为FTD配置RA VPN的LDAP身份验证和授权

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- 许可证要求

FMC的配置步骤

- 领域/ LDAP服务器配置
- RA VPN配置

验证

简介

本文档介绍如何在由Firepower管理中心管理的Firepower威胁防御(FTD)上使用LDAP AA配置远程访问VPN。

先决条件

要求

Cisco 建议您了解以下主题：

- 远程访问VPN(RA VPN)工作的基础知识。
- 了解通过Firepower管理中心(FMC)进行的导航。
- Microsoft Windows Server上的轻量级目录访问协议(LDAP)服务配置。

使用的组件

本文档中的信息基于以下软件版本：

- 思科Firepower管理中心版本7.3.0
- 思科Firepower威胁防御版本7.3.0
- Microsoft Windows Server 2016，配置为LDAP服务器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文档介绍在由Firepower管理中心(FMC)管理的Firepower威胁防御(FTD)上使用轻量级目录访问协议(LDAP)身份验证和授权配置远程访问VPN(RA VPN)。

LDAP是一种开放的、供应商中立的行业标准应用协议，用于访问和维护分布式目录信息服务。

LDAP属性映射将Active Directory(AD)或LDAP服务器中存在的属性与思科属性名称等同。然后，当AD或LDAP服务器在远程访问VPN连接建立期间向FTD设备返回身份验证响应时，FTD设备可以使用信息调整AnyConnect客户端如何完成连接。

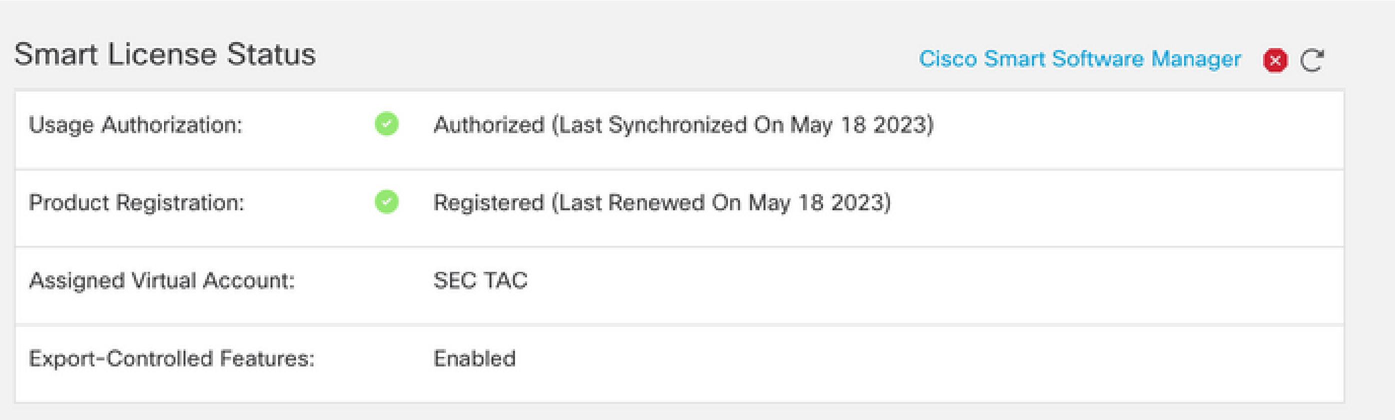
自6.2.1版本起，FMC支持使用LDAP身份验证的RA VPN，建议通过FlexConfig进行FMC 6.7.0版本之前的LDAP授权，以配置LDAP属性映射并将其与领域服务器关联。此功能（版本6.7.0）现已与FMC上的RA VPN配置向导集成，不再需要使用FlexConfig。

注意：此功能要求FMC在版本6.7.0上；而托管FTD可在任何高于6.3.0的版本上。

许可证要求

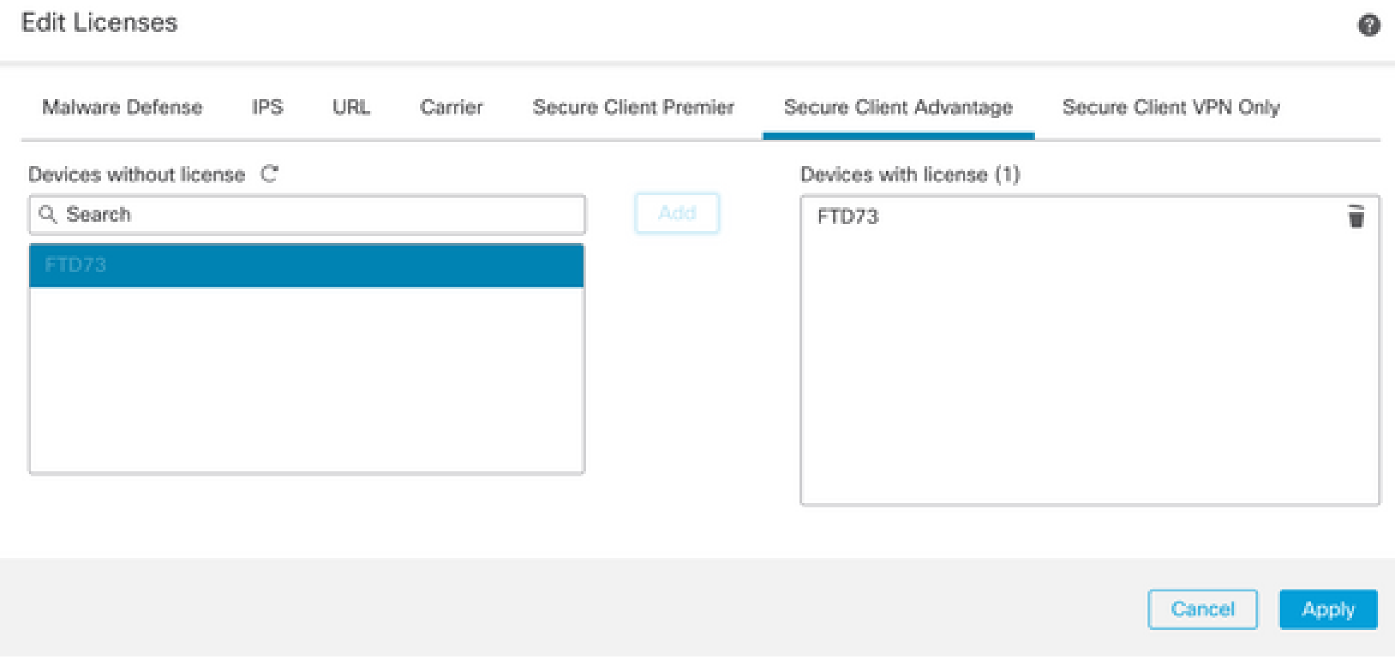
需要AnyConnect Apex、AnyConnect Plus或AnyConnect VPN Only许可证，并启用导出控制功能。

要检查许可证，请导航至 **System** > **Licenses** > **Smart Licenses**.



Smart License Status

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

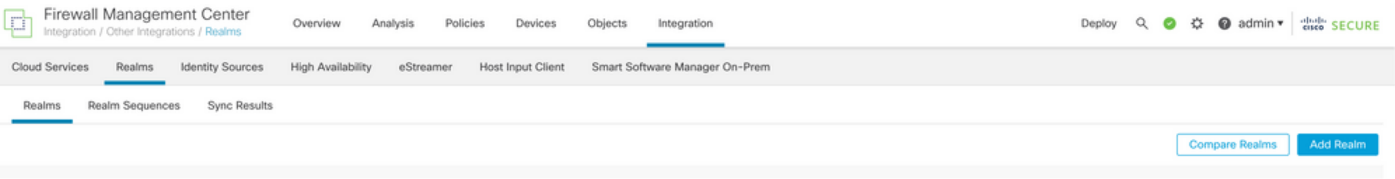


FMC的配置步骤

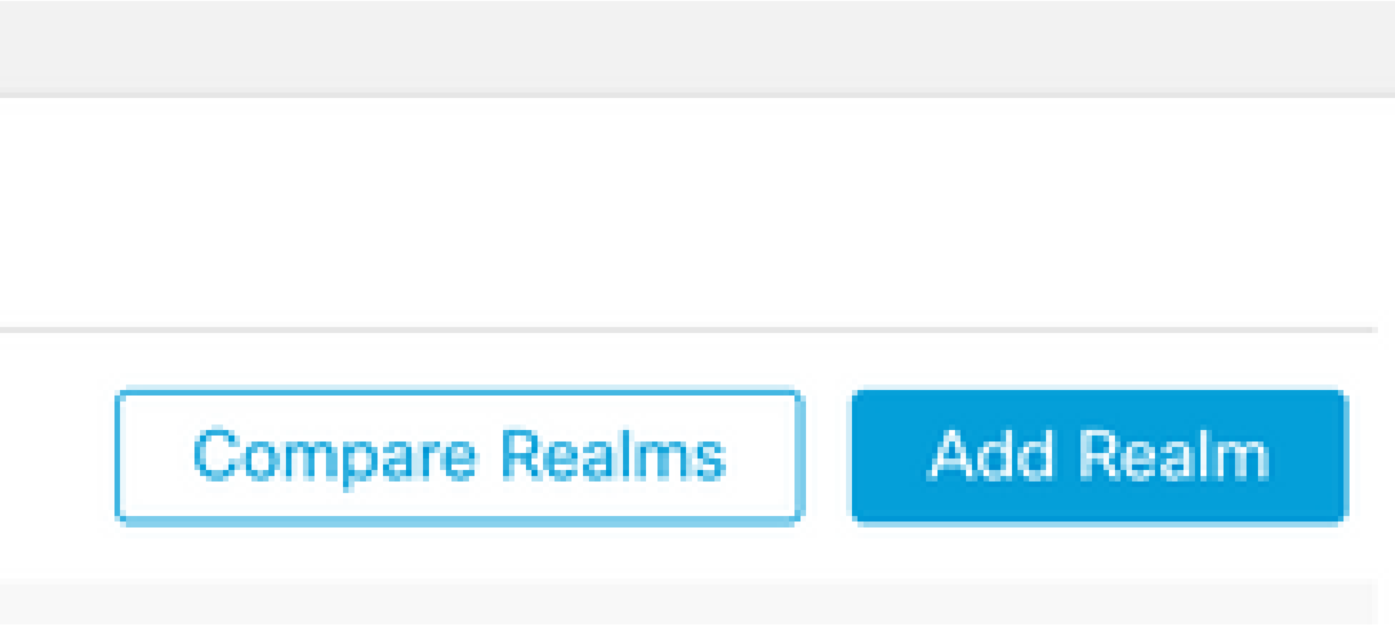
领域/ LDAP服务器配置

注意：只有在配置新的REALM/LDAP服务器时才需要列出的步骤。如果您有一个预配置的服务器，可用于在RA VPN中进行身份验证，则导航到RA VPN配置。

步骤1:导航至 System > Other Integrations > Realms ，如图所示。



第二步：如图所示，单击 **Add a new realm.**



第三步：提供AD服务器和目录的详细信息。点击 OK.

