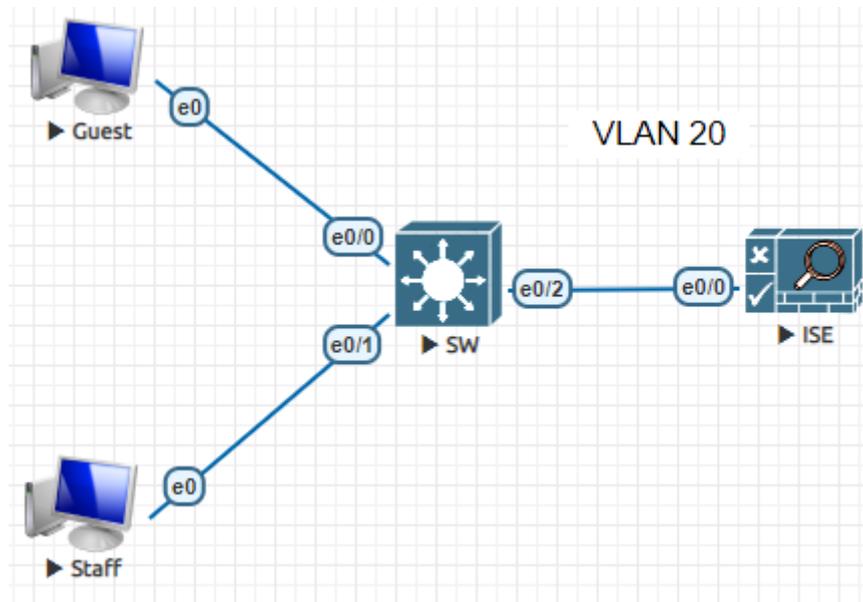


LAB - CISCO ISE TRUSTSEC

I. SƠ ĐỒ



II. Mục đích bài LAB:

✓ Tạo security group, xác thực nhận dạng user và gán user vào security group sau đó áp policy theo group

✓ Hệ thống gồm:

✓ Cisco ISE 2.3

✓ Switch 3560x loaded firmware support Cisco Trustsec SGACL

✓ Clients window 7

✓ Cụ thể:

Có 2 user thuộc 2 group VNE-staff và VNE-guest

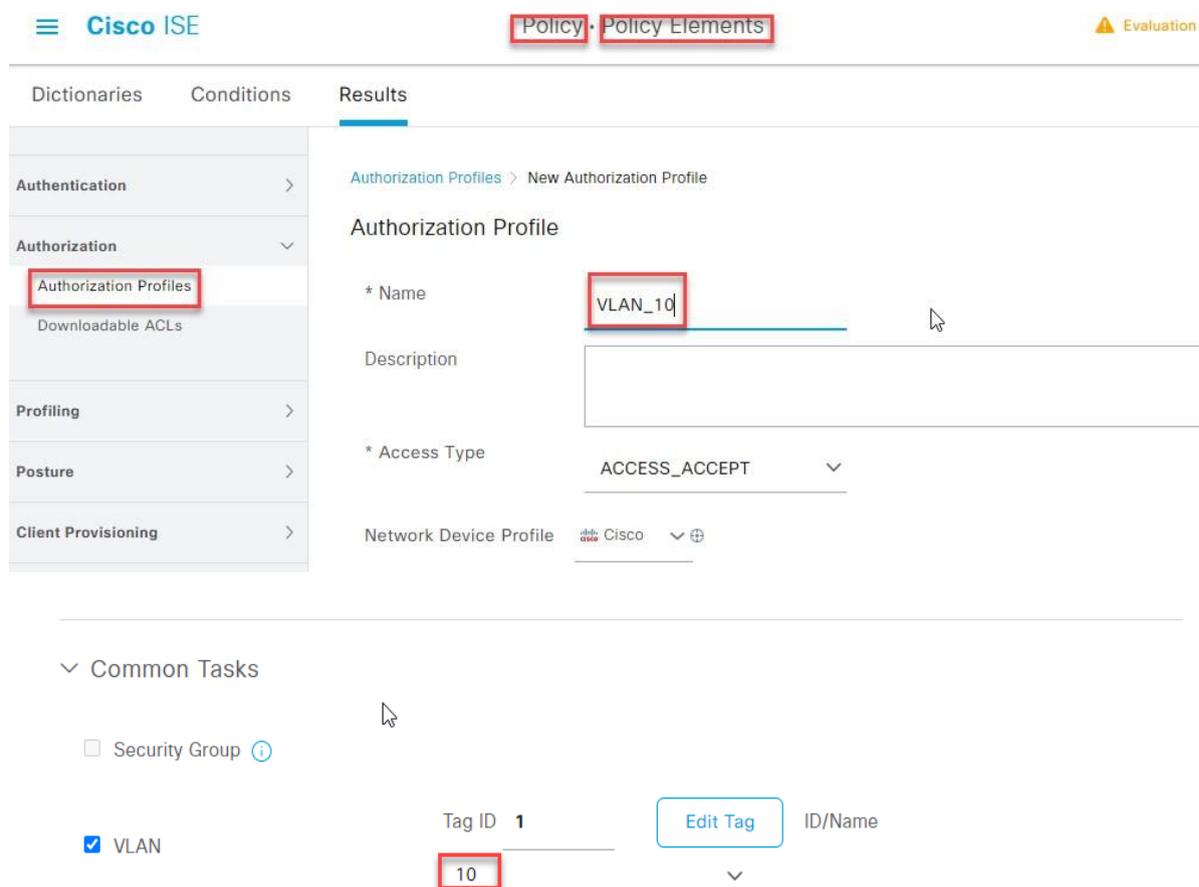
Sau khi xác thực bằng 802.1X, 2 users đc gán Vlan 10 và vào 2 security group VNE-staff, VNE-guest

