SSL AnyConnect Management VPN op FTD configureren

Inhoud

Inleiding

Dit document beschrijft hoe u een Cisco AnyConnect Management-tunnel kunt configureren op een Cisco Firepower Threat Defense (FTD) die wordt beheerd door Cisco Firepower Management Center (FMC). In het voorbeeld onder Secure Socket Layer (SSL) wordt gebruikt om Virtual Private Network (VPN) tussen FTD en een Windows 10-client te maken.

Bijgedragen door Daniel Perez Vertti Vazquez, Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco AnyConnect-profieleditor
- SSL AnyConnect-configuratie via FMC.
- Verificatie van clientcertificaten

Gebruikte componenten

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

- Cisco FTD versie 6.7.0 (gebouwd 65)
- Cisco FMC versie 6.7.0 (gebouwd 65)
- Cisco AnyConnect 4.9.01095 geïnstalleerd op Windows 10-machine

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Vanaf release 6.7 ondersteunt Cisco FTD de configuratie van AnyConnect Management-tunnels. Dit maakt eerder geopende verbeteringsaanvraag op CSCvs78215.

Met de functie AnyConnect Management kunt u direct nadat het eindpunt is beëindigd een VPN-tunnel maken. Het is niet nodig dat de gebruikers de AnyConnect-app handmatig starten, zodra hun systeem is ingeschakeld, detecteert de AnyConnect VPN-agent de Management VPN-functie en start een AnyConnect-sessie met behulp van de hostingvermelding die in de serverlijst van het AnyConnect Management VPN-profiel is gedefinieerd.

Beperkingen

- Alleen verificatie van clientcertificaten wordt ondersteund.
- Alleen Machine certificaatwinkel wordt ondersteund voor Windows-clients.
- Niet ondersteund op Cisco Firepower Apparaat Manager (FDM) CSCvx90058.
- Niet ondersteund op Linux-klanten.

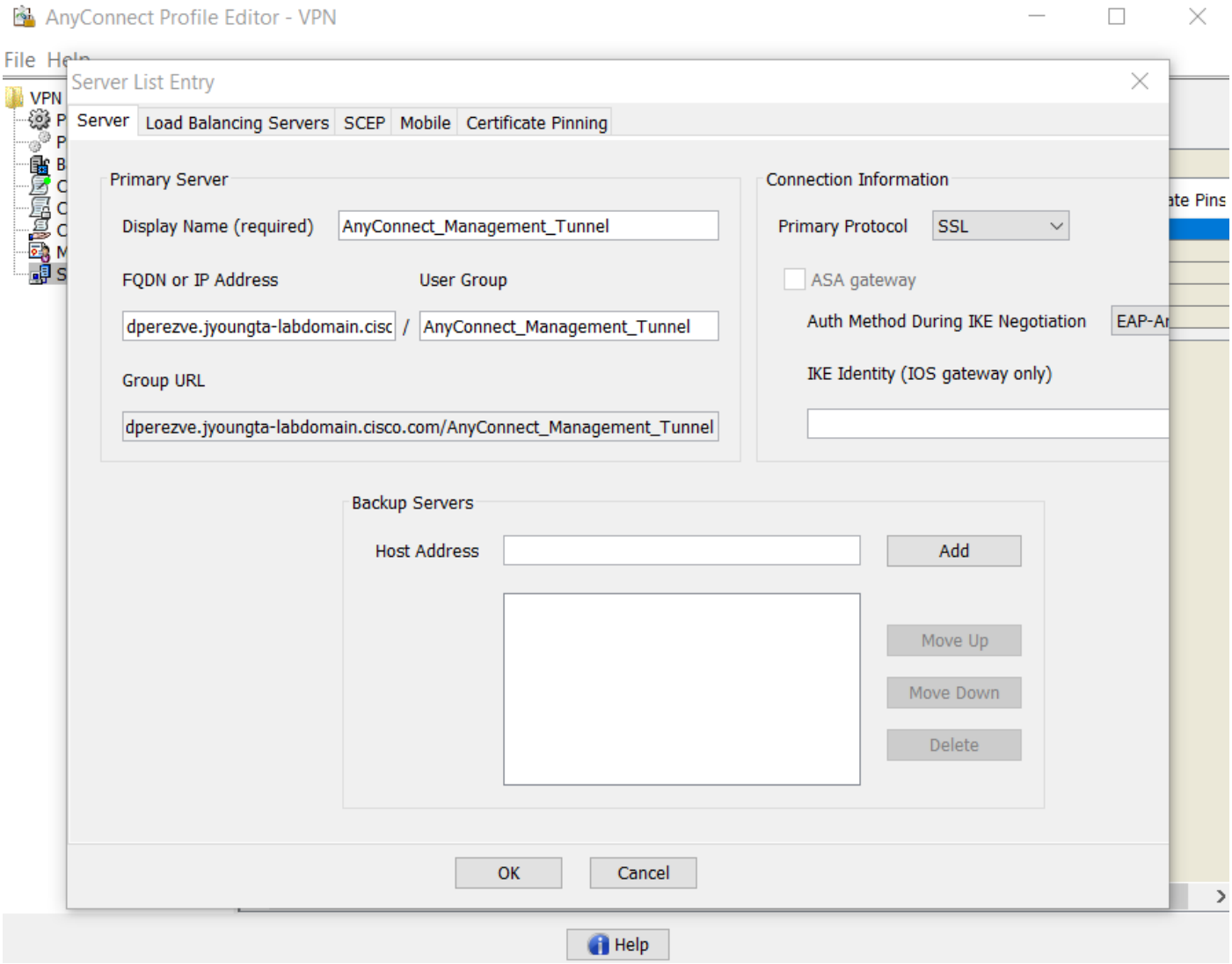
Configureren

Configuraties

Stap 1. Maak AnyConnect Management VPN-profiel

Open de AnyConnect Profile Editor om AnyConnect Management VPN-profiel te maken. Het beheerprofiel bevat alle instellingen die worden gebruikt om de VPN-tunnel te maken nadat de eindpunten zijn opgestart.

