AnyConnect VPN-client op FTD configureren: haarspeld en NAT-vrijstelling

Inhoud

Inleiding

In dit document wordt beschreven hoe u de Cisco Remote Access VPN-oplossing (AnyConnect) kunt configureren op Firepower Threat Defence (FTD), v6.3, beheerd door FMC.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basis externe toegang VPN, Secure Sockets Layer (SSL) en Internet Key Exchange versie 2 (IKEv2) kennis
- Basisverificatie, autorisatie en accounting (AAA) en RADIUS-kennis
- Basiskennis van het VCC
- Basiskennis van FTD

Gebruikte componenten

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

- Cisco VCC 6.4
- Cisco FTD 6.3
- AnyConnect 4.7

Dit document beschrijft de procedure voor het configureren van Cisco Remote Access VPN-oplossing (AnyConnect) op Firepower Threat Defence (FTD), versie 6.3, beheerd door Firepower Management Center (FMC).

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

Dit document is bedoeld voor de configuratie op FTD-apparaten. Als u naar het ASA-configuratievoorbeeld zoekt, raadpleegt u het document: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/100918-asa-sslvpn-00.html

Beperkingen:

Op dit moment worden deze functies niet ondersteund door FTD, maar nog wel door ASA-apparaten:

- Dubbele AAA-verificatie (beschikbaar op FTD versie 6.5)
- Dynamisch toegangsbeleid
- Hostscan
- ISE-houding
- RADIUS-CoA
- VPN-taakverdeling
- Lokale verificatie (beschikbaar op Firepower Device Manager 6.3). Cisco bug-id (CSCvf92680)
- LDAP-kenmerkkaart (beschikbaar via FlexConfig, Cisco-bug-id CSC64585)
- Aangepaste AnyConnect
- AnyConnect-scripts
- AnyConnect-lokalisatie
- VPN-services per app
- SCEP-proxy
- WSA-integratie
- SAML SSO (Cisco bug-id CSCvq90789)
- Gelijktijdige IKEv2 dynamische cryptokaart voor RNA en L2L VPN
- AnyConnect-modules (NAM, Hostscan, AMP Enabler, SBL, Umbrella, webbeveiliging, enzovoort). DART is de enige module die standaard op deze versie is geïnstalleerd.
- TACACS, Kerberos (KCD-verificatie en RSA/SDI)
- Browser Proxy

Configureren

Om door de wizard Externe toegang VPN in het VCC te kunnen lopen, moeten de volgende stappen worden voltooid:

Stap 1. Een SSL-certificaat importeren

Certificaten zijn essentieel wanneer u AnyConnect configureert. Alleen op RSA gebaseerde certificaten worden ondersteund voor SSL en IPSec.

Elliptic Curve Digital Signature Algorithm (ECDSA)-certificaten worden ondersteund in IPSec, maar het is niet mogelijk om een nieuw AnyConnect-pakket of XML-profiel te implementeren wanneer op ECDSA gebaseerd certificaat wordt gebruikt.

Het kan worden gebruikt voor IPSec, maar u moet de AnyConnect-pakketten samen met het XML-profiel vooraf implementeren, alle XML-profielupdates moeten handmatig worden uitgevoerd op elke client (Cisco bug-id CSCtx42595).

Daarnaast moet het certificaat een Common Name (CN)-extensie met DNS-naam en/of IP-adres bevatten

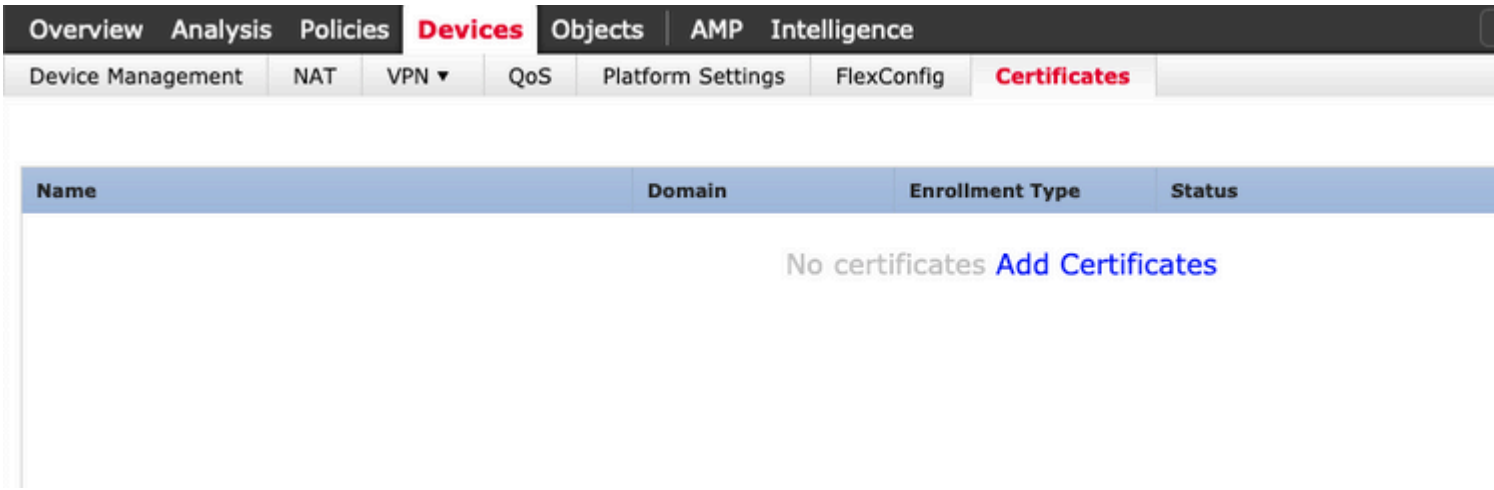
om fouten in het "Onbetrouwbare servercertificaat" in webbrowsers te voorkomen.

Opmerking: op FTD-apparatuur is het certificaat van de certificeringsinstantie (CA) vereist voordat het verzoek tot ondertekening van het certificaat (CSR) wordt gegenereerd.

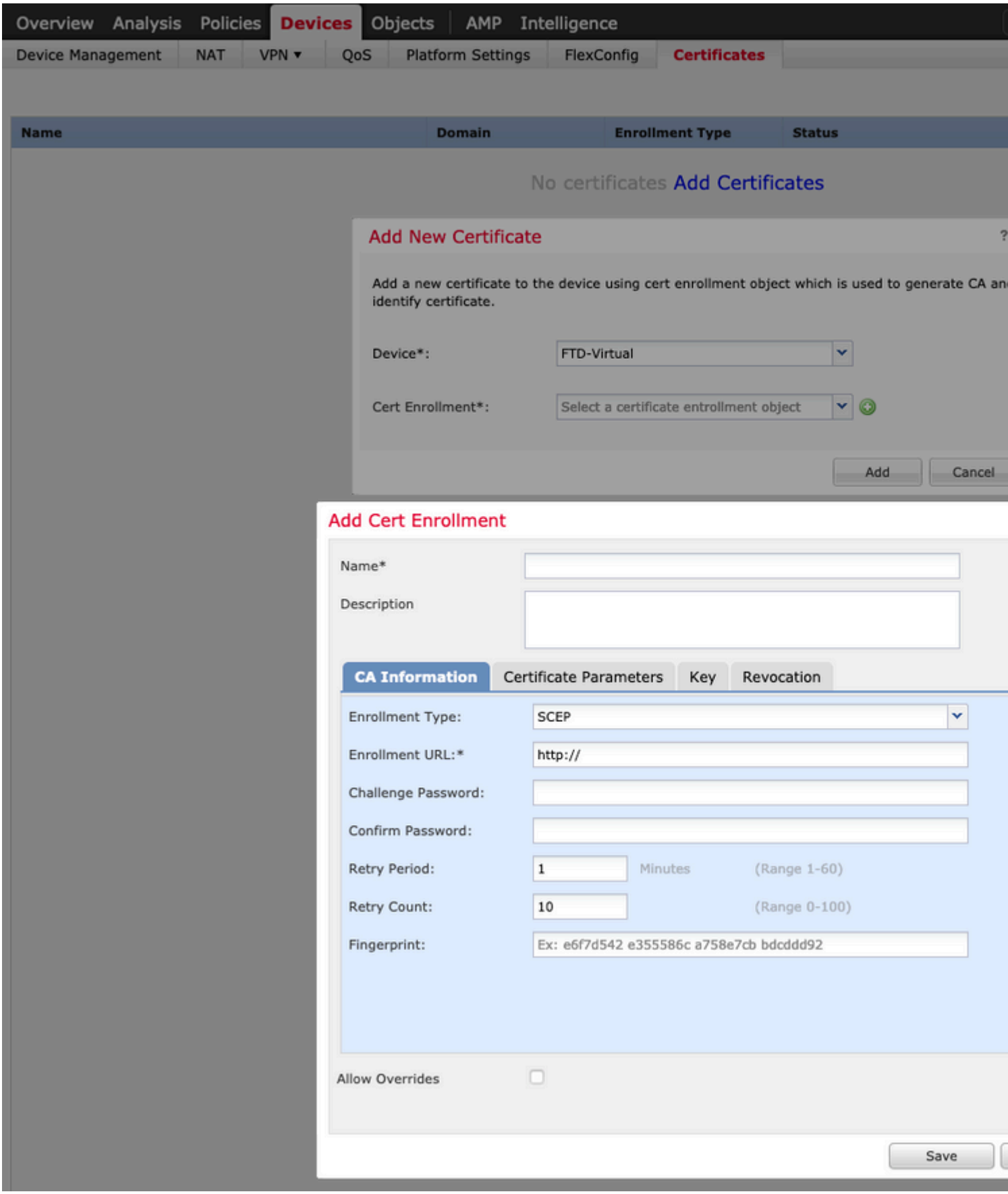
- Als de CSR wordt gegenereerd in een externe server (zoals Windows Server of OpenSSL), is de **handmatige inschrijvingsmethode** bedoeld om te mislukken, omdat FTD handmatige toeteninschrijving niet ondersteunt.
- Er moet een andere methode worden gebruikt, zoals PKCS12.

Om een certificaat voor het FTD-apparaat te verkrijgen met de handmatige inschrijvingsmethode, moet een CSR worden gegenereerd, ondertekend met een CA en vervolgens het identiteitscertificaat importeren.

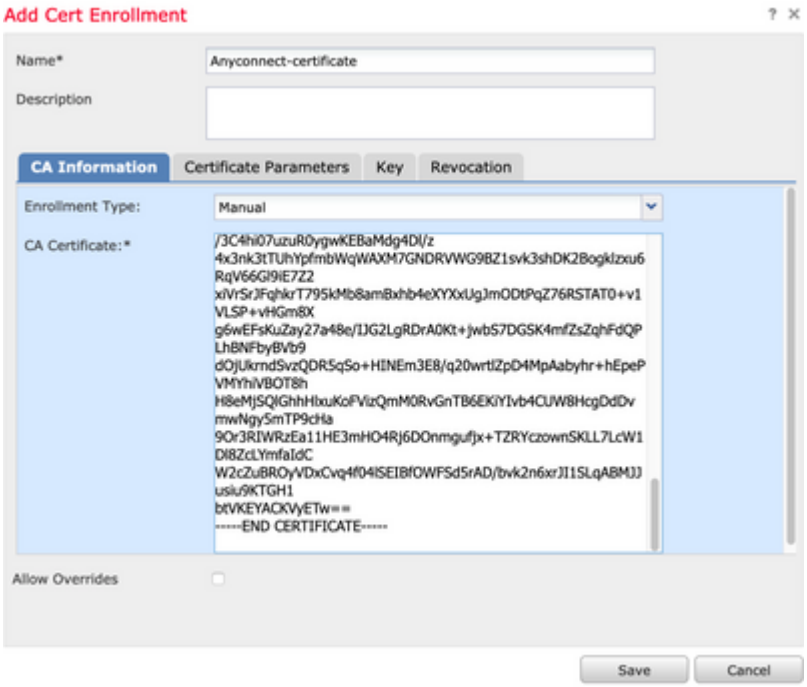
1. Navigeren naar **Apparaten > Certificaten** en selecteer **Toevoegen** zoals in de afbeelding.



