

FTD configureren vanuit ASA Configuration File met FirePOWER Migratietool

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Verifiëren](#)

[Bekende bogen gerelateerd aan het FirePOWER-migratietool](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt een voorbeeld beschreven van adaptieve security applicatie (ASA) naar Firepower Threat Defense (FTD) migratie op FPR4145.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van ASA
- Kennis van FireSIGHT Management Center (FMC) en FTD

Gebruikte componenten

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

- ASA versie 9.12(2)
- FTD versie 6.7.0
- FMC versie 6.7.0
- Firepower Migration Tool versie 2.5.0

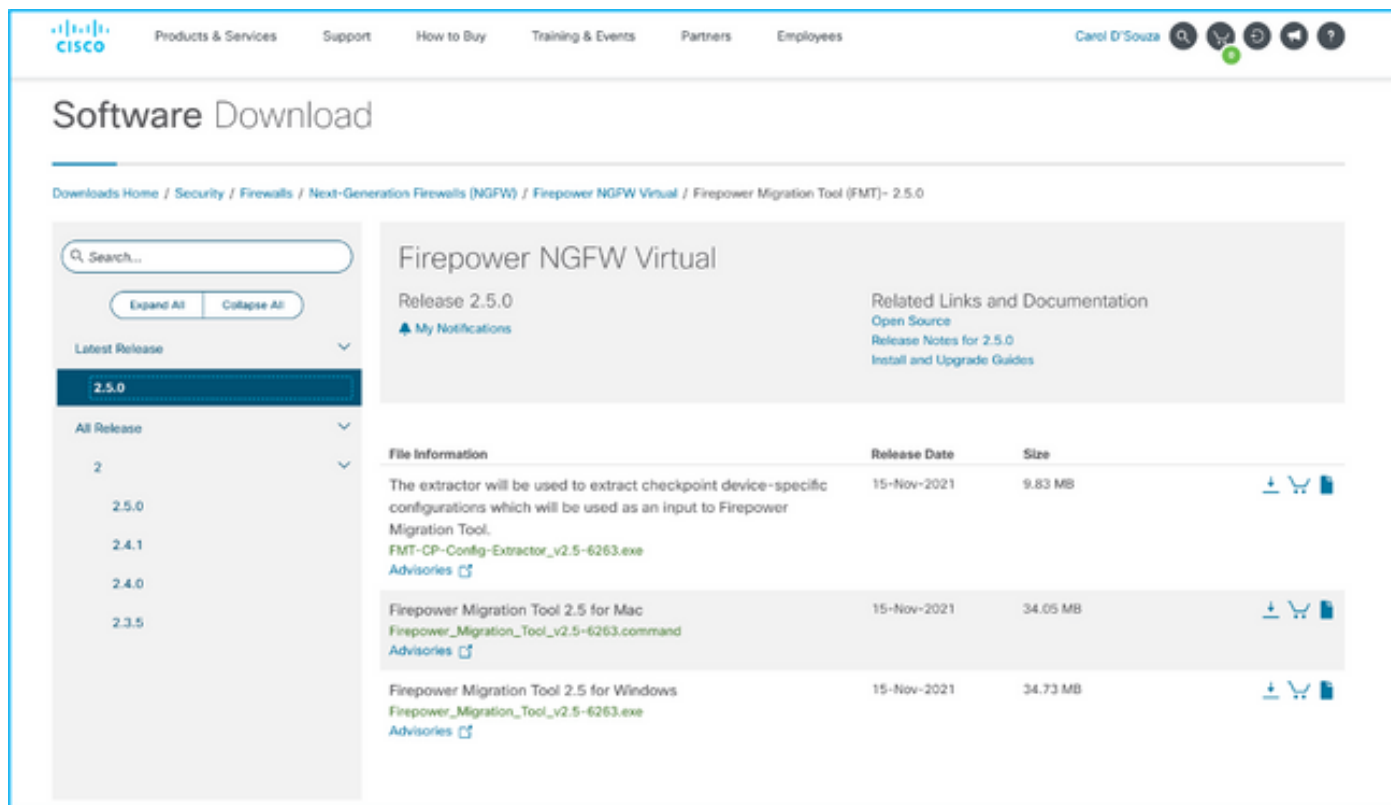
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

ASA-configuratiebestand exporteren in **.cfg**- of **.txt**-formaat. Het VCC moet worden ingezet met een onder het VCC geregistreerd FTD.

Configureren

1. Download het Firepower Migration Tool van software.cisco.com zoals in de afbeelding.



The screenshot shows the Cisco Software Download page for Firepower NGFW Virtual, Release 2.5.0. The page includes a search bar, a list of releases (2.5.0, 2.4.1, 2.4.0, 2.3.5), and a table of file information for the migration tool.

File Information	Release Date	Size
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_v2.5-6263.exe Advisories	15-Nov-2021	9.83 MB
Firepower Migration Tool 2.5 for Mac Firepower_Migration_Tool_v2.5-6263.command Advisories	15-Nov-2021	34.05 MB
Firepower Migration Tool 2.5 for Windows Firepower_Migration_Tool_v2.5-6263.exe Advisories	15-Nov-2021	34.73 MB

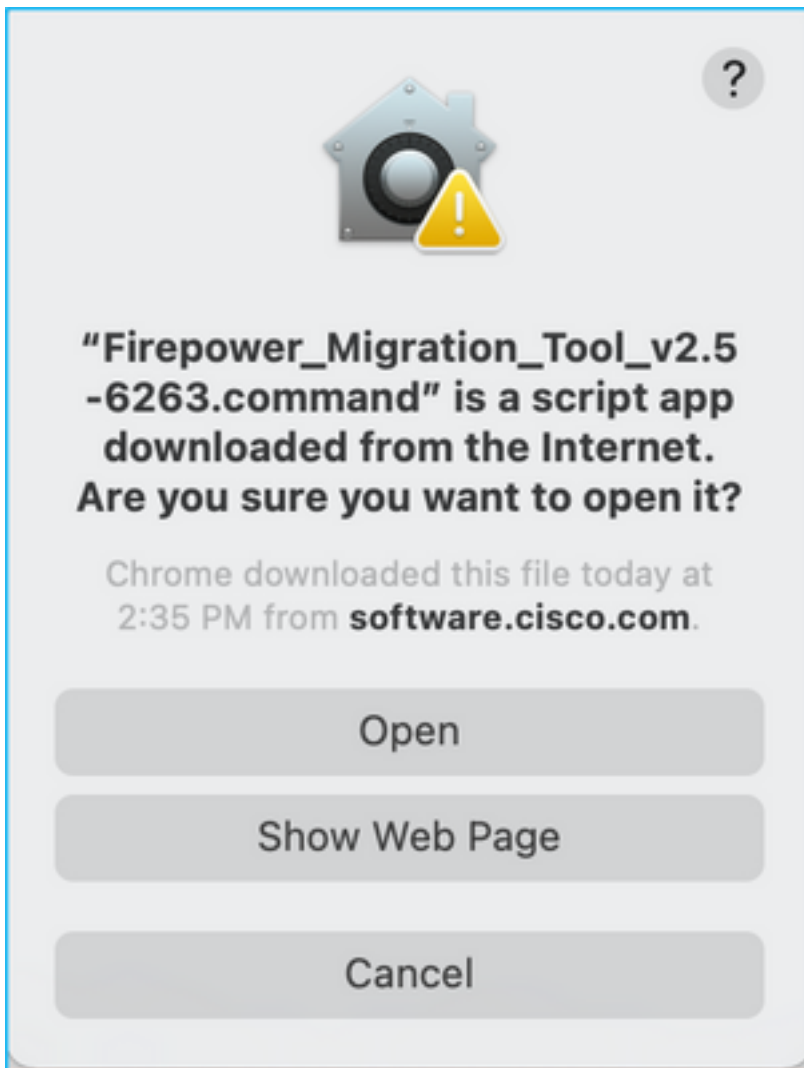
2. De eisen van de [richtsnoeren en beperkingen](#) voor het onderdeel Firepower Migration Tool opnieuw bekijken en controleren.

3. Indien u van plan bent een groot configuratiebestand te migreren, moet u de slaapstand-instellingen configureren zodat het systeem niet in slaap gaat tijdens een migratiestroom.

3.1. Vink voor Windows naar Aan/uit-opties in het bedieningspaneel. Klik op **Wijzigen** naast uw huidige energieplan. Wijzig **de computer in slaap tot nooit**. Klik op **Wijzigingen opslaan**.

3.2. Voor MAC, navigeer naar **stelselvoorkeuren > Energiebesparing**. Vink het vakje naast elkaar aan om te voorkomen dat de computer automatisch slaapt wanneer het display uit is en sleep het **display uit** nadat de schuifschakelaar is **uitgeschakeld** naar Nooit.

