

Configurazione, verifica e risoluzione dei problemi di registrazione delle periferiche Firepower

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Opzioni di progettazione](#)

[Quali informazioni vengono scambiate tramite SFTUNNEL?](#)

[Quale protocollo/porta viene utilizzato dallo sftunnel?](#)

[Come modificare la porta TCP Sftunnel su FTD?](#)

[Quante connessioni vengono stabilite dallo sftunnel?](#)

[Quale Dispositivo Avvia Ogni Canale?](#)

[Configurazione](#)

[Nozioni di base sulla registrazione](#)

[Scenario 1. Indirizzo IP statico FMC e FTD](#)

[Scenario 2. Indirizzo IP DHCP FTD - Indirizzo IP statico FMC](#)

[Scenario 3. Indirizzo IP statico FTD - Indirizzo IP DHCP FMC](#)

[Scenario 4. Registrazione FTD su HA FMC](#)

[Scenario 5. FTD HA](#)

[Scenario 6. Cluster FTD](#)

[Risoluzione dei problemi comuni](#)

[1. Sintassi non valida nella CLI FTD](#)

[2. Mancata corrispondenza della chiave di registrazione tra FTD e FMC](#)

[3. Problemi di connettività tra FTD e FMC](#)

[4. Software incompatibile tra FTD e FMC](#)

[5. Differenza temporale tra FTD e FMC](#)

[6. sftunnel Processo inattivo o disabilitato](#)

[7. Registrazione FTD in attesa sul CCP secondario](#)

[8. Registrazione non riuscita a causa dell'MTU del percorso](#)

[9. L'FTD viene annullato dopo una modifica del bootstrap dall'interfaccia utente di Gestione chassis](#)

[10. FTD perde l'accesso al FMC a causa dei messaggi di reindirizzamento ICMP](#)

Introduzione

Questo documento descrive il funzionamento, la verifica e le procedure di risoluzione dei problemi della connessione (sftunnel) tra un Firepower Threat Defense (FTD) gestito e il Firepower Management Center (FMC) gestito. Le informazioni e gli esempi si basano sul FTD, ma la

maggior parte dei concetti sono applicabili anche ai NGIPS (appliance serie 7000/8000) o a un modulo FirePOWER su ASA55xx.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software FTD 6.6.x e 6.5.x
- Software FMC 6.6.x

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

Un FTD supporta due modalità di gestione principali:

- Off-box tramite FMC (gestione remota)
- On-box tramite Firepower Device Manager (FDM) e/o Cisco Defense Orchestrator (CDO), noto anche come gestione locale

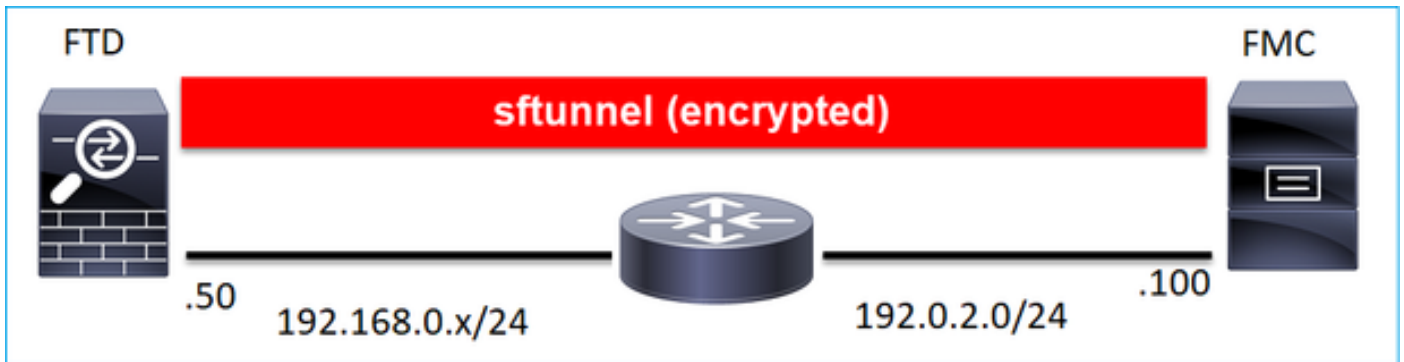
In caso di gestione remota, l'FTD deve prima registrarsi al CCP che utilizza una procedura nota come registrazione del dispositivo. Una volta effettuata la registrazione, l'FTD e il CCP istituiscono un tunnel protetto chiamato sftunnel (il nome deriva dal tunnel Sourcefire).

Opzioni di progettazione

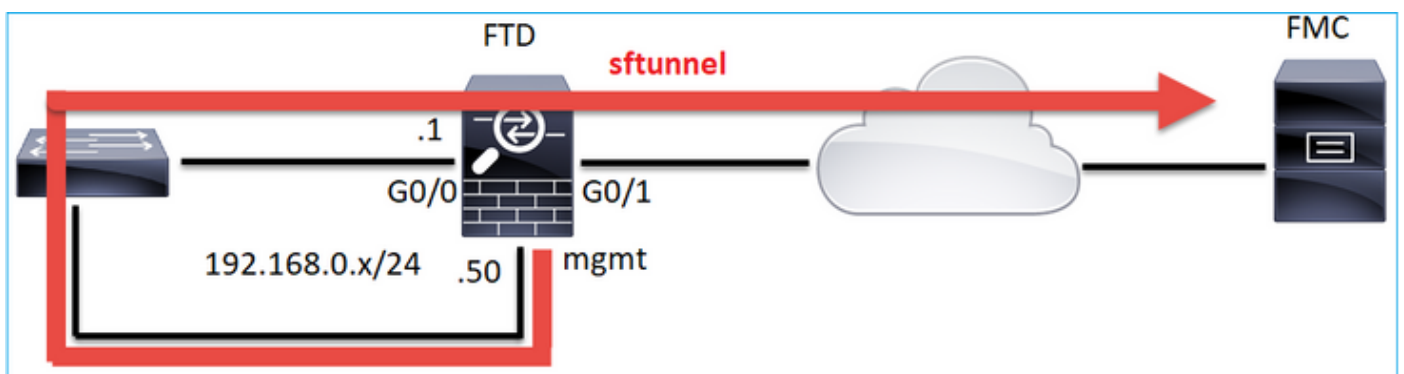
Dal punto di vista della progettazione, l'FTD - FMC può trovarsi nella stessa subnet L3:



o essere separati da reti diverse:



Nota: Il sftunnel può anche passare attraverso lo stesso FTD. Questa progettazione **non è consigliata**. Il motivo è che un problema del data-plane FTD può interrompere la comunicazione tra FTD e FMC.



Quali informazioni vengono scambiate tramite SFTUNNEL?

L'elenco contiene la maggior parte delle informazioni trasmesse tramite il tunnel sfc:

- Heartbeat dell'accessorio (keepalive)
- Sincronizzazione ora (NTP)
- Eventi (connessione, intrusione/IPS, file, SSL e così via)
- Ricerche malware

- Eventi/avvisi di integrità
- Informazioni su utenti e gruppi (per i criteri di identità)
- Informazioni sullo stato HA FTD
- Informazioni sullo stato del cluster FTD
- Informazioni/eventi Security Intelligent (SI)
- Informazioni/eventi Threat Intelligence Director (TID)
- File catturati
- Eventi di individuazione della rete
- Pacchetto di criteri (distribuzione criteri)
- Pacchetti di aggiornamento software
- Pacchetti di patch software
- VDB
- SRU

Quale protocollo/porta viene utilizzato dallo sftunnel?

Lo sftunnel utilizza la porta TCP 8305. Nel back-end è un tunnel TLS:

No.	Source	Destination	Protocol	Length	TCP Segment	Info
57	10.62.148.75	10.62.148.42	TCP	74	0 47709 → 8305	[SYN] Seq=2860693630 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1176730050 TSecr=0 WS=128
58	10.62.148.42	10.62.148.75	TCP	74	0 8305 → 47709	[SYN, ACK] Seq=279535377 Ack=2860693631 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=55847291
59	10.62.148.75	10.62.148.42	TCP	66	0 47709 → 8305	[ACK] Seq=2860693631 Ack=279535378 Win=29312 Len=0 TSval=1176730050 TSecr=55847291
60	10.62.148.75	10.62.148.42	TLSv1.2	229	163	Client Hello
61	10.62.148.42	10.62.148.75	TCP	66	0 8305 → 47709	[ACK] Seq=279535378 Ack=2860693794 Win=30080 Len=0 TSval=55847291 TSecr=1176730051
62	10.62.148.42	10.62.148.75	TLSv1.2	1514	1448	Server Hello
63	10.62.148.75	10.62.148.42	TCP	66	0 47709 → 8305	[ACK] Seq=2860693794 Ack=279536826 Win=32128 Len=0 TSval=1176730053 TSecr=55847292
64	10.62.148.42	10.62.148.75	TLSv1.2	803	737	Certificate, Certificate Request, Server Hello Done
65	10.62.148.75	10.62.148.42	TCP	66	0 47709 → 8305	[ACK] Seq=2860693794 Ack=279537563 Win=35072 Len=0 TSval=1176730053 TSecr=55847292
66	10.62.148.75	10.62.148.42	TLSv1.2	2581	2515	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
67	10.62.148.42	10.62.148.75	TCP	66	0 8305 → 47709	[ACK] Seq=279537563 Ack=2860696309 Win=35072 Len=0 TSval=55847292 TSecr=1176730056
68	10.62.148.42	10.62.148.75	TLSv1.2	1284	1218	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
69	10.62.148.75	10.62.148.42	TLSv1.2	364	298	Application Data
70	10.62.148.42	10.62.148.75	TLSv1.2	364	298	Application Data
71	10.62.148.42	10.62.148.75	TLSv1.2	103	37	Application Data
72	10.62.148.75	10.62.148.42	TCP	66	0 47709 → 8305	[ACK] Seq=2860696607 Ack=279539116 Win=40832 Len=0 TSval=1176730059 TSecr=55847292
73	10.62.148.42	10.62.148.75	TLSv1.2	367	301	Application Data
74	10.62.148.75	10.62.148.42	TLSv1.2	103	37	Application Data
75	10.62.148.75	10.62.148.42	TLSv1.2	367	301	Application Data

Come modificare la porta TCP Sftunnel su FTD?

