Configuration de l'accès de Gestion à FTD (HTTPS et SSH) par l'intermédiaire de FMC

Contenu

Introduction

Ce document décrit la configuration de l'accès de Gestion à une défense contre des menaces de FirePOWER (FTD) (HTTPS et SSH) par l'intermédiaire du centre de Gestion de FireSIGHT (FMC).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La connaissance de la technologie de FirePOWER
- Connaissance de base d'ASA (appliance de sécurité adaptable)
- La connaissance de la Gestion Access sur l'ASA par l'intermédiaire de HTTPS et SSH (sécurisez le shell)

Composants utilisés

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

- Image de défense contre des menaces de FirePOWER de l'appliance de sécurité adaptable (ASA) pour ASA (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X), qui fonctionne sur la version de logiciel 6.0.1 et en haut
- Image de défense contre des menaces ASA FirePOWER pour ASA (5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X), qui fonctionne sur la version de logiciel 6.0.1 et en haut
- Version 6.0.1 et ultérieures du centre de Gestion de FirePOWER (FMC)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Avec le début de la défense contre des menaces de FirePOWER (FTD), la configuration associée par ASA entière est faite sur le GUI.

Sur des périphériques FTD exécutant la version de logiciel 6.0.1, le diagnostic CLI ASA est accédé à pendant que vous écrivez le **support de système diagnostic-cli**. Cependant, sur des périphériques FTD exécutant la version de logiciel 6.1.0, le CLI est convergé et des commandes entières ASA 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
```

Afin de gagner l'accès de Gestion directement d'un réseau externe, vous devez configurer l'accès de Gestion par l'intermédiaire de HTTPS ou de SSH. Ce document fournit la configuration nécessaire exigée pour gagner l'accès de Gestion au-dessus du SSH ou du HTTPS extérieurement.

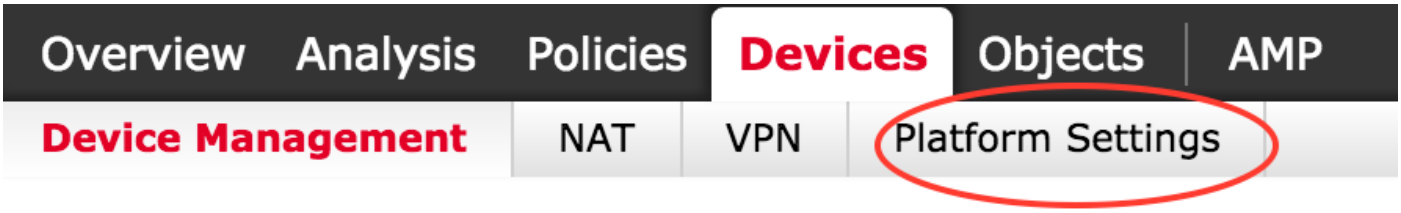
> **Note**: Sur des périphériques FTD exécutant la version de logiciel 6.0.1, le CLI ne peut pas être accédé à par un utilisateur local, une authentification externe doit être configuré afin d'authentifier les utilisateurs. Cependant, sur des périphériques FTD exécutant la version de logiciel 6.1.0, le CLI est accédé à par l'utilisateur local d'**admin** tandis qu'une authentification externe est exigée pour tous autres utilisateurs

> **Note**: Sur des périphériques FTD exécutant la version de logiciel 6.0.1, le diagnostic CLI n'est pas directement accessible au-dessus de l'IP qui est configuré pour **br1 du** FTD. Cependant, sur des périphériques FTD exécutant la version de logiciel 6.1.0, le CLI convergé est accessible au-dessus de n'importe quelle interface configurée pour l'accès de

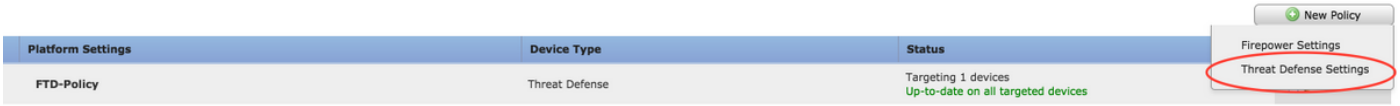
Gestion, cependant, l'interface doit être configurée avec un IP address.

