

LAB : XÁC THỰC VÀ PHÂN QUYỀN LOGIN BẰNG GIAO THỨC TACACS+ 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

2.1. Cấu hình ban đầu

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

2.2. 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 nội bộ trên switch với các mức thẩm quyền cho các người dùng như trên để khi hoạt động xác thực với Cisco ISE không thành công, chuyển sang phương 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 telnet:

```
Router(config)# line vty 0 4
```

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
```

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.



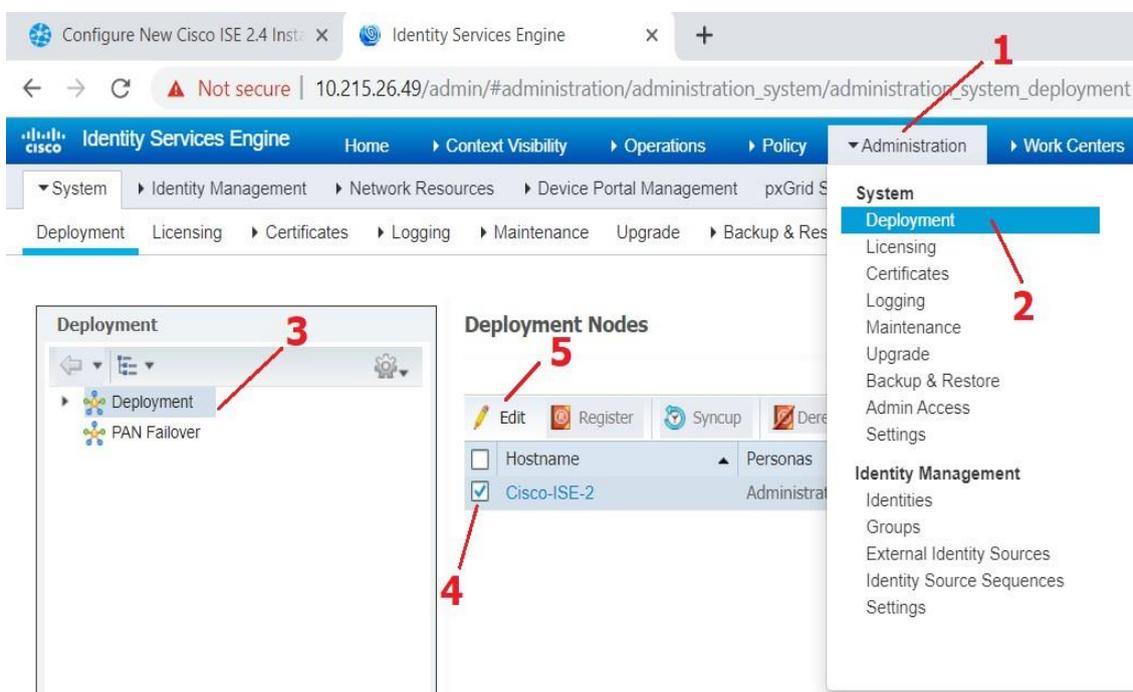
CÔNG TY TNHH TƯ VẤN VÀ DỊCH VỤ CHUYÊN VIỆT

TRUNG TÂM TIN HỌC VNPRO

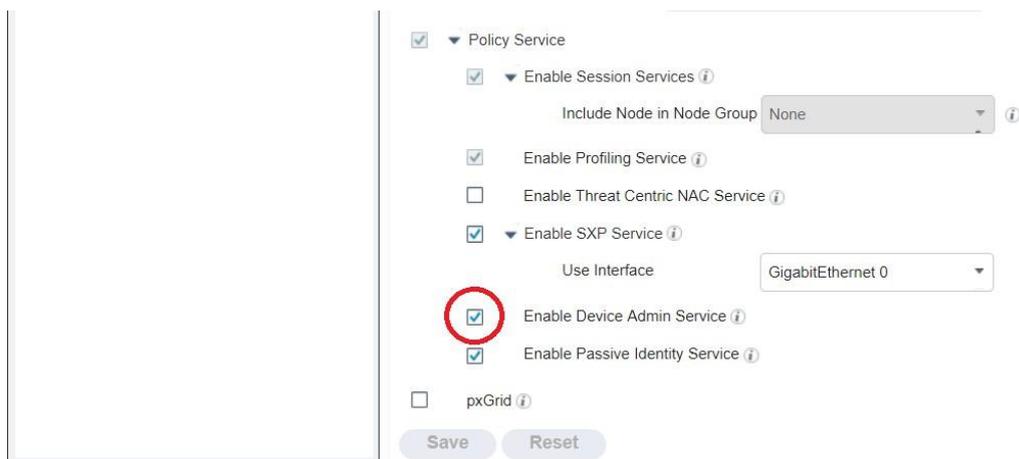
ĐC: 276 - 278 Ung Văn Khiêm, P.25, Q.Bình Thạnh, Tp Hồ Chí Minh

ĐT: (028) 35124257 | Hotline: 0933427079 Email: vnpro@vnpro.org

Vào Administration → Deployment → Tích chọn hostname của Cisco-ISE-2 → Edit:



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



Thêm Router vào ISE:

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

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Network Resources. The left sidebar contains: Network Devices, Network Device Groups, Default Devices, TACACS External Servers, and TACACS Server Sequence. The main content area is titled 'Network Devices' and features a toolbar with 'Edit', 'Add', 'Duplicate', 'Import', 'Export', 'Generate PAC', and 'Delete' buttons. Below the toolbar is a table with columns: Name, IP/Mask, Profile Name, and Location. A red arrow points to the 'Add' button.

