Beheerde AnyConnect VPN-tunnel op ASA configureren

Inhoud

Inleiding

Dit document beschrijft hoe u een ASA kunt configureren als de VPN-gateway verbindingen accepteert vanuit de Cisco AnyConnect Secure Mobility Client via de VPN-tunnel voor beheer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- VPN-configuratie via Adaptieve Security Device Manager (ASDM)
- CLI-configuratie voor basis adaptieve security applicatie (ASA)
- X509-certificaten

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ASA softwareversie 9.12(3)9
- Cisco ASDM-softwareversie 7.12.2
- Windows 10 met Cisco AnyConnect Secure Mobility-clientversie 4.8.03036

Opmerking: download het AnyConnect VPN-webimplementatiepakket (anyconnect-win*.pkg or anyconnect-macos*.pkg) vanuit de Cisco Software Download (alleen geregistreerde klanten). Kopieer de AnyConnect VPN-client naar het flitsgeheugen van de ASA dat moet worden gedownload naar de externe gebruikerscomputers om de SSL VPN-verbinding met de ASA tot stand te brengen. Raadpleeg het gedeelte AnyConnect-client installeren in de ASA-configuratiehandleiding voor meer informatie.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Een VPN-tunnel voor beheer zorgt voor verbinding met het bedrijfsnetwerk wanneer het clientsysteem is ingeschakeld, niet alleen wanneer een VPN-verbinding tot stand is gebracht door de eindgebruiker. U kunt patchbeheer uitvoeren op out-of-the-office endpoints, met name apparaten die niet vaak door de gebruiker, via VPN, worden verbonden met het kantoornetwerk. Endpoint OS login scripts die zakelijke netwerkconnectiviteit vereisen, profiteren ook van deze functie.

AnyConnect Management Tunnel stelt beheerders in staat om AnyConnect verbonden te hebben zonder tussenkomst van de gebruiker voordat de gebruiker zich aanmeldt. AnyConnect-beheertunnel kan werken in combinatie met Trusted Network Detection en wordt daarom alleen geactiveerd wanneer het eindpunt niet op de locatie beschikbaar is en is losgekoppeld van een door de gebruiker geïnitieerde VPN. AnyConnect-beheertunnel is transparant voor de eindgebruiker en wordt automatisch losgekoppeld wanneer de gebruiker VPN initieert.

Besturingssysteem/toepassing	Minimale versievereisten
ASA	9.0.1
ASDM	7.10.1
Windows AnyConnect versie	4.7.00136
MacOS AnyConnect versie	4.7.01076
Linux	Niet ondersteund

Werken met beheertunnels

De AnyConnect VPN-agentservice wordt automatisch gestart nadat het systeem is opgestart. Het detecteert dat de beheerstunnelfunctie is ingeschakeld (via het VPN-profiel voor beheer) en start daarom de beheerclienttoepassing om een beheertunnelverbinding te starten. De toepassing van de beheersclient gebruikt de hostingang van het VPN-beheerprofiel om de verbinding te starten. Dan is de VPN-tunnel zoals gebruikelijk, met één uitzondering: er wordt geen software-update uitgevoerd tijdens een beheertunnelverbinding, omdat de beheerstunnel bedoeld is om transparant te zijn voor de gebruiker.

De gebruiker initieert een VPN-tunnel via de AnyConnect UI, die de beëindiging van de beheerstunnel activeert. Op de beëindiging van de beheerstunnel, gaat de inrichting van de gebruikerstunnel verder zoals gebruikelijk.

De gebruiker verbreekt de VPN-tunnel, waardoor de beheerstunnel automatisch wordt hersteld.

Beperkingen

- Gebruikersinteractie wordt niet ondersteund
- Op certificaat gebaseerde verificatie via het machinecertificaat Store (Windows) wordt alleen ondersteund
- Er wordt strikte controle van servercertificaten uitgevoerd
- Een particuliere proxy wordt niet ondersteund
- Een openbare proxy wordt niet ondersteund (ProxyNative waarde wordt ondersteund op platforms waar Native Proxy-instellingen niet worden opgehaald van de browser)
- AnyConnect-aanpassingsscripts worden niet ondersteund

Opmerking: Raadpleeg Info over de VPN-tunnelleiding voor beheer voor meer informatie.

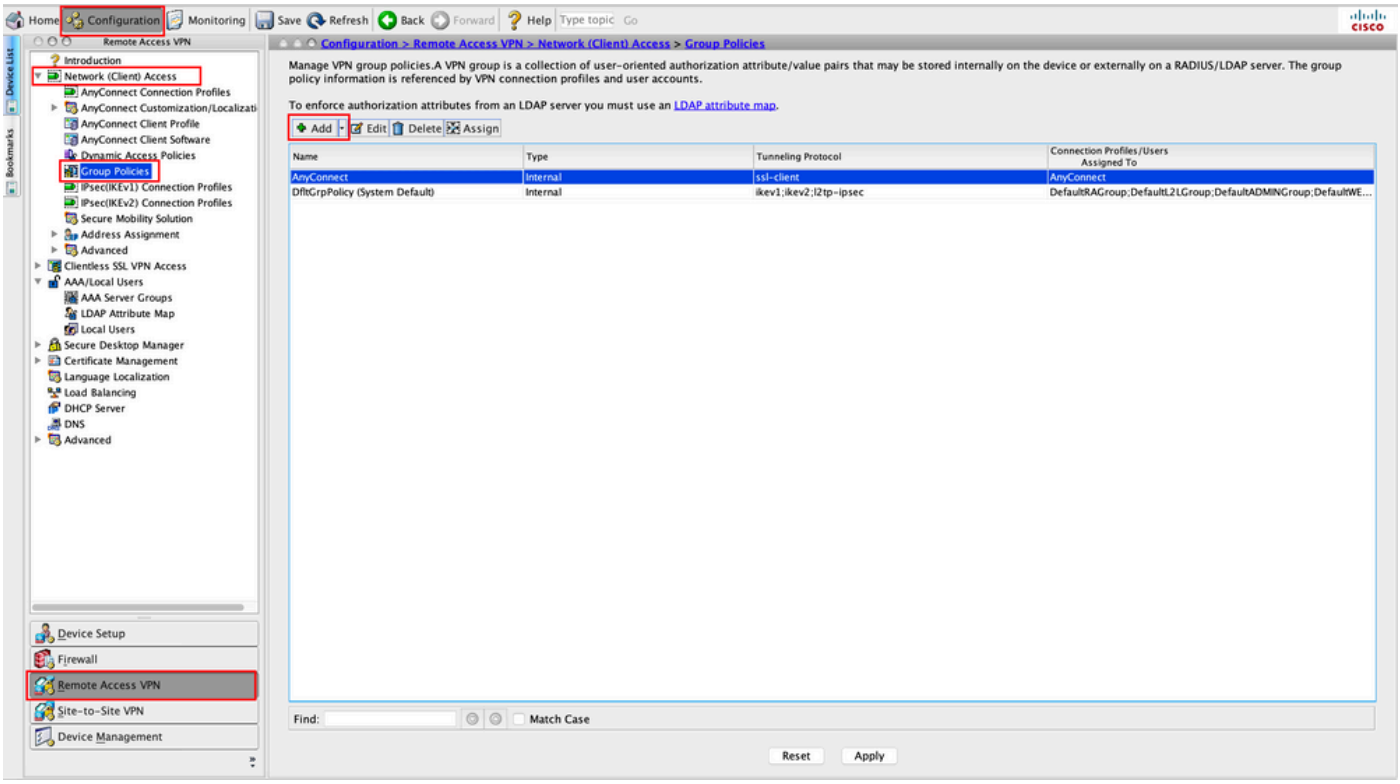
Configureren

In deze sectie wordt beschreven hoe u Cisco ASA kunt configureren als de VPN-gateway voor het accepteren van verbindingen van AnyConnect-clients via de VPN-tunnel voor beheer.

Configuratie op ASA via ASDM/CLI

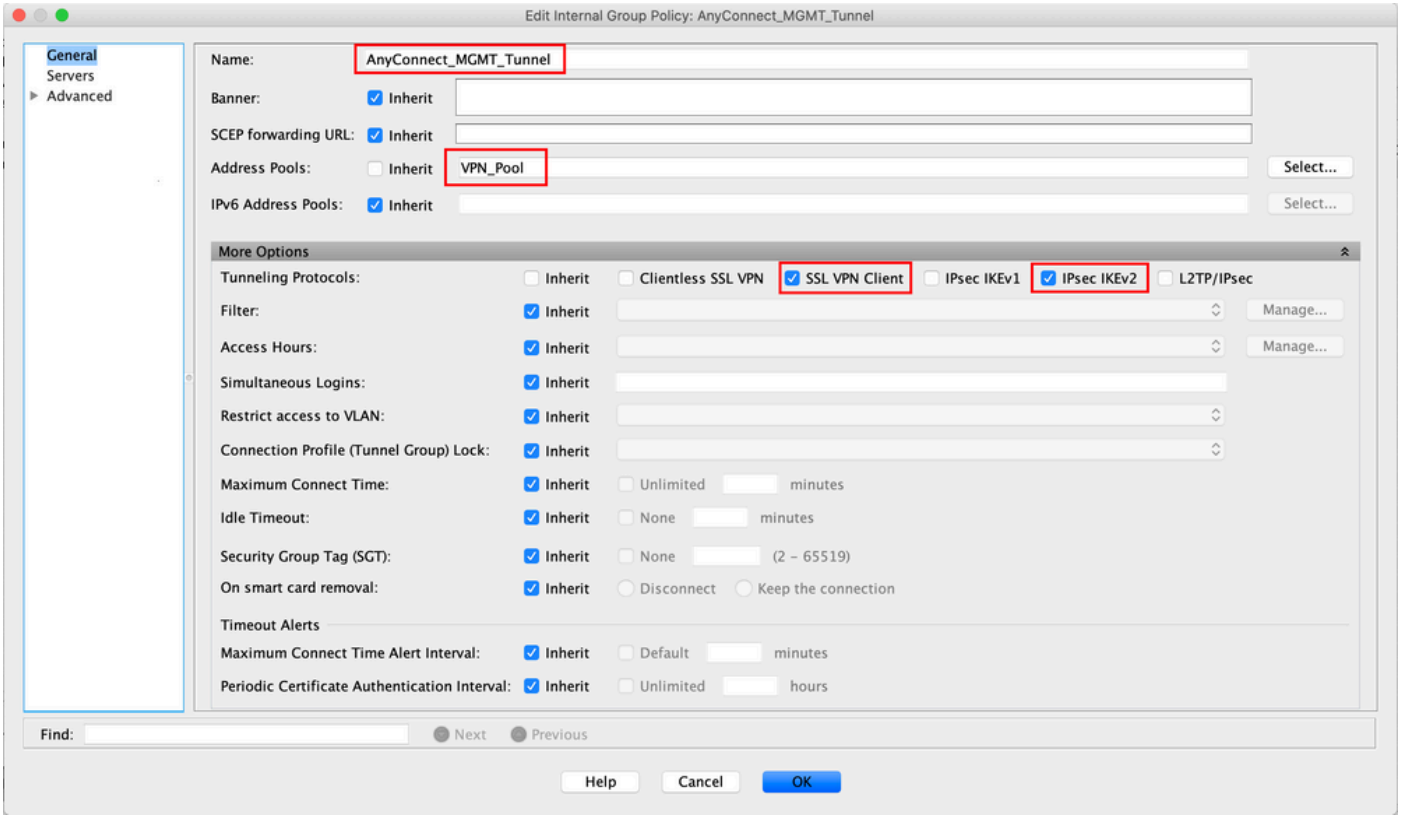
Stap 1. Maak het AnyConnect-groepsbeleid. Naar navigeren Configuration > Remote Access VPN > Network (Client) Access > Group Policies. Klik Add.

Opmerking: het is aan te raden om een nieuw AnyConnect-groepsbeleid te maken dat alleen voor de AnyConnect-beheerstunnel wordt gebruikt.

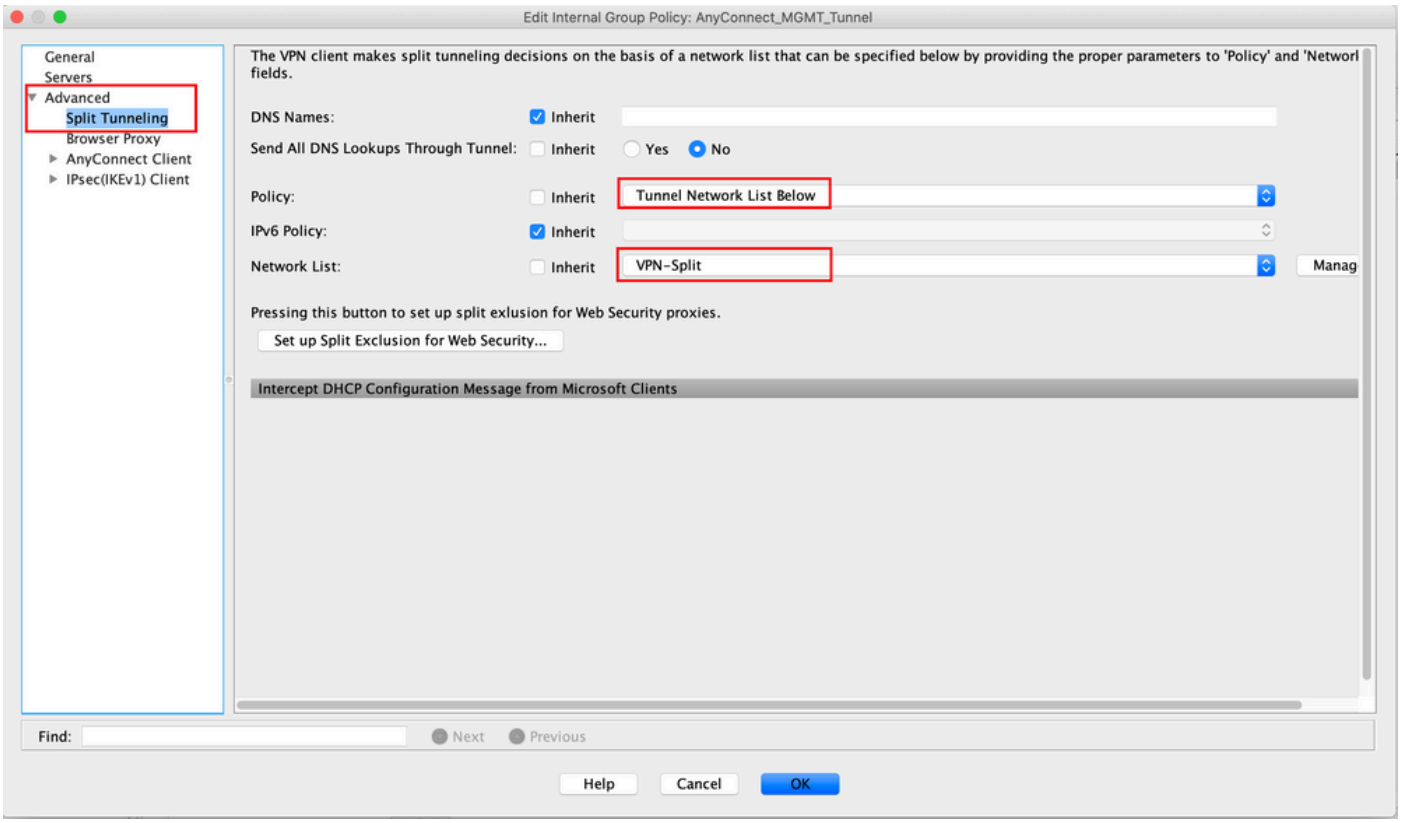


Stap 2. Een Name voor het groepsbeleid. Een bestand toewijzen/maken Address Pool.

