

Configuration du client VPN AnyConnect sur FTD : exemption Hairpin et NAT

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Étape 1. Importer un certificat SSL](#)

[Étape 2. Configurer un serveur RADIUS](#)

[Étape 3. Créer un pool d'adresses IP](#)

[Étape 4. Créer un profil XML](#)

[Étape 5. Télécharger un profil XML Anyconnect](#)

[Étape 6. Télécharger des images AnyConnect](#)

[Étape 7. Assistant VPN d'accès à distance](#)

[Exemption NAT et épingle à cheveux](#)

[Étape 1. Configuration des exemptions NAT](#)

[Étape 2. Configuration en épingle à cheveux](#)

[Vérifier](#)

[Dépannage](#)

Introduction

Ce document décrit comment configurer la solution VPN d'accès à distance Cisco (AnyConnect) sur Firepower Threat Defense (FTD), v6.3, gérée par FMC.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base en matière de VPN d'accès à distance, de protocole SSL (Secure Sockets Layer) et d'échange de clés Internet version 2 (IKEv2)
- Connaissances de base en authentification, autorisation et comptabilité (AAA) et RADIUS
- Connaissances FMC de base
- Connaissances FTD de base

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco FMC 6.4
- Cisco FTD 6.3
- AnyConnect 4.7

Ce document décrit la procédure de configuration de la solution VPN d'accès à distance Cisco (AnyConnect) sur Firepower Threat Defense (FTD), version 6.3, gérée par Firepower Management Center (FMC).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Ce document est destiné à couvrir la configuration sur les périphériques FTD. Si vous recherchez l'exemple de configuration ASA, veuillez vous reporter au document :

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/100918-asa-sslvpn-00.html>

Limites:

Actuellement, ces fonctionnalités ne sont pas prises en charge sur FTD, mais sont toujours disponibles sur les périphériques ASA :

- Double authentification AAA (disponible sur FTD version 6.5)
- Politique d'accès dynamique
- Analyse des hôtes
- posture ISE
- RADIUS CoA
- Équilibreur de charge VPN
- Authentification locale (disponible dans Firepower Device Manager 6.3). ID de bogue Cisco [CSCvf92680](#))
- Mappage des attributs LDAP (disponible via FlexConfig, ID de bogue Cisco [CSCvd64585](#))
- Personnalisation AnyConnect
- scripts AnyConnect
- Localisation AnyConnect
- VPN par application
- Proxy SCEP
- Intégration WSA
- SSO SAML (ID de bogue Cisco [CSCvq90789](#))
- Crypto-carte dynamique IKEv2 simultanée pour RA et VPN L2L
- Modules AnyConnect (NAM, Hostscan, AMP Enabler, SBL, Umbrella, Web Security, etc.) DART est le seul module installé par défaut sur cette version.
- TACACS, Kerberos (authentification KCD et RSA SDI)
- Proxy du navigateur

Configurer

Afin de passer par l'assistant VPN d'accès à distance dans le FMC, ces étapes doivent être effectuées :

Étape 1. Importer un certificat SSL

Les certificats sont essentiels lorsque vous configurez AnyConnect. Seuls les certificats RSA sont pris en charge pour SSL et IPSec.

Les certificats ECDSA (Elliptic Curve Digital Signature Algorithm) sont pris en charge dans IPSec, mais il n'est pas possible de déployer un nouveau package AnyConnect ou un nouveau profil XML lorsque le certificat basé sur ECDSA est utilisé.

Il peut être utilisé pour IPSec, mais vous devez pré-déployer les packages AnyConnect avec le profil XML, toutes les mises à jour de profil XML doivent être poussées manuellement sur chaque client (ID de bogue Cisco [CSCtx42595](#)).

