

Migration de Paloalto vers Firepower Threat Defense à l'aide de FMT

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Aperçu](#)

[Informations générales](#)

[Obtenir le fichier zip de configuration du pare-feu Paloalto](#)

[Liste de contrôle préalable à la migration](#)

[Configurer](#)

[Étapes de migration](#)

[Dépannage](#)

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

[Échecs de migration courants :](#)

[Utilisation du bundle d'assistance pour le dépannage :](#)

Introduction

Ce document décrit la procédure de migration du pare-feu Palo vers Cisco Firepower Threat Device .

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Outil de migration Firepower
- Pare-feu Paloalto
- Protection pare-feu contre les menaces (FTD)
- Cisco Secure Firewall Management Center (FMC)

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) v7.7
- PAN NGFW version 8.0+
- Centre de gestion du pare-feu sécurisé (FMCv) v7.6

- Protection pare-feu sécurisée version 7.4.2

Avertissement : Les réseaux et les adresses IP référencés dans ce document ne sont associés à aucun utilisateur, groupe ou organisation individuel. Cette configuration a été créée exclusivement pour une utilisation dans un environnement de travaux pratiques.

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 :

- PAN NGFW 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-r81)
- Fortinet (5.0+)
- Palo Alto Networks (8.0+)

Informations générales

Avant de migrer la configuration de votre pare-feu Palo vers , exécutez les activités suivantes :

Obtenir le fichier zip de configuration du pare-feu Paloalto

- Paloalto Firewall doit être version 8.4+.
- Exportez la configuration en cours du pare-feu Palo Alto (*.xml doit être au format xml).
- Connectez-vous à l'interface de ligne de commande du pare-feu Paloalto pour exécuter la commande show routing route et enregistrer le résultat au format texte (*.txt).
- Compressez le fichier de configuration en cours (*.xml) et le fichier de routage (*.txt) avec l'extension *.zip.

Liste de contrôle préalable à la migration

- Assurez-vous que le FTD a été enregistré auprès du FMC avant de commencer le processus de migration.
- Un nouveau compte d'utilisateur avec des privilèges d'administration a été créé sur le FMC.

Vous pouvez également utiliser des informations d'identification d'administrateur existantes.

- Le fichier de configuration en cours Palo Alto exporté doit être compressé avec l'extension .zip (suivez la procédure mentionnée dans la section précédente).
- Le périphérique Firepower doit avoir au moins le même nombre de canaux physiques, de sous-interfaces ou de ports que les interfaces Palo Firewall.

Configurer

Étapes de migration

1. Téléchargez l'outil de migration Firepower le plus récent à partir de Cisco Software Central et compatible avec votre ordinateur :

The screenshot shows the Cisco Software Central interface for downloading the Secure Firewall Migration Tool (FMT) version 7.7.0. The page title is "Software Download" and the breadcrumb trail is "Downloads Home / Security / Firewalls / Secure Firewall Migration Tool / Firewall Migration Tool (FMT)- 7.7.0".

On the left, there is a search bar and a filter menu for "Latest Release" with a dropdown arrow. The "7.7.0" version is selected, and there are "Expand All" and "Collapse All" buttons. Below the filter, it shows "All Release" with a dropdown arrow and the number "7".

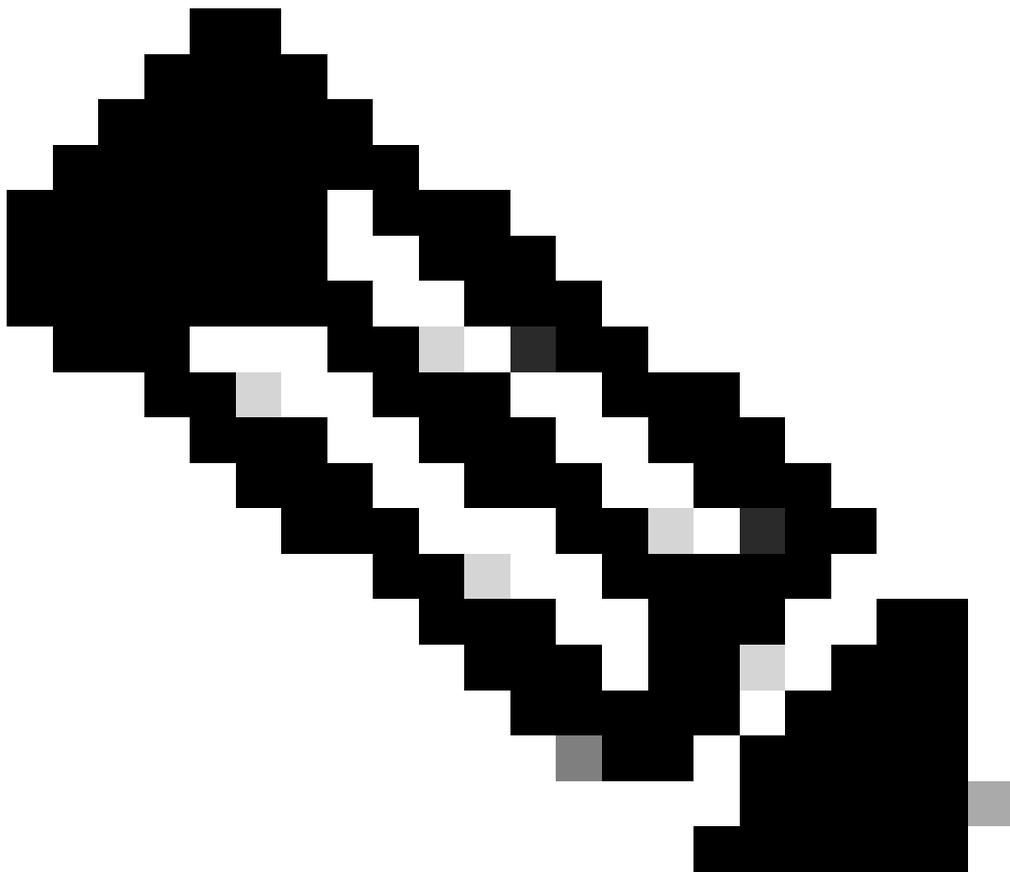
The main content area is titled "Secure Firewall Migration Tool" and shows "Release 7.7.0". There is a "My Notifications" button and a "Related Links and Documentation" section with links for "Open Source", "Release Notes for 7.7.0", and "Install and Upgrade Guides".

