

在FTD上配置AnyConnect VPN客户端：发夹和NAT免除

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[步骤1:导入SSL证书](#)

[第二步：配置RADIUS服务器](#)

[第三步：创建IP池](#)

[第四步：创建XML配置文件](#)

[第五步：上传Anyconnect XML配置文件](#)

[第六步：上传AnyConnect映像](#)

[步骤 7.远程访问VPN向导](#)

[NAT免除和发夹](#)

[步骤1:NAT免除配置](#)

[第二步：发夹配置](#)

[验证](#)

[故障排除](#)

简介

本文档介绍如何在FMC管理的Firepower威胁防御(FTD)v6.3上配置思科远程访问VPN解决方案(AnyConnect)。

先决条件

要求

Cisco 建议您了解以下主题：

- 基本的远程访问VPN、安全套接字层(SSL)和互联网密钥交换版本2(IKEv2)知识
- 基本身份验证、授权和记帐(AAA)以及RADIUS知识
- 基本的FMC知识
- 基本的FTD知识

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FMC 6.4
- 思科FTD 6.3
- AnyConnect 4.7

本文档介绍在Firepower威胁防御(FTD)版本6.3(由Firepower管理中心(FMC)管理)上配置思科远程访问VPN解决方案(AnyConnect)的过程。

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

本文档旨在介绍FTD设备上的配置。如果您寻找ASA配置示例，请参阅文档

：<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/100918-asa-sslvpn-00.html>

限制:

目前，这些功能在FTD上不受支持，但在ASA设备上仍然可用：

- 双AAA身份验证(在FTD 6.5版上可用)
- 动态访问策略
- 主机扫描
- ISE终端安全评估
- RADIUS CoA
- VPN负载均衡器
- 本地身份验证(在Firepower设备管理器6.3上可用。Cisco Bug ID [CSCvf92680](#))
- LDAP属性映射(通过FlexConfig提供，思科漏洞ID [CSCvd64585](#))
- AnyConnect自定义
- AnyConnect脚本
- AnyConnect本地化
- 每应用VPN
- SCEP代理
- WSA集成
- SAML SSO(思科漏洞ID [CSCvq90789](#))
- RA和L2L VPN的同步IKEv2动态加密映射
- AnyConnect模块(NAM、Hostscan、AMP Enabler、SBL、Umbrella、网络安全等)。DART是此版本中默认安装的唯一模块。
- TACACS、Kerberos(KCD身份验证和RSA SDI)
- 浏览器代理

配置

要通过FMC中的远程访问VPN向导，必须完成以下步骤：

步骤1:导入SSL证书

配置AnyConnect时，证书至关重要。SSL和IPSec仅支持基于RSA的证书。

IPSec支持椭圆曲线数字签名算法(ECDSA)证书，但是，当使用基于ECDSA的证书时，无法部署新的AnyConnect软件包或XML配置文件。

它可用于IPSec，但您必须预部署AnyConnect软件包和XML配置文件，所有XML配置文件更新必须在每个客户端上手动推送(Cisco bug ID [CSCtx42595](#))。

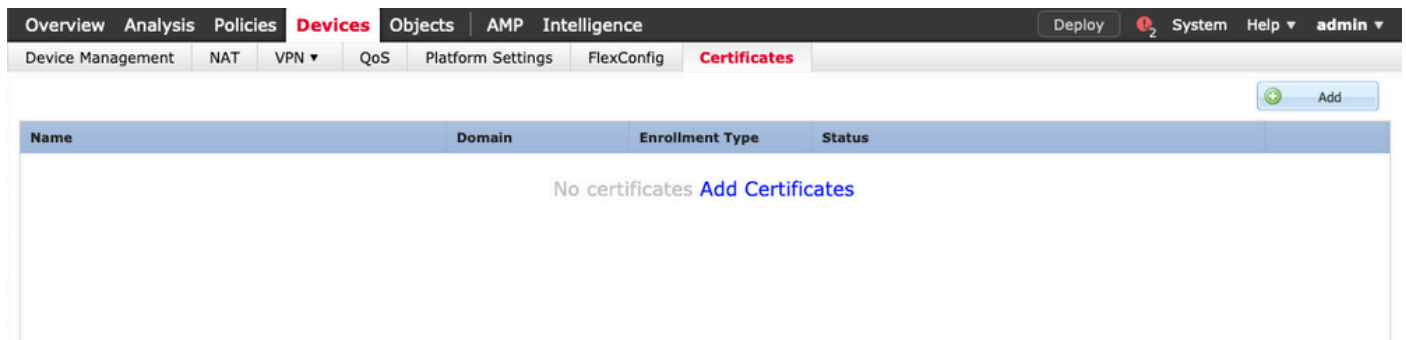
此外，证书必须包含带有DNS名称和/或IP地址的公用名(CN)扩展，以避免Web浏览器中出现“不受信任的服务器证书”错误。

