Configurez Secure Firewall Management Center sans Eth0 comme Mgmt

Table des matières

Introduction

Ce document décrit comment configurer le Centre de gestion de pare-feu sécurisé (FMC) avec un port différent au lieu de l'interface Eth0 par défaut.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de Cisco Secure Firewall Management Center (anciennement Firepower Management Center)
- Connaissance des réseaux de base

Composants utilisés

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

- Cisco Secure Firewall Management Center (FMC 1000, 1600, 2500, 2600, 4500, 4600 et virtuel) exécutant la version logicielle 5.x 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

À propos de Management Connection sur Secure Firewall Management Center

Après avoir configuré le périphérique avec les informations FMC et après avoir ajouté le périphérique au FMC, soit le périphérique, soit le FMC peut établir la connexion de gestion. Selon la configuration initiale :

- Le périphérique ou le FMC peut démarrer.
- Seul le périphérique peut démarrer.
- Seul le FMC peut démarrer.

L'initialisation provient toujours de eth0 sur le FMC ou avec l'interface de gestion dont le numéro est le plus bas sur le périphérique. Des interfaces de gestion supplémentaires sont essayées si la connexion n'est pas établie. Plusieurs interfaces de gestion sur le FMC vous permettent de vous connecter à des réseaux discrets ou de séparer le trafic de gestion et d'événements. Cependant, l’initiateur ne choisit pas la meilleure interface en fonction de la table de routage.

L'interface interne étiquetée Management (Eth0) est une interface 1 Gigabit Ethernet intégrée au châssis du périphérique. Certains modèles de châssis FMC disposent d'un logement d'extension pouvant accueillir une carte d'extension de module réseau, qui peut être en cuivre ou en fibre optique, et jusqu'à 10 Gigabit. Certains ports intégrés au châssis peuvent prendre en charge des émetteurs-récepteurs SFP+ 10 Gigabit Ethernet.

Cette figure illustre le panneau arrière du FMC 1000.

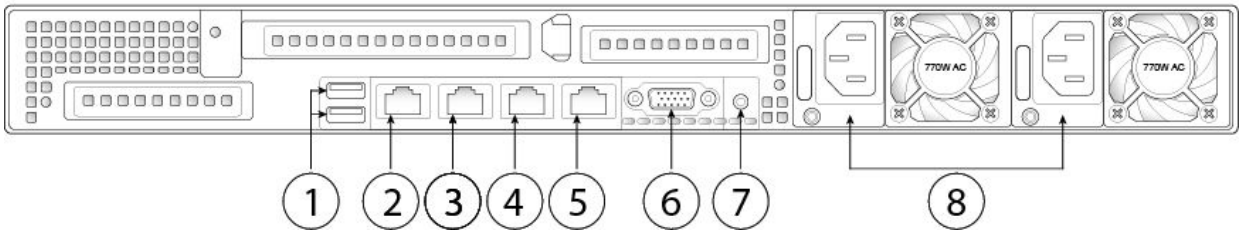

Figure 1. Panneau arrière du FMC 1000

1	2 ports clavier USB Vous pouvez connecter un clavier et, avec un	2	Interface CIMC (étiquetée « M »)

	moniteur sur le port VGA, vous pouvez accéder à la console.		Cette interface n'est pas prise en charge.
3	Port de console série Ce port est désactivé par défaut ; utilisez plutôt le port VGA et le port USB du clavier.	4	Interface de gestion eth0 (étiquetée « 1 ») Interface Gigabit Ethernet 10/100/1000 Mbits/s, RJ-45 eth0 est l'interface de gestion par défaut.
5	Interface de gestion eth1 (étiquetée « 2 ») Interface Gigabit Ethernet 10/100/1000 Mbits/s, RJ-45	6	interface VGA Activé par défaut.
7	Bouton/voyant d'identification	8	Deux modules d'alimentation CA 770 W

Cette figure illustre le panneau arrière des modèles FMC 2500 et 4500.

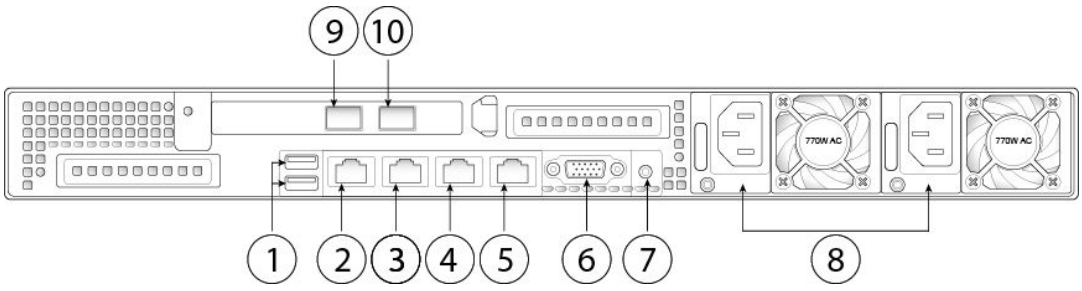

Figure 2. Panneau arrière des FMC 2500 et 4500

1	2 ports clavier USB Vous pouvez connecter un clavier et, avec un moniteur sur le port VGA, vous pouvez accéder à la console.	2	Interface CIMC (étiquetée « M ») Cette interface n'est pas prise en charge.