A table lists the available files for download:

| File Information | Release Date | Size | |
|---|--------------|----------|-------------------------------------|
| Firewall Migration Tool 7.7 for Mac Firewall_Migration_Tool_v7.7-12208.command Advisories | 03-Feb-2025 | 78.72 MB | ↓ 🛒 |
| Firewall Migration Tool 7.7 for Windows Firewall_Migration_Tool_v7.7-12208.exe Advisories | 03-Feb-2025 | 69.54 MB | ↓ 🛒 |

Téléchargement FMT

3. Ouvrez le fichier que vous avez téléchargé sur votre ordinateur.



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

-
4. Une fois que vous avez exécuté le programme, il ouvre un navigateur Web qui affiche le contrat de licence utilisateur final.
 1. Cochez la case pour accepter les conditions générales.
 2. Cliquez sur Continuer.
 5. Connectez-vous à l'aide d'informations d'identification CCO valides pour accéder à l'interface utilisateur FMT.

Security Cloud Sign On

Email

Continue

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

Or

[Other login options](#)

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

Invite de connexion FMT

6. Sélectionnez le pare-feu source à migrer et cliquez sur Start Migration.

Firewall Migration Tool (Version 7.7)

Select Source Configuration

Source Firewall Vendor
Palo Alto Networks (8.0+)

Start Migration Demo Mode

Palo Alto Networks (8.0+) Pre-Migration Instructions

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

Session Telemetry:
Cisco collects the firewall telemetry set forth below in connection with this migration. By completing the migration, you consent to Cisco's collection and use of this telemetry data for purposes of tracking and following up on firewall device migrations and performing related migration analytics.

Acronyms used:
FMT: Firewall Migration Tool FMC: Firewall Management Center
FTD: Firewall Threat Defense

Before you begin your Palo Alto Networks (PAN) to Firewall 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.
- Palo Alto Networks Configuration Requirements:** Export named configuration snapshot file from palo alto firewall to .xml format. If your NAT has polices with the same source and destination zone, then

GUI FMT

7. La section Méthodes d'extraction s'affiche maintenant, dans laquelle vous devez télécharger le fichier de configuration Zip de Paloalto Firewall vers le FMT.

Firewall Migration Tool (Version 7.7)

Extract Config Information

Extraction Methods

Manual Configuration Upload
The configuration file must be a zip file consisting of the following:

- Zip Config file derived from the PAN Tool.

Upload

Context Selection >

Parsed Summary >

Extract Config Information

Manual Configuration Upload

The configuration file must be a zip file consisting of the following:

- Zip Config

Downloads

config.zip

Assistant Téléchargement de configuration

8. Le résumé de la configuration analysée s'affiche à présent après le téléchargement du fichier de configuration. Dans le cas de VSYS, des sélections VSYS distinctes sont

disponibles. Chacun d'entre eux doit être analysé et migré l'un après l'autre. Validez le résumé analysé et cliquez sur l'icône Next.

