Migreer Paloalto naar Firepower Threat Defence met FMT

Inhoud

Inleiding

Voorwaarden

- Vereisten
- Gebruikte componenten
- Overzicht

Achtergrondinformatie

- Aanvragen PaloAlto Firewall Configuration zip-bestand
- Checklist vóór migratie

Configureren

- Migratiestappen

Problemen oplossen

- Problemen oplossen met Secure Firewall-migratietool
  - Veelvoorkomende migratieproblemen:
  - De ondersteuningsbundel gebruiken voor probleemoplossing:

Inleiding

In dit document wordt de procedure beschreven om Palosalto Firewall te migreren naar Cisco Firepower Threat Device.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Firepower-migratietool
- Paloalto-firewall
- Secure Firewall Threat Defence (FTD)
- Cisco Secure Firewall Management Center (FMC)

Gebruikte componenten

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

- Mac OS met Firepower Migration Tool (FMT) v7.7
- PAN NGFW versie 8.0+
- Secure Firewall Management Center (FMCv) v7.6
- Secure Firewall Threat Defense versie 7.4.2

Vrijwaring: De netwerken en IP-adressen waarnaar in dit document wordt verwezen, zijn niet gekoppeld aan individuele gebruikers, groepen of organisaties. Deze configuratie is exclusief gemaakt voor gebruik in een laboratoriumomgeving.

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.

Overzicht

Specifieke eisen voor dit document zijn onder meer:

- PAN NGFW versie 8.4+ of hoger
- Secure Firewall Management Center (FMCv) versie 6.2.3 of hoger

De Firewall Migration Tool ondersteunt deze lijst met apparaten:

- Cisco ASA (8,4+)
- Cisco ASA (9.2.2+) met FPS
- Cisco Secure Firewall-apparaatbeheer (7.2+)
- Controlepunt (r75-r77)
- Controlepunt (r80-r81)
- Fortinet (5,0+)
- Palo Alto Networks (8.0+)

Achtergrondinformatie

Voordat u uw Paloalto Firewall configuratie migreert, voer deze activiteiten uit:

Aanvragen PaloAlto Firewall Configuration zip-bestand

- Paloalto Firewall moet versie 8.4+ zijn.
- Exporteer de huidige actieve configuratie vanuit de Palo Alto firewall (*.xml moet in xml Format zijn).
- Log in op de Paloalto Firewall-client om de routebeschrijving te tonen en de output in de txt-indeling op te slaan (*.txt).
- Comprimeer het actieve configuratiebestand (*.xml) en het Routing-bestand (*.txt) met de extensie *.zip.

Checklist vóór migratie

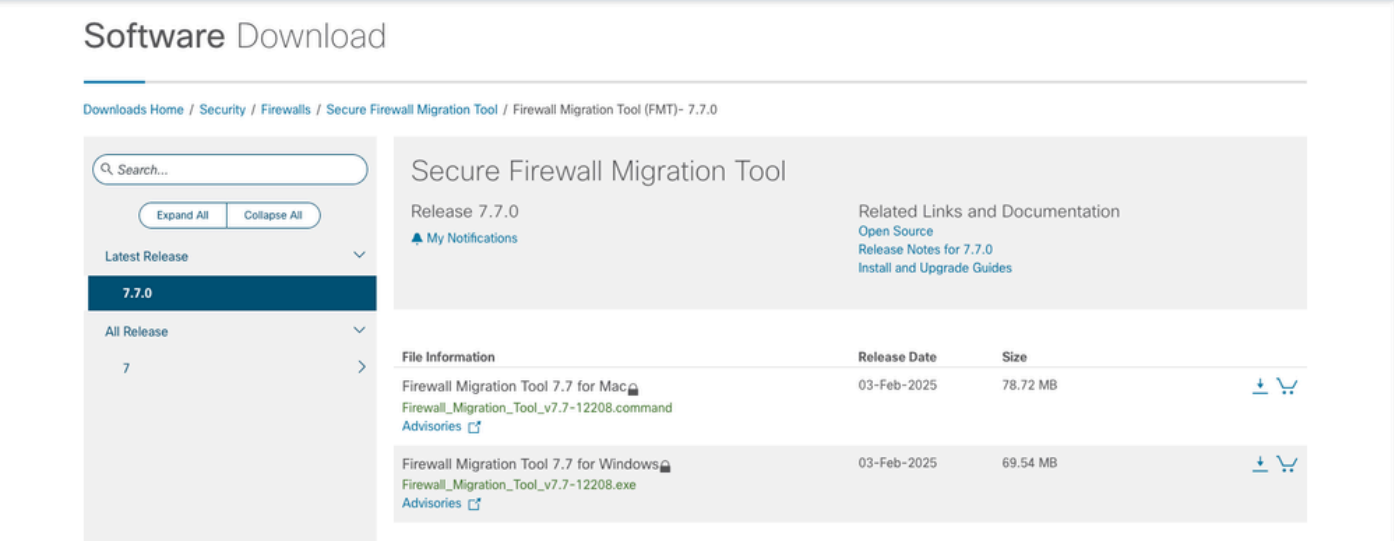
- Ervoor zorgen dat het FTD bij het VCC is geregistreerd voordat het migratieproces begint.
- Er is een nieuwe gebruikersaccount met administratieve rechten aangemaakt op het VCC. Of er kunnen bestaande Admin-referenties worden gebruikt.

- Uitgevoerde Palo Alto lopende configuratie file.xml moet worden gezipt met een extensie van .zip (volg de procedure vermeld in vorige sectie).
- Het FirePOWER-apparaat moet hetzelfde of meer fysieke of subinterface- of poortkanalen hebben in vergelijking met de Paloalto Firewall-interfaces.