Configurez

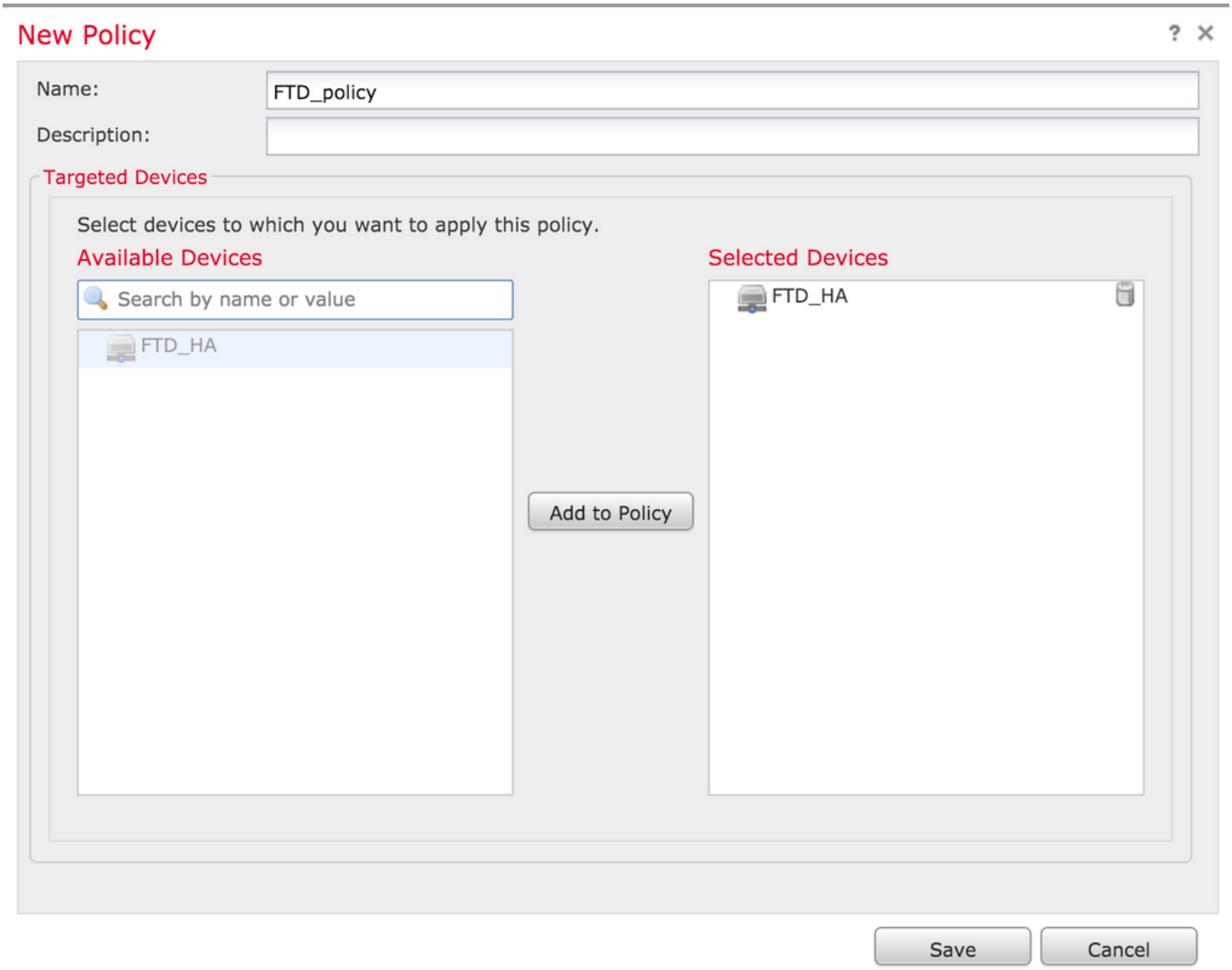
Toute la configuration associée par Access de Gestion est configurée pendant que vous naviguez vers l'**onglet Settings de plate-forme** dans des **périphériques**, suivant les indications de l'image :



L'un ou l'autre édite la stratégie qui existe pendant que vous cliquez sur en fonction l'icône de crayon ou créez une nouvelle stratégie FTD pendant que vous cliquez sur le bouton et le type de sélection de **nouvelle stratégie** comme **configurations de défense contre des menaces**, suivant les indications de l'image :



Sélectionnez l'appliance FTD pour appliquer cette stratégie et pour cliquer sur la **sauvegarde**, suivant les indications de l'image :



Configurez la Gestion Access

Ce sont les quatre étapes principales prises pour configurer la Gestion Access.

Étape 1. Configurez l'IP sur l'interface FTD par l'intermédiaire du GUI FMC.

Configurez un IP sur l'interface au-dessus de laquelle le FTD est accessible par l'intermédiaire du SSH ou du HTTPS. Éditez les interfaces qui existent pendant que vous naviguez vers l'onglet d'**interfaces du** FTD.

> **Note**: Sur des périphériques FTD exécutant la version de logiciel 6.0.1, l'interface de gestion par défaut sur le FTD est l'interface diagnostic0/0. Cependant, sur des périphériques FTD exécutant la version de logiciel 6.1.0, tout l'accès de Gestion de support d'interfaces excepté l'interface diagnostique.

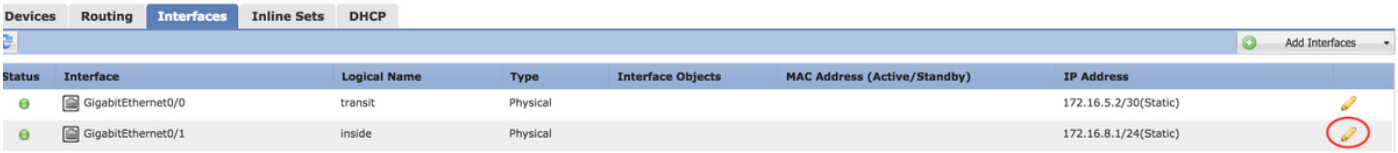
Il y a six étapes pour configurer l'interface diagnostique.

