# 在FTD上配置AnyConnect远程访问VPN

## 目录

## 简介

本文档介绍FTD上AnyConnect远程访问VPN的配置。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 基本VPN、TLS和IKEv2知识
- 基本身份验证、授权和记帐(AAA)以及RADIUS知识
- 使用Firepower管理中心的经验

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科FTD 7.2.0
- 思科FMC 7.2.1
- AnyConnect 4.10

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

本文档提供Firepower威胁防御(FTD)版本7.2.0及更高版本的配置示例，允许远程访问VPN使用传输层安全(TLS)和Internet密钥交换版本2(IKEv2)。作为客户端，可以使用Cisco AnyConnect，它受多个平台支持。

# 配置

## 1. 先决条件

要在Firepower管理中心中通过“远程访问”向导，请执行以下操作：

- 创建用于服务器身份验证的证书。
- 配置RADIUS或LDAP服务器以进行用户身份验证。
- 为VPN用户创建地址池。
- 上传不同平台的AnyConnect映像。

### a)导入SSL证书

配置AnyConnect时，证书至关重要。证书必须具有DNS名称和/或IP地址的主题备用名称扩展名以避免在Web浏览器中出错。

**注意**：只有注册的思科用户才能访问内部工具和漏洞信息。

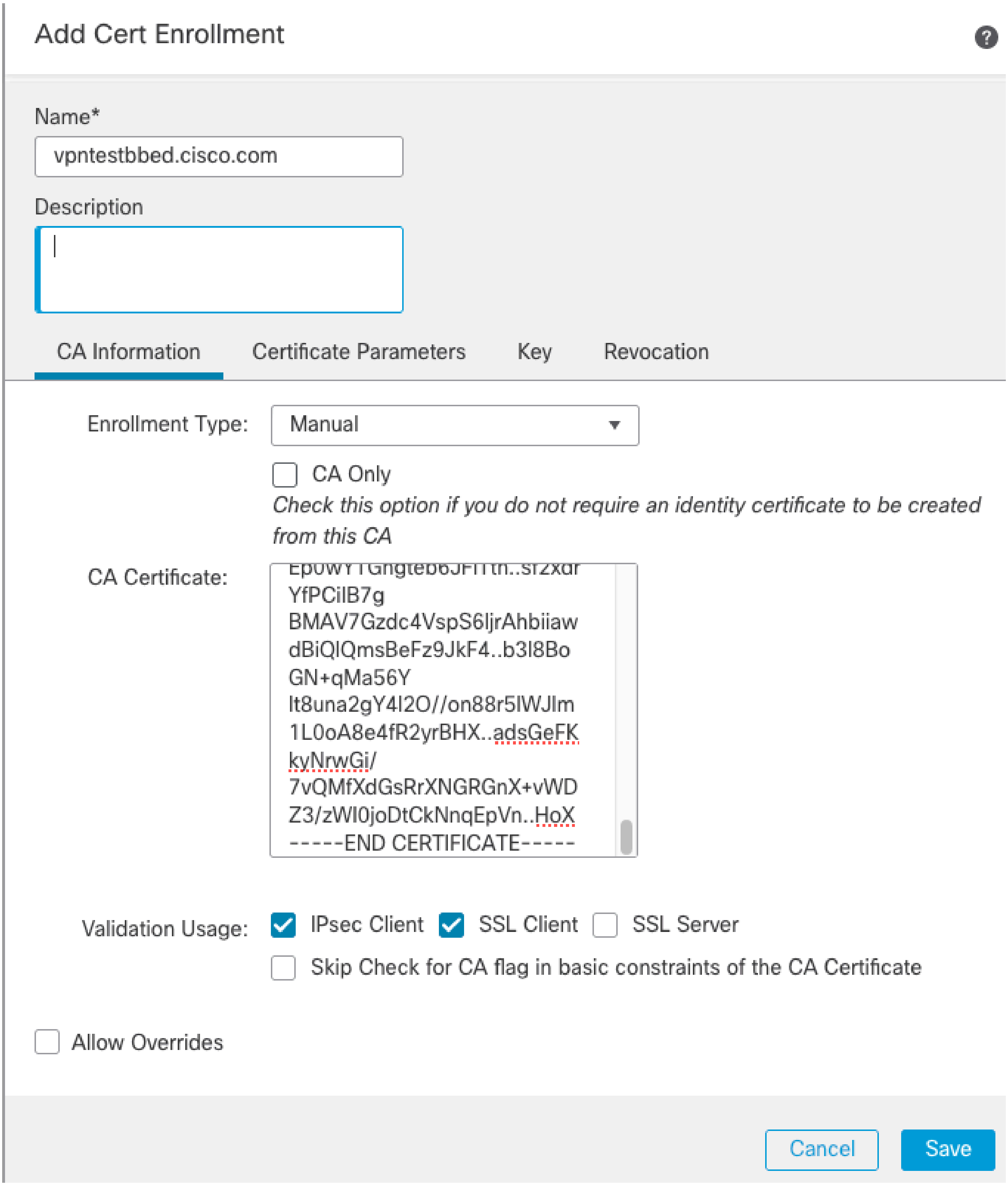
手动证书注册存在限制：

— 在FTD上，在生成CSR之前需要CA证书。

— 如果CSR是在外部生成的，则手动方法会失败，必须使用其他方法(PKCS12)。

在FTD设备上获取证书有多种方法，但安全且简单的方法是创建证书签名请求(CSR)，使用证书颁发机构(CA)对其进行签名，然后导入为CSR中的公钥颁发的证书。下面是如何做到这一点的：

- 转到 Objects > **Object Management > PKI > Cert Enrollment** ，单击**Add Cert Enrollment**。



Name*
vpntestbbed.cisco.com

Description

Enrollment Type: Manual

□ CA Only

*Check this option if you do not require an identity certificate to be created from this CA*

CA Certificate:

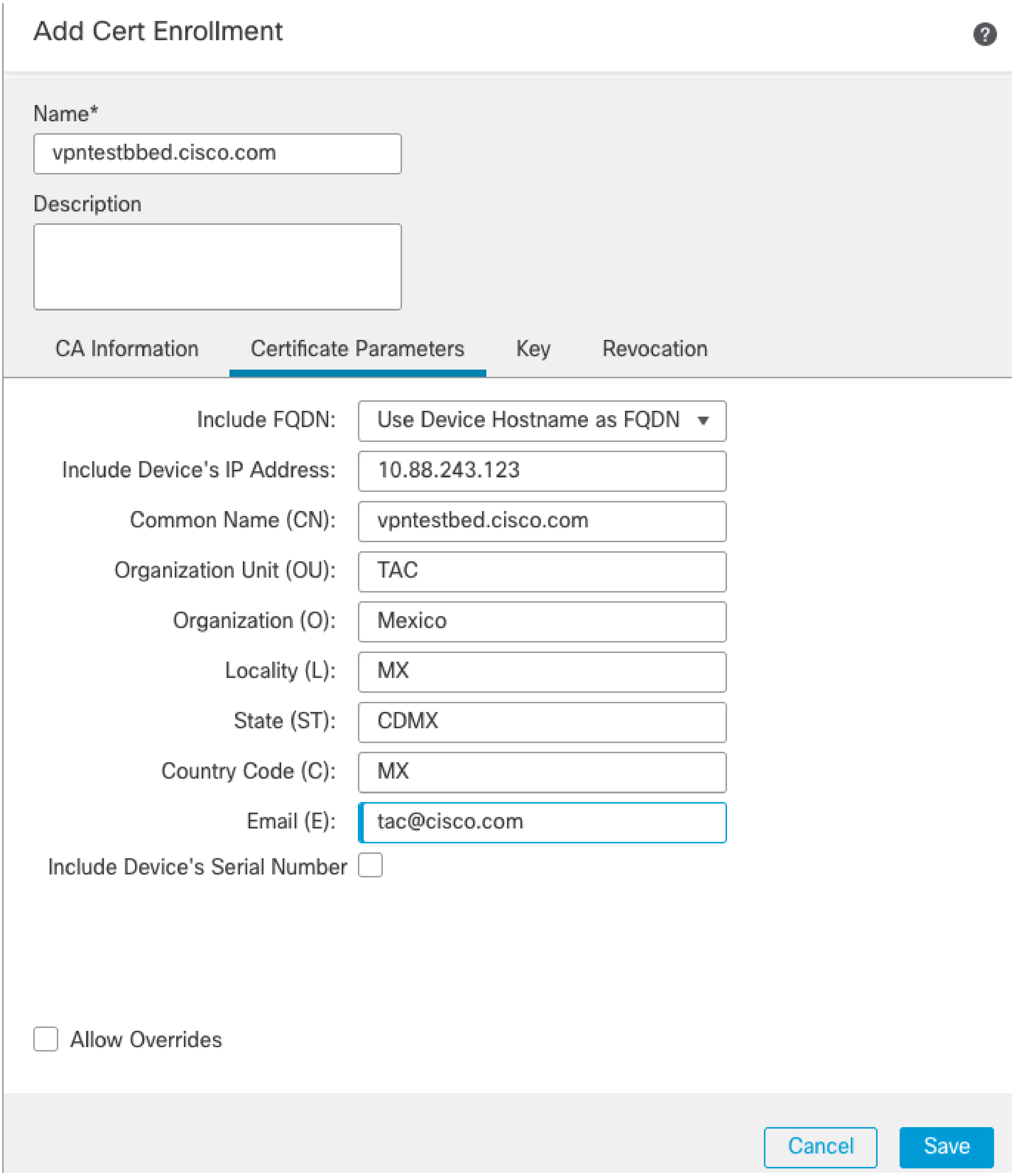
```
EpUwYTGngteb6JFITth..sf2xdr
YfPCilB7g
BMAV7Gzdc4VspS6ljrAhbiiaw
dBiQlQmsBeFz9JkF4..b3l8Bo
GN+qMa56Y
lt8una2gY4l2O//on88r5lWJlm
1L0oA8e4fR2yrBHX..adsGeFK
kyNrwGi/
7vQMfXdGsRrXNGRGnX+vWD
Z3/zWI0joDtCkNnqEpVn..HoX
-----END CERTIFICATE-----
```

