

FTD에서 AnyConnect VPN 클라이언트 구성: 헤어핀 및 NAT 예외

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[1단계. SSL 인증서 가져오기](#)

[2단계. RADIUS 서버 구성](#)

[3단계. IP 풀 생성](#)

[4단계. XML 프로파일 만들기](#)

[5단계. Anyconnect XML 프로파일 업로드](#)

[6단계. AnyConnect 이미지 업로드](#)

[7단계. 원격 액세스 VPN 마법사](#)

[NAT 예외 및 헤어핀](#)

[1단계. NAT 예외 컨피그레이션](#)

[2단계. 헤어핀 컨피그레이션](#)

[다음을 확인합니다.](#)

[문제 해결](#)

소개

이 문서에서는 FMC에서 관리하는 FTD(Firepower Threat Defense) v6.3에서 Cisco 원격 액세스 VPN 솔루션(AnyConnect)을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 기본 원격 액세스 VPN, SSL(Secure Sockets Layer) 및 IKEv2(Internet Key Exchange version 2) 지식
- AAA(Basic Authentication, Authorization, and Accounting) 및 RADIUS 지식
- 기본 FMC 지식
- 기본 FTD 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco FMC 6.4
- Cisco FTD 6.3
- AnyConnect 4.7

이 문서에서는 FMC(Firepower Management Center)에서 관리하는 FTD(Firepower Threat Defense) 버전 6.3에서 Cisco 원격 액세스 VPN 솔루션(AnyConnect)을 구성하는 절차에 대해 설명합니다.

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 FTD 디바이스의 컨피그레이션을 다룹니다. ASA 컨피그레이션 예를 찾을 경우 <https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/100918-asa-sslvpn-00.html> 문서를 참조하십시오.

제한 사항:

현재 FTD에서는 이러한 기능이 지원되지 않지만 ASA 디바이스에서는 계속 사용할 수 있습니다.

- 이중 AAA 인증(FTD 버전 6.5에서 사용 가능)
- 동적 액세스 정책
- 호스트 스캔
- ISE 상태
- RADIUS CoA
- VPN 로드 밸런서
- 로컬 인증(Firepower 장치 관리자 6.3에서 사용 가능) Cisco 버그 ID [CSCvf92680](#))
- LDAP 특성 맵(FlexConfig, Cisco 버그 ID CSCvd64585를 [통해 사용 가능](#))
- AnyConnect 사용자 지정
- AnyConnect 스크립트
- AnyConnect 현지화
- 애플당 VPN
- SCEP 프록시
- WSA 통합
- SAML SSO(Cisco 버그 ID [CSCvq90789](#))
- RA 및 L2L VPN에 대한 동시 IKEv2 동적 암호화 맵
- AnyConnect 모듈(NAM, Hostscan, AMP Enabler, SBL, Umbrella, Web Security 등). DART는 이 버전에 기본적으로 설치되는 유일한 모듈입니다.
- TACACS, Kerberos(KCD 인증 및 RSA SDI)
- 브라우저 프록시

구성

FMC에서 원격 액세스 VPN 마법사를 통과하려면 다음 단계를 완료해야 합니다.

1단계. SSL 인증서 가져오기

인증서는 AnyConnect를 구성할 때 필수적입니다. SSL 및 IPSec에는 RSA 기반 인증서만 지원됩니다.

ECDSA(Elliptic Curve Digital Signature Algorithm) 인증서는 IPSec에서 지원되지만, ECDSA 기반 인증서를 사용하는 경우 새 AnyConnect 패키지 또는 XML 프로파일을 배포할 수 없습니다.

IPSec에 사용할 수 있지만 XML 프로파일과 함께 AnyConnect 패키지를 사전 구축해야 하며 모든 XML 프로파일 업데이트는 각 클라이언트에서 수동으로 푸시해야 합니다(Cisco 버그 ID CSCtx42595).

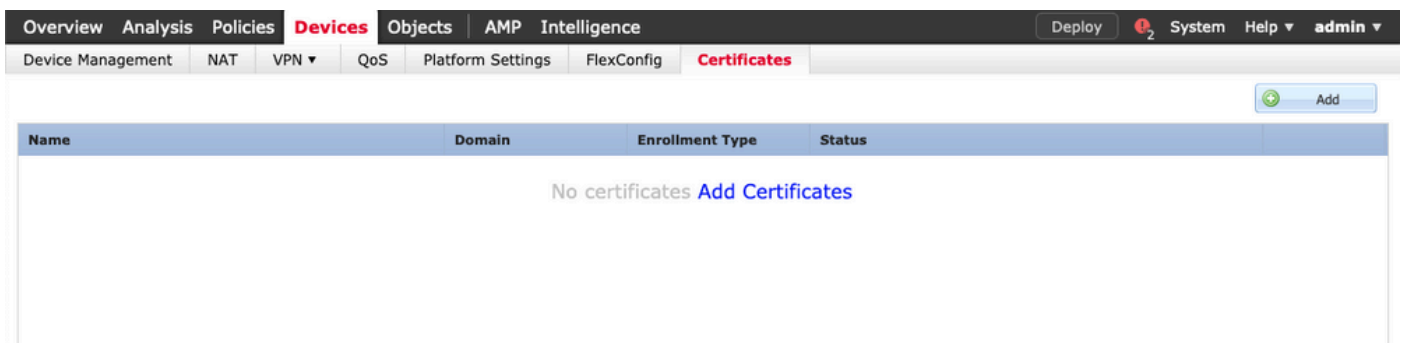
또한 웹 브라우저에서 "신뢰할 수 없는 서버 인증서" 오류가 발생하지 않도록 하려면 인증서에 DNS 이름 및/또는 IP 주소가 있는 CN(Common Name) 확장이 포함되어 있어야 합니다.

참고: FTD 디바이스에서는 CSR(Certificate Signing Request)을 생성하기 전에 CA(Certificate Authority) 인증서가 필요합니다.

