Migrer ASA vers Firepower Threat Defense (FTD) à l'aide de FMT

Table des matières

Introduction

Ce document décrit la procédure à suivre pour migrer le dispositif de sécurité adaptatif Cisco (ASA) vers le périphérique de menace Cisco Firepower .

Conditions préalables

Exigences

Cisco recommande que vous ayez une bonne connaissance de Cisco Firewall Threat Defense (FTD) et Adaptive Security Appliance (ASA).

Composants utilisés

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

- Mac OS avec Firepower Migration Tool (FMT) v7.0.1
- Appareil de sécurité adaptatif (ASA) v9.16(1)
- Centre de gestion du pare-feu sécurisé (FMCv) v7.4.2
- Pare-feu sécurisé FTDv (Threat Defense Virtual) v7.4.1

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.

Aperçu

Les exigences spécifiques de ce document sont les suivantes :

- Appareil de sécurité adaptatif Cisco (ASA) version 8.4 ou ultérieure
- Secure Firewall Management Center (FMCv) version 6.2.3 ou ultérieure

L'outil de migration de pare-feu prend en charge cette liste de périphériques :

- Cisco ASA (8.4+)
- Cisco ASA (9.2.2+) avec FPS
- Cisco Secure Firewall Device Manager (version 7.2 et ultérieure)
- Point de contrôle (r75-r77)
- Point de contrôle (r80)
- Fortinet (5.0+)

· Réseaux de Palo Alto (6.1+)

Informations générales

Avant de migrer votre configuration ASA, exécutez les activités suivantes :

Obtenir le fichier de configuration ASA

Pour migrer un périphérique ASA, utilisez la commande show running-config pour un contexte unique ou la commande show tech-support pour le mode multi-contexte afin d'obtenir la configuration, enregistrez-la sous la forme d'un fichier .cfg ou .txt, puis transférez-la sur l'ordinateur à l'aide de l'outil de migration Secure Firewall.

Exporter le certificat PKI depuis ASA et l'importer dans Management Center

Utilisez cette commande pour exporter le certificat PKI via l'interface de ligne de commande à partir de la configuration ASA source avec les clés vers un fichier PKCS12 :
ASA(config)#crypto ca export <trust-point-name> pkcs12 <phrase de passe>
Importez ensuite le certificat PKI dans un centre de gestion (Objets PKI de gestion d'objets). Pour plus d'informations, consultez Objets PKI dans le Guide de configuration de Firepower Management Center.

Récupérer les packages et profils AnyConnect

Les profils AnyConnect sont facultatifs et peuvent être téléchargés via le centre de gestion ou

l'outil de migration Secure Firewall.

Utilisez cette commande pour copier le package requis de l'ASA source vers un serveur FTP ou TFTP :

Copier <emplacement du fichier source : /nom du fichier source> <destination>

ASA# copy disk0:/anyconnect-win-4.10.02086-webdeploy-k9.pkg tftp://1.1.1.1 <----- Exemple de copie du package Anyconnect.

ASA# copy disk0:/ external-sso- 4.10.04071-webdeploy-k9.zip tftp://1.1.1.1 <----- Exemple de copie du package de navigateur externe.

ASA# copy disk0:/ hostscan_4.10.04071-k9.pkg tftp://1.1.1.1 <----- Exemple de copie du package Hostscan.

ASA# copy disk0:/ dap.xml tftp://1.1.1.1. <----- Exemple de copie de Dap.xml

ASA# copy disk0:/ sdesktop/data.xml tftp://1.1.1.1 <----- Exemple de copie de Data.xml

ASA# copy disk0:/ VPN_Profile.xml tftp://1.1.1.1 <----- Exemple de copie du profil Anyconnect.

Importez les packages téléchargés dans le centre de gestion (Object Management > VPN > AnyConnect File).

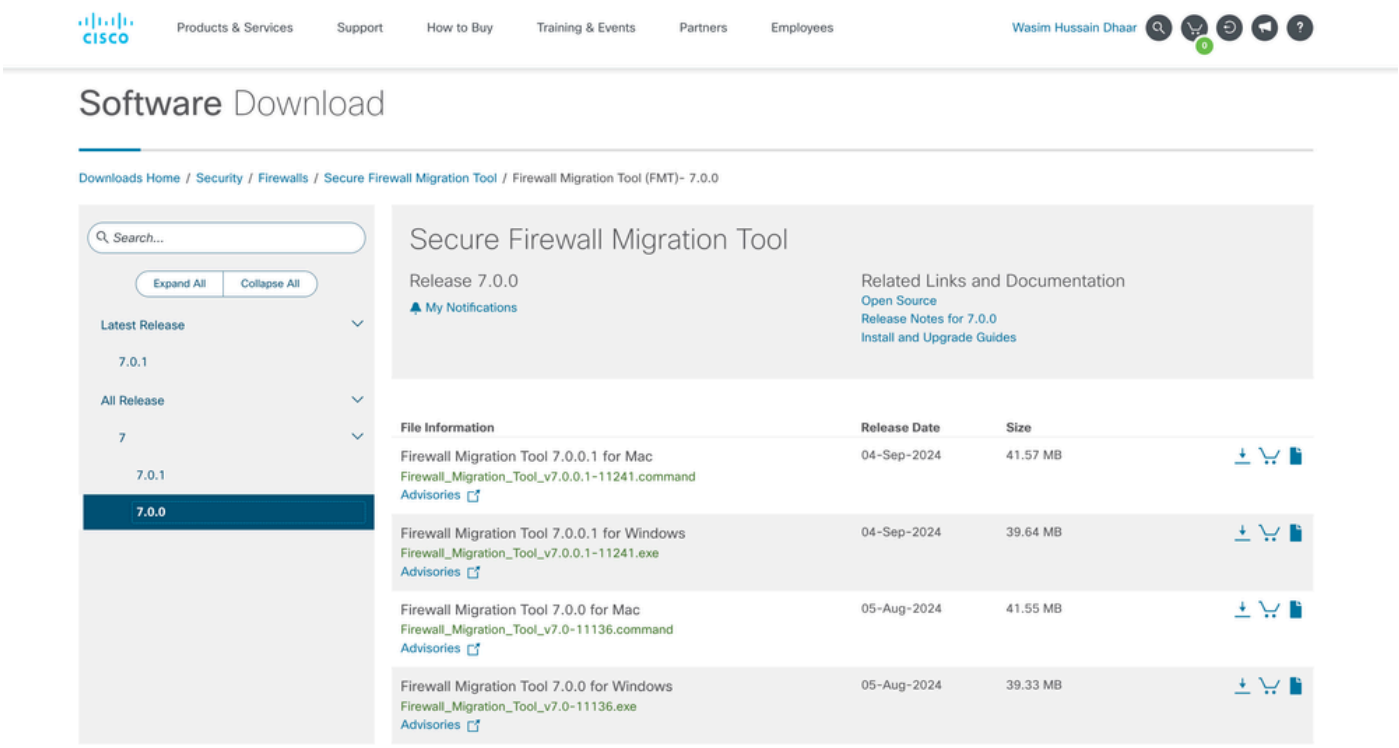
a-Dap.xml et Data.xml doivent être téléchargés vers le centre de gestion à partir de l'outil de migration Secure Firewall dans la section Review and Validate > Remote Access VPN > AnyConnect File.

b-Les profils AnyConnect peuvent être téléchargés directement vers le centre de gestion ou via l'outil de migration Secure Firewall dans la section Review and Validate > Remote Access VPN > AnyConnect File.

Configurer

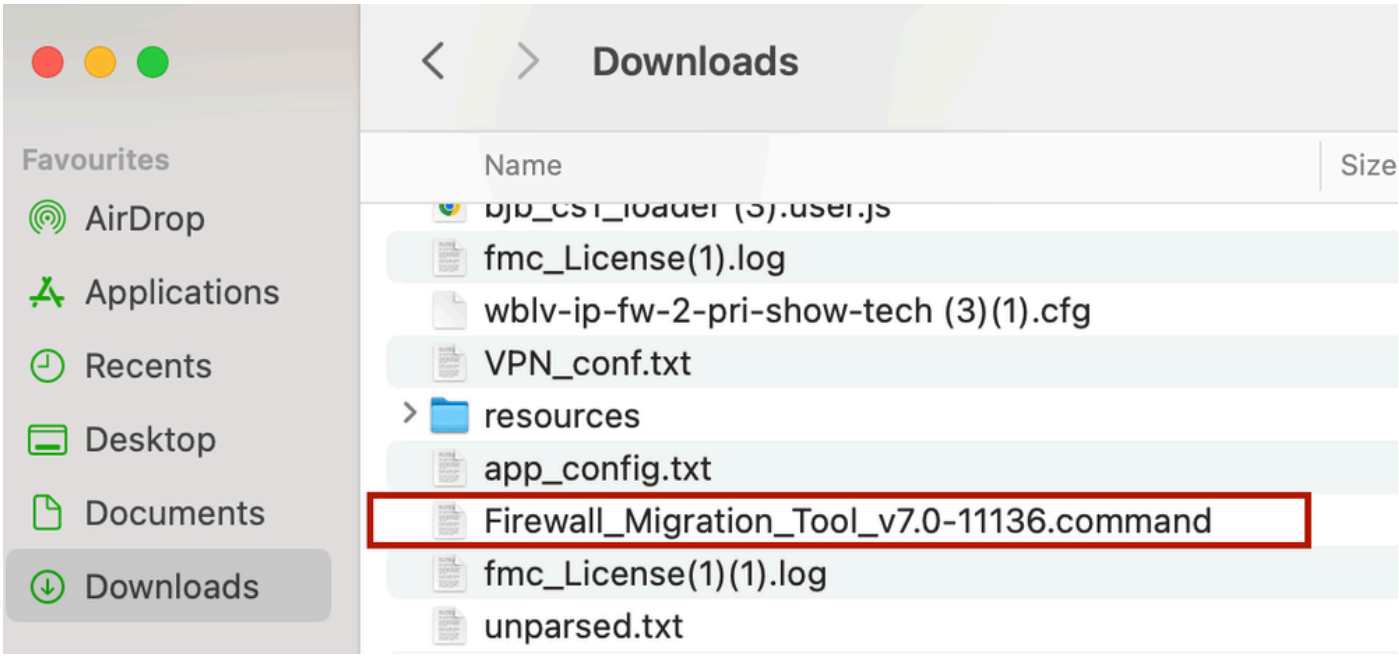
Configuration Steps:

