

Configurazione della VPN ad accesso remoto AnyConnect su FTD

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[1. Prerequisiti](#)

[a\) Importare il certificato SSL](#)

[c\) Creare un pool di indirizzi per gli utenti VPN](#)

[d\) Crea profilo XML](#)

[e\) Caricamento di immagini AnyConnect](#)

[2. Configurazione guidata Accesso remoto](#)

[Connessione](#)

[Limitazioni](#)

[Considerazioni sulla sicurezza](#)

[a\) Attivare uRPF](#)

[b\) Abilitare la connessione a syst allow-vpn Option](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive una configurazione per AnyConnect Remote Access VPN su FTD.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di VPN, TLS e IKEv2
- Autenticazione di base, autorizzazione e accounting (AAA) e conoscenza RADIUS
- Esperienza con Firepower Management Center

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco FTD 7.2.0

- Cisco FMC 7.2.1
- AnyConnect 4.10

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Questo documento offre un esempio di configurazione per Firepower Threat Defense (FTD) versione 7.2.0 e successive, che consente alla VPN ad accesso remoto di utilizzare Transport Layer Security (TLS) e Internet Key Exchange versione 2 (IKEv2). Come client, è possibile usare Cisco AnyConnect, che è supportato su più piattaforme.

Configurazione

1. Prerequisiti

Per eseguire la procedura guidata Accesso remoto in Firepower Management Center:

- Crea un certificato utilizzato per l'autenticazione del server.
- Configurare il server RADIUS o LDAP per l'autenticazione utente.
- Crea pool di indirizzi per gli utenti VPN.
- Caricare immagini AnyConnect per piattaforme diverse.

a) Importare il certificato SSL

I certificati sono essenziali quando si configura AnyConnect. Il certificato deve avere l'estensione Nome alternativo soggetto con nome DNS e/o indirizzo IP per evitare errori nei browser Web.

Nota: solo gli utenti Cisco registrati possono accedere agli strumenti interni e alle informazioni sui bug.

Esistono limitazioni per la registrazione manuale dei certificati:

- Nel FTD è necessario il certificato CA prima di generare il CSR.
- Se la CSR viene generata esternamente, il metodo manuale non riesce, è necessario utilizzare un metodo diverso (PKCS12).

Esistono diversi metodi per ottenere un certificato su un accessorio FTD, ma quello più semplice e sicuro consiste nel creare una richiesta di firma del certificato (CSR), firmarla con un'Autorità di certificazione (CA) e quindi importare un certificato rilasciato per la chiave pubblica, presente in CSR. A tale scopo, eseguire la procedura seguente:

- Vai a **Objects > Object Management > PKI > Cert Enrollment** , fare clic su **Aggiungi registrazione certificato**.

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..StZxr  
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

- Seleziona Enrollment Type e incollare il certificato dell'autorità di certificazione (il certificato utilizzato per firmare il CSR).
- Quindi andare alla seconda scheda e selezionare Custom FQDN e compilare tutti i campi necessari, ad esempio:

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

- Nella terza scheda, selezionare Key Type, scegliere nome e dimensioni. Per RSA, il valore minimo è 2048 bit.
- Fare clic su Save (Salva) e andare a Devices > Certificates > Add > New Certificate.
- Quindi selezionare Devicee al di sotto Cert Enrollment selezionare il trust point appena creato, fare clic su 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

- In seguito, accanto al nome del trust point, fare clic sul collegamento  icona, quindi Yes e quindi copiare CSR in CA e firmarlo. Gli attributi del certificato devono essere uguali a quelli di un server HTTPS normale.
- Dopo aver ricevuto il certificato da CA in formato base64, selezionarlo dal disco e fare clic su Import. Se l'operazione ha esito positivo, sarà possibile visualizzare:

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

b) Configurazione del server RADIUS

- Vai a **Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group**.
- Immettere il nome e aggiungere l'indirizzo IP insieme al segreto condiviso, fare clic su **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

- Il server verrà quindi visualizzato nell'elenco:

Name	Value	
RadiusServer	1 Server	

c) Creare un pool di indirizzi per gli utenti VPN

- Vai a **Objects > Object Management > Address Pools > Add IPv4 Pools**.
- Inserire il nome e l'intervallo, maschera non è necessaria:

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) Crea profilo XML

- Scaricare l'Editor di profili dal sito Cisco e aprirlo.
- Vai a **Server List > Add...**
- Inserire il nome visualizzato e il nome di dominio completo. Nell'elenco dei server sono visualizzate le voci seguenti:

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

- Clic OKE **File > Save as...**

e) Caricamento di immagini AnyConnect

- Scaricare le immagini pkg dal sito Cisco.
- Vai a **Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.**
- Digitare il nome e selezionare il file PKG dal disco, quindi fare clic su **Save:**

Edit AnyConnect File



Name:*

File Name:*

File Type:*

Description:

- Aggiungi altri pacchetti in base alle tue esigenze.