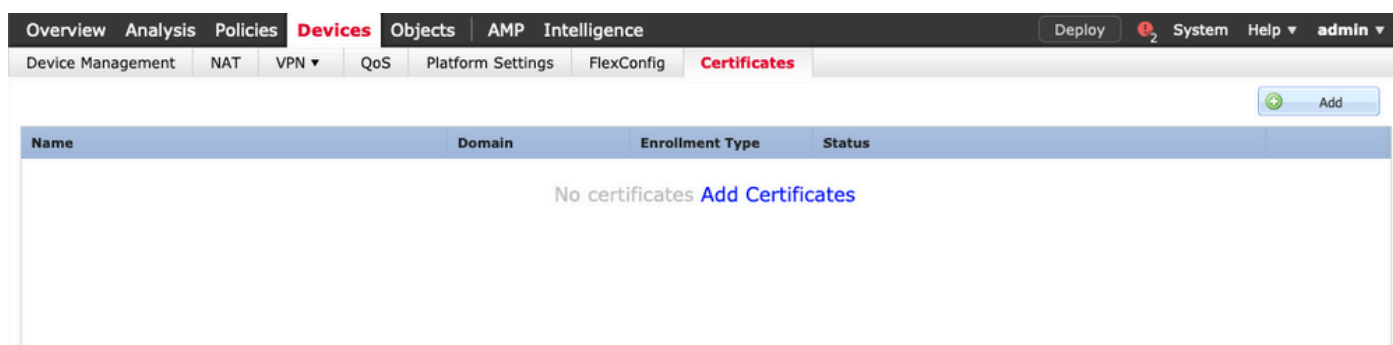
En outre, le certificat doit contenir une extension de nom commun (CN) avec un nom DNS et/ou une adresse IP afin d'éviter les erreurs de « certificat de serveur non approuvé » dans les navigateurs Web.

Remarque : sur les périphériques FTD, le certificat de l'autorité de certification (CA) est nécessaire avant la génération de la demande de signature de certificat (CSR).

- Si le CSR est généré dans un serveur externe (tel que Windows Server ou OpenSSL), la méthode d'inscription manuelle est censée échouer, car FTD ne prend pas en charge l'inscription manuelle de clé.
- Une autre méthode doit être utilisée, telle que PKCS12.

Pour obtenir un certificat pour l'appareil FTD avec la méthode d'inscription manuelle, un CSR doit être généré, signé avec une autorité de certification, puis importé le certificat d'identité.

1. Accédez à Périphériques > Certificats et sélectionnez Ajouter comme indiqué dans l'image.



2. Sélectionnez le périphérique et ajoutez un nouvel objet Inscription de certificat comme illustré dans l'image.

The screenshot displays a network management interface with a top navigation bar containing 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. Below this is a secondary navigation bar with 'Device Management', 'NAT', 'VPN', 'QoS', 'Platform Settings', 'FlexConfig', and 'Certificates'. A table with columns 'Name', 'Domain', 'Enrollment Type', and 'Status' is shown, with the text 'No certificates' and a link 'Add Certificates'. Two dialog boxes are open: 'Add New Certificate' and 'Add Cert Enrollment'. The 'Add New Certificate' dialog has fields for 'Device*' (FTD-Virtual) and 'Cert Enrollment*' (Select a certificate enrollment object). The 'Add Cert Enrollment' dialog has fields for 'Name*', 'Description', and tabs for 'CA Information', 'Certificate Parameters', 'Key', and 'Revocation'. The 'CA Information' tab is active, showing 'Enrollment Type' (SCEP), 'Enrollment URL: *' (http://), 'Challenge Password', 'Confirm Password', 'Retry Period' (1 Minutes), 'Retry Count' (10), and 'Fingerprint' (Ex: e6f7d542 e355586c a758e7cb bdcddd92). There is also an 'Allow Overrides' checkbox and 'Save' and 'Cancel' buttons.

3. Sélectionnez le type d'inscription manuelle et collez le certificat de l'autorité de certification (le certificat destiné à signer le CSR).

Add Cert Enrollment



Name*

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type:

CA Certificate:*

```
/3C4hi07uzuR0ygwKEBaMdg4Dl/z
4x3nk3lTUhYpfbWqWAXM7GNDRVWG9BZ1svk3shDK2BogklzXu6
RqV66G9IE7Z2
xIVrSrJFqhrT795kMb8am8xhb4eXYXxUgJmODIPqZ76RSTAT0+v1
VLSP+vHGm8X
g6wEFsKuZay27a48e/lJG2LgRDraOKt+jwbS7DGSK4mfZsZqhFdQP
LhBNFbyBvb9
dOjUkmdSvzQDRSqSo+HINEm3E8/q20wrtZp04MpAabyhr+hEpeP
VMrhvBOT8h
H8eMjSQjGhhHbuKofVlzQmM0RvGnTB6EKYIvb4CUW8HcgDdDr
mwNgy5mTP9cHa
9Cr3RlWRzEa11HE3mHC4Rj6DOnmguljx+TZRYczownSKLL7LcW1
D18ZclYmfaldC
W2cZuBR0yVdxCvq4#04ISE1BfOWFSd5rAD/bvk2n6xrJl1SLqABMJJ
uslu9KTGH1
bYKEYACKVvETw==
-----END CERTIFICATE-----
```

Allow Overrides

4. Sélectionnez l'onglet Certificate Parameters et sélectionnez "Custom FQDN" pour le champ Include FQDN et remplissez les détails du certificat comme indiqué dans l'image.

