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 :

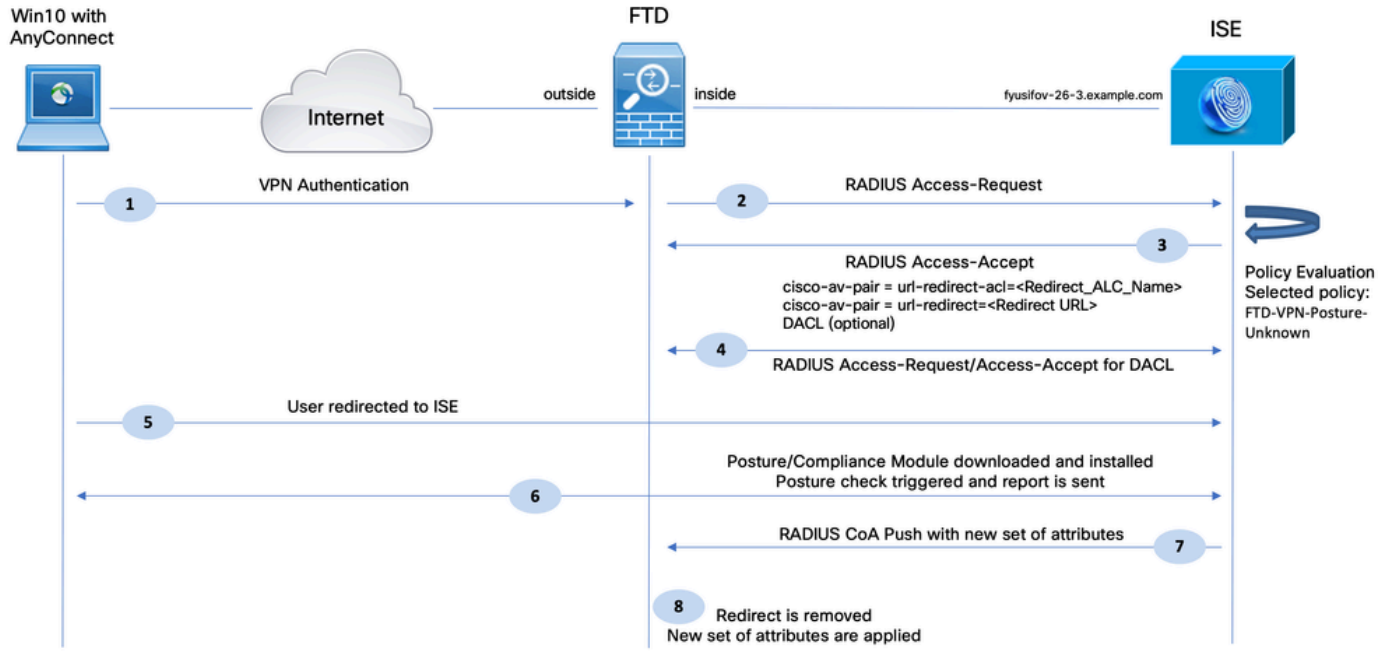
- Logiciel Cisco Firepower Threat Defense (FTD) versions 6.4.0
- Logiciel Cisco Firepower Management Console (FMC) version 6.5.0
- Microsoft Windows 10 avec Cisco AnyConnect Secure Mobility Client version 4.7
- Cisco Identity Services Engine (ISE) version 2.6 avec patch 3

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.

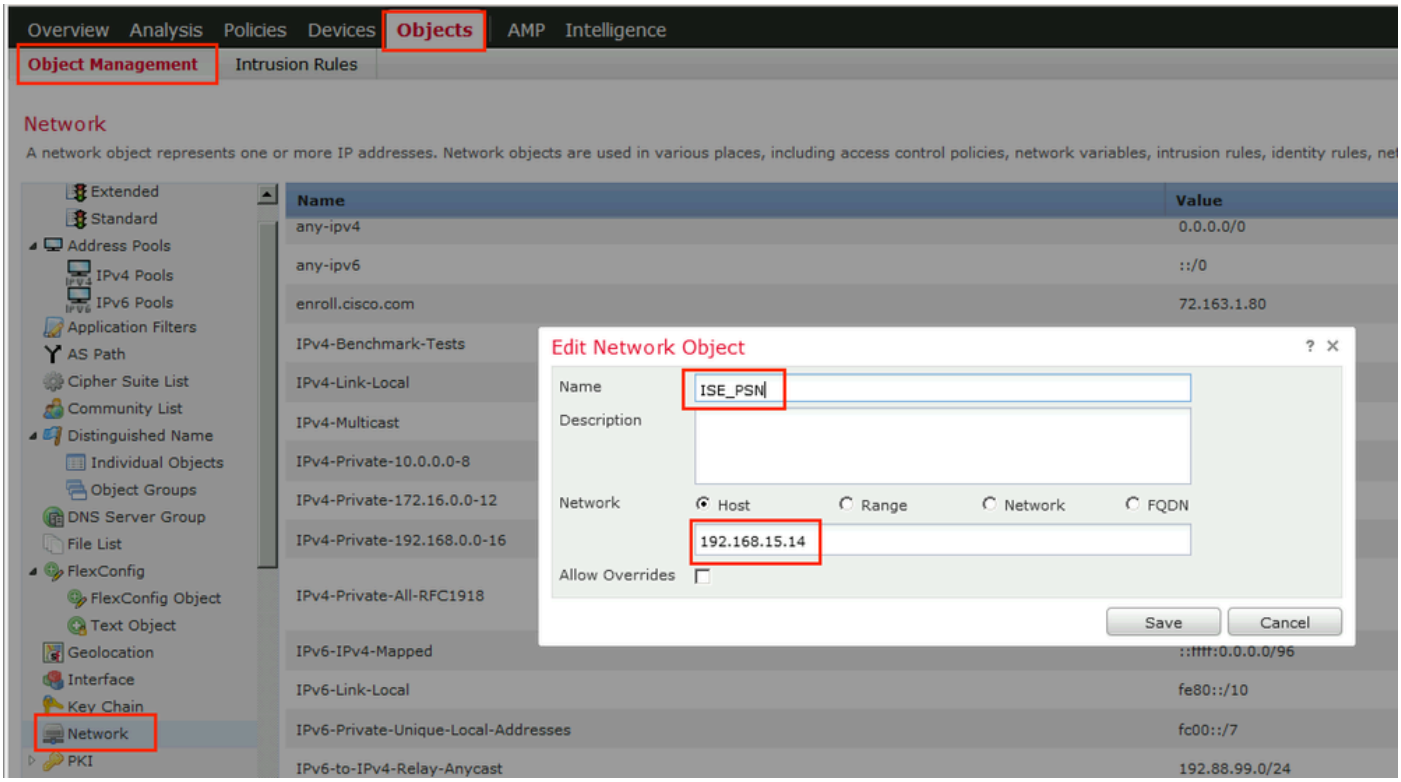
- Si l'utilisateur est conforme, un nom DACL autorisant un accès complet est envoyé.
- Si l'utilisateur n'est pas conforme, un nom DACL autorisant un accès limité est envoyé.

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.

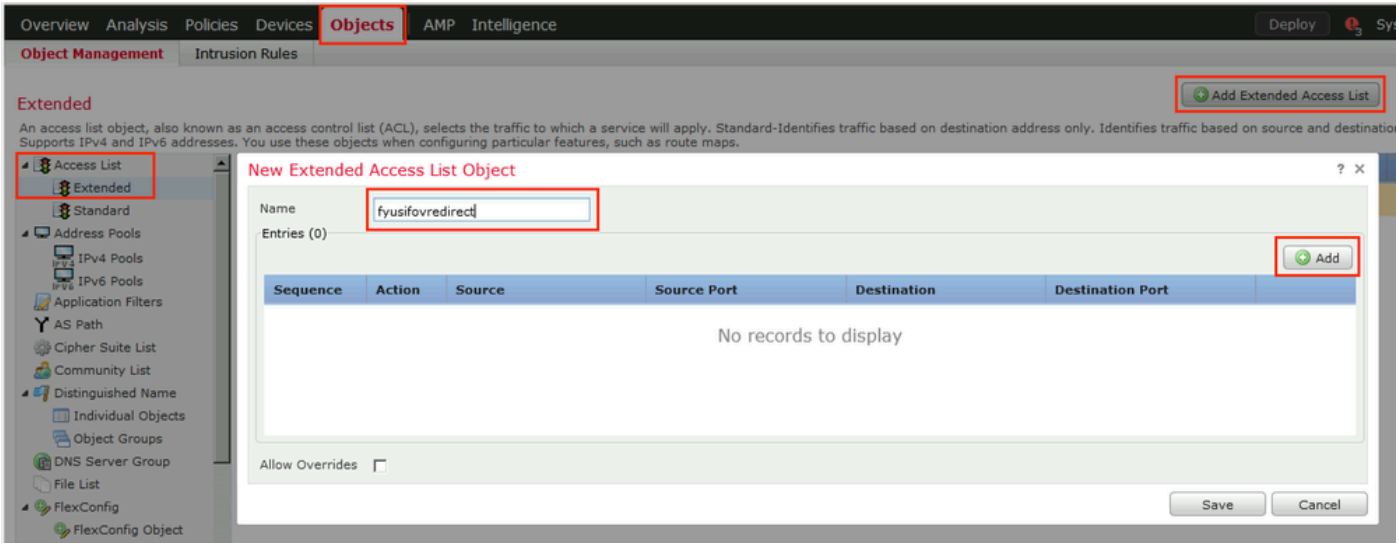
Configurations

FTD/FMC

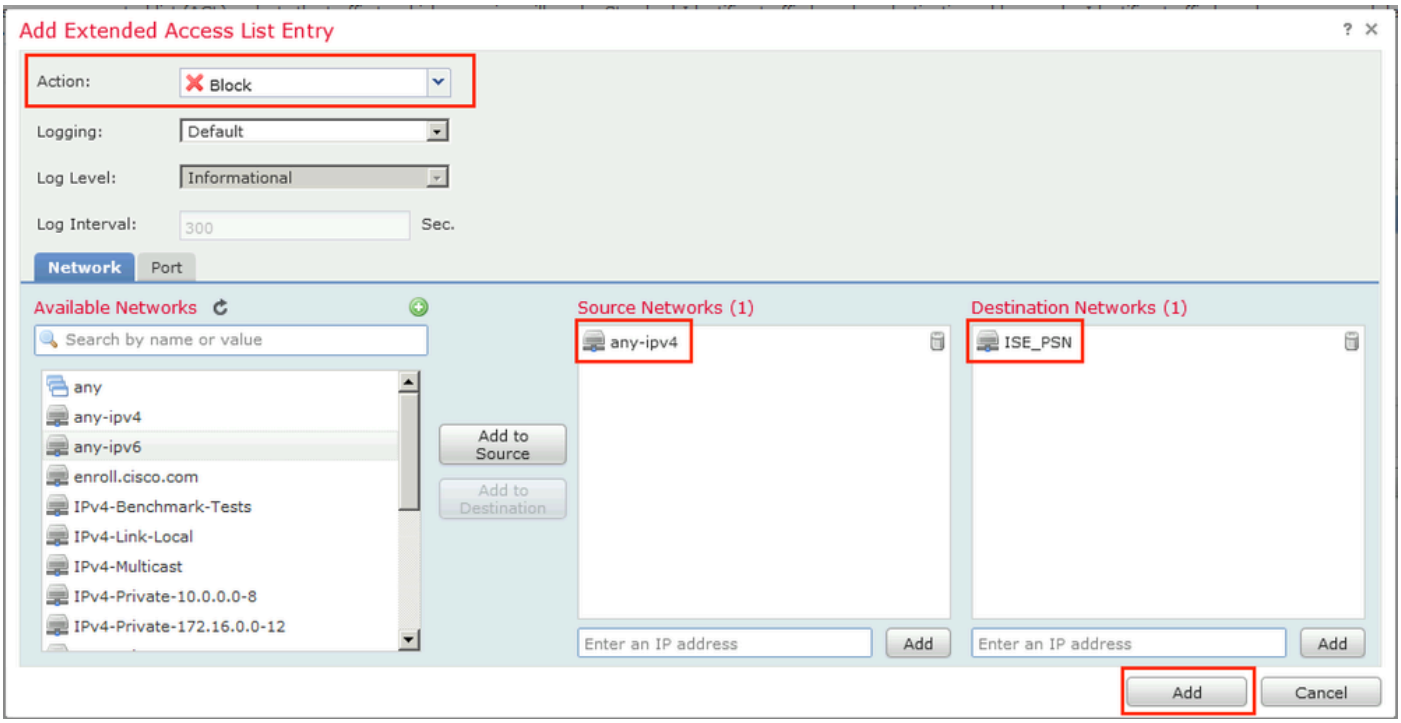
Étape 1 : création d'un groupe d'objets réseau pour ISE et les serveurs de résolution (le cas échéant) Accédez à Objets > Gestion des objets > Réseau.

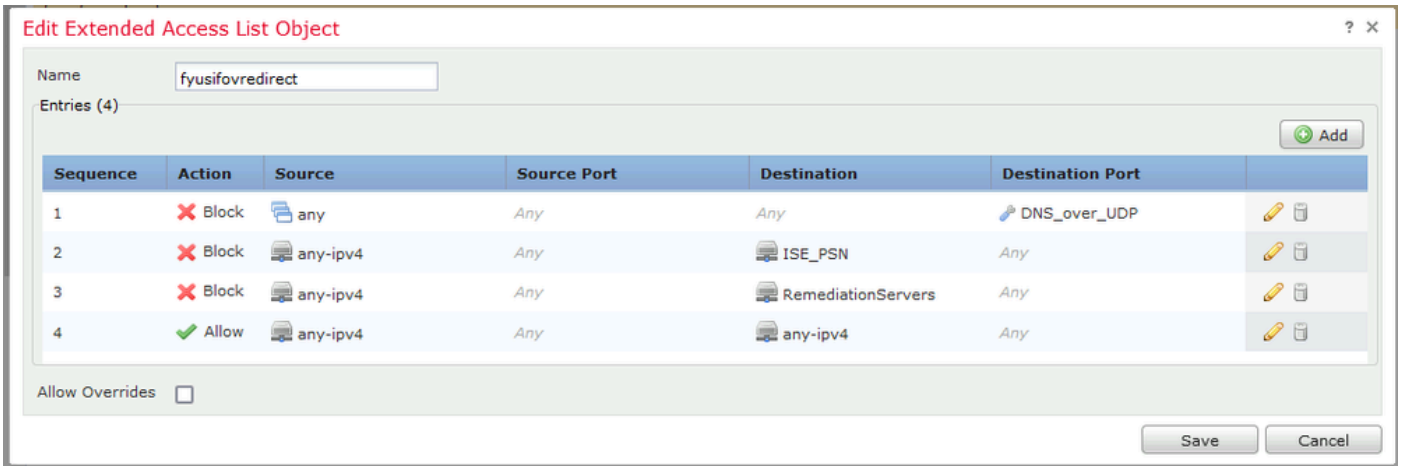


Étape 2 : création d'une liste de contrôle d'accès redirigée Accédez à Objets > Gestion des objets > Liste d'accès > Étendue. Cliquez sur Add Extended Access List et fournissez le nom de Redirect ACL. Ce nom doit être le même que dans le résultat de l'autorisation ISE.

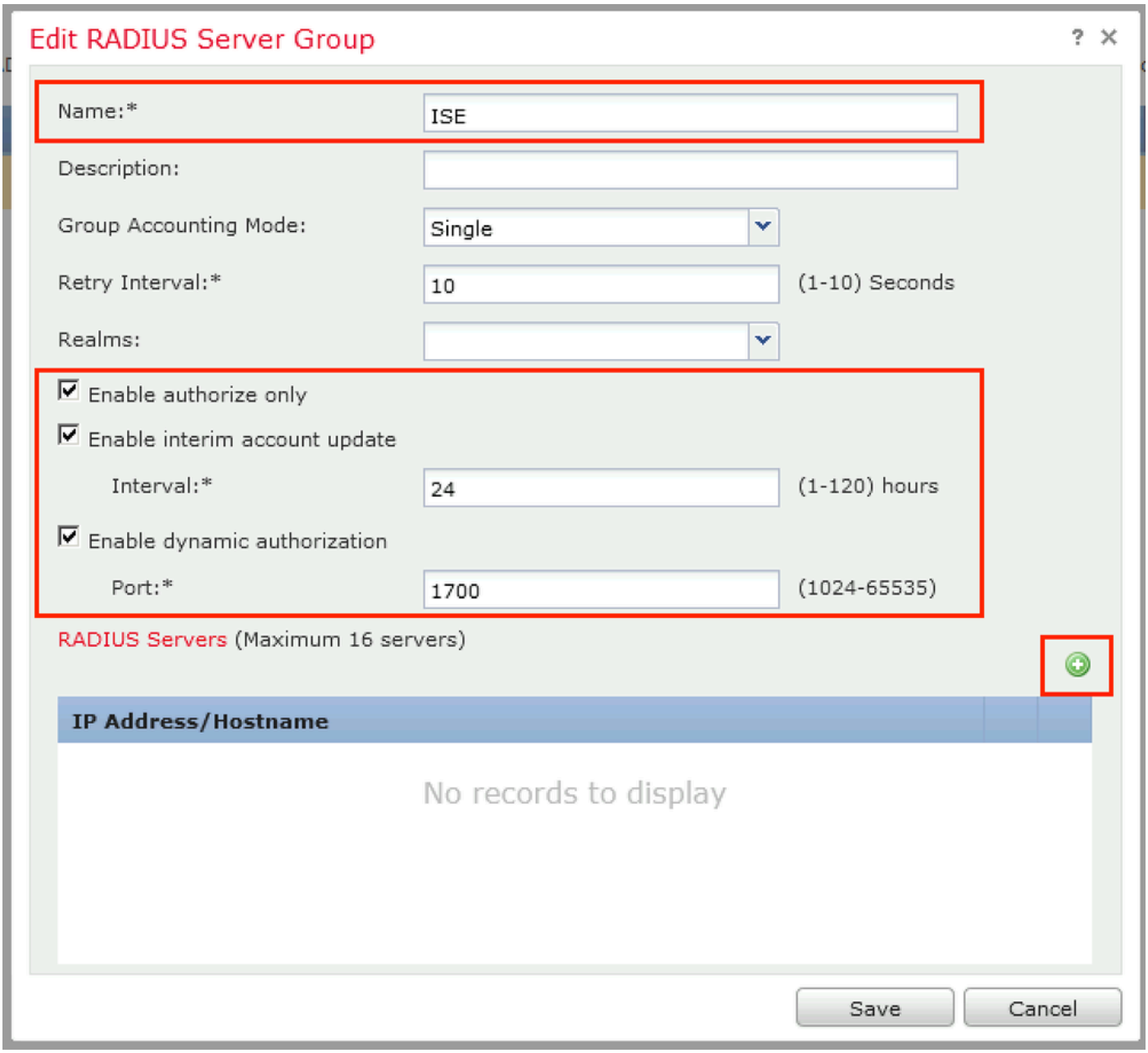


Étape 3 : ajout d'entrées de liste de contrôle d'accès redirigée Cliquez sur le bouton Add. Bloquez le trafic vers DNS, ISE et les serveurs de conversion pour les exclure de la redirection. Autorisez le reste du trafic, ce qui déclenche la redirection (les entrées de la liste de contrôle d'accès peuvent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