3	Port de console série Ce port est désactivé par défaut ; utilisez plutôt le port VGA et le port USB du clavier.	4	Interface de gestion eth0 (étiquetée « 1 ») Interface Gigabit Ethernet 10/100/1000 Mbits/s, RJ-45 eth0 est l'interface de gestion par défaut.
5	Interface de gestion eth1 (étiquetée « 2 ») Interface Gigabit Ethernet 10/100/1000 Mbits/s, RJ-45	6	interface VGA Activé par défaut.
7	Bouton/voyant d'identification	8	Deux modules d'alimentation CA 770 W
9	Interface de gestion eth2 Remarque : Utilisez uniquement des émetteurs-récepteurs SFP+ pris en charge par Cisco.	10	Interface d'administration eth3 Remarque : Utilisez uniquement des émetteurs-récepteurs SFP+ pris en charge par Cisco.

Cette figure illustre le panneau arrière des modèles FMC 1600, 2600 et 4600.

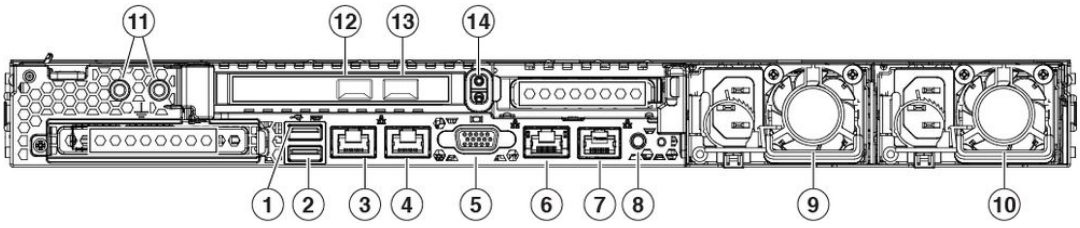

Figure 3. Panneau arrière des FMC 1600, 2600 et 4600

1	USB 3.0 de type A (USB 1)	2	USB 3.0 de type A (USB 2)

	Vous pouvez connecter un clavier et, avec un moniteur sur le port VGA, vous pouvez accéder à la console.		Vous pouvez connecter un clavier et, avec un moniteur sur le port VGA, vous pouvez accéder à la console.
3	Interface de gestion eth0 (étiquetée 1) Prise en charge de 100/1000/10000 Mbits/s en fonction des capacités du partenaire de liaison.	4	Interface de gestion eth1 (étiquetée 2) Interface Gigabit Ethernet 100/1000/10000 Mbits/s, RJ-45, LAN2
5	Port vidéo VGA (connecteur DB-15)	6	Interface CIMC (étiquetée M) Remarque : CIMC est pris en charge uniquement pour l'accès LOM. CIMC n'est pris en charge sur aucune autre interface.
7	Port de console série (connecteur RJ-45) Désactivé par défaut ; utilisez plutôt le port VGA et le port USB du clavier. Pour plus d'informations sur le port série, consultez la rubrique « Configurer l'accès série » dans le Guide de démarrage de Cisco Firepower Management Center pour les modèles 1600, 2600 et 4600 .	8	Bouton d'identification
9	Bloc d'alimentation CA 770 W (PSU 1)	10	Bloc d'alimentation CA 770 W (PSU 2)
11	Trous filetés pour cosse de mise à la	12	Interface de gestion eth2

	terre à deux trous		(Facultatif) Prise en charge du module SFP+ 10 Gigabit Ethernet Les modules SFP-10G-SR et SFP-10G-LR peuvent être utilisés sur le FMC.
13	Interface d'administration eth3 (Facultatif) Prise en charge du module SFP+ 10 Gigabit Ethernet Les modules SFP-10G-SR et SFP-10G-LR peuvent être utilisés sur le FMC.	14	Poignée de montage Non pris en charge

Documentation connexe

Pour obtenir des instructions détaillées sur l'installation matérielle, reportez-vous au Guide d'installation matérielle de Cisco Firepower Management Center 1600, 2600 et 4600.

Pour obtenir la liste complète de la documentation de la gamme Cisco Secure Firewall et savoir où la trouver, reportez-vous au plan de documentation.

