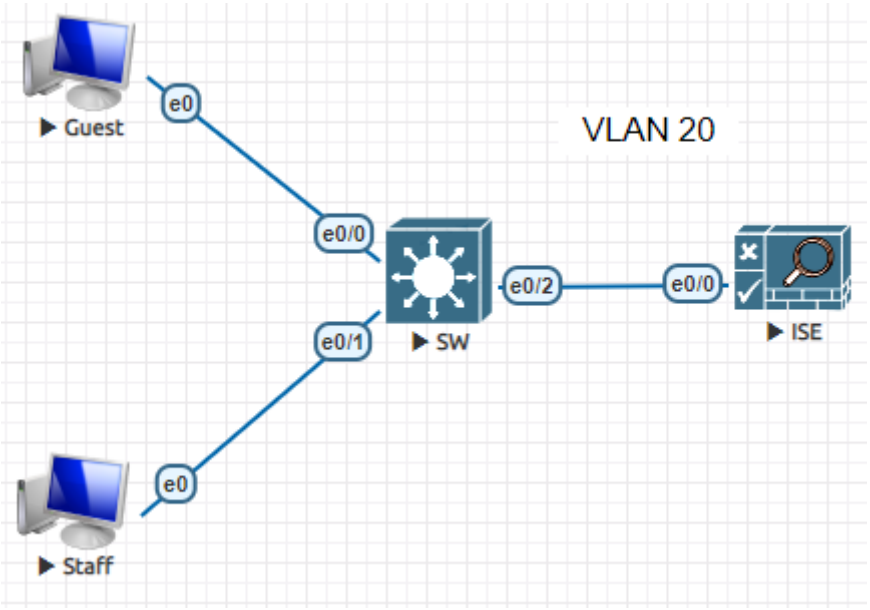
LAB - CISCO ISE TRUSTSEC

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

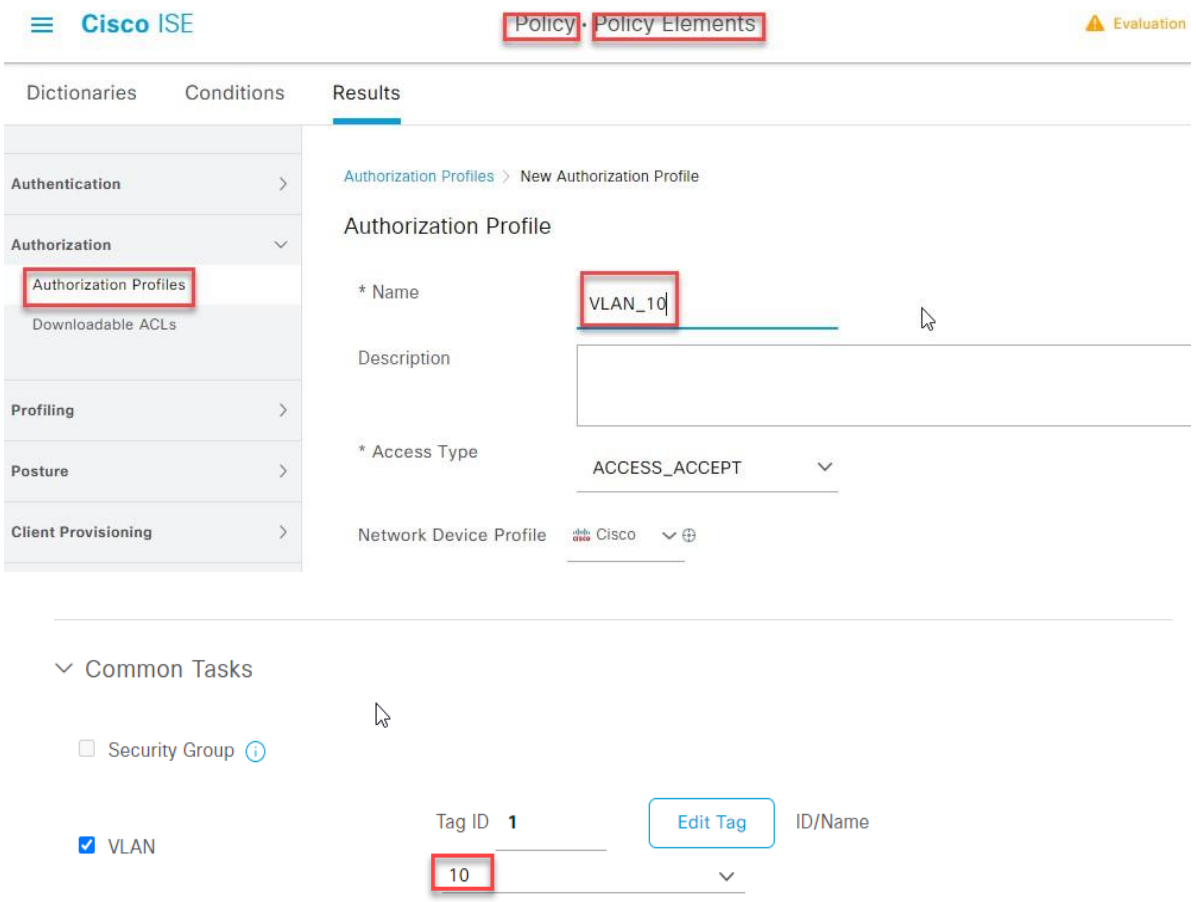
Sau khi xác thực bằng 802.1X, 2 users đc gán Vlan 10 và vào 2 security group VNE-staff, VNE-guest

✓ Áp policy:

