Configurer l'accès de gestion à FTD (HTTPS et SSH) via FMC

Contenu

Introduction

Ce document décrit la configuration de l'accès de gestion à un pare-feu FTD (Firepower Threat Defense) (HTTPS et SSH) via Firesight Management Center (FMC).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de la technologie Firepower
- Connaissances de base sur ASA (Adaptive Security Appliance)
- Connaissance de l'accès à la gestion sur ASA via HTTPS et SSH (Secure Shell)

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Adaptive Security Appliance (ASA) Firepower Threat Defense Image for ASA (5506X/5506H-

X/5506W-X, ASA 5508-X, ASA 5516-X), qui fonctionne sur les versions 6.0.1 et ultérieures du logiciel.
- Image ASA Firepower Threat Defense pour ASA (5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X), qui s'exécute sur les versions 6.0.1 et ultérieures du logiciel.
- Firepower Management Center (FMC) version 6.0.1 et ultérieure.

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.

Informations générales

Avec le début de Firepower Threat Defense (FTD), l'intégralité de la configuration associée à ASA est effectuée sur l'interface utilisateur graphique.

Sur les périphériques FTD qui exécutent le logiciel version 6.0.1, l'interface CLI de diagnostic ASA est accessible lorsque vous entrez dans le **support du système diagnostic-cli**. Cependant, sur les périphériques FTD qui exécutent le logiciel version 6.1.0, la CLI est convergée et des commandes ASA entières sont configurées sur le CLISH.

```
Cisco Fire Linux OS v6.0.1 (build 37)
Cisco Firepower Threat Defense for VMWare v6.0.1 (build 1213)

>                                                    CLISH
> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower> en
Password:
firepower#                                           DIAGNOSTIC CLI
```

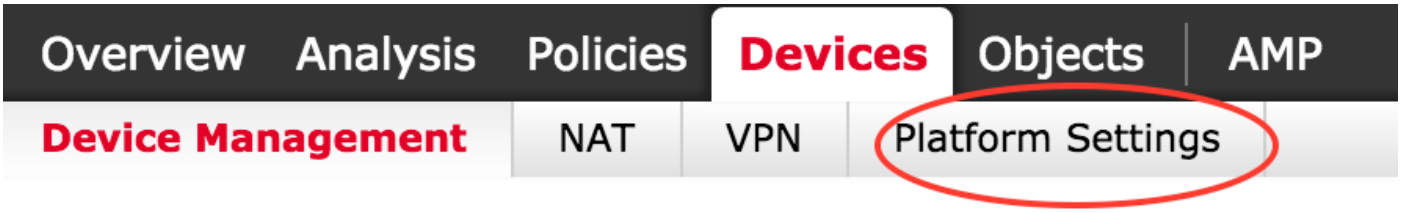
Pour obtenir un accès de gestion directement à partir d'un réseau externe, vous devez configurer l'accès de gestion via HTTPS ou SSH. Ce document fournit la configuration nécessaire pour obtenir un accès de gestion via SSH ou HTTPS en externe.

> **Note**: Sur les périphériques FTD qui exécutent la version 6.0.1 du logiciel, l'interface de ligne de commande n'est pas accessible par un utilisateur local, une authentification externe doit être configurée pour authentifier les utilisateurs. Cependant, sur les périphériques FTD qui exécutent la version 6.1.0 du logiciel, l'interface de ligne de commande est accessible par l'utilisateur **administrateur** local alors qu'une authentification externe est requise pour tous les autres utilisateurs.

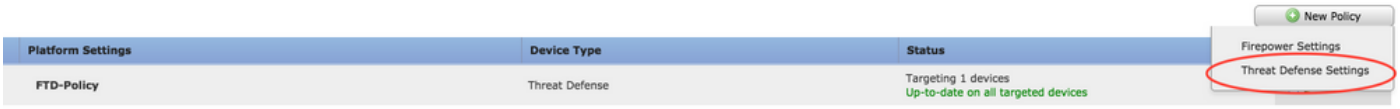
> **Note**: Sur les périphériques FTD qui exécutent la version 6.0.1 du logiciel, l'interface de ligne de commande de diagnostic n'est pas directement accessible sur l'adresse IP configurée pour **br1** du FTD. Cependant, sur les périphériques FTD qui exécutent le logiciel version 6.1.0, l'interface de ligne de commande convergée est accessible sur toute interface configurée pour l'accès à la gestion, mais l'interface doit être configurée avec une adresse IP.

