Configurare E Verificare Syslog In Gestione Periferiche Firepower

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Configurazioni](#)
[Verifica](#)
[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare Syslog in Firepower Device Manager (FDM).

Prerequisiti

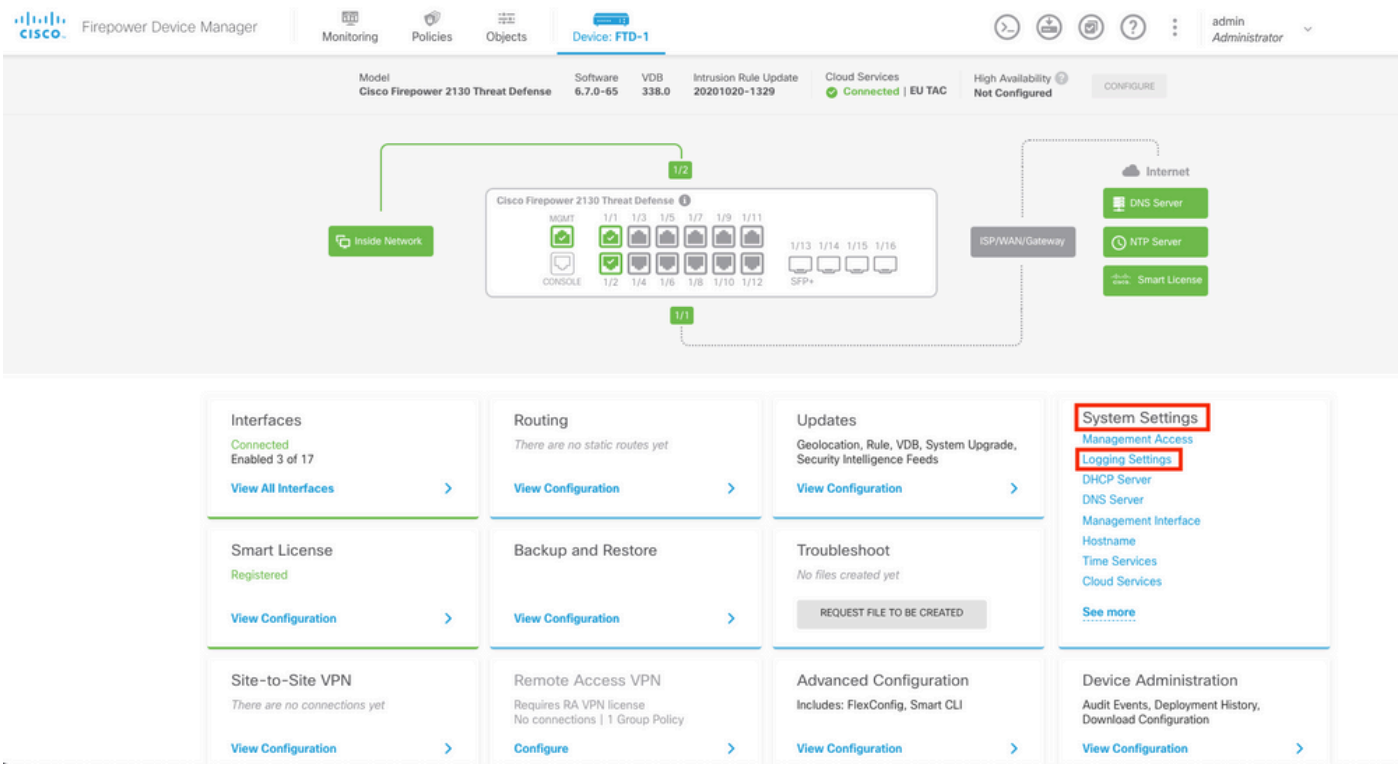
Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

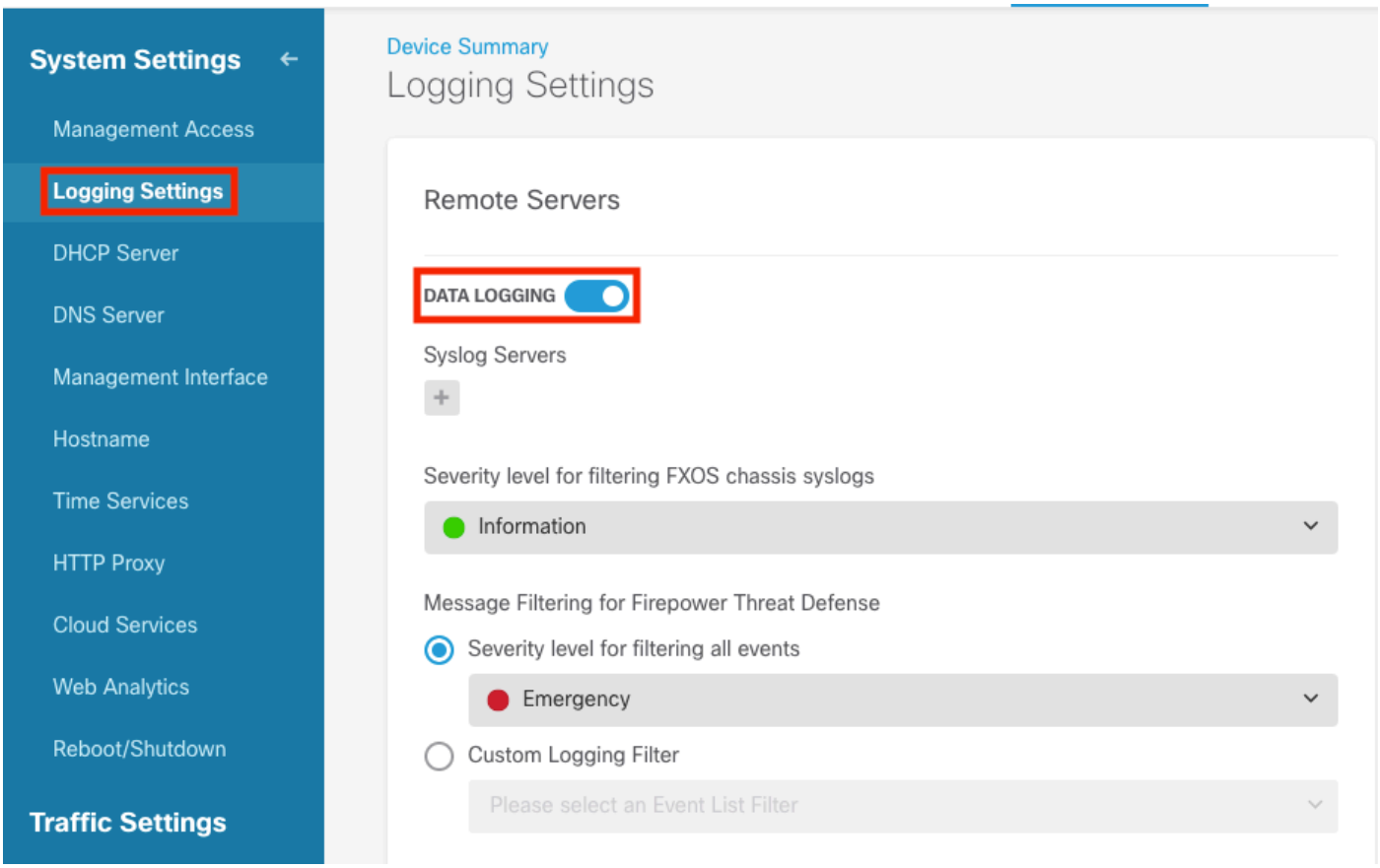
- Firepower Threat Defense
- Syslog Server che esegue il software Syslog per raccogliere dati