1.Télécharger l'outil de migration Firepower le plus récent de Cisco Software Central :

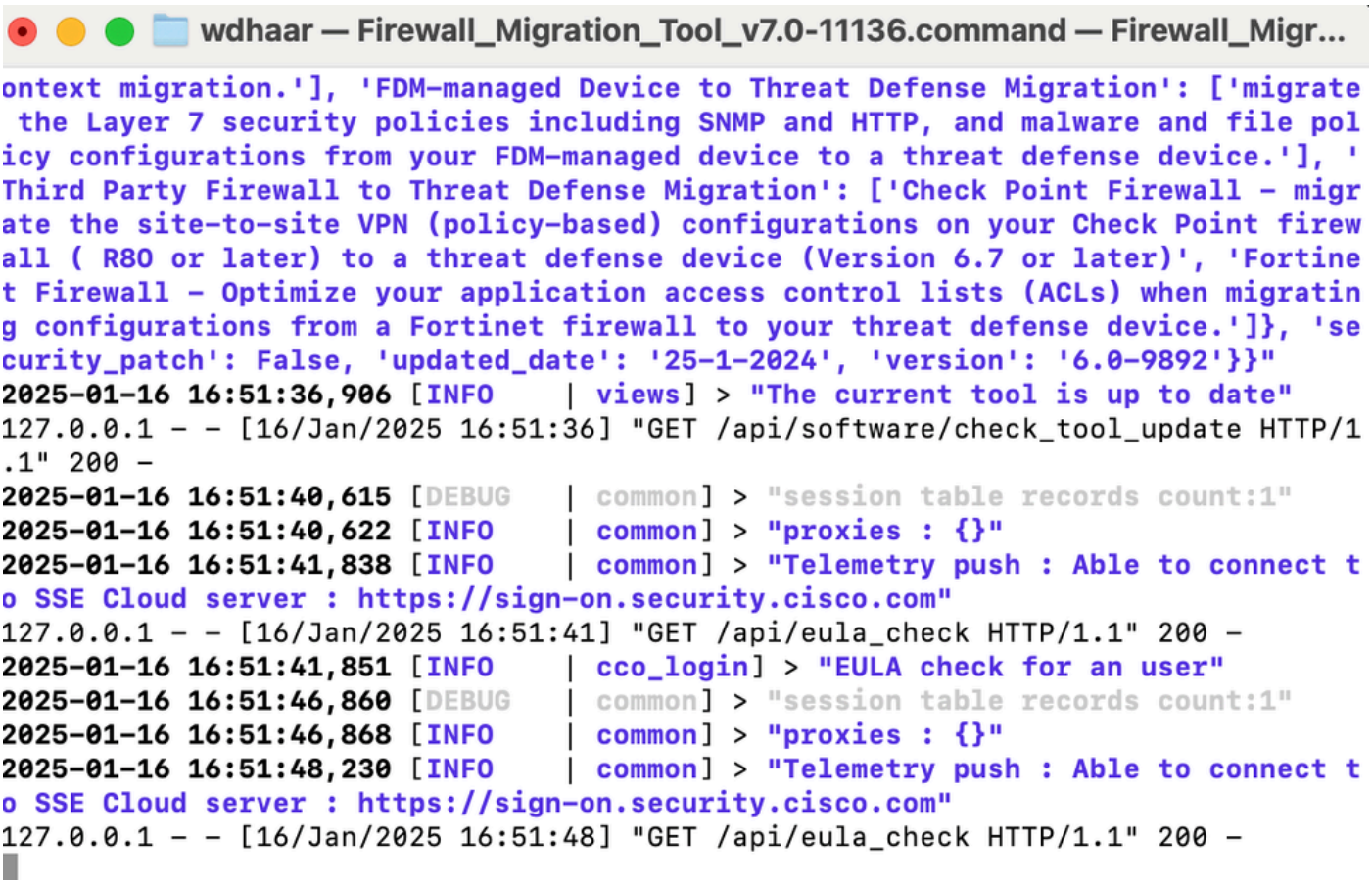


Téléchargement du logiciel

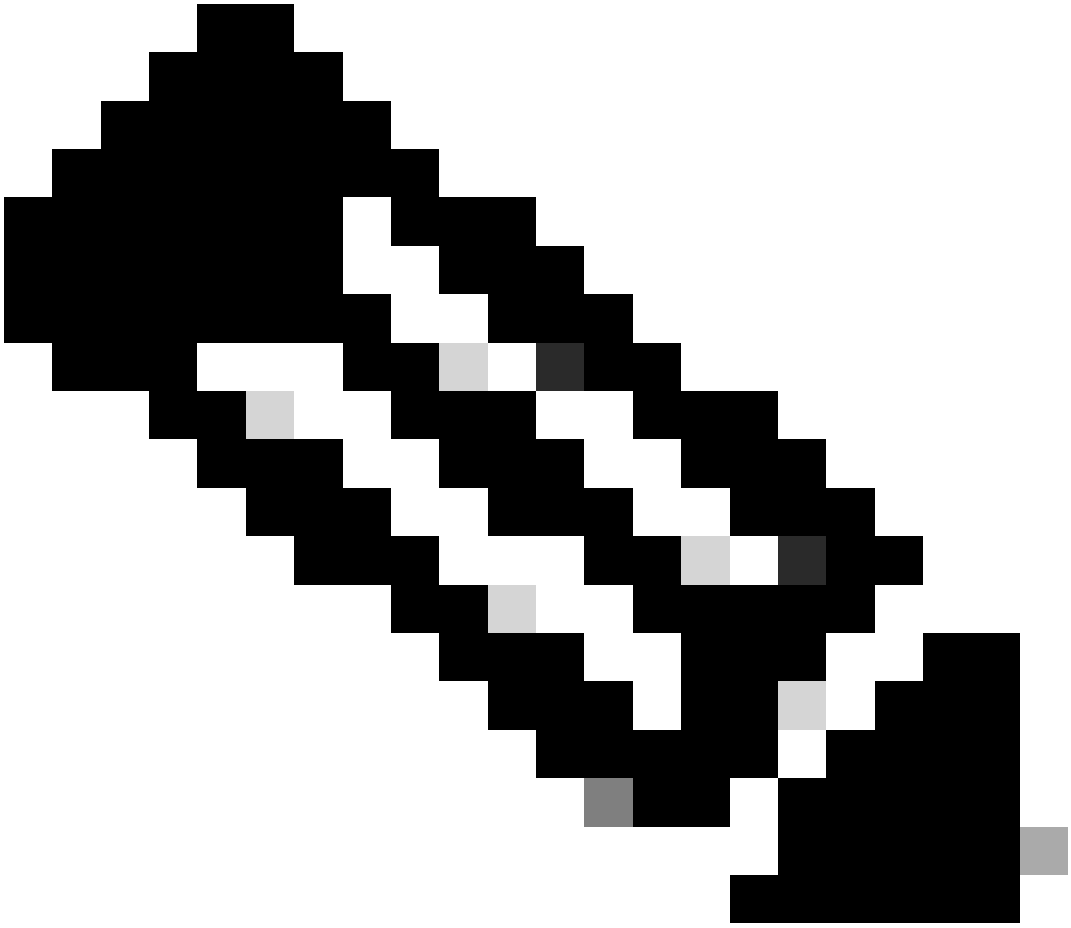
2. Cliquez sur le fichier que vous avez précédemment téléchargé sur votre ordinateur.



Le fichier

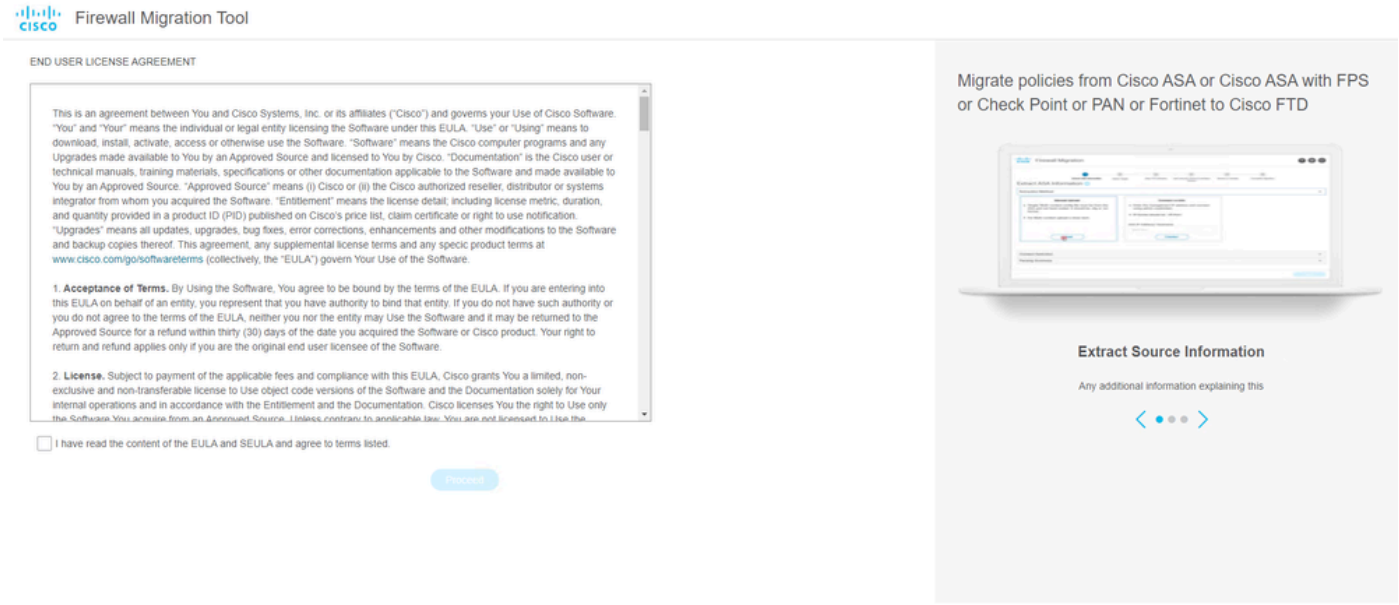


Journaux de console



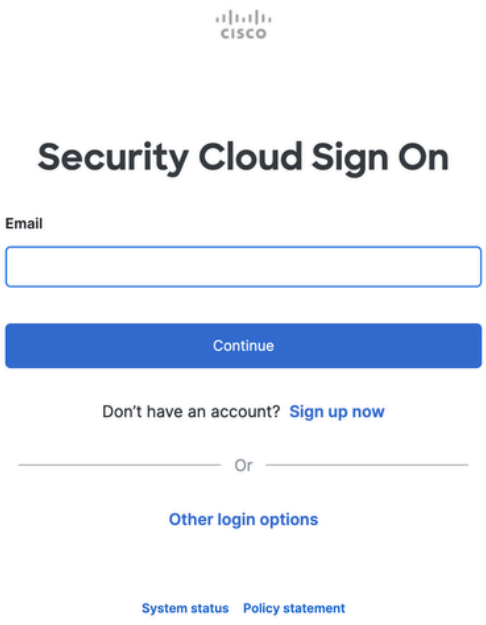
Remarque : Le programme s'ouvre automatiquement et une console génère automatiquement du contenu dans le répertoire dans lequel vous avez exécuté le fichier.

