

Configurer FTD à partir du fichier de configuration ASA avec l'outil de migration Firepower

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration](#)

[Vérification](#)

[Bogues connus liés à l'outil de migration Firepower](#)

[Informations connexes](#)

Introduction

Ce document décrit un exemple de migration de l'appliance de sécurité adaptative (ASA) vers Firepower Threat Defense (FTD) sur FPR4145.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base sur ASA
- Connaissance de Firepower Management Center (FMC) et FTD

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ASA version 9.12(2)
- FTD version 6.7.0
- FMC version 6.7.0
- Outil de migration Firepower version 2.5.0

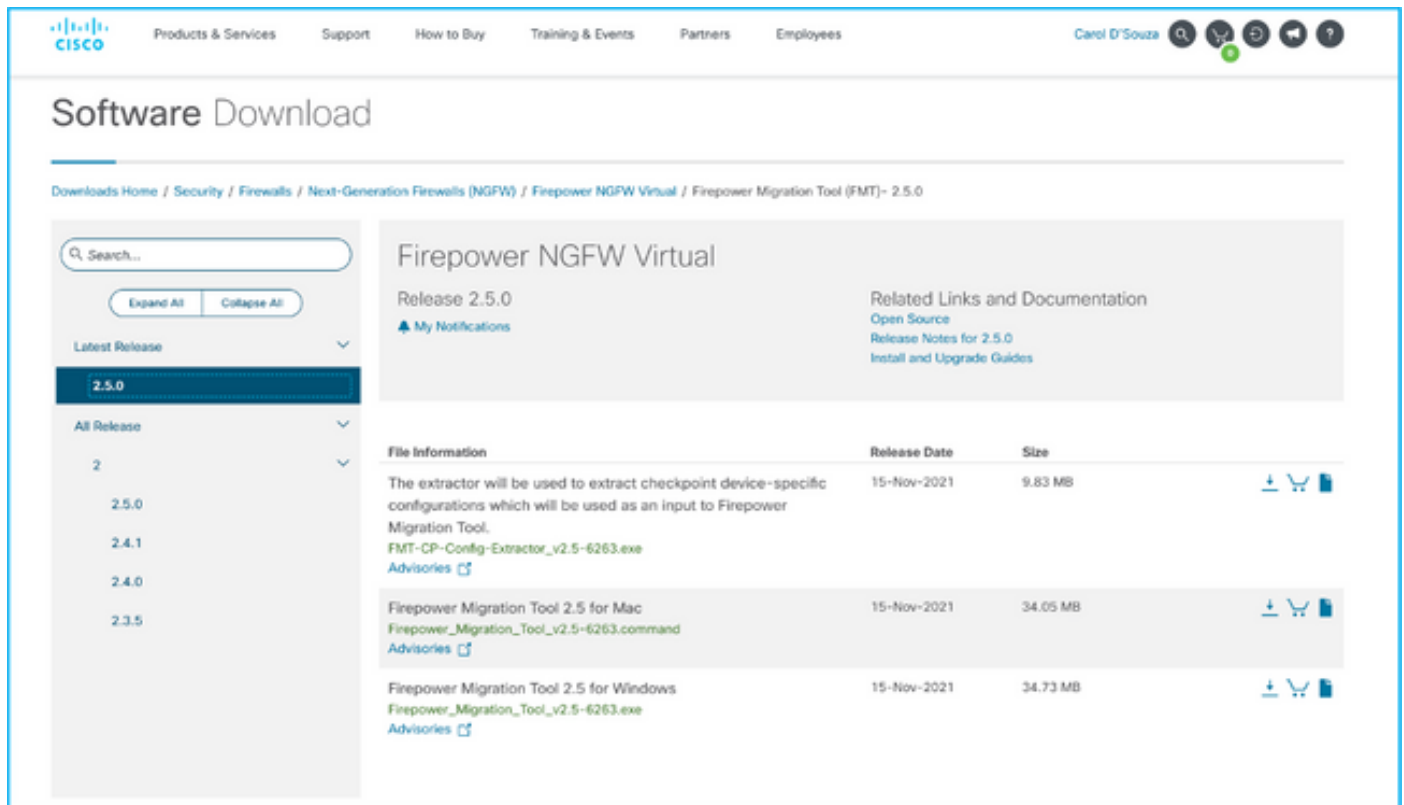
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Exporter le fichier de configuration ASA au format **.cfg** ou **.txt**. FMC doit être déployé avec FTD enregistré sous celui-ci.

Configuration

1. Téléchargez l'outil de migration Firepower à partir de software.cisco.com comme illustré dans l'image.



The screenshot shows the Cisco Software Download page for Firepower NGFW Virtual 2.5.0. The page includes a search bar, a list of releases with 2.5.0 selected, 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 | + - 📄 |

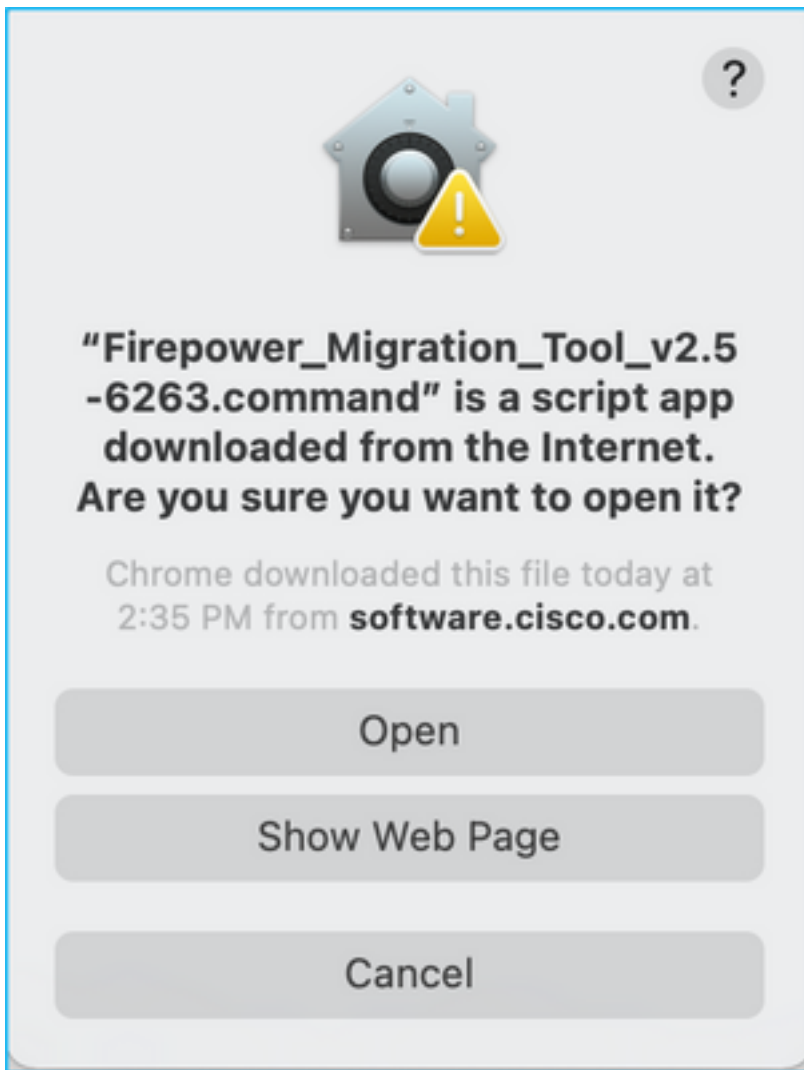
2. Examiner et vérifier les exigences de la section [Directives et limitations](#) pour l'outil de migration Firepower.

3. Si vous prévoyez de migrer un fichier de configuration volumineux, configurez les paramètres de veille de sorte que le système ne se mette pas en veille lors d'une migration.

3.1. Sous Windows, accédez à Options d'alimentation dans le Panneau de configuration. Cliquez sur **Modifier les paramètres du plan** en regard de votre plan d'alimentation actuel. Modifier **Mettre l'ordinateur en veille** sur **Jamais**. Cliquez sur **Enregistrer les modifications**.

3.2. Pour MAC, accédez à **Préférences système > Économie d'énergie**. Cochez la case en regard pour empêcher l'ordinateur de dormir automatiquement lorsque l'écran est éteint et faites glisser l'**option Désactiver l'affichage** après le curseur sur **Jamais**.

Note: Cette boîte de dialogue s'affiche lorsque les utilisateurs MAC tentent d'ouvrir le fichier téléchargé. Ignorez ceci et suivez l'étape 4 A.



