Transition transparente : Migration de Palo Alto Firewall vers Cisco FTD

Table des matières

Introduction

Ce document décrit le processus de transition d'un pare-feu Palo Alto à un système FTD Cisco en utilisant la version FMT 6.0.

Conditions préalables

Exigences

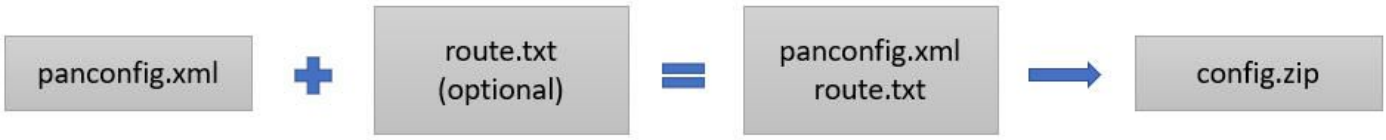
Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Exportation de la configuration en cours du pare-feu Palo Alto au format XML (*.xml).
- Accès à l'interface de ligne de commande du Palo Alto Firewall et exécution de la commande show routing route, puis enregistrement du résultat sous forme de fichier texte (*.txt).
- Compression du fichier de configuration (*.xml) et du fichier de sortie de routage (*.txt) dans une seule archive ZIP (*.zip).

Composants utilisés

Les informations contenues dans ce document sont basées sur la version 8.4.x ou ultérieure du pare-feu Palo Alto.

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.



Outil de migration Firepower (FMT)

Le FMT aide les équipes d'ingénierie à effectuer la transition des pare-feu des fournisseurs vers les pare-feu de nouvelle génération (NGFW)/Firepower Threat Defense (FTD) de Cisco. Veillez à utiliser la dernière version de FMT, téléchargée depuis le site Web de Cisco.

Guide de migration

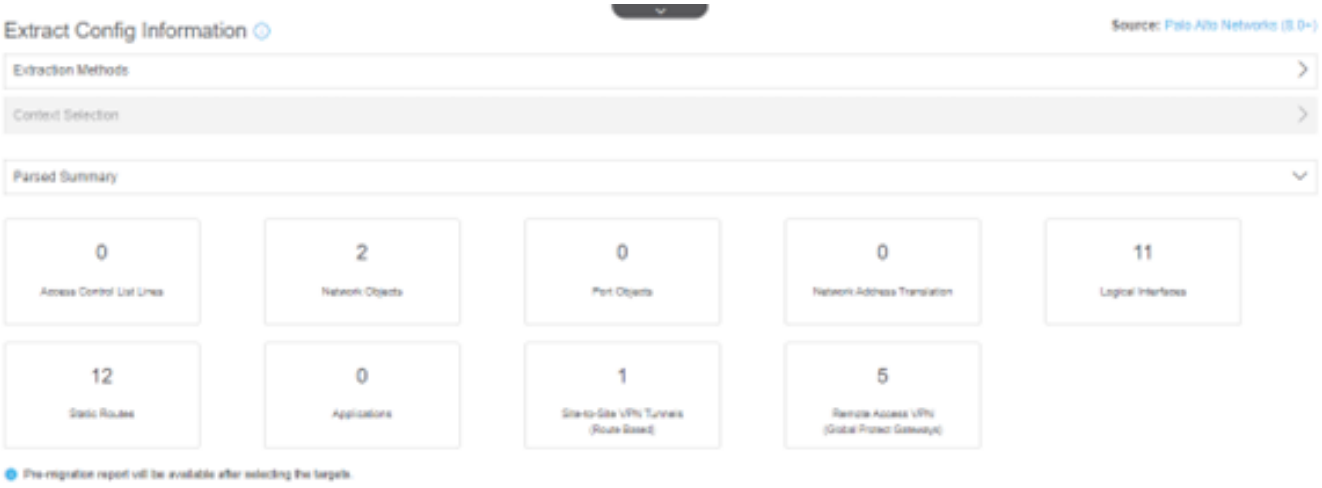
1. Liste de contrôle préalable à la migration

- Assurez-vous que le FTD a été ajouté au FMC avant de commencer le processus de migration.
- Un nouveau compte d'utilisateur avec des privilèges d'administration a été créé sur le FMC.
- Le fichier de configuration en cours Palo Alto exporté.xml doit être compressé avec l'extension .zip.
- Le pare-feu de nouvelle génération/FTD doit avoir le même nombre d'interfaces physiques ou de sous-interfaces ou de canaux de port que les interfaces du pare-feu Palo Alto.