在本演示中：

名称:LDAP

类型：AD

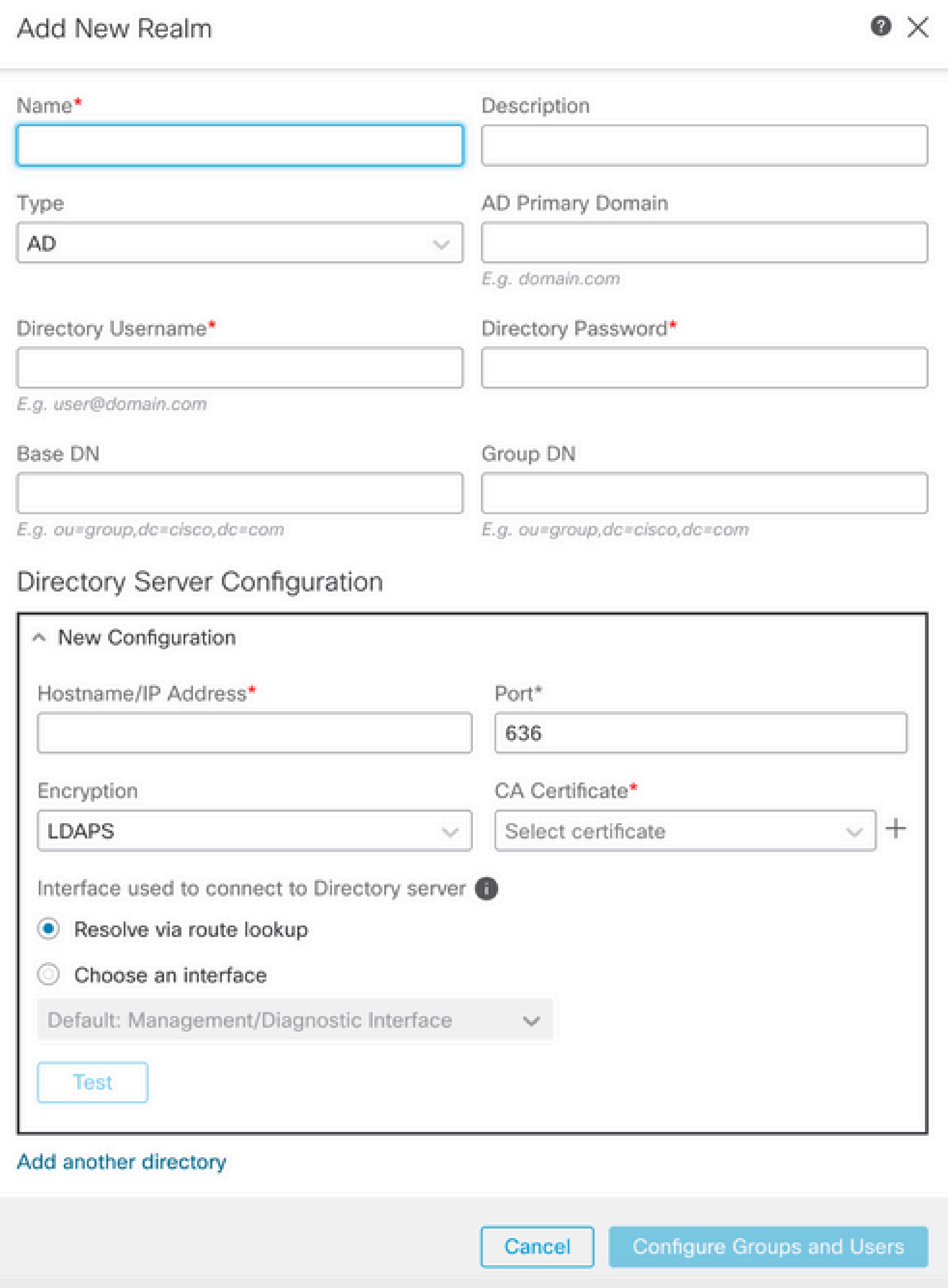
AD主域:test.com

目录用户名：CN=Administrator，CN=Users，DC=test，DC=com

目录密码： <Hidden>

基本DN:DC=test，DC=com

组DN:DC=test，DC=com



Add New Realm

Name*:

Description:

Type: AD

AD Primary Domain: *E.g. domain.com*

Directory Username*: *E.g. user@domain.com*

Directory Password*:

Base DN: *E.g. ou=group,dc=cisco,dc=com*

Group DN: *E.g. ou=group,dc=cisco,dc=com*

Directory Server Configuration

New Configuration

Hostname/IP Address*:

Port*: 636

Encryption: LDAPS

CA Certificate*: Select certificate

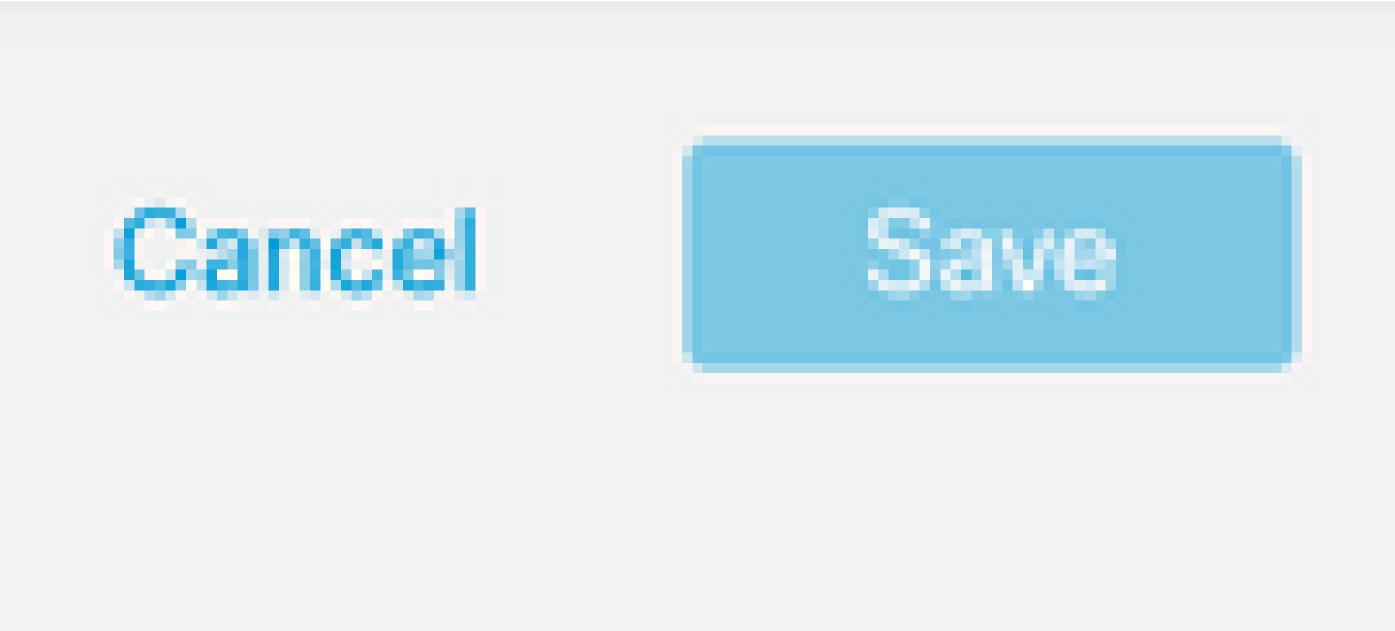
Interface used to connect to Directory server

