Configurer l'accès au gestionnaire sur FTD de l'interface de gestion à l'interface de données

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Configurer
  - Poursuivre la migration des interfaces
  - Activer SSH sur les paramètres de plateforme
- Vérifier
  - Vérification à partir de l'interface utilisateur graphique (GUI) FMC
  - Vérification à partir de l'interface de ligne de commande FTD
- Dépannage
  - État de la connexion de gestion
    - Scénario de travail
    - Scénario de non-fonctionnement
  - Validation des informations réseau
  - Valider l'état du manager
  - Valider la connectivité réseau
    - Envoyez une requête ping au Management Center
    - Vérification de l'état, des statistiques et du nombre de paquets
    - Valider la route sur FTD pour atteindre FMC
    - Vérifier les statistiques Sftunnel et Connection
- Informations connexes

Introduction

Ce document décrit le processus de modification de l'accès du manager sur Firepower Threat Defense (FTD) d'une interface de gestion à une interface de données.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)

Composants utilisés

- Défense contre les menaces Firepower Virtual 7.2.5
- Firepower Management Center Virtual 7.4.1

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

Chaque périphérique inclut une interface de gestion dédiée unique pour communiquer avec le FMC. Vous pouvez éventuellement configurer le périphérique pour qu'il utilise une interface de données pour la gestion au lieu de l'interface de gestion dédiée. L'accès FMC sur une interface de données est utile si vous souhaitez gérer Firepower Threat Defense à distance depuis l'interface externe ou si vous ne disposez pas d'un réseau de gestion distinct. Cette modification doit être effectuée sur le Centre de gestion Firepower pour FTD géré par FMC.

L’accès FMC à partir d’une interface de données présente quelques limitations :

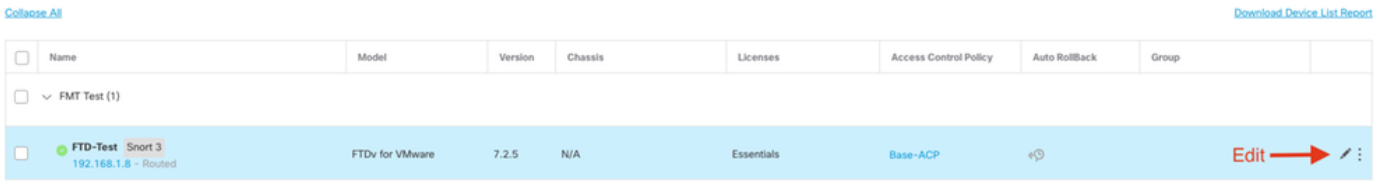
- Vous ne pouvez activer l'accès au gestionnaire que sur une seule interface de données physique. Vous ne pouvez pas utiliser une sous-interface ou EtherChannel.
- Mode pare-feu routé uniquement, à l’aide d’une interface routée.
- PPPoE n'est pas pris en charge. Si votre FAI nécessite le protocole PPPoE, vous devez inclure un routeur avec prise en charge PPPoE entre le pare-feu Firepower Threat Defense et le modem WAN.
- Vous ne pouvez pas utiliser des interfaces de gestion et d'événements distinctes.

Configurer

Poursuivre la migration des interfaces

Remarque : Il est fortement recommandé d'avoir la dernière sauvegarde du FTD et du FMC avant de procéder à toute modification.

