

Konfiguration von AnyConnect Remote Access VPN auf FTD

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfiguration](#)

[1. Voraussetzungen](#)

[a\) SSL-Zertifikat importieren](#)

[c\) Erstellen eines Adresspools für VPN-Benutzer](#)

[d\) XML-Profil erstellen](#)

[e\) AnyConnect-Images hochladen](#)

[2. Assistent für den Remotezugriff](#)

[Verbindung](#)

[Einschränkungen](#)

[Sicherheitsüberlegungen](#)

[a\) uRPF aktivieren](#)

[b\) Aktivieren Sie die Option `sysopt-connection permit-vpn`.](#)

[Zugehörige Informationen](#)

Einleitung

Dieses Dokument beschreibt eine Konfiguration für AnyConnect Remote Access VPN auf FTD.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundlegendes VPN-, TLS- und IKEv2-Wissen
- AAA- (Basic Authentication, Authorization, and Accounting) und RADIUS-Kenntnisse
- Erfahrung mit FirePOWER Management Center

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco FTD 7.2.0

- Cisco FMC 7.2.1
- AnyConnect 4.10

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Dieses Dokument enthält ein Konfigurationsbeispiel für Firepower Threat Defense (FTD), Version 7.2.0 und höher, das es dem Remote-Access-VPN ermöglicht, Transport Layer Security (TLS) und Internet Key Exchange Version 2 (IKEv2) zu verwenden. Als Client kann Cisco AnyConnect verwendet werden, das auf mehreren Plattformen unterstützt wird.

Konfiguration

1. Voraussetzungen

So wechseln Sie durch den Remote Access-Assistenten im FirePOWER Management Center:

- Erstellen Sie ein Zertifikat, das für die Serverauthentifizierung verwendet wird.
- Konfigurieren Sie den RADIUS- oder LDAP-Server für die Benutzerauthentifizierung.
- Erstellen Sie einen Adresspool für VPN-Benutzer.
- Laden Sie AnyConnect-Images für verschiedene Plattformen hoch.

a) SSL-Zertifikat importieren

Zertifikate sind für die Konfiguration von AnyConnect unerlässlich. Um Fehler in Webbrowsern zu vermeiden, muss das Zertifikat über eine Erweiterung für den alternativen Antragstellernamen mit dem DNS-Namen und/oder der IP-Adresse verfügen.

Hinweis: Nur registrierte Cisco Benutzer haben Zugriff auf interne Tools und Fehlerinformationen.

Die manuelle Zertifikatregistrierung unterliegt folgenden Einschränkungen:

- Auf FTD benötigen Sie das Zertifizierungsstellenzertifikat, bevor Sie die CSR-Anfrage erstellen.
- Wenn der CSR extern generiert wird, schlägt die manuelle Methode fehl, es muss eine andere Methode verwendet werden (PKCS12).

Es gibt verschiedene Methoden, um ein Zertifikat auf der FTD-Appliance zu erhalten. Die sichere und einfache Methode besteht jedoch darin, eine Zertifikatsanforderung (Certificate Signing Request, CSR) zu erstellen, sie mit einer Zertifizierungsstelle (Certificate Authority, CA) zu signieren und dann ein Zertifikat zu importieren, das für einen öffentlichen Schlüssel ausgestellt wurde, der in der CSR enthalten war. So gehen Sie vor:

- Gehe zu Objects > Object Management > PKI > Cert Enrollment klicken Sie auf **Add Certificate Enrollment** (Zertifikatregistrierung hinzufügen).

