Configuration initiale du châssis Firepower 4100

Est-ce que ce chapitre s'adresse à vous?

Ce chapitre décrit comment effectuer la configuration initiale du châssis Cisco Firepower 4100, y compris la configuration des interfaces à utiliser avec l'ASA et les dispositifs logiques Défense contre les menaces.

- Ce guide est-il pour vous?, à la page 1
- À propos du châssis Firepower 4100, à la page 2
- Procédure de bout en bout, à la page 4
- Câbler le châssis, à la page 5
- Effectuer la configuration initiale du châssis, à la page 9
- Se connecter au Gestionnaire de châssis, à la page 13
- Configurer NTP, à la page 14
- Ajouter des utilisateurs FXOS, à la page 16
- Interfaces de configuration, à la page 18
- Téléverser des images logicielles dans le châssis, à la page 24
- Historique de FXOS, à la page 25

Ce guide est-il pour vous?

Ce guide décrit comment configurer le châssis Firepower 4100 pour une utilisation avec l'ASA ou Défense contre les menaces. Ce guide décrit les déploiements suivants :

- Défense contre les menaces autonome en tant qu'instance native ou de contenant (fonctionnalité multi-instances) à l'aide de centre de gestion
- Défense contre les menaces autonome utilisant le gestionnaire d'appareil

Remarque Le gestionnaire d'appareil ne prend pas en charge la fonctionnalité multi-instances.

- Défense contre les menaces autonome utilisant CDO

Remarque CDO ne prend pas en charge la fonctionnalité multi-instances.

- ASA autonome utilisant ASDM

Ce chapitre n'aborde pas les déploiements suivants. Pour en savoir plus à ce sujet, consultez les guides de configuration pour FXOS, ASA, FDM, CDO et FMC :

- Haute disponibilité/Basculement
- Mise en grappe (ASA ou Défense contre les menaces utilisant centre de gestion uniquement)
- Multi-instances (Défense contre les menaces utilisant centre de gestion uniquement)
- Application de décorateurs Radware DefensePro
- Configuration de l'interface de ligne de commande (ASA ou FXOS uniquement)

Ce guide vous montre la configuration d'une politique de sécurité de base; si vous avez des exigences plus avancées, consultez le guide de configuration.

À propos du châssis Firepower 4100

Le châssis Firepower 4100 est une plateforme de nouvelle génération pour les solutions de sécurité du réseau et du contenu. Le châssis Firepower 4100 comprend un superviseur et un seul moteur de sécurité sur lesquels vous pouvez installer des dispositifs logiques. Il accepte également plusieurs modules de réseau haute performance.

Fonctionnement du dispositif logique avec Firepower 4100/9300

Le Firepower 4100/9300 exécute son propre système d'exploitation sur le superviseur appelé le Firepower eXtensible Operating System (FXOS). Le gestionnaire de châssis sur la boîte offre des fonctionnalités de gestion simples et basées sur l'interface graphique utilisateur. Vous configurez les paramètres de l'interface matérielle, l'octroi de licences Smart (pour l'ASA) et d'autres paramètres opérationnels de base sur le superviseur à l'aide de l'interface de ligne de commande FXOS de . Pour utiliser l'interface de ligne de commande de FXOS, consultez le FXOS CLI configuration guide (Guide de configuration de l'interface de ligne de commande FXOS).

Un dispositif logique vous permet d'exécuter une instance d'application ainsi qu'une application de décorateurs facultative pour former une chaîne de services. Lorsque vous déployez le dispositif logique, le superviseur télécharge une image d'application de votre choix et établit une configuration par défaut. Vous pouvez ensuite configurer la politique de sécurité dans le système d'exploitation de l'application.

Les dispositifs logiques ne peuvent pas former de chaîne de service entre eux et ne peuvent pas communiquer entre eux sur le fond de panier. Tout le trafic doit quitter le châssis sur une interface et revenir sur une autre interface pour atteindre un autre dispositif logique. Pour les instances de contenant, vous pouvez partager des interfaces de données; seulement dans ce cas, plusieurs dispositifs logiques peuvent communiquer sur le fond de panier.

Applications prises en charge

Vous pouvez déployer des dispositifs logiques sur votre châssis en utilisant les types d'applications suivants.

Défense contre les menaces

Défense contre les menaces fournit des services de pare-feu de nouvelle génération, notamment le pare-feu dynamique, le routage, le VPN, le système de prévention des intrusions de nouvelle génération (NGIPS), la visibilité et le contrôle des applications (AVC), le filtrage des URL et la protection contre les logiciels malveillants.

Vous pouvez gérer Défense contre les menaces à l'aide de l'un des gestionnaires suivants :

- Centre de gestion : un gestionnaire multidispositif complet sur un serveur séparé.
- Gestionnaire d'appareil : un gestionnaire simplifié pour un seul dispositif inclus sur le dispositif.
- CDO : un gestionnaire multidispositif en nuage

ASA

L'ASA offre des fonctionnalités avancées de pare-feu dynamique et de concentrateur VPN dans un seul dispositif. Vous pouvez gérer l'ASA en utilisant l'une des solutions de gestion suivantes :

- ASDM : un gestionnaire simplifié pour un seul dispositif inclus sur le dispositif. *Ce guide décrit comment gérer l'ASA à l'aide d'ASDM.*
- Interface de ligne de commande
- CDO : un gestionnaire multidispositif en nuage
- CSM : un gestionnaire multidispositif sur un serveur séparé.

Radware DefensePro (Décorateur)

Vous pouvez installer Radware DefensePro (vDP) pour qu'il s'exécute en premier plan sur l'ASA ou Défense contre les menaces comme application de décorateurs. vDP est une plateforme virtuelle basée sur KVM qui fournit des fonctionnalités de détection et d'atténuation des dénis de service distribués (DDoS) sur Firepower 4100/9300. Le trafic du réseau doit d'abord passer par le vDP avant d'atteindre l'ASA ou Défense contre les menaces.

Pour déployez vDP, consultez le FXOS configuration guide (Guide de configuration de FXOS).

Instances d'application du dispositif logique : instance de conteneur ou instance native

Les instances d'application du dispositif logique s'exécutent dans les types de déploiement suivants :

- Instance native : Une instance native utilise toutes les ressources (CPU, RAM et espace disque) de security engine. Vous ne pouvez donc installer qu'une seule instance native.
- Instance de conteneur : Une instance de conteneur utilise un sous-ensemble de ressources de security engine. Vous pouvez donc installer plusieurs instances de conteneur. **Remarque :** La fonctionnalité multi-instance n'est prise en charge que pour Défense contre les menaces; elle n'est pas prise en charge pour l'ASA ou conjointement avec vDP.

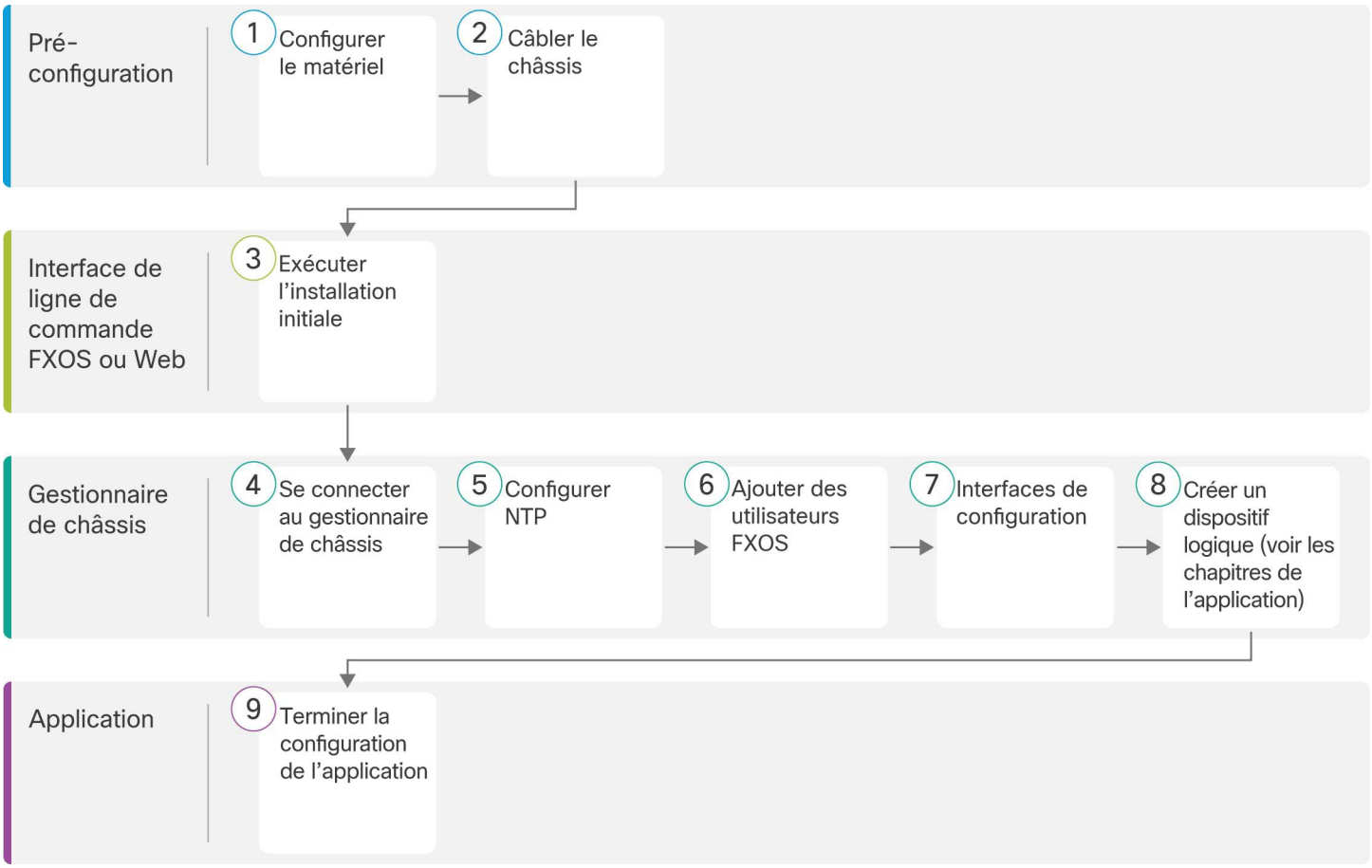
Nombre maximal d'instances de conteneur par modèle

