

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

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Aperçu](#)

[Informations générales](#)

[Obtenir le fichier de configuration ASA](#)

[Exporter le certificat PKI depuis ASA et l'importer dans Management Center](#)

[Récupérer les packages et profils AnyConnect](#)

[Configurer](#)

[Configuration Steps:](#)

[Dépannage](#)

[Dépannage de l'outil de migration Secure Firewall](#)

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 :

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](#)

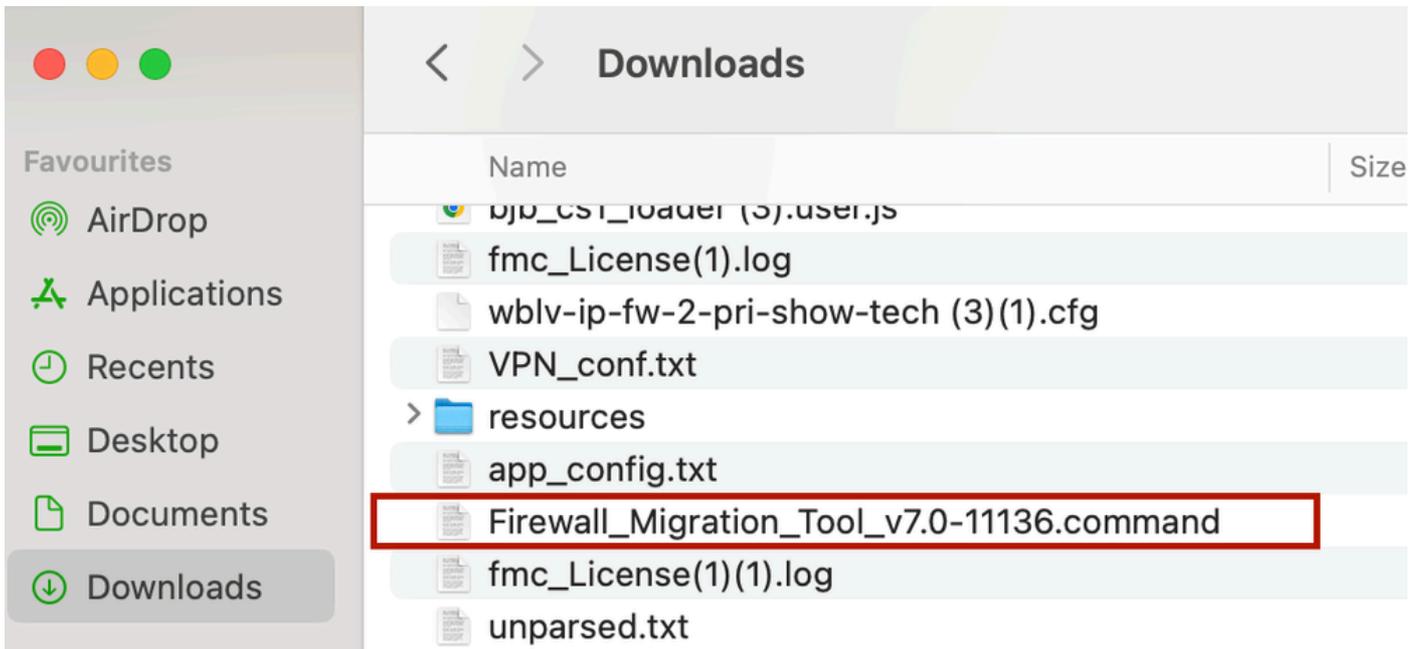
[Release Notes for 7.0.0](#)

[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	↓ 🛒 📄

Téléchargement du logiciel

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



Le fichier

```
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 -
```



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.