Nhập tên và IP của Router ta muốn thêm:

The screenshot shows the 'New Network Device' form in the Cisco ISE interface. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Network Resources > Network Devices List > New Network Device. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Network Devices' and contains the following form fields:

- * Name: Router
- Description: (empty)
- IP Address: (dropdown menu)
- * IP: 192.168.3.135 / 24

Ở phần TACACS Authentication Settings ta chỉ định chuỗi “Shared Secret” để Router và ISE giao tiếp với nhau, sau đó chọn submit:

The screenshot shows the 'TACACS Authentication Settings' form in the Cisco ISE interface. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Network Resources > Network Devices List > New Network Device > TACACS Authentication Settings. The left sidebar contains: RADIUS Authentication Settings, TACACS Authentication Settings, SNMP Settings, and Advanced TrustSec Settings. The main content area is titled 'TACACS Authentication Settings' and contains the following form fields:

- Shared Secret: (password field with dots, highlighted with a red arrow and the text '123abc')
- Show: (button)
- Enable Single Connect Mode: (checkbox)
- Legacy Cisco Device: (radio button, selected)
- TACACS Draft Compliance Single Connect Support: (radio button)

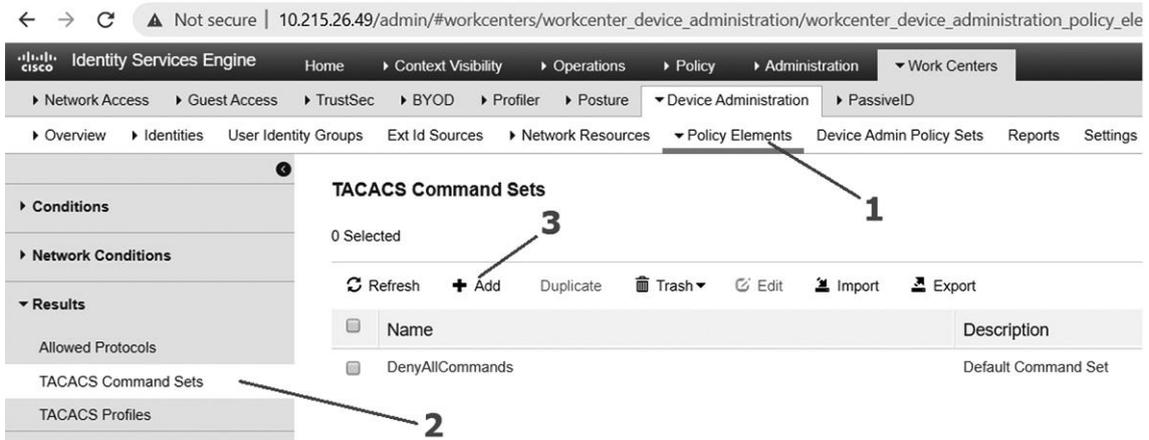
 At the bottom of the form are 'Submit' and 'Cancel' buttons.

