Configurer le tunnel VPN de gestion d’AnyConnect sur l’ASA

Table des matières

Introduction

Ce document décrit la configuration de l'ASA comme passerelle VPN accepte les connexions du client AnyConnect Secure Mobility via le tunnel VPN de gestion.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration VPN via Adaptive Security Device Manager (ASDM)
- Configuration de base de l'interface de ligne de commande ASA
- Certificats X509

Composants utilisés

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

- Logiciel Cisco ASA version 9.12(3)9

- Logiciel Cisco ASDM version 7.12.2
- Windows 10 avec Cisco AnyConnect Secure Mobility Client version 4.8.03036

Remarque : téléchargez le package de déploiement Web AnyConnect VPN (anyconnect-win*.pkg or anyconnect-macos*.pkg) à partir de la page Cisco Software Download (clients enregistrés uniquement). Copiez le client VPN AnyConnect dans la mémoire flash de l'ASA qui doit être téléchargé sur les ordinateurs des utilisateurs distants pour établir la connexion VPN SSL avec l'ASA. Référez-vous à la section Installation du client AnyConnect du guide de configuration ASA pour plus d'informations.

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

Informations générales

Un tunnel VPN de gestion assure la connectivité au réseau d'entreprise chaque fois que le système client est mis sous tension, et pas seulement lorsqu'une connexion VPN est établie par l'utilisateur final. Vous pouvez effectuer la gestion des correctifs sur les terminaux hors du bureau, en particulier les périphériques qui sont rarement connectés par l'utilisateur, via un VPN, au réseau du bureau. Les scripts de connexion au système d'exploitation des terminaux qui nécessitent une connectivité réseau d'entreprise bénéficient également de cette fonctionnalité.

AnyConnect Management Tunnel permet aux administrateurs de connecter AnyConnect sans intervention de l'utilisateur avant la connexion de l'utilisateur. Le tunnel de gestion AnyConnect peut fonctionner en association avec la détection de réseau sécurisé et n'est donc déclenché que lorsque le terminal est hors site et déconnecté d'un VPN initié par l'utilisateur. Le tunnel de gestion AnyConnect est transparent pour l'utilisateur final et se déconnecte automatiquement lorsque l'utilisateur lance le VPN.

SE/Application	Version minimale requise
ASA	9.0.1
ASDM	7.10.1
Version de Windows AnyConnect	4.7.00136
Version de macOS AnyConnect	4.7.01076
Linux	Non Pris En Charge

Fonctionnement du tunnel de gestion

Le service d'agent VPN AnyConnect est automatiquement démarré au démarrage du système. Il détecte que la fonctionnalité de tunnel de gestion est activée (via le profil VPN de gestion), par conséquent il lance l'application cliente de gestion pour initier une connexion de tunnel de gestion. L'application cliente de gestion utilise l'entrée d'hôte du profil VPN de gestion pour initier la

connexion. Ensuite, le tunnel VPN est établi comme d'habitude, à une exception près : aucune mise à jour logicielle n'est effectuée pendant une connexion de tunnel de gestion puisque le tunnel de gestion est censé être transparent pour l'utilisateur.

L'utilisateur lance un tunnel VPN via l'interface utilisateur AnyConnect, ce qui déclenche la fin du tunnel de gestion. À la fin du tunnel de gestion, l'établissement du tunnel utilisateur se poursuit comme d'habitude.

L'utilisateur déconnecte le tunnel VPN, ce qui déclenche le rétablissement automatique du tunnel de gestion.

Limites

- Interaction utilisateur non prise en charge
- L'authentification basée sur les certificats via le magasin de certificats de l'ordinateur (Windows) est uniquement prise en charge
- Vérification stricte du certificat du serveur
- Un proxy privé n'est pas pris en charge
- Un proxy public n'est pas pris en charge (la valeur ProxyNative est prise en charge sur les plates-formes où les paramètres du proxy natif ne sont pas récupérés du navigateur)
- Les scripts de personnalisation AnyConnect ne sont pas pris en charge

---

Remarque : pour plus d'informations, reportez-vous à A propos du tunnel VPN de gestion.

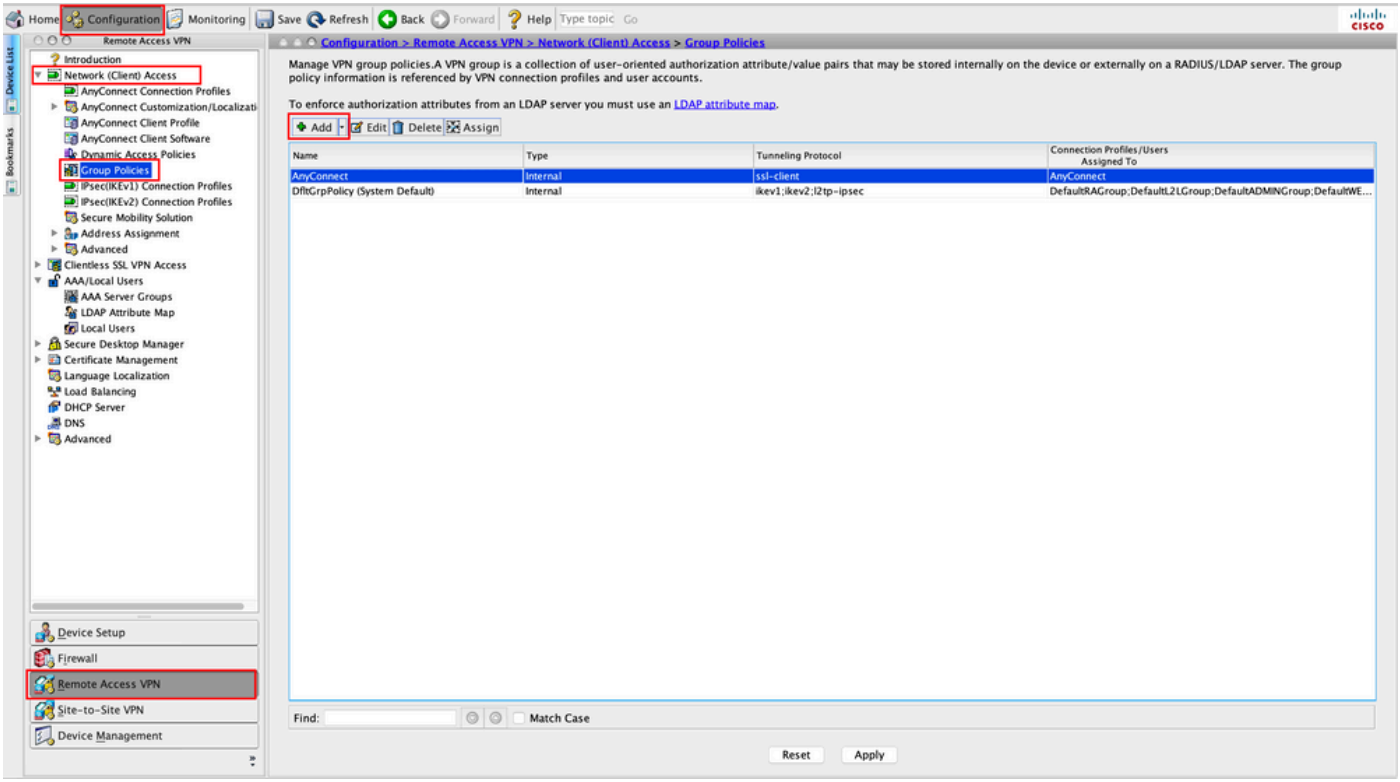
Configurer

Cette section décrit comment configurer Cisco ASA en tant que passerelle VPN pour accepter les connexions des clients AnyConnect via le tunnel VPN de gestion.

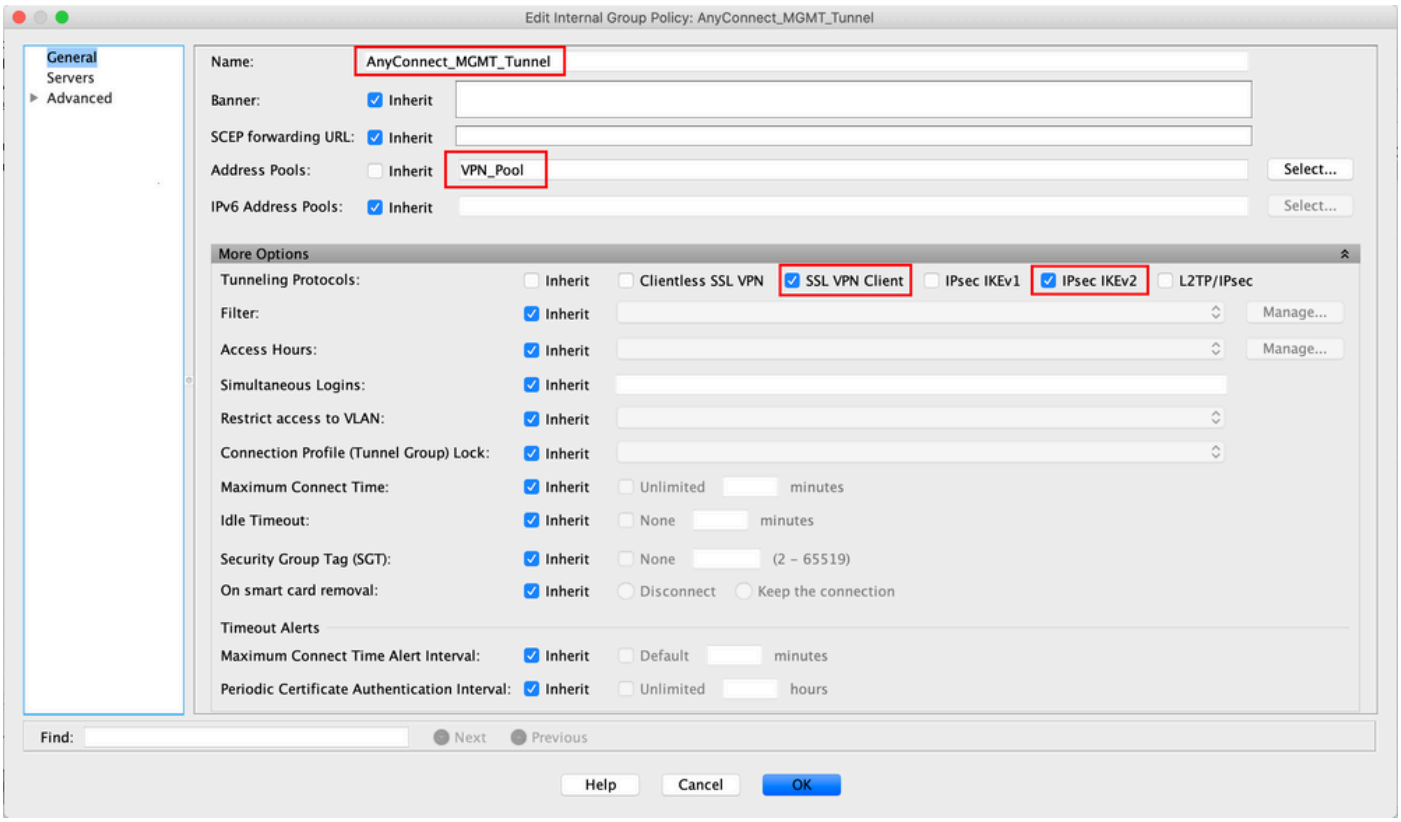
Configuration sur ASA via ASDM/CLI

Étape 1. Créez la stratégie de groupe AnyConnect. Accédez à`Configuration > Remote Access VPN > Network (Client) Access > Group Policies`. Cliquez sur`Add`.

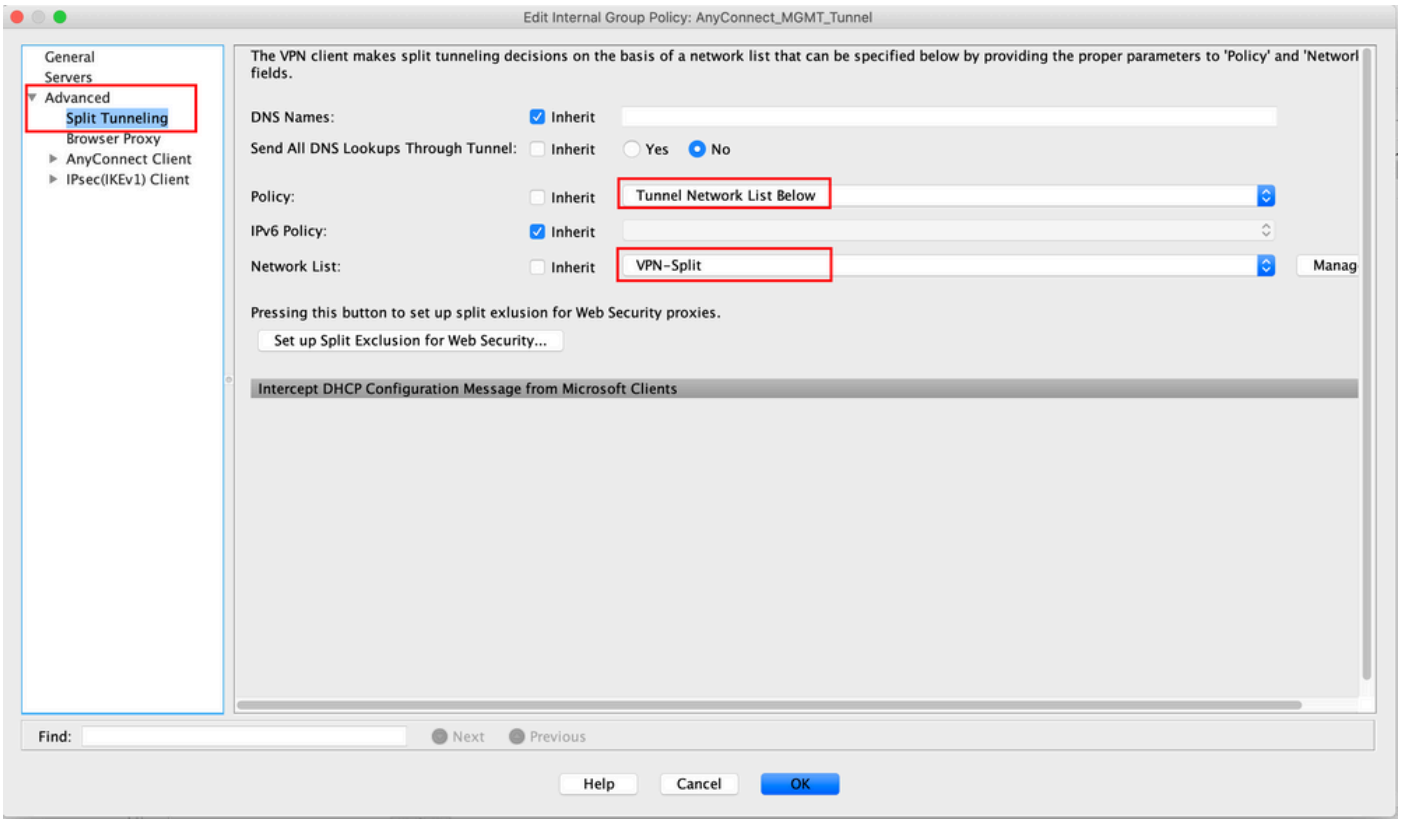
Remarque : il est conseillé de créer une nouvelle stratégie de groupe AnyConnect qui est utilisée pour le tunnel de gestion AnyConnect uniquement.



