

# FTDでのAnyConnectリモートアクセスVPNの設定

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[コンフィギュレーション](#)

[1. 前提条件](#)

[a\) SSL証明書のインポート](#)

[c\) VPNユーザのアドレスプールの作成](#)

[d\) XMLプロファイルの作成](#)

[e\) AnyConnectイメージのアップロード](#)

[2. リモートアクセスウィザード](#)

[Connection](#)

[制限](#)

[セキュリティに関する考慮事項](#)

[a\) uRPFの有効化](#)

[b\) sysopt connection permit-vpnオプションを有効にします。](#)

[関連情報](#)

## 概要

このドキュメントでは、FTDでのAnyConnectリモートアクセスVPNの設定について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- VPN、TLS、およびIKEv2の基礎知識
- 認証、認可、およびアカウントティング ( AAA )、および RADIUS に関する基本的な知識
- Firepower Management Centerの使用経験

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco FTD 7.2.0
- Cisco FMC 7.2.1

- AnyConnect 4.10

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

このドキュメントでは、リモートアクセスVPNでTransport Layer Security(TLS)とInternet Key Exchange(IKEv2)バージョン2(IKEv2)を使用できるようにする、Firepower Threat Defense(FTD)バージョン7.2.0以降の設定例について説明します。Cisco AnyConnectはクライアントとして使用でき、複数のプラットフォームでサポートされています。

## コンフィギュレーション

### 1. 前提条件

Firepower Management Center(FMC)でリモートアクセスウィザードを実行するには、次の手順を実行します。

- サーバ認証に使用する証明書を作成します。
- ユーザ認証用にRADIUSサーバまたはLDAPサーバを設定します。
- VPNユーザ用のアドレスプールを作成します。
- 異なるプラットフォームのAnyConnectイメージをアップロードします。

#### a) SSL証明書のインポート

証明書は、AnyConnectを設定するときに不可欠です。Webブラウザでのエラーを回避するために、証明書にはDNS名やIPアドレスを含むサブジェクト代替名拡張子が必要です。

注：内部ツールとバグ情報にアクセスできるのは、登録されたシスコユーザだけです。

証明書の手動登録には、次のような制限があります。

- FTDでは、CSRを生成する前にCA証明書が必要です。
- CSRが外部で生成された場合、手動の方法が失敗し、別の方法を使用する必要があります(PKCS12)。

FTDアプライアンスで証明書を取得するには複数の方法がありますが、安全かつ簡単な方法は、証明書署名要求(CSR)を作成し、認証局(CA)で署名してから、CSRに含まれる公開キーに対して発行された証明書をインポートすることです。その方法を次に示します。

- 次に `Objects > Object Management > PKI > Cert Enrollment [Add Cert Enrollment]` をクリックします。