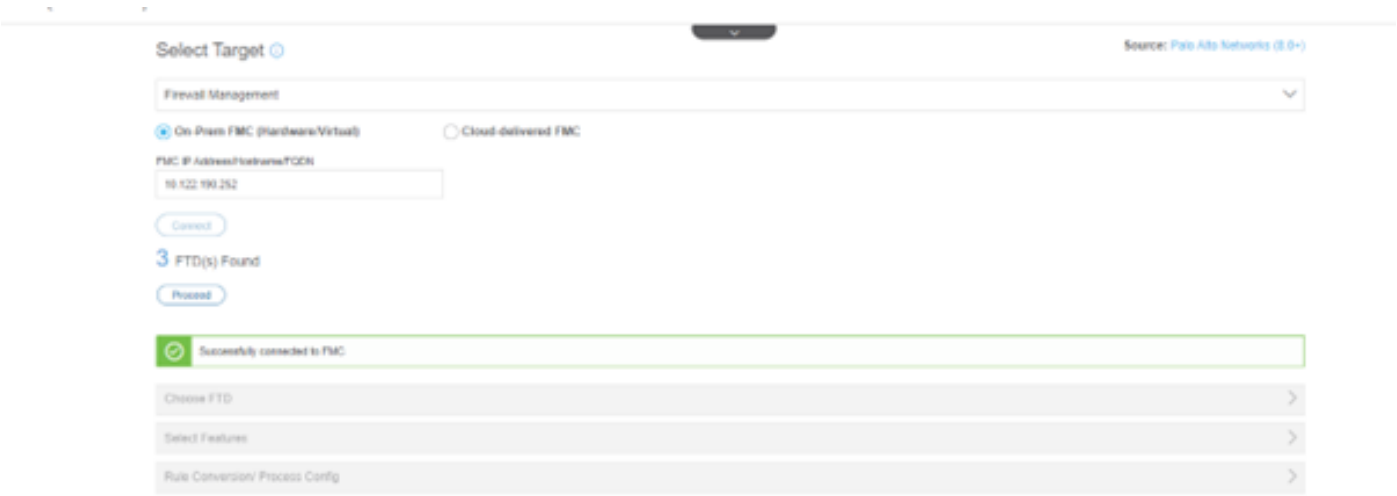
2. Utilisation des outils de migration

- Téléchargez l'outil FMT .exe et exécutez-le en tant qu'administrateur.
- FMT a besoin d'un ID CEC ou d'un compte utilisateur cisco pour se connecter.
- Après une connexion réussie, l'outil affiche un tableau de bord où vous pouvez choisir le fournisseur de pare-feu et télécharger le fichier *.zip correspondant ; reportez-vous à l'image suivante.

- Lisez attentivement les instructions fournies à droite avant de procéder à la migration.
- Cliquez sur Start Migration lorsque vous êtes prêt à commencer.
- Téléchargez le fichier *.zip qui contient les paramètres de configuration de votre pare-feu Palo Alto.
- Une fois le fichier de configuration téléchargé, vous pourrez voir un résumé analysé du contenu et cliquer sur next ; reportez-vous à l'image suivante.

