Configuration de la migration VPN entre les FTD gérés par un seul FMC

Table des matières

Introduction

Ce document décrit la migration d'un VPN de site à site d'un FTD à un autre, géré par le même FMC, tout en conservant la connexion VPN au routeur.

Conditions préalables

Exigences

Pour mener à bien le processus de migration, Cisco recommande de se familiariser avec les sujets suivants :
· Inscription FTD auprès de FMC : Présentation de l'enregistrement des périphériques Firepower Threat Defense (FTD) auprès du Centre de gestion Firepower (FMC).
· Configuration VPN de site à site : Expérience de la configuration de VPN de site à site sur des périphériques FTD gérés par FMC.

Composants utilisés

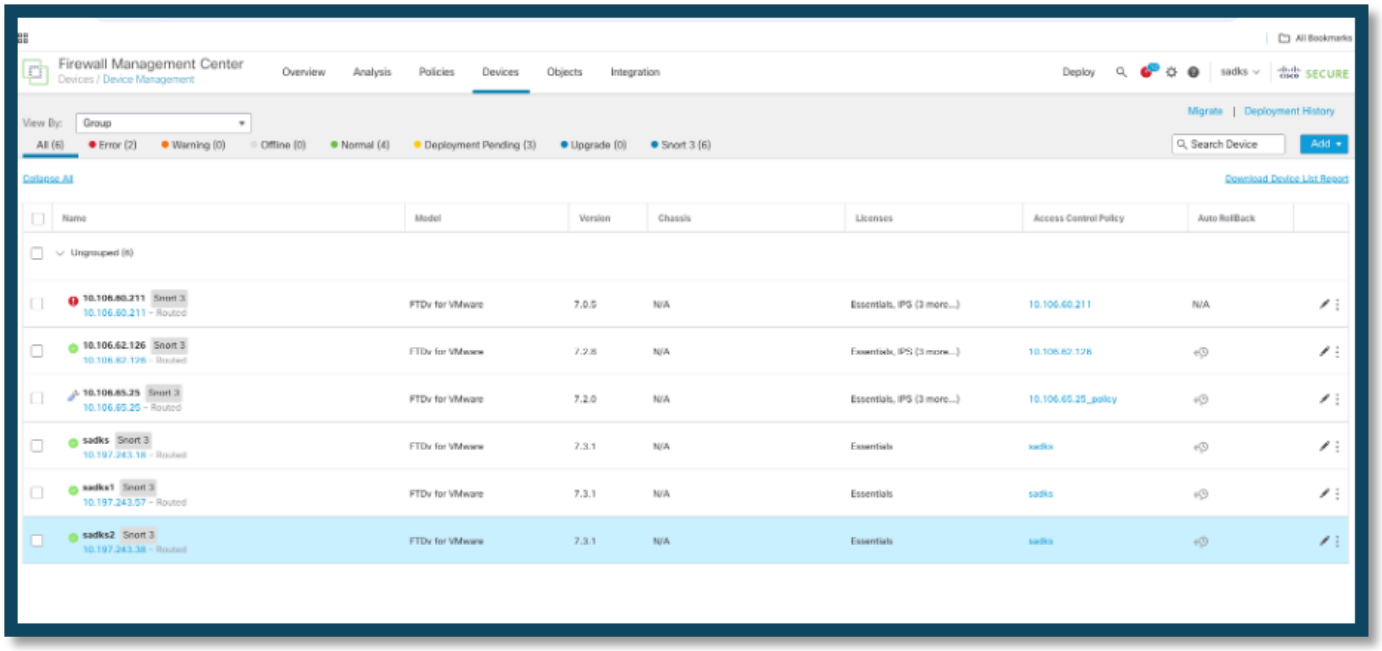
Ce document est basé sur les versions logicielles et matérielles fournies :
· Firepower Threat Defense Virtual (FTDv) : Deux instances exécutant la version 7.3.1.
· Firepower Management Center (FMC) : Version 7.4.0.

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.