2. Configurazione guidata Accesso remoto

- Vai a **Devices > VPN > Remote Access > Add a new configuration.**
- Assegnare un nome al profilo e selezionare il dispositivo 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 

- Nel passo Profilo connessione digitare **Connection Profile Name**, selezionare il **Authentication Server e Address Pools** creato in precedenza:

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](#)

- Fare clic su **Edit Group Policy** e sulla scheda AnyConnect, selezionare Client Profile, quindi scegliere 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](#).

- Nella pagina successiva, selezionare le immagini AnyConnect e fare clic su 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

- Nella schermata successiva, selezionare **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.

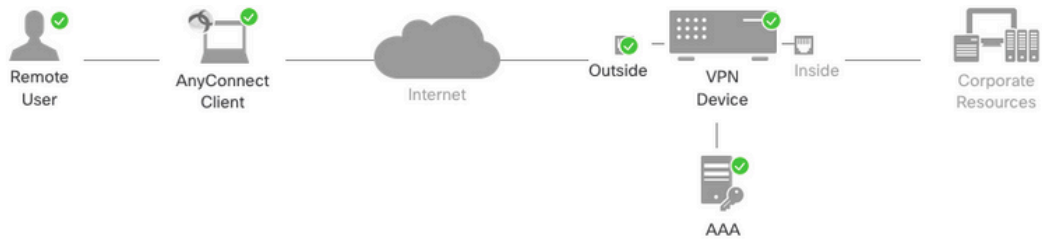
Certificate Enrollment:* +

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.

- Quando tutti gli elementi sono configurati correttamente, è possibile fare clic su Finish e poi 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'

- Questa opzione copia l'intera configurazione con i certificati e i pacchetti AnyConnect sull'accessorio FTD.

Connessione

Per connettersi a FTD è necessario aprire un browser, digitare il nome DNS o l'indirizzo IP che punta all'interfaccia esterna. È quindi possibile eseguire l'accesso con le credenziali archiviate nel server RADIUS e seguire le istruzioni visualizzate. Dopo aver installato AnyConnect, occorre inserire lo stesso indirizzo nella finestra di AnyConnect e fare clic su **Connect**.

Limitazioni

Al momento non è supportato sull'FTD, ma è disponibile sull'ASA:

- La selezione dell'interfaccia nel server RADIUS non è supportata in Firepower Threat Defense 6.2.3 o versioni precedenti. L'opzione di interfaccia viene ignorata durante la distribuzione.
- Un server RADIUS con autorizzazione dinamica richiede Firepower Threat Defense 6.3 o versione successiva per il corretto funzionamento dell'autorizzazione dinamica.

- La VPN FTDposture non supporta la modifica dei criteri di gruppo tramite l'autorizzazione dinamica o la modifica dell'autorizzazione RADIUS (CoA).
- Personalizzazione AnyConnect (miglioramento: Cisco bug ID [CSCvq87631](#))
- Script AnyConnect
- Localizzazione AnyConnect
- Integrazione WSA
- Mappa crittografica dinamica IKEv2 simultanea per RA e VPN L2L (miglioramento: Cisco bug ID [CSCvr52047](#))
- Moduli AnyConnect (NAM, Hostscan, AMP Enabler, SBL, Umbrella, Web Security e così via) - DART è installato per impostazione predefinita (miglioramenti per AMP Enabler e Umbrella: Cisco bug ID [CSCvs03562](#) e Cisco bug ID [CSCvs06642](#)).
- TACACS, Kerberos (autenticazione KCD e RSA SDI)
- Proxy browser

Considerazioni sulla sicurezza

Per impostazione predefinita, il `sysopt connection permit-vpn` è disattivata. Ciò significa che è necessario autorizzare il traffico proveniente dal pool di indirizzi sull'interfaccia esterna tramite i criteri di controllo di accesso. Anche se la regola di prefiltro o di controllo dell'accesso viene aggiunta per consentire solo il traffico VPN, se il traffico in chiaro corrisponde ai criteri della regola, è erroneamente consentito.