3. Une fois le programme exécuté, un navigateur Web s'ouvre et affiche le « Contrat de licence utilisateur final ».
    1. Cochez cette case pour accepter les conditions générales.
    2. Cliquez sur Continuer.



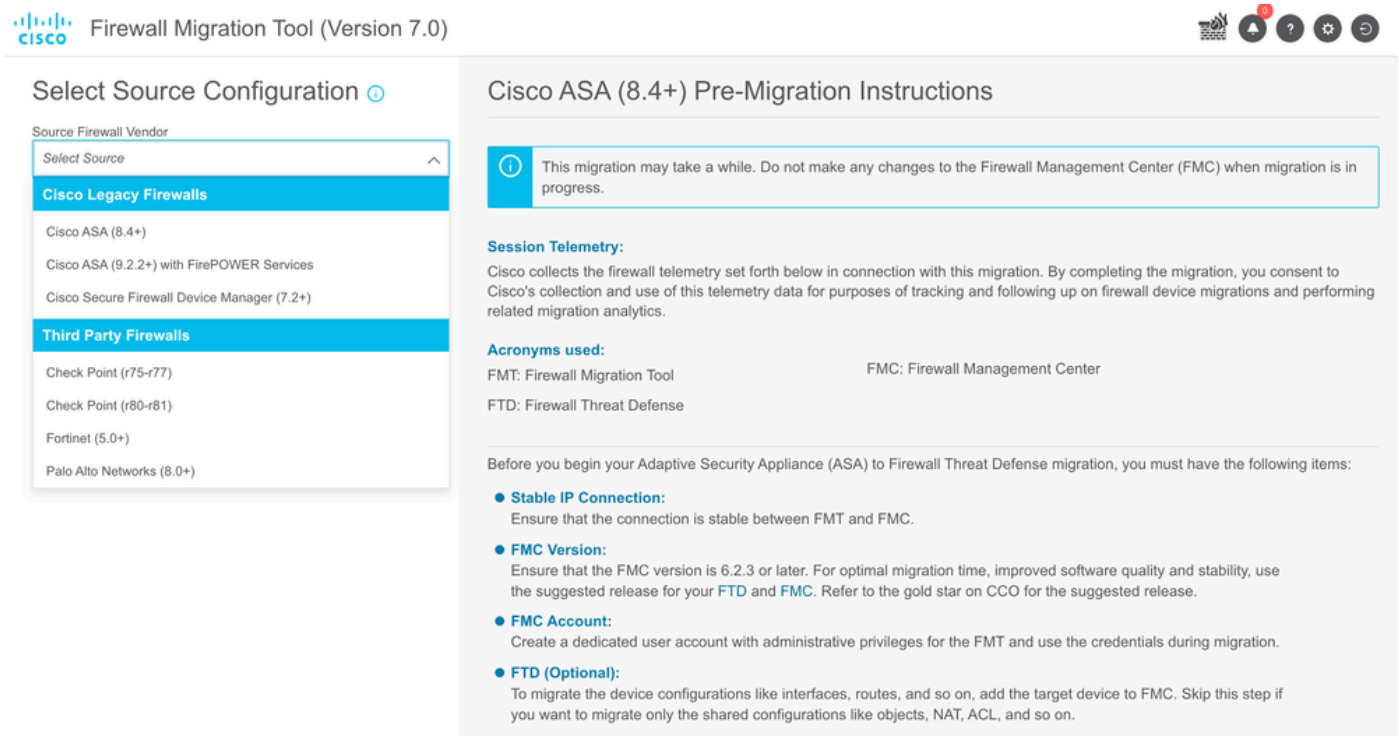
CLUF

4. Connectez-vous à l'aide d'un compte CCO valide et l'interface utilisateur graphique FMT apparaît dans le navigateur Web.



