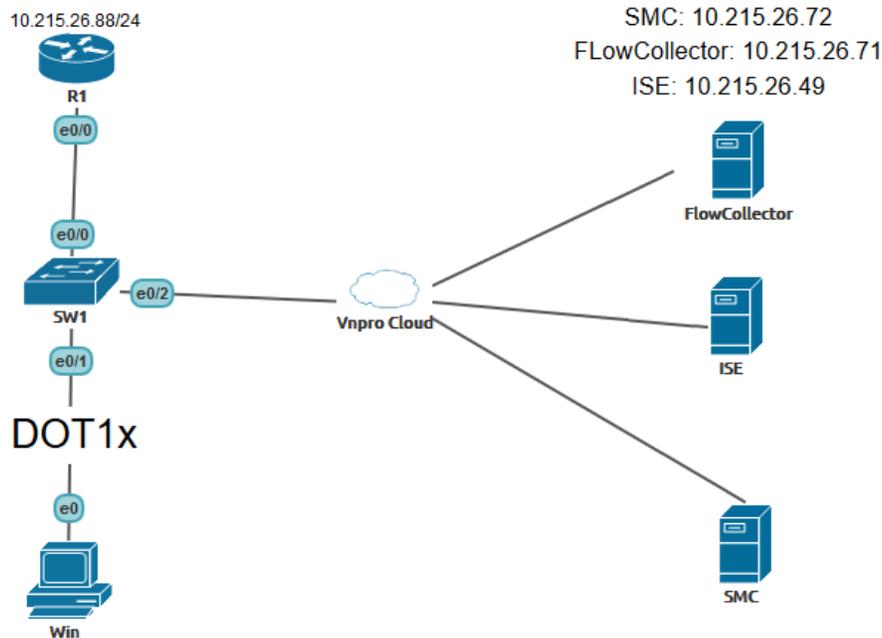


Lab – Steathwatch kết hợp Cisco ISE



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**.

BUỐC 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
-----
```

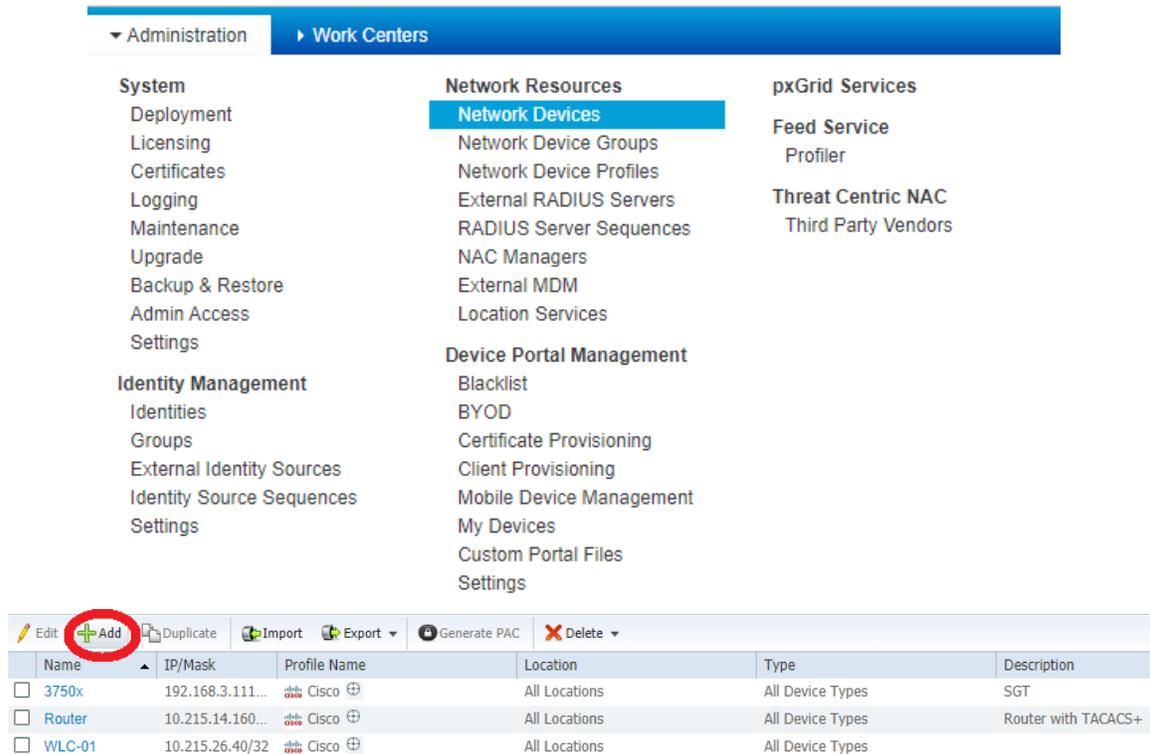
1	default	active	Et0/0, Et0/1, Et0/2, Et0/3
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

