Migreer ASA naar Firepower Threat Defence (FTD) met FMT

Inhoud

Inleiding

Dit document beschrijft de procedure om Cisco adaptieve security applicatie (ASA) te migreren naar Cisco Firepower Threat Device.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van Cisco Firewall Threat Defence (FTD) en Adaptieve Security Applicatie (ASA).

Gebruikte componenten

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

- Mac OS met Firepower Migration Tool (FMT) v7.0.1
- Adaptieve security applicatie (ASA) v9.16(1)
- Secure Firewall Management Center (FMCv) v7.4.2
- Secure Firewall Threat Defense Virtual (FTDv) v7.4.1

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:

- Cisco adaptieve security applicatie (ASA) 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)
- Fortinet (5,0+)

· Palo Alto Networks (6.1+)

Achtergrondinformatie

Voordat u uw ASA-configuratie migreert, voert u deze activiteiten uit:

Het ASA-configuratiebestand verkrijgen

Om een ASA apparaat te migreren, gebruik de show in werking stellen-config voor enige context, of toon technologie-steun voor multi-context wijze om de configuratie te verkrijgen, bewaar het als .cfg of .txt dossier, en breng het over naar de computer met het Veilige de migratiehulpmiddel van de Firewall.

PKI-certificaat exporteren vanuit ASA en importeren in beheercentrum

Gebruik deze opdracht om het PKI-certificaat via de CLI uit de bron ASA-configuratie met de sleutels naar een PKCS12-bestand te exporteren:
ASA (config)#crypto kan <trust-point-name> pkcs12 <passphrase> exporteren
Importeer vervolgens het PKI-certificaat in een beheercentrum (Object Management PKI-objecten). Zie PKI-objecten in de configuratiehandleiding van Firepower Management Center voor meer informatie.

AnyConnect-pakketten en -profielen ophalen

AnyConnect-profielen zijn optioneel en kunnen worden geüpload via het beheercentrum of de

Secure Firewall-migratietool.

Gebruik deze opdracht om het vereiste pakket van de bron ASA naar een FTP- of TFTP-server te kopiëren:

Kopieer <locatie bron bestand:/naam bronbestand> <bestemming>

ASA# kopieer disk0:/anyconnect-win-4.10.02086-webimplementation-k9.pkg tftp://1.1.1.1 <----- Voorbeeld van het kopiëren van een AnyConnect-pakket.

ASA# kopieer disk0:/ extern-sso- 4.10.04071-webimplementation-k9.zip tftp://1.1.1.1 <----- Voorbeeld van het kopiëren van externe browser pakket.

ASA# kopieer disk0:/ hostscan_4.10.04071-k9.pkg tftp://1.1.1.1 <----- Voorbeeld van het kopiëren van Hostscan-pakket.

ASA# kopieer disk0:/ dap.xml tftp://1.1.1.1. <----- Voorbeeld van het kopiëren van Dap.xml

ASA# kopieer disk0:/ sdesktop/data.xml tftp://1.1.1.1 <----- voorbeeld van het kopiëren van Data.xml

ASA# kopieer disk0:/ VPN_Profile.xml tftp://1.1.1.1 <----- Voorbeeld van het kopiëren van een AnyConnect-profiel.

Importeer de gedownloade pakketten naar het beheercentrum (Objectbeheer > VPN > AnyConnect File).

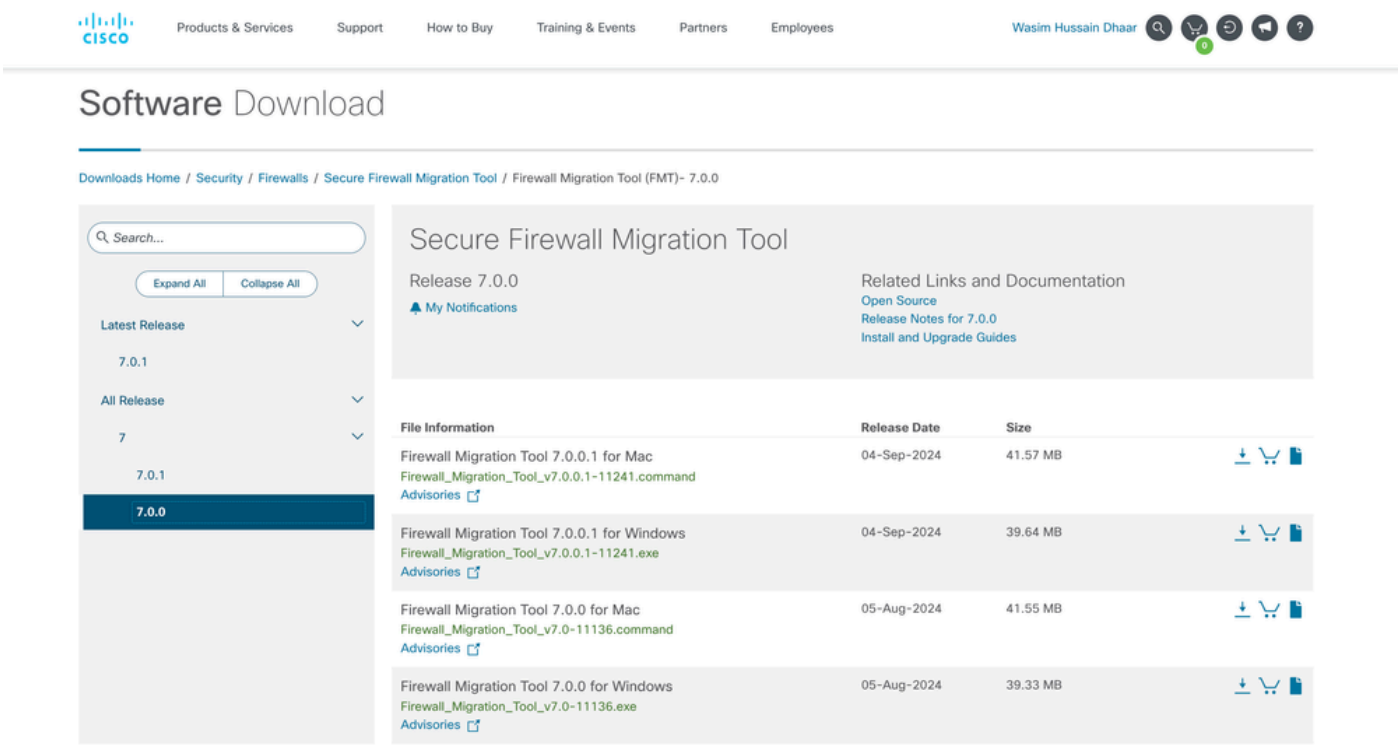
a-Dap.xml en Data.xml moeten naar het beheercentrum worden geüpload vanuit de Secure Firewall-migratietool in het gedeelte Beoordeling en valideren > Externe toegang VPN > AnyConnect File.

De b-AnyConnect-profielen kunnen rechtstreeks naar het beheercentrum worden geüpload of via de Secure Firewall-migratietool in het gedeelte Review and Validate > Remote Access VPN > AnyConnect File.

Configureren

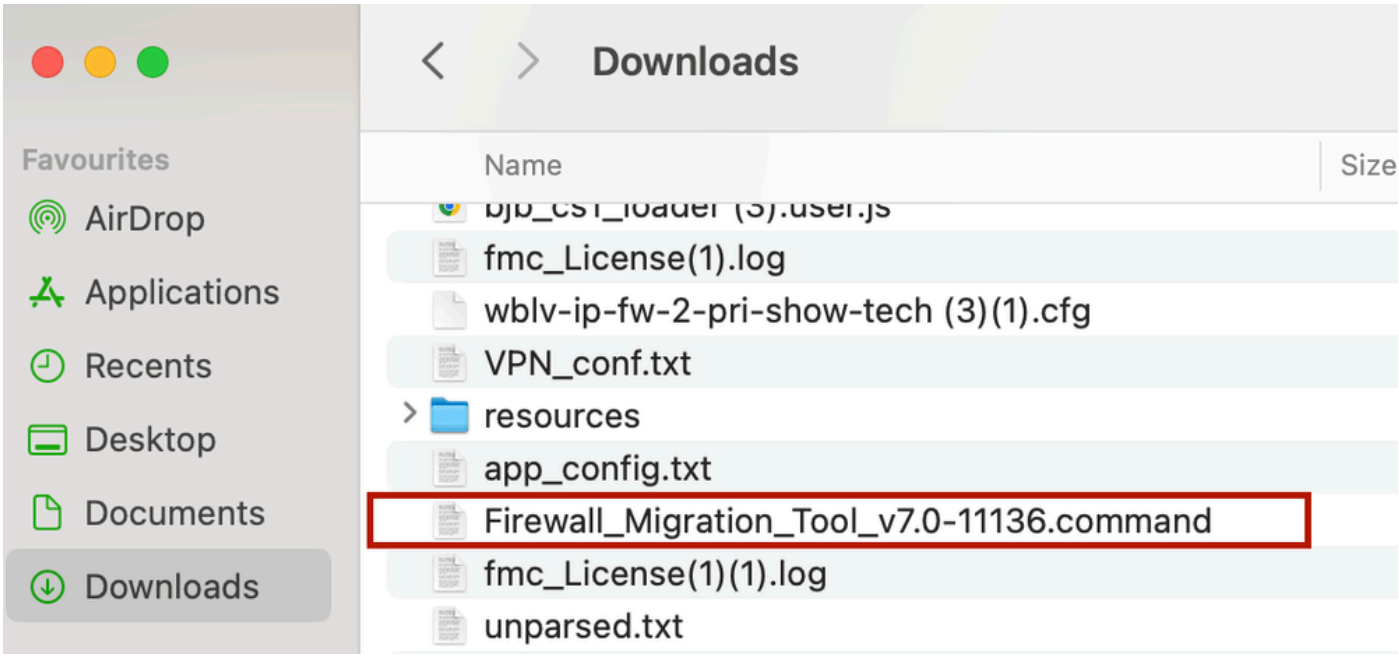
Configuratiestappen :

1.Downloaden het meest recente Firepower Migration Tool van Cisco Software Central:

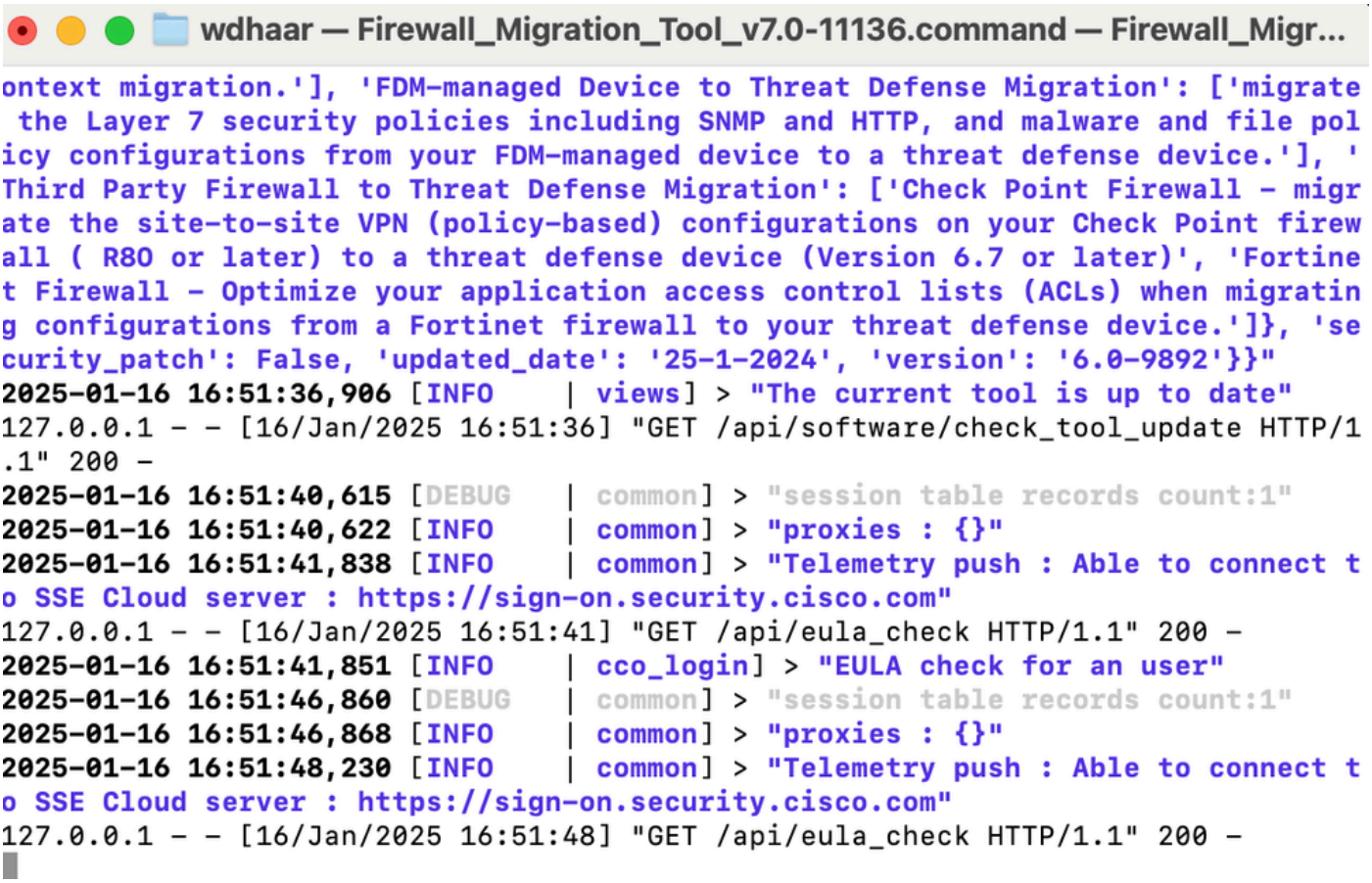


Software downloaden

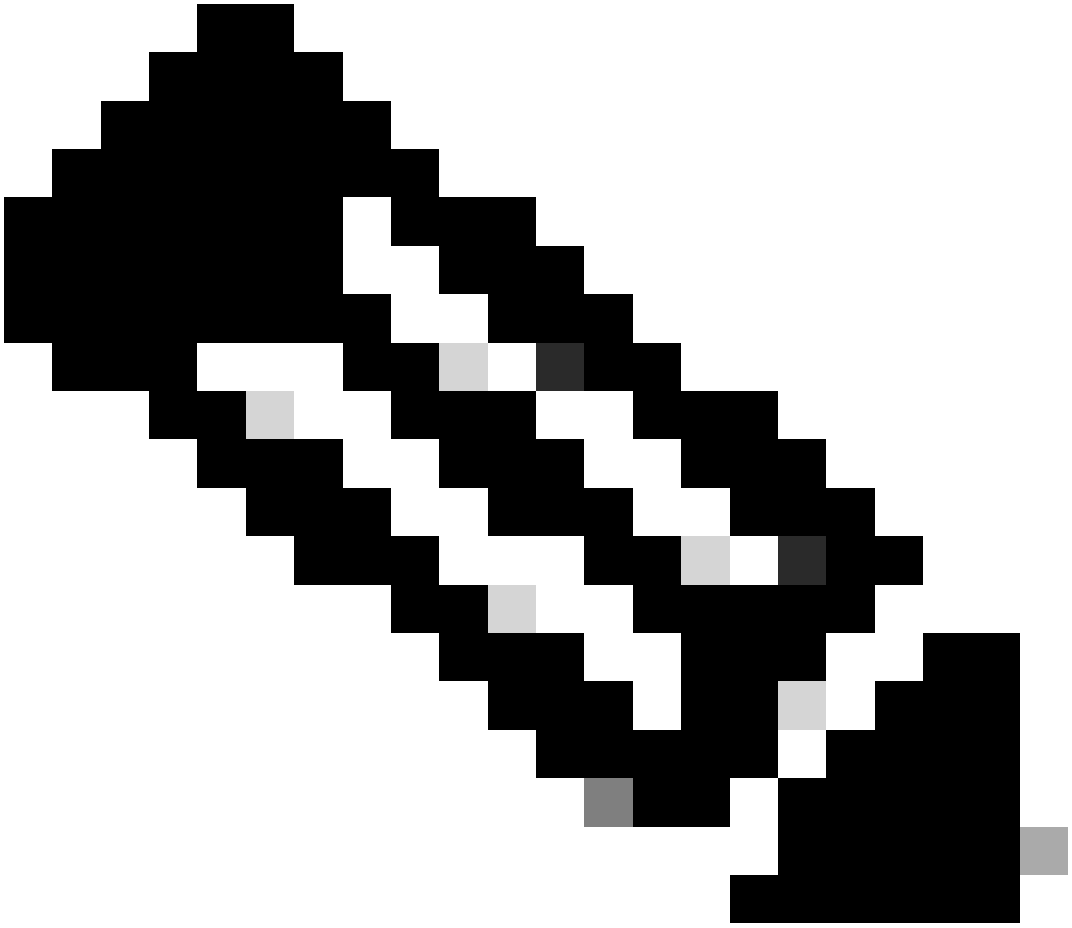
2. Klik op het bestand dat u eerder naar uw computer hebt gedownload.



Het bestand



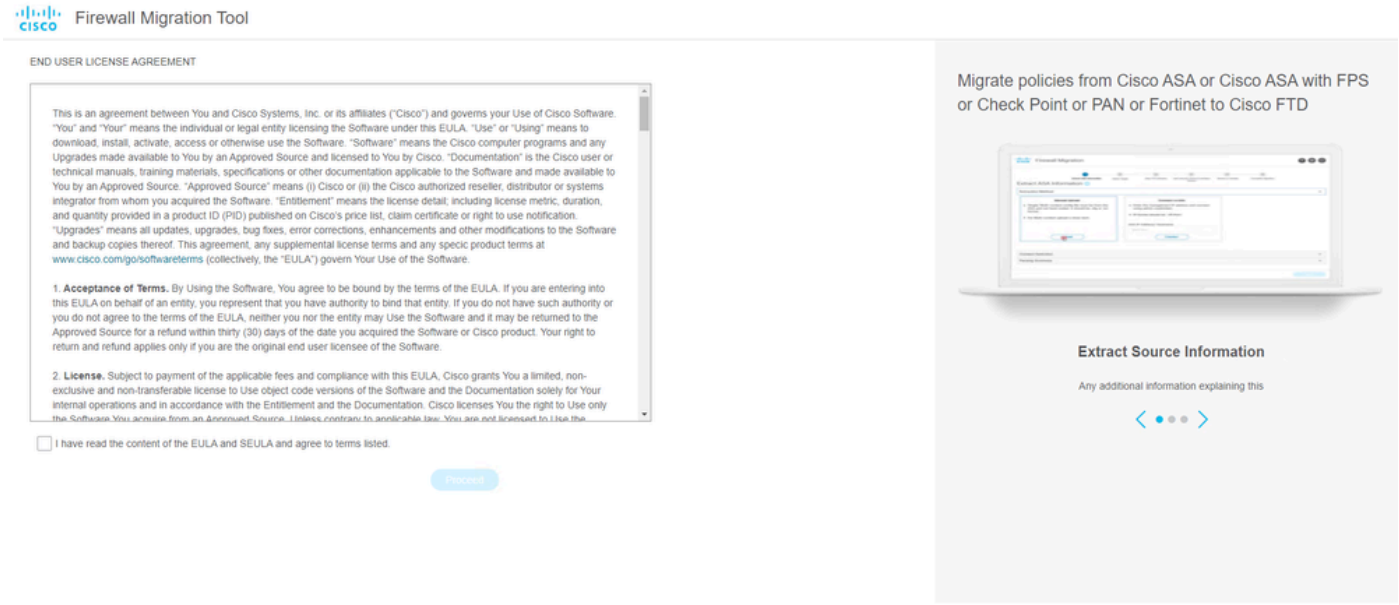
Logboeken voor console



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

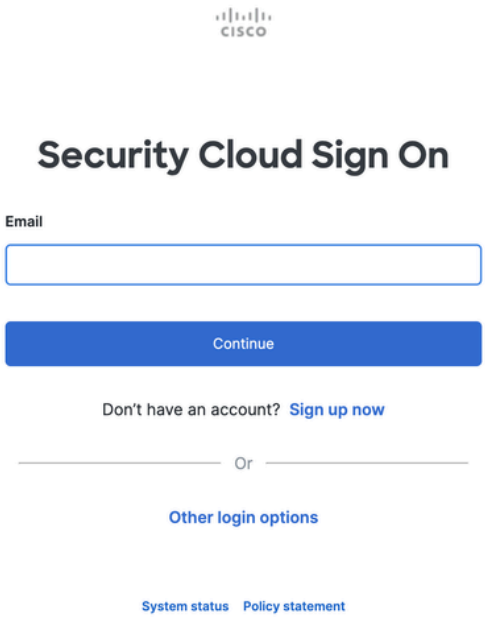
---

3. Nadat u het programma hebt uitgevoerd, wordt er een webbrowser geopend die de 'Gebruiksrechtovereenkomst' weergeeft.
    1. Vink het aanvinkvakje aan om de voorwaarden te aanvaarden.
    2. Klik op Doorgaan.