Firewall Migration Tool (Version 7.7) Source: Palo Alto Networks (8.0+)

Extract Config Information

Extraction Methods

Context Selection

Parsed Summary

| | | | | |
|---------------------------|-----------------|--|---|--------------------|
| 184 | 908 | 150 | 49 | 9 |
| Access Control List Lines | Network Objects | Port Objects | Network Address Translation | Logical Interfaces |
| 15 | 73 | 4 | 13 | |
| Static Routes | Applications | Site-to-Site VPN Tunnels (Route Based) | Remote Access VPN (Global Protect Gateways) | |

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

Success
Context list Collected Successfully

Back Next

Récapitulatif de validation de configuration

9. Vous pouvez choisir le type de FMC dans cette section. Fournissez son adresse IP de gestion et cliquez sur Connect. Une fenêtre contextuelle s'affiche et vous invite à fournir les informations d'identification FMC. Entrez les informations d'identification et cliquez sur Login.

Firewall Migration Tool (Version 7.7) Source: Palo Alto Networks (8.0+)

Select Target

Firewall Management

On-Prem FMC (Hardware/Virtual) Cloud-delivered FMC Multicloud Defense

FMC IP Address/Hostname/FQDN
10.225.107.99

Connect

Choose FTD

Select Features

Rule Conversion/ Process Config

FMC Login

IP Address/Hostname/FQDN
10.225.107.99

Username
admin

Password

Login

Connexion FMC

10. Une fois la connexion à FMC établie, vous pouvez maintenant choisir le domaine (le cas échéant) et cliquer sur Continuer.

Select Target ⓘ Source: Palo Alto Networks (8.0+)

Firewall Management ⌵

On-Prem FMC (Hardware/Virtual)
 Cloud-delivered FMC
 Multicloud Defense

FMC IP Address/Hostname/FQDN: 10.225.107.99

Choose Domain: Global/Cisco ⌵

[Connect](#)

[Proceed](#)

✔ Successfully connected to FMC

Sélection du domaine

11. Choisissez le FTD vers lequel vous allez migrer et cliquez sur Continuer.

Select Target ⓘ Source: Palo Alto Networks (8.0+)

Firewall Management ➤

FMC IP Address/Hostname/FQDN: 10.225.107.99 Selected Domain: Global/Cisco

Choose FTD ⌵

Select FTD Device
 Proceed without FTD

FW1 (10.105.209.80) - NA (R) ⌵

[Proceed](#)

Select Features ➤

Rule Conversion/ Process Config ➤

Sélectionner le FTD cible

12. L'outil répertorie maintenant les fonctionnalités qui vont être migrées. Cliquez sur Continuer.

Select Target ⓘ Source: Palo Alto Networks (8.0+)

