

FTD에서 AnyConnect 원격 액세스 VPN 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[설정](#)

[1. 사전 요구 사항](#)

[a\) SSL 인증서 가져오기](#)

[c\) VPN 사용자를 위한 주소 풀 생성](#)

[d\) XML 프로파일 만들기](#)

[e\) AnyConnect 이미지 업로드](#)

[2. 원격 액세스 마법사](#)

[연결](#)

[제한 사항](#)

[보안 고려 사항](#)

[a\) uRPF 활성화](#)

[b\) sysopt connection permit-vpn 옵션 활성화](#)

[관련 정보](#)

소개

이 문서에서는 FTD의 AnyConnect 원격 액세스 VPN 구성에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 기본 VPN, TLS 및 IKEv2 지식
- AAA(Basic Authentication, Authorization, and Accounting) 및 RADIUS 지식
- Firepower Management Center를 사용한 경험

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco FTD 7.2.0
- Cisco FMC 7.2.1
- AnyConnect 4.10

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서에서는 원격 액세스 VPN에서 TLS(Transport Layer Security) 및 IKEv2(Internet Key Exchange version 2)를 사용할 수 있도록 하는 FTD(Firepower Threat Defense) 버전 7.2.0 이상의 컨피그레이션 예를 제공합니다. 클라이언트로서 Cisco AnyConnect를 사용할 수 있으며, 이는 여러 플랫폼에서 지원됩니다.

설정

1. 사전 요구 사항

Firepower Management Center에서 원격 액세스 마법사를 통과하려면

- 서버 인증에 사용되는 인증서를 만듭니다.
- 사용자 인증을 위해 RADIUS 또는 LDAP 서버를 구성합니다.
- VPN 사용자를 위한 주소 풀을 생성합니다.
- 다른 플랫폼에 대한 AnyConnect 이미지를 업로드합니다.

a) SSL 인증서 가져오기

인증서는 AnyConnect를 구성할 때 필수적입니다. 웹 브라우저에서 오류를 방지하려면 인증서에 DNS 이름 및/또는 IP 주소가 있는 주체 대체 이름 확장명이 있어야 합니다.

참고: 등록된 Cisco 사용자만 내부 톨 및 버그 정보에 액세스할 수 있습니다.

수동 인증서 등록에는 제한이 있습니다.

- FTD에서 CSR을 생성하기 전에 CA 인증서가 필요합니다.

- CSR이 외부에서 생성된 경우 수동 방법이 실패하고 다른 방법을 사용해야 합니다(PKCS12).

FTD 어플라이언스에서 인증서를 가져오는 몇 가지 방법이 있지만 안전하고 쉬운 방법은 CSR(Certificate Signing Request)을 생성하고 CA(Certificate Authority)로 서명한 다음 CSR에 있는 공개 키에 대해 발급된 인증서를 가져오는 것입니다. 그 방법은 다음과 같습니다.

- 이동 Objects > Object Management > PKI > Cert Enrollment Add Cert Enrollment를 클릭합니다.

