

Configuration de RA VPN avec authentification et autorisation LDAP pour FTD

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Exigences de licence](#)

[Étapes de configuration sur FMC](#)

[Configuration du serveur REALM/LDAP](#)

[Configuration VPN RA](#)

[Vérifier](#)

Introduction

Ce document décrit comment configurer un VPN d'accès à distance avec LDAP AA sur un pare-feu Firepower Threat Defense (FTD) géré par un centre de gestion Firepower.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base du fonctionnement du VPN d'accès à distance (RA VPN).
- Comprendre la navigation dans le Centre de gestion Firepower (FMC).
- Configuration des services LDAP (Lightweight Directory Access Protocol) sur Microsoft Windows Server.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Cisco Firepower Management Center version 7.3.0
- Cisco Firepower Threat Defense version 7.3.0
- Microsoft Windows Server 2016, configuré comme serveur LDAP

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.


Informations générales

Ce document décrit la configuration d'un VPN d'accès à distance (RA VPN) avec authentification et autorisation LDAP (Lightweight Directory Access Protocol) sur une défense contre les menaces Firepower (FTD) gérée par un centre de gestion Firepower (FMC).

LDAP est un protocole d'application ouvert, indépendant du fournisseur et conforme aux normes de l'industrie, qui permet d'accéder aux services d'informations d'annuaire distribués et de les gérer.

Un mappage d'attributs LDAP met en correspondance les attributs qui existent dans Active Directory (AD) ou le serveur LDAP avec les noms d'attributs Cisco. Ensuite, lorsque le serveur AD ou LDAP renvoie des réponses d'authentification au périphérique FTD lors de l'établissement d'une connexion VPN d'accès à distance, le périphérique FTD peut utiliser les informations pour ajuster la façon dont le client AnyConnect établit la connexion.

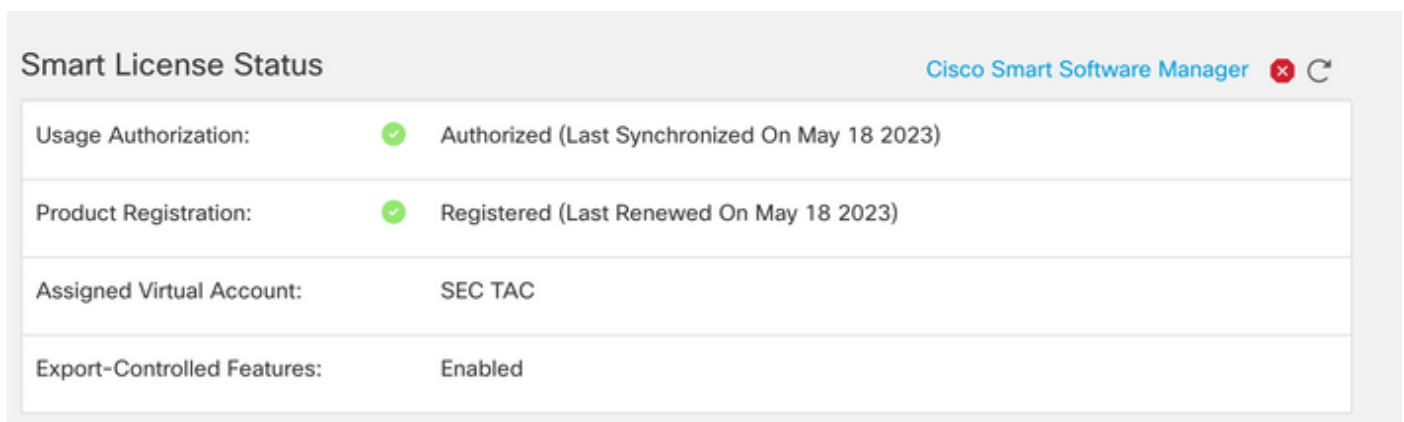
Un VPN RA avec authentification LDAP a été pris en charge sur le FMC depuis la version 6.2.1 et l'autorisation LDAP avant la version 6.7.0 du FMC a été conseillée via FlexConfig afin de configurer la carte d'attribut LDAP et de l'associer au serveur de domaine. Cette fonctionnalité, avec la version 6.7.0, a été intégrée à l'assistant de configuration VPN RA sur le FMC et ne nécessite plus l'utilisation de FlexConfig.

