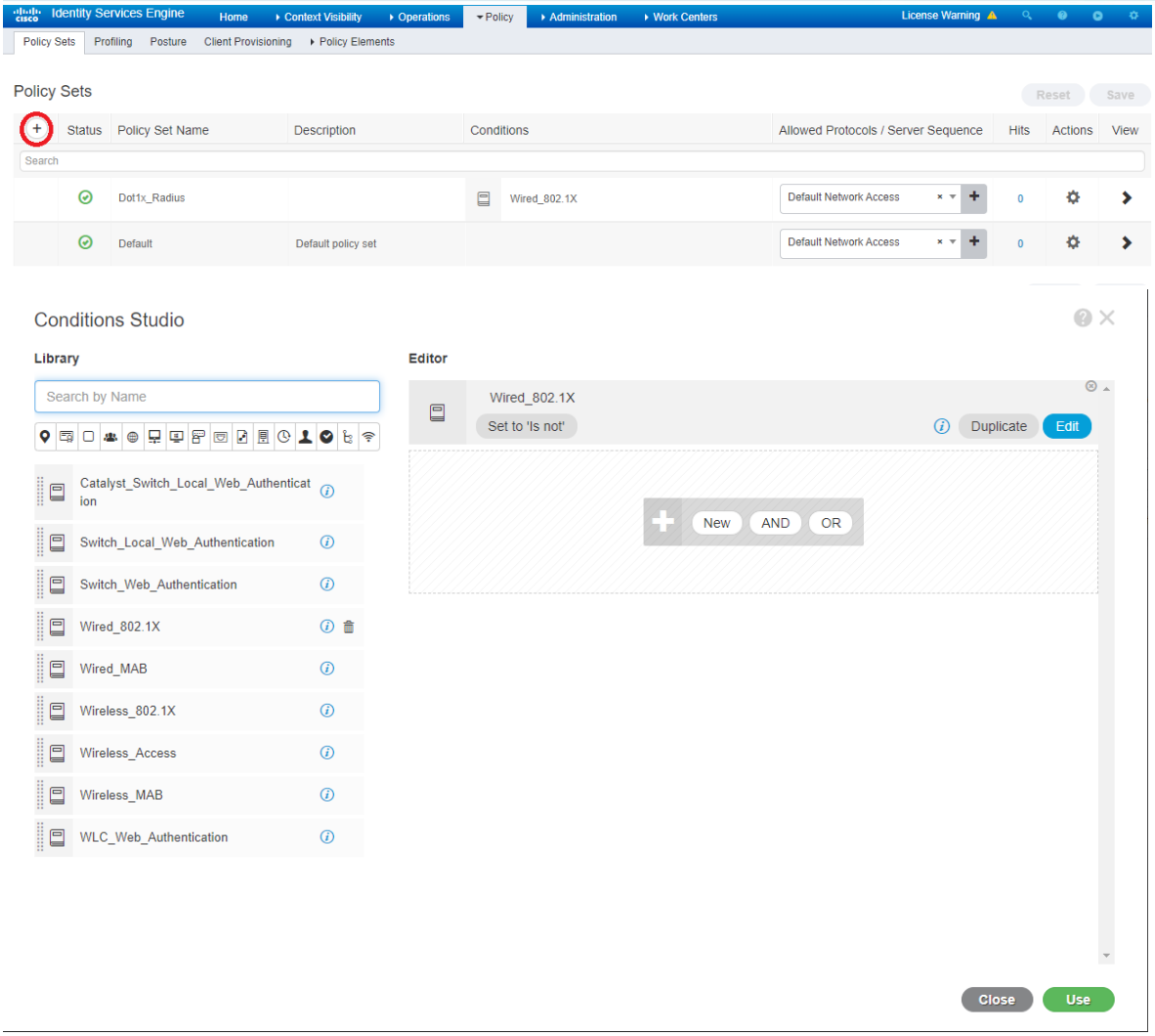




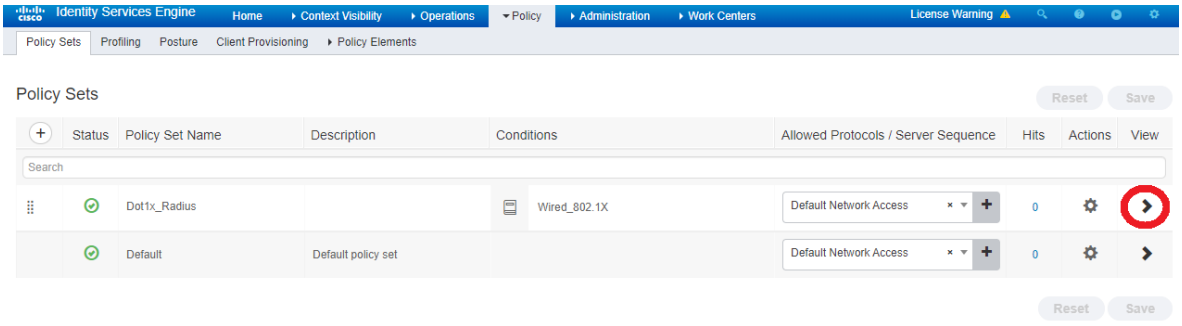
Tiếp tục chúng ta set policy dot1x và radius trên cisco ISE.Vào tab **Policy → Policy Sets**.