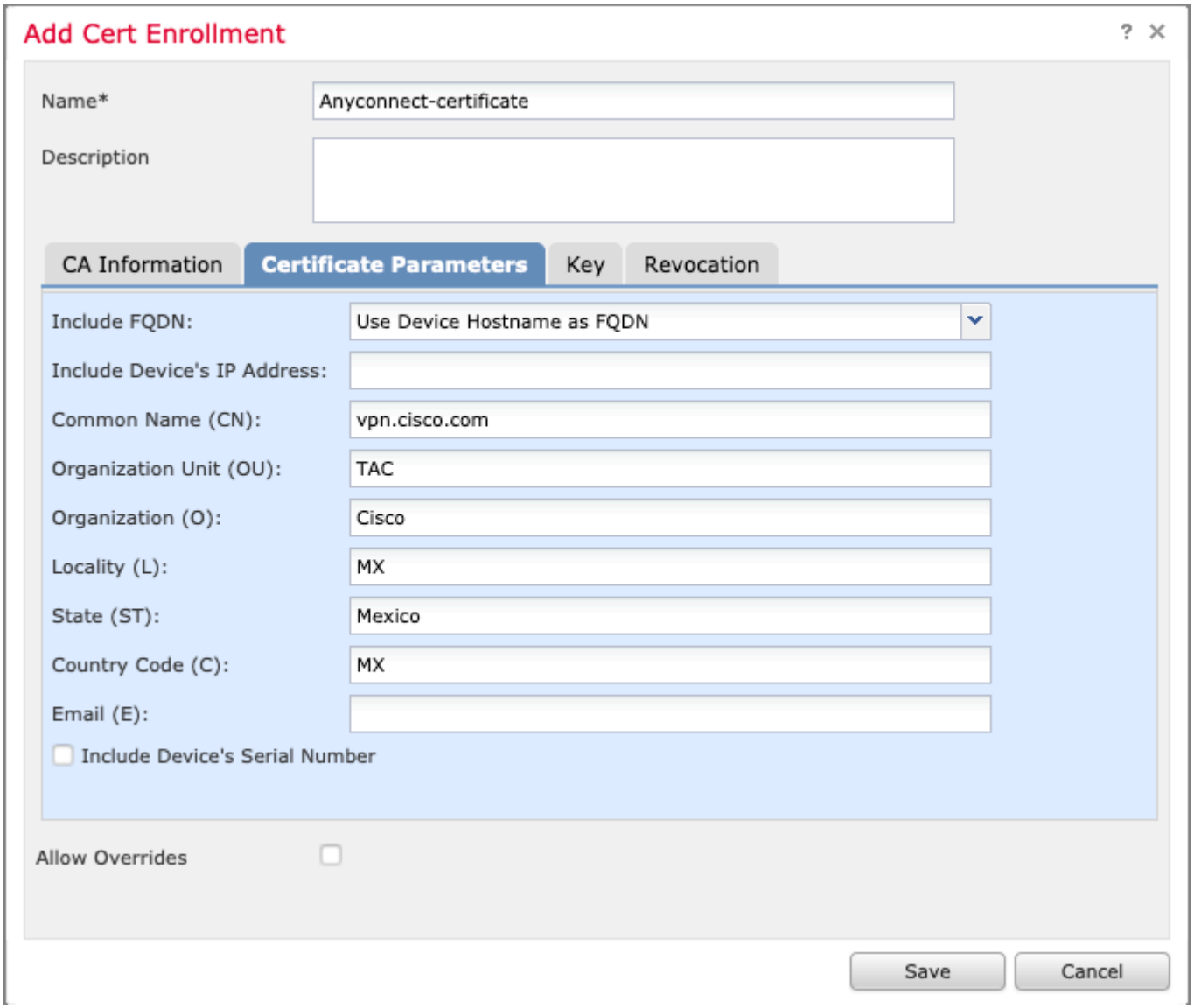
2. Selecteer het **apparaat** en voeg een nieuw object **Cert Enrollment toe** zoals in de afbeelding.



3. Selecteer handmatig **Inschrijftype** en plak het CA-certificaat (het certificaat dat bedoeld is om de CSR te ondertekenen).

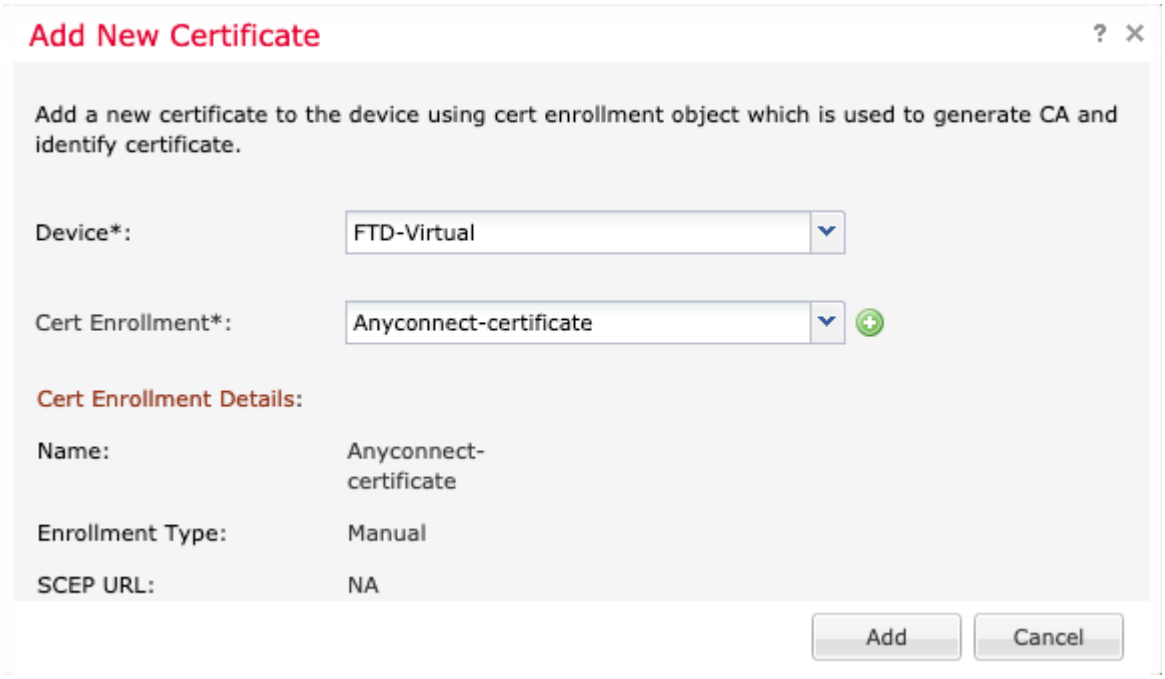


4. Selecteer het tabblad **Certificaatparameters** en selecteer "Aangepaste FQDN" voor het veld **Inclusief FQDN** en vul de certificaatgegevens in zoals in de afbeelding.

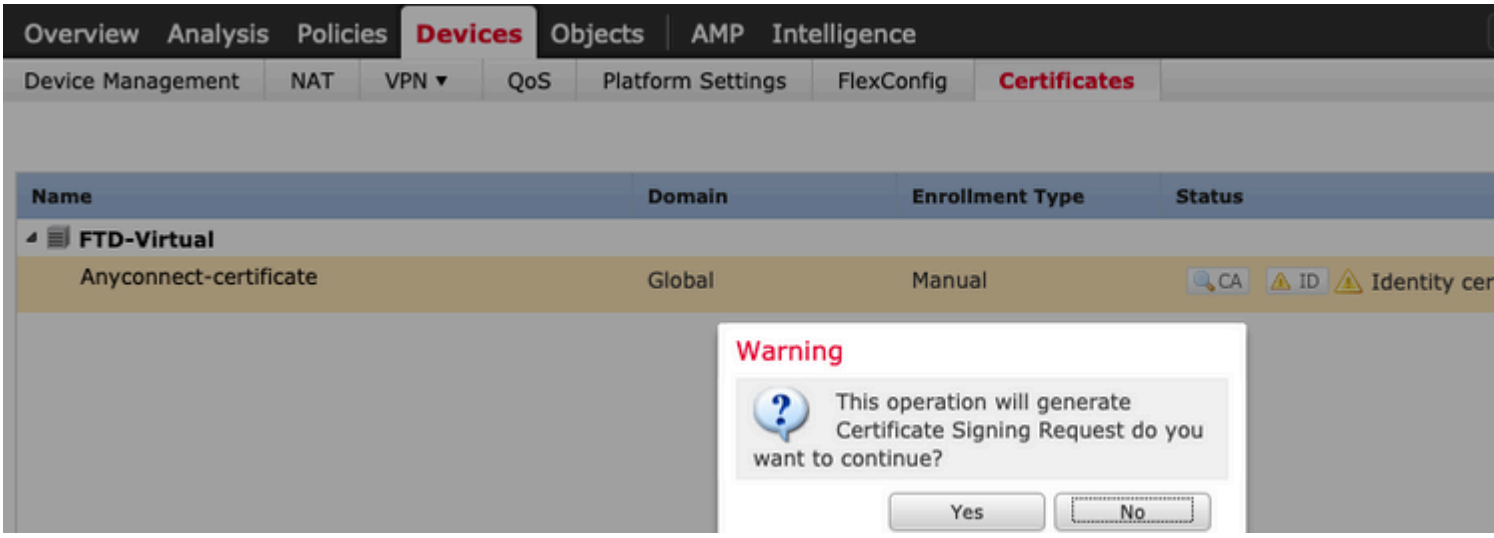


5. Selecteer het tabblad **Sleutel** en selecteer het type toets. U kunt naam en grootte kiezen. Voor RSA is 2048 bytes een minimumvereiste.

6. Selecteer Opslaan, bevestig het **apparaat** en selecteer onder **Volledige inschrijving** het trustpoint dat zojuist is gemaakt, selecteer **Toevoegen** om het certificaat te implementeren.

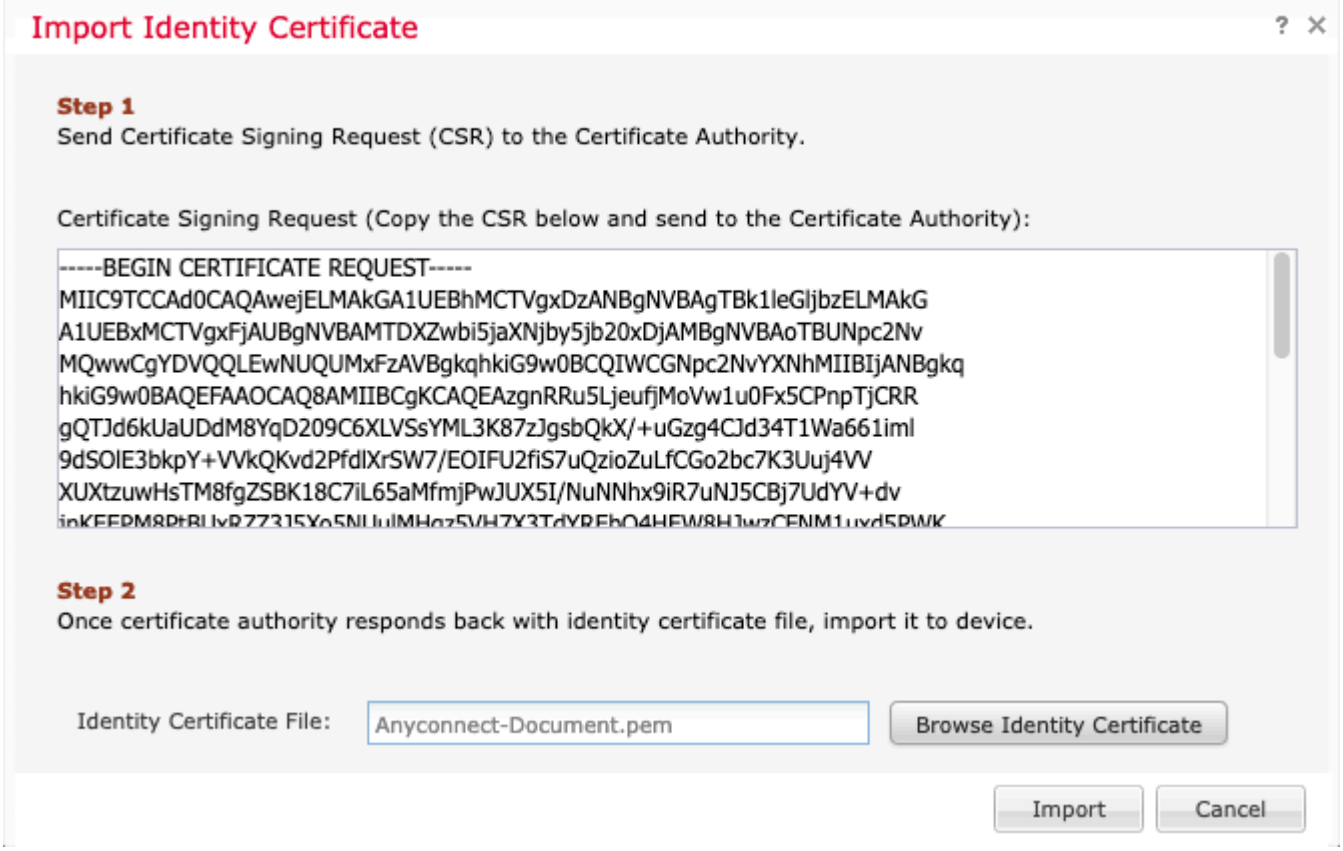


7. Selecteer in de kolom **Status** het **ID**-pictogram en selecteer **Ja** om de MVO te genereren zoals in de afbeelding.

