

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

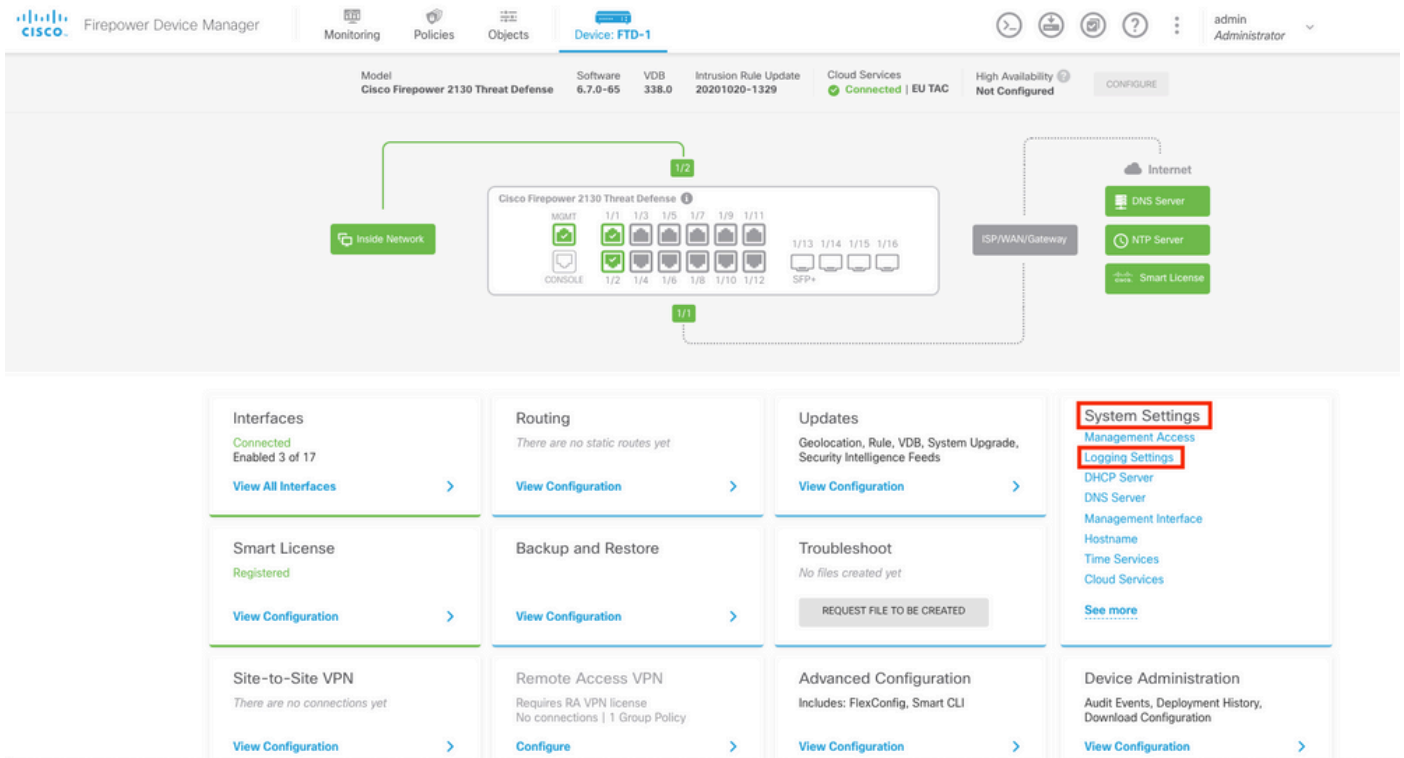
Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

