Configurez AnyConnect VPN sur FTD utilisant Cisco ISE en tant que serveur de RADIUS avec la racine CA des Windows Server 2012

Contenu

Contenu

Introduction

Ce document décrit comment configurer AnyConnect VPN (réseau privé virtuel) sur un Pare-feu FTD (défense contre des menaces de FirePOWER) utilisant Cisco ISE (Cisco Identity Services Engine) en tant que serveur de RADIUS. Nous utilisons des Windows Server 2012 en tant que notre racine CA (autorité de certification) de sorte que la transmission au-dessus du VPN soit

sécurisée par des Certificats c.-à-d. l'employé que le PC fera confiance au certificat du FTD parce que le certificat FTD VPN a été signé par notre racine CA des Windows Server 2012

Conditions préalables

Exigences

Vous devez avoir déployé suivant et s'exécuter dans votre réseau :

- Le centre de Gestion de FirePOWER et le Pare-feu de défense contre des menaces de FirePOWER se sont déployés avec la Connectivité de base
- Cisco ISE déployé et s'exécutant dans votre réseau
- Windows Server (avec le Répertoire actif) déployés et Windows des employés/PC de MAC joints vers le domaine d'AD (Répertoire actif)

Dans notre exemple ci-dessous, les employés ouvriront le client d'AnyConnect sur leur PC de Windows/MAC, et ils se connecteront sécurisé à l'interface extérieure du FTD par l'intermédiaire du VPN utilisant leurs qualifications. Le FTD vérifiera leur nom d'utilisateur et mot de passe contre Cisco ISE (qui vérifiera avec le Répertoire actif de Windows Server pour vérifier leur nom d'utilisateur, le mot de passe, et des utilisateurs de groupe c.-à-d. seulement dans le groupe « employés » d'AD pourra au VPN dans le réseau de société.

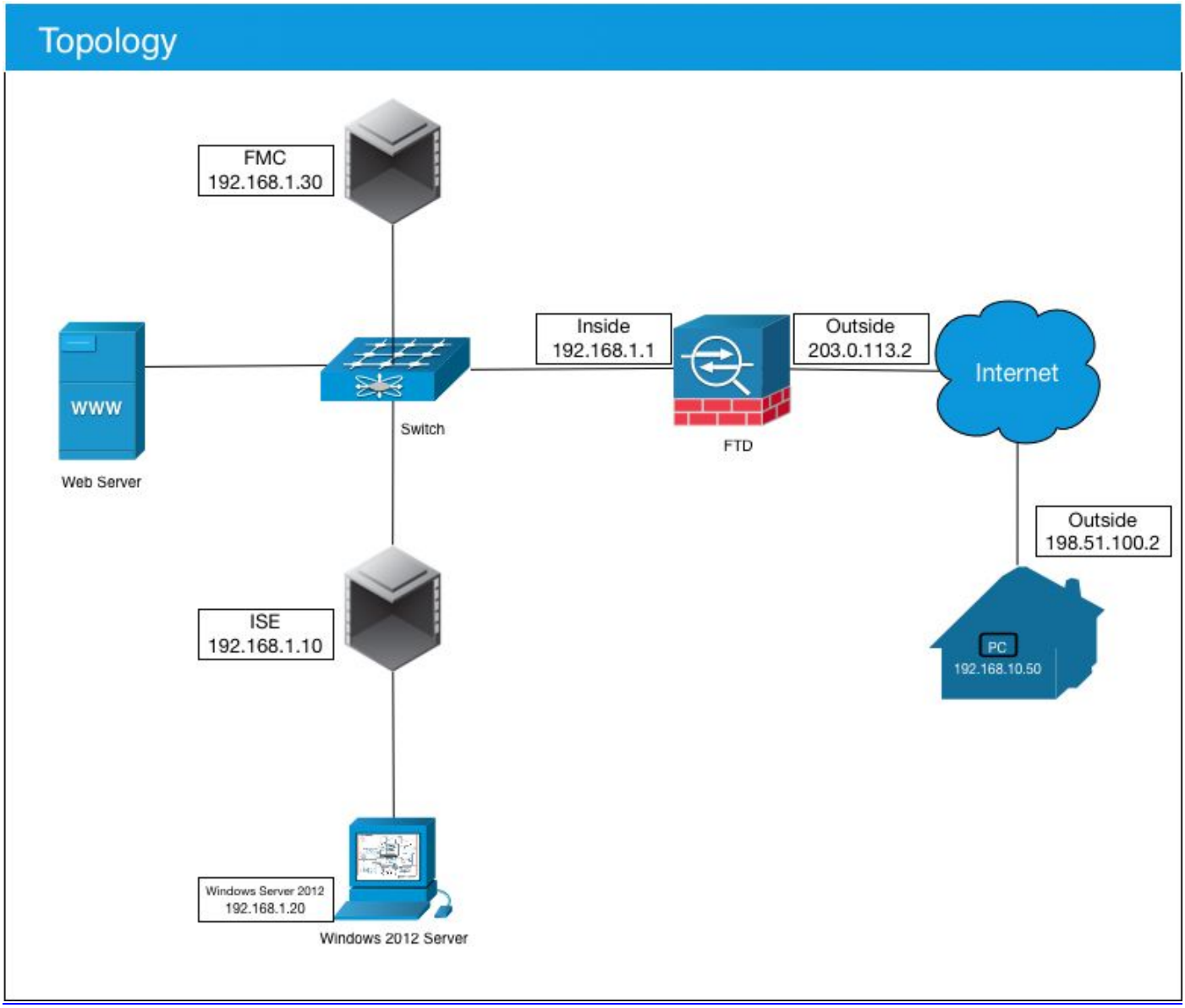
Composants utilisés

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

- Centre de Gestion de FirePOWER et défense contre des menaces de FirePOWER exécutant 6.2.3
- Logiciel Cisco Identity Services Engine exécutant 2.4
- Client à mobilité sécurisé Cisco AnyConnect exécutant 4.6.03049
- Services du Répertoire actif R2 courant et du certificat des Windows Server 2012 (c'est notre racine le CA pour tous les Certificats)
- Windows 7, Windows 10, PC de MAC

Configurer

Diagramme du réseau



Dans ce cas d'utilisation, le PC de Windows des employés/MAC exécutant le client d'Anyconnect VPN se connectera à l'adresse IP publique extérieure du Pare-feu FTD, et Cisco ISE les accordera dynamiquement a limité ou accès complet à certaines ressources internes ou en Internet (configurables) une fois qu'ils sont connectés par l'intermédiaire du VPN selon quel groupe d'AD ils sont un membre de dans Répertoire actif

Périphérique	Hostname/FQDN	Adresse IP publique	Adresse IP privée	Adresse IP d'AnyConne
PC Windows	-	198.51.100.2	10.0.0.1	192.168.10.50
FTD	ciscofp3.cisco.com	203.0.113.2	192.168.1.1	-
FMC	-	-	192.168.1.30	-
Cisco ISE	ciscoise.cisco.com	-	192.168.1.10	-
Windows Server 2012	ciscodc.cisco.com	-	192.168.1.20	-
Serveurs internes	-	-	192.168.1.x	-

Configuration

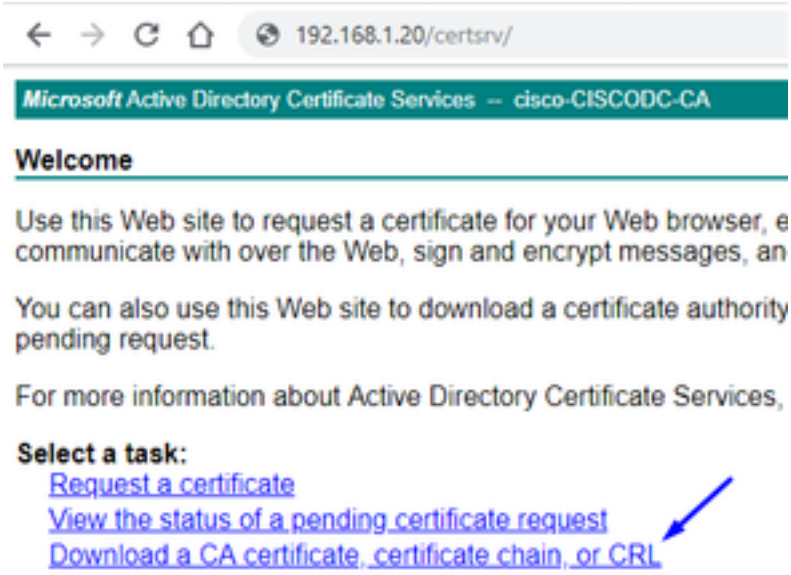
Exportez le certificat de CA de racine des Windows Server

Dans ce document, nous utiliserons la Microsoft Windows Server 2012 en tant que notre racine CA pour des Certificats. La confiance de la volonté du PC de client cette racine CA à connecter sécurisé au FTD par l'intermédiaire du VPN (voir les étapes ci-dessous). Ceci s'assurera qu'ils

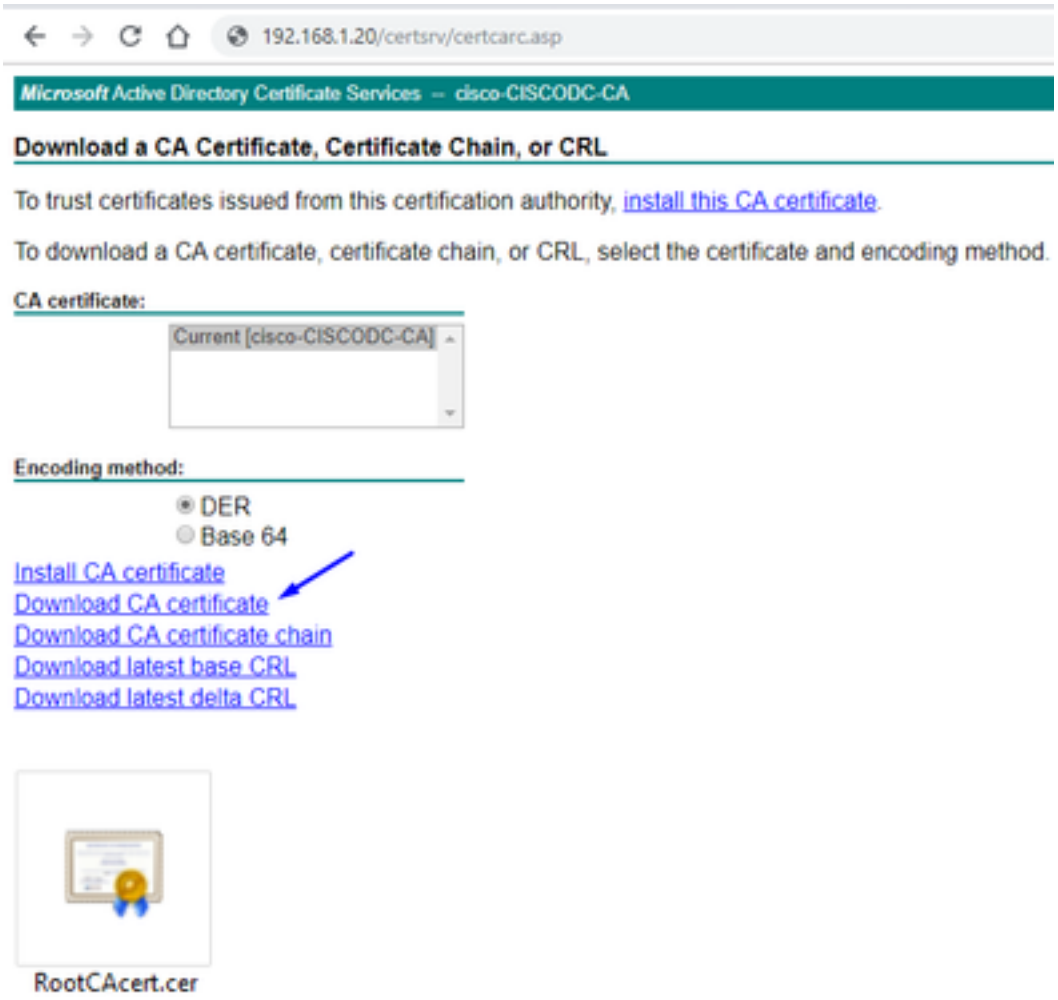
peuvent se connecter sécurisé au FTD au-dessus de l'Internet et accéder à des ressources internes de maison. Leur PC fera confiance à la connexion dans leur navigateur et client d'AnyConnect.

Allez à http://192.168.1.20/certsrv et suivez les étapes ci-dessous pour télécharger votre certificat de CA de racine de Windows Server :

Cliquez sur Download un **certificat de CA, une chaîne de certificat, ou un CRL**



Cliquez sur Download le **certificat** et renommez-le à 'RootCAcert3.cer



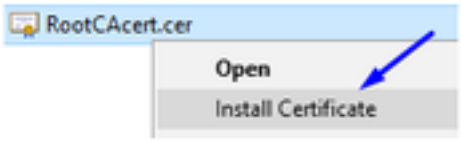
Installez le certificat de CA de racine sur l'employé Windows/PC de MAC

Méthode 1 : Installez le certificat sur tous les PC des employés en le poussant par l'intermédiaire de la stratégie de groupe de Windows Server (idéale pour n'importe quoi plus de 10 utilisateurs VPN) :

Comment utiliser des Windows Server pour distribuer des Certificats aux ordinateurs client à l'aide de la stratégie de groupe

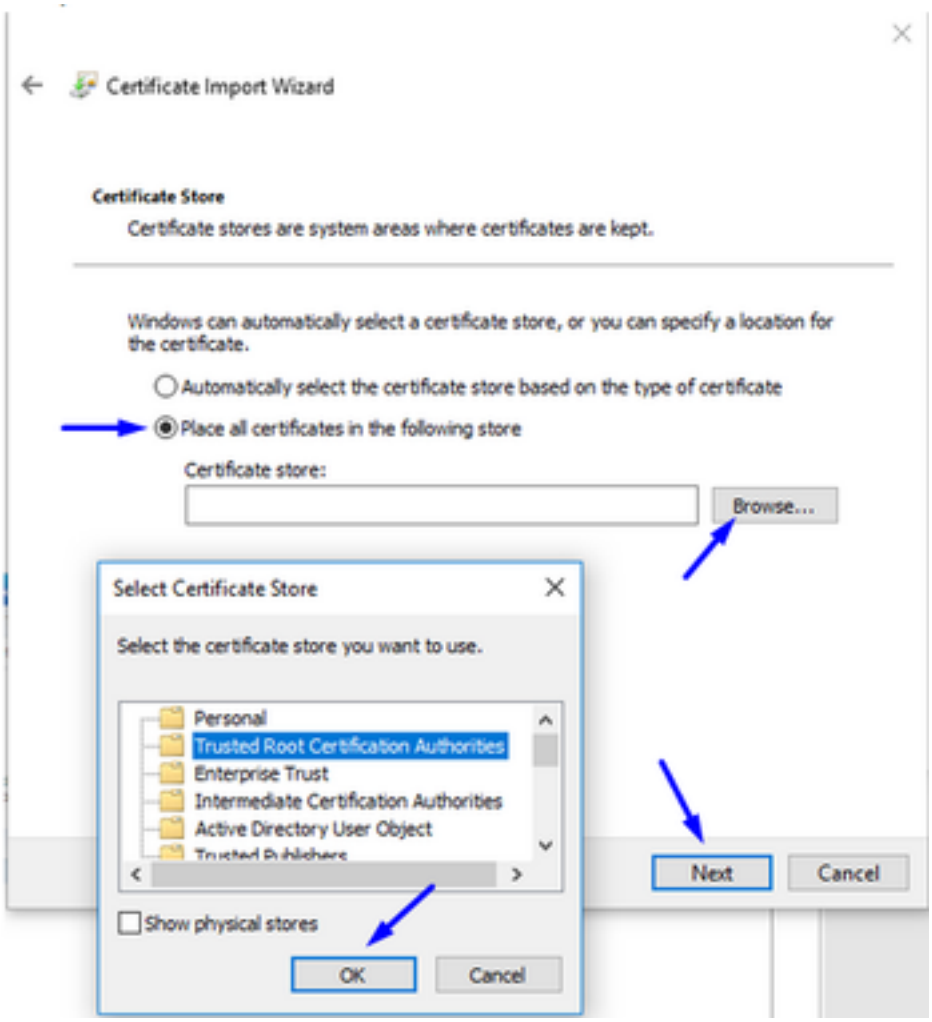
Méthode 2 : Installez le certificat sur tous les PC des employés en l'installant individuellement sur chaque PC (idéal pour examiner un utilisateur VPN) :

Cliquez avec le bouton droit le certificat sur le PC de Windows/MAC des vos employés et le clic **installent le certificat**



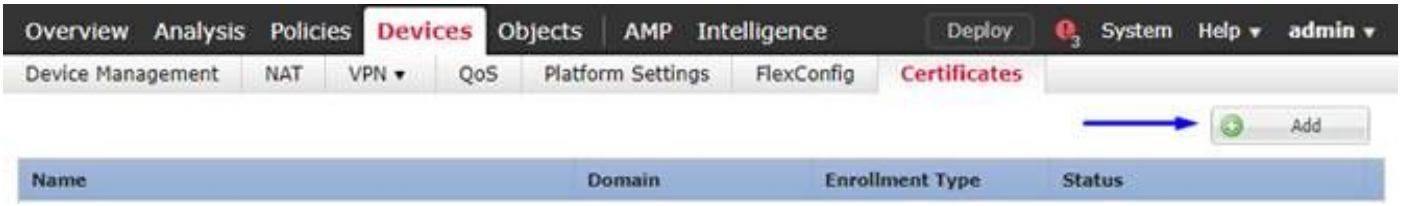
Sélectionnez le « utilisateur courant »

L'endroit choisi **tous les Certificats dans la mémoire suivante** et les **Autorités de certification racine approuvée** choisies, **ok de** clic, cliquent sur Next, et cliquent sur Finish

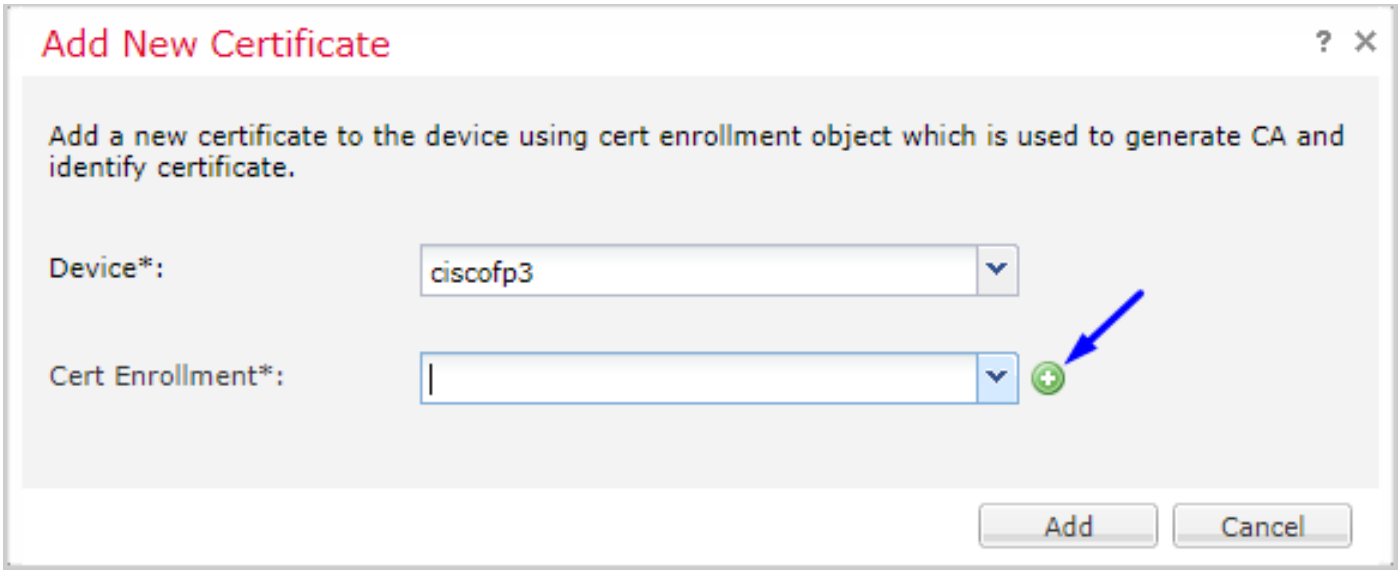


Générez un CSR sur FTD, obtenez le CSR signé par la racine CA de Windows Server, et installez ce certificat signé sur FTD

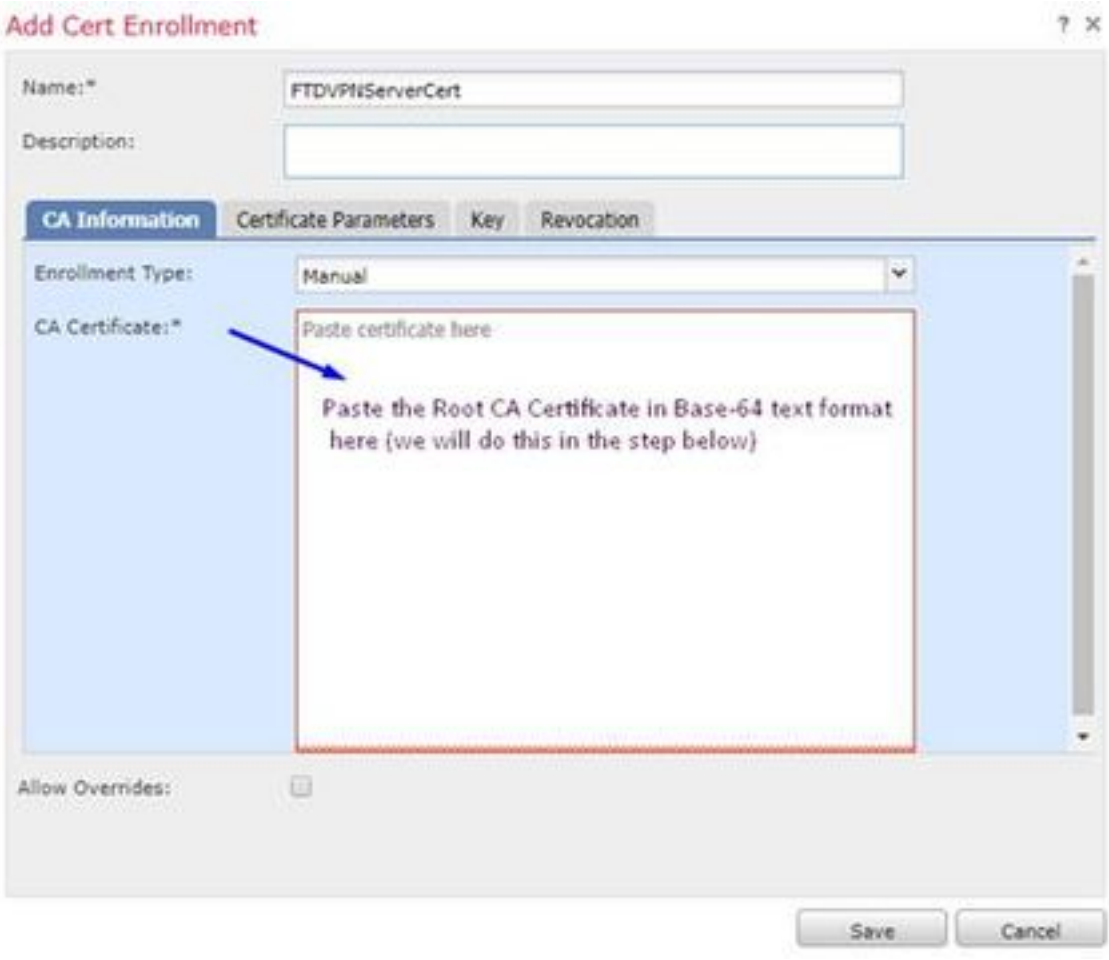
Allez aux **objets** > à la **Gestion d'objet** > à l'**inscription de PKI** > de **CERT**, cliquez sur en fonction l'**inscription de CERT Add**



Cliquez sur Add le bouton d'**inscription de CERT**



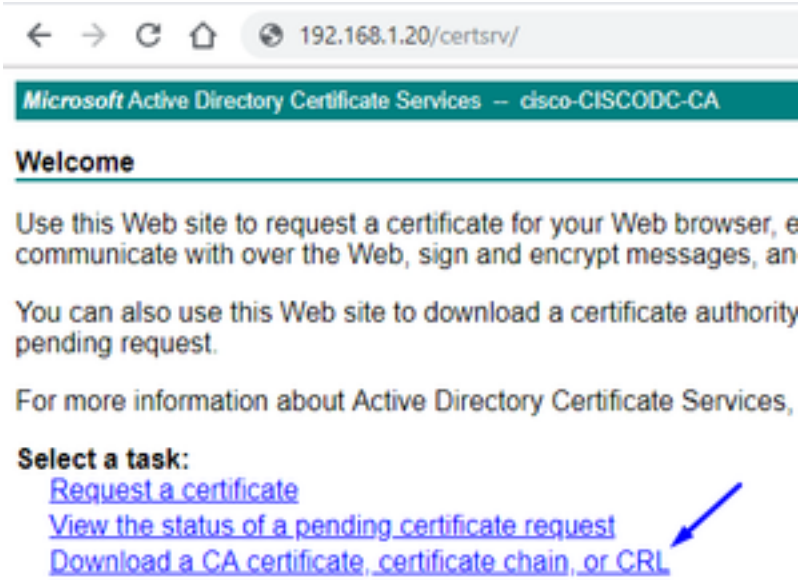
Type > manuel choisis d'**inscription**
Comme vu dans l'image ci-dessous, nous devons coller notre certificat de CA de racine ici :



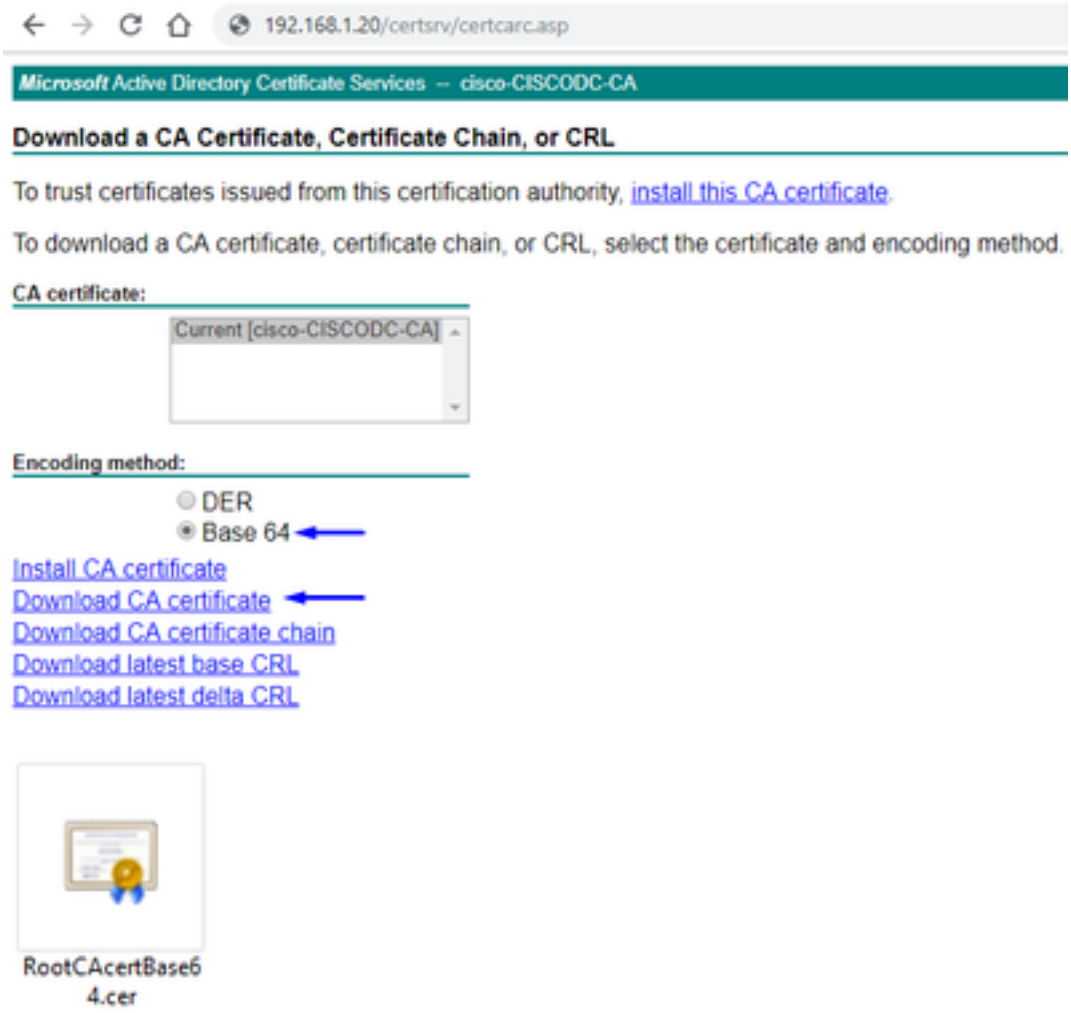
Voici comment télécharger votre certificat de CA de racine, le visualiser dans le format texte, et le coller dans la case ci-dessus :

Allez à http://192.168.1.20/certsrv

Cliquez sur Download un **certificat de CA, une chaîne de certificat, ou un CRL**

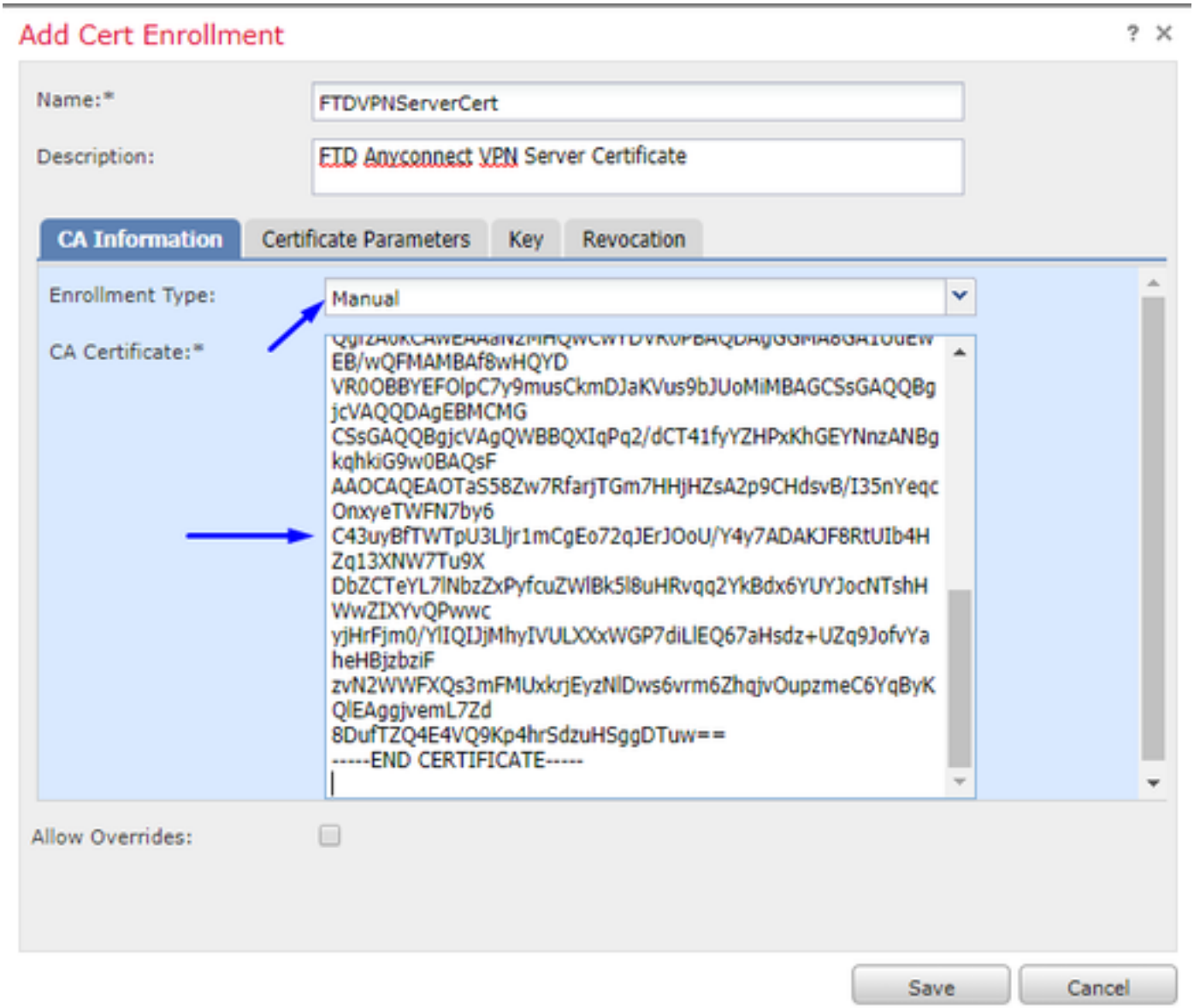


Le bouton de la **base 64 de** clic > cliquent sur Download le **certificat de CA**



