

# 設定FTD上的AnyConnect遠端存取VPN

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[組態](#)

[1. 必要條件](#)

[a\) 匯入SSL證書](#)

[c\) 為VPN使用者建立地址池](#)

[d\) 建立XML配置檔案](#)

[e\) 上傳AnyConnect映像](#)

[2. 遠端訪問嚮導](#)

[連線](#)

[限制](#)

[安全注意事項](#)

[a\) 啟用uRPF](#)

[b\) 啟用sysopt connection permit-vpn選項](#)

[相關資訊](#)

## 簡介

本檔案將介紹FTD上AnyConnect遠端存取VPN的組態。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 基本VPN、TLS和IKEv2知識
- 基本驗證、授權及記帳(AAA)和RADIUS知識
- 使用Firepower管理中心的經驗

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco FTD 7.2.0
- Cisco FMC 7.2.1
- AnyConnect 4.10

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

本檔案將提供Firepower威脅防禦(FTD)版本7.2.0及更高版本的組態範例，其中允許遠端存取VPN使用傳輸層安全(TLS)和網際網路金鑰交換版本2(IKEv2)。作為客戶端，可以使用Cisco AnyConnect，它受多個平台支援。

## 組態

### 1. 必要條件

要通過Firepower管理中心中的「遠端訪問」嚮導，請執行以下操作：

- 建立用於伺服器身份驗證的證書。
- 配置RADIUS或LDAP伺服器以進行使用者身份驗證。
- 為VPN使用者建立地址池。
- 上傳不同平台的AnyConnect映像。

#### a) 匯入SSL證書

設定AnyConnect時，憑證是必需的。證書必須具有DNS名稱和/或IP地址的使用者替代名稱副檔名以避免在Web瀏覽器中出錯。

**附註：**只有註冊思科使用者才能訪問內部工具和錯誤資訊。

手動證書註冊存在限制：

— 在FTD上，您需要CA憑證才能產生CSR。

— 如果從外部生成CSR，則手動方法失敗，必須使用其他方法(PKCS12)。

有幾種方法可在FTD裝置上取得憑證，但安全且簡易的方法是建立憑證簽署請求(CSR)，使用憑證授權單位(CA)簽署，然後匯入為公鑰核發的憑證（在CSR中）。以下是操作方法：

- 轉到 **Objects > Object Management > PKI > Cert Enrollment** 按一下**Add Cert Enrollment**。

