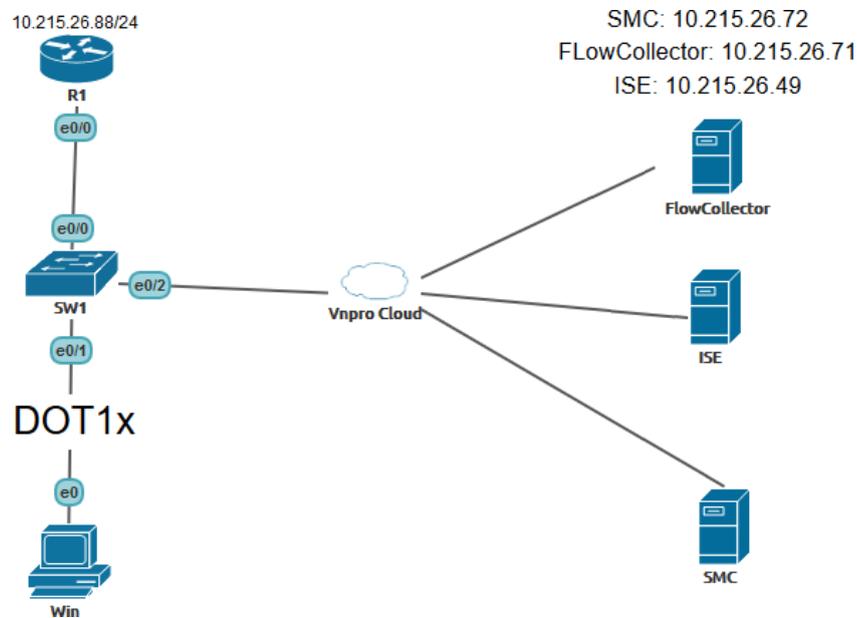


LAB - TÍCH HỢP STEALTHWATCH

I. SƠ ĐỒ:



II. MỤC ĐÍCH:

Trong bối cảnh an ninh mạng thì tầm quan trọng của visibility trong hệ thống mạng là rất lớn. Để đáp ứng nhu cầu của quản trị mạng thì Cisco đã mang đến cho các quản trị viên hay các giải pháp chuyên về bảo mật trong đó là Cisco ISE và Stealthwatch, hai thiết bị này có chức năng và thế mạnh khác nhau. Chính vì thế Cisco đã đưa ra giải pháp tích hợp hai thiết bị trên thông qua giao thức PxGrid

III. THỰC HIỆN:

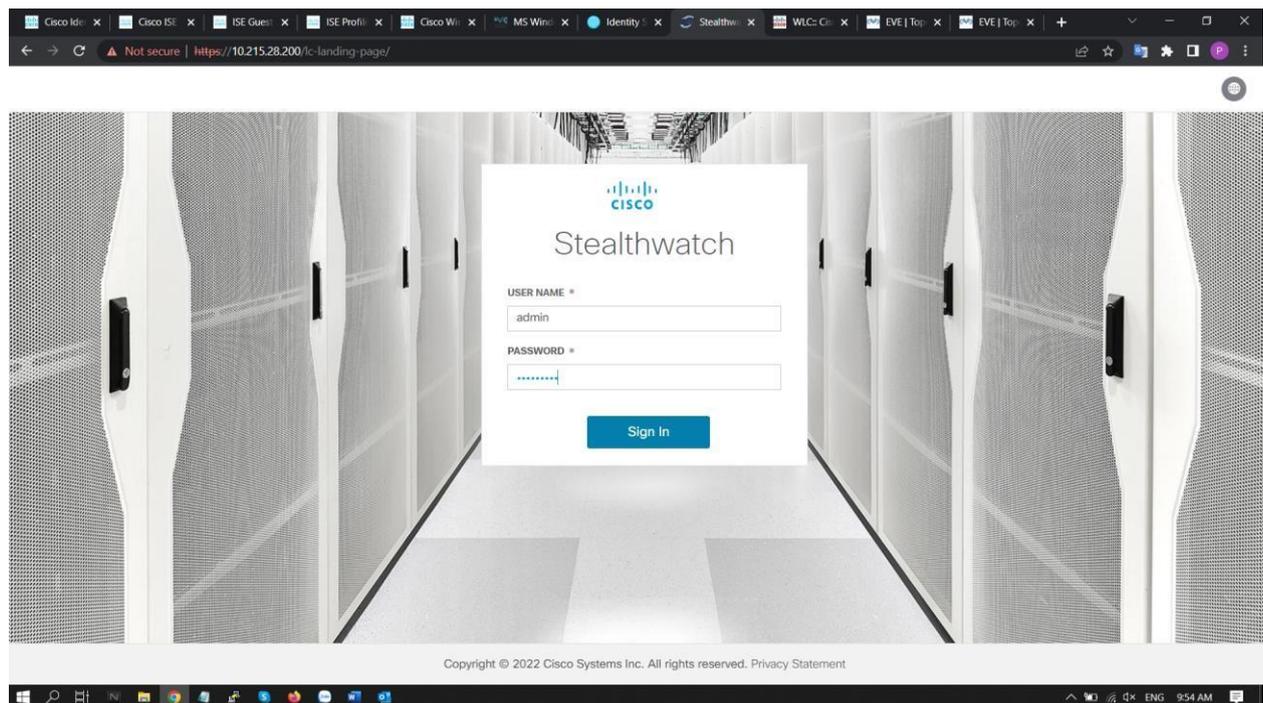
Phần 1: liên kết Stealth Watch và Cisco Ise qua giao thức PxGrid

Cấu hình:

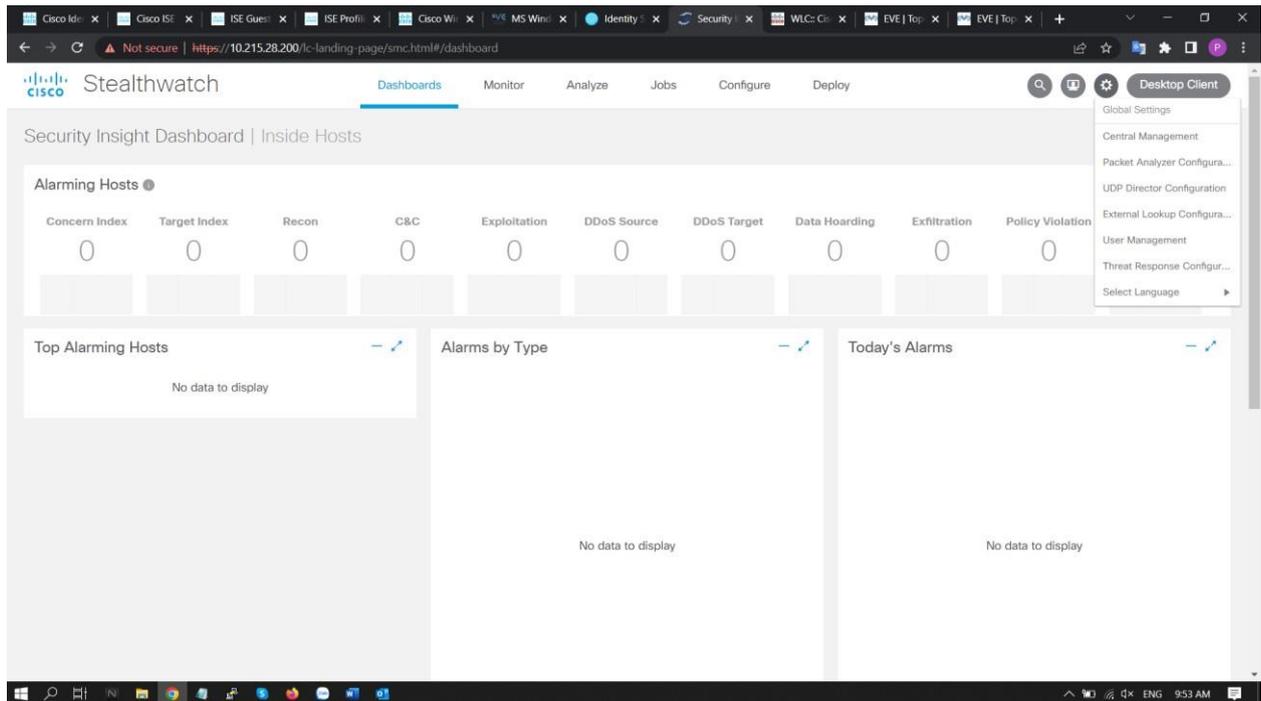
- ✓ Đầu tiên ở bước 1 chúng ta tiến hành vào Stealthwatch Management Console để tạo ra 1 CSR file (Cisco Cloud Services Router) có đuôi .csr để có thể dùng cho Cisco ISE ở bước 2 để Cisco ISE có thể tạo ra 1 Certificate phản hồi.

Bước 1:

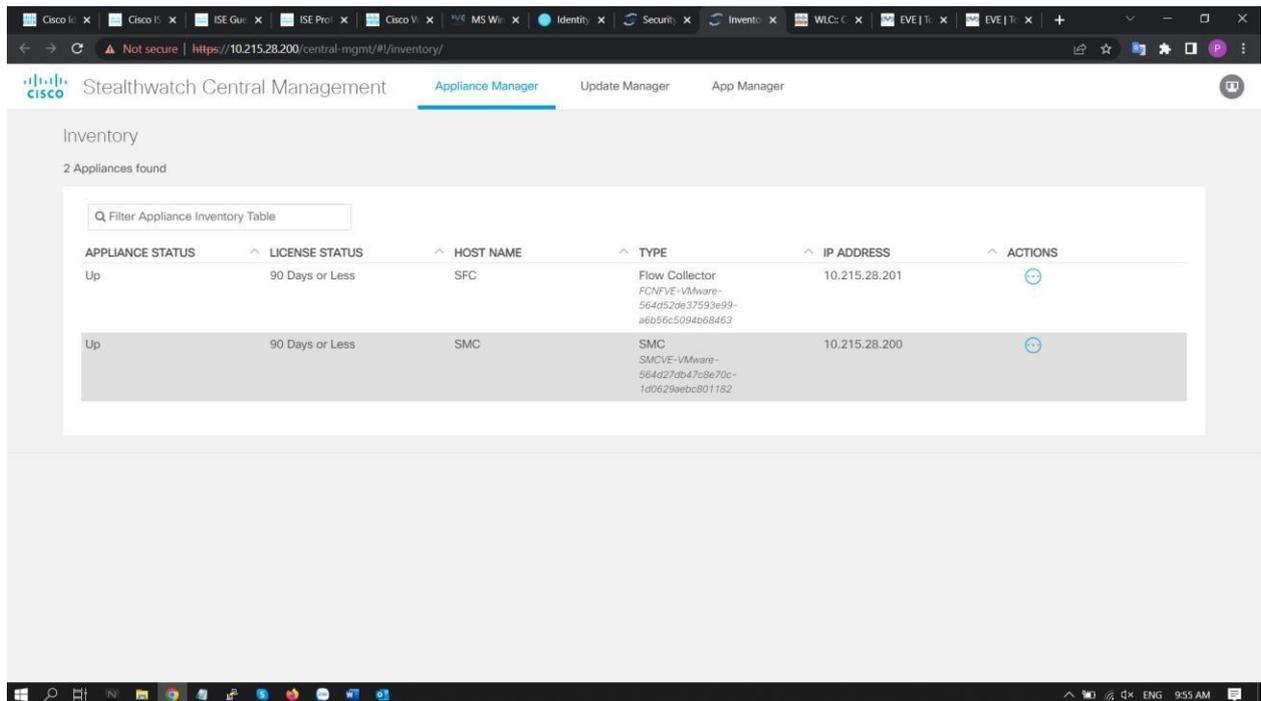
1.1 : Đăng nhập vào Stealthwatch Management Console.