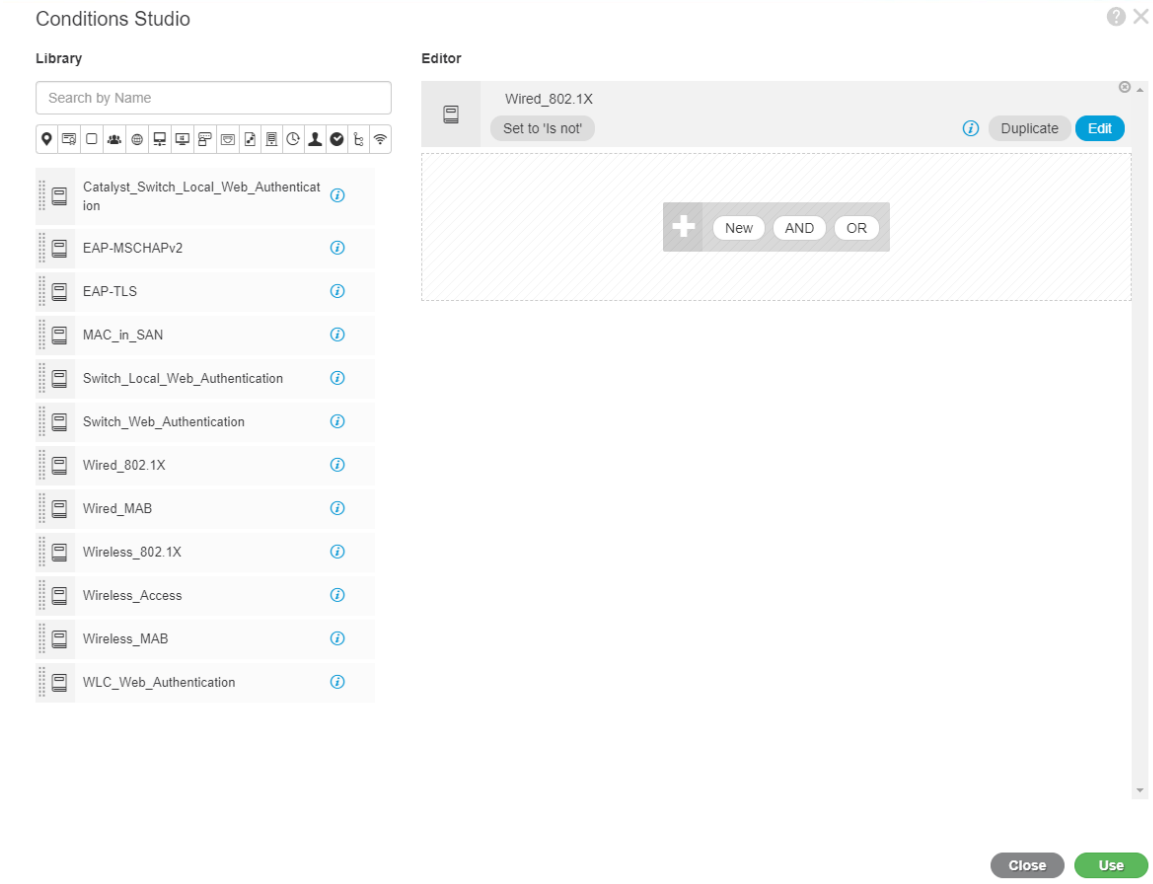
Nếu chưa tạo Policy cho wired dot1x thì click vào vòng khoanh đỏ → điền **policy name** → Trong mục **condition** bấm vào dấu + hoặc **dấu cây bút** → kéo thả như ảnh dưới đây.



Chọn Use, sau đó bấm vào mũi tên ở cuối hàng.

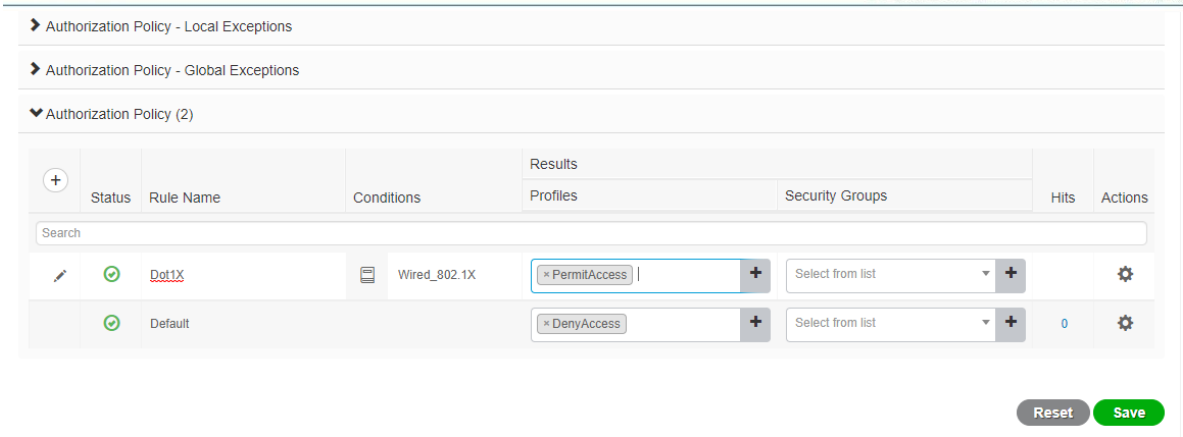


Trong mục **Authentication Policy** → Tick chọn dấu **"+"** để add policy → Trong mục **Condition** kéo thả mục **wired_802.1X** từ bên trái qua bên phải như ảnh dưới đây → Chọn **Use**.