Firewall Management ➤

FMC IP Address/Hostname/FQDN: 10.225.107.99 Selected Domain: Global/Cisco

Choose FTD ➤

Selected FTD: FW1

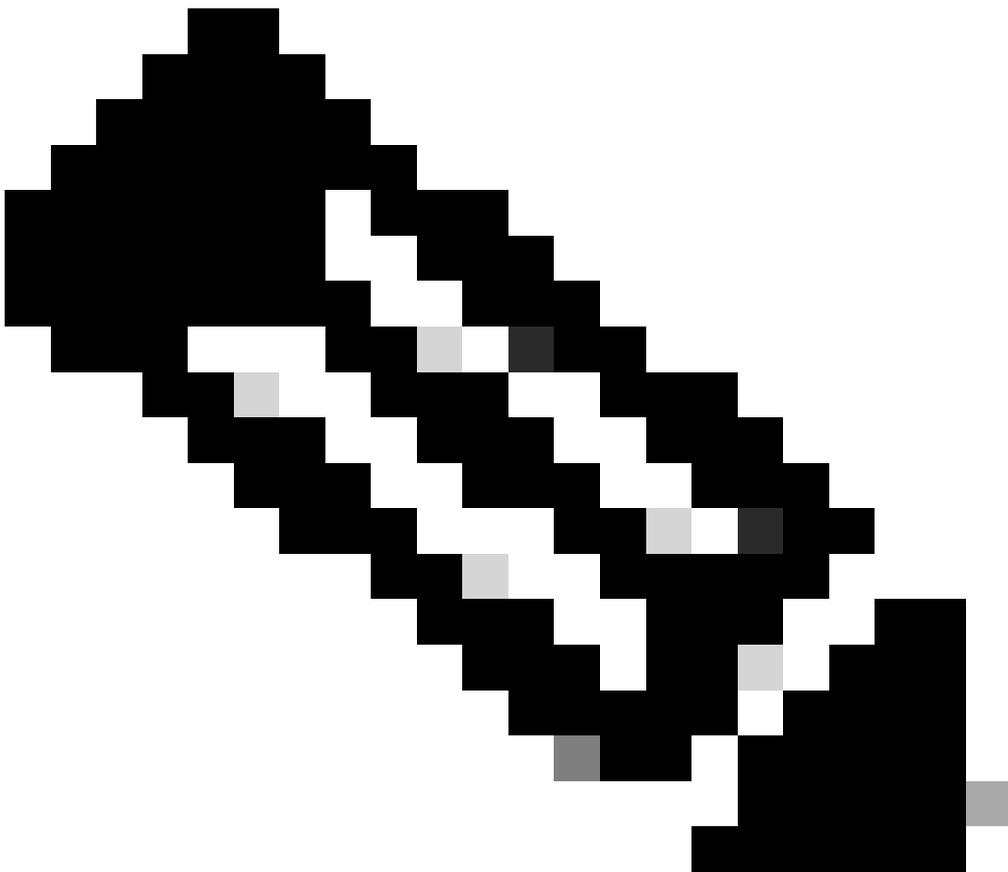
Select Features ⌵

| | | |
|---|--|--|
| <p>Device Configuration</p> <p><input checked="" type="checkbox"/> Interfaces</p> <p><input checked="" type="checkbox"/> Routes</p> <p><input checked="" type="checkbox"/> Site-to-Site VPN Tunnels</p> <p><input type="checkbox"/> Policy Based (Unsupported) ⓘ</p> <p><input checked="" type="checkbox"/> Route Based (VTI)</p> | <p>Shared Configuration</p> <p><input checked="" type="checkbox"/> Access Control</p> <p><input type="checkbox"/> Migrate policies with Application-default as Enabled ⓘ</p> <p><input checked="" type="checkbox"/> Network Objects</p> <p><input checked="" type="checkbox"/> Port Objects</p> <p><input checked="" type="checkbox"/> Remote Access VPN</p> | <p>Advanced Configuration</p> <p>Optimization</p> <p><input checked="" type="checkbox"/> Migrate Only Referenced Objects</p> <p>Access Control Options</p> <p><input checked="" type="checkbox"/> Discovered Identities ⌵ ⓘ</p> |
|---|--|--|

[Proceed](#)

Rule Conversion/ Process Config ➤

Sélection des fonctionnalités



Remarque : Toutes les fonctions sont sélectionnées par défaut. Vous pouvez désélectionner toute configuration qui ne doit pas être migrée.

13. Cliquez sur Start Conversion pour convertir la configuration.



Configuration d'analyse

L'outil analyse la configuration et affiche le résumé de conversion comme illustré dans l'image. Vous pouvez également télécharger le rapport de pré-migration pour valider la configuration migrée pour toute erreur ou avertissement, le cas échéant. Accédez à la page

suivante en cliquant sur Next.

| Category | Count |
|---|-------|
| Access Control List Lines | 195 |
| Network Objects | 752 |
| Port Objects | 98 |
| Network Address Translation | 52 |
| Logical Interfaces | 8 |
| Static Routes | 2 |
| Site-to-Site VPN Tunnels (Route Based) | 0 |
| Applications | 70 |
| Remote Access VPN (Global Protect Gateways) | 9 |

Résumé de la configuration analysée

14. Vous pouvez définir le mappage d'interface Paloalto-FTD ainsi que modifier le nom de chaque interface dans la section Interface Mapping. Cliquez sur Next une fois le mappage d'interface terminé.

| PAN Interface Name | FTD Interface Name | Mapped Name |
|--------------------|--------------------|-------------|
| ethernet1/2 | Select Interface | ethernet_2 |
| ethernet1/3 | ✓ Ethernet1/1 | ethernet_3 |
| ethernet1/4 | Ethernet1/10 | ethernet_4 |
| ethernet1/5 | Ethernet1/11 | ethernet_5 |
| ethernet1/6 | Ethernet1/12 | ethernet_6 |
| ethernet1/7 | Ethernet1/13 | ethernet_7 |
| | Ethernet1/14 | |
| | Ethernet1/15 | |
| | Ethernet1/16 | |
| | Ethernet1/17 | |
| | Ethernet1/18 | |
| | Ethernet1/19 | |

Mappage d'interface

15. Vous pouvez soit Ajouter la zone de sécurité manuellement pour chaque interface, soit la créer automatiquement dans la section Mapper la zone de sécurité . Cliquez sur Next après avoir créé et mappé les zones de sécurité.

Map Security Zones

| PAN Zone Name | FMC Security Zones |
|---------------|----------------------|
| G...-Inside | Select Security Zone |
| Outside | Select Security Zone |
| GP/PA- | Select Security Zone |
| I...Ine | Select Security Zone |
| DMZ | Select Security Zone |
| I...C | Select Security Zone |
| Mel | Select Security Zone |
| OT- | Select Security Zone |
| Wireless- | Select Security Zone |
| I...-Inside | Select Security Zone |

Add SZ Auto-Create Save

First option is to add Security Zone manually and second option is to auto create Security Zone

Note: Interfaces that are used in multiple configurations are allowed to have their unique security zones. The security zone mapping section for these interfaces will be grayed out.

