

# Configuration d'AnyConnect Remote Access VPN sur FTD

## Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configuration](#)

[1. Conditions préalables](#)

[a\) Importer le certificat SSL](#)

[c\) Créer un pool d'adresses pour les utilisateurs VPN](#)

[d\) Créer un profil XML](#)

[e\) Télécharger des images AnyConnect](#)

[2. Assistant Accès à distance](#)

[Connexion](#)

[Limites](#)

[Considérations de sécurité](#)

[a\) Activer uRPF](#)

[b\) Activez l'option de connexion sysopt permit-vpn](#)

[Informations connexes](#)

## Introduction

Ce document décrit une configuration pour AnyConnect Remote Access VPN sur FTD.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base en VPN, TLS et IKEv2
- Connaissances de base en authentification, autorisation et comptabilité (AAA) et RADIUS
- Expérience avec Firepower Management Center

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco FTD 7.2.0

- Cisco FMC 7.2.1
- AnyConnect 4.10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

Ce document fournit un exemple de configuration pour Firepower Threat Defense (FTD) version 7.2.0 et ultérieure, qui permet au VPN d'accès à distance d'utiliser Transport Layer Security (TLS) et Internet Key Exchange version 2 (IKEv2). En tant que client, Cisco AnyConnect peut être utilisé, qui est pris en charge sur plusieurs plates-formes.

## Configuration

### 1. Conditions préalables

Afin de passer par l'assistant d'accès à distance dans Firepower Management Center :

- Créez un certificat utilisé pour l'authentification du serveur.
- Configurez le serveur RADIUS ou LDAP pour l'authentification des utilisateurs.
- Créez un pool d'adresses pour les utilisateurs VPN.
- Téléchargez des images AnyConnect pour différentes plates-formes.

#### a) Importer le certificat SSL

Les certificats sont essentiels lorsque vous configurez AnyConnect. Le certificat doit avoir une extension Subject Alternative Name avec un nom DNS et/ou une adresse IP pour éviter des erreurs dans les navigateurs Web.

**Remarque** : seuls les utilisateurs Cisco enregistrés ont accès aux outils internes et aux informations de bogue.

L'inscription manuelle des certificats comporte des limites :

- Sur FTD, vous avez besoin du certificat CA avant de générer le CSR.
- Si le CSR est généré en externe, la méthode manuelle échoue, une autre méthode doit être utilisée (PKCS12).

Il existe plusieurs méthodes pour obtenir un certificat sur l'appareil FTD, mais la plus sûre et la plus simple est de créer une demande de signature de certificat (CSR), de la signer avec une autorité de certification (CA), puis d'importer le certificat émis pour la clé publique, qui était dans CSR. Voici comment procéder :

- Aller à **Objects > Object Management > PKI > Cert Enrollment** , cliquez sur **Ajouter une inscription de certificat**.

## Add Cert Enrollment



Name\*

vpntestbbbed.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
lt8una2gY4l2O//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

- Sélectionner Enrollment Type et collez le certificat de l'autorité de certification (le certificat utilisé pour signer le CSR).
- Accédez ensuite au deuxième onglet et sélectionnez Custom FQDN et remplissez tous les champs nécessaires, par exemple :

## 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

- Dans le troisième onglet, sélectionnez Key Type, choisissez le nom et la taille. Pour RSA, 2048 bits est minimum.
- Cliquez sur Enregistrer et accédez à Devices > Certificates > Add > New Certificate.
- Sélectionnez ensuite Device, et sous Cert Enrollment sélectionnez le point de confiance que vous venez de créer, puis cliquez sur 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

- Plus tard, en regard du nom du point de confiance, cliquez sur le bouton , puis Yes, puis copiez CSR à CA et signez-le. Les attributs du certificat doivent être identiques à ceux d'un serveur HTTPS normal.
- Après avoir reçu le certificat de CA au format base64, sélectionnez-le sur le disque et cliquez sur Import. Lorsque cette opération réussit, vous voyez :

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

### b) Configurer le serveur RADIUS

- Aller à **Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group**.
- Remplissez le nom et ajoutez l'adresse IP avec le secret partagé, cliquez sur **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

- Après cela, vous voyez le serveur sur la liste :

Name	Value	
RadiusServer	1 Server	

c) Créer un pool d'adresses pour les utilisateurs VPN

- Aller à **Objects > Object Management > Address Pools > Add IPv4 Pools.**
- Mettez le nom et la plage, le masque n'est pas nécessaire :

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)

Cancel

OK

#### d) Créer un profil XML

- Téléchargez l'Éditeur de profil depuis le site Cisco et ouvrez-le.
- Aller à **Server List > Add...**
- Placez le nom d'affichage et le FQDN. Vous voyez des entrées dans la liste des serveurs :

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

- Cliquer oket **File > Save as...**

## e) Télécharger des images AnyConnect

- Téléchargez les images du package depuis le site Cisco.
- Aller à Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.
- Tapez le nom et sélectionnez le fichier PKG sur le disque, puis cliquez sur Save:

### Edit AnyConnect File ?

---

Name:\*

File Name:\*

File Type:\*

Description:

- Ajoutez d'autres packages en fonction de vos propres besoins.

