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

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Configurer

- ConfigurerAccès à la gestion
- Étape 1 : configuration du protocole IP sur l'interface FTD via l'interface utilisateur FMC
- Étape 2 : configuration de l'authentification externe
- Étape 3 : configuration de l'accès SSH
- Étape 4 : configuration de l'accès HTTPS

Vérifier

Dépannage

Informations connexes

Introduction

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

Conditions préalables

Exigences

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)

Composants utilisés

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

- Image de défense contre les menaces Firepower de l'appliance de sécurité adaptatif (ASA) pour ASA (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X), qui s'exécute sur la version logicielle 6.0.1 et ultérieure.
- 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 la version logicielle 6.0.1 et ultérieure.
- 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 l'apparition de Firepower Threat Defense (FTD), la configuration ASA complète est effectuée sur l'interface utilisateur graphique.

Sur les périphériques FTD qui exécutent la version logicielle 6.0.1, l'interface de ligne de commande de diagnostic ASA est accessible lorsque vous entrez dans l'interface de ligne de commande de diagnostic de support système. Cependant, sur les périphériques FTD qui exécutent la version logicielle 6.1.0, l'interface de ligne de commande est convergée et des commandes ASA entières sont configurées sur l'interface 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 à la gestion directement à partir d'un réseau externe, vous devez configurer l'accès à la gestion via HTTPS ou SSH. Ce document fournit la configuration requise pour obtenir un accès de gestion sur SSH ou HTTPS en externe.

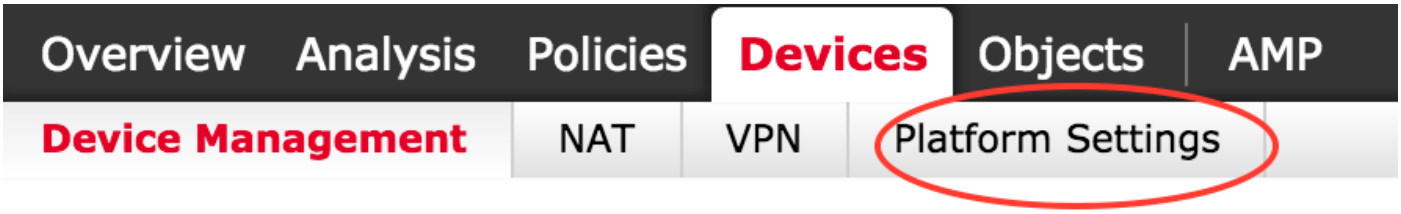
Remarque : Sur les périphériques FTD qui exécutent la version logicielle 6.0.1, l'interface de ligne de commande n'est pas accessible par un utilisateur local, une authentification externe doit être configurée afin d'authentifier les utilisateurs. Cependant, sur les périphériques FTD qui exécutent la version logicielle 6.1.0, l'interface de ligne de commande est accessible par l'utilisateur admin local tandis qu'une authentification externe est requise pour tous les autres utilisateurs.

Remarque : Sur les périphériques FTD qui exécutent la version logicielle 6.0.1, l'interface de

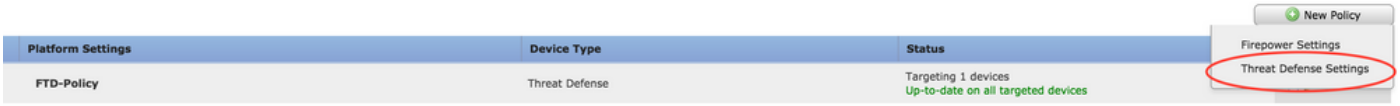
ligne de commande de diagnostic n'est pas directement accessible sur l'adresse IP configurée pour br1 du FTD. Cependant, sur les périphériques FTD qui exécutent la version logicielle 6.1.0, l'interface de ligne de commande convergée est accessible sur toute interface configurée pour l'accès à la gestion,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