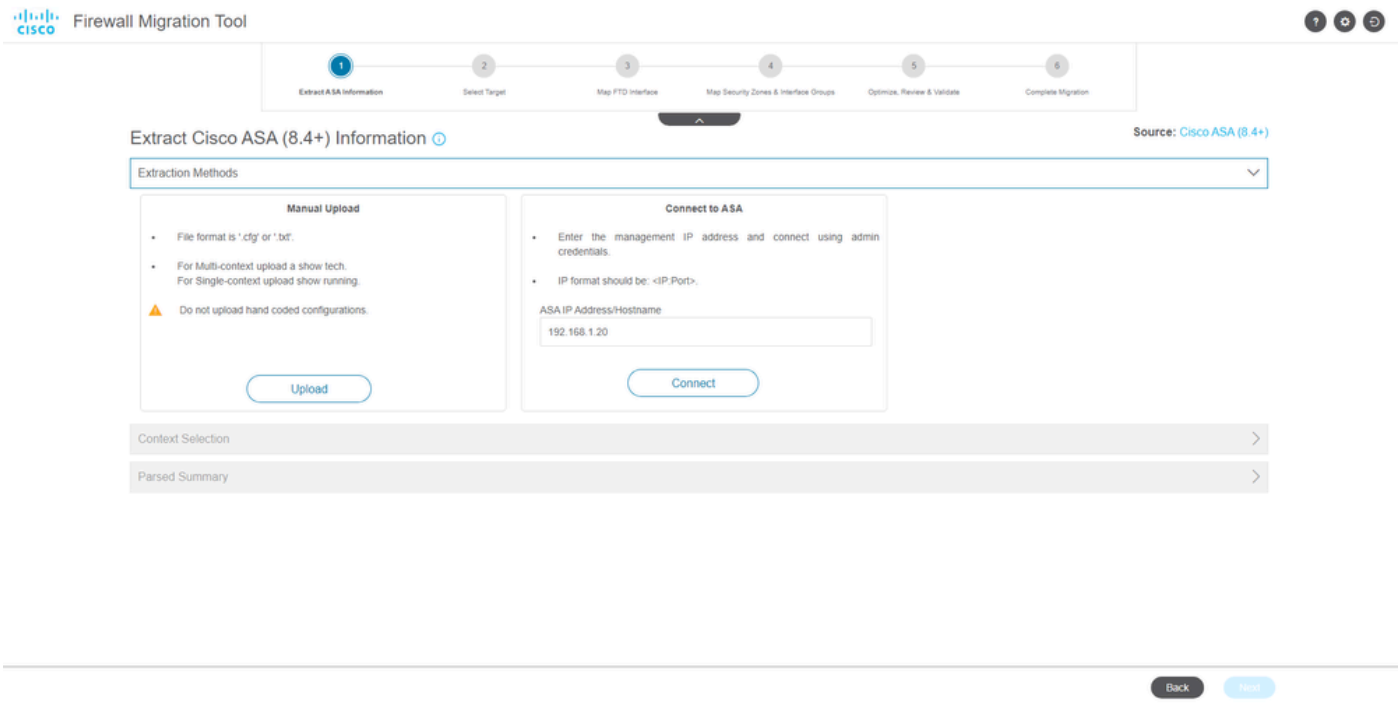
Connexion FMT

5. Sélectionnez le pare-feu source à migrer.

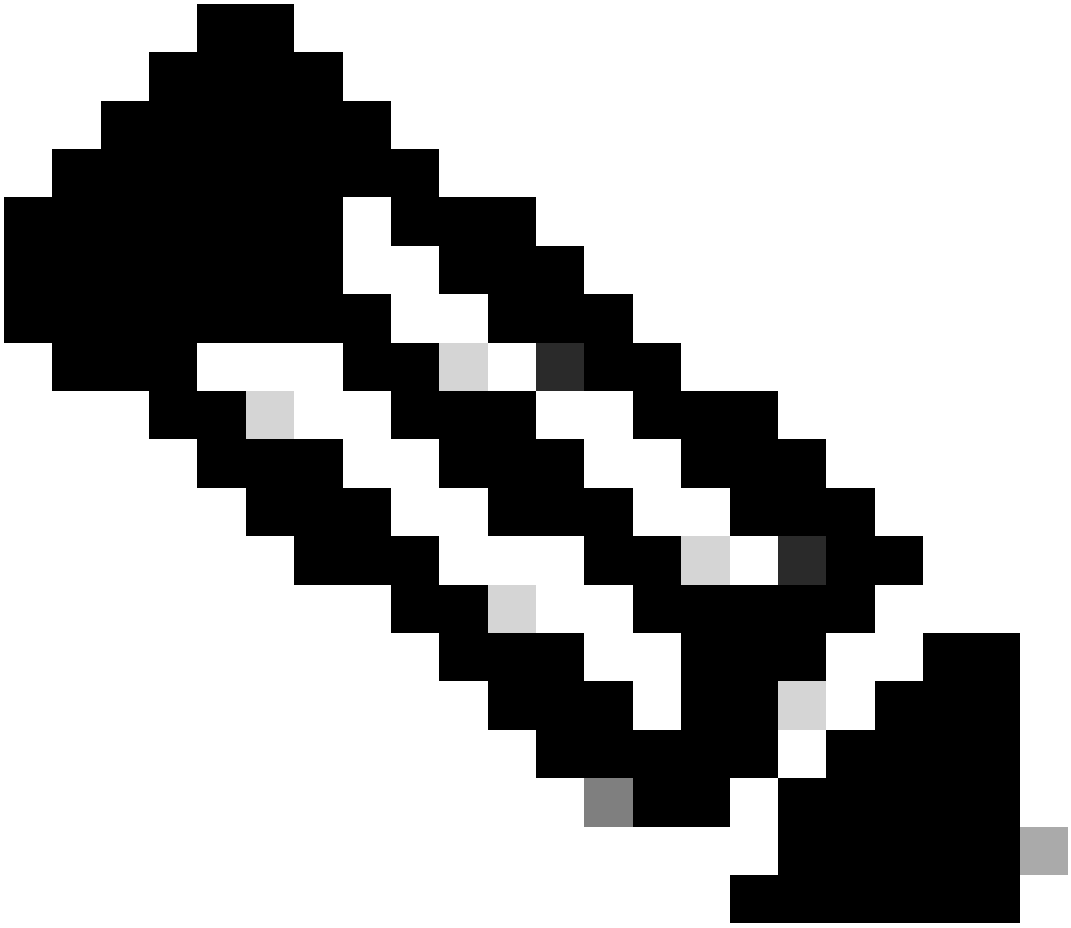


Pare-feu source

6. Sélectionnez la méthode d'extraction à utiliser pour obtenir la configuration.
    1. Manual Upload (Téléchargement manuel) nécessite que vous téléchargiez le **Running Config** fichier de l'ASA au format « .cfg » ou « .txt ».
    2. Connectez-vous à l'ASA pour extraire les configurations directement du pare-feu.

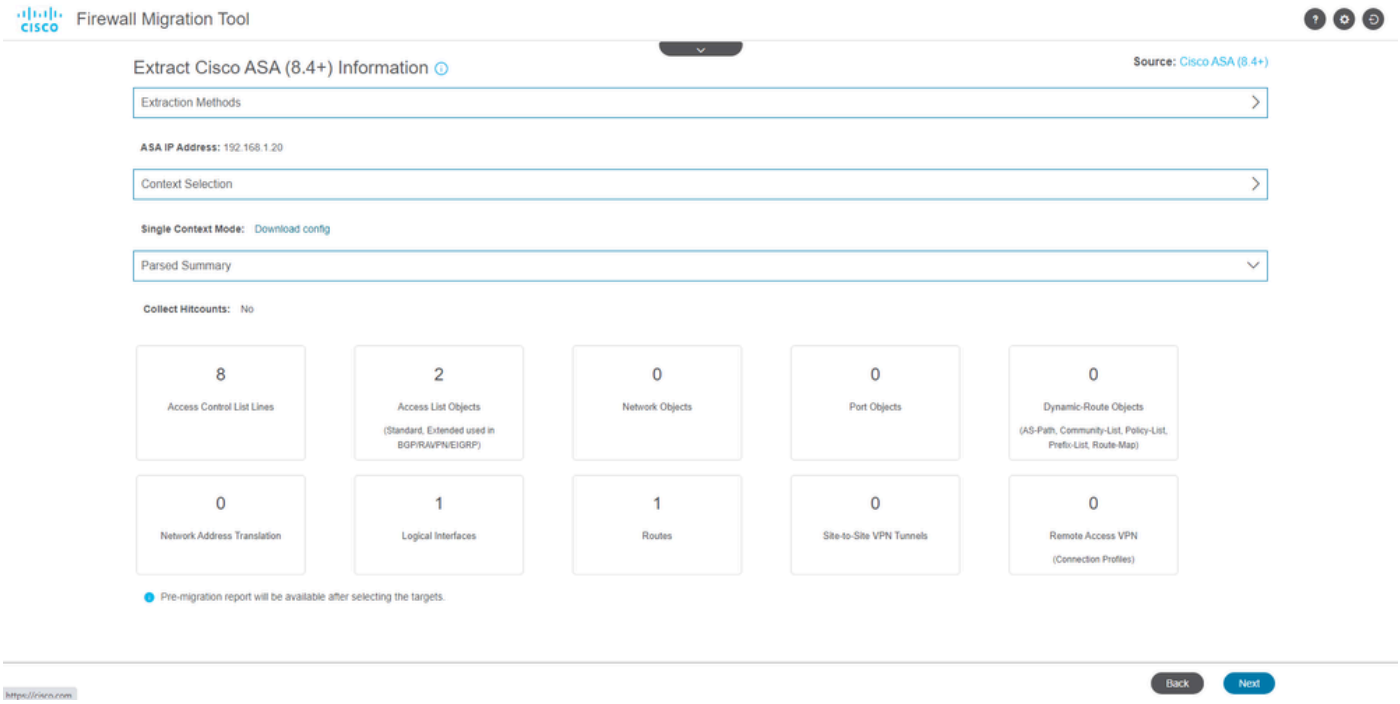


Extraction



Remarque : Dans cet exemple, connectez-vous directement à l'ASA.

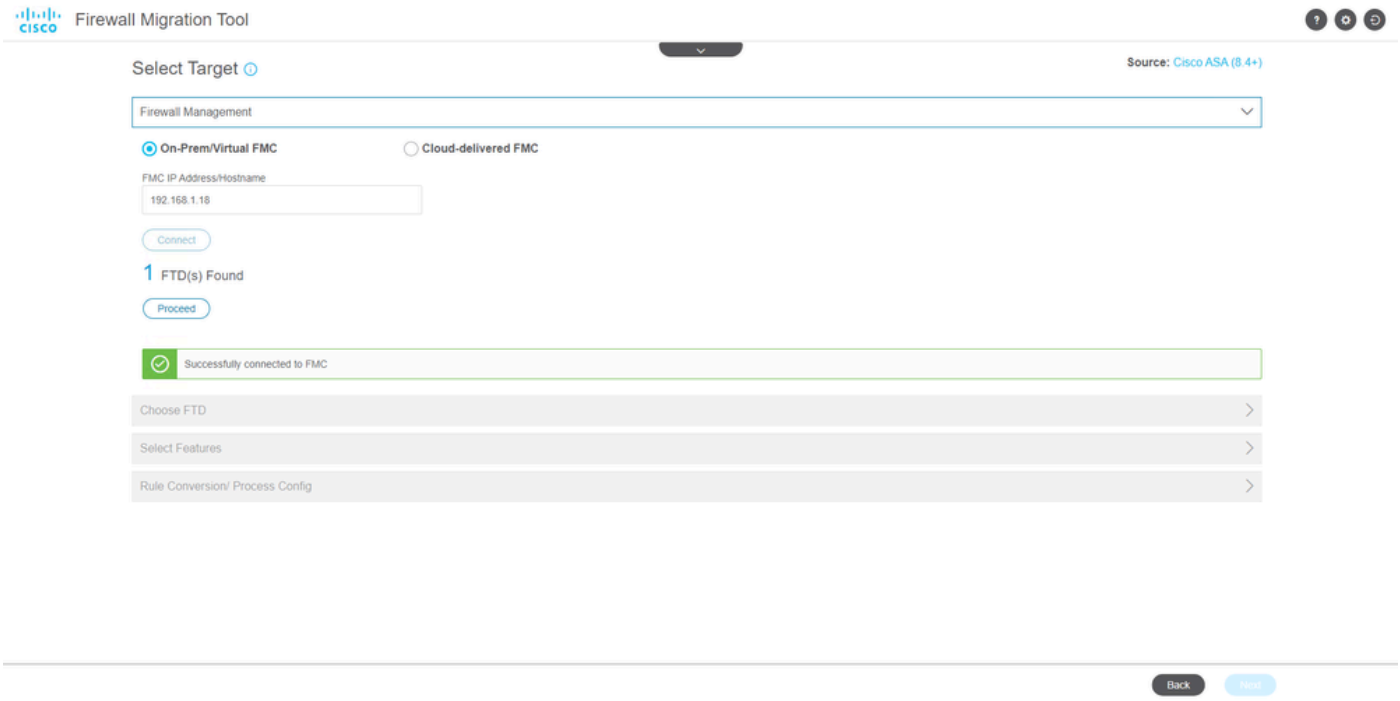
7. Un résumé de la configuration trouvée sur le pare-feu s'affiche sous la forme d'un tableau de bord, cliquez sur Next.