## Add Cert Enrollment



Name\*

vpntestbbed.cisco.com

Description

|

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

Manual

CA Only

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

CA Certificate:

```
Ep0WYTGngteb6JFITtn..StZxdr  
YfPCilB7g  
BMAV7Gzdc4VspS6lJrAhbiiaw  
dBiIQmsBeFz9JkF4..b3l8Bo  
GN+qMa56Y  
It8una2gY4l2O//on88r5IWJlm  
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

Cancel

Save

- 選擇 Enrollment Type 以及貼上憑證授權單位(CA)憑證 (用於簽署CSR的憑證)。
- 然後轉到第二個頁籤並選擇 Custom FQDN 並填寫所有必要的欄位，例如：

## Add Cert Enrollment



Name\*

vpntestbed.cisco.com

Description

CA Information

Certificate Parameters

Key

Revocation

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

Cancel

Save

- 在第三個頁籤上，選擇 Key Type 中，選擇名稱和大小。對於RSA，最少為2048位。
- 按一下儲存並轉到 Devices > Certificates > Add > New Certificate.
- 然後選擇 Device、和下 Cert Enrollment 選擇您剛剛建立的信任點，按一下 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\*:

Cert Enrollment\*:

 +

Cert Enrollment Details:

Name: vpntestbed.cisco.com

- 稍後，點選信任點名稱旁邊的  圖示，然後 Yes 並將該CSR複製到CA並簽署之後。證書的屬性必須與HTTPS伺服器的正常屬性相同。
- 從CA收到base64格式的證書後，從磁碟中選擇該證書，然後按一下 Import. 當此操作成功時，您會看到：

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

### b) 配置RADIUS伺服器

- 轉到 **Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group.**
- 填寫名稱並新增IP地址以及共用金鑰，按一下 **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 ▾ +

Redirect ACL:



Cancel

Save

- 之後，您會看到清單中的伺服器：

Name	Value	
RadiusServer	1 Server	

c)為VPN使用者建立地址池

- 轉到 **Objects > Object Management > Address Pools > Add IPv4 Pools**.
- 輸入名稱和範圍，不需要掩碼：

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

- ① Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

▶ Override (0)

Cancel

OK

#### d)建立XML配置檔案

- 從思科網站下載配置檔案編輯器，然後將其開啟。
- 轉到 **Server List > Add...**
- 放置顯示名稱和FQDN。您將在伺服器清單中看到以下條目：

AnyConnect Profile Editor - VPN

File Help

**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.

Add... Delete Edit... Details

- 按一下 **OK**和 **File > Save as...**

## e)上傳AnyConnect映像

- 從思科網站下載pkg映像。
- 轉到 Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.
- 鍵入名稱並從磁碟中選擇PKG檔案，按一下 Save:

---

### Edit AnyConnect File ?

---

Name:\*

File Name:\*

File Type:\*

Description:

- 根據您自己的要求新增更多軟體包。

## 2.遠端訪問嚮導

- 轉到 Devices > VPN > Remote Access > Add a new configuration.
- 命名設定檔並選擇FTD裝置：



## 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

FTD
-----

Add

