

Migreer ASA naar Firepower Threat Defence (FTD) met FMT

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Overzicht](#)

[Achtergrondinformatie](#)

[Het ASA-configuratiebestand verkrijgen](#)

[PKI-certificaat exporteren vanuit ASA en importeren in beheercentrum](#)

[AnyConnect-pakketten en -profielen ophalen](#)

[Configureren](#)

[Configuratiestappen :](#)

[Problemen oplossen](#)

[Problemen oplossen met Secure Firewall-migratietool](#)

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-ss0- 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 gedownloadde 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 Download

Downloads Home / Security / Firewalls / Secure Firewall Migration Tool / Firewall Migration Tool (FMT)- 7.0.0

Expand All Collapse All

Latest Release ▼

7.0.1

All Release ▼

7 ▼

7.0.1

7.0.0

Secure Firewall Migration Tool

Release 7.0.0

[My Notifications](#)

Related Links and Documentation

[Open Source](#)

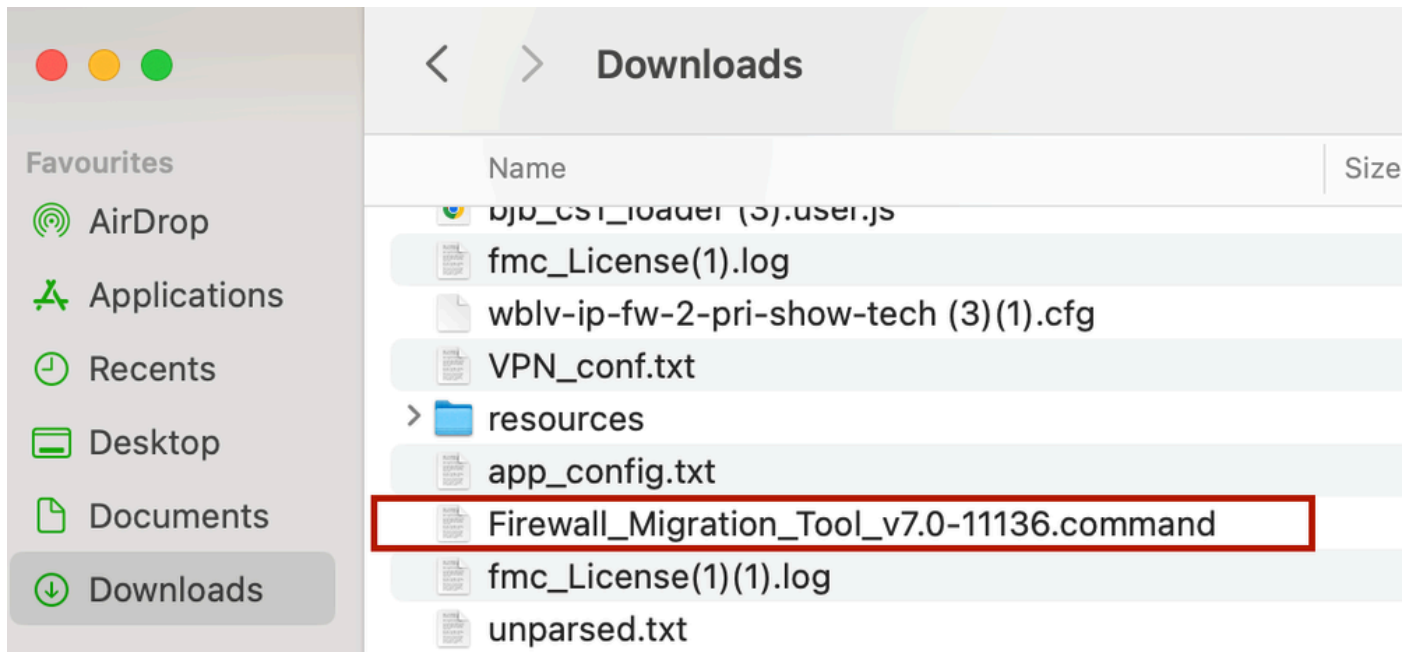
[Release Notes for 7.0.0](#)