Résumé

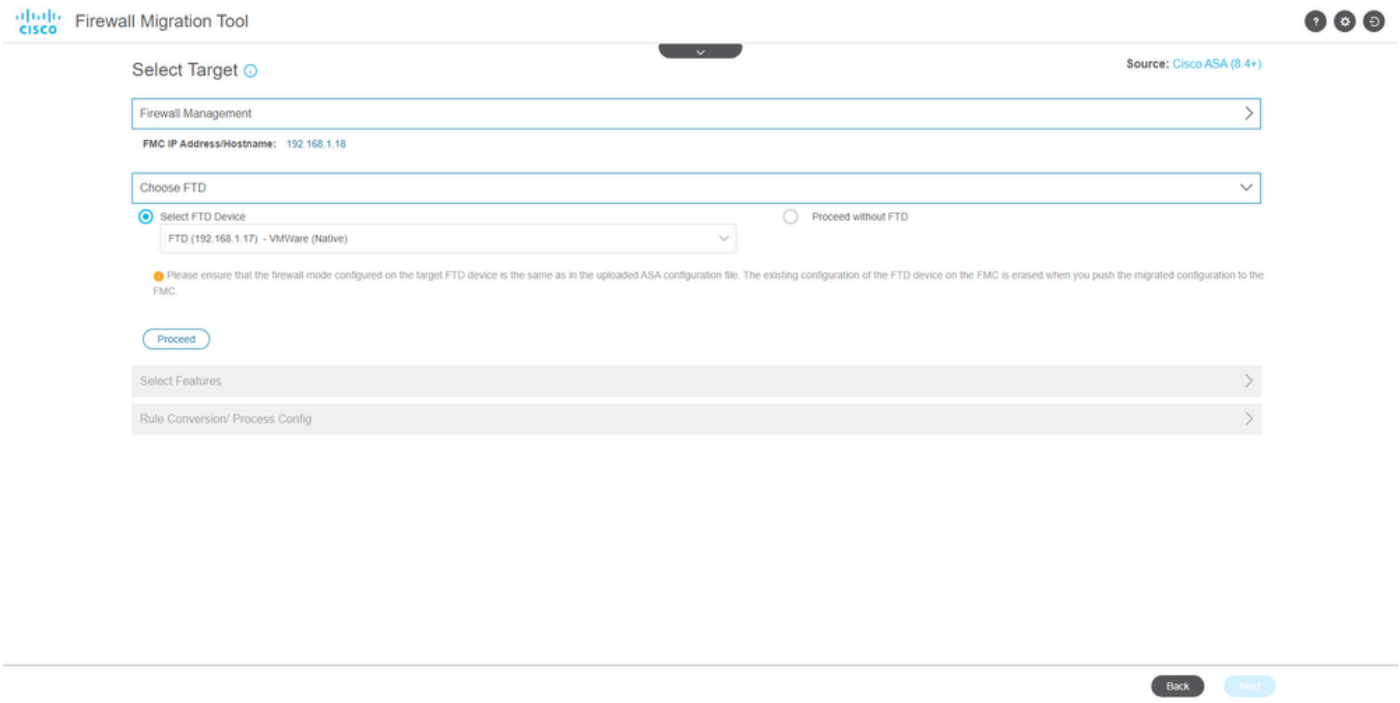
8. Sélectionnez le FMC cible à utiliser lors de la migration.

Indiquez l'adresse IP du FMC.Une fenêtre contextuelle s'ouvre et vous invite à entrer les informations d'identification de connexion du FMC.



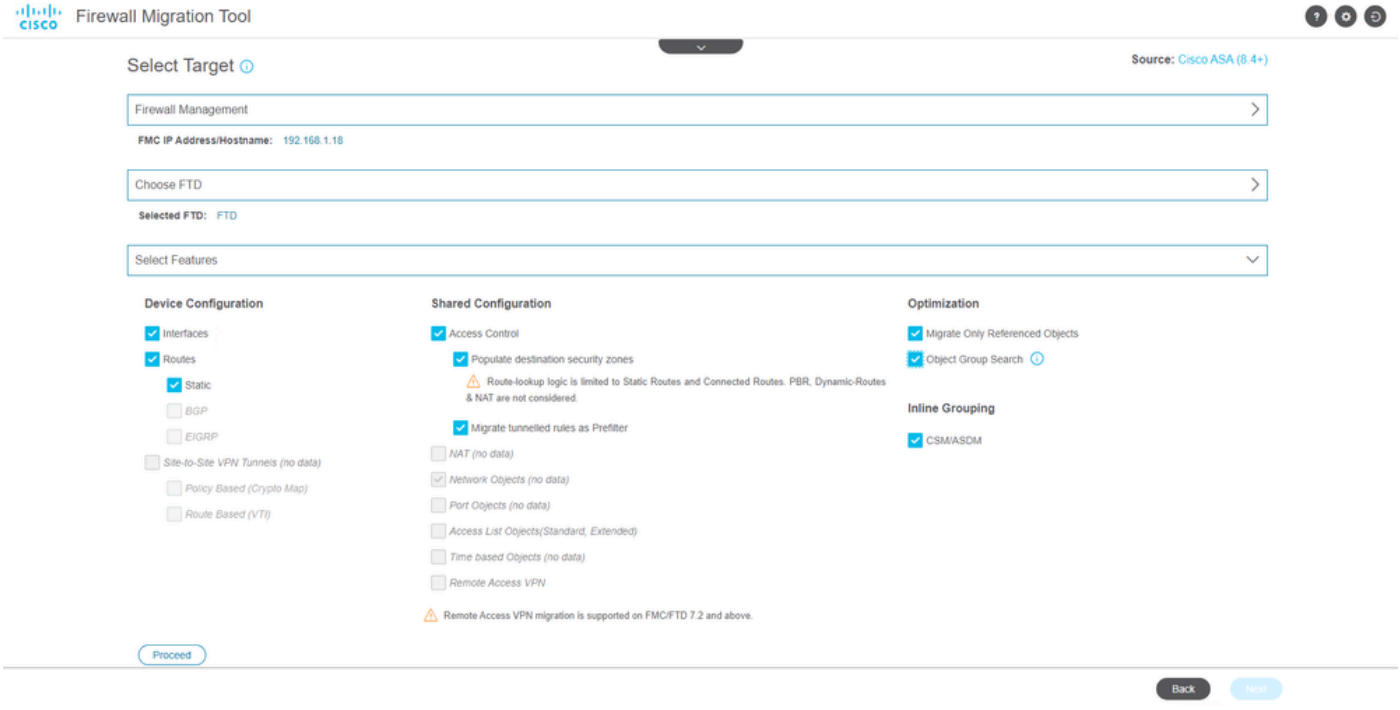
IP FMC

9. (Facultatif)Sélectionnez le FTD cible que vous souhaitez utiliser.
    1. Si vous choisissez de migrer vers un FTD, sélectionnez le FTD que vous souhaitez utiliser.
    2. Si vous ne souhaitez pas utiliser de FTD, vous pouvez cocher la case Proceed without FTD