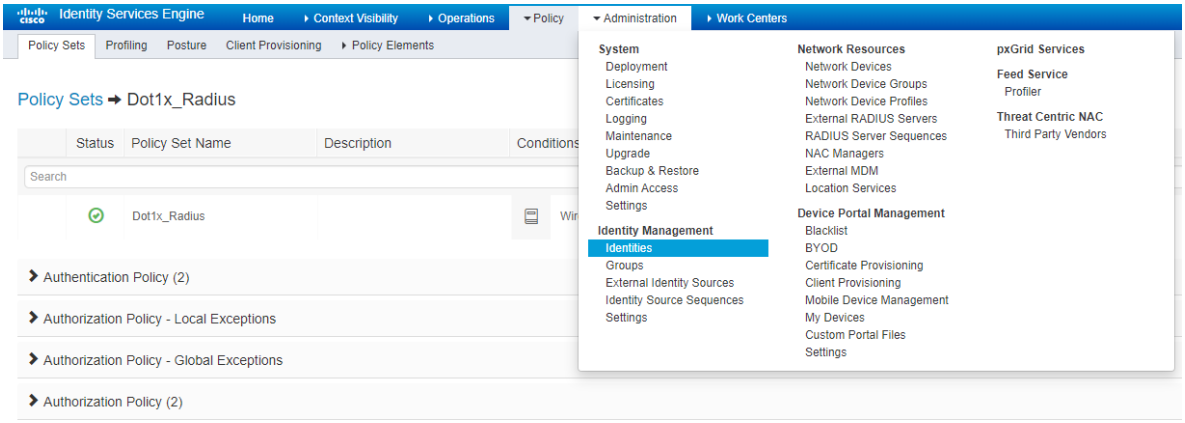


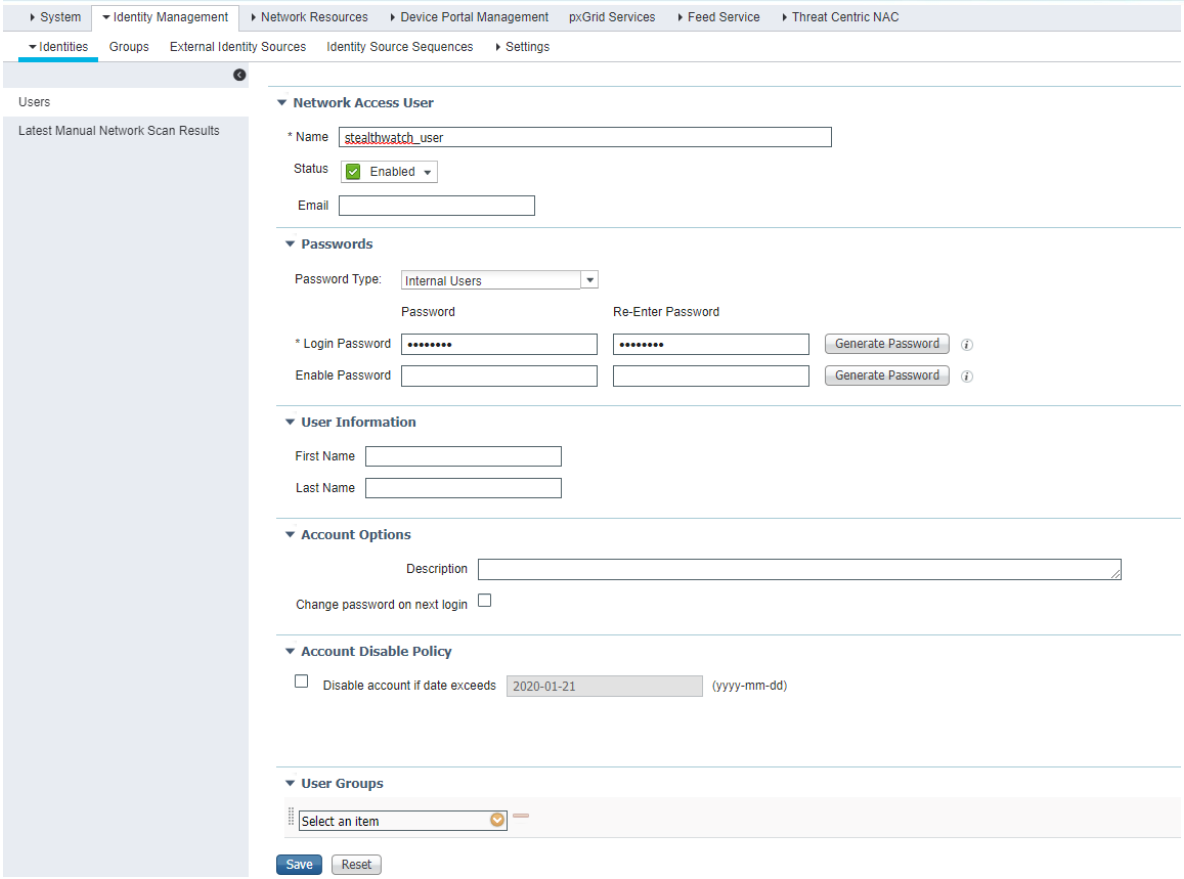
Chúng ta có thể điều chỉnh các option để hiệu chỉnh cho việc xác thực, chẳng hạn nếu xác thực fail thì sẽ REJECT.

Chúng ta tiếp tục set policy Authorization.Thực hiện như ảnh dưới đây.

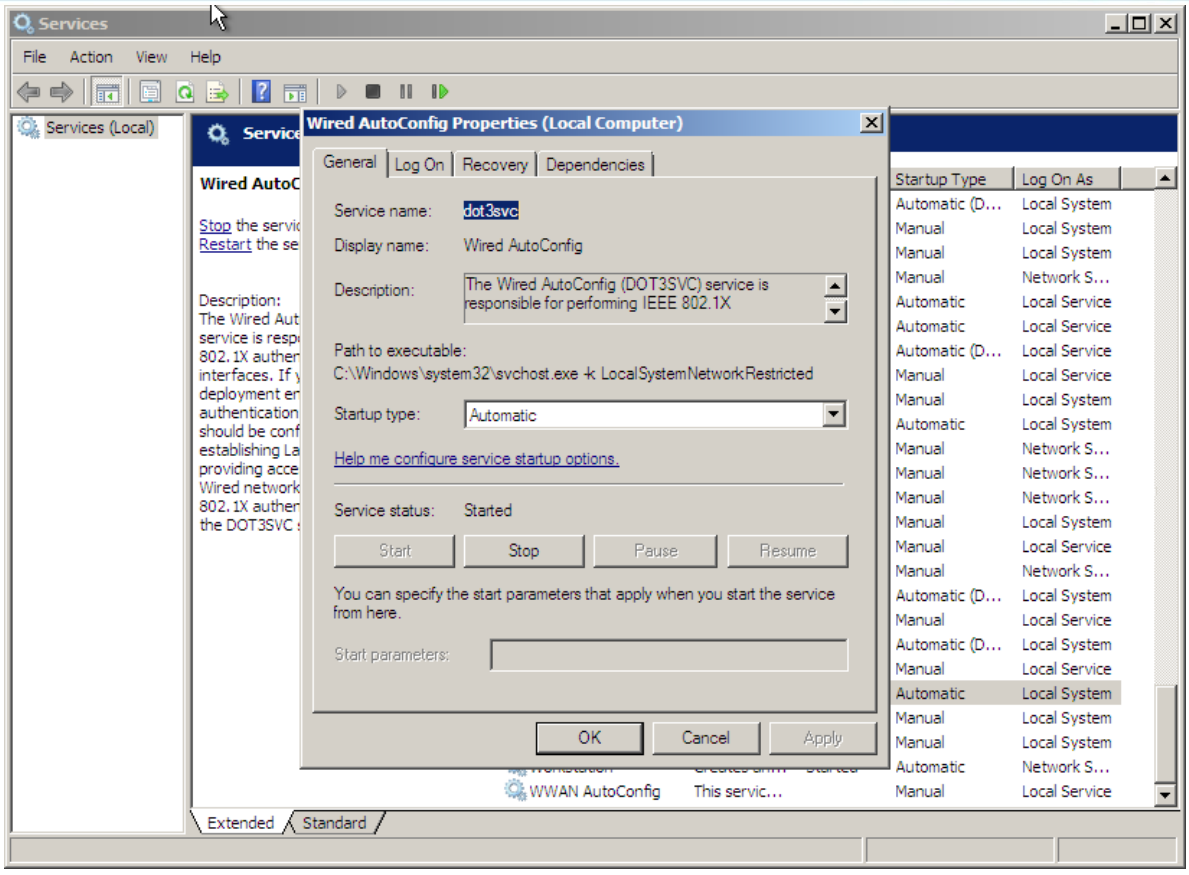


Như vậy chúng ta đã set xong policy. Bây giờ chúng ta tiến hành tạo user trên cisco ISE → **Chọn tab Administration → Identity Management → Identities**. Chúng ta tiến hành tạo user như 2 ảnh dưới đây.