Configurazioni

Passaggio 1. Dalla schermata Main Firepower Device Manager (Gestione periferiche Firepower), selezionare Logging Settings (Impostazioni di registrazione) in System Settings (Impostazioni di sistema) nell'angolo inferiore destro della schermata.



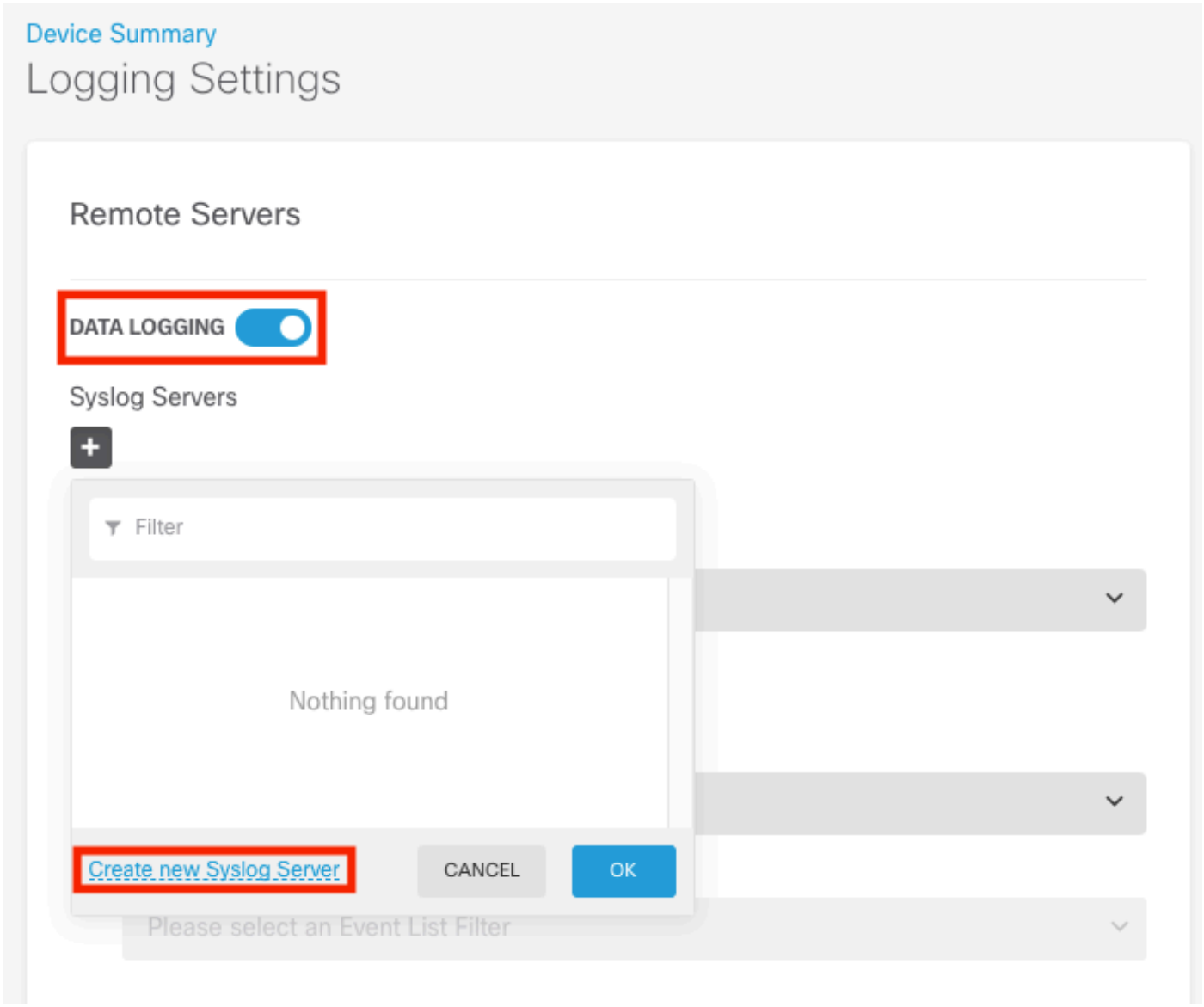
Passaggio 2. Nella schermata System Settings (Impostazioni di sistema), selezionare Logging Settings (Impostazioni di registrazione) nel menu a sinistra.



