

Configuración de VPN de RA con autenticación LDAP y autorización para FTD

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Requisitos de Licencia](#)

[Pasos de configuración en FMC](#)

[Configuración del servidor LDAP/RANGO](#)

[Configuración de VPN de RA](#)

[Verificación](#)

Introducción

Este documento describe cómo configurar VPN de acceso remoto con LDAP ASA en Firepower Threat Defense (FTD) administrado por Firepower Management Center.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos sobre el funcionamiento de VPN de acceso remoto (RA VPN).
- Comprender la navegación a través de Firepower Management Center (FMC).
- Configuración de los servicios del protocolo ligero de acceso a directorios (LDAP) en Microsoft Windows Server.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Cisco Firepower Management Center versión 7.3.0
- Cisco Firepower Threat Defense versión 7.3.0
- Microsoft Windows Server 2016, configurado como servidor LDAP

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo,

asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Este documento describe la configuración de VPN de acceso remoto (VPN de RA) con autenticación y autorización LDAP (protocolo ligero de acceso a directorios) en una defensa contra amenazas (FTD) de Firepower gestionada por un centro de administración de Firepower (FMC).

LDAP es un protocolo de aplicación abierto, independiente del proveedor y estándar del sector para acceder y mantener los servicios de información de directorios distribuidos.

Un mapa de atributos LDAP equipara los atributos que existen en el Active Directory (AD) o el servidor LDAP con los nombres de atributos de Cisco. A continuación, cuando el servidor AD o LDAP devuelve respuestas de autenticación al dispositivo FTD durante un establecimiento de conexión VPN de acceso remoto, el dispositivo FTD puede utilizar la información para ajustar cómo el cliente AnyConnect completa la conexión.

El FMC admite VPN de RA con autenticación LDAP desde la versión 6.2.1 y se aconsejó la autorización LDAP anterior a la versión 6.7.0 del FMC a través de FlexConfig para configurar el mapa de atributos LDAP y asociarlo con el servidor de rango. Esta función, con la versión 6.7.0, se ha integrado ahora con el asistente de configuración de VPN de RA en el FMC y ya no requiere el uso de FlexConfig.

 Nota: Esta función requiere que el FMC esté en la versión 6.7.0; mientras que el FTD administrado puede estar en cualquier versión superior a la 6.3.0.

Requisitos de Licencia

Requiere licencia AnyConnect Apex, AnyConnect Plus o AnyConnect VPN Only con la funcionalidad de control de exportación habilitada.

Para comprobar la licencia, vaya a **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

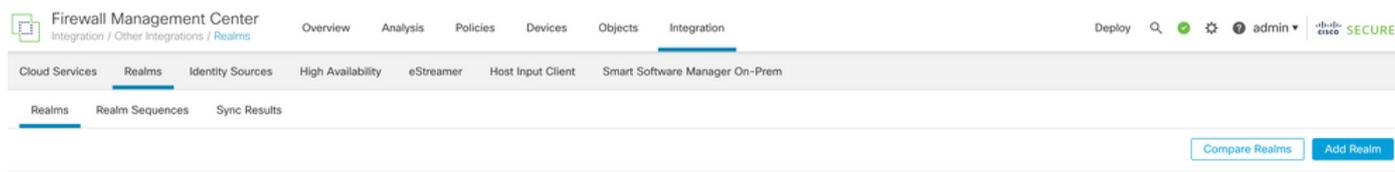
Apply

Pasos de configuración en FMC

Configuración del servidor LDAP/RANGO

 Nota: Los pasos enumerados sólo son necesarios si es para la configuración de un nuevo servidor REALM / LDAP. Si tiene un servidor preconfigurado, que se podría utilizar para la autenticación en RA VPN, navegue hasta [Configuración de RA VPN](#).

Paso 1. Desplácese hasta System > Other Integrations > Realms, como se muestra en esta imagen.



Paso 2. Como se muestra en la imagen, haga clic en Add a new realm.

A rectangular button with a blue border and a white background, containing the text "Compare Realms" in blue.A solid blue rectangular button containing the text "Add Realm" in white.

Paso 3. Proporcione los detalles del directorio y el servidor de AD. Haga clic en **OK**.