Pré-configuration

Installer le Secure Firewall Management Center pour les versions 6.5 et ultérieures

Pour obtenir des instructions d'installation détaillées, reportez-vous au Guide de démarrage de Cisco Firepower Management Center 1600, 2600 et 4600, jusqu'à l'étape Connexion des câbles Mise sous tension Vérification de l'état de l'alimentation pour les versions 6.5 et ultérieures. Connectez le câble sur l'interface requise en vous basant sur les schémas arrière.

Configuration initiale de Secure Firewall Management Center à l'aide de la CLI pour les versions 6.5 et ultérieures

Effectuez la configuration initiale de Management Center à l'aide de l'interface de ligne de commande détaillée dans le document Configuration initiale de Management Center à l'aide de l'interface de ligne de commande pour les versions 6.5 et ultérieures en 8 étapes.

Modifier l'interface de gestion via la CLI de console

Procédure

1. Connectez-vous au centre de gestion virtuel sur la console en utilisant admin comme nom d'utilisateur et mot de passe pour le compte admin que vous avez défini lors de la configuration initiale. Notez que le mot de passe est sensible à la casse.
2. Utilisez la commande expert pour passer en mode shell Linux.
3. Modifiez le fichier ims.conf à l'aide de l'éditeur vi avec la commande sudo vi /etc/sf/ims.conf:

Figure 4

4. Utilisez les touches fléchées de votre clavier et recherchez la ligne MANAGEMENT=eth0 :

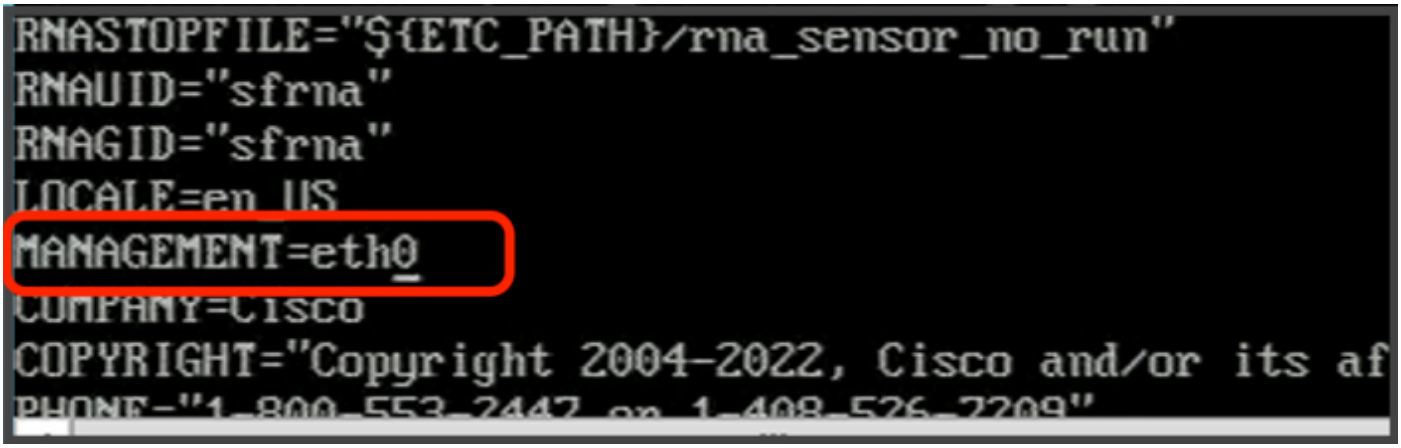

Figure 5

5. Passez en mode INSERT pour éditer en tapant la touche "I", la ligne inférieure à l'écran peut confirmer avec le message INSERT que nous sommes en mode édition, et remplacez eth0 par l'interface conçue, utilisez les tableaux précédents comme référence :

Figure 6

6. Appuyez sur la touche Échap du clavier pour quitter le mode INSERTION et utilisez les deux-points « : » pour passer en mode commande, tapez « wq ! » pour enregistrer les modifications et quitter le fichier :

