

# Configura accesso Manager su FTD da Gestione a interfaccia dati

## Sommario

---

### [Introduzione](#)

### [Prerequisiti](#)

#### [Requisiti](#)

#### [Componenti usati](#)

### [Premesse](#)

### [Configurazione](#)

#### [Procedere con la migrazione dell'interfaccia](#)

#### [Abilitazione del protocollo SSH sulle impostazioni della piattaforma](#)

### [Verifica](#)

#### [Verifica dall'interfaccia grafica utente \(GUI\) di FMC](#)

#### [Verifica da CLI \(Command Line Interface\) FTD](#)

### [Risoluzione dei problemi](#)

#### [Stato connessione di gestione](#)

##### [Scenario di lavoro](#)

##### [Scenario non lavorativo](#)

#### [Convalida le informazioni di rete](#)

#### [Convalida lo stato del manager](#)

#### [Convalida connettività di rete](#)

##### [Eseguire il ping del centro di gestione](#)

##### [Controllo dello stato dell'interfaccia, delle statistiche e del numero di pacchetti](#)

##### [Convalida ciclo di lavorazione su FTD per raggiungere FMC](#)

##### [Controllare le statistiche di Sftunnel e connessione](#)

### [Informazioni correlate](#)

---

## Introduzione

In questo documento viene descritto il processo di modifica di Manager Access su Firepower Threat Defense (FTD) da un'interfaccia di gestione a un'interfaccia dati.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Firepower Threat Defense
- Firepower Management Center

## Componenti usati

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

Ogni dispositivo è dotato di un'unica interfaccia di gestione dedicata per la comunicazione con il CCP. Se si desidera, è possibile configurare il dispositivo in modo che utilizzi un'interfaccia dati per la gestione anziché l'interfaccia di gestione dedicata. L'accesso FMC a un'interfaccia dati è utile se si desidera gestire Firepower Threat Defense in remoto dall'interfaccia esterna oppure non si dispone di una rete di gestione separata. Questa modifica deve essere eseguita su Firepower Management Center (FMC) per FTD gestito da FMC.

L'accesso al FMC da un'interfaccia dati presenta alcune limitazioni:

- È possibile abilitare l'accesso al manager solo su un'interfaccia dati fisica. Non è possibile utilizzare una sottointerfaccia o EtherChannel.
- Solo modalità firewall con routing, tramite un'interfaccia con routing.
- PPPoE non supportato. Se l'ISP richiede PPPoE, è necessario collegare un router con supporto PPPoE tra Firepower Threat Defense e il modem WAN.
- Non è possibile utilizzare interfacce separate di gestione e solo eventi.

## Configurazione

Procedere con la migrazione dell'interfaccia

---

Nota: si consiglia di disporre del backup più recente di FTD e FMC prima di procedere con le modifiche.

1. Passare alla pagina Dispositivi > Gestione dispositivi, quindi fare clic su Modifica per il dispositivo che si sta modificando.

[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. Andare alla sezione Dispositivo > Gestione e fare clic sul collegamento per Interfaccia di accesso Manager.

Management <span style="float: right;">✎ <input type="checkbox"/></span>	
Remote Host Address:	192.168.1.8
Secondary Address:	
Status:	<span style="color: green;">✔</span>
Manager Access Interface:	<span style="color: red;">→</span> <a href="#">Management Interface</a>

Nel campo Interfaccia di accesso responsabile viene visualizzata l'interfaccia di gestione esistente. Fare clic sul collegamento per selezionare il nuovo tipo di interfaccia, ovvero l'opzione Interfaccia dati nell'elenco a discesa Gestisci dispositivo per e fare clic su Salva.

## 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. A questo punto, è necessario passare a Abilita accesso di gestione su un'interfaccia dati, selezionare Dispositivi > Gestione dispositivi > Interfacce > Modifica interfaccia fisica > Accesso manager.