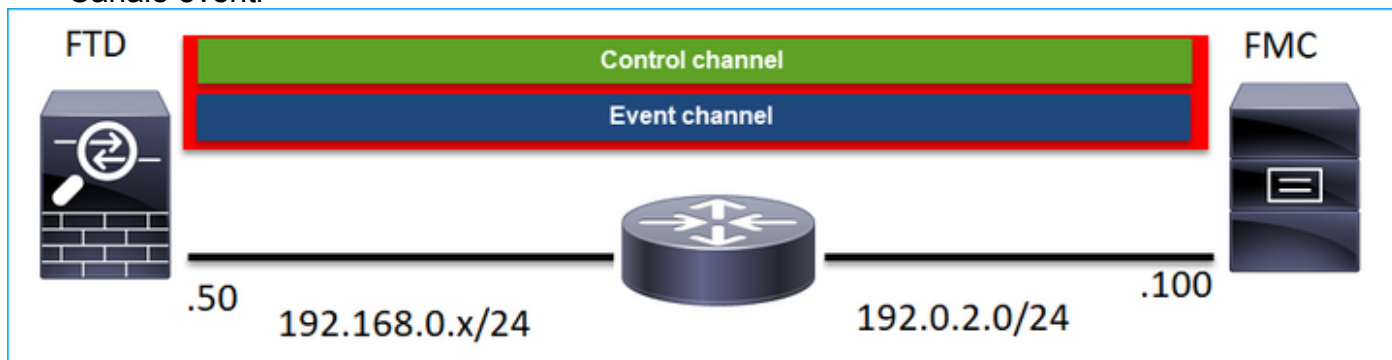
```
> configure network management-port 8306
Management port changed to 8306.
```

Nota: In questo caso è necessario modificare anche la porta su FMC (**Configurazione > Interfacce di gestione > Impostazioni condivise**). Ciò riguarda tutti gli altri dispositivi già registrati sullo stesso CCP. Cisco consiglia di mantenere le impostazioni predefinite per la porta di gestione remota, ma se la porta di gestione è in conflitto con altre comunicazioni sulla rete, è possibile scegliere una porta diversa. Se si modifica la porta di gestione, è necessario modificarla per tutti i dispositivi della distribuzione che devono comunicare tra loro.

Quante connessioni vengono stabilite dallo sftunnel?

Il sftunnel stabilisce 2 connessioni (canali):

- Canale di controllo
- Canale eventi



Quale Dispositivo Avvia Ogni Canale?

Dipende dallo scenario. Verificare gli scenari descritti nel resto del documento.

Configurazione

Nozioni di base sulla registrazione

CLI FTD

Su FTD la sintassi di base per la registrazione del dispositivo è:

```
>configurare manager add <Host FMC> <Chiave di registrazione> <ID NAT>
```

Valore

Host FMC

Chiave di registrazione

ID NAT

Descrizione

Può essere:

- Nome host
- indirizzo ipv4
- indirizzo ipv6
- DONTRESOLVE

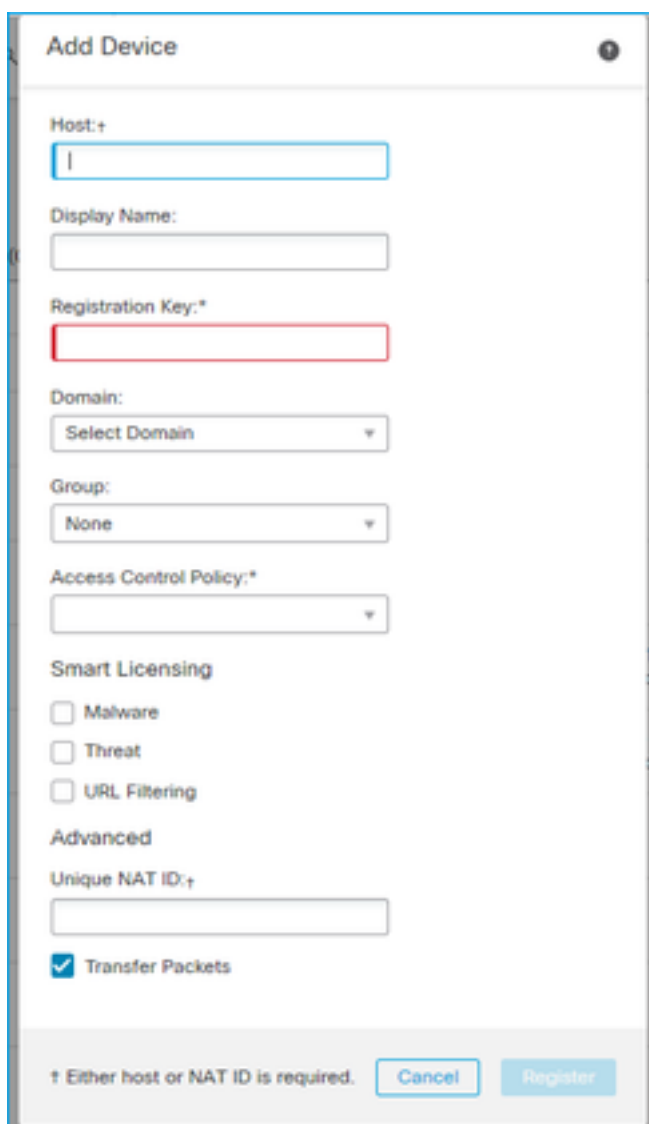
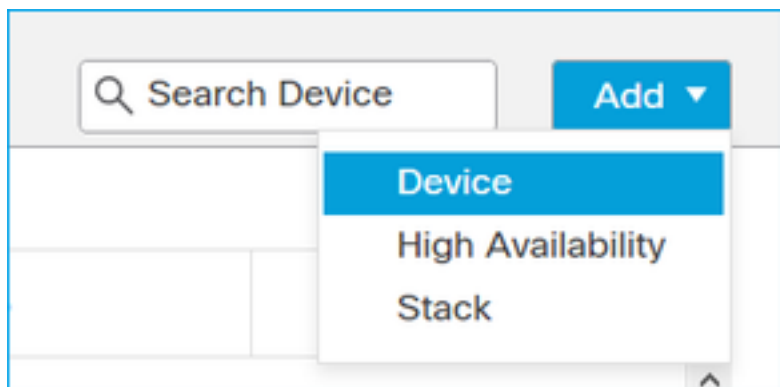
Si tratta di una stringa alfanumerica segreta (compresa tra 2 e 36 caratteri) utilizzata per la registrazione del dispositivo. Sono consentiti solo caratteri alfanumerici, trattini (-), caratteri di sottolineatura (_) e punti (.).

Stringa alfanumerica utilizzata durante il processo di registrazione tra il CCP e il dispositivo **quando un ID NAT non specifica un indirizzo IP**. Specificare lo stesso ID NAT nel CCP.

Per ulteriori informazioni, consultare la [guida di riferimento dei comandi di Cisco Firepower Threat Defense](#)

UI FMC

In FMC selezionare **Dispositivi > Gestione dispositivi**. Selezionare **Aggiungi > Dispositivo**

A screenshot of the 'Add Device' form in FMC. The form contains the following fields and options:

- Host:** A text input field with a cursor.
- Display Name:** A text input field.
- Registration Key:** A text input field with a red border, indicating it is required.
- Domain:** A dropdown menu with 'Select Domain' as the current selection.
- Group:** A dropdown menu with 'None' as the current selection.
- Access Control Policy:** A dropdown menu.
- Smart Licensing:** Three checkboxes: 'Malware', 'Threat', and 'URL Filtering', all of which are currently unchecked.
- Advanced:** A section containing:
 - Unique NAT ID:** A text input field.
 - Transfer Packets:** A checked checkbox.

At the bottom of the form, there is a note: '† Either host or NAT ID is required.' and two buttons: 'Cancel' and 'Register'.