● Resolve via route lookup

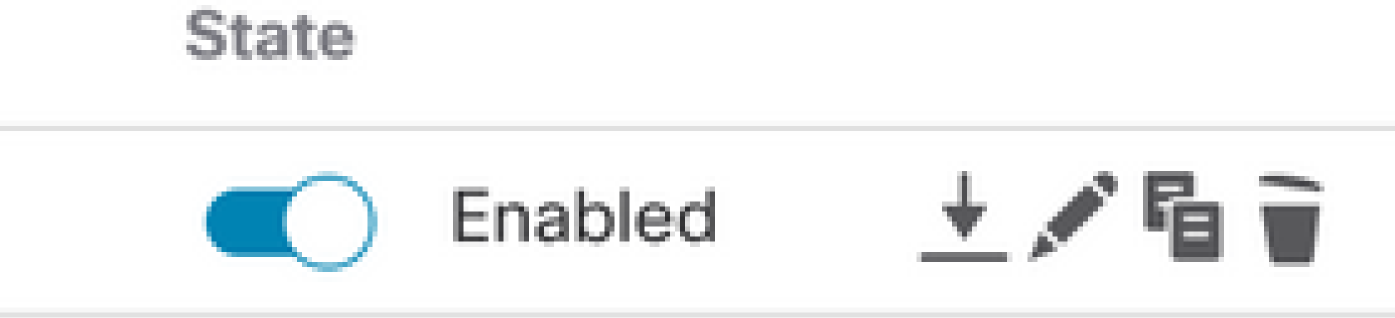
○ Choose an interface

Default: Management/Diagnostic Interface

第四步：点击 Save 保存领域/目录更改，如本图所示。



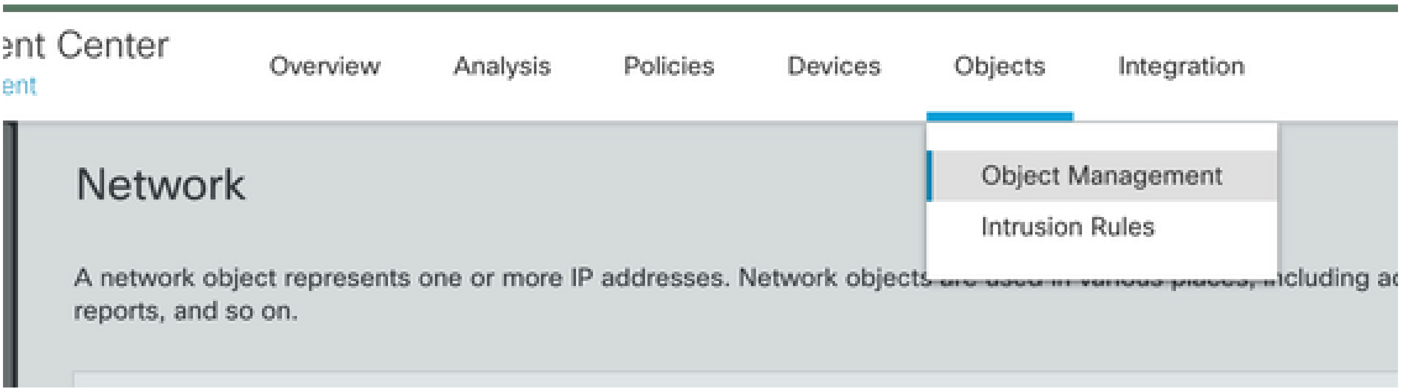
第五步：切换 State 按钮可将服务器的状态更改为“已启用”，如下图所示。



RA VPN配置

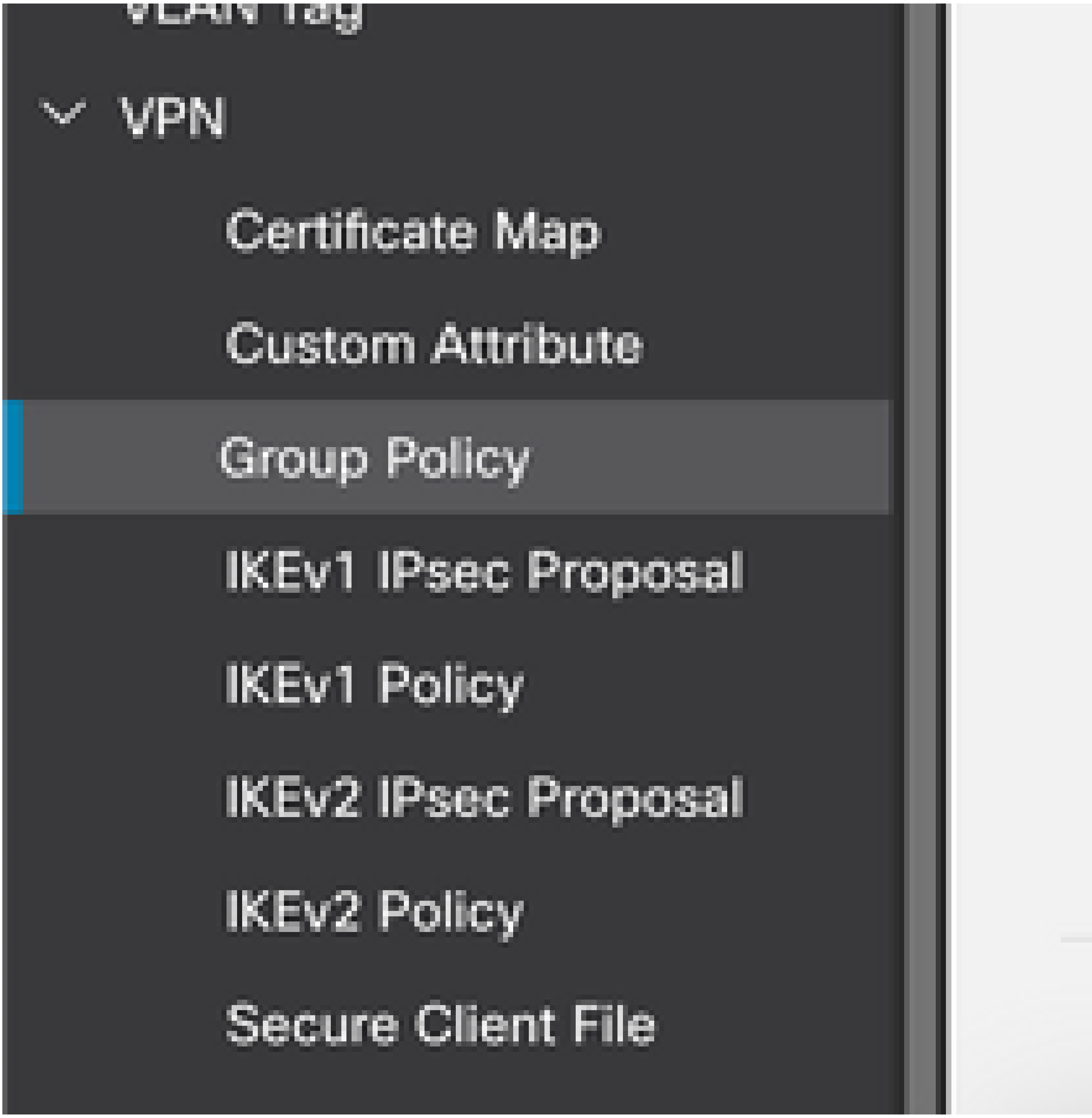
配置组策略（分配给授权VPN用户）需要执行以下步骤。如果已定义组策略，请转到步骤5。

步骤1:导航至 Objects > Object Management.

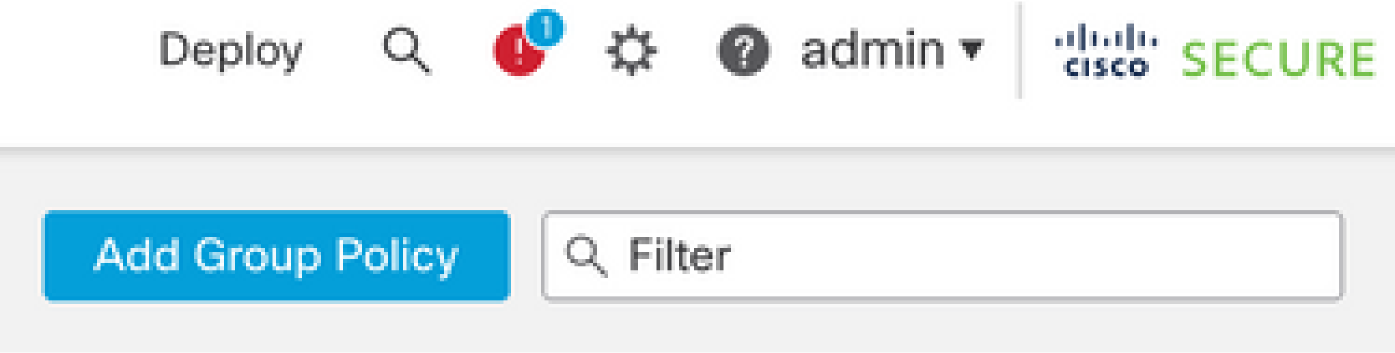


A network object represents one or more IP addresses. Network objects ...including ad reports, and so on.

第2步：在左侧窗格中，导航到 VPN > Group Policy.



第3步：点击 **Add Group Policy**.



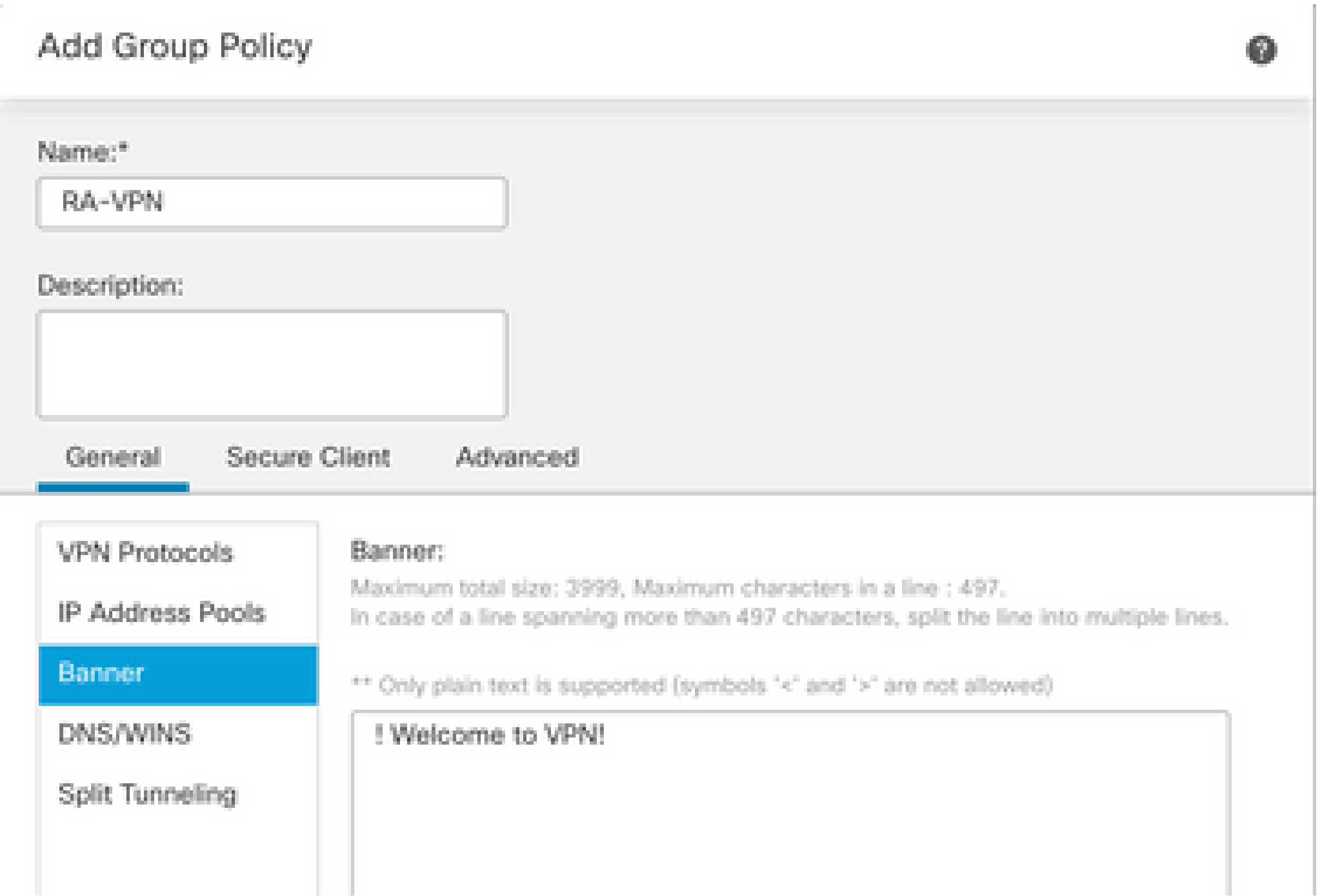
第4步：提供组策略值。

在本演示中：

名称：RA-VPN

横幅： !欢迎使用VPN!