4. A. Pour MAC : utilisez le terminal et exécutez ces commandes.

```
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. Pour Windows - double-cliquez sur l'outil de migration Firepower pour le lancer dans un navigateur Google Chrome.

5. Acceptez la licence comme indiqué dans l'image.

← → ↻ 🏠 ⓘ 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

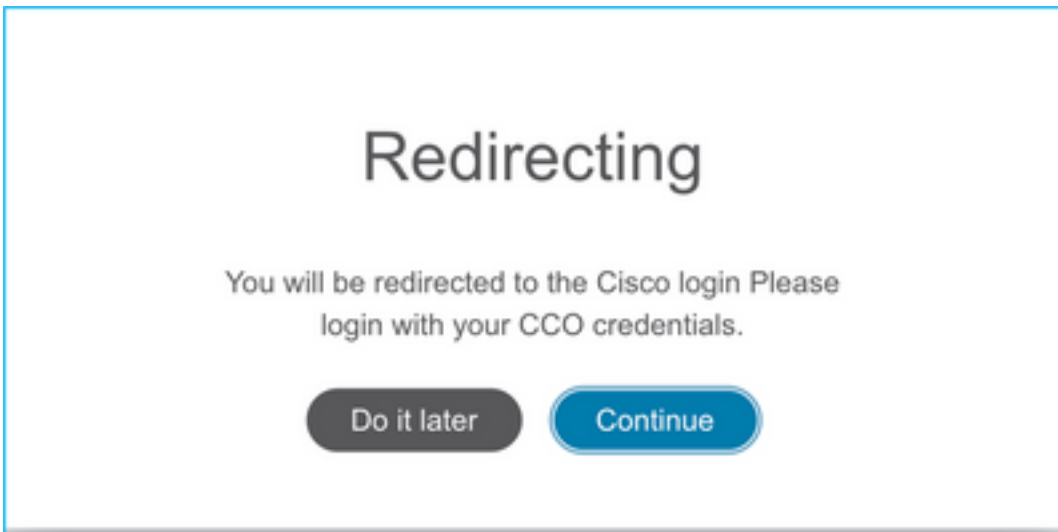
I have read the content of the EULA and SEULA and agree to terms listed.

Proceed

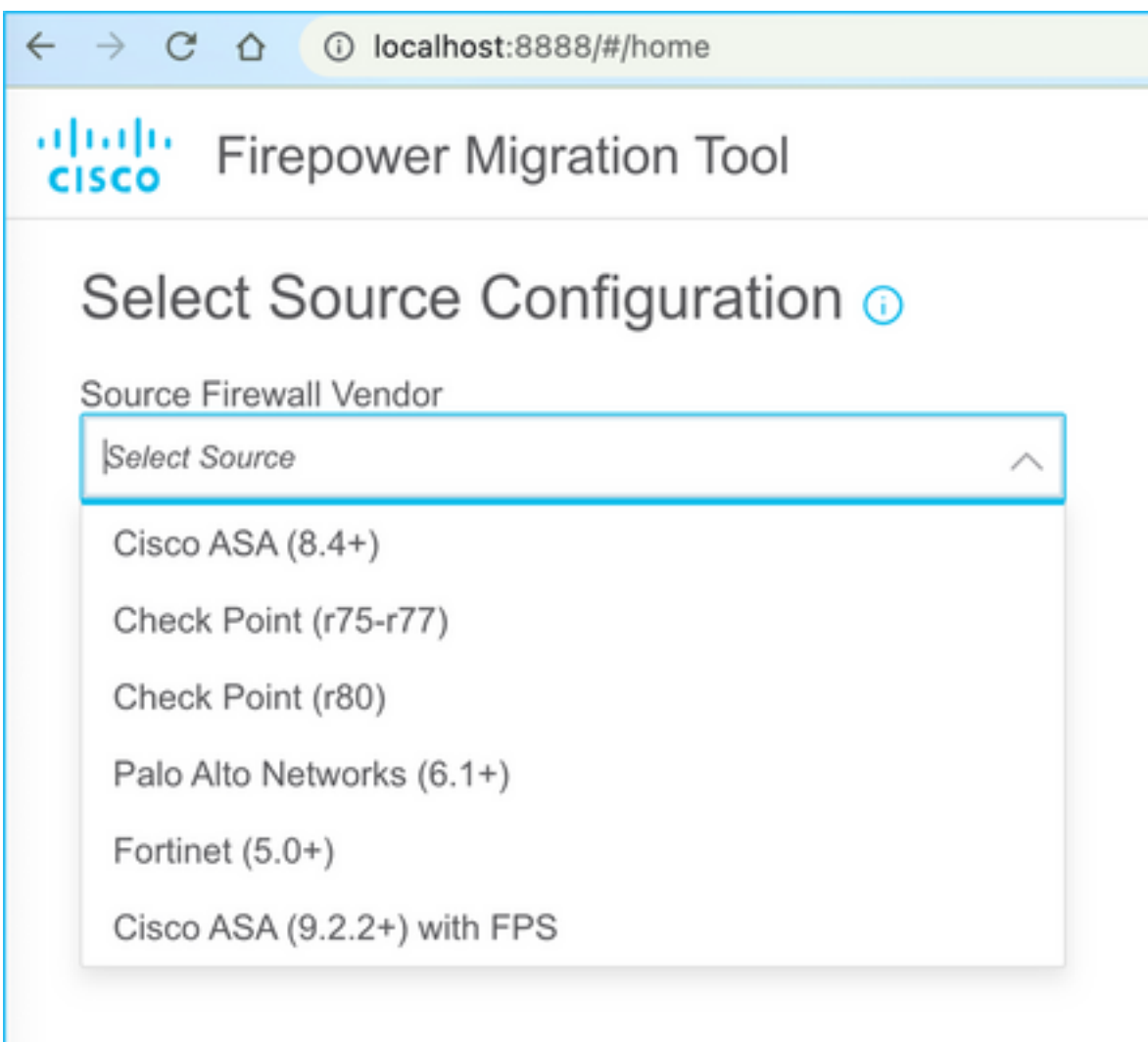
6. Sur la page de connexion de Firepower Migration Tool, cliquez sur le lien de connexion CCO pour vous connecter à votre compte Cisco.com avec vos identifiants de connexion uniques.

Note: Si vous n'avez pas de compte Cisco.com, créez-le sur la page de connexion

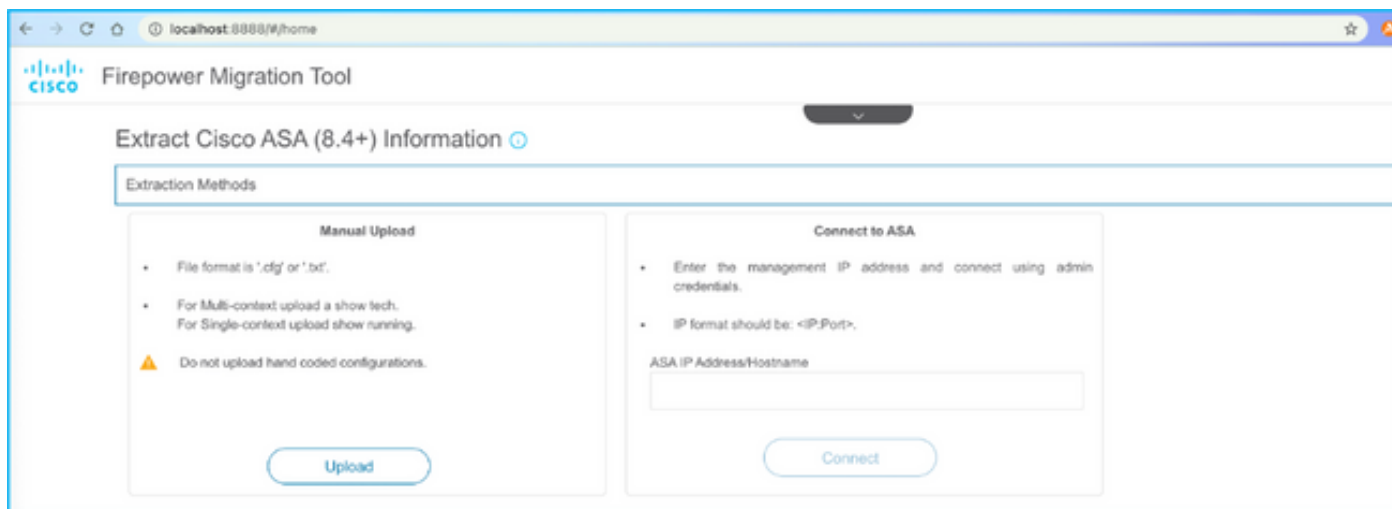