```
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 trở 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 hành thực hiện cấu hình Cisco ISE theo dãy hình bên dưới.



Administration | Work Centers

- System
 - Deployment
 - Licensing
 - Certificates
 - Logging
 - Maintenance
 - Upgrade
 - Backup & Restore
 - Admin Access
 - Settings
- Identity Management
 - Identities
 - Groups
 - External Identity Sources
 - Identity Source Sequences
 - Settings
- Network Resources
 - Network Devices**
 - Network Device Groups
 - Network Device Profiles
 - External RADIUS Servers
 - RADIUS Server Sequences
 - NAC Managers
 - External MDM
 - Location Services
 - Device Portal Management
 - Blacklist
 - BYOD
 - Certificate Provisioning
 - Client Provisioning
 - Mobile Device Management
 - My Devices
 - Custom Portal Files
 - Settings
- pxGrid Services
 - Feed Service Profiler
 - Threat Centric NAC Third Party Vendors

Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/> 3750x	192.168.3.111...	Cisco	All Locations	All Device Types	SGT
<input type="checkbox"/> Router	10.215.14.160...	Cisco	All Locations	All Device Types	Router with TACACS+
<input type="checkbox"/> WLC-01	10.215.26.40/32	Cisco	All Locations	All Device Types	

* Name
Description

IP Address * IP: /

IPv6 is supported only for TACACS. At least one IPv4 must be defined when RADIUS is selected

* Device Profile

Model Name
Software Version

* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

CoA Port

RADIUS DTLS Settings ⓘ

DTLS Required ⓘ

Shared Secret ⓘ

CoA Port

Issuer CA of ISE Certificates for CoA ⓘ

DNS Name

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

CoA Port

RADIUS DTLS Settings ⓘ

DTLS Required ⓘ

Shared Secret ⓘ

CoA Port

Issuer CA of ISE Certificates for CoA ⓘ

DNS Name

General Settings

Enable KeyWrap ⓘ

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECEIMAL

TACACS Authentication Settings

SNMP Settings

Advanced TrustSec Settings

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 quanh → điền **policy name** → Trong mục **condition** bấm vào dấu + hoặc **dấu cây bút** → kéo thả như ảnh dưới đây.

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
+	Dot1x_Radius		Wired_802.1X	Default Network Access	0		
+	Default	Default policy set		Default Network Access	0		

Conditions Studio

Library

Search by Name

- Catalyst_Switch_Local_Web_Authentication
- Switch_Local_Web_Authentication
- Switch_Web_Authentication
- Wired_802.1X
- Wired_MAB
- Wireless_802.1X
- Wireless_Access
- Wireless_MAB
- WLC_Web_Authentication

Editor

Wired_802.1X

Set to 'Is not'

+ New AND OR

Close Use

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

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
+	Dot1x_Radius		Wired_802.1X	Default Network Access	0		
+	Default	Default policy set		Default Network Access	0		

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.

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (2)

+	Status	Rule Name	Conditions	Results		Hits	Actions
				Profiles	Security Groups		
Search							
		Dot1X	Wired_802.1X	PermitAccess	Select from list		
		Default		DenyAccess	Select from list	0	

Reset Save

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.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb navigation is: Administration > Identity Management > Identities. The left sidebar shows the 'Policy Sets' section with 'Dot1X_Radius' selected. The main content area displays a table of policy sets and a list of navigation options under 'Identity Management'.