Configureren

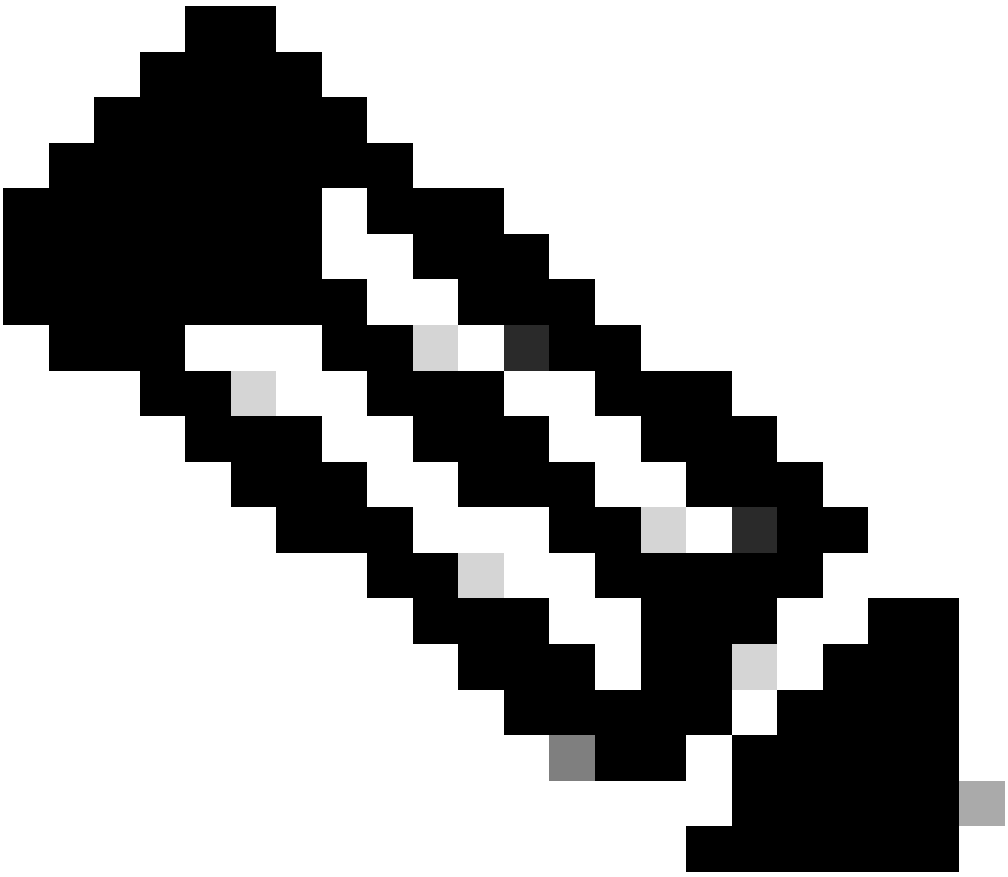
Migratiestappen

1. Download de meest recente Firepower Migration Tool van Cisco Software Central die compatibel is met uw computer:



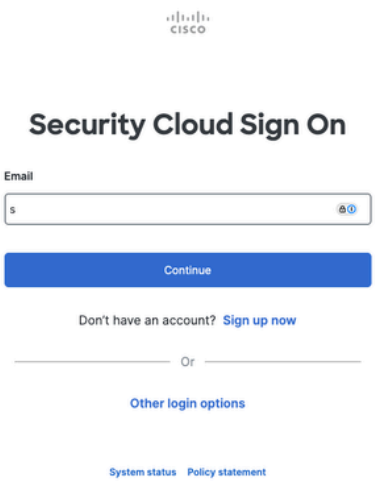
FMT-download

3. Open het bestand dat u eerder naar uw computer hebt gedownload.



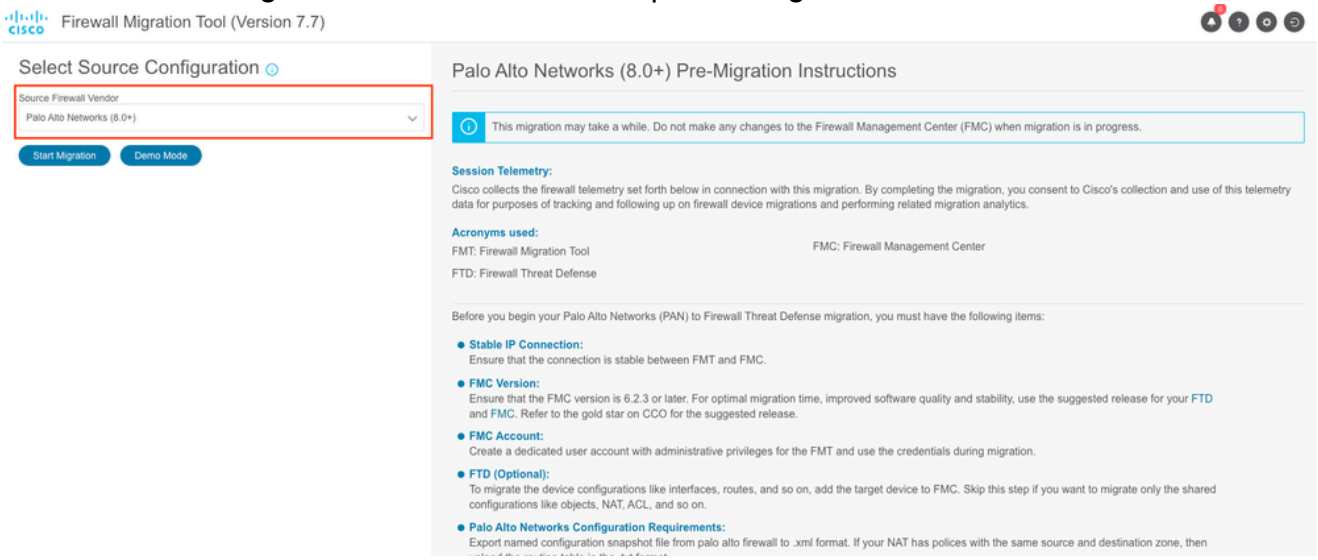
Opmerking: Het programma wordt automatisch geopend en een console-auto genereert inhoud in de map waarin u het bestand hebt uitgevoerd.

4. Nadat u het programma hebt uitgevoerd, opent het een webbrowser die de Gebruiksrechtovereenkomst weergeeft.
    1. Selecteer het aankruisvakje om de voorwaarden te aanvaarden.
    2. Klik op Doorgaan.
5. Log in met een geldige CCO-referenties om toegang te krijgen tot FMT GUI.



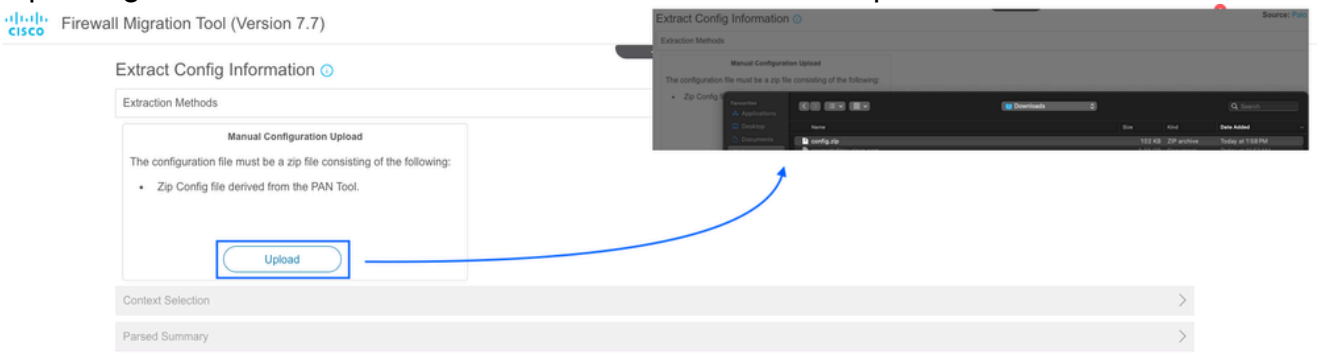
Aanvraag voor FMT-aanmelding

6. Selecteer de te migreren bronfirewall en klik op Start Migration.



FMT GUI

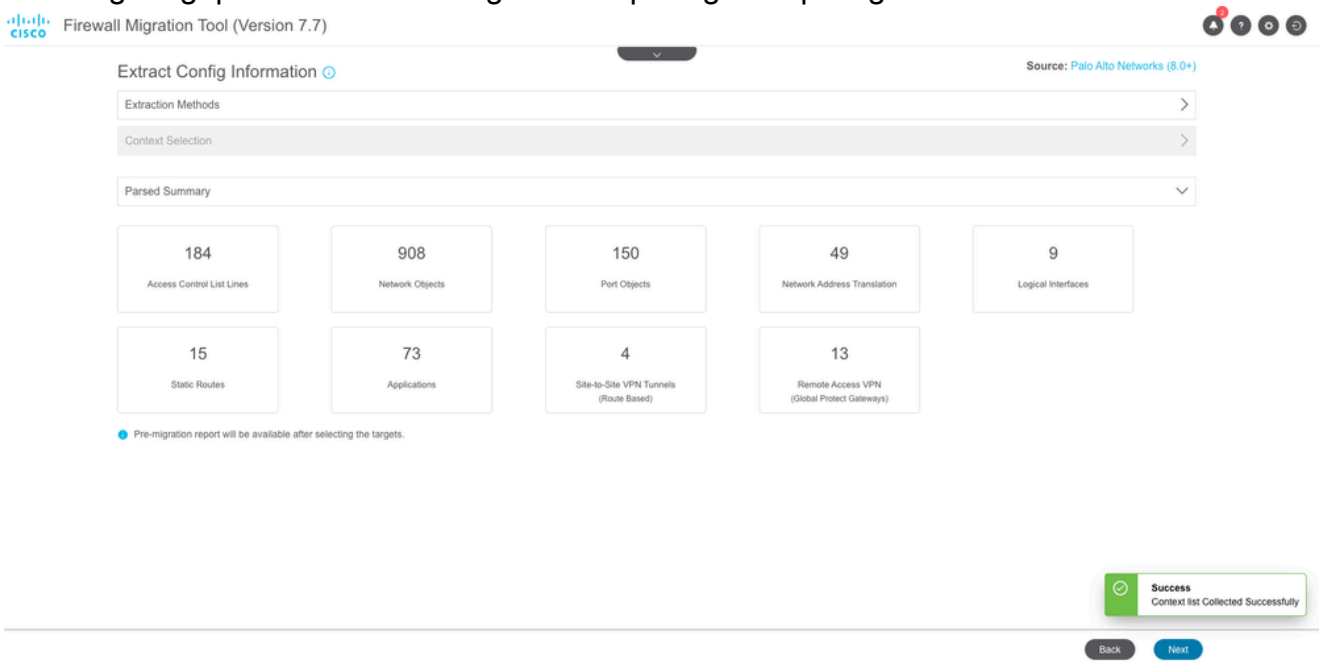
7. De sectie van de Methodes van de extractie wordt nu getoond, waar u het dossier van de Zip configuratie van de Firewall van Paloalto aan FMT moet uploaden.