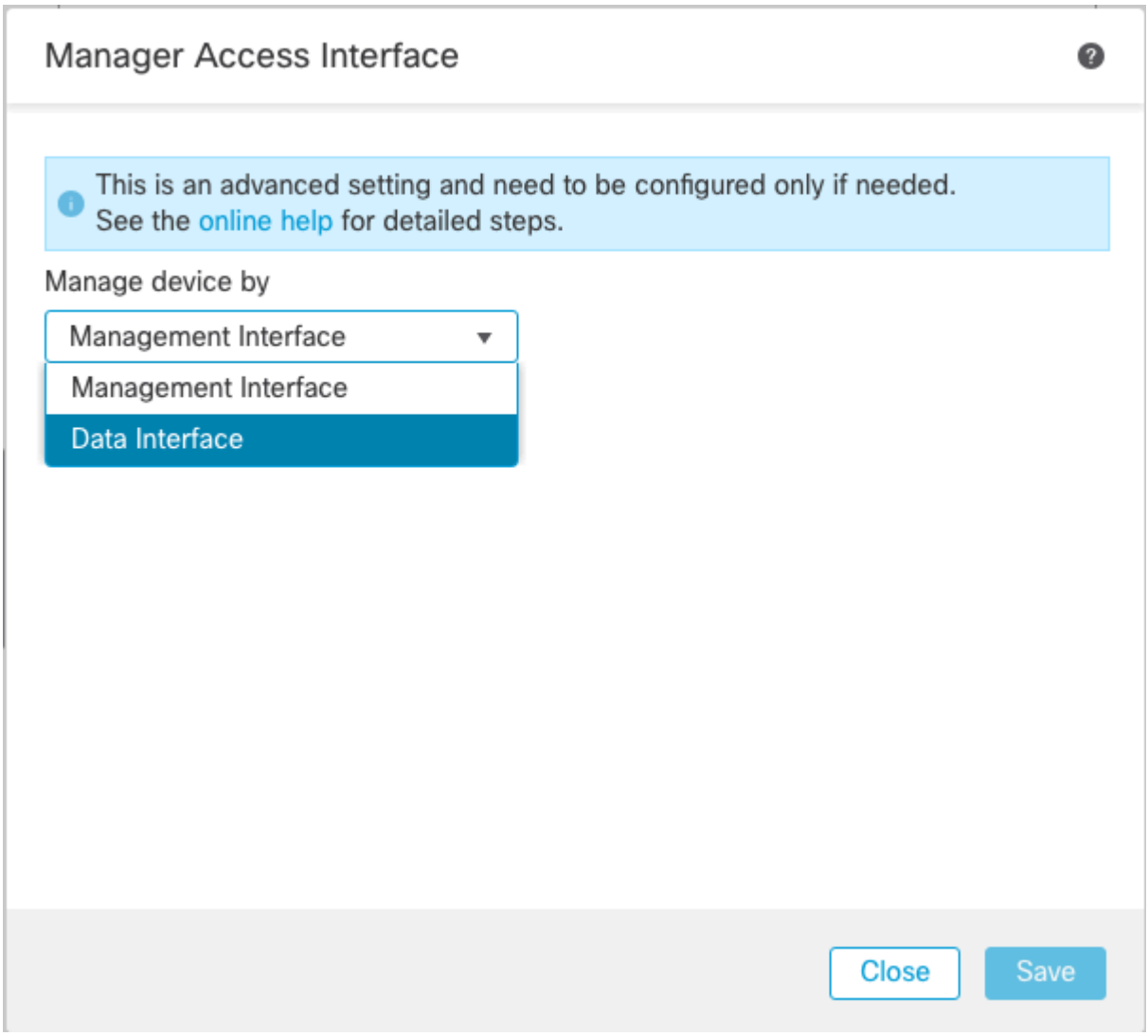
1. Accédez à la page Périphériques > Gestion des périphériques, puis cliquez sur Modifier pour le périphérique que vous modifiez.