Cấu hình xác thực/phân quyền bằng TACACS+:

Vào Work Centers → Device Administration → Device Admin Policy Sets:



Chọn Policy Elements → Results → TACACS Command Sets → Add:



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

TACACS Command Sets > CommandSet1

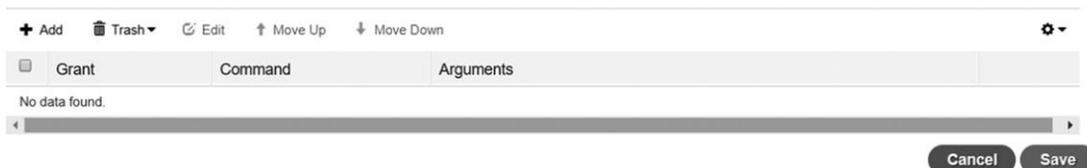
Command Set

Name:

Description:

Commands

Permit any command that is not listed below



Chọn “Permit any command that is not listed below” và chọn 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 chọn submit:

TACACS Command Sets > CommandSet7

Command Set

Name: CommandSet7

Description: Privilege level 7 for Guest

Commands

Permit any command that is not listed below

Grant	Command	Arguments
<input type="checkbox"/>	PERMIT	show*

Tiếp theo, ta vào TACACS Profiles → Add:

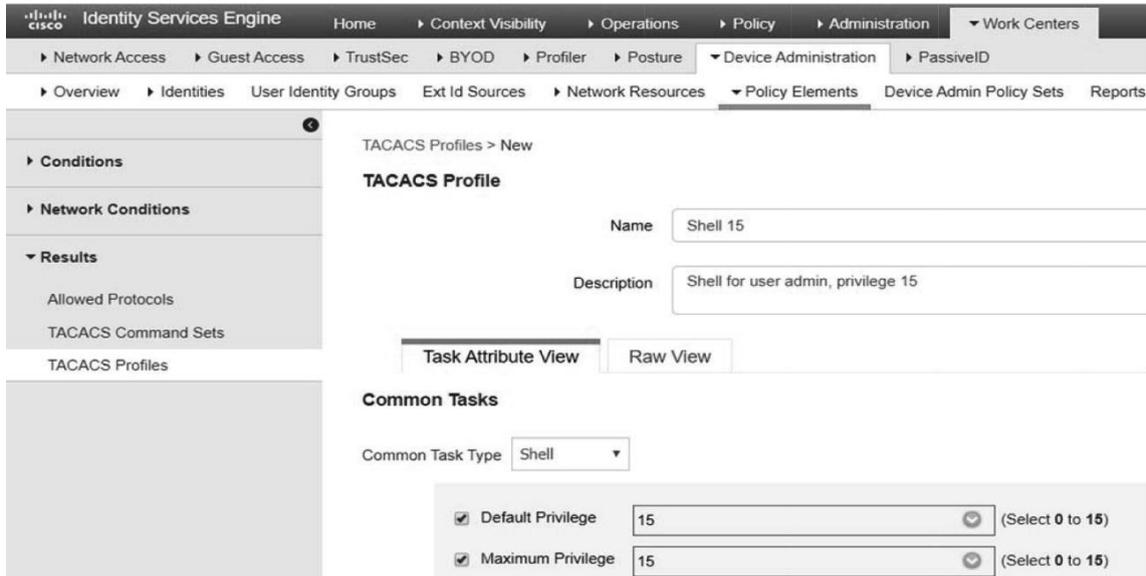
TACACS Profiles

0 Selected

Refresh + Add Duplicate Trash Edit

Name	Type	Description
Default Shell Profile	Shell	Default Shell Profile
Deny All Shell Profile	Shell	Deny All Shell Profile
WLC ALL	WLC	WLC ALL
WLC MONITOR	WLC	WLC MONITOR

Tạo profile cho adminvnpro với privilege 15:

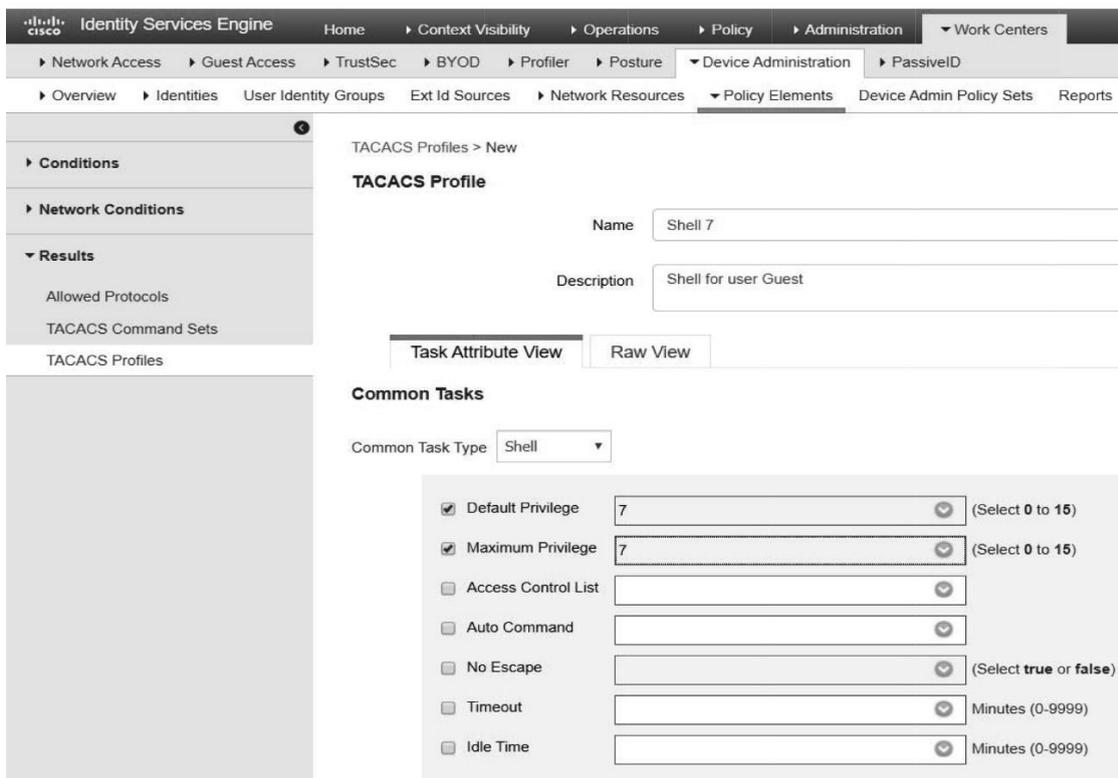


The screenshot shows the Cisco Identity Services Engine (ISE) configuration page for a new TACACS Profile. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > PassiveID > Policy Elements > TACACS Profiles > New.

TACACS Profile Configuration:

- Name:** Shell 15
- Description:** Shell for user admin, privilege 15
- Common Task Type:** Shell
- Default Privilege:** 15 (Select 0 to 15)
- Maximum Privilege:** 15 (Select 0 to 15)

Profile cho *guest* với privilege 7:



The screenshot shows the Cisco Identity Services Engine (ISE) configuration page for a new TACACS Profile. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > PassiveID > Policy Elements > TACACS Profiles > New.

