

Configuration de la position ISE sur AnyConnect Remote Access VPN sur FTD

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme et flux du trafic du réseau](#)

[Configurations](#)

[FTD/FMC](#)

[ISE](#)

[Vérifier](#)

[Dépannage](#)

Introduction

Ce document décrit comment configurer Firepower Threat Defense (FTD) version 6.4.0 pour positionner les utilisateurs VPN par rapport à Identity Services Engine (ISE).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- VPN d'accès à distance AnyConnect
- Configuration VPN d'accès à distance sur le FTD
- Services Identity Services Engine et services de posture

Composants utilisés

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

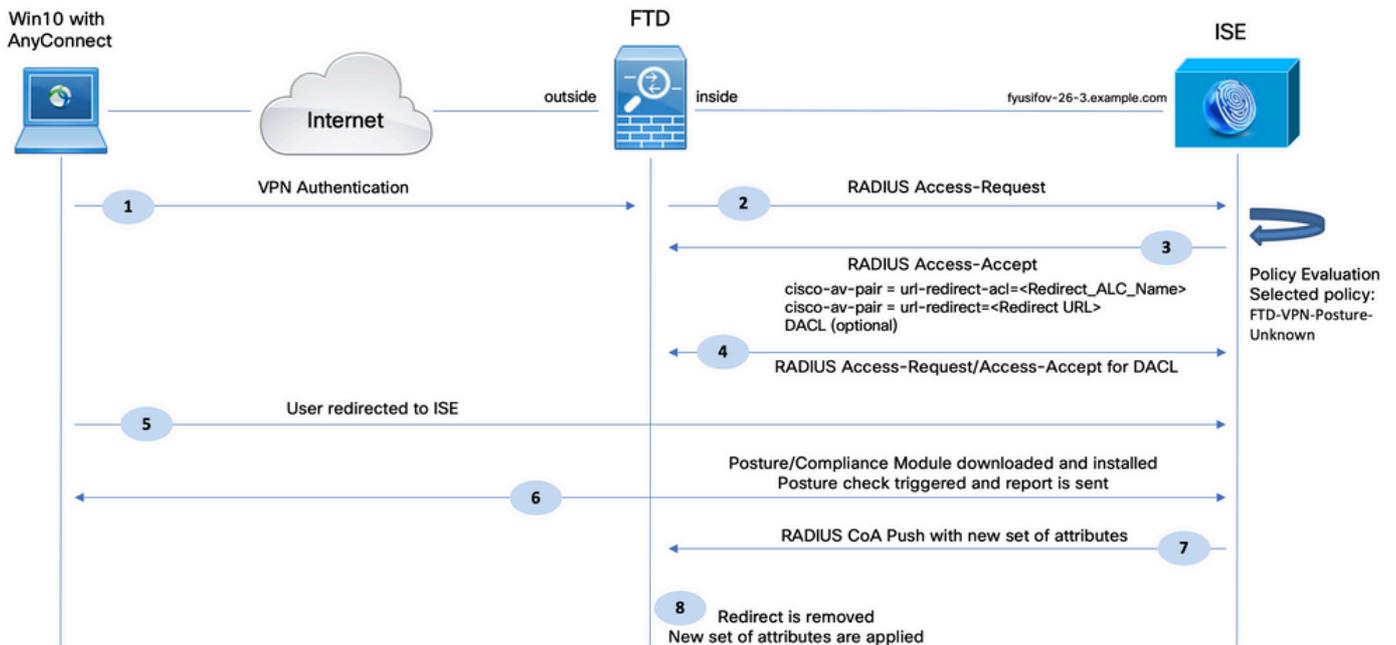
- Logiciel Cisco Firepower Threat Defense (FTD) versions 6.4.0
- Logiciel Cisco Firepower Management Console (FMC) version 6.5.0
- Microsoft Windows 10 avec Cisco AnyConnect Secure Mobility Client version 4.7
- Cisco Identity Services Engine (ISE) version 2.6 avec patch 3

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.

Configurer

Diagramme et flux du trafic du réseau



1. L'utilisateur distant utilise Cisco Anyconnect pour l'accès VPN au FTD.

2. Le FTD envoie une requête d'accès RADIUS pour cet utilisateur à l'ISE.

3. Cette demande atteint la stratégie nommée FTD-VPN-Posture-Unknown sur l'ISE. L'ISE envoie un message d'acceptation d'accès RADIUS avec trois attributs :

- cisco-av-pair = url-redirect-acl=fyusifovredirect - Il s'agit du nom de la liste de contrôle d'accès (ACL) définie localement sur le FTD, qui décide du trafic qui est redirigé.
- cisco-av-pair = url-redirect=<https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp> - Il s'agit de l'URL vers laquelle l'utilisateur distant est redirigé.
- DACL = PERMIT_ALL_IPV4_TRAFFIC - ACL téléchargeable : cet attribut est facultatif. Dans ce scénario, tout le trafic est autorisé dans DACL)

4. Si la DACL est envoyée, RADIUS Access-Request/Access-Accept est échangé afin de télécharger le contenu de la DACL

5. Lorsque le trafic provenant de l'utilisateur VPN correspond à la liste de contrôle d'accès définie localement, il est redirigé vers le portail d'approvisionnement du client ISE. ISE provisionne le module de posture et le module de conformité AnyConnect.

6. Une fois l'agent installé sur l'ordinateur client, il recherche automatiquement ISE avec des sondes. Lorsque ISE est détecté avec succès, les exigences de posture sont vérifiées sur le terminal. Dans cet exemple, l'agent recherche tout logiciel anti-programme malveillant installé. Il envoie ensuite un rapport de position à l'ISE.

7. Lorsqu'ISE reçoit le rapport de position de l'agent, elle modifie l'état de position pour cette session et déclenche le type RADIUS CoA Push avec de nouveaux attributs. Cette fois, l'état de la position est connu et une autre règle est activée.

- Si l'utilisateur est conforme, un nom DACL autorisant un accès complet est envoyé.
- Si l'utilisateur n'est pas conforme, un nom DACL autorisant un accès limité est envoyé.

8. Le FTD supprime la redirection. FTD envoie une requête d'accès afin de télécharger la liste de contrôle d'accès depuis ISE. La liste de contrôle d'accès spécifique est attachée à la session VPN.

Configurations

FTD/FMC

Étape 1. Créez un groupe d'objets réseau pour ISE et les serveurs de conversion (le cas échéant). Accédez à Objets > Gestion des objets > Réseau.

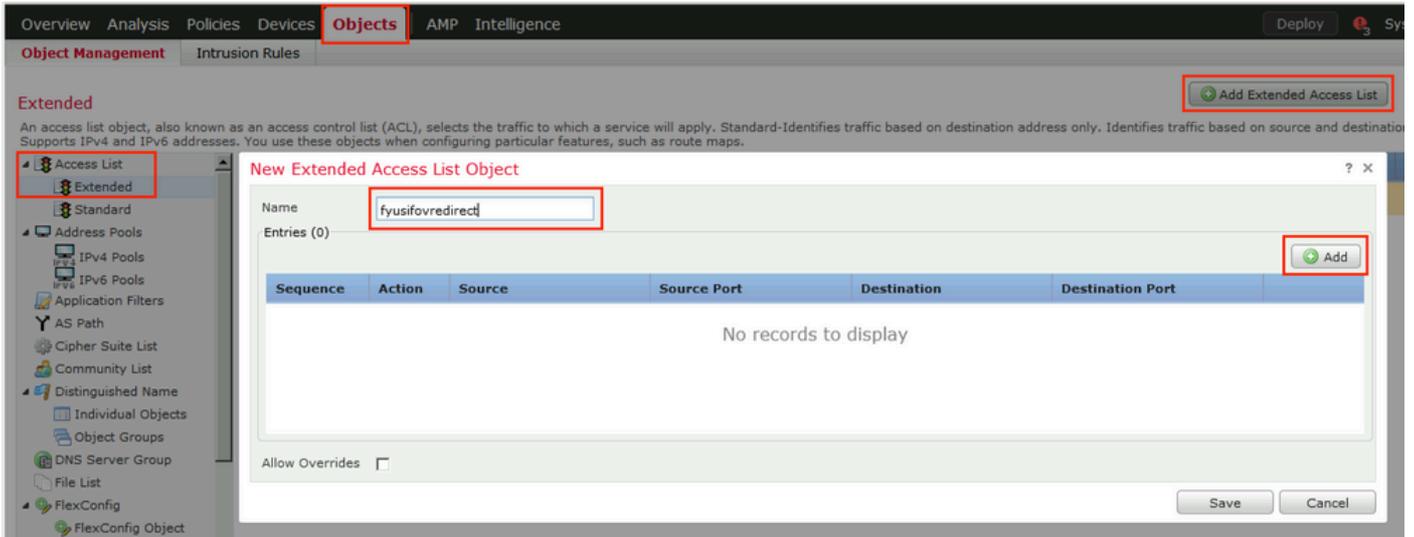
The screenshot displays the Cisco FTD/FMC configuration interface. The 'Objects' menu is selected, and the 'Edit Network Object' dialog box is open. The dialog box has the following fields and options:

- Name:** ISE_PSN
- Description:** (empty)
- Network:** 192.168.15.14
- Network Type:** Host (selected), Range, Network, FQDN
- Allow Overrides:** (unchecked)

