

# AnyConnect在FTD的远程访问VPN配置

## 目录

[简介](#)

[要求](#)

[使用的组件](#)

[配置](#)

1. [Preresiquites](#)

a) [导入SSL证书](#)

b) [配置RADIUS服务器](#)

c) [创建VPN用户的地址池](#)

d) [创建XML配置文件](#)

e) [上载AnyConnect镜像](#)

2. [远程访问向导](#)：

[连接](#)

[限制](#)

[传统选项](#)

## 简介

本文为Firepower威胁防御(FTD)版本6.2.2和以上提供配置示例，那允许远程访问VPN使用传输层安全(TLS)和互联网密钥交换版本2 (IKEv2)。作为客户端，将使用思科AnyConnect，多个平台支持。

## 要求

Cisco 建议您了解以下主题：

- 基本VPN、TLS和IKEv2知识
- 基本认证、授权和核算(AAA)和RADIUS知识
- 体验与Firepower管理中心

## 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 6.2.2
- AnyConnect 4.5

## 配置

### 1. Preresiquites

为了通过远程访问向导在Firepower管理中心，您首先将需要遵从这些步骤：

- 创建用于服务器验证的证书，

- 配置RADIUS或LDAP服务器用户认证的，
- 创建VPN用户的地址池，
- 上载另外平台的AnyConnect镜像。

## a) 导入SSL证书

当您配置AnyConnect时，证书是重要的。RSA SSL和IPSec支持仅基于证书。IPSec，但是它支持椭圆曲线数字签名算法证书(ECDSA)不是可能部署新建的AnyConnect包或XML配置文件，当ECDSA使用时基于证书。意味着您能使用它IPSec，但是您将必须predeploy AnyConnect包，并且对每个用户的XML配置文件和在XML配置文件上的所有变化在每个客户端(bug将必须手工反射：[CSCtx42595](#))。证书应该另外有与DNS名和IP地址的避免附属的替代方案名称的分机在Web浏览器的错误。

有获取在FTD设备的一证书的几个方法，但是安全和容易那个是创建证书签名请求(CSR)，签署为公共密钥然后进口证明书发出的它，在CSR。这是如何执行那：

- 去对象>对象Management> PKI > Cert登记，点击Add Cert登记：

**Add Cert Enrollment** ? X

Name:\*

Description:

**CA Information** Certificate Parameters Key Revocation

Enrollment Type:

CA Certificate:\*

```

CNOwa/3Kzu1me0eiDduhgwwsIDGSS5+yngvwuIKZaiQOxvVXJGRM
L6/bXeoHTiIFM
PJqzP/S58YbpyEWFmrHSZ3wNhvq3keHtAw5KcwHtA4nKOKxuA82zX
nQLIXYI2r8h
HcbaVabAufb7CV1mdwSVDtJOBFI2ftpQONj67VN902vtN8FwA8UAsy
73zzRPbIIH
Yh5Nr9WhZn/wcxvRMi+sEi7cBrpXG1g8+cbVr5z4LWXD28zoKKoSZjx
LfJurARIW
SENBXsxAuKRQc9wgDZKHR9sA2r1AGFMm0NpSKmSNkGbkS4q37V
N9EyToUg9OXRKI
AMImjysdgAQ7O9HmeFgxbQqL8GdczEYs7VMNxQ2Jih+oRnDASSXg
AsNmi2/xIN9H
CfyjTgclvfm9gOI8JjbuX8O85RhO2cKMI3ZEGIIpeYcUbv+cWCeUSL6
mox6p9CXe
HGyUpYafhN1D78+Y8eeW9YSai0B9b54yKI5YdXjphYHXmZQ18edtZv
WIq3Ysrns2
qBojiQ==
-----END CERTIFICATE-----

```

Allow Overrides:

Save Cancel

- 选择登记类型并且粘贴Certificate Authority (CA)证书，
- 即然后请去第二选项卡并且选择自定义FQDN并且填装所有必要的字段，：

## Add Cert Enrollment



Name:\*

Description:

CA Information

**Certificate Parameters**

Key

Revocation

Include FQDN:  ▼

Custom 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:

Save

Cancel

- 在第三选项卡， Select键类型， 选择名称和大小。对于RSA， 2048个字节最低。
- 点击保存并且去设备>证书>Add >New证书。然后请选择设备， 和在精选Cert的登记下， 并且信任点您已创建， 单击添加：

