

De Secure Firewall Migration Tool voor ASA

Migratie configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuratiestappen](#)

[Problemen oplossen](#)

Inleiding

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

Bijgedragen door Ricardo Vera, Cisco TAC Engineer.

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:

- Windows PC met Firepower Migration Tool (FMT) v3.0.1
- Adaptieve security applicatie (ASA) v9.16.1
- Secure Firewall Management Center (FMCv) v7.0.1
- Secure Firewall Threat Defense Virtual (FTDv) v7.0.1

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.

Achtergrondinformatie

Specifieke eisen voor dit document zijn:

- Cisco adaptieve security applicatie (ASA) versie 8.4 of hoger
- Secure Firewall Management Center (FMCv) versie 6.2.3 of hoger

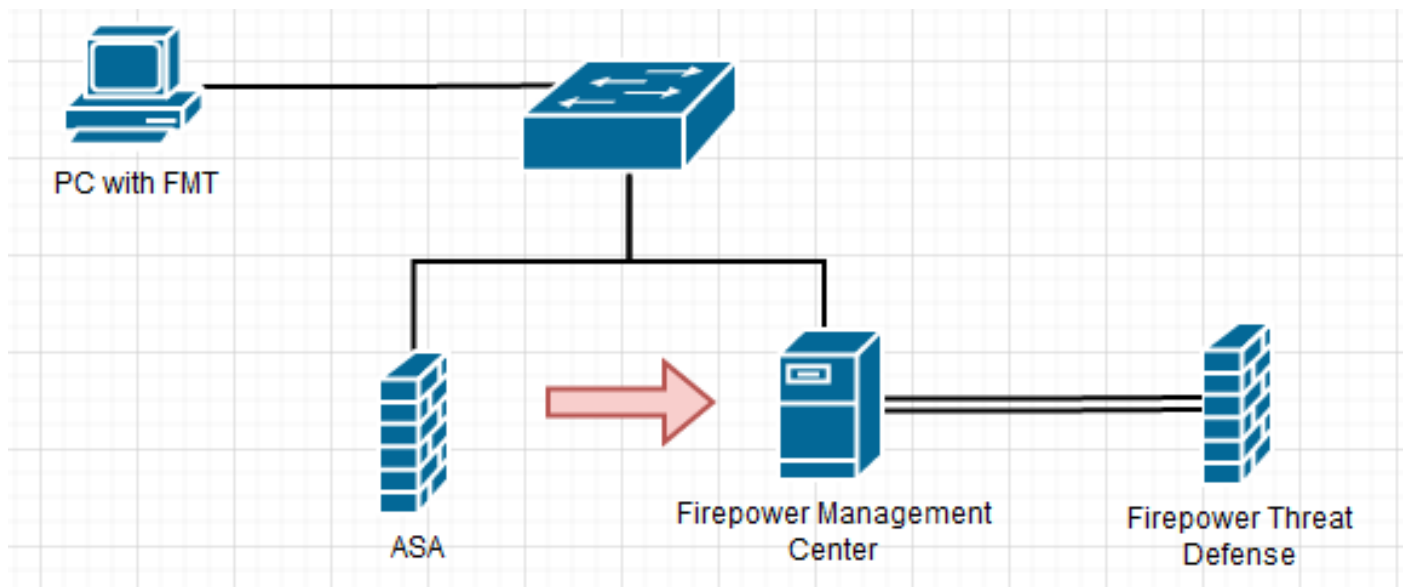
De Firewall Migration Tool ondersteunt deze lijst met apparaten:

- Cisco ASA (8,4+)
- Cisco ASA (9.2.2+) met FPS
- Controlepunt (r75-r77)
- Controlepunt (r80)
- Fortinet (5,0+)
- Palo Alto-netwerken (6.1+)

Voordat u doorgaat met de migratie, moet u rekening houden met de [Richtlijnen en Beperkingen voor de Firewall Migration Tool](#).