每个用户的同时登录：3（默认值）



Add Group Policy

Name:* RA-VPN

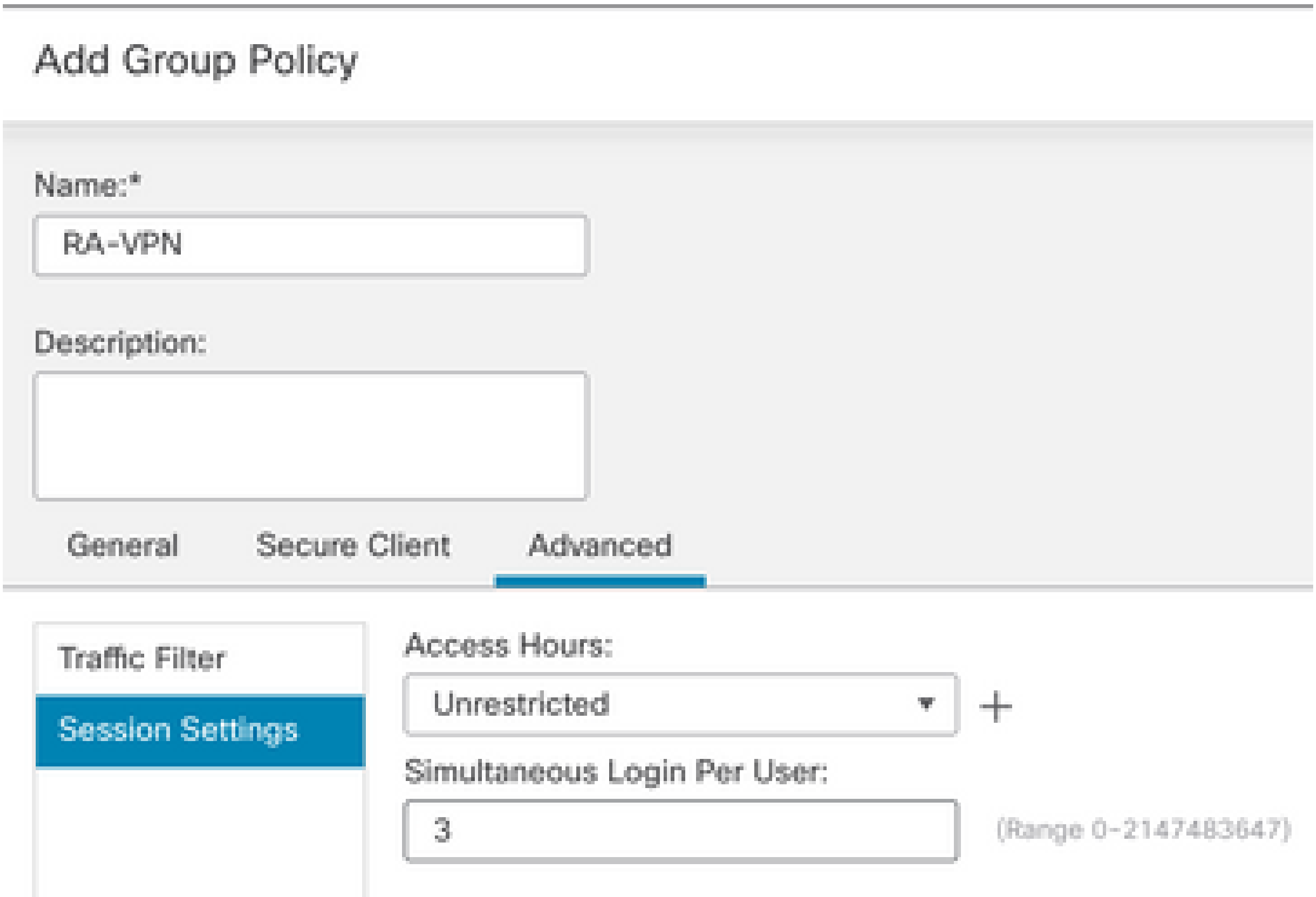
Description:

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:

Access Hours:

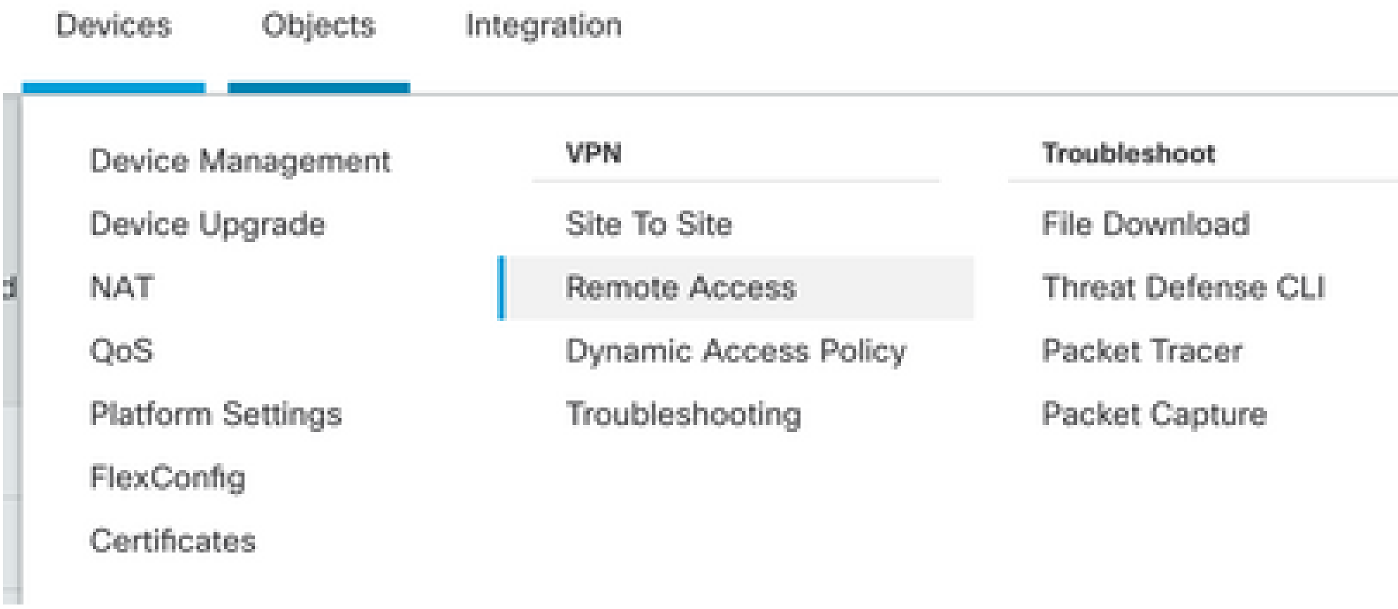
Unrestricted

Simultaneous Login Per User:

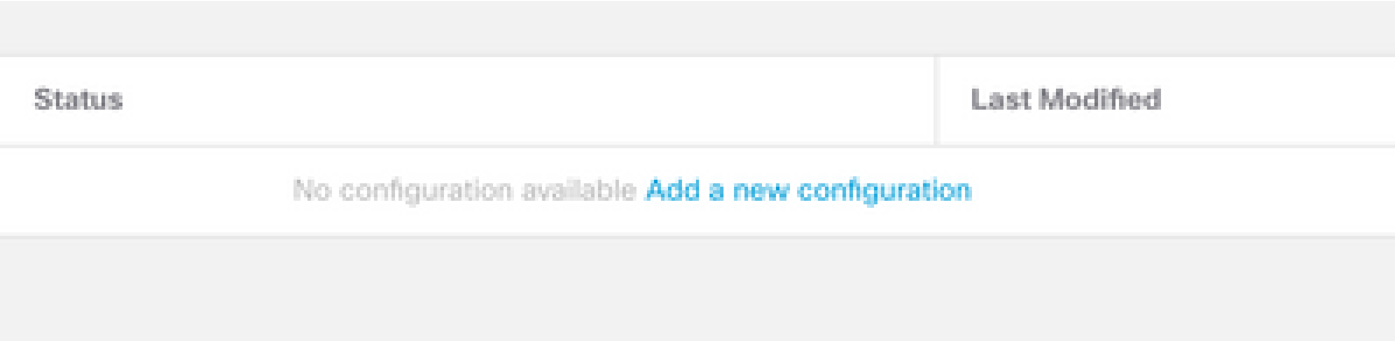
3

(Range 0-2147483647)

第五步：导航至 Devices > VPN > Remote Access.



第六步：点击 **Add a new configuration.**



Status	Last Modified
No configuration available Add a new configuration	

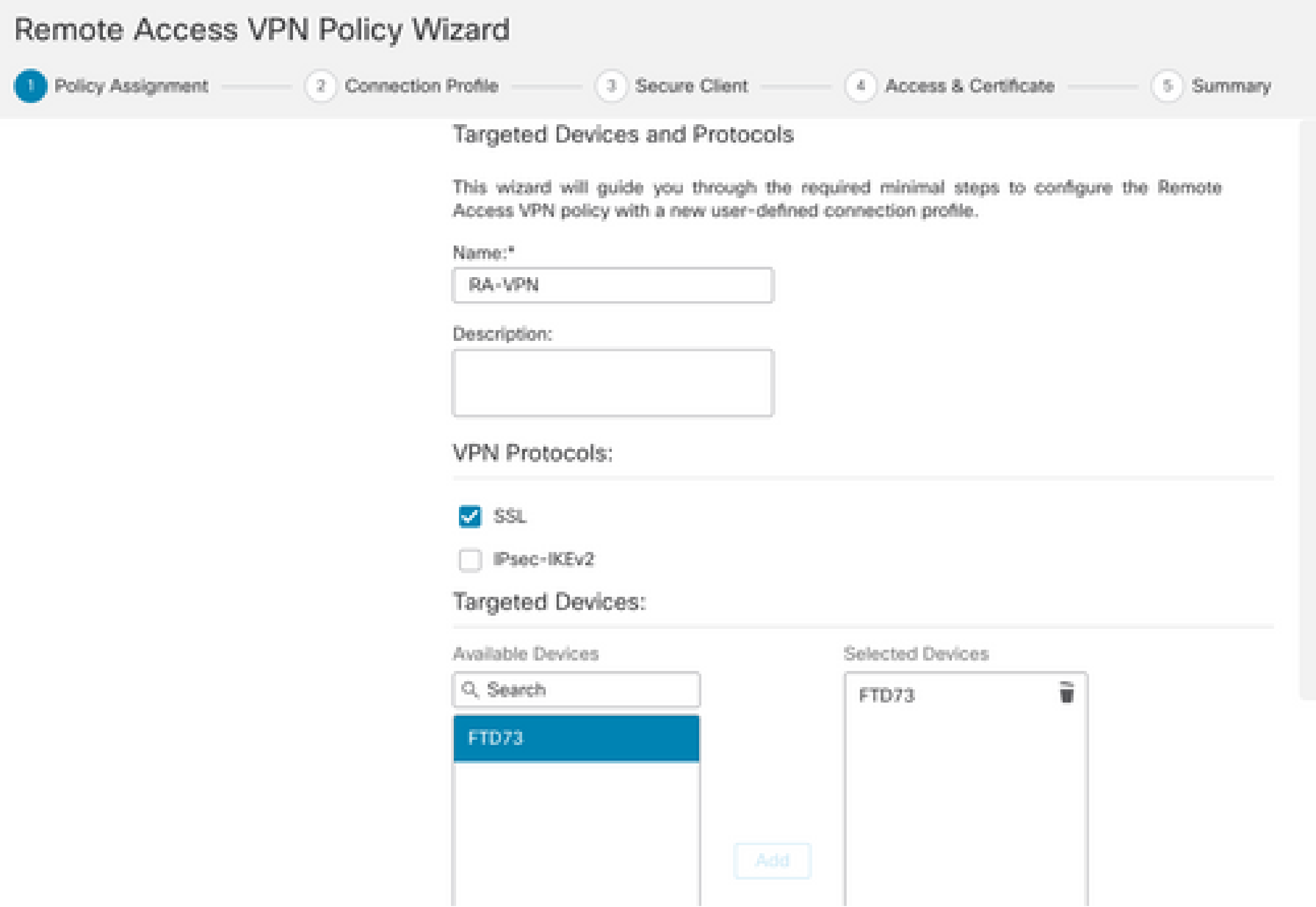
步骤 7.提供 Name RA VPN策略。选择 **VPN Protocols** 选择 **Targeted Devices**.点击 **Next.**