Status	Policy Set Name	Description	Conditions
	Dot1X_Radius		Wired

- System
 - Deployment
 - Licensing
 - Certificates
 - Logging
 - Maintenance
 - Upgrade
 - Backup & Restore
 - Admin Access
 - Settings
- Identity Management**
 - Identities**
 - Groups
 - External Identity Sources
 - Identity Source Sequences
 - Settings
- Network Resources
 - Network Devices
 - Network Device Groups
 - Network Device Profiles
 - External RADIUS Servers
 - RADIUS Server Sequences
 - NAC Managers
 - External MDM
 - Location Services
- Device Portal Management
 - Blacklist
 - BYOD
 - Certificate Provisioning
 - Client Provisioning
 - Mobile Device Management
 - My Devices
 - Custom Portal Files
 - Settings
- pxGrid Services
 - Feed Service
 - Profiler
 - Threat Centric NAC
 - Third Party Vendors

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access User

* Name

Status Enabled

Email

Passwords

Password Type:

Password Re-Enter Password

* Login Password ⓘ

Enable Password ⓘ

User Information

First Name

Last Name

Account Options

Description

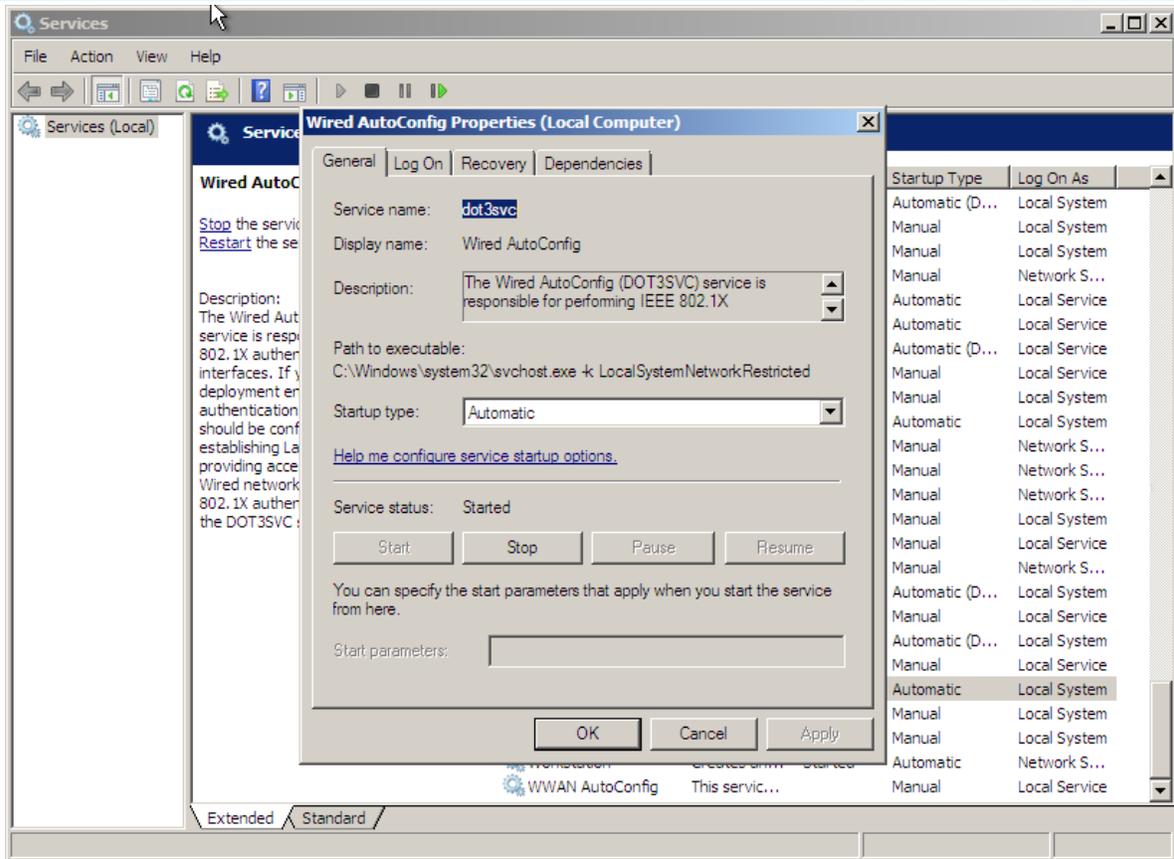
Change password on next login

Account Disable Policy

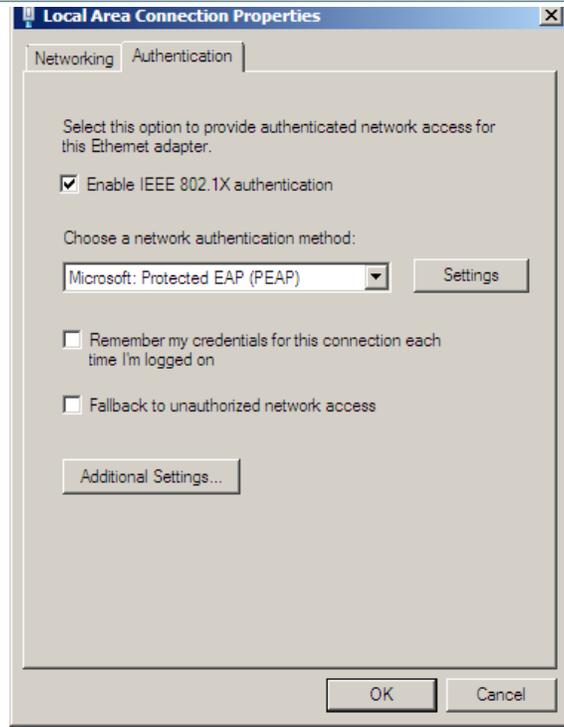
Disable account if date exceeds (yyyy-mm-dd)

User Groups

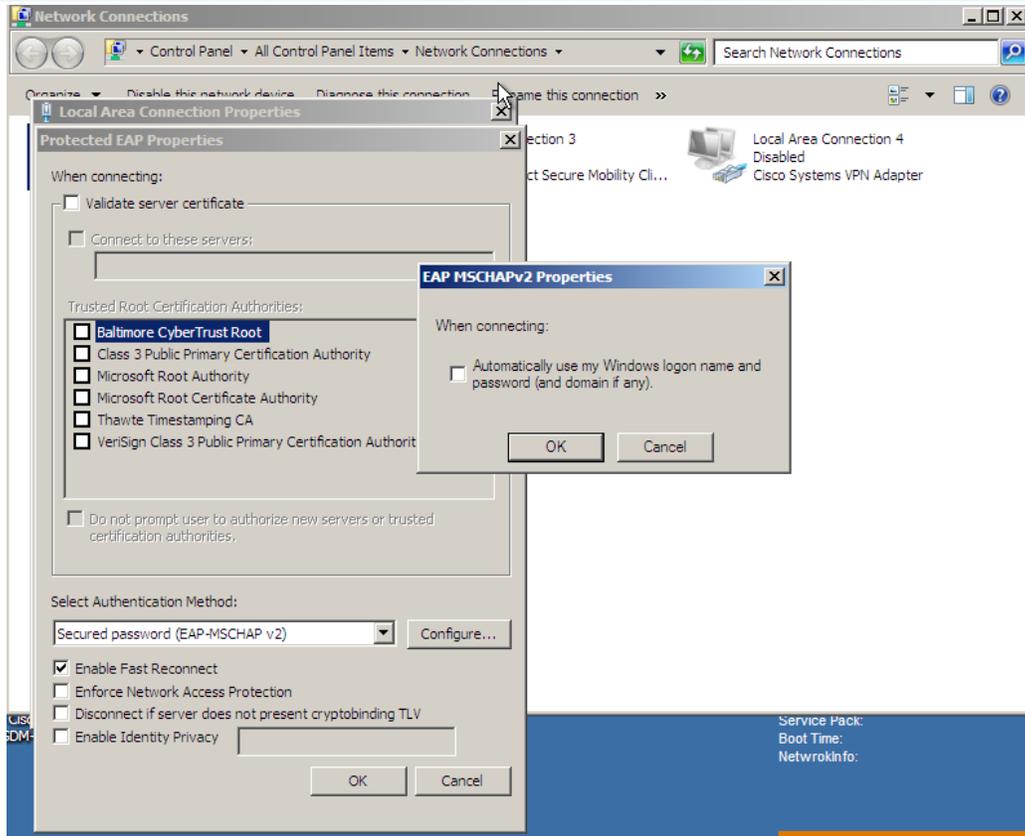
Như vậy chúng ta đã tạo được user và set policy cho wired dot1x trên Cisco ISE.
Trên PC chúng ta tiến hành điều chỉnh card mạng cho việc xác thực dot1x. Đầu tiên, ta bấm tổ hợp phím Windows+R → services.msc → Tìm services Wired Autoconfig → Chuột phải chọn **Properties** → Trong tab **General** chọn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