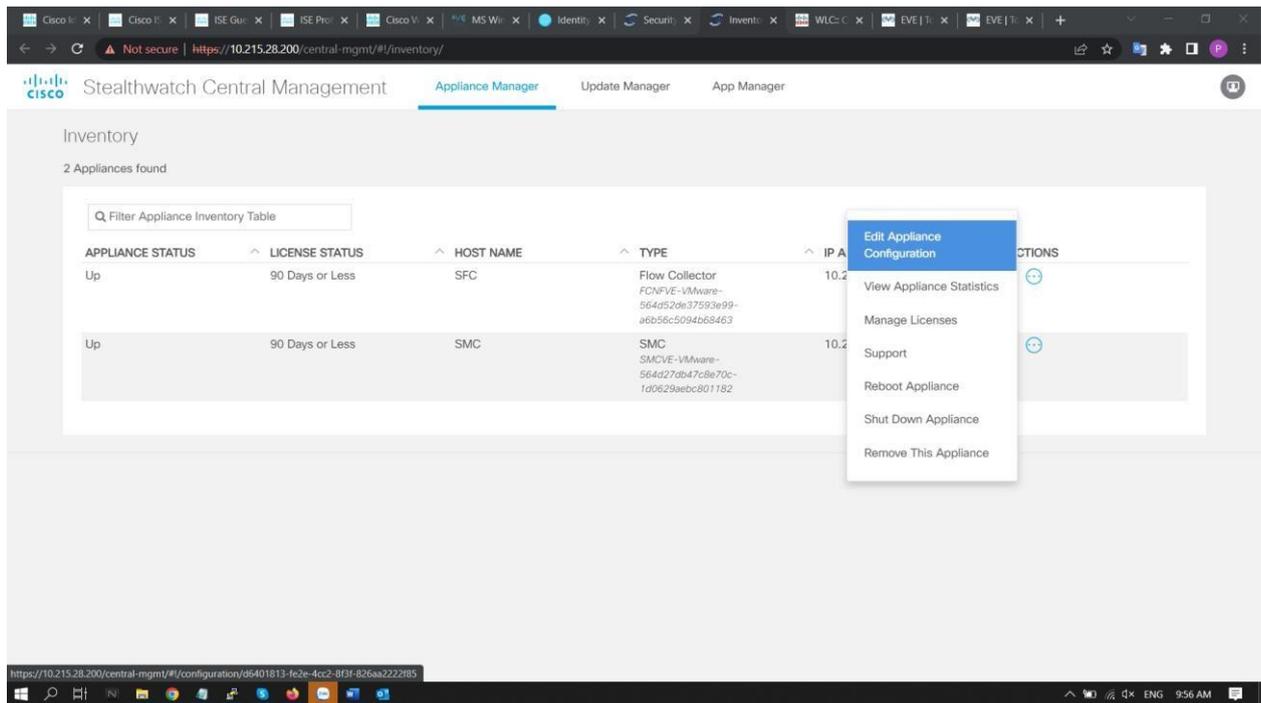


1.2: Click vào biểu tượng Global Settings sau đó click Central Management.

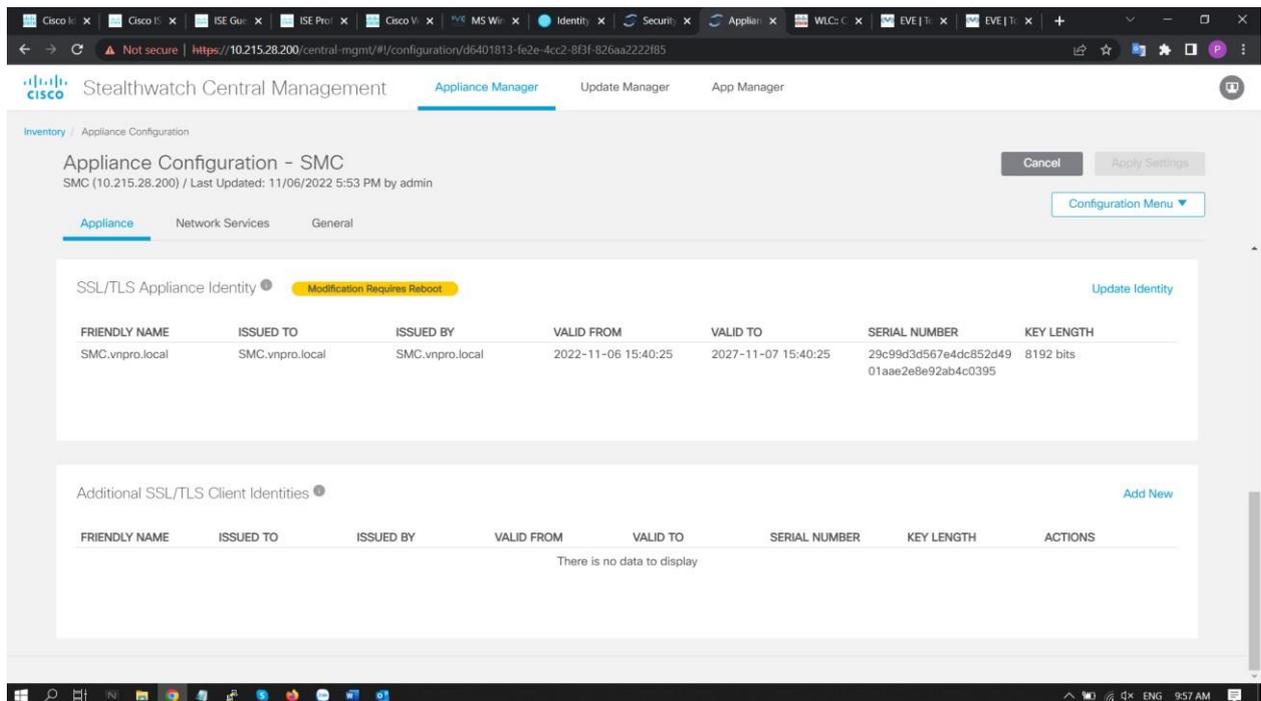


1.3: Tại Appliance Manager inventory, click vào biểu tượng mở rộng của phía bên phải cùng của SMC (biểu tượng hình tròn màu xanh như hình bên dưới):

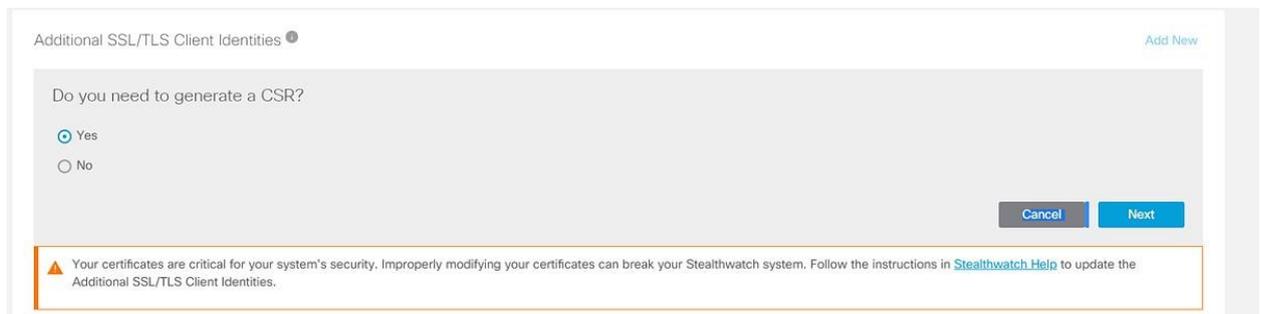
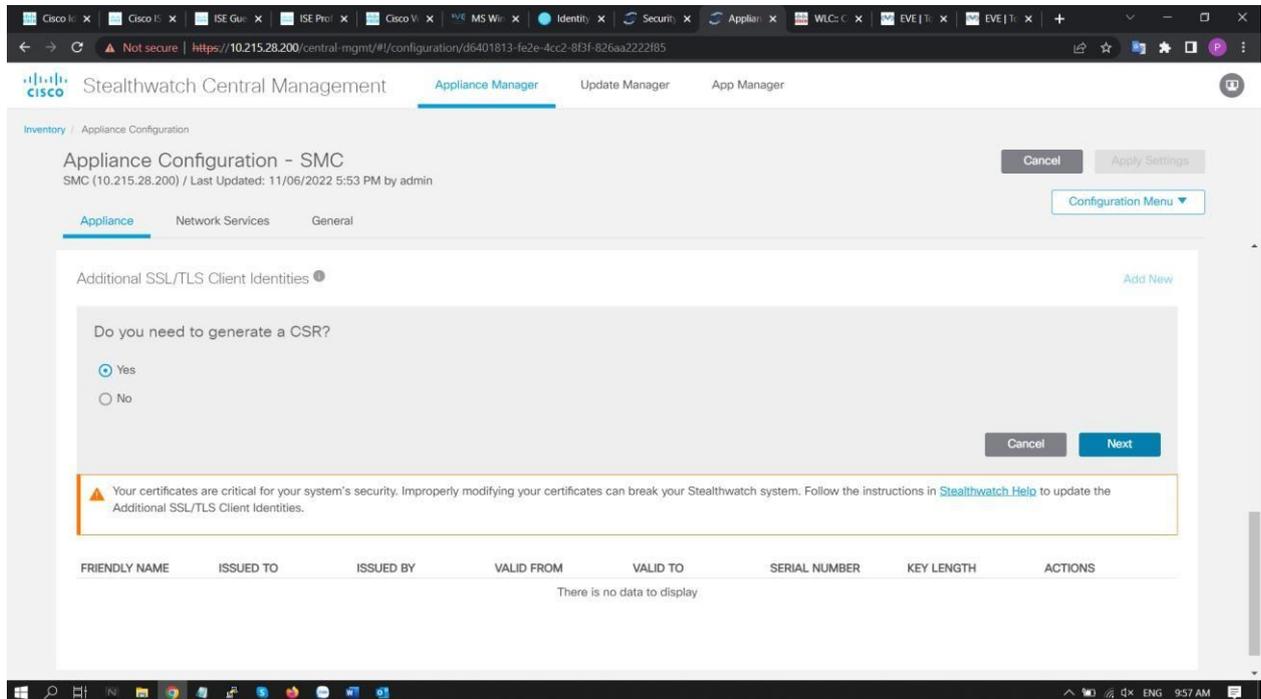




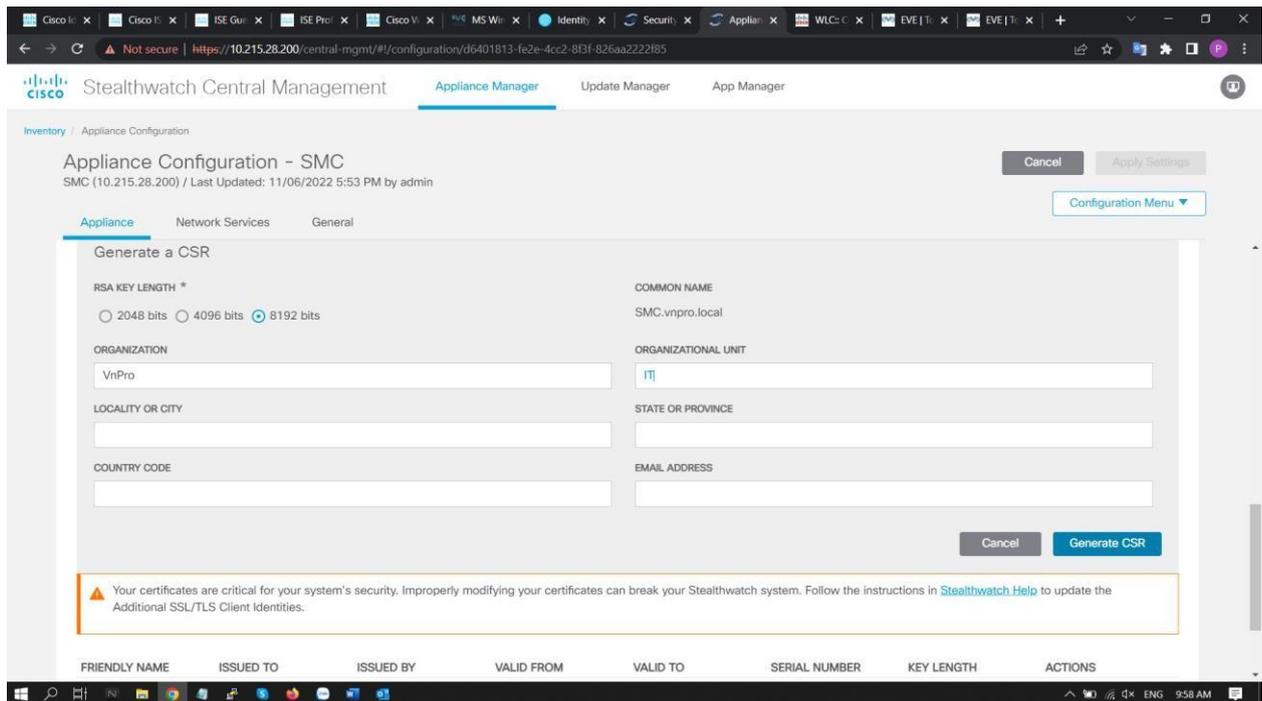
1.4: Tiếp tục ta vào Additional SSL/TLS Client Identities ngay phía dưới của mục Appliance