Configurer

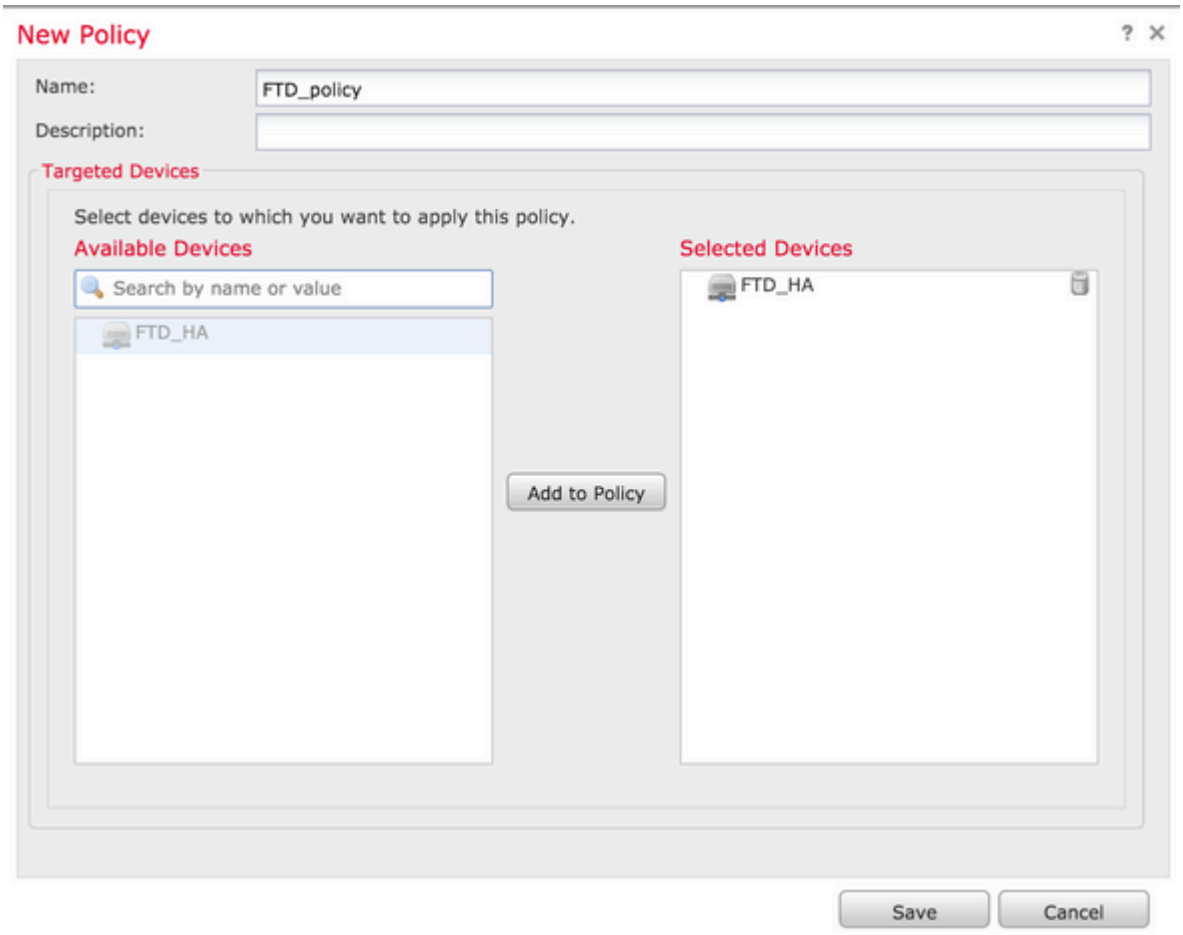
La configuration relative à l'accès à la gestion est configurée lorsque vous accédez à l'onglet Paramètres de la plate-forme dans Périphériques, comme illustré dans l'image :



Vous pouvez modifier la stratégie qui existe lorsque vous cliquez sur l'icône du crayon ou créer une nouvelle stratégie FTD lorsque vous cliquez sur le bouton Nouvelle stratégie et sélectionnez le type Paramètres de défense contre les menaces, comme illustré dans l'image :



Sélectionnez l'appliance FTD pour appliquer cette stratégie et cliquez sur Save, comme indiqué dans l'image :



Configurer l'accès de gestion

Voici les quatre principales étapes suivies pour configurer l'accès de gestion.

Étape 1 : configuration du protocole IP sur l’interface FTD via l’interface utilisateur FMC

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

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

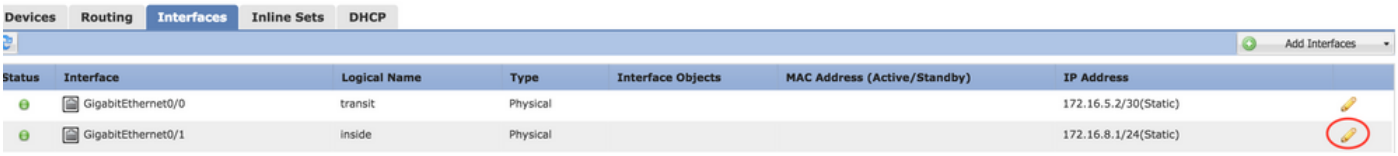
La configuration de l’interface de diagnostic s’effectue en six étapes.

Étape 1. Accédez à Device > Device Management.