[Install and Upgrade Guides](#)

File Information	Release Date	Size	
Firewall Migration Tool 7.0.0.1 for Mac Firewall_Migration_Tool_v7.0.0.1-11241.command Advisories	04-Sep-2024	41.57 MB	↓ 🛒 📄
Firewall Migration Tool 7.0.0.1 for Windows Firewall_Migration_Tool_v7.0.0.1-11241.exe Advisories	04-Sep-2024	39.64 MB	↓ 🛒 📄
Firewall Migration Tool 7.0.0 for Mac Firewall_Migration_Tool_v7.0-11136.command Advisories	05-Aug-2024	41.55 MB	↓ 🛒 📄
Firewall Migration Tool 7.0.0 for Windows Firewall_Migration_Tool_v7.0-11136.exe Advisories	05-Aug-2024	39.33 MB	↓ 🛒 📄

Software downloaden

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



Het bestand

```
ontext migration.'], 'FDM-managed Device to Threat Defense Migration': ['migrate
the Layer 7 security policies including SNMP and HTTP, and malware and file pol
icy configurations from your FDM-managed device to a threat defense device.'], '
Third Party Firewall to Threat Defense Migration': ['Check Point Firewall - migr
ate the site-to-site VPN (policy-based) configurations on your Check Point firew
all ( R80 or later) to a threat defense device (Version 6.7 or later)', 'Fortine
t Firewall - Optimize your application access control lists (ACLs) when migratin
g configurations from a Fortinet firewall to your threat defense device.']], 'se
curity_patch': False, 'updated_date': '25-1-2024', 'version': '6.0-9892'}}"
2025-01-16 16:51:36,906 [INFO      | views] > "The current tool is up to date"
127.0.0.1 - - [16/Jan/2025 16:51:36] "GET /api/software/check_tool_update HTTP/1
.1" 200 -
2025-01-16 16:51:40,615 [DEBUG    | common] > "session table records count:1"
2025-01-16 16:51:40,622 [INFO     | common] > "proxies : {}"
2025-01-16 16:51:41,838 [INFO     | common] > "Telemetry push : Able to connect t
o SSE Cloud server : https://sign-on.security.cisco.com"
127.0.0.1 - - [16/Jan/2025 16:51:41] "GET /api/eula_check HTTP/1.1" 200 -
2025-01-16 16:51:41,851 [INFO     | cco_login] > "EULA check for an user"
2025-01-16 16:51:46,860 [DEBUG    | common] > "session table records count:1"
2025-01-16 16:51:46,868 [INFO     | common] > "proxies : {}"
2025-01-16 16:51:48,230 [INFO     | common] > "Telemetry push : Able to connect t
o SSE Cloud server : https://sign-on.security.cisco.com"
127.0.0.1 - - [16/Jan/2025 16:51:48] "GET /api/eula_check HTTP/1.1" 200 -
```



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.

END USER LICENSE AGREEMENT

This is an agreement between You and Cisco Systems, Inc. or its affiliates ("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the individual or legal entity licensing the Software under this EULA. "Use" or "Using" means to download, install, activate, access or otherwise use the Software. "Software" means the Cisco computer programs and any Upgrades made available to You by an Approved Source and licensed to You by Cisco. "Documentation" is the Cisco user or technical manuals, training materials, specifications or other documentation applicable to the Software and made available to You by an Approved Source. "Approved Source" means (i) Cisco or (ii) the Cisco authorized reseller, distributor or systems integrator from whom you acquired the Software. "Entitlement" means the license detail, including license metric, duration, and quantity provided in a product ID (PID) published on Cisco's price list, claim certificate or right to use notification. "Upgrades" means all updates, upgrades, bug fixes, error corrections, enhancements and other modifications to the Software and backup copies thereof. This agreement, any supplemental license terms and any specific product terms at www.cisco.com/go/software/terms (collectively, the "EULA") govern Your Use of the Software.

