

FTDでのAnyConnect VPN Clientの設定：ヘアピンとNAT除外

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ステップ 1：SSL証明書のインポート](#)

[ステップ 2：RADIUSサーバの設定](#)

[ステップ 3：IPプールの作成](#)

[ステップ 4：XMLプロファイルの作成](#)

[ステップ 5：Anyconnect XMLプロファイルのアップロード](#)

[手順 6：AnyConnectイメージのアップロード](#)

[手順 7：リモートアクセスVPNウィザード](#)

[NAT除外とヘアピン](#)

[ステップ 1：NAT 免除の設定](#)

[ステップ 2：ヘアピン設定](#)

[確認](#)

[トラブルシューティング](#)

はじめに

このドキュメントでは、FMCによって管理されるFirepower Threat Defense(FTD)v6.3でCiscoリモートアクセスVPNソリューション(AnyConnect)を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 基本的なリモートアクセスVPN、Secure Sockets Layer(SSL)、およびInternet Key Exchange version 2(IKEv2)の知識
- 認証、認可、およびアカウントテイング (AAA)、および RADIUS に関する基本的な知識
- FMCの基礎知識
- FTDの基礎知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco FMC 6.4
- Cisco FTD 6.3
- AnyConnect 4.7

このドキュメントでは、Firepower Management Center(FMC)によって管理されるFirepower Threat Defense(FTD)バージョン6.3でCiscoリモートアクセスVPN(AnyConnect)ソリューションを設定する手順について説明します。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントは、FTDデバイスの設定を対象としています。ASAの設定例については、<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/100918-asa-sslvpn-00.html>を参照してください。

制限：

現在、次の機能はFTDではサポートされていませんが、ASAデバイスでは引き続き使用できます。

- ダブルAAA認証 (FTDバージョン6.5で使用可能)
- ダイナミック アクセス ポリシー
- ホストスキャン
- ISE ポスチャ
- RADIUS CoA
- VPNロードバランサ
- ローカル認証(Firepower Device Manager 6.3で使用可能)Cisco Bug ID [CSCvf92680](#) (登録ユーザ専用)
- LDAP属性マップ(FlexConfig、Cisco Bug ID [CSCvd64585](#)で利用可能)
- AnyConnectのカスタマイズ
- AnyConnectスクリプト
- AnyConnectのローカリゼーション
- アプリごとのVPN
- SCEPプロキシ
- WSAの統合
- SAML SSO(Cisco Bug ID [CSCvg90789](#))
- RAおよびL2L VPNの同時IKEv2ダイナミック暗号マップ
- AnyConnectモジュール (NAM、Hostscan、AMPイネーブラ、SBL、Umbrella、Webセキュリティなど) DARTは、このバージョンにデフォルトでインストールされる唯一のモジュールです。
- TACACS、Kerberos (KCD認証およびRSA SDI)
- ブラウザプロキシ

設定

FMCでリモートアクセスVPNウィザードを実行するには、次の手順を実行する必要があります。

ステップ 1：SSL証明書のインポート

証明書は、AnyConnectを設定する際に不可欠です。SSLおよびIPSecでサポートされているのは、RSAベースの証明書だけです。

楕円曲線デジタル署名アルゴリズム(ECDSA)証明書はIPSecでサポートされていますが、ECDSAベースの証明書を使用する場合、新しいAnyConnectパッケージまたはXMLプロファイルを展開することはできません。

これはIPSecに使用できますが、XMLプロファイルとともにAnyConnectパッケージを事前展開する必要があります。すべてのXMLプロファイルの更新は、各クライアントに手動でプッシュする必要があります(Cisco Bug ID [CSCtx42595](#))。

