

FTD에 대한 LDAP 인증 및 권한 부여를 사용하여 RA VPN 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[라이선스 요구 사항](#)

[FMC의 컨피그레이션 단계](#)

[영역/LDAP 서버 컨피그레이션](#)

[RA VPN 컨피그레이션](#)

[다음을 확인합니다.](#)

소개

이 문서에서는 Firepower Management Center에서 관리하는 Firepower FTD(Threat Defense)에서 LDAP AA를 사용하는 원격 액세스 VPN을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- RA VPN(Remote Access VPN) 작동에 대한 기본 지식
- FMC(Firepower 관리 센터)를 통한 탐색 이해
- Microsoft Windows Server에서 LDAP(Lightweight Directory Access Protocol) 서비스 구성

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco Firepower Management Center 버전 7.3.0
- Cisco Firepower Threat Defense 버전 7.3.0
- LDAP 서버로 구성된 Microsoft Windows Server 2016

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서에서는 FMC(Firepower 관리 센터)에서 관리하는 FTD(Firepower Threat Defense)에서 LDAP(Lightweight Directory Access Protocol) 인증 및 권한 부여를 사용하는 RA VPN(Remote Access VPN)의 구성에 대해 설명합니다.

LDAP는 분산형 디렉토리 정보 서비스에 액세스하고 이를 유지 관리하기 위한 개방적이고 벤더에 종립적인 업계 표준 애플리케이션 프로토콜입니다.

LDAP 특성 맵은 AD(Active Directory) 또는 LDAP 서버에 있는 특성을 Cisco 특성 이름과 일치시킵니다. 그런 다음 AD 또는 LDAP 서버가 원격 액세스 VPN 연결 설정 중에 FTD 디바이스에 인증 응답을 반환하면 FTD 디바이스는 이 정보를 사용하여 AnyConnect 클라이언트가 연결을 완료하는 방법을 조정할 수 있습니다.

LDAP 특성 맵을 구성하고 영역 서버와 연결하기 위해 버전 6.2.1 및 FMC 버전 6.7.0 이전의 LDAP 권한 부여가 FlexConfig를 통해 권고되었기 때문에 LDAP 인증을 사용하는 RA VPN이 FMC에서 지원됩니다. 버전 6.7.0의 이 기능은 이제 FMC의 RA VPN 컨피그레이션 마법사와 통합되었으며 더 이상 FlexConfig를 사용할 필요가 없습니다.



참고: 이 기능을 사용하려면 FMC가 버전 6.7.0에 있어야 하지만 관리되는 FTD는 버전 6.3.0보다 큰 모든 버전에 있어야 합니다.

라이선스 요구 사항

내보내기 제어 기능이 활성화된 AnyConnect Apex, AnyConnect Plus 또는 AnyConnect VPN Only 라이선스가 필요합니다.

라이선스를 확인하려면 **System > Licenses > Smart Licenses**.

Smart License Status		Cisco Smart Software Manager  
Usage Authorization:		Authorized (Last Synchronized On May 18 2023)
Product Registration:		Registered (Last Renewed On May 18 2023)
Assigned Virtual Account:		SEC TAC
Export-Controlled Features:		Enabled

Devices without license ⌵

Q Search

FTD73

Add

Devices with license (1)