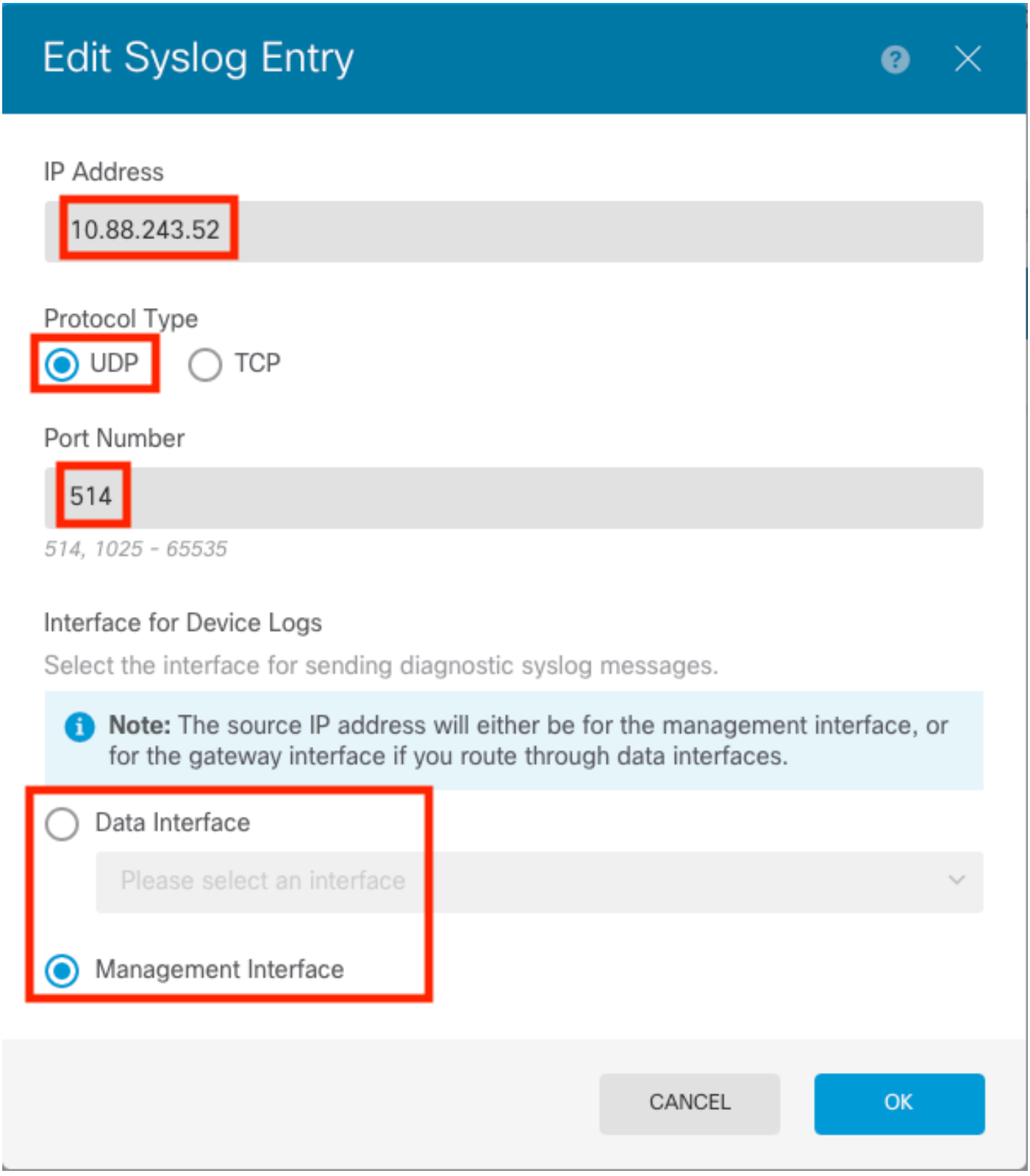
Passaggio 3. Impostare l'interruttore di attivazione/disattivazione della registrazione dei dati selezionando il segno + in Server Syslog.

Passaggio 4. Selezionare Add Syslog Server (Aggiungi server syslog). In alternativa, è possibile

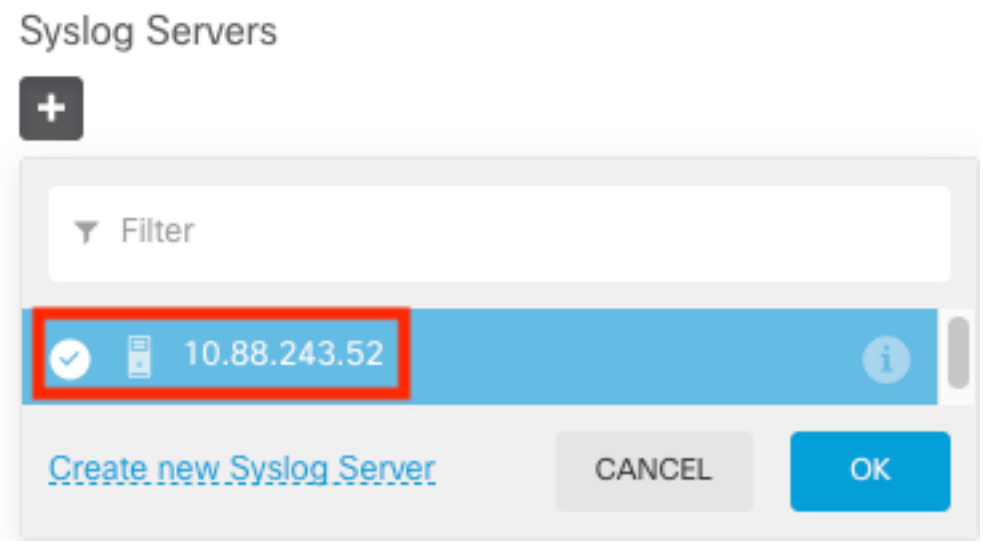
creare l'oggetto Syslog Server in Oggetti - Syslog Server.



