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

Table des matières

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

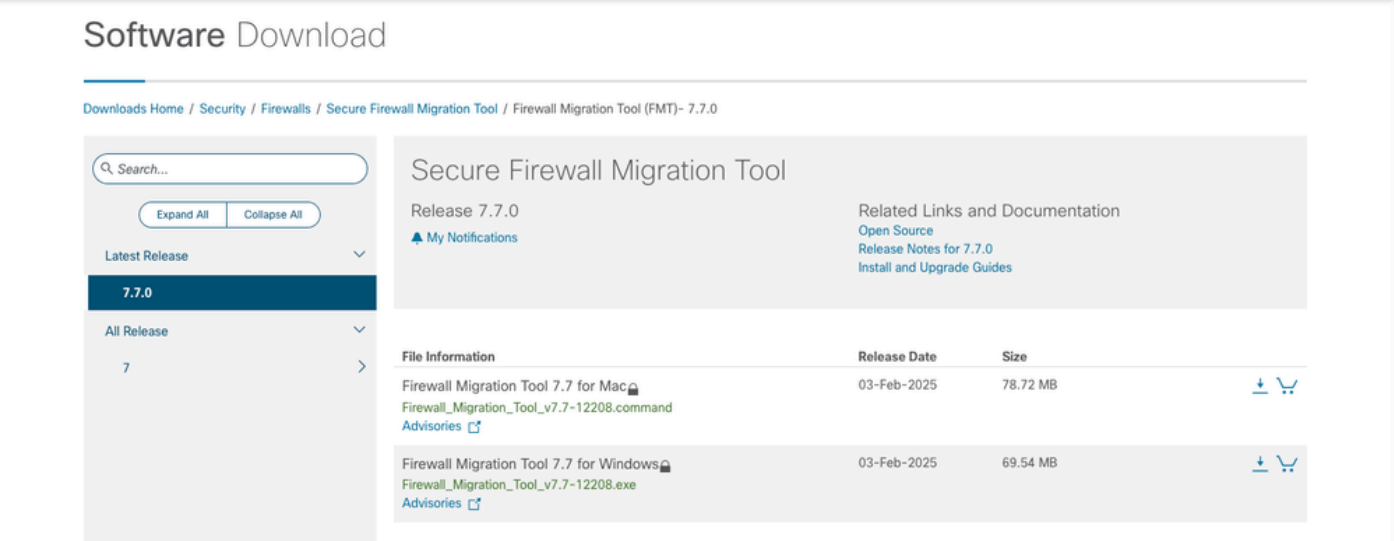
- Assurez-vous que le FTD a été enregistré auprès du FMC avant de commencer le processus de migration.
- Un nouveau compte d'utilisateur avec des privilèges d'administration a été créé sur le FMC.

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

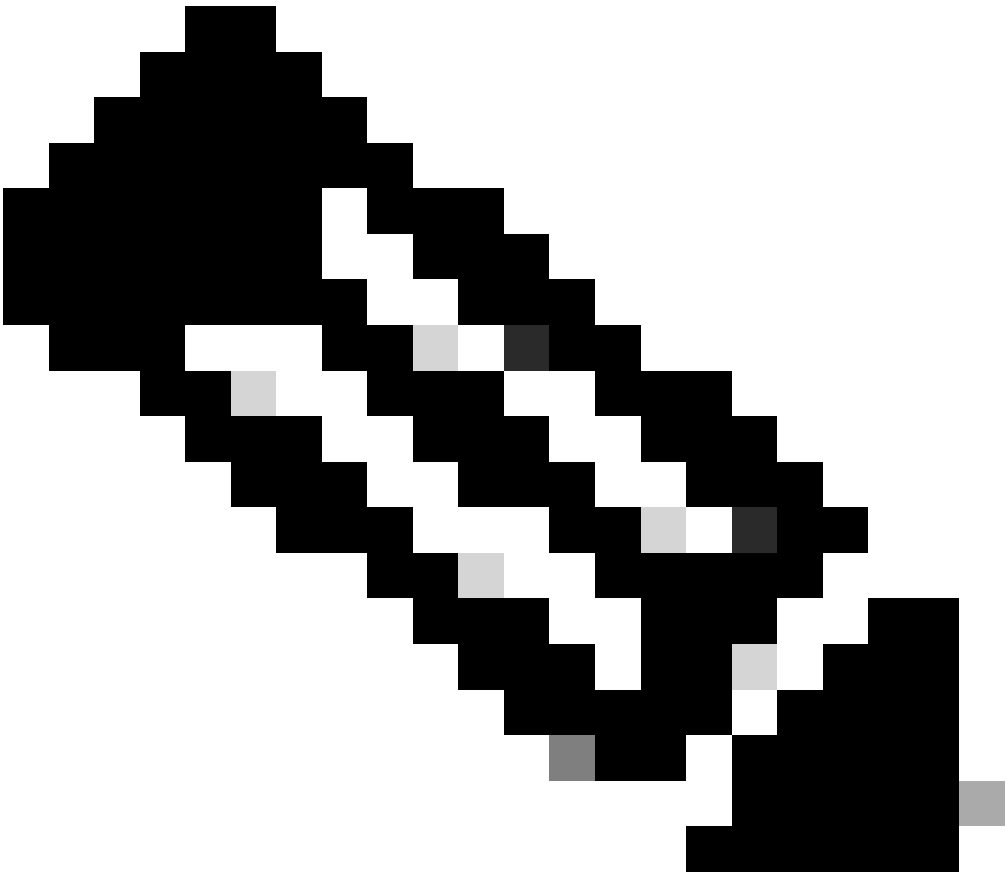
Étapes de migration

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



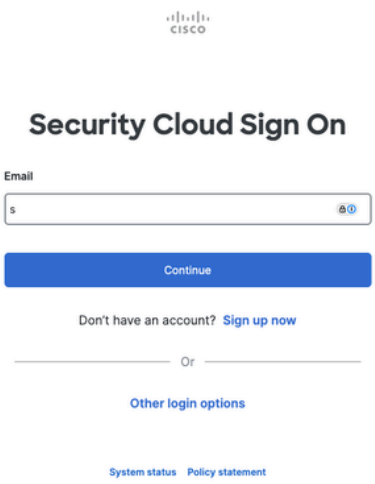
Téléchargement FMT

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



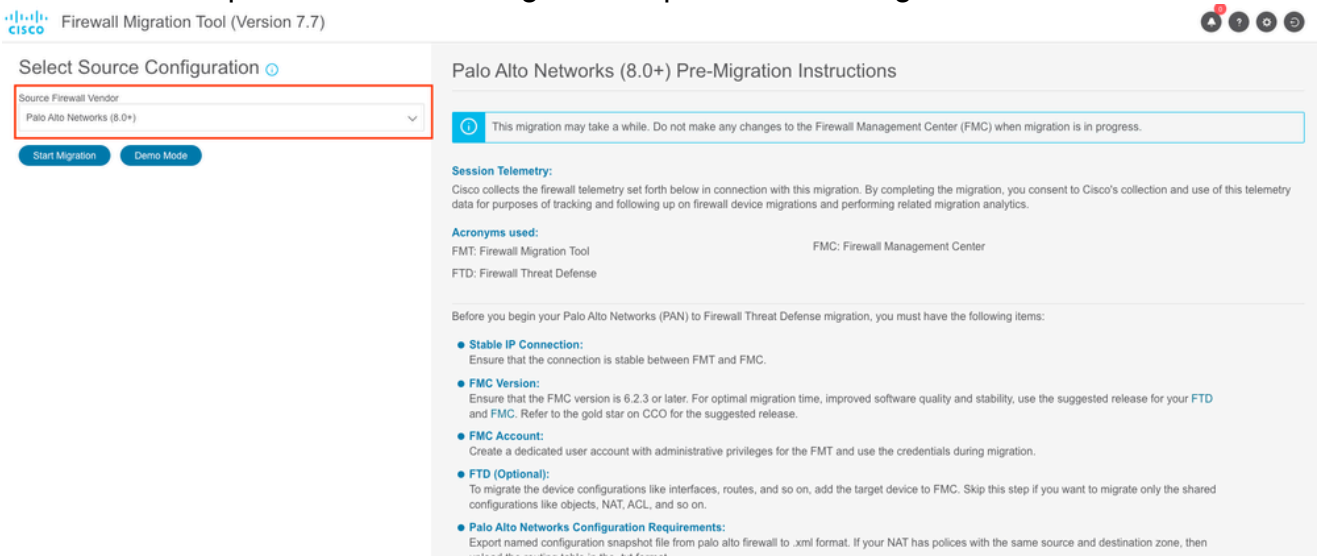
Remarque : Le programme s'ouvre automatiquement et une console génère automatiquement du contenu dans le répertoire dans lequel vous avez exécuté le fichier.