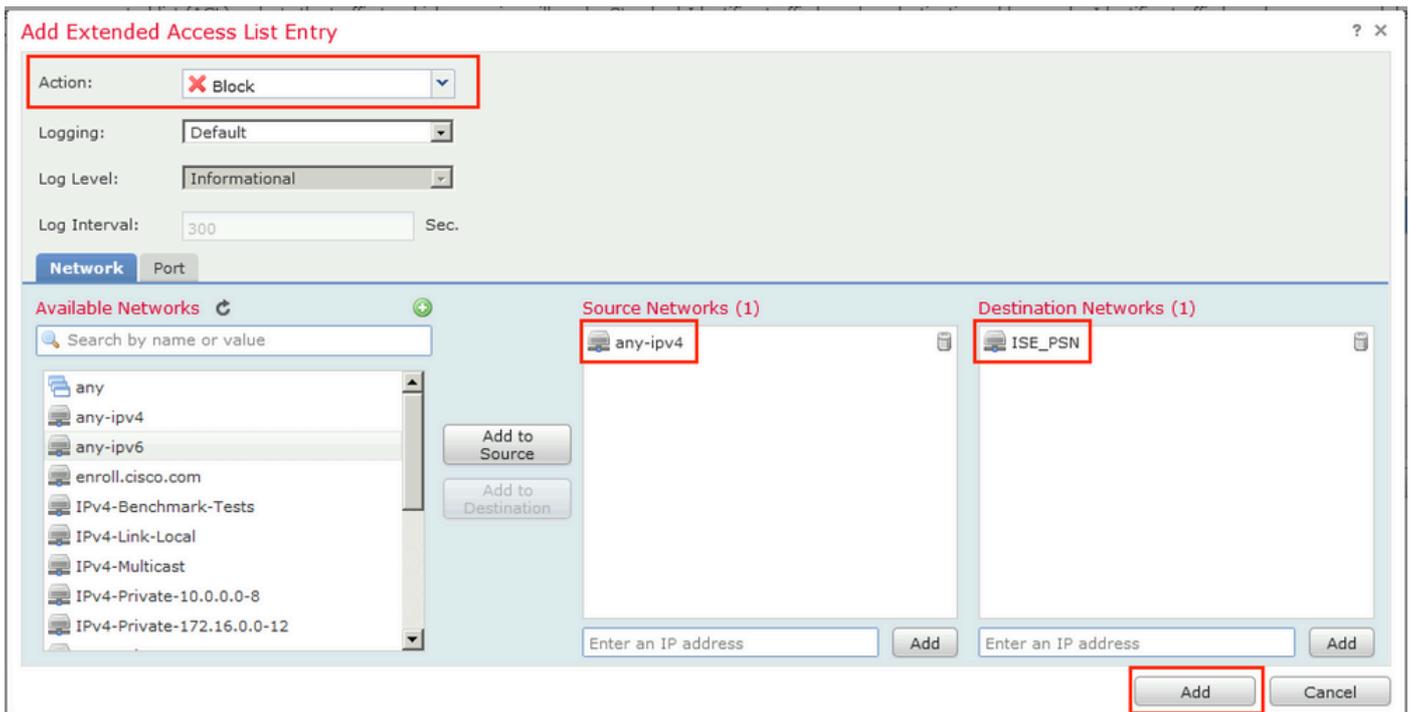
The background shows a table of network objects:

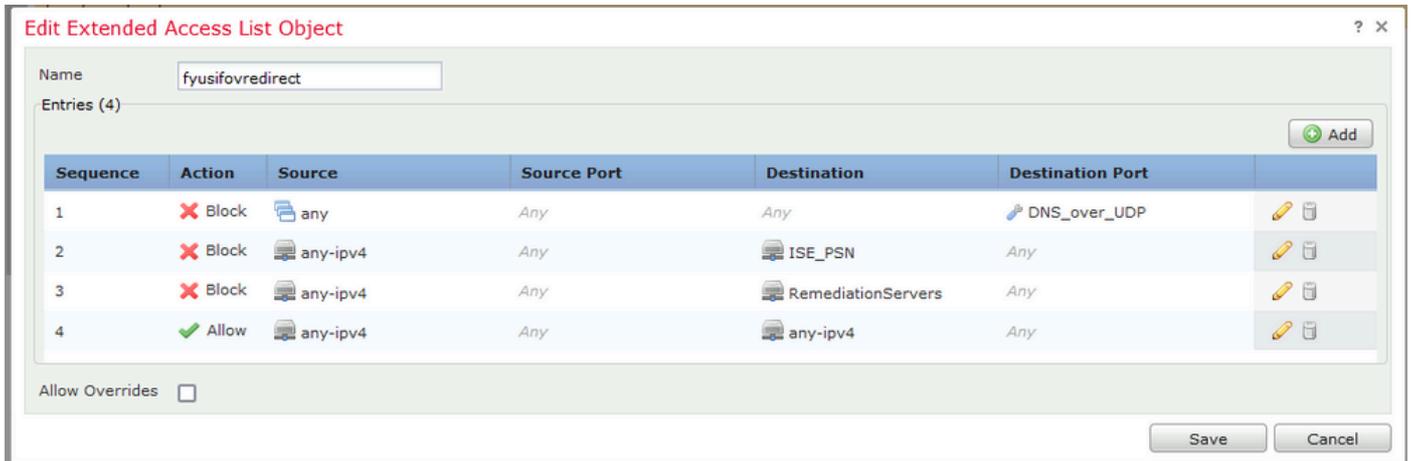
Name	Value
any-ipv4	0.0.0.0/0
any-ipv6	::/0
enroll.cisco.com	72.163.1.80
IPV4-Benchmark-Tests	
IPV4-Link-Local	
IPV4-Multicast	
IPV4-Private-10.0.0.0-8	
IPV4-Private-172.16.0.0-12	
IPV4-Private-192.168.0.0-16	
IPV4-Private-All-RFC1918	
IPV6-IPV4-Mapped	::ffff:0.0.0.0/96
IPV6-Link-Local	fe80::/10
IPV6-Private-Unique-Local-Addresses	fc00::/7
IPV6-to-IPV4-Relay-Anycast	192.88.99.0/24

Étape 2. Créer une ACL de redirection. Accédez à Objets > Gestion des objets > Liste d'accès > Étendue. Cliquez sur Add Extended Access List et fournissez le nom de Redirect ACL. Ce nom doit être le même que dans le résultat de l'autorisation ISE.



Étape 3. Ajouter des entrées ACL de redirection. Cliquez sur le bouton Add. Bloquez le trafic vers DNS, ISE et les serveurs de conversion pour les exclure de la redirection. Autorisez le reste du trafic, ce qui déclenche la redirection (les entrées de la liste de contrôle d'accès peuvent être plus spécifiques si nécessaire).





Étape 4. Ajoutez des noeuds PSN ISE. Accédez à Objets > Gestion des objets > Groupe de serveurs RADIUS. Cliquez sur Add RADIUS Server Group, puis fournissez un nom, activez toutes les cases à cocher et cliquez sur l'icône plus.

Edit RADIUS Server Group ? X

Name:* ISE

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
No records to display

Save Cancel

Étape 5. Dans la fenêtre ouverte, fournissez l'adresse IP du PSN ISE, la clé RADIUS, sélectionnez Specific Interface et sélectionnez l'interface à partir de laquelle ISE est accessible (cette interface est utilisée comme source de trafic RADIUS), puis sélectionnez Redirect ACL qui a été configuré précédemment.

New RADIUS Server

IP Address/Hostname:* Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:* (1-65535)

Key:*

Confirm Key:*

Accounting Port: (1-65535)

Timeout: (1-300) Seconds

Connect using: Routing Specific Interface i

Redirect ACL: +

+

Étape 6. Créez un pool d'adresses pour les utilisateurs VPN. Accédez à Objets > Gestion des objets > Pools d'adresses > Pools IPv4. Cliquez sur Add IPv4 Pools et renseignez les détails.

Overview Analysis Policies Devices **Objects** AMP Intelligence Deploy 5

Object Management Intrusion Rules + Add IPv4 Pools

IPv4 Pools IPv4 Pools

IPv4 pool contains list of IPv4 addresses, it is used for diagnostic interface with clustering, or for VPN remote access profiles.