## 2. Assistant Accès à distance

- Aller à Devices > VPN > Remote Access > Add a new configuration.
- Nommez le profil et sélectionnez le périphérique FTD :



## 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 
---

- Dans l'étape Profil de connexion, tapez **Connection Profile Name**, sélectionnez l'option **Authentication Server** et **Address Pools** que vous avez créé précédemment :

## 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](#)

- Cliquez sur **Edit Group Policy** et dans l'onglet AnyConnect, sélectionnez Client Profile, puis cliquez sur 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](#).

- Sur la page suivante, sélectionnez Images AnyConnect et cliquez sur 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 ▾

- Dans l'écran suivant, sélectionnez **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.

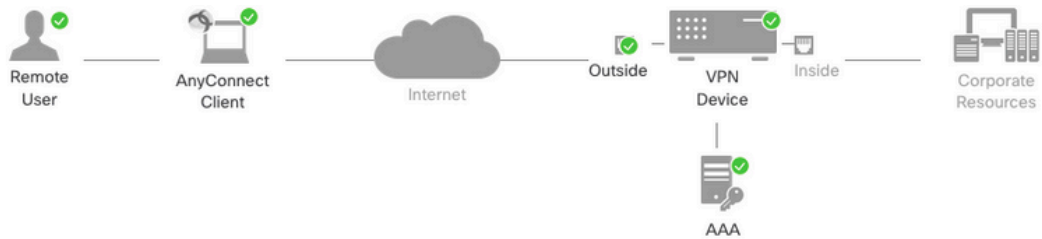
Certificate Enrollment:\*  +

## 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.*

- Lorsque tout est correctement configuré, vous pouvez cliquer sur **Finish** et ensuite **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'

- Cette opération copie l'intégralité de la configuration avec les certificats et les packages AnyConnect vers l'appliance FTD.

## Connexion

Pour vous connecter à FTD, vous devez ouvrir un navigateur, tapez le nom DNS ou l'adresse IP qui pointe vers l'interface externe. Vous vous connectez ensuite avec les informations d'identification stockées sur le serveur RADIUS et suivez les instructions à l'écran. Une fois AnyConnect installé, vous devez placer la même adresse dans la fenêtre AnyConnect et cliquer sur Connect.

## Limites

Actuellement non pris en charge sur FTD, mais disponible sur ASA :

- La sélection d'interface dans le serveur RADIUS n'est pas prise en charge sur Firepower Threat Defense 6.2.3 ou les versions antérieures. L'option d'interface est ignorée pendant le déploiement.
- Un serveur RADIUS activé pour l'autorisation dynamique nécessite Firepower Threat

- Defense6.3 ou version ultérieure pour que l'autorisation dynamique fonctionne.
- Le VPN FTDposture ne prend pas en charge la modification de stratégie de groupe via l'autorisation dynamique ou la modification d'autorisation RADIUS (CoA).
  - Personnalisation AnyConnect (amélioration : ID de bogue Cisco [CSCvq87631](#))
  - scripts AnyConnect
  - Localisation AnyConnect
  - Intégration WSA
  - Carte de cryptage dynamique IKEv2 simultanée pour les VPN RA et L2L (amélioration : ID de bogue Cisco [CSCvr52047](#))
  - Modules AnyConnect (NAM, Hostscan, AMP Enabler, SBL, Umbrella, Web Security, etc.) - DART est installé par défaut (améliorations pour AMP Enabler et Umbrella : ID de bogue Cisco [CSCvs03562](#) et ID de bogue Cisco [CSCvs06642](#)).
  - TACACS, Kerberos (authentification KCD et RSA SDI)
  - Proxy du navigateur

## Considérations de sécurité

Par défaut, le `sysopt connection permit-vpn` est désactivée. Cela signifie que vous devez autoriser le trafic provenant du pool d'adresses sur l'interface externe via la politique de contrôle d'accès. Bien que la règle de préfiltrage ou de contrôle d'accès soit ajoutée pour autoriser uniquement le trafic VPN, si le trafic en texte clair correspond aux critères de la règle, il est autorisé par erreur.