1. **Acceptance of Terms.** By Using the Software, You agree to be bound by the terms of the EULA. If you are entering into this EULA on behalf of an entity, you represent that you have authority to bind that entity. If you do not have such authority or you do not agree to the terms of the EULA, neither you nor the entity may Use the Software and it may be returned to the Approved Source for a refund within thirty (30) days of the date you acquired the Software or Cisco product. Your right to return and refund applies only if you are the original end user licensee of the Software.

2. **License.** Subject to payment of the applicable fees and compliance with this EULA, Cisco grants You a limited, non-exclusive and non-transferable license to Use object code versions of the Software and the Documentation solely for Your internal operations and in accordance with the Entitlement and the Documentation. Cisco licenses You the right to Use only the Software You acquire from an Approved Source. It makes no warranty, no applicable law. You are not licensed to Use the

I have read the content of the EULA and SEULA and agree to terms listed.

Proceed

Migrate policies from Cisco ASA or Cisco ASA with FPS or Check Point or PAN or Fortinet to Cisco FTD



Extract Source Information

Any additional information explaining this



EULA

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



Security Cloud Sign On

Email

Continue

Don't have an account? [Sign up now](#)

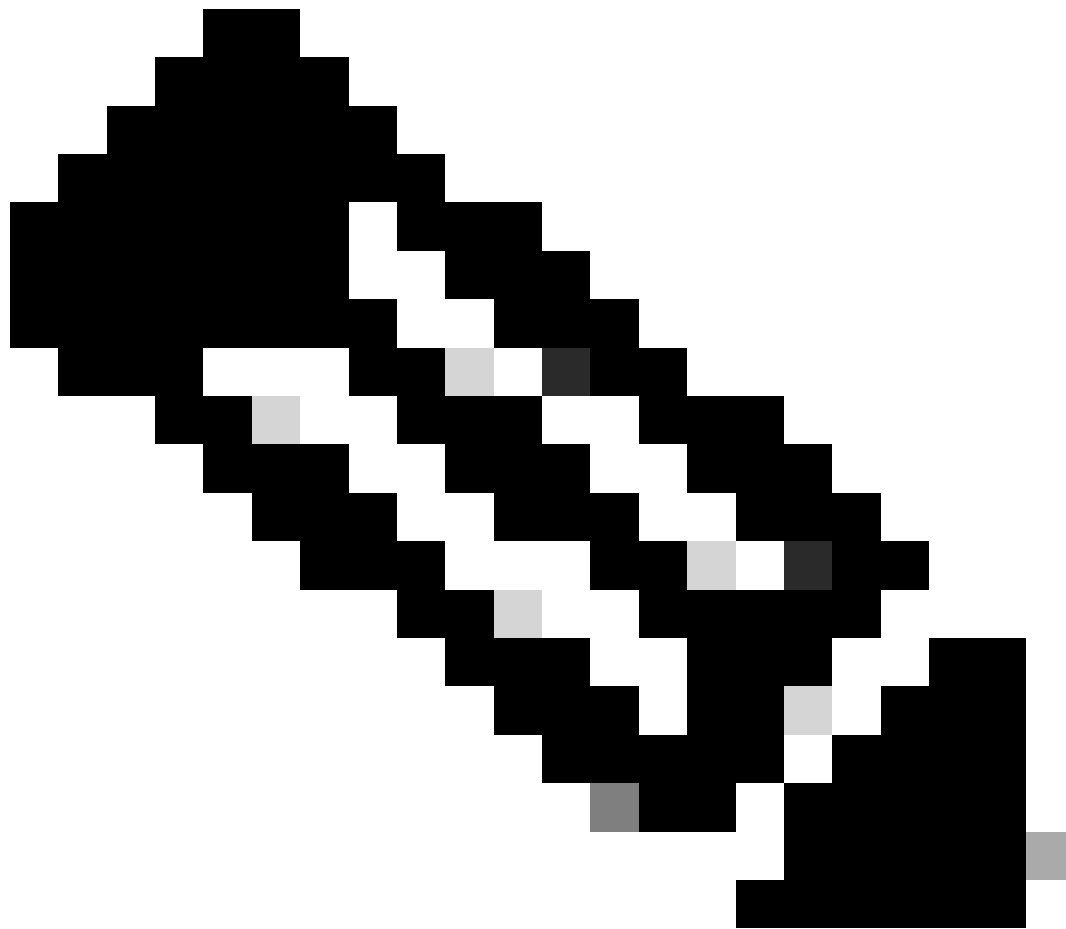
Or

[Other login options](#)

[System status](#) [Policy statement](#)

Aanmelden voor FMT

5. Selecteer de te migreren bronfirewall.