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, and Cisco does not license 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



CLUF

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



Security Cloud Sign On

Email

Continue

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

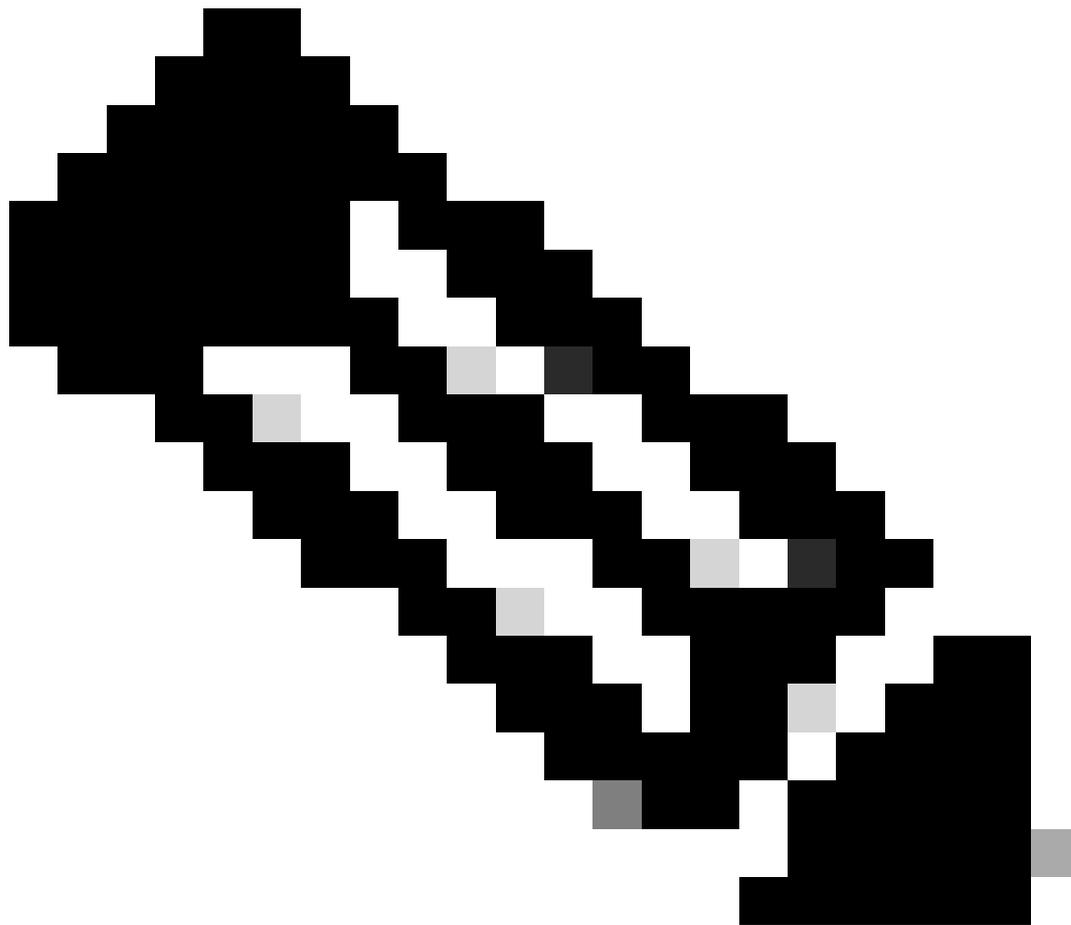
Or

[Other login options](#)

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

Connexion FMT

5. Sélectionnez le pare-feu source à migrer.



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.

Extract Cisco ASA (8.4+) Information

Source: Cisco ASA (8.4+)

Extraction Methods >

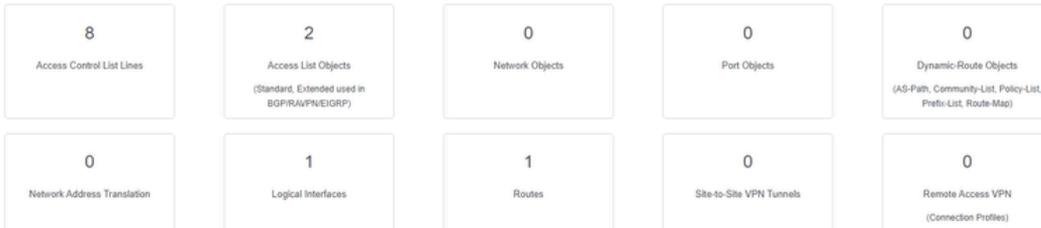
ASA IP Address: 192.168.1.20

Context Selection >

Single Context Mode: Download config

Parsed Summary v

Collect Hitcounts: No



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

https://cisco.com

Back

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.