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. Sélectionnez l'onglet Clé, puis sélectionnez le type de clé, vous pouvez choisir le nom et la taille. Pour RSA, 2 048 octets sont requis au minimum.

6. Sélectionnez save, confirm the Device, et sous Cert Enrollment sélectionnez le point de confiance qui vient d'être créé, sélectionnez Add afin de déployer le certificat.

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

Add

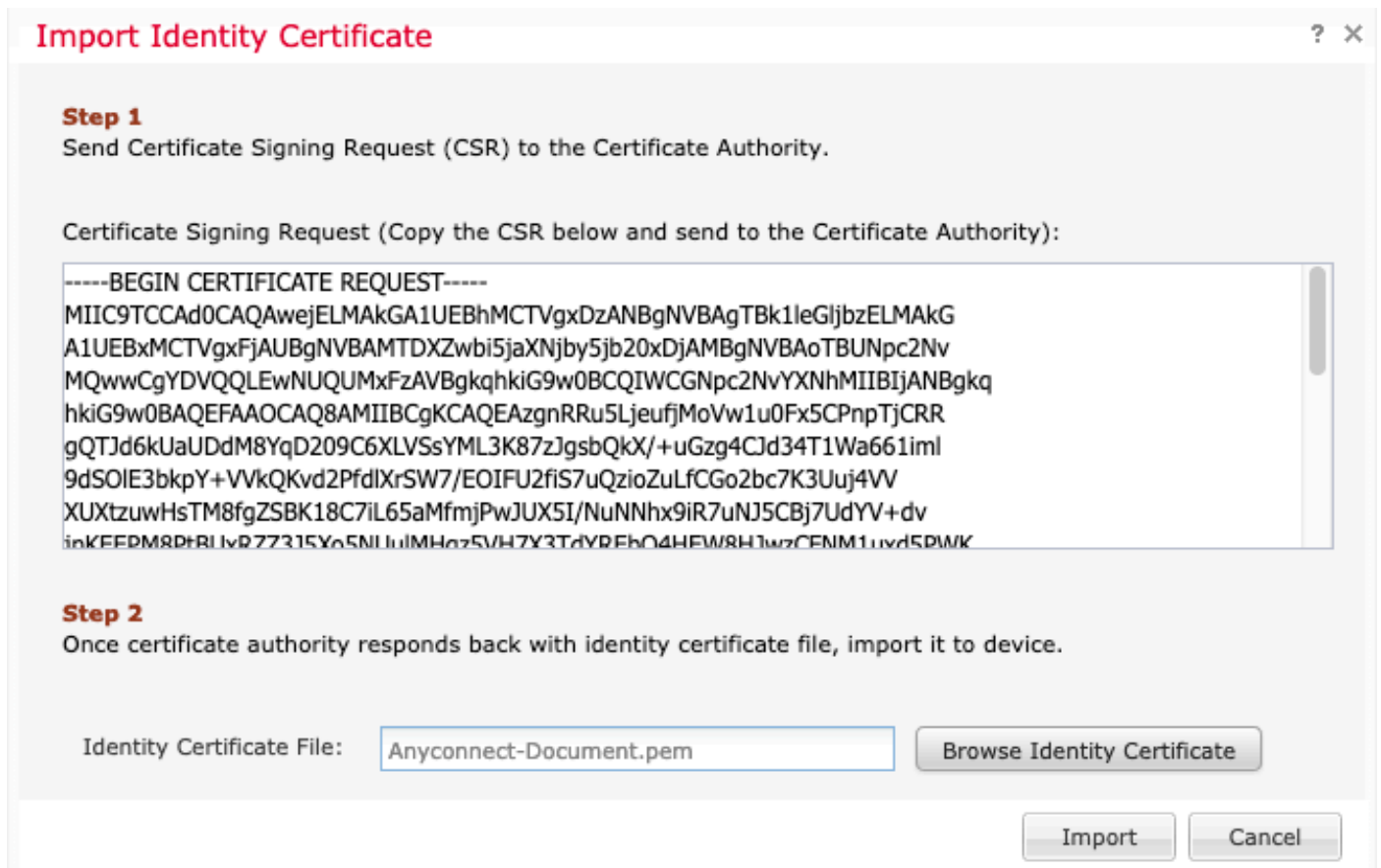
Cancel

7. Dans la colonne Statut, sélectionnez l'icône ID et sélectionnez Oui pour générer le CSR comme indiqué dans l'image.

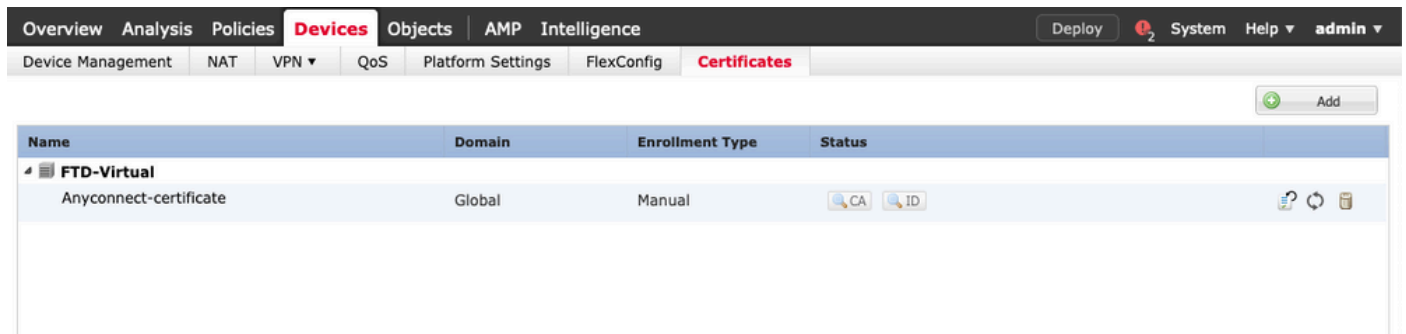
The screenshot shows the Cisco Firepower Management Center interface. The top navigation bar includes Overview, Analysis, Policies, Devices (selected), Objects, AMP, and Intelligence. Below this, there are tabs for Device Management, NAT, VPN, QoS, Platform Settings, FlexConfig, and Certificates. The Certificates table is visible, with columns for Name, Domain, Enrollment Type, and Status. A row is selected for 'Anyconnect-certificate' under the 'FTD-Virtual' device. The Status column shows icons for CA, ID, and a warning icon with the text 'Identity certificate import required'. A warning dialog box is open in the foreground, asking 'This operation will generate Certificate Signing Request do you want to continue?' with 'Yes' and 'No' buttons.

8. Copiez CSR et signez-le avec votre CA préférée (par exemple GoDaddy ou DigiCert).

9. Une fois le certificat d'identité reçu de l'autorité de certification (qui doit être au format base64), sélectionnez Browse Identity Certificate et recherchez le certificat sur l'ordinateur local. Sélectionnez Importer.



10. Une fois importés, les détails du certificat CA et ID peuvent être affichés.



Étape 2. Configurer un serveur RADIUS

Sur les périphériques FTD gérés par FMC, la base de données utilisateur locale n'est pas prise en charge, une autre méthode d'authentification doit être utilisée, telle que RADIUS ou LDAP.