Ouvrez le fichier de RootCAcertBase64.cer dans Notepad

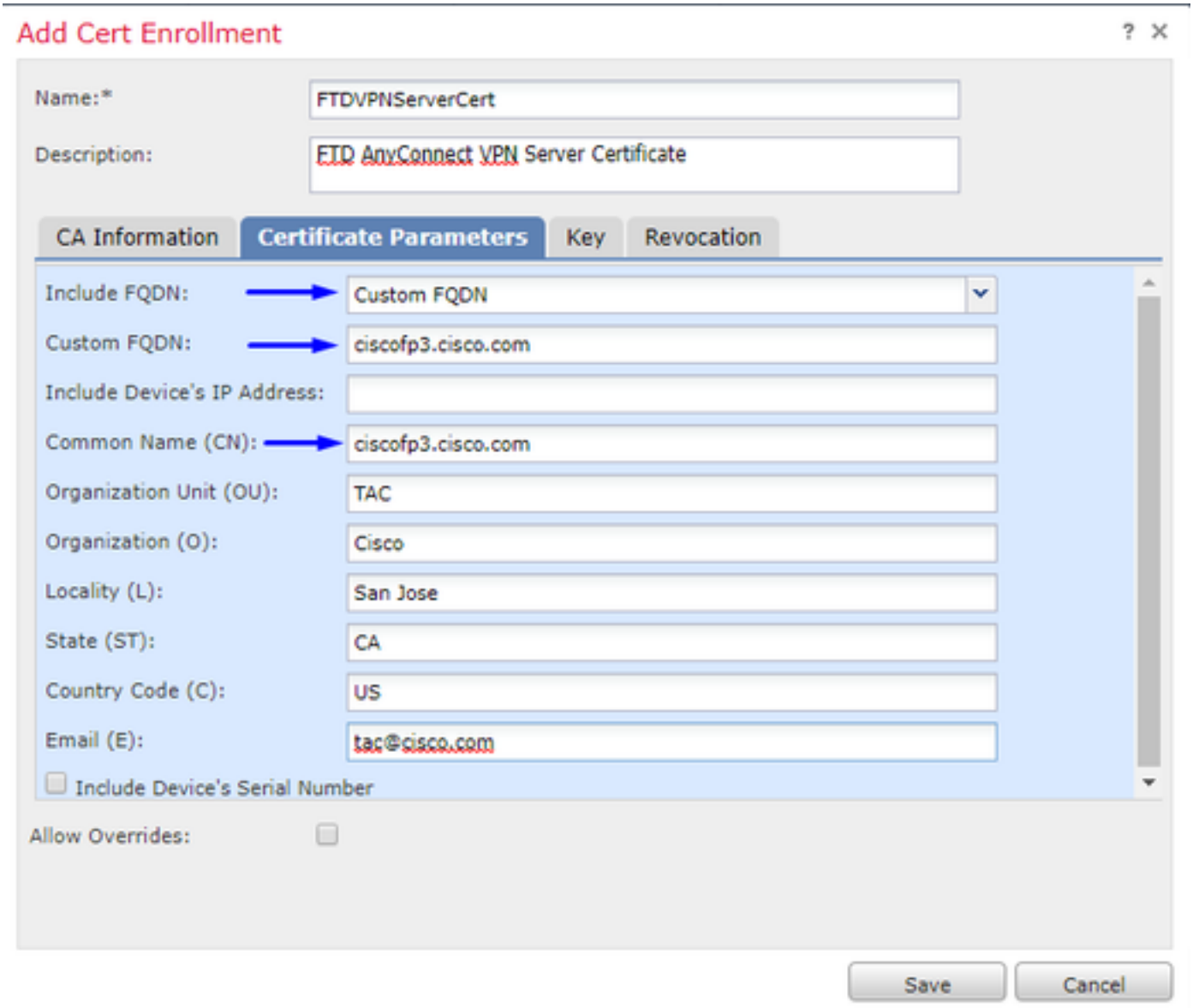
Copiez et collez le contenu de .cer (certificat de CA de racine) du serveur d'AD de Windows ici :



Onglet >> type de **paramètres de certificat de** clic vos informations de certificat

Remarque:
Le champ FQDN de coutume doit être le FQDN de votre FTD

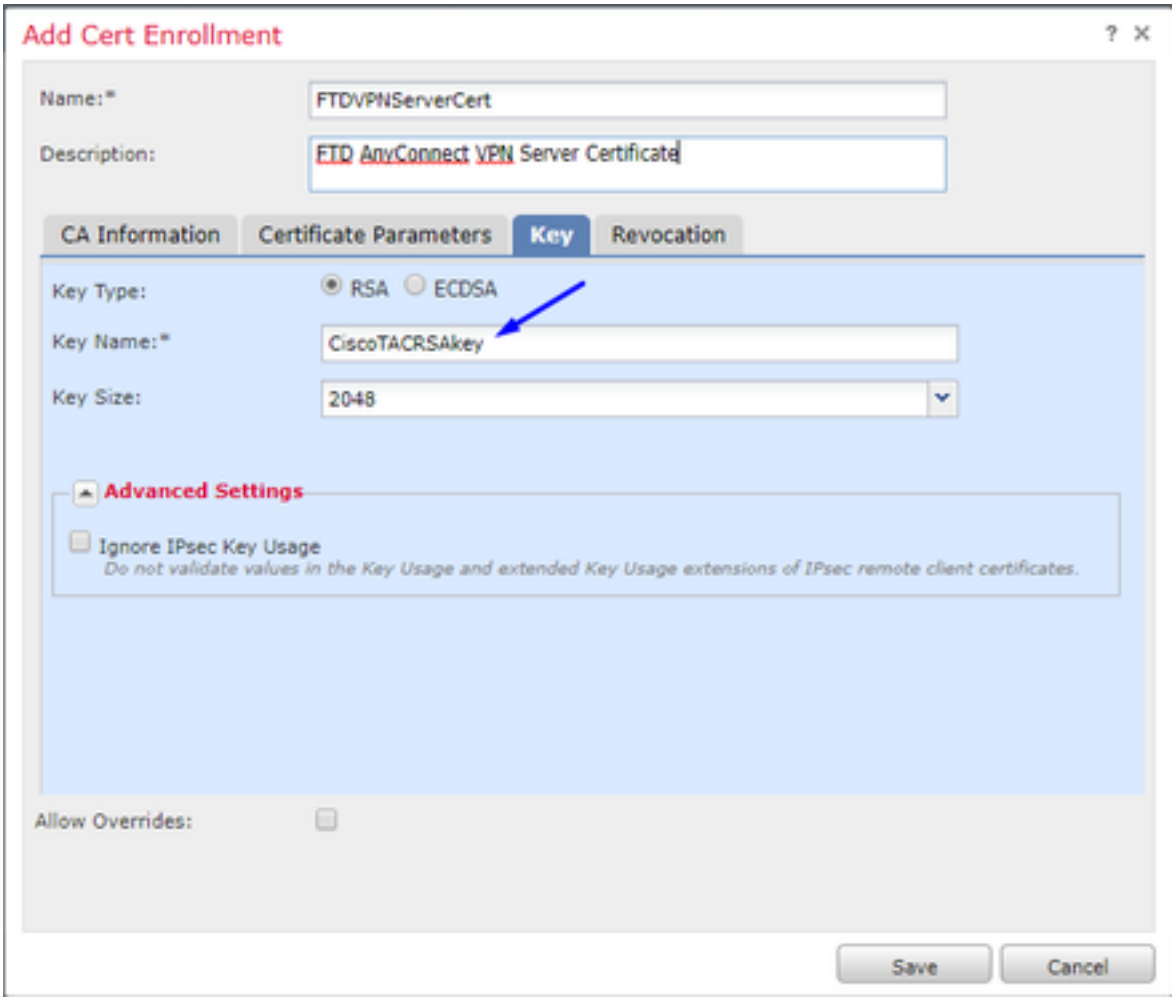
La zone d'identification commune doit être le FQDN de votre FTD



Conseil : vous pouvez obtenir le FQDN de votre FTD en tapant la commande suivante du FTD CLI :

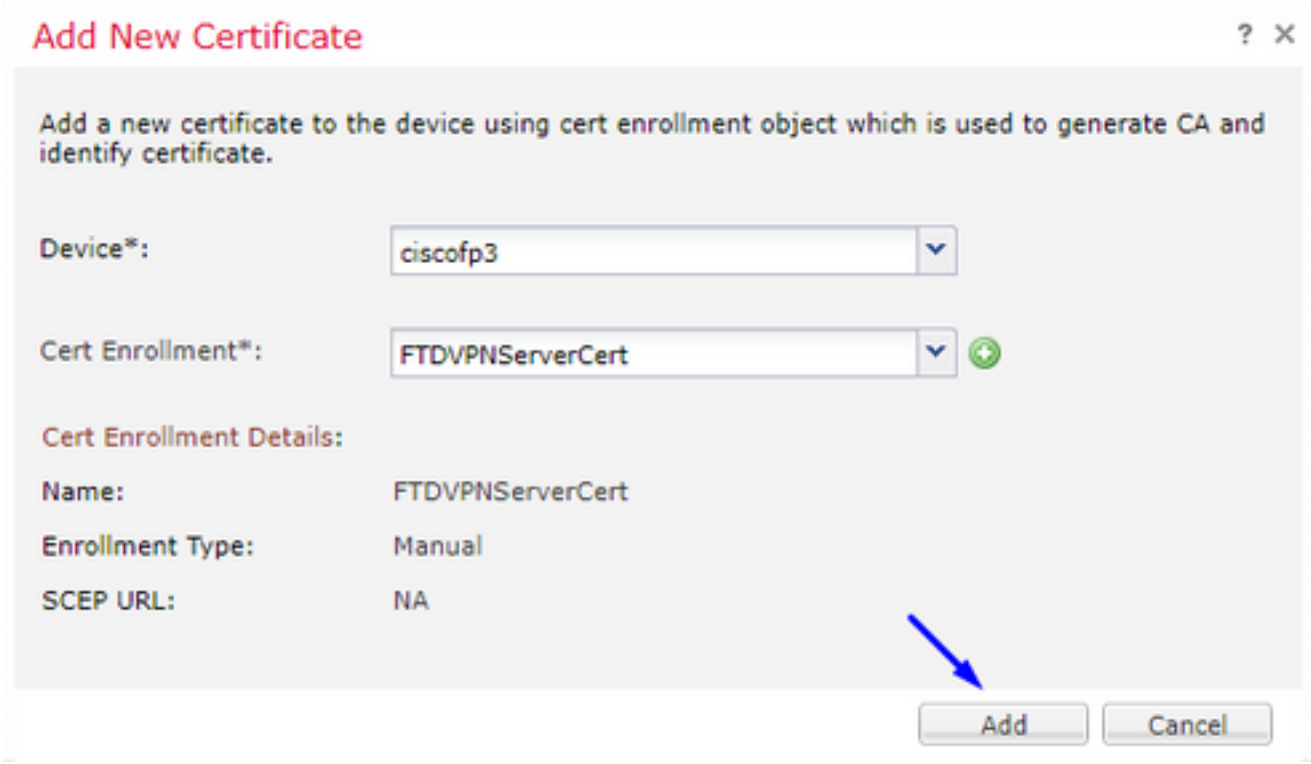
```
> show network
===============[ System Information ]===============
Hostname : ciscofp3.cisco.com
Domains : cisco
DNS Servers : 192.168.1.20
Management port : 8305
IPv4 Default route
Gateway : 192.168.1.1

======================[ br1 ]=======================
State : Enabled
Channels : Management & Events
Mode : Non-Autonegotiation
MDI/MDIX : Auto/MDIX
MTU : 1500
MAC Address : 00:0C:29:4F:AC:71
----------------------[ IPv4 ]----------------------
Configuration : Manual
Address : 192.168.1.2
Netmask : 255.255.255.0
```

Cliquez sur l'onglet **principal** et introduisez n'importe quel **nom de clé**



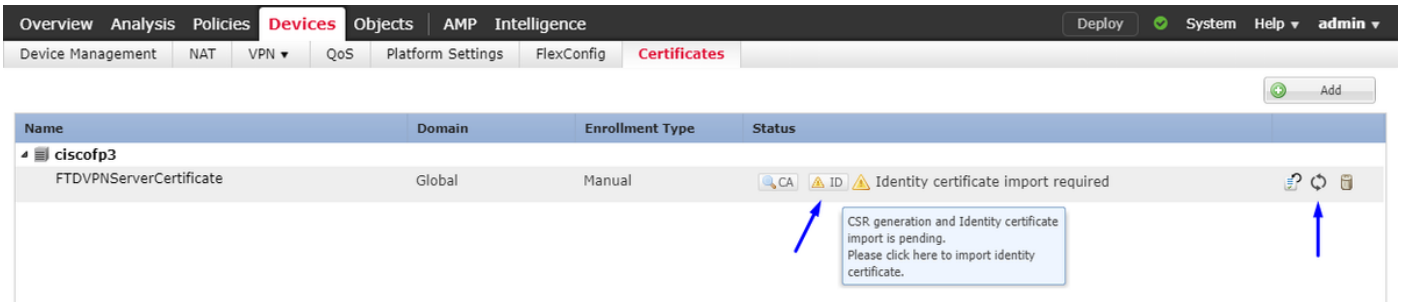
Sauvegarde de clic

Sélectionnez votre FTDVPNServerCert que nous juste avons créé en haut et cliquez sur Add

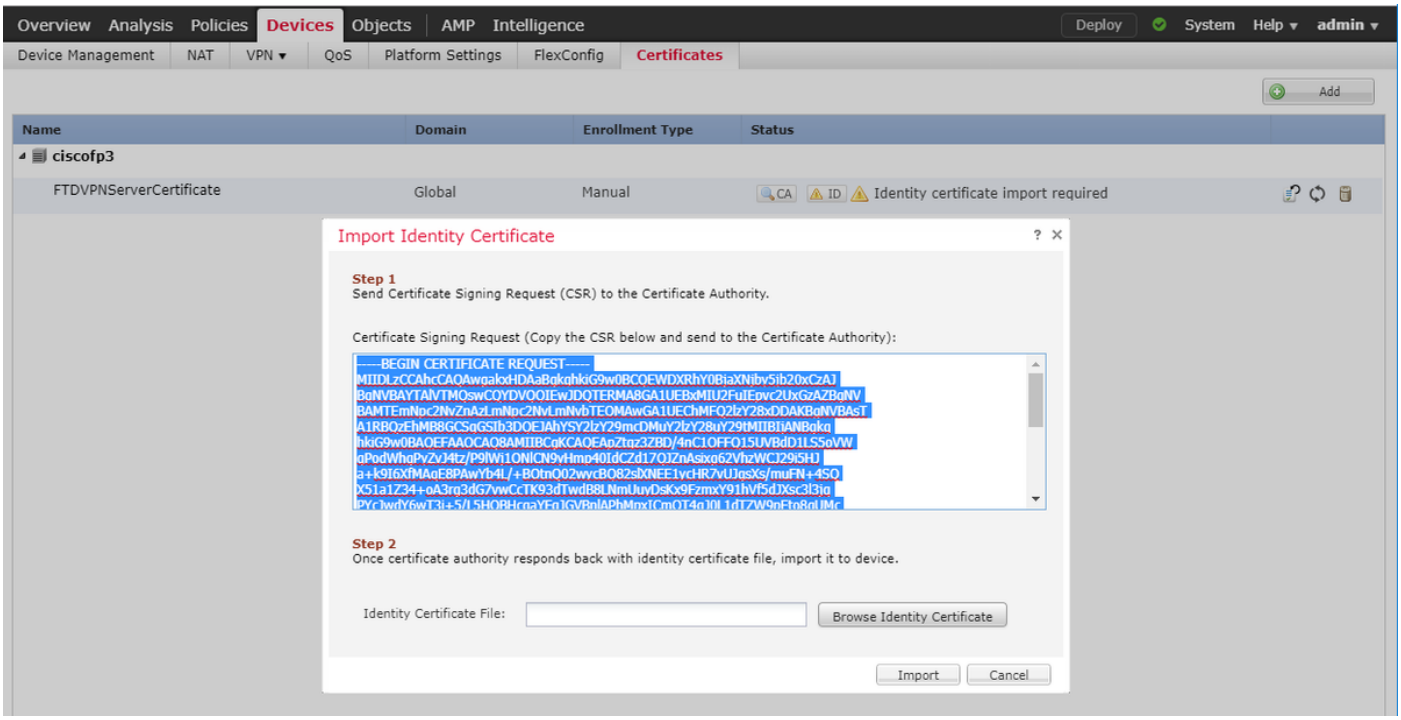


Conseil : Attendez environ 10-30 secondes FMC + FTD pour vérifier et installer le certificat de CA de racine (le clic régénèrent l'icône s'il ne fait pas exposition)

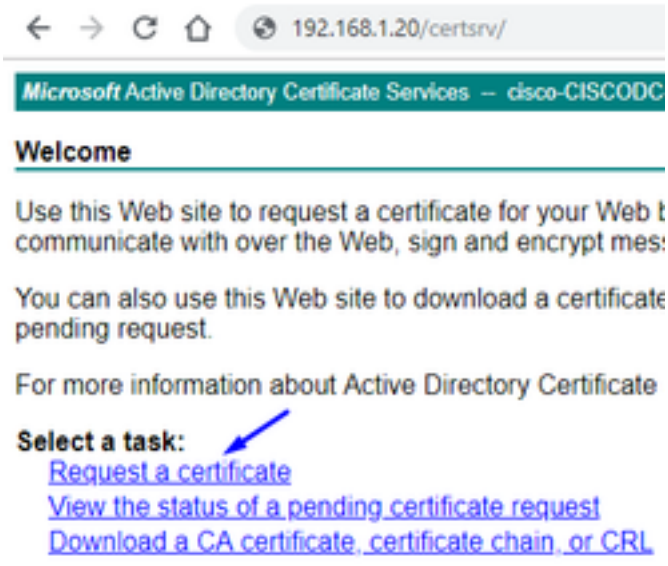
Cliquez sur le bouton d'**ID** :



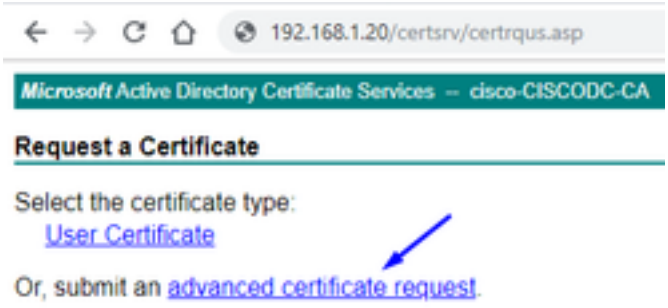
Copiez et collez ce CSR, et prenez-le à votre racine CA de Windows Server :



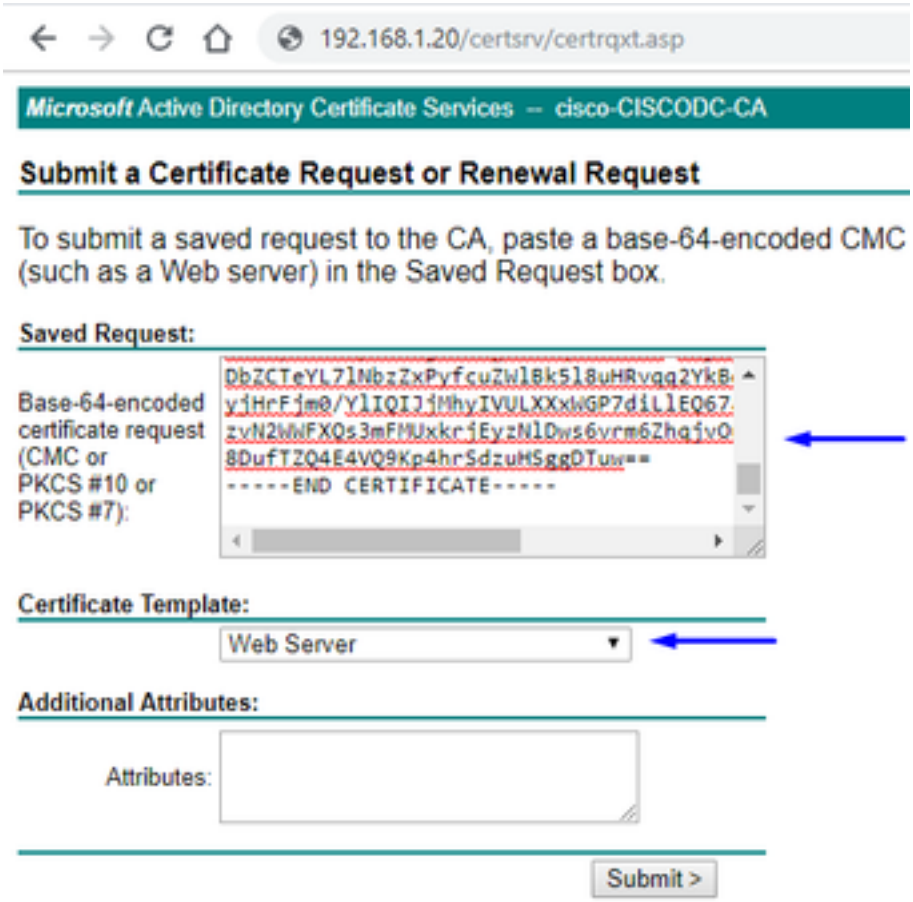
Allez à http://192.168.1.20/certsrv



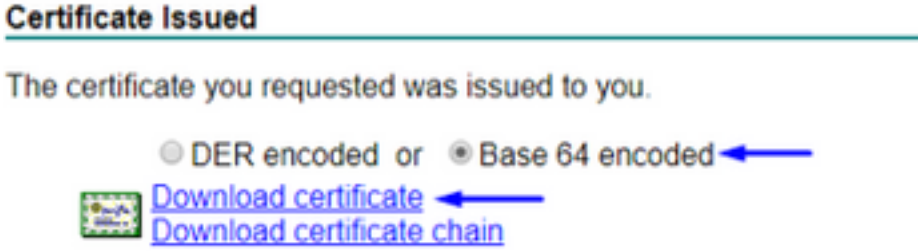
Demande de certificat avancée par clic

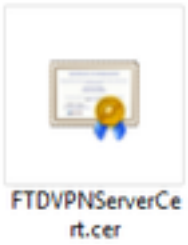


Collez votre demande de signature de certificat (CSR) dans le champ ci-dessous et sélectionnez le **serveur Web** comme modèle de certificat

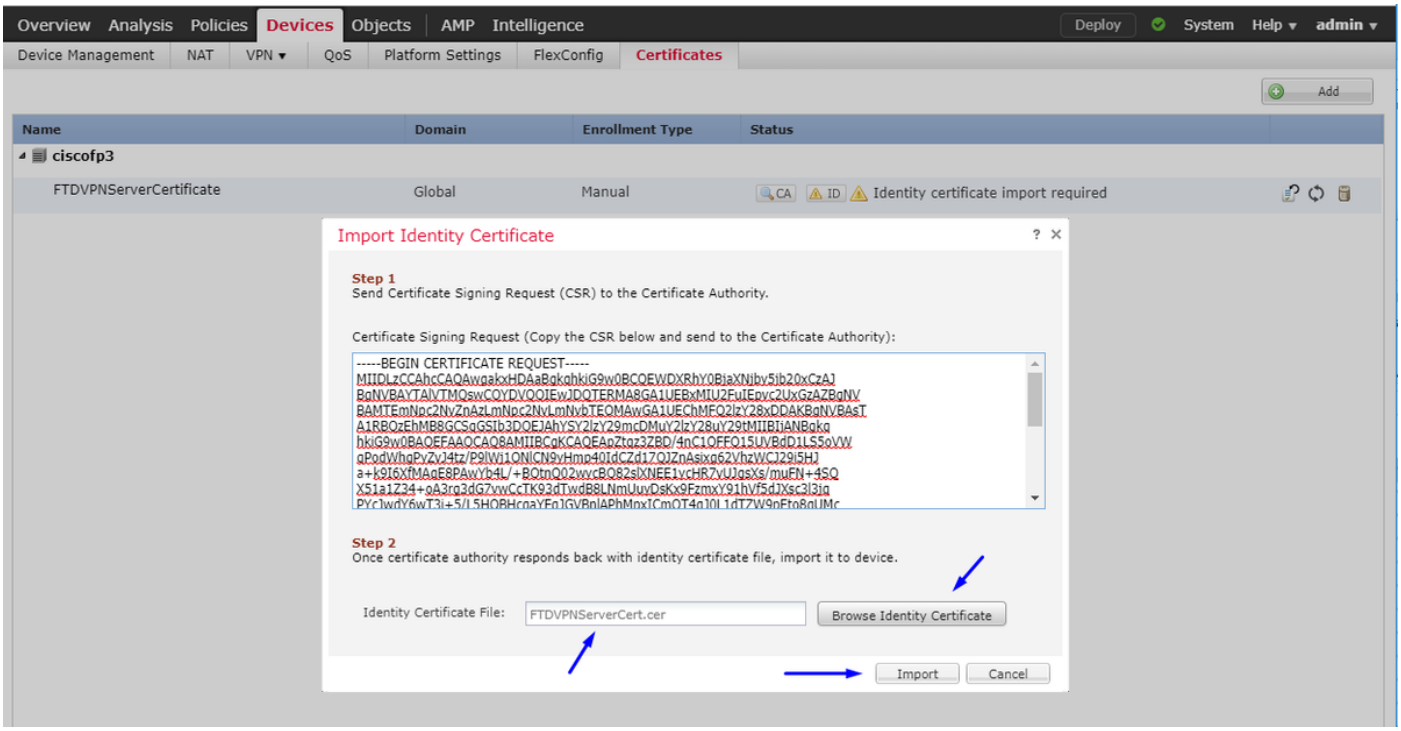


Cliquez sur Submit
Cliquez sur le bouton **encodé par 64 de base** et cliquez sur Download le **certificat**

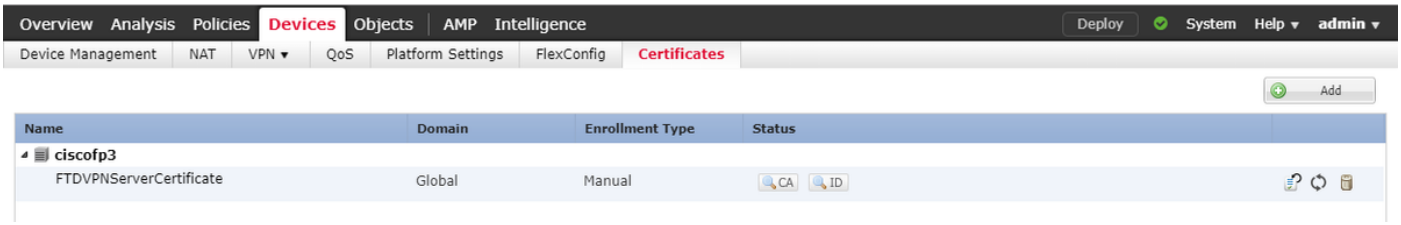




Cliquez sur **parcourent le certificat d'identité** et sélectionnent le certificat que nous les avons juste téléchargé



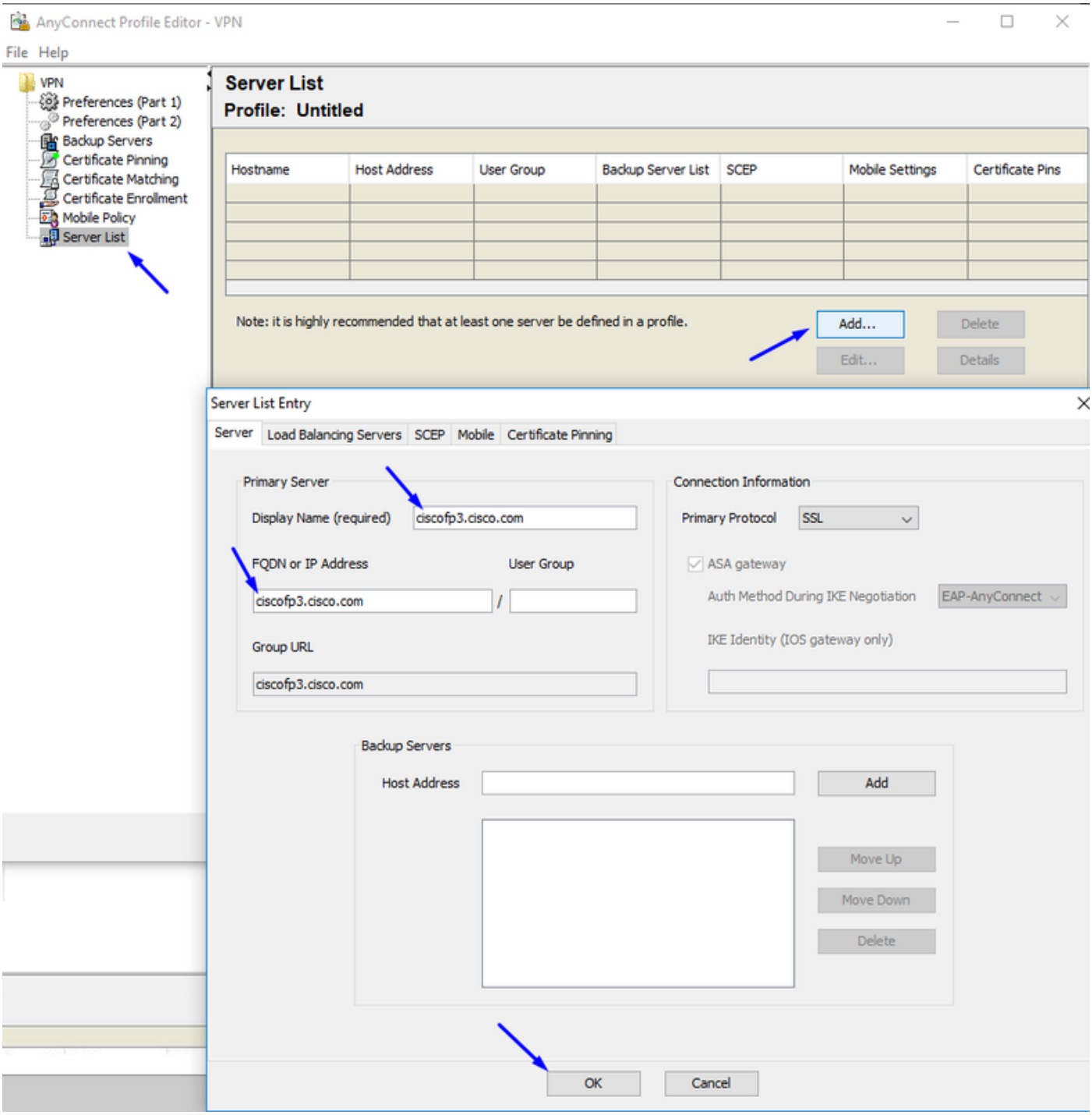
Le certificat de serveur VPN FTD (signé par racine CA de Windows Server) a été installé avec succès

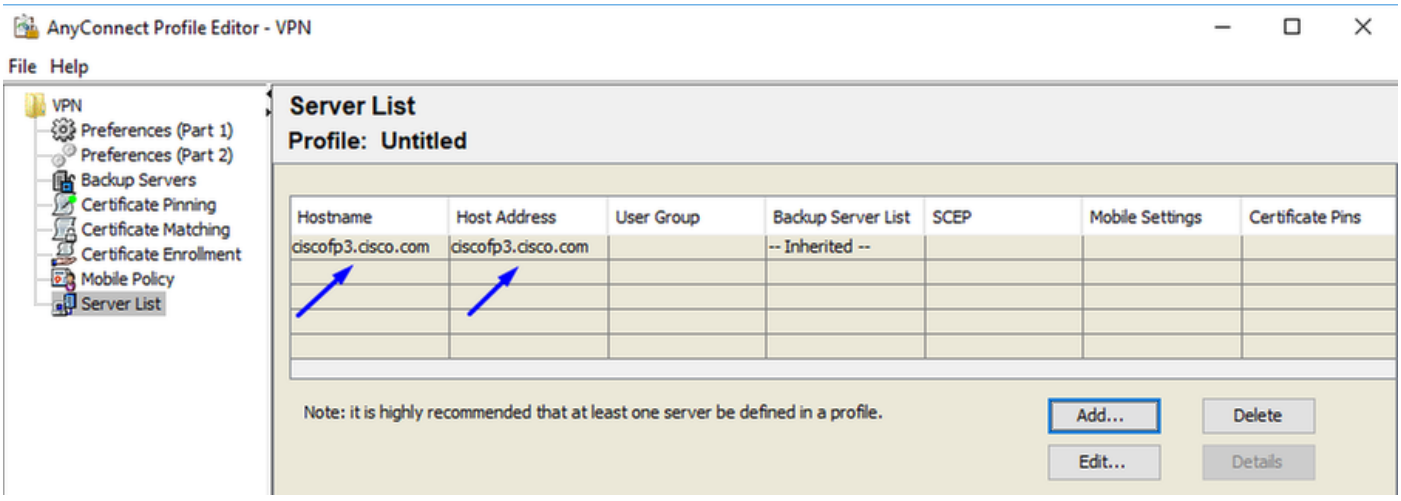


Téléchargez l'image d'AnyConnect + l'éditeur de profil d'AnyConnect et créez un profil .xml