Configureren

Netwerkdigram



Configuratiestappen

1. **Download** de meest recente Firepower Migration Tool van Cisco Software Central:

Software Download

Downloads Home / Security / Firewalls / Next-Generation Firewalls (NGFW) / Secure Firewall Threat Defense Virtual / Firepower Migration Tool (FMT) - 3.0.1

Expand All Collapse All

Latest Release

- 3.0.1
- 2.5.3

All Release

- 3
- 2

Secure Firewall Threat Defense Virtual

Release 3.0.1

My Notifications

Related Links and Documentation

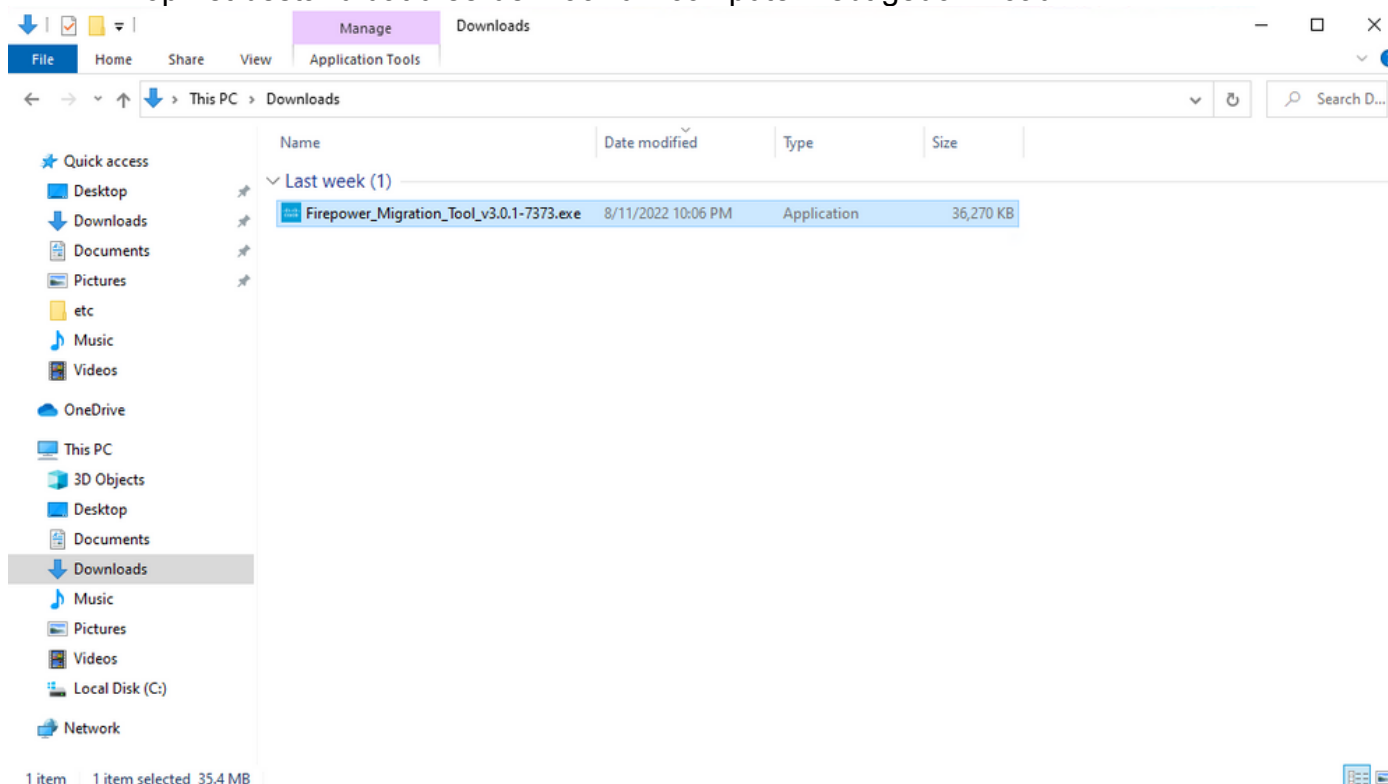
[Open Source](#)

[Release Notes for 3.0.1](#)