Opmerking: Deze waarschuwing verschijnt wanneer MAC-gebruikers proberen het gedownloade bestand te openen. Negeer dit en volg Stap 4 A.



4. A. Voor MAC - gebruik de terminal en voer deze opdrachten uit.

```
CAROLDSO-M-WGYT:~ caroldso$ cd Downloads/  
CAROLDSO-M-WGYT:Downloads caroldso$ chmod 750 Firepower_Migration_Tool_v2.5-6263  
.command  
CAROLDSO-M-WGYT:Downloads caroldso$ ./Firepower_Migration_Tool_v2.5-6263.command  
  
[75653] PyInstaller Bootloader 3.x  
[75653] LOADER: executable is /Users/caroldso/Downloads/Firepower_Migration_Tool  
_v2.5-6263.command  
[75653] LOADER: hompath is /Users/caroldso/Downloads  
[75653] LOADER: _MEIPASS2 is NULL  
[75653] LOADER: archivename is /Users/caroldso/Downloads/Firepower_Migration_Too  
l_v2.5-6263.command  
[75653] LOADER: Cookie found at offset 0x219AE08  
[75653] LOADER: Extracting binaries  
[75653] LOADER: Executing self as child
```

```

127.0.0.1 - - [23/Nov/2021 14:49:47] "GET /inline.318b50c57b4eba3d437b.bundle.js
HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:47] "GET /cui-font.880241c0aa87aa899c6a.woff2 H
TTP/1.1" 200 -
2021-11-23 14:49:47,999 [INFO      | cco_login] > "EULA check for an user"
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/cisco.svg HTTP/1.1" 200 -
2021-11-23 14:49:48,013 [DEBUG     | common] > "session table records count:1"
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /api/eula_check HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/icons/login.png HTTP/1.1" 200
-
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/images/1.png HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/images/3.png HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/images/2.png HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /favicon.ico HTTP/1.1" 200 -

```

4. B. Voor Windows - dubbelklik op het Firepower Migration Tool om het te starten in een Google Chrome-browser.

5. Neem de licentie aan zoals in de afbeelding.

← → ↻ 🏠 ⓘ localhost:8888/#/eula

cisco Firepower Migration Tool

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 specic product terms at www.cisco.com/go/softwareterms (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. Unless contrary to applicable law, You are not licensed to Use the Software on

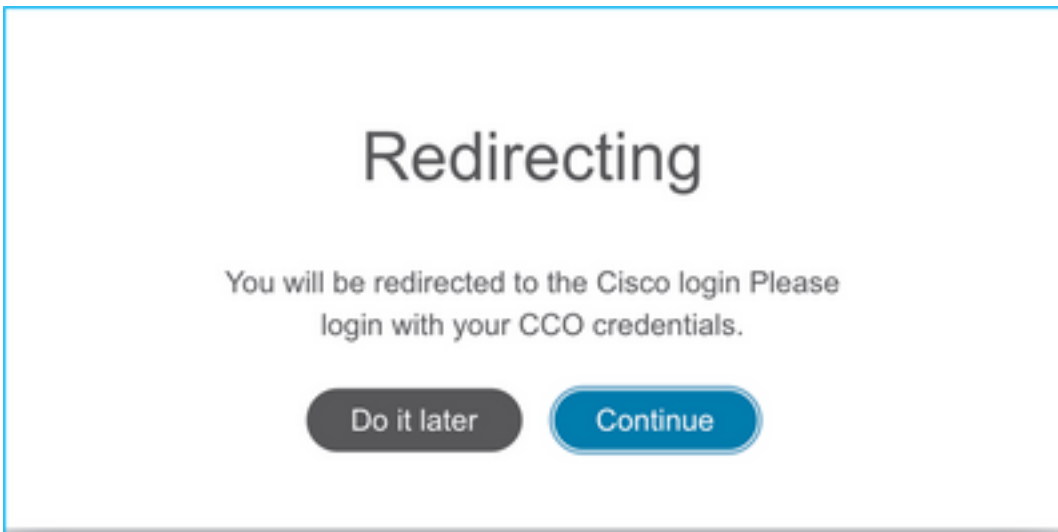
I have read the content of the EULA and SEULA and agree to terms listed.

Proceed

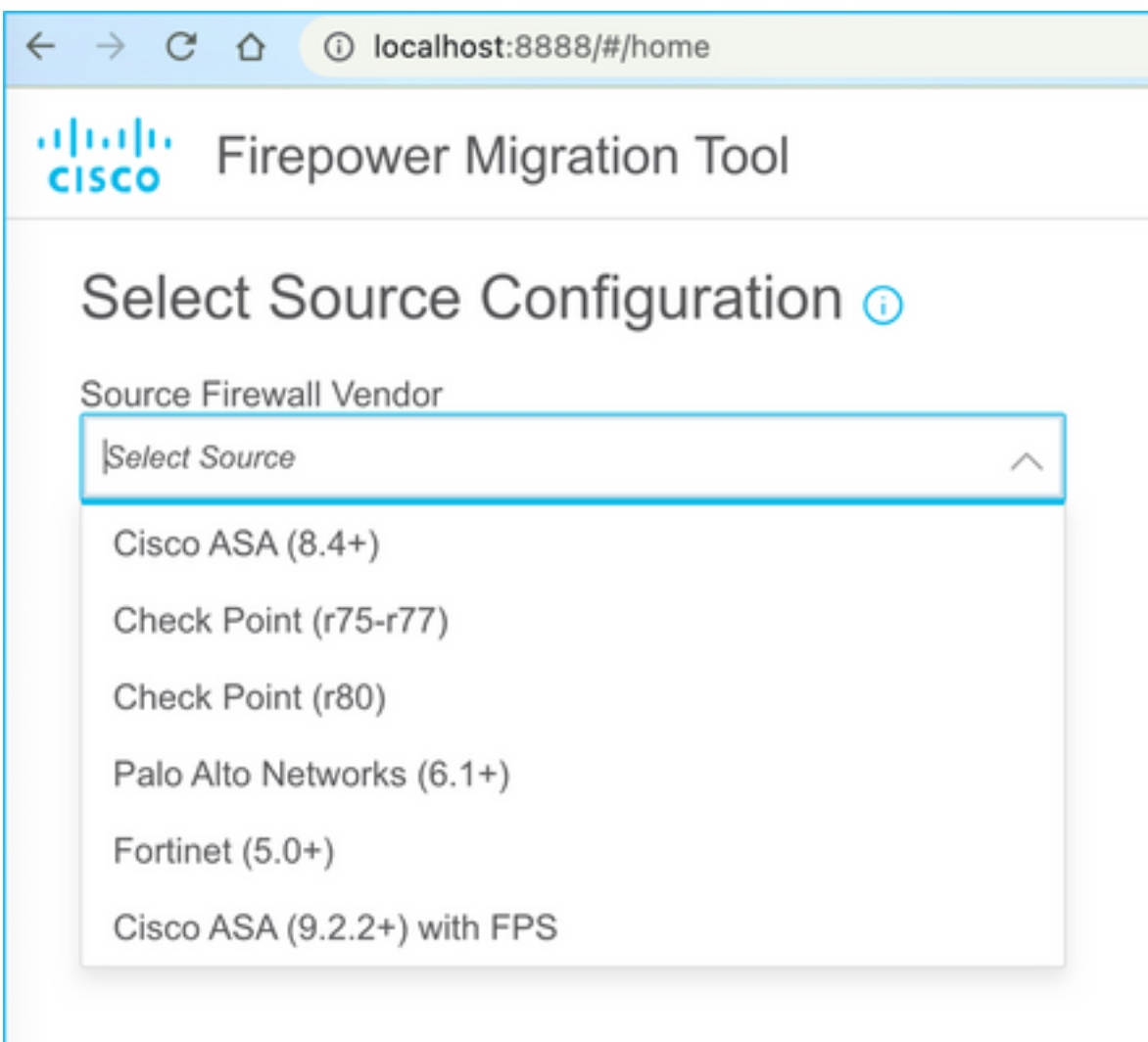
6. Klik op de inlogpagina van de FirePOWER-migratietool op de inlognaam met de CCO-link om aan uw Cisco.com-account te loggen met uw inloggegevens.

