Configurer l'accès à la gestion pour SSH et HTTPS sur FTD via FDM ou CLISH

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Configurer

- Étapes FDM
- Étapes CLISH

Vérifier

Références

Introduction

Ce document décrit le processus de configuration et de vérification de la liste d'accès de gestion pour SSH et HTTPS sur FTD géré localement ou à distance.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

- Cisco Secure Firewall Threat Defense version 7.4.1 gérée par FDM.

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.

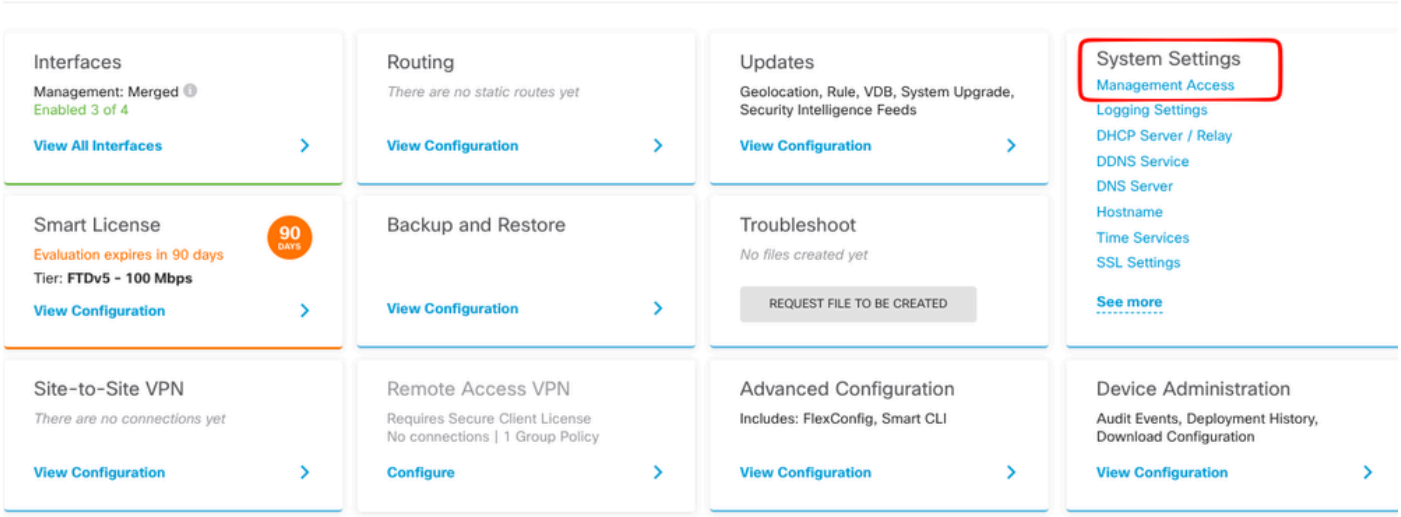
Configurer

FTD peut être géré localement à l'aide de FDM ou via FMC. L'objectif principal de ce document est l'accès à la gestion via FDM et CLI. Grâce à l'interface de ligne de commande, vous pouvez apporter des modifications à FDM et FMC.

⚠ Mise en garde : Configurez les listes d'accès SSH ou HTTPS une par une pour éviter le verrouillage de session. Tout d'abord, mettez à jour et déployez un protocole, vérifiez l'accès, puis passez à l'autre.

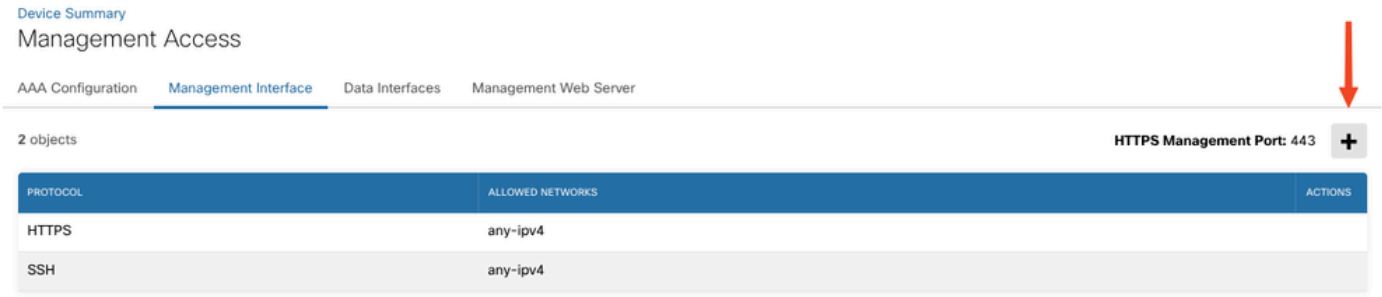
Étapes FDM

1. Connectez-vous au Gestionnaire de périphériques Firepower (FDM) et accédez à Paramètres système > Accès à la gestion > Interface de gestion.