Wizard Configuratie uploaden

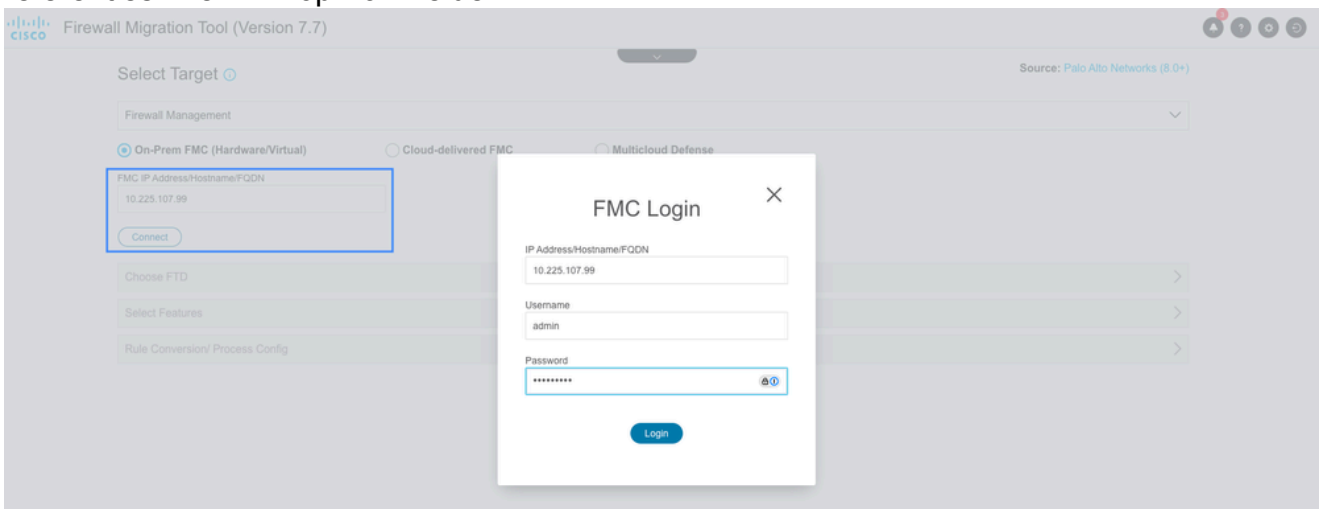
8. De geparste samenvatting van de Configuratie wordt nu weergegeven nadat het configuratiebestand is geüpload. In het geval van VSYS zijn afzonderlijke VSYS-selecties

beschikbaar. Elk van hen moet worden geparseerd en de een na de ander migreren. Bevestig de geparste samenvatting en klik op Volgende pictogram.



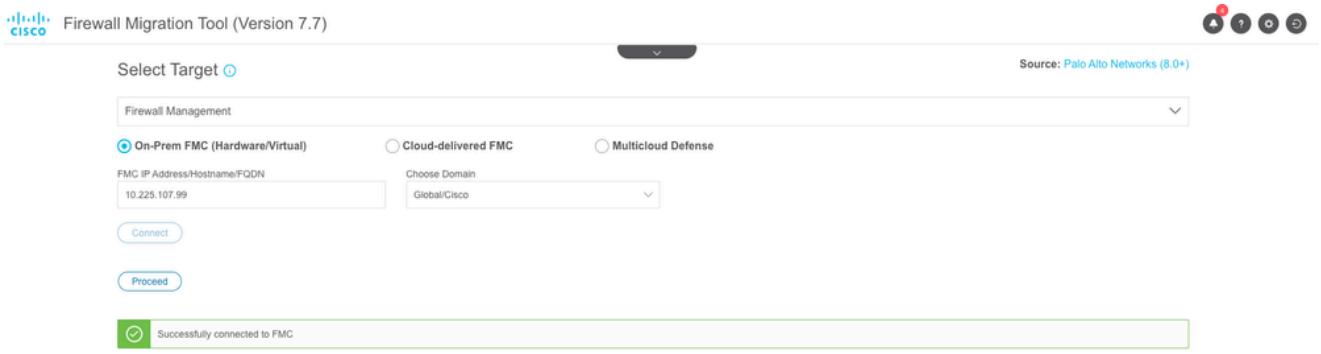
Samenvatting van configuratievalidatie

9. U kunt het type VCC in deze sectie kiezen. Geef het IP-adres voor beheer op en klik op Connect.
   Er wordt een pop-up weergegeven waarin wordt gevraagd om FMC-referenties. Voer de referenties in en klik op Aanmelden.



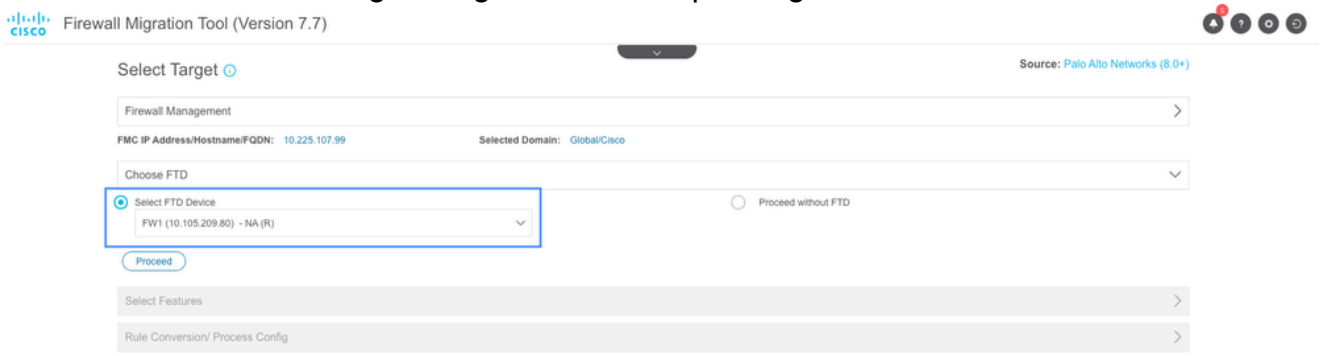
Aanmelden bij FMC

10. Nadat u met succes verbinding hebt gemaakt met FMC, kunt u nu het domein kiezen (indien aanwezig) en op Doorgaan klikken.