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.



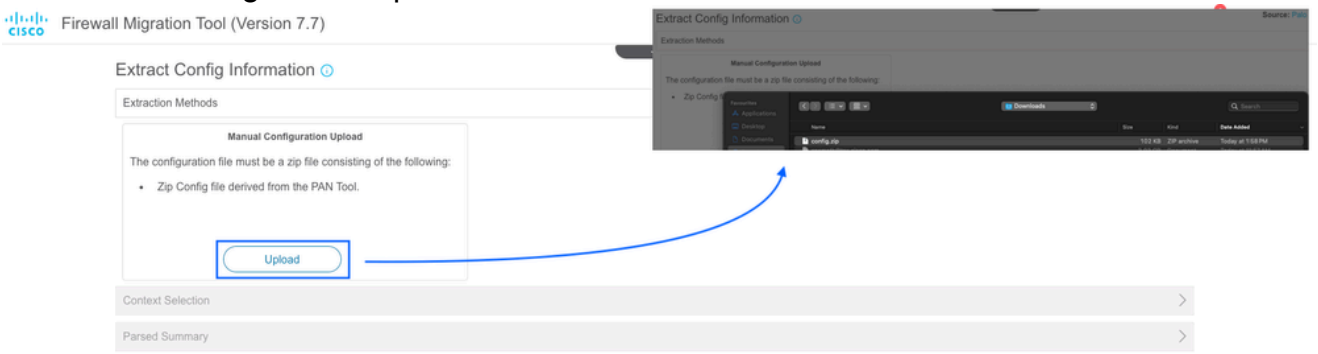
Invite de connexion FMT

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



GUI FMT

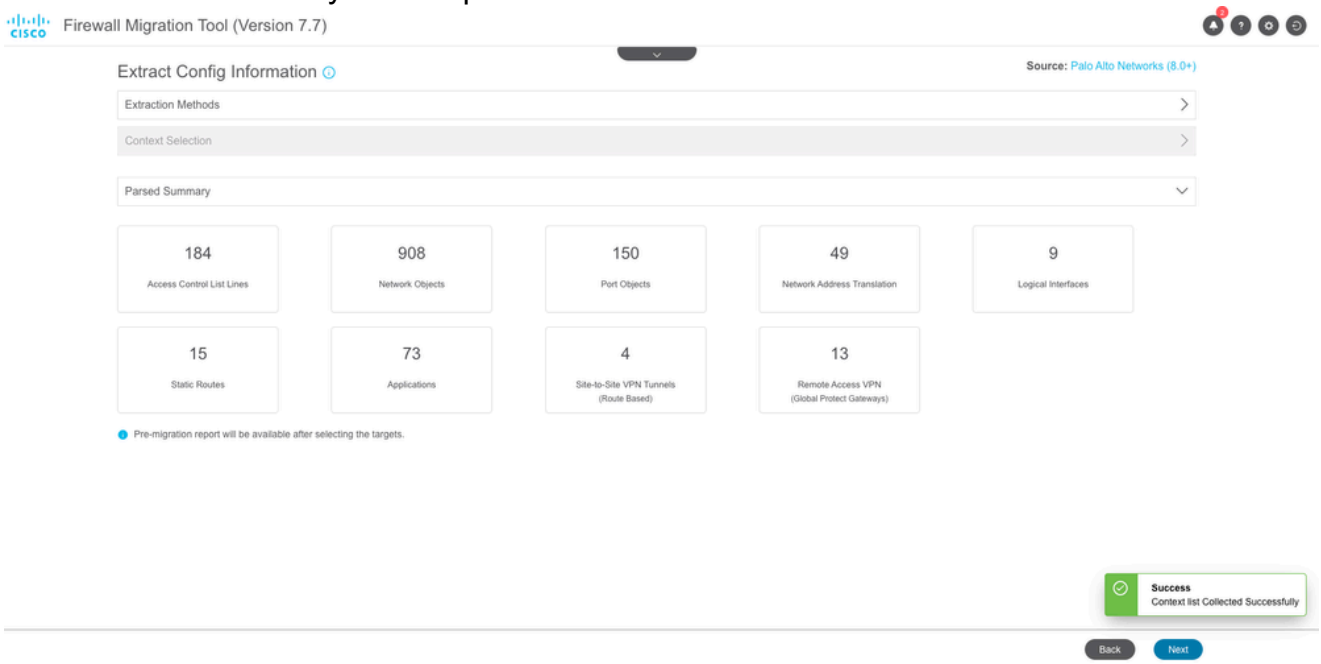
7. La section Méthodes d'extraction s'affiche maintenant, dans laquelle vous devez télécharger le fichier de configuration Zip de Paloalto Firewall vers le FMT.



Assistant Téléchargement de configuration

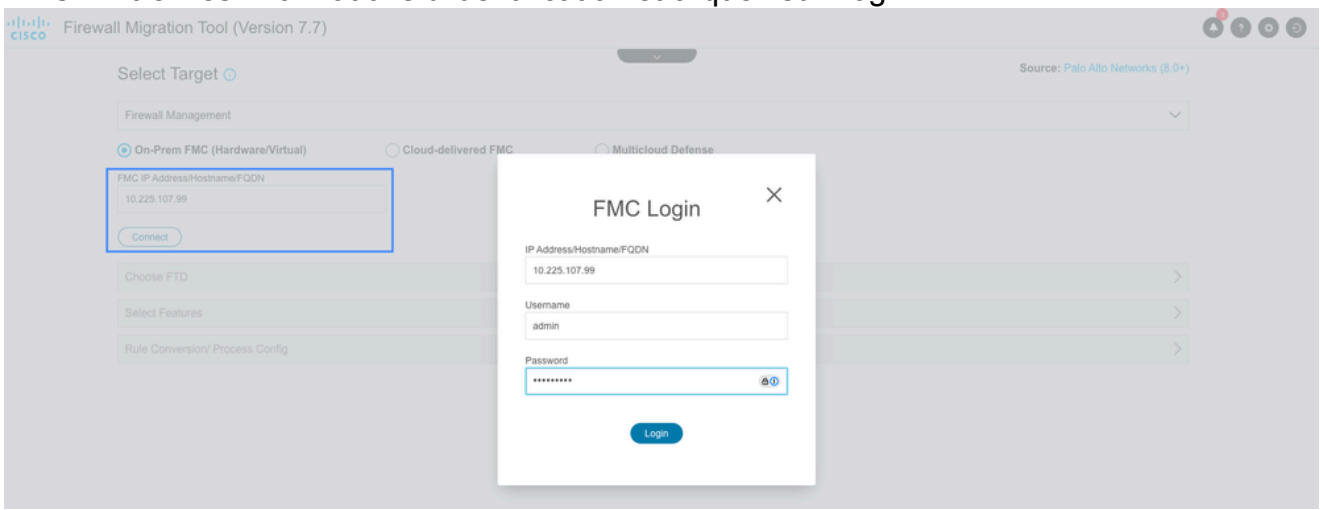
8. Le résumé de la configuration analysée s'affiche à présent après le téléchargement du fichier de configuration. Dans le cas de VSYS, des sélections VSYS distinctes sont

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.