Cisco.com. Connectez-vous avec les informations d'identification par défaut suivantes :
Username—admin Password—Admin123.



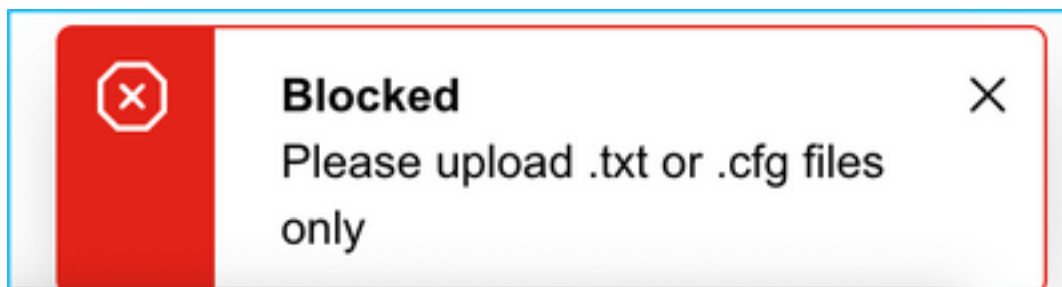
7. Sélectionnez la configuration source. Dans ce scénario, il s'agit de Cisco ASA (8.4+).



8. Sélectionnez Manual Upload (Téléchargement manuel) si vous n'avez pas de connectivité à l'ASA. Sinon, vous pouvez récupérer la configuration en cours à partir de l'ASA et saisir l'adresse IP de gestion et les détails de connexion. Dans notre scénario, un téléchargement manuel a été effectué.

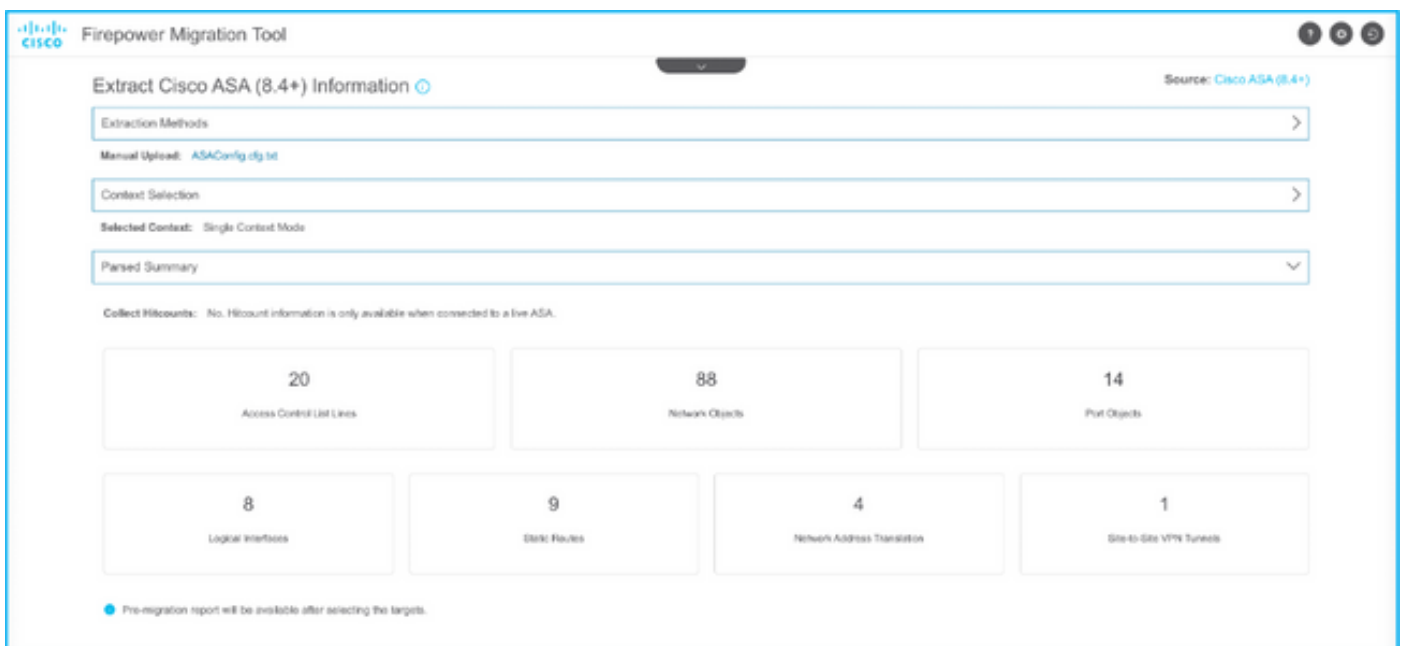


Note: Cette erreur s'affiche si le fichier n'est pas pris en charge. Veuillez à modifier le format en texte brut. (Une erreur s'affiche malgré l'extension .cfg).

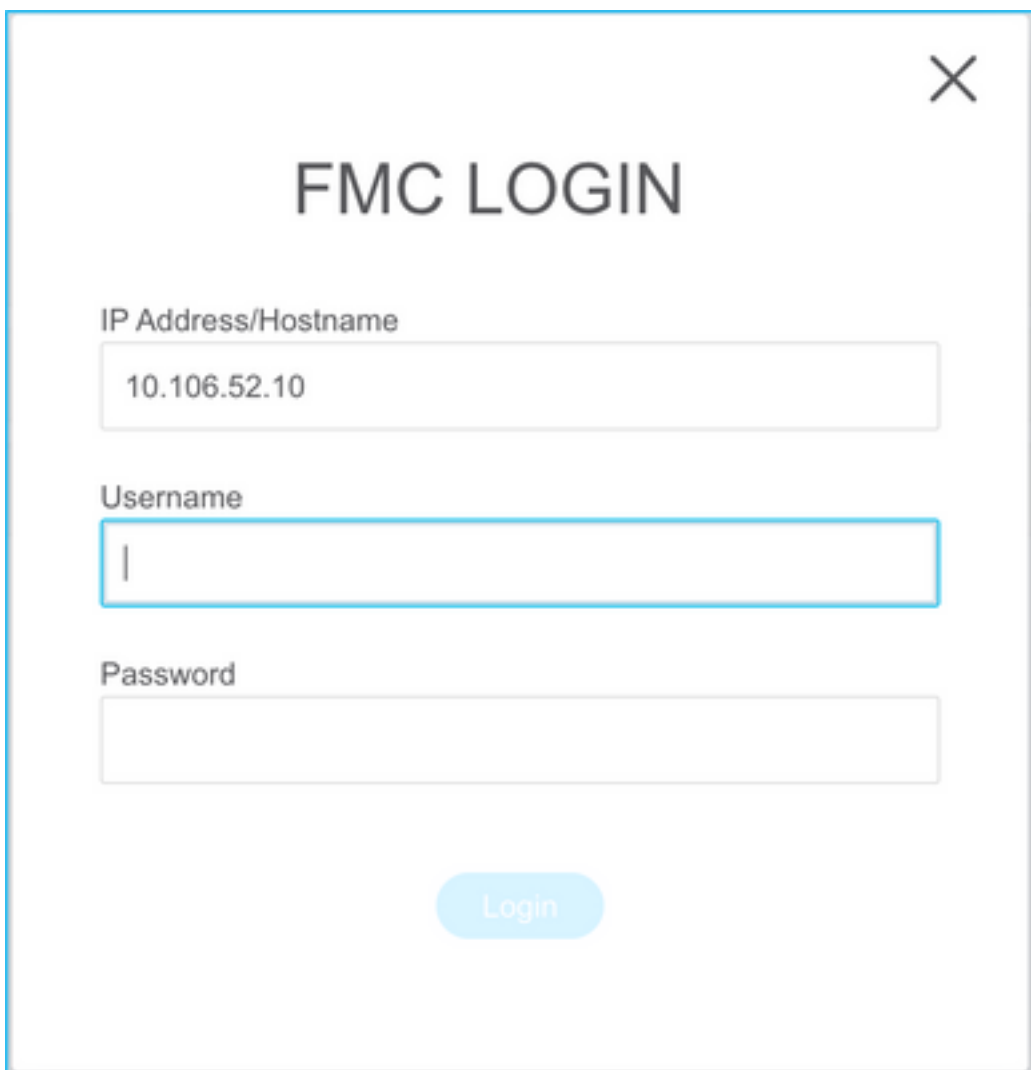
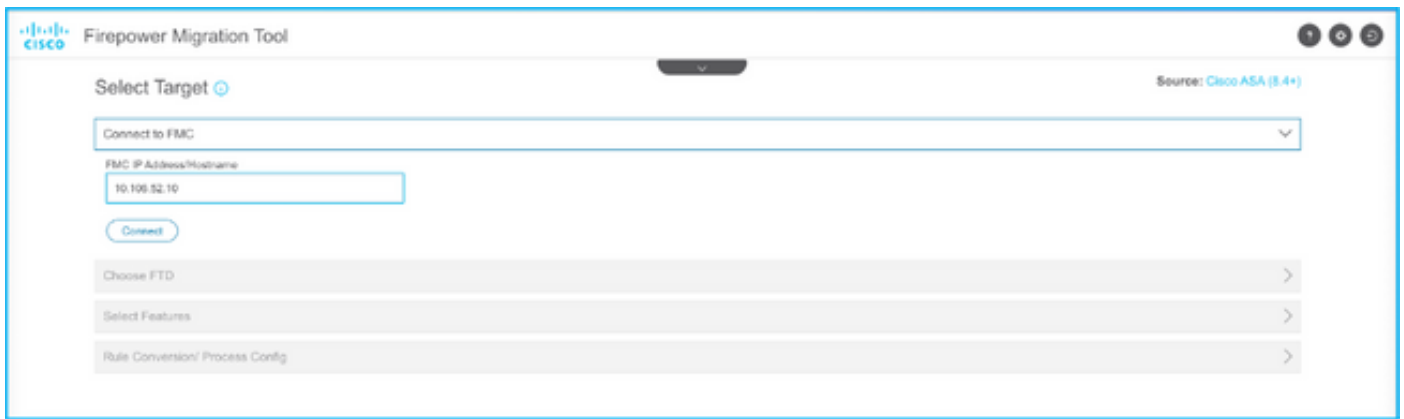