Edit IPv4 Pool

Name*

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

Mask

Description

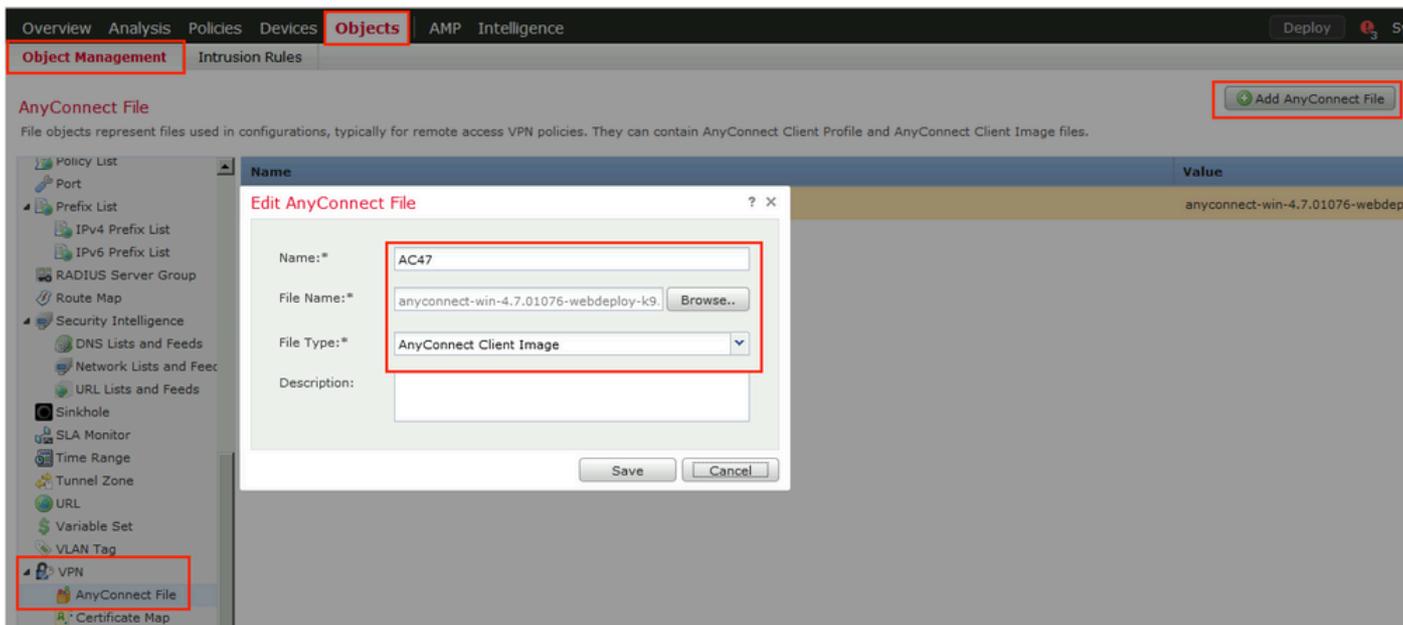
Allow Overrides

Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

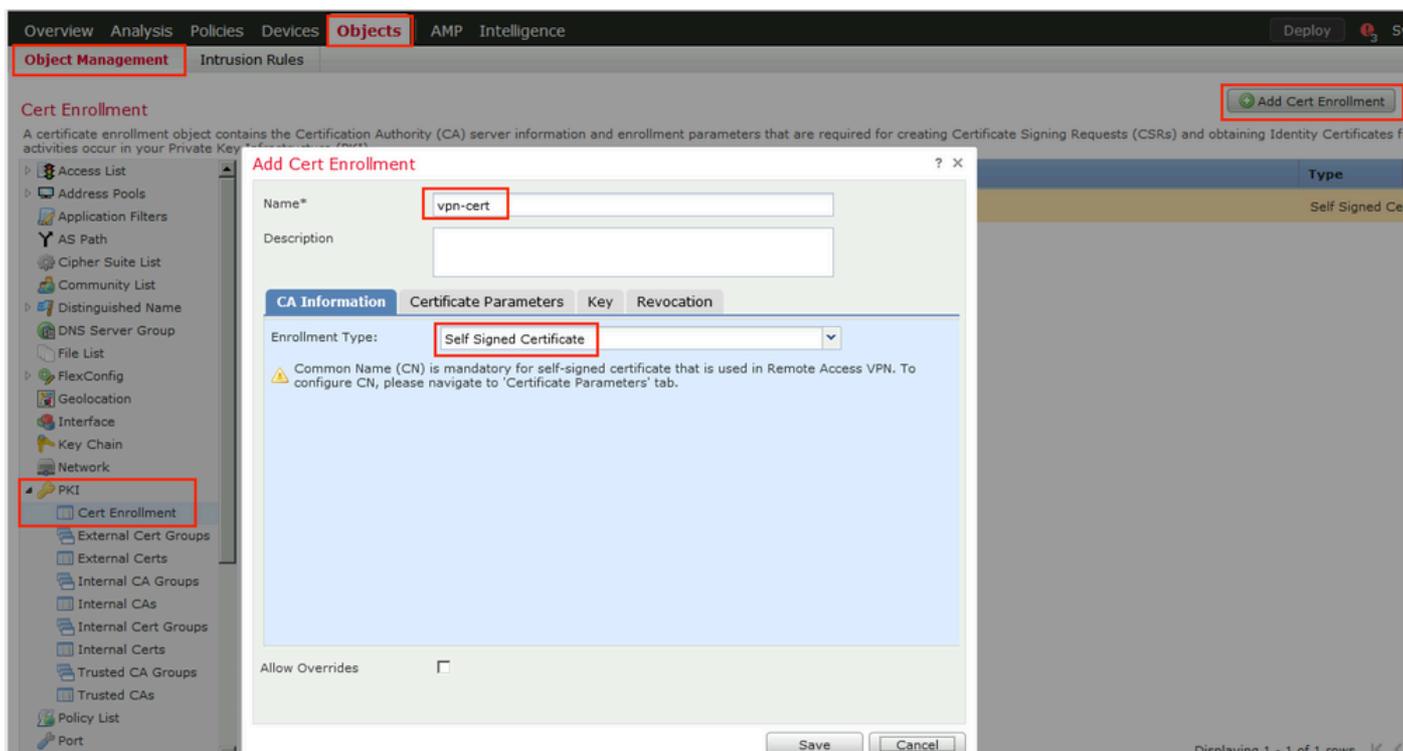
Override (0)

Étape 7. Créez un package AnyConnect. Accédez à Objets > Gestion des objets > VPN > Fichier AnyConnect. Cliquez sur Add AnyConnect File, fournissez le nom du package, téléchargez le

package à partir de [Cisco Software Download](#) et sélectionnez Anyconnect Client Image File Type.



Étape 8. Accédez à Objets de certificat > Gestion des objets > PKI > Inscription de certificat. Cliquez sur Add Cert Enrollment, fournissez un nom, choisissez Self Signed Certificate in Enrollment Type. Cliquez sur l'onglet Certificate Parameters et indiquez CN.



Add Cert Enrollment

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):

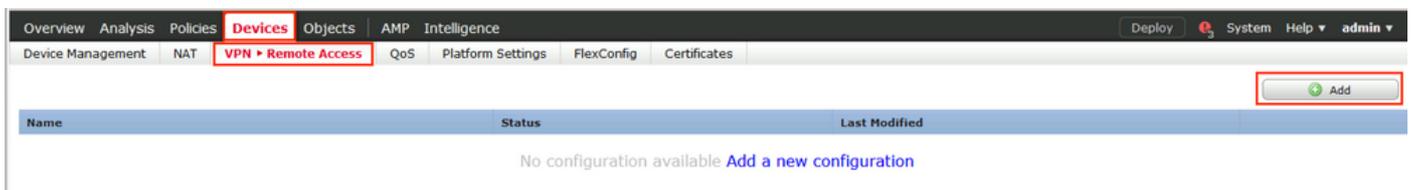
Email (E):

Include Device's Serial Number

Allow Overrides

Save Cancel

Étape 9. Lancez l'assistant VPN d'accès à distance. Accédez à Devices > VPN > Remote Access et cliquez sur Add.



Étape 10. Fournissez le nom, cochez SSL as VPN Protocol, choisissez FTD qui est utilisé comme concentrateur VPN et cliquez sur Next.

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:
192.168.15.11

Selected Devices:

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

Étape 11. Fournissez le nom du profil de connexion, sélectionnez Serveurs d'authentification/de comptabilité, sélectionnez le pool d'adresses qui a été configuré précédemment et cliquez sur Suivant.

 Remarque : ne sélectionnez pas le serveur d'autorisation. Il déclenche deux demandes d'accès pour un seul utilisateur (une fois avec le mot de passe utilisateur et la deuxième fois avec le mot de passe cisco).

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:

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) ⓘ

Use DHCP Servers

Use IP Address Pools

IPv4 Address:

IPv6 Address:

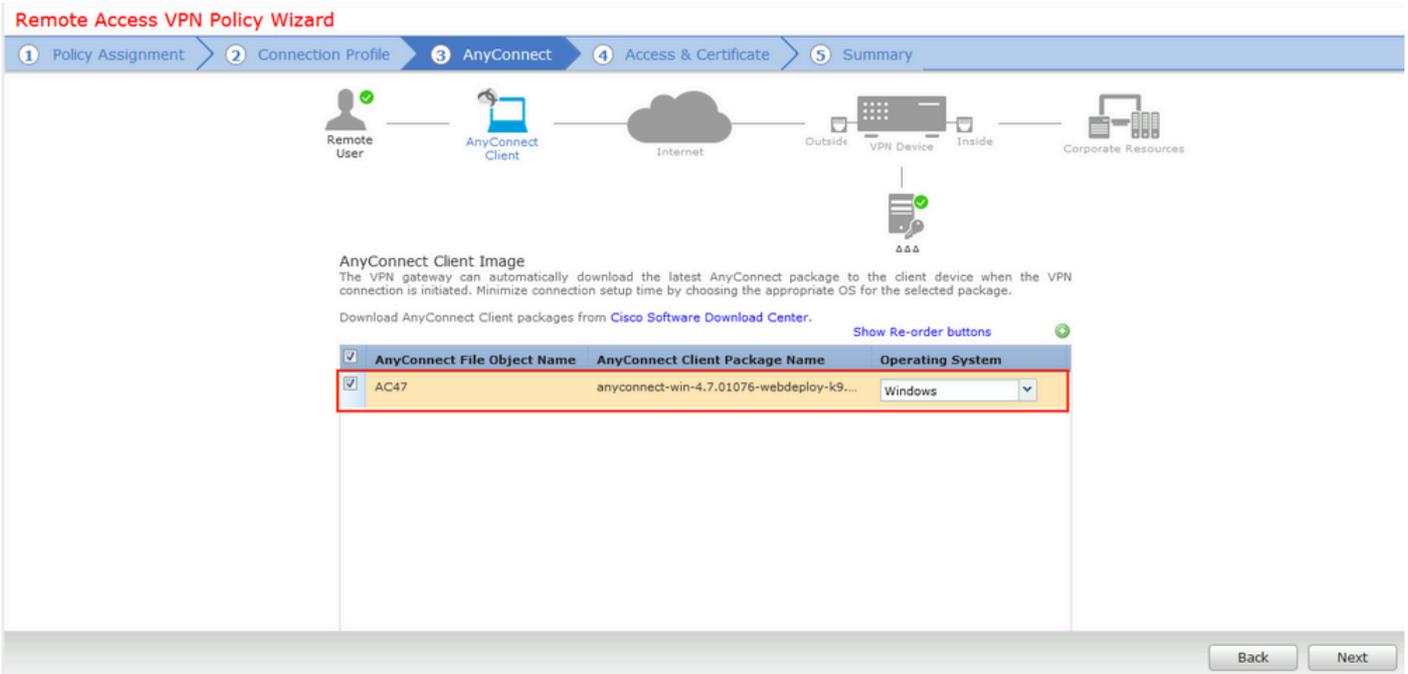
Group Policy:

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.