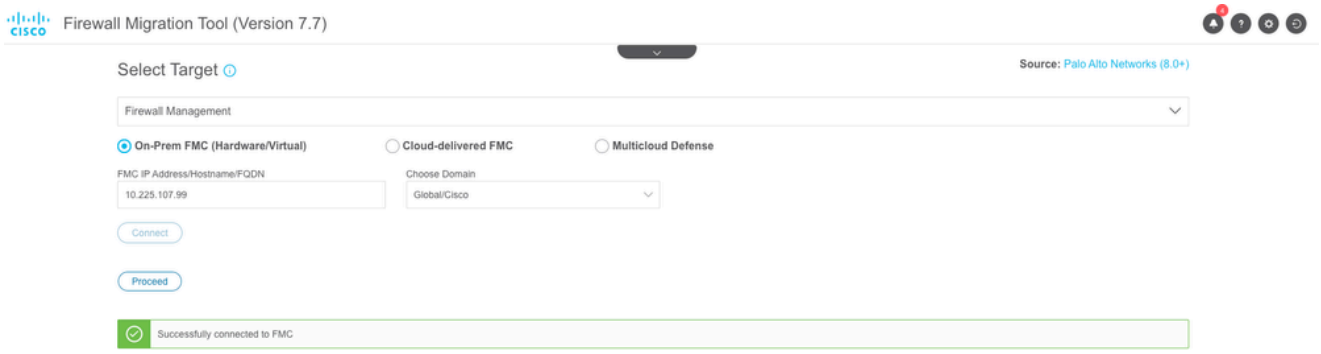
Récapitulatif de validation de configuration

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.