```
ASAConfig.cfg — Edited
asa# show running-config
: Saved
:
: Serial Number: FLM22160652
: Hardware: FPR4K-SM-12, 56533 MB RAM, CPU Xeon E5 series 2200 MHz, 1 CPU (24 cores)
:
ASA Version 9.12(2)
:
hostname asa
enable password ***** pbkdf2
:
license smart
feature tier standard
names
no mac-address 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
```

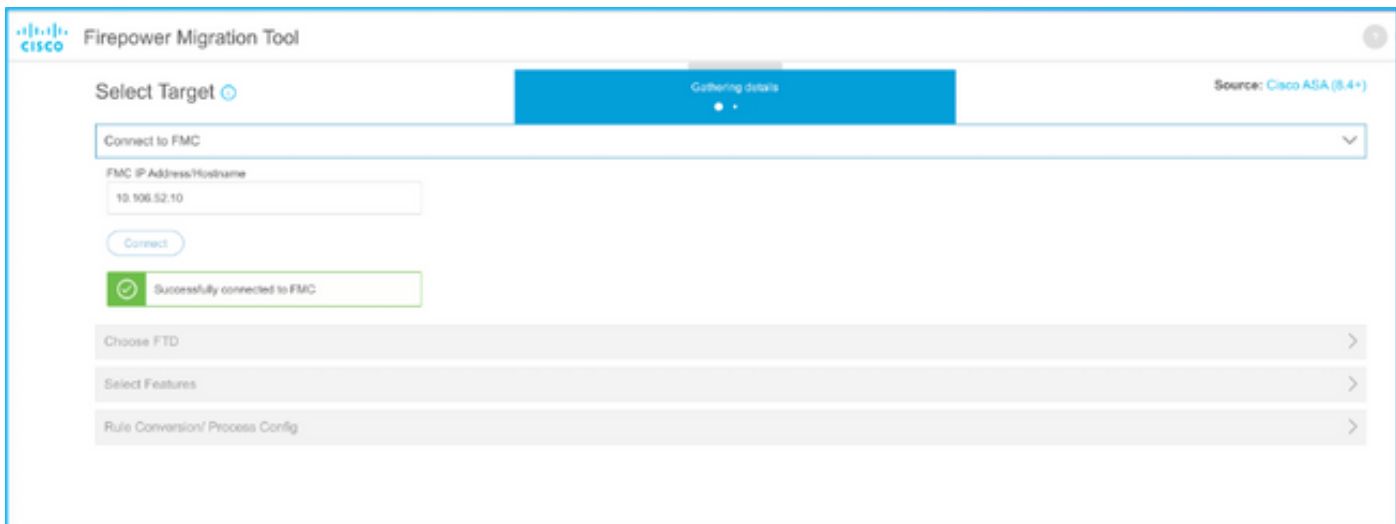
9. Une fois le fichier téléchargé, les éléments sont analysés en fournissant un résumé comme illustré dans l'image :



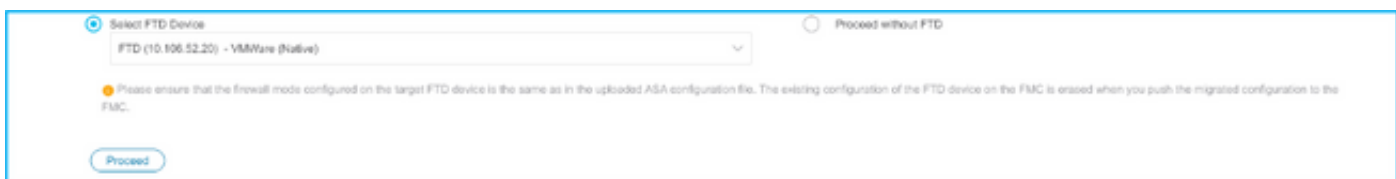
10. Saisissez l'adresse IP FMC et les informations d'identification de connexion auxquelles la configuration ASA doit être migrée. Assurez-vous que l'adresse IP FMC est accessible depuis votre station de travail.



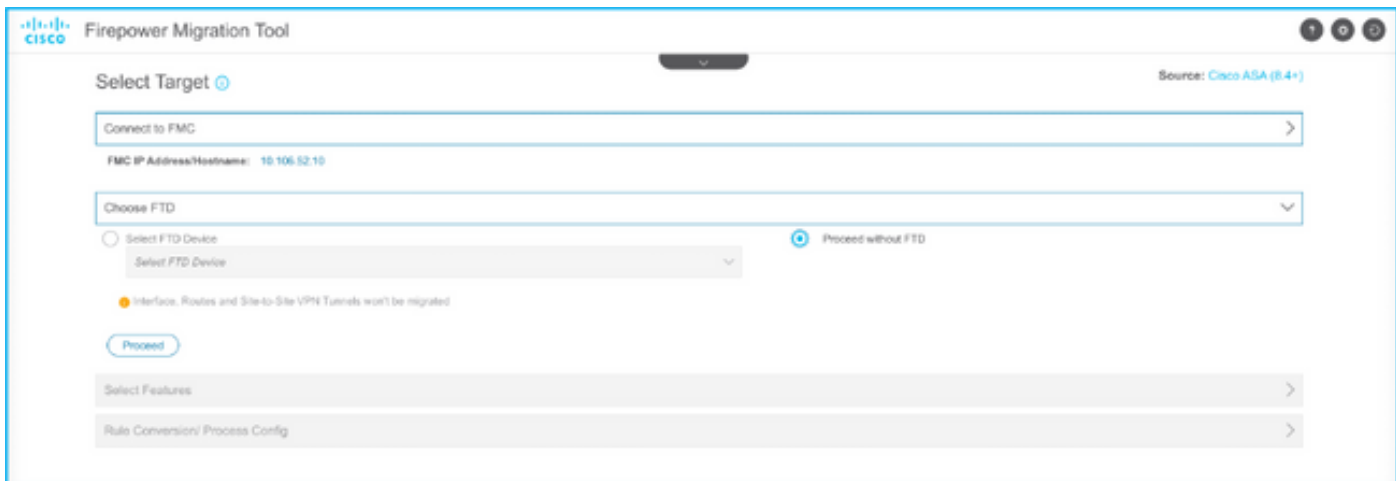
11. Une fois que le FMC est connecté, les FTD gérés sous celui-ci s'affichent.



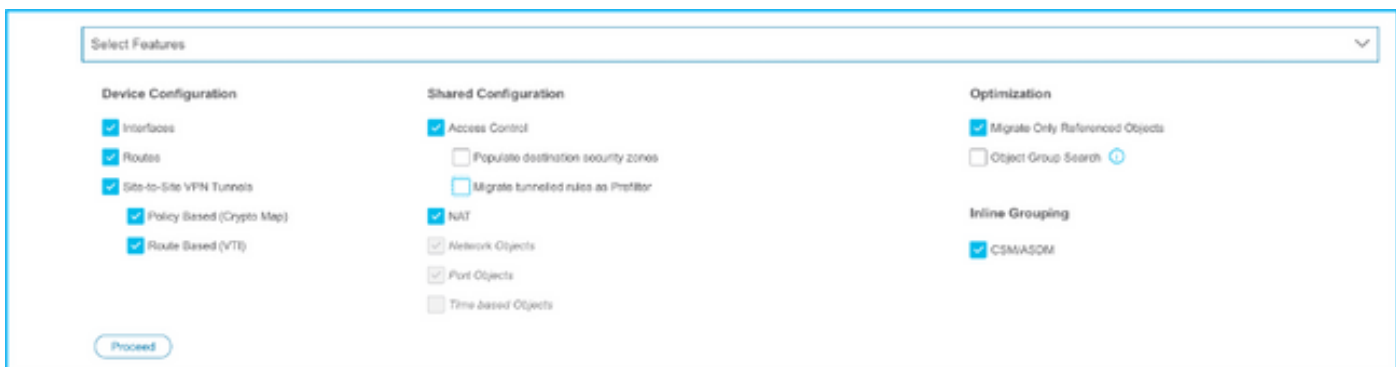
12. Choisissez le FTD vers lequel vous voulez effectuer la migration de la configuration ASA.



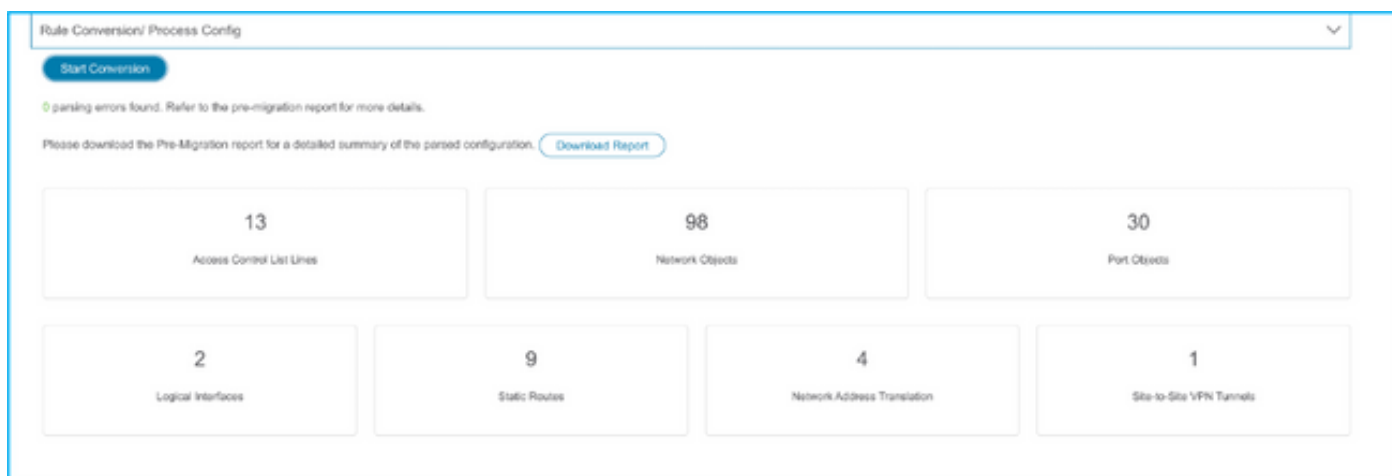
Note: Il est recommandé de sélectionner le périphérique FTD, sinon les interfaces, les routes et la configuration VPN de site à site devront être effectuées manuellement.



13. Sélectionnez les fonctions à migrer, comme l'illustre l'image.



14. Sélectionnez **Commencer la conversion** pour lancer la pré-migration qui remplira les éléments relatifs à la configuration FTD.




The screenshot displays the 'Rule Conversion/ Process Config' interface. 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 contains seven summary cards for different configuration elements:

| Configuration 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. Cliquez sur **Télécharger le rapport** précédemment affiché pour afficher le rapport de pré-migration tel qu'illustré dans l'image.

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

 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 |

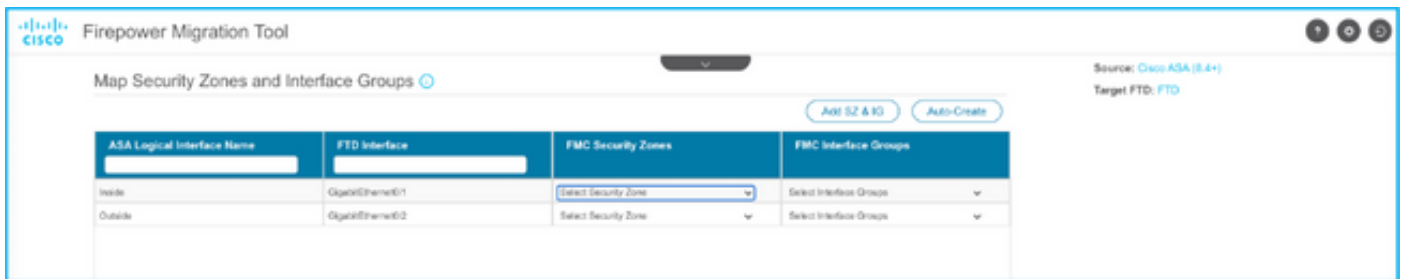
Note: ACEs that are applied outbound or not attached to interfaces using the access-group command are ignored.

16. Mapper les interfaces ASA aux interfaces FTD, comme indiqué dans l'image.

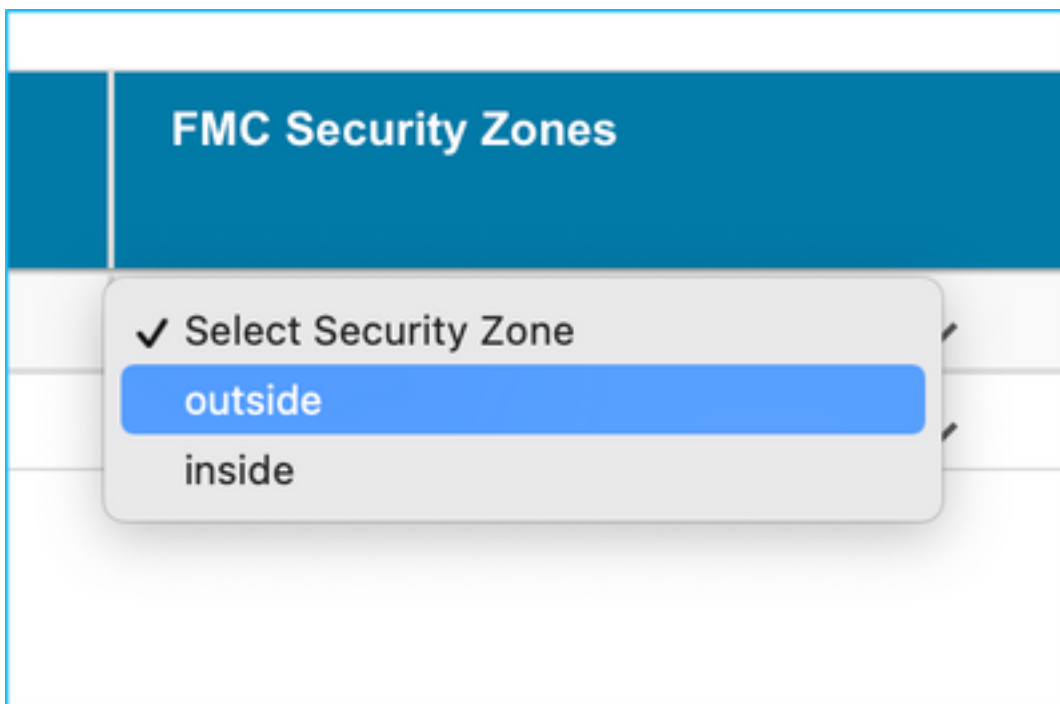
Refresh

| ASA Interface Name | FTD Interface Name |
|----------------------|----------------------|
| <input type="text"/> | Select Interface |
| Ethernet1/2 | GigabitEthernet0/0 |
| Ethernet1/3 | GigabitEthernet0/1 |
| | ✓ GigabitEthernet0/2 |

17. Attribuez des zones de sécurité et des groupes d'interfaces aux interfaces FTD.



A. Si des zones de sécurité et des groupes d'interface sont déjà créés sur le FMC, vous pouvez les sélectionner selon les besoins :



B. Si vous devez créer des zones de sécurité et un groupe d'interfaces, cliquez sur **Ajouter une zone de sécurité et un IG** comme indiqué dans l'image.

✕

Add SZ & IG

Security Zones (SZ) **Interface Groups (IG)**

Add

iMax 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. Sinon, vous pouvez opter pour l'option **Auto-Create** qui créera des zones de sécurité et des groupes d'interfaces avec le nom **ASA interface logique_sz** et **ASA interface_ig** respectivement.

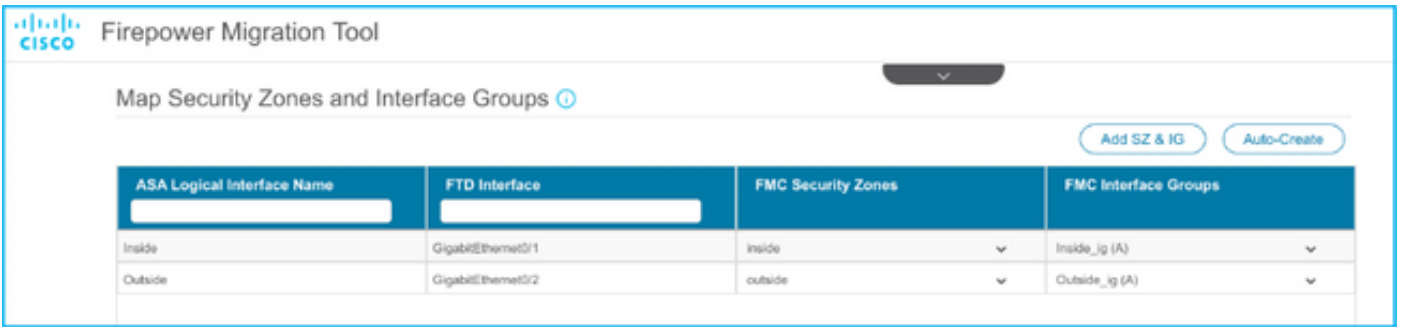
Auto-Create

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.