1.5: Ta tiến hành click vào Add new, hộp thoại bên dưới sẽ hiện ra ta tiến hành click Next



1.6: Ta tiến hành Generate CSR theo mẫu ví dụ bên dưới, sau đó click Generate CSR:



Additional SSL/TLS Client Identities 0

[Add New](#)

Generate a CSR

RSA KEY LENGTH *
 2048 bits 4096 bits 8192 bits

COMMON NAME
StealthWatchManagementConsole.stealthwatch.vnpro.org

ORGANIZATION
VnPro

ORGANIZATIONAL UNIT
IT

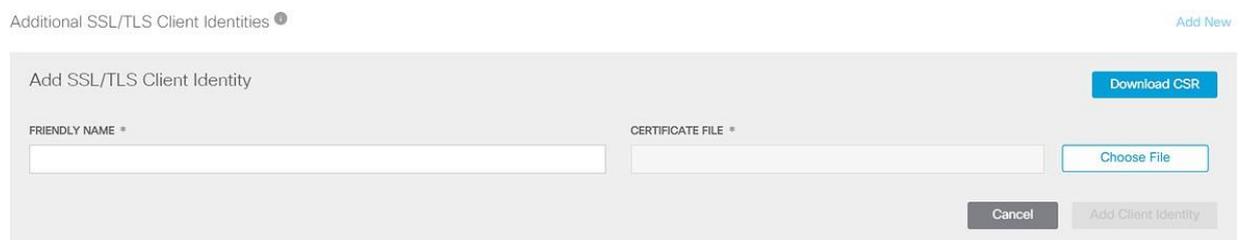
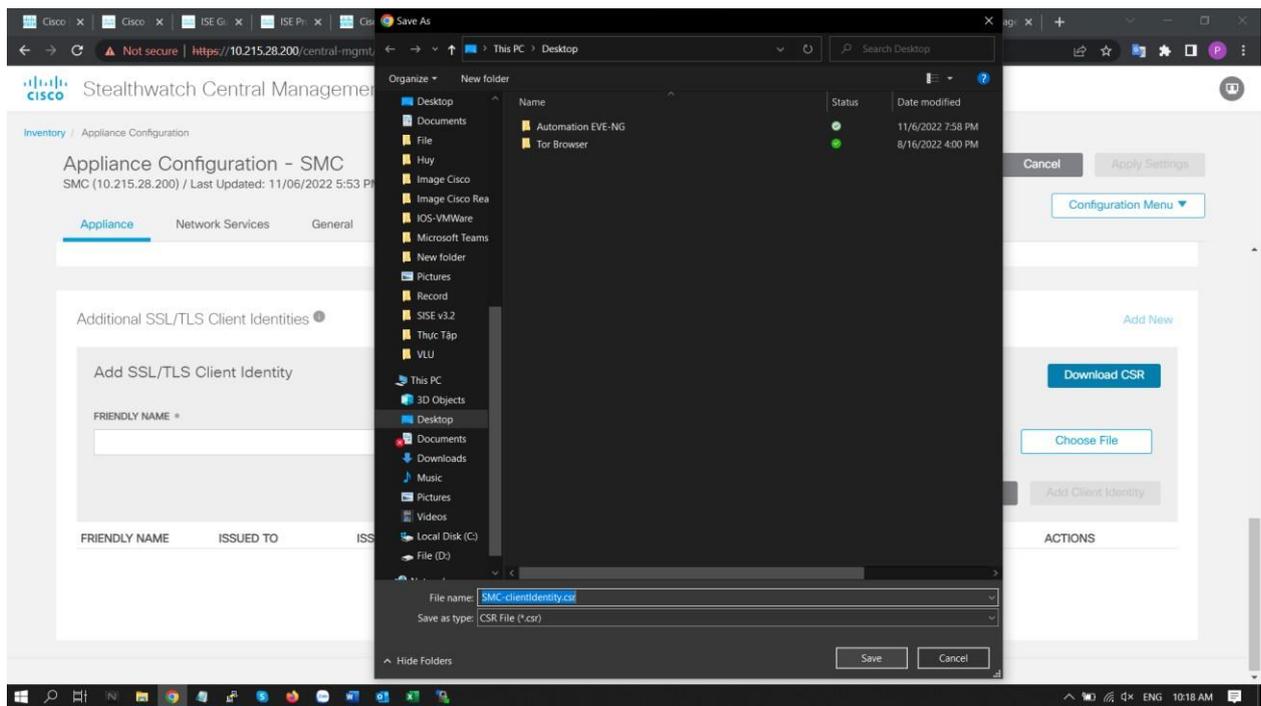
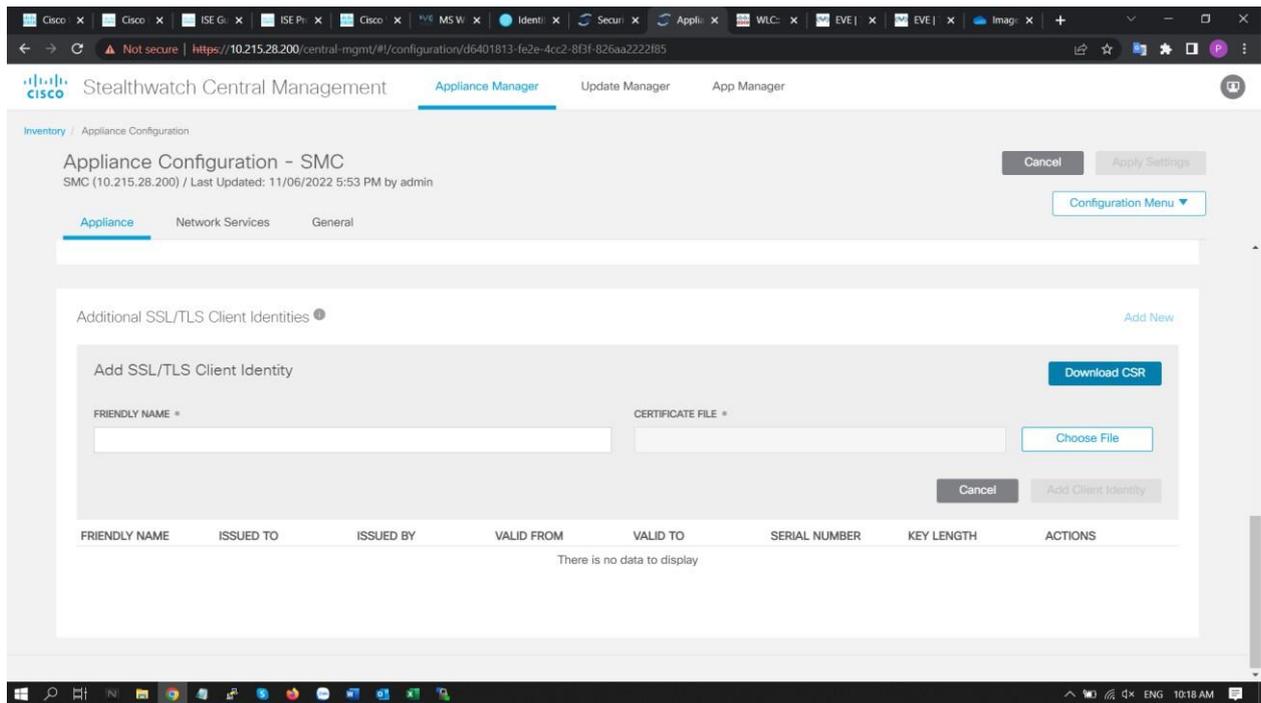
LOCALITY OR CITY

STATE OR PROVINCE

COUNTRY CODE

EMAIL ADDRESS

1.7: Tiếp theo tại Additional SSL/TLS Client Identities ta click vào biểu tượng Download CSR.



✓ Sau khi có được 1 CSR file từ Stealthwatch ta tiến hành thực hiện bước tiếp

theo là đưa CSR file này vào Cisco ISE để Cisco ISE có thể tạo ra 1 chứng

chỉ (Certificate) phản hồi có đuôi .cer lại cho Stealthwatch với mật khẩu của chứng chỉ phản hồi này sẽ được thiết đặt trên Cisco ISE.

Bước 2:

2.1 : Ta đăng nhập vào Cisco ISE Management Interface.

2.2: Tiến hành vào Cisco ISE để bật PxGrid cho phép Stealthwatch giao tiếp với Cisco ISE thông qua giao thức này: ta vào Administration → System → Deployment.



The screenshot shows the Cisco Identity Services Engine (ISE) Management Interface. The navigation menu includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Under Administration, the path System → Deployment is selected. The main content area displays the 'Deployment Nodes' configuration page. On the left, a tree view shows 'Deployment' and 'PAN Failover'. The main table lists deployment nodes with columns for Hostname and Personas. The 'Cisco-ISE-2' node is selected, and its associated personas are 'Administration, Monitoring, Policy Service, pxGrid'.

Hostname	Personas
<input type="checkbox"/> Cisco-ISE-2	Administration, Monitoring, Policy Service, pxGrid

✓ Ta click vào Cisco-ISE-2 → tick vào box PxGrid và click Save.