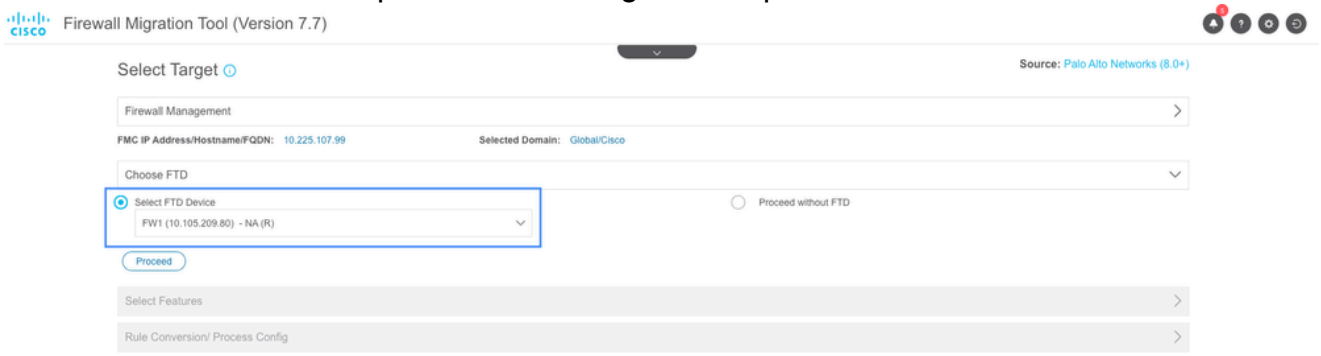
Connexion FMC

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



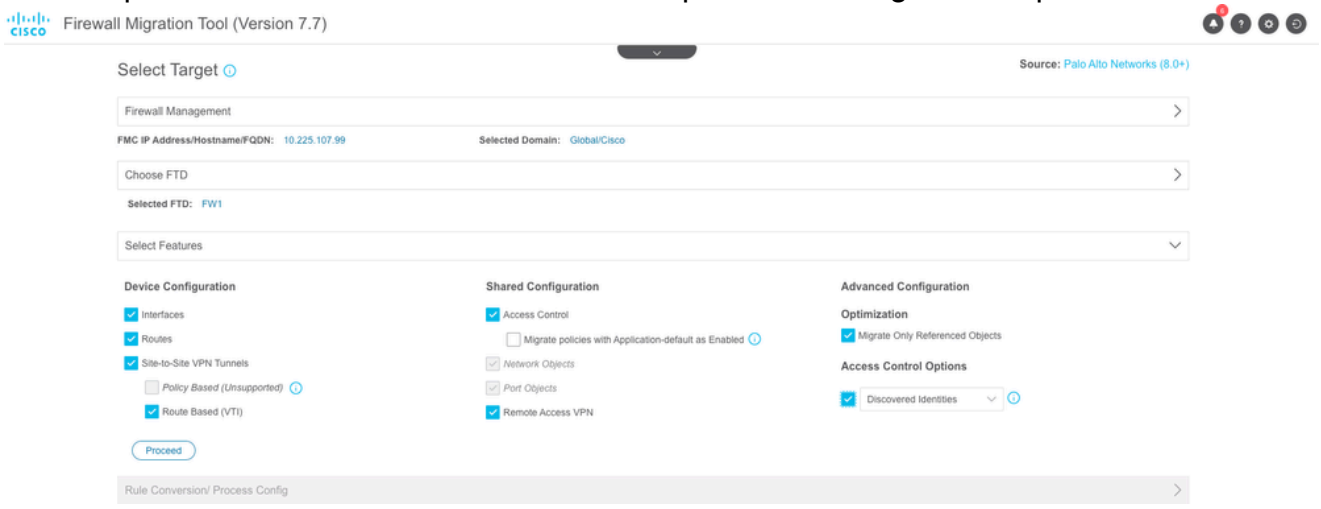
Sélection du domaine

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

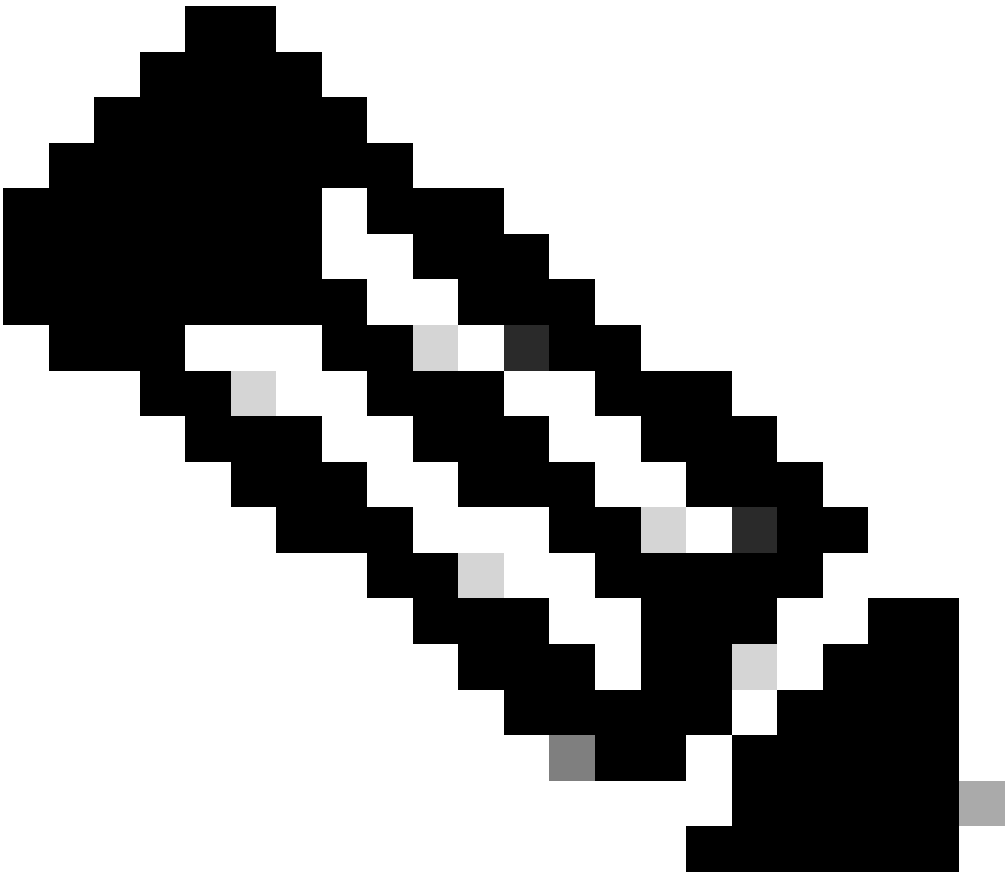


Sélectionner le FTD cible

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

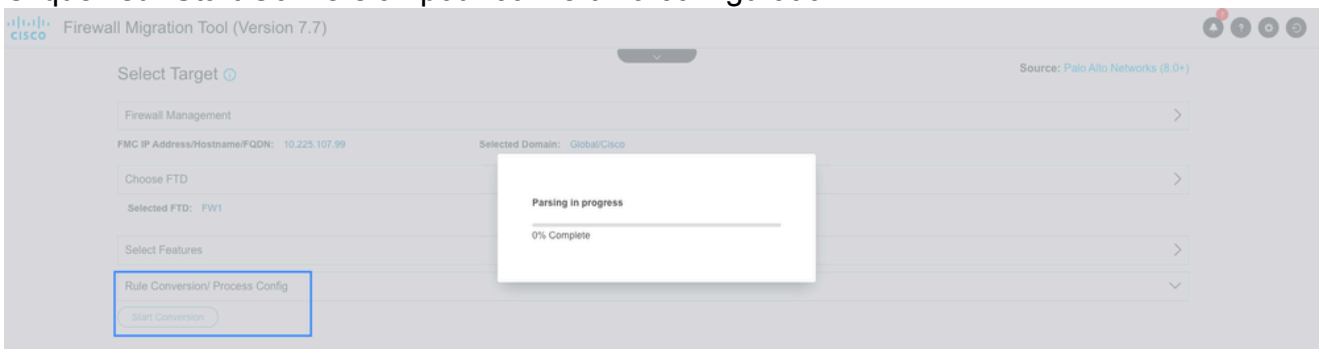


Sélection des fonctionnalités



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

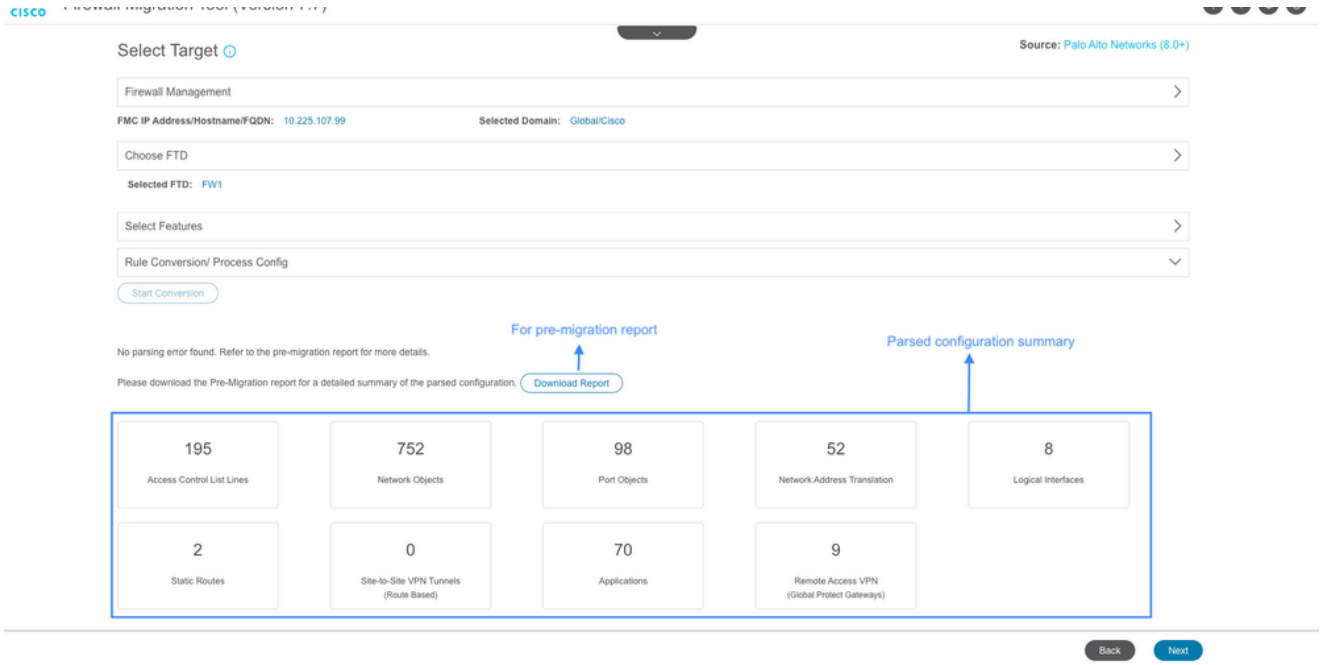
13. Cliquez sur Start Conversion pour convertir la configuration.



Configuration d'analyse

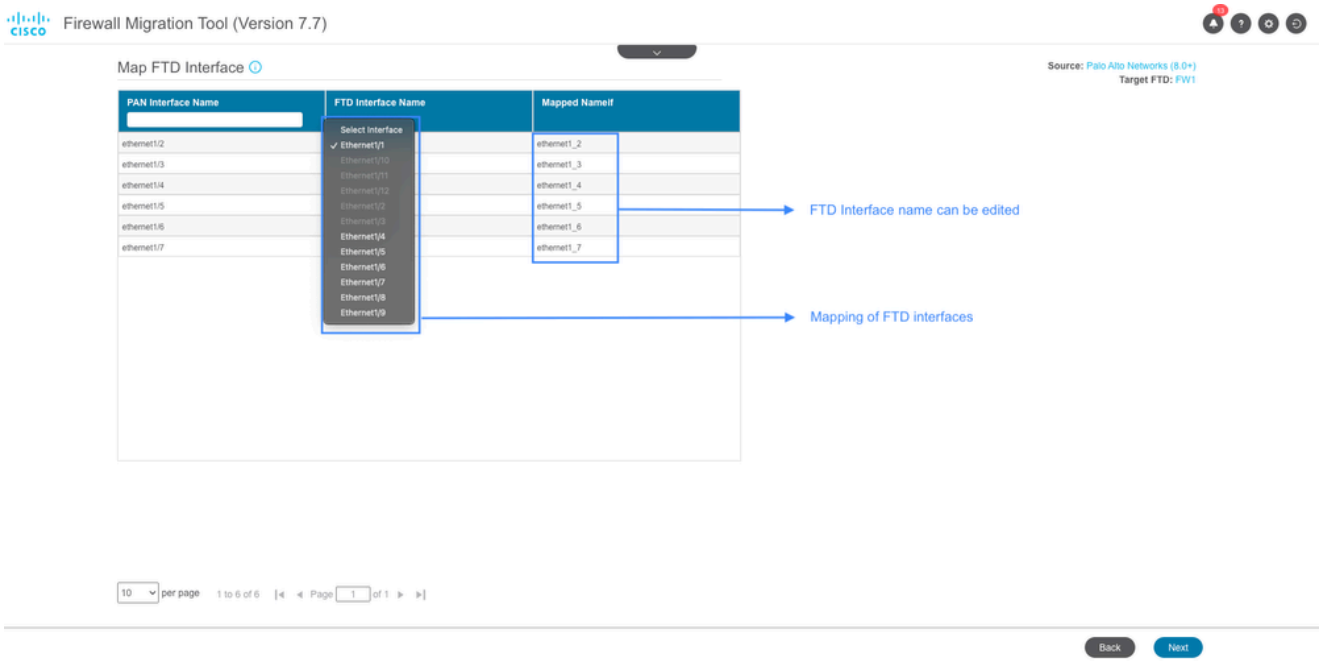
L'outil analyse la configuration et affiche le résumé de conversion comme illustré dans l'image. Vous pouvez également télécharger le rapport de pré-migration pour valider la configuration migrée pour toute erreur ou avertissement, le cas échéant. Accédez à la page

suivante en cliquant sur Next.