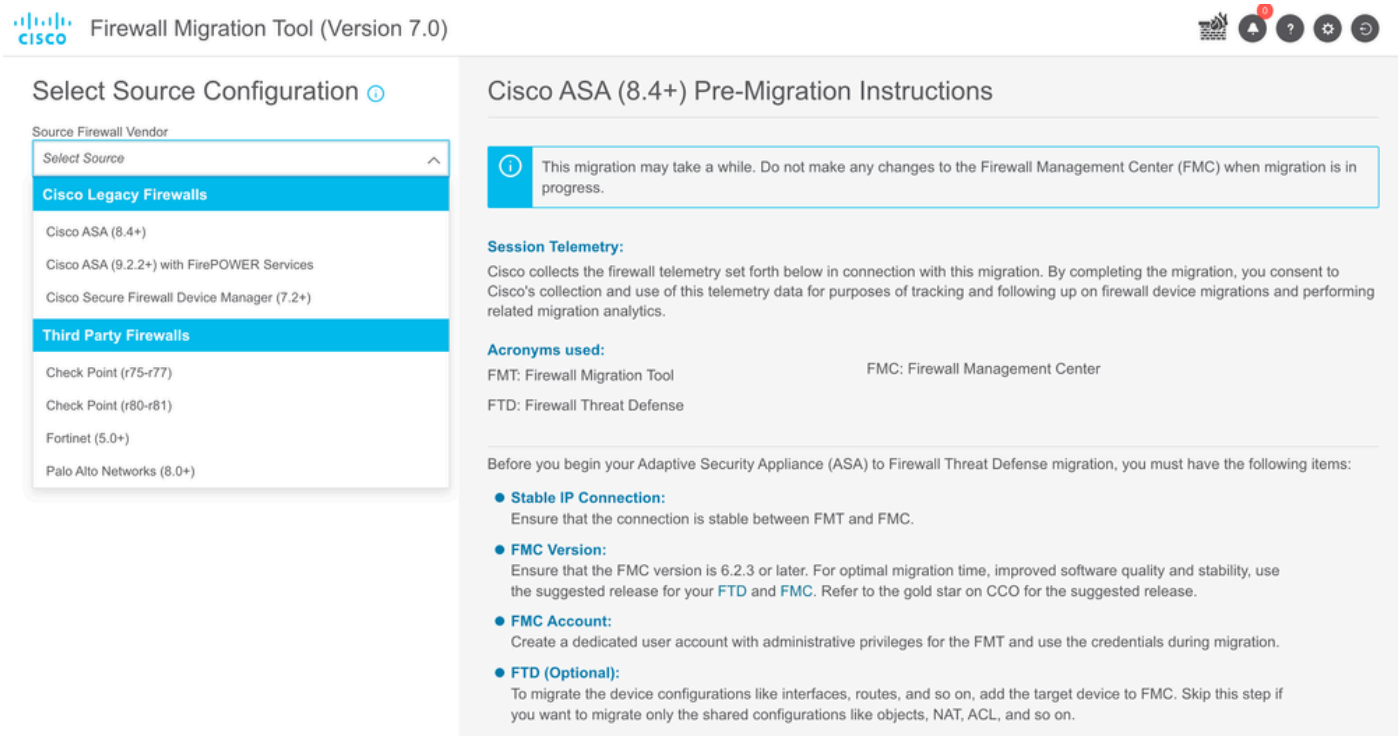
EULA

4. Log in met een geldige CCO-account en de FMT GUI-interface wordt weergegeven in de webbrowser.



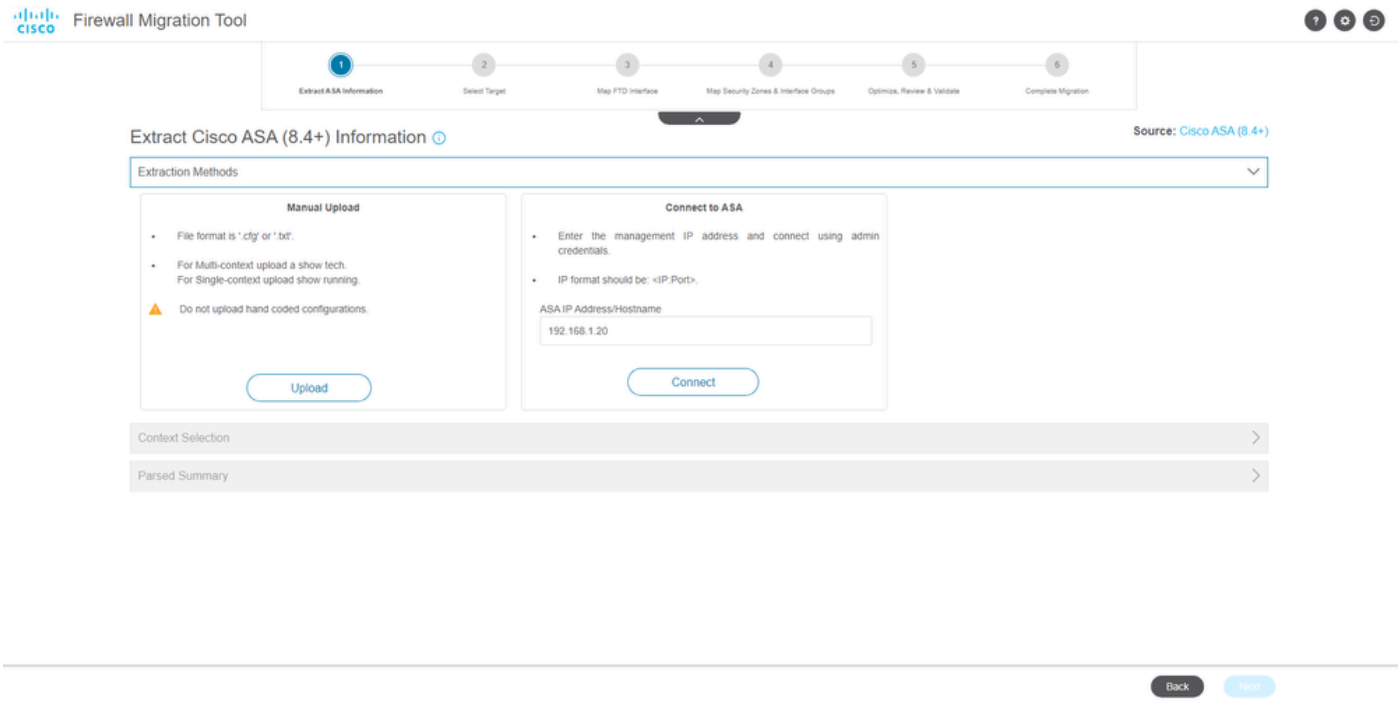
Aanmelden voor FMT

5. Selecteer de te migreren bronfirewall.

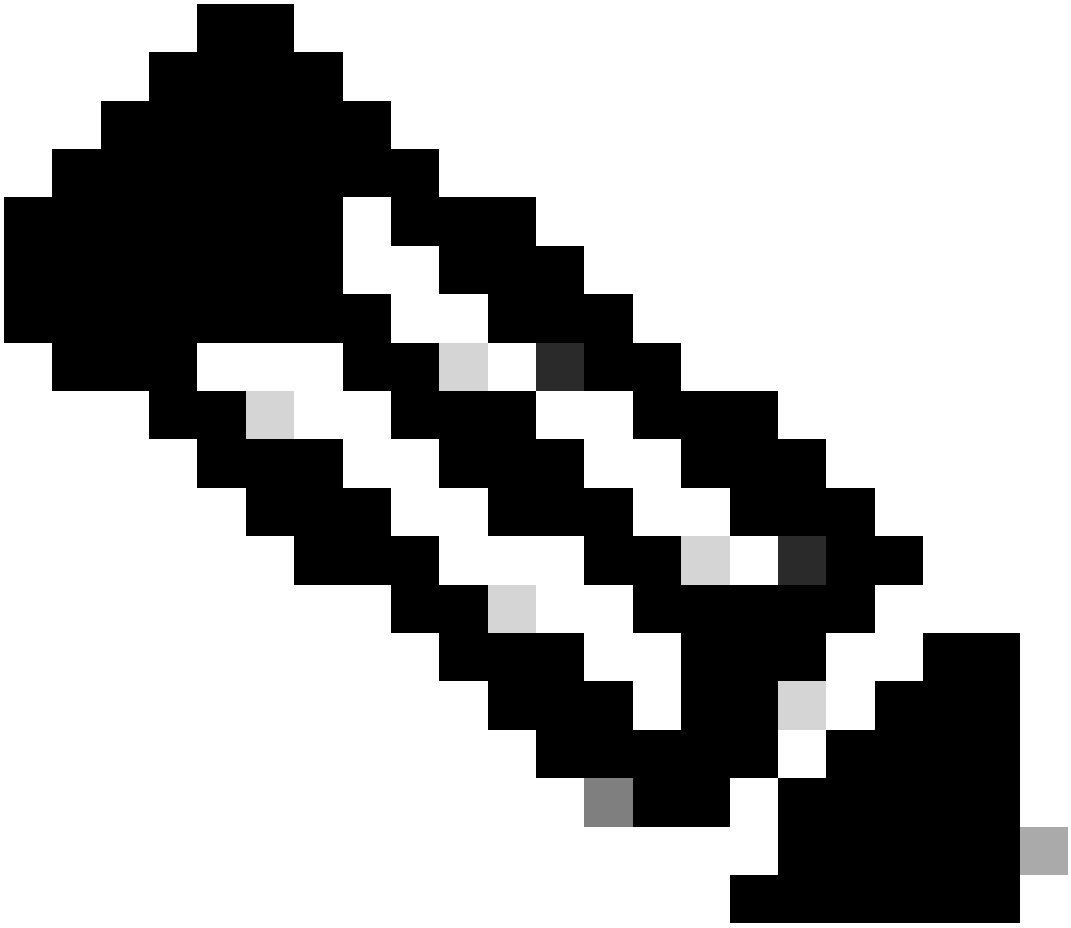


Bronfirewall

6. Selecteer de extractiemethode die gebruikt moet worden om de configuratie te verkrijgen.
    1. Handmatige uploadmethode: u moet het **Running Config** bestand van de ASA uploaden in ".cfg"- of ".txt"-indeling.
    2. Verbind met de ASA om configuraties rechtstreeks uit de firewall te halen.