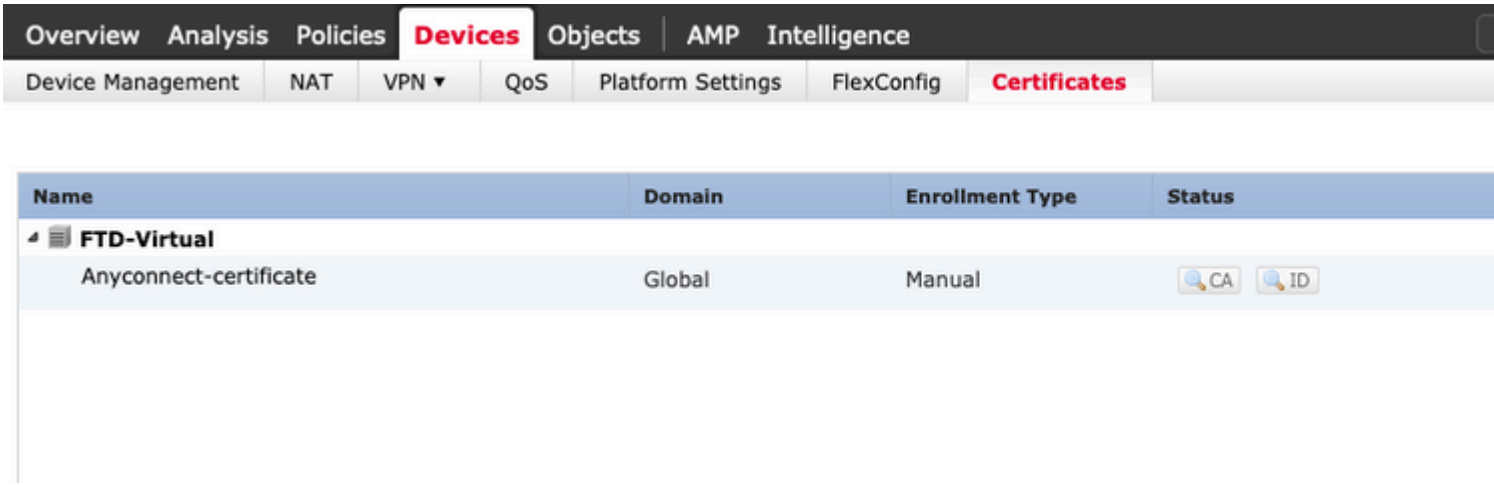


8. Kopieer CSR en onderteken het met uw gewenste CA (bijvoorbeeld GoDaddy of DigiCert).

9. Zodra het identiteitscertificaat van de CA (die in het base64-formaat moet zijn) is ontvangen, selecteert u **Identiteitscertificaat doorbladeren** en plaatst u het certificaat in de lokale computer. Selecteer **Importeren.**



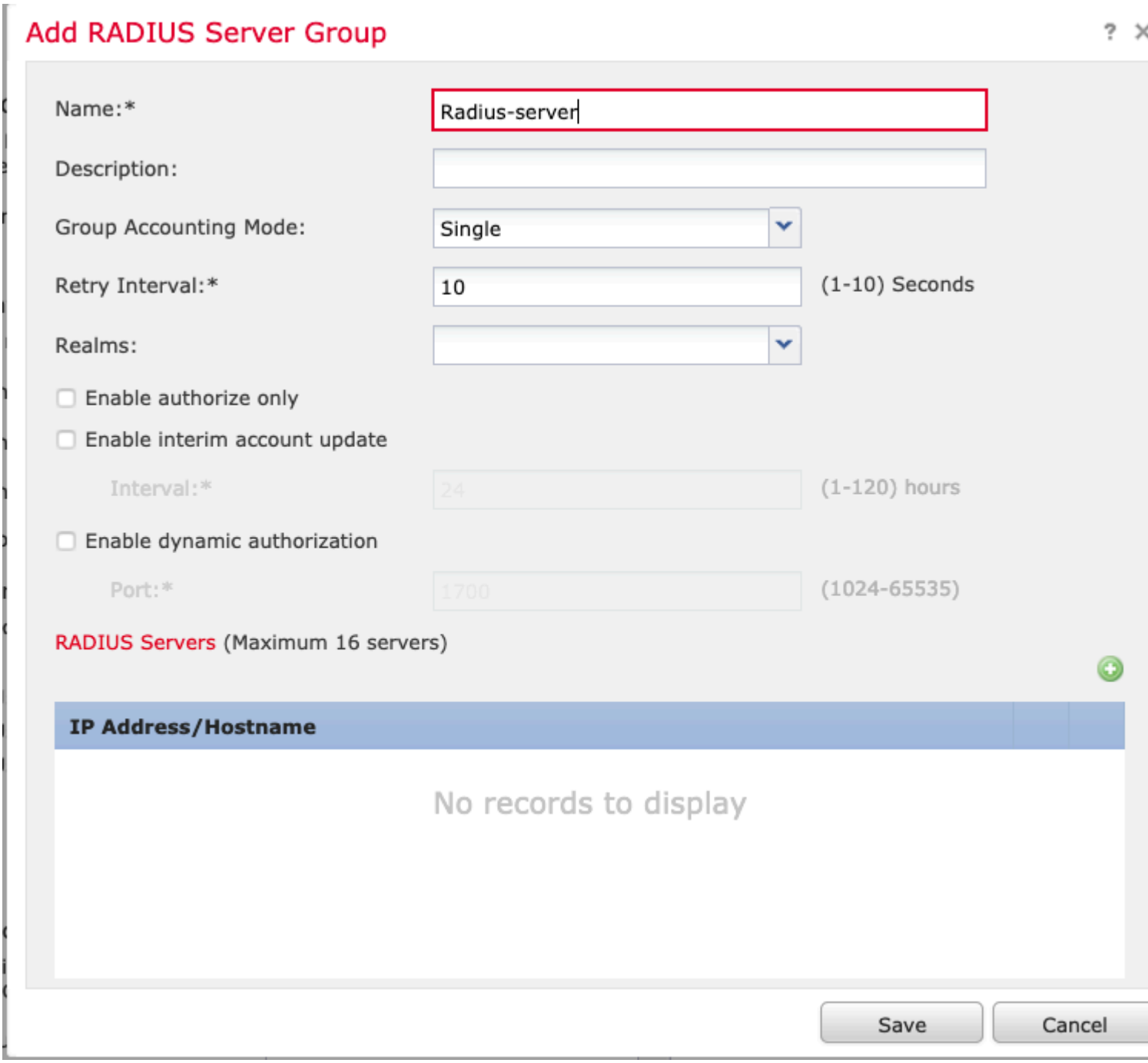
10. Na invoer kunnen zowel CA- als ID-certificaatgegevens worden weergegeven.



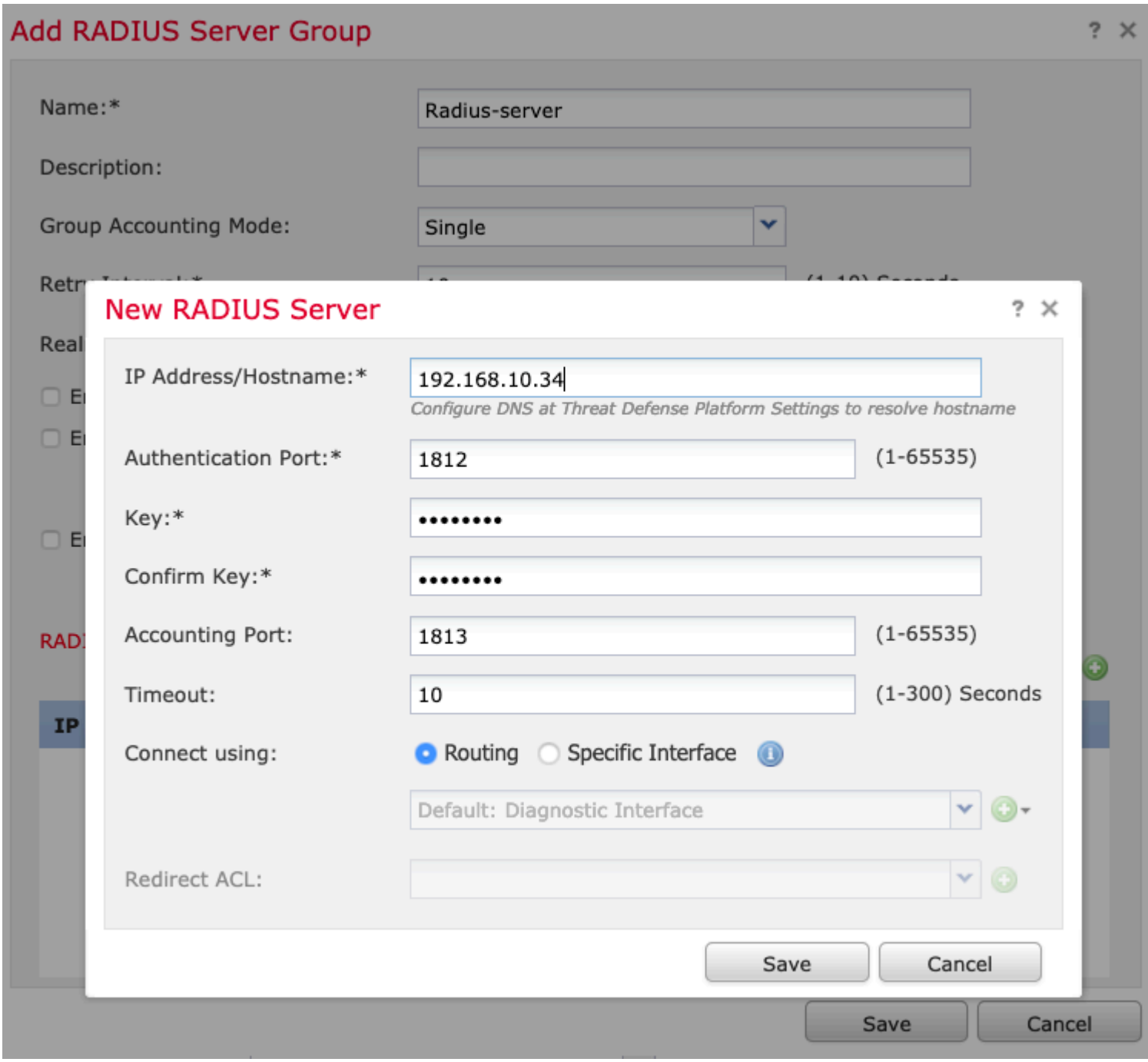
Stap 2. Een RADIUS-server configureren

Op door het VCC beheerde FTD-apparaten wordt de lokale gebruikersdatabase niet ondersteund. Er moet een andere verificatiemethode worden gebruikt, zoals RADIUS of LDAP.

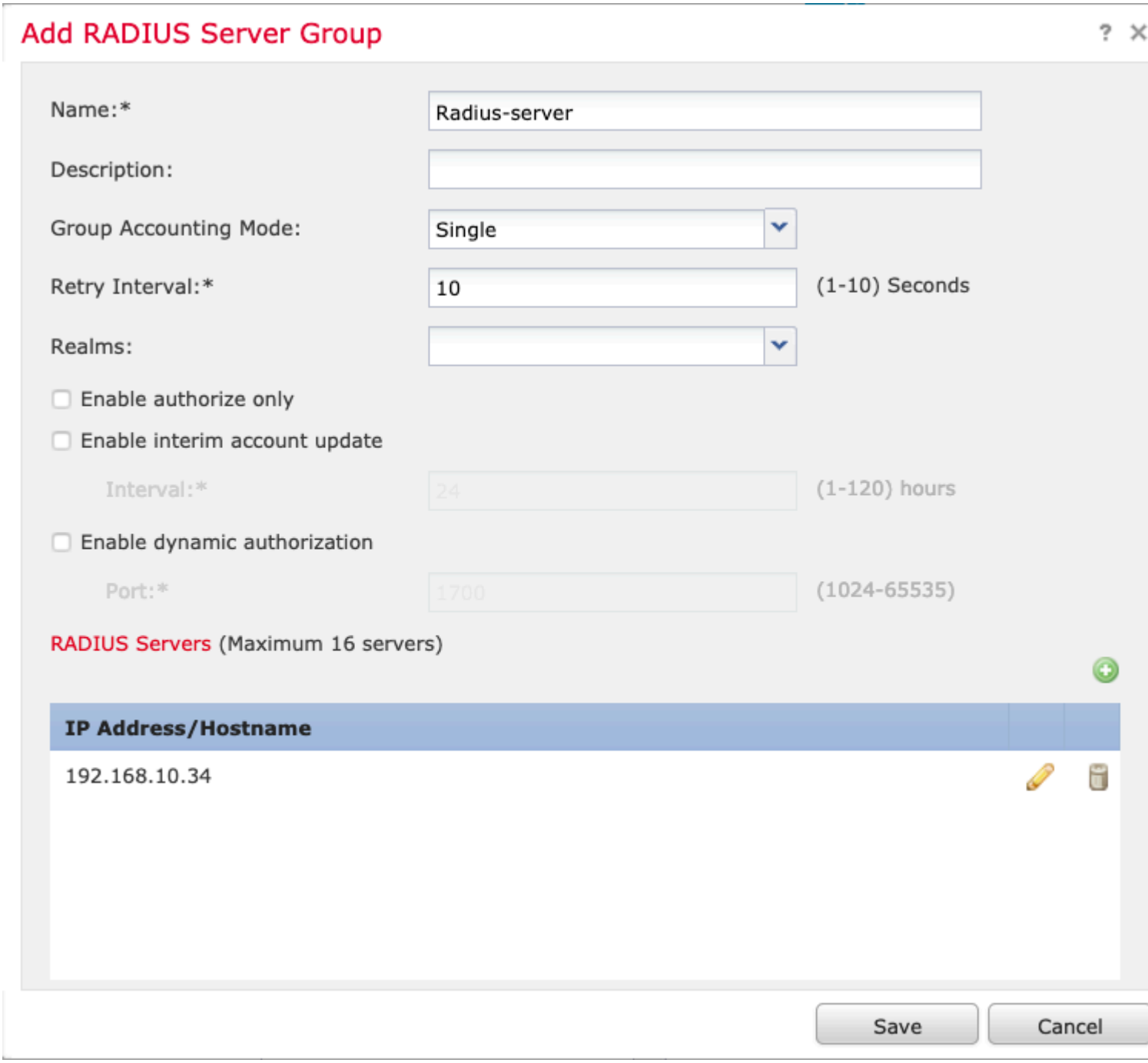
1. Navigeer naar **objecten** > **Objectbeheer** > **RADIUS-servergroep** > **RADIUS-servergroep toevoegen** zoals in de afbeelding wordt weergegeven.