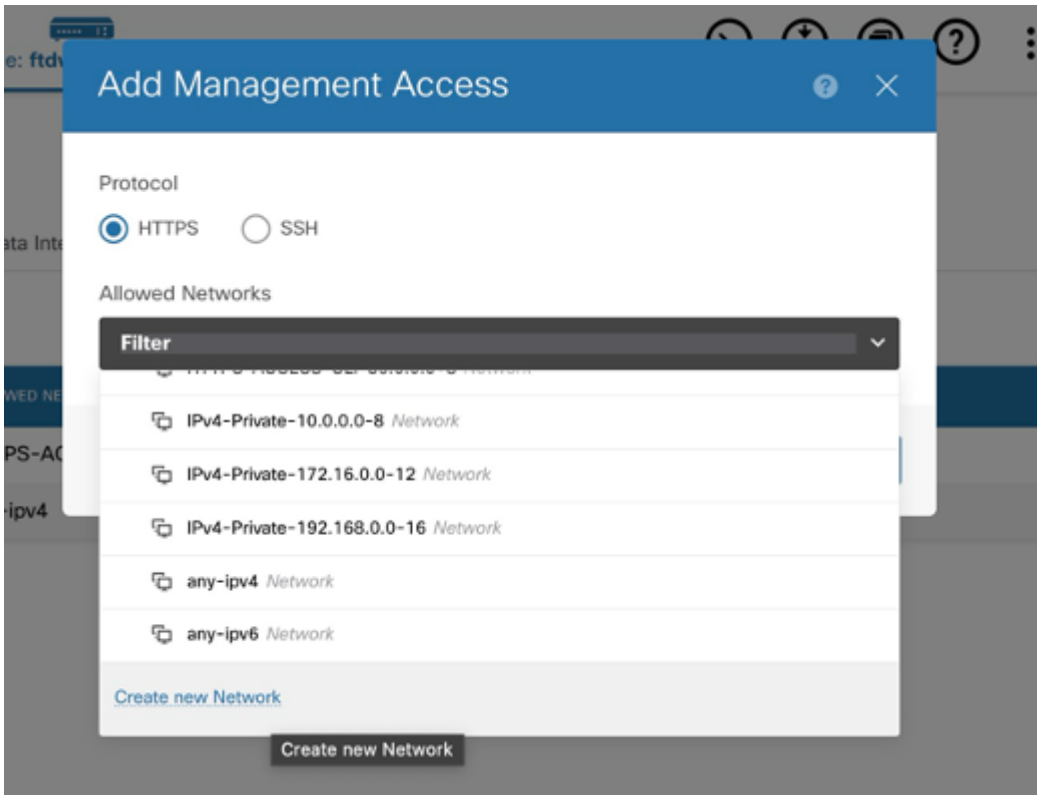
---

2. Cliquez sur l'icône + pour ouvrir la fenêtre d'ajout du réseau.



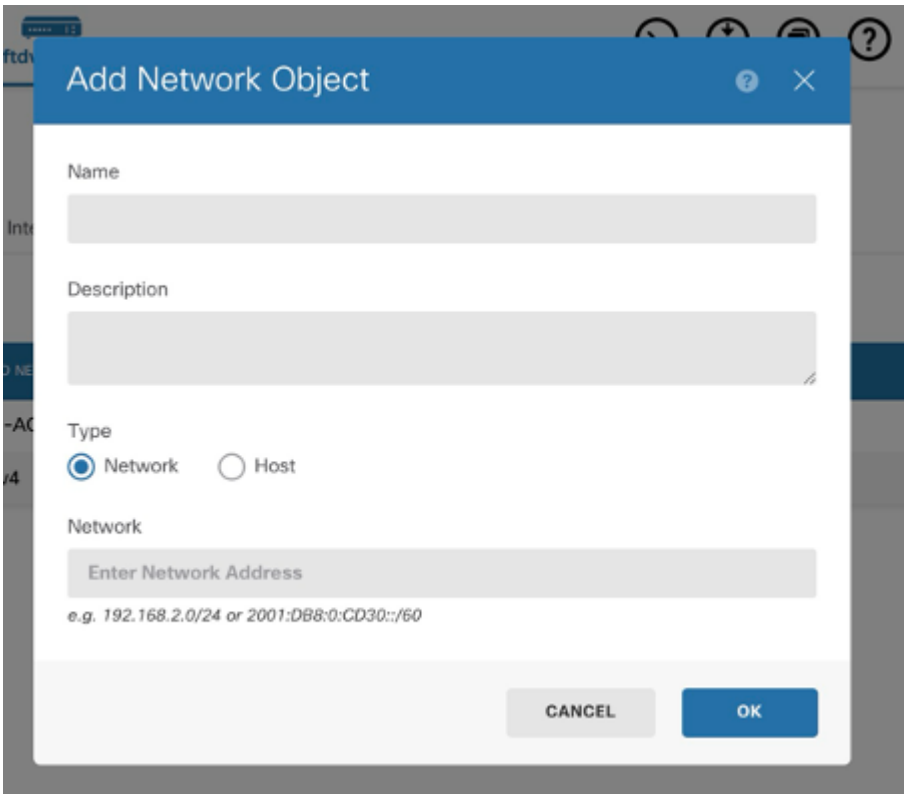
---

3. Ajoutez l'objet réseau pour accéder à SSH ou HTTPS. Si vous devez créer un nouveau réseau, sélectionnez l'option Create New Network. Vous pouvez ajouter plusieurs entrées pour les réseaux ou les hôtes dans la section Accès à la gestion.



