

Configurar el acceso de administrador en FTD desde la gestión a la interfaz de datos

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Continúe con la migración de la interfaz](#)

[Activar SSH en la configuración de la plataforma](#)

[Verificación](#)

[Verificar desde la interfaz gráfica de usuario \(GUI\) de FMC](#)

[Verificar desde la interfaz de línea de comandos \(CLI\) de FTD](#)

[Troubleshoot](#)

[Estado de conexión de administración](#)

[Escenario de trabajo](#)

[Situación de no funcionamiento](#)

[Validar la información de red](#)

[Validar el estado del jefe](#)

[Validar la conectividad de red](#)

[Hacer ping en el Management Center](#)

[Comprobar el estado de la interfaz, las estadísticas y el recuento de paquetes](#)

[Validar ruta en FTD para alcanzar FMC](#)

[Comprobación de las estadísticas de conexión y del túnel seguro](#)

[Información Relacionada](#)

Introducción

Este documento describe el proceso para modificar el acceso de administrador en Firepower Threat Defense (FTD) de una interfaz de administración a una interfaz de datos.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Firepower Threat Defense (FTD)
- Centro de administración Firepower (FMC)

Componentes Utilizados

- Firepower Management Center Virtual 7.4.1
- Firepower Threat Defense Virtual 7.2.5

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.

Antecedentes

Cada dispositivo incluye una única interfaz de gestión dedicada para comunicarse con el FMC. Si lo desea, puede configurar el dispositivo para que utilice una interfaz de datos para la gestión en lugar de la interfaz de gestión dedicada. El acceso a FMC en una interfaz de datos es útil si desea gestionar Firepower Threat Defense de forma remota desde la interfaz externa o si no dispone de una red de gestión independiente. Este cambio debe realizarse en Firepower Management Center para FTD gestionado por FMC.

El acceso a FMC desde una interfaz de datos tiene algunas limitaciones:

- Solo puede habilitar el acceso de administrador en una interfaz de datos física. No puede utilizar una subinterfaz o EtherChannel.
- Sólo modo de firewall enrutado, mediante una interfaz enrutada.
- No se admite PPPoE. Si el ISP requiere PPPoE, debe colocar un router compatible con PPPoE entre Firepower Threat Defence y el módem WAN.
- No puede utilizar interfaces de administración y de sólo eventos independientes.

Configurar

Continúe con la migración de la interfaz


Nota: Se recomienda encarecidamente disponer de la última copia de seguridad del FTD y del FMC antes de proceder a cualquier cambio.

1. Vaya a la página Devices > Device Management, haga clic en Edit para el dispositivo que está realizando los cambios.

[Collapse All](#) [Download Device List Report](#)

<input type="checkbox"/>	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	Group	
<input type="checkbox"/>	▼ FMT Test (1)								
<input type="checkbox"/>	● FTD-Test Short 3 192.168.1.8 - Routed	FTDv for VMware	7.2.5	N/A	Essentials	Base-ACP	↺		Edit → ↗ ⋮

2. Vaya a la sección Device > Management, y haga clic en el link para la Interfaz de acceso del administrador.

Management	
Remote Host Address:	192.168.1.8
Secondary Address:	
Status:	✔
Manager Access Interface:	 Management Interface

El campo Interfaz de acceso del jefe muestra la interfaz de gestión existente. Haga clic en el enlace para seleccionar el nuevo tipo de interfaz, que es la opción Interfaz de datos en la lista desplegable Administrar dispositivo por y haga clic en Guardar.

Manager Access Interface

This is an advanced setting and need to be configured only if needed. See the [online help](#) for detailed steps.

Manage device by

Management Interface ▼

Management Interface

Data Interface

Close Save

3. Ahora debe proceder a Habilitar el acceso a la administración en una interfaz de datos, navegue hasta Dispositivos > Administración de dispositivos > Interfaces > Editar interfaz física > Acceso al administrador.