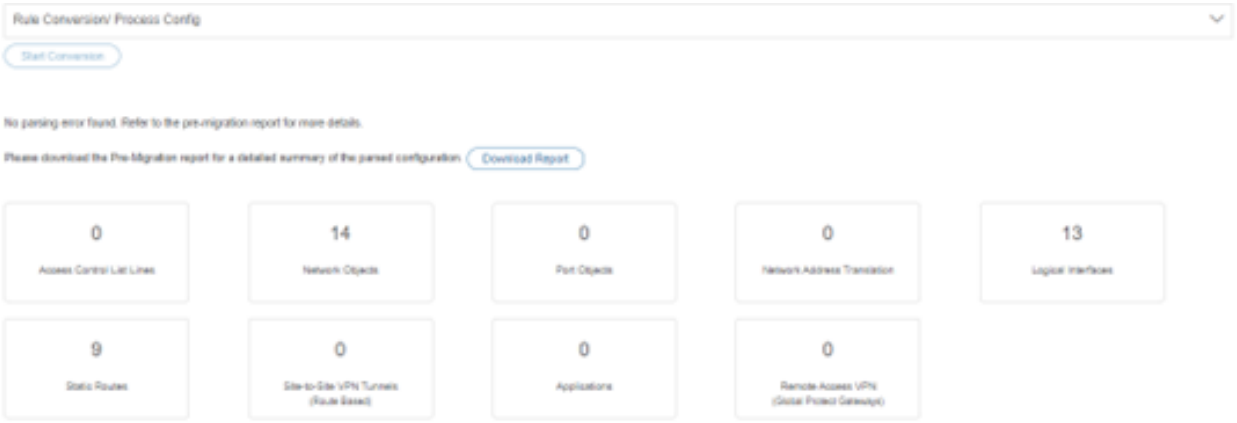


- Saisissez l'adresse IP du FMC et connectez-vous.
- L'outil recherche un FTD actif qui a été enregistré auprès du FMC.
- Choisissez le FTD que vous souhaitez migrer et cliquez sur Continuer, comme illustré dans l'image suivante.