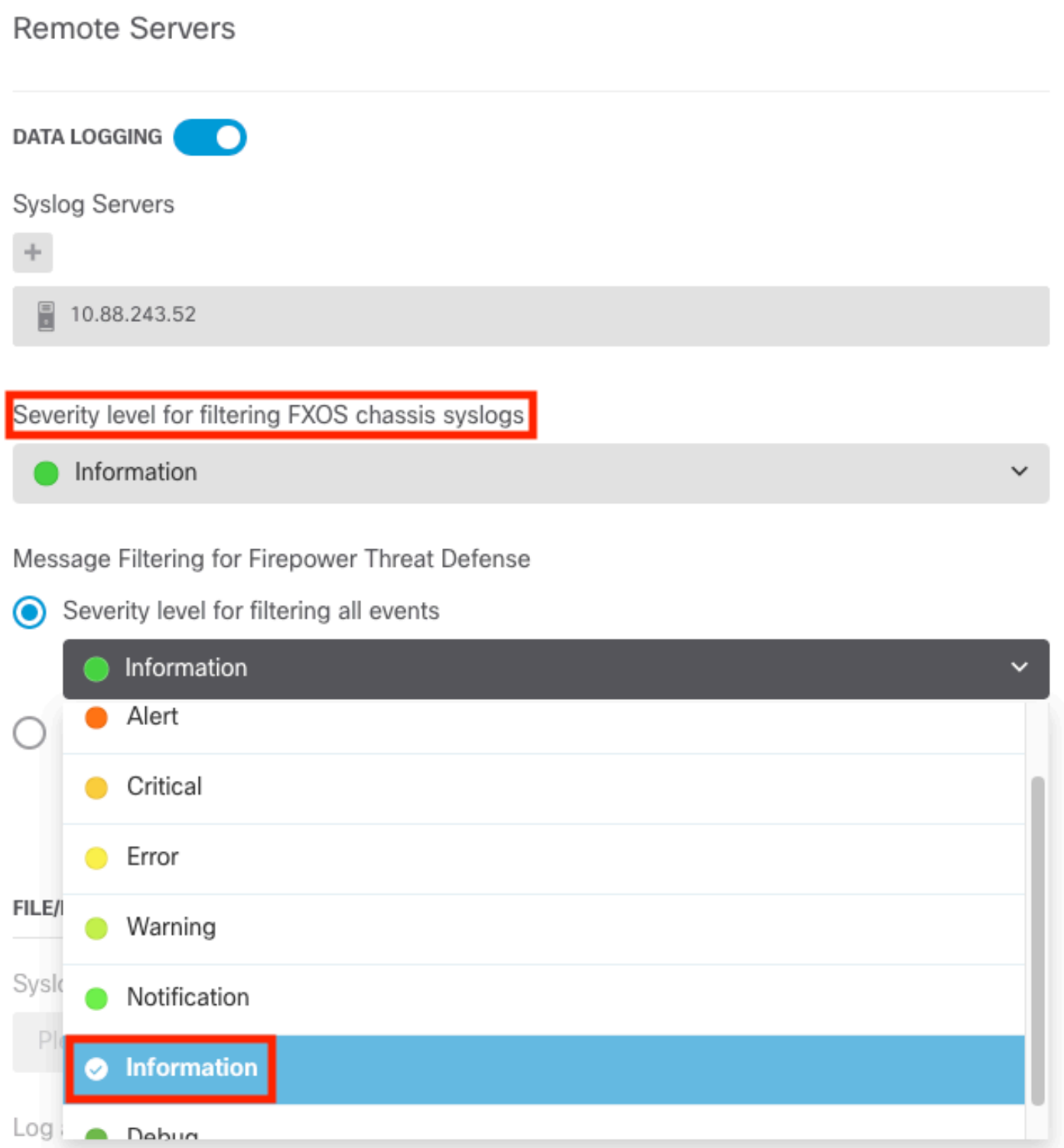
Passaggio 5. Immettere l'indirizzo IP del server Syslog e il numero di porta. Selezionare il pulsante di opzione per Interfaccia dati e scegliere OK.



Passaggio 6. Selezionare quindi il nuovo server Syslog e scegliere OK.

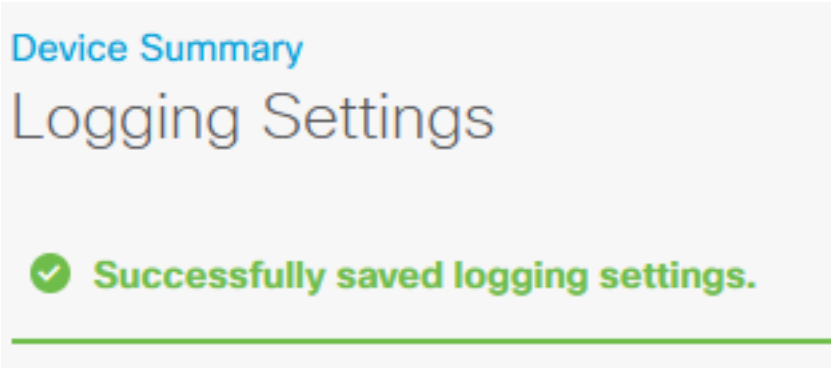


Passaggio 7. Selezionare il pulsante di opzione Livello di gravità per filtrare tutti gli eventi e selezionare il livello di registrazione desiderato.