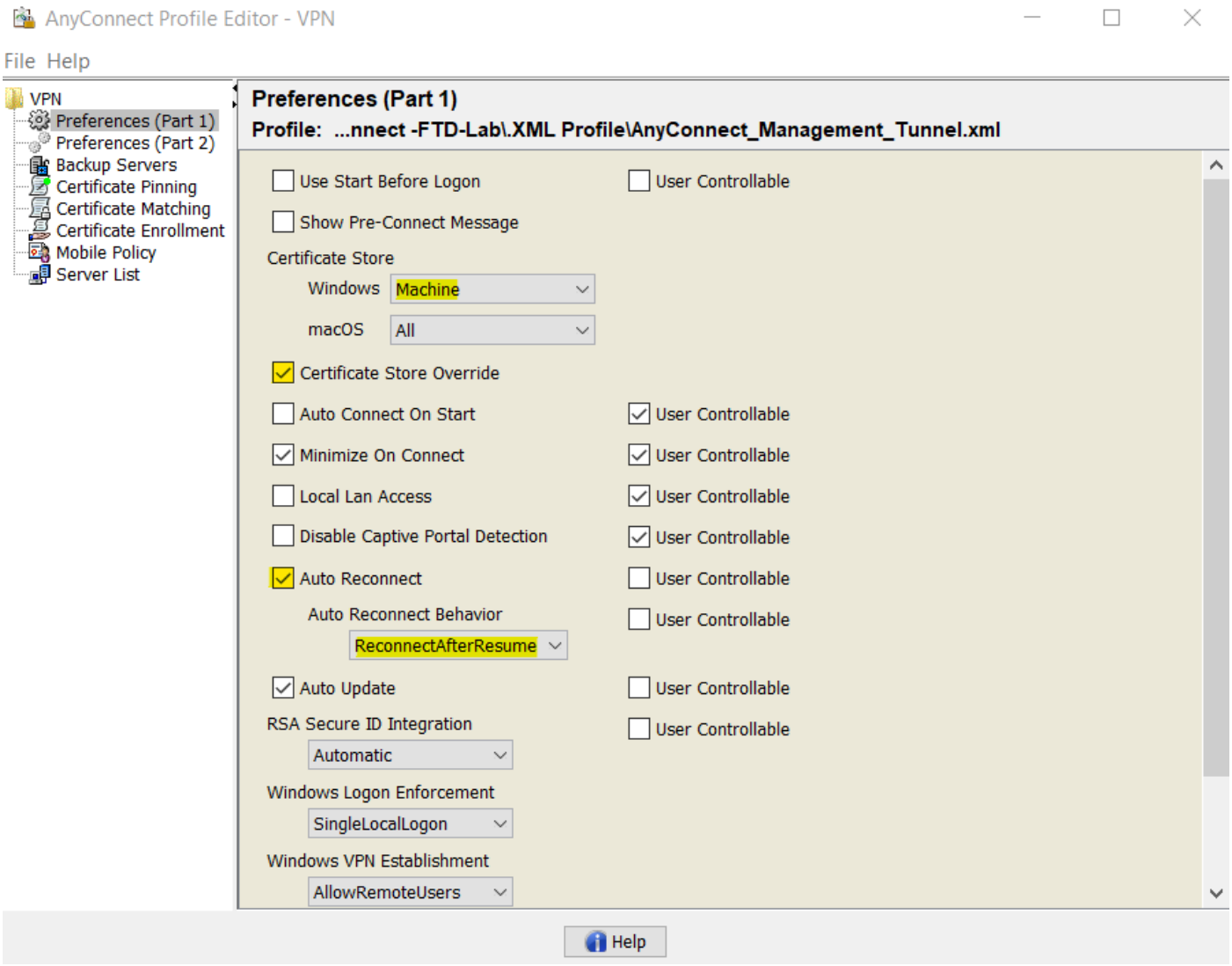
In dit voorbeeld wordt een Server List die naar Full Qualified Domain Name (FQDN) wijst, dperezve.jyoungta-labdomein.cisco.com gedefinieerd en SSL is geselecteerd als het primaire protocol. Als u een serverlijst wilt toevoegen, navigeer dan in de **lijst met servers** en selecteer de knop **Toevoegen**, vult u de gewenste velden in en slaat u de wijzigingen op.



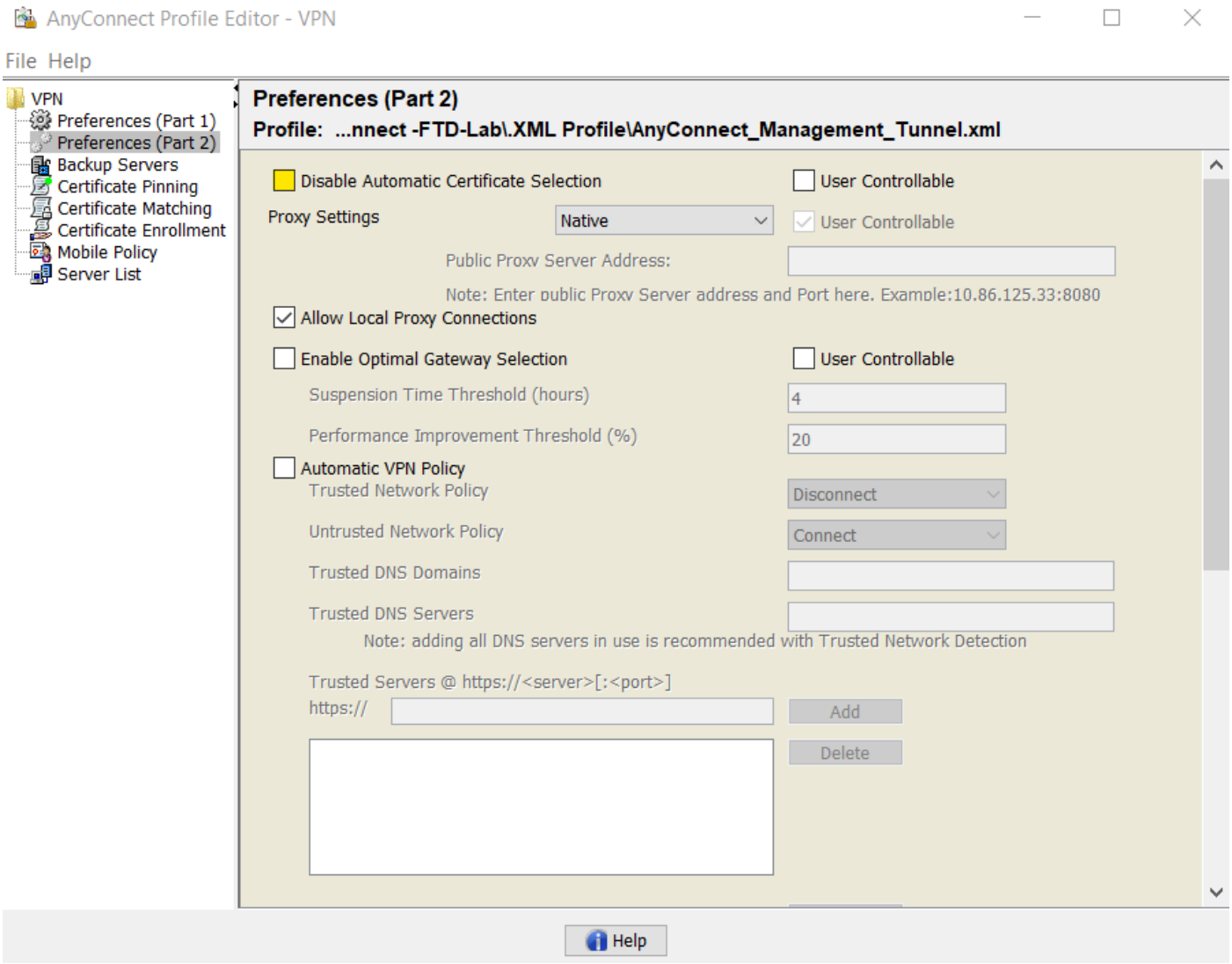
Naast de serverlijst moet het VPN-profiel van het beheer een aantal verplichte voorkeuren bevatten:

- **Automatische** selectie moet op **waarheid** worden ingesteld.
- **AutoReconconnect** moet worden ingesteld op **waarheid**.
- **AutoReconnectBehavior** moet worden ingesteld voor **ReconconnectAfterResume**.
- **AutoUpdate** moet op **fout** worden ingesteld.
- **BlockUnvertrouwde servers** moet op **waar** ingesteld worden.
- **certificaatwinkel** moet worden ingesteld voor **MachineStore**.
- **certificaatnummerStoreOverride** moet op **waarheid** worden ingesteld.
- **AutomatischServerSelecteren inschakelen** moet op **onjuist** zijn ingesteld.
- **Schakel de** toepassing **in** voor de **scripts** op **vals** moeten worden ingesteld.
- **BewaarVPNOnLogoff** moet op **waarheid** worden ingesteld.

In AnyConnect Profile Editor navigeer naar **voorkeuren (Deel 1)** en stel de instellingen als volgt in:



navigeer vervolgens naar **voorkeuren (Deel 2)** en controleer de optie **Automatisch certificaat selecteren** niet.



Stap 2. Maak AnyConnect VPN-profiel

Naast het VPN-profiel voor beheer moet het normale AnyConnect VPN-profiel worden geconfigureerd. Het AnyConnect VPN-profiel wordt tijdens de eerste verbindingspoging gebruikt en tijdens deze sessie wordt het Beheersprofiel gedownload van FTD.