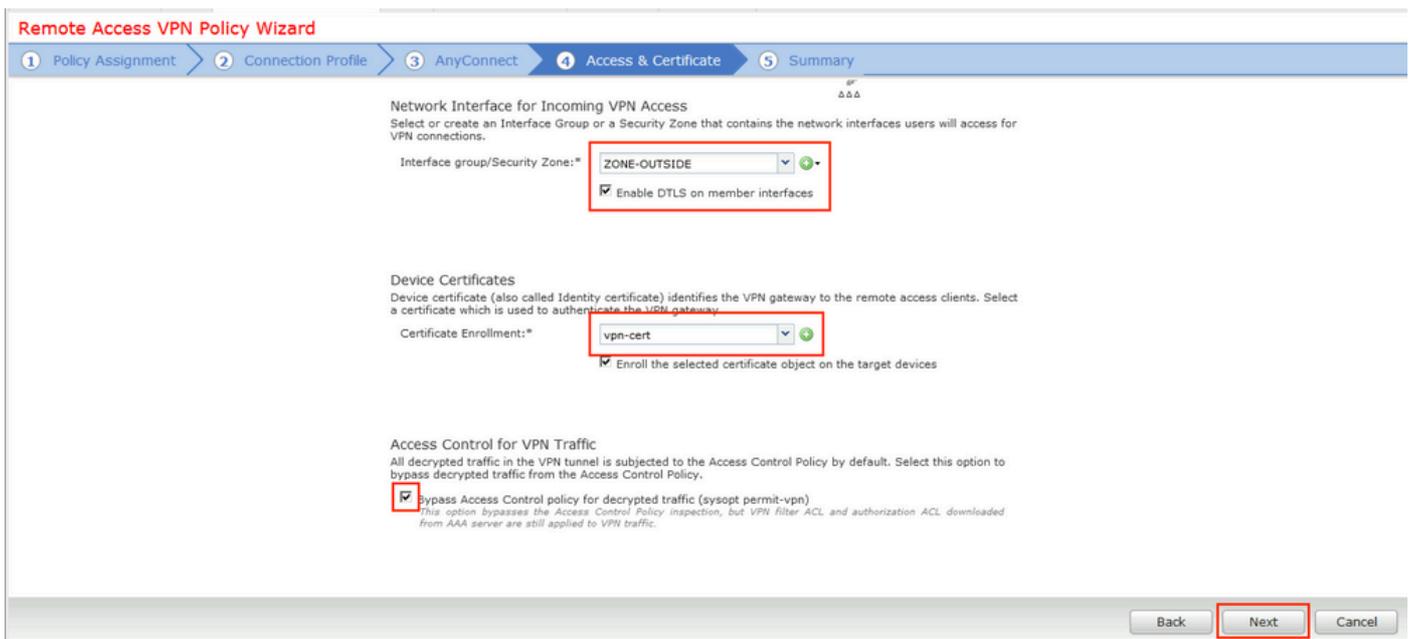
Group Policy:* ⓘ
[Edit Group Policy](#)

Back Next Cancel

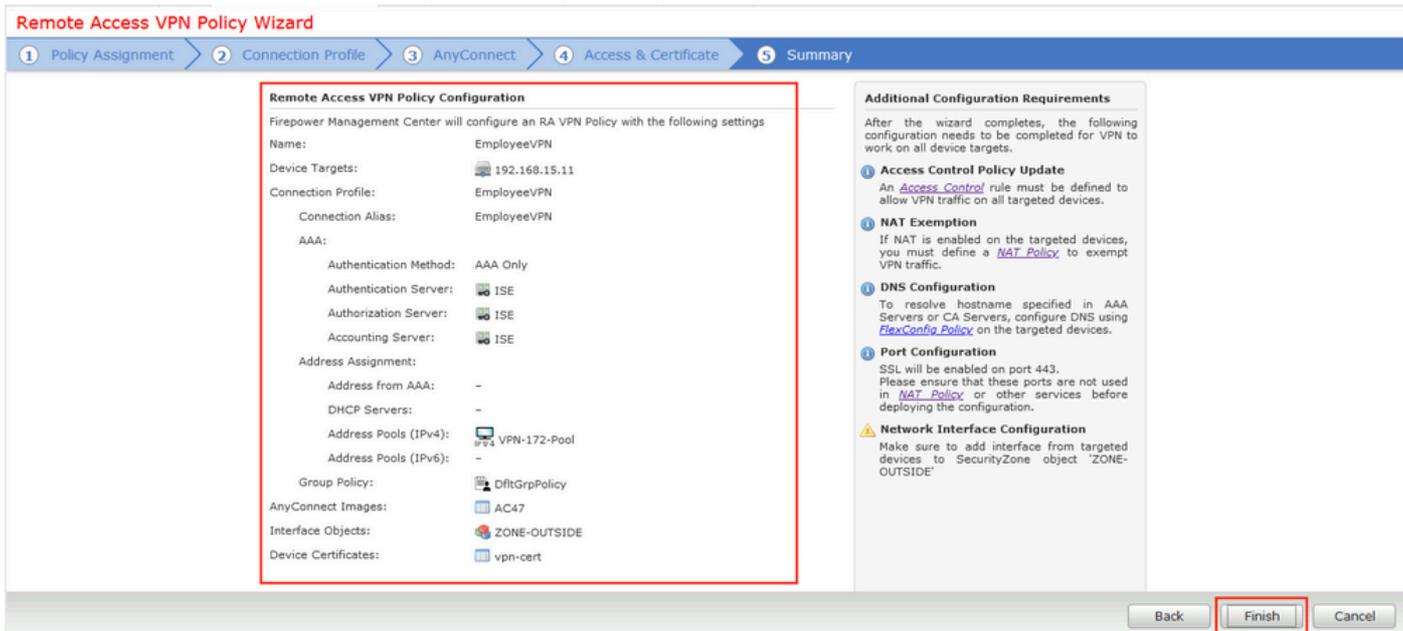
Étape 12. Sélectionnez le package AnyConnect qui a été configuré précédemment et cliquez sur Next.



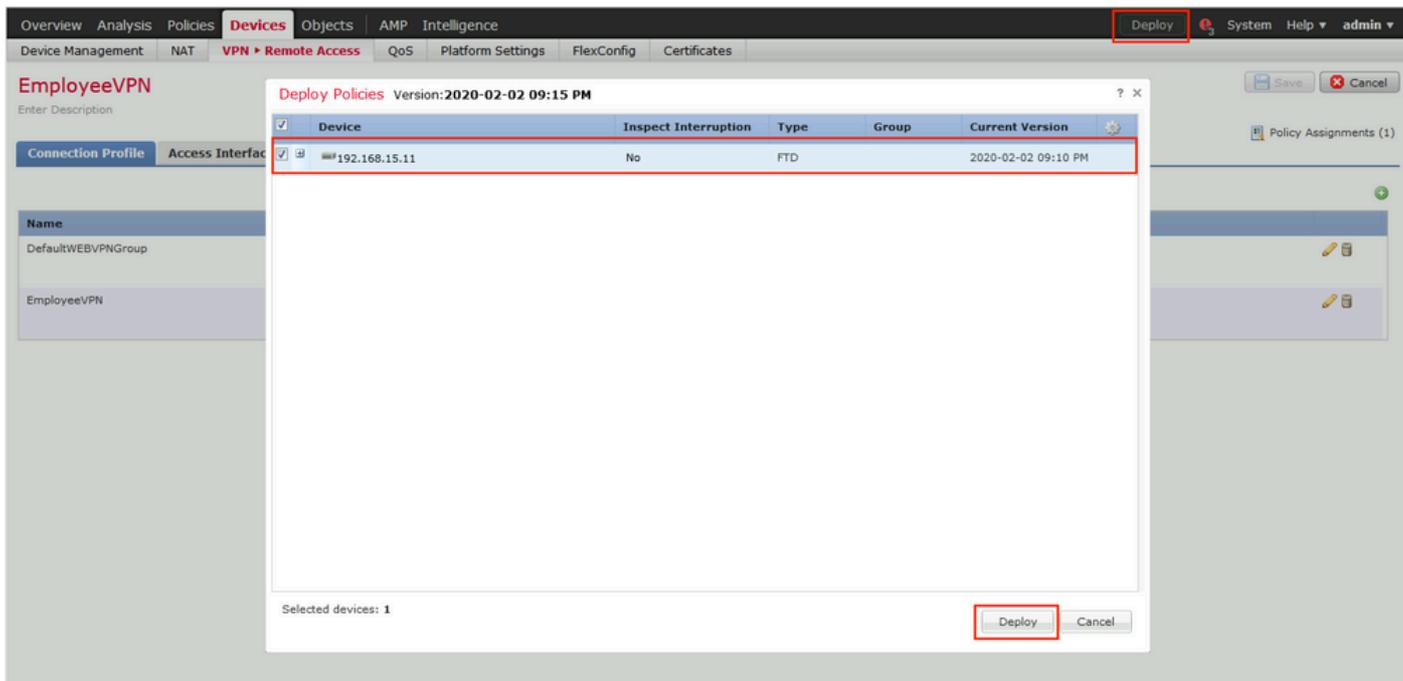
Étape 13. Sélectionnez l'interface à partir de laquelle le trafic VPN est attendu, sélectionnez Certificate Enrollment qui a été configuré précédemment et cliquez sur Next.



Étape 14. Consultez la page de résumé et cliquez sur Terminer.



Étape 15. Déployer la configuration sur FTD. Cliquez sur Deploy et sélectionnez FTD qui est utilisé comme concentrateur VPN.



ISE

Étape 1. Exécutez les mises à jour de posture. Accédez à Administration > System > Settings > Posture > Updates.