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

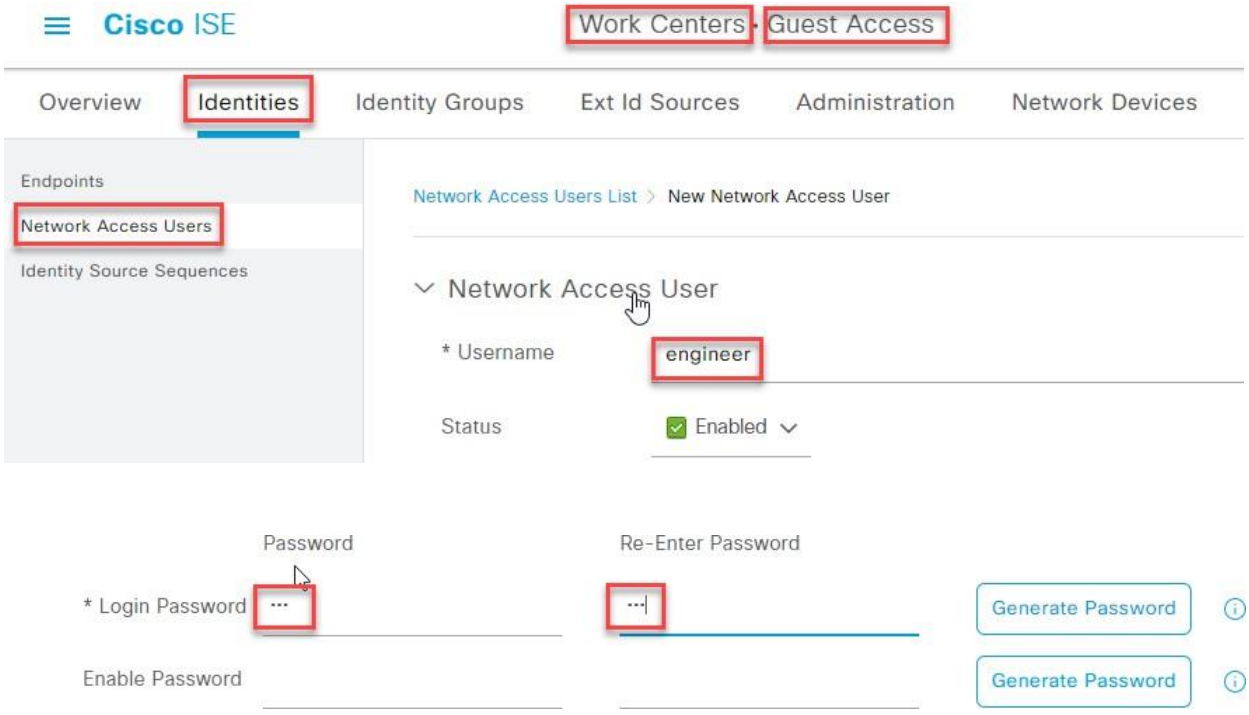
VNE-guest to VNE-staff (chỉ được Ping)