Hostname **Cisco-ISE-2**
FQDN **Cisco-ISE-2.CiscoISE**
IP Address **10.215.26.49**
Node Type **Identity Services Engine (ISE)**

Role **STANDALONE**

Make Primary

Administration

Monitoring

Role

PRIMARY

Other Monitoring Node

Policy Service

Enable Session Services ⓘ

Include Node in Node Group

None ⓘ

Enable Profiling Service ⓘ

Enable Threat Centric NAC Service ⓘ

Enable SXP Service ⓘ

Use Interface

GigabitEthernet 0

Enable Device Admin Service ⓘ

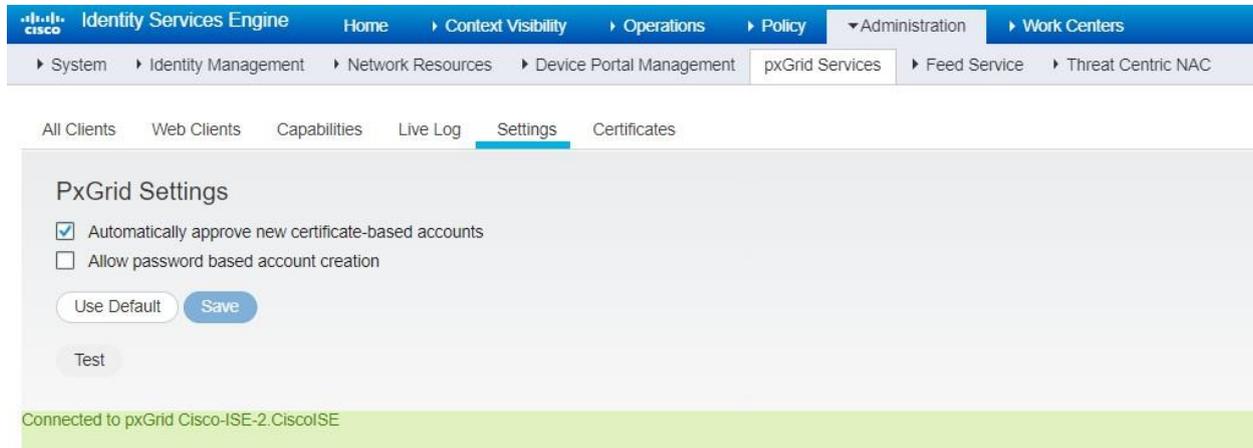
Enable Passive Identity Service ⓘ

pxGrid ⓘ

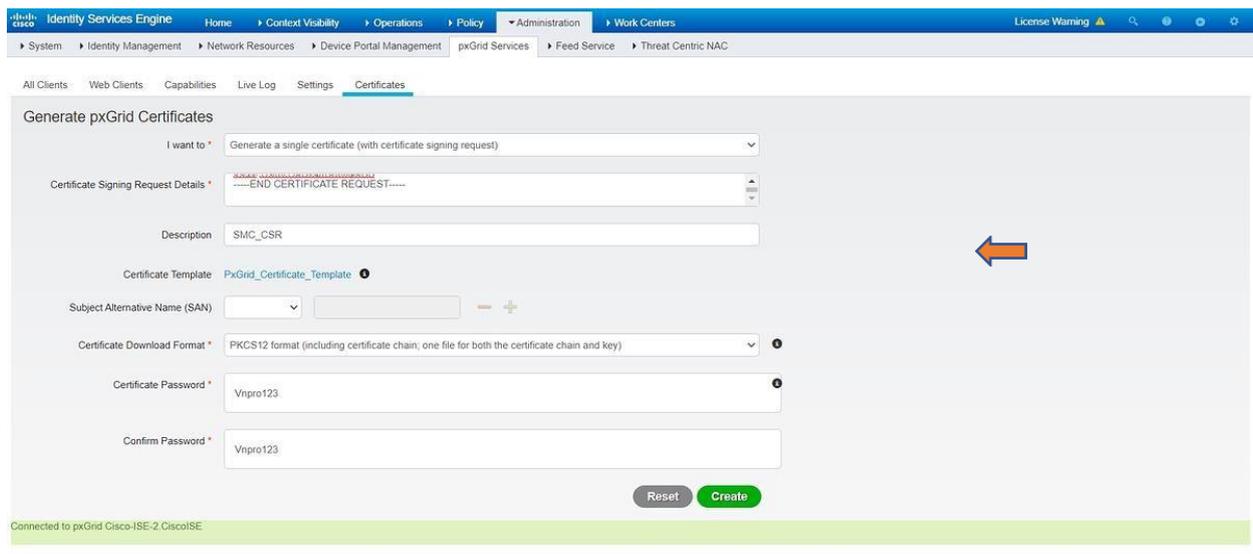
Save

Reset

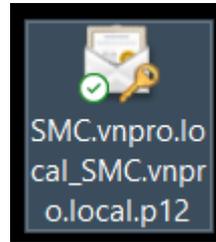
2.3: Tiếp theo ta tiến hành vào Administration/ PxGrid Services/ Settings và tick vào box Automatically approve new certificate-based accounts/ Save.



2.4: Sau đó tiến hành tạo Certificate: di chuyển đến Administration / PxGrid Services / Certificates.(Ta tiến hành điền vào mẫu như bên dưới sau đó click Create). Với thông tin trong mục Certificate Signing Request Details là nội dung của file .csr vừa download ở bước trên.



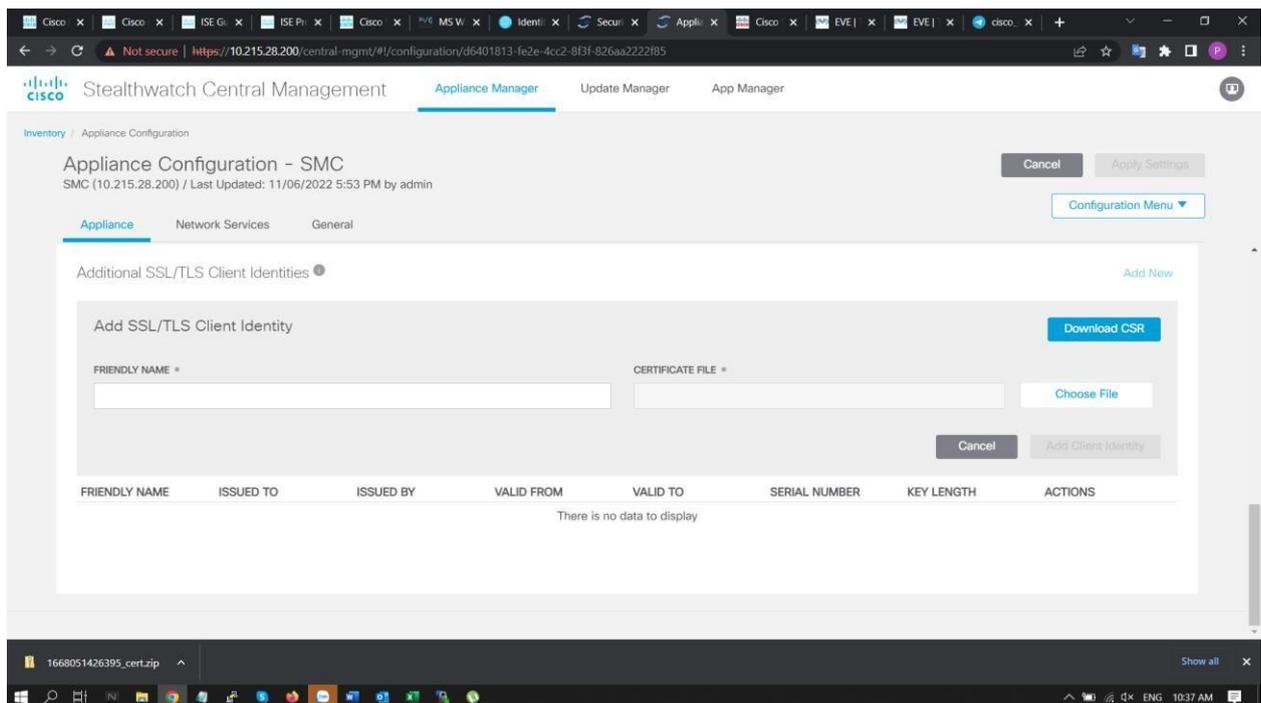
- ✓ Sau khi click Create ta lập tức được file dạng .zip, giải nén file .zip được 1 file dạng .p12

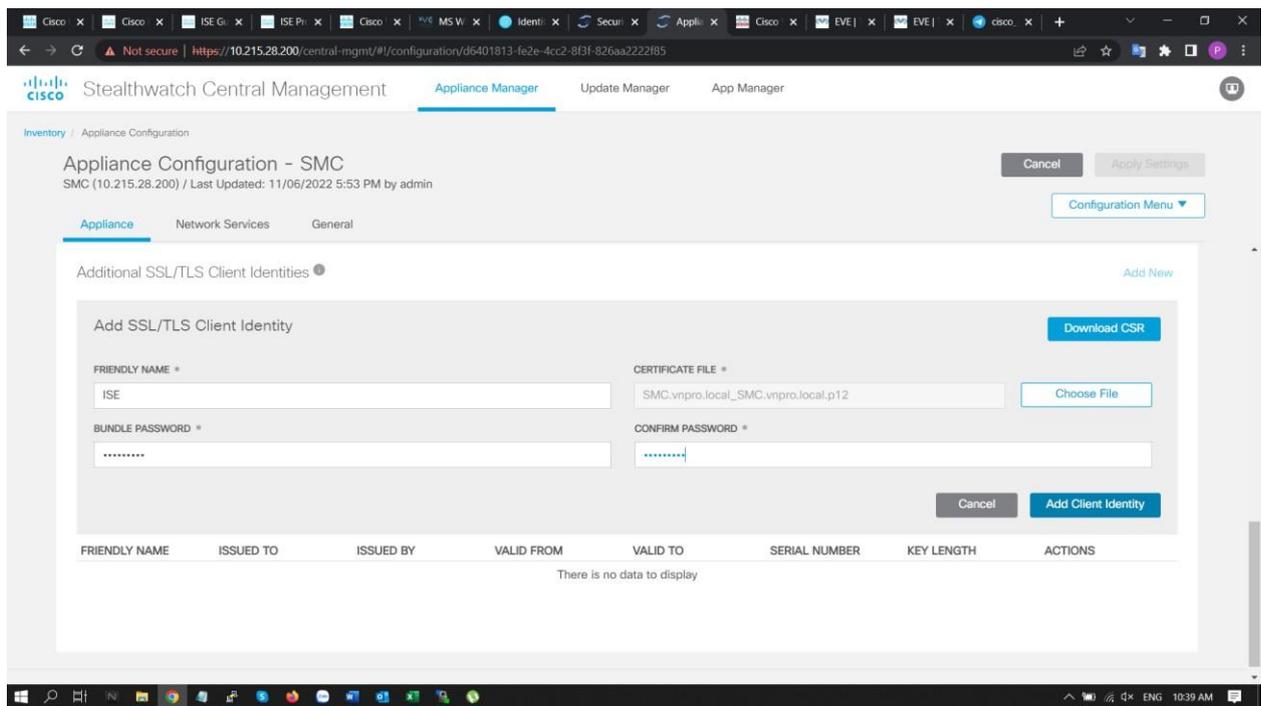
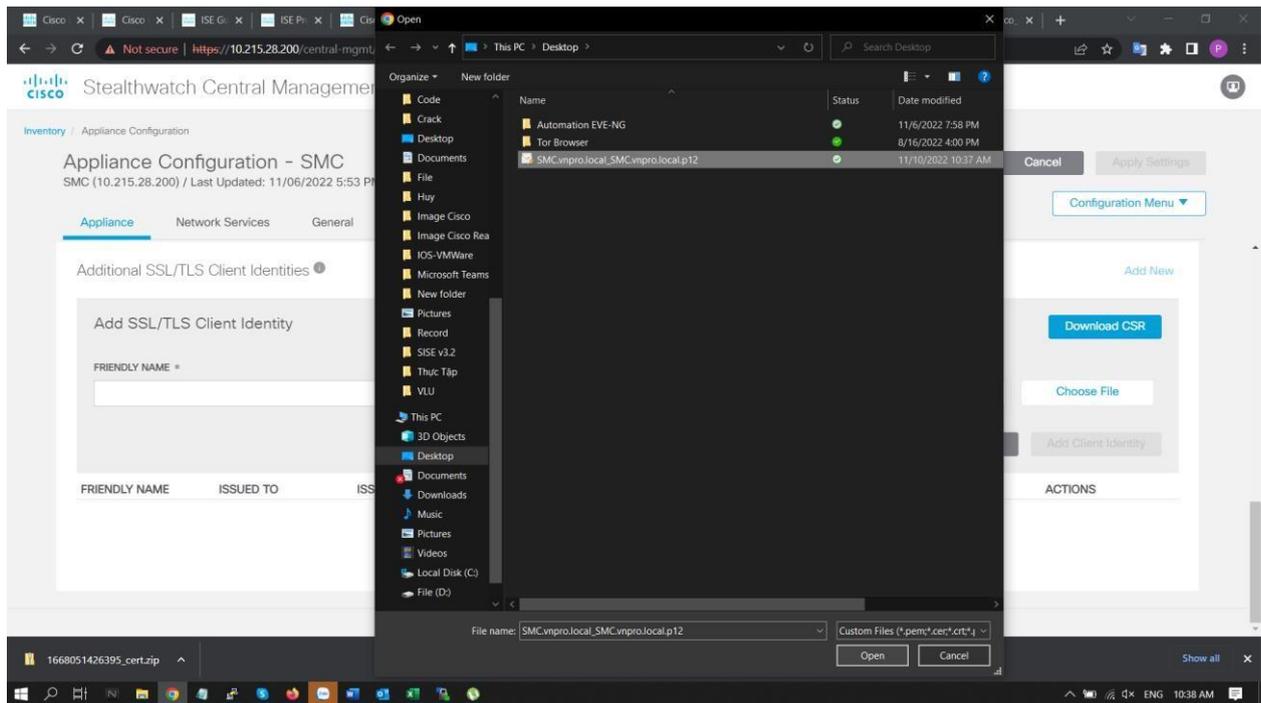