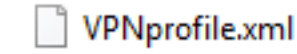
Téléchargez et installez l'éditeur de profil de Cisco AnyConnect

Ouvrez l'éditeur de profil d'AnyConnect
La liste de serveur de clic > cliquent sur Add…
Tapez un **nom d'affichage** et le **FQDN de** vos FTD en dehors de l'adresse IP d'interface. Vous devriez voir des entrées dans la liste de serveur



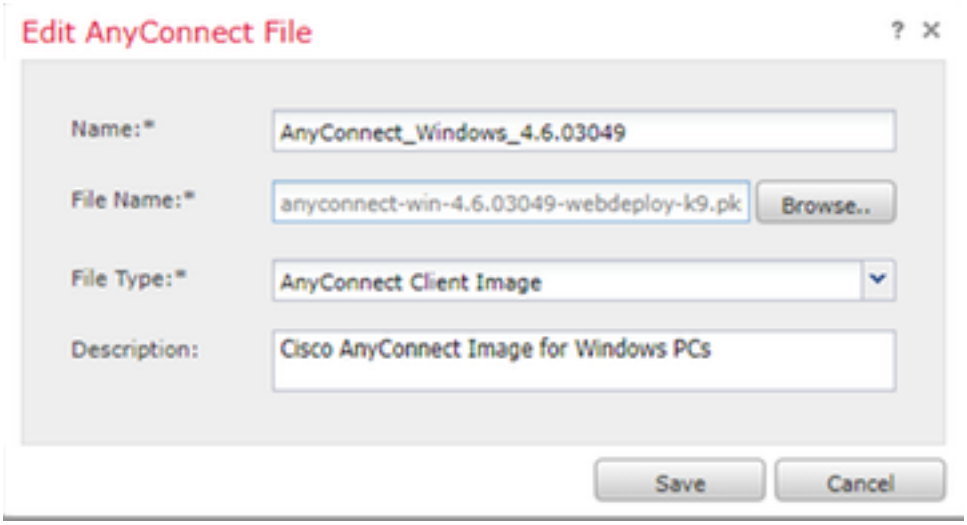


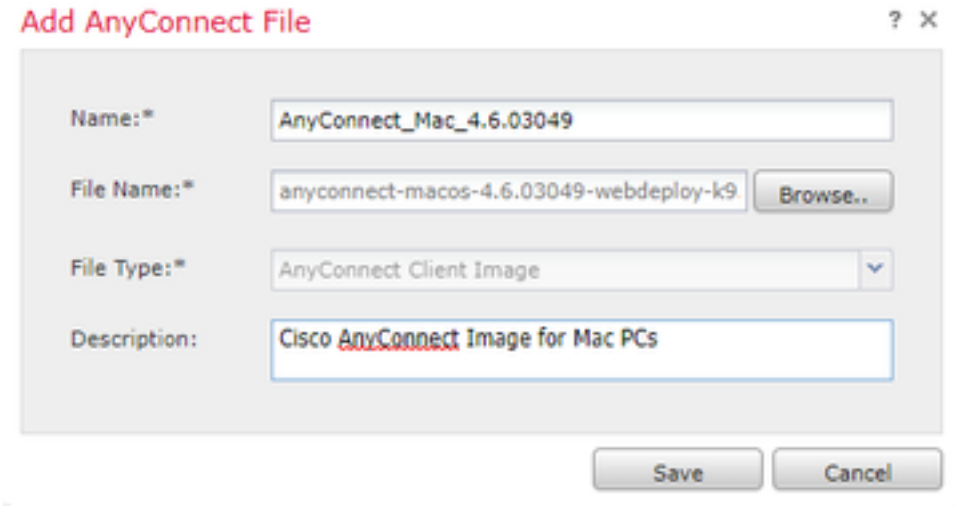
Cliquez sur OK et **fichier > sauvegarde en tant que…**



Images de Windows et Mac .package de téléchargement

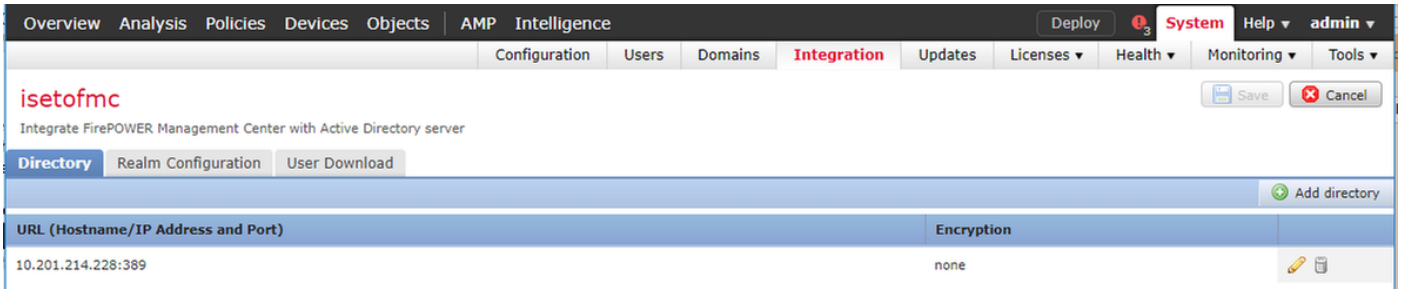
Allez aux **objets** > à la **Gestion d'objet** > au **fichier VPN** > d'**AnyConnect** > cliquent sur Add le **fichier d'AnyConnect**

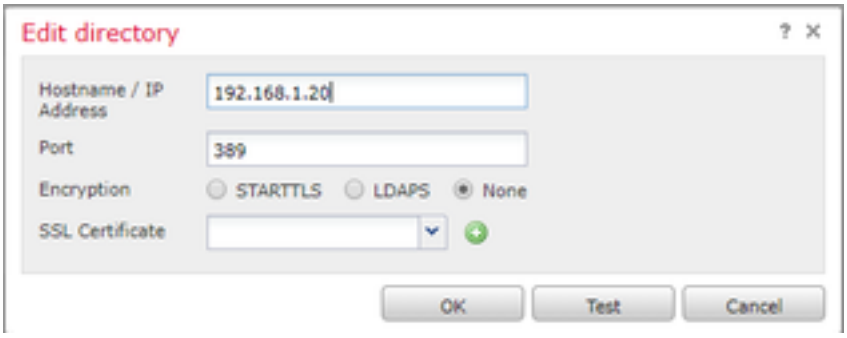




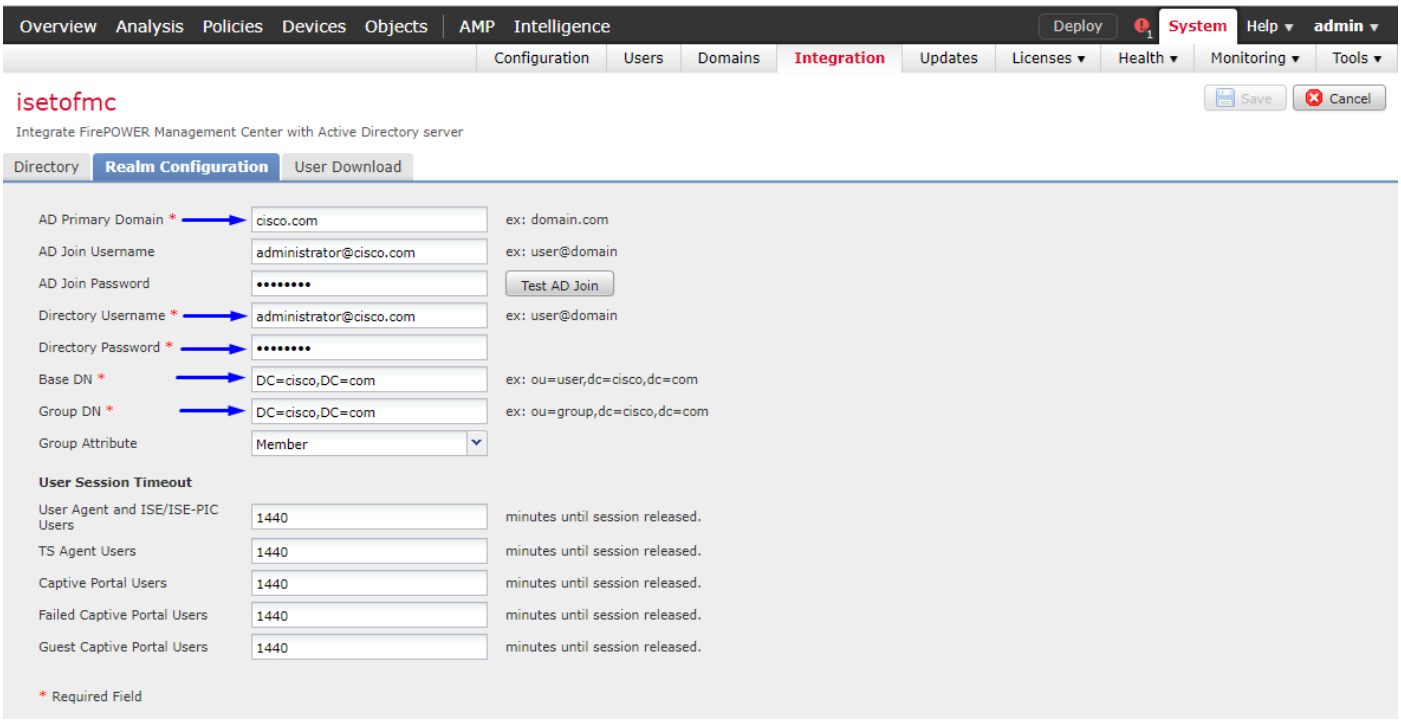
Configurez l'Anyconnect VPN sur FTD (utilisez le certificat de CA de racine)

Procédure de connexion au **centre de Gestion de FirePOWER**
Le système > l'**intégration** > les **royaumes de** clic > cliquent sur New l'**onglet de répertoire de royaume** >> de clic > cliquent sur Add le **répertoire**



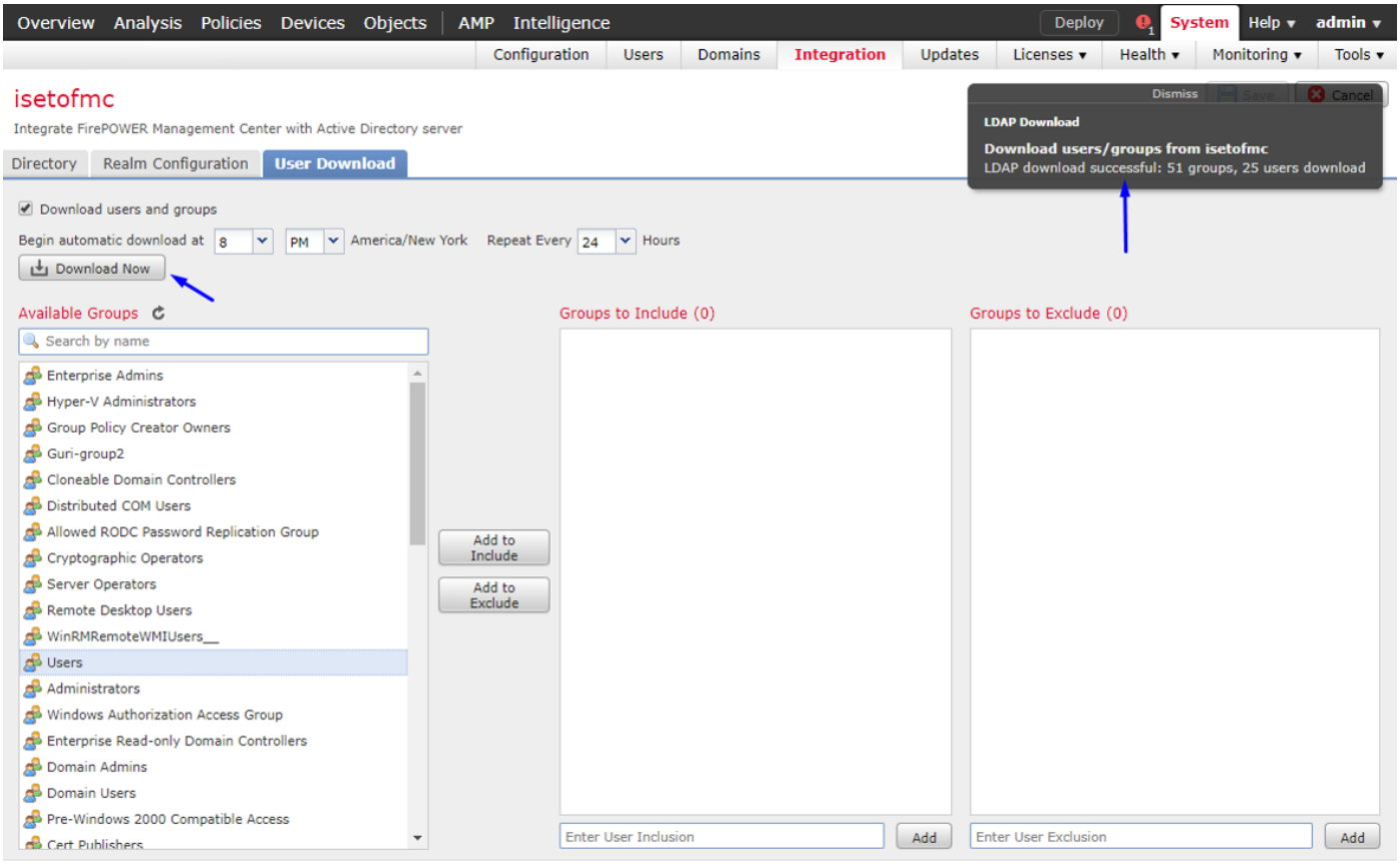


Onglet de **configuration de royaume de** clic - configurez les informations de votre contrôleur de domaine ici

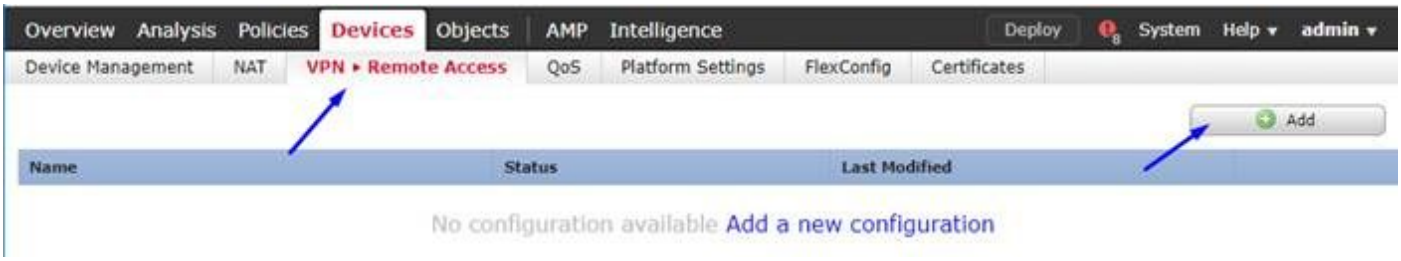


Remarque: Dans l'exemple ci-dessus, un nom d'utilisateur d'AD avec des privilèges « d'admin de domaine » dans le serveur d'AD de Windows est utilisé. Si vous voulez configurer un utilisateur avec des autorisations plus spécifiques et plus minimum pour que le FMC joigne votre domaine de Répertoire actif pour votre configuration de royaume, vous pouvez voir les étapes ici

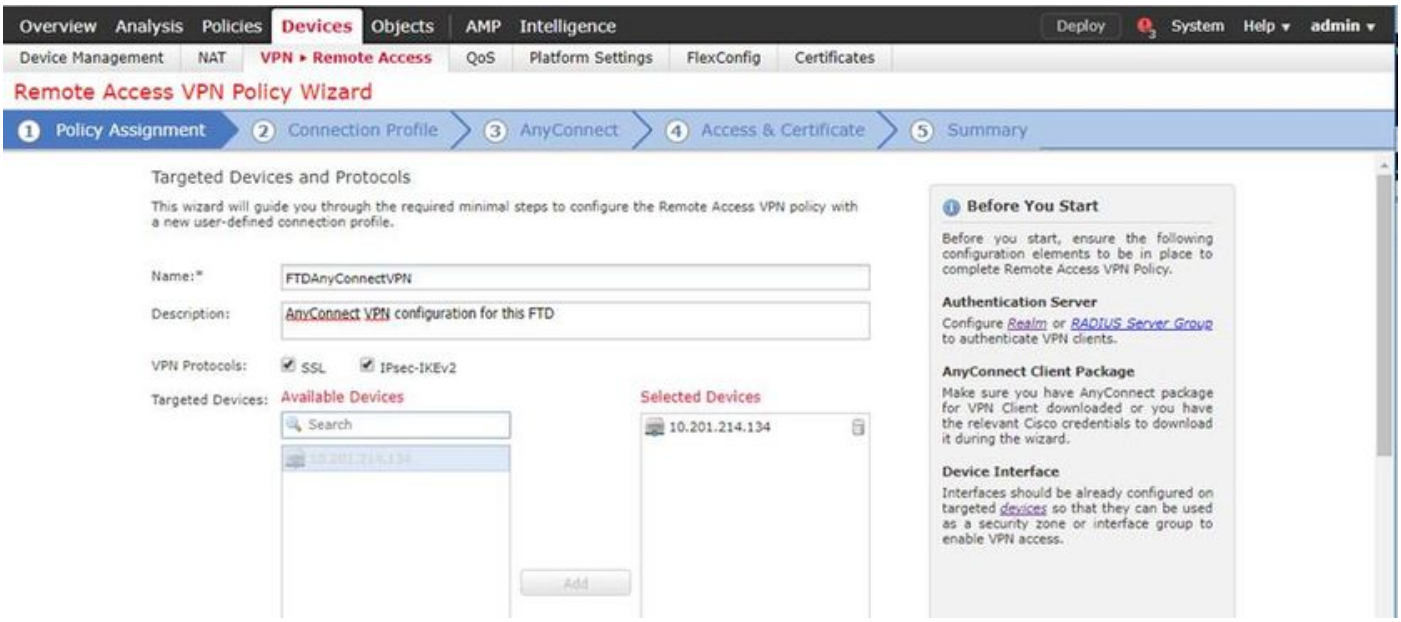
Onglet de **téléchargement d'utilisateur de** clic - assurez-vous que téléchargement d'utilisateur réussit



Les périphériques de clic > le **VPN** > l'**Accès à distance** > cliquent sur Add

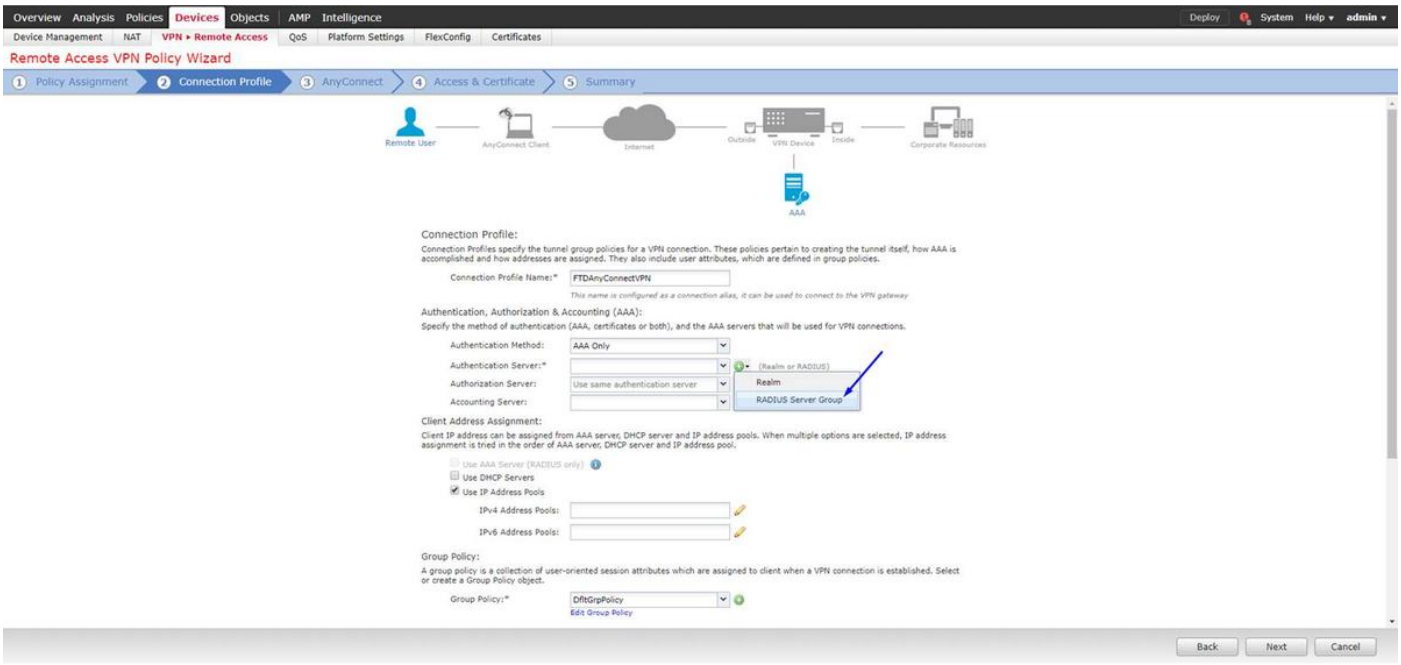


Introduisez un **nom**, **description**, et cliquez sur Add pour sélectionner le périphérique FTD sur lequel vous voulez configurer l'Anyconnect VPN

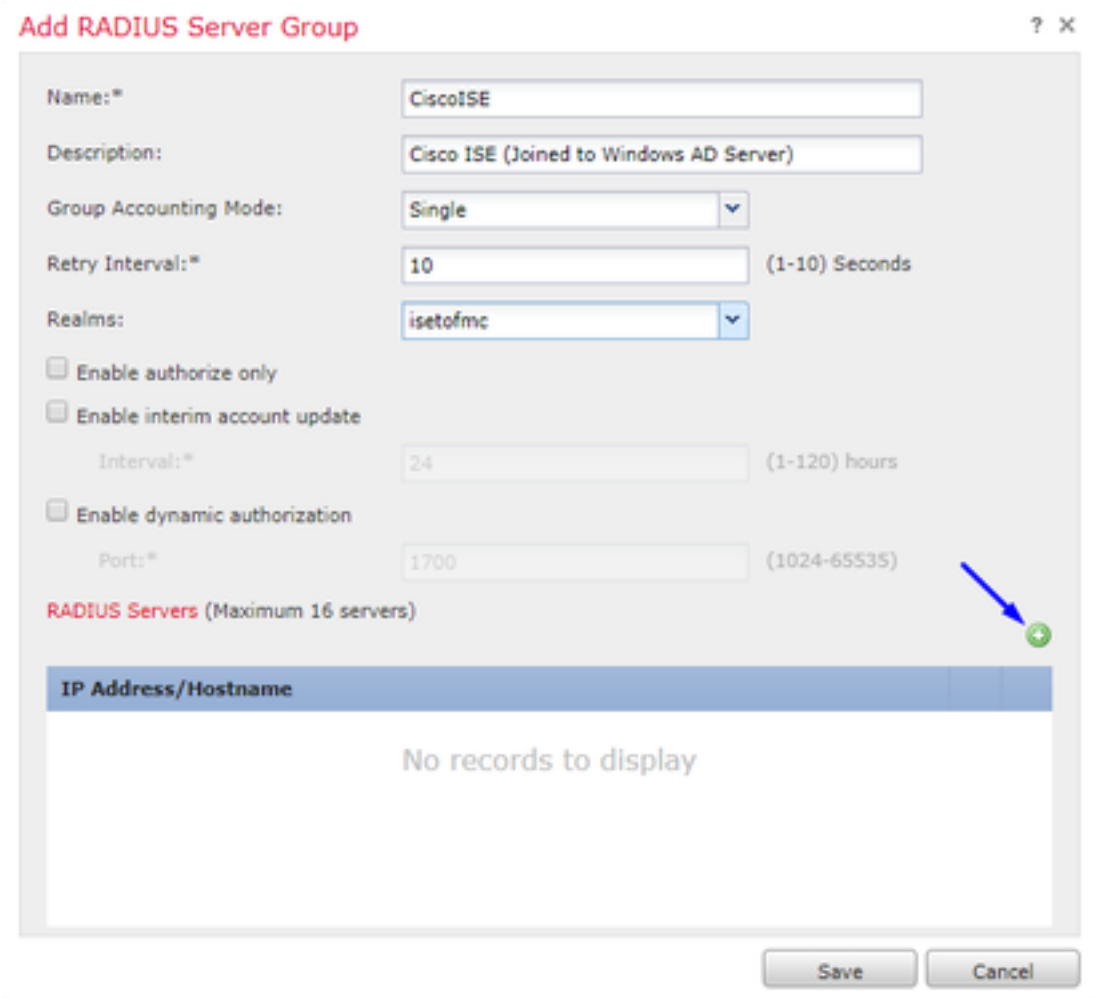


Cliquez sur Add pour le serveur d'authentification et choisissez le **groupe de serveurs de RADIUS**

- ce sera votre RPC de Logiciel Cisco Identity Services Engine (la stratégie entretient le noeud)



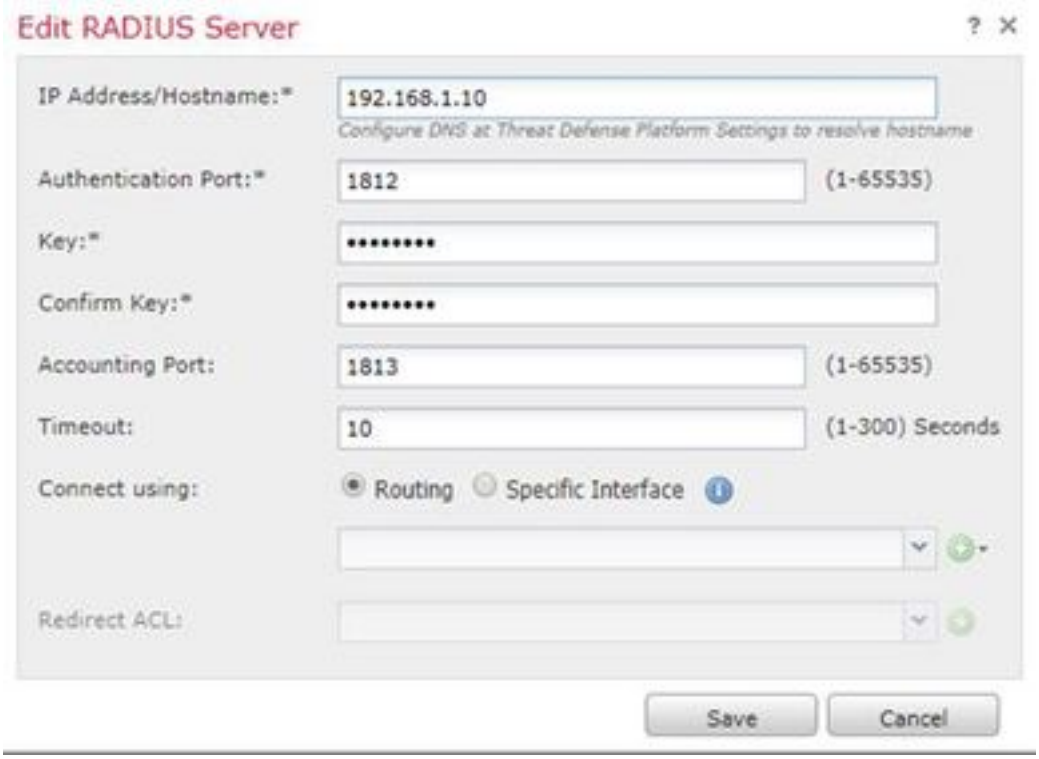
Introduisez un **nom** pour le serveur de RADIUS
Sélectionnez votre **royaume** configuré ci-dessus
Cliquez sur Add



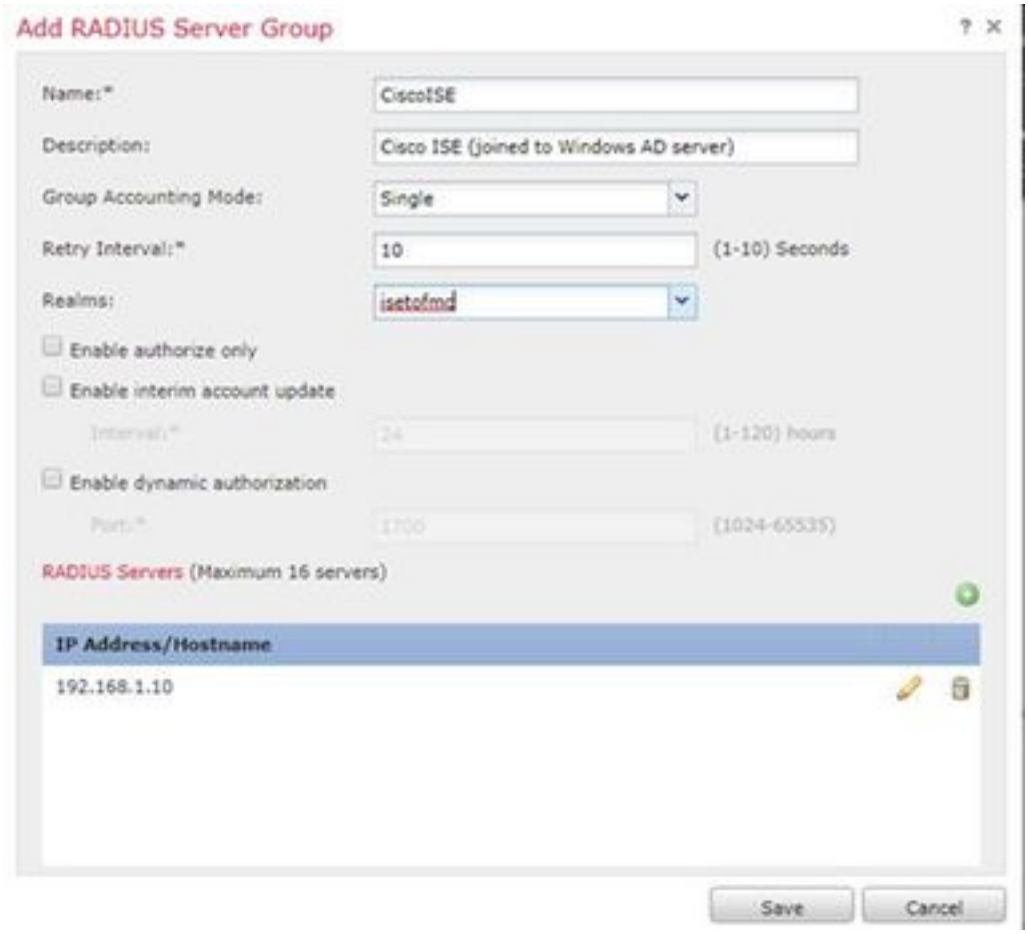
Tapez les informations suivantes pour votre noeud de Cisco ISE :
Adresse IP/adresse Internet : L'adresse IP du RPC de Cisco ISE (noeud de service de stratégie) -

ceci est où les demandes d'authentification disparaîtront
Clé : cisco123
Confirmez la clé : cisco123