Validation Usage: ☑ IPsec Client ☑ SSL Client □ SSL Server

□ Skip Check for CA flag in basic constraints of the CA Certificate

□ Allow Overrides

- 选择 Enrollment Type 并粘贴证书颁发机构(CA)证书（用于签署CSR的证书）。
- 然后转至第二个选项卡并选择 Custom FQDN 并填写所有必填字段，例如：



Add Cert Enrollment

Name*

vpntestbbed.cisco.com

Description

Include FQDN: Use Device Hostname as FQDN

Include Device's IP Address: 10.88.243.123

Common Name (CN): vpntestbed.cisco.com

Organization Unit (OU): TAC

Organization (O): Mexico

Locality (L): MX

State (ST): CDMX

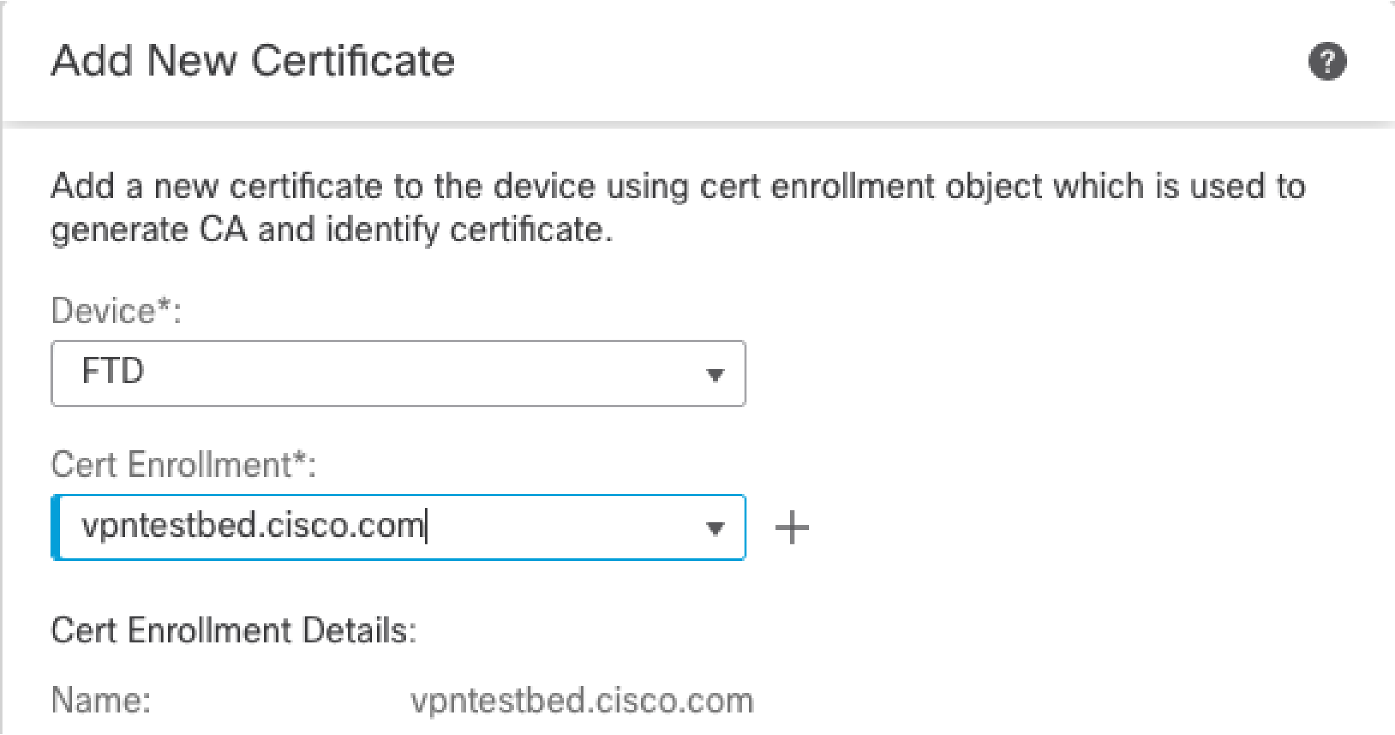
Country Code (C): MX

Email (E): tac@cisco.com

Include Device's Serial Number □

□ Allow Overrides

- 在第三个选项卡上，选择 Key Type，选择名称和大小。对于RSA，最少2048位。
- 点击保存并转至 Devices > Certificates > Add > New Certificate。
- 然后选择 Device、和 Cert Enrollment 选择您刚刚创建的信任点，点击 Add:



Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

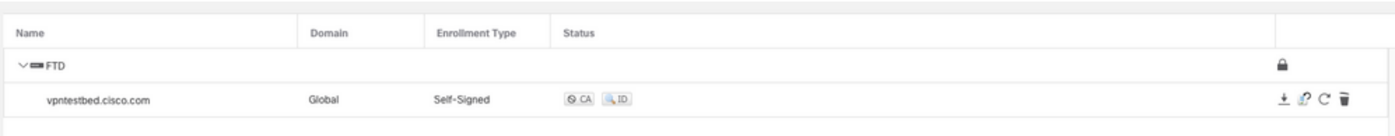
Device*: FTD

Cert Enrollment*: vpntestbed.cisco.com

Cert Enrollment Details:

Name: vpntestbed.cisco.com

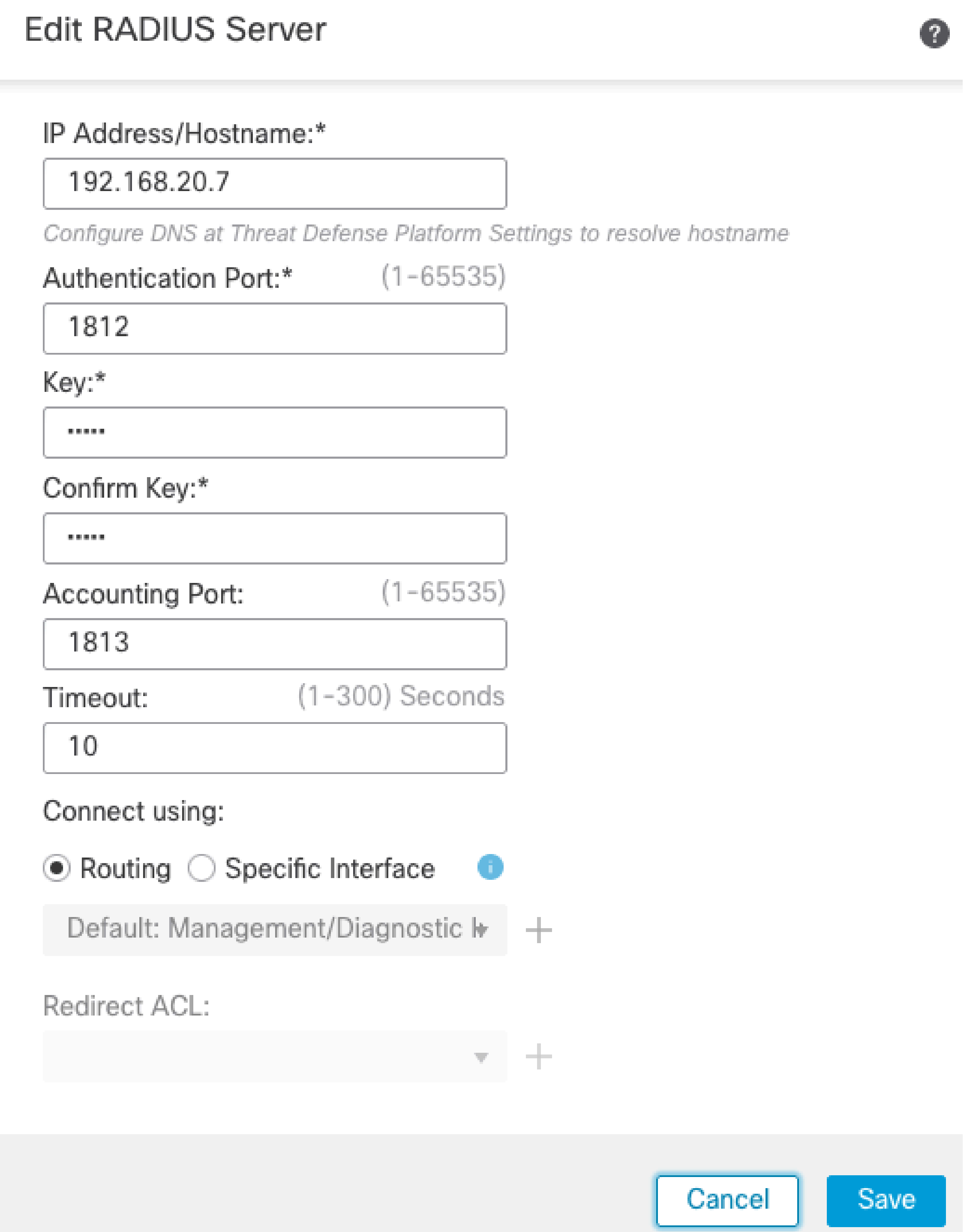
- 之后，点击信任点名称旁边的 🔄 图标，然后 Yes，然后将CSR复制到CA并签名。 证书的属性必须与HTTPS服务器的普通属性相同。
- 从CA收到base64格式的证书后，从磁盘中选择该证书，然后单击 Import.当此操作成功时，您会看到：



| Name | Domain | Enrollment Type | Status |
|---|---|---|---|
| FTD | | | |
| vpntestbed.cisco.com | Global | Self-Signed | CA ID |