Select Target

Source: Cisco ASA (8.4+)

Firewall Management v

 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

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**

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

Objectif FTD

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

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"> <small>Route-lookup logic is limited to Static Routes and Connected Routes. PBR, Dynamic-Routes & NAT are not considered.</small> <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><small>Remote Access VPN migration is supported on FMC/FTD 7.2 and above.</small></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

Configurations

11. Commencez la conversion des configurations de ASA en 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

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.

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 BGP/RAVP/VEIGRP)	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

Télécharger le rapport

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

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 de pré-migration

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

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

Mapper les interfaces

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

Map Security Zones and Interface Groups

Add SZ & IG Auto-Create

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

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 :



Map Security Zones and Interface Groups

Add SZ & IG Auto-Create

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

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 sur Valider.



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

Vérifier et valider

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

Validation Status

Successfully Validated

Validation Summary (Pre-push)

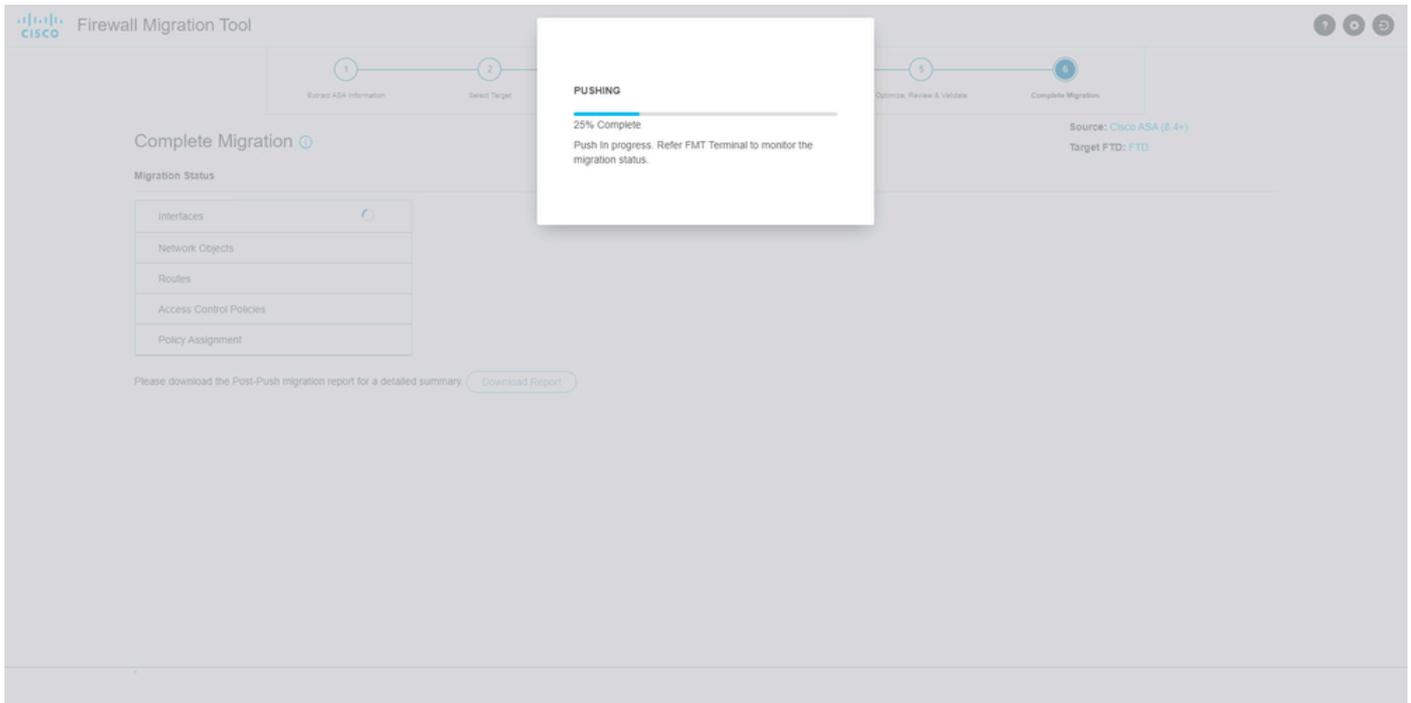
0 Access Control List Lines	Not selected for migration Access List Objects <small>(Standard, Extended used in BGP/RAVPN/EIGRP)</small>	1 Network Objects	Not selected for migration Port Objects	Not selected for migration Dynamic-Route Objects <small>(AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)</small>
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 <small>(Connection Profiles)</small>

