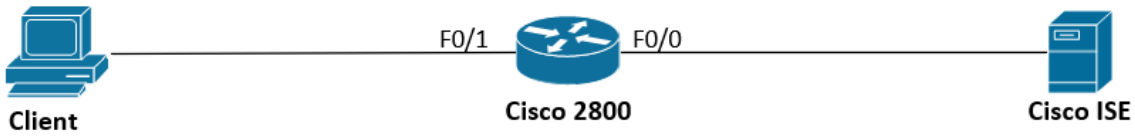
# Authentication, Authorization, Accounting

# LAB – Xác thực và phân quyền login bằng giao thức TACAS+ sử dụng Cisco ISE

## I. Sơ đồ:




*Hình 1: Sơ đồ bài lab.*

Ta có bảng thông tin như sau:

| Tên thiết bị | Interface | IP/Netmask | Gateway |
|---|---|---|---|
| Cisco ISE | NIC | 10.215.26.49 | - |
| Router | F0/0 | DHCP | - |
| | F0/1 | 192.168.99.1/24 | - |
| Client | NIC | 192.168.99.99/24 | 192.168.99.1 |

## II. Yêu cầu:

### 1. Cấu hình ban đầu

- Thực hiện cấu hình IP cho PC, Router, thực hiện NAT sao cho PC có thể ping thấy ISE server.

### 2. Cấu hình TACACS+:

- Tiến hành xác thực và phân quyền privilege cho các user truy cập telnet đến Router như sau (việc xác thực/phân quyền phải do Cisco ISE kiểm soát):
  - Username: ***guest***, password ***VnPro@123***, privilege 7
  - Username: ***adminvnpro***, password ***VnPro@123***, privilege 15
- Cấu hình xác thực local với privilege cho các user như trên để khi hoạt động xác thực với Cisco ISE không thành công, chuyển sang phương thức xác thực/phân quyền local.

## III. Hướng dẫn:

**Cấu hình cho Router**

```
Router(config)#int f0/0
Router(config-if)#ip address dhcp
Router(config-if)#no shutdown

Router(config)#int f0/1
Router(config-if)#ip address 192.168.99.1 255.255.255.0
Router(config-if)#no shutdown
```

**Cấu hình NAT cho Router:**

```
Router(config)#access-list 1 permit 192.168.99.0 0.0.0.255
Router(config)#ip nat inside source list 1 interface f0/0 overload
Router(config)#int f0/0
Router(config-if)#ip nat outside
Router(config)#int f0/1
Router(config)#ip nat inside
```

Kết nối PC với Router, đặt IP và Gateway. Kiểm tra kết nối tới ISE Server:

```
C:\Users\hoang>ping 10.215.26.49

Pinging 10.215.26.49 with 32 bytes of data:
Reply from 10.215.26.49: bytes=32 time=2ms TTL=61
Reply from 10.215.26.49: bytes=32 time=2ms TTL=61
Reply from 10.215.26.49: bytes=32 time=1ms TTL=61
Reply from 10.215.26.49: bytes=32 time=2ms TTL=61
```

**Chỉ định TACACS+ Server cho Router:**

```
Router(config)#tacacs-server host 10.215.26.49
Router(config)#tacacs-server key 123abc
```

**Cấu hình Router xác thực với ISE bằng giao thức TACACS+:**

Trên Router, ta dùng các lệnh sau:

```
Router(config)#aaa new-model
Router(config)#aaa group server tacacs+ ISESRV
Router(config-sg-tacacs+)#server 10.215.26.49
Router(config-sg-tacacs+)#exit

Router(config)#aaa authentication login VTY group ISESRV local
Router(config)#aaa authorization console
Router(config)#aaa authorization exec CON none
Router(config)#aaa authorization exec VTY group ISESRV local if-authenticated
```

```
Router(config)#aaa accounting exec default
Router(cfg-acct-mlist)#action-type start-stop
Router(cfg-acct-mlist)#group ISESRV
Router(cfg-acct-mlist)#exit

Router(config)#aaa accounting commands 1 default
Router(cfg-acct-mlist)#action-type start-stop
Router(cfg-acct-mlist)#group ISESRV
Router(cfg-acct-mlist)#exit

Router(config)#aaa accounting commands 15 default
Router(cfg-acct-mlist)#action-type start-stop
Router(cfg-acct-mlist)#group ISESRV
Router(cfg-acct-mlist)#exit

Router(config)#aaa accounting network default
Router(cfg-acct-mlist)#action-type start-stop
Router(cfg-acct-mlist)#group ISESRV
Router(cfg-acct-mlist)#exit

Router(config)#aaa accounting connection default
Router(cfg-acct-mlist)#action-type start-stop
Router(cfg-acct-mlist)#group ISESRV
Router(cfg-acct-mlist)#exit

Router(config)#aaa accounting system default
Router(cfg-acct-mlist)#action-type start-stop
Router(cfg-acct-mlist)#group ISESRV
```

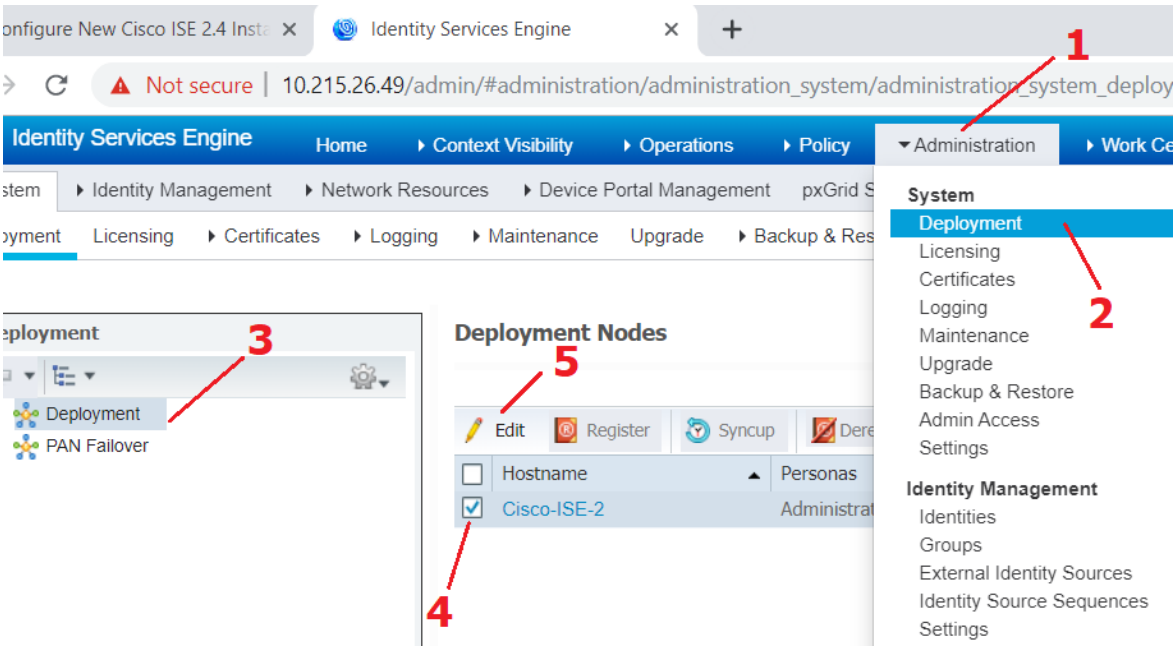
**Cấu hình telnet cho Router:**

```
Router(config)#line vty 0 4
Router(config-line)#login authentication VTY
Router(config-line)#authorization exec VTY
Router(config-line)#exit
```

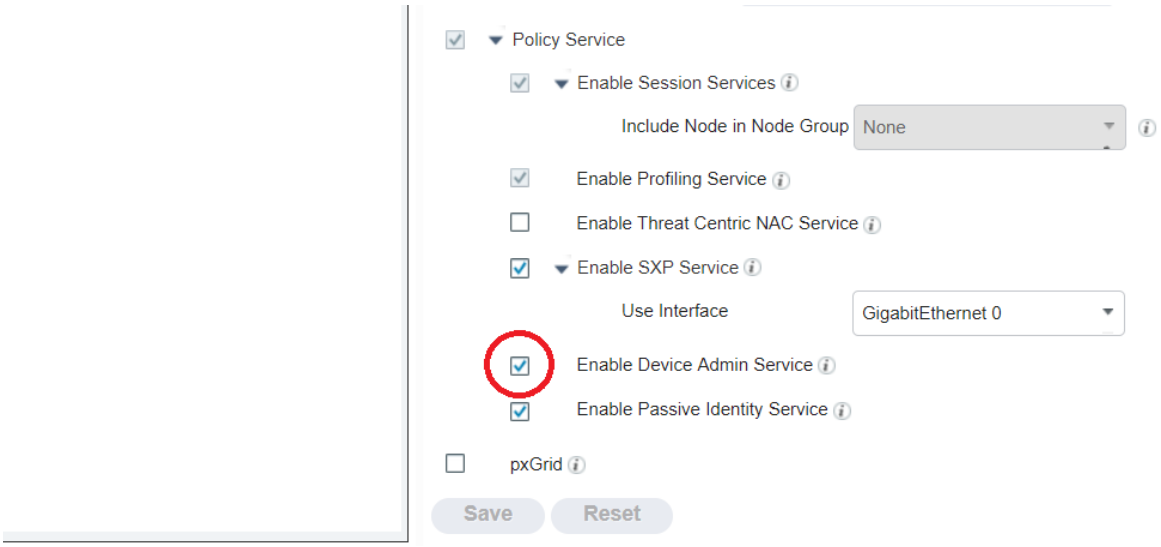
**Bật tính năng TACACS+ trên ISE:**

Đầu tiên, ta mở trình duyệt và truy cập vào IP 10.215.26.49 (IP của ISE Server). Đăng nhập bằng username và password được cung cấp.

