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

Contenido

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.

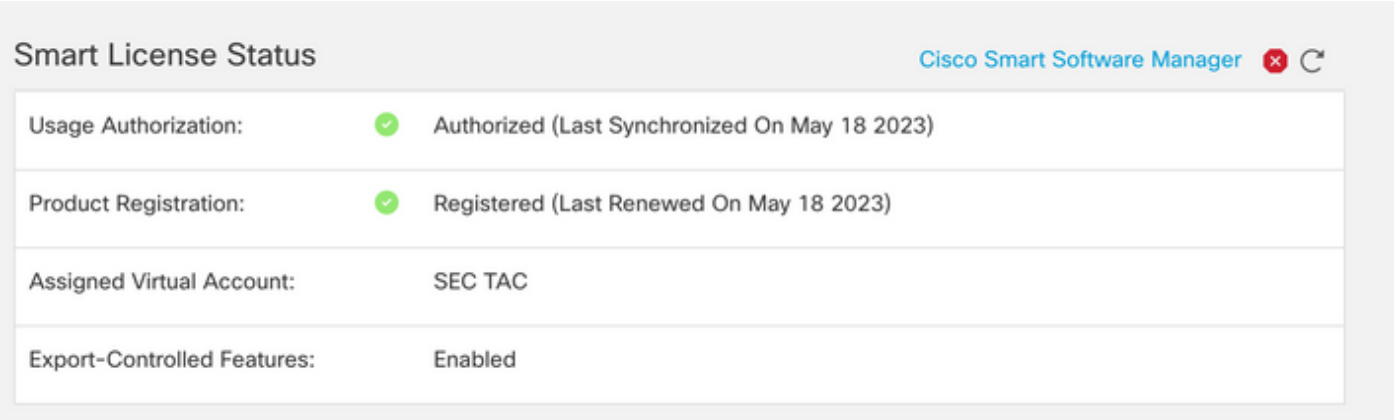
El FMC admite VPN de RA con autenticación LDAP desde la versión 6.2.1 y se aconsejó la autorización LDAP anterior a la versión 6.7.0 del FMC a través de FlexConfig para configurar el mapa de atributos LDAP y asociarlo con el servidor de rango. Esta función, con la versión 6.7.0, se ha integrado ahora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

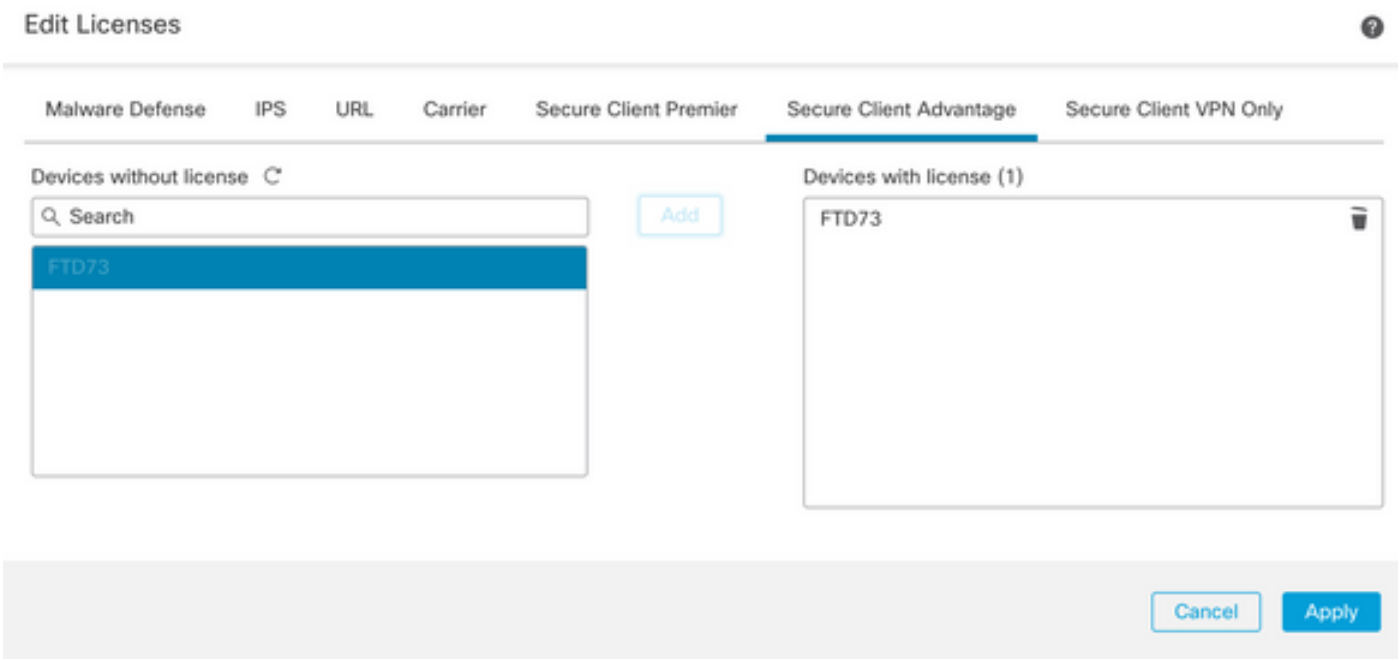
Nota: Esta función requiere que el FMC esté en la versión 6.7.0; mientras que el FTD administrado puede estar en cualquier versión superior a la 6.3.0.

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.**



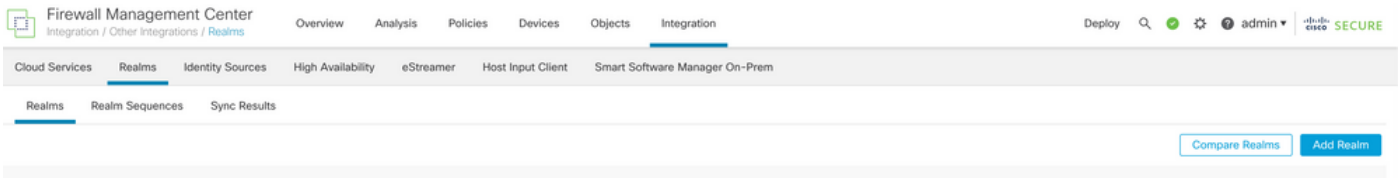


Pasos de configuración en FMC

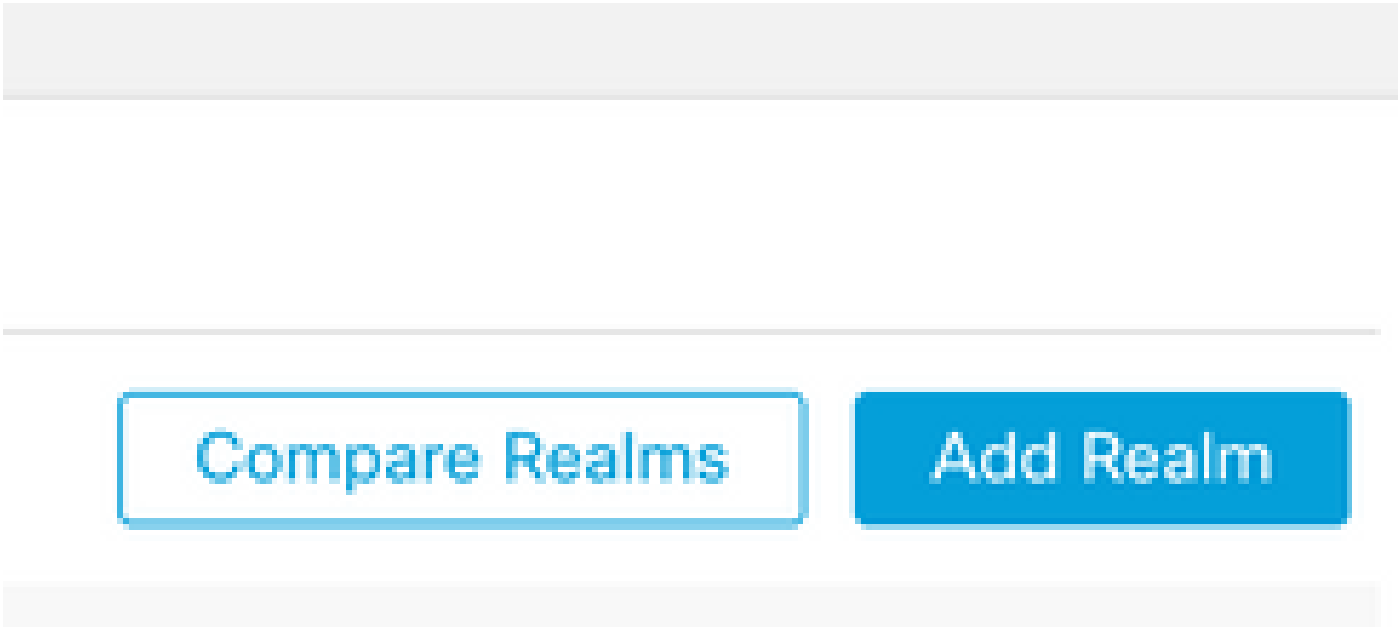
Configuración del servidor LDAP/RANGO

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**.