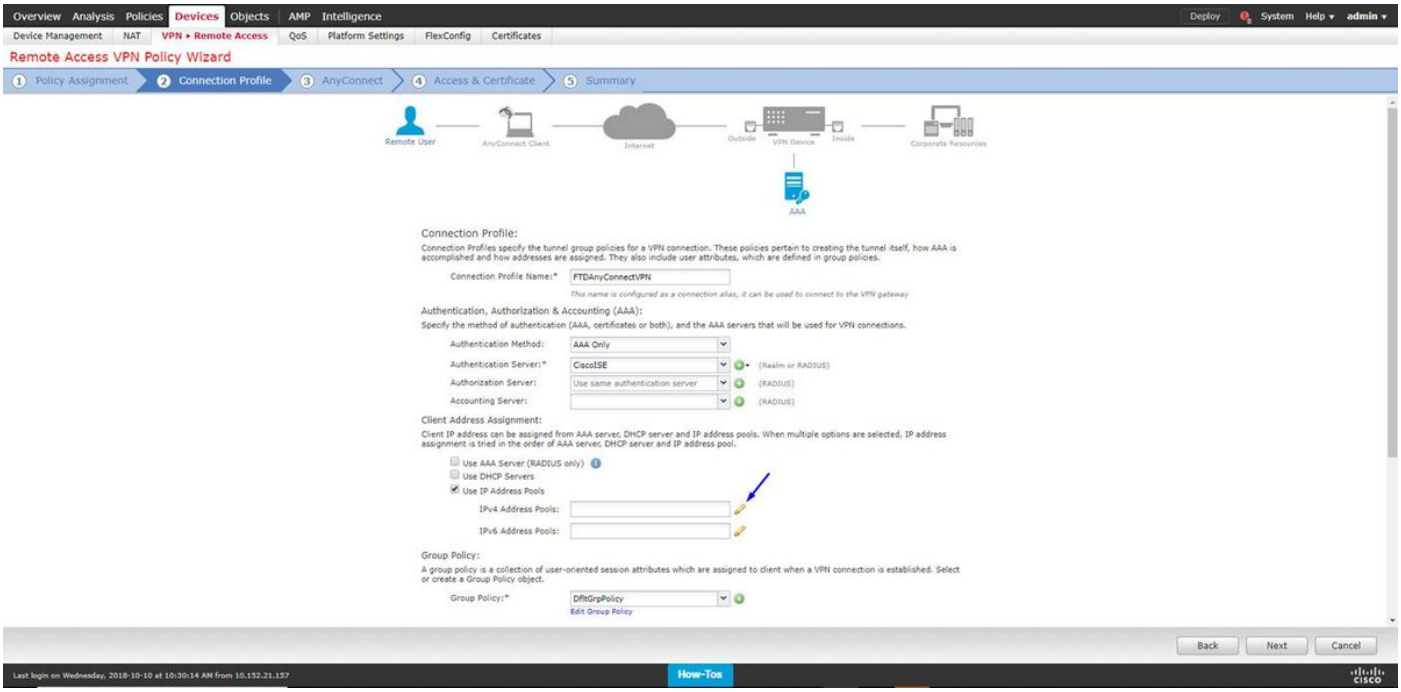
Attention : ce qui précède est votre clé secrète partagée par RADIUS - nous utiliserons cette clé dans une étape postérieure



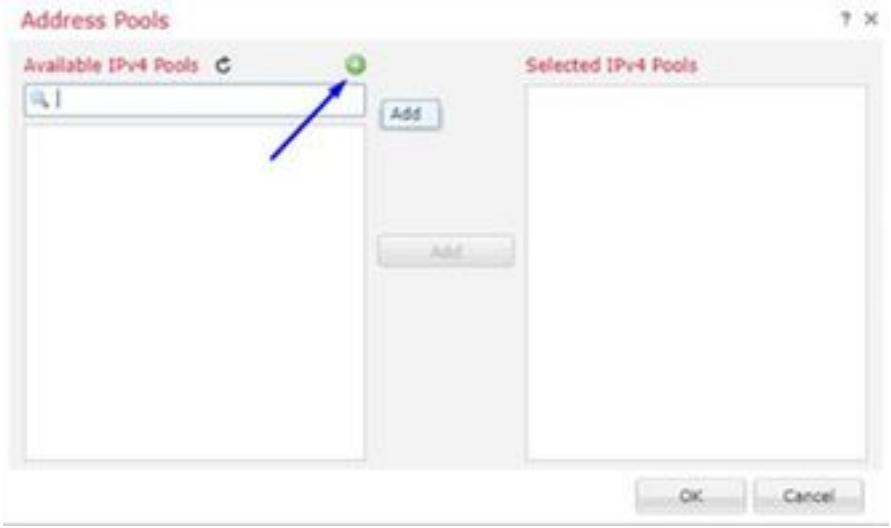
Remarque: Quand les tentatives d'utilisateur final de se connecter au FTD par l'intermédiaire d'AnyConnect VPN, le nom d'utilisateur + mot de passe qu'ils tapent sera envoyé comme demande d'authentification à ce FTD. Le FTD fera suivre à cette demande le noeud RPC de Cisco ISE pour l'authentification (Répertoire actif de viseur de volonté de Cisco ISE puis pour ce nom d'utilisateur et mot de passe, et imposent le contrôle d'accès/accès au réseau selon la condition que nous avons actuellement configurée à Cisco ISE)



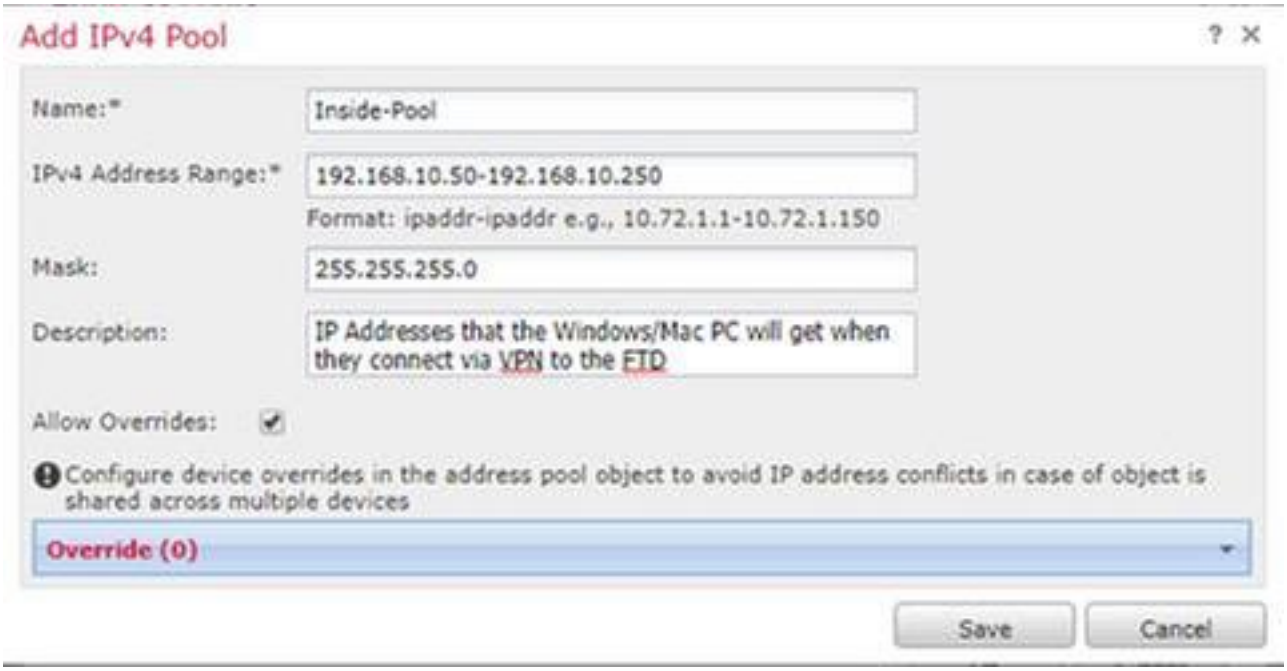
Sauvegarde de clic
Cliquez sur Edit pour le **groupe d'ipv4 addres**



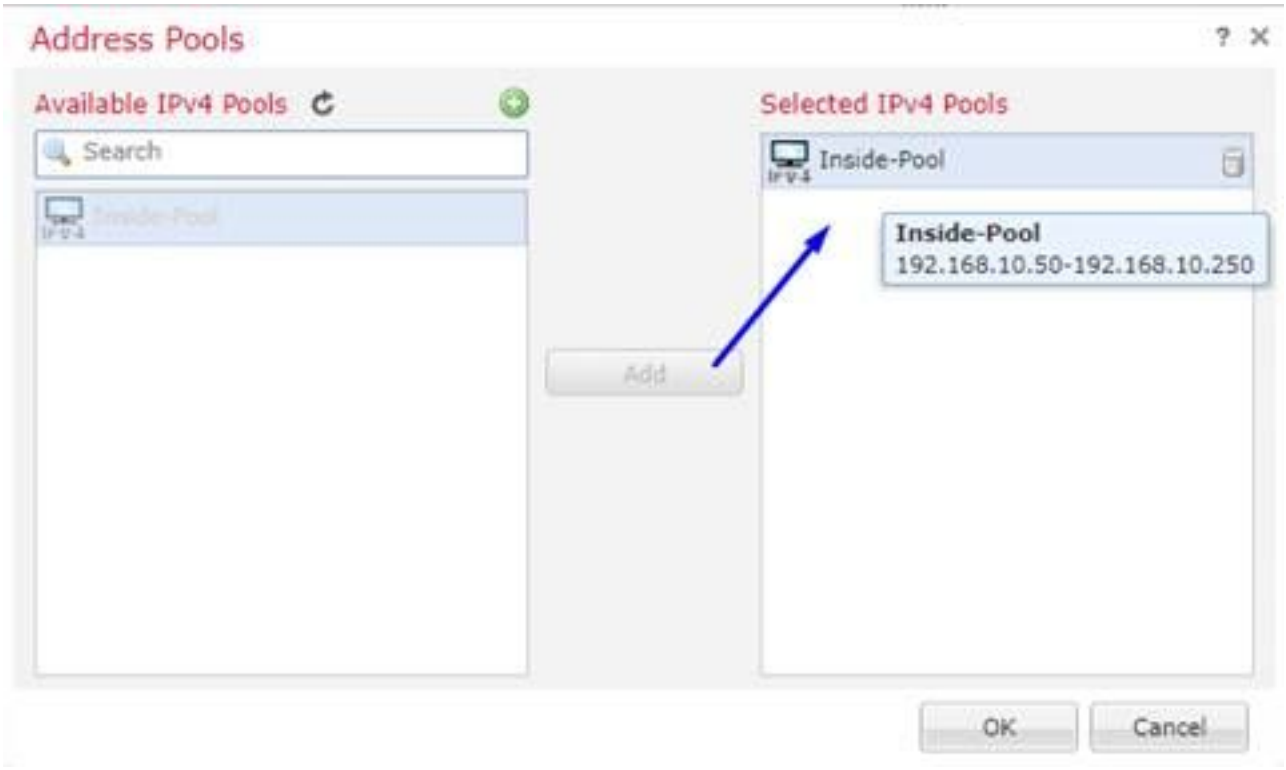
Cliquez sur Add



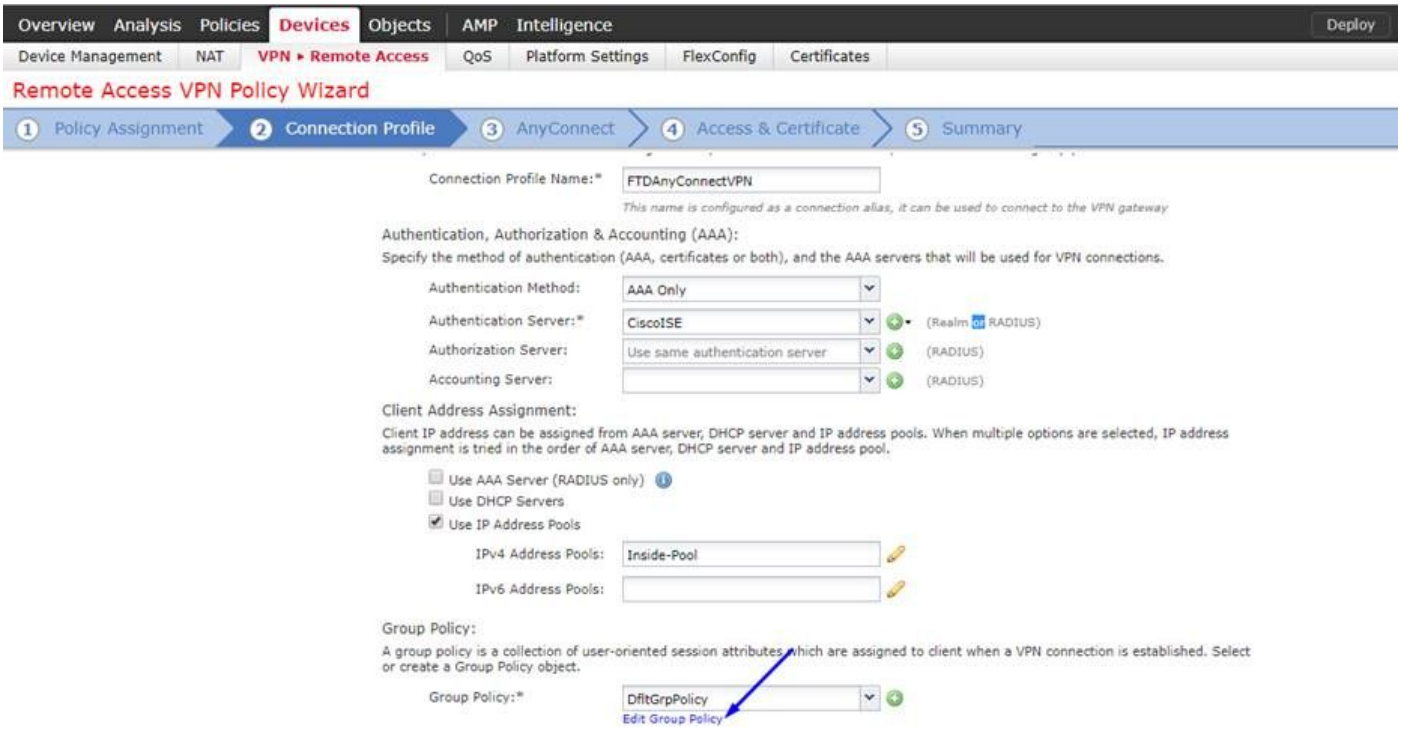
Tapez un **nom**, une **chaîne d'ipv4 addres**, et un **masque de sous-réseau**



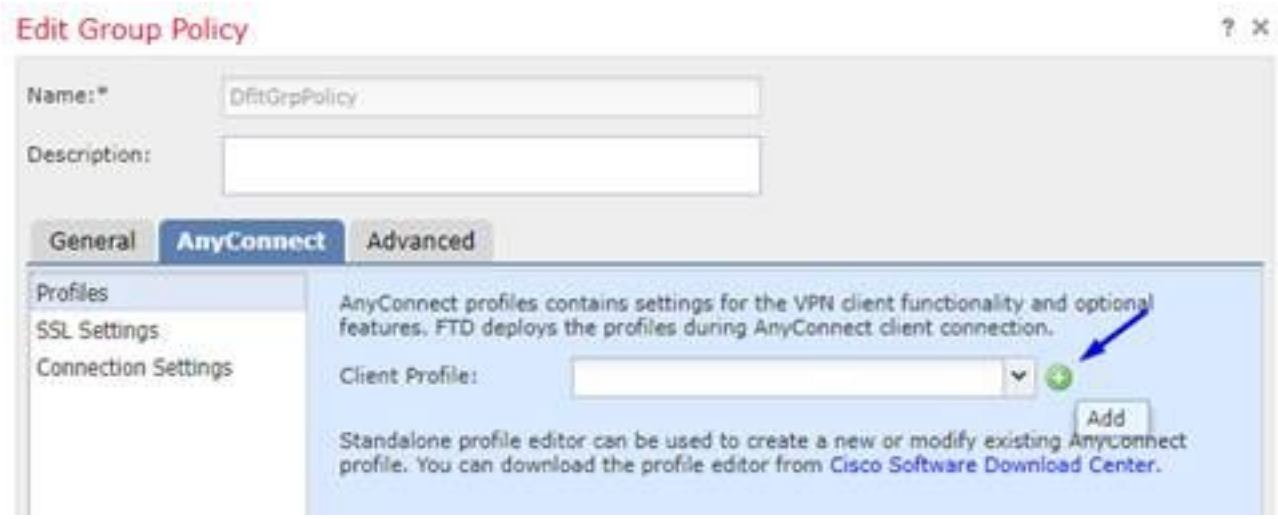
Sélectionnez votre groupe d'adresse IP et cliquez sur l'**ok**



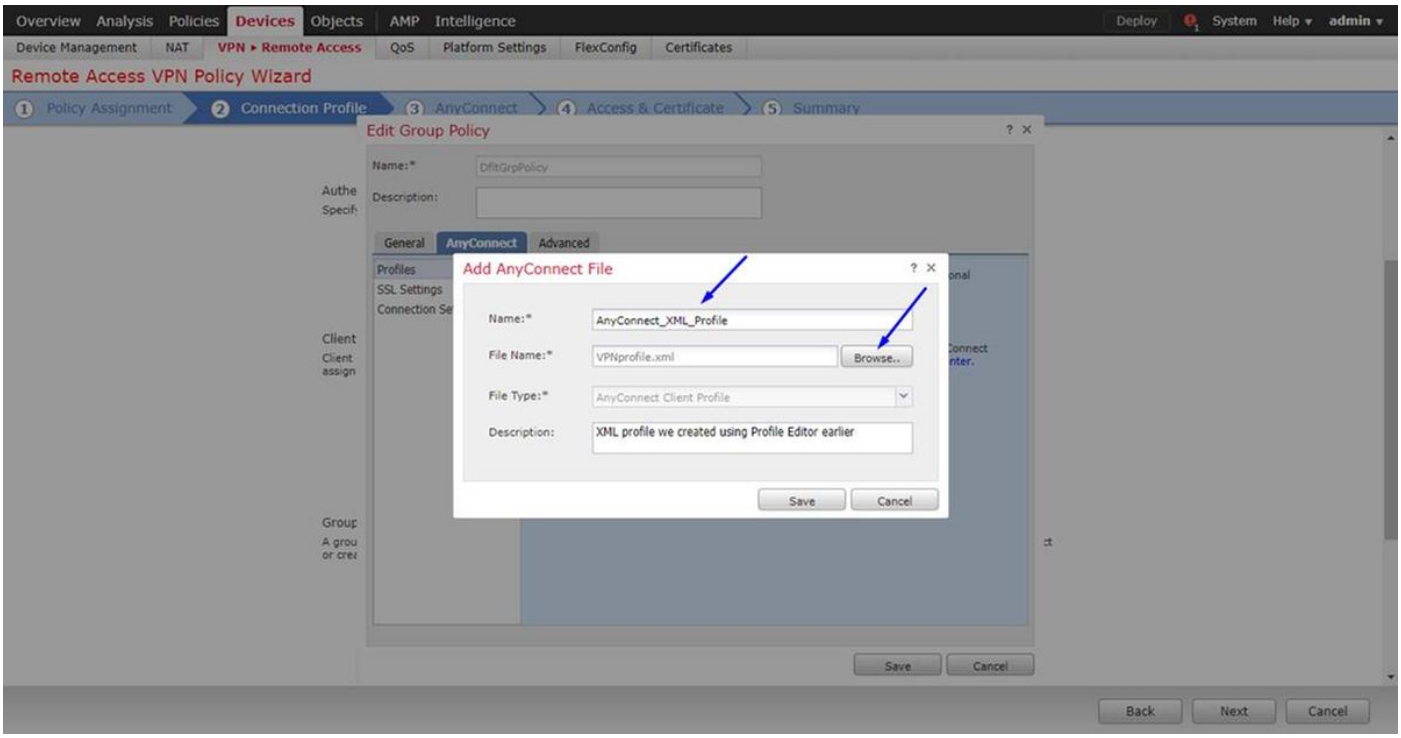
Cliquez sur Edit la **stratégie de groupe**



L'onglet > les **profils d'Anyconnect de** clic > cliquent sur Add

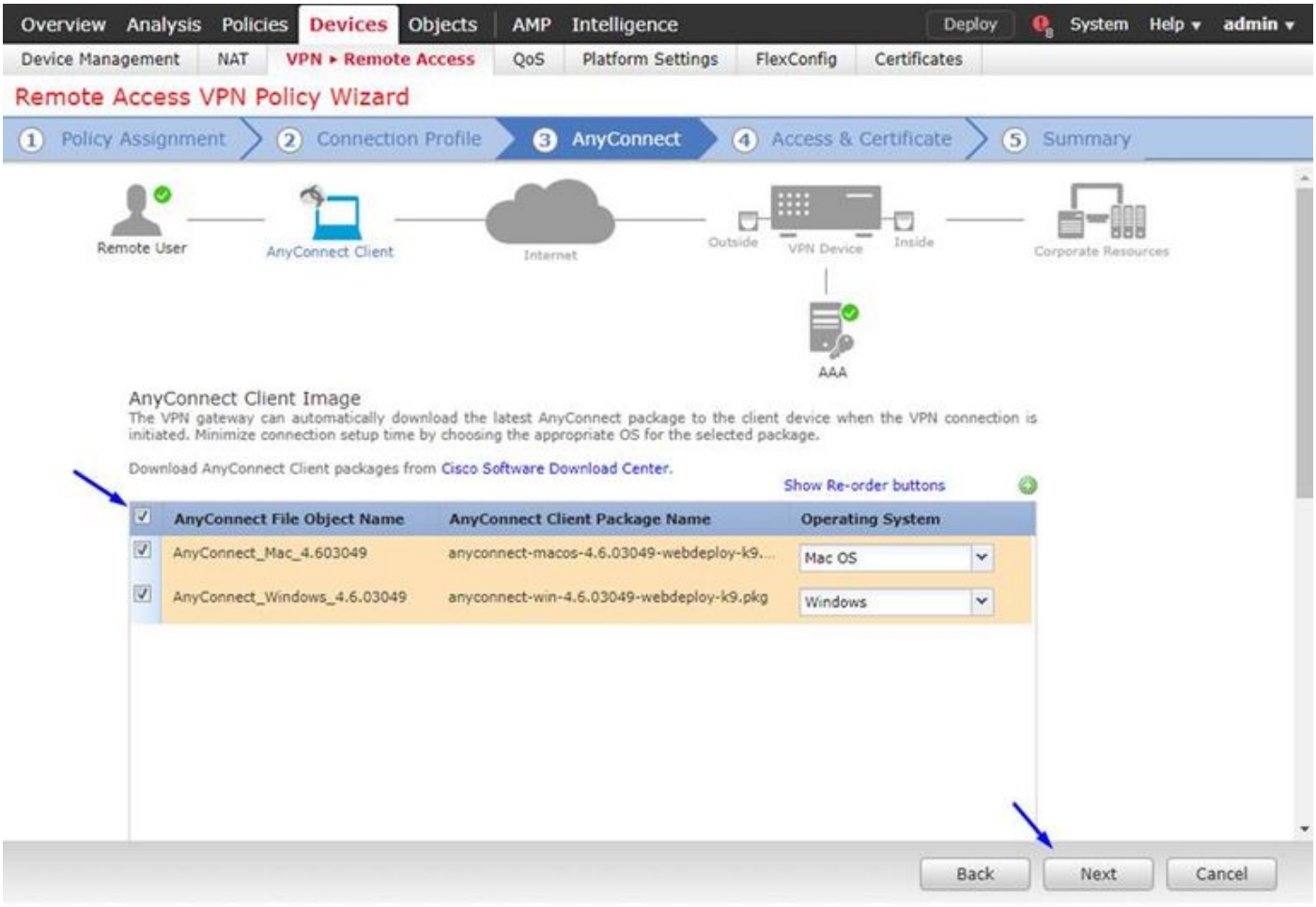


Introduisez un **nom** et le clic **parcourent**… et sélectionnent votre fichier VPNprofile.xml de l'étape 4 ci-dessus

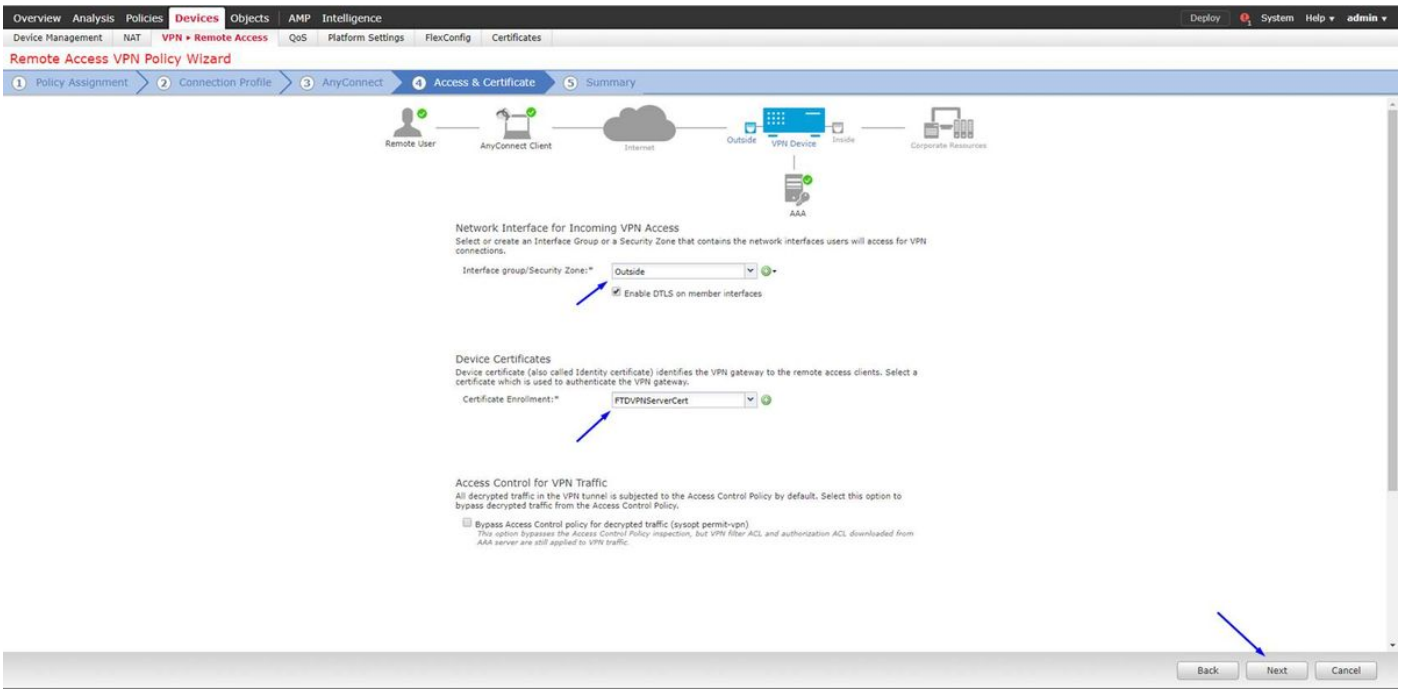


Cliquez sur la **sauvegarde** et cliquez sur Next

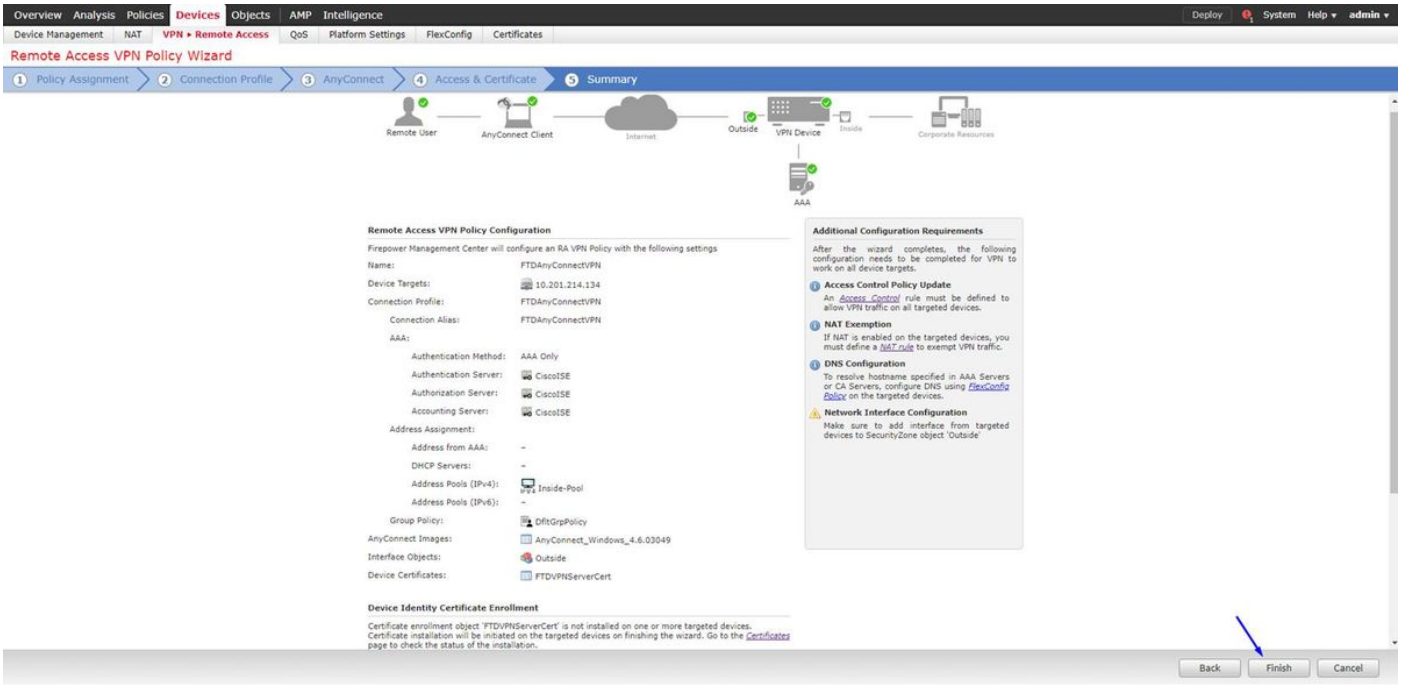
Sélectionnez les cases à cocher pour votre fichier d'AnyConnect Windows/MAC de l'étape 4 ci-dessus



Cliquez sur Next
Zone choisie de **groupe d'interface/Sécurité** comme **extérieur**
Inscription de certificat choisie en tant que votre certificat que nous avons rendu dans l'étape 3 ci-dessus

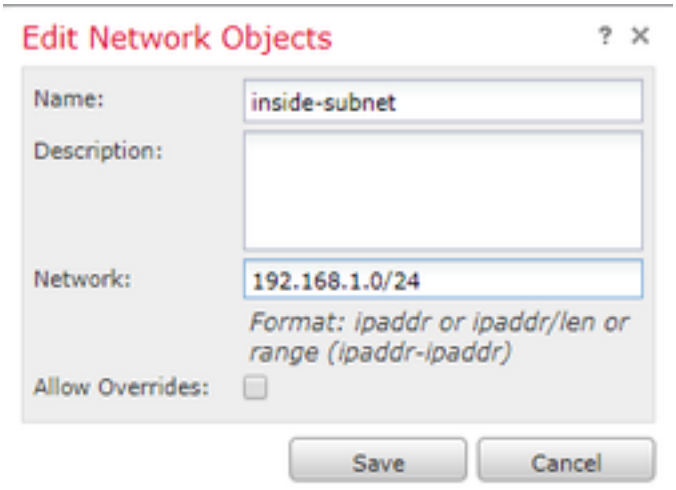


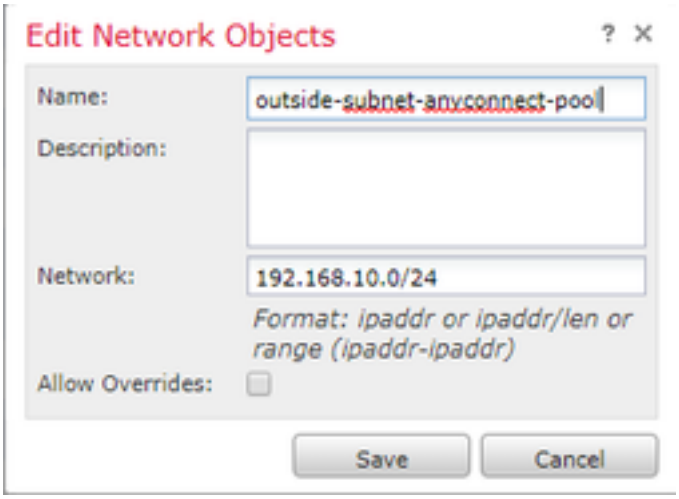
Passez en revue votre configuration et cliquez sur Next

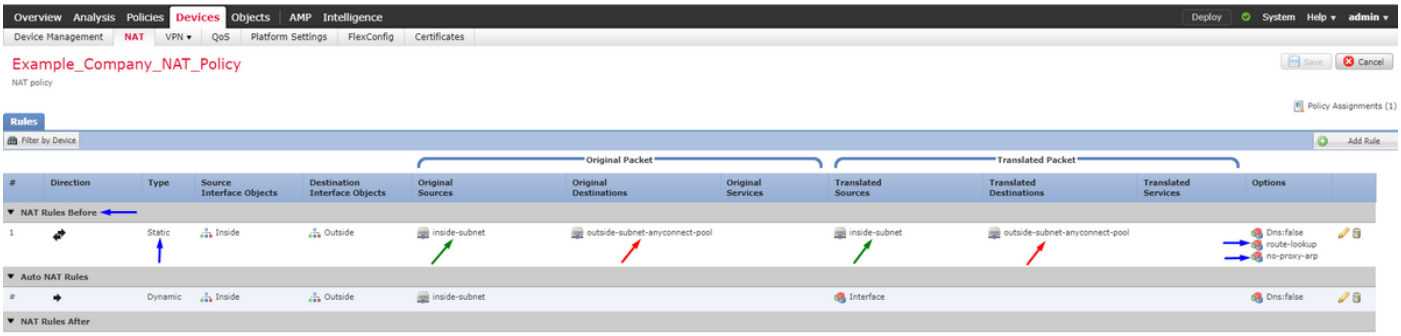


Configurez la règle NAT FTD d'exempter le trafic VPN de NAT puisqu'il sera déchiffré de toute façon et créer la stratégie de contrôle d'accès/règles