Posture Updates

Web Offline

* Update Feed URL

Proxy Address ⓘ

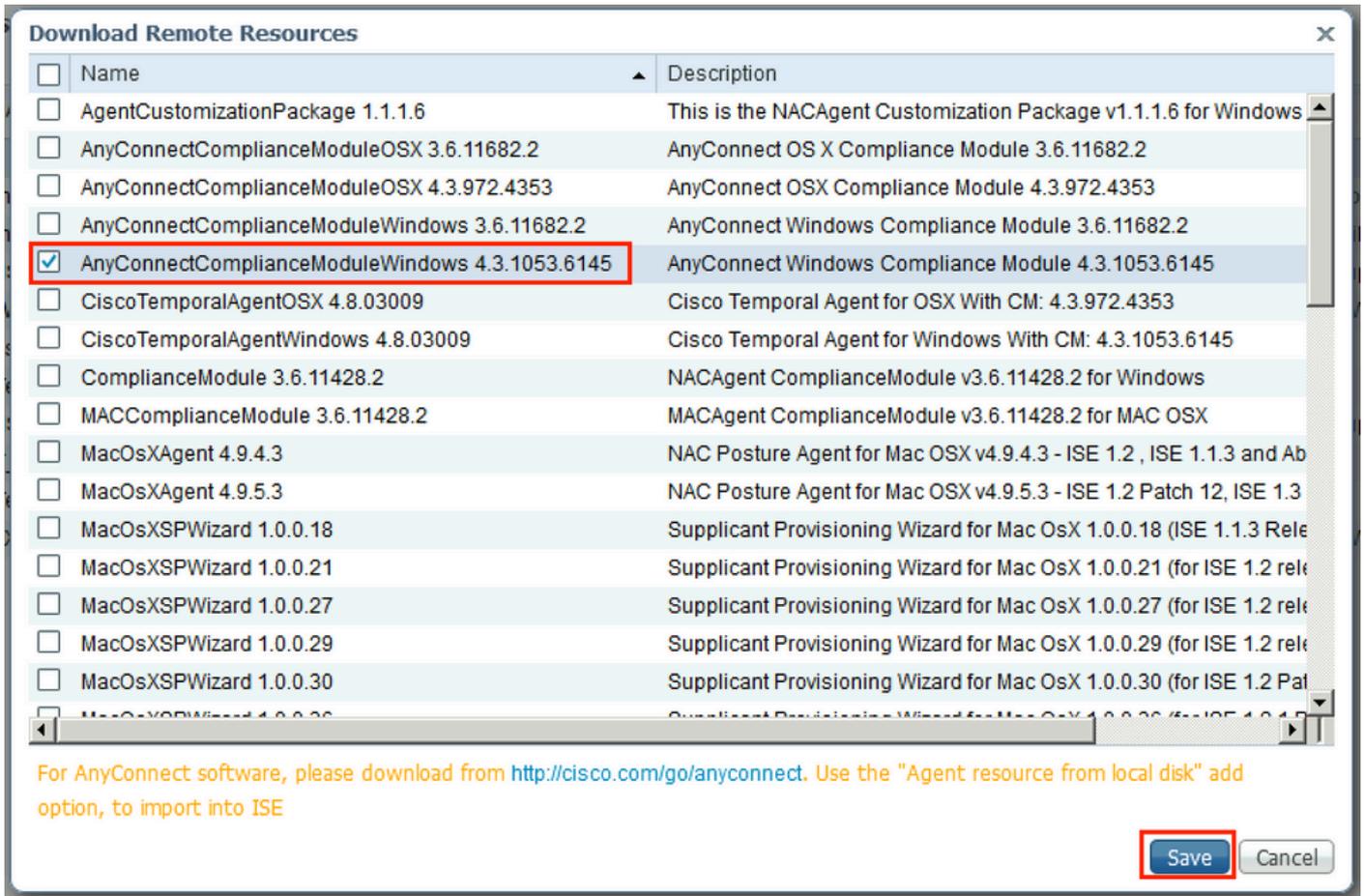
Proxy Port HH MM SS

Automatically check for updates starting from initial delay every hours ⓘ

▼ Update Information

Last successful update on	2020/02/02 20:44:27 ⓘ
Last update status since ISE was started	Last update attempt at 2020/02/02 20:44:27 was successful ⓘ
Cisco conditions version	257951.0.0.0
Cisco AV/AS support chart version for windows	227.0.0.0
Cisco AV/AS support chart version for Mac OSX	148.0.0.0
Cisco supported OS version	49.0.0.0

Étape 2. Téléchargez le module de conformité. Accédez à Policy > Policy Elements > Results > Client Provisioning > Resources. Cliquez sur Add et sélectionnez Agent resources from Cisco site



Étape 3. Téléchargez AnyConnect à partir de [Cisco Software Download](http://cisco.com/go/anyconnect), puis téléchargez-le vers ISE. Accédez à Policy > Policy Elements > Results > Client Provisioning > Resources.

Cliquez sur Add et sélectionnez Agent Resources From Local Disk. Choisissez Cisco Provided Packages sous Category, sélectionnez le package AnyConnect à partir du disque local et cliquez sur Submit.

Agent Resources From Local Disk > Agent Resources From Local Disk
Agent Resources From Local Disk

Category

▼ AnyConnect Uploaded Resources

Name	Type	Version	Description
AnyConnectDesktopWindows 4.7.10...	AnyConnectDesktopWindows	4.7.1076.0	AnyConnect Secure Mobility Cle...

Submit Cancel

Étape 4. Créez un profil de position AnyConnect. Accédez à Policy > Policy Elements > Results > Client Provisioning > Resources.

Cliquez sur Add et sélectionnez AnyConnect Posture Profile. Renseignez le nom et le protocole de posture.

Sous *Server name rules, placez * et placez toute adresse IP factice sous Discovery host.

ISE Posture Agent Profile Settings > AC_Posture_Profile

* Name:

Description:

Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	<input type="text" value="120"/> secs		This is the agent retry period if there is a Passive Reassessment communication failure
Discovery host	<input type="text" value="1.2.3.4"/>		The server that the agent should connect to
* Server name rules	<input type="text" value="*"/>	need to be blank by default to force admin to enter a value. "*" means agent will connect to all	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. *.cisco.com
Call Home List	<input type="text"/>	List of IP addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPAddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)	A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer	<input type="text" value="30"/> secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.	Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

Étape 5. Accédez à Policy > Policy Elements > Results > Client Provisioning > Resources et créez AnyConnect Configuration. Cliquez sur Add et sélectionnez AnyConnect Configuration.

Sélectionnez AnyConnect Package, indiquez le nom de la configuration, sélectionnez Compliance Module, activez Diagnostic and Reporting Tool, sélectionnez Posture Profile et cliquez sur Save.

* Select AnyConnect Package: AnyConnectDesktopWindows 4.7.1076.0

* Configuration Name: AC CF 47

Description:

DescriptionValue **Notes**

* Compliance Module: AnyConnectComplianceModuleWindows 4.3.1012.6

AnyConnect Module Selection

- ISE Posture
- VPN
- Network Access Manager
- Web Security
- AMP Enabler
- ASA Posture
- Network Visibility
- Umbrella Roaming Security
- Start Before Logon
- Diagnostic and Reporting Tool**

Profile Selection

- * ISE Posture: AC_Posture_Profile
- VPN
- Network Access Manager
- Web Security
- AMP Enabler
- Network Visibility
- Umbrella Roaming Security
- Customer Feedback

Étape 6. Accédez à Policy > Client Provisioning et créez Client Provisioning Policy. Cliquez sur Edit, puis sélectionnez Insert Rule Above, fournissez un nom, sélectionnez OS et choisissez AnyConnect Configuration qui a été créé à l'étape précédente.

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers | License Warning

Policy Sets | Profiling | Posture | Client Provisioning | Policy Elements

Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
 For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
 For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
AC_47_Win	If Any	and Windows All	and Condition(s)	then AC_CF_47
IOS	If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP
Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP
Windows	If Any	and Windows All	and Condition(s)	then CiscoTemporalAgentWindows 4.7.00135 And WinSPWizard 2.5.0.1 And Cisco-ISE-NSP
MAC OS	If Any	and Mac OSX	and Condition(s)	then CiscoTemporalAgentIOSX 4.7.00135 And MacOSXSPWizard 2.1.0.42 And Cisco-ISE-NSP
Chromebook	If Any	and Chrome OS All	and Condition(s)	then Cisco-ISE-Chrome-NSP

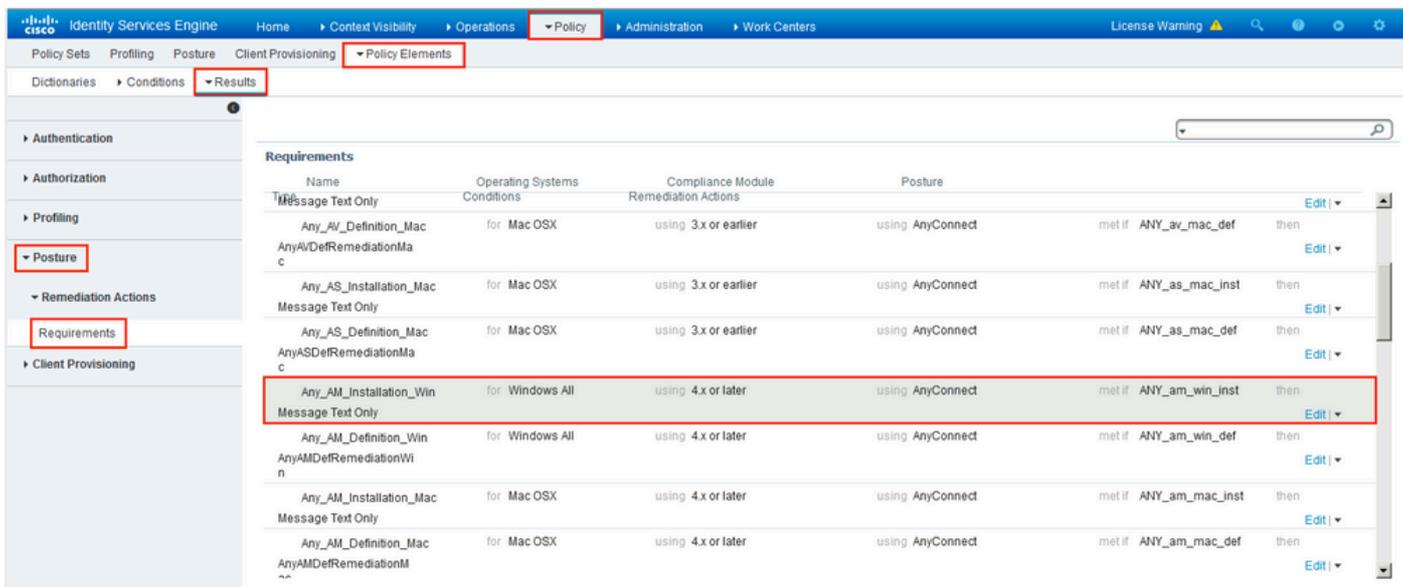
Étape 7. Créez une condition de posture sous Stratégie > Éléments de stratégie > Conditions > Posture > Condition anti-programme malveillant. Dans cet exemple, "ANY_am_win_inst" prédéfini est utilisé.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The breadcrumb navigation is: Policy > Policy Elements > Conditions > Posture > Anti-Malware Condition. The main content area displays a table of Anti-Malware Conditions. The condition 'ANY_am_win_inst' is highlighted with a red box.