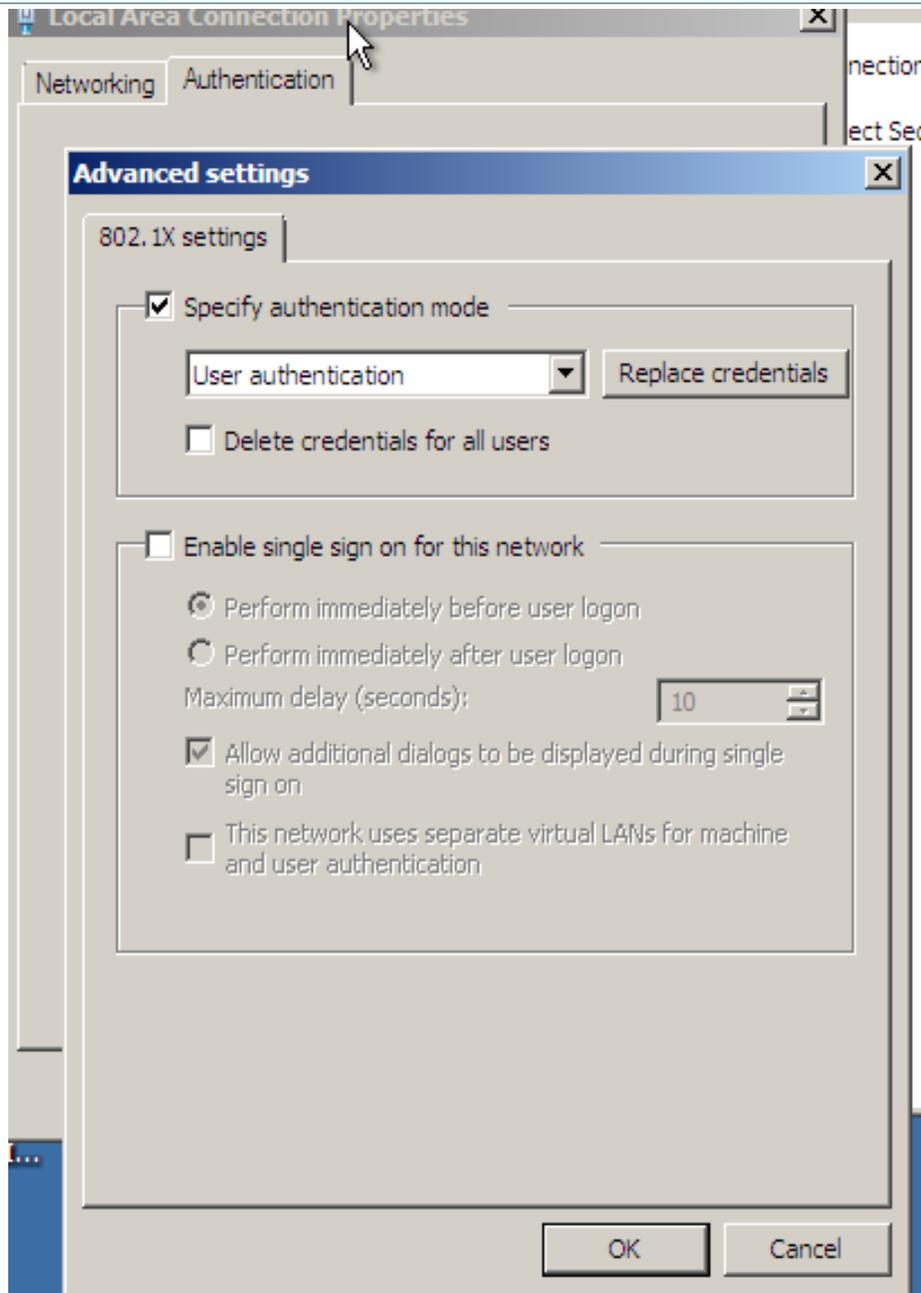
Chuyển sang điều chỉnh card mạng, Chuột phải vào card mạng đang chạy → Prperties → Trong tab Authentication tick chọn như ảnh dưới đây.