2. Accédez à la section Device > Management et cliquez sur le lien pour l'interface d'accès au gestionnaire.

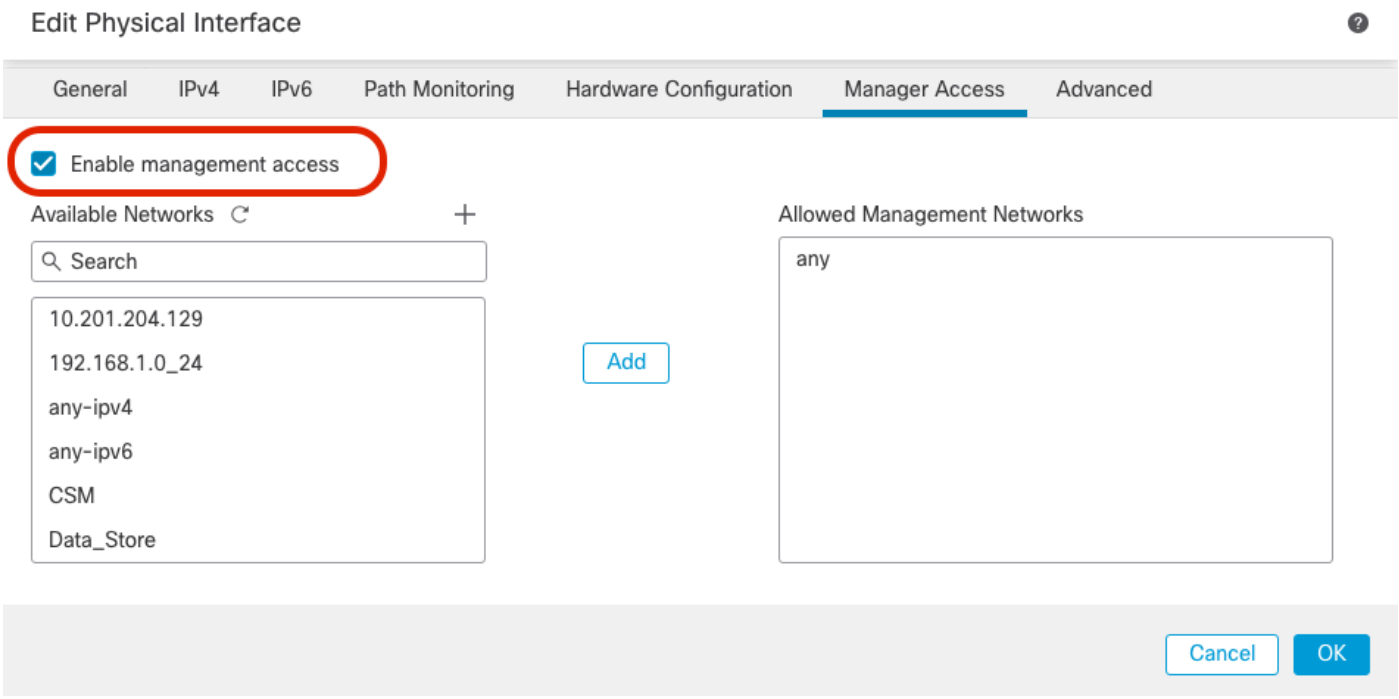


3. Le champ Interface d'accès du manager affiche l'interface de gestion existante. Cliquez sur le lien pour sélectionner le nouveau type d'interface, qui est l'option Interface de données dans la liste déroulante Gérer le périphérique par et cliquez sur Enregistrer.



---

4. Vous devez maintenant passer à Activer l'accès à la gestion sur une interface de données, accédez à Périphériques > Gestion des périphériques > Interfaces > Modifier l'interface physique > Accès au gestionnaire.



Facultatif: Si vous utilisez une interface secondaire pour la redondance, assurez-vous d'activer l'accès à la gestion sur l'interface utilisée à des fins de redondance. Si vous utilisez DHCP pour l'interface, activez la méthode DDNS de type Web dans la boîte de dialogue Devices > Device Management > DHCP > DDNS. Vous pouvez configurer DNS dans une stratégie de paramètres de plate-forme et l'appliquer à ce périphérique sous Périphériques > Paramètres de plate-forme > DNS.

---

5. Assurez-vous que la défense contre les menaces peut être acheminée vers le centre de gestion via l'interface de données ; ajoutez une route statique si nécessaire sur Devices > Device Management > Routing > Static Route.