- Nell'host specificare l'indirizzo IP FTD.
- Nella casella Nome visualizzato specificare il nome desiderato.
- La chiave di registrazione deve corrispondere a quella specificata nella CLI FTD.
- Se si utilizzano più domini, specificare il dominio in cui si desidera aggiungere l'FTD.

- In Gruppo, specificare il gruppo di dispositivi sotto il quale si desidera aggiungere l'FTD.
- In Criteri di controllo di accesso specificare il criterio di sicurezza che si desidera distribuire in FTD.
- Licenze Smart: Specificare le licenze necessarie per le funzionalità configurate.
- ID NAT: Necessario in scenari specifici descritti più avanti in questo documento.

Per ulteriori informazioni, consultare la guida alla configurazione di Firepower Management Center, [Add Devices to the Firepower Management Center](#)

Scenario 1. Indirizzo IP statico FMC e FTD



CLI FTD

>configurare manager add <IP statico FMC> <Chiave di registrazione>

Ad esempio:

```
> configure manager add 10.62.148.75 Cisco-123
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

Informazioni sullo sfondo

Non appena si immette il comando FTD, l'FTD tenta di connettersi al CCP ogni 20 secondi, ma poiché il CCP non è ancora configurato risponde con TCP RST:

```
> capture-traffic
```

```
Please choose domain to capture traffic from:
 0 - eth0
 1 - Global
```

```
Selection? 0
```

```
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
```

Options: **-n host 10.62.148.75**

HS_PACKET_BUFFER_SIZE is set to 4.

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes

18:53:33.365513 IP 10.62.148.42.46946 > 10.62.148.75.8305: Flags **[S]**, seq 2274592861, win 29200, options [mss 1460,sackOK,TS val 55808298 ecr 0,nop,wscale 7], length 0

18:53:33.365698 IP 10.62.148.75.8305 > 10.62.148.42.46946: Flags **[R.]**, seq 0, ack 2274592862, win 0, length 0

18:53:53.365973 IP 10.62.148.42.57607 > 10.62.148.75.8305: Flags **[S]**, seq 1267517632, win 29200, options [mss 1460,sackOK,TS val 55810298 ecr 0,nop,wscale 7], length 0

18:53:53.366193 IP 10.62.148.75.8305 > 10.62.148.42.57607: Flags **[R.]**, seq 0, ack 1267517633, win 0, length 0

18:54:13.366383 IP 10.62.148.42.55484 > 10.62.148.75.8305: Flags **[S]**, seq 4285875151, win 29200, options [mss 1460,sackOK,TS val 55812298 ecr 0,nop,wscale 7], length 0

18:54:13.368805 IP 10.62.148.75.8305 > 10.62.148.42.55484: Flags **[R.]**, seq 0, ack 4285875152, win 0, length 0

Lo stato di registrazione del dispositivo:

> **show managers**

```
Host                : 10.62.148.75
Registration Key    : ****
Registration        : pending
RPC Status         :
Type               : Manager
Host               : 10.62.148.75
Registration        : Pending
```

L'FTD resta in ascolto sulla porta TCP 8305:

admin@vFTD66:~\$ **netstat -na | grep 8305**

```
tcp        0      0 10.62.148.42:8305  0.0.0.0:*          LISTEN
```

UI FMC

In questo caso, specificare:

- Host (indirizzo IP dell'FTD)
- Nome visualizzato
- Chiave di registrazione (deve corrispondere a quella configurata su FTD)
- Policy di controllo dell'accesso
- Dominio
- Informazioni su Smart Licensing

Add Device

Host:

Display Name:

Registration Key:

Domain:

Group:

Access Control Policy:

Smart Licensing

- Malware
- Threat
- URL Filtering

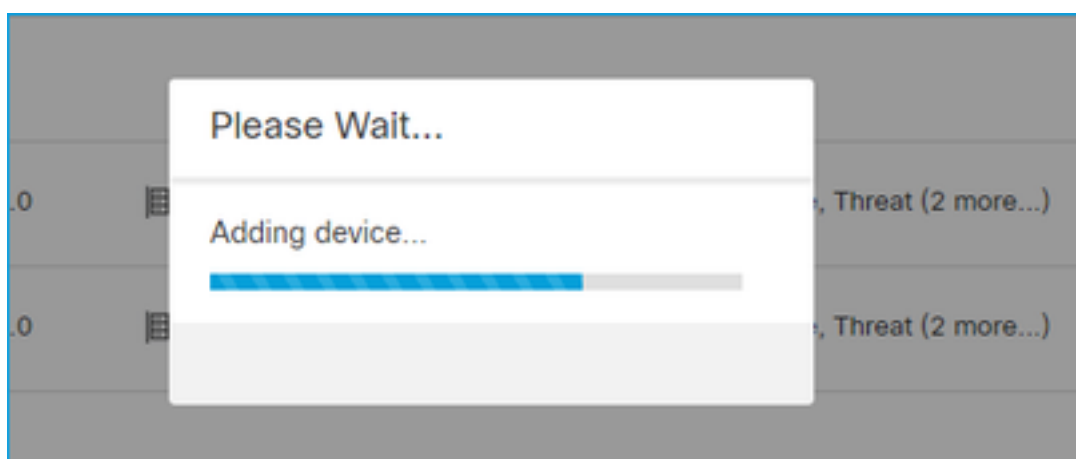
Advanced

Unique NAT ID:

- Transfer Packets

Seleziona **registro**

Il processo di registrazione ha inizio:



Il FMC inizia l'ascolto sulla porta TCP 8305:

```
admin@FMC2000-2:~$ netstat -na | grep 8305
tcp        0      0 10.62.148.75:8305    0.0.0.0:*          LISTEN
```

In background, il CCP avvia una connessione TCP:

```
20:15:55.437434 IP 10.62.148.42.49396 > 10.62.148.75.8305: Flags [S], seq 655146775, win 29200,
options [mss 1460,sackOK,TS val 56302505 ecr 0,nop,wscale 7], length 0
20:15:55.437685 IP 10.62.148.75.8305 > 10.62.148.42.49396: Flags [R.], seq 0, ack 655146776, win
0, length 0
20:16:00.463637 ARP, Request who-has 10.62.148.42 tell 10.62.148.75, length 46
20:16:00.463655 ARP, Reply 10.62.148.42 is-at 00:50:56:85:7b:1f, length 28
20:16:08.342057 IP 10.62.148.75.50693 > 10.62.148.42.8305: Flags [S], seq 2704366385, win 29200,
options [mss 1460,sackOK,TS val 1181294721 ecr 0,nop,wscale 7], length 0
20:16:08.342144 IP 10.62.148.42.8305 > 10.62.148.75.50693: Flags [S.], seq 1829769842, ack
2704366386, win 28960, options [mss 1460,sackOK,TS val 56303795 ecr 1181294721,nop,wscale 7],
length 0
20:16:08.342322 IP 10.62.148.75.50693 > 10.62.148.42.8305: Flags [.), ack 1, win 229, options
[nop,nop,TS val 1181294722 ecr 56303795], length 0
20:16:08.342919 IP 10.62.148.75.50693 > 10.62.148.42.8305: Flags [P.], seq 1:164, ack 1, win
229, options [nop,nop,TS val 1181294722 ecr 56303795], length 163
20:16:08.342953 IP 10.62.148.42.8305 > 10.62.148.75.50693: Flags [.), ack 164, win 235, options
[nop,nop,TS val 56303795 ecr 1181294722], length 0
```

Viene stabilito il canale di controllo sftunnel:

```
admin@FMC2000-2:~$ netstat -na | grep 8305
tcp        0      0 10.62.148.75:8305    0.0.0.0:*          LISTEN
tcp        0      0 10.62.148.75:50693   10.62.148.42:8305  ESTABLISHED
```

```
> sftunnel-status
```

```
SFTUNNEL Start Time: Sat Apr 18 20:14:20 2020
```

```
Both IPv4 and IPv6 connectivity is supported
Broadcast count = 4
Reserved SSL connections: 0
Management Interfaces: 1
eth0 (control events) 10.62.148.42,
```

```
*****
```

```
**RUN STATUS**ksec-fs2k-2-mgmt.cisco.com*****
Cipher used = AES256-GCM-SHA384 (strength:256 bits)
ChannelA Connected: Yes, Interface eth0
ChannelB Connected: No
Registration: Completed.
IPv4 Connection to peer '10.62.148.75' Start Time: Sat Apr 18 20:16:08 2020
```

```
PEER INFO:
```

```
sw_version 6.6.0
sw_build 90
Management Interfaces: 1
eth0 (control events) 10.62.148.75,
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to
```

```
'10.62.148.75' via '10.62.148.42'  
Peer channel Channel-B is not valid
```

Dopo alcuni minuti viene stabilito il canale Evento. L'iniziatore del canale Evento può essere **entrambi i lati**. Nell'esempio riportato di seguito è stato utilizzato il CCP:

```
20:21:15.347587 IP 10.62.148.75.43957 > 10.62.148.42.8305: Flags [S], seq 3414498581, win 29200,  
options [mss 1460,sackOK,TS val 1181601702 ecr 0,nop,wscale 7], length 0  
20:21:15.347660 IP 10.62.148.42.8305 > 10.62.148.75.43957: Flags [S.], seq 2735864611, ack  
3414498582, win 28960, options [mss 1460,sackOK,TS val 56334496 ecr 1181601702,nop,wscale 7],  
length 0  
20:21:15.347825 IP 10.62.148.75.43957 > 10.62.148.42.8305: Flags [.), ack 1, win 229, options  
[nop,nop,TS val 1181601703 ecr 56334496], length 0  
20:21:15.348415 IP 10.62.148.75.43957 > 10.62.148.42.8305: Flags [P.], seq 1:164, ack 1, win  
229, options [nop,nop,TS val 1181601703 ecr 56334496], length 163
```

La porta di origine casuale indica l'iniziatore della connessione:

```
admin@FMC2000-2:~$ netstat -na | grep 10.62.148.42  
tcp        0      0 10.62.148.75:50693    10.62.148.42:8305    ESTABLISHED  
tcp        0      0 10.62.148.75:43957    10.62.148.42:8305    ESTABLISHED
```

Se il canale Event è stato avviato dall'FTD, l'output è:

```
admin@FMC2000-2:~$ netstat -na | grep 10.62.148.42  
tcp        0      0 10.62.148.75:58409    10.62.148.42:8305    ESTABLISHED  
tcp        0      0 10.62.148.75:8305     10.62.148.42:46167   ESTABLISHED
```

Dal lato FTD:

```
> sftunnel-status
```

```
SFTUNNEL Start Time: Sat Apr 18 20:14:20 2020
```

```
Both IPv4 and IPv6 connectivity is supported  
Broadcast count = 6  
Reserved SSL connections: 0  
Management Interfaces: 1  
eth0 (control events) 10.62.148.42,
```

```
*****
```

```
**RUN STATUS**ksec-fs2k-2-mgmt.cisco.com*****  
Cipher used = AES256-GCM-SHA384 (strength:256 bits)  
ChannelA Connected: Yes, Interface eth0  
Cipher used = AES256-GCM-SHA384 (strength:256 bits)  
ChannelB Connected: Yes, Interface eth0  
Registration: Completed.  
IPv4 Connection to peer '10.62.148.75' Start Time: Sat Apr 18 20:16:08 2020
```

```
PEER INFO:
```

```
sw_version 6.6.0  
sw_build 90  
Management Interfaces: 1
```

```
eth0 (control events) 10.62.148.75,  
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to  
'10.62.148.75' via '10.62.148.42'  
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.62.148.75'  
via '10.62.148.42'
```

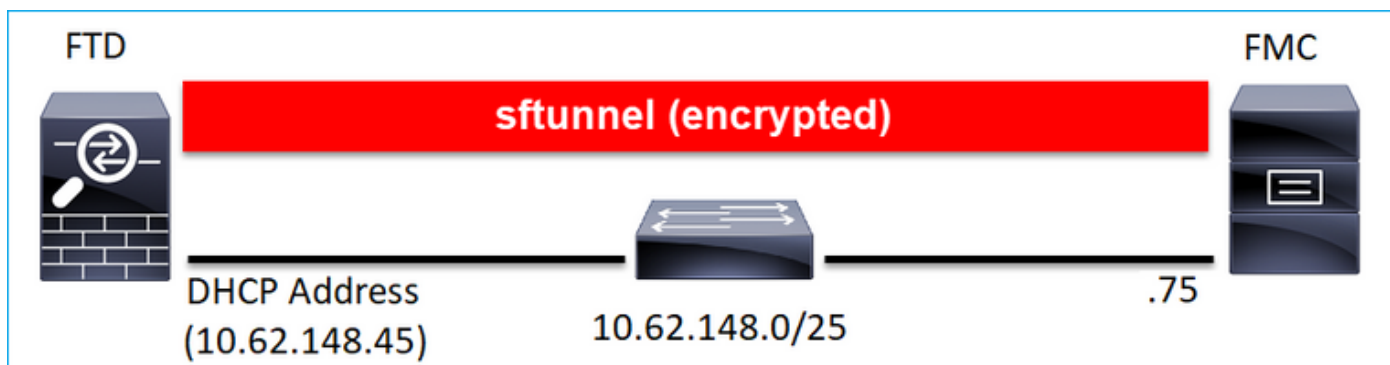
```
> show managers
```

```
Type : Manager  
Host : 10.62.148.75  
Registration : Completed
```

```
>
```

Scenario 2. Indirizzo IP DHCP FTD - Indirizzo IP statico FMC

In questo scenario, l'interfaccia di gestione FTD ha ottenuto il suo indirizzo IP da un server DHCP:



CLI FTD

Specificare l'ID NAT:

```
>configure manager add <IP statico FMC> <Chiave di registrazione> <ID NAT>
```

Ad esempio:

```
> configure manager add 10.62.148.75 Cisco-123 nat123  
Manager successfully configured.  
Please make note of reg_key as this will be required while adding Device in FMC.
```

```
>
```

Stato di registrazione FTD:

```
> show managers  
Host : 10.62.148.75  
Registration Key : ****  
Registration : pending  
RPC Status :
```

Type : Manager
Host : 10.62.148.75
Registration : Pending

UI FMC

In questo caso, specificare:

- Nome visualizzato
- Chiave di registrazione (deve corrispondere a quella configurata su FTD)
- Policy di controllo dell'accesso
- Dominio
- Informazioni su Smart Licensing
- ID NAT (**obbligatorio** quando **non si specifica l'host**. Deve corrispondere a quella configurata su FTD)

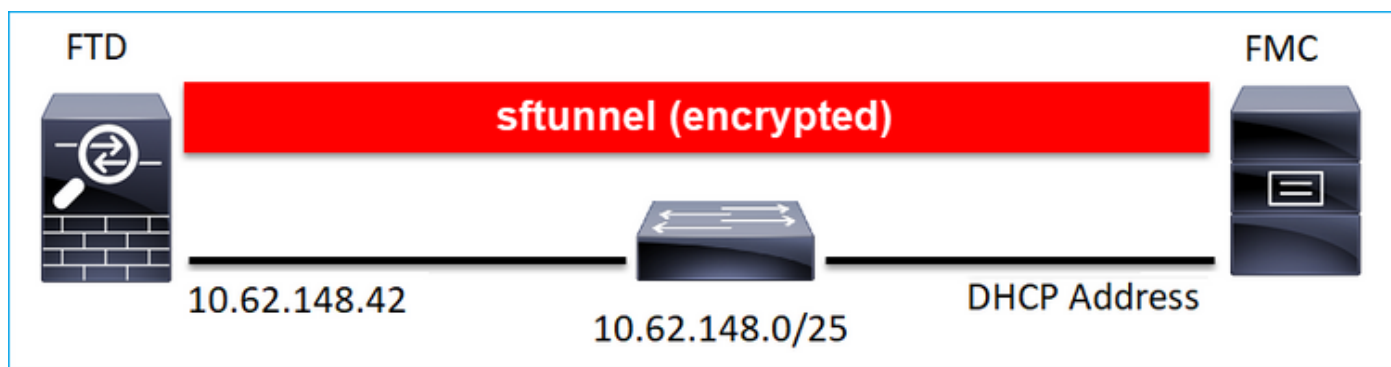
The screenshot shows the 'Add Device' configuration window. The 'Host' field is empty and highlighted with an orange box. The 'Unique NAT ID' field contains 'nat123' and is also highlighted with an orange box. Other fields include 'Display Name' (FTD1), 'Registration Key' (masked), 'Domain' (Global \ mzafeiro), 'Group' (None), and 'Access Control Policy' (FTD_ACP1). Smart Licensing options (Malware, Threat, URL Filtering) are checked. The 'Transfer Packets' checkbox is also checked. 'Cancel' and 'Register' buttons are at the bottom.

Chi avvia lo sftunnel in questo caso?

L'FTD avvia entrambe le connessioni di canale:

```
ftd1:/home/admin# netstat -an | grep 148.75
tcp        0      0 10.62.148.45:40273    10.62.148.75:8305    ESTABLISHED
tcp        0      0 10.62.148.45:39673    10.62.148.75:8305    ESTABLISHED
```

Scenario 3. Indirizzo IP statico FTD - Indirizzo IP DHCP FMC



```
> configure manager add DONTRESOLVE Cisco-123 nat123
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
>
```

Nota: Con DONTRESOLVE è necessario l'ID NAT.

UI FMC

In questo caso specificare:

- Indirizzo IP FTD
- Nome visualizzato
- Chiave di registrazione (deve corrispondere a quella configurata su FTD)
- Policy di controllo dell'accesso
- Dominio
- Informazioni su Smart Licensing

- ID NAT (deve corrispondere a quello configurato su FTD)

FTD dopo la registrazione:

> **show managers**