2. Wijs een naam toe aan de **Radius Server Group** en voeg het IP-adres van de Radius-server toe, samen met een gedeeld geheim (het gedeelde geheim is vereist om het FTD te koppelen met de Radius-server). Selecteer **Opslaan** zodra dit formulier is ingevuld zoals in de afbeelding.



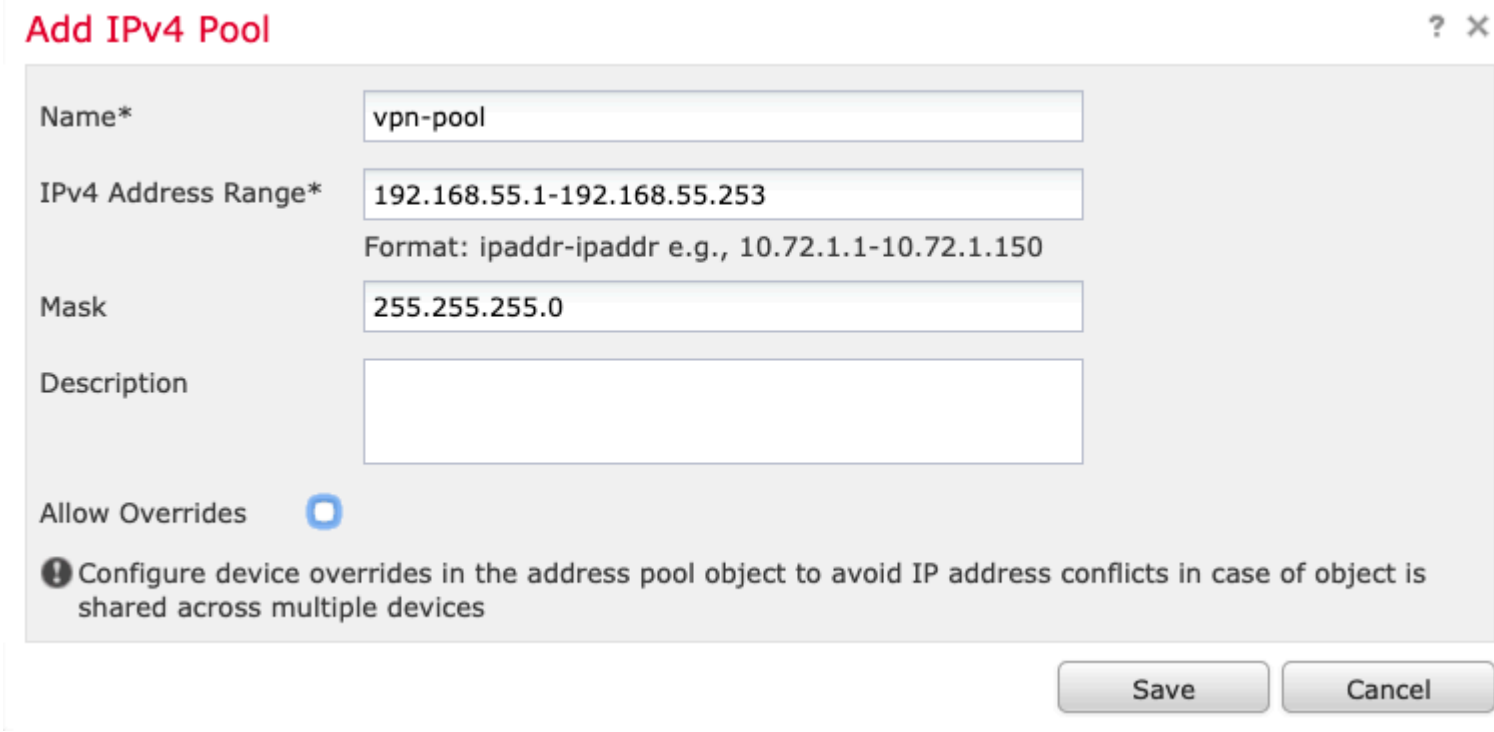
3. De RADIUS-serverinformatie is nu beschikbaar in de lijst Radius Server zoals in de afbeelding.



Stap 3. Een IP-groep maken

1. Navigeer naar **objecten** > **Objectbeheer** > **Adrespools** > **IPv4-pools toevoegen**.

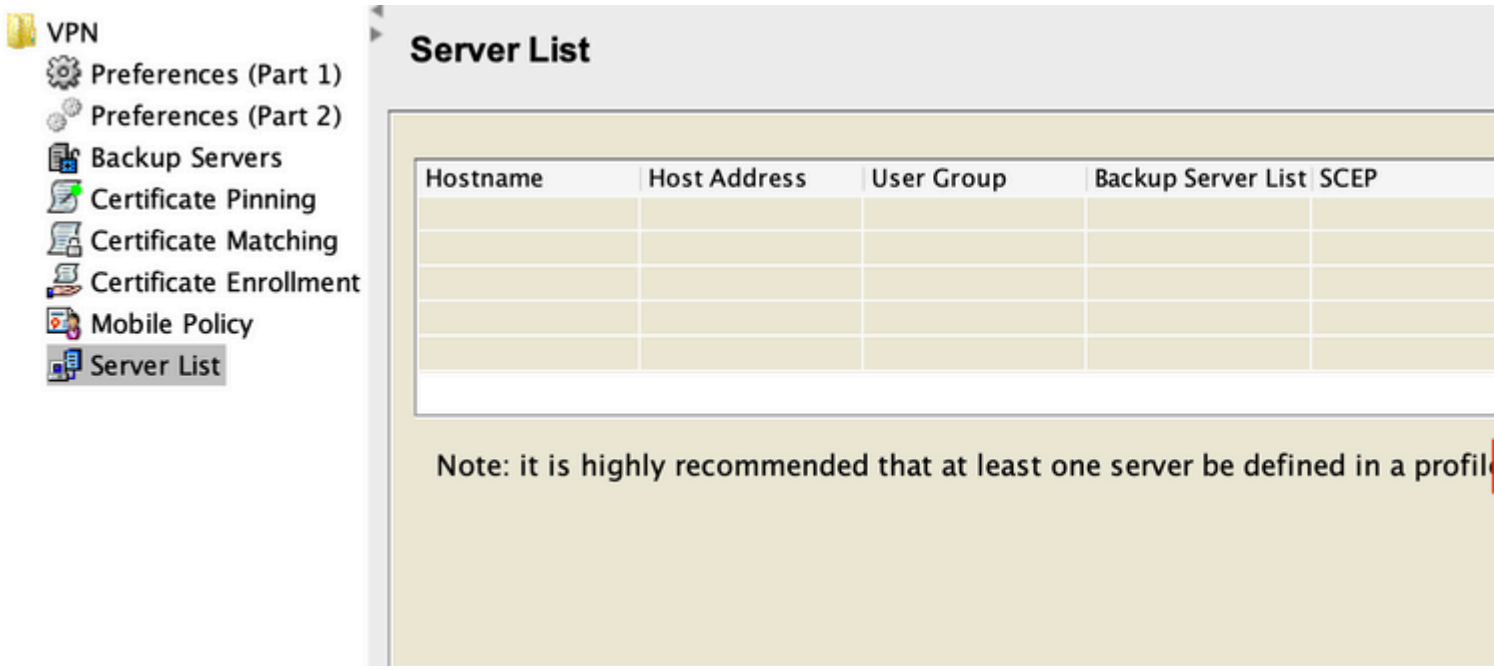
2. Wijs de naam en het bereik van IP-adressen toe. Het veld **Masker** is niet vereist, maar kan worden gespecificeerd zoals in de afbeelding.



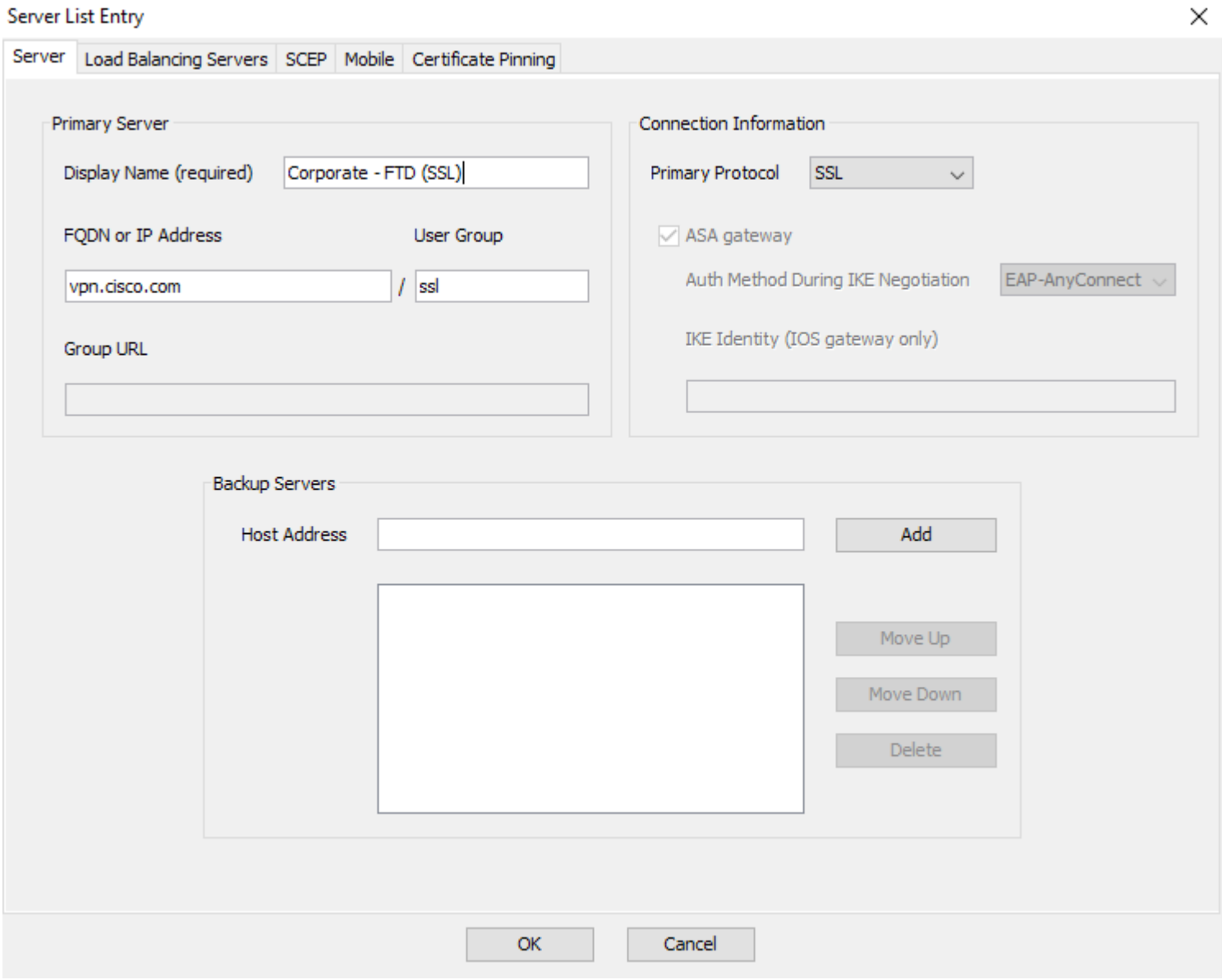
Stap 4. Een XML-profiel maken

1. Download de **Profile Editor** tool van Cisco.com en voer de applicatie uit.

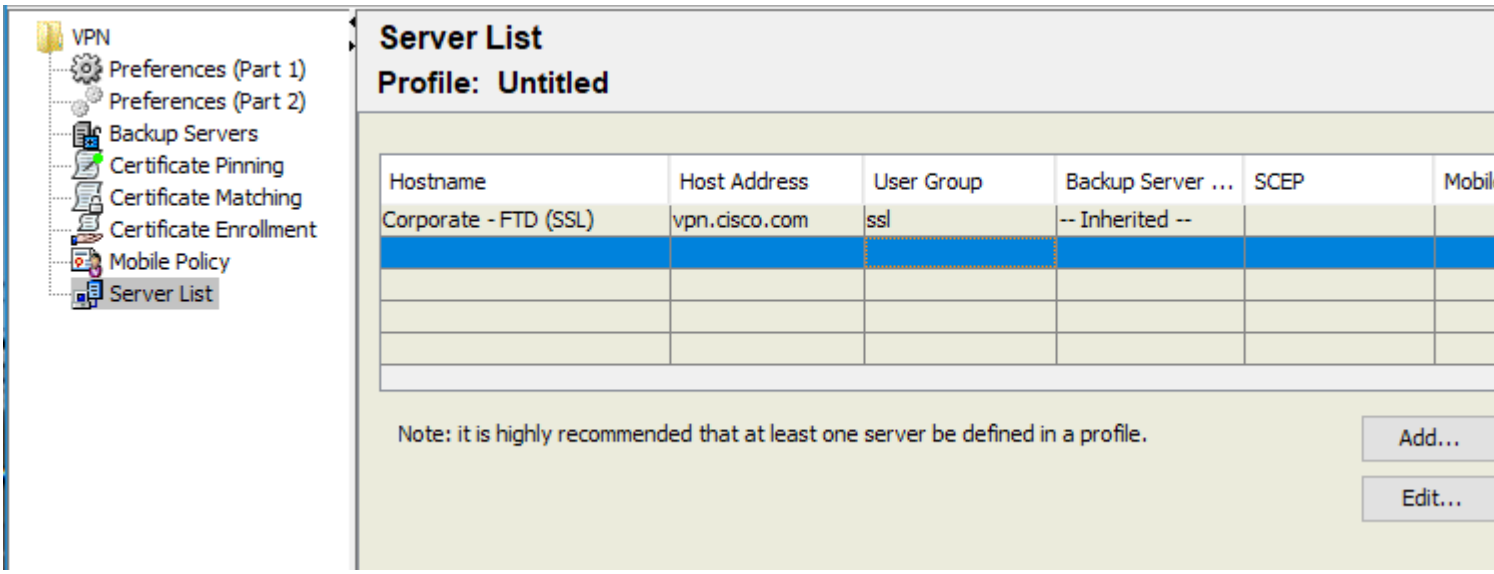
2. Navigeer in de toepassing Profile Editor naar **Server List** en selecteer **Add** zoals in de afbeelding.