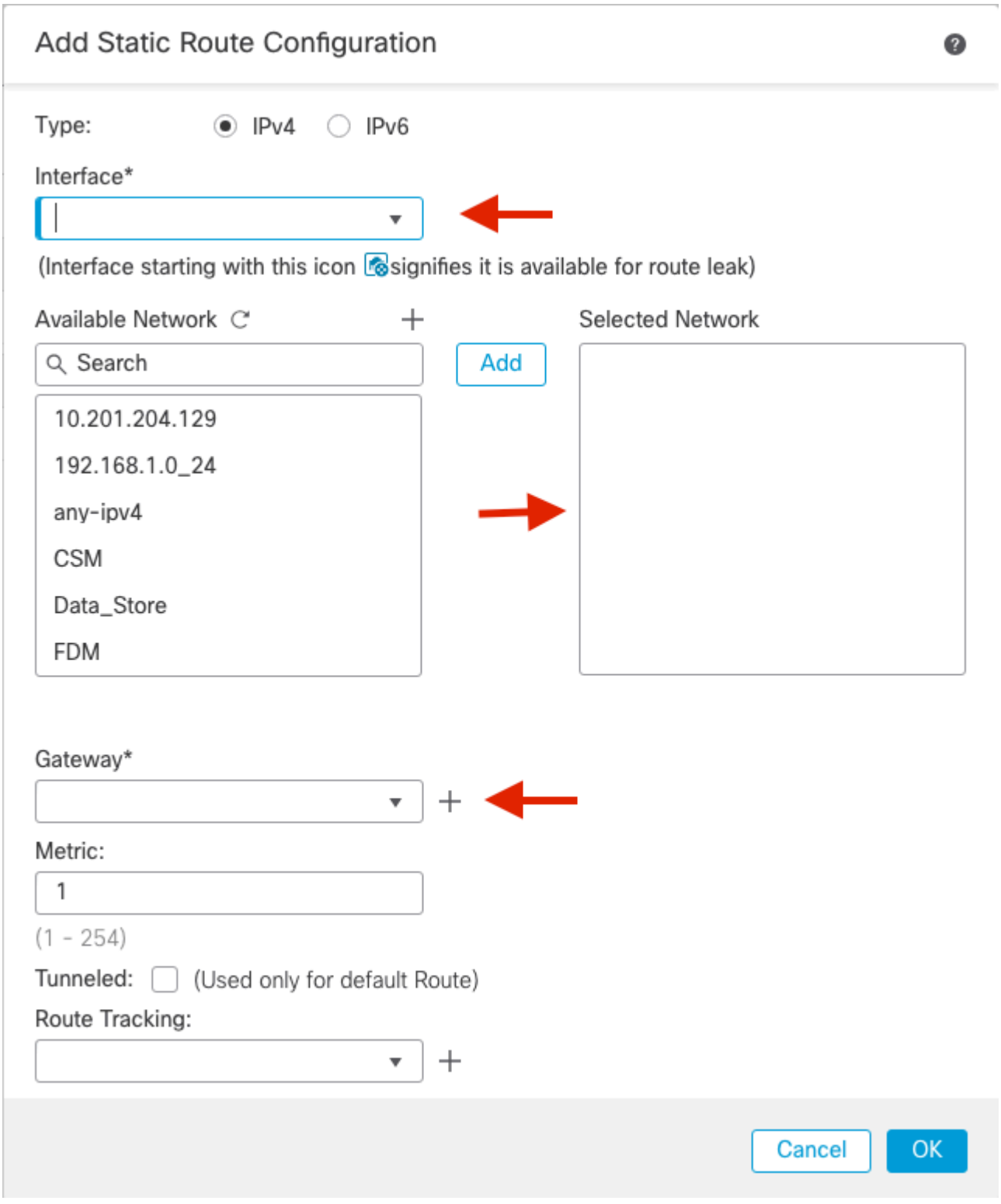
a. Cliquez sur IPv4 ou IPv6 selon le type de route statique que vous ajoutez.

b. Choisissez l'interface où cette route statique s'applique.

c. Dans la liste Available Network (Réseau disponible), sélectionnez le réseau de destination.

d. Dans le champ Gateway ou IPv6 Gateway, entrez ou sélectionnez le routeur de passerelle qui est le tronçon suivant pour cette route.

Facultatif: Pour surveiller la disponibilité de la route, saisissez ou sélectionnez le nom d'un objet de surveillance SLA (Service Level Agreement) qui définit la stratégie de surveillance dans le champ Suivi de route.



6. Déployez les modifications de configuration, car ces mises à jour sont désormais déployées sur

l'interface de gestion actuelle.

