

Configurar o Acesso do Gerente no FTD a partir do Gerenciamento para a Interface de Dados

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Prosseguir com a migração da interface](#)

[Habilitar SSH nas configurações da plataforma](#)

[Verificar](#)

[Verificar a partir da interface gráfica do usuário \(GUI\) do FMC](#)

[Verificar a partir da Interface de Linha de Comando \(CLI\) do FTD](#)

[Troubleshooting](#)

[Status da conexão de gerenciamento](#)

[Cenário de trabalho](#)

[Cenário não funcional](#)

[Validar as informações de rede](#)

[Validar o Estado do Gerente](#)

[Validar Conectividade de Rede](#)

[Faça ping no Management Center](#)

[Verifique o status da interface, as estatísticas e a contagem de pacotes](#)

[Validar rota no FTD para alcançar o FMC](#)

[Verificar as estatísticas de conexão e de encapsulamento](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve o processo para modificar o Manager Access no Firepower Threat Defense (FTD) de uma interface de Gerenciamento para uma interface de Dados.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firepower Threat Defense
- Firepower Management Center

Componentes Utilizados

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Cada dispositivo inclui uma única interface de gestão dedicada para a comunicação com o FMC. Você pode, opcionalmente, configurar o dispositivo para usar uma interface de dados para gerenciamento em vez da interface de gerenciamento dedicada. O acesso do FMC em uma interface de dados é útil se você quiser gerenciar o Firepower Threat Defense remotamente a partir da interface externa ou se você não tiver uma rede de gerenciamento separada. Essa alteração deve ser realizada no Firepower Management Center (FMC) para FTD gerenciado pelo FMC.

O acesso ao CVP a partir de uma interface de dados tem algumas limitações:

- Você só pode ativar o acesso de gerente em uma interface de dados física. Você não pode usar uma subinterface ou EtherChannel.
- Apenas modo de firewall roteado, usando uma interface roteada.
- Não há suporte para PPPoE. Se o seu ISP exigir PPPoE, você deverá colocar um roteador com suporte a PPPoE entre o Firepower Threat Defense e o modem WAN.
- Você não pode usar interfaces separadas de gerenciamento e somente de eventos.

Configurar

Prosseguir com a migração da interface


Observação: é altamente recomendável ter o backup mais recente do FTD e do FMC antes de continuar com as alterações.

1. Navegue até a página Devices > Device Management e clique em Edit para o dispositivo que está sendo alterado.

[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. Vá para a seção Device > Management e clique no link para Manager Access Interface.

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

O campo Interface de acesso do gerente exibe a interface de gerenciamento existente. Clique no link para selecionar o novo tipo de interface, que é a opção Data Interface na lista suspensa Manage device by e clique em Save.

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. Agora você deve prosseguir para Habilitar o acesso de gerenciamento em uma interface de dados, navegar para Dispositivos > Gerenciamento de Dispositivos > Interfaces > Editar Interface Física > Acesso do Gerenciador.

Edit Physical Interface



- General
- IPv4
- IPv6
- Path Monitoring
- Hardware Configuration
- Manager Access**
- Advanced

Enable management access

Available Networks: +

-
- 10.201.204.129
 - 192.168.1.0_24
 - any-ipv4
 - any-ipv6
 - CSM
 - Data_Store