Créez une **règle NAT** statique de s'assurer que le trafic VPN n'obtient pas NAT'd (FTD déchiffre déjà les paquets d'AnyConnect pendant qu'ils sont livré à l'interface extérieure, ainsi elle est comme si ce PC est déjà derrière l'interface interne, et ils ont *déjà une* adresse IP privée - nous devons toujours configurer une règle (NO--NAT) Nat-exempte pour ce trafic VPN) :
Allez aux **objets** > cliquent sur Add le **réseau** > cliquent sur Add l'**objet**





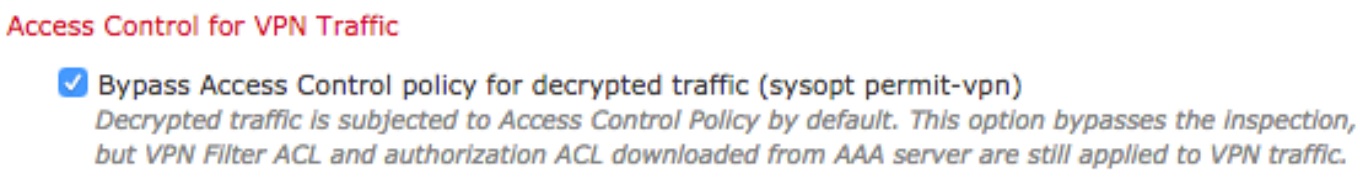


Supplémentaire, vous devez permettre au trafic de données pour entrer après l'utilisateur VPN. Vous avez deux choix pour ceci :

a. Créez permettent ou refusent des règles de permettre ou refuser à des utilisateurs VPN pour accéder à certaines ressources

b. Enable « stratégie de contrôle d'accès de contournement pour le trafic déchiffré » - ceci permet n'importe qui qui peut se connecter avec succès au FTD par l'intermédiaire du contournement ACL VPN et de l'accès que quelque chose derrière le FTD sans aller permettent ou refusent des règles dans la stratégie de contrôle d'accès

Stratégie de contrôle d'accès de contournement d'enable pour le trafic déchiffré dessous : Périphériques > VPN > Accès à distance > profil VPN > interfaces d'Access :

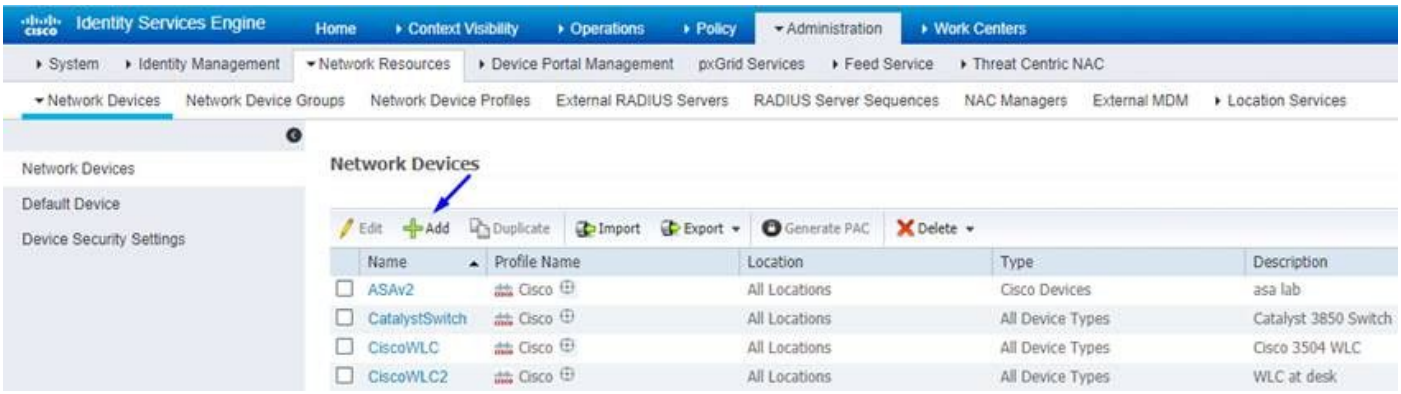


Remarque: Si vous n'activez pas cette option, vous devrez aller aux **stratégies > à la stratégie de contrôle d'accès** et créer permettez les règles pour que les utilisateurs VPN puissent accéder aux choses derrière intérieures ou le dmz

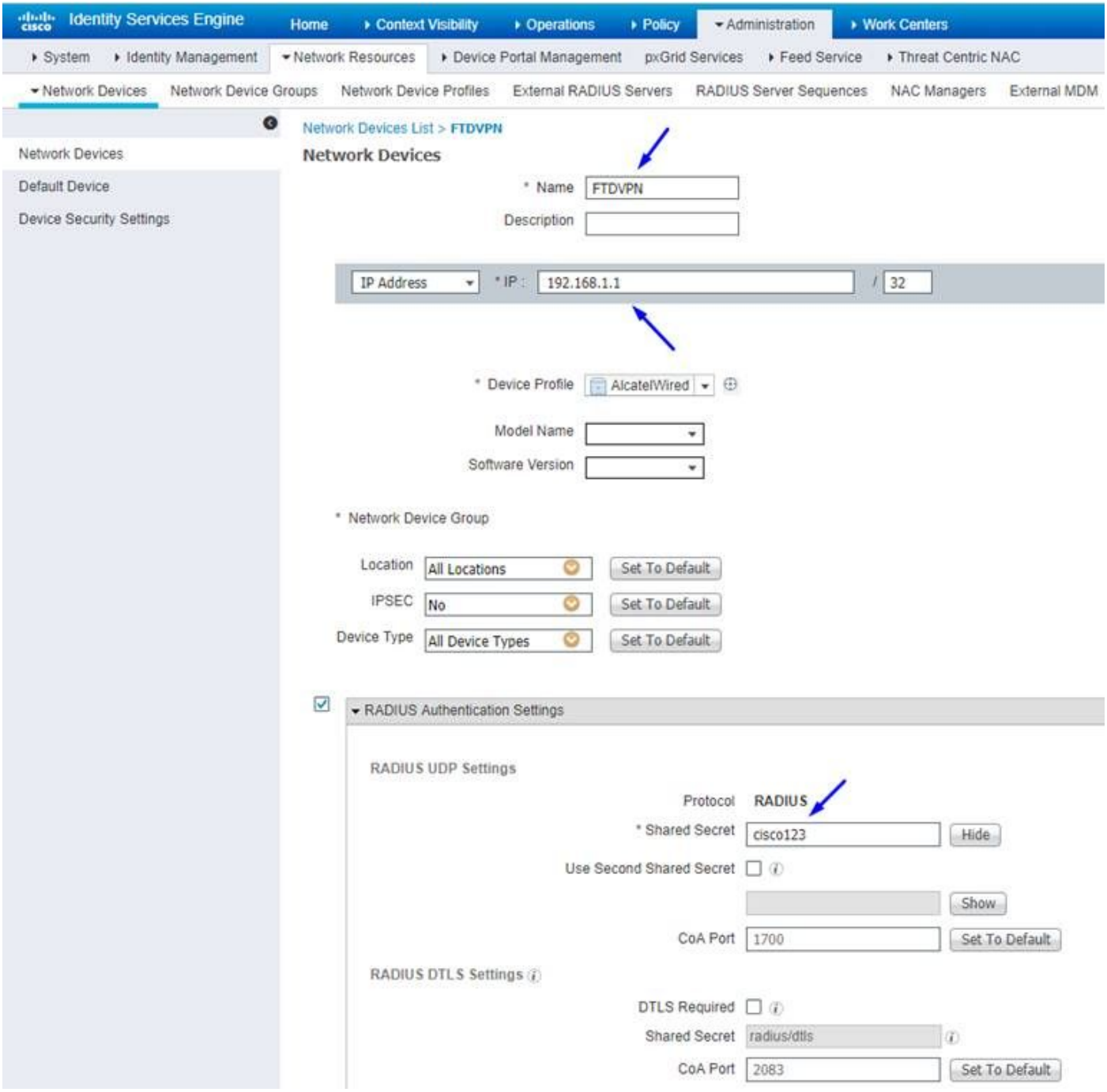
ClickDeployin l'en haut à droite du centre de Gestion de FirePOWER

Ajoutez FTD comme périphérique de réseau et configurez le positionnement de stratégie sur Cisco ISE (le secret partagé par RADIUS d'utilisation)

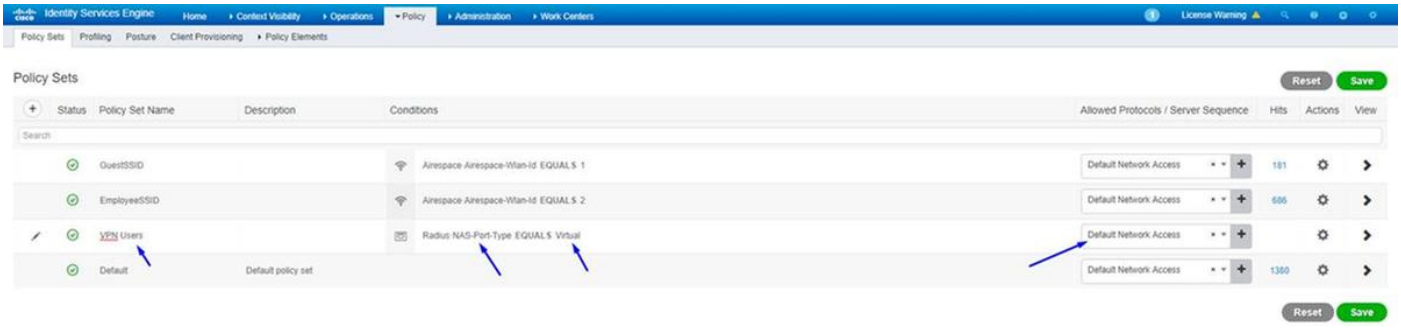
Les périphériques de procédure de connexion au Logiciel Cisco Identity Services Engine et de **gestion** > de **réseau de** clic > cliquent sur Add



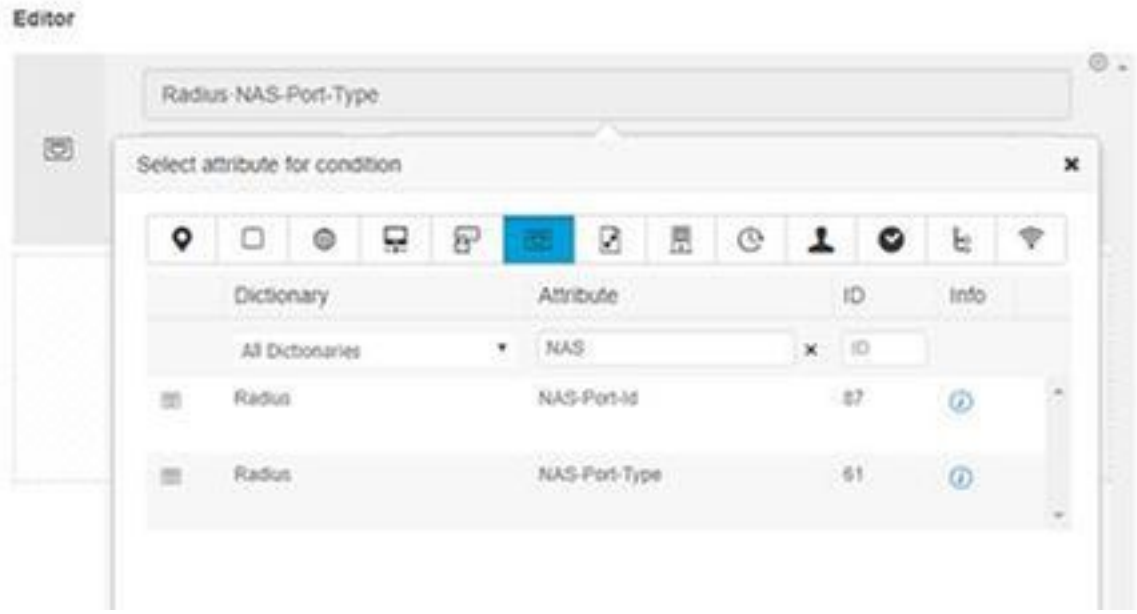
Introduisez un **nom**, tapez l'**adresse IP de** votre FTD, et tapez votre **secret partagé par RADIUS des** étapes ci-dessus
Attention : Ceci doit être l'interface/IP address que le FTD peut atteindre votre Cisco ISE (serveur de RADIUS) c.-à-d. l'interface FTD au-dessus dont votre Cisco ISE peut atteindre le FTD



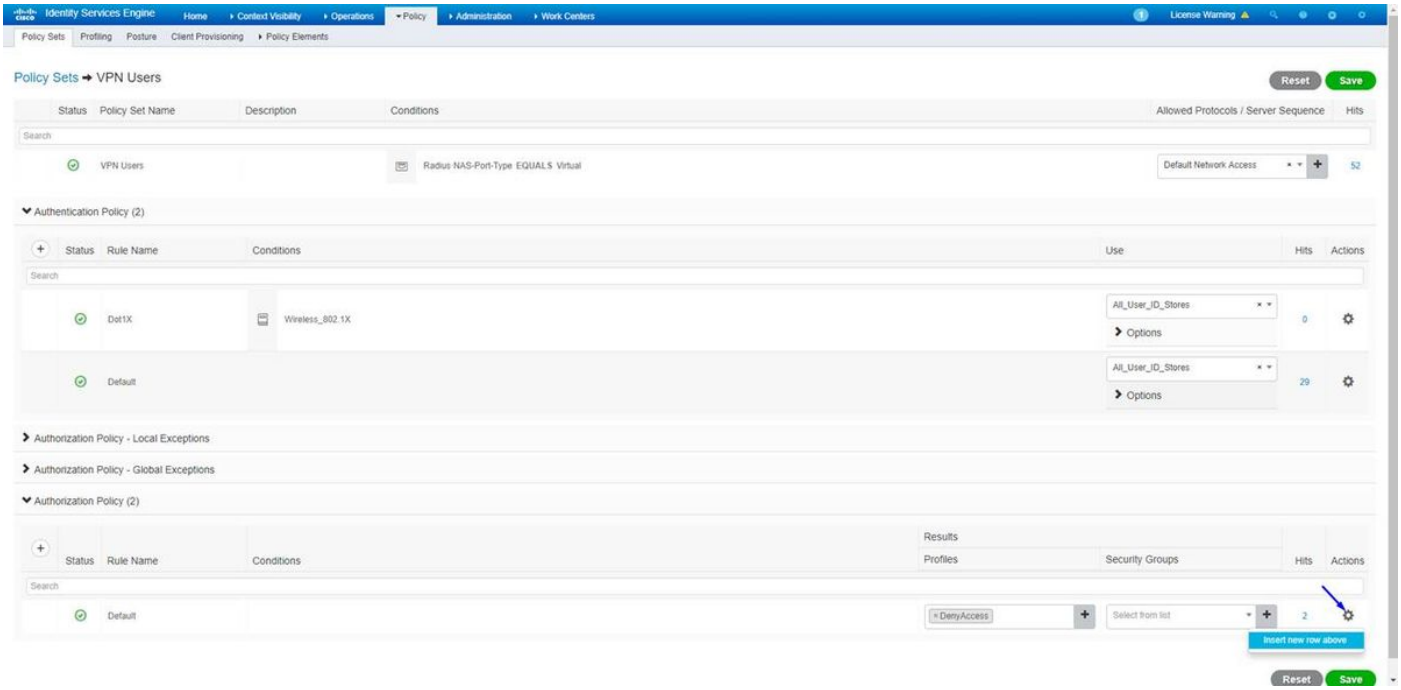
La stratégie de clic > la **stratégie réglée** > créent une **stratégie réglée** pour toutes les demandes d'authentification qui entrent du type suivant :
Le RADIUS-NAs-port-type ÉGALE virtuel
Ceci signifie si des demandes RADIUS qui entrent dans ISE qui ressemblent à des connexions VPN, elles frapperont ce positionnement de stratégie



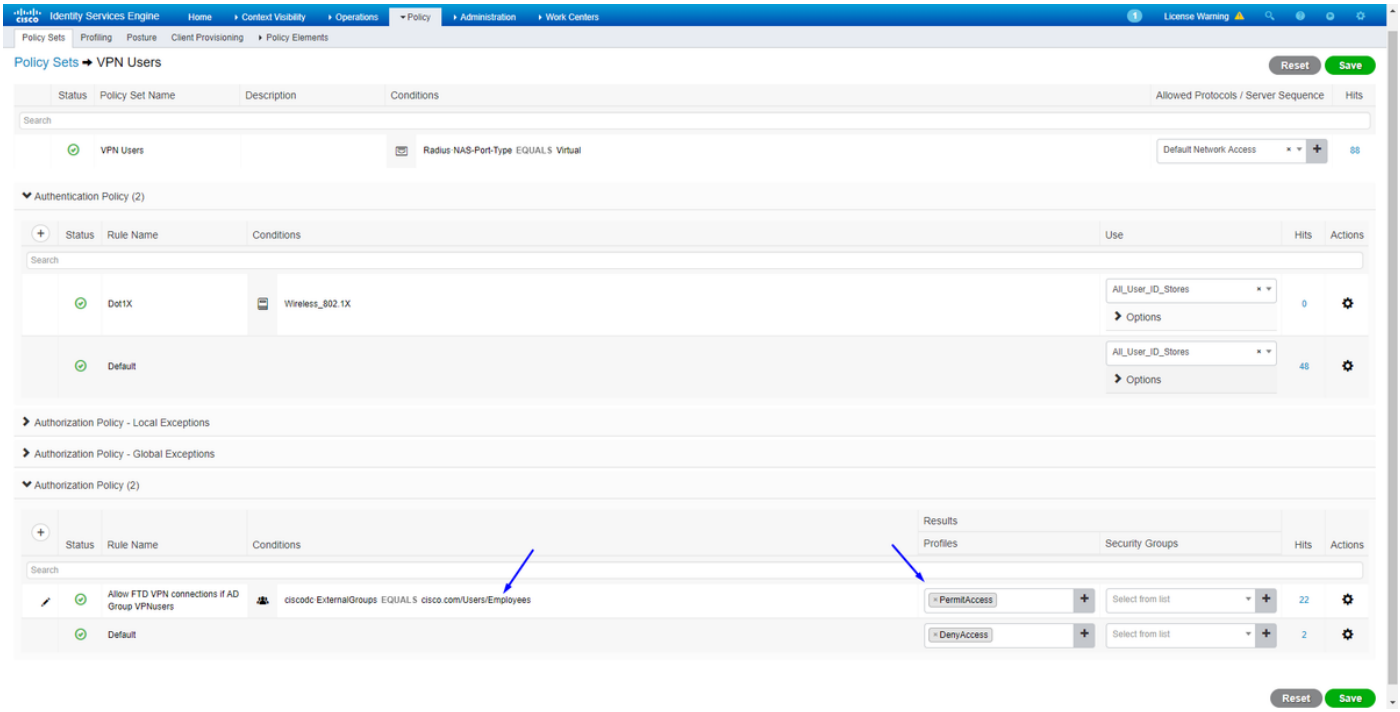
Voici où vous pouvez trouver cette condition à Cisco ISE :



Éditez la **stratégie vous placent** créé ci-dessus
Ajoutez une règle au-dessus de la règle par défaut de bloc de donner le profil d'autorisation de « **Access d'autorisation** » de personnes seulement s'ils sont dans le groupe de Répertoire actif appelé les « **employés** » :

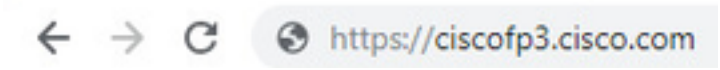


Est ci-dessous à quoi votre règle ressemblera une fois complète

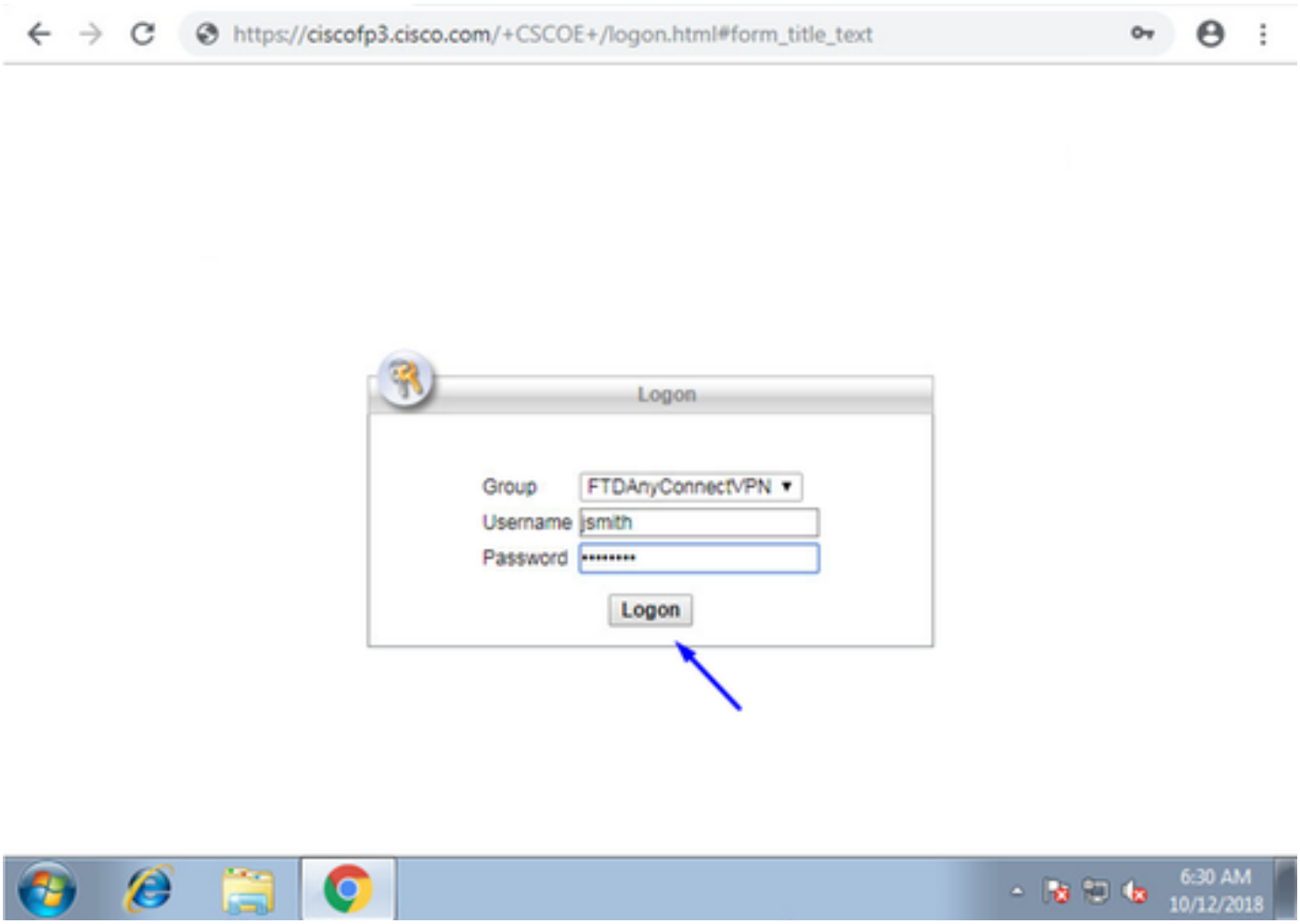


Le téléchargement, installent et se connectent au FTD utilisant l'AnyConnect VPN Client sur l'employé Windows/PC de MAC

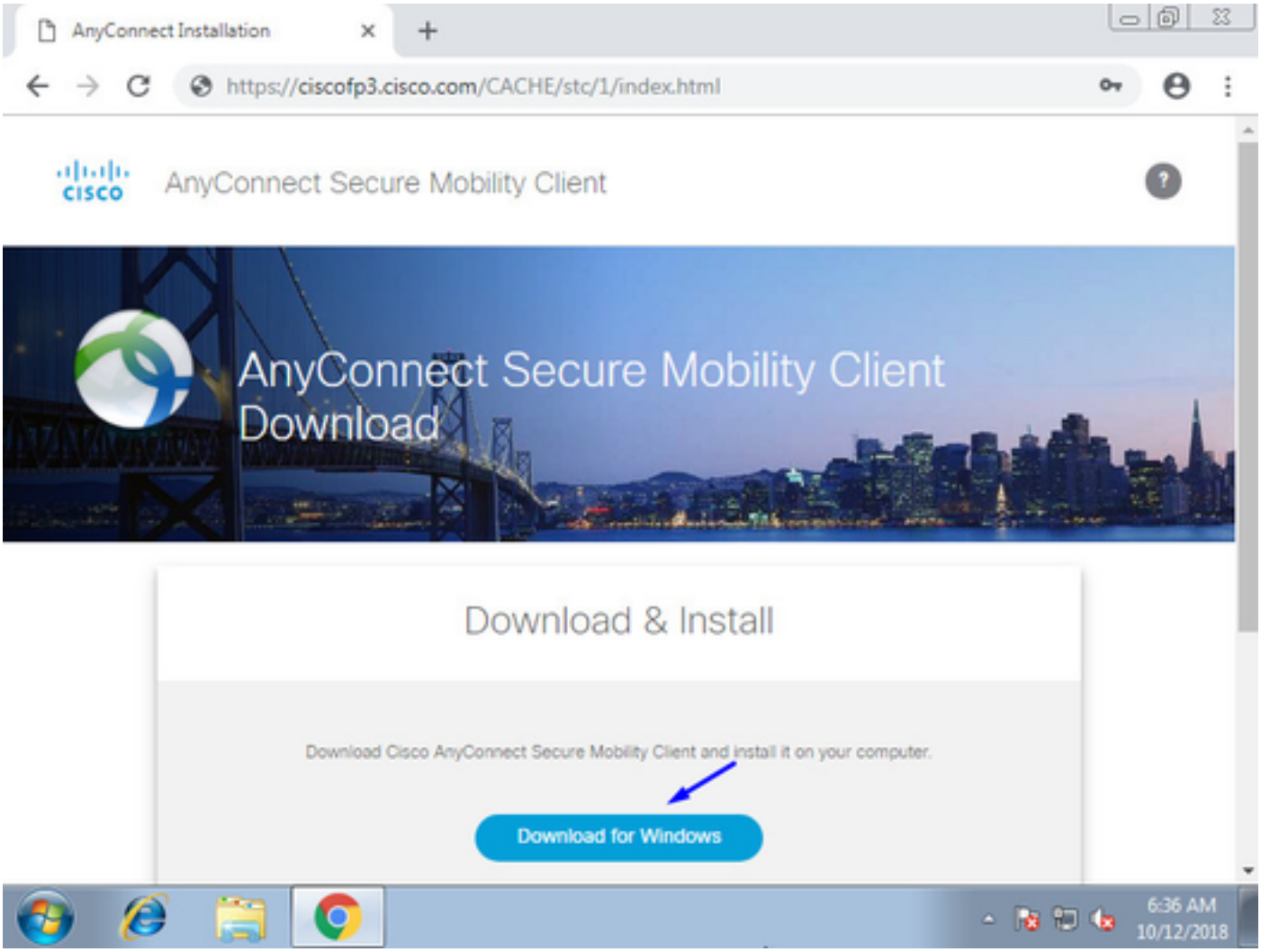
Ouvrez votre navigateur sur l'employé Windows/PC de MAC, et allez à l'adresse d'extérieur de votre FTD en votre navigateur



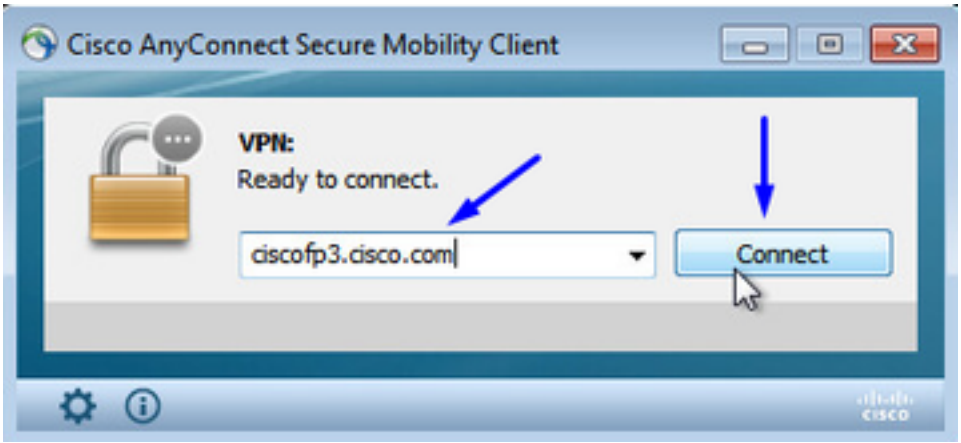
Tapez votre nom d'utilisateur et mot de passe de Répertoire actif



Cliquez sur Download

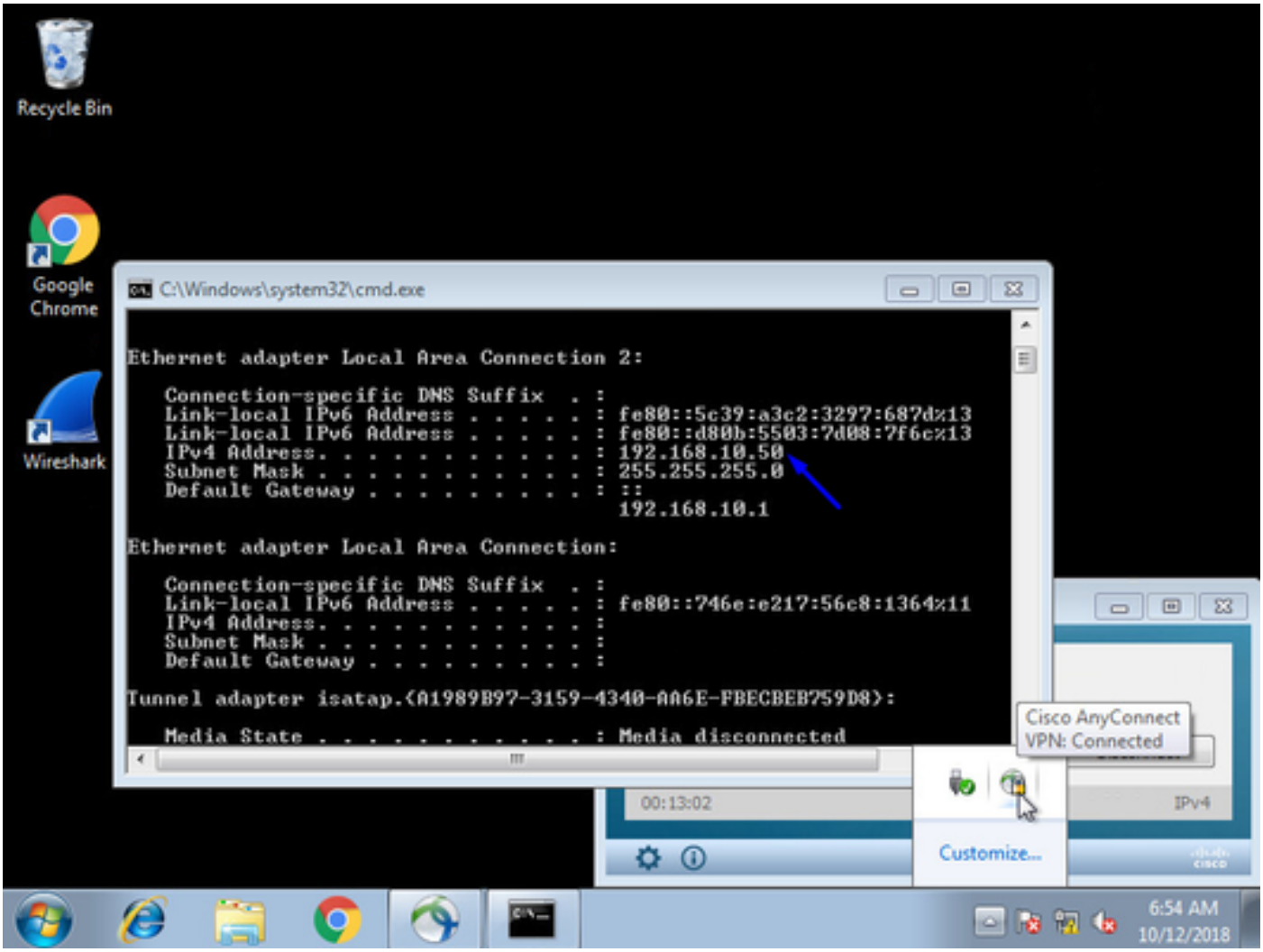


Installez et exécutez le client de mobilité de VPN Secure d'AnyConnect sur le PC de Windows/MAC