Opmerking: Als u geen Cisco.com-account hebt, kunt u dit maken op de inlogpagina van

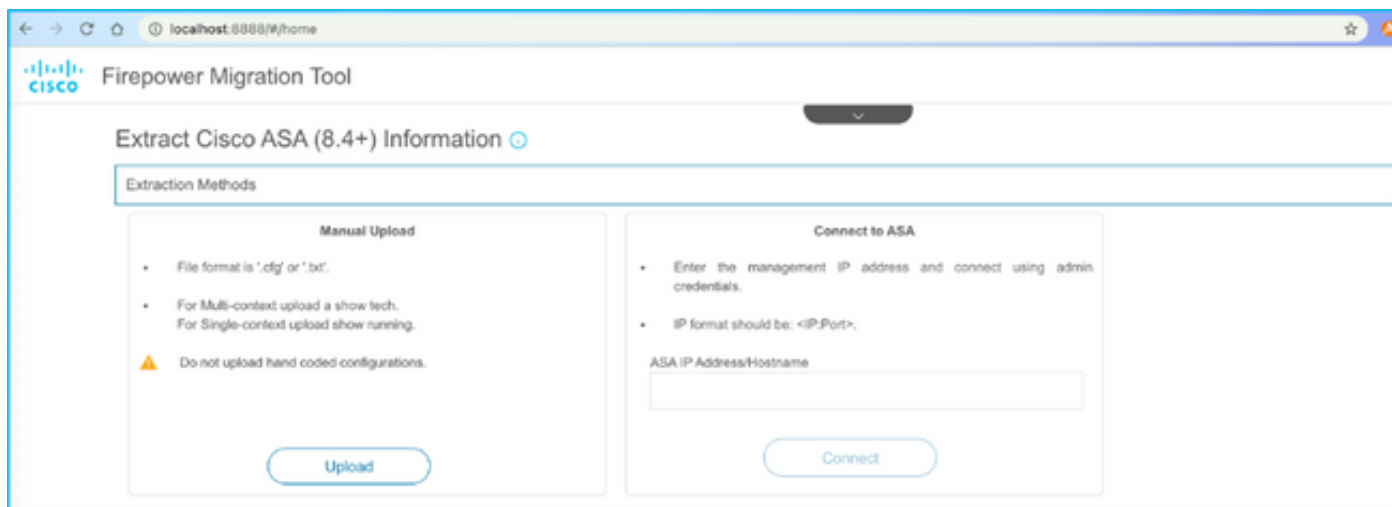
Cisco.com. Inloggen met de volgende standaardaanmeldingsgegevens: Wachtwoord voor gebruikersnaam en beheerder: Admin123.



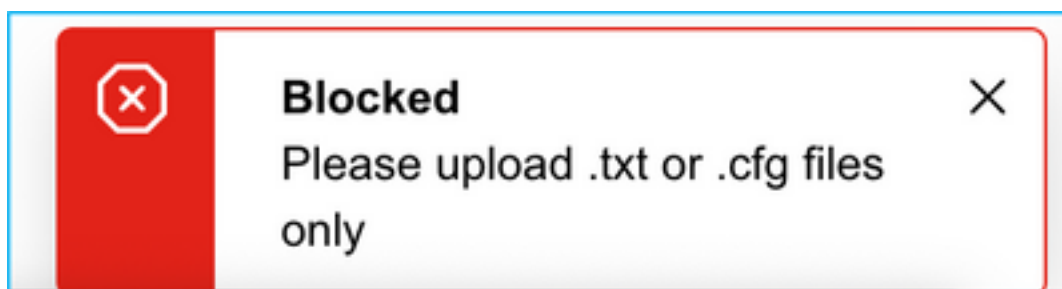
7. Selecteer de bronconfiguratie. In dit scenario is het Cisco ASA (8.4+).



8. Selecteer Handmatig uploaden als u geen verbinding met de ASA hebt. Elders, kunt u de actieve configuratie van de ASA herstellen en de beheers-IP en logindetails invoeren. In ons scenario werd een handmatige uploaden uitgevoerd.

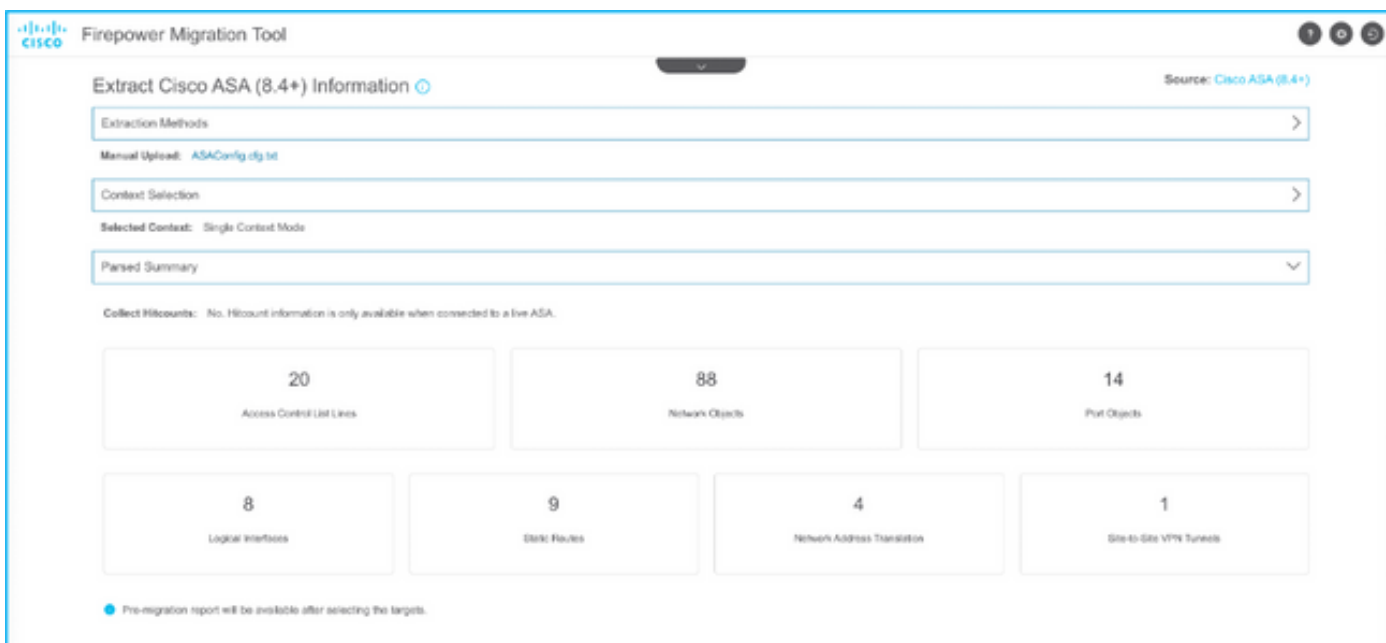


Opmerking: Deze fout wordt weergegeven als het bestand niet wordt ondersteund. Zorg ervoor dat u de indeling in onbewerkte tekst wijzigt. (Fout wordt gezien ondanks het hebben van extensie .cfg).



```
ASAConfig.cfg — Edited
asa# show running-config
: Saved
:
:
: Serial Number: FLM22160652
: Hardware: FPR4K-SM-12, 56533 MB RAM, CPU Xeon E5 series 2200 MHz, 1 CPU (24 cores)
:
ASA Version 9.12(2)
:
hostname asa
enable password ***** pbkdf2
:
license smart
feature tier standard
names
no mac-address auto
:
:
interface Ethernet1/1
no nameif
no security-level
no ip address
:
interface Ethernet1/2
nameif Inside
cts manual
security-level 0
no ip address
:
interface Ethernet1/3
nameif Outside
cts manual
security-level 0
no ip address
```

9. Nadat het bestand is geüpload, worden de elementen geparkeerd met een samenvatting zoals in de afbeelding:



10. Voer de FMC IP- en inlogreferenties in waaraan de ASA-configuratie moet worden gemigreerd. Zorg ervoor dat de FMC IP vanaf uw werkstation bereikbaar is.

Firepower Migration Tool Source: Cisco ASA (8.4+)