✓ Áp policy:

VNE-staff to VNE-guest (cho phép Ping & Remote)

VNE-guest to VNE-staff (chỉ được Ping)

- ✓ **Trên Cisco ISE:** cấu hình 802.1x với 3560X, tạo các Policy cho group Guest và Staff
- ✓ Chuyển hướng đến Policy / Policy Elements/ Authorization / Authorization Profile
- ✓ Name: VLAN_VNE
- ✓ Vlan tag: ID/Name:10



The screenshot shows the Cisco ISE web interface. At the top, there are navigation tabs for 'Policy' and 'Policy Elements', both highlighted with red boxes. A yellow 'Evaluation' warning icon is visible in the top right corner. The main content area is divided into three sections: 'Dictionaries', 'Conditions', and 'Results'. Under 'Dictionaries', the 'Authorization Profiles' option is highlighted with a red box. The 'Authorization Profile' configuration form is displayed, with the following fields:

- * Name: VLAN_10 (highlighted with a red box)
- Description: (empty text area)
- * Access Type: ACCESS_ACCEPT (dropdown menu)
- Network Device Profile: Cisco (dropdown menu)

Below the configuration form, there is a 'Common Tasks' section with a checkbox for 'Security Group' (unchecked) and a checkbox for 'VLAN' (checked). Under the 'VLAN' checkbox, there is a 'Tag ID' field with the value '1' and an 'Edit Tag' button. Below this, a dropdown menu shows the value '10' (highlighted with a red box) and the label 'ID/Name'.

✓ Ta chuyển hướng Work Centers / Guest Access / Identity / Network Access Users

✓ Username: engineer

The screenshot shows the Cisco ISE web interface. At the top, the navigation menu includes 'Work Centers' and 'Guest Access'. Below this, the 'Identities' tab is selected, showing a sidebar with 'Network Access Users' highlighted. The main content area is titled 'Network Access Users List > New Network Access User'. Under the 'Network Access User' section, the '* Username' field contains 'engineer' and the 'Status' is set to 'Enabled'. Below these fields are two password fields: '* Login Password' and 'Re-Enter Password', both with masked characters and 'Generate Password' buttons. There are also 'Enable Password' fields.

✓ Username: engineer

The screenshot shows the Cisco ISE web interface. At the top, the navigation menu includes 'Work Centers' and 'Guest Access', and a notification for 'Evaluation Mode 87 Days' is visible. Below this, the 'Identities' tab is selected, showing a sidebar with 'Network Access Users' highlighted. The main content area is titled 'Network Access Users List > New Network Access User'. Under the 'Network Access User' section, the '* Username' field contains 'employee' and the 'Status' is set to 'Enabled'.