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

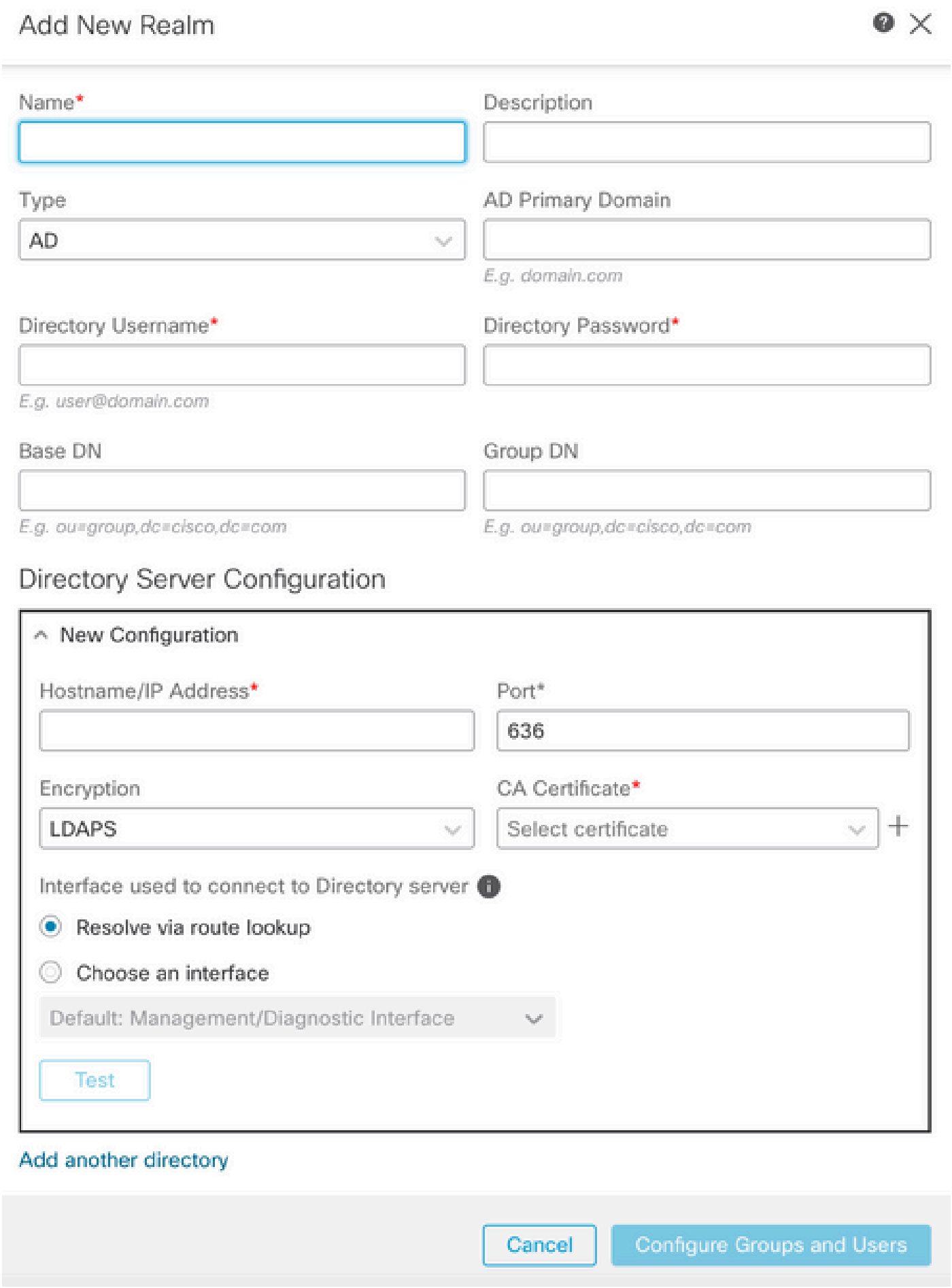
Dominio principal de AD: test.com

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

Contraseña del directorio: <Oculto>

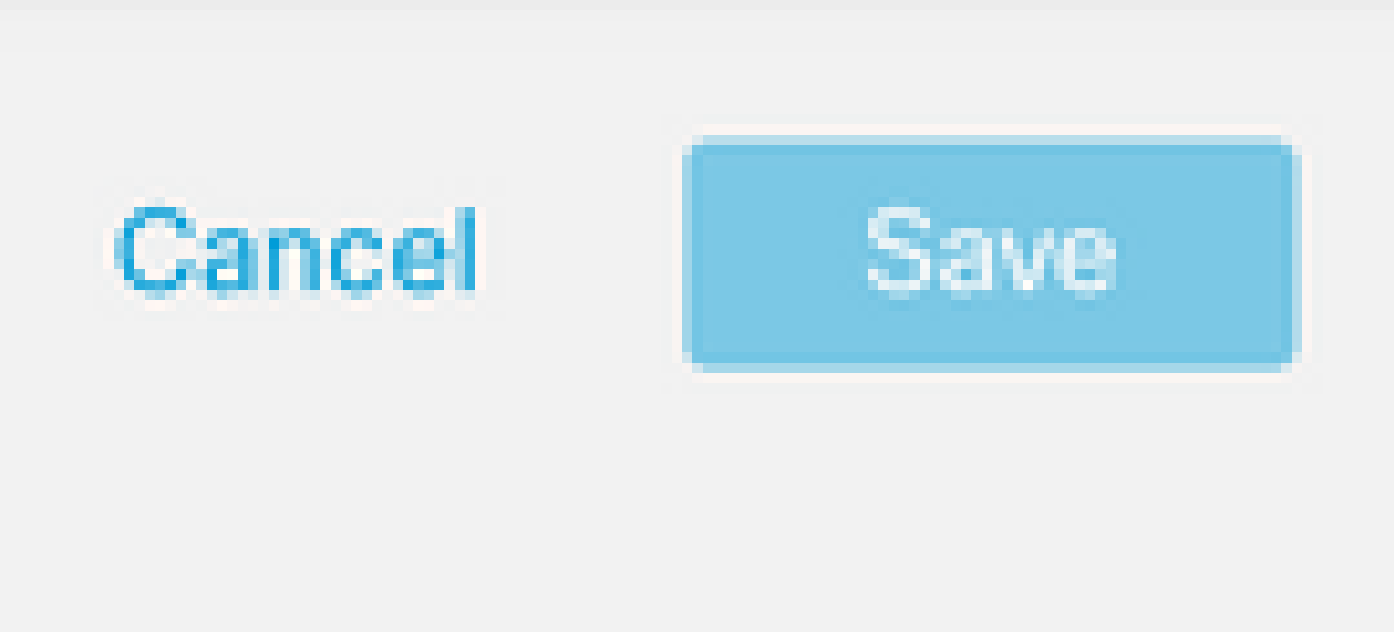
DN base: DC=prueba,DC=com

Grupo DN: DC=test,DC=com

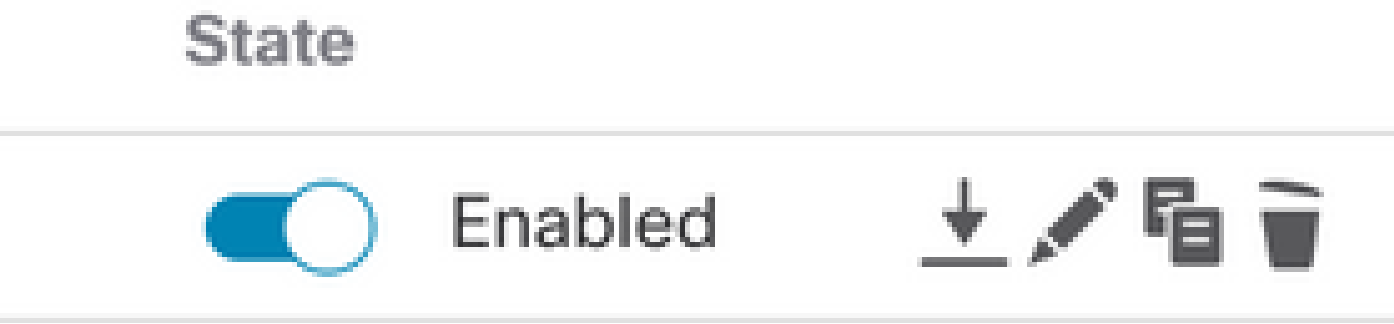


Paso 4. Haga clic en Save para guardar los cambios de rango/directorio, como se muestra en esta

imagen.



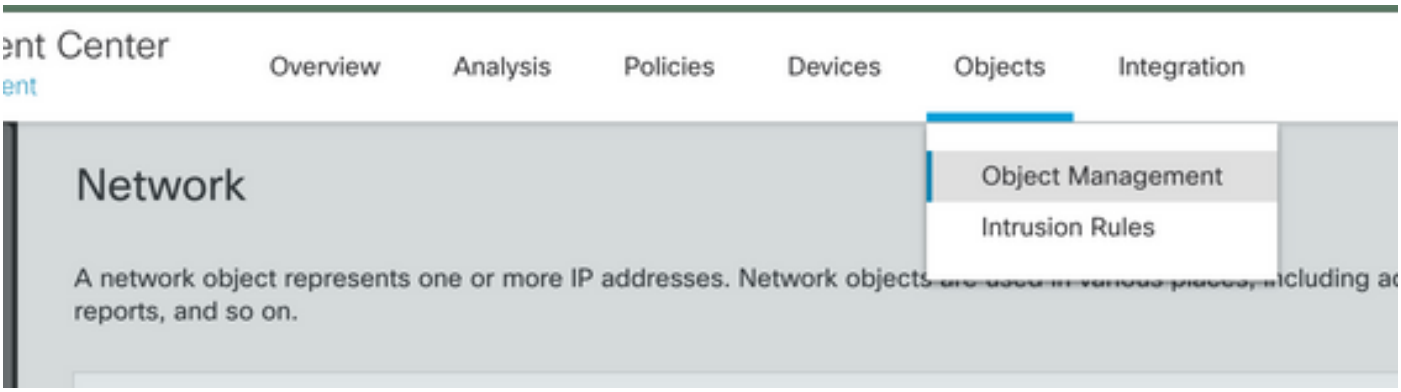
Paso 5. Active o desactive la State para cambiar el estado del servidor a Activado, como se muestra en esta imagen.