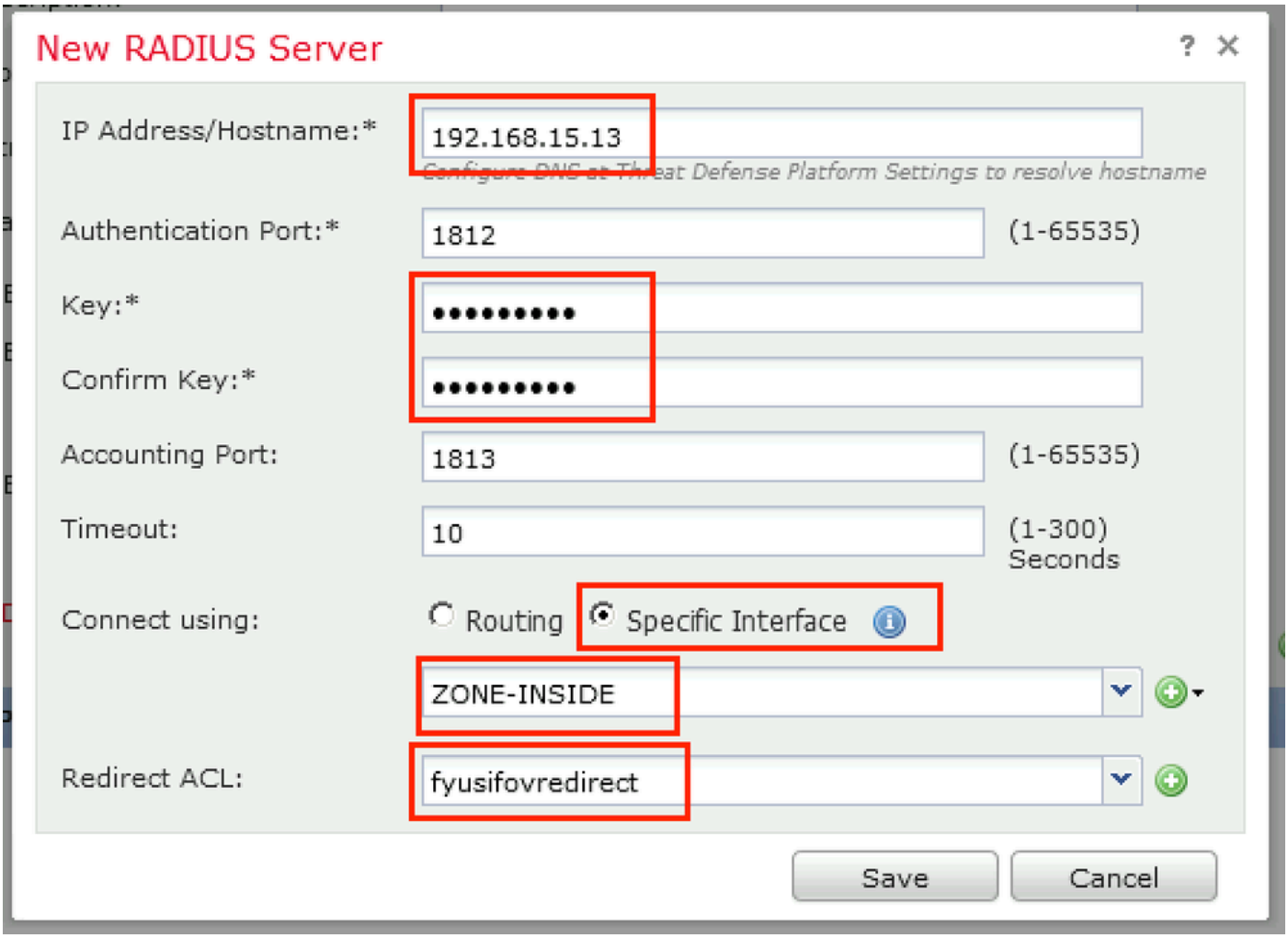




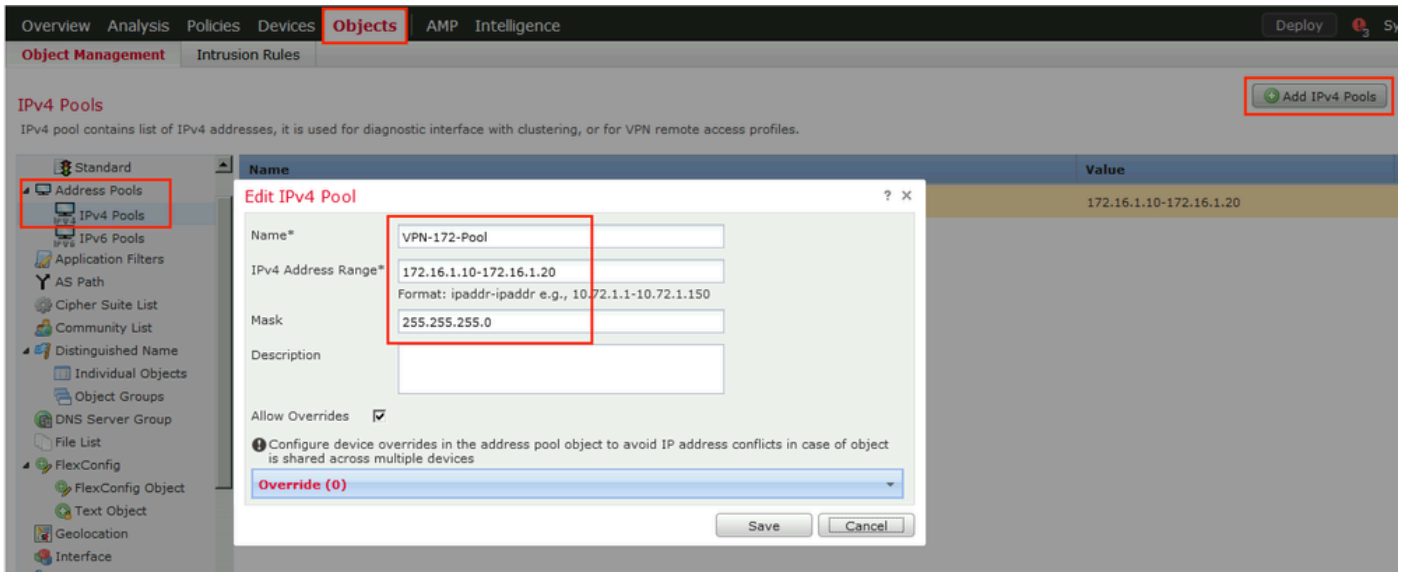
Étape 4 : ajout de noeuds PSN ISE Accédez à Objets > Gestion des objets > Groupe de serveurs RADIUS. Cliquez sur Add RADIUS Server Group, puis fournissez un nom, activez toutes les cases à cocher et cliquez sur l'icône plus.



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.

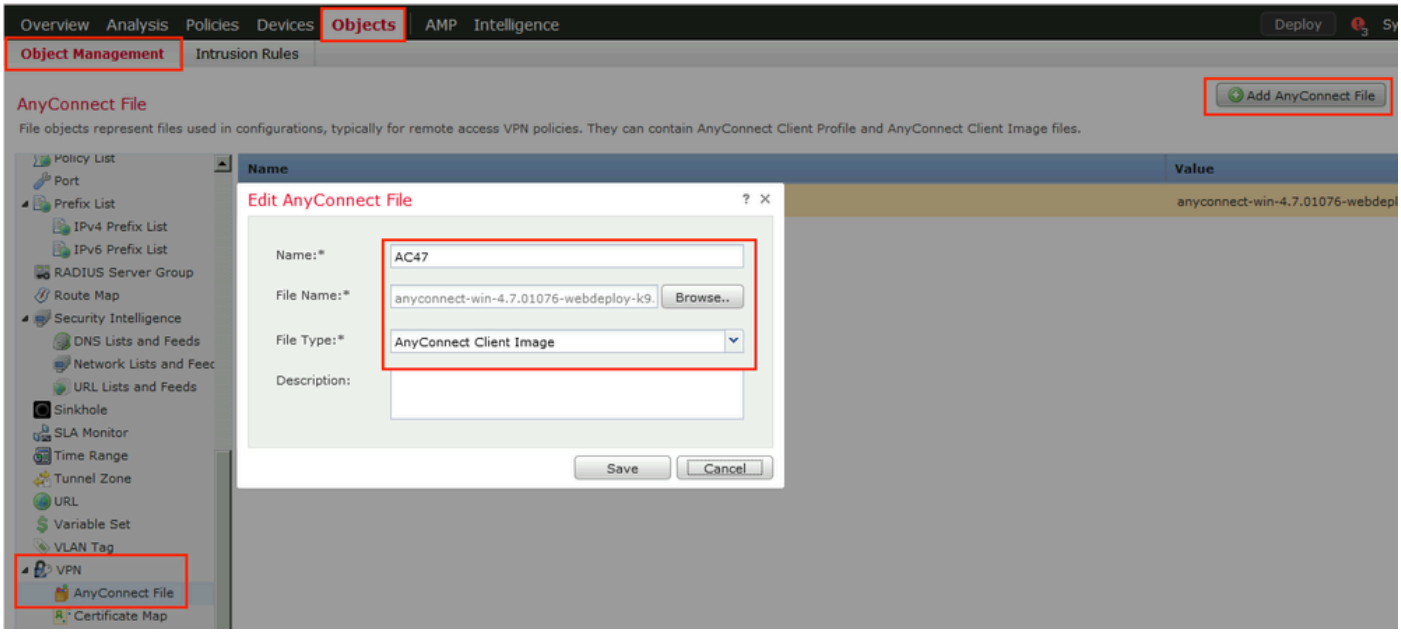


Étape 6 : création d'un pool d'adresses pour les utilisateurs VPN Accédez à Objets > Gestion des objets > Pools d'adresses > Pools IPv4. Cliquez sur Add IPv4 Pools et renseignez les détails.

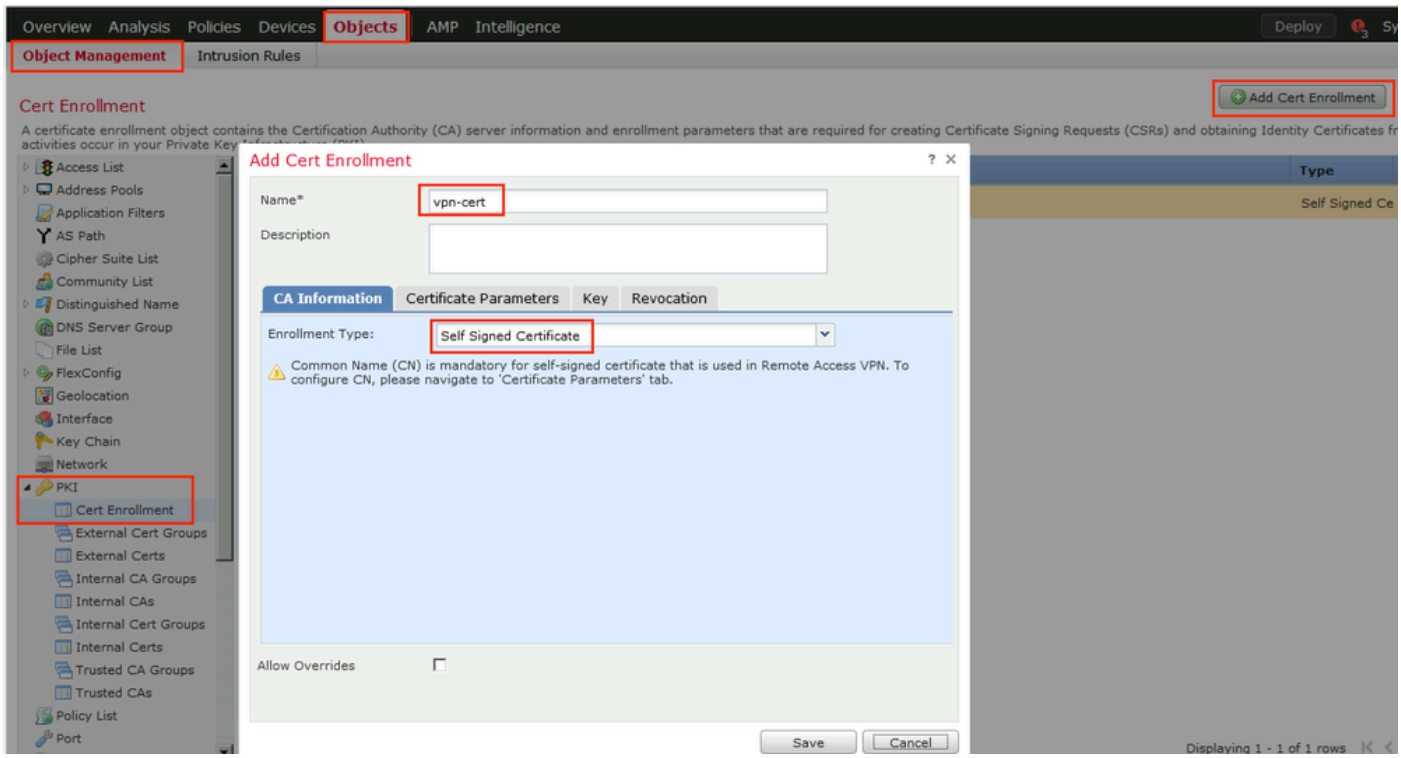


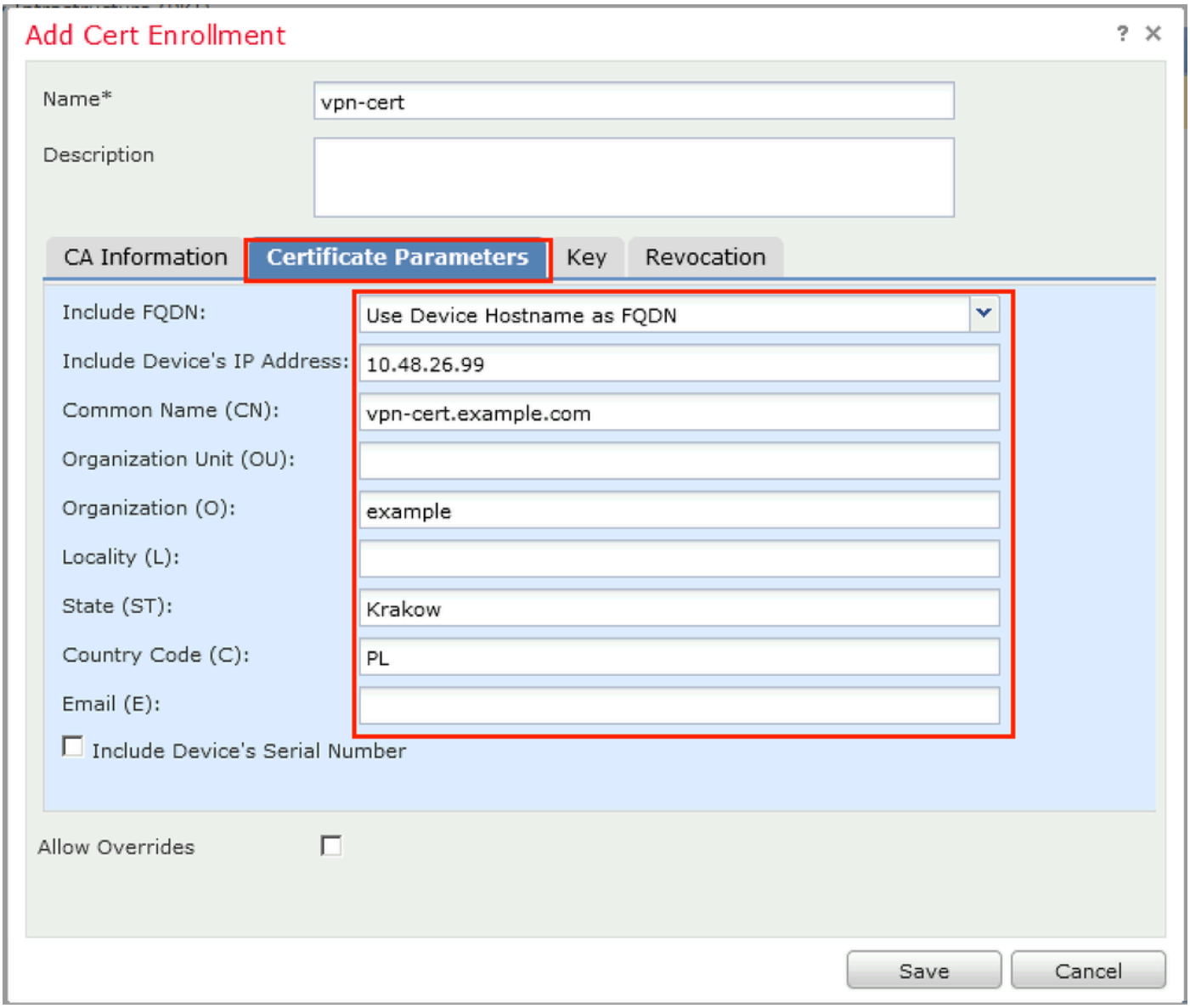
Étape 7 : création du package AnyConnect Accédez à Objets > Gestion des objets > VPN > Fichier AnyConnect. Cliquez sur Add AnyConnect File, fournissez le nom du package, téléchargez

le package à partir de Cisco Software Download et sélectionnez Anyconnect Client Image File Type.