- Firepower 4110—3

- Firepower 4112—3
- Firepower 4115—7
- Firepower 4120—3
- Firepower 4125—10
- Firepower 4140—7
- Firepower 4145—14
- Firepower 4150—7

Procédure de bout en bout

Consultez les tâches suivantes pour configurer le châssis Firepower 4100 et déployer des dispositifs logiques sur votre châssis.



1	Pré-configuration	Configurez le matériel Firepower 4100. Consultez le (Guide matériel Firepower 9300) et le Firepower 4100 hardware guide (Guide matériel Firepower 4100).

2	Pré-configuration	Câbler le châssis, à la page 5.
3	Interface de ligne de commande FXOS ou Web	Effectuer la configuration initiale du châssis, à la page 9.
4	Gestionnaire de châssis	Se connecter au Gestionnaire de châssis, à la page 13.
5	Gestionnaire de châssis	Configurer NTP, à la page 14.
6	Gestionnaire de châssis	Ajouter des utilisateurs FXOS, à la page 16.
7	Gestionnaire de châssis	Interfaces de configuration, à la page 18.
8	Gestionnaire de châssis	Créez des dispositifs logiques : • Défense contre les menaces avec le centre de gestion : consultez Déploiement de Défense contre les menaces avec le Centre de gestion. • Défense contre les menaces avec le gestionnaire d'appareil : consultez Déploiement de Défense contre les menaces avec le Gestionnaire d'appareil. • Défense contre les menaces avec le CDO : consultez Défense contre les menaces Déploiement avec CDO. • ASA : consultez Déploiement d'ASA avec ASDM. **Remarque** La prise en charge de Défense contre les menaces avec le gestionnaire d'appareil a été ajoutée dans FXOS 2.7.1/Défense contre les menaces 6.5
9	Application	Terminez la configuration de l'application : • Défense contre les menaces avec le centre de gestion : consultez Déploiement de Défense contre les menaces avec le Centre de gestion. • Défense contre les menaces avec le gestionnaire d'appareil : consultez Déploiement de Défense contre les menaces avec le Gestionnaire d'appareil. • Défense contre les menaces avec le CDO : consultez Défense contre les menaces Déploiement avec CDO. • ASA : consultez Déploiement d'ASA avec ASDM.

Câbler le châssis

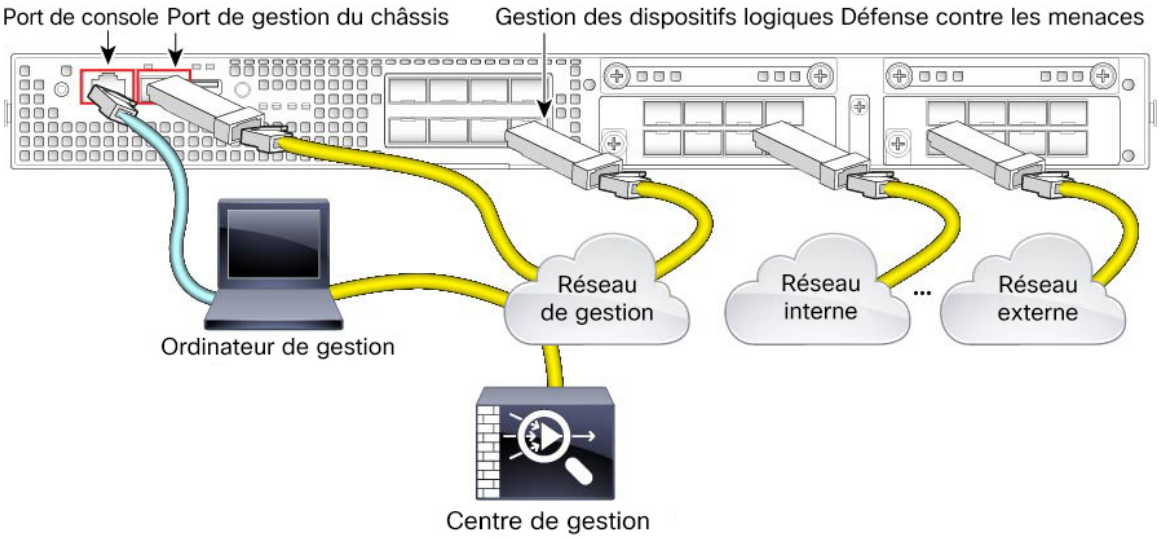
Câblez les interfaces suivantes pour la configuration initiale du châssis, la surveillance continue et l'utilisation de dispositifs logiques.

- Console port (Port de console) : (facultatif) si vous n'effectuez pas la configuration initiale sur le port de gestion du châssis, connectez votre ordinateur de gestion au port de console pour effectuer la configuration initiale du châssis. Le Firepower 4100 comprend un câble de console de série RS-232 à RJ-45. Vous devrez peut-être utiliser un câble série tiers vers USB pour établir la connexion.
- Chassis Management port (Port de gestion du châssis) : connectez le port de gestion du châssis à votre réseau de gestion pour la configuration et la gestion continue du châssis. Vous pouvez effectuer la configuration initiale de ce port s'il reçoit une adresse IP d'un serveur DHCP.
- Logical device Management interface (Interface de gestion des dispositifs logiques) : utilisez une ou plusieurs interfaces pour gérer les dispositifs logiques. Ce guide suppose que vous avez un réseau de gestion distinct avec son propre accès Internet. Vous pouvez choisir n'importe quelle interface sur le châssis à cette fin, sauf le port de gestion du châssis, qui est réservé à la gestion FXOS. Pour la prise en charge de plusieurs instances, les interfaces de gestion peuvent être partagées entre les dispositifs logiques, ou vous pouvez utiliser une interface distincte par dispositif logique. En règle générale, vous partagez une interface de gestion avec tous les dispositifs logiques, ou si vous utilisez des interfaces distinctes, vous pouvez les placer sur un seul réseau de gestion. Mais vos exigences précises en matière de réseau peuvent varier. Pour défense contre les menaces, l'interface de gestion est une interface distincte des interfaces de données et elle possède ses propres paramètres réseau. Dans la version 6.7 et ultérieure, vous pouvez éventuellement configurer une interface de données pour avoir l'accès gestionnaire au lieu de l'interface de gestion. Dans ce cas, vous devez toujours attribuer une interface de gestion au dispositif logique pour des raisons d'architecture interne, mais vous n'avez pas besoin de la câbler. Notez que pour centre de gestion, l'accès gestionnaire à partir d'une interface de données n'est pas pris en charge dans les déploiements à haute disponibilité ou de mise en grappe. Pour de plus amples informations, consultez la commande **configure network management-data-interface** dans la référence de commande FTD.
- Data interfaces (Interfaces de données) : connectez les interfaces de données aux réseaux de données de votre dispositif logique. Vous pouvez configurer des interfaces physiques, des EtherChannel, des sous-interfaces VLAN (pour les instances de conteneur uniquement) et des ports de séparation pour diviser les interfaces à haute capacité. Pour la prise en charge des instances multiples,ous pouvez câbler plusieurs dispositifs logiques aux mêmes réseaux ou à des réseaux différents, selon les besoins de votre réseau. Pour les instances de contenant, vous pouvez partager des interfaces de données; seulement dans ce cas, plusieurs dispositifs logiques peuvent communiquer sur le fond de panier. Autrement, tout le trafic doit quitter le châssis sur une interface et revenir sur une autre interface pour atteindre un autre dispositif logique. Pour en savoir plus sur les limites et les directives relatives aux interfaces partagées, consultez le FXOS configuration guide (Guide de configuration FXOS).

Remarque Toutes les interfaces, à l'exception du port de console, nécessitent des émetteurs-récepteurs SFP, SFP+ et QSFP. Consultez le hardware installation guide (guide d'installation du matériel) pour connaître les émetteurs-récepteurs pris en charge.

