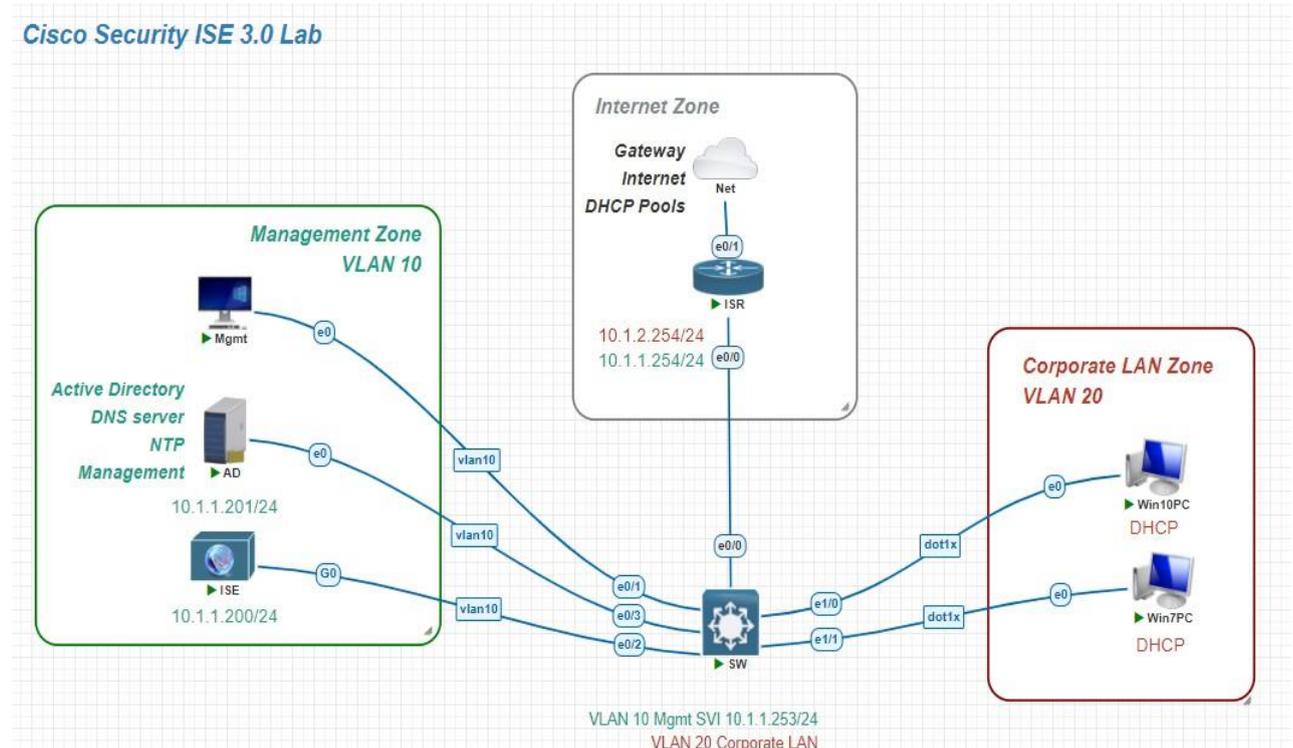
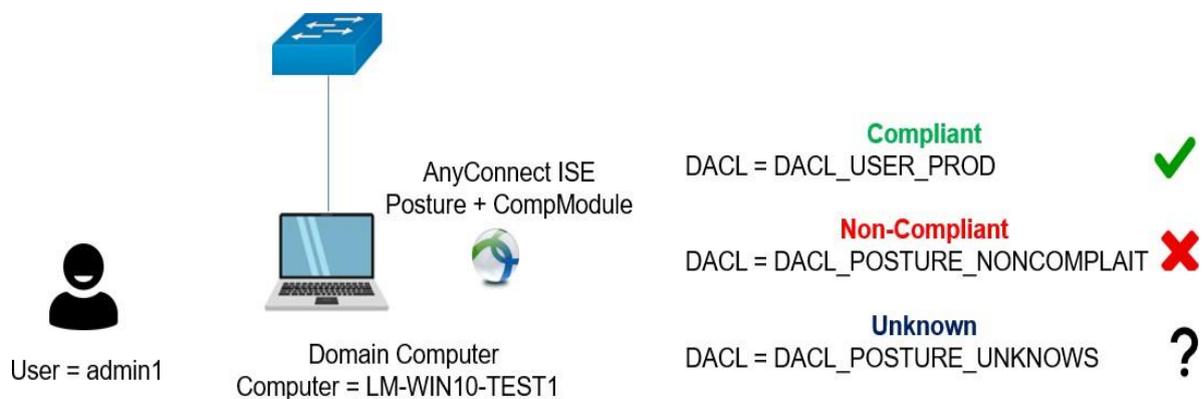


LAB - POSTURE

I. Sơ đồ:



II. Mục đích thực hiện:



Trong trường hợp này, Ta giả sử đang có một thiết bị muốn truy cập vào hệ thống mạng của công ty. Đầu tiên, ISE sẽ chặn tất cả lưu lượng không phải WEB cho đến khi ISE nhận được, Thiết bị đó sẽ redirect đến ISE Provisioning Portal và download anyconnect về, và anyconnect sẽ quét các product trong Thiết bị xem có đáp ứng yêu cầu của ISE hay không và tiến hành cho phép truy cập hệ thống.

Quy trình tạo ra Posture :

1 Posture Conditions => 2 Posture Remediations => 3 Posture Requirement => 4 Posture Policy => 5 Client Provision => 6 Posture Policy

Posture Conditions là tập hợp các quy tắc trong **chính sách bảo mật** nhằm xác định một điểm cuối tuân thủ. Một số mục này bao gồm cài đặt tường lửa, phần mềm chống virus, chống phần mềm độc hại, các bản sửa lỗi, mã hóa ổ đĩa và hơn thế nữa.

Sau khi các **Posture Conditions** được xác định, các biện pháp **Posture Remediation** (nếu cần) có thể được định cấu hình. **Posture Remediation** là phương pháp **AnyConnect** sẽ xử lý các điểm cuối không tuân thủ. Một số biện pháp khắc phục có thể được giải quyết tự động thông qua AnyConnect trong khi các biện pháp khác có thể được người dùng cuối giải quyết theo cách thủ công.

Posture Requirement là các bước hành động tức thì được **AnyConnect** thực hiện khi một điểm cuối không tuân thủ. Một điểm cuối được coi là tuân thủ nếu nó thỏa mãn tất cả các điều kiện về tư thế.

Sau khi được định cấu hình, các **Posture Requirement** sau đó có thể được tham chiếu bởi **Posture Policy** để thực thi tuân thủ. **Client Provision** là chính sách được sử dụng để xác định phiên bản **AnyConnect** được sử dụng cũng như mô-đun tuân thủ sẽ được cài đặt trên điểm cuối trong quá trình cung cấp. Mô-đun tuân thủ là một thư viện mà tác nhân tư thế sử dụng để xác định xem điểm cuối có tuân thủ các điều kiện tư thế xác định hay không. Cuối cùng.

Cuối cùng, **Policy access** sẽ cho **Posture Policy** của chúng tôi và xác định dạng chính sách nào mà điểm cuối sẽ phải tuân theo nếu nó tuân thủ, không tuân thủ hoặc yêu cầu cung cấp AnyConnect.

III. Thực hiện:

1. Cấu hình Download ACL:

✓ Name: LM_COMPUTER

✓ DACL: permit ip any any

The screenshot shows the Cisco ISE interface for configuring a Downloadable ACL. The left sidebar has 'Downloadable ACLs' selected. The main area shows the configuration for 'LM_COMPUTER'. The 'Name' field is 'LM_COMPUTER', the 'IP version' is 'IPv4', and the 'DACL Content' is 'permit ip any any'. The breadcrumb path is 'Downloadable ACL List > LM_COMPUTER'.

2. Cấu hình Authorization Profiles:

The screenshot shows the Cisco ISE interface for configuring an Authorization Profile. The left sidebar has 'Authorization Profiles' selected. The main area shows the configuration for 'WIRED_COMPUTER'. The 'Name' field is 'WIRED_COMPUTER' and the 'Access Type' is 'ACCESS_ACCEPT'. The breadcrumb path is 'Authorization Profiles > New Authorization Profile'.

Cisco ISE Work Centers · Posture

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy Policy Sets

Conditions >
Remediations >
Requirements
Allowed Protocols
Authorization Profiles
Downloadable ACLs

Common Tasks

DACL Name IPv6 DAACL Name ACL

LM_COMPUTER

✓ Name: LM_USER

✓ DAACL: permit ip any any

Cisco ISE Work Centers · Posture

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy

Conditions >
Remediations >
Requirements
Allowed Protocols
Authorization Profiles
Downloadable ACLs

Downloadable ACL List > New Downloadable ACL

Downloadable ACL

* Name LM_USER

Description

IP version IPv4 IPv6 Agnostic ⓘ

* DAACL Content 1234567 8910111 **permit ip any any**

Cisco ISE Work Centers · Posture

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy Policy Sets

Conditions >
Remediations >
Requirements
Allowed Protocols
Authorization Profiles
Downloadable ACLs

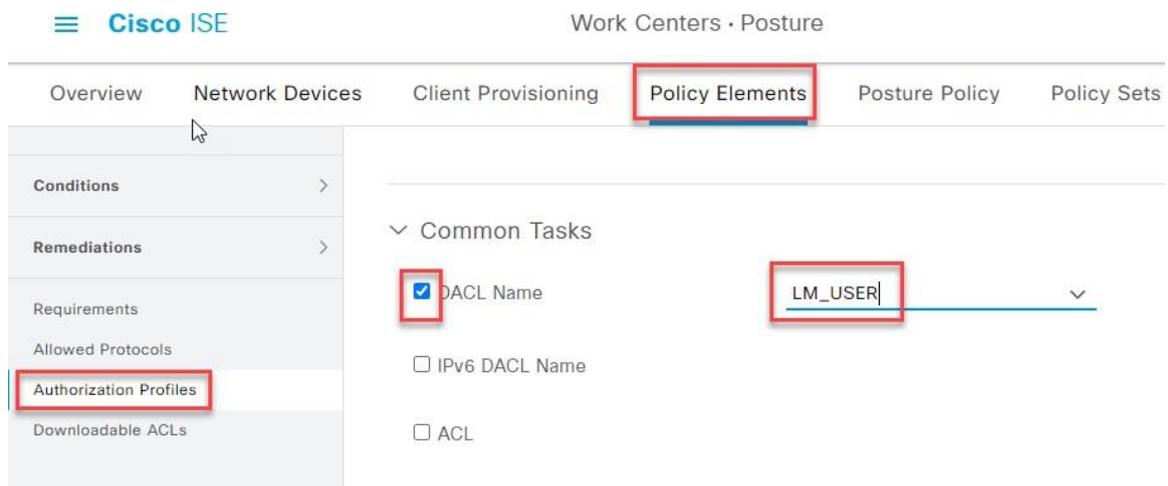
Authorization Profiles > New Authorization Profile

Authorization Profile

* Name WIRED_USER

Description

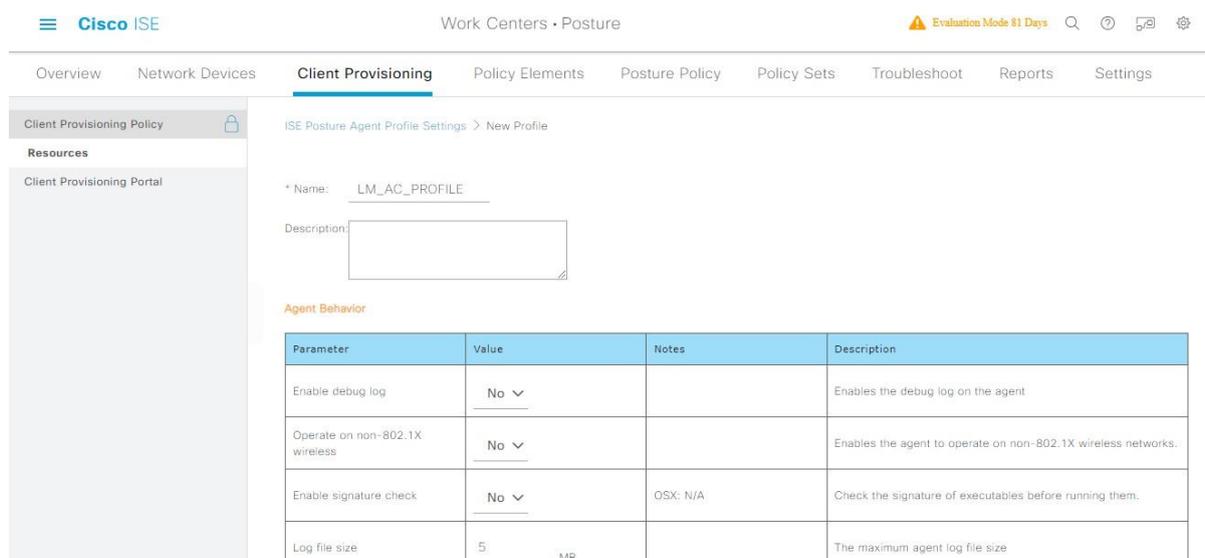
* Access Type ACCESS_ACCEPT



3. Cấu hình Client Provisioning:

3.1 Tạo AnyConnect Posture Profile:

- ✓ Vào Resource → +Add → Anyconnect Posture Profile
- ✓ Name: LM_AC_PROFILE
- ✓ Remediation timer: 10
- ✓ Server name rule: *.eve.lab



Cisco ISE Work Centers · Posture Evaluation Mode 78 Days

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy

Resources

Client Provisioning Portal

Agent Behavior

Parameter	Value	Notes	Description
Enable debug log	No		Enables the debug log on the agent
Operate on non-802.1X wireless	No		Enables the agent to operate on non-802.1X wireless networks.
Enable signature check	No	OSX: N/A	Check the signature of executables before running them.
Log file size	5 MB		The maximum agent log file size
Remediation timer	10 mins	Default Value of global setting : 4. Acceptable Range between 1 to 300. Accept only integer Values.	If the user fails to remediate within this specified time, mark them as non-compliant.

Cisco ISE Work Centers · Posture Evaluation Mode 81 Days

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy

Resources

Client Provisioning Portal

Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	120 secs		This is the agent retry period if there is a Passive Reasses communication failure
Retransmission Delay	60 secs	Default Value: 60. Acceptable Range between 5 to 300. Accept only integer Values.	Time (in seconds) to wait before retrying.
Retransmission Limit	4	Default value: 4. Acceptable Range between 0 to 10. Accept only integer Values.	Number of retries allowed for a message.
Discovery host		IPv4 or IPv6 addresses or FQDNs. IPv6 address should be without square brackets[]	The server that the agent should connect to
* Server name rules	*.eve.lab	need to be blank by default to force admin to enter a value. *** means agent will connect to all	A list of wildcarded, comma-separated names that define servers that the agent can connect to. E.g. "*.cisco.com"
		List of IPv4 or IPv6 addresses, FQDNs with or without port	

3.2 Tạo AnyConnect Configuration:

- ✓ Đầu tiên ta vào Resource , ta chọn +Add, chuyển đến mục Agent resource from local disk

Name	Version	Last Update	Description
Agent resources from local disk	Not Applicable	2022/11/05 15:11:28	
Native Supplicant Profile	4.8.176.0	2020/08/29 19:46:08	With CM: 4.3.838.6145
AnyConnect Configuration	Not Applicable	2016/10/06 20:01:12	Pre-configured Native Supplic...
AnyConnect Posture Profile	4.9.1095.0	2020/08/29 19:46:14	With CM: 4.3.1249.4353
AMP Enabler Profile	Not Applicable	2022/11/02 13:25:43	
LM_AC_PROFILE	Not Applicable	2022/11/06 08:33:12	
WinSPWizard 3.0.0.2	3.0.0.2	2020/08/29 19:46:06	Supplicant Provisioning Wizar...

✓ Trong mục Category: chọn mục Cisco Provided Package

✓ Chọn 2 file **AnyConnectDesktopWindows4.5**,

AnyConnectCompliantModule và lần lượt import vào

✓ Lưu ý: File Anyconnect Desktop và Compliant sẽ có sẵn trên các PC, chỉ cần chọn và import vào là được. 2 file này được dùng cho các user tải về khi họ truy cập vào hệ thống.

Cisco ISE Work Centers · Posture Evaluation Mode 81 Days

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy

Resources

Client Provisioning Portal

Client Provisioning Policy: `Client Provisioning Policy: anyconnect-win_deploy-k9.pkg`

AnyConnect Uploaded Resources

Name	Type	Version	Description
AnyConnectDesktopWindows 4.5...	AnyConnectDesktopWind...	4.5.3040.0	AnyConnect Secure Mobility C...