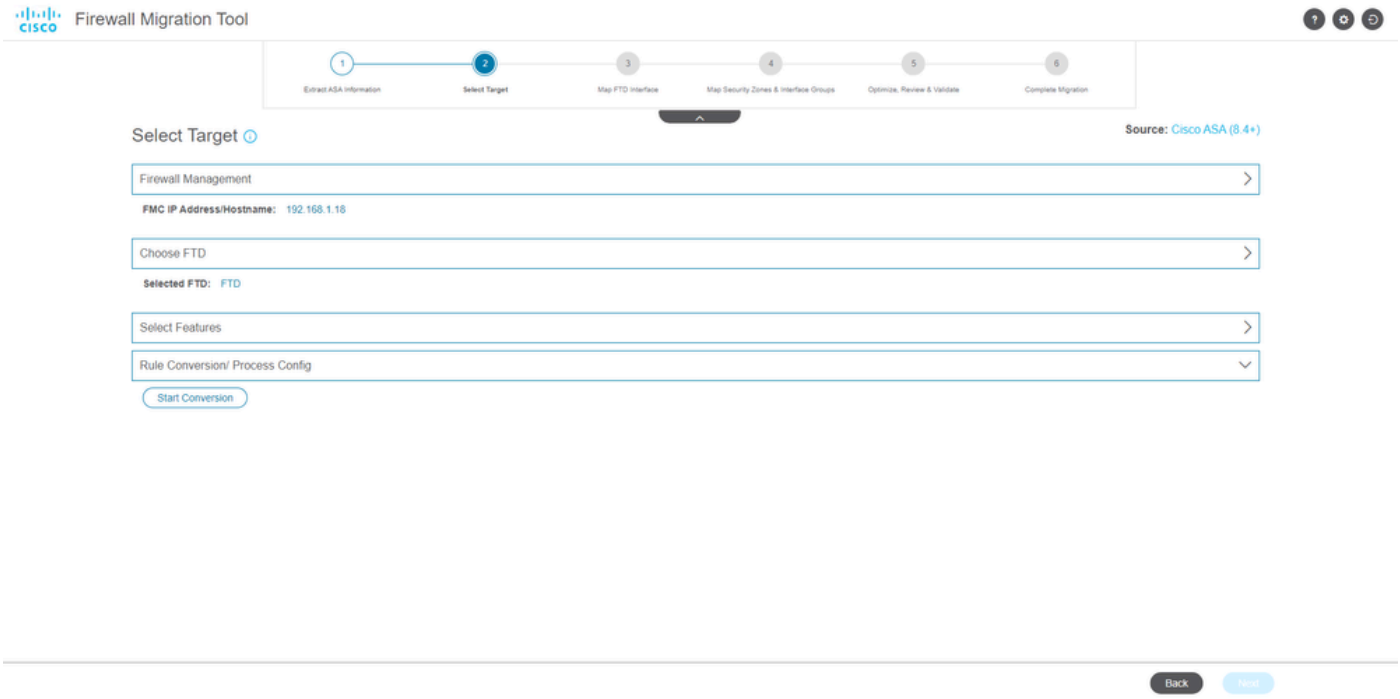
Objectif FTD

10. Sélectionnez les configurations que vous souhaitez migrer, les options sont affichées sur les captures d'écran.



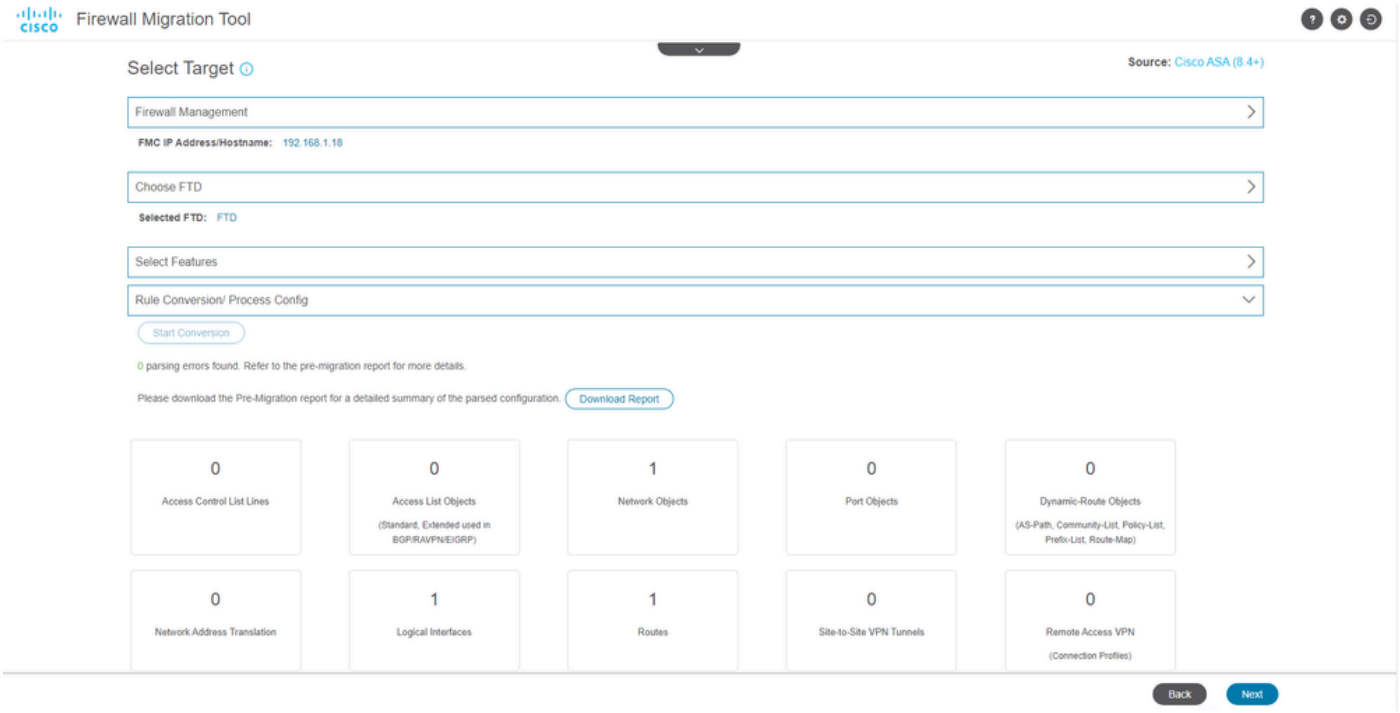
Configurations

11. Commencez la conversion des configurations de ASA en FTD.



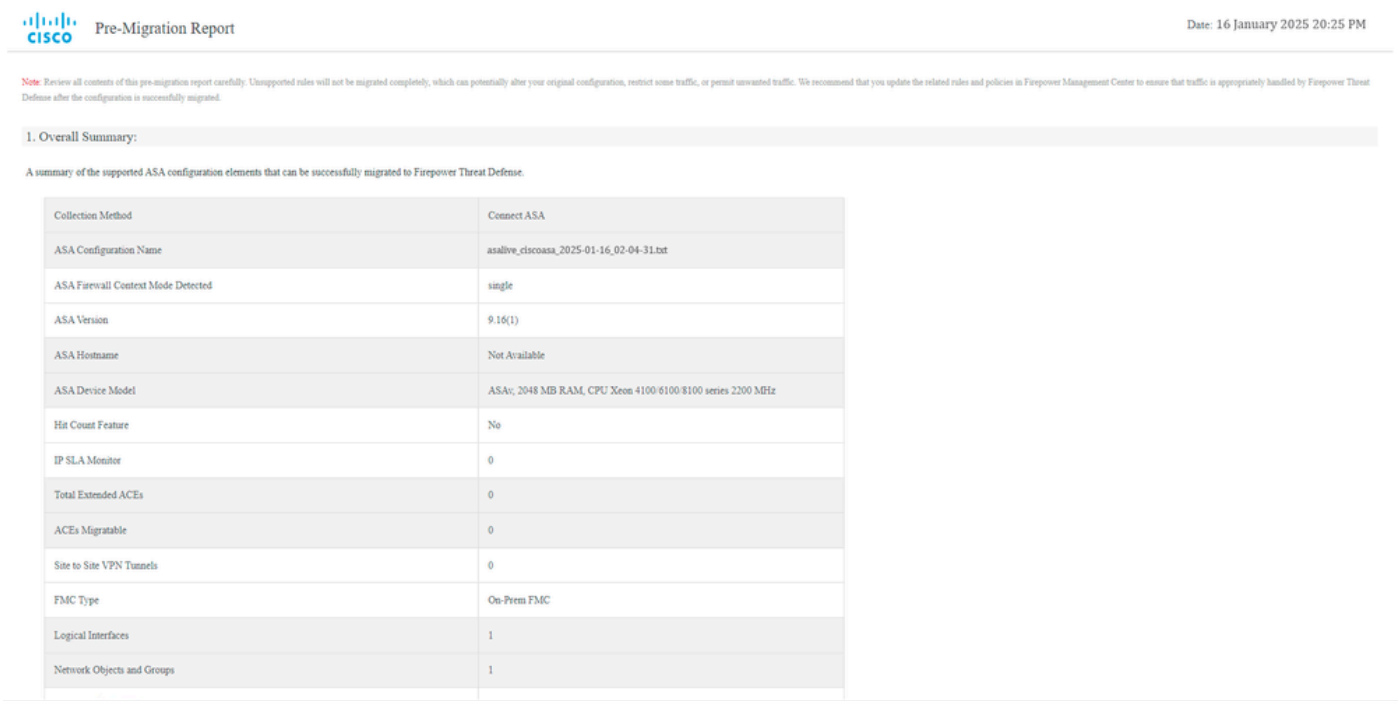
Démarrer la conversion

12. Une fois la conversion terminée, il affiche un tableau de bord avec le résumé des objets à migrer (limité à la compatibilité).
    1. Vous pouvez éventuellement cliquer sur **Download Report** pour recevoir un résumé des configurations à migrer.



Télécharger le rapport

Exemple de rapport de pré-migration, comme illustré dans l'image :



Pre-Migration Report

Date: 16 January 2025 20:25 PM

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

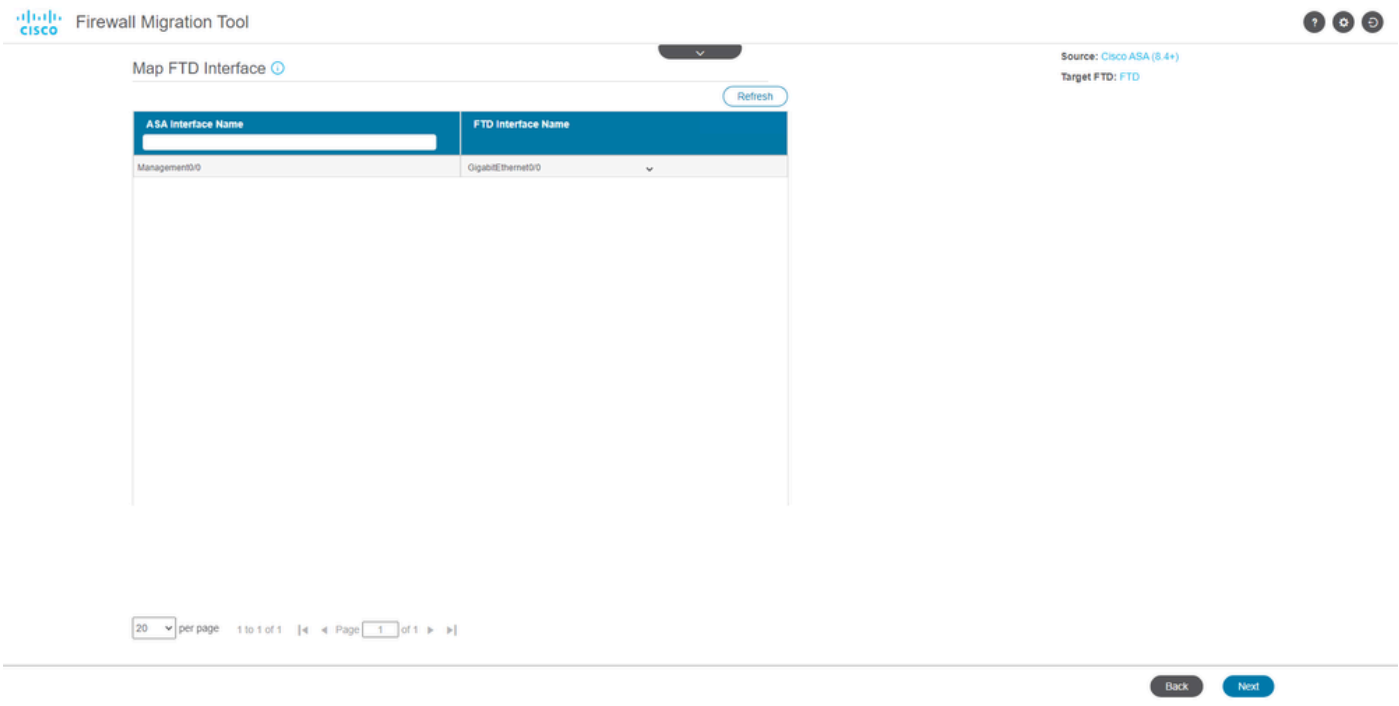
1. Overall Summary:

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

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

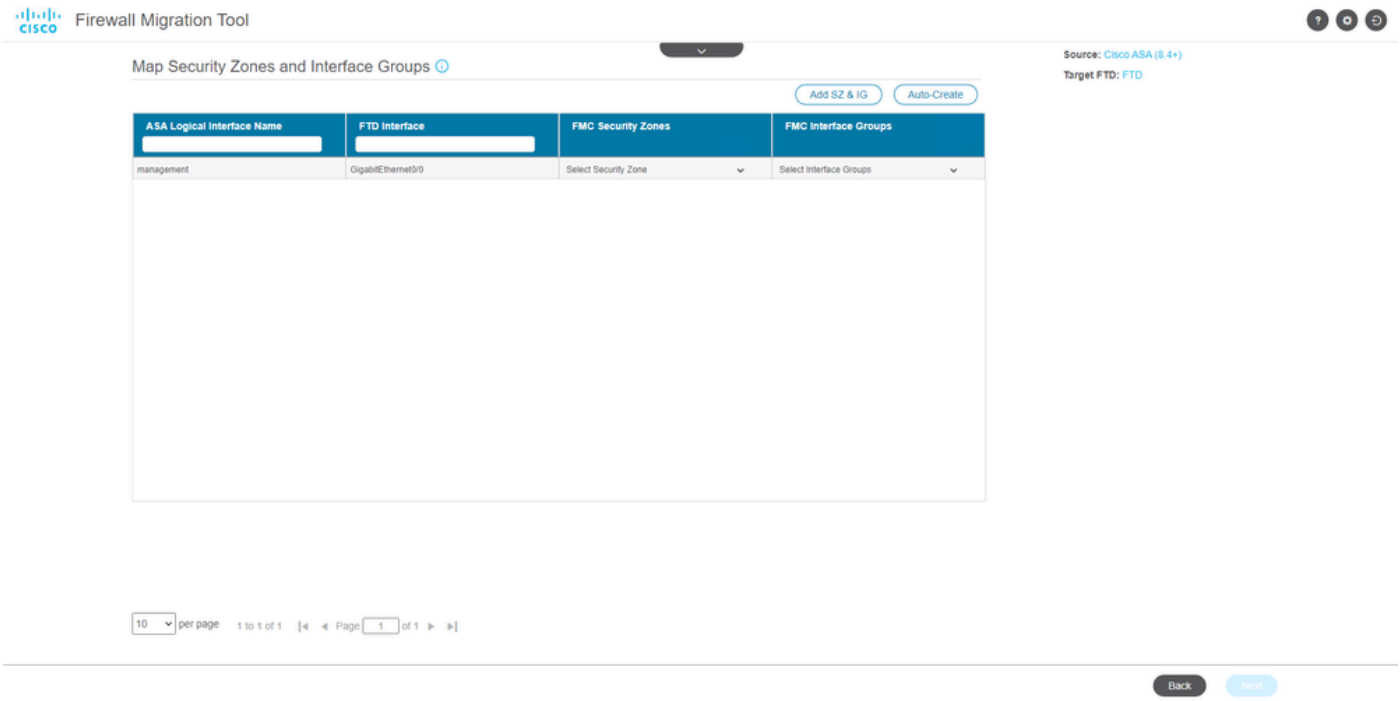
Rapport de pré-migration

13. Mappez les interfaces ASA avec les interfaces FTD sur l'outil de migration.



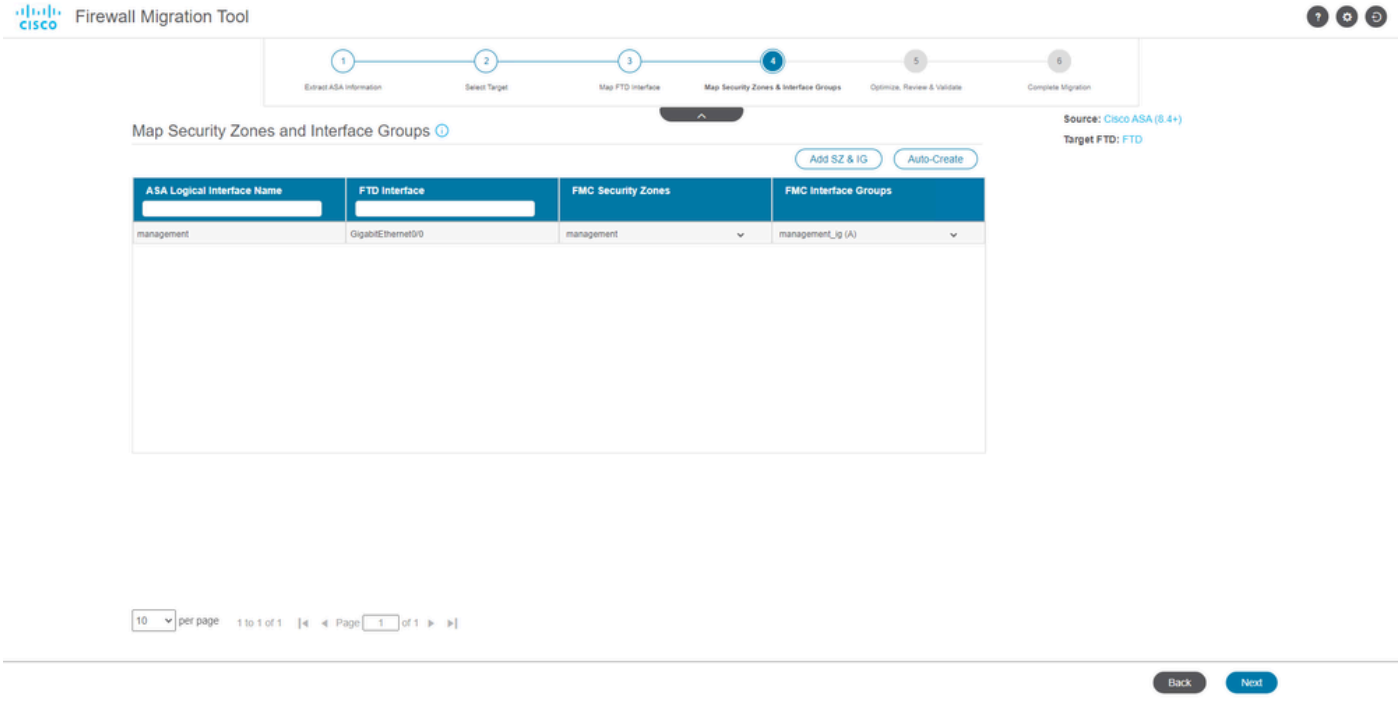
Mapper les interfaces

14. Créez les zones de sécurité et les groupes d'interfaces pour les interfaces sur le FTD



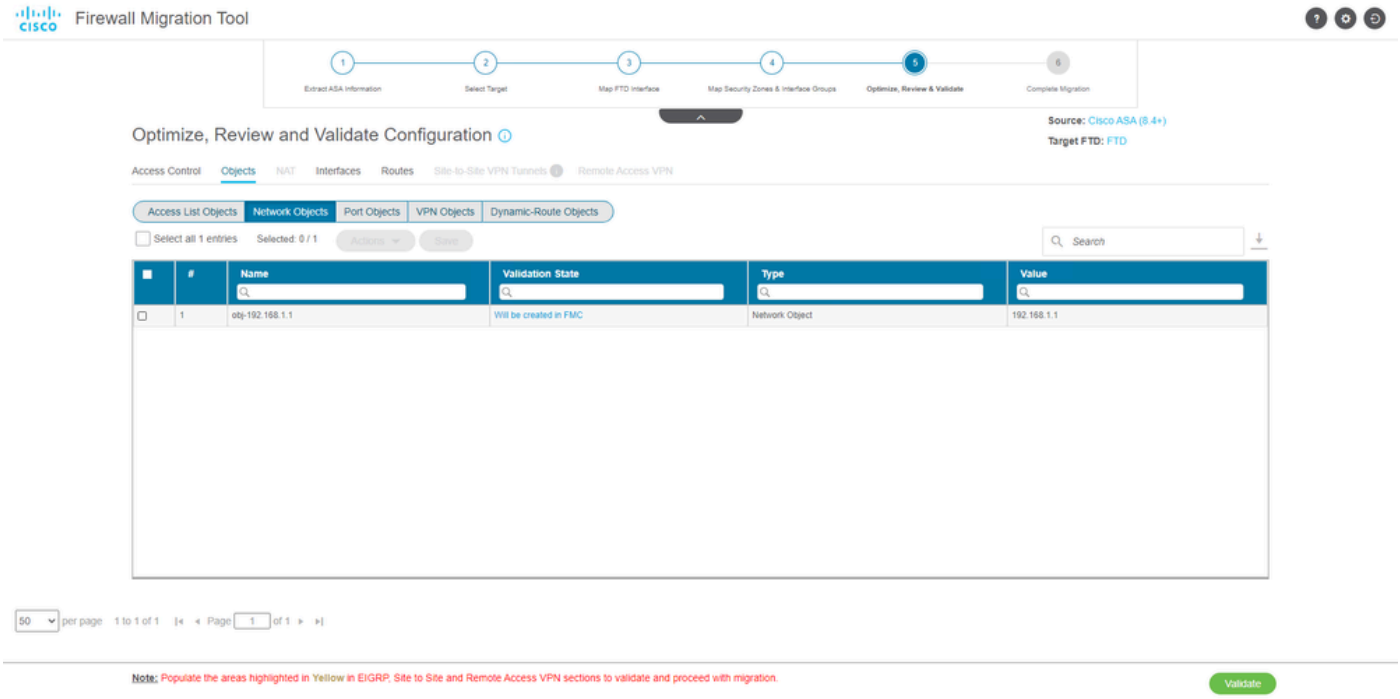
Zones de sécurité et groupes d'interfaces

Les zones de sécurité (SZ) et les groupes d'interfaces (IG) sont créés automatiquement par l'outil, comme illustré dans l'image :