Étape 2. Fournissez uneNamebase pour la stratégie de groupe. Attribuer/Créer unAddress Pool. ChoisissezTunneling ProtocolsasSSL VPN Clientet/ouIPsec IKEv2, comme illustré dans l'image.

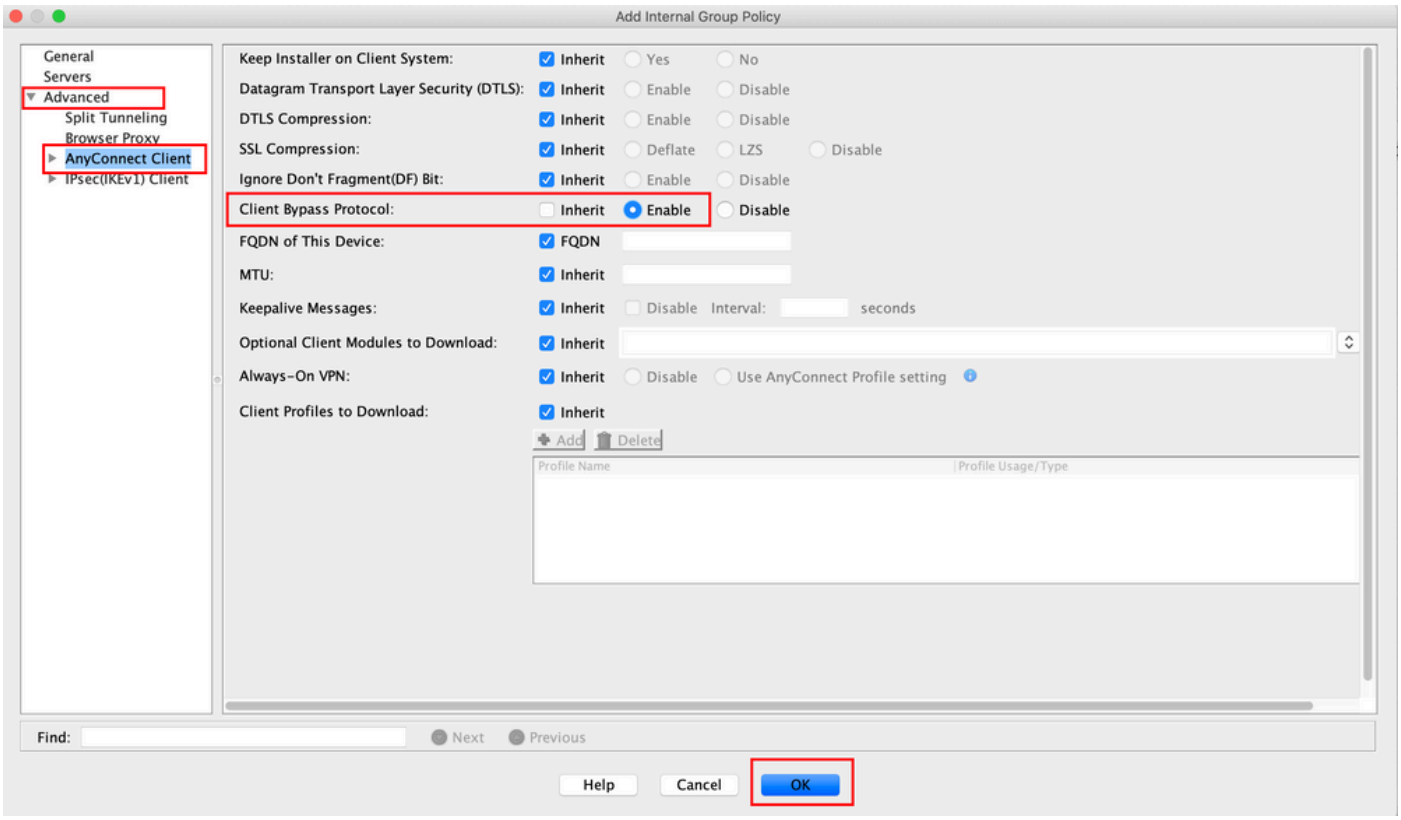


Étape 3. Accédez àAdvanced > Split Tunneling. Configurez lePolicyen tant queTunnel Network List Belowet choisissez leNetwork List, comme illustré dans l'image.

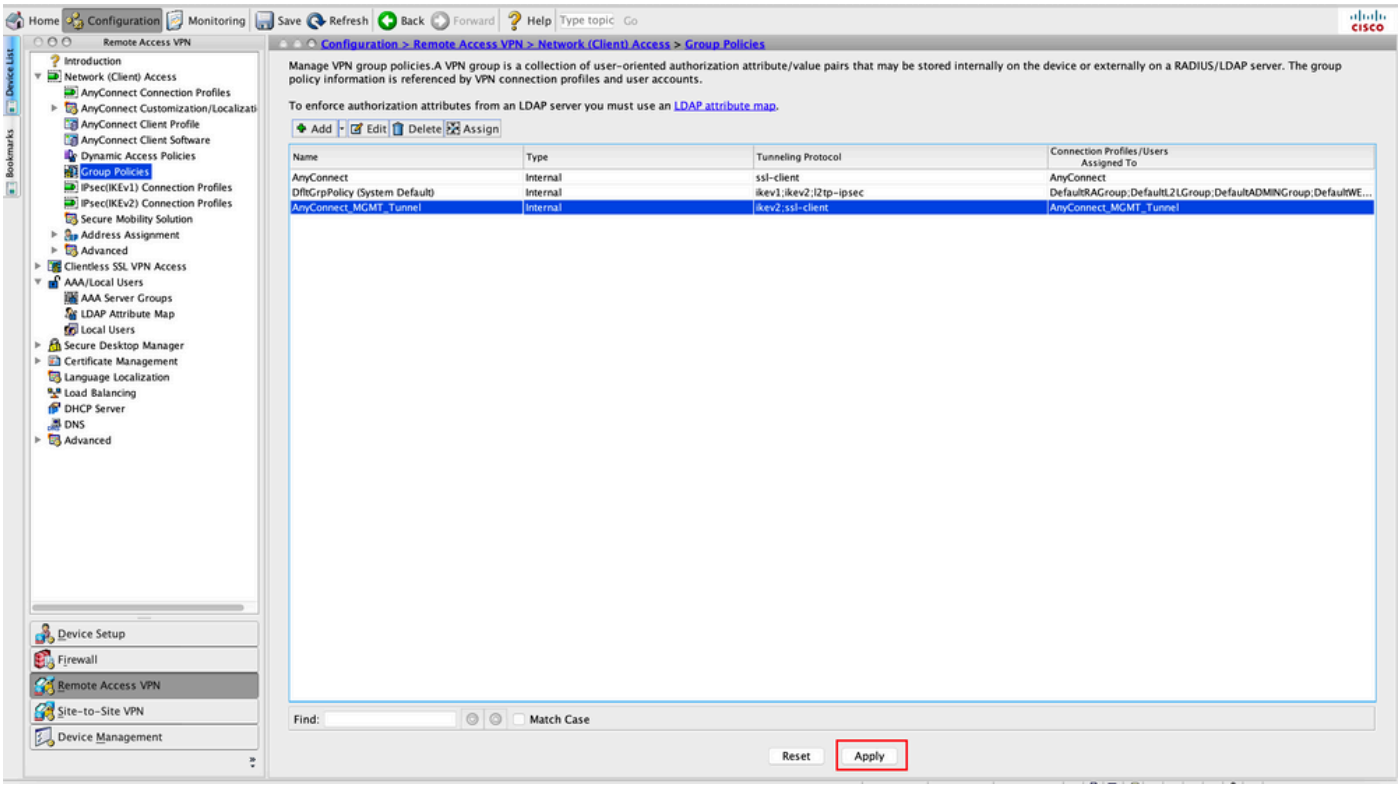


Remarque : si une adresse de client n'est pas transmise pour les deux protocoles IP (IPv4 et IPv6), le paramètre doit êtreClient Bypass Protocolenableddéfini de sorte que le trafic correspondant ne soit pas perturbé par le tunnel de gestion. Pour configurer, reportez-vous à l'étape 4.

Étape 4. Accédez àAdvanced > AnyConnect Client. DéfiniClient Bypass ProtocolsurEnable. Cliquez surOKSave (Enregistrer), comme illustré dans l'image.



Étape 5. Comme le montre cette image, cliquez surApplypour transmettre la configuration à l'ASA.



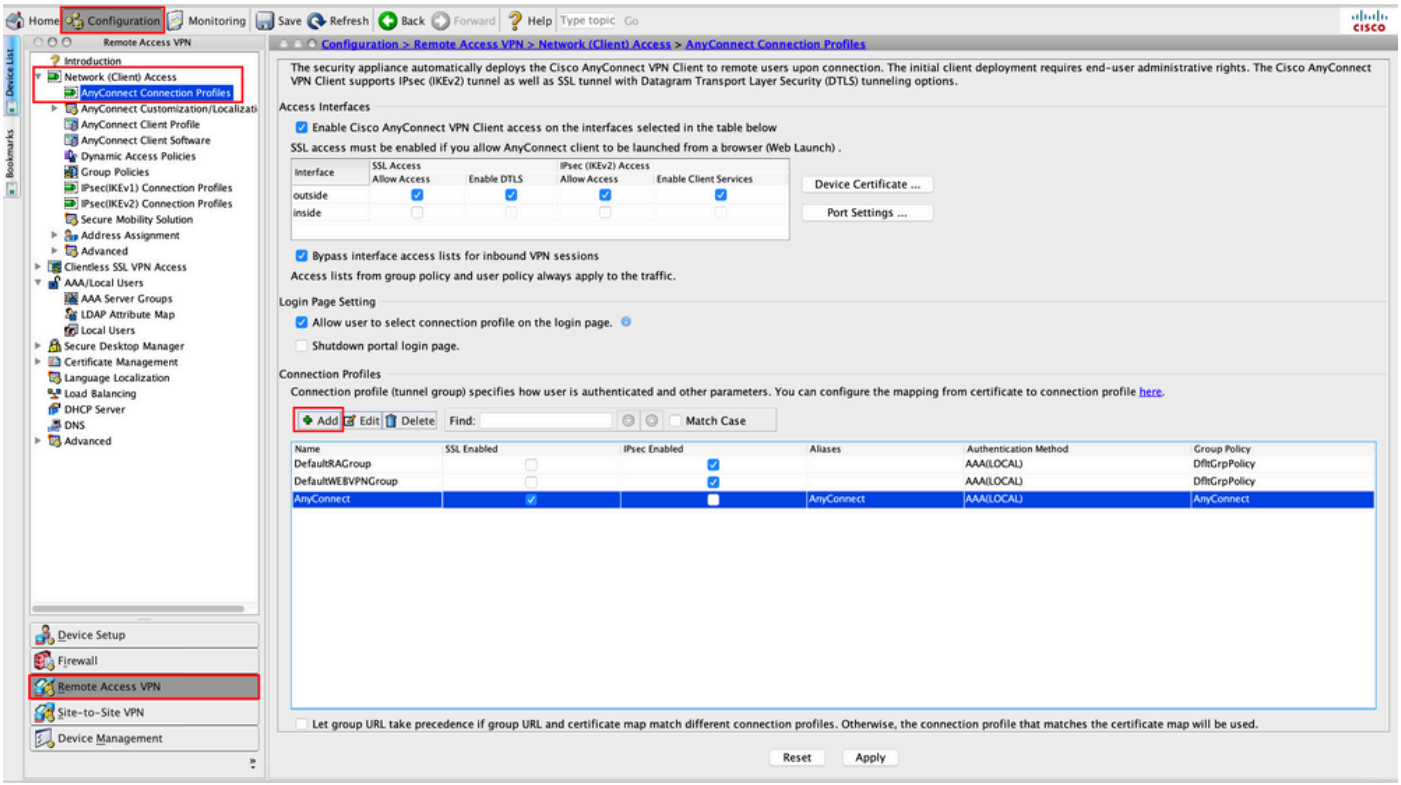
Configuration CLI pour la stratégie de groupe :

```
<#root>

ip local pool

VPN_Pool

 192.168.10.1-192.168.10.100 mask 255.255.255.0
!
access-list

VPN-Split

 standard permit 172.16.0.0 255.255.0.0
!
group-policy

AnyConnect_MGMT_Tunnel

 internal
group-policy

AnyConnect_MGMT_Tunnel

 attributes
 vpn-tunnel-protocol

ikev2 ssl-client


 split-tunnel-network-list value

VPN-Split
```

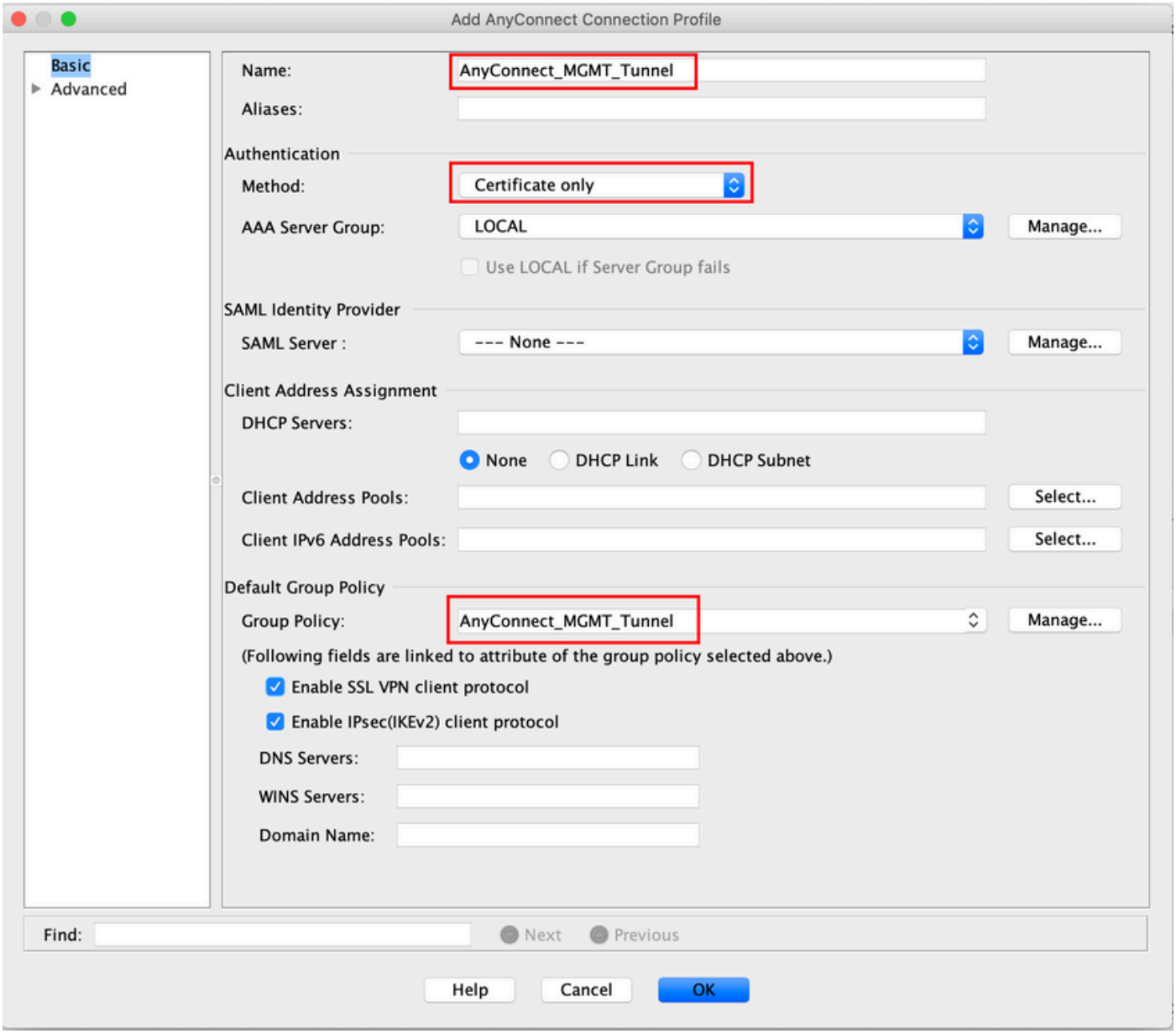
```
client-bypass-protocol enable
address-pools value
VPN_Pool
```

Étape 6. Créez le profil de connexion AnyConnect. Accédez àConfiguration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profile. Cliquez surAdd.