1. Accédez à **Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group** comme indiqué dans l'image.

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

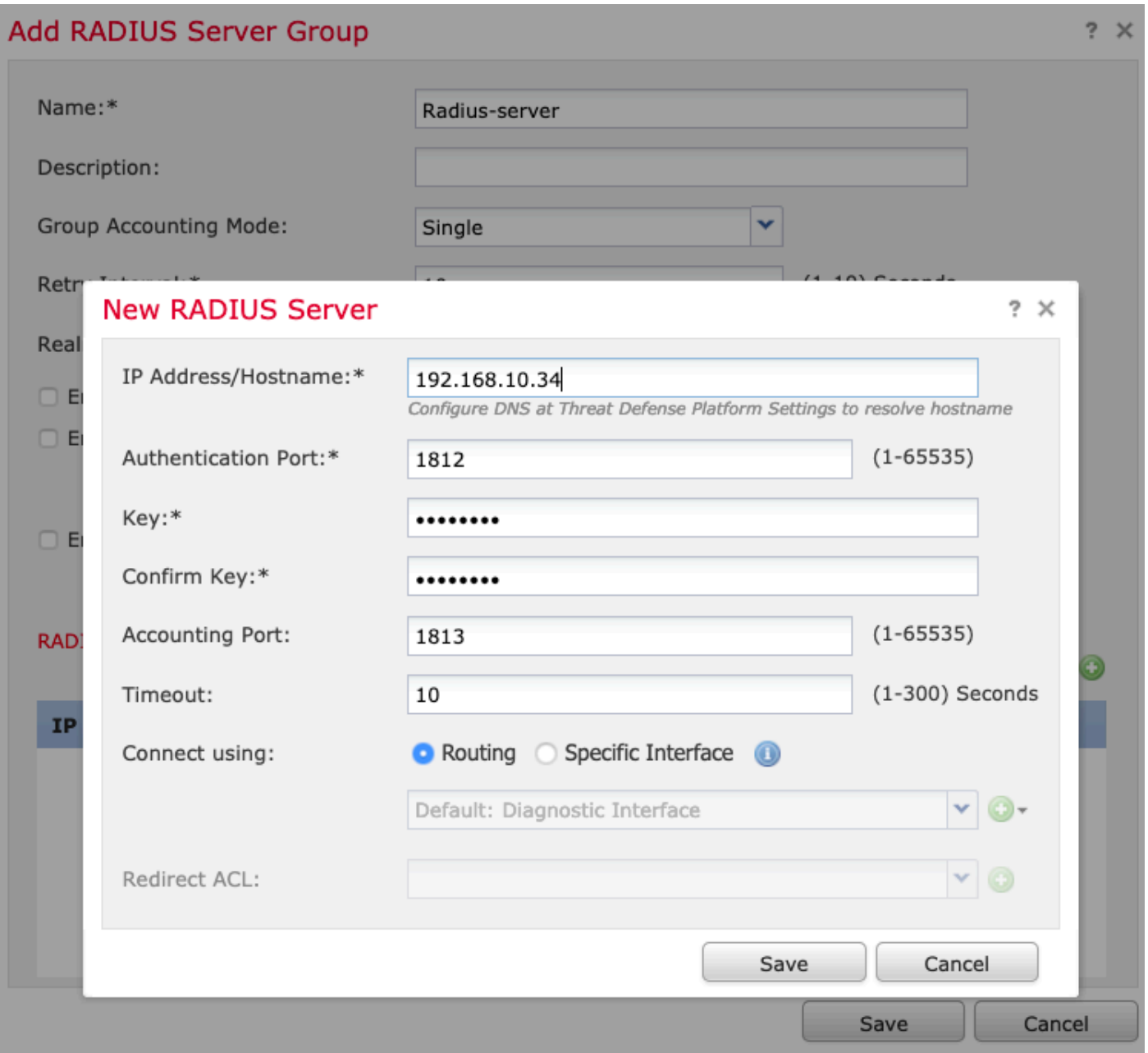
Enable dynamic authorization

Port:* (1024-65535)

RADIUS Servers (Maximum 16 servers) 

IP Address/Hostname	
No records to display	

2. Attribuez un nom au groupe de serveurs Radius et ajoutez l'adresse IP du serveur Radius avec un secret partagé (le secret partagé est requis pour associer le FTD au serveur Radius), sélectionnez Enregistrer une fois que ce formulaire est rempli comme indiqué dans l'image.



3. Les informations sur le serveur RADIUS sont désormais disponibles dans la liste des serveurs RADIUS, comme illustré dans l'image.

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

Étape 3. Créer un pool d'adresses IP

1. Accédez à Objets > Gestion des objets > Pools d'adresses > Ajouter des pools IPv4.
2. Attribuez le nom et la plage d'adresses IP, le champ Mask n'est pas obligatoire mais il peut être spécifié comme indiqué dans l'image.

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

Étape 4. Créer un profil XML

1. Téléchargez l'outil Éditeur de profil à partir de Cisco.com et exécutez l'application.
2. Dans l'application Éditeur de profil, naviguez jusqu'à Liste des serveurs et sélectionnez Ajouter comme indiqué dans l'image.

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. Attribuez un nom d'affichage, un nom de domaine complet (FQDN) ou une adresse IP et sélectionnez OK comme indiqué dans l'image.

Server List Entry



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

4. L'entrée est maintenant visible dans le menu Liste de serveurs :

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. Accédez à Fichier > Enregistrer sous.

Remarque : enregistrez le profil sous un nom facilement identifiable avec une extension .xml.

Étape 5. Télécharger un profil XML Anyconnect

1. Dans FMC, accédez à Objets > Gestion des objets > VPN > Fichier AnyConnect > Ajouter un fichier AnyConnect.

2. Attribuez un nom à l'objet et cliquez sur Parcourir, localisez le profil client dans votre système local et sélectionnez Enregistrer.