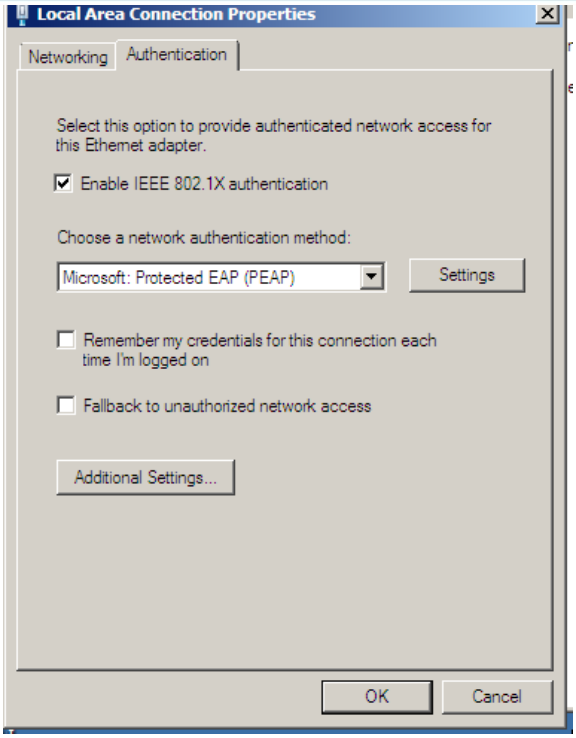




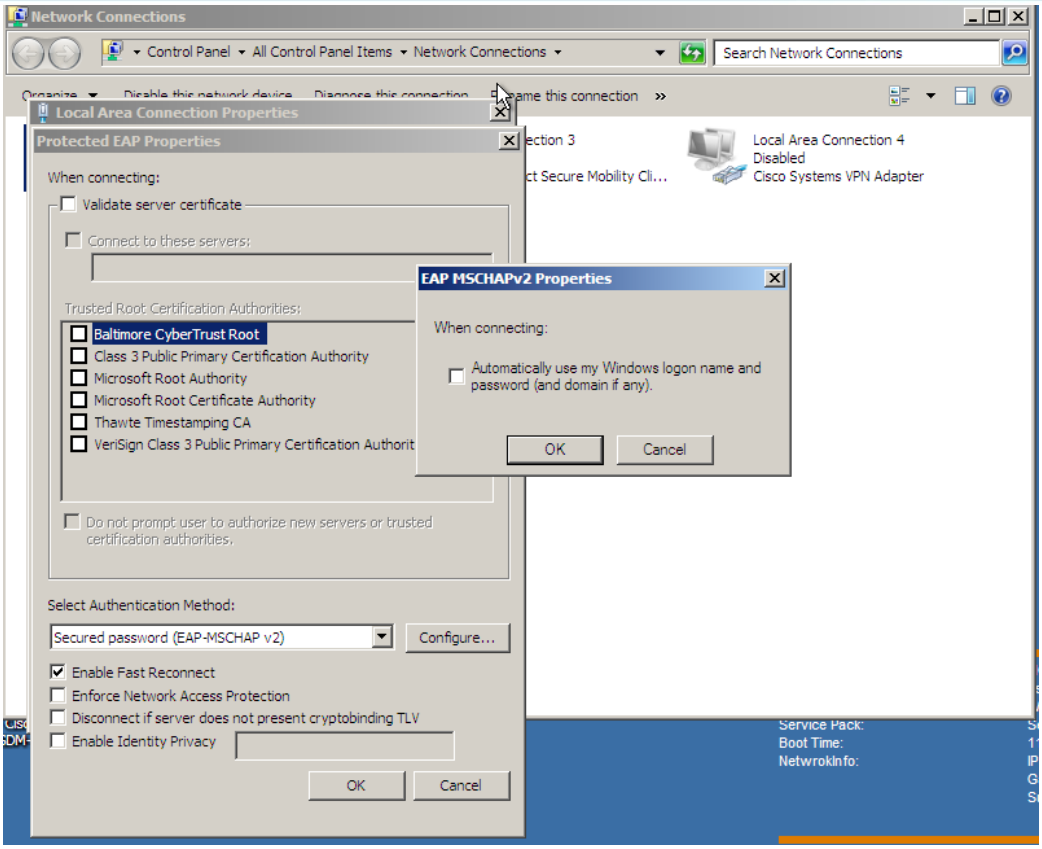
Như vậy chúng ta đã tạo được user và set policy cho wired dot1x trên Cisco ISE.
Trên PC chúng ta tiến hành điều chỉnh card mạng cho việc xác thực dot1x. Đầu tiên, ta bấm tổ hợp phím Windows+R → services.msc → Tìm services Wired Autoconfig → Chuột phải trọn **Properties** → Trong tab **General** chọn các chỉ mục như ảnh dưới đây.



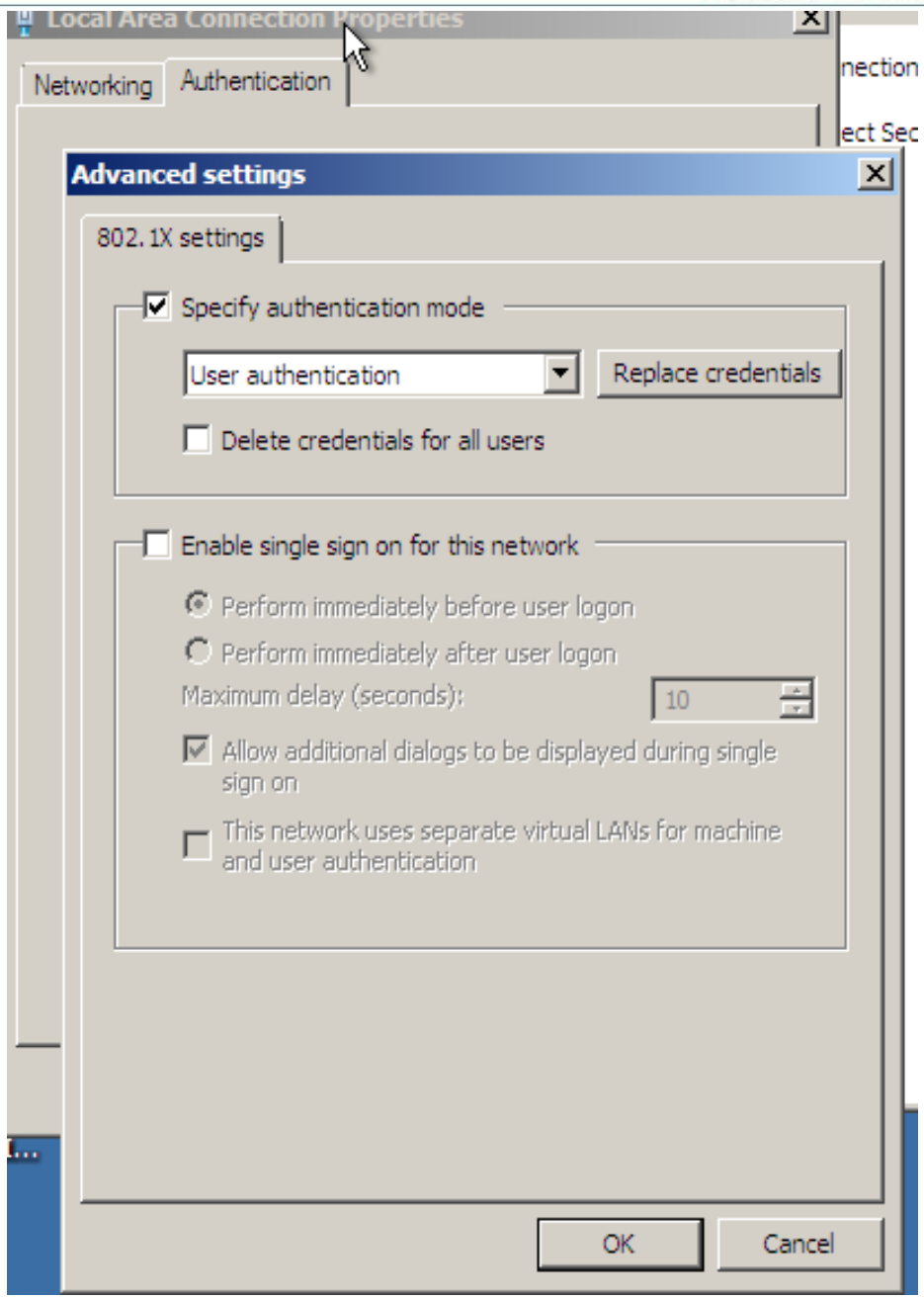
Chuyển sang điều chỉnh card mạng, Chuột phải vào card mạng đang chạy → Prperties → Trong tab Authentication tick chọn như ảnh dưới đây.