Remarque Bien que non traité dans ce guide, pour le déploiement à haute disponibilité, utilisez une interface de données pour le lien de basculement/état. Pour la mise en grappe inter-châssis, utilisez un EtherChannel défini sur le châssis comme interface de type de grappe.

Défense contre les menaces avec le câblage du Centre de gestion

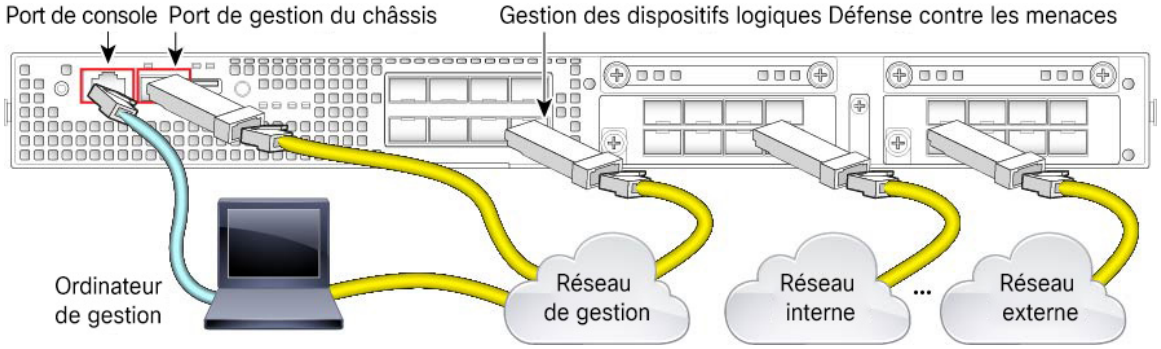


Ce guide suppose que vous avez un réseau de gestion distinct avec son propre accès Internet. Par défaut, l'interface de gestion est préconfigurée lorsque vous le déployez, mais vous devez configurer les interfaces de données ultérieurement.

Placez le centre de gestion sur le réseau de gestion des dispositifs logiques (ou rendez-le accessible à partir de ce dernier). Défense contre les menaces et le centre de gestion nécessitent un accès à Internet par l'entremise du réseau de gestion pour les mises à jour et les licences. Dans la version 6.7 et ultérieure, vous pouvez éventuellement configurer une interface de données pour la gestion de centre de gestion au lieu de l'interface de gestion. Notez que l'accès à centre de gestion à partir d'une interface de données n'est pas pris en charge dans les déploiements à haute disponibilité ou à mise en grappe. Pour en savoir plus sur la configuration d'une interface de données pour l'accès à centre de gestion, consultez la commande **configure network management-data-interface** dans la référence de commande FTD.

Remarque La connexion de gestion est un canal de communication sécurisé et chiffré par SSL entre elle et le dispositif. Vous n'avez pas besoin d'exécuter ce trafic sur un tunnel chiffré supplémentaire comme un VPN de site à site pour des raisons de sécurité. Si le VPN tombe en panne, par exemple, vous perdrez votre connexion de gestion. Nous vous recommandons donc un chemin de gestion simple.

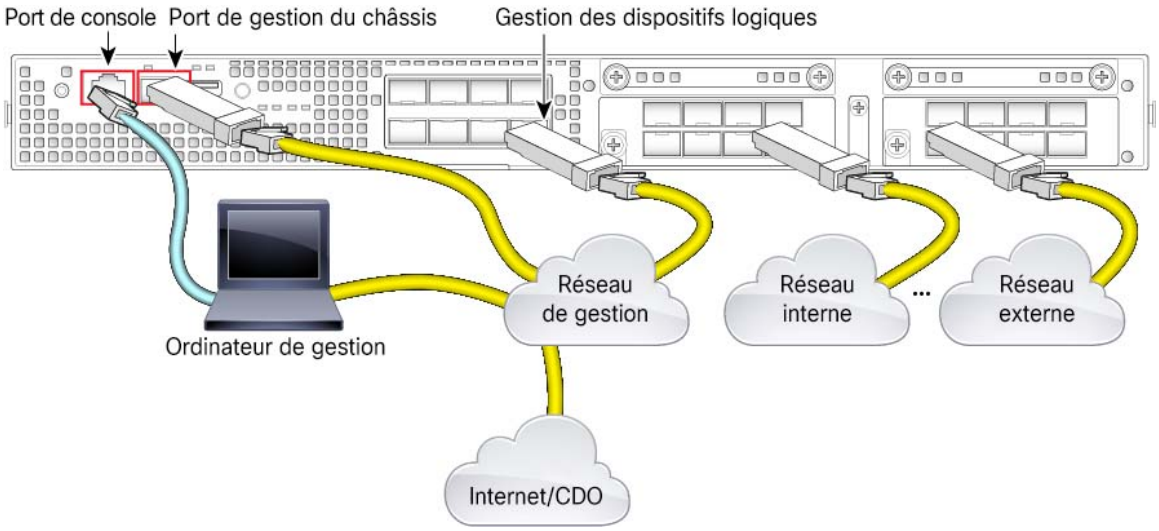
Défense contre les menaces avec le câblage du Gestionnaire d'appareil



Ce guide suppose que vous avez un réseau de gestion distinct avec son propre accès Internet. Par défaut, l'interface de gestion est préconfigurée lorsque vous le déployez, mais vous devez configurer les interfaces de données ultérieurement.

Effectuez la configuration initiale de Défense contre les menaces sur l'interface de gestion du dispositif logique. Défense contre les menaces nécessite un accès Internet pour les licences, les mises à jour et la gestion des CDO, et le comportement par défaut consiste à acheminer le trafic de gestion vers l'adresse IP de la passerelle que vous avez spécifiée lors du déploiement de Défense contre les menaces. Vous pourrez activer ultérieurement la gestion de gestionnaire d'appareil à partir de n'importe quelle interface de données.

Défense contre les menaces avec câblage CDO

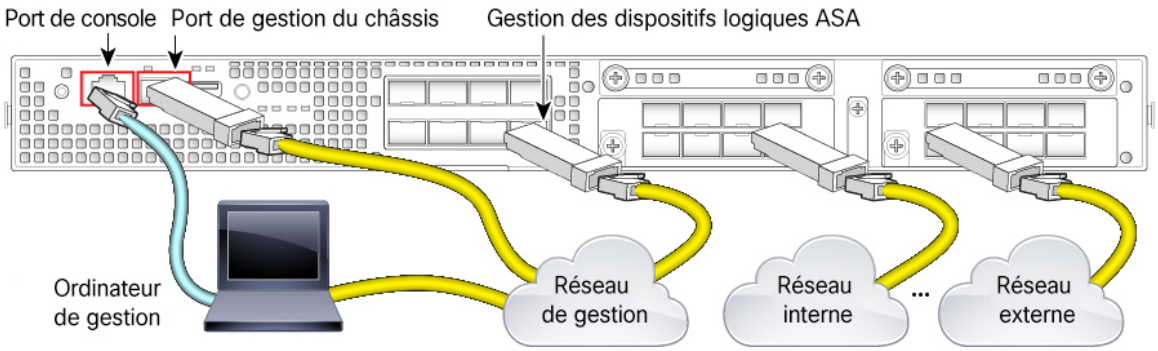


Ce guide suppose que vous avez un réseau de gestion distinct avec son propre accès Internet. Par défaut, l'interface de gestion est préconfigurée lorsque vous le déployez, mais vous devez configurer les interfaces de données ultérieurement.

Assurez-vous qu'Internet soit accessible à partir du réseau de gestion des dispositifs logiques. Défense contre les menaces nécessite un accès à Internet par l'entremise du réseau de gestion du CDO, les mises à jour et les licences. Vous pouvez éventuellement configurer une interface de données pour la gestion du CDO au lieu de l'interface de gestion. Pour en savoir plus sur la configuration d'une interface de données pour l'accès du gestionnaire, consultez la commande **configure network management-data-interface**dans la référence de commande FTD.

Remarque La connexion de gestion est un canal de communication sécurisé et chiffré par SSL entre elle et le dispositif. Vous n'avez pas besoin d'exécuter ce trafic sur un tunnel chiffré supplémentaire comme un VPN de site à site pour des raisons de sécurité. Si le VPN tombe en panne, par exemple, vous perdrez votre connexion de gestion. Nous vous recommandons donc un chemin de gestion simple.

Câblage de l'ASA



Ce guide suppose que vous avez un réseau de gestion distinct avec son propre accès Internet. Par défaut, l'interface de gestion est préconfigurée lorsque vous le déployez, mais vous devez configurer les interfaces de données ultérieurement.

Effectuez la configuration initiale de l'ASA sur l'interface de gestion du dispositif logique. Vous pourrez activer ultérieurement la gestion à partir de n'importe quelle interface de données.

Effectuer la configuration initiale du châssis

Avant de pouvoir utiliser le gestionnaire de châssis pour configurer et gérer votre système, vous devez effectuer certaines tâches de configuration initiale. Vous pouvez effectuer la configuration initiale en utilisant l'interface de ligne de commande de FXOS sur le port de console ou une session SSH sur le port de gestion du châssis, ou en utilisant le protocole HTTPS sur le port de gestion du châssis.