Configuration

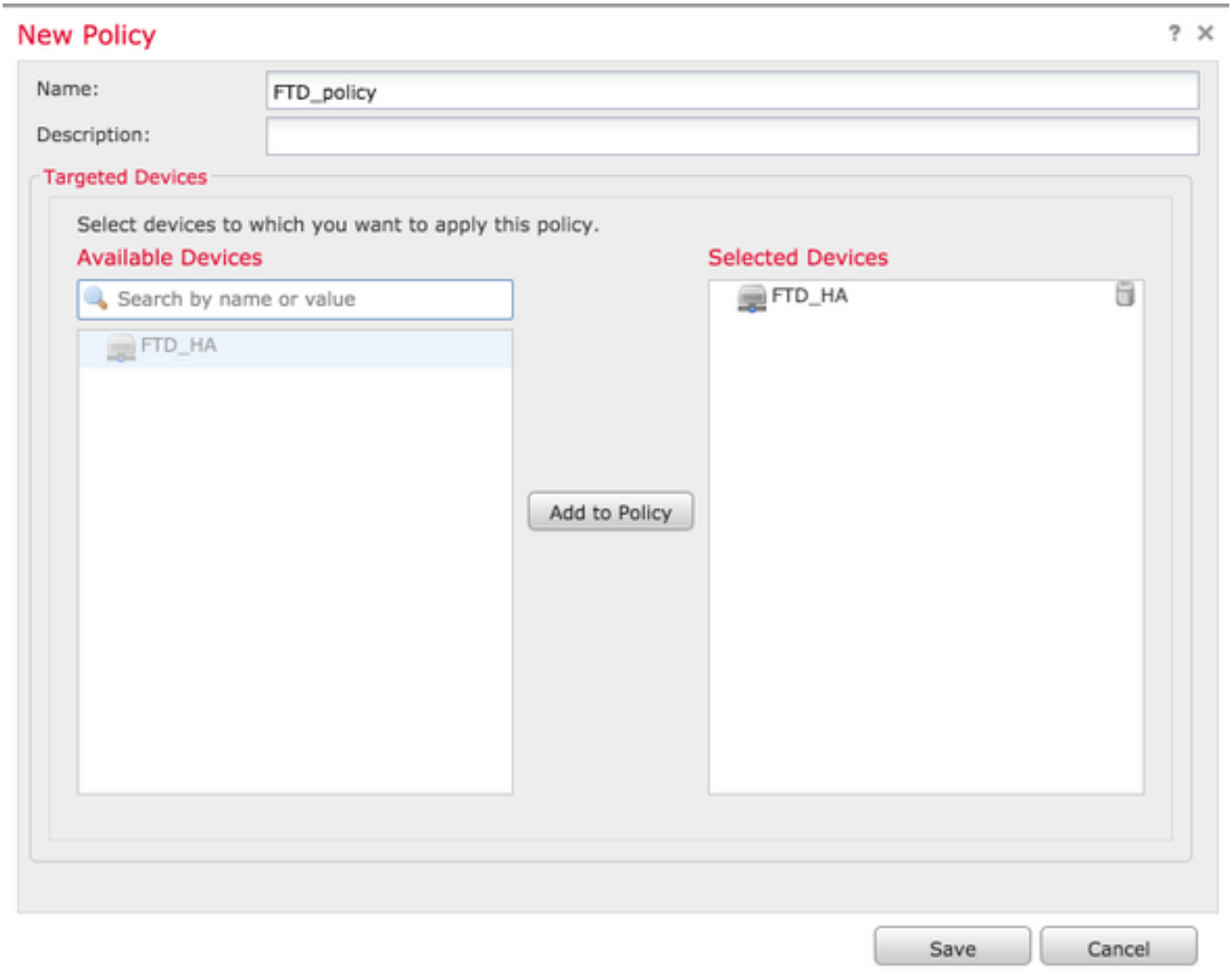
Toute la configuration associée à Management Access est configurée lorsque vous accédez à l'onglet **Platform Settings** dans **Devices**, comme illustré dans l'image :



Modifiez la stratégie qui existe lorsque vous cliquez sur l'icône représentant un crayon ou créez une nouvelle stratégie FTD lorsque vous cliquez sur le bouton **Nouvelle stratégie** et sélectionnez le type **Threat Defense Settings**, comme illustré dans l'image :



Sélectionnez l'appliance FTD pour appliquer cette stratégie et cliquez sur **Enregistrer**, comme illustré dans l'image :



Configurer l'accès à la gestion

Voici les quatre principales étapes de configuration de Management Access.

Étape 1. Configurez IP sur l'interface FTD via l'interface graphique FMC.

Configurez une adresse IP sur l'interface sur laquelle le FTD est accessible via SSH ou HTTPS. Modifiez les interfaces qui existent lorsque vous accédez à l'onglet **Interfaces** du FTD.

> **Note**: Sur les périphériques FTD qui exécutent le logiciel version 6.0.1, l'interface de gestion par défaut sur le FTD est l'interface diagnostic0/0. Cependant, sur les périphériques FTD qui exécutent le logiciel version 6.1.0, toutes les interfaces prennent en charge l'accès de gestion, à l'exception de l'interface de diagnostic.

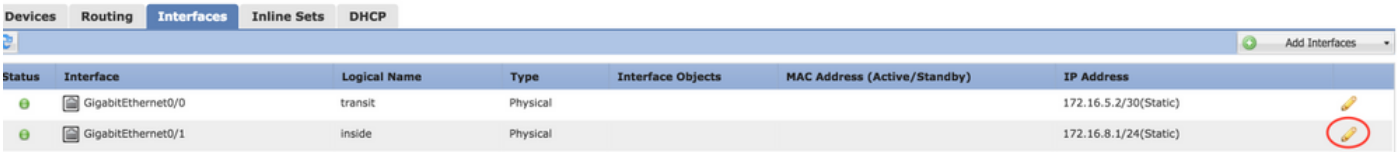
Il existe six étapes pour configurer l'interface de diagnostic.