[Install and Upgrade Guides](#)

File Information	Release Date	Size	Actions
The extractor will be used to extract checkpoint device-specific configurations which will be used as an input to Firepower Migration Tool. FMT-CP-Config-Extractor_v3.0.1-7373.exe Advisories	10-Aug-2022	9.83 MB	
Firepower Migration Tool 3.0.1 for Mac Firepower_Migration_Tool_v3.0.1-7373.command Advisories	10-Aug-2022	34.75 MB	
Firepower Migration Tool 3.0.1 for Windows Firepower_Migration_Tool_v3.0.1-7373.exe Advisories	10-Aug-2022	35.42 MB	

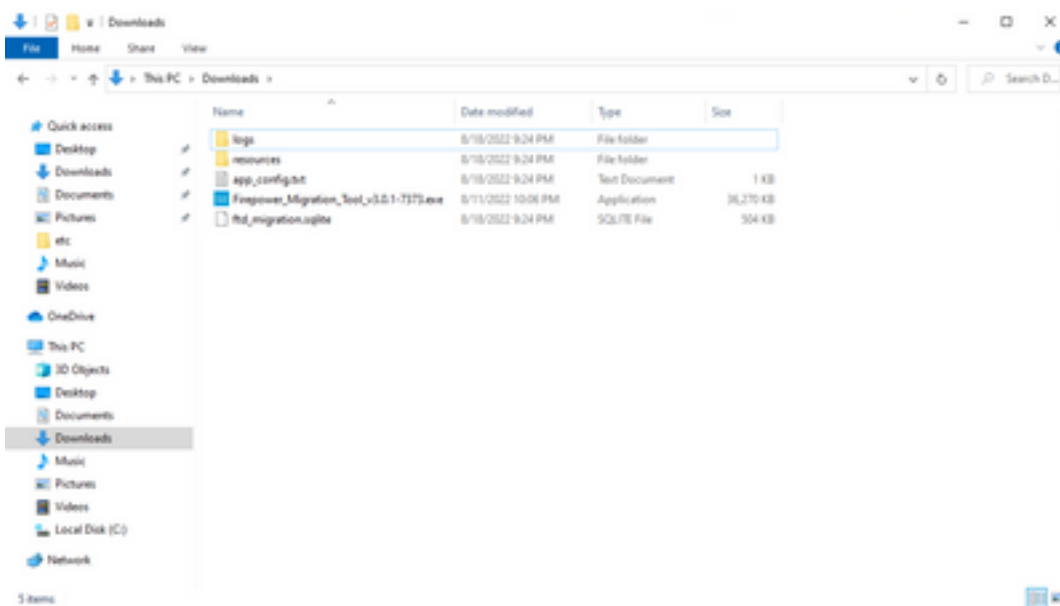
2. Klik op het bestand dat u eerder naar uw computer hebt gedownload.



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

```
C:\Users\cali\Downloads\Firepower_Migration_Tool_v1.0.1-7373.exe
2022-08-18 21:24:49,752 [INFO] __init__ > "Initializing..."
2022-08-18 21:24:49,767 [INFO] settings > "Settings:[global_suffix]"
2022-08-18 21:24:50,189 [INFO] tool_version > "toolVersion:[0817373]"
2022-08-18 21:24:50,252 [INFO] __init__ > "Initializing..."
2022-08-18 21:24:51,252 [INFO] config > "loading settings"
2022-08-18 21:24:51,268 [INFO] client > "Getting ssl context for auth server"
2022-08-18 21:24:51,299 [INFO] tools > "Not verifying ssl certificates"
2022-08-18 21:24:51,299 [INFO] client > "No discovery url configured, all endpoints needs to be configured manually"

2022-08-18 21:24:51,314 [INFO] settings > "Disabled console quick edit mode"
2022-08-18 21:24:51,314 [DEBUG] common > "session table records count:1"
2022-08-18 21:24:51,314 [INFO] common > "Using port: 8888"
2022-08-18 21:24:51,799 [INFO] run > "***** Starting server at http://localhost:8888 *****"
 * Running on http://localhost:8888/ (Press CTRL+C to quit)
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /styles.a0d79d8031ca159b236f.bundle.css HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /inline.318b58c57b4eba3d437b.bundle.js HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /cui-font.880241c8aa87aa899c6a.woff2 HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /polyfills.76c2f21d4e2a1188f46c.bundle.js HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /main.777e77bd49fe82694a1a.bundle.js HTTP/1.1" 200 -
2022-08-18 21:24:57,675127.0.0.1 - - [18/Aug/2022 21:24:57] "GET /assets/cisco.svg HTTP/1.1" 200 -
[INFO] cco_login > "USA check for an user"
2022-08-18 21:24:57,704 [DEBUG] common > "session table records count:1"
127.0.0.1 - - [18/Aug/2022 21:24:57] "GET /api/eula_check HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:57] "GET /assets/icons/login.png HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:58] "GET /assets/images/1.png HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:58] "GET /assets/images/3.png HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:58] "GET /assets/images/2.png HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:58] "GET /favicon.ico HTTP/1.1" 200 -
```



