

設定FTD上從管理到資料介面的管理員存取許可權

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[繼續進行介面遷移](#)

[在平台設定上啟用SSH](#)

[驗證](#)

[從FMC圖形使用者介面\(GUI\)進行驗證](#)

[從FTD指令行介面\(CLI\)進行驗證](#)

[疑難排解](#)

[管理連線狀態](#)

[工作案例](#)

[非工作案例](#)

[驗證網路資訊](#)

[驗證管理員狀態](#)

[驗證網路連線](#)

[Ping管理中心](#)

[檢查介面狀態、統計資訊和資料包計數](#)

[驗證FTD上到達FMC的路由](#)

[檢查Sftunnel和連線統計資訊](#)

[相關資訊](#)

簡介

本文檔介紹將Firepower威脅防禦(FTD)上的Manager訪問從管理介面修改為資料介面的過程。

必要條件

需求

思科建議您瞭解以下主題：

- Firepower威脅防禦
- Firepower管理中心

採用元件

- Firepower管理中心虛擬7.4.1
- Firepower威脅防禦虛擬7.2.5

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

每台裝置都包括一個專用管理介面，用於與FMC通訊。您可以選擇將裝置配置為使用資料介面而不是專用管理介面進行管理。如果要從外部介面遠端管理Firepower威脅防禦，或者沒有單獨的管理網路，資料介面上的FMC訪問非常有用。此更改必須在FMC管理的FTD的Firepower管理中心(FMC)上執行。

從資料介面進行FMC存取有一些限制：

- 您只能在一個物理資料介面上啟用管理員訪問。不能使用子介面或EtherChannel。
- 僅路由防火牆模式，使用路由介面。
- 不支援PPPoE。如果您的ISP需要PPPoE，則必須將支援PPPoE的路由器置於Firepower威脅防禦和WAN數據機之間。
- 不能使用單獨的管理介面和僅事件介面。

設定

繼續進行介面遷移


附註：強烈建議先備份FTD和FMC，再繼續進行任何變更。

1. 導航到裝置>裝置管理頁面，點選要更改的裝置的編輯。

[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 Snort 3 192.168.1.8 - Routed	FTDv for VMware	7.2.5	N/A	Essentials	Base-ACP	↺		Edit → ↗

2. 轉至裝置 > 管理部分，按一下管理器訪問介面的連結。

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

Manager Access Interface欄位顯示現有的管理介面。點選連結選擇新介面型別，這是管理裝置方式下拉選單中的資料介面選項，然後點選儲存。

Manager Access Interface ?

i 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. 您現在必須繼續在資料介面上啟用管理訪問，導航到「裝置」 > 「裝置管理」 > 「介面」 > 「編輯物理介面」 > 「管理器訪問」。