- CSR이 외부 서버(예: Windows Server 또는 OpenSSL)에서 생성된 경우, FTD는 수동 키 등록을 지원하지 않으므로 수동 등록 방법이 실패할 수 있습니다.
- 다른 메서드(예: PKCS12)를 사용해야 합니다.

수동 등록 방법으로 FTD 어플라이언스에 대한 인증서를 가져오려면 CSR을 생성하고 CA로 서명한 다음 ID 인증서를 가져와야 합니다.

1. 이미지에 표시된 대로 Devices(디바이스) > Certificates(인증서)로 이동하고 Add(추가)를 선택합니다.



2. 이미지와 같이 장치를 선택하고 새 인증서 등록 개체를 추가합니다.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT VPN QoS Platform Settings FlexConfig **Certificates** Add

Name	Domain	Enrollment Type	Status
No certificates Add Certificates			

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*: FTD-Virtual

Cert Enrollment*: Select a certificate enrollment object

Add Cancel

Add Cert Enrollment

Name* Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: SCEP

Enrollment URL: * http://

Challenge Password:

Confirm Password:

Retry Period: 1 Minutes (Range 1-60)

Retry Count: 10 (Range 0-100)

Fingerprint: Ex: e6f7d542 e355586c a758e7cb bdcddd92

Allow Overrides

Save Cancel

3. 수동 등록 유형을 선택하고 CA 인증서(CSR에 서명할 인증서)를 붙여넣습니다.

Add Cert Enrollment



Name*

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type:

CA Certificate:*

```
/3C4hi07uzuR0ygwKEBaMdg4Dl/z
4x3nk3tTUhYpfbWqWAXM7GNDRVWG9BZ1svk3shDK2Bogklzou6
RqV66G9IE7Z2
xIVrSrJFqhrT795kMb8am8xhb4eXYXxUgJmODIPqZ76RSTAT0+v1
VLSP+vHGm8X
g6wEFsKuZay27a48e/1JG2LgRDraOKt+jwbS7DGSK4mfZsZqhFdQP
LhBNFbyBvb9
dOjUkmdSvzQDRSqSo+HINEm3E8/q20wrtZp04MpAabyhr+hEpeP
VMrhvBOT8h
H8eMjSQjGhhHbuKofVlzQmM0RvGnTB6EKYIvb4CUW8HcgDdDr
mwNgy5mTP9cHa
9Or3RlWRzEa11HE3mHC4Rj6DOnmgufjx+TZRYczownSKLL7LcW1
D18ZclYmfaldC
W2cZuBR0yVdxCvq4#04ISE1BfOWF5d5rAD/bvk2n6xrJl1SLqABMJJ
uslu9KTGH1
bYKEYACKVvETw==
-----END CERTIFICATE-----
```

Allow Overrides

4. [인증서 매개변수] 탭을 선택하고 [FQDN 포함] 필드에 대해 "사용자 정의 FQDN"을 선택하고 이 이미지에 표시된 인증서 세부 정보를 채웁니다.

Add Cert Enrollment ? X

Name*

Description

CA Information **Certificate Parameters** Key Revocation

Include FQDN:

Include Device's IP Address:

Common Name (CN):

Organization Unit (OU):

Organization (O):

Locality (L):

State (ST):

Country Code (C):

Email (E):

Include Device's Serial Number

Allow Overrides

5. 키 탭을 선택하고 키 유형을 선택하면 이름과 크기를 선택할 수 있습니다. RSA의 경우 2048바이트가 최소 요구 사항입니다.

6. 저장을 선택하고 장치를 확인한 후 인증서 등록에서 방금 생성한 신뢰 지점을 선택하고 추가를 선택하여 인증서를 배포합니다.