Password	ReEnter Password	
* Login Password <input type="password" value="...."/>	<input type="password" value="...."/>	<input type="button" value="Generate Password"/> ⓘ
Enable Password		<input type="button" value="Generate Password"/> ⓘ

✓ Ta đã tạo được 2 user:

Network Access Users

⏏ Edit + Add ⚙ Change Status ↓ Import ↑ Export 🗑 Delete 📄 Duplicate

Status	Username	Description	First Name	Last Name	Email Address
<input type="checkbox"/>	Enabled	👤 employee			
<input type="checkbox"/>	Enabled	👤 engineer			

✓ Chuyển hướng đến Work Centers / Guest Access / Identity Groups / User Identity Groups

✓ Name: Guest

☰ Cisco ISE

Work Centers · Guest Access

Overview Identities **Identity Groups** Ext Id Sources Administration Network Devices

Identity Groups

User Identity Groups > Guest

Identity Group

* Name

Description

✓ Member User: chọn engineer

The screenshot shows the 'Member Users' management interface. At the top, the title 'Member Users' is highlighted with a red box. Below it, there are controls for 'Add' and 'Delete', and a status filter set to 'All'. A table lists users with columns for 'Status', 'Email', 'Username', and 'First Name'. The first user is 'engineer', with a status of 'Enabled', which is also highlighted with a red box.

Chuyển hướng đến Work Centers / Guest Access / Identity Groups / User Identity Groups

✓ Name: Staff

✓ Member User: chọn employee

The screenshot shows the Cisco ISE configuration interface. The navigation menu includes 'Work Centers' and 'Guest Access', both highlighted with red boxes. The 'Identity Groups' tab is selected. On the left, a sidebar shows 'User Identity Groups' highlighted with a red box. The main area shows the configuration for the 'Staff' identity group, with the name 'Staff' entered in the '* Name' field and highlighted with a red box. There are 'Save' and 'Reset' buttons at the bottom.

Member Users

Users Selected 0 Total 1

+ Add Delete All

Status	Email	Username	First Name	Last
<input checked="" type="checkbox"/> Enabled		employee		

- ✓ Chuyển hướng đến Work Centers / Trust Set / Components / Trustsec
AAA Servers / AAA Server
- ✓ Name: CISCOISE
- ✓ IP: 192.168.20.100

Cisco ISE Work Centers · TrustSec

Overview **Components** TrustSec Policy Policy Sets SXP ACI Troubleshoot Reports Settings

Security Groups
 IP SGT Static Mapping
 Security Group ACLs
 Network Devices

Trustsec Servers

Trustsec AAA Servers

HTTPS Servers

AAA Servers List > CISCOISE

AAA Servers

* Name **CISCOISE**

Description

* IP **192.168.20.100** (Example: 10.1.1.1)

* Port 1812 (Valid Range 1 to 65535)

- ✓ Chuyển hướng đến Work Centers / TrustSec / Component / Network
Devices
- ✓ Name: SW
- ✓ IP Address: 192.168.20.150

Work Centers · TrustSec

Overview Components TrustSec Policy Policy Sets SXP ACI Troubleshoot Reports Settings

Security Groups
IP SGT Static Mapping
Security Group ACLs
Network Devices
Trustsec Servers >