Remarque : il est conseillé de créer un nouveau profil de connexion AnyConnect, utilisé uniquement pour le tunnel de gestion AnyConnect.



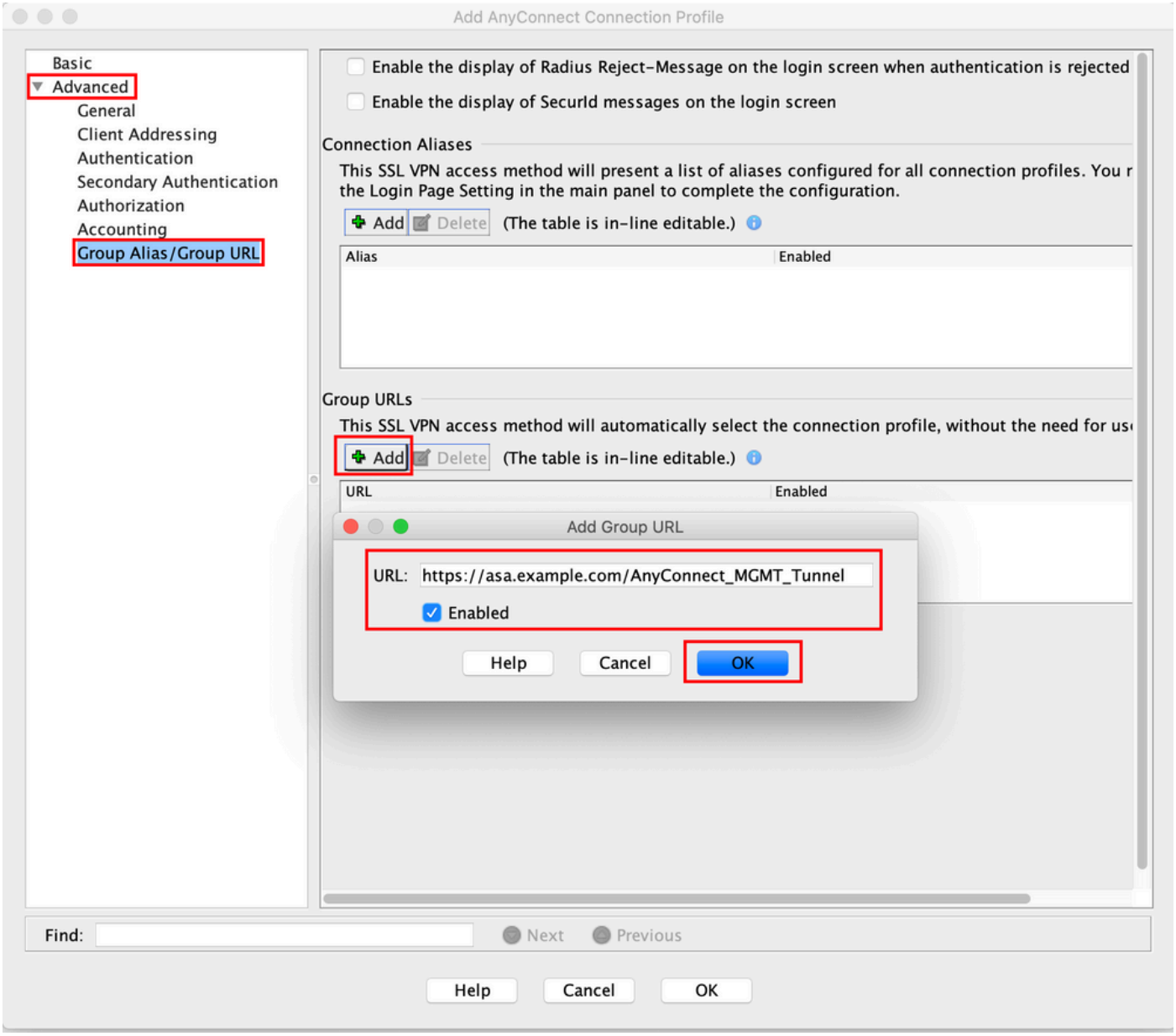
Étape 7. Fournissez unNamepour le profil de connexion et définissez-leAuthentication MethodsurCertificate only. Sélectionnez laGroup Policycomme celle créée à l'étape 1.



Remarque : assurez-vous que le certificat racine de l'autorité de certification locale est présent sur l'ASA. Accédez àConfiguration > Remote Access VPN > Certificate Management > CA Certificatespour ajouter/afficher le certificat.

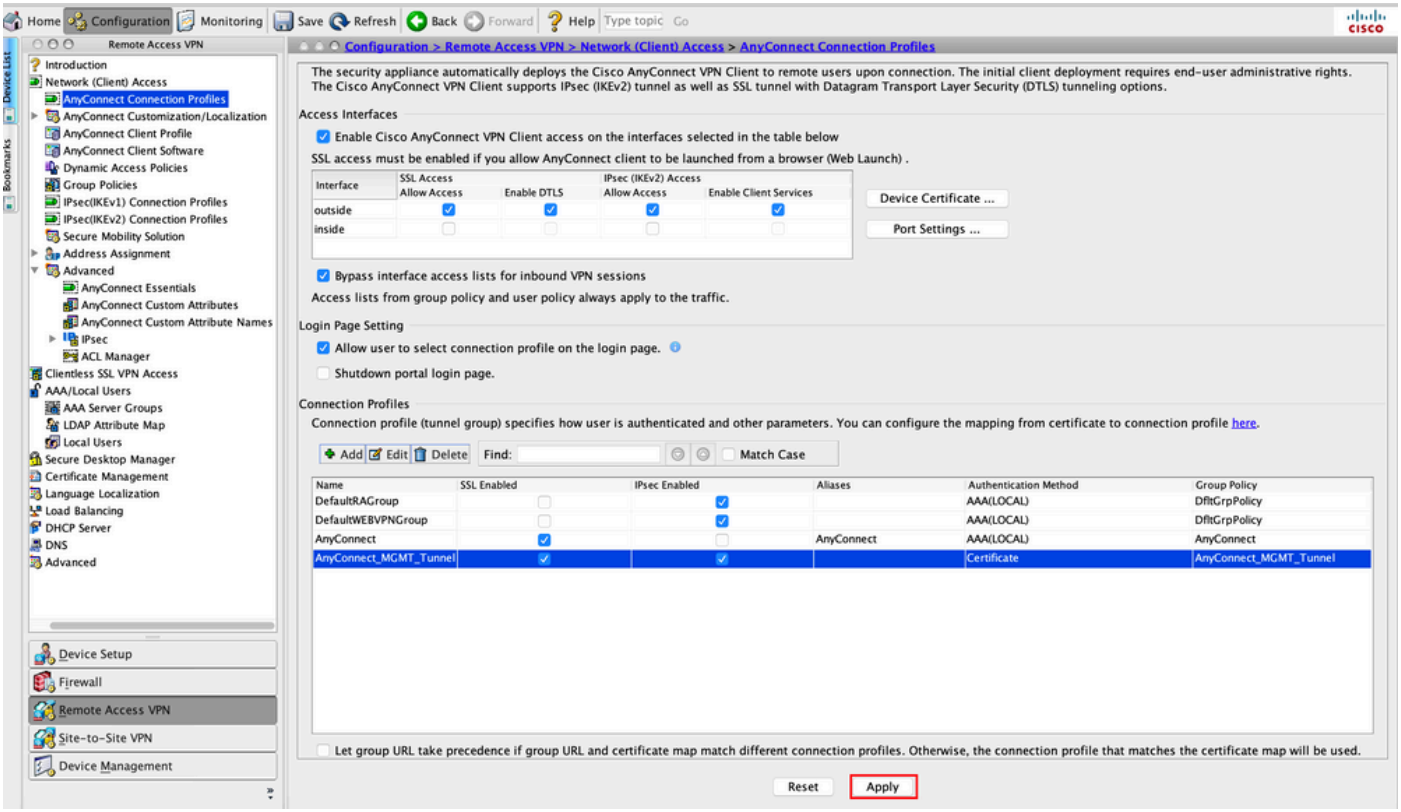
Remarque : vérifiez qu'un certificat d'identité émis par la même autorité de certification locale existe dans le magasin de certificats de l'ordinateur (pour Windows) et/ou dans la chaîne de clés système (pour macOS).

Étape 8. Accédez àAdvanced > Group Alias/Group URL. CliquezAddsousGroup URLset ajoutez unURL. Assurez-vous queEnabledest coché. Cliquez surOKSave (Enregistrer), comme illustré dans l'image.



Si IKEv2 est utilisé, assurez-vous queIPsec (IKEv2) Accessest activé sur l'interface utilisée pour AnyConnect.

Étape 9. Cliquez surApplypour transmettre la configuration à l'ASA.

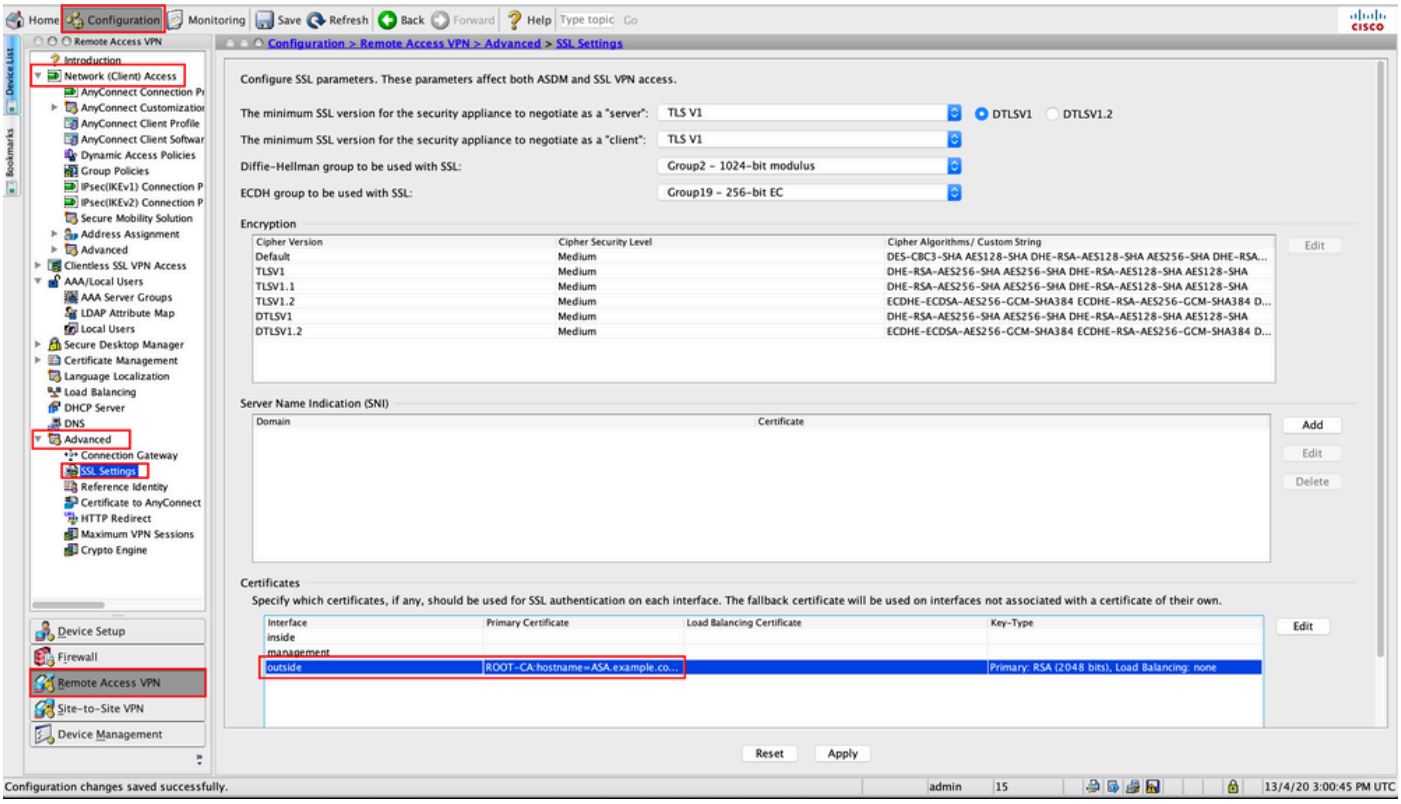


Configuration CLI pour le profil de connexion (tunnel-group) :

```
<#root>

tunnel-group

AnyConnect_MGMT_Tunnel

 type remote-access
tunnel-group

AnyConnect_MGMT_Tunnel

 general-attributes

 default-group-policy AnyConnect_MGMT_Tunnel

tunnel-group AnyConnect_MGMT_Tunnel webvpn-attributes

 authentication certificate
 group-url https://asa.example.com/AnyConnect_MGMT_Tunnel enable
```

Étape 10. Assurez-vous qu'un certificat sécurisé est installé sur l'ASA et lié à l'interface utilisée pour les connexions AnyConnect. Accédez à pourConfiguration > Remote Access VPN > Advanced > SSL Settingsajouter/afficher ce paramètre.

Remarque : reportez-vous à Installation of Identity Certificate on ASA.