## b)配置RADIUS服务器

- 转到 **Objects > Object Management > RADIUS Server Group > Add RADIUS Server Grou**p**.**
- 填写名称并添加IP地址和共享密钥，单击 Save:



Edit RADIUS Server

IP Address/Hostname:* 192.168.20.7

*Configure DNS at Threat Defense Platform Settings to resolve hostname*

Authentication Port:* (1-65535) 1812

Key:* •••••

Confirm Key:* •••••

Accounting Port: (1-65535) 1813

Timeout: (1-300) Seconds 10

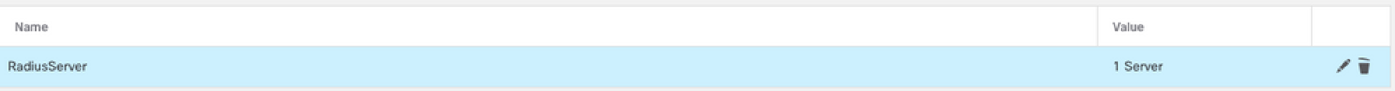
Connect using:

● Routing ○ Specific Interface

Default: Management/Diagnostic I

Redirect ACL:

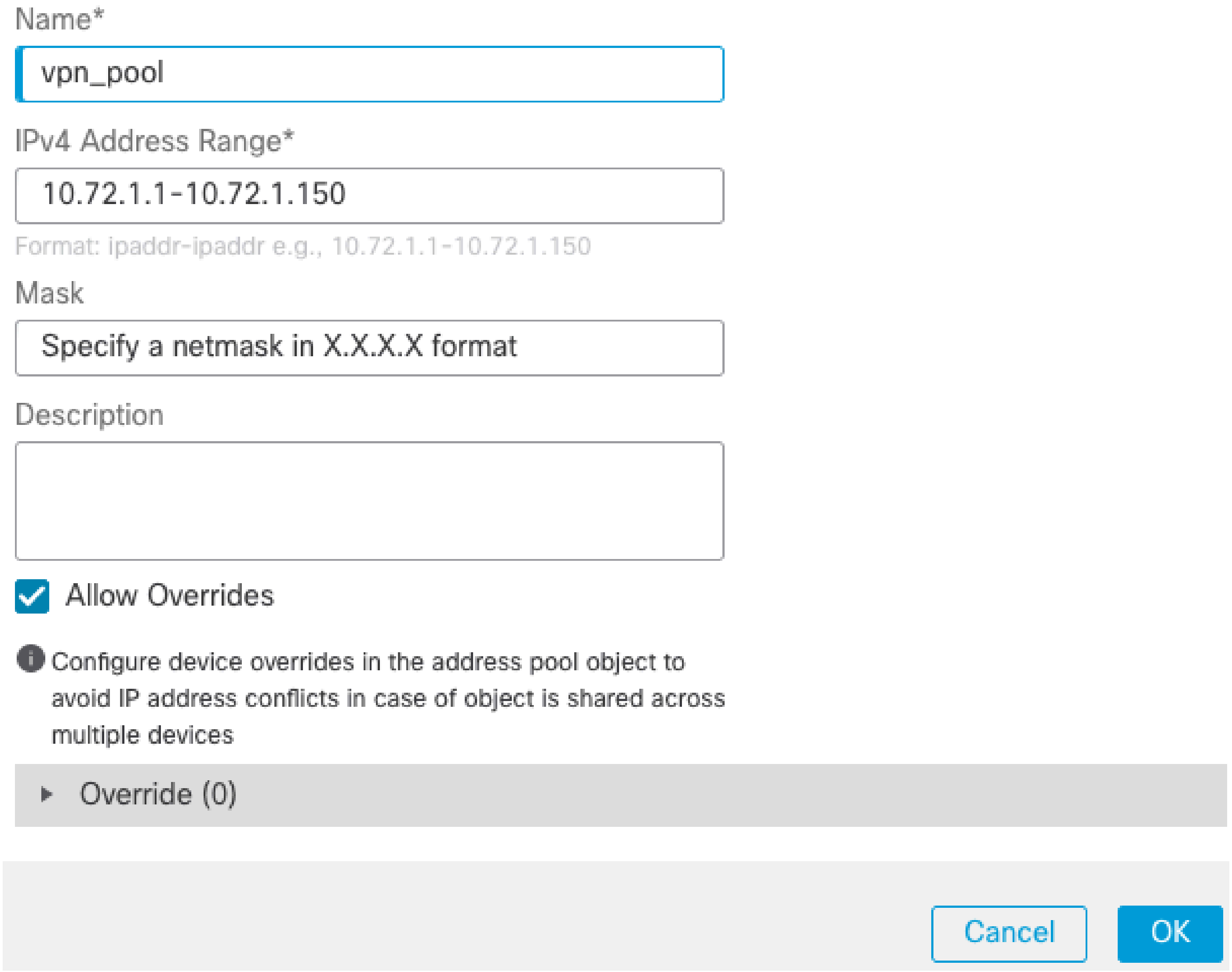
- 之后，您会看到列表中的服务器：



| Name | Value |
|---|---|
| RadiusServer | 1 Server |

### c)为VPN用户创建地址池

- 转到 **Objects > Object Management > Address Pools > Add IPv4 Pools**.
- 输入名称和范围，不需要掩码：



Name*

vpn_pool

IPv4 Address Range*

10.72.1.1-10.72.1.150

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask

Specify a netmask in X.X.X.X format

Description

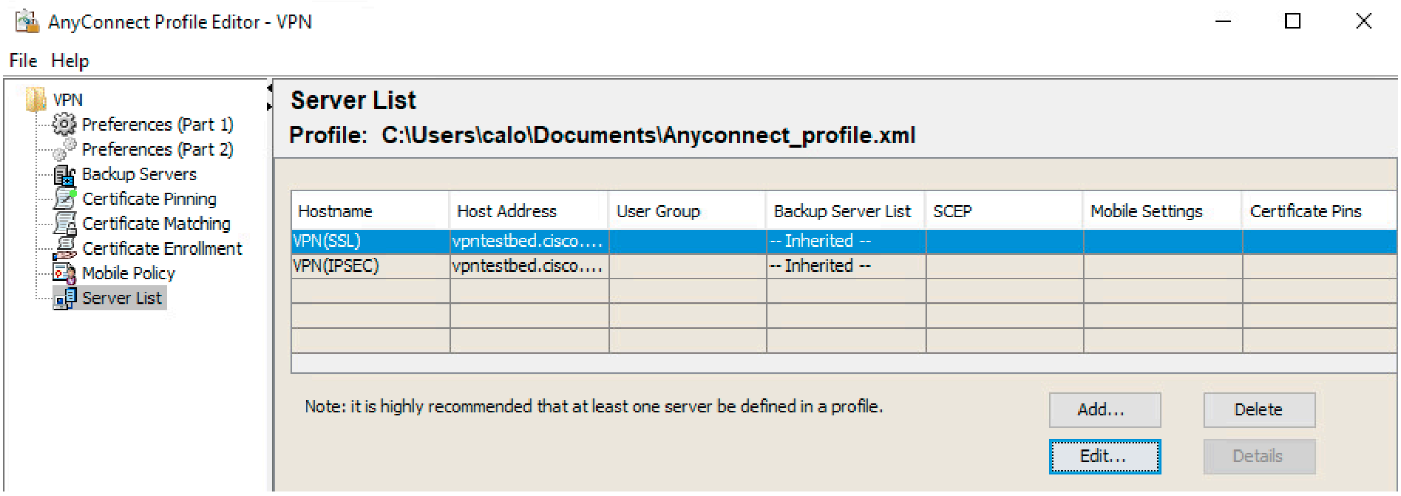
☑ Allow Overrides

Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

▸ Override (0)