Effectuer la configuration initiale du châssis à l'aide d'un navigateur

Le port de gestion de châssis obtient une adresse IP en utilisant DHCP. Pour la configuration initiale, vous pouvez utiliser un navigateur Web pour configurer les paramètres de base du châssis. Si vous n'avez pas de serveur DHCP, vous devez utiliser le port de console pour la configuration initiale.

Remarque Pour relancer la configuration initiale, vous devez effacer toute configuration existante à l'aide des commandes suivantes à partir de l'interface de ligne de commande :

```
Firepower-chassis# connect local-mgmt
firepower-chassis(local-mgmt)# erase configuration
```

Avant de commencer

Recueillez les informations suivantes à utiliser avec le script de configuration :

- Nouveau mot de passe de l'administrateur
- Adresse IP de gestion et filtre d'adresse locale
- Adresse IP de la passerelle

- Sous-réseaux à partir desquels vous souhaitez autoriser l'accès HTTPS et SSH
- Nom d'hôte et le nom de domaine
- Adresse IP du serveur DNS

Procédure

Étape 1 Configurez votre serveur DHCP pour attribuer une adresse IP au port de gestion du châssis.

La demande du client DHCP du châssis contient les informations suivantes :

- L'adresse MAC de l'interface de gestion.
- L'option DHCP 60 (vendor-class-identifier) : définie sur « FPR4100 ».
- L'option DHCP 61 (dhcp-client-identifier) : définie sur le numéro de série du châssis. Ce numéro de série se trouve sur un onglet amovible sur le châssis.

Étape 2 Démarrez le châssis.

Étape 3 Entrez l'URL suivante dans votre navigateur :

https://*adresse_ip*/**api**

Précisez l'adresse IP attribuée par le serveur DHCP au port de gestion du châssis.

Étape 4 Lorsque vous y êtes invité, connectez-vous avec le nom d'utilisateur **install** et le mot de passe *numéro_de_série_du_châssis*.

Le *numéro_de_série_du_châssis* se trouve sur un onglet amovible sur le châssis.

Étape 5 Terminez la configuration du système en suivant les invites.

- Politique de mise en application de mots de passe robustes.
- Mot de passe du compte administrateur.
- Nom du système
- Adresse IPv4 et masque de sous-réseau, ou adresse et préfixe IPv6 de gestion du superviseur.
- Adresse IPv4 ou IPv6 de la passerelle par défaut.
- Hôte/adresse de réseau et masque de réseau/préfixe à partir duquel l'accès SSH est autorisé.
- Hôte/adresse réseau et masque réseau/préfixe à partir duquel l'accès HTTPS est autorisé.
- Adresse IPv4 ou IPv6 du serveur DNS.
- Nom de domaine par défaut

Étape 6 Cliquez sur **Submit** (Soumettre).

Effectuez la configuration initiale du châssis dans l'interface de ligne de commande

La première fois que vous accédez à l'interface de ligne de commande FXOS au niveau de la console ou à l'aide d'une session SSH au port de gestion du châssis, un assistant de configuration vous invite à entrer la configuration du réseau de base afin que vous puissiez accéder à gestionnaire de châssis (en utilisant le protocole HTTPS) ou à l'interface de ligne de commande FXOS (en utilisant le protocole SSH) du port de gestion du châssis.

Le port de gestion de châssis obtient une adresse IP en utilisant DHCP. Si vous n'avez pas de serveur DHCP, vous devez utiliser le port de console pour la configuration initiale.

Remarque Pour relancer la configuration initiale, vous devez effacer toute configuration existante à l'aide des commandes suivantes :

```
Firepower-chassis# connect local-mgmt
firepower-chassis(local-mgmt)# erase configuration
```

Avant de commencer

Recueillez les informations suivantes à utiliser avec le script de configuration :

- Nouveau mot de passe de l'administrateur
- Adresse IP de gestion et filtre d'adresse locale
- Adresse IP de la passerelle
- Sous-réseaux à partir desquels vous souhaitez autoriser l'accès HTTPS et SSH
- Nom d'hôte et le nom de domaine
- Adresse IP du serveur DNS

Procédure

Étape 1 Démarrez le châssis.

Étape 2 Connectez-vous au port de console de série à l'aide d'un émulateur de terminal ou utilisez le protocole SSH pour vous connecter au port de gestion du châssis.

Le Firepower 4100 comprend un câble de console de série RS-232 à RJ-45. Vous devrez peut-être utiliser un câble série tiers vers USB pour établir la connexion. Utilisez les paramètres de série suivants :

- 9600 bauds
- 8 bits de données
- Pas de parité
- 1 bit d'arrêt

Étape 3 Lorsqu'on vous y invitera, connectez-vous avec le nom d'utilisateur **admin** et le mot de passe **cisco123**.

Étape 4 Terminez la configuration du système en suivant les invites.

Exemple :

```
          ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Only minimal configuration including IP connectivity to
the FXOS Supervisor is performed through these steps.

Type Ctrl-C at any time for more options or to abort configuration
and reboot system.
To back track or make modifications to already entered values,
complete input till end of section and answer no when prompted
to apply configuration.


You have chosen to setup a new Security Appliance.
      Continue? (yes/no): y

Enforce strong password? (yes/no) [y]: n

Enter the password for "admin": Farscape&32
Confirm the password for "admin": Farscape&32
Enter the system name:  firepower-4125

Supervisor Mgmt IP address : 10.80.6.12

Supervisor Mgmt IPv4 netmask : 255.255.255.0

IPv4 address of the default gateway : 10.80.6.1

The system cannot be accessed via SSH if SSH Mgmt Access is not configured.

Do you want to configure SSH Mgmt Access? (yes/no) [y]: y

SSH Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

SSH Mgmt Access IPv4 netmask: 255.0.0.0

Firepower Chassis Manager cannot be accessed if HTTPS Mgmt Access is not configured.

Do you want to configure HTTPS Mgmt Access? (yes/no) [y]: y

HTTPS Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

HTTPS Mgmt Access IPv4 netmask: 255.0.0.0

Configure the DNS Server IP address? (yes/no) [n]: y

  DNS IP address : 10.164.47.13

Configure the default domain name? (yes/no) [n]: y

  Default domain name : cisco.com

Following configurations will be applied:

  Switch Fabric=A
  System Name=firepower-4125
  Enforced Strong Password=no
  Supervisor Mgmt IP Address=10.89.5.14
```

```
    Supervisor Mgmt IP Netmask=255.255.255.192
    Default Gateway=10.89.5.1
    SSH Access Configured=yes
        SSH IP Address=10.0.0.0
        SSH IP Netmask=255.0.0.0
    HTTPS Access Configured=yes
        HTTPS IP Address=10.0.0.0
        HTTPS IP Netmask=255.0.0.0
    DNS Server=72.163.47.11
    Domain Name=cisco.com

  Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): y
  Applying configuration. Please wait...  Configuration file - Ok
.....

Cisco FPR Series Security Appliance
firepower-9300 login:  admin
Password: Farscape&32
Successful login attempts for user 'admin' : 1
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2019, Cisco Systems, Inc. All rights reserved.

[...]

firepower-chassis#
```

Étape 5 Vous pouvez vous déconnecter du port de console, le cas échéant, ou mettre fin à votre session SSH.

Se connecter au Gestionnaire de châssis

Utilisez le gestionnaire de châssis pour configurer les paramètres du châssis, y compris l'activation des interfaces et le déploiement de dispositifs logiques.

Avant de commencer

- Pour en savoir plus sur les navigateurs pris en charge, consultez les notes de mise à jour pour la version que vous utilisez (http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.html).
- Vous ne pouvez accéder à gestionnaire de châssis qu'à partir d'un ordinateur de gestion avec une adresse IP dans la plage que vous avez spécifiée lors de la configuration initiale du châssis.

Procédure

Étape 1 À l'aide d'un navigateur pris en charge, entrez l'URL suivante.

https://*adresse_ip_de_gestion_du_châssis*

- *adresse_ip_de_gestion_du_châssis* : identifie l'adresse IP ou le nom d'hôte du port de gestion de châssis que vous avez saisi lors de la configuration initiale.

Étape 2 Saisissez le nom d'utilisateur **admin** et un nouveau mot de passe.

Vous pouvez ajouter d'autres utilisateurs ultérieurement conformément à Ajouter des utilisateurs FXOS, à la page 16.

Étape 3 Cliquez sur **Ouvrir une session**.
Vous êtes connecté, et le gestionnaire de châssis s'ouvre pour afficher la page **Overview** (Vue d'ensemble).

Configurer NTP

Bien que vous puissiez définir l'heure manuellement, nous vous recommandons d'utiliser un serveur NTP. Vous devez régler la bonne heure pour la licence logicielle Smart pour l'ASA et pour Défense contre les menaces avec le gestionnaire d'appareil. Pour Défense contre les menaces avec le centre de gestion, l'heure doit correspondre entre le châssis et le centre de gestion. Dans ce cas, nous vous recommandons d'utiliser le même serveur NTP sur le châssis et sur le centre de gestion. N'utilisez pas le centre de gestion lui-même comme serveur NTP; cette méthode n'est pas prise en charge.