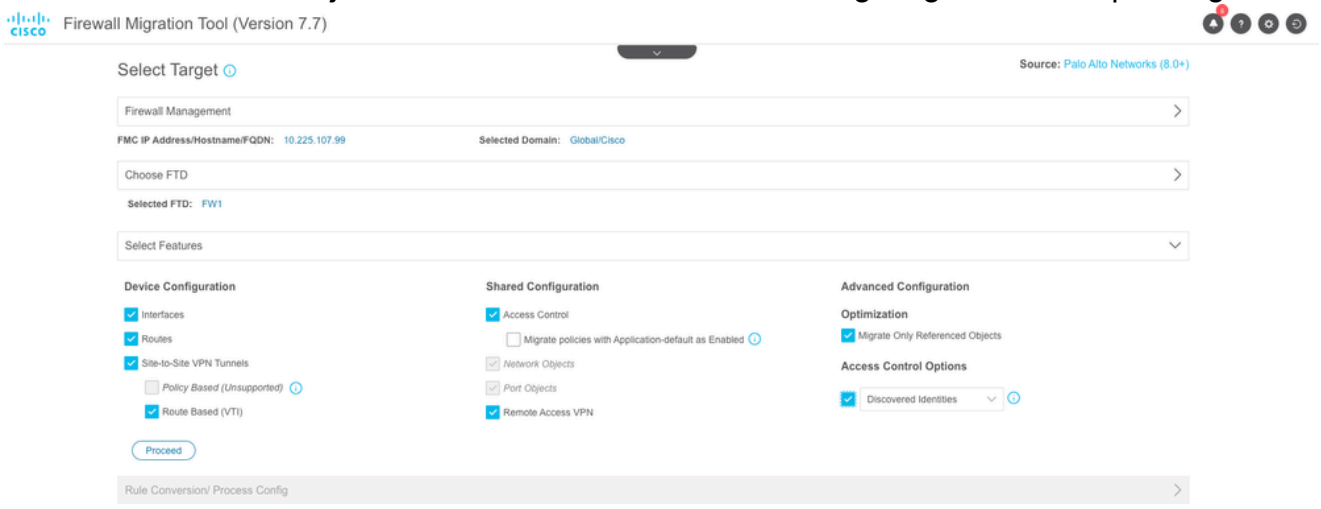
Domeinselectie

11. Kies het FTD waarnaar u gaat migreren en klik op Doorgaan.

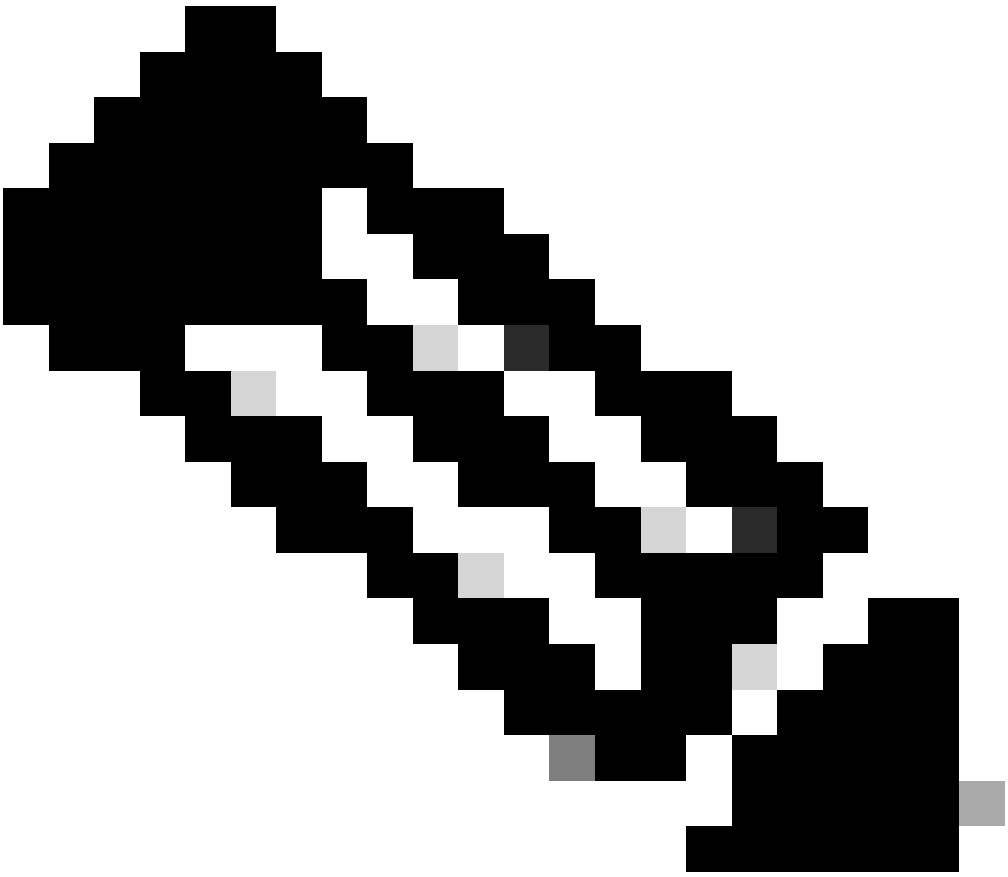


Selecteer Doel FTD

12. De tool maakt nu een lijst van de functies die zullen worden gemigreerd. Klik op Doorgaan.

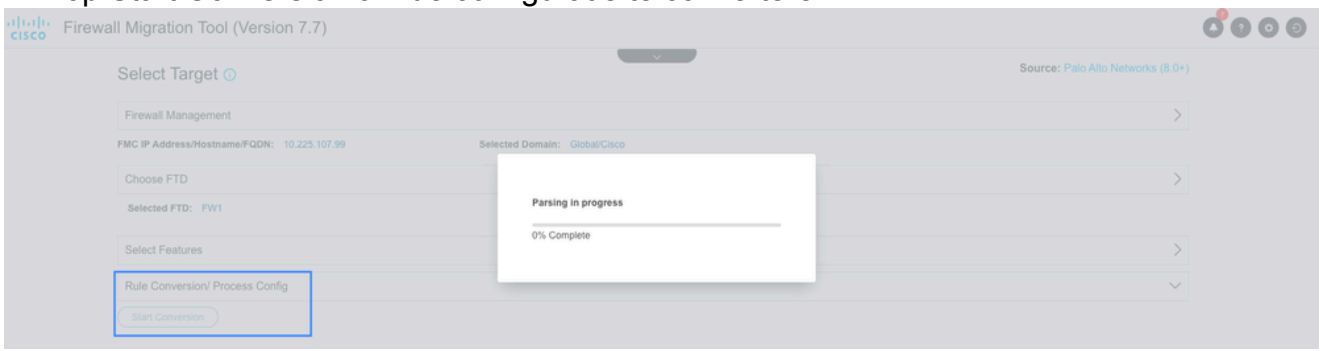


Functieselectie



Opmerking: Alle functies zijn standaard geselecteerd. U kunt elke configuratie die niet gemigreerd hoeft te worden, deselecteren.

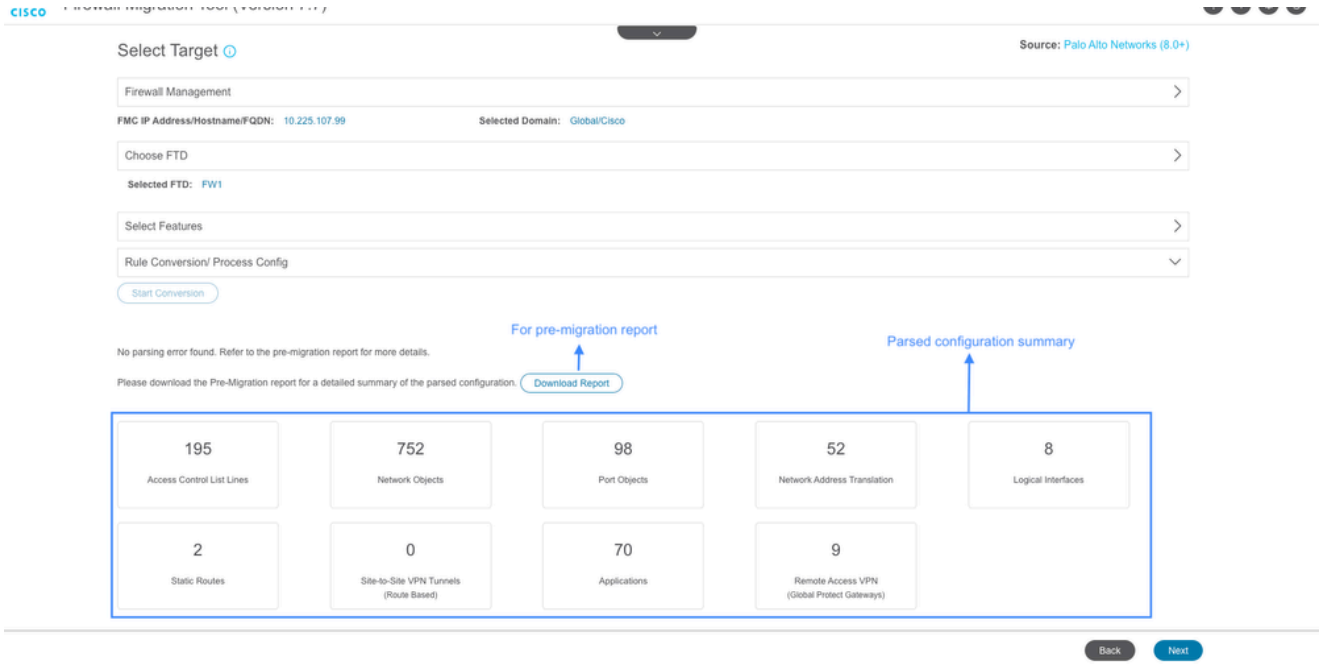
13. Klik op Start Conversion om de configuratie te converteren.



Configuratie parseren

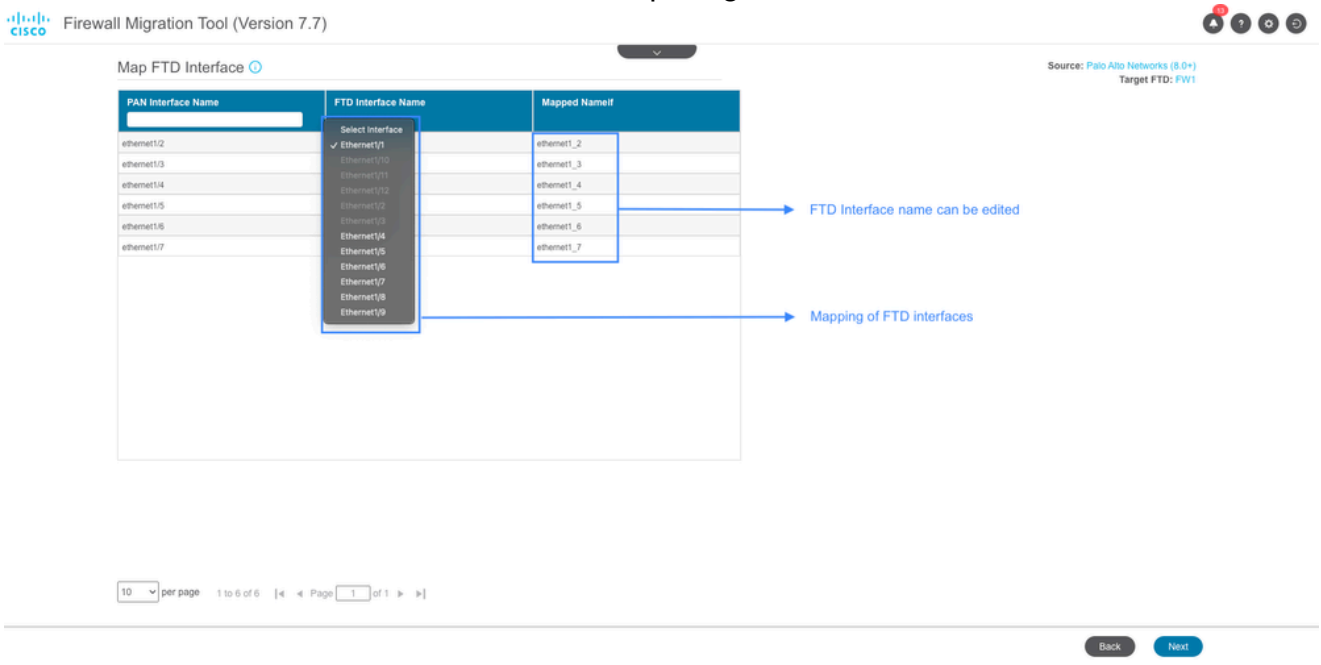
Het gereedschap parseert de configuratie en geeft de conversiesamenvatting weer zoals in de afbeelding. U kunt ook het Pre-Migration Report downloaden voor het valideren van de gemigreerde configuratie voor eventuele fouten of waarschuwingen. Navigeer naar de