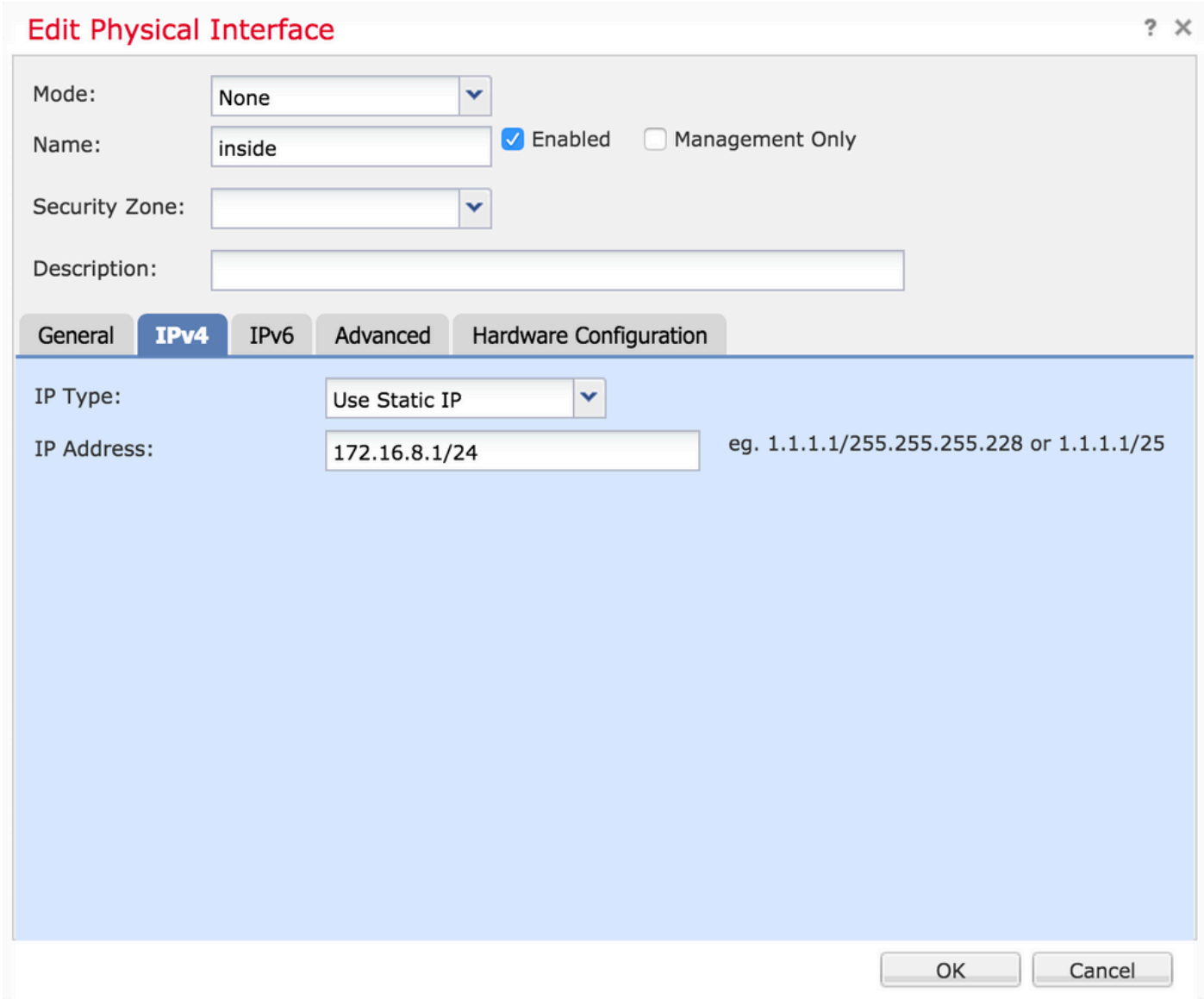
Étape 2. Sélectionnez le périphérique ou le cluster haute disponibilité FTD.

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, choisissez le type d'IP static ou DHCP. Entrez maintenant une adresse IP pour l'interface et cliquez sur OK, comme indiqué dans l'image :



Étape 6. Cliquez sur Save, 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 sur SSH sur des périphériques dotés de la version logicielle 6.1.0

Étape 2 : configuration de l’authentification externe

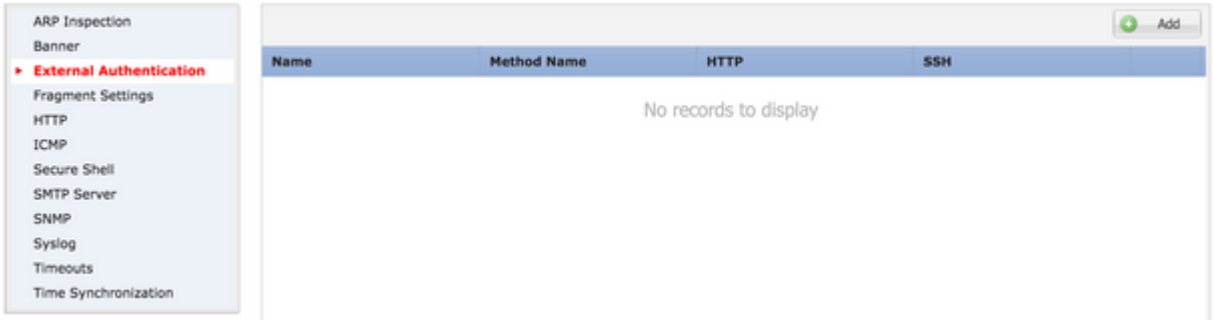
L'authentification externe facilite l'intégration du FTD à un serveur Active Directory ou RADIUS pour l'authentification des utilisateurs. Cette étape est nécessaire car les utilisateurs configurés localement n'ont pas d'accès direct à l'interface de ligne de commande de diagnostic. L'interface de ligne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

La configuration de l'authentification externe s'effectue en 6 étapes.