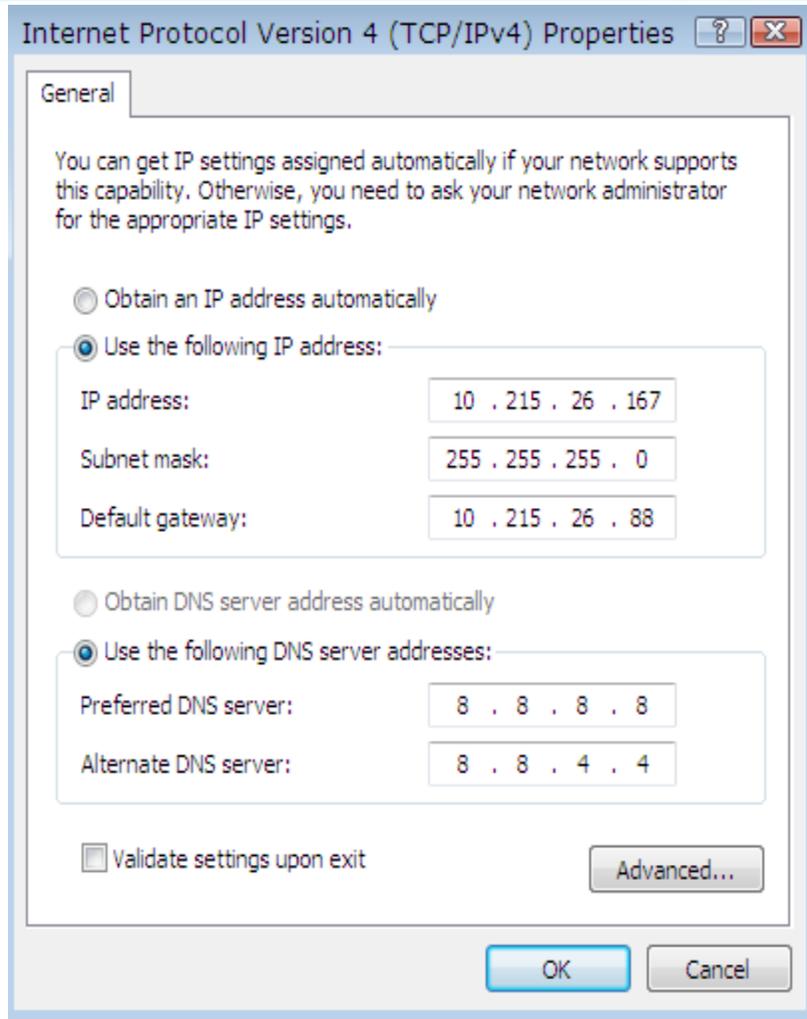


Trong tab Choose a network authentication method Chọn Settings → Bỏ tick Validate server certificate (trong môi trường lab, chúng ta không cần windows xác thực chứng chỉ của Cisco ISE) → Trong mục Select Authentication Method Chọn Configure... → Bỏ tick Automatically use my Windows logon name and password (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.