## Add New Certificate



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

Device\*:

ASA5512-X\_FTD

Cert Enrollment\*:

vpn.cisco.com

Cert Enrollment Details:

Name:

vpn.cisco.com

Enrollment Type:


Manual



SCEP URL:

NA

Add

Cancel

- 以后，在信任点名称旁边，请点击  图标、然后是和以后该复制CSR对CA并且签署它。证书应该有属性作为正常HTTPS服务器。
- 在接收从CA的证书以后在base64格式，请从磁盘选择它并且点击导入。当这成功时，您应该看到：

Name	Enrollment Type	CA Certificate	Identity Certificate	
ASA5512-X_FTD				
vpn.cisco.com	Manual	Available	Available	 

## b) 配置RADIUS服务器

在FTD platform，不可能使用本地用户数据库，因此您需要RADIUS或LDAP服务器用户认证的。配置RADIUS：

- 去对象>对象Management> RADIUS服务器组>Add RADIUS服务器组。
- 填写名称并且与共享机密一起添加IP地址，点击“Save”：

### New RADIUS Server

IP Address/Hostname:\*   
*When using hostname, configure DNS using FlexConfig Policy*


Authentication Port:\*  (1-65535)

Key:\*

Confirm Key:\*

Accounting Port:  (1-65535)

- 以后您应该看到在列表的服务器：

Name	Value	Override	
ISE	1 Server	✘	 

## c) 创建VPN用户的地址池

- 去对象>对象Management>地址池>Add IPv4普尔斯：
- 放置名称，并且范围，掩码不是需要的：

### Add IPv4 Pool

Name:\*

IPv4 Address Range:\*   
 Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask:

Description:

Allow Overrides:

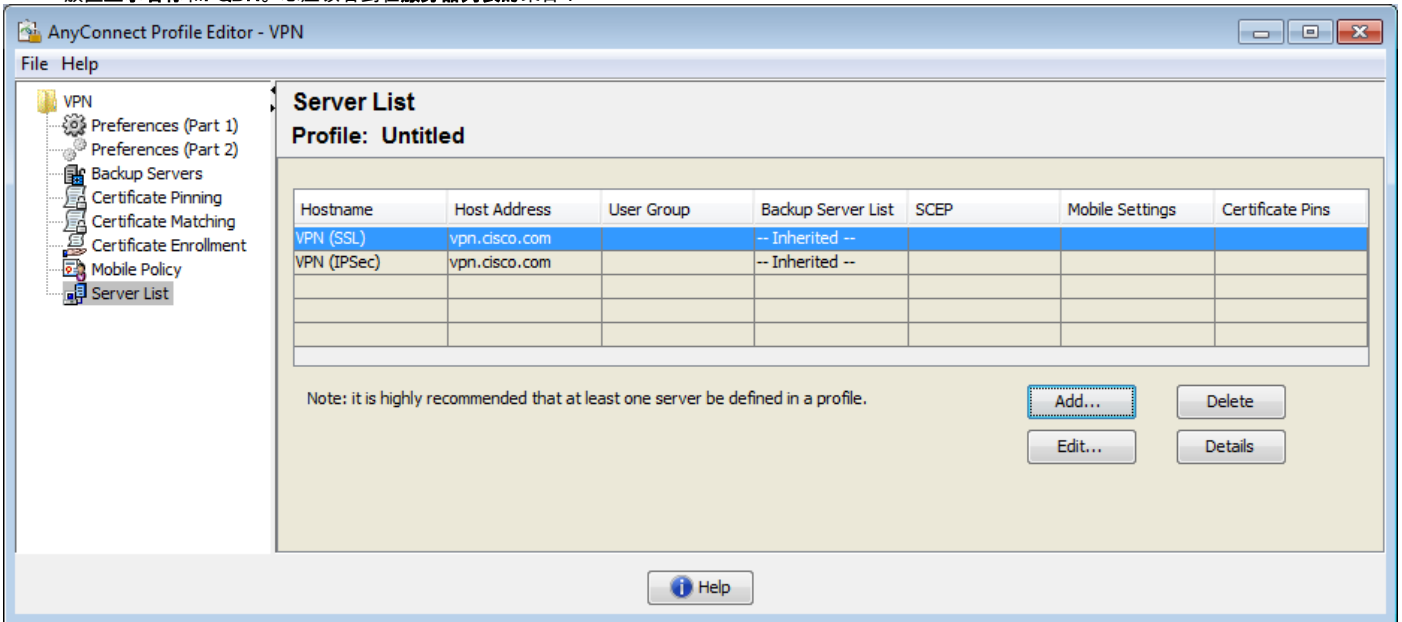
⚠ Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

**Override (0)**

## d) 创建XML配置文件

- 下载从思科站点的配置文件编辑器并且打开它。
- 去服务器列表>Add...

