Modifier l'interface de données d'accès FTD Manager

Table des matières

Introduction

Ce document décrit les étapes à suivre pour modifier l'interface de données d'accès du gestionnaire Secure Firewall Threat Defense (FTD).

Conditions préalables

Exigences

- Connaissances de base sur les produits.
- Connaissance de la gestion FTD et de la gestion des interfaces de données.

Composants utilisés

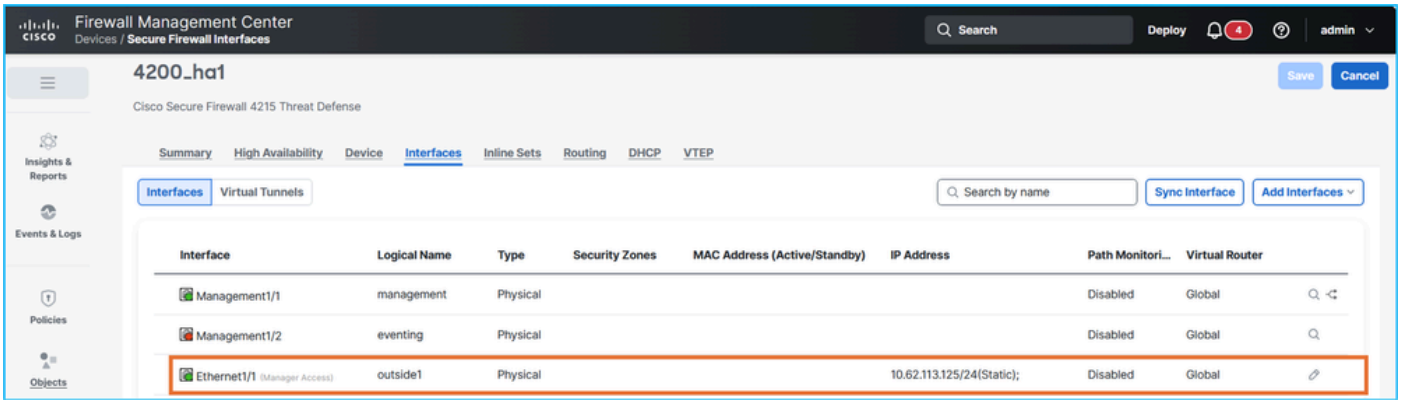
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

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

- Pare-feu sécurisé 4200
- Protection pare-feu sécurisée contre les menaces (FTD) 10.0.x, 7.6.4
- Centre de gestion du pare-feu sécurisé (FMC) 10.0.x

Configuration initiale

1. Le FMC gère le FTD en haute disponibilité (HA) via l'interface de données Ethernet1/1 avec le nom if outside1, en utilisant les adresses IP actives et de secours 10.62.113.125 et 10.62.113.126 respectivement :



Vérification sur FTD CLISH :

<#root>

>

show network management-data-interface

Physical Interface Name of the Interface

Ethernet1/1 outside1

>

show network

```
===============[ System Information ]===============
Hostname                  : CSF4215-3
..
DNS from router           : enabled
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces
…
======[ System Information - Data Interfaces ]======
DNS Servers               : 192.0.2.100

Interfaces                : Ethernet1/1



==================[

Ethernet1/1

 ]===================

State                     : Enabled
Link                      : Up

Name                      : outside1


MTU                       : 1500
MAC Address               : 40:F4:9F:3D:5A:0E

----------------------[ IPv4 ]----------------------



Configuration             : Manual



Address                   : 10.62.113.125



Netmask                   : 255.255.255.0



Gateway                   : 10.62.113.1


…
```

2. Les connexions sftunnel sont établies entre l'unité FTD HA et le FMC :

<#root>

>

sftunnel-status-brief

PEER:fmc.example.org

SFTunnel Status:-

Channel A: Connected

Channel B: Connected

Peer channel Channel-A is valid type (CONTROL), using 'tap_nlp', connected to '198.51.100.23' v
Peer channel Channel-B is valid type (EVENT), using 'tap_nlp', connected to '198.51.100.23' vi
Registration: Completed.
IPv4 Connection to peer 'fmc.example.org' Start Time: Fri Jul 17 08:22:31 2026 UTC
Heartbeat Send Time: Fri Jul 17 08:52:42 2026 UTC
Heartbeat Received Time: Fri Jul 17 08:53:03 2026 UTC
Last disconnect time : Fri Jul 17 08:22:16 2026 UTC
Last disconnect reason : Process shutdown due to stop request from PM