Submit Cancel

✓ Ta chọn Confirm

Cisco ISE Work Centers · Posture Evaluation Mode 81 Days

Overview Network Devices Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy

Resources

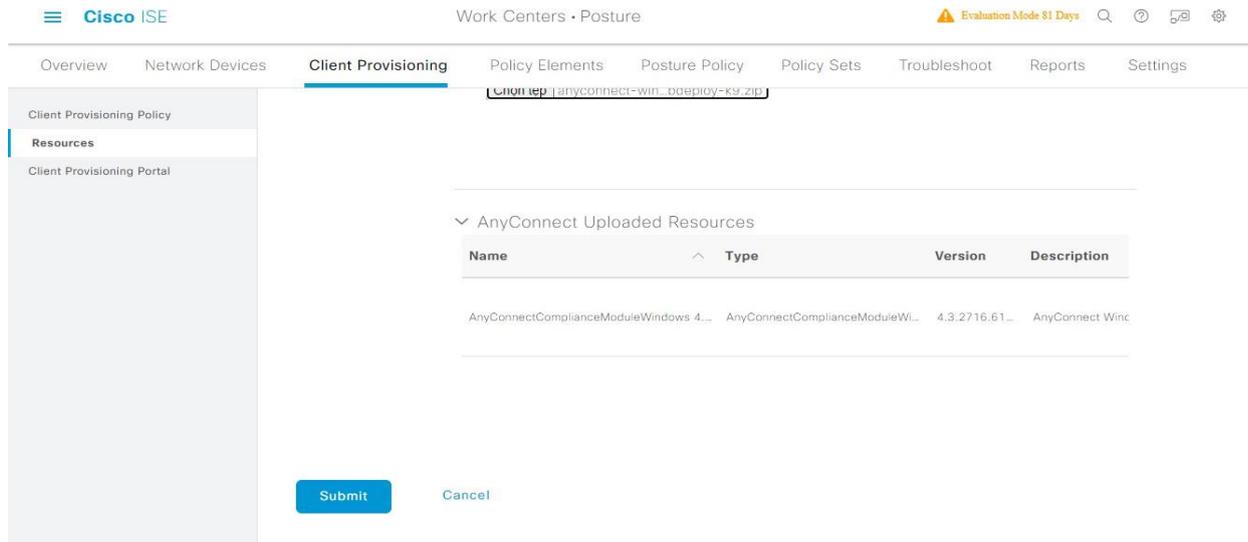
Client Provisioning Portal

Warning

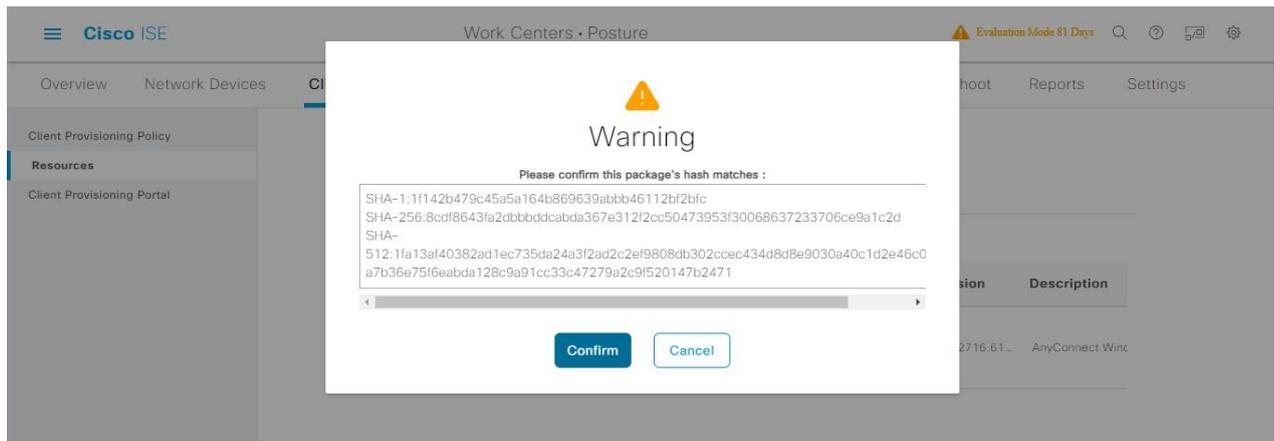
Please confirm this package's hash matches :

```
SHA-1: f2ef6fd5a3a9933a486b4bb0482309932d392cd3  
SHA-256: 293cce2beb98b735649c37cd51cf0e83d8048ce5cae5dc37f540596f9c8ec5c6  
SHA-  
512: 926b88e657078074d09fd75ac0411ddb6eb95e97e5cd3e0b0fed7225c0aec3754c688a  
fe5caf5e6b13965cebe969b753d6ae1ccf16c663278e2cfeba
```

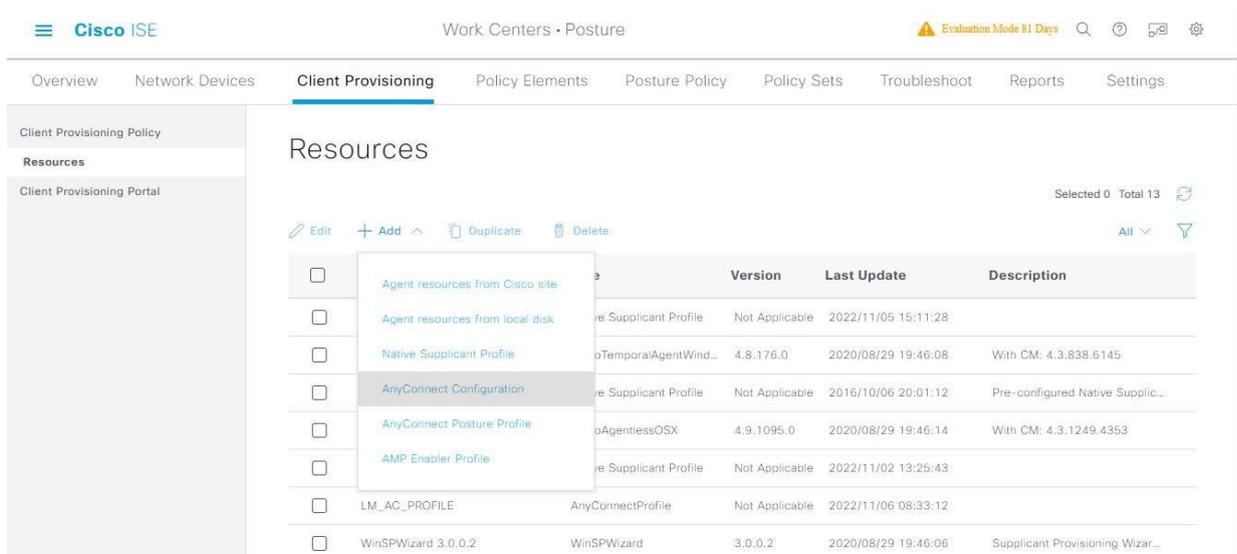
Confirm Cancel



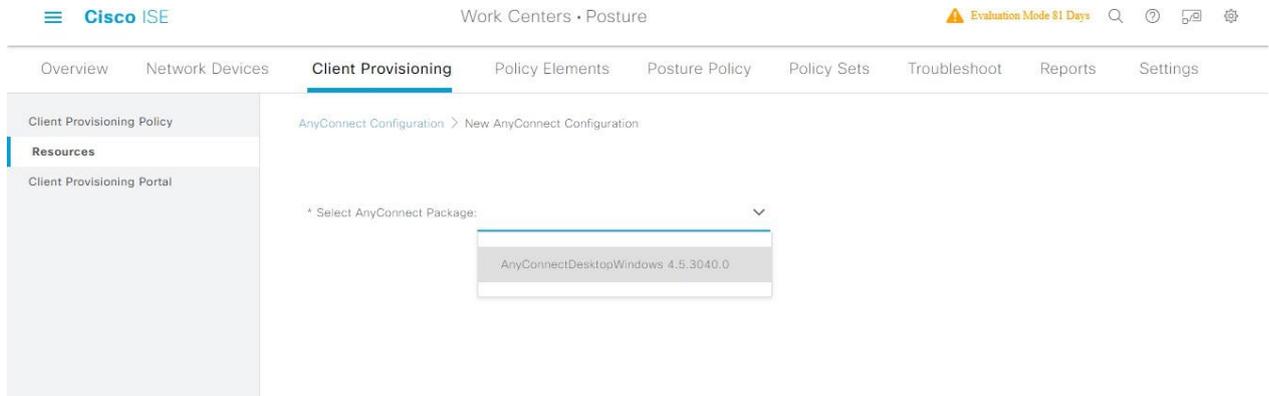
✓ Ta tiếp tục chọn Confirm



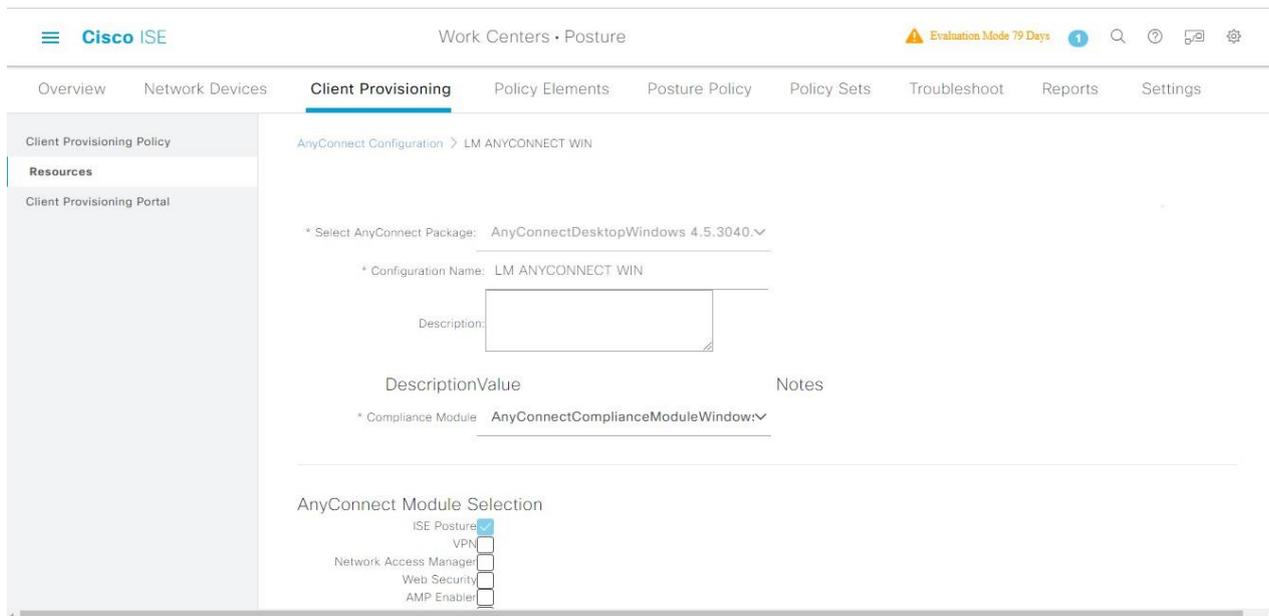
✓ Trên tab Client Provisioning, chọn mục AnyConnect Configuration.



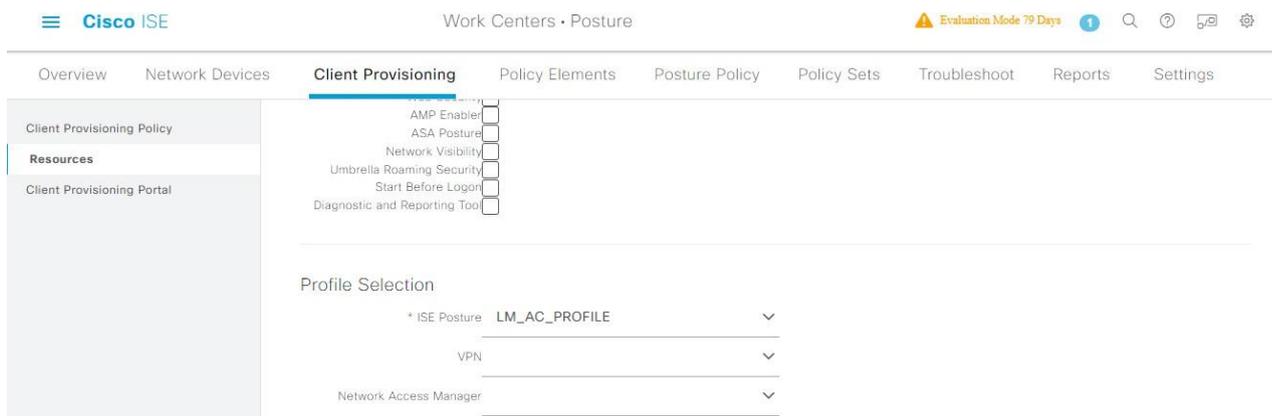
✓ Mục Select AnyConnect Package: chọn AnyconnectWindow 4.5 3040.0



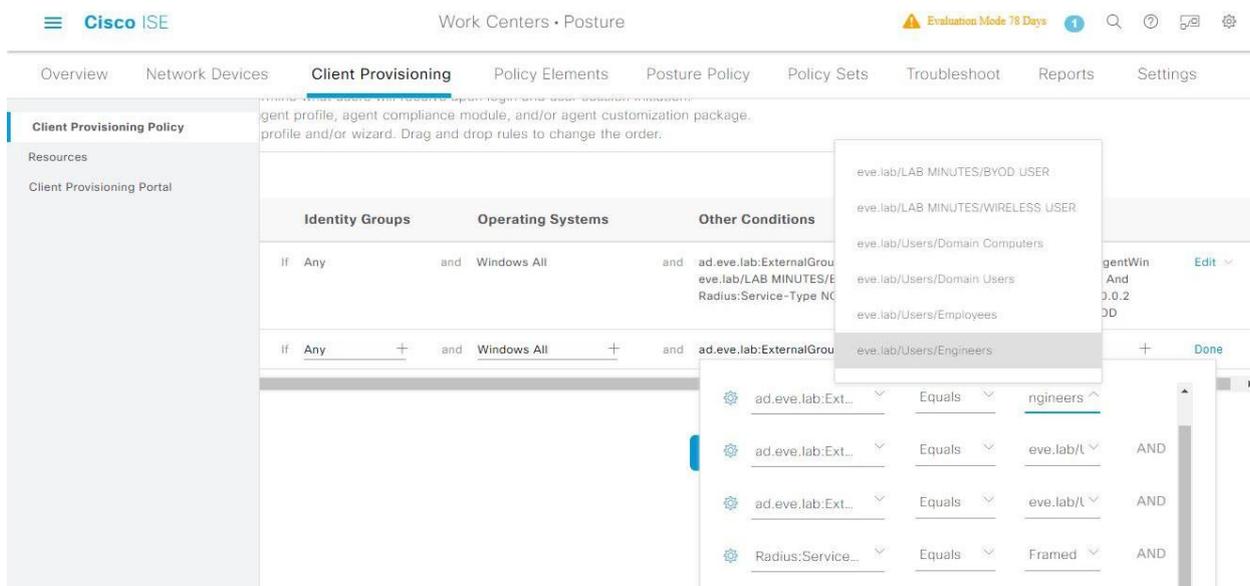
- ✓ Mục Configuration Name: LM ANYCONNECT WIN
- ✓ Compliance Module: AnyConnectCompliantModuleWindow
- ✓ Bỏ tick VPN



- ✓ ISE Posture: chọn LM_AC_PROFILE



- ✓ Chuyển hướng đến Client Provisioning
- ✓ Chọn tab Client Provisioning Policy
- ✓ Chọn edit
- ✓ Insert new policy
- ✓ Identify Groups: Any
- ✓ Operating Systems: Windows All
- ✓ Other Conditions:
 - ad.eve.lab:ExternalGroup EQUALS eve.lab/Users/Domain Computers
 - Radius:Service-Type EQUALS Framed
- ✓ Results: LM ANYCONNECT WIN



Cisco ISE Work Centers - Posture Evaluation Mode 81 Days

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports

Client Provisioning Policy
 Resources
 Client Provisioning Portal

agent profile, agent compliance module, and/or agent customization package.
 profile and/or wizard. Drag and drop rules to change the order.

Identity Groups	Operating Systems	Other Conditions
If Any	and Apple iOS All	and Condition(s)
If Any	and Windows All	and Condition(s)
If Any	and Windows All	and

Condition Name
 ad.eve.lab:Ext...
 Select Attribute

Radius
 Framed-IP-Address
 NAS-Identifier
 NAS-IP-Address
 NAS-Port-Type
Service-Type
 User-Name

Cisco ISE Work Centers - Posture Evaluation Mode 78 Days

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy
 Resources
 Client Provisioning Portal

agent profile, agent compliance module, and/or agent customization package.
 rd profile and/or wizard. Drag and drop rules to change the order.

Identity Groups	Operating Systems	Other Conditions	Results
If Any	and Windows All	and ad.eve.lab:ExternalGroups EQUALS eve.lab/LAB MINUTES/BYOD USER AND Radius:Service-Type NOT_EQUALS Framed	then CiscoTemporalAgentWindows 4.8.00176 And WinSPWizard 3.0.0.2 And LM NSP BYOD Edit
If Any	and Windows All	and ad.eve.lab:ExternalGroups EQUALS eve.lab/Users/Domain Computers AND ad.eve.lab:ExternalGroups EQUALS eve.lab/Users/Engineers AND ad.eve.lab:ExternalGroups EQUALS eve.lab/Users/Employees AND Radius:Service-Type EQUALS Framed	then LM ANYCONNECT WIN Edit
If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP Edit
If Any	and Windows All	and ad.eve.lab:ExternalGroups EQU eve.lab/LAB MINUTES/BYOD US Radius:NAS-Port-Type EQUALS	

Server Response
 Policy Saved Successfully

Cisco ISE Work Centers · Posture Evaluation Mode 78 Days

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy Resources Client Provisioning Portal

agent profile, agent compliance module, and/or agent customization package.
 rd profile and/or wizard. Drag and drop rules to change the order.