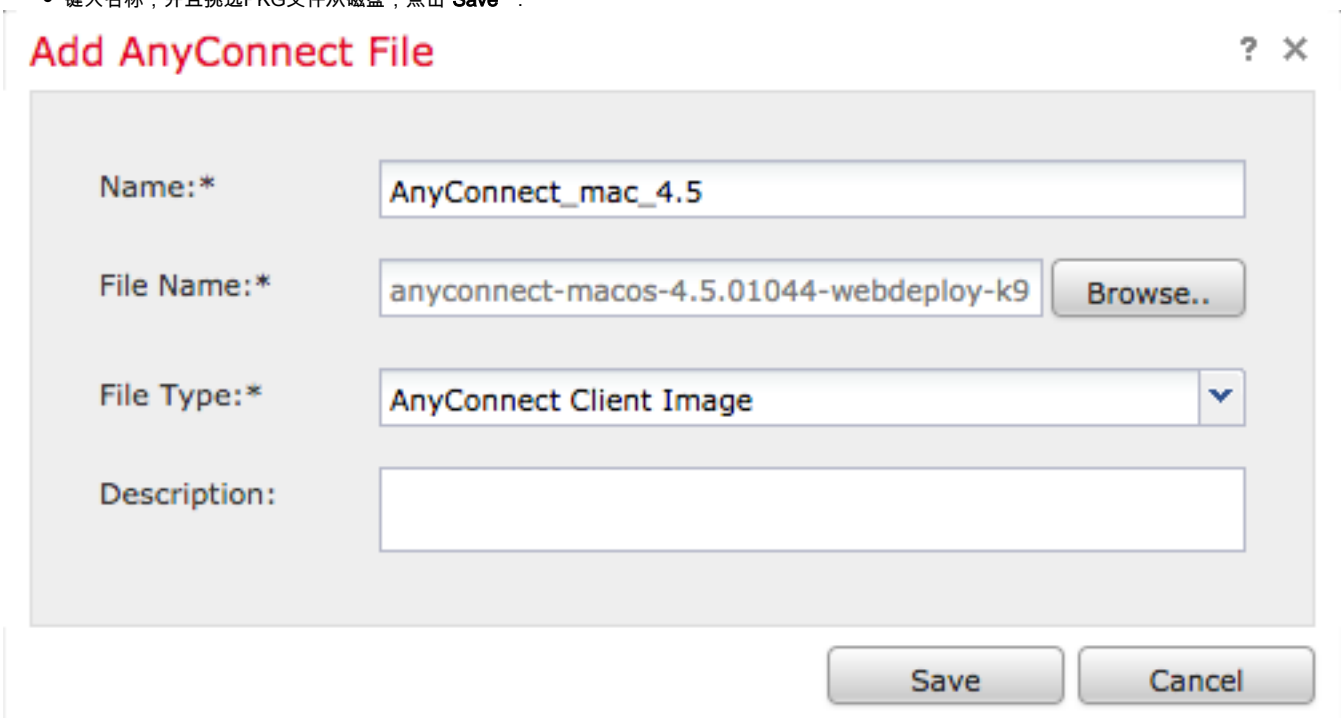
- 放置**显示名称**和**FQDN**。您应该看到在**服务器列表**的条目：



- 点击**OK**键和**File > Save As...**

## e) 上载AnyConnect镜像

- 下载从思科站点的pkg镜像。
- 去**对象>对象Management> VPN > AnyConnect File>添加AnyConnect文件**。
- 键入名称，并且挑选PKG文件从磁盘，点击“**Save**”：



- 根据您的需求添加更多包。

## 2. 远程访问向导：

- 去**设备> VPN >远程访问>Add一新的配置**。
- 根据您的需要给出配置文件，挑选FTD设备：

Name:\*

Description:

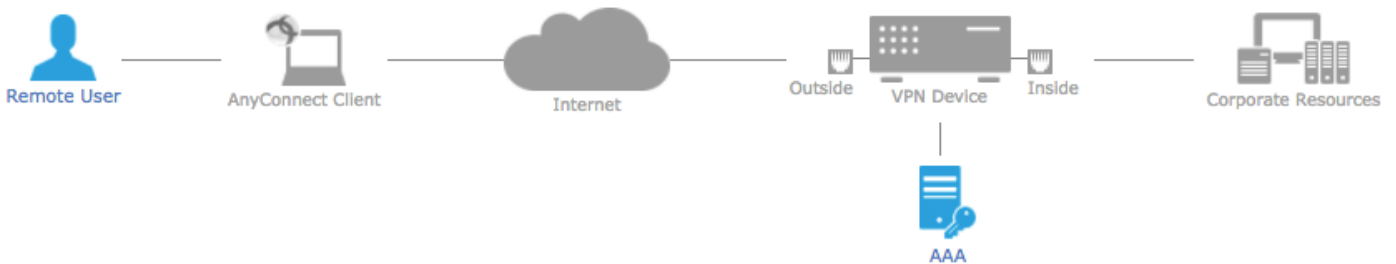
VPN Protocols:  SSL  IPsec-IKEv2

Targeted Devices: **Available Devices** **Selected Devices**

ASA5512-X\_FTD

ASA5512-X\_FTD ✕

- 在步骤**连接配置文件**，类型**连接配置文件名称**，选择您及早创建的**认证服务器和地址池**：



#### 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:  ▼

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) ⓘ

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools:

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:\*  ▼ +  
[Edit Group Policy](#)

- 点击**Edit组策略**和在选项卡**AnyConnect**，选择**客户端配置文件**，然后点击“**Save**”：

## Edit 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](#).

- 在Next页，请选择AnyConnect镜像并且其次单击：

<input type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input checked="" type="checkbox"/>	AnyConnect_mac_4.5	anyconnect-macos-4.5.01044-webdeploy-k9....	Mac OS
<input checked="" type="checkbox"/>	AnyConnect_win_4.5	anyconnect-win-4.5.01044-webdeploy-k9.pkg	Windows

- 在Next屏幕上，请选择网络接口和DeviceCertificates：

### 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

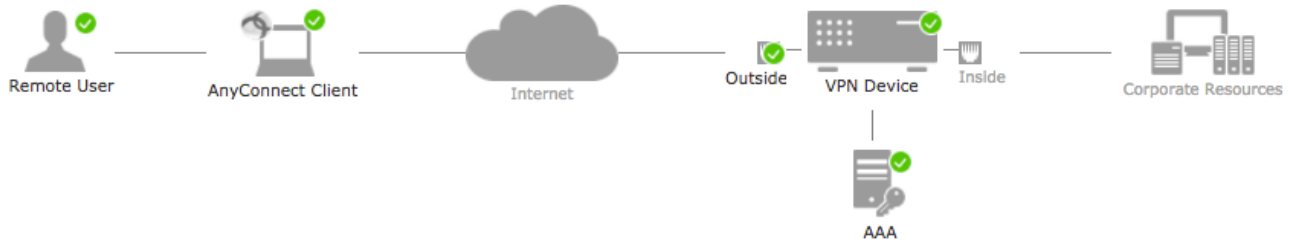
Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:\*

Certificate enrollment must be completed before deploying this VPN configuration.

- 当一切正确地配置，您能点击芬通社然后部署：





## Remote Access VPN Policy Configuration

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

Name:	AnyConnect_RA
Device Targets:	ASA5512-X_FTD
Connection Profile:	AnyConnect_RA
Connection Alias:	AnyConnect_RA
AAA:	
Authentication Method:	AAA Only
Authentication Server:	ISE
Authorization Server:	ISE
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	IPv4 Address_pool
Address Pools (IPv6):	-
Group Policy:	DfltGrpPolicy
AnyConnect Images:	AnyConnect_mac_4.5 AnyConnect_win_4.5
Interface Objects:	Outside
Device Certificates:	vpn.cisco.com

## 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 rule](#) 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.

### Network Interface Configuration

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

### Device Identity Certificate Enrollment

Make sure to install identity certificate on targeted devices using PKI Cert object 'vpn.cisco.com'

