

AnyConnect Remote Access VPN configureren op FTD

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configuratie](#)

[1. Voorwaarden](#)

[a\) Het SSL-certificaat invoeren](#)

[c\) Maak een pool van adressen voor VPN-gebruikers](#)

[d\) XML-profiel maken](#)

[e\) AnyConnect-afbeeldingen uploaden](#)

[2. Wizard Externe toegang](#)

[Connection](#)

[Beperkingen](#)

[Beveiligingsoverwegingen](#)

[a\) uRPF inschakelen](#)

[b\) Schakel optie voor sysopt connection-vpn in](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft een configuratie voor AnyConnect Remote Access VPN op FTD.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basis VPN-, TLS- en IKEv2-kennis
- Basisverificatie, autorisatie en accounting (AAA) en RADIUS-kennis
- Ervaring met Firepower Management Center

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco FTD 7.2.0
- Cisco VCC 7.2.1

- AnyConnect 4.10

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Dit document biedt een configuratievoorbeeld voor Firepower Threat Defence (FTD), versie 7.2.0 en hoger, waarmee externe toegang tot VPN mogelijk is om Transport Layer Security (TLS) en Internet Key Exchange versie 2 (IKEv2) te gebruiken. Als client kan Cisco AnyConnect worden gebruikt, wat op meerdere platforms wordt ondersteund.

Configuratie

1. Voorwaarden

Zo gaat u door de wizard Externe toegang in Firepower Management Center:

- Maak een certificaat aan dat wordt gebruikt voor serververificatie.
- Configureer RADIUS- of LDAP-server voor gebruikersverificatie.
- Maak een pool van adressen voor VPN-gebruikers.
- Upload AnyConnect-afbeeldingen voor verschillende platforms.

a) Het SSL-certificaat invoeren

Certificaten zijn essentieel wanneer u AnyConnect configureert. Het certificaat moet de extensie Alternatieve Naam hebben met DNS-naam en/of IP-adres om fouten in webbrowsers te voorkomen.

Opmerking: alleen geregistreerde Cisco-gebruikers hebben toegang tot interne tools en buginformatie.

Er zijn beperkingen voor handmatige inschrijving van certificaten:

- Op FTD hebt u het CA-certificaat nodig voordat u de CSR genereert.
- Indien de MVO extern wordt gegenereerd, kan de handmatige methode niet werken, maar moet een andere methode worden gebruikt (PKCS12).

Er zijn verschillende methoden om een certificaat op FTD-apparaat te verkrijgen, maar de veilige en makkelijke manier is om een Certificate Signing Verzoek (CSR) te maken, het te ondertekenen met een Certificate Authority (CA) en vervolgens een geïmporteerd certificaat afgegeven voor publieke sleutel, die in CSR was. Dit is de manier om dat te doen:

- Ga naar veld `Objects > Object Management > PKI > Cert Enrollment` , klik op **Cert-inschrijving toevoegen**.

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  
dBiIQmsBeFz9JkF4..b3l8Bo  
GN+qMa56Y  
lt8una2gY4l2O//on88r5IWJlm  
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

- Kiezen Enrollment Type certificaat van de certificeringsinstantie (CA) (het certificaat dat wordt gebruikt om de CSR te ondertekenen).
- Ga vervolgens naar het tweede tabblad en selecteer Custom FQDN en vul alle nodige velden in, bijvoorbeeld:

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

- Selecteer in het derde tabblad de optie Key Type Kies naam en grootte. Voor RSA zijn minimaal 2048 bits vereist.
- Klik op Opslaan en ga naar Devices > Certificates > Add > New Certificate.
- Selecteer vervolgens Device, en Cert Enrollment selecteer het trustpoint dat u zojuist hebt gemaakt, klik op 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

- Later, naast de trustpoint naam, klikt u op de  pictogram, gevolgd Yes, en daarna CSR naar CA kopiëren en ondertekenen. Certificaat moet dezelfde kenmerken hebben als een HTTPS-server.
- Nadat u het certificaat van CA in base64-formaat hebt ontvangen, selecteert u het van de schijf en klikt u op Import. Als dit lukt, zie je:

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

b) RADIUS-server configureren

- Ga naar veld **Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group**.
- Vul de naam in en voeg IP-adres toe samen met gedeeld geheim, klik op **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

- Daarna ziet u de server in de lijst:

Name	Value	
RadiusServer	1 Server	

c) Maak een pool van adressen voor VPN-gebruikers

- Ga naar veld **Objects > Object Management > Address Pools > Add IPv4 Pools**.
- Zet de naam en bereik, masker is niet nodig:

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) XML-profiel maken

- Download de Profile Editor van de Cisco-site en open deze.
- Ga naar veld **Server List > Add...**
- Zet de naam en FQDN van het display. U ziet vermeldingen in de serverlijst:

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

- Klik oken **File > Save as...**

e) AnyConnect-afbeeldingen uploaden

- Download pkg-afbeeldingen van de Cisco-site.
- Ga naar veld Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.
- Typ de naam en selecteer PKG-bestand vanaf schijf, klik op Save:

Edit AnyConnect File



Name:*

File Name:*

File Type:*

Description:

- Voeg meer pakketten toe op basis van uw eigen vereisten.