Tapez votre nom d'utilisateur et mot de passe de Répertoire actif une fois incité

Vous serez donné une adresse IP du groupe d'adresse IP créé ci-dessus dans l'étape 5 et une passerelle par défaut du .1 dans ce sous-réseau



Vérifiez

FTD

Commandes show

Vérifiez sur FTD que l'utilisateur final est connecté à AnyConnect VPN :

```
> show ip
System IP Addresses:
Interface          Name    IP address  Subnet mask     Method
GigabitEthernet0/0 inside 192.168.1.1 255.255.255.240 CONFIG
GigabitEthernet0/1 outside 203.0.113.2   255.255.255.240 CONFIG
Current IP Addresses:
Interface          Name    IP address  Subnet mask     Method
GigabitEthernet0/0 inside 192.168.1.1 255.255.255.240 CONFIG
GigabitEthernet0/1 outside 203.0.113.2   255.255.255.240 CONFIG

> show vpn-sessiondb detail anyconnect
Session Type: AnyConnect Detailed
Username : jsmith Index : 2
Assigned IP : 192.168.10.50 Public IP : 198.51.100.2
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 : 18458 Bytes Rx : 2706024
Pkts Tx : 12 Pkts Rx : 50799
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy Tunnel Group : FTDAnyConnectVPN
Login Time : 15:08:19 UTC Wed Oct 10 2018
Duration : 0h:30m:11s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0ac9d68a000020005bbe15e3
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:
Tunnel ID : 2.1
Public IP : 198.51.100.2
Encryption : none Hashing : none
TCP Src Port : 53956 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 0 Minutes
Client OS : win
Client OS Ver: 6.1.7601 Service Pack 1
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.6.03049
Bytes Tx : 10572 Bytes Rx : 289
Pkts Tx : 6 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 2.2
Assigned IP : 192.168.10.50 Public IP : 198.51.100.2
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 54634
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.6.03049
Bytes Tx : 7886 Bytes Rx : 2519
Pkts Tx : 6 Pkts Rx : 24
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 2.3
Assigned IP : 192.168.10.50 Public IP : 198.51.100.2
Encryption : AES256 Hashing : SHA1
Ciphersuite : DHE-RSA-AES256-SHA
Encapsulation: DTLSv1.0 UDP Src Port : 61113
UDP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.6.03049
Bytes Tx : 0 Bytes Rx : 2703216
Pkts Tx : 0 Pkts Rx : 50775
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

Une fois que vous allez sur le PC de Windows 7 et cliquez sur le « débranchement » sur le client de Cisco AnyConnect, vous obtiendrez :

```
> show vpn-sessiondb detail anyconnect
INFO: There are presently no active sessions
```

Captures

Comment une capture fonctionnante ressemble à sur l'interface extérieure quand vous frappez se connectent sur le client d'AnyConnect

Exemple :
L'IP du public de l'utilisateur final sera l'IP de public de leur routeur à la maison par exemple

```
ciscofp3# capture capin interface outside trace detail trace-count 100 match ip any host
<enduser'sPublicIPAddress>
<now hit Connect on AnyConnect Client from employee PC>
ciscofp3# show cap
capture capin type raw-data trace detail trace-count 100 interface outside [Buffer Full - 524153
bytes]
match ip any host 198.51.100.2
```

Visualisez les paquets qui ont été livré à l'interface extérieure du FTD du PC de l'utilisateur final de s'assurer qu'ils arrivent sur notre interface extérieure FTD :

```
ciscofp3# capture capin interface outside trace detail trace-count 100 match ip any host
<enduser'sPublicIPAddress>
<now hit Connect on AnyConnect Client from employee PC>
ciscofp3# show cap
capture capin type raw-data trace detail trace-count 100 interface outside [Buffer Full - 524153
bytes]
match ip any host 198.51.100.2
```

Visualisez les détails de ce qui arrive à ce paquet qui entre de l'utilisateur final dans le Pare-feu

```
ciscofp3# show cap capin packet-number 1 trace detail
2943 packets captured

1: 17:05:56.580994 006b.f1e7.6c5e 000c.294f.ac84 0x0800 Length: 66
198.51.100.2.55928 > 203.0.113.2.443: S [tcp sum ok] 2933933902:2933933902(0) win 8192 <mss
1460,nop,wscale 8,nop,nop,sackOK> (DF) (ttl 127, id 31008)

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x2ace13beec90, priority=13, domain=capture, deny=false
hits=2737, user_data=0x2ace1232af40, cs_id=0x0, l3_type=0x0
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0000.0000.0000
input_ifc=outside, output_ifc=any

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
```

```
Forward Flow based lookup yields rule:
in id=0x2ace107c8480, priority=1, domain=permit, deny=false
hits=183698, user_data=0x0, cs_id=0x0, l3_type=0x8
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0100.0000.0000
input_ifc=outside, output_ifc=any

Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 203.0.113.2 using egress ifc identity

Phase: 4
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in id=0x2ace1199f680, priority=119, domain=permit, deny=false
hits=68, user_data=0x0, cs_id=0x0, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=443, tag=any, dscp=0x0
input_ifc=outside, output_ifc=identity

Phase: 5
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x2ace1199efd0, priority=8, domain=conn-set, deny=false
hits=68, user_data=0x2ace1199e5d0, cs_id=0x0, reverse, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=443, tag=any, dscp=0x0
input_ifc=outside, output_ifc=identity

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x2ace0fa81330, priority=0, domain=nat-per-session, deny=false
hits=178978, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x2ace107cdb00, priority=0, domain=inspect-ip-options, deny=true
hits=174376, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
```

```
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside, output_ifc=any

Phase: 8
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x2ace107c90c0, priority=208, domain=cluster-redirect, deny=false
hits=78, user_data=0x0, cs_id=0x0, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside, output_ifc=identity

Phase: 9
Type: TCP-MODULE
Subtype: webvpn
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x2ace1199df20, priority=13, domain=soft-np-tcp-module, deny=false
hits=58, user_data=0x2ace061efb00, cs_id=0x0, reverse, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=443, tag=any, dscp=0x0
input_ifc=outside, output_ifc=identity

Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x2ace11d455e0, priority=13, domain=ipsec-tunnel-flow, deny=true
hits=87214, user_data=0x0, cs_id=0x0, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside, output_ifc=any

Phase: 11
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x2ace11da7000, priority=13, domain=capture, deny=false
hits=635, user_data=0x2ace1232af40, cs_id=0x2ace11f21620, reverse, flags=0x0, protocol=0
src ip/id=198.51.100.2, mask=255.255.255.255, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside, output_ifc=any

Phase: 12
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
out id=0x2ace10691780, priority=13, domain=capture, deny=false
```

```
hits=9, user_data=0x2ace1232af40, cs_id=0x2ace11f21620, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=198.51.100.2, mask=255.255.255.255, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=outside

Phase: 13
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 87237, packet dispatched to next module
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_tcp_mod
snp_fp_adjacency
snp_fp_fragment
snp_fp_drop

Module information for reverse flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow

1 packet shown
ciscofp3#
```

Copiez la capture sur disk0 : de votre FTD. Vous pouvez alors le télécharger par l'intermédiaire du SCP, du FTP, ou du TFTP

(ou de l'âme centrale de Gestion de FirePOWER UI **>>** système **>>** santés **>>** moniteur de santés **>>** dépannage avancé de clic **>>** cliquent sur Download l'onglet de fichier)

```
ciscofp3# copy /pcap capture:capin disk0:/capin.pcap
Source capture name [capin]? <hit Enter>
Destination filename [capin.pcap]? <hit Enter>
!!!!!!!!!!!!!!!
207 packets copied in 0.0 secs

ciscofp3# dir
Directory of disk0:/
122 -rwx 198 05:13:44 Apr 01 2018 lina_phase1.log
49 drwx 4096 21:42:20 Jun 30 2018 log
53 drwx 4096 21:42:36 Jun 30 2018 coredumpinfo
110 drwx 4096 14:59:51 Oct 10 2018 csm
123 -rwx 21074 01:26:44 Oct 10 2018 backup-config.cfg
124 -rwx 21074 01:26:44 Oct 10 2018 startup-config
125 -rwx 20354 01:26:44 Oct 10 2018 modified-config.cfg
160 -rwx 60124 17:06:22 Oct 10 2018 capin.pcap

ciscofp3# copy disk0:/capin.pcap tftp:/
Source filename [capin.pcap]? <hit Enter>
```

```
Address or name of remote host []? 192.168.1.25 (your TFTP server IP address (your PC if using
tftpd32 or Solarwinds TFTP Server))
Destination filename [capin.pcap]? <hit Enter>
113645 bytes copied in 21.800 secs (5411 bytes/sec)
ciscofp3#

(or from FirePOWER Management Center Web GUI >> System >> Health >> Health Monitor >> click
Advanced Troubleshooting >> click Download File tab)
```

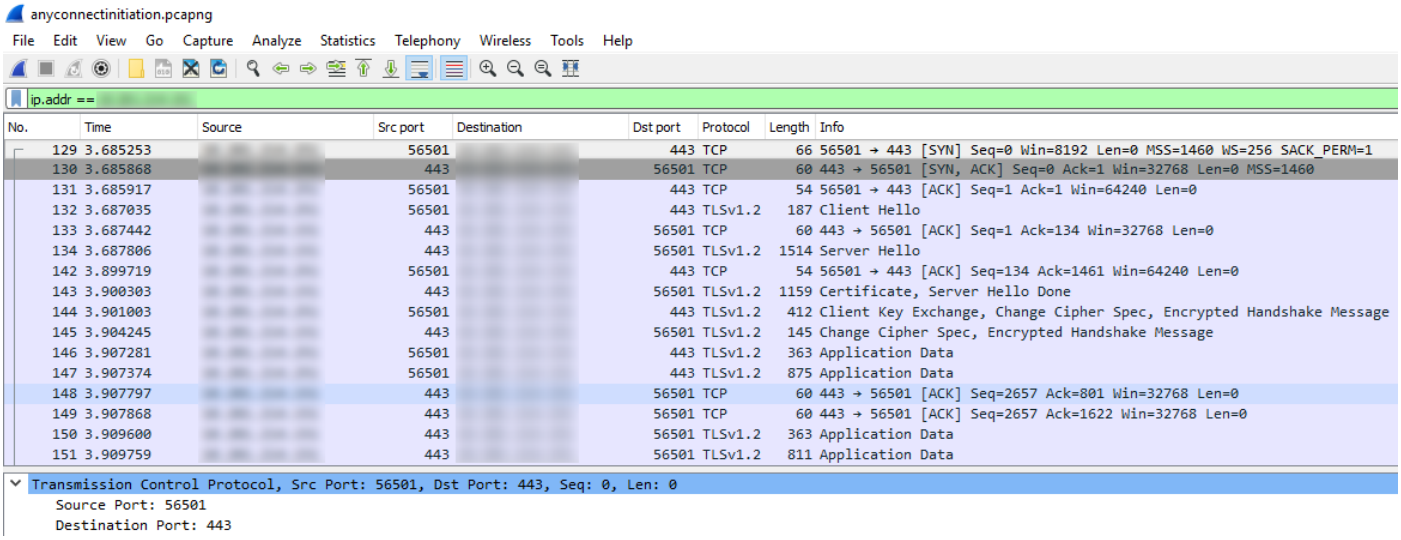
Vérifiez la règle NAT est correctement configuré :

```
ciscofp3# packet-tracer input outside tcp 192.168.10.50 1234 192.168.1.30 443 detailed

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x2ace0fa90e70, priority=13, domain=capture, deny=false
hits=11145169, user_data=0x2ace120c4910, cs_id=0x0, l3_type=0x0
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0000.0000.0000
input_ifc=outside, output_ifc=any

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in id=0x2ace107c8480, priority=1, domain=permit, deny=false
hits=6866095, user_data=0x0, cs_id=0x0, l3_type=0x8
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0100.0000.0000
input_ifc=outside, output_ifc=any

Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.1.30 using egress ifc inside

Phase: 4
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,outside) source static inside-subnet inside-subnet destination static outside-
subnet-anyconnect-po ol outside-subnet-anyconnect-pool no-proxy-arp route-lookup
Additional Information:
NAT divert to egress interface inside
Untranslate 192.168.1.30/443 to 192.168.1.30/443

Phase: 5
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
```

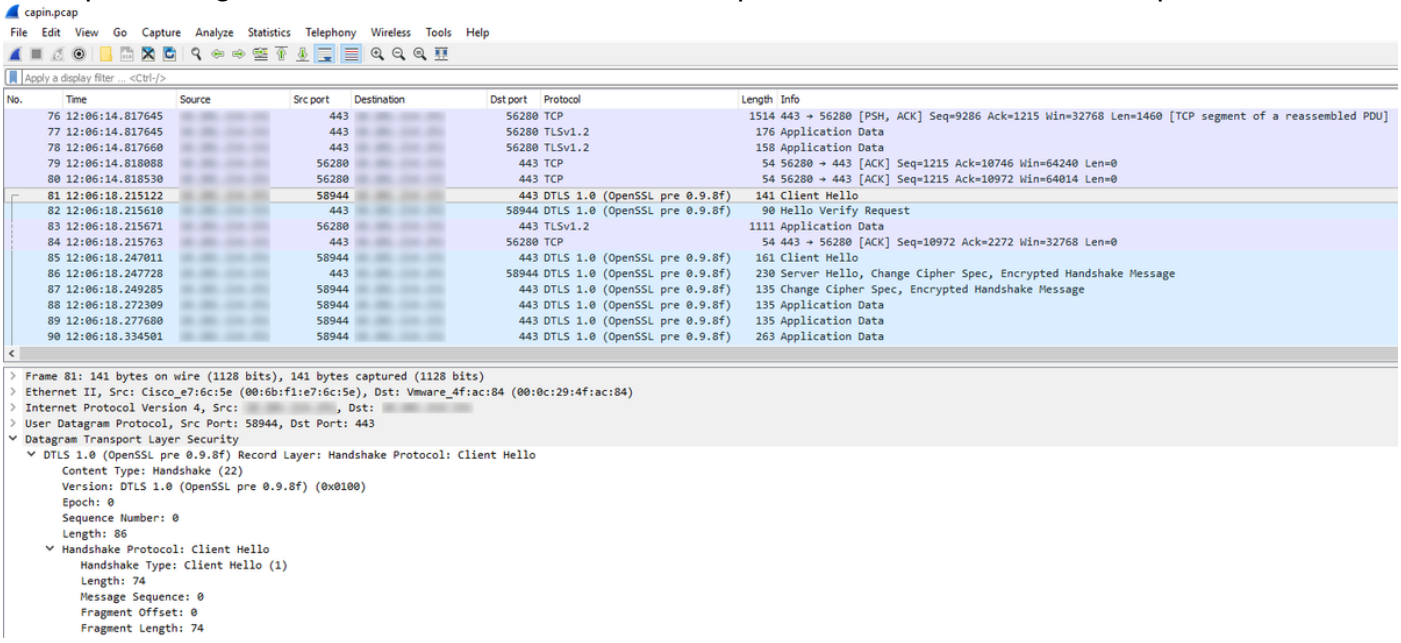
```
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced trust ip ifc outside any any rule-id 268436481 event-log flow-
end
access-list CSM_FW_ACL_ remark rule-id 268436481: PREFILTER POLICY:
Example_Company_Prefilter_Policy
access-list CSM_FW_ACL_ remark rule-id 268436481: RULE: AllowtoVPNOutsideinterface
Additional Information:
Forward Flow based lookup yields rule:
in id=0x2ace0fa8f4e0, priority=12, domain=permit, trust
hits=318637, user_data=0x2ace057b9a80, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=outside
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
input_ifc=any, output_ifc=any

...

Phase: 7
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source static inside-subnet inside-subnet destination static outside-
subnet-anyconnect-po ol outside-subnet-anyconnect-pool no-proxy-arp route-lookup
Additional Information:
Static translate 192.168.10.50/1234 to 192.168.10.50/1234
Forward Flow based lookup yields rule:
in id=0x2ace11975cb0, priority=6, domain=nat, deny=false
hits=120, user_data=0x2ace0f29c4a0, cs_id=0x0, flags=0x0, protocol=0
src ip/id=192.168.10.0, mask=255.255.255.0, port=0, tag=any
dst ip/id=10.201.214.128, mask=255.255.255.240, port=0, tag=any, dscp=0x0
input_ifc=outside, output_ifc=inside

...
Phase: 10 Type: VPN Subtype: ipsec-tunnel-flow Result: ALLOW Config: Additional Information:
Forward Flow based lookup yields rule: in id=0x2ace11d455e0, priority=13, domain=ipsec-tunnel-
flow, deny=true hits=3276174, user_data=0x0, cs_id=0x0, flags=0x0, protocol=0 src ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside, output_ifc=any Phase: 11 Type: NAT Subtype: rpf-check Result: ALLOW Config:
nat (inside,outside) source static inside-subnet inside-subnet destination static outside-
subnet-anyconnect-po ol outside-subnet-anyconnect-pool no-proxy-arp route-lookup
Additional Information:
Forward Flow based lookup yields rule:
out id=0x2ace0d5a9800, priority=6, domain=nat-reverse, deny=false
hits=121, user_data=0x2ace1232a4c0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=192.168.10.0, mask=255.255.255.0, port=0, tag=any
dst ip/id=10.201.214.128, mask=255.255.255.240, port=0, tag=any, dscp=0x0
input_ifc=outside, output_ifc=inside

...

Phase: 14
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 3279248, packet dispatched to next module

Module information for reverse flow ...
...

Phase: 15
Type: ROUTE-LOOKUP
```

```
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.1.30 using egress ifc inside