## 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:

```
Ep0WYTGngteb6JFITIn..StZxdr
YfPCiIB7g
BMAV7Gzdc4VspS6lJrAhbiiaw
dBiQIQmsBeFz9JkF4..b3l8Bo
GN+qMa56Y
It8una2gY4l2O//on88r5IWJIm
1L0oA8e4fR2yrBHX..adsGeFK
kyNrwGi/
7vQMfXdGsRrXNGRGnX+vWD
Z3/zWl0joDtCkNnqEpVn..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

- 選択 Enrollment Type [Certificate Authority (CA) certificate ( CSRの署名に使用される証明書 )]を貼り付けます。
- 次に、2番目のタブに移動し、 Custom FQDN 必要なフィールドをすべて入力します。次に例を示します。

## Add Cert Enrollment



Name\*

vpntestbbed.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

- 3番目のタブで、Key Type、名前とサイズを選択します。RSAの場合、2048ビット以上です。
- [保存(Save)]をクリックして、Devices > Certificates > Add > New Certificate.
- 次に、Device、およびの下 Cert Enrollment 作成したトラストポイントを選択し、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

- 後で、トラストポイント名の横にある  アイコンをクリックし、Yesその後、CSRをCAにコピーして署名します。証明書には、通常のHTTPSサーバと同じ属性が必要です。
- CAからbase64形式の証明書を受信したら、ディスクから選択し、Import.これが成功すると、次のように表示されます。

Name	Domain	Enrollment Type	Status	
▼ FTD				🔒
vpntestbed.cisco.com	Global	Self-Signed	📄 CA 🆔 ID	📄 🔄 🗑️

### b) RADIUSサーバの設定

- 次に **Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group.**
- 名前を入力し、IPアドレスと共有秘密を追加して、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

- その後、サーバがリストに表示されます。

Name	Value	
RadiusServer	1 Server	

## c) VPNユーザのアドレスプールの作成

- 次に **Objects > Object Management > Address Pools > Add IPv4 Pools.**
- 名前と範囲を入力します。マスクは必要ありません。

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) XMLプロファイルの作成

- シスコのサイトからProfile Editorをダウンロードして開きます。
- 次に **Server List > Add...**
- [Display Name]と[FQDN]を入力します。[Server List]に次のエントリがあります。

AnyConnect Profile Editor - VPN

File Help

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

### 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

- クリック OKと **File > Save as...**

## e) AnyConnectイメージのアップロード

- シスコサイトからpkgイメージをダウンロードします。
- 次に Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.
- 名前を入力し、ディスクからPKGファイルを選択し、 Save:

---

### Edit AnyConnect File ?

---

Name:\*

File Name:\*

File Type:\*

Description:

- 独自の要件に基づいてパッケージを追加します。