---

7. À l'interface de ligne de commande FTD, configurez l'interface de gestion pour qu'elle utilise une adresse IP statique et la passerelle pour qu'elle soit des interfaces de données.

a. configuration du réseau {ipv4} | ipv6} adresse_ip manuelle masque_réseau interfaces-données

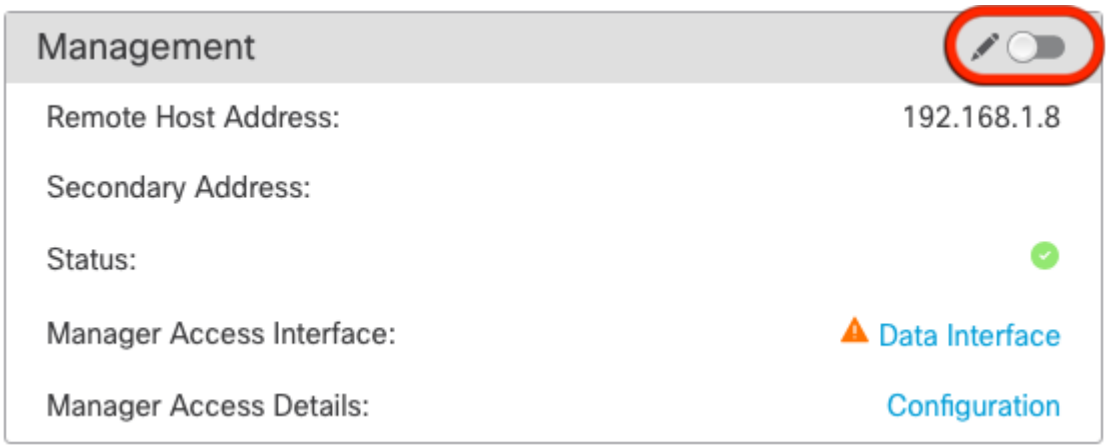
---

```
>
>                                    IP_ADDRESS      NETMASK         GATEWAY
> configure network ipv4 manual 192.168.1.8 255.255.255.0 data-interfaces
Setting IPv4 network configuration...
Interface eth0 speed is set to '10000baseT/Full'
Network settings changed.
```

Remarque : Bien que vous ne prévoyiez pas d'utiliser l'interface de gestion, vous devez définir une adresse IP statique. Par exemple, une adresse privée pour que vous puissiez définir la passerelle sur des interfaces de données. Cette gestion est utilisée pour transférer le trafic de gestion vers l'interface de données à l'aide de l'interface tap_nlp.

---

8. Désactivez la gestion dans Management Center. Cliquez sur Edit and update the Remote Host Address IP address and (Optional) Secondary Address pour la défense contre les menaces dans la section Devices > Device Management > Device > Management, puis activez la connexion.



Activer SSH sur les paramètres de plateforme

1. Activez SSH pour l'interface de données dans la stratégie des paramètres de plate-forme et appliquez-le au périphérique dans Périphériques > Paramètres de plate-forme > Accès SSH.