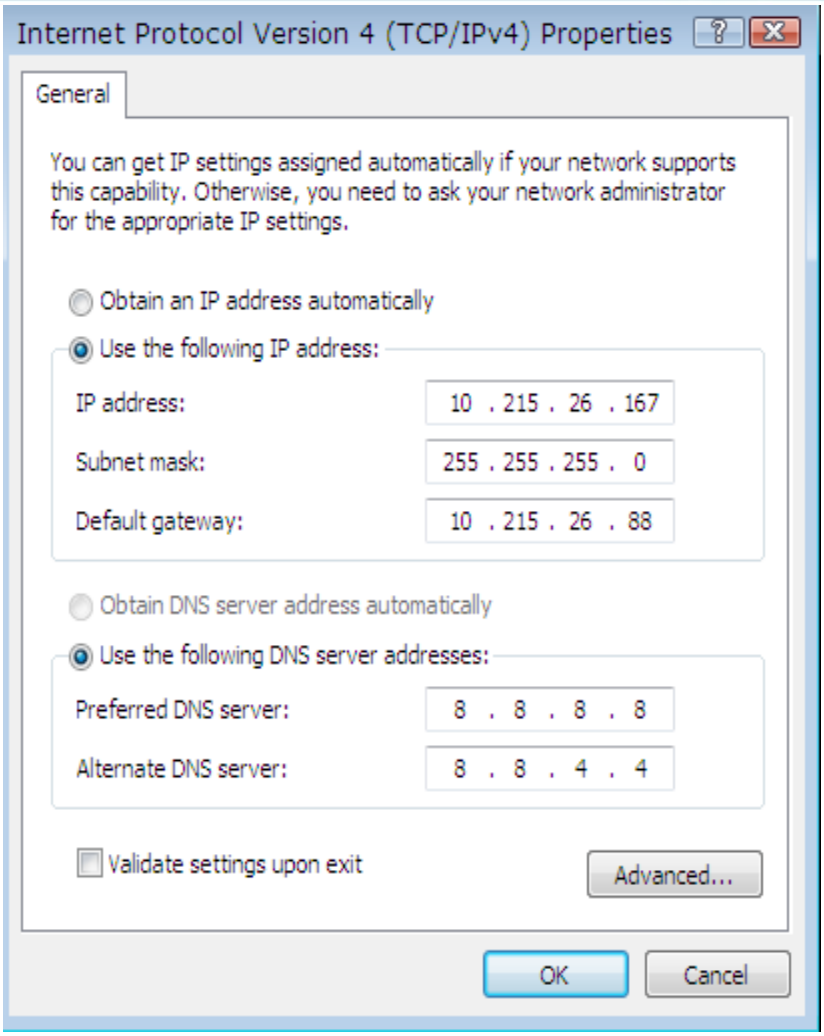


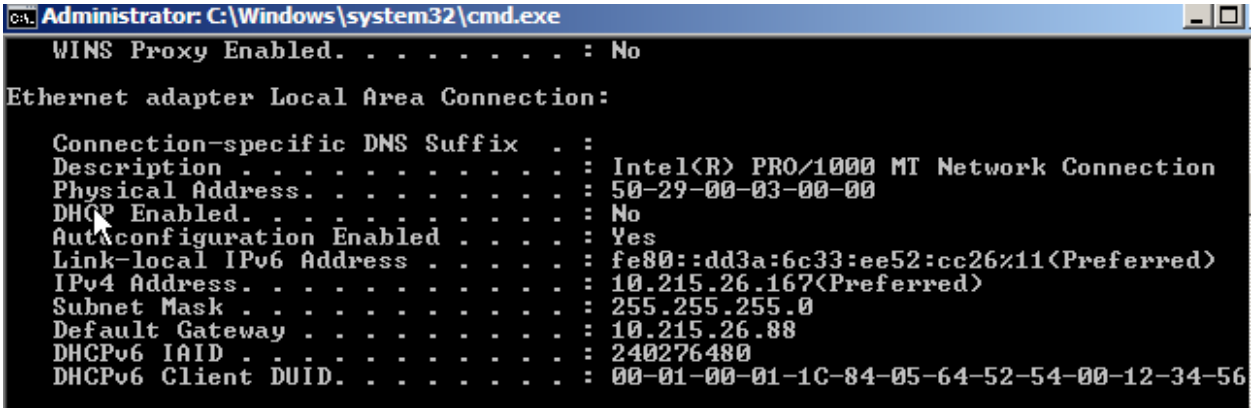
Trong tab Choose a network authentication method Chọn Settings → Bỏ tick Validate server certificate (trong môi trường lab, chúng ta không cần windows xác thực chứng chỉ của Cisco ISE) → Trong mục Select Authentication Method Chọn Configure… → Bỏ tick Automatically use my Windows logon name and password (do chúng ta không dùng domain nên không cần dùng đến mục này)→ Chọn Ok → Tiếp tục Ok để quay lại tab Authentication.



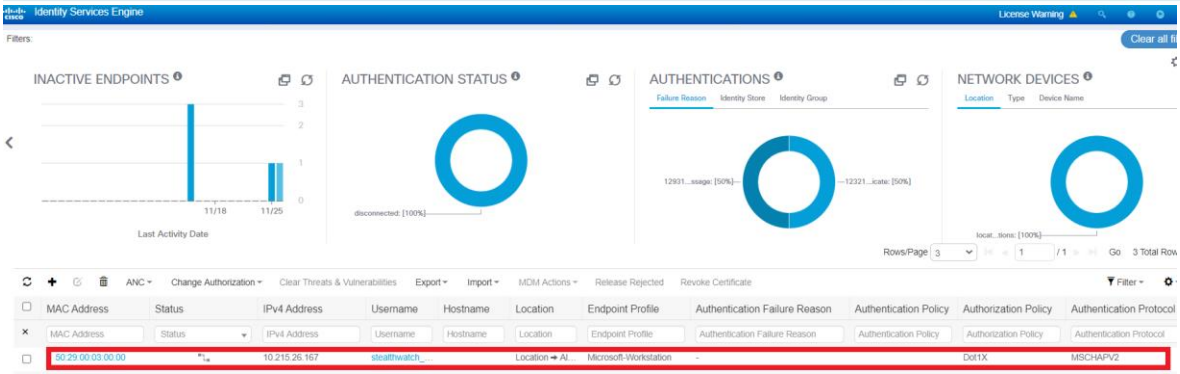
Ta tiếp tục chọn Additional Settings… → Tick chọn Specify authentication mode → Chọn user authentication → Chọn Save/Replace credentials để nhập username/password đã tạo trên cisco ISE.