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: Anyconnect-certificate

Enrollment Type: Manual

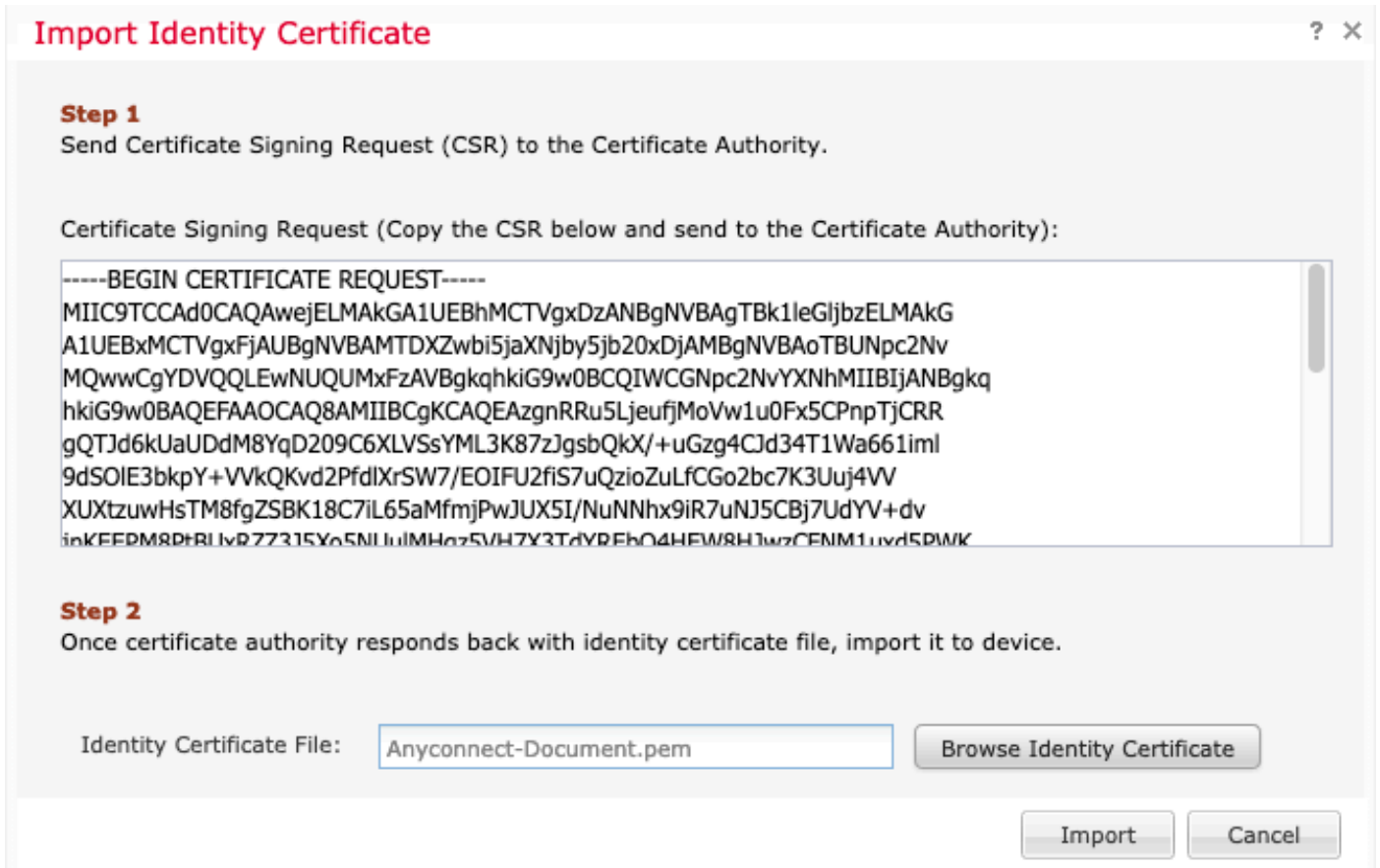
SCEP URL: NA

7. 상태 열에서 ID 아이콘을 선택하고 예를 선택하여 이미지에 표시된 CSR을 생성합니다.

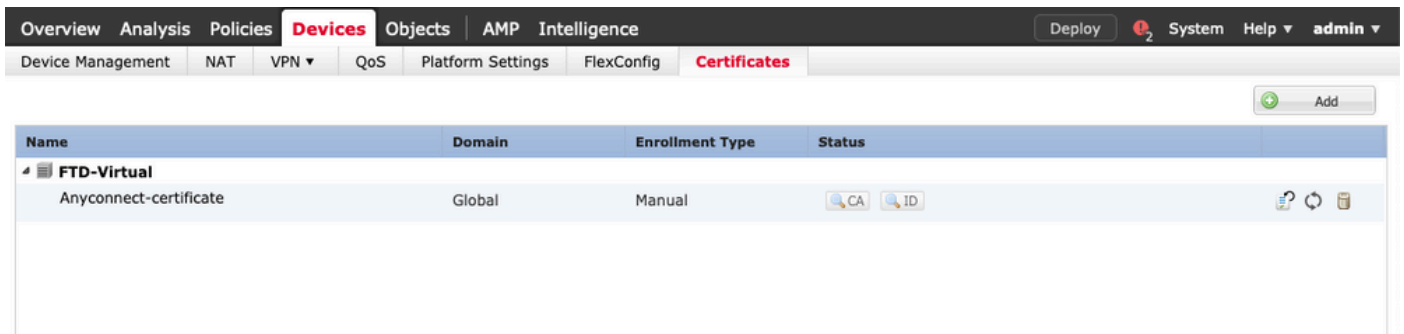
Name	Domain	Enrollment Type	Status
Anyconnect-certificate	Global	Manual	CA ID Identity certificate import required

8. CSR을 복사하고 원하는 CA로 서명합니다(예: GoDaddy 또는 DigiCert).

9. CA에서 ID 인증서를 받으면(base64 형식이어야 함) Browse Identity Certificate(ID 인증서 찾아 보기)를 선택하고 로컬 컴퓨터에서 인증서를 찾습니다. Import(가져오기)를 선택합니다.



10. 가져온 CA 및 ID 인증서 세부사항을 모두 표시할 수 있습니다.



2단계. RADIUS 서버 구성

FMC에서 관리하는 FTD 디바이스에서는 로컬 사용자 데이터베이스가 지원되지 않으며 RADIUS 또는 LDAP와 같은 다른 인증 방법을 사용해야 합니다.

1. 그림과 같이 Objects(개체) > Object Management(개체 관리) > RADIUS Server Group(RADIUS 서버 그룹) > Add RADIUS Server Group(RADIUS 서버 그룹 추가)으로 이동합니다.

Add RADIUS Server Group



Name:*

Description:

Group Accounting Mode: ▼

Retry Interval:* (1-10) Seconds

Realms: ▼


Enable authorize only

Enable interim account update

Interval:* (1-120) hours

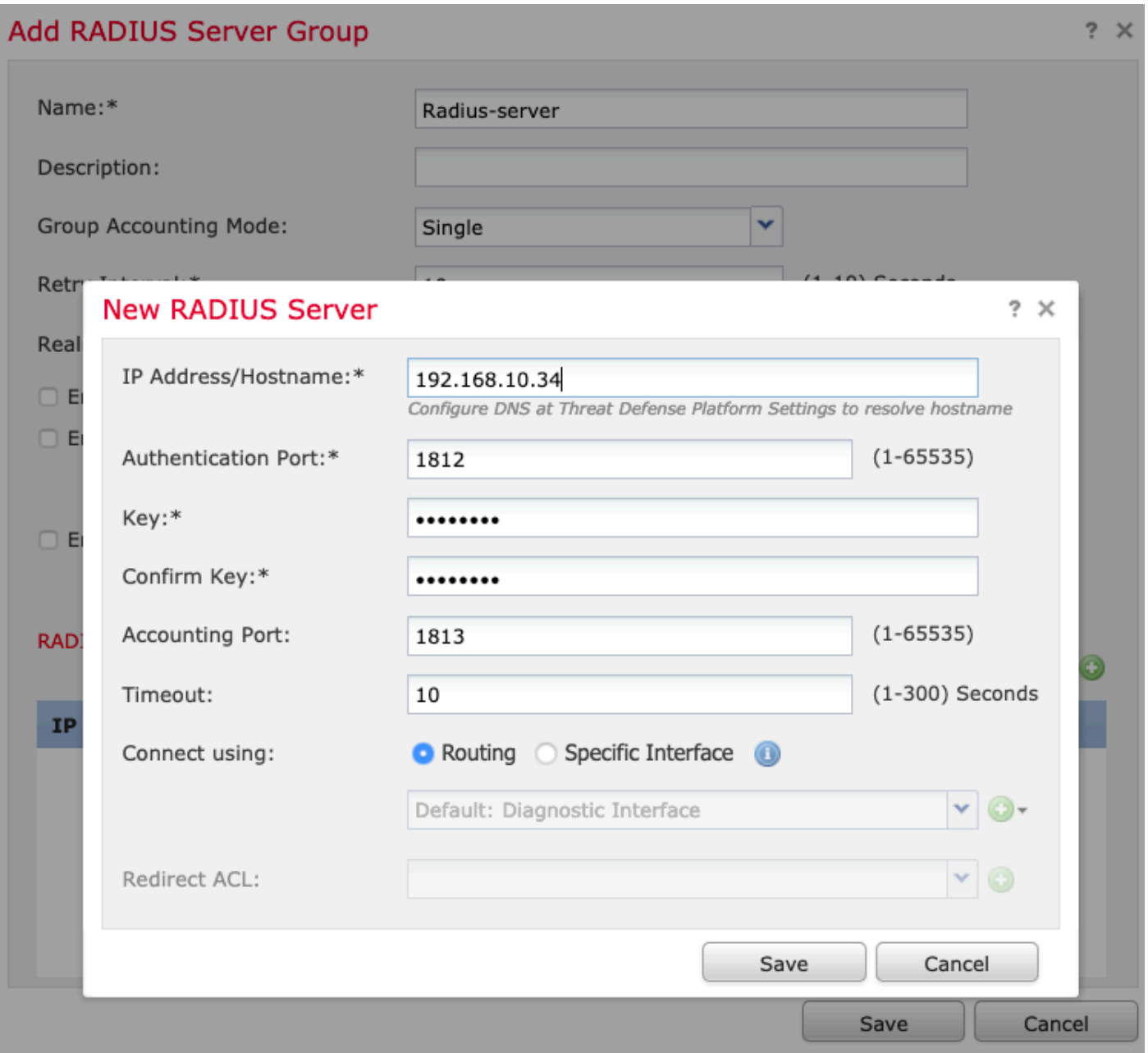
Enable dynamic authorization

Port:* (1024-65535)

RADIUS Servers (Maximum 16 servers) 

IP Address/Hostname	
No records to display	

2. Radius 서버 그룹에 이름을 지정하고 공유 암호와 함께 Radius 서버 IP 주소를 추가합니다 (FTD를 Radius 서버와 페어링하는 데 공유 암호가 필요함). 이미지에 표시된 대로 이 양식이 완료 되면 Save(저장)를 선택합니다.



3. 이제 이미지에 표시된 대로 RADIUS 서버 정보를 Radius 서버 목록에서 사용할 수 있습니다.

Add RADIUS Server Group



Name:* Radius-server

Description:

Group Accounting Mode: Single

Retry Interval:* 10 (1-10) Seconds

Realms:

Enable authorize only

Enable interim account update

Interval:* 24 (1-120) hours

Enable dynamic authorization

Port:* 1700 (1024-65535)

RADIUS Servers (Maximum 16 servers)

IP Address/Hostname		
192.168.10.34		

Save Cancel

3단계. IP 풀 생성

1. Objects(개체) > Object Management(개체 관리) > Address Pools(주소 풀) > Add IPv4 Pools(IPv4 풀 추가)로 이동합니다.

2. IP 주소의 이름과 범위를 지정합니다. 마스크 필드는 필요하지 않지만 이미지에 표시된 대로 지정할 수 있습니다.

Add IPv4 Pool



Name*

IPv4 Address Range*
Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask

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

4단계. XML 프로파일 만들기

1. Cisco.com에서 프로파일 편집기 도구를 다운로드하고 응용 프로그램을 실행합니다.
2. 프로파일 편집기 애플리케이션에서, 이미지에 표시된 대로 서버 목록으로 이동하여 추가를 선택합니다.

VPN

- Preferences (Part 1)
- Preferences (Part 2)
- Backup Servers
- Certificate Pinning
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List

Server List

Hostname	Host Address	User Group	Backup Server List	SCEP	Mobile Settings	Certificate Pins

Note: it is highly recommended that at least one server be defined in a profile

3. 표시 이름, FQDN(정규화된 도메인 이름) 또는 IP 주소를 지정하고 이미지에 표시된 대로 OK(확인)를 선택합니다.

Server Load Balancing Servers SCEP Mobile Certificate Pinning

Primary Server

Display Name (required)

FQDN or IP Address / User Group

Group URL

Connection Information

Primary Protocol

ASA gateway

Auth Method During IKE Negotiation

IKE Identity (IOS gateway only)

Backup Servers

Host Address	
<input type="text"/>	<input type="button" value="Add"/>
	<input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Delete"/>

4. 이제 서버 목록 메뉴에 항목이 표시됩니다.

- VPN
- Preferences (Part 1)
- Preferences (Part 2)
- Backup Servers
- Certificate Pinning
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List**

Server List
Profile: Untitled

Hostname	Host Address	User Group	Backup Server ...	SCEP	Mobile Settings	Certificate Pins
Corporate - FTD (SSL)	vpn.cisco.com	ssl	-- Inherited --			

Note: it is highly recommended that at least one server be defined in a profile.


5. 파일 > 다른 이름으로 저장으로 이동합니다.

참고: 확장자가 .xml인 쉽게 식별할 수 있는 이름으로 프로파일을 저장합니다.