Ci sono due approcci a questo problema. Innanzitutto, l'opzione consigliata da TAC è quella di abilitare l'anti-spoofing (sull'appliance ASA era nota come Unicast Reverse Path Forwarding - uRPF) per l'interfaccia esterna e, in secondo luogo, quella di abilitare `sysopt connection permit-vpn` per ignorare completamente l'ispezione Snort. La prima opzione consente una normale ispezione del traffico che va a e da utenti VPN.

a) Attivare uRPF

- Creare una route null per la rete utilizzata per gli utenti di accesso remoto, definita nella sezione C. Andare alla pagina `Devices > Device Management > Edit > Routing > Static Route` e selezionare `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

- Quindi, abilitare uRPF sull'interfaccia a cui terminano le connessioni VPN. Per individuare questa condizione, passare a **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:

Quando un utente è connesso, il percorso a 32 bit viene installato per tale utente nella tabella di routing. Cancella il traffico di testo originato dagli altri indirizzi IP inutilizzati del pool che viene eliminato da uRFP. Per visualizzare una descrizione di **Anti-Spoofing** fare riferimento a [Impostazione dei parametri di configurazione della sicurezza su Firepower Threat Defense](#).

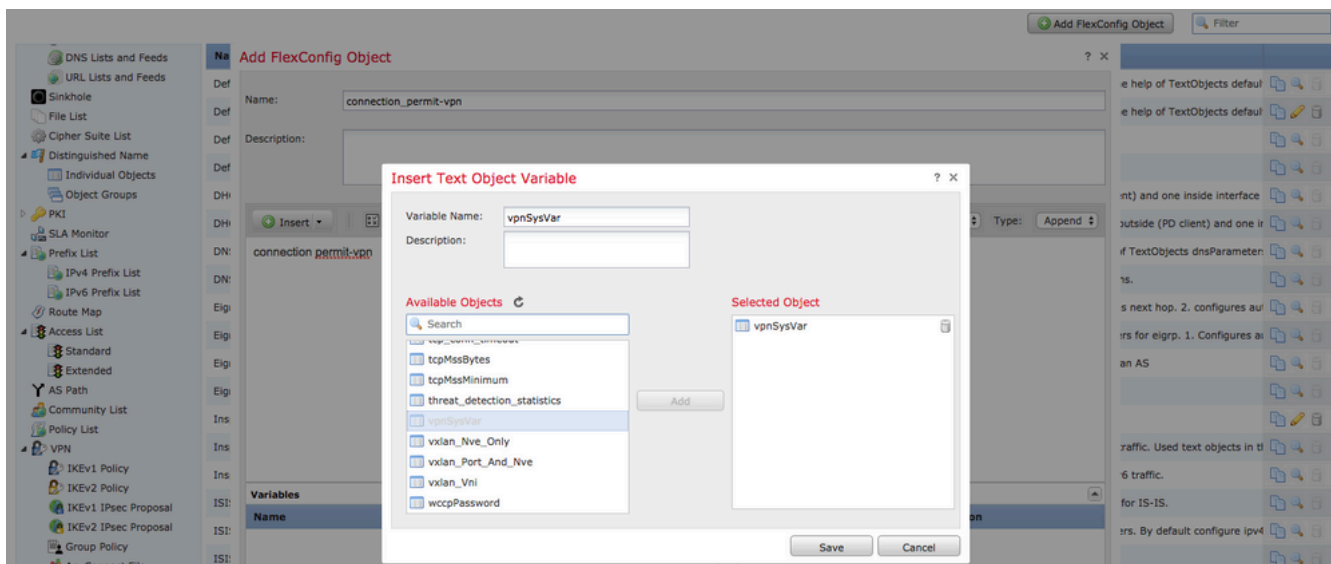
b) Abilita `sysopt connection permit-vpn` Opzione

- Se si dispone della versione 6.2.3 o successiva, è possibile utilizzare la procedura guidata oppure `Devices > VPN > Remote Access > VPN Profile > Access Interfaces`.