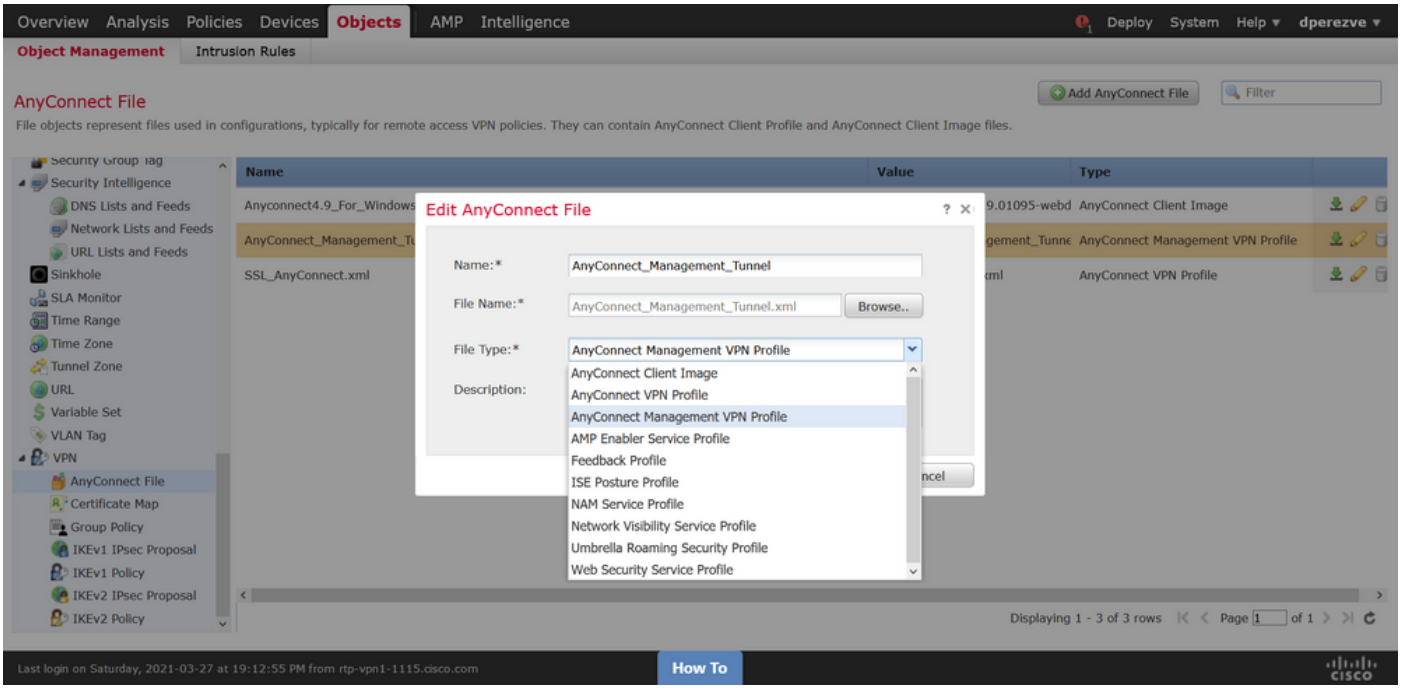
Gebruik de AnyConnect Profile Editor om het AnyConnect VPN-profiel te maken. In dit geval bevatten beide bestanden dezelfde instellingen, zodat dezelfde procedure kan worden gevolgd.

Stap 3. Upload AnyConnect Management VPN-profiel en AnyConnect VPN-profiel naar FMC

Zodra de profielen zijn gemaakt, wordt de volgende stap gezet door ze te uploaden naar het FMC, zoals AnyConnect File Objects.

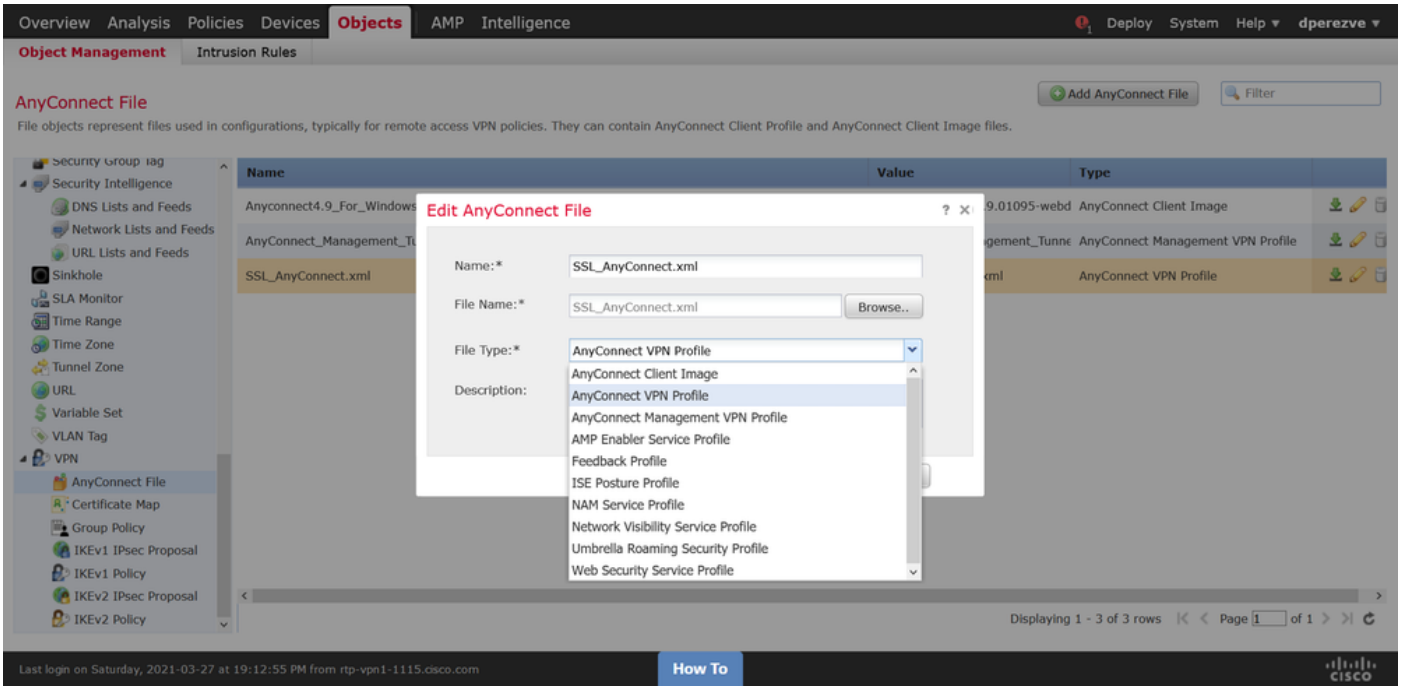
Om het nieuwe AnyConnect Management VPN-profiel naar FMC te uploaden, navigeer naar **Objecten > Objectbeheer** en kies de optie **VPN** uit de inhoudsopgave en selecteer de knop **Add AnyConnect File**.

Geef een naam voor het bestand op, kies **AnyConnect Management VPN Profile** als het bestandstype en slaat het object op.