Edit Physical Interface



General

IPv4

IPv6

Path Monitoring

Hardware Configuration

Manager Access

Advanced

Enable management access

Available Networks



Search

10.201.204.129

192.168.1.0_24

any-ipv4

any-ipv6

CSM

Data_Store

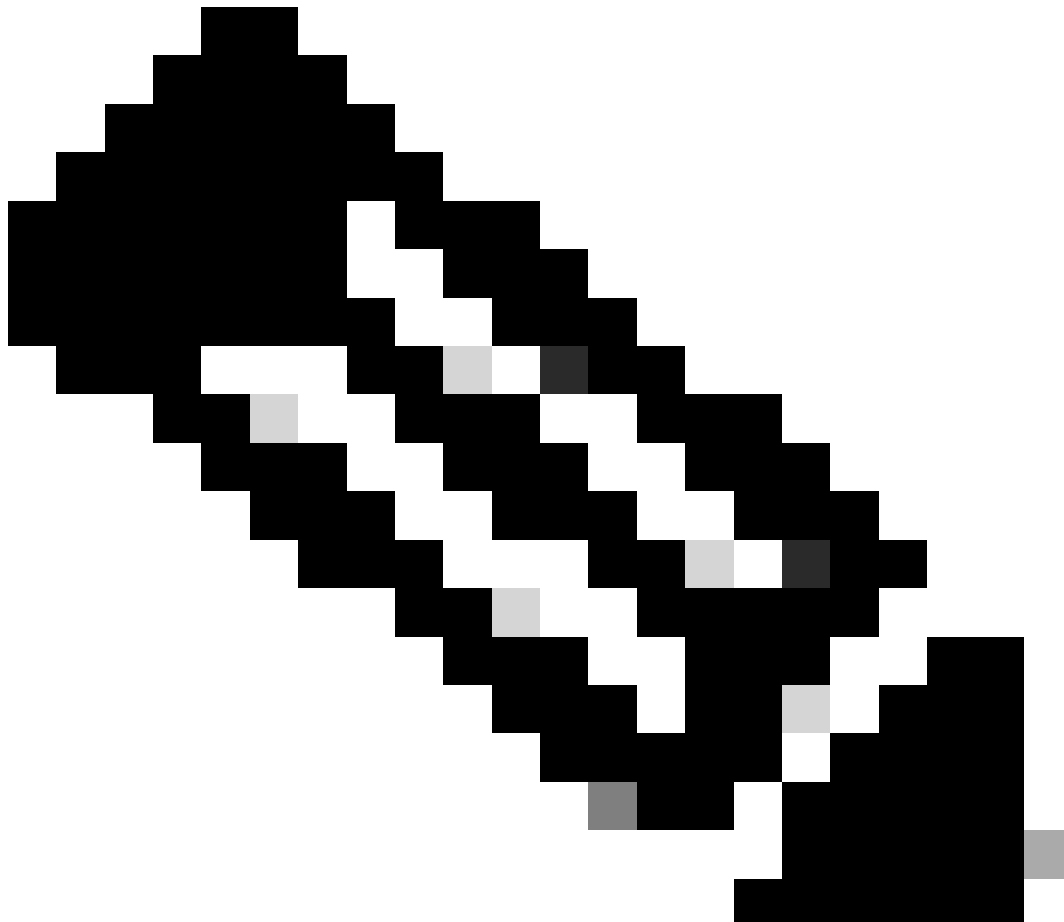
Add

Allowed Management Networks

any

Cancel

OK



Nota: (Opcional) Si utiliza una interfaz secundaria para redundancia, active el acceso de administración en la interfaz utilizada para redundancia.

(Opcional) Si utiliza DHCP para la interfaz, habilite el método DDNS de tipo web en el cuadro de diálogo Dispositivos > Administración de dispositivos > DHCP > DDNS.

(Opcional) Configure DNS en una política de configuración de la plataforma y aplíquelo a este dispositivo en Dispositivos > Configuración de la plataforma > DNS.

4. Asegúrese de que la defensa contra amenazas pueda dirigirse al centro de administración a través de la interfaz de datos; agregue una ruta estática si es necesario en Devices > Device Management > Routing > Static Route.