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

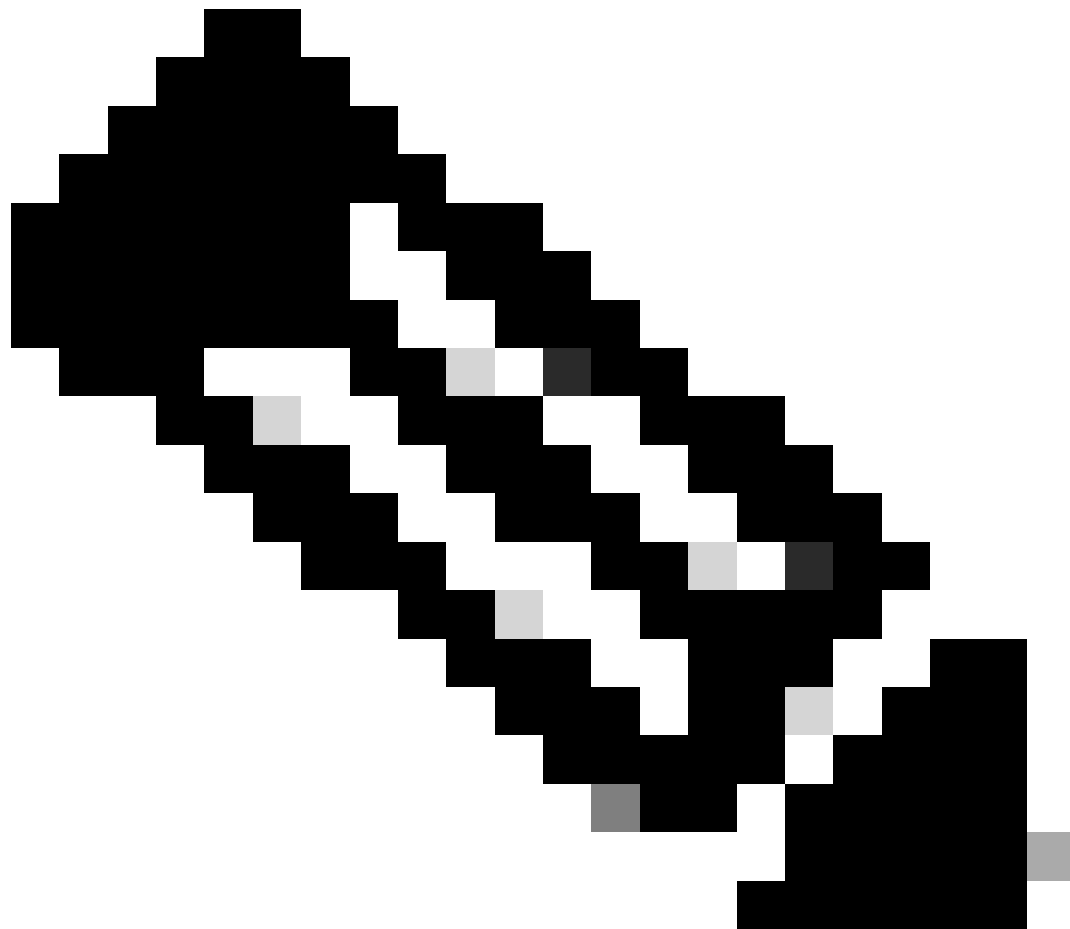
Add

Allowed Management Networks

- any

Cancel

OK



注意：(可選) 如果使用輔助介面實現冗餘，請在用於冗餘目的的介面上啟用管理訪問。

(可選) 如果使用DHCP作為介面，請在Devices > Device Management > DHCP > DDNS對話方塊中啟用Web型別「DDNS」方法。

(可選) 在平台設定策略中配置DNS，並將其應用於裝置>平台設定> DNS中的此裝置。

4. 確保威脅防禦可以透過資料介面路由到管理中心；如有必要，可在Devices > Device Management > Routing > Static Route上增加靜態路由。

1. 根據所增加的靜態路由型別，按一下IPv4或IPv6。
2. 選擇此靜態路由所應用的介面。
3. 在Available Network清單中，選擇destination network。
4. 在網關或IPv6網關欄位中，輸入或選擇作為此路由的下一跳的網關路由器。