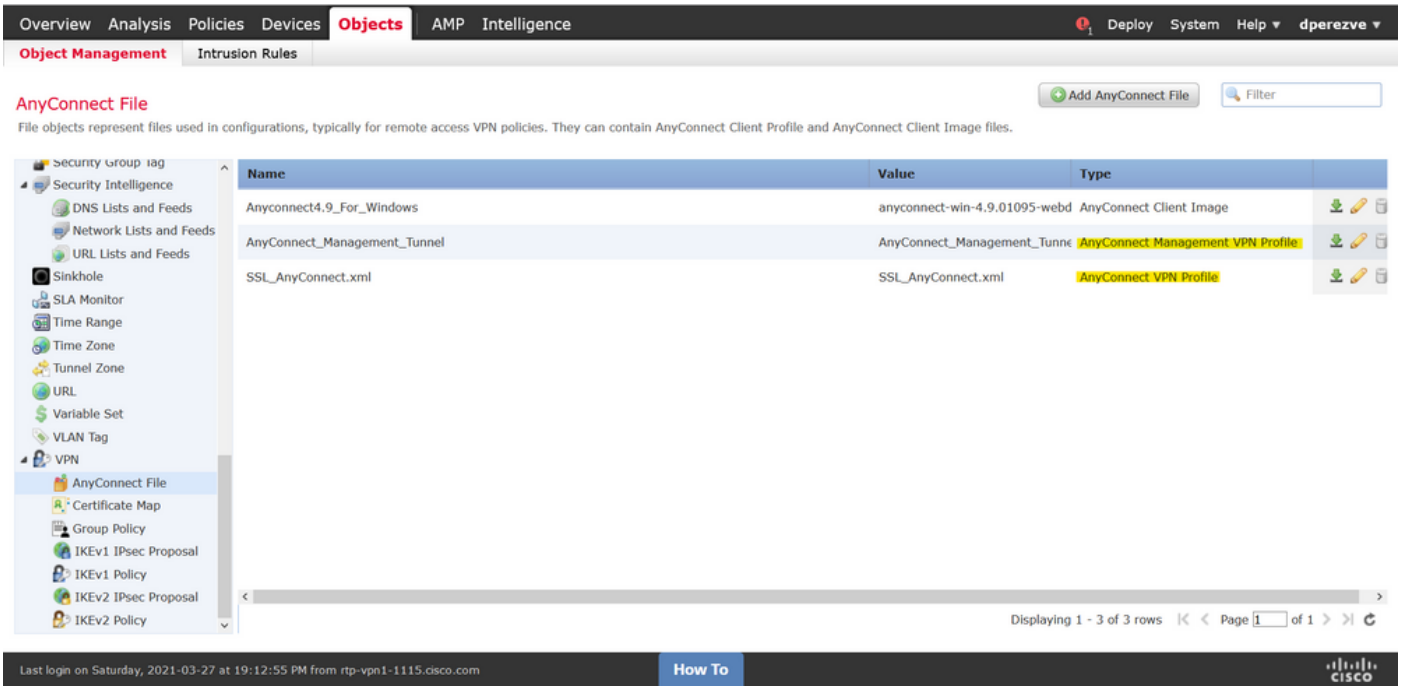


Als u het AnyConnect VPN-profiel opnieuw wilt uploaden, navigeer dan opnieuw naar **Objecten > Objectbeheer** en kies de **VPN-**optie uit de inhoudsopgave en selecteer de knop **Add AnyConnect File**.

Geef een naam voor het bestand op maar kies nu **AnyConnect VPN Profile** als bestandstype en slaat het nieuwe object op.



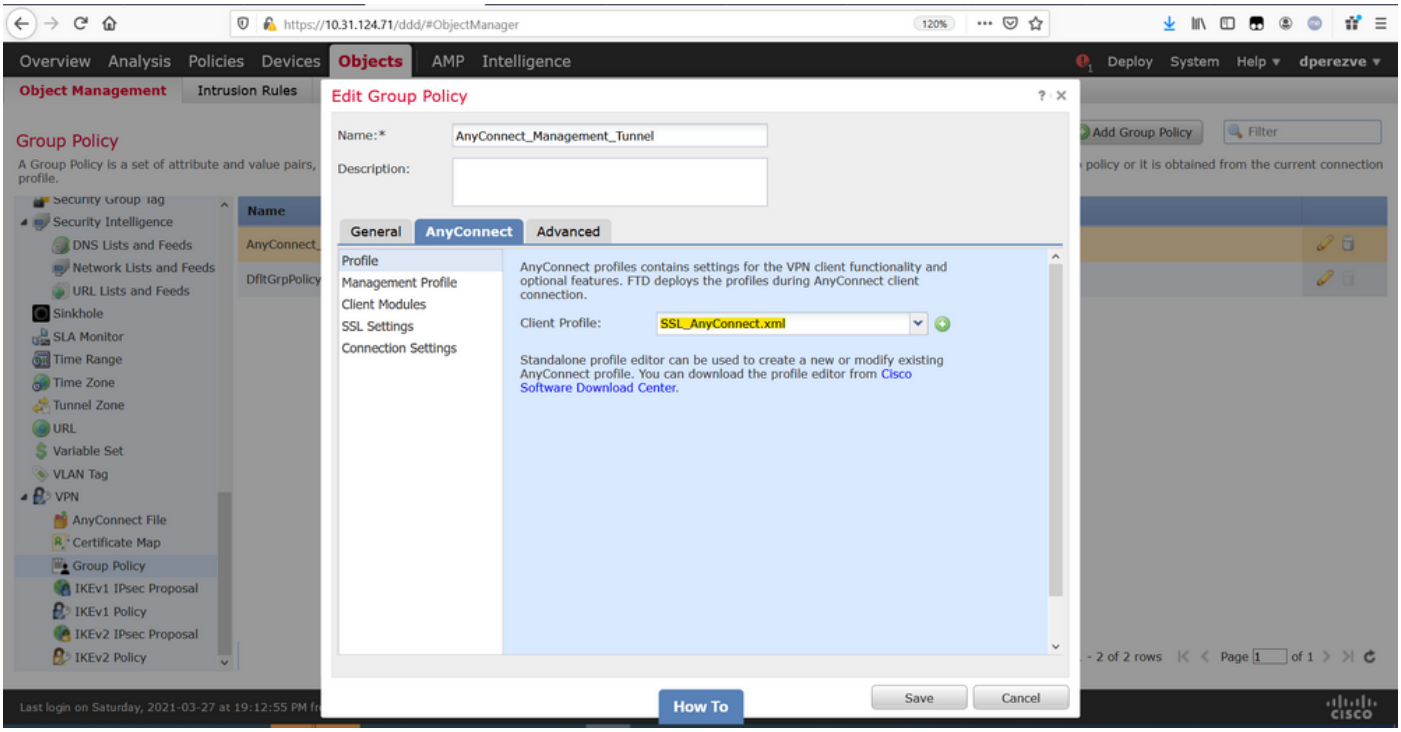
profielen moeten aan de objectlijst worden toegevoegd en als **AnyConnect Management VPN-profiel** en **AnyConnect VPN-profiel** worden gemarkeerd.