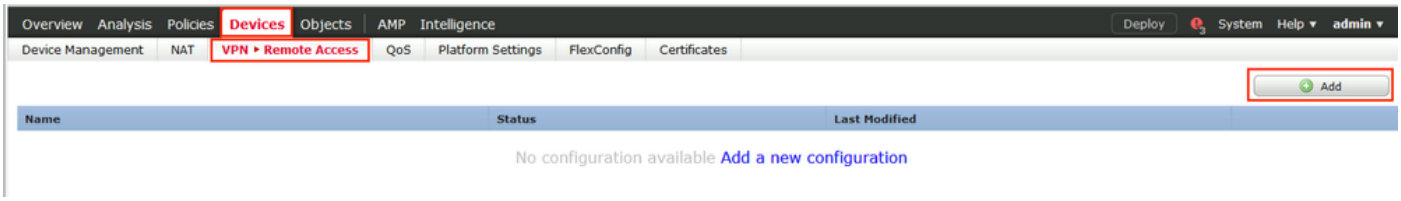


Étape 8. Accédez à Objets de certificat > Gestion des objets > PKI > Inscription de certificat. Cliquez sur Add Cert Enrollment, fournissez un nom, choisissez Self Signed Certificate in Enrollment Type. Cliquez sur l'onglet Certificate Parameters et indiquez CN.

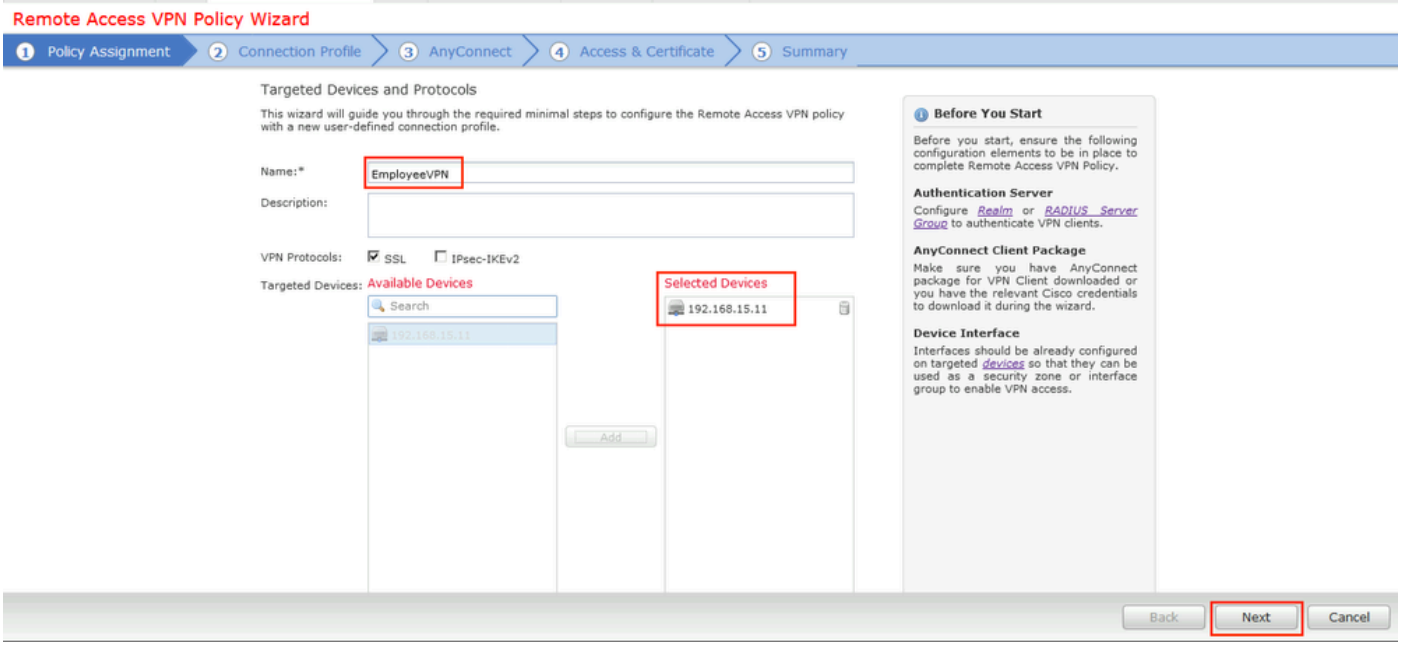




Étape 9. Lancez l'assistant VPN d'accès à distance. Accédez à Devices > VPN > Remote Access et cliquez sur Add.

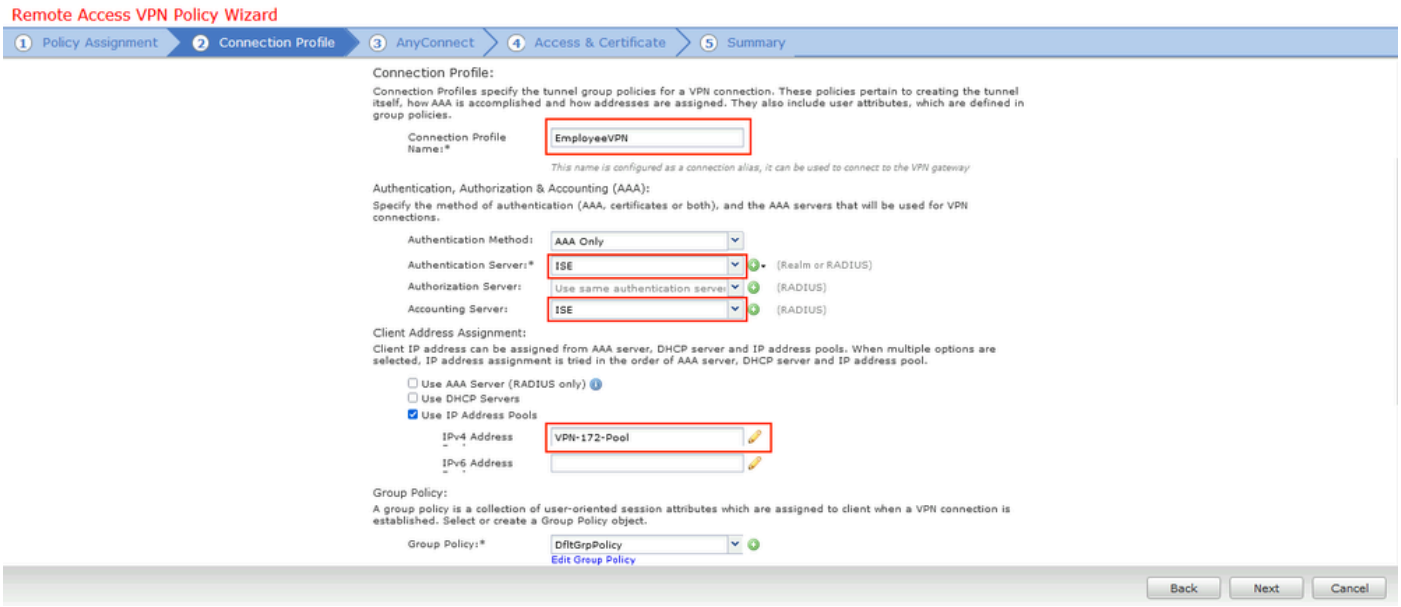


Étape 10. Fournissez le nom, cochez SSL comme protocole VPN, choisissez FTD qui est utilisé comme concentrateur VPN et cliquez sur Next.

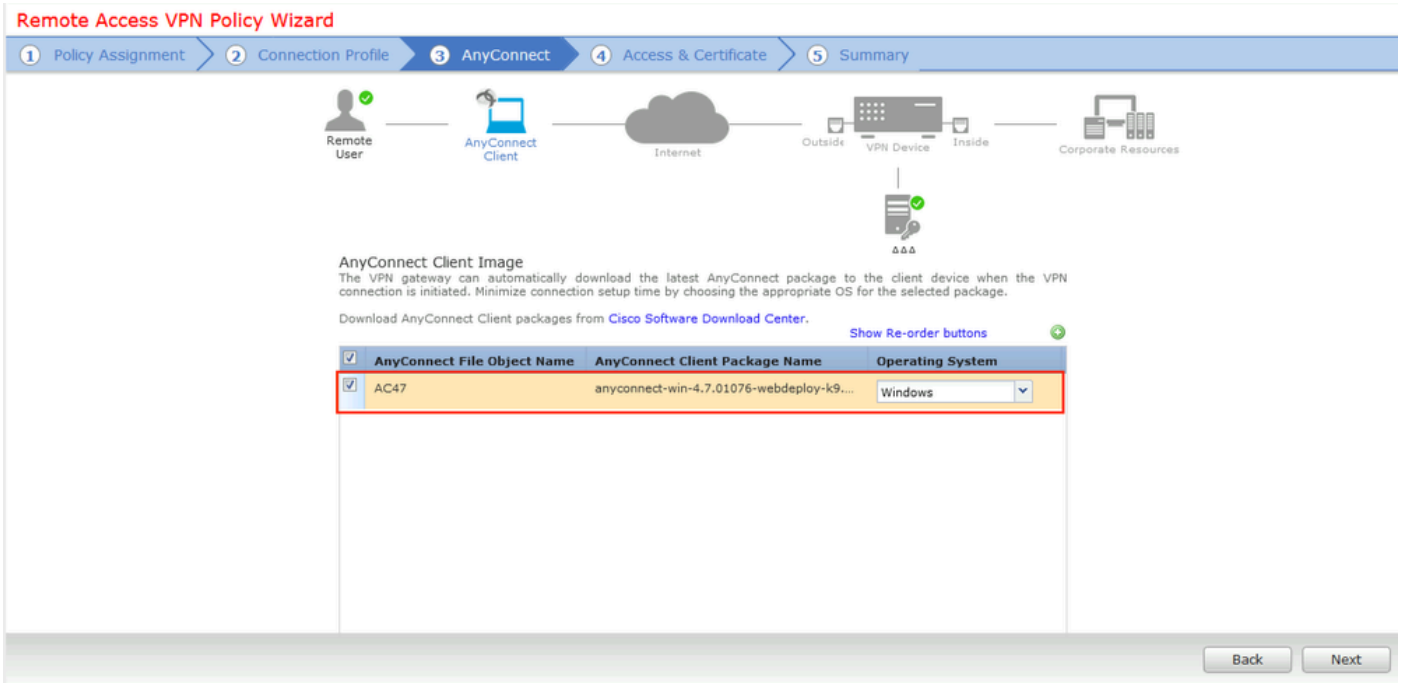


Étape 11. Fournissez le nom du profil de connexion, sélectionnez Serveurs d'authentification/de comptabilité, sélectionnez le pool d'adresses qui a été configuré précédemment et cliquez sur Suivant.

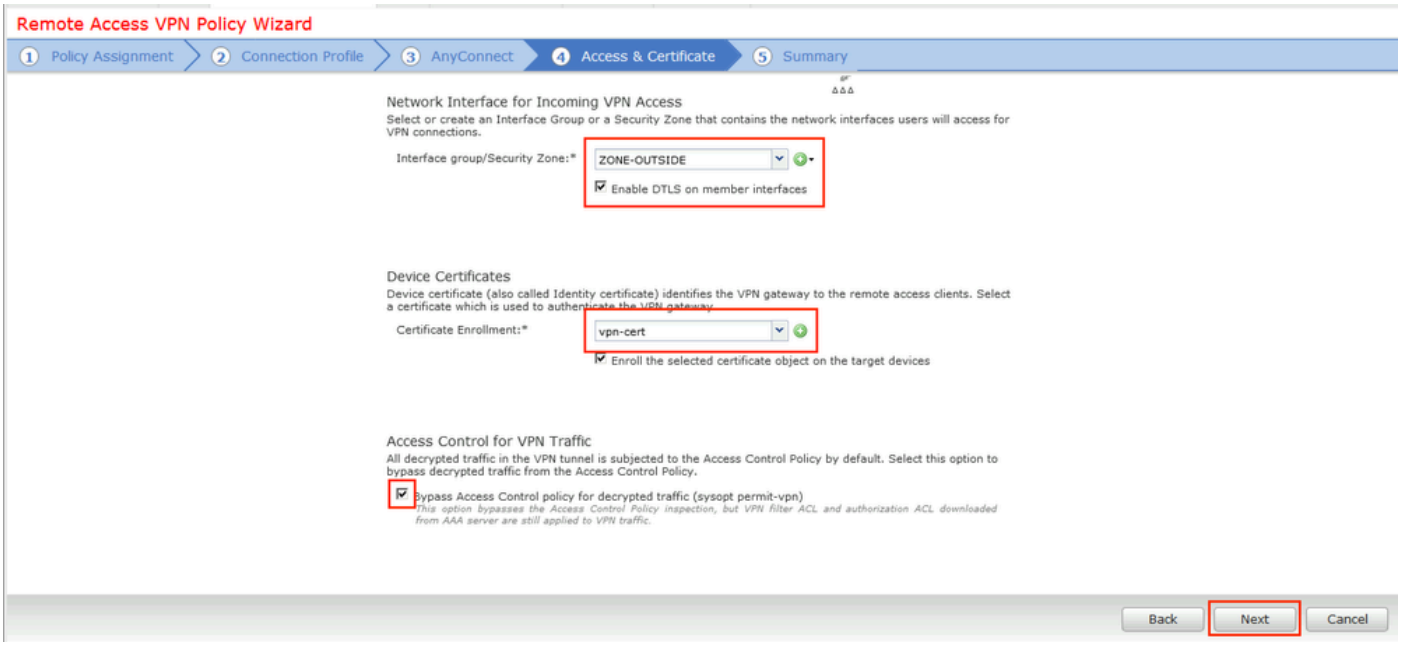
Remarque : Ne sélectionnez pas le serveur d'autorisation. Il déclenche deux demandes d'accès pour un seul utilisateur (une fois avec le mot de passe utilisateur et la deuxième fois avec le mot de passe cisco).



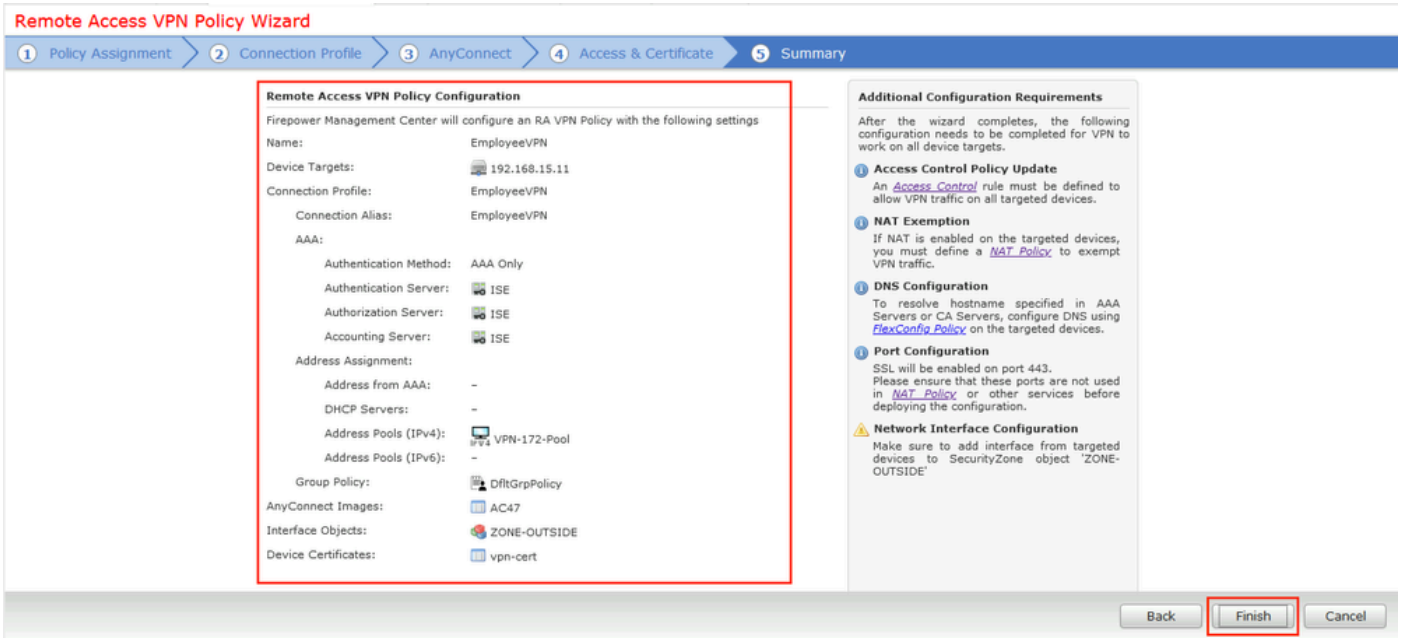
Étape 12. Sélectionnez le package AnyConnect qui a été configuré précédemment et cliquez sur Next.