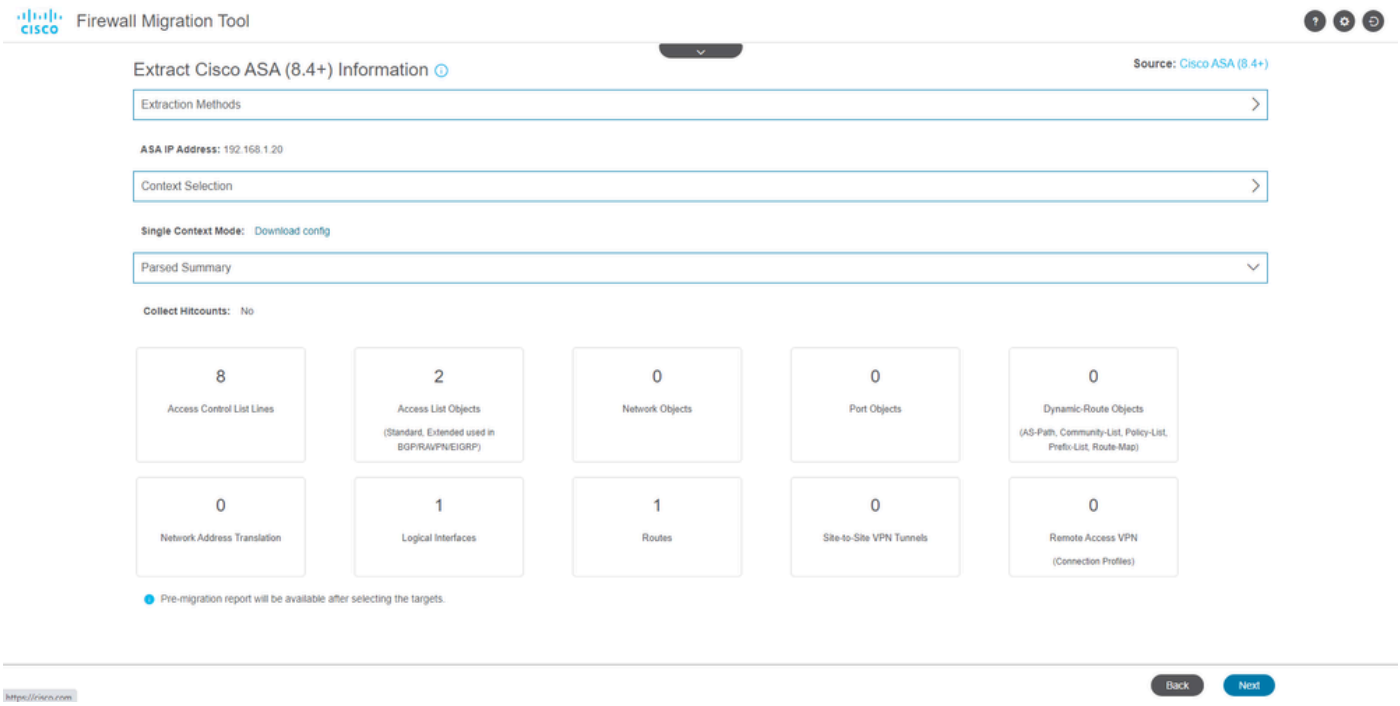


extractie



Opmerking: Sluit bijvoorbeeld rechtstreeks aan op de ASA.

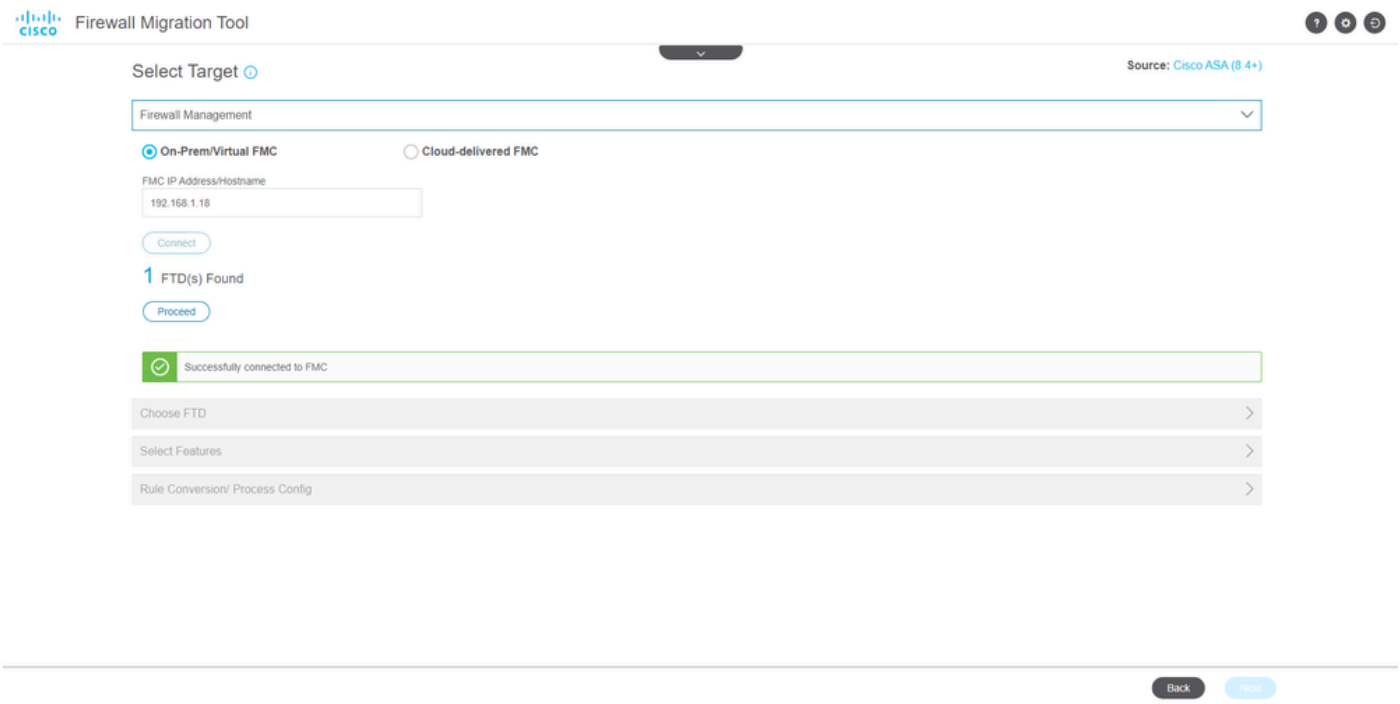
7. Een samenvatting van de configuratie gevonden op de firewall wordt weergegeven als een dashboard, gelieve op Volgende te klikken.



Samenvatting

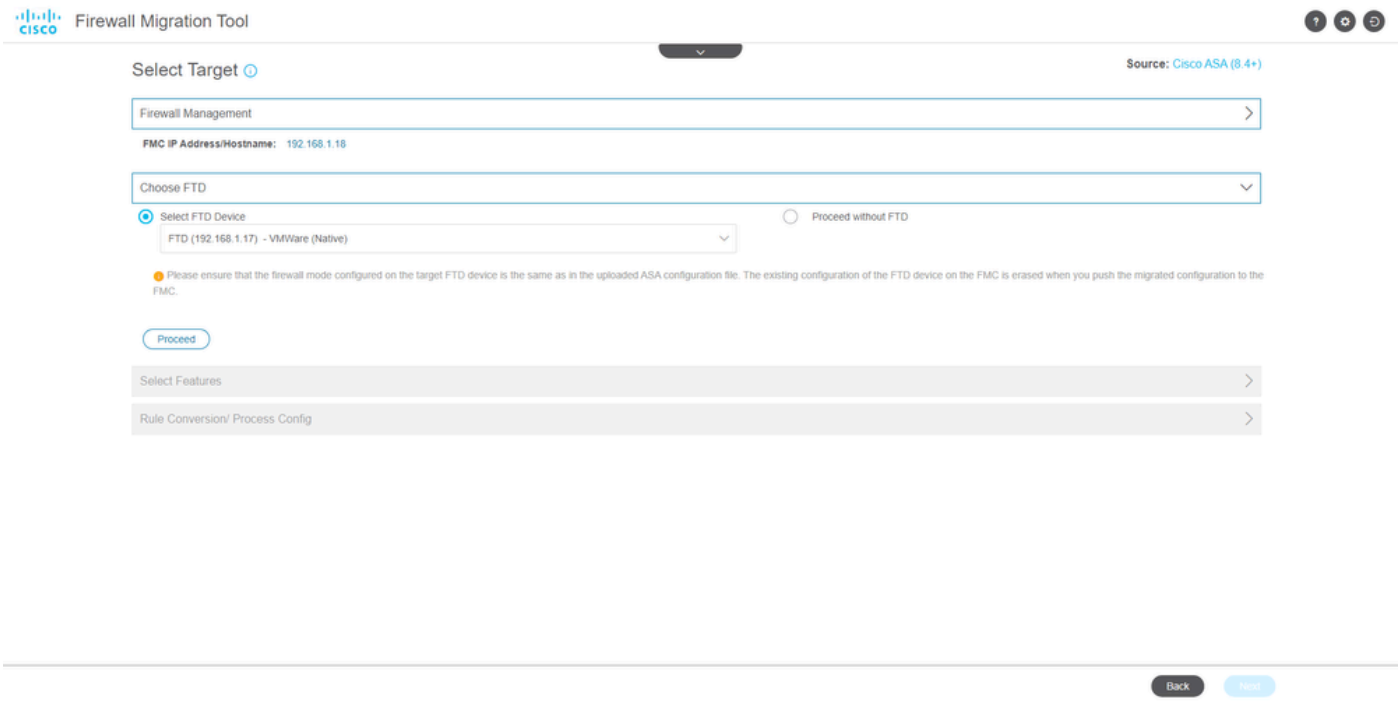
8. Selecteer het beoogde VCC voor de migratie.