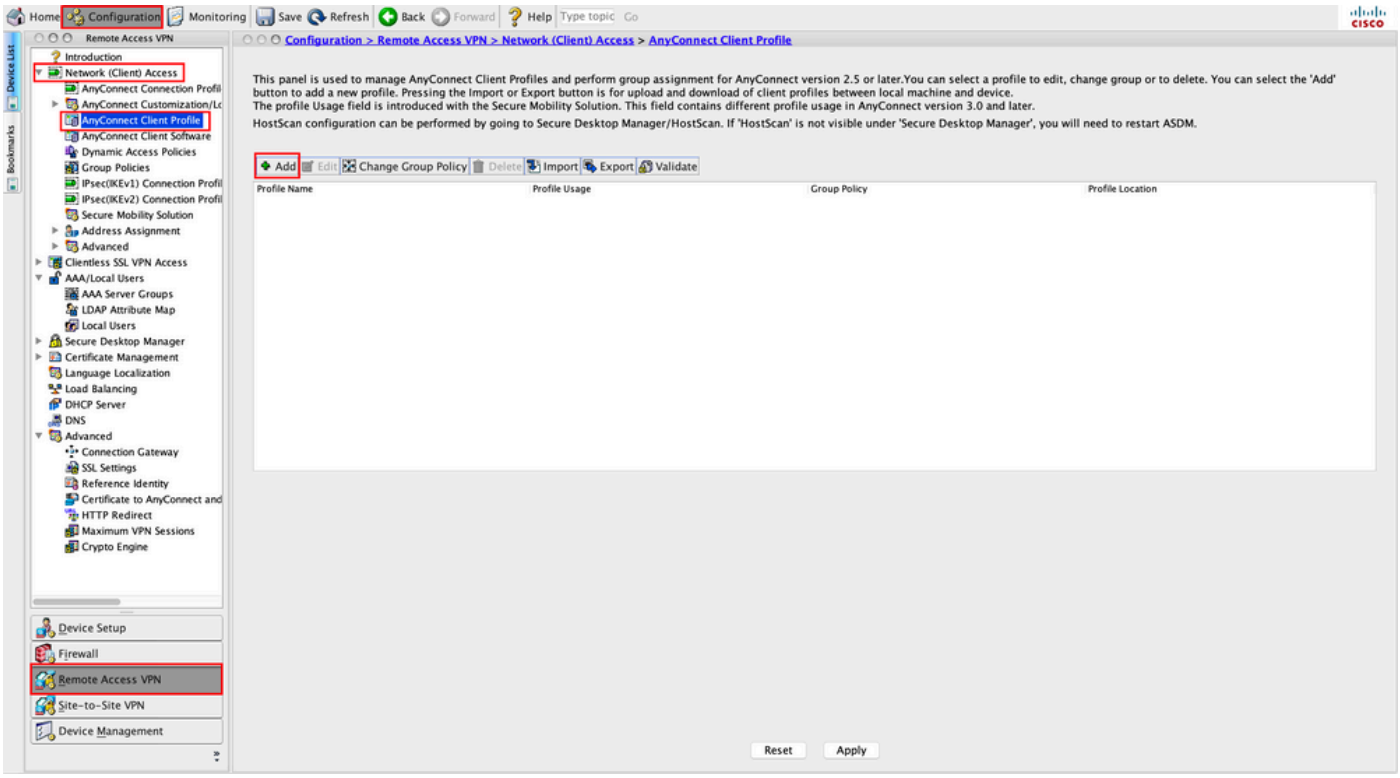


Configuration CLI pour le point de confiance SSL :

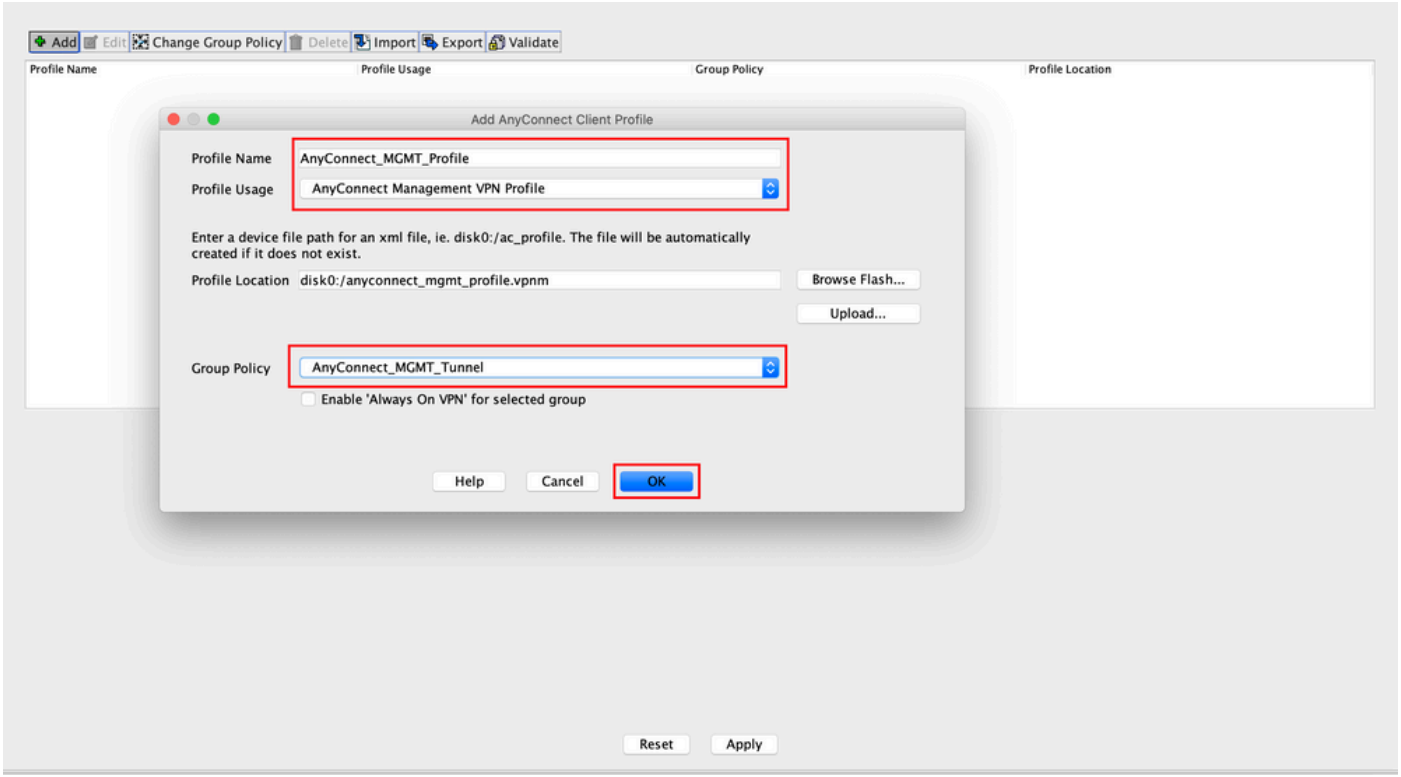
```
<#root>

ssl trust-point ROOT-CA outside
```

Création du profil VPN de gestion AnyConnect

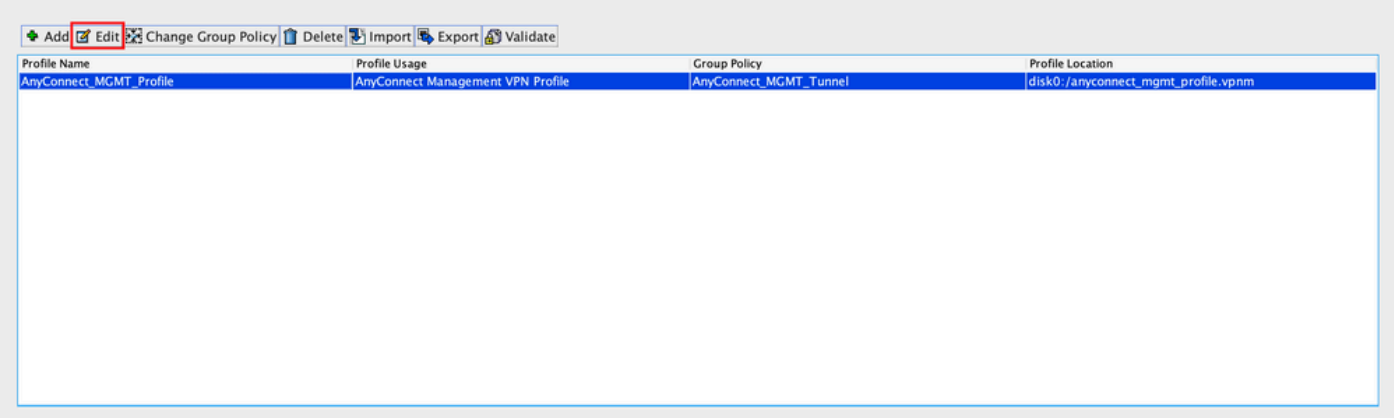
Étape 1. Créez le profil client AnyConnect. Accédez àConfiguration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile. Cliquez surAdd, comme illustré dans l'image.



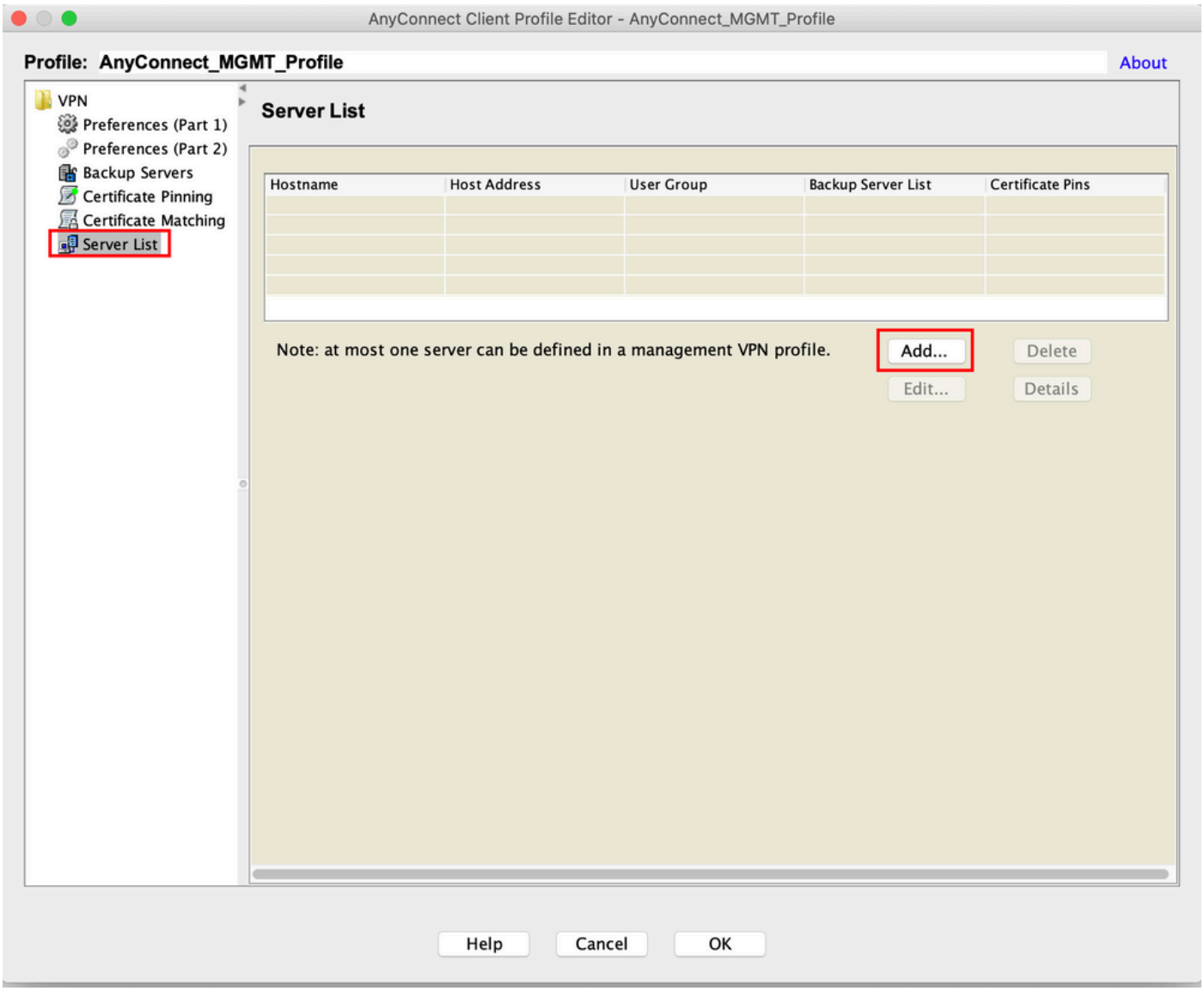
Étape 2. Fournissez unProfile Name. Sélectionnez leProfile UsagecommeAnyConnect Management VPN profile. Sélectionnez leGroup Policyqui a été créé à l'étape 1. Cliquez surOK, comme illustré dans l'image.



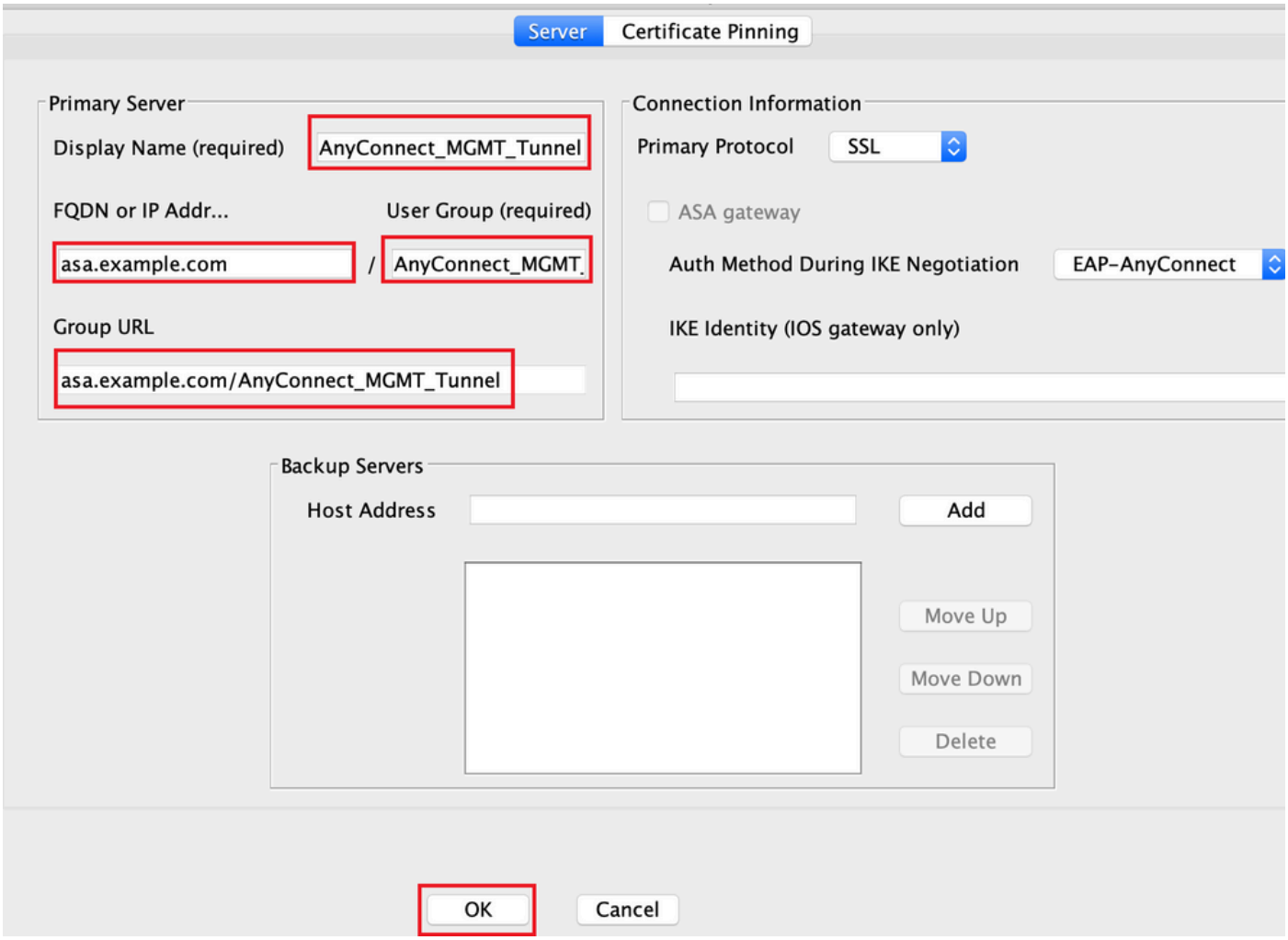
Étape 3. Choisissez le profil créé et cliquez sur Edit, comme indiqué dans l'image.



Étape 4. Accédez à Server List. CliquezAdd pour ajouter une nouvelle entrée de liste de serveurs, comme illustré dans l'image.