注意：在FTD设备上，生成证书签名请求(CSR)之前需要证书颁发机构(CA)证书。

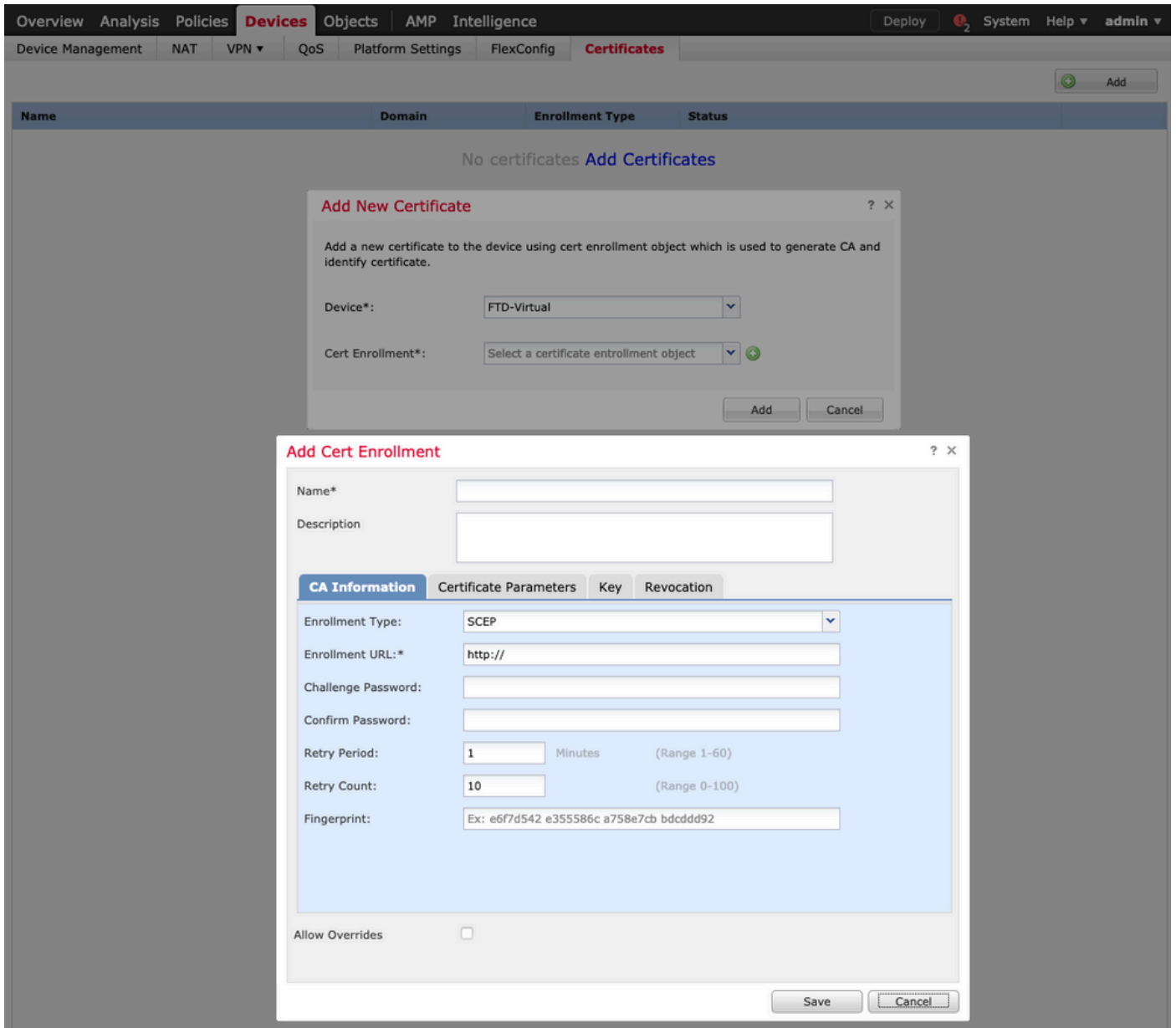
- 如果在外部服务器（例如Windows Server或OpenSSL）中生成CSR，manual enrollment method将会失败，因为FTD不支持手动密钥注册。
- 必须使用其他方法，例如PKCS12。

为了使用手动注册方法获取FTD设备的证书，需要生成CSR，使用CA对其进行签名，然后导入身份证书。

1.导航到设备>证书，然后选择添加，如图所示。



2.选择Device并添加新的Cert Enrollment对象，如图所示。



3.选择手动注册类型并粘贴CA证书（用于签署CSR的证书）。

Add Cert Enrollment



Name*

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type:

CA Certificate:*

```
/3C4hi07uzuR0ygwKEBaMdg4Dl/z
4x3nk3tTUhYpmbiWqWAXM7GNDRVWG9BZ1svk3shDK2Bogklzou6
RqV66Gj9IE7Z2
xIVrSrJFqhkrT795kMb8am8xhb4eXYXxUgJmODIPqZ76RSTAT0+v1
VLSP+vHGm8X
g6wEFsKuZay27a48e/lJG2LgRDraOKt+jwbS7DGSK4mfZsZqhFdQP
LhBNFbyBvb9
dOjUkmdSvzQDRSqSo+HINEm3E8/q20wrtIZp04MpAabyhr+hEpeP
VMrhvBOT8h
H8eMjSQjGhhHbuKofVlzQmM0RvGnTB6EKYIvb4CUW8HcgDdDr
mwNgy5mTP9cHa
9Or3RlWRzEa11HE3mHC4Rj6DOnmgufjx+TZRYczownSKLL7LcW1
Dl8ZclYmfaldC
W2cZuBR0yVdxcVq4#04ISE1BfOWF5d5rAD/bvk2n6xrJI1SLqABMJJ
uslu9KTGH1
bVKEYACKVvETw==
-----END CERTIFICATE-----
```