Étape 1. Accéder à **Device > Device Management.**

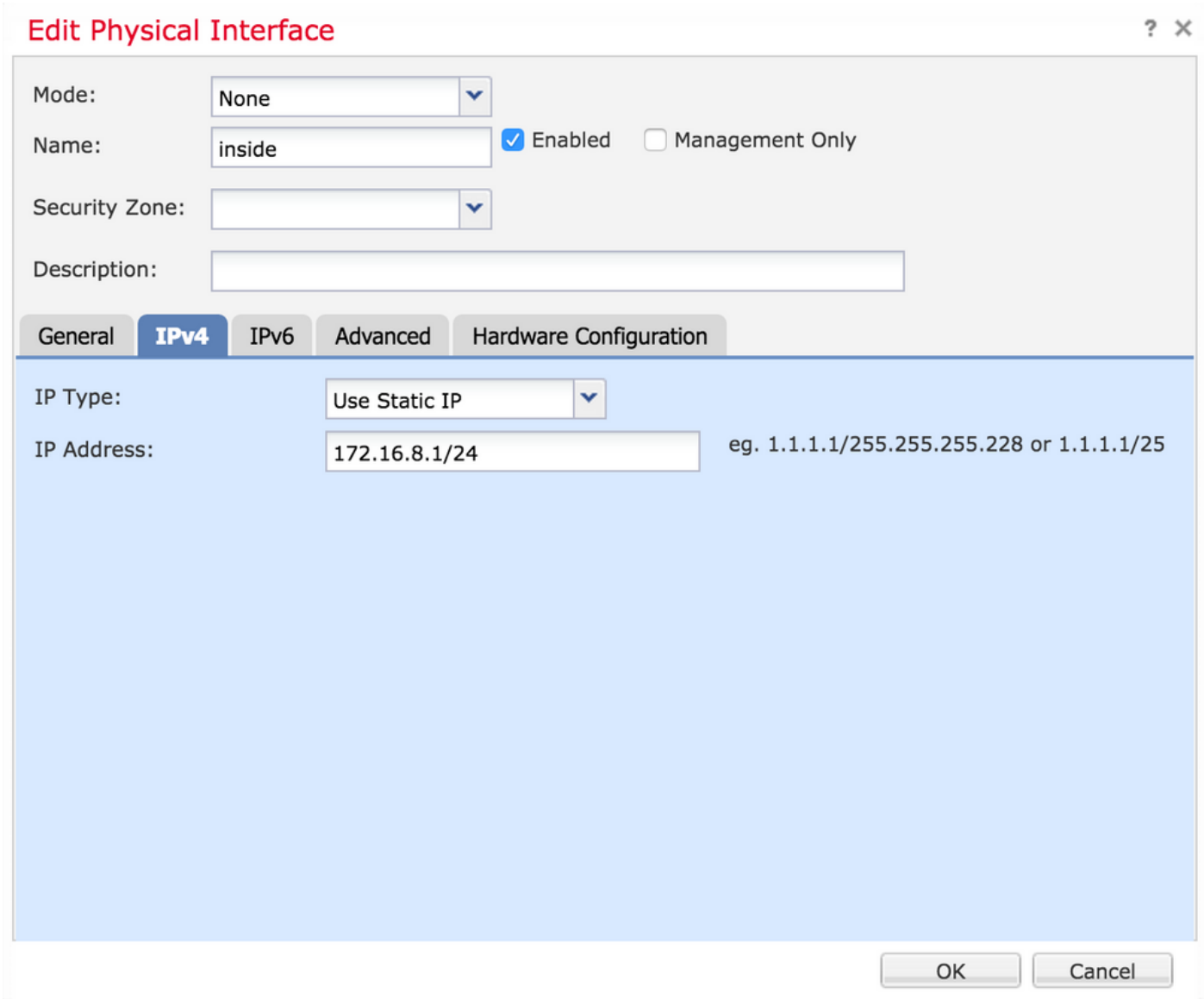
Étape 2. Sélectionnez le périphérique ou le cluster FTD HA.

Étape 3. Accédez à l'onglet **Interfaces**.

Étape 4. Cliquez sur l'**icône représentant un crayon** pour configurer/modifier l'interface afin d'obtenir l'accès à la gestion, comme illustré dans l'image :



Étape 5. Cochez la case **enable** pour activer les interfaces. Accédez à l'onglet **Ipv4**, sélectionnez le type IP comme **statique ou DHCP**. Entrez maintenant une adresse IP pour l'interface et cliquez sur **OK**, comme illustré dans l'image :



Étape 6. Cliquez sur **Enregistrer**, puis déployez la stratégie sur le FTD.

Remarque : l'interface de diagnostic ne peut pas être utilisée pour accéder à l'interface de

ligne de commande convergée via SSH sur les périphériques dotés de la version 6.1.0 du logiciel.

Étape 2. Configurez l'authentification externe.

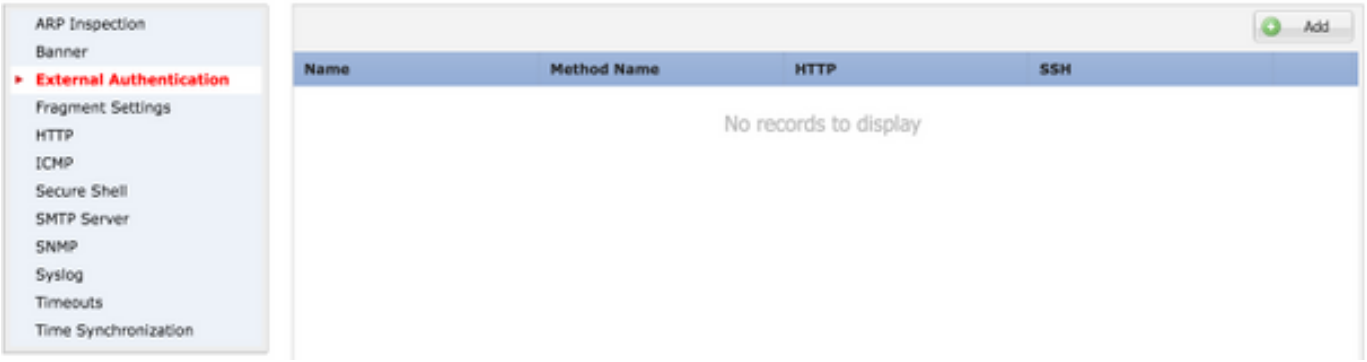
L'authentification externe facilite l'intégration du FTD à un serveur Active Directory ou RADIUS pour l'authentification des utilisateurs. Cette étape est nécessaire car les utilisateurs configurés localement n'ont pas d'accès direct à la CLI de diagnostic. L'interface CLI de diagnostic et l'interface utilisateur graphique sont accessibles uniquement par les utilisateurs authentifiés via LDAP (Lightweight Directory Access Protocol) ou RADIUS.

Il existe 6 étapes pour configurer l'authentification externe.