# 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

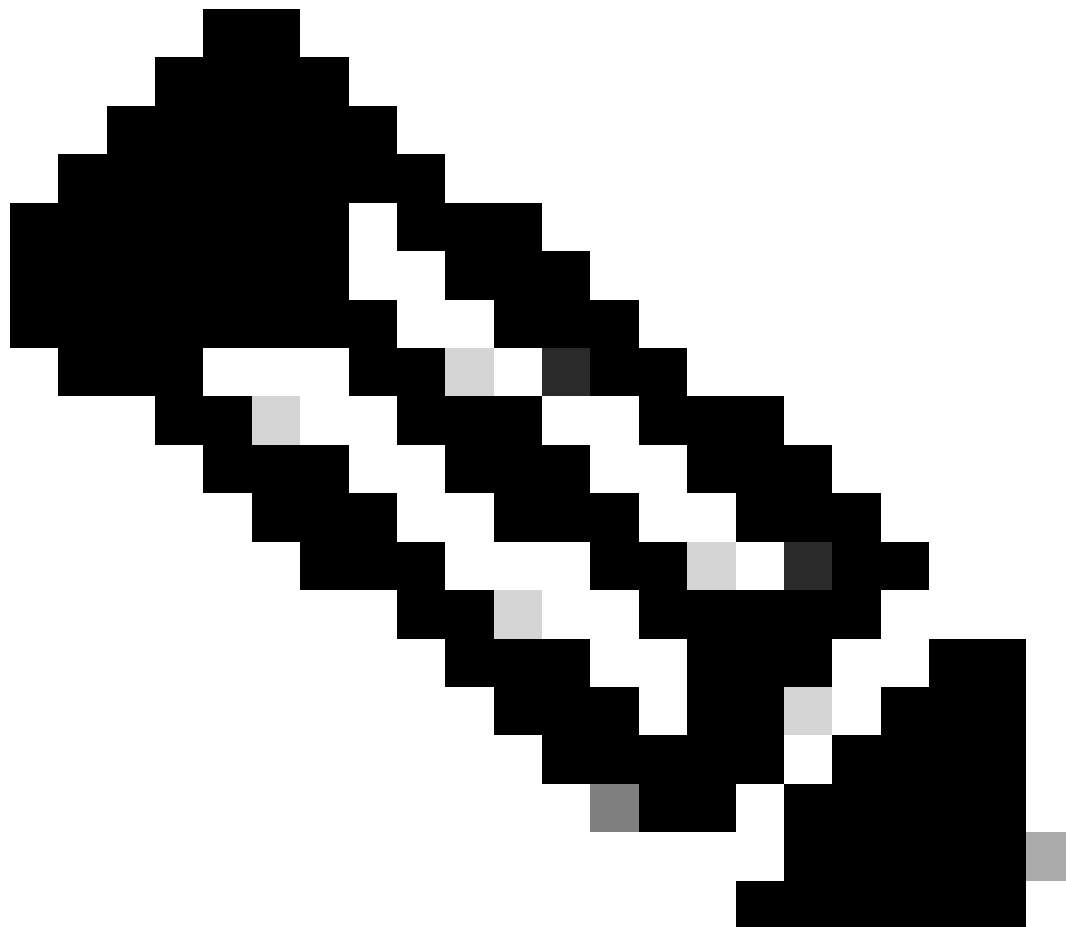
Add

Allowed Management Networks

any

Cancel

OK



---

Nota: (facoltativo) se si utilizza un'interfaccia secondaria per la ridondanza, abilitare l'accesso di gestione sull'interfaccia utilizzata a scopo di ridondanza.

(Facoltativo) Se si utilizza DHCP per l'interfaccia, abilitare il metodo DDNS di tipo Web nella finestra di dialogo Dispositivi > Gestione dispositivi > DHCP > DNS.

(Facoltativo) Configurare il DNS in un criterio Impostazioni piattaforma e applicarlo al dispositivo in Dispositivi > Impostazioni piattaforma > DNS.

---

4. Assicurarsi che la difesa dalle minacce possa indirizzare al centro di gestione tramite l'interfaccia dati; aggiungere una route statica, se necessario, su Dispositivi > Gestione dispositivi > Routing > Route statica.

1. Fare clic su IPv4o IPv6 a seconda del tipo di route statica che si sta aggiungendo.
2. Selezionare l'interfaccia a cui applicare la route statica.
3. Nell'elenco Reti disponibili, scegliere la rete di destinazione.
4. Nel campo Gateway o Gateway IPv6, immettere o scegliere il router gateway che rappresenta l'hop successivo per la route.

(Facoltativo) Per controllare la disponibilità del ciclo di lavorazione, immettere o scegliere il nome di un oggetto di monitoraggio del contratto di servizio (SLA) che definisce il criterio di monitoraggio nel campo Tracciamento del ciclo di lavorazione.