Allow Overrides

4. 选择Certificate Parameters选项卡，然后为Include FQDN字段选择“自定义FQDN”，并填写图像中所示的证书详细信息。

Add Cert Enrollment ? X

Name*

Description

CA Information **Certificate Parameters** Key Revocation

Include FQDN:

Include Device's IP Address:

Common Name (CN):

Organization Unit (OU):

Organization (O):

Locality (L):

State (ST):

Country Code (C):

Email (E):

Include Device's Serial Number

Allow Overrides

5.选择键选项卡，然后选择键类型，您可以选择名称和大小。对于RSA，最低要求为2048字节。

6.选择“保存”，确认设备，然后在证书注册下，选择刚创建的信任点，选择添加以部署证书。

Add New Certificate



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

Device*:

Cert Enrollment*:

Cert Enrollment Details:

Name: Anyconnect-certificate

Enrollment Type: Manual

SCEP URL: NA

Add

Cancel

7.在状态列中，选择ID图标，然后选择是以生成CSR，如图所示。

The screenshot shows the Cisco FTD GUI with the 'Certificates' tab selected. The table below shows the certificate configuration:

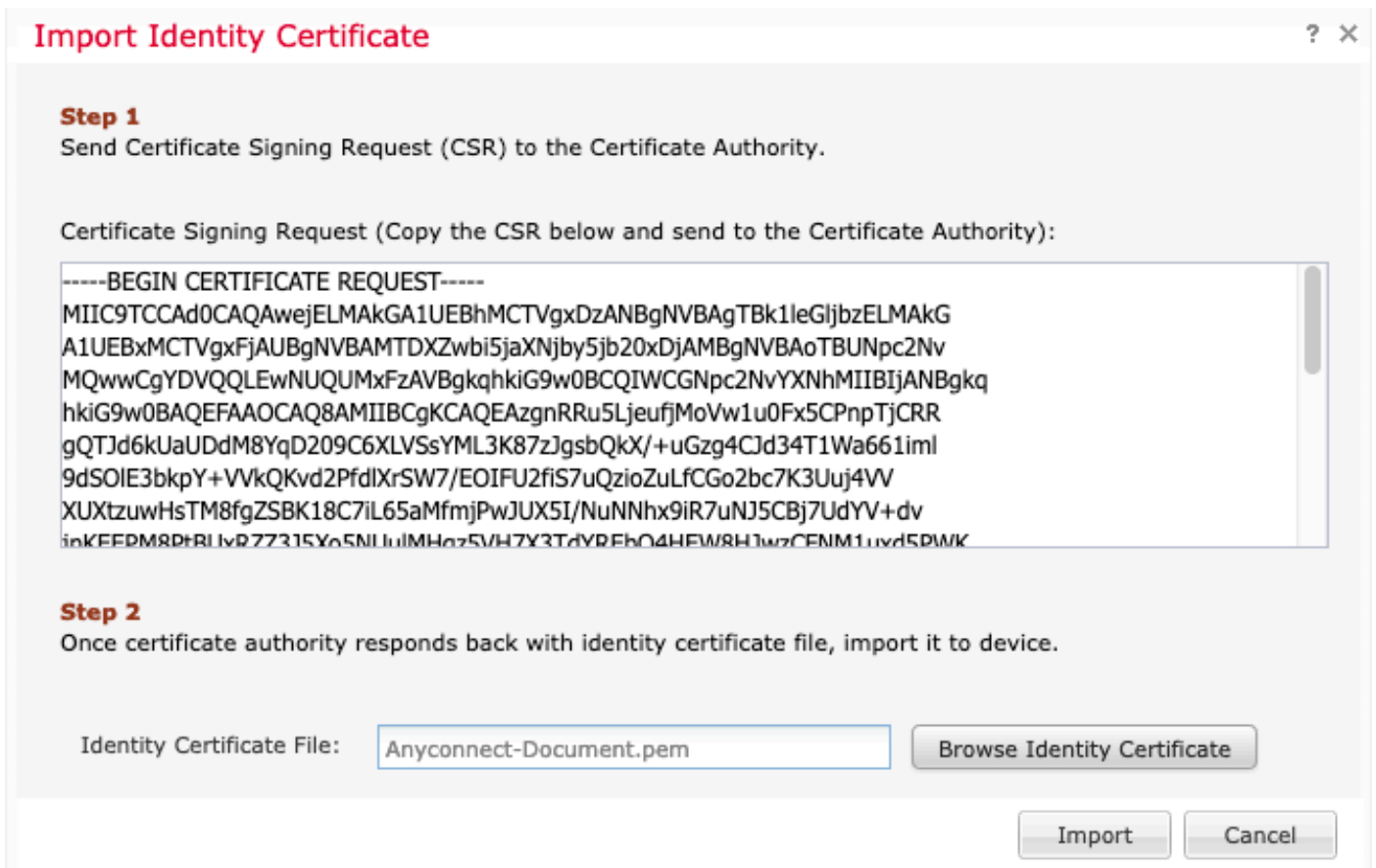
Name	Domain	Enrollment Type	Status
Anyconnect-certificate	Global	Manual	CA ID Identity certificate import required

A warning dialog box is displayed over the table, asking for confirmation to generate a CSR.