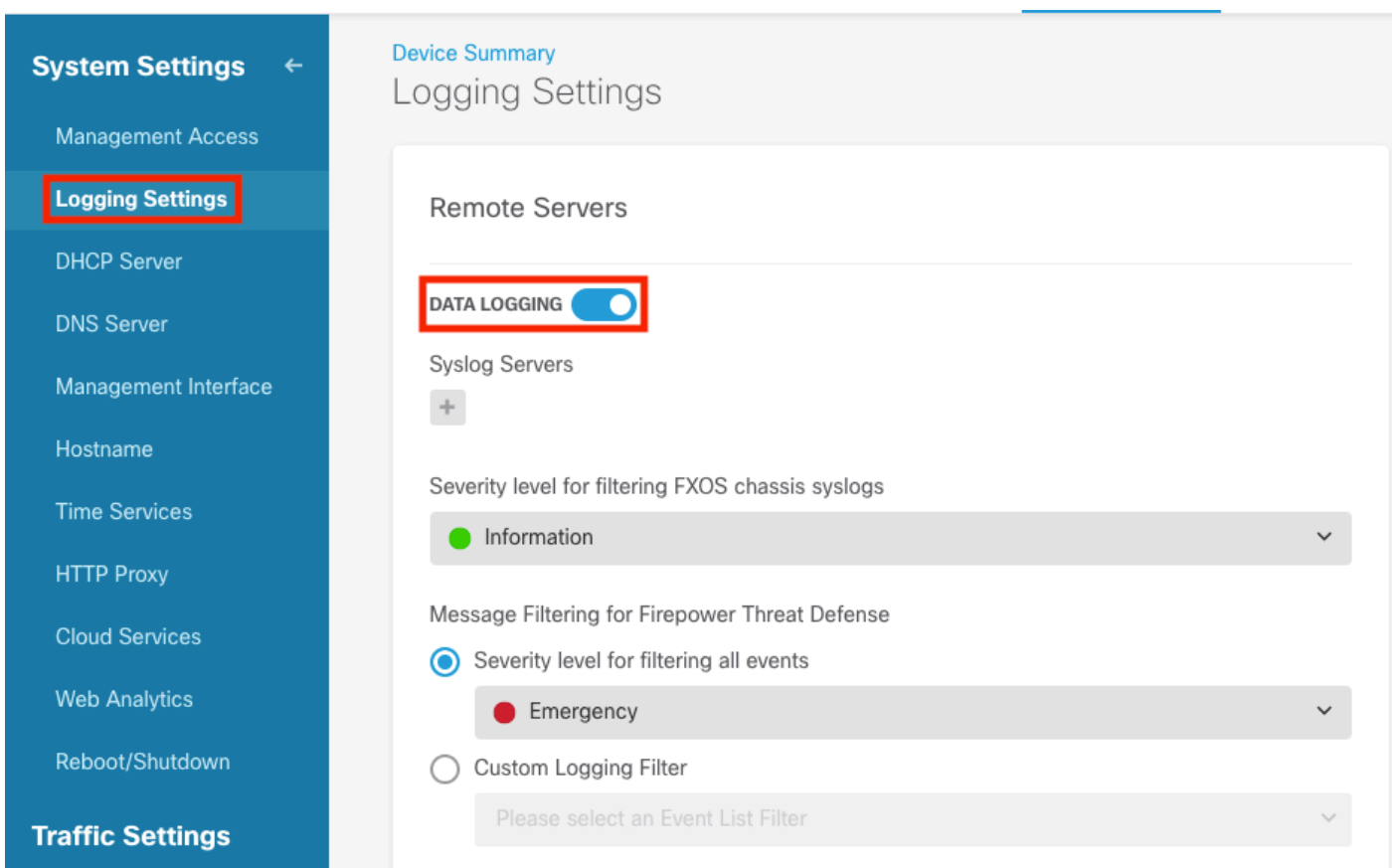
- Firepower Threat Defense
- Syslog Server che esegue il software Syslog per raccogliere dati

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.