Vào **Administration → Deployment →** Tích chọn hostname của Cisco ISE **→ Edit**:



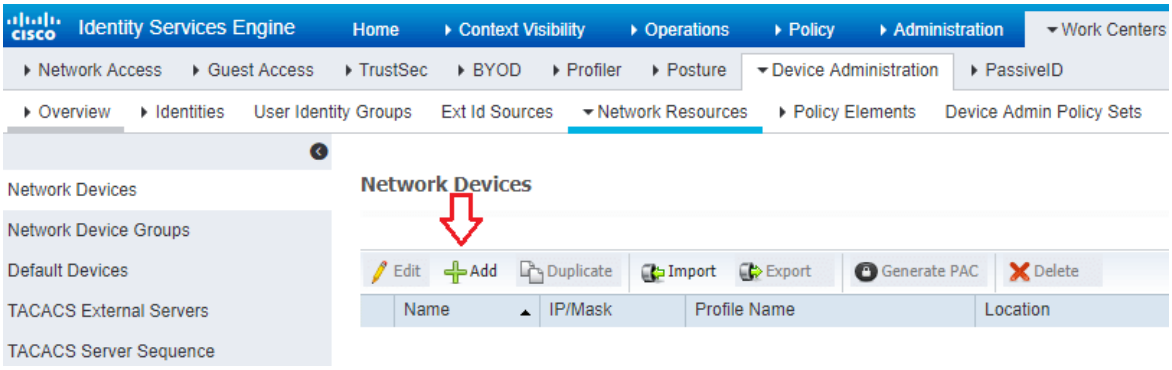

Ở phần Policy Service, chọn **Enable Device Admin Service** và Save lại:

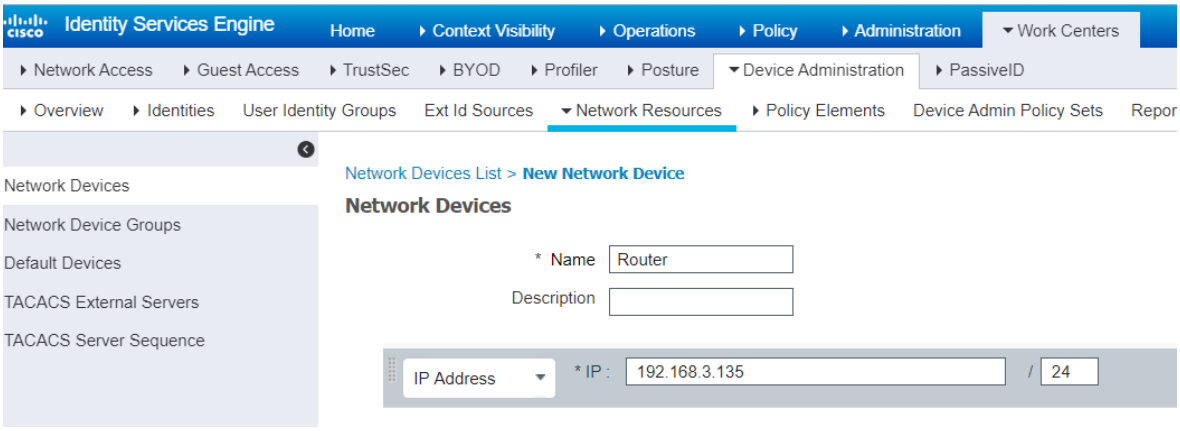



## Thêm Router vào ISE:

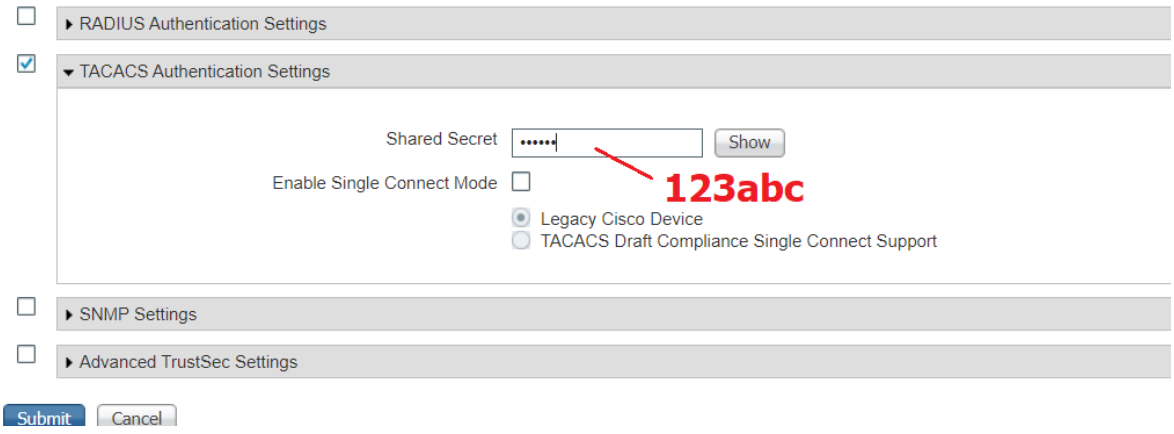
Vào **Work Centers → Device Administration → Network Resources → Network Devices → Add:**

Nhập tên, và IP của Router ta muốn thêm:



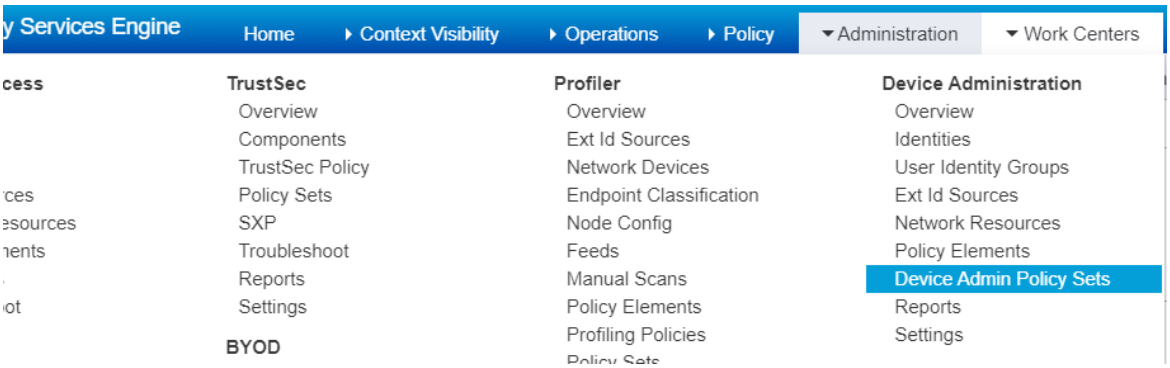

Ở phần **TACACS Authentication** Settings ta chỉ định chuỗi "**Shared Secret**" để Router và ISE giao tiếp với nhau.