Identity Groups	Operating Systems	Other Conditions	Radius
If Any	and Windows All	and ad.eve.lab:ExternalGroups EQ... eve.lab/LAB MINUTES/BYOD L... Radius:Service-Type NOT_EQ...	<ul style="list-style-type: none"> Framed-IP-Address NAS-Identifier NAS-IP-Address NAS-Port-Type Service-Type User-Name
If Any	and Windows All	and ad.eve.lab:ExternalGroups EQ...	
If Any	and Apple iOS All	and ad.eve.lab:Ext...	
If Any	and Windows All	and ad.eve.lab:Ext...	
If Any	and Apple iOS All or Android	and ad.eve.lab:Ext...	
		and Radius:Service...	<ul style="list-style-type: none"> Equals Framed AND

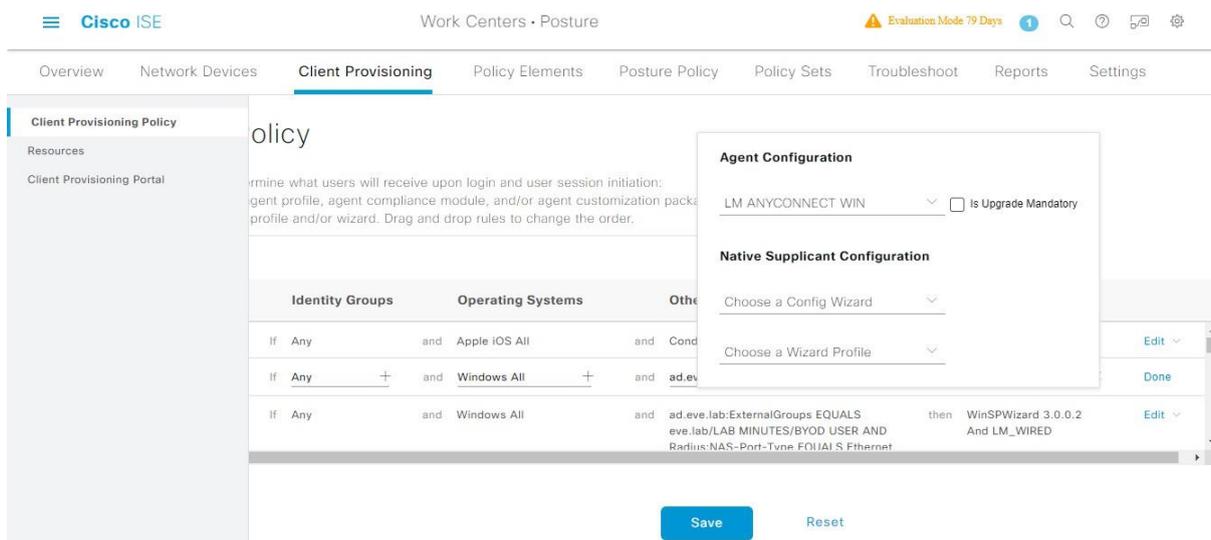
Cisco ISE Work Centers · Posture Evaluation Mode 78 Days

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy Resources Client Provisioning Portal

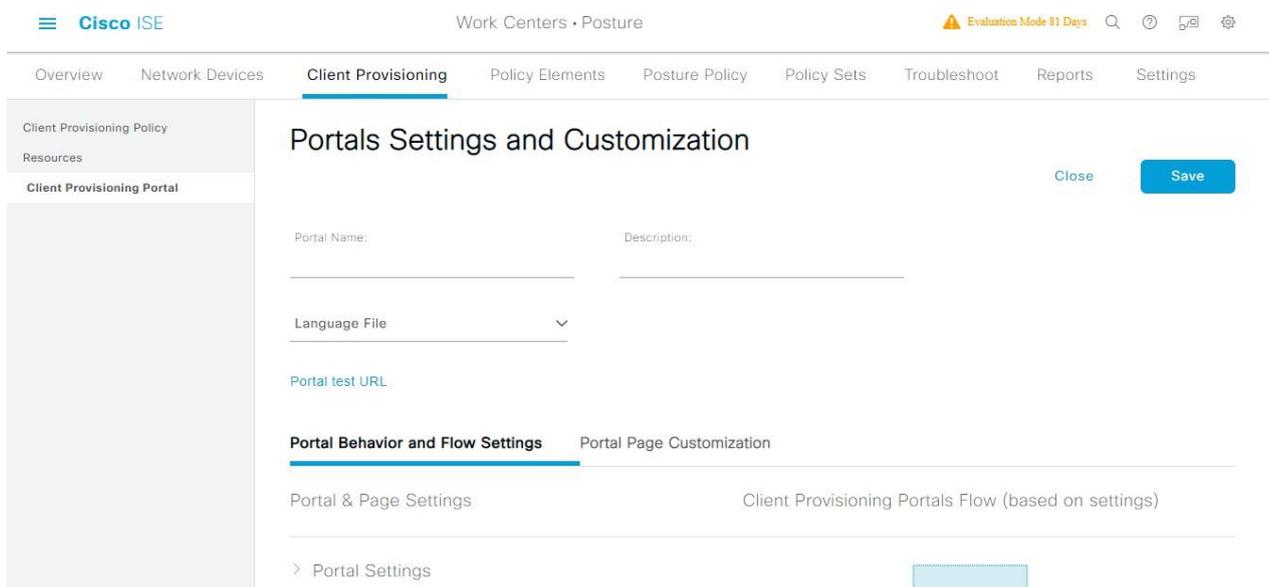
agent profile, agent compliance module, and/or agent customization package.
 rd profile and/or wizard. Drag and drop rules to change the order.

Identity Groups	Operating Systems	Other Conditions	Radius
If Any	and Windows All	and ad.eve.lab:ExternalGroups EQUALS eve.lab/LAB MINUTES/BYOD USER AND Radius:Service-Type NOT_EQUALS Framed	<ul style="list-style-type: none"> Callback Framed Callback Login Callback NAS Prompt Fax Framed HP-Oper HP-User IAPP-AP-Check IAPP-Register
If Any	and Windows All	and ad.eve.lab:ExternalGroups EQ...	
If Any	and Apple iOS All	and ad.eve.lab:Ext... Equals	
If Any	and Windows All	and ad.eve.lab:Ext... Equals	
If Any	and Apple iOS All or Android	and ad.eve.lab:Ext... Equals	
		and Radius:Service... Equals	<ul style="list-style-type: none"> Framed AND

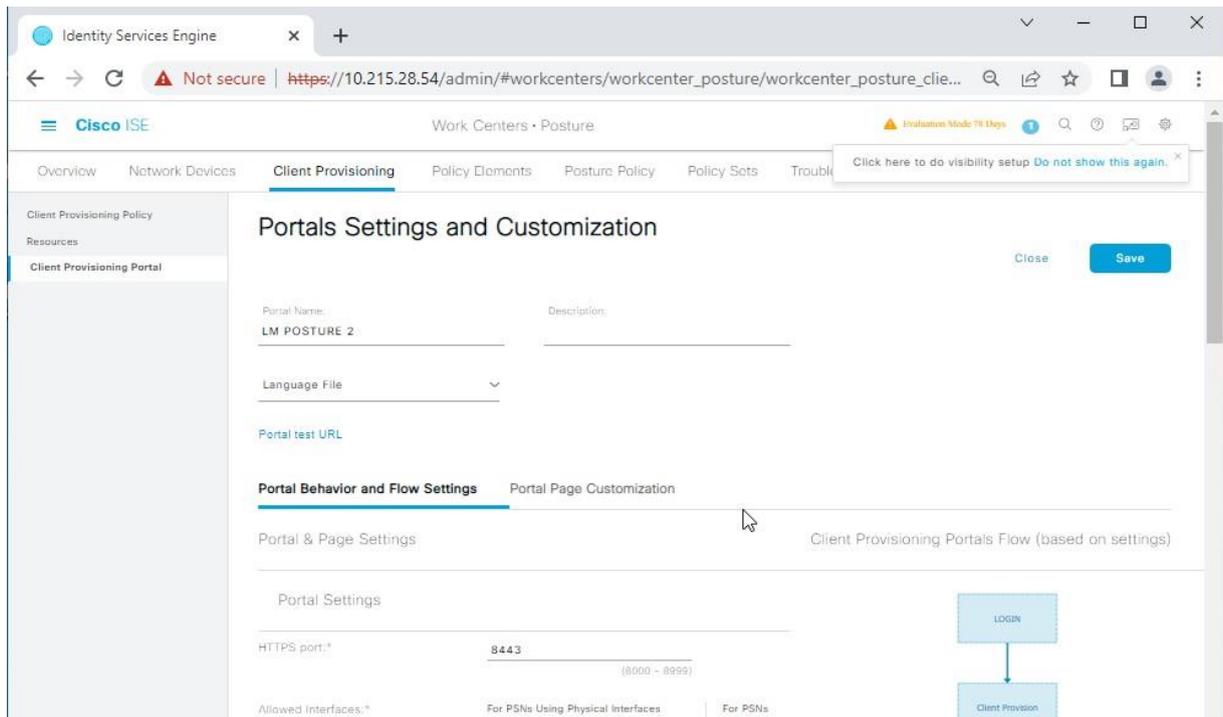


3.3 Cấu hình Portal Settings and Customization:

- ✓ Ta sẽ tạo giao diện Portal để các user đăng nhập và download Anyconnect về thiết bị của họ
- ✓ Vào Client Provisioning Portal
- ✓ Tạo Portal mới



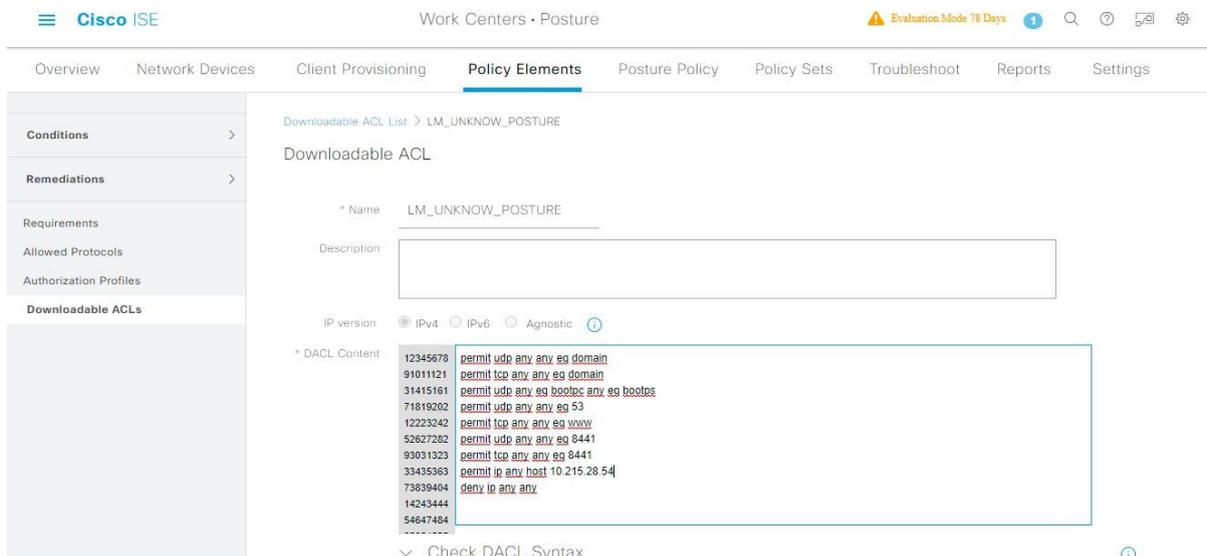
- ✓ Portal Name: LM POSTURE 2, sau đó Save



3.4 Cấu hình DACL:

✓ Name: LM_UNKNOW_POSTURE

✓ DACL Content:



✓ Name: LM_INTERNET_ONLY

Cisco ISE Work Centers - Posture

Downloadable ACL

* Name: LM_INTERNET_ONLY

Description: [Empty text box]

IP version: IPv4 IPv6 Agnostic ⓘ

* DACL Content

```

12345678 permit udp any eq bootpc any eq bootps
91011121 permit udp any any eq 53
31415161 deny ip any 10.215.28.0 255.255.254.0
71819202 permit ip any any
12223242
52627282
93031323
33435363
73839404
14243444
54647484
    
```

Check DACL Syntax ⓘ

3.5 Cấu hình Authorization Profiles:

- ✓ Name: WIRED_USER_UNKNOWN
- ✓ Common Task: LM_UNKNOWN_POSTURE

Cisco ISE Work Centers - Posture

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name: WIRED_USER_UNKNOWN

Description: [Empty text box]

* Access Type: ACCESS_ACCEPT ▼

Network Device Profile: Cisco ⓘ

Service Template:

Track Movement: ⓘ

Agentless Posture: ⓘ

Passive Identity Tracking: ⓘ

Work Centers - Posture

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy Policy Sets Troubleshoot Reports Settings

Conditions >

Remediations >

Requirements

Allowed Protocols

Authorization Profiles

Downloadable ACLs

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

Common Tasks

DACL Name: LM_UNKNOW_POSTURE

IPv6 DACL Name

ACL (Filter-ID)

Voice Domain Permission

- ✓ Tại mục Web Redirection:
- ✓ Ta chọn mục: Client Provisioning (Posture)
- ✓ ACL : 101 (ACL này đã có trên switch 3k)
- ✓ Value: LM POSTURE 2

Work Centers - Posture

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy Policy Sets Troubleshoot Reports Settings

Conditions >

Remediations >

Requirements

Allowed Protocols

Authorization Profiles

Downloadable ACLs

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

Common Tasks

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP) ⓘ

Client Provisioning (Posture) ACL 101 Value LM POSTURE 2

Static IP/Host name/FQDN

Success Profile Co&E configuration

✓ Name: WIRED_USER_NONCOMPLIANT

The screenshot shows the Cisco ISE interface for configuring an Authorization Profile. The breadcrumb path is "Authorization Profiles > WIRED_USER_NONCOMPLIANT". The main configuration area includes:

- * Name: WIRED_USER_NONCOMPLIANT
- Description: (empty text box)
- * Access Type: ACCESS_ACCEPT
- Network Device Profile: Cisco
- Service Template:
- Track Movement: ⓘ
- Agentless Posture: ⓘ
- Passive Identity Tracking: ⓘ

✓ Authorization Profiles, mục DACL Name: LM_INTERNET_ONLY

The screenshot shows the "Common Tasks" section of the Authorization Profile configuration. The breadcrumb path is "Authorization Profiles > LM_INTERNET_ONLY". The configuration includes:

- Passive Identity Tracking: ⓘ
- Common Tasks:
 - DACL Name: LM_INTERNET_ONLY
 - IPv6 DACL Name
 - ACL
 - ...

✓ Authorization Profiles: WIRED_USER_COMPLIANT

The screenshot shows the Cisco ISE interface for configuring an Authorization Profile. The breadcrumb path is "Authorization Profiles > WIRED_USER_COMPLIANT". The main configuration area includes:

- * Name: WIRED_USER_COMPLIANT
- Description: (empty text box)
- * Access Type: ACCESS_ACCEPT
- Network Device Profile: Cisco
- Service Template:
- Track Movement: ⓘ
- Agentless Posture: ⓘ
- Passive Identity Tracking: ⓘ

- ✓ Policy Elements:
- ✓ DACL Name: LM_USER

The screenshot shows the Cisco ISE interface for configuring Policy Elements. The 'Policy Elements' tab is selected. In the 'Common Tasks' section, the 'DACL Name' is configured to 'LM_USER'. Other options like 'IPv6 DACL Name', 'ACL', and 'Downloadable ACLs' are visible but not selected.

- ✓ Cấu hình Policy set:
- ✓ Dưới các mục authorization đã tạo, bấm vào biểu tượng bánh răng, insert policy below

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	AD_PC_RULE	ad.eve.lab-ExternalGroups EQUALS eve.lab/Users/Domain Computers	PermitAccess x	Domain_PC	0	⚙️
✓	Engineers	ad.eve.lab-ExternalGroups EQUALS eve.lab/Users/Engineers AND Network Access-WasMachineAuthenticated EQUALS True	Engineers-PROFILE x	Engineers	0	⚙️
⋮	Employees	ad.eve.lab-ExternalGroups EQUALS eve.lab/Users/Employees AND Network Access-WasMachineAuthenticated EQUALS True	Employees-PROFILE x	Employees	0	⚙️

✓ Name: USER UNKNOWN

		Results				
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
<input type="text" value="Search"/>						
✓	USER_UNKNOWN_WS	AND <ul style="list-style-type: none"> ad.eve.lab-ExternalGroups EQUALS eve.lab/Users/Domain Computers Network Access-WasMachineAuthenticated EQUALS True Session-PostureStatus EQUALS Unknown 	WIRED_USER_UNKNO... x	Select from list	0	⚙️

Mục Condition chọn:

- ✓ ad.eve.lab-ExternalGroup EQUALS eve.lab/Users/Domain Computers
- ✓ Network Access-WasMachineAuthenticated EQUALS True
- ✓ Session-PostureStatus EQUALS Unknown

Mục Profiles:

- ✓ WIRED_USER_UNKNOWN

Cisco ISE Policy - Policy Sets ⚠️ Evaluation Mode 79 Days

		Results				
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
<input type="text" value="Search"/>						
✓	USER_UNKNOWN_WS	AND <ul style="list-style-type: none"> Computers Network Access-WasMachineAuthenticated EQUALS True Session-PostureStatus EQUALS Unknown 	WIRED_USER_UNKNO... x	Select from list	0	⚙️
⋮	USER_NONCOMPLIANT	AND <ul style="list-style-type: none"> ad.eve.lab-ExternalGroups EQUALS eve.lab/Users/Domain Computers Network Access-WasMachineAuthenticated EQUALS True Session-PostureStatus EQUALS NonCompliant 	WIRED_USER_NONCO... x	Select from list	0	⚙️

Cisco ISE Policy - Policy Sets

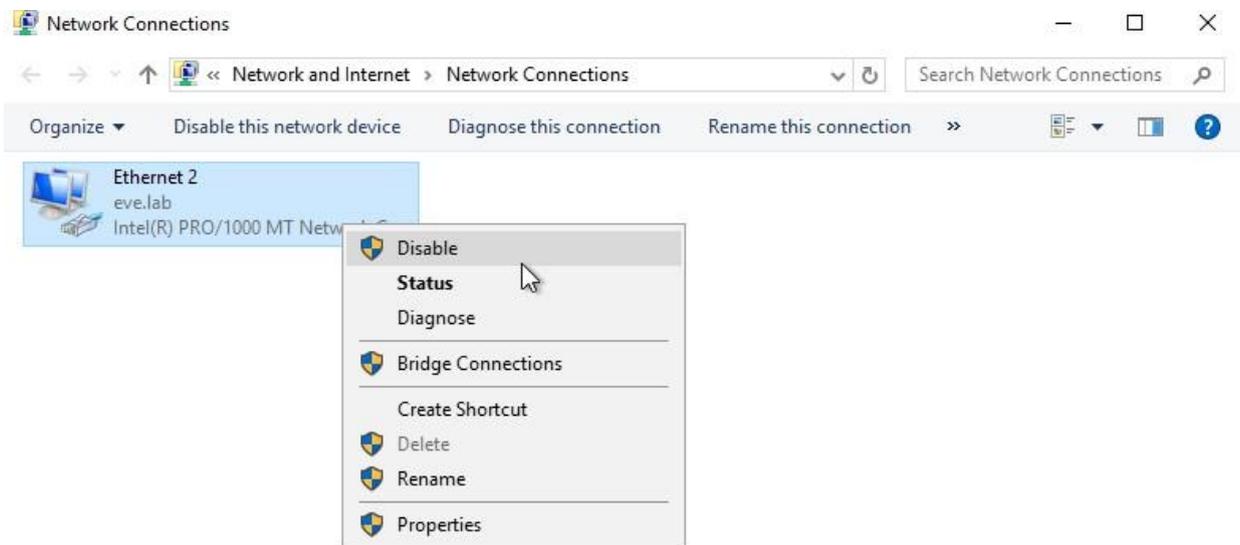
Evaluation Mode 79 Days

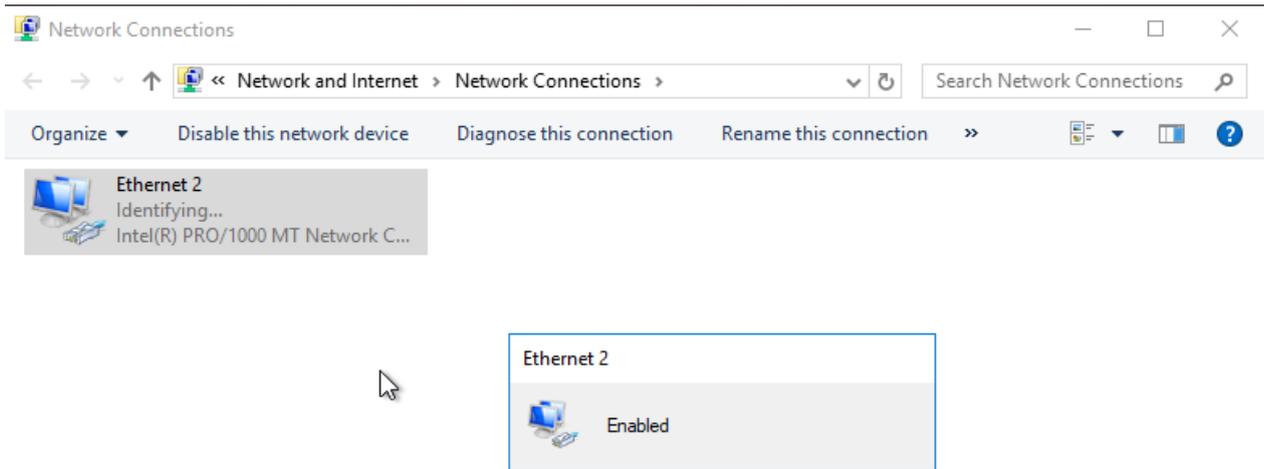
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	USER_NONCOMPLIANT	AND Computers Network Access-WasMachineAuthenticated EQUALS True Session-PostureStatus EQUALS NonCompliant	WIRED_USER_NONCO...	Select from list	0	⚙️
✓	USER_COMPLIANT	AND ad.eve.lab-ExternalGroups EQUALS eve.lab/Users/Domain Computers Network Access-WasMachineAuthenticated EQUALS True Session-PostureStatus EQUALS Compliant	WIRED_USER_COMPLI...	Select from list	0	⚙️

✓ Save.

