Remote Access VPN configureren op FTD beheerde via FDM

Inhoud

Inleiding

Dit document beschrijft hoe de implementatie van een RA VPN op FTD die wordt beheerd door de on-box manager FDM die versie 6.5.0 en hoger uitvoert, moet worden geconfigureerd.

Voorwaarden

Vereisten

Cisco raadt u aan bekend te zijn met de configuratie van Remote Access Virtual Private Network (RA VPN) op Firepower Device Manager (FDM).

Licentie

- Firepower Threat Defense (FTD) is geregistreerd bij het slimme licentieportal met de optie Exporteren gecontroleerde functies (zodat het tabblad RA VPN-configuratie kan worden ingeschakeld)
- Alle AnyConnect-licenties ingeschakeld (APEX, Plus of alleen VPN)

Gebruikte componenten

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

- Cisco FTD waarop versie 6.5.0-15 wordt uitgevoerd
- Cisco AnyConnect Secure Mobility Client, versie 4.7.01076

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.

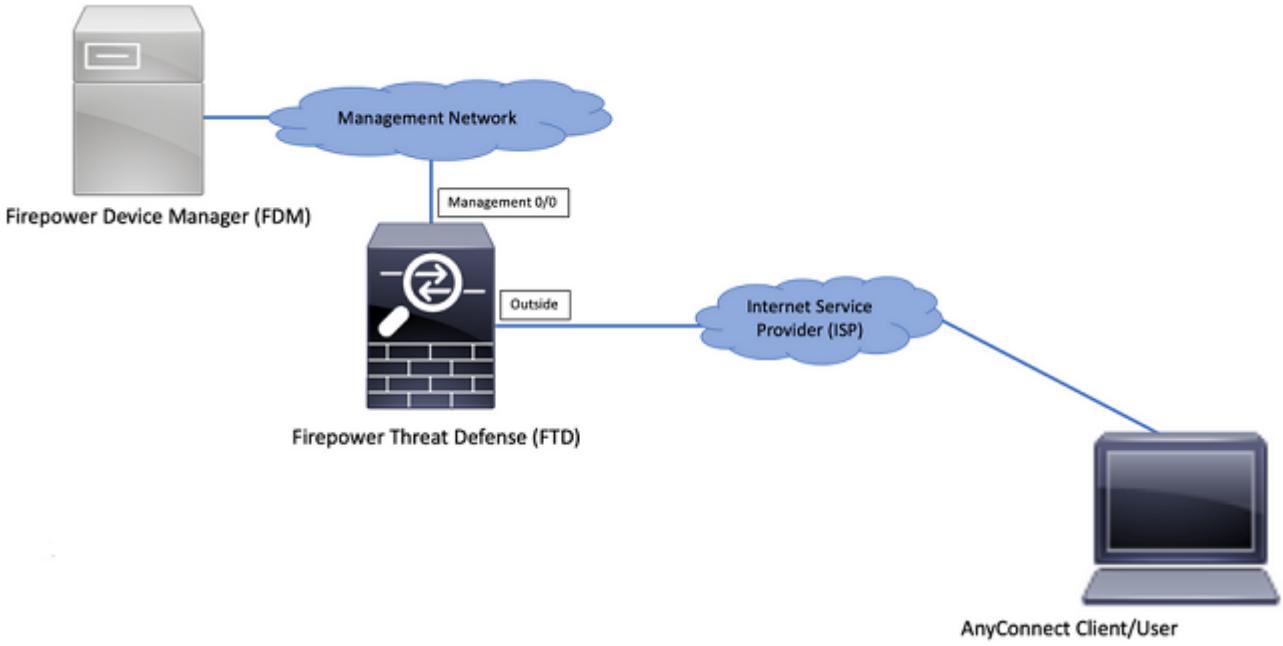
Achtergrondinformatie

De configuratie van FTD via FDM levert problemen op wanneer u probeert verbindingen te maken voor AnyConnect-clients via de externe interface terwijl het beheer via dezelfde interface wordt benaderd. Dit is een bekende beperking van FDM. Voor dit probleem is een verbeteringsverzoek ingediend voor CSCvm76499.

Configureren

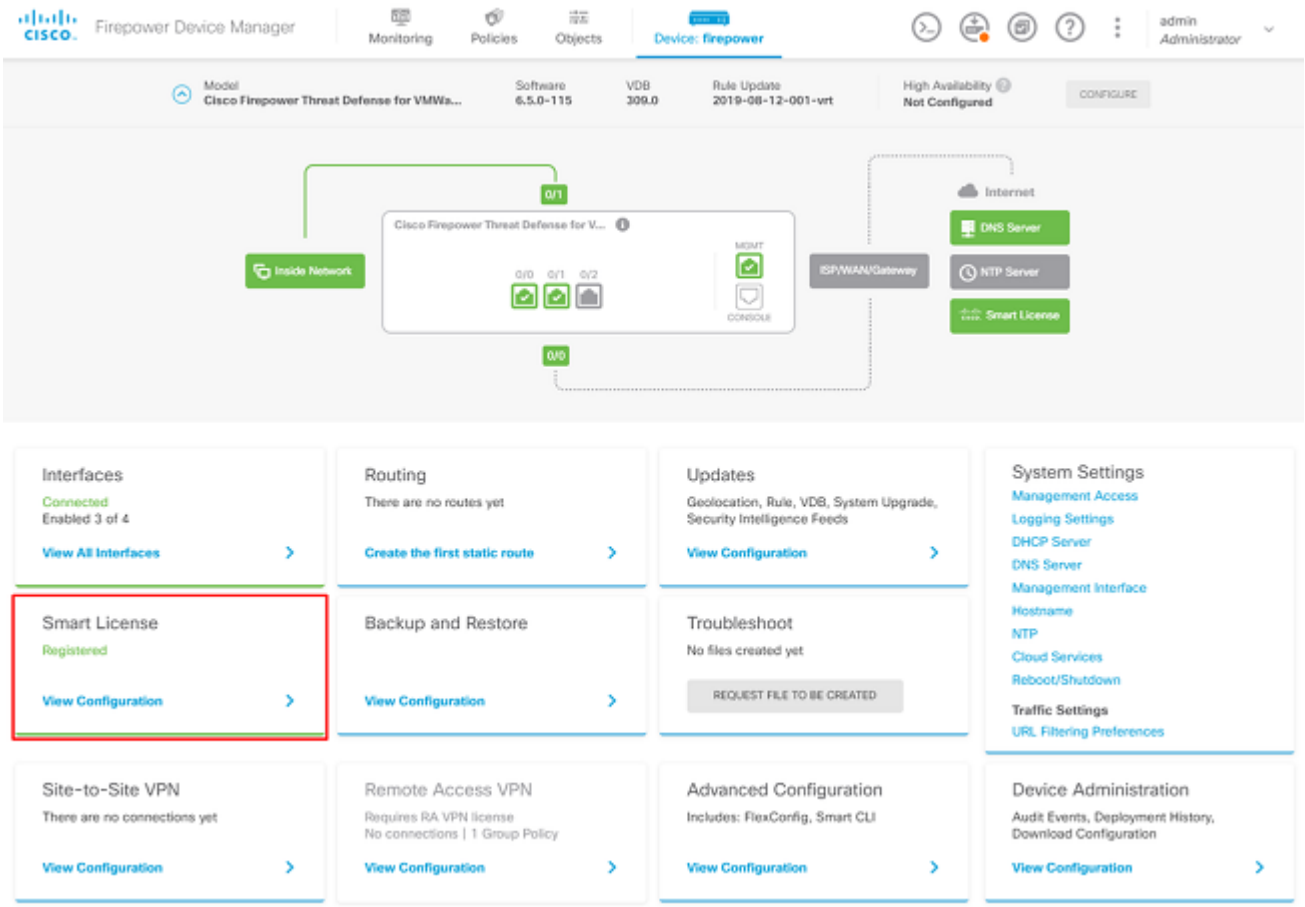
Netwerkdiagram

AnyConnect-clientverificatie met het gebruik van lokaal.