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: allow

ciscofp3#
```

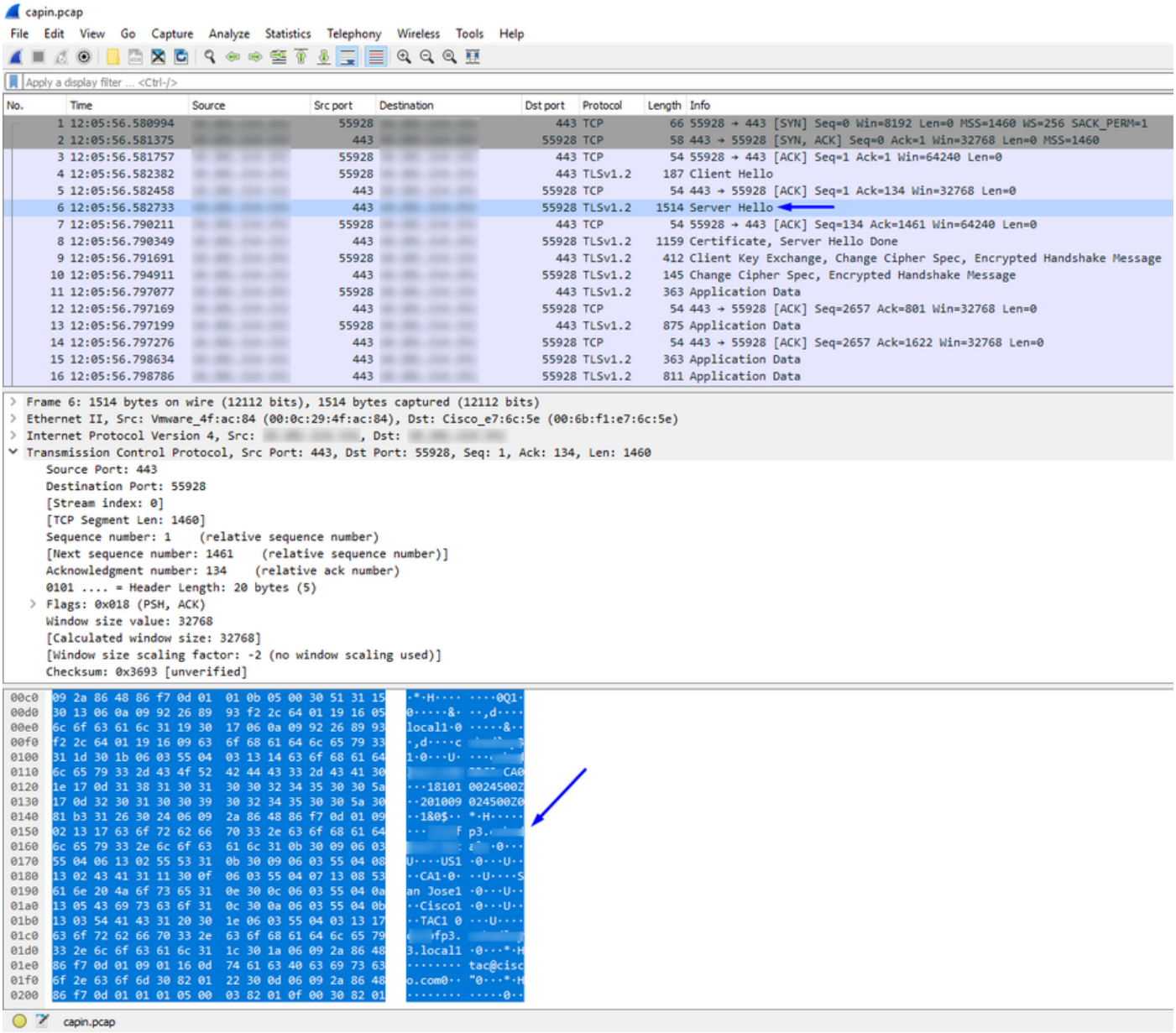
Le capturez pris le PC des employés du PC se connectant avec succès au FTD par l'intermédiaire d'AnyConnect VPN



Vous pouvez également voir le tunnel DTLS former plus tard dans cette même capture

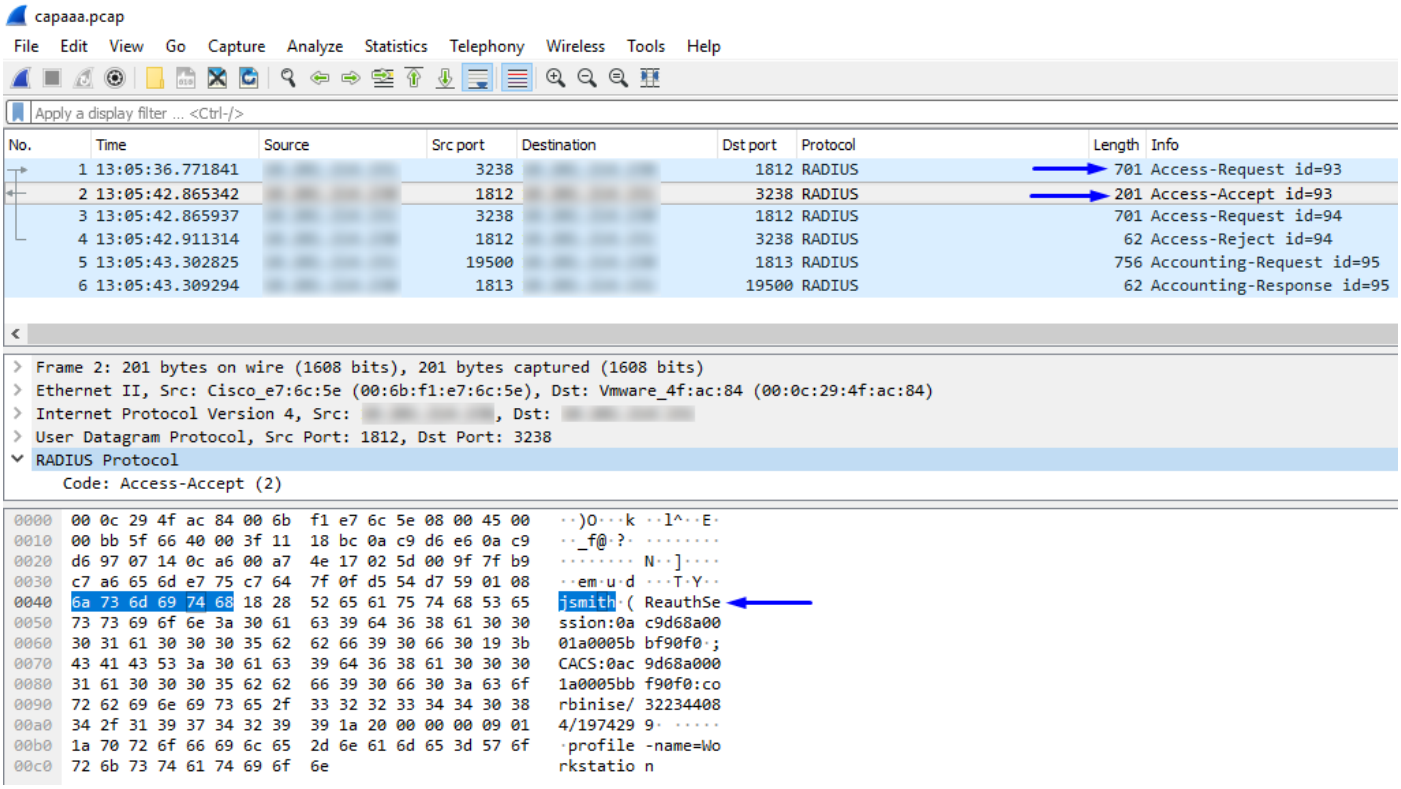


La capture prise sur l'interface extérieure du FTD affichant le PC d'AnyConnect se connecte avec succès au VPN



Remarque: vous pouvez voir le certificat de serveur VPN FTD dans « le paquet des hellos de serveur pendant que nous nous connectons à l'interface extérieure du FTD par l'intermédiaire du VPN. Le PC des employés fera confiance à ce certificat parce que le PC des employés a le certificat de CA de racine là-dessus, et le certificat de serveur VPN FTD a été signé par cette même racine CA.

Le capturez pris le FTD derrière le serveur FTD demandant RADIUS si le nom d'utilisateur + le mot de passe sont corrects (Cisco ISE)

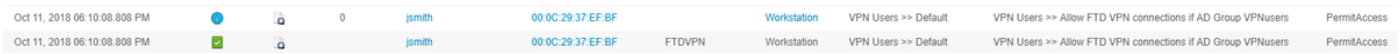


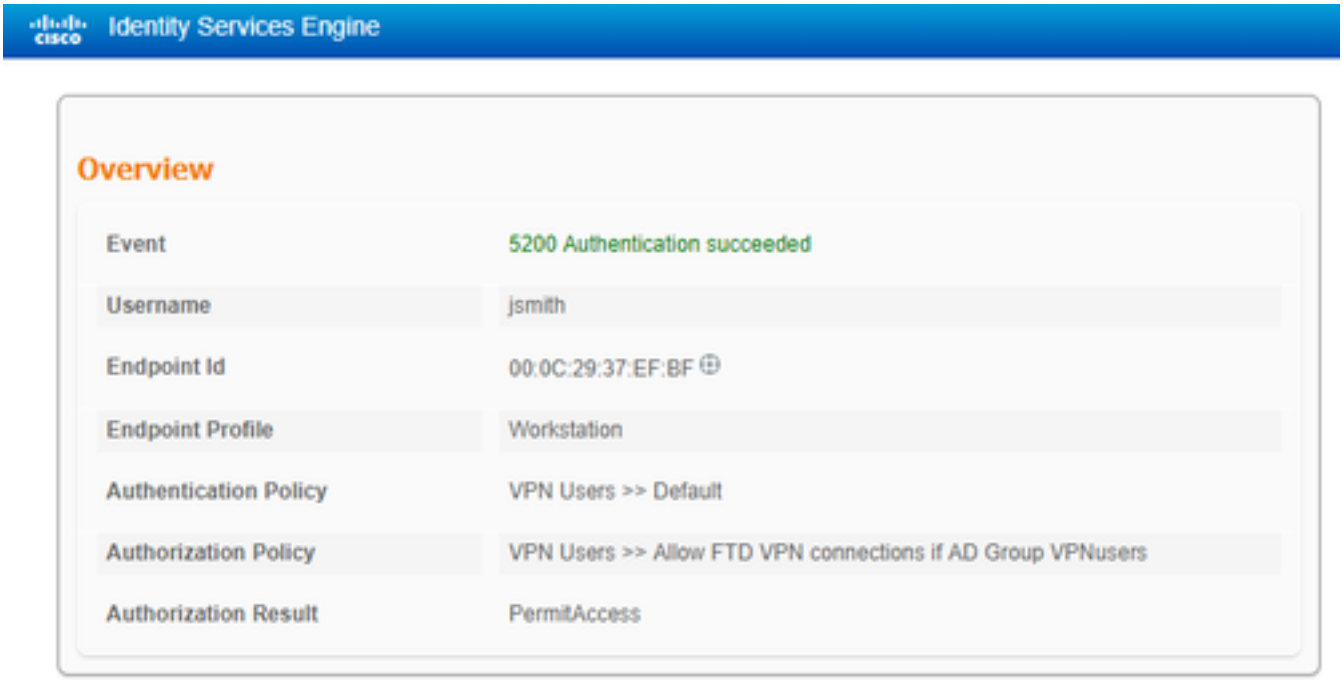
Comme vous pouvez voir en haut, notre connexion VPN obtient un Access-recevoir, et notre AnyConnect VPN Client se connecte avec succès au FTD par l'intermédiaire du VPN

La capture (CLI) de FTD demandant à Cisco ISE si le nom d'utilisateur + le mot de passe sont valides (c.-à-d. s'assurent que les demandes RADIUS vont avec succès entre FTD et ISE et vérifient quelle interface sont elles partant)

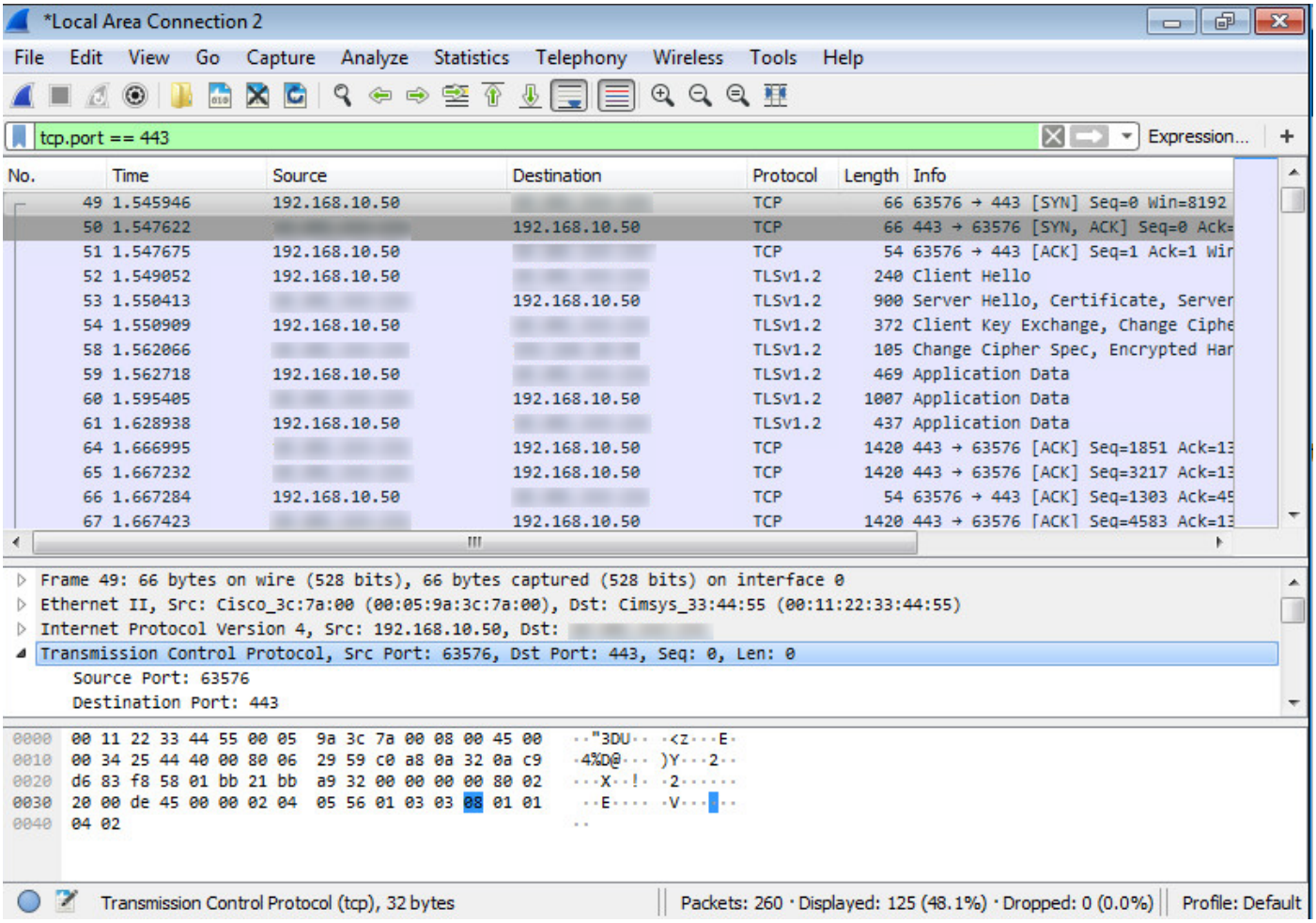
```
ciscofp3# capture capout interface inside trace detail trace-count 100 [Capturing - 35607 bytes]
ciscofp3# show cap
ciscofp3# show cap capout | i 192.168.1.10
37: 01:23:52.264512 192.168.1.1.3238 > 192.168.1.10.1812: udp 659
38: 01:23:52.310210 192.168.1.10.1812 > 192.168.1.1.3238: udp 159
39: 01:23:52.311064 192.168.1.1.3238 > 192.168.1.10.1812: udp 659
40: 01:23:52.326734 192.168.1.10.1812 > 192.168.1.1.3238: udp 20
82: 01:23:52.737663 192.168.1.1.19500 > 192.168.1.10.1813: udp 714
85: 01:23:52.744483 192.168.1.10.1813 > 192.168.1.1.19500: udp 20
```

Au-dessous de Cisco ISE RADIUS le serveur affiche cette authentification réussie. Cliquez sur la loupe pour voir les détails de l'authentification réussie





Capture sur l'adaptateur d'AnyConnect du PC des employés du PC des employés allant à un site Web intérieur par l'intermédiaire de HTTPS (c.-à-d. tandis que c'est avec succès VPN'd dedans) :



Débogages

debug radius tout

anyconnect 255 de debug webvpn

Exécutez le « debug radius toute la » commande sur le diagnostic CLI (le support diagnostic-cli FTD de >system) et le hit « se connectent » sur le PC de Windows/MAC sur le client de Cisco Anyconnect

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
ciscofp3> enable
Password: <hit enter>
ciscofp3# terminal monitor
ciscofp3# debug radius all
<hit Connect on Anyconnect client on PC>

radius mkreq: 0x15
alloc_rip 0x00002ace10875428
new request 0x15 --> 16 (0x00002ace10875428)
got user 'jsmith'
got password
add_req 0x00002ace10875428 session 0x15 id 16
RADIUS_REQUEST
radius.c: rad_mkpkt
rad_mkpkt: ip:source-ip=198.51.100.2

RADIUS packet decode (authentication request)

--------------------------------------
Raw packet data (length = 659).....
01 10 02 93 fb 19 19 df f6 b1 c7 3e 34 fc 88 ce | ...........>4...
75 38 2d 55 01 08 6a 73 6d 69 74 68 02 12 a0 83 | u8-U..jsmith....
c9 bd ad 72 07 d1 bc 24 34 9e 63 a1 f5 93 05 06 | ...r...$4.c.....
00 00 50 00 1e 10 31 30 2e 32 30 31 2e 32 31 34 | ..P...198.51.100.2
2e 31 35 31 1f 10 31 30 2e 32 30 31 2e 32 31 34 | .151..198.51.100.2
2e 32 35 31 3d 06 00 00 00 05 42 10 31 30 2e 32 | .4=.....B.198.
30 31 2e 32 31 34 2e 32 35 31 1a 23 00 00 00 09 | 51.100.2#....
01 1d 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 | ..mdm-tlv=device
2d 70 6c 61 74 66 6f 72 6d 3d 77 69 6e 1a 2c 00 | -platform=win.,.
00 00 09 01 26 6d 64 6d 2d 74 6c 76 3d 64 65 76 | ....&mdm-tlv=dev
69 63 65 2d 6d 61 63 3d 30 30 2d 30 63 2d 32 39 | ice-mac=00-0c-29
2d 33 37 2d 65 66 2d 62 66 1a 33 00 00 00 09 01 | -37-ef-bf.3.....
2d 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d | -mdm-tlv=device-
70 75 62 6c 69 63 2d 6d 61 63 3d 30 30 2d 30 63 | public-mac=00-0c
2d 32 39 2d 33 37 2d 65 66 2d 62 66 1a 3a 00 00 | -29-37-ef-bf.:..
00 09 01 34 6d 64 6d 2d 74 6c 76 3d 61 63 2d 75 | ...4mdm-tlv=ac-u
73 65 72 2d 61 67 65 6e 74 3d 41 6e 79 43 6f 6e | ser-agent=AnyCon
6e 65 63 74 20 57 69 6e 64 6f 77 73 20 34 2e 36 | nect Windows 4.6
2e 30 33 30 34 39 1a 3f 00 00 00 09 01 39 6d 64 | .03049.?.....9md
6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 6c 61 | m-tlv=device-pla
74 66 6f 72 6d 2d 76 65 72 73 69 6f 6e 3d 36 2e | tform-version=6.
31 2e 37 36 30 31 20 53 65 72 76 69 63 65 20 50 | 1.7601 Service P
61 63 6b 20 31 1a 40 00 00 00 09 01 3a 6d 64 6d | ack 1.@.....:mdm
2d 74 6c 76 3d 64 65 76 69 63 65 2d 74 79 70 65 | -tlv=device-type
3d 56 4d 77 61 72 65 2c 20 49 6e 63 2e 20 56 4d | =VMware, Inc. VM
77 61 72 65 20 56 69 72 74 75 61 6c 20 50 6c 61 | ware Virtual Pla
74 66 6f 72 6d 1a 5b 00 00 00 09 01 55 6d 64 6d | tform.[.....Umdm
2d 74 6c 76 3d 64 65 76 69 63 65 2d 75 69 64 3d | -tlv=device-uid=
33 36 39 33 43 36 34 30 37 43 39 32 35 32 35 31 | 3693C6407C925251
46 46 37 32 42 36 34 39 33 42 44 44 38 37 33 31 | FF72B6493BDD8731
38 41 42 46 43 39 30 43 36 32 31 35 34 32 43 33 | 8ABFC90C621542C3
38 46 41 46 38 37 38 45 46 34 39 36 31 34 41 31 | 8FAF878EF49614A1
04 06 00 00 00 00 1a 31 00 00 00 09 01 2b 61 75 | .......1.....+au
64 69 74 2d 73 65 73 73 69 6f 6e 2d 69 64 3d 30 | dit-session-id=0
61 63 39 64 36 38 61 30 30 30 30 30 35 30 30 30 35 | ac9d68a000050005
62 62 65 31 66 39 31 1a 23 00 00 00 09 01 1d 69 | bbe1f91.#......i
```

```
70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e 32 | p:source-ip=192.1
30 31 2e 32 31 34 2e 32 35 31 1a 18 00 00 0c 04 | 68.10.50........
92 12 46 54 44 41 6e 79 43 6f 6e 6e 65 63 74 56 | ..FTDAnyConnectV
50 4e 1a 0c 00 00 0c 04 96 06 00 00 00 02 1a 15 | PN..............
00 00 00 09 01 0f 63 6f 61 2d 70 75 73 68 3d 74 | ......coa-push=t
72 75 65 | rue

Parsed packet data.....
Radius: Code = 1 (0x01)
Radius: Identifier = 16 (0x10)
Radius: Length = 659 (0x0293)
Radius: Vector: FB1919DFF6B1C73E34FC88CE75382D55
Radius: Type = 1 (0x01) User-Name
Radius: Length = 8 (0x08)
Radius: Value (String) =
6a 73 6d 69 74 68 | jsmith
Radius: Type = 2 (0x02) User-Password
Radius: Length = 18 (0x12)
Radius: Value (String) =
a0 83 c9 bd ad 72 07 d1 bc 24 34 9e 63 a1 f5 93 | .....r...$4.c...
Radius: Type = 5 (0x05) NAS-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x5000
Radius: Type = 30 (0x1E) Called-Station-Id
Radius: Length = 16 (0x10)
Radius: Value (String) =
31 30 2e 32 30 31 2e 32 31 34 2e 31 35 31 | 203.0.113.2
Radius: Type = 31 (0x1F) Calling-Station-Id
Radius: Length = 16 (0x10)
Radius: Value (String) =
31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2
Radius: Type = 61 (0x3D) NAS-Port-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x5
Radius: Type = 66 (0x42) Tunnel-Client-Endpoint
Radius: Length = 16 (0x10)
Radius: Value (String) =
31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 35 (0x23)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 29 (0x1D)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p
6c 61 74 66 6f 72 6d 3d 77 69 6e | latform=win
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 44 (0x2C)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 38 (0x26)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 6d | mdm-tlv=device-m
61 63 3d 30 30 2d 30 63 2d 32 39 2d 33 37 2d 65 | ac=00-0c-29-37-e
66 2d 62 66 | f-bf
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 51 (0x33)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 45 (0x2D)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p
75 62 6c 69 63 2d 6d 61 63 3d 30 30 2d 30 63 2d | ublic-mac=00-0c-
32 39 2d 33 37 2d 65 66 2d 62 66 | 29-37-ef-bf
```

```
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 58 (0x3A)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 52 (0x34)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 61 63 2d 75 73 65 72 2d | mdm-tlv=ac-user-
61 67 65 6e 74 3d 41 6e 79 43 6f 6e 6e 65 63 74 | agent=AnyConnect
20 57 69 6e 64 6f 77 73 20 34 2e 36 2e 30 33 30 | Windows 4.6.030
34 39 | 49
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 63 (0x3F)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 57 (0x39)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p
6c 61 74 66 6f 72 6d 2d 76 65 72 73 69 6f 6e 3d | latform-version=
36 2e 31 2e 37 36 30 31 20 53 65 72 76 69 63 65 | 6.1.7601 Service
20 50 61 63 6b 20 31 | Pack 1
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 64 (0x40)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 58 (0x3A)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 74 | mdm-tlv=device-t
79 70 65 3d 56 4d 77 61 72 65 2c 20 49 6e 63 2e | ype=VMware, Inc.
20 56 4d 77 61 72 65 20 56 69 72 74 75 61 6c 20 | VMware Virtual
50 6c 61 74 66 6f 72 6d | Platform
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 91 (0x5B)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 85 (0x55)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 75 | mdm-tlv=device-u
69 64 3d 33 36 39 33 43 36 34 30 37 43 39 32 35 | id=3693C6407C925
32 35 31 46 46 37 32 42 36 34 39 33 42 44 44 38 | 251FF72B6493BDD8
37 33 31 38 41 42 46 43 39 30 43 36 32 31 35 34 | 7318ABFC90C62154
32 43 33 38 46 41 46 38 37 38 45 46 34 39 36 31 | 2C38FAF878EF4961
34 41 31 | 4A1
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 0.0.0.0 (0x00000000)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 49 (0x31)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 43 (0x2B)
Radius: Value (String) =
61 75 64 69 74 2d 73 65 73 73 69 6f 6e 2d 69 64 | audit-session-id
3d 30 61 63 39 64 36 38 61 30 30 30 30 35 30 30 | =0ac9d68a0000500
30 35 62 62 65 31 66 39 31 | 05bbe1f91
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 35 (0x23)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 29 (0x1D)
Radius: Value (String) =
69 70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e | ip:source-ip=192.
32 30 31 2e 32 31 34 2e 32 35 31 | 168.10.50
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 24 (0x18)
```

```
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 146 (0x92) Tunnel-Group-Name
Radius: Length = 18 (0x12)
Radius: Value (String) =
46 54 44 41 6e 79 43 6f 6e 6e 65 63 74 56 50 4e | FTDAnyConnectVPN
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 150 (0x96) Client-Type
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 2 (0x0002)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 21 (0x15)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 15 (0x0F)
Radius: Value (String) =
63 6f 61 2d 70 75 73 68 3d 74 72 75 65 | coa-push=true
send pkt 192.168.1.10/1812
rip 0x00002ace10875428 state 7 id 16
rad_vrfy() : response message verified
rip 0x00002ace10875428
: chall_state ''
: state 0x7
: reqauth:
fb 19 19 df f6 b1 c7 3e 34 fc 88 ce 75 38 2d 55
: info 0x00002ace10875568
session_id 0x15
request_id 0x10
user 'jsmith'
response '***'
app 0
reason 0
skey 'cisco123'
sip 192.168.1.10
type 1

RADIUS packet decode (response)

--------------------------------------
Raw packet data (length = 159).....
02 10 00 9f 39 45 43 cf 05 be df 2f 24 d5 d7 05 | ....9EC..../$...
47 67 b4 fd 01 08 6a 73 6d 69 74 68 18 28 52 65 | Gg....jsmith.(Re
61 75 74 68 53 65 73 73 69 6f 6e 3a 30 61 63 39 | authSession:0ac9
64 36 38 61 30 30 30 30 35 30 30 30 35 62 62 65 | d68a000050005bbe
31 66 39 31 19 3b 43 41 43 53 3a 30 61 63 39 64 | 1f91.;CACS:0ac9d
36 38 61 30 30 30 30 35 30 30 30 35 62 62 65 31 | 68a000050005bbe1
66 39 31 3a 63 6f 72 62 69 6e 69 73 65 2f 33 32 | f91:corbinise/32
32 33 34 34 30 38 34 2f 31 39 33 31 36 38 32 1a | 2344084/1931682.
20 00 00 00 09 01 1a 70 72 6f 66 69 6c 65 2d 6e | ......profile-n
61 6d 65 3d 57 6f 72 6b 73 74 61 74 69 6f 6e | ame=Workstation

Parsed packet data.....
Radius: Code = 2 (0x02)
Radius: Identifier = 16 (0x10)
Radius: Length = 159 (0x009F)
Radius: Vector: 394543CF05BEDF2F24D5D7054767B4FD
Radius: Type = 1 (0x01) User-Name
Radius: Length = 8 (0x08)
Radius: Value (String) =
6a 73 6d 69 74 68 | jsmith
Radius: Type = 24 (0x18) State
Radius: Length = 40 (0x28)
Radius: Value (String) =
```

```
52 65 61 75 74 68 53 65 73 73 69 6f 6e 3a 30 61 | ReauthSession:0a
63 39 64 36 38 61 30 30 30 30 35 30 30 30 35 62 | c9d68a000050005b
62 65 31 66 39 31 | be1f91
Radius: Type = 25 (0x19) Class
Radius: Length = 59 (0x3B)
Radius: Value (String) =
43 41 43 53 3a 30 61 63 39 64 36 38 61 30 30 30 | CACS:0ac9d68a000
30 35 30 30 30 35 62 62 65 31 66 39 31 3a 63 6f | 050005bbe1f91:co
72 62 69 6e 69 73 65 2f 33 32 32 33 34 34 30 38 | rbinise/32234408
34 2f 31 39 33 31 36 38 32 | 4/1931682
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 32 (0x20)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 26 (0x1A)
Radius: Value (String) =
70 72 6f 66 69 6c 65 2d 6e 61 6d 65 3d 57 6f 72 | profile-name=Wor
6b 73 74 61 74 69 6f 6e | kstation
rad_procpkt: ACCEPT
Got AV-Pair with value profile-name=Workstation
RADIUS_ACCESS_ACCEPT: normal termination
radius mkreq: 0x16
alloc_rip 0x00002ace10874b80
new request 0x16 --> 17 (0x00002ace10874b80)
got user 'jsmith'
got password
add_req 0x00002ace10874b80 session 0x16 id 17
RADIUS_DELETE
remove_req 0x00002ace10875428 session 0x15 id 16
free_rip 0x00002ace10875428
RADIUS_REQUEST
radius.c: rad_mkpkt
rad_mkpkt: ip:source-ip=198.51.100.2

RADIUS packet decode (authentication request)

--------------------------------------
Raw packet data (length = 659).....
01 11 02 93 c6 fc 11 c1 0e c4 81 ac 09 a7 85 a8 | ................
83 c1 e4 88 01 08 6a 73 6d 69 74 68 02 12 79 41 | ......jsmith..yA
0e 71 13 38 ae 9f 49 be 3c a9 e4 81 65 93 05 06 | .q.8..I.<...e...
00 00 50 00 1e 10 31 30 2e 32 30 31 2e 32 31 34 | ..P...203.0.113
2e 31 35 31 1f 10 31 30 2e 32 30 31 2e 32 31 34 | .2..203.0.113
2e 32 35 31 3d 06 00 00 00 05 42 10 31 30 2e 32 | .2=.....<ip addr
30 31 2e 32 31 34 2e 32 35 31 1a 23 00 00 00 09 | ess>.#....
01 1d 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 | ..mdm-tlv=device
2d 70 6c 61 74 66 6f 72 6d 3d 77 69 6e 1a 2c 00 | -platform=win.,.
00 00 09 01 26 6d 64 6d 2d 74 6c 76 3d 64 65 76 | ....&mdm-tlv=dev
69 63 65 2d 6d 61 63 3d 30 30 2d 30 63 2d 32 39 | ice-mac=00-0c-29
2d 33 37 2d 65 66 2d 62 66 1a 33 00 00 00 09 01 | -37-ef-bf.3.....
2d 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d | -mdm-tlv=device-
70 75 62 6c 69 63 2d 6d 61 63 3d 30 30 2d 30 63 | public-mac=00-0c
2d 32 39 2d 33 37 2d 65 66 2d 62 66 1a 3a 00 00 | -29-37-ef-bf.:..
00 09 01 34 6d 64 6d 2d 74 6c 76 3d 61 63 2d 75 | ...4mdm-tlv=ac-u
73 65 72 2d 61 67 65 6e 74 3d 41 6e 79 43 6f 6e | ser-agent=AnyCon
6e 65 63 74 20 57 69 6e 64 6f 77 73 20 34 2e 36 | nect Windows 4.6
2e 30 33 30 34 39 1a 3f 00 00 00 09 01 39 6d 64 | .03049.?.....9md
6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 6c 61 | m-tlv=device-pla
74 66 6f 72 6d 2d 76 65 72 73 69 6f 6e 3d 36 2e | tform-version=6.
31 2e 37 36 30 31 20 53 65 72 76 69 63 65 20 50 | 1.7601 Service P
61 63 6b 20 31 1a 40 00 00 00 09 01 3a 6d 64 6d | ack 1.@.....:mdm
2d 74 6c 76 3d 64 65 76 69 63 65 2d 74 79 70 65 | -tlv=device-type
3d 56 4d 77 61 72 65 2c 20 49 6e 63 2e 20 56 4d | =VMware, Inc. VM
77 61 72 65 20 56 69 72 74 75 61 6c 20 50 6c 61 | ware Virtual Pla
```

```
74 66 6f 72 6d 1a 5b 00 00 00 09 01 55 6d 64 6d | tform.[.....Umdm
2d 74 6c 76 3d 64 65 76 69 63 65 2d 75 69 64 3d | -tlv=device-uid=
33 36 39 33 43 36 34 30 37 43 39 32 35 32 35 31 | 3693C6407C925251
46 46 37 32 42 36 34 39 33 42 44 44 38 37 33 31 | FF72B6493BDD8731
38 41 42 46 43 39 30 43 36 32 31 35 34 32 43 33 | 8ABFC90C621542C3
38 46 41 46 38 37 38 45 46 34 39 36 31 34 41 31 | 8FAF878EF49614A1
04 06 00 00 00 00 1a 31 00 00 00 09 01 2b 61 75 | .......1.....+au
64 69 74 2d 73 65 73 73 69 6f 6e 2d 69 64 3d 30 | dit-session-id=0
61 63 39 64 36 38 61 30 30 30 30 35 30 30 30 35 | ac9d68a000050005
62 62 65 31 66 39 31 1a 23 00 00 00 09 01 1d 69 | bbe1f91.#......i
70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e 32 | p:source-ip=192.1
30 31 2e 32 31 34 2e 32 35 31 1a 18 00 00 0c 04 | 68.10.50......
92 12 46 54 44 41 6e 79 43 6f 6e 6e 65 63 74 56 | ..FTDAnyConnectV
50 4e 1a 0c 00 00 0c 04 96 06 00 00 00 02 1a 15 | PN..............
00 00 00 09 01 0f 63 6f 61 2d 70 75 73 68 3d 74 | ......coa-push=t
72 75 65 | rue

Parsed packet data.....
Radius: Code = 1 (0x01)
Radius: Identifier = 17 (0x11)
Radius: Length = 659 (0x0293)
Radius: Vector: C6FC11C10EC481AC09A785A883C1E488
Radius: Type = 1 (0x01) User-Name
Radius: Length = 8 (0x08)
Radius: Value (String) =
6a 73 6d 69 74 68 | jsmith
Radius: Type = 2 (0x02) User-Password
Radius: Length = 18 (0x12)
Radius: Value (String) =
79 41 0e 71 13 38 ae 9f 49 be 3c a9 e4 81 65 93 | yA.q.8..I.<...e.
Radius: Type = 5 (0x05) NAS-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x5000
Radius: Type = 30 (0x1E) Called-Station-Id
Radius: Length = 16 (0x10)
Radius: Value (String) =
31 30 2e 32 30 31 2e 32 31 34 2e 31 35 31 | 203.0.113.2
Radius: Type = 31 (0x1F) Calling-Station-Id
Radius: Length = 16 (0x10)
Radius: Value (String) =
31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2
Radius: Type = 61 (0x3D) NAS-Port-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x5
Radius: Type = 66 (0x42) Tunnel-Client-Endpoint
Radius: Length = 16 (0x10)
Radius: Value (String) =
31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 35 (0x23)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 29 (0x1D)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p
6c 61 74 66 6f 72 6d 3d 77 69 6e | latform=win
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 44 (0x2C)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 38 (0x26)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 6d | mdm-tlv=device-m
61 63 3d 30 30 2d 30 63 2d 32 39 2d 33 37 2d 65 | ac=00-0c-29-37-e
```

```
66 2d 62 66 | f-bf
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 51 (0x33)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 45 (0x2D)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p
75 62 6c 69 63 2d 6d 61 63 3d 30 30 2d 30 63 2d | ublic-mac=00-0c-
32 39 2d 33 37 2d 65 66 2d 62 66 | 29-37-ef-bf
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 58 (0x3A)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 52 (0x34)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 61 63 2d 75 73 65 72 2d | mdm-tlv=ac-user-
61 67 65 6e 74 3d 41 6e 79 43 6f 6e 6e 65 63 74 | agent=AnyConnect
20 57 69 6e 64 6f 77 73 20 34 2e 36 2e 30 33 30 | Windows 4.6.030
34 39 | 49
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 63 (0x3F)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 57 (0x39)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p
6c 61 74 66 6f 72 6d 2d 76 65 72 73 69 6f 6e 3d | latform-version=
36 2e 31 2e 37 36 30 31 20 53 65 72 76 69 63 65 | 6.1.7601 Service
20 50 61 63 6b 20 31 | Pack 1
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 64 (0x40)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 58 (0x3A)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 74 | mdm-tlv=device-t
79 70 65 3d 56 4d 77 61 72 65 2c 20 49 6e 63 2e | ype=VMware, Inc.
20 56 4d 77 61 72 65 20 56 69 72 74 75 61 6c 20 | VMware Virtual
50 6c 61 74 66 6f 72 6d | Platform
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 91 (0x5B)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 85 (0x55)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 75 | mdm-tlv=device-u
69 64 3d 33 36 39 33 43 36 34 30 37 43 39 32 35 | id=3693C6407C925
32 35 31 46 46 37 32 42 36 34 39 33 42 44 44 38 | 251FF72B6493BDD8
37 33 31 38 41 42 46 43 39 30 43 36 32 31 35 34 | 7318ABFC90C62154
32 43 33 38 46 41 46 38 37 38 45 46 34 39 36 31 | 2C38FAF878EF4961
34 41 31 | 4A1
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 0.0.0.0 (0x00000000)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 49 (0x31)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 43 (0x2B)
Radius: Value (String) =
61 75 64 69 74 2d 73 65 73 73 69 6f 6e 2d 69 64 | audit-session-id
3d 30 61 63 39 64 36 38 61 30 30 30 30 35 30 30 | =0ac9d68a0000500
30 35 62 62 65 31 66 39 31 | 05bbe1f91
```

```
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 35 (0x23)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 29 (0x1D)
Radius: Value (String) =
69 70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e | ip:source-ip=192.
32 30 31 2e 32 31 34 2e 32 35 31 | 168.10.50
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 24 (0x18)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 146 (0x92) Tunnel-Group-Name
Radius: Length = 18 (0x12)
Radius: Value (String) =
46 54 44 41 6e 79 43 6f 6e 6e 65 63 74 56 50 4e | FTDAnyConnectVPN
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 150 (0x96) Client-Type
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 2 (0x0002)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 21 (0x15)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 15 (0x0F)
Radius: Value (String) =
63 6f 61 2d 70 75 73 68 3d 74 72 75 65 | coa-push=true
send pkt 192.168.1.10/1812
rip 0x00002ace10874b80 state 7 id 17
rad_vrfy() : response message verified
rip 0x00002ace10874b80
: chall_state ''
: state 0x7
: reqauth:
c6 fc 11 c1 0e c4 81 ac 09 a7 85 a8 83 c1 e4 88
: info 0x00002ace10874cc0
session_id 0x16
request_id 0x11
user 'jsmith'
response '***'
app 0
reason 0
skey 'cisco123'
sip 192.168.1.10
type 1

RADIUS packet decode (response)

--------------------------------------
Raw packet data (length = 20).....
03 11 00 14 15 c3 44 44 7d a6 07 0d 7b 92 f2 3b | ......DD}...{..;
0b 06 ba 74 | ...t

Parsed packet data.....
Radius: Code = 3 (0x03)
Radius: Identifier = 17 (0x11)
Radius: Length = 20 (0x0014)
Radius: Vector: 15C344447DA6070D7B92F23B0B06BA74
rad_procpkt: REJECT
RADIUS_DELETE
remove_req 0x00002ace10874b80 session 0x16 id 17
free_rip 0x00002ace10874b80
radius: send queue empty
```

```
radius mkreq: 0x18
alloc_rip 0x00002ace10874b80
new request 0x18 --> 18 (0x00002ace10874b80)
add_req 0x00002ace10874b80 session 0x18 id 18
ACCT_REQUEST
radius.c: rad_mkpkt

RADIUS packet decode (accounting request)

--------------------------------------
Raw packet data (length = 714).....
04 12 02 ca be a0 6e 46 71 af 5c 65 82 77 c7 b5 | ......nFq.\e.w..
50 78 61 d7 01 08 6a 73 6d 69 74 68 05 06 00 00 | Pxa...jsmith....
50 00 06 06 00 00 00 02 07 06 00 00 00 01 08 06 | P...............
c0 a8 0a 32 19 3b 43 41 43 53 3a 30 61 63 39 64 | ...2.;CACS:0ac9d
36 38 61 30 30 30 30 35 30 30 30 35 62 62 65 31 | 68a000050005bbe1
66 39 31 3a 63 6f 72 62 69 6e 69 73 65 2f 33 32 | f91:corbinise/32
32 33 34 34 30 38 34 2f 31 39 33 31 36 38 32 1e | 2344084/1931682.
10 31 30 2e 32 30 31 2e 32 31 34 2e 31 35 31 1f | .203.0.113.2.
10 31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 28 | .198.51.100.2(
06 00 00 00 01 29 06 00 00 00 00 2c 0a 43 31 46 | .....).....,.C1F
30 30 30 30 35 2d 06 00 00 00 01 3d 06 00 00 00 | 00005-.....=....
05 42 10 31 30 2e 32 30 31 2e 32 31 34 2e 32 35 | .B.203.0.113.2
31 1a 18 00 00 0c 04 92 12 46 54 44 41 6e 79 43 | ........FTDAnyC
6f 6e 6e 65 63 74 56 50 4e 1a 0c 00 00 0c 04 96 | onnectVPN.......
06 00 00 00 02 1a 0c 00 00 0c 04 97 06 00 00 00 | ................
01 1a 0c 00 00 0c 04 98 06 00 00 00 03 1a 23 00 | ..............#.
00 00 09 01 1d 6d 64 6d 2d 74 6c 76 3d 64 65 76 | .....mdm-tlv=dev
69 63 65 2d 70 6c 61 74 66 6f 72 6d 3d 77 69 6e | ice-platform=win
1a 2c 00 00 00 09 01 26 6d 64 6d 2d 74 6c 76 3d | .,.....&mdm-tlv=
64 65 76 69 63 65 2d 6d 61 63 3d 30 30 2d 30 63 | device-mac=00-0c
2d 32 39 2d 33 37 2d 65 66 2d 62 66 1a 31 00 00 | -29-37-ef-bf.1..
00 09 01 2b 61 75 64 69 74 2d 73 65 73 73 69 6f | ...+audit-sessio
6e 2d 69 64 3d 30 61 63 39 64 36 38 61 30 30 30 | n-id=0ac9d68a000
30 35 30 30 30 35 62 62 65 31 66 39 31 1a 33 00 | 050005bbe1f91.3.
00 00 09 01 2d 6d 64 6d 2d 74 6c 76 3d 64 65 76 | ....-mdm-tlv=dev
69 63 65 2d 70 75 62 6c 69 63 2d 6d 61 63 3d 30 | ice-public-mac=0
30 2d 30 63 2d 32 39 2d 33 37 2d 65 66 2d 62 66 | 0-0c-29-37-ef-bf
1a 3a 00 00 00 09 01 34 6d 64 6d 2d 74 6c 76 3d | .:.....4mdm-tlv=
61 63 2d 75 73 65 72 2d 61 67 65 6e 74 3d 41 6e | ac-user-agent=An
79 43 6f 6e 6e 65 63 74 20 57 69 6e 64 6f 77 73 | yConnect Windows
20 34 2e 36 2e 30 33 30 34 39 1a 3f 00 00 00 09 | 4.6.03049.?....
01 39 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 | .9mdm-tlv=device
2d 70 6c 61 74 66 6f 72 6d 2d 76 65 72 73 69 6f | -platform-versio
6e 3d 36 2e 31 2e 37 36 30 31 20 53 65 72 76 69 | n=6.1.7601 Servi
63 65 20 50 61 63 6b 20 31 1a 40 00 00 00 09 01 | ce Pack 1.@.....
3a 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d | :mdm-tlv=device-
74 79 70 65 3d 56 4d 77 61 72 65 2c 20 49 6e 63 | type=VMware, Inc
2e 20 56 4d 77 61 72 65 20 56 69 72 74 75 61 6c | . VMware Virtual
20 50 6c 61 74 66 6f 72 6d 1a 5b 00 00 00 09 01 | Platform.[.....
55 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d | Umdm-tlv=device-
75 69 64 3d 33 36 39 33 43 36 34 30 37 43 39 32 | uid=3693C6407C92
35 32 35 31 46 46 37 32 42 36 34 39 33 42 44 44 | 5251FF72B6493BDD
38 37 33 31 38 41 42 46 43 39 30 43 36 32 31 35 | 87318ABFC90C6215
34 32 43 33 38 46 41 46 38 37 38 45 46 34 39 36 | 42C38FAF878EF496
31 34 41 31 04 06 00 00 00 00 | 14A1......

Parsed packet data.....
Radius: Code = 4 (0x04)
Radius: Identifier = 18 (0x12)
Radius: Length = 714 (0x02CA)
Radius: Vector: BEA06E4671AF5C658277C7B5507861D7
Radius: Type = 1 (0x01) User-Name
Radius: Length = 8 (0x08)
```

```
Radius: Value (String) =
6a 73 6d 69 74 68 | jsmith
Radius: Type = 5 (0x05) NAS-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x5000
Radius: Type = 6 (0x06) Service-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x2
Radius: Type = 7 (0x07) Framed-Protocol
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x1
Radius: Type = 8 (0x08) Framed-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 192.168.10.50 (0xC0A80A32)
Radius: Type = 25 (0x19) Class
Radius: Length = 59 (0x3B)
Radius: Value (String) =
43 41 43 53 3a 30 61 63 39 64 36 38 61 30 30 30 | CACS:0ac9d68a000
30 35 30 30 30 35 62 62 65 31 66 39 31 3a 63 6f | 050005bbe1f91:co
72 62 69 6e 69 73 65 2f 33 32 32 33 34 34 30 38 | rbinise/32234408
34 2f 31 39 33 31 36 38 32 | 4/1931682
Radius: Type = 30 (0x1E) Called-Station-Id
Radius: Length = 16 (0x10)
Radius: Value (String) =
31 30 2e 32 30 31 2e 32 31 34 2e 31 35 31 | 203.0.113.2
Radius: Type = 31 (0x1F) Calling-Station-Id
Radius: Length = 16 (0x10)
Radius: Value (String) =
31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2
Radius: Type = 40 (0x28) Acct-Status-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x1
Radius: Type = 41 (0x29) Acct-Delay-Time
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x0
Radius: Type = 44 (0x2C) Acct-Session-Id
Radius: Length = 10 (0x0A)
Radius: Value (String) =
43 31 46 30 30 30 30 35 | C1F00005
Radius: Type = 45 (0x2D) Acct-Authentic
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x1
Radius: Type = 61 (0x3D) NAS-Port-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x5
Radius: Type = 66 (0x42) Tunnel-Client-Endpoint
Radius: Length = 16 (0x10)
Radius: Value (String) =
31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 24 (0x18)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 146 (0x92) Tunnel-Group-Name
Radius: Length = 18 (0x12)
Radius: Value (String) =
46 54 44 41 6e 79 43 6f 6e 6e 65 63 74 56 50 4e | FTDAnyConnectVPN
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 150 (0x96) Client-Type
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 2 (0x0002)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
```

```
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 151 (0x97) VPN-Session-Type
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 1 (0x0001)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 152 (0x98) VPN-Session-Subtype
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 3 (0x0003)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 35 (0x23)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 29 (0x1D)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p
6c 61 74 66 6f 72 6d 3d 77 69 6e | latform=win
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 44 (0x2C)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 38 (0x26)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 6d | mdm-tlv=device-m
61 63 3d 30 30 2d 30 63 2d 32 39 2d 33 37 2d 65 | ac=00-0c-29-37-e
66 2d 62 66 | f-bf
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 49 (0x31)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 43 (0x2B)
Radius: Value (String) =
61 75 64 69 74 2d 73 65 73 73 69 6f 6e 2d 69 64 | audit-session-id
3d 30 61 63 39 64 36 38 61 30 30 30 30 35 30 30 | =0ac9d68a0000500
30 35 62 62 65 31 66 39 31 | 05bbe1f91
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 51 (0x33)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 45 (0x2D)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p
75 62 6c 69 63 2d 6d 61 63 3d 30 30 2d 30 63 2d | ublic-mac=00-0c-
32 39 2d 33 37 2d 65 66 2d 62 66 | 29-37-ef-bf
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 58 (0x3A)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 52 (0x34)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 61 63 2d 75 73 65 72 2d | mdm-tlv=ac-user-
61 67 65 6e 74 3d 41 6e 79 43 6f 6e 6e 65 63 74 | agent=AnyConnect
20 57 69 6e 64 6f 77 73 20 34 2e 36 2e 30 33 30 | Windows 4.6.030
34 39 | 49
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 63 (0x3F)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 57 (0x39)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p
6c 61 74 66 6f 72 6d 2d 76 65 72 73 69 6f 6e 3d | latform-version=
36 2e 31 2e 37 36 30 31 20 53 65 72 76 69 63 65 | 6.1.7601 Service
```

```
20 50 61 63 6b 20 31 | Pack 1
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 64 (0x40)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 58 (0x3A)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 74 | mdm-tlv=device-t
79 70 65 3d 56 4d 77 61 72 65 2c 20 49 6e 63 2e | ype=VMware, Inc.
20 56 4d 77 61 72 65 20 56 69 72 74 75 61 6c 20 | VMware Virtual
50 6c 61 74 66 6f 72 6d | Platform
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 91 (0x5B)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 85 (0x55)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 75 | mdm-tlv=device-u
69 64 3d 33 36 39 33 43 36 34 30 37 43 39 32 35 | id=3693C6407C925
32 35 31 46 46 37 32 42 36 34 39 33 42 44 44 38 | 251FF72B6493BDD8
37 33 31 38 41 42 46 43 39 30 43 36 32 31 35 34 | 7318ABFC90C62154
32 43 33 38 46 41 46 38 37 38 45 46 34 39 36 31 | 2C38FAF878EF4961
34 41 31 | 4A1
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 0.0.0.0 (0x00000000)
send pkt 192.168.1.10/1813
rip 0x00002ace10874b80 state 6 id 18
rad_vrfy() : response message verified
rip 0x00002ace10874b80
: chall_state ''
: state 0x6
: reqauth:
be a0 6e 46 71 af 5c 65 82 77 c7 b5 50 78 61 d7
: info 0x00002ace10874cc0
session_id 0x18
request_id 0x12
user 'jsmith'
response '***'
app 0
reason 0
skey 'cisco123'
sip 192.168.1.10
type 3

RADIUS packet decode (response)

--------------------------------------
Raw packet data (length = 20).....
05 12 00 14 e5 fd b1 6d fb ee 58 f0 89 79 73 8e | .......m..X..ys.
90 dc a7 20 | ...

Parsed packet data.....
Radius: Code = 5 (0x05)
Radius: Identifier = 18 (0x12)
Radius: Length = 20 (0x0014)
Radius: Vector: E5FDB16DFBEE58F08979738E90DCA720
rad_procpkt: ACCOUNTING_RESPONSE
RADIUS_DELETE
remove_req 0x00002ace10874b80 session 0x18 id 18
free_rip 0x00002ace10874b80
radius: send queue empty
ciscofp3#
```