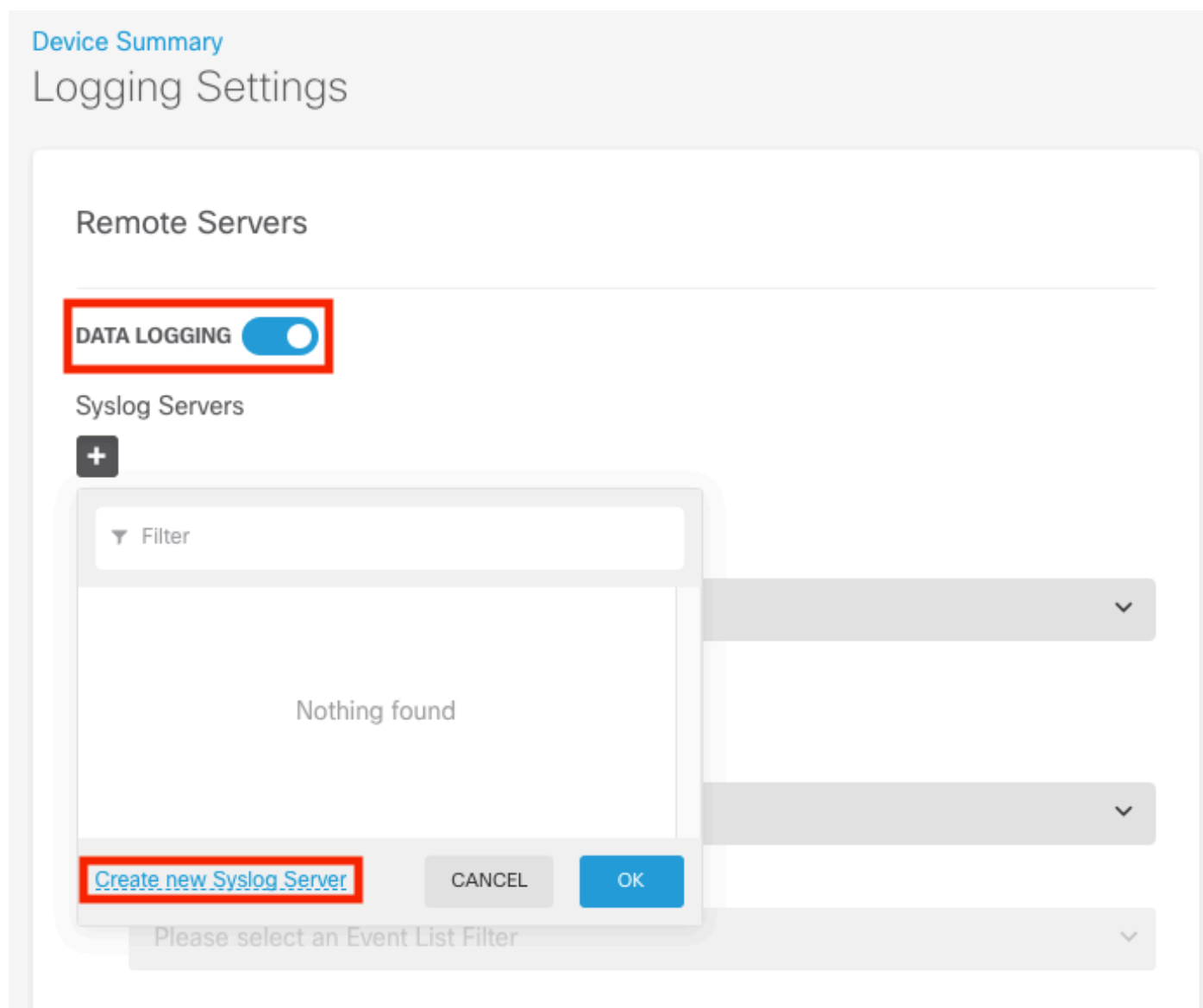
Passaggio 2. Nella schermata System Settings (Impostazioni di sistema), selezionare Logging Settings (Impostazioni di registrazione) nel menu a sinistra.



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.