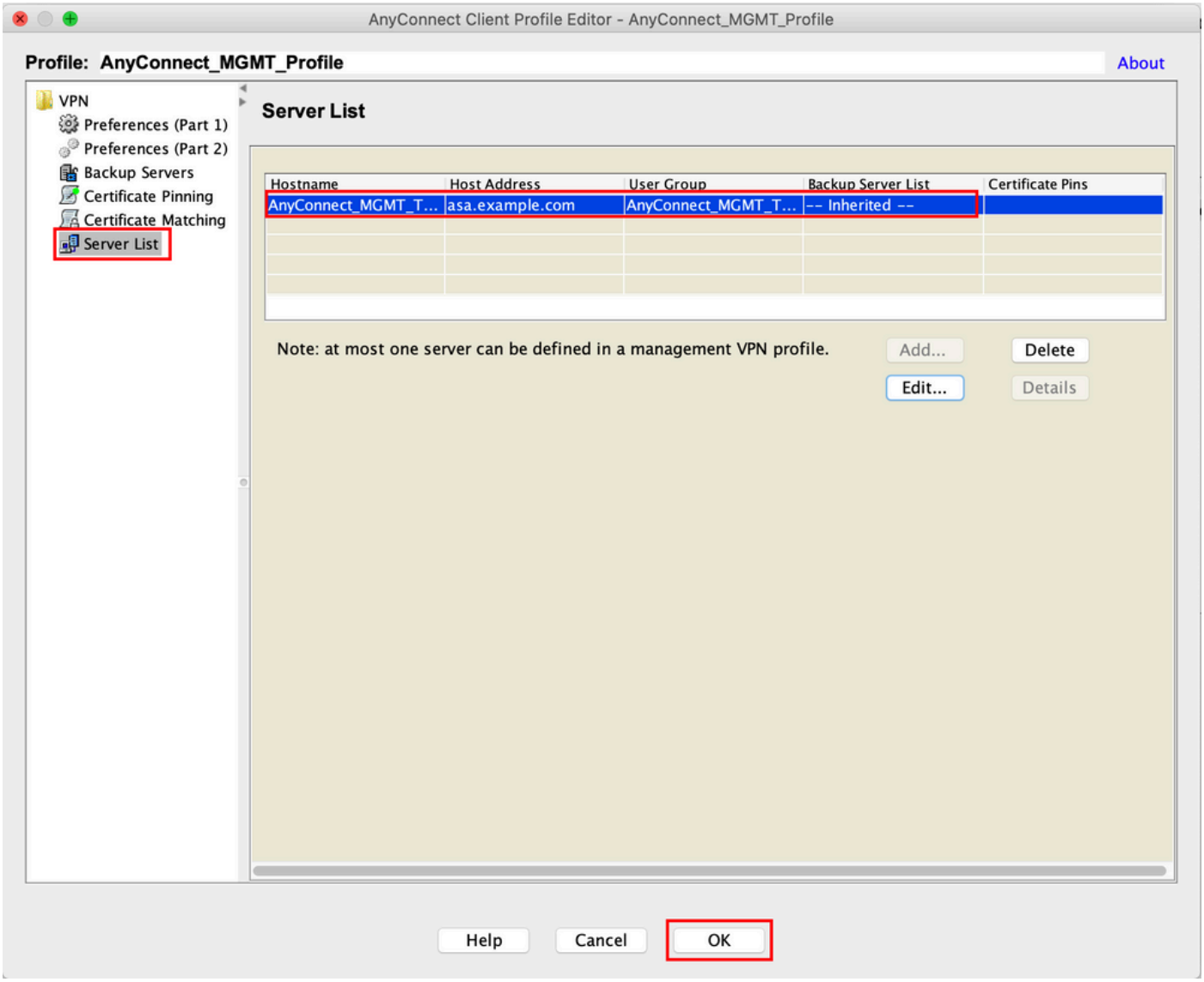
Étape 5. Fournissez unDisplay Name. Ajoutez leFQDN/IP addressde l'ASA. Fournissez leUser Groupcomme nom du groupe de tunnels.Group URLest automatiquement renseigné avec leFQDNet leUser Group. Cliquez surOK.



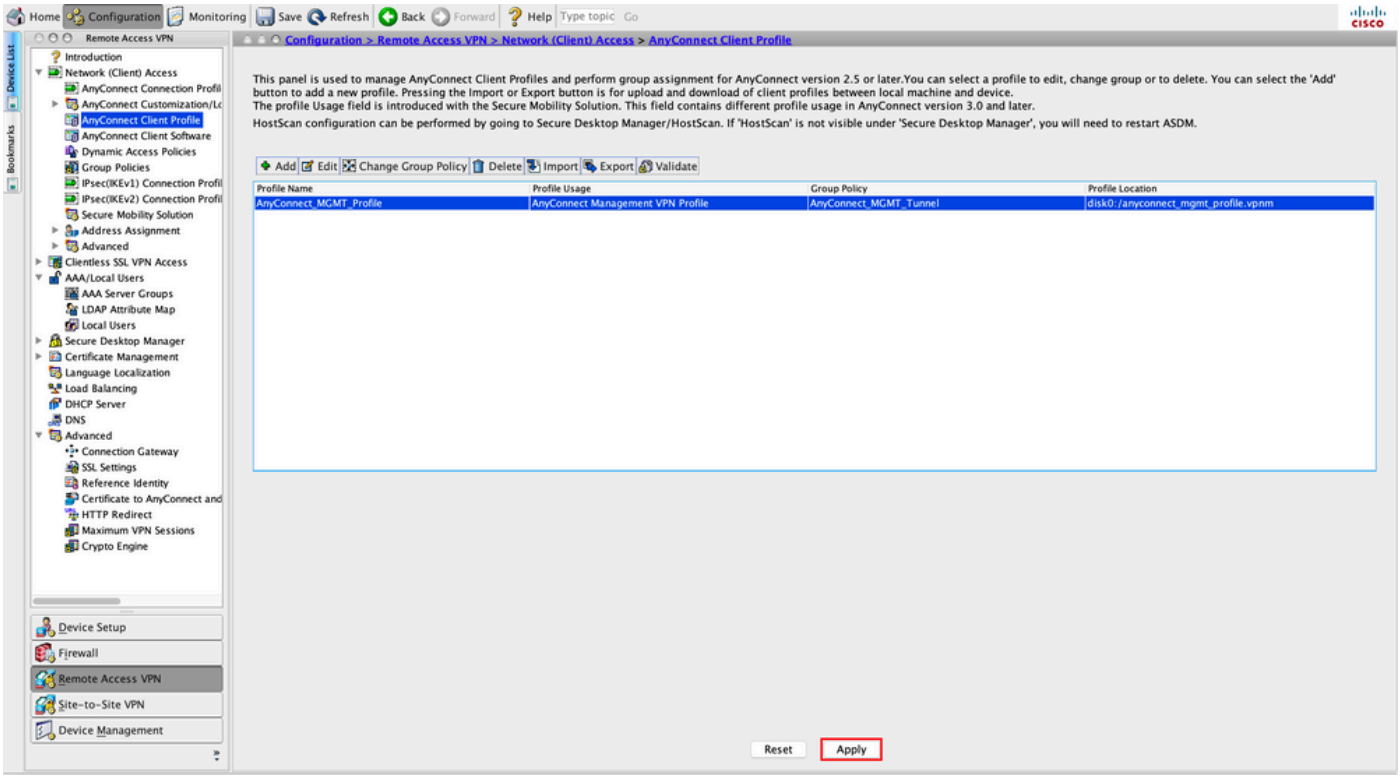
Remarque : le nom de domaine complet/adresse IP + groupe d'utilisateurs doit être identique à l'URL du groupe mentionnée lors de la configuration du profil de connexion AnyConnect à l'étape 8.

Remarque : AnyConnect avec IKEv2 en tant que protocole peut également être utilisé pour établir un VPN de gestion vers ASA. Assurez-vousPrimary Protocolque est défini surIPsecà l'étape 5.

Étape 6. Comme le montre l'image, cliquez surOKEnregistrer.



Étape 7. Cliquez surApplypour envoyer la configuration à l'ASA, comme illustré dans l'image.



Configuration CLI après l'ajout du profil VPN de gestion AnyConnect.

```
<#root>
webvpn

 enable outside
 hsts
  enable
  max-age 31536000
  include-sub-domains
  no preload
 no anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1

 anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm

 anyconnect enable
 tunnel-group-list enable
 cache
  disable
 error-recovery disable
!
group-policy AnyConnect_MGMT_Tunnel internal

group-policy AnyConnect_MGMT_Tunnel attributes

 vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-network-list value VPN-Split
 client-bypass-protocol enable
 address-pools value VPN_Pool


webvpn

  anyconnect profiles value AnyConnect_MGMT_Profile type vpn-mgmt
```

Profil VPN de gestion AnyConnect sur la machine cliente AnyConnect :

<#root>

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSc
    <ClientInitialization>
        <UseStartBeforeLogon UserControllable="false">false</UseStartBeforeLogon>
```

true

```
  <ShowPreConnectMessage>false</ShowPreConnectMessage>
```

Machine

System

true

```
        <ProxySettings>IgnoreProxy</ProxySettings>
        <AllowLocalProxyConnections>true</AllowLocalProxyConnections>
        <AuthenticationTimeout>30</AuthenticationTimeout>

--- Output Omitted ---

        <CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
        <AllowManualHostInput>false</AllowManualHostInput>
    </ClientInitialization>
```

AnyConnect_MGMT_Tunnel

asa.example.com