3.6 Tiến hành test :

✓ Ta vào PC , disable và enable lại card mạng



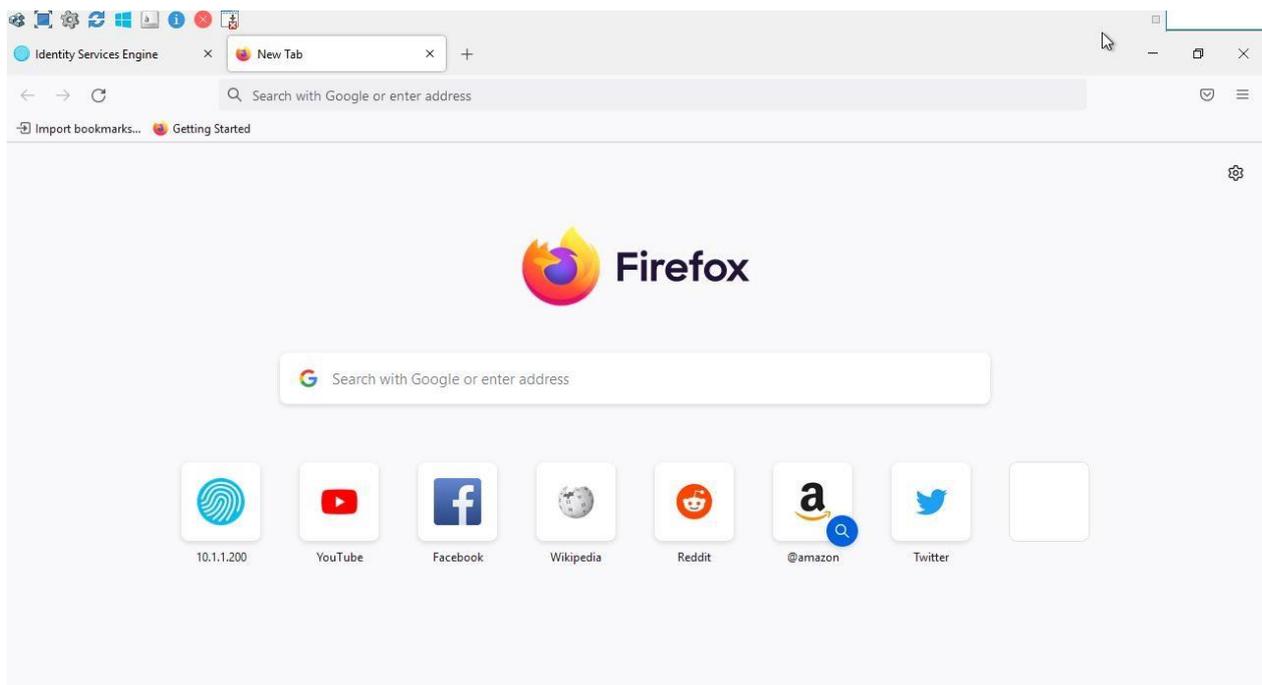


Kiểm tra lại trên SW3K:

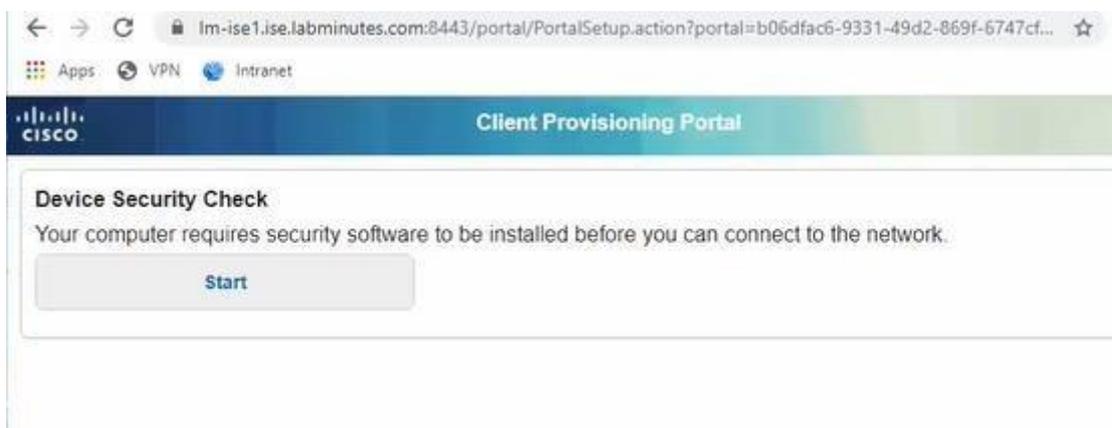
- ✓ show authentication sessions interface G0/1 details
- ✓ SW1#show authentication sessions interface G0/1 details

Xem mục Server Policy đã có DACL và Link URL Redirection web từ ISE

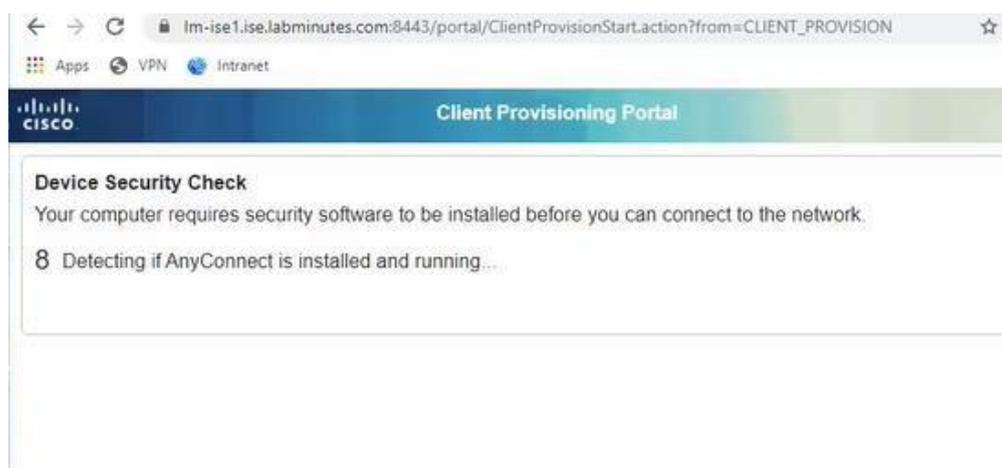
- ✓ Server Policies:
- ✓ Vlan Group:
 - ACS ACL: **xACSACLx-IP-EVE_DHCP_ACL-5fe79837**
 - URL WEB:
- ✓ SGT Value: 5
- ✓ Nếu đã có đủ điều trên, Trên PC, ta truy cập web bất kỳ để redirect sang portal :8443 của ISE



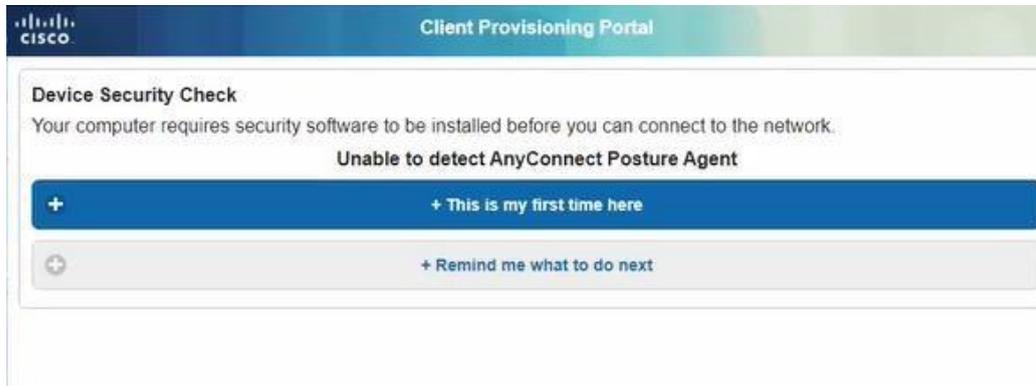
✓ Chọn Start để bắt đầu truy cập mạng



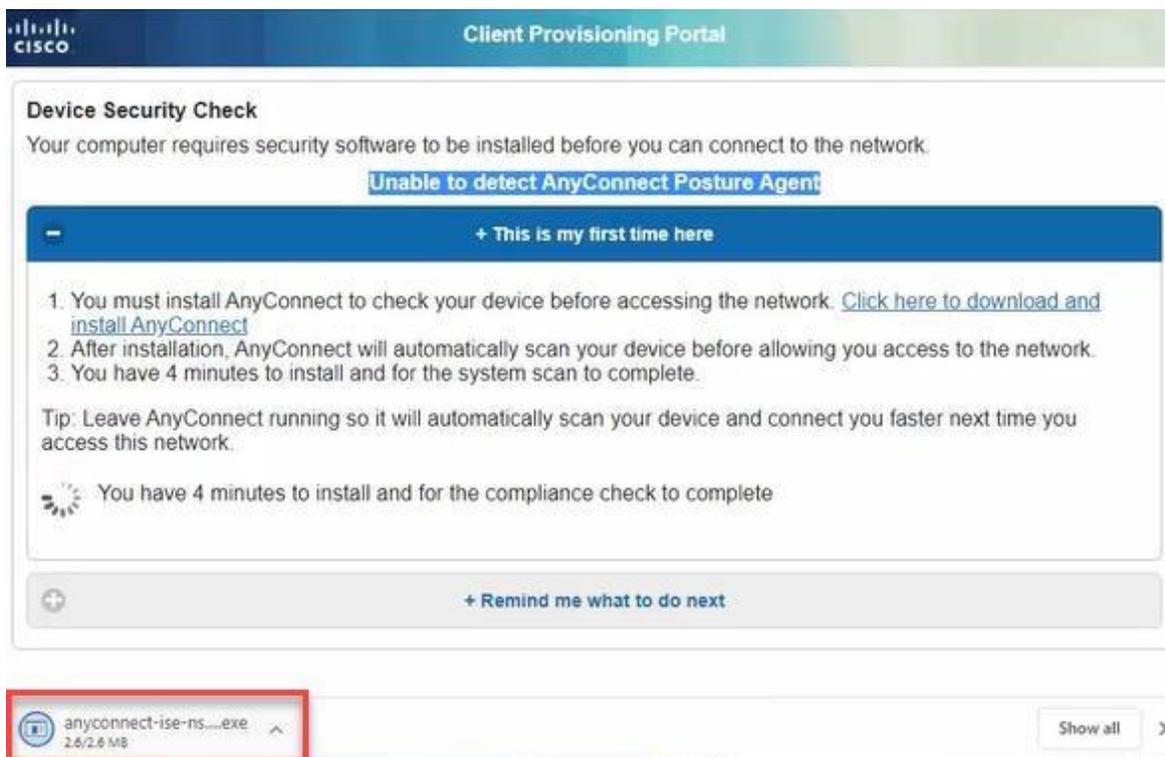
✓ Device Security Check: đợi vài giây để bắt đầu cài đặt và chạy



- ✓ Để Unable to detect AnyConnect Posture Agent
- ✓ Click vào “ This is my first time here ”



- ✓ Ta tiến hành Download AnyConnect về



- ✓ Sau khi Download AnyConnect và Tiến hành truy cập mạng : Click vào Connect



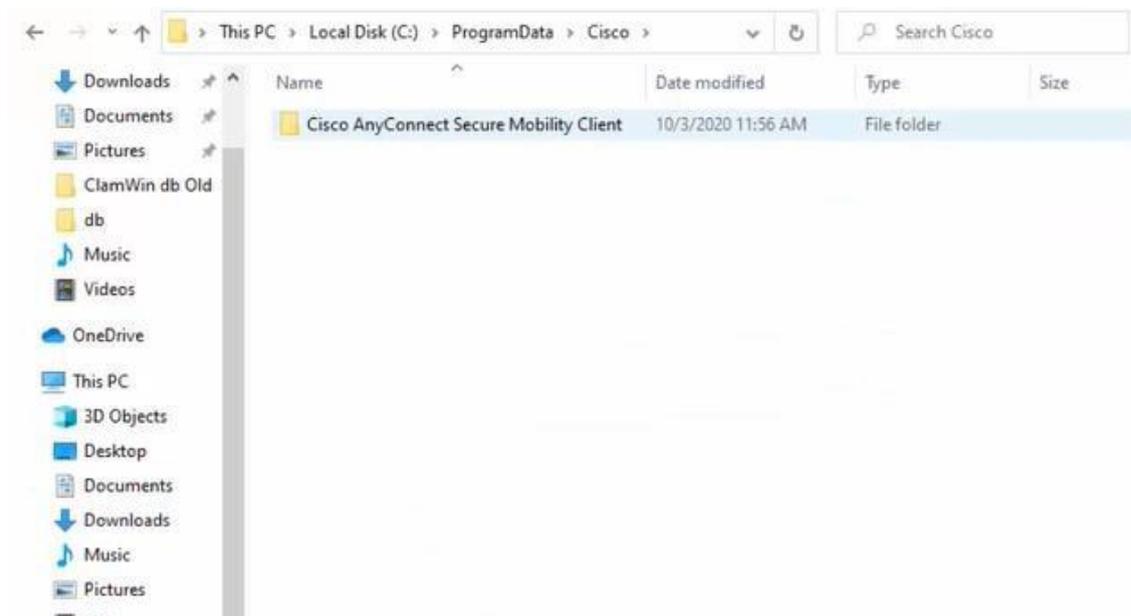
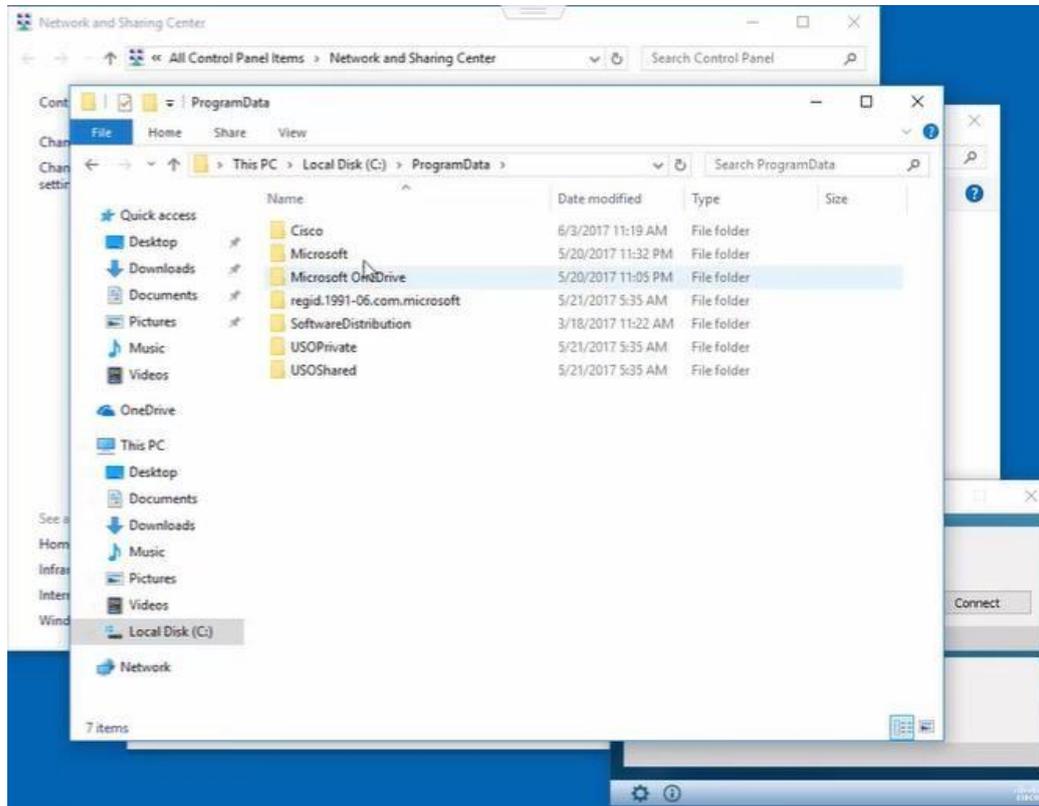
- ✓ Quá trình Download và cài đặt đang diễn ra