Network Devices List > SW

Network Devices

Name	SW
Description	LAB SW
IP Address	192.168.20.150 / 32

- ✓ Tick vào RADIUS
- ✓ Shared Secret

RADIUS Authentication Settings

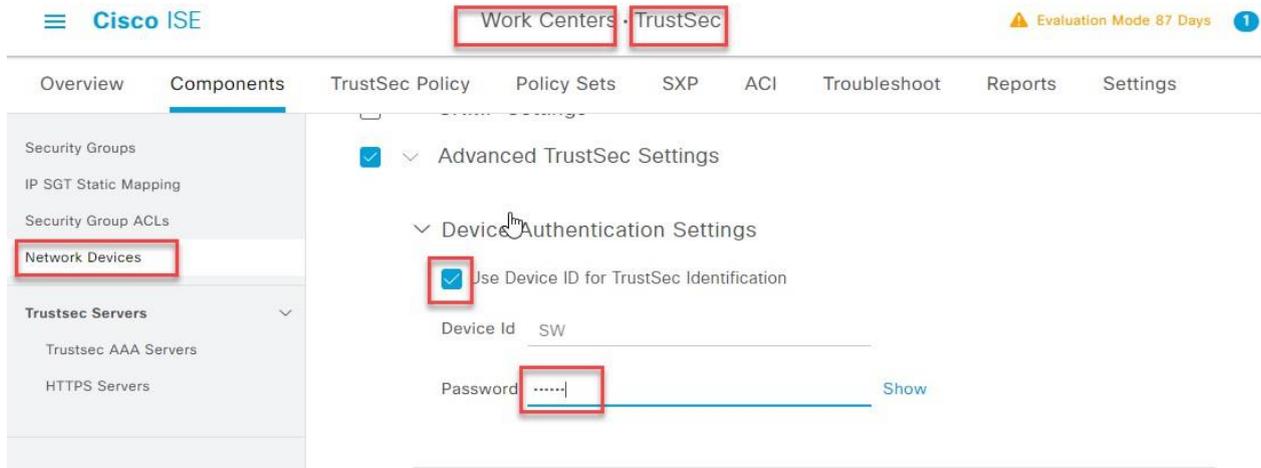
RADIUS UDP Settings

Protocol **RADIUS**

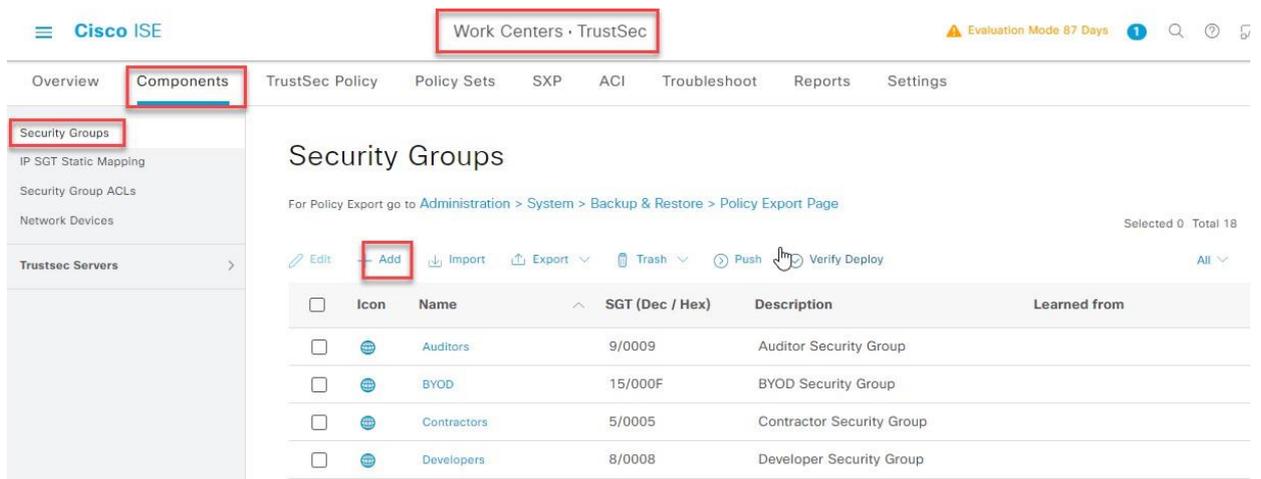
Shared Secret **....** Show

Use Second Shared Secret ⓘ

- ✓ Chuyển hướng đến Work Center / TrustSec Network Devices /
- ✓ Tick vào Advanced TrustSec Settings
- ✓ Tick vào Use Device ID for TrustSec Identification



- ✓ Chuyển hướng đến Work Centers / TrustSec / Components / Security Group / +Add
- ✓ Tạo 2 Security Groups: guest và Staff