3. Nadat u het programma hebt uitgevoerd, wordt er een webbrowser geopend die de 'Gebruiksrechtovereenkomst' weergeeft. Vink het aanvinkvakje aan om de voorwaarden te aanvaarden. 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 is illegal to copy, modify, or otherwise use the Software for any purpose other than the intended use. You are not licensed to Use the Software for any other purpose.

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

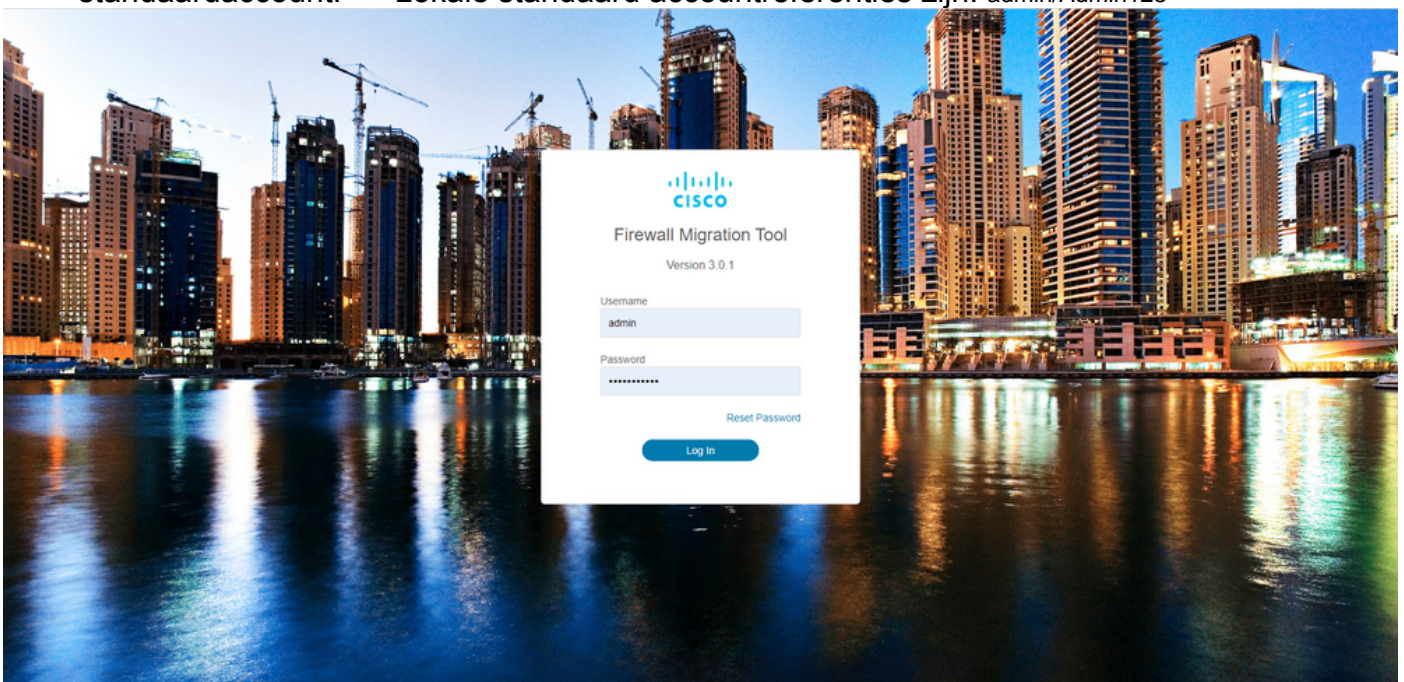


Extract Source Information

Any additional information explaining this



4. Log in op het migratietool. U kunt inloggen met de CCO-account of met de lokale standaardaccount. Lokale standaard accountreferenties zijn: admin/Admin123



5. Selecteer de te migreren bronfirewall. In dit voorbeeld wordt Cisco ASA (8.4+) gebruikt als bron.

Select Source Configuration

Source Firewall Vendor

- Cisco ASA (8.4+)
- Cisco ASA (9.2.2+) with FPS
- Check Point (75-77)
- Check Point (80)
- Fortinet (5.0+)
- Palo Alto Networks (6.1+)

Cisco ASA (8.4+) Pre-Migration Instructions

1 This migration may take a while. Do not make any changes to the Firepower Management Center (FMC) when migration is in progress.

Acronyms used:

FMT: Firewall Migration Tool

FMC: Firepower Management Center

FTD: Firepower Threat Defense

Before you begin your Adaptive Security Appliance (ASA) to Firepower Threat Defense migration, you must have the following items:

- **Stable IP Connection:**
Ensure that the connection is stable between FMT and FMC.
- **FMC Version:**
Ensure that the FMC version is 6.2.3 or later. For optimal migration time, improved software quality and stability, use the suggested release for your FTD and FMC. Refer to the gold star on CCO for the suggested release.
- **FMC Account:**
Create a dedicated user account with administrative privileges for the FMT and use the credentials during migration.
- **FTD (Optional):**