 Attention : veillez à sélectionner Anyconnect Client Profile comme type de fichier.

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"/> <input type="button" value="v"/>
Description:	<input type="text"/>

Étape 6. Télécharger des images AnyConnect

1. Téléchargez les images webdeploy (.pkg) à partir de la page Web de téléchargement de Cisco.

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



2. Accédez à Objets > Gestion des objets > VPN > Fichier AnyConnect > Ajouter un fichier AnyConnect.

3. Attribuez un nom au fichier de package Anyconnect et sélectionnez le fichier .pkg dans votre système local, une fois le fichier sélectionné.

4. Sélectionnez Enregistrer.

Add AnyConnect File ? X

Name:*

File Name:*

File Type:* ▼

Description:

Remarque : des paquets supplémentaires peuvent être téléchargés, en fonction de vos besoins (Windows, Mac, Linux).

Étape 7. Assistant VPN d'accès à distance

D'après les étapes précédentes, l'assistant d'accès à distance peut être suivi en conséquence.

1. Accédez à Devices > VPN > Remote Access.
2. Attribuez le nom de la stratégie d'accès à distance et sélectionnez un périphérique FTD dans Périphériques disponibles.

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

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:* TAC

Description:

VPN Protocols: SSL IPsec-IKEv2

Targeted Devices:

Available Devices

Search

FTD-Virtual

Selected Devices

FTD-Virtual

Add

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.

Back Next Cancel

3. Attribuez le nom du profil de connexion (le nom du profil de connexion est le nom du groupe de tunnels), sélectionnez Authentication Server et Address Pools comme indiqué dans l'image.

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

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. Sélectionnez le symbole + afin de créer une stratégie de groupe.

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. (Facultatif) Un pool d'adresses IP locales peut être configuré sur la base d'une stratégie de groupe. S'il n'est pas configuré, le pool est hérité du pool configuré dans le profil de connexion (tunnel-group).

Add Group Policy



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. Pour ce scénario, tout le trafic est routé sur le tunnel, la politique de Fractionnement de tunnel IPv4 est définie sur Autoriser tout le trafic sur le tunnel comme indiqué dans l'image.

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. Sélectionnez le profil .xml pour Anyconnect et sélectionnez Enregistrer comme indiqué dans l'image.

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. Sélectionnez les images AnyConnect souhaitées en fonction de la configuration système requise, puis sélectionnez Next a dans l'image.

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. Sélectionnez la zone de sécurité et les certificats de périphérique :

- Cette configuration définit l'interface sur laquelle le VPN se termine et le certificat qui est présenté sur une connexion SSL.

Remarque : dans ce scénario, le FTD est configuré pour ne pas inspecter le trafic VPN, contourner l'option Access Control Policies (ACP) est basculé.

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. Sélectionnez Terminer et Déployer les modifications :

- Toutes les configurations relatives aux VPN, aux certificats SSL et aux packages AnyConnect sont transmises via FMC Deploy, comme illustré dans l'image.

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

Exemption NAT et épingle à cheveux

Étape 1. Configuration des exemptions NAT

L'exemption NAT est une méthode de traduction préférée utilisée pour empêcher le trafic d'être routé vers Internet lorsqu'il est destiné à circuler sur un tunnel VPN (accès à distance ou site à site).

Cela est nécessaire lorsque le trafic provenant de votre réseau interne est destiné à circuler sur les tunnels sans aucune traduction.

1. Accédez à Objets > Réseau > Ajouter un réseau > Ajouter un objet comme indiqué dans l'image.

New Network Object ? X

Name: vpn-pool

Description:

Network: Host Range Network FQDN

192.168.55.0/24

Allow Overrides:

Save Cancel

2. Accédez à Device > NAT, sélectionnez la stratégie NAT qui est utilisée par le périphérique en question et créez une nouvelle instruction.

 Remarque : le flux de trafic va de l'intérieur vers l'extérieur.

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

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. Sélectionnez les ressources internes derrière le FTD (source d'origine et source traduite) et la destination en tant que pool ip local pour les utilisateurs Anyconnect (destination d'origine et destination traduite) comme indiqué dans l'image.