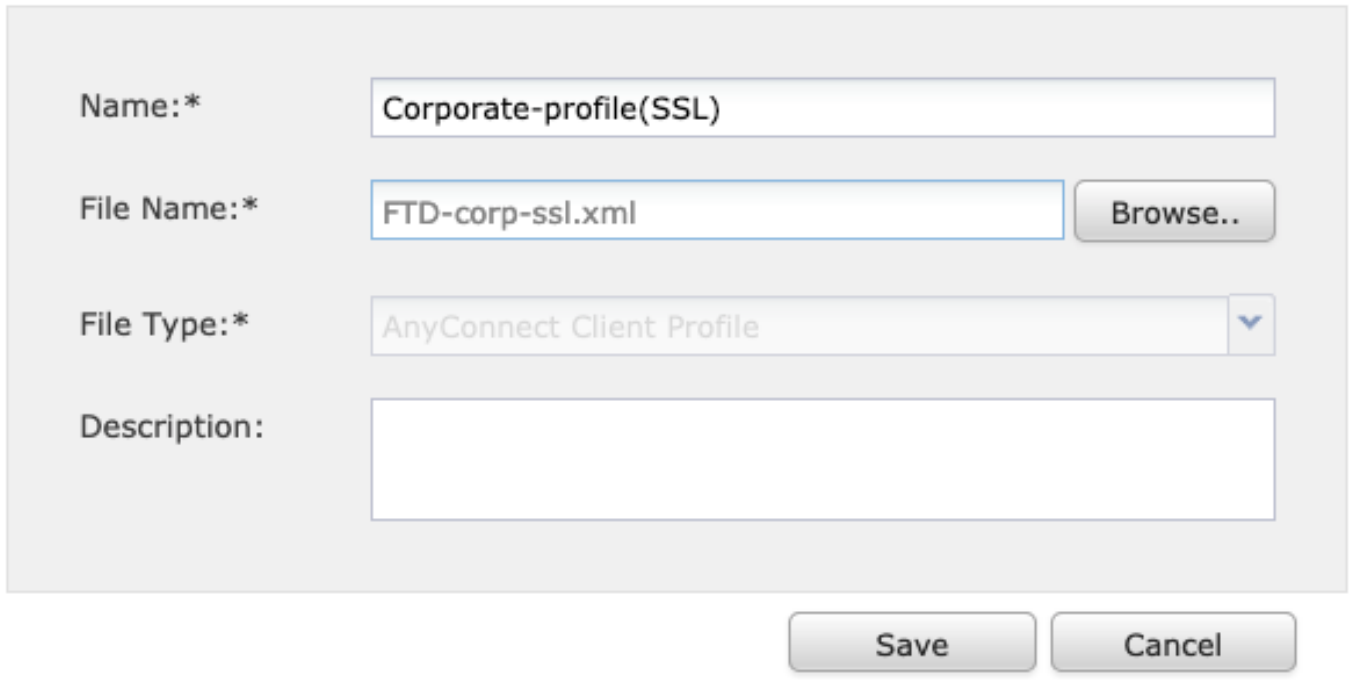
5단계. Anyconnect XML 프로파일 업로드

1. FMC에서 Objects(개체) > Object Management(개체 관리) > VPN > AnyConnect File(AnyConnect 파일) > Add AnyConnect File(AnyConnect 파일 추가)로 이동합니다.

2. 객체에 이름을 지정하고 Browse를 클릭하고 로컬 시스템에서 클라이언트 프로파일을 찾은 다음 Save를 선택합니다.

 주의: Anyconnect 클라이언트 프로파일을 파일 유형으로 선택해야 합니다.

Add AnyConnect File



Name:* Corporate-profile(SSL)

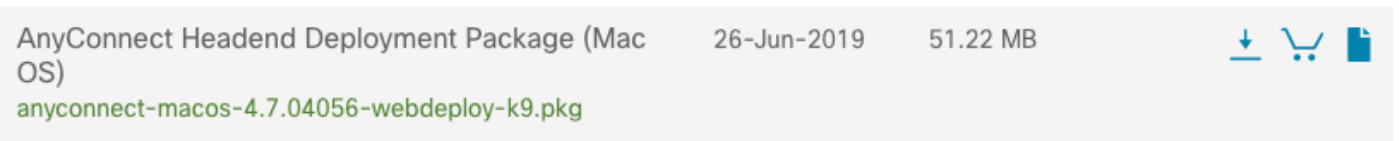
File Name:* FTD-corp-ssl.xml

File Type:* AnyConnect Client Profile

Description:

6단계. AnyConnect 이미지 업로드

1. Cisco 다운로드 웹 페이지에서 webdeploy(.pkg) 이미지를 다운로드합니다.



2. Objects(개체) > Object Management(개체 관리) > VPN > AnyConnect File(AnyConnect 파일) > Add AnyConnect File(AnyConnect 파일 추가)로 이동합니다.

3. Anyconnect 패키지 파일에 이름을 지정하고 파일이 선택된 후 로컬 시스템에서 .pkg 파일을 선택합니다.

4. 저장을 선택합니다.

Add AnyConnect File

Name:*

File Name:*

File Type:*

Description:

참고: 요구 사항에 따라 추가 패키지를 업로드할 수 있습니다(Windows, Mac, Linux).

7단계. 원격 액세스 VPN 마법사

이전 단계를 기반으로 원격 액세스 마법사를 따라 수행할 수 있습니다.

1. Devices(디바이스) > VPN(VPN) > Remote Access(원격 액세스)로 이동합니다.
2. 원격 액세스 정책의 이름을 지정하고 사용 가능한 디바이스에서 FTD 디바이스를 선택합니다.

Remote Access VPN Policy Wizard

1 Policy Assignment | 2 Connection Profile | 3 AnyConnect | 4 Access & Certificate | 5 Summary

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	Selected Devices
<input type="text" value="Search"/> FTD-Virtual	FTD-Virtual

Before You Start

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

Authentication Server
 Configure [Realm](#) or [RADIUS Server Group](#) to authenticate VPN clients.