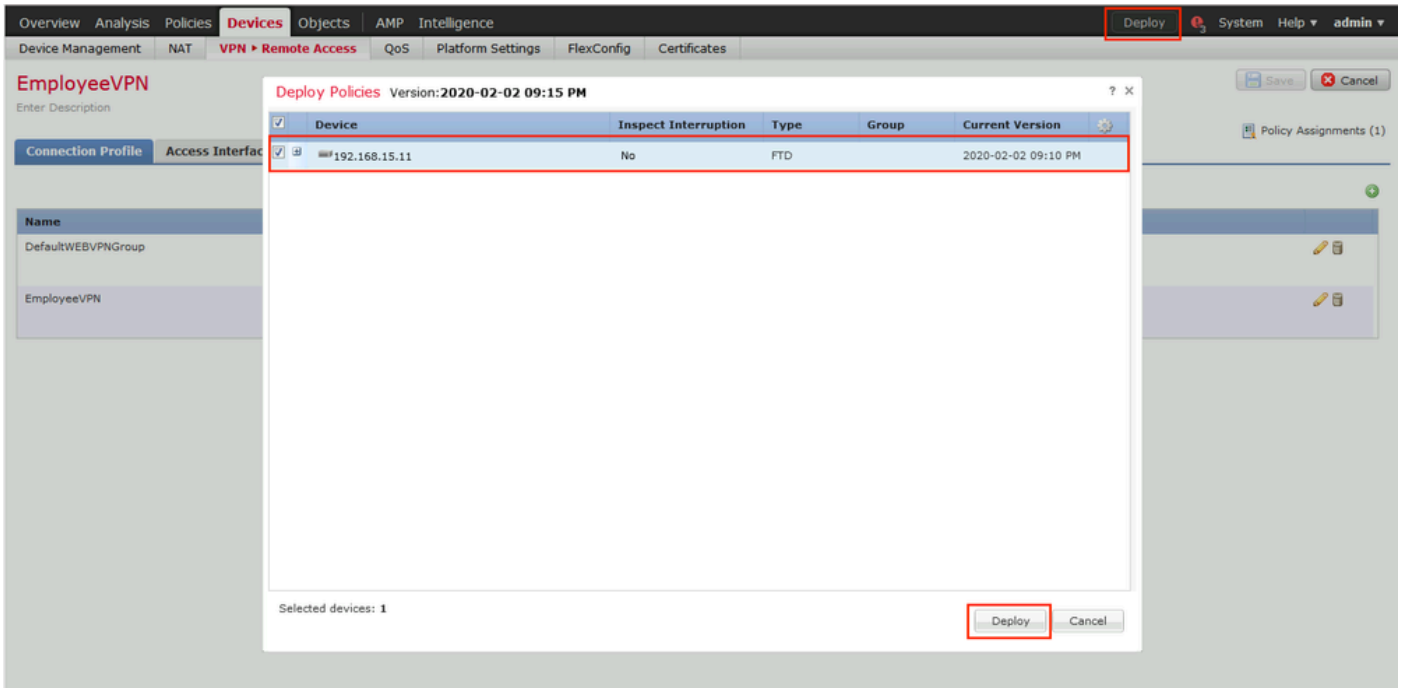
Étape 13. Sélectionnez l'interface à partir de laquelle le trafic VPN est attendu, sélectionnez Certificate Enrollment qui a été configuré précédemment et cliquez sur Next.



Étape 14. Vérifiez la page de résumé et cliquez sur Finish.

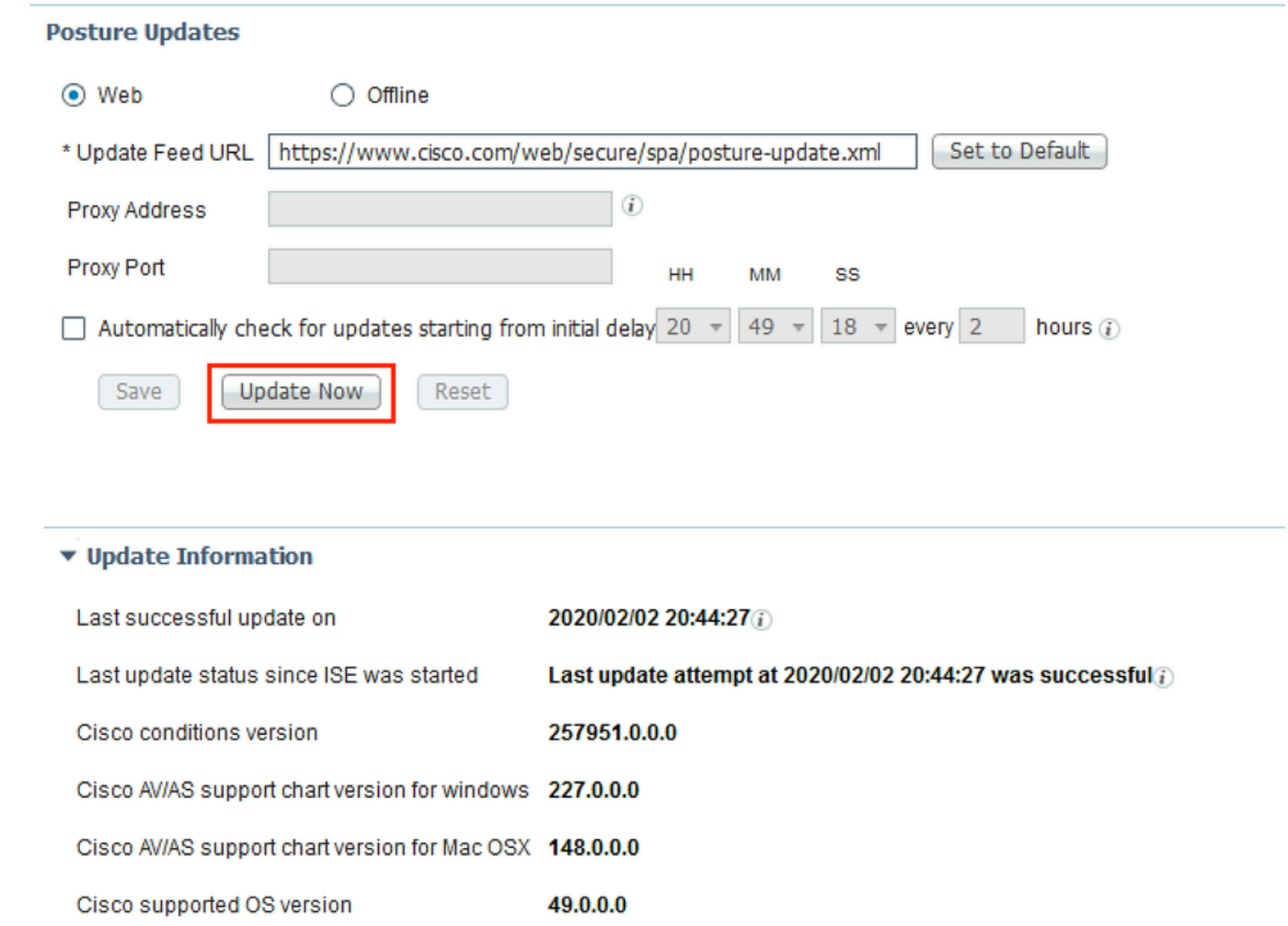


Étape 15. Déployez la configuration sur FTD. Cliquez sur Deploy et sélectionnez FTD qui est utilisé comme concentrateur VPN.

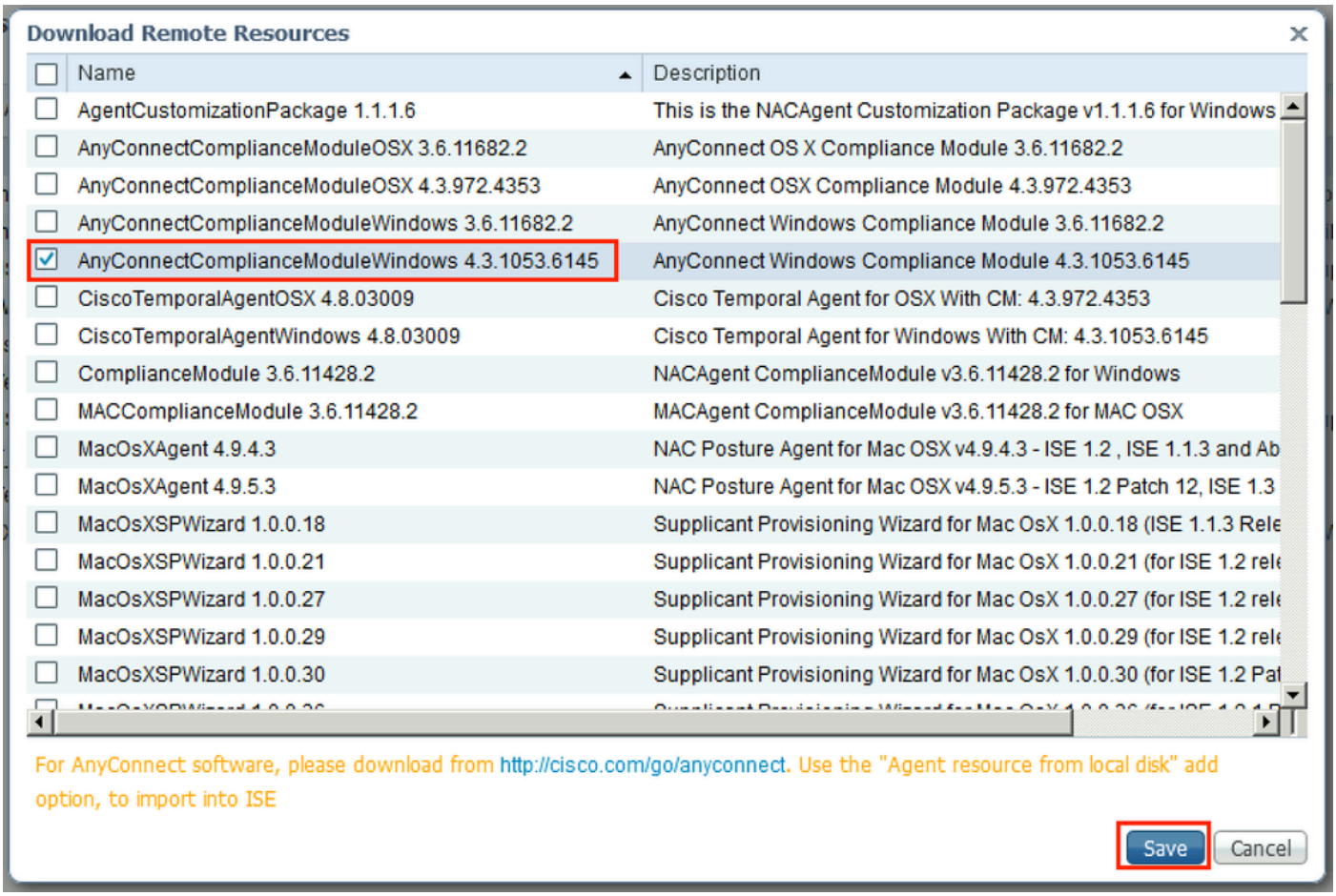


ISE

Étape 1 : exécution des mises à jour de posture Accédez à Administration > System > Settings > Posture > Updates.

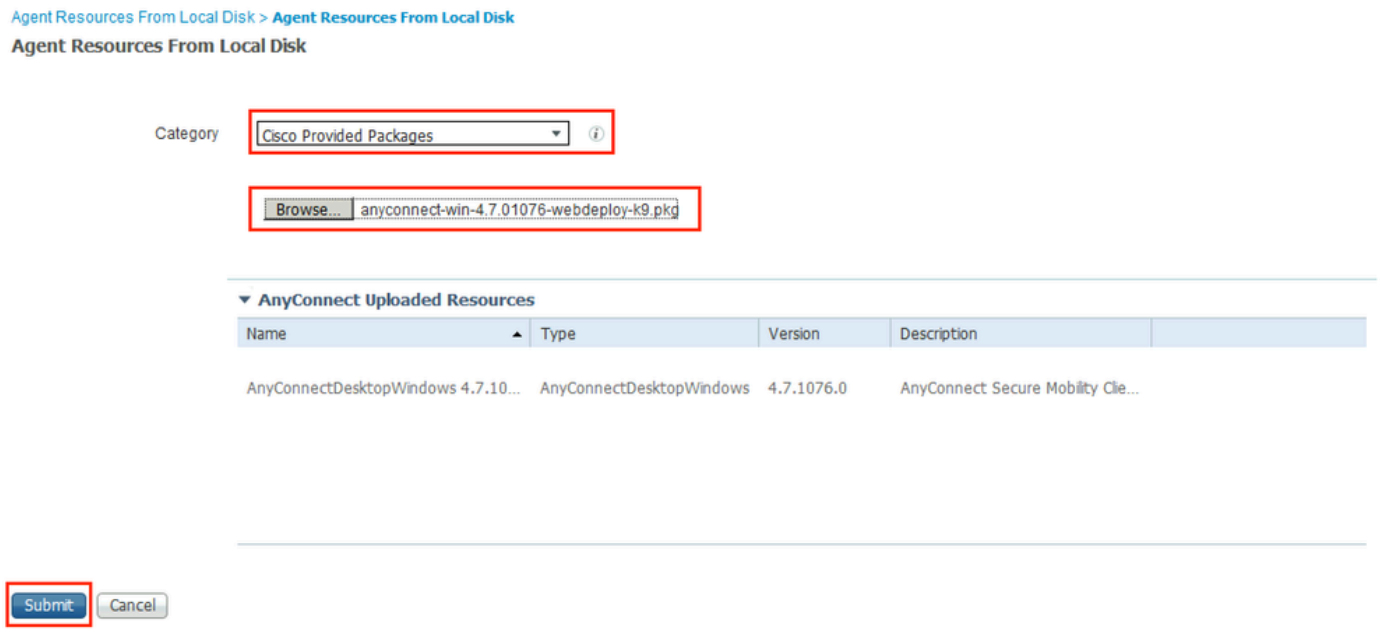


Étape 2 : chargement du module de conformité Accédez à Policy > Policy Elements > Results > Client Provisioning > Resources. Cliquez sur Add et sélectionnez Agent resources from Cisco site



Étape 3. Téléchargez AnyConnect à partir de Cisco Software Download, puis téléchargez-le vers ISE. Accédez à Policy > Policy Elements > Results > Client Provisioning > Resources.

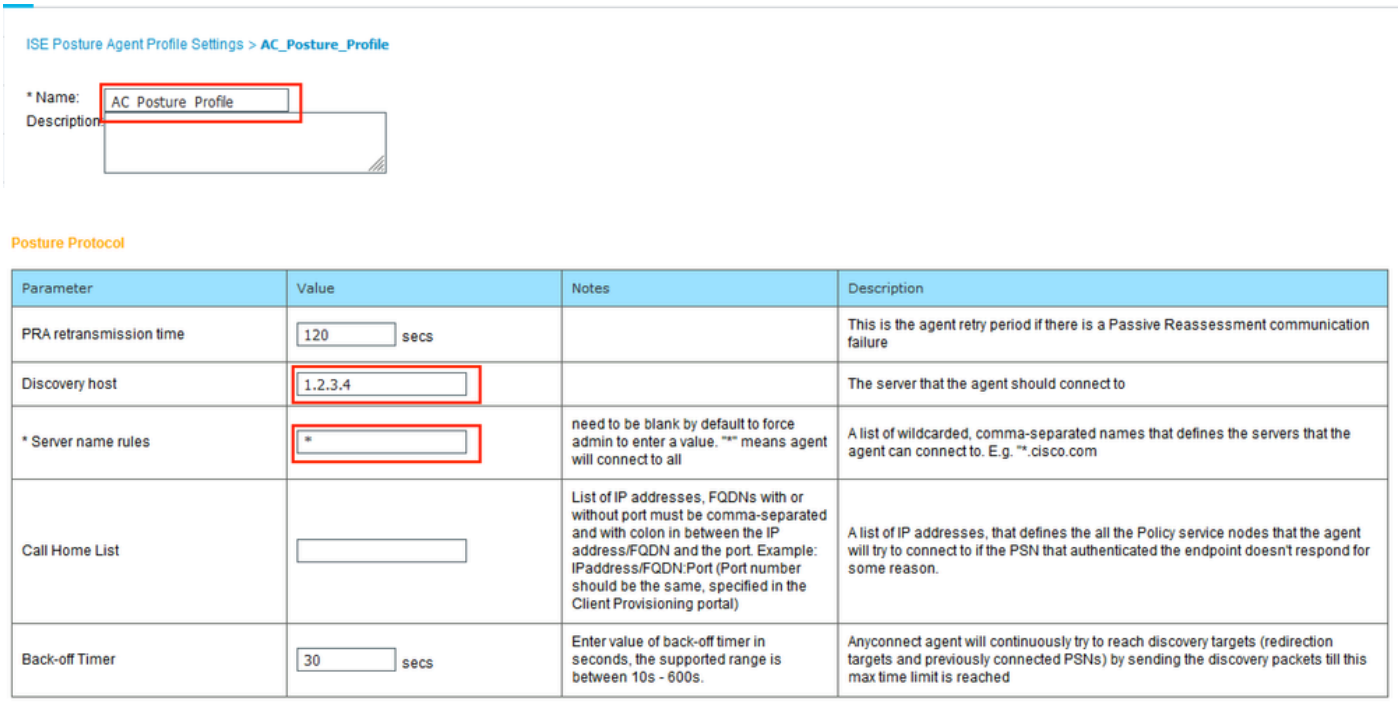
Cliquez sur Add et sélectionnez Agent Resources From Local Disk. Choisissez Cisco Provided Packages sous Category, sélectionnez le package AnyConnect à partir du disque local et cliquez sur Submit.



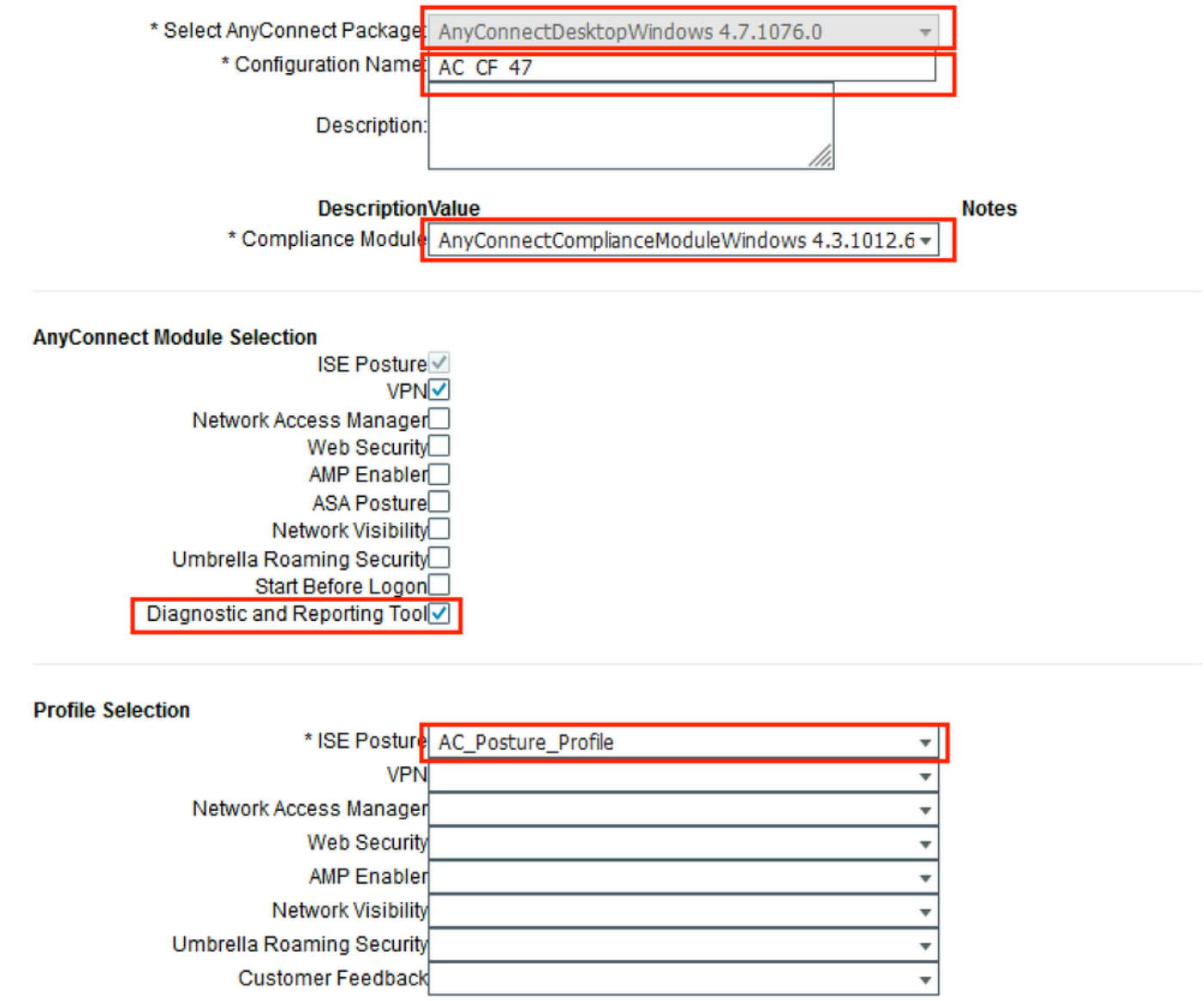
Étape 4 : création du profil de position AnyConnect Accédez à Policy > Policy Elements > Results > Client Provisioning > Resources.