在本演示中：

名称：RA-VPN

VPN协议:SSL

目标设备:FTD



Remote Access VPN Policy Wizard

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:* RA-VPN

Description:

VPN Protocols:

☑ SSL

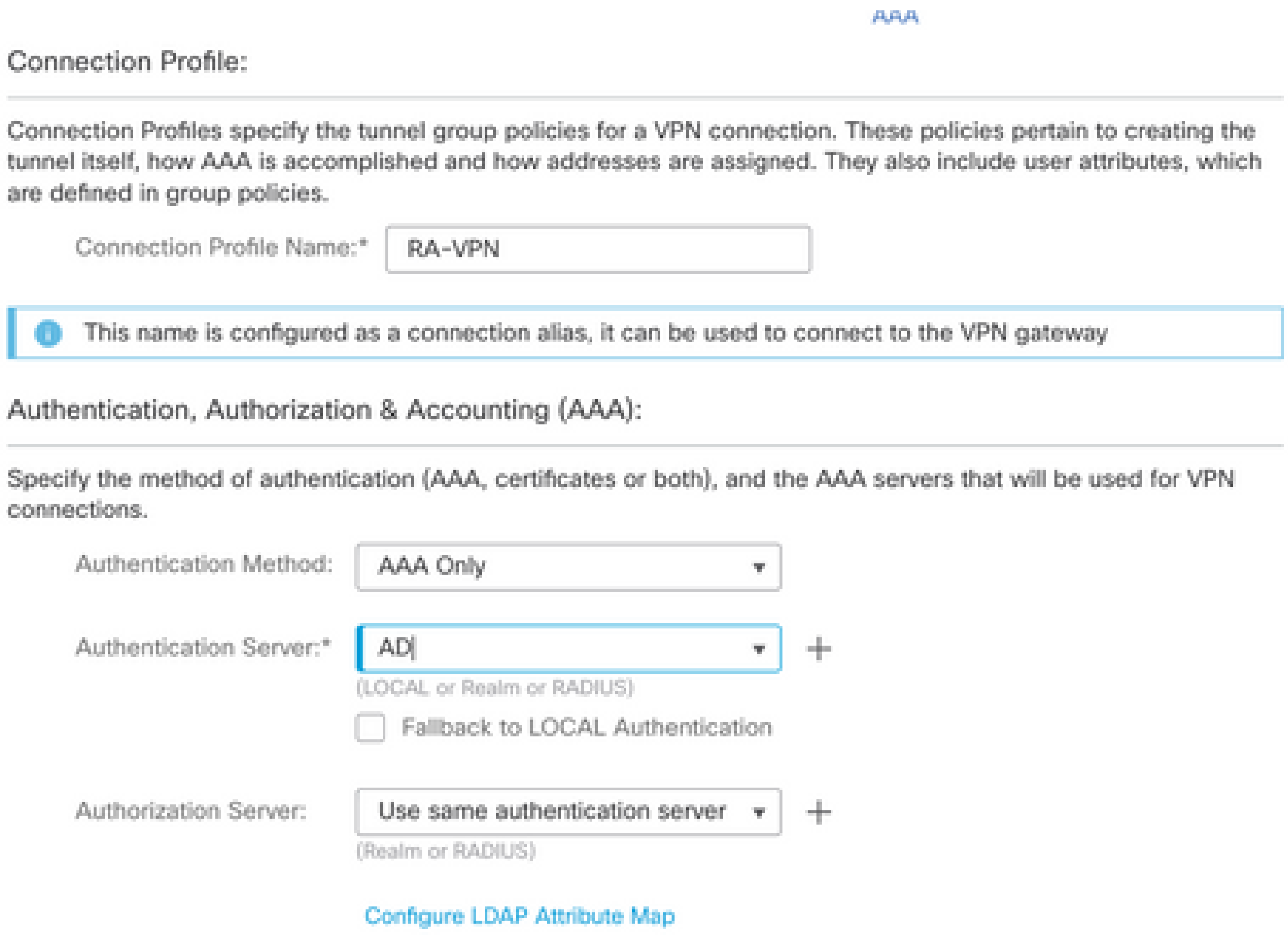
□ IPsec-IKEv2

Targeted Devices:

Available Devices: FTD73

Selected Devices: FTD73

步骤 8对于 Authentication Method，选择 **AAA Only**.为选择领域/LDAP服务器 Authentication Server.点击 **Configure LDAP Attribute Map** （配置LDAP授权）。



AAA

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:* RA-VPN

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: AAA Only

Authentication Server:* AD

(LOCAL or Realm or RADIUS)

□ Fallback to LOCAL Authentication

Authorization Server: Use same authentication server

(Realm or RADIUS)

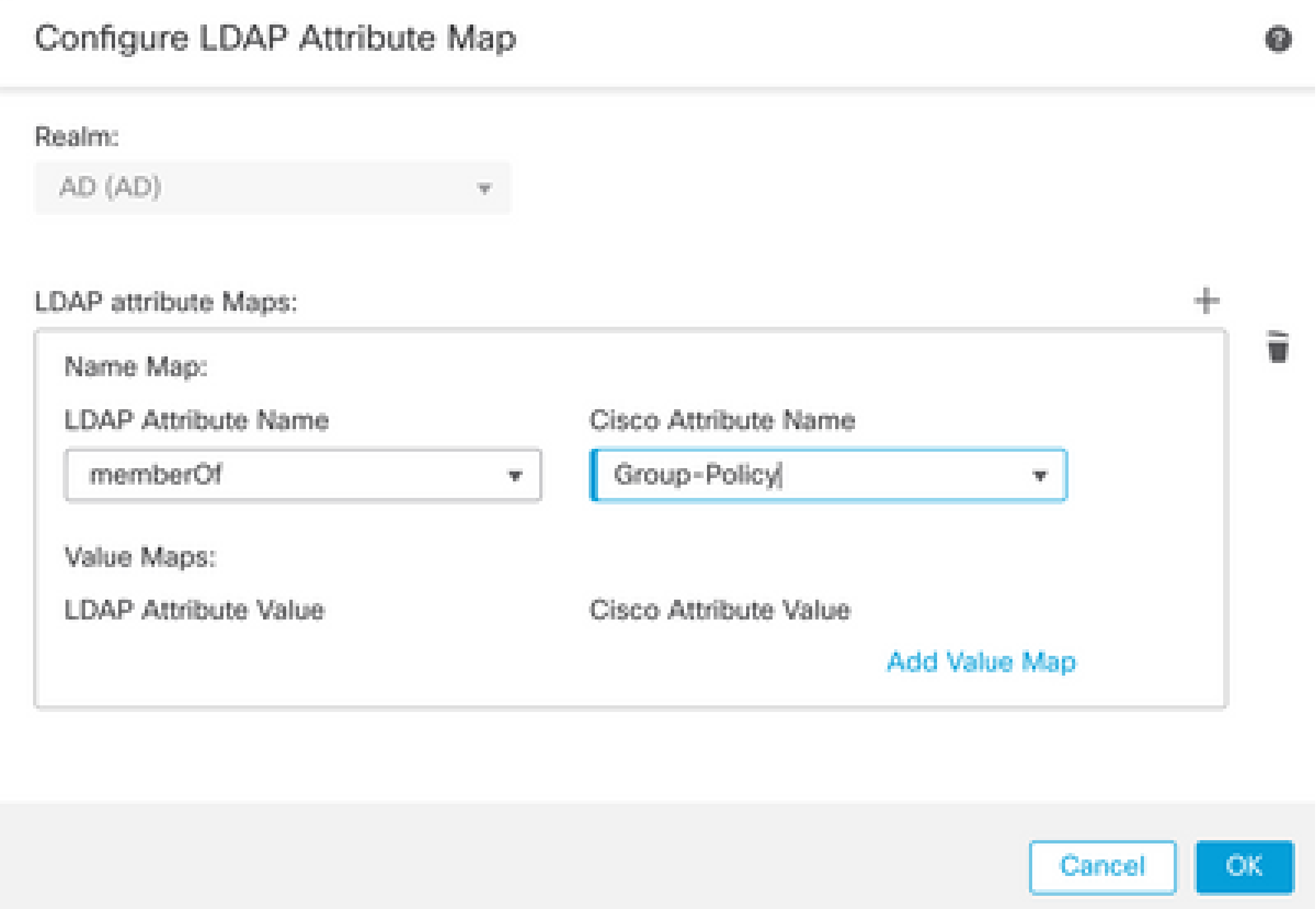
Configure LDAP Attribute Map

步骤 9提供 LDAP Attribute Name 和 Cisco Attribute Name.点击 **Add Value Map.**

在本演示中：

LDAP属性名称:memberOfI

Cisco属性名称：Group-Policy



Configure LDAP Attribute Map

Realm: AD (AD)

LDAP attribute Maps:

Name Map:

LDAP Attribute Name: memberOf

Cisco Attribute Name: Group-Policy

Value Maps:

LDAP Attribute Value

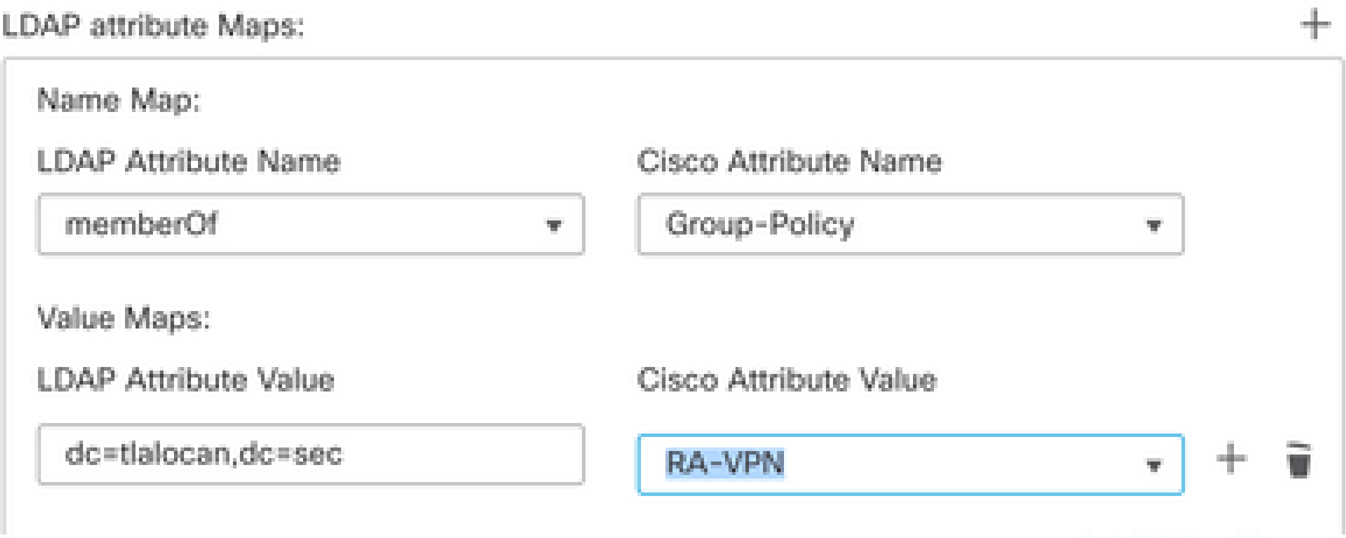
Cisco Attribute Value

步骤 10提供 LDAP Attribute Value 和 Cisco Attribute Value.点击 **OK**.