```
Type : Manager
Host : 5a8454ea-8273-11ea-a7d3-d07d71db8f19DONTRESOLVE
Registration : Completed
```

Chi avvia lo sftunnel in questo caso?

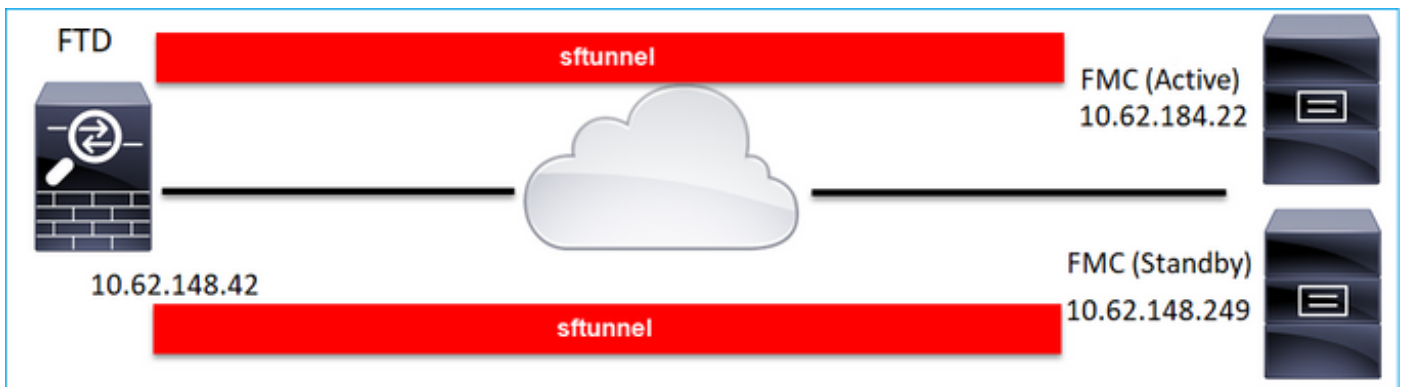
- Il CCP avvia il canale di controllo.
- Il canale Evento può essere avviato da entrambi i lati.

```
root@FMC2000-2: /Volume/home/admin# netstat -an | grep 148.42
tcp        0      0 10.62.148.75:50465  10.62.148.42:8305  ESTABLISHED
tcp        0      0 10.62.148.75:48445  10.62.148.42:8305  ESTABLISHED
```

Scenario 4. Registrazione FTD su HA FMC

In FTD configurare solo il CCP attivo:

```
> configure manager add 10.62.184.22 cisco123
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

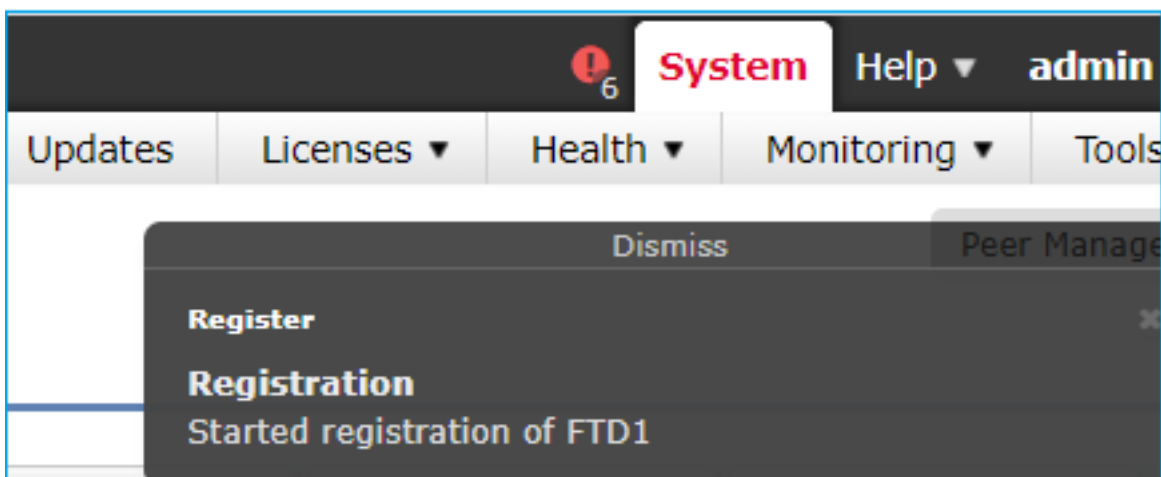


Nota: Verificare che il traffico della porta TCP 8305 sia consentito dal FTD a entrambi i CCP.

In primo luogo, viene stabilito il tunnel sftunnel verso il CCP attivo:

```
> show managers
Type           : Manager
Host           : 10.62.184.22
Registration   : Completed
```

Dopo alcuni minuti, l'FTD avvia la registrazione al CCP di standby:



> **show managers**

Type : Manager
Host : **10.62.184.22**
Registration : Completed

Type : Manager
Host : **10.62.148.249**
Registration : Completed

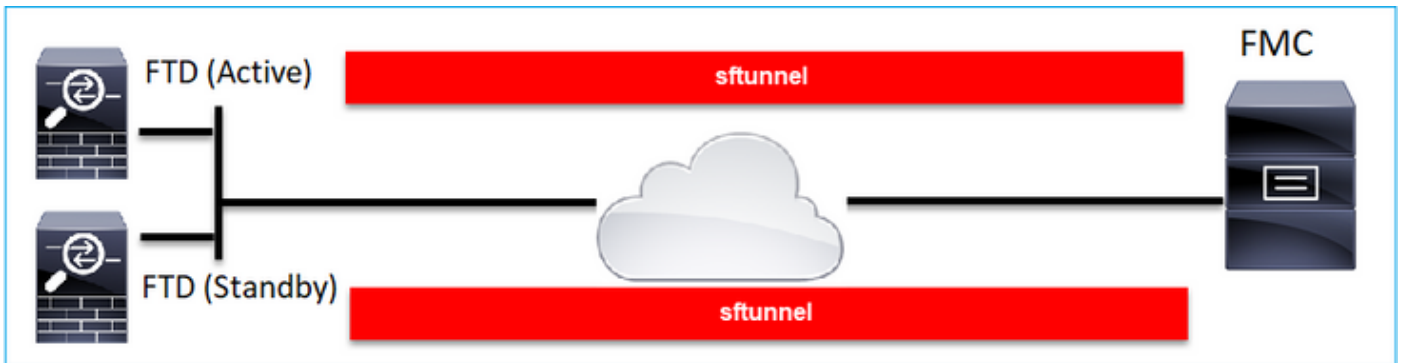
Nel back-end FTD sono stabiliti due canali di controllo (uno per ciascun CCP) e due canali eventi (uno per ciascun CCP):

```
ftd1:/home/admin# netstat -an | grep 8305
```

```
tcp      0      0 10.62.148.42:8305      10.62.184.22:36975     ESTABLISHED  
tcp      0      0 10.62.148.42:42197     10.62.184.22:8305     ESTABLISHED  
tcp      0      0 10.62.148.42:8305      10.62.148.249:45373   ESTABLISHED  
tcp      0      0 10.62.148.42:8305      10.62.148.249:51893   ESTABLISHED
```

Scenario 5. FTD HA

Nel caso di FTD HA, ciascuna unità dispone di una galleria separata per il CCP:

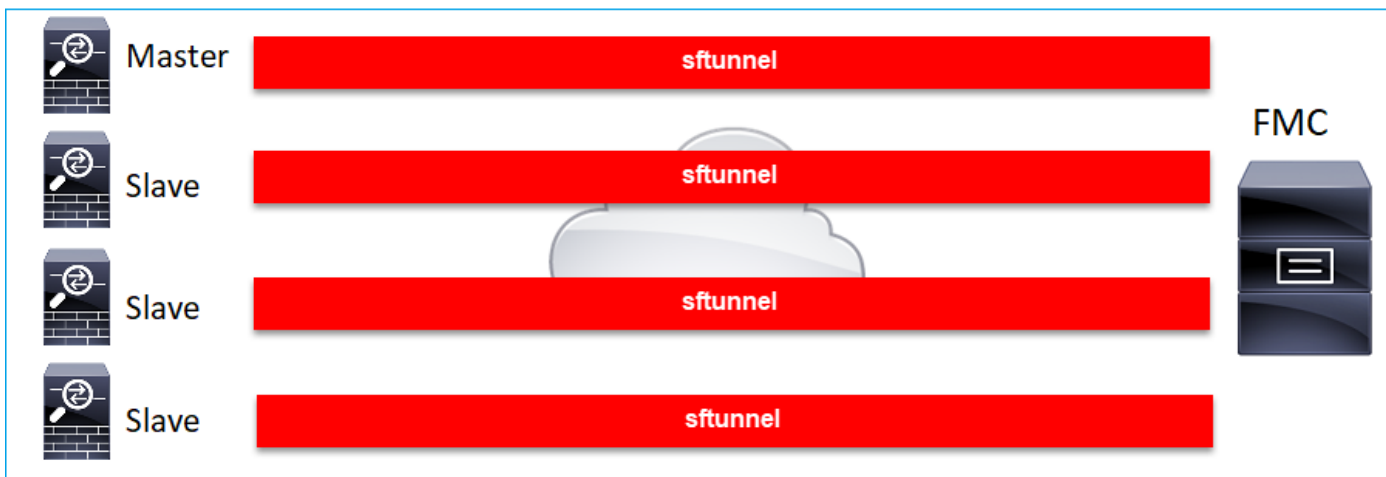


Entrambi i FTD vengono registrati in modo indipendente, quindi dal FMC viene creato l'FTD HA. Per maggiori dettagli, consultare:

- [Configurazione della funzionalità FTD High Availability nei dispositivi Firepower](#)
- [Alta disponibilità per Firepower Threat Defense](#)

Scenario 6. Cluster FTD

Nel caso del cluster FTD, ogni unità dispone di un tunnel separato al CCP. A partire dalla versione 6.3 del CCP, è necessario registrare solo il master FTD nel CCP. Quindi la FMC si occupa del resto delle unità e le rileva automaticamente e le registra.