- ✓ **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

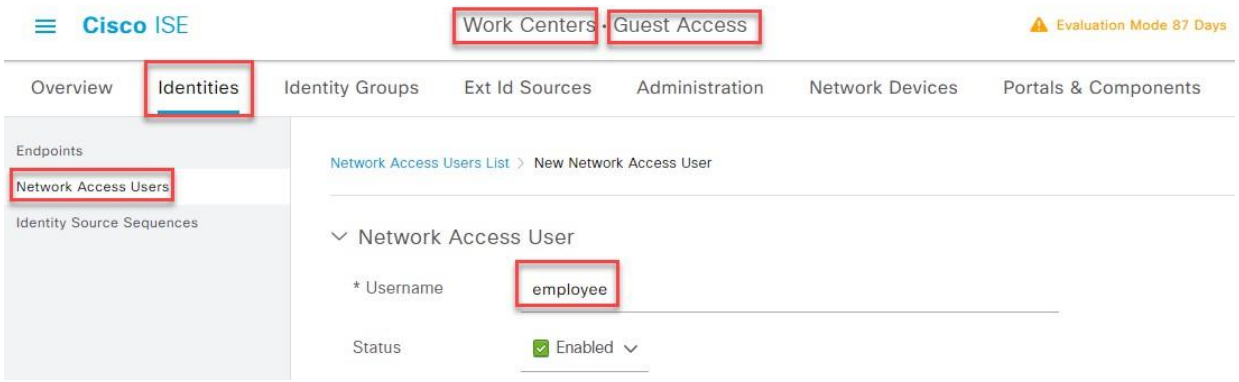


✓ Ta chuyển hướng Work Centers / Guest Access / Identity / Network Access Users

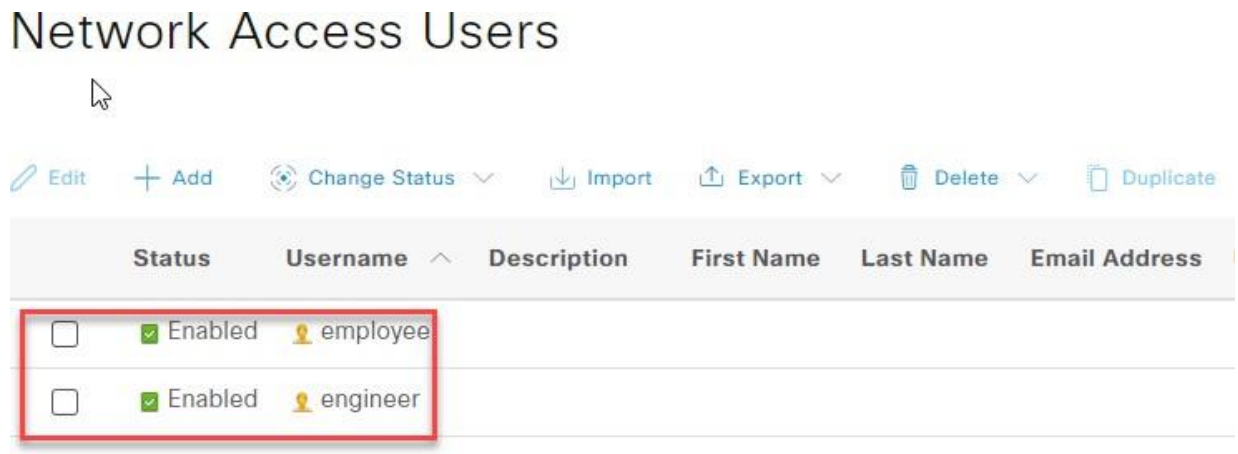
✓ Username: engineer



✓ Username: engineer

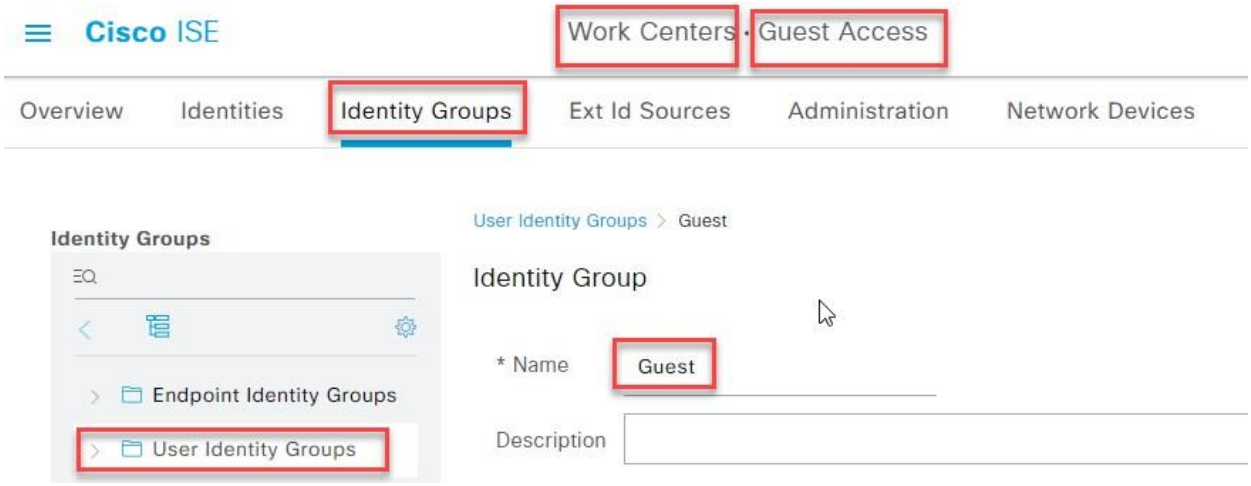


✓ Ta đã tạo được 2 user:

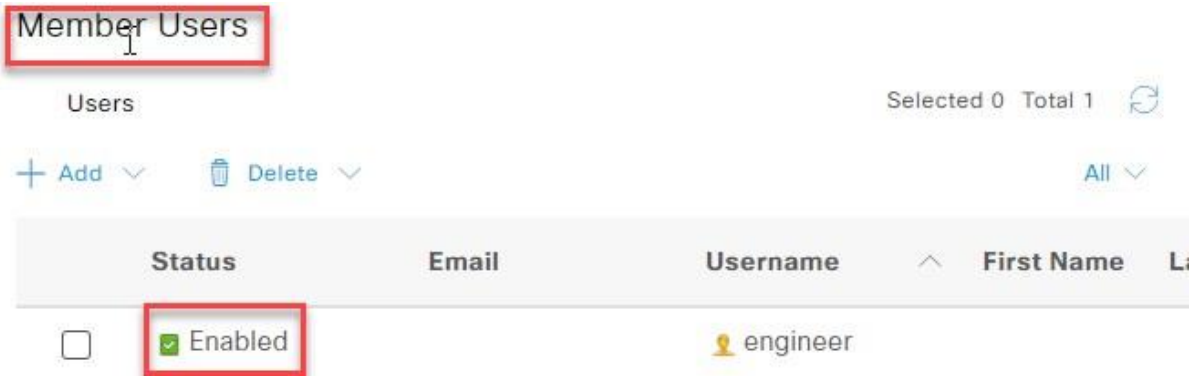


✓ Chuyển hướng đến Work Centers / Guest Access / Identity Groups / User Identity Groups