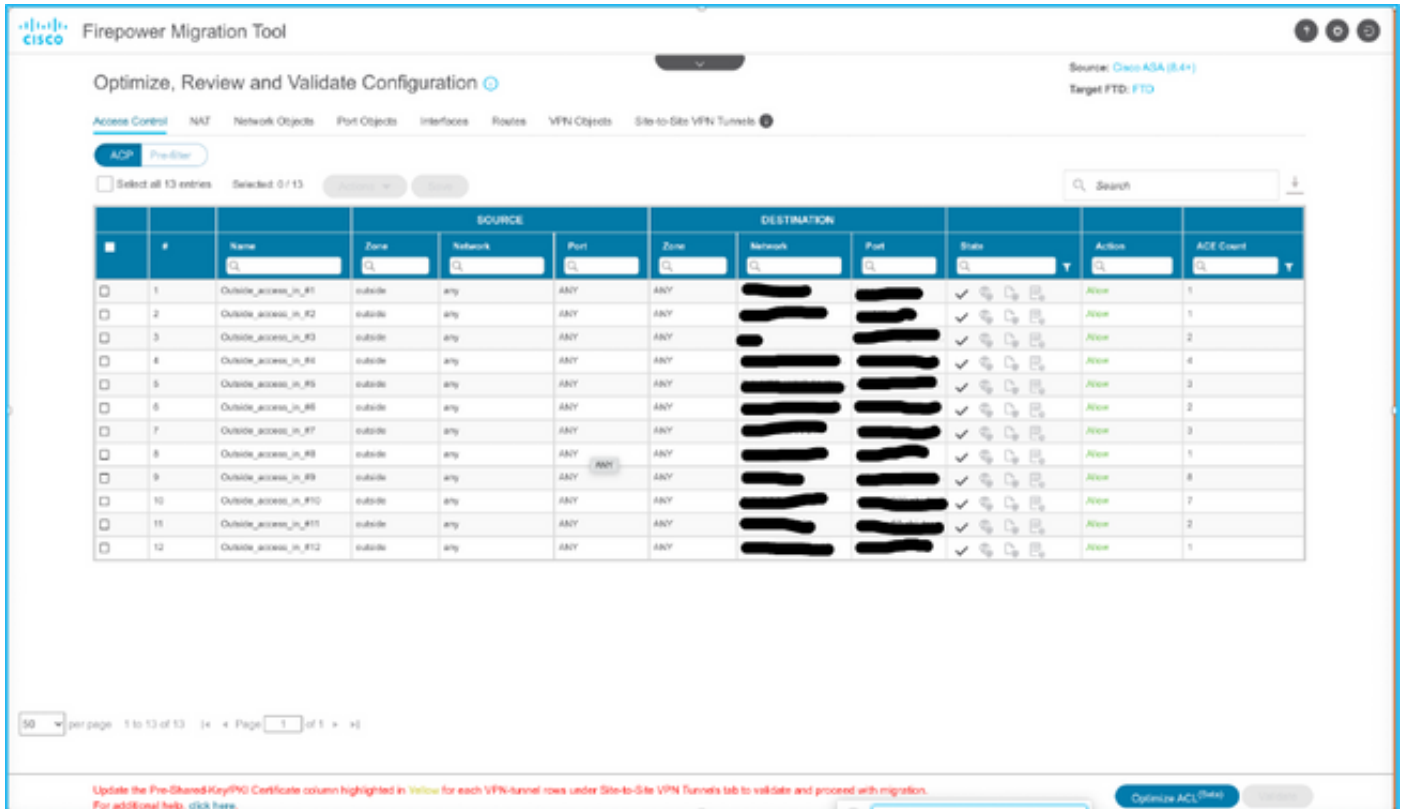
Select the objects that you want to map to ASA interfaces

Security Zones Interface Groups

CancelAuto-Create



18. Examiner et valider chacun des éléments FTD créés. Les alertes sont affichées en rouge comme l'illustre l'image.



19. Les actions de migration peuvent être sélectionnées comme indiqué dans l'image si vous souhaitez modifier une règle. Les fonctions FTD d'ajout de fichiers et de stratégie IPS peuvent être effectuées à cette étape.

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 | FILE 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 | Rule Action | outside any |

Note: Si des stratégies de fichiers existent déjà dans le FMC, elles seront renseignées comme indiqué dans l'image. Il en va de même pour les stratégies IPS et les stratégies par défaut.

✕

File Policy

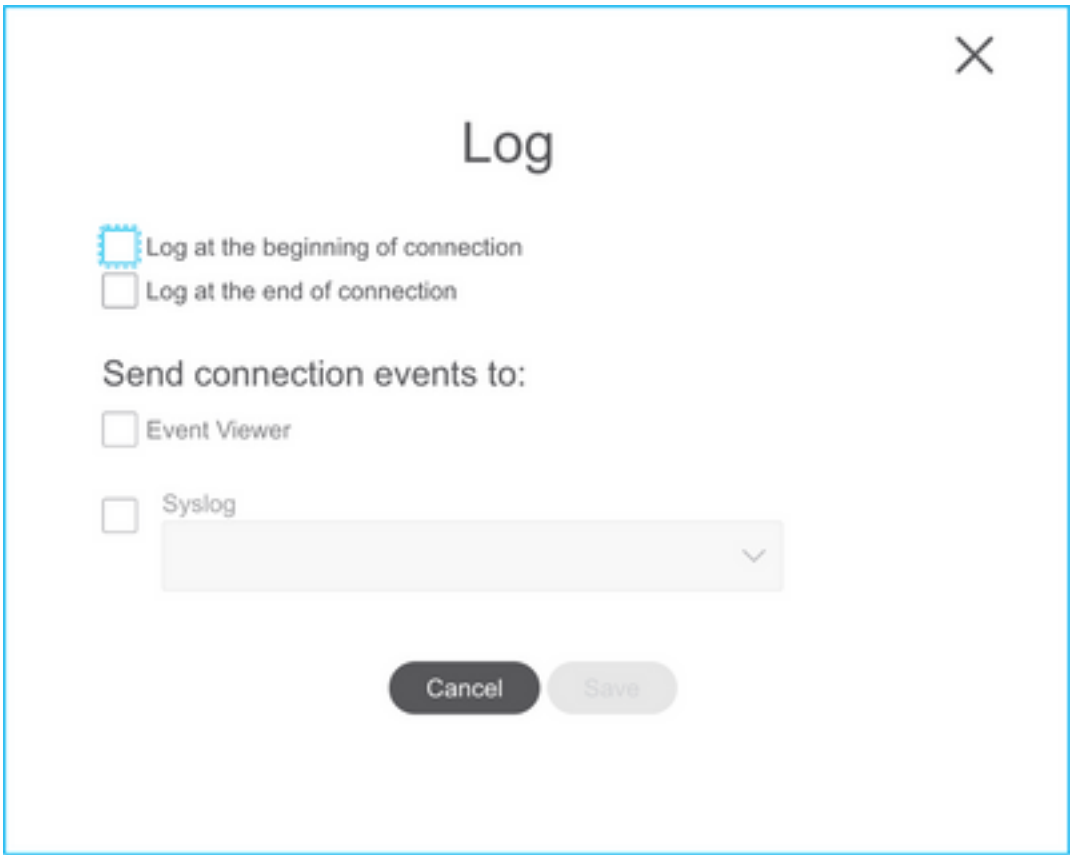
Select File Policy *

eicar

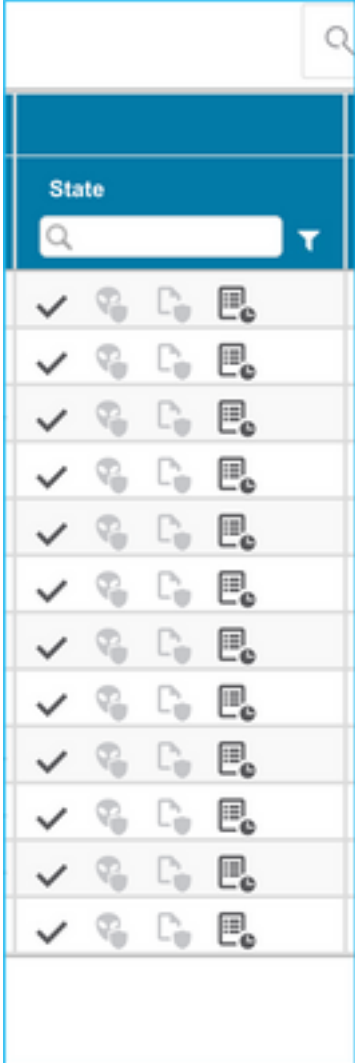
None

Cancel
Select

La configuration du journal peut être effectuée pour les règles requises. La configuration du serveur Syslog existant sur le FMC peut être sélectionnée à ce stade.

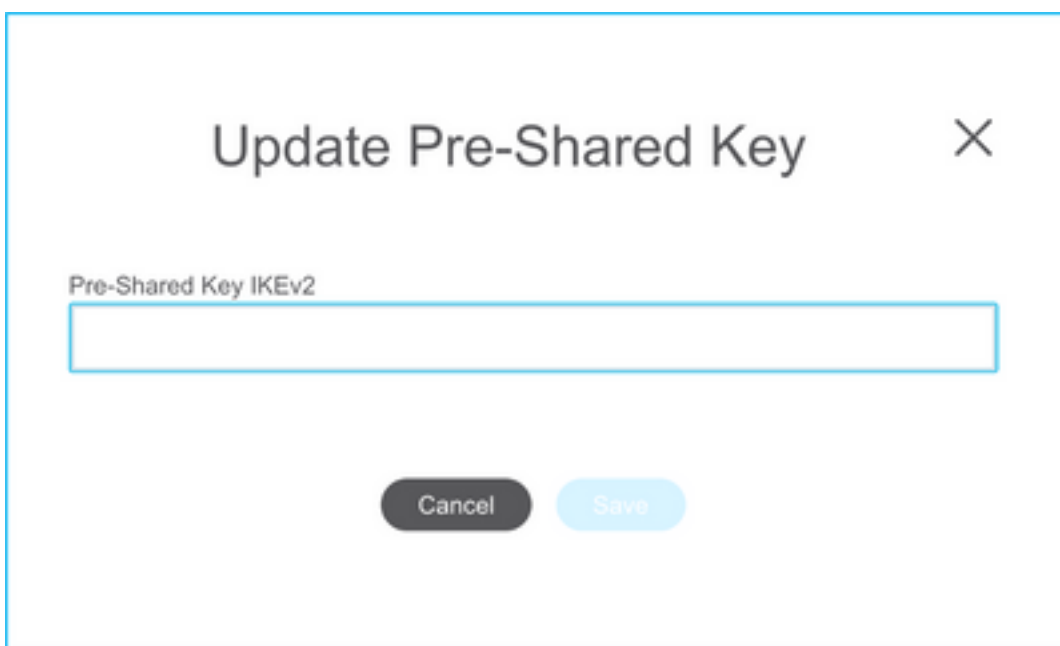
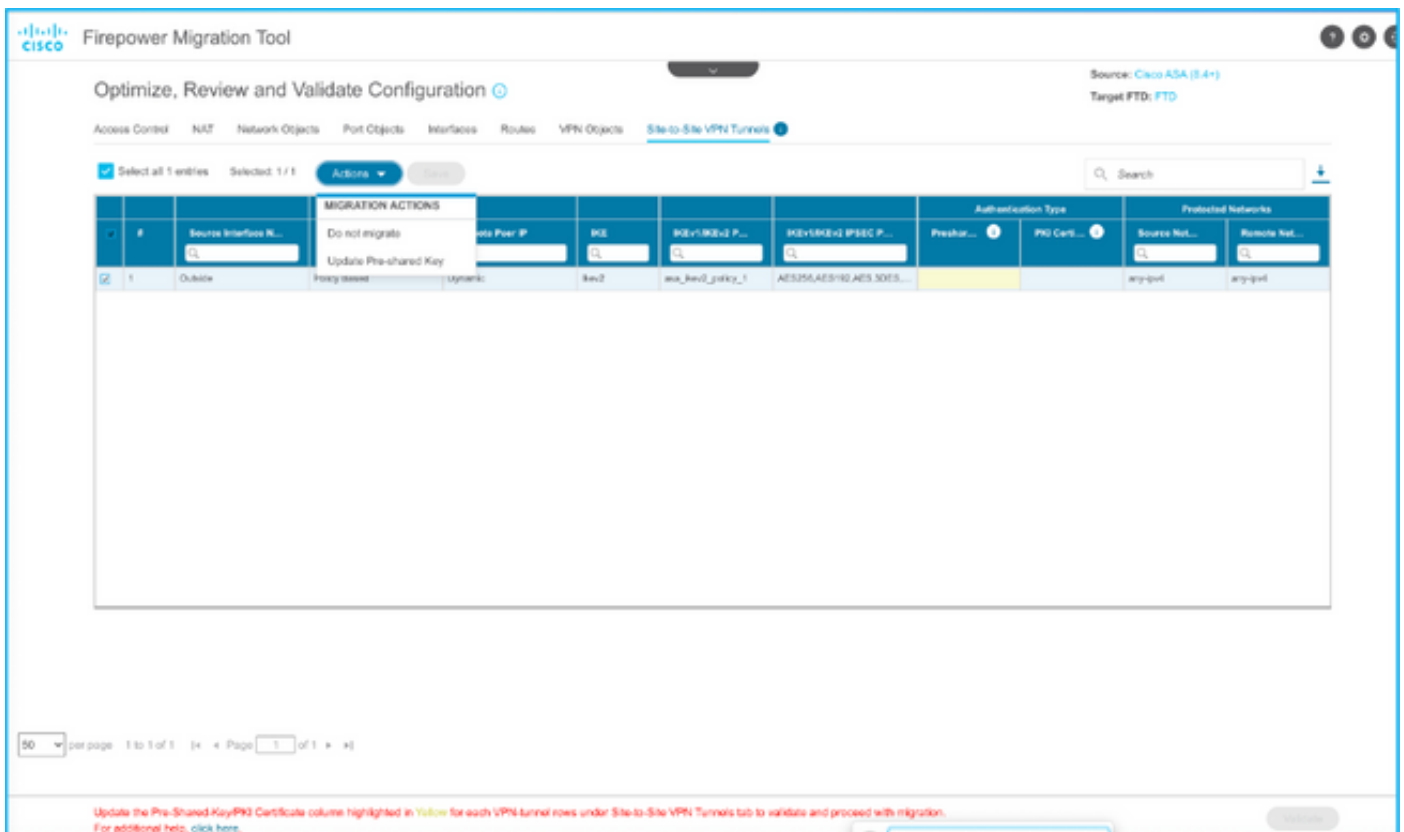


Les actions de règle sélectionnées sont mises en surbrillance pour chaque règle.

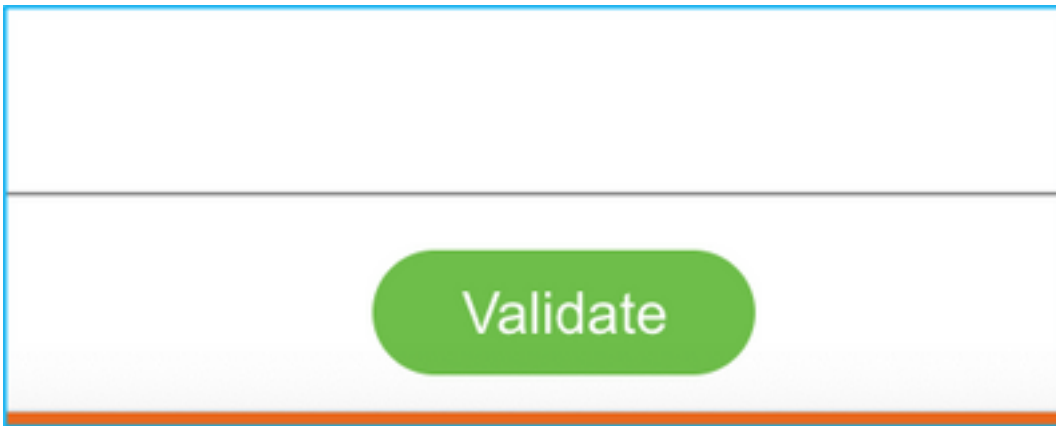


20. De même, NAT, Network Object, Port Objects, Interfaces, Routes, VPN Objects, Site-to-Site VPN Tunnels et d'autres éléments selon votre configuration peuvent être examinés étape par étape.

Note: L'alerte sera avertie, comme l'illustre l'image, de la mise à jour de la clé pré-partagée, car elle ne sera pas copiée dans le fichier de configuration ASA. Sélectionnez **Actions > Mettre à jour la clé prépartagée** pour entrer la valeur.