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.

Extract Cisco ASA (8.4+) Information

Source: Cisco ASA (8.4+)

Extraction Methods >

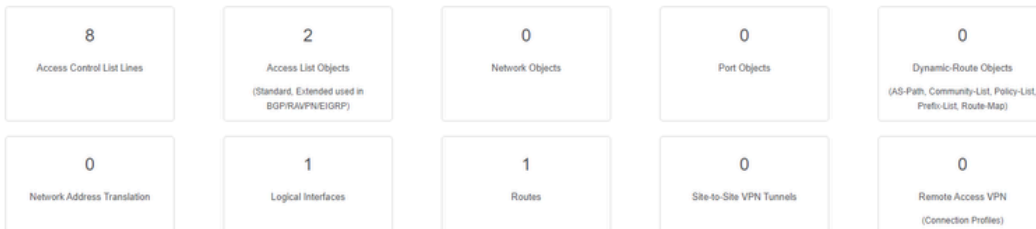
ASA IP Address: 192.168.1.20

Context Selection >

Single Context Mode: Download config

Parsed Summary ▾

Collect Hitcounts: No



• Pre-migration report will be available after selecting the targets.

https://cisco.com

Back

Next

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.

Select Target

Source: Cisco ASA (8.4+)

Firewall Management ▾

 On-Prem/Virtual FMC

 Cloud-delivered FMC

FMC IP Address/Hostname

192.168.1.18

Connect

1 FTD(s) Found

Proceed

Successfully connected to FMC

Choose FTD >

Select Features >

Rule Conversion/ Process Config >

Back

Next

FMC IP

9. (Optioneel) Selecteer de gewenste FTD.

- Als u ervoor kiest om naar een FTD te migreren, selecteert u de FTD die u wilt gebruiken.
- Als u geen FTD wilt gebruiken, kunt u het aankruisvakje invullen `Proceed without FTD`

Select Target

Source: Cisco ASA (8.4+)

Firewall Management >

FMC IP Address/Hostname: 192.168.1.18

Choose FTD >

Select FTD Device Proceed without FTD

FTD (192.168.1.17) - VMWare (Native)

Please ensure that the firewall mode configured on the target FTD device is the same as in the uploaded ASA configuration file. The existing configuration of the FTD device on the FMC is erased when you push the migrated configuration to the FMC.

Proceed

Select Features >

Rule Conversion/ Process Config >

Back Next

Doel FTD

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

Select Target

Source: Cisco ASA (8.4+)