(可選) 要監控路由可用性，請在路由跟蹤欄位中輸入或選擇定義監控策略的服務級別協定(SLA)監控對象的名稱。

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

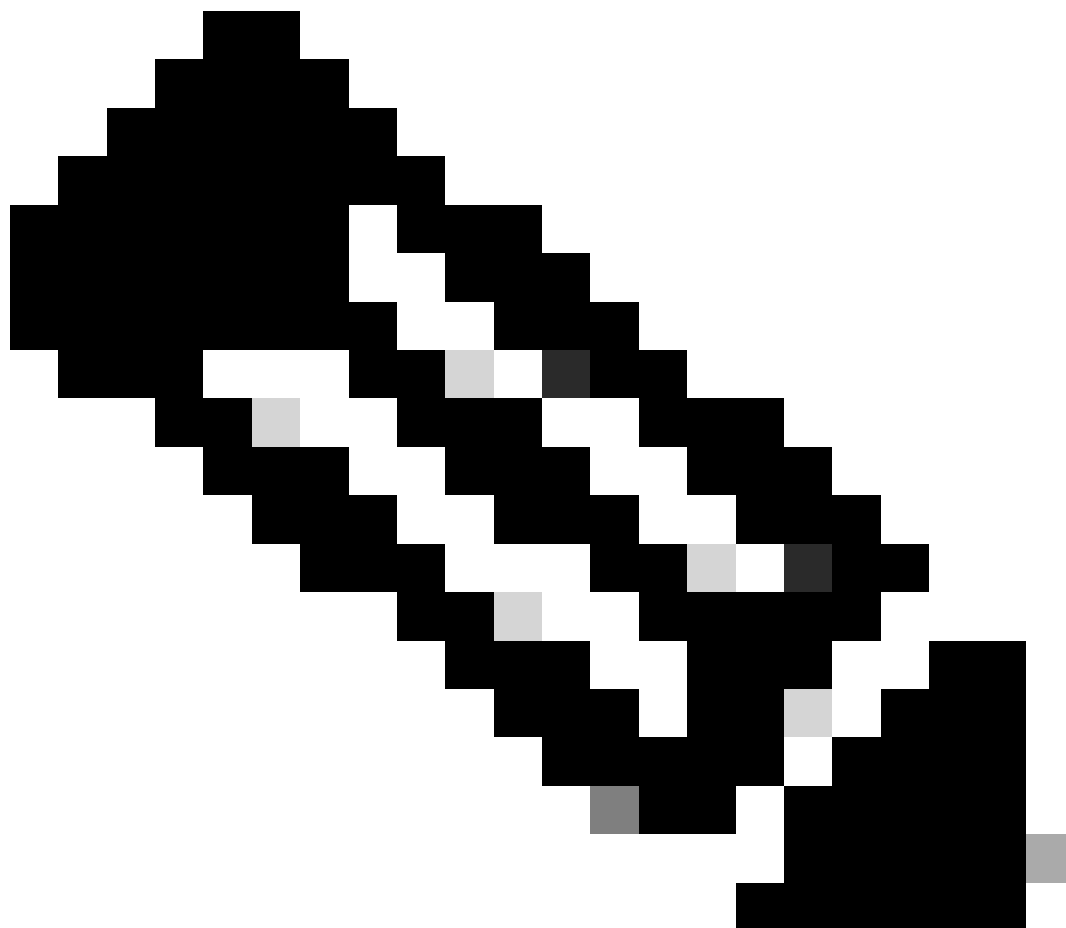
OK

5. 部署配置更改。配置更改現在透過當前管理介面進行部署。

6. 在FTD CLI上，將「管理」介面設定為使用靜態IP位址，並將閘道設定為資料介面。



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

```
>
>
> configure network ipv4 manual IP_ADDRESS192.168.1.8 NETMASK255.255.255.0 GATEWAYdata-interfaces
Setting IPv4 network configuration...
Interface eth0 speed is set to '10000baseT/Full'
Network settings changed.
```




注意：雖然不打算使用管理介面，但必須設定靜態IP地址。例如，一個私有地址，以便您可以將網關設定為**data-interfaces**。此管理用於使用tap_nlp介面將管理流量轉發到資料介面。


7. 停用管理中心中的管理，按一下「編輯」並在「裝置」(Devices) > 「裝置管理」(Device Management) > 「裝置」(Device) > 「管理」(Management)部分中更新用於威脅防禦的「遠端主機地址IP地址」(可選)和「輔助地址」(Secondary Address)，然後啟用連線。

Management  

Remote Host Address: 192.168.1.8

Secondary Address:

Status: 

Manager Access Interface:  [Data Interface](#)

Manager Access Details: [Configuration](#)

在平台設定上啟用SSH

在平台設定策略中為資料介面啟用SSH，並在Devices > **Platform Settings** > SSH Access將其應用於此裝置。按一下Add。

- 允許進行SSH連線的主機或網路。
- 增加包含允許SSH連線的介面的區域。對於不在區域中的介面，可以在Selected Zones/Interfaces欄位鍵入interface name，然後按一下Add。
- 按一下「OK」（確定）。部署變更