A efectos de esta demostración, se entenderá por:

Nombre: LDAP

Tipo: AD

Dominio principal de AD: test.com

Nombre de usuario del directorio: CN=Administrator,CN=Users,DC=test,DC=com

Contraseña del directorio: <Oculto>

DN base: DC=prueba,DC=com

Grupo 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

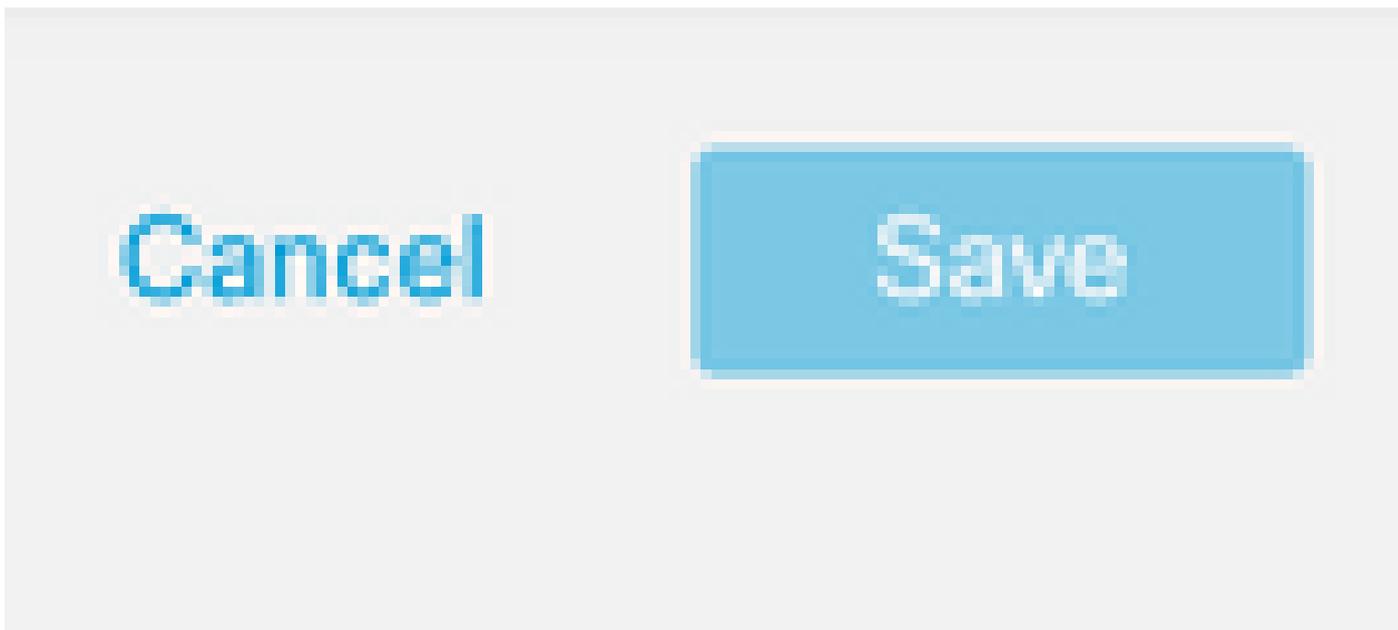
[Add another directory](#)

Cancel

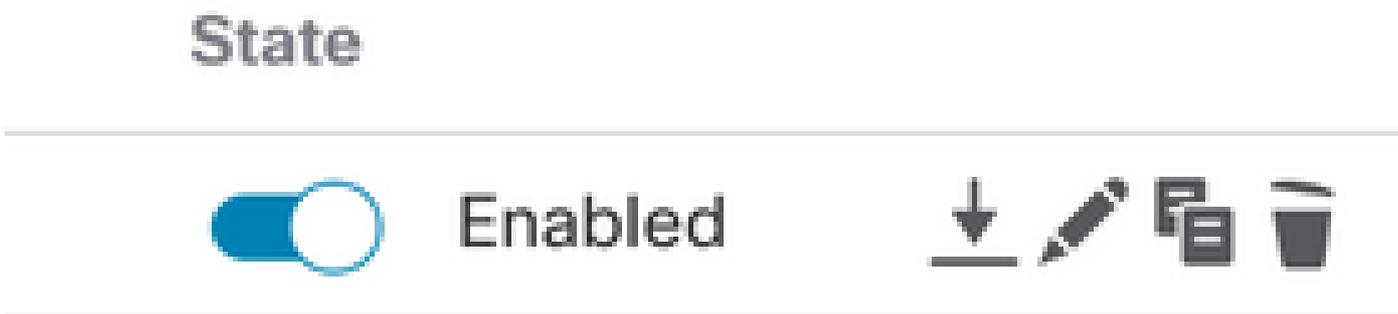
Configure Groups and Users

Paso 4. Haga clic en `Save` para guardar los cambios de rango/directorio, como se muestra en esta

imagen.



