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

Table des matières

Introduction

Ce document décrit la procédure pour configurer et vérifier 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.

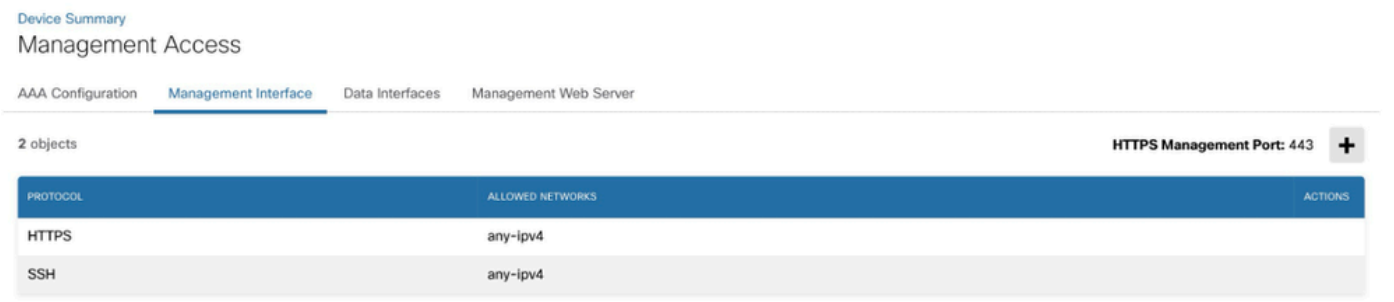
Configurer

FTD peut être géré localement à l'aide de FDM ou via FMC. Dans ce document, l'accent est mis sur l'accès à la gestion via FDM et CLI. L'interface de ligne de commande vous permet d'apporter des modifications aux scénarios 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.

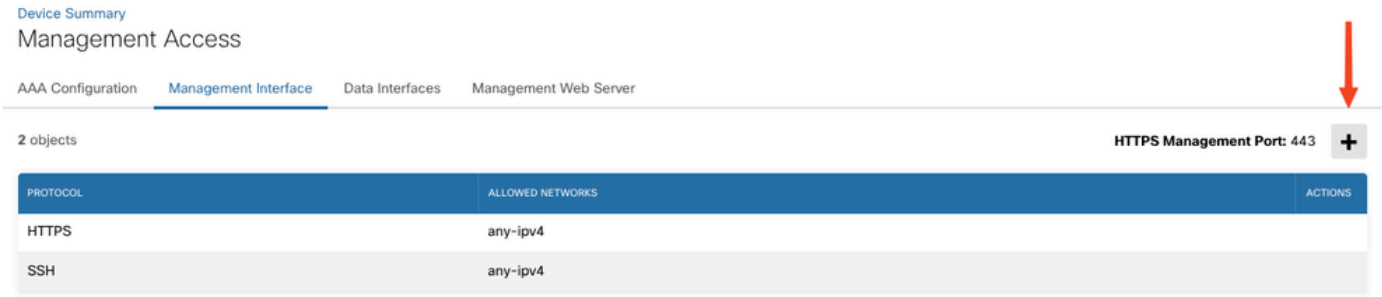
Étapes FDM :