Geef het IP-adres van het VCC.Het opent een pop-upvenster waarin u wordt gevraagd om de inlogreferenties van het VCC.



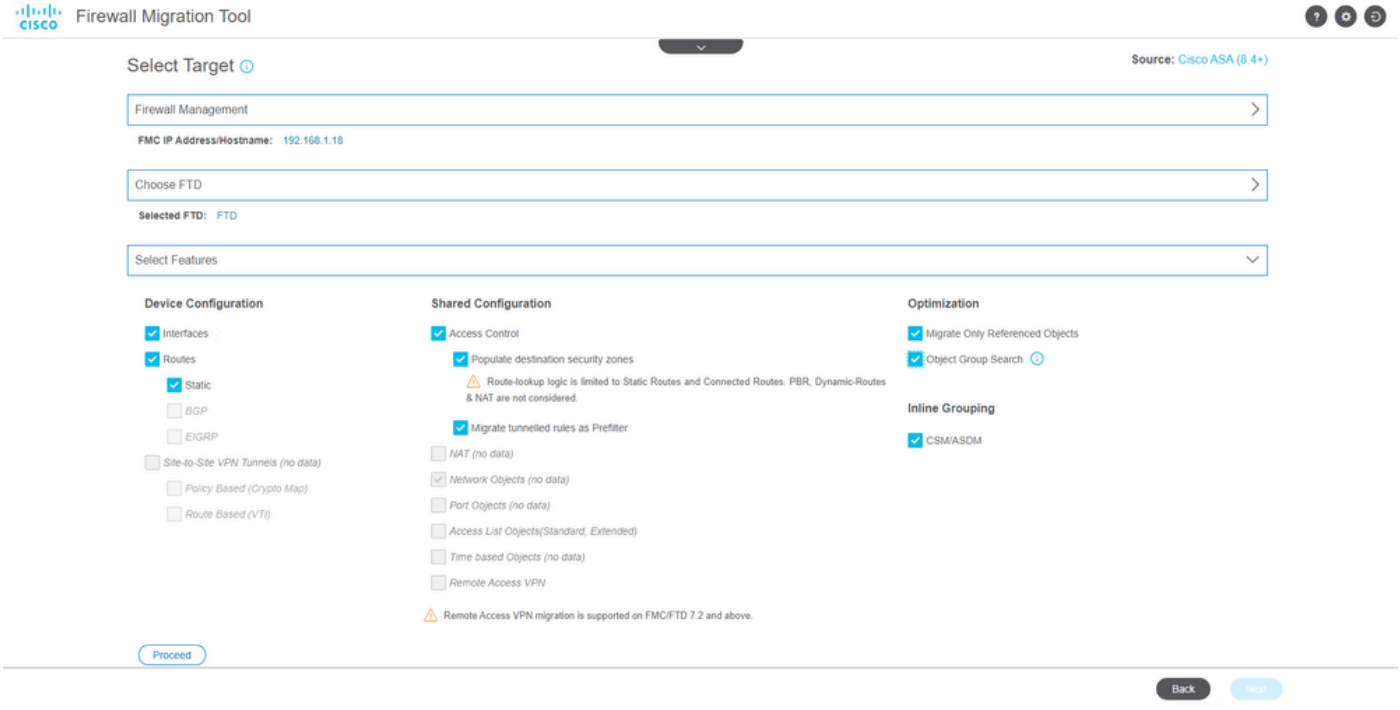
FMC IP

9. (Optioneel)Selecteer de gewenste FTD.
    1. Als u ervoor kiest om naar een FTD te migreren, selecteert u de FTD die u wilt gebruiken.
    2. Als u geen FTD wilt gebruiken, kunt u het aankruisvakje invullen Proceed without FTD