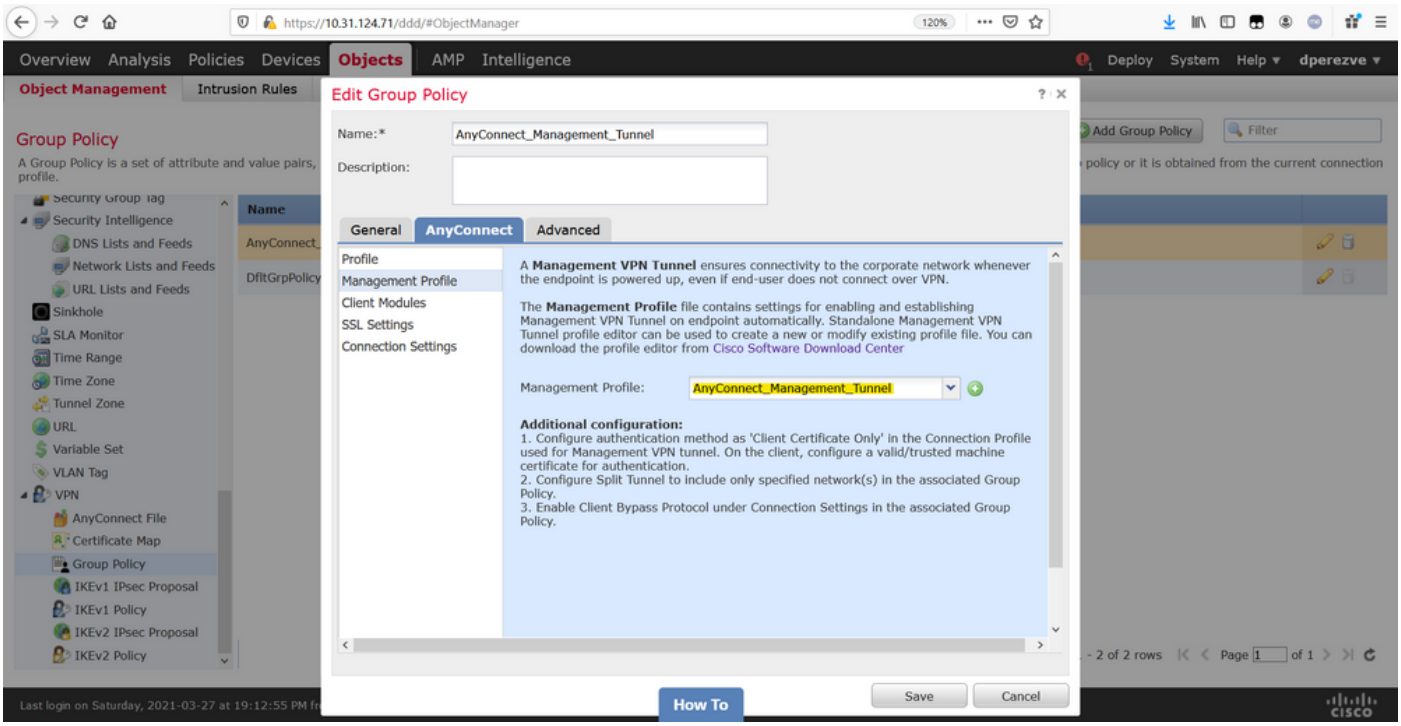
Stap 4. Groepsbeleid maken

Als u een nieuw Groepsbeleid wilt maken, navigeer dan naar **Objecten > Objectbeheer** en kies **VPN** optie uit de inhoudsopgave, selecteer **Groepsbeleid** en klik op de knop **Toevoegen groepsbeleid**.

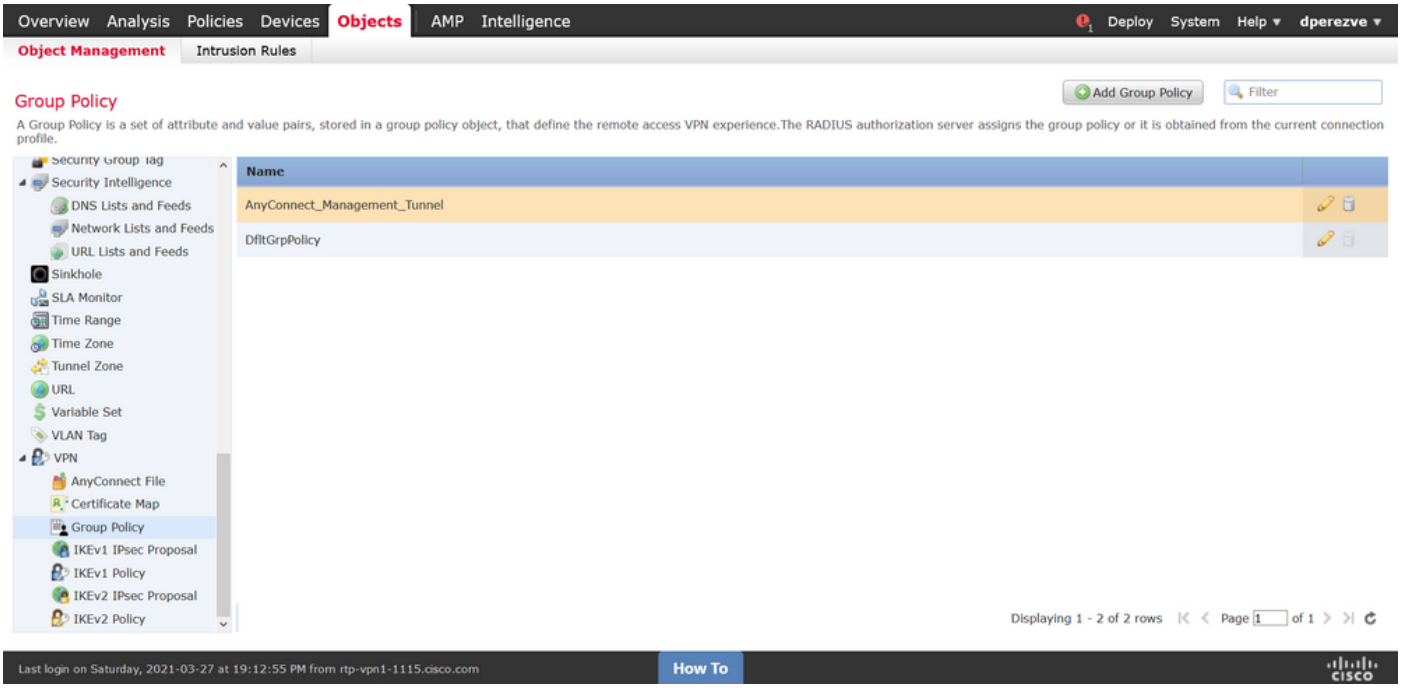
Zodra het venster **Add Group Policy** wordt geopend, selecteert u een naam, definieert u een AnyConnect-pool en opent u het tabblad **AnyConnect**. Navigeren in op **Profile** en selecteer het object dat het normale AnyConnect VPN-profiel in het vervolgkeuzemenu van **Clientprofiel** vertegenwoordigt.



navigeren naar het tabblad **Management Profile** en selecteer het object dat het VPN-profiel beheren in het vervolgkeuzemenu **Management Profile** bevat.



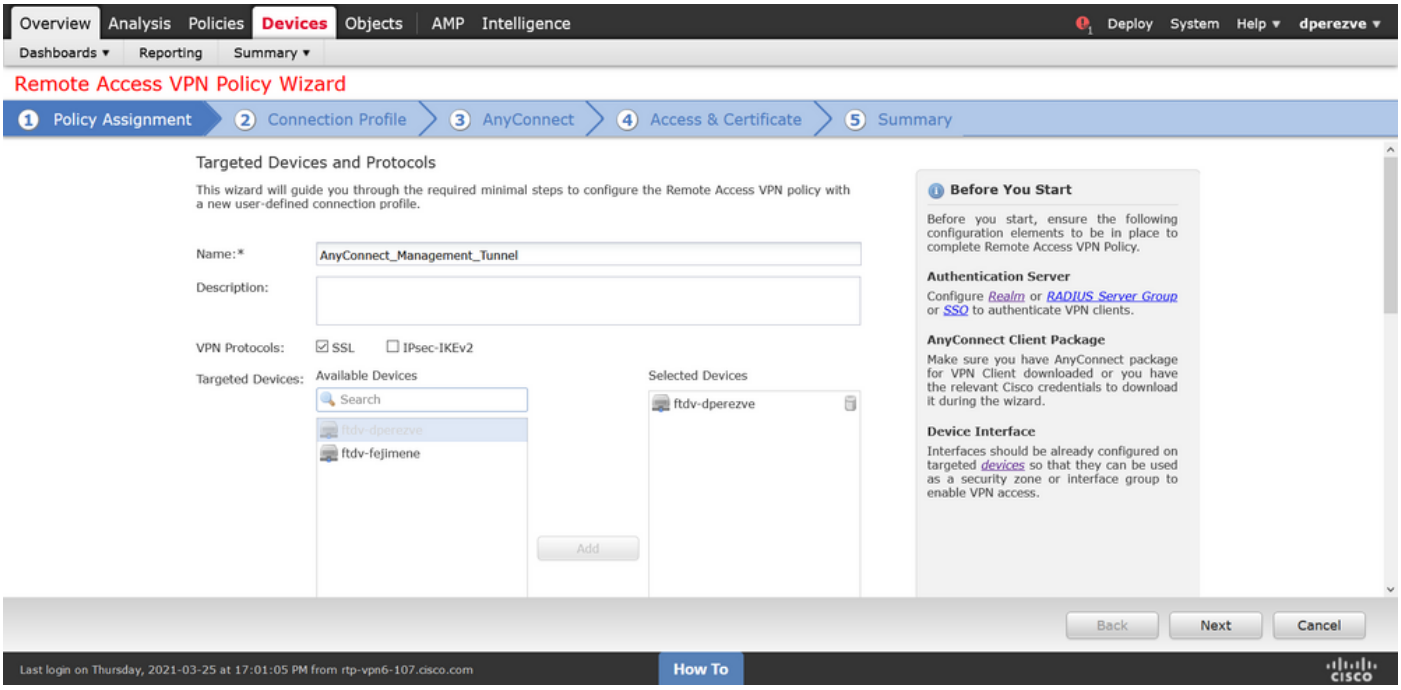
Sla de wijzigingen op om het nieuwe object aan het bestaande groepsbeleid toe te voegen.