FTD73

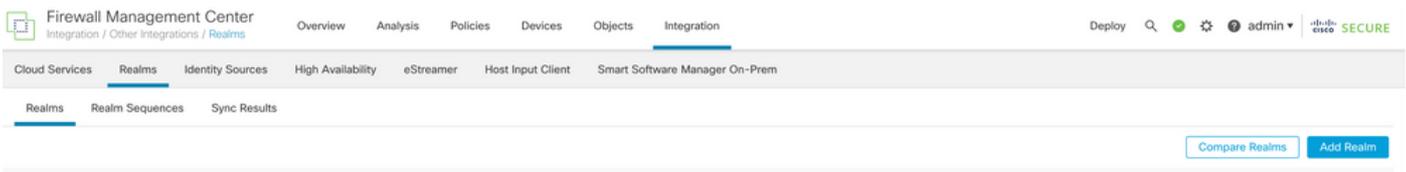
Cancel Apply

FMC의 컨피그레이션 단계

영역/LDAP 서버 컨피그레이션

참고: 나열된 단계는 새 REALM/LDAP 서버의 컨피그레이션을 위한 경우에만 필요합니다. RA VPN에서 인증에 사용할 수 있는 사전 구성된 서버가 있는 경우 [RA VPN Configuration\(RA VPN 컨피그레이션\)](#)으로 [이동합니다](#).

1단계. 탐색 System > Other Integrations > Realms이 그림에 나와 있는 것처럼.



2단계. 그림에 표시된 대로 Add a new realm.

Compare Realms

Add Realm

3단계. AD 서버 및 디렉터리에 대한 세부 정보를 제공합니다. 클릭 OK.

이 데모의 목적:

이름: LDAP

유형: AD

AD 주 도메인: test.com

디렉토리 사용자 이름: CN=Administrator,CN=Users,DC=test,DC=com

디렉터리 암호: <숨김>

기본 DN: DC=test,DC=com

그룹 DN: DC=test,DC=com

Add New Realm



Name*	Description
<input type="text"/>	<input type="text"/>
Type	AD Primary Domain
AD	<input type="text"/>
	<i>E.g. domain.com</i>
Directory Username*	Directory Password*
<input type="text"/>	<input type="password"/>
<i>E.g. user@domain.com</i>	
Base DN	Group DN
<input type="text"/>	<input type="text"/>
<i>E.g. ou=group,dc=cisco,dc=com</i>	<i>E.g. ou=group,dc=cisco,dc=com</i>

Directory Server Configuration

^ New Configuration

Hostname/IP Address*	Port*
<input type="text"/>	636
Encryption	CA Certificate*
LDAPS	Select certificate

Interface used to connect to Directory server ⓘ

Resolve via route lookup

Choose an interface

Default: Management/Diagnostic Interface

[Add another directory](#)

Cancel

Configure Groups and Users

4단계. 클릭 Save 이 이미지에 표시된 대로 영역/디렉토리 변경 사항을 저장합니다.

Cancel

Save

5단계. 전환 State 이 이미지에 표시된 대로 서버의 상태를 Enabled(활성화됨)로 변경하는 버튼입니다.

State



Enabled



RA VPN 컨피그레이션

이 단계는 인증된 VPN 사용자에게 할당되는 그룹 정책을 구성하는 데 필요합니다. 그룹 정책이 이미 정의된 경우 [5단계](#)로 이동합니다.

1단계. 탐색 Objects > Object Management.