Étape 1. Accéder à **Périphériques > Paramètres de la plate-forme.**

Étape 2. Modifiez la stratégie qui existe lorsque vous cliquez sur l'icône de crayon ou créez une nouvelle stratégie FTD lorsque vous cliquez sur le bouton **Nouvelle stratégie** et sélectionnez le type comme **Paramètres de protection contre les menaces.**

Étape 3. Accédez à l'onglet **Authentification externe**, comme illustré dans l'image :



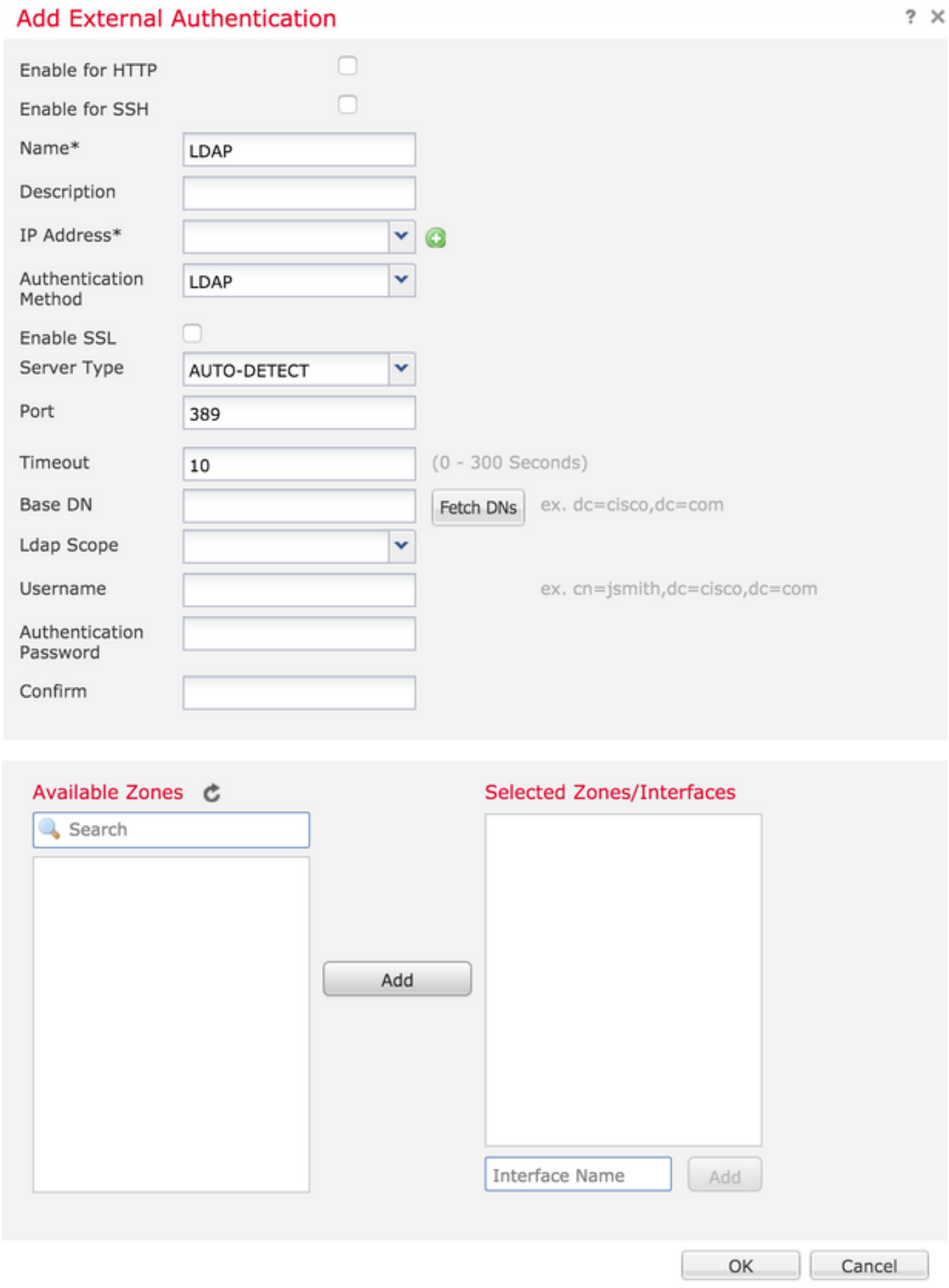
Étape 4. Lorsque vous cliquez sur **Ajouter**, une boîte de dialogue s'affiche comme illustré dans l'image :

- **Enable for HTTP** - Activez cette option pour fournir l'accès FTD sur HTTPS.
- **Enable for SSH** - Activez cette option pour fournir l'accès au FTD sur SSH.
- **Name** - Entrez le nom de la connexion LDAP.
- **Description** - Entrez une description facultative pour l'objet Authentification externe.
- **Adresse IP** - Entrez un objet réseau qui stocke l'adresse IP du serveur d'authentification externe. Si aucun objet réseau n'est configuré, créez-en un nouveau. Cliquez sur l'icône **(+)**.
- **Authentication Method** - Sélectionnez le protocole RADIUS ou LDAP pour l'authentification.

- **Enable SSL** - Activez cette option pour chiffrer le trafic d'authentification.
- **Type de serveur** - Sélectionnez le type de serveur. Les types de serveurs connus sont MS Active Directory, Sun, OpenLDAP et Novell. Par défaut, l'option est définie pour détecter automatiquement le type de serveur.
- **Port** - Entrez le port sur lequel l'authentification a lieu.
- **Timeout** - Entrez une valeur de délai d'attente pour les demandes d'authentification.
- **DN de base** - Entrez un DN de base pour fournir une étendue dans laquelle l'utilisateur peut être présent.
- **Étendue LDAP** - Sélectionnez l'étendue LDAP à rechercher. L'étendue se trouve dans le même niveau ou à regarder dans la sous-arborescence.
- **Username** - Entrez un nom d'utilisateur à lier au répertoire LDAP.
- **Authentication password** : saisissez le mot de passe de cet utilisateur.
- **Confirmer** - Entrez à nouveau le mot de passe.
- **Interfaces disponibles** - Une liste des interfaces disponibles sur le FTD s'affiche.
- **Zones et interfaces sélectionnées** - Affiche la liste des interfaces à partir desquelles le serveur d'authentification est accessible.

Pour l'authentification RADIUS, il n'existe pas de DN de base ou d'étendue LDAP de type serveur. Le port est le port RADIUS 1645.