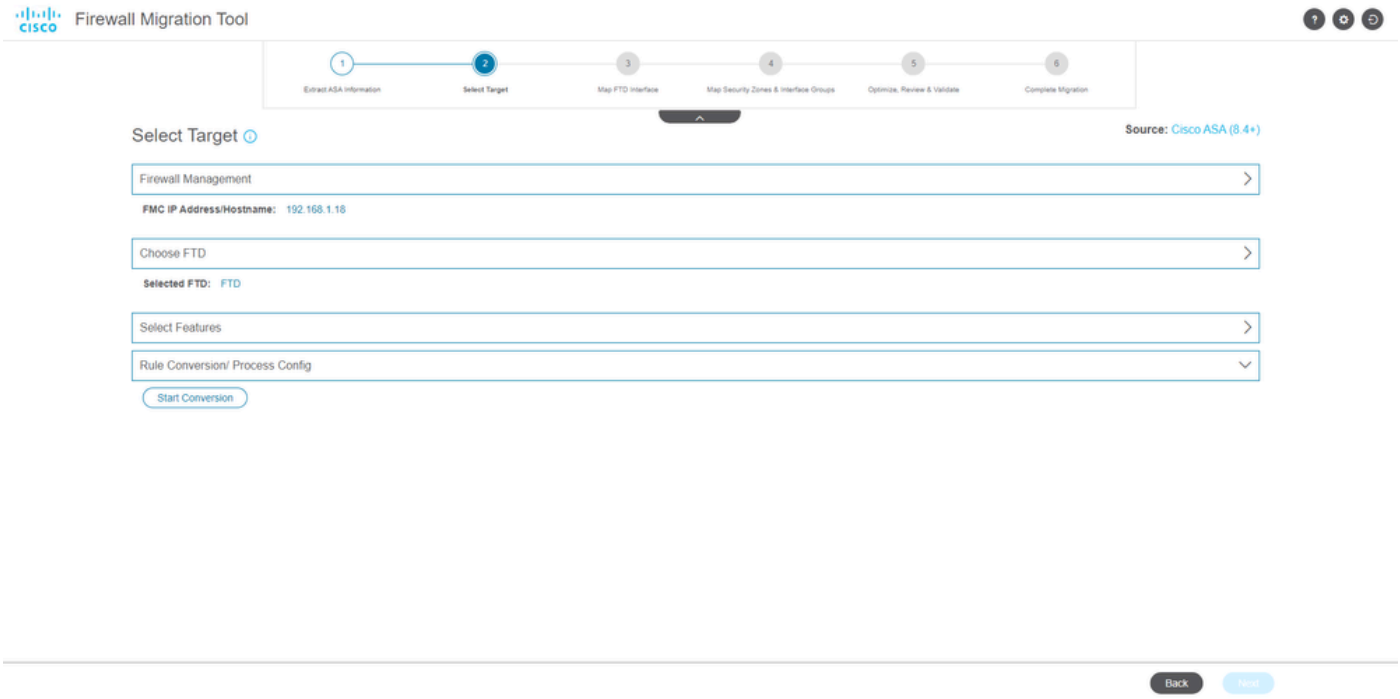
Doel FTD

10. Selecteer de configuraties die u wilt migreren, de opties worden weergegeven in de screenshots.



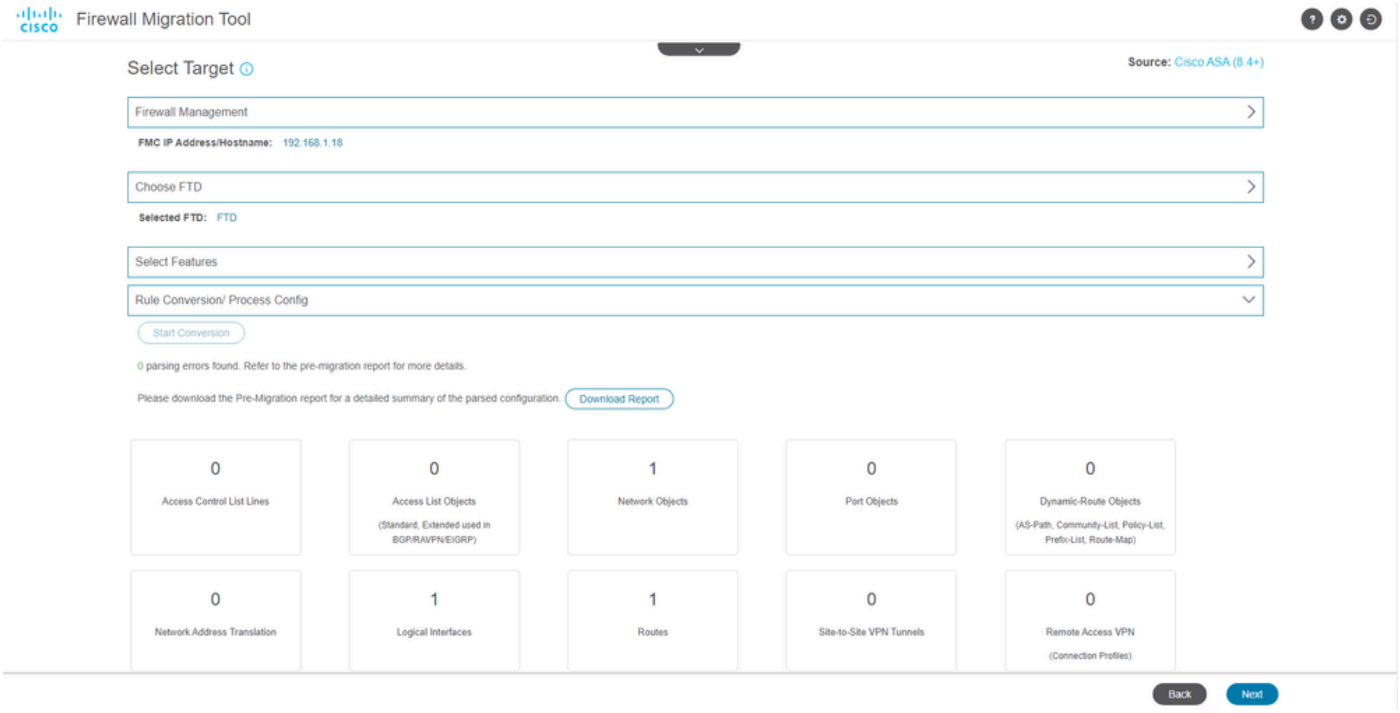
Configuraties

11. Start de conversie van de configuraties van ASA naar FTD.



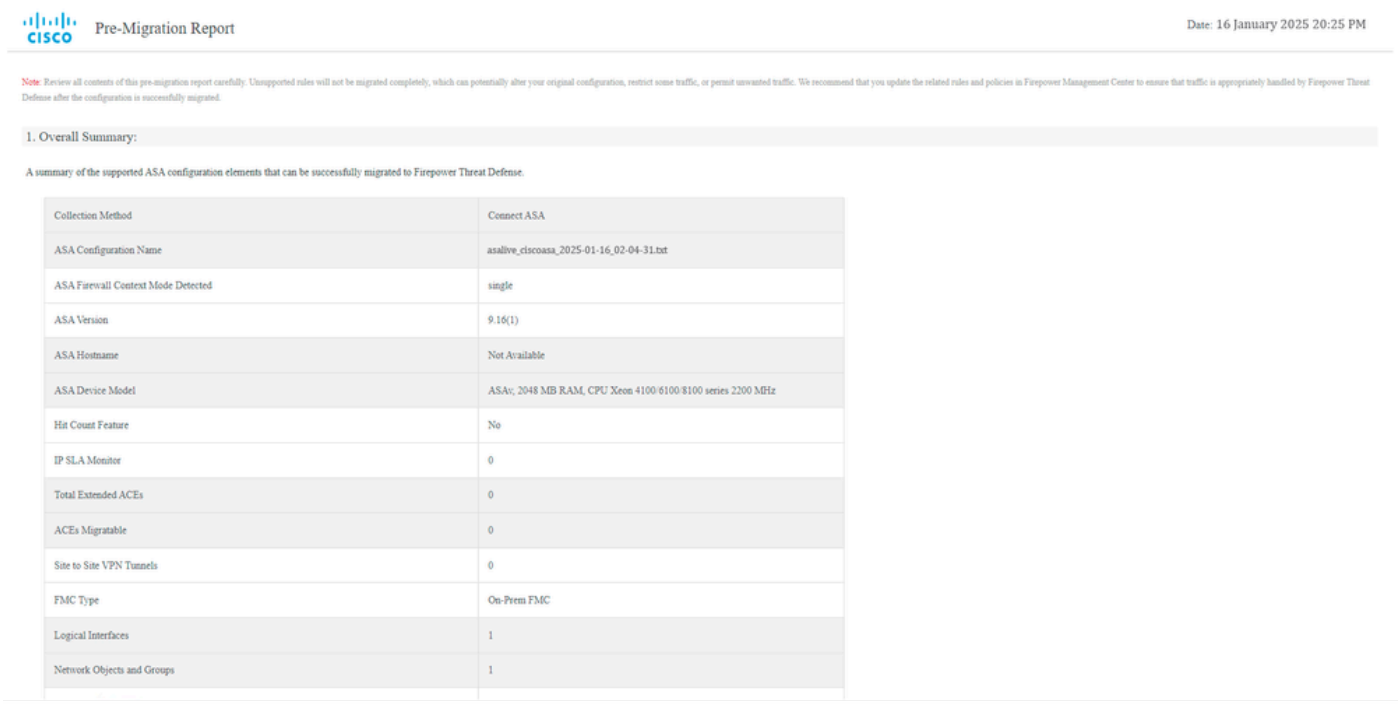
Conversie starten

12. Wanneer de conversie is voltooid, wordt er een dashboard weergegeven met een overzicht van de te migreren objecten (beperkt tot compatibiliteit).
    1. U kunt optioneel klikken **Download Report** om een samenvatting van de te migreren configuraties te ontvangen.



Downloadrapport

Voorbeeld van een pre-migratierapport, zoals in de afbeelding:



Pre-Migration Report

Date: 16 January 2025 20:25 PM

Note: Review all contents of this pre-migration report carefully. Unsupported rules will not be migrated completely, which can potentially alter your original configuration, restrict some traffic, or permit unwanted traffic. We recommend that you update the related rules and policies in Firepower Management Center to ensure that traffic is appropriately handled by Firepower Threat Defense after the configuration is successfully migrated.

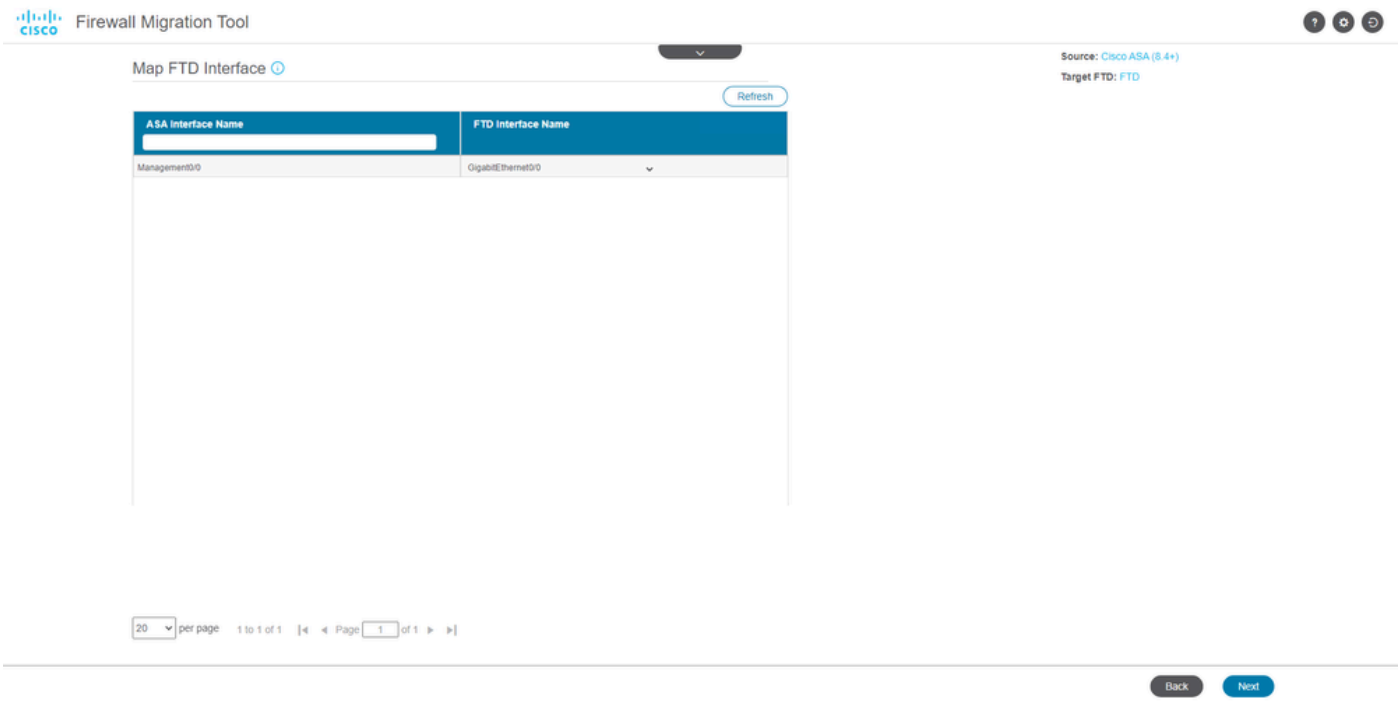
1. Overall Summary:

A summary of the supported ASA configuration elements that can be successfully migrated to Firepower Threat Defense.

Collection Method	Connect ASA
ASA Configuration Name	asalive_ciscoasa_2025-01-16_02-04-31.txt
ASA Firewall Context Mode Detected	single
ASA Version	9.16(1)
ASA Hostname	Not Available
ASA Device Model	ASAv, 2048 MB RAM, CPU Xeon 4100/6100/8100 series 2200 MHz
Hit Count Feature	No
IP SLA Monitor	0
Total Extended ACEs	0
ACEs Migratable	0
Site to Site VPN Tunnels	0
FMC Type	On-Prem FMC
Logical Interfaces	1
Network Objects and Groups	1