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:

```
Ep0WYTGngteb6JFITtn..SZXdR
YfPCiIB7g
BMAV7Gzdc4VspS6lJrAhbiiaw
dBiQIQmsBeFz9JkF4..b3l8Bo
GN+qMa56Y
lt8una2gY4l2O//on88r5lWJlm
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

- 선택 Enrollment Type CA(Certificate Authority) 인증서(CSR 서명에 사용되는 인증서)를 붙여넣습니다.
- 그런 다음 두 번째 탭으로 이동하여 Custom FQDN 다음과 같이 필요한 필드를 모두 입력합니다.

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

- 세 번째 탭에서 Key Type, 이름 및 크기를 선택합니다. RSA의 경우 최소 2048비트입니다.
- Save(저장)를 클릭하고 Devices > Certificates > Add > New Certificate.
- 그런 다음 Device, 및 아래 Cert Enrollment 방금 생성한 신뢰 지점을 선택하고 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

- 나중에 신뢰 지점 이름 옆에 있는  아이콘, YesCSR을 CA에 복사하고 서명합니다. 인증서에는 HTTPS 서버와 동일한 특성이 있어야 합니다.
- CA에서 base64 형식으로 인증서를 받은 후 디스크에서 해당 인증서를 선택하고 Import. 성공하면 다음이 표시됩니다.

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

b) RADIUS 서버 구성

- 이동 Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group.
- 이름을 입력하고 공유 암호와 함께 IP 주소를 추가하려면 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

- 그런 다음 목록에 서버가 표시됩니다.

Name	Value	
RadiusServer	1 Server	

c) VPN 사용자를 위한 주소 풀 생성

- 이동 **Objects > Object Management > Address Pools > Add IPv4 Pools.**
- 이름과 범위를 입력하면 마스크가 필요하지 않습니다.

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

i 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 프로파일 만들기

- Cisco 사이트에서 프로파일 편집기를 다운로드하고 엽니다.
- 이동 **Server List > Add...**
- 표시 이름 및 FQDN을 입력합니다. 서버 목록에 다음 항목이 표시됩니다.

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