Secret - Entrez la clé secrète de RADIUS.



Étape 5. Une fois la configuration terminée, cliquez sur **OK.**

Étape 6. Enregistrez la stratégie et déployez-la sur le périphérique Firepower Threat Defense.

Remarque : l'authentification externe ne peut pas être utilisée pour accéder à l'interface de ligne de commande convergée via SSH sur les périphériques dotés de la version 6.1.0 du logiciel

Étape 3. Configurez l'accès SSH.

SSH fournit un accès direct à la CLI convergente. Utilisez cette option pour accéder directement à la CLI et exécuter les commandes debug.Cette section décrit comment configurer SSH afin d'accéder à la CLI FTD.

Note: Sur les périphériques FTD qui exécutent le logiciel version 6.0.1, la configuration SSH sur les paramètres de la plate-forme fournit un accès direct à l'interface CLI de diagnostic et non à l'interface CLISH. Vous devez vous connecter à l'adresse IP configurée sur **br1** pour accéder au CLISH. Cependant, sur les périphériques FTD qui exécutent la version 6.1.0 du logiciel, toutes les interfaces naviguent vers l'interface de ligne de commande convergée lorsqu'elles sont accessibles via SSH

Il y a 6 étapes pour configurer SSH sur l'ASA

Sur les périphériques 6.0.1 uniquement :

Ces étapes sont effectuées sur les périphériques FTD dont la version logicielle est inférieure à 6.1.0 et supérieure à 6.0.1. Sur les périphériques 6.1.0, ces paramètres sont hérités du système d'exploitation.

Étape 1. Accédez à **Périphériques>Paramètres de la plate-forme.**

Étape 2. Modifiez la stratégie qui existe lorsque vous cliquez sur l'icône représentant un crayon ou créez une nouvelle stratégie de défense contre les menaces Firepower lorsque vous cliquez sur le bouton **Nouvelle stratégie** et sélectionnez le type **Paramètres de défense contre les menaces.**

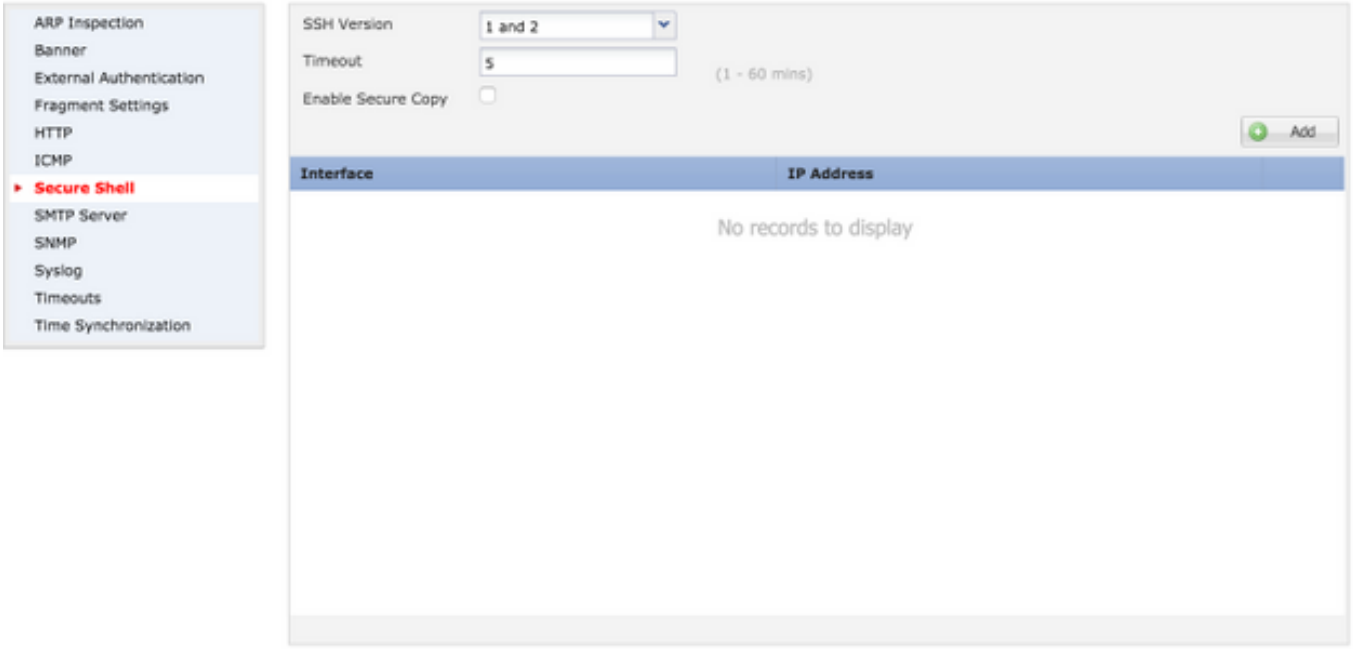
Étape 3. Accédez à la section **Secure Shell**. Une page s'affiche, comme le montre l'image :

Version SSH : Sélectionnez la version SSH à activer sur l'ASA. Il existe trois options :

- **1:** Activer uniquement SSH version 1
- **2:** Activer uniquement SSH version 2
- **1 et 2 :** Activer les versions 1 et 2 de SSH