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



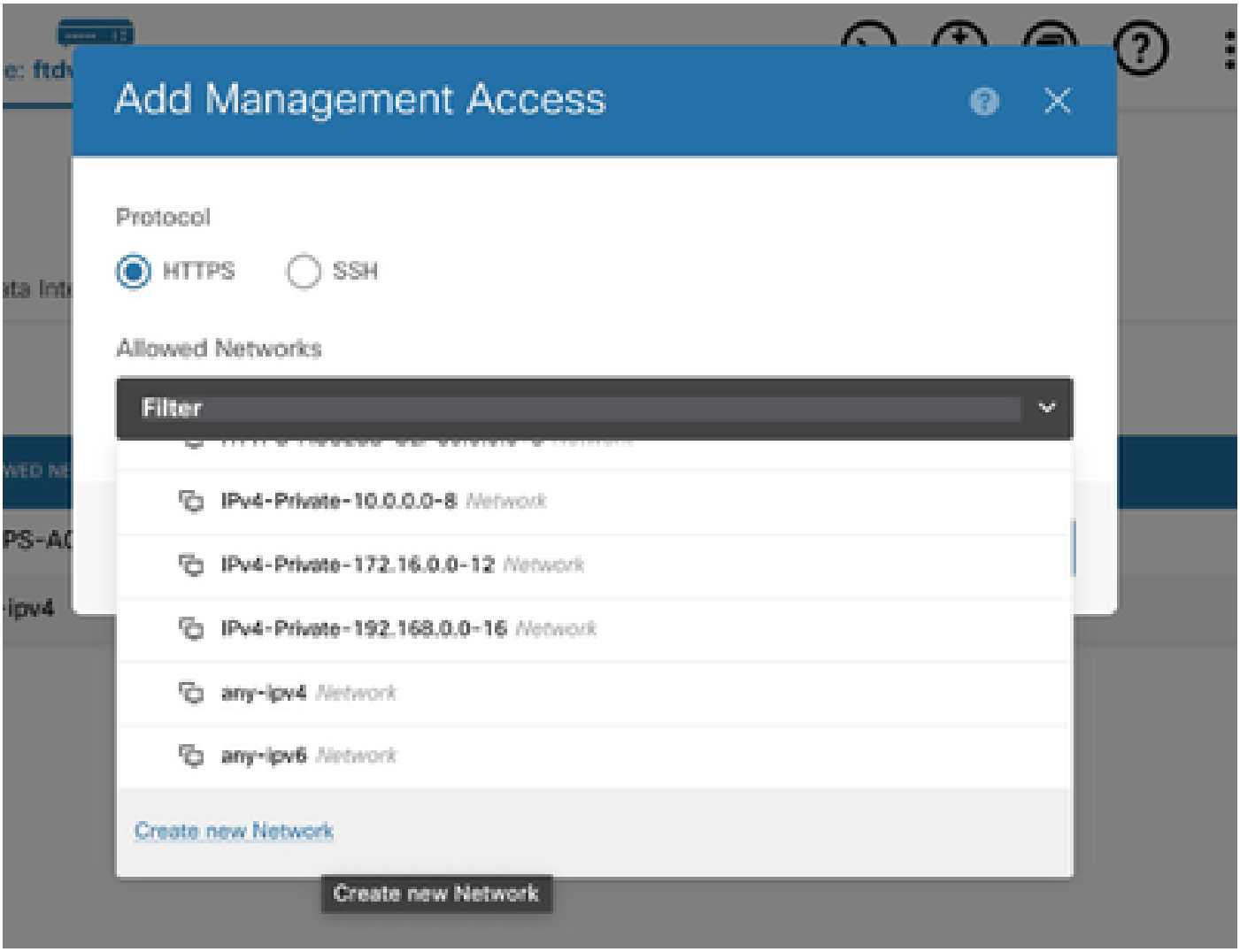
Par défaut, tout accès IPv4 est autorisé sur le port de gestion pour SSH et HTTPS

Étape 2 : cliquez sur l'icône + pour ouvrir la fenêtre d'ajout du réseau.