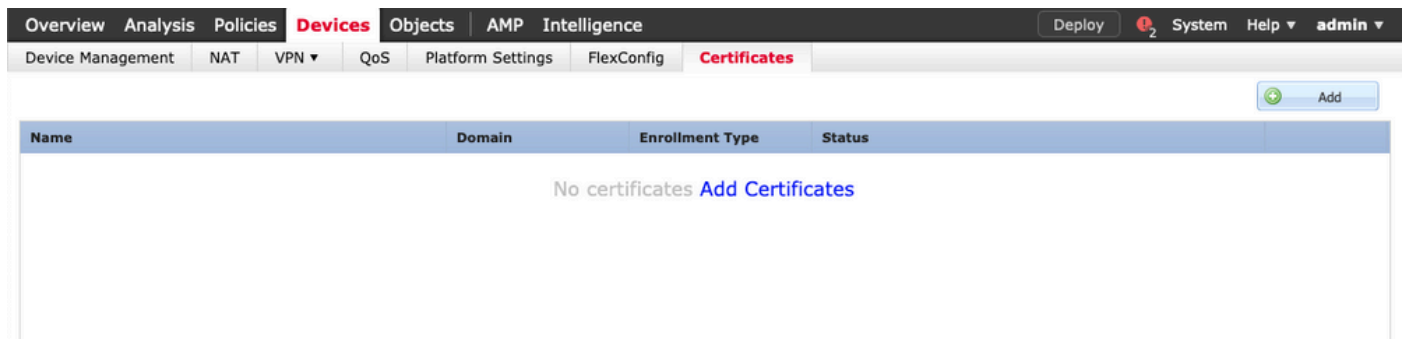
さらに、Webブラウザで「信頼できないサーバ証明書」エラーを回避するために、証明書にはDNS名やIPアドレスを持つ共通名(CN)拡張子が含まれている必要があります。

注:FTDデバイスでは、証明書署名要求(CSR)を生成する前に認証局(CA)証明書が必要です。

- CSRが外部サーバ (Windows ServerやOpenSSLなど) で生成される場合、FTDはキーの手動登録をサポートしていないため、手動登録の方法は失敗します。
- PKCS12など、別の方式を使用する必要があります。

手動登録方式でFTDアプライアンスの証明書を取得するには、CSRを生成し、CAで署名してから、ID証明書をインポートする必要があります。

1. Devices > Certificatesの順に移動し、図に示すようにAddを選択します。



2. Deviceを選択し、図に示すように新しいCert Enrollmentオブジェクトを追加します。

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.手動登録タイプを選択し、CA証明書 (CSRへの署名を目的とした証明書) を貼り付けます。

Add Cert Enrollment



Name*

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type:

CA Certificate:*

```
/3C4hi07uzuR0ygwKEBaMdg4Dl/z
4x3nk3tTUhYpfbWqWAXM7GNDRVWG9BZ1svk3shDK2Bogklzou6
RqV66GI9IE7Z2
xIVrSrJFqhkrT795kMb8am8xhb4eXYXxUgJmODIPqZ76RSTAT0+v1
VLSP+vHGm8X
g6wEFsKuZay27a48e/1JG2LgRDraOKt+jwbS7DGSK4mfZsZqhFdQP
LhBNFbyBvb9
dOjUkmdSvzQDRSqSo+HINEm3E8/q20wrtZp04MpAabyhr+hEpeP
VMrhvBOT8h
H8eMjSQjGhhHbuKofVlzQmM0RvGnTB6EKYIvb4CUW8HcgDdDr
mwNgy5mTP9cHa
9Or3RlWRzEa11HE3mHC4Rj6DOnmgufjx+TZRYczownSKLL7LcW1
DIBZclYmfaldC
W2cZuBR0yVdxCvq4#04ISEIBfOWFsd5rAD/bvk2n6xrJI1SLqABMJJ
uslu9KTGH1
bYKEYACKVvETw==
-----END CERTIFICATE-----
```

Allow Overrides

4. Certificate Parametersタブを選択し、Include FQDNフィールドで「Custom FQDN」を選択し、図に示すように証明書の詳細を入力します。

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. 「キー」タブを選択し、キーのタイプを選択します。名前とサイズを選択できます。RSAの最小要件は2048バイトです。

6. 「保存」を選択し、デバイスを確認して、「証明書の登録」で作成したトラストポイントを選択し、「追加」を選択して証明書を展開します。

Add New Certificate

? X

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

Add

Cancel

7. 「ステータス」列で「ID」アイコンを選択し、「はい」を選択して、図に示すようにCSRを生成します。

The screenshot shows the Cisco FTD GUI with the 'Certificates' tab selected. The table below shows the certificate configuration:

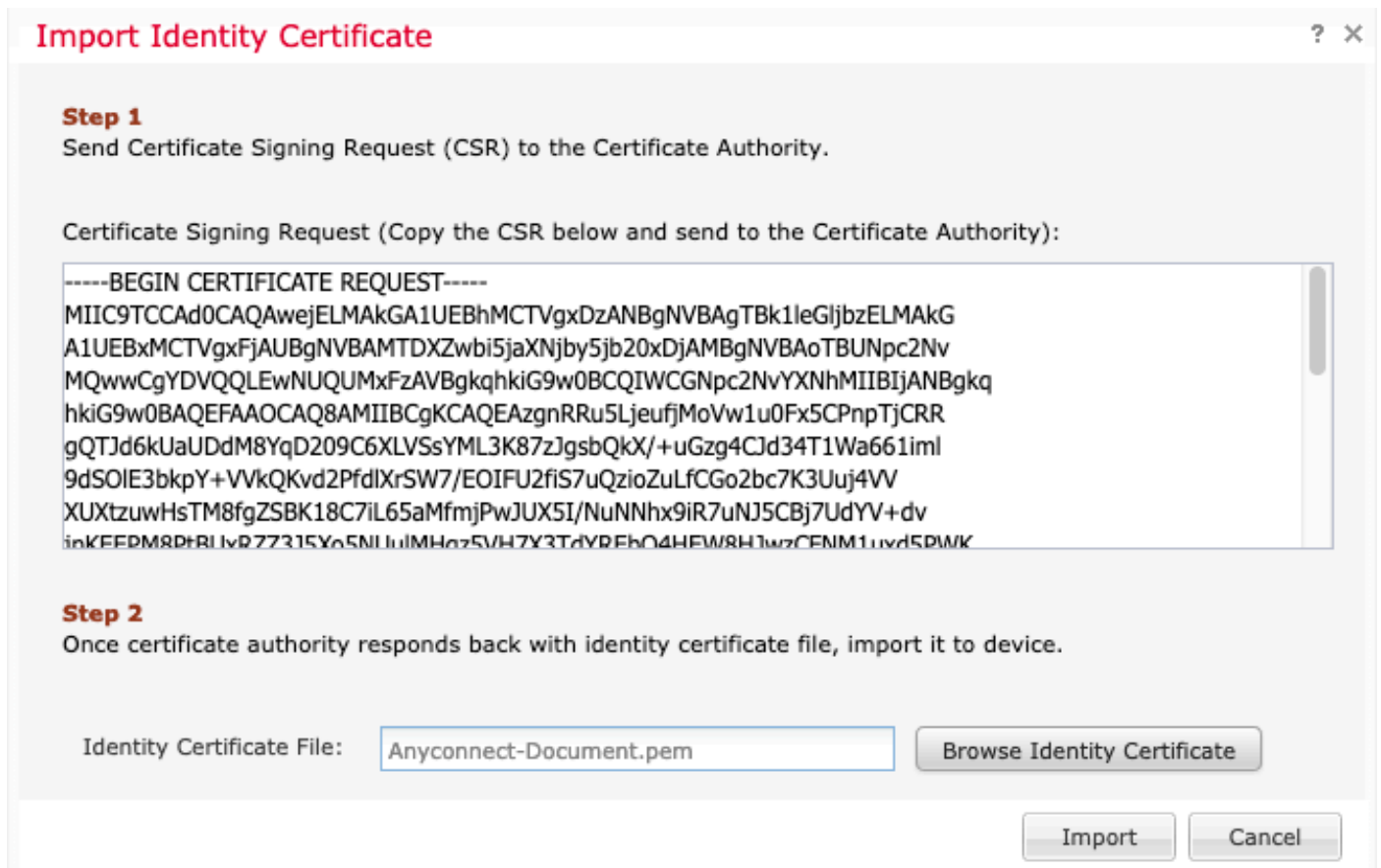
Name	Domain	Enrollment Type	Status
Anyconnect-certificate	Global	Manual	CA ID Identity certificate import required

A warning dialog box is displayed in the foreground with the following text:

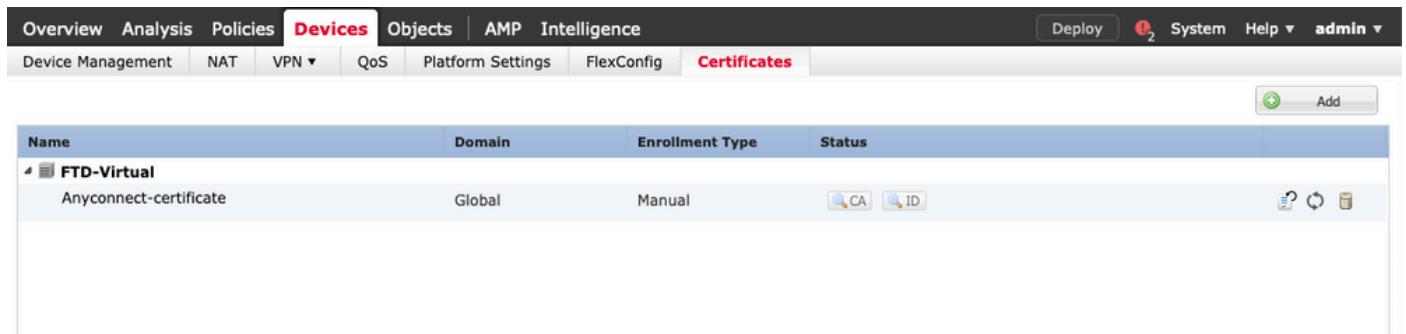
Warning
This operation will generate Certificate Signing Request do you want to continue?
Yes No