## 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

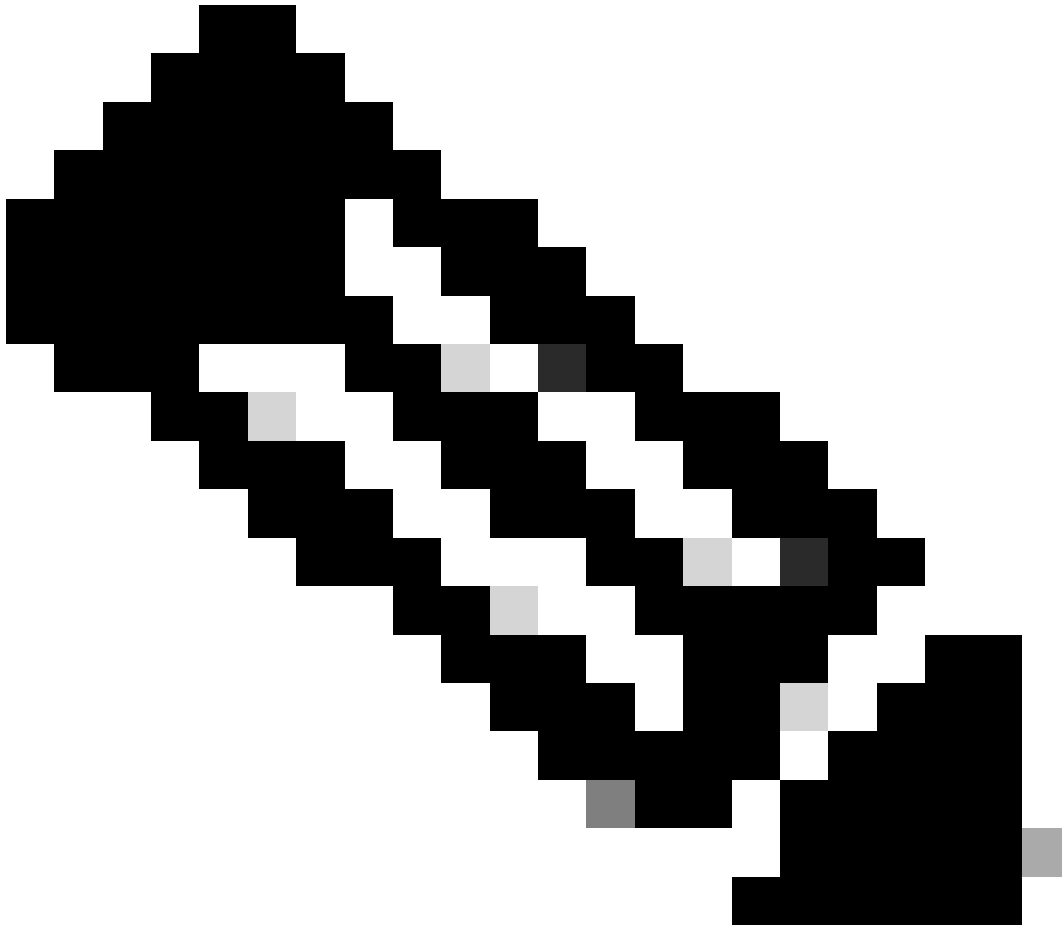
5. Distribuire le modifiche alla configurazione. Le modifiche alla configurazione vengono ora distribuite sull'interfaccia di gestione corrente.

6. Dalla CLI dell'FTD, impostare l'interfaccia di gestione in modo che utilizzi un indirizzo IP statico e il gateway come interfacce dati.