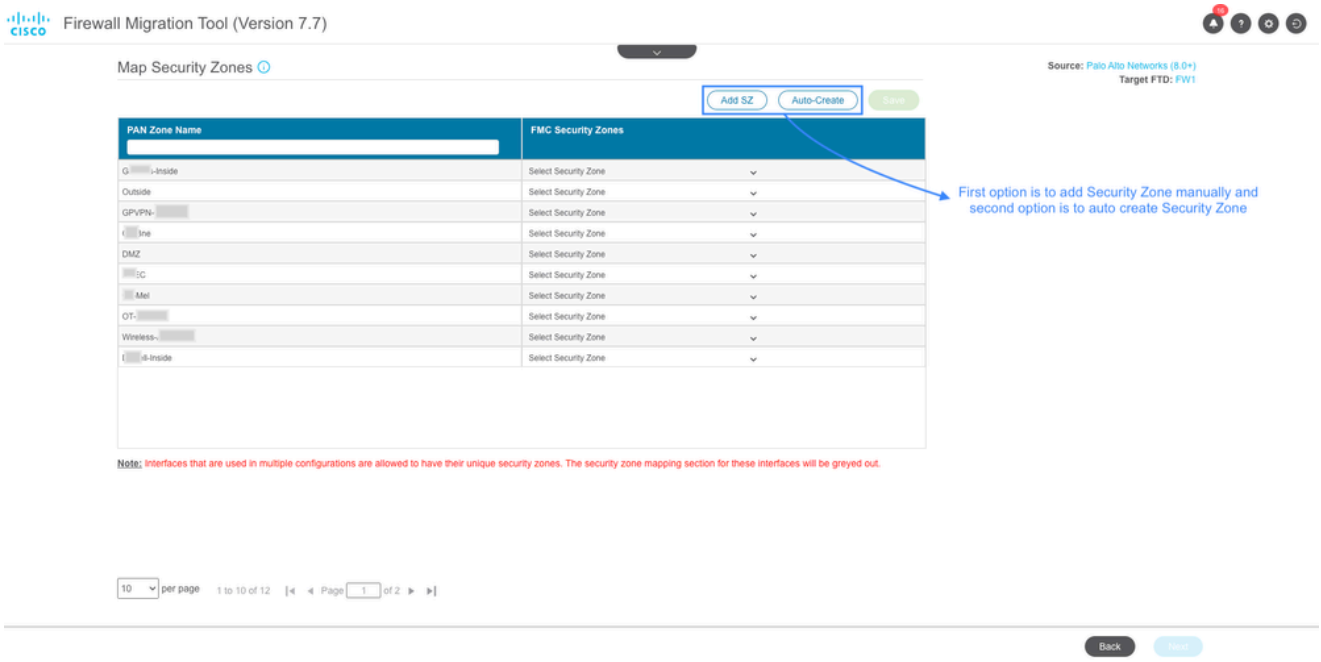
Résumé de la configuration analysée

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.



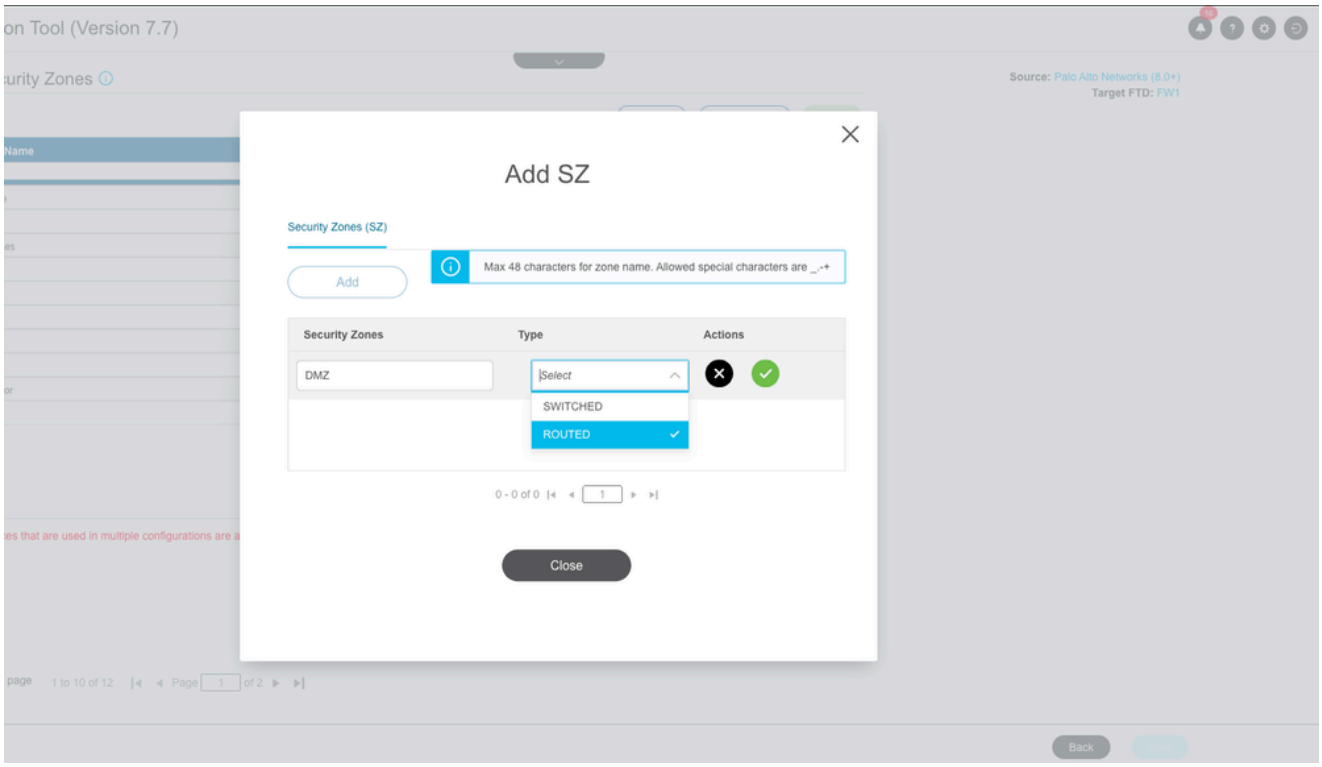
Mappage d'interface

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.