TACACS Profile Configuration:

- Name:** Shell 7
- Description:** Shell for user Guest
- Common Task Type:** Shell
- Default Privilege:** 7 (Select 0 to 15)
- Maximum Privilege:** 7 (Select 0 to 15)
- Access Control List:** (Empty)
- Auto Command:** (Empty)
- No Escape:** (Select true or false)
- Timeout:** (Empty) Minutes (0-9999)
- Idle Time:** (Empty) Minutes (0-9999)

Vào Administration → Groups → User Identity Groups → Add:

The screenshot shows the Cisco Identity Services Engine Administration console. The breadcrumb navigation is: Administration > Work Centers > System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Identities > Groups > External Identity Sources > Identity Source Sequences > Settings. The 'Groups' menu is expanded, showing 'System' and 'Identity Management' sub-menus. Under 'Identity Management', 'Groups' is selected. The 'User Identity Groups' page is visible, showing a list of groups: Admin7, ALL_ACCOUNTS (default), Employee, GROUP_ACCOUNTS (default), and GroupAdmin. The 'Add' button is highlighted.

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

The screenshot shows the 'New User Identity Group' form in the Cisco Identity Services Engine Administration console. The breadcrumb navigation is: Administration > Work Centers > System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Identities > Groups > External Identity Sources > Identity Source Sequences > Settings. The 'Groups' menu is expanded, and 'User Identity Groups' is selected. The 'New User Identity Group' form is displayed, with the following fields: Name: Group_Admin, Description: Group for user admin. The 'Submit' and 'Cancel' buttons are visible.