2. Wizard Externe toegang

- Ga naar veld Devices > VPN > Remote Access > Add a new configuration.
- Geef het profiel een naam en selecteer FTD-apparaat:

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 

- Typ in de stap Verbindingsprofiel het volgende: **Connection Profile Name**, selecteert u de **Authentication Server** en **Address Pools** die u eerder hebt gemaakt:

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](#)

- Klik op **Edit Group Policy** en selecteer op het tabblad AnyConnect de optie **Client Profile** klik u vervolgens op **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](#).

- Selecteer op de volgende pagina de optie AnyConnect-afbeeldingen en klik op 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

- Selecteer in het volgende scherm de optie **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.

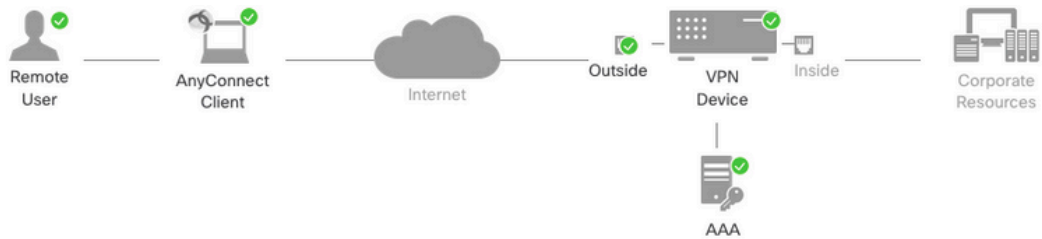
Certificate Enrollment:* +

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.

- Als alles goed is ingesteld, kunt u op Finish en vervolgens 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'

- Hierdoor wordt de gehele configuratie gekopieerd, samen met certificaten en AnyConnect-pakketten naar FTD-toepassing.

Connection

Om verbinding te maken met FTD moet u een browser, type DNS naam of IP-adres dat naar de buiteninterface wijst openen. U logt vervolgens in met referenties die zijn opgeslagen in een RADIUS-server en voert de instructies uit op het scherm. Nadat AnyConnect is geïnstalleerd, moet u hetzelfde adres in het AnyConnect-venster plaatsen en op Connect.

Beperkingen

Momenteel niet ondersteund op FTD, maar beschikbaar op ASA:

- De interfacekeuze in RADIUS-server wordt niet ondersteund op Firepower Threat Defence 6.2.3 of eerdere versies. De interfaceoptie wordt genegeerd tijdens plaatsing.
- Voor een dynamische RADIUS-server met autorisatie is Firepower Threat Defense 6.3 of hoger vereist om de dynamische autorisatie te kunnen gebruiken.
- FTD posture VPN ondersteunt groepsbeleidswijzigingen niet via dynamische autorisatie of

RADIUS-wijziging van autorisatie (CoA).

- AnyConnect-aanpassing (verbetering: Cisco-bug-id [CSCvq87631](#))
- AnyConnect-scripts
- AnyConnect-lokalisatie
- WSA-integratie
- Gelijktijdige IKEv2 dynamische cryptografische kaart voor RNA en L2L VPN (verbetering: Cisco bug-id [CSCvr52047](#))
- AnyConnect-modules (NAM, Hostscan, AMP Enabler, SBL, Umbrella, Web Security enzovoort) - DART is standaard geïnstalleerd (verbeteringen voor AMP Enabler en Umbrella: Cisco bug-id [CSCvs03562](#) en Cisco bug-id [CSCvs06642](#)).
- TACACS, Kerberos (KCD-verificatie en RSA/SDI)
- Browser Proxy

Beveiligingsoverwegingen

Standaard wordt de `sysopt connection permit-vpn` optie is uitgeschakeld. Dit betekent dat u het verkeer moet toestaan dat afkomstig is van de pool van adressen op buiteninterface via Access Control Policy. Hoewel de voorfilter- of toegangscontroleregel wordt toegevoegd om alleen VPN-verkeer toe te staan, wordt deze bij vergissing toegestaan als er clear-text verkeer gebeurt om aan de regelcriteria te voldoen.