Il y a deux approches à ce problème. Premièrement, l'option recommandée par le TAC est d'activer l'anti-usurpation (sur ASA, il était connu sous le nom de Unicast Reverse Path Forwarding - uRPF) pour l'interface externe, et deuxièmement, est d'activer `sysopt connection permit-vpn` pour contourner complètement l'inspection Snort. La première option permet une inspection normale du trafic qui va vers et depuis les utilisateurs VPN.

### a) Activer uRPF

- Créez une route Null pour le réseau utilisé pour les utilisateurs d'accès à distance, défini dans la section C. Accédez à `Devices > Device Management > Edit > Routing > Static Route` et sélectionnez `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

- Activez ensuite uRPF sur l'interface où se terminent les connexions VPN. Pour le trouver, accédez à **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

Lorsqu'un utilisateur est connecté, la route 32 bits est installée pour cet utilisateur dans la table de routage. Effacer le trafic texte provenant des autres adresses IP inutilisées du pool est abandonné par uRFP. Pour afficher une description de **Anti-Spoofing** référez-vous à [Définir les paramètres de configuration de sécurité sur Firepower Threat Defense](#).

## b) Activer `sysopt connection permit-vpn` Option

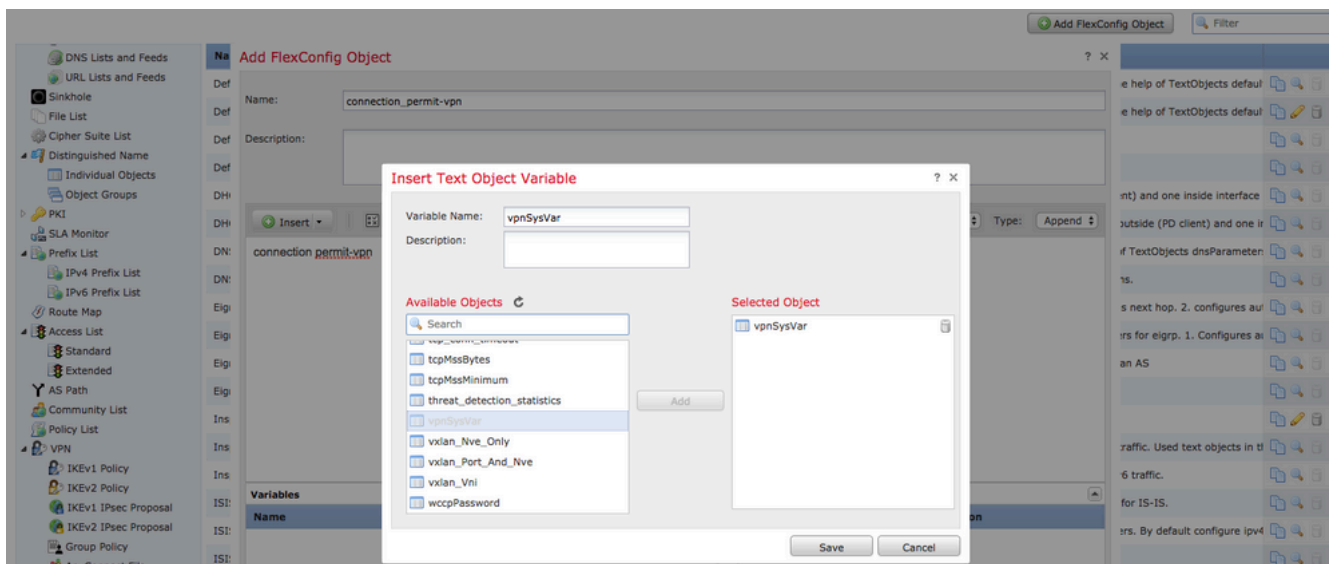
- Si vous disposez de la version 6.2.3 ou d'une version ultérieure, vous pouvez le faire avec l'Assistant ou sous `Devices > VPN > Remote Access > VPN Profile > Access Interfaces`.