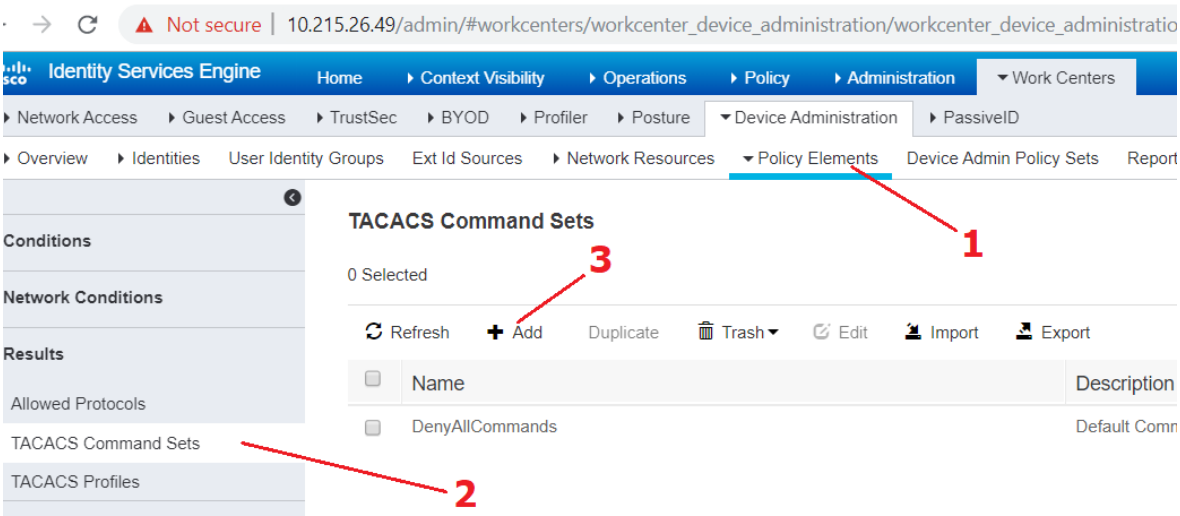

Sau đó bấm submit.

**<u>Cấu hình xác thực/phân quyền bằng TACACS+:</u>**

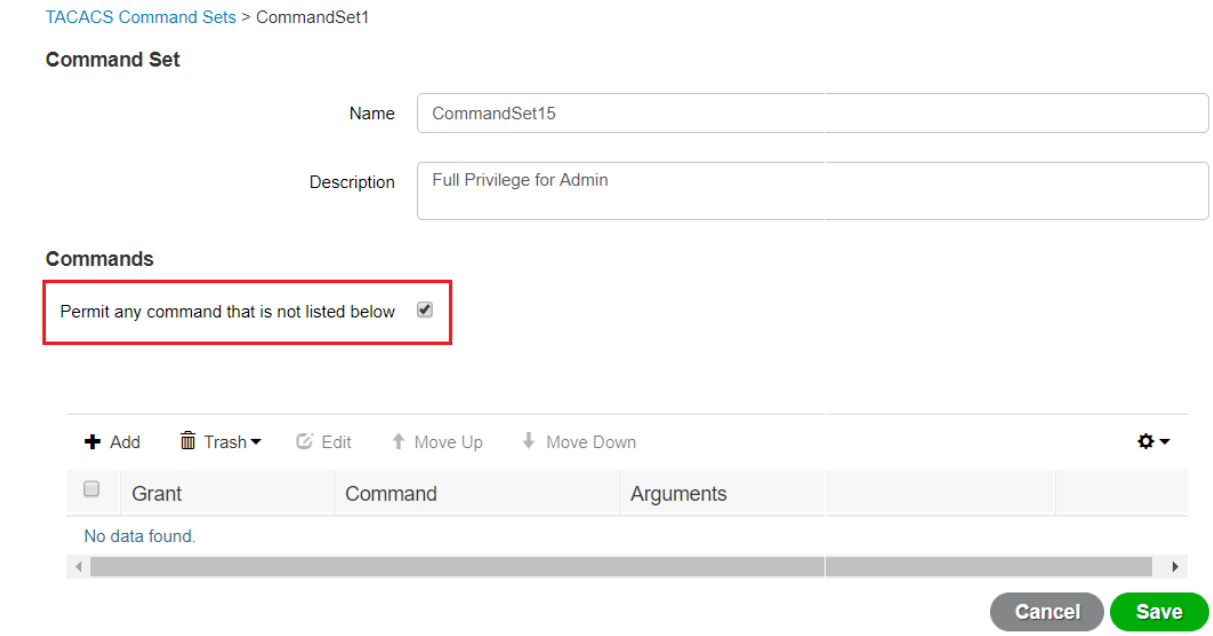
Vào **Work Center → Device Admin Policy Sets**:




Chọn **Policy Elements → Result → TACACS Command Sets → Add**:

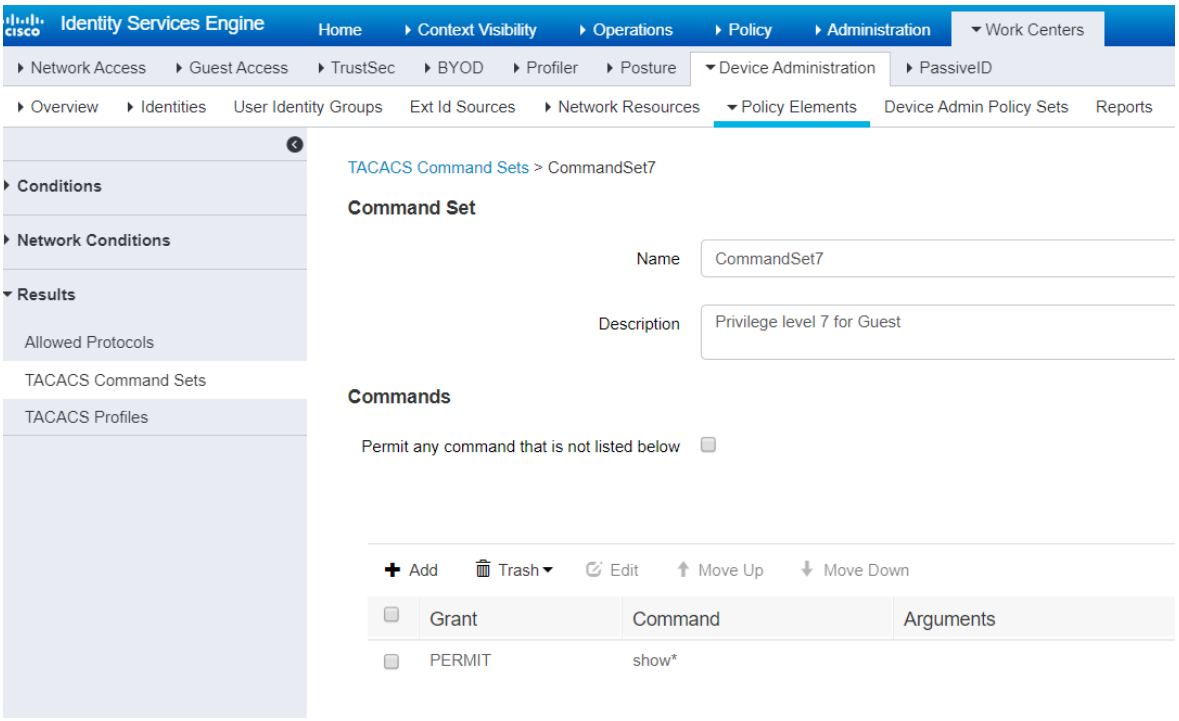



Tạo command set cho user ***adminvnpro*** có thể dùng đầy đủ các lệnh khi telnet:



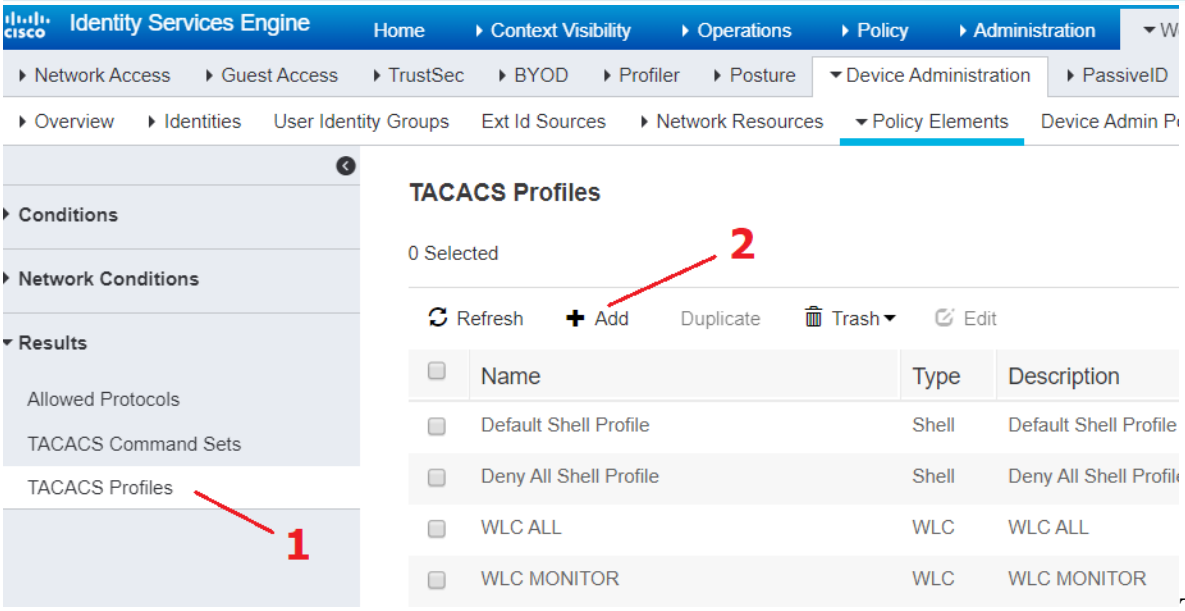
Tích chọn "**Permit any command that is not listed below**" và bấm Save.