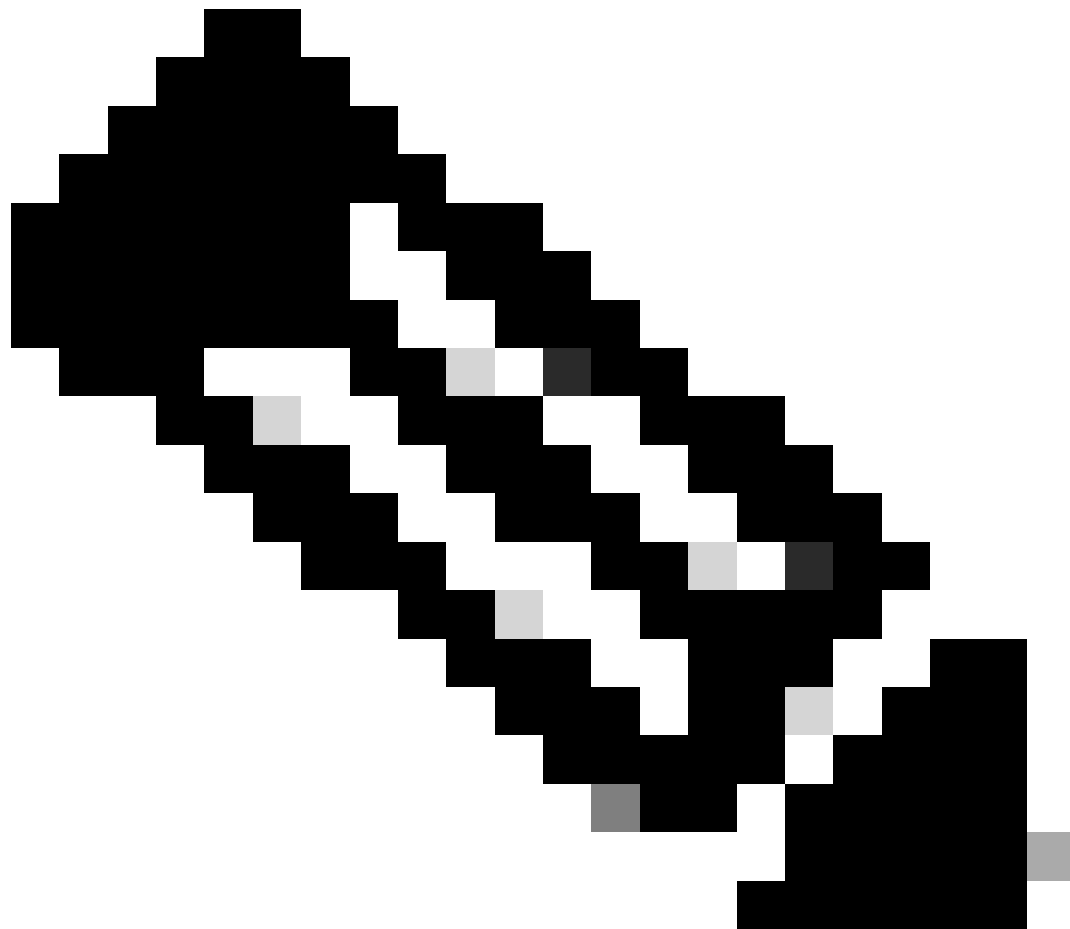
Add

Allowed Management Networks

- any

Cancel

OK



Observação: (opcional) Se você usar uma interface secundária para redundância, habilite o acesso de gerenciamento na interface usada para fins de redundância.

(Opcional) Se você usar DHCP para a interface, habilite o método DDNS do tipo de Web na caixa de diálogo Devices > Device Management > DHCP > DDNS.

(Opcional) Configure DNS em uma política de Configurações de plataforma e aplique-a a este dispositivo em Dispositivos > Configurações de plataforma > DNS.

4. Certifique-se de que a defesa contra ameaças possa rotear para o centro de gerenciamento através da interface de dados; adicione uma rota estática, se necessário, em Devices > Device Management > Routing > Static Route.

1. Clique em IPv4 ou IPv6 dependendo do tipo de rota estática que você está adicionando.
2. Escolha a Interface à qual esta rota estática se aplica.
3. Na lista Available Network, escolha a rede de destino.
4. No campo Gateway ou IPv6 Gateway, digite ou escolha o roteador do gateway, que é o próximo salto para essa rota.

(Opcional) Para monitorar a disponibilidade da rota, insira ou escolha o nome de um objeto Monitor do Contrato de Nível de Serviço (SLA) que define a política de monitoramento, no campo Rastreamento de Rota.