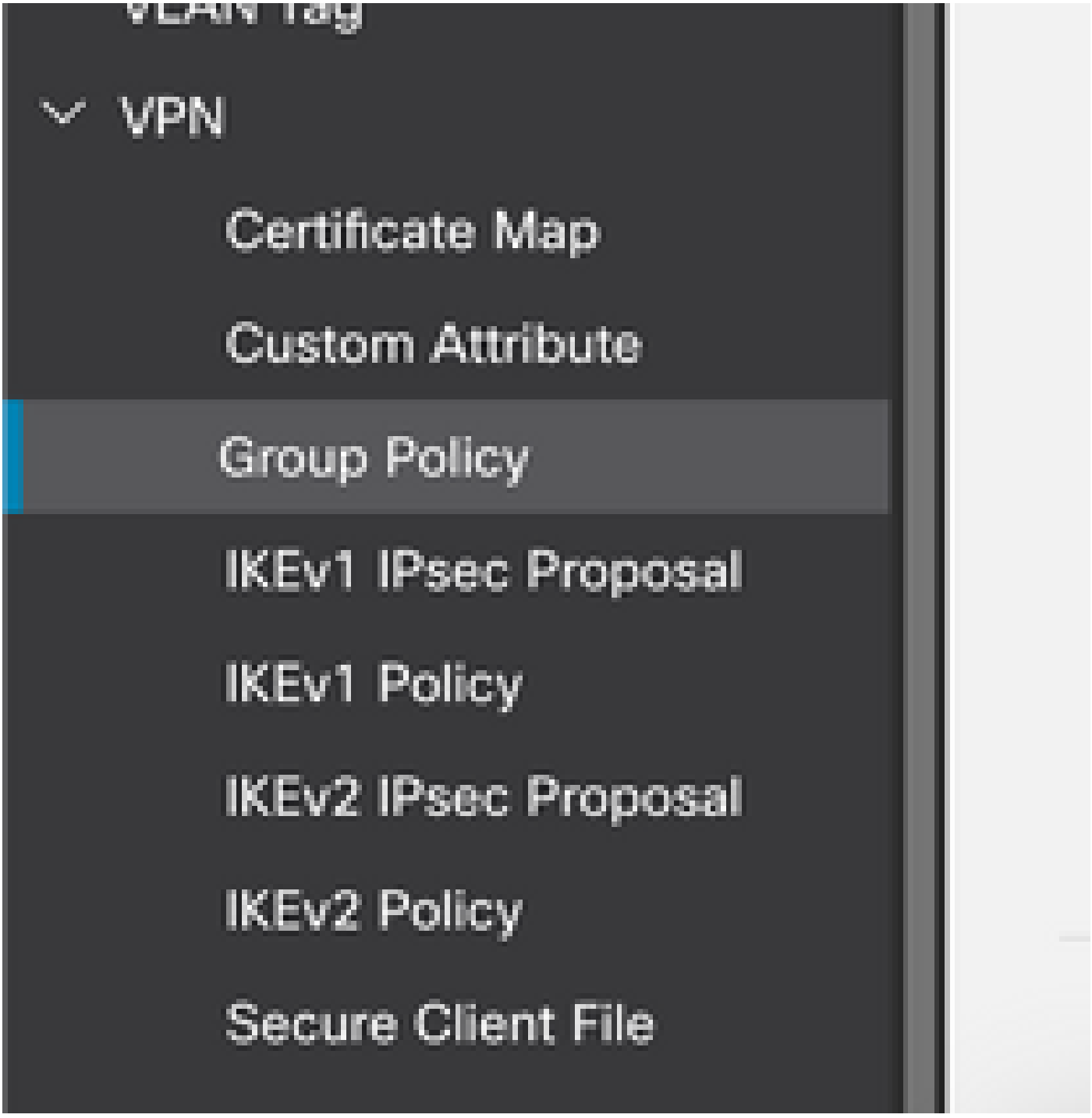
Configuración de VPN de RA

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.

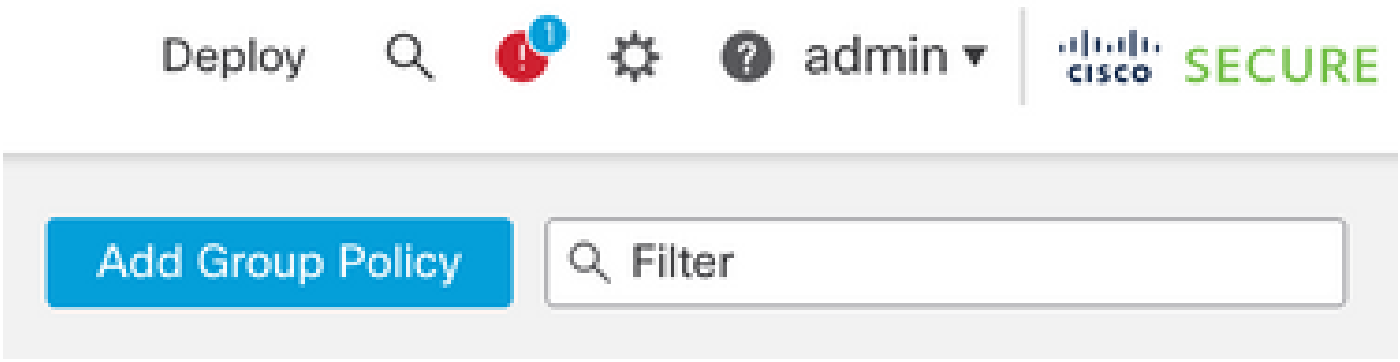
Paso 1. Desplácese hasta Objects > Object Management.



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



Paso 3: Haga clic en **Add Group Policy**.



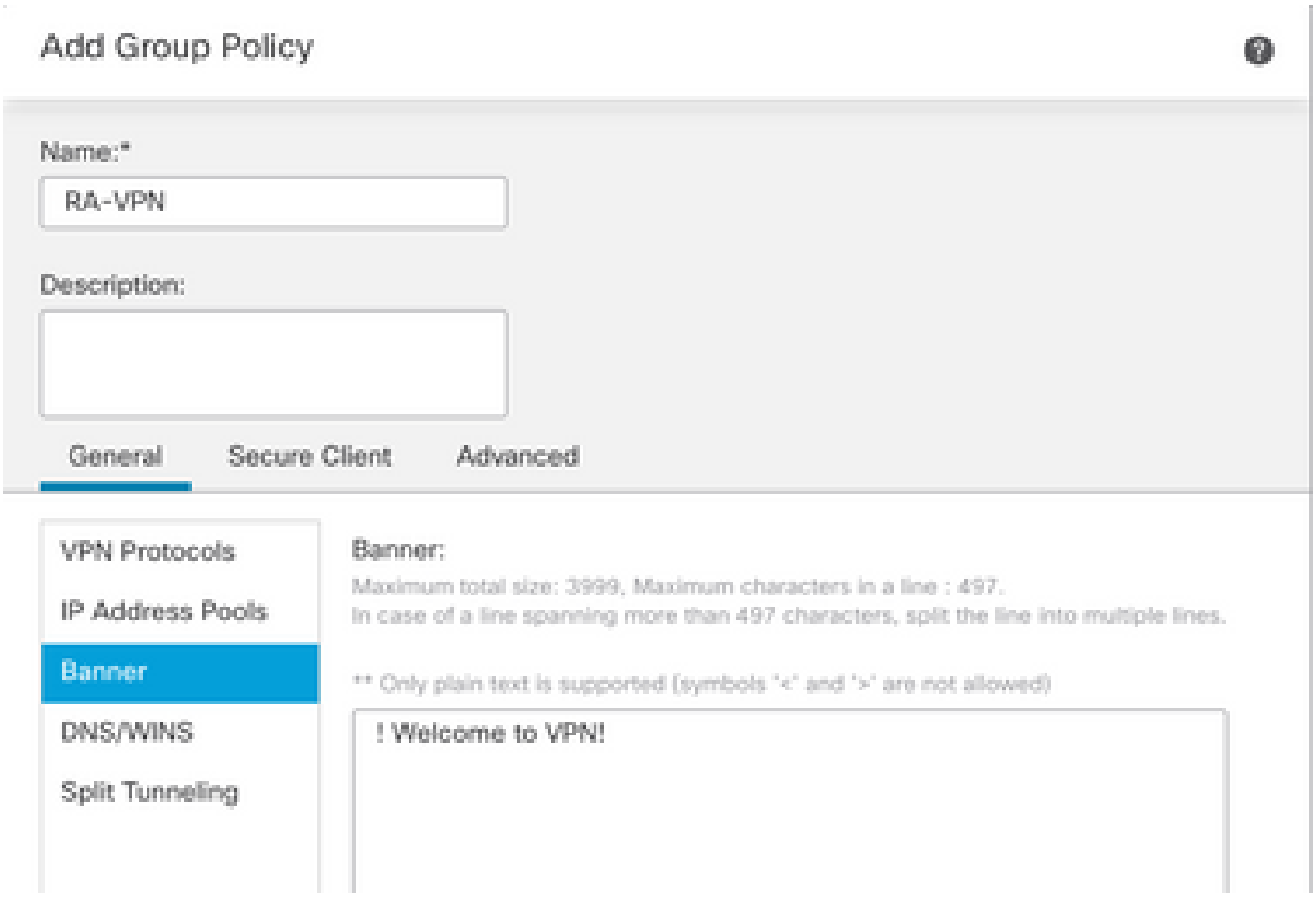
Paso 4: Proporcione los valores de Directiva de grupo.