✓ Name: Guest



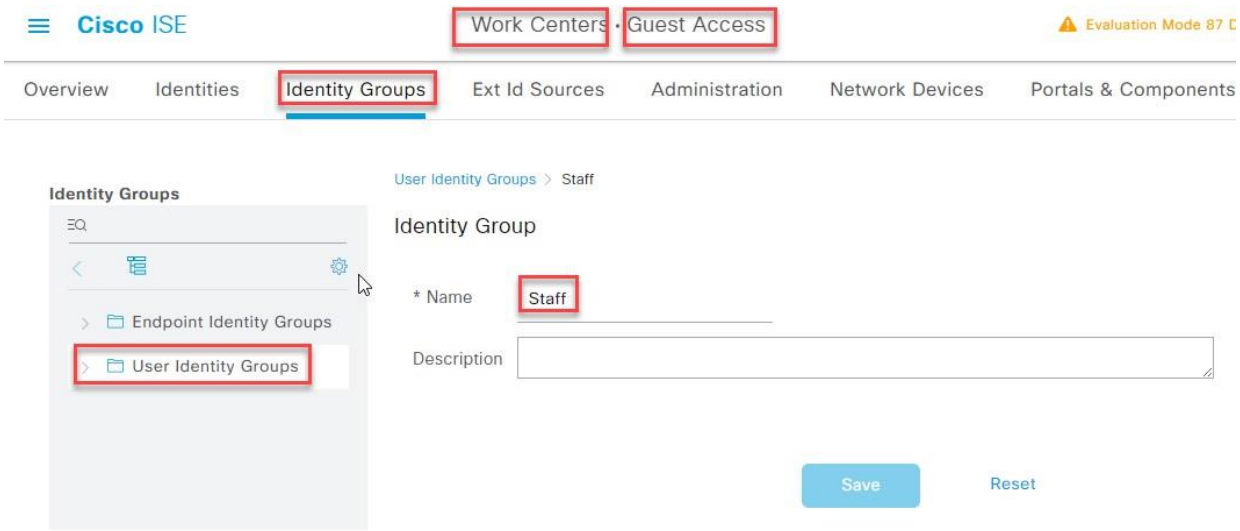
✓ Member User: chọn engineer

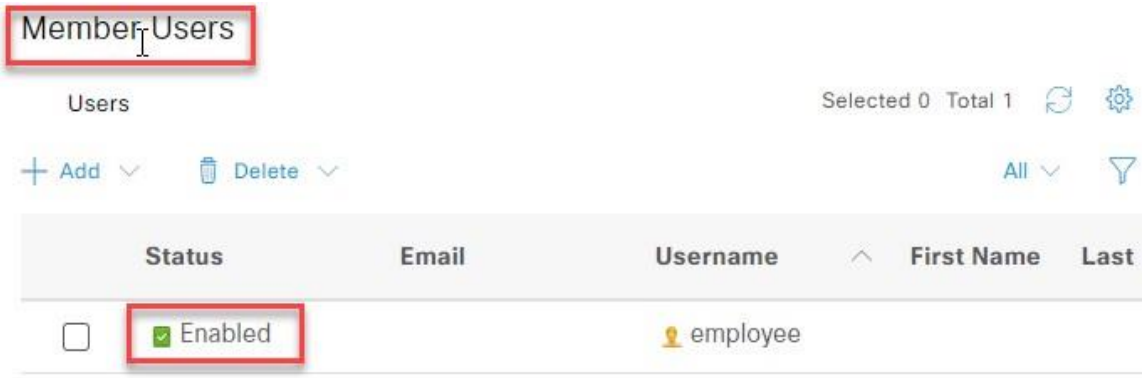


Chuyển hướng đến Work Centers / Guest Access / Identity Groups / User Identity Groups