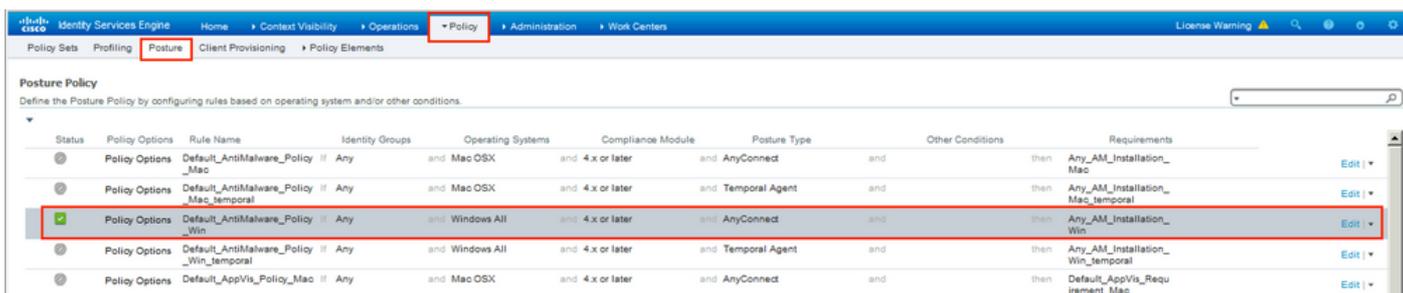
Name	Description
<input type="checkbox"/> ANY_am_win_inst	Any AM installation check on Wi...
<input type="checkbox"/> ANY_am_win_def	Any AM definition check on Wind...
<input type="checkbox"/> ANY_am_mac_inst	Any AM installation check on Mac
<input type="checkbox"/> ANY_am_mac_def	Any AM definition check on Mac

Étape 8. Naviguez jusqu'à Policy > Policy Elements > Results > Posture > Remediation Actions et créez Posture Remediation. Dans cet exemple, il est ignoré. L'action corrective peut être un message texte.

Étape 9. Accédez à Policy > Policy Elements > Results > Posture > Requirements et créez Posture Requirements. Condition prédéfinie : Any_AM_Installation_Win est utilisé.



Étape 10. Créez des stratégies de posture sous Stratégies > Posture. La stratégie de posture par défaut de tout contrôle anti-programme malveillant pour le système d'exploitation Windows est utilisée.



Étape 11. Accédez à Policy > Policy Elements > Results > Authorization > Downloadable ACLS et créez des DACL pour différents états de posture.

Dans cet exemple :

- DACL Posture Unknown : autorise le trafic vers DNS, PSN, HTTP et HTTPS.
- DACL non conforme à la position : refuse l'accès aux sous-réseaux privés et autorise uniquement le trafic Internet.
- Permet All DACL : autorise tout le trafic pour l'état de conformité à la position.

Downloadable ACL

* Name

Description

IP version IPv4 IPv6 Agnostic 

* DACL Content

1234567	permit	udp	any	any	eq	domain
8910111	permit	ip	any	host		192.168.15.14
2131415	permit	tcp	any	any	eq	80
1617181	permit	tcp	any	any	eq	443
9202122						
2324252						
6272829						
3031323						
3343536						
3738394						

Downloadable ACL

* Name

Description

IP version IPv4 IPv6 Agnostic 

* DACL Content

1234567	deny	ip	any	10.0.0.0	255.0.0.0	
8910111	deny	ip	any	172.16.0.0	255.240.0.0	
2131415	deny	ip	any	192.168.0.0	255.255.0.0	
1617181	permit	ip	any	any		
9202122						
2324252						
6272829						
3031323						
3343536						
3738394						

Downloadable ACL

* Name

Description

IP version IPv4 IPv6 Agnostic 

* DACL Content

123456	permit	ip	any	any		
7891011						
121314						
151617						
181920						
212223						
242526						
272829						
303132						
333435						
363738						

 Check DACL Syntax



et Posture Compliant. Pour ce faire, accédez à Policy > Policy Elements > Results > Authorization > Authorization Profiles. Dans le profil Posture Unknown, sélectionnez Posture Unknown DACL, cochez Web Redirection, sélectionnez Client Provisioning, fournissez le nom de la liste de contrôle d'accès de redirection (qui est configurée sur FTD) et sélectionnez le portail.

Authorization Profiles > **New Authorization Profile**

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

▼ **Common Tasks**

DACL Name

Web Redirection (CWA, MDM, NSP, CPP) ⓘ

ACL Value

▼ **Attributes Details**

Access Type = ACCESS_ACCEPT
DACL = PostureUnknown
cisco-av-pair = url-redirect-acl=fyusifovredirect
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp

Dans le profil Posture NonCompliant, sélectionnez DACL afin de limiter l'accès au réseau.

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

DACL Name

Attributes Details

Access Type = ACCESS_ACCEPT
DACL = PostureNonCompliant

Dans le profil Posture Compliant, sélectionnez DACL afin d'autoriser l'accès complet au réseau.

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

DACL Name

Attributes Details

Access Type = ACCESS_ACCEPT
DACL = PermitAll

Étape 13. Créez des stratégies d'autorisation sous Stratégie > Jeux de stratégies > Par défaut > Stratégie d'autorisation. En tant que condition Posture Status et VNP TunnelGroup Name est utilisé.

The screenshot shows the Cisco ISE Policy configuration interface. The 'Policy' tab is active, and the 'Authorization Policy (18)' section is expanded. Three policies are listed:

Status	Rule Name	Conditions	Results	Hits	Actions
✔	FTD-VPN-Posture-Compliant	AND Session PostureStatus EQUALS Compliant Cisco-VPN3000 CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS EmployeeVPN	PermitAll	4	+
✔	FTD-VPN-Posture-NonCompliant	AND Session PostureStatus EQUALS NonCompliant Cisco-VPN3000 CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS EmployeeVPN	FTD-VPN-NonCompliant	0	+
✔	FTD-VPN-Posture-Unknown	AND Session PostureStatus EQUALS Unknown Cisco-VPN3000 CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS EmployeeVPN	FTD-VPN-Redirect	9	+

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Sur ISE, la première étape de vérification est RADIUS Live Log. Accédez à Operations > RADIUS Live Log. Ici, l'utilisateur Alice est connecté et la stratégie d'autorisation attendue est sélectionnée.

The screenshot shows the RADIUS Live Log interface. The 'Live Logs' tab is active, and the log entry for 'Feb 03, 2020 07:13:29.73...' is highlighted. The log entry details are as follows:

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Pr...	Authenticat...	Authorizati...	Authorizati...	IP Address	Network Device	Device Port	Identity Group	Posture Sta...
Feb 03, 2020 07:13:31.92...	✔	...	0	alice@training.e...	00:0C:29:5C:5A:96	Windows10...	Default >> ...	Default >> ...	FTD-VPN-R...	172.16.1.10	FTD			Pending
Feb 03, 2020 07:13:29.74...	✔	...		#ACSACL#IP.P...										
Feb 03, 2020 07:13:29.73...	✔	...		alice@training.e...	00:0C:29:5C:5A:96	Windows10...	Default >> ...	Default >> ...	FTD-VPN-R...		FTD		Workstation	Pending

La stratégie d'autorisation FTD-VPN-Posture-Unknown est mise en correspondance et, par conséquent, FTD-VPN-Profile est envoyé à FTD.

Overview

Event 5200 Authentication succeeded

Username alice@training.example.com

Endpoint Id 00:0C:29:5C:5A:96 ⓘ

Endpoint Profile Windows10-Workstation

Authentication Policy Default >> Default

Authorization Policy Default >> FTD-VPN-Posture-Unknown

Authorization Result FTD-VPN-Redirect

Authentication Details

Source Timestamp 2020-02-03 07:13:29.738

Received Timestamp 2020-02-03 07:13:29.738

Policy Server fysisfov-26-3

Event 5200 Authentication succeeded

Username alice@training.example.com

État de la position en attente.

NAS IPv4 Address 192.168.15.15

NAS Port Type Virtual

Authorization Profile FTD-VPN-Redirect

Posture Status Pending

Response Time 365 milliseconds

La section Résultat indique quels attributs sont envoyés au FTD.

Result

Class	CACS:000000000000c0005e37c81a:fyusifov-26-3/368560500/45
cisco-av-pair	url-redirect-acl=fyusifovredirect
cisco-av-pair	url-redirect=https://fyusifov-26-3.example.com:8443/portal/gateway?sessionId=000000000000c0005e37c81a&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp&token=0d90f1cdf40e83039a7ad6a226603112
cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-PostureUnknown-5e37414d
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base and Apex license consumed

Sur FTD, afin de vérifier la connexion VPN, établissez une connexion SSH au boîtier, exécutez la commande `system support diagnostic-cli` et ensuite `show vpn-sessiondb detail anyconnect`. À partir de ce résultat, vérifiez que les attributs envoyés depuis ISE sont appliqués pour cette session VPN.

```
<#root>
```

```
fyusifov-ftd-64#
```

```
show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username      : alice@training.example.com
```

```
Index         : 12
```

```
Assigned IP   : 172.16.1.10
```

```
Public IP    : 10.229.16.169
```

```
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
```

```
License      : AnyConnect Premium
```

```
Encryption   : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
```

```
Hashing      : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
```

```
Bytes Tx     : 15326 Bytes Rx      : 13362
```

```
Pkts Tx      : 10 Pkts Rx       : 49
```

```
Pkts Tx Drop : 0 Pkts Rx Drop  : 0
```

```
Group Policy : DfltGrpPolicy
```

```
Tunnel Group : EmployeeVPN
```

```
Login Time   : 07:13:30 UTC Mon Feb 3 2020
```

```
Duration     : 0h:06m:43s
```

```
Inactivity   : 0h:00m:00s
```

```
VLAN Mapping : N/A VLAN           : none
```

```
Audt Sess ID : 000000000000c0005e37c81a
```

Security Grp : none Tunnel Zone : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 12.1
Public IP : 10.229.16.169
Encryption : none Hashing : none
TCP Src Port : 56491 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 23 Minutes
Client OS : win
Client OS Ver: 10.0.18363
Client Type : AnyConnect

Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076

Bytes Tx : 7663 Bytes Rx : 0
Pkts Tx : 5 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 12.2
Assigned IP : 172.16.1.10 Public IP : 10.229.16.169
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 56495
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 23 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076
Bytes Tx : 7663 Bytes Rx : 592
Pkts Tx : 5 Pkts Rx : 7
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Filter Name : #ACSACL#-IP-PostureUnknown-5e37414d

DTLS-Tunnel:

Tunnel ID : 12.3
Assigned IP : 172.16.1.10 Public IP : 10.229.16.169
Encryption : AES256 Hashing : SHA1
Ciphersuite : DHE-RSA-AES256-SHA
Encapsulation: DTLSv1.0 UDP Src Port : 59396
UDP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076
Bytes Tx : 0 Bytes Rx : 12770
Pkts Tx : 0 Pkts Rx : 42
Pkts Tx Drop : 0 Pkts Rx Drop : 0

Filter Name : #ACSACL#-IP-PostureUnknown-5e37414d

ISE Posture:

Redirect URL : <https://fyusifov-26-3.example.com:8443/portal/gateway?sessionId=00000000000c0005e37c81>
Redirect ACL : fyusifovredirect

fyusifov-ftd-64#

Les stratégies de provisionnement client peuvent être vérifiées. Accédez à Operations > Reports > Endpoints and Users > Client Provisioning.