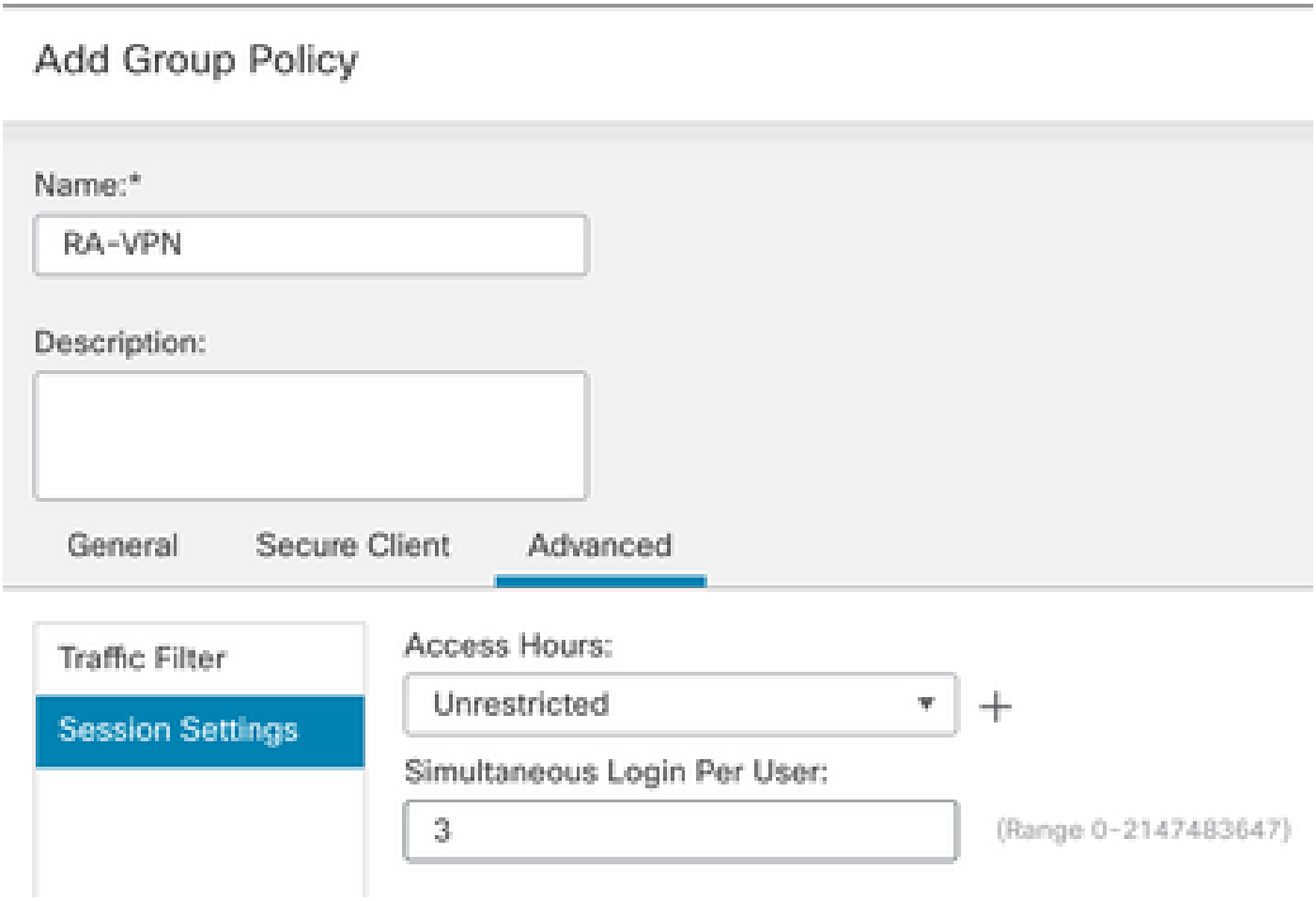
A efectos de esta demostración, se entenderá por:

Nombre: RA-VPN

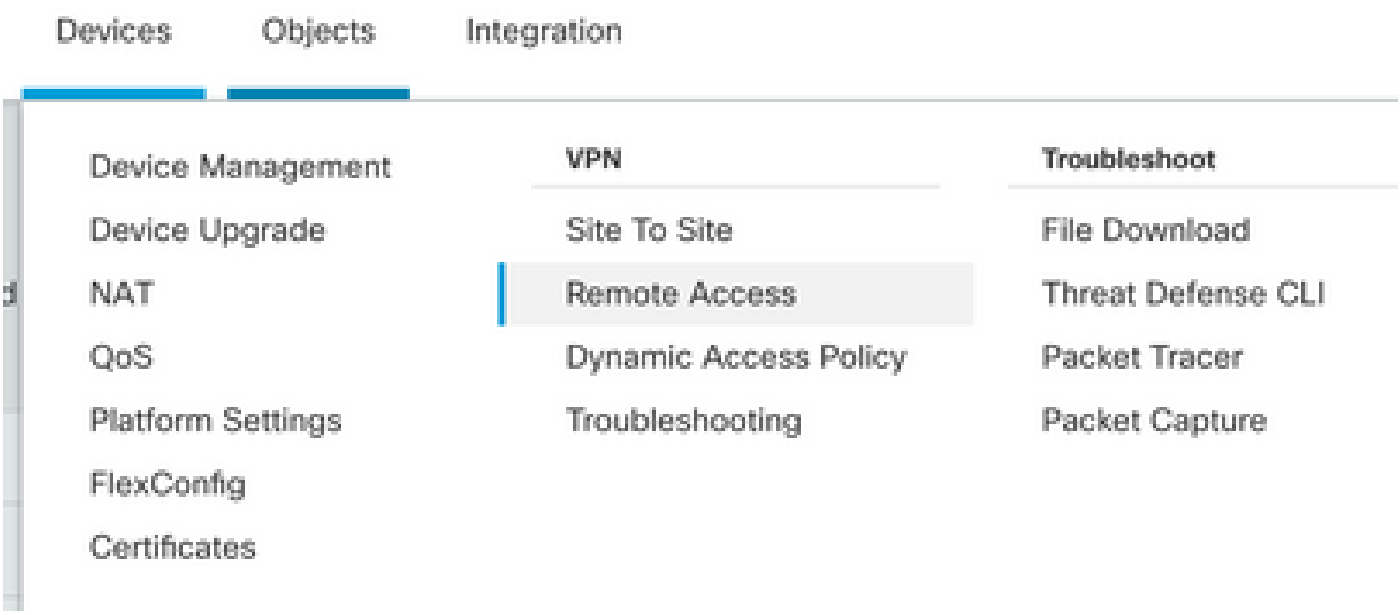
Banner: ! Bienvenido a VPN.

Inicio de sesión simultáneo por usuario: 3 (predeterminado)

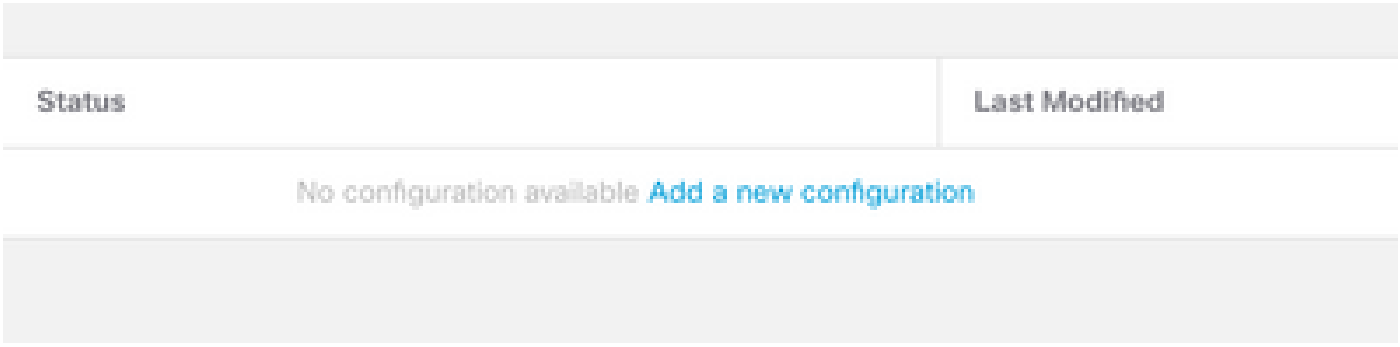




Paso 5. Desplácese hasta Devices > VPN > Remote Access.



Paso 6. Haga clic en **Add a new configuration**.



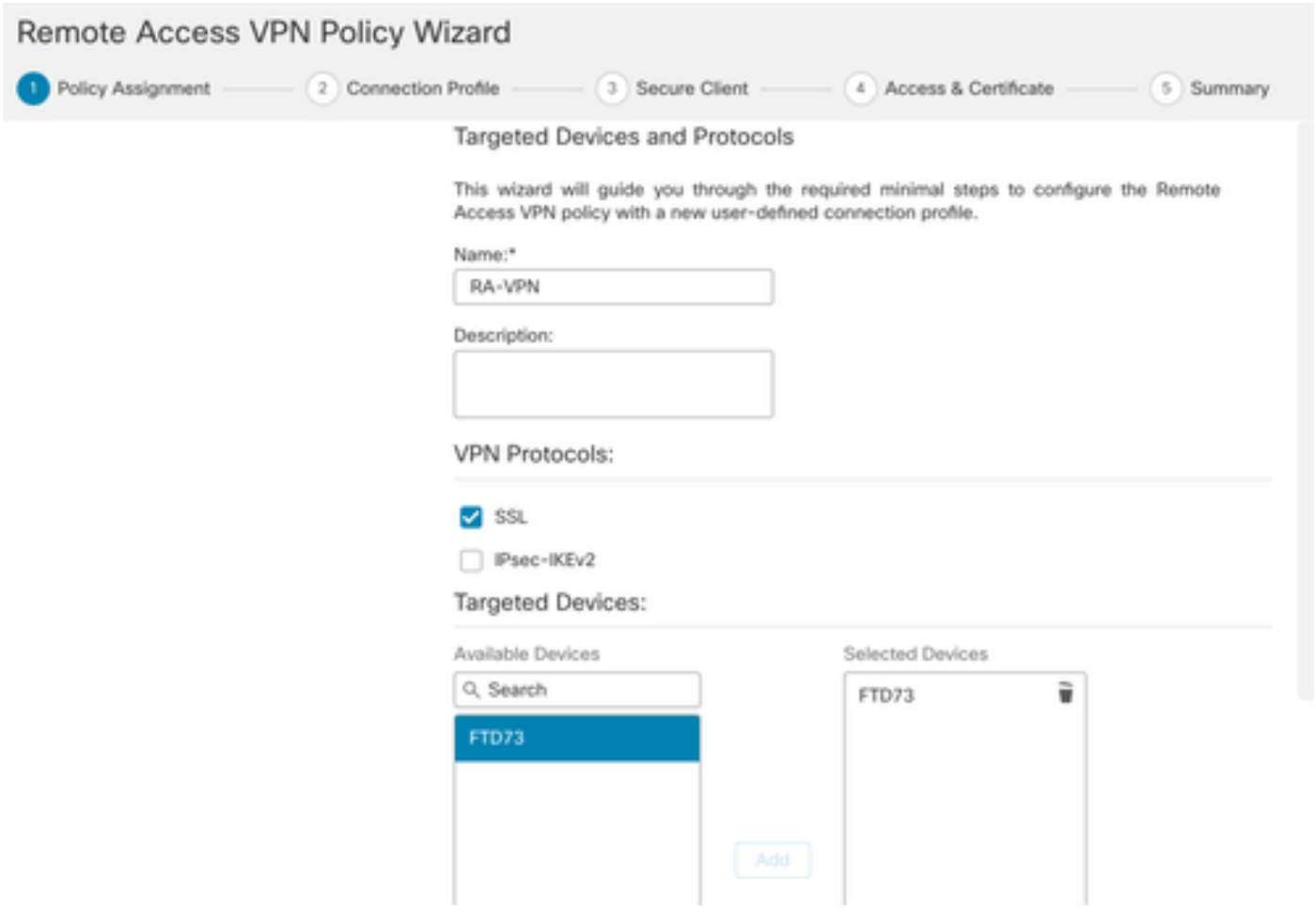
Paso 7. Proporcionar una Name para la política VPN de RA. Elegir **VPN Protocols** y elija **Targeted Devices**. Haga clic en **Next**.