在本演示中：

LDAP属性值：DC=tlalocan，DC=sec

思科属性值：RA-VPN



LDAP attribute Maps:

Name Map:

LDAP Attribute Name: memberOf

Cisco Attribute Name: Group-Policy

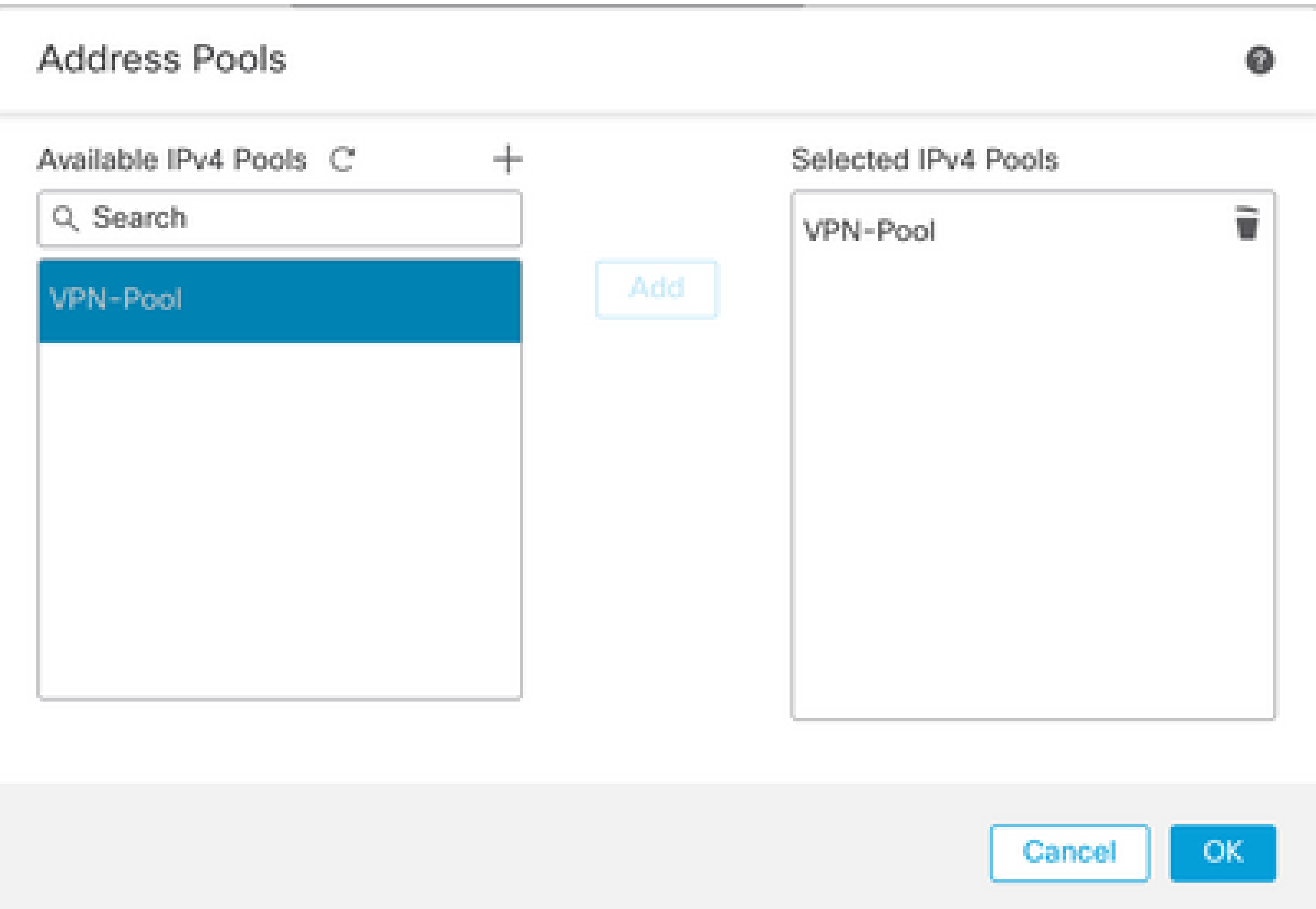
Value Maps:

LDAP Attribute Value: dc=tlalocan,dc=sec

Cisco Attribute Value: RA-VPN

注意：您可以根据需要添加更多价值映射。

步骤 11添加 Address Pool 本地地址分配。点击 **OK**.



步骤 12提供 **Connection Profile Name** 和 Group-Policy.点击 Next.

在本演示中：

连接配置文件名称：RA-VPN

身份验证方法：仅AAA

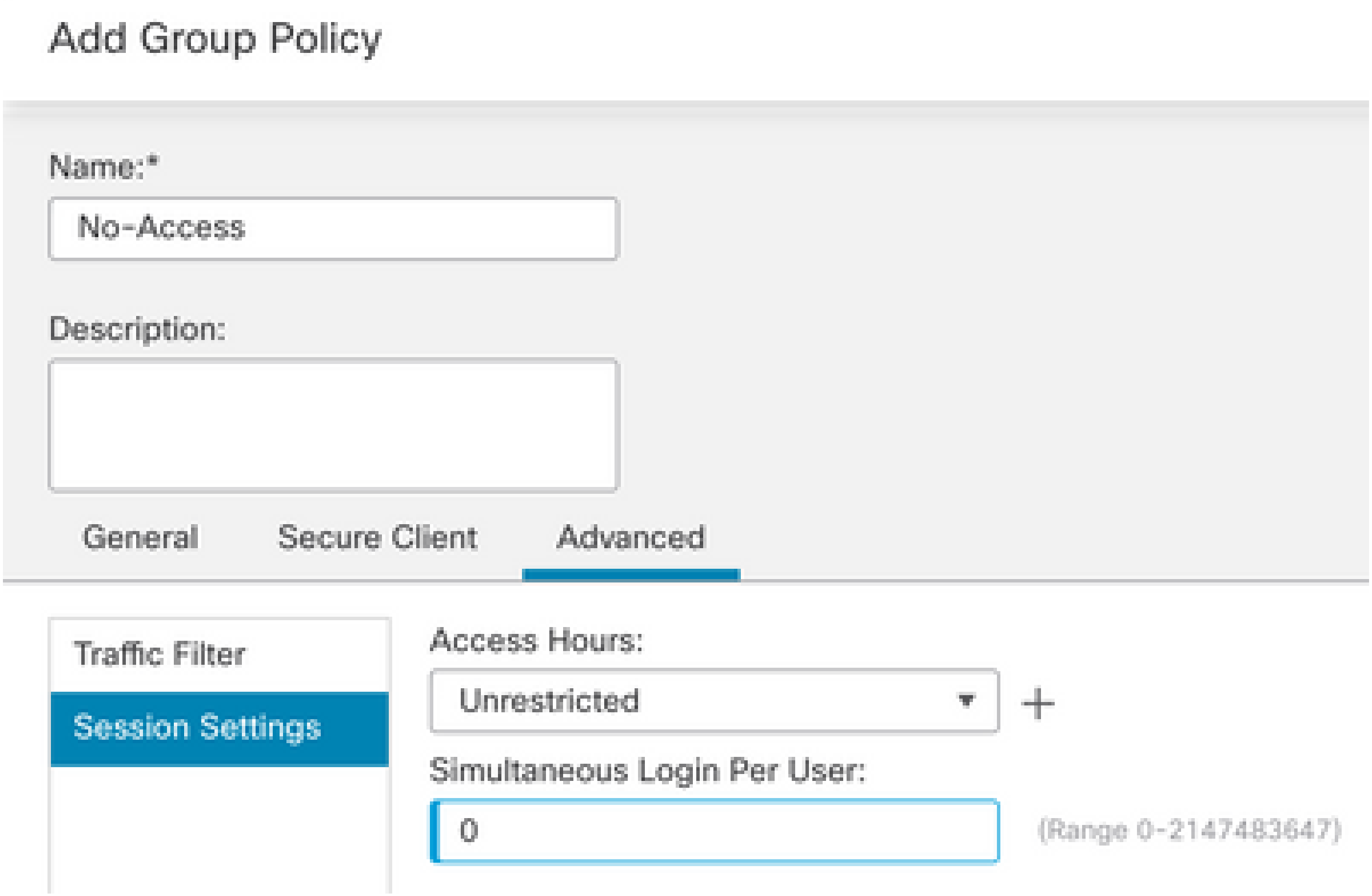
身份验证服务器：LDAP

IPv4地址池：VPN-Pool

组策略：无访问权限

注意：在前面的步骤中配置了身份验证方法、身份验证服务器和IPV4地址池。

No-Access组策略具有 Simultaneous Login Per User 参数设置为0（如果用户收到默认的No-Access组策略，则不允许用户登录）。



Add Group Policy

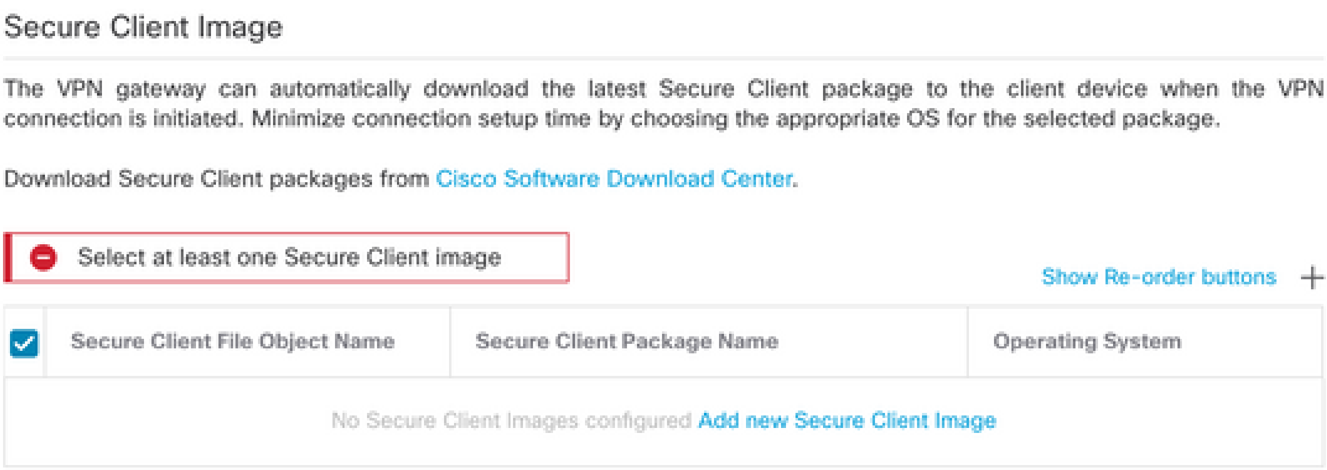
Name:* No-Access

Description:

Access Hours: Unrestricted

Simultaneous Login Per User: 0 (Range 0-2147483647)

步骤 13点击 Add new AnyConnect Image 为了添加 **AnyConnect Client Image** 到FTD。



Secure Client Image

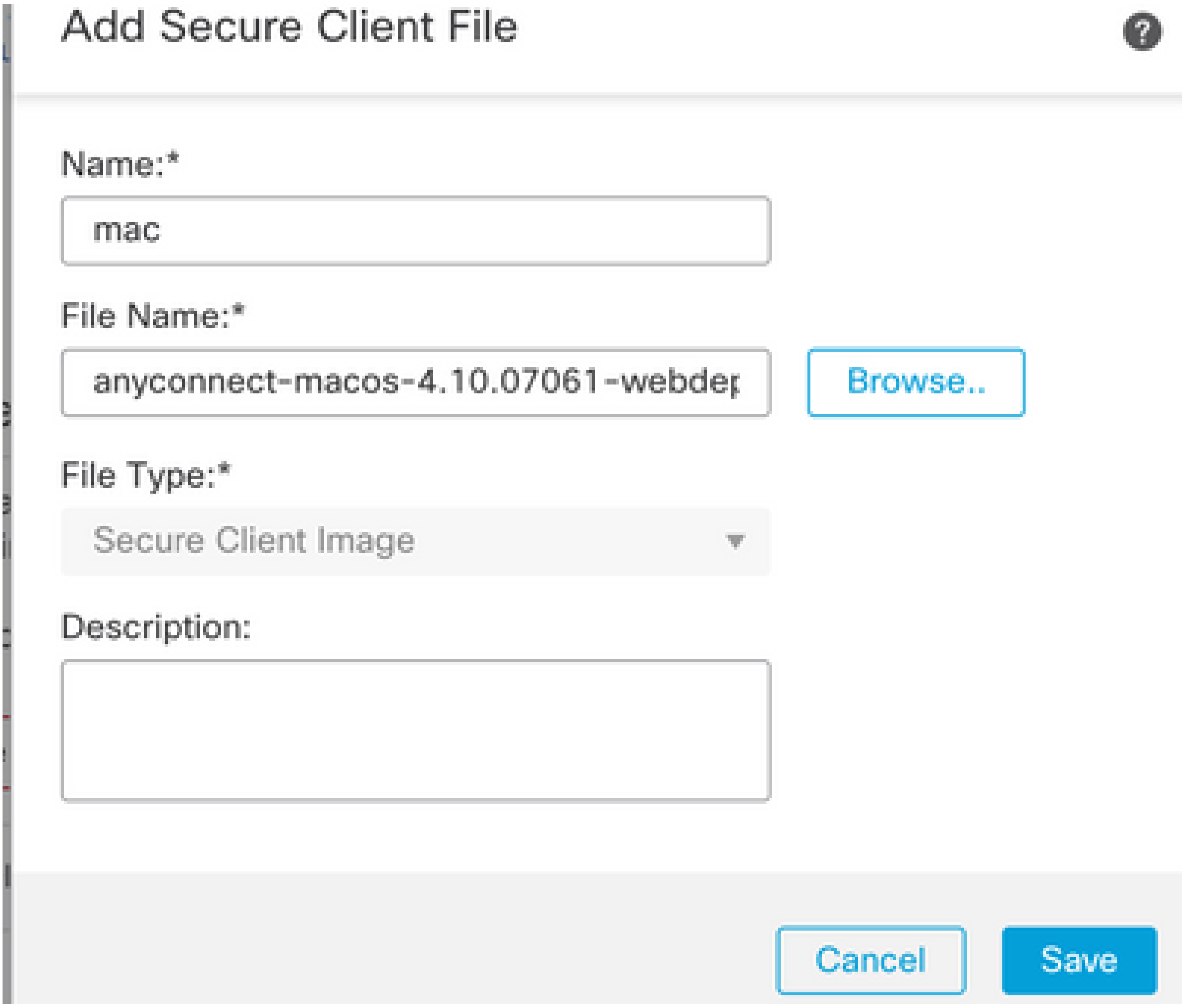
The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download Secure Client packages from Cisco Software Download Center.

Select at least one Secure Client image

☑	Secure Client File Object Name	Secure Client Package Name	Operating System
	No Secure Client Images configured Add new Secure Client Image		

步骤 14提供 Name 上传的映像并从本地存储中浏览以上传映像。点击 Save。



Add Secure Client File

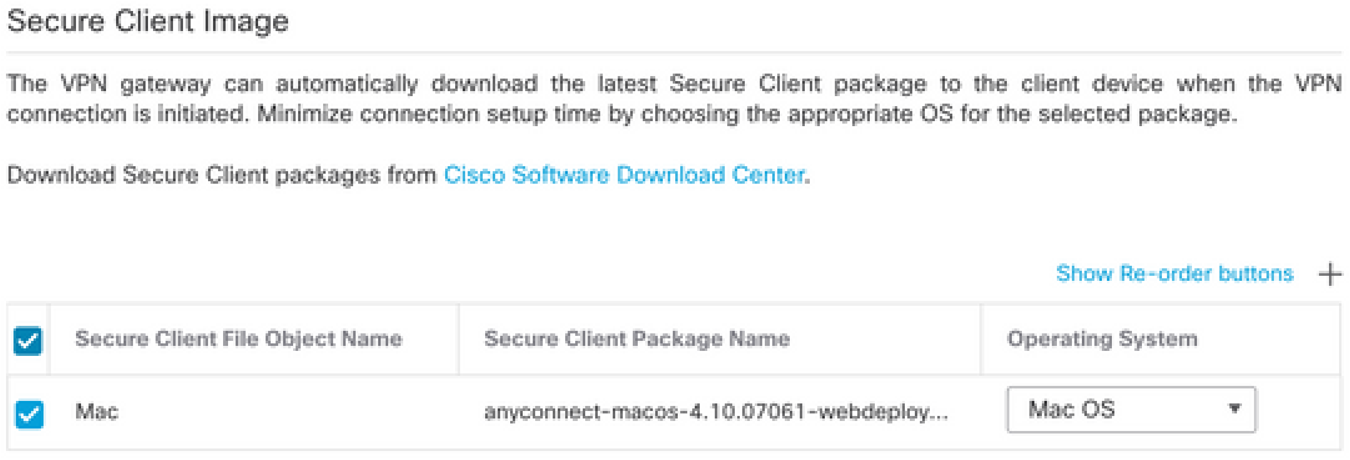
Name:* mac

File Name:* anyconnect-macos-4.10.07061-webdep

File Type:* Secure Client Image

Description:

步骤 15单击图像旁边的复选框以启用该图像以供使用。 点击 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.

☑	Secure Client File Object Name	Secure Client Package Name	Operating System
☑	Mac	anyconnect-macos-4.10.07061-webdeploy...	Mac OS ▾

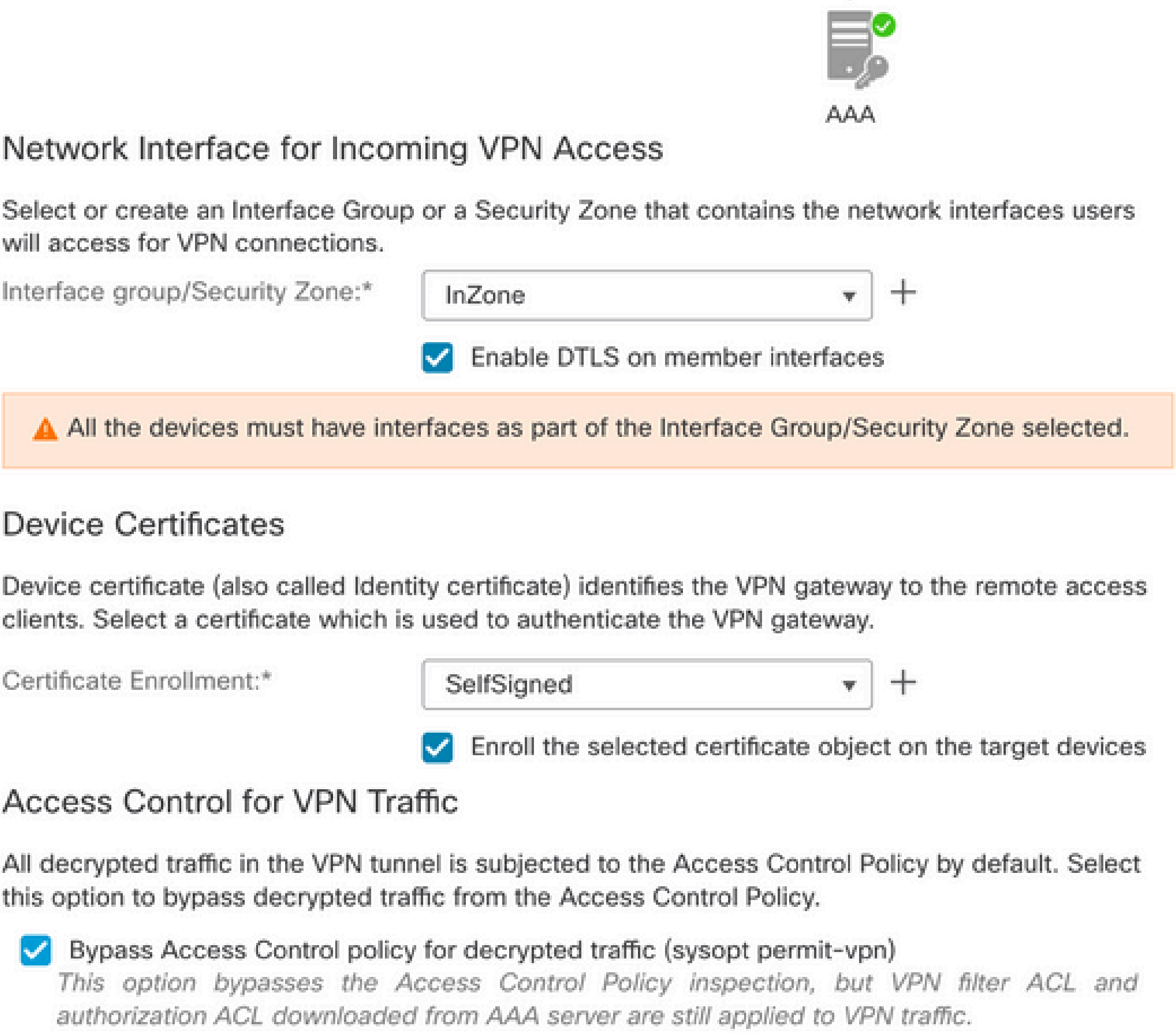
步骤 16选择 Interface group/Security Zone 和 Device Certificate.点击 Next.