ent Center
ent

Overview

Analysis

Policies

Devices

Objects

Integration

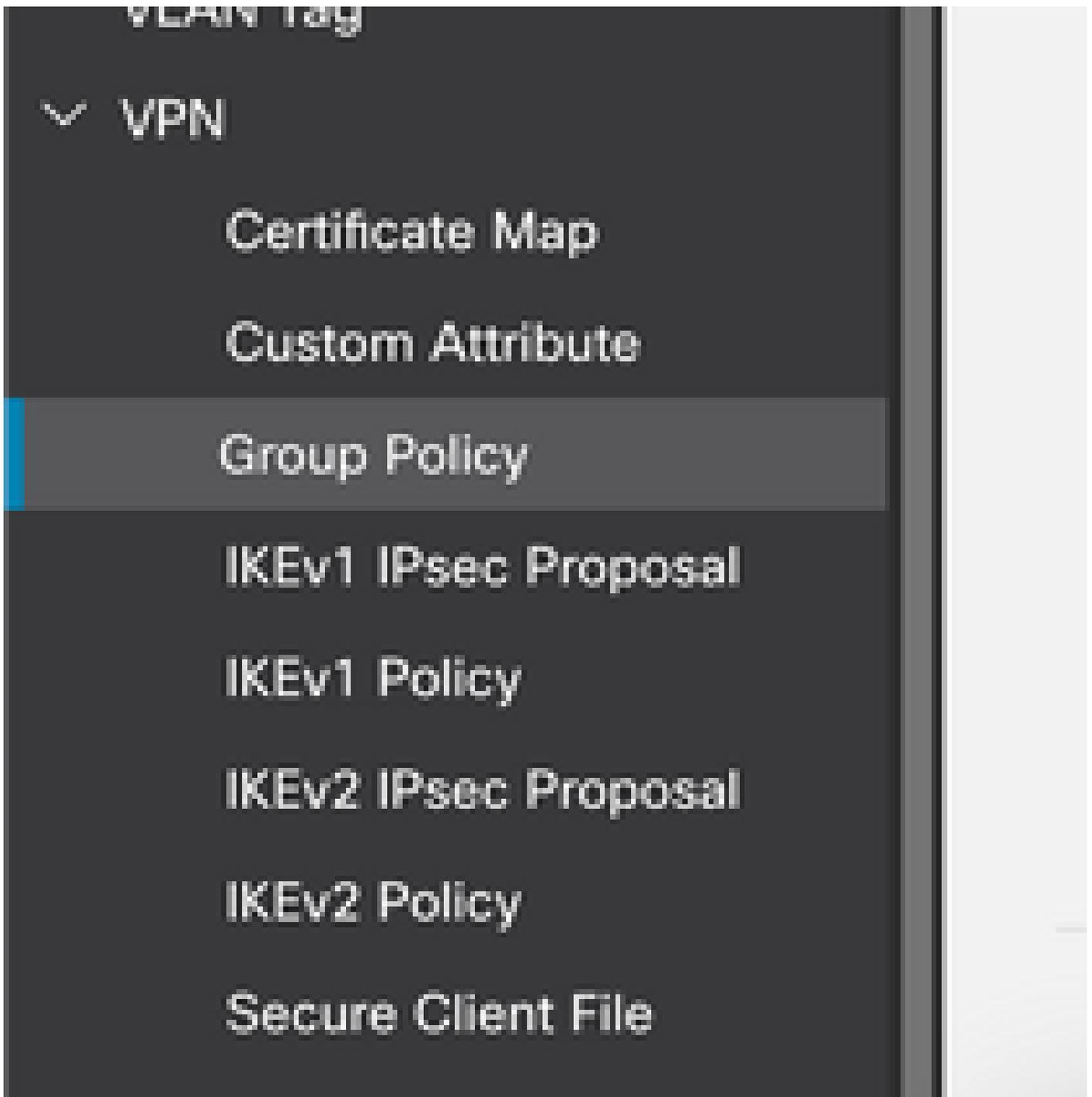
Network

A network object represents one or more IP addresses. Network objects are used in various processes, including access control lists, intrusion detection, and so on.

Object Management

Intrusion Rules

2단계: 왼쪽 창에서 VPN > Group Policy.



3단계: Add Group Policy.

[Add Group Policy](#)

4단계: Group Policy(그룹 정책) 값을 제공합니다.

이 데모의 목적:

이름: RA-VPN

배너: ! VPN에 오신 것을 환영합니다!

사용자당 동시 로그인: 3(기본값)

Add Group Policy



Name:*

Description:

General

Secure Client

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

Banner:

Maximum total size: 3999, Maximum characters in a line : 497.

In case of a line spanning more than 497 characters, split the line into multiple lines.

** Only plain text is supported (symbols '<' and '>' are not allowed)

Add Group Policy

Name:*

RA-VPN

Description:

General

Secure Client

Advanced

Traffic Filter

Session Settings

Access Hours:

Unrestricted



Simultaneous Login Per User:

3

(Range 0-2147483647)

5단계. 탐색 [Devices](#) > [VPN](#) > [Remote Access](#).