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

Étape 2. Modifiez la stratégie existante lorsque vous cliquez sur l'icône du crayon ou créez une nouvelle stratégie FTD lorsque vous cliquez sur le bouton Nouvelle stratégie et sélectionnez le type Paramètres de défense contre les menaces.

Étape 3. Accédez à l’onglet External Authentication, comme indiqué dans l’image :



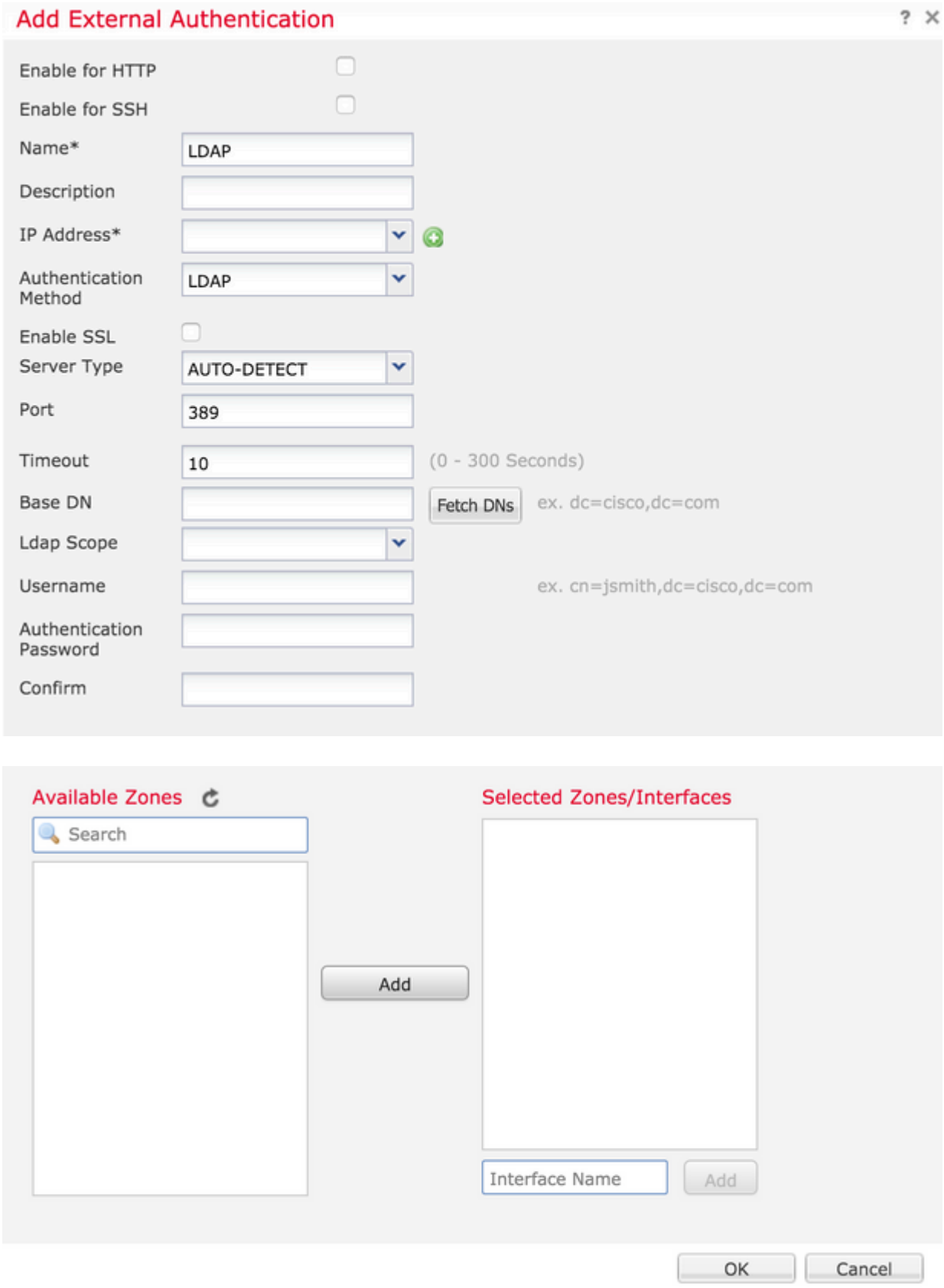
Étape 4. Lorsque vous cliquez sur Add, une boîte de dialogue s’affiche, comme illustré dans l’image :

- Enable for HTTP : activez cette option pour fournir l'accès au FTD sur HTTPS.
- Enable for SSH : activez cette option pour fournir l'accès au FTD sur SSH.
- Name : saisissez le nom de la connexion LDAP.
- Description : saisissez une description facultative pour l'objet Authentification externe.