Edit Syslog Entry



IP Address

10.88.243.52

Protocol Type

UDP TCP

Port Number

514

514, 1025 - 65535

Interface for Device Logs

Select the interface for sending diagnostic syslog messages.

i Note: The source IP address will either be for the management interface, or for the gateway interface if you route through data interfaces.

Data Interface

Please select an interface

Management Interface

CANCEL

OK

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

Syslog Servers



<input checked="" type="checkbox"/>		10.88.243.52	
-------------------------------------	--	--------------	--

[Create new Syslog Server](#) CANCEL OK

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

Remote Servers

DATA LOGGING

Syslog Servers



10.88.243.52

Severity level for filtering FXOS chassis syslogs

Information

Message Filtering for Firepower Threat Defense

Severity level for filtering all events

Information

Alert

Critical

Error

Warning

Notification

Information

Debug

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

SAVE

Passaggio 9. Verificare che le impostazioni siano corrette.

Device Summary

Logging Settings

✔ **Successfully saved logging settings.**

Passaggio 10. Distribuire le nuove impostazioni.



E

Pending Changes

✔ **Last Deployment Completed Successfully**
18 Aug 2022 03:18 PM. [See Deployment History](#)

Deployed Version (18 Aug 2022 03:18 PM)	Pending Version
Access Rule Edited: <i>Inside_Outside_Rule</i>	
ruleAction: TRUST	PERMIT
eventLogAction: LOG_BOTH	LOG_FLOW_END
+ Syslog Server Added: 172.16.1.250:514	
-	syslogServerIpAddress: 172.16.1.250
-	portNumber: 514
-	protocol: UDP
-	name: 172.16.1.250:514
deviceInterface:	
-	inside
Device Log Settings Edited: <i>Device-Log-Settings</i>	
syslogServerLogFilter.dataLogging.loggingEnabled: true	true
syslogServerLogFilter.dataLogging.platformLogLevel: INFORMATIONAL	INFORMATIONAL
-	syslogServerLogFilter.fileMalwareLogging.loggingEn: true
-	syslogServerLogFilter.fileMalwareLogging.severityL: true
syslogServerLogFilter.dataLogging.syslogServers:	
-	172.16.1.250:514
Access Policy Edited: <i>NGFW-Access-Policy</i>	

MORE ACTIONS ▾ CANCEL **DEPLOY NOW** ▾

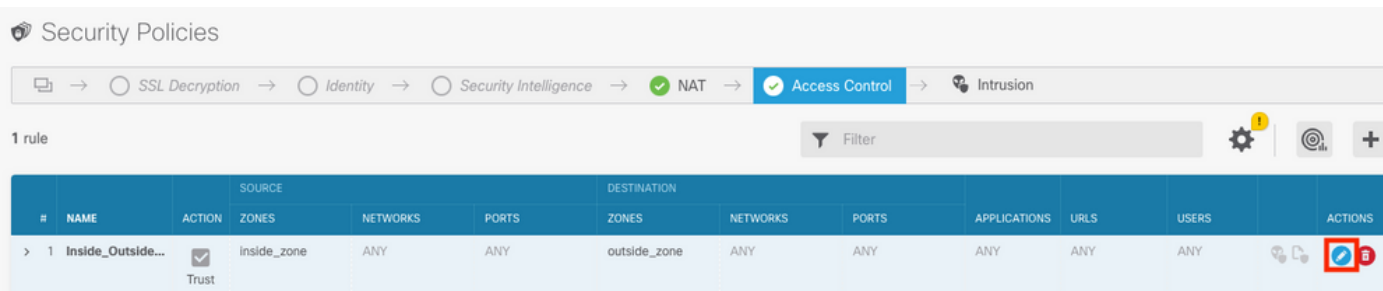
FACOLTATIVO.