Kiezen Tunneling Protocols als SSL VPN Client en/of IPsec IKEv2, zoals aangegeven in de afbeelding.

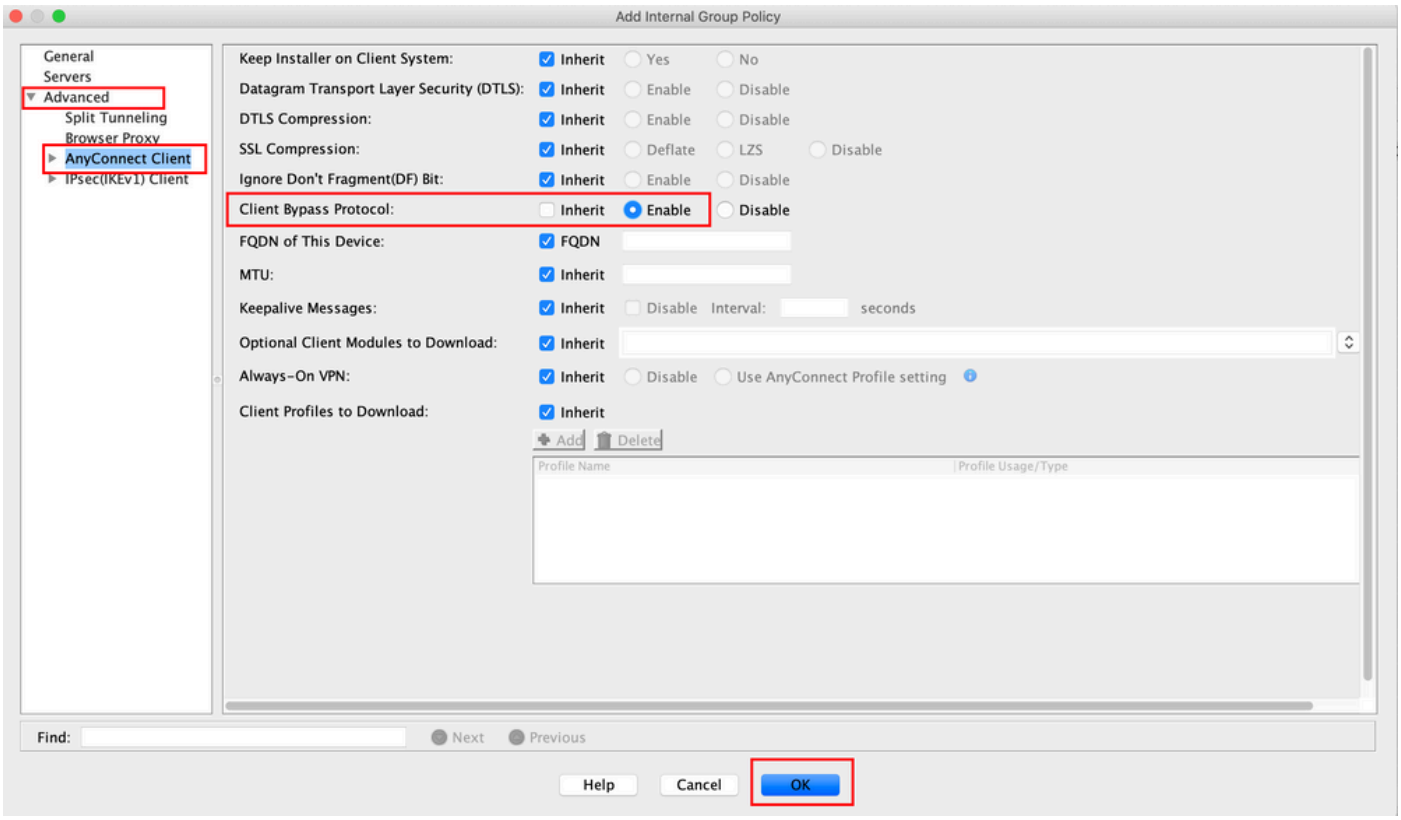


Stap 3. Naar navigeren Advanced > Split Tunneling. Configureer de Policy als Tunnel Network List Below en kies de Network List, zoals aangegeven in de afbeelding.

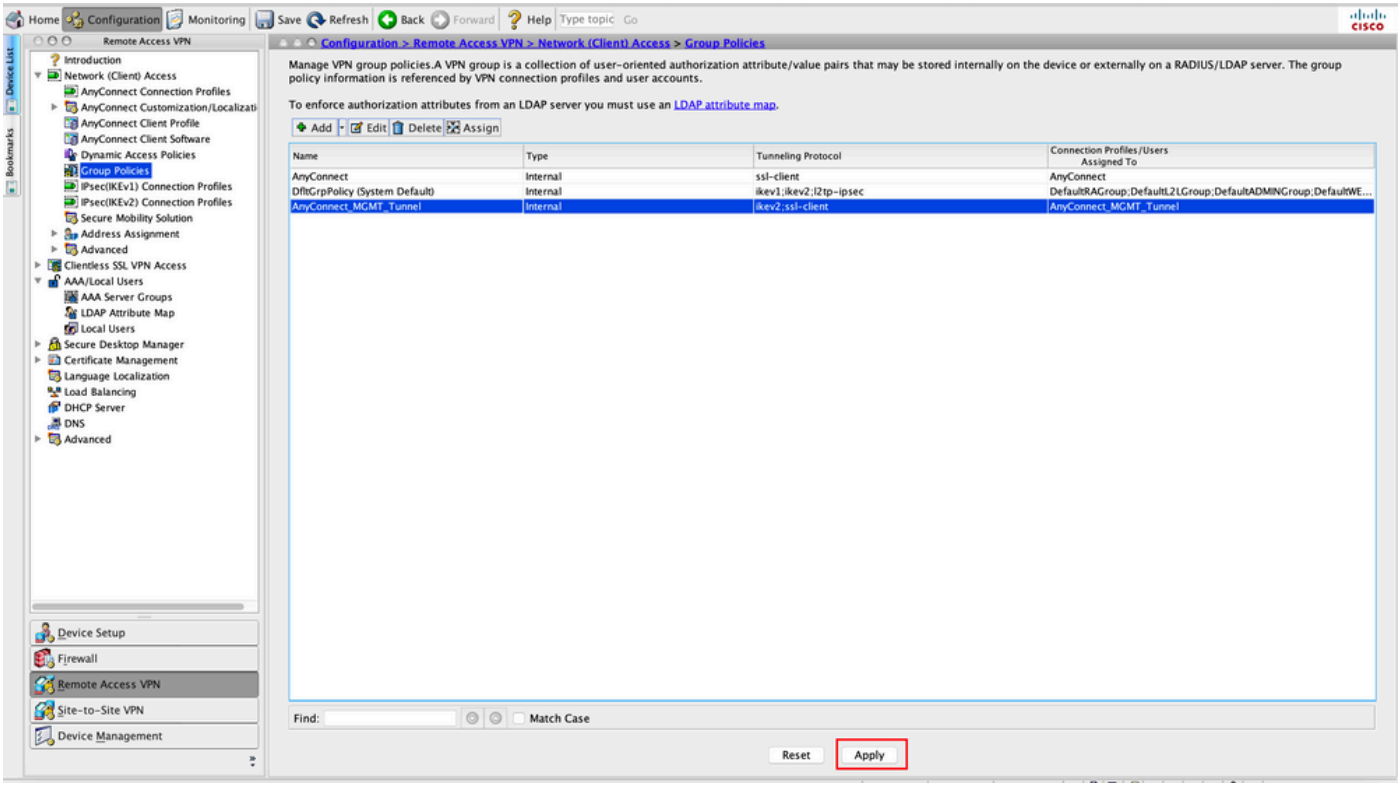


Opmerking: Als een clientadres niet voor beide IP-protocollen (IPv4 en IPv6) wordt ingedrukt, wordt het **Client Bypass Protocol** instelling moet enabled zodat het overeenkomstige verkeer niet door de beheerstunnel wordt verstoord. Raadpleeg voor het configureren stap 4.

Stap 4. Naar navigeren Advanced > AnyConnect Client. instellen Client Bypass Protocol in Enable. Klik OK om op te slaan, zoals in de afbeelding.



Stap 5. Zoals in deze afbeelding, klikt u op Apply om de configuratie naar de ASA te duwen.



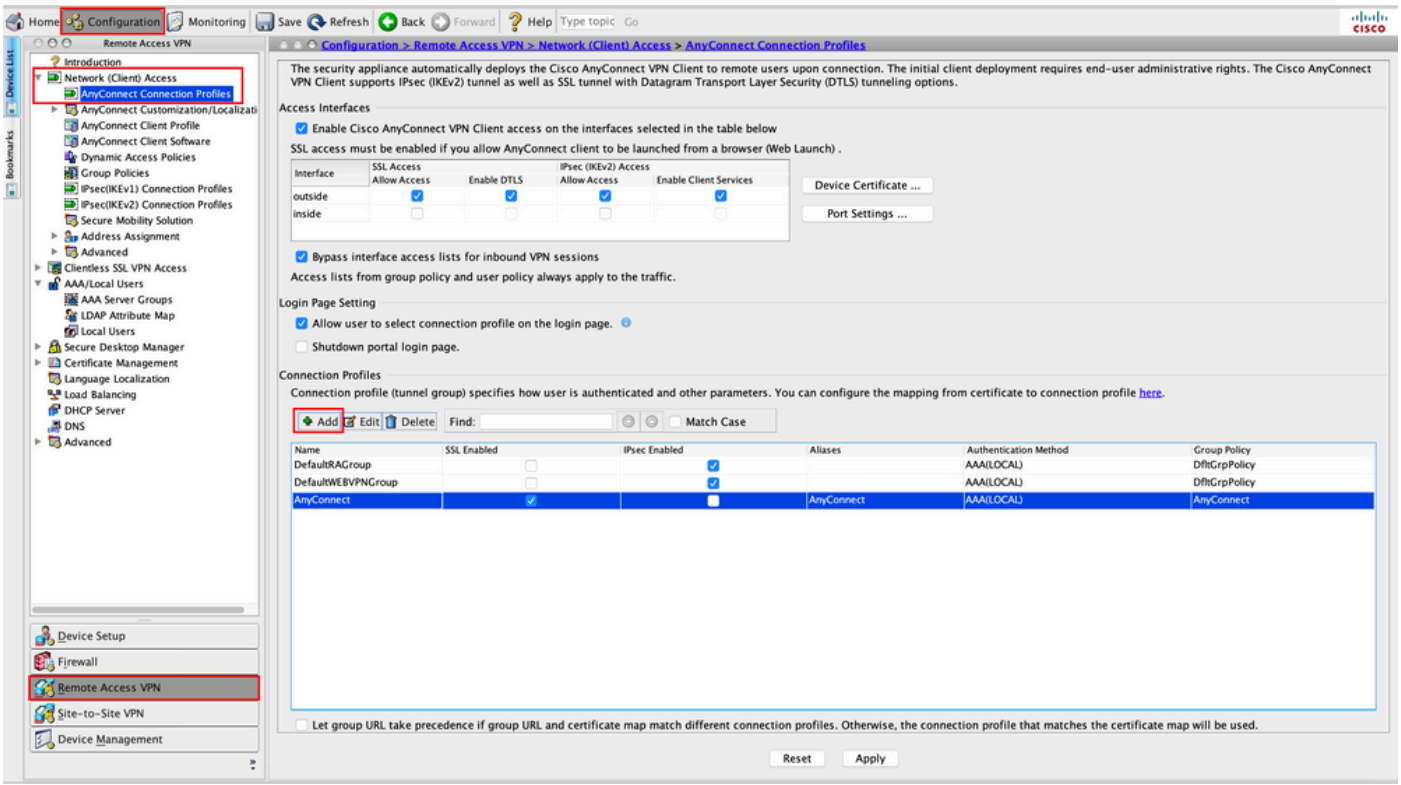
CLI-configuratie voor groepsbeleid:

```
ip local pool VPN_Pool 192.168.10.1-192.168.10.100 mask 255.255.255.0
```

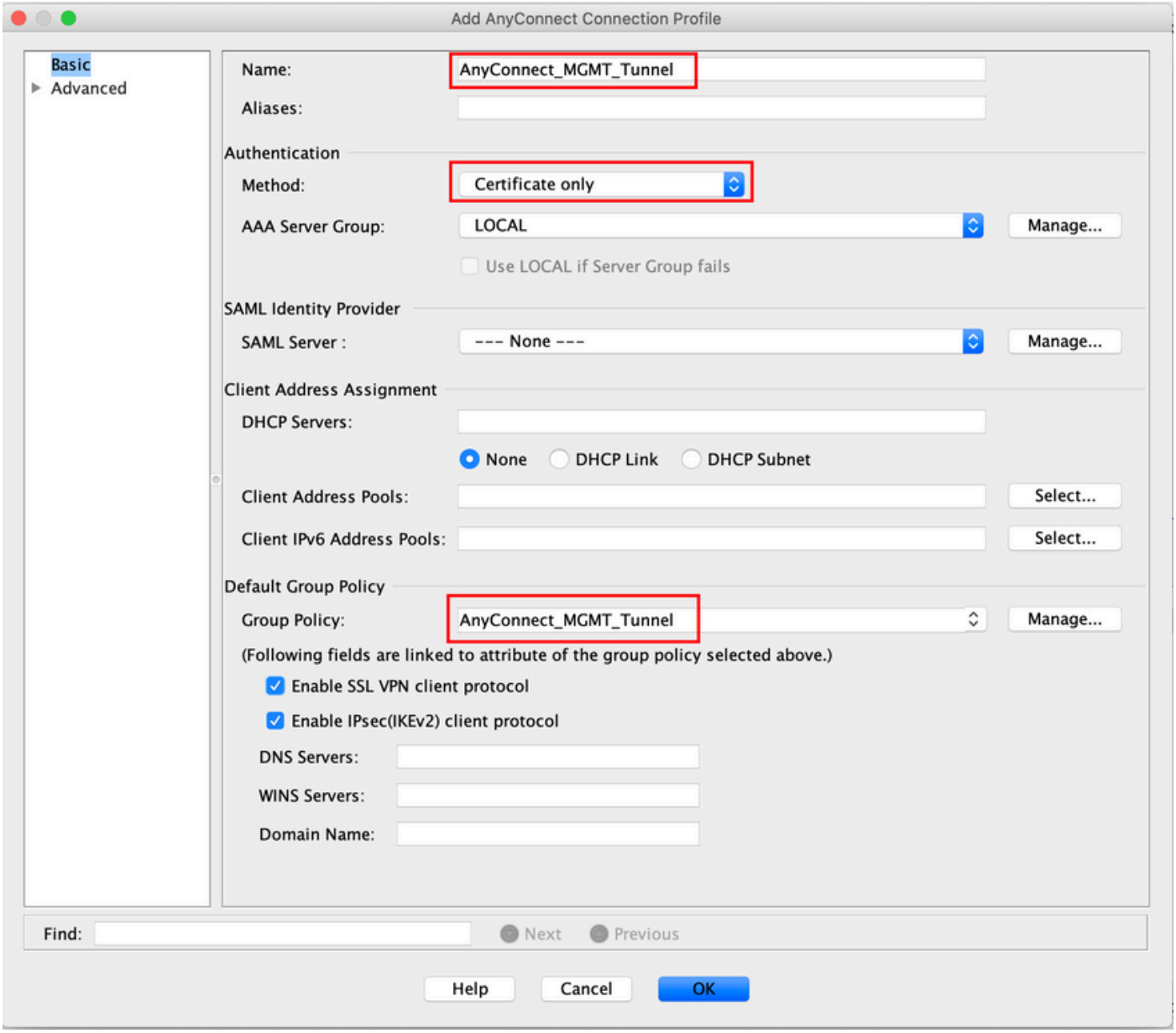
```
! access-list VPN-Split standard permit 172.16.0.0 255.255.0.0
! group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
 vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-network-list value VPN-Split
 client-bypass-protocol enable
 address-pools value VPN_Pool
```

Stap 6. Maak het AnyConnect-verbindingsprofiel. Naar navigeren Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profile. Klik Add.