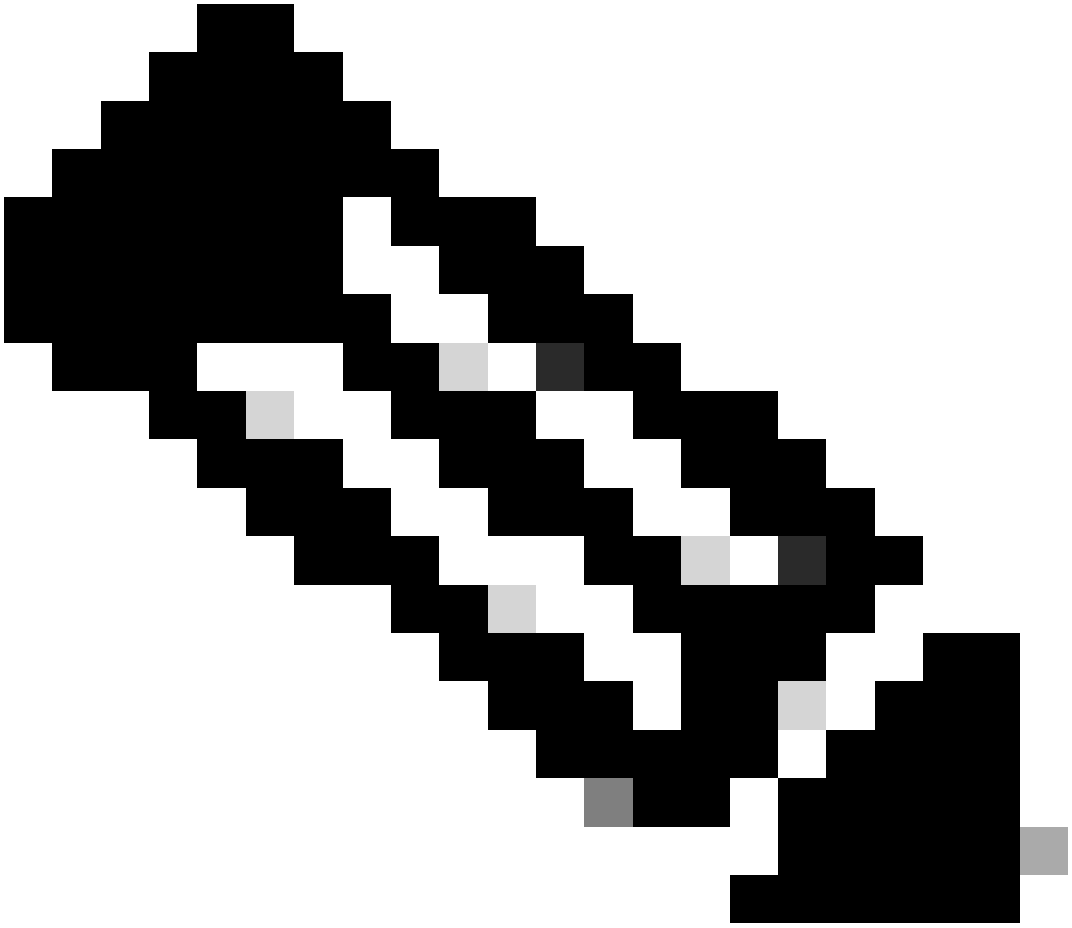


- Choisissez les fonctionnalités spécifiques afin de migrer en fonction des exigences du client. Notez que les pare-feu Palo Alto possèdent un jeu de fonctions différent de celui des pare-feu FTD.
- Cliquez sur Proceed et consultez l'image suivante pour référence.

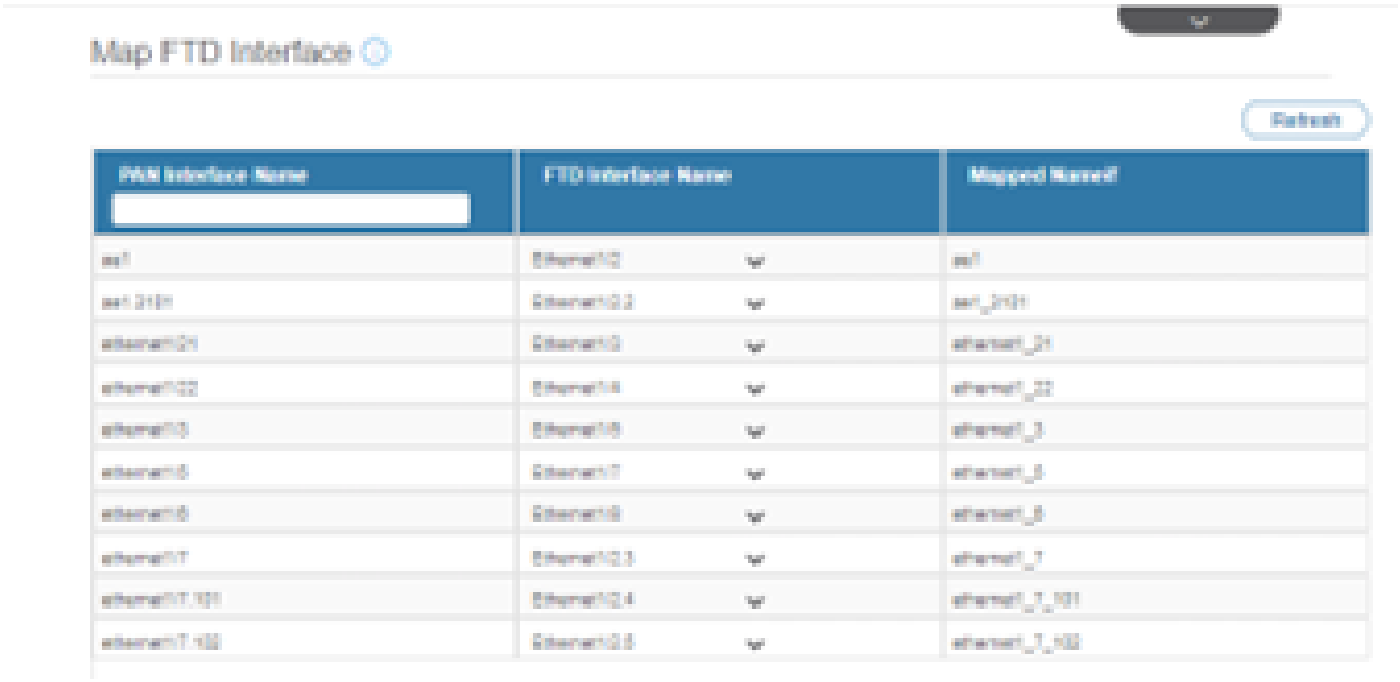
- Le FMT exécutera la conversion selon vos sélections. Vérifiez les modifications dans le rapport de pré-migration, puis cliquez sur Continuer. Reportez-vous à l'image suivante pour obtenir des conseils.