---

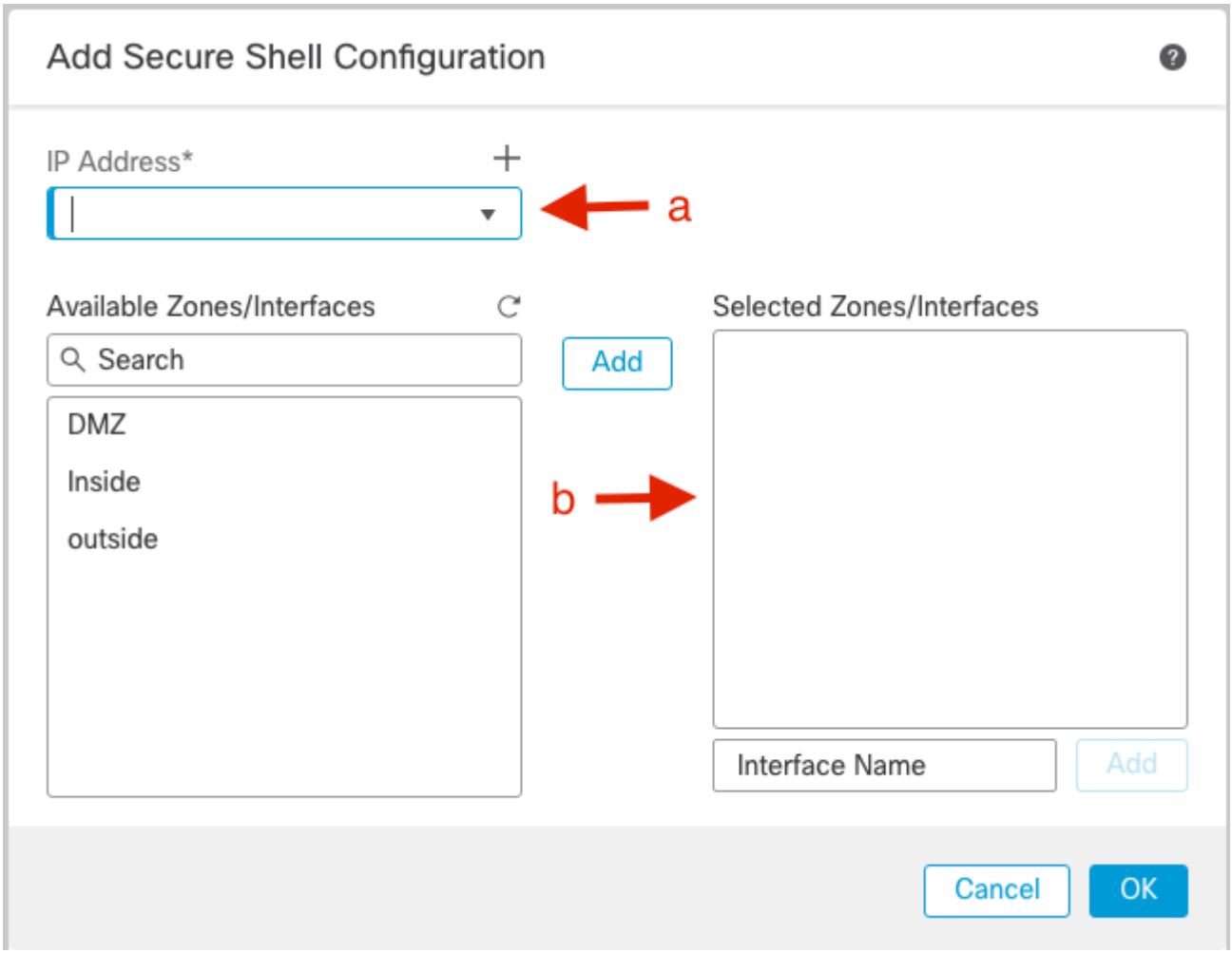
2. Cliquez sur Ajouter.

---

3. Hôtes ou réseaux que vous autorisez à établir des connexions SSH. Ajoutez les zones qui contiennent les interfaces pour autoriser les connexions SSH. Pour les interfaces qui ne se trouvent pas dans une zone, vous pouvez taper le nom de l'interface dans le champ Zones/Interfaces sélectionnées liste et cliquez sur Add.

---

4. Cliquez sur OK. Déployez les modifications.



Remarque : SSH n'est pas activé par défaut sur les interfaces de données, donc si vous voulez gérer la défense contre les menaces à l'aide de SSH, vous devez l'autoriser

---

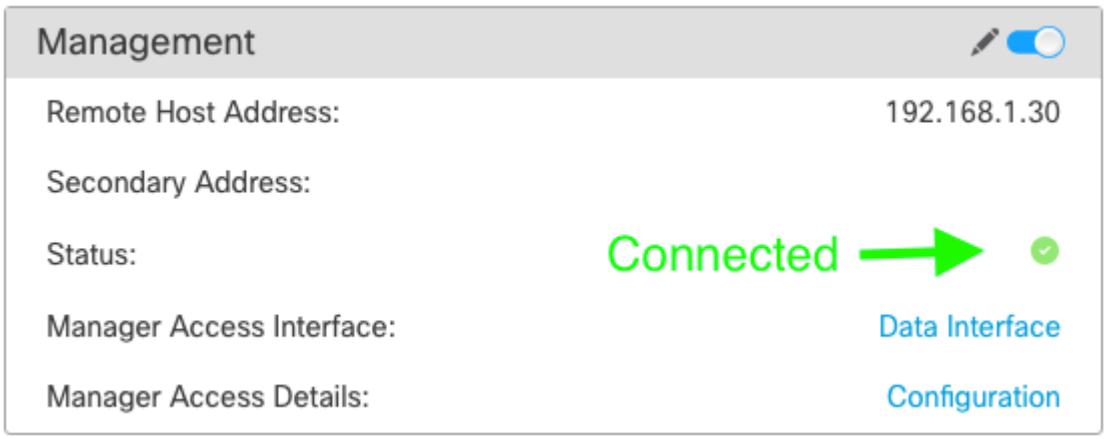
explicitement.