- IP address : saisissez 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 (Méthode d'authentification) : sélectionnez le protocole RADIUS ou LDAP pour l'authentification.
- Enable SSL-Activez cette option pour chiffrer le trafic d'authentification.
- Server Type : sélectionnez le type de serveur. Les types de serveurs les plus connus sont MS Active Directory, Sun, OpenLDAP et Novell. Par défaut, l'option est définie pour détecter automatiquement le type de serveur.
- Port : saisissez le port sur lequel l'authentification a lieu.
- Timeout : saisissez une valeur de délai d'attente pour les demandes d'authentification.
- DN de base : saisissez 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 dans la sous-arborescence.
- Username : saisissez un nom d'utilisateur à lier à l'annuaire LDAP.
- Authentication password : saisissez le mot de passe de cet utilisateur.
- Confirm- Saisissez à nouveau le mot de passe.
- Available Interfaces : une liste des interfaces disponibles sur le FTD s'affiche.
- Selected zones and interfaces : affiche la liste des interfaces à partir desquelles le serveur d'authentification est accessible.

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

Secret : saisissez 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 sur SSH sur des périphériques dotés de la version logicielle

6.1.0

Étape 3 : configuration de l’accès SSH

SSH fournit un accès direct à l'interface de ligne de commande convergée. Utilisez cette option pour accéder directement à l'interface de ligne de commande et exécuter les commandes debug.Cette section décrit comment configurer SSH afin d'accéder à l'interface de ligne de commande FTD.

Remarque : Sur les périphériques FTD qui exécutent la version logicielle 6.0.1, la configuration SSH sur les paramètres de la plate-forme permet d'accéder directement à l'interface de ligne de commande de diagnostic et non à l'interface CLISH. Vous devez vous connecter à l'adresse IP configurée sur br1 pour accéder à CLISH. Cependant, sur les périphériques FTD qui exécutent la version logicielle 6.1.0, toutes les interfaces accèdent à 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 avec une version logicielle antérieure 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 du crayon ou créez une nouvelle stratégie Firepower Threat Defense lorsque vous cliquez sur le bouton New Policy et sélectionnez le type comme Threat Defense Settings.

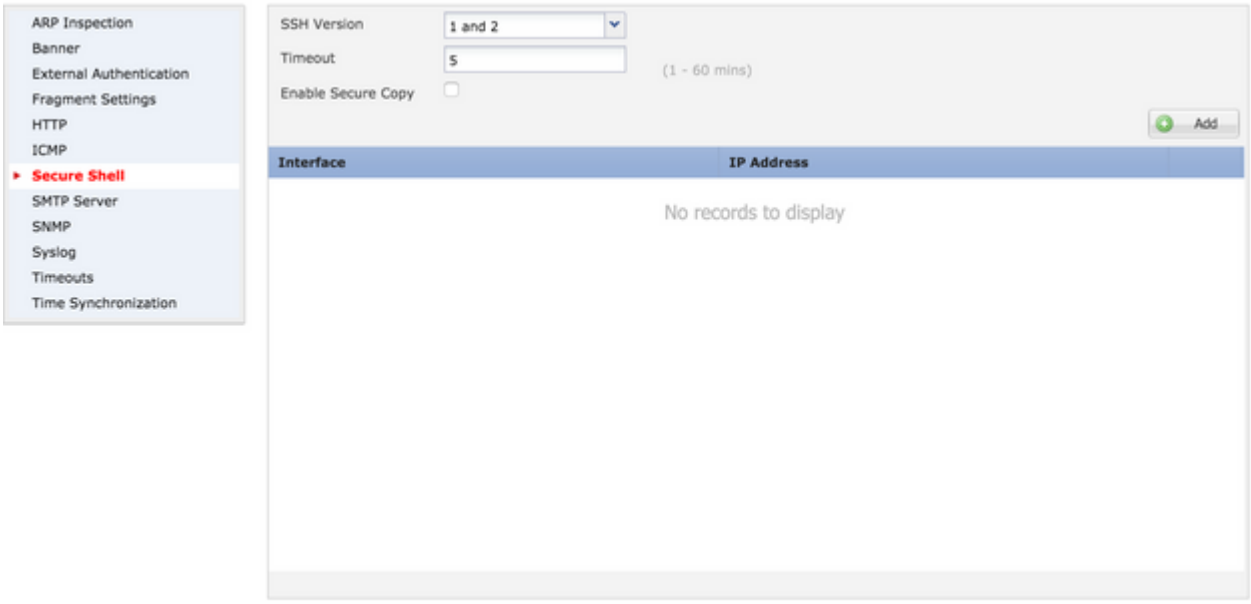
Étape 3. Accédez à la section Secure Shell. Une page s'affiche, comme illustré dans l'image :

Version SSH : Sélectionnez la version SSH à activer sur l'ASA. Trois options sont disponibles :

- 1: Activer uniquement SSH version 1
- 2: Activer uniquement SSH version 2
- 1 et 2 : Activer SSH versions 1 et 2