Select Target ⓘ

Connect to FMC ▼

FMC IP Address/Hostname
10.106.52.10

Connect

Choose FTD >

Select Features >

Rule Convention/ Process Config >

✕

FMC LOGIN

IP Address/Hostname

10.106.52.10

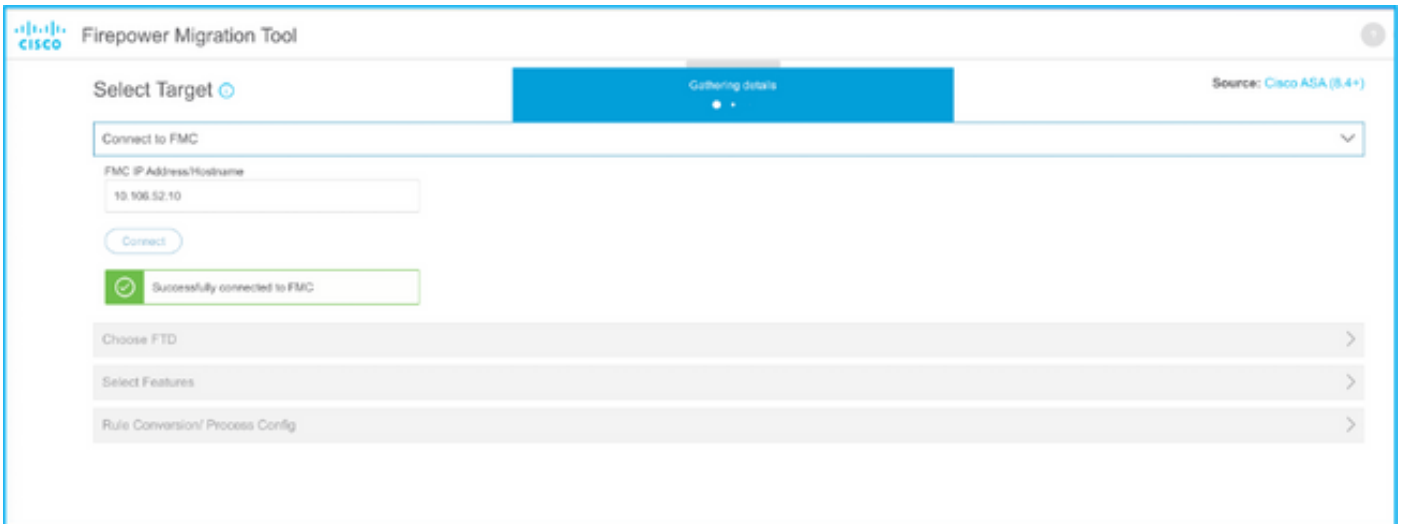
Username

|

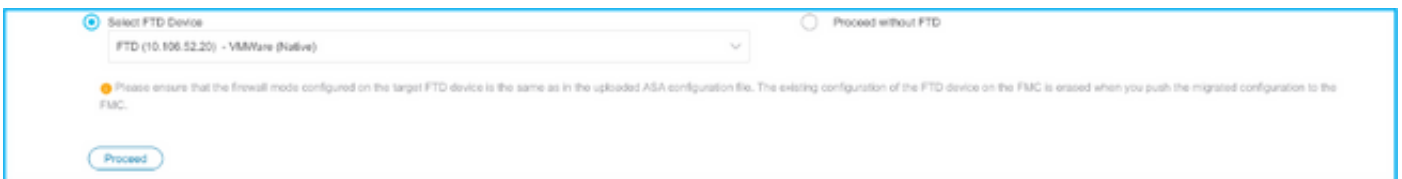
Password

Login

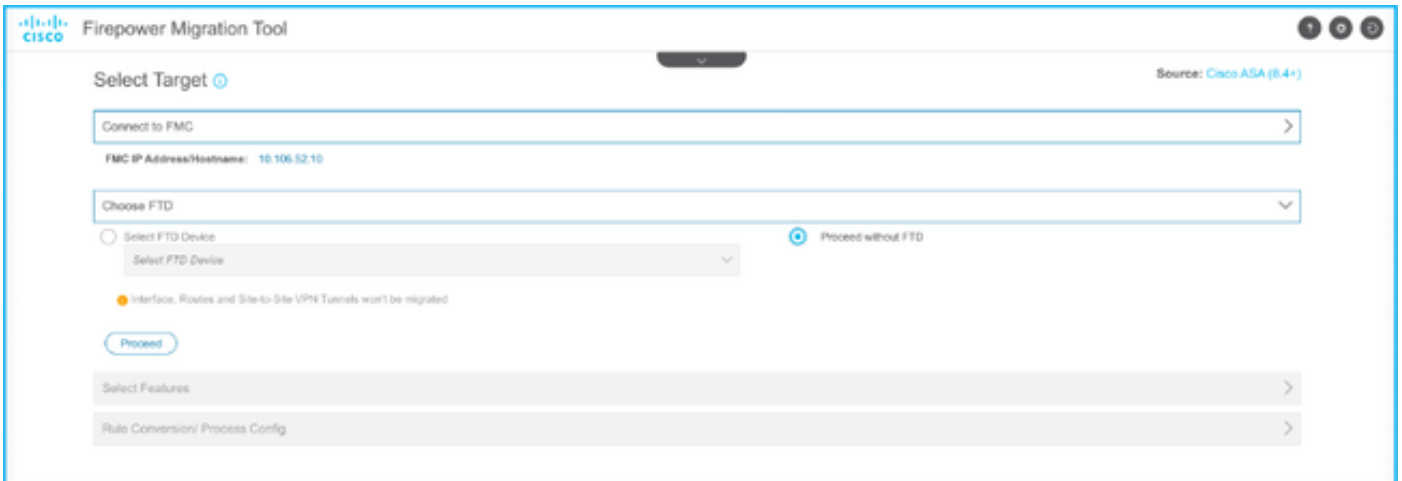
11. Zodra de FMC is aangesloten, worden de onder deze code beheerde FTD's weergegeven.



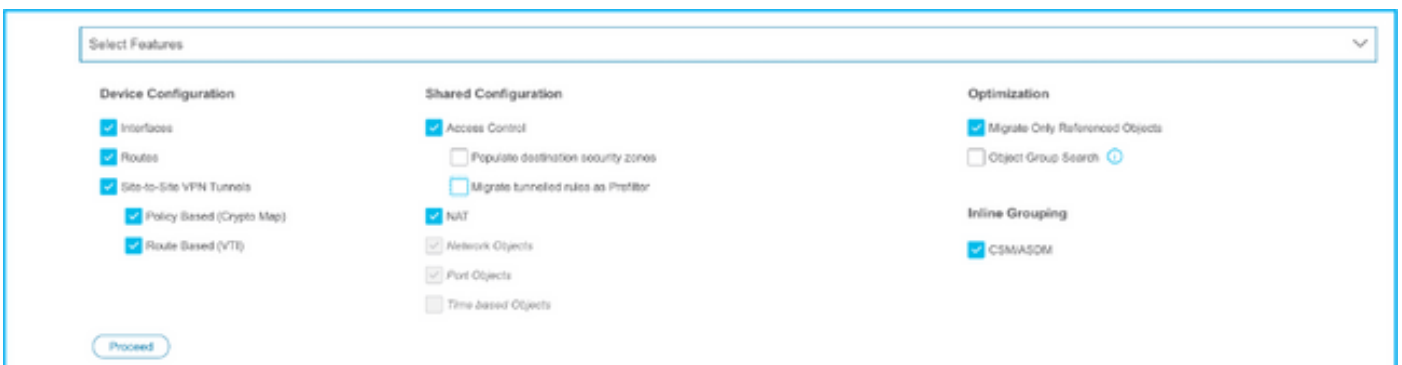
12. Kies de FTD waaraan u de migratie van de ASA-configuratie wilt uitvoeren.



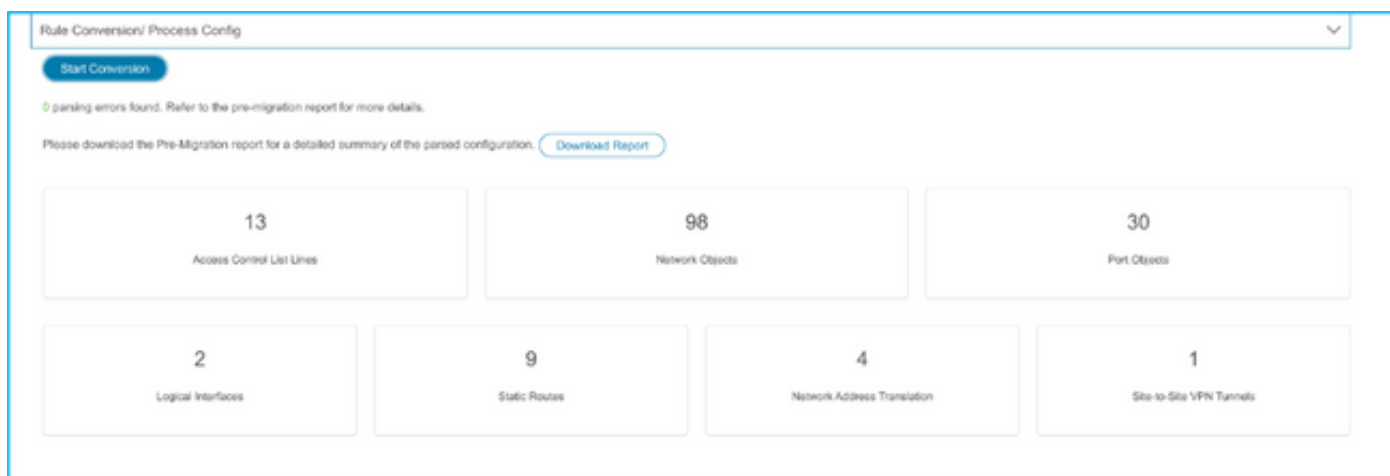
Opmerking: Het wordt aanbevolen het FTD-apparaat te selecteren, anders moeten de interfaces, routes en de site-to-site VPN-configuratie handmatig worden uitgevoerd.