Configurer

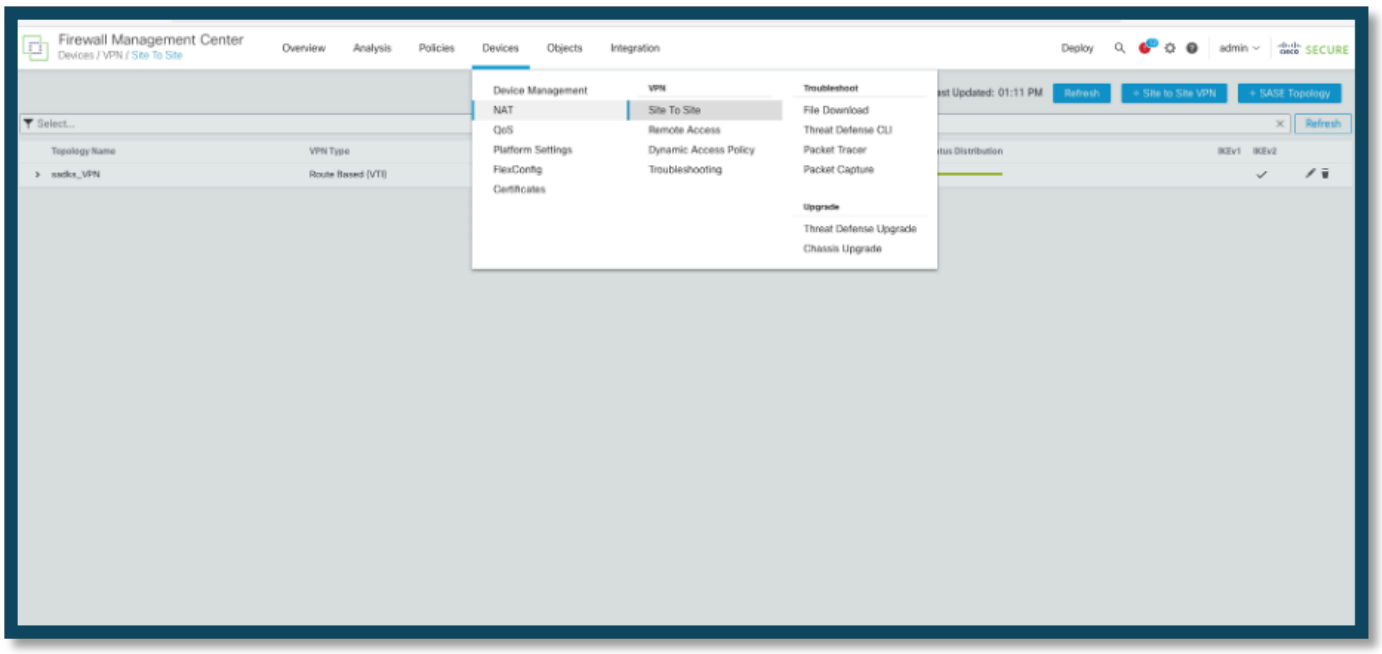
Procédure

1. Enregistrement du nouveau FTD auprès du FMC :
   · Commencez par enregistrer le nouveau périphérique Firepower Threat Defense (FTD) dans le Centre de gestion Firepower (FMC) sous Périphériques > Gestion des périphériques.
   · Dans cet exemple, le nouveau périphérique enregistré est nommé « sadks2 ».



Nouveau FTD enregistré

2. Accédez à la configuration du tunnel site à site :
   · Accédez aux paramètres de tunnel site à site en accédant à Périphériques > Site à site dans l'interface FMC.