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

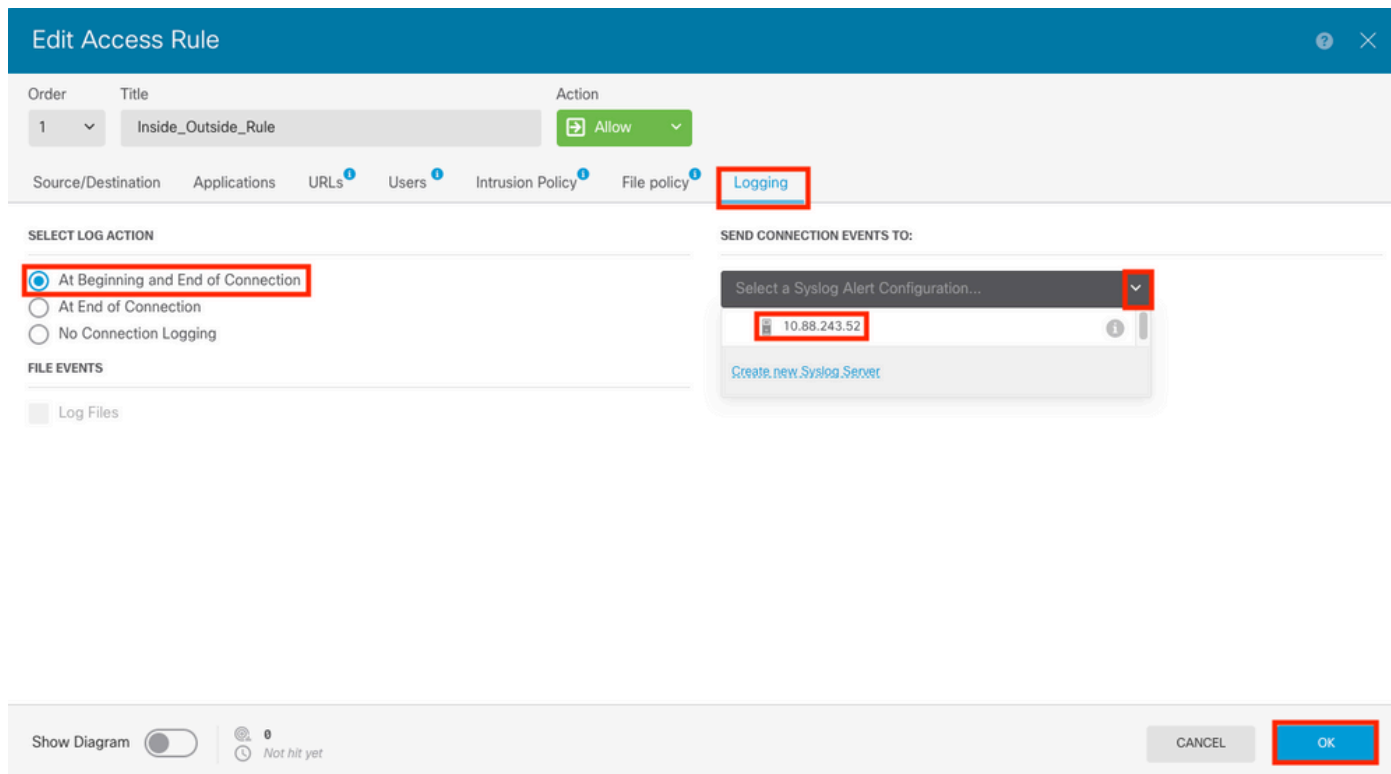
Passaggio 1. Fare clic sul pulsante Criteri nella parte superiore della schermata.