13. Selecteer de functies die moeten worden gemigreerd zoals in de afbeelding.



14. Selecteer **Start Conversion** om de pre-migratie te starten, welke dan de elementen met betrekking tot de FTD configuratie zal bevolken.



The screenshot shows a web interface for 'Rule Conversion/ Process Config'. At the top, there is a 'Start Conversion' button. Below it, a message states '0 parsing errors found. Refer to the pre-migration report for more details.' A 'Download Report' button is also present. The main area displays seven summary cards for different configuration elements:

Element	Count
Access Control List Lines	13
Network Objects	98
Port Objects	30
Logical Interfaces	2
Static Routes	9
Network Address Translation	4
Site-to-Site VPN Tunnels	1

15. Klik op **Download Report** dat eerder is gezien om het Pre-Migration Report te bekijken, zoals in de afbeelding te zien is.

← → ↻ 🏠 📄 File | /Users/caroldso/Downloads/pre_migration_report_asa_2021-11-23_09-41-15.html

CISCO Pre-Migration Report

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 reviewing the configuration 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	Manual
ASA Configuration Name	ASAConfig.cfg.txt
ASA Version	9.12(2)
ASA Hostname	asa
ASA Device Model	FPR4K-SM-12, 56533 MB RAM, CPU Xeon E5 series 2200 MHz, 1 CPU (24 cores)
Hit Count Feature	No
IP SLA Monitor	0
Total Extended ACEs	13
ACEs Migratable	13
Site to Site VPN Tunnels	1
Logical Interfaces	2
Network Objects and Groups	98
Service Objects and Groups	30
Static Routes	9
NAT Rules	4

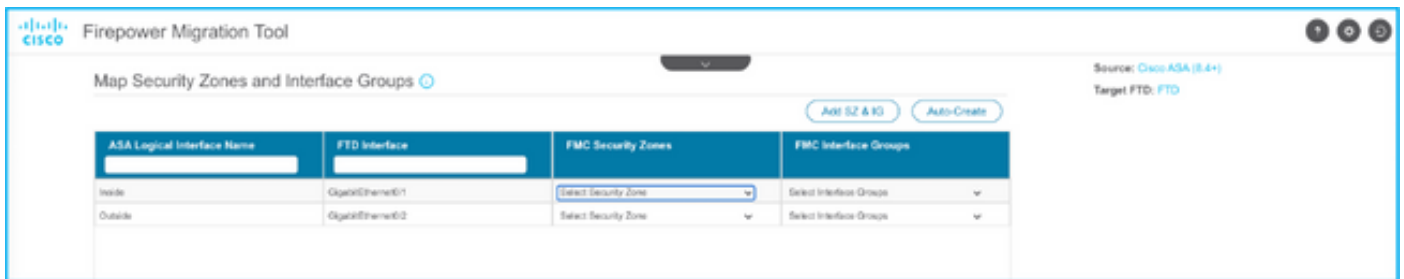
Note: ACEs that are applied outbound or not attached to interfaces using the access-group command are ignored.

16. Stel ASA interfaces op FTD in zoals vereist in de afbeelding.

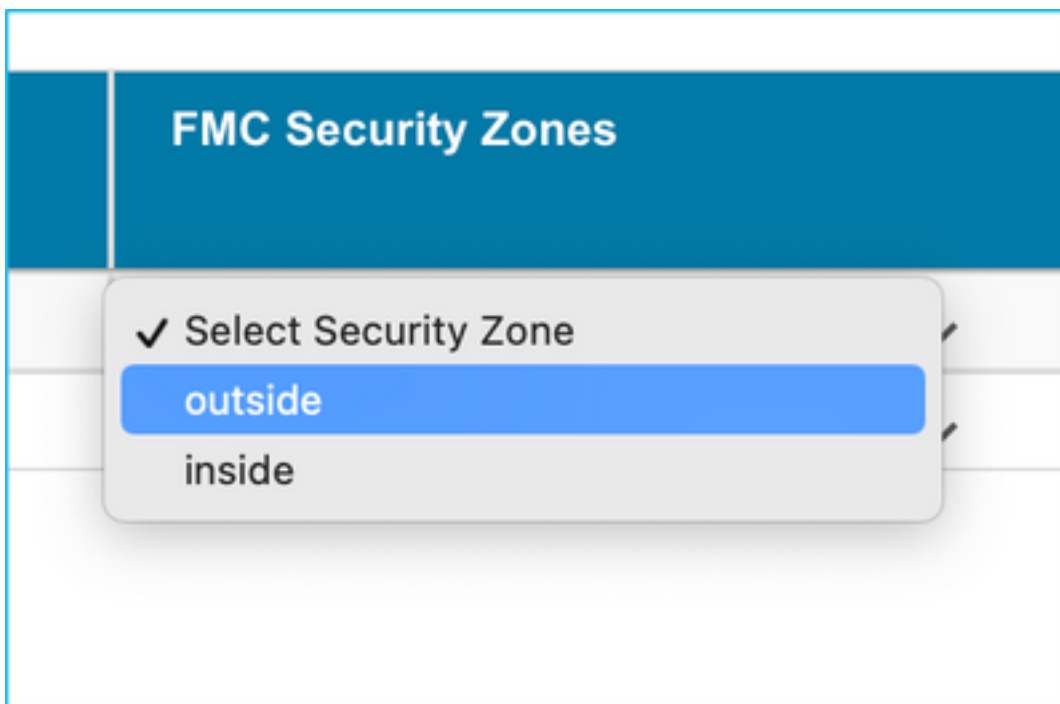
Refresh

ASA Interface Name	FTD Interface Name
Ethernet1/2	Select Interface
Ethernet1/3	GigabitEthernet0/0
	GigabitEthernet0/1
	✓ GigabitEthernet0/2

17. Toewijzen van beveiligingszones en interfacegroepen aan de FTD-interfaces.



A. Als het FMC al beveiligingszones en interfacegroepen heeft gecreëerd, kunt u deze naar wens selecteren:



B. Als er een noodzaak is om beveiligingsgebieden en een interfacegroep te maken, klikt u op **Add SZ & IG** zoals in de afbeelding.

✕

Add SZ & IG

Security Zones (SZ) Interface Groups (IG)

Add

i

Max 48 characters for Interface Group name. Allowed special characters are _.-+

Interface Groups	Type	Actions
<input style="width: 100%;" type="text" value="Inside"/>	ROUTED	✕ ✓

0 - 0 of 0 |< < > >|

Close

C. Else, kunt u voor optie **Auto-Maken** gaan die veiligheidszones en interfacegroepen met de naam **ASA logische interface_sz** en **ASA logische interface_ig** respectievelijk zullen creëren.

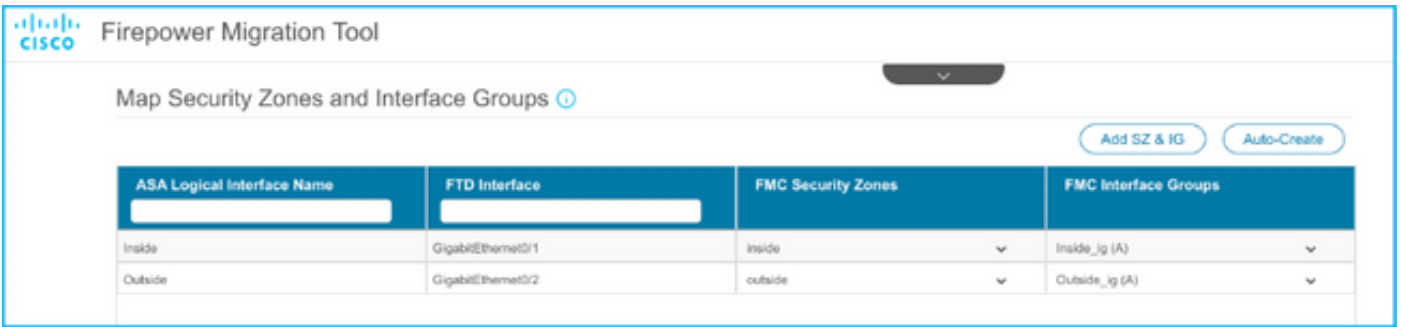
Auto-Create

Auto-create maps ASA interfaces to existing FTD security zones and interface groups in FMC that have the same name. If no match is found, the Migration Tool creates a new FTD security zone and interface group with the same name in FMC.