<input type="checkbox"/>		Auditors	9/0009	Auditor Security Group
<input type="checkbox"/>		BYOD	15/000F	BYOD Security Group
<input type="checkbox"/>		Contractors	5/0005	Contractor Security Group
<input type="checkbox"/>		Developers	8/0008	Developer Security Group
<input type="checkbox"/>		Development_Servers	12/000C	Development Servers Security Group
<input type="checkbox"/>		Employees	4/0004	Employee Security Group
<input type="checkbox"/>		Guest	16/0010	Guest
<input type="checkbox"/>		Guests	6/0006	Guest Security Group
<input type="checkbox"/>		Point_of_Sale_Systems	10/000A	Point of Sale Security Group
<input type="checkbox"/>		Production_Servers	11/000B	Production Servers Security Group
<input type="checkbox"/>		Production_Users	7/0007	Production User Security Group
<input type="checkbox"/>		Quarantined_Systems	255/00FF	Quarantine Security Group
<input type="checkbox"/>		Staff	17/0011	Staff
<input type="checkbox"/>		Test_Servers	13/000D	Test Servers Security Group
<input type="checkbox"/>		TrustSec_Devices	2/0002	TrustSec Devices Security Group
<input type="checkbox"/>		Unknown	0/0000	Unknown Security Group

- ✓ Chuyển hướng đến Policy / Policy Sets / +Add
- ✓ Policy Name: SGT 802.1X Test
- ✓ Condition: Wired_802.1X
- ✓ Allowed Protocols / Server Sequence: Default Network Access

Cisco ISE Policy · Policy Sets Evaluation Mode 87 Days 1

Policy Sets Reset

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	SGT 802.1X Test		Wired_802.1X	Default Network Access			
	Default	Default policy set		Default Network Access	0		

- ✓ Mục Authentication Policy:
- ✓ Rule name: 802.1X
- ✓ Conditions: Wired_802.1X

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	802.1X	Wired_802.1X	Internal Users > Options		

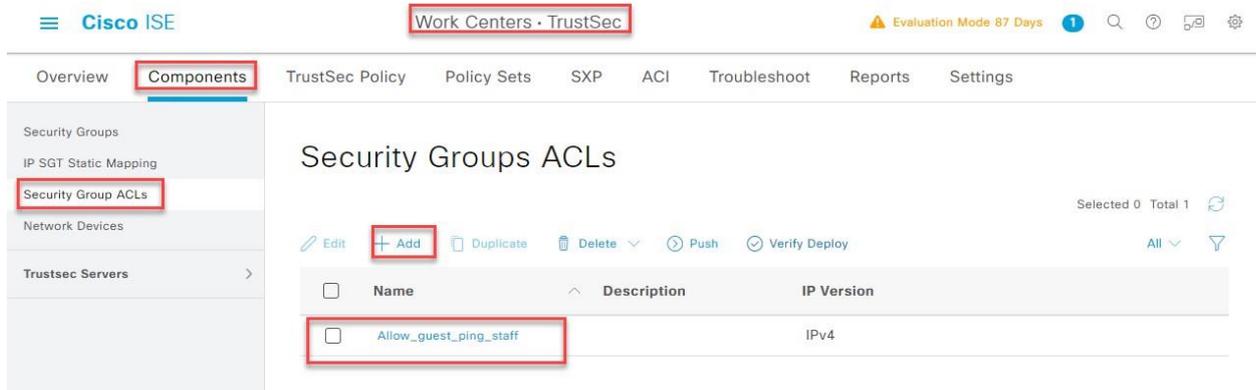
Authorization Policy:

- ✓ Rule Name: Guest
- ✓ Conditions: InternalUser-IdentityGroup EQUALS User Identity
Groups:Guest
- ✓ Profile: VLAN_10
- ✓ Security Groups: Guest
- ✓ Tương tự với Staff

Authorization Policy (3)