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

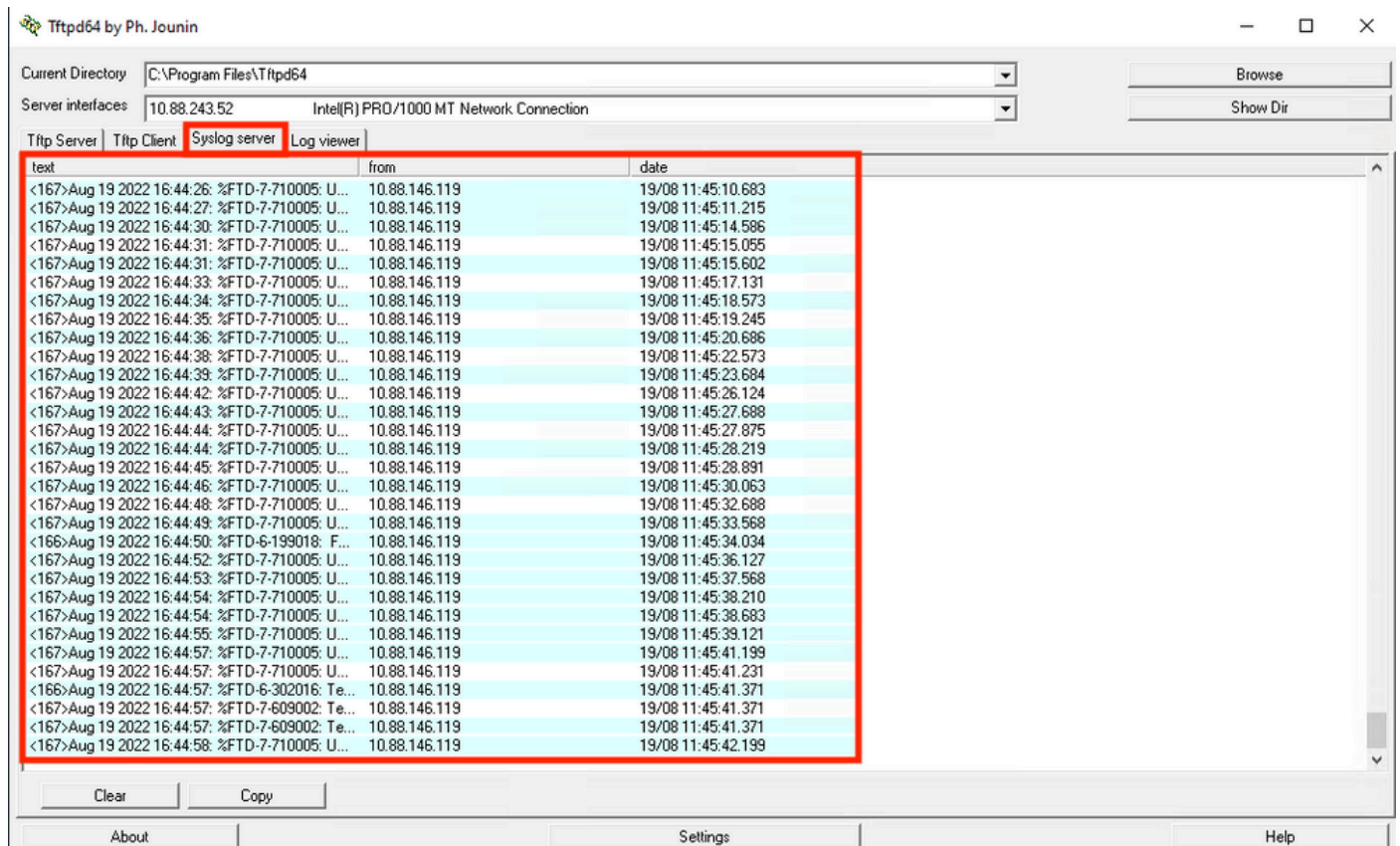
Passaggio 1. Al termine dell'operazione, è possibile verificare le impostazioni nella modalità di compressione FTD CLI usando il comando show running-config logging.

```
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