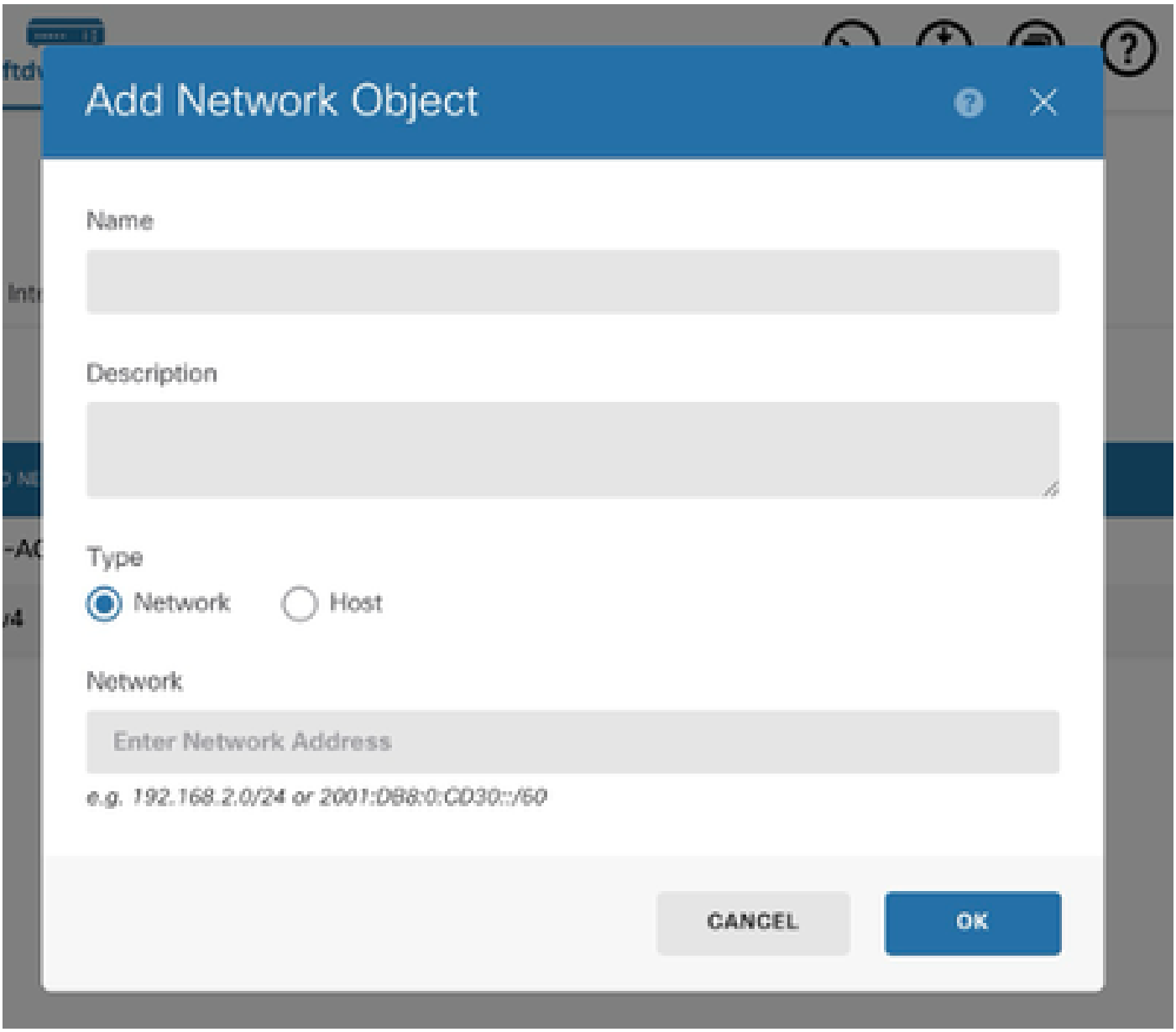
Cliquez sur le bouton Ajouter en haut à droite.

Étape 3 : ajoutez l'objet réseau pour avoir un accès 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 l'accès de gestion.



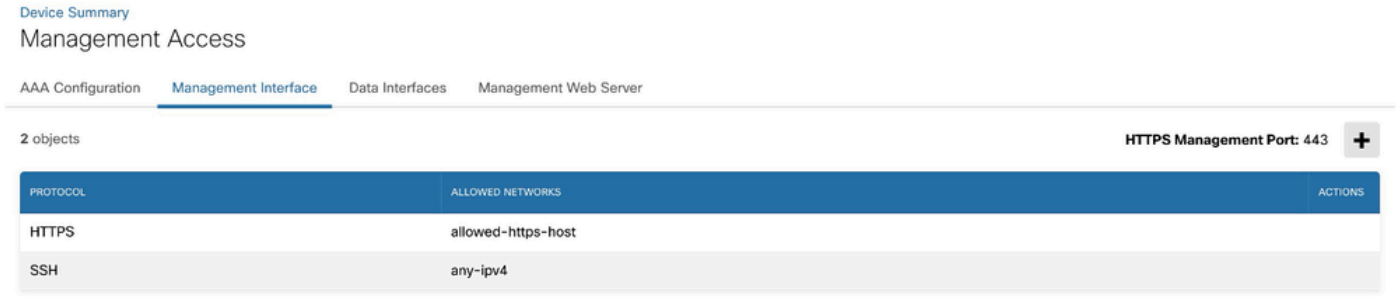
Sélectionnez le réseau.