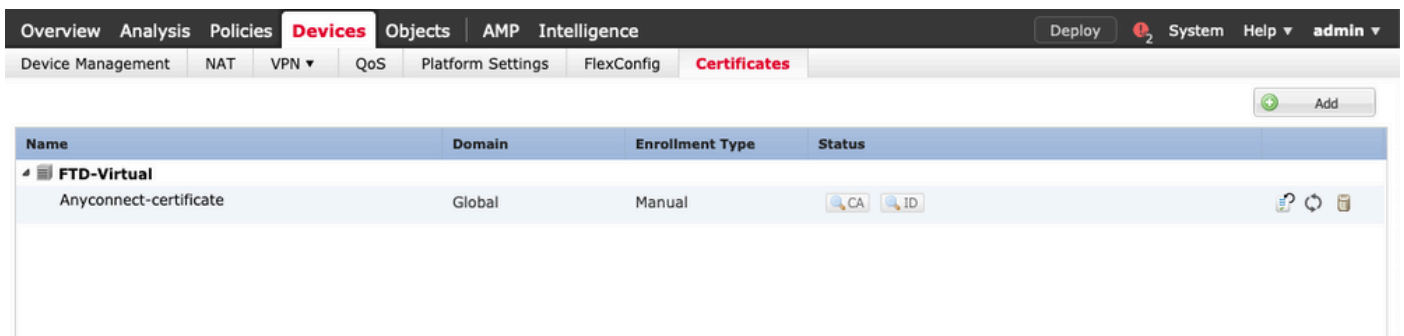
Warning
This operation will generate Certificate Signing Request do you want to continue?
Yes No

8.复制CSR并用您首选的CA（例如GoDaddy或DigiCert）签名。

9.从CA收到身份证书（必须采用base64格式）后，选择Browse Identity Certificate，然后在本地计算机上查找证书。选择导入。



10. 导入后，CA和ID证书详细信息将可供显示。



第二步：配置RADIUS服务器

在FMC管理的FTD设备上，不支持本地用户数据库，必须使用其他身份验证方法，例如RADIUS或LDAP。

1. 导航到对象 > 对象管理 > RADIUS服务器组 > 添加RADIUS服务器组，如图所示。

Add RADIUS Server Group



Name:*

Description:

Group Accounting Mode: ▼

Retry Interval:* (1-10) Seconds

Realms: ▼

Enable authorize only

Enable interim account update

Interval:* (1-120) hours

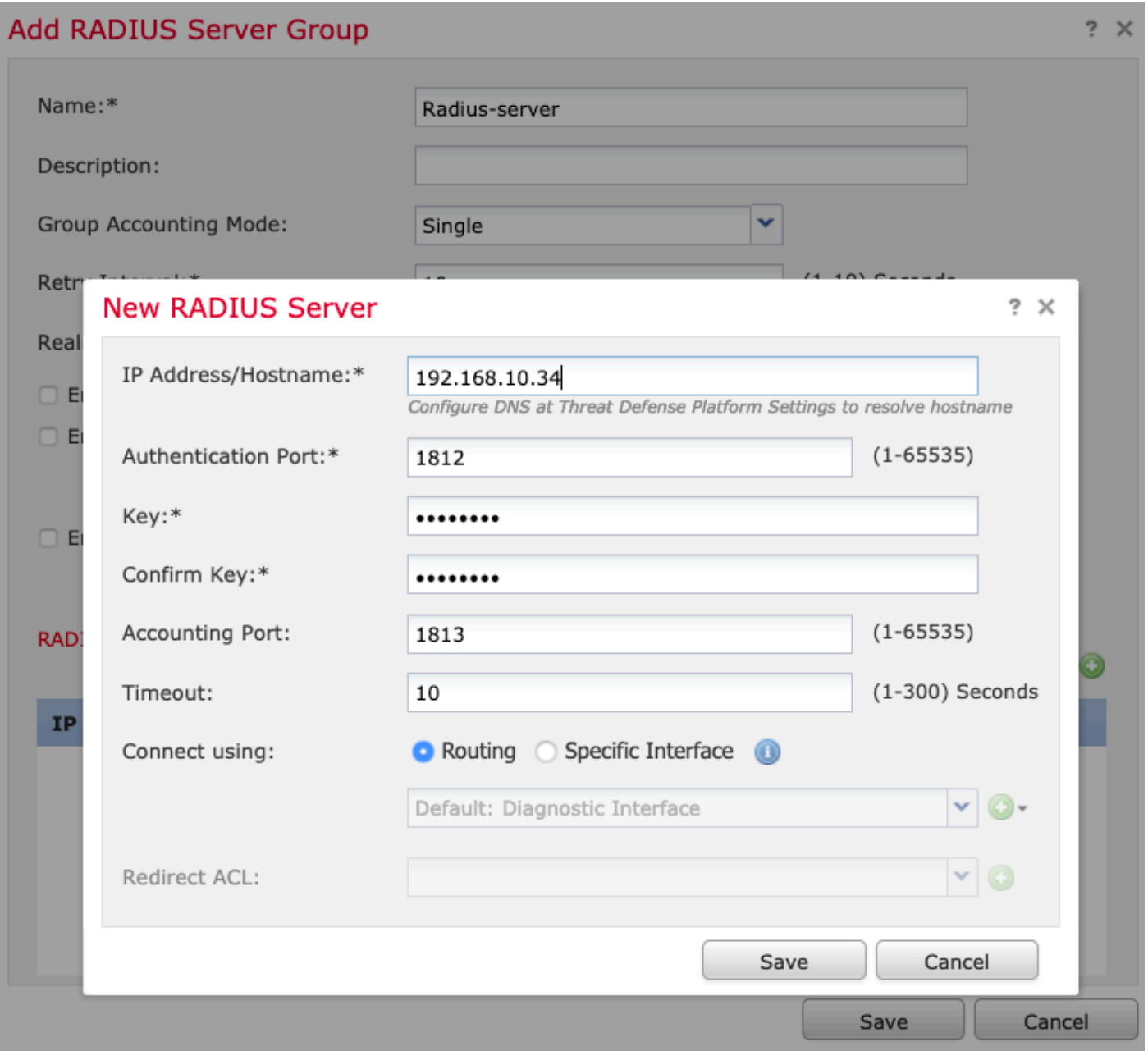
Enable dynamic authorization

Port:* (1024-65535)

RADIUS Servers (Maximum 16 servers) +

IP Address/Hostname		
No records to display		

2.为Radius Server Group分配名称并添加Radius服务器IP地址以及共享密钥（需要共享密钥才能将FTD与Radius服务器配对），完成此表单后，请选择Save（如图所示）。



3. RADIUS服务器信息现在在Radius服务器列表中可用，如图所示。

Add RADIUS Server Group ? X

Name:*

Description:

Group Accounting Mode: ▼

Retry Interval:* (1-10) Seconds

Realms: ▼

Enable authorize only



Enable interim account update

Interval:* (1-120) hours

Enable dynamic authorization

Port:* (1024-65535)

RADIUS Servers (Maximum 16 servers) +

IP Address/Hostname		
192.168.10.34		

第三步：创建IP池

- 1.导航到对象 > 对象管理 > 地址池 > 添加IPv4池。
- 2.分配IP地址的名称和范围，不需要Mask字段，但可以如图所示指定。

Add IPv4 Pool



Name*	<input type="text" value="vpn-pool"/>
IPv4 Address Range*	<input type="text" value="192.168.55.1-192.168.55.253"/> Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150
Mask	<input type="text" value="255.255.255.0"/>
Description	<input type="text"/>
Allow Overrides	<input type="checkbox"/>

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

第四步：创建XML配置文件

- 1.从Cisco.com下载配置文件编辑器工具并运行该应用程序。
- 2.在“配置文件编辑器”应用程序中，导航到服务器列表，然后选择添加，如图所示。

The screenshot shows the VPN configuration interface. On the left is a navigation menu with items: VPN, Preferences (Part 1), Preferences (Part 2), Backup Servers, Certificate Pinning, Certificate Matching, Certificate Enrollment, Mobile Policy, and Server List. The main area is titled "Server List" and contains a table with the following columns: Hostname, Host Address, User Group, Backup Server List, SCEP, Mobile Settings, and Certificate Pins. Below the table is a note: "Note: it is highly recommended that at least one server be defined in a profile." To the right of the note are four buttons: "Add..." (highlighted with a red box), "Delete", "Edit...", and "Details".

- 3.分配显示名称、完全限定域名(FQDN)或IP地址，然后选择确定（如图所示）。

Server Load Balancing Servers SCEP Mobile Certificate Pinning

Primary Server

Display Name (required)

FQDN or IP Address / User Group

Group URL

Connection Information

Primary Protocol

ASA gateway

Auth Method During IKE Negotiation

IKE Identity (IOS gateway only)

Backup Servers

Host Address	
<input type="text"/>	<input type="button" value="Add"/>
<input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Delete"/>	

4.现在可在Server List菜单中看到该条目：

- VPN
- Preferences (Part 1)
- Preferences (Part 2)
- Backup Servers
- Certificate Pinning
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List**

Server List
Profile: Untitled

Hostname	Host Address	User Group	Backup Server ...	SCEP	Mobile Settings	Certificate Pins
Corporate - FTD (SSL)	vpn.cisco.com	ssl	-- Inherited --			

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

5.定位至文件 > 另存为。

注意：使用带有.xml扩展名的易于识别名称保存配置文件。

第五步：上传Anyconnect XML配置文件

1.在FMC中，导航至Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File。

2.为对象指定名称，然后单击浏览，在本地系统中找到客户端配置文件，然后选择保存。

 注意：确保选择Anyconnect Client Profile作为文件类型。




Add AnyConnect File



Name:*	<input type="text" value="Corporate-profile(SSL)"/>
File Name:*	<input type="text" value="FTD-corp-ssl.xml"/> <input type="button" value="Browse.."/>
File Type:*	<input type="text" value="AnyConnect Client Profile"/> <input type="button" value="v"/>
Description:	<input type="text"/>

第六步：上传AnyConnect映像

1.从思科下载网页下载webdeploy(.pkg)映像。

AnyConnect Headend Deployment Package (Mac OS)	26-Jun-2019	51.22 MB	  
anyconnect-macos-4.7.04056-webdeploy-k9.pkg			