## d)创建XML配置文件

- 从思科站点下载配置文件编辑器并打开它。
- 转到 Server List > Add...
- 放置显示名称和FQDN。您会看到服务器列表中的条目：



**Server List**

**Profile: C:\Users\calo\Documents\Anyconnect_profile.xml**

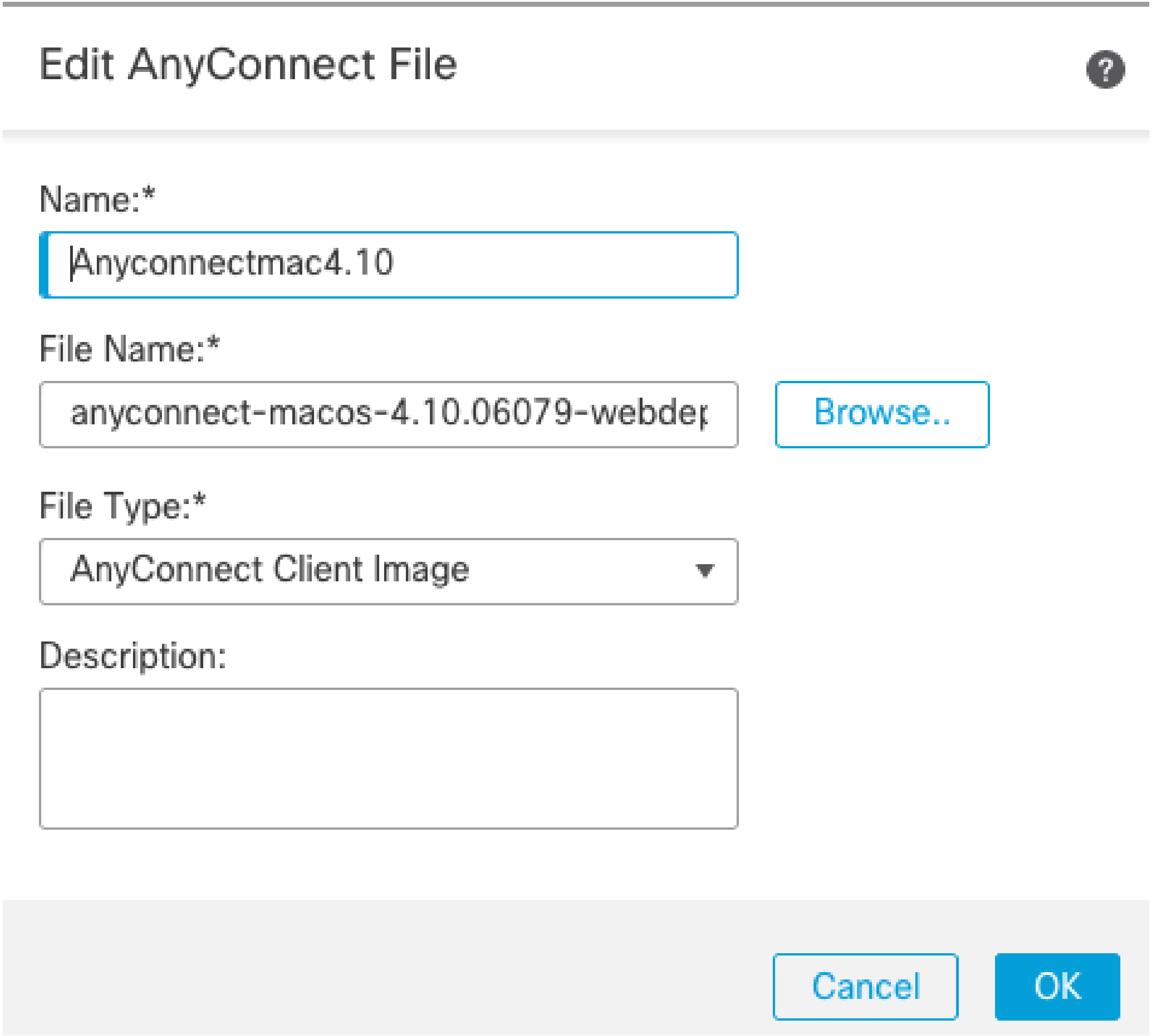
| Hostname | Host Address | User Group | Backup Server List | SCEP | Mobile Settings | Certificate Pins |
|---|---|---|---|---|---|---|
| VPN(SSL) | vpntestbed.cisco.... |  | -- Inherited -- |  |  |  |
| VPN(IPSEC) | vpntestbed.cisco.... |  | -- Inherited -- |  |  |  |

Note: it is highly recommended that at least one server be defined in a profile.

- 点击 OK和 **File** > **Save as...**

### e)上传AnyConnect映像

- 从思科站点下载软件包映像。
- 转到 Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.
- 键入名称并从磁盘中选择PKG文件，单击 Save:



Edit AnyConnect File

Name:* Anyconnectmac4.10

File Name:* anyconnect-macos-4.10.06079-webdep

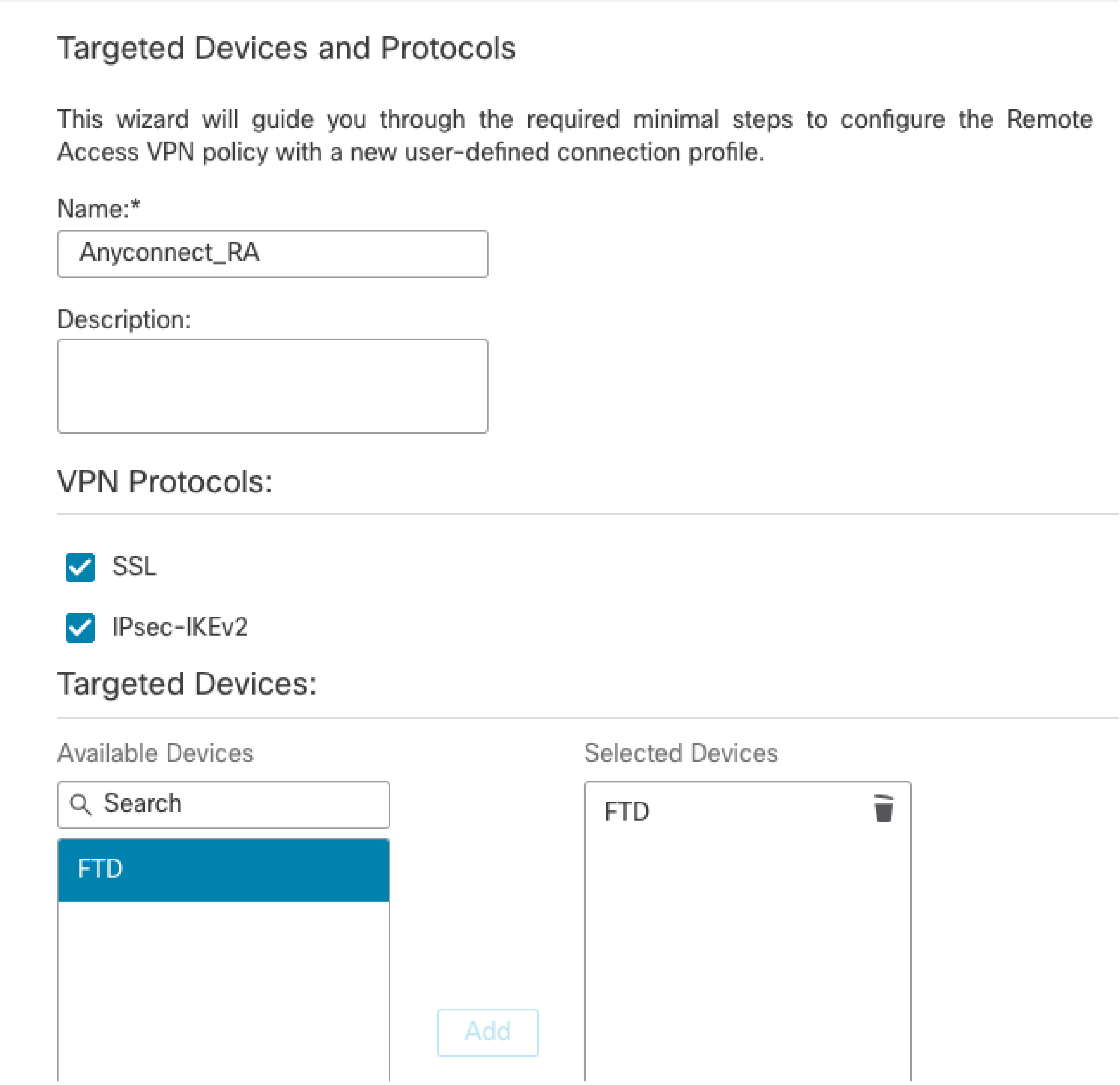
File Type:* AnyConnect Client Image

Description:

- 根据您自己的要求添加更多软件包。

## 2.远程访问向导

- 转到 Devices > VPN > Remote Access > Add a new configuration.
- 命名配置文件并选择FTD设备：



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:*

Anyconnect_RA

Description:

VPN Protocols:

☑ SSL

☑ IPsec-IKEv2

Targeted Devices:

Available Devices

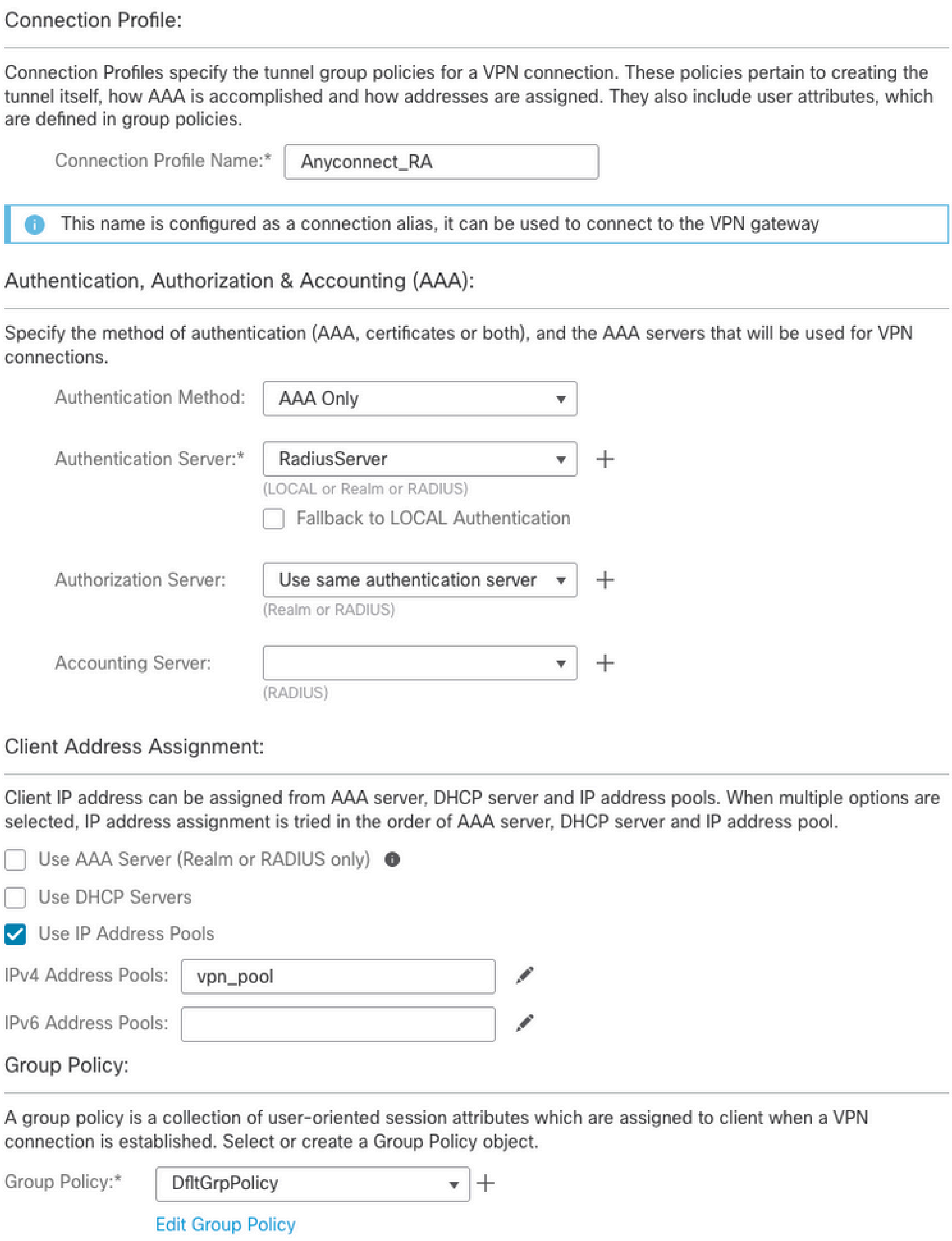
Search

FTD

Selected Devices

FTD

- 在连接配置文件步骤中，键入 **Connection Profile Name**，选择 **Authentication Server** 和 Address Pools 您之前创建的内容：



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:* Anyconnect_RA

ⓘ 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:* RadiusServer ▾ +
(LOCAL or Realm or RADIUS)
□ Fallback to LOCAL Authentication

Authorization Server: Use same authentication server ▾ +
(Realm or RADIUS)

Accounting Server: ▾ +
(RADIUS)

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

□ Use AAA Server (Realm or RADIUS only) ⓘ

□ Use DHCP Servers

☑ Use IP Address Pools

IPv4 Address Pools: vpn_pool

IPv6 Address Pools:

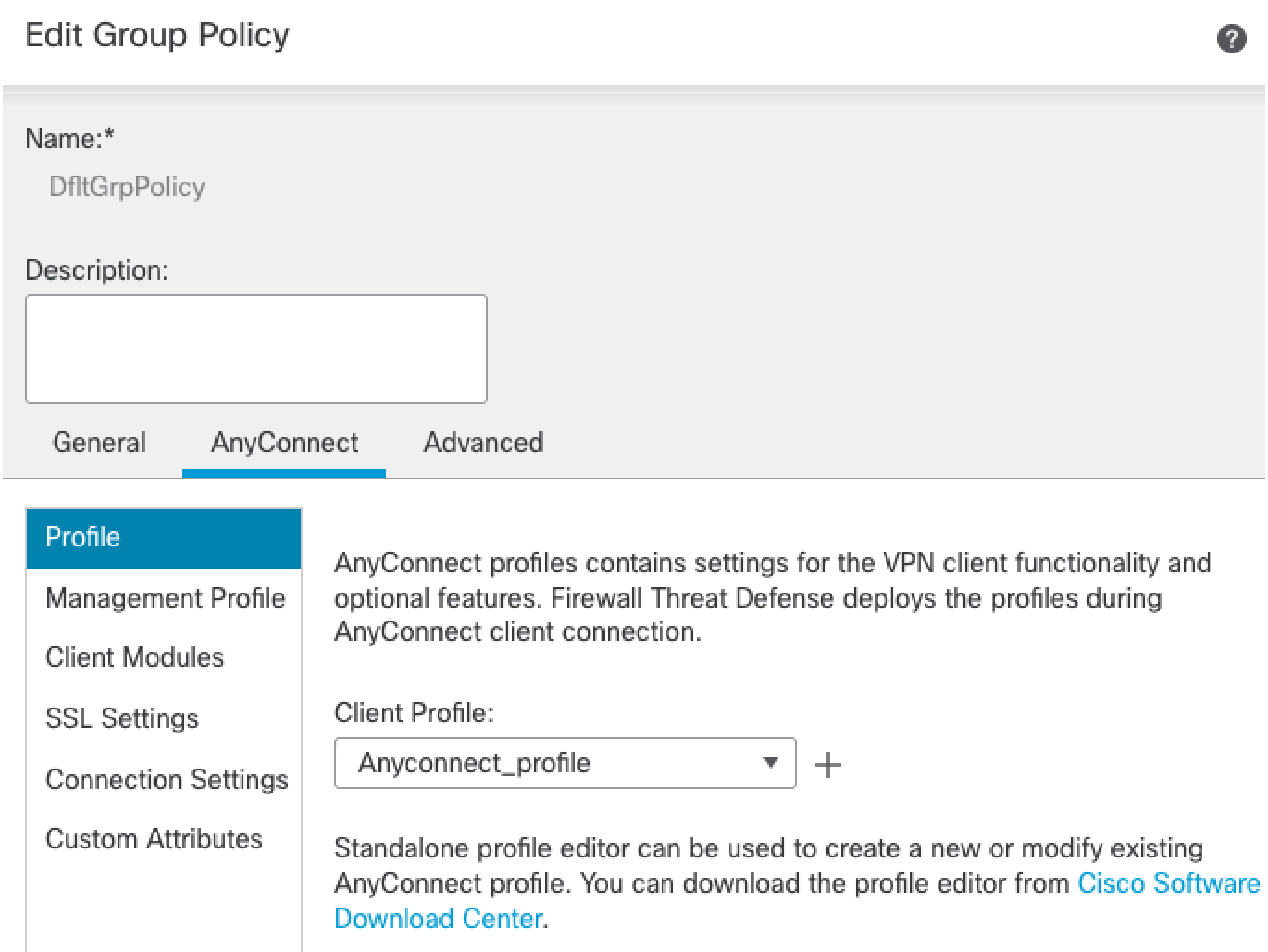
Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:* DfltGrpPolicy ▾ +

Edit Group Policy

- 点击 **Edit Group Policy** 在AnyConnect选项卡上，选择 Client Profile，然后单击 Save:



Edit Group Policy

Name:*

DfltGrpPolicy

Description:

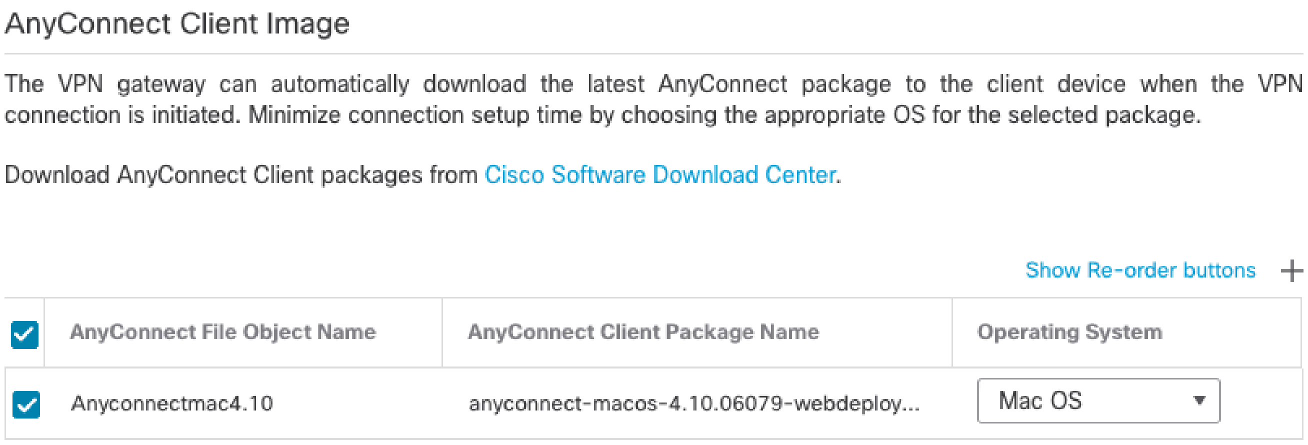
AnyConnect profiles contains settings for the VPN client functionality and optional features. Firewall Threat Defense deploys the profiles during AnyConnect client connection.

Client Profile:

Anyconnect_profile ▾ +

Standalone profile editor can be used to create a new or modify existing AnyConnect profile. You can download the profile editor from Cisco Software Download Center.

- 在下一页上，选择AnyConnect映像，然后单击 Next.