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:

```
EPUWYTGngteD6JFITtn..STZXR  
YfPCiIB7g  
BMAV7Gzdc4VspS6lJrAhbiiaw  
dBiIQmsBeFz9JkF4..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

- Auswählen Enrollment Type und fügen Sie ein Zertifikat der Zertifizierungsstelle (Certificate Authority, CA) ein (das Zertifikat, das zum Signieren des CSR verwendet wird).
- Wechseln Sie dann zur zweiten Registerkarte, und wählen Sie Custom FQDN und füllen Sie alle erforderlichen Felder aus, z. B.:

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

- Wählen Sie auf der dritten Registerkarte *Key Type*, wählen Sie Name und Größe. Für RSA sind mindestens 2048 Bit erforderlich.
- Klicken Sie auf Speichern und gehen Sie zu *Devices > Certificates > Add > New Certificate*.
- Wählen Sie *Device* und unter *Cert Enrollment* den soeben erstellten Vertrauenspunkt auswählen, klicken Sie auf *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

- Klicken Sie später neben dem Namen des Vertrauenspunkts auf  Symbol, dann Yes und anschließend CSR auf CA kopieren und signieren. Das Zertifikat muss über dieselben Attribute wie ein normaler HTTPS-Server verfügen.
- Nachdem Sie das Zertifikat von CA im Base64-Format erhalten haben, wählen Sie es auf der Festplatte aus, und klicken Sie auf Import. Wenn dies erfolgreich ist, sehen Sie Folgendes:

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

b) Konfigurieren des RADIUS-Servers

- Gehe zu **Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group**.
- Geben Sie den Namen ein, und fügen Sie die IP-Adresse zusammen mit dem geheimen Schlüssel hinzu. Klicken Sie auf **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

- Danach sehen Sie den Server auf der Liste:

Name	Value	
RadiusServer	1 Server	

c) Erstellen eines Adresspools für VPN-Benutzer

- Gehe zu **Objects > Object Management > Address Pools > Add IPv4 Pools**.
- Legen Sie den Namen und den Bereich, Maske ist nicht erforderlich:

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-Profil erstellen

- Laden Sie den Profil-Editor von der Cisco Website herunter, und öffnen Sie ihn.
- Gehe zu **Server List > Add...**
- Geben Sie den Anzeigenamen und den FQDN ein. Einträge werden in der Serverliste angezeigt:

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