- ✓ Sau khi ta có được Certificate Request từ Cisco ISE thì lúc này ta tiến hành đưa file .p12 trên vào Stealthwatch để Stealthwatch có thể thêm Cisco ISE vào SSL/TLS Client Identities của mình

Bước 3:

3.1: Quay trở lại màn hình của bước 1.7 ta tiến hành chọn Choose File, sau đó chọn đường dẫn đến file mà ta đã giải nén có đuôi .p12 đã giải nén ở bước 2.4 vào, sau đó tiến hành điền password mà ta đã nhập ở bước 2.4 và click Add Client Identity:





Add SSL/TLS Client Identity Download CSR

FRIENDLY NAME *

BUNDLE PASSWORD *

CERTIFICATE FILE * Choose File

CONFIRM PASSWORD *

Cancel Add Client Identity

3.2: Tiếp theo ta tiến hành click Apply Change và thu được kết quả như sau:

Additional SSL/TLS Client Identities Modified Add New

FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH	ACTIONS
ISE	VnPro	Certificate Services Endpoint Sub CA - ISE	2022-11-09 10:37:05	2024-11-09 10:37:05	14120e834a7b4111ab 5d6657d30b7842	2048 bits	Delete

[Revert](#)

FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH	ACTIONS
SelfSMC	selfSMC	Certificate Services Endpoint Sub CA - Cisco-ISE-2	2019-11-17 20:47:34	2021-11-17 20:15:34	29c3cbb353aa464808 aff5a496e4506	2048 bits	Delete

- ✓ Sau khi hoàn tất bước 3 lúc này ta vào lại Cisco ISE để có thể lấy Certificate có đuôi .pem, khi có file Cert từ Cisco ISE chúng ta có thể quay lại Trust Store của Stealthwatch và thêm Cisco ISE vào Trust Store của mình thông qua file .pem mà Cisco ISE đã cung cấp.

Bước 4:

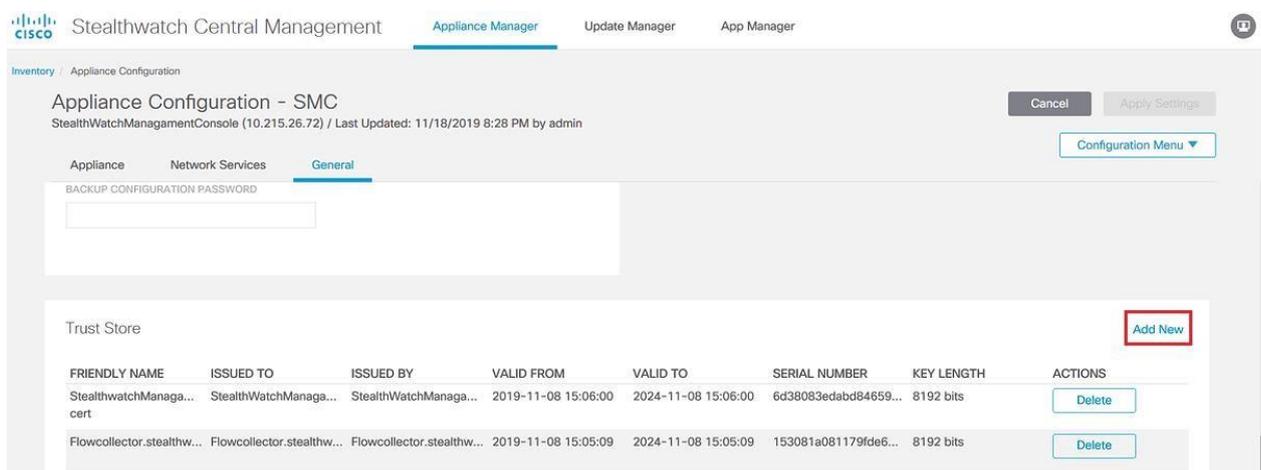
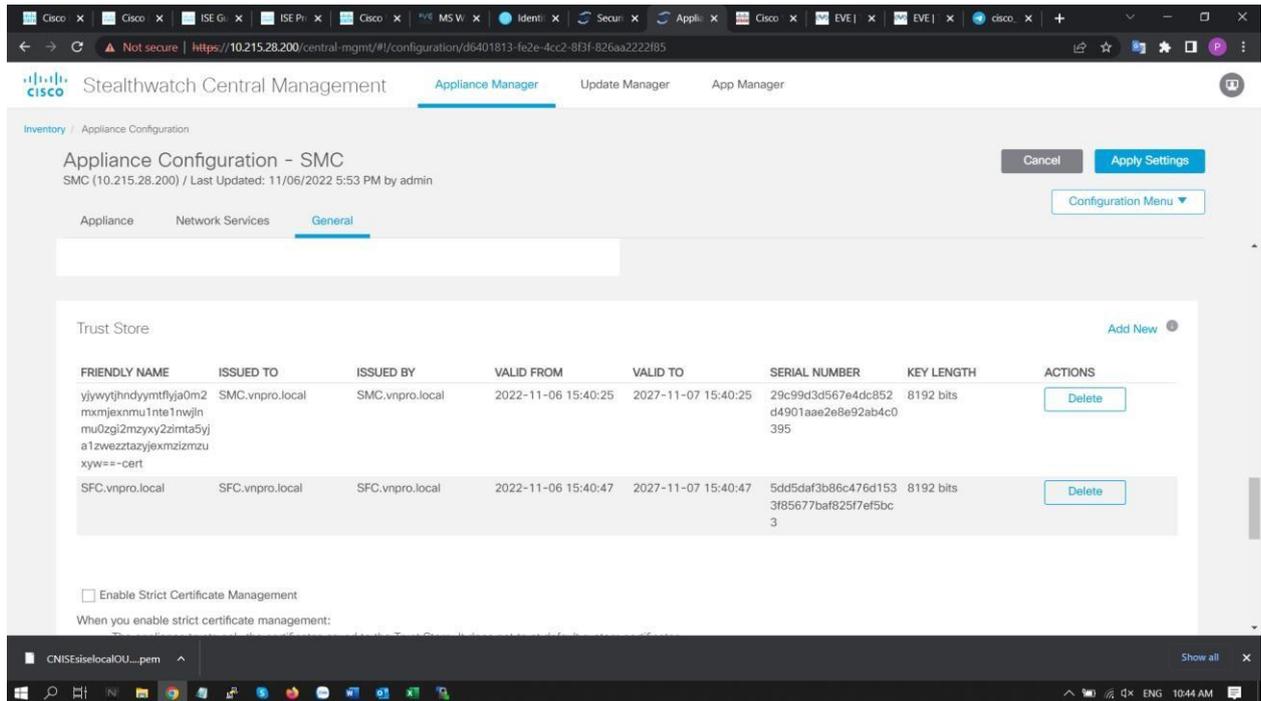
4.1: Tại giao diện Cisco ISE, ta di chuyển vào Administration > System > Certificates, chọn tiếp tục Certificate Authority và click Certificates Authority Certificates. Tại đây ta chọn Certificate Services Endpoint Sub CA - cisco-ISE và Click Export.

CA Certificates

	Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration Status
▼ cisco-ISE-6									
<input type="checkbox"/>	Certificate Services Root CA - cisco-ISE-6#00001	Enabled	Infrastructure,Endpoints	3D 90 E3 12 38 7E 4F 45 A7 37 9A D1 AC 03 B4 A4	Certificate Services Root CA - cisco-ISE-6	Certificate Services Root CA - cisco-ISE-6	Sun, 29 Nov 2020	Sat, 30 Nov 2030	✓
<input type="checkbox"/>	Certificate Services Node CA - cisco-ISE-6#00002	Enabled	Infrastructure,Endpoints	30 6A 45 8A 7C D7 4E 37 9B 87 2D 78 52 5C 36 F9	Certificate Services Node CA - cisco-ISE-6	Certificate Services Root CA - cisco-ISE-6	Sun, 29 Nov 2020	Sat, 30 Nov 2030	✓
<input checked="" type="checkbox"/>	Certificate Services Endpoint Sub CA - cisco-ISE-6#00003	Enabled	Infrastructure,Endpoints	4F 6C DF 6A 34 E3 4D A4 BE 16 30 EC C5 7F DA 4A	Certificate Services Endpoint Sub CA - cisco-ISE-6	Certificate Services Node CA - cisco-ISE-6	Sun, 29 Nov 2020	Sat, 30 Nov 2030	✓
<input type="checkbox"/>	Certificate Services OCSP Responder - cisco-ISE-6#00004	Enabled	Infrastructure,Endpoints	78 9C 72 77 BC B6 4D C8 A3 AB 8C 06 E5 6E D0 8A	Certificate Services OCSP Responder - cisco-ISE-6	Certificate Services Node CA - cisco-ISE-6	Sun, 29 Nov 2020	Sun, 30 Nov 2025	✓

- ✓ Sau khi click Export ta được popup để tải về 1 file .pem (Lưu ý trình duyệt web cho phép bật popup để tải file)

4.2: Tại Appliance Configuration – SMC ta chuyển sang tab General như hình bên dưới và click Add New tại mục Trust Store:



4.3: Ta điền Friendly Name sau đó click Choose File để chọn file mà ta đã Export ở bước 4.1.

Add Certification Authority Certificate

FRIENDLY NAME *
CiscoSE

CERTIFICATE FILE *
Defaultselfsignedservercert.pem

Choose File

4.4: Click Apply Changes, sau đó chờ quá trình thiết đặt cấu hình hoàn thành.

Stealthwatch Central Management

Appliance Configuration - SMC
SMC (10.215.28.200) / Last Updated: 11/06/2022 5:53 PM by admin

Cancel Apply Settings

Configuration Menu

Trust Store Modified

FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH	ACTIONS
yjwyfjhdymtftfja0m2 mxxjexnmu1nte1nwjln mu0zgi2mzyxy2zmta5yj a1zwezttazyjexmzizmzu xyw==cert	SMC.vnpro.local	SMC.vnpro.local	2022-11-06 15:40:25	2027-11-07 15:40:25	29c99d3d567e4dc852 d4901aae2e8e92ab4c0 395	8192 bits	Delete
SFC.vnpro.local	SFC.vnpro.local	SFC.vnpro.local	2022-11-06 15:40:47	2027-11-07 15:40:47	5dd5daf3b86c476d153 3f85677ba8257ef5bc 3	8192 bits	Delete
ISE	ISE.sise.local	Certificate Services	2022-11-07 18:43:13	2027-11-08 18:43:13	247ea9d2323541e6a94 -----	4096 bits	Delete

Enable Strict Certificate Management

When you enable strict certificate management:

- The appliance trusts only the certificates saved to the Trust Store. It does not trust default system certificates.
- The SMC Desktop Client trusts only certificates saved on your local computer.