Paso 5. Active o desactive la *State* para cambiar el estado del servidor a Activado, como se muestra en esta imagen.



Configuración de VPN de RA

Estos pasos son necesarios para configurar la directiva de grupo, que se asigna a los usuarios de VPN autorizados. Si la directiva de grupo ya está definida, vaya al [paso 5](#).

Paso 1. Desplácese hasta *Objects > Object Management*.

Network

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

Object Management

Intrusion Rules

Paso 2: en el panel izquierdo, navegue hasta VPN > Group Policy.

▼ VPN

Certificate Map

Custom Attribute

Group Policy

IKEv1 IPsec Proposal

IKEv1 Policy

IKEv2 IPsec Proposal

IKEv2 Policy

Secure Client File

Paso 3: Haga clic en Add Group Policy.

Add Group Policy

 Filter

Paso 4: Proporcione los valores de Directiva de grupo.

A efectos de esta demostración, se entenderá por:

Nombre: RA-VPN

Banner: ! Bienvenido a VPN.

Inicio de sesión simultáneo por usuario: 3 (predeterminado)

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)

Paso 5. Desplácese hasta [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

Paso 6. Haga clic en [Add a new configuration](#).

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

Paso 7. Proporcionar una **Name** para la política VPN de RA. Elegir **VPN Protocols** y elija **Targeted Devices**. Haga clic en **Next**.

A efectos de esta demostración, se entenderá por:

Nombre: RA-VPN

Protocolos VPN: SSL

Dispositivos objetivo: 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"/> | |

Paso 8. Para el **Authentication Method**, elija **AAA Only**. Elija el servidor **REALM / LDAP** para el **Authentication Server**. Haga clic en **Configure LDAP Attribute Map** (para configurar la autorización 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](#)

Paso 9. Proporcione la LDAP Attribute Name y el Cisco Attribute Name. Haga clic en Add Value Map.

A efectos de esta demostración, se entenderá por:

Nombre de atributo LDAP: memberOf

Nombre de atributo de Cisco: política de grupo

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

Paso 10. Proporcione la LDAP Attribute Value y el Cisco Attribute Value. Haga clic en OK.

A efectos de esta demostración, se entenderá por:

Valor del atributo LDAP: DC=tlalocan,DC=sec

Valor del atributo de 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](#)



 Nota: Puede añadir más Value Maps según los requisitos.

Paso 11. Agregue el `Address Pool` para la asignación de dirección local. Haga clic en `OK`.

Address Pools ?

Available IPv4 Pools +

VPN-Pool

Add

Selected IPv4 Pools

VPN-Pool 🗑

Cancel

OK

Paso 12. Proporcione la `Connection Profile Name` y el `Group-Policy`. Haga clic en `Next`.

A efectos de esta demostración, se entenderá por:

Nombre del perfil de conexión: RA-VPN

Método de autenticación: sólo AAA

Servidor de autenticación: LDAP

Pool de Direcciones IPv4: VPN-Pool

Directiva de grupo: Sin acceso

 Nota: El Método de Autenticación, el Servidor de Autenticación y el Pool de Direcciones IPV4 fueron configurados en pasos anteriores.

La política de grupo Sin acceso tiene el `Simultaneous Login Per User` parámetro establecido en 0 (para no permitir que los usuarios puedan iniciar sesión si reciben la directiva de grupo predeterminada Sin

acceso).

Add Group Policy

Name:*

Description:

General Secure Client **Advanced**

Traffic Filter

Session Settings

Access Hours:

 +

Simultaneous Login Per User:

 (Range 0-2147483647)

Paso 13. Haga clic en [Add new AnyConnect Image](#) para agregar un [AnyConnect Client Image](#) al 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](#).