10 per page 1 to 10 of 12 Page 1 of 2

Back Next

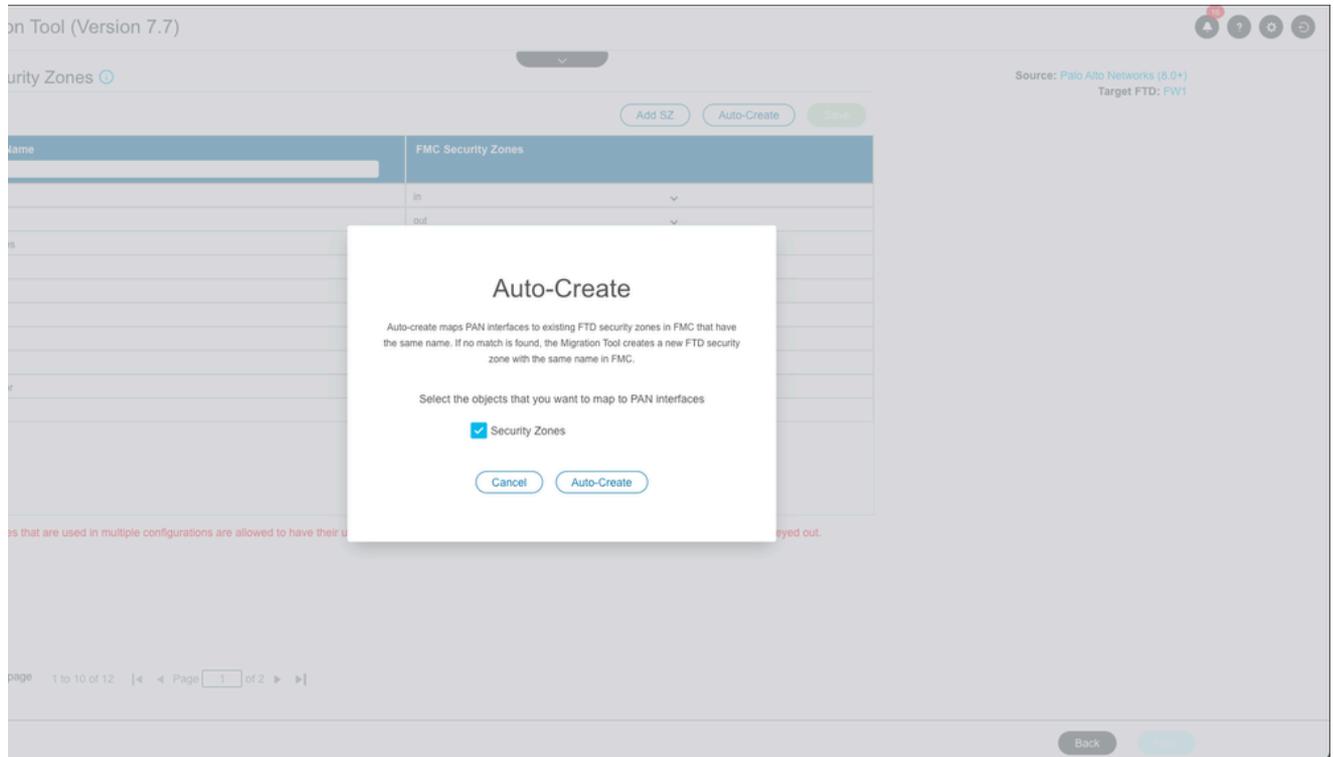
Création de zones de sécurité

Création manuelle de zones de sécurité :

The screenshot shows a modal window titled "Add SZ" with a close button (X) in the top right. Inside the modal, there is a "Security Zones (SZ)" section with an "Add" button and a text input field containing "DMZ". A tooltip above the field states "Max 48 characters for zone name. Allowed special characters are _.-*+". Below this is a table with columns "Security Zones", "Type", and "Actions". The "Security Zones" column contains "DMZ". The "Type" column has a dropdown menu with "Routed" selected. The "Actions" column contains a red 'X' and a green checkmark. At the bottom of the modal, there is a "Close" button and a pagination indicator "0 - 0 of 0 | Page 1 of 2".