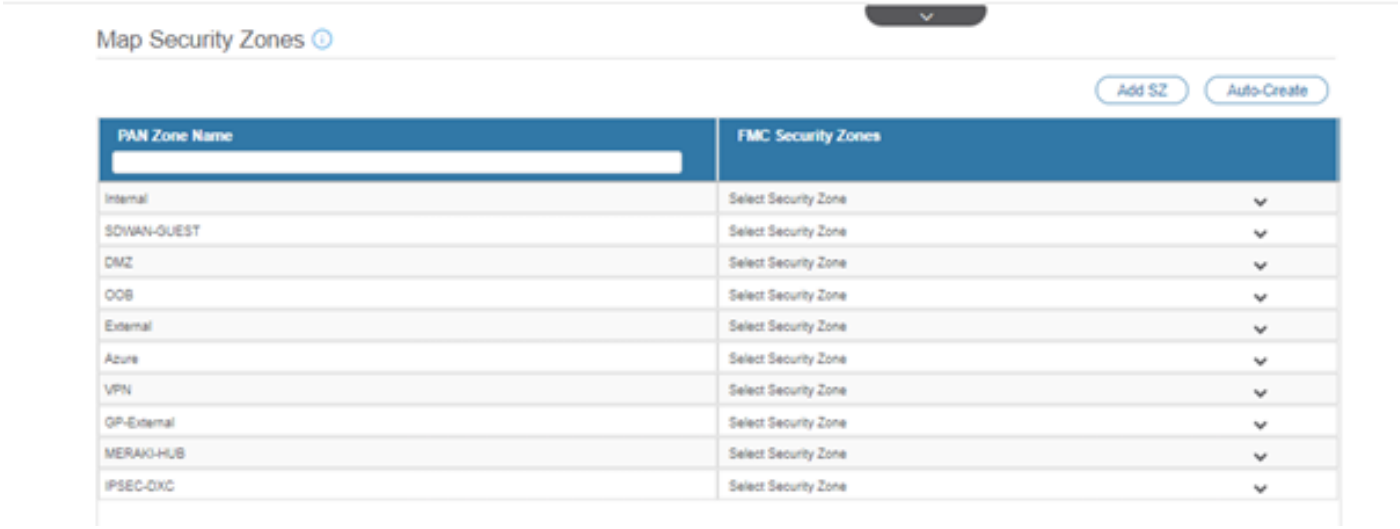
- Mappez les interfaces du pare-feu Palo Alto à celles du FTD. Reportez-vous à l'image suivante pour plus de détails.



Remarque : Le pare-feu de nouvelle génération/FTD doit avoir le même nombre d'interfaces physiques ou de sous-interfaces ou de canaux de port que les interfaces Palo Alto Firewall, y compris les sous-interfaces.