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 | | | |

Paso 14. Proporcionar una [Name](#) para la imagen cargada y navegue desde el almacenamiento local para cargar la imagen. Haga clic en [Save](#).

Add Secure Client File



Name:*

mac

File Name:*

anyconnect-macos-4.10.07061-webdep

Browse..

File Type:*

Secure Client Image

Description:

Cancel

Save

Paso 15. Haga clic en la casilla de verificación junto a la imagen para habilitarla para su uso. Haga clic en 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 |

Paso 16. Elija el Interface group/Security Zone y el Device Certificate. Haga clic en Next.

A efectos de esta demostración, se entenderá por:

Grupo de interfaz/Zona de seguridad: Zona externa

Certificado de dispositivo: firmado automáticamente

 Nota: Puede optar por activar la opción de directiva Omitir control de acceso para omitir cualquier comprobación de control de acceso para el tráfico cifrado (VPN) (deshabilitada de forma predeterminada).



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.

Paso 17. Vea el resumen de la configuración VPN de RA. Haga clic en **Finish** para guardar, como se muestra en la imagen.

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

Paso 18. Desplácese hasta Deploy > Deployment. Elija el FTD en el que debe implementarse la configuración. Haga clic en Deploy.

La configuración se envía a la CLI de FTD después de una implementación correcta:

```
<#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
```

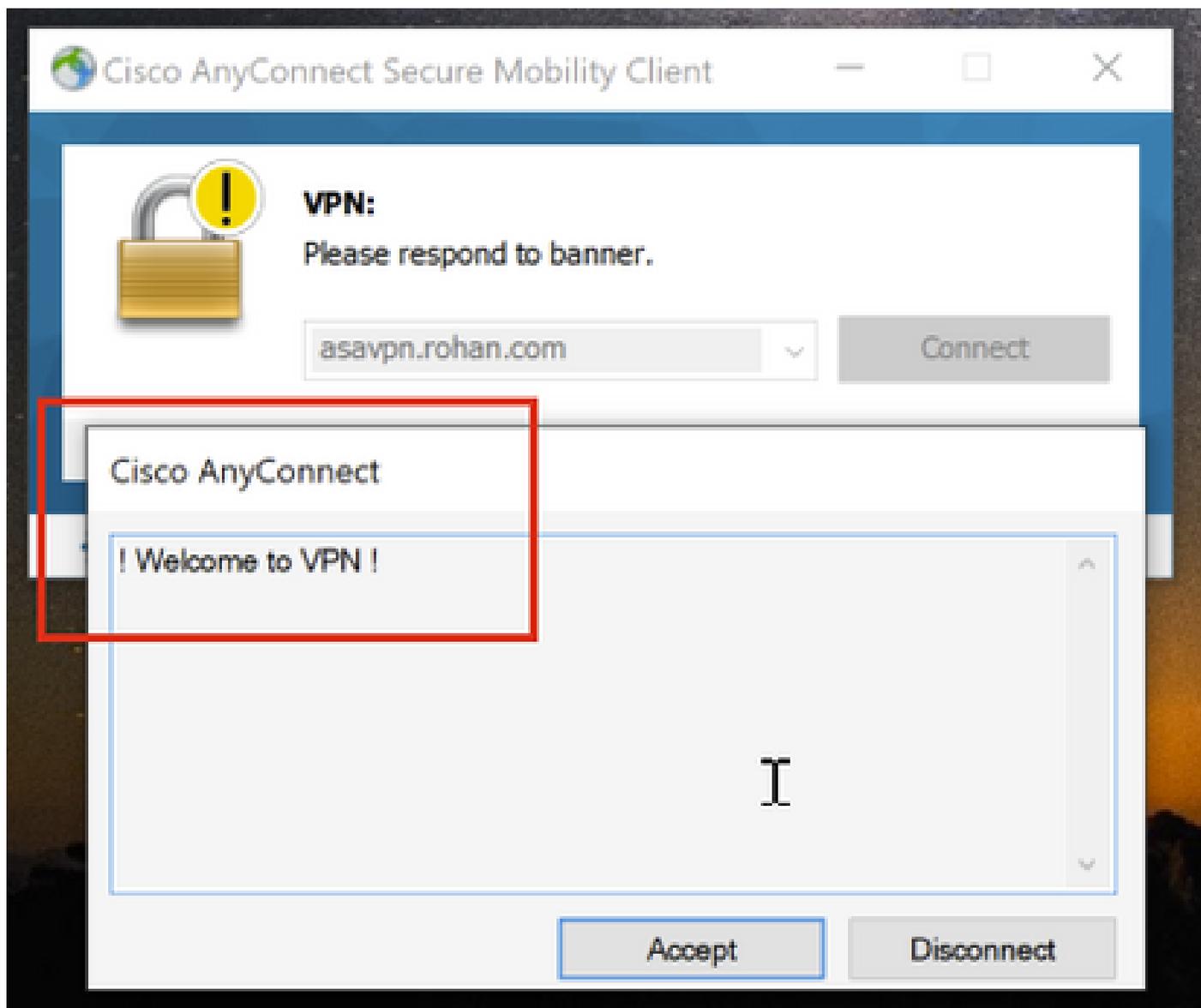
```
authentication-server-group LDAP
```