Dit probleem wordt op twee manieren benaderd. Ten eerste, TAC aanbevolen optie, is anti-Spoofing inschakelen (op ASA was het bekend als Unicast Reverse Path Forwarding - uRPF) voor buiteninterface, en ten tweede, moet inschakelen `sysopt connection permit-vpn` om de inspectie van de snort volledig te omzeilen. De eerste optie staat een normale inspectie van het verkeer toe dat naar en van VPN-gebruikers gaat.

a) uRPF inschakelen

- Maak een nulroute voor het netwerk dat wordt gebruikt voor gebruikers van externe toegang, zoals gedefinieerd in sectie C. Ga naar `Devices > Device Management > Edit > Routing > Static Route` en selecteer `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

- Schakel vervolgens uRPF in op de interface waar de VPN-verbindingen eindigen. Om dit te vinden, navigeer naar **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

Wanneer een gebruiker is verbonden, wordt de 32-bits route voor die gebruiker in de routingstabel geïnstalleerd. Wis het tekstverkeer dat afkomstig is van de andere, ongebruikte IP-adressen uit de pool wordt door uRFP verwijderd. Om een beschrijving te zien van Anti-spoofing Raadpleeg [Beveiligingsconfiguratieparameters instellen bij Firepower Threat Defence](#).

b) Inschakelen Oysopt connection permit-vpn Optioneel

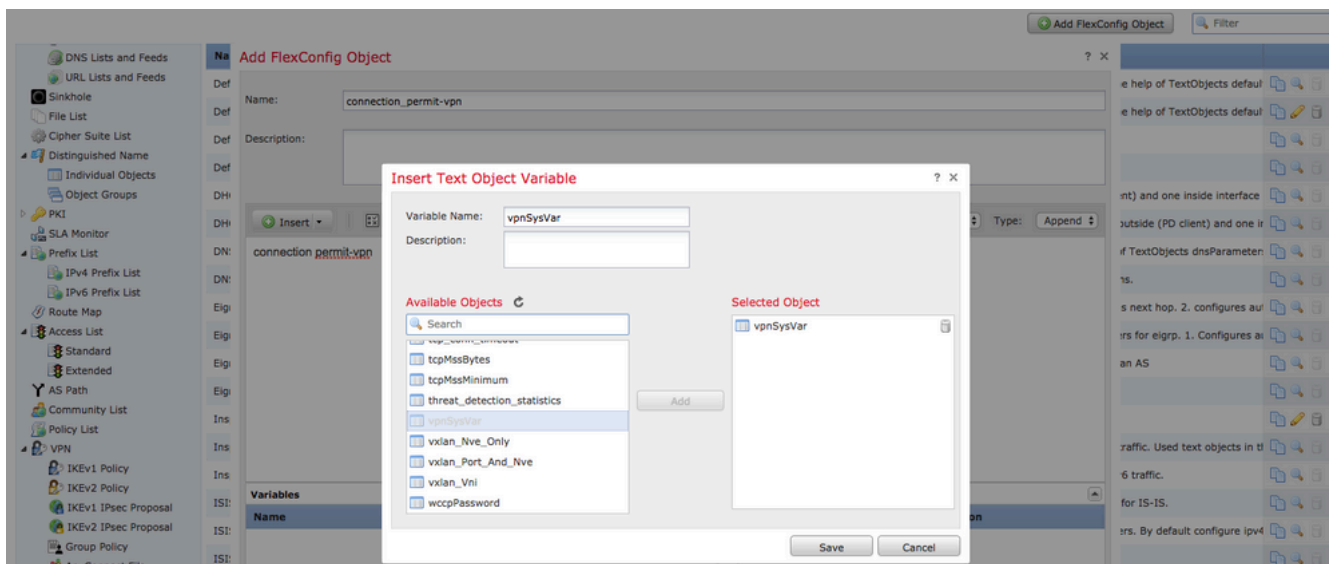
- Als u versie 6.2.3 of hoger hebt, is er een optie om dit te doen met de wizard of onder `Devices > VPN > Remote Access > VPN Profile > Access Interfaces`.