To migrate the device configurations like interfaces, routes, and so on, add the target device to FMC. Skip this step if you want to migrate only the shared configurations like objects, NAT, ACL, and so on.
- **ASA Configuration Requirements:**
Export configuration file from ASA to .cfg or .txt format. Connect to live ASA to extract the configuration file for one or more contexts. To migrate following features in ASA:
 1. **Time Based ACLs:** FMC and FTD must be on 6.6 or later versions.
 2. **IP SLA Monitor:** FMC must be on 6.6 or later and FTD must be on 6.2.3 or later.
 3. **Object Group Search:** FMC and FTD must be on 6.6 or later versions.
 4. **ASA5505 Support:** FMC and FTD must be on 6.6 or later versions.
 5. **Remote Deployment:** FMC and FTD must be on 6.7 or later versions. If remote deployment is enabled, Firewall Migration Tool will only migrate ACLs, Network Object and Port Objects. Interface and Route configuration have to be migrated manually on to FMC.
 6. **Site-to-Site VPN Tunnels:** Policy Based (Crypto Map) VPN needs FMC and FTD to be on 6.6 or later. Route Based (VTI) Support, FMC and FTD to be on 6.7 or later. Ensure FTD must be added to FMC before migration. Firewall Migration Tool will migrate VPN tunnels as Point-to-Point network

6. Selecteer de extractiemethode die gebruikt moet worden om de configuratie te verkrijgen. Handmatig uploaden vereist dat u de **Running Config** bestand van de ASA in ".cfg"- of ".txt"-formaat. Verbind met de ASA om configuraties rechtstreeks uit de firewall te halen.

1 2 3 4 5 6

Extract ASA Information Select Target Map FTD Interface Map Security Zones & Interface Groups Optimize, Review & Validate Complete Migration

Extract Cisco ASA (8.4+) Information
Source: Cisco ASA (8.4+)

Extraction Methods

Manual Upload

- File format is '.cfg' or '.txt'.
- For Multi-context upload a show tech.
For Single-context upload show running.