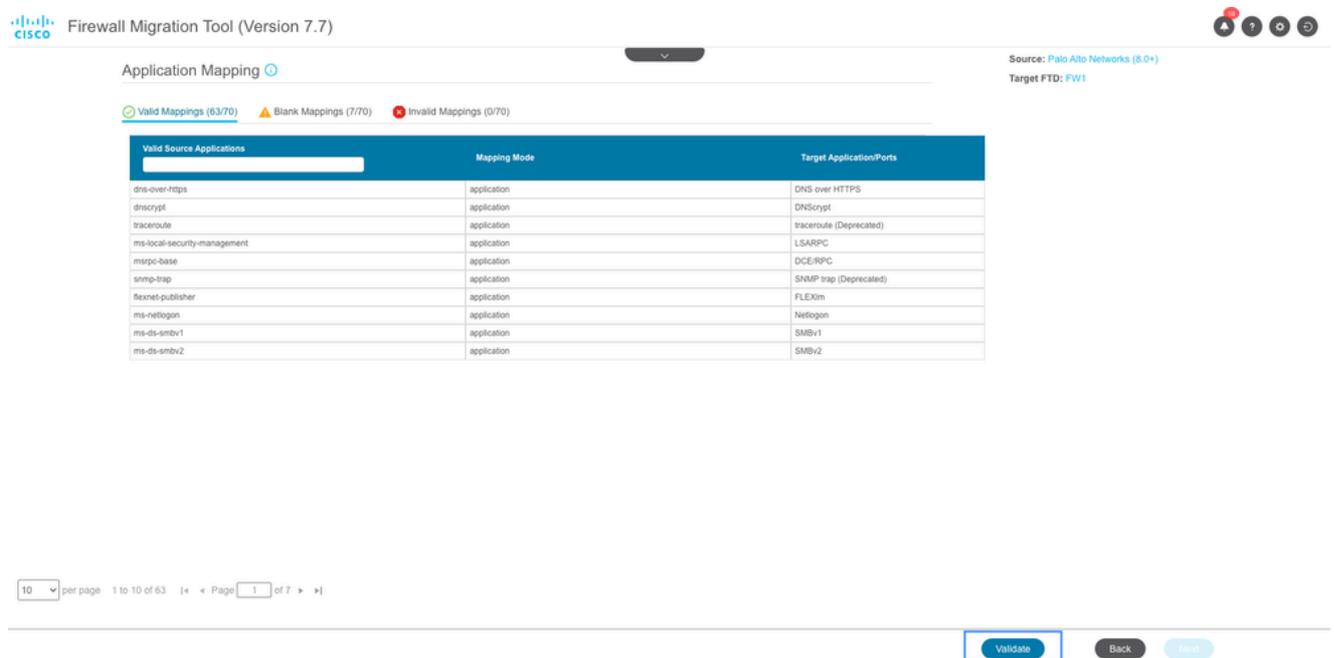
Création manuelle de zones de sécurité

Création automatique des zones de sécurité :



Création de zones de sécurité automatique

16. Vous pouvez maintenant passer à la section Application Mapping. Cliquez sur le bouton Valider pour valider le mappage d'application.



Mappage des applications

Application Mapping

Validation of application mapping is in progress. Please wait

Source: Palo Alto Networks (8.0+)
Target FTD: FW1

Valid Mappings (63/70) Blank Mappings (7/70) Invalid Mappings (0/70)

| Valid Source Applications | Mapping Mode | Target Application/Ports |
|-----------------------------|--------------|--------------------------|
| dns-over-https | application | DNS over HTTPS |
| dnscrypt | application | DNScrypt |
| traceroute | application | traceroute (Deprecated) |
| ms-local-securitymanagement | application | LSARPC |
| mrpc-base | application | DCE/RPC |
| snmp-trap | application | SNMP trap (Deprecated) |
| flexnet-publisher | application | FLEXim |
| ms-netlogon | application | Netlogon |
| ms-ds-smbv1 | application | SMBv1 |
| ms-ds-smbv2 | application | SMBv2 |

10 per page 1 to 10 of 63 Page 1 of 7

Validate Back Next

Validation du mappage des applications

Lors de la validation, FMT répertorie les mappages vides et non valides. Les mappages non valides doivent être corrigés avant de poursuivre et la correction des mappages vides est facultative.

Cliquez à nouveau sur Valider pour valider les mappages corrigés. Cliquez sur Next une fois la validation terminée.

Application Mapping

Clear Mapped Data

Source: Palo Alto Networks (8.0+)
Target FTD: FW1

Valid Mappings (61/70) Blank Mappings (7/70) Invalid Mappings (2/70)

| Invalid Source Applications | Mapping Mode | Target Application/Ports |
|-----------------------------|--------------|--------------------------|
| traceroute | Application | netmg-traceroute |
| snmp-trap | Port(s) | udp/162 |

10 per page 1 to 2 of 2 Page 1 of 1

Validate Back Next

Mappage d'application vide et non valide

- La liste de contrôle d'accès peut être optimisée dans la section suivante, si nécessaire. Examinez la configuration dans chaque section, telle que le contrôle d'accès, les objets, la NAT, les interfaces, les routes et le VPN d'accès à distance. Cliquez sur Valider après avoir examiné les configurations.