8. CSRをコピーし、任意のCA (GoDaddyやDigiCertなど) で署名します。

9. CAからID証明書を受信したら (Base64形式である必要があります)、Browse Identity Certificateを選択し、ローカルコンピュータで証明書を見つけます。Importを選択します。



10.インポートすると、CA証明書とID証明書の両方の詳細を表示できるようになります。



ステップ 2 : RADIUSサーバの設定

FMCによって管理されるFTDデバイスでは、ローカルユーザデータベースはサポートされていません。RADIUSやLDAPなどの別の認証方式を使用する必要があります。

1.図に示すように、Objects > Object Management > RADIUS Server Group > Add RADIUS Server Groupの順に移動します。

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

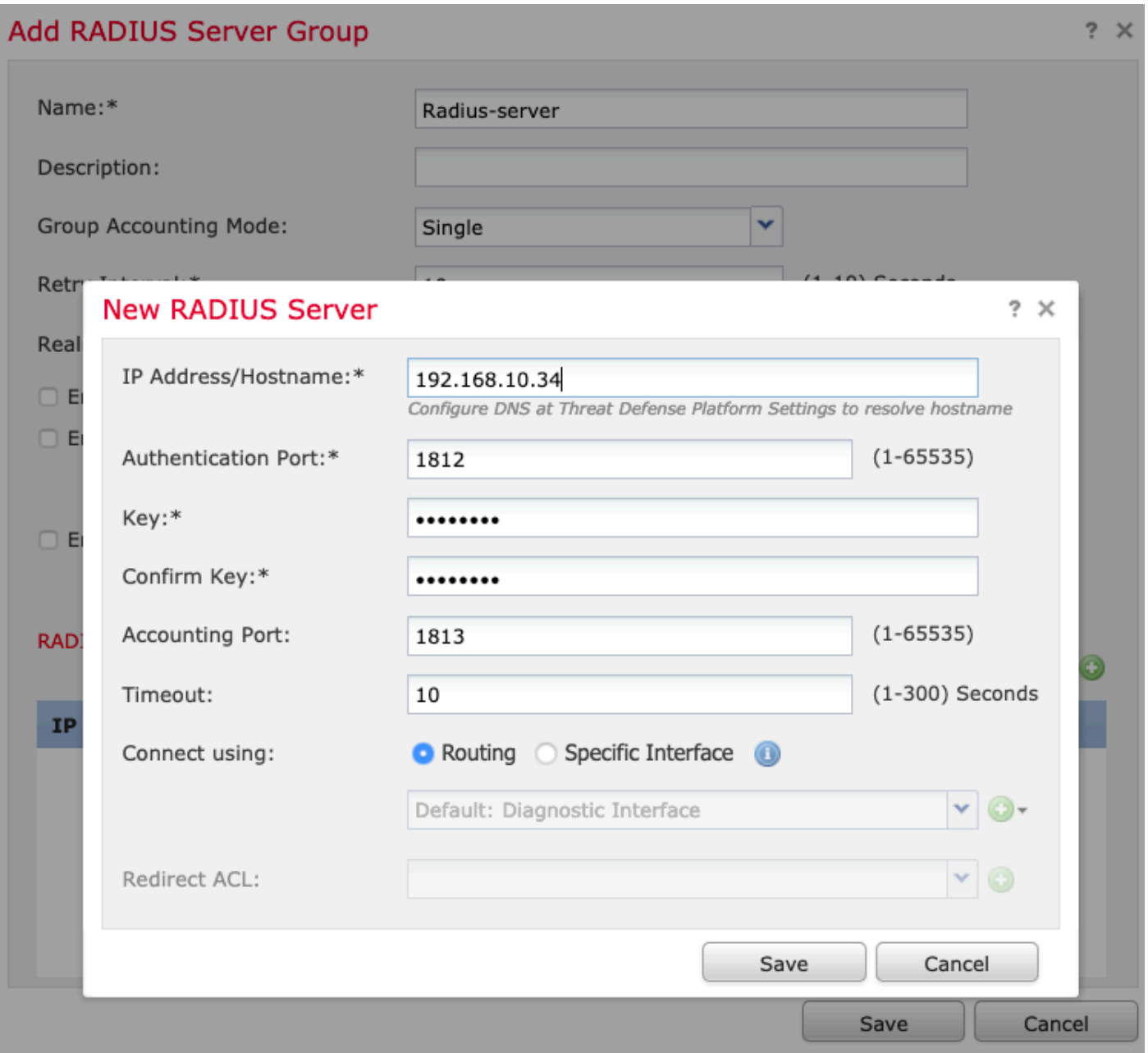
Enable dynamic authorization

Port:* (1024-65535)

RADIUS Servers (Maximum 16 servers) +

IP Address/Hostname		
No records to display		

2. RADIUSサーバグループに名前を割り当て、RADIUSサーバのIPアドレスと共有秘密 (FTDとRADIUSサーバをペアにするには共有秘密が必要) を追加し、このフォームの入力が完了したら、次の図に示すようにSaveを選択します。






3.図に示すように、RADIUSサーバ情報がRADIUSサーバリストで使用できるようになりました。

Add RADIUS Server Group



Name:*	<input type="text" value="Radius-server"/>
Description:	<input type="text"/>
Group Accounting Mode:	<input type="text" value="Single"/> ▼
Retry Interval:*	<input type="text" value="10"/> (1-10) Seconds
Realms:	<input type="text"/> ▼
<input type="checkbox"/> Enable authorize only	
<input type="checkbox"/> Enable interim account update	
Interval:*	<input type="text" value="24"/> (1-120) hours
<input type="checkbox"/> Enable dynamic authorization	
Port:*	<input type="text" value="1700"/> (1024-65535)

RADIUS Servers (Maximum 16 servers) 

IP Address/Hostname		
192.168.10.34		

ステップ 3 : IPプールの作成

1. Objects > Object Management > Address Pools > Add IPv4 Poolsの順に移動します。
2. IPアドレスの名前と範囲を割り当てます。Maskフィールドは必須ではありませんが、図に示すように指定できます。

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