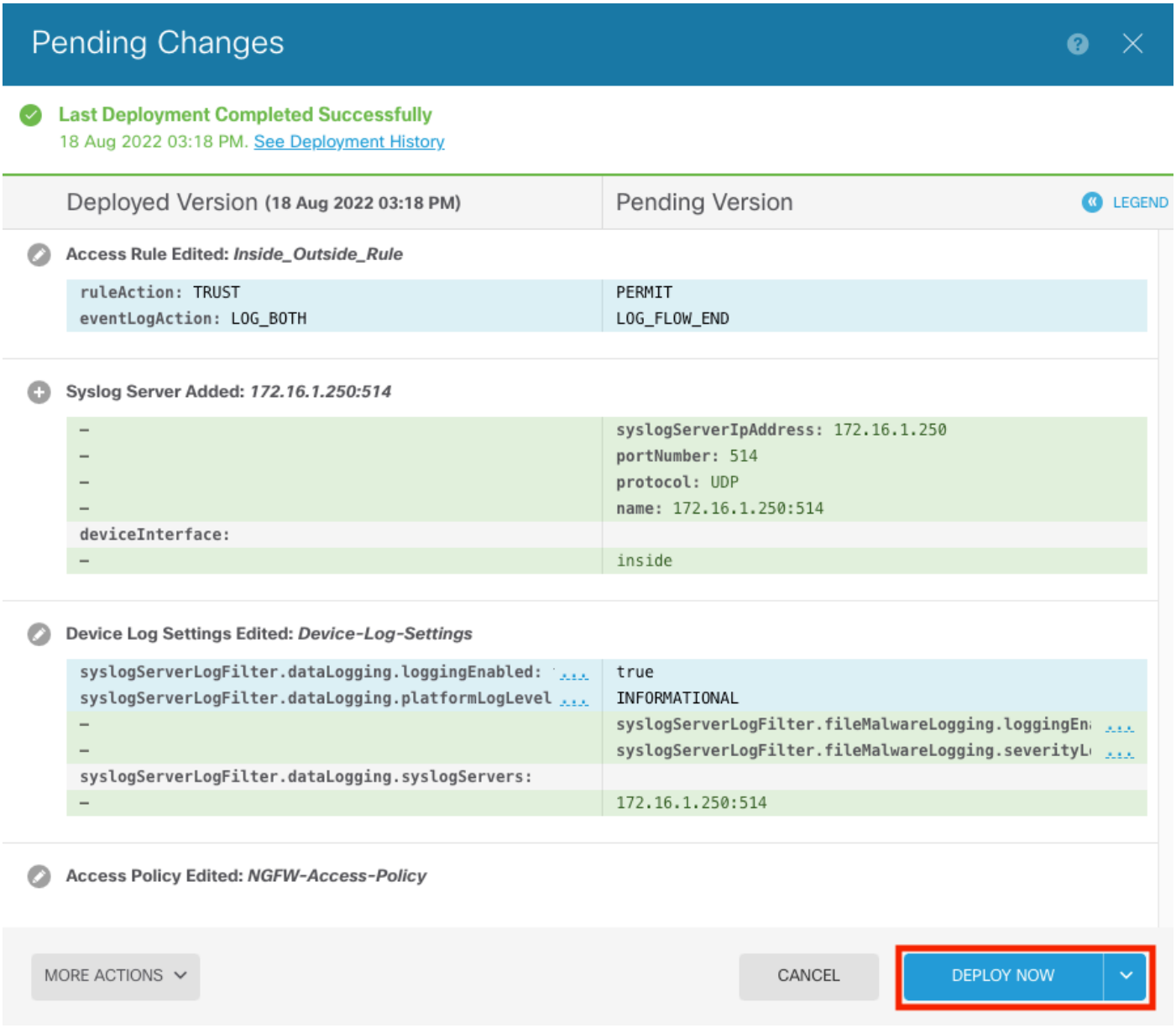
Passaggio 8. Selezionare Save (Salva) nella parte inferiore dello schermo.

Passaggio 9. Verificare che le impostazioni siano corrette.



Passaggio 10. Distribuire le nuove impostazioni.

E

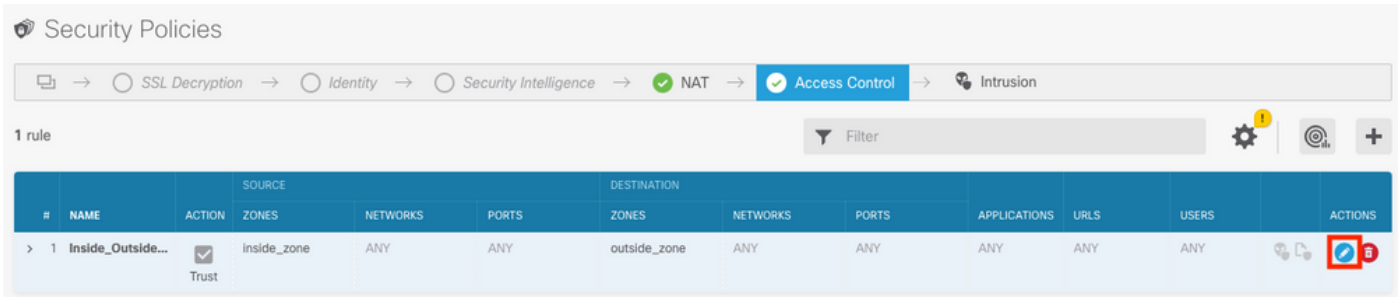


FACOLTATIVO.