Vérifier

Assurez-vous que la connexion de gestion est établie sur l'interface de données.

Vérification à partir de l'interface utilisateur graphique (GUI) FMC

Dans le Management Center, vérifiez l'état de la connexion de gestion sur la page Devices > Device Management > Device > Management > Manager Access - Configuration Details > Connection Status.



Vérification à partir de l'interface de ligne de commande FTD

Dans l'interface de ligne de commande threat defense, exécutez la commande sftunnel-status-brief pour afficher l'état de la connexion de gestion.

```
>
> sftunnel-status-brief

PEER:192.168.1.2
        Peer channel Channel-A is valid  type (CONTROL), using 'tap_nlp', connected to '192.168.1.2' via '169.254.1.2'
        Peer channel Channel-B is valid  type (EVENT), using 'tap_nlp', connected to '192.168.1.2' via '169.254.1.2'
        Registration: Completed.
        IPv4 Connection to peer '192.168.1.2' Start Time: Tue Jul 16 22:23:54 2024 UTC
        Heartbeat Send Time:     Tue Jul 16 22:39:52 2024 UTC
        Heartbeat Received Time: Tue Jul 16 22:39:52 2024 UTC
        Last disconnect time   : Tue Jul 16 22:17:42 2024 UTC
        Last disconnect reason : Both control and event channel connections with peer went down
```

L'état indique une connexion réussie pour une interface de données, indiquant l'interface interne tap_nlp.

Dépannage

Dans le Management Center, vérifiez l'état de la connexion de gestion sur la page Devices > Device Management > Device > Management > Manager Access - Configuration Details > Connection Status.

Dans l'interface de ligne de commande threat defense, exécutez la commande sftunnel-status-brief pour afficher l'état de la connexion de gestion. Vous pouvez également exécuter sftunnel-status pour afficher des informations plus complètes.

État de la connexion de gestion

Scénario de travail

```
> sftunnel-status-brief

PEER:192.168.1.2
        Peer channel Channel-A is valid  type (CONTROL), using 'eth0', connected to '192.168.1.2' via '192.168.1.8'
        Peer channel Channel-B is valid  type (EVENT), using 'tap_nlp', connected to '192.168.1.2' via '169.254.1.2'
        Registration: Completed.
        IPv4 Connection to peer '192.168.1.2' Start Time: Wed Jul 17 06:21:15 2024 UTC
        Heartbeat Send Time:     Wed Jul 17 17:15:20 2024 UTC
        Heartbeat Received Time: Wed Jul 17 17:16:55 2024 UTC
        Last disconnect time   : Wed Jul 17 06:21:12 2024 UTC
        Last disconnect reason : Process shutdown due to stop request from PM
```

Scénario de non-fonctionnement

```
> sftunnel-status-brief

PEER:192.168.1.2
        Registration: Completed.
        Connection to peer '192.168.1.2' Attempted at Wed Jul 17 17:20:26 2024 UTC
        Last disconnect time   : Wed Jul 17 17:20:26 2024 UTC
        Last disconnect reason : Both control and event channel connections with peer went down
```

Validation des informations réseau

Dans l'interface de ligne de commande de défense contre les menaces, affichez les paramètres réseau de l'interface de données d'accès Management and Manager :