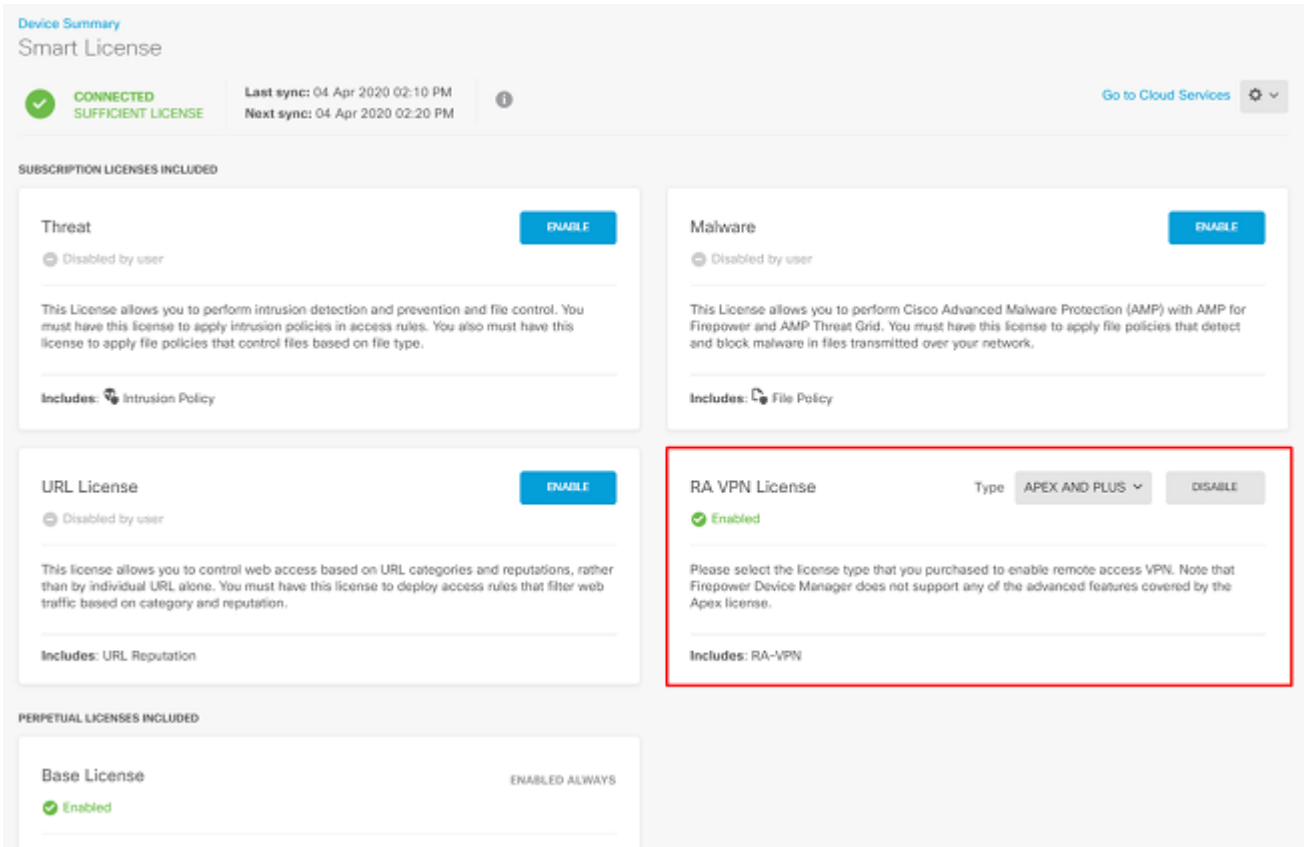


Controleer de licentiëring op de FTD

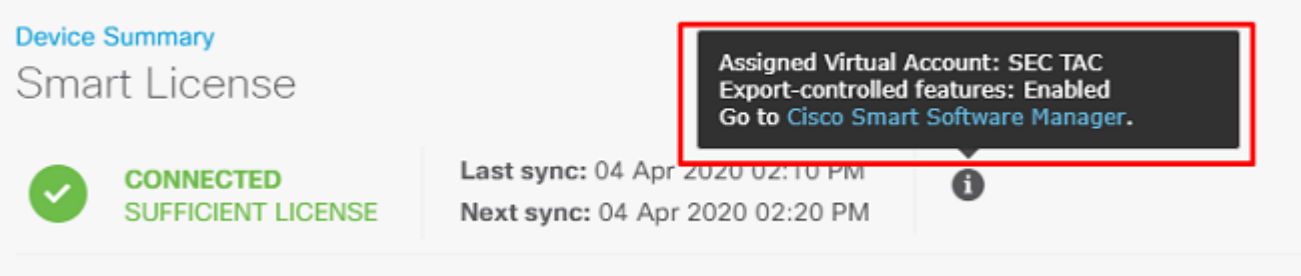
Stap 1. Controleer of het apparaat is geregistreerd voor Smart Licensing zoals in de afbeelding:



Stap 2. Controleer of AnyConnect-licenties op het apparaat zijn ingeschakeld zoals in het beeld wordt weergegeven.

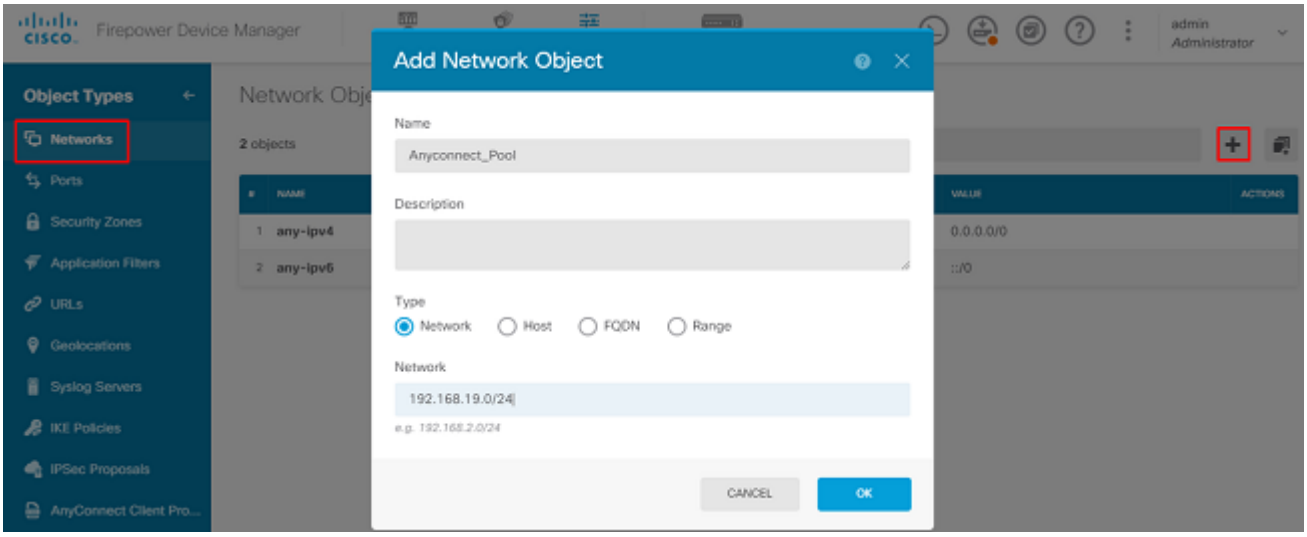


Stap 3. Controleer of door export gestuurde functies in het token zijn ingeschakeld zoals in het afbeelding:

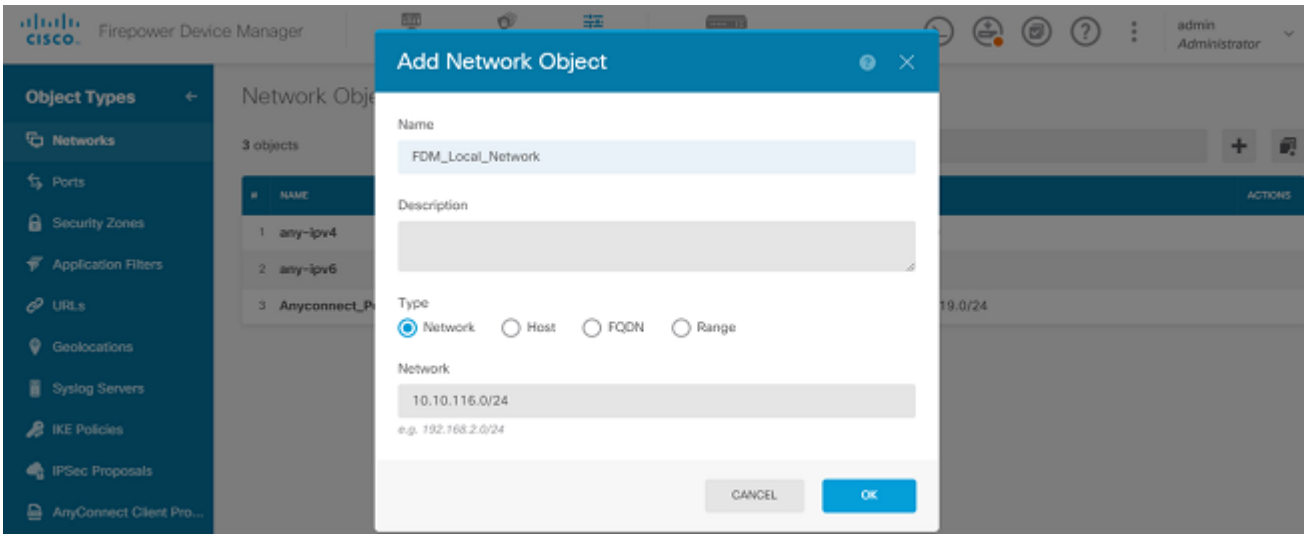


Beschermde netwerken definiëren

Naar navigeren Objects > Networks > Add new Network. Configureer VPN Pool- en LAN-netwerken vanuit FDM GUI. Maak een VPN-pool om te worden gebruikt voor lokale adrestoewijzing aan AnyConnect-gebruikers zoals in de afbeelding:

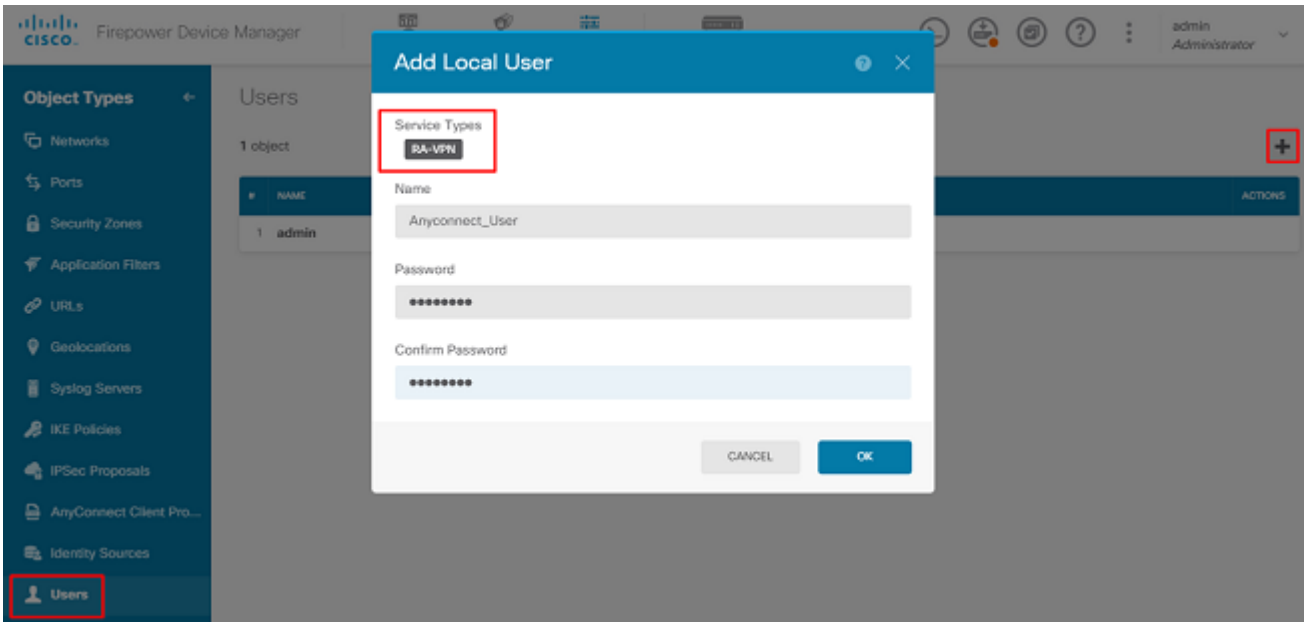


Maak een object voor het lokale netwerk achter het FDM-apparaat zoals in de afbeelding:



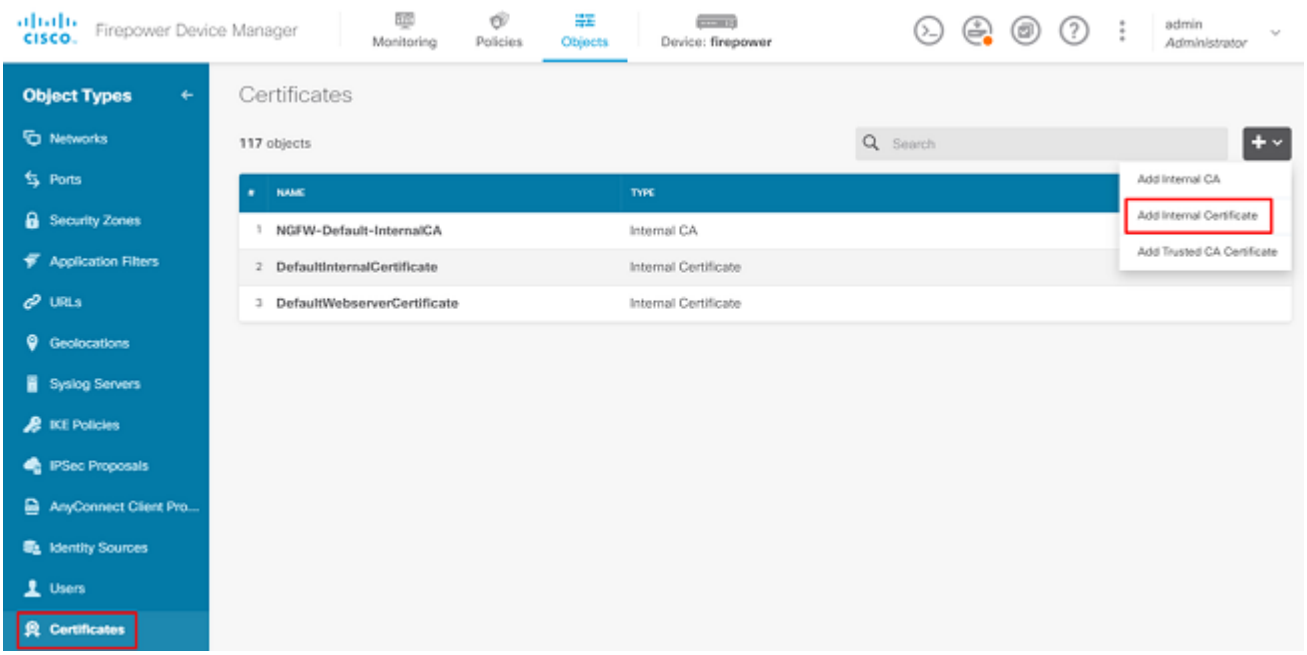
Lokale gebruikers maken

Naar navigeren Objects > Users > Add User. Voeg VPN Local gebruikers toe die verbinding maken met FTD via AnyConnect. Lokale gebruikers maken zoals in de afbeelding:

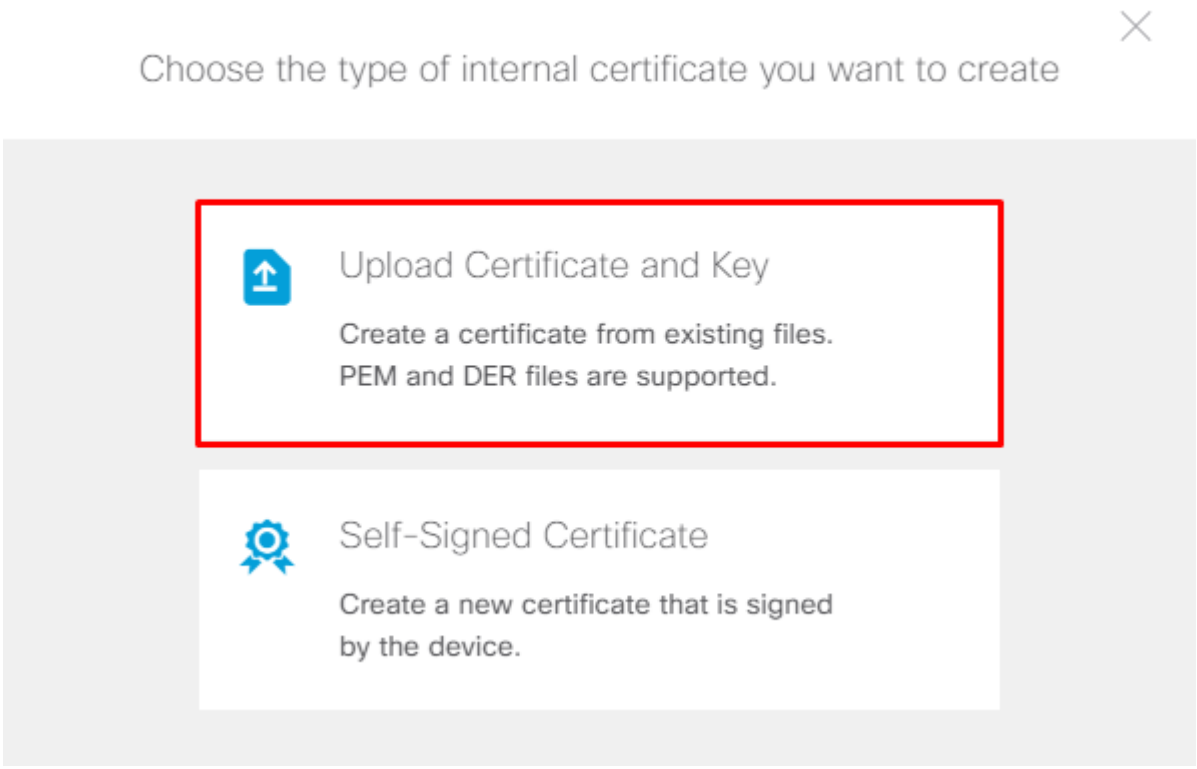


Certificaat toevoegen

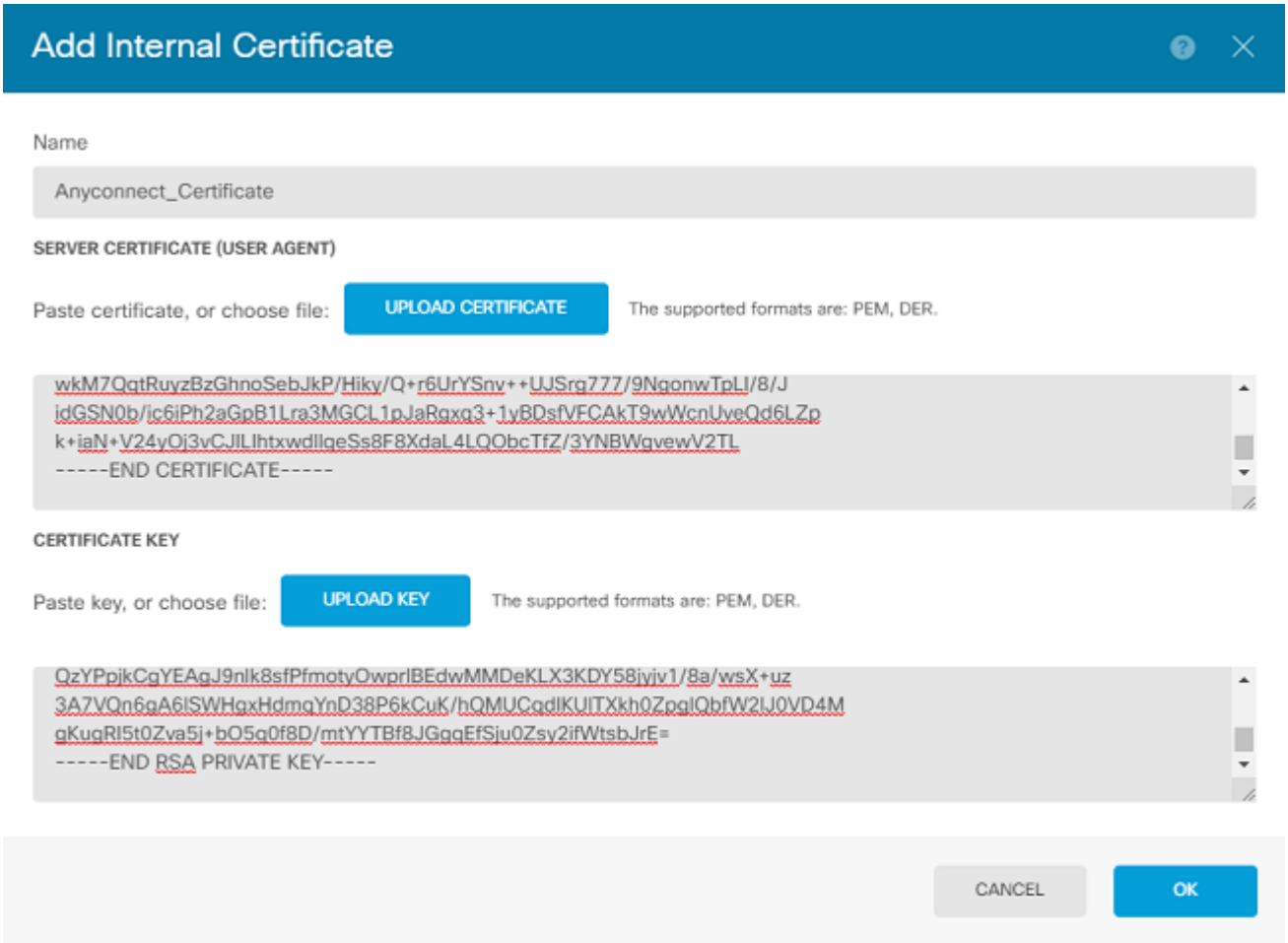
Naar navigeren Objects > Certificates > Add Internal Certificate. Configureer een certificaat zoals in de afbeelding:



Upload zowel het certificaat als de persoonlijke sleutel zoals in de afbeelding:

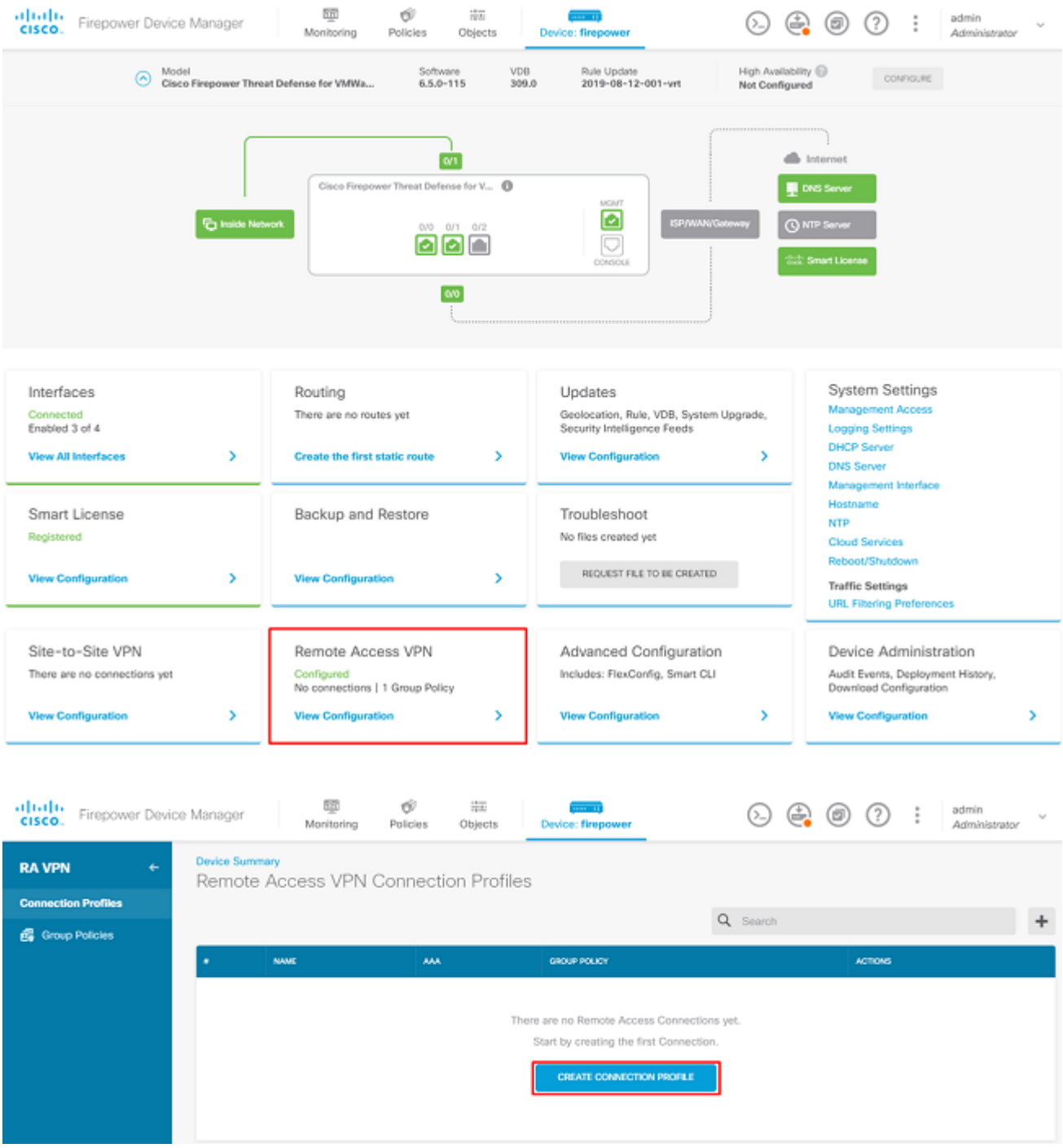


Het certificaat en de sleutel kunnen worden geüpload door kopiëren en plakken of de uploadknop voor elk bestand zoals in de afbeelding:

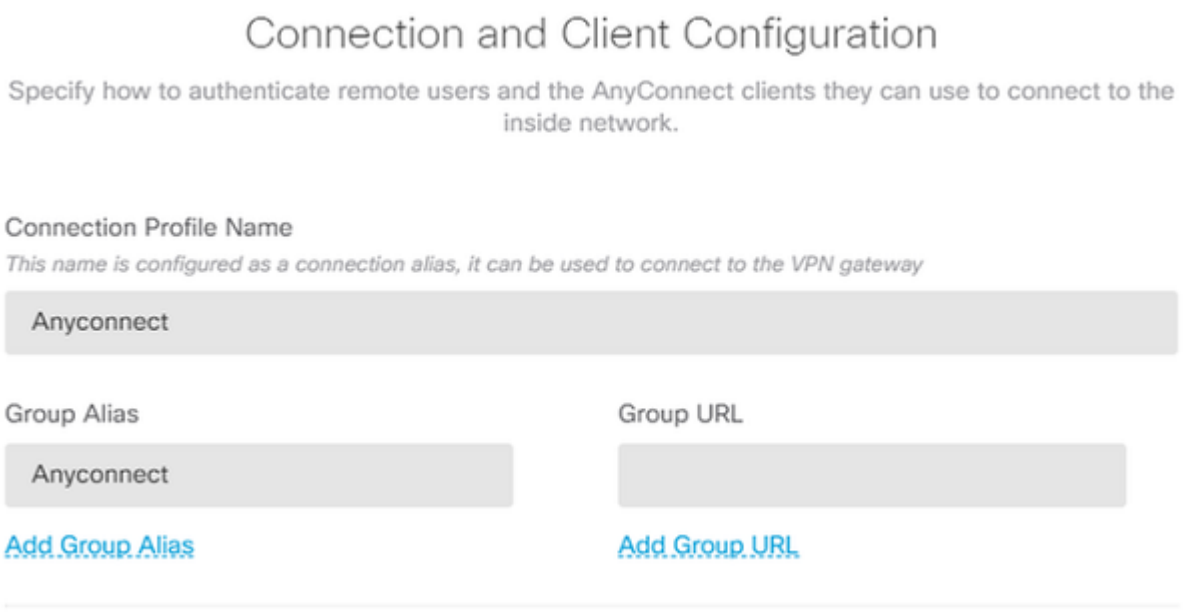


Remote Access VPN configureren

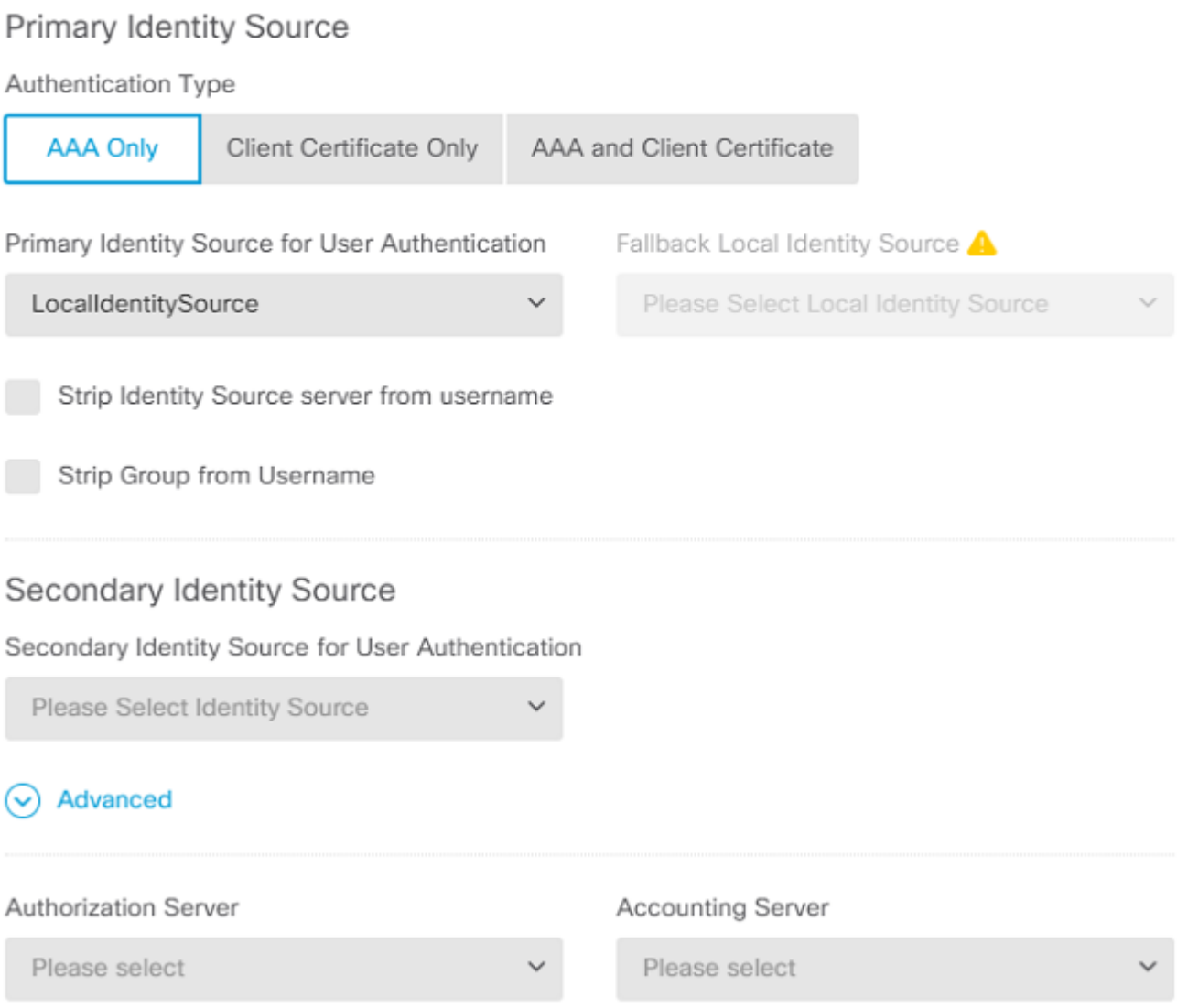
Naar navigeren Remote Access VPN > Create Connection Profile. Navigeer door de RA VPN Wizard op FDM zoals in de afbeelding:



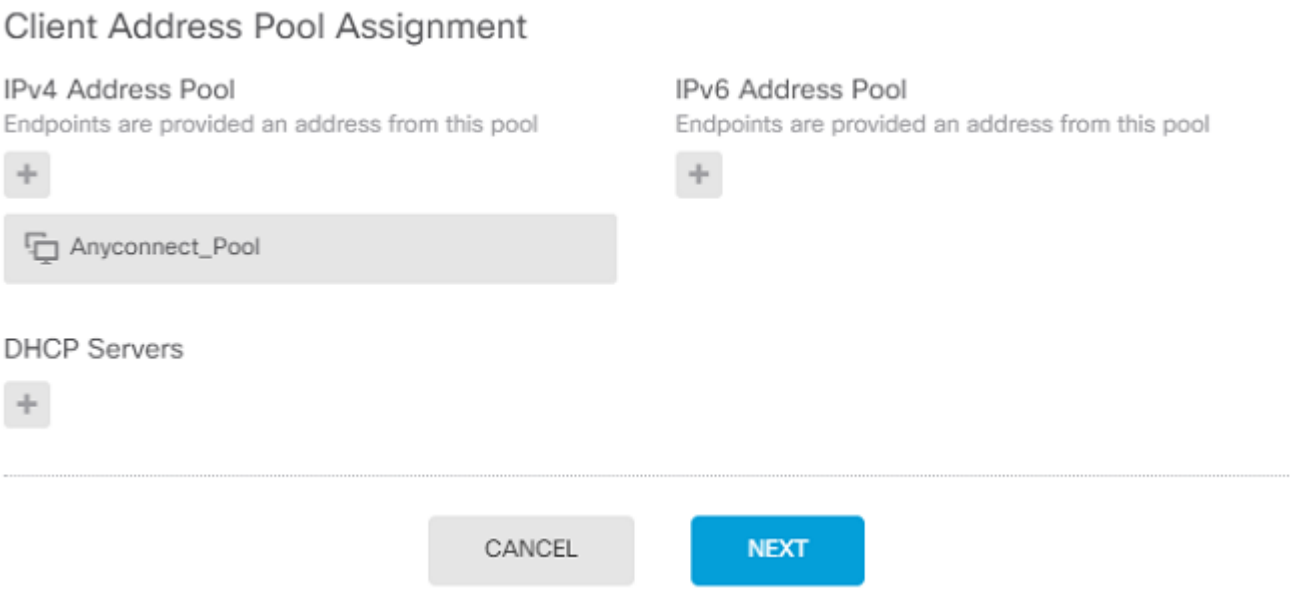
Maak een verbindingsprofiel en start de configuratie zoals in de afbeelding:



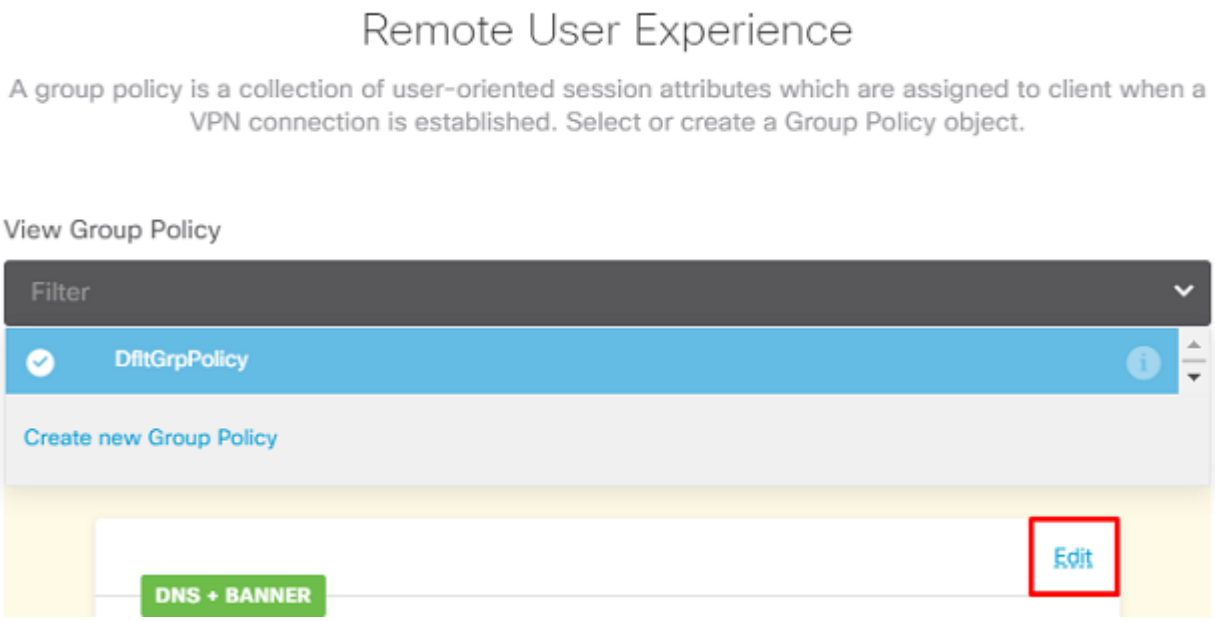
Kies de verificatiemethoden zoals in de afbeelding. Deze handleiding gebruikt lokale verificatie.



Kies de Anyconnect_Pool object zoals in de afbeelding:

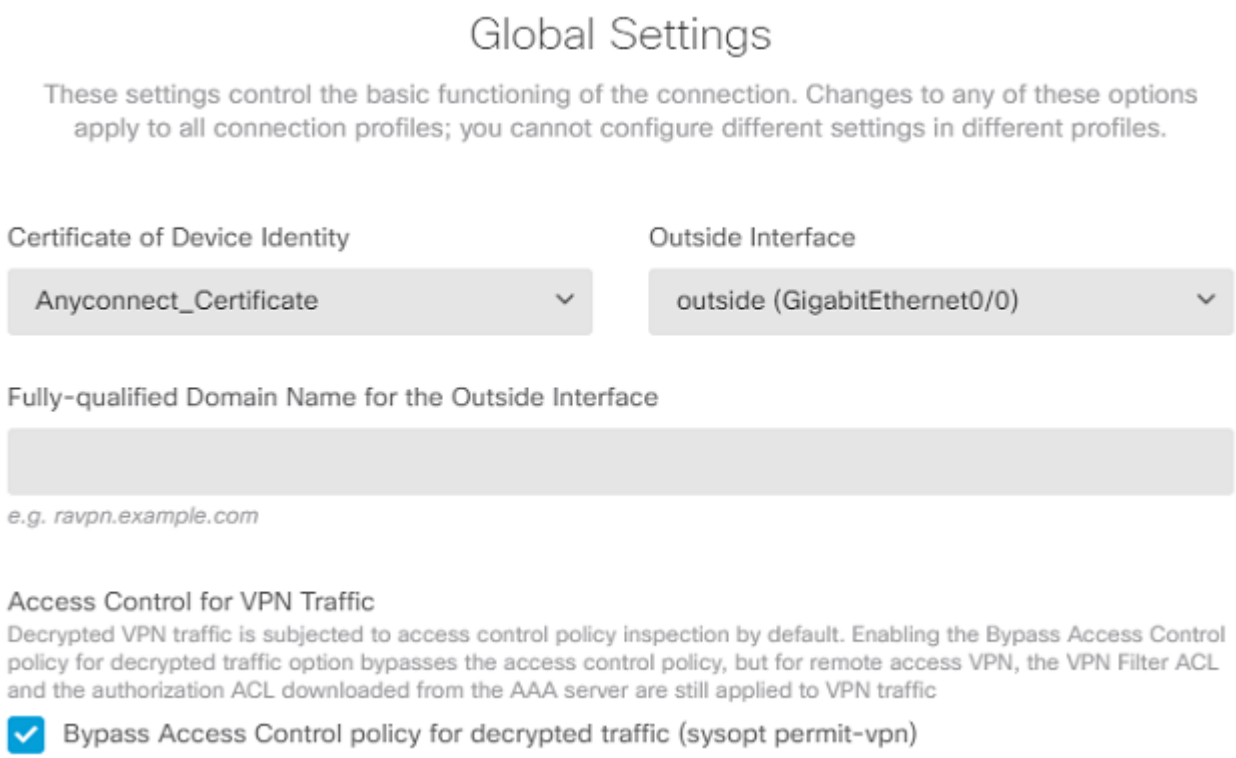


Op de volgende pagina wordt een samenvatting weergegeven van het standaard groepsbeleid. Er kan een nieuw groepsbeleid worden gemaakt wanneer u op de vervolgkeuzelijst klikt en de optie kiest om Create a new Group Policy. Voor deze handleiding wordt het standaard groepsbeleid gebruikt. Kies de bewerkingsoptie boven aan het beleid zoals in de afbeelding:

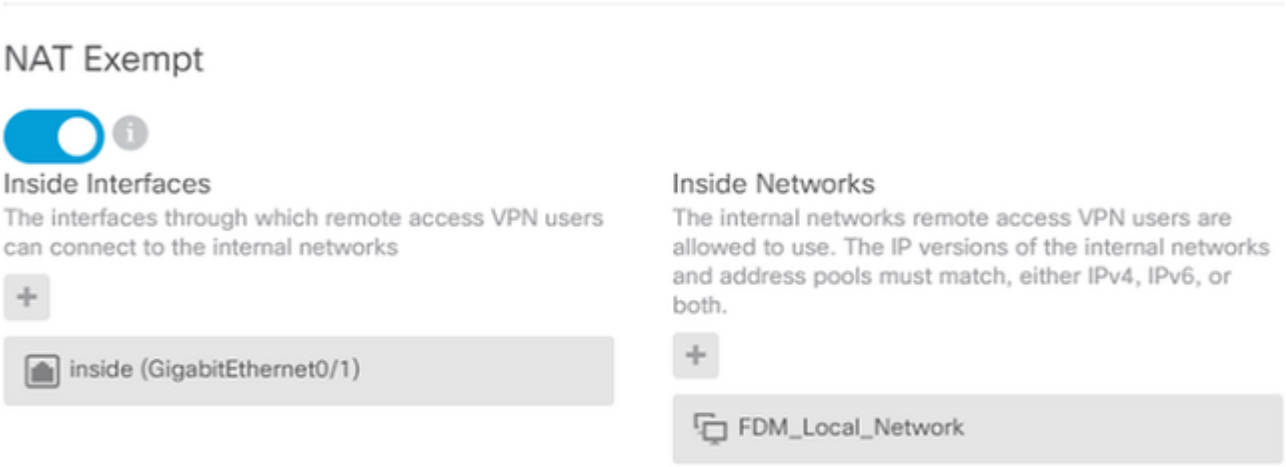


In het groepsbeleid voegt u Split-tunneling toe, zodat gebruikers die zijn verbonden met AnyConnect alleen verkeer verzenden dat is bestemd voor het interne FTD-netwerk via de AnyConnect-client terwijl al het andere verkeer uit de ISP-verbinding van de gebruiker verdwijnt zoals in de afbeelding:

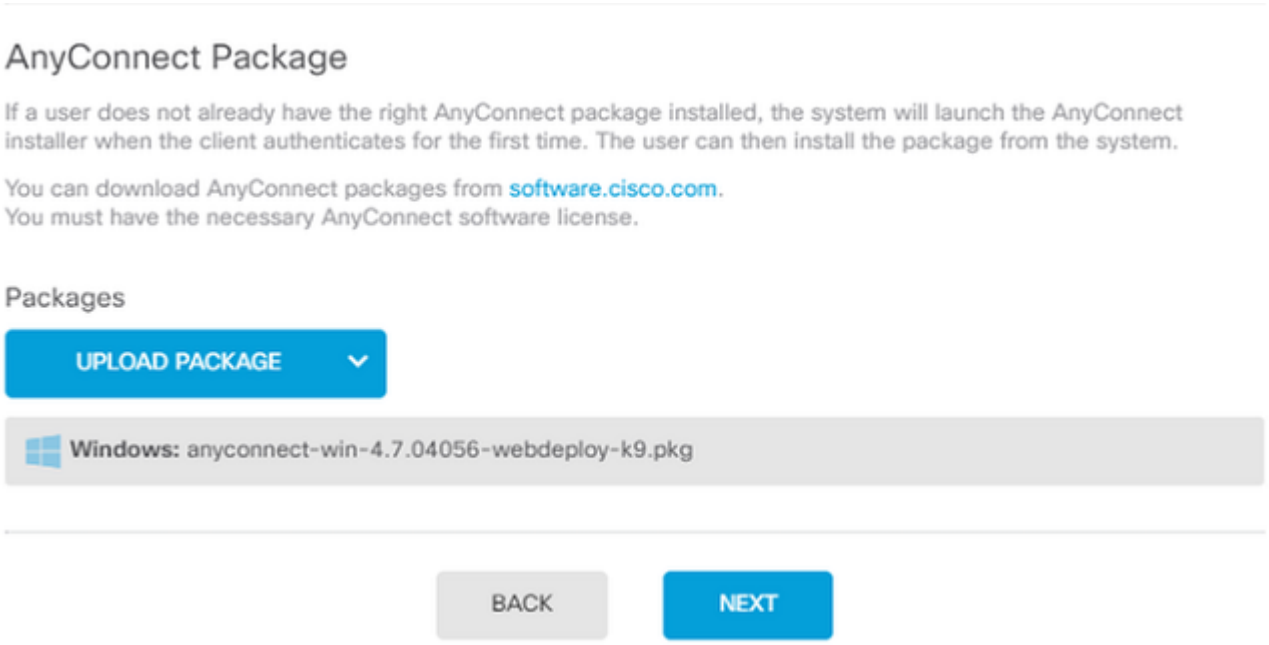
Kies op de volgende pagina de Anyconnect_Certificate toegevoegd in het certificaatgedeelte. Selecteer vervolgens de interface waarop de FTD naar AnyConnect-verbindingen luistert. Kies het beleid voor toegangscontrole omzeilen voor gedecrypteerd verkeer (sysopt permit-vpn). Dit is een optionele opdracht als de sysopt permit-vpn niet wordt gekozen. Er moet een toegangscontrolebeleid worden gemaakt waarmee verkeer van de AnyConnect-clients toegang kan krijgen tot het interne netwerk zoals in de afbeelding:



NAT-vrijstelling kan handmatig worden ingesteld onder Policies > NAT U kunt dit ook automatisch configureren door de wizard. Kies de binneninterface en de netwerken die AnyConnect-clients nodig hebben om toegang te krijgen zoals in de afbeelding.



Kies het AnyConnect-pakket voor elk besturingssysteem (Windows/Mac/Linux) waarmee gebruikers verbinding kunnen maken, zoals in de afbeelding wordt getoond.

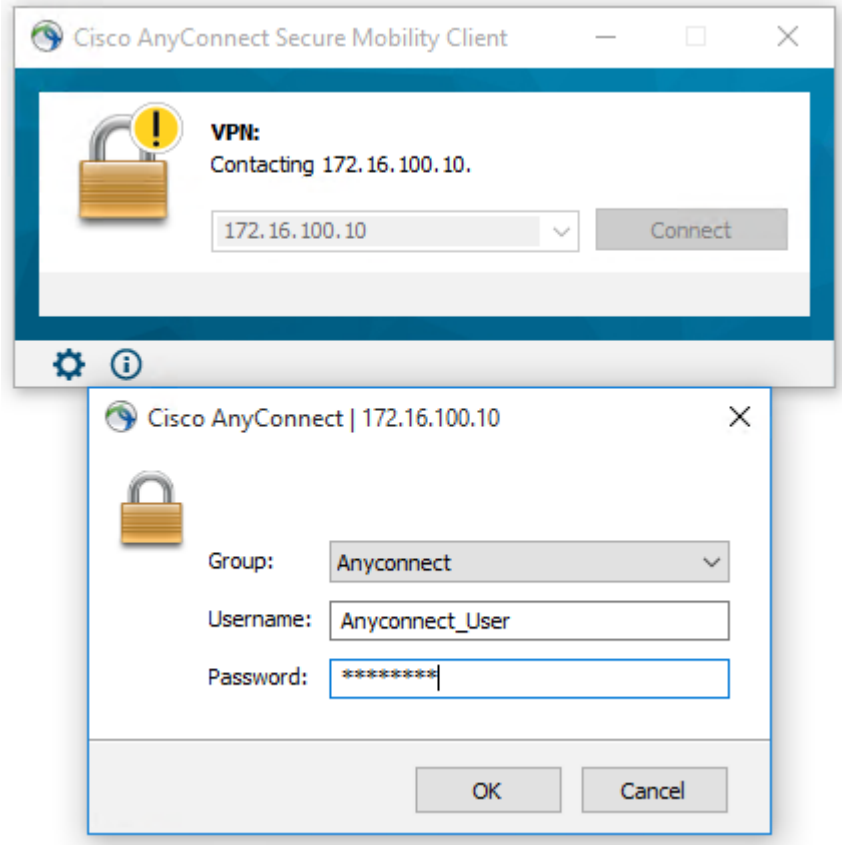


De laatste pagina geeft een samenvatting van de gehele configuratie. Bevestig dat de juiste parameters zijn ingesteld en druk op de knop Voltooien en stel de nieuwe configuratie in.