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

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

Verificación

En el cliente AnyConnect, inicie sesión con las credenciales del grupo de usuarios VPN válidos y obtendrá la política de grupo correcta asignada por el mapa de atributos LDAP:



Desde el fragmento de depuración LDAP (debug ldap 255) puede ver que hay una coincidencia en el mapa de atributos LDAP:

```
<#root>
```

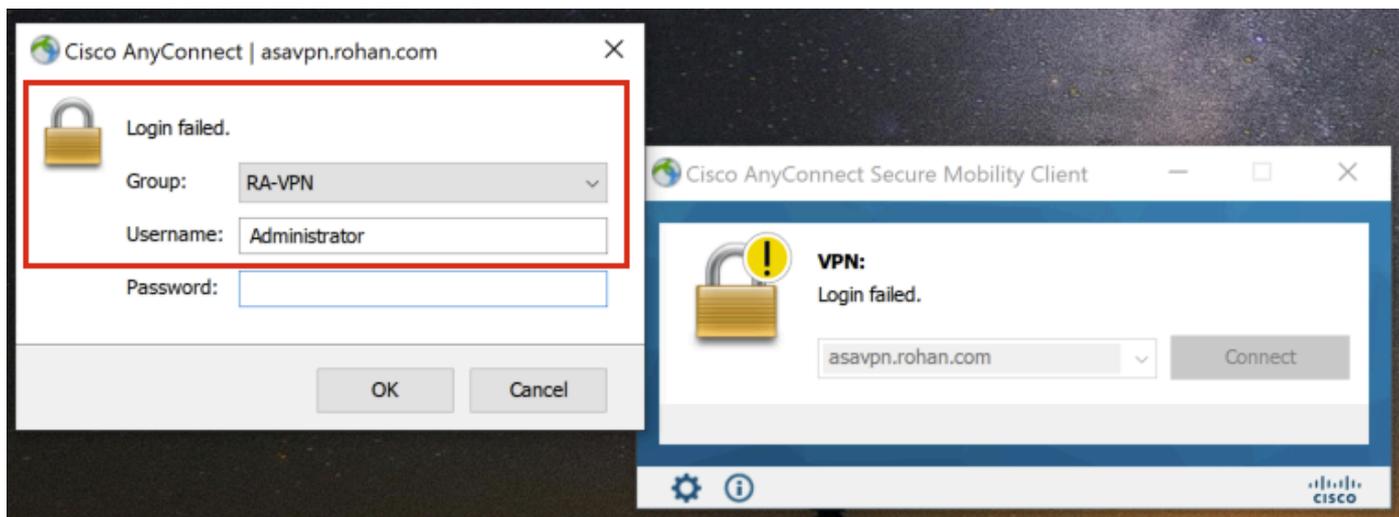
```
Authentication successful for test to 10.106.56.137
```

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

mapped to Group-Policy: value = RA-VPN

mapped to LDAP-Class: value = RA-VPN

En el cliente AnyConnect, inicie sesión con una credencial de grupo de usuarios VPN no válida y obtendrá la directiva de grupo Sin acceso.



<#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
```

Desde el fragmento de depuración LDAP (debug ldap 255), puede ver que no hay coincidencia en el mapa de atributos 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

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).