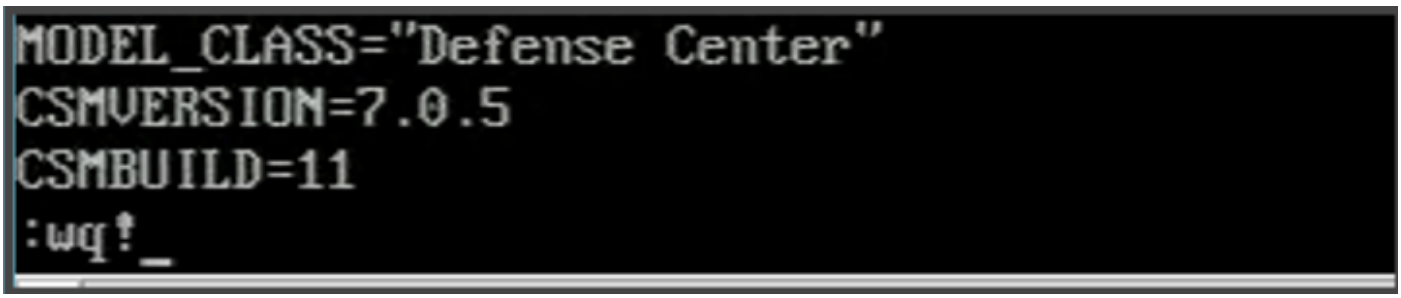

Figure 7

7. Désactivez l'interface eth0 avec la commande sudo ip link set eth0 down :

Figure 8

8. Exécutez l'Assistant Configuration du réseau pour saisir à nouveau l'adresse IP, le masque de réseau et l'adresse de passerelle avec la commande sudo usr/local/sf/bin/configure-network, cette commande peut créer l'interface et attribuer une route par défaut :

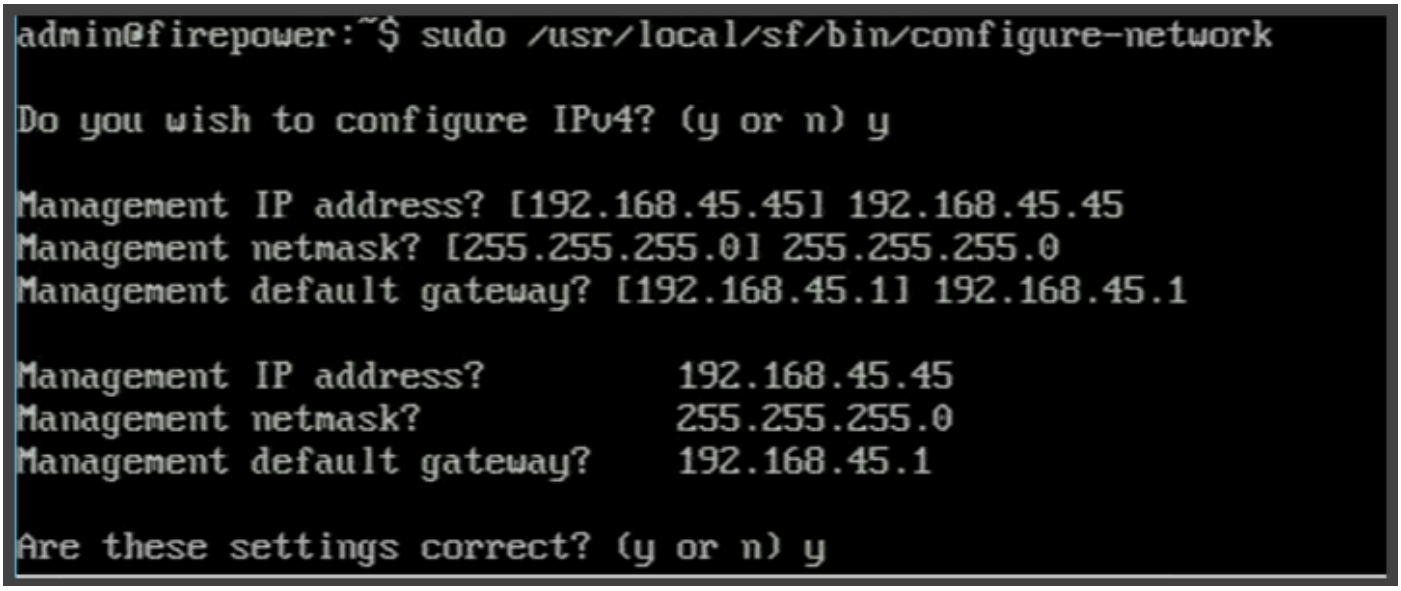

Figure 9

9. Quittez le mode shell Linux avec la commande exit.

Vérifier

Pour vérifier si l'interface sélectionnée a été activée, procédez comme suit :

1. Exécutez la commande sudo route -n à partir du mode shell Linux pour confirmer la table de routage par défaut pour la nouvelle interface de gestion :

Figure 10

Dépannage

Si la nouvelle interface n’est pas renseignée dans la table de routage, validez ceci :

1. Vérifiez que vous avez désactivé l'interface eth0 avec la commande sudo ifconfig.
2. Si l'interface est toujours activée, exécutez à nouveau l'étape 7.
3. Exécutez à nouveau le script configure network à l'étape 8 pour générer la configuration d'interface et la route par défaut.

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.