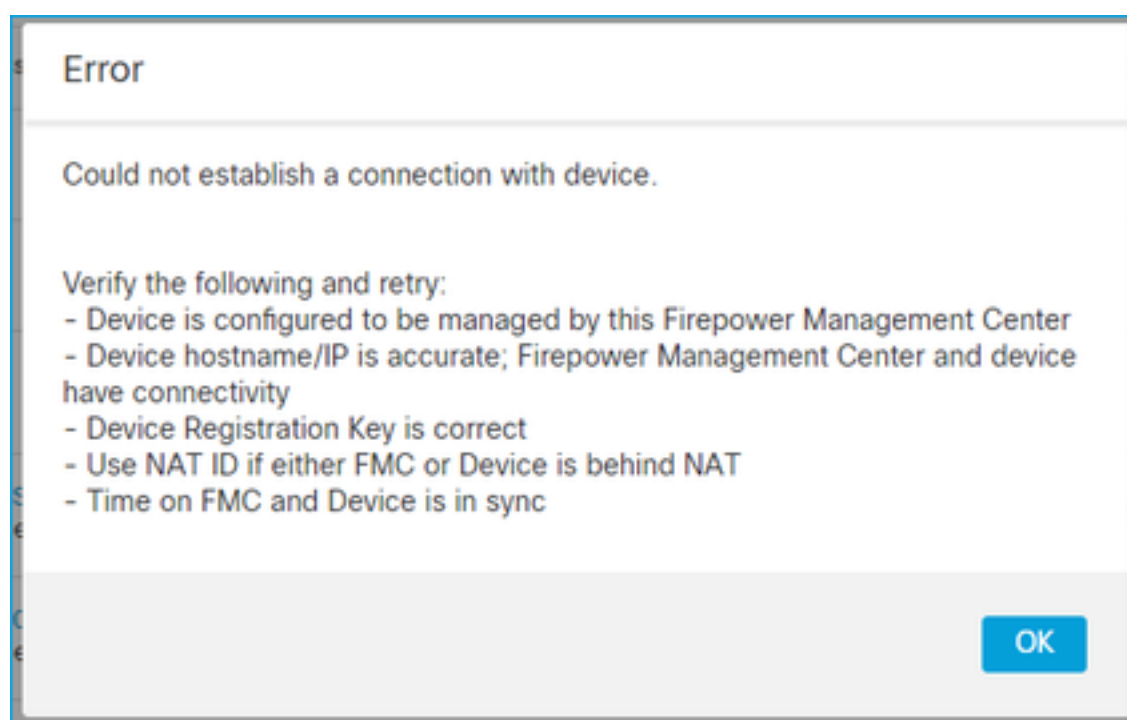


Nota: È consigliabile aggiungere l'unità Master per ottenere prestazioni ottimali, ma è possibile aggiungere qualsiasi unità del cluster. Per ulteriori informazioni, consultare: [Creare un cluster Firepower Threat Defense](#)

Risoluzione dei problemi comuni

1. Sintassi non valida nella CLI FTD

In caso di sintassi non valida su FTD e di tentativo di registrazione non riuscito, nell'interfaccia utente del CCP viene visualizzato un messaggio di errore piuttosto generico:



In questo comando la parola chiave **key** è la chiave di registrazione, mentre **cisco123** è l'ID NAT. È abbastanza comune aggiungere la parola chiave quando tecnicamente non c'è:

```
> configure manager add 10.62.148.75 key cisco123
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

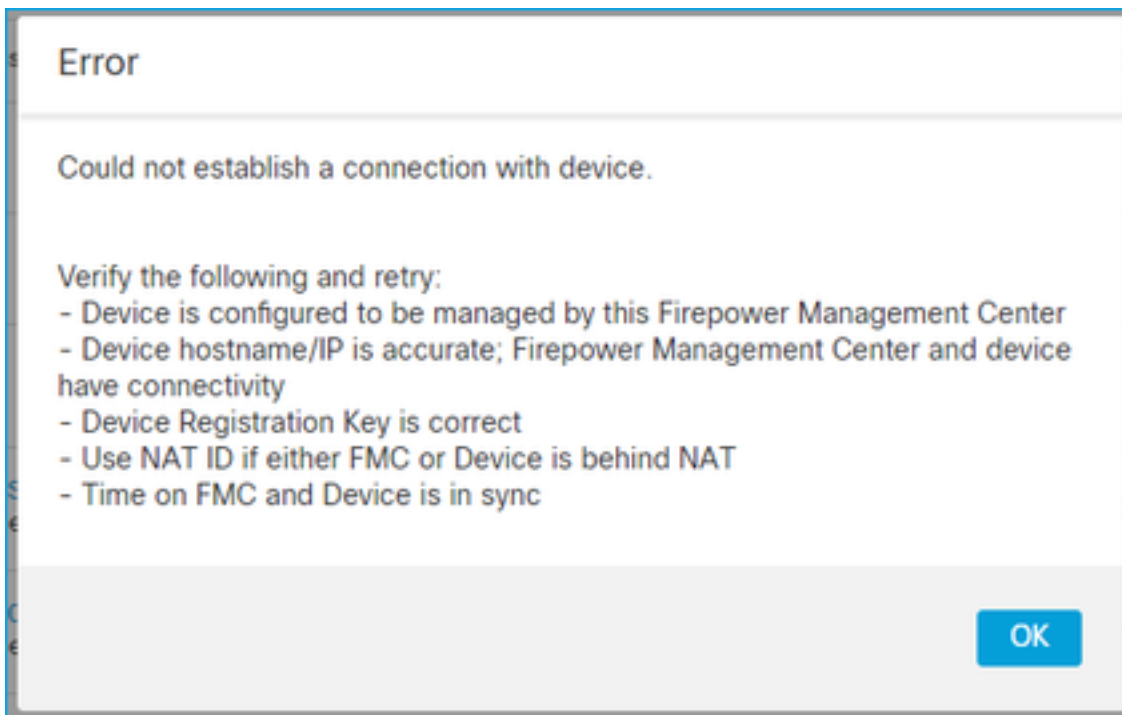
Azione consigliata

Utilizzare la sintassi corretta e non utilizzare parole chiave inesistenti.

```
> configure manager add 10.62.148.75 cisco123
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

2. Mancata corrispondenza della chiave di registrazione tra FTD e FMC

L'interfaccia utente del CCP mostra:



Azione consigliata

In FTD controllare il file `/ngfw/var/log/messages` per individuare eventuali problemi di autenticazione.

Modo 1 - Controllare i registri passati

```
> system support view-files
```

```
Type a sub-dir name to list its contents: s
```

```
Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
```

```
> messages
```

```
Apr 19 04:02:05 vFTD66 syslog-ng[1440]: Configuration reload request received, reloading configuration;
```

```
Apr 19 04:02:07 vFTD66 SF-IMS[3116]: [3116] pm:control [INFO] ControlHandler auditing message->type 0x9017, from '', cmd '/ngf
```

```
w/usr/bin/perl /ngfw/usr/local/sf/bin/run_hm.pl --persistent', pid 19455 (uid 0, gid 0) /authenticate
```

```
Apr 19 20:17:14 vFTD66 SF-IMS[18974]: [19131] sftunneId:sf_ssl [WARN] Accept: Failed to authenticate peer '10.62.148.75' <- The problem
```

Modo 2 - Controllare i log attivi

```
> expert
```

```
ftd1:~$ sudo su
```

```
Password:
```