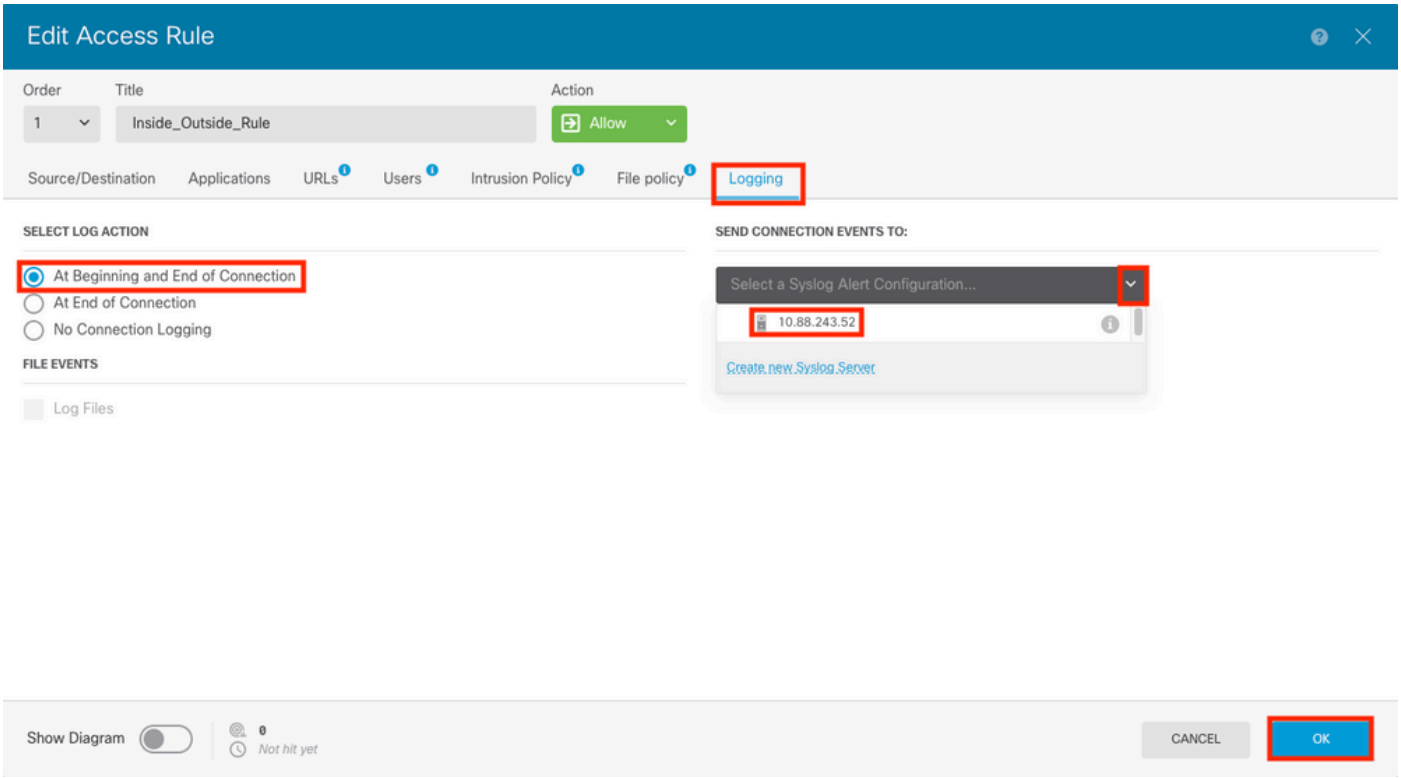
Èinoltre possibile impostare le regole di controllo d'accesso di Access Control Policy per accedere al server Syslog:

Passaggio 1. Fare clic sul pulsante Criteri nella parte superiore della schermata.

Passaggio 2. Posizionare il puntatore del mouse sul lato destro della regola ACP per aggiungere la registrazione e selezionare l'icona della matita.



Passaggio 3. Selezionare la scheda Logging, selezionare il pulsante di opzione per Al termine della connessione, selezionare la freccia in giù in Selezionare una configurazione di avviso syslog, selezionare sul server syslog e scegliere OK.



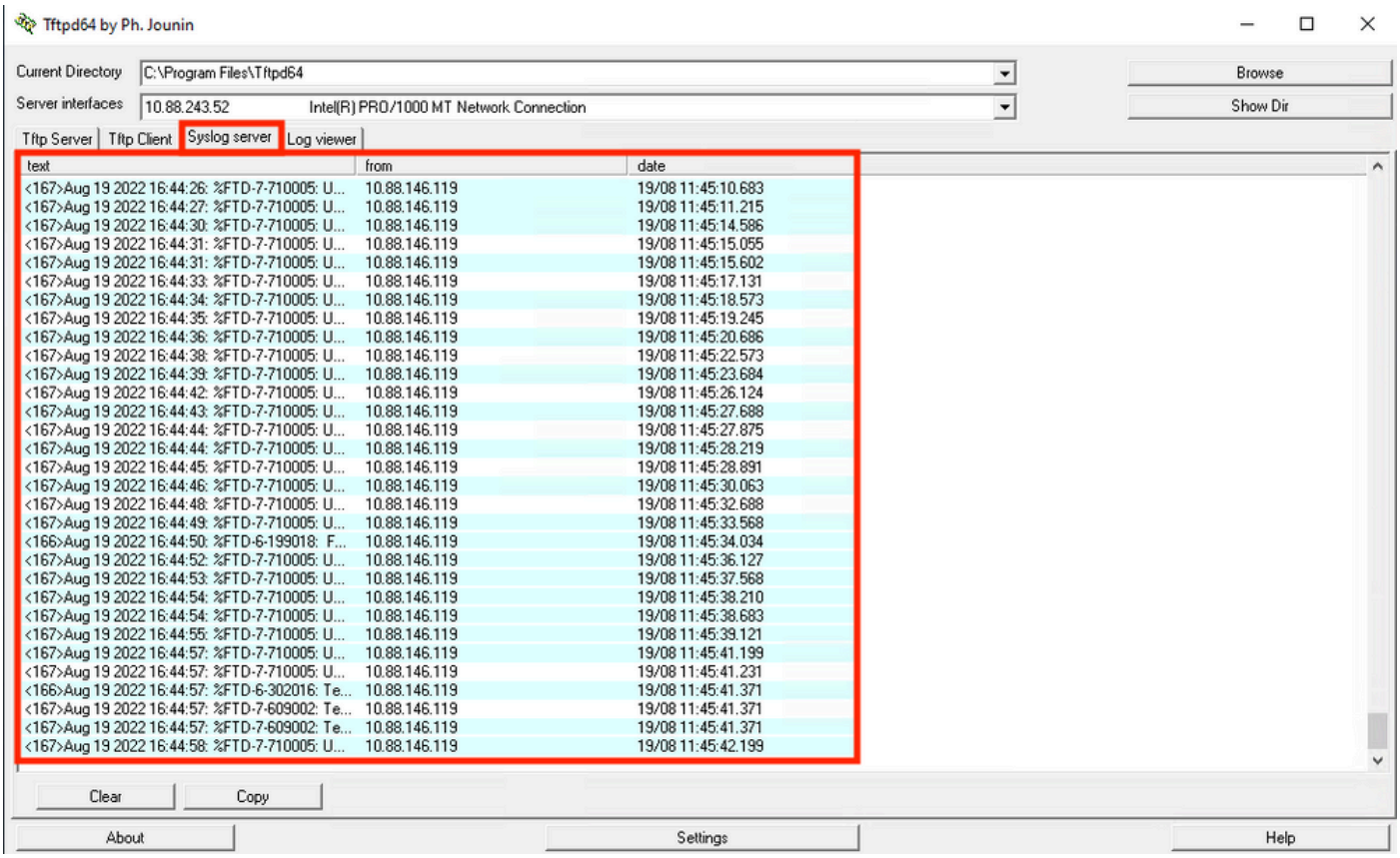
Passaggio 4. Distribuire le modifiche alla configurazione.