21. Enfin, cliquez sur l'icône **Valider** en bas à droite de l'écran, comme indiqué dans l'image.



22. Une fois la validation terminée, cliquez sur **Push Configuration** comme indiqué dans l'image.

The dialog box is titled "Validation Status" and features a close button (X) in the top right corner. A green progress bar with a checkmark icon and the text "Successfully Validated" is displayed below the title. Underneath, a section titled "Validation Summary (Pre-push)" contains seven summary cards arranged in two rows. The first row includes "Access Control List Lines" (13), "Network Objects" (37), and "Port Objects" (14). The second row includes "Logical Interfaces" (2), "Static Routes" (9), "Network Address Translation" (4), and "Site-to-Site VPN Tunnels" (1). A yellow note at the bottom states: "Note: The configuration on the target FTD device FTD (10.106.52.20) will be overwritten as part of this migration." A green "Push Configuration" button is located at the bottom center of the dialog.

| Category | 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 |

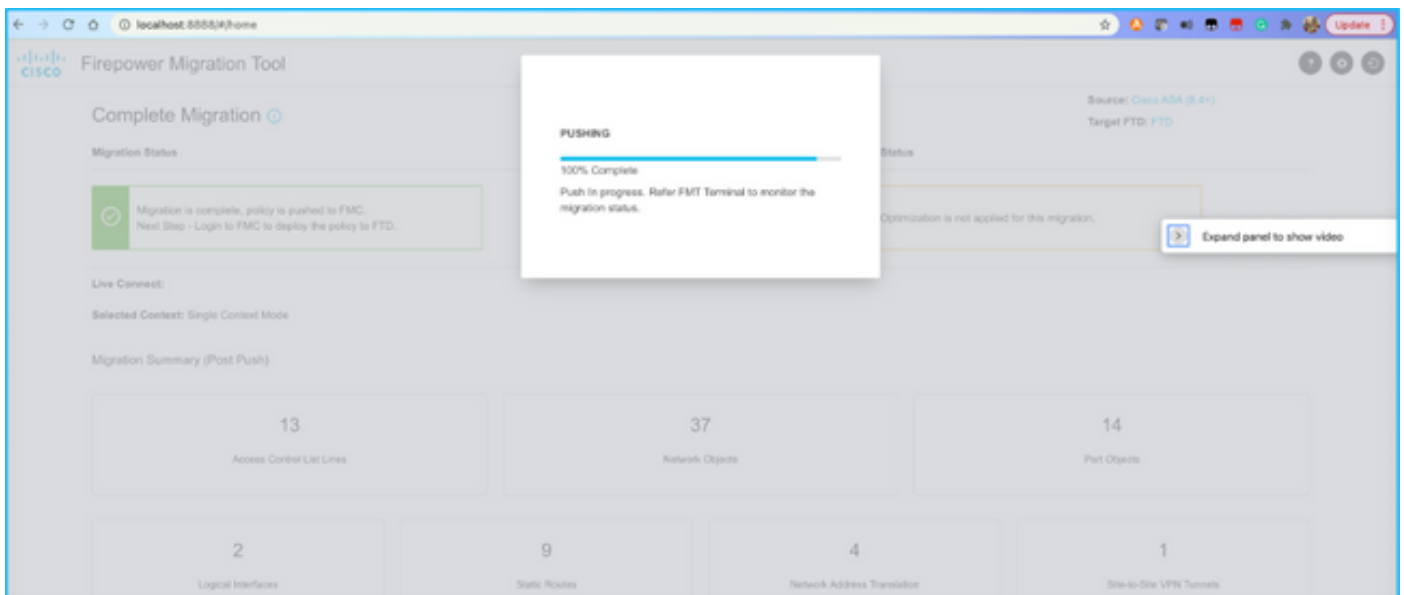
Note: The configuration on the target FTD device FTD (10.106.52.20) will be overwritten as part of this migration.

Push Configuration

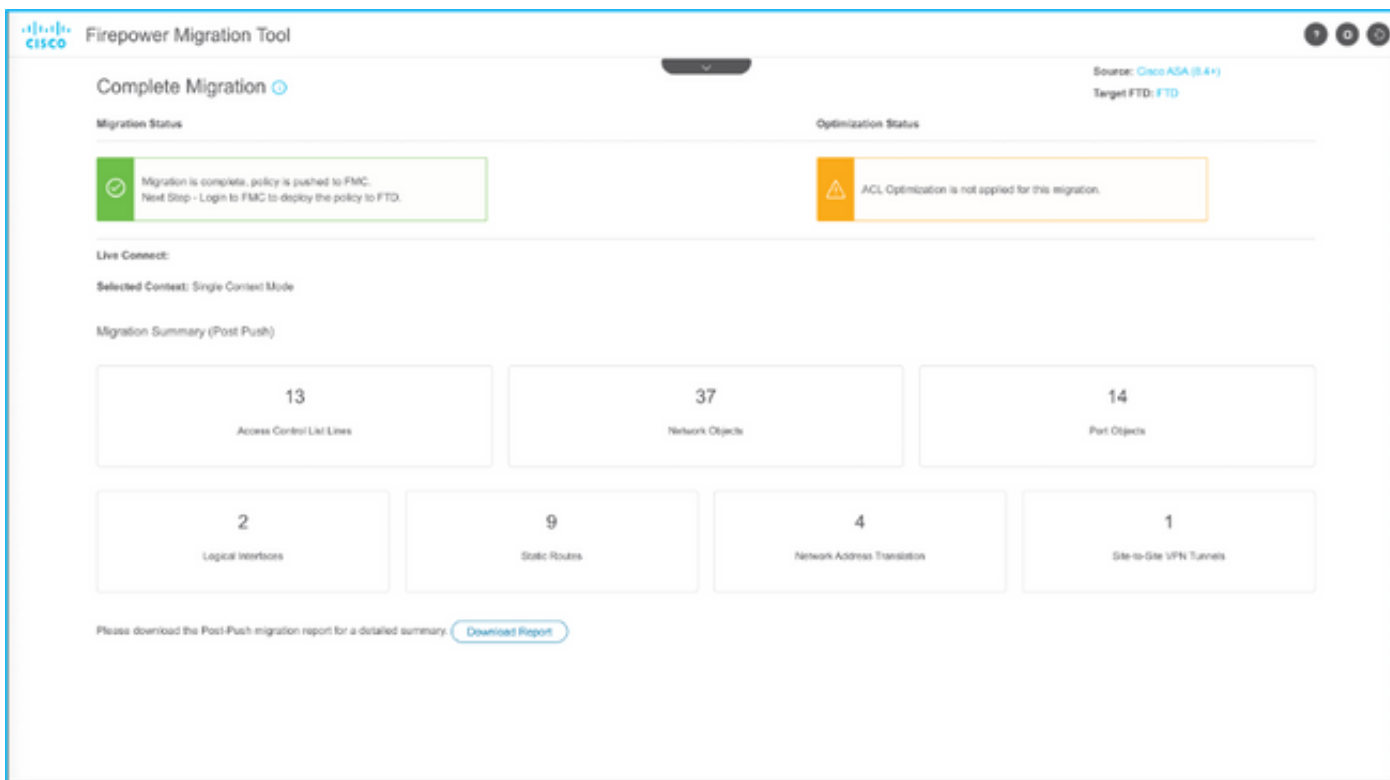
PUSHING

0% Complete

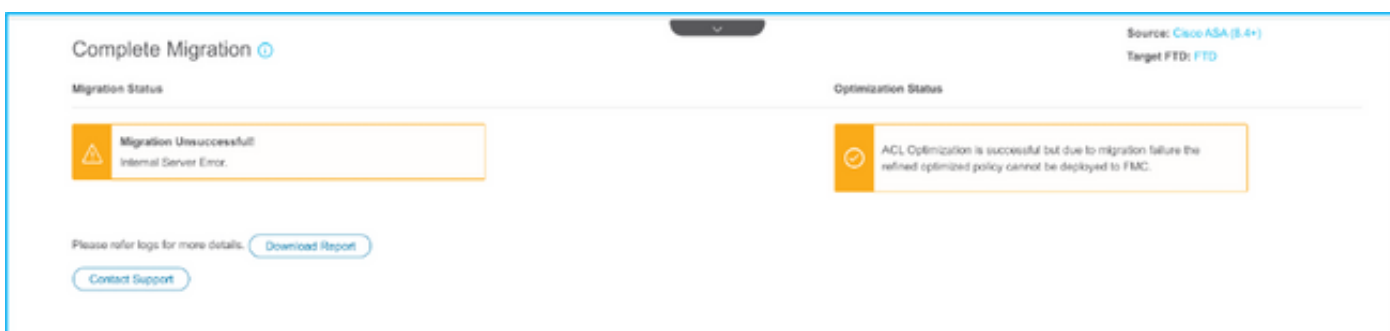
Push In progress. Refer FMT Terminal to monitor the migration status.



23. Une fois la migration réussie, le message qui s'affiche s'affiche dans l'image.