Avant de commencer

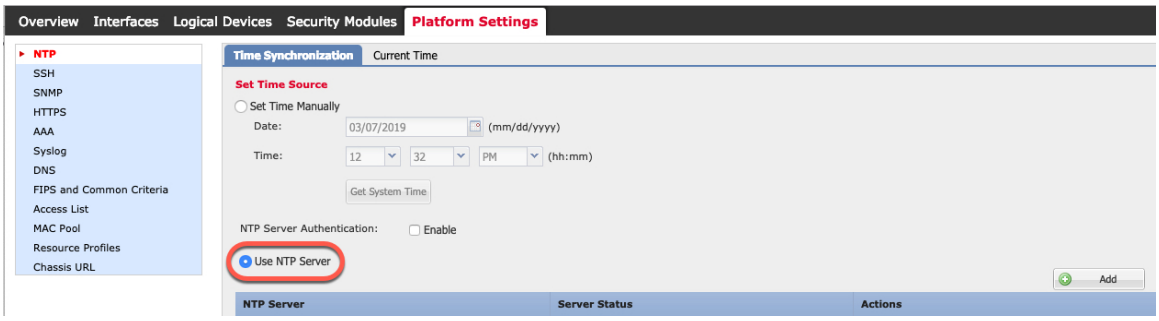
Si vous utilisez un nom d'hôte pour le serveur NTP, vous devez configurer un serveur DNS si vous ne l'avez pas déjà fait durant la configuration initiale. Consultez **Platform Settings (Configurations de plateforme)** > **DNS**.

Procédure

Étape 1 Choisissez **Platform Settings (Configurations de plateforme)** > **NTP**.

La page **Time Synchronization** (Synchronisation de l'heure) est sélectionnée par défaut.

Étape 2 Cliquez sur le bouton radio **Use NTP Server** (Utiliser le serveur NTP).

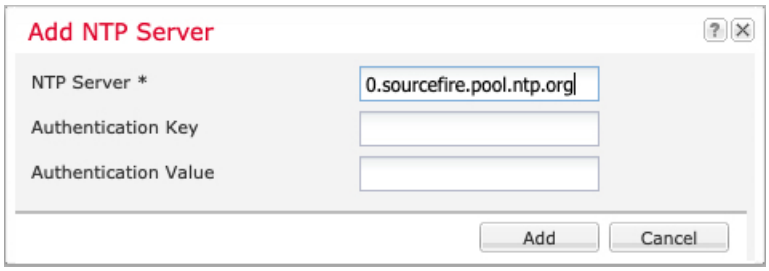


Étape 3 (Facultatif) Cochez la case **NTP Server Authentication: Enable** (Authentification du serveur NTP : activer) si vous devez authentifier le serveur NTP.

Vous serez invité à activer l'authentification NTP. Cliquez sur **Yes** (Oui) pour exiger un identifiant et une valeur de clé d'authentification pour toutes les entrées du serveur NTP.

Seul SHA1 est pris en charge pour l'authentification du serveur NTP.

Étape 4 Cliquez sur **Add** (Ajouter) et réglez les paramètres suivants :



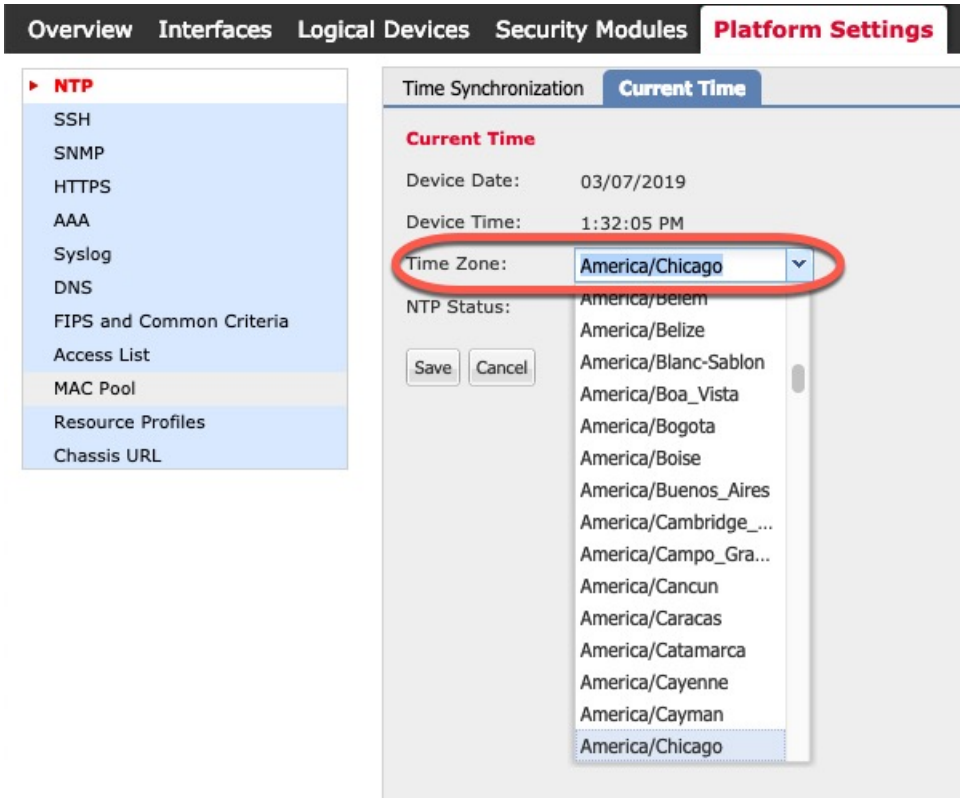
- **NTP Server** (Serveur NTP) : l'adresse IP ou le nom d'hôte du serveur NTP.
- **Authentication Key** et **Authentication Value** (clé et valeur d'authentification) : obtenez l'ID de clé et la valeur du serveur NTP. Par exemple, pour générer la clé SHA1 sur le serveur NTP version 4.2.8p8 ou ultérieure avec OpenSSL installé, saisissez la commande **ntp-keygen -M** , puis affichez l'ID de clé et la valeur dans le fichier ntp.keys. La clé est utilisée pour indiquer au client et au serveur quelle valeur utiliser lors du calcul du condensé du message.

Étape 5 Cliquez sur **Add** (Ajouter) pour ajouter le serveur distant.

Vous pouvez ajouter jusqu'à 4 serveurs NTP.

Étape 6 Cliquez sur **Save** (Enregistrer) pour enregistrer les serveurs.

Étape 7 Cliquez sur **Current Time** (Heure actuelle) et dans la liste déroulante **Time Zone** (Fuseau horaire), choisissez le fuseau horaire approprié pour le châssis.



Étape 8 Cliquez sur **Save** (Enregistrer).

Remarque
Si vous modifiez l'horloge système de plus de 10 minutes, le système vous déconnectera et vous devrez vous reconnecter au gestionnaire de châssis.

Ajouter des utilisateurs FXOS

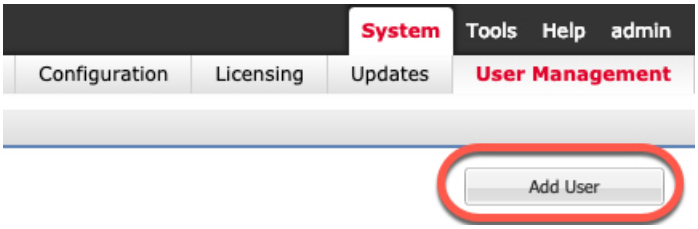
Ajoutez des utilisateurs locaux pour les connexions à gestionnaire de châssis et à l'interface de ligne de commande FXOS.

Procédure

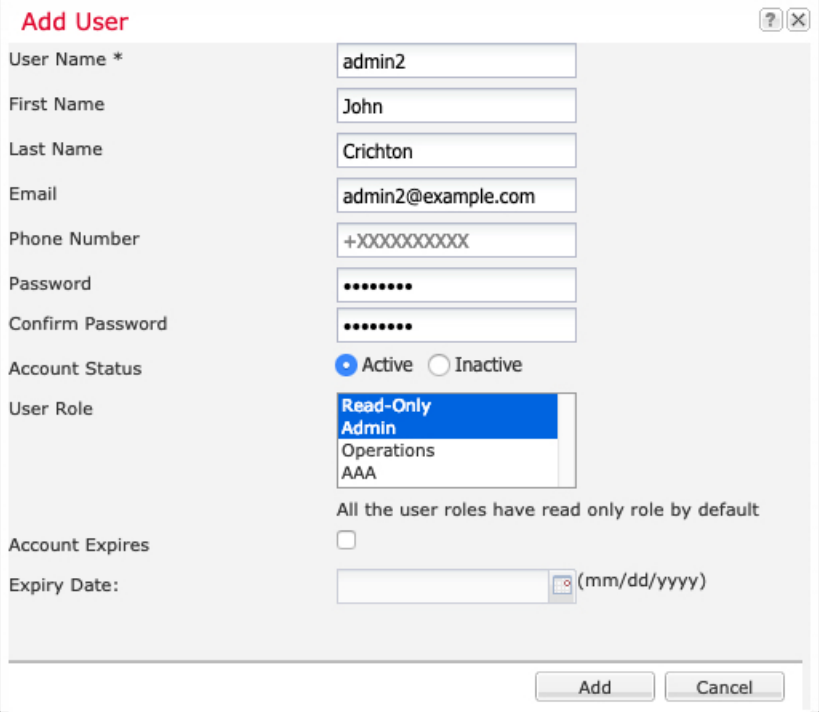
Étape 1 Choisissez **System (Système)** > **User Management (Gestion des utilisateurs)**.