 Remarque : cette fonctionnalité nécessite que le FMC soit sur la version 6.7.0, alors que le FTD managé peut être sur toute version supérieure à 6.3.0.

Exigences de licence

Nécessite une licence AnyConnect Apex, AnyConnect Plus ou AnyConnect VPN Only avec fonctionnalité de contrôle des exportations activée.

Pour vérifier la licence, accédez à [System > Licenses > Smart Licenses](#).



The screenshot shows the 'Smart License Status' page in the Cisco Smart Software Manager. The page title is 'Smart License Status' and the Cisco Smart Software Manager logo is in the top right corner. The status is summarized in a table below:

| | | |
|-----------------------------|---|---|
| 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 |

Malware Defense

IPS

URL

Carrier

Secure Client Premier

Secure Client Advantage

Secure Client VPN Only

Devices without license C

FTD73

Add

Devices with license (1)


FTD73

Cancel

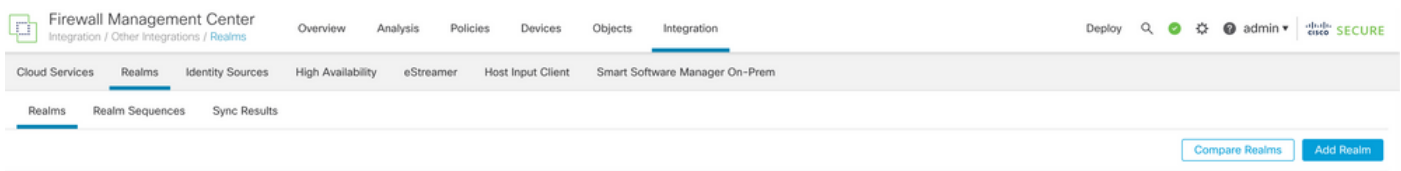
Apply

Étapes de configuration sur FMC

Configuration du serveur REALM/LDAP

 Remarque : les étapes répertoriées ne sont requises que si elles concernent la configuration d'un nouveau serveur REALM / LDAP. Si vous avez un serveur préconfiguré, qui pourrait être utilisé pour l'authentification dans RA VPN, alors naviguez vers [RA VPN Configuration](#).

Étape 1. Naviguez jusqu'à System > Other Integrations > Realms, comme le montre cette image.



Étape 2. Comme l'illustre l'image, cliquez sur **Add a new realm**.

[Compare Realms](#)

[Add Realm](#)

Étape 3. Fournissez les détails du serveur et du répertoire Active Directory. Cliquer OK.

Pour les besoins de cette démonstration :

Nom : LDAP

Type : AD

Domaine principal AD : test.com

Nom d'utilisateur du répertoire : CN=Administrateur, CN=Utilisateurs, DC=test, DC=com