1. Haga clic en IPv4 o IPv6, según el tipo de ruta estática que esté agregando.
2. Elija la Interfaz a la que se aplica esta ruta estática.
3. En la lista Available Network, elija la red de destino.
4. En el campo Gateway o IPv6 Gateway, ingrese o elija el router de gateway que es el salto siguiente para esta ruta.

(Opcional) Para supervisar la disponibilidad de rutas, introduzca o seleccione el nombre de un objeto Monitor de acuerdo de nivel de servicio (SLA) que defina la política de supervisión en el campo Seguimiento de rutas.

Add Static Route Configuration



Type: IPv4 IPv6

Interface*



(Interface starting with this icon  signifies it is available for route leak)

Available Network  +

Add

Selected Network



10.201.204.129

192.168.1.0_24

any-ipv4

CSM

Data_Store

FDM

Gateway*

+



Metric:

(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:

+

Cancel

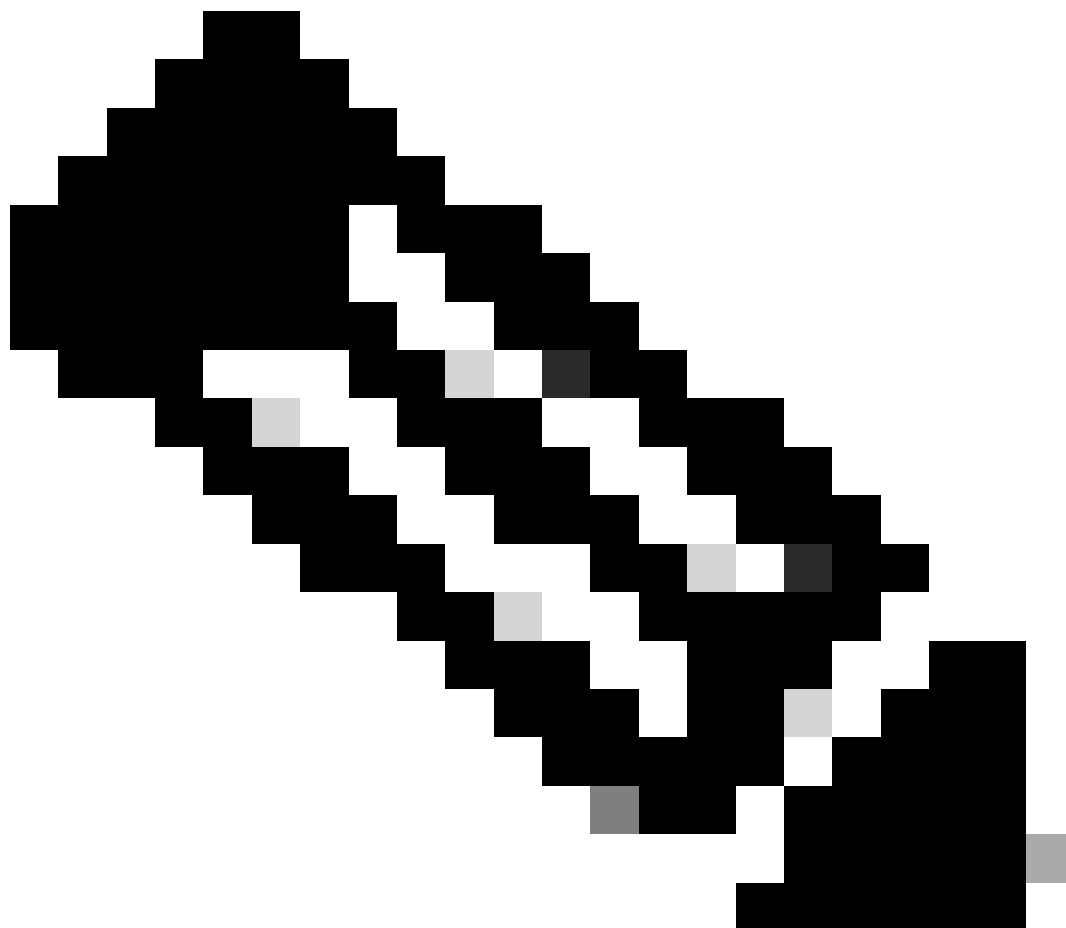
OK

5. Implementar cambios de configuración. Los cambios de configuración se implementan ahora en la interfaz de administración actual.