Étape 2 Cliquez sur **Local Users** (Utilisateurs locaux).

Étape 3 Cliquez sur **Add User** (Ajouter un utilisateur) pour ouvrir la boîte de dialogue **Add User** (Ajouter un utilisateur).



Étape 4 Remplir les champs suivants avec les renseignements requis sur l'utilisateur :



- **User Name** (Nom d'utilisateur) : définit le nom d'utilisateur, jusqu'à 32 caractères. Après avoir enregistré l'utilisateur, l'identifiant de connexion ne peut pas être modifié. Vous devez supprimer le compte d'utilisateur et en créer un nouveau.
- (Facultatif) **First Name** (Prénom) : définit le prénom de l'utilisateur, jusqu'à 32 caractères.
- (Facultatif) **Last Name** (Nom de famille) : définit le nom de famille de l'utilisateur, jusqu'à 32 caractères.
- (Facultatif) **Email** (Adresse courriel) : définit l'adresse courriel de l'utilisateur.
- (Facultatif) **Phone Number** (Numéro de téléphone) : définit le numéro de téléphone de l'utilisateur.
- **Password** (Mot de passe) et **Confirm Password** (Confirmer le mot de passe) : définissent le mot de passe associé à ce compte. Si vous activez la vérification de la robustesse du mot de passe, le mot de passe doit être robuste. FXOS rejettera tout mot de passe qui ne répond pas aux exigences de vérification de la robustesse. Consultez le FXOS configuration guide (Guide de configuration FXOS) pour connaître les directives concernant les mots de passe sécurisés.
- **Account Status** (État du compte) : définit l'état sur **Active** (Actif) ou **Inactive** (Inactif).
- **User Role** (Rôle d'utilisateur) : définit le rôle qui représente les privilèges que vous souhaitez attribuer au compte d'utilisateur. Tous les utilisateurs se voient attribuer le rôle **Read-Only** (En lecture seule) par défaut. Ce rôle ne peut pas être désélectionné. Pour attribuer un autre rôle, cliquez sur le nom du rôle dans la fenêtre pour qu'il soit en surbrillance. Vous pouvez utiliser l'un des rôles d'utilisateur suivants :
  - **Admin** (Administrateur) : accès complet en lecture et écriture à l'ensemble du système.
  - **Read-Only** (En lecture seule) : accès en lecture seule à la configuration système sans privilège de modification de l'état du système.

- **Operations** (Opérations) : accès en lecture et écriture à la configuration NTP, à la configuration de Smart Call Home pour les licences Smart et aux journaux du système, y compris aux serveurs de journalisation du système et aux défaillances. Accès en lecture au reste du système.
- **AAA Administrator** (Administrateur AAA) : accès en lecture et écriture aux utilisateurs, aux rôles et à la configuration AAA. Accès en lecture au reste du système.

- (Facultatif) **Account Expires** (Expiration du compte) : définit que ce compte expire. Le compte ne peut pas être utilisé après la date indiquée dans le champ **Expiry Date** (Date d'expiration). Après avoir configuré un compte d'utilisateur avec une date d'expiration, vous ne pouvez pas reconfigurer le compte pour qu'il n'expire pas. Vous pouvez toutefois configurer le compte avec la dernière date d'expiration disponible. Par défaut, les comptes d'utilisateur n'expirent pas.
- (Facultatif) **Expiry Date** (Date d'expiration) : date à laquelle le compte expire. La date doit être au format *aaaa-mm-jj*. Cliquez sur l'icône du calendrier à la fin de ce champ pour afficher un calendrier que vous pouvez utiliser pour sélectionner la date d'expiration.

Étape 5 Cliquez sur **Add** (Ajouter).

Interfaces de configuration

Par défaut, les interfaces physiques sont désactivées. Dans FXOS, vous pouvez activer les interfaces, ajouter des canaux EtherChannel, ajouter des sous-interfaces VLAN et modifier les propriétés de l'interface. Pour utiliser une interface, vous devez l'activer physiquement dans FXOS, puis l'activer logiquement dans l'application.

Pour configurer les ports de répartition, consultez le guide de configuration FXOS.

Types d'interface

Chaque interface est de l'un des types suivants :

- Data (Données) : à utiliser pour les données normales. Les interfaces de données ne peuvent pas être mises en commun entre les dispositifs logiques, et les dispositifs logiques ne peuvent pas communiquer avec d'autres dispositifs logiques par le fond de panier Pour le trafic sur les interfaces de données, tout le trafic doit quitter le châssis sur une interface et revenir sur une autre interface pour atteindre un autre dispositif logique.
- Data-sharing (Partage de données) : à utiliser pour les données normales. Pris en charge uniquement avec les instances de conteneur, ces interfaces de données peuvent être partagées par un ou plusieurs dispositifs logiques/Instances de conteneur (Défense contre les menaces-utilisant-centre de gestion seulement). Chaque instance de conteneur peut communiquer sur le fond de panier avec toutes les autres instances qui partagent cette interface. Les interfaces partagées peuvent avoir une incidence sur le nombre d'instances de conteneur que vous pouvez déployer. Les interfaces partagées ne sont pas prises en charge pour les interfaces de membre de groupe de ponts (en mode transparent ou en mode routage), les ensembles en ligne, les interfaces passives, les grappes, ou les liens de basculement.
- Mgmt (Gestion) : permet de gérer les instances d'application. Ces interfaces peuvent être partagées par un ou plusieurs dispositifs logiques pour accéder à des hôtes externes; les dispositifs logiques ne peuvent pas communiquer sur cette interface avec d'autres dispositifs logiques qui partagent l'interface. Vous ne

pouvez affecter qu'une seule interface de gestion par dispositif logique. En fonction de votre application et de votre gestionnaire, vous pouvez ultérieurement activer la gestion à partir d'une interface de données; mais vous devez attribuer une interface de gestion au dispositif logique même si vous n'avez pas l'intention de l'utiliser après avoir activé la gestion des données.

Remarque La modification de l'interface de gestion entraînera le redémarrage du dispositif logique. Par exemple, une gestion des modifications de e1/1 à e1/2 entraînera le redémarrage du dispositif logique pour appliquer la nouvelle gestion.

- Eventing (Création d'événements) : sert d'interface de gestion secondaire pour les dispositifs Défense contre les menacesqui utilisent le centre de gestion. Pour utiliser cette interface, vous devez configurer son adresse IP et d'autres paramètres au niveau de l'interface de ligne de commande Défense contre les menaces. Par exemple, vous pouvez séparer le trafic de gestion des événements (comme les événements Web). Reportez-vous au guide de configuration du centre de gestion pour obtenir plus de renseignements. Les interfaces d'événements peuvent être partagées par un ou plusieurs dispositifs logiques pour accéder à des hôtes externes. Les dispositifs logiques ne peuvent pas communiquer sur cette interface avec d'autres dispositifs logiques qui partagent l'interface. Si vous configurez ultérieurement une interface de données pour la gestion, vous ne pouvez pas utiliser une interface d'événement distincte.

Remarque Une interface Ethernet virtuelle est attribuée lors de l'installation de chaque instance applicative. Si l'application n'utilise pas d'interface événementielle, l'interface virtuelle sera dans un état "admin down".

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- Cluster (grappe) : à utiliser comme liaison de commande de grappe pour un dispositif logique en grappe. Par défaut, la liaison de commande de grappe est automatiquement créée sur le canal de port 48. Le type de grappe est uniquement pris en charge sur les interfaces EtherChannel. Pour la mise en grappe multi-instances, vous ne pouvez pas partager une interface de type grappe sur plusieurs appareils. Vous pouvez ajouter des sous-interfaces VLAN à la grappe EtherChannel pour fournir des liaisons de commande de grappe distinctes par grappe. Si vous ajoutez des sous-interfaces à une interface Cluster, vous ne pouvez pas utiliser cette interface pour une grappe native. Le gestionnaire d'appareil et CDO ne prend pas en charge le regroupement (clustering).

Vous devez configurer une interface de gestion et au moins une interface de données (ou de partage de données) avant de déployer un dispositif logique.

Configurer une interface physique

Vous pouvez physiquement activer et désactiver les interfaces, ainsi que définir la vitesse d'interface et le mode duplex. Pour utiliser une interface, vous devez l'activer physiquement dans FXOS, puis l'activer logiquement dans l'application.

Avant de commencer

Les interfaces qui sont déjà membres d'un EtherChannel ne peuvent pas être modifiées individuellement. Assurez-vous de configurer les paramètres avant d'ajouter une interface au canal EtherChannel.