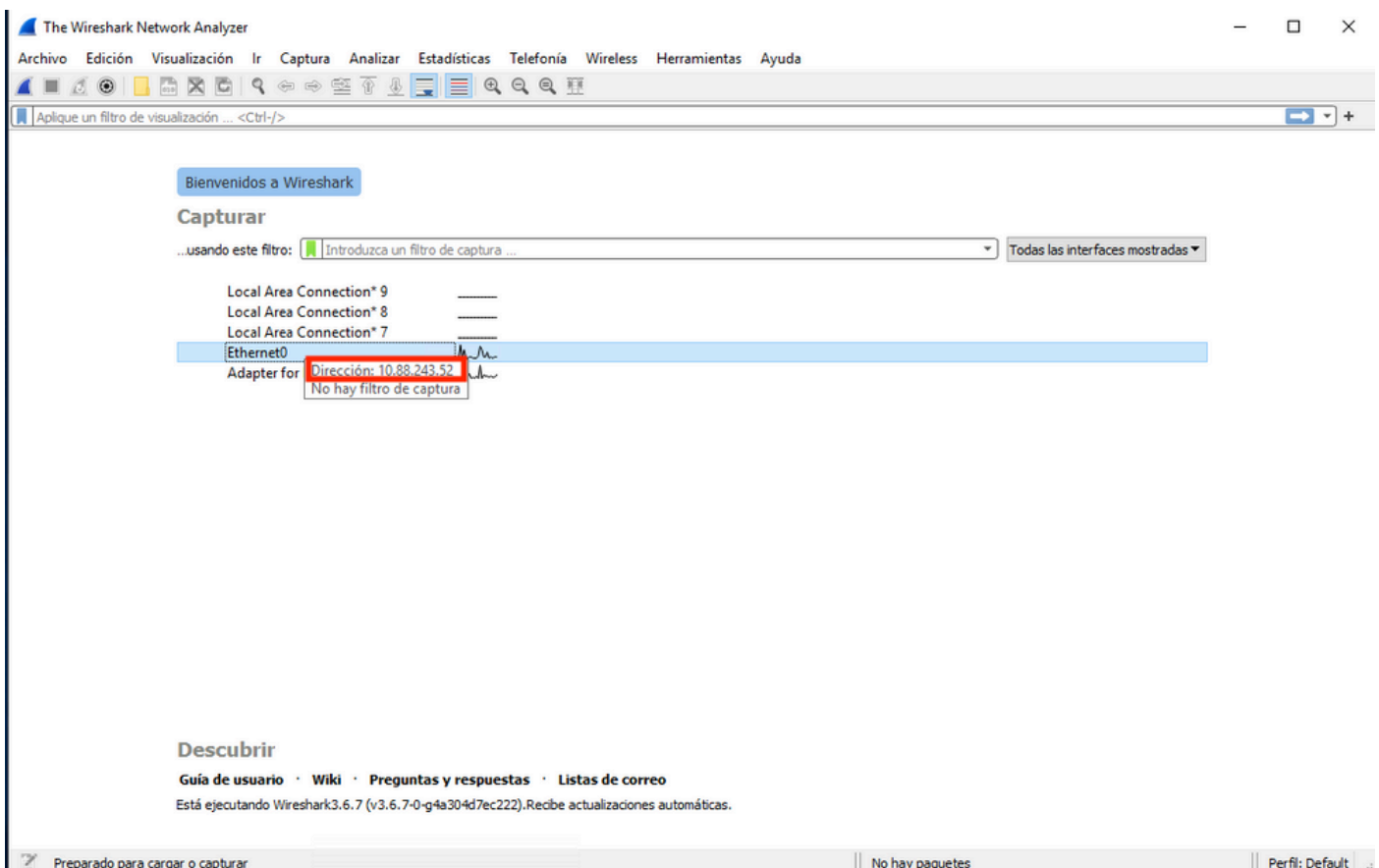
Passaggio 1. Se i messaggi Syslog sull'applicazione Syslog producono messaggi, eseguire un'acquisizione di pacchetto dalla CLI FTD per controllare la presenza di pacchetti. Passare dalla modalità Clish a LINA immettendo il comando **system support diagnostic-cli** al prompt dei comandi clish.