Étape 1. Naviguez vers le **périphérique > la Gestion de périphériques.**

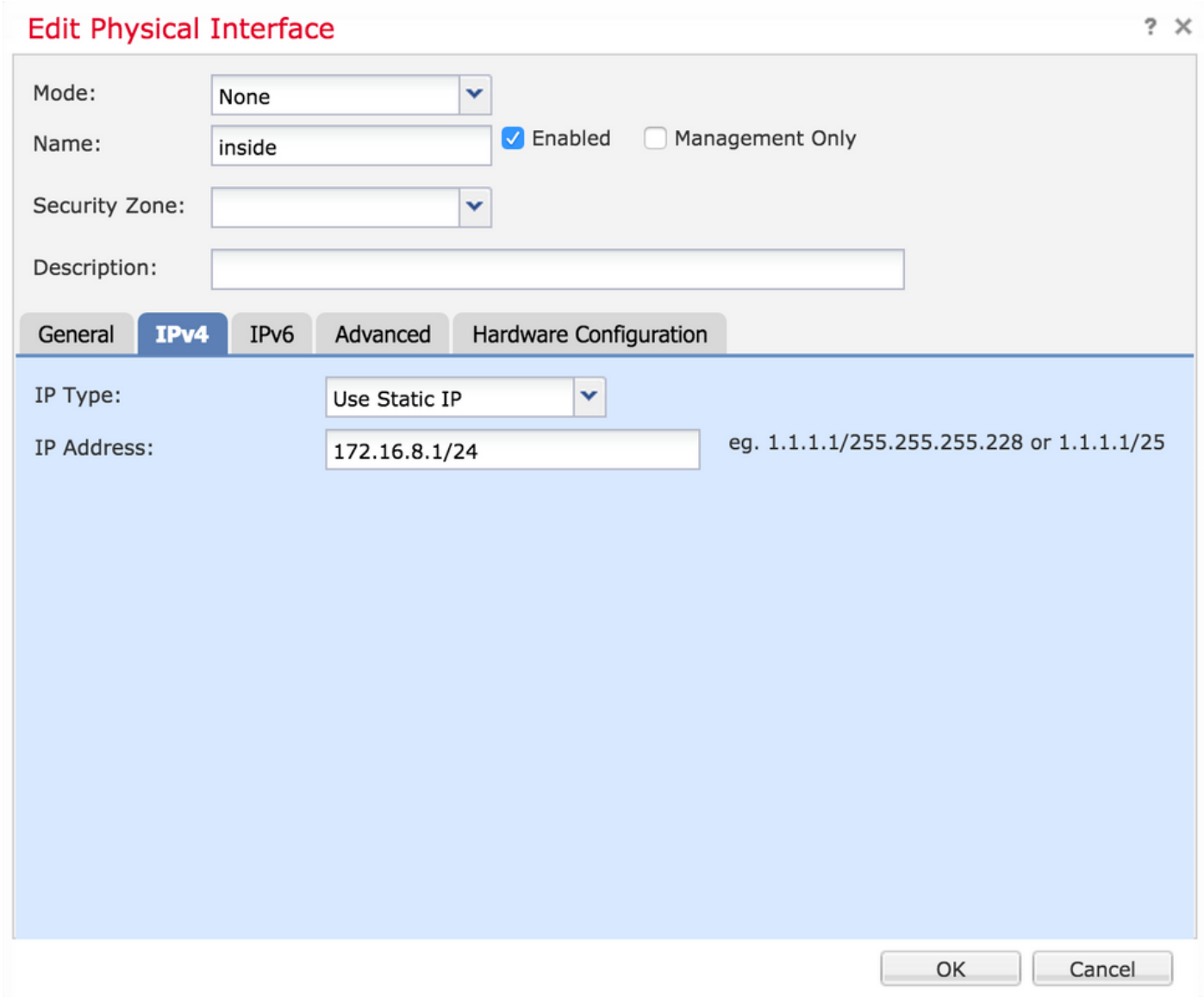
Étape 2. Sélectionnez le périphérique ou la batterie FTD ha.

Étape 3. Naviguez vers l'onglet d'**interfaces**.

Étape 4. Cliquez sur l'**icône de crayon** pour configurer/éditez l'interface pour gagner l'accès de Gestion, suivant les indications de l'image :



Étape 5. Sélectionnez la case à cocher d'**enable** pour activer les interfaces. Naviguez vers l'onglet d'**ipv4**, choisissez le type IP comme **charge statique ou DHCP**. Maintenant écrivez une adresse IP pour l'interface et cliquez sur OK, suivant les indications de l'image :



Étape 6. Cliquez sur la **sauvegarde** et puis déployez la stratégie vers le FTD.

Note: L'interface diagnostique ne peut pas être utilisée pour accéder au CLI convergé au-

dessus du SSH sur des périphériques avec la version de logiciel 6.1.0

Étape 2. Configurez l'authentification externe.

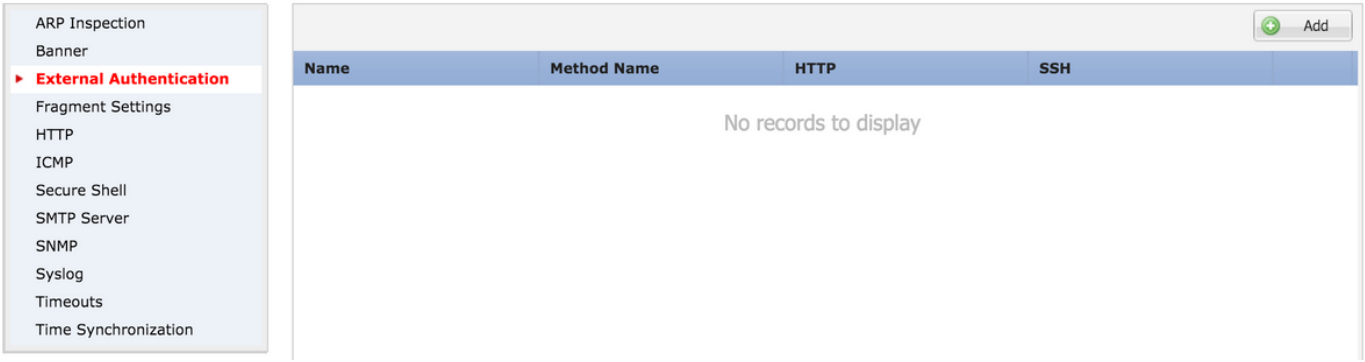
L'authentification externe facilite l'intégration du FTD à un Répertoire actif ou à un serveur de RAYON pour l'authentification de l'utilisateur. C'est une étape nécessaire parce que les utilisateurs localement configurés n'ont pas l'accès direct au diagnostic CLI. Le diagnostic CLI et le GUI sont accédés à seulement par les utilisateurs qui sont authentifiés par l'intermédiaire du Protocole LDAP (Lightweight Directory Access Protocol) ou du RAYON.

Il y a 6 étapes pour configurer l'authentification externe.