Procédure

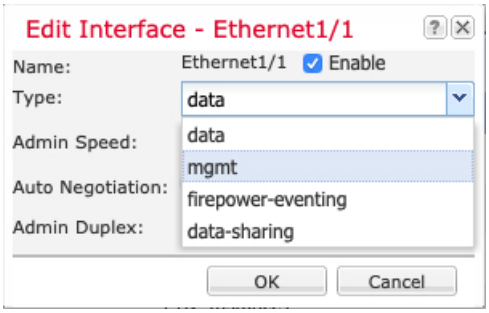
Étape 1 Cliquez sur **Interfaces**.

La page **All Interfaces** (toutes les interfaces) présente une représentation visuelle des interfaces actuellement installées en haut de la page et fournit une liste des interfaces installées dans un tableau (voir ci-dessous).

Étape 2 Cliquez sur **Modifier** ( ) dans la ligne de l'interface à modifier pour ouvrir la boîte de dialogue **Edit Interface** (Modifier l'interface).

Étape 3 Cochez la case **Enable** (activer).

Étape 4 Choisissez le **Type** d'interface : **Data** (Données), **Data-sharing** (Partage de données), **Mgmt** (Gestion) ou **Firepower-eventing** (événement Firepower)



Remarque
Il y a des limites lors de l'utilisation d'interfaces de type partage de données; consultez le FXOS configuration guide (Guide de configuration de FXOS) pour de plus amples renseignements.

Pour Firepower-eventing, consultez le Guide de configuration de Firepower Management Center.

Étape 5 (Facultatif) Choisissez la **Speed** (Vitesse) de l'interface.

Étape 6 (Facultatif) Si votre interface prend en charge la négociation automatique (**Auto Negotiation**), cliquez sur le bouton radio **Yes** (oui) ou **No** (non).

Étape 7 (Facultatif) Choisissez le **Duplex** de l'interface.

Étape 8 Cliquez sur **OK**.

Ajouter un canal EtherChannel (canal de port)

Un EtherChannel (également appelé canal de port) peut inclure jusqu'à 16 interfaces membres de même type de support et de capacité, et doit être réglé à la même vitesse et au même duplex. Le type de support peut être RJ-45 ou SFP. Des SFP de différents types (cuivre et fibre optique) peuvent être mélangés. Vous ne pouvez pas combiner les capacités d'interface (par exemple, interfaces de 1 Go et de 10 Go) en réduisant la vitesse sur l'interface de plus grande capacité.

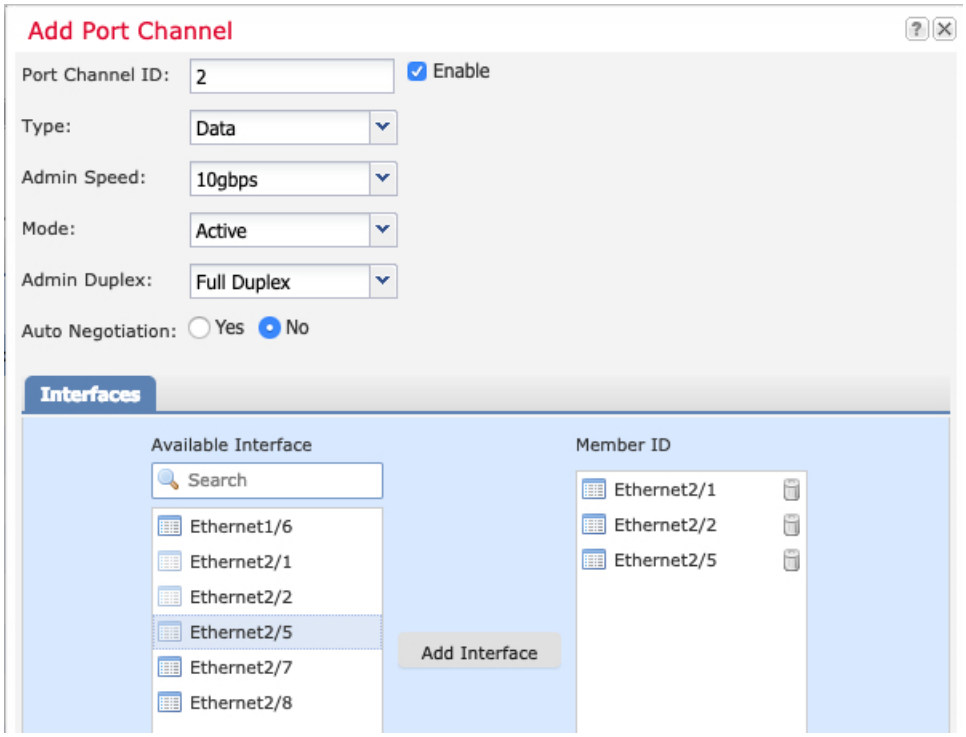
Remarque Lorsque le châssis crée un EtherChannel, l'EtherChannel reste dans un état **Suspended** (En attente) pour le mode LACP actif ou à l'arrêt pour le mode LACP activé jusqu'à ce que vous l'**affectiez** à un dispositif logique, même si la liaison physique est opérationnelle.

Procédure

Étape 1 Cliquez sur **Interfaces**.

La page **All Interfaces** (toutes les interfaces) présente une représentation visuelle des interfaces actuellement installées en haut de la page et fournit une liste des interfaces installées dans un tableau (voir ci-dessous).

Étape 2 Cliquez sur **Add New (Ajouter)** > **Port Channel (Canal de port)**.



Étape 3 Saisissez un **Port Channel ID** (Identifiant de canal de port), compris entre 1 et 47.

Étape 4 Cochez la case **Enable** (activer).

Étape 5 Choisissez le **Type** d'interface :

- **Données**
- **Data-sharing (mise en commun des données)** : pour les instances de conteneur uniquement.
- **Gestion**
- **Firepower-eventing**— Pour défense contre les menaces seulement.
- **Cluster** (Grappe) : pour la mise en grappe seulement.

Remarque
Il y a des limites lors de l'utilisation d'interfaces de type partage de données; consultez le FXOS configuration guide (Guide de configuration de FXOS) pour de plus amples renseignements.

Pour Firepower-eventing, consultez le Guide de configuration de Firepower Management Center.

Étape 6 Définissez l'**Admin Speed** (Vitesse d'administration) des interfaces membres dans la liste déroulante.

Étape 7 Pour les interfaces de données ou de partage de données, choisissez le **mode** du canal de port LACP : **Active** (Actif) ou **On** (Activé).

Pour les interfaces sans données ou qui ne partagent pas de données, le mode est toujours actif. Vous devez utiliser le mode actif, sauf si vous devez réduire au minimum le trafic LACP.

Étape 8 Définissez **Admin Duplex** (Duplex d'administration) dans la liste déroulante.

Étape 9 Pour ajouter une interface au canal de port, sélectionnez l'interface dans la liste **Available Interface** (Interface disponible) et cliquez sur **Add Interface** (Ajouter une interface) pour la déplacer vers la liste **Member ID** (Identification de membre).

Vous pouvez ajouter jusqu'à 16 interfaces.

Astuces
Vous pouvez ajouter plusieurs interfaces en même temps. Cliquez sur les interfaces souhaitées tout en maintenant la touche **Ctrl** enfoncée. Pour sélectionner une plage d'interfaces, sélectionnez la première interface de la plage, puis, tout en maintenant la touche **Shift** (Maj) enfoncée, cliquez pour sélectionner la dernière interface de la plage.

Étape 10 Pour supprimer une interface du canal de port, cliquez sur le **Supprimer** ( ) à droite de l'interface dans la liste **Member ID** (Identification de membre).

Étape 11 Cliquez sur **OK**.

Ajouter une sous-interface VLAN pour les instances de conteneur

Vous pouvez ajouter jusqu'à 500 sous-interfaces à votre châssis. Les sous-interfaces ne sont prises en charge que pour les instances de contenant; pour en savoir plus, consultez Instances d'application du dispositif logique : instance de conteneur ou instance native, à la page 3.

Pour la mise en grappe à instances multiples, vous ne pouvez ajouter des sous-interfaces qu'à l'interface de type grappe; les sous-interfaces des interfaces de données ne sont pas prises en charge.

Les ID de VLAN par interface doivent être uniques et, dans une instance de conteneur, les ID de VLAN doivent être uniques pour toutes les interfaces attribuées. Vous pouvez réutiliser les ID de VLAN sur des interfaces *distinctes*, à condition qu'ils soient affectés à différentes instances de conteneur. Cependant, chaque sous-interface compte toujours dans la limite, même si elle utilise le même ID.

Vous pouvez également ajouter des sous-interfaces dans l'application. Pour plus d'informations sur le moment d'utilisation des sous-interfaces FXOS par rapport aux sous-interfaces d'application, consultez le FXOS configuration guide (Guide de configuration FXOS).

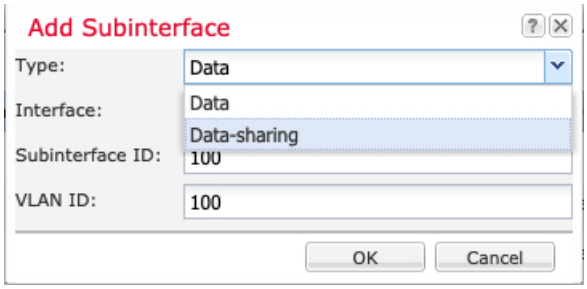
Procédure

Étape 1 Cliquez sur **Interfaces**.