Exécutez 'la commande de l'anyconnect 255' de debug webvpn sur le diagnostic CLI (le support diagnostic-cli FTD de >system) et le hit « se connectent » sur le PC de Windows/MAC sur le client de Cisco Anyconnect

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
ciscofp3> enable
Password: <hit enter>
ciscofp3# terminal monitor
ciscofp3# debug webvpn anyconnect 255
<hit Connect on Anyconnect client on PC>

http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: ciscofp3.cisco.com'
Processing CSTP header line: 'Host: ciscofp3.cisco.com'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 4.6.03049'
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 4.6.03049'
Setting user-agent to: 'Cisco AnyConnect VPN Agent for Windows 4.6.03049'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
Processing CSTP header line: 'Cookie:
webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
Found WebVPN cookie: 'webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
WebVPN Cookie: 'webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Version: 1'
Processing CSTP header line: 'X-CSTP-Version: 1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Hostname: jsmith-PC'
Processing CSTP header line: 'X-CSTP-Hostname: jsmith-PC'
Setting hostname to: 'jsmith-PC'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-MTU: 1399'
Processing CSTP header line: 'X-CSTP-MTU: 1399'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv6,IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv6,IPv4'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Local-Address-IP4: 198.51.100.2'
Processing CSTP header line: 'X-CSTP-Local-Address-IP4: 198.51.100.2'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Base-MTU: 1500'
Processing CSTP header line: 'X-CSTP-Base-MTU: 1500'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Remote-Address-IP4: 203.0.113.2'
Processing CSTP header line: 'X-CSTP-Remote-Address-IP4: 203.0.113.2'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Full-IPv6-Capability: true'
Processing CSTP header line: 'X-CSTP-Full-IPv6-Capability: true'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret:
1FA92A96D5E82C13CB3A5758F11371EE6B54C6F36F0A8DCE8F4DECB73A034EEF4FE95DA614A5872E1EE5557C3BF4765A
'
Processing CSTP header line: 'X-DTLS-Master-Secret:
1FA92A96D5E82C13CB3A5758F11371EE6B54C6F36F0A8DCE8F4DECB73A034EEF4FE95DA614A5872E1EE5557C3BF4765A
'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-CipherSuite: DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-
SHA:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:AES256-SHA:AES128-
```

```
SHA:DES-CBC3-SHA'
Processing CSTP header line: 'X-DTLS-CipherSuite: DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-
SHA256:DHE-RSA-AES256-SHA:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-
SHA:AES256-SHA:AES128-SHA:DES-CBC3-SHA'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Accept-Encoding: lzs'
Processing CSTL header line: 'X-DTLS-Accept-Encoding: lzs'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Header-Pad-Length: 0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: lzs,deflate'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: lzs,deflate'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Processing CSTP header line: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
cstp_util_address_ipv4_accept: address asigned: 192.168.10.50
cstp_util_address_ipv6_accept: No IPv6 Address
np_svc_create_session(0x7000, 0x00002acdff1d6440, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
vpn_put_uauth success for ip 192.168.10.50!
No SVC ACL
Iphdr=20 base-mtu=1500 def-mtu=1500 conf-mtu=1406
tcp-mss = 1460
path-mtu = 1460(mss)
TLS Block size = 16, version = 0x303
mtu = 1460(path-mtu) - 0(opts) - 5(ssl) - 16(iv) = 1439
mod-mtu = 1439(mtu) & 0xfff0(complement) = 1424
tls-mtu = 1424(mod-mtu) - 8(cstp) - 48(mac) - 1(pad) = 1367
DTLS Block size = 16
mtu = 1500(base-mtu) - 20(ip) - 8(udp) - 13(dtlshdr) - 16(dtlsiv) = 1443
mod-mtu = 1443(mtu) & 0xfff0(complement) = 1440
dtls-mtu = 1440(mod-mtu) - 1(cdtp) - 20(mac) - 1(pad) = 1418
computed tls-mtu=1367 dtls-mtu=1418 conf-mtu=1406
DTLS enabled for intf=3 (outside)
overide computed dtls-mtu=1418 with conf-mtu=1406
tls-mtu=1367 dtls-mtu=1406
SVC: adding to sessmgmt
Sending X-CSTP-MTU: 1367
Sending X-DTLS-MTU: 1406
Sending X-CSTP-FW-RULE msgs: Start
Sending X-CSTP-FW-RULE msgs: Done
Sending X-CSTP-Quarantine: false
Sending X-CSTP-Disable-Always-On-VPN: false
Sending X-CSTP-Client-Bypass-Protocol: false
```

Cisco ISE

Cisco ISE > exécutions > RADIUS > logs vivants > détails de clic de chaque authentification

Vérifiez sur Cisco ISE votre procédure de connexion VPN et le résultat « PermitAccess » d'ACL est donné
Les logs vivants affichent le jsmith authentifié à FTD par l'intermédiaire du VPN avec succès

Identity Services Engine

Overview

Event	5200 Authentication succeeded
Username	jsmith
Endpoint Id	
Endpoint Profile	
Authentication Policy	VPN Users >> Default
Authorization Policy	VPN Users >> Allow ASA VPN connections if AD Group VPNusers
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2018-10-09 01:47:55.112
Received Timestamp	2018-10-09 01:47:55.113
Policy Server	corbinise
Event	5200 Authentication succeeded
Username	jsmith
Endpoint Id	
Calling Station Id	
Authentication Identity Store	corbdc3
Audit Session Id	00000000000070005bbc08c3
Authentication Method	PAP_ASCII
Authentication Protocol	PAP_ASCII
Network Device	FTDVPN
Device Type	All Device Types
Location	All Locations

Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - Airespace.Airespace-Wlan-Id
15048	Queried PIP - Radius.NAS-Port-Type
15041	Evaluating Identity Policy
15048	Queried PIP - Normalised Radius.RadiusFlowType
22072	Selected identity source sequence - All_User_ID_Stores
15013	Selected Identity Source - Internal Users
24210	Looking up User in Internal Users IDStore - jsmith
24216	The user is not found in the internal users identity store
15013	Selected Identity Source - All_AD_Join_Points
24430	Authenticating user against Active Directory - All_AD_Join_Points
24325	Resolving identity - jsmith (⏰ Step latency=7106 ms)
24313	Search for matching accounts at join point -
24319	Single matching account found in forest -
24313	Search for matching accounts at join point - windows_ad_server.com
24366	Skipping unjoined domain - Windows_AD_Server.com
24323	Identity resolution detected single matching account
24343	RPC Logon request succeeded - jsmith
24402	User authentication against Active Directory succeeded - All_AD_Join_Points
22037	Authentication Passed
24715	ISE has not confirmed locally previous successful machine authentication for user in Active Directory
15036	Evaluating Authorization Policy
24432	Looking up user in Active Directory -
24355	LDAP fetch succeeded -
24416	User's Groups retrieval from Active Directory succeeded -
15048	Queried PIP - ExternalGroups
15016	Selected Authorization Profile - PermitAccess
22081	Max sessions policy passed
22080	New accounting session created in Session cache
11002	Returned RADIUS Access-Accept

Location	All Locations
NAS IPv4 Address	0.0.0.0
NAS Port Type	Virtual
Authorization Profile	PermitAccess
Response Time	7294 milliseconds

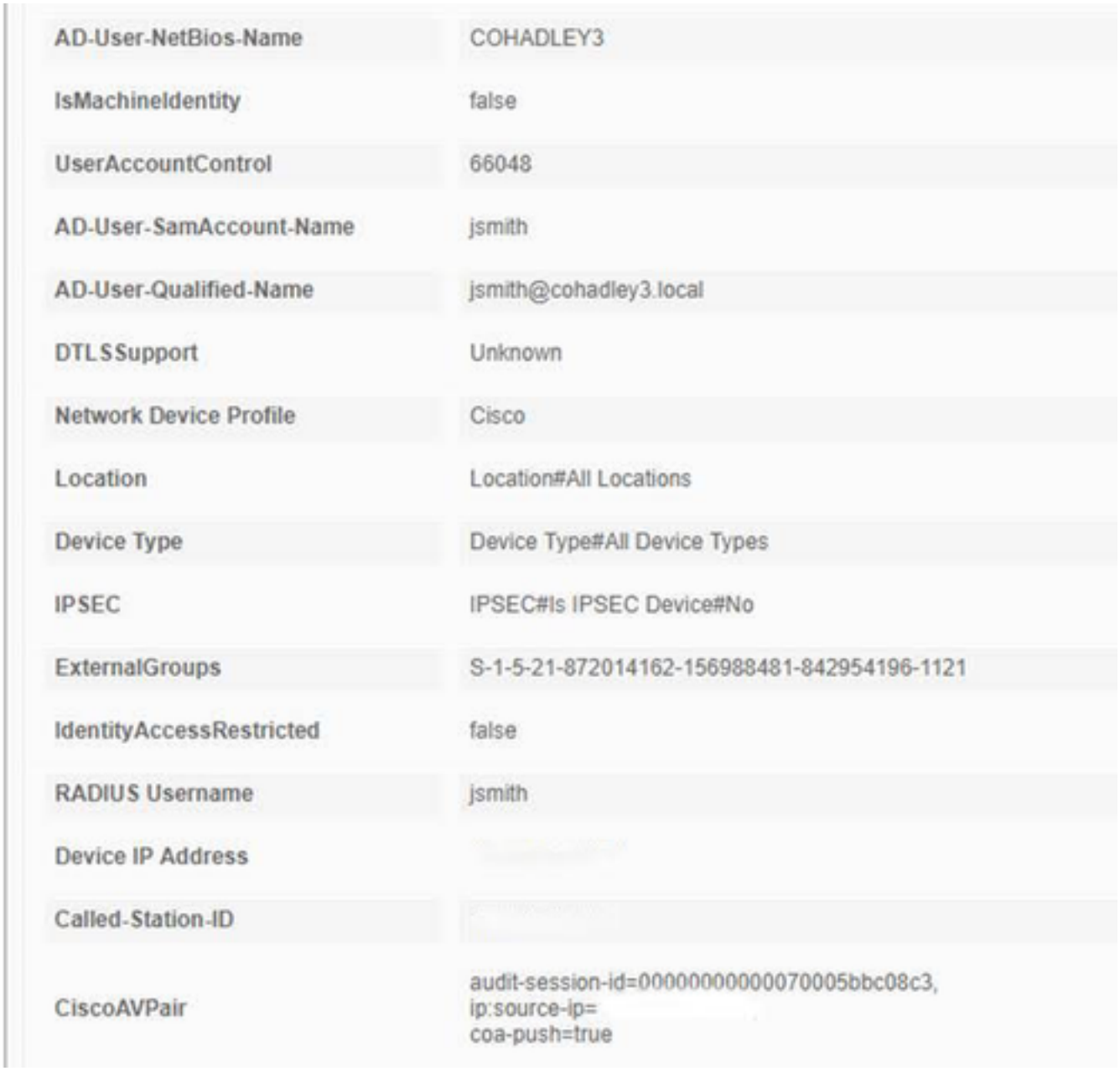
11002 Returned RADIUS Access-Accept

Other Attributes

ConfigVersionId	257
DestinationPort	1812
Protocol	Radius
NAS-Port	28672
Tunnel-Client-Endpoint	(tag=0)
CVPN3000/ASA/PIX7x-Tunnel-Group-Name	FTDAnyConnectVPN
OriginalUserName	jsmith
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
CVPN3000/ASA/PIX7x-Client-Type	3
AcsSessionID	corbinise/322344084/1870108
SelectedAuthenticationIdentityStores	Internal Users
SelectedAuthenticationIdentityStores	All_AD_Join_Points
SelectedAuthenticationIdentityStores	Guest Users
AuthenticationStatus	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Allow ASA VPN connections if AD Group VPNusers
CPMSessionID	00000000000070005bbc08c3

Identity Services Engine

CPMSessionID	00000000000070005bbc08c3
ISEPolicySetName	VPN Users
IdentitySelectionMatchedRule	Default
StepLatency	14=7106
AD-User-Resolved-Identities	jsmith@cohadley3.local
AD-User-Candidate-Identities	jsmith@cohadley3.local
AD-User-Join-Point	COHADLEY3.LOCAL
AD-User-Resolved-DNs	CN=John Smith,CN=Users,DC=cohadley3,DC=local
AD-User-DNS-Domain	cohadley3.local



AD-User-NetBios-Name	COHADLEY3
IsMachineIdentity	false
UserAccountControl	66048
AD-User-SamAccount-Name	jsmith
AD-User-Qualified-Name	jsmith@cohadley3.local
DTLSSupport	Unknown
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
ExternalGroups	S-1-5-21-872014162-156988481-842954196-1121
IdentityAccessRestricted	false
RADIUS Username	jsmith
Device IP Address	
Called-Station-ID	
CiscoAVPair	audit-session-id=0000000000070005bbc08c3, ip:source-ip= coa-push=true

AnyConnect VPN Client

Paquet de DART

Comment collecter le paquet de DART pour AnyConnect

Dépanner

DNS

Vérifiez Cisco ISE, FTD, les Windows Server 2012, et Windows/PC de MAC peut tout se résoudre en avant et s'inverser (des DN de contrôle sur tous les périphériques)

PC Windows
Lancez une invite de commande, et assurez-vous que vous pouvez exécuter un « nslookup » sur l'adresse Internet du FTD

FTD CLI

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
ciscofp3> enable
Password: <hit enter>
ciscofp3# terminal monitor
ciscofp3# debug webvpn anyconnect 255
<hit Connect on Anyconnect client on PC>

http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: ciscofp3.cisco.com'
Processing CSTP header line: 'Host: ciscofp3.cisco.com'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 4.6.03049'
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 4.6.03049'
Setting user-agent to: 'Cisco AnyConnect VPN Agent for Windows 4.6.03049'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
Processing CSTP header line: 'Cookie:
webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
Found WebVPN cookie: 'webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
WebVPN Cookie: 'webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Version: 1'
Processing CSTP header line: 'X-CSTP-Version: 1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Hostname: jsmith-PC'
Processing CSTP header line: 'X-CSTP-Hostname: jsmith-PC'
Setting hostname to: 'jsmith-PC'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-MTU: 1399'
Processing CSTP header line: 'X-CSTP-MTU: 1399'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv6,IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv6,IPv4'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Local-Address-IP4: 198.51.100.2'
Processing CSTP header line: 'X-CSTP-Local-Address-IP4: 198.51.100.2'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Base-MTU: 1500'
Processing CSTP header line: 'X-CSTP-Base-MTU: 1500'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Remote-Address-IP4: 203.0.113.2'
Processing CSTP header line: 'X-CSTP-Remote-Address-IP4: 203.0.113.2'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Full-IPv6-Capability: true'
Processing CSTP header line: 'X-CSTP-Full-IPv6-Capability: true'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret:
1FA92A96D5E82C13CB3A5758F11371EE6B54C6F36F0A8DCE8F4DECB73A034EEF4FE95DA614A5872E1EE5557C3BF4765A
'
Processing CSTP header line: 'X-DTLS-Master-Secret:
1FA92A96D5E82C13CB3A5758F11371EE6B54C6F36F0A8DCE8F4DECB73A034EEF4FE95DA614A5872E1EE5557C3BF4765A
'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-CipherSuite: DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-
SHA:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:AES256-SHA:AES128-
SHA:DES-CBC3-SHA'
Processing CSTP header line: 'X-DTLS-CipherSuite: DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-
```

```
SHA256:DHE-RSA-AES256-SHA:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-
SHA:AES256-SHA:AES128-SHA:DES-CBC3-SHA'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Accept-Encoding: lzs'
Processing CSTL header line: 'X-DTLS-Accept-Encoding: lzs'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Header-Pad-Length: 0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: lzs,deflate'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: lzs,deflate'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Processing CSTP header line: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
cstp_util_address_ipv4_accept: address asigned: 192.168.10.50
cstp_util_address_ipv6_accept: No IPv6 Address
np_svc_create_session(0x7000, 0x00002acdff1d6440, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
vpn_put_uauth success for ip 192.168.10.50!
No SVC ACL
Iphdr=20 base-mtu=1500 def-mtu=1500 conf-mtu=1406
tcp-mss = 1460
path-mtu = 1460(mss)
TLS Block size = 16, version = 0x303
mtu = 1460(path-mtu) - 0(opts) - 5(ssl) - 16(iv) = 1439
mod-mtu = 1439(mtu) & 0xfff0(complement) = 1424
tls-mtu = 1424(mod-mtu) - 8(cstp) - 48(mac) - 1(pad) = 1367
DTLS Block size = 16
mtu = 1500(base-mtu) - 20(ip) - 8(udp) - 13(dtlshdr) - 16(dtlsiv) = 1443
mod-mtu = 1443(mtu) & 0xfff0(complement) = 1440
dtls-mtu = 1440(mod-mtu) - 1(cdtp) - 20(mac) - 1(pad) = 1418
computed tls-mtu=1367 dtls-mtu=1418 conf-mtu=1406
DTLS enabled for intf=3 (outside)
overide computed dtls-mtu=1418 with conf-mtu=1406
tls-mtu=1367 dtls-mtu=1406
SVC: adding to sessmgmt
Sending X-CSTP-MTU: 1367
Sending X-DTLS-MTU: 1406
Sending X-CSTP-FW-RULE msgs: Start
Sending X-CSTP-FW-RULE msgs: Done
Sending X-CSTP-Quarantine: false
Sending X-CSTP-Disable-Always-On-VPN: false
Sending X-CSTP-Client-Bypass-Protocol: false

> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
ciscofp3> enable
Password: <hit enter>
ciscofp3# terminal monitor
ciscofp3# debug webvpn anyconnect 255
<hit Connect on Anyconnect client on PC>

http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: ciscofp3.cisco.com'
Processing CSTP header line: 'Host: ciscofp3.cisco.com'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 4.6.03049'
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 4.6.03049'
Setting user-agent to: 'Cisco AnyConnect VPN Agent for Windows 4.6.03049'
webvpn_cstp_parse_request_field()
```

```
...input: 'Cookie: webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
Processing CSTP header line: 'Cookie:
webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
Found WebVPN cookie: 'webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
WebVPN Cookie: 'webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Version: 1'
Processing CSTP header line: 'X-CSTP-Version: 1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Hostname: jsmith-PC'
Processing CSTP header line: 'X-CSTP-Hostname: jsmith-PC'
Setting hostname to: 'jsmith-PC'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-MTU: 1399'
Processing CSTP header line: 'X-CSTP-MTU: 1399'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv6,IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv6,IPv4'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Local-Address-IP4: 198.51.100.2'
Processing CSTP header line: 'X-CSTP-Local-Address-IP4: 198.51.100.2'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Base-MTU: 1500'
Processing CSTP header line: 'X-CSTP-Base-MTU: 1500'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Remote-Address-IP4: 203.0.113.2'
Processing CSTP header line: 'X-CSTP-Remote-Address-IP4: 203.0.113.2'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Full-IPv6-Capability: true'
Processing CSTP header line: 'X-CSTP-Full-IPv6-Capability: true'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret:
1FA92A96D5E82C13CB3A5758F11371EE6B54C6F36F0A8DCE8F4DECB73A034EEF4FE95DA614A5872E1EE5557C3BF4765A
'
Processing CSTP header line: 'X-DTLS-Master-Secret:
1FA92A96D5E82C13CB3A5758F11371EE6B54C6F36F0A8DCE8F4DECB73A034EEF4FE95DA614A5872E1EE5557C3BF4765A
'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-CipherSuite: DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-
SHA:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:AES256-SHA:AES128-
SHA:DES-CBC3-SHA'
Processing CSTP header line: 'X-DTLS-CipherSuite: DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-
SHA256:DHE-RSA-AES256-SHA:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-
SHA:AES256-SHA:AES128-SHA:DES-CBC3-SHA'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Accept-Encoding: lzs'
Processing CSTL header line: 'X-DTLS-Accept-Encoding: lzs'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Header-Pad-Length: 0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: lzs,deflate'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: lzs,deflate'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Processing CSTP header line: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
cstp_util_address_ipv4_accept: address asigned: 192.168.10.50
cstp_util_address_ipv6_accept: No IPv6 Address
np_svc_create_session(0x7000, 0x00002acdff1d6440, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
vpn_put_uauth success for ip 192.168.10.50!
No SVC ACL
Iphdr=20 base-mtu=1500 def-mtu=1500 conf-mtu=1406
```

```
tcp-mss = 1460
path-mtu = 1460(mss)
TLS Block size = 16, version = 0x303
mtu = 1460(path-mtu) - 0(opts) - 5(ssl) - 16(iv) = 1439
mod-mtu = 1439(mtu) & 0xfff0(complement) = 1424
tls-mtu = 1424(mod-mtu) - 8(cstp) - 48(mac) - 1(pad) = 1367
DTLS Block size = 16
mtu = 1500(base-mtu) - 20(ip) - 8(udp) - 13(dtlshdr) - 16(dtlsiv) = 1443
mod-mtu = 1443(mtu) & 0xfff0(complement) = 1440
dtls-mtu = 1440(mod-mtu) - 1(cdtp) - 20(mac) - 1(pad) = 1418
computed tls-mtu=1367 dtls-mtu=1418 conf-mtu=1406
DTLS enabled for intf=3 (outside)
overide computed dtls-mtu=1418 with conf-mtu=1406
tls-mtu=1367 dtls-mtu=1406
SVC: adding to sessmgmt
Sending X-CSTP-MTU: 1367
Sending X-DTLS-MTU: 1406
Sending X-CSTP-FW-RULE msgs: Start
Sending X-CSTP-FW-RULE msgs: Done
Sending X-CSTP-Quarantine: false
Sending X-CSTP-Disable-Always-On-VPN: false
Sending X-CSTP-Client-Bypass-Protocol: false
```

ISE CLI :

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
ciscofp3> enable
Password: <hit enter>
ciscofp3# terminal monitor
ciscofp3# debug webvpn anyconnect 255
<hit Connect on Anyconnect client on PC>

http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: ciscofp3.cisco.com'
Processing CSTP header line: 'Host: ciscofp3.cisco.com'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 4.6.03049'
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 4.6.03049'
Setting user-agent to: 'Cisco AnyConnect VPN Agent for Windows 4.6.03049'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
Processing CSTP header line: 'Cookie:
webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
Found WebVPN cookie: 'webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
WebVPN Cookie: 'webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Version: 1'
Processing CSTP header line: 'X-CSTP-Version: 1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Hostname: jsmith-PC'
Processing CSTP header line: 'X-CSTP-Hostname: jsmith-PC'
Setting hostname to: 'jsmith-PC'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-MTU: 1399'
Processing CSTP header line: 'X-CSTP-MTU: 1399'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv6,IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv6,IPv4'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Local-Address-IP4: 198.51.100.2'
```

```
Processing CSTP header line: 'X-CSTP-Local-Address-IP4: 198.51.100.2'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Base-MTU: 1500'
Processing CSTP header line: 'X-CSTP-Base-MTU: 1500'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Remote-Address-IP4: 203.0.113.2'
Processing CSTP header line: 'X-CSTP-Remote-Address-IP4: 203.0.113.2'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Full-IPv6-Capability: true'
Processing CSTP header line: 'X-CSTP-Full-IPv6-Capability: true'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret:
1FA92A96D5E82C13CB3A5758F11371EE6B54C6F36F0A8DCE8F4DECB73A034EEF4FE95DA614A5872E1EE5557C3BF4765A
'
Processing CSTP header line: 'X-DTLS-Master-Secret:
1FA92A96D5E82C13CB3A5758F11371EE6B54C6F36F0A8DCE8F4DECB73A034EEF4FE95DA614A5872E1EE5557C3BF4765A
'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-CipherSuite: DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-
SHA:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:AES256-SHA:AES128-
SHA:DES-CBC3-SHA'
Processing CSTP header line: 'X-DTLS-CipherSuite: DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-
SHA256:DHE-RSA-AES256-SHA:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-
SHA:AES256-SHA:AES128-SHA:DES-CBC3-SHA'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Accept-Encoding: lzs'
Processing CSTL header line: 'X-DTLS-Accept-Encoding: lzs'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Header-Pad-Length: 0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: lzs,deflate'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: lzs,deflate'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Processing CSTP header line: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
cstp_util_address_ipv4_accept: address asigned: 192.168.10.50
cstp_util_address_ipv6_accept: No IPv6 Address
np_svc_create_session(0x7000, 0x00002acdff1d6440, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
vpn_put_uauth success for ip 192.168.10.50!
No SVC ACL
Iphdr=20 base-mtu=1500 def-mtu=1500 conf-mtu=1406
tcp-mss = 1460
path-mtu = 1460(mss)
TLS Block size = 16, version = 0x303
mtu = 1460(path-mtu) - 0(opts) - 5(ssl) - 16(iv) = 1439
mod-mtu = 1439(mtu) & 0xfff0(complement) = 1424
tls-mtu = 1424(mod-mtu) - 8(cstp) - 48(mac) - 1(pad) = 1367
DTLS Block size = 16
mtu = 1500(base-mtu) - 20(ip) - 8(udp) - 13(dtlshdr) - 16(dtlsiv) = 1443
mod-mtu = 1443(mtu) & 0xfff0(complement) = 1440
dtls-mtu = 1440(mod-mtu) - 1(cdtp) - 20(mac) - 1(pad) = 1418
computed tls-mtu=1367 dtls-mtu=1418 conf-mtu=1406
DTLS enabled for intf=3 (outside)
overide computed dtls-mtu=1418 with conf-mtu=1406
tls-mtu=1367 dtls-mtu=1406
SVC: adding to sessmgmt
Sending X-CSTP-MTU: 1367
Sending X-DTLS-MTU: 1406
Sending X-CSTP-FW-RULE msgs: Start
Sending X-CSTP-FW-RULE msgs: Done
Sending X-CSTP-Quarantine: false
```

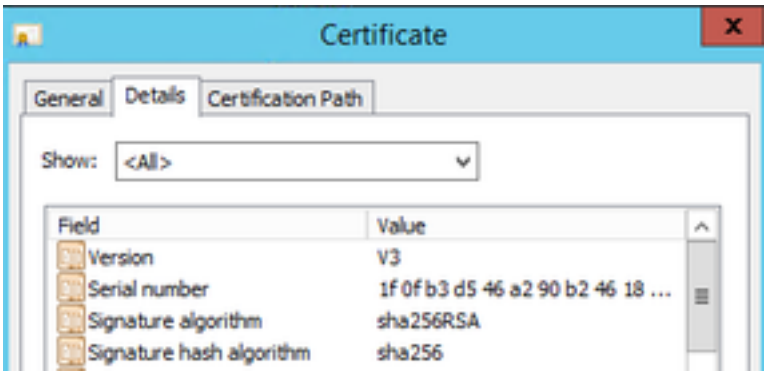
```
Sending X-CSTP-Disable-Always-On-VPN: false
Sending X-CSTP-Client-Bypass-Protocol: false
```

Windows Server 2012

Lancez une invite de commande, et assurez-vous que vous pouvez exécuter un « nslookup » sur le hostname/FQDN du FTD

Point fort de certificat (pour la compatibilité de navigateur)

Vérifiez les Certificats de signes des Windows Server 2012 comme SHA256 ou plus élevé. Double-cliquer votre certificat de CA de racine dans Windows et vérifiez les champs « d'algorithme de signature »



S'ils sont SHA1, la plupart des navigateurs afficheront un avertissement de navigateur pour ces Certificats. Pour le changer, vous pouvez vérifier ici :

Comment améliorer l'autorité de certification de Windows Server à SHA256

Vérifiez le certificat de serveur VPN FTD a les champs suivants corrects (quand vous vous connectez en navigateur à FTD)

Nom commun = <FTDFQDN>

Nom alternatif soumis (SAN) = <FTDFQDN>

Exemple :

Nom commun : **ciscofp3.cisco.com**

Nom alternatif soumis (SAN) : **DN Name=cicscofp3.cisco.com**

Configuration de Connectivité et de Pare-feu

Vérifiez utilisant des captures sur FTD CLI et des captures sur le PC des employés utilisant Wireshark pour vérifier que les paquets sont livré au-dessus de TCP+UDP 443 à l'IP extérieur du FTD. Vérifiez que ces paquets sont originaires de l'adresse IP publique du routeur domestique des employés

```
ciscofp3# capture capin interface outside trace detail trace-count 100 match ip any host
<enduser'sPublicIPAddress>
<now hit Connect on AnyConnect Client from employee PC>
ciscofp3# show cap
```

```
capture capin type raw-data trace detail trace-count 100 interface outside [Buffer Full - 524153 bytes]
match ip any host 198.51.100.2

ciscofp3# show cap capin
2375 packets captured
1: 17:05:56.580994 198.51.100.2.55928 > 203.0.113.2.443: S 2933933902:2933933902(0) win 8192
<mss 1460,nop,wscale 8,nop,nop,sackOK>
2: 17:05:56.581375 203.0.113.2.443 > 198.51.100.2.55928: S 430674106:430674106(0) ack 2933933903
win 32768 <mss 1460>
3: 17:05:56.581757 198.51.100.2.55928 > 203.0.113.2.443: . ack 430674107 win 64240
...
```