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

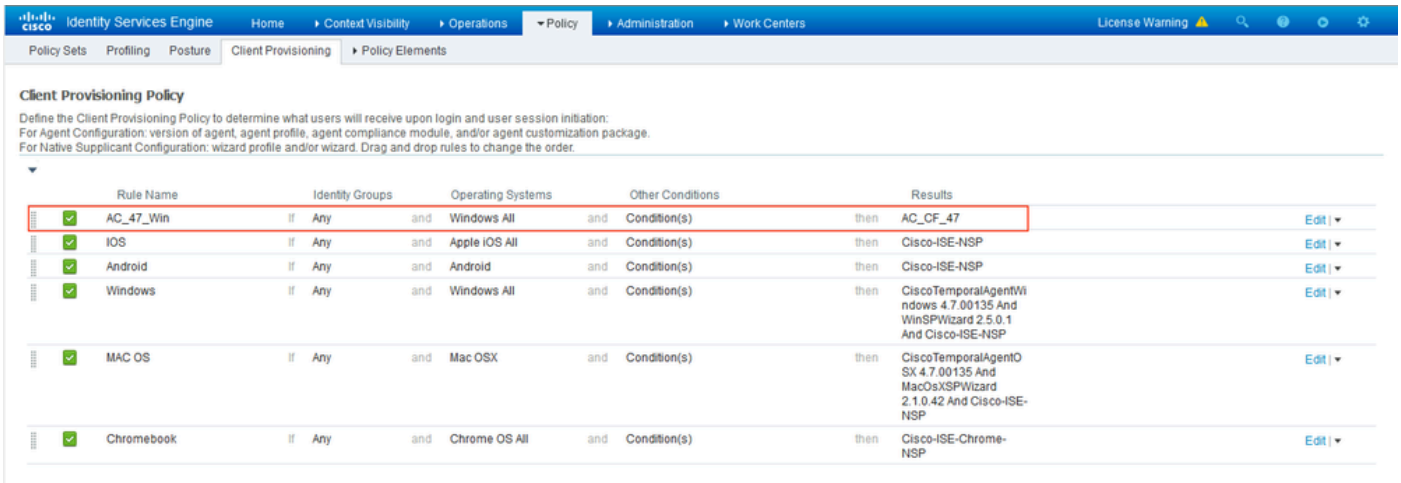
Sous *Server name rules, placez * et placez toute adresse IP factice sous Discovery host.



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.

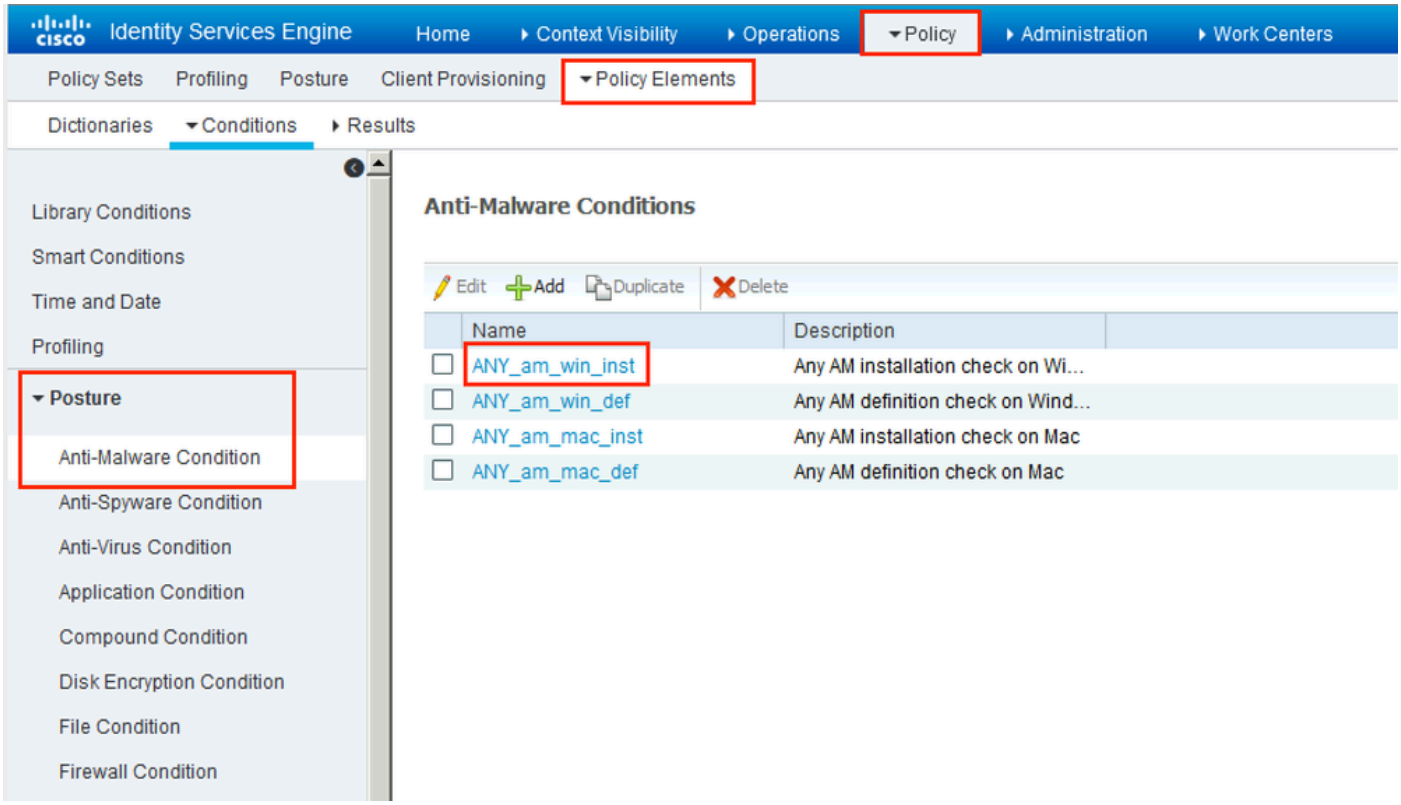


Étape 6. Accédez à Policy > Client Provisioning et créez Client Provisioning Policy. Cliquez sur Edit, puis sélectionnez Insert Rule Above, fournissez un nom, sélectionnez OS et choisissez AnyConnect Configuration qui a été créé à l'étape précédente.



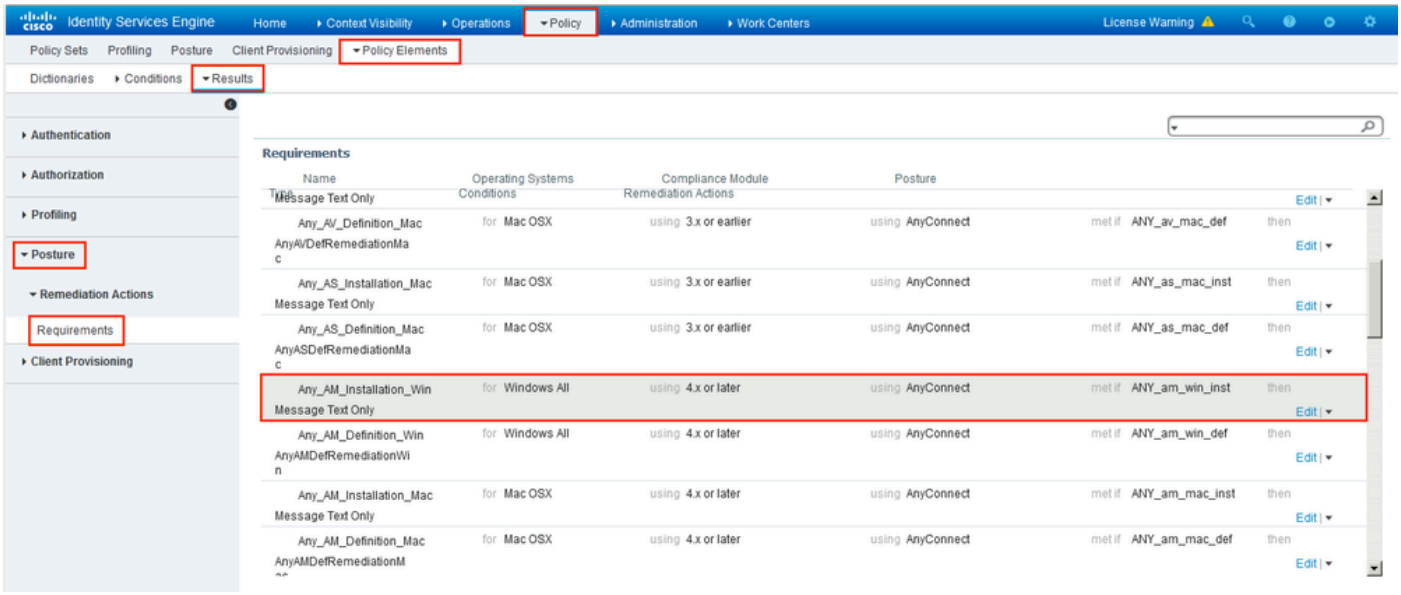
Étape 7. Créez une condition de position sous Stratégie > Éléments de stratégie > Conditions > Position > Condition anti-programme malveillant. Dans cet exemple, "ANY_am_win_inst" prédéfini est utilisé.

.

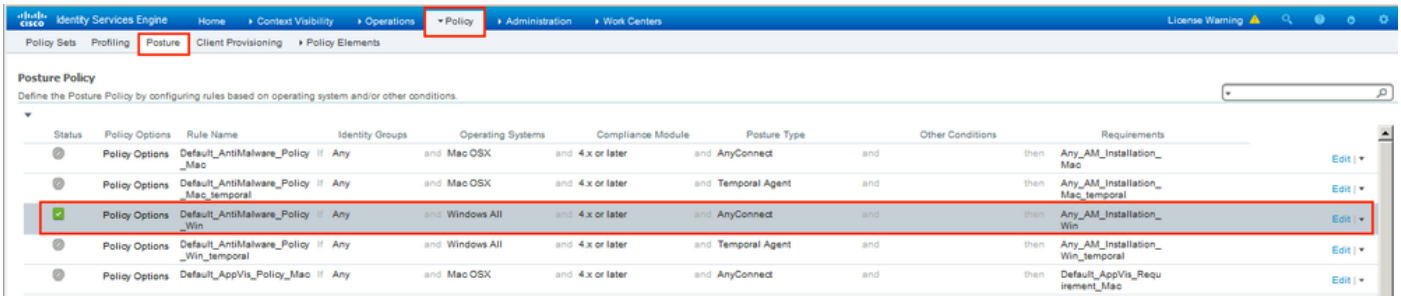


Étape 8. Accédez à Politique > Éléments de politique > Résultats > Posture > Actions correctives et créez la correction de posture. Dans cet exemple, il est ignoré. L'action corrective peut être un message texte.

Étape 9. Accédez à Règle > Eléments de règle > Résultats > Posture > Exigences et créez des exigences de posture. Condition prédéfinie : Any_AM_Installation_Win est utilisé.



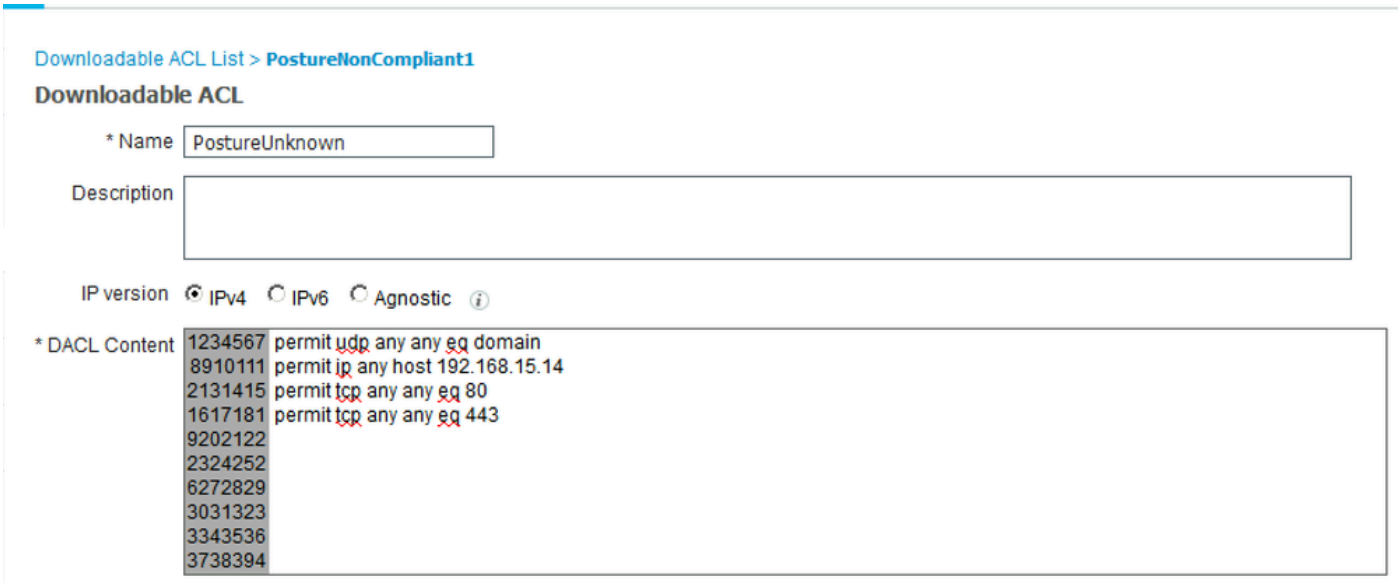
Étape 10. Créez des stratégies de posture sous Stratégies > Posture. La stratégie de posture par défaut de tout contrôle anti-programme malveillant pour le système d'exploitation Windows est utilisée.