⚠ Do not upload hand coded configurations.

Upload

Connect to ASA

- Enter the management IP address and connect using admin credentials.
- IP format should be: <IP>Port>.

ASA IP Address/Hostname

Connect

Context Selection >

Parsed Summary >

Back

Next

Opmerking: Sluit bijvoorbeeld rechtstreeks aan op de ASA.

7. Een samenvatting van de configuratie gevonden op de firewall wordt weergegeven als een dashboard, klik op **Volgende**.

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.

8. Selecteer het beoogde VCC dat bij de migratie moet worden gebruikt. Verstrek de IP 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 >

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](#)

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

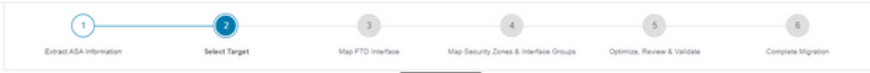
Select Features >

Device Configuration	Shared Configuration	Optimization
<input checked="" type="checkbox"/> Interfaces	<input checked="" type="checkbox"/> Access Control	<input checked="" type="checkbox"/> Migrate Only Referenced Objects
<input checked="" type="checkbox"/> Routes	<input checked="" type="checkbox"/> Populate destination security zones	<input checked="" type="checkbox"/> Object Group Search ⓘ
<input checked="" type="checkbox"/> Static	⚠️ Route-lookup logic is limited to Static Routes and Connected Routes. PBR, Dynamic-Routes & NAT are not considered.	Inline Grouping
<input type="checkbox"/> BGP	<input checked="" type="checkbox"/> Migrate tunnelled rules as Prefilter	<input checked="" type="checkbox"/> CSM/ASDM
<input type="checkbox"/> EIGRP	<input type="checkbox"/> NAT (no data)	
<input type="checkbox"/> Site-to-Site VPN Tunnels (no data)	<input checked="" type="checkbox"/> Network Objects (no data)	
<input type="checkbox"/> Policy Based (Crypto Map)	<input type="checkbox"/> Port Objects (no data)	
<input type="checkbox"/> Route Based (VTI)	<input type="checkbox"/> Access List Objects(Standard, Extended)	
	<input type="checkbox"/> Time based Objects (no data)	
	<input type="checkbox"/> Remote Access VPN	
	⚠️ Remote Access VPN migration is supported on FMC/FTD 7.2 and above.	

[Proceed](#)

[Back](#) [Next](#)

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

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

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 (Standard, Extended used in BGPRAVPNEIGRP)	1 Network Objects	0 Port Objects	0 Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)
0 Network Address Translation	1 Logical Interfaces	1 Routes	0 Site-to-Site VPN Tunnels	0 Remote Access VPN (Connection Profiles)

Back Next

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.

I. 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	aaalive_ciscoasa_2022-08-19_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
Hic 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

13. Breng de ASA interfaces met de FTD interfaces in kaart via 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 |< 4 Page 1 of 1 >|

Back Next

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

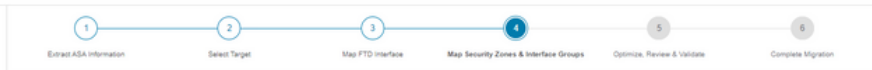
ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
management	GigabitEthernet0/0	Select Security Zone	Select Interface Groups

Add SZ & IG Auto-Create

10 per page 1 to 1 of 1 Page 1 of 1

Back Next

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

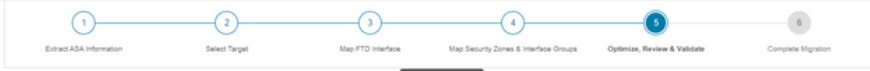
ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
management	GigabitEthernet0/0	management	management_ig (A)

Add SZ & IG Auto-Create

10 per page 1 to 1 of 1 Page 1 of 1

Back Next

- Bekijk en valideer de configuraties die op de Migration Tool moeten worden gemigreerd. 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