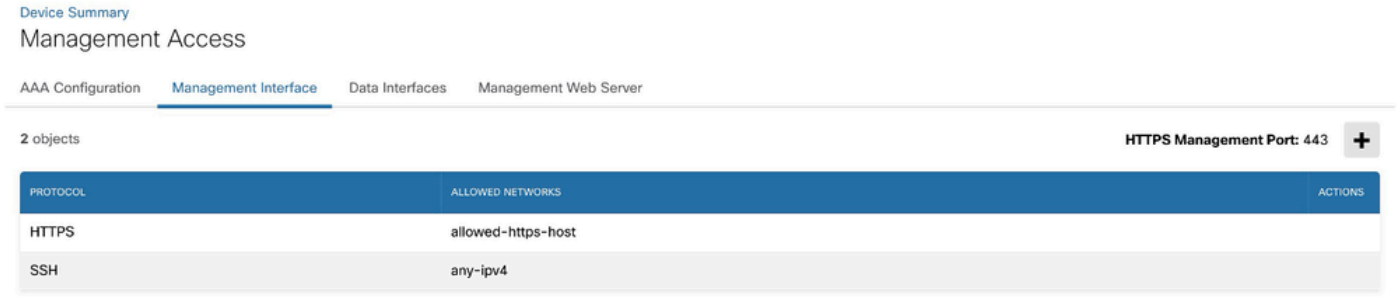
---

4. Facultatif : Sélectionnez l'option Créer un nouveau réseau pour ouvrir la fenêtre Ajouter un objet réseau.



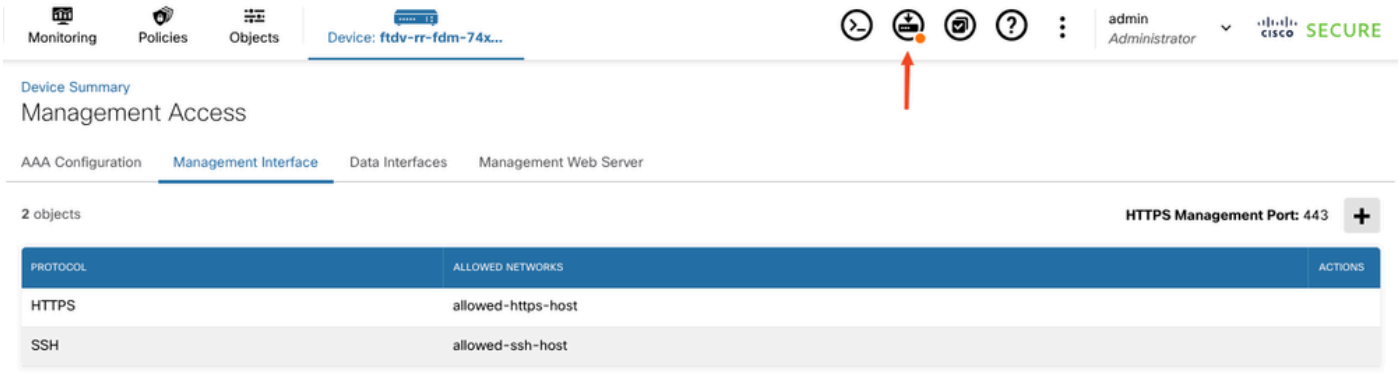
---

5. Vérifiez les modifications apportées et déployez.

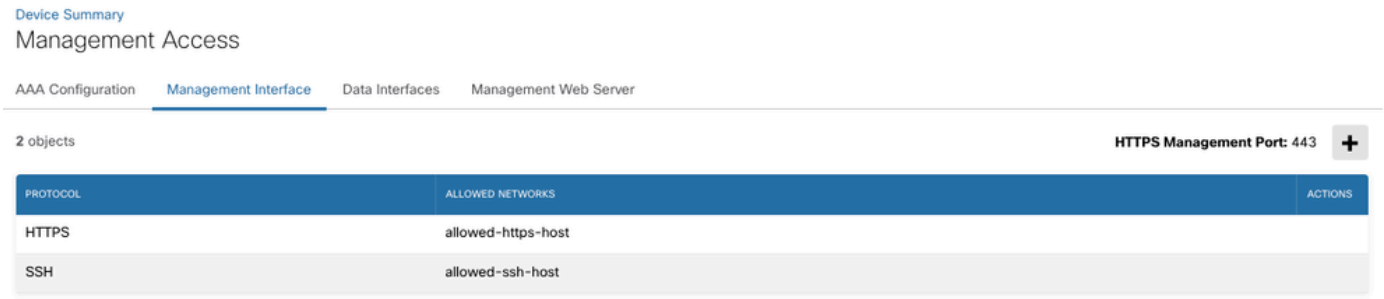


---

6. Facultatif : une fois les modifications précédentes pour HTTPS vérifiées, répétez la même chose pour SSH.



7. Déployez les modifications et vérifiez votre accès à FTD à partir du réseau et de l'hôte autorisés.



Étapes CLISH

Les étapes CLI peuvent être utilisées si FDM ou FMC sont tous deux gérés. Pour configurer le périphérique afin qu'il accepte les connexions HTTPS ou SSH à partir d'une adresse IP ou d'un réseau spécifié, exécutez la commande configure https-access-list ou configure ssh-access-list.

- Vous devez inclure tous les hôtes ou réseaux pris en charge dans une seule commande. Les adresses spécifiées dans cette commande écrasent le contenu actuel de la liste de contrôle d’accès correspondante.
- S'il s'agit d'une unité d'un groupe haute disponibilité géré localement, vos modifications sont remplacées lors du prochain déploiement des mises à jour de configuration par l'unité active. S'il s'agit de l'unité active, les modifications sont propagées à l'homologue lors du déploiement.

```
> configure https-access-list x.x.x.x/x,y.y.y.y/y
```

```
The https access list was changed successfully.

> show https-access-list
ACCEPT     tcp  --  x.x.x.x/x            anywhere             state NEW tcp dpt:https
ACCEPT     tcp  --  y.y.y.y/y            anywhere             state NEW tcp dpt:https
```

Remarque : x.x.x.x/x et y.y.y.y/y représente une adresse IPv4 avec notation CIDR. Pour spécifier tous les hôtes IPv4, entrez 0.0.0.0/0. Pour spécifier tous les hôtes IPv6, spécifiez ::/0.