Apply Configuration Changes to Appliance

While the system applies changes, you cannot make any additional modifications. If a reboot is required, the appliance will go offline until the process has finished.

The following configurations have changed:

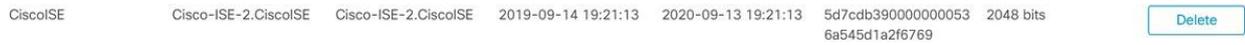
Appliance:

- Additional SSL/TLS Client Identities

General:

Cancel Apply Changes

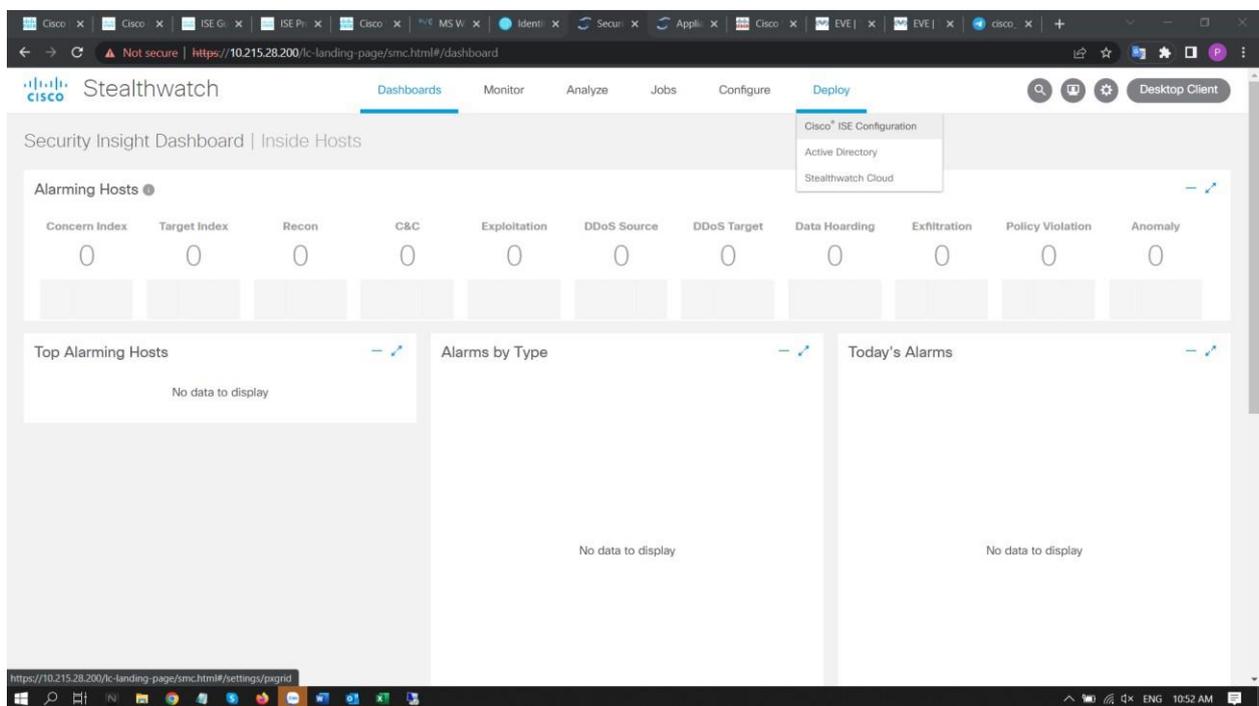
- ✓ Sau khi hoàn tất bước 4.4 thì tại tab General của Stealwatch Central Management ở mục Trust Store sẽ thấy Cisco ISE đã được thêm vào:

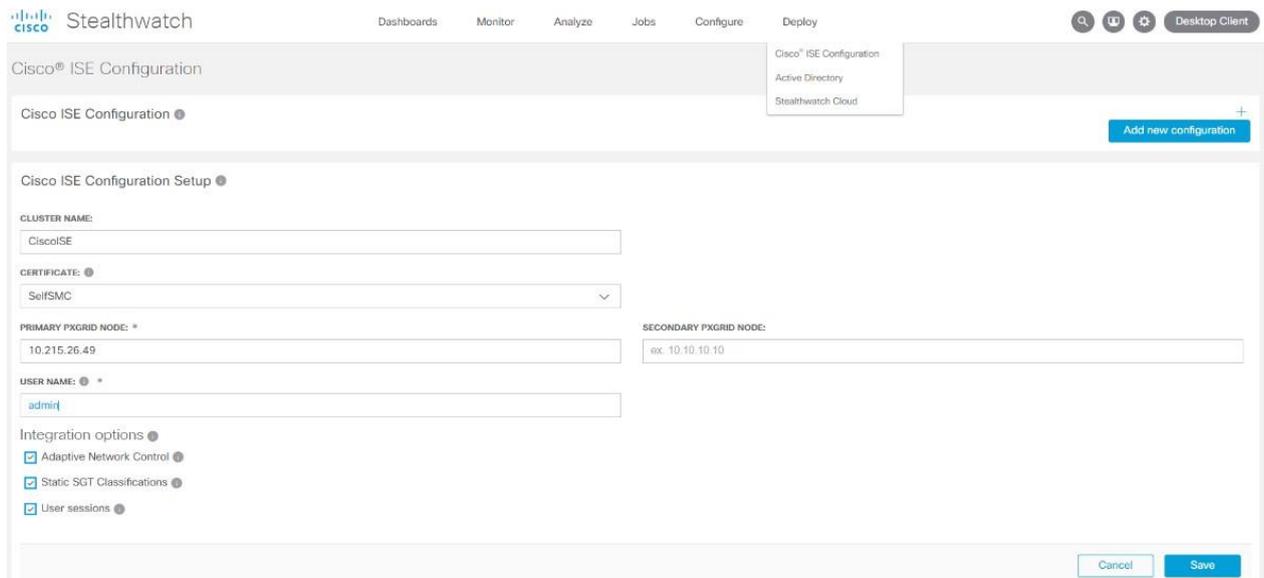


- ✓ Sau khi đã hoàn tất bước 4 chúng ta tiến hành Cisco ISE Configuration vào Stealwatch SMC.

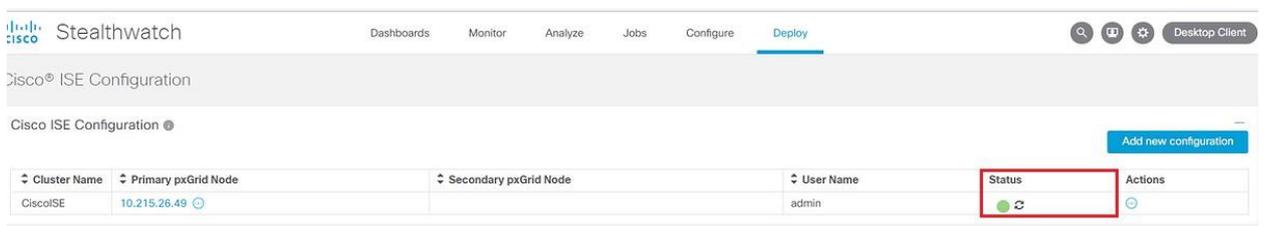
Bước 5:

5.1 : Ta quay trở lại giao diện của Stealwatch Management Console: Chọn Deploy → Cisco ISE configuration → click Add new configuration, Ta điền thông tin name, chọn Certificate, điền IP của Cisco ISE, điền username và click Save.

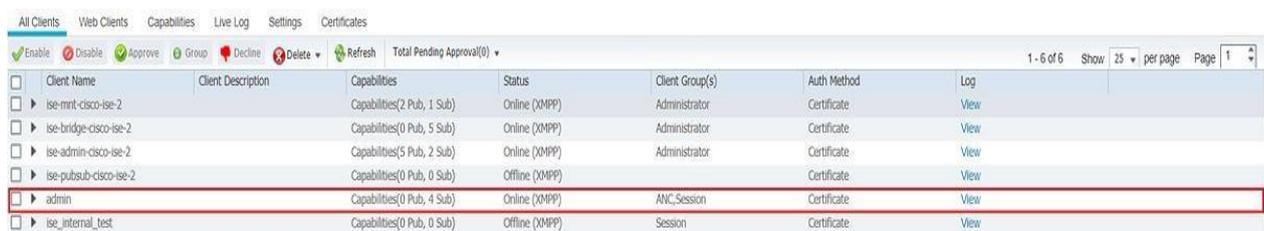




- ✓ Ta chờ quá trình thiết đặt hoàn tất. sau khi hoàn tất bước 5.1 trên SMC ta vào Deploy → Cisco ISE Configuration sẽ thấy được trạng thái tại tab Status thì Active như sau:



5.2: Trên Cisco ISE ta vào Administration → PxGrid Services để kiểm tra xem Cisco ISE đã có thể giao tiếp với Stealthwatch qua giao thức PxGrid hay chưa.



- ✓ Ta đã thấy được Client name “admin” mà chúng ta đã tạo tại bước 5.1 trên stealthwatch SMC.
- ✓ Sau khi hoàn thành bước 5.2 thì chúng ta đã có thể thấy được rằng lúc này cả Cisco ISE và Stealthwatch đều có thể thấy nhau thông qua giao thức PxGrid.

Tiếp theo, 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.

- ✓ Đầu tiên trên các cổng của switch cấu hình đưa về mode access và đặt ip cho interface vlan 1

```
SW1(config)#int range g0/0-2  
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 bri
```