Firewall Management >

FMC IP Address/Hostname: 192.168.1.18

Choose FTD >

Selected FTD: FTD

Select Features >

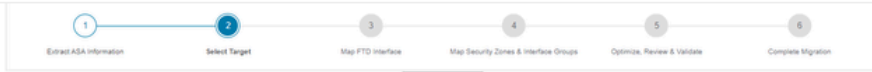
<p>Device Configuration</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Interfaces <input checked="" type="checkbox"/> Routes <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Static <input type="checkbox"/> BGP <input type="checkbox"/> EIGRP <input type="checkbox"/> Site-to-Site VPN Tunnels (no data) <input type="checkbox"/> Policy Based (Crypto Map) <input type="checkbox"/> Route Based (VTI) 	<p>Shared Configuration</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Access Control <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Populate destination security zones <ul style="list-style-type: none"> ⚠ Route-lookup logic is limited to Static Routes and Connected Routes. PBR, Dynamic-Routes & NAT are not considered. <input checked="" type="checkbox"/> Migrate tunnelled rules as Prefilter <input type="checkbox"/> NAT (no data) <input checked="" type="checkbox"/> Network Objects (no data) <input type="checkbox"/> Port Objects (no data) <input type="checkbox"/> Access List Objects(Standard, Extended) <input type="checkbox"/> Time based Objects (no data) <input type="checkbox"/> Remote Access VPN <p>⚠ Remote Access VPN migration is supported on FMC/FTD 7.2 and above.</p>	<p>Optimization</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Migrate Only Referenced Objects <input checked="" type="checkbox"/> Object Group Search <p>Inline Grouping</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> CSM/ASDM
--	---	--

Proceed

Back Next

Configuraties

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



Select Target

Source: Cisco ASA (8.4+)

Firewall Management

FMC IP Address/Hostname: 192.168.1.18

Choose FTD

Selected FTD: FTD

Select Features

Rule Conversion/ Process Config

Start Conversion

Back Next

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.

Select Target

Source: Cisco ASA (8.4+)

Firewall Management

FMC IP Address/Hostname: 192.168.1.18

Choose FTD

Selected FTD: FTD

Select Features

Rule Conversion/ Process Config

Start Conversion

0 parsing errors found. Refer to the pre-migration report for more details.

Please download the Pre-Migration report for a detailed summary of the parsed configuration. [Download Report](#)

0 Access Control List Lines	0 Access List Objects <small>(Standard, Extended used in BGP/RAVP/NEIGRP)</small>	1 Network Objects	0 Port Objects	0 Dynamic-Route Objects <small>(AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)</small>
0 Network-Address Translation	1 Logical Interfaces	1 Routes	0 Site-to-Site VPN Tunnels	0 Remote Access VPN <small>(Connection Profiles)</small>

Back Next

Downloadrapport

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

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	ASA; 2048 MB RAM, CPU Xeon 4100 6100 8100 series 2200 MHz
Hat 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.

Firewall Migration Tool

Map FTD Interface

Source: Cisco ASA (8.4+)
Target FTD: FTD

ASA Interface Name	FTD Interface Name
Management0/0	GigabitEthernet0/0

20 per page 1 to 1 of 1 Page 1 of 1

Back Next

Kaartinterfaces

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

Map Security Zones and Interface Groups

Source: Cisco ASA (8.4+)
Target FTD: FTD

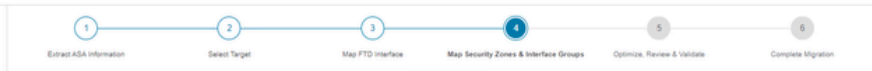
ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
management	GigabitEthernet0/0	Select Security Zone	Select Interface Groups

10 per page 1 to 1 of 1 |< < Page 1 of 1 > >|

Back Next

Security zones en interfacegroepen

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



Map Security Zones and Interface Groups

Source: Cisco ASA (8.4+)
Target FTD: FTD

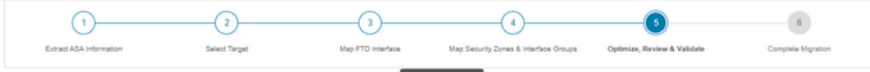
ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
management	GigabitEthernet0/0	management	management_lg (A)

10 per page 1 to 1 of 1 |< < Page 1 of 1 > >|

Back Next

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 op **validate**.