## Access Control for VPN Traffic

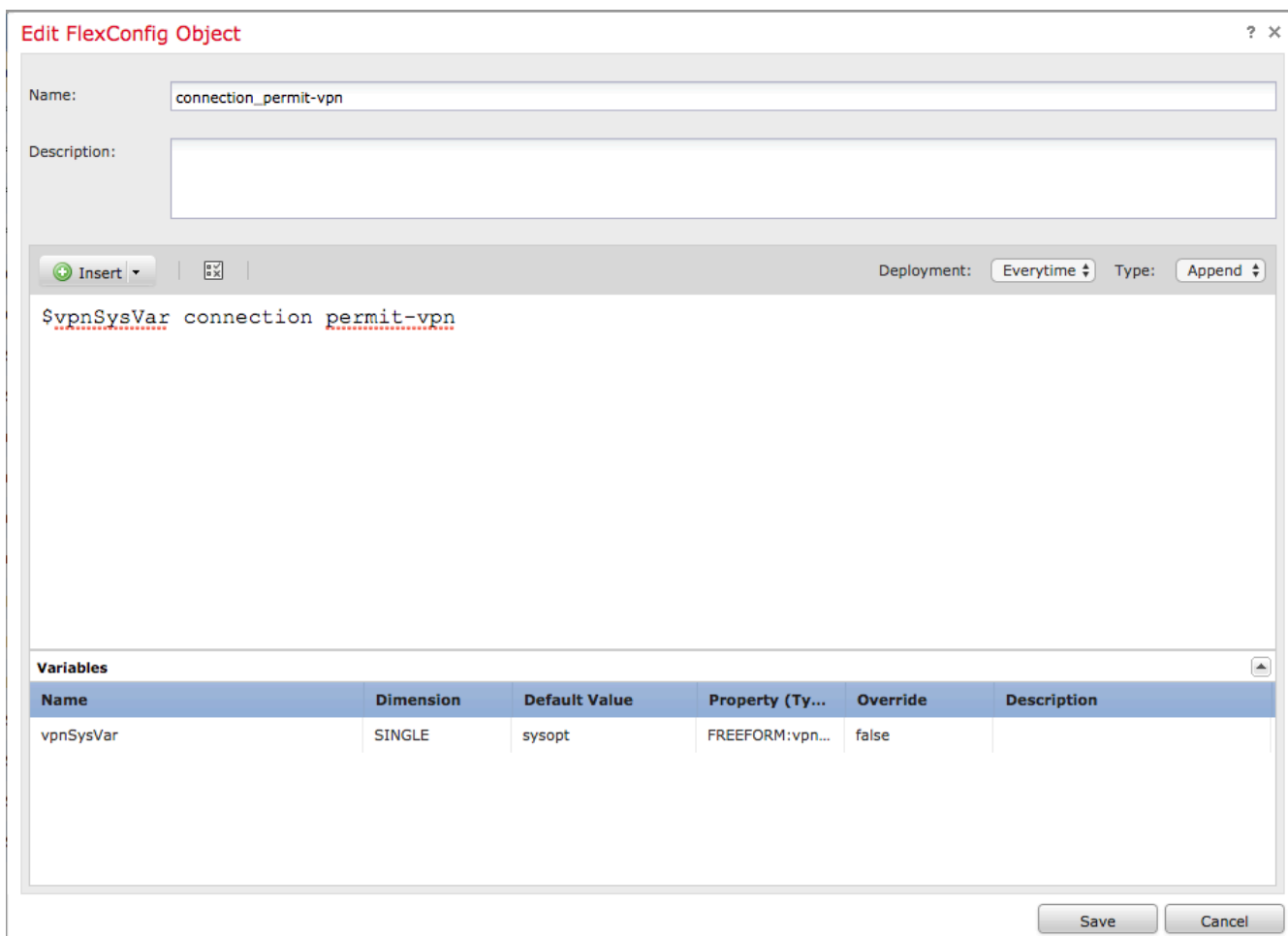
- Bypass Access Control policy for decrypted traffic (`sysopt permit-vpn`)**  
*Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.*

- Pour les versions antérieures à la version 6.2.3, accédez à `Objects > Object Management > FlexConfig > Text Object > Add Text Object`.
- Créez une variable d'objet texte, par exemple : `vpnSysVar` une entrée unique avec une valeur `sysopt`.
- Aller à `Objects > Object Management > FlexConfig > FlexConfig Object > Add FlexConfig Object`.
- Créez le FlexConfig objet avec CLI `connection permit-vpn`.
- Insère la variable d'objet texte dans le FlexConfig au niveau de l'interface CLI avec `$vpnSysVar connection permit-vpn`. Cliquer `Save`:





- Appliquez le FlexConfigobjet en tant que **Append** et sélectionnez le déploiement à **Everytime**:



- Aller à **Devices > FlexConfig** et modifiez la stratégie actuelle ou créez-en une nouvelle avec **New Policy** s'affiche.
- Ajoutez uniquement le fichier créé FlexConfig, cliquez sur **Save**.
- Déployer la configuration pour provisionner **sysopt connection permit-vpn** sur le périphérique.

Après cela, cependant, vous ne pouvez pas utiliser la stratégie de contrôle d'accès pour inspecter le trafic provenant des utilisateurs. Vous pouvez toujours utiliser un filtre VPN ou une liste de contrôle d'accès téléchargeable pour filtrer le trafic utilisateur.

Si vous voyez des paquets abandonnés avec Snort provenant des utilisateurs VPN, contactez le TAC et référencez l'ID de bogue Cisco [CSCvg91399](#).

## Informations connexes

- [Assistance technique et téléchargements Cisco](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.