Local Area Connection Properties
Networking
Authentication
nection
ect Sec
Advanced settings
802.1X settings
Specify authentication mode
User authentication
Replace credentials
Delete credentials for all users
Enable single sign on for this network
Perform immediately before user logon
Perform immediately after user logon
Maximum delay (seconds):
10
Allow additional dialogs to be displayed during single sign on
This network uses separate virtual LANs for machine and user authentication
OK
Cancel





Trên cisco ISE chúng ta có thể thấy PC đã xác thực thành công và truy cập được vào mạng.



BƯỚC 2: Cấu hình Flexible netflow trên switch và router.

Trên R1:

Flow Record định nghĩa các thông tin Netflow, chẳng hạn như những packet trong flow. Nếu chúng ta muốn thiết lập 1 Flow Record tùy chỉnh, thì chúng ta sẽ sử dụng tổ hợp lệnh match và collect để chỉ định các thông tin cần gửi đi trong gói NetFlow PDU. "Match" sử dụng cho định nghĩa các flow chính(key flow), "Match" quyết định tính duy nhất của flow. "Collect" chỉ chỉ định những thông tin thêm-phụ trợ bao gồm việc cung cấp những chi tiết đến Stealthwatch FlowCollector để report và phân tích.

Những thông tin trong tổ hợp lệnh flow record bên dưới:

Tos: type of service.

TTL: time to live

Source port và destination port của gói TCP hoặc application chạy trên nền tcp.

Interface vào/ra (input/output).

Ngoài ra còn có thể cấu hình thêm những thông số quan trọng như *ipv4 source address*, *ipv4 destination address*….

```
R1(config)#flow record FLOW-RECORD
R1(config-flow-record)#description stealthwatch_router
R1(config-flow-record)#match ipv4 tos
R1(config-flow-record)#match ipv4 ttl
R1(config-flow-record)#match ipv4 protocol
R1(config-flow-record)#match transport tcp source-port
R1(config-flow-record)#match transport tcp destination-port
R1(config-flow-record)#match interface input
R1(config-flow-record)#match interface output
R1(config-flow-record)#collect transport tcp flags
R1(config-flow-record)#collect counter bytes long
R1(config-flow-record)#collect counter packets long
```

```
R1(config)#flow exporter FLOW-EXPORTER
//Trong destination cần trỏ về stealthwatch FlowCollector
R1(config-flow-exporter)#destination 10.215.26.71
//source trong exporter chúng ta sẽ chọn cổng cần gửi thông tin về
stealthwatch, đó là cổng e0/0 trên R1
```

```
R1(config-flow-exporter)#source Ethernet0/0
//Stealthwatch sử dụng port 2055 để nhận flow
R1(config-flow-exporter)#transport udp 2055
```

Flow monitor dùng để liên kết các flow exporter và record hay các cấu trúc khác của flexible netflow lại với nhau. Ngoài ra trong flow monitor, cấu hình *cache timeout* được khuyên dùng vì mặc định stealthwatch chỉ định thời gian này là 30 phút. Trong cấu hình này thòi gian được tính bằng giây.

```
R1(config)#flow monitor FLOW-MON
R1(config-flow-monitor)#exporter FLOW-EXPORTER
R1(config-flow-monitor)#cache timeout inactive 60
R1(config-flow-monitor)#cache timeout active 15
R1(config-flow-monitor)#record FLOW-RECORD
```

Sau đó chúng ta cần cho phép các cấu hình netflow trên từng cổng mà chúng ta cần phân tích flow.

```
R1(config)#interface Ethernet0/0
R1(config-if)#ip flow monitor FLOW-MON input
R1(config-if)#ip flow monitor FLOW-MON output
R1(config-if)#ip flow ingress
R1(config-if)#ip flow egress
R1(config)#ip flow-export destination 10.215.26.71 2055
```

Trên Switch 1: Chúng ta thực hiện tương tự trên router.

```
SW1(config)#flow record FLOW-RECORD
SW1(config-flow-record)#description stealthwatch
SW1(config-flow-record)#match ipv4 tos
SW1(config-flow-record)#match ipv4 ttl
SW1(config-flow-record)#match ipv4 protocol
SW1(config-flow-record)#match transport source-port
SW1(config-flow-record)#match transport destination-port
SW1(config-flow-record)#match interface input
SW1(config-flow-record)#match interface output
SW1(config-flow-record)#collect transport tcp flags
SW1(config-flow-record)#collect counter bytes long
SW1(config-flow-record)#collect counter packets long
```

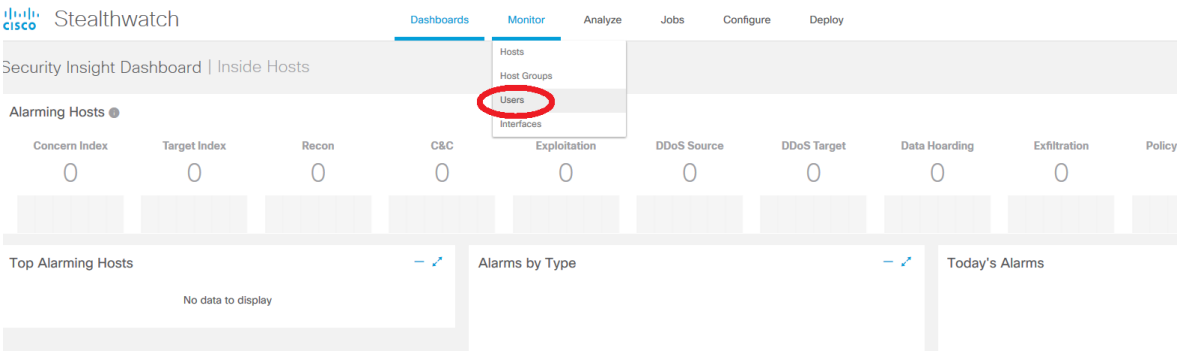
```
SW1(config)#flow exporter FLOW-EXPORTER
//Destination sẽ trỏ về stealthwatch FlowCollector.
SW1(config-flow-exporter)#destination 10.215.26.71
SW1(config-flow-exporter)#transport udp 2055
```