Optimize, Review and Validate Configuration

Source: Palo Alto Networks (8.0+)
Target FTD: FW1

Access Control Objects NAT Interfaces Routes Site-to-Site VPN Remote Access VPN

Select all 195 entries Selected: 0 / 195

| # | Name | SOURCE | | | | DESTINATION | | | | Application | URLs | State | Action | TIME BASED |
|----|--------------|--------|----------------|------|------|-------------|---------|---------|-----------------------|-------------|------|-------|--------|------------|
| | | Zone | Network | Port | User | Zone | Network | Port | Application | | | | | |
| 1 | Allow Tm... | Dc | GRP_ADDR... | ANY | ANY | | | ANY | NTP | NA | ✓ | Allow | None | |
| 2 | Allow Tm... | Df | ANY | ANY | ANY | | | 3M... | NTP | NA | ✓ | Allow | None | |
| 3 | Allow Tm... | Df | GRP_ADDR... | ANY | ANY | | | com | NTP | NA | ✓ | Allow | None | |
| 4 | Allow DNS | Df | ANY | ANY | ANY | | | 3R... | DNS, DNSCrypt, DN... | NA | ✓ | Allow | None | |
| 5 | Allow DNS | O | ANY | ANY | ANY | Inside | | 3R... | DNS | NA | ✓ | Allow | None | |
| 6 | Allow API | Dc | ANY | ANY | ANY | | | 3M... | TCP-80, TCP... | NA | ✓ | Allow | None | |
| 7 | Allow traffi | G. | ADDR_10.11... | ANY | ANY | | | 2.16... | TCP-443 | NA | ✓ | Allow | None | |
| 8 | Allow Acco | G. | ADDR_192.16... | ANY | ANY | DT... | | | ANY | NA | ✓ | Allow | None | |
| 9 | Allow ICM | O | ANY | ANY | ANY | Inside | | | netmg-traceroute | NA | ✓ | Allow | None | |
| 10 | Allow ICM | O | ANY | ANY | ANY | Inside | | | ICMPv4 | NA | ✓ | Allow | None | |
| 11 | Allow DHC | O | ANY | ANY | ANY | Inside | | .11... | DHCP | NA | ✓ | Allow | None | |
| 12 | Allow NetE | O | ANY | ANY | ANY | Inside | | .11... | NetBIOS-ns, NetBIO... | NA | ✓ | Allow | None | |
| 13 | Allow DNS | O | ANY | ANY | ANY | Inside | | .11... | DNS | NA | ✓ | Allow | None | |

50 per page 1 to 50 of 195 Page 1 of 4

Optimize access control list and validate

Optimize ACL Validate

Validation de configuration

18. Un récapitulatif de validation s'affiche une fois la validation terminée. Cliquez sur Push Configuration pour transmettre la configuration au FMC ciblé.

Validation Status

Successfully Validated

Validation Summary (Pre-push)

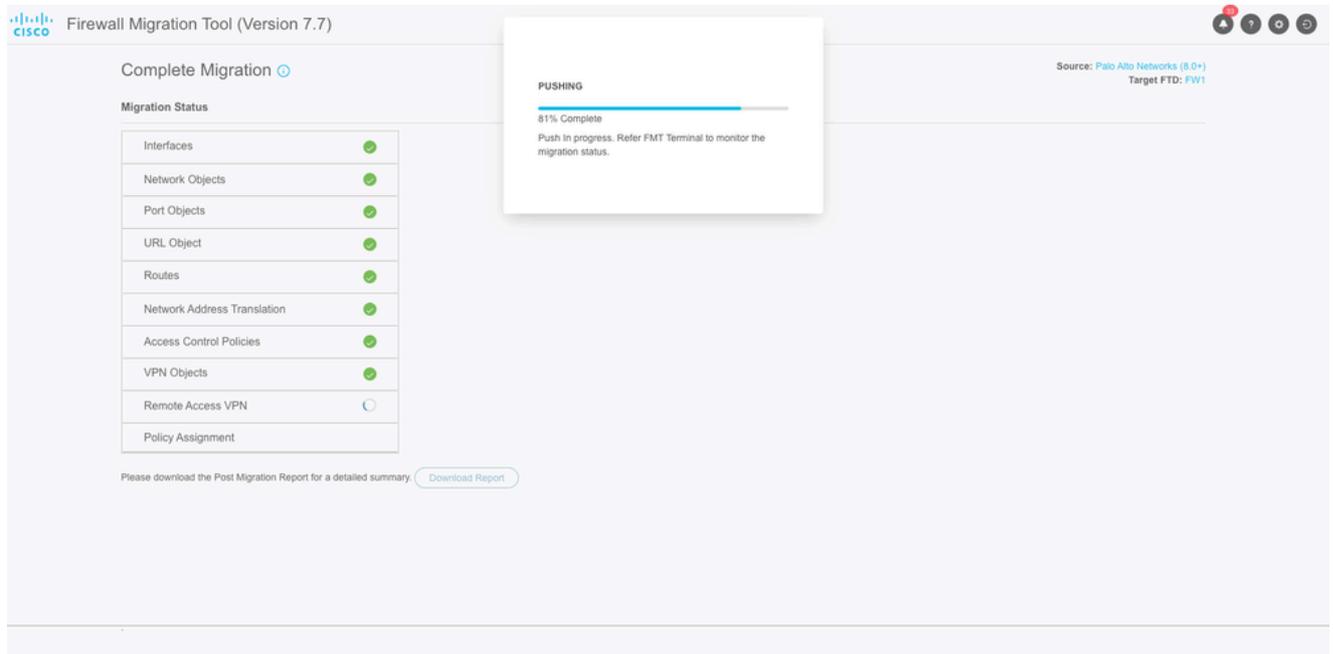
| | | | | |
|----------------------------------|---|---------------------|--|-------------------------|
| 195 Access Control List Lines | 752 Network Objects | 100 Port Objects | 52 Network Address Translation | 8 Logical Interfaces |
| 2 Static Routes | 0 Site-to-Site VPN Tunnels (Route Based) | 62 Applications | 9 Remote Access VPN (Global Protect Gateways) | |