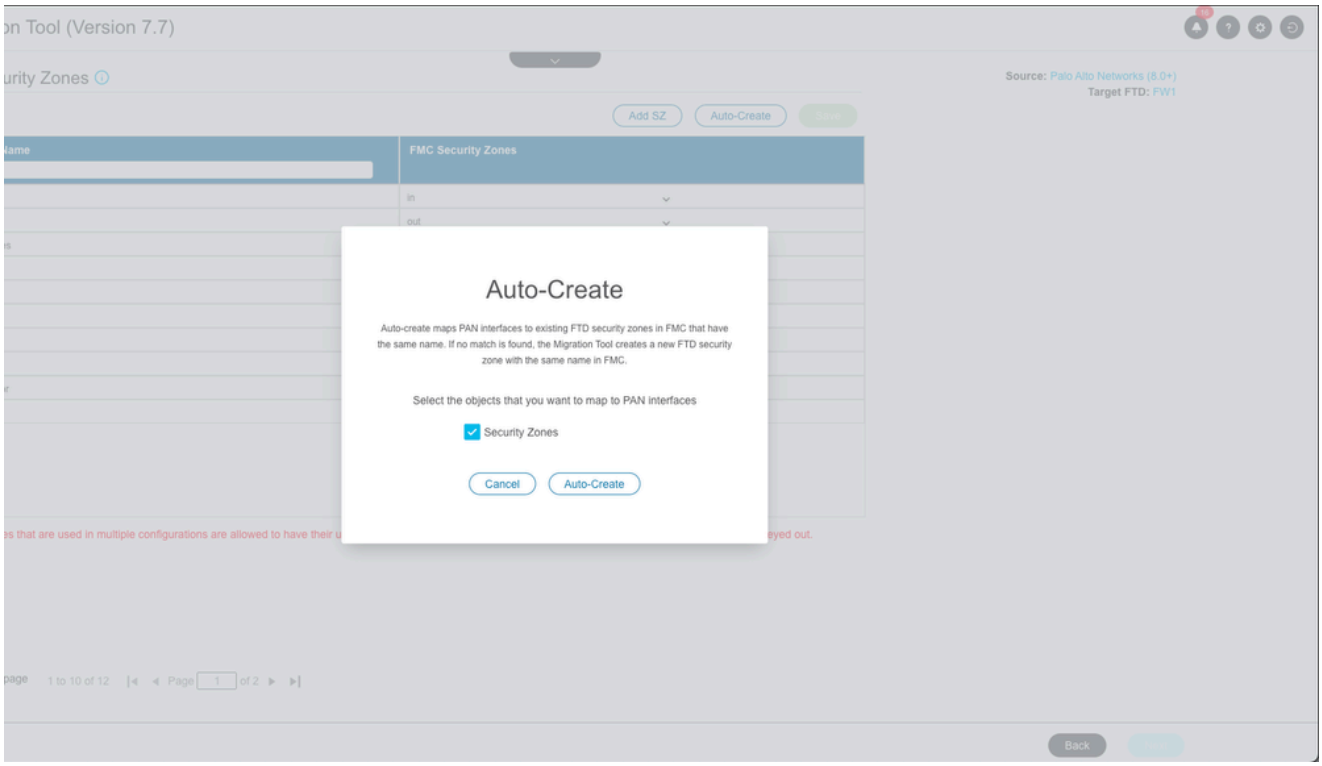
Création de zones de sécurité

Création manuelle de zones de sécurité :



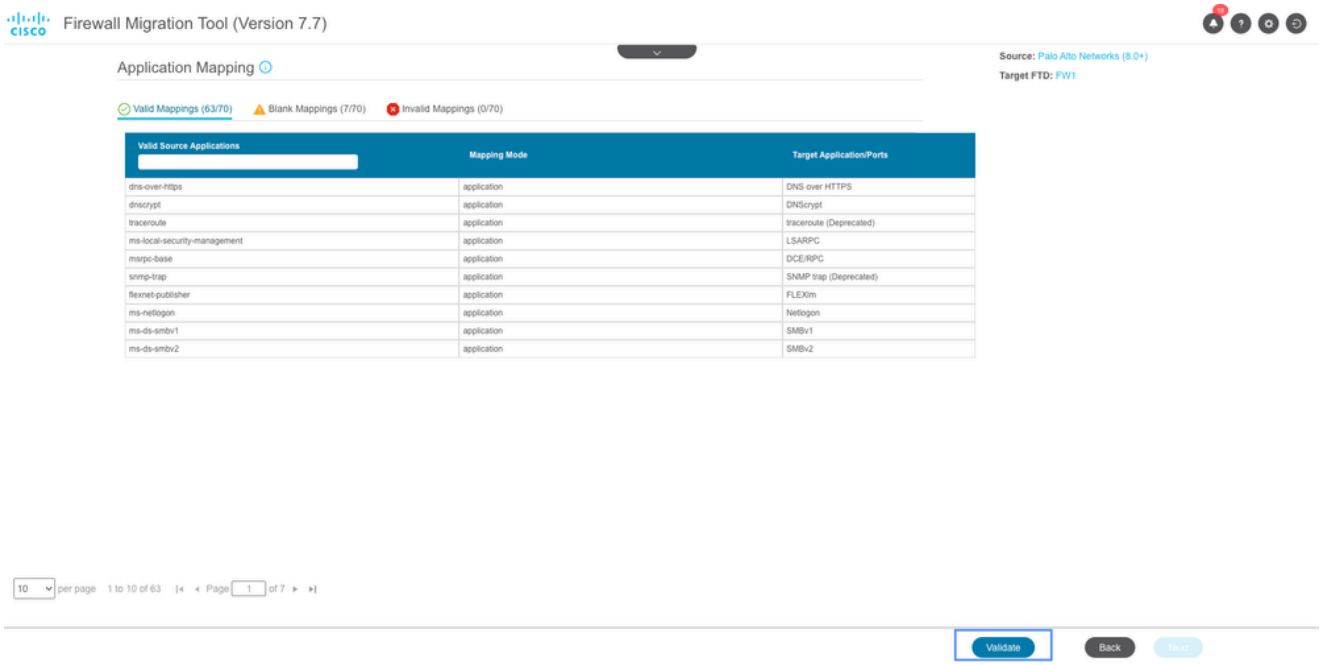
Création manuelle de zones de sécurité

Création automatique des zones de sécurité :