- Klicken Sie auf **OK** und **File > Save as...**

e) AnyConnect-Images hochladen

- Laden Sie Paketbilder von der Cisco Website herunter.
- Gehe ZU **Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File**.
- Geben Sie den Namen ein, und wählen Sie die PKG-Datei auf der Festplatte aus. Klicken Sie auf **Save**:

Edit AnyConnect File ?

Name:*

File Name:*

File Type:*

Description:

- Fügen Sie weitere Pakete entsprechend Ihrer Anforderungen hinzu.

2. Assistent für den Remotezugriff

- Gehe ZU **Devices > VPN > Remote Access > Add a new configuration**.
- Nennen Sie das Profil, und wählen Sie ein FTD-Gerät:

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 

- Geben Sie im Schritt Verbindungsprofil Folgendes ein: **Connection Profile Name**, wählen Sie **Authentication Server** und **Address Pools** die Sie zuvor erstellt haben:

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](#)

- Klicken Sie **Edit Group Policy** und wählen Sie auf der Registerkarte AnyConnect Client Profile, und klicken Sie dann auf **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](#).

- Wählen Sie auf der nächsten Seite AnyConnect-Bilder aus, und klicken Sie auf 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 ▾

- Wählen Sie auf dem nächsten Bildschirm **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.

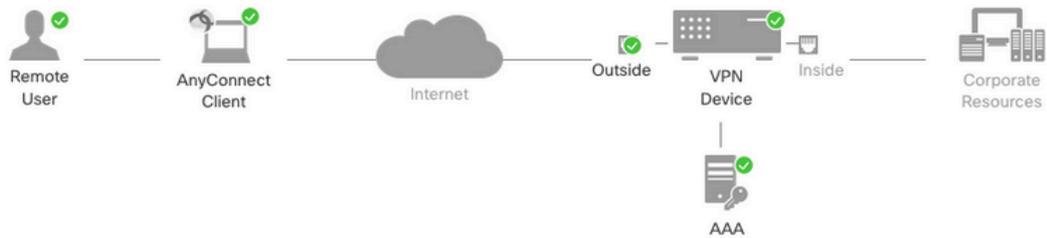
Certificate Enrollment:* +

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.

- Wenn alles richtig konfiguriert ist, können Sie auf **Finish** und dann **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'

- Dadurch wird die gesamte Konfiguration zusammen mit Zertifikaten und AnyConnect-Paketen in die FTD-Appliance kopiert.

Verbindung

Um eine Verbindung zu FTD herzustellen, müssen Sie einen Browser öffnen, indem Sie den DNS-Namen oder die IP-Adresse eingeben, die auf die externe Schnittstelle verweist. Anschließend melden Sie sich mit den Anmeldeinformationen an, die im RADIUS-Server gespeichert sind, und führen die Anweisungen auf dem Bildschirm aus. Nach der Installation von AnyConnect müssen Sie dieselbe Adresse in das AnyConnect-Fenster eingeben und auf Connect.

Einschränkungen

Derzeit nicht unterstützt auf FTD, aber verfügbar auf ASA:

- Die Schnittstellenauswahl auf dem RADIUS-Server wird von Firepower Threat Defense 6.2.3 oder früheren Versionen nicht unterstützt. Die Schnittstellenoption wird bei der Bereitstellung ignoriert.
- Ein RADIUS-Server mit aktivierter dynamischer Autorisierung erfordert Firepower Threat

- Defense6.3 oder höher, damit die dynamische Autorisierung funktioniert.
- FTDposture VPN unterstützt keine Gruppenrichtlinienänderungen durch dynamische Autorisierung oder RADIUS-Autorisierungsänderung (CoA).
 - AnyConnect-Anpassung (Erweiterung: Cisco Bug-ID [CSCvq87631](#))
 - AnyConnect-Skripte
 - AnyConnect-Lokalisierung
 - WSA-Integration
 - Gleichzeitige dynamische IKEv2-Kryptografiezuordnung für RA und L2L VPN (Erweiterung: Cisco Bug-ID [CSCvr52047](#))
 - AnyConnect-Module (NAM, Hostscan, AMP Enabler, SBL, Umbrella, Web Security usw.) - DART ist standardmäßig installiert (Verbesserungen für AMP Enabler und Umbrella: Cisco Bug-ID [CSCvs03562](#) und Cisco Bug-ID [CSCvs06642](#)).
 - TACACS, Kerberos (KCD-Authentifizierung und RSA SDI)
 - Browser-Proxy

Sicherheitsüberlegungen

Standardmäßig wird das `sysopt connection permit-vpn` deaktiviert. Das bedeutet, dass Sie den Datenverkehr, der aus dem Adresspool an einer externen Schnittstelle stammt, über die Zugriffskontrollrichtlinie zulassen müssen. Obwohl die Vorfilter- oder Zugriffskontrollregel hinzugefügt wird, um nur VPN-Datenverkehr zuzulassen, wird dieser irrtümlicherweise zugelassen, wenn der Klartextdatenverkehr den Regelkriterien entspricht.

Für dieses Problem gibt es zwei Ansätze. Die empfohlene Option für das TAC besteht zum einen darin, Anti-Spoofing (auf ASA wurde es als Unicast Reverse Path Forwarding - uRPF bezeichnet) für eine externe Schnittstelle zu aktivieren, und zum anderen darin, `sysopt connection permit-vpn` um Snort Inspection vollständig zu umgehen. Die erste Option ermöglicht eine normale Überprüfung des Datenverkehrs von und zu VPN-Benutzern.

a) uRPF aktivieren

- Erstellen Sie eine Null-Route für das Netzwerk, das für RAS-Benutzer verwendet wird, wie in Abschnitt C definiert. Gehen Sie zu `Devices > Device Management > Edit > Routing > Static Route` und wählen `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