> **Opmerking:** aanbevolen wordt om een nieuw AnyConnect-verbindingsprofiel te maken dat alleen voor de AnyConnect-beheertunnel wordt gebruikt.



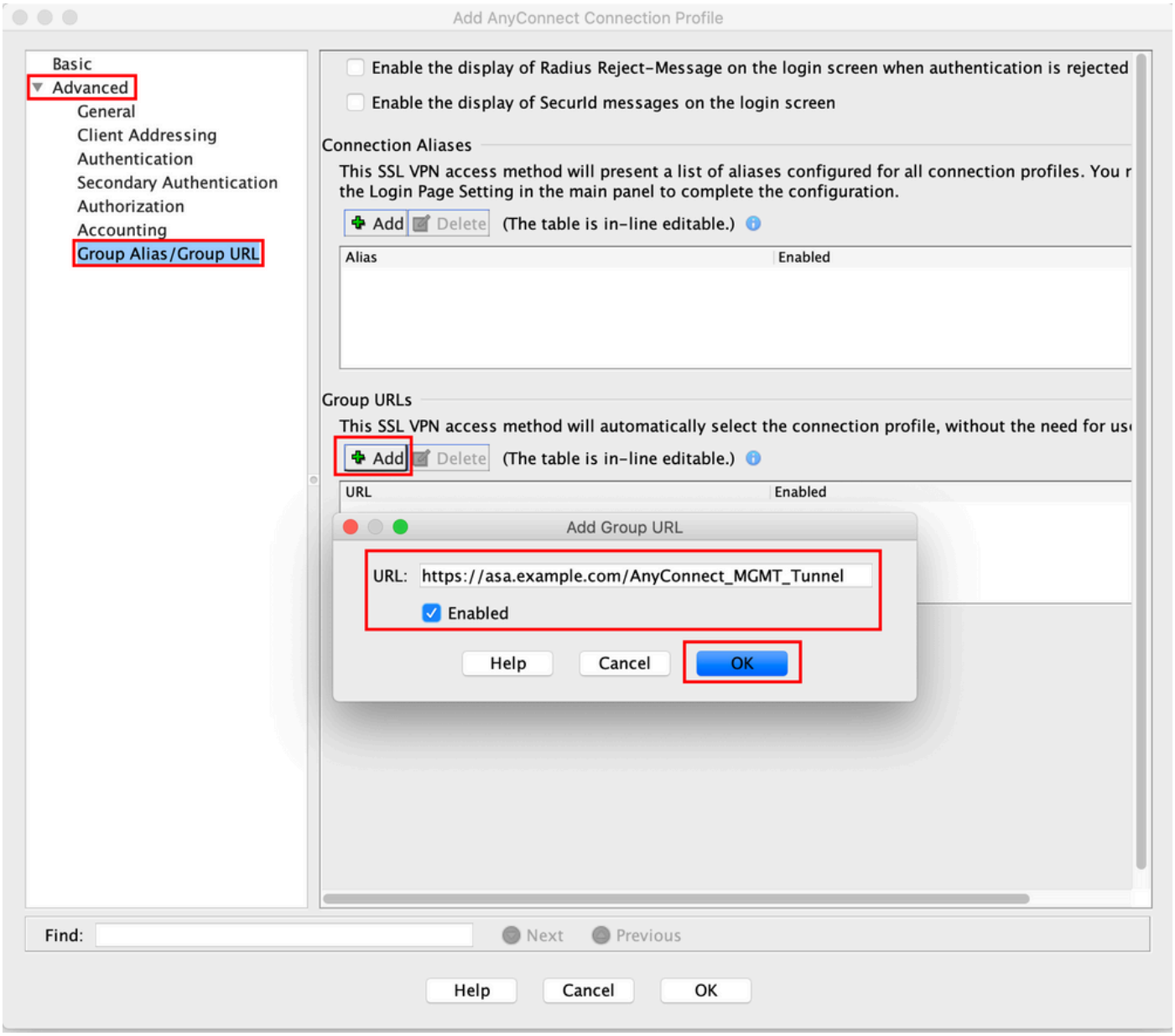
Stap 7. Een Name voor het verbindingsprofiel en instellen Authentication Method als Certificate only. Kies de Group Policy als degene die in Stap 1 is gemaakt.



Opmerking: Zorg ervoor dat het basiscertificaat van Local CA op de ASA aanwezig is. Naar navigeren Configuration > Remote Access VPN > Certificate Management > CA Certificates om het certificaat toe te voegen/weer te geven.

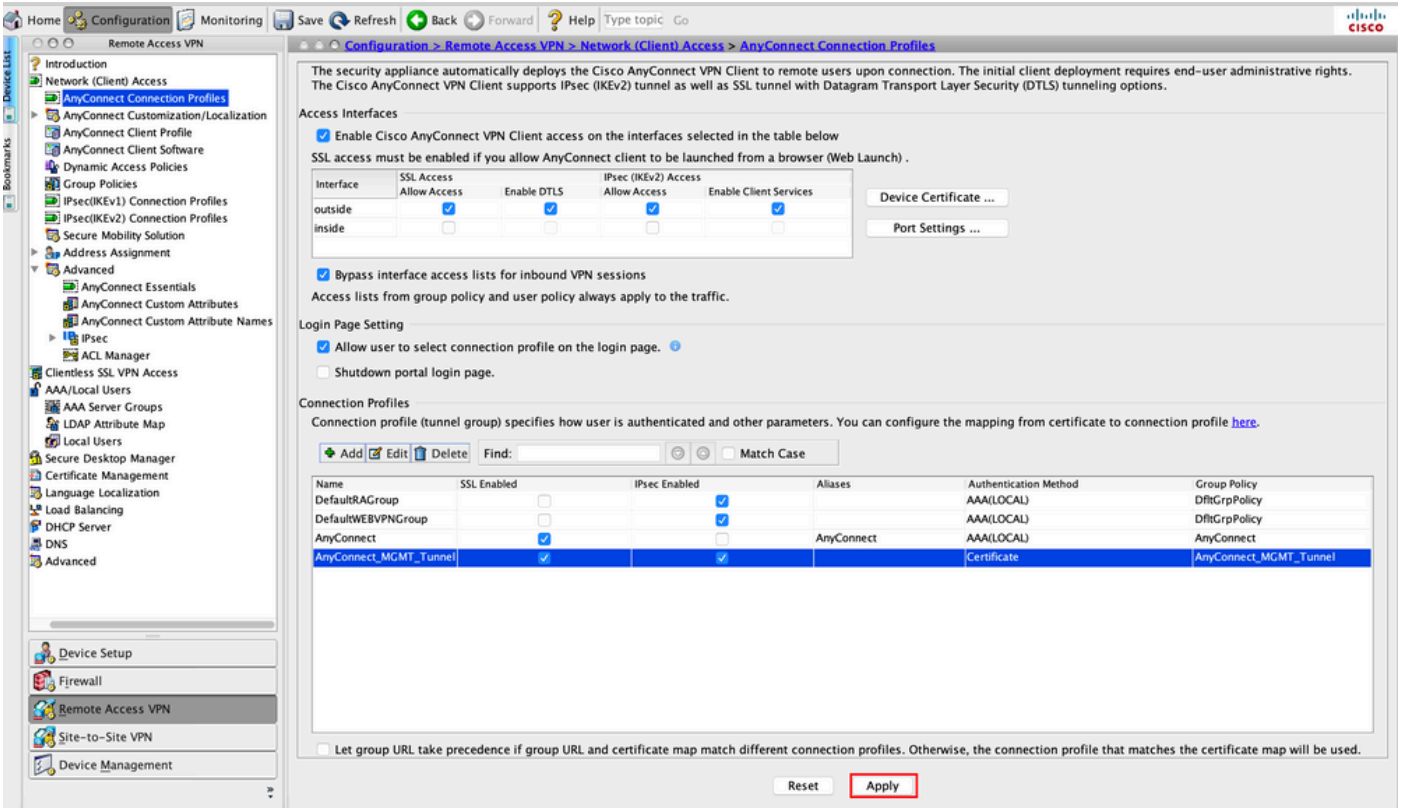
Opmerking: zorg ervoor dat een door dezelfde lokale certificeringsinstantie afgegeven identiteitsbewijs bestaat in de machinecertificaatwinkel (voor Windows) en/of in de systeemsleutelhanger (voor macOS).

Stap 8. Naar navigeren Advanced > Group Alias/Group URL. Klik Add onder Group URLs en voeg een URL. verzekeren Enabled wordt gecontroleerd. Klik OK om op te slaan, zoals in de afbeelding.



Als IKEv2 wordt gebruikt, zorg dan voor IPsec (IKEv2) Access is ingeschakeld op de interface die wordt gebruikt voor AnyConnect.

Stap 9. Klik Apply om de configuratie naar de ASA te duwen.

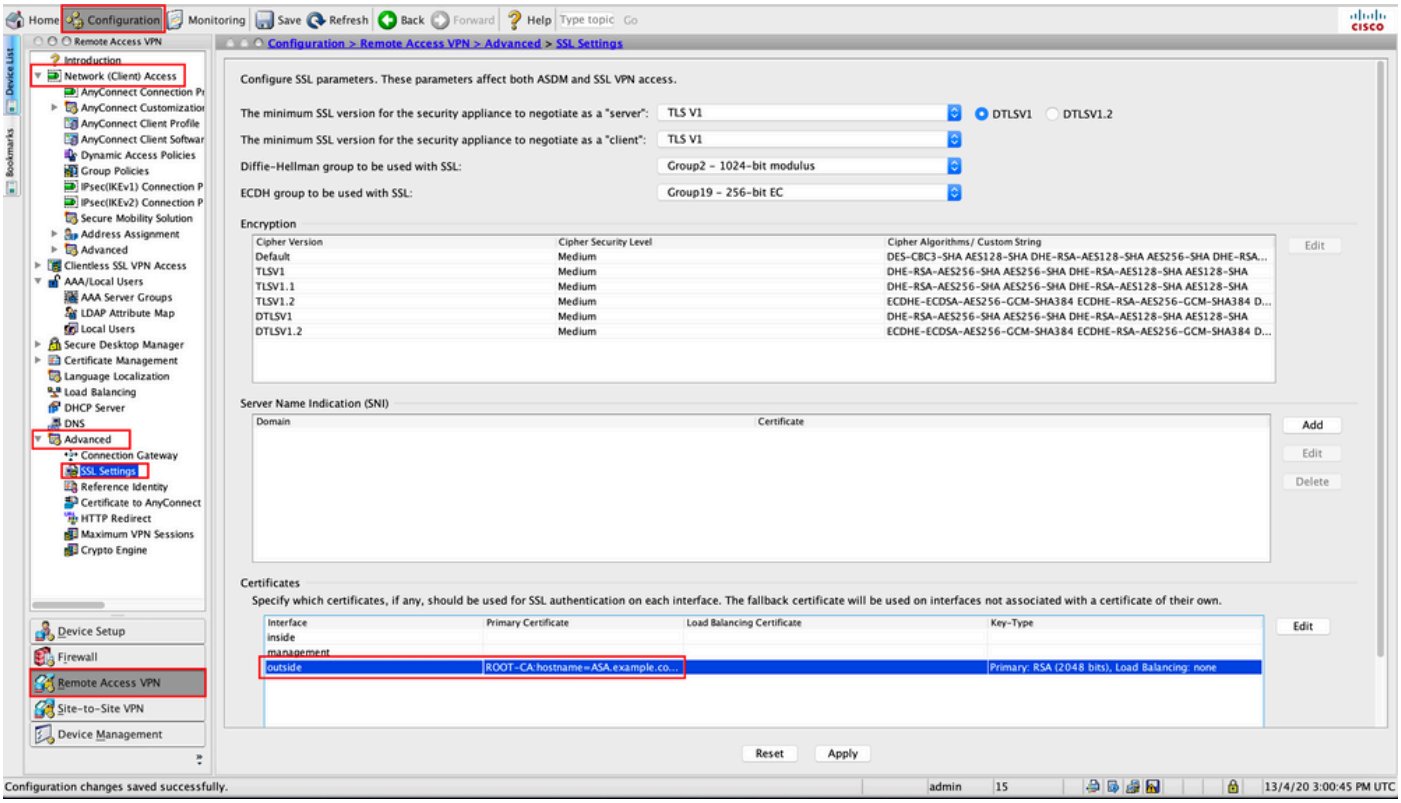


CLI-configuratie voor verbindingsprofiel (tunnelgroep):

```
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
```

Stap 10. Zorg ervoor dat een betrouwbaar certificaat is geïnstalleerd op de ASA en is gebonden aan de interface die wordt gebruikt voor AnyConnect-verbindingen. Naar navigeren Configuration > Remote Access VPN > Advanced > SSL Settings om deze instelling toe te voegen/weer te geven.

Opmerking: Raadpleeg Installatie van identiteitsbewijs op ASA.