A efectos de esta demostración, se entenderá por:

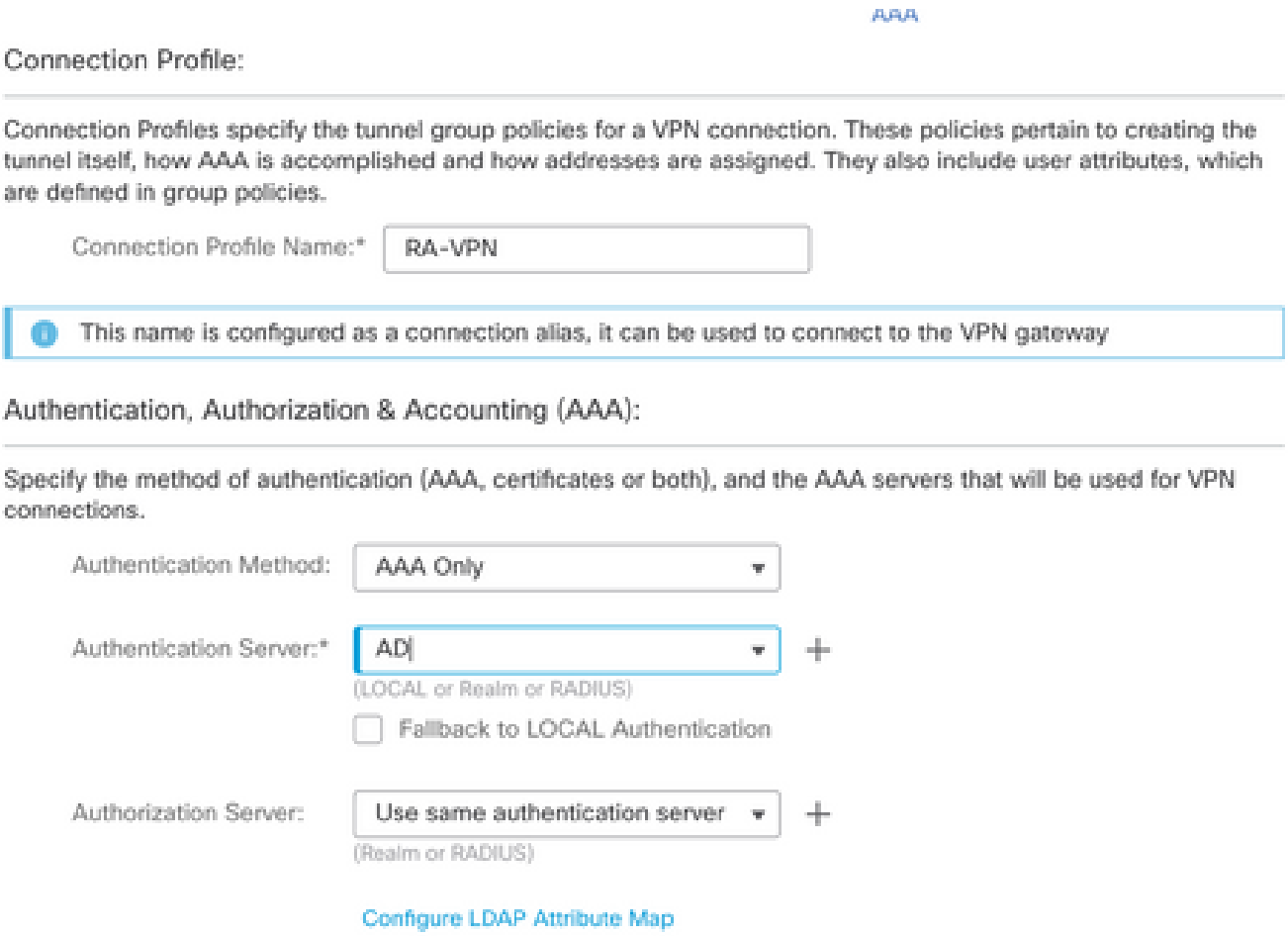
Nombre: RA-VPN

Protocolos VPN: SSL

Dispositivos objetivo: FTD



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).

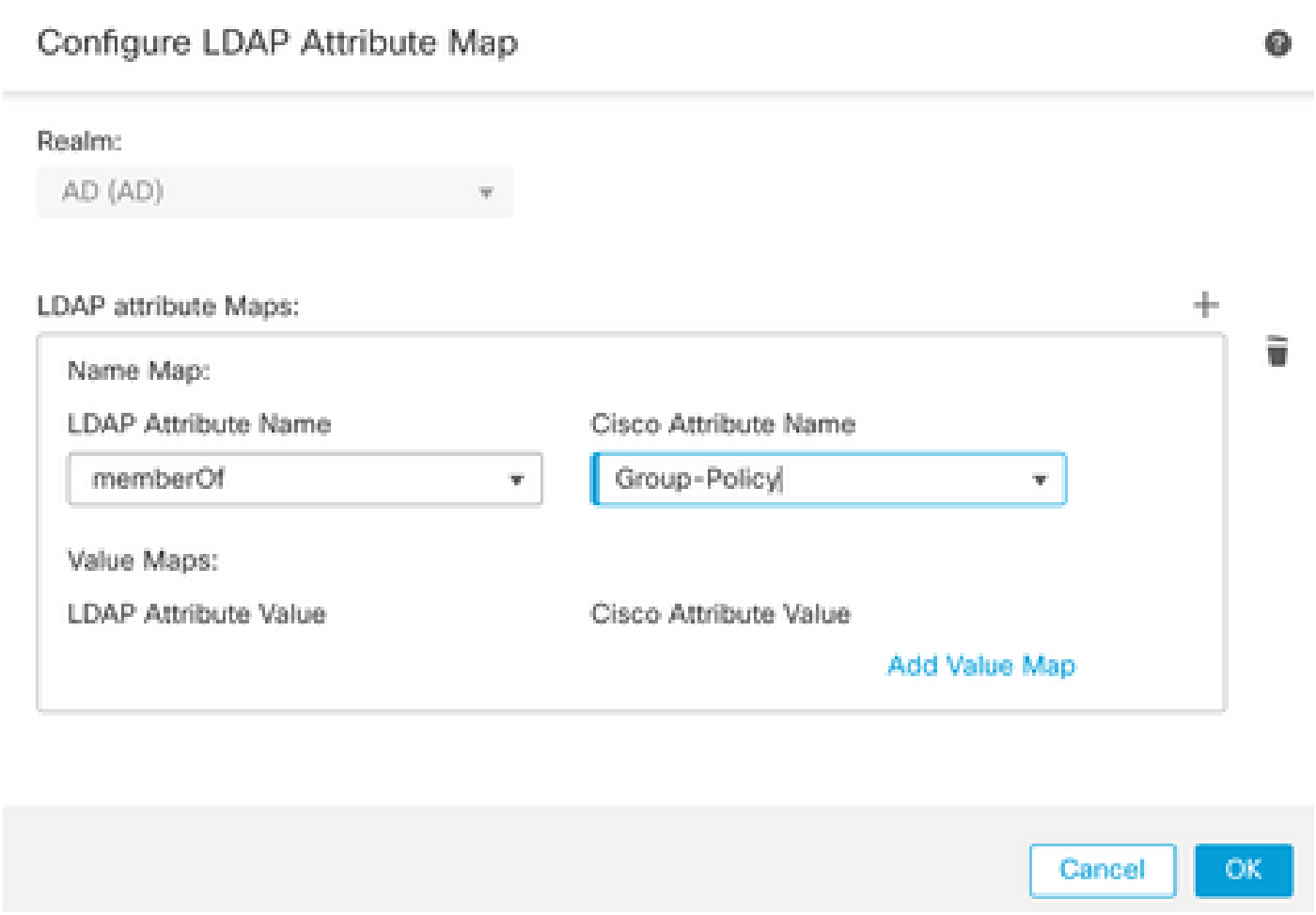


Paso 9. Proporcione la LDAP Attribute Name y el Cisco Attribute Name. Haga clic en **Add Value Map**.

A efectos de esta demostración, se entenderá por:

Nombre de atributo LDAP: memberOfI

Nombre de atributo de Cisco: política de grupo

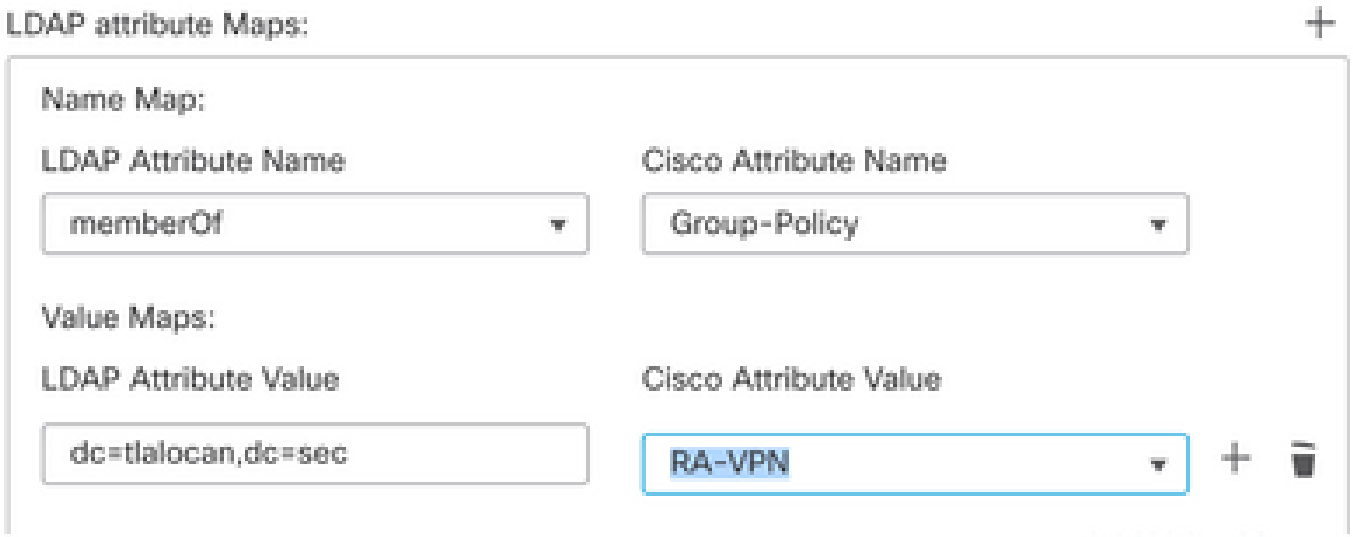


Paso 10. Proporcione la LDAP Attribute Value y el Cisco Attribute Value. Haga clic en OK.