3. FTD s’appuie sur la résolution DNS pour se connecter à FMC. Le gestionnaire est configuré en fonction du nom de domaine complet (FQDN) :

<#root>

>

show managers

Type : Manager

Host : fmc.example.org

```
Display name              : fmc.example.org


Version                   : 10.0.1 (Build 1)
Identifier                : 6d86efc4-c095-11f0-9244-48f1a7894b18
Registration              : Completed
Management type           : Configuration and analytics

>

show network


===============[ System Information ]===============
Hostname                  : KSEC-FPR-4215-3

Domains                   : example.org



DNS Servers               : 192.0.2.100


DNS from router           : enabled
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces
…
```

Les serveurs DNS sont accessibles via l'interface outside1.

4. Les connexions sftunnel sont établies via le moteur Lina :

<#root>

```
>

show conn all port 8305


26 in use, 32 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect


TCP nlp_int_tap  10.62.113.125(169.254.1.3):8305 outside1  198.51.100.23:45647, idle 0:00:03, bytes 2129
```

```
TCP nlp_int_tap  10.62.113.125(169.254.1.3):37141 outside1  198.51.100.23:8305, idle 0:00:04, bytes 1485
```

Configuration Steps

L'objectif est de déplacer l'accès du gestionnaire de l'interface outside1 actuelle vers l'interface outside2 cible. Les adresses IP active et de secours outside2 sont respectivement 10.62.114.51/24 et 10.62.114.52/24.

Notez que les versions FTD 7.7.0 ou ultérieures prennent en charge les interfaces de données d'accès au gestionnaire redondantes, qui permettent la configuration et le déploiement de plus d'une interface d'accès au gestionnaire. Cette fonctionnalité n'est pas prise en charge dans les versions antérieures à 7.7.0.

Pour cette raison, des étapes spécifiques sont ignorées ou contiennent des actions différentes.

⚠ Mise en garde : N'annulez pas l'inscription/la suppression des FTD du FMC à aucune étape.

1. Il est recommandé de disposer d'un accès console aux FTD :

- Dans le cas de Firepower 4100/9300, vous pouvez vous connecter au châssis à l'aide de SSH, puis vous connecter à la console FTD native à l'aide de la commande connect module x console, où x est l'ID du logement/module de sécurité.
- Dans le cas de Firepower 4100/9300 exécutant FTD en mode multi-instance (MI), vous pouvez vous connecter au châssis à l'aide de SSH, puis vous connecter à la console FTD native à l'aide de la commande connect module x telnet, où x est l'ID du logement/module de sécurité. Connectez-vous ensuite à l'instance FTD à l'aide de la commande connect ftd <ftd_id>.
- Dans le cas de Secure Firewall 3100/4200 en mode MI, vous pouvez vous connecter au châssis à l'aide de SSH, puis vous connecter à la console FTD à l'aide de la commande connect ftd <identifier>.