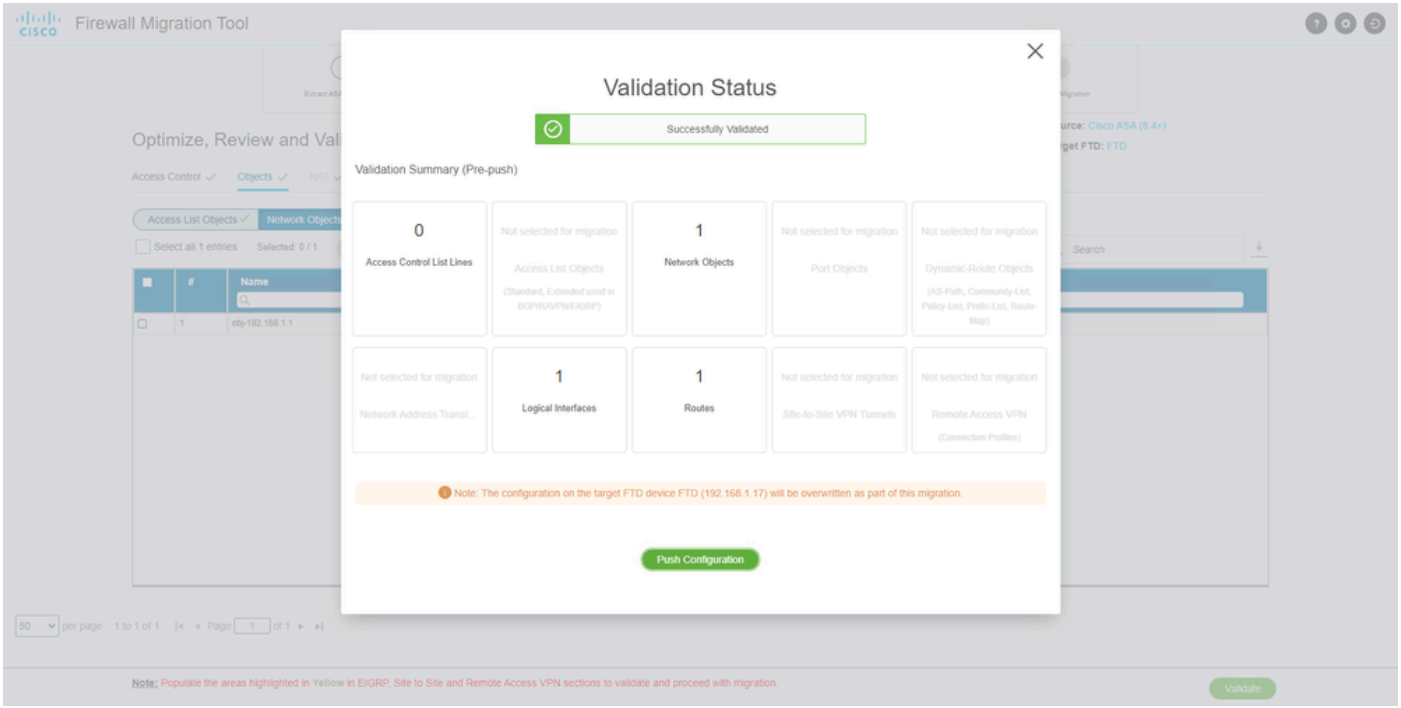
Outil de création automatique

15. Vérifiez et validez les configurations à migrer dans l'outil de migration.
    1. Si vous avez déjà terminé la révision et l'optimisation des configurations, cliquez surValidate.



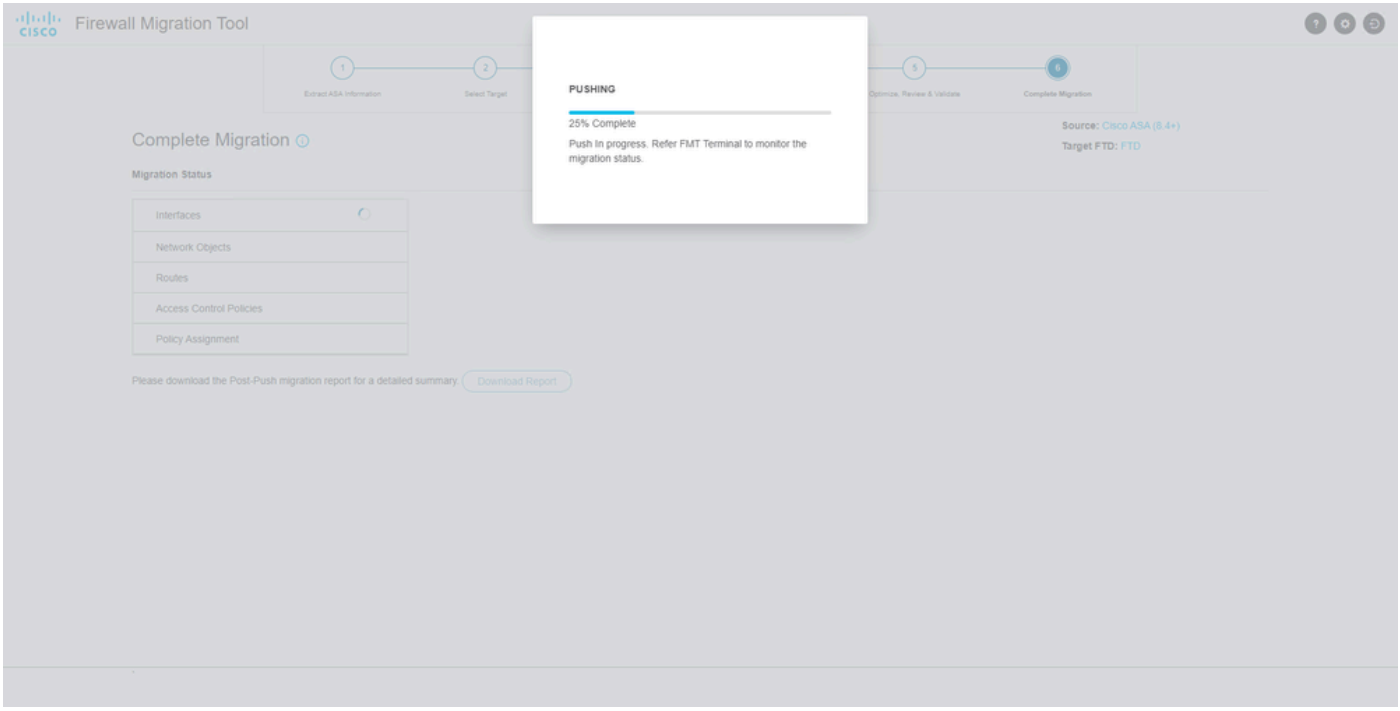
Vérifier et valider

16. Si l'état de validation est réussi, envoyez les configurations aux équipements cibles.



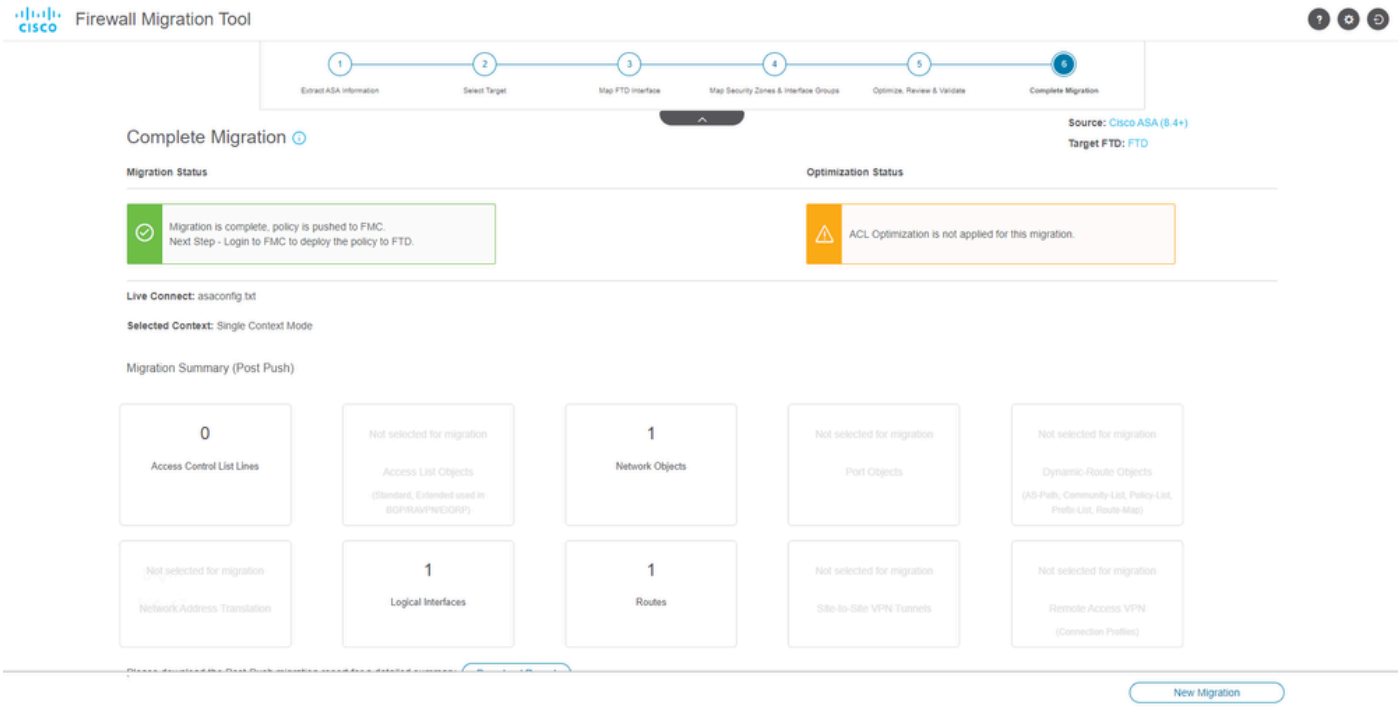
Validation

Exemple de configuration poussée à travers l'outil de migration, comme illustré dans l'image :



Pousser

Exemple d'une migration réussie, comme illustré dans l'image :



Migration réussie

(Facultatif) Si vous avez choisi de migrer la configuration vers un FTD, un déploiement est nécessaire pour transmettre la configuration disponible du FMC au pare-feu.

Afin de déployer la configuration :

1. Connectez-vous à l'interface graphique FMC.
2. Accédez à l'Deployonglet.

3. Sélectionnez le déploiement pour transmettre la configuration au pare-feu.
4. Cliquez sur Deploy.

Dépannage

Dépannage de l'outil de migration Secure Firewall

- Échecs de migration courants :
    - Caractères inconnus ou non valides dans le fichier de configuration ASA.
    - Éléments de configuration manquants ou incomplets.
    - Problèmes de connectivité réseau ou latence.
    - Problèmes lors du téléchargement ou de la diffusion de la configuration vers le centre de gestion.
    - Les problèmes courants sont les suivants :
- Utilisation du bundle d'assistance pour le dépannage :
    - Dans l'écran « Terminer la migration », cliquez sur le bouton Support.
    - Sélectionnez Support Bundle et choisissez les fichiers de configuration à télécharger.
    - Les fichiers journaux et de base de données sont sélectionnés par défaut.
    - Cliquez sur Download pour obtenir un fichier .zip.
    - Extrayez le fichier .zip pour afficher les journaux, la base de données et les fichiers de configuration.
    - Cliquez sur Email us pour envoyer les détails de l'échec à l'équipe technique.
    - Joignez le bundle d'assistance dans votre e-mail.
    - Cliquez sur Visiter la page TAC pour créer un dossier TAC Cisco pour obtenir de l'aide.
    - L'outil vous permet de télécharger un bundle de support pour les fichiers journaux, les bases de données et les fichiers de configuration.
    - Étapes de téléchargement :
    - Pour obtenir une assistance supplémentaire :

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.