Add NAT Rule

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects: **Translation** PAT Pool Advanced

Original Packet	Translated Packet
Original Source:* <input type="text" value="FTDv-Inside-SUPERNE"/>	Translated Source: <input type="text" value="Address"/>
Original Destination: <input type="text" value="Address"/>	Translated Destination: <input type="text" value="FTDv-Inside-SUPERNE"/>
<input type="text" value="vpn-pool"/>	Translated Destination: <input type="text" value="vpn-pool"/>
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. Assurez-vous de basculer les options (comme indiqué dans l'image), afin d'activer "no-proxy-arp" et "route-lookup" dans la règle NAT, sélectionnez OK comme indiqué dans l'image.

Edit NAT Rule

NAT Rule: Insert:

Type: 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. Il s'agit du résultat de la configuration d'exemption NAT.



Les objets utilisés dans la section précédente sont ceux décrits ci-dessous.

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"/>

Étape 2. Configuration en épingle à cheveux

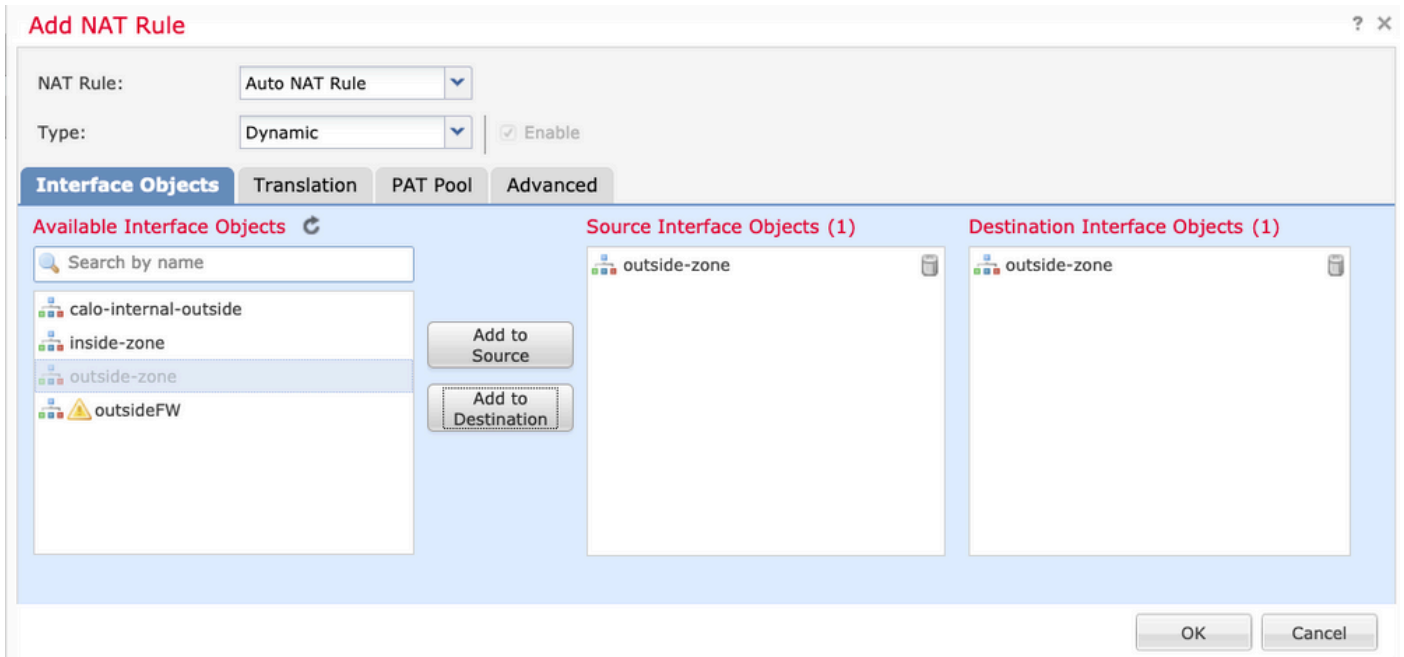
Également appelée U-turn, il s'agit d'une méthode de traduction qui permet au trafic de circuler sur la même interface sur laquelle le trafic est reçu.

Par exemple, quand Anyconnect est configuré avec une politique de tunnel Full split-tunnel, les ressources internes sont accédées selon la politique d'exemption NAT. Si le trafic client Anyconnect est destiné à atteindre un site externe sur Internet, la fonction NAT hairpin (ou U-turn) est chargée d'acheminer le trafic de l'extérieur vers l'extérieur.