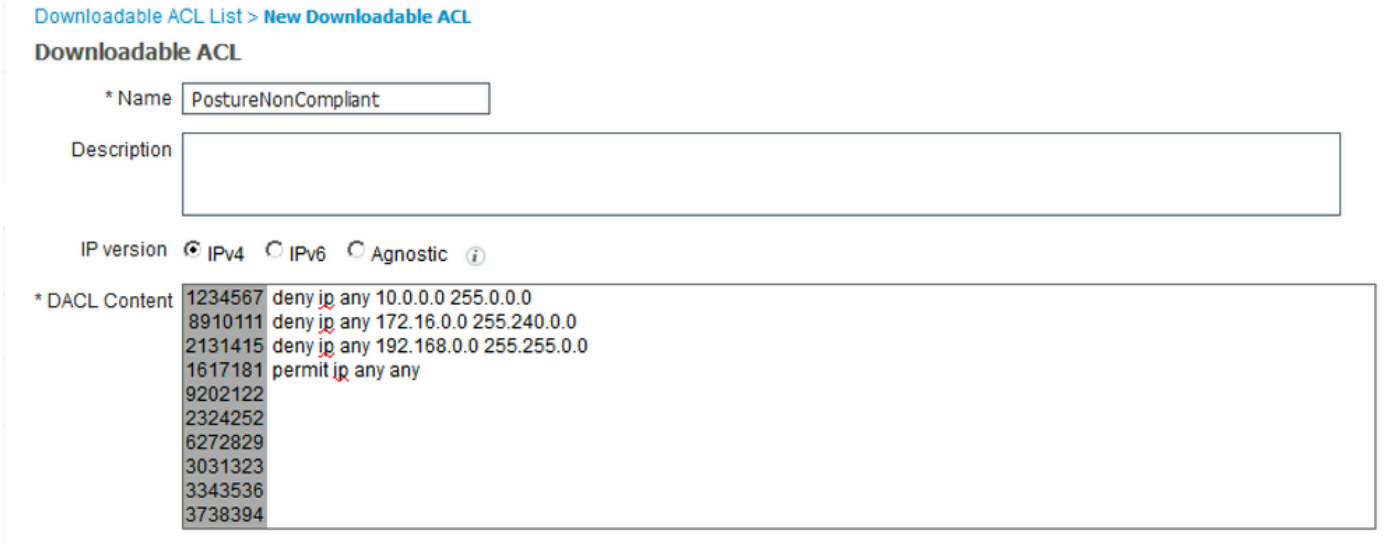


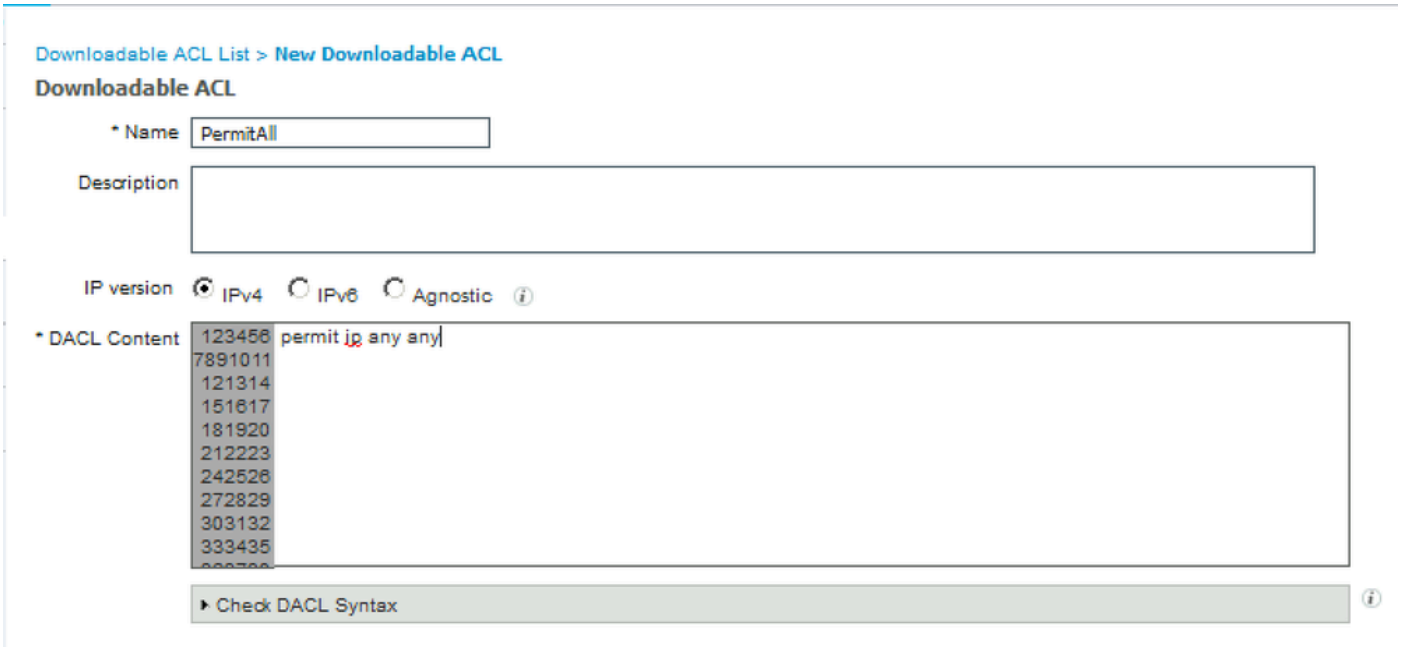
Étape 11. Accédez à Policy > Policy Elements > Results > Authorization > Downlodable ACLS et créez des DACL pour différents états de position.

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.
- Permit All DACL : autorise tout le trafic pour l'état de conformité à la position.

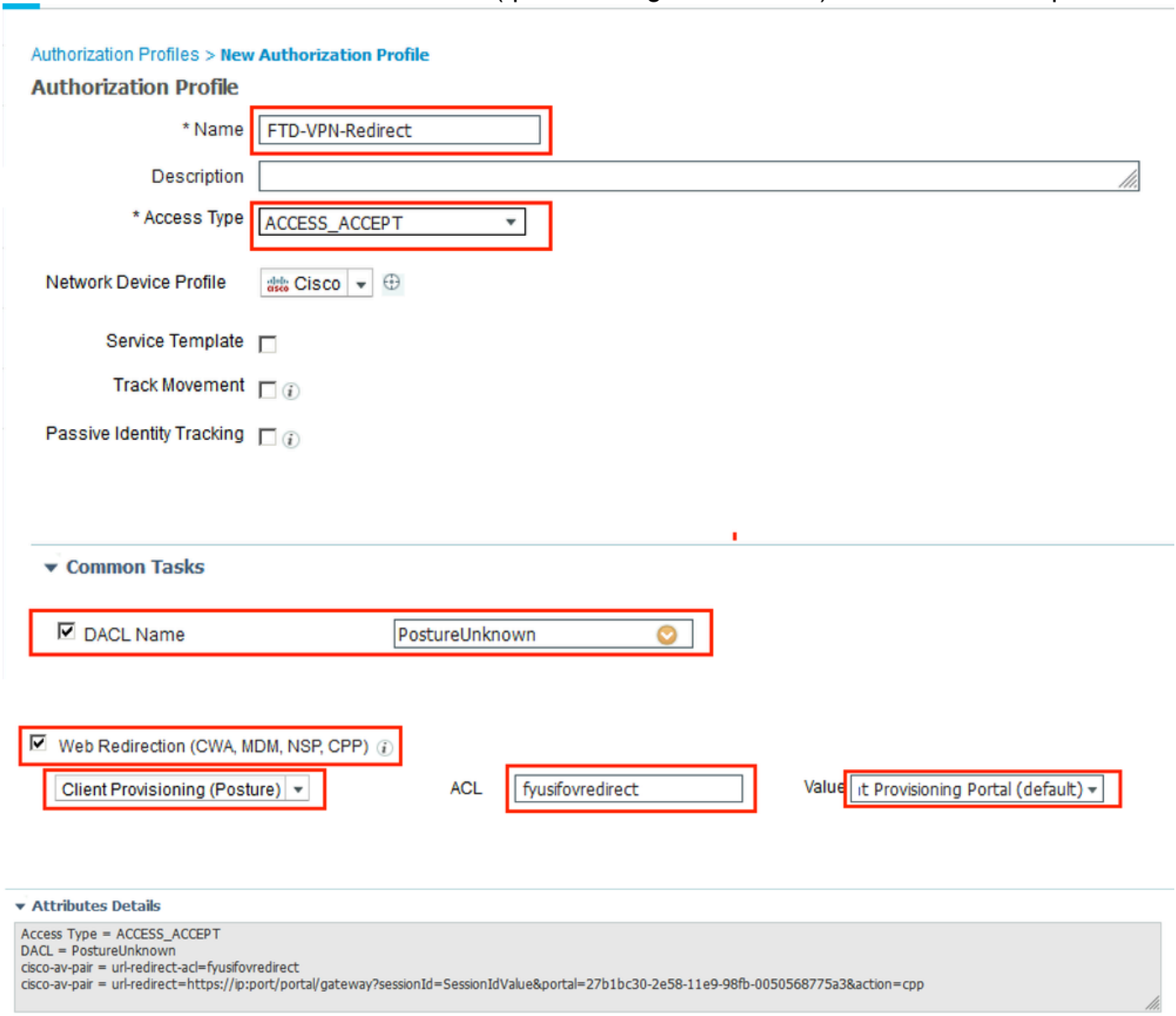




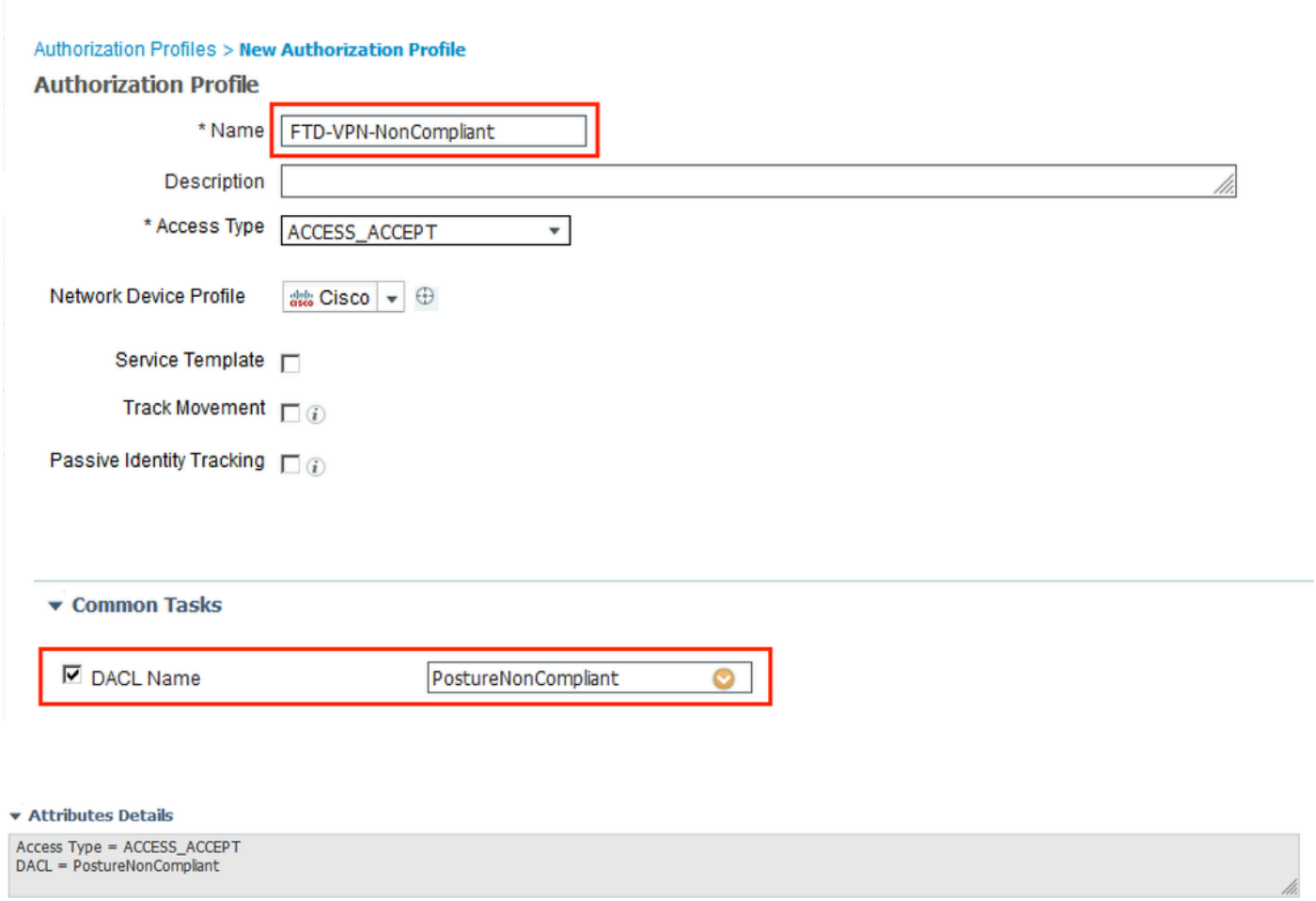


Étape 12. Créez trois profils d’autorisation pour les statuts Posture Unknown, Posture

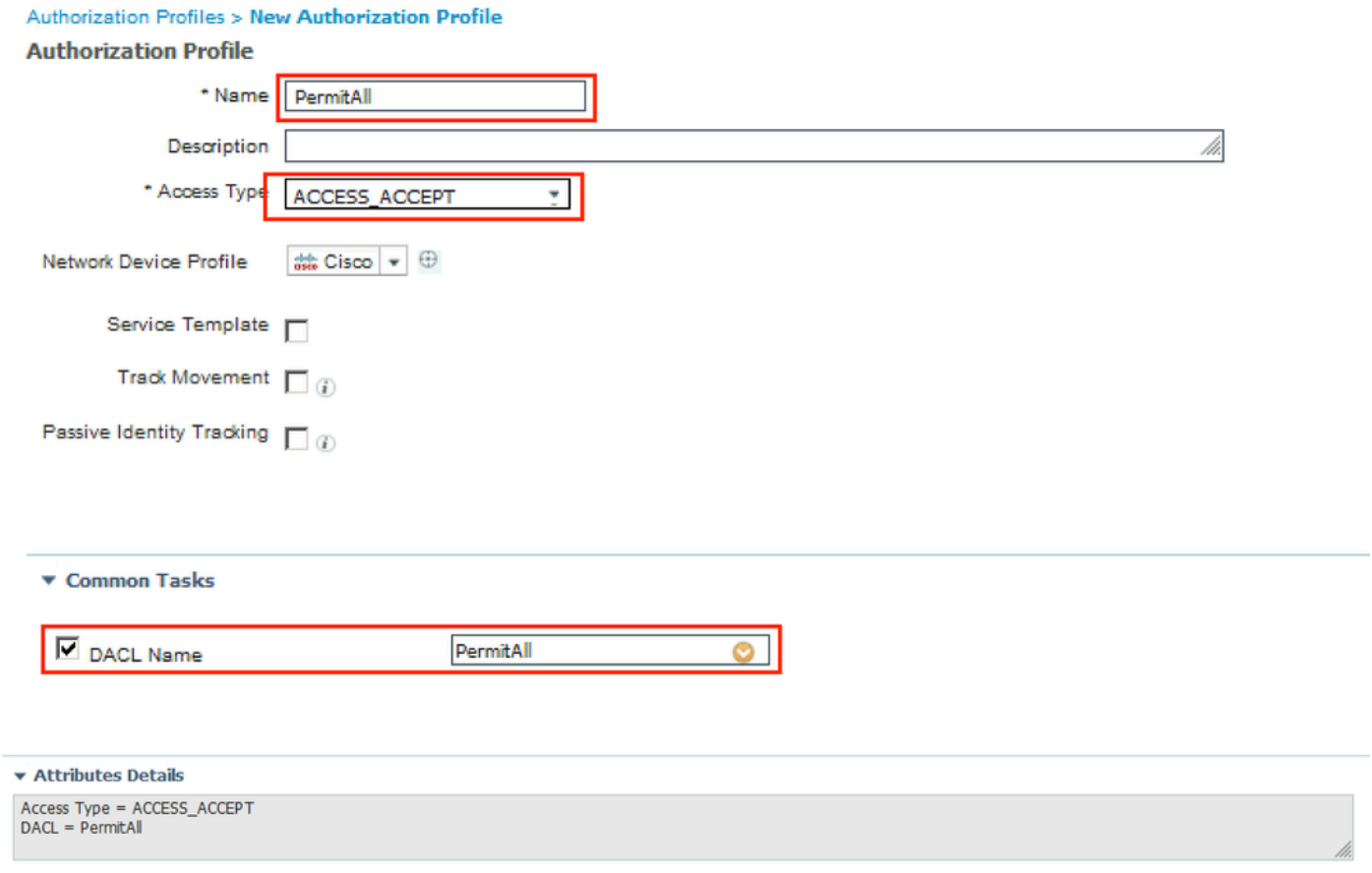
NonCompliant et Posture Compliant. Pour ce faire, accédez à Policy > Policy Elements > Results > Authorization > Authorization Profiles. Dans le profil Posture Unknown, sélectionnez Posture Unknown DACL, cochez Web Redirection, sélectionnez Client Provisioning, fournissez le nom de la liste de contrôle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



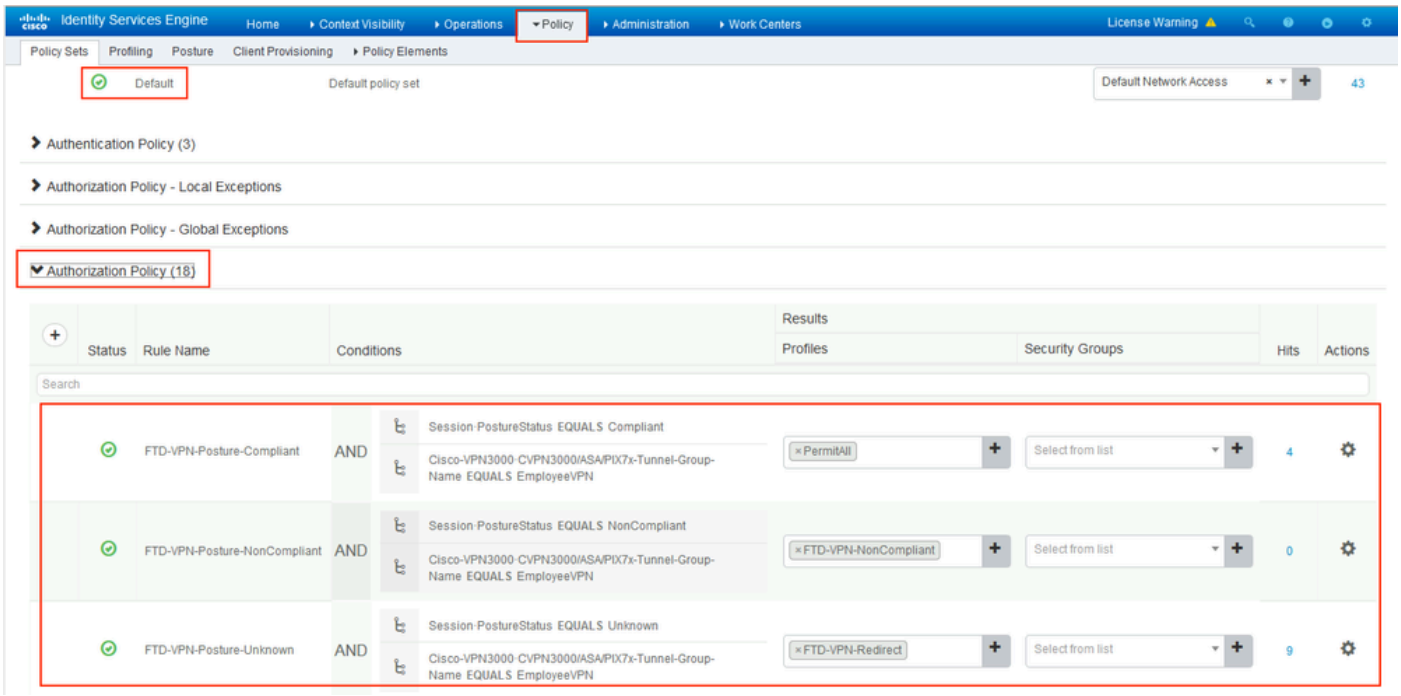
Dans le profil Posture NonCompliant, sélectionnez DACL afin de limiter l'accès au réseau.