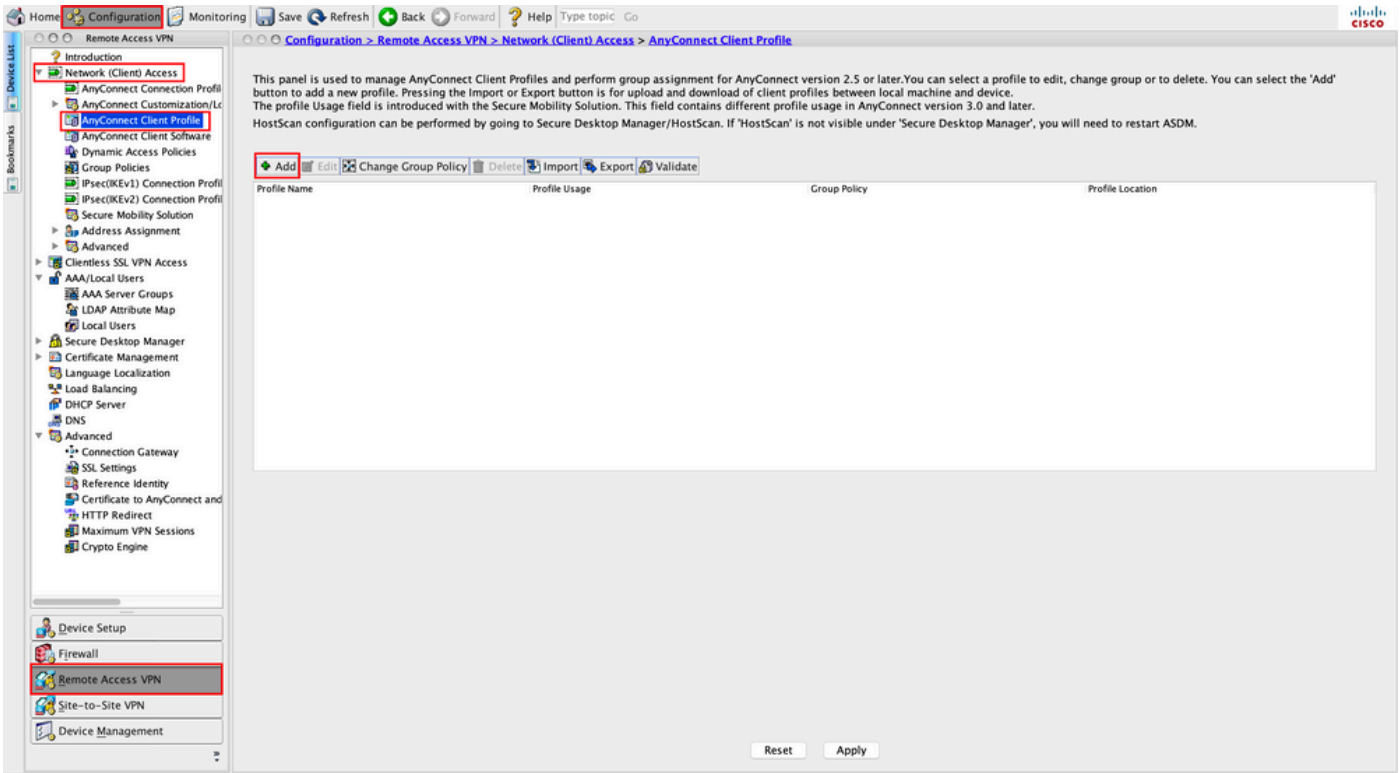


CLI-configuratie voor SSL Trustpoint:

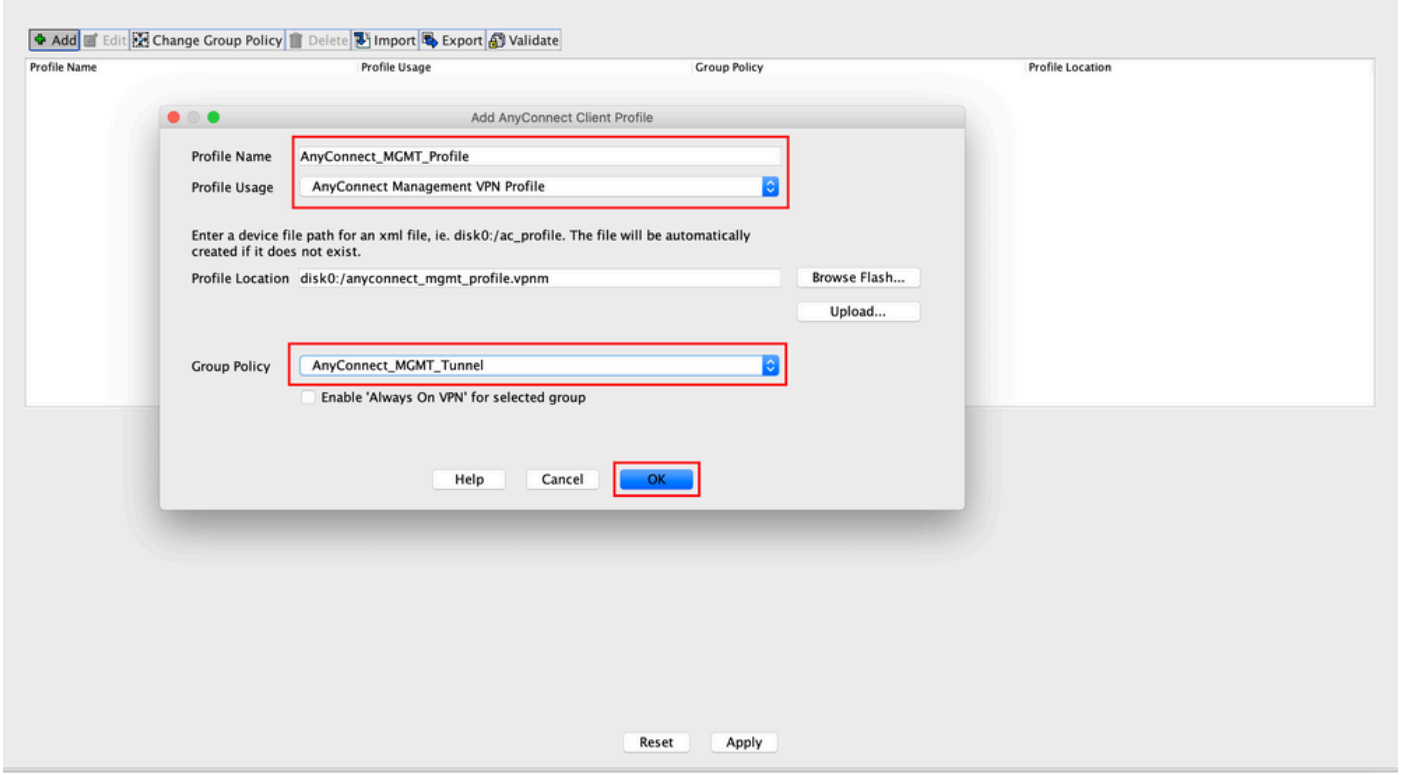
```
ssl trust-point ROOT-CA outside
```

VPN-profiel voor AnyConnect-beheer maken

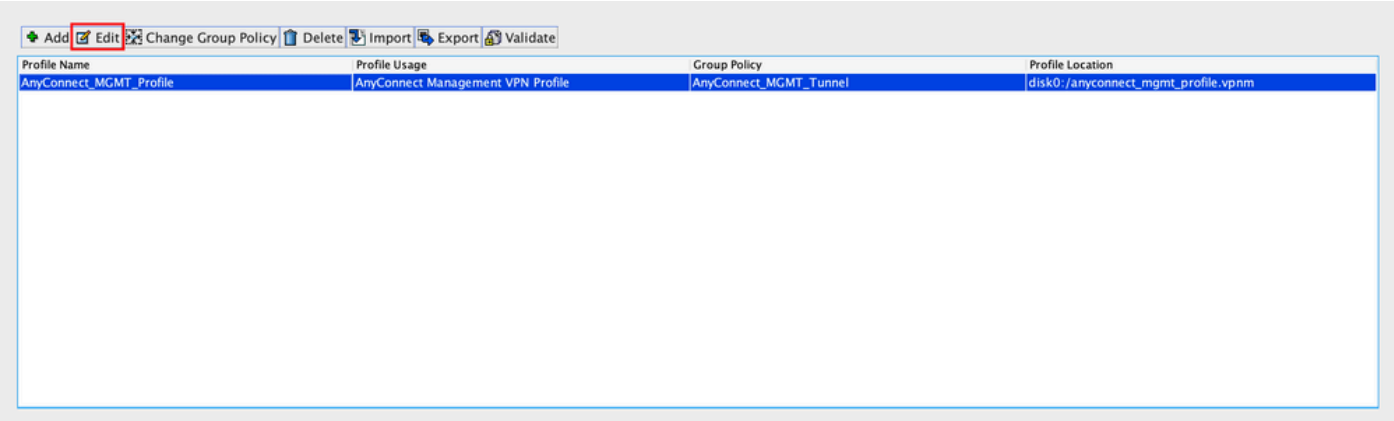
Stap 1. Maak het AnyConnect-clientprofiel. Naar navigeren Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile. Klik Add, zoals aangegeven in de afbeelding.



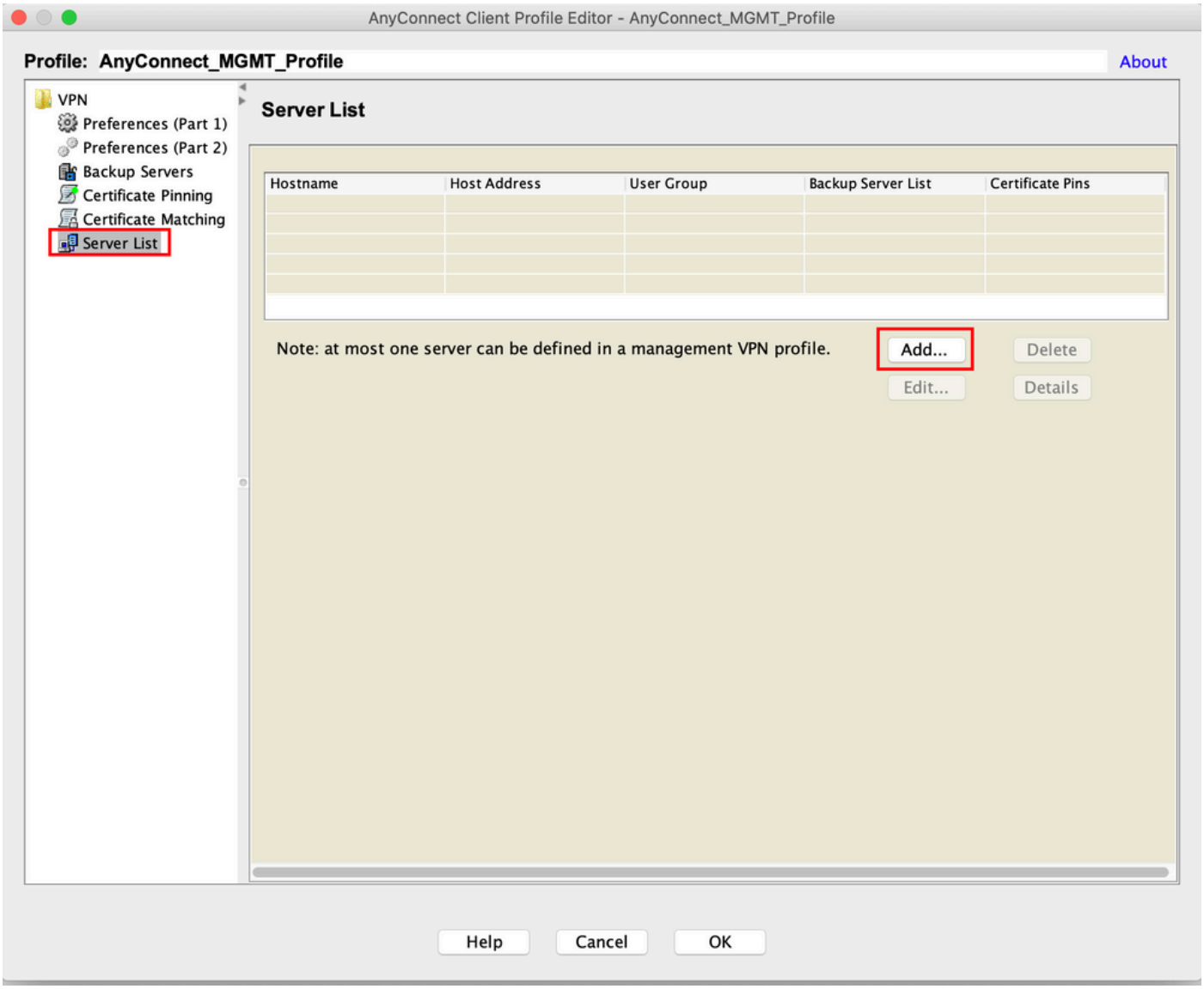
Stap 2. Een Profile Name. Kies de Profile Usage als AnyConnect Management VPN profile. Kies de Group Policy gemaakt in Stap 1. Klik OK , zoals aangegeven in de afbeelding.



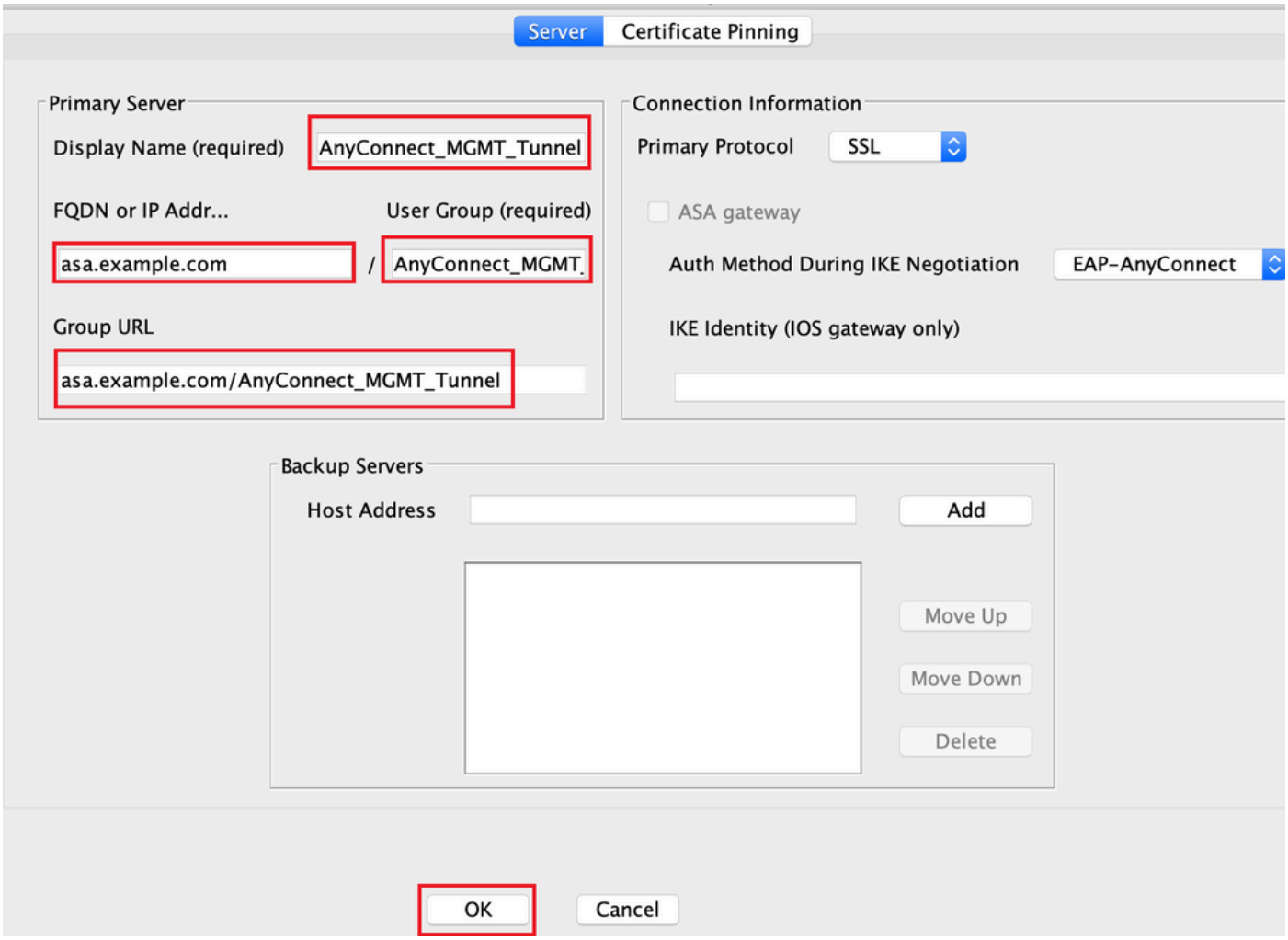
Stap 3. Kies het profiel dat u hebt gemaakt en klik op Edit, zoals aangegeven in de afbeelding.