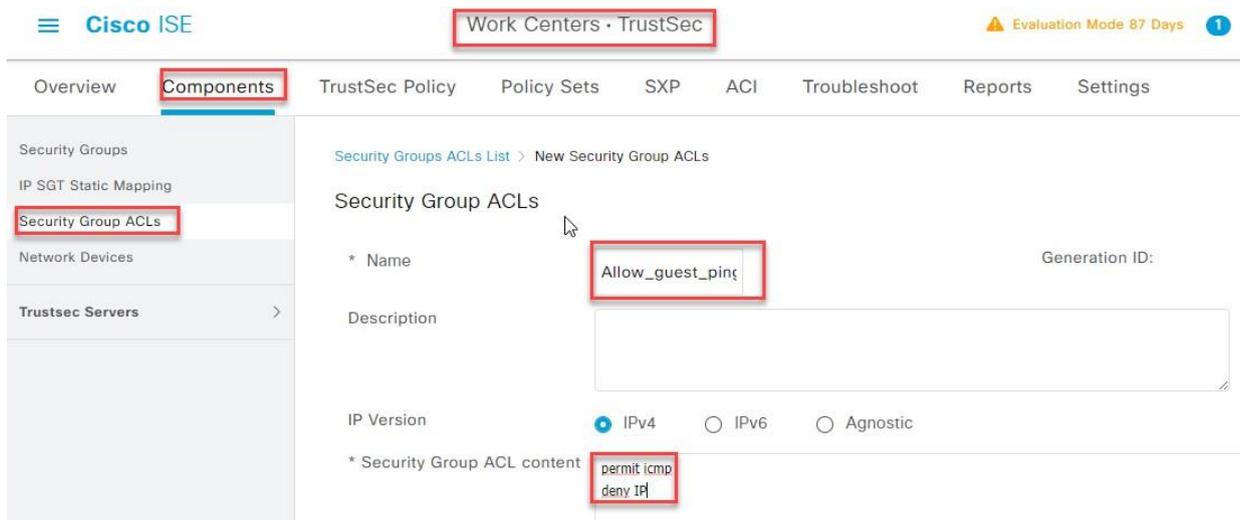
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	Guest	InternalUser-IdentityGroup EQUALS User Identity Groups:Guest	VLAN_10	Guest	0	
✓	Staff	InternalUser-IdentityGroup EQUALS User Identity Groups:Staff	VLAN_10	Staff	0	

- ✓ Work Centers / TrustSec / Components / Security Group ACLs / +Add /
- ✓ Name: Allow_guest_ping_staff



Security Group ACL content:

- ✓ permit icmp
- ✓ deny IP



- ✓ Work Centers / TrustSec / Components / Security Group ACLs
- ✓ Name: Allow_staff_remove_guest
- ✓ Description: cho phép staff remote guest
- ✓ Security Group ACL content:
 - permit tcp dst eq 3389
 - permit icmp
 - deny IP

The screenshot shows the Cisco ISE interface for configuring a Security Group ACL. The breadcrumb trail is Work Centers > TrustSec > Components > Security Group ACLs. The configuration form includes:

- Name:** Allow_staff_remc
- Description:** Cho phép staff remote guest
- IP Version:** IPv4 (selected)
- Security Group ACL content:** permit tcp dst eq 3389, permit icmp, deny IP

The screenshot shows the Cisco ISE interface for configuring a TrustSec Policy. The breadcrumb trail is Work Centers > TrustSec > TrustSec Policy. The configuration page displays a matrix for the policy:

Source	Auditors (9/0009)	BYOD (15/000F)	Contractors (5/0005)	Developers (8/0008)	Development_Ser... (12/000C)	Employees (4/0004)	Guest (16/0010)	Guests (6/0006)	Network_S (3/0003)	PCL_Server (14/000E)
Auditors (9/0009)										
BYOD (15/000F)										
Contractors (5/0005)										
Developers (8/0008)										
Development_Ser... (12/000C)										
Employees (4/0004)										

At the bottom, the policy is set to **Enabled** with a description: Default egress rule.