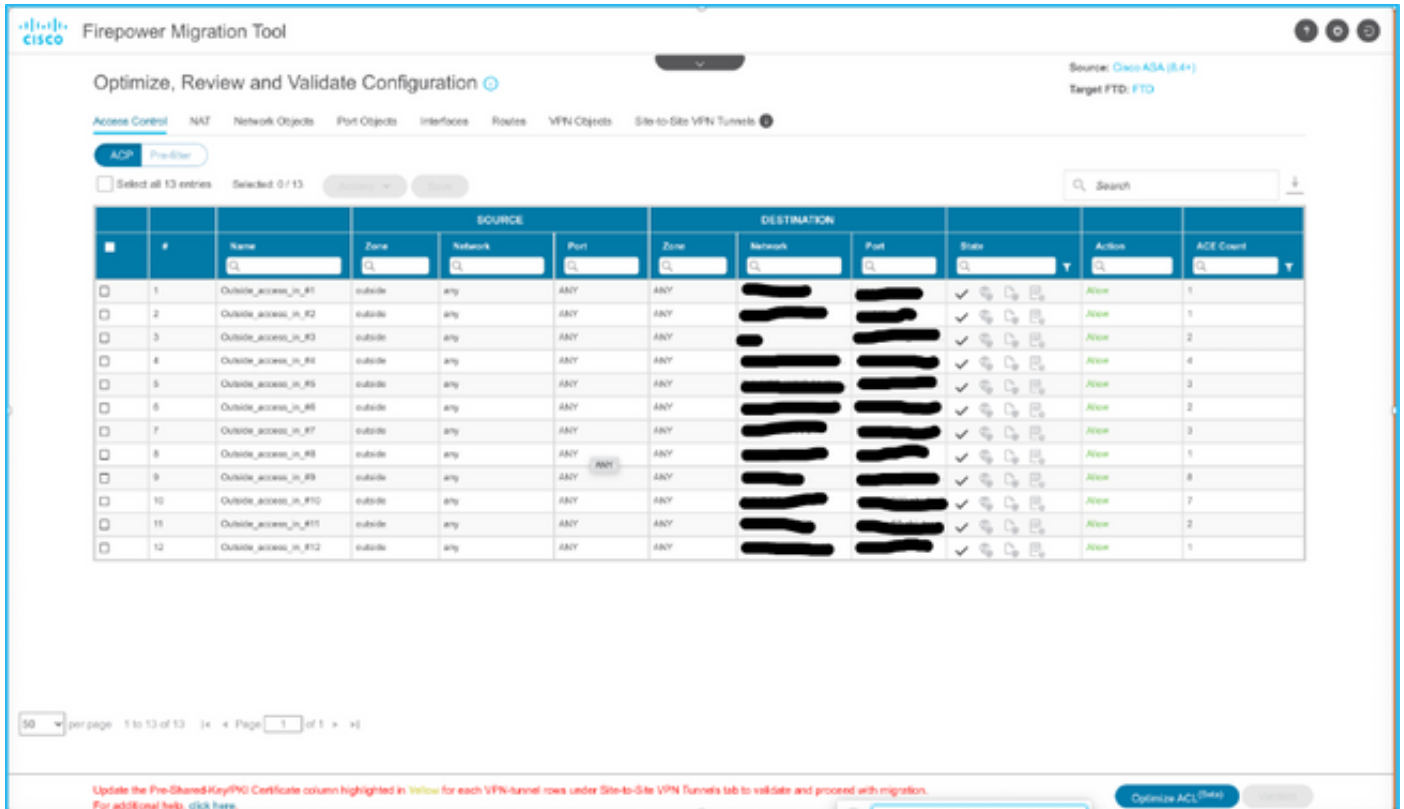
Select the objects that you want to map to ASA interfaces

Security Zones Interface Groups

CancelAuto-Create



18. Evalueer en validering van elk van de nieuwe FTD-elementen. Waarschuwingen worden in rood weergegeven zoals in de afbeelding.



19. De migratieacties kunnen worden geselecteerd zoals in de afbeelding, als u een regel wilt bewerken. FTD-functies van het toevoegen van bestanden en IPS-beleid kunnen in deze stap worden uitgevoerd.

ACP Pre-filter

Select all 13 entries Selected: 13 / 13 Actions Save

<input checked="" type="checkbox"/>	#	Name	MIGRATION ACTIONS		SOURCE
<input checked="" type="checkbox"/>	1	Outside_access_in_#1	Do not migrate		network
<input checked="" type="checkbox"/>	2	Outside_access_in_#2	RULE ACTIONS		
<input checked="" type="checkbox"/>	3	Outside_access_in_#3	File Policy		
<input checked="" type="checkbox"/>	4	Outside_access_in_#4	IPS Policy		
<input checked="" type="checkbox"/>	5	Outside_access_in_#5	Log		
<input checked="" type="checkbox"/>	6	Outside_access_in_#6	outside	any	

Opmerking: Als het bestandsbeleid al in het FMC bestaat, worden deze ingevuld zoals in de afbeelding. Hetzelfde geldt voor IPS-beleid en het standaardbeleid.

✕

File Policy

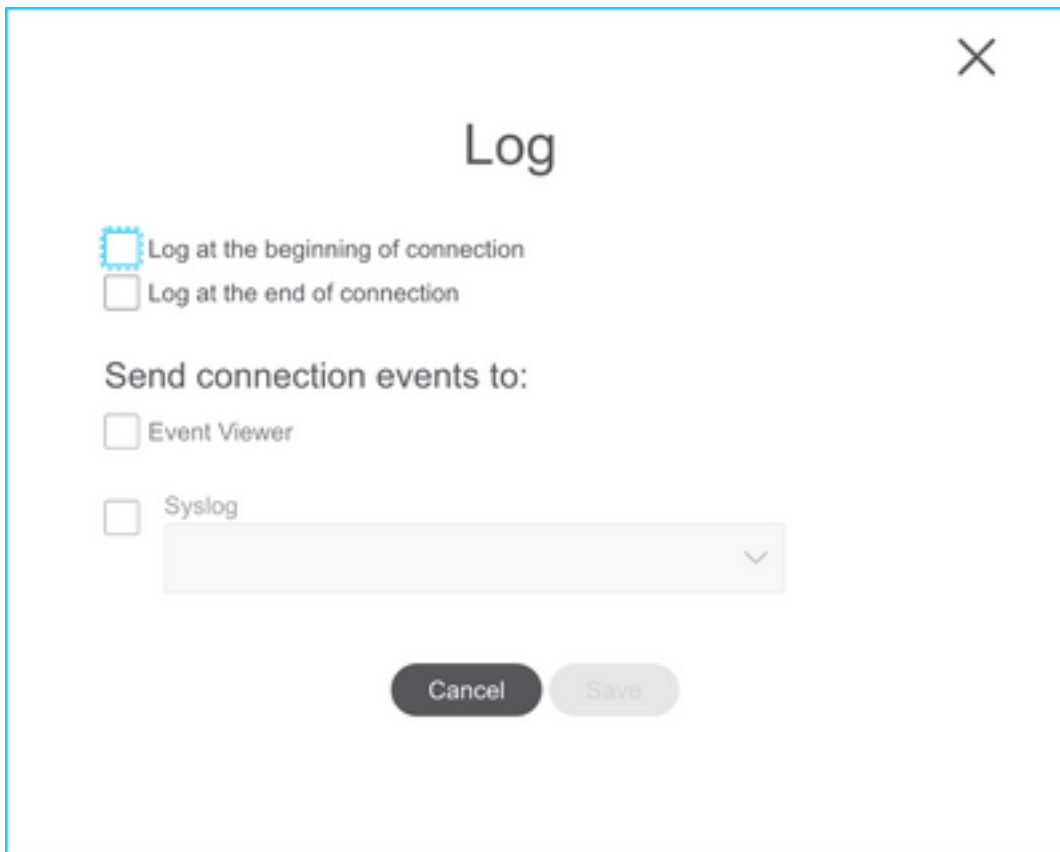
Select File Policy *

^

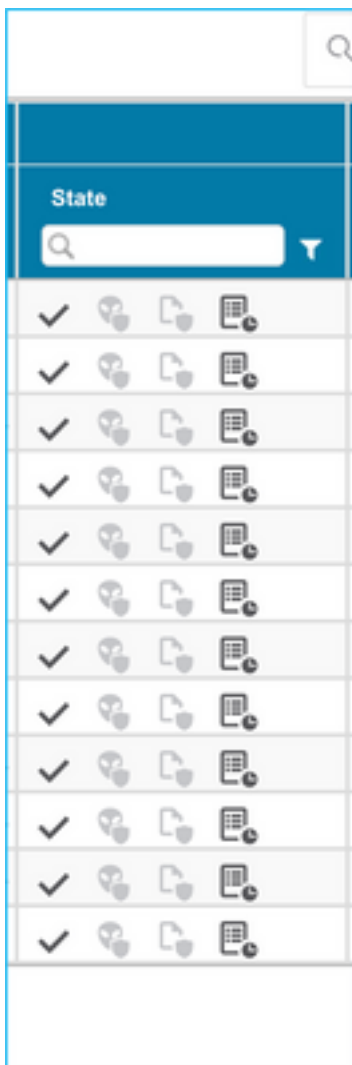
eicar
None

Cancel
Select

Voor de vereiste regels kan de logboek worden ingesteld. De configuratie van de schrijfservers die op de FMC bestaat, kan in deze fase worden geselecteerd.