Étape 1. Naviguez vers des **périphériques > des configurations de plate-forme.**

Étape 2. L'un ou l'autre édite la stratégie qui existe pendant que vous cliquez sur en fonction l'icône de crayon ou créez une nouvelle stratégie FTD pendant que vous cliquez sur le bouton et le type de sélection de **nouvelle stratégie** comme **configurations de défense contre des menaces.**

Étape 3. Naviguez vers l'onglet d'**authentification externe**, suivant les indications de l'image :



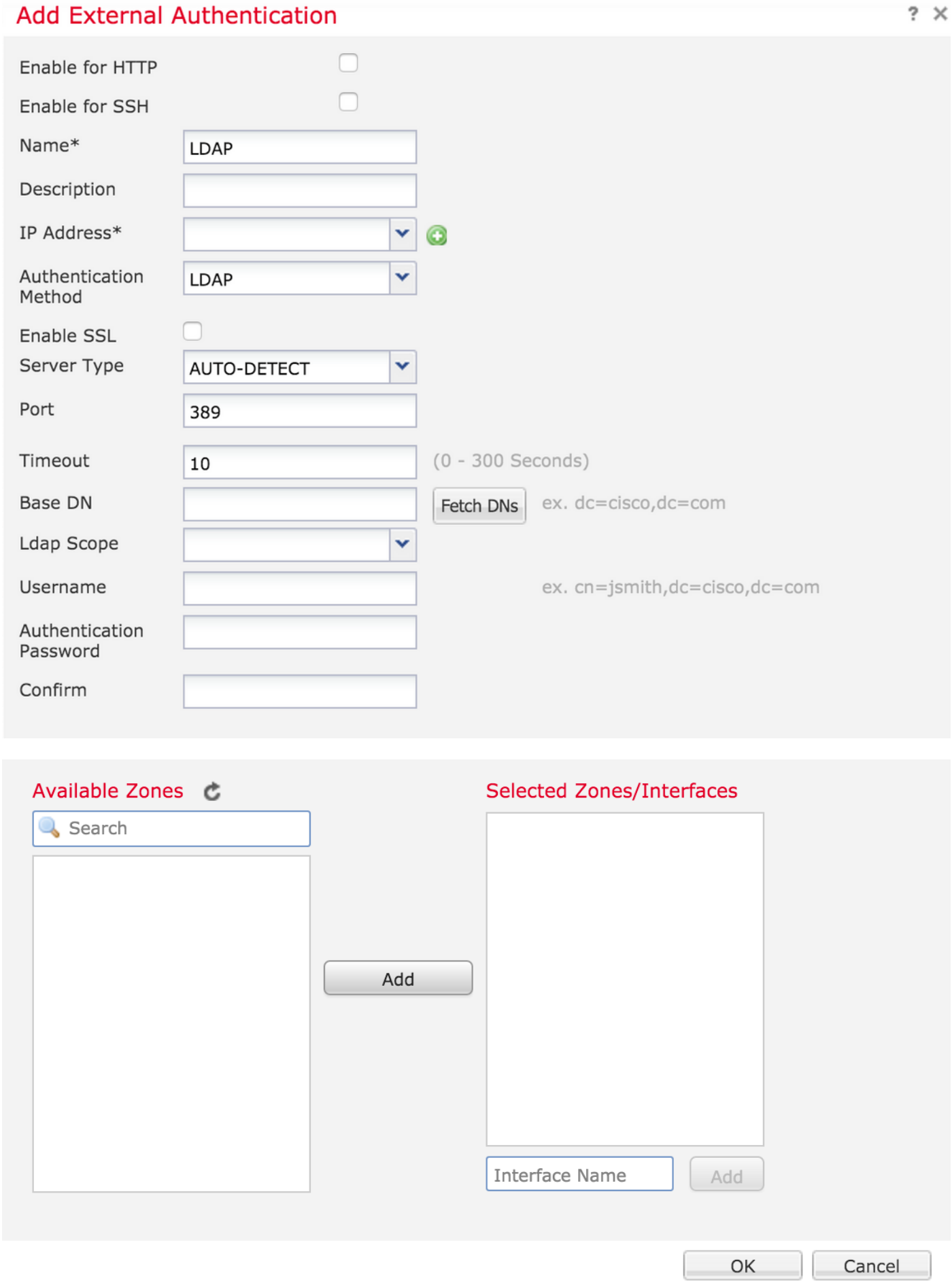
Étape 4. Car vous cliquez sur en fonction **Add**, une zone de dialogue apparaît suivant les indications de l'image :

- **Enable pour l'**enable **HTTP** cette option de fournir l'accès le FTD au-dessus de HTTPS.
- **Enable pour l'**enable **SSH-** cette option de fournir l'accès le FTD au-dessus du SSH.
- **Le nom** écrivent le nom pour la connexion de LDAP.
- **La description** écrivent une description facultative pour l'objet d'authentification externe.
- **L'adresse IP** écrivent un objet de réseau qui enregistre l'IP du serveur d'authentification externe. S'il y a aucun objet de réseau n'est configuré créent un neuf en cliquant sur sur **(+) l'**icône.

- Protocole Méthode-**choisi de** RAYON ou de LDAP d'**authentification** pour l'authentification.
- **SSL-enable d'enable** cette option de chiffrer le trafic d'authentification.
- **Le type de serveur** sélectionnent le type de serveur. Les types de serveur réputés sont Répertoire actif, Sun, OpenLDAP et Novell de MS. Par défaut, l'option est placée automatique-de détecter le type de serveur.
- **Le port** entrent dans le port au-dessus dont l'authentification a lieu.
- **La minuterie** écrivent une valeur du dépassement de durée pour les demandes d'authentification.
- **La base DN** écrivent un DN de base pour fournir une portée dans laquelle l'utilisateur devrait être présent.
- **La portée de LDAP** sélectionnent la portée de LDAP pour regarder. La portée est dans le même niveau ou pour regarder dans le sous-arbre.
- **Username** écrivez un nom d'utilisateur pour lier au répertoire LDAP.
- **L'authentification mot de passe-entrent le** mot de passe pour cet utilisateur.
- **Confirmez la** confirmation le mot de passe.
- **Disponible relie la** liste A d'interfaces disponibles sur le FTD est affiché.
- **Les zones sélectionnées et relie** ceci affiche une liste d'interfaces au-dessus de dont on accède au serveur d'authentification.