6. En la CLI de FTD, configure la interfaz de administración para que utilice una dirección IP estática y la puerta de enlace para que sean interfaces de datos.



- `configure network {ipv4 | ipv6} manual ip_address netmask data-interfaces`

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




Nota: Aunque no tiene pensado utilizar la interfaz de administración, debe establecer una dirección IP estática. Por ejemplo, una dirección privada para que pueda establecer la puerta de enlace en interfaces de datos. Esta gestión se utiliza para reenviar el tráfico de gestión a la interfaz de datos mediante la interfaz tap_nlp.


7. Desactive la gestión en Management Center. Haga clic en Editar y actualizar la dirección IP de dirección remota del host y la dirección secundaria (opcional) para la defensa contra amenazas en la sección Dispositivos > Administración de dispositivos > Dispositivo > Gestión y active la conexión.

Management  

Remote Host Address: 192.168.1.8

Secondary Address:

Status: 

Manager Access Interface:  [Data Interface](#)

Manager Access Details: [Configuration](#)

Activar SSH en la configuración de la plataforma

Habilite SSH para la interfaz de datos en la política de configuración de la plataforma, y aplíquelo a este dispositivo en Dispositivos > Configuración de la plataforma > Acceso SSH. Haga clic en Agregar.

1. Los hosts o las redes a los que permite realizar conexiones SSH.
2. Agregue las zonas que contienen las interfaces para permitir las conexiones SSH. Para las interfaces que no se encuentran en una zona, puede escribir el nombre de la interfaz en el campo Selected Zones/Interfaces y hacer clic en Add.
3. Haga clic en Aceptar. Implemente los cambios.