The screenshot shows the 'New User Identity Group' form in the Cisco Identity Services Engine Administration console. The breadcrumb navigation is: Administration > Work Centers > System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Identities > Groups > External Identity Sources > Identity Source Sequences > Settings. The 'Groups' menu is expanded, and 'User Identity Groups' is selected. The 'New User Identity Group' form is displayed, with the following fields: Name: Group_Guest, Description: Group for user guest. The 'Submit' and 'Cancel' buttons are visible.

Vào Identities → Add → Tạo user *adminvnpro*:

The screenshot shows the 'New Network Access User' configuration page in Cisco ISE. The user name is 'adminvnpro', status is 'Enabled', and email is empty. Under 'Passwords', the type is 'Internal Users'. The login password is 'VnPro@123' and the re-enter password is also 'VnPro@123'. The 'User Groups' section shows 'Group_Admin' selected. 'Submit' and 'Cancel' buttons are at the bottom.

Trong đó:

- Password Type: Internal Users
- User Group: Group_Admin

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

The screenshot shows the 'New Network Access User' configuration page for user 'guest'. The user name is 'guest', status is 'Enabled', and email is empty. Under 'User Groups', 'Group_Guest' is selected. 'Submit' and 'Cancel' buttons are at the bottom.

Kết quả:

Status	Name	User Identity Groups
<input checked="" type="checkbox"/> Enabled	adminvnpro	Group_Admin
<input checked="" type="checkbox"/> Enabled	guest	Group_Guest

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

Status	Policy Set Name	Description	Conditions
<input checked="" type="checkbox"/>	Policy for Tacacs		
<input checked="" type="checkbox"/>	Default	Tacacs Default policy set	

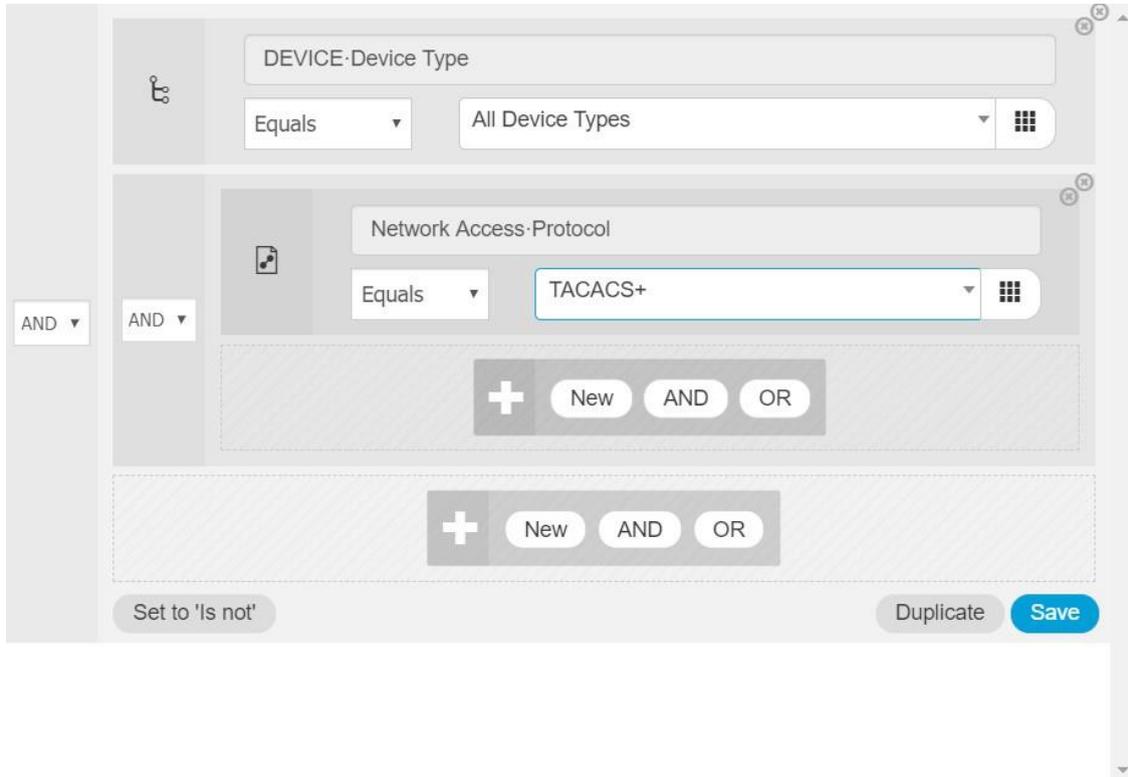
Tạo policy như sau:

1. Click vào chọn **DEVICE: Device Type**

2. Click vào chọn **All Device Types**

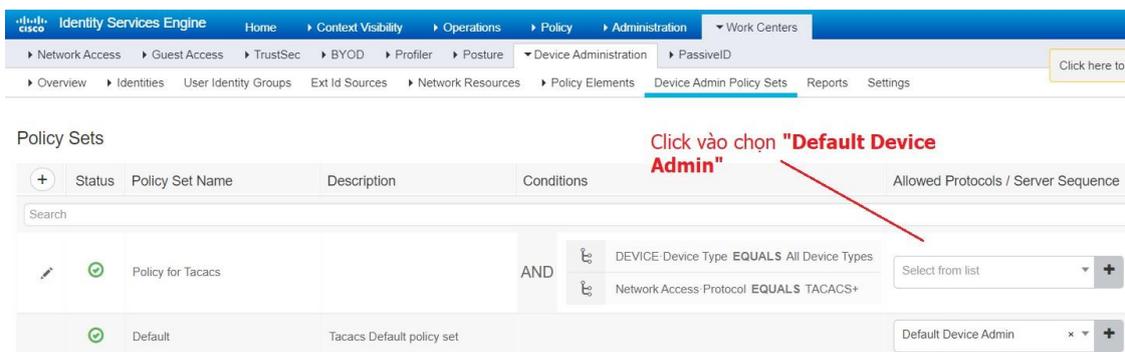
3

Sau khi click “AND” ta chọn “New” và thiết lập như sau:



Close **Use**

Sau đó bấm “Use”, ta được kết quả:



Và save lại.

Click vào mũi tên qua phải của policy vừa mới tạo:

Allowed Protocols / Server Sequence	Hits	Actions	View
Default Device Admin	0		
Default Device Admin	0		

Ở phần “Authentication Policy” ta chọn Use: Internal Users:

Policy Sets → Policy for Tacacs

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
✓	Policy for Tacacs		AND DEVICE Device Type EQUALS All Device Types NetworkAccess Protocol EQUALS TACACS+	Default Device Admin

Authentication Policy (1)

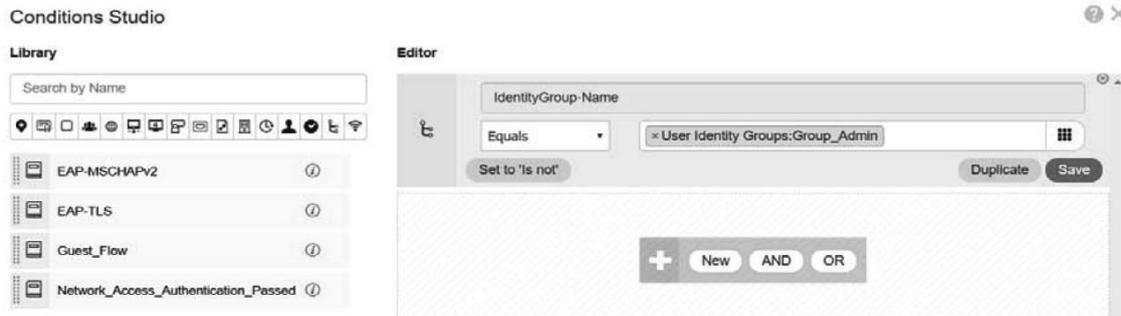
+	Status	Rule Name	Conditions	Use
	✓	Default		Internal Users

Tiếp theo, ta cấu hình phần Authorization Policy:

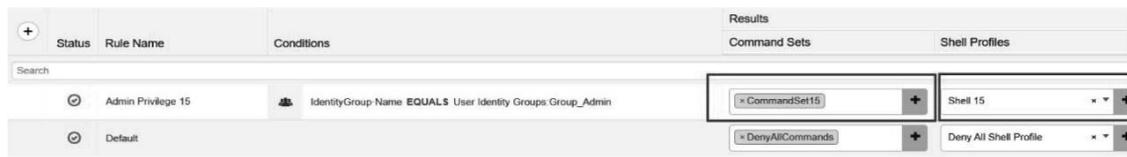
Authorization Policy (2)