- 클릭 OK 및 **File > Save as...**

e) AnyConnect 이미지 업로드

- Cisco 사이트에서 pkg 이미지를 다운로드합니다.
- 이동 Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.
- 이름을 입력하고 디스크에서 PKG 파일을 선택한 다음 Save:

Edit AnyConnect File



Name:*

File Name:*

File Type:*

Description:

- 자체 요구 사항에 따라 패키지를 더 추가합니다.

2. 원격 액세스 마법사

- 이동 Devices > VPN > Remote Access > Add a new configuration.
- 프로파일의 이름을 지정하고 FTD 디바이스를 선택합니다.

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 

- 연결 프로파일 단계에서 다음을 입력합니다 **Connection Profile Name**을 선택합니다. **Authentication Server** 및 **Address Pools** 만들 수 있습니다.

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](#)

- 클릭 **Edit Group Policy AnyConnect** 탭에서 Client Profile를 클릭한 다음 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](#).

- 다음 페이지에서 AnyConnect 이미지를 선택하고 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 ▾

- 다음 화면에서 **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.

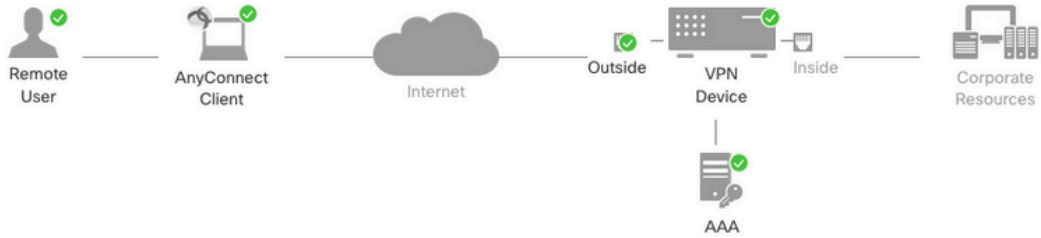
Certificate Enrollment:* +

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.

- 모든 항목이 올바르게 구성되면 Finish 그리고 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'

- 이렇게 하면 전체 컨피그레이션이 인증서 및 AnyConnect 패키지와 함께 FTD 어플라이언스에 복사됩니다.

연결

FTD에 연결하려면 브라우저를 열어야 합니다. 외부 인터페이스를 가리키는 DNS 이름 또는 IP 주소를 입력합니다. 그런 다음 RADIUS 서버에 저장된 자격 증명으로 로그인하고 화면의 지침을 수행합니다. AnyConnect가 설치되면 AnyConnect 창에 동일한 주소를 입력하고 Connect.

제한 사항

현재 FTD에서 지원되지 않지만 ASA에서 사용 가능:

- RADIUS 서버의 인터페이스 선택은 Firepower Threat Defense 6.2.3 이전 버전에서 지원되지 않습니다. 인터페이스 옵션은 구축 과정에서 무시됩니다.