2.导航到“对象”(Objects)> “对象管理”(Object Management)> “VPN”(VPN)> AnyConnect文件 (AnyConnect File)> 添加AnyConnect文件(Add AnyConnect File)。

3.为Anyconnect软件包文件指定名称，并在选择文件后从本地系统选择.pkg文件。

4.选择保存。

Add AnyConnect File

Name:*

File Name:*

File Type:*

Description:

注意：可根据您的要求(Windows、Mac、Linux)上传其他软件包。

步骤 7.远程访问VPN向导

根据前面的步骤，可以相应地执行远程访问向导。

1.导航到设备 > VPN > 远程访问。

2.分配远程访问策略的名称，然后从Available Devices中选择FTD设备。

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 **AnyConnect** 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**

Available Devices	Selected Devices
<input type="text" value="Search"/> <input type="text" value="FTD-Virtual"/>	<input type="text" value="FTD-Virtual"/>

Before You Start

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

Authentication Server
Configure [Realm](#) or [RADIUS Server Group](#) to authenticate VPN clients.

AnyConnect Client Package
Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface
Interfaces should be already configured on targeted [devices](#) so that they can be used as a security zone or interface group to enable VPN access.

3.分配连接配置文件名称（连接配置文件名称是隧道组名称），选择Authentication Server和Address Pools，如图所示。

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

Remote User — AnyConnect Client — Internet — Outside — VPN Device — Inside — Corporate Resources

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:*
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: (v)

Authentication Server:* (+) (Realm or RADIUS)

Authorization Server: (+) (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 (RADIUS only) (i)

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools: (pencil)

IPv6 Address Pools: (pencil)

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:* (+)
[Edit Group Policy](#)

Back Next Cancel

4.选择+符号以创建组策略。

Add Group Policy



Name:* RemoteAccess-GP

Description:

General AnyConnect Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

VPN Tunnel Protocol:

Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

SSL

IPsec-IKEv2

Save Cancel

5. (可选) 可以基于组策略配置本地IP地址池。如果未配置，则从连接配置文件 (隧道组) 中配置的池继承该池。

Add Group Policy



Name:* RemoteAccess-GP

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

IP Address Pools:

Name	IP Address Range	
vpn-pool	192.168.55.1-192.168.55.253	 

Save

Cancel

6.对于此场景，所有流量都通过隧道路由，IPv4分割隧道策略设置为Allow all traffic over the tunnel，如图所示。

Edit Group Policy



Name: *

Description:

General AnyConnect Advanced

VPN Protocols
IP Address Pools
Banner
DNS/WINS
Split Tunneling

IPv4 Split Tunneling:

IPv6 Split Tunneling:

Split Tunnel Network List Type: Standard Access List Extended Access List

Standard Access List:

DNS Request Split Tunneling

DNS Requests:

Domain List:

Save Cancel

7.为Anyconnect配置文件选择.xml配置文件，然后选择保存，如图所示。

Add Group Policy



Name:*

Description:

General

AnyConnect


Advanced

Profiles

SSL Settings

Connection Settings

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

Client 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](#).

Save

Cancel

8.根据运行的系统要求选择所需的AnyConnect映像，然后选择Next（如图所示）。

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy 2 System Help admin

Device Management NAT **VPN Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 **AnyConnect** 4 Access & Certificate 5 Summary

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](#).

Show Re-order buttons

<input checked="" type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input checked="" type="checkbox"/>	MAC4.7	anyconnect-macos-4.7.04056-webdeploy-k9...	Mac OS

Back Next Cancel

9.选择安全区和设备证书:

- 此配置定义VPN终止所在的接口以及SSL连接上显示的证书。

注意:在此场景中，FTD配置为不检查任何VPN流量，并会切换访问控制策略(ACP)选项。

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

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

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:* +

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.

Back Next Cancel

10.选择完成并部署更改：

- 与VPN、SSL证书和AnyConnect软件包相关的所有配置均通过FMC Deploy进行推送，如图所示。

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

Remote Access VPN Policy Configuration

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

Name:	TAC
Device Targets:	FTD-Virtual
Connection Profile:	TAC
Connection Alias:	TAC
AAA:	
Authentication Method:	AAA Only
Authentication Server:	Radius-server
Authorization Server:	Radius-server
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	vpn-pool
Address Pools (IPv6):	-
Group Policy:	RemoteAccess-GP-SSL
AnyConnect Images:	MAC4.7
Interface Objects:	outside
Device Certificates:	Anyconnect-certificate

Additional Configuration Requirements

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- 1 Access Control Policy Update**
An [Access Control](#) rule must be defined to allow VPN traffic on all targeted devices.
- 1 NAT Exemption**
If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.
- 1 DNS Configuration**
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.
- 1 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 'outside'

Device Identity Certificate Enrollment

Certificate enrollment object 'Anyconnect-certificate' 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.