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

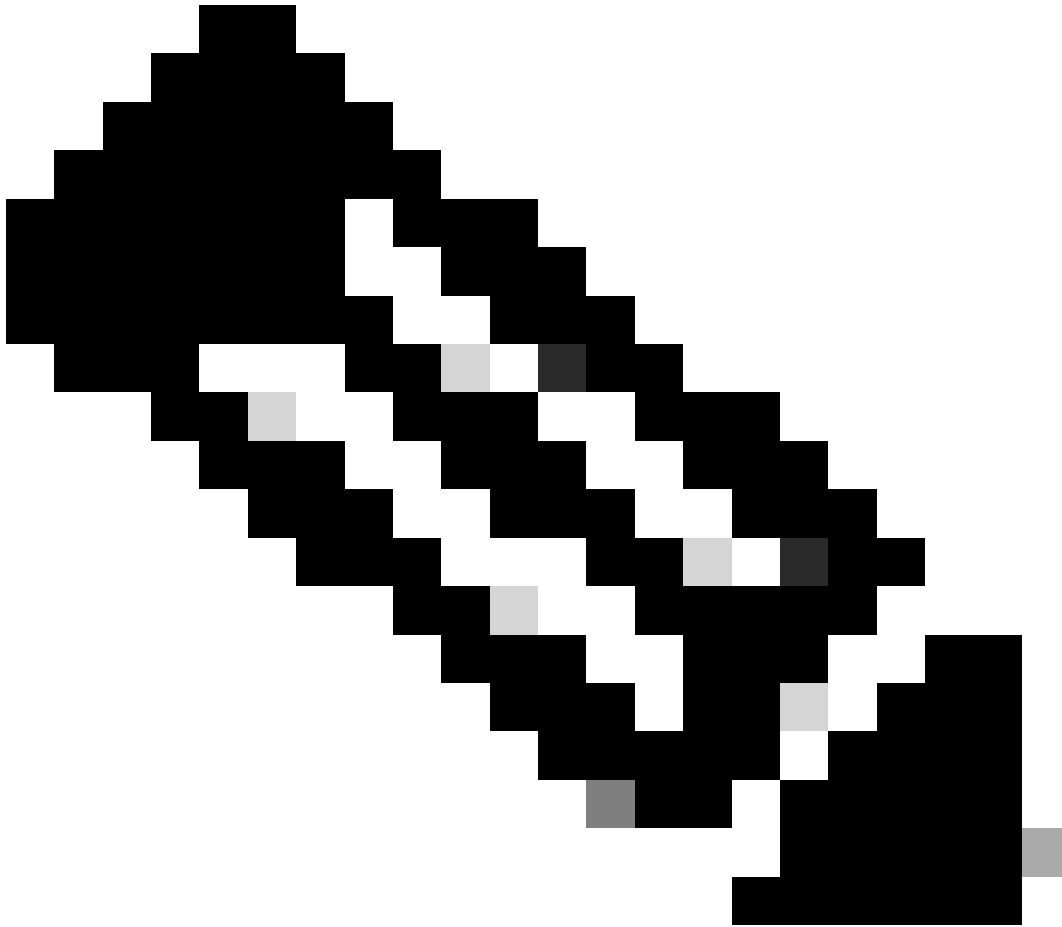
OK

5. Implantar alterações de configuração. As alterações de configuração agora são implantadas na interface de gerenciamento atual.

6. Na CLI do FTD, defina a interface de Gerenciamento para usar um endereço IP estático e o gateway como interfaces de dados.

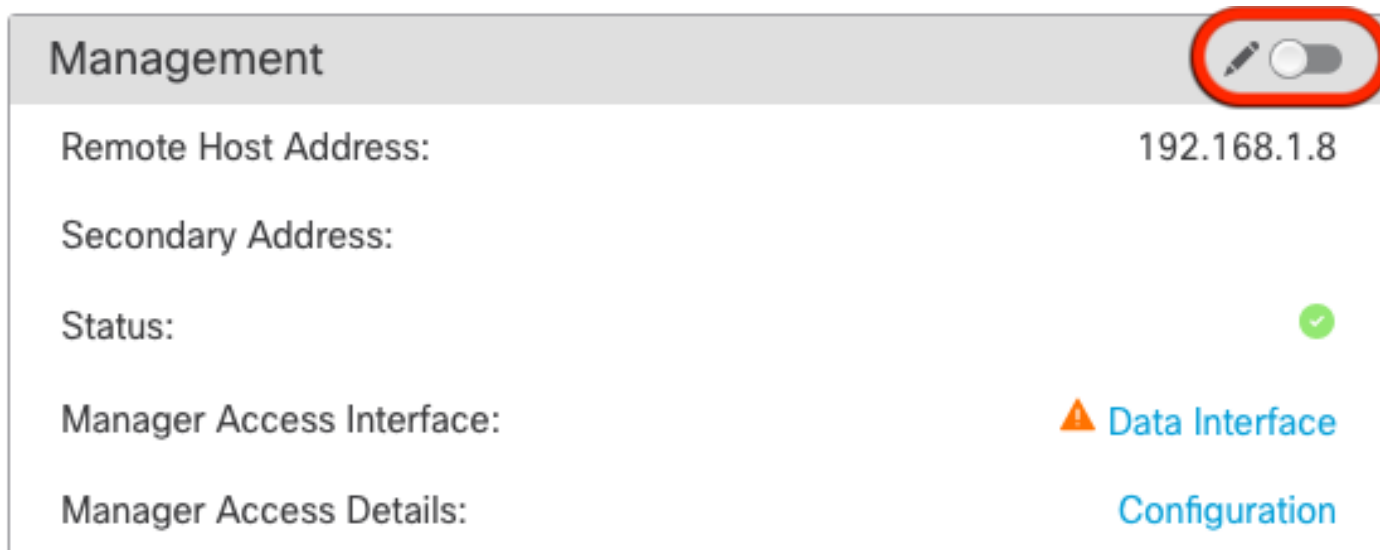
- `configure network {ipv4 | ipv6} manual ip_address netmask data-interfaces`

```
>  
>  
> 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.
```



Observação: embora você não planeje usar a interface de gerenciamento, você deve definir um endereço IP estático. Por exemplo, um endereço privado para que você possa definir o gateway como **interfaces de dados**. Esse gerenciamento é usado para encaminhar o tráfego de gerenciamento para a interface de dados usando a interface tap_nlp.