Pour les connexions SSH, exécutez la commande configure ssh-access-list.

```
> configure ssh-access-list x.x.x.x/x

The ssh access list was changed successfully.

> show ssh-access-list
ACCEPT     tcp  --  x.x.x.x/x            anywhere             state NEW tcp dpt:ssh
```

Remarque : Vous pouvez exécuter des commandes configure disable-https-access ou configure disable-ssh-access pour désactiver l'accès HTTPS ou SSH respectivement. Assurez-vous que vous êtes au courant de ces modifications, car elles peuvent vous verrouiller hors de la session.

Vous pouvez également configurer plusieurs entrées dans une seule commande avec une virgule séparée pour les valeurs ipaddress/CIDR.

Vérifier

Pour vérifier à partir de CLISH, vous pouvez exécuter les commandes suivantes :

```
> show ssh-access-list
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:ssh

> show https-access-list
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:https
```

L'exemple de sortie montre l'entrée f2b-ssh. Après 10 tentatives SSH infructueuses consécutives, le système ajoute automatiquement une entrée f2b-sshd pour exécuter la sortie de commande show ssh-access-list.

```
> show ssh-access-list
f2b-sshd   tcp  --  anywhere            anywhere            tcp dpt:ssh
ACCEPT     tcp  --  anywhere            anywhere            state NEW tcp dpt:ssh
Chain f2b-sshd (1 references)
```

Reportez-vous à f2b dans la section des références.

Références

- Référence des commandes de Cisco Secure Firewall Threat Defense
- Guide de configuration de Cisco Firepower Threat Defense pour Firepower Device Manager

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.