## 2. リモートアクセスウィザード

- 次に Devices > VPN > Remote Access > Add a new configuration.
- プロファイルに名前を付け、FTDデバイスを選択します。



## 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 

- [Connection Profile]ステップで、次のように入力します **Connection Profile Name**を選択し、**Authentication Server** と **Address Pools** 以前に作成したもの :

## 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](#)

- クリック [Edit Group Policy \[AnyConnect\]](#) タブで、 [Client Profile](#) をクリックし、 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](#).

- 次のページで、[AnyConnect images]を選択し、 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

- 次の画面で、 **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.

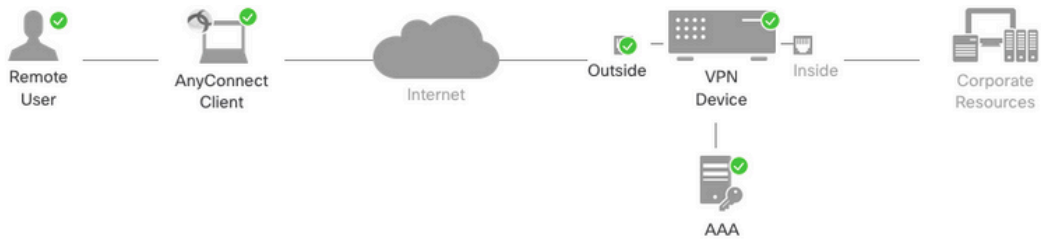
Certificate Enrollment:\*  +

## 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.*

- すべてが正しく設定されたら、Finish その後 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'

- これにより、証明書およびAnyConnectパッケージとともに設定全体がFTDアプライアンスにコピーされます。

## Connection

FTDに接続するには、ブラウザを開き、外部インターフェイスをポイントするDNS名またはIPアドレスを入力する必要があります。次に、RADIUSサーバに保存されたクレデンシアルを使用してログインし、画面の指示に従います。AnyConnectがインストールされたら、AnyConnectウィンドウに同じアドレスを入力し、Connect.

## 制限

現在FTDではサポートされていませんが、ASAでは使用可能です。

- RADIUSサーバでのインターフェイスの選択は、Firepower Threat Defense6.2.3以前のバージョンではサポートされていません。interfaceオプションは導入時に無視されます。
- ダイナミック認証が有効なRADIUSサーバが動作するには、Firepower Threat Defense 6.3以降が必要です。
- FTDポスチャVPNは、動的認可またはRADIUS認可変更(CoA)によるグループポリシーの変更

をサポートしていません。

- AnyConnectのカスタマイズ(機能拡張 : Cisco Bug ID [CSCvq87631](#))
- AnyConnectスクリプト
- AnyConnectのローカリゼーション
- WSAの統合
- RAおよびL2L VPNの同時IKEv2ダイナミッククリプトマップ(機能拡張 : Cisco Bug ID [CSCvr52047](#))
- AnyConnectモジュール ( NAM、Hostscan、AMPイネーブラ、SBL、Umbrella、Webセキュリティなど ) :DARTはデフォルトでインストールされます(AMPイネーブラおよびUmbrellaの機能拡張 : Cisco Bug ID [CSCvs03562](#)およびCisco Bug ID [CSCvs06642](#))。
- TACACS、Kerberos ( KCD認証およびRSA SDI )
- ブラウザプロキシ

## セキュリティに関する考慮事項

デフォルトでは、`sysopt connection permit-vpn` オプションは無効です。つまり、アクセスコントロールポリシーを介して外部インターフェイスのアドレスプールから送信されるトラフィックを許可する必要があります。VPNトラフィックのみを許可するためにプレフィルタまたはアクセス制御ルールが追加されますが、クリアテキストトラフィックがルールの条件に一致する場合は、誤って許可されます。