Stap 4. Naar navigeren Server List. Klik Add om een nieuwe serverlijst toe te voegen, zoals in de afbeelding wordt getoond.



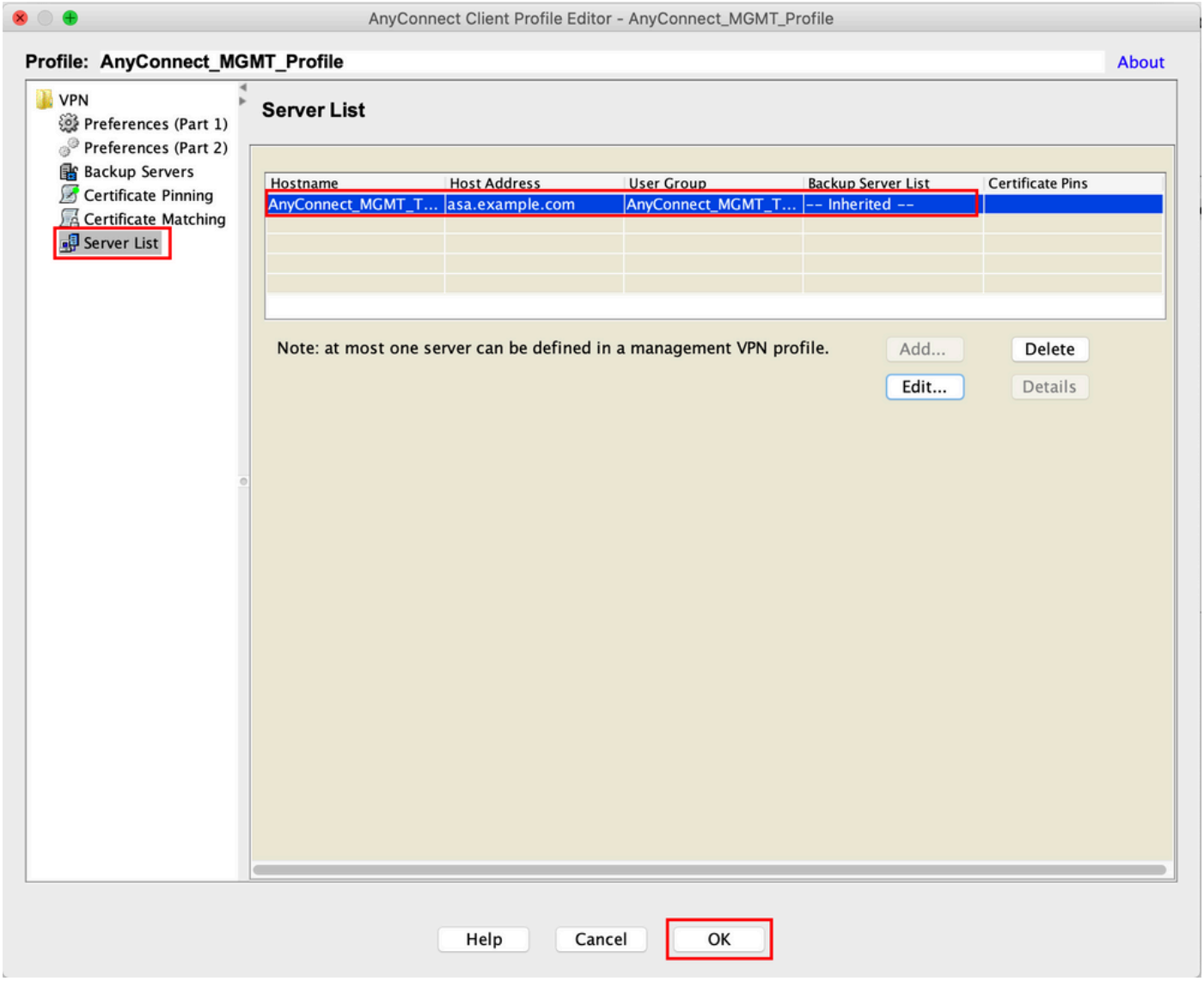
Stap 5. Een Display Name. Voeg het FQDN/IP address van de ASA. Geef de User Group als naam van de tunnelgroep. Group URL wordt automatisch ingevuld met de FQDN en User Group. Klik OK.



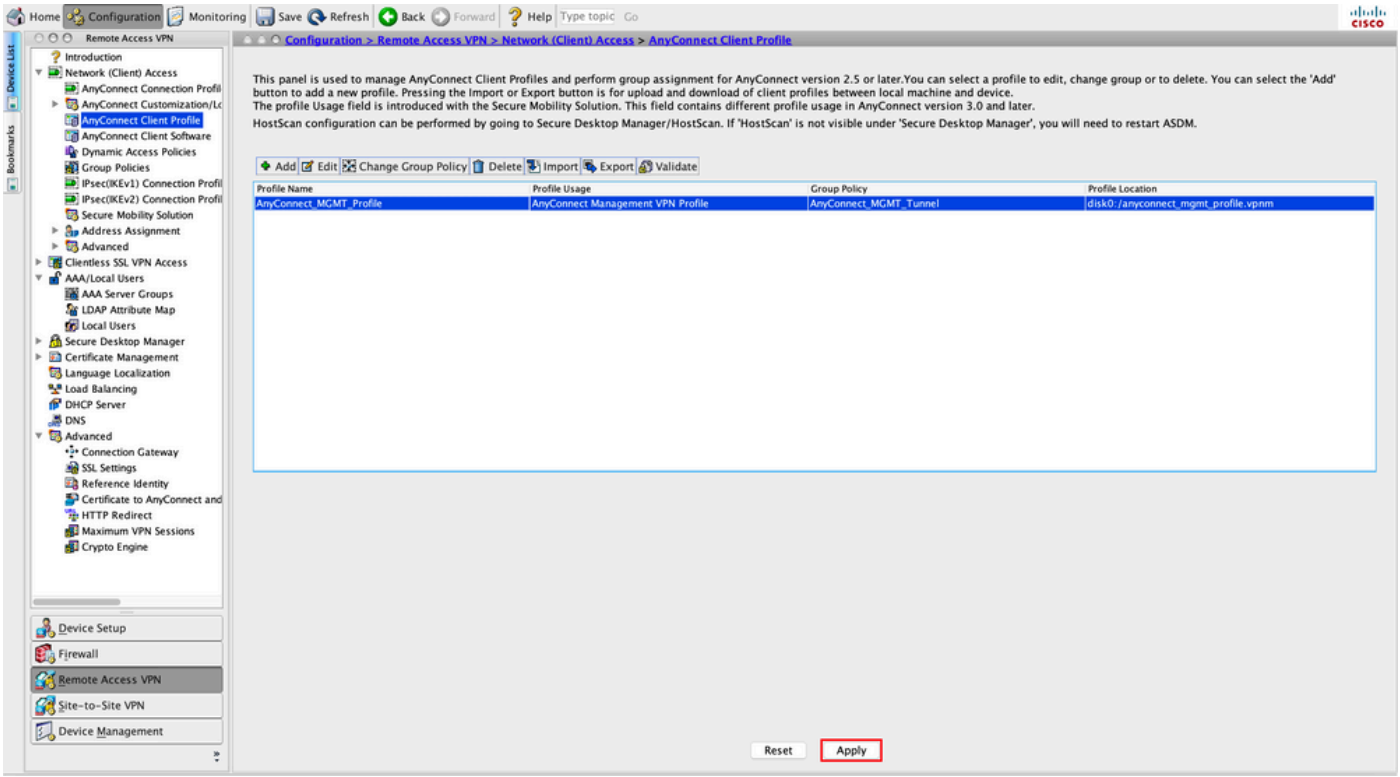
Opmerking: de FQDN/IP-adres + gebruikersgroep moet gelijk zijn aan de URL van de groep die wordt vermeld tijdens de configuratie van het AnyConnect-verbindingsprofiel in stap 8.

Opmerking: AnyConnect met IKEv2 als protocol kan ook worden gebruikt om Management VPN naar ASA te implementeren. verzekeren Primary Protocol is ingesteld op IPsec in stap 5.

Stap 6. Zoals in de afbeelding, klikt u op OK Opslaan.



Stap 7. Klik Apply tOm de configuratie naar de ASA te duwen, zoals in de afbeelding.



CLI-configuratie na toevoeging van AnyConnect Management VPN-profiel.

```
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
```

AnyConnect Management VPN-profiel op AnyConnect-clientmachine:

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




       <ShowPreConnectMessage>false</ShowPreConnectMessage>




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

--- Output Omitted ---
<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
<AllowManualHostInput>false</AllowManualHostInput> </ClientInitialization>
```