Pour l'authentification de RAYON, il n'y a aucune portée de DN ou de LDAP de base de type de serveur. Le port est le port 1645 de RAYON.

Le secret introduisent la clé secrète pour le RAYON.



Étape 5. Une fois que la configuration est faite, cliquez sur OK.

Étape 6. Sauvegardez la stratégie et déployez-la vers le périphérique de défense contre des

menaces de FirePOWER.

> **Note**: L'authentification externe ne peut pas être utilisée pour accéder au CLI convergé au-dessus du SSH sur des périphériques avec la version de logiciel 6.1.0

Étape 3. Configurez le SSH Access.

Le SSH fournit l'accès direct au CLI convergé. Utilisez cette option d'accéder à directement les commandes de débogage CLI et de passage. Cette section décrit comment configurer le SSH afin d'accéder au FTD CLI.

> **Note**: Sur des périphériques FTD exécutant la version de logiciel 6.0.1, la configuration de SSH sur des configurations de plate-forme fournit l'accès au diagnostic CLI directement et pas le CLISH. Vous devez se connecter à l'IP address configuré sur **br1** pour accéder au CLISH. Cependant, sur des périphériques FTD exécutant la version de logiciel 6.1.0, toutes les interfaces naviguent vers le CLI convergé une fois accédées à au-dessus du SSH

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

Sur 6.0.1 périphériques seulement :

Ces étapes sont exécutées sur des périphériques FTD avec la version de logiciel moins de 6.1.0 et plus considérablement que 6.0.1. Sur 6.1.0 périphériques ces paramètres sont hérités du SYSTÈME D'EXPLOITATION.