Devices

Objects

Integration

Device Management

Device Upgrade

NAT

QoS

Platform Settings

FlexConfig

Certificates

VPN

Site To Site

Remote Access

Dynamic Access Policy

Troubleshooting

Troubleshoot

File Download

Threat Defense CLI

Packet Tracer

Packet Capture

6단계. 클릭 [Add a new configuration](#).

Status	Last Modified
No configuration available Add a new configuration	

7단계. 제공: Name RA VPN 정책. 선택 VPN Protocols 선택 Targeted Devices. 클릭 Next.

이 데모의 목적:

이름: RA-VPN

VPN 프로토콜: SSL

대상 장치: FTD

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 Secure Client — 4 Access & Certificate — 5 Summary

Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:*

Description:

VPN Protocols:

SSL
 IPsec-IKEv2

Targeted Devices:

Available Devices	Selected Devices
<input type="text" value="Q Search"/> <div style="background-color: #0070C0; color: white; padding: 2px;">FTD73</div>	<div style="border: 1px solid #ccc; padding: 5px;">FTD73 🗑️</div>

8단계. 의 경우 Authentication Method, 선택 AAA Only. 에 대한 REALM/LDAP 서버를 선택합니다.
 Authentication Server. 클릭 Configure LDAP Attribute Map (LDAP 권한 부여를 구성합니다.)

Connection Profile:

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name:*

i This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method:

Authentication Server:* +

(LOCAL or Realm or RADIUS)

Fallback to LOCAL Authentication

Authorization Server: +

(Realm or RADIUS)

[Configure LDAP Attribute Map](#)

9단계. 제공: LDAP Attribute Name 및 Cisco Attribute Name. **클릭 Add Value Map.**

이 데모의 목적:

LDAP 특성 이름: memberOf

Cisco 특성 이름: 그룹 정책

Configure LDAP Attribute Map



Realm:

AD (AD)

LDAP attribute Maps:



Name Map:	
LDAP Attribute Name	Cisco Attribute Name
<input type="text" value="memberOf"/>	<input type="text" value="Group-Policy"/>
Value Maps:	
LDAP Attribute Value	Cisco Attribute Value
	Add Value Map

Cancel

OK

10단계. 제공: LDAP Attribute Value 및 Cisco Attribute Value. 클릭 OK.

이 데모의 목적:

LDAP 특성 값: DC=taolocan,DC=sec

Cisco 특성 값: RA-VPN

LDAP attribute Maps:



Name Map:	
LDAP Attribute Name	Cisco Attribute Name
<input type="text" value="memberOf"/>	<input type="text" value="Group-Policy"/>
Value Maps:	
LDAP Attribute Value	Cisco Attribute Value
<input type="text" value="dc=taolocan,dc=sec"/>	<input type="text" value="RA-VPN"/>

Copyright © 2013 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

 참고: 요구 사항에 따라 더 많은 값 맵을 추가할 수 있습니다.

11단계. 추가 Address Pool 로컬 주소 할당. 클릭 OK.

Address Pools ?

Available IPv4 Pools ⊞

VPN-Pool

Add

Selected IPv4 Pools

VPN-Pool 🗑

Cancel

OK

12단계. 제공: **Connection Profile Name** 및 Group-Policy. 클릭 Next.

이 데모의 목적:

연결 프로파일 이름: RA-VPN

인증 방법: AAA만

인증 서버: LDAP

IPv4 주소 풀: VPN 풀

그룹 정책: 액세스 금지

 참고: 인증 방법, 인증 서버 및 IPV4 주소 풀은 이전 단계에서 구성되었습니다.

No-Access 그룹 정책에는 Simultaneous Login Per User 매개변수를 0(사용자가 기본 No-Access group-policy를 수신하는 경우 로그인할 수 없도록 설정)으로 설정합니다.