```
</AnyConnectProfile>
```

Opmerking: als Trusted Network Detection (TND) wordt gebruikt in het VPN-profiel van AnyConnect, is het raadzaam dezelfde instellingen in het VPN-profiel voor beheer aan te passen voor een consistente gebruikerservaring. De VPN-tunnel voor beheer wordt geactiveerd op basis van de TND-instellingen die zijn toegepast op het tunnelprofiel van de gebruiker VPN. Bovendien is de TND Connect-actie in het VPN-beheerprofiel (alleen afgedwongen wanneer de VPN-tunnel voor beheernetwerken actief is) altijd van toepassing op de VPN-tunnel van de gebruiker om ervoor te zorgen dat de VPN-tunnel voor beheernetwerken transparant is voor de eindgebruiker.

Opmerking: op elke eindgebruiker-pc, als de TND-instellingen in het VPN-profiel voor beheer zijn ingeschakeld en als het VPN-profiel van de gebruiker ontbreekt, worden de standaardinstellingen voor de TND (het is uitgeschakeld op de standaardvoorkeuren in de AC-clienttoepassing) in plaats van het ontbrekende VPN-profiel van de gebruiker bekeken. Deze mismatch kan leiden tot onverwacht/niet gedefinieerd gedrag.
In de standaardinstellingen worden de TND-instellingen standaard uitgeschakeld.
Om de standaardvoorkeuren voor hardgecodeerde instellingen in de AnyConnect-clienttoepassing te overwinnen, moet de eindgebruiker-pc twee VPN-profielen hebben, een VPN-profiel voor gebruikers en een VPN-profiel voor AC Management, en moeten beide dezelfde TND-instellingen hebben.
De logica achter de VPN-tunnelverbinding en ontkoppeling van het beheer is dat om een VPN-tunnel voor het beheer tot stand te brengen, de AC-agent de TND-instellingen van het VPN-profiel van de gebruiker gebruikt en voor het ontkoppelen van de VPN-tunnel voor het beheer controleert op TND-instellingen voor het VPN-profiel van het beheer.

Implementatiemethoden voor AnyConnect Management VPN-profiel

- Een succesvolle VPN-verbinding van de gebruiker is voltooid met het ASA-verbindingsprofiel om het AnyConnect Management VPN-profiel te downloaden van de VPN-gateway.

  Opmerking: als het protocol voor de VPN-tunnel voor beheer IKEv2 is, moet de eerste verbinding tot stand worden gebracht via SSL (om het AnyConnect Management VPN-profiel van de ASA te downloaden).

- Het AnyConnect Management VPN-profiel kan handmatig naar de clientmachines worden geüpload via een GPO-push of via een handmatige installatie (Controleer of de naam van het profiel juist is `VpnMgmtTunProfile.xml`).

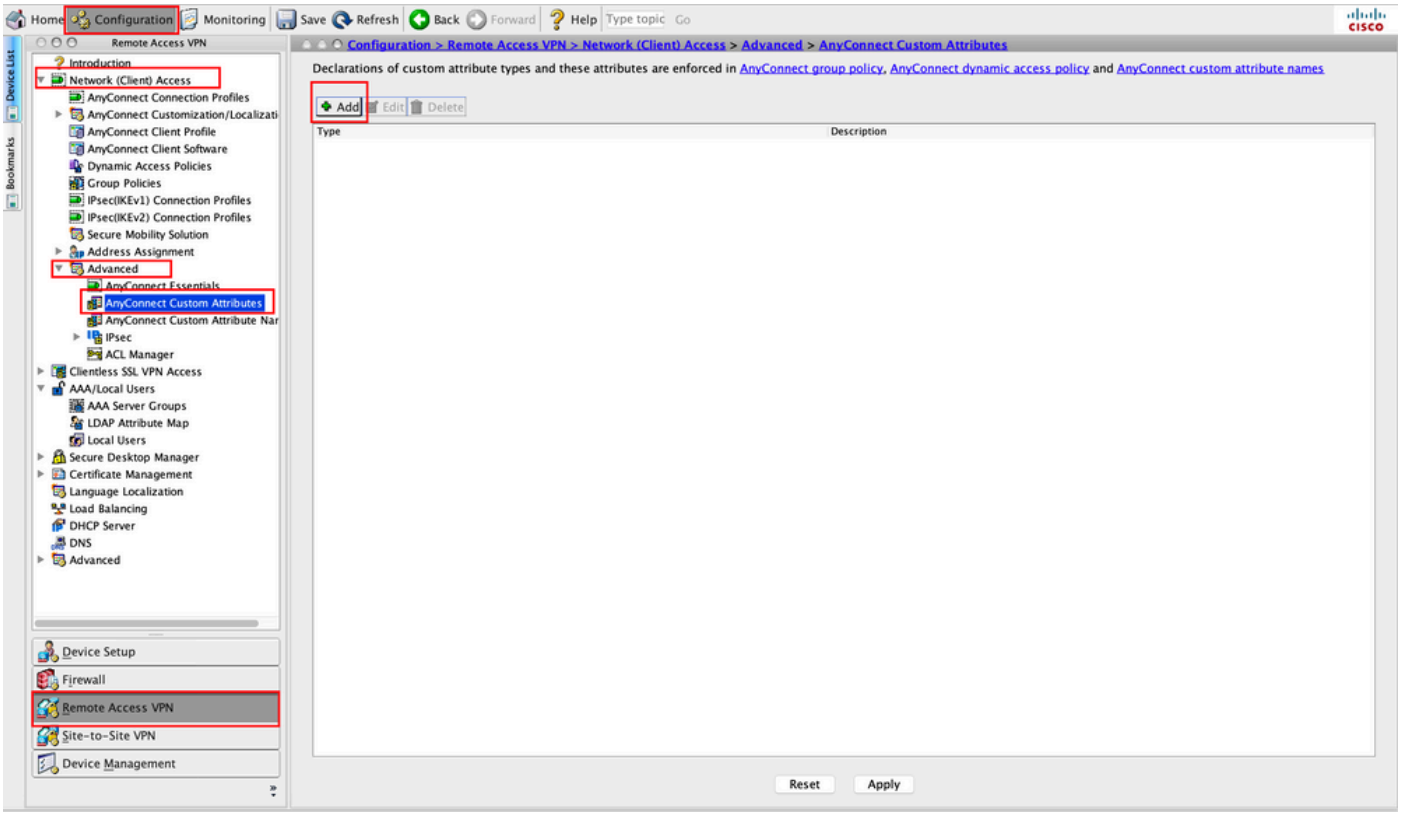
  Locatie van map waarin het profiel moet worden toegevoegd:
  Windows: **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun**
  macOS: /opt/cisco/anyconnect/profile/mgmttun/

(Optioneel) Configureer een aangepast kenmerk om de configuratie van alle tunnels te ondersteunen

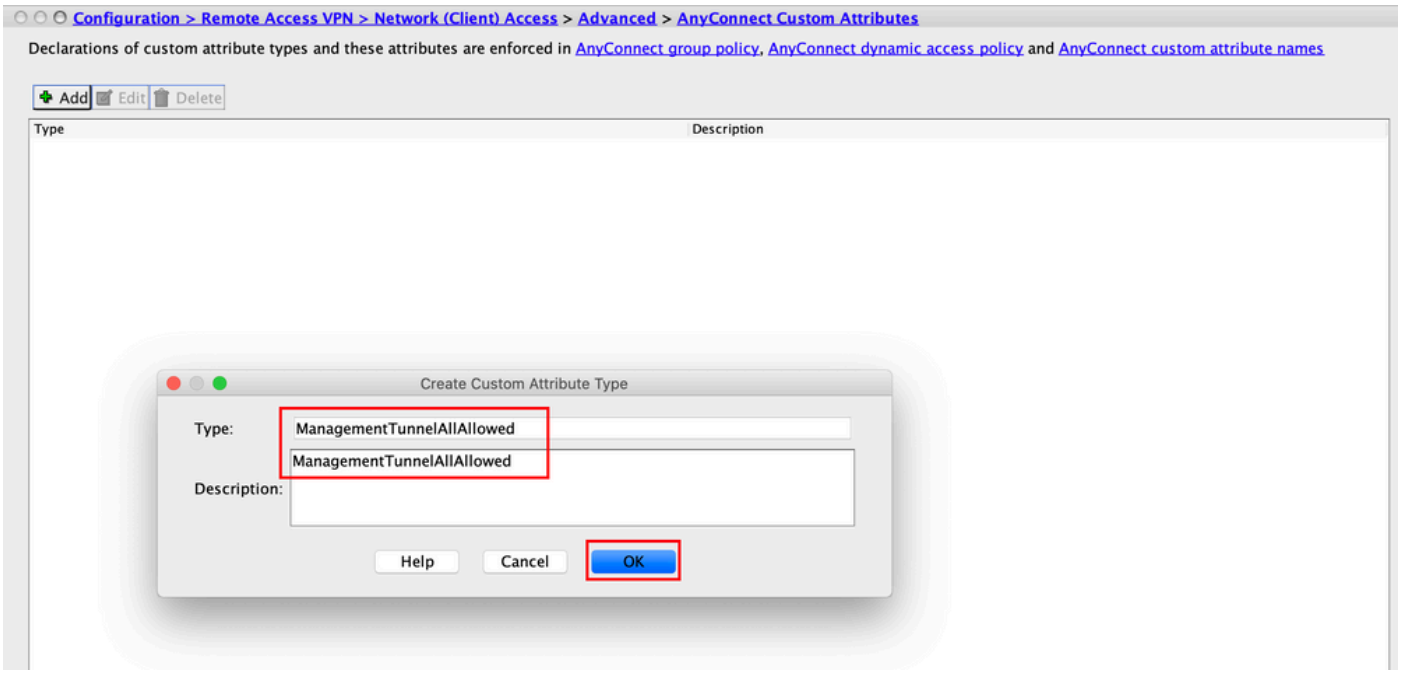
Een VPN-tunnel voor beheer vereist standaard een splitsing die tunnelconfiguratie omvat om gevolgen voor de door de gebruiker geïnitieerde netwerkcommunicatie te voorkomen. Dit kan worden overschreven wanneer u het aangepaste kenmerk configureert in het groepsbeleid dat

wordt gebruikt door de beheertunnelverbinding.

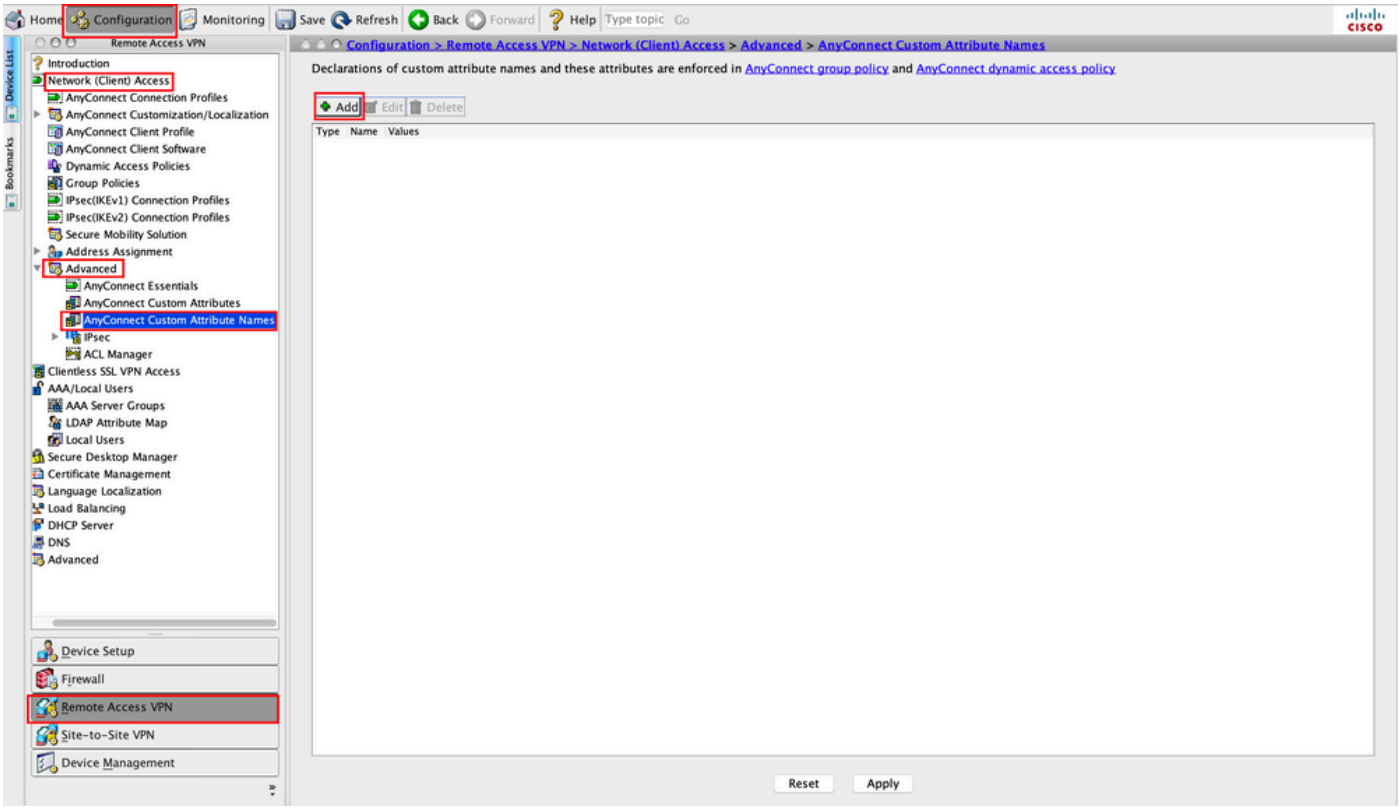
Stap 1. Naar navigerenConfiguration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes. Klik Add, zoals aangegeven in de afbeelding.



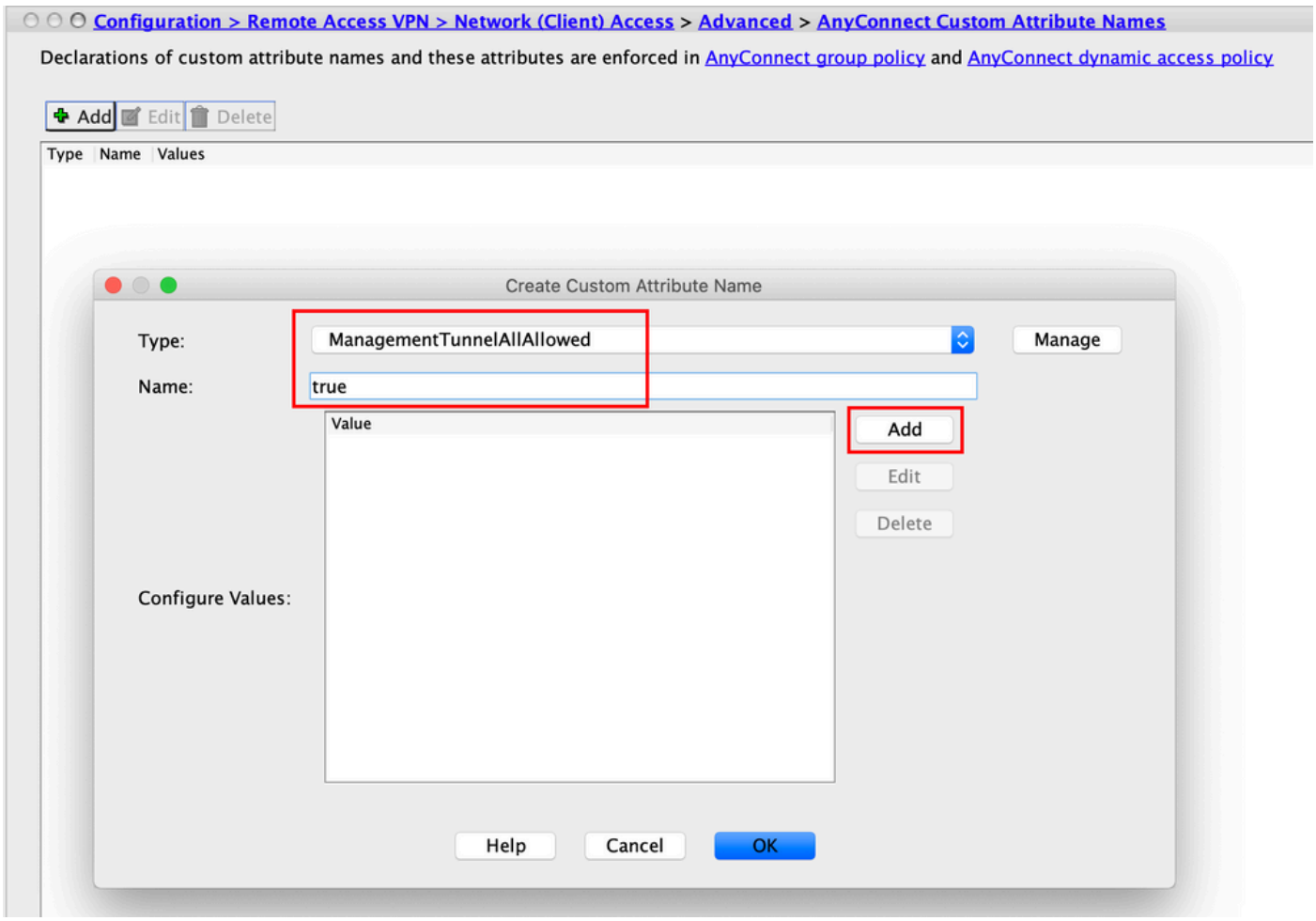
Stap 2. Stel het aangepaste attribuut Type in op ManagementTunnelAllAllowed en bieden een Description. Klik OK, zoals aangegeven in de afbeelding.



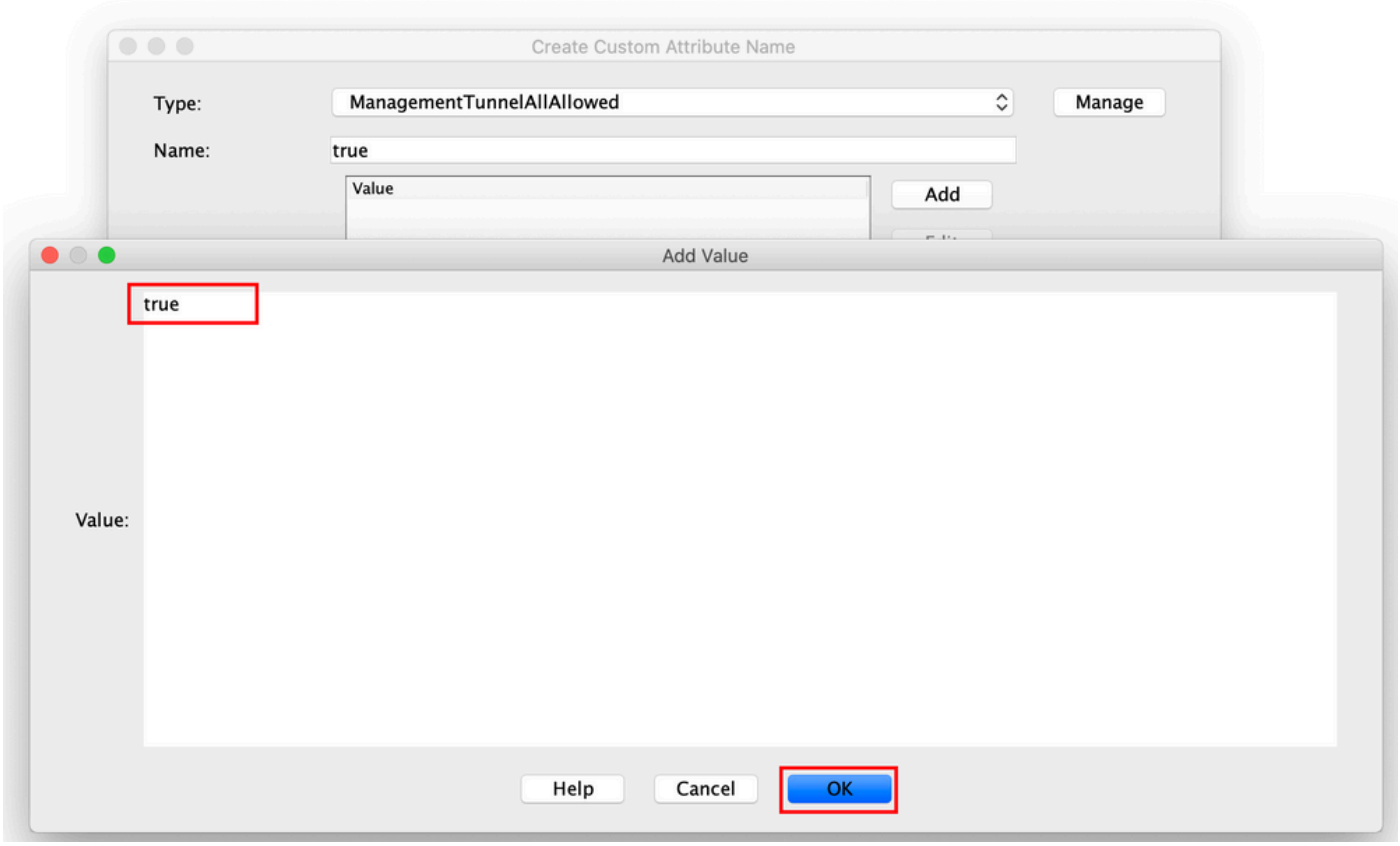
Stap 3. Naar navigeren **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names.** Klik Add, zoals aangegeven in de afbeelding.



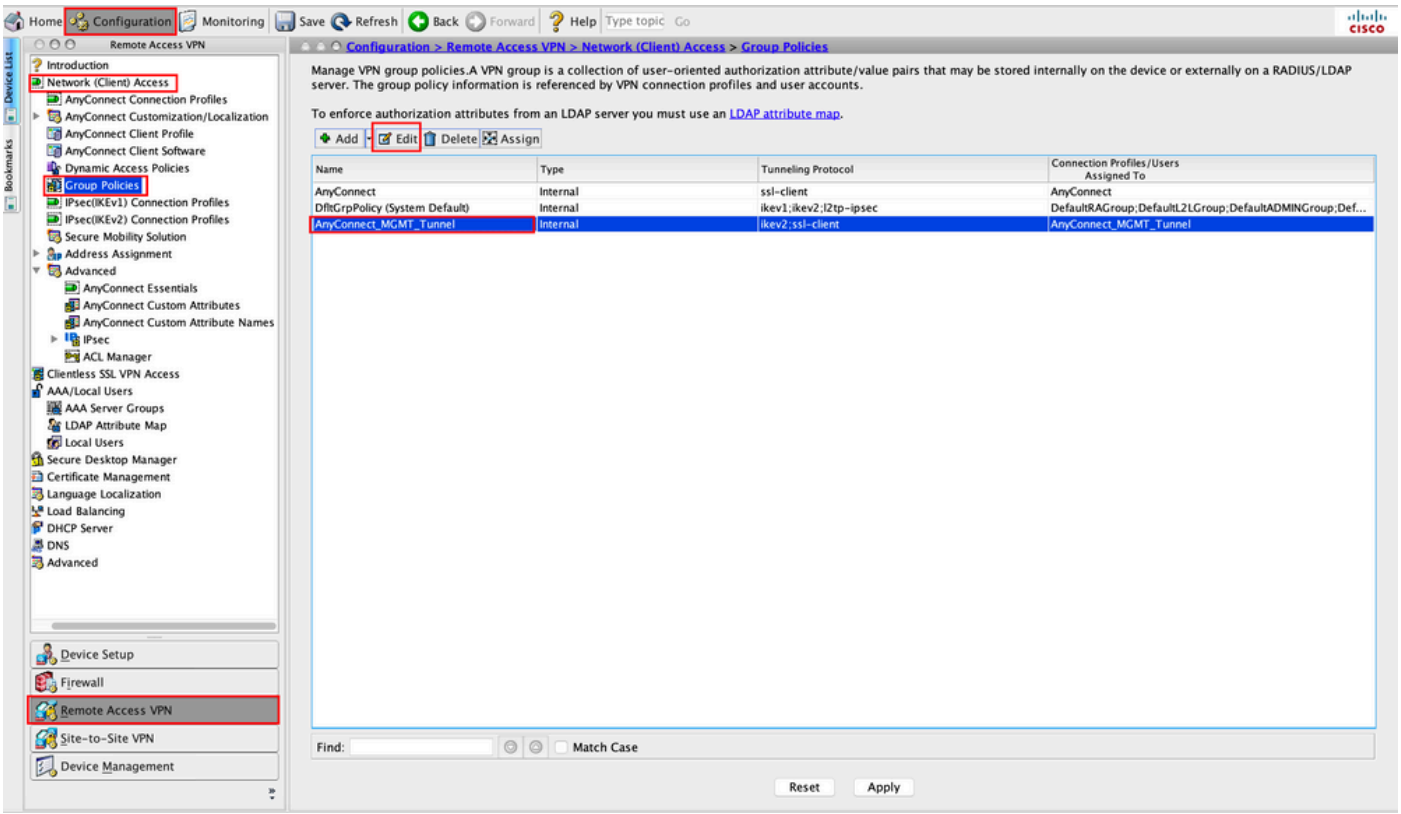
Stap 4. Kies het type als **ManagementTunnelAllAllowed** . Stel de naam in op true. Klik Addom een waarde voor eigen kenmerken te bepalen, zoals in de afbeelding.



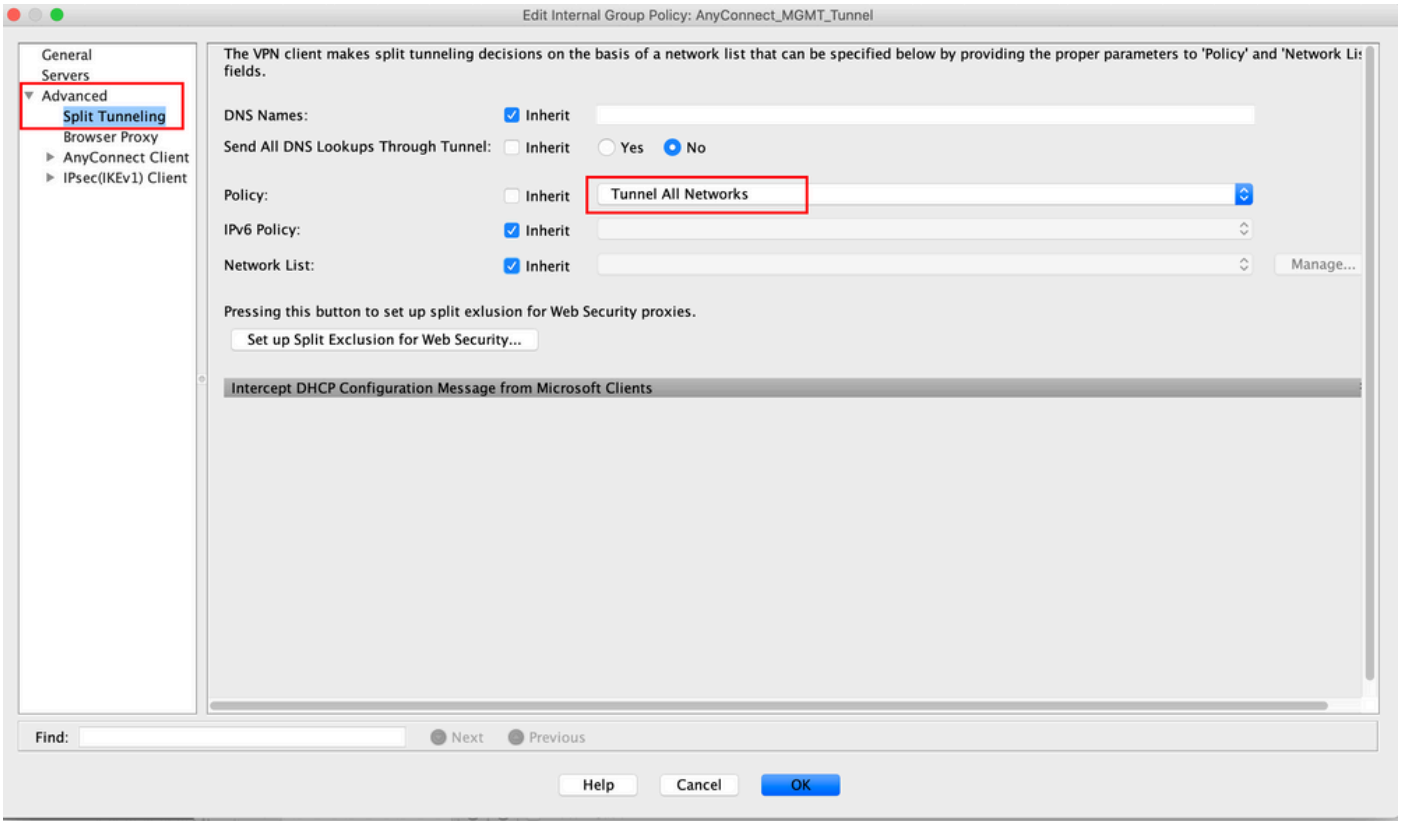
Stap 5. Stel de waarde in op true. Klik OK, zoals aangegeven in de afbeelding.



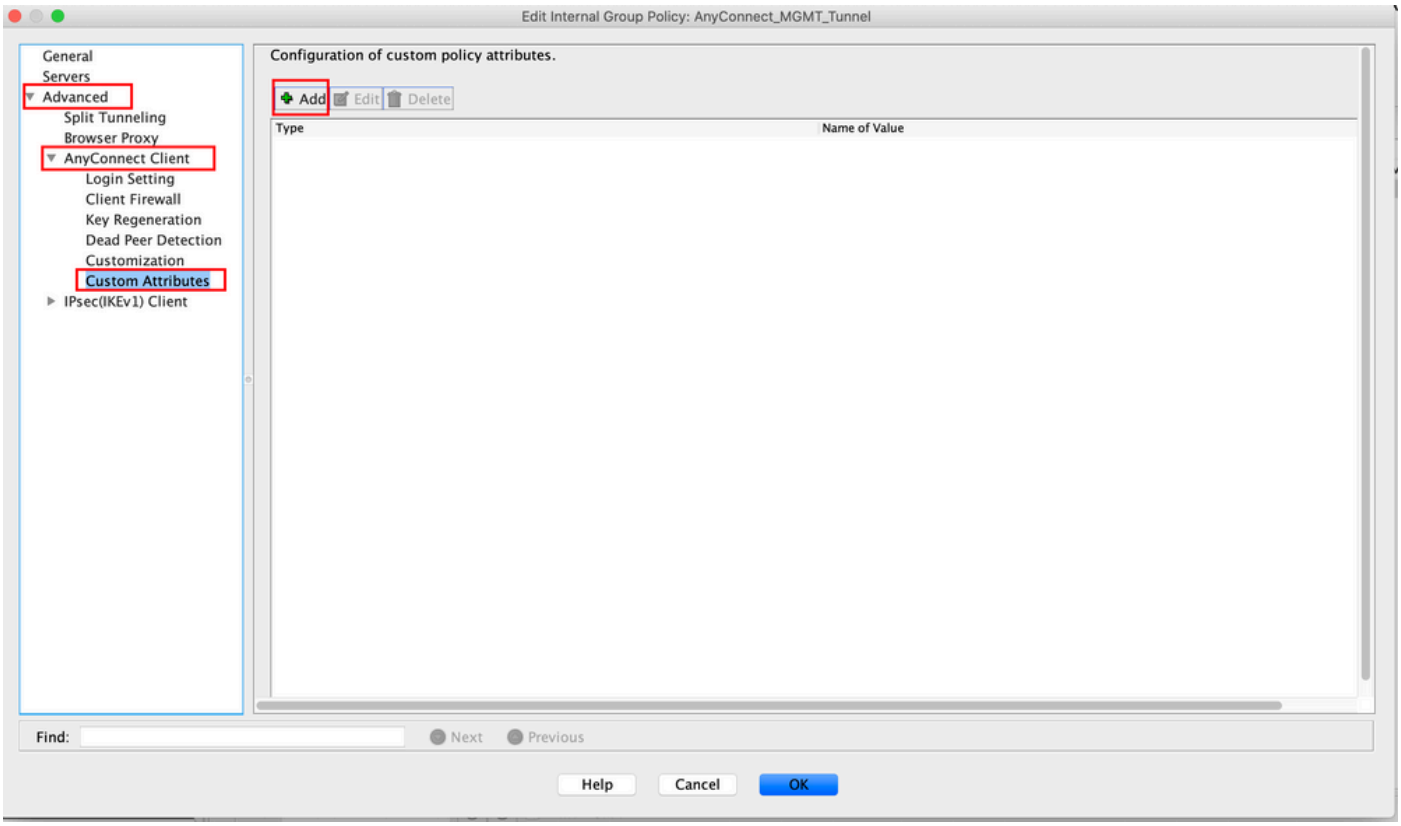
Stap 6. Naar navigeren Configuration > Remote Access VPN > Network (Client) Access > Group Policies. Kies het groepsbeleid. Klik Edit , zoals aangegeven in de afbeelding.



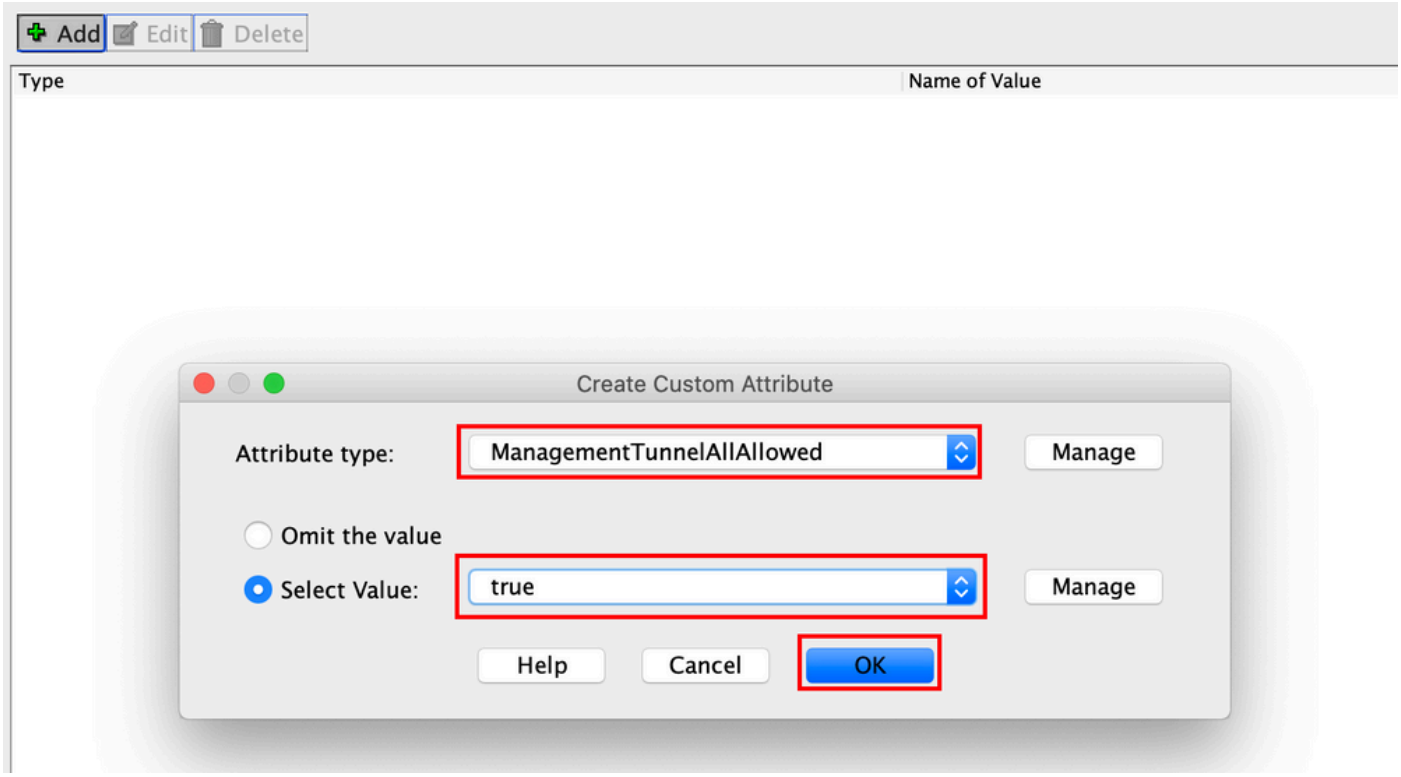
Stap 7. Zoals in deze afbeelding wordt getoond, navigeer naar Advanced > Split Tunneling. Het beleid configureren als Tunnel All Networks.



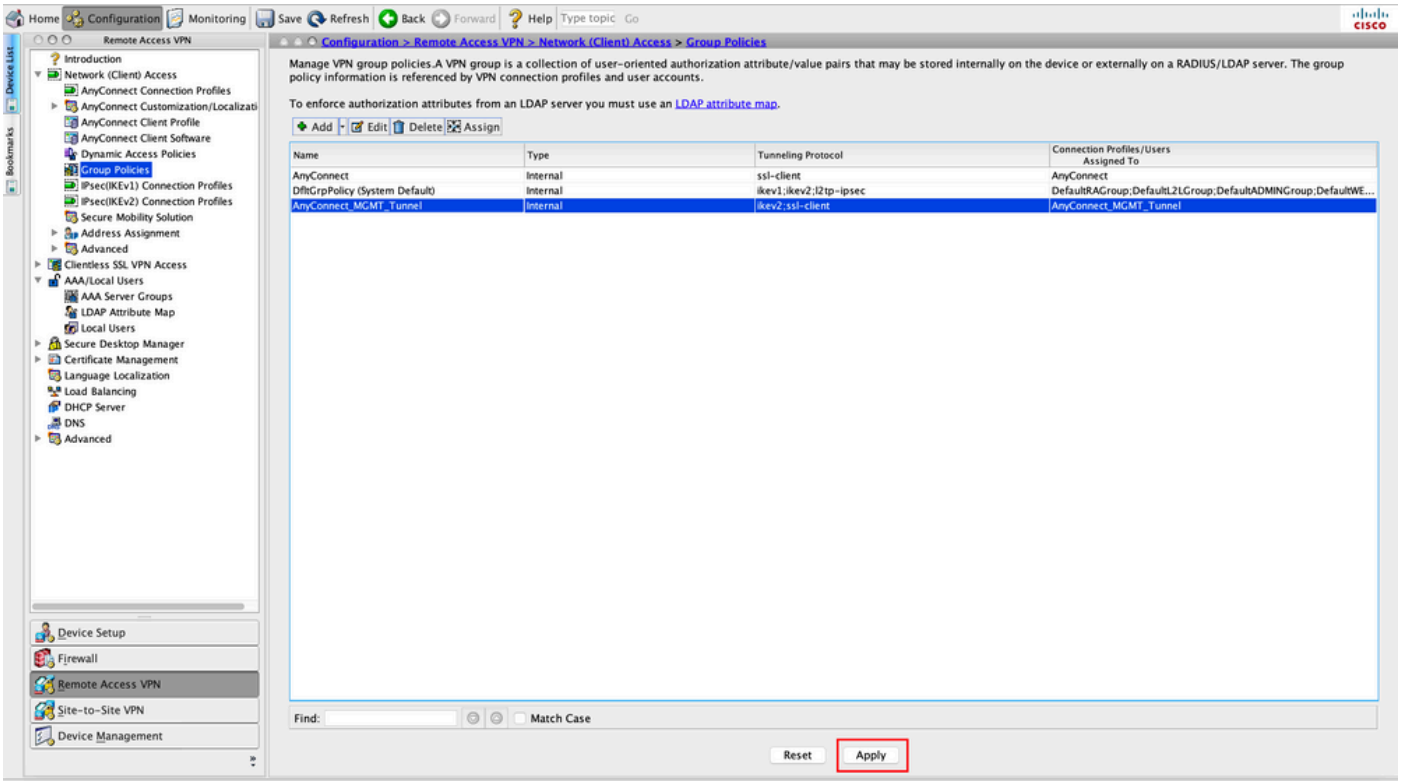
Stap 8. Naar navigeren Advanced > Anyconnect Client > Custom Attributes. Klik Add, zoals aangegeven in de afbeelding.



Stap 9. Type kenmerk kiezen als ManagementTunnelAllAllowed en kies de Waarde als true. Klik OK, zoals aangegeven in de afbeelding.



Stap 10. Klik Apply om de configuratie naar de ASA te duwen, zoals in de afbeelding wordt getoond.



CLI-configuratie na de ManagementTunnelAllAllowed Aangepaste eigenschap wordt toegevoegd:

```
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
```

Verifiëren

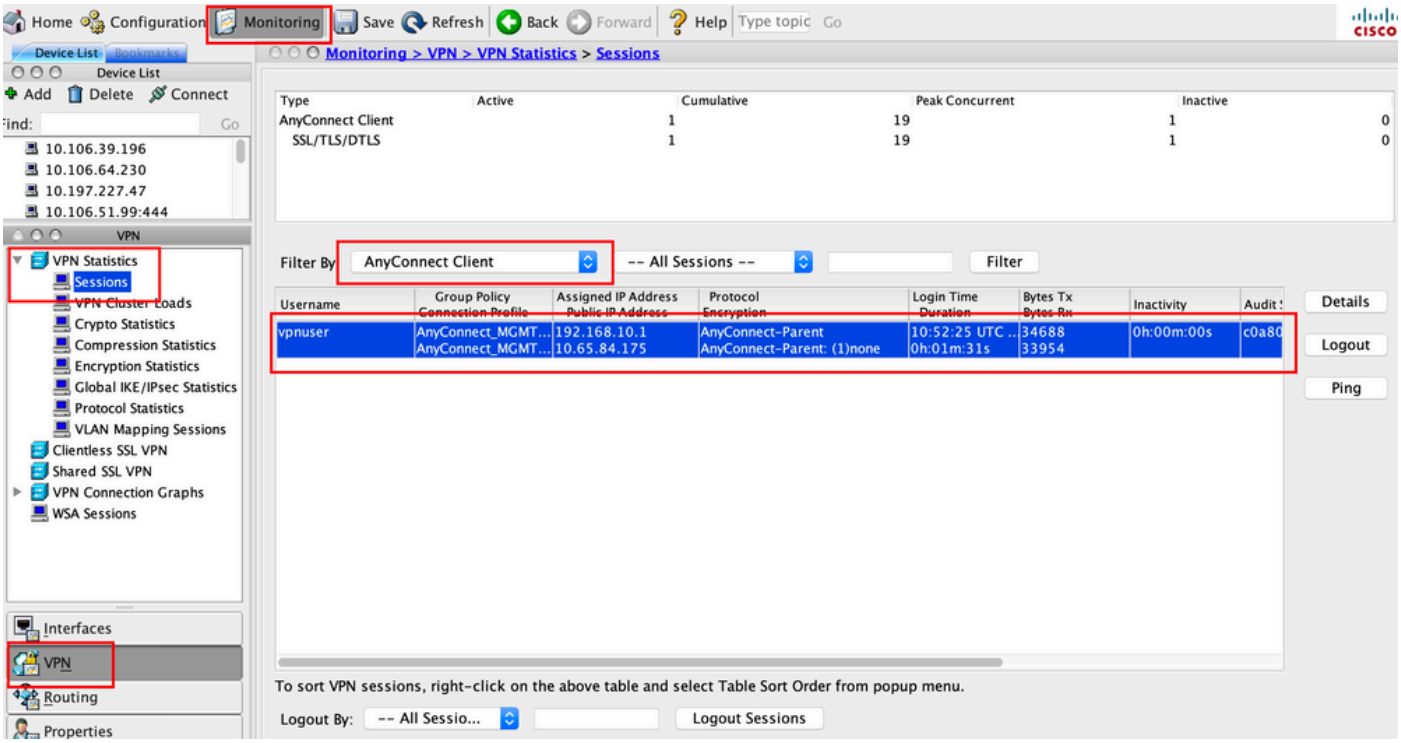
Controleer de VPN-tunnelverbinding van beheer op ASA CLI met de `show vpn-sessiondb detail anyconnect` uit.