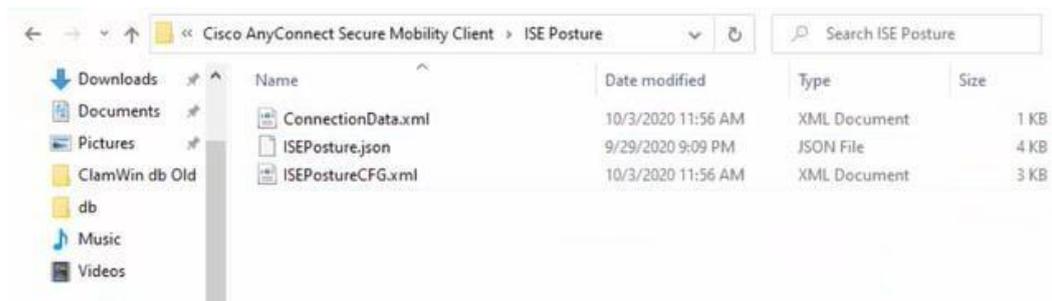
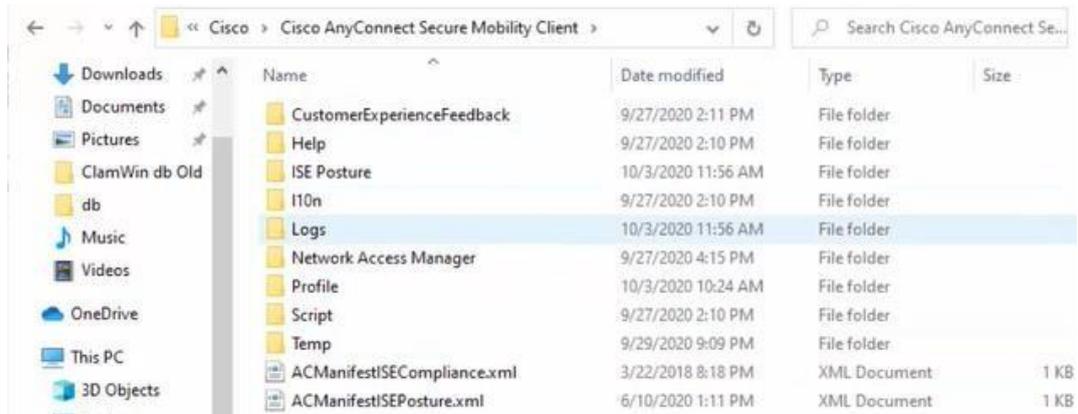
✓ Cài đặt thành công



✓ Truy cập ổ C / ProgramData / Cisco / Cisco AnyConnect Secure Mobility Client



✓ Chọn tiếp Profile / ISE Posture / ISEPostureCFG.xml



C:\ProgramData\Cisco\Cis... x

```
<?xml version="1.0"?>
- <records>
  - <record>
    <primary>LM-ISE1.ise.labminutes.com</primary>
    <port>8443</port>
    <status_path>/auth/status</status_path>
    <ng-discovery>/auth/ng-discovery</ng-discovery>
    <time>1601751403</time>
  </record>
  - <record>
    <primary>lm-ise1.ise.labminutes.com</primary>
    <port>8443</port>
    <status_path>/auth/status</status_path>
    <ng-discovery>/auth/ng-discovery</ng-discovery>
    <time>1601751365</time>
  </record>
</records>
```

✓ Cấu hình Posture Condition

✓ Work Center/ Posture / Policy Element / Application / +Add

Work Centers - Posture

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy Policy Sets

Conditions

- Anti-Malware
- Anti-Spyware
- Anti-Virus
- Application**
- Compound
- Dictionary Compound
- Dictionary Simple
- Disk Encryption

Application Condition

Rows/Page ▼ ⏪

↻ **Add** Duplicate Trash ▼ Edit

<input type="checkbox"/>	Name	Description	Application
<input type="checkbox"/>	Default_AppVis_Condition_Mac	Cisco Predefined Check for installe...	Installed and
<input type="checkbox"/>	Default_AppVis_Condition_Win	Cisco Predefined Check for installe...	Installed and

✓ Name: LM_WIN_APP_COLLECTION

✓ Operating System: Windows All

✓ Check By: Application

✓ Compliant Module: 4.x or later

✓ Provision by: Everything

Work Centers - Posture

Overview Network Devices Client Provisioning **Policy Elements**

Conditions

- Anti-Malware
- Anti-Spyware
- Anti-Virus
- Application**
- Compound
- Dictionary Compound
- Dictionary Simple
- Disk Encryption
- External DataSource
- File
- Firewall
- Hardware Attributes
- Patch Management
- Registry

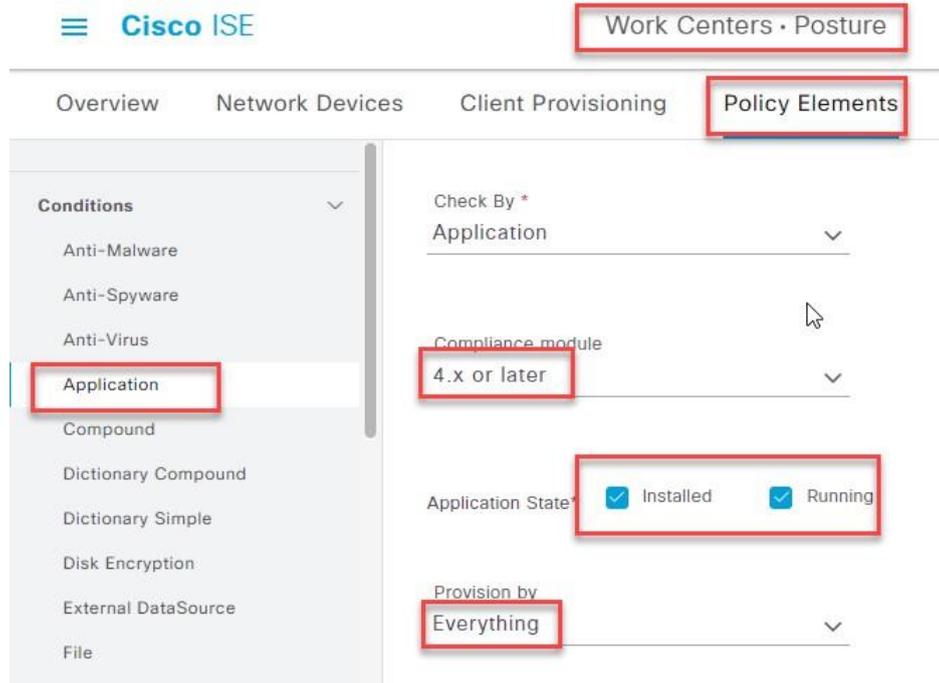
Application Condition > New

Name*
LM_WIN_APP_COLLECTION

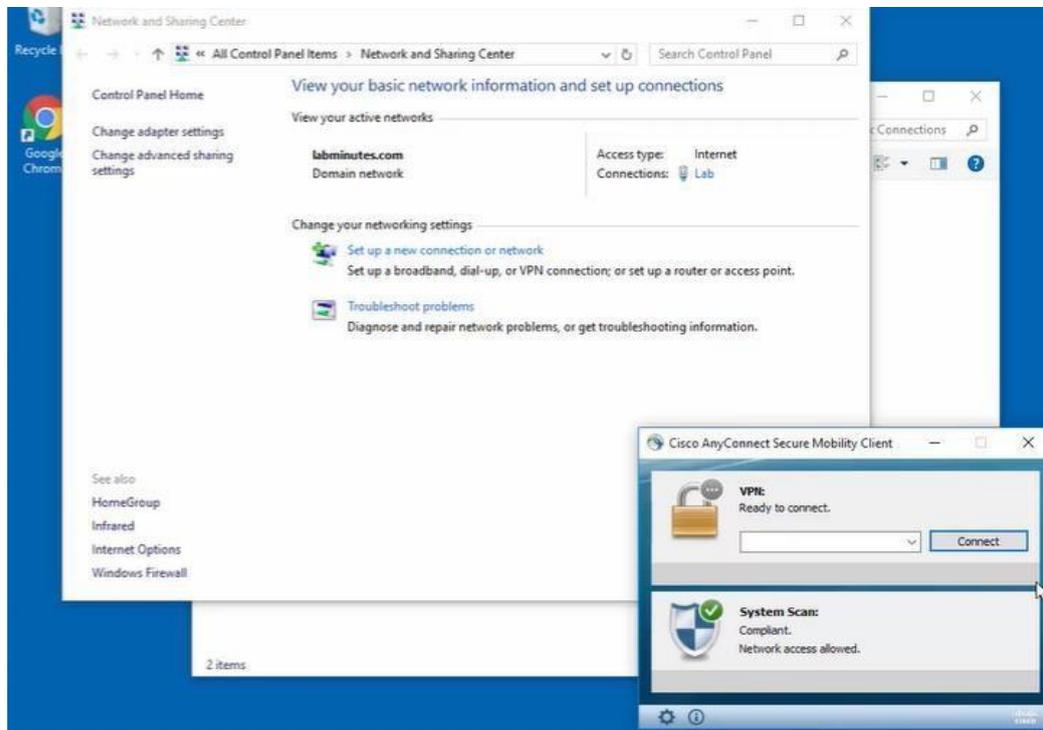
Description

Operating System*
Windows All

Check By*
Application



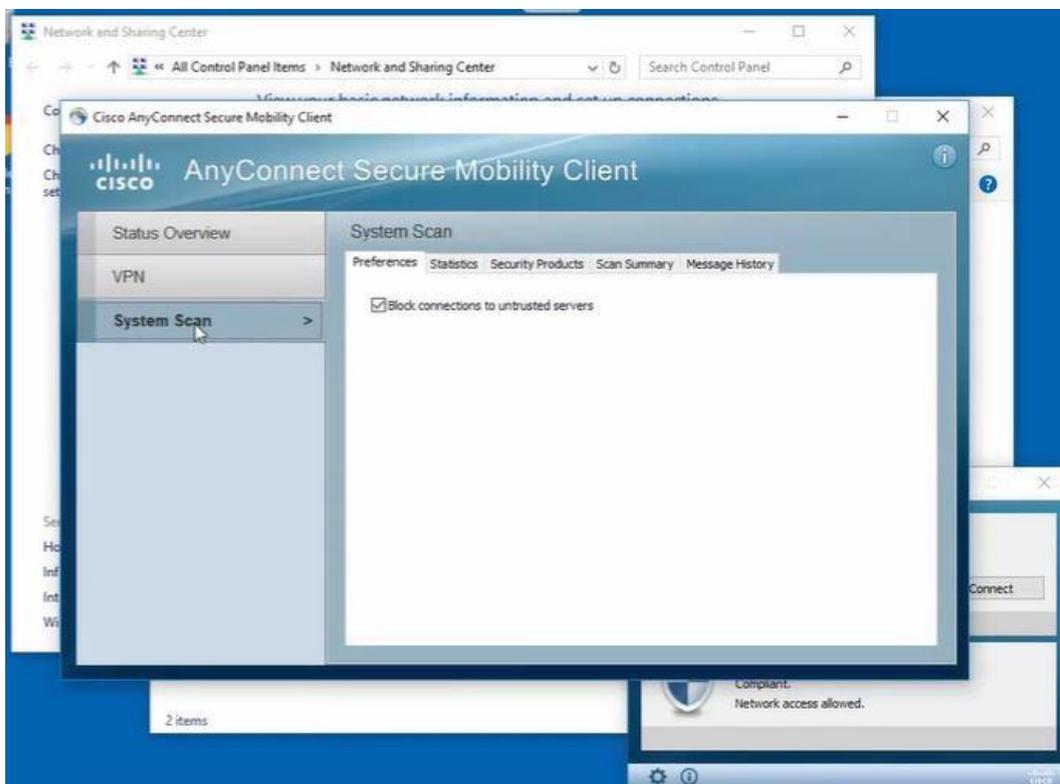
✓ System Scan: phần mềm anyconnect : Compliance



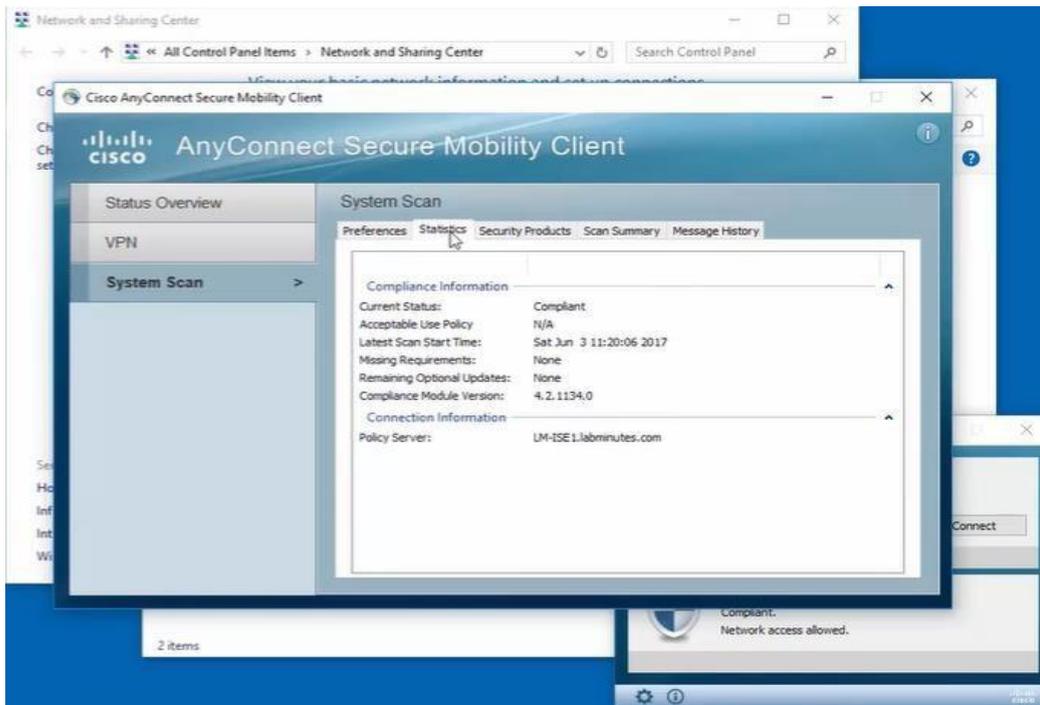
✓ **Bật Setting Scan:**



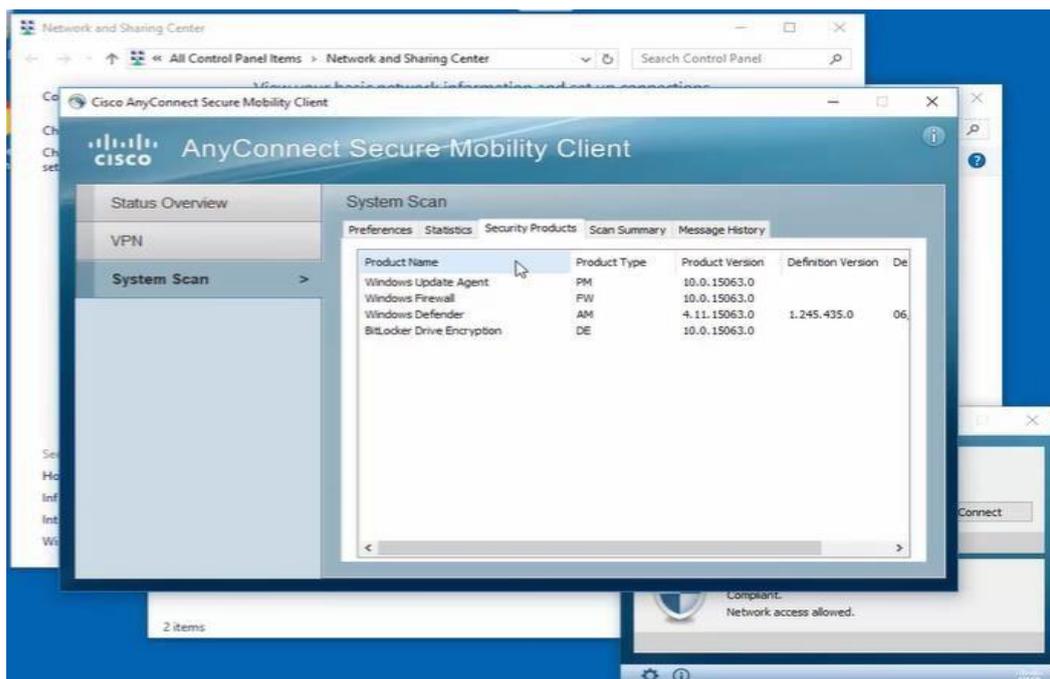
✓ **System Scan: Click vào Connection to untrusted servers**