A efectos de esta demostración, se entenderá por:

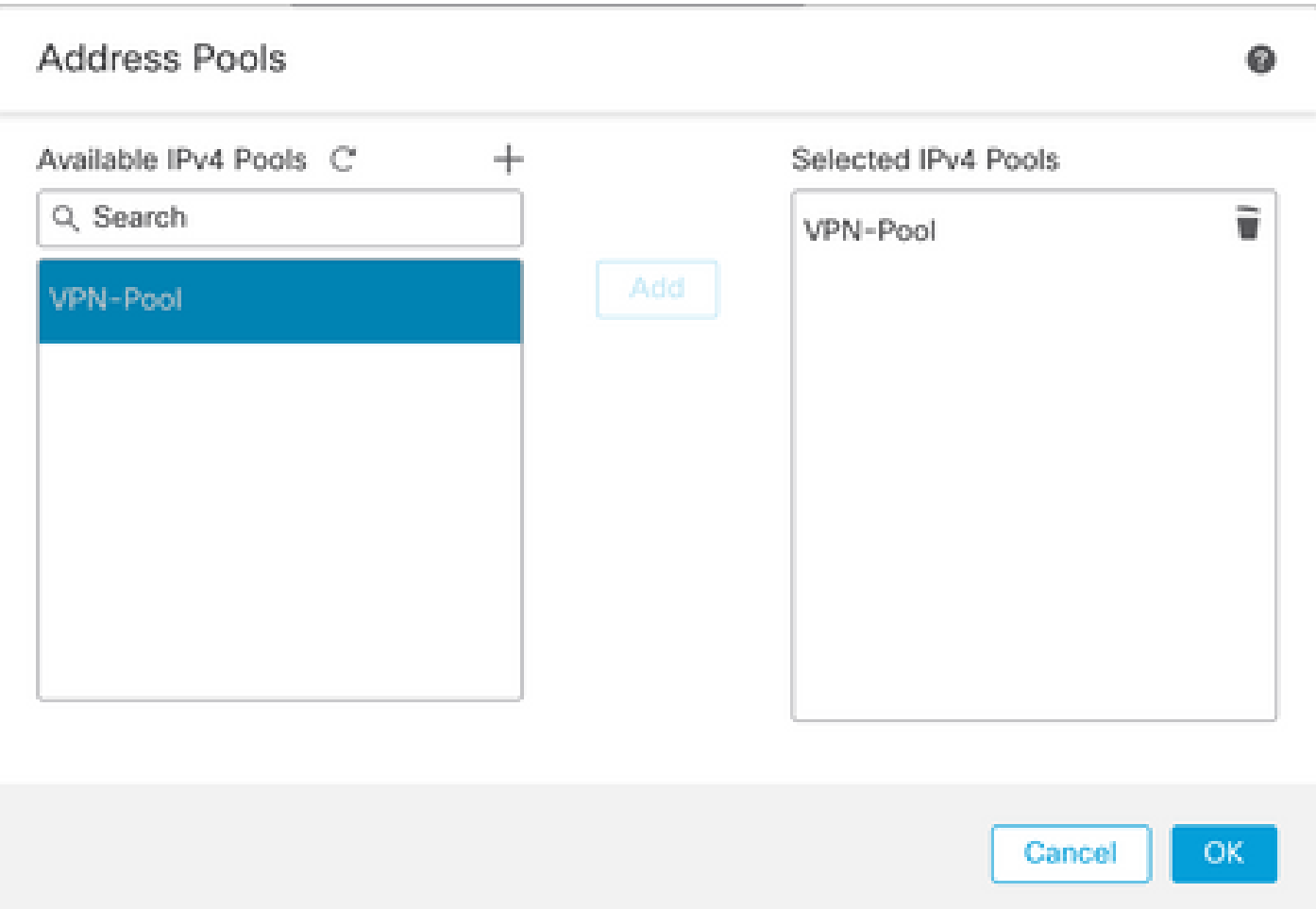
Valor del atributo LDAP: DC=tlalocan,DC=sec

Valor del atributo de Cisco: RA-VPN



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.



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

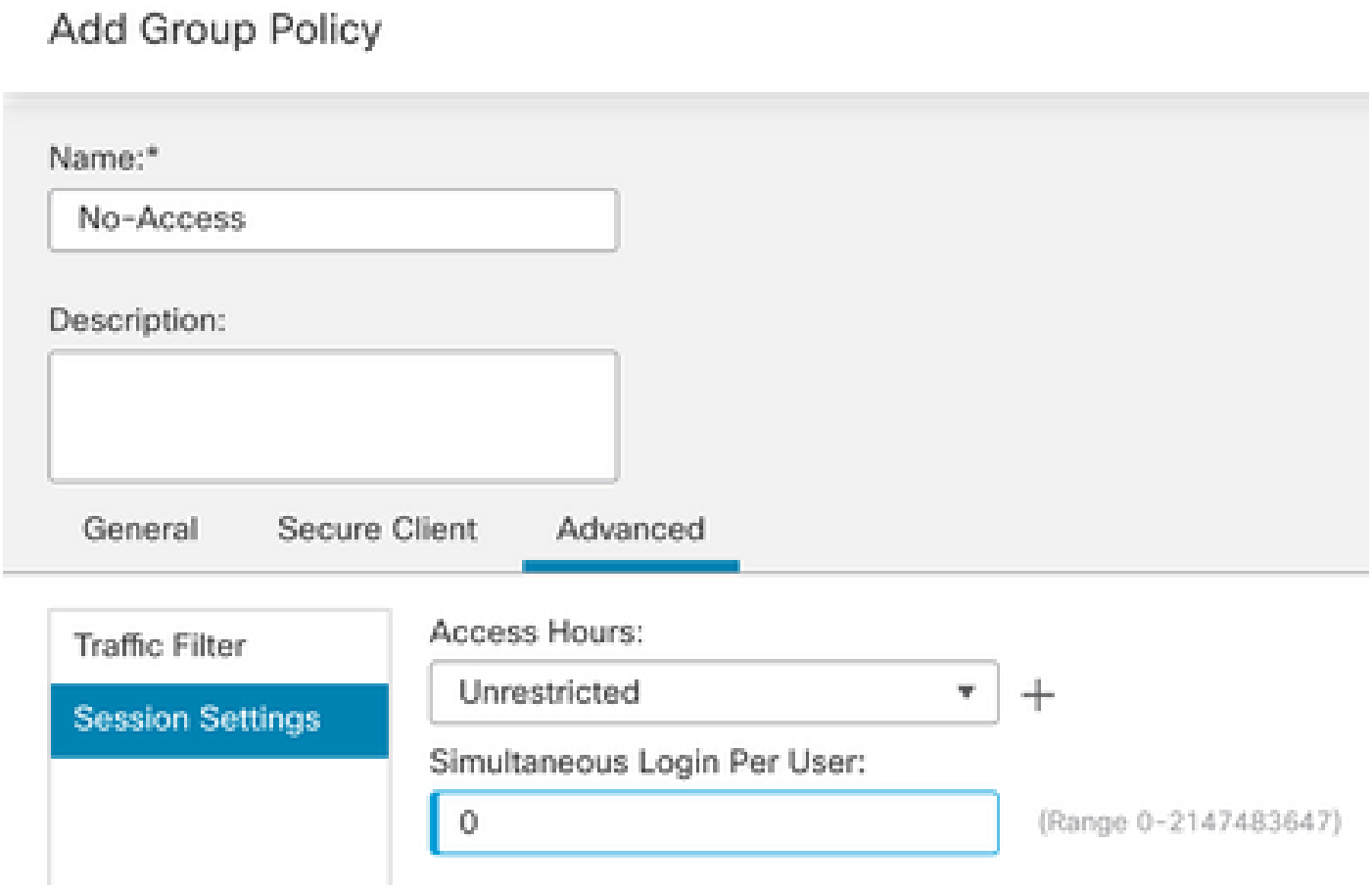
Pool de Direcciones IPv4: VPN-Pool

Directiva de grupo: Sin acceso

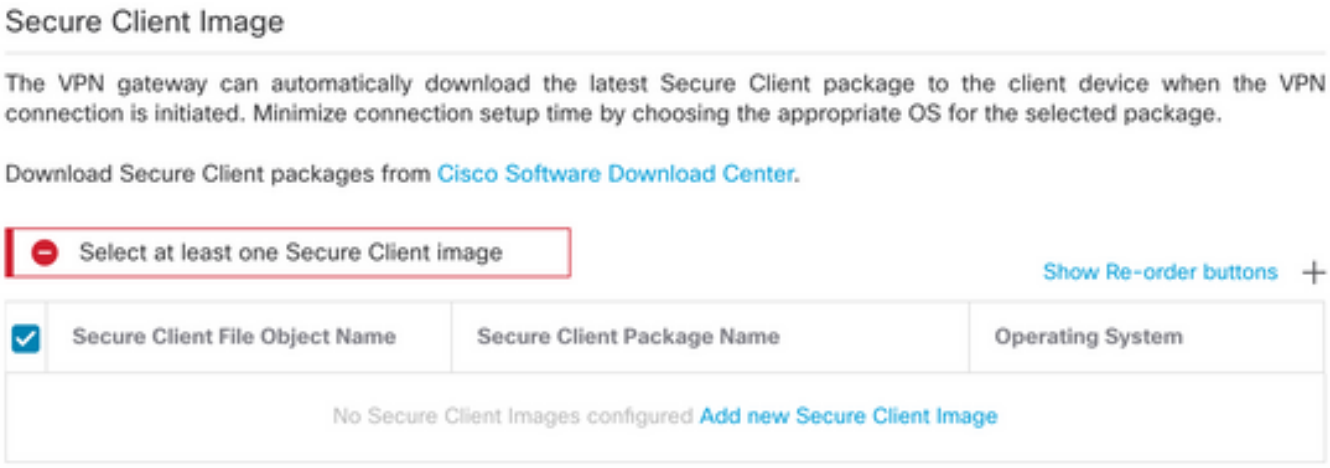
Nota: El Método de Autenticación, el Servidor de Autenticación y el Pool de Direcciones IPV4 fueron configurados en pasos anteriores.