- `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.
```

---

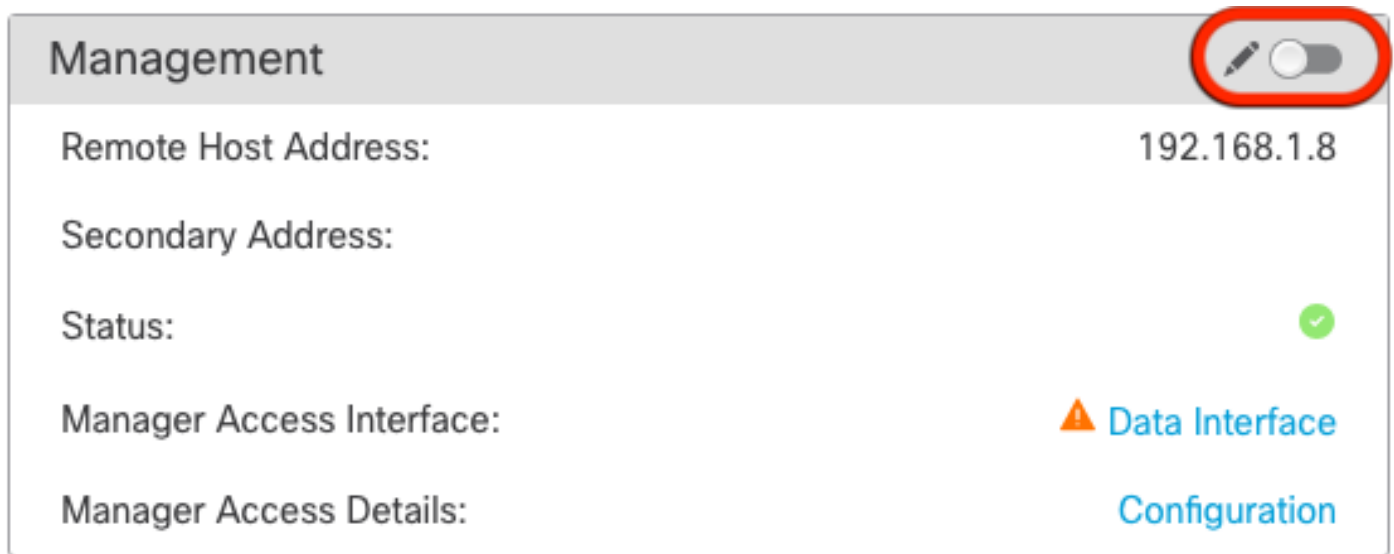


**Nota:** sebbene non si preveda di utilizzare l'interfaccia di gestione, è necessario impostare un indirizzo IP statico. Ad esempio, un indirizzo privato che consente di impostare il gateway sulle **interfacce dati**. Questa gestione viene utilizzata per inoltrare il traffico di gestione all'interfaccia dati tramite l'interfaccia tap\_nlp.

---



7. Disabilitare la gestione nel centro di gestione, fare clic su **Modifica** e aggiornare l'**indirizzo IP dell'indirizzo** dell'host remoto e l'**(Facoltativo)indirizzo secondario** per la difesa dalle minacce nella **sezione Dispositivi > Gestione dispositivi > Dispositivo > Gestione e abilitare la connessione**.



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

Abilitazione del protocollo SSH sulle impostazioni della piattaforma

Abilitare SSH per l'interfaccia dati nel criterio Impostazioni piattaforma e applicarlo al dispositivo in **Dispositivi > Impostazioni piattaforma > Accesso SSH**. Fare clic su **Aggiungi**.

- Gli host o le reti a cui è consentito effettuare connessioni SSH.
- Aggiungere le zone contenenti le interfacce a cui consentire le connessioni SSH. Per le interfacce non incluse in una zona, è possibile digitare il **nome dell'interfaccia** nell'elenco **Zone selezionate/Interfacce** e fare clic su **Aggiungi**.
- Fare clic su **OK. Distribuire** le modifiche

# Add Secure Shell Configuration



IP Address\* +



Available Zones/Interfaces C

- DMZ
- Inside
- outside

Add

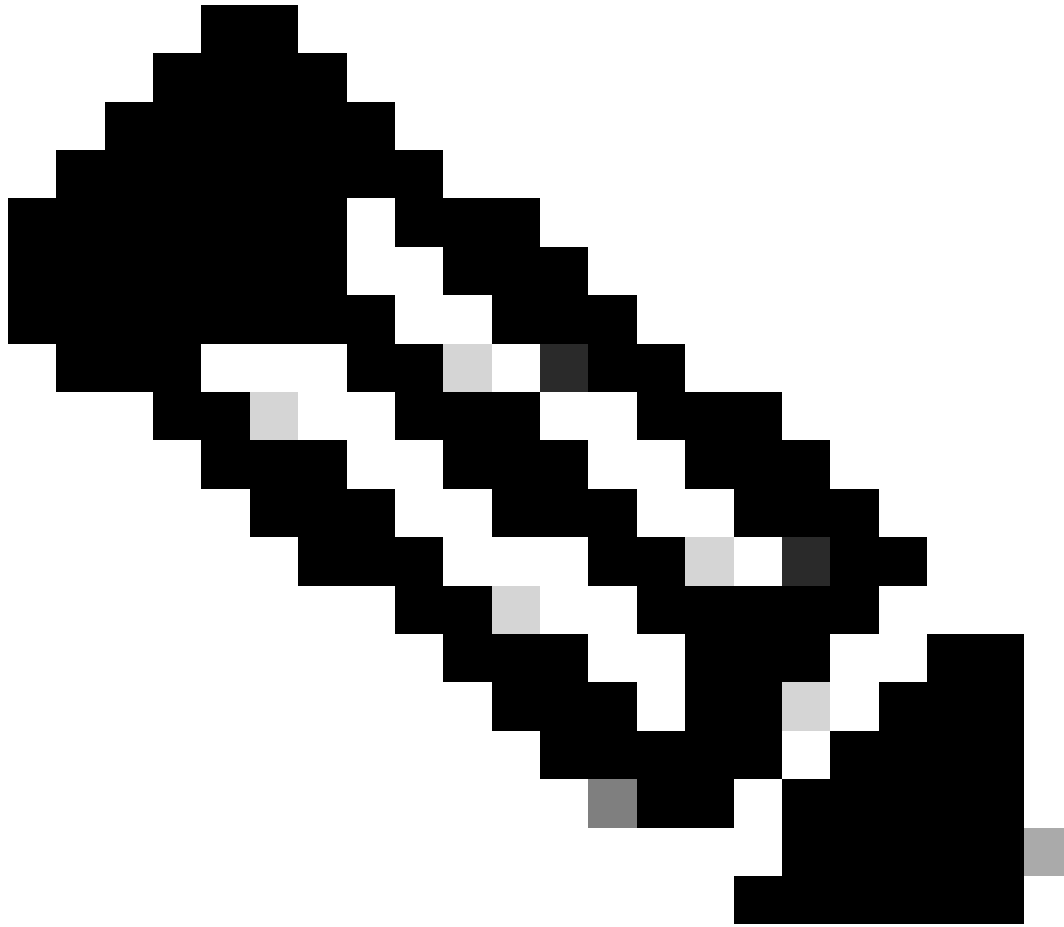


Selected Zones/Interfaces

Add

Cancel

OK



**Nota:** SSH non è abilitato per impostazione predefinita sulle interfacce dati, quindi se si desidera gestire la difesa dalla minaccia con SSH, è necessario abilitarlo esplicitamente.

---

Verifica

Verificare che la connessione di gestione sia stabilita tramite l'interfaccia dati.

Verifica dall'interfaccia grafica utente (GUI) di FMC

Nel centro di gestione, controllare lo stato della connessione di gestione nella **pagina** Dispositivi > **Gestione dispositivi** > **Dispositivo** > **Gestione** > **Accesso manager - Dettagli configurazione** > **Stato connessione**.

**Management**

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

Verifica da CLI (Command Line Interface) FTD

In corrispondenza di threat defenseCLI, immettere **thesftunnel-status-brief** per visualizzare lo stato della connessione di gestione.