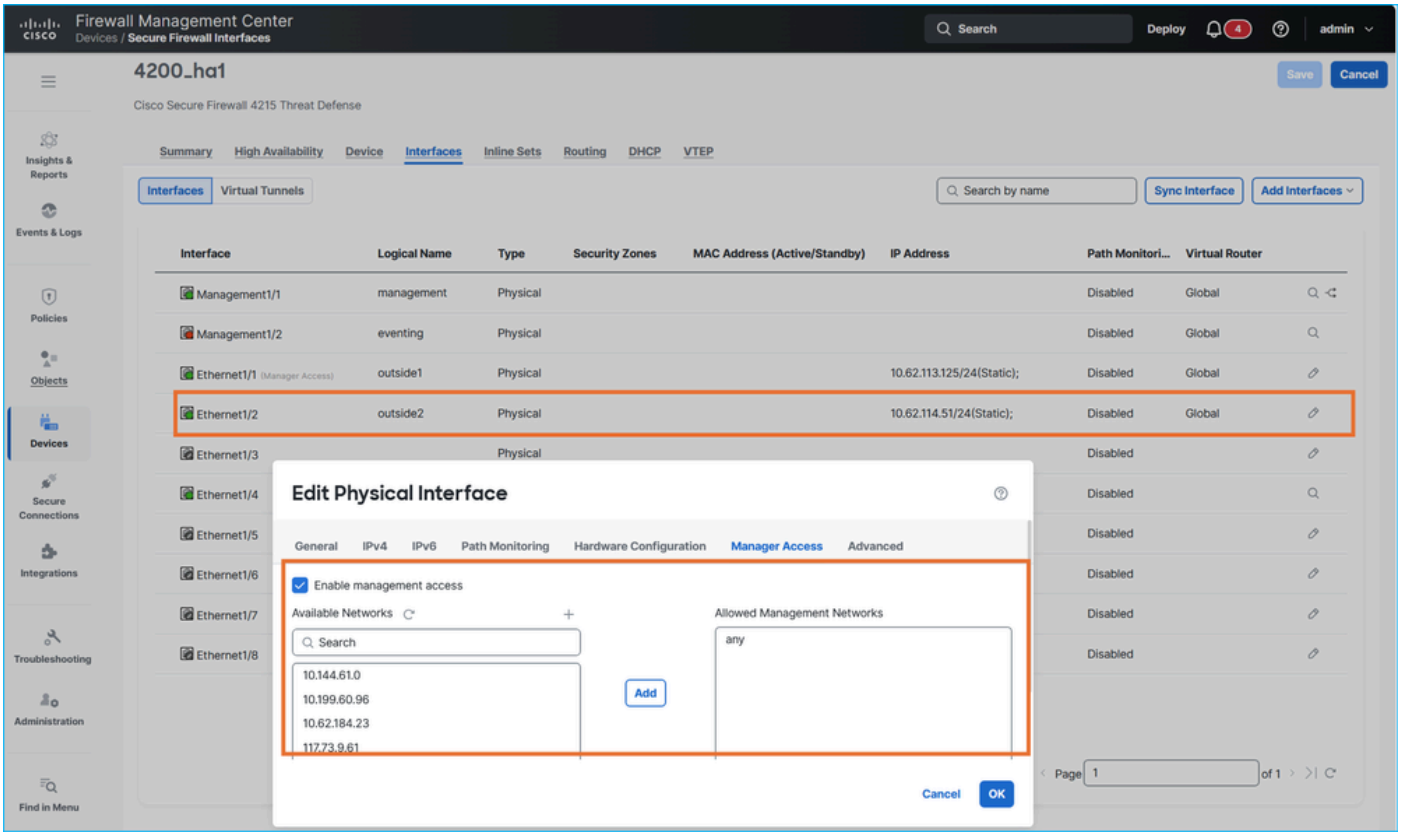
2. Déployer les stratégies en attente.

3. Il est fortement recommandé de prendre des sauvegardes FTD et FMC. Dans le cas de FTD HA, prendre le renfort des deux unités.

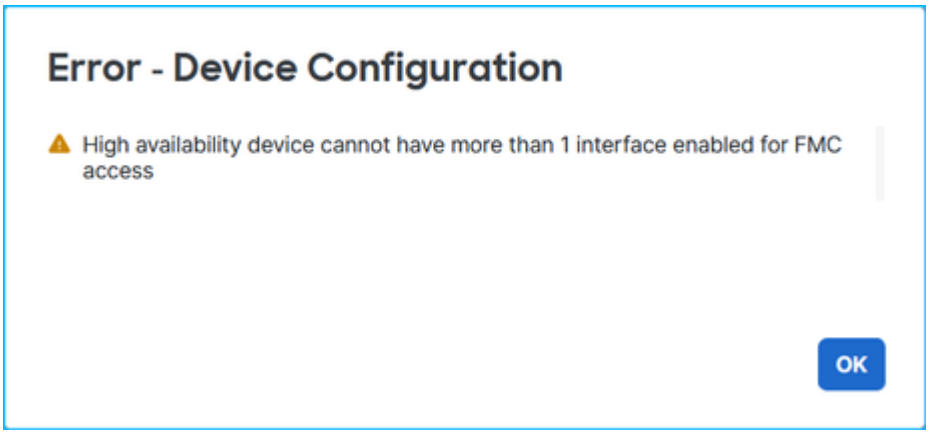
4. Configurez le nom de l'interface cible, l'adresse IP, la zone de sécurité et d'autres paramètres liés à l'interface, le cas échéant.