Note: The configuration on the target FTD device FW1 (10.105.209.80) will be overwritten as part of this migration.

Push Configuration

Récapitulatif de validation de configuration

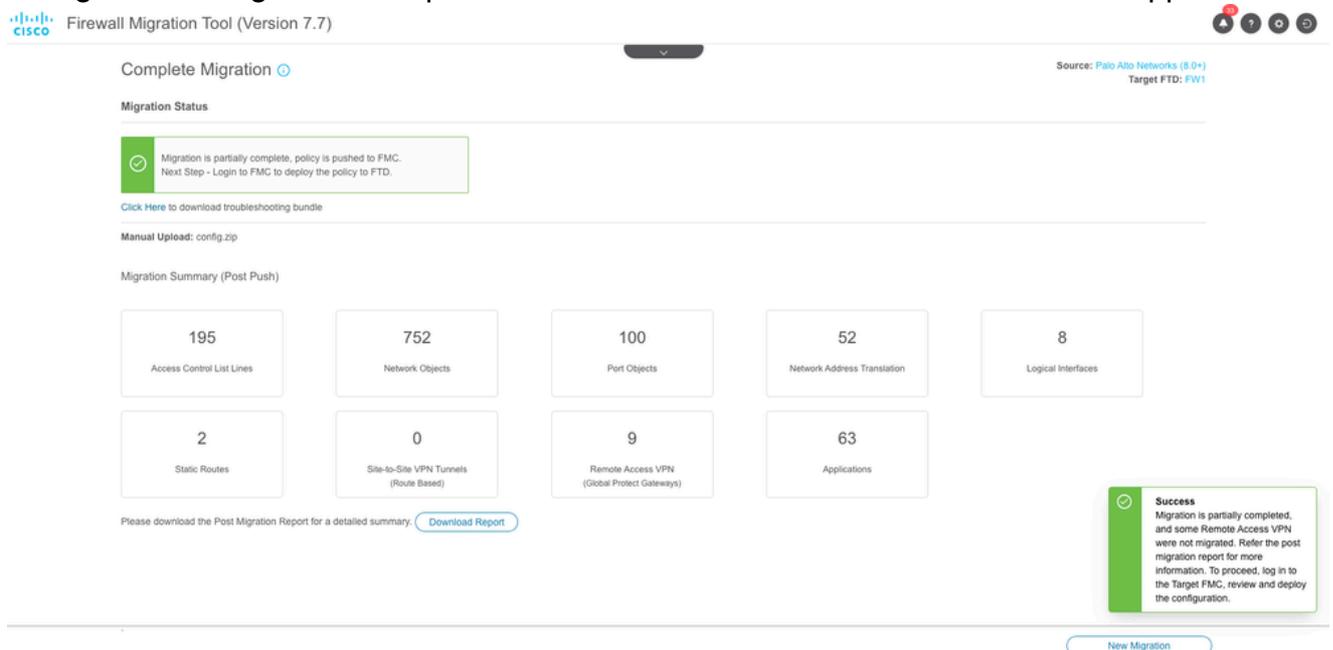
19. La progression de la transmission de la configuration à FMC est désormais visible dans la section État de la migration. Vous pouvez également utiliser la fenêtre de terminal FMT pour surveiller l'état de la migration.



État de migration

20. Un résumé de la migration s'affiche lorsque l'outil a réussi la migration. Il répertorie également les configurations partiellement migrées, le cas échéant. Par exemple, la configuration VPN d'accès à distance dans ce scénario en raison de l'absence de package client sécurisé.

Vous pouvez également télécharger le rapport post-migration pour examiner les configurations migrées ainsi que si des erreurs ou des corrections doivent être apportées.



Récapitulatif de migration réussie

21. La dernière étape consiste à examiner la configuration migrée de FMC et à déployer la configuration vers FTD.

Afin de déployer la configuration :

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

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

Dépannage

Dépannage de l'outil de migration Secure Firewall

Échecs de migration courants :

- Caractères inconnus ou non valides dans le fichier de configuration PaloAlto.
- Éléments de configuration manquants ou incomplets.
- Problèmes de connectivité réseau ou latence.
- Problèmes lors du chargement du fichier de configuration PaloAlto ou lors de la transmission de la configuration au FMC.

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.

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.