Trên Switch Cisco 3560X: cấu hình xác thực 802.1x với Cisco ISE và nhận các policy từ ISE.

```
interface g0/2

no shut

no switchport

ip add 192.168.20.1 255.255.255.0

exit

ip dhcp pool LAN

network 192.168.20.0 255.255.255.0

default-router 192.168.20.1

dns-server: 8.8.8.8

aaa new-model

aaa group server radius AAASERVER

server name CISCOISE

aaa authentication login default local

aaa authentication dot1x default group radius

aaa authorization network default group AAASERVER

aaa authorization network SGLIST group radius
```

```
aaa authorization auth-proxy default group AAASERVER
```

```
aaa accounting dot1x default start-stop group AAASERVER
```

```
aaa server radius policy-device
```

```
aaa server radius dynamic-author
```

```
client 192.168.20.100 server-key Admin123
```

```
dot1x system-auth-control
```

```
interface GigabitEthernet0/3
```

```
switchport mode access
```

```
authentication port-control auto
```

```
dot1x pae authenticator
```

```
interface GigabitEthernet0/4
```

```
switchport mode access
```

```
authentication port-control auto
```

```
dot1x pae authenticator
```

```
interface GigabitEthernet0/5
```

```
switchport mode access
```

```
authentication port-control auto
```

```
dot1x pae authenticator
```

```
radius-server attribute 6 on-for-login-auth  
radius-server attribute 6 support-multiple  
radius-server attribute 8 include-in-access-req  
radius-server attribute 25 access-request include
```

```
radius server CISCOISE  
  
address ipv4 192.168.20.100 auth-port 1812 acct-port 1813  
  
pac key Admin123
```

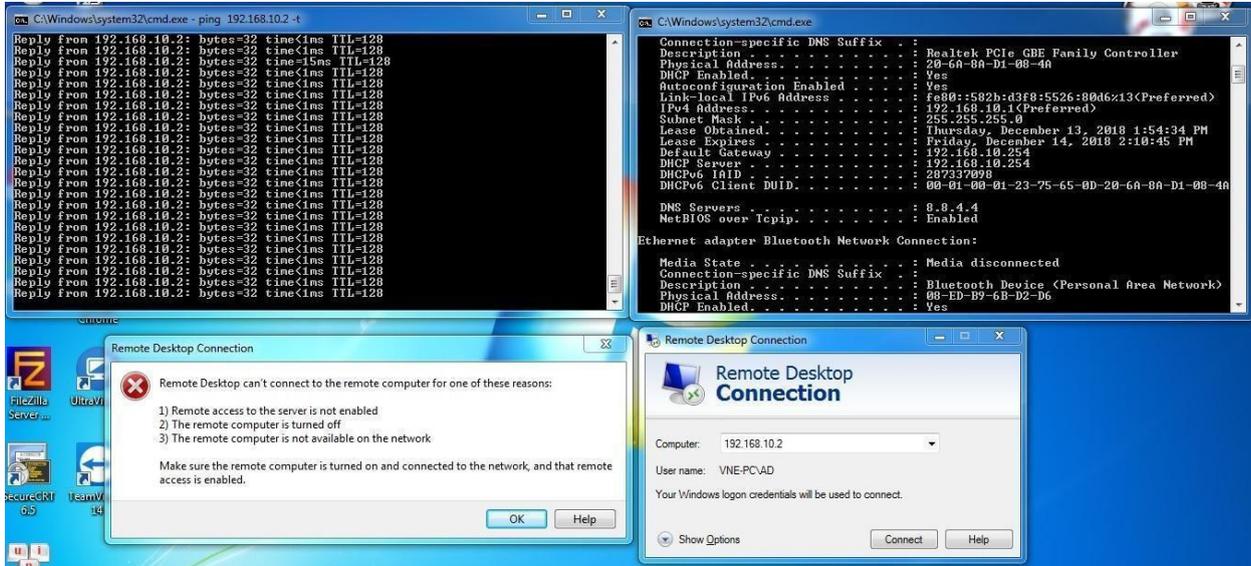
Kết quả:

Trên switch kiểm tra các rule nhận được từ ISE:

```
Switch#show cts role-based permissions  
  
IPv4 Role-based permissions default:  
  
    Permit IP-00  
  
IPv4 Role-based permissions from group 17:guest to group 16:staff:  
  
    Deny_guest_remote_staff-10  
  
IPv4 Role-based permissions from group 16:staff to group 17:guest:  
  
    Allow_staff_remote_guest-40  
  
RBACL Monitor All for Dynamic Policies : FALSE  
RBACL Monitor All for Configured Policies : FALSE
```

Guest chỉ có thể ping sang Staff, còn Staff thì có full quyền có thể remote sang Guest mặc dù cả 2 đang trong cùng lớp mạng Vlan 10.

User Guest: ping thông, remote không được.



User Staff: ping thông, remote thông.