Client Provisioning

From 2020-02-03 00:00:00.0 to 2020-02-03 08:14:07.0
Reports exported in last 7 days: 0

Logged At	Server	Event	Identity	Endpoint ID	IP Address	Client Provisioning Pol
Today	fyusifov-25-3	Client provisioning succeeded	alice@training.example.com	00:0C:29:5C:5A:96	172.16.1.10	AC_47_Win

Le rapport de position envoyé depuis AnyConnect peut être vérifié. Accédez à Operations > Reports > Endpoints and Users > Posture Assessment by Endpoint.

Posture Assessment by Endpoint

From 2020-02-03 00:00:00.0 to 2020-02-03 08:15:48.0
Reports exported in last 7 days: 0

Logged At	Status	Details	PRA Action	Identity	Endpoint ID	IP Address	Endpoint OS
Today	Success		N/A	alice@training.example.com	00:0C:29:5C:5A:96	172.16.1.10	Windows 10 Professional

Afin de voir plus de détails sur le rapport de posture, cliquez sur Détails.

Posture More Detail Assessment

From 2020-01-04 00:00:00.0 to 2020-02-03 08:13:36.0
Generated At: 2020-02-03 08:13:37.37

Client Details

Username	alice@training.example.com
Mac Address	00:0C:29:5C:5A:96
IP address	172.16.1.10
Location	All Locations
Session ID	00000000000c0005e37c81a
Client Operating System	Windows 10 Professional 64-bit
Client NAC Agent	AnyConnect Posture Agent for Windows 4.7.01076
PRA Enforcement	0
CoA	Received a posture report from an endpoint
PRA Grace Time	0
PRA Interval	0
PRA Action	N/A
User Agreement Status	NotEnabled
System Name	DESKTOP-IE3556M
System Domain	n/a

Une fois le rapport reçu sur ISE, l'état de la position est mis à jour. Dans cet exemple, l'état de posture est conforme et la poussée CoA est déclenchée avec un nouvel ensemble d'attributs.

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Pr...	Authenticat...	Authorizati...	Authorizati...	IP Address	Network Device	Device Port	Identity Group	Posture S
Feb 03, 2020 08:07:52.05...	✓	ⓘ		Identity	10.229.16.169	Endpoint Pr...	Authenticati...	Authorization	Authorization	IP Address	Network Device	Device Port	Identity Group	Posture S
Feb 03, 2020 08:07:50.03...	ⓘ	ⓘ	0	alice@training.e...	00:0C:29:5C:5A:96	Windows10...	Default >> ...	Default >> ...	FTD-VPN-R...	172.16.1.10	FTD	Device Port	Identity Group	Complia
Feb 03, 2020 07:13:29.74...	✓	ⓘ		#ACSACL#IP.P...							FTD			
Feb 03, 2020 07:13:29.73...	✓	ⓘ		alice@training.e...	00:0C:29:5C:5A:96	Windows10...	Default >> ...	Default >> ...	FTD-VPN-R...		FTD		Workstation	Pending

Last Updated: Mon Feb 03 2020 09:10:20 GMT+0100 (Central European Standard Time) Records Shown: 4

Overview

Event	5205 Dynamic Authorization succeeded
Username	
Endpoint Id	10.55.218.19 ⓘ
Endpoint Profile	
Authorization Result	PermitAll

Authentication Details

Source Timestamp	2020-02-03 16:58:39.687
Received Timestamp	2020-02-03 16:58:39.687
Policy Server	fysifov-26-3
Event	5205 Dynamic Authorization succeeded
Endpoint Id	10.55.218.19
Calling Station Id	10.55.218.19
Audit Session Id	000000000000e0005e385132
Network Device	FTD
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.168.15.15
Authorization Profile	PermitAll
Posture Status	Compliant
Response Time	2 milliseconds

Other Attributes

ConfigVersionId	21
Event-Timestamp	1580749119
Device CoA type	Cisco CoA
Device CoA port	1700
NetworkDeviceProfileId	b0699505-3150-4215-a80e-8753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	af49ce55-d55c-4778-ad40-b03ea12924d2
CoASourceComponent	Posture
CoAReason	posture status changed
CoAType	COA-push
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
Device IP Address	192.168.15.15
CiscoAVPair	audit-session-id=000000000000e0005e385132, coa-push=true, ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-PermitAll-5e384dc0

Vérifiez sur FTD que les nouvelles ACL de redirection et URL de redirection sont supprimées pour la session VPN et que la liste DACL PermitAll est appliquée.

```
<#root>
```

```
fyusifov-ftd-64#
```

```
show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username      :
```

```
alice@training.example.com
```

```
Index        : 14
```

```
Assigned IP   : 172.16.1.10      Public IP    : 10.55.218.19
```

Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Bytes Tx : 53990 Bytes Rx : 23808
Pkts Tx : 73 Pkts Rx : 120
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy Tunnel Group :

EmployeeVPN

Login Time : 16:58:26 UTC Mon Feb 3 2020
Duration : 0h:02m:24s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 000000000000e0005e385132
Security Grp : none Tunnel Zone : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 14.1
Public IP : 10.55.218.19
Encryption : none Hashing : none
TCP Src Port : 51965 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes
Client OS : win
Client OS Ver: 10.0.18363
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076
Bytes Tx : 7663 Bytes Rx : 0
Pkts Tx : 5 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 14.2
Assigned IP : 172.16.1.10 Public IP : 10.55.218.19
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 51970
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076
Bytes Tx : 7715 Bytes Rx : 10157
Pkts Tx : 6 Pkts Rx : 33
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Filter Name :

#ACSACL#-IP-PermitAll-5e384dc0

DTLS-Tunnel:

Tunnel ID : 14.3
Assigned IP : 172.16.1.10 Public IP : 10.55.218.19
Encryption : AES256 Hashing : SHA1
Ciphersuite : DHE-RSA-AES256-SHA
Encapsulation: DTLSv1.0 UDP Src Port : 51536
UDP Dst Port : 443 Auth Mode : userPassword

Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076
Bytes Tx : 38612 Bytes Rx : 13651
Pkts Tx : 62 Pkts Rx : 87
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Filter Name :

#ACSACL#-IP-PermitAll-5e384dc0

fyusifov-ftd-64#

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Pour un flux de posture détaillé et pour dépanner AnyConnect et ISE, cliquez sur ce lien : [Comparaison des styles de posture ISE pour Pre et Post 2.2.](#)

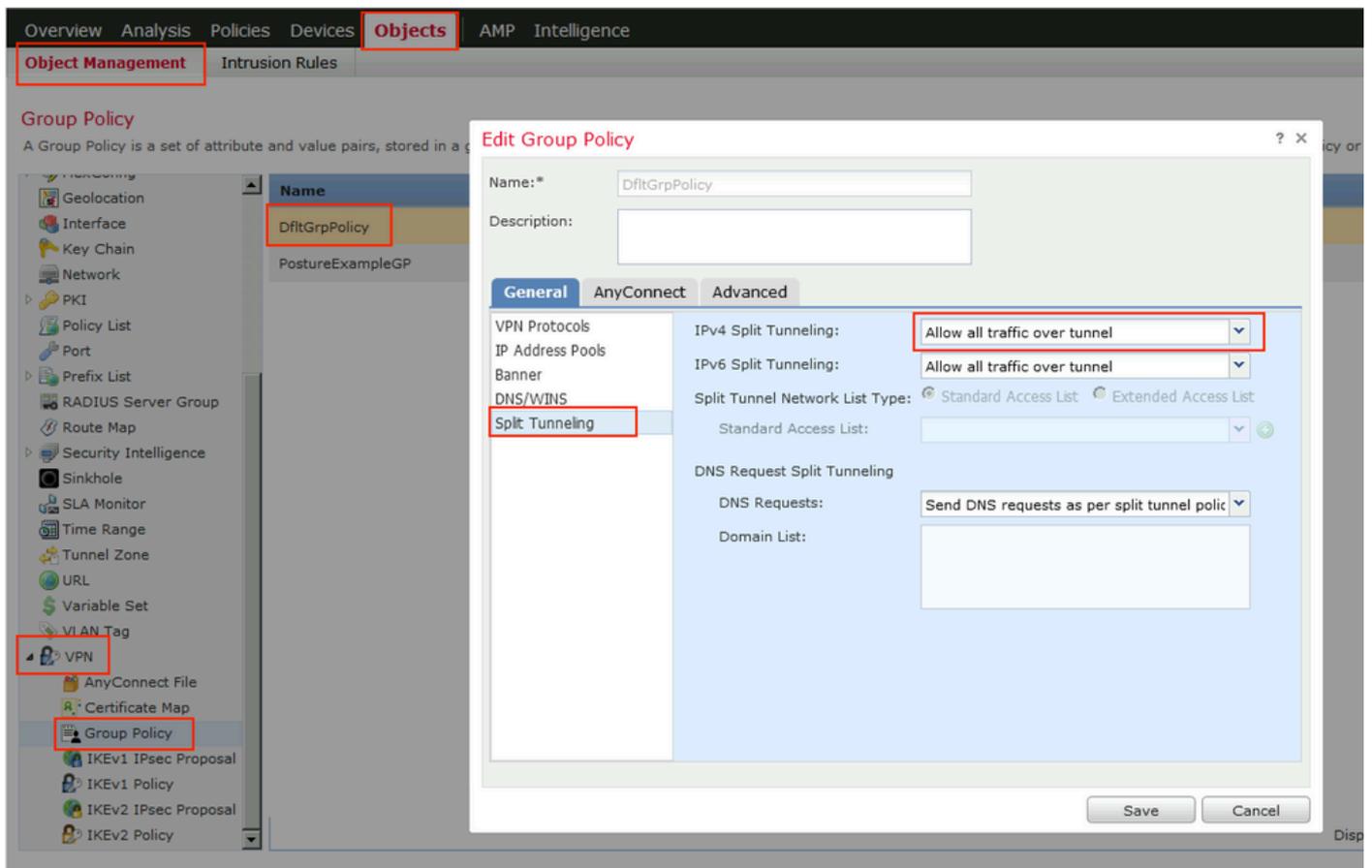
- Tunnel Fractionné

L'un des problèmes courants, lorsqu'il y a un tunnel de broche est configuré. Dans cet exemple, la stratégie de groupe par défaut est utilisée, ce qui permet de tunnels tout le trafic. Dans le cas où seul un trafic spécifique est tunnalisé, les sondes AnyConnect (enroll.cisco.com et hôte de découverte) doivent traverser le tunnel en plus du trafic vers ISE et d'autres ressources internes.