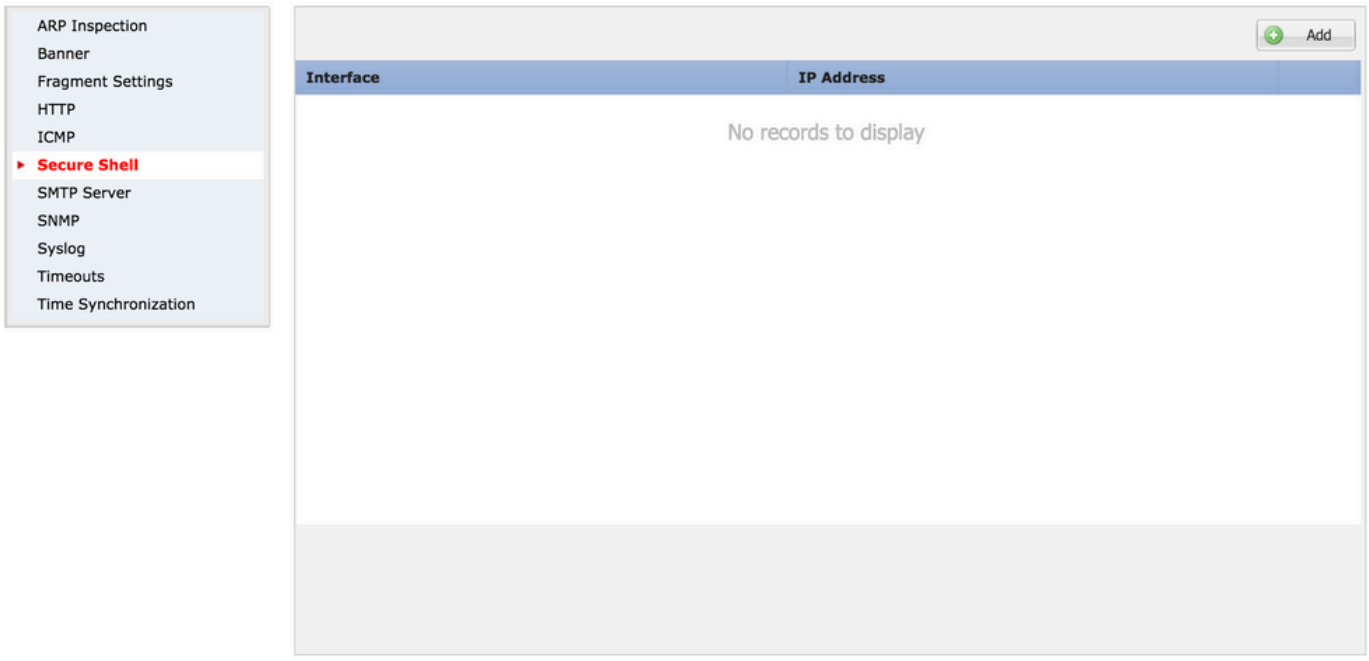
timeout : Entrez le délai d'attente SSH souhaité en minutes.

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 à la gestion via SSH à des interfaces spécifiques et à des adresses IP spécifiques.