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

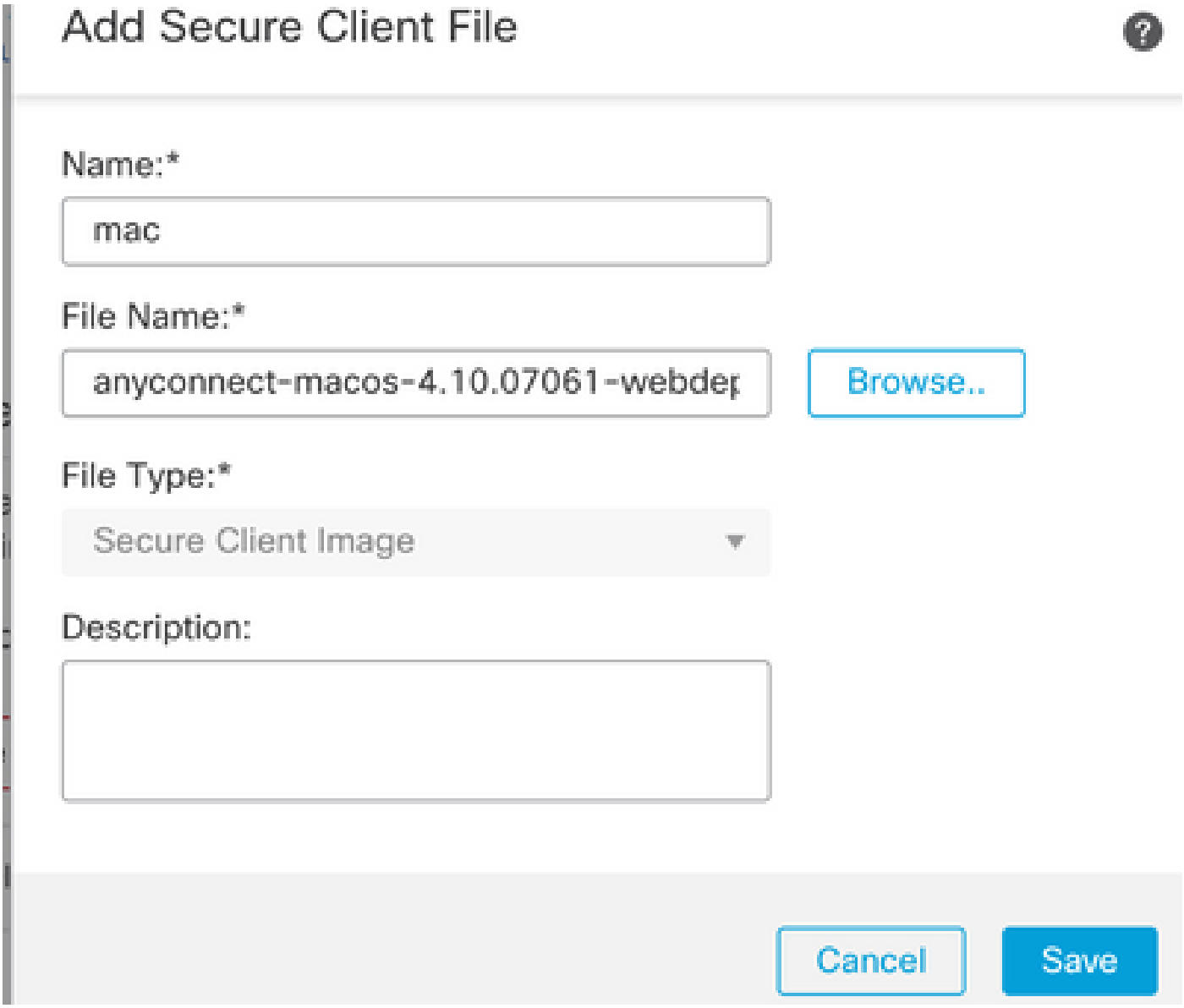
acceso).



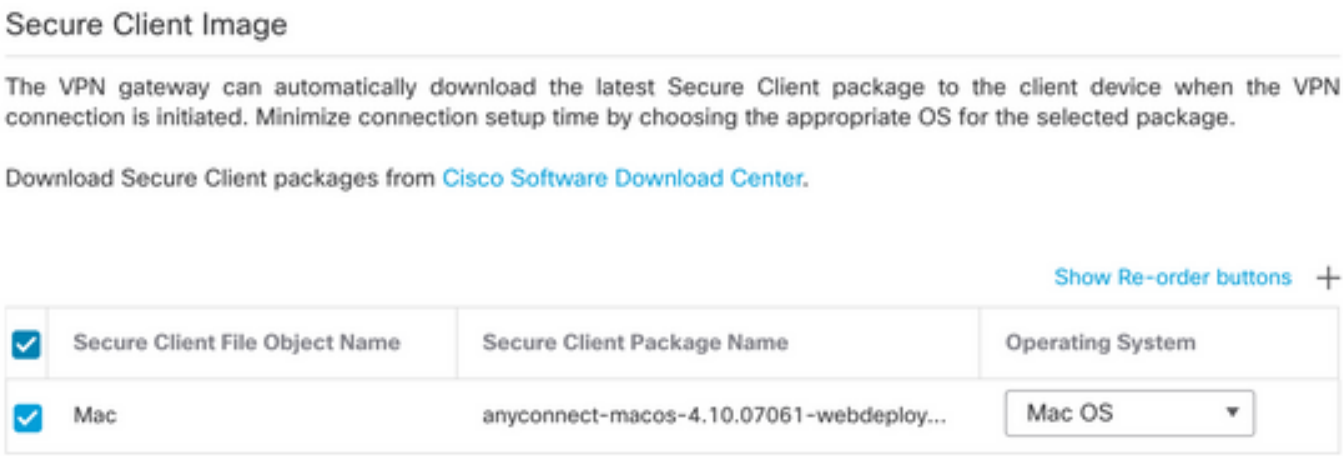
Paso 13. Haga clic en Add new AnyConnect Image para agregar un **AnyConnect Client Image** al FTD.



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



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



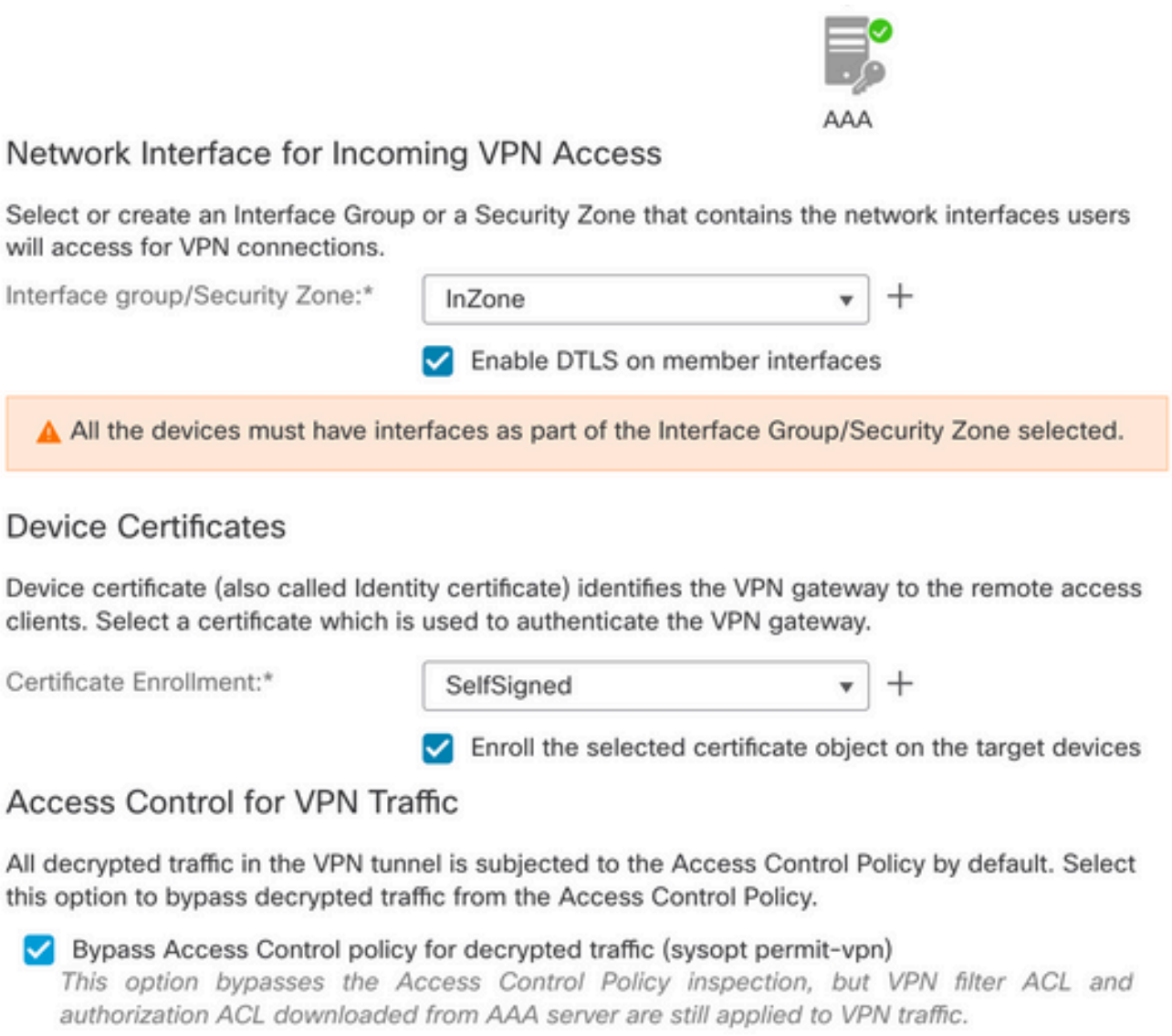
Paso 16. Elija el Interface group/Security Zone y el Device Certificate. Haga clic en Next.