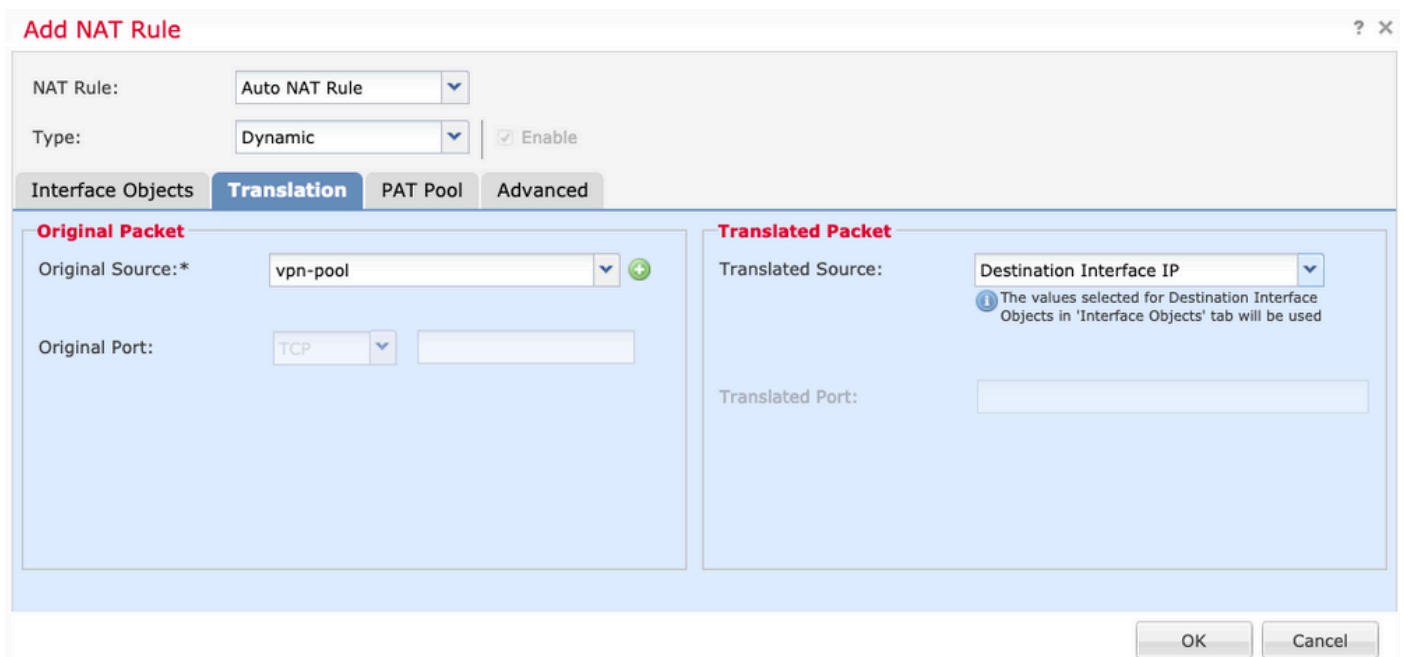
Un objet pool VPN doit être créé avant la configuration NAT.

1. Créez une nouvelle instruction NAT, sélectionnez Auto NAT Rule dans le champ NAT Rule et sélectionnez Dynamic comme NAT Type.

2. Sélectionnez la même interface pour les objets d'interface source et de destination (externe) :



3. Dans l'onglet Traduction, sélectionnez comme source d'origine l'objet vpn-pool et sélectionnez Destination Interface IP comme source traduite, sélectionnez OK comme indiqué dans l'image.



4. Ceci est le résumé de la configuration NAT telle qu'illustrée dans l'image.

Rules											
Filter by Device											
Filter Rules											
Add Rule											
#	Direction	Type	Source Interface Obj...	Destination Interface Obj...	Original Packet			Translated Packet			Options
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	
▼ NAT Rules Before											
1		Static	inside-zone	outside-zone	FTDv-Inside-SUPERNE	vpn-pool		FTDv-Inside-SUPERNE	vpn-pool		Dns:false route-lookup no-proxy-arp
▼ Auto NAT Rules											
#		Dyna...	outside-zone	outside-zone	vpn-pool			Interface			Dns:false
▼ NAT Rules After											

5. Cliquez sur Enregistrer et déployer les modifications.

Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Exécutez ces commandes dans la ligne de commande FTD.

- `certificats sh crypto ca`
- `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`

Dépannage

Aucune information de dépannage spécifique n'est actuellement disponible pour cette configuration.</1>

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.