3. Wijs een **weergavenaam, volledig gekwalificeerde domeinnaam (FQDN) of IP-adres toe** en selecteer **OK** zoals in de afbeelding.



4. De ingang is nu zichtbaar in het menu **Serverlijst**:



5. Navigeren naar **Bestand** > **Opslaan als.**

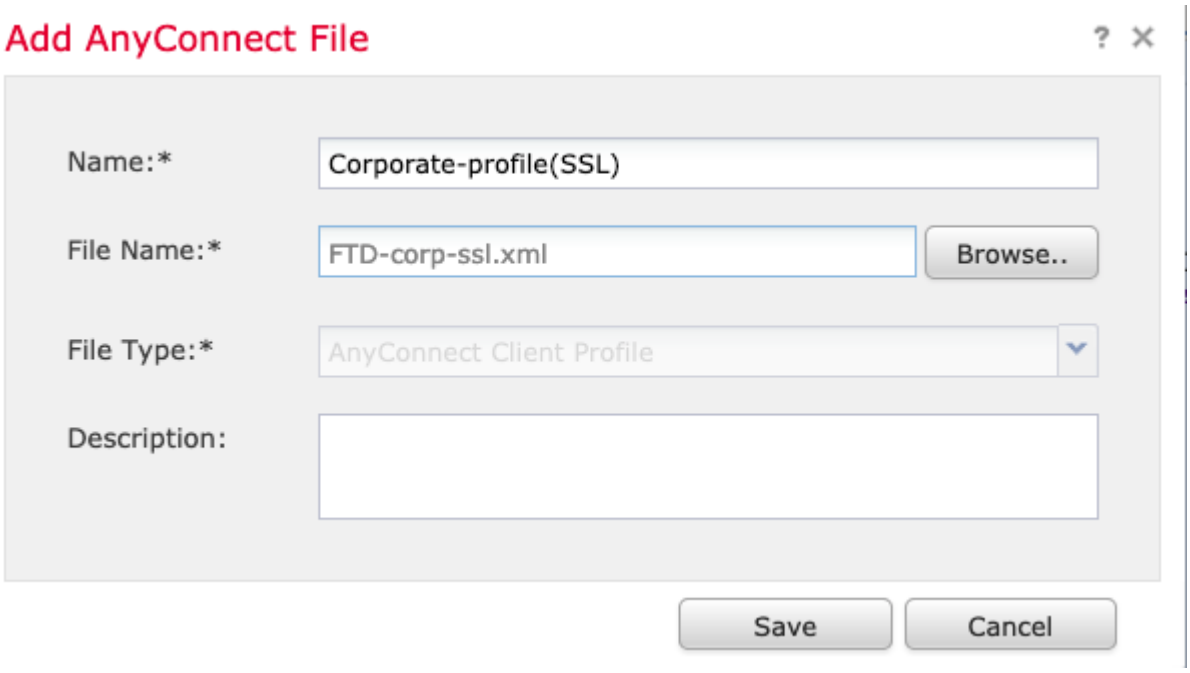
Opmerking: Sla het profiel op met een gemakkelijk herkenbare naam met de extensie **.xml**.

Stap 5. AnyConnect XML-profiel uploaden

1. Ga in het VCC naar Objecten > **Objectbeheer** > **VPN** > **AnyConnect File** > **Add AnyConnect File**.

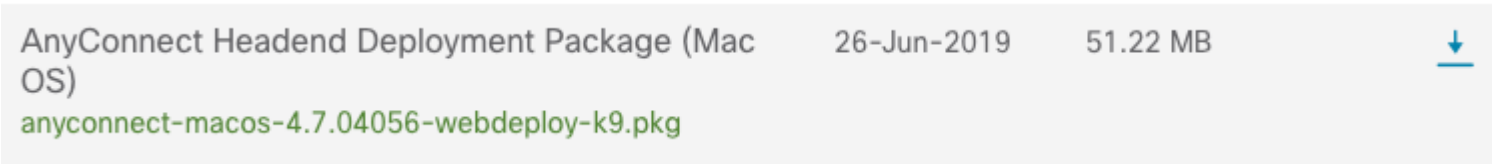
2. Wijs een **naam** aan het object toe en klik op **Bladeren,** zoek het clientprofiel in uw lokale systeem en selecteer **Opslaan**.

Waarschuwing: Zorg ervoor dat u het **AnyConnect-clientprofiel** selecteert als het bestandstype.



Stap 6. AnyConnect-afbeeldingen uploaden

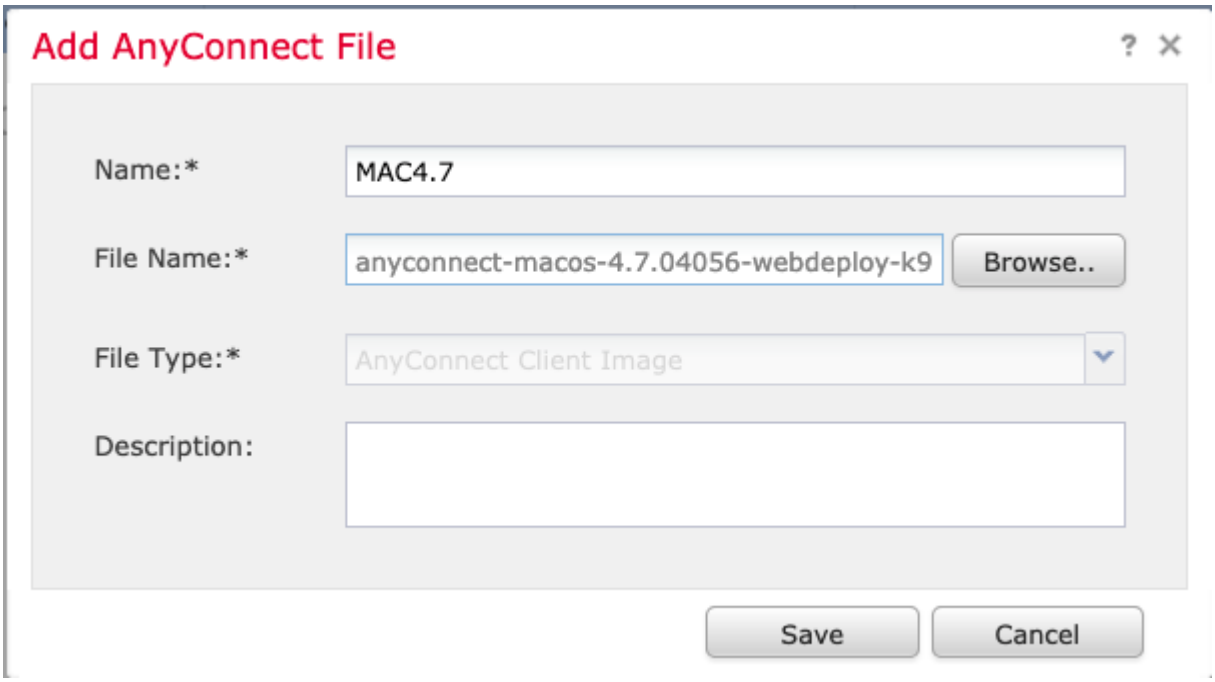
1. Download de afbeeldingen van webimplementation (**.pkg**) van de downloadwebpagina van Cisco.



2. Navigeer naar objecten > **Objectbeheer** > **VPN** > **AnyConnect File** > **AnyConnect File**.

3. Wijs een naam toe aan het AnyConnect-pakketbestand en selecteer het bestand **.pkg** uit uw lokale systeem nadat het is geselecteerd.

4. Selecteer **Opslaan**.



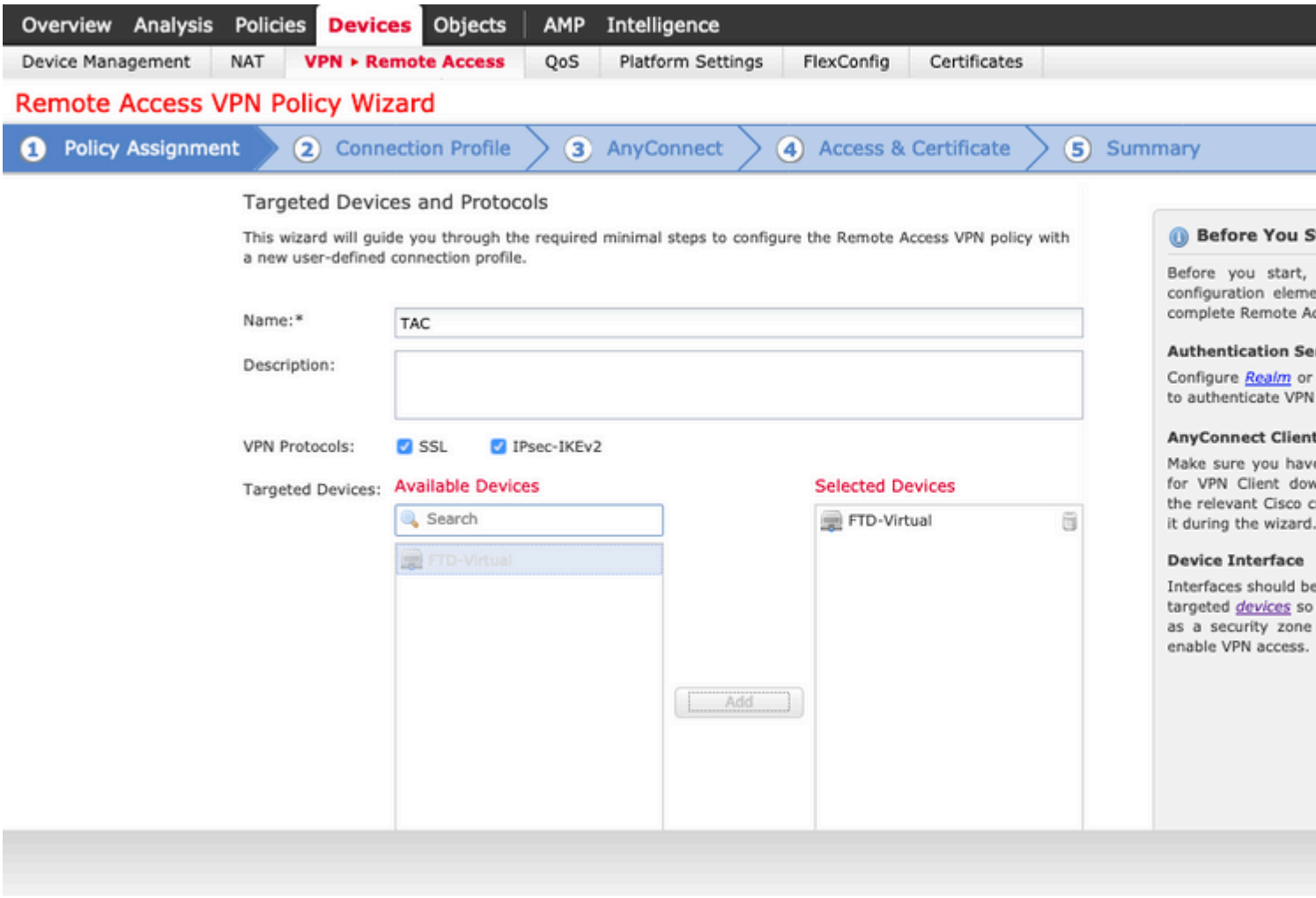
Opmerking: extra pakketten kunnen worden geüpload op basis van uw vereisten (Windows, Mac, Linux).