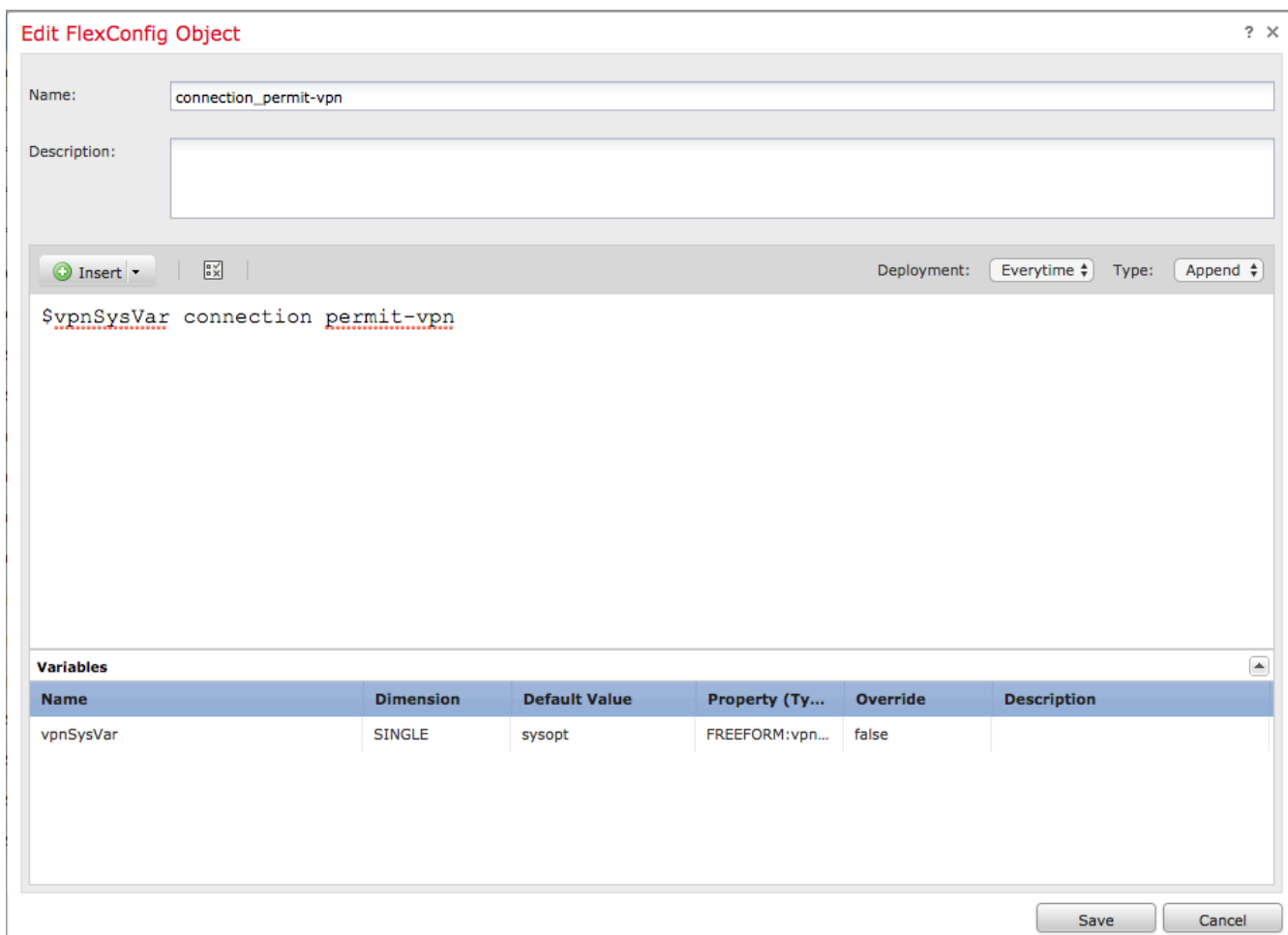
Access Control for VPN Traffic

- 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.

- Per le versioni precedenti alla 6.2.3, andare su `Objects > Object Management > FlexConfig > Text Object > Add Text Object`.
- Creare una variabile oggetto testo, ad esempio: `vpnSysVar` una singola voce con valore `sysopt`.
- Vai a `Objects > Object Management > FlexConfig > FlexConfig Object > Add FlexConfig Object`.
- Creare la `FlexConfig` oggetto con CLI `connection permit-vpn`.
- Inserire la variabile oggetto testo nella `FlexConfig` oggetto nella CLI con `$vpnSysVar connection permit-vpn`. Clic Save:



- Applicare la FlexConfig oggetto come **Append** e selezionare la distribuzione in **Everytime**:



- Vai a **Devices > FlexConfig** e modificare il criterio corrente o crearne uno nuovo con **New Policy** pulsante.
- Aggiungi solo il file creato FlexConfig, fare clic su **Save**.
- Distribuire la configurazione per il provisioning **sysopt connection permit-vpn** sul dispositivo.

In seguito, tuttavia, non è possibile utilizzare i criteri di controllo di accesso per ispezionare il traffico proveniente dagli utenti. È comunque possibile usare il filtro VPN o l'ACL scaricabile per filtrare il traffico degli utenti.

Se vengono visualizzati pacchetti ignorati con Snort dagli utenti VPN, contattare TAC e fare riferimento all'ID bug Cisco [CSCvg91399](#).

Informazioni correlate

- [Supporto tecnico e download Cisco](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).