Optimize, Review and Validate Configuration

Source: Cisco ASA (8.4+)
Target FTD: FTD

Access Control **Objects** NAT Interfaces Routes Site-to-Site VPN Tunnels Remote Access VPN

Access List Objects **Network Objects** Port Objects VPN Objects Dynamic-Route Objects

Select all 1 entries Selected: 0/1

#	Name	Validation State	Type	Value
1	obj-192.168.1.1	Will be created in FMC	Network Object	192.168.1.1

50 per page 1 to 1 of 1 Page 1 of 1

Note: Populate the areas highlighted in Yellow in EIGRP, Site to Site and Remote Access VPN sections to validate and proceed with migration

Validate

Evalueren en valideren

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

Validation Status

Successfully Validated

Validation Summary (Pre-push)

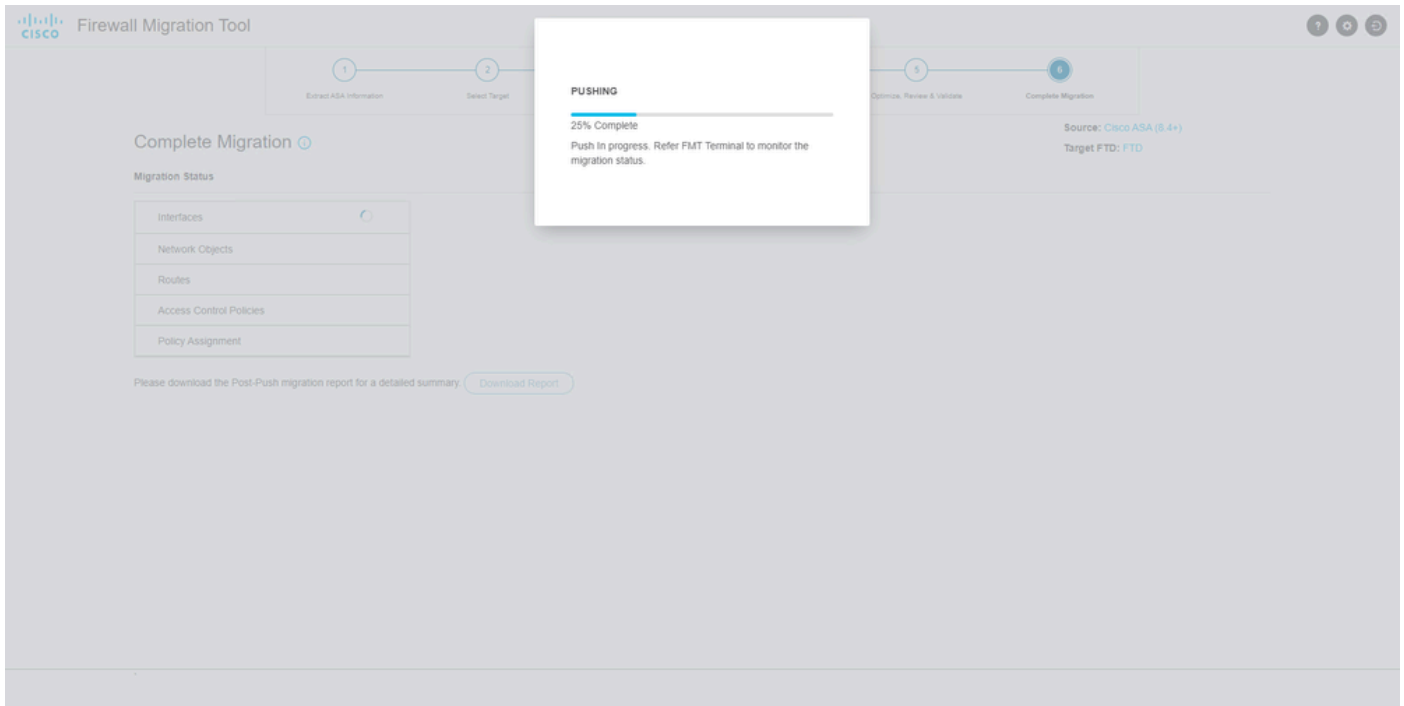
0 Access Control List Lines	Not selected for migration Access List Objects (Standard, Extended used in BGP/RAVPN/EIGRP)	1 Network Objects	Not selected for migration Port Objects	Not selected for migration Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)
Not selected for migration Network Address Transl...	1 Logical Interfaces	1 Routes	Not selected for migration Site-to-Site VPN Tunnels	Not selected for migration Remote Access VPN (Connection Profiles)

Note: The configuration on the target FTD device FTD (192.168.1.17) will be overwritten as part of this migration.