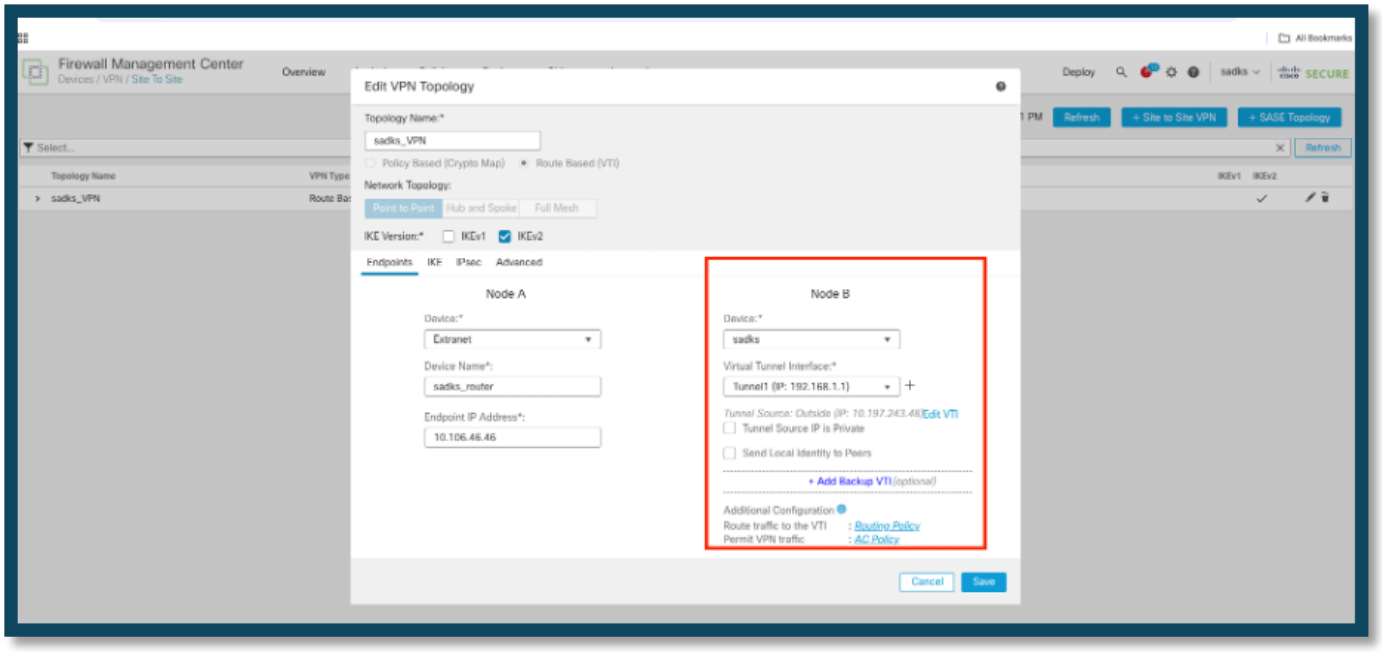


Accédez à VPN Config

3. Modifier la configuration VPN :

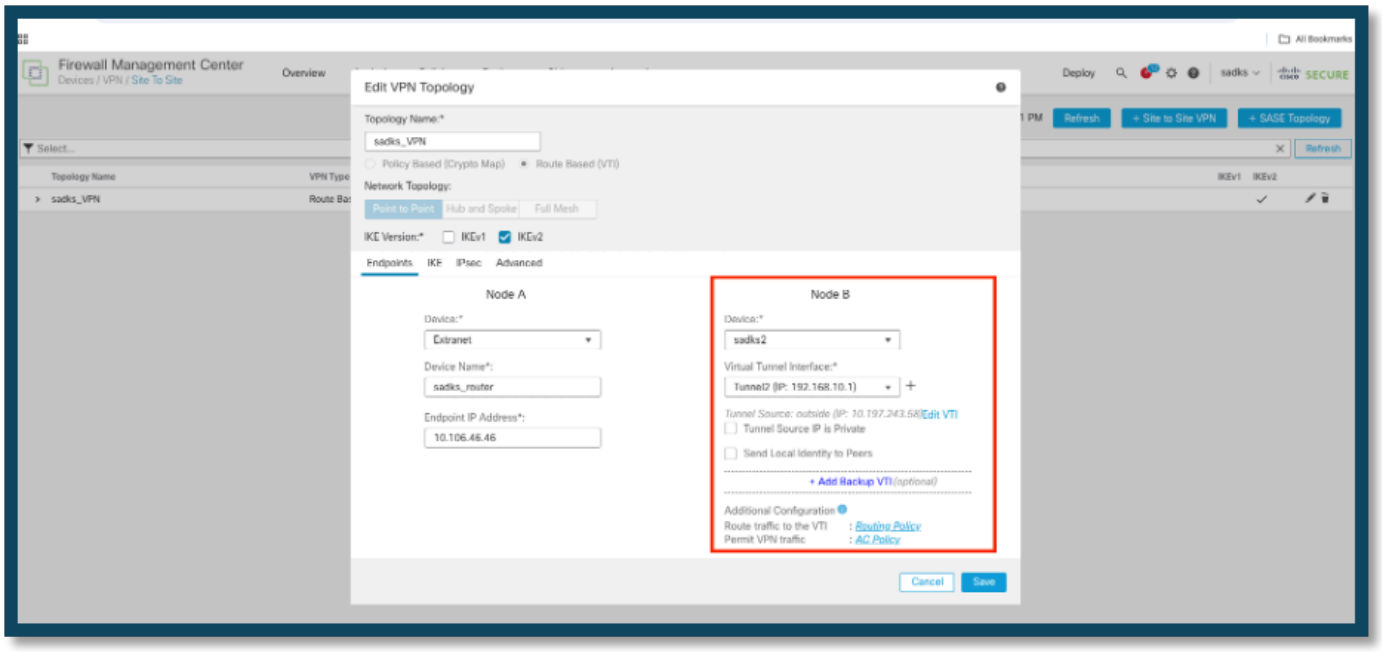
· Sélectionnez la configuration VPN que vous souhaitez mettre à jour.

•Exemple : Dans ce scénario, la configuration VPN implique un périphérique FTD et un routeur. Ici, le noeud B représente le périphérique FTD, et la configuration a été mise à jour pour changer l'association de périphérique de "sadks" à "sadks2".