ステップ 4 : XMLプロファイルの作成

1. Cisco.comからProfile Editorツールをダウンロードし、アプリケーションを実行します。
2. Profile Editorアプリケーションで、Server Listに移動し、図に示すようにAddを選択します。

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. 表示名、完全修飾ドメイン名(FQDN)またはIPアドレスを割り当て、図に示すようにOKを選択します。

Server Load Balancing Servers SCEP Mobile Certificate Pinning

Primary Server

Display Name (required) Corporate - FTD (SSL)

FQDN or IP Address vpn.cisco.com / User Group ssl

Group URL

Connection Information

Primary Protocol SSL

ASA gateway

Auth Method During IKE Negotiation EAP-AnyConnect

IKE Identity (IOS gateway only)

Backup Servers

Host Address Add

Move Up

Move Down

Delete

OK Cancel

4. エントリが Server List メニューに表示されます。

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.

Add... Delete

Edit... Details


5. File > Save as の順に移動します。

注: プロファイルを .xml 拡張子の付いた識別しやすい名前で保存します。

ステップ 5 : Anyconnect XML プロファイルのアップロード

1. FMCで、Objects > Object Management > VPN > AnyConnect File > Add AnyConnect Fileの順に移動します。

2. オブジェクトに名前を割り当て、Browseをクリックし、ローカルシステムでクライアントプロファイルを検索して、Saveを選択します。

 注意：ファイルタイプとしてAnyconnect Client Profileを選択していることを確認してください。




Add AnyConnect File



Name:*	<input type="text" value="Corporate-profile(SSL)"/>
File Name:*	<input type="text" value="FTD-corp-ssl.xml"/> <input type="button" value="Browse.."/>
File Type:*	<input type="text" value="AnyConnect Client Profile"/> ▼
Description:	<input type="text"/>

手順 6：AnyConnectイメージのアップロード

1. CiscoダウンロードWebページからwebdeploy(.pkg)イメージをダウンロードします。

AnyConnect Headend Deployment Package (Mac OS)	26-Jun-2019	51.22 MB	  
anyconnect-macos-4.7.04056-webdeploy-k9.pkg			