7. Desative o Gerenciamento no Management Center, clique em Editar e atualize o Endereço do Host Remoto **endereço IP** e o Endereço Secundário (Opcional) para a defesa contra ameaças na seção Dispositivos > Gerenciamento de Dispositivos > Dispositivo > **Gerenciamento e habilite a conexão.**



Management	
Remote Host Address:	192.168.1.8
Secondary Address:	
Status:	
Manager Access Interface:	Data Interface
Manager Access Details:	Configuration

Habilitar SSH nas configurações da plataforma

Ative SSH para a interface de dados na política Configurações de plataforma e aplique-o a este dispositivo em Dispositivos > Configurações de plataforma > Acesso SSH. Clique em **Adicionar**.

- Os hosts ou redes que você está permitindo para fazer conexões SSH.
- Adicione as regiões que contêm as interfaces para as quais permitir conexões SSH. Para interfaces que não estão em uma região, você pode digitar o **nome da interface** no campo **Zonas/interfaces selecionadas** e clicar em **Adicionar**.
- Click **OK. Implantar** as alterações

Add Secure Shell Configuration



IP Address*

+



Available Zones/Interfaces

C

- DMZ
- Inside
- outside

Add



Selected Zones/Interfaces

Add

Cancel

OK



Observação: o SSH não é habilitado por padrão nas interfaces de dados, portanto, se você quiser gerenciar a defesa contra ameaças usando o SSH, precisará permitir explicitamente.

Verificar

Verifique se a conexão de gerenciamento está estabelecida na interface de dados.



Verificar a partir da interface gráfica do usuário (GUI) do FMC

No centro de gerenciamento, verifique o status da conexão de gerenciamento na página Dispositivos > **Gerenciamento de dispositivos** > **Dispositivo** > Gerenciamento > Acesso do gerenciador - Detalhes da configuração > Status da conexão.

Management

Remote Host Address: 192.168.1.30

Secondary Address:

Status: **Connected**  

Manager Access Interface: [Data Interface](#)

Manager Access Details: [Configuration](#)

Verificar a partir da Interface de Linha de Comando (CLI) do FTD

Na CLI threat, insira o comando **ftunnel-status-brief** para exibir o status da conexão de gerenciamento.

```
>
> 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
```

O status mostra uma conexão bem-sucedida para uma interface de dados, mostrando a interface tap_nlp interna.

Troubleshooting

No centro de gerenciamento, verifique o status da conexão de gerenciamento na página Dispositivos > **Gerenciamento de dispositivos** > **Dispositivo** > Gerenciamento > Acesso do gerenciador - Detalhes da configuração > Status da conexão.

Na CLI threat, insira o comando **ftunnel-status-brief** para exibir o status da conexão de gerenciamento. Você também pode usar **suctunnel-status** para exibir informações mais completas.

Status da conexão de gerenciamento

Cenário de trabalho

```
> 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
```

Cenário não funcional

```
> 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 as informações de rede

Na CLI de defesa contra ameaças, exiba as configurações de rede da interface de dados de acesso do gerenciador e de gerenciamento:

```
> 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
```

Observação: este comando não mostra o status atual da conexão de gerenciamento.

Validar Conectividade de Rede

Faça ping no Management Center

Na CLI threat defense, use o comando para fazer ping no centro de gerenciamento a partir das interfaces de dados:

```
> 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
```

Na CLI threat defense, use o comando para fazer ping no centro de gerenciamento a partir da interface de gerenciamento, que roteia o painel traseiro para as interfaces de dados:

```
> 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
```

Verifique o status da interface, as estatísticas e a contagem de pacotes

Na CLI threat, consulte as informações sobre a interface interna do painel traseiro, 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 rota no FTD para alcançar o FMC

Na CLI threat, verifique se a rota padrão (S*) foi adicionada e se existem regras de NAT internas para a interface de gerenciamento (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
```

Verificar as estatísticas de conexão e de encapsulamento

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

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



Aviso: Durante todo o processo de alteração do acesso do gestor, não suprimir o gestor no DTF nem cancelar/forçar a supressão do DTF no CVP.

Informações Relacionadas

- [Configurar DNS sobre configurações de plataforma](#)
- [Configurar o acesso de gerenciamento ao FTD \(HTTPS e SSH\) através do FMC](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.