Access Control for VPN Traffic

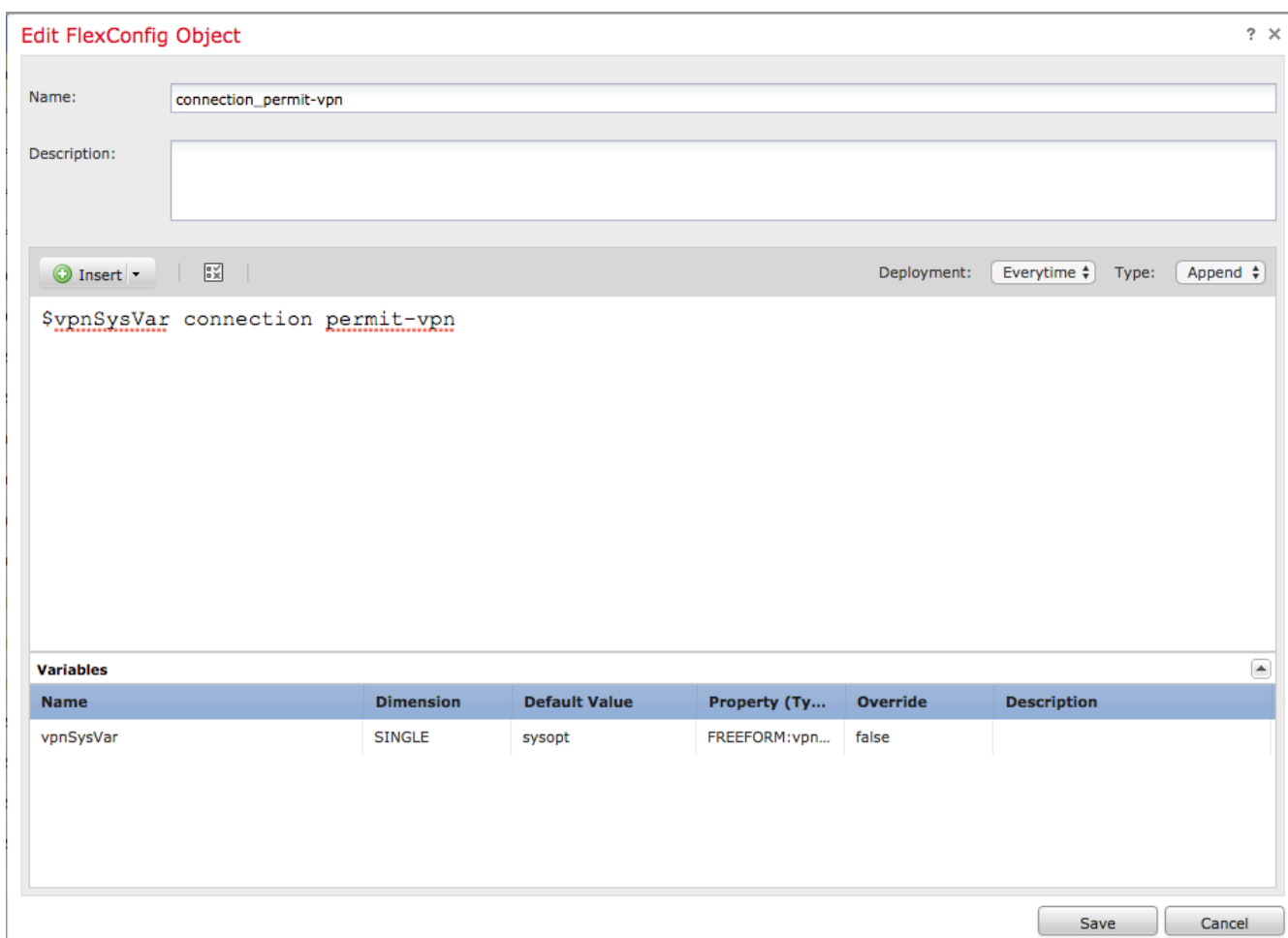
Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

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.

- Voor versies voor 6.2.3, ga naar `Objects > Object Management > FlexConfig > Text Object > Add Text Object`.
- Maak een tekstobject variabele, bijvoorbeeld: `vpnSysVar` een enkele ingang met waarde `sysopt`.
- Ga naar veld `Objects > Object Management > FlexConfig > FlexConfig Object > Add FlexConfig Object`.
- Maak de FlexConfig object met CLI `connection permit-vpn`.
- Plaats de variabele van het tekstobject in het veld FlexConfig object op de CLI met `$vpnSysVar connection permit-vpn`. Klik `Save`:



- Pas de FlexConfigobject als **Append** en selecteer implementatie om **Everytime**:



- Ga naar veld **Devices > FlexConfig** en het huidige beleid te bewerken of een nieuw beleid te maken met **New Policy** knop.
- Voeg alleen de gemaakte toe FlexConfigklickt u op **Save**.
- Stel de configuratie aan voorziening op **sysopt connection permit-vpn** opdracht op het apparaat.

Hierna kunt u echter geen toegangscontrolebeleid gebruiken om verkeer te inspecteren dat van de gebruikers afkomstig is. U kunt nog steeds VPN-filter of downloadbare ACL gebruiken om gebruikersverkeer te filteren.

Als u gedropte pakketten met snort van VPN-gebruikers ziet, neemt u contact op met TAC en verwijst u naar Cisco bug-id [CSCvg91399](#).

Gerelateerde informatie

- [Cisco technische ondersteuning en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.