volgende pagina door op Volgende te klikken.



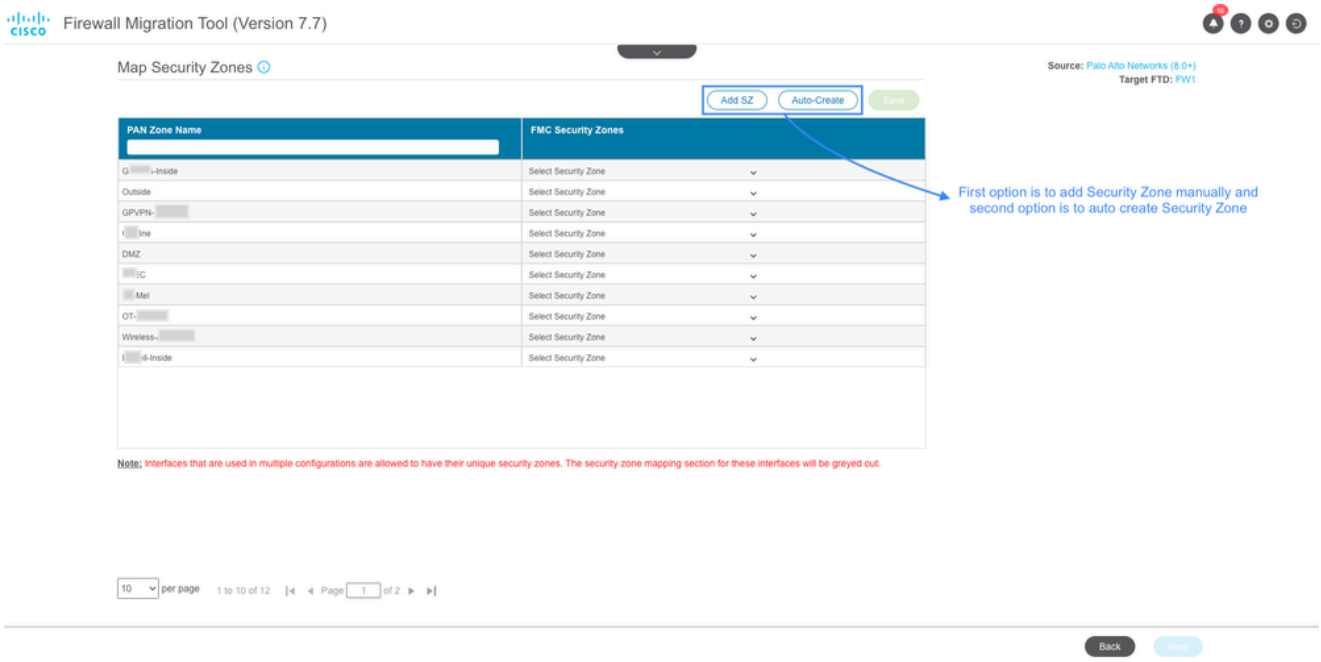
Samenvatting van geparste configuratie

14. U kunt Paloalto-FTD-interfacekaarten definiëren en de interfacenaam voor elke interface bewerken in de sectie Interfacekaarten. Klik op Volgende nadat de interfacekaart is voltooid.



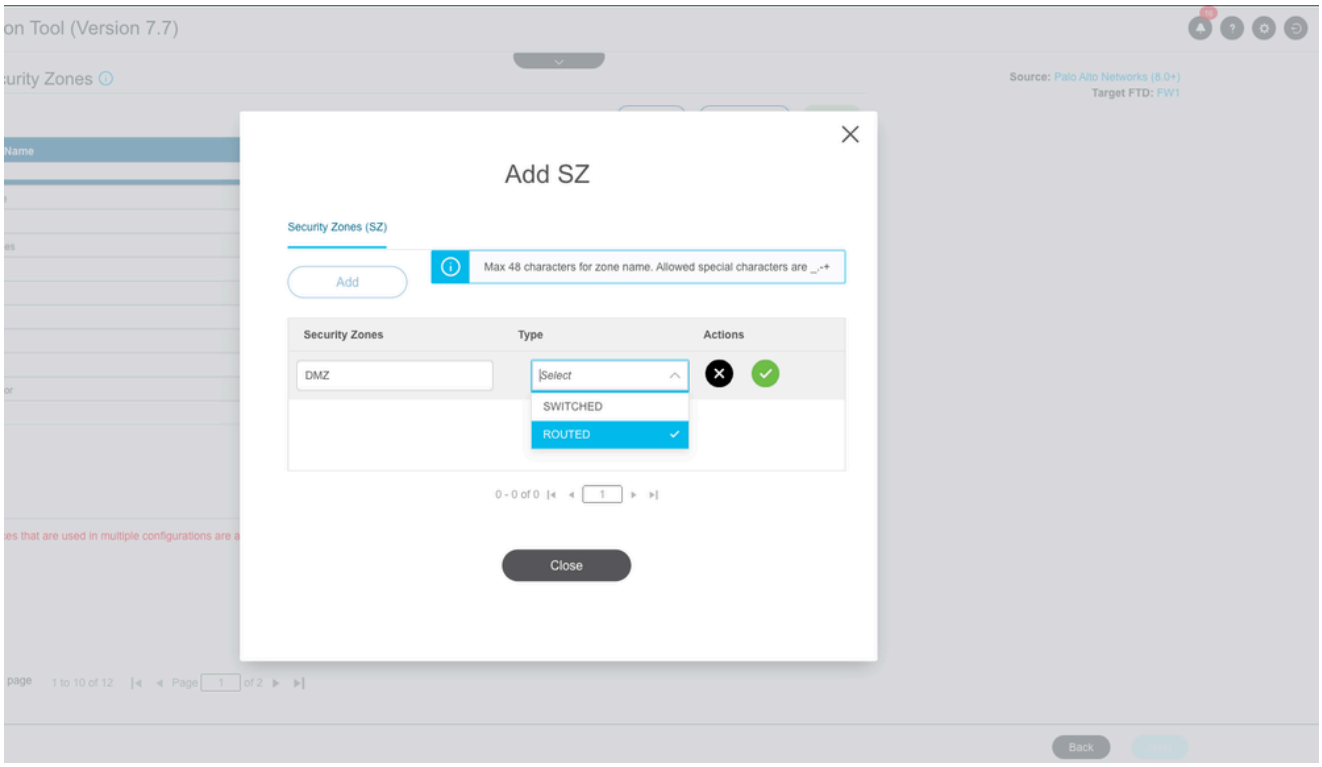
Toewijzing van interfaces

15. U kunt de Security Zone voor elke interface handmatig toevoegen of automatisch maken in Map de Security Zone sectie. Klik op Volgende na het maken en toewijzen van Security Zones.