Add Group Policy

Name:*

No-Access

Description:

General

Secure Client

Advanced

Traffic Filter

Session Settings

Access Hours:

Unrestricted

+

Simultaneous Login Per User:

0

(Range 0-2147483647)

13단계. 클릭 [Add new AnyConnect Image](#) 을(를) 추가하려면 [AnyConnect Client Image](#) FTD에 연결합니다

Secure Client Image

The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download Secure Client packages from [Cisco Software Download Center](#).

Select at least one Secure Client image

[Show Re-order buttons](#) +

<input checked="" type="checkbox"/>	Secure Client File Object Name	Secure Client Package Name	Operating System
No Secure Client Images configured Add new Secure Client Image			

14단계. 제공: Name 업로드된 이미지의 경우 로컬 스토리지에서 찾아 이미지를 업로드합니다. 클릭 Save.

Add Secure Client File



Name:*

mac

File Name:*

anyconnect-macos-4.10.07061-webdep

Browse..

File Type:*

Secure Client Image

Description:

Cancel

Save

15단계. 사용할 수 있도록 하려면 이미지 옆에 있는 확인란을 클릭합니다. 클릭 Next.

Secure Client Image

The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download Secure Client packages from [Cisco Software Download Center](#).

Show Re-order buttons +

<input checked="" type="checkbox"/>	Secure Client File Object Name	Secure Client Package Name	Operating System
<input checked="" type="checkbox"/>	Mac	anyconnect-macos-4.10.07061-webdeploy...	Mac OS

16단계. 다음을 선택합니다. Interface group/Security Zone 및 Device Certificate. 클릭 Next.

이 데모의 목적:

인터페이스 그룹/보안 영역: Out-Zone

디바이스 인증서: 자체 서명

 참고: 암호화된(VPN) 트래픽에 대한 액세스 제어 검사를 우회하려면 Bypass Access Control(액세스 제어 우회) 정책 옵션을 활성화할 수 있습니다(기본적으로 비활성화됨).



AAA

Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:* +

Enable DTLS on member interfaces

 All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* +

Enroll the selected certificate object on the target devices

Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

17단계. RA VPN 컨피그레이션의 요약을 확인합니다. 클릭 **Finish** 을 클릭하면 그림과 같이 저장할 수 있습니다.

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 Secure Client — 4 Access & Certificate — 5 Summary



Remote Access VPN Policy Configuration

Firewall Management Center will configure an RA VPN Policy with the following settings

Name:	RA-VPN
Device Targets:	FTD73
Connection Profile:	RA-VPN
Connection Alias:	RA-VPN
AAA:	
Authentication Method:	AAA Only
Authentication Server:	AD (AD)
Authorization Server:	-
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	VPN-Pool
Address Pools (IPv6):	-
Group Policy:	No-Access
Secure Client Images:	Mac
Interface Objects:	InZone

Additional Configuration Requirements

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

Access Control Policy Update

An **Access Control** rule must be defined to allow VPN traffic on all targeted devices.

NAT Exemption

If NAT is enabled on the targeted devices, you must define a **NAT Policy** to exempt VPN traffic.

DNS Configuration

To resolve hostname specified in AAA Servers or CA Servers, configure DNS using **FlexConfig Policy** on the targeted devices.

Port Configuration

SSL will be enabled on port 443.
IPsec-IKEv2 uses port 500 and Client Services will be enabled on port 443 for Secure Client image download. NAT-Traversal will be enabled

18단계. 탐색 Deploy > Deployment. 컨피그레이션을 구축해야 하는 FTD를 선택합니다. 클릭 Deploy.