Verifica

Passaggio 1. Al termine dell'operazione, è possibile verificare le impostazioni nella modalità di compressione FTD CLI usando il comando **show running-config logging**.

```
Copyright 2004-2020, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.7.0 (build 62)
Cisco Firepower 2130 Threat Defense v6.7.0 (build 65)

> show running-config logging
logging enable
logging timestamp
logging buffer-size 5242880
logging buffered informational
logging trap debugging
logging host ngfw-management 10.88.243.52
logging permit-hostdown
>
```

Passaggio 2. Accedere al server Syslog e verificare che l'applicazione del server Syslog accetti i messaggi Syslog.



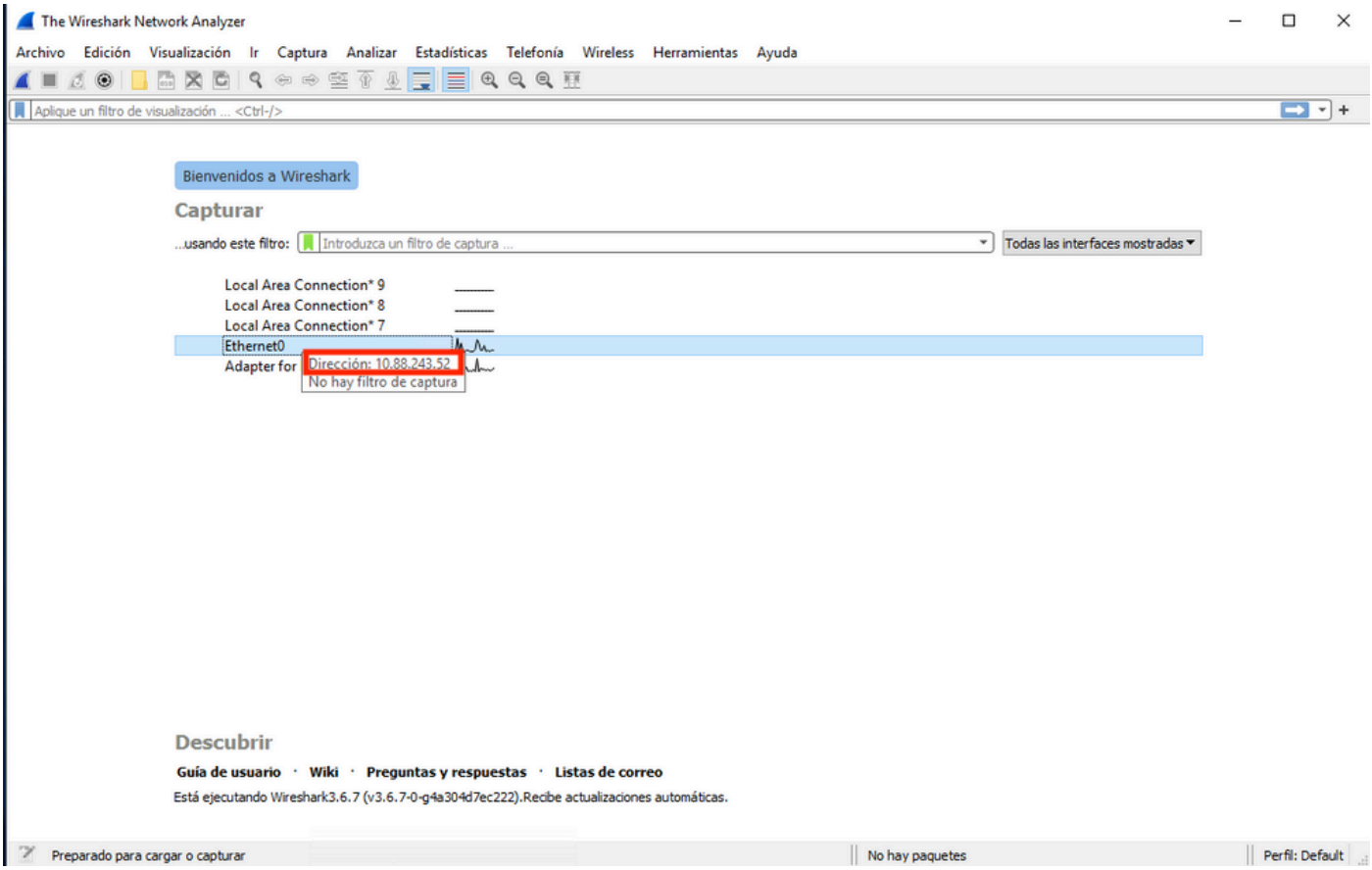
Risoluzione dei problemi

Passaggio 1. Se i messaggi Syslog sull'applicazione Syslog producono messaggi, eseguire un'acquisizione di pacchetto dalla CLI FTD per controllare la presenza di pacchetti. Passare dalla modalità Clish a LINA immettendo il comando **system support diagnostic-cli** al prompt dei comandi clish.