> show network

```
> show network
==============[ System Information ]==============
Hostname                  : ftdcdo.breakstuff.com
Domains                   : breakstuff.com
DNS Servers               : 192.168.1.103
DNS from router           : enabled
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces
IPv6 Default route
  Gateway                 : data-interfaces

======================[ eth0 ]======================
State                     : Enabled
Link                      : Up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 00:0C:29:54:D4:47
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 192.168.1.8
Netmask                   : 255.255.255.0
Gateway                   : 192.168.1.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

==============[ Proxy Information ]===============
State                     : Disabled
Authentication            : Disabled

======[ System Information - Data Interfaces ]======
DNS Servers               :
Interfaces                : GigabitEthernet0/0

==============[ GigabitEthernet0/0 ]==============
State                     : Enabled
Link                      : Up
Name                      : Outside
MTU                       : 1500
MAC Address               : 00:0C:29:54:D4:5B
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 192.168.1.30
Netmask                   : 255.255.255.0
----------------------[ IPv6 ]----------------------
Configuration             : Disabled
```

Valider l'état du manager

À l'interface CLI de défense contre les menaces, vérifiez que l'enregistrement du centre de gestion a été effectué.

```
> show managers
```

```
> show managers
Type                    : Manager
Host                    : 192.168.1.2
Display name            : 192.168.1.2
Identifier              : d4cd32d6-da7f-11ee-840e-b88231b3fd47
Registration            : Completed
Management type         : Configuration and analytics
```

Remarque : Cette commande n'affiche pas l'état actuel de la connexion de gestion.

Valider la connectivité réseau

Envoyez une requête ping au Management Center

Dans l'interface de ligne de commande de défense contre les menaces, exécutez la commande pour envoyer une requête ping au centre de gestion à partir des interfaces de données :

```
> ping fmc_ip
```

```
> ping 192.168.1.2
Please use 'CTRL+C' to cancel/abort...
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Dans l'interface de ligne de commande de défense contre les menaces, exécutez la commande pour envoyer une requête ping au centre de gestion à partir de l'interface de gestion, qui effectue le routage sur le fond de panier vers les interfaces de données :

> ping system fmc_ip

```
> ping system 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.340 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.291 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=0.333 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=0.282 ms
^C
--- 192.168.1.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 132ms
rtt min/avg/max/mdev = 0.282/0.311/0.340/0.030 ms
```

Vérification de l’état, des statistiques et du nombre de paquets

Dans l'interface de ligne de commande de défense contre les menaces, passez en revue les informations sur l'interface de fond de panier interne, nlp_int_tap :

> show interface detail

```
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0000.0100.0001, MTU 1500
        IP address 169.254.1.1, subnet mask 255.255.255.248
        311553 packets input, 41414494 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        232599 packets output, 165049822 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (0/0)
        output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
        311553 packets input, 37052752 bytes
        232599 packets output, 161793436 bytes
        167463 packets dropped
      1 minute input rate 0 pkts/sec,  3 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  3 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
        Interface number is 14
        Interface config status is active
        Interface state is active
```

Valider la route sur FTD pour atteindre FMC

À l'interface de ligne de commande de défense contre les menaces, vérifiez que la route par défaut (S*) a été ajoutée et que les règles NAT internes existent pour l'interface de gestion (nlp_int_tap).

```
> show route
```

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is not set

C        192.168.1.0 255.255.255.0 is directly connected, Outside
L        192.168.1.30 255.255.255.255 is directly connected, Outside
```

> show nat

```
> show nat
Manual NAT Policies Implicit (Section 0)
1 (nlp_int_tap) to (Outside) source static nlp_server__sftunnel_0.0.0.0_intf3 interface  destination static 0_0.0.0.0_5 0_0.0.0.0_5 service tcp 8305 8305
    translate_hits = 5, untranslate_hits = 6
2 (nlp_int_tap) to (Outside) source static nlp_server__sftunnel_::_intf3 interface ipv6  destination static 0_::_6 0_::_6 service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 0
3 (nlp_int_tap) to (Outside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 10, untranslate_hits = 0
4 (nlp_int_tap) to (Outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
    translate_hits = 0, untranslate_hits = 0
```

Vérifier les statistiques Sftunnel et Connection

> show running-config sftunnel

```
> show running-config sftunnel
sftunnel interface Outside
sftunnel port 8305
```

Avertissement : Tout au long du processus de modification de l'accès du gestionnaire, évitez de supprimer le gestionnaire sur le FTD ou de désinscrire/forcer la suppression du FTD du FMC.

Informations connexes

- Configurer les paramètres DNS sur la plate-forme
- Configurer l'accès de gestion à FTD (HTTPS et SSH) via FMC

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.