5. Configurez l'adresse IP de secours de l'interface cible.

6. Si la version du logiciel FTD est 7.7.0 ou ultérieure, activez l'accès au gestionnaire sur l'interface cible et ajustez les réseaux d'accès à la gestion selon les besoins :



Notez que les versions FTD antérieures à la version 7.7.0 ne prennent pas en charge les interfaces de données d'accès au gestionnaire redondantes. La tentative de configuration de la seconde interface d'accès du gestionnaire entraîne le message d'erreur suivant :



Veillez à ignorer les étapes 7 et 8 pour les versions FTD antérieures à 7.7.0.

7. Déployez les stratégies et vérifiez les paramètres sur le FTD CLISH. Dans cet exemple, l'interface Ethernet1/2 avec le nom if outside2 a les adresses IP 10.62.114.51 et 10.62.114.52 respectivement :

```
<#root>

>

show ip


System IP Addresses:
Interface                Name                IP address      Subnet mask     Method
Ethernet1/1              outside1            10.62.113.125   255.255.255.0   manual <- source interf

Ethernet1/2              outside2            10.62.114.51    255.255.255.0   manual

<- target interface
Ethernet1/4              fover               10.9.0.21       255.255.255.0   unset
```

L'interface outside2 est ajoutée à la configuration sftunnel :

```
<#root>

>

show running-config sftunnel


sftunnel interface outside2
```

```
<- target interface

sftunnel interface outside1

<- source interface
sftunnel port 8305
sftunnel route-map FMC_GEN_19283746_RBD_DUAL_WAN_RMAP_91827346
```

Bien que des règles supplémentaires soient installées dans la table de traduction d'adresses de réseau (NAT), les règles avec l'interface outside1 sont utilisées :

<#root>

```
>

show nat detail


Manual NAT Policies Implicit (Section 0)
1 (nlp_int_tap) to (outside1) source static nlp_server__sftunnel_0.0.0.0_intf5 interface  destination s
    translate_hits = 1448, untranslate_hits = 1448
    Source - Origin: 169.254.1.3/32, Translated: 10.62.113.125/24
    Destination - Origin: 0.0.0.0/0, Translated: 0.0.0.0/0
    Service - Protocol: tcp Real: 8305 Mapped: 8305

2 (nlp_int_tap) to (outside2) source static nlp_server__sftunnel_0.0.0.0_intf6 interface  destination st


    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 169.254.1.3/32, Translated: 10.62.114.51/24
    Destination - Origin: 0.0.0.0/0, Translated: 0.0.0.0/0
    Service - Protocol: tcp Real: 8305 Mapped: 8305
3 (nlp_int_tap) to (outside1) source static nlp_server__sftunnel_::_intf5 interface ipv6  destination s
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: fd00:0:0:1::3/128, Translated:
    Destination - Origin: ::/0, Translated: ::/0
    Service - Protocol: tcp Real: 8305 Mapped: 8305
4

(nlp_int_tap) to (outside2) source static nlp_server__sftunnel_::_intf6 interface ipv6  destination stat


    translate_hits = 0, untranslate_hits = 0
    Source - Origin: fd00:0:0:1::3/128, Translated:
    Destination - Origin: ::/0, Translated: ::/0
    Service - Protocol: tcp Real: 8305 Mapped: 8305
5 (nlp_int_tap) to (outside1) source dynamic nlp_client_0_intf5 interface
    translate_hits = 653, untranslate_hits = 0
    Source - Origin: 169.254.1.3/32, Translated: 10.62.113.125/24
6

(nlp_int_tap) to (outside2) source dynamic nlp_client_0_intf6 interface
```

```
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 169.254.1.3/32, Translated: 10.62.114.51/24
7 (nlp_int_tap) to (outside1) source dynamic nlp_client_0_ipv6_intf5 interface ipv6
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: fd00:0:0:1::3/128, Translated:
8
```