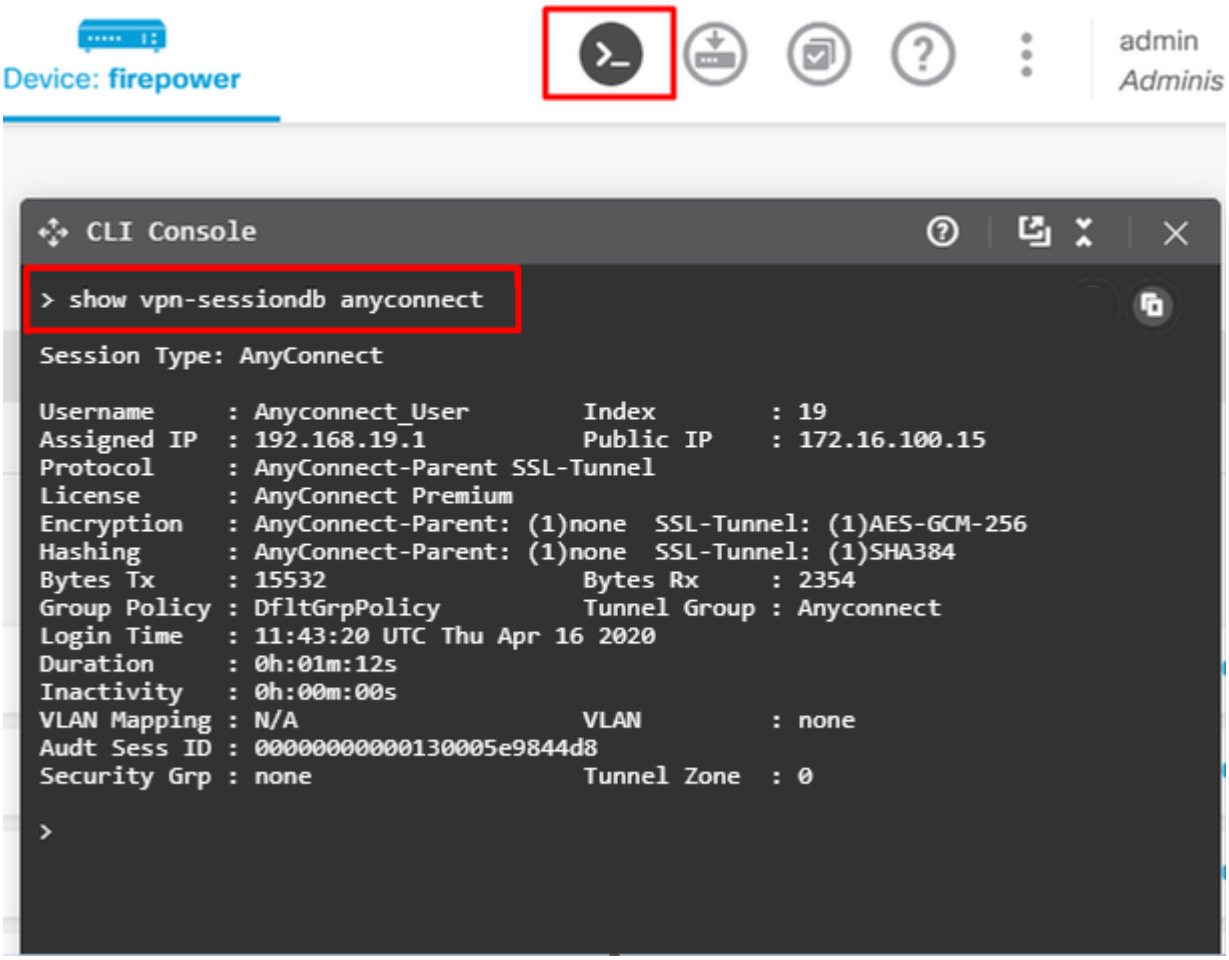
Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Probeer verbinding te maken zodra de configuratie is geïmplementeerd. Als u een FQDN hebt die zich in de buitenste IP van de FTD bevindt, voert u deze in het vak AnyConnect-verbinding in. In dit voorbeeld wordt het buitenste IP-adres van de FTD gebruikt. Gebruik de gebruikersnaam/het wachtwoord dat in de objectensectie van FDM is gemaakt zoals in de afbeelding.



Vanaf FDM 6.5.0 is er geen manier om de AnyConnect-gebruikers te monitoren via de FDM GUI. De enige optie is om de AnyConnect-gebruikers via CLI te bewaken. De CLI-console van de FDM GUI kan ook worden gebruikt om te controleren of gebruikers zijn verbonden. Gebruik deze opdracht, Show vpn-sessiondb anyconnect.



Het zelfde bevel kan direct van CLI worden in werking gesteld.

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : Anyconnect_User        Index        : 15
Assigned IP  : 192.168.19.1           Public IP    : 172.16.100.15
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384
Bytes Tx     : 38830                  Bytes Rx     : 172
Group Policy : DfltGrpPolicy          Tunnel Group : Anyconnect
Login Time   : 01:08:10 UTC Thu Apr 9 2020
Duration     : 0h:00m:53s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 000000000000f0005e8e757a
Security Grp : none                   Tunnel Zone  : 0
```

Problemen oplossen

Deze sectie verschaft de informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Als een gebruiker geen verbinding met het FTD met SSL kan maken, voert u deze stappen uit om de SSL-onderhandelingsproblemen te isoleren:

1. Controleer of het IP-adres buiten FTD door de computer van de gebruiker kan worden gepingeld.
2. Gebruik een extern snuifje om te verifiëren of de TCP-handdruk met drie richtingen succesvol is.

Problemen met AnyConnect-client

Deze paragraaf bevat richtlijnen voor het oplossen van de twee meest voorkomende problemen met AnyConnect VPN-clients. Een handleiding voor probleemoplossing voor de AnyConnect-client kunt u hier vinden: AnyConnect VPN-handleiding voor probleemoplossing voor clients.

Aanvankelijke connectiviteitsproblemen

Als een gebruiker eerste connectiviteitsproblemen heeft, schakel debug in webvpn AnyConnect op de FTD en analyse van de debug-berichten. Debugs moeten uitgevoerd worden op de CLI van de FTD. Gebruik de opdracht debug webvpn anyconnect 255.

Verzamel een DART bundel van de clientmachine om de logboeken van AnyConnect te krijgen. Hier vindt u instructies voor het verzamelen van een DART bundel: DART bundels verzamelen.

Verkeerspecifieke problemen

Als een verbinding succesvol is maar het verkeer via de SSL VPN-tunnel mislukt, bekijk dan de verkeersstatistieken op de client om te controleren of het verkeer door de client wordt ontvangen en verzonden. Gedetailleerde clientstatistieken zijn beschikbaar in alle versies van AnyConnect. Als de client aantoont dat verkeer wordt verzonden en ontvangen, controleert u het FTD op ontvangen en verzonden verkeer. Als de FTD een filter toepast, wordt de filternaam weergegeven en kunt u de ACL-vermeldingen bekijken om te controleren of uw verkeer wordt verbroken. Gemeenschappelijke verkeersproblemen die gebruikers ervaren zijn:

- Problemen met routing achter de FTD - het interne netwerk kan geen pakketten terugsturen naar de toegewezen IP-adressen en VPN-clients
- Toegangscontrolelijsten die verkeer blokkeren
- Netwerkadresomzetting wordt niet overgeslagen voor VPN-verkeer

Voor meer informatie over externe toegang VPNâ€™s op de FTD beheerd door FDM, vind hier de volledige configuratiehandleiding: Remote Access FTD beheerd door FDM.

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.