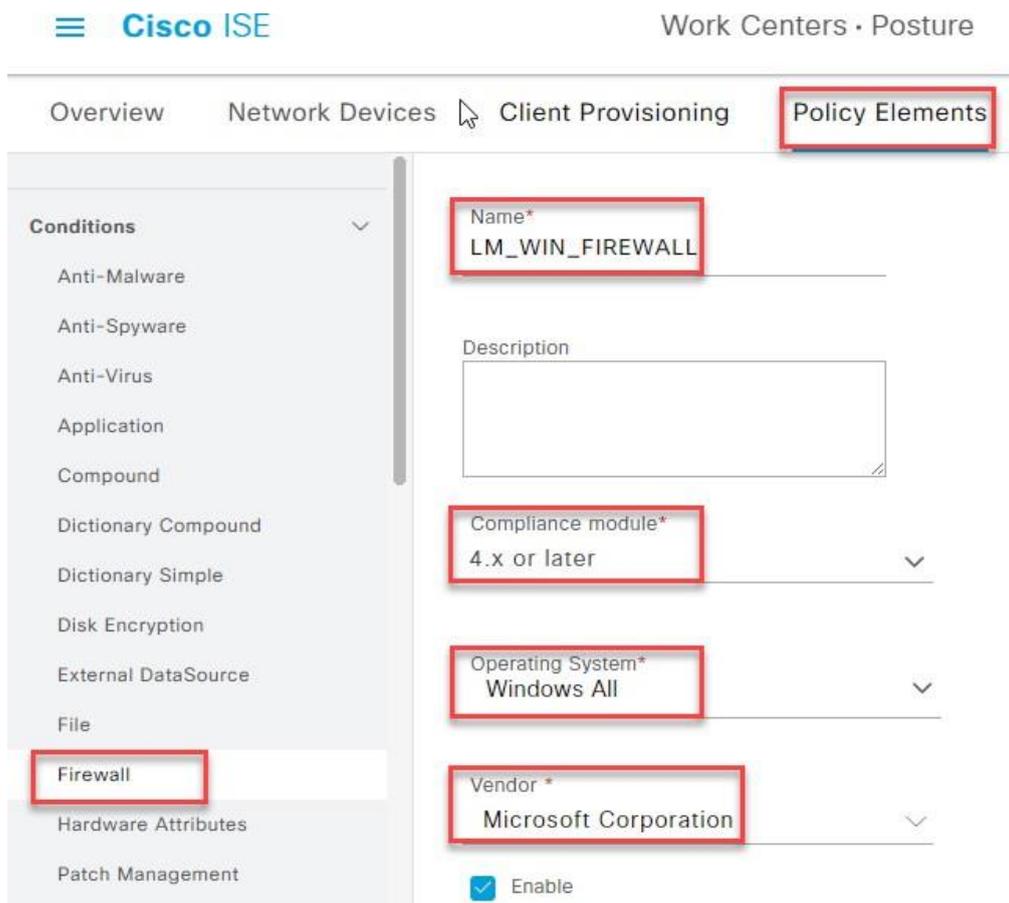
✓ System Scan: mở tab Statistics để xem thông tin Compliance



✓ System Scan: chọn tab Security Product , Product Name



- ✓ Sau khi qua khỏi mode Unknown, ta tiếp tục cấu hình thêm phần Condition Posture
- ✓ Work Centers / Posture / Policy Elements / Firewall Condition
- ✓ Name: LM_WIN_FIREWALL
- ✓ Compliance module: 4.x or later
- ✓ Operating System: Windows All
- ✓ Vendor: Microsoft Corporation
- ✓ Tick vào mục Windows firewall và version 10.x



The screenshot shows the Cisco ISE configuration interface for Policy Elements. The breadcrumb path is Work Centers > Posture > Policy Elements. The left sidebar shows the 'Conditions' menu with 'Firewall' selected. The main configuration area has the following fields:

- Name*: LM_WIN_FIREWALL
- Description: (empty text area)
- Compliance module*: 4.x or later
- Operating System*: Windows All
- Vendor*: Microsoft Corporation
- Enable

Cisco ISE Work Centers · Posture

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy Pol

Conditions

- Anti-Malware
- Anti-Spyware
- Anti-Virus
- Application
- Compound
- Dictionary Compound
- Dictionary Simple
- Disk Encryption
- External DataSource
- File
- Firewall**
- Hardware Attributes
- Patch Management

Vendor *
 Microsoft Corporation

Enable

At least one product must be selected*

<input type="checkbox"/>	Product Name	Version
<input checked="" type="checkbox"/>	Windows Firewall	10.x
<input type="checkbox"/>	Windows Firewall	6.x
<input type="checkbox"/>	Windows Firewall	ANY
<input type="checkbox"/>	ANY	ANY

- ✓ Posture / Policy Elements / Anti-Malware
- ✓ Name: LM_WINS
- ✓ Operating System: Windows All
- ✓ Vendor: Microsoft Corporation
- ✓ Tab Product for Selected Vendor:
- ✓ Baseline Condition: Windows Defender 4.x

Cisco ISE Work Centers · Posture

Overview Network Devices Client Provisioning **Policy Elements** Posture

Conditions

- Anti-Malware**
- Anti-Spyware
- Anti-Virus
- Application
- Compound
- Dictionary Compound
- Dictionary Simple
- Disk Encryption
- External DataSource
- File

Anti-Malware Condition

* Name **LM_WINS**

Description

Compliance Module 4.x or later ⓘ

* Operating System **Windows All**

Vendor **Microsoft Corporation**

Check Type Installation Definition

Products for Selected Vendor

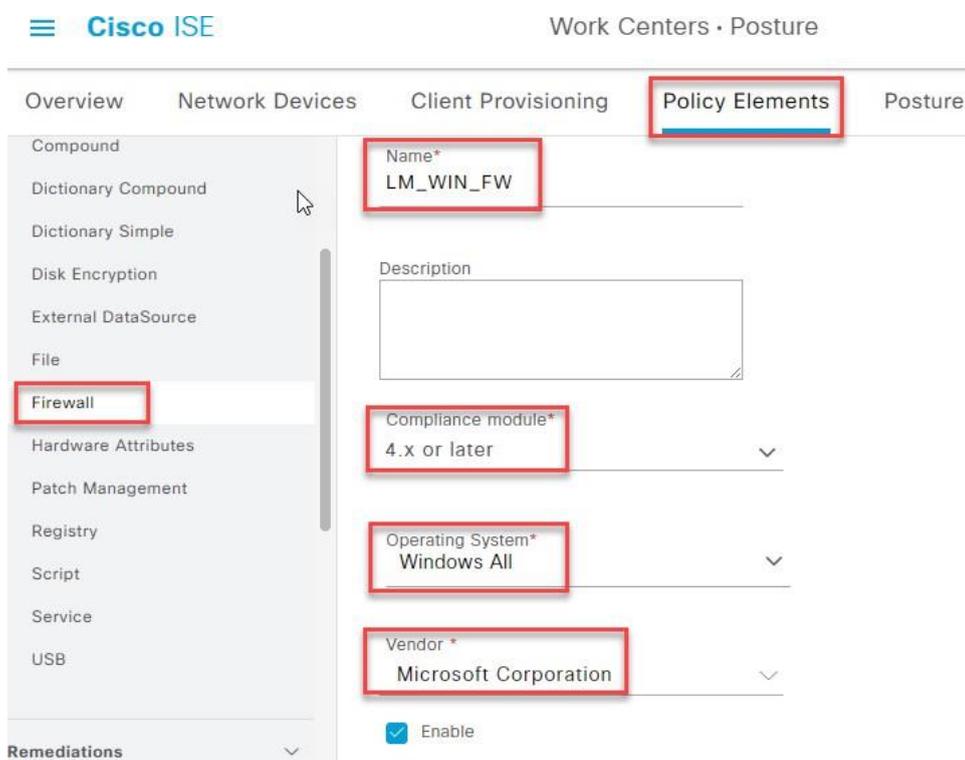
Baseline Condition Advanced Condition

i You can select products either on baseline condition or advanced condition.

	Product Name	Minimum Version	Maximum Version	Minimum C
<input checked="" type="checkbox"/>	Windows Defender	4.x	6.x	4.2.520.0
<input type="checkbox"/>	System Center Endpoint Protect...	4.x	4.x	4.2.520.0
<input type="checkbox"/>	Microsoft Security Essentials	1.x	4.x	4.2.520.0

3.6 Cấu hình Posture Remediation:

- ✓ Work Center / Posture / Firewall
- ✓ Name: LM_WIN_FW
- ✓ Operating System: Windows All
- ✓ Compliance module: 4.x or later
- ✓ Remediation Type: Manual
- ✓ Vendor name: Microsoft operation
- ✓ Window firewall + Any



The screenshot shows the Cisco ISE interface for configuring a Policy Element. The 'Policy Elements' tab is selected, and the 'Firewall' category is chosen from the left-hand menu. The configuration details are as follows:

- Name*:** LM_WIN_FW
- Description:** (Empty text area)
- Compliance module*:** 4.x or later
- Operating System*:** Windows All
- Vendor*:** Microsoft Corporation
- Enable:**

Cisco ISE Work Centers • Posture

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy Poli

Compound
 Dictionary Compound
 Dictionary Simple
 Disk Encryption
 External DataSource
 File
Firewall
 Hardware Attributes
 Patch Management
 Registry
 Script
 Service
 USB

Vendor *
 Microsoft Corporation

Enable

At least one product must be selected*

<input type="checkbox"/>	Product Name	Version
<input type="checkbox"/>	Windows Firewall	10.x
<input type="checkbox"/>	Windows Firewall	6.x
<input checked="" type="checkbox"/>	Windows Firewall	ANY
<input type="checkbox"/>	ANY	ANY

3.6 Cấu hình Posture Requirement:

- ✓ Work Centers / Posture / Policy Element / Requirement
- ✓ Edit /new
- ✓ Name: LM_WIN_FW
- ✓ Operating System: Windows All
- ✓ Compliance module: 4.x or later

Cisco ISE Work Centers · Posture

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy Policy Sets Troubleshoot Reports

Anti-Malware
 Anti-Spyware
 Anti-Virus
 File
 Firewall
 Launch Program
 Link
 Patch Management
 Windows Server Update S...
 Windows Update
 USB

Requirements

Allowed Protocols
 Authorization Profiles
 Downloadable ACLs

Guide Me

Name	Operating System	Compliance Module	Posture Type
Any_AV_Installation_Win	for Windows All	using 3.x or earlier	using AnyConnect met ANY_av if
LM_WIN-FW	for Windows All	using 4.x or later	using AnyConnect

Note: Remediation Action is filtered based on the operating system and stealth mode selection.
 Remediation Actions are not applicable for Application Conditions (configured using the Provision By Category or Provision By Everything options), Hardware C External Data source conditions.
 Remediations Actions are not applicable for Agentless Posture type.

Save

✓ Mục Conditions: Chọn User Defined Conditions / Firewall Condition / LM_WIN_FIREWALL

Cisco ISE Work Centers · Posture

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy Policy Sets Troubleshoot Reports

Anti-Malware
 Anti-Spyware
 Anti-Virus
 File
 Firewall
 Launch Program
 Link
 Patch Management
 Windows Server Update S...
 Windows Update
 USB

Requirements

Allowed Protocols

Guide Me

Compliance Module	Posture Type
earlier using AnyConnect	met ANY_av_win_inst if
using 4.x or later using AnyConnect	met

Note: Remediation Action is filtered based on the operating system and stealth mode selection.
 Remediation Actions are not applicable for Application Conditions (configured using the Provision By Category or Provision By Everything options), Hardware C External Data source conditions.
 Remediations Actions are not applicable for Agentless Posture type.

Conditions

User Defined Conditions >
 Cisco Defined Conditions >

Select Conditions

Cisco ISE Work Centers - Posture Evaluation Mode 79 Days

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy

Anti-Malware
Anti-Spyware
Anti-Virus
File
Firewall
Launch Program
Link
Patch Management
Windows Server Update S...
Windows Update
USB

Requirements

Compliance Module	Posture Type
earlier	using AnyConnect if ANY_av_win_inst
using 4.x or later	using AnyConnect

Note: Remediation Action is filtered based on the operating system and stealth mode selection.
Remediation Actions are not applicable for Application Conditions (configured using the Provisioning External Data source conditions).
Remediations Actions are not applicable for Agentless Posture type.

User Defined Conditions

- Anti-Virus Condition
- Anti-Spyware Condition
- Anti-Malware Condition
- Firewall Condition**
- Patch Management Condition
- Disk Encryption Condition

Select Conditions

Save

Cisco ISE Work Centers - Posture Evaluation Mode 79 Days

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy

Anti-Malware
Anti-Spyware
Anti-Virus
File
Firewall
Launch Program
Link
Patch Management
Windows Server Update S...
Windows Update
USB

Requirements

Compliance Module	Posture Type
using Temporal Agent	met Default_Firewall_Condition_Mac
x or later	using AnyConnect

Note: Remediation Action is filtered based on the operating system and stealth mode selection.
Remediation Actions are not applicable for Application Conditions (configured using the Provisioning External Data source conditions).
Remediations Actions are not applicable for Agentless Posture type.

Firewall Condition

- Default_Firewall_Condition_Win
- LM_WIN_FIREWALL**
- Default_Firewall_Condition_Win

✓ Mục Remediation: LW_WIN_FW

The screenshot shows the Cisco ISE interface for configuring a Policy Element. The 'Remediations' dropdown menu is open, showing a list of remediation actions. 'LW_WIN_FW' is selected and highlighted.

Compliance Module	Posture Type	Conditions
using Temporal Agent	met if Default_Firewall_Condition_Mac	then Default_Firewall_Re-mediation_Mac
x or later	using AnyConnect	met if LM_WI...

Note: Remediation Action is filtered based on the operating system and stealth mode selection. Remediation Actions are not applicable for Application Conditions (configured using the Provision By Category or Provision External Data source conditions). Remediations Actions are not applicable for Agentless Posture type.

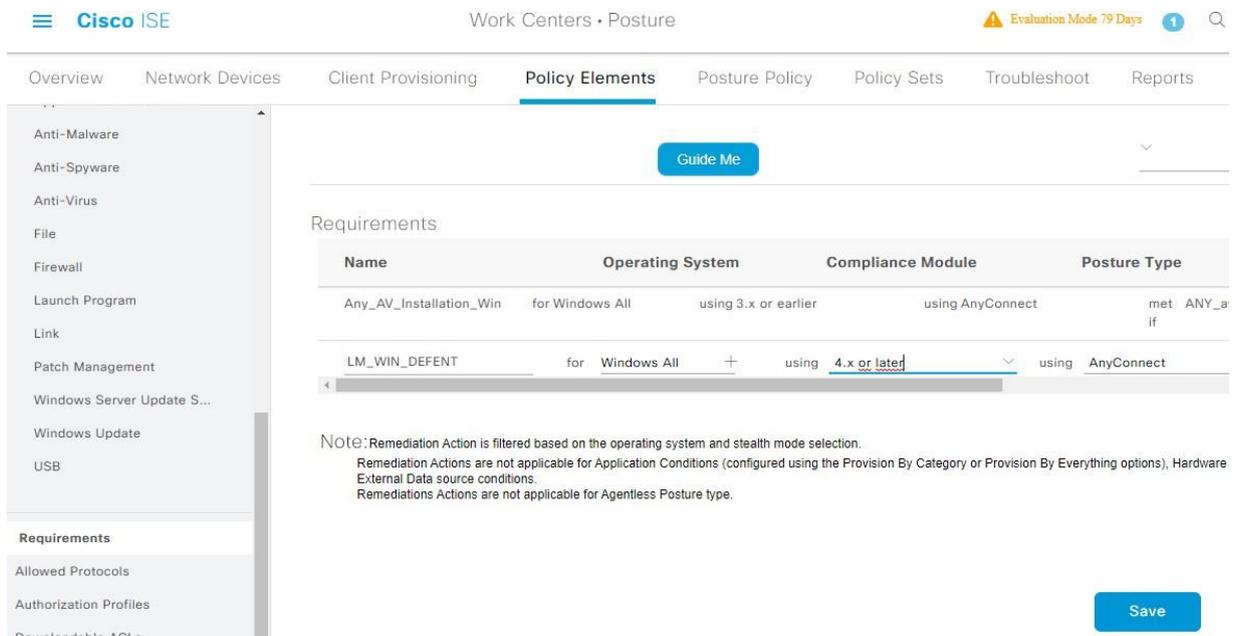
✓ Mục Message Show to Agent User: “Window firewall disable, please click to enable manually”

The screenshot shows the Cisco ISE interface for configuring a Policy Element. The 'Message Shown to Agent User' field is visible, containing the text: "Window firewall disable, please click to enable manually".

Compliance Module	Posture Type	Conditions	Remediations Ac
using Temporal Agent	met if Default_Firewall_Condition_Mac	then Default_Firewall_Re-mediation_Mac	
x or later	using AnyConnect	met if LM_WI...	LW_WIN_FW

Note: Remediation Action is filtered based on the operating system and stealth mode selection. Remediation Actions are not applicable for Application Conditions (configured using the Provision By Category or Provision External Data source conditions). Remediations Actions are not applicable for Agentless Posture type.