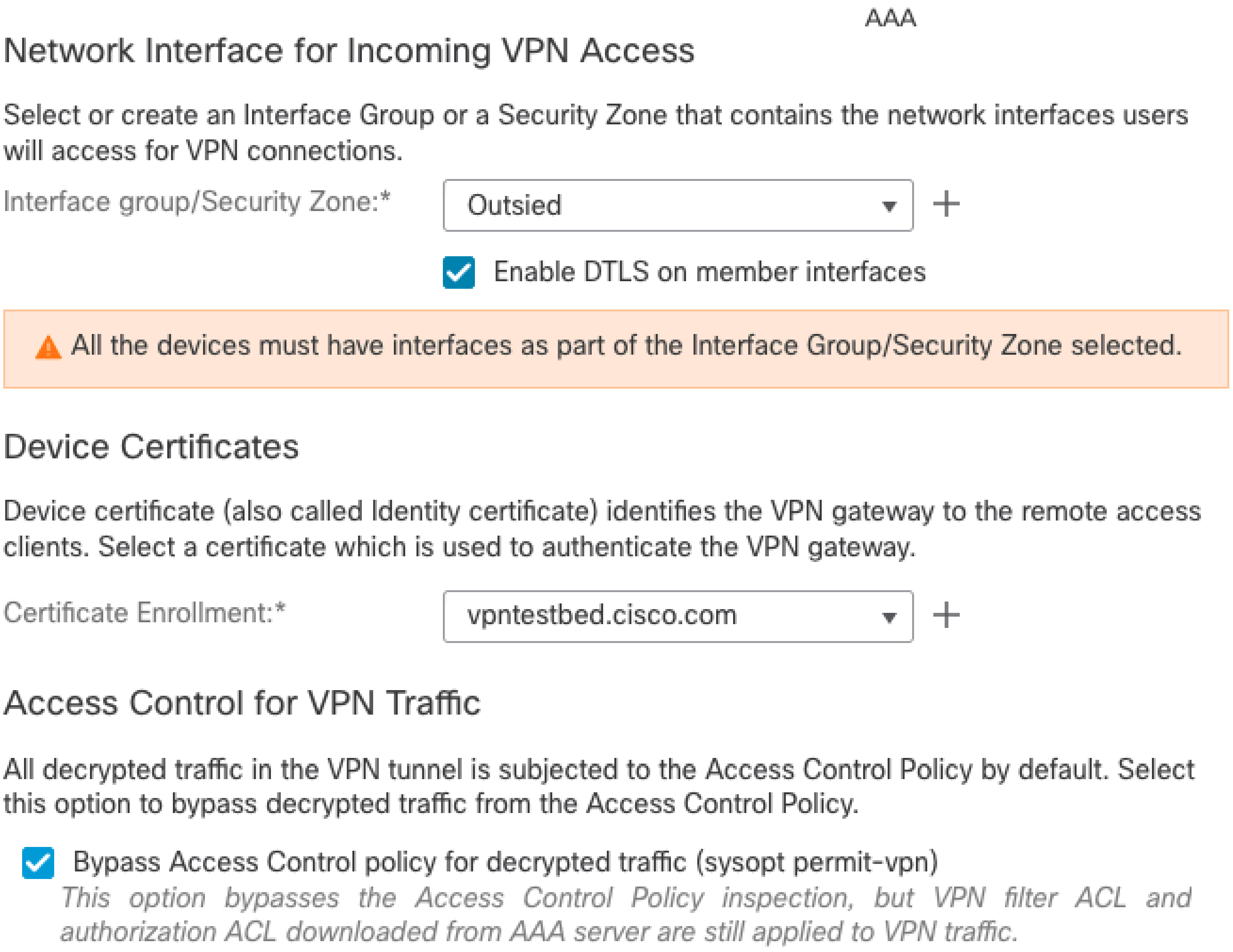
AnyConnect Client Image

The VPN gateway can automatically download the latest AnyConnect 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 AnyConnect Client packages from Cisco Software Download Center.

| ☑ | AnyConnect File Object Name | AnyConnect Client Package Name | Operating System |
|---|---|---|---|
| ☑ | Anyconnectmac4.10 | anyconnect-macos-4.10.06079-webdeploy... | Mac OS ▾ |

- 在下一个屏幕上，选择 **Network Interface and Device Certificates**:



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:* Outsied ▾ +

☑ 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:* vpntestbed.cisco.com ▾ +

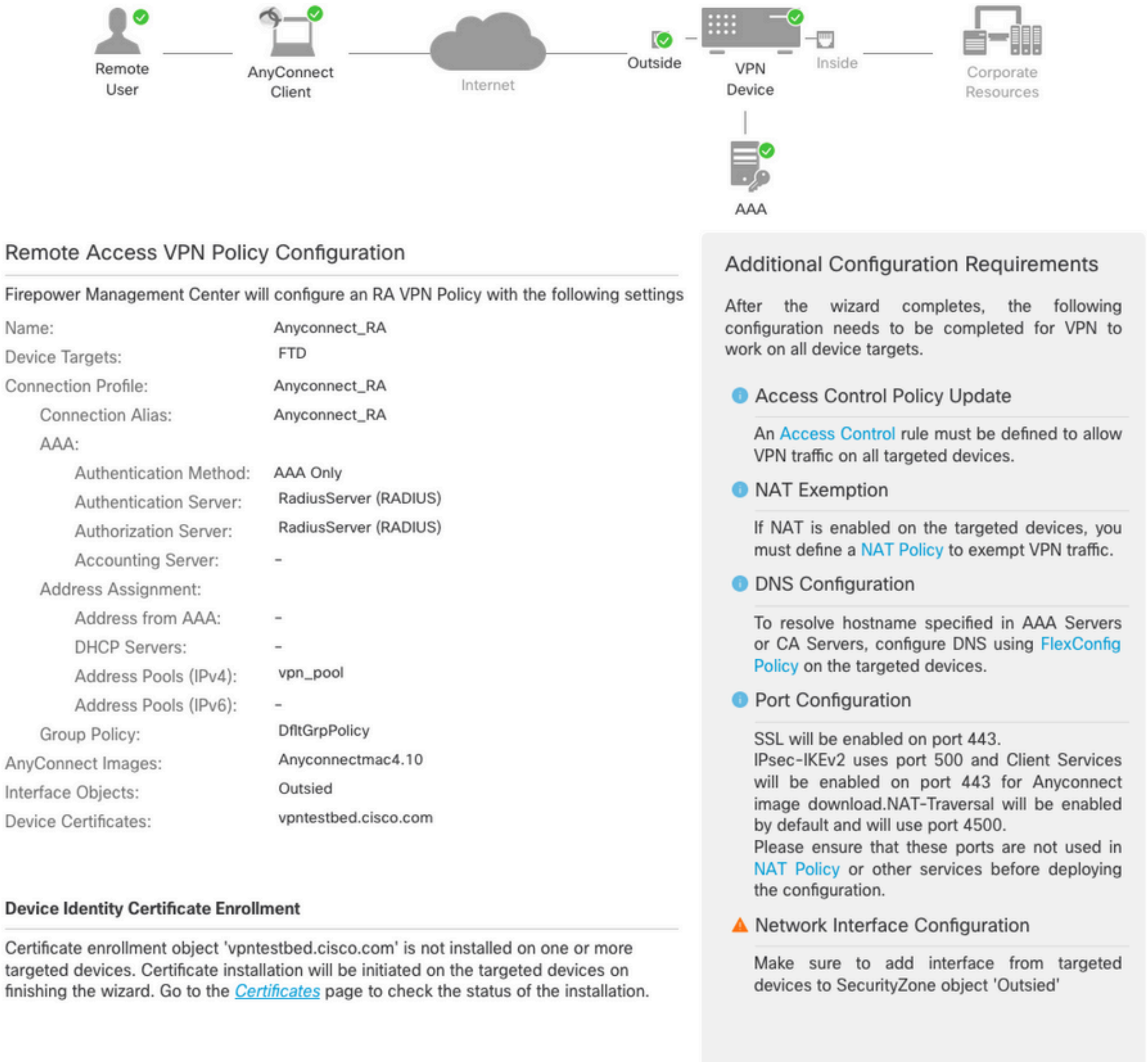
Access Control for VPN Traffic

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.*

- 当所有配置都正确时，您可以单击 Finish 然后 Deploy:



Remote Access VPN Policy Configuration

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

| | |
|---|---|
| Name: | Anyconnect_RA |
| Device Targets: | FTD |
| Connection Profile: | Anyconnect_RA |
| Connection Alias: | Anyconnect_RA |
| AAA: | |
| Authentication Method: | AAA Only |
| Authentication Server: | RadiusServer (RADIUS) |
| Authorization Server: | RadiusServer (RADIUS) |
| Accounting Server: | - |
| Address Assignment: | |
| Address from AAA: | - |
| DHCP Servers: | - |
| Address Pools (IPv4): | vpn_pool |
| Address Pools (IPv6): | - |
| Group Policy: | DfltGrpPolicy |
| AnyConnect Images: | Anyconnectmac4.10 |
| Interface Objects: | Outsied |
| Device Certificates: | vpntestbed.cisco.com |

**Device Identity Certificate Enrollment**

Certificate enrollment object 'vpntestbed.cisco.com' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the *Certificates* page to check the status of the installation.

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 Anyconnect image download.NAT-Traversal will be enabled by default and will use port 4500.
Please ensure that these ports are not used in NAT Policy or other services before deploying the configuration.

Network Interface Configuration

Make sure to add interface from targeted devices to SecurityZone object 'Outsied'

- 这会将整个配置、证书和AnyConnect软件包复制到FTD设备。

# 连接

要连接到FTD，您需要打开浏览器，键入指向外部接口的DNS名称或IP地址。然后使用存储在RADIUS服务器中的凭证登录，并在屏幕上执行说明。 安装AnyConnect后，您需要在AnyConnect窗口中放置相同的地址，然后单击 Connect.