在本演示中：

接口组/安全区域：区域外

设备证书：自签名

注意：您可以选择启用Bypass Access Control策略选项，以绕过针对加密(VPN)流量的任何访问控制检查（默认情况下禁用）。



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:* InZone ▾ +

☑ 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:* SelfSigned ▾ +

☑ Enroll the selected certificate object on the target devices

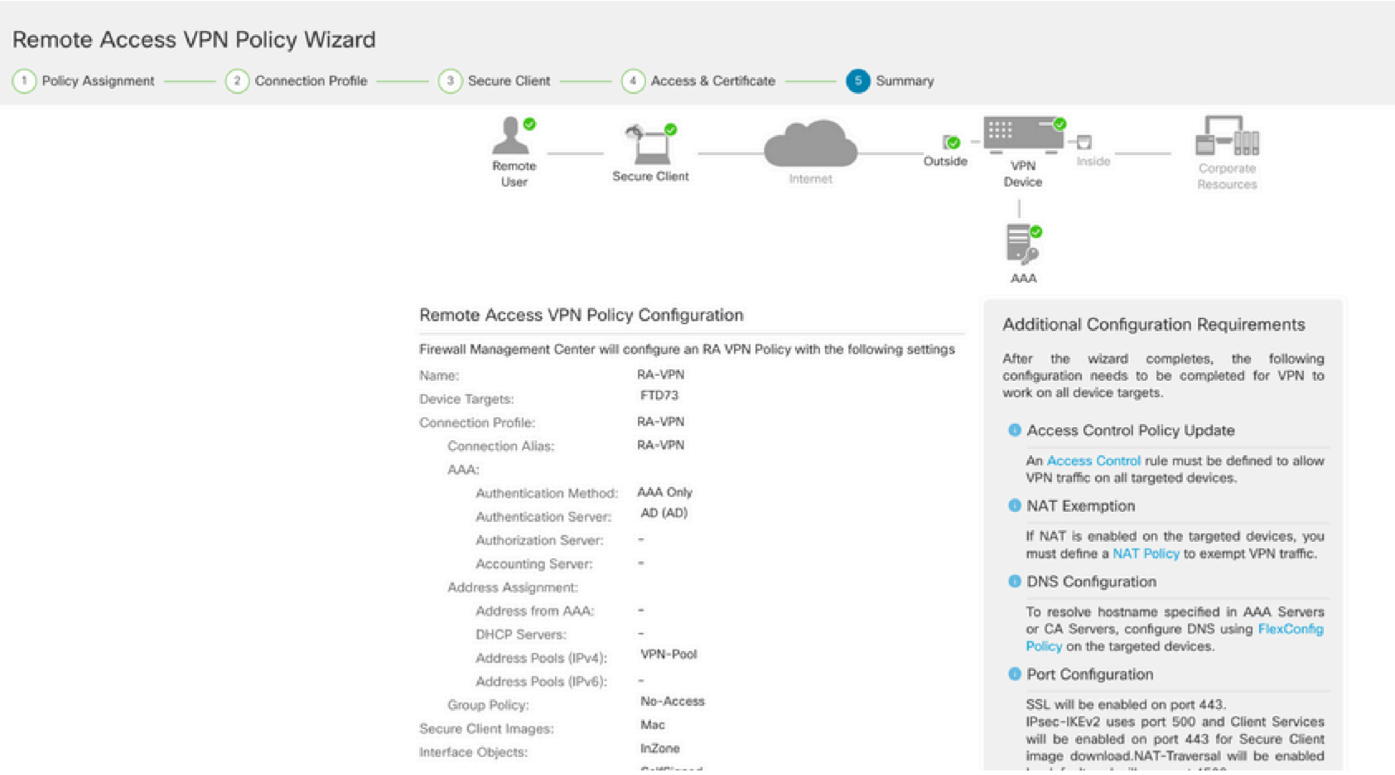
Access Control for VPN Traffic

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.

步骤 17查看RA VPN配置的摘要。点击 Finish 保存，如图所示。



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

步骤 18.导航至 Deploy > Deployment.选择配置需要部署到的FTD。点击 Deploy.

成功部署后，配置将被推送到FTD CLI:

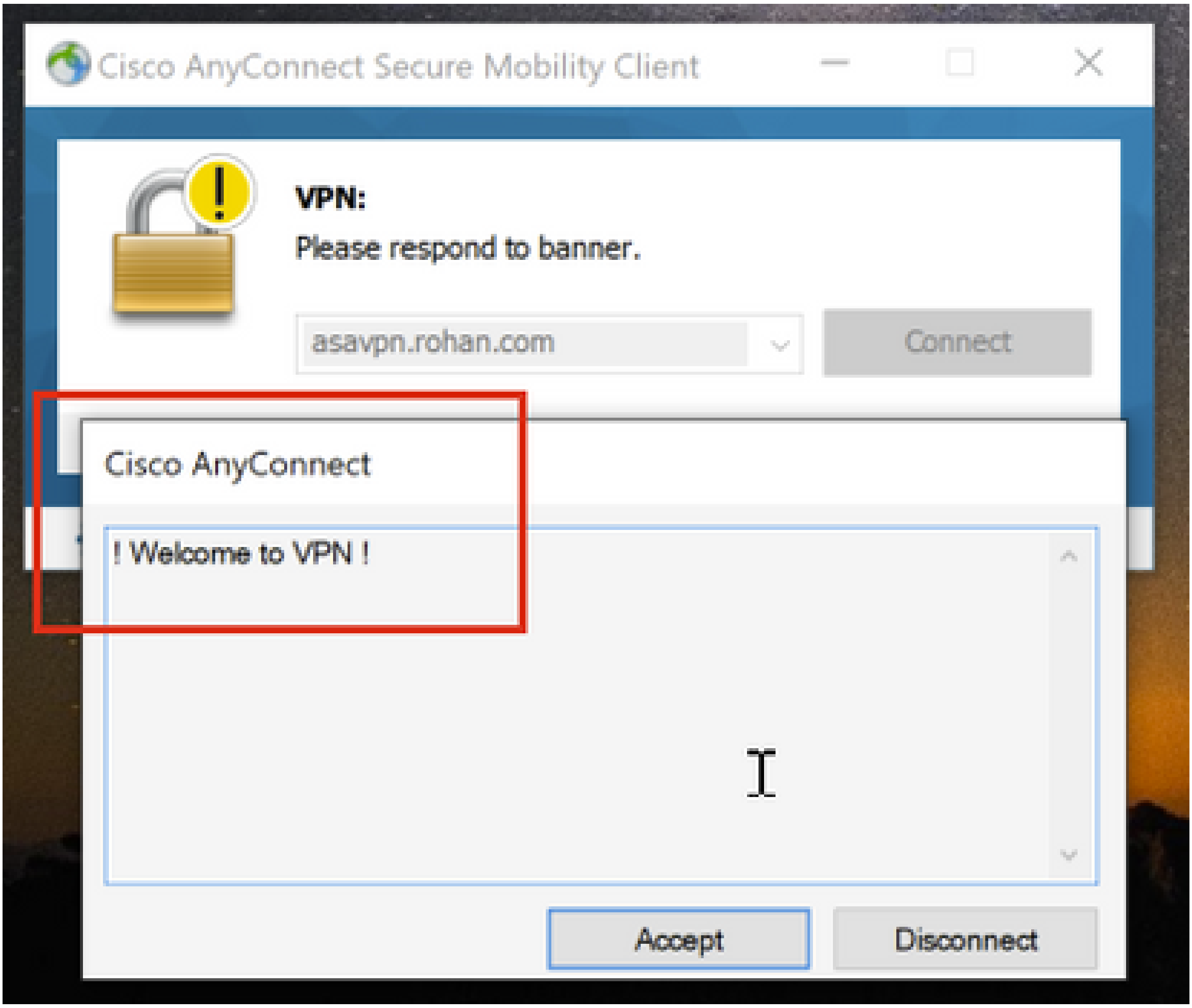
<#root>

```
!--- 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
```

验证

在AnyConnect客户端上，使用有效的VPN用户组凭据登录，然后您将获得由LDAP属性映射分配的正确的组策略：


Cisco AnyConnect Secure Mobility Client
VPN:
Please respond to banner.
asavpn.rohan.com
Connect
Cisco AnyConnect
Accept
Disconnect

! Welcome to VPN !

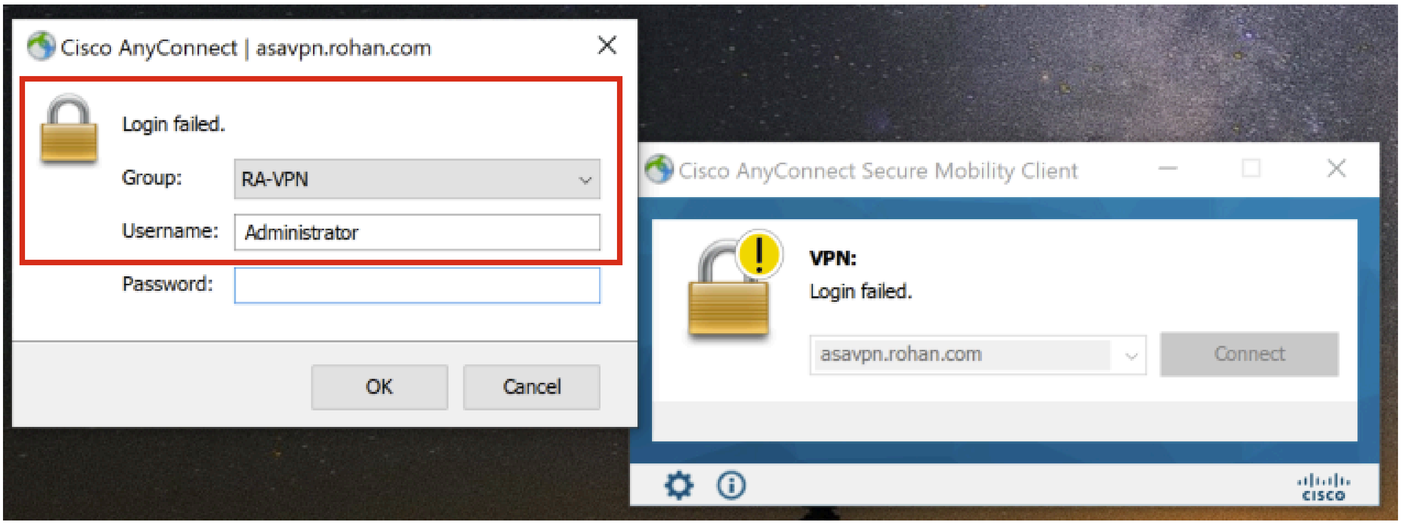
从LDAP调试片段(debug ldap 255)中，您可以看到LDAP属性映射上有匹配项：

<#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
```

在AnyConnect客户端上，使用无效的VPN用户组凭证登录，然后您将获得禁止访问组策略。



Cisco AnyConnect | asavpn.rohan.com

Login failed.

Group: RA-VPN

Username: Administrator

Password:

Cisco AnyConnect Secure Mobility Client

VPN:
Login failed.

asavpn.rohan.com

<#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
```

从LDAP调试片段(debug ldap 255)，您可以看到LDAP属性映射上没有匹配项：

<#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
```