- 这与证书和AnyConnect包一起将复制全部的配置到FTD设备。

## 连接

连接到您需要打开浏览器的FTD，类型DNS名或者IP地址指向外部接口，在本例中<https://vpn.cisco.com>。您然后将必须登陆使用在RADIUS服务器存储的凭证和遵从关于屏幕的说明。一旦AnyConnect安装，您在AnyConnect窗口然后需要放置同一个地址并且单击**连接**。

## 限制

当前不支持的在FTD，但是联机在ASA：

- 双AAA认证
- 动态访问策略
- 主机扫描
- ISE状态
- VPN负载均衡设备
- 本地认证(增强：[CSCvf92680](#))
- LDAP属性地图
- RSA令牌的验证
- AnyConnect自定义
- AnyConnect脚本
- AnyConnect本地化

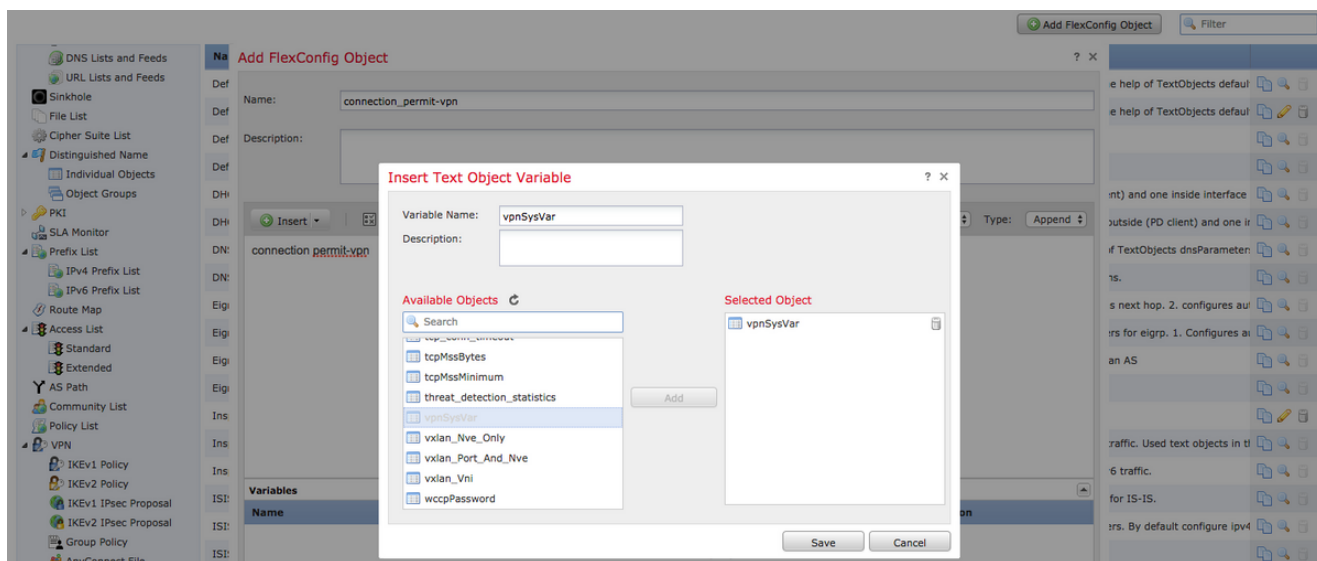
- 每APP VPN
- SCEP代理
- WSA集成
- SAML SSO
- RA和L2L的VPN同时IKEv2动态加密映射