De gekozen regelacties zullen voor elke regel dienovereenkomstig worden gemarkeerd.



20. Op dezelfde manier kunnen NAT, Network Object, Port Objects, Interfaces, Routes, VPN- objecten, Site-to-Site VPN-tunnels en andere elementen per configuratie stap voor stap worden bekeken.

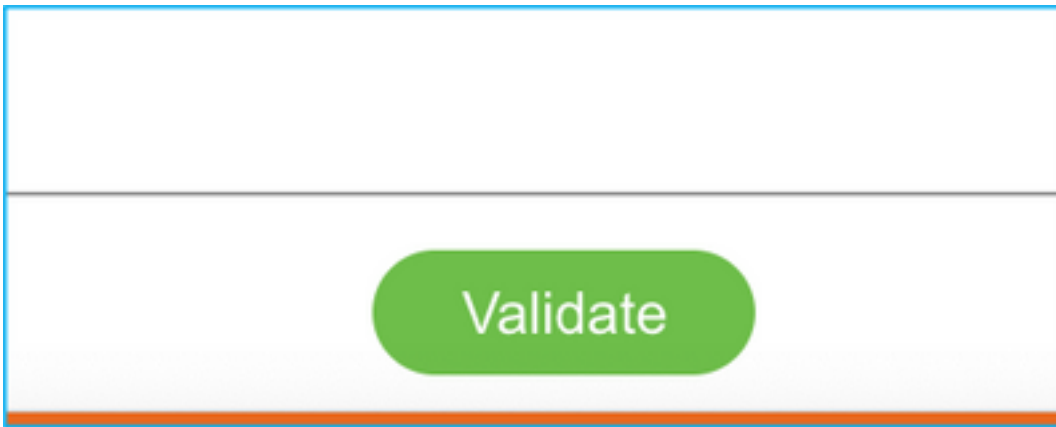
Opmerking: Alert zal worden gemeld zoals in het beeld wordt getoond om de vooraf gedeelde sleutel bij te werken aangezien het niet in het ASA configuratiebestand gekopieerd wordt. Selecteer **Handelingen > Vooraf gedeelde sleutel bijwerken** om de waarde in te voeren.

The screenshot shows the Cisco Firepower Migration Tool interface. The main heading is "Optimize, Review and Validate Configuration". The navigation tabs include "Access Control", "NAT", "Network Objects", "Port Objects", "Interfaces", "Routes", "VPN Objects", and "Site-to-Site VPN Tunnels". The "Site-to-Site VPN Tunnels" tab is active. A table lists VPN tunnels with columns for "Source Interface", "Peer IP", "IKE", "IKEv2", "IKEv2 IPSEC", "Pre-shared Key", and "PKI Cert". The "Pre-shared Key" column for the first tunnel is highlighted in yellow. A "MIGRATION ACTIONS" dropdown menu is open over the first row, showing options like "Do not migrate" and "Update Pre-shared Key". A red alert message at the bottom states: "Update the Pre-Shared Key/PKI Certificate column highlighted in Yellow for each VPN tunnel rows under Site-to-Site VPN Tunnels tab to validate and proceed with migration. For additional help, click here."

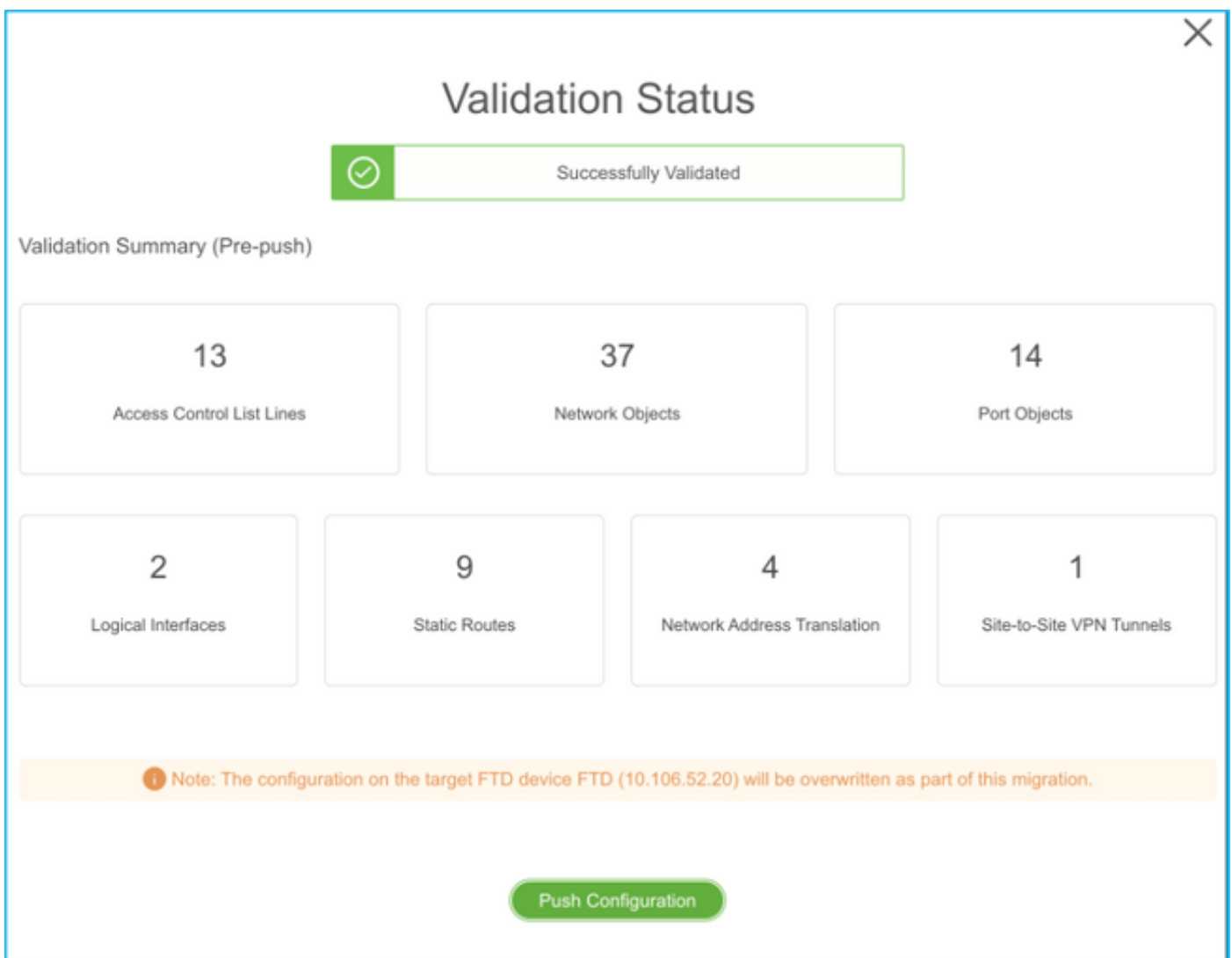
The screenshot shows a dialog box titled "Update Pre-Shared Key". The dialog has a close button (X) in the top right corner. The main text is "Update Pre-Shared Key". Below the title is a label "Pre-Shared Key IKEv2" and a text input field. At the bottom are two buttons: "Cancel" and "Save".

21. Klik tot slot op het pictogram voor validatie rechtsonder op het scherm zoals in de afbeelding

wordt getoond.