- 동적 권한 부여가 활성화된 RADIUS 서버에서는 동적 권한 부여가 작동하려면 Firepower Threat Defense 6.3 이상이 필요합니다.
- FTDposture VPN은 동적 권한 부여 또는 RADIUS CoA(Change of Authorization)를 통한 그룹 정책 변경을 지원하지 않습니다.

- AnyConnect 사용자 지정(개선 사항: Cisco 버그 ID [CSCvq87631](#))
- AnyConnect 스크립트
- AnyConnect 현지화
- WSA 통합
- RA 및 L2L VPN에 대한 동시 IKEv2 동적 암호화 맵(개선 사항: Cisco 버그 ID [CSCvr52047](#))
- AnyConnect 모듈(NAM, Hostscan, AMP Enabler, SBL, Umbrella, Web Security 등) - DART가 기본적으로 설치됩니다(AMP Enabler 및 Umbrella의 향상된 기능: Cisco 버그 ID [CSCvs03562](#) 및 Cisco 버그 ID [CSCvs06642](#)).
- TACACS, Kerberos(KCD 인증 및 RSA SDI)
- 브라우저 프록시

보안 고려 사항

기본적으로 `sysopt connection permit-vpn` 옵션이 비활성화되어 있습니다. 즉, 액세스 제어 정책을 통해 외부 인터페이스의 주소 풀에서 오는 트래픽을 허용해야 합니다. VPN 트래픽만 허용하기 위해 사전 필터 또는 액세스 제어 규칙이 추가되지만, 일반 텍스트 트래픽이 규칙 기준과 일치하는 경우 잘못 허용됩니다.

이 문제에 대한 두 가지 접근법이 있다. 먼저 TAC의 권장 옵션은 외부 인터페이스에 대해 스푸핑 방지(ASA에서는 Unicast Reverse Path Forwarding - uRPF라고 함)를 활성화하는 것이며, 두 번째는 활성화하는 것입니다 `sysopt connection permit-vpn Snort` 검사를 완전히 우회할 수 있습니다 첫 번째 옵션은 VPN 사용자를 오가는 트래픽에 대한 정상적인 검사를 허용합니다.

a) uRPF 활성화

- C 섹션에 정의된 원격 액세스 사용자에게 사용되는 네트워크에 대해 null 경로를 생성합니다. 다음으로 이동 `Devices > Device Management > Edit > Routing > Static Route` 및 선택 `Add route`

Add Static Route Configuration



Type: IPv4 IPv6

Interface*

(Interface starting with this icon signifies it is available for route leak)

Available Network

Add

- any-ipv4
- FMC
- GW
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast

Selected Network

objvpnusers

Gateway*

Metric:

(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:

Cancel

OK

- 다음으로, VPN 연결이 종료되는 인터페이스에서 uRPF를 활성화합니다. 이 항목을 찾으려면 다음으로 이동합니다. **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

사용자가 연결되면 라우팅 테이블에 해당 사용자에게 대한 32비트 경로가 설치됩니다. uRFP에 의해 삭제된 다른 풀의 미사용 IP 주소에서 오는 텍스트 트래픽을 지웁니다. 에 대한 설명을 보려면 [Anti-Spoofingfirepower Threat Defense에서 보안 컨피그레이션 매개변수 설정을 참조하십시오.](#)

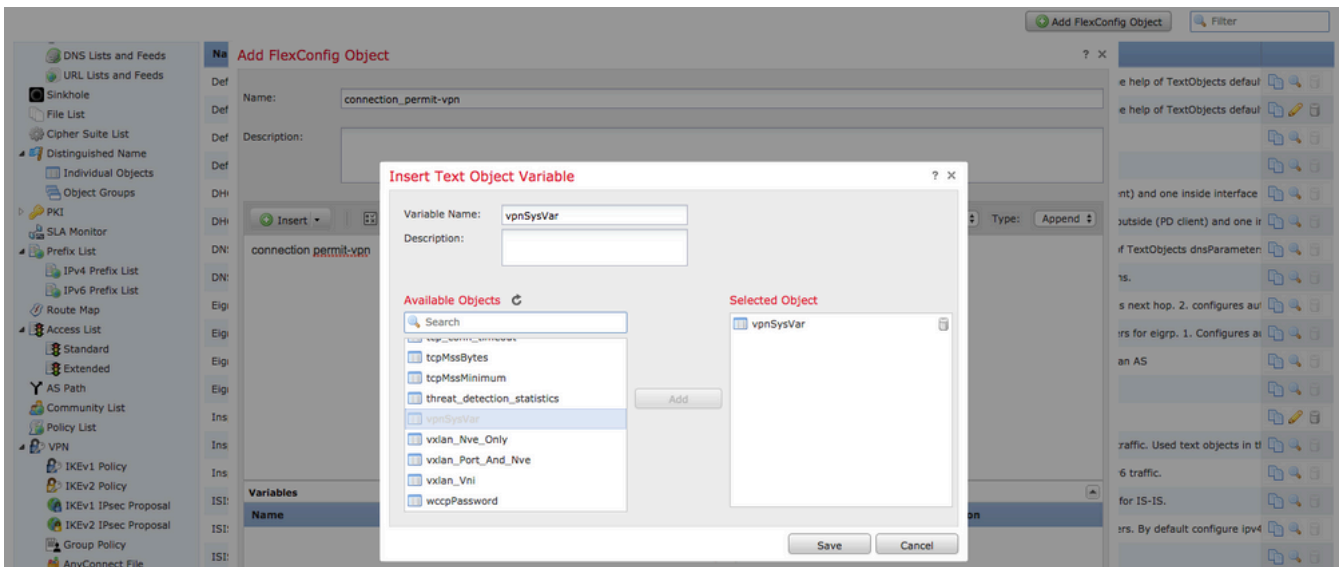
b) 활성화 초sysopt connection permit-vpn 옵션

- 버전 6.2.3 이상이 있는 경우 마법사나 아래에 이를 수행할 수 있는 옵션이 있습니다 Devices > VPN > Remote Access > VPN Profile > Access Interfaces.

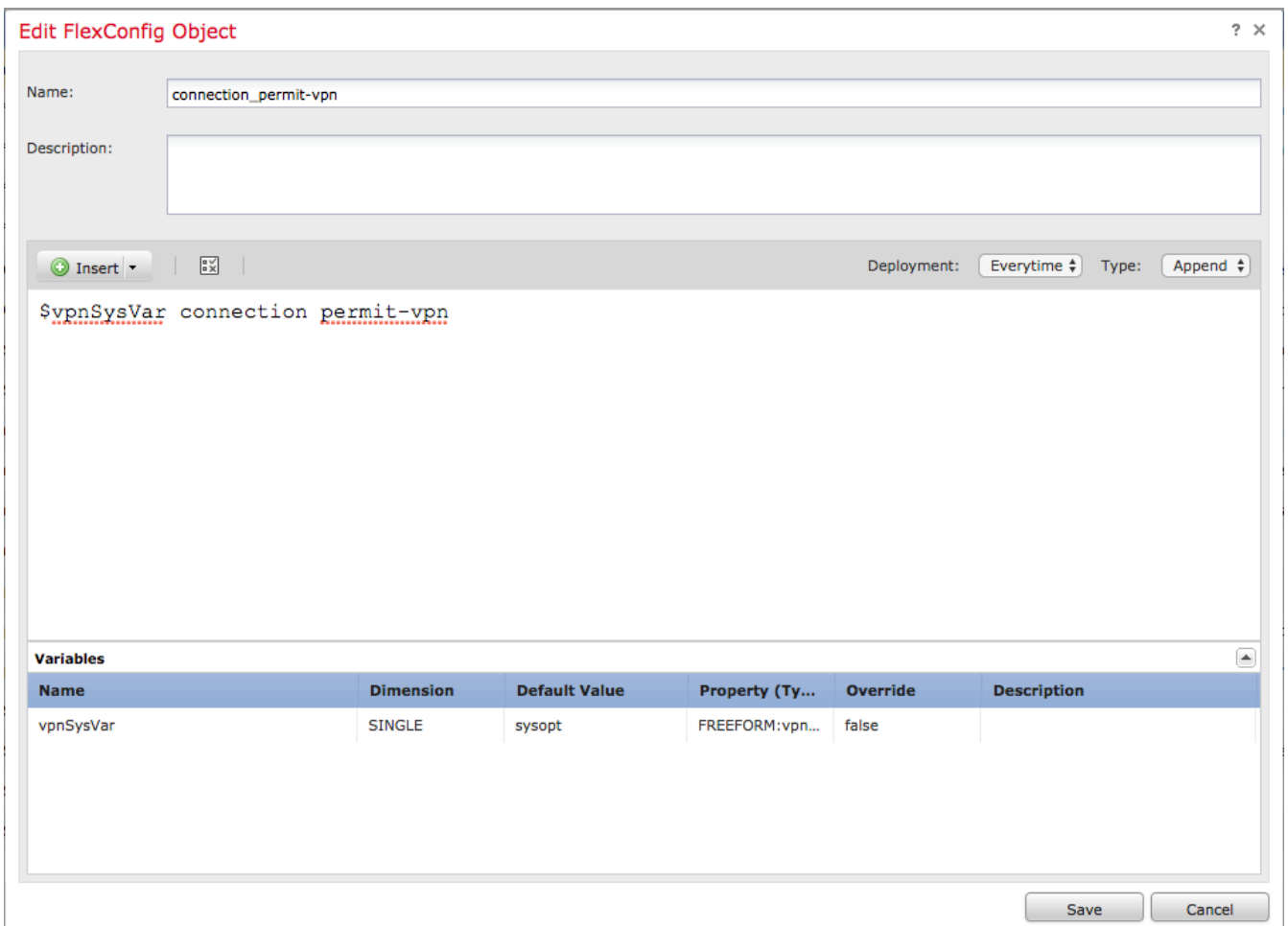
Access Control for VPN Traffic

- 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 이전 버전의 경우 Objects > Object Management > FlexConfig > Text Object > Add Text Object.
- 텍스트 객체 변수를 생성합니다(예: vpnSysVar 값이 있는 단일 항목). sysopt.
- 이동 Objects > Object Management > FlexConfig > FlexConfig Object > Add FlexConfig Object.
- Create(생성) FlexConfig object with CLI(CLI가 있는 개체) connection permit-vpn.
- 텍스트 개체 변수를 FlexConfig CLI에서 \$vpnSysVar connection permit-vpn. 클릭 Save:



- 적용 FlexConfig 객체 **Append** 구축을 선택하여 **Everytime**:



- 이동 **Devices > FlexConfig** 현재 정책을 수정하거나 **New Policy** 버튼을 클릭합니다.
- 만든 항목만 추가 FlexConfig, 클릭 **Save**.
- 프로비저닝할 컨피그레이션 구축 **sysopt connection permit-vpn** 명령을 실행합니다.

그러나 그 이후에는 액세스 제어 정책을 사용하여 사용자로부터 오는 트래픽을 검사할 수 없습니다. VPN 필터 또는 다운로드 가능한 ACL을 계속 사용하여 사용자 트래픽을 필터링할 수 있습니다.

VPN 사용자의 Snort로 삭제된 패킷이 표시되면 TAC에 문의하고 Cisco 버그 ID CSCvg91399를 [참조하십시오](#).

관련 정보

- [Cisco 기술 지원 및 다운로드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.