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



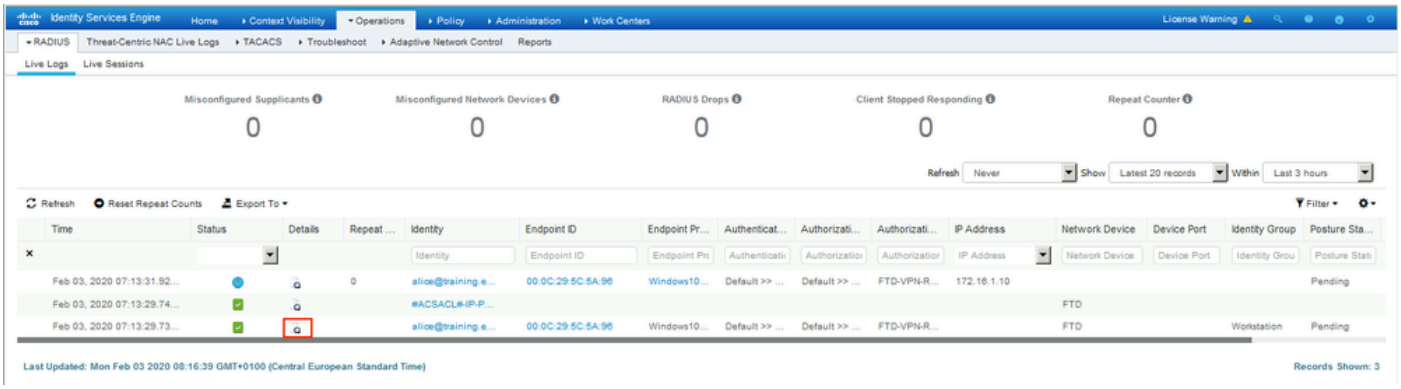
Étape 13. Créez des stratégies d'autorisation sous Stratégie > Jeux de stratégies > Par défaut > Stratégie d'autorisation. En tant que condition Posture Status et VNP TunnelGroup Name est utilisé.



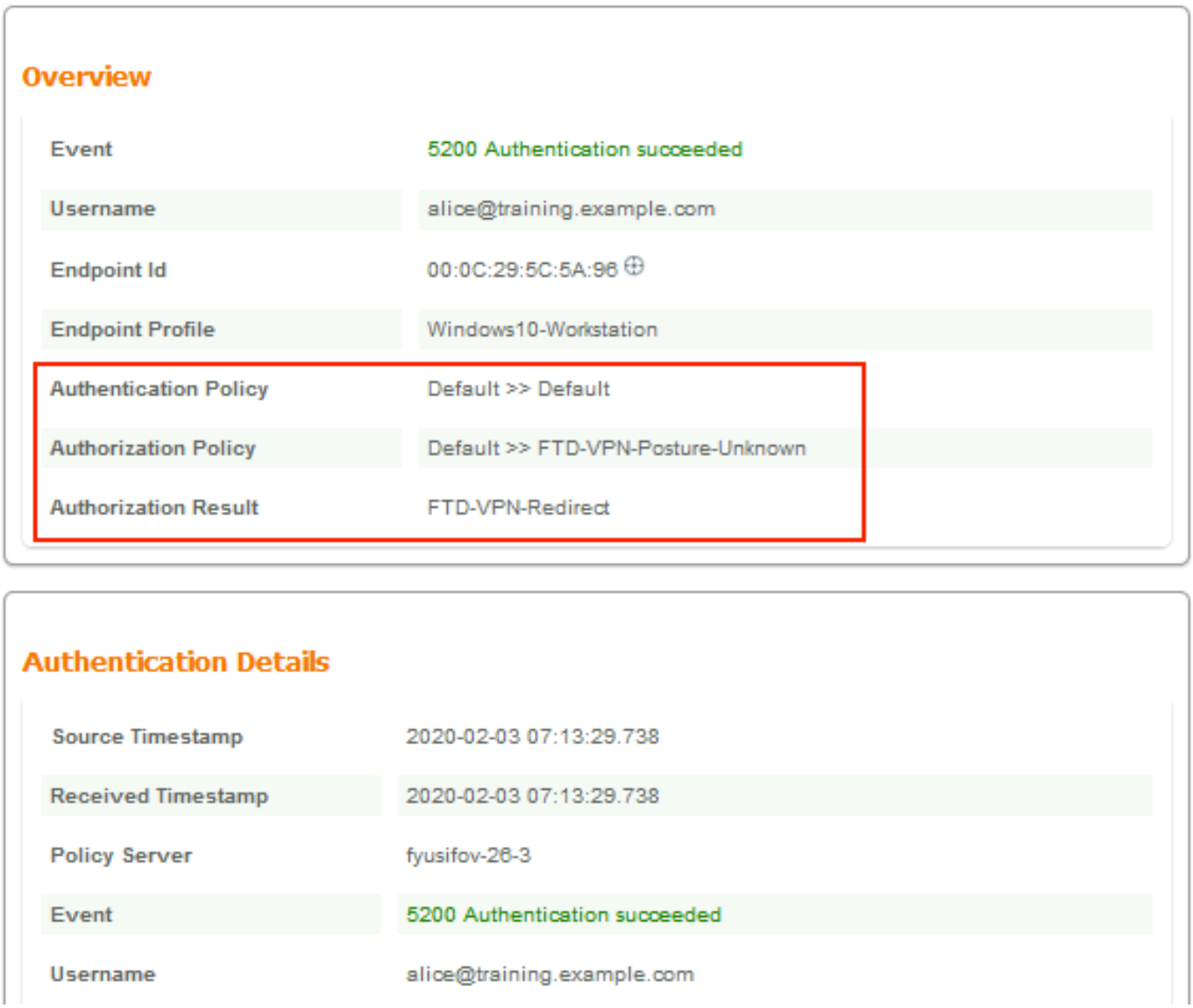
Vérifier

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.



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



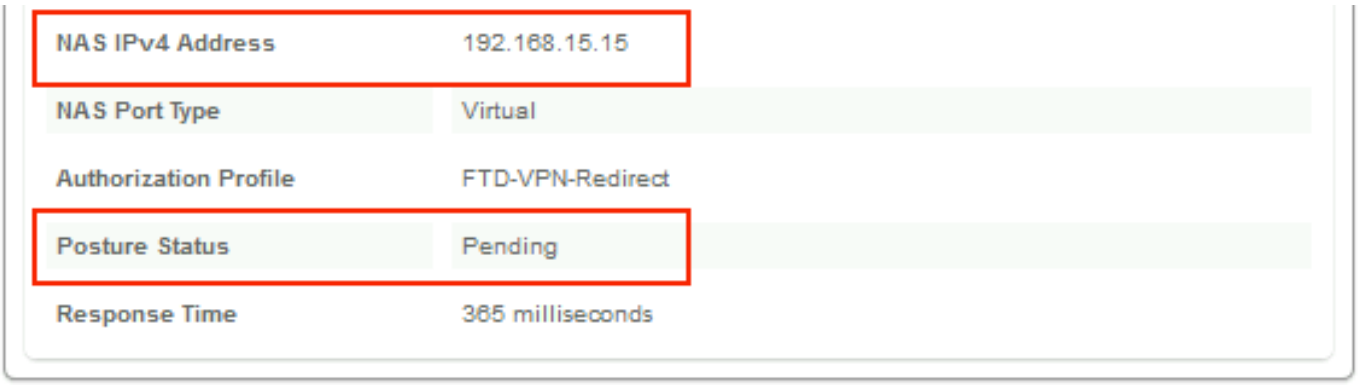
Overview

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	fyusifov-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.



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

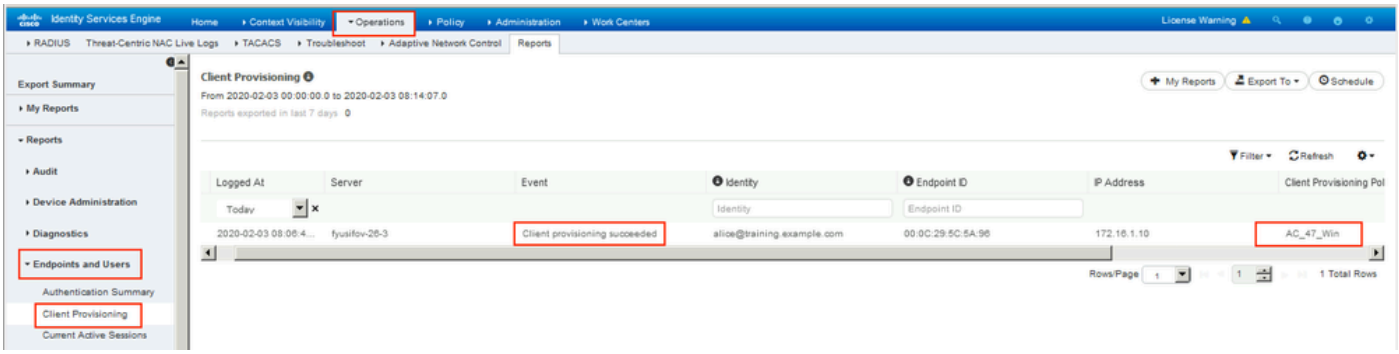
DTLS-Tunnel:
  Tunnel ID    : 12.3
  Assigned IP  : 172.16.1.10            Public IP    : 10.229.16.169
  Encryption   : AES256                 Hashing      : SHA1
  Ciphersuite  : DHE-RSA-AES256-SHA
  Encapsulation: DTLSv1.0               UDP Src Port : 59396
  UDP Dst Port : 443                    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