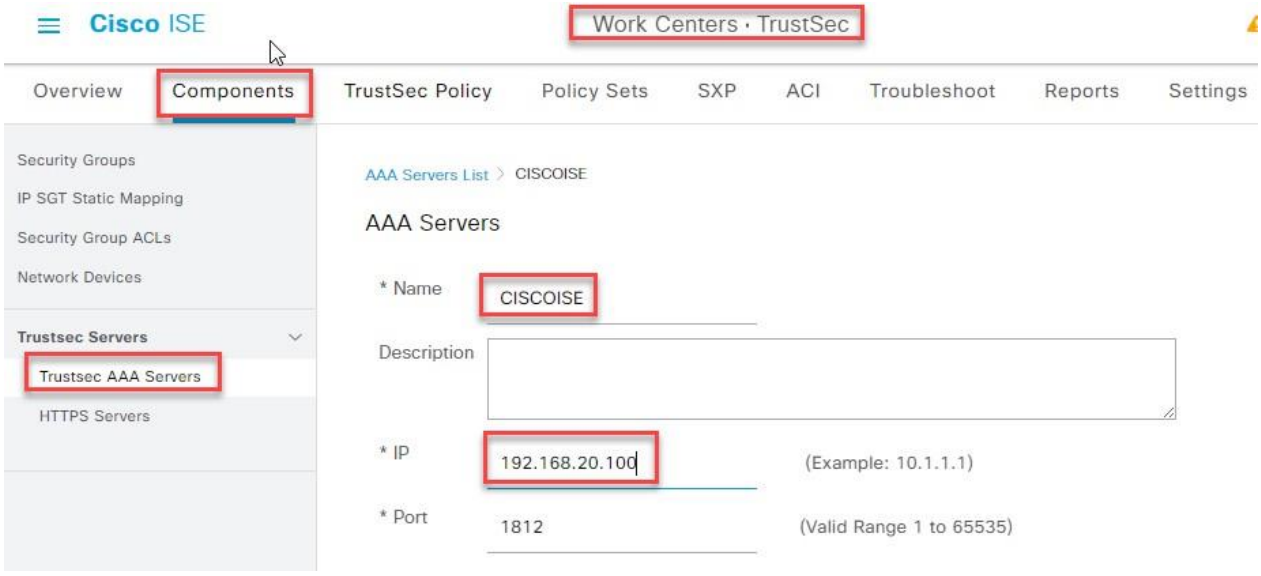
✓ Name: Staff

✓ Member User: chọn employee

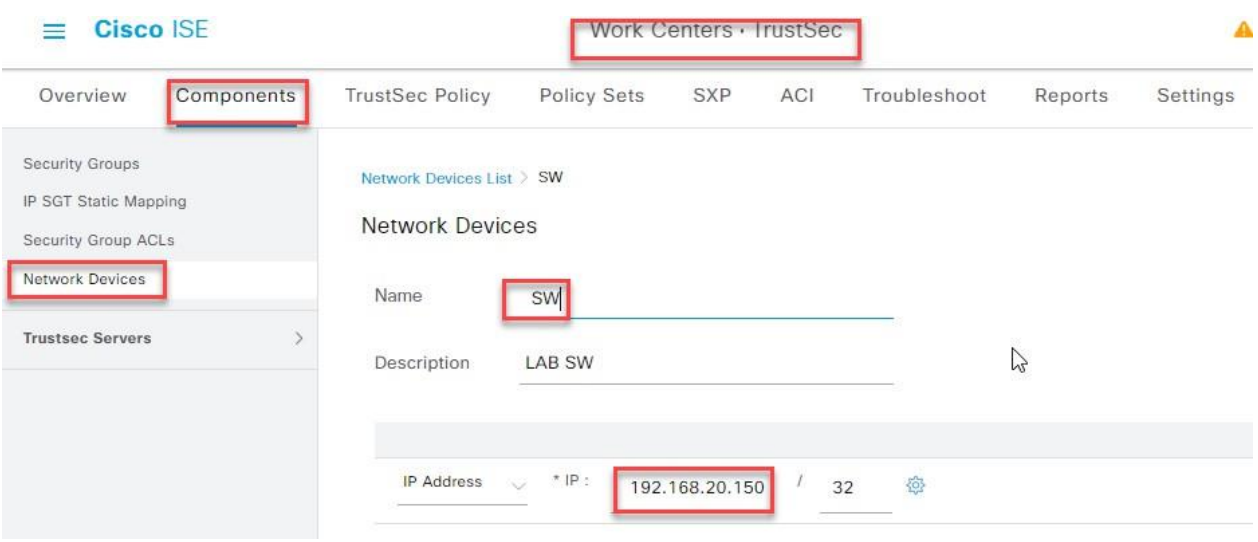




- ✓ Chuyển hướng đến Work Centers / Trust Set / Components / Trustsec AAA Servers / AAA Server
- ✓ Name: CISCOISE
- ✓ IP: 192.168.20.100

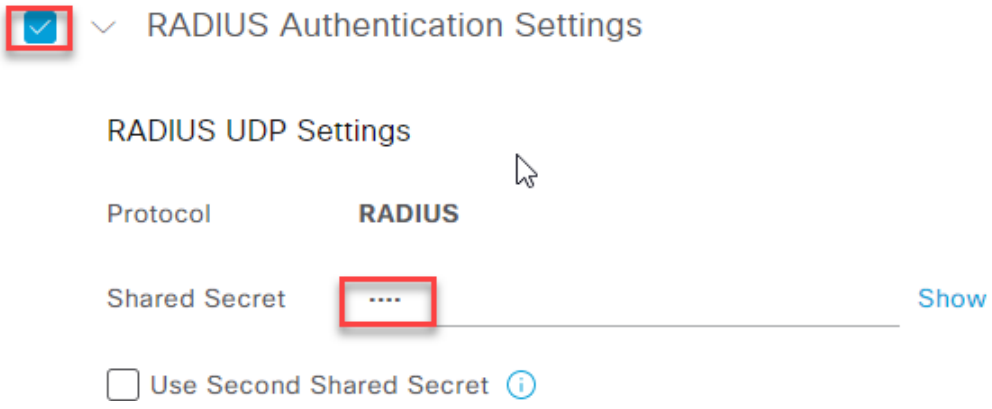


- ✓ Chuyển hướng đến Work Centers / TrustSec / Component / Network Devices
- ✓ Name: SW
- ✓ IP Address: 192.168.20.150



✓ Tick vào RADIUS

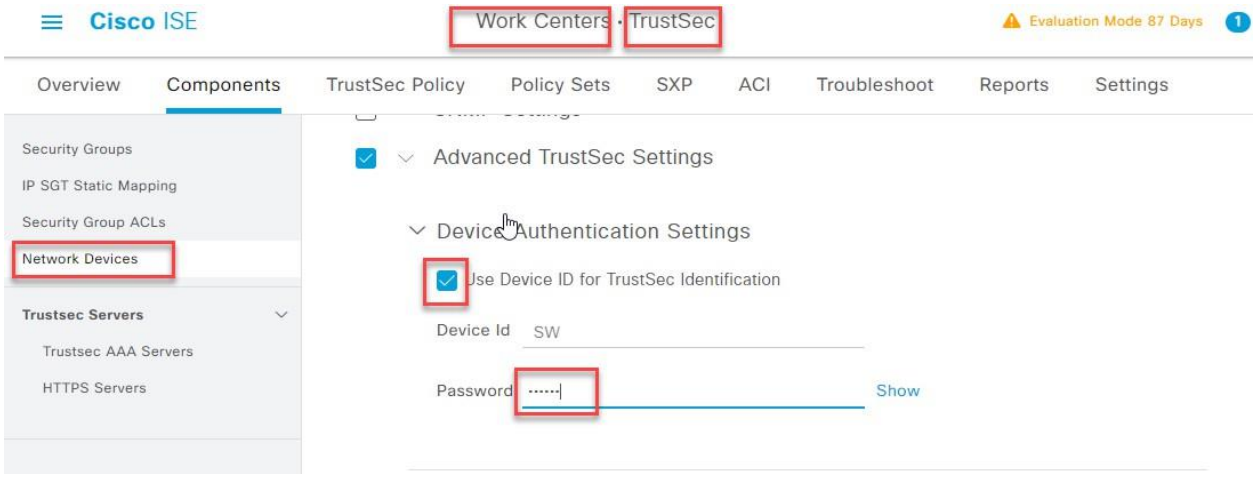
✓ Shared Secret



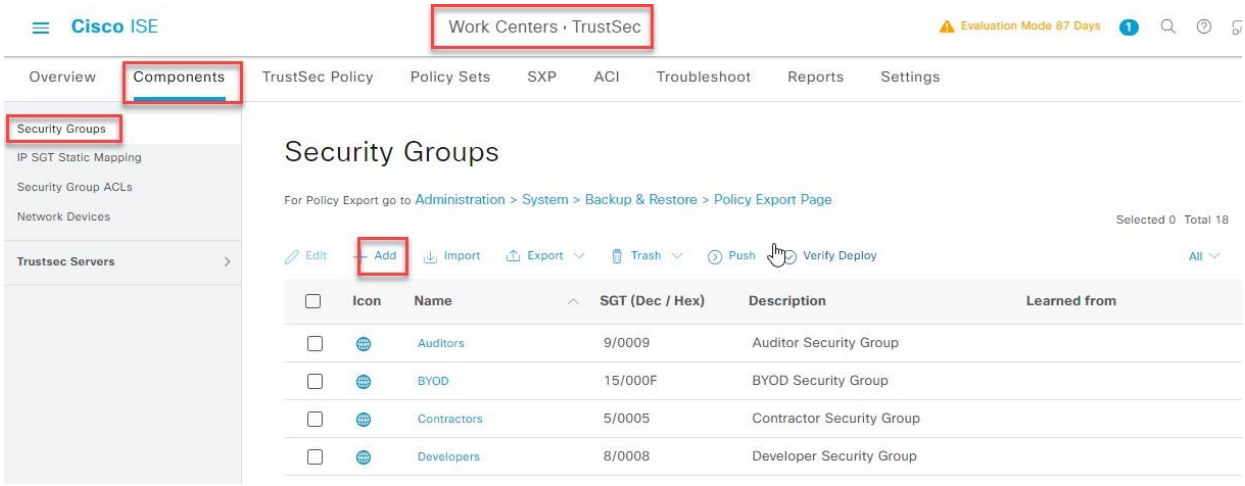
✓ Chuyển hướng đến Work Center / TrustSec Network Devices /