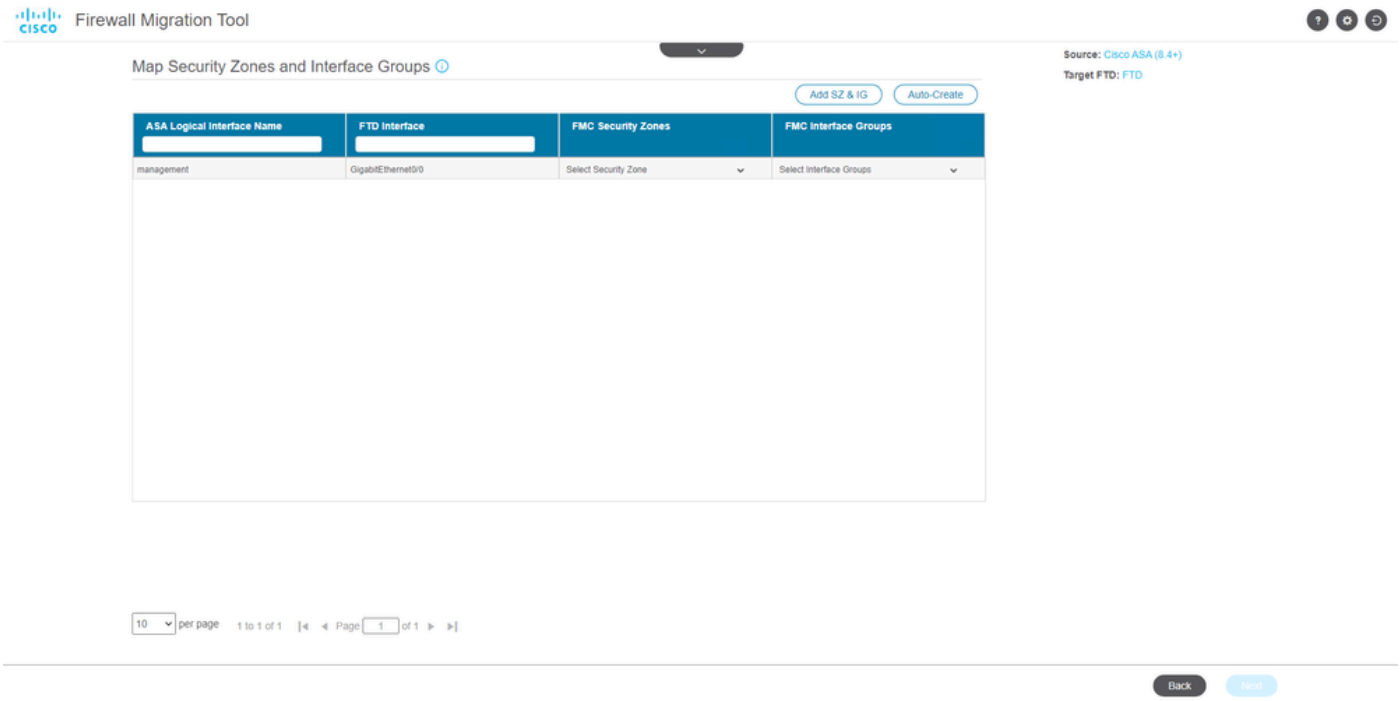
Rapport vóór migratie

13. Breng de ASA-interfaces in kaart met de FTD-interfaces op de Migration Tool.



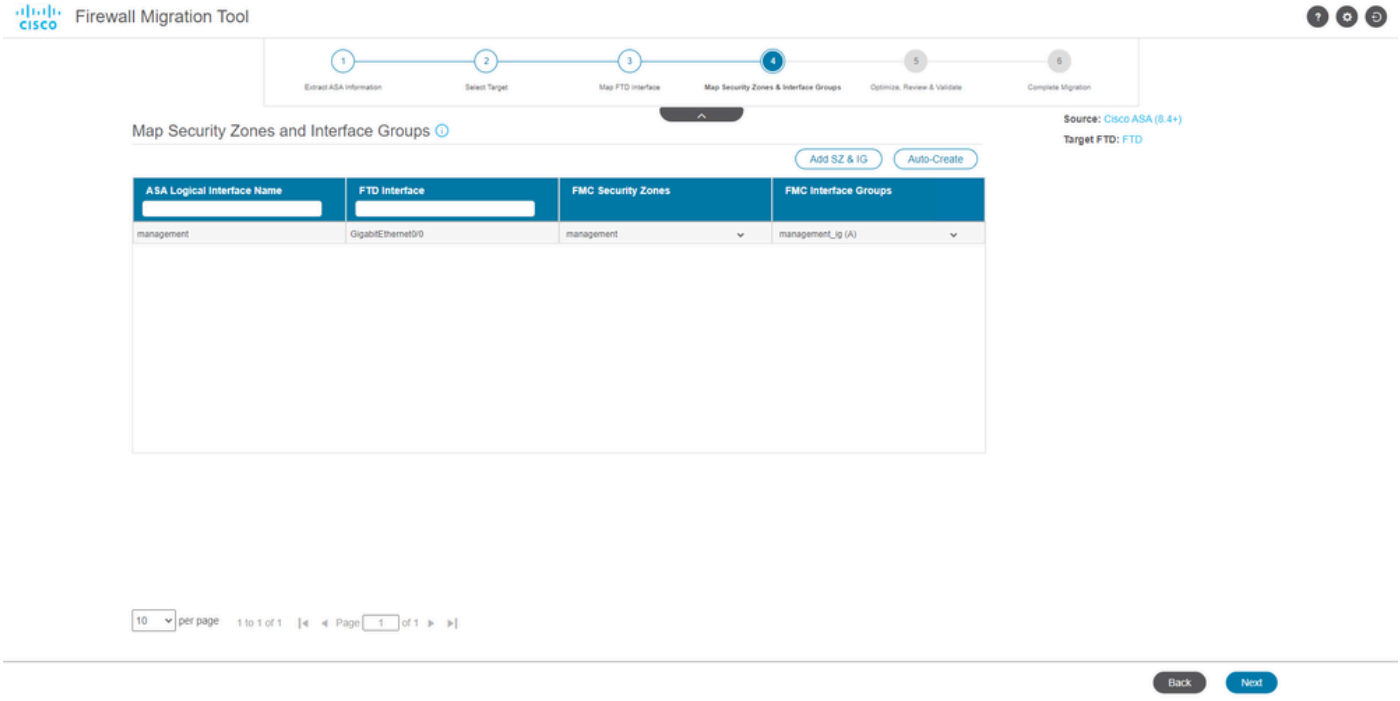
Kaartinterfaces

14. De Security Zones en Interfacegroepen voor de interfaces op de FTD maken



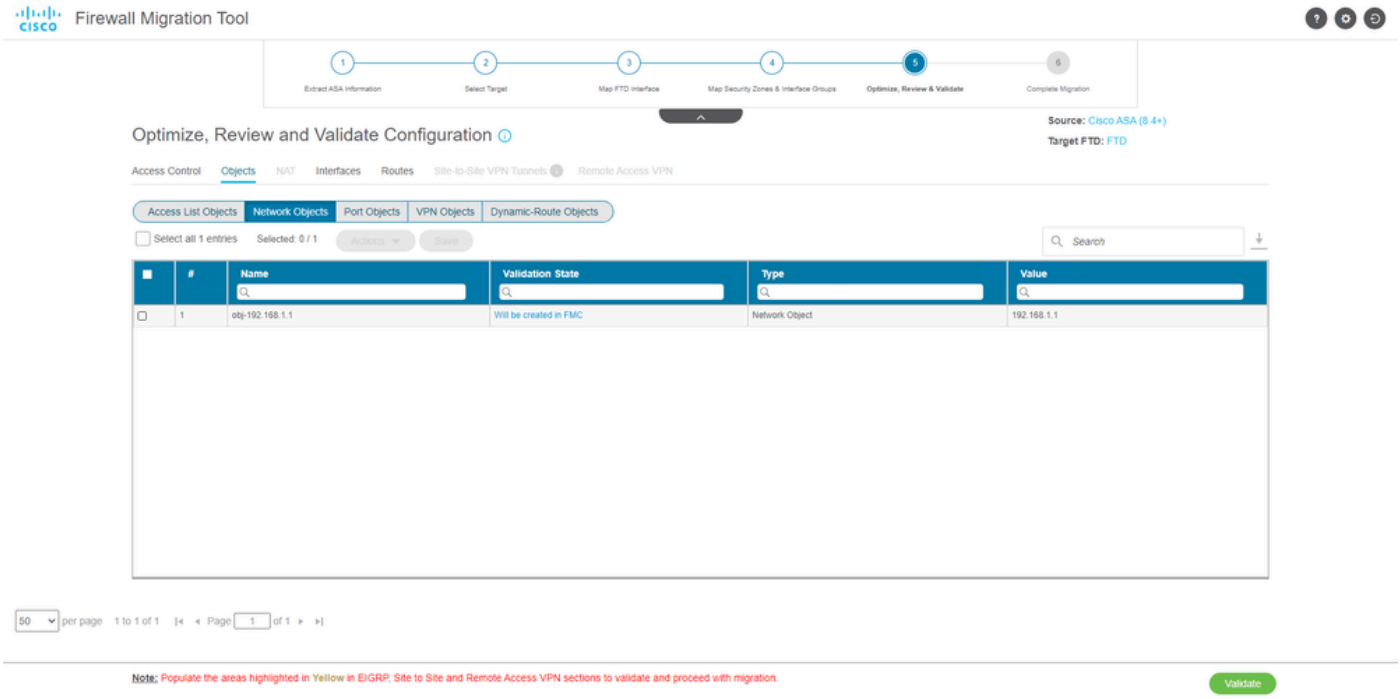
Security zones en interfacegroepen

Security Zones (SZ) en Interfacegroepen (IG) worden automatisch door het gereedschap gemaakt, zoals in de afbeelding:



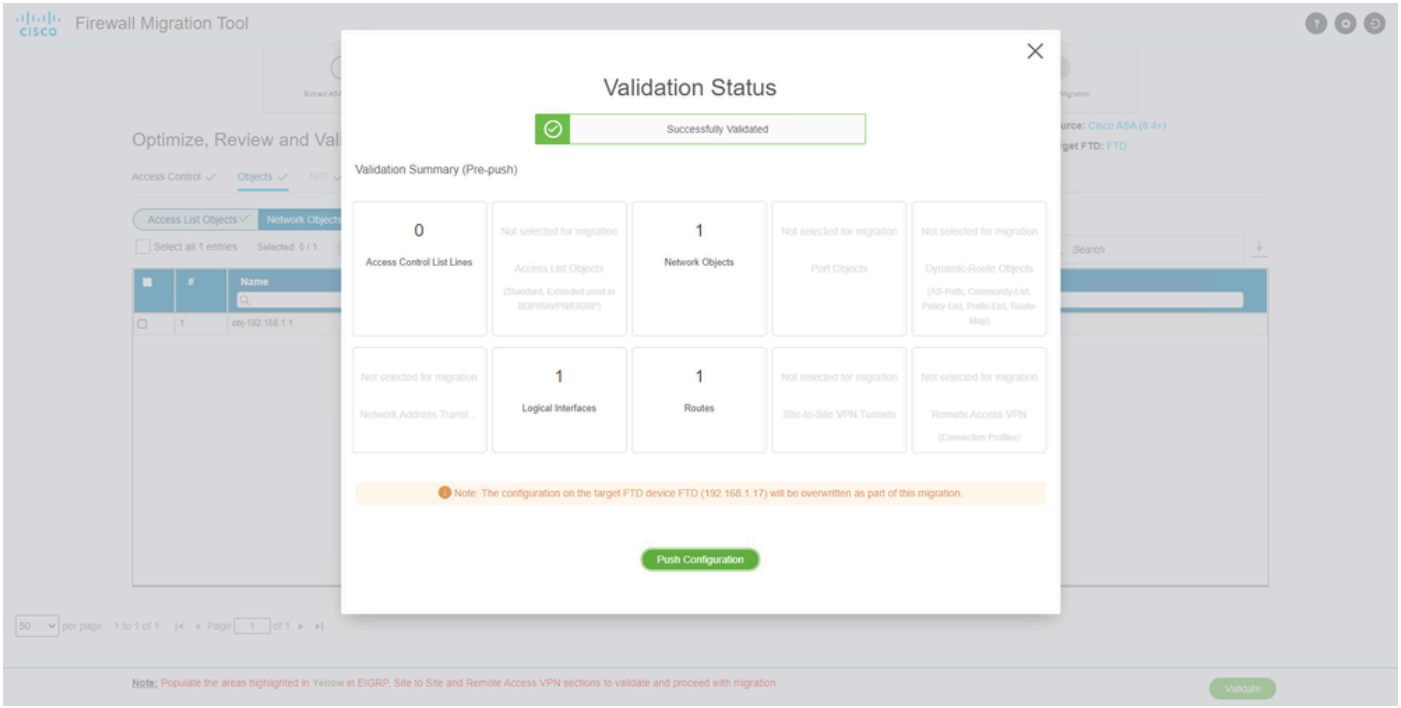
Automatisch maken

15. Bekijk en valideer de configuraties die op de Migration Tool moeten worden gemigreerd.
    1. Als u de configuraties al hebt beoordeeld en geoptimaliseerd, klikt u opValidate.



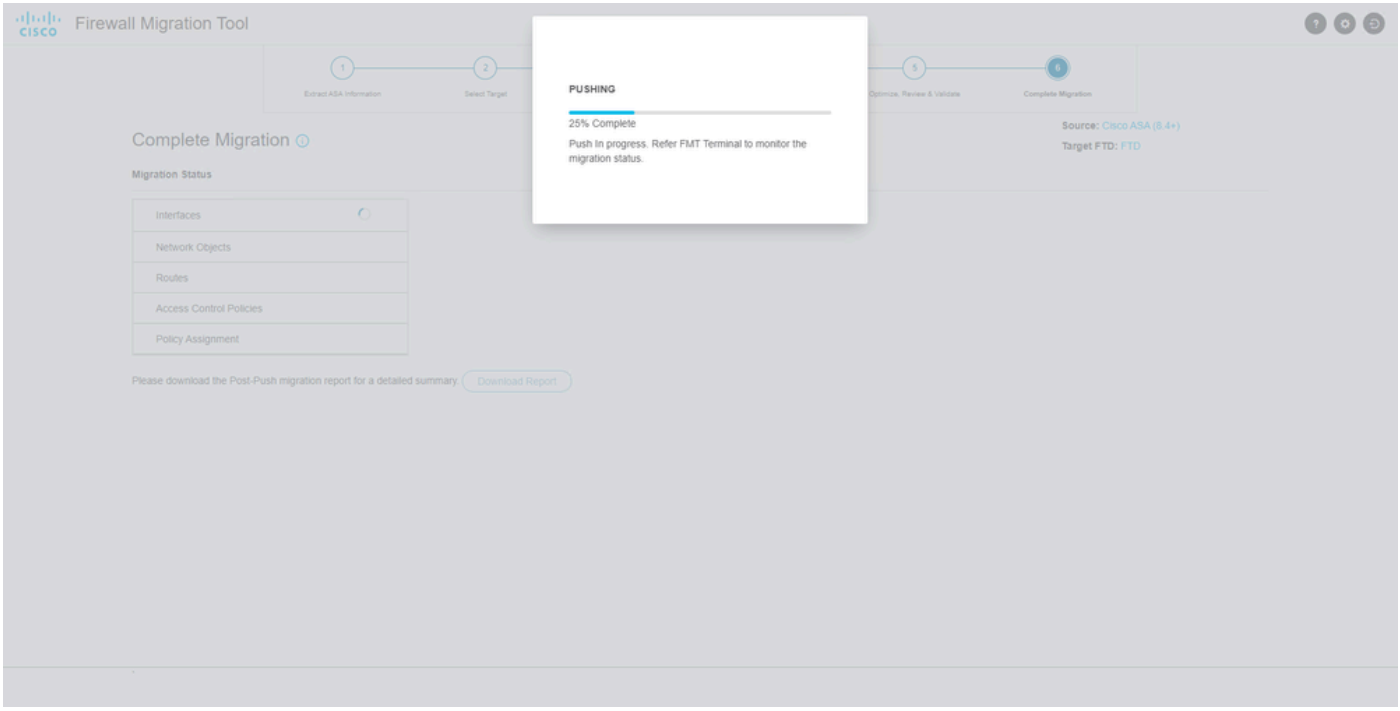
Evalueren en valideren

16. Als de validatiestatus succesvol is, duw dan de configuraties naar de doelapparaten.



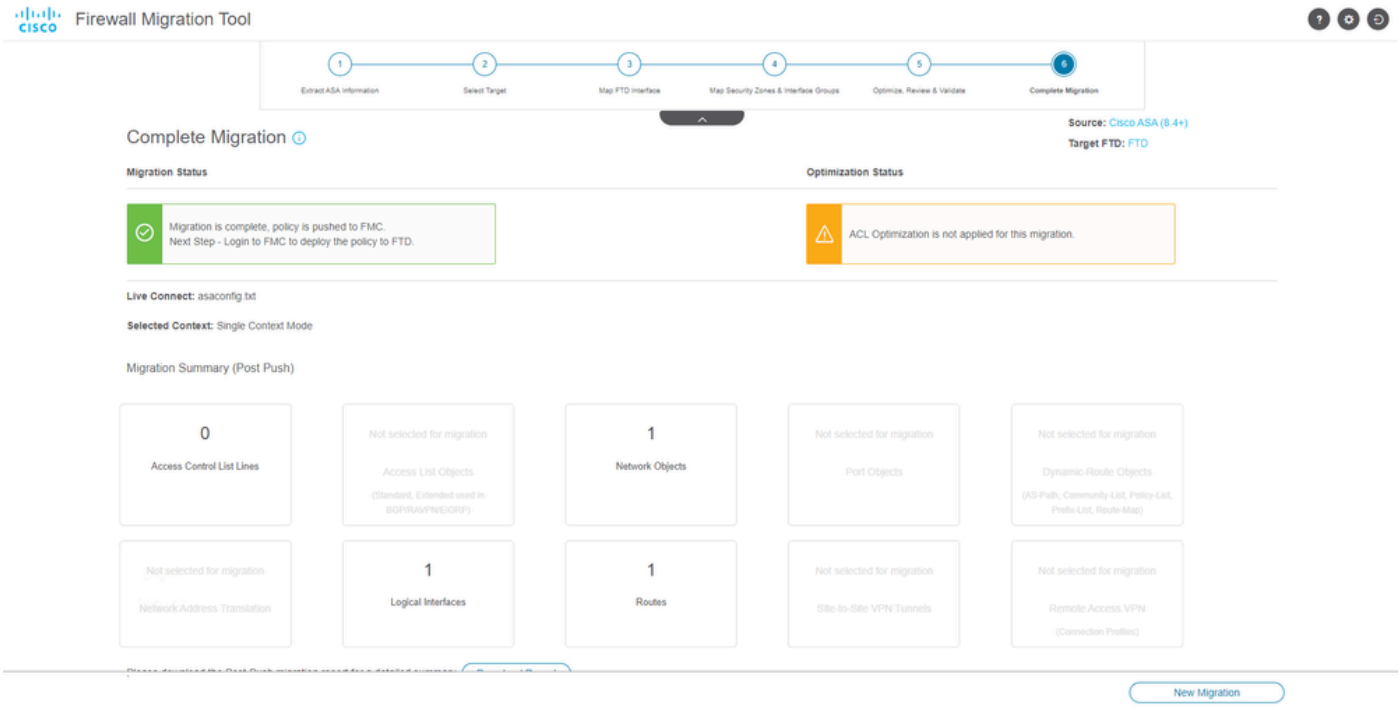
Validatie

Voorbeeld van configuratie die door het migratietool wordt gedrukt, zoals in de afbeelding:



Duw

Voorbeeld van een geslaagde migratie, zoals in de afbeelding:



Succesvolle migratie

(Optioneel) Als u ervoor hebt gekozen om de configuratie naar een FTD te migreren, dient u de beschikbare configuratie van het FMC naar de firewall te verplaatsen.

Zo implementeert u de configuratie:

1. Log in op de GUI van het VCC.
2. Navigeer naar hetDeploytabblad.

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

Problemen oplossen

Problemen oplossen met Secure Firewall-migratietool

- Vaak voorkomende migratiefouten:
  - Onbekende of ongeldige tekens in het ASA-configuratiebestand.
  - Ontbrekende of onvolledige configuratie-elementen.
  - Problemen met netwerkconnectiviteit of latentie.
  - Problemen tijdens het uploaden van ASA-configuratiebestanden of het instellen van een configuratie naar het beheercentrum.
  - Vaak voorkomende problemen zijn:
- 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.
  - Met deze tool kunt u een ondersteuningsbundel downloaden voor logbestanden, database- en configuratiebestanden.
  - Te downloaden stappen:
  - Voor verdere ondersteuning:

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.