Back Finish Cancel

NAT免除和发夹

步骤1:NAT免除配置

NAT免除是首选转换方法，用于防止流量在流经VPN隧道（远程访问或站点到站点）时路由到互联网。

当来自内部网络的流量要流经隧道而不进行任何转换时，需要执行此操作。

1. 导航至对象>网络>添加网络>添加对象，如图所示。

New Network Object

? X

Name: vpn-pool

Description:


Network: Host Range Network FQDN

192.168.55.0/24

Allow Overrides:

Save Cancel

2. 导航到设备(Device)> NAT，选择相关设备使用的NAT策略，并创建新语句。

 注：流量从内部流向外部。

Add NAT Rule

NAT Rule: Manual NAT Rule

Insert: In Category NAT Rules Before

Type: Static Enable

Description:

Interface Objects

Available Interface Objects

- calo-internal-outside
- inside-zone
- outside-zone
- outsideFW

Source Interface Objects (1)

- inside-zone

Destination Interface Objects (1)

- outside-zone

Add to Source

Add to Destination

OK Cancel

3. 选择FTD(原始源和转换后的源)后面的内部资源和目标作为Anyconnect用户的ip本地池(原始目标和转换后的目标)，如图所示。

4. 确保切换选项（如图所示），要在NAT规则中启用“no-proxy-arp”和“route-lookup”，请选择OK（如图所示）。

5. 这是NAT免除配置的结果。



上一节中使用的对象如下所述。

Name	<input type="text" value="FTDv-Inside-SUPERNE"/>
Description	<input type="text"/>
Network	<input type="radio"/> Host <input type="radio"/> Range <input checked="" type="radio"/> Network <input type="radio"/> FQDN
	<input type="text" value="10.124.0.0/16"/>
Allow Overrides	<input type="checkbox"/>

Name	<input type="text" value="vpn-pool"/>
Description	<input type="text"/>
Network	<input type="radio"/> Host <input type="radio"/> Range <input checked="" type="radio"/> Network <input type="radio"/> FQDN
	<input type="text" value="192.168.55.0/24"/>
Allow Overrides	<input type="checkbox"/>