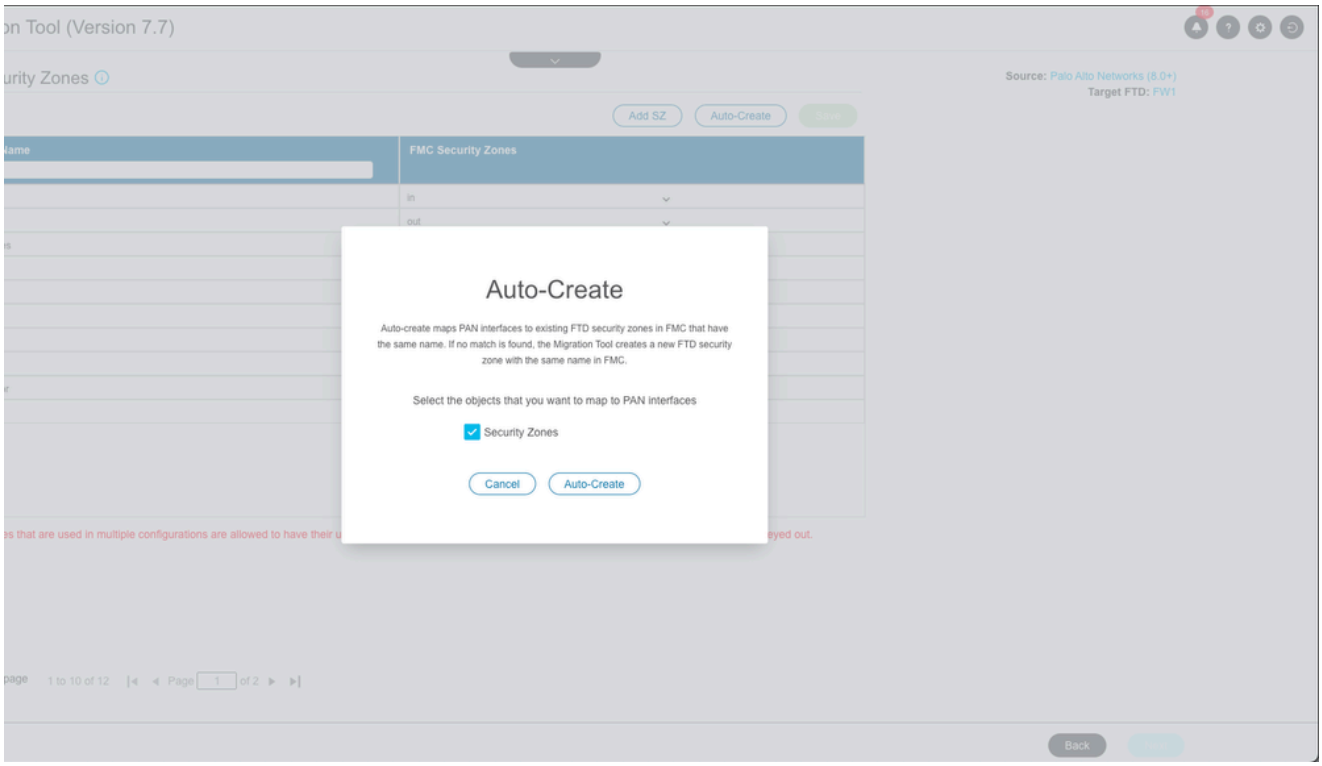
Security zone maken

Handmatige instelling van beveiligingszones:



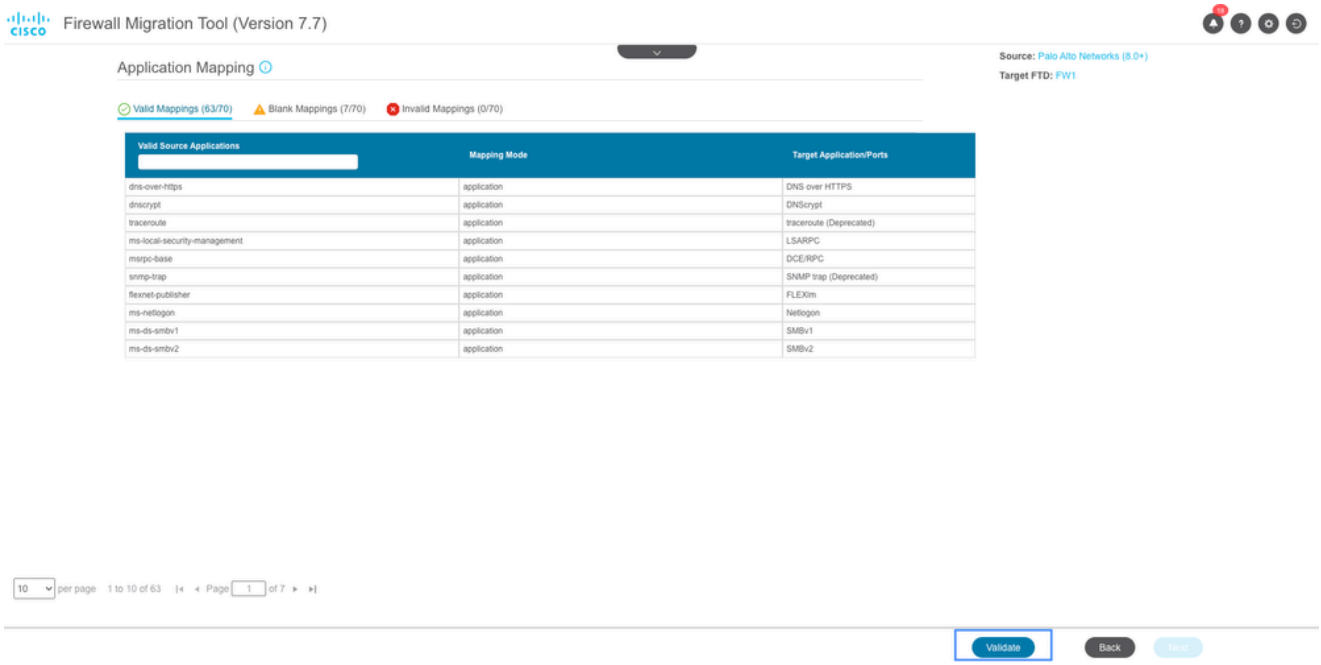
Handmatige security zone maken

Beveiligingszones automatisch maken:

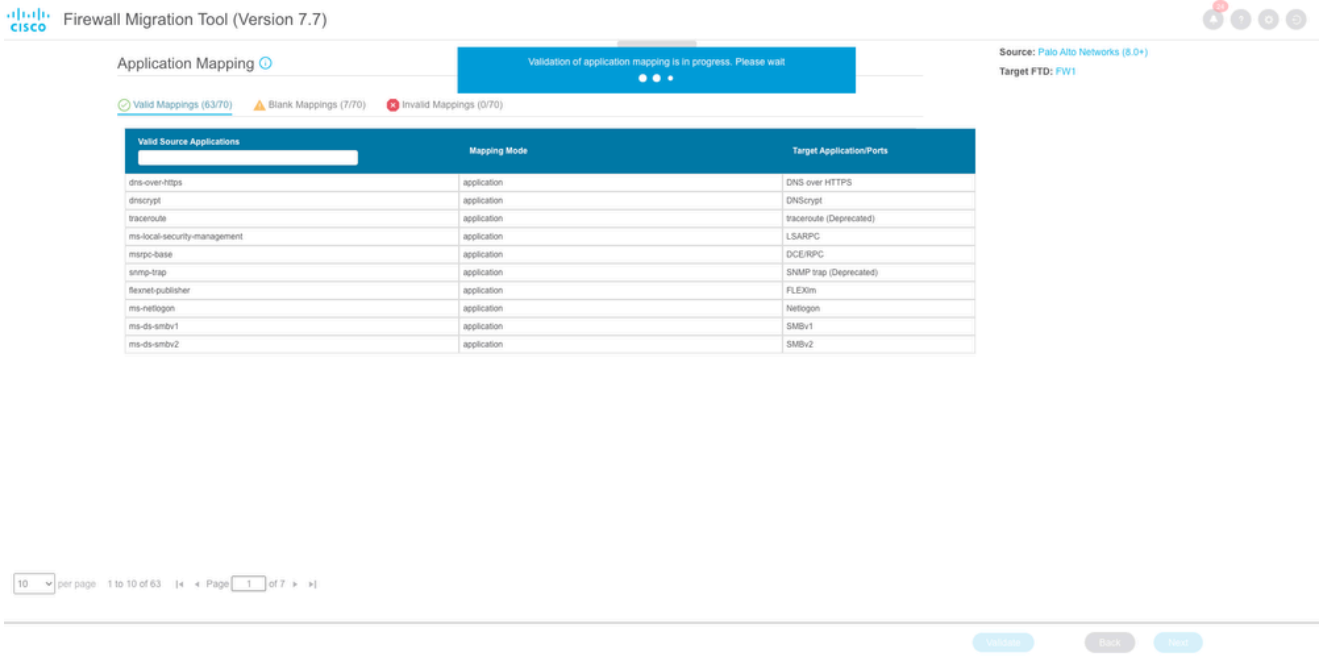


Auto Security Zone maken

16. U kunt nu overgaan naar het gedeelte Toewijzing van toepassingen. Klik op de knop Validate om de applicatie-mapping te valideren.