구축에 성공한 후 컨피그레이션이 FTD CLI로 푸시됩니다.

```
<#root>
```

```
!--- LDAP Server Configuration ---!
```

```
ldap attribute-map LDAP
```

```
map-name memberOf Group-Policy  
map-value memberOf DC=t1alocan,DC=sec RA-VPN
```

```
aaa-server LDAP protocol ldap  
max-failed-attempts 4  
realm-id 2  
aaa-server LDAP host 10.106.56.137  
server-port 389  
ldap-base-dn DC=t1alocan,DC=sec  
ldap-group-base-dn DC=t1alocan,DC=sec  
ldap-scope subtree  
ldap-naming-attribute sAMAccountName  
ldap-login-password *****  
ldap-login-dn CN=Administrator,CN=Users,DC=test,DC=com  
server-type microsoft
```

```
ldap-attribute-map LDAP
```

```
!--- RA VPN Configuration ---!
```

```
webvpn
enable Outside
anyconnect image disk0:/csm/anyconnect-win-4.10.07061-webdeploy-k9.pkg 1 regex "Mac"
anyconnect enable
tunnel-group-list enable
error-recovery disable
```

```
ssl trust-point Self-Signed
```

```
group-policy No-Access internal
```

```
group-policy No-Access attributes
```

```
vpn-simultaneous-logins 0
```

```
vpn-idle-timeout 30
```

```
!--- Output Omitted ---!
```

```
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-tunnel-network-list none
```

```
group-policy RA-VPN internal
```

```
group-policy RA-VPN attributes
```

```
banner value ! Welcome to VPN !
```

```
vpn-simultaneous-logins 3
```

```
vpn-idle-timeout 30
```

```
!--- Output Omitted ---!
```

```
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-tunnel-network-list non
```

```
ip local pool VPN-Pool 10.72.1.1-10.72.1.150 mask 255.255.255.0
```

```
tunnel-group RA-VPN type remote-access
```

```
tunnel-group RA-VPN general-attributes
```

```
address-pool VPN-Pool
```

```
authentication-server-group LDAP
```

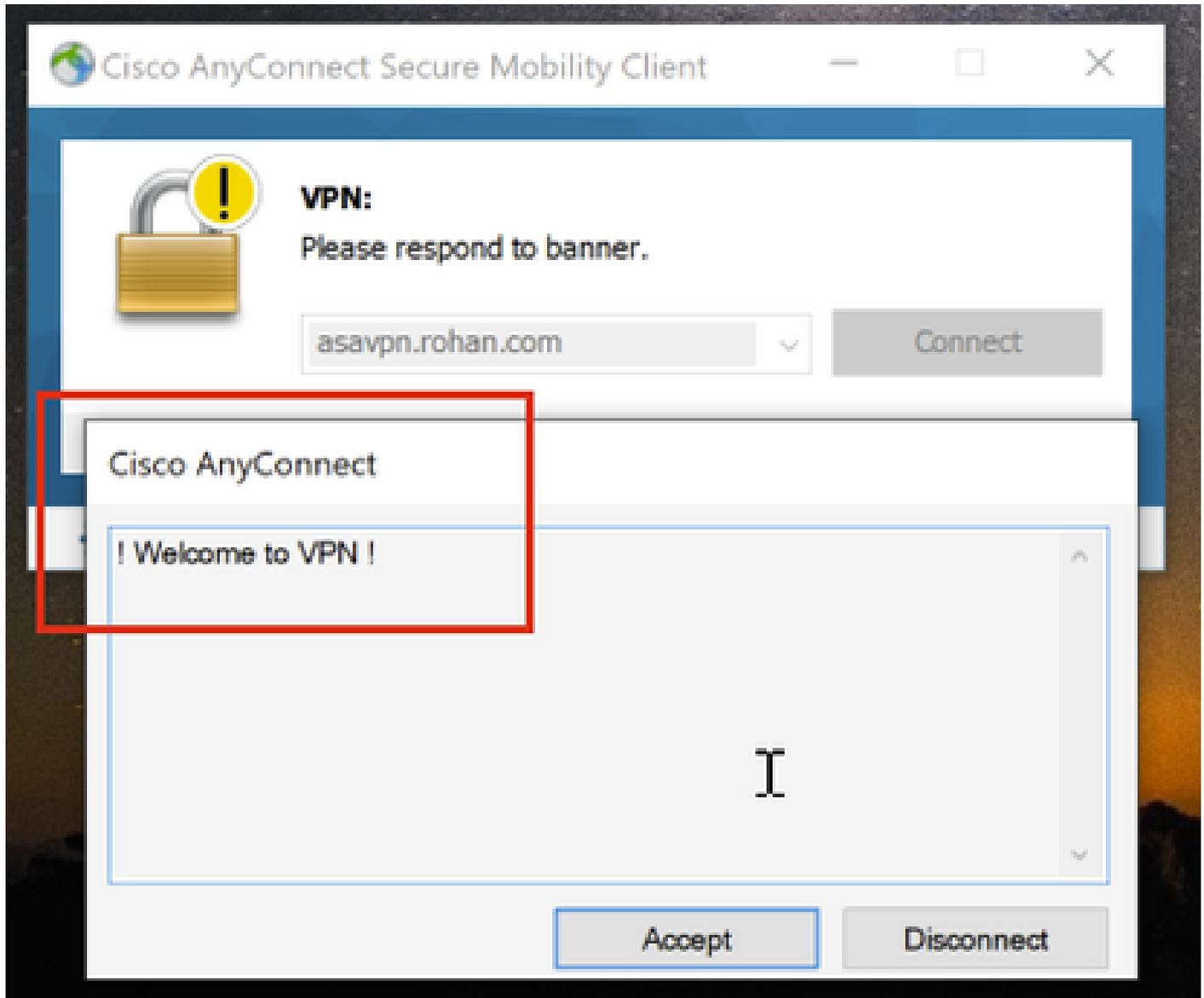
```
default-group-policy No-Access
```

```
tunnel-group RA-VPN webvpn-attributes
```

```
group-alias RA-VPN enable
```