#### Selected Devices

FTD 
---

- 在「連線配置檔案」步驟中，鍵入 **Connection Profile Name**，選擇 **Authentication Server** 和 **Address Pools** 您之前建立的專案：

## 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:\*

**i** 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:\*  +

(LOCAL or Realm or RADIUS)

Fallback to LOCAL Authentication

Authorization 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) **i**

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](#)

- 按一下 **Edit Group Policy** 在AnyConnect頁籤上，選擇 Client Profile，然後按一下 Save:

Name:\*

DfltGrpPolicy

Description:

General    **AnyConnect**    Advanced

## Profile

Management Profile

Client Modules

SSL Settings

Connection Settings

Custom Attributes

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](#).

- 在下一頁上，選擇AnyConnect映像，然後按一下 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](#).

Show Re-order buttons +

<input checked="" type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input checked="" type="checkbox"/>	Anyconnectmac4.10	anyconnect-macos-4.10.06079-webdeploy...	Mac OS

- 在下一個螢幕上，選擇 **Network Interface and Device Certificates**:

## 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.

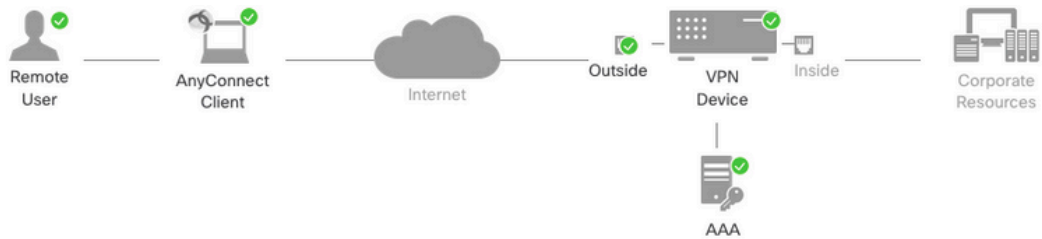
Certificate Enrollment:\*  +

## 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.*

- 當所有配置都正確時，可以按一下 Finish 然後 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.

#### 1 Access Control Policy Update

An [Access Control](#) rule must be defined to allow VPN traffic on all targeted devices.

#### 2 NAT Exemption

If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.

#### 3 DNS Configuration

To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.

#### 4 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'

- 這會將整個組態，連同憑證和AnyConnect封包複製到FTD裝置。

## 連線

若要連線到FTD，您需要開啟瀏覽器，鍵入指向外部介面的DNS名稱或IP位址。然後使用儲存在RADIUS伺服器中的憑據登入，並在螢幕上執行說明。安裝AnyConnect後，您需要在AnyConnect視窗中放置相同的地址，然後按一下 Connect。

## 限制

FTD目前不支援，但ASA上可用：

- Firepower Threat Defense 6.2.3或更早版本不支持在RADIUS伺服器中選擇介面。在部署過程中忽略介面選項。
- 啟用動態授權的RADIUS伺服器需要Firepower威脅防禦6.3或更高版本才能使動態授權生效。
- FTDposture VPN不支援通過動態授權或RADIUS授權更改(CoA)進行組策略更改。
- AnyConnect自定義(增強：思科錯誤ID [CSCvq87631](#))
- AnyConnect指令碼
- AnyConnect本地化

- WSA整合
- 適用於RA和L2L VPN的同步IKEv2動態密碼編譯對應(增強功能：思科錯誤ID [CSCvr52047](#))
- AnyConnect模組 ( NAM、Hostscan、AMP Enabler、SBL、Umbrella、Web Security等 ) — 預設情況下安裝DART(AMP Enabler和Umbrella的增強功能：思科錯誤ID [CSCvs03562](#)和思科錯誤ID [CSCvs0642](#))。