Mot de passe du répertoire : <Masqué>

DN de base : DC=test, DC=com

Nom de domaine du groupe : 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

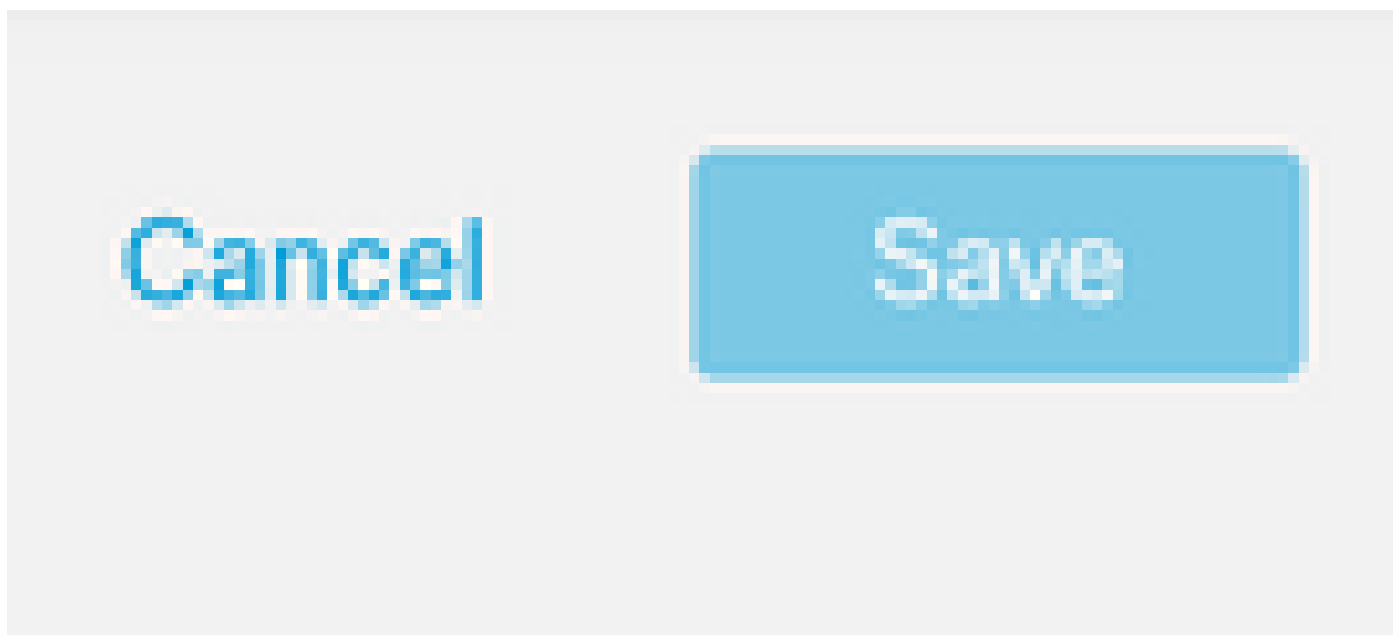
[Add another directory](#)

Cancel

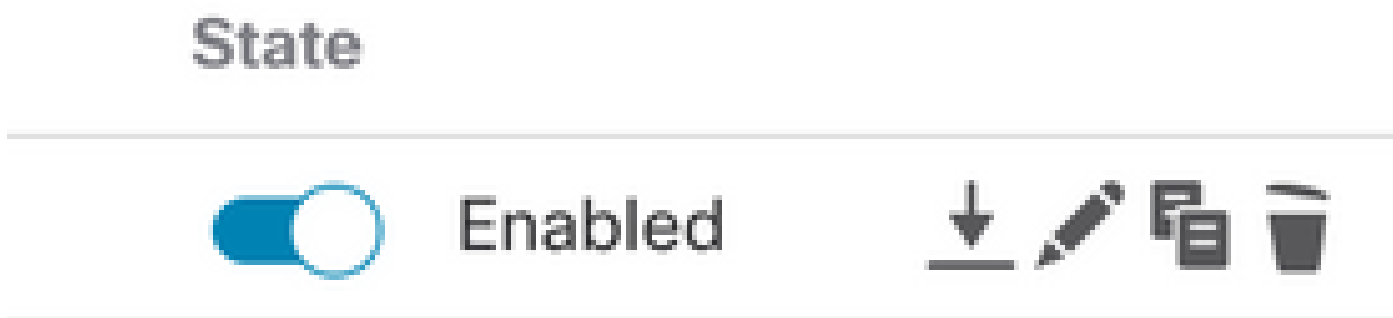
Configure Groups and Users

Étape 4. Cliquer `Save` pour enregistrer les modifications apportées au domaine (realm)/répertoire,

comme illustré dans cette image.



Étape 5. Basculer le `State` pour modifier l'état du serveur en `Activé`, comme illustré dans cette image.



Configuration VPN RA

Ces étapes sont nécessaires pour configurer la stratégie de groupe, qui est attribuée aux utilisateurs VPN autorisés. Si la stratégie de groupe est déjà définie, passez à [l'étape 5](#).

Étape 1. Naviguez jusqu'à `Objects > Object Management`.

Network

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

Object Management

Intrusion Rules

Étape 2 : Dans le volet gauche, accédez à VPN > Group Policy.

▼ VPN

Certificate Map

Custom Attribute

Group Policy

IKEv1 IPsec Proposal

IKEv1 Policy

IKEv2 IPsec Proposal

IKEv2 Policy

Secure Client File

Étape 3 : cliquez sur Add Group Policy.

Add Group Policy

 Filter

Étape 4 : fournissez les valeurs de stratégie de groupe.

Pour les besoins de cette démonstration :

Nom : RA-VPN

Bannière : ! Bienvenue sur VPN !

