Cambiar interfaz de datos de acceso del administrador de FTD

Contenido

Introducción

Este documento describe los pasos para cambiar la interfaz de datos de acceso del administrador de Secure Firewall Threat Defence (FTD).

Prerequisites

Requirements

- Conocimiento básico del producto.
- Familiaridad con la gestión y gestión de FTD en interfaces de datos.

Componentes Utilizados

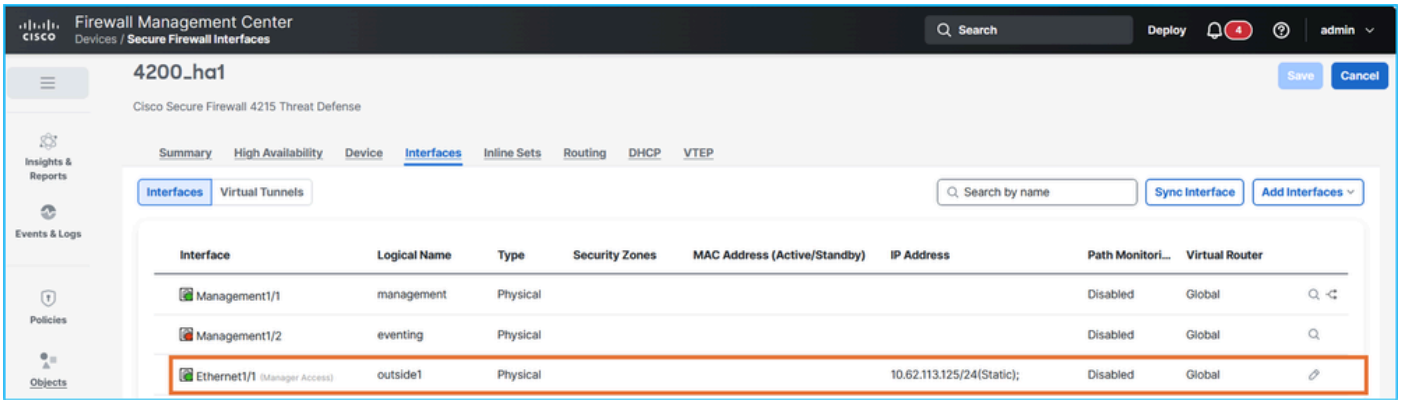
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Firewall seguro 4200
- Secure Firewall Threat Defence (FTD) 10.0.x, 7.6.4
- Secure Firewall Management Center (FMC) 10.0.x

Configuración inicial

1. El CSP gestiona el FTD en alta disponibilidad (HA) a través de la interfaz de datos Ethernet1/1 con el nombre if outside1, utilizando las direcciones IP activas y en espera 10.62.113.125 y 10.62.113.126 respectivamente:



Verificación en 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. Las conexiones sftunnel se establecen entre la unidad FTD HA y el 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. El FTD se basa en la resolución DNS para conectarse al FMC. El administrador es una configuración basada en el nombre de dominio completo (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
…
```

Los servidores DNS son accesibles a través de la interfaz outside1.

4. Las conexiones sftunnel se establecen a través del motor 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

El objetivo es mover el acceso del administrador de la interfaz actual outside1 a la interfaz de destino outside2. Las direcciones IP outside2 activas y en espera son 10.62.114.51/24 y 10.62.114.52/24 respectivamente.

Tenga en cuenta que las versiones de FTD 7.7.0 o posteriores admiten interfaces redundantes de datos de acceso de administrador, que permiten la configuración e implementación de más de 1 interfaz de acceso de administrador. Esta característica no se admite en versiones anteriores a la 7.7.0.

Debido a este hecho, los pasos específicos se omiten o contienen acciones diferentes.

⚠ Precaución: No cancele el registro/elimine FTD del FMC en ningún paso.

1. Se recomienda tener acceso de consola a los FTD:

- En el caso de Firepower 4100/9300, puede conectarse al chasis mediante SSH y, a continuación, conectarse a la consola FTD nativa mediante el comando connect module x console, donde x es el ID del módulo de ranura/seguridad.
- En el caso de Firepower 4100/9300 que ejecuta FTD en modo de instancia múltiple (MI), puede conectarse al chasis mediante SSH y, a continuación, conectarse a la consola FTD nativa mediante el comando connect module x telnet, donde x es el ID del módulo de ranura/seguridad. A continuación, conéctese a la instancia de FTD mediante el comando connect ftd <ftd_id>.
- En el caso de Secure Firewall 3100/4200 en modo MI, puede conectarse al chasis mediante SSH y luego conectarse a la consola FTD mediante el comando connect ftd <identifier>.

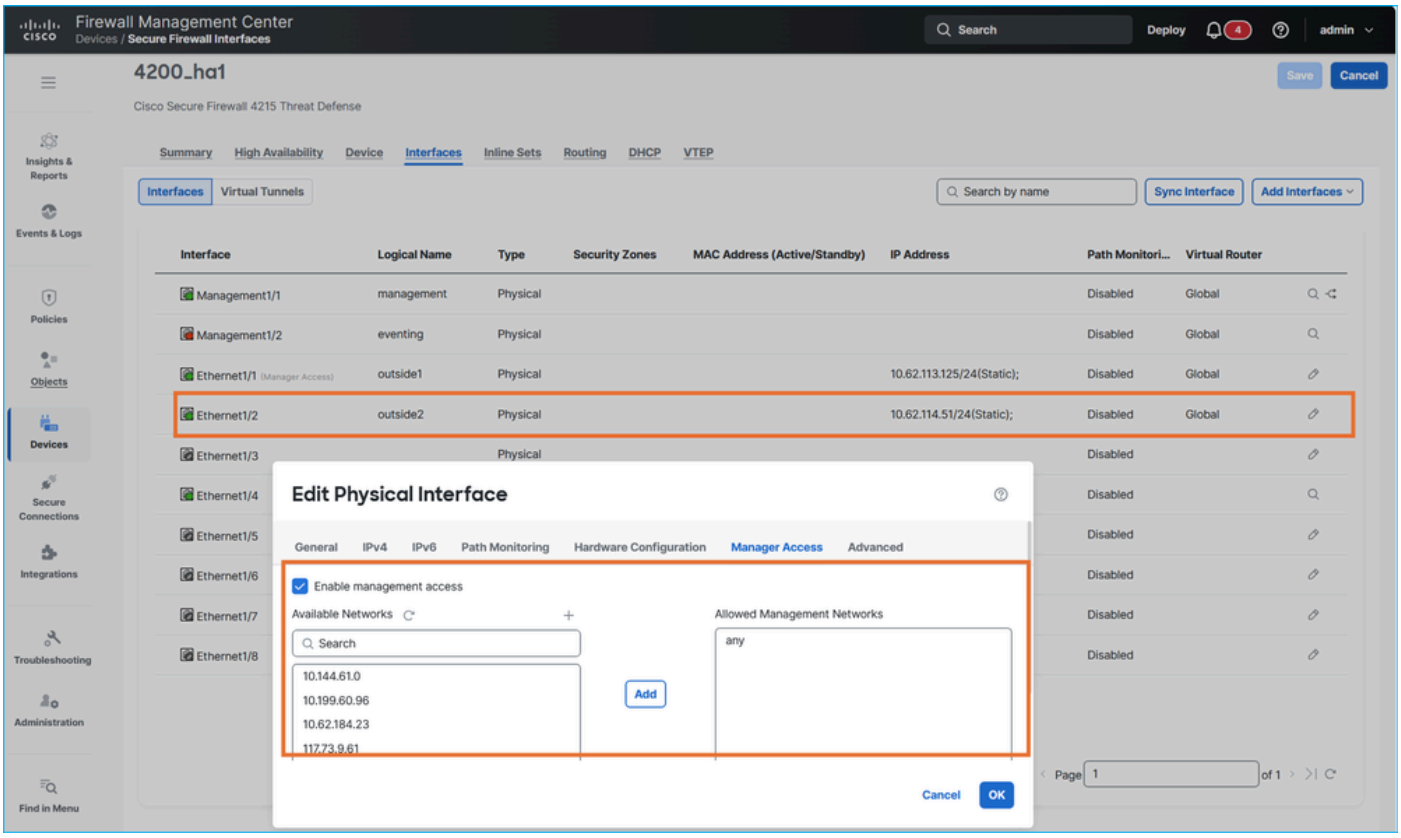
2. Implementar directivas pendientes.

3. Se recomienda encarecidamente realizar copias de seguridad de FTD y FMC. En el caso de FTD HA, tome el respaldo de ambas unidades.

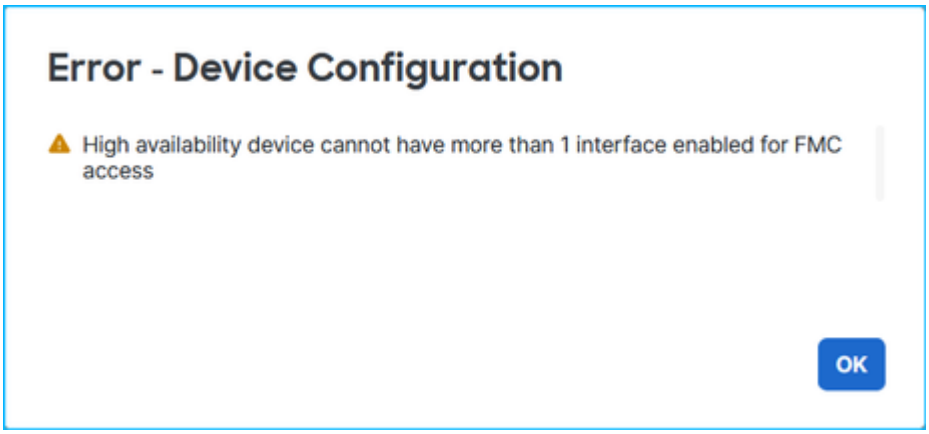
4. Configure el nombre de la interfaz de destino, la dirección IP, la zona de seguridad y otros parámetros relacionados con la interfaz, si procede.

5. Configure la dirección IP en espera de la interfaz de destino.

6. Si la versión del software FTD es 7.7.0 o posterior, habilite el acceso del administrador en la interfaz de destino y ajuste las redes de acceso a la administración según sea necesario:



Tenga en cuenta que las versiones de FTD anteriores a la 7.7.0 no admiten interfaces de datos de acceso de administrador redundantes. Al intentar configurar la interfaz de acceso del segundo administrador, aparece este mensaje de error:



Asegúrese de omitir los pasos 7 y 8 para las versiones de FTD anteriores a la 7.7.0.

7. Implemente las directivas y verifique la configuración en FTD CLISH. En este ejemplo, la interfaz Ethernet1/2 con nameif outside2 tiene direcciones IP 10.62.114.51 y 10.62.114.52 respectivamente:

```
<#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
```

La interfaz outside2 se agrega a la configuración de 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
```

Aunque hay reglas adicionales instaladas en la tabla de traducción de direcciones de red (NAT), las reglas con la interfaz outside1 están en uso:

```
<#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. Verifique el estado de alta disponibilidad y la supervisión de la interfaz:

<#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 planea administrar los FTDs a través de la interfaz outside2, asegúrese de que se permita el acceso en la sección Acceso SSH de la configuración de la plataforma.

10. Realice los cambios necesarios para permitir la conectividad a través de la interfaz de destino con los servidores de nombres de dominio (DNS) y FMC:

- Si se requiere la resolución de nombres de dominio (DNS) para la conectividad entre FMC y

FTD, asegúrese de que los FTD tengan disponibilidad a través de la interfaz de destino hasta el siguiente salto utilizado para alcanzar los servidores DNS. También se debe permitir la resolución de DNS en la ruta de tránsito.
- Asegúrese de que los FTD tengan disponibilidad en la interfaz de destino hasta el siguiente salto que se utilizará para alcanzar el FMC.
- Asegúrese de que la conectividad bidireccional entre FMC y FTDs sobre el puerto TCP 8305 esté permitida en la trayectoria de tránsito sobre la interfaz de destino. La conexión debe estar permitida en ambas direcciones.

En este caso, IP 10.62.114.1 debe utilizarse como el gateway predeterminado sobre la interfaz de destino. La dirección IP del siguiente salto es accesible mediante el protocolo de mensajes de control de Internet (ICMP):