この問題には2つのアプローチがあります。1つ目は、TACが推奨するオプションで、外部インターフェイスに対してアンチスプーフィングを有効にすることです(ASAではUnicast Reverse Path Forwarding(uRPF)と呼ばれていました)。2つ目は、有効にすることです `sysopt connection permit-vpn Snort` 検査を完全にバイパスします。最初のオプションでは、VPNユーザとの間でやり取りされるトラフィックを通常の方法で検査できます。

### a) uRPFの有効化

- セクションCで定義した、リモートアクセスユーザに使用するネットワークのヌルルートを作成します。 `Devices > Device Management > Edit > Routing > Static Route` を選択し、 `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

- 次に、VPN接続が終端するインターフェイスでuRPFを有効にします。これを見つけるには、**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

ユーザが接続されると、そのユーザの32ビットルートがルーティングテーブルにインストールされます。プールから送信された他の未使用IPアドレスから送信されたテキストトラフィックをクリアすると、uRFPによって廃棄されます。説明を表示するには **Anti-Spoofing** 『[Firepower Threat Defenseでのセキュリティ設定パラメータの設定](#)』を参照してください。

## b)有効 Sysopt connection permit-vpn オプション

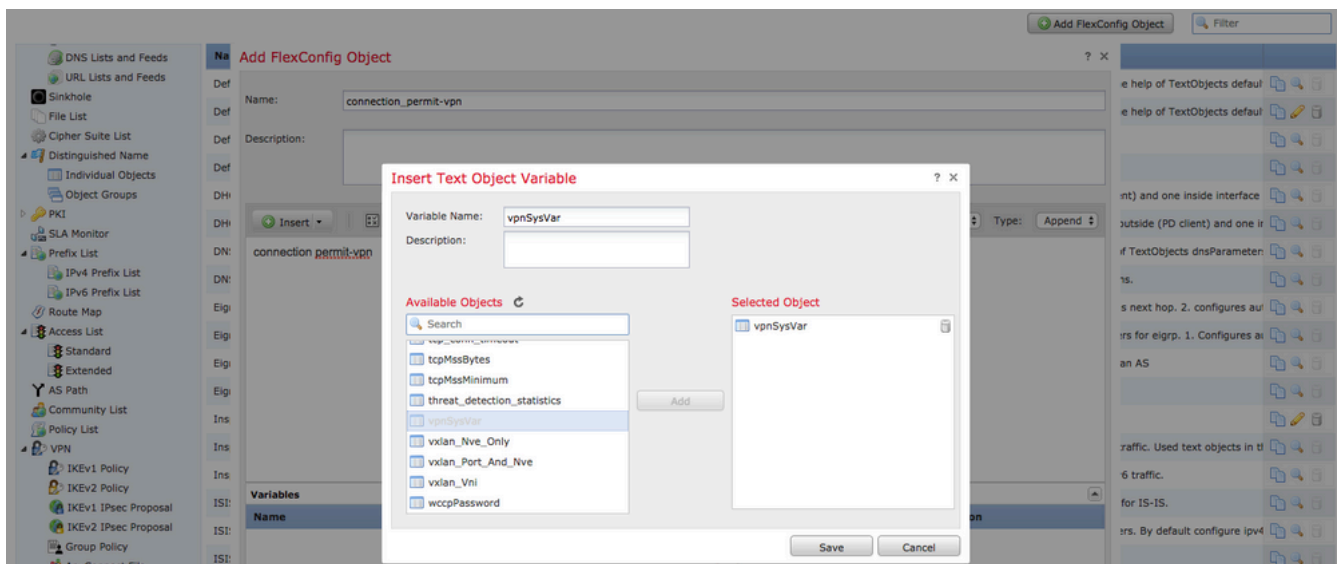
- バージョン6.2.3以降を使用している場合は、ウィザードまたはの下で実行するオプションがあります Devices > VPN > Remote Access > VPN Profile > Access Interfaces.

## Access Control for VPN Traffic

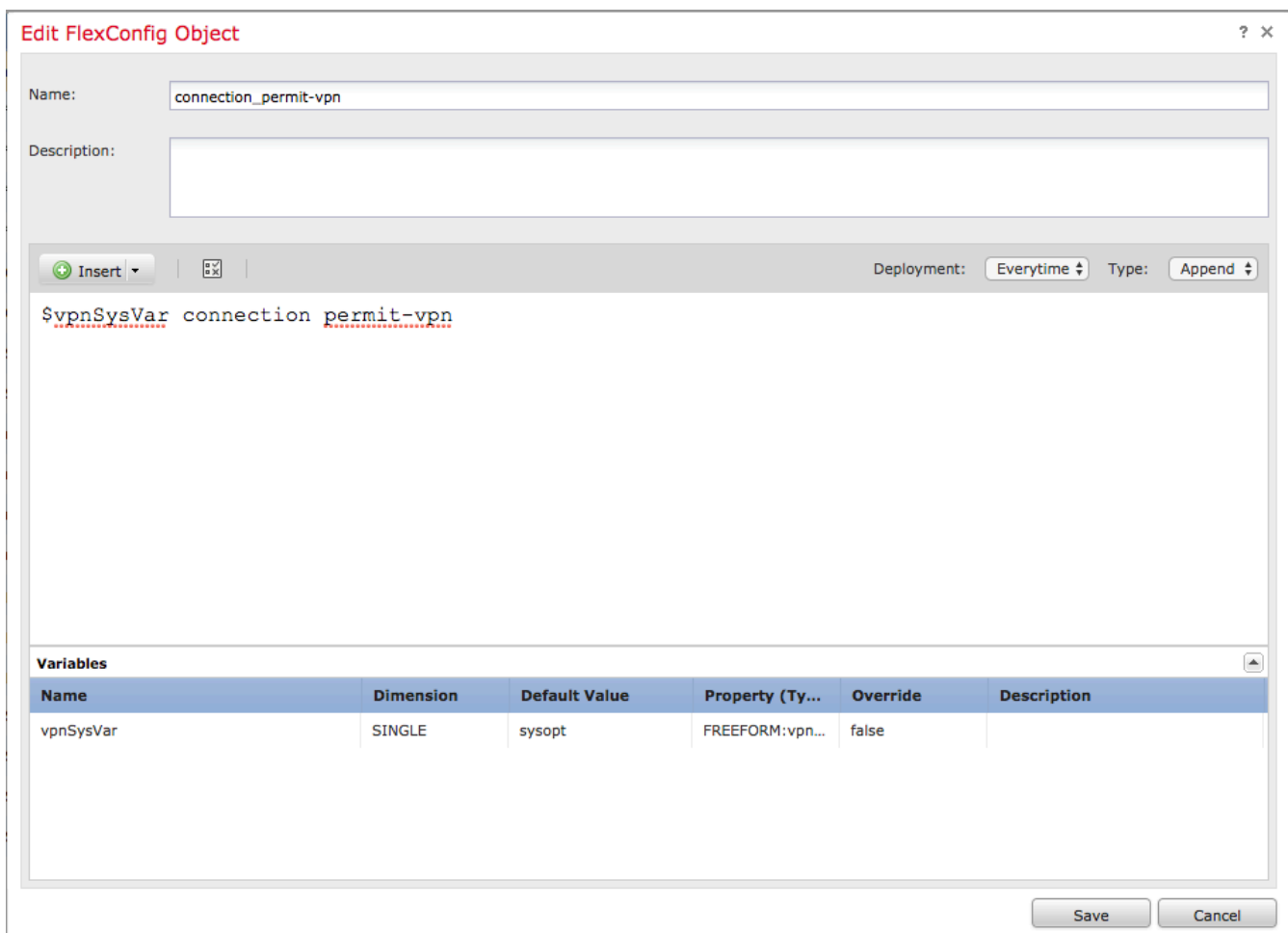
- Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)**  
*Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.*

- 6.2.3より前のバージョンについては、を参照してください。 Objects > Object Management > FlexConfig > Text Object > Add Text Object.
- テキストオブジェクト変数を作成します。例：vpnSysVar値を持つ単一のエントリ sysopt.
- 次に Objects> **Object Management** > FlexConfig > FlexConfig Object > Add FlexConfig Object.
- Cisco Unified Communications Managerの FlexConfig CLIを使用したオブジェクト connection permit-vpn.
- テキストオブジェクト変数を FlexConfig CLIでオブジェクトを指定します。 \$vpnSysVar connection permit-vpn. クリック Save:





- Cisco Unified Communications Managerの FlexConfig ~として異議を唱える Append 導入を選択して Evertime:



- 次に Devices > FlexConfig 現在のポリシーを編集するか、新しいポリシーを作成します。 New Policy をクリックして、クエリーを実行します。
- 作成した FlexConfig をクリックし、 Save.
- プロビジョニングする構成を展開します sysopt connection permit-vpn コマンドをデバイスで発行します。

ただし、この後は、アクセスコントロールポリシーを使用してユーザから着信するトラフィックを検査することはできません。ユーザトラフィックのフィルタリングには、引き続きVPNフィル

またはダウンロード可能ACLを使用できます。

VPNユーザからのSnortでパケットのドロップが見られる場合は、TACに問い合わせてCisco Bug ID [CSCvg91399](#)を参照してください。

## 関連情報

- [シスコテクニカルサポートおよびダウンロード](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。