Connexion simultanée par utilisateur : 3 (par défaut)

Add Group Policy

Name:*

RA-VPN

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)

! Welcome to VPN!

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)

Étape 5. Naviguez jusqu'à [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

Étape 6. Cliquer [Add a new configuration](#).

| Status | Last Modified |
|--|---------------|
| No configuration available Add a new configuration | |

Étape 7. Fournir un **Name** pour la stratégie VPN RA. Choisir **VPN Protocols** et choisissez **Targeted Devices**. Cliquer **Next**.

Pour les besoins de cette démonstration :

Nom : RA-VPN

Protocoles VPN : SSL

Périphériques ciblés : 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="Search"/> <div style="border: 1px solid #ccc; padding: 2px;">FTD73</div> | <div style="border: 1px solid #ccc; padding: 2px;">FTD73 ✕</div> |
| <input type="button" value="Add"/> | |

Étape 8. Pour le **Authentication Method**, choisissez **AAA Only**. Choisissez le serveur **REALM / LDAP** pour le **Authentication Server**. Cliquer **Configure LDAP Attribute Map** (pour configurer l'autorisation LDAP).

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](#)

Étape 9. Fournir le LDAP Attribute Name et la Cisco Attribute Name. Cliquer **Add Value Map**.

Pour les besoins de cette démonstration :

Nom d'attribut LDAP : memberOf

Nom d'attribut Cisco : Stratégie de groupe

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 |
| | <input type="text" value=""/> |

[Add Value Map](#)

Cancel

OK

Étape 10. Fournir le LDAP Attribute Value et la Cisco Attribute Value. Cliquer **OK**.

Pour les besoins de cette démonstration :

Valeur d'attribut LDAP : DC=tlalocan, DC=sec

Valeur d'attribut Cisco : 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=tlalocan,dc=sec"/> | <input type="text" value="RA-VPN"/> |

[Add Value Map](#)



 Remarque : vous pouvez ajouter d'autres mappages de valeur en fonction des besoins.

Étape 11. Ajoutez le `Address Pool` pour l'attribution de l'adresse locale. Cliquez `OK`.

Address Pools ?

Available IPv4 Pools ⌂ +

VPN-Pool

Add

Selected IPv4 Pools

VPN-Pool 🗑

Cancel

OK

Étape 12. Fournir le `Connection Profile Name` et la `Group-Policy`. Cliquez `Next`.

Pour les besoins de cette démonstration :


Nom du profil de connexion : RA-VPN

Méthode d'authentification : AAA uniquement

Serveur d'authentification : LDAP

Pool d'adresses IPv4 : VPN-Pool

Stratégie de groupe : Aucun accès

 Remarque : la méthode d'authentification, le serveur d'authentification et le pool d'adresses IPV4 ont été configurés au cours des étapes précédentes.

La stratégie de groupe No-Access a la valeur `Simultaneous Login Per User` paramètre défini sur 0 (pour empêcher les utilisateurs de se connecter s'ils reçoivent la stratégie de groupe No-Access par

défaut).

Add Group Policy

Name:*

Description:

General Secure Client **Advanced**

Traffic Filter

Session Settings

Access Hours:
 +

Simultaneous Login Per User:
 (Range 0-2147483647)

Étape 13. Cliquer [Add new AnyConnect Image](#) afin d'ajouter un [AnyConnect Client Image](#) au FTD.

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 |
|--|--------------------------------|----------------------------|------------------|
| No Secure Client Images configured Add new Secure Client Image | | | |

Étape 14. Fournir un [Name](#) pour l'image téléchargée et naviguez à partir du stockage local pour télécharger l'image. Cliquer [Save](#).

Add Secure Client File



Name:*

mac

File Name:*

anyconnect-macos-4.10.07061-webdep

Browse..

File Type:*

Secure Client Image

Description:

Cancel

Save

Étape 15. Cochez la case en regard de l'image afin de l'activer. Cliquer 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 |

Étape 16. Sélectionnez la Interface group/Security Zone et la Device Certificate. Cliquer Next.

Pour les besoins de cette démonstration :

Groupe d'interfaces/Zone de sécurité : zone de sortie

Certificat de périphérique : auto-signé


 Remarque : vous pouvez choisir d'activer l'option de stratégie Contourner le contrôle d'accès afin de contourner toute vérification de contrôle d'accès pour le trafic crypté (VPN) (Désactivé par défaut).