- Aktivieren Sie anschließend uRPF an der Schnittstelle, an der die VPN-Verbindungen enden. Navigieren Sie zu **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:

Wenn ein Benutzer verbunden ist, wird die 32-Bit-Route für diesen Benutzer in der Routing-Tabelle installiert. Löschen Sie den Textverkehr, der von den anderen, nicht verwendeten IP-Adressen aus dem Pool stammt, und wird vom RFP fallen gelassen. Um eine Beschreibung von Anti-Spoofing Weitere Informationen finden Sie unter [Sicherheitskonfigurationsparameter für Firepower Threat Defense festlegen](#).

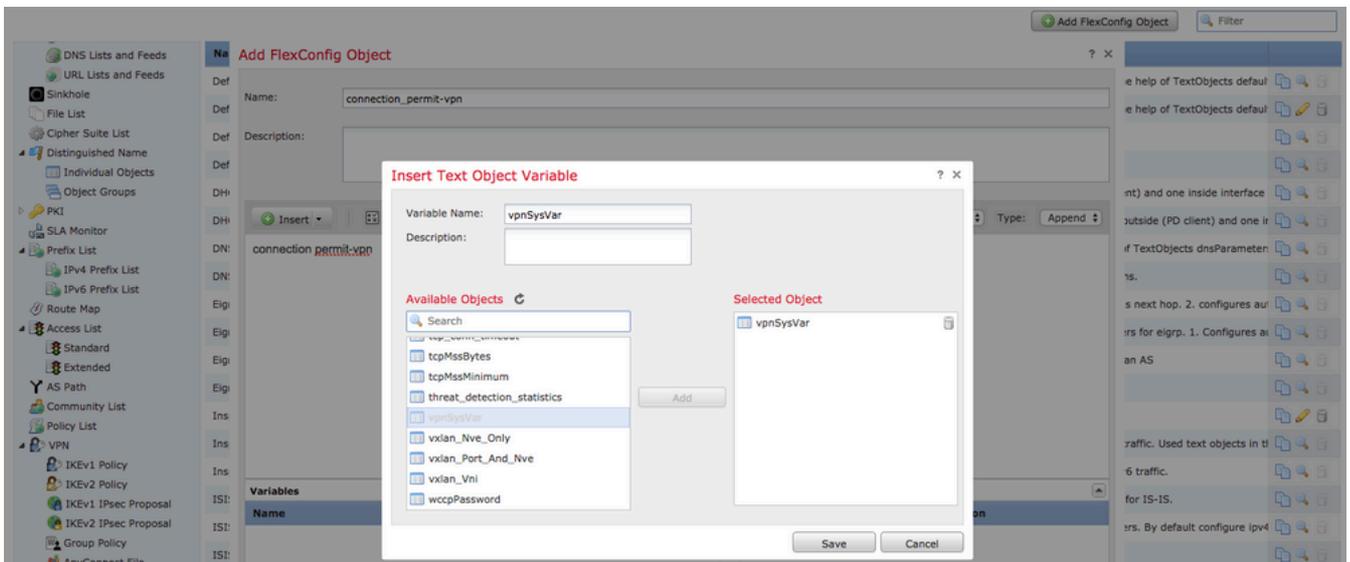
b) Aktivieren `sysopt connection permit-vpn` Option

- Wenn Sie Version 6.2.3 oder höher haben, gibt es eine Option, dies mit dem Assistenten oder unter `Devices > VPN > Remote Access > VPN Profile > Access Interfaces`.

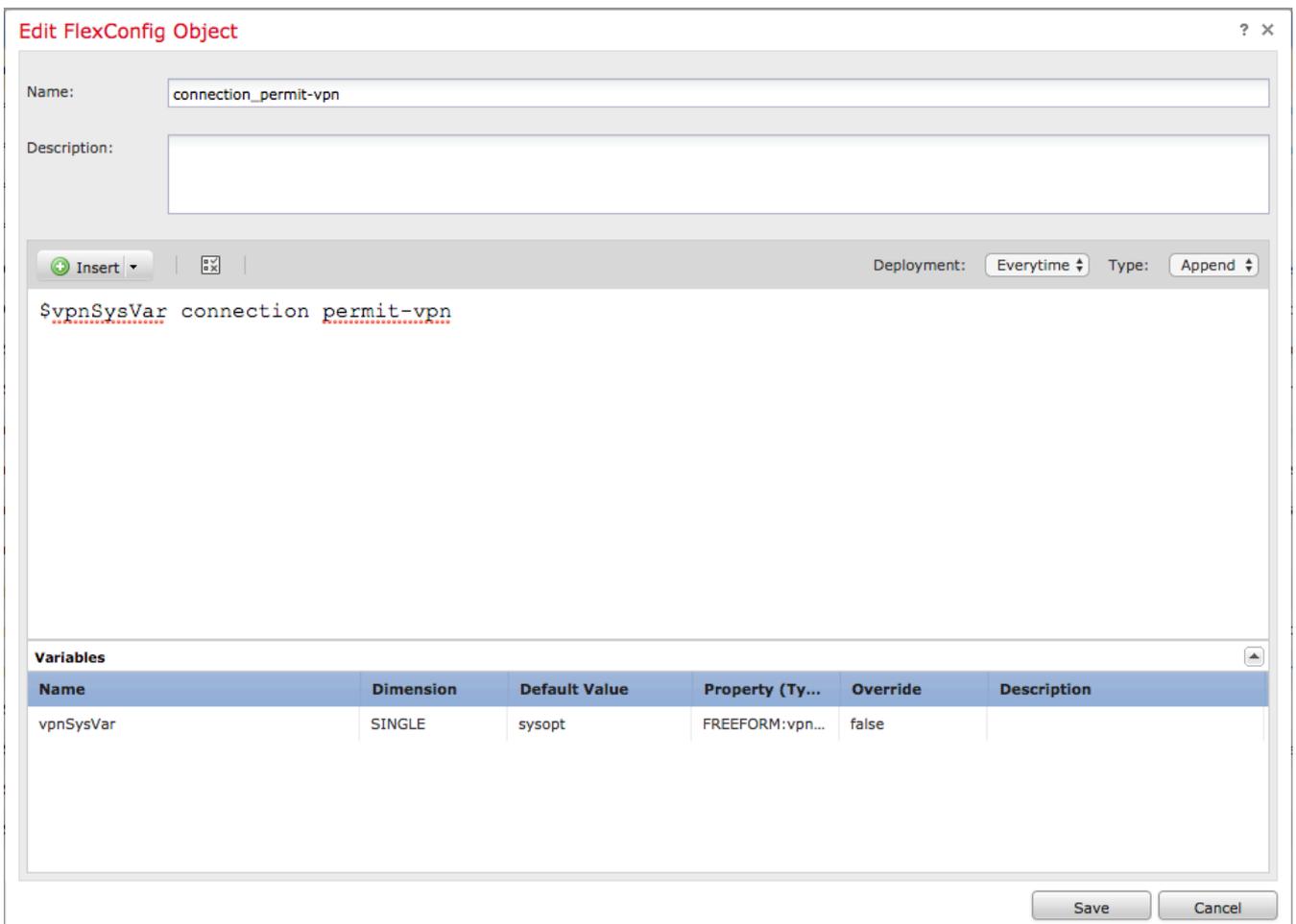
Access Control for VPN Traffic

- 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.

- Versionen vor 6.2.3 finden Sie unter `Objects > Object Management > FlexConfig > Text Object > Add Text Object`.
- Erstellen Sie eine Textobjektvariable, z. B.: `vpnSysVar` ein einzelner Eintrag mit Wert `sysopt`.
- Gehe zu `Objects > Object Management > FlexConfig > FlexConfig Object > Add FlexConfig Object`.
- Erstellen Sie FlexConfig Objekt mit CLI `connection permit-vpn`.
- Fügen Sie die Textobjektvariable in das Feld FlexConfig Objekt in der Kommandozeile mit `$vpnSysVar connection permit-vpn`. Klicken Sie auf `Save`:



- Anwenden des FlexConfigObjekt als **Append** und die Bereitstellung auswählen, **Everytime**:



- Gehe zu **Devices > FlexConfig** und die aktuelle Richtlinie bearbeiten oder eine neue mit **New Policy** - Taste.
- Nur erstellte hinzufügen FlexConfig, klicken Sie auf **Save**.
- Bereitstellung der Konfiguration für die Bereitstellung **sysopt connection permit-vpn**-Befehls auf dem Gerät.

Danach können Sie jedoch nicht mehr die Zugriffskontrollrichtlinie verwenden, um den Datenverkehr der Benutzer zu überprüfen. Sie können weiterhin VPN-Filter oder herunterladbare ACL verwenden, um den Benutzerdatenverkehr zu filtern.

Wenn Sie Paketverluste mit Snort von den VPN-Benutzern sehen, wenden Sie sich an das TAC und verweisen Sie auf die Cisco Bug-ID [CSCvg91399](#).

Zugehörige Informationen

- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.