Étape 1. Naviguez vers des **configurations de Devices>Platform.**

Étape 2. L'un ou l'autre édite la stratégie qui existe pendant que vous cliquez sur en fonction l'icône de crayon ou créez une nouvelle stratégie de défense contre des menaces de FirePOWER pendant que vous cliquez sur le bouton et le type de sélection de **nouvelle stratégie** comme **configurations de défense contre des menaces.**

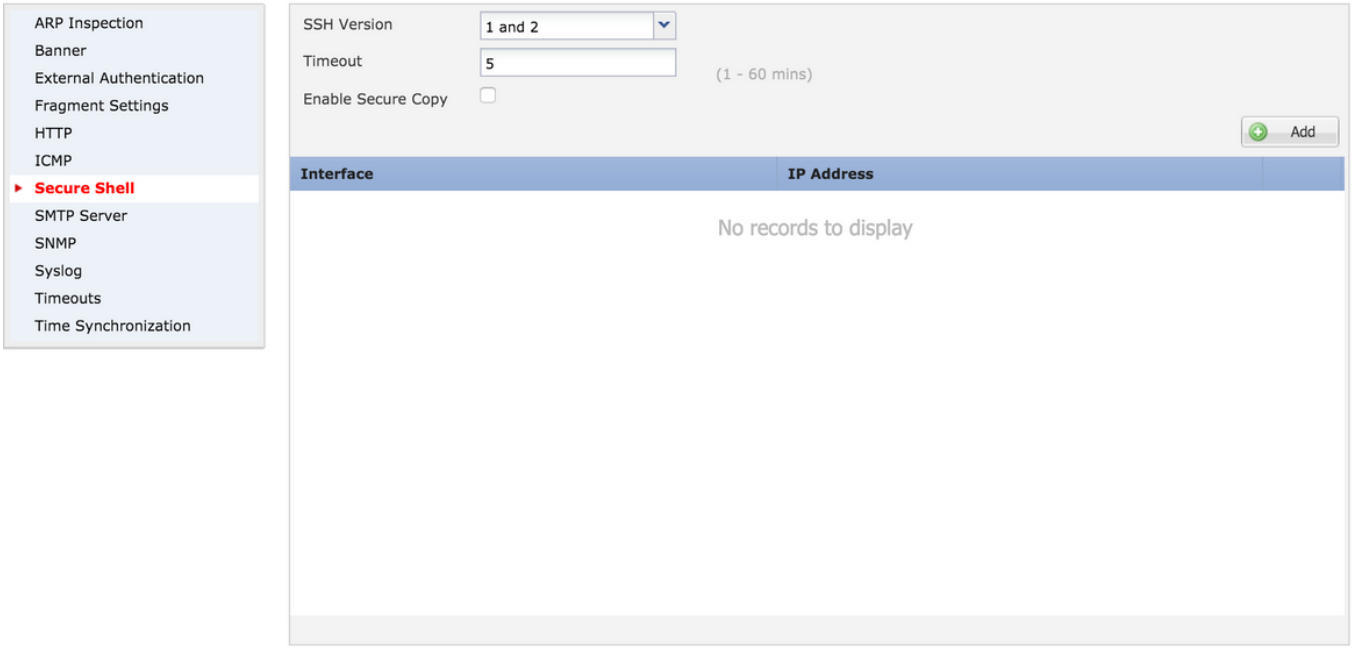
Étape 3. Naviguez vers la section **sécurisée de shell**. Une page paraît, suivant les indications de l'image :

Version SSH : Sélectionnez la version SSH pour activer sur l'ASA. Il y a trois options :

- **1 :** Version SSH 1 d'enable seulement
- **2 :** Version SSH 2 d'enable seulement
- **1 et 2 :** Activez la version SSH 1 et 2

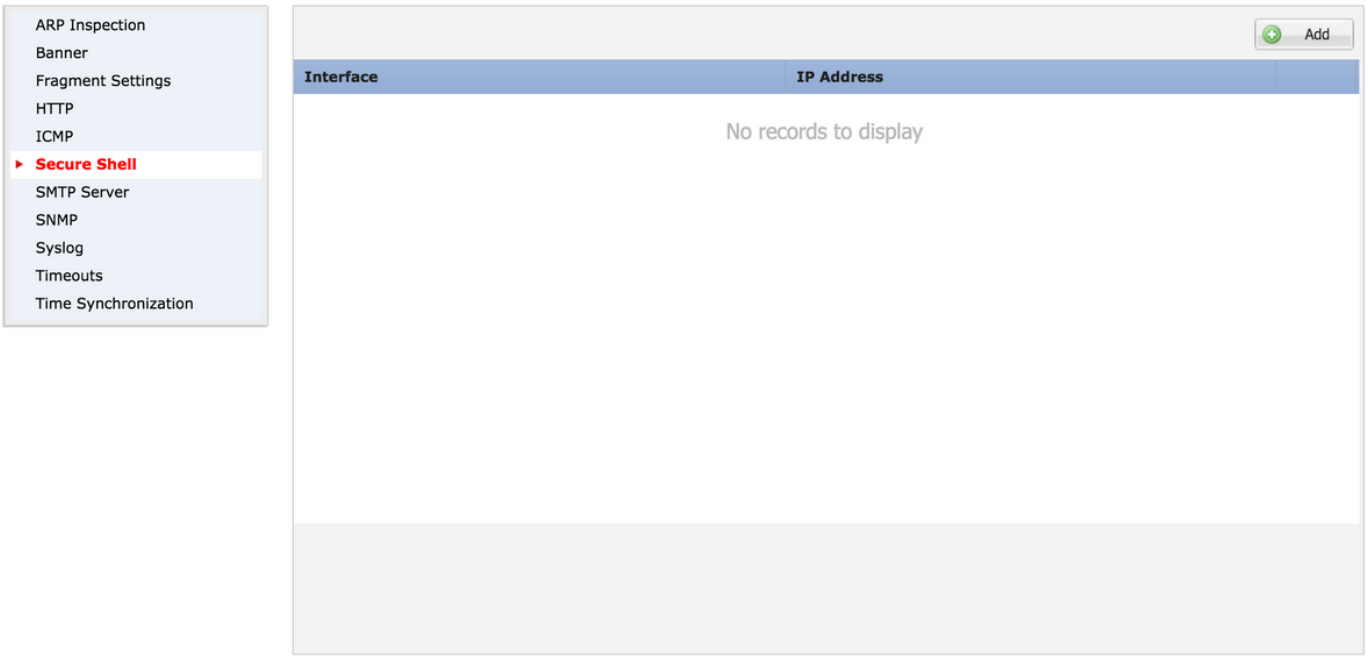
Délai d'attente : Écrivez le ssh timeout désiré en quelques minutes.

Enable **sécurisé de copie d'enable** cette option de configurer le périphérique pour permettre les connexions sécurisées de Copy(SCP) et pour agir en tant que serveur SCP.



Sur 6.0.1 et 6.1.0 périphériques :

Ces étapes sont configurées pour limiter l'accès de Gestion par l'intermédiaire du SSH aux interfaces spécifiques et aux adresses IP spécifiques.

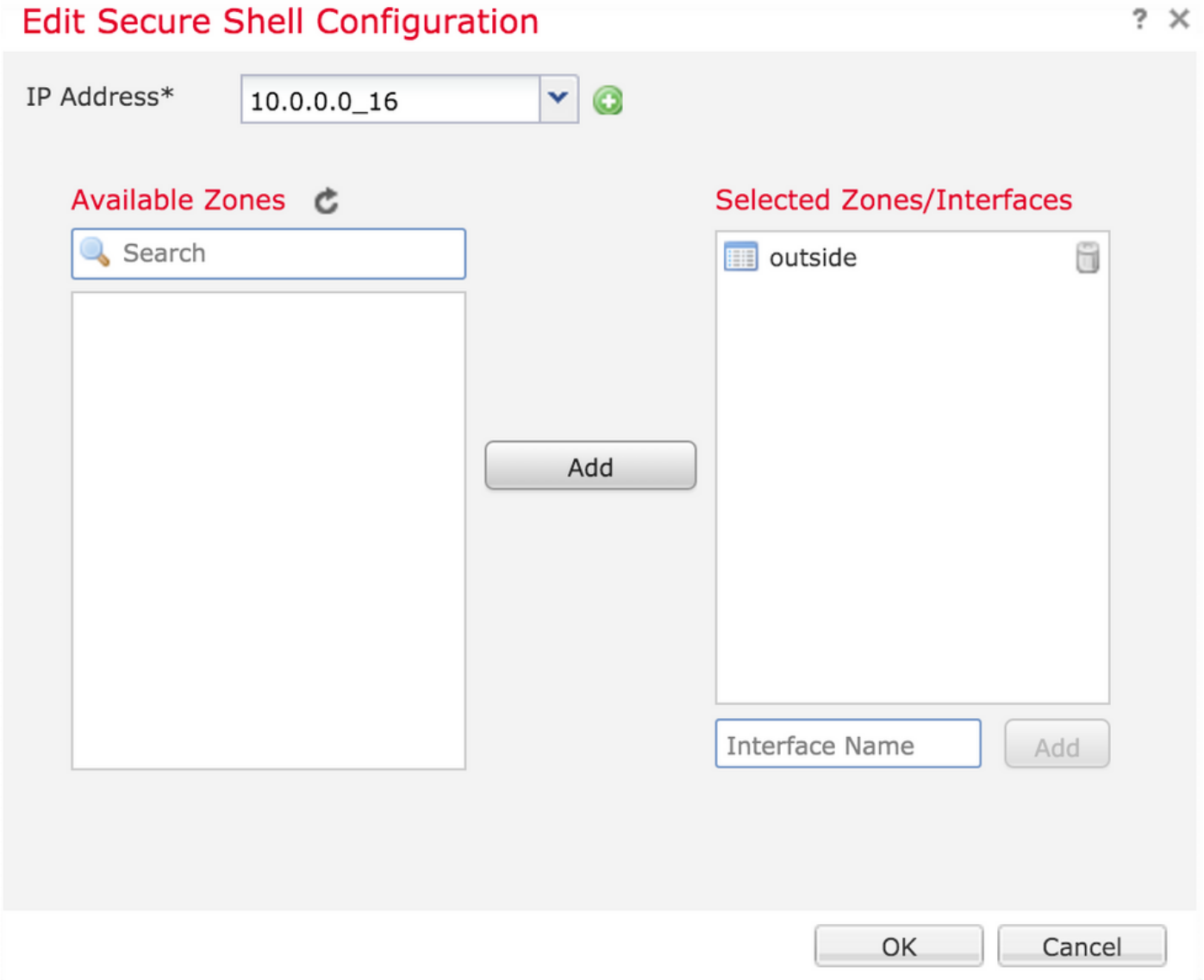


Étape 1. Cliquez sur Add et configurez ces options :

Adresse IP : Sélectionnez un objet de réseau qui contient les sous-réseaux qui sont permis pour accéder au CLI au-dessus du SSH. Si un objet de réseau n'est pas présent, créez un comme vous cliquez sur en fonction **(+) l'**icône.