✓ Tick vào Advanced TrustSec Settings

✓ Tick vào Use Device ID for TrustSec Identification

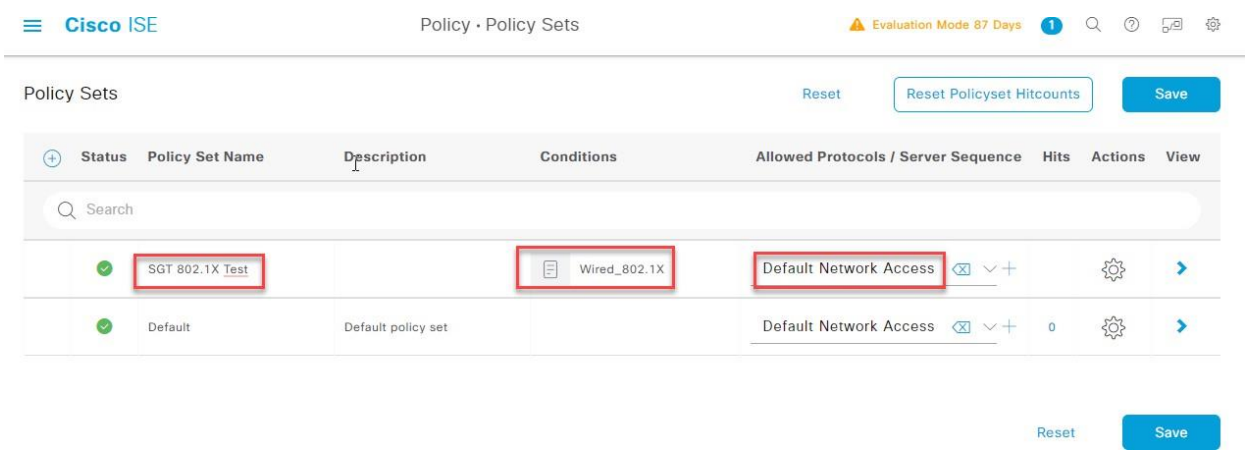


- ✓ Chuyển hướng đến Work Centers / TrustSec / Components / Security Group / +Add
- ✓ Tạo 2 Security Groups: guest và Staff

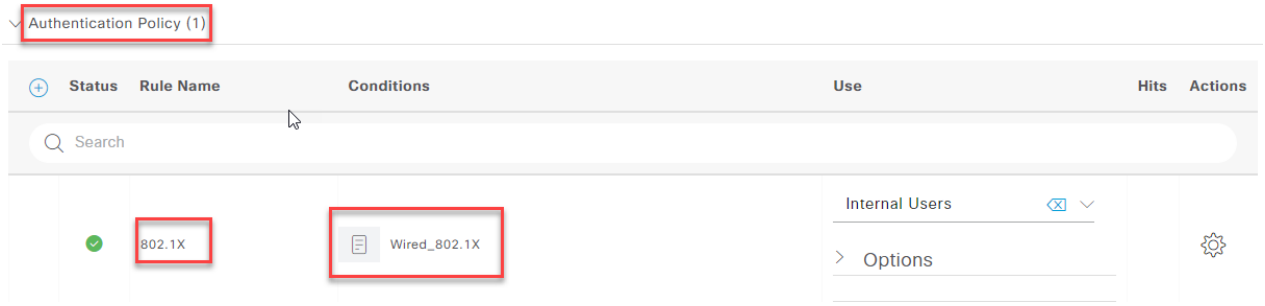


Auditors	9/0009	Auditor Security Group
BYOD	15/000F	BYOD Security Group
Contractors	5/0005	Contractor Security Group
Developers	8/0008	Developer Security Group
Development_Servers	12/000C	Development Servers Security Group
Employees	4/0004	Employee Security Group
Guest	16/0010	Guest
Guests	6/0006	Guest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

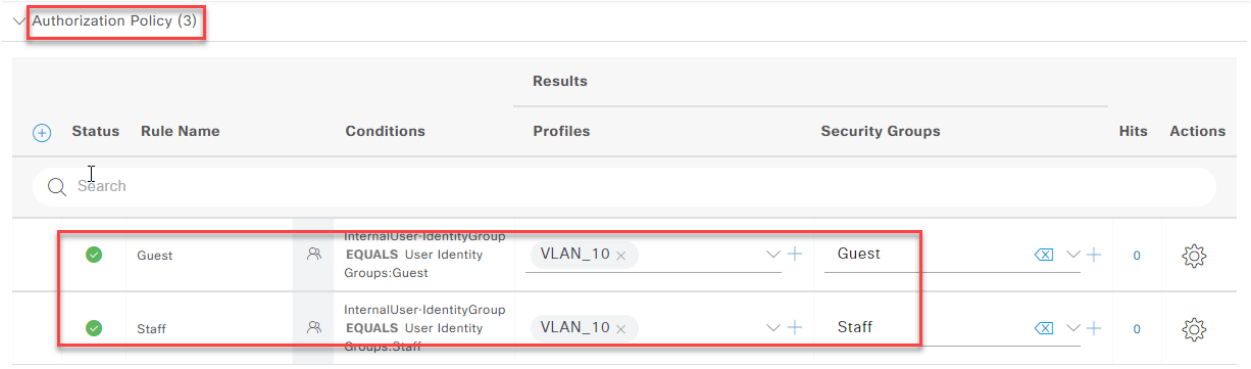


- ✓ Mục Authentication Policy:
- ✓ Rule name: 802.1X
- ✓ Conditions: Wired_802.1X