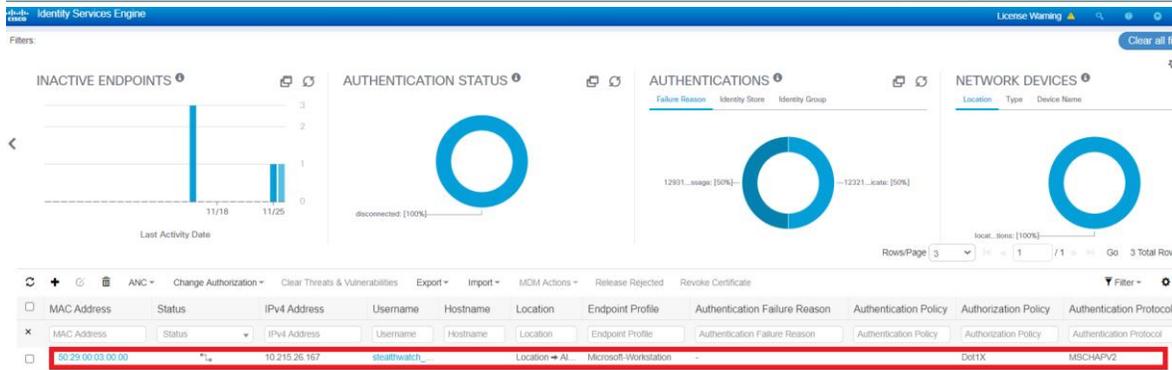




```
Administrator: C:\Windows\system32\cmd.exe
WINS Proxy Enabled. . . . . : No
Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 50-29-00-03-00-00
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::dd3a:6c33:ee52:cc26%11(Preferred)
IPv4 Address. . . . . : 10.215.26.167(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.215.26.88
DHCPv6 IAID . . . . . : 240276480
DHCPv6 Client DUID. . . . . : 00-01-00-01-1C-84-05-64-52-54-00-12-34-56
```

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



BUỚC 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 khuyến dùng vì mặc định stealthwatch chỉ định thời gian này là 30 phút. Trong cấu hình này thời 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 trở 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:

Stealthwatch Monitor Dashboard. The 'Monitor' tab is selected. A dropdown menu is open over the 'Users' option, which is circled in red. The dashboard shows various security metrics like Concern Index, Target Index, Recon, C&C, Exploitation, DDoS Source, DDoS Target, Data Hoarding, and Exfiltration, all with a value of 0. Below these are sections for 'Top Alarming Hosts' (No data to display) and 'Alarms by Type'.

Stealthwatch Users (1) page. The 'Monitor' tab is selected. The page title is 'Users (1)'. On the left, there are 'Current Filters' (Inside Hosts, Clear All) and 'Filter Results By' (LOCATIONS, RFC 1918 (1), Select Multiple). The main content area shows a table of users, sorted by overall severity. The table has columns for User Name, Sessions, CI, TI, RC, C&C, EP, DS, DT, DH, and EX. The first row shows 'stealthwatch_user' with 1 session. Below the table are 'Previous', '1', and 'Next' navigation links.

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.

Stealthwatch Monitor

Users (3)

Current Filters: Inside Hosts, Clear All

Filter Results By: LOCATIONS (RFC 1918 (3), Select Multiple)

Users

Severity Sorting: By default the list is sorted by alarm category severity, so the users with the worst alarms are at the top of the list. The order is based on the aggregate (combination) of alarm categories for each user. To change the sort, click an arrow in any column heading. To restore the default sorting based on aggregate of alarm categories, click the link above the table. (More...)

User Name	EP	DS	Locations in 24 hours	Devices	Last
stealthwatch_user			RFC 1918 RFC 1918	1	11/26
stealthwatch_user2	1 / 1		RFC 1918 RFC 1918	1	11/26
khoinguyen	1 / 1		RFC 1918 RFC 1918	1	11/26

Host Summary

Host IP: 10.215.26.170

Flows | Classify | History

Status: --

Hostname: --

Host Groups: Catch All

Location: RFC 1918

First Seen: 11/26/19 5:57 PM

Last Seen: 11/26/19 6:26 PM

Policies: Inside

MAC Address: 50:29:00:03:00:01

ISE ANC Policy: -- Edit

Traffic by Peer Host Group (last 12 hours)

Top Security Events for 10.215.26.170

No events were found. If you are sure this result is incorrect, contact your Stealthwatch administrator.