AnyConnect Client Package
 Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface
 Interfaces should be already configured on targeted [devices](#) so that they can be used as a security zone or interface group to enable VPN access.

3. 연결 프로파일 이름(연결 프로파일 이름은 터널 그룹 이름)을 지정하고 이미지에 표시된 대로 인증 서버 및 주소 풀을 선택합니다.

Remote Access VPN Policy Wizard

1 Policy Assignment 2 **Connection Profile** 3 AnyConnect 4 Access & Certificate 5 Summary

Remote User — AnyConnect Client — Internet — VPN Device (Outside/Inside) — Corporate Resources

AAA

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:*
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: (v)

Authentication Server:* (+) (Realm or RADIUS)

Authorization Server: (+) (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 (RADIUS only) (i)

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools: (pencil)

IPv6 Address Pools: (pencil)

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](#)

Back Next Cancel

4. 그룹 정책을 생성하려면 + 기호를 선택합니다.

Add Group Policy



Name:* RemoteAccess-GP

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

VPN Tunnel Protocol:

Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

SSL

IPsec-IKEv2

Save

Cancel

5. (선택 사항) 로컬 IP 주소 풀은 그룹 정책 기반으로 구성할 수 있습니다. 구성되지 않은 경우 연결 프로파일(터널 그룹)에 구성된 풀에서 풀이 상속됩니다.

Add Group Policy

? X

Name:* RemoteAccess-GP

Description:

General AnyConnect Advanced

VPN Protocols



IP Address Pools

Banner

DNS/WINS

Split Tunneling

IP Address Pools:

Name	IP Address Range	
vpn-pool	192.168.55.1-192.168.55.253	 

Save Cancel

6. 이 시나리오에서 모든 트래픽은 터널을 통해 라우팅됩니다. IPv4 스플릿 터널링 정책은 이미지에 표시된 대로 터널을 통해 모든 트래픽을 허용하도록 설정됩니다.

Edit Group Policy



Name: *

Description:

General AnyConnect Advanced

VPN Protocols
IP Address Pools
Banner
DNS/WINS
Split Tunneling

IPv4 Split Tunneling:

IPv6 Split Tunneling:

Split Tunnel Network List Type: Standard Access List Extended Access List

Standard Access List:

DNS Request Split Tunneling

DNS Requests:

Domain List:

Save Cancel

7. Anyconnect 프로파일의 .xml 프로파일을 선택하고 이미지에 표시된 대로 저장을 선택합니다.

Add Group Policy



Name:*

Description:

General

AnyConnect


Advanced

Profiles

SSL Settings

Connection Settings

AnyConnect profiles contains settings for the VPN client functionality and optional features. FTD deploys the profiles during AnyConnect client connection.

Client 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](#).

Save

Cancel

8. 작동 중인 시스템 요구 사항에 따라 원하는 AnyConnect 이미지를 선택하고 이미지에 표시된 다음 a를 선택합니다.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy 2 System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 **AnyConnect** 4 Access & Certificate 5 Summary

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"/>	MAC4.7	anyconnect-macos-4.7.04056-webdeploy-k9....	Mac OS

Back Next Cancel

9. 보안 영역 및 장치 인증서를 선택합니다.

- 이 컨피그레이션은 VPN이 종료되는 인터페이스와 SSL 연결 시 제공되는 인증서를 정의합니다.

참고: 이 시나리오에서 FTD는 VPN 트래픽을 검사하지 않도록 구성되며, ACP(Access Control Policies) 옵션이 전환됩니다.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 **Access & Certificate** 5 Summary

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

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.

Back Next Cancel

10. 완료를 선택하고 변경 사항을 배치합니다.

- VPN, SSL 인증서 및 AnyConnect 패키지와 관련된 모든 컨피그레이션은 이미지에 표시된 대로 FMC Deploy를 통해 푸시됩니다.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN ▶ Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

Remote Access VPN Policy Configuration

Firepower Management Center will configure an RA VPN Policy with the following settings

Name:	TAC
Device Targets:	FTD-Virtual
Connection Profile:	TAC
Connection Alias:	TAC
AAA:	
Authentication Method:	AAA Only
Authentication Server:	Radius-server
Authorization Server:	Radius-server
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	vpn-pool
Address Pools (IPv6):	-
Group Policy:	RemoteAccess-GP-SSL
AnyConnect Images:	MAC4.7
Interface Objects:	outside
Device Certificates:	Anyconnect-certificate

Additional Configuration Requirements

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- Access Control Policy Update**
An [Access Control](#) rule must be defined to allow VPN traffic on all targeted devices.
- NAT Exemption**
If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.
- DNS Configuration**
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.
- 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 'outside'

Device Identity Certificate Enrollment

Certificate enrollment object 'Anyconnect-certificate' 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.

Back Finish Cancel

NAT 예외 및 헤어핀

1단계. NAT 예외 컨피그레이션

NAT 예외는 VPN 터널(원격 액세스 또는 Site-to-Site)을 통해 트래픽이 이동할 때 인터넷으로 라우팅되는 것을 방지하는 데 사용되는 기본 변환 방법입니다.

이는 내부 네트워크의 트래픽이 변환 없이 터널을 통해 흐르도록 하려는 경우에 필요합니다.

1. 이미지에 표시된 대로 객체 > 네트워크 > 네트워크 추가 > 객체 추가를 이동합니다.

New Network Object

? X

Name: vpn-pool

Description:


Network: Host Range Network FQDN

192.168.55.0/24

Allow Overrides:

Save Cancel

2. Device(디바이스) > NAT로 이동하여 해당 디바이스에서 사용하는 NAT 정책을 선택하고 새 명령문을 생성합니다.

 참고: 트래픽 흐름은 내부에서 외부로 이동합니다.