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 bri

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	

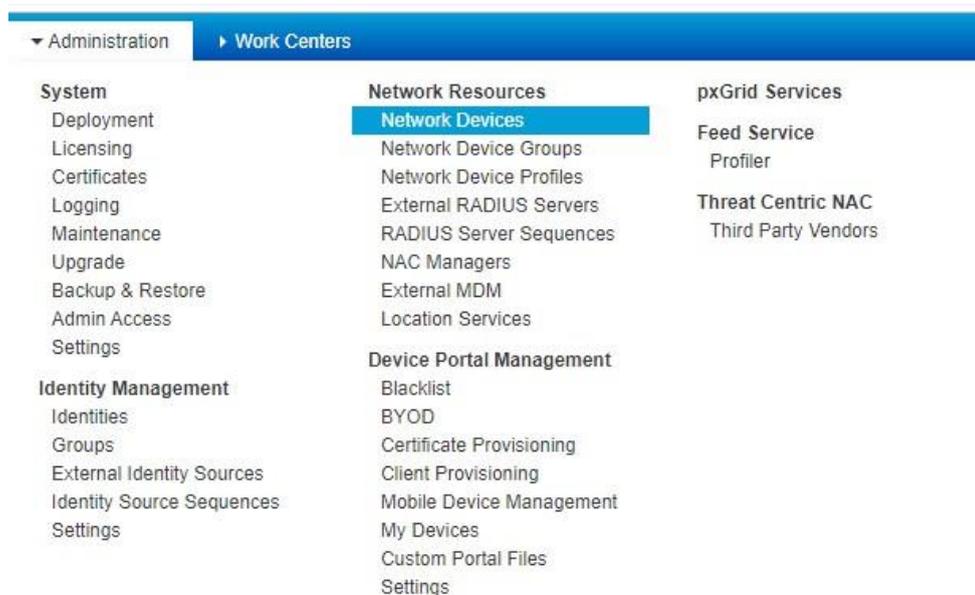
```
SW1(config)#aaa new-model
SW1(config)#aaa authentication dot1x default group radius
SW1(config)#dot1x system-auth-control
SW1(config)#int g0/1
SW1(config-if)#dot1x port-control auto
SW1(config-if)#dot1x pae authenticator
SW1(config-if)# authentication host-mode multi-auth
SW1(config)#radius-server 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 g0/0  
  
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 chúng thực.
- ✓ Chúng ta tiến hành thực hiện cấu hình cisco theo dãy hình bên dưới.



- ✓ Chuyển hướng đến Administration / Network Resources / Network Devices
- ✓ Name: SW1
- ✓ IP: 10.215.26.85/32
- ✓ Click vào RADIUS: và điền share secret

* Name
Description
IP Address /

ⓘ 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

General Settings

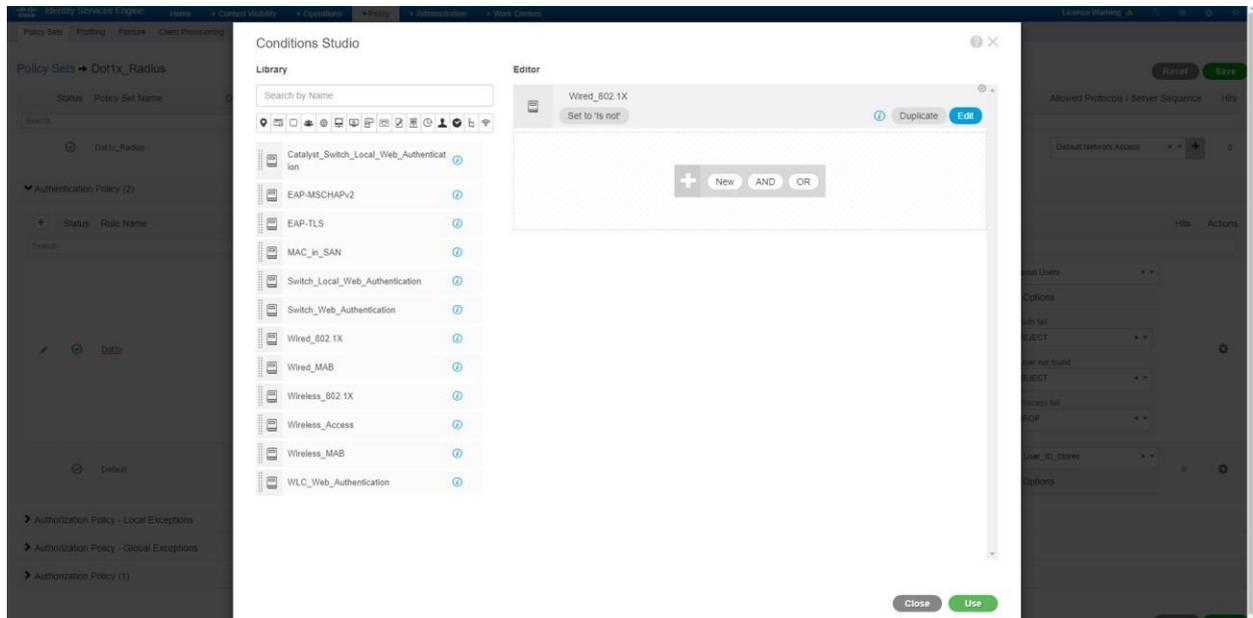
Enable KeyWrap ⓘ
* Key Encryption Key
* Message Authenticator Code Key
Key Input Format ASCII HEXADECIMAL

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

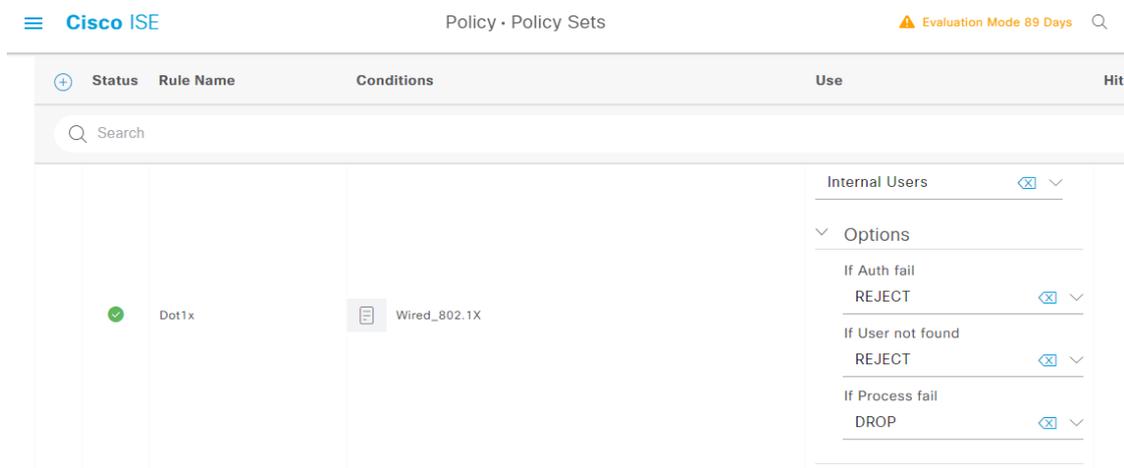




Trong mục **Authentication Policy** → Tick chọn dấu “+” để add policy → Trong mục **Condition** kéo thả mục **wired_802.1X** từ bên trái qua bên phải như ảnh dưới đây → Chọn **Use**.



✓ 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.

Authorization Policy (1)

			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
<input checked="" type="checkbox"/>	Dot1x	Wired_802.1X	PermitAccess x	Select from list		
<input checked="" type="checkbox"/>	Default		DenyAccess x	Select from list	0	

ps://10.215.28.20/admin/#collapse3-authorization

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.

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: Internal Users

Password: Re-Enter Password:

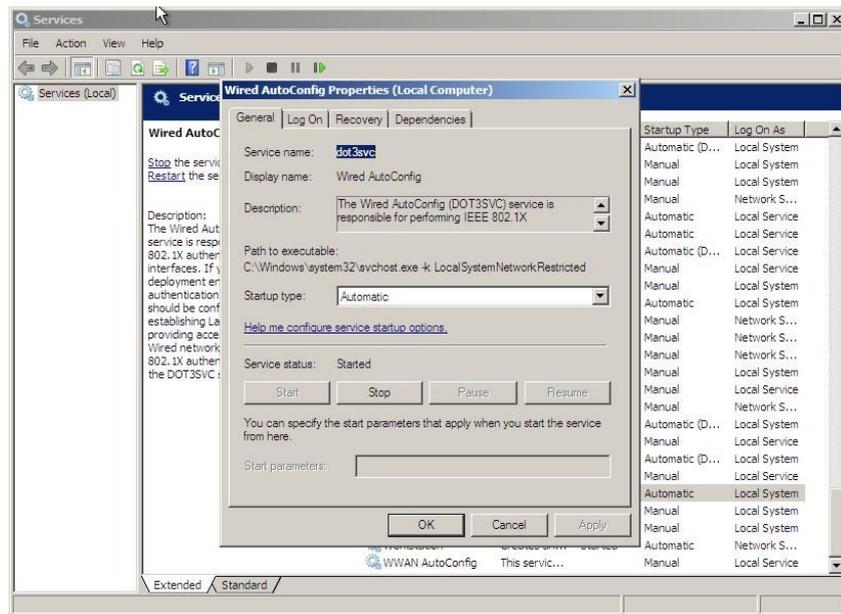
Enable Password:

User Information

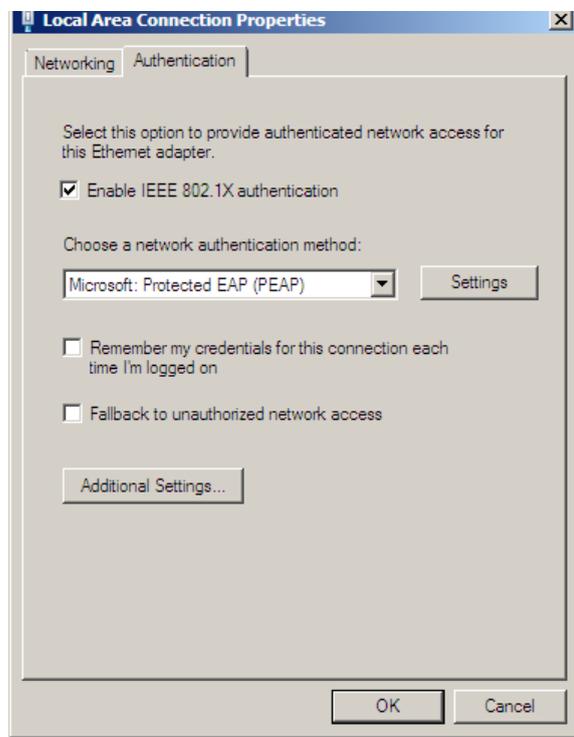
First Name:

Last Name:

- ✓ 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.

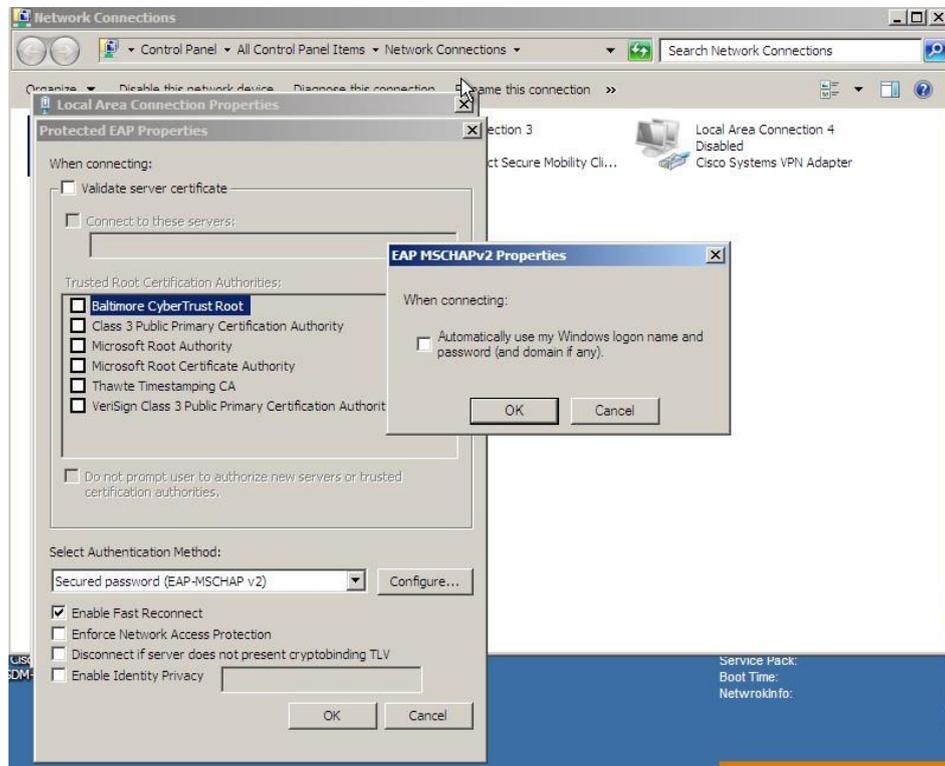


- ✓ Chuyển sang điều chỉnh card mạng, Chuột phải vào card mạng đang chạy → Properties → Trong tab Authentication tick chọn như ảnh dưới đây.

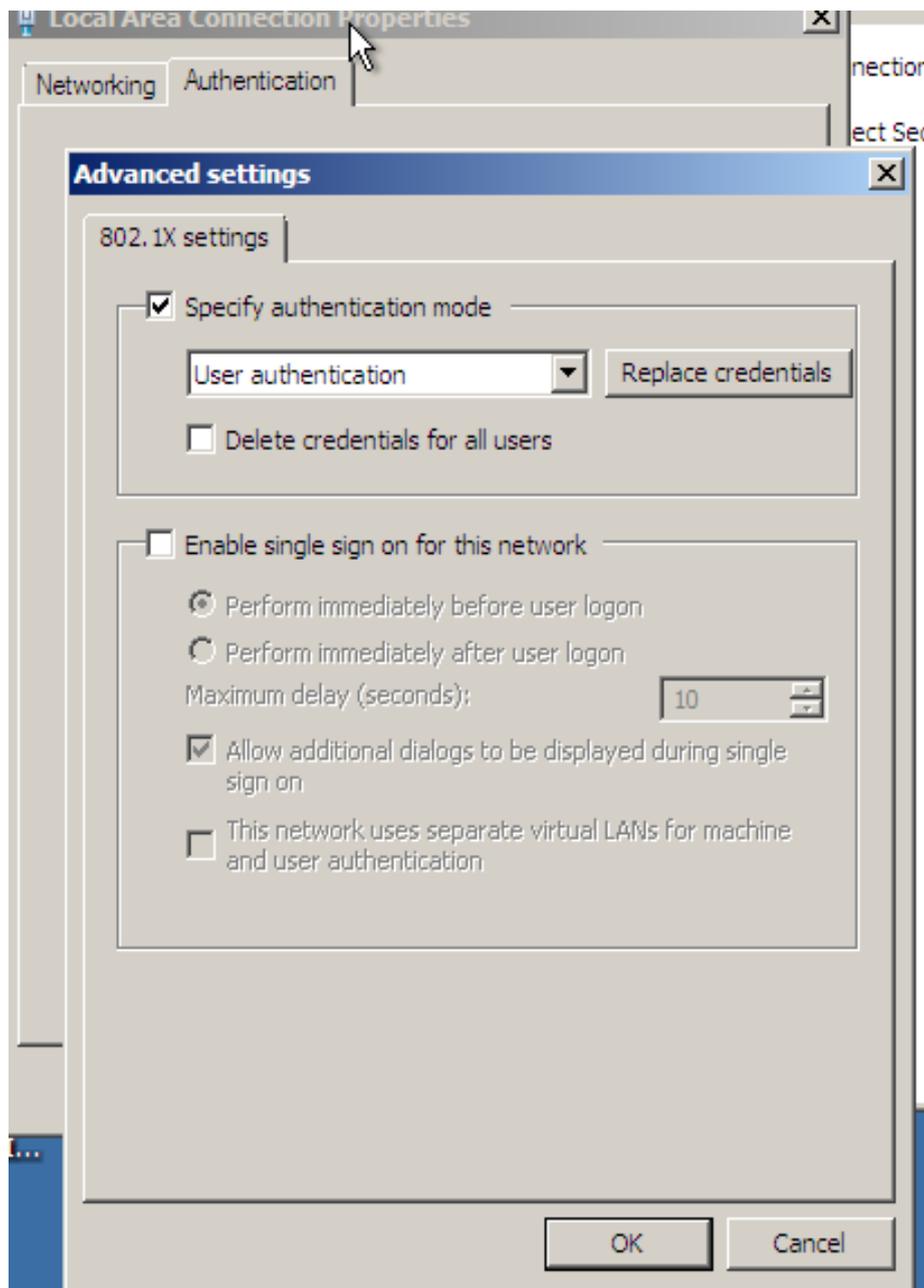


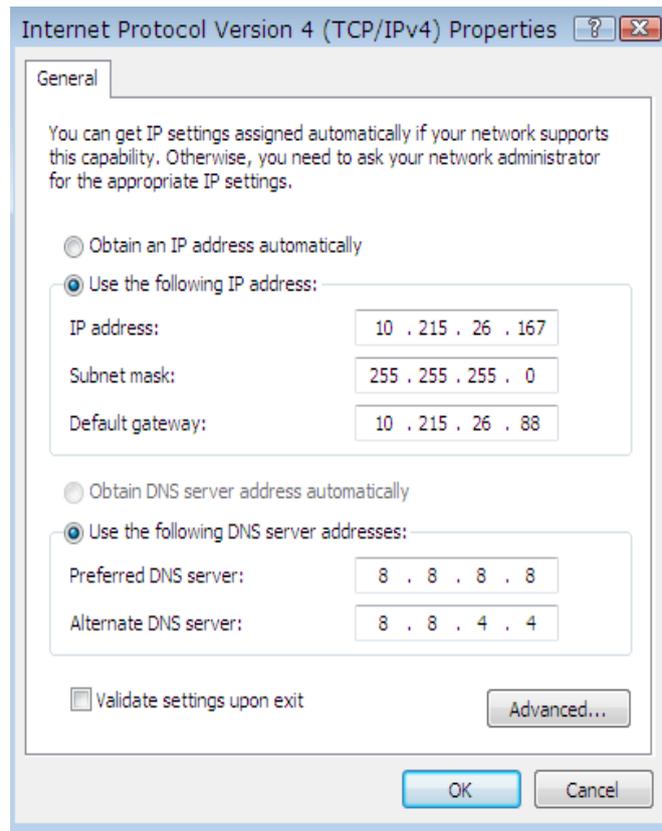
- ✓ Trong tab Choose a network authentication method Chọn Settings → Bỏ tick Validate server certificate (trong môi trường lab, chúng ta không cần windows xác thực chứng chỉ của Cisco ISE) → Trong mục Select Authentication Method Chọn Configure... → Bỏ tick Automatically use my Windows logon

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.

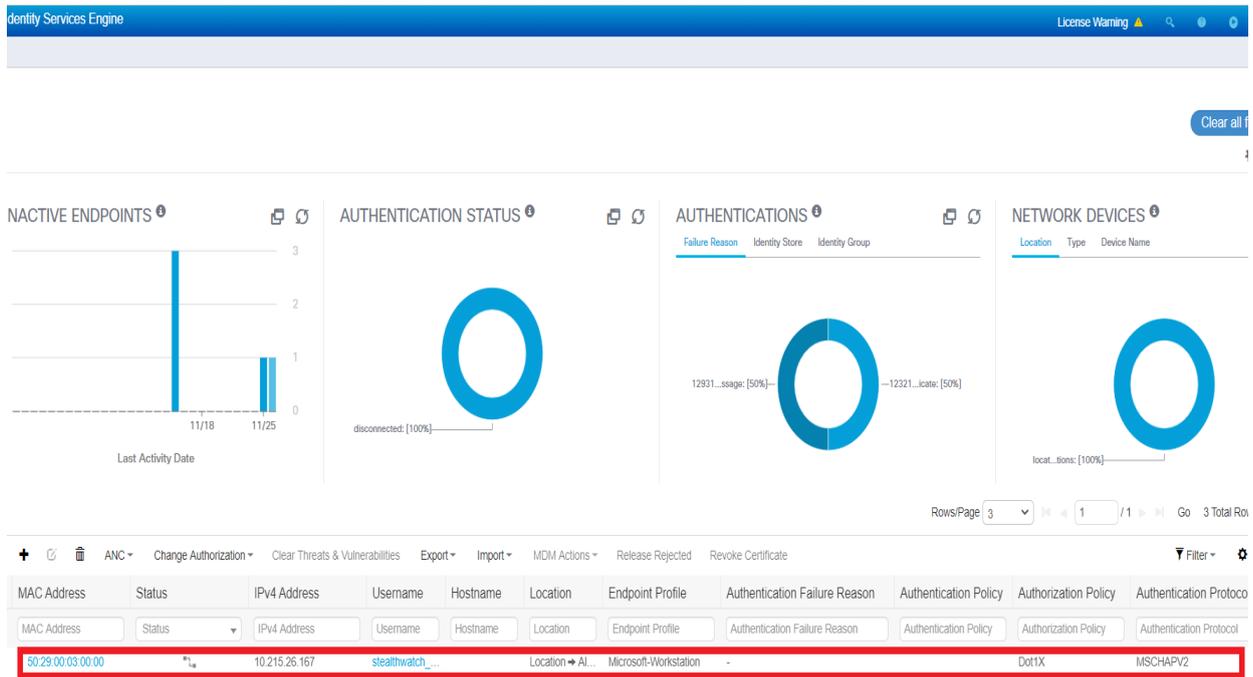