다음을 확인합니다.

AnyConnect 클라이언트에서 Valid VPN User Group Credentials(유효한 VPN 사용자 그룹 자격 증명)로 로그인하면 LDAP 특성 맵에 의해 할당된 올바른 그룹 정책을 가져옵니다.



LDAP Debug Snippet(debug ldap 255)에서 LDAP 특성 맵에 일치하는 항목이 있음을 확인할 수 있습니다.

```
<#root>
```

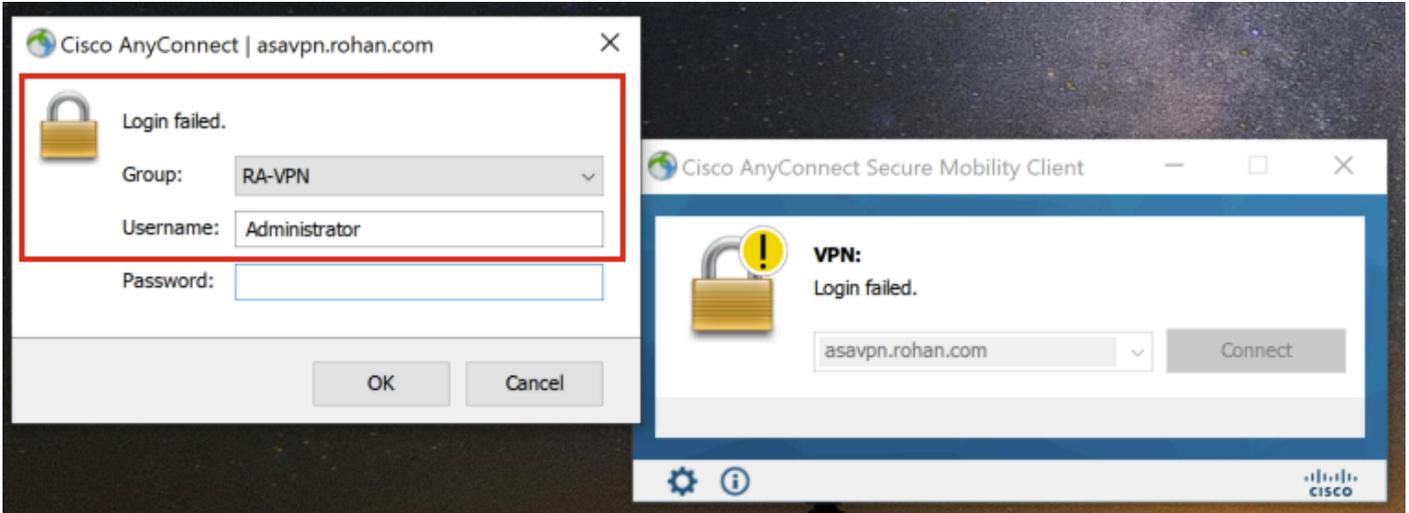
```
Authentication successful for test to 10.106.56.137
```

```
memberOf: value = DC=tlalocan,DC=sec
```

```
mapped to Group-Policy: value = RA-VPN
```