Ancien périphérique FTD

PAR



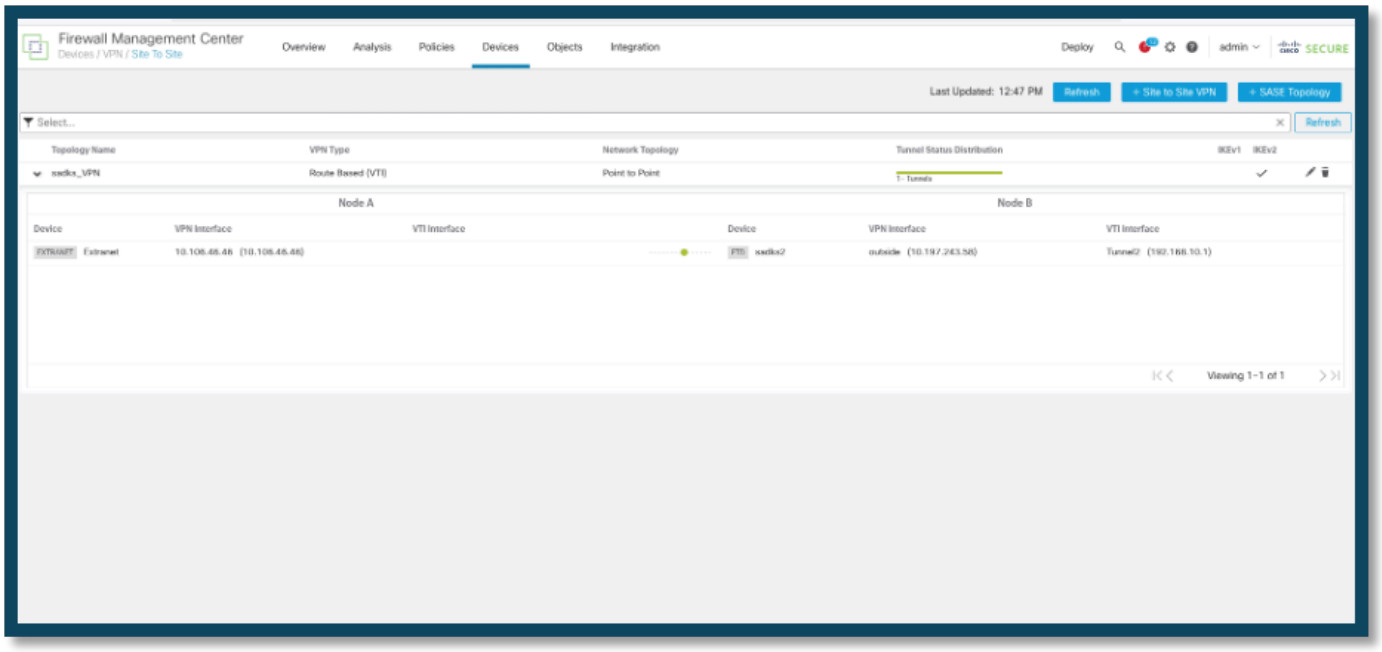
Nouveau périphérique FTD

4. Enregistrez et déployez la configuration :

· Après avoir effectué les modifications nécessaires, enregistrez la configuration et déployez-la pour activer les mises à jour.

Vérifier

Le tunnel s'active une fois déployé.



État du tunnel

Dépannage

Problèmes de connectivité initiaux

Lors de la construction d'un VPN, deux parties négocient le tunnel. Par conséquent, il est préférable d'obtenir les deux côtés de la conversation lorsque vous dépannez un type de défaillance de tunnel. Un guide détaillé sur la façon de déboguer les tunnels IKEv2 peut être trouvé ici : Comment déboguer les VPN IKEv2

La cause la plus fréquente des pannes de tunnel est un problème de connectivité. La meilleure façon de le déterminer est d'effectuer des captures de paquets sur le périphérique. Utilisez cette commande pour effectuer des captures de paquets sur le périphérique :

<#root>

```
capture capout interface outside match ip host 10.106.46.46 host 10.197.243.58
```

Une fois la capture en place, essayez d'envoyer le trafic sur le VPN et vérifiez le trafic bidirectionnel dans la capture de paquets.

Examinez la capture de paquets avec cette commande :

<#root>

```
show cap capout
```

Problèmes spécifiques au trafic

Les problèmes de trafic courants que vous rencontrez sont les suivants :

- Problèmes de routage derrière le FTD : le réseau interne ne peut pas router les paquets vers les adresses IP et les clients VPN attribués.
- Listes de contrôle d'accès bloquant le trafic.
- Traduction d'adresses réseau non contournée pour le trafic VPN.

Pour plus d'informations sur les VPN sur le FTD géré par FMC, vous pouvez trouver le guide de configuration complet ici : FTD géré par le guide de configuration FMC

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.