## 传统选项

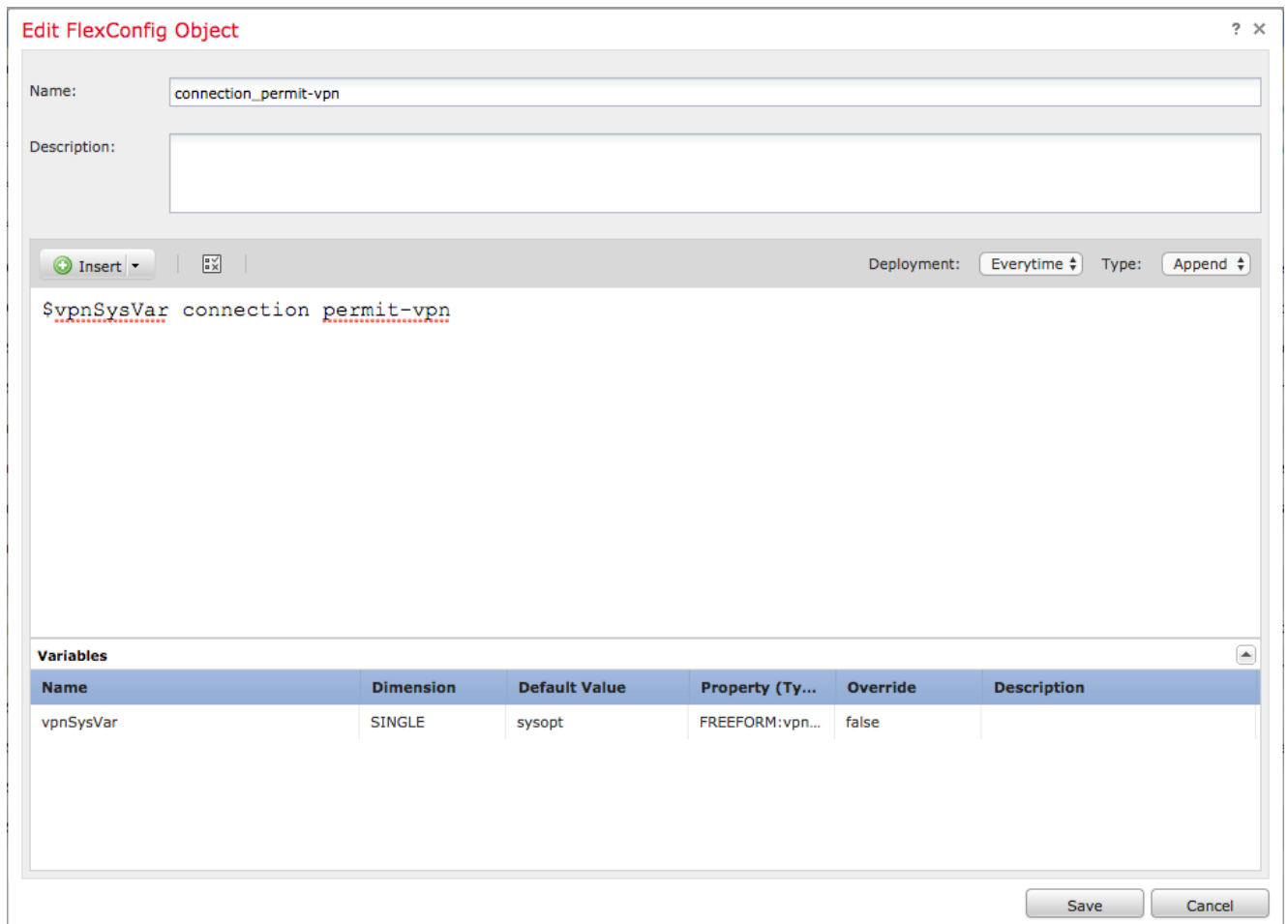
默认情况下您需要记住那， sysopt连接permit-vpn选项禁用。这意味着，您需要允许来自外部接口的地址池的流量通过访问控制策略的那。虽然PRE过滤器或访问控制规则是被添加的打算允许仅VPN流量，如果明文流量偶然匹配规则标准，不正确允许。

您能仍然启用sysopt连接permit-vpn选项：

1. 去对象>对象Management> FlexConfig > 文本对象>Add文本对象。
2. 例如创建文本对象变量， : vpnSysVar与值“sysopt”的单个条目
3. 去对象>对象Management> FlexConfig > FlexConfig对象>Add FlexConfig对象。
4. 创建与CLI “permit-vpn”的FlexConfig对象：
5. 在CLI的开始插入在flexconfig对象的文本对象变量作为“\$vpnSysVarpermit-vpn”，点击“Save”：



6. 应用FlexConfig对象如追加并且选择部署对每次：



7. 去设备 > FlexConfig 并且编辑现有策略或创建新的用新的策略按钮。

8. 添加已创建FlexConfig，点击“Save”。

9. 部署配置设置“sysopt连接permit-vpn” on命令设备。

然而这，将删除可能性使用访问控制策略检查来自用户的流量。您能仍然使用VPN过滤器或可下载的ACLs过滤用户数据流。