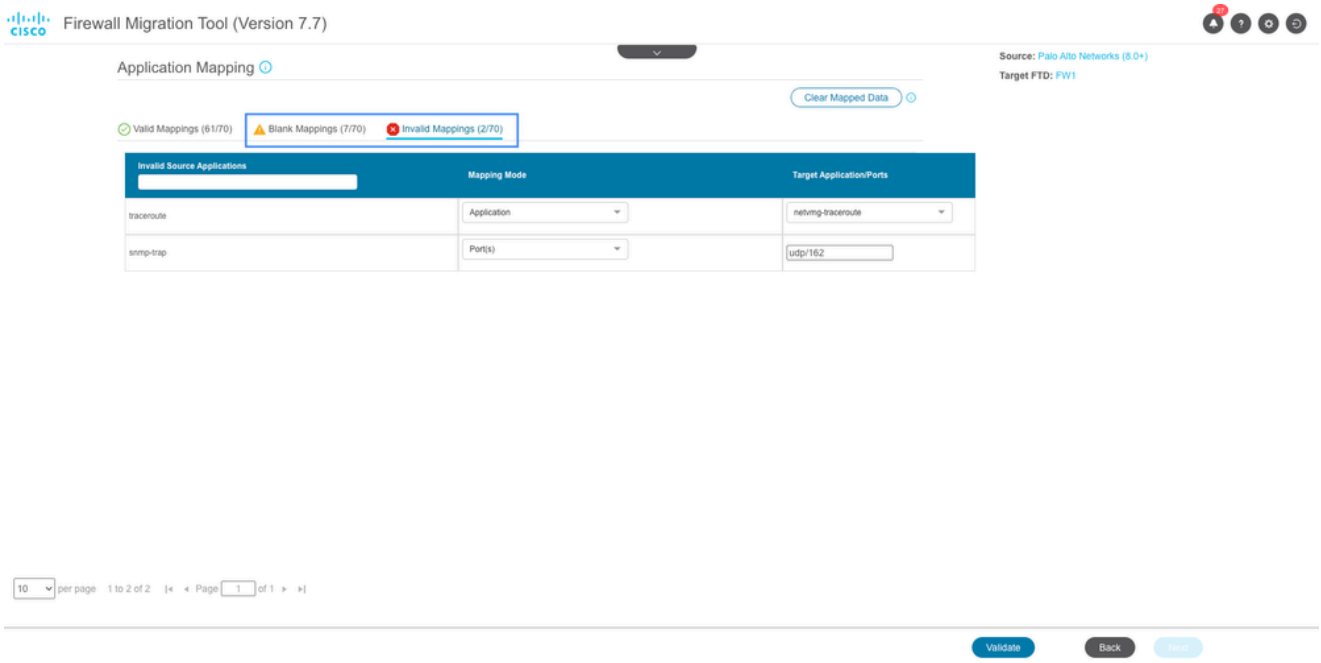
Toewijzing van toepassingen



Validatie van Toewijzing van toepassingen

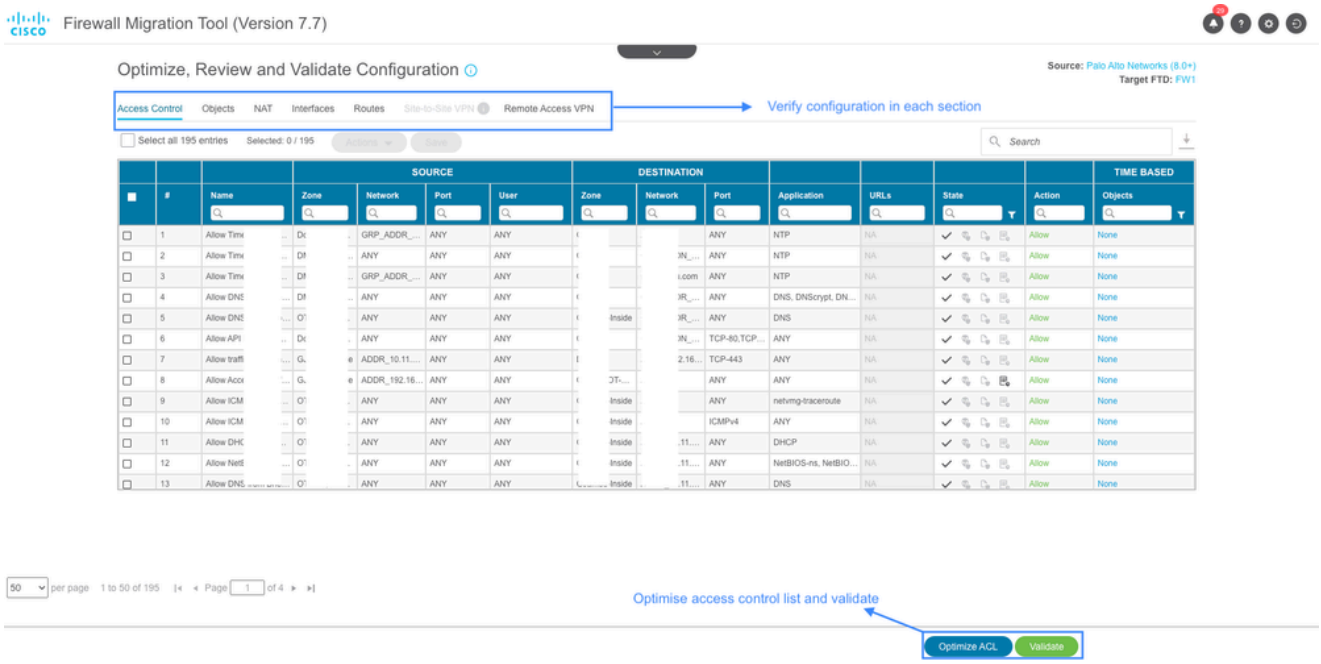
Na validatie vermeldt FMT de lege en ongeldige toewijzingen. Ongeldige toewijzingen moeten worden gecorrigeerd voordat u verder gaat en blancotoewijzingen zijn optioneel.

Klik nogmaals op Valideren om de gecorrigeerde toewijzingen te valideren. Klik op Volgende nadat de validatie is geslaagd.



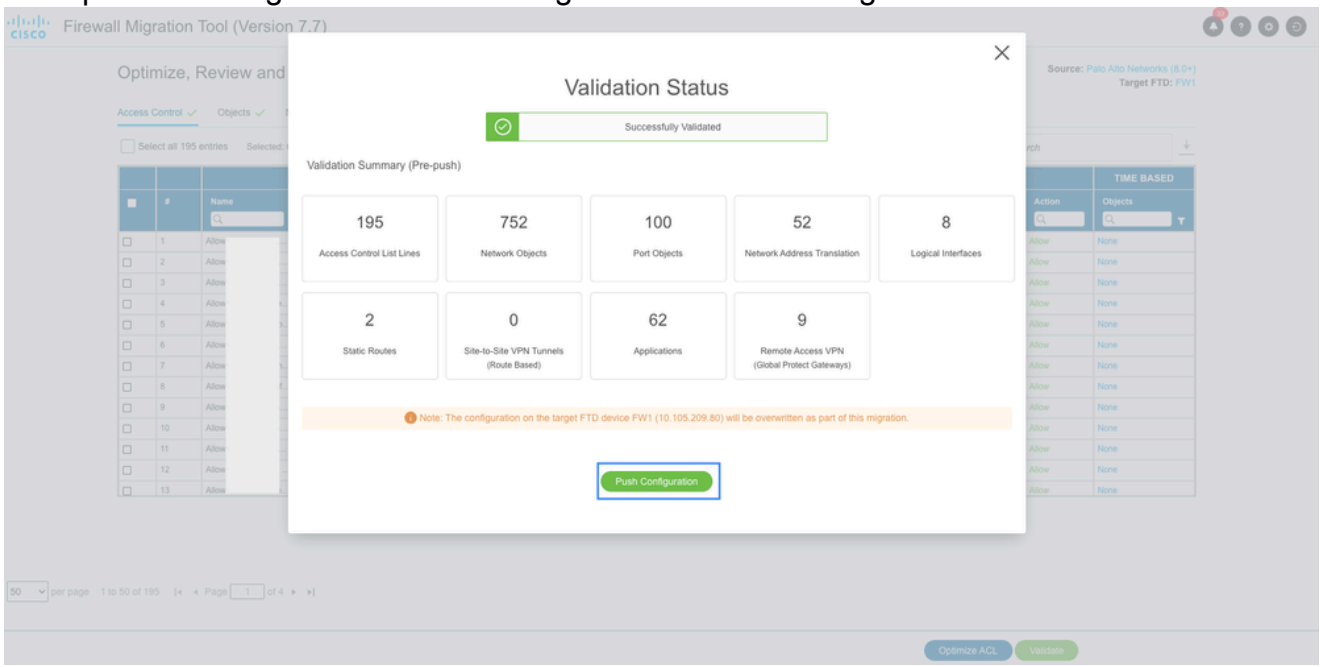
Blind en ongeldig Toewijzing van toepassingen

17. ACL kan indien nodig in de volgende sectie worden geoptimaliseerd. Herzie de configuratie in elke sectie zoals Toegangsbeheer, Voorwerpen, NAT, Interfaces, Routes, en Verre Toegang VPN. Klik op Validate na het bekijken van de configuraties.