Étape 4 (facultative): L'option Créer un réseau ouvre la fenêtre Ajouter un objet réseau.

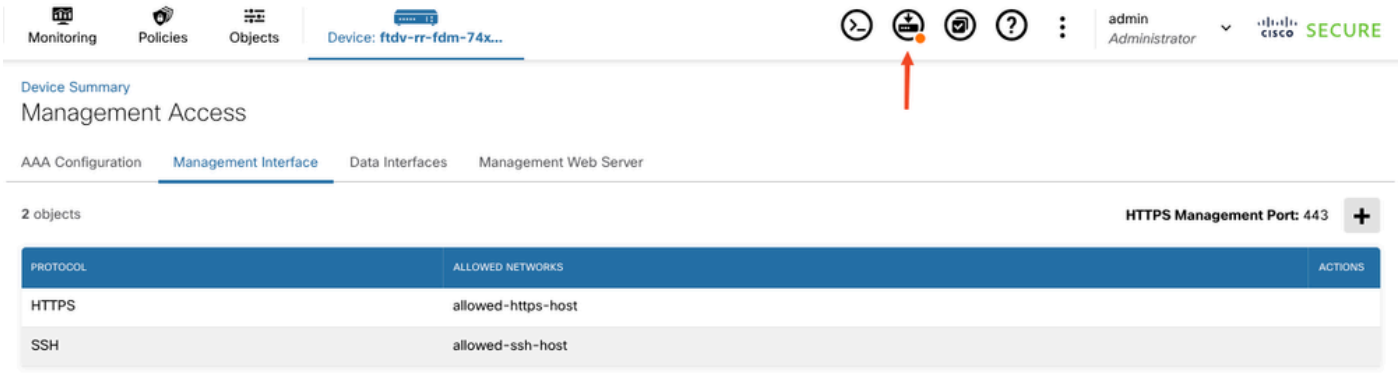


Créez un réseau d'hôtes selon vos besoins.

Étape 5 : vérifiez les modifications apportées et déployez.

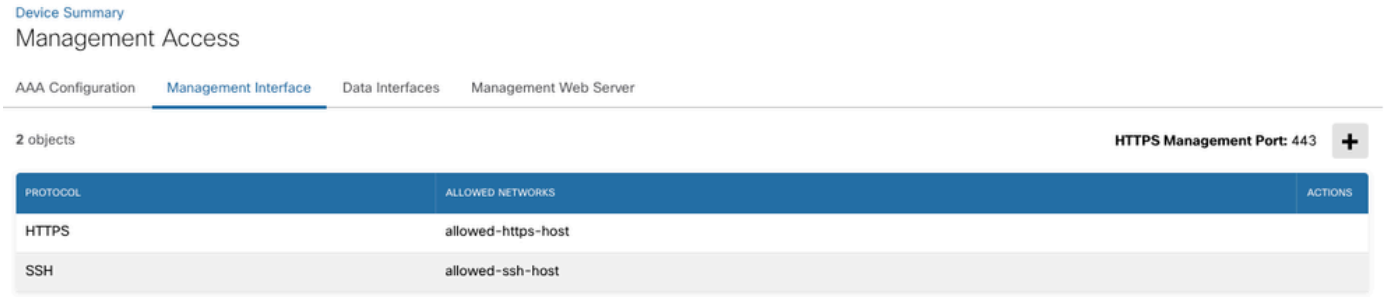


L'accès à la gestion HTTPS a changé et any-ipv4 est supprimé.