Note: Si la migration échoue, cliquez sur **Télécharger le rapport** afin d'afficher le rapport post-migration.

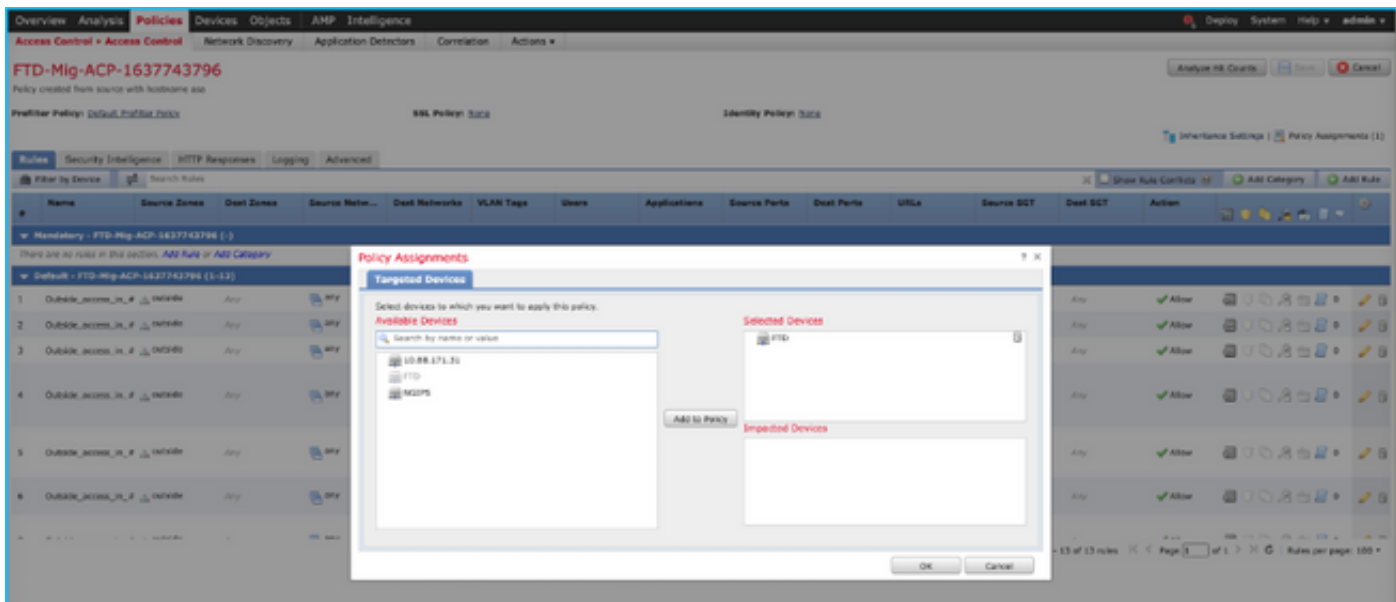


Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

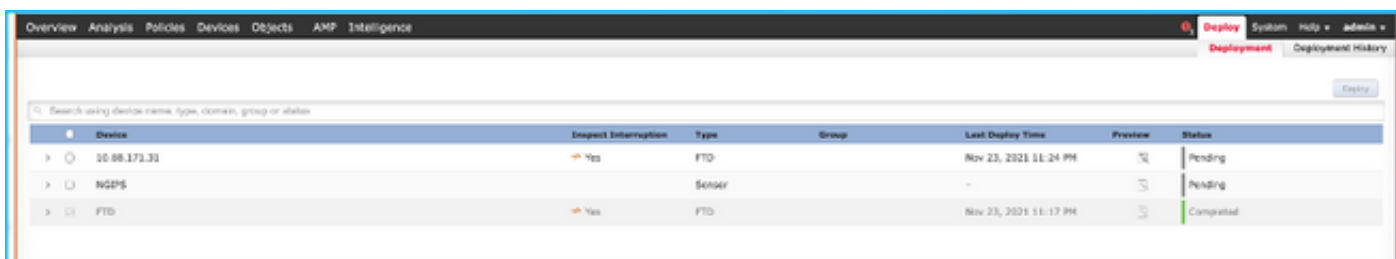
Validation sur le FMC.

1. Accédez à **Stratégies > Contrôle d'accès > Stratégie de contrôle d'accès > Affectation de stratégie** afin de confirmer que le FTD sélectionné est renseigné.



Note: La stratégie de contrôle d'accès à la migration aurait un nom avec le préfixe **FTD-Mig-ACP**. Si aucun FTD n'a été sélectionné à l'étape 2.8, le FTD doit être sélectionné sur le FMC.

2. Poussez la stratégie vers le FTD. Accédez à **Déployer > Déploiement > Nom du FTD > Déployer** comme indiqué dans l'image.



Bogues connus liés à l'outil de migration Firepower

- ID de bogue Cisco [CSCwa56374](#) - L'outil FMT se bloque sur la page de mappage de zone avec une erreur avec une utilisation élevée de la mémoire
- ID de bogue Cisco [CSCvz88730](#) - Échec de transmission d'interface pour le type d'interface de gestion Port-Channel FTD
- ID de bogue Cisco [CSCvx21986](#) - Migration Port-Channel vers la plate-forme cible - Virtual FTD non pris en charge
- ID de bogue Cisco [CSCvy63003](#) - L'outil de migration doit désactiver la fonctionnalité d'interface si FTD fait déjà partie du cluster
- ID de bogue Cisco [CSCvx08199](#) - La liste de contrôle d'accès doit être fractionnée lorsque la référence de l'application est supérieure à 50

Informations connexes

- [Migration du pare-feu ASA vers la protection contre les menaces grâce à l'outil de migration du pare-feu](#)

- [Support et documentation techniques - Cisco Systems](#)