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.

Étape 17. Affichez le résumé de la configuration du VPN RA. Cliquez **Finish** pour l'enregistrer, comme illustré dans l'image.

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

Étape 18. Naviguez jusqu'à Deploy > Deployment. Sélectionnez le FTD vers lequel la configuration doit être déployée. Cliquer Deploy.

La configuration est poussée vers l'interface de ligne de commande FTD après un déploiement réussi :

```
<#root>
```

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

```
ldap attribute-map LDAP
```

```
map-name memberOf Group-Policy
map-value memberOf DC=tlalocan,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=tlalocan,DC=sec
ldap-group-base-dn DC=tlalocan,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
```

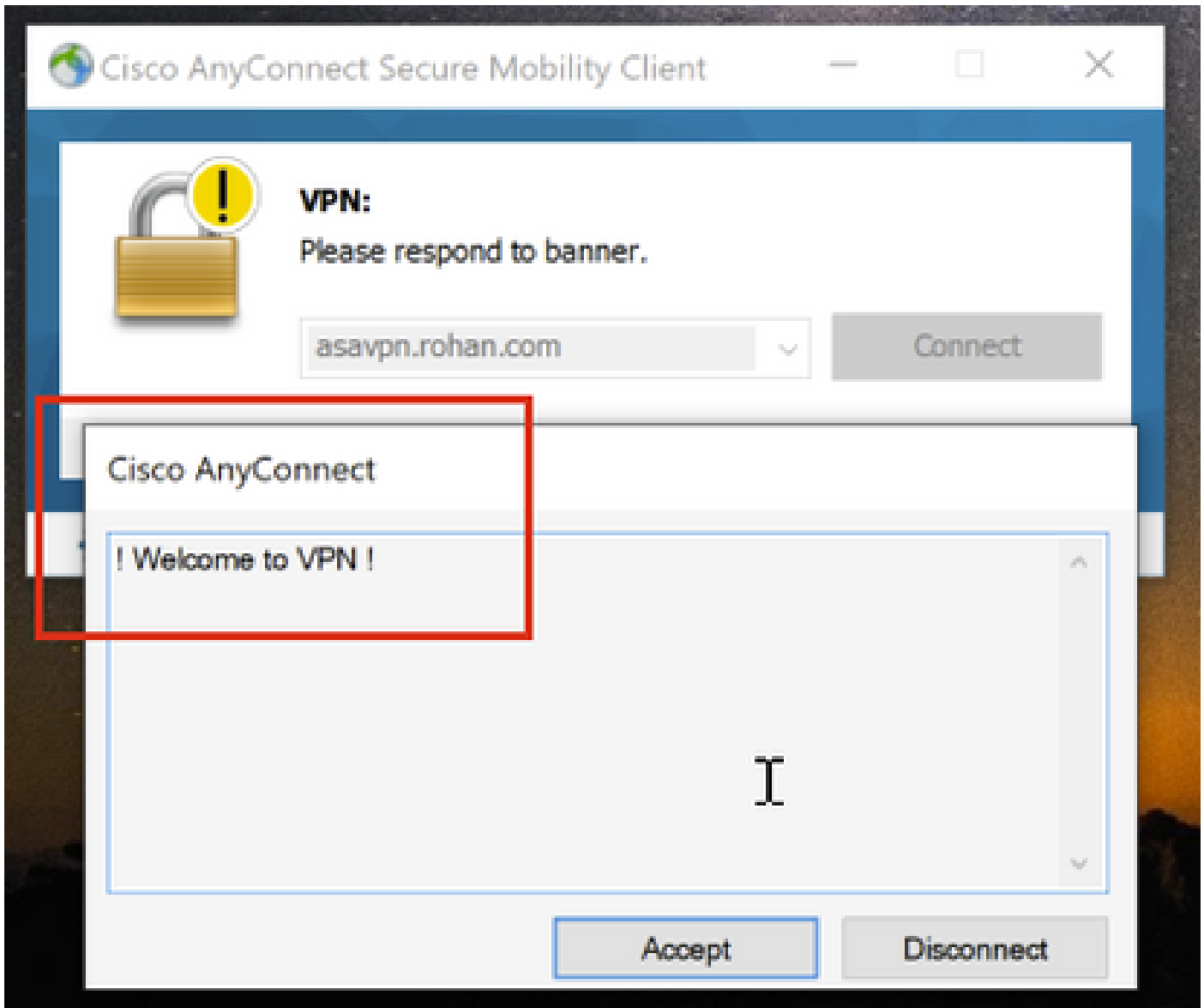
```
authentication-server-group LDAP
```