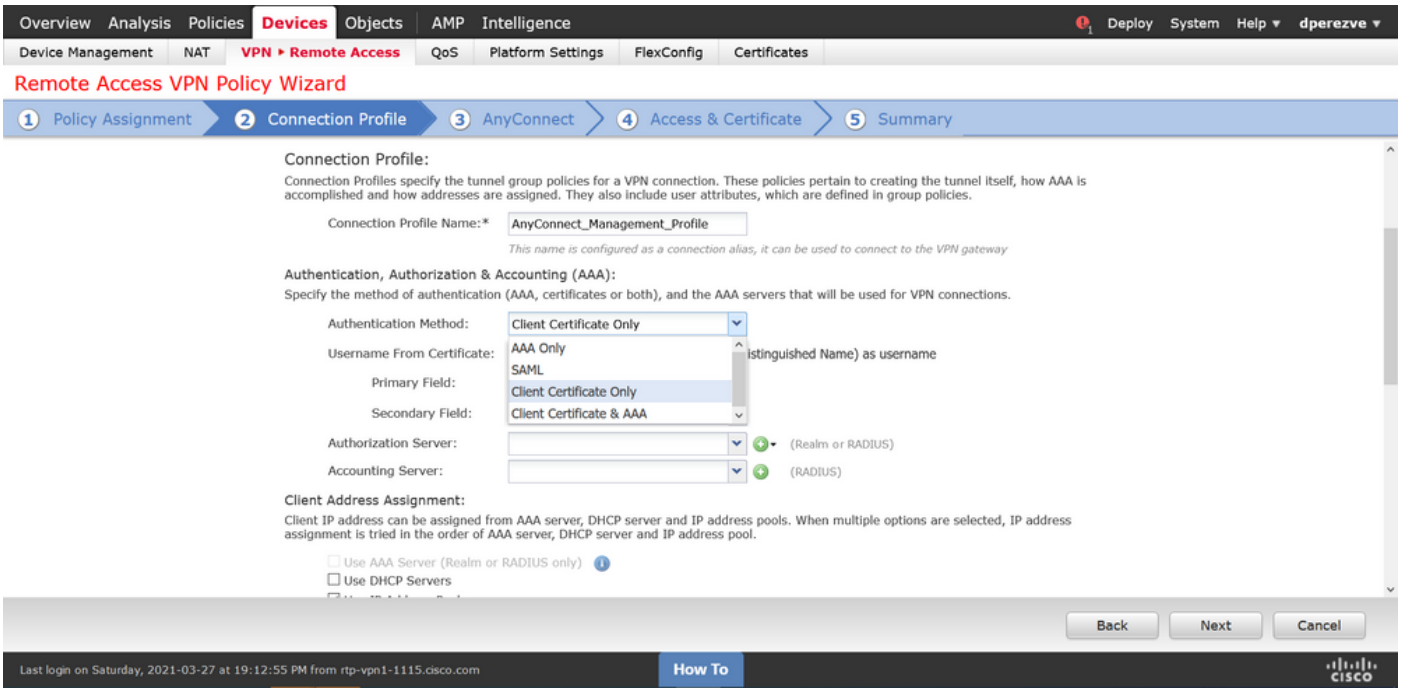
Stap 5. Maak een nieuwe AnyConnect-configuratie

De configuratie van SSL AnyConnect in FMC is samengesteld uit 4 verschillende stappen. Om AnyConnect te configureren stuurt u naar **Apparaten > VPN > Externe toegang** en selecteert u de knop **Add**. Hierdoor moet de **VPN-beleidswizard Externe toegang** openen.

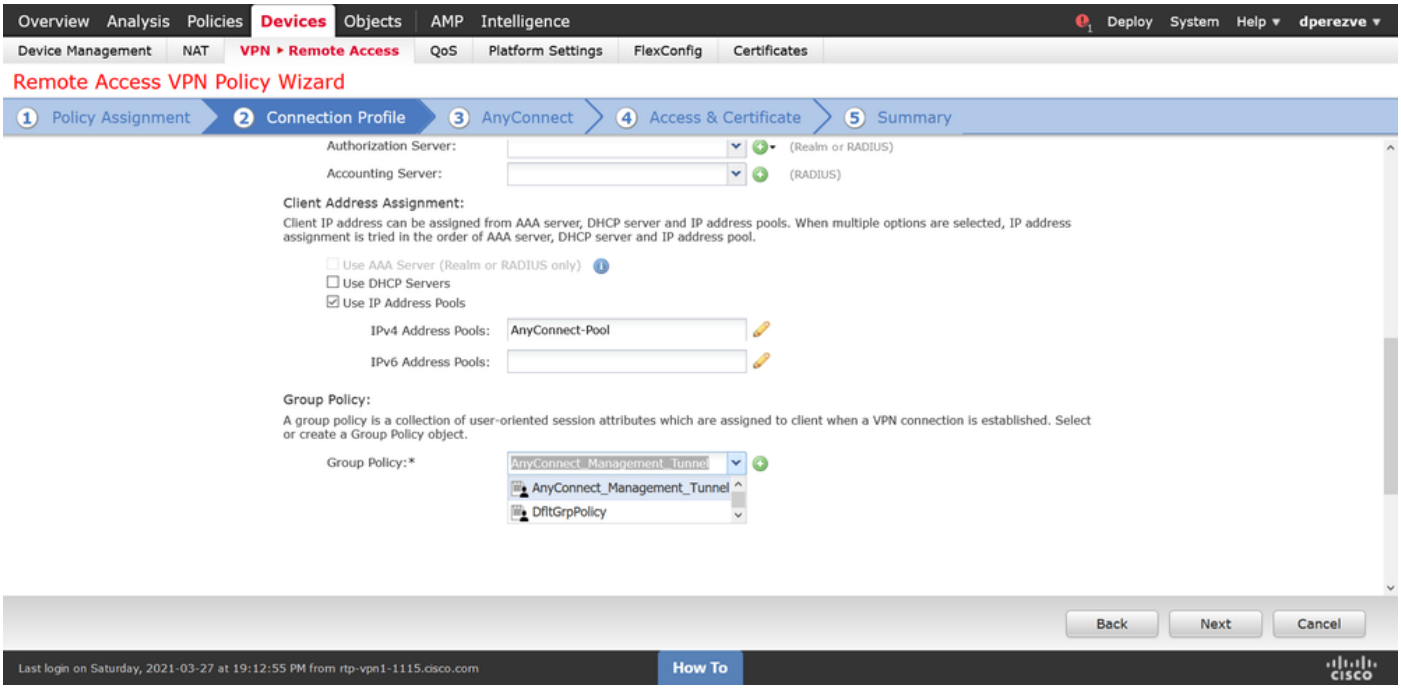
Selecteer in **het** tabblad **Policy Assignatie** het FTD-apparaat in handen, definieer een naam voor het verbindingsprofiel en controleer het SSL-selectieteken.