```
C:\Administrator: C:\Windows\system32\cmd.exe
WINS Proxy Enabled. . . . . : No
Ethernet adapter Local Area Connection:

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.



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 giây. 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 g0/0  
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 g0/0-2
```

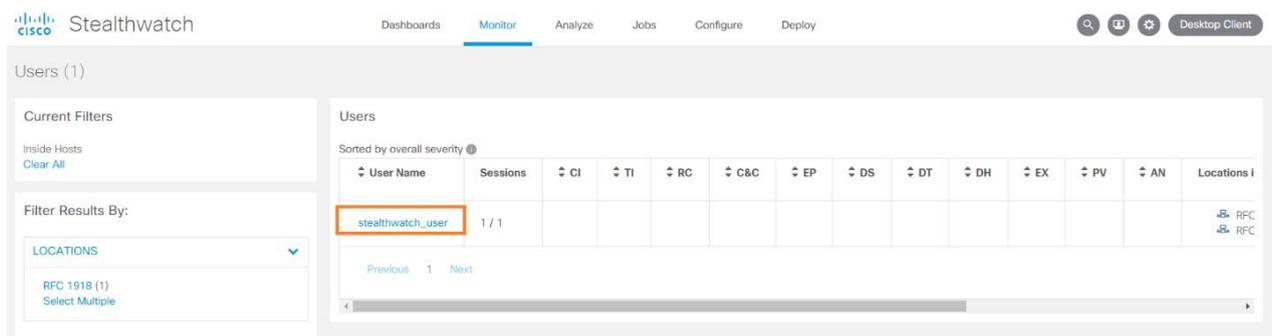
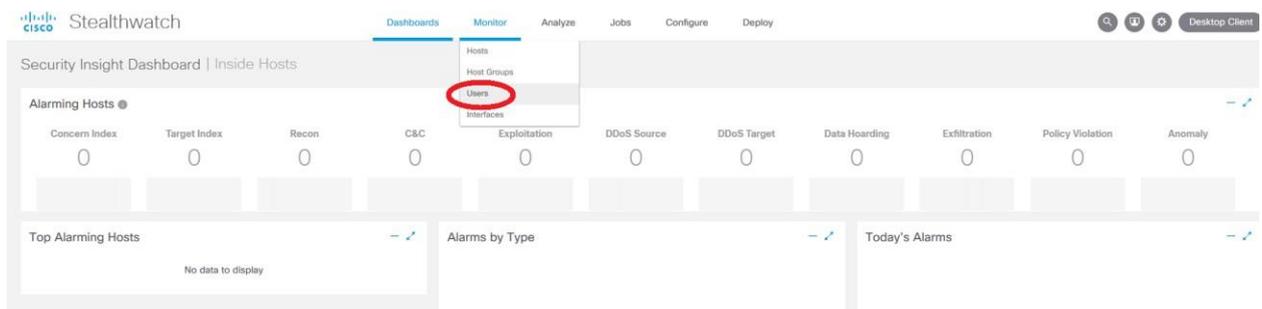
```
SW1(config-if-range)# ip flow ingress
```

```
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 Stealth Watch-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.

The screenshot shows the Cisco Stealthwatch 'Users' page. On the left, there are filters for 'Current Filters' (Inside Hosts, Clear All) and 'Filter Results By' (LOCATIONS, RFC 1918 (3)). The main area displays a table of users with columns for User Name, Severity, and various alarm categories (EP, DS, DT, DH, EX, PV, AN). A tooltip for 'Severity Sorting' explains that the list is sorted by alarm category severity. The table lists three users: stealthwatch_user, stealthwatch_user2, and khoinguyen, each with a severity of 1/1 and associated with RFC 1918 locations.

The screenshot shows the 'Host Summary' page for IP 10.215.26.170. It includes a 'Host Summary' section with details like Hostname, Host Groups (Catch All), Location (RFC 1918), and MAC Address (50:29:00:03:00:01). A 'Traffic by Peer Host Group (last 12 hours)' chart shows a flow between 'Multicast' and 'United Sta...'. A 'Users & Sessions' table at the bottom shows a session for user 'khoinguyen' starting at 11/26/19 5:47 PM, which is circled in red. The 'Application Traffic' section shows no 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