```
        AnyConnect_MGMT_Tunnel

</AnyConnectProfile>
```

Remarque : si le protocole TND (Trusted Network Detection) est utilisé dans le profil VPN AnyConnect de l'utilisateur, il est conseillé de faire correspondre les mêmes paramètres dans le profil VPN de gestion pour une expérience utilisateur cohérente. Le tunnel VPN de gestion est déclenché en fonction des paramètres TND appliqués au profil de tunnel VPN utilisateur. En outre, l'action TND Connect dans le profil VPN de gestion (appliquée uniquement lorsque le tunnel VPN de gestion est actif), s'applique toujours au tunnel VPN de l'utilisateur, afin de garantir que le tunnel VPN de gestion est transparent pour l'utilisateur final.

Remarque : sur tout PC d'utilisateur final, si les paramètres TND sont activés sur le profil VPN de gestion et si le profil VPN d'utilisateur est manquant, il considère les paramètres de préférences par défaut pour le TND (il est désactivé sur les préférences par défaut dans l'application cliente AC) à la place du profil VPN d'utilisateur manquant. Cette non-correspondance peut conduire à un comportement inattendu/indéfini.
Par défaut, les paramètres TND sont désactivés dans les préférences par défaut.
Pour surmonter les préférences par défaut des paramètres codés en dur dans l'application client AnyConnect, l'ordinateur de l'utilisateur final doit avoir deux profils VPN, un profil VPN utilisateur et un profil VPN de gestion AC, et les deux doivent avoir les mêmes paramètres TND.
La logique derrière la connexion et la déconnexion du tunnel VPN de gestion est que pour établir un tunnel VPN de gestion, l'agent AC utilise les paramètres TND du profil VPN utilisateur et pour la déconnexion du tunnel VPN de gestion, il vérifie les paramètres TND du profil VPN de gestion.

Méthodes de déploiement pour profil VPN de gestion AnyConnect

- Une connexion VPN utilisateur réussie est établie avec le profil de connexion ASA afin de télécharger le profil VPN de gestion AnyConnect à partir de la passerelle VPN.

Remarque : si le protocole utilisé pour le tunnel VPN de gestion est IKEv2, la première

connexion doit être établie via SSL (afin de télécharger le profil VPN de gestion AnyConnect depuis l'ASA).

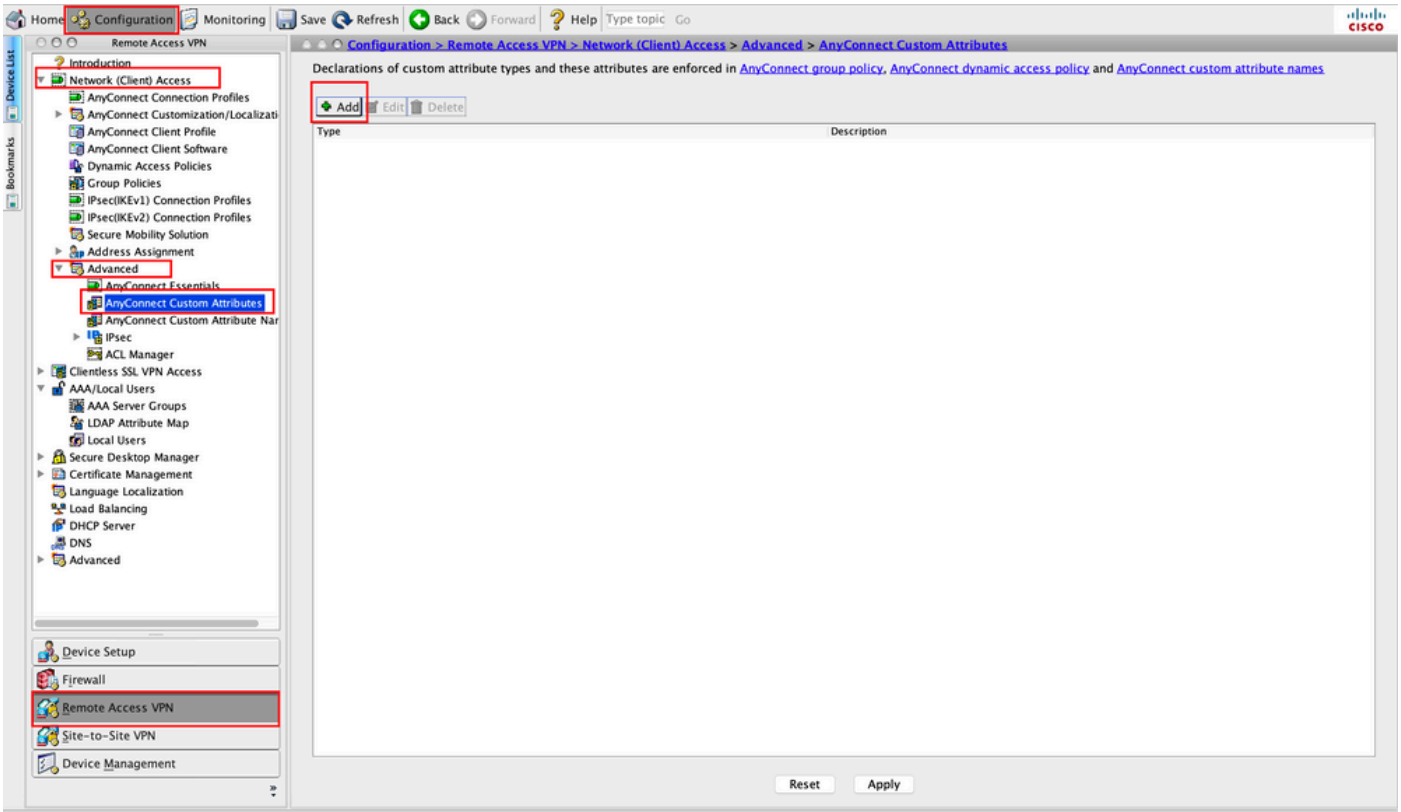
- Le profil VPN de gestion AnyConnect peut être téléchargé manuellement sur les ordinateurs clients, soit par diffusion d'un objet de stratégie de groupe, soit par installation manuelle (assurez-vous que le nom du profil estVpnMgmtTunProfile.xml).