Ta cũng tạo thêm command set cho user ***guest*** có privilege là 7, khi user này telnet vào router chỉ dùng được lệnh các lệnh *show*:

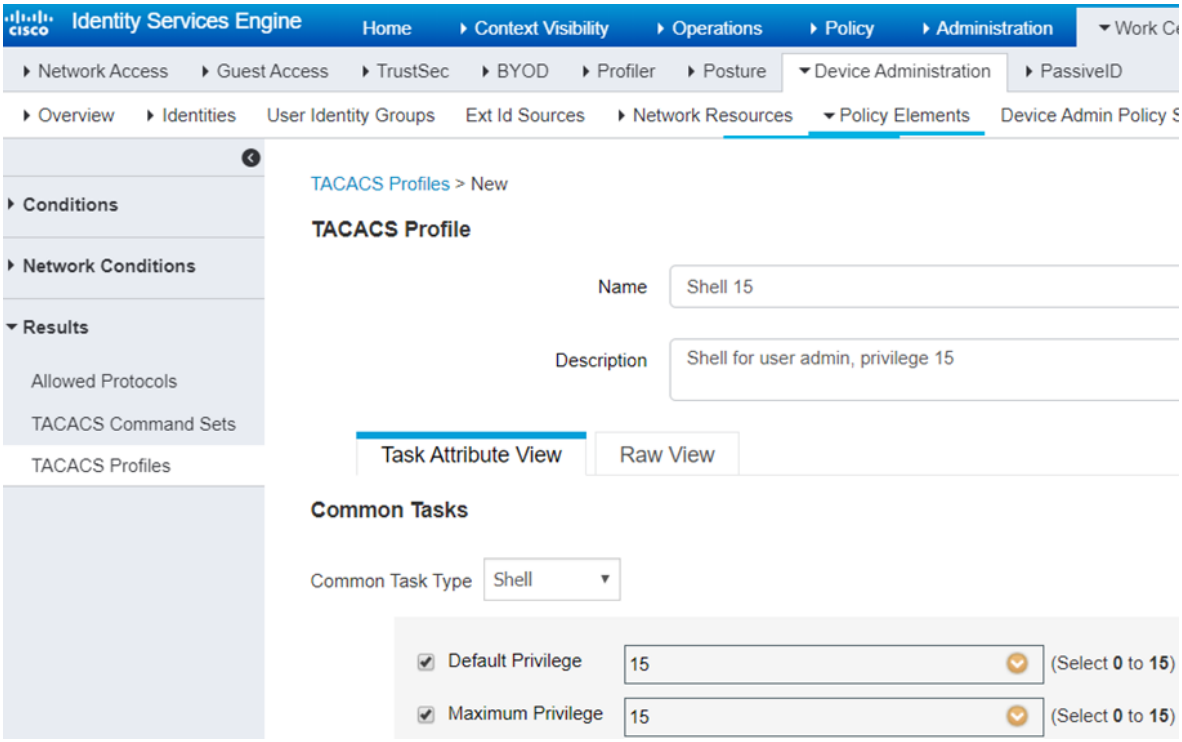



Sau đó bấm **Submit**.

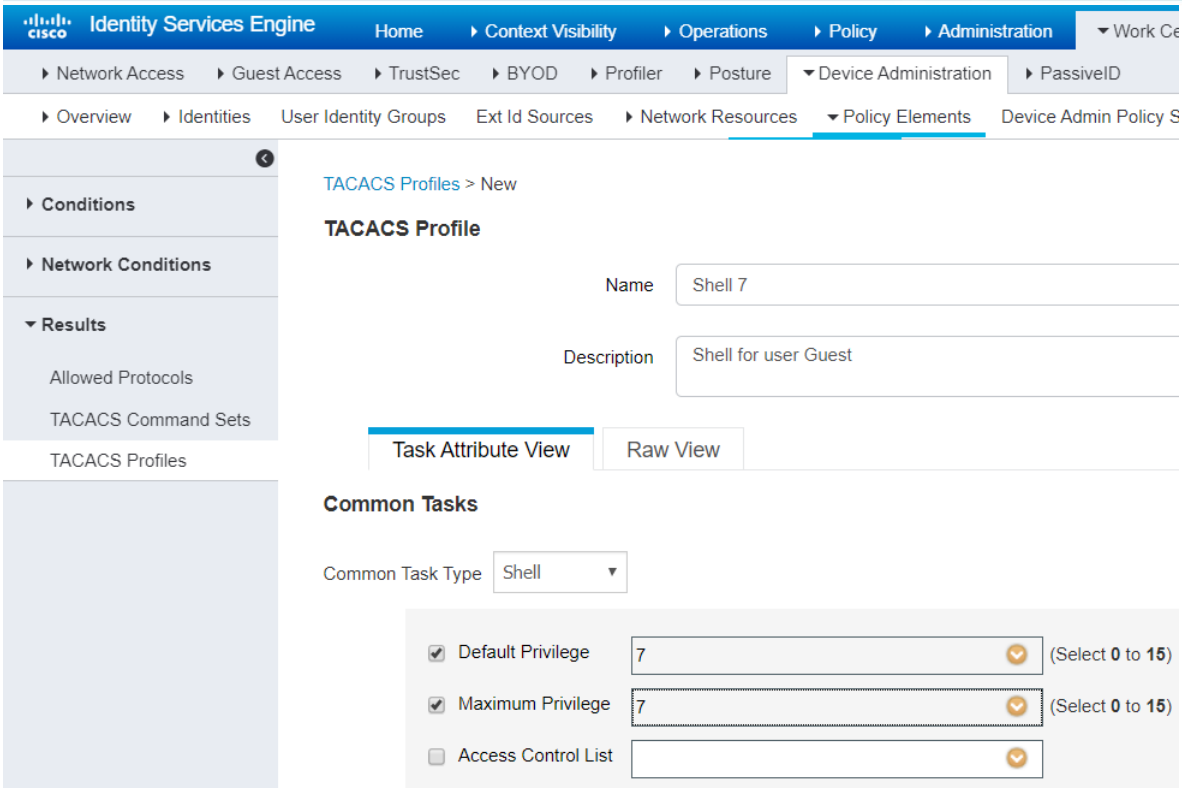
Tiếp theo, ta vào **TACACS Profiles → Add**:



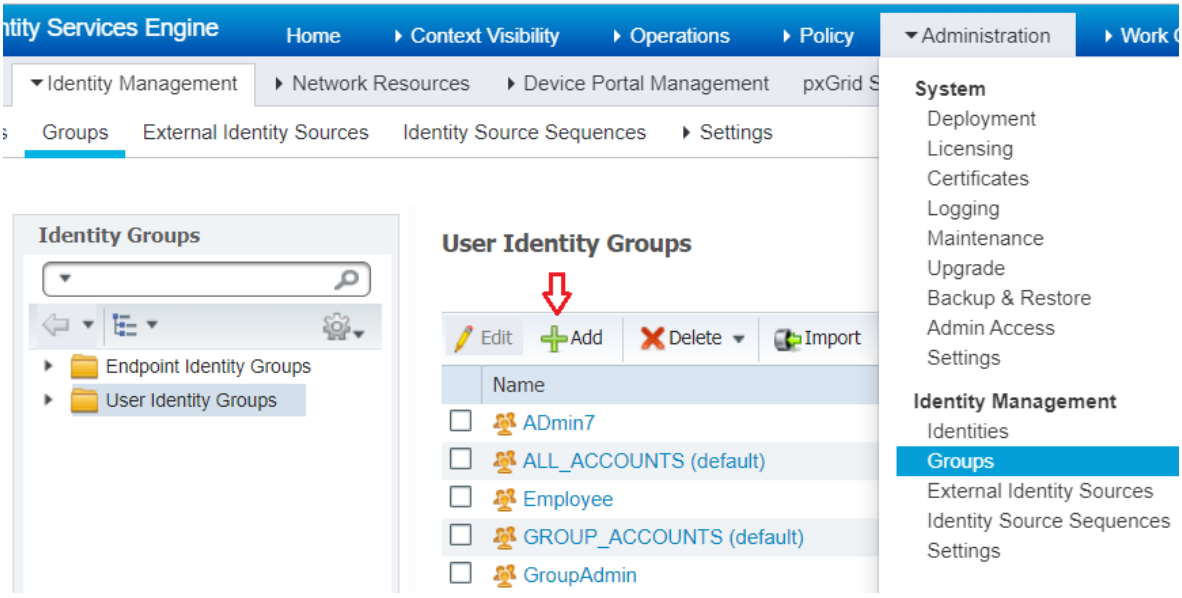

Tạo profile cho ***adminvnpro*** với privilege 15:



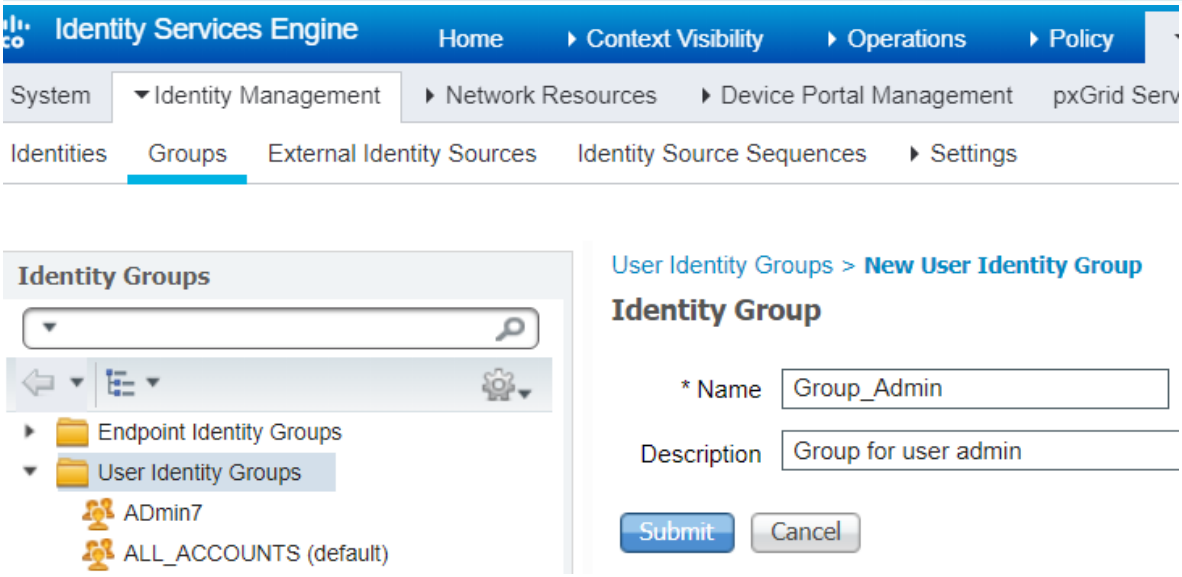

Profile cho ***guest*** với privilege 7:

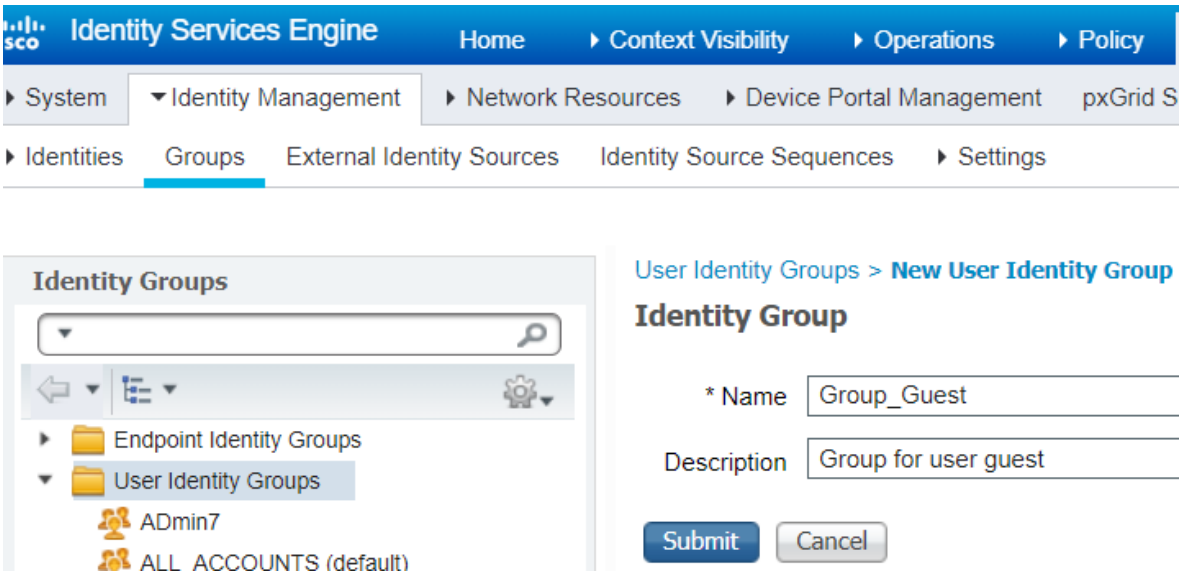



Vào **Administration → Groups → User Identify Groups → Add**:

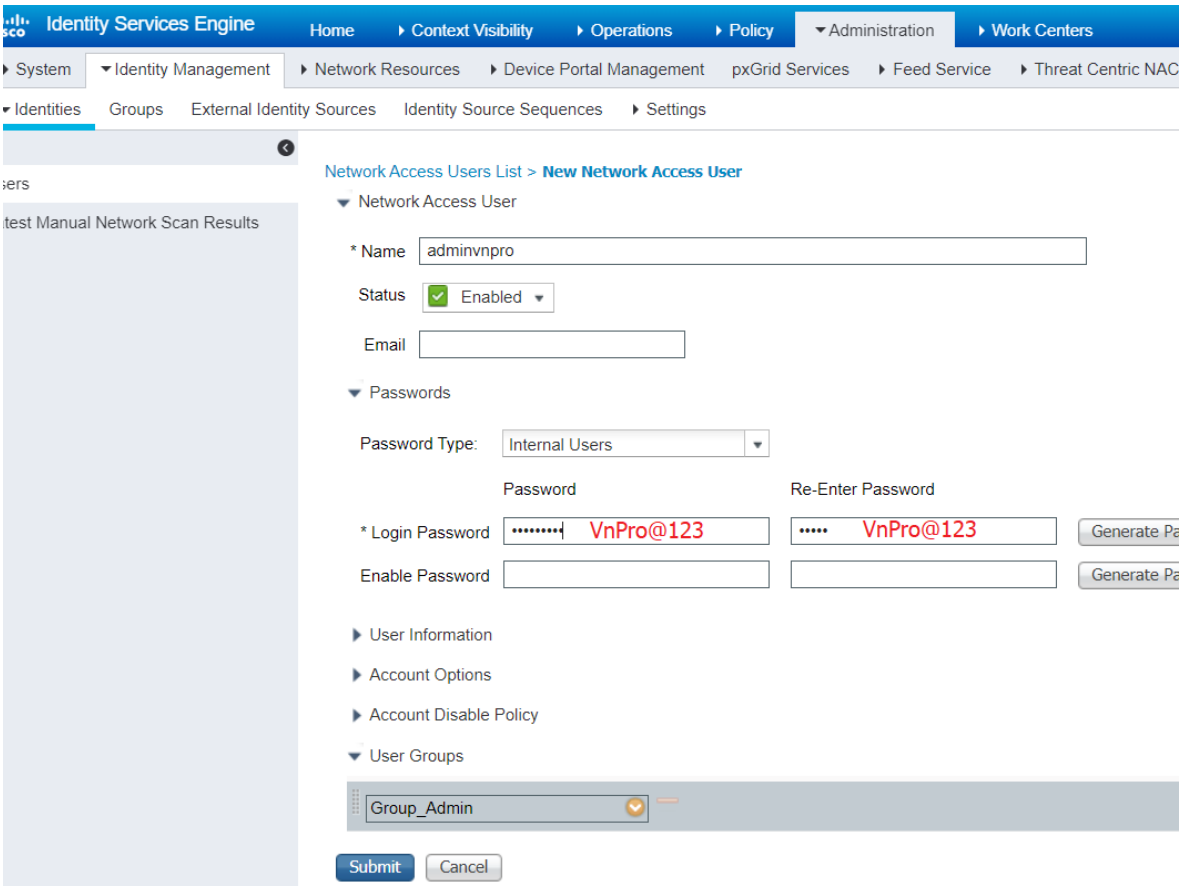



Tạo 2 group cho user ***adminvnpro*** và user ***guest*:**


Identity Services Engine
Home
Context Visibility
Operations
Policy
System
Identity Management
Network Resources
Device Portal Management
pxGrid Serv
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
Identity Groups
Endpoint Identity Groups
User Identity Groups
ADmin7
ALL_ACCOUNTS (default)
User Identity Groups > New User Identity Group
Identity Group
* Name
Group_Admin
Description
Group for user admin
Submit
Cancel