Stap 7. Wizard Externe toegang VPN

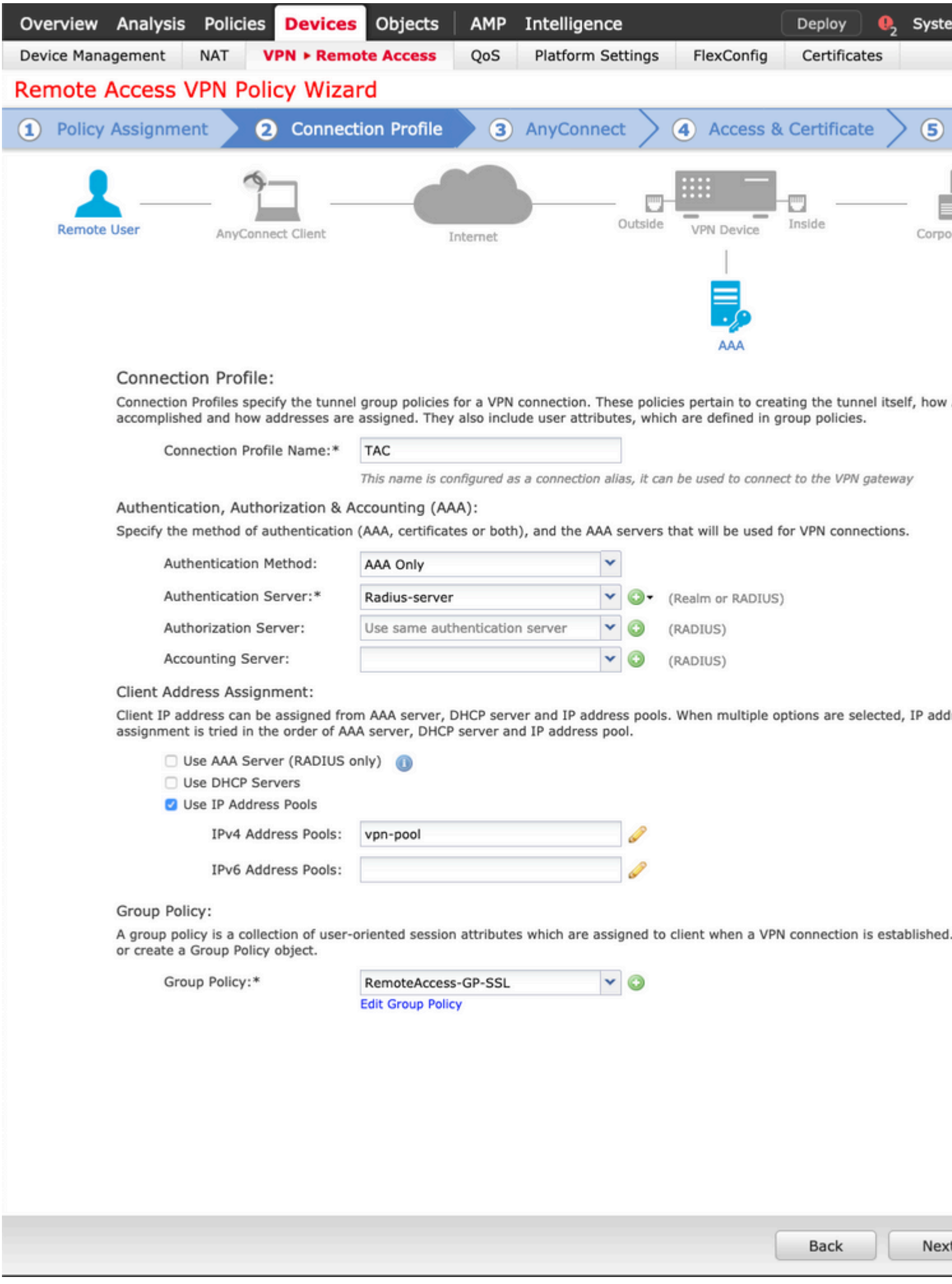
Gebaseerd op de vorige stappen kan de Wizard Externe toegang dienovereenkomstig worden gevolgd.

1. Navigeer naar **Apparaten** > **VPN** > **Externe toegang**.

2. Wijs de naam van het beleid voor externe toegang toe en selecteer een FTD-apparaat uit de lijst met **beschikbare apparaten**.

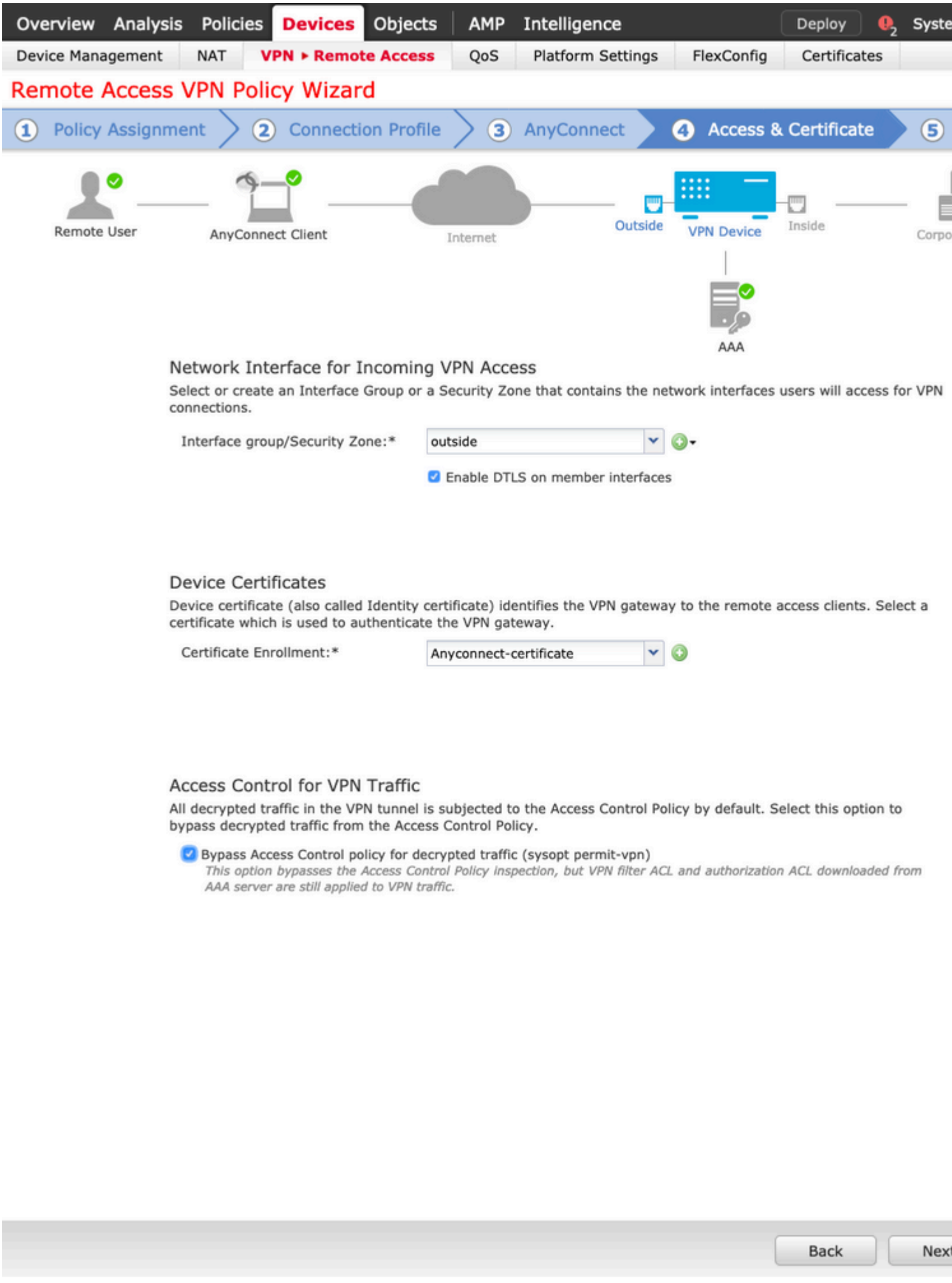


3. Wijs de **naam** van het **verbindingsprofiel toe** (de naam van het verbindingsprofiel is de naam van de tunnelgroep), selecteer de **verificatieserver** en **adresgroepen** zoals in de afbeelding.



4. Selecteer het +-symbool om **Groepsbeleid** te maken.

in dit scenario is de FTD zo geconfigureerd dat hij geen VPN-verkeer inspecteert, wordt de optie Toegangsbeheer (ACS) omzeild.



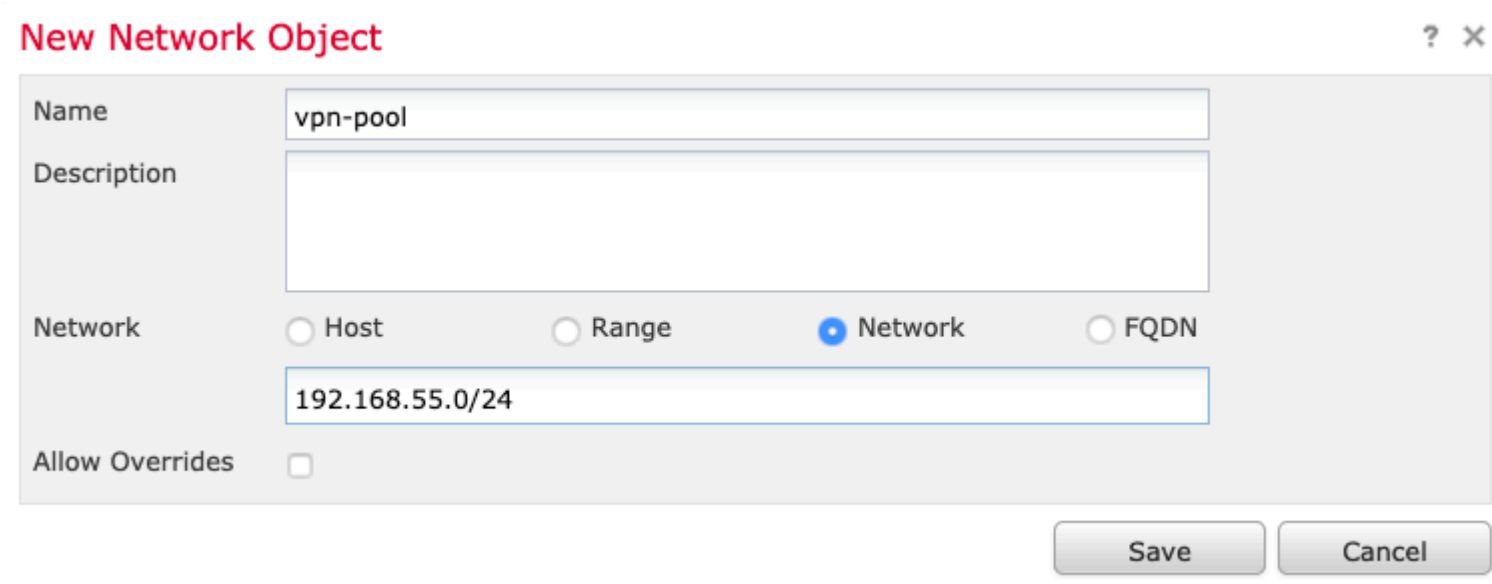
10. Selecteer **Voltooien** en **wijzig** de wijzigingen:

    Alle configuratie met betrekking tot VPN, SSL-certificaten en AnyConnect-pakketten wordt via FMC

is een voorkeursvertaalmethode die wordt gebruikt om te voorkomen dat verkeer naar het internet wordt geleid als het is bedoeld om via een VPN-tunnel te stromen (Externe toegang of Site-to-Site).

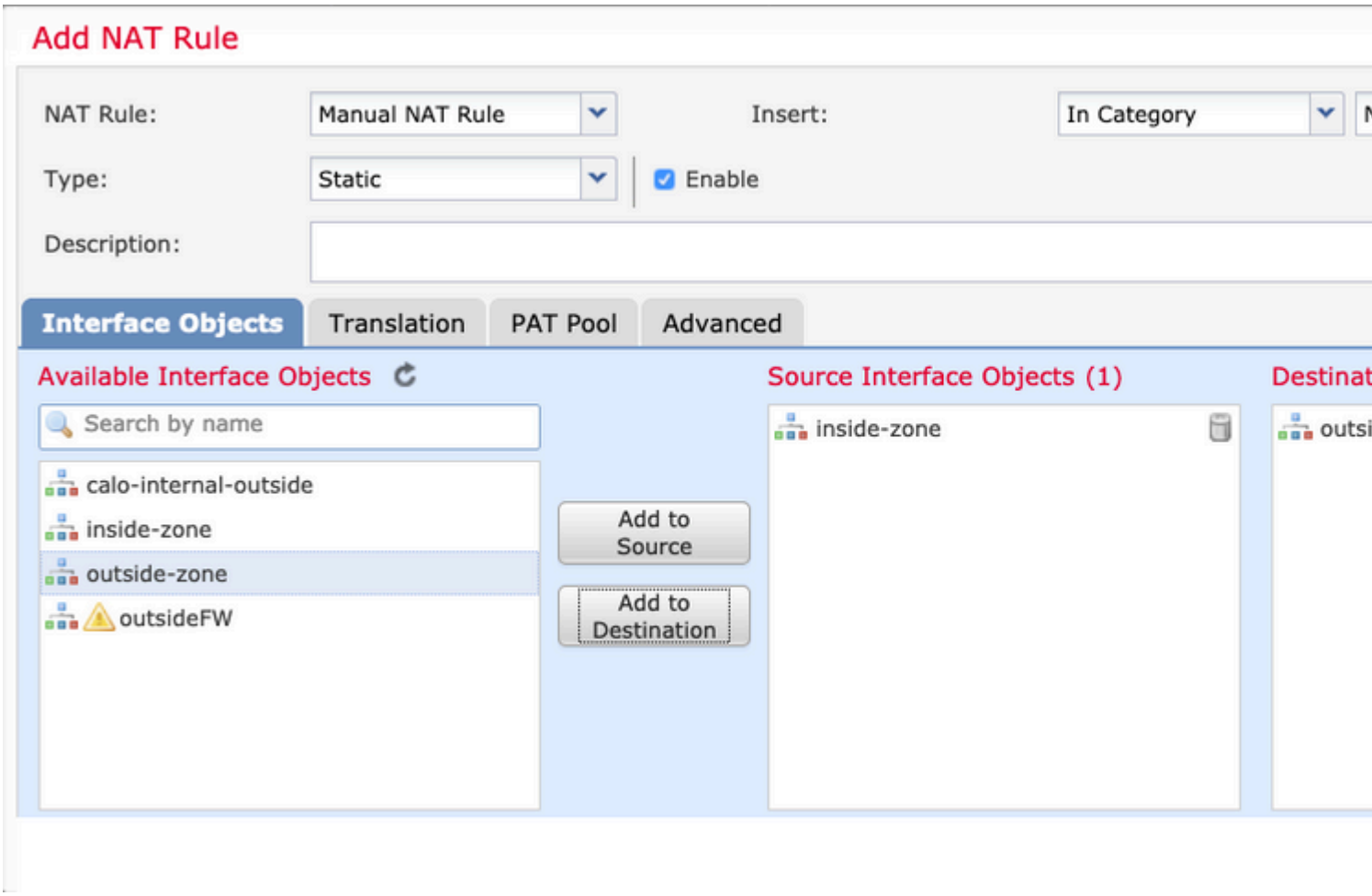
Dit is nodig wanneer het verkeer van uw interne netwerk bedoeld is om over de tunnels te stromen zonder enige vertaling.