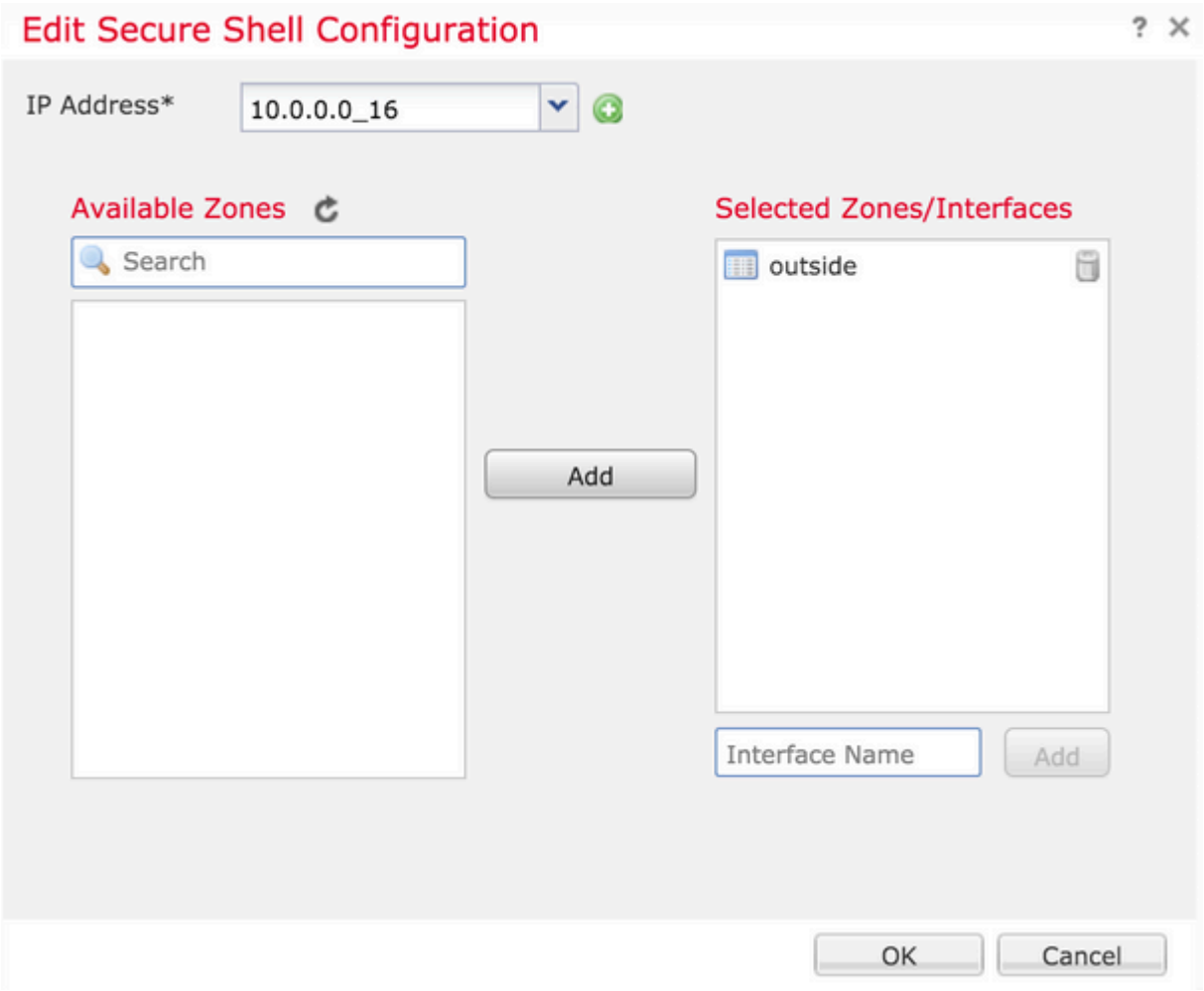


Étape 1. Cliquez sur Add et configurez ces options :

Adresse IP: Sélectionnez un objet réseau qui contient les sous-réseaux autorisés à accéder à l'interface de ligne de commande sur SSH. Si aucun objet réseau n'est présent, créez-en un en cliquant 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 pour SSH est affichée dans l'interface de ligne de commande convergée (interface de ligne de commande 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 Save, puis déployez la stratégie sur le FTD.

Étape 4 : configuration de l'accès HTTPS

Afin d'activer l'accès HTTPS à une ou plusieurs interfaces, naviguez jusqu'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.

La configuration de l'accès HTTPS s'effectue en 6 étapes.

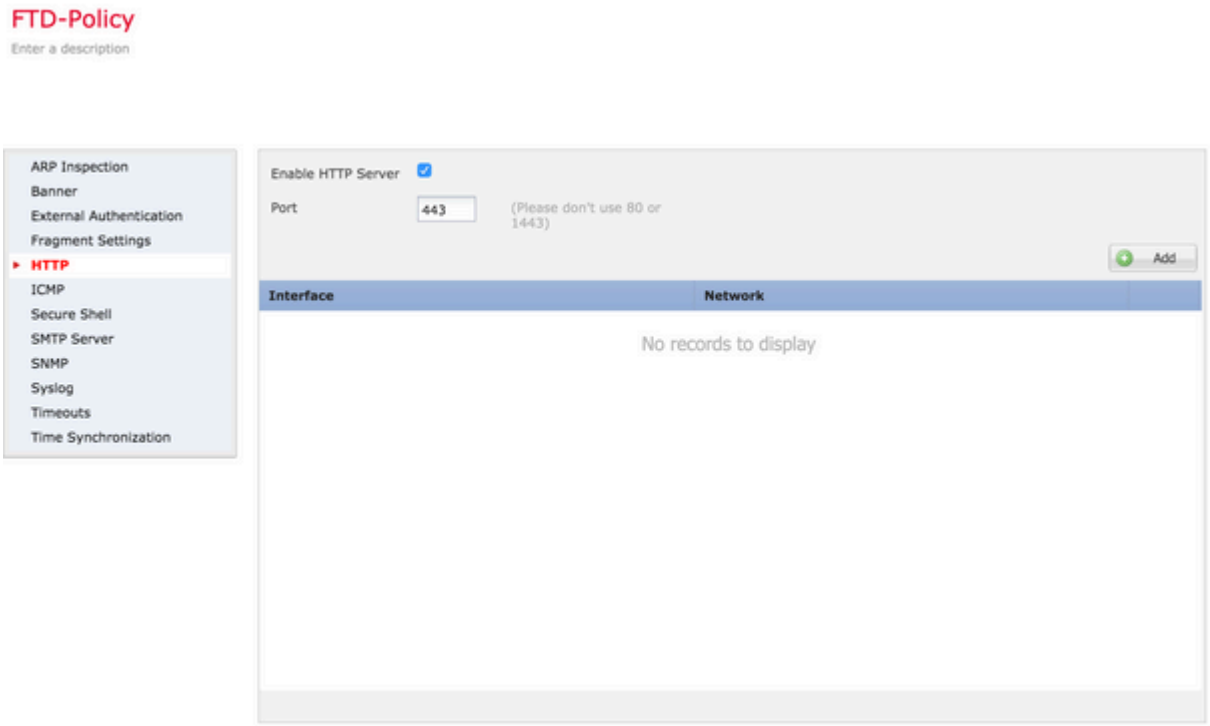
Étape 1. Accédez à Devices > Platform Settings

Étape 2. Modifiez la stratégie de paramètres de plate-forme qui existe lorsque vous cliquez sur l'icône de crayon à côté 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 illustré dans l'image.