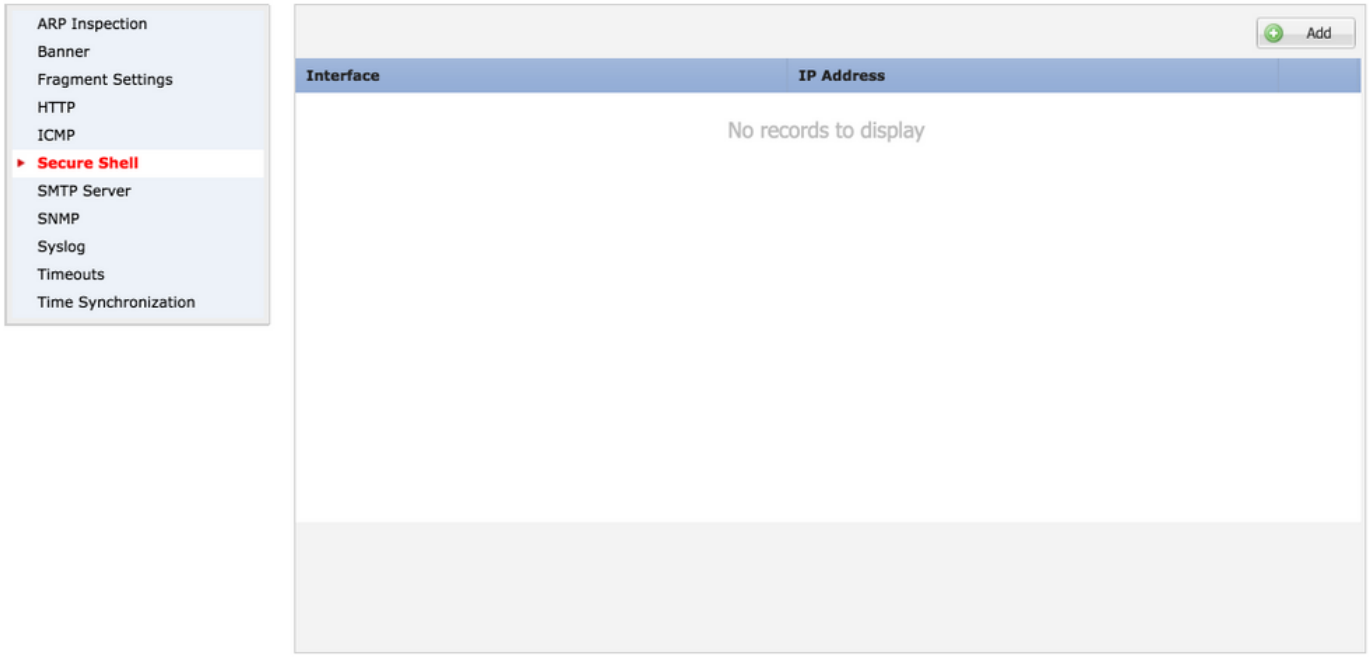
timeout : Saisissez le délai d'attente SSH souhaité en minutes.

Enable Secure Copy - Activez cette option pour configurer le périphérique afin qu'il autorise les connexions Secure Copy (SCP) et agisse en tant que serveur SCP.



Sur les périphériques 6.0.1 et 6.1.0 :

Ces étapes sont configurées pour limiter l'accès de gestion via SSH à des interfaces spécifiques et à des adresses IP spécifiques.

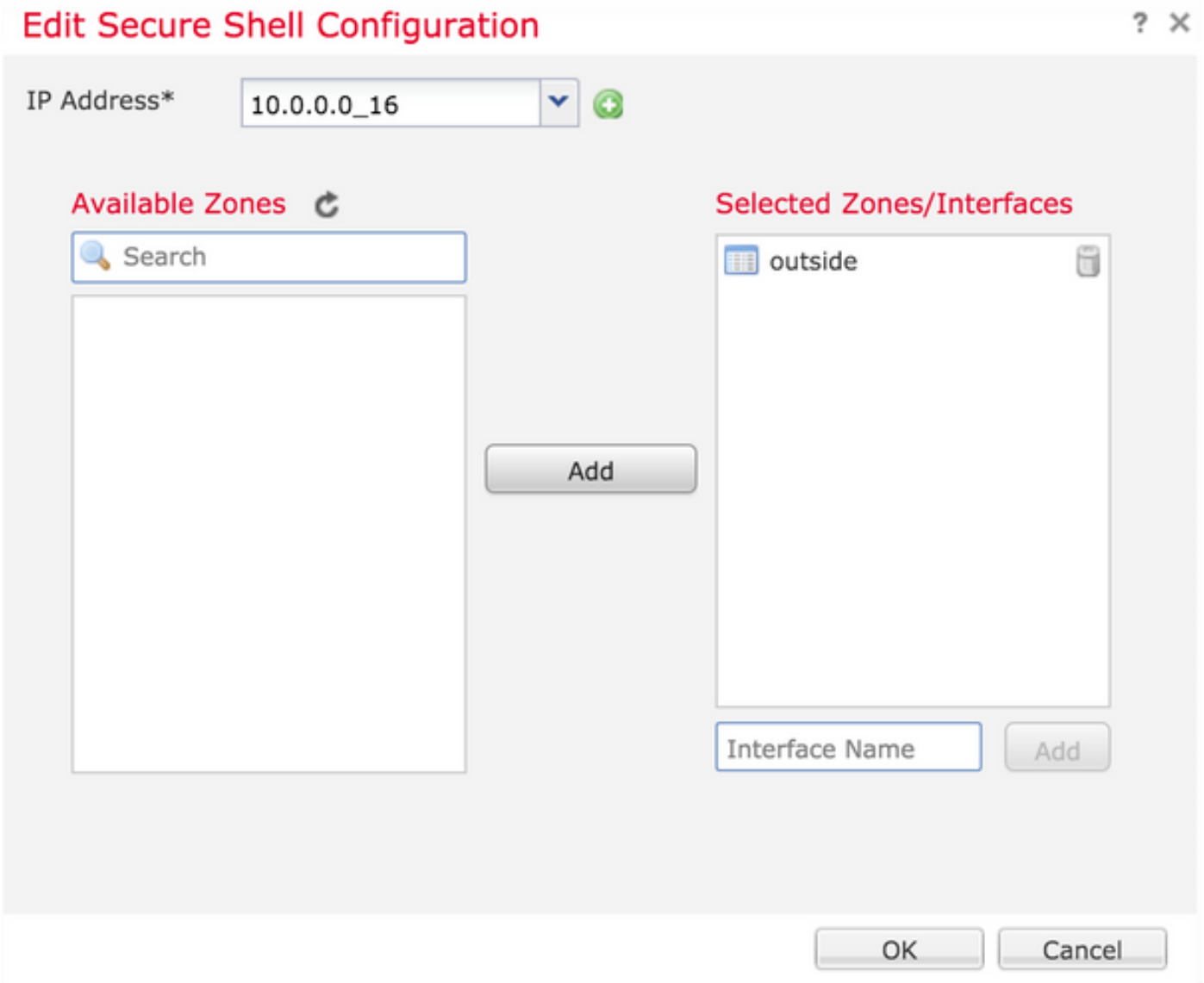


Étape 1. Cliquez sur **Ajouter** et configurez les options suivantes :