Add NAT Rule

NAT Rule: Manual NAT Rule Insert: In Category NAT Rules Before

Type: Static Enable

Description:

Interface Objects Translation PAT Pool Advanced

Available Interface Objects

- calo-internal-outside
- inside-zone
- outside-zone
- outsideFW

Source Interface Objects (1)

- inside-zone

Destination Interface Objects (1)

- outside-zone

Add to Source

Add to Destination

OK Cancel

3. 이미지에 표시된 대로 FTD(원본 소스 및 변환된 소스) 뒤의 내부 리소스와 대상을 Anyconnect 사용자의 ip 로컬 풀(원본 대상 및 변환된 대상)로 선택합니다.

Add NAT Rule ? X

NAT Rule: Manual NAT Rule Insert: In Category NAT Rules Before

Type: Static Enable

Description:

Interface Objects **Translation** PAT Pool Advanced

Original Packet	Translated Packet
Original Source:* FTDv-Inside-SUPERNE	Translated Source: Address
Original Destination: Address	Translated Destination: FTDv-Inside-SUPERNE
Original Source Port: <input type="text"/>	Translated Source Port: <input type="text"/>
Original Destination Port: <input type="text"/>	Translated Destination Port: <input type="text"/>

OK Cancel

4. 옵션(이미지에 표시된 대로)을 전환해야 NAT 규칙에서 "no-proxy-arp" 및 "route-lookup"을 활성화하려면 이미지에 표시된 대로 OK를 선택합니다.

Edit NAT Rule ? X

NAT Rule: Manual NAT Rule Insert: In Category NAT Rules Before

Type: Static Enable

Description:

Interface Objects Translation PAT Pool **Advanced**

- Translate DNS replies that match this rule
- Fallthrough to Interface PAT(Destination Interface)
- IPv6
- Net to Net Mapping
- Do not proxy ARP on Destination Interface
- Perform Route Lookup for Destination Interface
- Unidirectional

OK Cancel

5. NAT 예외 컨피그레이션의 결과입니다.



이전 섹션에서 사용된 객체는 아래에 설명된 객체입니다.

Name	FTDv-Inside-SUPERNE		
Description			
Network	<input type="radio"/> Host	<input type="radio"/> Range	<input checked="" type="radio"/> Network
	<input type="radio"/> FQDN		
	10.124.0.0/16		
Allow Overrides	<input type="checkbox"/>		

Name	vpn-pool		
Description			
Network	<input type="radio"/> Host	<input type="radio"/> Range	<input checked="" type="radio"/> Network
	<input type="radio"/> FQDN		
	192.168.55.0/24		
Allow Overrides	<input type="checkbox"/>		

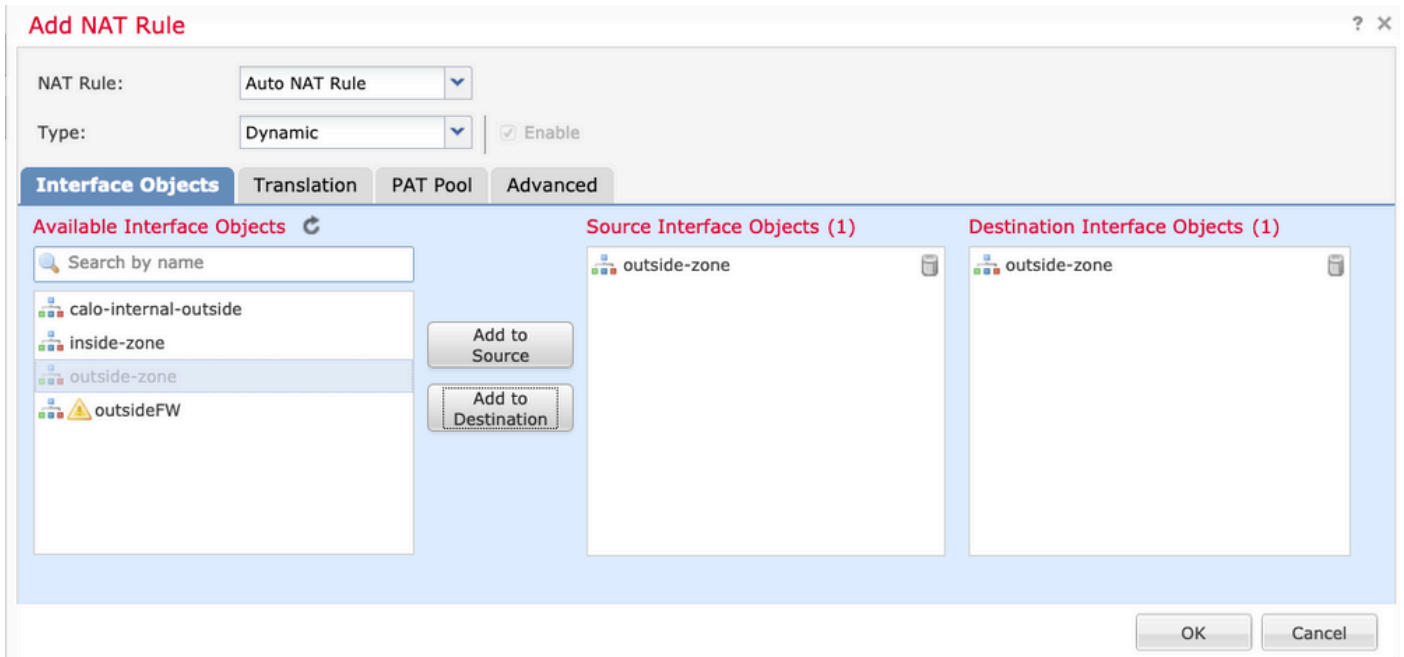
2단계. 헤어핀 컨피그레이션

U-turn이라고도 하는 이 변환 방법은 트래픽이 수신되는 동일한 인터페이스를 통해 트래픽이 이동하도록 허용하는 변환 방법입니다.