```
>
> 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
```

Lo stato indica che la connessione per un'interfaccia dati è stata stabilita correttamente e mostra l'interfaccia tap\_nlp interna.

Risoluzione dei problemi

Nel centro di gestione, controllare lo stato della connessione di gestione nella **pagina** Dispositivi > **Gestione dispositivi** > **Dispositivo** > **Gestione** > **Accesso manager - Dettagli configurazione** > **Stato connessione**.

In corrispondenza di threat defenseCLI, immettere **thesftunnel-status-brief** per visualizzare lo stato della connessione di gestione. È inoltre possibile **utilizzare ftunnel-status** per visualizzare informazioni più complete.

Stato connessione di gestione

Scenario di lavoro

```
> 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
```

Scenario non lavorativo

```
> 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
```

Convalida le informazioni di rete

In corrispondenza di threat defenseCLI, visualizzare le impostazioni di rete dell'interfaccia di accesso ai dati di gestione e 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
```

---

**Nota:** questo comando non visualizza lo stato corrente della connessione di gestione.

---

Convalida connettività di rete

Eseguire il ping del centro di gestione

Su threat defenseCLI, usare il comando per eseguire il ping del centro di gestione dalle interfacce dati:

```
> ping ip_fmc
```

```
> 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
```

In corrispondenza di threat defenseCLI, usare il comando per eseguire il ping del centro di gestione dall'interfaccia di gestione, che instrada il backplane verso le interfacce dati:

```
> sistema ping 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
```

Controllo dello stato dell'interfaccia, delle statistiche e del numero di pacchetti

Su threat defenseCLI, vedere le informazioni sull'interfaccia del backplane interno, 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
```

Convalida ciclo di lavorazione su FTD per raggiungere FMC

In corrispondenza di threat defenseCLI, verificare che la route predefinita (S\*) sia stata aggiunta e che esistano regole NAT interne per l'interfaccia di gestione (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
```

Controllare le statistiche di Sftunnel e connessione

> show running-config tunnel

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



**Avvertenza:** durante il processo di modifica dell'accesso del responsabile, evitare di eliminare il responsabile sull'FTD o annullare la registrazione/forzare l'eliminazione dell'FTD dall'FMC.

---

#### Informazioni correlate

- [Configurare le impostazioni DNS su piattaforma](#)
- [Configurazione dell'accesso di gestione a FTD \(HTTPS e SSH\) tramite FMC](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).