+	Status	Rule Name	Conditions	Use
	✓	Admin Privilege 15		
	✓	Default		

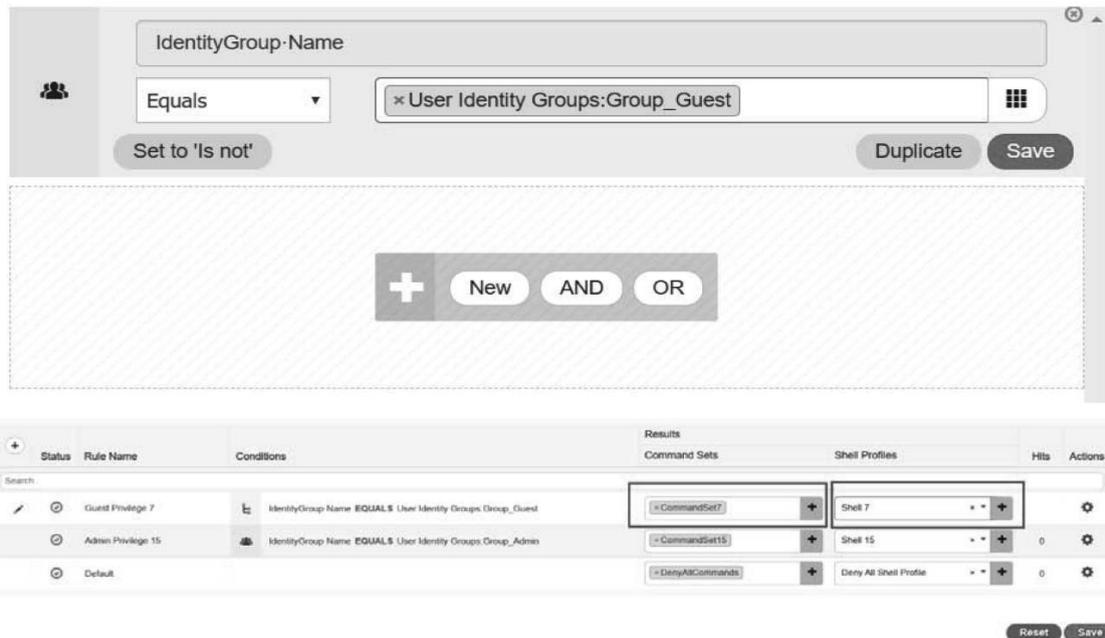
Cấu hình conditions như sau:



Sau đó bấm “Use” để quay lại mục Authorization Policy, ở mục bên phải, ta chọn command sets là “CommandSet15” và shell profiles là “Shell 15”.



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



Cuối cùng ta save lại.

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 IS
Router(config)#aaa authentication login VTY group ISESRV lo
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

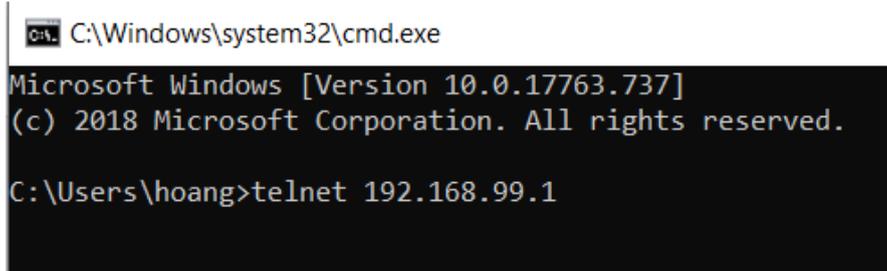
Router(config)#aaa accounting connection default
Router(cfg-acct-mlist)#action-type start-stop
Router(cfg-acct-mlist)#group ISESRV
Router(cfg-acct-mlist)#exit

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
```

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



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\hoang>telnet 192.168.99.1
```

Kết quả: Telet thành công:



```
C:\> Telnet 192.168.99.1
Username:adminvnpro
Password:
Router#
```

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

```
CVL Telnet 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>
```

Cấu hình xác thực/phân quyền local:

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:

```
C:\> 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.

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