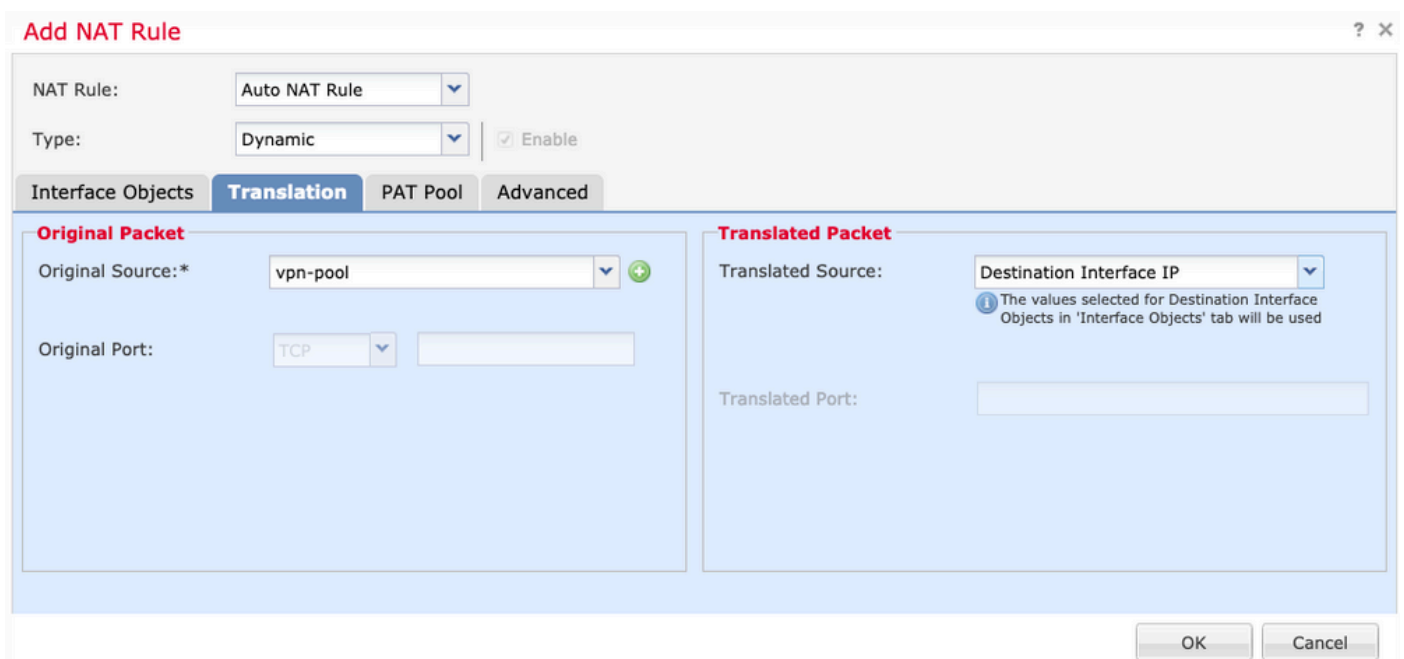
예를 들어 Anyconnect가 전체 터널 스플릿 터널 정책으로 구성된 경우 NAT 예외 정책에 따라 내부 리소스에 액세스합니다. Anyconnect 클라이언트 트래픽이 인터넷의 외부 사이트에 도달하려는 경우, 헤어핀 NAT(또는 U-turn)는 트래픽을 외부에서 외부로 라우팅합니다.

NAT 컨피그레이션을 수행하기 전에 VPN 풀 개체를 만들어야 합니다.

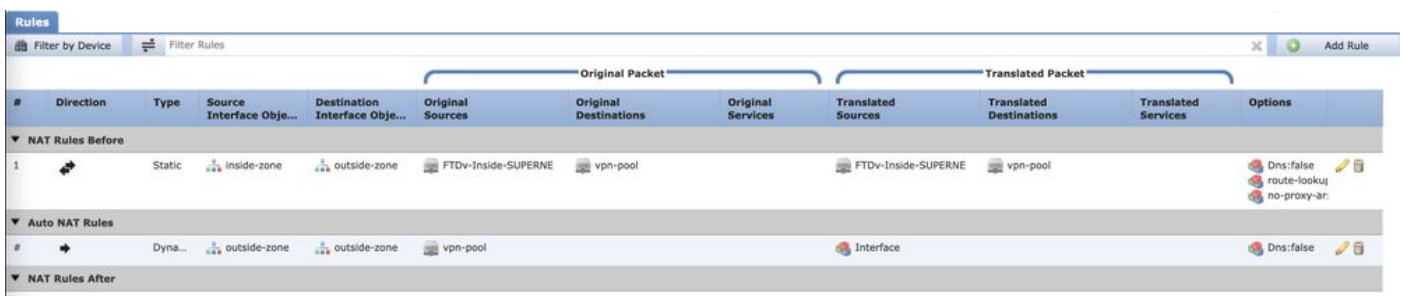
1. 새 NAT 문을 생성하고, NAT Rule 필드에서 Auto NAT Rule을 선택하고 NAT Type으로 Dynamic을 선택합니다.
2. 소스 및 목적지 인터페이스 객체(외부)에 대해 동일한 인터페이스를 선택합니다.



3. Translation(변환) 탭에서 vpn-풀 객체의 Original Source로 선택하고 Destination Interface IP를 Translated Source(변환된 소스)로 선택한 다음 이미지와 같이 OK(확인)를 선택합니다.



4. 이미지에 표시된 대로 NAT 컨피그레이션의 요약입니다.



5. 저장 및 변경 사항 배포를 클릭합니다.

다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

FTD 명령줄에서 이러한 명령을 실행합니다.

- sh crypto ca 인증서
- show running-config ip local pool
- show running-config webvpn
- show running-config tunnel-group
- show running-config group-policy
- show running-config ssl
- show running-config nat

문제 해결

현재 이 구성에 사용할 수 있는 특정 문제 해결 정보가 없습니다.</>

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.