La page **All Interfaces** (toutes les interfaces) présente une représentation visuelle des interfaces actuellement installées en haut de la page et fournit une liste des interfaces installées dans un tableau (voir ci-dessous).

Étape 2 Cliquez sur **Add New** > **Subinterface** (Ajouter une nouvelle sous-interface) pour ouvrir la boîte de dialogue Add **Subinterface (ajouter** une sous-interface).

Étape 3 Choisissez le **Type** d'interface :



- **Données**
- **Partage de données**
- **Grappe** : si vous ajoutez des sous-interfaces à une interface de grappe, vous ne pouvez pas utiliser cette interface pour une grappe native.

Pour les données et les interfaces de partage de données : le type est indépendant du type d'interface parent; vous pouvez avoir un parent de partage de données et une sous-interface de données, par exemple.

Il y a des limites lors de l'utilisation d'interfaces de type partage de données; consultez le FXOS configuration guide (Guide de configuration de FXOS) pour de plus amples renseignements.

Étape 4 Choisissez **l'interface** parente dans la liste déroulante.

Vous ne pouvez pas ajouter une sous-interface à une interface physique qui est actuellement allouée à une unité logique. Si d'autres sous-interfaces du parent sont allouées, vous pouvez ajouter une nouvelle sous-interface tant que l'interface parente elle-même n'est pas allouée.

Étape 5 Entrez **l'ID de la sous-interface** comme un nombre entier entre 1 et 4294967295.

Cet ID sera ajouté à l'ID de l'interface parente sous le nom *identifiant_d_interface***.***identifiant_de_sous_interface*. Par exemple, si vous ajoutez une sous-interface à Ethernet1/1 avec l'ID 100, l'ID de la sous-interface sera : Ethernet1/1.100. Cet ID est différent de l'ID VLAN, bien que vous puissiez définir ces ID pour des raisons de commodité.

Étape 6 Définissez l'**ID VLAN** entre 1 et 4095.

Étape 7 Cliquez sur **OK**.

Développez l'interface parente pour afficher toutes les sous-interfaces qu'elle contient.

Téléverser des images logicielles dans le châssis

Cette procédure décrit comment charger de nouvelles images FXOS et d'application, et comment mettre à niveau l'image FXOS. Vous devrez peut-être charger de nouvelles images si les images préinstallées ne sont pas les versions dont vous avez besoin.

Avant de commencer

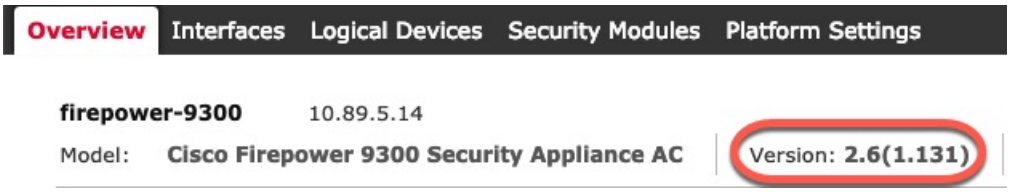
- Vérifiez la compatibilité entre FXOS, l'ASA et les versions Défense contre les menaces dans le FXOS compatibility guide (Guide de compatibilité FXOS).
- Assurez-vous que l'image que vous souhaitez télécharger est disponible sur votre ordinateur local. Pour obtenir FXOS et les logiciels d'application pour Firepower 4100, consultez :

  http://www.cisco.com/go/firepower4100-software
- Pour vous assurer un chargement réussi pendant votre session HTTPS, vous devrez peut-être modifier le délai d'expiration absolu au niveau de l'interface de ligne de commande de FXOS. Le délai d'expiration absolu est de 60 minutes (le maximum), et les téléversements volumineux peuvent prendre plus de 60 minutes. Pour désactiver le délai d'expiration absolu, saisissez :

```
Firepower-chassis# scope security
Firepower-chassis /security # scope default-auth
Firepower-chassis /security/default-auth # set absolute-session-timeout 0
Firepower-chassis /security/default-auth* # commit-buffer
```

Procédure

Étape 1 Vérifiez votre version FXOS actuelle en consultant la page **Overview** (Vue d'ensemble).



Vous pourrez afficher les images des applications actuellement disponibles sur le châssis à l'étape suivante.

Étape 2 Sélectionnez **System** > **Updates**.

La page **Available Updates** (Mises à jour disponibles) affiche une liste des images de l'ensemble de la plateforme FXOS et des applications.

Étape 3 Cliquez sur **Upload Image**(Charger une image) pour ouvrir la boîte de dialogue **Upload Image** (Charger une image).

Étape 4 Cliquez sur **Browse** (Naviguer) pour accéder à l'image à charger et la sélectionner.

Étape 5 Cliquez sur **Upload** (charger). L'image sélectionnée est chargée sur le châssis.

La boîte de dialogue **Upload Image** (Charger une image) affiche une barre de progression, puis une boîte de dialogue **Success** (Réussite) à la fin du chargement de l'image.

Étape 6 Pour mettre à niveau l'image FXOS :

a) Cliquez sur le Icône mise à niveau ( ) de l'offre groupée de la plateforme FXOS vers laquelle vous souhaitez effectuer la mise à niveau.

b) Cliquez sur **Yes** (Oui) pour confirmer que vous souhaitez poursuivre l'installation.

Le châssis se recharge. Le processus de mise à niveau prend généralement entre 20 et 30 minutes.

Historique de FXOS

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Sous-interfaces VLAN à utiliser avec des instances de conteneur	2.4.1	Pour fournir une utilisation flexible de l'interface physique, vous pouvez créer des sous-interfaces VLAN dans FXOS et également partager des interfaces entre plusieurs instances. **Remarque** Nécessite la version 6.3 ou une version ultérieure de défense contre les menaces. Écrans Nouveaux ou modifiés : **Interfaces** > **All Interfaces (Toutes les interfaces)** > **Add New (Ajouter)** menu déroulant > **Subinterface (Sous-interface)** Écrans Nouveaux ou modifiés de centre de gestion : **Devices (dispositifs)** > **Device Management (Gestion des dispositifs)** > **icône Edit (Modifier)** > **Interfaces**
Interfaces de partage de données pour les instances de conteneurs	2.4.1	Pour fournir une utilisation de l'interface physique flexible, vous pouvez partager des interfaces entre plusieurs instances. **Remarque** Nécessite la version 6.3 ou une version ultérieure de défense contre les menaces. Écrans Nouveaux ou modifiés : **Interfaces** > **All Interfaces (Toutes les interfaces)** > **Type**
Prise en charge des données EtherChannel en mode activé	2.4.1	Vous pouvez maintenant définir les données et les EtherChannel de partage de données en mode LACP actif ou en mode Activé. Les autres types d'EtherChannel ne prennent en charge que le mode actif. Écrans Nouveaux ou modifiés : **Interfaces** > **All Interfaces (Toutes les interfaces)** > **Edit Port Channel (Modifier le canal de port)** > **Mode**
Prise en charge des EtherChannel dans les ensembles en ligne défense contre les menaces	2.1.1	Vous pouvez désormais utiliser les EtherChannel dans l'ensemble en ligne défense contre les menaces.

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Prise en charge de la propagation de l'état de la liaison défini en ligne pour défense contre les menaces	2.0.1	Lorsque vous configurez un ensemble en ligne dans l'application défense contre les menaces et activez la propagation de l'état de la liaison, défense contre les menaces envoie l'appartenance à l'ensemble en ligne au châssis FXOS. La propagation de l'état de la liaison signifie que le châssis met automatiquement hors service la deuxième interface de la paire d'interfaces en ligne lorsque l'une des interfaces d'un ensemble en ligne tombe en panne. Commandes FXOS nouvelles ou modifiées : **show fall |grep link-down**, **show interface detail**
Prise en charge des modules de réseau de contournement du matériel pour défense contre les menaces	2.0.1	Le contournement matériel garantit que le trafic continue de circuler entre une paire d'interfaces en ligne pendant une panne de courant. Cette fonctionnalité peut servir à maintenir la connectivité du réseau en cas de défaillance matérielle ou logicielle. Écrans Nouveaux ou modifiés de centre de gestion : **Devices (Dispositifs)** > **Device Management (Gestion des dispositifs)** > **Interfaces** > **Edit Physical Interface (Modifier les interfaces physiques)**
Interface de type firepower-eventing pour défense contre les menaces	1.1.4	Vous pouvez spécifier une interface comme événement firepower-eventing à utiliser avec défense contre les menaces. Cette interface est une interface de gestion secondaire pour les dispositifs défense contre les menaces. Pour utiliser cette interface, vous devez configurer son adresse IP et d'autres paramètres à l'aide de l'interface de ligne de commande défense contre les menaces. Par exemple, vous pouvez séparer le trafic de gestion des événements (comme les événements Web). Consultez la section « Management Interfaces » (Interfaces de gestion) dans le chapitre *System Configuration* (Configuration système) du guide de configuration centre de gestion. Écrans Nouveaux ou modifiés de gestionnaire de châssis : **Interfaces** > **All Interfaces (Toutes les interfaces)** > **Type**

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.