Afin de vérifier la stratégie de tunnel sur FMC, vérifiez d'abord quelle stratégie de groupe est utilisée pour la connexion VPN. Accédez à Devices > VPN Remote Access.

Name	AAA	Group Policy
DefaultWEBVPGGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy
EmployeeVPN	Authentication: ISE (RADIUS) Authorization: ISE (RADIUS) Accounting: ISE (RADIUS)	DfltGrpPolicy

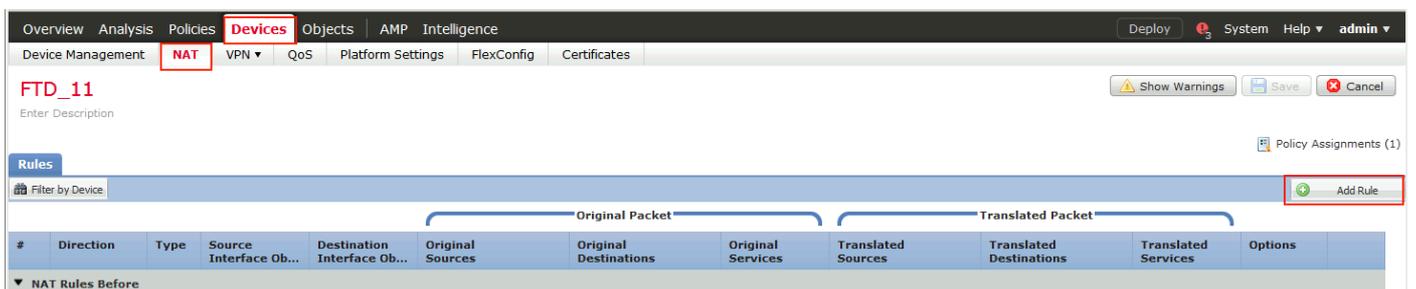
Accédez ensuite à Objects > Object Management > VPN > Group Policy et cliquez sur Group Policy configured for VPN.



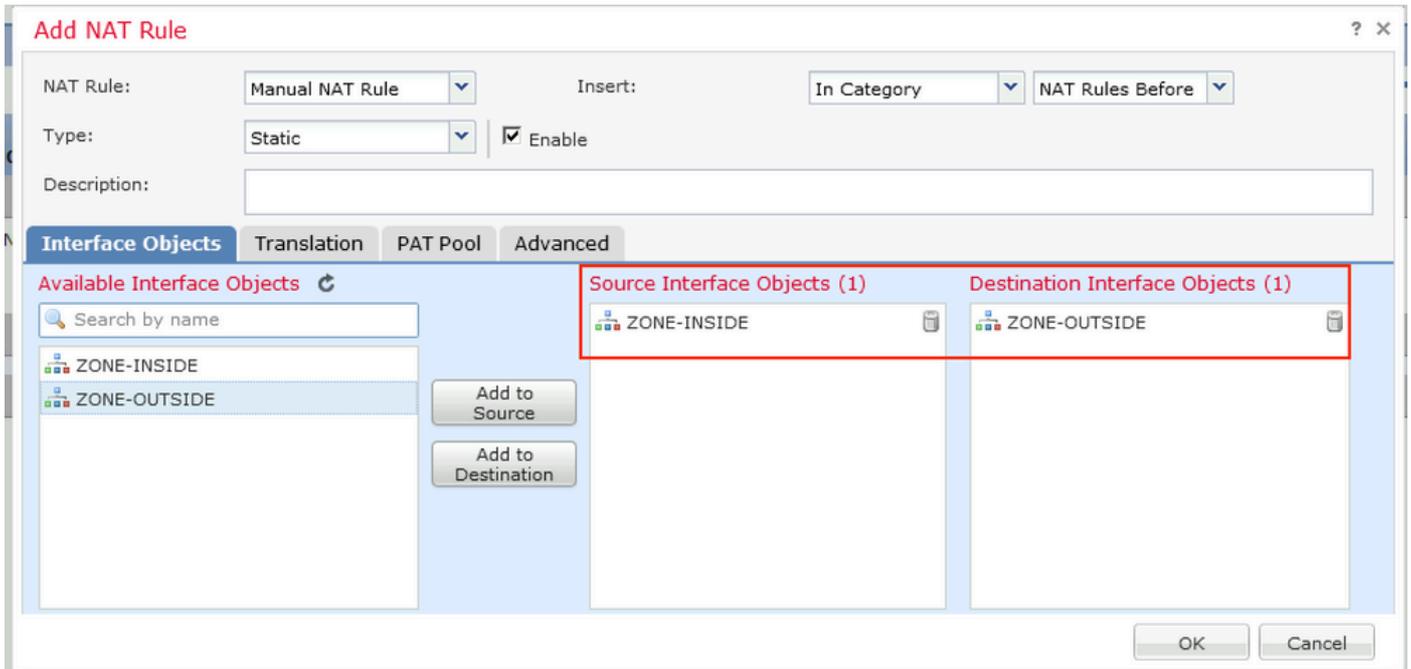
- NAT d'identité

Un autre problème courant, lorsque le trafic de retour des utilisateurs VPN est traduit avec l'utilisation d'une entrée NAT incorrecte. Afin de résoudre ce problème, la NAT d'identité doit être créée dans un ordre approprié.

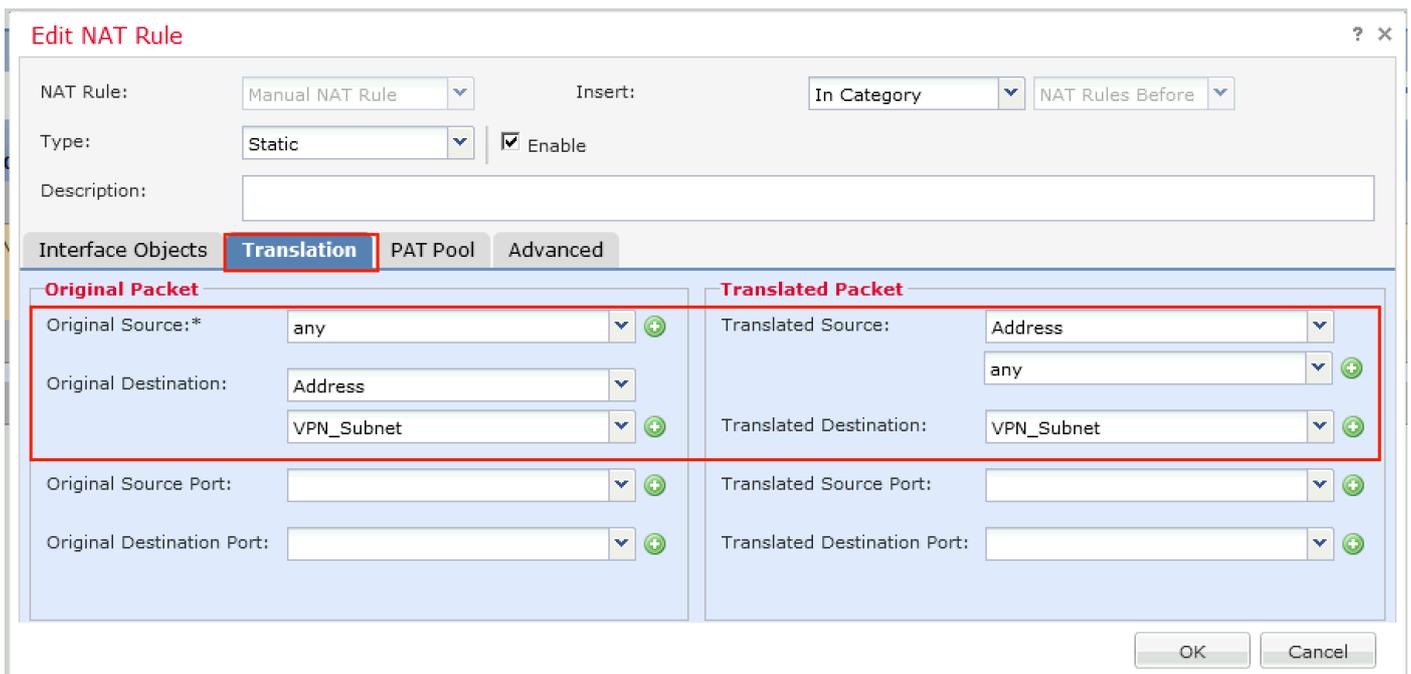
Tout d'abord, vérifiez les règles NAT pour ce périphérique. Accédez à **Devices > NAT**, puis cliquez sur **Add Rule** pour créer une nouvelle règle.



Dans la fenêtre ouverte, sous l'onglet **Interface Objects**, sélectionnez **Security Zones**. Dans cet exemple, l'entrée NAT est créée de **ZONE-INSIDE** à **ZONE-OUTSIDE**.



Sous l'onglet Translation, sélectionnez les détails des paquets d'origine et traduits. Comme il s'agit de la NAT d'identité, la source et la destination restent inchangées :



Sous l'onglet Advanced, cochez les cases comme indiqué dans cette 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

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.