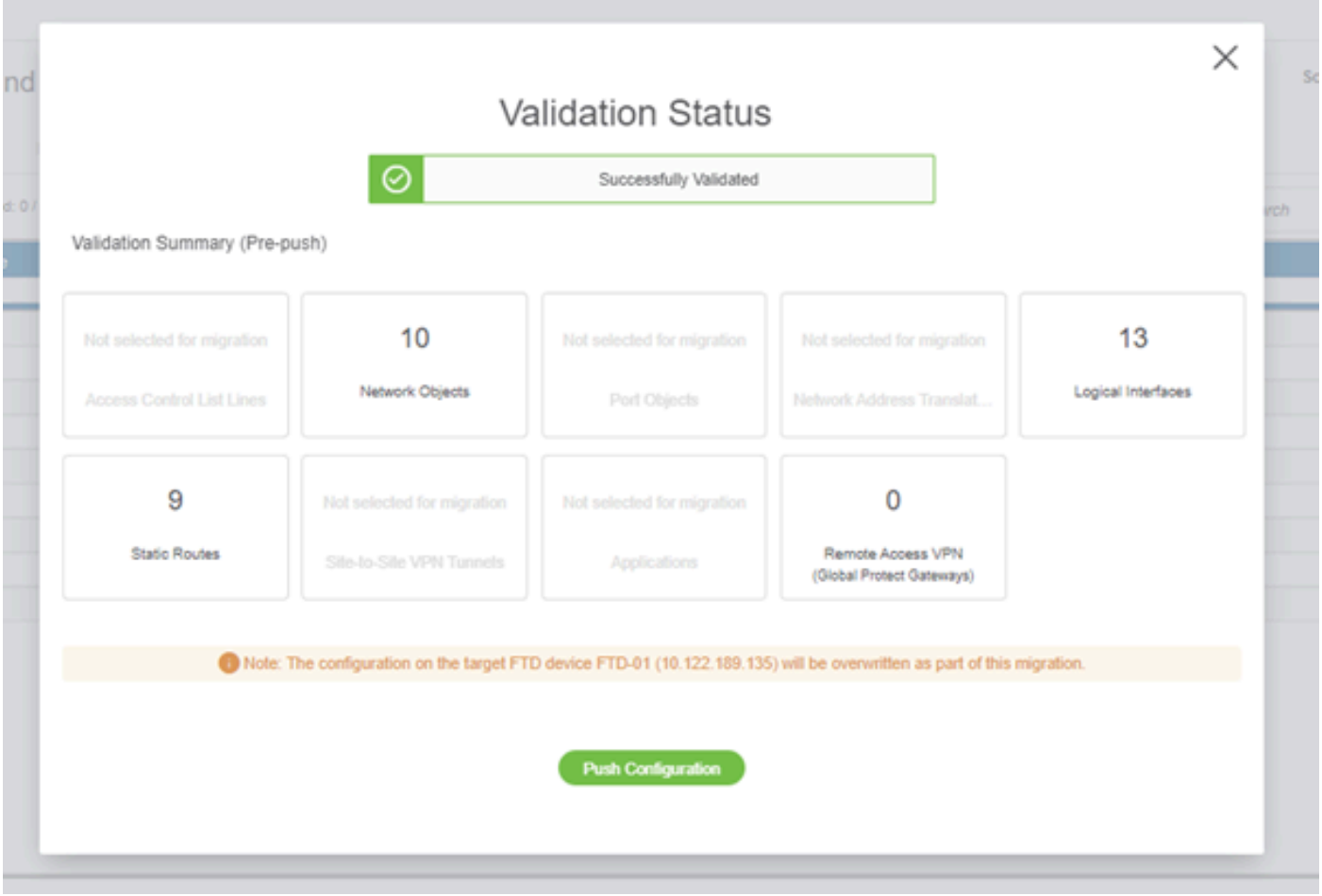
- Déterminez le mappage des zones, qui peut être effectué manuellement ou à l'aide de la fonction de création automatique. Pour la visualisation, reportez-vous à l'image suivante.



- Attribuez votre profil de blocage d'application. Comme il s’agit d’un périphérique de travaux pratiques sans mappage d’application, vous pouvez continuer avec les paramètres par défaut. Cliquez sur Next, et reportez-vous à l'image fournie.

- Optimisez les listes de contrôle d’accès, les objets, les interfaces et les routes selon vos besoins. Comme il s’agit d’une configuration de TP avec des configurations minimales, vous pouvez continuer avec les options par défaut. Cliquez ensuite sur Valider, en faisant référence à l'image suivante.

- Une fois la validation réussie, la configuration est prête à être déployée sur le FTD ciblé. Reportez-vous à l'image suivante pour obtenir des instructions supplémentaires.



- La configuration Push enregistre les configurations migrées dans FMC et est automatiquement déployée sur le FTD.
- En cas de problème lors de la migration, n'hésitez pas à ouvrir un dossier TAC pour obtenir de l'aide.