```
<#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 está bloqueado administrativamente en la trayectoria de tránsito o en el salto siguiente, asegúrese de que la dirección de control de acceso a medios (MAC) del salto siguiente esté visible en la salida del comando show arp y sea válida:

```
<#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. Realice estos pasos en función de la versión de FTD:

- Versión 7.7.0 o posterior: en FMC, desactive el acceso del administrador a través de la interfaz de origen (outside1), ajuste el enrutamiento, incluido el enrutamiento a los servidores DNS (si se utiliza DNS para acceder a FMC) y FMC a través de la interfaz de destino (outside2). Por ejemplo, configure rutas estáticas específicas o configure el gateway predeterminado a través de la interfaz de destino.
- Versión anterior a 7.7.0: en FMC, desactive el acceso del administrador a través de la interfaz de origen (outside1), active el acceso del administrador a través de la interfaz de destino (outside2), ajuste el enrutamiento, incluido el enrutamiento a servidores DNS (si se utiliza DNS para acceder a FMC) y FMC a través de la interfaz de destino (outside2). Por ejemplo, configure rutas estáticas específicas o configure el gateway predeterminado a través de la interfaz de destino.

12. Implemente políticas.

13. Verificar en 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

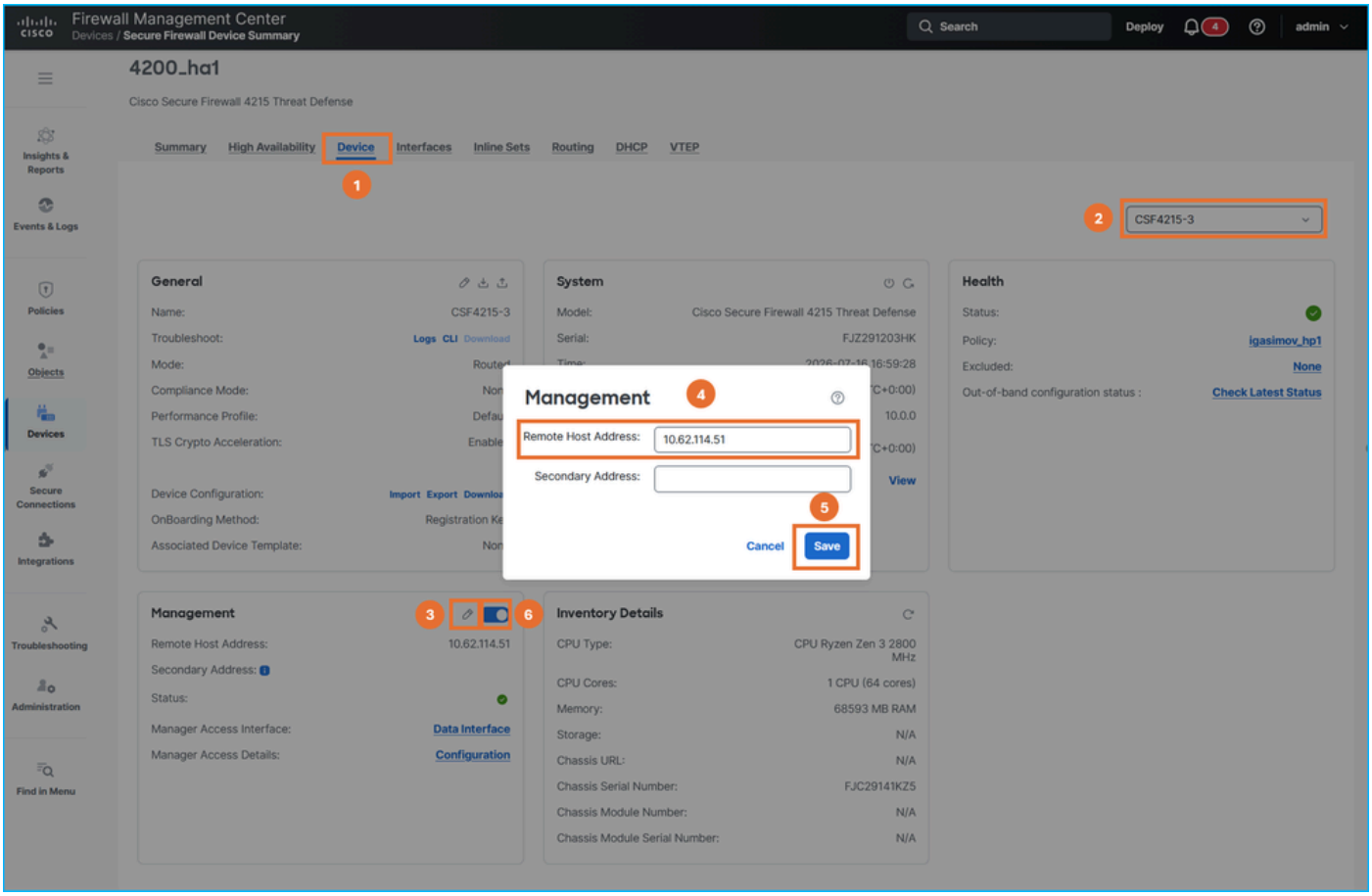
14. Si es necesario cambiar los servidores DNS en la salida del comando 'show network' CLISH, configure los nuevos servidores DNS:

<#root>

>

configure network dns servers 192.0.2.184

15. En el FMC, cambie la dirección IP de gestión del FTD por la dirección IP outside2 y, a continuación, desactive y vuelva a activar la conectividad mediante el control deslizante. Repita este paso para ambas unidades en HA:



16. Verifique la conectividad del túnel seguro en todos los 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 los servidores DNS de la configuración de las plataformas deben cambiarse, realice los cambios de configuración adecuados e implemente políticas.

Solucionar problemas de conexión de administración

Utilice estos comandos para las verificaciones:

1. show network - muestra la configuración de la interfaz de administración.
2. sftunnel-status-brief - muestra el estado de conectividad de sftunnel.
3. show run sftunnel - muestra la configuración de sftunnel en el motor del firewall (Lina).
4. show conn all port 8305 - muestra las conexiones sftunnel a través del motor Lina.

Para resolver problemas de conexiones de administración, consulte la sección Resolución de problemas de conexión de administración en la guía oficial.

Referencias

1. Guía de configuración de dispositivos de Cisco Secure Firewall Management Center, 10.x
2. Cambiar la interfaz de acceso del jefe
3. Solución de problemas de conexión de administración

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).