Déploiement sur FDM

Étape 6 (Facultatif) : une fois les modifications apportées précédemment pour HTTPS vérifiées, répétez la même procédure pour SSH.



Objet réseau ajouté pour SSH et HTTPS.

Étape 7 : Enfin, déployez les modifications et vérifiez votre accès au FTD à partir du réseau et de l'hôte autorisés.

Étapes CLISH :

Les étapes CLI peuvent être utilisées en cas de gestion FDM ou FMC.

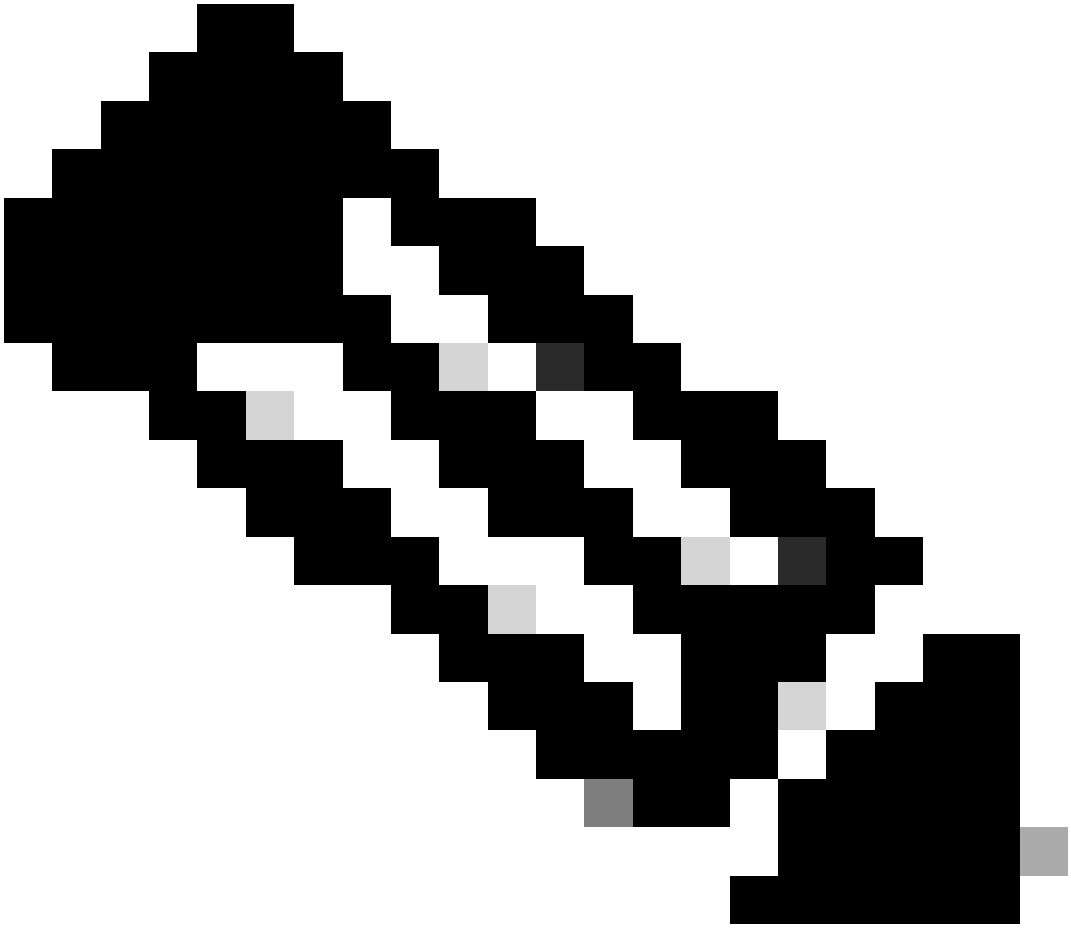
Pour configurer le périphérique afin qu'il accepte les connexions HTTPS ou SSH à partir d'adresses IP ou d'un réseau spécifié, utilisezconfigure https-access-listconfigure ssh-access-listla commande theorcommand.