1. Navigeer naar **Objecten> Netwerk > Netwerk toevoegen > Object toevoegen** zoals in de afbeelding.

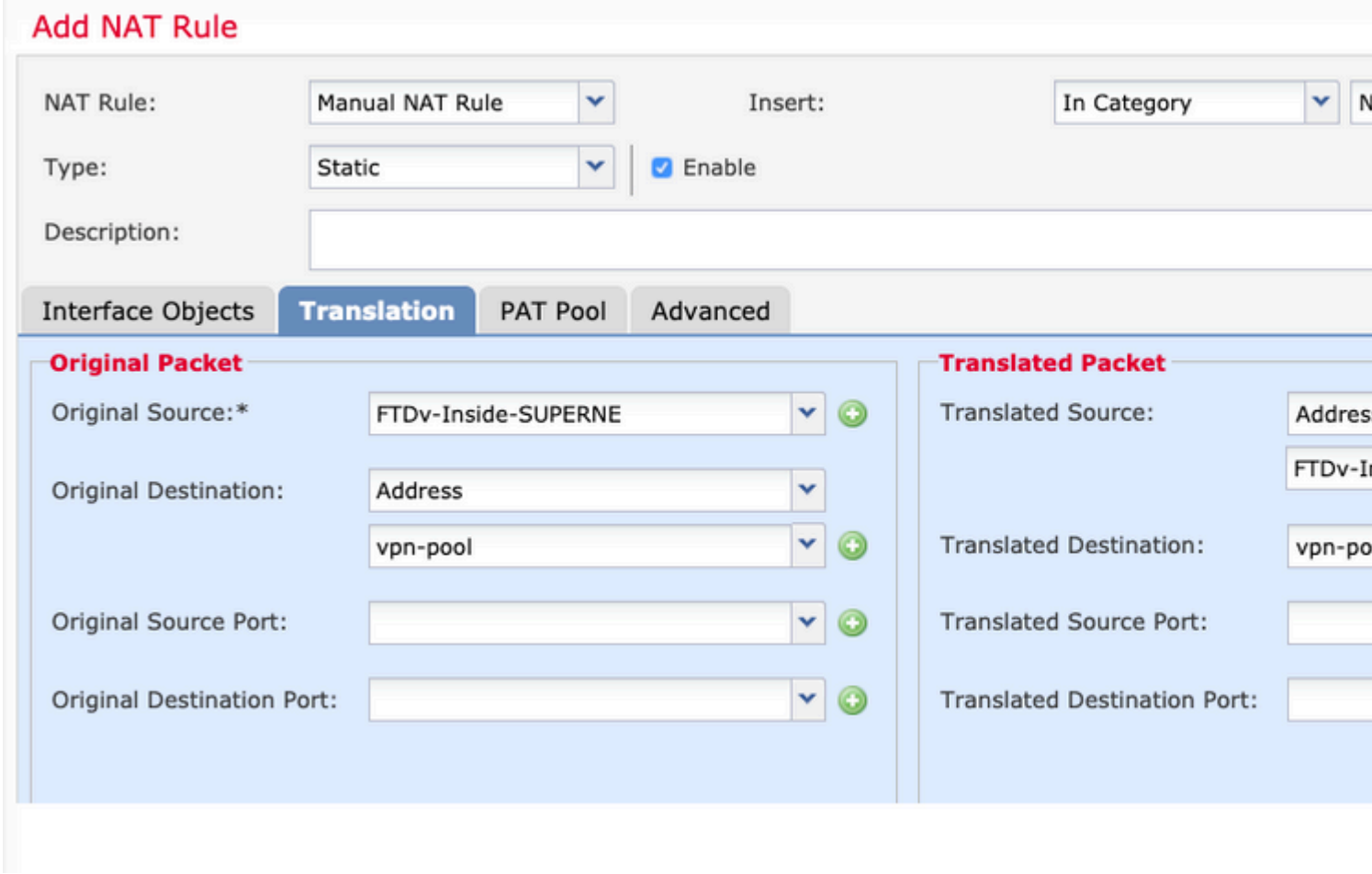


2. Navigeer naar **apparaat > NAT,** selecteer het NAT-beleid dat door het apparaat in kwestie wordt gebruikt en maak een nieuwe instructie**.**

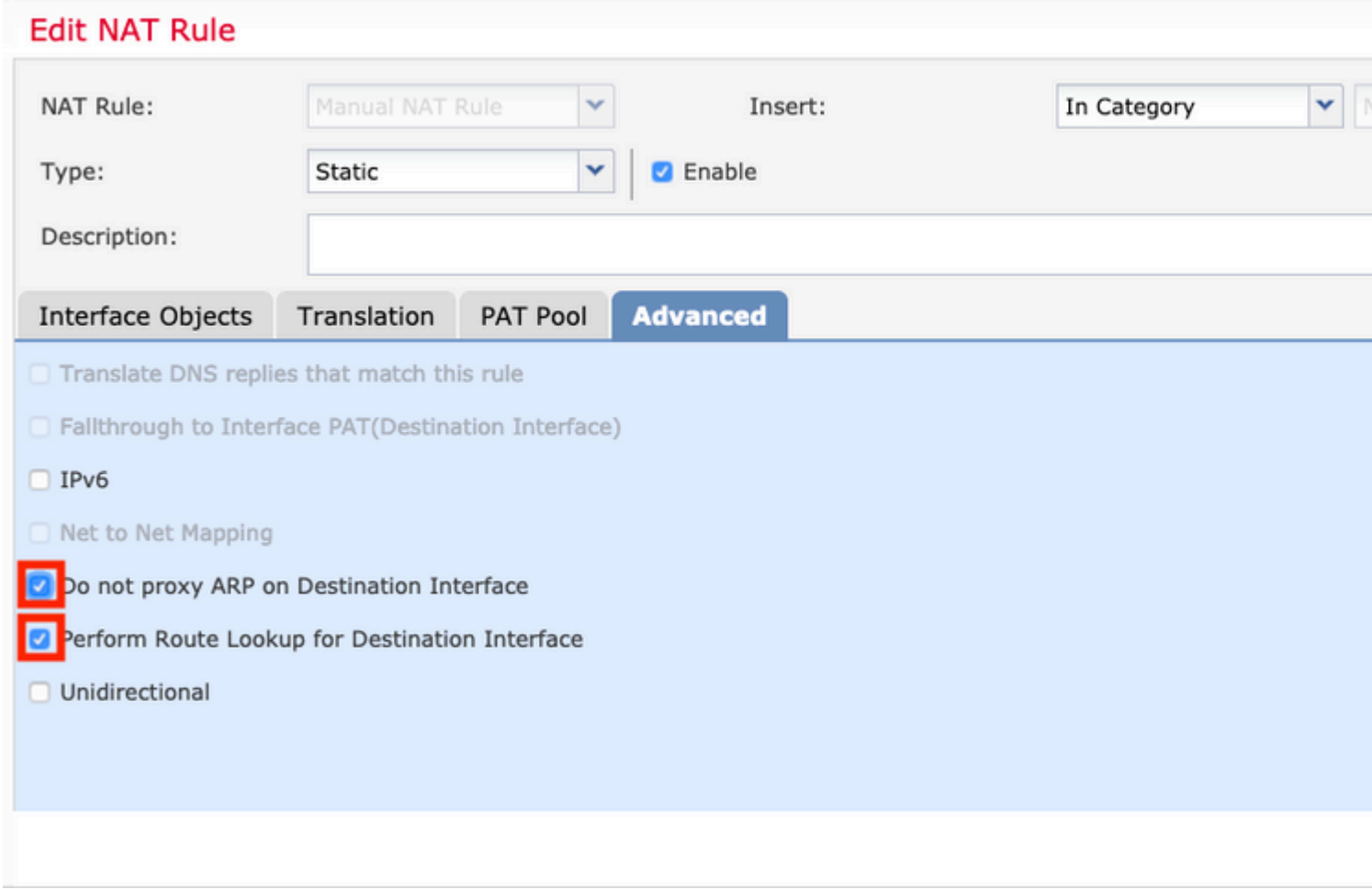
Opmerking: de verkeersstroom gaat van binnen naar buiten.



3. Selecteer de interne bronnen achter de FTD (**oorspronkelijke bron** en **vertaalde bron**) en de bestemming als de lokale ip-pool voor de AnyConnect-gebruikers (**oorspronkelijke bestemming** en **vertaalde bestemming**) zoals in de afbeelding.

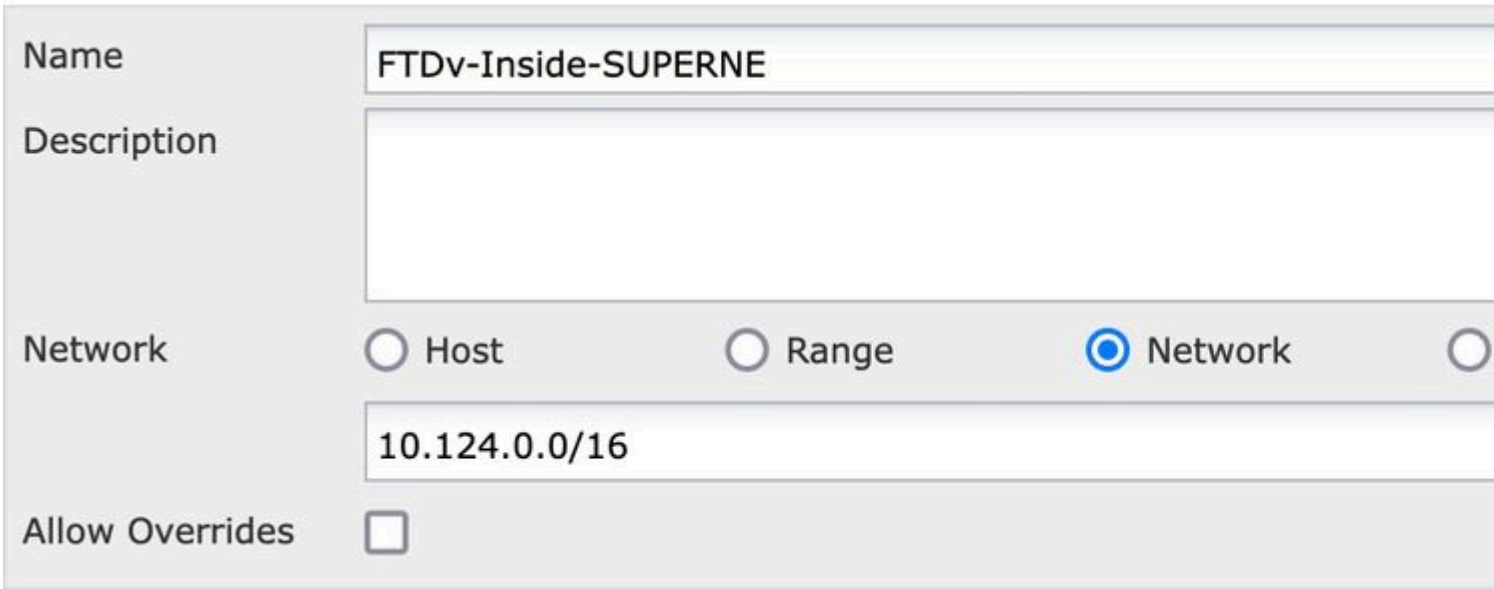


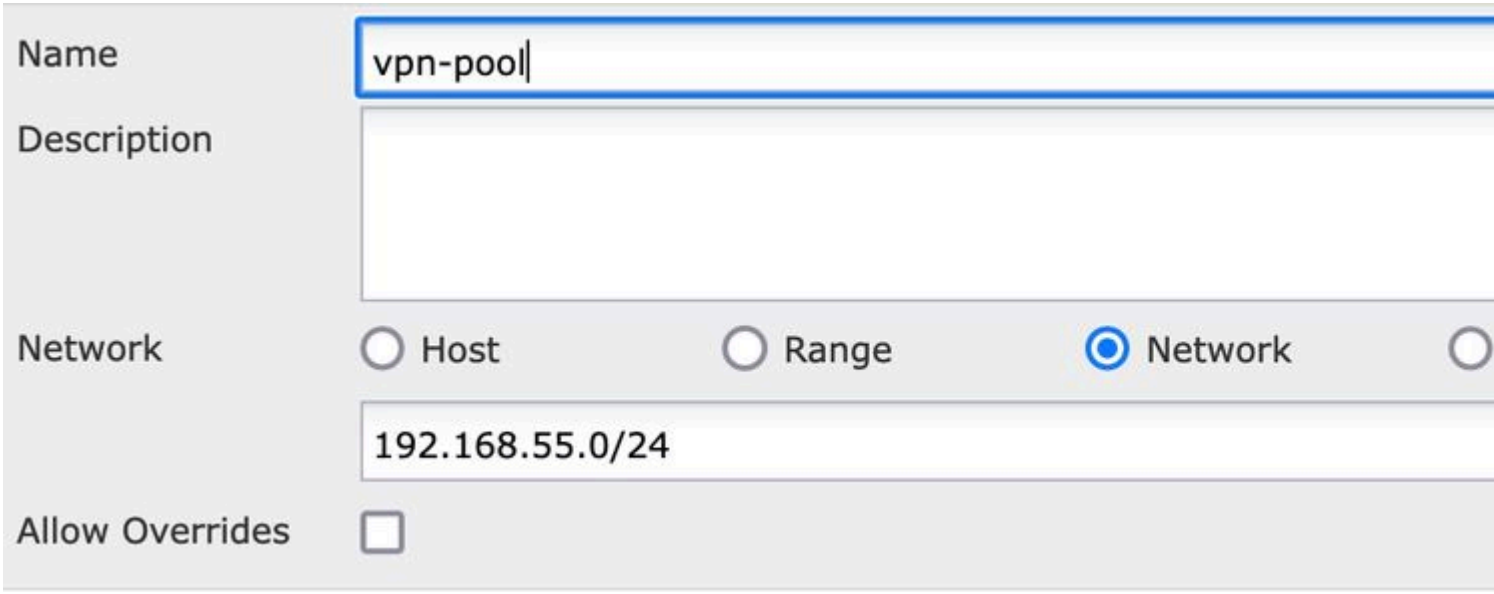
4. Zorg ervoor dat de opties (zoals in de afbeelding) van elkaar worden gewisseld, zodat "**no-proxy-arp**" en "**route-lookup**" in de NAT-regel zijn ingeschakeld, en selecteer **OK** zoals in de afbeelding.