2. Objects > Object Management > VPN > AnyConnect File > Add AnyConnect Fileの順に移動します。

3. Anyconnectパッケージファイルを選択したら、そのファイルに名前を割り当て、ローカルシステムから.pkgファイルを選択します。

4. Saveを選択します。

Add AnyConnect File

Name:*

File Name:*

File Type:* ▼

Description:

注：要件(Windows、Mac、Linux)に基づいて、追加のパッケージをアップロードできます。

手順 7：リモートアクセスVPNウィザード

前の手順に基づいて、リモートアクセスウィザードに従うことができます。

1. Devices > VPN > Remote Accessの順に移動します。
2. リモートアクセスポリシーの名前を割り当て、Available DevicesからFTDデバイスを選択します。

The screenshot shows the 'Remote Access VPN Policy Wizard' in a network management system. The breadcrumb trail is: Overview > Analysis > Policies > **Devices** > Objects > AMP > Intelligence. The current page is 'Remote Access VPN Policy Wizard' with steps: 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** (Search: FTD-Virtual) **Selected Devices** (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.

Buttons: Back, Next, Cancel

3. 接続プロファイル名（接続プロファイル名はトンネルグループ名）を割り当て、図に示すように認証サーバとアドレスプールを選択します。

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 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. グループポリシーを作成するには、+記号を選択します。

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. (オプション) ローカルIPアドレスプールは、グループポリシー単位で設定できます。設定されていない場合、プールは接続プロファイル(トンネルグループ)で設定されたプールから継承されます。

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.このシナリオでは、すべてのトラフィックがトンネル経由でルーティングされ、IPv4スプリットトンネリングポリシーは図に示すようにトンネル経由のすべてのトラフィックを許可するように設定されます。

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プロファイルの.xmlプロファイルを選択し、図に示すようにSaveを選択します。

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.動作環境のシステム要件に基づいて必要なAnyConnectイメージを選択し、図に示すようにNextを選択します。

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. Security ZoneとDeviceCertificatesを選択します。

- この設定では、VPNが終端するインターフェイスと、SSL接続時に提示される証明書を定義します。

注：このシナリオでは、FTDはVPNトラフィックを検査しないように設定され、アクセスコントロールポリシー(ACP)オプションはバイパスされます。

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

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. Finishを選択し、変更を展開します。

- 図に示すように、VPN、SSL証明書、およびAnyConnectパッケージに関連するすべての設定は、FMC Deployを介してプッシュされます。

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.

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

ステップ 1 : NAT 免除の設定

NAT除外は、トラフィックがVPNトンネル（リモートアクセスまたはサイト間）を経由して流れることを目的としているときにインターネットにルーティングされることを防ぐために使用される、推奨される変換方式です。

これは、内部ネットワークからのトラフィックが、変換を行わずにトンネルを通過することを目的としている場合に必要です。

1. 図に示すように、Objects > Network > Add Network > Add Objectの順に移動します。

New Network Object

Name: vpn-pool

Description:


Network: Host Range Network FQDN

192.168.55.0/24

Allow Overrides:

Save Cancel

2. Device > NATに移動し、問題のデバイスで使用されているNATポリシーを選択し、新しい文を作成します。

 注：トラフィックフローは内部から外部に向かいます。

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

Search by name

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

Add to Source

Add to Destination

Source Interface Objects (1)

- inside-zone

Destination Interface Objects (1)

- outside-zone

OK Cancel

3. 図に示すように、FTDの背後にある内部リソース(元の送信元および変換済みの送信元)と、AnyconnectユーザのIPローカルプールとしての宛先(元の宛先および変換済みの宛先)を選択します。

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:	Translated Source Port:
Original Destination Port:	Translated Destination Port:
vpn-pool	vpn-pool

OK Cancel

4.オプションを切り替えてください(図を参照)。NATルールで「no-proxy-arp」と「route-lookup」を有効にするには、図に示すように「OK」を選択します。