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

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

Vérifier

Sur le client AnyConnect, connectez-vous avec des informations d'identification de groupe d'utilisateurs VPN valides, et vous obtenez la stratégie de groupe correcte attribuée par la carte d'attributs LDAP :



Dans l'extrait de débogage LDAP (debug ldap 255), vous pouvez voir qu'il y a une correspondance sur le mappage d'attribut LDAP :

```
<#root>
```

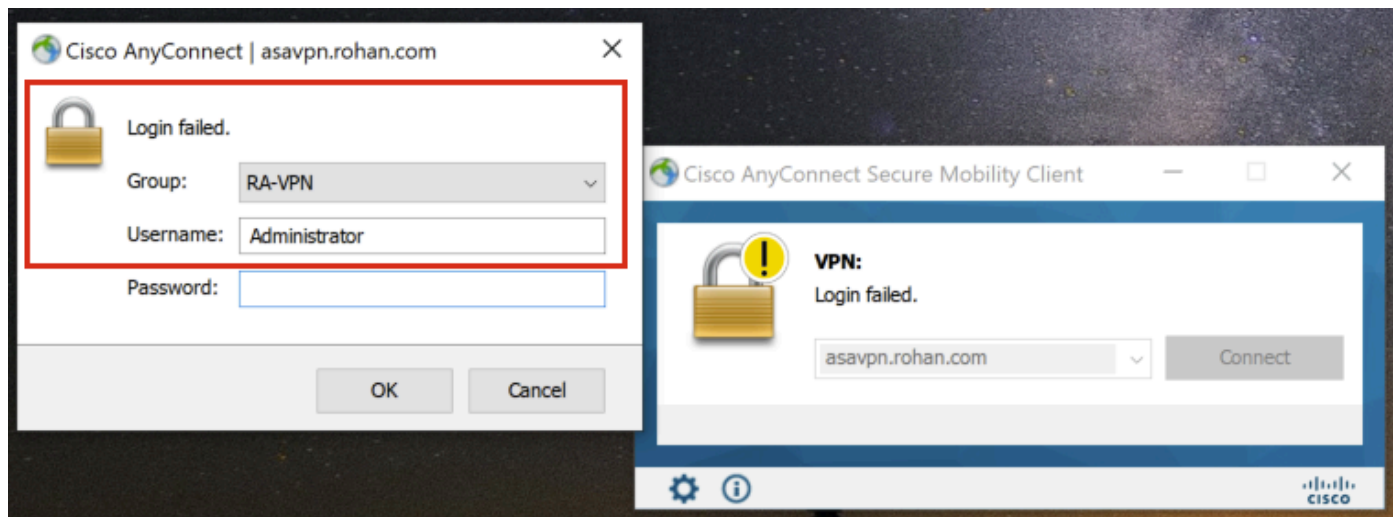
```
Authentication successful for test to 10.106.56.137
```

memberOf: value = DC=tlalocan,DC=sec

mapped to Group-Policy: value = RA-VPN

mapped to LDAP-Class: value = RA-VPN

Sur le client AnyConnect, connectez-vous avec un identifiant de groupe d'utilisateurs VPN non valide et vous obtenez la stratégie de groupe No-Access.



<#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
```

À partir de l'extrait de débogage LDAP (debug ldap 255), vous pouvez voir qu'il n'y a aucune correspondance sur la carte d'attributs LDAP :

<#root>

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

```
memberOf: value = CN=Group Policy Creator Owners,CN=Users,DC=tlalocan,DC=sec
```

```
mapped to Group-Policy: value = CN=Group Policy Creator Owners,CN=Users,DC=tlalocan,DC=sec
```

```
mapped to LDAP-Class: value = CN=Group Policy Creator Owners,CN=Users,DC=tlalocan,DC=sec
```

```
memberOf: value = CN=Domain Admins,CN=Users,DC=tlalocan,DC=sec
```

```
mapped to Group-Policy: value = CN=Domain Admins,CN=Users,DC=tlalocan,DC=sec
```

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

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.