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

Push Configuration

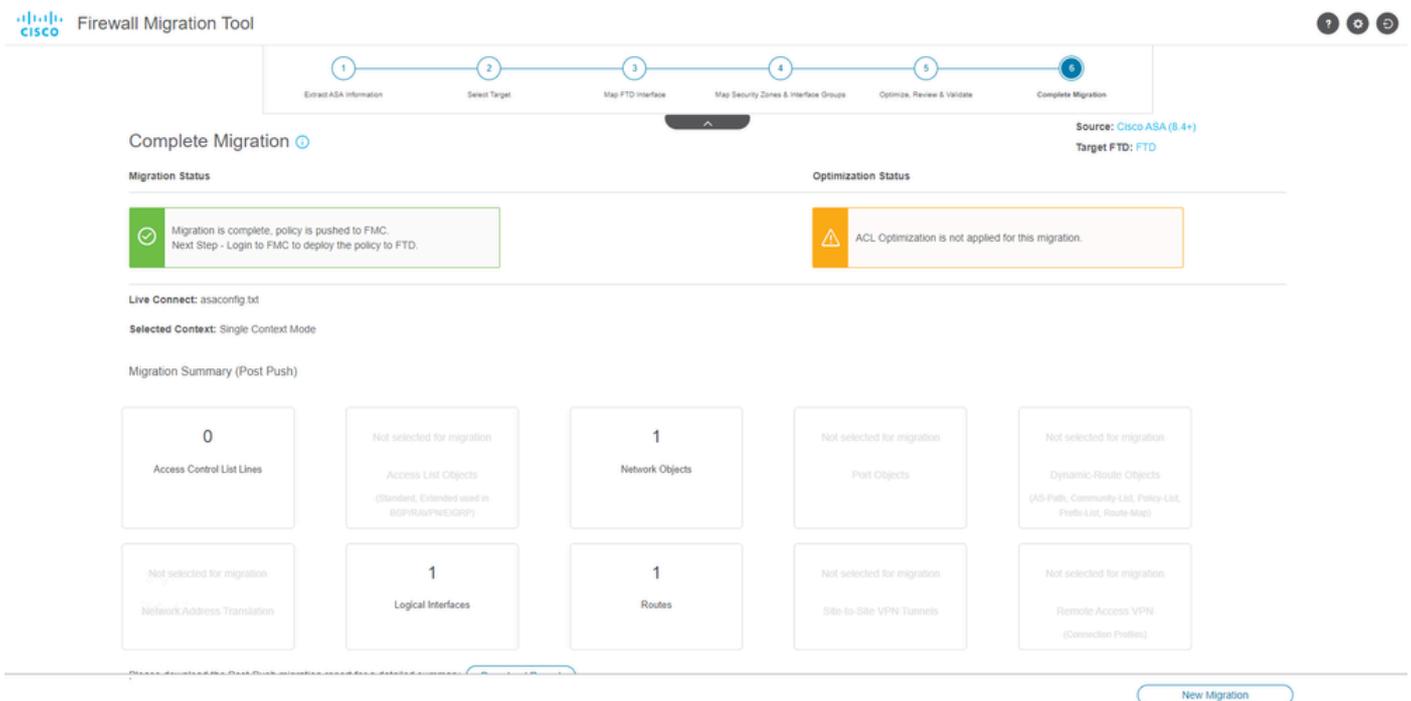
Validation

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'onglet 'Deploy'.

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.