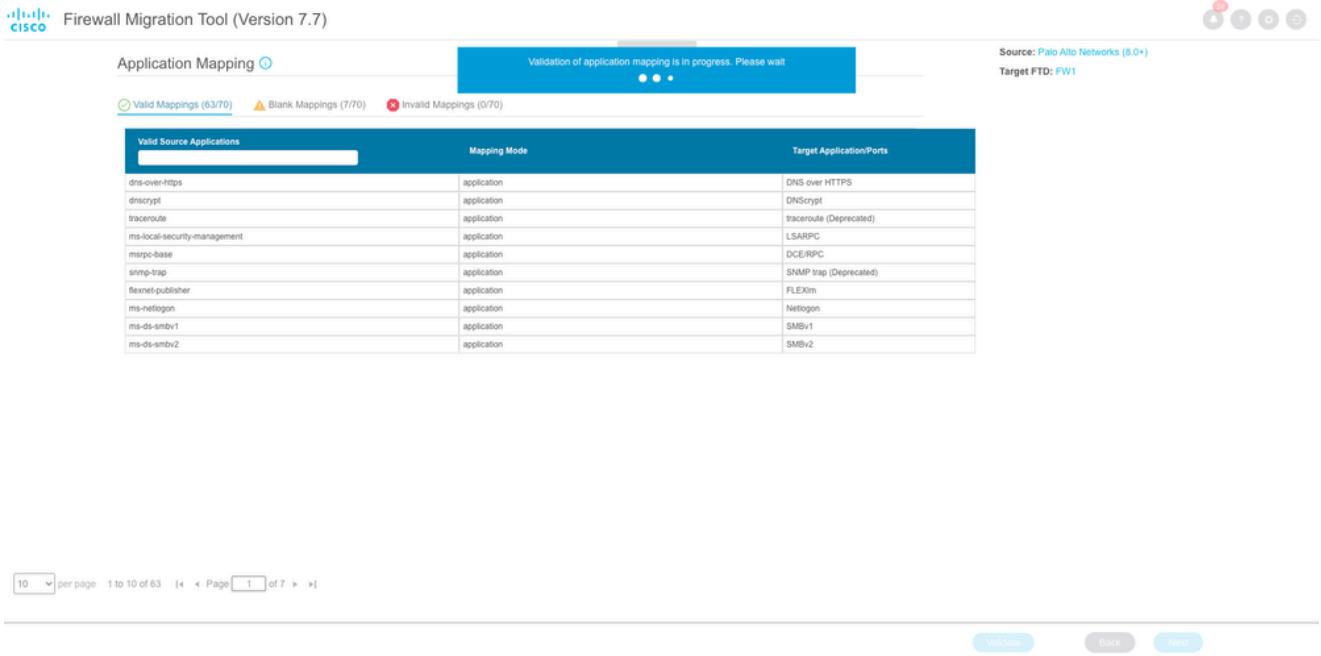


Création de zones de sécurité automatique

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



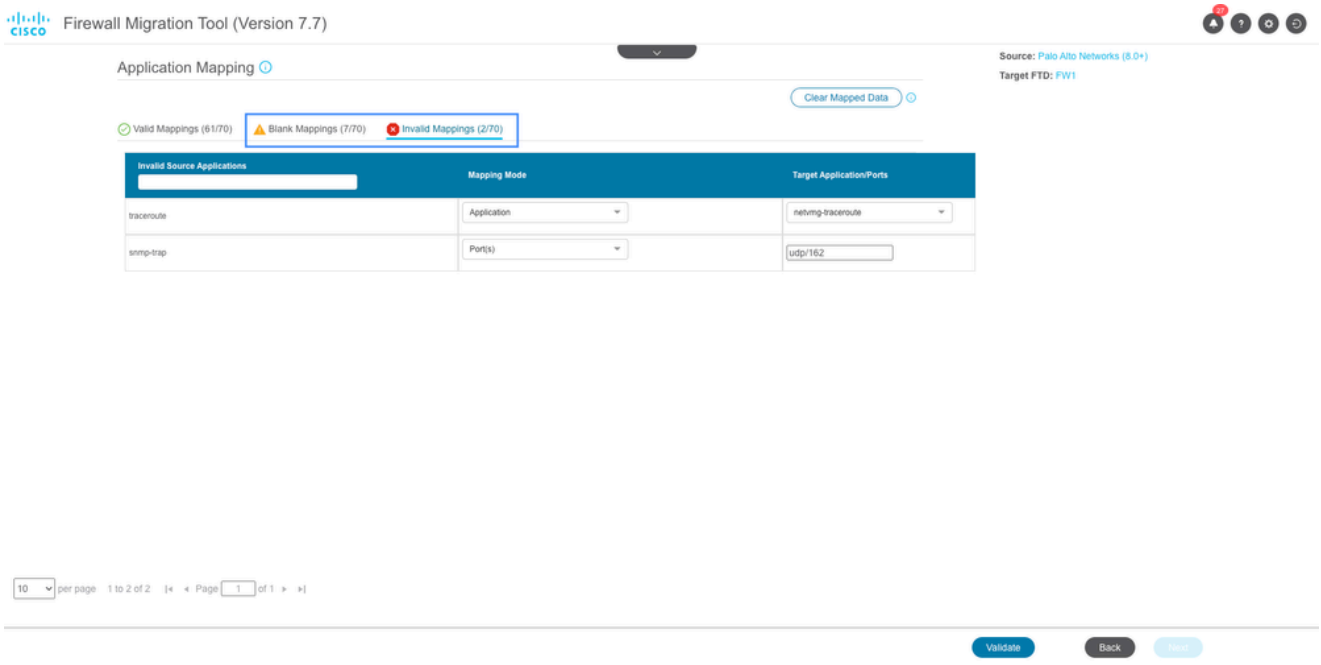
Mappage des applications



Validation du mappage des applications

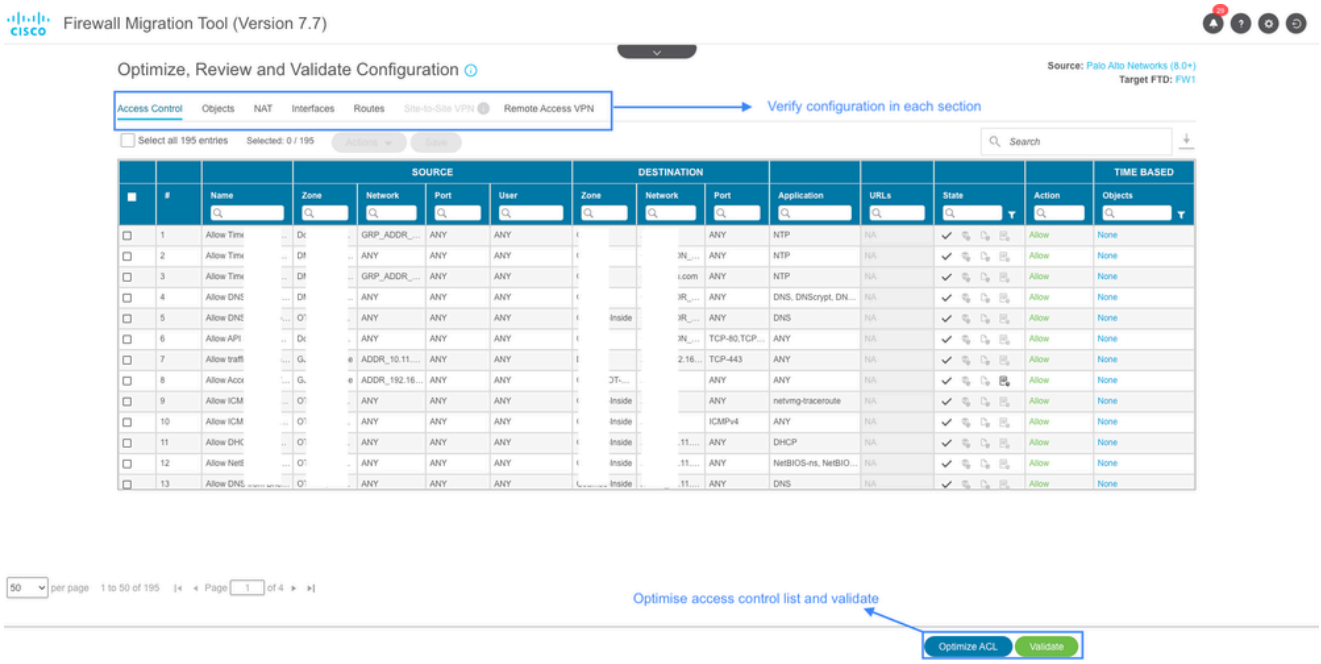
Lors de la validation, FMT répertorie les mappages vides et non valides. Les mappages non valides doivent être corrigés avant de poursuivre et la correction des mappages vides est facultative.