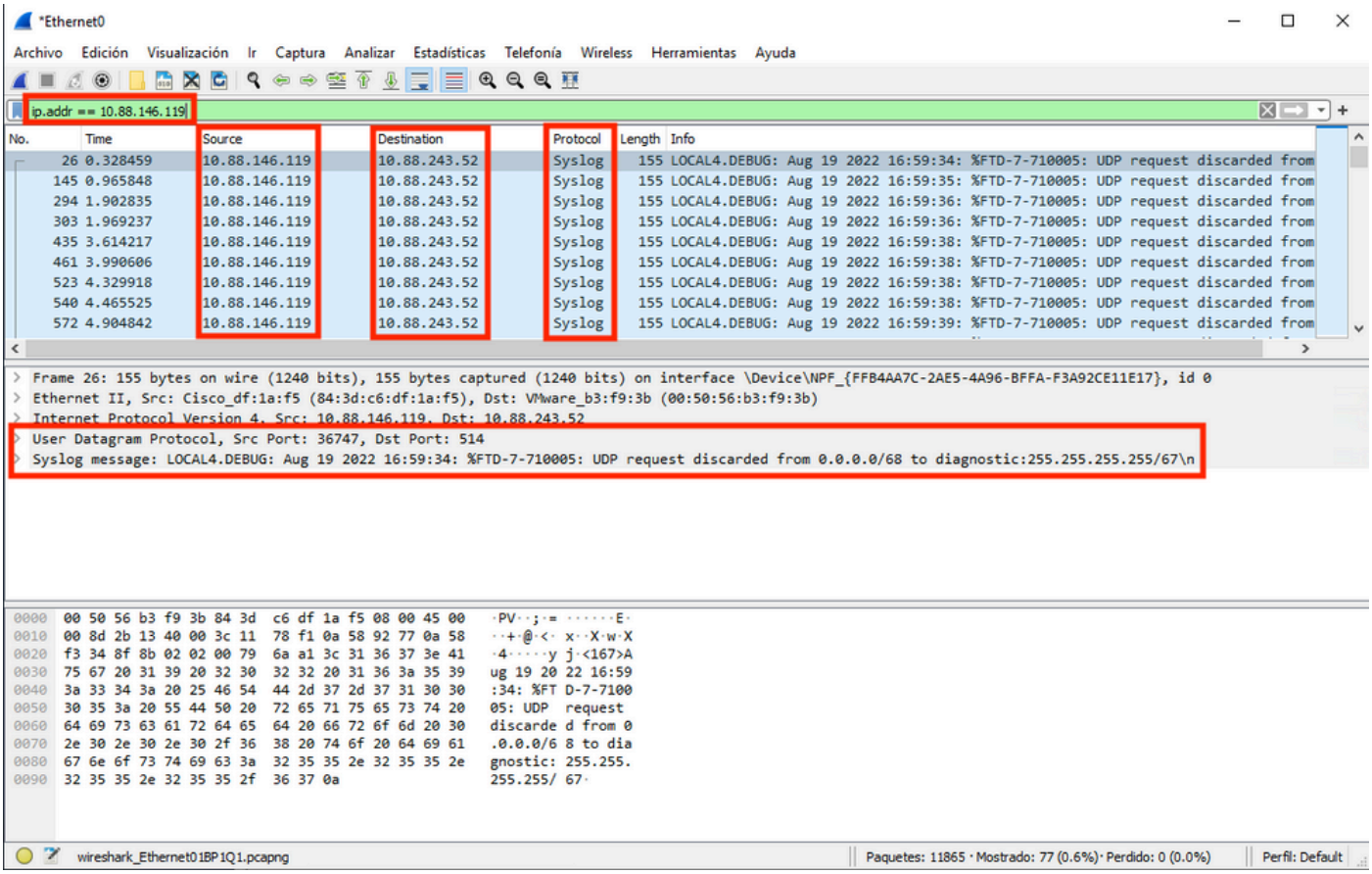
```
[> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

[FTD-1> en
[FTD-1> enable
[Password:
[FTD-1#
FTD-1#
```

Passaggio 2. Creare un'acquisizione pacchetto per l'udp 514 (o tcp 1468 se si utilizza tcp)

Passaggio 3. Verificare che la comunicazione sia diretta alla scheda di interfaccia di rete sul server Syslog. Usare Wireshark o un altro programma di acquisizione pacchetti caricato. Fare doppio clic sull'interfaccia in Wireshark per il server Syslog per avviare l'acquisizione dei pacchetti.



Passaggio 4. Impostare un filtro di visualizzazione nella barra superiore per udp 514 digitando udp.port==514 e selezionando la freccia a destra della barra. Dall'output, verificare se i pacchetti stanno raggiungendo il server Syslog.



Passaggio 5. Se i dati non vengono visualizzati nell'applicazione Syslog Server, risolvere il problema relativo all'impostazione nell'applicazione Syslog Server. Verificare che venga utilizzato il protocollo udp/tcp corretto e la porta 514/1468 corretta.

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).