# 限制

当前在FTD上不受支持，但在ASA上可用：

- Firepower Threat Defense 6.2.3或更早版本不支持RADIUS服务器中的接口选择。在部署期间将忽略接口选项。
- 启用动态授权的RADIUS服务器需要Firepower威胁防御6.3或更高版本才能运行动态授权。
- FTDposture VPN不支持通过动态授权或RADIUS授权更改(CoA)进行组策略更改。
- AnyConnect自定义(增强功能：Cisco bug ID CSCvq87631)
- AnyConnect脚本
- AnyConnect本地化

- WSA集成
- RA和L2L VPN同步IKEv2动态加密映射(增强功能：Cisco Bug ID CSCvr52047)
- AnyConnect模块（NAM、Hostscan、AMP Enabler、SBL、Umbrella、网络安全等）— 默认情况下安装DART(AMP Enabler和Umbrella的增强功能：Cisco bug ID CSCvs03562和Cisco bug ID CSCvs0642)。
- TACACS、Kerberos（KCD身份验证和RSA SDI）
- 浏览器代理

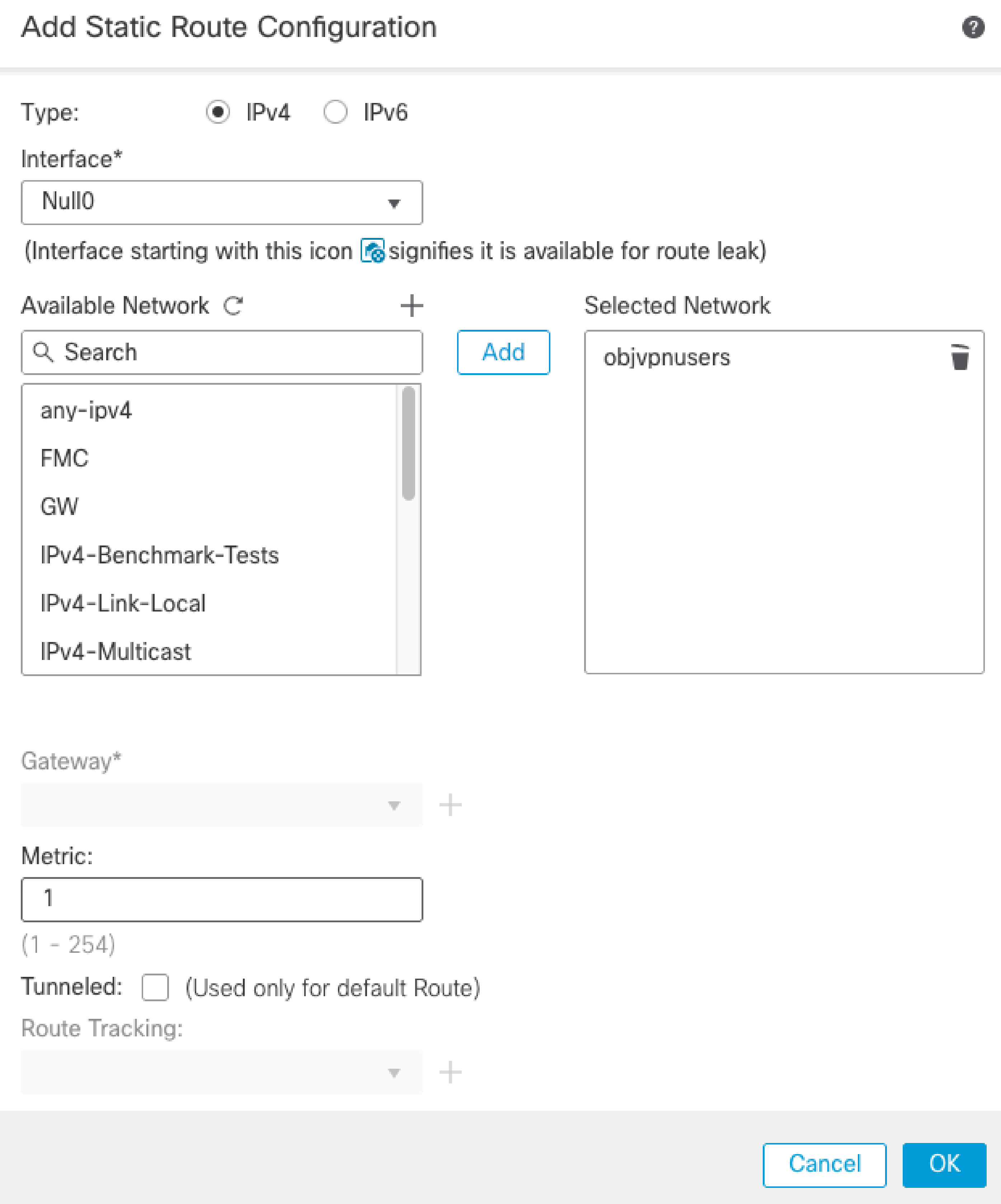
# 安全考虑

默认情况下， sysopt connection permit-vpn选项处于禁用状态。这意味着您需要允许来自外部接口上的地址池的流量通过访问控制策略。虽然添加预过滤器或访问控制规则以仅允许VPN流量，但如果明文流量与规则条件匹配，则会错误地允许该流量。

有两种方法可以解决此问题。首先，TAC推荐的选项是为外部接口启用反欺骗（在ASA上称为单播反向路径转发 — uRPF），其次，启用 sysopt connection permit-vpn 完全绕过Snort检测。第一个选项允许对进出VPN用户的流量进行正常检查。

### a)启用uRPF

- 为用于远程访问用户的网络创建空路由（在C部分中定义）。转到 Devices > Device Management > Edit > Routing > Static Route 并选择 Add route



Add Static Route Configuration

Type: ● IPv4 ○ IPv6

Interface*

Null0

(Interface starting with this icon signifies it is available for route leak)

Available Network

Selected Network

objvpnusers

Gateway*

Metric:

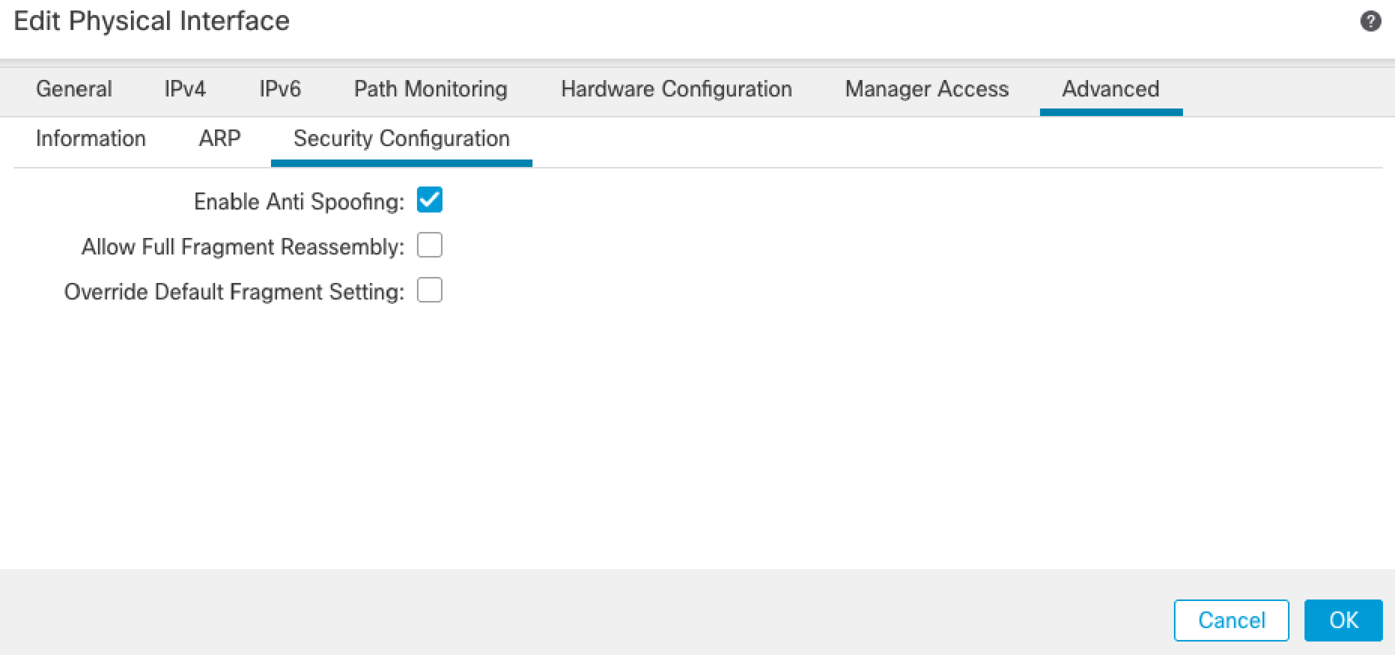
1

(1 - 254)

Tunneled: □ (Used only for default Route)

Route Tracking:

- 接下来，在VPN连接终止的接口上启用uRPF。要查找此内容，请导航至 **Devices > Device Management > Edit > Interfaces > Edit > Advanced > Security Configuration > Enable Anti Spoofing**.