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

Validation Status

Successfully Validated

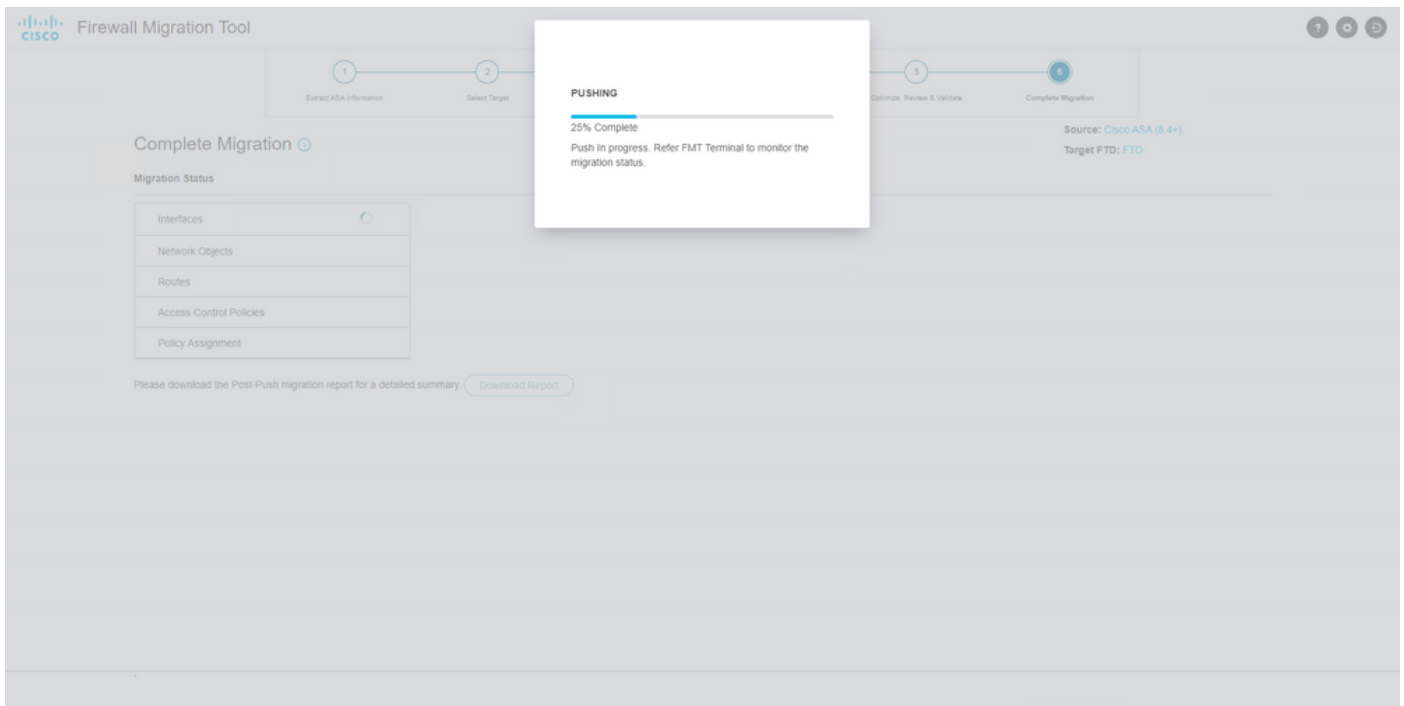
Validation Summary (Pre-push)

0 Access Control List Lines	Not selected for migration Access List Objects (Standard, Extended used in BGP/RAV/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)