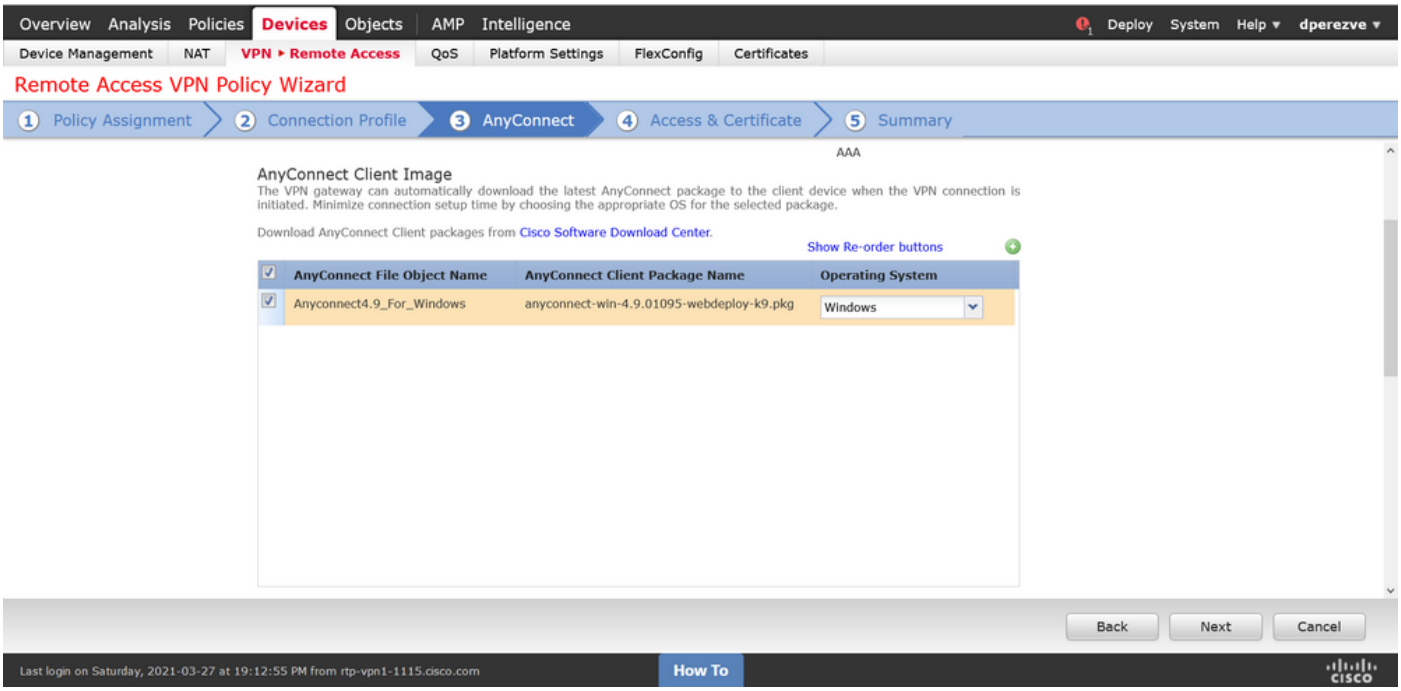
Selecteer in **Connection Profile alleen** het **Clientcertificaat** als verificatiemethode. Dit is de enige echtheidscontrole die voor de functie wordt ondersteund.



Selecteer vervolgens het object Group Policy dat in stap 3 is gemaakt in de vervolgkeuzelijst **Groepsbeleid**.



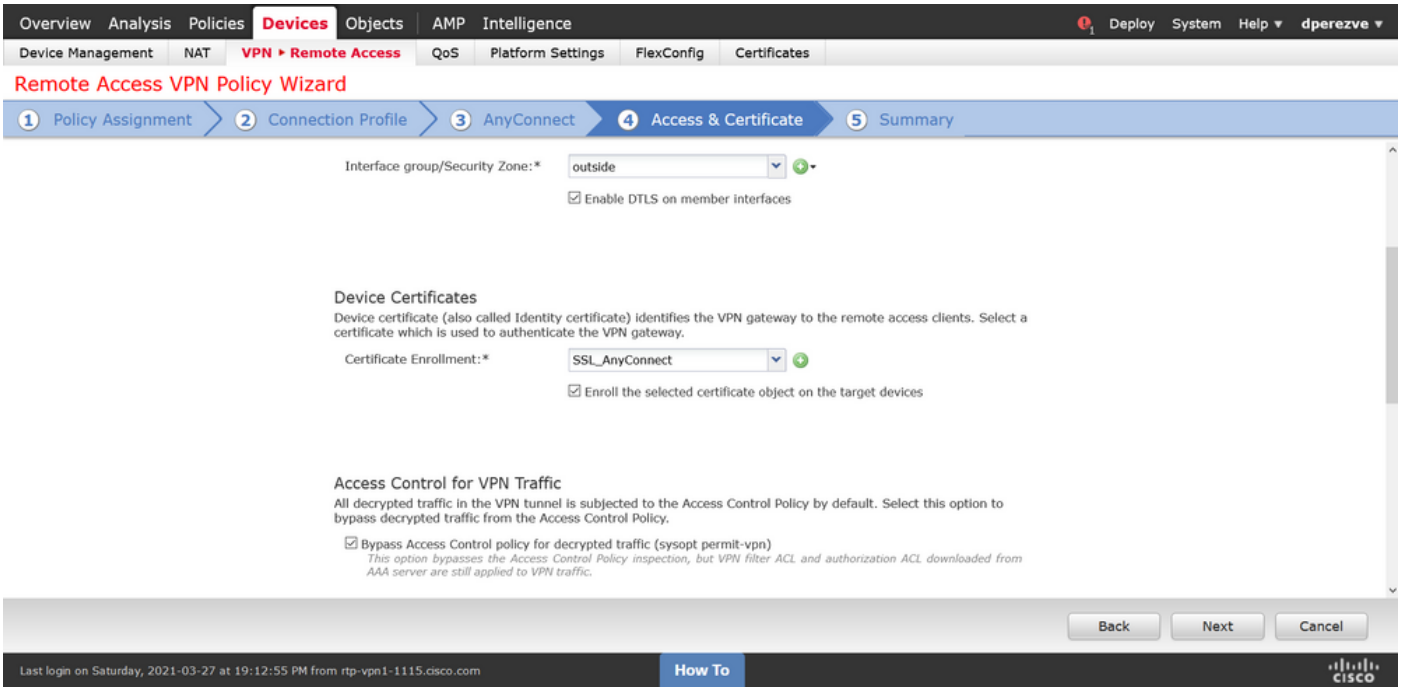
Selecteer op **AnyConnect** het **AnyConnect File Object** op het eindpunt in overeenstemming met het besturingssysteem.



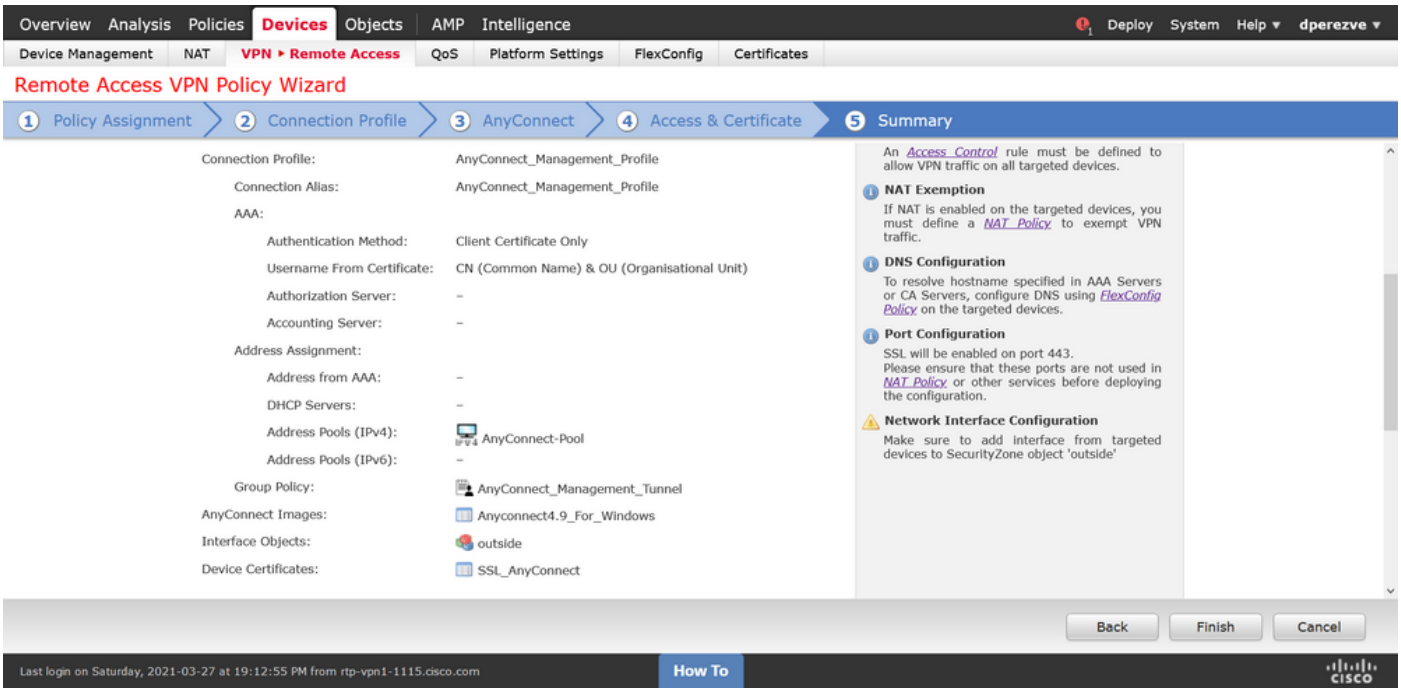
Specificeer op **Access & Certificate** dat door de FTD moet worden gebruikt om zijn identiteit aan de Windows-client te controleren.