Edit Physical Interface

Enable Anti Spoofing: ☑

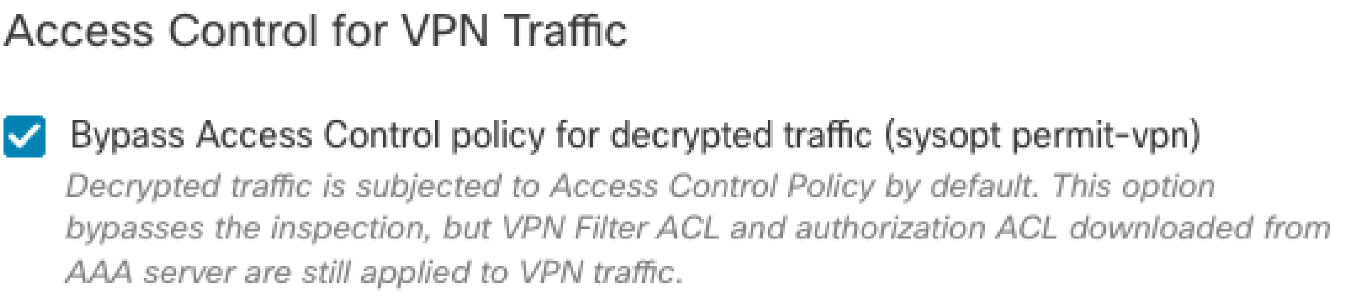
Allow Full Fragment Reassembly: □

Override Default Fragment Setting: □

当用户连接时，路由表中会为该用户安装32位路由。清除来自池中其他未使用IP地址的文本流量会被uRFP丢弃。要查看的描述，请执行以下操作： **Anti-Spoofing**请参阅[在Firepower威胁防御上设置安全配置参数。](#)

**b)启用 Sysopt connection permit-vpn 选项**

- 如果您有版本6.2.3或更高版本，则可以选择使用向导或在其下执行该操作 Devices > VPN > Remote Access > VPN Profile > Access Interfaces.

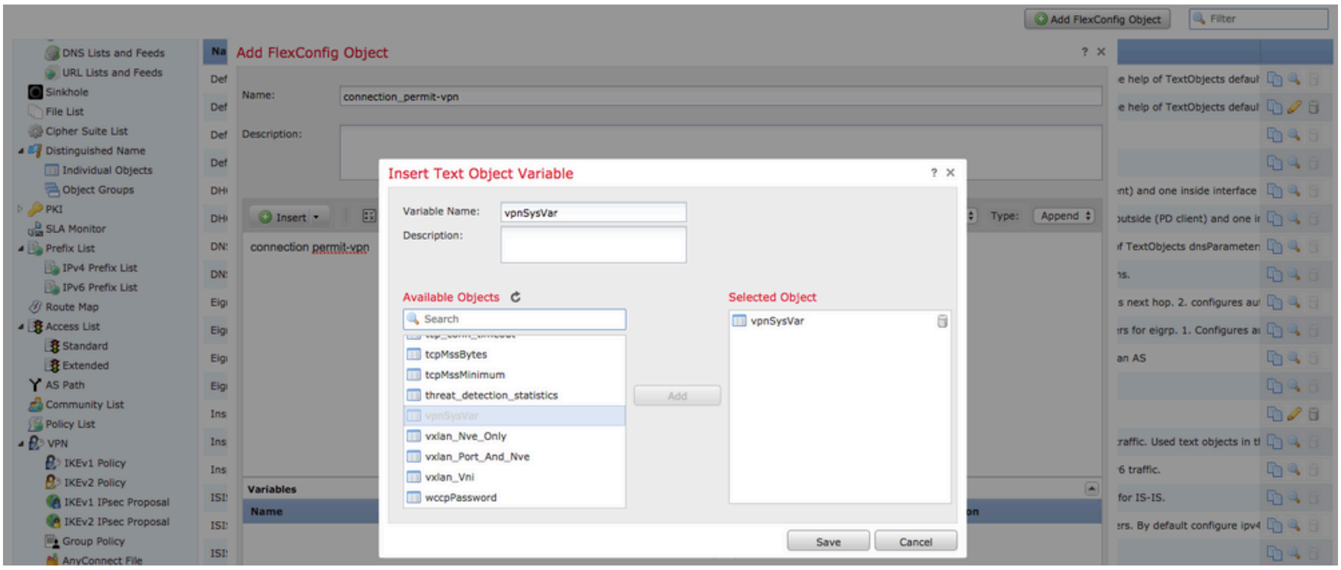


Access Control for VPN Traffic

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

*Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.*

- 对于6.2.3之前的版本，请转到 Objects > Object Management > FlexConfig > Text Object > Add Text Object.
- 创建文本对象变量，例如：vpnSysVar具有值的单个条目 sysopt.
- 转到 Objects**> Object Management > FlexConfig > FlexConfig Object > Add FlexConfig Object.**
- 创建 FlexConfig 使用CLI的对象  connection permit-vpn.
- 将文本对象变量插入 FlexConfig CLI上的对象 **$vpnSysVar connection permit-vpn**. 点击 Save:



Add FlexConfig Object

Name: connection_permit-vpn

Description:

Insert Text Object Variable

Variable Name: vpnSysVar

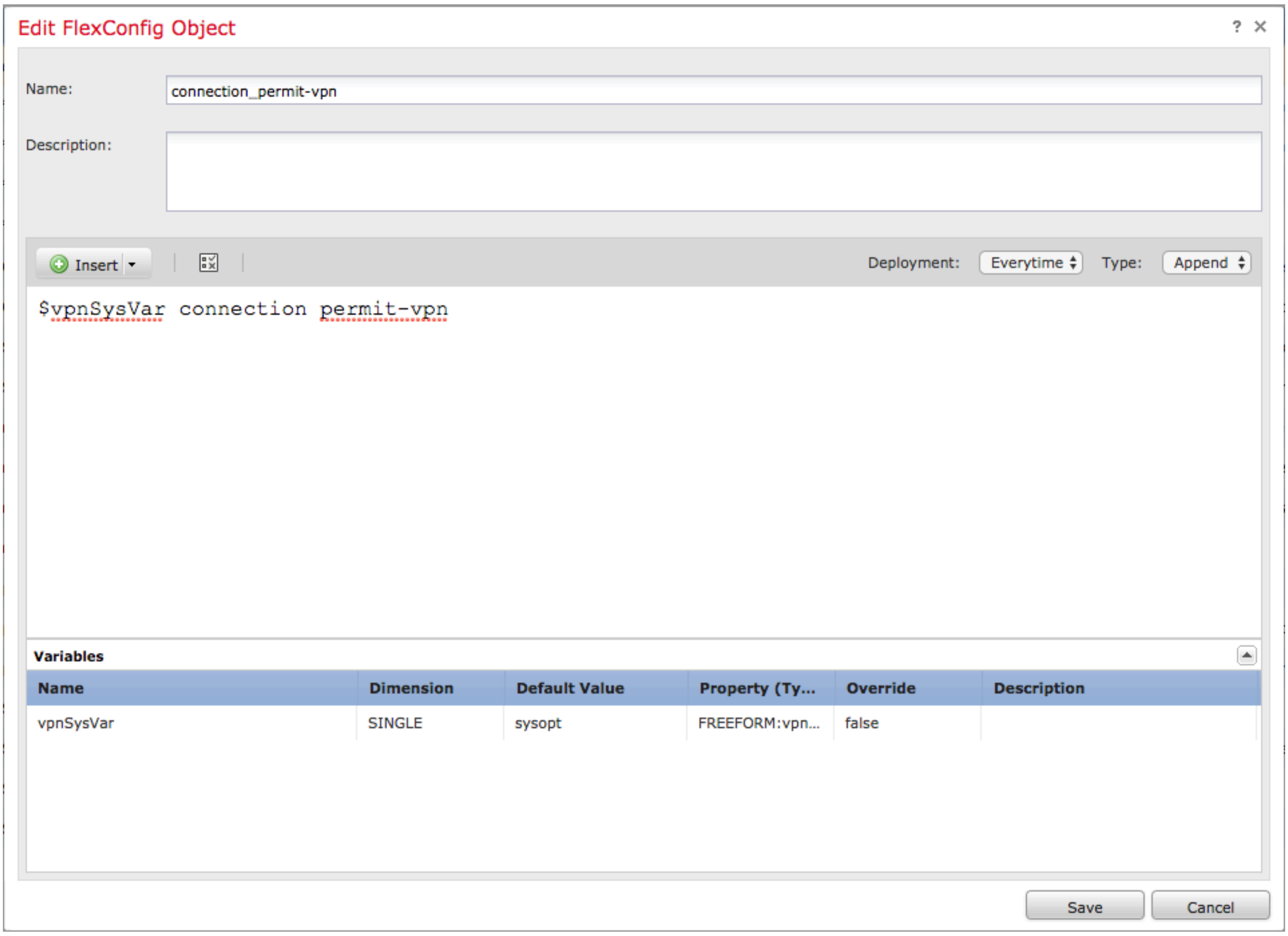
Description:

Available Objects

Selected Object

vpnSysVar

- 对此行 FlexConfig对象为 **Append** 并选择部署到 Everytime:



Edit FlexConfig Object

Name: connection_permit-vpn

Description:

Deployment: Everytime　Type: Append

```
$vpnSysVar connection permit-vpn
```

Variables

| Name | Dimension | Default Value | Property (Ty... | Override | Description |
|---|---|---|---|---|---|
| vpnSysVar | SINGLE | sysopt | FREEFORM:vpn... | false | |

- 转到**Devices > FlexConfig** 并编辑当前策略或创建新策略 New Policy 按钮。
- 仅添加已创建的 FlexConfig，单击 Save.
- 部署配置以调配**sysopt connection permit-vpn**命令。

但是，在此之后，您不能使用访问控制策略来检查来自用户的流量。您仍然可以使用VPN过滤器或可下载ACL来过滤用户流量。

如果您看到来自VPN用户的Snort数据包被丢弃，请联系TAC并参考Cisco Bug ID CSCvg91399。

# 相关信息

- **思科技术支持和下载**

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。