(nlp_int_tap) to (outside2) source dynamic nlp_client_0_ipv6_intf6 interface ipv6

```
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: fd00:0:0:1::3/128, Translated:
```

8. Vérifiez l'état de haute disponibilité et la surveillance des interfaces :

<#root>

>

show monitor-interface

This host: Primary - Active

```
        Interface management (203.0.113.130): Normal (Monitored)
        Interface outside1 (10.62.113.125): Normal (Monitored)
        Interface outside2 (10.62.114.51): Normal (Monitored)
```

Other host: Secondary - Standby Ready

```
        Interface management (203.0.113.131): Normal (Monitored)
        Interface outside1 (10.62.113.126): Normal (Monitored)
        Interface outside2 (10.62.114.52): Normal (Monitored)
```

9. Si vous prévoyez de gérer les FTD sur l'interface outside2, assurez-vous que l'accès dans la section Accès SSH des paramètres de la plate-forme est autorisé.

10. Effectuez les modifications nécessaires pour permettre la connectivité sur l'interface cible aux serveurs de noms de domaine (DNS) et FMC :

- Si la résolution de noms de domaine (DNS) est requise pour la connectivité entre FMC et les

FTD, assurez-vous que les FTD sont accessibles sur l'interface cible jusqu'au prochain saut utilisé pour atteindre les serveurs DNS. La résolution DNS doit également être autorisée dans le chemin de transit.
- Assurez-vous que les FTD sont accessibles sur l'interface cible jusqu'au prochain saut à utiliser pour atteindre FMC.
- Assurez-vous que la connectivité bidirectionnelle entre FMC et FTD sur le port TCP 8305 est autorisée dans le chemin de transit sur l'interface cible. La connexion doit être autorisée dans les deux sens.

Dans ce cas, IP 10.62.114.1 doit être utilisé comme passerelle par défaut sur l'interface cible. L'adresse IP du tronçon suivant est accessible à l'aide du protocole ICMP (Internet Control Message Protocol) :

```
<#root>

>

ping 10.62.114.1


Please use 'CTRL+C' to cancel/abort...

Sending 5, 100-byte ICMP Echos to 10.62.114.1, timeout is 2 seconds:



!!!!!


Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Si ICMP est bloqué administrativement dans le chemin de transit ou le saut suivant, assurez-vous que l'adresse MAC (Media Access Control) du saut suivant est visible dans le résultat de la commande show arp et est valide :

```
<#root>

>

show arp


        fover 10.9.0.22 4c01.f7e9.e111 13275
        outside1 10.62.113.1 c02c.1782.2cbf 1
        outside1 10.62.113.126 4c01.f7e9.e10e 5453
```

```
outside2 10.62.114.1 c02c.1782.2cbf 0


        outside2 10.62.114.52 4c01.f7e9.e10f 5453
```

11. Effectuez ces étapes en fonction de la version FTD :

- Version 7.7.0 ou ultérieure : sur FMC, désactivez l'accès du gestionnaire sur l'interface source (outside1), ajustez le routage, y compris le routage vers les serveurs DNS (si DNS est utilisé pour accéder à FMC) et FMC sur l'interface cible (outside2). Par exemple, configurez des routes statiques spécifiques ou configurez la passerelle par défaut sur l'interface cible.
- Version antérieure à 7.7.0 : sur FMC, désactivez l'accès du gestionnaire sur l'interface source (outside1), activez l'accès du gestionnaire sur l'interface cible (outside2), ajustez le routage, y compris le routage vers les serveurs DNS (si DNS est utilisé pour accéder à FMC) et FMC sur l'interface cible (outside2). Par exemple, configurez des routes statiques spécifiques ou configurez la passerelle par défaut sur l'interface cible.

12. Déployez des stratégies.

13. Vérifiez sur FTD CLISH :

```
<#root>

>

show route 0.0.0.0



Routing entry for 0.0.0.0 0.0.0.0, supernet
  Known via "static", distance 1, metric 0, candidate default path
  Routing Descriptor Blocks:

  * 10.62.114.1, via outside2

<- default route over outside2
      Route metric is 0, traffic share count is 1


>

show running-config sftunnel
```

sftunnel interface outside2

<- sftunnel is enabled only over outside2
sftunnel port 8305

>

show nat detail

Manual NAT Policies Implicit (Section 0)

1 (nlp_int_tap) to (outside2) source static nlp_server__sftunnel_0.0.0.0_intf6 interface destination st

translate_hits = 3, untranslate_hits = 3

Source - Origin: 169.254.1.3/32, Translated: 10.62.114.51/24
Destination - Origin: 0.0.0.0/0, Translated: 0.0.0.0/0
Service - Protocol: tcp Real: 8305 Mapped: 8305
2 (nlp_int_tap) to (outside2) source static nlp_server__sftunnel_::_intf6 interface ipv6 destination s
translate_hits = 0, untranslate_hits = 0
Source - Origin: fd00:0:0:1::3/128, Translated:
Destination - Origin: ::/0, Translated: ::/0
Service - Protocol: tcp Real: 8305 Mapped: 8305
3 (nlp_int_tap) to (outside2) source dynamic nlp_client_0_intf6 interface
translate_hits = 407, untranslate_hits = 0
Source - Origin: 169.254.1.3/32, Translated: 10.62.114.51/24
4 (nlp_int_tap) to (outside2) source dynamic nlp_client_0_ipv6_intf6 interface ipv6
translate_hits = 0, untranslate_hits = 0
Source - Origin: fd00:0:0:1::3/128, Translated:

>

show conn all port 8305

31 in use, 42 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap 10.62.114.51(169.254.1.3):56853 outside2 198.51.100.23:8305, idle 0:00:06, bytes 33008

<- connectivity over outside2

TCP nlp_int_tap 10.62.114.51(169.254.1.3):32905 outside2 198.51.100.23:8305, idle 0:00:00, bytes 15959

<- connectivity over outside2

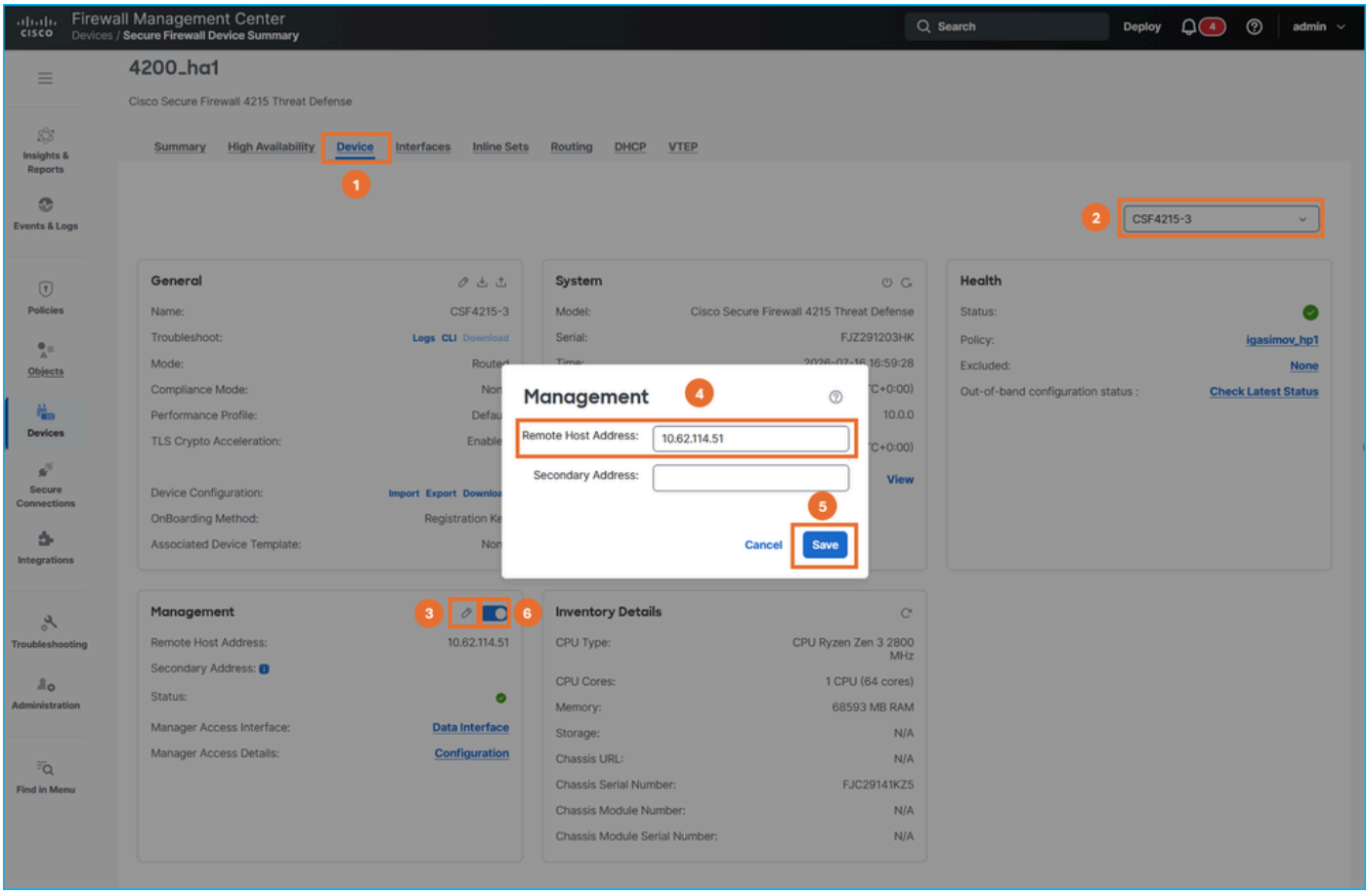
14. Si les serveurs DNS dans le résultat de la commande CLISH « show network » doivent être modifiés, configurez les nouveaux serveurs DNS :

<#root>

>

configure network dns servers 192.0.2.184

15. Sur FMC, remplacez l'adresse IP de gestion FTD par l'adresse IP outside2, puis désactivez et réactivez la connectivité à l'aide du curseur. Répétez cette étape pour les deux unités en haute disponibilité :



16. Vérifiez la connectivité sftunnel sur tous les FTD :

<#root>

>

sftunnel-status-brief