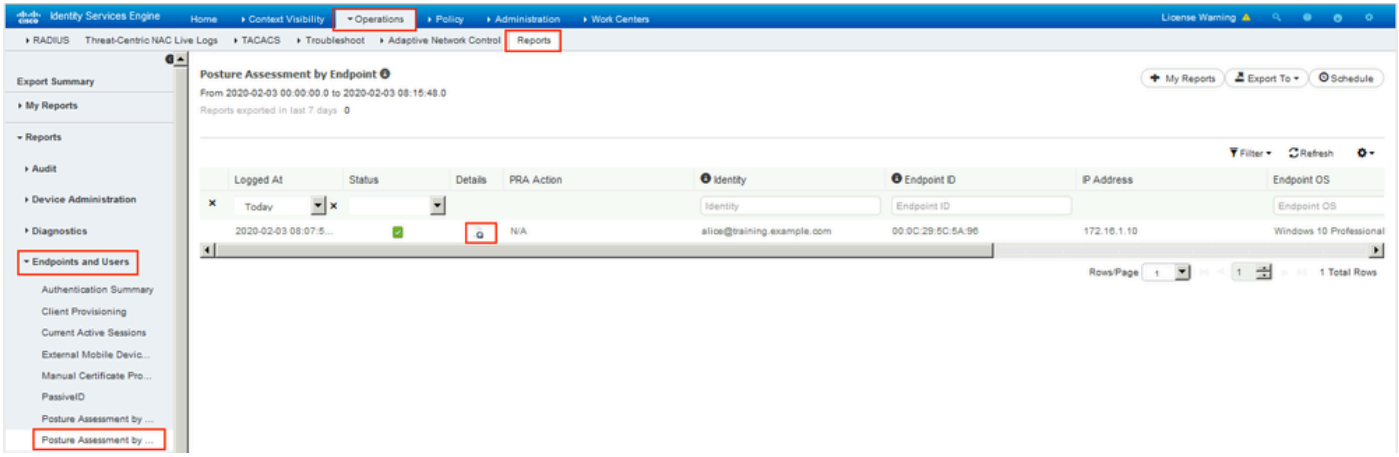

ISE Posture:
  Redirect URL : https://fyusifov-26-3.example.com:8443/portal/gateway?sessionId=000000000000c0005e37c81
  Redirect ACL : fyusifovredirect
```

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

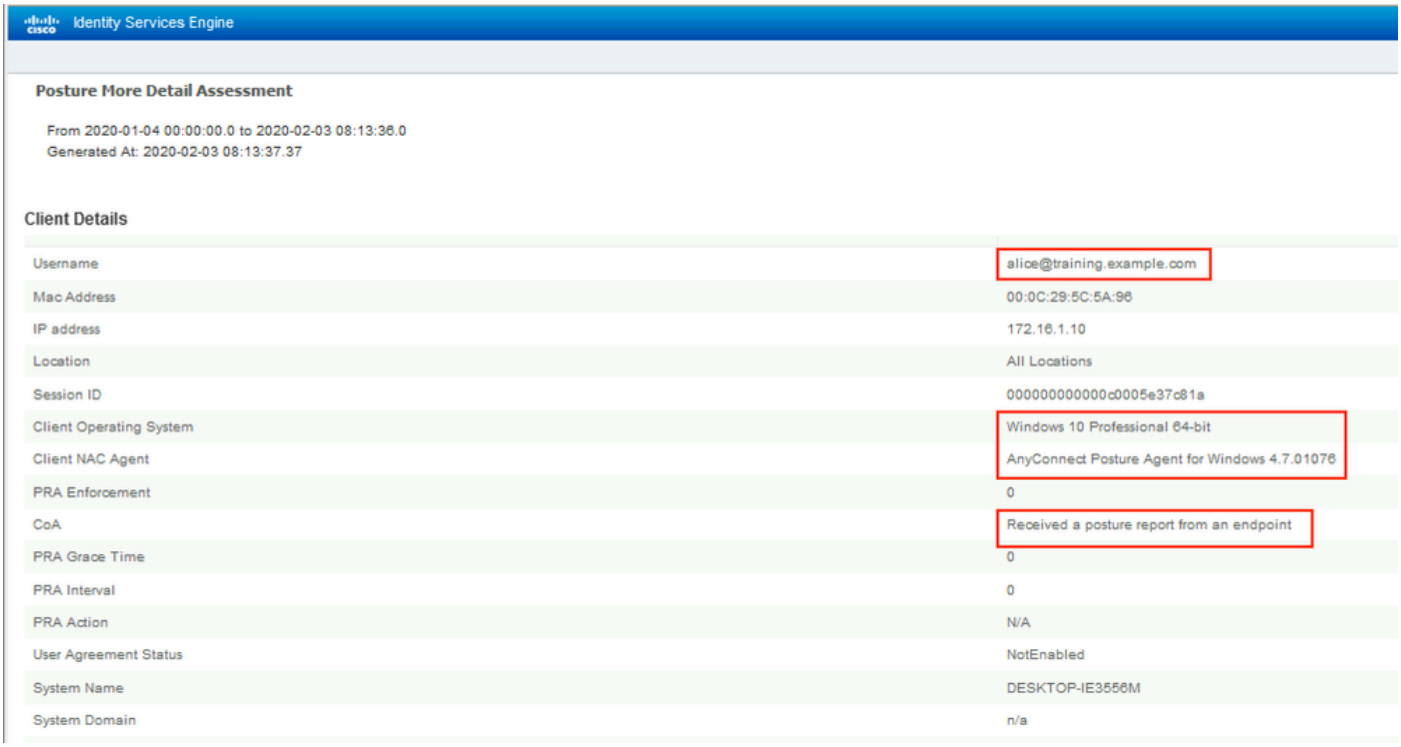
Les stratégies de provisionnement client peuvent être vérifiées. Accédez à Operations > Reports > Endpoints and Users > Client Provisioning.



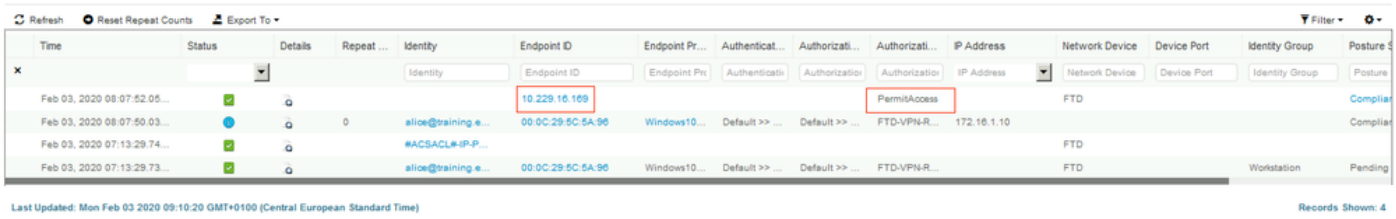
Le rapport de position envoyé depuis AnyConnect peut être vérifié. Accédez à Operations > Reports > Endpoints and Users > Posture Assessment by Endpoint.



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



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.

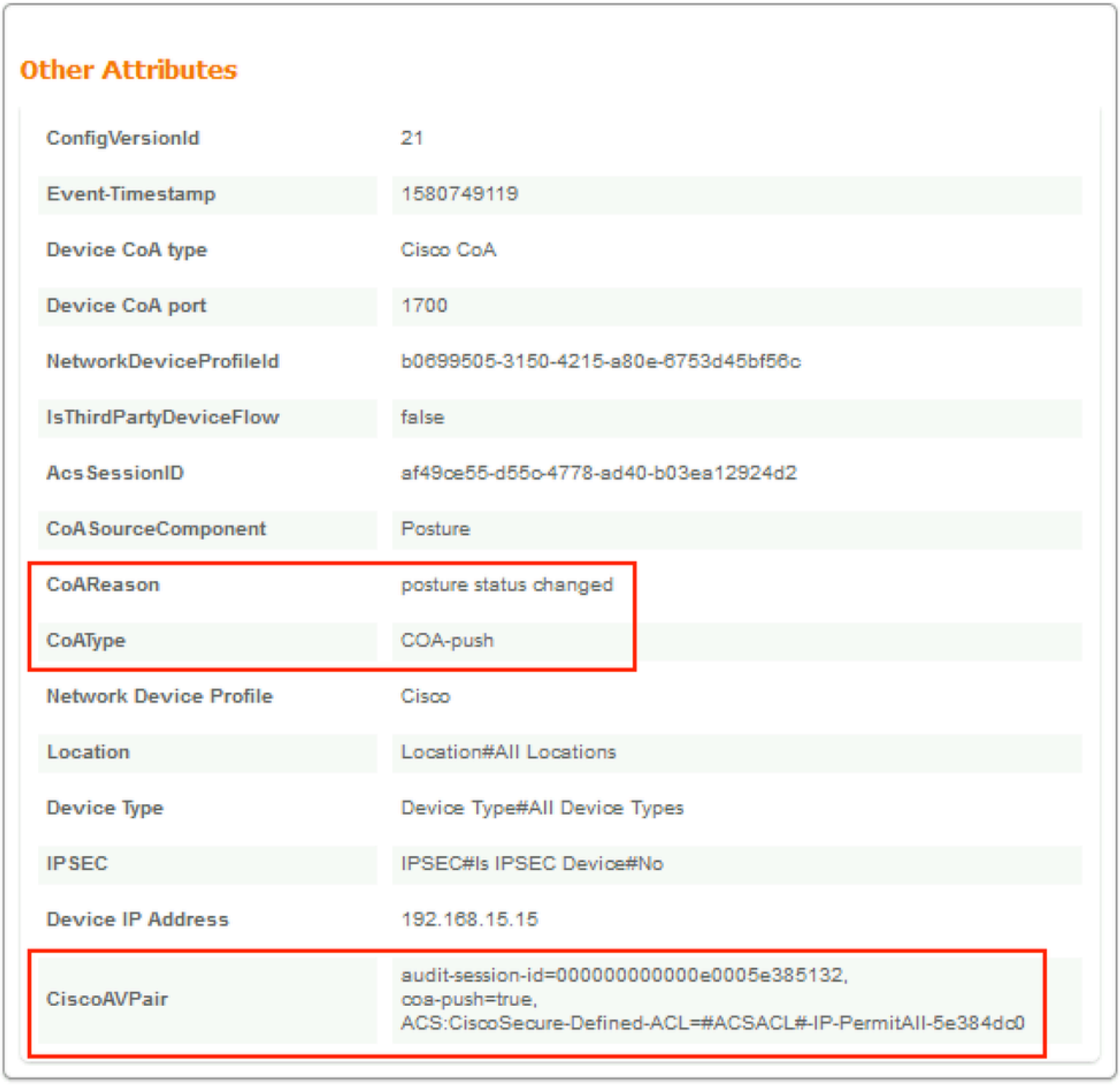


Overview

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	fyusifov-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



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

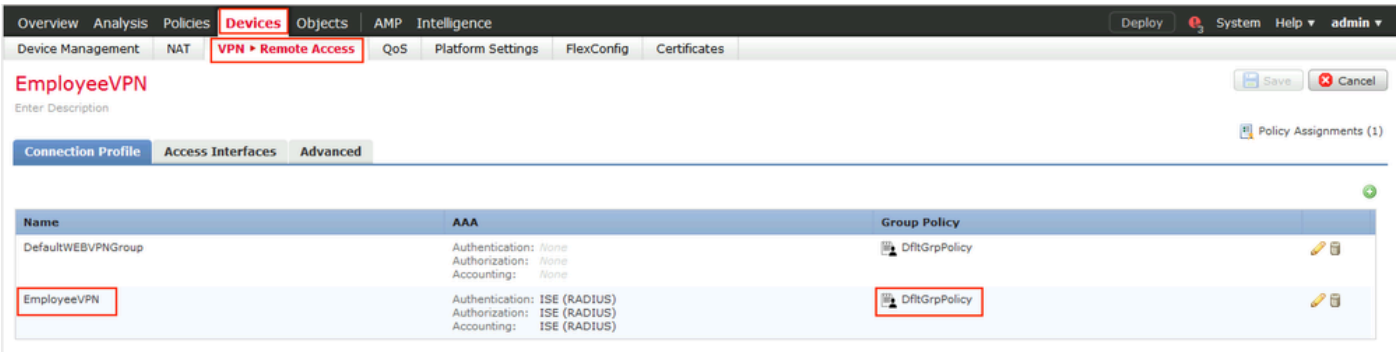
Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

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.]

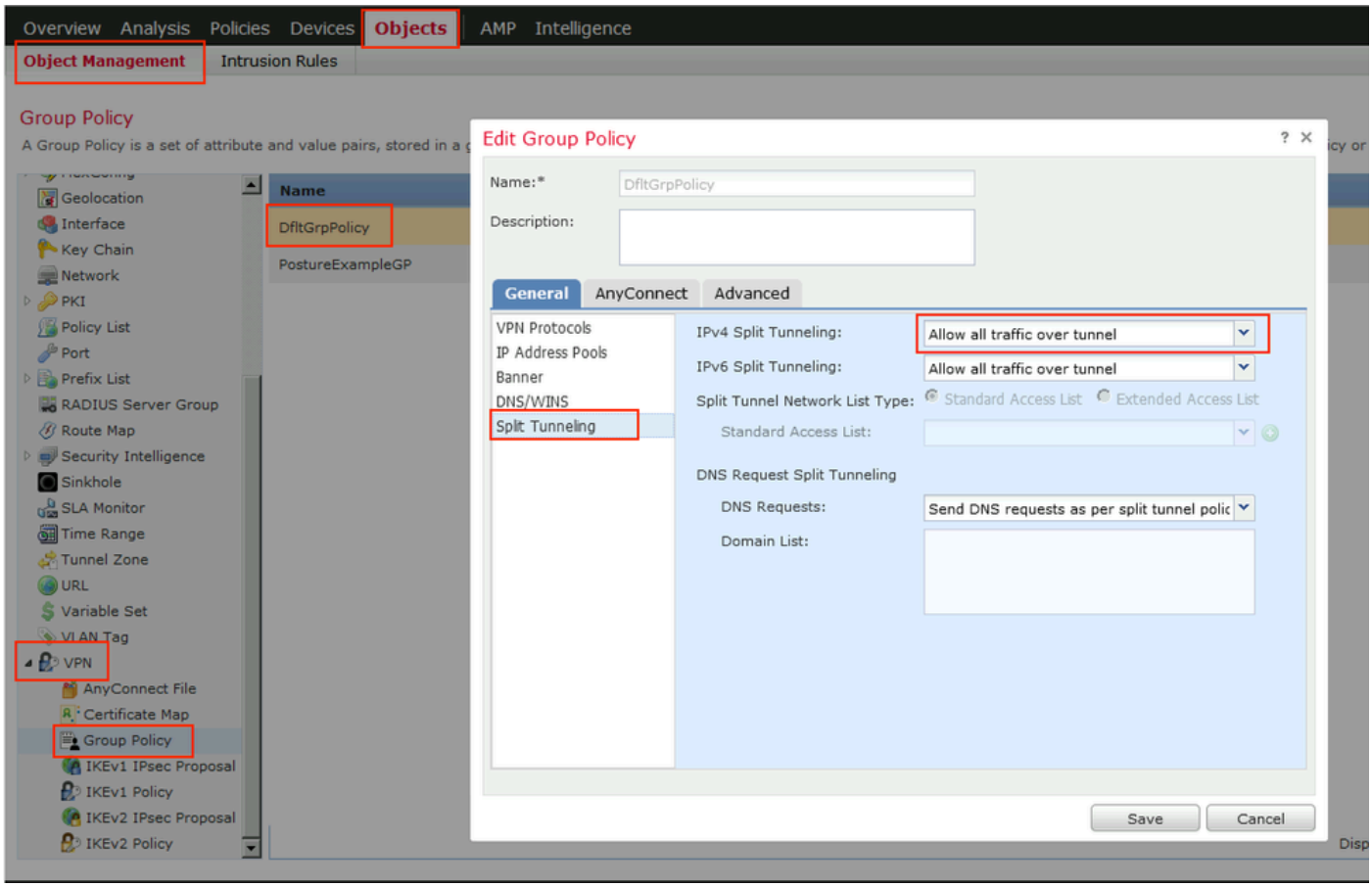
- Tunnel Fractionné

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 tunnellisé, 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.



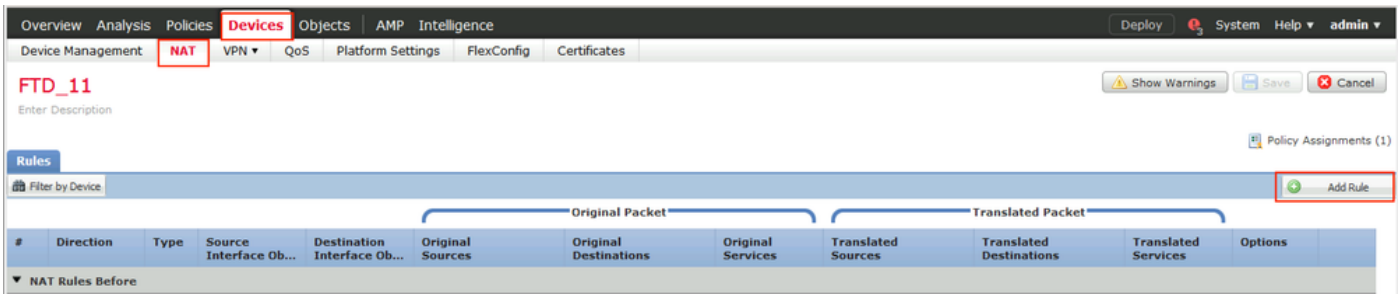
Accédez ensuite à Objects > Object Management > VPN > Group Policy et cliquez sur Group Policy configured for VPN.



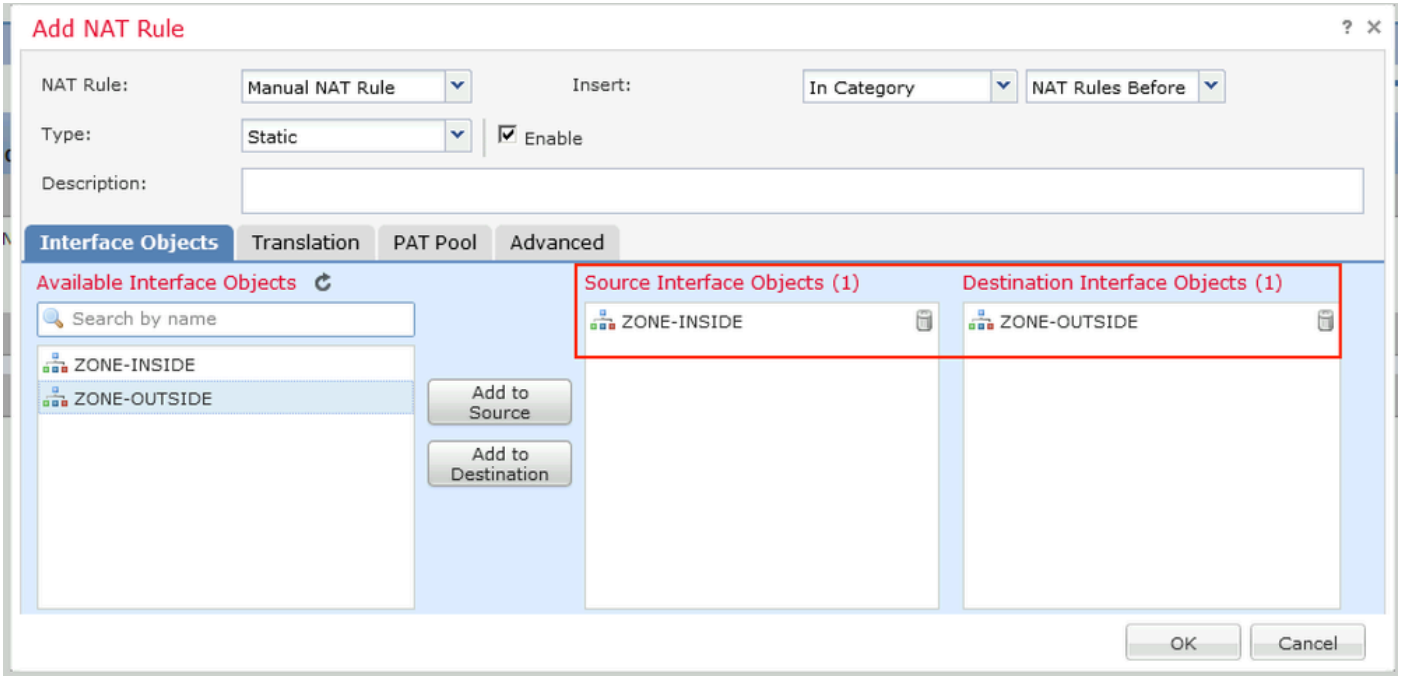
- NAT d'identité

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.

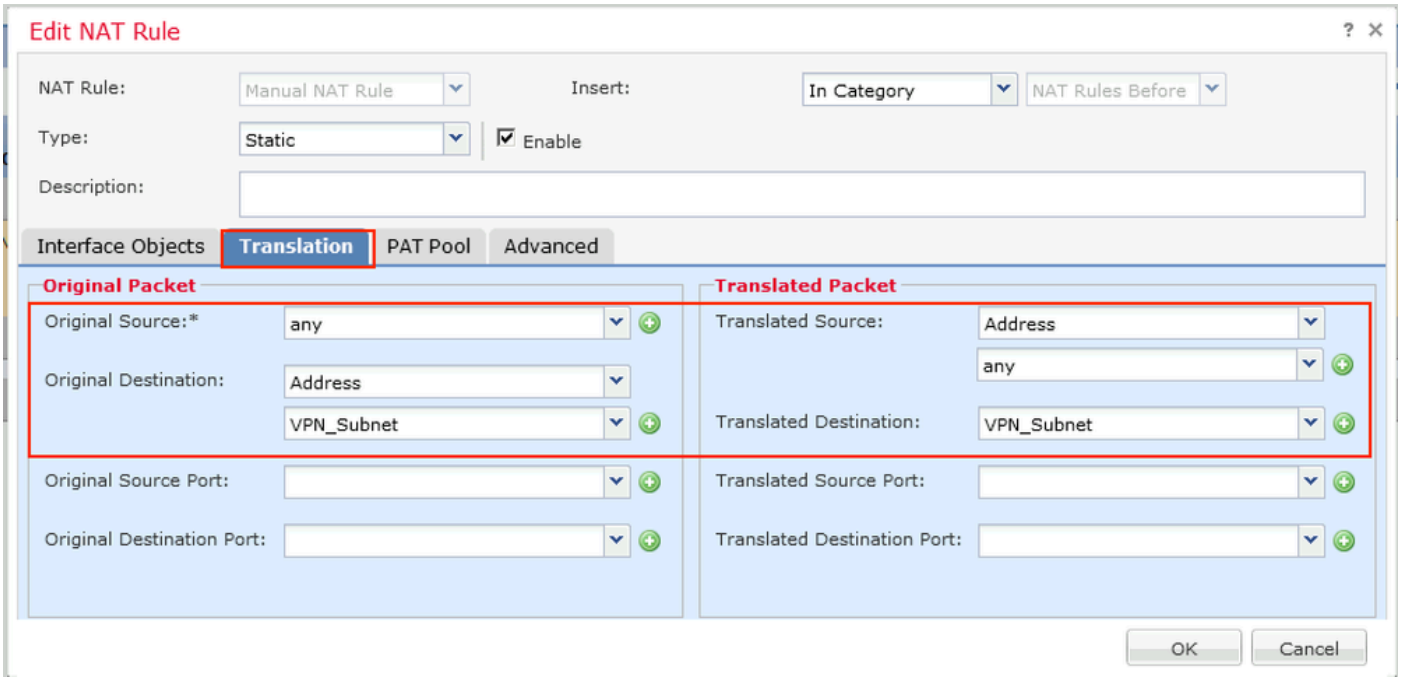
Tout d'abord, vérifiez les règles NAT pour ce périphérique. Accédez à Devices > NAT, puis cliquez sur Add Rule pour créer une nouvelle règle.



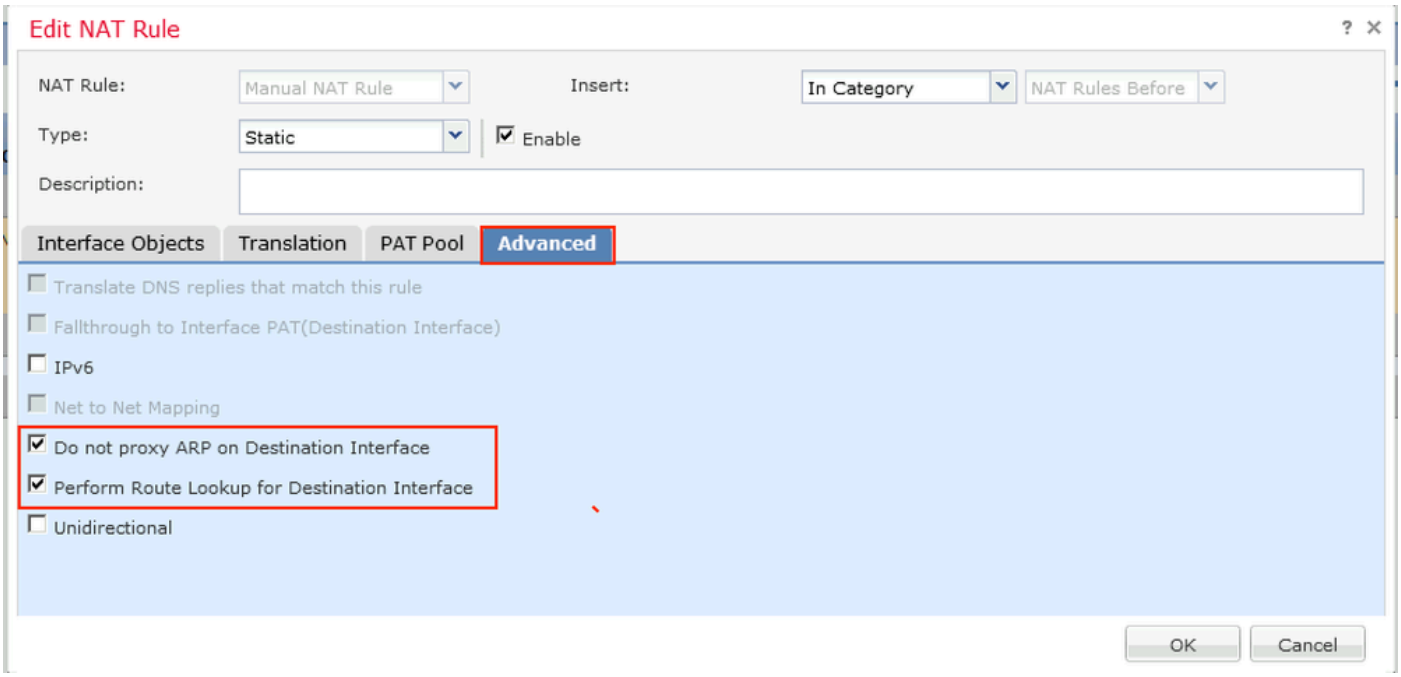
Dans la fenêtre ouverte, sous l'onglet Interface Objects, sélectionnez Security Zones. Dans cet exemple, l'entrée NAT est créée de ZONE-INSIDE à ZONE-OUTSIDE.



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:
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

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.