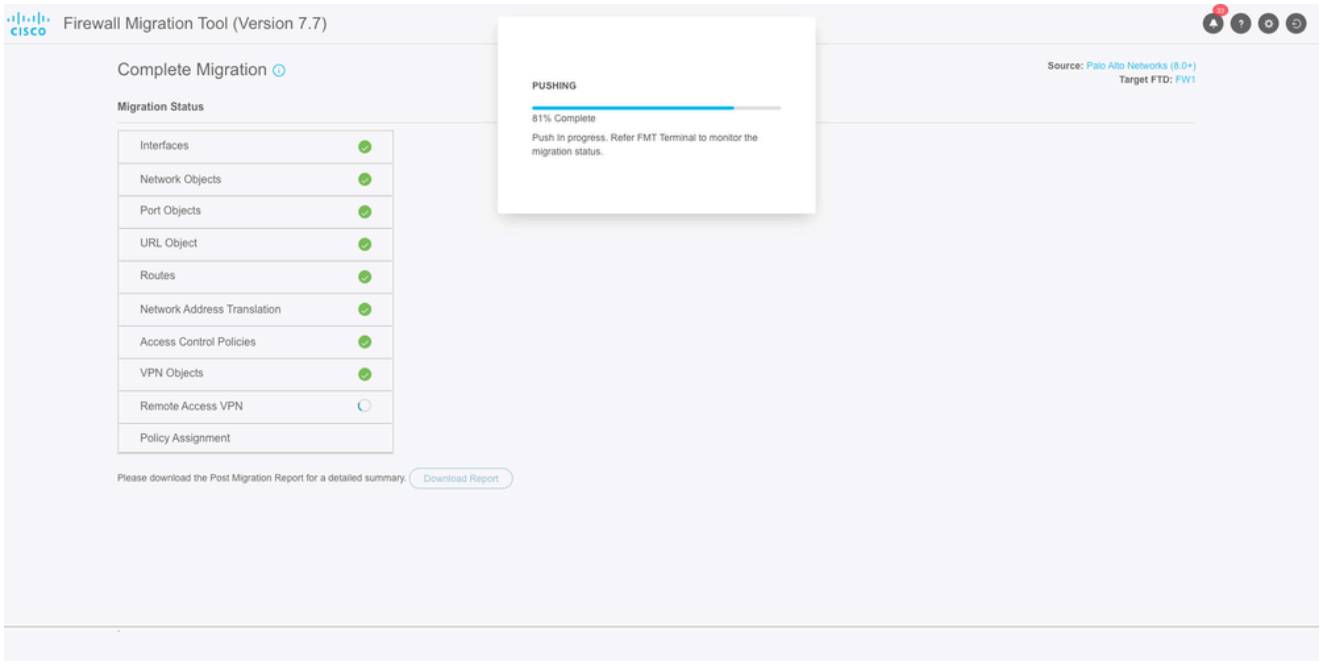
Configuratievalidatie

18. Een valideringssamenvatting wordt weergegeven nadat de validering met succes is voltooid. Klik op Push Configuration om de configuratie naar het beoogde VCC te duwen.



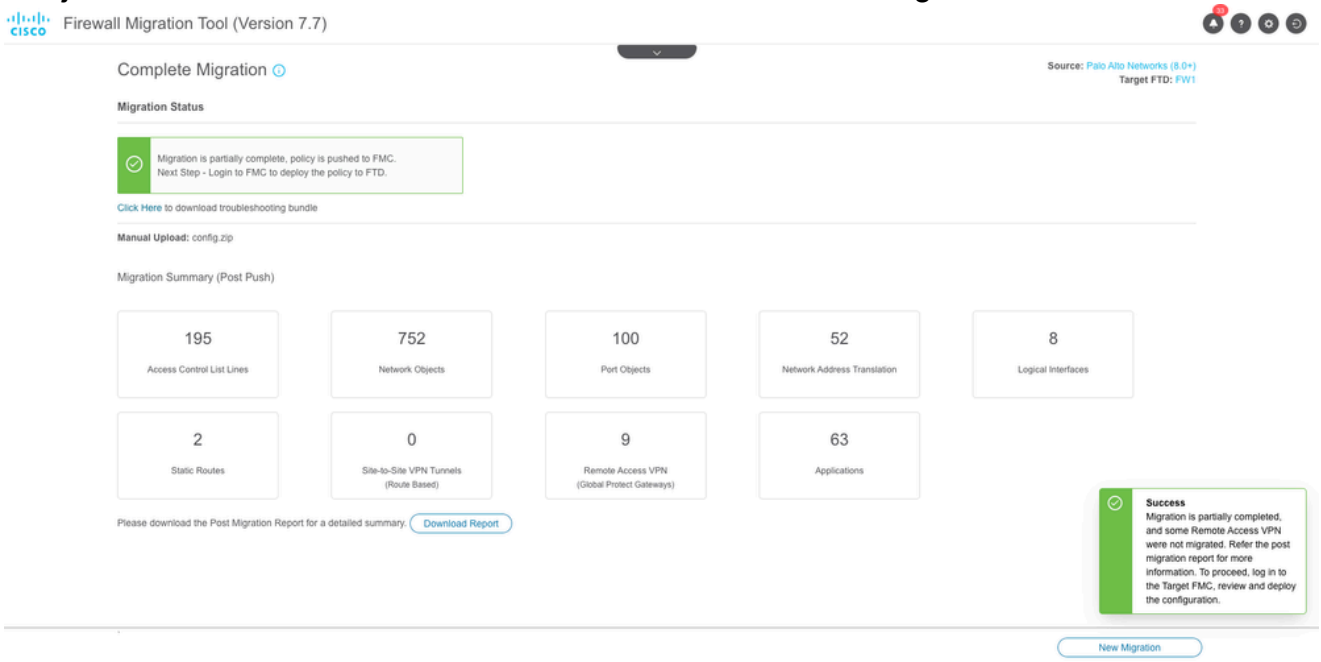
Samenvatting van configuratievalidatie

19. De voortgang van de configuratie van het VCC is nu zichtbaar in de sectie Migratiestatus. U kunt het FMT terminal venster ook gebruiken voor de controle van de migratiestatus.



Migratiestatus

20. Een migratieoverzicht wordt weergegeven door de tool omhoog op succesvolle migratie. Tevens worden eventuele gedeeltelijk gemigreerde configuraties vermeld. Bijvoorbeeld, de configuratie van de Verre toegang VPN in dit scenario toe te schrijven aan het missen Veilig Pakket van de Cliënt.
    U kunt ook het Post Migration Report downloaden om de gemigreerde configuraties te bekijken en om te zien of er fouten of correcties moeten worden gemaakt.



Samenvatting van succesvolle migratie

21. De laatste stap is het bekijken van de gemigreerde configuratie van het VCC en implementeren van de configuratie naar FTD.
    Zo implementeert u de configuratie:
    1. Log in op de GUI van het VCC.
    2. Navigeer naar het tabblad Implementatie.

3. Selecteer de implementatie om de configuratie naar de firewall te duwen.
4. Klik op Implementeren.

Problemen oplossen

Problemen oplossen met Secure Firewall-migratietool

Veelvoorkomende migratieproblemen:

- Onbekende of ongeldige tekens in het configuratiebestand van PaloAlto.
- Ontbrekende of onvolledige configuratie-elementen.
- Problemen met netwerkconnectiviteit of latentie.
- Problemen tijdens het uploaden van het configuratiebestand van PaloAlto of tijdens het indrukken van de configuratie in het VCC.

De ondersteuningsbundel gebruiken voor probleemoplossing:

- Klik in het scherm "Complete Migration" op de knop Support.
- Selecteer Ondersteuningsbundel en kies de configuratiebestanden die u wilt downloaden.
- Log- en DB-bestanden worden standaard geselecteerd.
- Klik op Downloaden om een .zip-bestand te krijgen.
- Haal de .zip om logbestanden, DB en configuratiebestanden te bekijken.
- Klik op E-mail ons om storingsgegevens naar het technische team te sturen.
- Bevestig het ondersteuningsbundel in uw e-mail.
- Klik op Bezoek TAC-pagina om een Cisco TAC-case voor ondersteuning te maken.

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.