```
PEER:198.51.100.23
        SFTunnel Status:-
```

Channel A: Connected

Channel B: Connected

```
        Peer channel Channel-A is valid  type (CONTROL), using 'tap_nlp', connected to '198.51.100.23' v
        Peer channel Channel-B is valid  type (EVENT), using 'tap_nlp', connected to '198.51.100.23' vi
        Registration: Completed.
        IPv4 Connection to peer '198.51.100.23' Start Time: Thu Jul 16 16:37:14 2026 UTC
        Heartbeat Send Time:     Thu Jul 16 16:38:13 2026 UTC
        Heartbeat Received Time: Thu Jul 16 16:39:13 2026 UTC
        Last disconnect time   : Thu Jul 16 16:37:11 2026 UTC
        Last disconnect reason : Both control and event channel connections with peer went down

>
```

show conn all port 8305

```
32 in use, 42 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect
```

TCP nlp_int_tap 10.62.114.51(169.254.1.3):8305 outside2 198.51.100.23:36383, idle 0:00:00, bytes 23575

```
<- new connection over different source port
```

TCP nlp_int_tap 10.62.114.51(169.254.1.3):8305 outside2 198.51.100.23:50963, idle 0:00:01, bytes 12319

```
<- new connection over different source port
```

17. Si vous devez modifier les paramètres des serveurs DNS dans les plates-formes, modifiez la configuration et déployez les stratégies appropriées.

Dépannage de la connexion de gestion

Utilisez ces commandes pour les vérifications :

1. show network : affiche la configuration de l'interface de gestion.
2. sftunnel-status-brief - affiche l'état de connectivité de sftunnel.
3. show run sftunnel - affiche la configuration de sftunnel dans le moteur de pare-feu (Lina).
4. show conn all port 8305 - affiche les connexions sftunnel via le moteur Lina.

Pour dépanner les problèmes de connexions de gestion, référez-vous à la section Dépannage de la connexion de gestion dans le guide officiel.

Références

1. Guide de configuration des périphériques Cisco Secure Firewall Management Center, 10.x
2. Modifier l'interface d'accès Manager
3. Dépannage de la connexion de gestion

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.