3. Validation post - migration

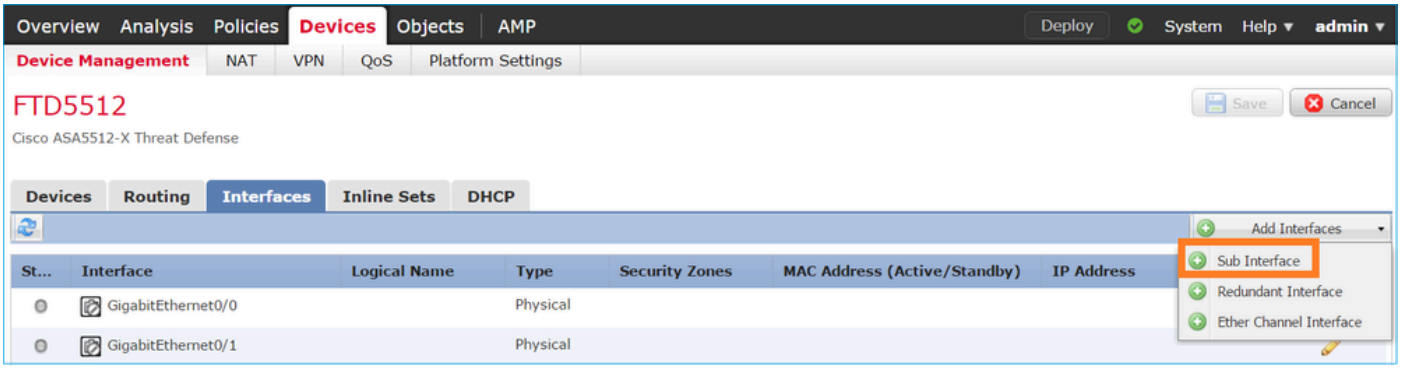
- Validation de la configuration sur le FTD et le FMC.
- Test des listes de contrôle d'accès, de la stratégie, de la connectivité et des autres fonctionnalités avancées du périphérique.
- Créez un point d'annulation avant d'effectuer des modifications.
- Test de la migration dans l'environnement de laboratoire avant le lancement dans l'environnement de production.

Problèmes identifiés

1. Interfaces manquantes sur FTD

- Connectez-vous à l'interface de ligne de commande Palo Alto et exécutez la commande show interface all. Vous devez avoir un nombre d'interfaces égal ou supérieur au nombre d'interfaces dans FTD.
- Créez un nombre égal ou supérieur d’interfaces : sous-interface, Port-channel ou interface physique via l’interface utilisateur graphique FMC.

- Accédez à FMC GUI Device > Device Management, cliquez sur le FTD dans lequel l'interface requise doit être créée. Dans la section Interface, dans le menu déroulant du coin droit, choisissez Create Sub-interface/BVI en conséquence et créez l'interface et associez les interfaces correspondantes. Enregistrez la configuration et synchronisez-la sur le périphérique.



- Vérifiez que les interfaces sont créées sur FTD en exécutant Show interface ip brief et poursuivez la migration pour le mappage d'interface.

2. Table de routage

- Vérifiez la table de routage sur le pare-feu Palo Alto en exécutant la commande Show routing ou Show routing summary.
- Avant de migrer les routes vers FTD, vérifiez la table et choisissez les routes requises en fonction des besoins du projet.
- Validez la même table de routage dans le FTD par Show route all et show route summary.

3. Optimiser

- Le panneau Optimisation des objets est grisé. Vous devez parfois créer un objet manuel dans FMC et le mapper. Pour afficher l'objet dans FTD, utilisez Show Running | dans les objets et dans Palo Alto, utilisez Afficher l'adresse <nom de l'objet>.
- La migration d'applications nécessite un audit du pare-feu Palo Alto avant la migration, FTD dispose d'un périphérique IPS dédié ou vous pouvez activer la fonctionnalité dans FTD afin que vous ayez besoin de planifier la tâche de migration d'applications selon les exigences du client.
- La configuration NAT du pare-feu Palo Alto doit être vérifiée par show running nat-policy et vous devez avoir une stratégie NAT personnalisée dans FTD, qui peut être affichée dans FTD par Show Running nat.

Conclusion

Le pare-feu Palo Alto a été migré vers Cisco FTD avec l'aide de FMT. En cas de problème après la migration sur le FTD et pour le dépannage, ouvrez un dossier TAC.

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.