```
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
```

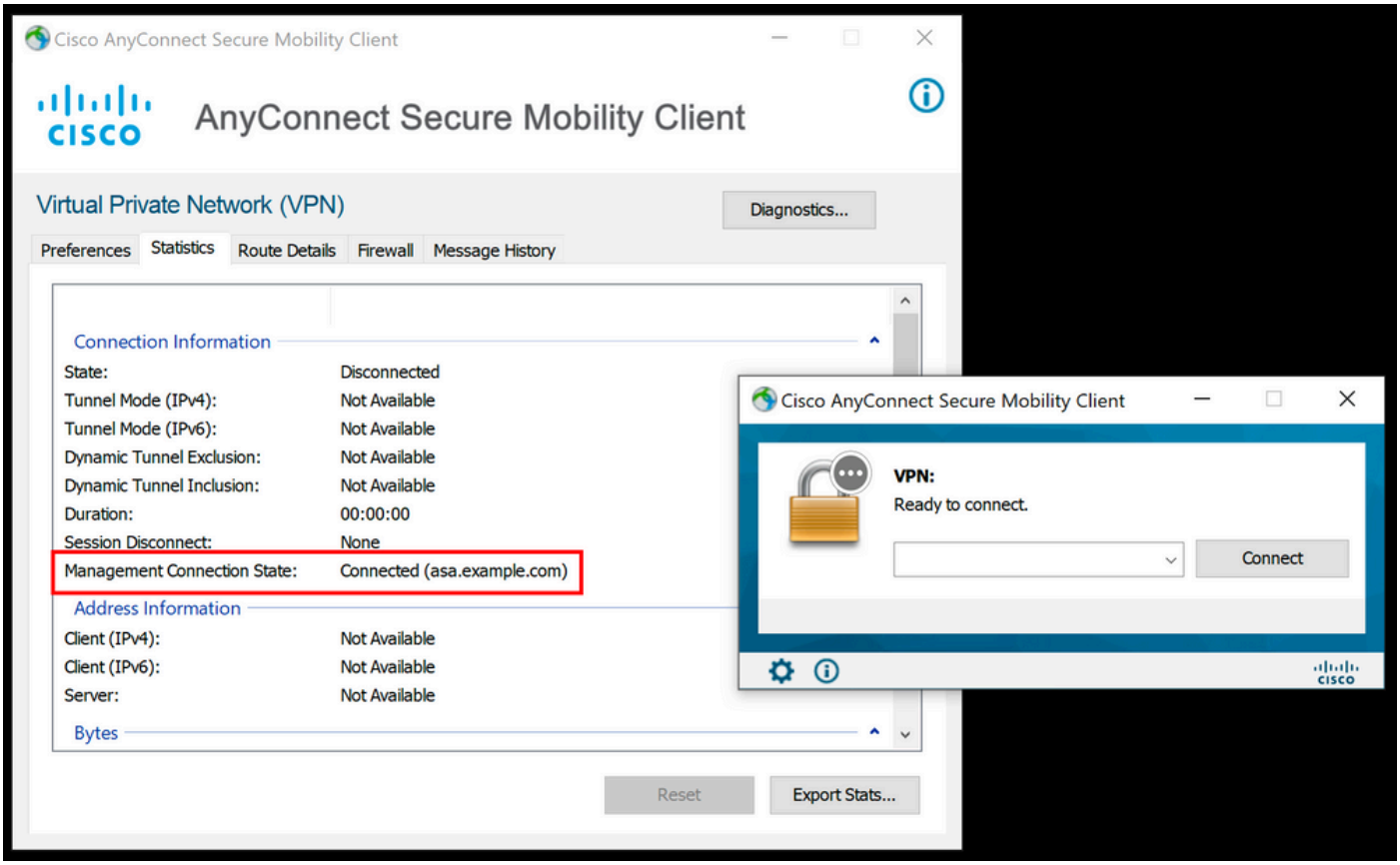
```
Ciphersuite  : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2              UDP Src Port : 57053
UDP Dst Port : 443                   Auth Mode    : Certificate
Idle Time Out: 30 Minutes            Idle TO Left : 18 Minutes
Client OS    : Windows
Client Type  : DTLS VPN Client
Client Ver   : 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
```

Controleer de VPN-tunnelverbinding van het beheer op ASDM.

Navigeer naar **Monitoring > VPN > VPN-statistieken > Sessies** . Filteren op **AnyConnect-client** om de clientsessie te bekijken.



Verificatie van de VPN-tunnelverbinding van beheer op de clientmachine:



Problemen oplossen

De nieuwe UI Statistics-lijn (Management Connection State) kan worden gebruikt om problemen op te lossen met de connectiviteit van de beheerstunnel. Dit zijn de meest voorkomende fouttoestanden:

Verbinding verbroken (uitgeschakeld):

- Deze optie is uitgeschakeld.
- Zorg ervoor dat het VPN-beheerprofiel is geïmplementeerd op de client, via een verbinding met een gebruikerstunnel (u moet het VPN-beheerprofiel toevoegen aan het beleid van de gebruikerstunnel-groep) of buiten de band via de handmatige upload van het profiel.
- Zorg ervoor dat het VPN-beheerprofiel is geconfigureerd met één hostingang die een tunnelgroep omvat.

Verbroken (vertrouwd netwerk):

- TND heeft een vertrouwd netwerk gedetecteerd zodat de beheerstunnel niet tot stand is gebracht.

Verbroken (gebruikerstunnel actief):

- Een VPN-tunnel voor gebruikers is momenteel actief.

Verbinding verbroken (proces is niet gestart):

- Een fout bij de start van het proces is opgetreden wanneer de verbinding met de

beheerstunnel wordt geprobeerd.

Verbinding verbroken (verbinding mislukt):

- Een verbindingsmislukking werd ontmoet toen de beheerstunnel wordt gevestigd.
- Zorg ervoor dat de certificaatverificatie is geconfigureerd in de tunnelgroep, dat er geen banner aanwezig is in het groepsbeleid en dat het servercertificaat moet worden vertrouwd.

Verbroken (ongeldige VPN-configuratie):

- Een ongeldige gesplitste tunnelconfiguratie is ontvangen van de VPN-server.
- Controleer de configuratie van gesplitste tunnels in het beleid van de beheertunnelgroep.

Verbinding verbroken (software-update in behandeling):

- Een AnyConnect-software-update is momenteel in behandeling.

Verbroken:

- De beheerstunnel staat op het punt te worden opgezet of kan om een andere reden niet worden opgezet.

Verzamel DART voor verdere probleemoplossing.

Gerelateerde informatie

- Configuratie van VPN-tunnelbeheer
- VPN-tunnel voor probleemoplossing
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.