> **Opmerking:** Aangezien gebruikers geen contact moeten opnemen met AnyConnect-app wanneer ze de functie Management VPN gebruiken, moet het certificaat volledig worden vertrouwd en mag u geen waarschuwingsbericht afdrukken.

> **Opmerking:** Om fouten in de validering van certificaten te voorkomen, moet het veld Gemeenschappelijke Naam (GN) dat in de Onderwerp Naam van het certificaat is opgenomen, overeenkomen met de FQDN die is gedefinieerd in de lijst van XML-profielen van de server (Stap 1 en Stap 2).



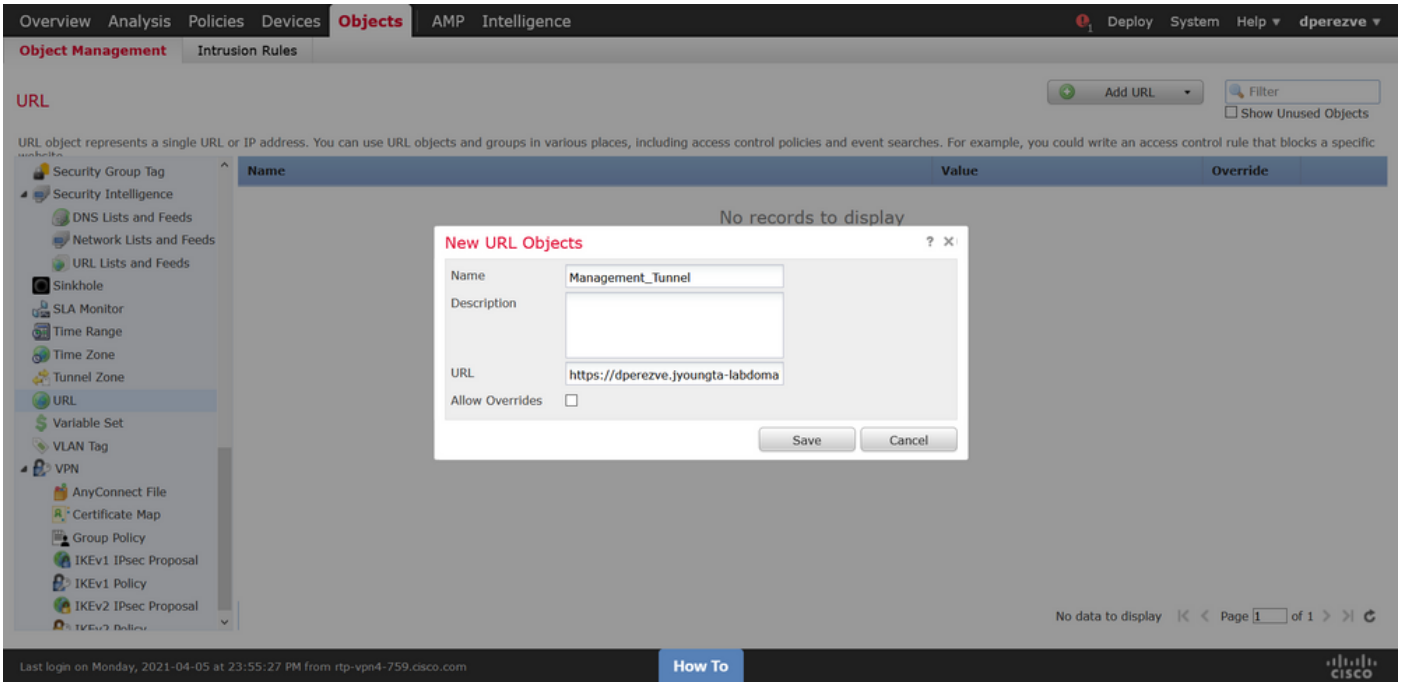
Tenslotte selecteert u de knop **Voltooien** in het **tabblad Samenvatting** om de nieuwe AnyConnect-configuratie toe te voegen.



Stap 6. URL-object maken

Navigeer aan **Exemplaar > Objectbeheer** en selecteer **URL** uit de inhoudsopgave. Selecteer vervolgens **Object toevoegen** in de vervolgkeuzelijst **URL** toevoegen.

Geef een naam voor het object op en definieer de URL met behulp van dezelfde FQDN/gebruikersgroep die in de Lijst van VPN-profiel van beheer is gespecificeerd (Stap 2). In dit voorbeeld moet URL dperezve.jyoungta-labdomain.cisco.com/AnyConnect_Management_Tunnel zijn.



Sla de wijzigingen op om het object aan de lijst toe te voegen.

Stap 7. Bepaal URL-alias

Om de URL-alias in de AnyConnect-configuratie in te schakelen, navigeert u op **Apparaten > VPN > Externe toegang** en klikt u op het potlood-pictogram om te bewerken.

Vervolgens selecteert u op het tabblad **Connection Profile** de configuratie in uw hand, navigeer naar **Aliases**, klik op **Add** en selecteer u het **URL-object** in de **lijst URL Alias.** Zorg ervoor dat het aankruisvakje Ingeschakeld is geselecteerd.

Wijzigingen opslaan en configuraties op FTD implementeren.

Verifiëren

Nadat de implementatie is voltooid, is er een eerste handmatige AnyConnect-verbinding met het AnyConnect VPN-profiel nodig. Tijdens deze verbinding wordt het VPN-profiel van het beheer gedownload van FTD en opgeslagen in **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun**. Vanaf dit punt moeten de volgende verbindingen via het VPN-profiel van het beheer zonder enige gebruikersinteractie worden geïnitieerd.

Problemen oplossen

Voor fouten in certificatie:

- Zorg ervoor dat het basiscertificaat voor de certificeringsinstantie (CA) op het FTD is geïnstalleerd.
- Zorg ervoor dat een identiteitsbewijs dat is ondertekend door dezelfde CA is geïnstalleerd in Windows Machine Store.
- Zorg ervoor dat het GN-veld in het certificaat is opgenomen en hetzelfde is als de FQDN die is gedefinieerd in de serverlijst van het VPN-profiel van het beheer en FQDN die is gedefinieerd in URL-alias.

Voor niet geïnitieerde beheertunnel:

- Zorg ervoor dat het VPN-profiel van het beheer is gedownload en opgeslagen in **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun**.
- Zorg ervoor dat de naam voor het VPN-profiel van het beheer is **VPNMgmtTunProfile.xml**.

Voor aansluitingsproblemen verzamelt u DART-bundel en neemt u contact op met Cisco TAC voor verder onderzoek.