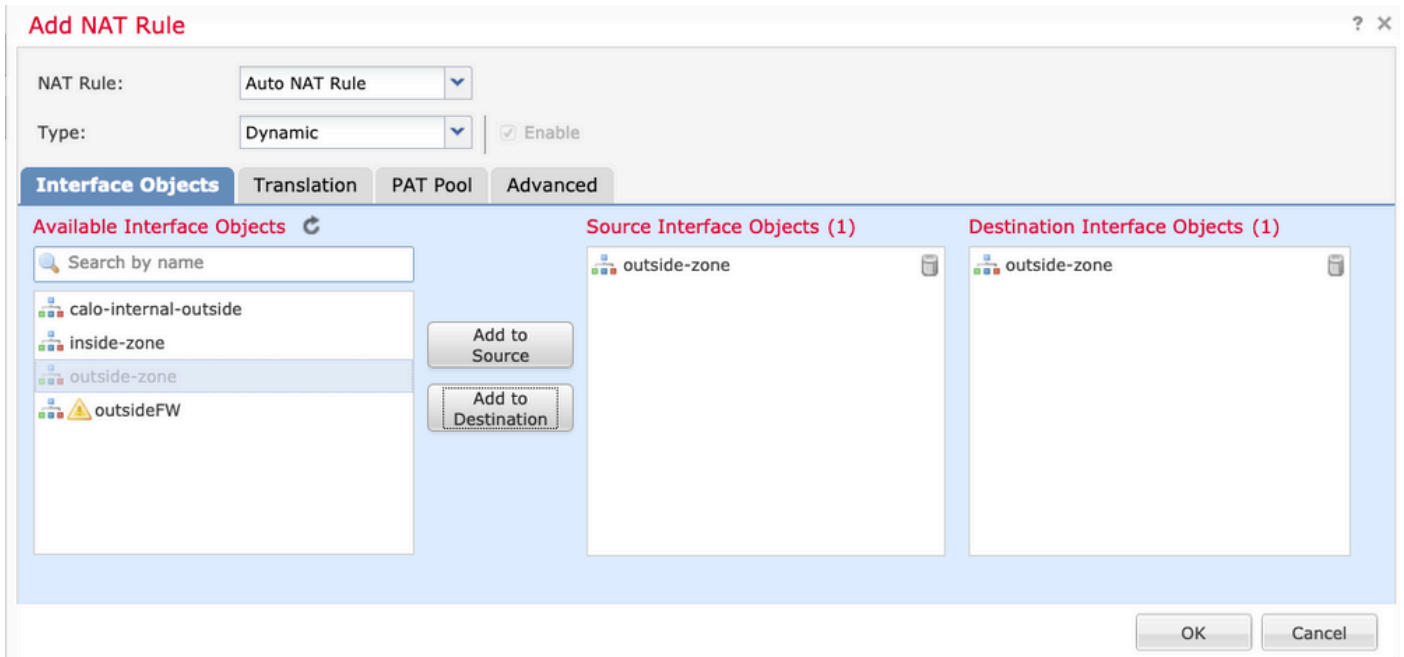
第二步：发夹配置

这种转换方法也称为U-turn，它允许流量通过接收流量的同一接口进行传输。

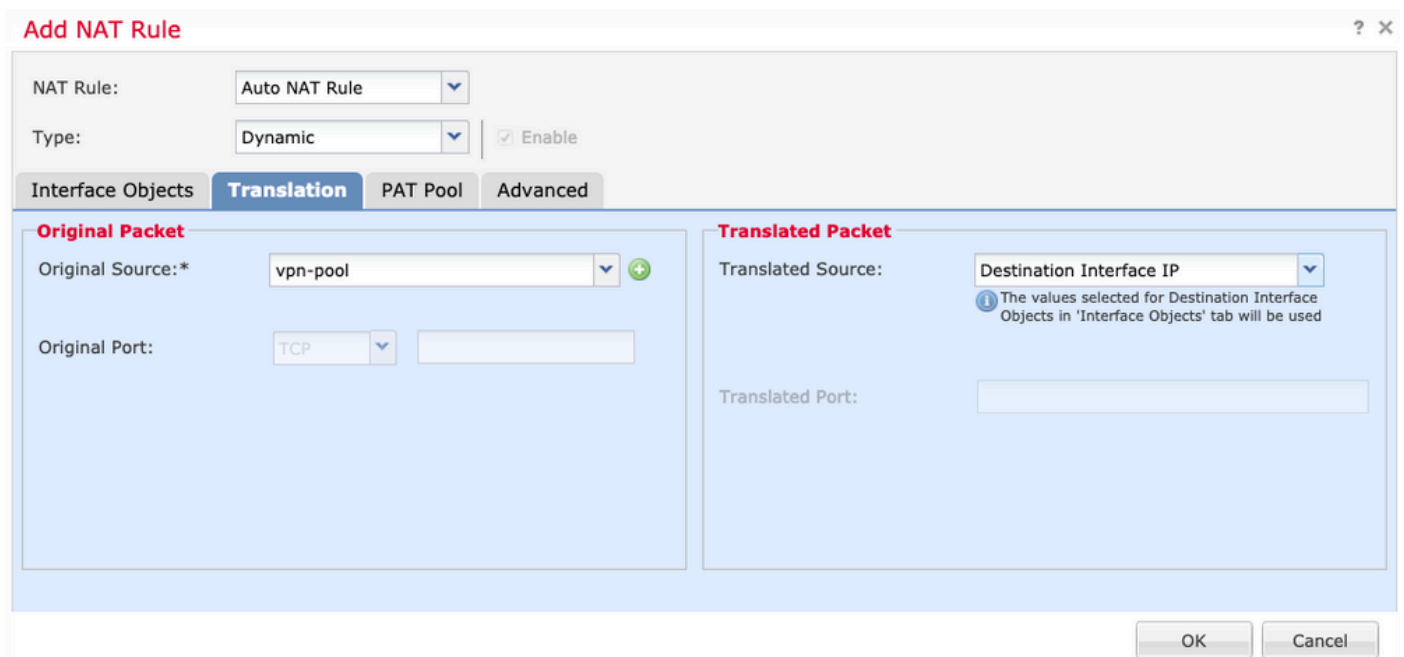
例如，当Anyconnect配置了Full tunnel拆分隧道策略时，根据NAT免除策略访问内部资源。如果Anyconnect客户端流量要到达互联网上的外部站点，发夹NAT（或U-turn）负责将流量从外部路由到外部。

在NAT配置之前，必须创建VPN池对象。

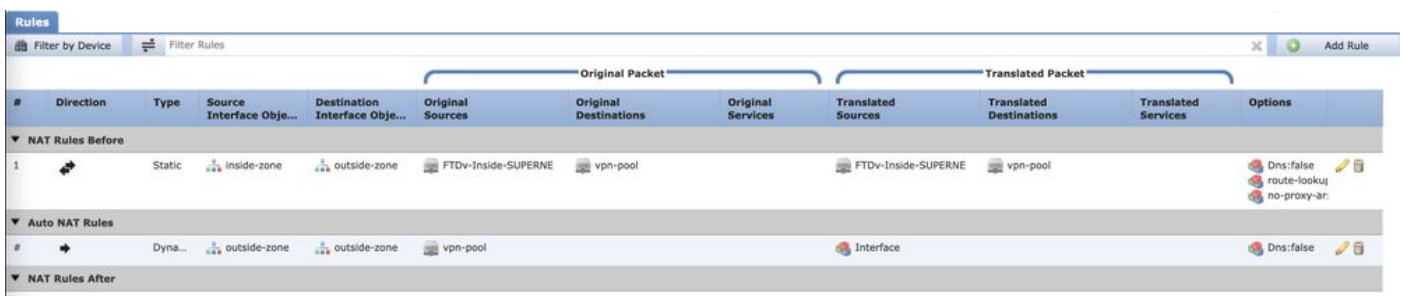
- 1.创建新的NAT语句，在NAT Rule字段中选择Auto NAT Rule，然后选择Dynamic作为NAT Type。
- 2.为源接口对象和目标接口对象（外部）选择同一接口：



3.在“转换”选项卡中，选择vpn-pool对象作为原始源，然后选择目标接口IP作为转换源，然后选择确定（如图所示）。



4.这是NAT配置的摘要，如图所示。



5.单击保存并部署更改。

验证

使用本部分可确认配置能否正常运行。

在FTD命令行中运行这些命令。

- sh crypto ca certificates
- show running-config ip local pool
- show running-config webvpn
- show running-config tunnel-group
- show running-config group-policy
- show running-config ssl
- show running-config nat

故障排除

当前没有可用于此配置的特定故障排除信息。 </>

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）。