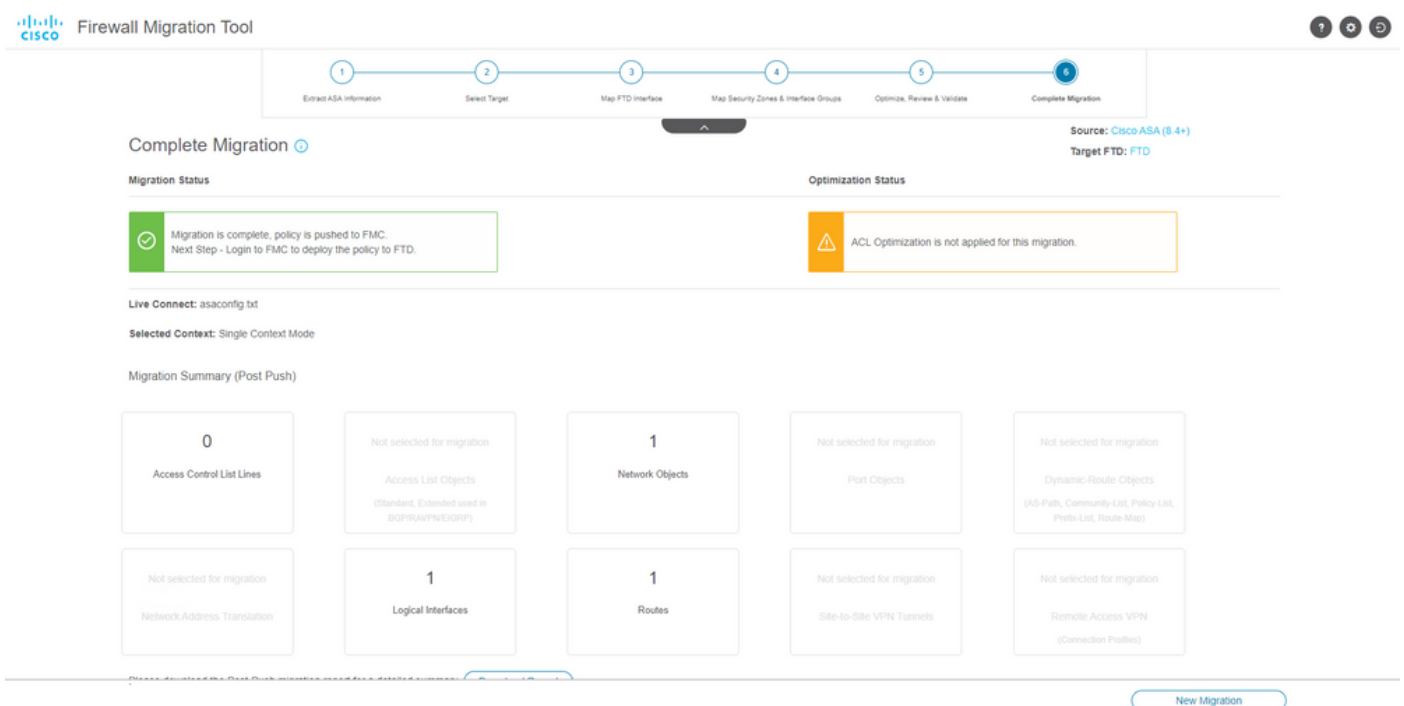
Note: The configuration on the target FTD device FTD (192.168.1.17) will be overwritten as part of this migration.

Push Configuration

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



Voorbeeld van een geslaagde migratie, zoals in de afbeelding:



- (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 om de configuratie te kunnen implementeren: Log in op de GUI van het VCC. Naar het Deploy tabblad. Selecteer de implementatie om de configuratie naar de firewall te duwen. Klik Deploy.

The screenshot shows the Cisco Firepower Management Center interface. At the top, there is a navigation bar with the following tabs: Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. The current page is titled "Deploy / Deployment" and includes a "Deploy" button in the top right corner. Below the navigation bar is a search bar with the text "Search using device name, type, domain, group or status".

Device	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
FTD		FTD		8/13/2022, 6:01:52 PM		Pending

Below the table is a tree view of configurations:

- Device Configurations
 - Interface Policy
 - Advanced Settings
 - Routing Group
 - IPv4 Static Route Policy

At the bottom of the interface, there is a "How To" button.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Controleer de logbestanden in de map waarin het bestand Firepower Migration Tool is geplaatst, bijvoorbeeld:

Firepower_Migration_Tool_v3.0.1-7373.exe/logs/log_2022-08-18-21-24-46.log

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.