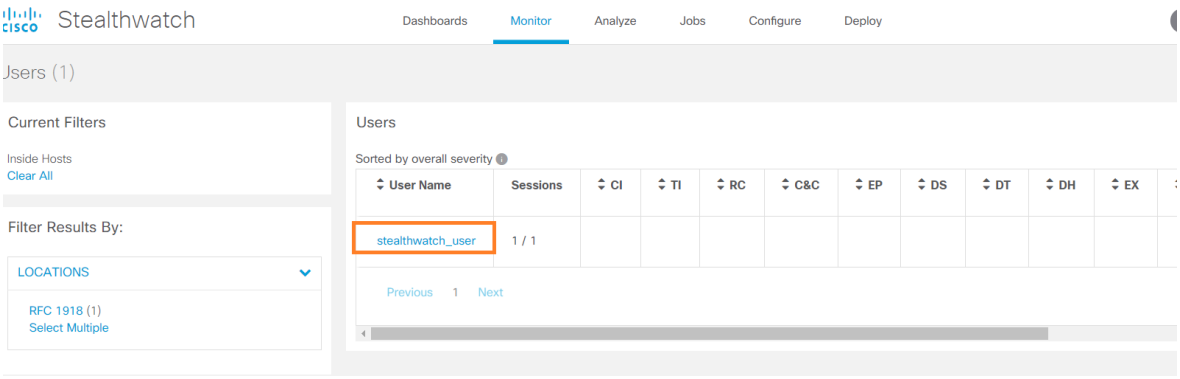
```
SW1(config)#flow monitor FLOW-MON
```

```
SW1(config-flow-monitor)#exporter FLOW-EXPORTER
SW1(config-flow-monitor)#cache timeout inactive 15
SW1(config-flow-monitor)#cache timeout inactive 15
SW1(config)#ip flow-exporter destination 10.215.26.71 2055
```

```
SW1(config)#interface Ethernet0/0-2
SW1(config-if-range)#ip flow ingress
SW1(config-if-range)#ip flow egress
SW1(config-if-range)#ip flow monitor FLOW-MON input
SW1(config-if-range)#ip flow monitor FLOW-MON output
```

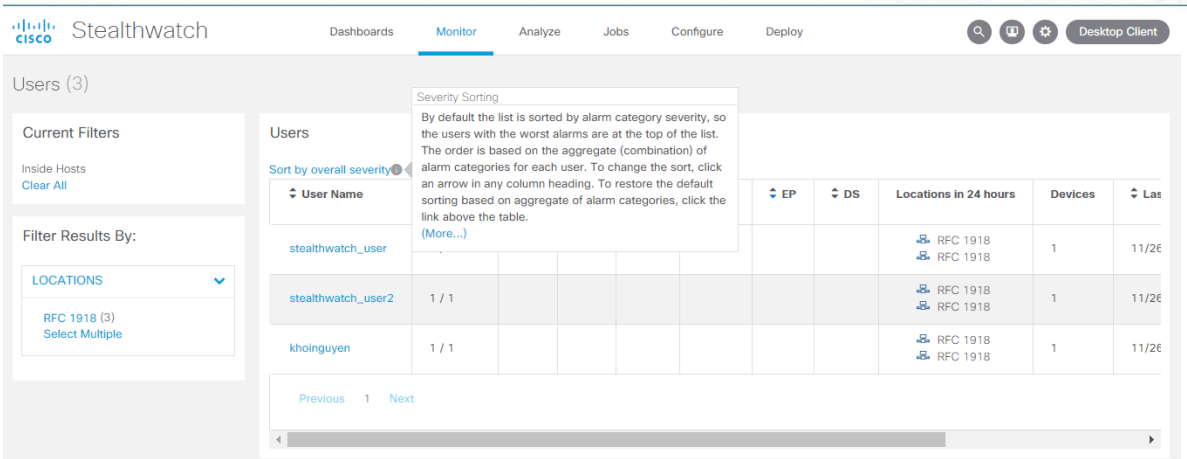
TRÊN STEALTHWATCH-SMC:

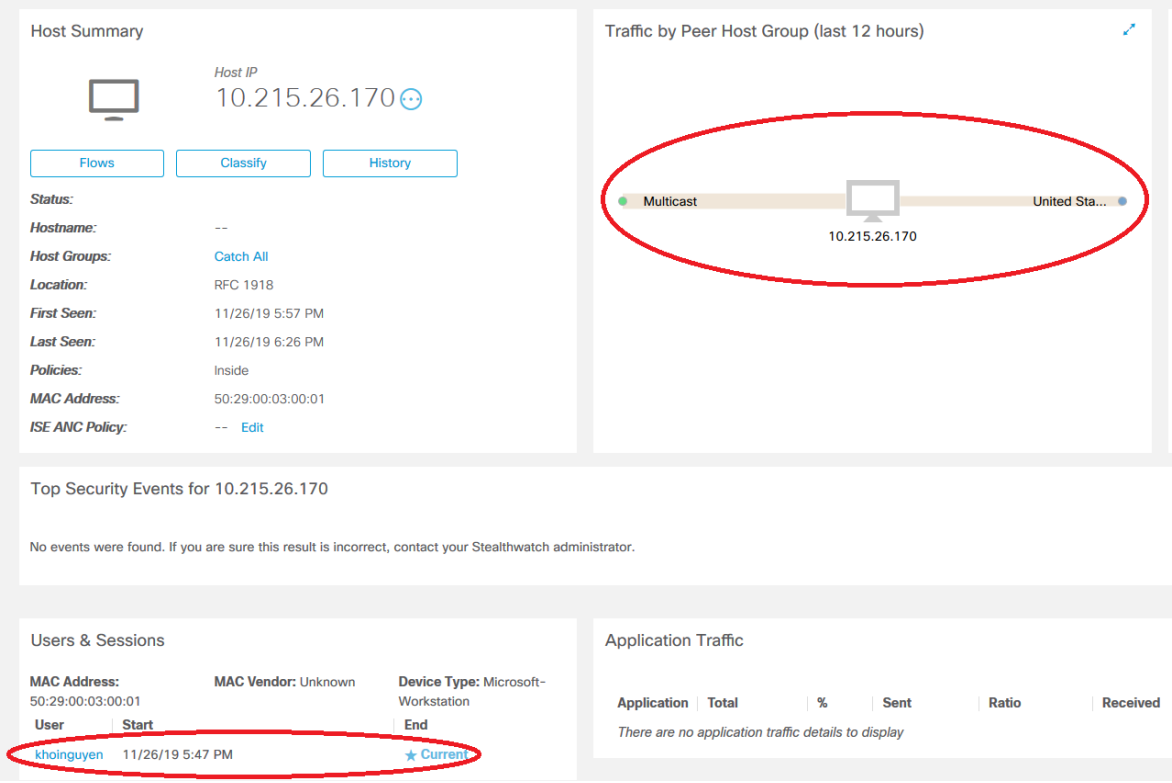




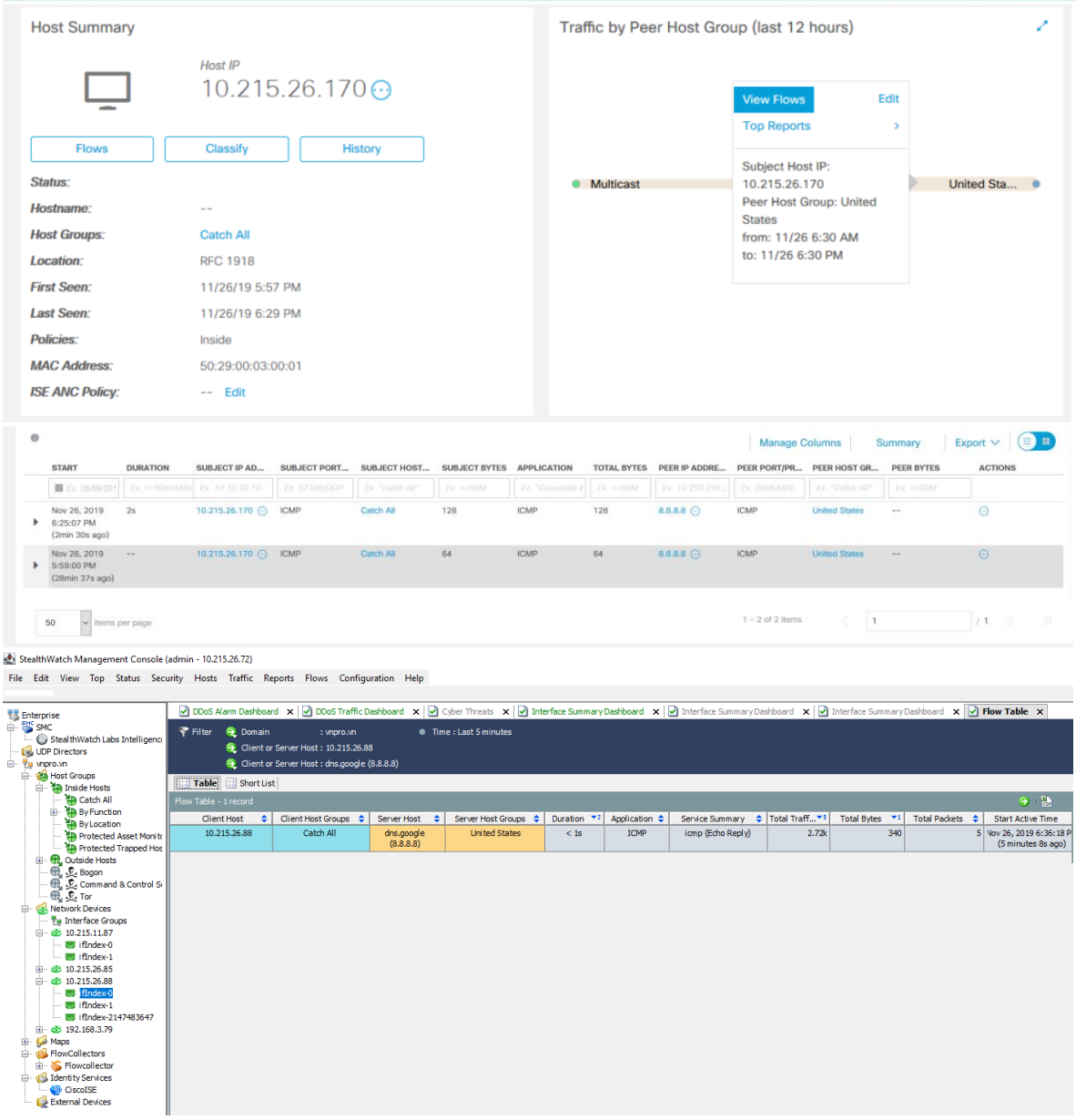
Thử đổi địa chỉ MAC hoặc dùng PC khác để login vào user khác ở card mạng và đi traffic bất kỳ.

Có thể thấy trong hình dưới đây, stealthwatch đã bắt được 3 user đã login vào mạng với username người dùng được gửi từ Cisco ISE.

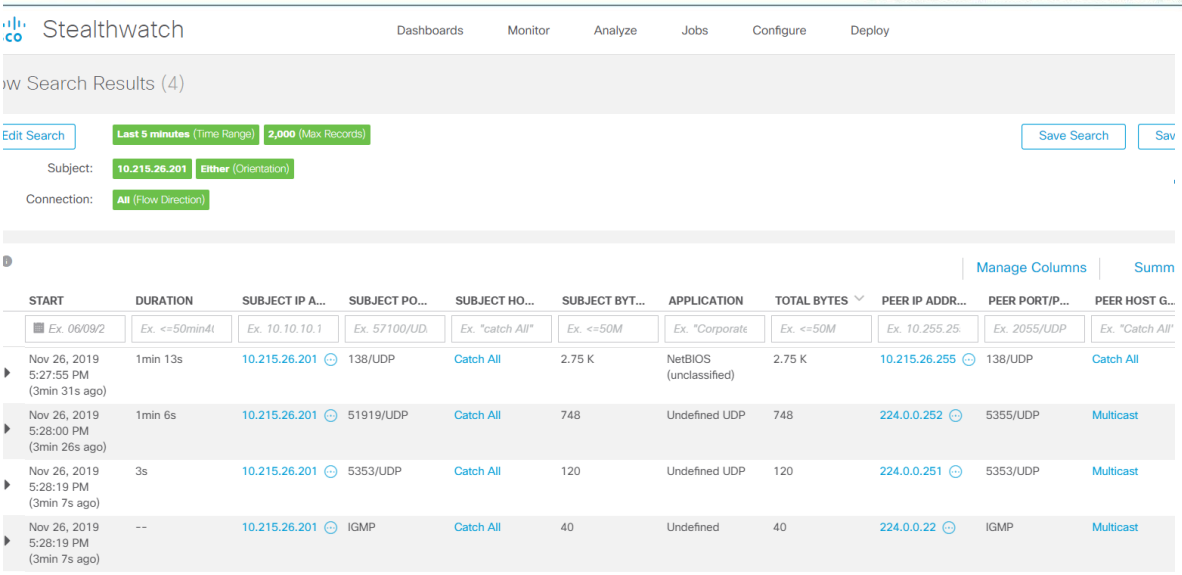




Chuột phải vào đường flow từ 10.215.26.172 đi US chọn **View Flows**, chúng ta có thể quan sát flows đi được từ client trên mà cụ thể là gói icmp đi đến 8.8.8.8



Ngoài ra chúng ta còn có thể quan sát được những dữ liệu application khác hay các transport udp/tcp.


Stealthwatch
Dashboards
Monitor
Analyze
Jobs
Configure
Deploy
w Search Results (4)
Edit Search
Last 5 minutes (Time Range)
2,000 (Max Records)
Save Search
Subject:
10.215.26.201
Either (Orientation)
Connection:
All (Flow Direction)
Manage Columns
Summ
START
DURATION
SUBJECT IP A...
SUBJECT PO...
SUBJECT HO...
SUBJECT BYT...
APPLICATION
TOTAL BYTES
PEER IP ADDR...
PEER PORT/P...
PEER HOST G...
Nov 26, 2019 5:27:55 PM (3min 31s ago)
1min 13s
10.215.26.201
138/UDP
Catch All
2.75 K
NetBIOS (unclassified)
2.75 K
10.215.26.255
138/UDP
Catch All
Nov 26, 2019 5:28:00 PM (3min 26s ago)
1min 6s
10.215.26.201
51919/UDP
Catch All
748
Undefined UDP
748
224.0.0.252
5355/UDP
Multicast
Nov 26, 2019 5:28:19 PM (3min 7s ago)
3s
10.215.26.201
5353/UDP
Catch All
120
Undefined UDP
120
224.0.0.251
5353/UDP
Multicast
Nov 26, 2019 5:28:19 PM (3min 7s ago)
--
10.215.26.201
IGMP
Catch All
40
Undefined
40
224.0.0.22
IGMP
Multicast