5. Dit is het resultaat van de NAT-vrijstellingsconfiguratie.

De in de vorige sectie gebruikte objecten worden hieronder beschreven.





Stap 2. haarspeldconfiguratie

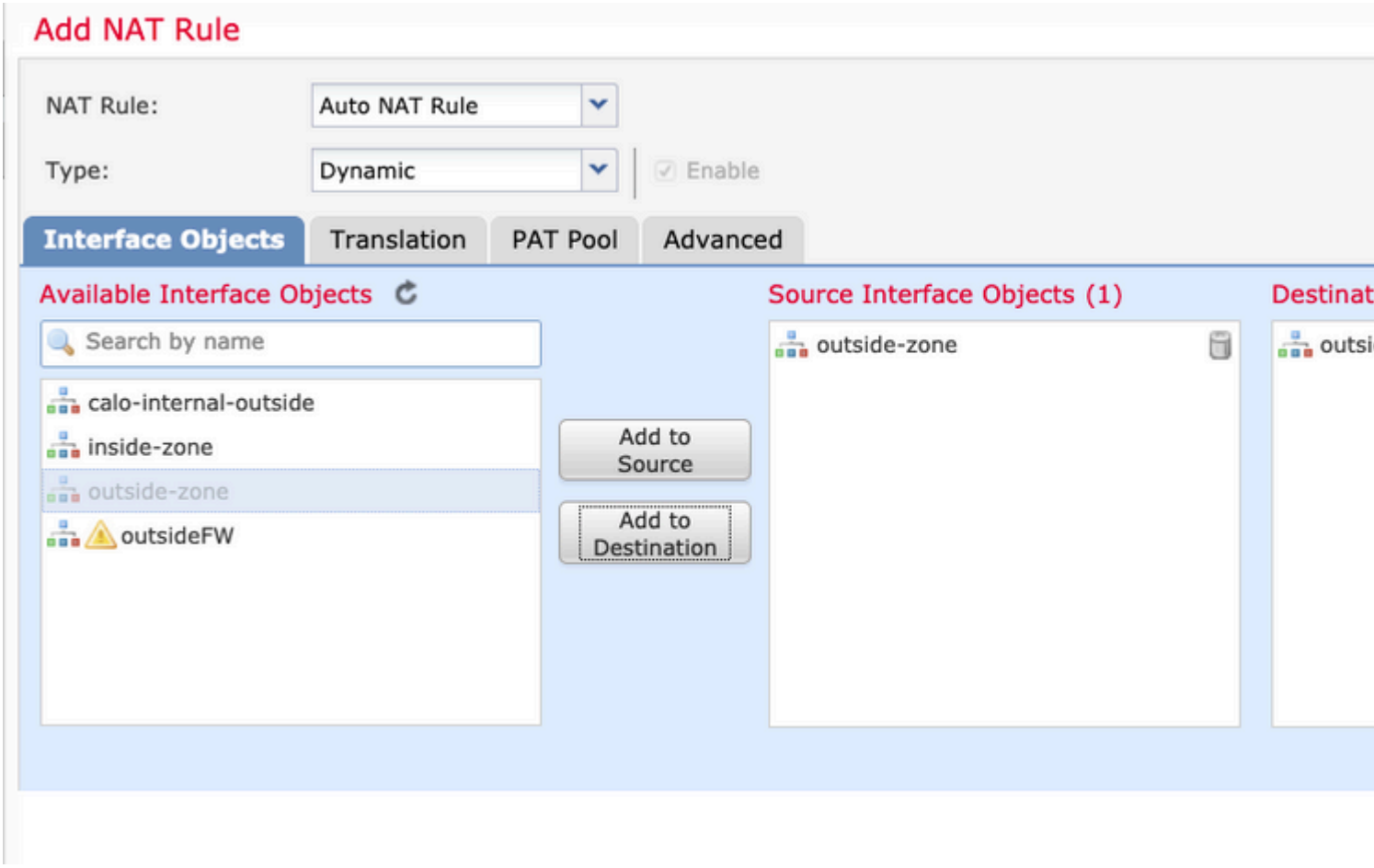
Ook bekend als **U-turn**, dit is een vertaalmethode die het verkeer toelaat om over dezelfde interface te stromen als het verkeer ontvangen wordt.

Bijvoorbeeld, wanneer AnyConnect wordt geconfigureerd met een **Full-tunnel** split-tunnelbeleid, worden de interne bronnen benaderd volgens het NAT-vrijstellingsbeleid. Als het AnyConnect-clientverkeer bedoeld is om een externe site op internet te bereiken, is de haarspeld NAT (of U-turn) verantwoordelijk voor het routeren van het verkeer van buiten naar buiten.

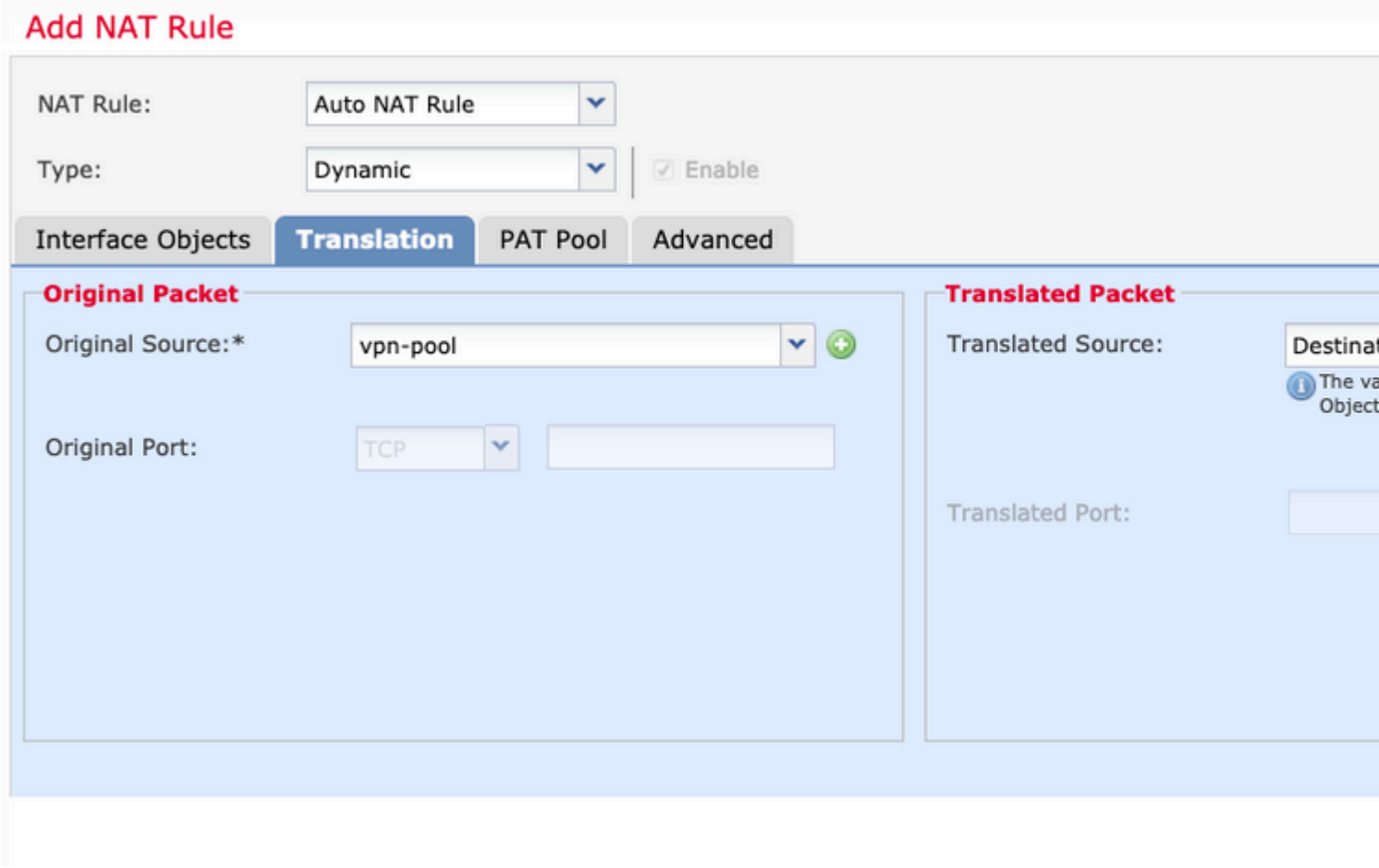
Een VPN pool object moet gemaakt worden voor de NAT configuratie.

1. Maak een nieuwe NAT-verklaring, selecteer **Auto NAT-regel** in het veld **NAT-regel** en selecteer **Dynamisch** als NAT-**type**.

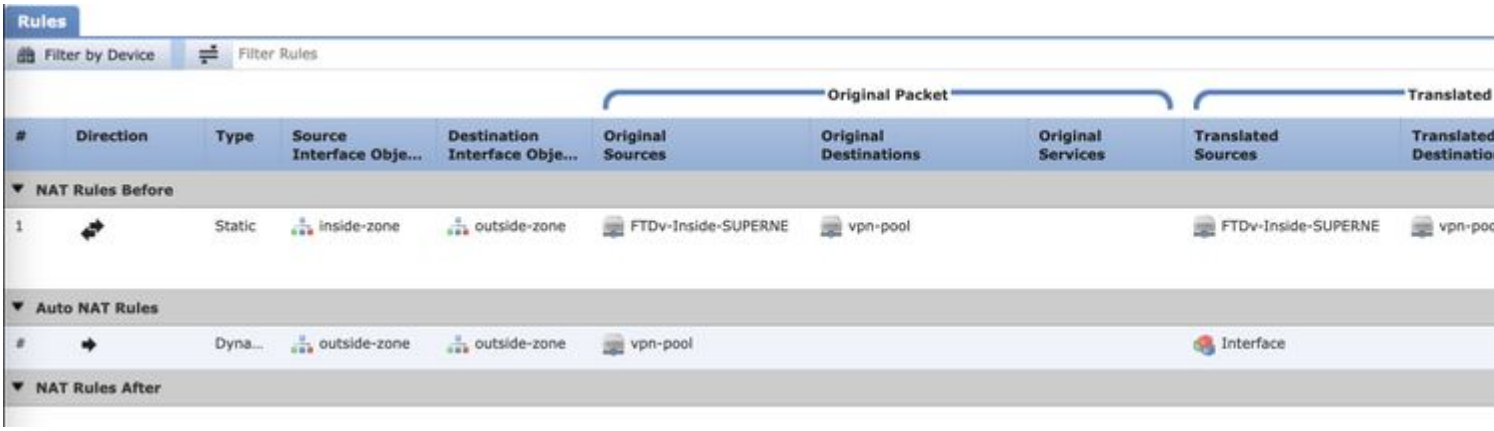
2. Selecteer dezelfde interface voor de **bron-** en doelinterfaceobjecten (buiten):



3. Selecteer op het tabblad Vertaling als **Oorspronkelijke bron** het VPN-pool object en selecteer **Doelinterface IP** als **Vertaalde bron**, selecteer **OK** zoals in de afbeelding.



4. Dit is de samenvatting van de NAT-configuratie zoals in de afbeelding.



5. Klik op **Opslaan** en de wijzigingen **implementeren**.

Verifiëren

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

Voer deze opdrachten uit in de FTD-opdrachtregel.

- **sh crypto ca-certificaten**
- **tonen in werking stellen-configuratie ip lokale pool**
- **tonen in werking stellen-configuratiewebvpn**
- **tonen in werking stelt-Config tunnel-groep**

- **tonen in werking stelt-configuratiegroepsbeleid**
- **Toon in werking stelt -in werking stellen-configuratiesl**
- **toon in werking stelt -in werking stellen-Config NAT**

Problemen oplossen

Er is momenteel geen specifieke informatie over probleemoplossing beschikbaar voor deze configuratie.

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.