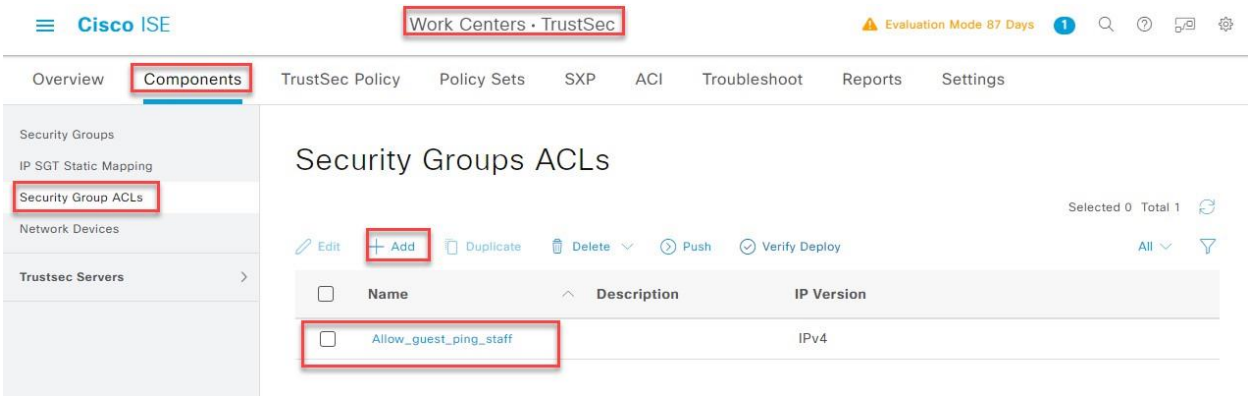


Authorization Policy:

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

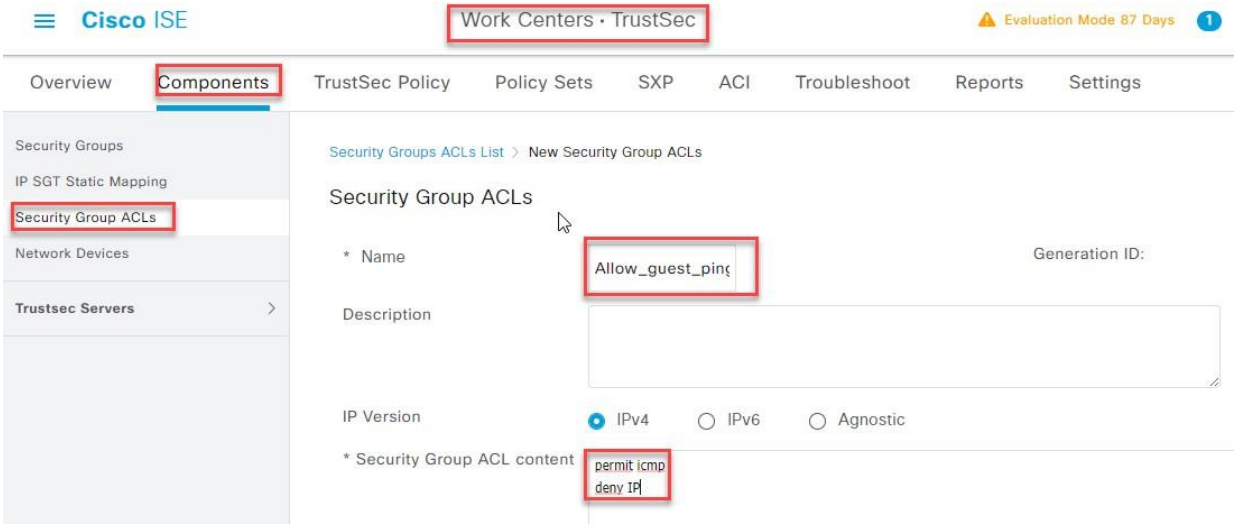


- ✓ Work Centers / TrustSec / Components / Security Group ACLs / +Add /
- ✓ Name: Allow_guest_ping_staff