Adresse IP : Sélectionnez un objet réseau qui contient les sous-réseaux autorisés à accéder à l'interface de ligne de commande via SSH. Si aucun objet réseau n'est présent, créez-en un lorsque vous cliquez sur l'icône **(+)**.

Zones/interfaces sélectionnées : Sélectionnez les zones ou les interfaces à partir desquelles le serveur SSH est accessible.

Étape 2. Cliquez sur **OK**, comme illustré dans l'image :



La configuration de SSH est affichée dans l'interface de ligne de commande convergée (CLI de diagnostic ASA dans les périphériques 6.0.1) à l'aide de cette commande.

```
> show running-config ssh
ssh 172.16.8.0 255.255.255.0 inside
```

Étape 3. Une fois la configuration SSH terminée, cliquez sur **Enregistrer**, puis déployez la stratégie sur le FTD.

Étape 4. Configurez l'accès HTTPS.

Afin d'activer l'accès HTTPS à une ou plusieurs interfaces, accédez à la section **HTTP** dans les paramètres de la plate-forme. L'accès HTTPS est particulièrement utile pour télécharger les captures de paquets à partir de l'interface Web sécurisée de diagnostic directement pour l'analyse.

Il existe 6 étapes pour configurer l'accès HTTPS.

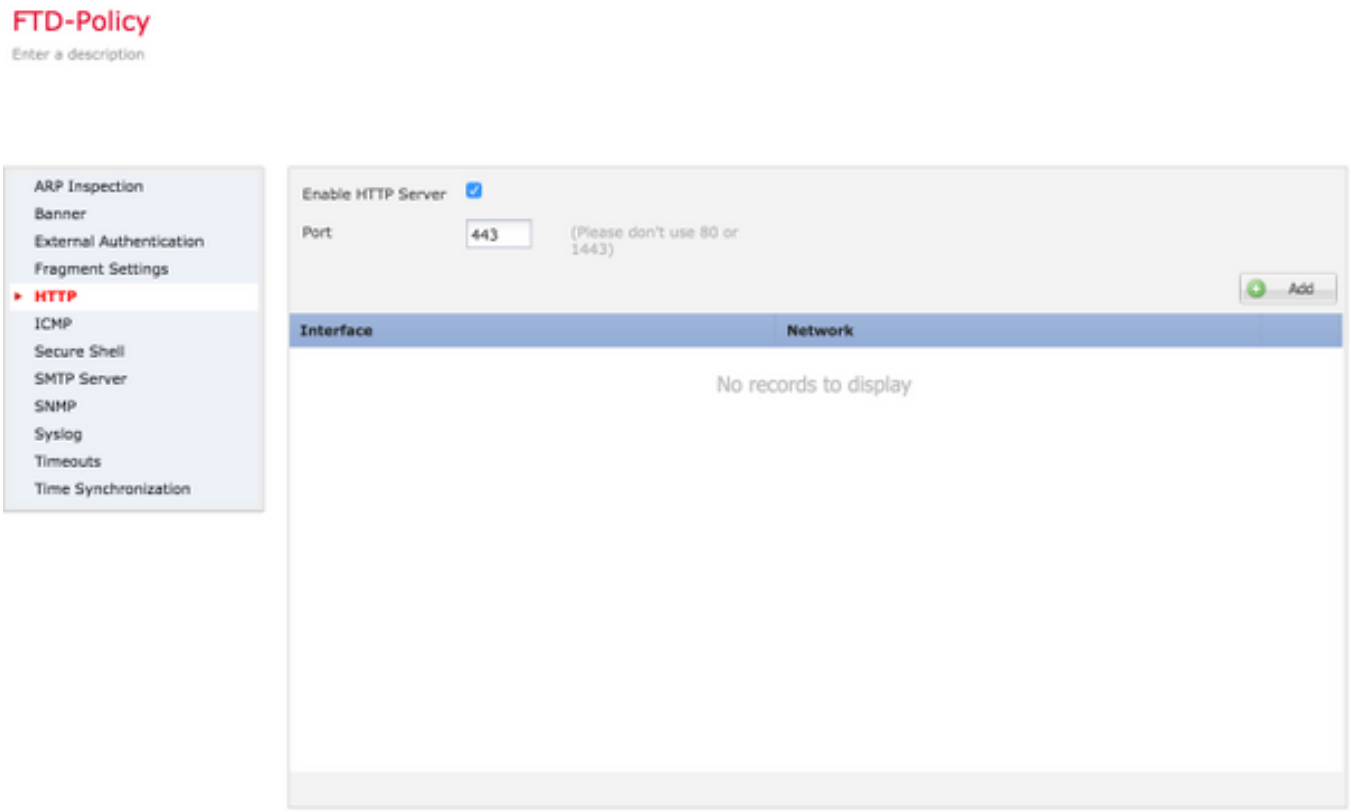
Étape 1. Naviguez jusqu'à **Devices > Platform Settings**

Étape 2. Modifiez la stratégie de paramètres de plateforme qui existe lorsque vous cliquez sur l'**icône de crayon** en regard de la stratégie ou créez une nouvelle stratégie FTD lorsque vous cliquez sur **Nouvelle stratégie**. Sélectionnez le type **Firepower Threat Defense.**

Étape 3. Lorsque vous accédez à la section **HTTP**, une page s'affiche comme indiqué dans l'image.