A efectos de esta demostración, se entenderá por:

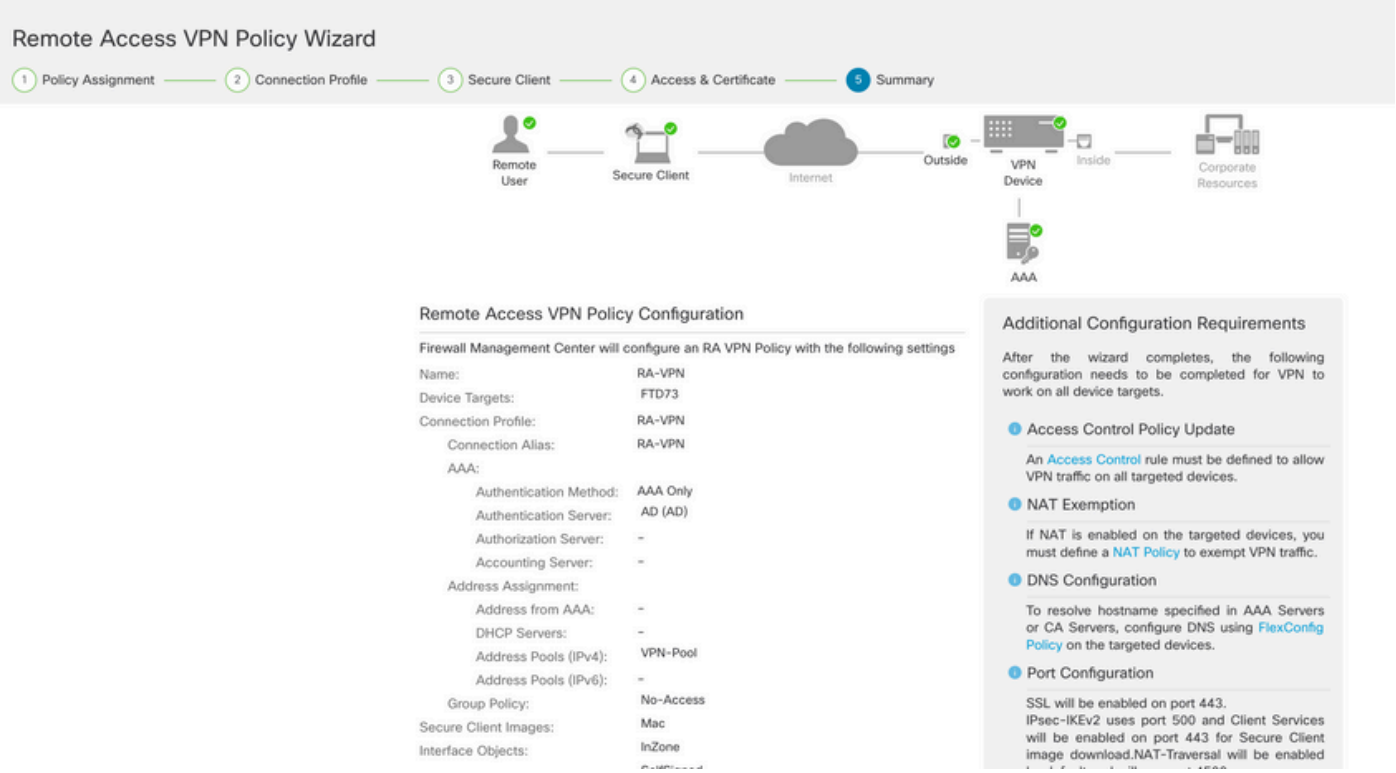
Grupo de interfaz/Zona de seguridad: Zona externa

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).



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



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>

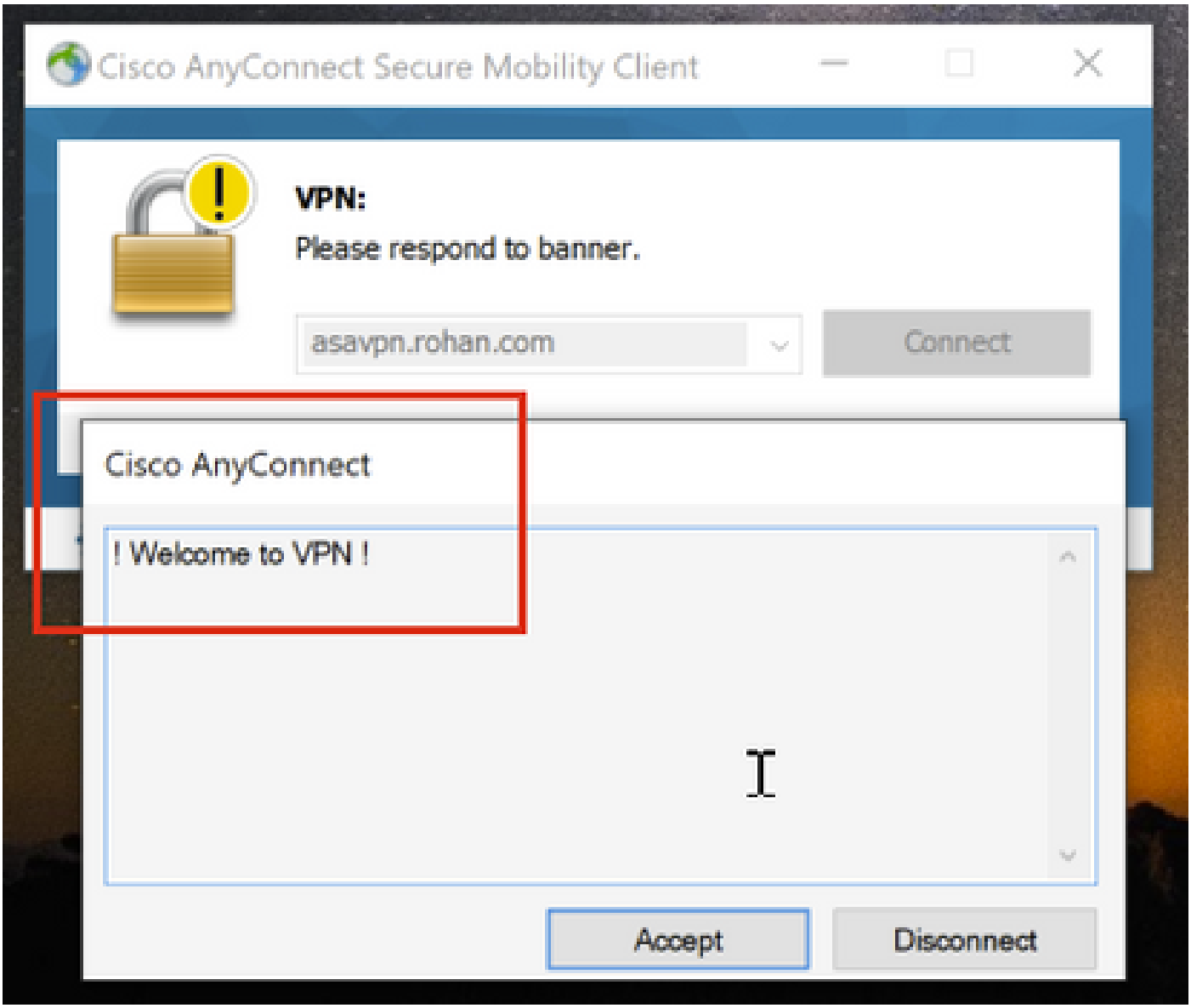
```
!--- LDAP Server Configuration ---!


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:

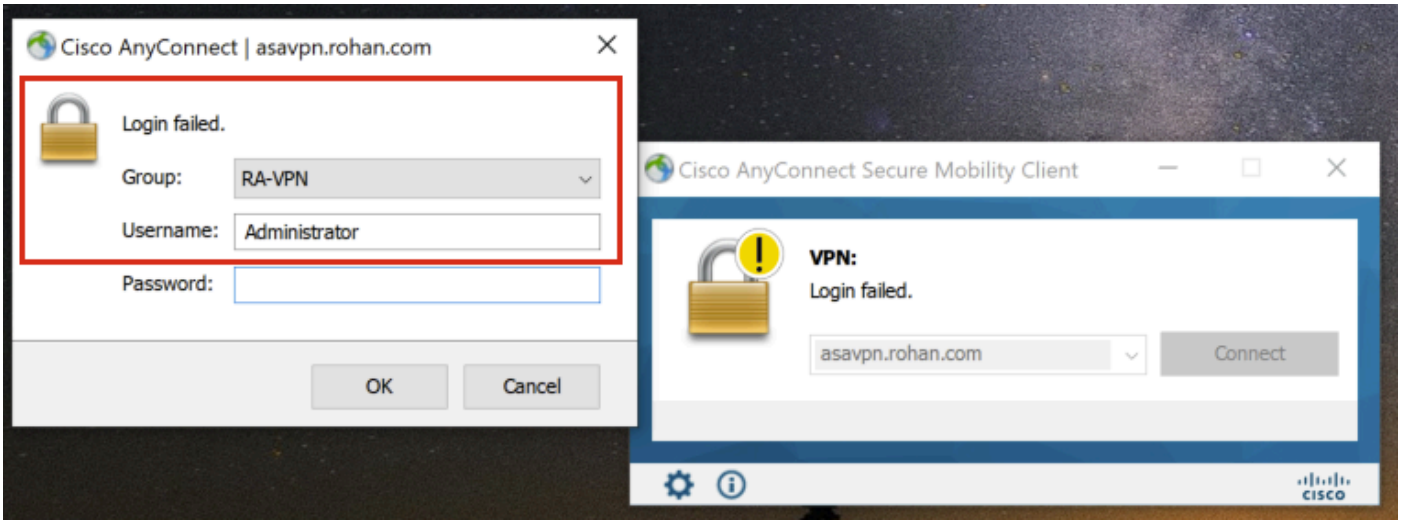
<#root>

```
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).