2. Zodra de validatie geslaagd is, klikt u op **Push Configuration** zoals in de afbeelding.



The image shows a "Validation Status" dialog box with a close button (X) in the top right corner. The status is "Successfully Validated", indicated by a green checkmark icon. Below the status, a "Validation Summary (Pre-push)" section displays the following configuration counts:

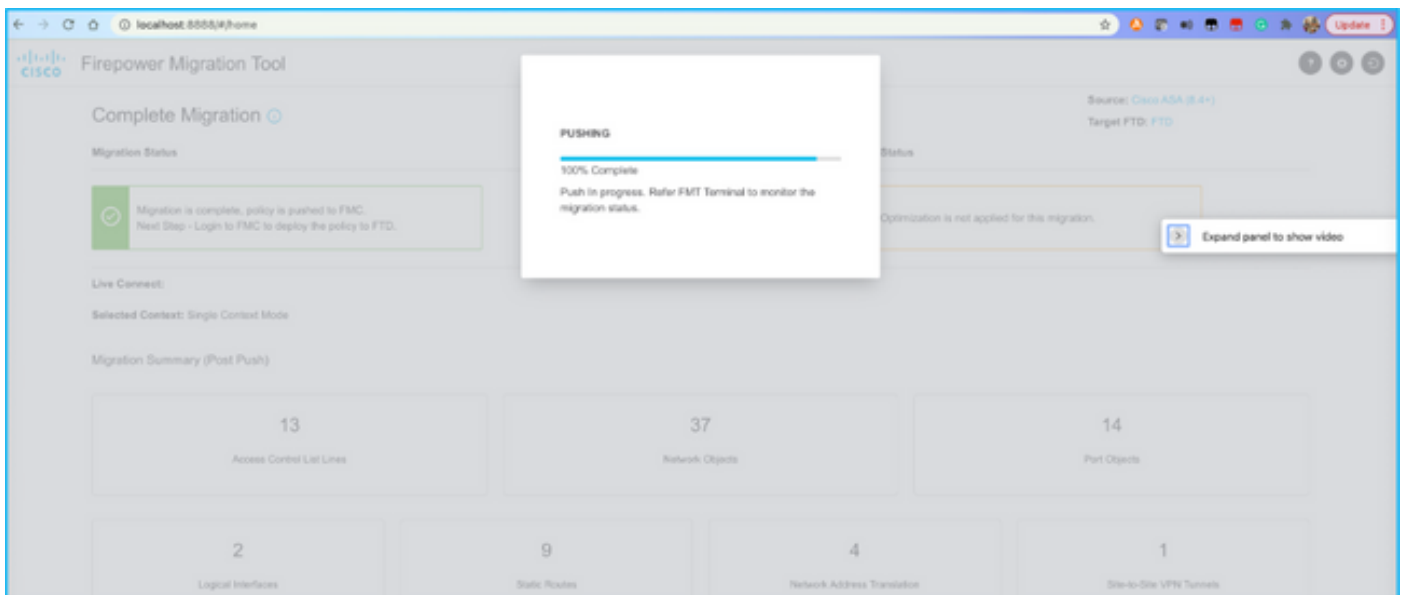
Configuration Type	Count
Access Control List Lines	13
Network Objects	37
Port Objects	14
Logical Interfaces	2
Static Routes	9
Network Address Translation	4
Site-to-Site VPN Tunnels	1

Below the summary, a note states: "Note: The configuration on the target FTD device FTD (10.106.52.20) will be overwritten as part of this migration." At the bottom of the dialog is a green "Push Configuration" button.

PUSHING

0% Complete

Push In progress. Refer FMT Terminal to monitor the migration status.



23. Zodra de migratie is voltooid, wordt het bericht dat wordt weergegeven in de afbeelding weergegeven.

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

Migration Status Optimization Status

Migration is complete, policy is pushed to FMC.
Next Step - Login to FMC to deploy the policy to FTD.

ACL Optimization is not applied for this migration.

Live Connect:
Selected Context: Single Context Mode

Migration Summary (Post Push)

13 Access Control List Lines	37 Network Objects	14 Port Objects
2 Logical Interfaces	9 Static Routes	4 Network Address Translation
		1 Site-to-Site VPN Tunnels

Please download the Post-Push migration report for a detailed summary. [Download Report](#)

Opmerking: Als de migratie niet succesvol is, klik dan op **Downloadrapport** om het Post-migratierapport te bekijken.

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

Migration Status Optimization Status

Migration Unsuccessful!
Internal Server Error.

ACL Optimization is successful but due to migration failure the refined optimized policy cannot be deployed to FMC.

Please refer logs for more details. [Download Report](#)

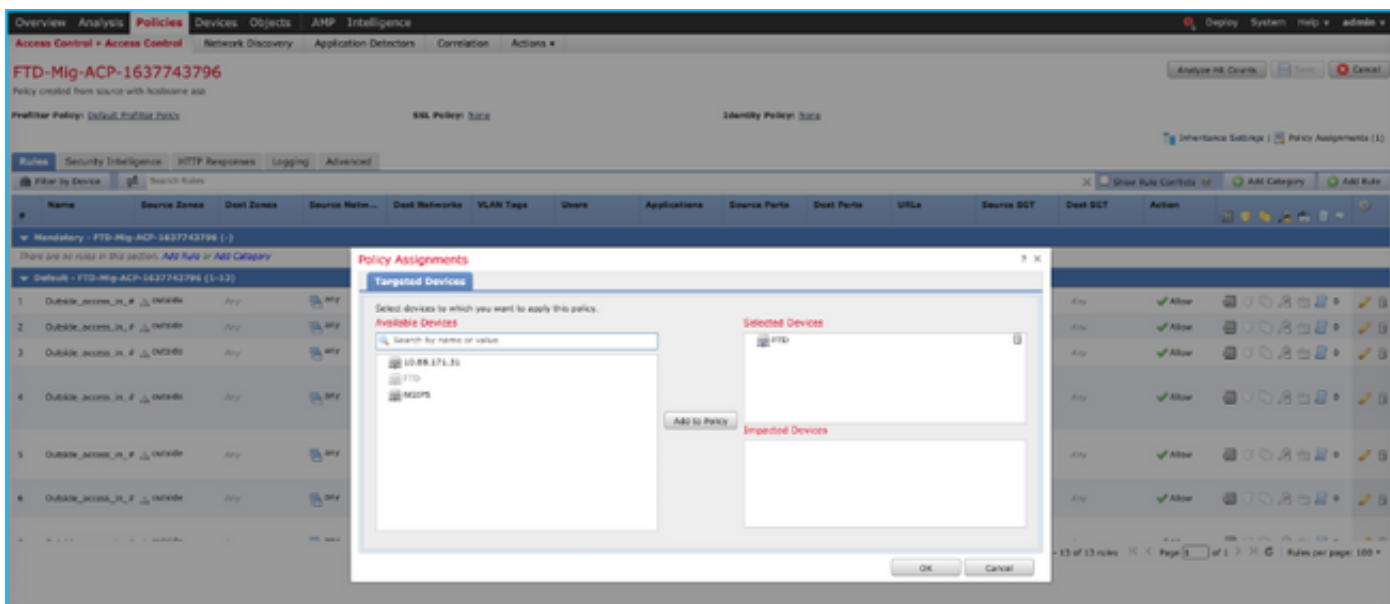
[Contact Support](#)

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

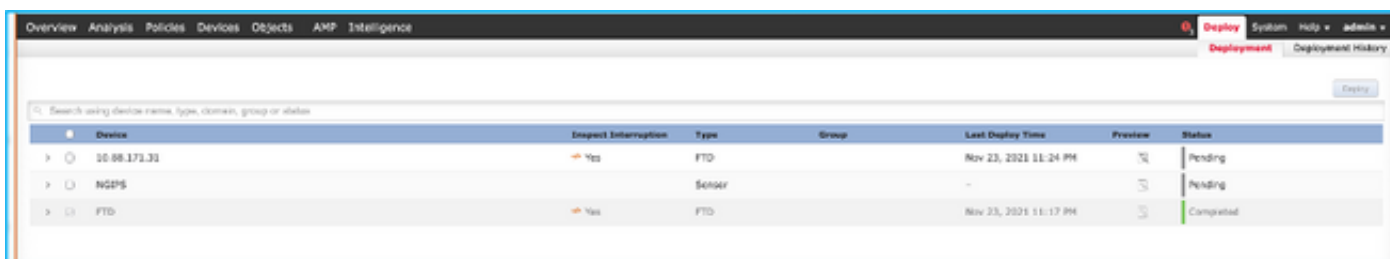
Validering op het VCC.

1. Navigeer naar **beleid > Toegangsbeheer > Toegangsbeheer > Beleidstoeiwijzing** om te bevestigen dat de geselecteerde FTD ingevuld is.



Opmerking: Het beleid inzake toegangscontrole voor migratie zou een naam hebben met het voorvoegsel **FTD-Mig-ACP**. Als in stap 2.8 geen FTD is geselecteerd, moet de FTD op het VCC worden geselecteerd.

2. Het beleid op de FTD duwen. Navigeren in om > **Plaatsing** > **Naam FTD** > **Deploy** zoals in het beeld getoond.



Bekende bogen gerelateerd aan het FirePOWER-migratietool

- Cisco bug-ID [CSCwa56374](#) - FMT-gereedschap hangt op pagina met overzicht van zone-mapping met een fout bij gebruik van een hoog geheugen
- Cisco bug-ID [CSCvz88730](#) - interfacestoring voor FTD Port-Channel Management-interfacetype
- Cisco bug-ID [CSCvx21986](#) - poortkanaals migratie naar Target-platform - Virtual FTD wordt niet ondersteund
- Cisco bug ID [CSCvy63003](#) - migratietool moet de interfacemodule uitschakelen als FTD al deel uitmaakt van het cluster
- Cisco bug-ID [CSCvx08199](#) - ACL's moeten worden gesplitst wanneer de toepassingsreferentie meer dan 50 is

Gerelateerde informatie

- [ASA firewall-firewall naar Threat-verdediging verplaatsen met de firewallmigratietool](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)