Activer le serveur HTTP : Activez cette option pour activer le serveur HTTP sur le FTD.

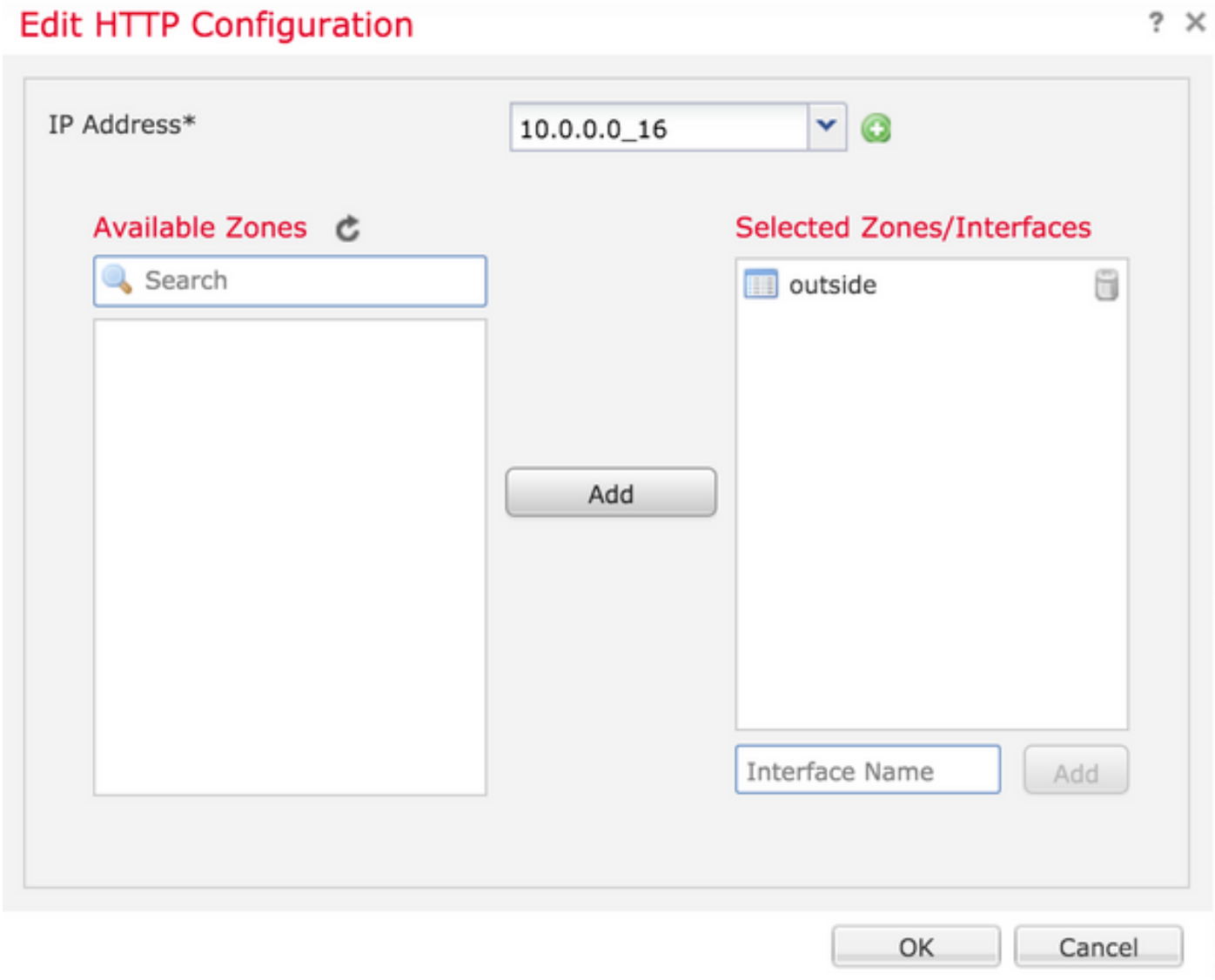
Port : sélectionnez le port sur lequel le FTD accepte les connexions de gestion.



Étape 4.Cliquez sur **Ajouter** et sur la page comme indiqué dans l'image :

Adresse IP - Entrez les sous-réseaux autorisés à avoir accès HTTPS à l'interface de diagnostic. Si aucun objet réseau n'est présent, créez-en un et utilisez l'option **(+)**.

Zones/Interfaces sélectionnées - Comme pour SSH, la configuration HTTPS doit avoir une interface configurée sur laquelle elle est accessible via HTTPS. Sélectionnez les zones ou l'interface sur lesquelles le FTD doit être accessible via HTTPS.



La configuration de HTTPS est affichée dans l'interface de ligne de commande convergée (CLI de diagnostic ASA dans les périphériques 6.0.1) et utilise cette commande.

```
> show running-config http
http 172.16.8.0 255.255.255.0 inside
```

Étape 5. Une fois la configuration requise terminée, sélectionnez **OK.**

Étape 6. Une fois toutes les informations requises entrées, cliquez sur **Enregistrer**, puis déployez la stratégie sur le périphérique.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Voici les étapes de base pour résoudre le problème d'accès à la gestion sur le FTD.

Étape 1. Assurez-vous que l'interface est activée et configurée avec une adresse IP.

Étape 2. Assurez-vous qu'une authentification externe fonctionne comme configurée et qu'elle est accessible à partir de l'interface appropriée spécifiée dans la section **Authentification externe** de la **plateforme Settings**.

Étape 3. Assurez-vous que le routage sur le FTD est précis. Dans le logiciel FTD version 6.0.1, accédez à **system support diagnostic-cli.** Exécutez les commandes **show route** et **show route management-only** pour voir les routes pour FTD et les interfaces de gestion respectivement.

Dans le logiciel FTD version 6.1.0, exécutez les commandes directement dans l'interface de ligne de commande convergée.

Informations connexes

- Support et documentation techniques - Cisco Systems