- ✓ Add +
- ✓ Name: LM_WIN_DEFENT
- ✓ Windows All: Windows All
- ✓ Compliance Module : 4.x or later
- ✓ Posture Type: Anyconnect

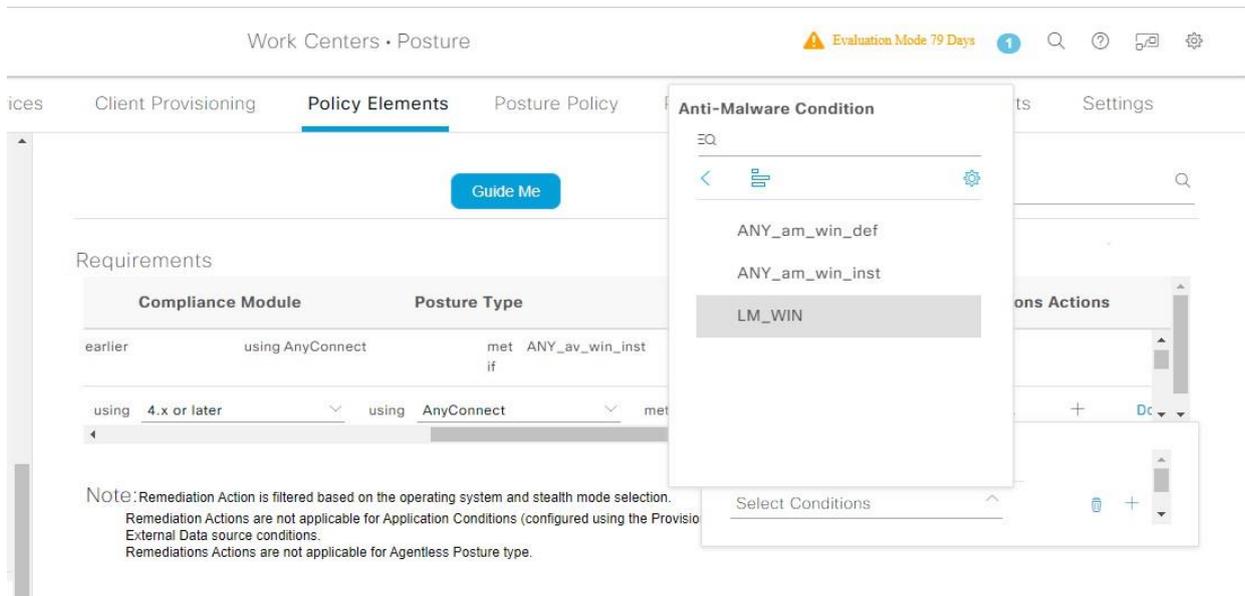
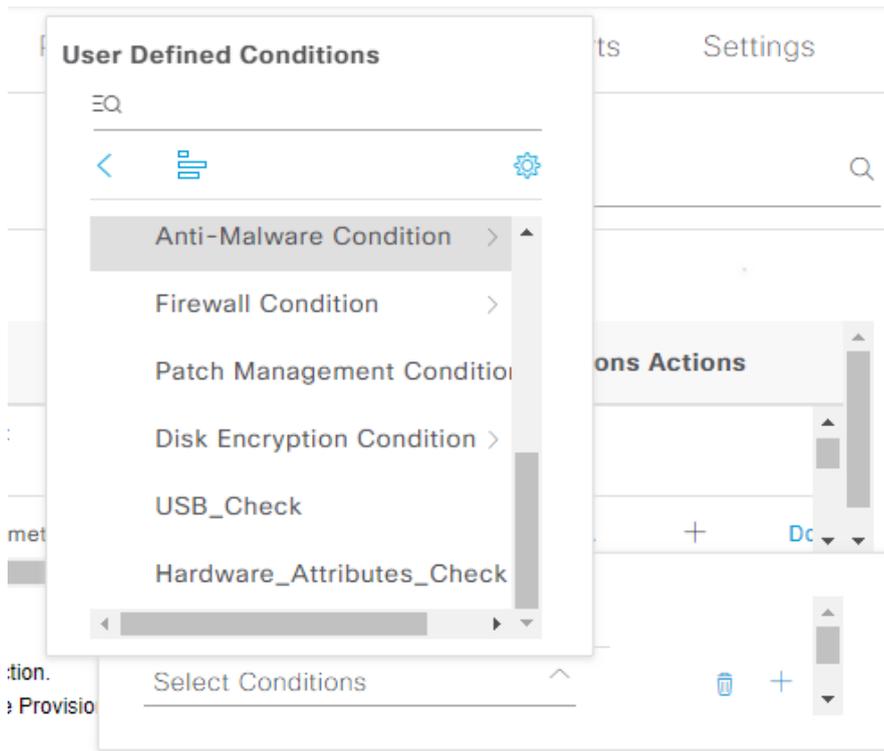


The screenshot shows the Cisco ISE interface for configuring a Posture Policy Element. The left sidebar lists various categories like Anti-Malware, Firewall, and Windows Update. The main area is titled 'Requirements' and contains a table with the following data:

Name	Operating System	Compliance Module	Posture Type
Any_AV_Installation_Win	for Windows All	using 3.x or earlier	using AnyConnect
LM_WIN_DEFENT	for Windows All	using 4.x or later	using AnyConnect

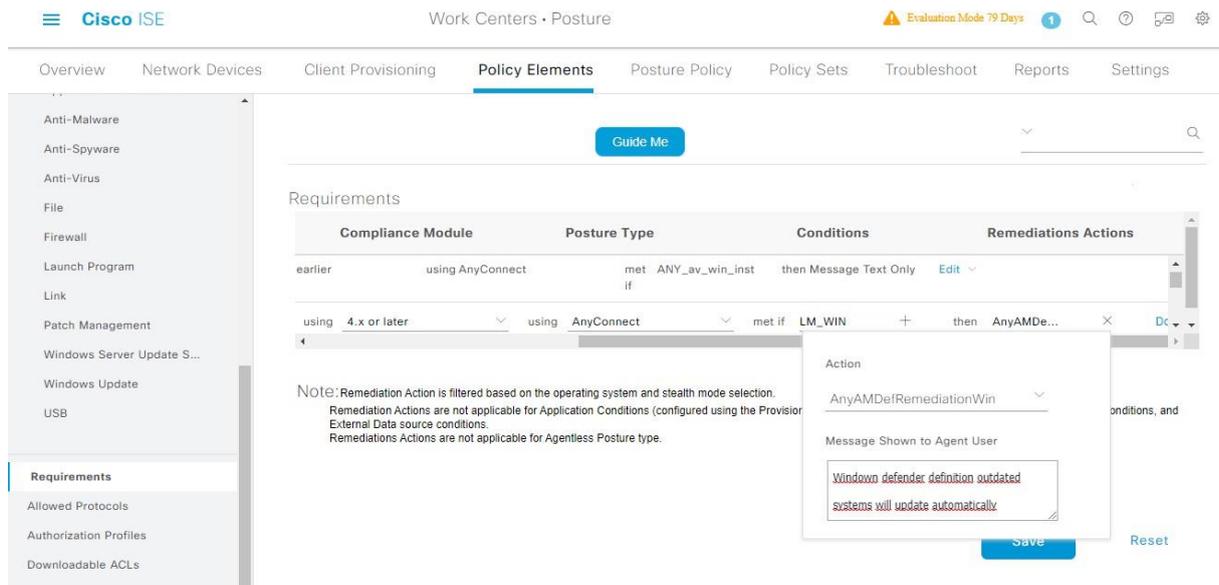
Below the table, there is a note: "Note: Remediation Action is filtered based on the operating system and stealth mode selection. Remediation Actions are not applicable for Application Conditions (configured using the Provision By Category or Provision By Everything options), Hardware External Data source conditions. Remediations Actions are not applicable for Agentless Posture type." A 'Save' button is located at the bottom right of the configuration area.

- ✓ User Defined Conditions / Anti-Malware Condition / LM_WIN

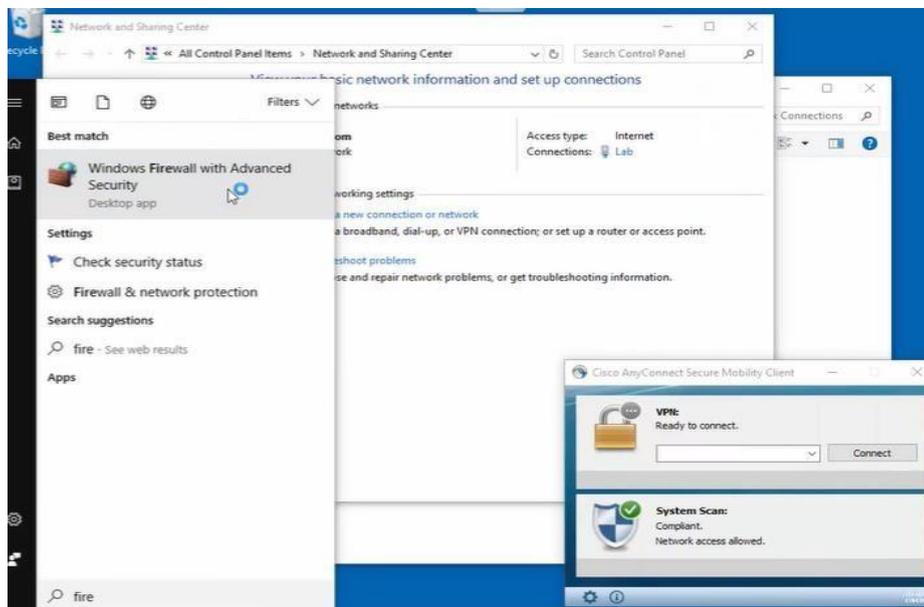


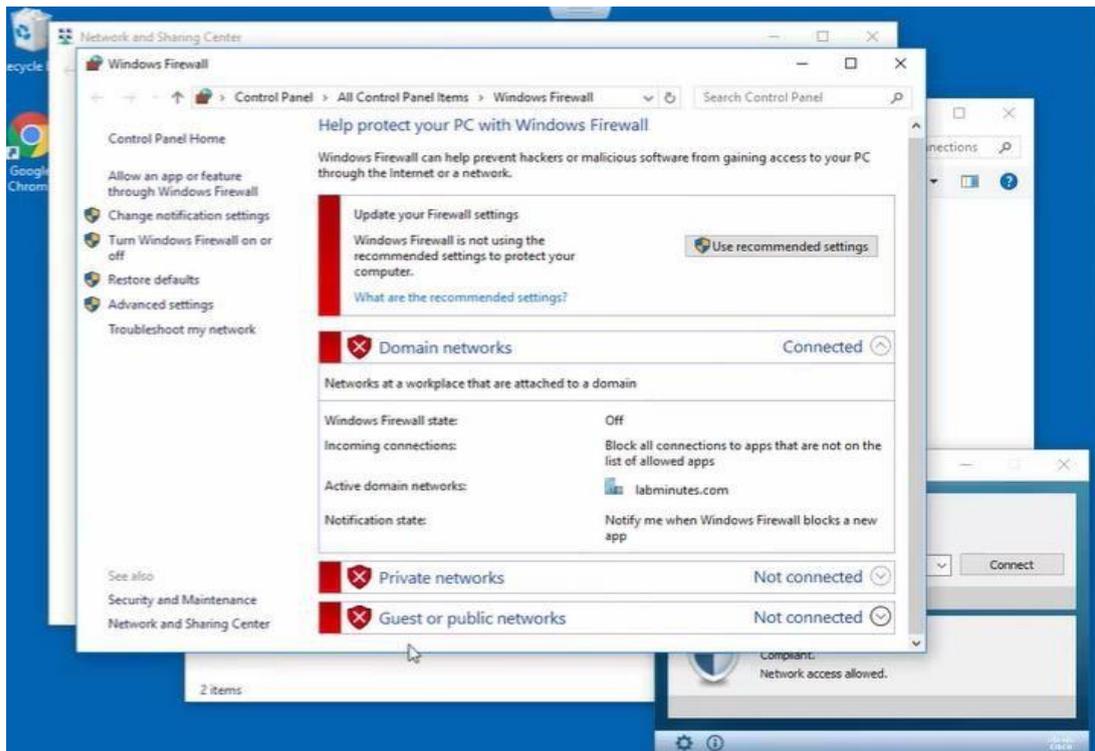
✓ Remediations Action: Chọn AnyAMDefRemediation /

✓ Message Show to Agent User: Win Windows defender definition outdated systems will update automatically

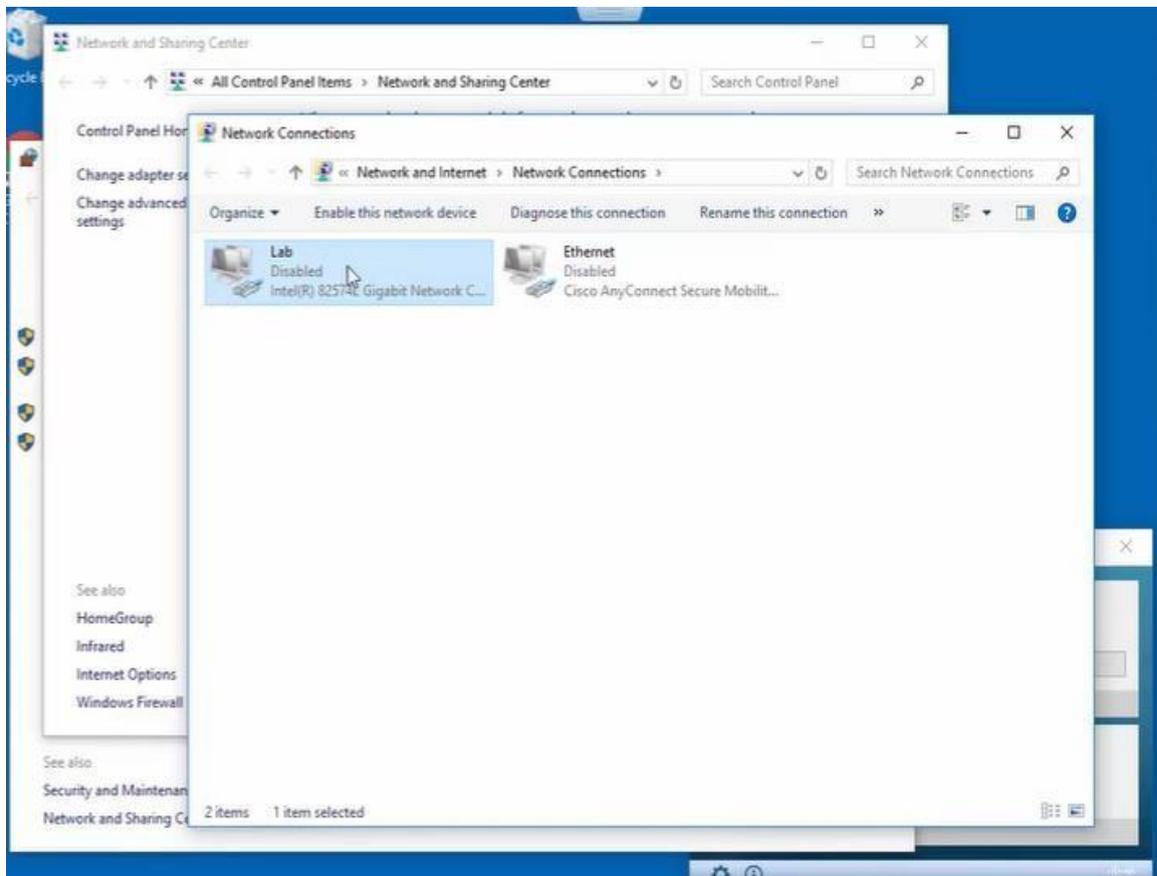


- ✓ Chuyển hướng đến Windows: mở Windows Firewall with Advanced Security
- ✓ Tắt firewall để đáp ứng điều kiện Non Compliant của Anyconnect Complaint

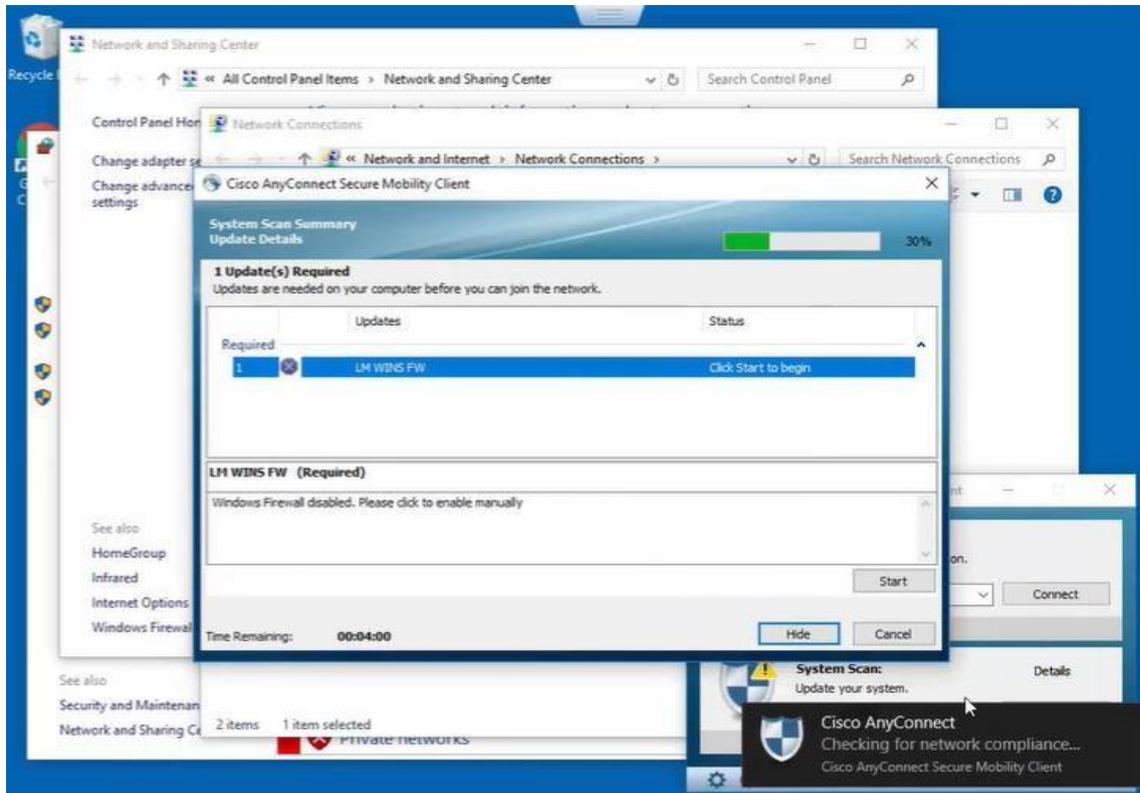




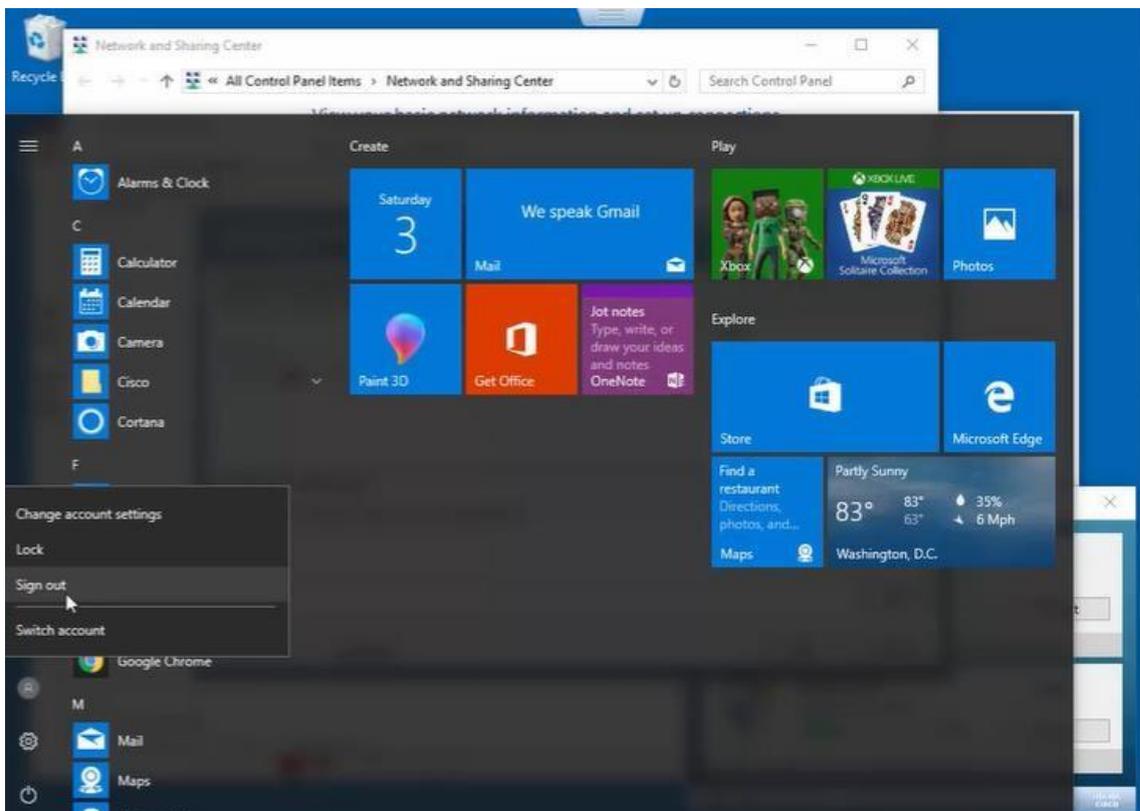
✓ Tắt mở lại card mạng:

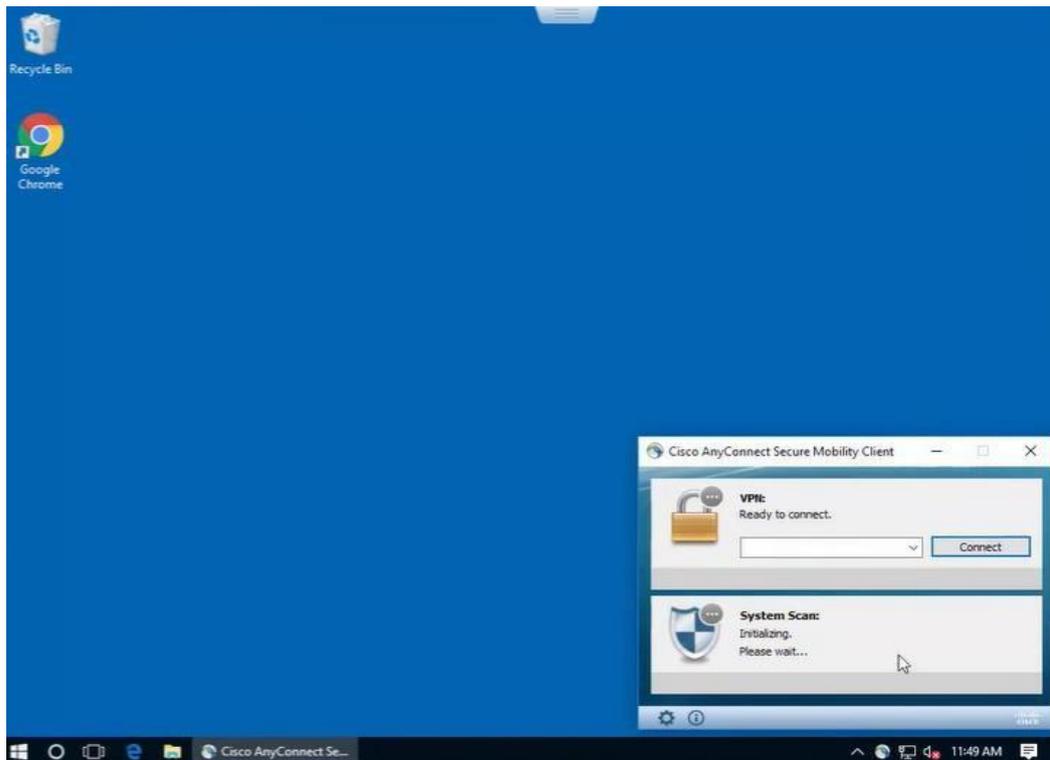


✓ Lick vào Systems scan: Cisco AnyConnect Secure Mobility Client: LM WINS FW



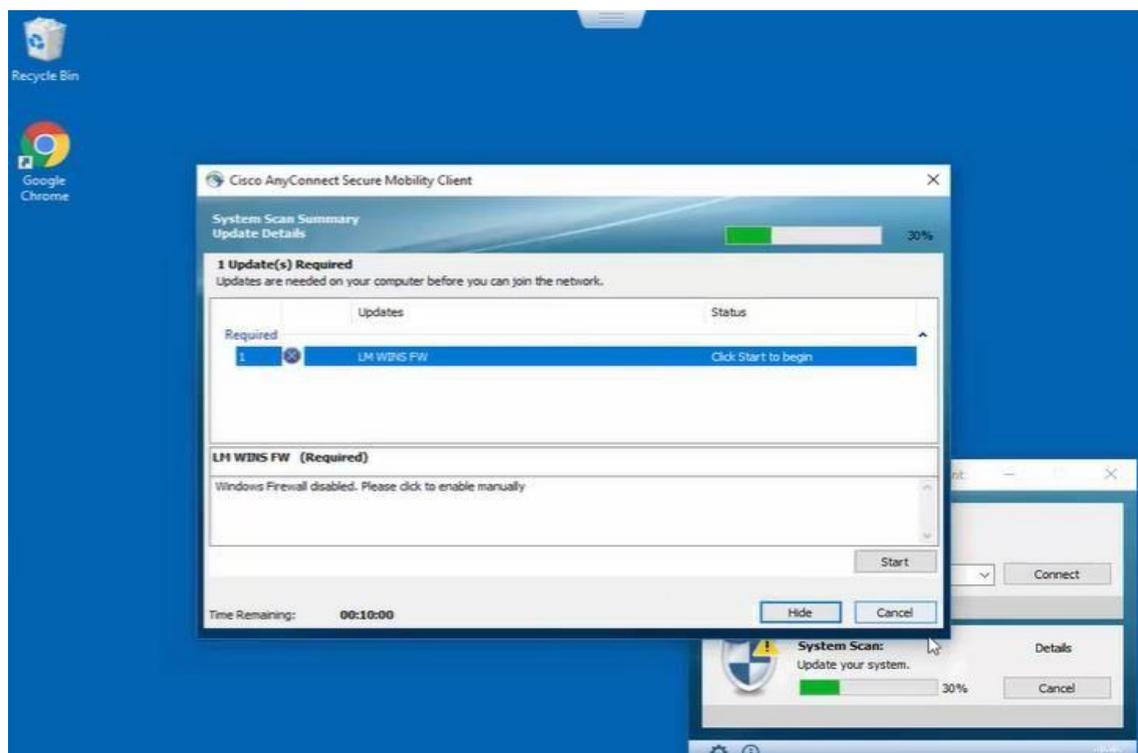
✓ Log out

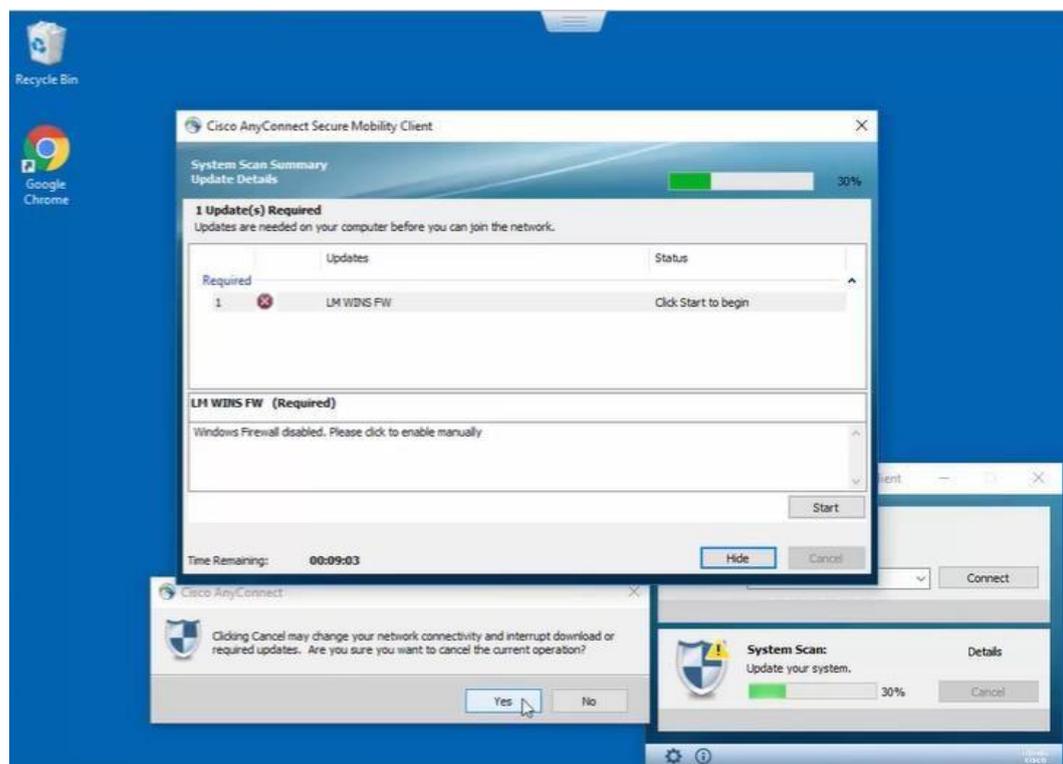
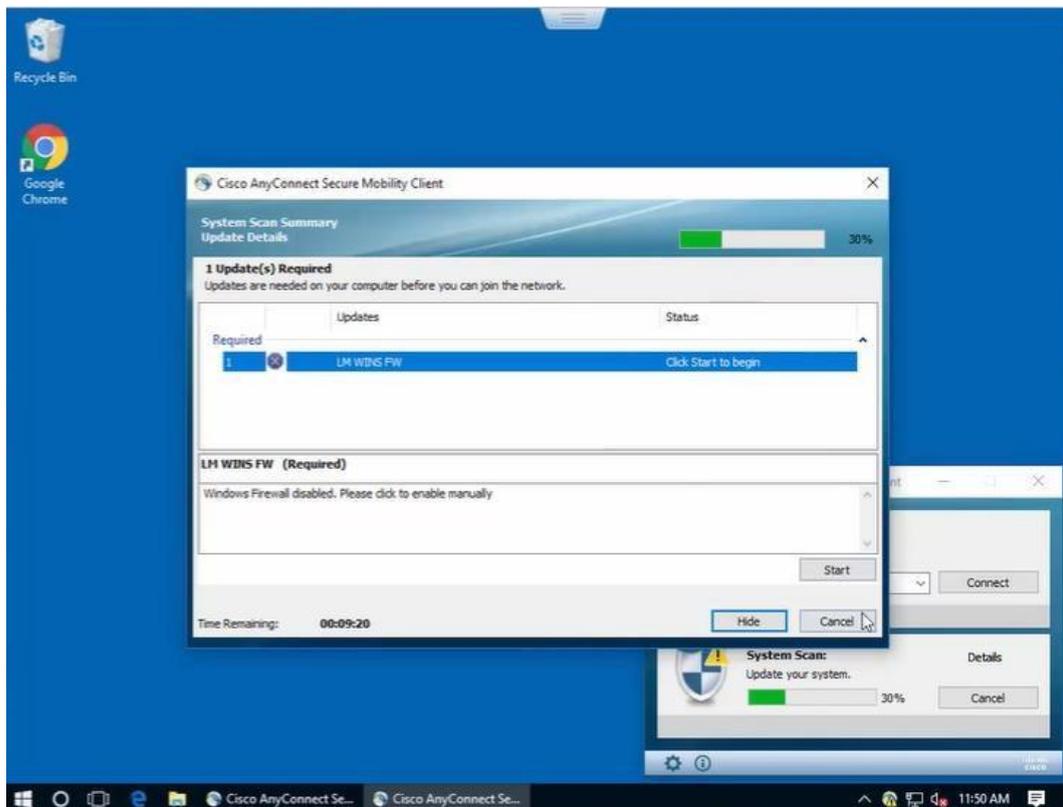




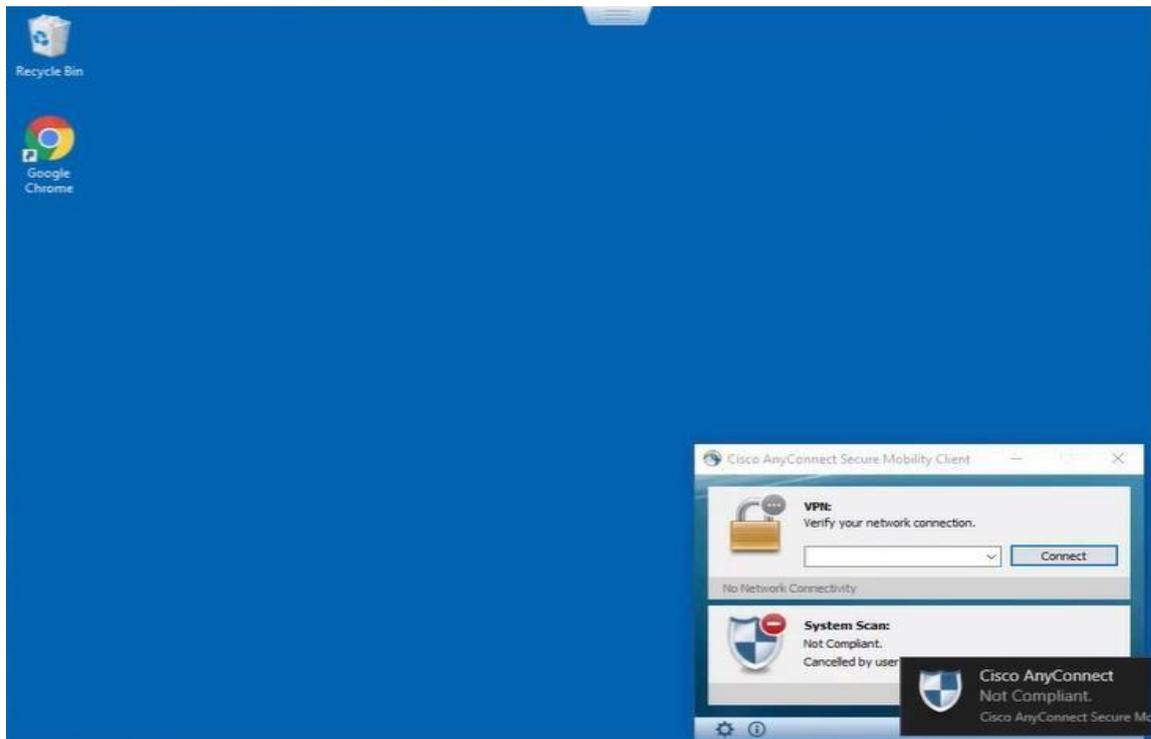
✓ Chú ý dòng LM WIN FW (Required)

✓ Windows Firewall disabled. Please click to enable manually

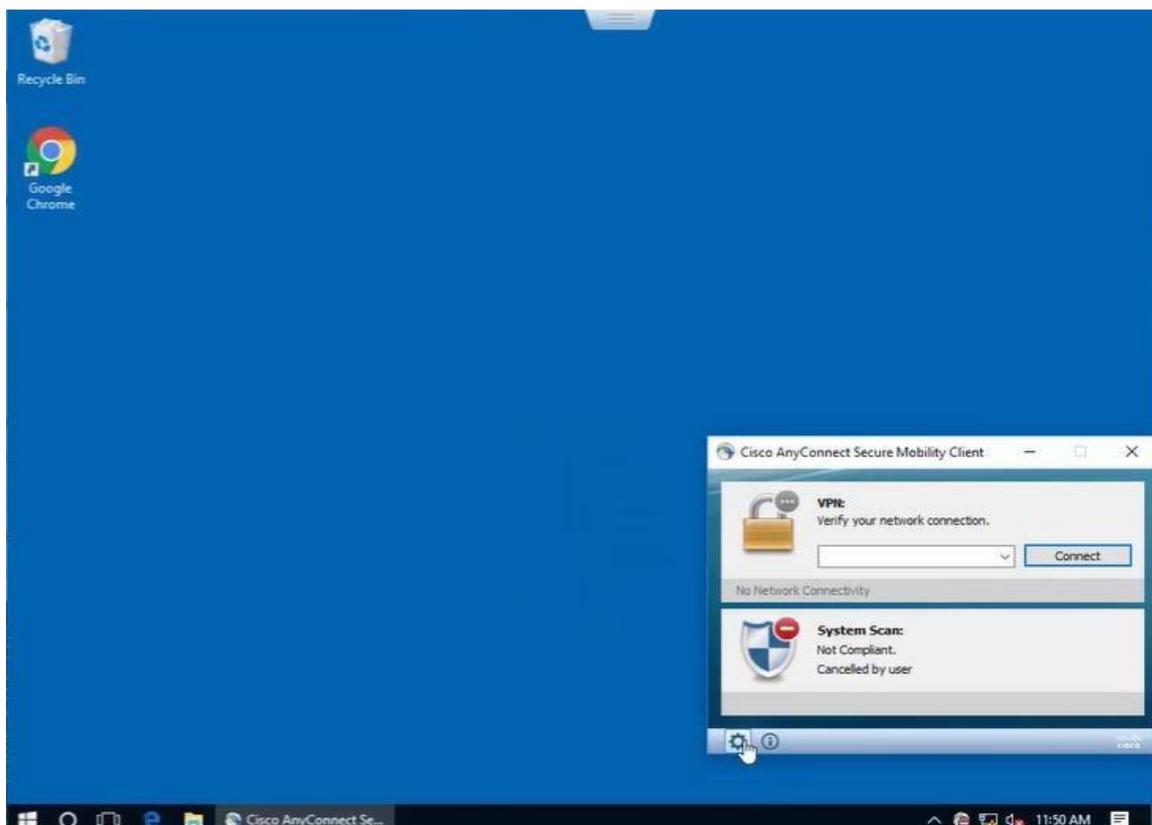




✓ Hệ thống System Scan: chuyển sang trạng thái Not Complain



✓ Click vào biểu tượng bánh răng để setting



Mục System Scan: chuyển đến tab Scan Summary:

- ✓ LM WIN FW (Not Requireds)
- ✓ LM WIN DEFENDER DEF (Requires)