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.これはNAT免除の設定の結果です。



前のセクションで使用したオブジェクトは、次のとおりです。

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

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

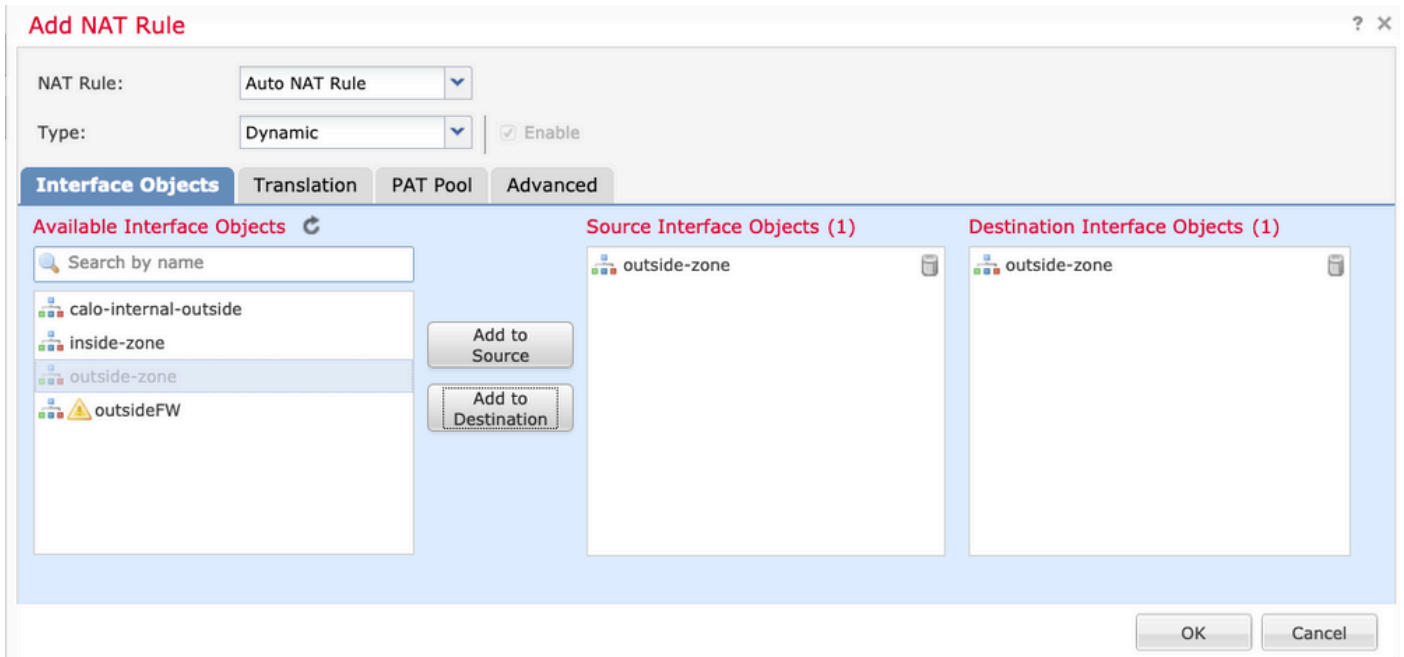
ステップ 2 : ヘアピン設定

U-turnとも呼ばれるこの変換方式を使用すると、トラフィックを受信したのと同じインターフェイス上でトラフィックを流すことができます。

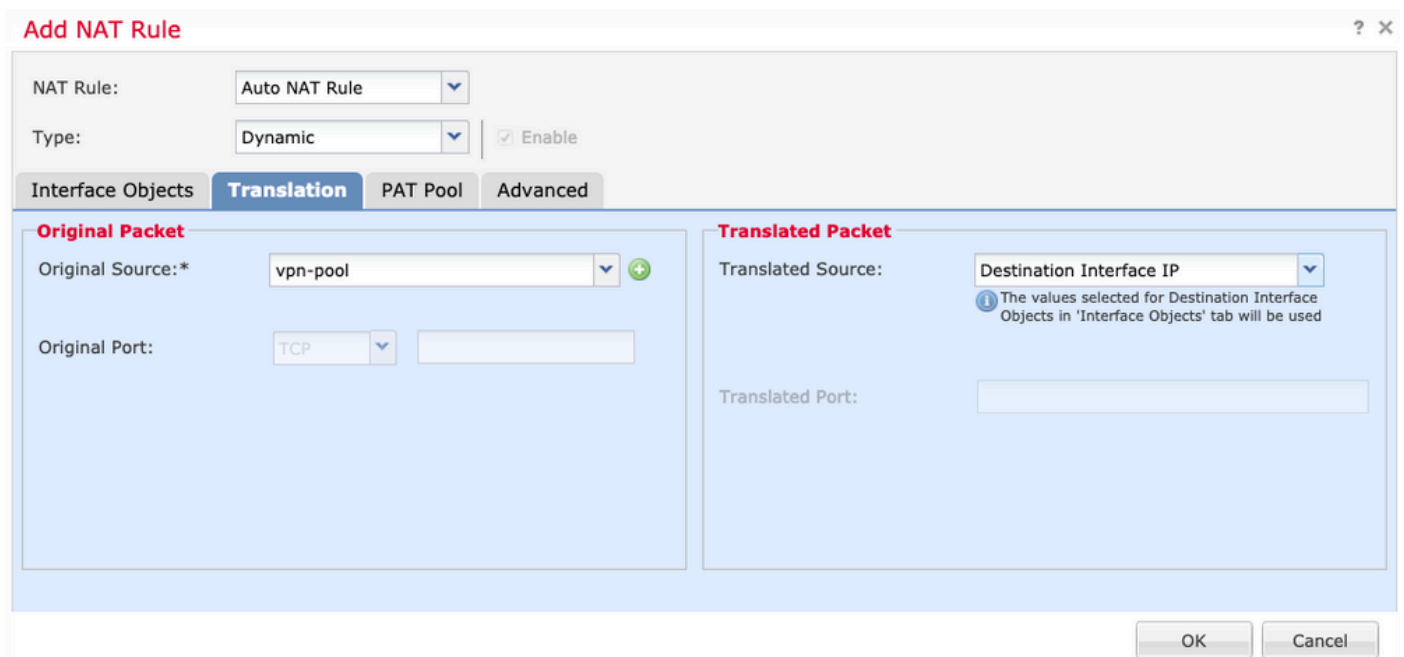
たとえば、Anyconnectがフルトンネルスプリットトンネルポリシーで設定されている場合、内部リソースにはNAT除外ポリシーに従ってアクセスされます。Anyconnectクライアントトラフィックがインターネット上の外部サイトに到達することを目的としている場合、ヘアピンNAT (またはUターン) は外部から外部へのトラフィックのルーティングを行います。

VPNプールオブジェクトは、NAT設定の前に作成する必要があります。

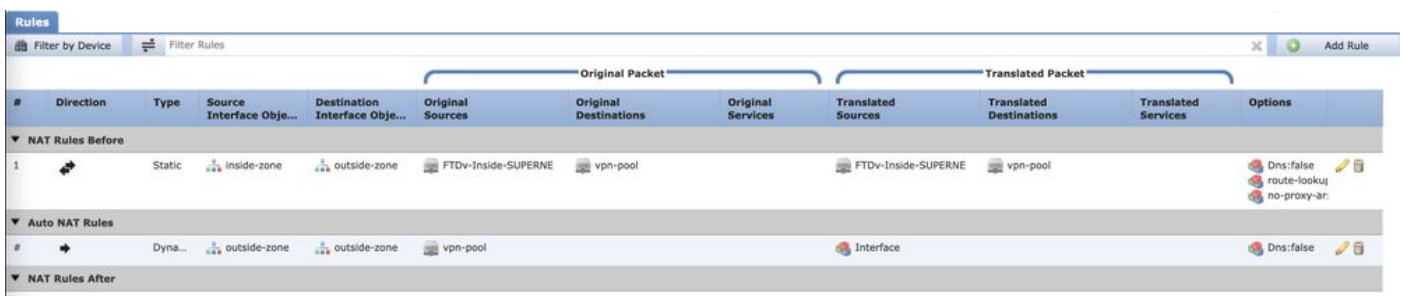
- 1.新しいNATステートメントを作成し、NAT RuleフィールドでAuto NAT Ruleを選択し、NAT TypeとしてDynamicを選択します。
- 2.送信元と宛先のインターフェイスオブジェクト(outside)に同じインターフェイスを選択します。



3. Translationタブで、vpn-poolオブジェクトのOriginal Sourceとして選択し、Destination Interface IPをTranslated Sourceとして選択し、図に示すようにOKを選択します。



4. 次の図に示すように、NAT設定の要約を示します。



5. 「保存」をクリックし、変更を配置します。

確認

このセクションでは、設定が正常に動作していることを確認します。

FTDコマンドラインで次のコマンドを実行します。

- sh crypto ca certificates
- show running-config ip local pool
- show running-config webvpnを発行します。
- show running-config tunnel-groupを発行します。
- show running-config group-policyを発行します。
- show running-config ssl
- show running-config nat

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。 </>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。