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



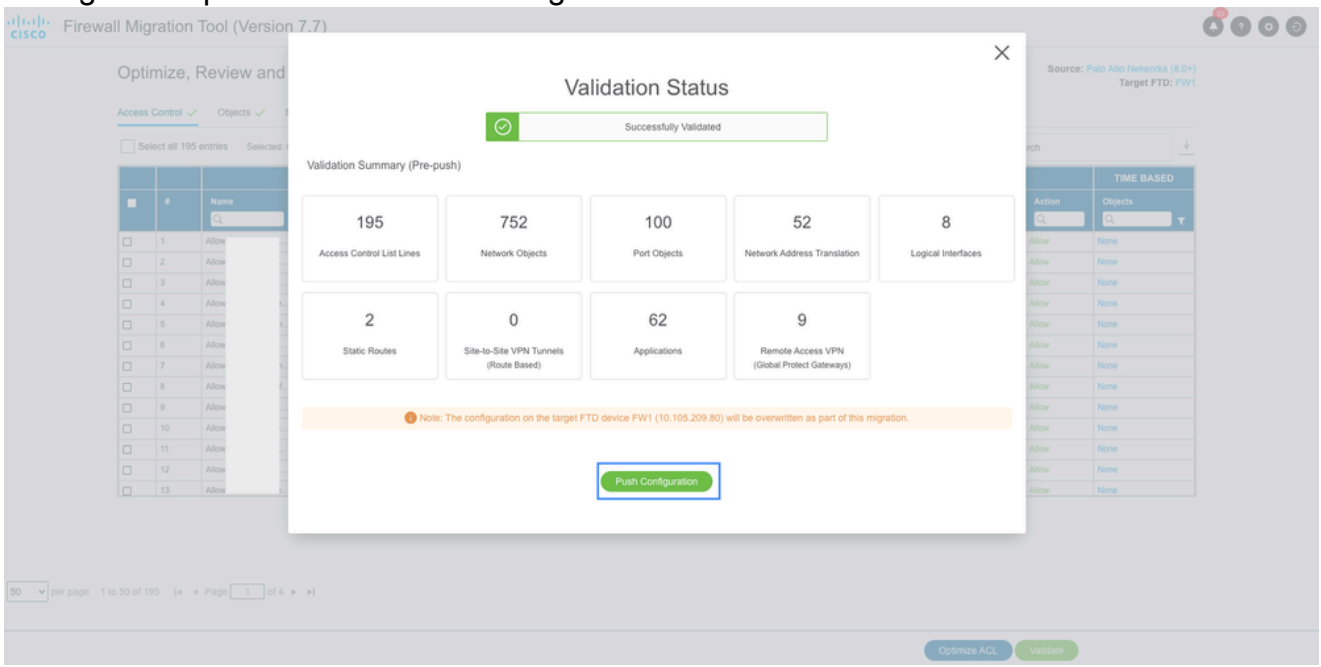
Mappage d'application vide et non valide

17. 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.



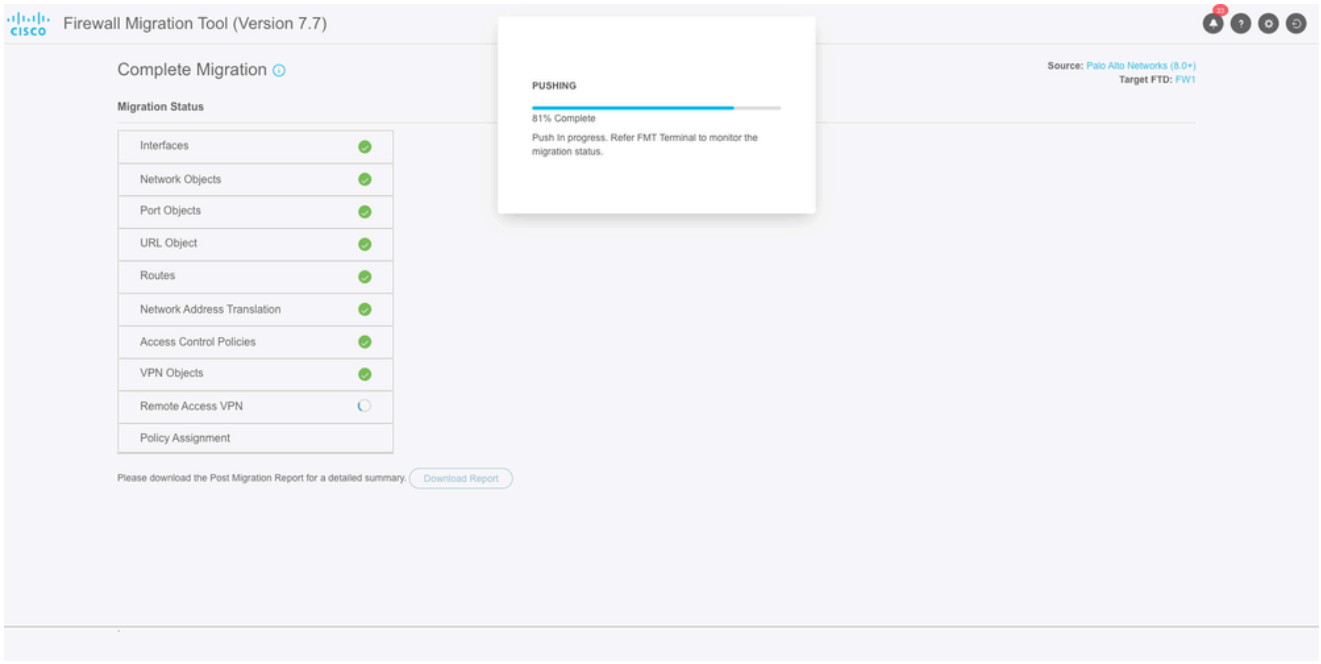
Validation de configuration

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



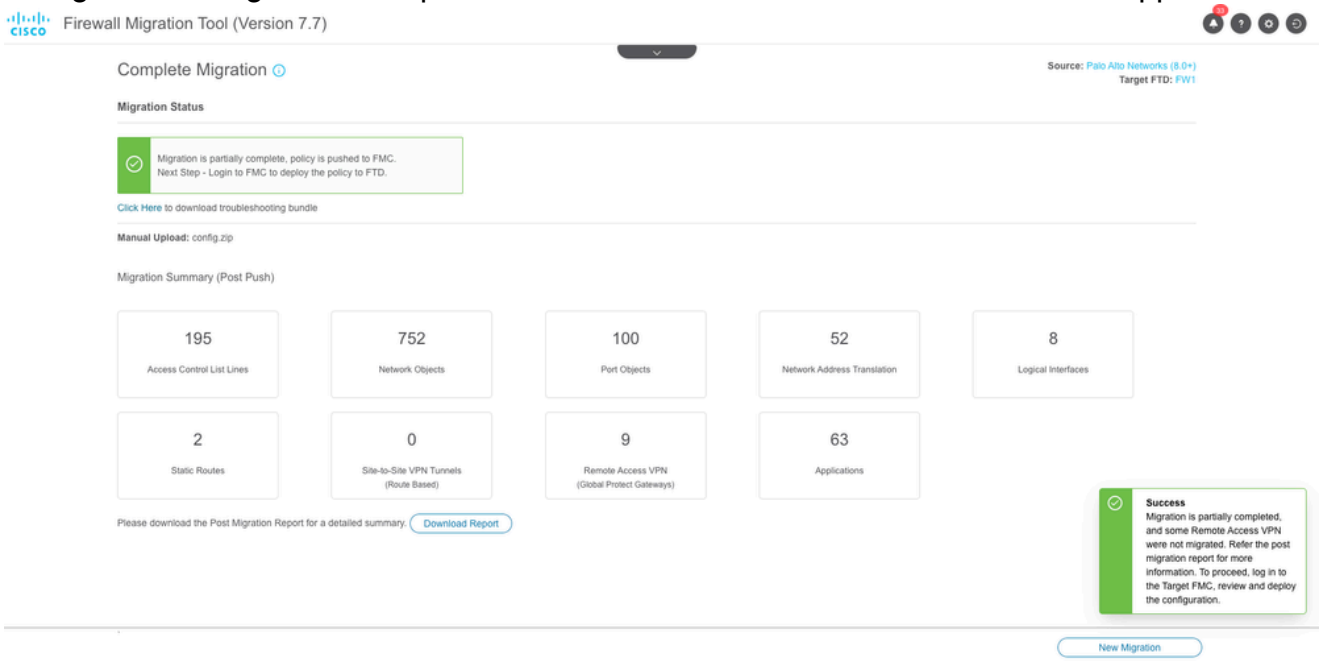
Récapitulatif de validation de configuration

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.