Users & Sessions

MAC Address: 50:29:00:03:00:01 | MAC Vendor: Unknown | Device Type: Microsoft-Workstation

User	Start	End
khoinguyen	11/26/19 5:47 PM	★ Current

Application Traffic

Application	Total	%	Sent	Ratio	Received
There are no application traffic details to display					

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

Host Summary

Host IP: 10.215.26.170

Flows | Classify | History

Status: --

Hostname: --

Host Groups: Catch All

Location: RFC 1918

First Seen: 11/26/19 5:57 PM

Last Seen: 11/26/19 6:29 PM

Policies: Inside

MAC Address: 50:29:00:03:00:01

ISE ANC Policy: -- Edit

Traffic by Peer Host Group (last 12 hours)

View Flows | Edit

Top Reports >

Subject Host IP: 10.215.26.170
Peer Host Group: United States
from: 11/26 6:30 AM
to: 11/26 6:30 PM

Multicast → United Sta...

START	DURATION	SUBJECT IP AD...	SUBJECT PORT...	SUBJECT HOST...	SUBJECT BYTES	APPLICATION	TOTAL BYTES	PEER IP ADDRE...	PEER PORT/PR...	PEER HOST GR...	PEER BYTES	ACTIONS
Nov 26, 2019 6:25:07 PM (2min 30s ago)	2s	10.215.26.170	ICMP	Catch All	128	ICMP	128	8.8.8.8	ICMP	United States	--	
Nov 26, 2019 5:59:00 PM (28min 37s ago)	--	10.215.26.170	ICMP	Catch All	64	ICMP	64	8.8.8.8	ICMP	United States	--	

StealthWatch Management Console (admin - 10.215.26.72)

File Edit View Top Status Security Hosts Traffic Reports Flows Configuration Help

- Enterprise
- SMC
- StealthWatch Labs Intelligeno
- UDP Directors
- vnpro.vn
- Host Groups
 - Inside Hosts
 - Catch All
 - By Function
 - By Location
 - Protected Asset Monit
 - Protected Trapped Host
 - Outside Hosts
 - Bogon
 - Command & Control S
 - SC: Top
- Network Devices
- Interface Groups
 - 10.215.11.87
 - ifIndex-0
 - ifIndex-1
 - 10.215.26.85
 - 10.215.26.88
 - ifIndex-0
 - ifIndex-1
 - ifIndex-2147483647
- 192.168.3.79
- Mass
- FlowCollectors
 - Flowcollector
- Identify Services
- CiscoISE
- External Devices

DDoS Alarm Dashboard
DDoS Traffic Dashboard
Cyber Threats
Interface Summary Dashboard
Interface Summary Dashboard
Interface Summary Dashboard
Flow Table

Filter: Domain: vnpro.vn | Time: Last 5 minutes

Client or Server Host: 10.215.26.88
Client or Server Host: dns.google (8.8.8.8)

Client Host	Client Host Groups	Server Host	Server Host Groups	Duration	Application	Service Summary	Total Traff...	Total Bytes	Total Packets	Start Active Time
10.215.26.88	Catch All	dns.google (8.8.8.8)	United States	< 1s	ICMP	icmp (Echo Reply)	2.72k	340	5	Nov 26, 2019 6:36:18 P (5 minutes 8s ago)

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



Search Results (4)

Edit Search

Last 5 minutes (Time Range)

2,000 (Max Records)

Save Search

Save

Subject: 10.215.26.201 Ether (Orientation)

Connection: All (Flow Direction)

START	DURATION	SUBJECT IP A...	SUBJECT PO...	SUBJECT HO...	SUBJECT BYT...	APPLICATION	TOTAL BYTES	PEER IP ADDR...	PEER PORT/P...	PEER HOST G...
Ex. 06/09/2	Ex. <=50min/dt	Ex. 10.10.10.1	Ex. 57100/UD.	Ex. "catch All"	Ex. <=50M	Ex. "Corporate	Ex. <=50M	Ex. 10.255.25	Ex. 2055/UDP	Ex. "catch All"
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



CÔNG TY TNHH TƯ VẤN VÀ DỊCH VỤ CHUYÊN VIỆT
TRUNG TÂM TIN HỌC VNPRO

ĐC: 276 - 278 Ung Văn Khiêm, P. Thanh Mỹ Tây, Tp. Hồ Chí Minh
ĐT: (028) 35124257 | Hotline: 0933427079 Email: vnpro@vnpro.org