Zones/interfaces sélectionnées : Sélectionnez les zones ou les interfaces au-dessus de dont on accède au serveur de SSH.

Étape 2. Cliquez sur OK, suivant les indications de l'image :



La configuration pour le SSH est visualisée dans le CLI convergé (diagnostic CLI ASA dans des 6.0.1 périphériques) utilisant cette commande.

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

Étape 3. Une fois que la configuration de SSH est faite, cliquez sur la **sauvegarde** et puis déployez la stratégie vers le FTD.

Étape 4. Configurez l'accès HTTPS.

Afin d'activer l'accès HTTPS à un ou plusieurs interfaces, naviguez vers la section de **HTTP** dans des configurations de plate-forme. L'accès HTTPS est spécifiquement utile pour télécharger les captures de paquet de l'interface web sécurisée de diagnostic directement pour l'analyse.

Il y a 6 étapes pour configurer l'accès HTTPS.

Étape 1. Naviguez vers des **périphériques > des configurations de plate-forme**

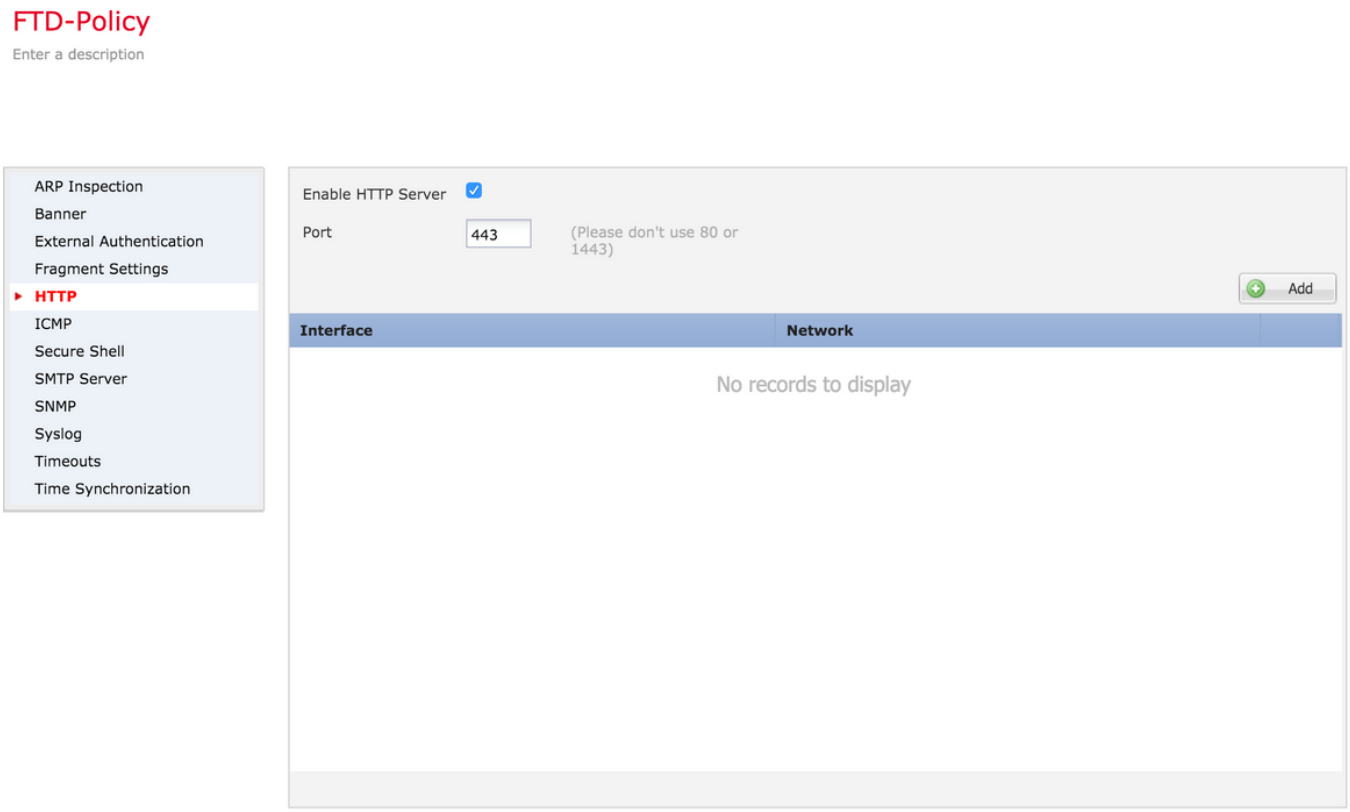
Étape 2. L'un ou l'autre édite la stratégie de configurations de plate-forme qui existe pendant que

vous cliquez sur l'**icône de crayon** près de la stratégie ou créez une nouvelle stratégie FTD pendant que vous cliquez sur New la **stratégie**. Sélectionnez le type comme **défense contre des menaces de FirePOWER.**

Étape 3. Pendant que vous naviguez vers la section de **HTTP**, une page paraît suivant les indications de l'image.