mapped to LDAP-Class: value = RA-VPN

AnyConnect 클라이언트에서 Invalid VPN User Group Credential(유효하지 않은 VPN 사용자 그룹 자격 증명)로 로그인하면 No-Access 그룹 정책이 적용됩니다.



<#root>

```
%FTD-6-113004: AAA user authentication Successful : server = 10.106.56.137 : user = Administrator
```

```
%FTD-6-113009: AAA retrieved default group policy (No-Access) for user = Administrator
```

```
%FTD-6-113013: AAA unable to complete the request Error : reason =
```

```
Simultaneous logins exceeded for user : user = Administrator
```

LDAP Debug Snippet(디버그 ldap 255)에서 LDAP 특성 맵에 일치하는 항목이 없음을 확인할 수 있습니다.

<#root>

```
Authentication successful for Administrator to 10.106.56.137
```

```
memberOf: value = CN=Group Policy Creator Owners,CN=Users,DC=t1alocan,DC=sec  
mapped to Group-Policy: value = CN=Group Policy Creator Owners,CN=Users,DC=t1alocan,DC=sec  
mapped to LDAP-Class: value = CN=Group Policy Creator Owners,CN=Users,DC=t1alocan,DC=sec  
memberOf: value = CN=Domain Admins,CN=Users,DC=t1alocan,DC=sec  
mapped to Group-Policy: value = CN=Domain Admins,CN=Users,DC=t1alocan,DC=sec  
mapped to LDAP-Class: value = CN=Domain Admins,CN=Users,DC=t1alocan,DC=sec  
memberOf: value = CN=Enterprise Admins,CN=Users,DC=t1alocan,DC=sec  
mapped to Group-Policy: value = CN=Enterprise Admins,CN=Users,DC=t1alocan,DC=sec  
mapped to LDAP-Class: value = CN=Enterprise Admins,CN=Users,DC=t1alocan,DC=sec  
memberOf: value = CN=Schema Admins,CN=Users,DC=t1alocan,DC=sec  
mapped to Group-Policy: value = CN=Schema Admins,CN=Users,DC=t1alocan,DC=sec
```

mapped to LDAP-Class: value = CN=Schema Admins,CN=Users,DC=tlalocan,DC=sec
memberOf: value = CN=IIS_IUSRS,CN=Builtin,DC=tlalocan,DC=sec
mapped to Group-Policy: value = CN=IIS_IUSRS,CN=Builtin,DC=tlalocan,DC=sec
mapped to LDAP-Class: value = CN=IIS_IUSRS,CN=Builtin,DC=tlalocan,DC=sec
memberOf: value = CN=Administrators,CN=Builtin,DC=tlalocan,DC=sec
mapped to Group-Policy: value = CN=Administrators,CN=Builtin,DC=tlalocan,DC=sec
mapped to LDAP-Class: value = CN=Administrators,CN=Builtin,DC=tlalocan,DC=sec

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.