- 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, votre modification est remplacée lors du prochain déploiement des mises à jour de configuration par l'unité active. S'il s'agit de l'unité active, la modification est propagée 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
```



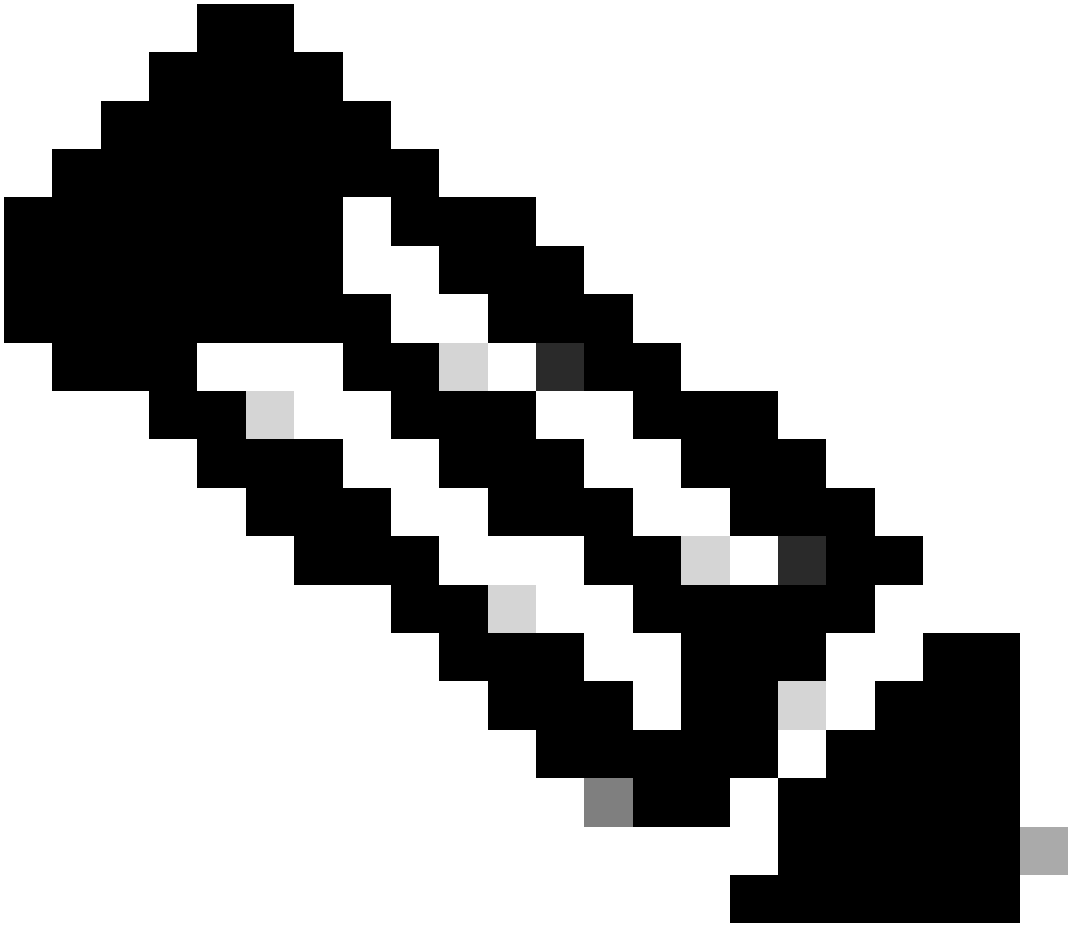
Remarque : x.x.x.x/x et y.y.y.y/y représente une adresse ipv4 avec la notation CIDR.

De même, pour les connexions SSH, utilisez la`configure ssh-access-list`commande avec une ou plusieurs commandes séparées.

```
> 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 utiliser des commandes **configure disable-https-access** ouconfigure disable-ssh-accesspour 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.

Vérifier

Pour vérifier à partir de CLISH, vous pouvez utiliser 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
```

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.