Add Secure Shell Configuration



IP Address*

+



Available Zones/Interfaces

C

- DMZ
- Inside
- outside

Add



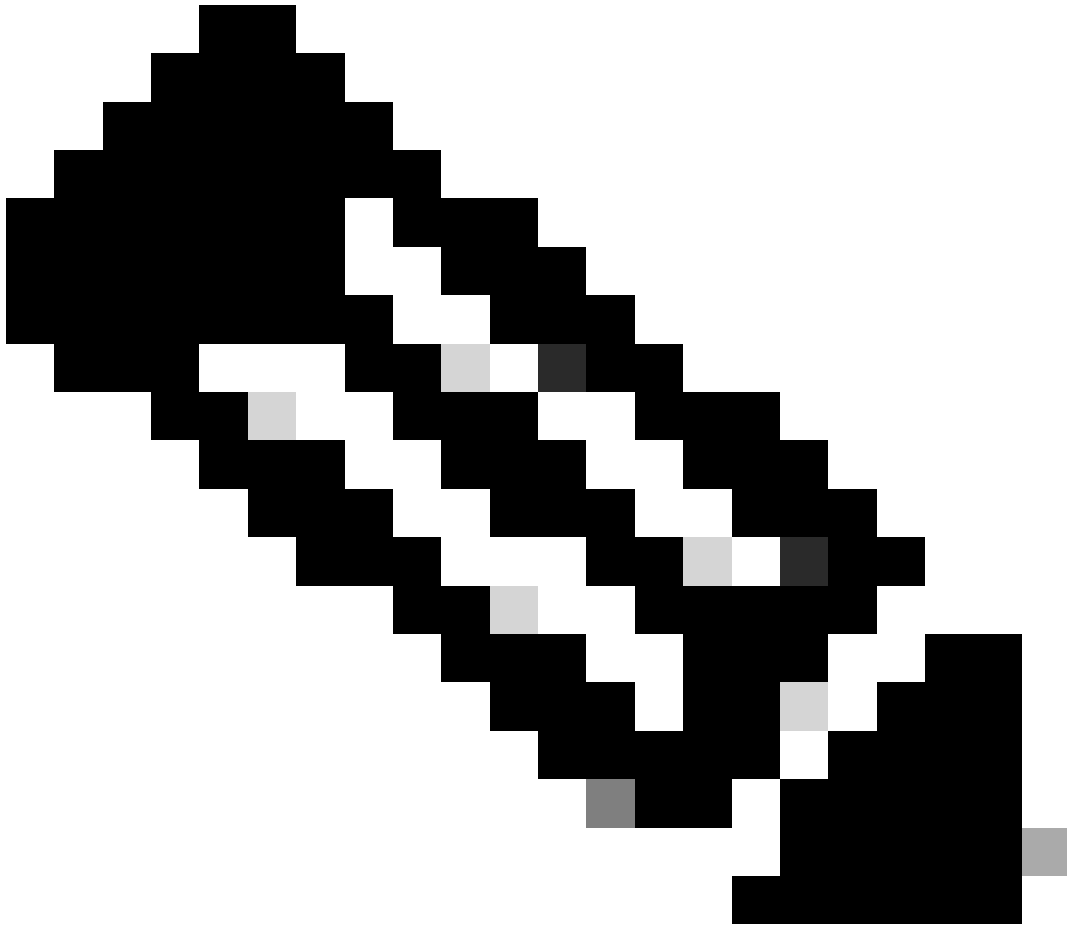
Selected Zones/Interfaces

Interface Name

Add

Cancel

OK






注意：預設情況下，資料介面上未啟用SSH，因此，如果要使用SSH管理威脅防禦，需要明確允許它。

驗證

確保已透過Data介面建立管理連線。

從FMC圖形使用者介面(GUI)進行驗證

在管理中心，檢查Devices > **Device Management** > Device > **Management** > **Manager Access - Configuration Details** > **Connection Status**頁上的管理連線狀態。

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

從FTD命令行介面(CLI)進行驗證

在威脅防禦CLI上，輸入`thesftunnel-status-brief`檢視管理連線狀態。

```
>
> 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
```

狀態顯示資料介面連線成功，並顯示內部tap_nlp介面。

疑難排解

在管理中心，檢查Devices > **Device Management** > Device > **Management** > **Manager Access - Configuration Details** > **Connection Status**頁上的管理連線狀態。

在威脅防禦CLI上，輸入`thesftunnel-status-brief`檢視管理連線狀態。您還可以使用`esftunnel-status`檢視更完整的資訊。

管理連線狀態

工作案例

```
> 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
```

非工作案例

```
> 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
```

驗證網路資訊

在威脅防禦CLI上，檢視管理和管理器訪問資料介面網路設定：

```
> 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
```

注意：此命令不顯示管理連線的當前狀態。

驗證網路連線

Ping管理中心

在threat defenseCLI中，使用命令從資料介面ping management 中心：

```
> 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
```

在threat defenseCLI中，使用命令從管理介面（透過背板路由到資料介面）對管理中心執行ping操作：

```
> ping系統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
```

檢查介面狀態、統計資訊和資料包計數

在threat防禦CLI中，請參閱關於內部底板介面的資訊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
```

驗證FTD上到達FMC的路由

在threat defenseCLI中，檢查是否已增加預設路由(S*)，以及管理介面(nlp_int_tap)是否存在內部NAT規則。

>顯示路由


```
> 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
```

```
>顯示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
```

檢查Sftunnel和連線統計資訊

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

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



警告：在變更管理員存取權的整個過程中，請勿刪除FTD上的管理員或取消註冊/強制刪除FTD自FMC。

相關資訊

- [透過平台設定配置DNS](#)
- [透過FMC設定對FTD \(HTTPS和SSH\) 的管理存取](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。