```
[> 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.

*Ethernet0

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

ip.addr == 10.88.146.119

No.	Time	Source	Destination	Protocol	Length	Info
26	0.328459	10.88.146.119	10.88.243.52	Syslog	155	LOCAL4.DEBUG: Aug 19 2022 16:59:34: %FTD-7-710005: UDP request discarded from
145	0.965848	10.88.146.119	10.88.243.52	Syslog	155	LOCAL4.DEBUG: Aug 19 2022 16:59:35: %FTD-7-710005: UDP request discarded from
294	1.902835	10.88.146.119	10.88.243.52	Syslog	155	LOCAL4.DEBUG: Aug 19 2022 16:59:36: %FTD-7-710005: UDP request discarded from
303	1.969237	10.88.146.119	10.88.243.52	Syslog	155	LOCAL4.DEBUG: Aug 19 2022 16:59:36: %FTD-7-710005: UDP request discarded from
435	3.614217	10.88.146.119	10.88.243.52	Syslog	155	LOCAL4.DEBUG: Aug 19 2022 16:59:38: %FTD-7-710005: UDP request discarded from
461	3.990606	10.88.146.119	10.88.243.52	Syslog	155	LOCAL4.DEBUG: Aug 19 2022 16:59:38: %FTD-7-710005: UDP request discarded from
523	4.329918	10.88.146.119	10.88.243.52	Syslog	155	LOCAL4.DEBUG: Aug 19 2022 16:59:38: %FTD-7-710005: UDP request discarded from
540	4.465525	10.88.146.119	10.88.243.52	Syslog	155	LOCAL4.DEBUG: Aug 19 2022 16:59:38: %FTD-7-710005: UDP request discarded from
572	4.904842	10.88.146.119	10.88.243.52	Syslog	155	LOCAL4.DEBUG: Aug 19 2022 16:59:39: %FTD-7-710005: UDP request discarded from

> Frame 26: 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits) on interface \Device\NPF_{FFB4AA7C-2AE5-4A96-BFFA-F3A92CE11E17}, id 0

> Ethernet II, Src: Cisco_df:1a:f5 (84:3d:c6:df:1a:f5), Dst: VMware_b3:f9:3b (00:50:56:b3:f9:3b)

> Internet Protocol Version 4, Src: 10.88.146.119, Dst: 10.88.243.52

> User Datagram Protocol, Src Port: 36747, Dst Port: 514

> Syslog message: LOCAL4.DEBUG: Aug 19 2022 16:59:34: %FTD-7-710005: UDP request discarded from 0.0.0.0/68 to diagnostic:255.255.255.255/67\n

```

0000  00 50 56 b3 f9 3b 84 3d c6 df 1a f5 08 00 45 00  ·PV·;·= ······E·
0010  00 8d 2b 13 40 00 3c 11 78 f1 0a 58 92 77 0a 58  ·+·@·<·x·X·w·X
0020  f3 34 8f 8b 02 02 00 79 6a a1 3c 31 36 37 3e 41  ·4······y·j·<167>A
0030  75 67 20 31 39 20 32 30 32 32 20 31 36 3a 35 39  ug 19 20 22 16:59
0040  3a 33 34 3a 20 25 46 54 44 2d 37 2d 37 31 30 30  :34: %FT D-7-7100
0050  30 35 3a 20 55 44 50 20 72 65 71 75 65 73 74 20  05: UDP request
0060  64 69 73 63 61 72 64 65 64 20 66 72 6f 6d 20 30  discarde d from 0
0070  2e 30 2e 30 2e 30 2f 36 38 20 74 6f 20 64 69 61  .0.0.0/6 8 to dia
0080  67 6e 6f 73 74 69 63 3a 32 35 35 2e 32 35 35 2e  gnostic: 255.255.
0090  32 35 35 2e 32 35 35 2f 36 37 0a 255.255/ 67·

```

wireshark_Ethernet01BP1Q1.pcapng Paquetes: 11865 · Mostrado: 77 (0.6%) · Perdido: 0 (0.0%) Perfil: Default

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).