Identity Services Engine
Home
Context Visibility
Operations
Policy
System
Identity Management
Network Resources
Device Portal Management
pxGrid S
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
Identity Groups
Endpoint Identity Groups
User Identity Groups
ADmin7
ALL_ACCOUNTS (default)
User Identity Groups > New User Identity Group
Identity Group
* Name
Group_Guest
Description
Group for user guest
Submit
Cancel

Vào **Identities** → **Add** → Tạo user ***adminvnpro***:

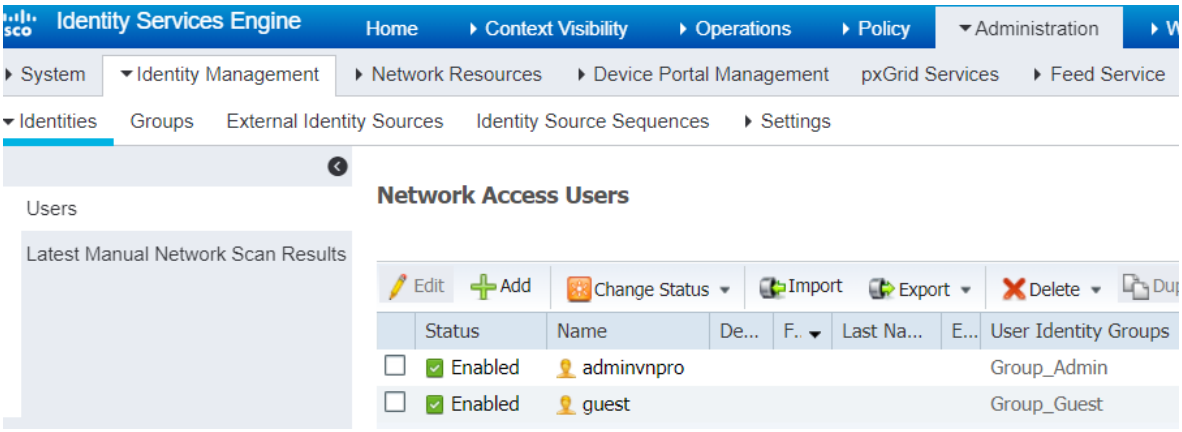



Trong đó:

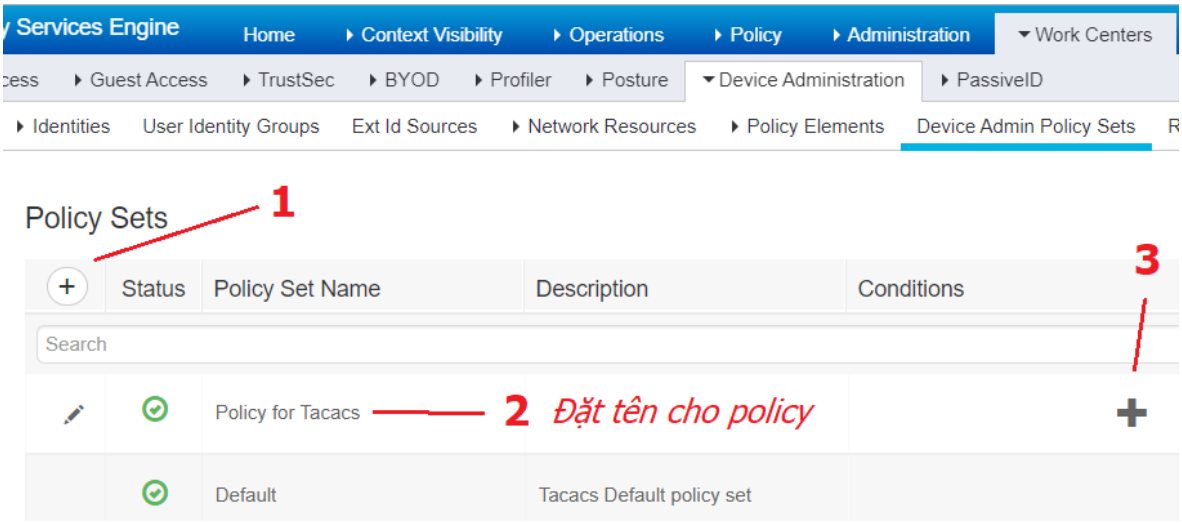
- **Password Type:** Internal Users
- **User Group:** Group_Admin

Tương tự, ta cũng tạo thêm user ***guest*** với **User Groups** là Group_Guest:


Kết quả:

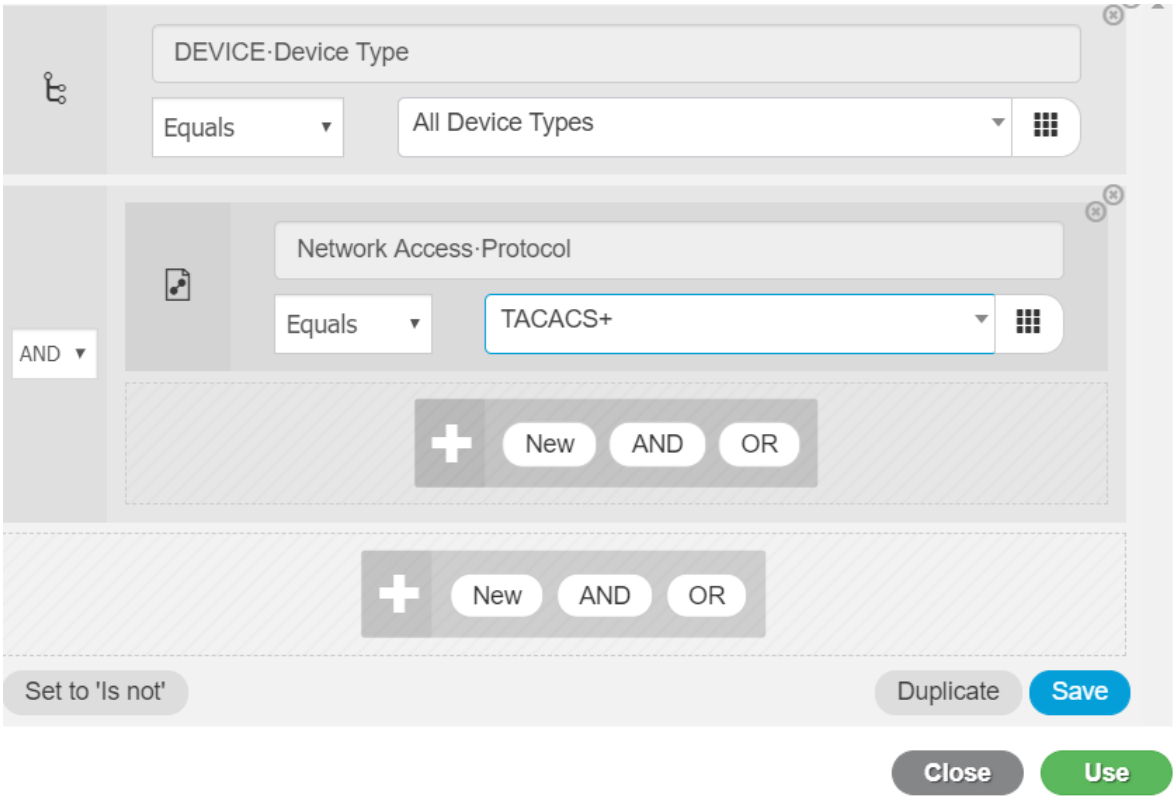



Tiếp theo, ta vào **Work Center → Device Admin Policy Sets → bấm ( + ):**

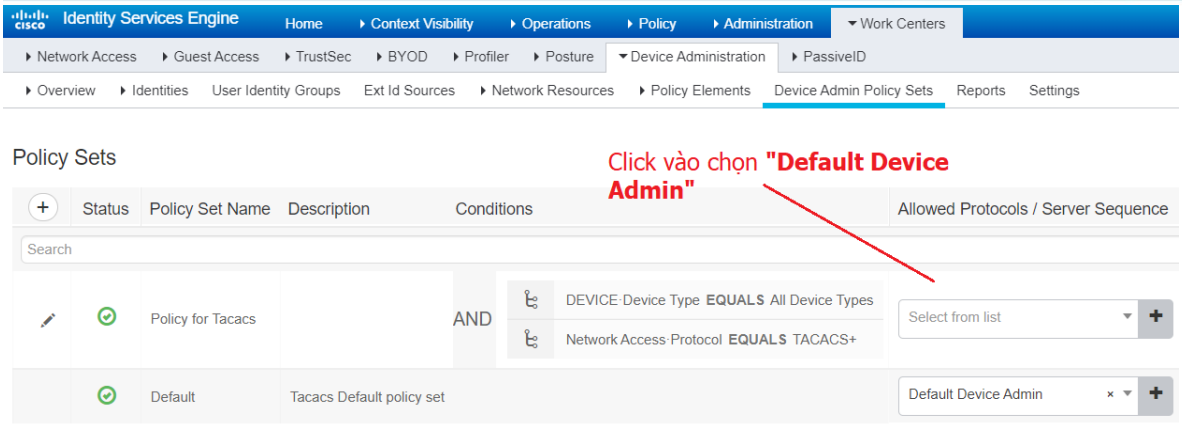



Tạo policy như sau:


Sau khi click **"AND"** ta chọn **"New"** và thiết lập như sau:

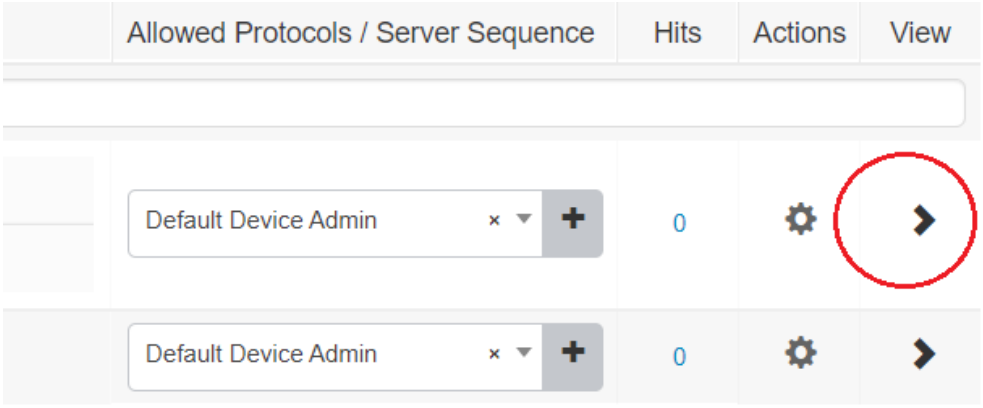



Sau đó bấm **"Use"**, ta được kết quả:

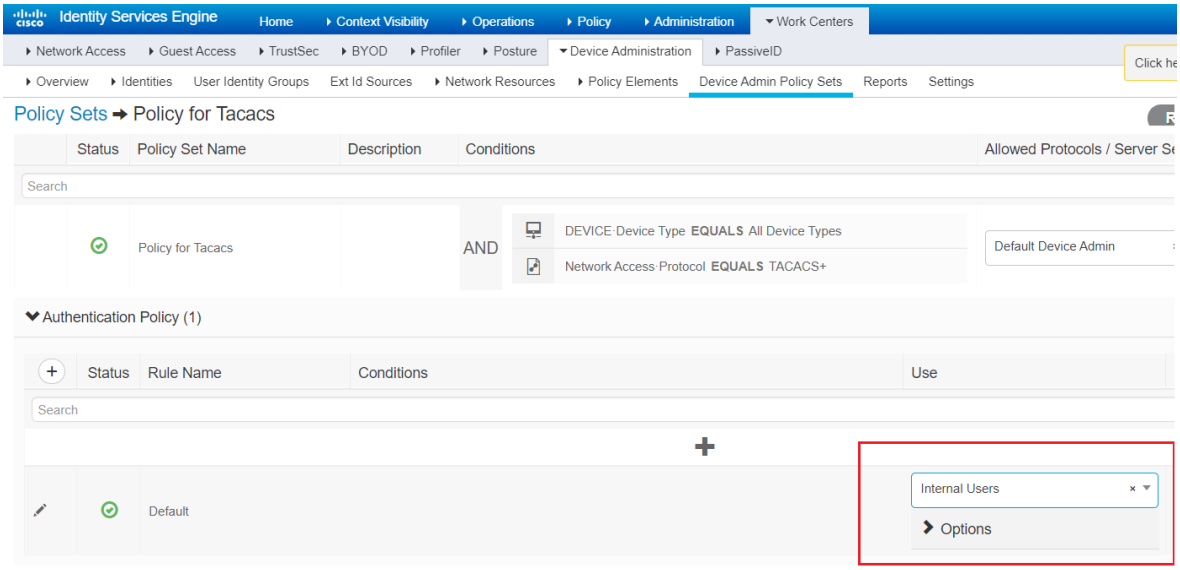



Sau đó save lại.

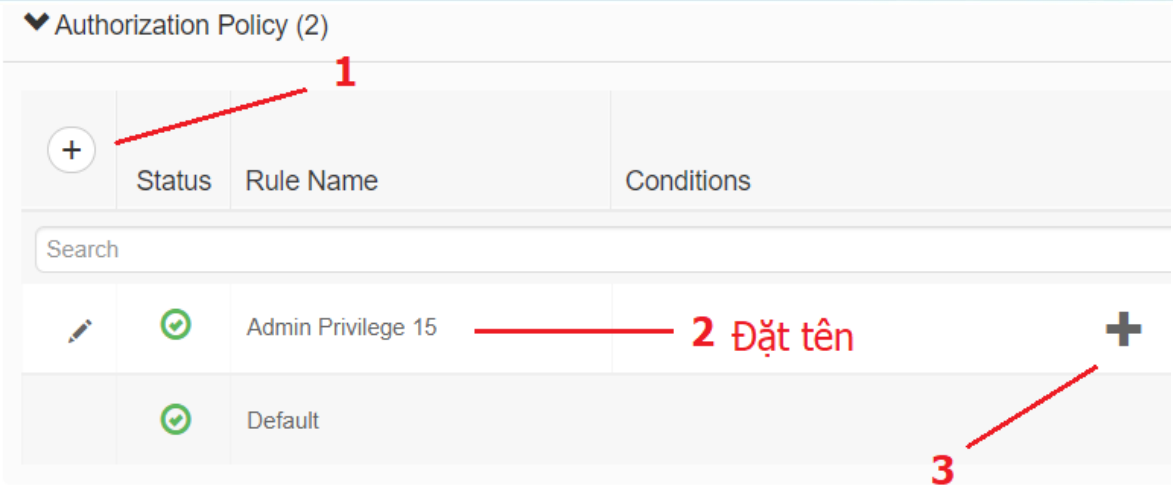
Sau đó, ta click vào mũi tên qua phải của policy vừa mới tạo:



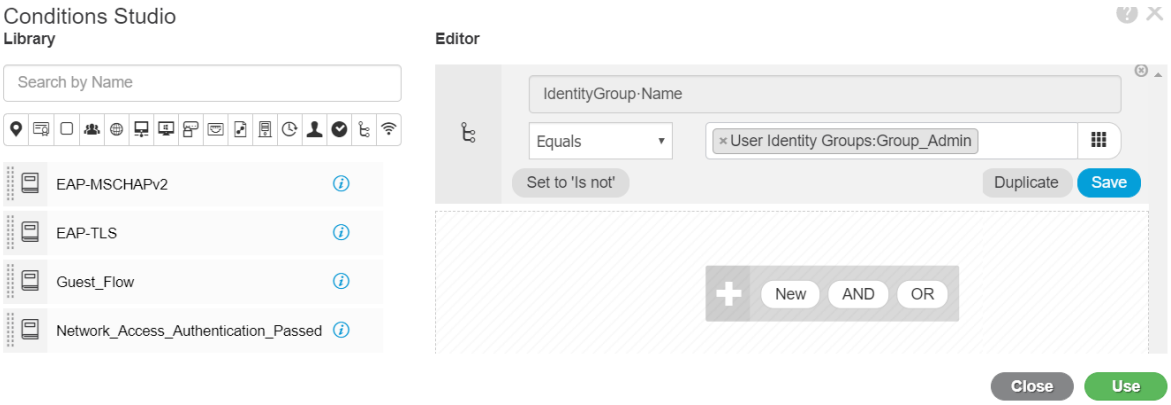

Ở phần **"Authentication Policy"** ta chọn Use: **Internal Users**:



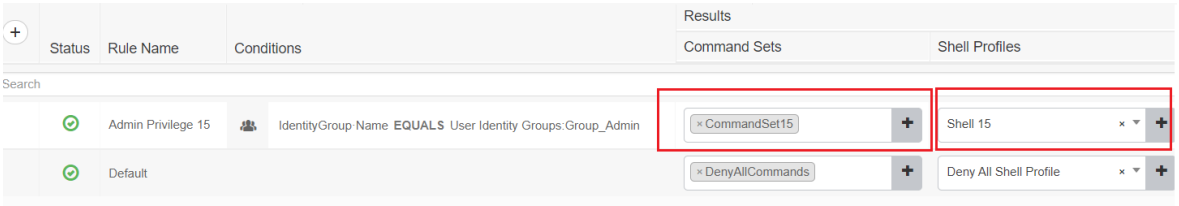

Tiếp theo, ta cấu hình phần **Authorization Policy:**



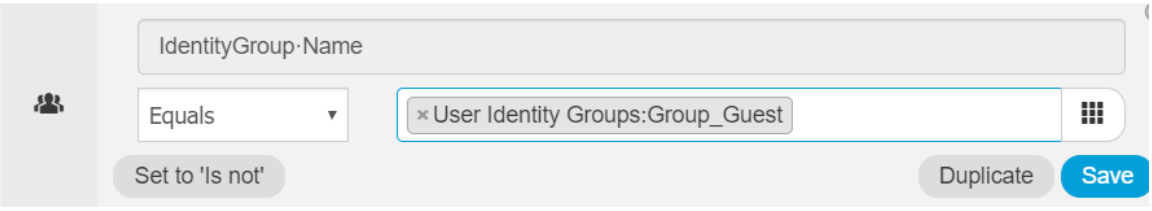

Cấu hình conditions như sau:

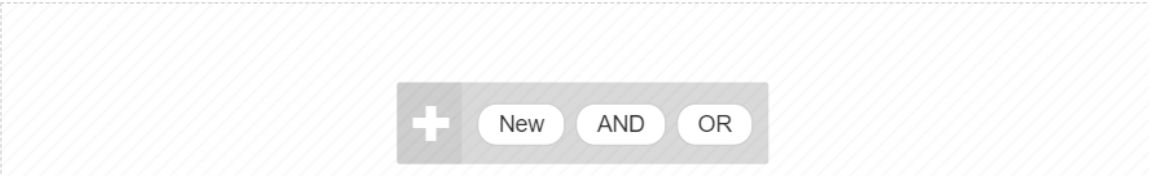


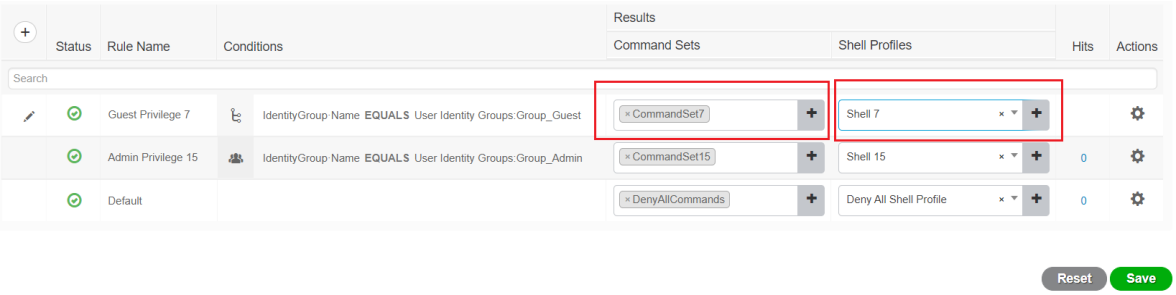

Sau đó bấm **"Use"** để quay lại mục **Authorization Policy**, ở mục bên phải, ta chọn command set là "**CommandSet15**" và shell profile là "**Shell 15**".




Tương tự vậy, ta cũng tạo **Authorization Policy** cho account ***guest***:



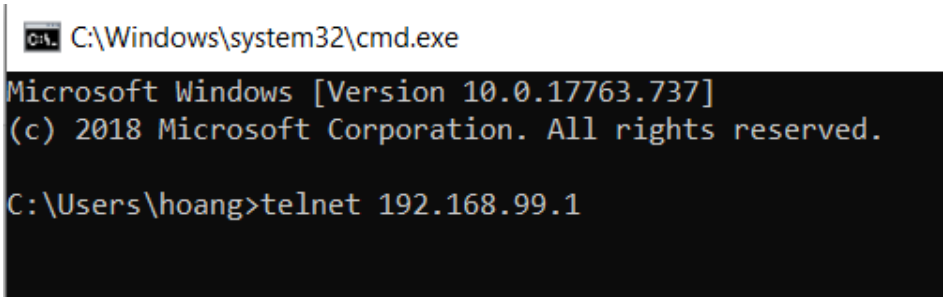







Sau đó ta save lại.

Ta dùng PC telnet vào Router với username là ***adminvnpro*** password là ***VnPro@123*:**




Kết quả: Telet thành công:


Gõ "?" để kiểm tra các lệnh user này có thể sử dụng, ta thấy user adminvnpro có thể dùng tất cả các lệnh:

```
Te net 192.168.99.1

Username:adminvnpro
Password:

Router#?
Exec commands:
  <1-99>           Session number to resume
  access-enable    Create a temporary Access-List entry
  access-profile   Apply user-profile to interface
  access-template  Create a temporary Access-List entry
  alps             ALPS exec commands
  archive          manage archive files
  audio-prompt     load ivr prompt
  auto             Exec level Automation
  beep             Blocks Extensible Exchange Protocol commands
  bert             Bit Error Rate Testing
  bfe              For manual emergency modes setting
  calendar         Manage the hardware calendar
  call             Voice call
  ccm-manager      Call Manager Application exec commands
  cd               Change current directory
  clear            Reset functions
  clock            Manage the system clock
  cns              CNS agents
  configure        Enter configuration mode
  connect          Open a terminal connection
  copy             Copy from one file to another
  credential       load the credential info from file system
  crypto           Encryption related commands.
  debug            Debugging functions (see also 'undebug')
  delete           Delete a file
  dir              List files on a filesystem
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection
 --More--
```

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

Thử lại với account ***guest*** ta thấy account này được sử dụng rất ít lệnh và chỉ sử dụng được các lệnh *show*:

```
Router#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.3.1 to network 0.0.0.0

C    192.168.99.0/24 is directly connected, FastEthernet0/1
C    192.168.3.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [254/0] via 192.168.3.1
Router#conf t
          ^
% Invalid input detected at '^' marker.

Router#
```

Không dùng được lệnh "**Configure terminal**"

Shutdown cổng F0/0 của Router. Ta sẽ không còn telnet vào Router được nữa vì đã mất kết nối đến ISE server:

```
User Access Verification

Username: adminvnpro
Password:

% Authentication failed

Username: adminvnpro
Password:

% Authentication failed

Username:
% Username:  timeout expired!

Connection to host lost.

C:\Users\hoang>
```

**<u>Cấu hình xác thực/phân quyền local:</u>**

Kết nối vào cổng console của Router, ta dùng các lệnh sau:

```
Router(config)#privilege exec level 7 show

Router(config)#username adminvnpro privilege 15 password VnPro@123
```

Telnet lại vào Router, sử dụng account ***adminvnpro,*** ta thấy telnet thành công:

Telnet 192.168.99.1

```
User Access Verification

Username: adminvnpro
Password:

Router#show privilege
Current privilege level is 15
Router#
```

Sử dụng account ***guest*** ta vẫn không kết nối được do không kết nối được với ISE và ta chưa tạo account ***guest*** trong local:

```
User Access Verification

Username: guest
Password:

% Authentication failed

Username:
% Username:  timeout expired!

Connection to host lost.

C:\Users\hoang>
```

Bật trở lại cổng F0/0 của router, ta telnet lại lần nữa với account **guest:**

```
Router(config)#int f0/0

Router(config-if)#no shutdown
```

Telnet 192.168.99.1

```
Username:guest
Password:

Router#
```

Telnet thành công do kết nối được với ISE và dùng user guest trên ISE.

***Chú ý:** Do sử dụng giao thức DHCP nên khi bật lại cổng F0/0 của Router có thể IP sẽ bị thay đổi, có thể ta sẽ phải add lại thiết bị trên ISE Server.