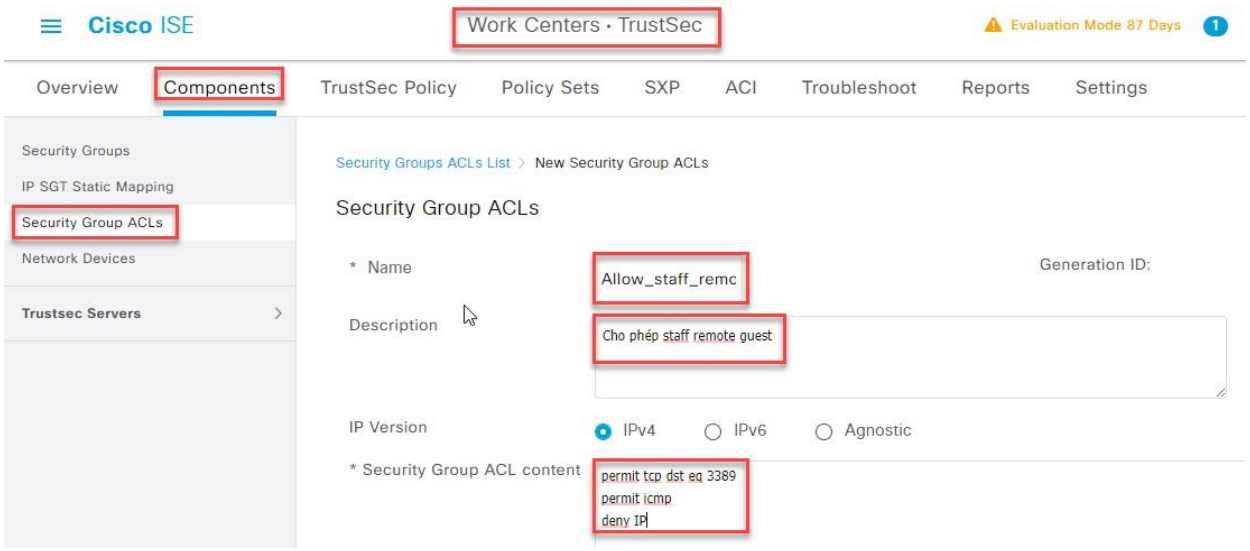


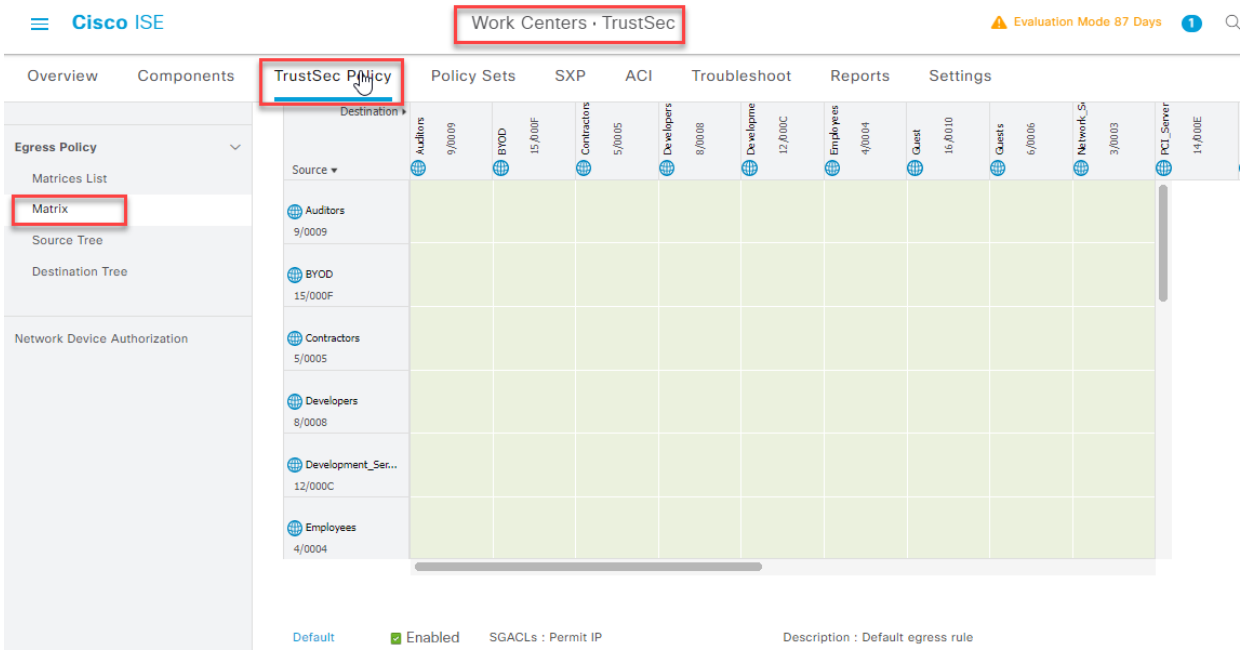
Security Group ACL content:

- ✓ 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





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
```

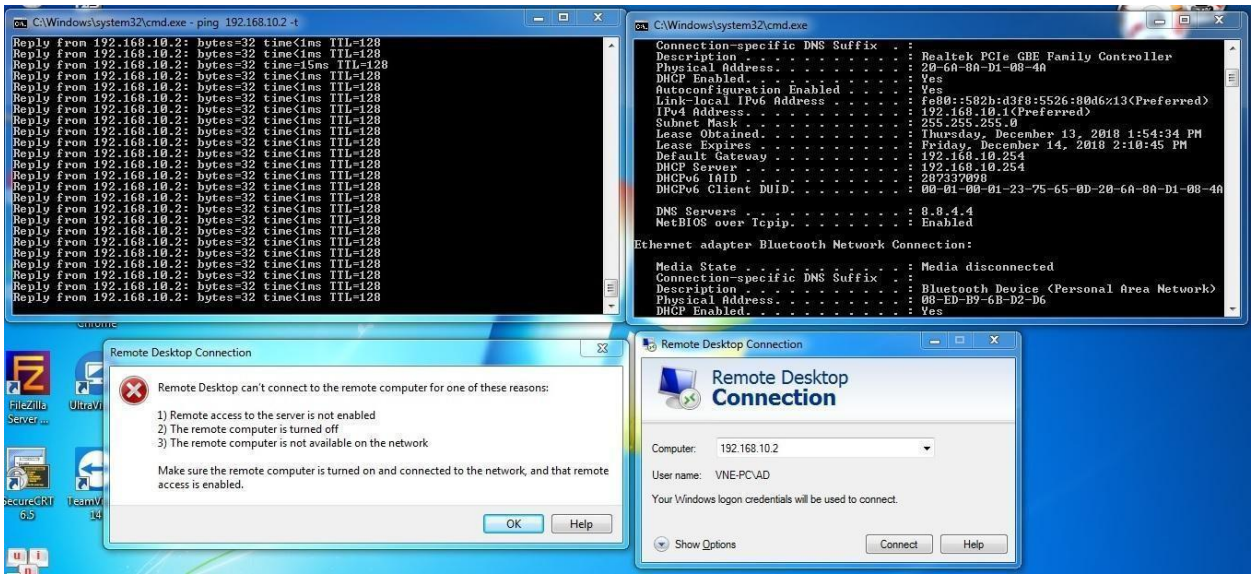
Kết quả:

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.