Serveur HTTP d'enable : Activez cette option de faire pour activer le serveur HTTP sur le FTD.

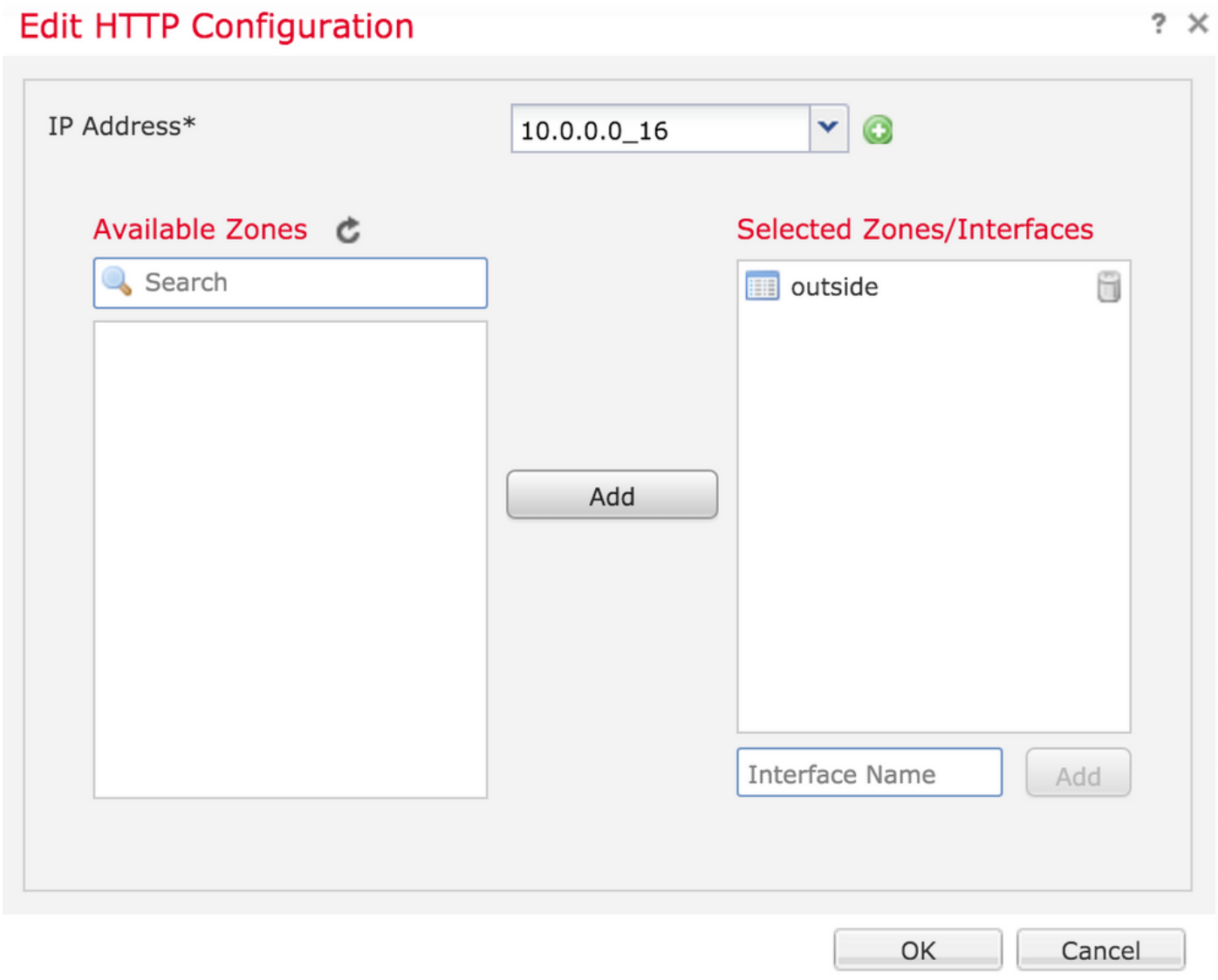
Port : Sélectionnez le port sur lequel le FTD reçoit des connexions de Gestion.



L'étape 4.Click **ajoutent** et l'apage apparaît suivant les indications de l'image :

L'adresse IP écrivent les sous-réseaux qui sont permis pour avoir accès HTTPS à l'interface diagnostique. Si un objet de réseau n'est pas présent créez un utilisant **(+) l'**option.

Les zones/interfaces sélectionnées semblables au SSH, configuration HTTPS doit avoir une interface configurée au-dessus de ce qu'il est accessible par l'intermédiaire de HTTPS. Sélectionnez les zones ou l'interface au-dessus dont le FTD doit être accédé à par l'intermédiaire de HTTPS.



La configuration pour HTTPS est visualisée dans le CLI convergé (diagnostic CLI ASA dans des 6.0.1 périphériques) utilisant cette commande.

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

Étape 5. Une fois que la configuration nécessaire est **OK** choisi fait.

Étape 6. Une fois que toute l'information requise a été **sauvegarde** écrite de clic et déployez alors la stratégie vers le périphérique.

Vérifiez

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

Dépannez

Ce sont les étapes de base pour dépannage de la question d'accès de Gestion sur le FTD.

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

Étape 2. Assurez-vous qu'une authentification externe fonctionne comme configuré et son accessibilité de l'interface appropriée spécifié dans la section d'**authentification externe des configurations de plate-forme**.

Étape 3. Assurez que le routage sur le FTD est précis. Dans la version de logiciel 6.0.1 FTD, naviguez vers le **support de système diagnostic-cli.** Exécutez les commandes **show route** et **show route réservés à la Gestion** de voir les artères pour le FTD et les interfaces de gestion respectivement.

Dans la version de logiciel 6.1.0 FTD, exécutez les commandes directement dans le CLI convergé.

Informations connexes

- Guide de démarrage rapide de défense contre des menaces de Cisco FirePOWER pour l'ASA
- Support et documentation techniques - Cisco Systems