Push Configuration

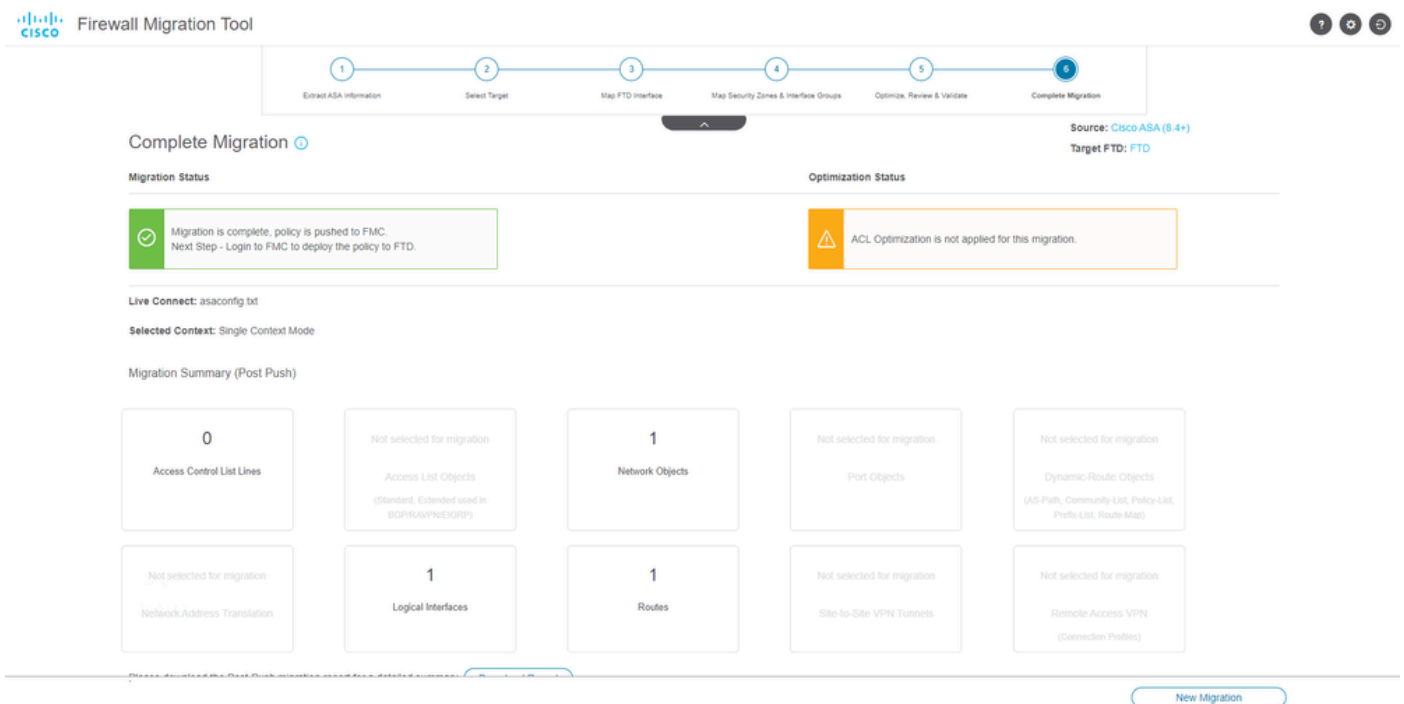
Validatie

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 het Deploy tabblad.

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.