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

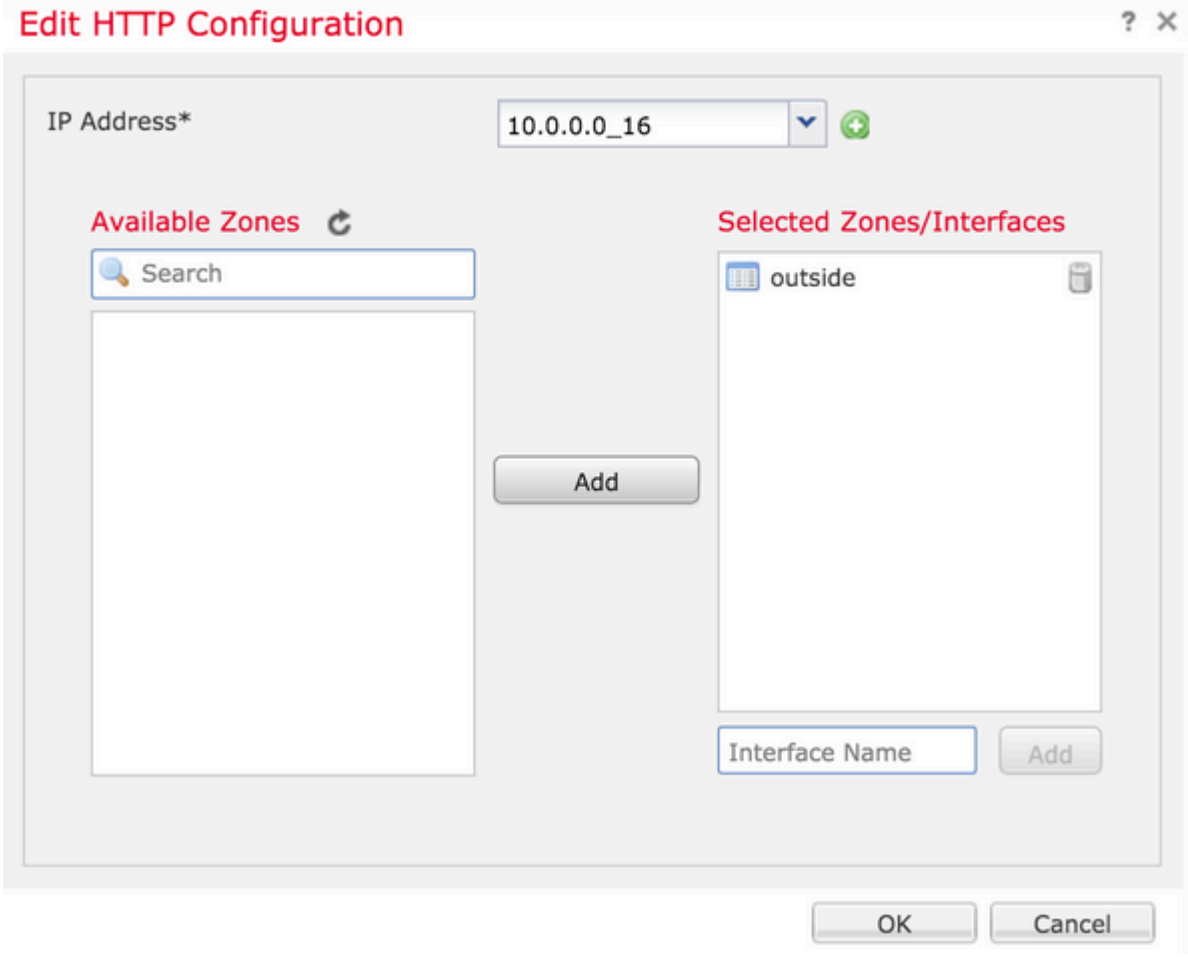
Port : sélectionnez le port sur lequel le FTD accepte les connexions de gestion.



Étape 4. Cliquez sur Add et la page s'affiche comme illustré dans l'image :

IP address : saisissez les sous-réseaux qui sont autorisés à avoir un 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 disposer d'une interface sur laquelle elle est accessible via HTTPS. Sélectionnez les zones ou l'interface sur lesquelles le FTD doit être accessible via HTTPS.



La configuration pour HTTPS est affichée dans la CLI 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 nécessaire terminée, sélectionnez OK.

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

Vérifier

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

Dépannage

Voici les étapes de base pour dépanner un 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 configuré et que son accessibilité est assurée à partir de l’interface appropriée spécifiée dans la section Authentification externe des Paramètres de plate-forme.

Étape 3. Assurez-vous que le routage sur le FTD est correct. 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 afficher les routes pour le FTD et les interfaces de gestion respectivement.

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

Informations connexes

- Assistance et documentation techniques - Cisco Systems

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.

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.