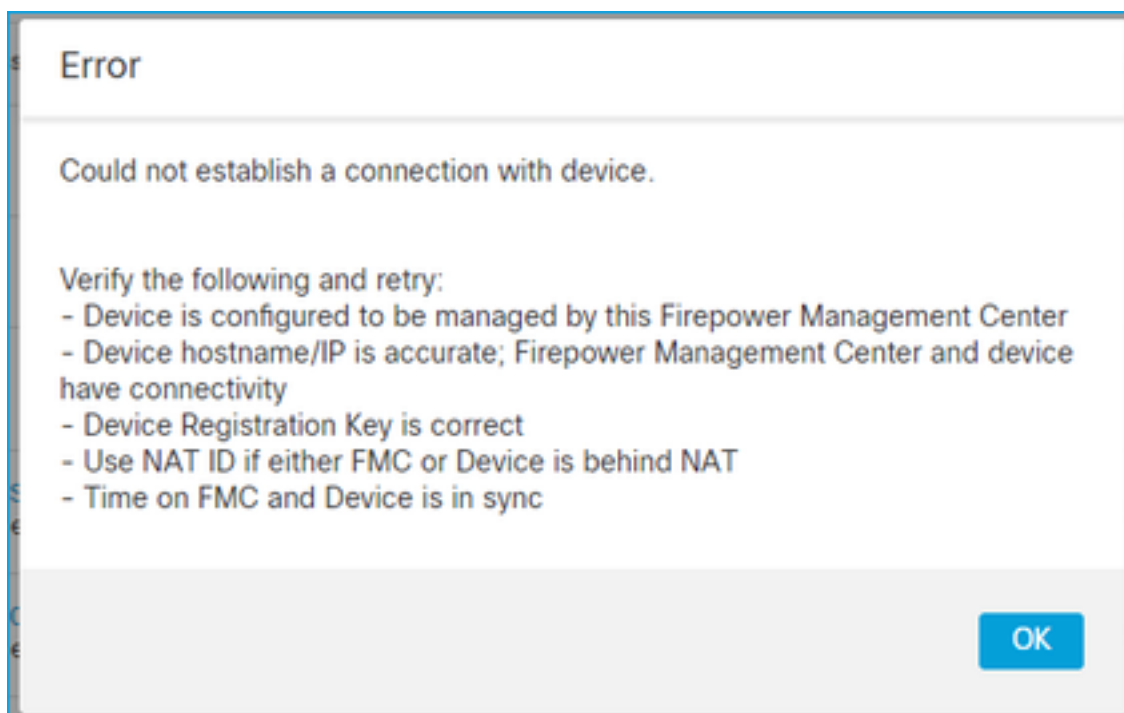
```
ftd1:~/home/admin# tail -f /ngfw/var/log/messages
```

In FTD controllare il contenuto del file `/etc/sf/sftunnel.conf` per verificare che la chiave di registrazione sia corretta:

```
ftd1:~$ cat /etc/sf/sftunnel.conf | grep reg_key  
reg_key cisco-123;
```

3. Problemi di connettività tra FTD e FMC

L'interfaccia utente del CCP mostra:



Azioni consigliate

- Accertarsi che il percorso non contenga alcun dispositivo (ad esempio, un firewall) che blocchi il traffico (TCP 8305). Nel caso di FMC HA, verificare che il traffico verso la porta TCP 8305 sia consentito verso entrambi i FMC.
- Acquisire immagini per verificare la comunicazione bidirezionale. Su FTD utilizzare il comando **capture-traffic**. Verificare che sia presente un handshake TCP a 3 vie e nessun pacchetto TCP FIN o RST.

```
> capture-traffic
```

```
Please choose domain to capture traffic from:
```

- 0 - eth0
- 1 - Global

```
Selection? 0
```

```
Please specify tcpdump options desired.
```

```
(or enter '?' for a list of supported options)
```

```
Options: -n host 10.62.148.75
```

```
HS_PACKET_BUFFER_SIZE is set to 4.
```

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
```

```
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
20:56:09.393655 IP 10.62.148.42.53198 > 10.62.148.75.8305: Flags [S], seq 3349394953, win 29200, options [mss 1460,sackOK,TS val 1033596 ecr 0,nop,wscale 7], length 0
```

```
20:56:09.393877 IP 10.62.148.75.8305 > 10.62.148.42.53198: Flags [R.], seq 0, ack 3349394954, win 0, length 0
```

```
20:56:14.397412 ARP, Request who-has 10.62.148.75 tell 10.62.148.42, length 28
```

```
20:56:14.397602 ARP, Reply 10.62.148.75 is-at a4:6c:2a:9e:ea:10, length 46
```

Allo stesso modo, prendi una cattura su FMC per garantire la comunicazione bidirezionale:

```
root@FMC2000-2: /var/common# tcpdump -i eth0 host 10.62.148.42 -n -w sftunnel.pcap
```

Si consiglia inoltre di esportare l'acquisizione in formato pcap e controllare il contenuto del pacchetto:

```
ftd1:/home/admin# tcpdump -i eth0 host 10.62.148.75 -n -w tunnel.pcap
```

```
HS_PACKET_BUFFER_SIZE is set to 4.
```

```
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Possibili cause:

- Il dispositivo FTD non è stato aggiunto al CCP.
- Un dispositivo nel percorso, ad esempio un firewall, blocca o modifica il traffico.
- I pacchetti non vengono indirizzati correttamente nel percorso.
- Il processo sftunnel su FTD o FMC è inattivo (controllare lo scenario 6)
- Nel percorso è presente un problema MTU (verificare lo scenario).

Per l'analisi di acquisizione, controllare questo documento:

[Analisi delle acquisizioni di Firepower Firewall per la risoluzione efficace dei problemi di rete](#)

5. Differenza temporale tra FTD e FMC

La comunicazione FTD-FMC è sensibile alle differenze temporali tra i due dispositivi. È necessario che FTD e FMC siano sincronizzati dallo stesso server NTP.

In particolare, quando il FTD è installato su una piattaforma come 41xx o 93xx, le sue impostazioni di tempo derivano dallo chassis principale (FXOS).

Azione consigliata

Verificare che il gestore dello chassis (FCM) e il FMC utilizzino la stessa fonte di ora (server NTP)

6. sftunnel Processo inattivo o disabilitato

Su FTD il processo di **sftunnel** gestisce il processo di registrazione. Questo è lo stato del processo prima della configurazione del manager:

```
> pmtool status
...
sftunnel (system) - Waiting
Command: /ngfw/usr/local/sf/bin/sftunnel -d -f /etc/sf/sftunnel.conf
PID File: /ngfw/var/sf/run/sftunnel.pid
Enable File: /ngfw/etc/sf/sftunnel.conf
CPU Affinity:
Priority: 0
Next start: Mon Apr 20 06:12:06 2020
Required by: sfmgr,sfmbservice,sfiproxy
CGroups: memory=System/ProcessHigh
```

Stato della registrazione:

```
> show managers
No managers configured.
```

Configurare il manager:

```
> configure manager add 10.62.148.75 cisco123
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

Ora il processo è attivo:

```
> pmtool status
...
sftunnel (system) - Running 24386
Command: /ngfw/usr/local/sf/bin/sftunnel -d -f /etc/sf/sftunnel.conf
PID File: /ngfw/var/sf/run/sftunnel.pid
Enable File: /ngfw/etc/sf/sftunnel.conf
CPU Affinity:
Priority: 0
Next start: Mon Apr 20 07:12:35 2020
Required by: sfmgr,sfmbbservice,sfiproxy
CGroups: memory=System/ProcessHigh(enrolled)
```

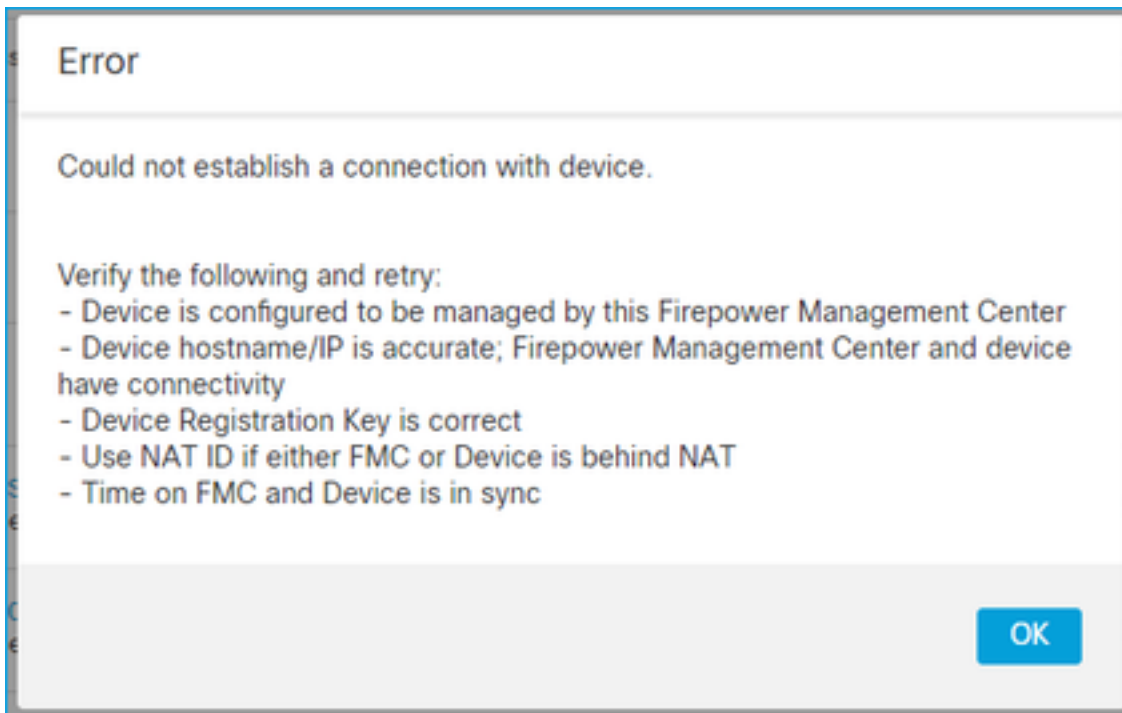
In alcuni rari casi il processo può essere inattivo o disattivato:

```
> pmtool status
...
sftunnel (system) - User Disabled
Command: /ngfw/usr/local/sf/bin/sftunnel -d -f /etc/sf/sftunnel.conf
PID File: /ngfw/var/sf/run/sftunnel.pid
Enable File: /ngfw/etc/sf/sftunnel.conf
CPU Affinity:
Priority: 0
Next start: Mon Apr 20 07:09:46 2020
Required by: sfmgr,sfmbbservice,sfiproxy
CGroups: memory=System/ProcessHigh
```

Lo stato del manager è normale:

```
> show managers
Host : 10.62.148.75
Registration Key : ****
Registration : pending
RPC Status :
```

D'altra parte, la registrazione del dispositivo non riesce:



In FTD non vengono visualizzati messaggi correlati in `/ngfw/var/log/messages`

Azione consigliata

Raccogliere il file FTD per la risoluzione dei problemi e contattare Cisco TAC

7. Registrazione FTD in attesa sul CCP secondario

In alcuni casi, dopo la registrazione iniziale di un FTD in un'installazione HA del FMC, il dispositivo FTD non viene aggiunto al FMC secondario.

Azione consigliata

Attenersi alla procedura descritta in questo documento:

[Utilizzare la CLI per risolvere il problema relativo alla registrazione dei dispositivi in Firepower Management Center High Availability](#)

Avviso: Questa procedura è intrusiva in quanto contiene l'annullamento della registrazione del dispositivo. Questo influisce sulla configurazione del dispositivo FTD (viene eliminato). Si consiglia di utilizzare questa procedura solo durante la registrazione e la configurazione iniziale di FTD. In diversi casi, raccogliere i file FTD e FMC per la risoluzione dei problemi e contattare Cisco TAC.

8. Registrazione non riuscita a causa dell'MTU del percorso

In Cisco TAC, esistono scenari in cui il traffico del tunnel deve attraversare un collegamento con

MTU ridotta. Il bit **Don't Fragment** (Non frammentare) è **impostato** sui pacchetti sftunnel, quindi la frammentazione non è consentita:

Source	Destination	Protocol	Length	TCP Segment	Don't fragment	Info
57 10.62.148.75	10.62.148.42	TCP	74	0	Set	47709 → 8305 [SYN] Seq=2860693630 Win=29200 Len=0 MS
58 10.62.148.42	10.62.148.75	TCP	74	0	Set	8305 → 47709 [SYN, ACK] Seq=279535377 Ack=2860693631
59 10.62.148.75	10.62.148.42	TCP	66	0	Set	47709 → 8305 [ACK] Seq=2860693631 Ack=279535378 Win=
60 10.62.148.75	10.62.148.42	TLSv1.2	229	163	Set	Client Hello
61 10.62.148.42	10.62.148.75	TCP	66	0	Set	8305 → 47709 [ACK] Seq=279535378 Ack=2860693794 Win=
62 10.62.148.42	10.62.148.75	TLSv1.2	1514	1448	Set	Server Hello
63 10.62.148.75	10.62.148.42	TCP	66	0	Set	47709 → 8305 [ACK] Seq=2860693794 Ack=279536826 Win=
64 10.62.148.42	10.62.148.75	TLSv1.2	803	737	Set	Certificate, Certificate Request, Server Hello Done
65 10.62.148.75	10.62.148.42	TCP	66	0	Set	47709 → 8305 [ACK] Seq=2860693794 Ack=279537563 Win=
66 10.62.148.75	10.62.148.42	TLSv1.2	2581	2515	Set	Certificate, Client Key Exchange, Certificate Verify
67 10.62.148.42	10.62.148.75	TCP	66	0	Set	8305 → 47709 [ACK] Seq=279537563 Ack=2860696309 Win=
68 10.62.148.42	10.62.148.75	TLSv1.2	1284	1218	Set	New Session Ticket, Change Cipher Spec, Encrypted Ha
69 10.62.148.75	10.62.148.42	TLSv1.2	364	298	Set	Application Data
70 10.62.148.42	10.62.148.75	TLSv1.2	364	298	Set	Application Data

Inoltre, nei file `/ngfw/var/log/messages` è possibile visualizzare un messaggio simile al seguente:

```
MESSAGGI: 10-09 14:41:11 ftd1 SF-IMS[7428]: [6612] sftunnel:sf_ssl [ERRORE] Handshake
Connect:SSL non riuscito
```

Azione consigliata

Per verificare se vi è una perdita di pacchetti dovuta alla frammentazione, acquisire le clip su FTD, FMC e, idealmente, sui dispositivi nel percorso. Verificare se vengono visualizzati pacchetti in arrivo su entrambe le estremità.

Su FTD abbassare l'MTU sull'interfaccia di gestione FTD. Il valore predefinito è 1500 byte. MAX è 1500 per l'interfaccia di gestione e 9000 per l'interfaccia di gestione degli eventi. Il comando è stato aggiunto nella release FTD 6.6.

[Guida di riferimento ai comandi di Cisco Firepower Threat Defense](#)

Esempio

```
> configure network mtu 1300
MTU set successfully to 1300 from 1500 for eth0
Refreshing Network Config...
Interface eth0 speed is set to '10000baseT/Full'
```

Verifica

```
> show network
===== [ System Information ] =====
Hostname                : ksec-sfvm-kali-3.cisco.com
DNS Servers             : 192.168.200.100
Management port        : 8305
IPv4 Default route
  Gateway                : 10.62.148.1
```

Netmask : 0.0.0.0

```
=====[ eth0 ]=====
State : Enabled
Link : Up
Channels : Management & Events
Mode : Non-Autonegotiation
MDI/MDIX : Auto/MDIX
MTU : 1300
MAC Address : 00:50:56:85:7B:1F
-----[ IPv4 ]-----
Configuration : Manual
Address : 10.62.148.42
Netmask : 255.255.255.128
Gateway : 10.62.148.1
-----[ IPv6 ]-----
```

Per verificare l'MTU del percorso dal file FTD, usare questo comando:

```
root@firepower:/home/admin# ping -M do -s 1500 10.62.148.75
```

L'opzione **do** imposta il bit **non frammentare** nei pacchetti ICMP

Su FMC abbassare il valore MTU sull'interfaccia di gestione FMC come descritto nel presente documento:

[Configurazione delle interfacce di gestione di Firepower Management Center](#)

9. L'FTD viene annullato dopo una modifica del bootstrap dall'interfaccia utente di Gestione chassis

Ciò è applicabile alle piattaforme FP41xx e FP93xx e documentato nell>ID bug Cisco [CSCvn45138](#)

In generale, non è necessario eseguire modifiche di bootstrap da Gestione chassis (FCM) a meno che non si esegua un ripristino di emergenza.

Azione consigliata

Nel caso in cui sia stata apportata una modifica al bootstrap e sia stata soddisfatta la condizione (la comunicazione FTD-FMC è interrotta mentre il FTD si accende dopo la modifica del bootstrap), è necessario eliminare e registrare nuovamente il FTD nel FMC.

10. FTD perde l'accesso al FMC a causa dei messaggi di reindirizzamento ICMP

Questo problema può influire sul processo di registrazione o interrompere la comunicazione FTD-FMC dopo la registrazione.

Il problema in questo caso è un dispositivo di rete che invia messaggi di **reindirizzamento ICMP** all'interfaccia di gestione FTD e alla comunicazione FTD-FMC con buchi neri.

Come identificare questo problema

In questo caso, 10.100.1.1 è l'indirizzo IP del CCP. Su FTD è presente un percorso memorizzato nella cache a causa del messaggio di reindirizzamento ICMP ricevuto dall'FTD sull'interfaccia di gestione:

```
ftd1:/ngfw/var/common# ip route get 10.100.1.1
10.100.1.1 via 10.10.1.1 dev br1 src 10.10.1.23
    cache
```

Azione consigliata

Passaggio 1

Disabilitare il reindirizzamento ICMP sul dispositivo che lo invia (ad esempio, switch L3 upstream, router e così via).

Passaggio 2

Cancellare la cache route FTD dalla CLI FTD:

```
ftd1:/ngfw/var/common# ip route flush 10.100.1.1
```

Quando non viene reindirizzato, ha il seguente aspetto:

```
ftd1:/ngfw/var/common# ip route get 10.100.1.1
10.100.1.1 via 10.62.148.1 dev eth0 src 10.10.1.23
    cache mtu 1500 advmss 1460 hoplimit 64
```

Riferimenti

- [Informazioni sui messaggi di reindirizzamento ICMP](#)
- [ID bug Cisco CSCvm53282 FTD: Le tabelle di routing aggiunte dai reindirizzamenti ICMP vengono bloccate nella cache della tabella di routing per sempre](#)

Informazioni correlate

- [Guide alla configurazione NGFW](#)

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).