Add Secure Shell Configuration



IP Address*

+



Available Zones/Interfaces

C

- DMZ
- Inside
- outside

Add



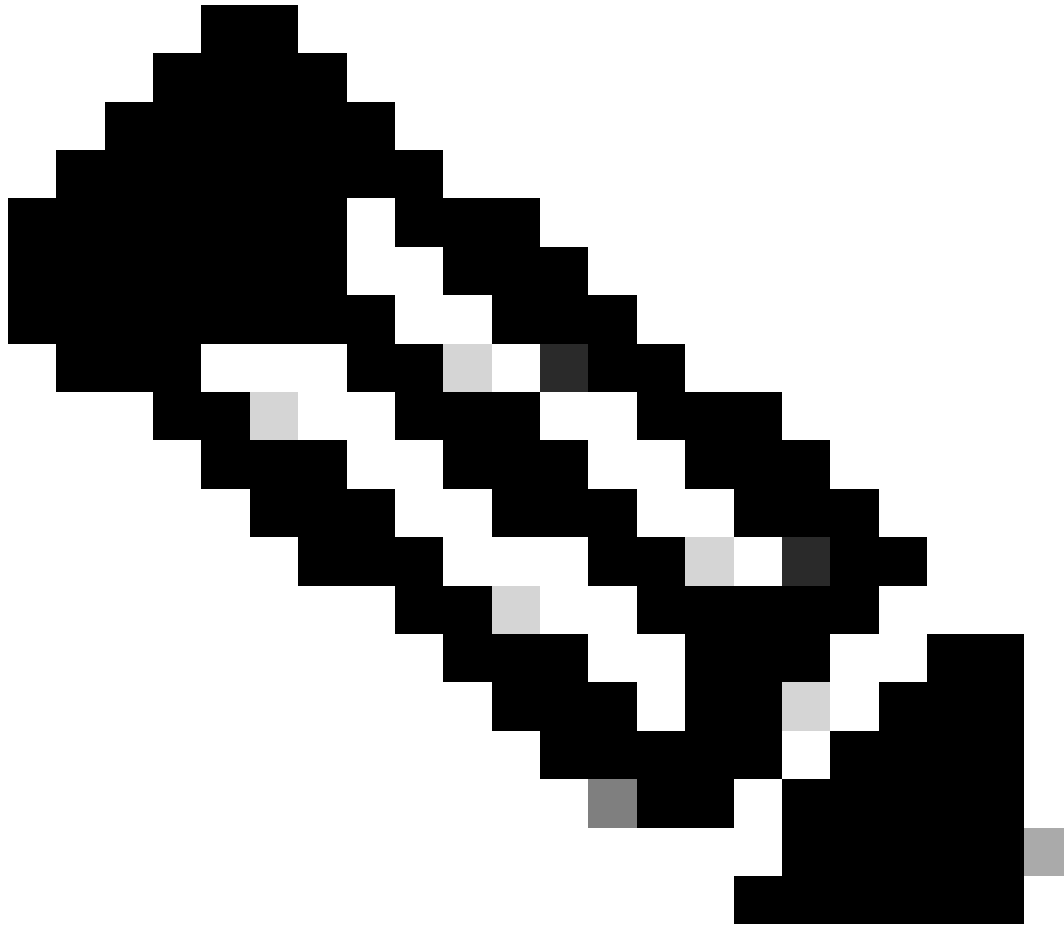
Selected Zones/Interfaces

Interface Name

Add

Cancel

OK



Nota: SSH no está habilitado de forma predeterminada en las interfaces de datos, por lo que si desea administrar la defensa contra amenazas mediante SSH, debe permitirlo explícitamente.

Verificación

Asegúrese de que la conexión de administración se establece a través de la interfaz de datos.

Verificar desde la interfaz gráfica de usuario (GUI) de FMC

En el centro de administración, verifique el estado de la conexión de administración en la página [Dispositivos > Administración de dispositivos > Dispositivo > Administración > Acceso del administrador - Detalles de configuración > Estado de conexión](#).

Management ✎

Remote Host Address:	192.168.1.30
Secondary Address:	
Status:	Connected → ✔
Manager Access Interface:	Data Interface
Manager Access Details:	Configuration

Verificar desde la interfaz de línea de comandos (CLI) de FTD

En threat defenseCLI, ingrese el comando `thesftunnel-status-brief` para ver el estado de la conexión de administración.

```
>
> 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
```

El estado muestra una conexión correcta para una interfaz de datos, mostrando la interfaz `tap_nlp` interna.

Troubleshoot

En el centro de administración, verifique el estado de la conexión de administración en la página Dispositivos > Administración de dispositivos > Dispositivo > Administración > Acceso del administrador - Detalles de configuración > Estado de conexión.

En threat defenseCLI, ingrese el comando `thesftunnel-status-brief` para ver el estado de la conexión de administración. También puede utilizar `ftunnel-status` para ver información más completa.

Estado de conexión de administración

Escenario de trabajo

```
> 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
```

Situación de no funcionamiento

```
> 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
```

Validar la información de red

En la CLI de Threat Defence, vea la configuración de red de la interfaz de datos de administración y acceso del administrador:

```
> 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
```

defenseCLI, utilice el comando para hacer ping al centro de administración desde las interfaces de datos:

```
> 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
```

En threat defenseCLI, utilice el comando para hacer ping al centro de administración desde la interfaz de administración, que enruta por la placa de interconexiones a las interfaces de datos:

```
> 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
```

Comprobar el estado de la interfaz, las estadísticas y el recuento de paquetes

En threatdefenseCLI, consulte la información sobre la interfaz de la placa de interconexiones interna, 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
```

Validar ruta en FTD para alcanzar FMC

En threatdefenseCLI, compruebe que se ha agregado la ruta predeterminada (S*) y que existen reglas NAT internas para la interfaz de administración (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
```

Comprobación de las estadísticas de conexión y del túnel seguro

```
> show running-config sftunnel
```

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



Advertencia: Durante todo el proceso de cambio de acceso del administrador, abstenerse de suprimir al administrador en el FTD o anular el registro/forzar la supresión del FTD del FMC.

Información Relacionada

- [Configuración de DNS sobre los parámetros de la plataforma](#)
- [Configuración del acceso de gestión a FTD \(HTTPS y SSH\) mediante FMC](#)

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).