- TACACS、Kerberos ( KCD身份驗證和RSA SDI )
- 瀏覽器代理

## 安全注意事項

預設情況下，`sysopt connection permit-vpn`選項被禁用。這意味著您需要允許來自外部介面上地址池的流量通過訪問控制策略。雖然新增了預過濾器或訪問控制規則以僅允許VPN流量，但如果明文流量與規則條件匹配，則會錯誤地允許該流量。

解決這個問題有兩種方法。首先，TAC推薦的選項是為外部介面啟用反欺騙（在ASA上稱為單播反向路徑轉發 — uRPF）；其次，要啟用`sysopt connection permit-vpn`完全繞過Snort檢測。第一個選項允許對進出於VPN使用者的流量進行正常檢查。

### a) 啟用uRPF

- 為用於遠端訪問使用者的網路建立空路由（在C部分中定義）。轉到 `Devices > Device Management > Edit > Routing > Static Route` 並選取 `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 +

Search

Add

any-ipv4  
FMC  
GW  
IPv4-Benchmark-Tests  
IPv4-Link-Local  
IPv4-Multicast

Selected Network

objvpnusers

Gateway\*

Metric:

1

(1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:

Cancel

OK

- 接下來，在VPN連線終止的介面上啟用uRPF。要查詢此項，請導航至 **Devices > Device Management > Edit > Interfaces > Edit > Advanced > Security Configuration > Enable Anti Spoofing**.

General	IPv4	IPv6	Path Monitoring	Hardware Configuration	Manager Access	Advanced
Information	ARP	Security Configuration				

Enable Anti Spoofing:

Allow Full Fragment Reassembly:

Override Default Fragment Setting:

Cancel OK

當使用者連線時，將在路由表中為該使用者安裝32位路由。清除來源為池中其他未使用IP地址的文本流量會被uRFP丟棄。要檢視的描述，請執行以下操作：**Anti-Spoofing**請參閱[在Firepower威脅防禦上設定安全配置引數。](#)

#### b)啟用 Sysopt connection permit-vpn 選項

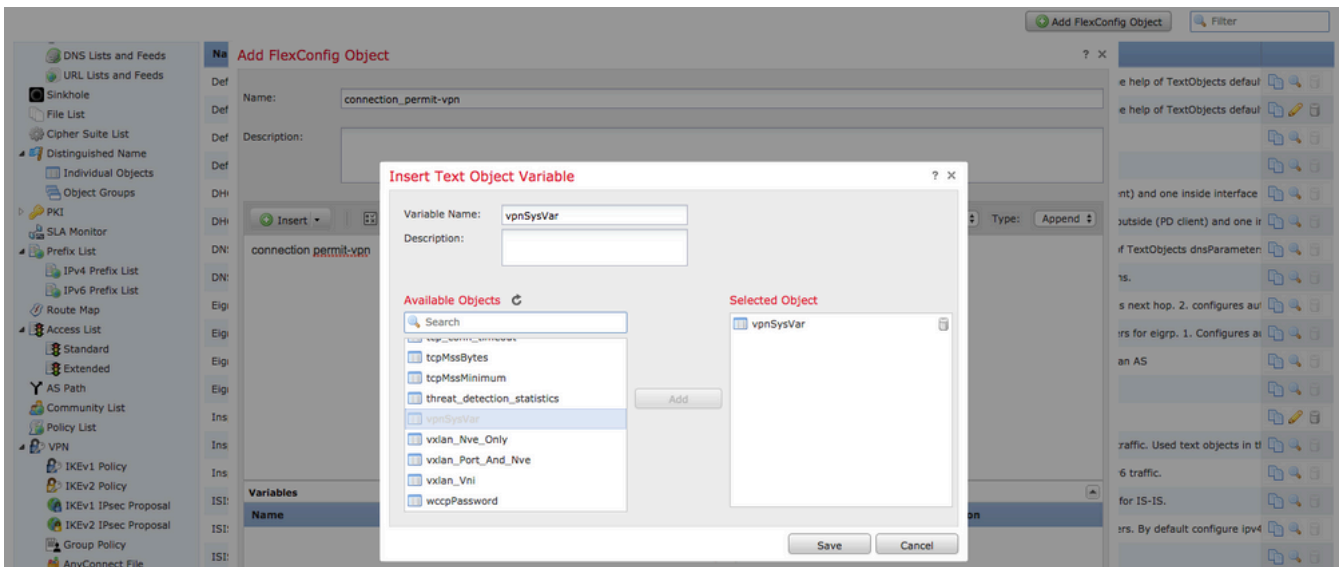
- 如果您有6.2.3版或更高版本，則可以選擇使用嚮導或在其下執行該操作 Devices > VPN > Remote Access > VPN Profile > Access Interfaces.

## Access Control for VPN Traffic

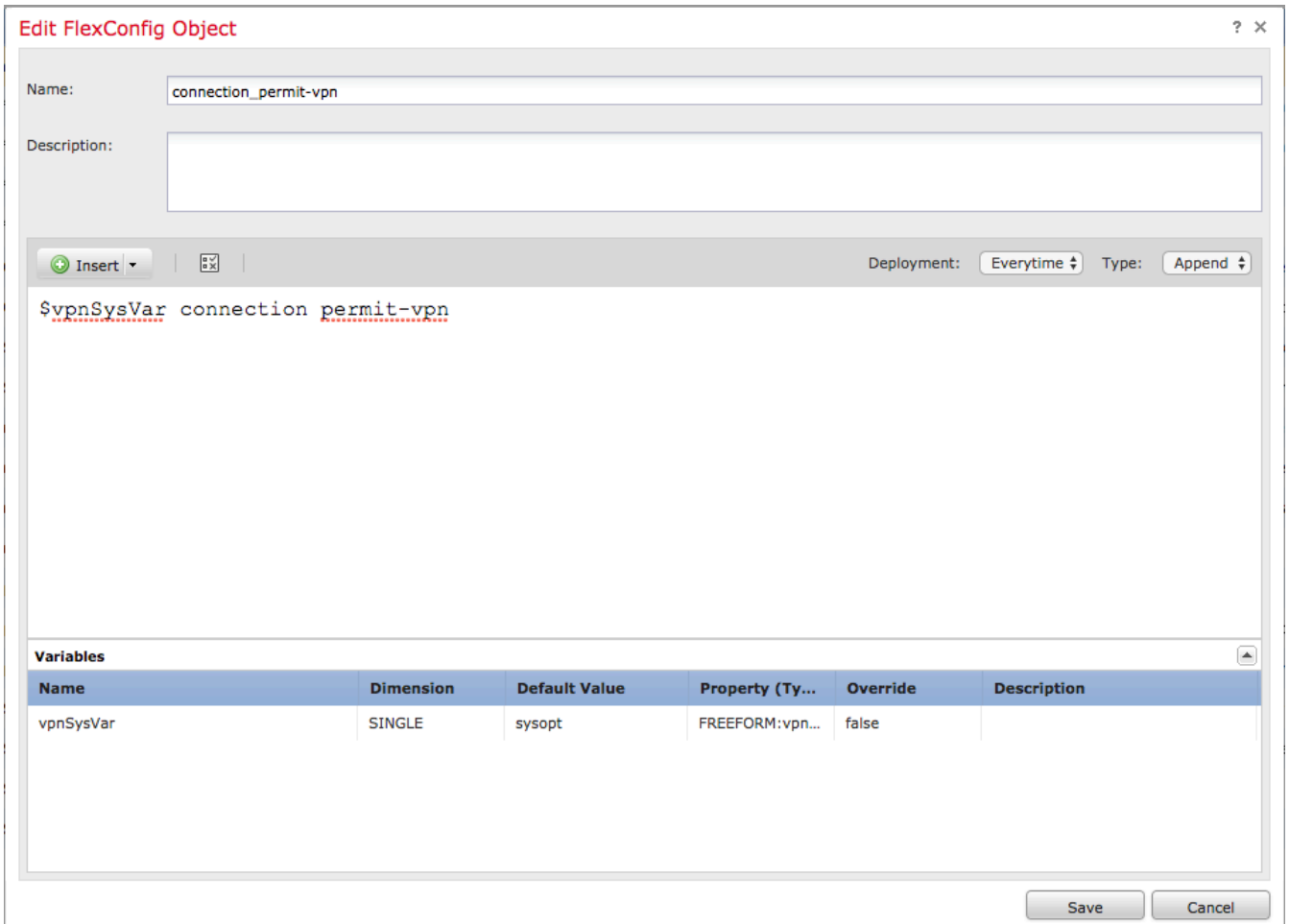
- Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)**  
*Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.*

- 對於6.2.3之前的版本，請轉到 Objects > Object Management > FlexConfig > Text Object > Add Text Object.
- 建立文本對象變數，例如：vpnSysVar具有值的單個條目 sysopt.
- 轉到 Objects> **Object Management > FlexConfig > FlexConfig Object > Add FlexConfig Object.**
- 建立 FlexConfig 使用CLI的對象 connection permit-vpn.
- 將文本對象變數插入 FlexConfig CLI上的對象 \$vpnSysVar connection permit-vpn. 按一下 Save:





- 套用 FlexConfig對象為 **Append** 並選擇部署到 **Everytime**:



- 轉到 **Devices > FlexConfig** 並編輯當前策略或使用 **New Policy** 按鈕。
- 僅新增已建立的 FlexConfig，按一下 **Save**。
- 部署配置以調配 **sysopt connection permit-vpn** 命令。

但是在此之後，您不能使用訪問控制策略來檢查來自使用者的流量。您仍然可以使用VPN過濾器或可下載ACL來過濾使用者流量。

如果您看到來自VPN使用者且具有Snort的已捨棄封包，請聯絡TAC並參考思科錯誤ID [CSCvg91399](#)。

## 相關資訊

- [思科技術支援與下載](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。