  Emplacement du dossier où le profil doit être ajouté :
  Fenêtres: C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun
  macOS : /opt/cisco/anyconnect/profile/mgmttun/

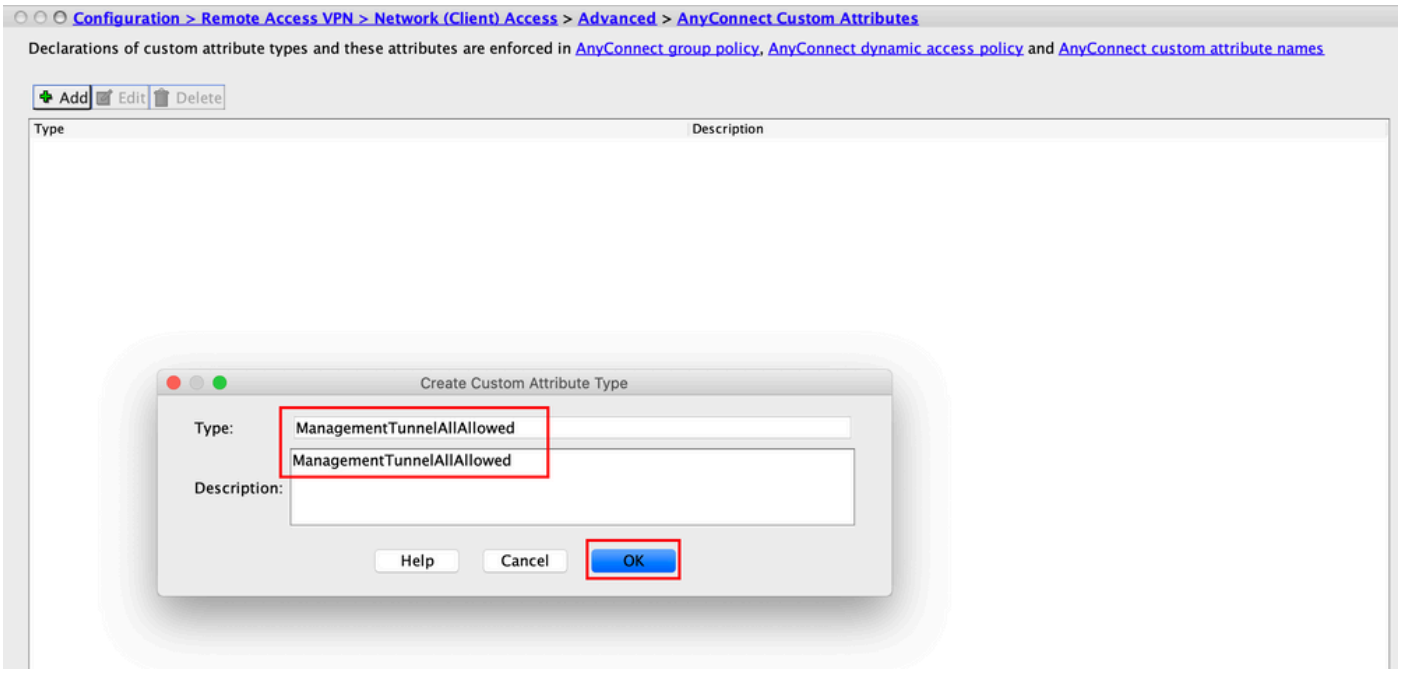
(Facultatif) Configurez un attribut personnalisé pour prendre en charge la configuration de tous les tunnels

Le tunnel VPN de gestion nécessite un fractionnement qui inclut la configuration du tunneling, par défaut, pour éviter un impact sur la communication réseau initiée par l'utilisateur. Cela peut être remplacé lorsque vous configurez l'attribut personnalisé dans la stratégie de groupe utilisée par la connexion du tunnel de gestion.

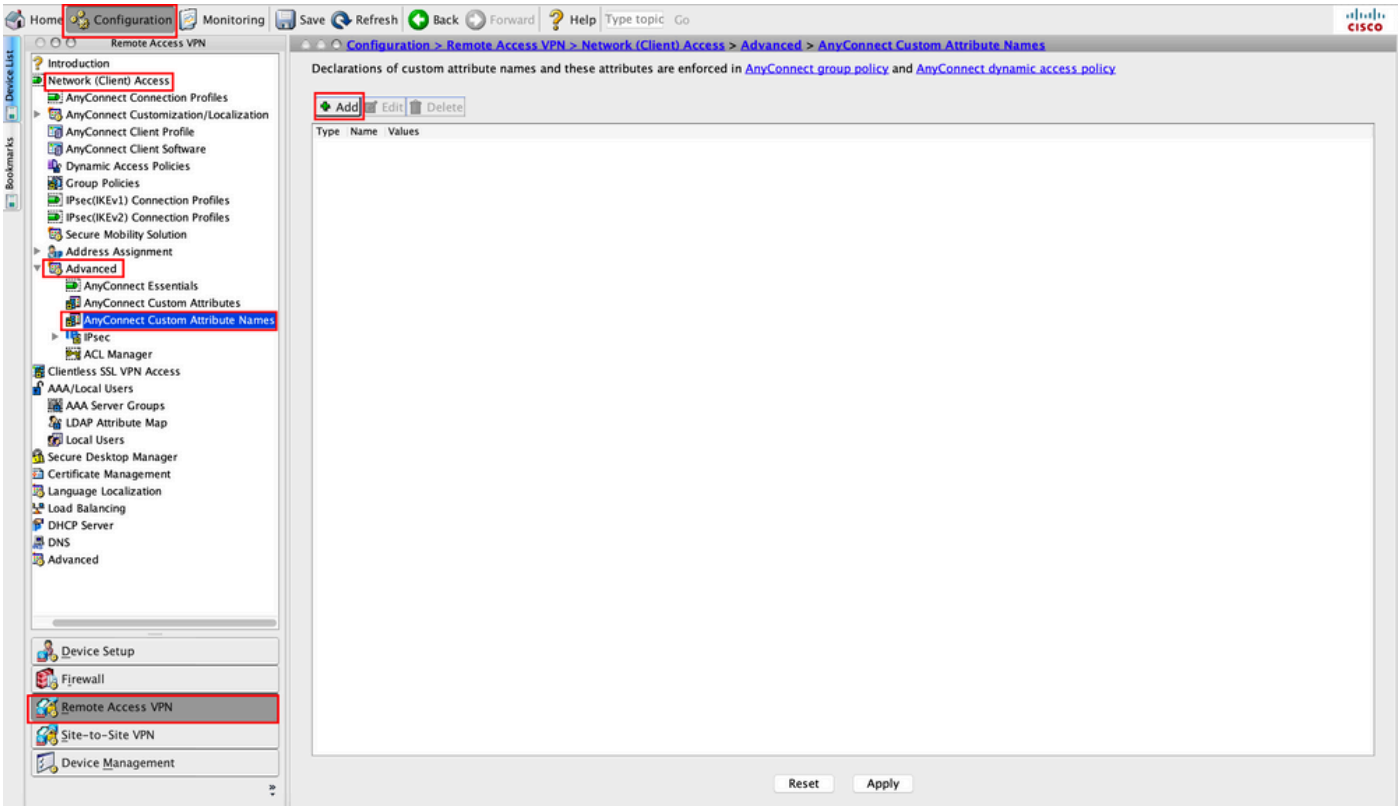
Étape 1. Accédez àConfiguration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes. Cliquez sur , comme illustré dans l'image.



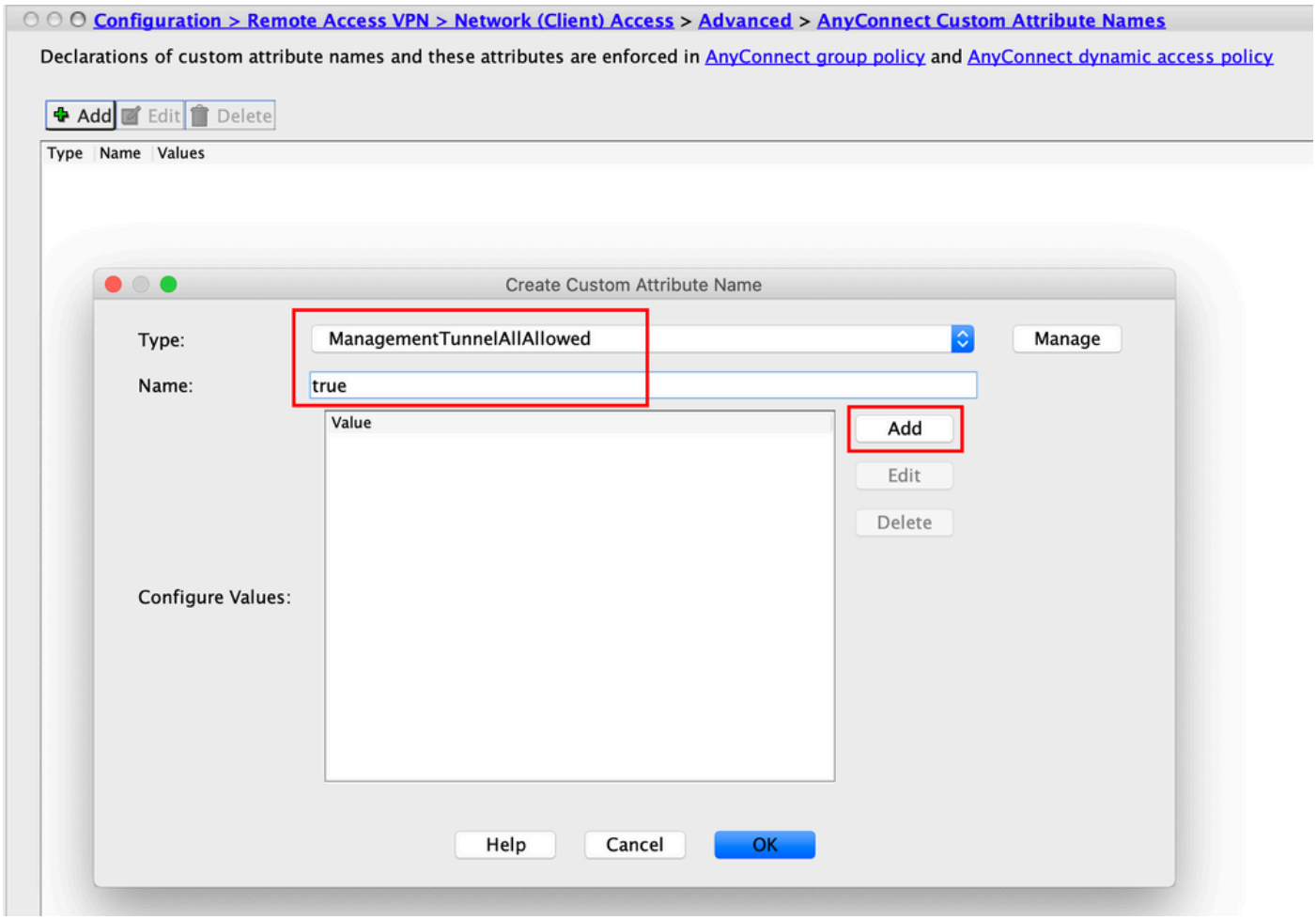
Étape 2. Définissez l'attribut personnalisé Type surManagementTunnelAllAllowed et fournissez un Description. Cliquez surOK, comme illustré dans l'image.



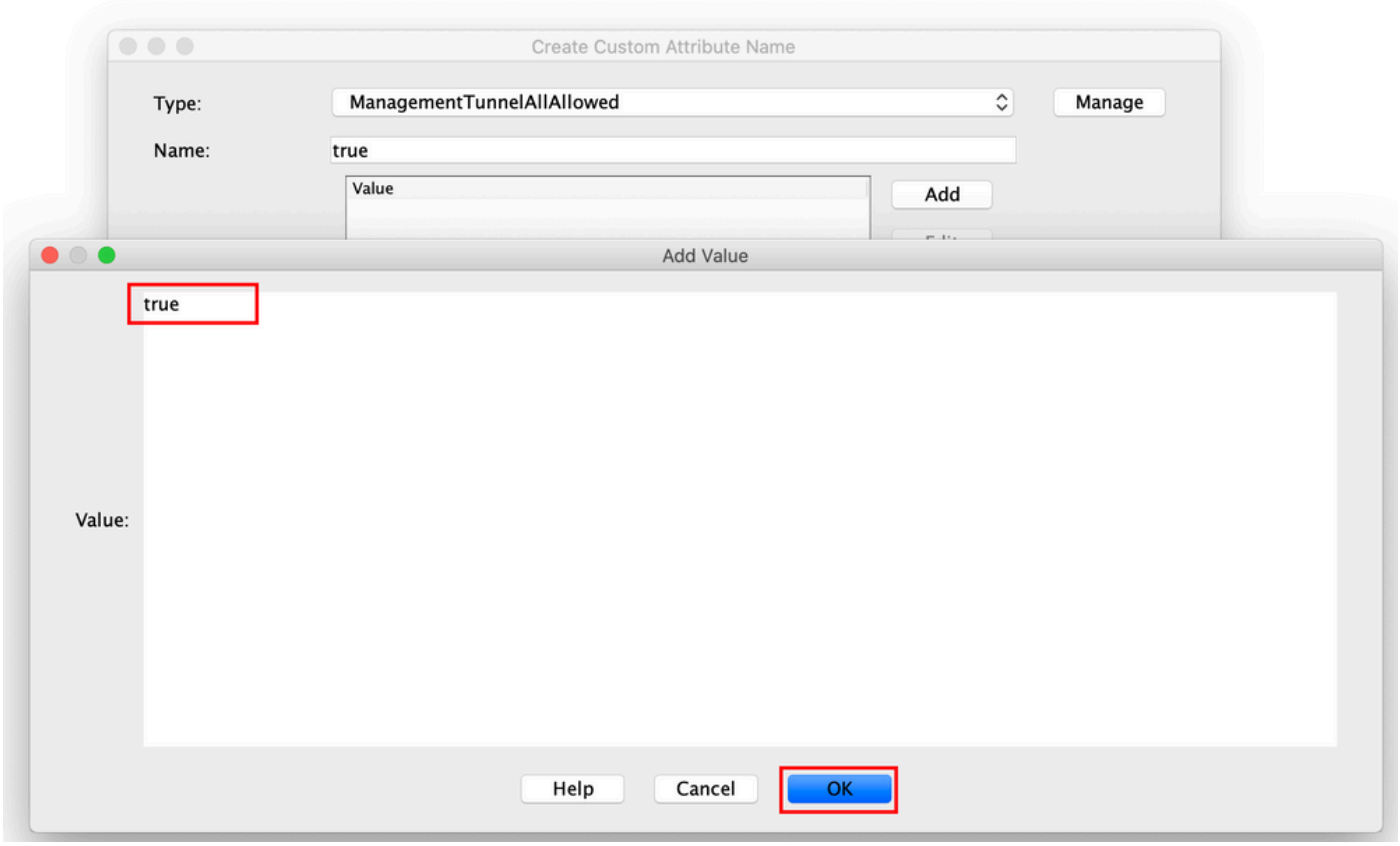
Étape 3. Accédez à Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names. Cliquez sur , comme illustré dans l'image.



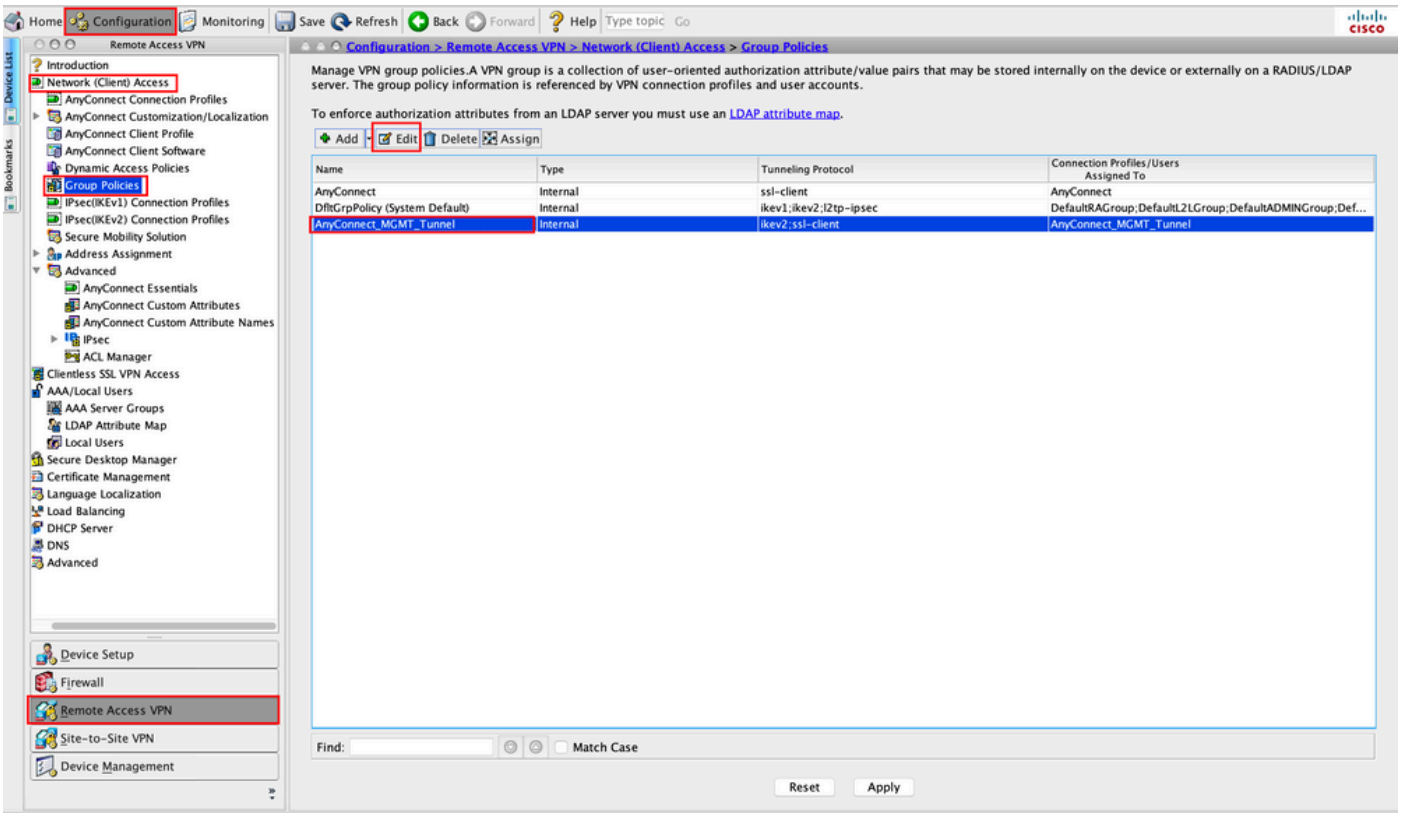
Étape 4. Sélectionnez le type ManagementTunnelAllAllowed. Définissez le nom surtrue. CliquezAddpour fournir une valeur d'attribut personnalisée, comme illustré dans l'image.



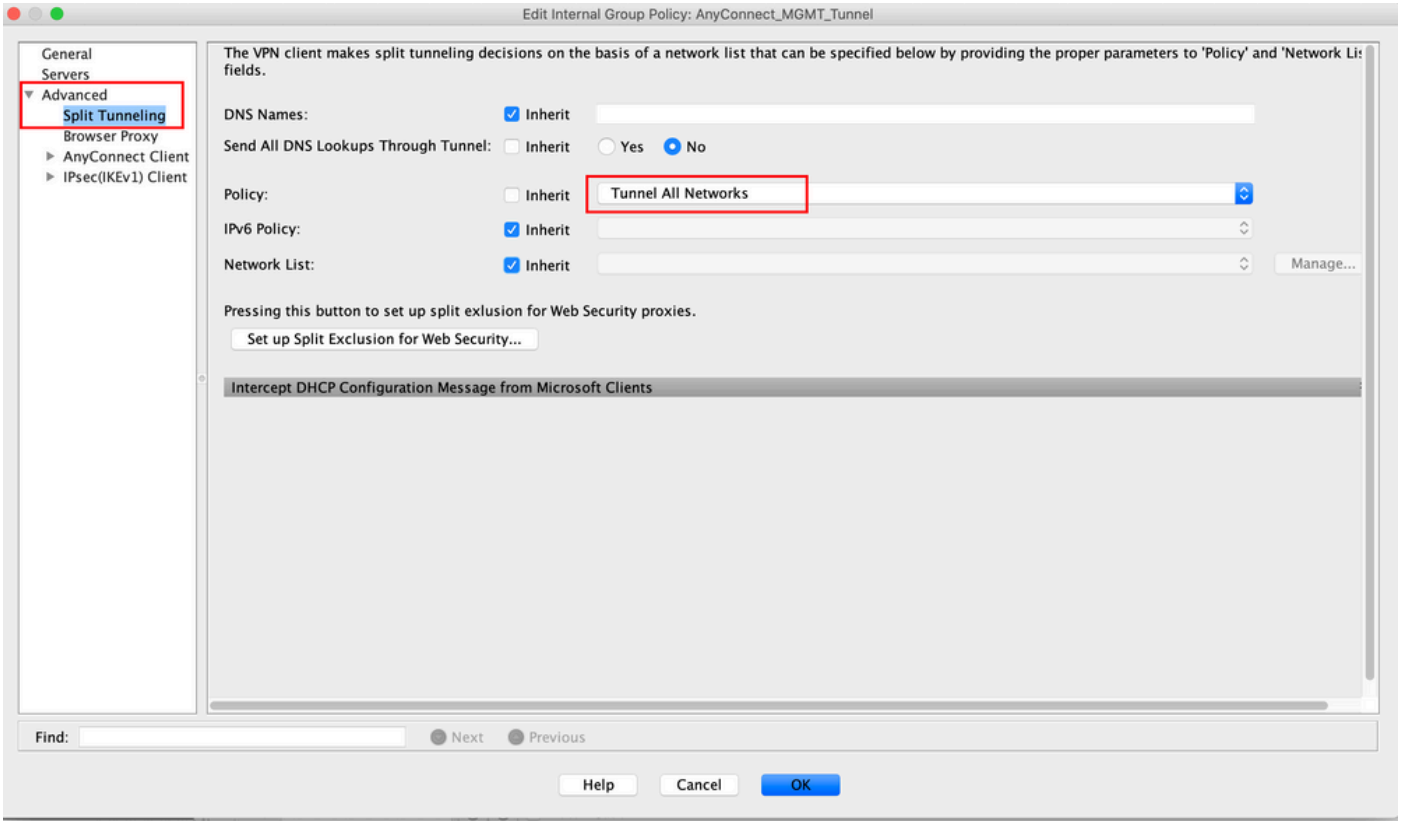
Étape 5. Définissez la valeur surtrue. Cliquez surOK, comme illustré dans l'image.



Étape 6. Accédez àConfiguration > Remote Access VPN > Network (Client) Access > Group Policies. Sélectionnez la stratégie de groupe. Cliquez sur **Edit** , comme illustré dans l'image.

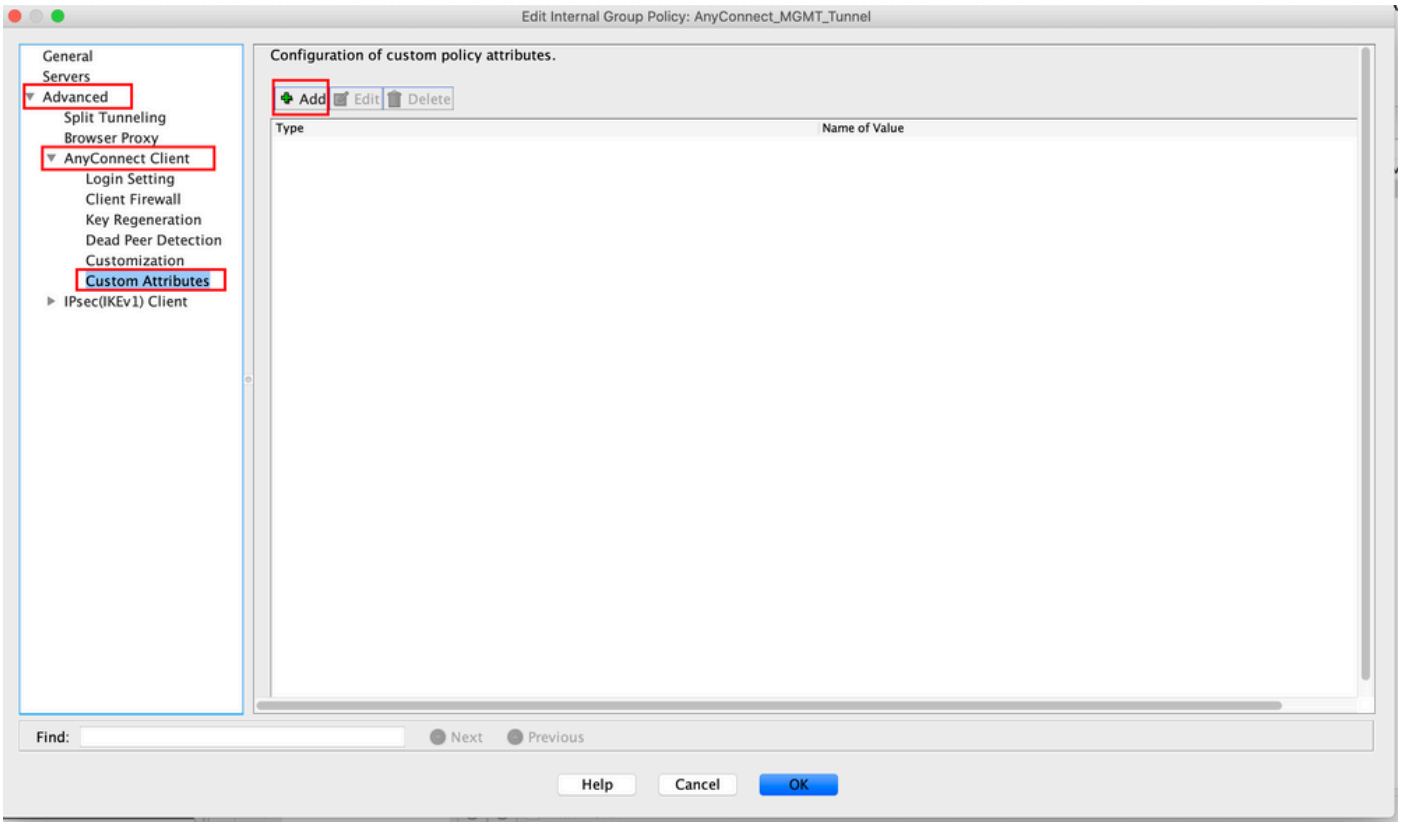


Étape 7. Comme le montre cette image, accédez àAdvanced > Split Tunneling. Configurez la stratégie en tant queTunnel All Networks.

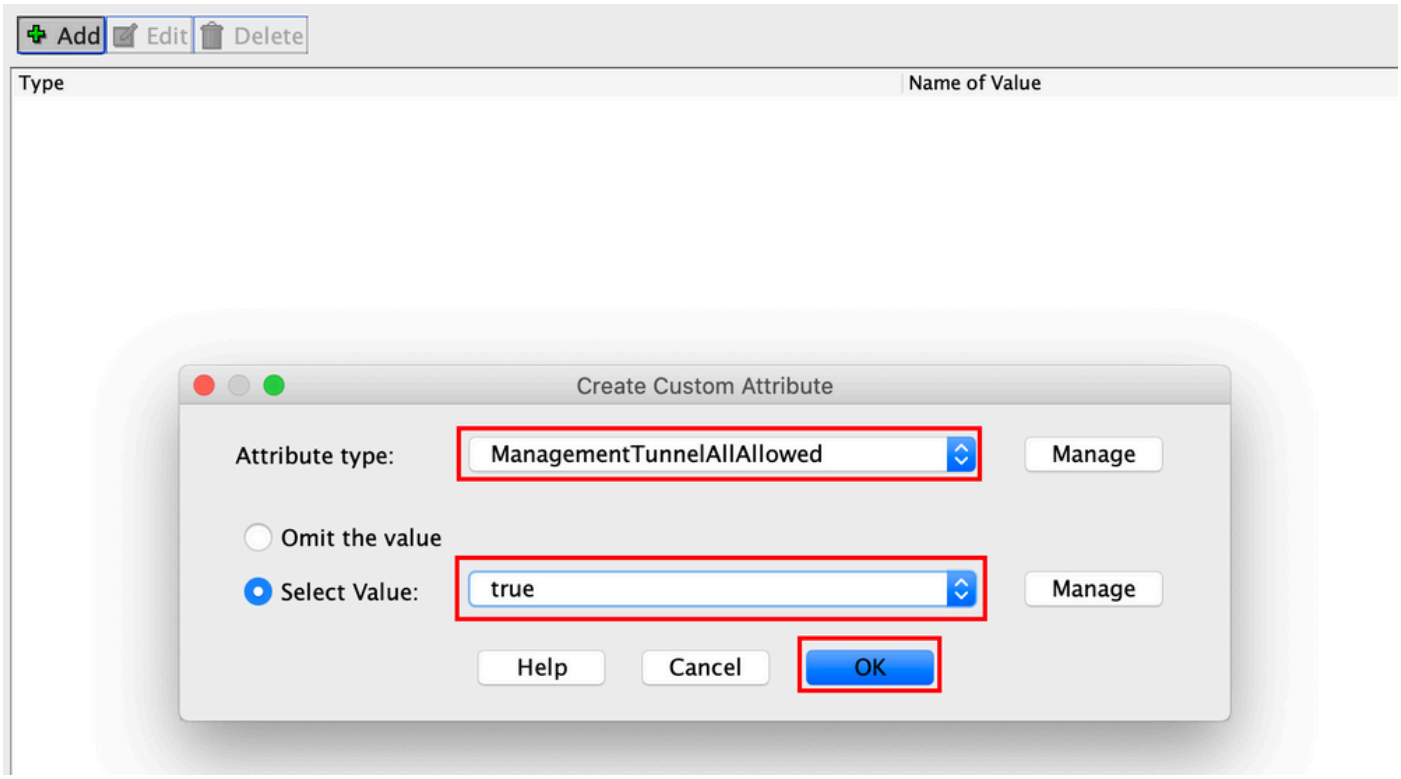


Étape 8. Accédez àAdvanced > Anyconnect Client > Custom Attributes. Cliquez surAdd, comme illustré dans

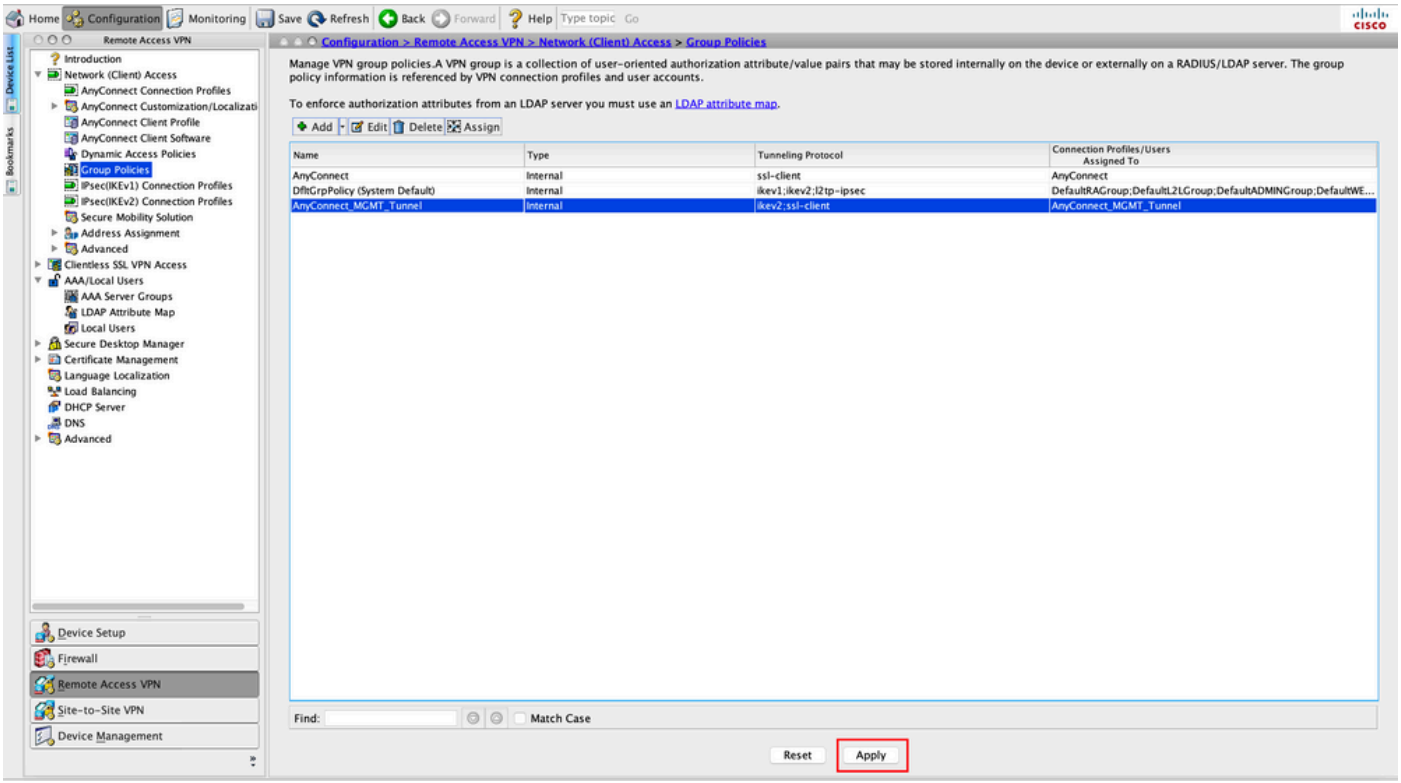
l'image.



Étape 9. Sélectionnez le type d'attributManagementTunnelAllAllowed et sélectionnez Valeur true. Cliquez OKsur, comme illustré dans l'image.



Étape 10. Cliquez surApplypour transmettre la configuration à l'ASA, comme illustré dans l'image.



Configuration CLI après l'ajout de l'attribut personnaliséManagementTunnelAllAllowed:

```
<#root>

webvpn

 enable outside

 anyconnect-custom-attr ManagementTunnelAllAllowed description ManagementTunnelAllAllowed

 hsts
  enable
  max-age 31536000
  include-sub-domains
  no preload
 no anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1

 anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm

 anyconnect enable
 tunnel-group-list enable
 cache
  disable
 error-recovery disable
!

anyconnect-custom-data ManagementTunnelAllAllowed true true

!
group-policy AnyConnect_MGMT_Tunnel internal

group-policy AnyConnect_MGMT_Tunnel attributes

 vpn-tunnel-protocol ikev2 ssl-client
```

```
 split-tunnel-policy tunnelall

 client-bypass-protocol enable
 address-pools value VPN_Pool

 anyconnect-custom ManagementTunnelAllAllowed value true

 webvpn

  anyconnect profiles value AnyConnect_MGMT_Profile type vpn-mgmt
```

Vérifier

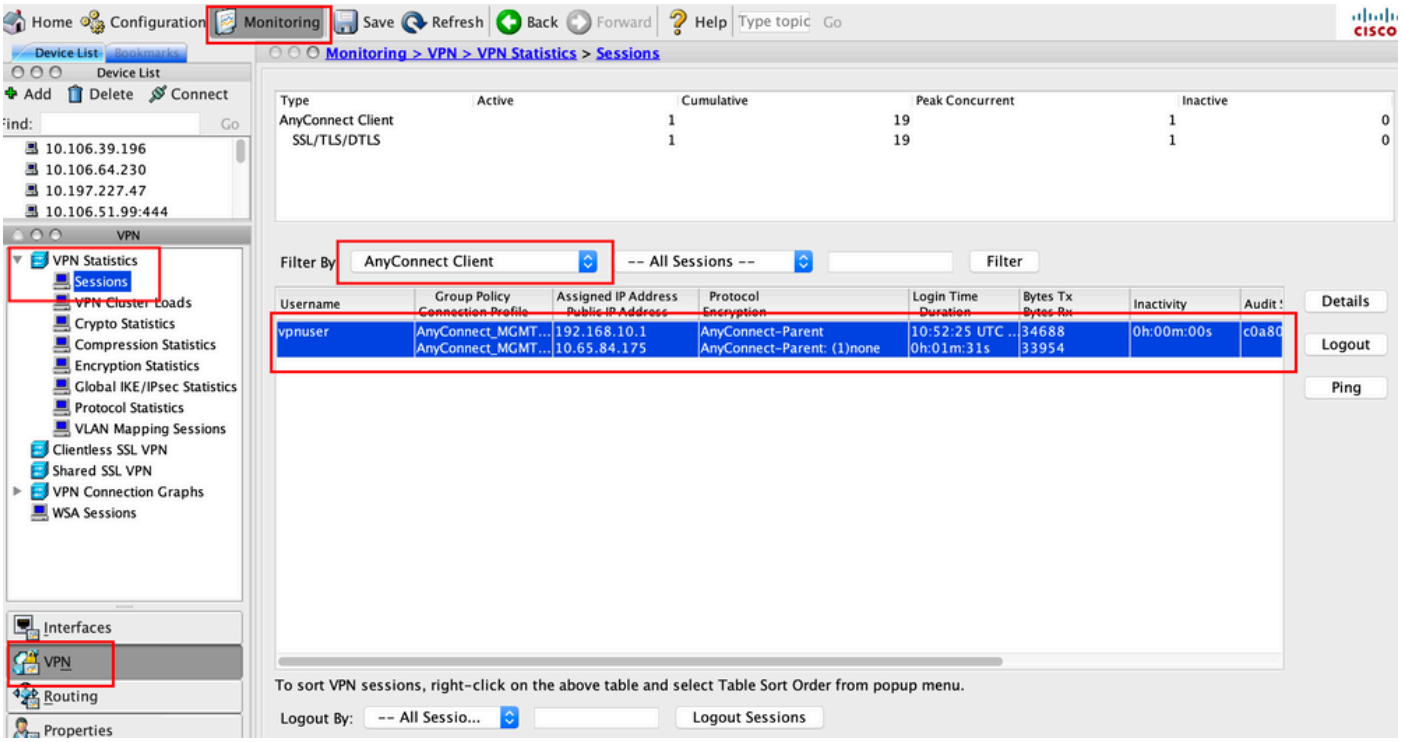
Vérifiez la connexion du tunnel VPN de gestion sur l'interface de ligne de commande ASA avec la`show vpn-sessiondb detail anyconnect` commande.

```
<#root>

ASA#

show vpn-sessiondb detail anyconnect


Session Type: AnyConnect Detailed

Username     :

vpnuser

                Index        : 10
Assigned IP  :

192.168.10.1

 Public IP    : 10.65.84.175
Protocol     :

AnyConnect-Parent SSL-Tunnel DTLS-Tunnel

License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA384
Bytes Tx     : 17238                  Bytes Rx     : 1988
Pkts Tx      : 12                     Pkts Rx      : 13
Pkts Tx Drop : 0                      Pkts Rx Drop : 0

Group Policy : AnyConnect_MGMT_Tunnel Tunnel Group : AnyConnect_MGMT_Tunnel

Login Time   : 01:23:55 UTC Tue Apr 14 2020
Duration     : 0h:11m:36s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a801010000a0005e9510ab
Security Grp : none

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

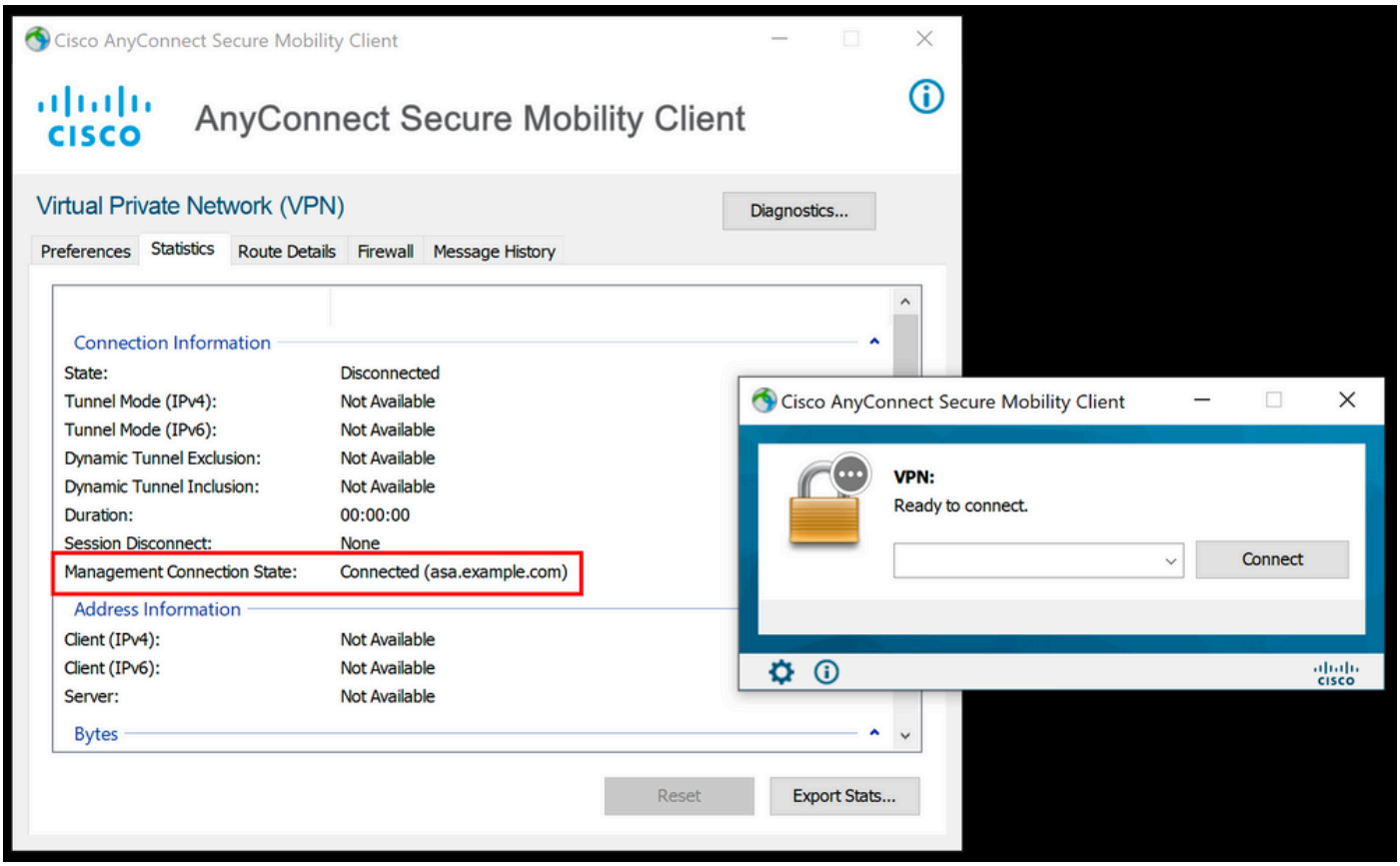
```
--- Output Omitted ---

DTLS-Tunnel:

  Tunnel ID    : 10.3
  Assigned IP  : 192.168.10.1           Public IP    : 10.65.84.175
  Encryption   : AES-GCM-256            Hashing      : SHA384
  Ciphersuite  : ECDHE-ECDSA-AES256-GCM-SHA384
  Encapsulation: DTLSv1.2               UDP Src Port : 57053
  UDP Dst Port : 443
Auth Mode    : Certificate

  Idle Time Out: 30 Minutes             Idle TO Left : 18 Minutes
  Client OS    : Windows
  Client Type  : DTLS VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.8.03036
  Bytes Tx     : 17238                  Bytes Rx     : 1988
  Pkts Tx      : 12                     Pkts Rx      : 13
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0
```

Vérifiez la connexion du tunnel VPN de gestion sur ASDM.

Accédez à Monitoring > VPN > VPN Statistics > Sessions. Filter By AnyConnect Client pour afficher la session client.



Vérification de la connexion du tunnel VPN de gestion sur l'ordinateur client :



Dépannage

La nouvelle ligne UI Statistics (Management Connection State) peut être utilisée pour résoudre les problèmes de connectivité du tunnel de gestion. Voici les états d'erreur courants :

Déconnecté (désactivé) :

- La fonctionnalité est désactivée.
- Assurez-vous que le profil VPN de gestion a été déployé sur le client, via une connexion de tunnel utilisateur (nécessite que vous ajoutiez le profil VPN de gestion à la stratégie de groupe de tunnels utilisateur) ou hors bande par le biais du téléchargement manuel du profil.
- Assurez-vous que le profil VPN de gestion est configuré avec une seule entrée d'hôte qui inclut un groupe de tunnels.

Déconnecté (réseau approuvé) :

- TND a détecté un réseau approuvé et le tunnel de gestion n'est donc pas établi.

Déconnecté (tunnel utilisateur actif) :

- Un tunnel VPN utilisateur est actuellement actif.

Déconnecté (échec du lancement du processus) :

- Une erreur de lancement de processus a été rencontrée lors de la tentative de connexion au tunnel de gestion.

Déconnecté (échec de la connexion) :

- Une défaillance de connexion s'est produite lors de l'établissement du tunnel de gestion.
- Assurez-vous que l'authentification du certificat est configurée dans le groupe de tunnels, qu'aucune bannière n'est présente dans la stratégie de groupe et que le certificat du serveur doit être approuvé.

Déconnecté (configuration VPN non valide) :

- Une configuration de tunnel partagé ou de protocole de contournement de client non valide a été reçue du serveur VPN.
- Vérifiez votre configuration dans la politique de groupe de tunnels de gestion par rapport à la documentation.

Déconnecté (mise à jour logicielle en attente) :

- Une mise à jour du logiciel AnyConnect est actuellement en attente.

Déconnecté :

- Le tunnel de gestion est sur le point d'être établi ou ne peut pas l'être pour une autre raison.

Collectez le DART pour un dépannage plus approfondi.

Informations connexes

- Configuration du tunnel VPN de gestion
- Dépannage du tunnel VPN de gestion
- Assistance et documentation techniques - Cisco Systems

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

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