

Konfiguration und Überprüfung des Syslog im FirePOWER Geräte-Manager

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Konfigurationen](#)

[Überprüfung](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie Syslog im FirePOWER Device Manager (FDM) konfigurieren.

Voraussetzungen

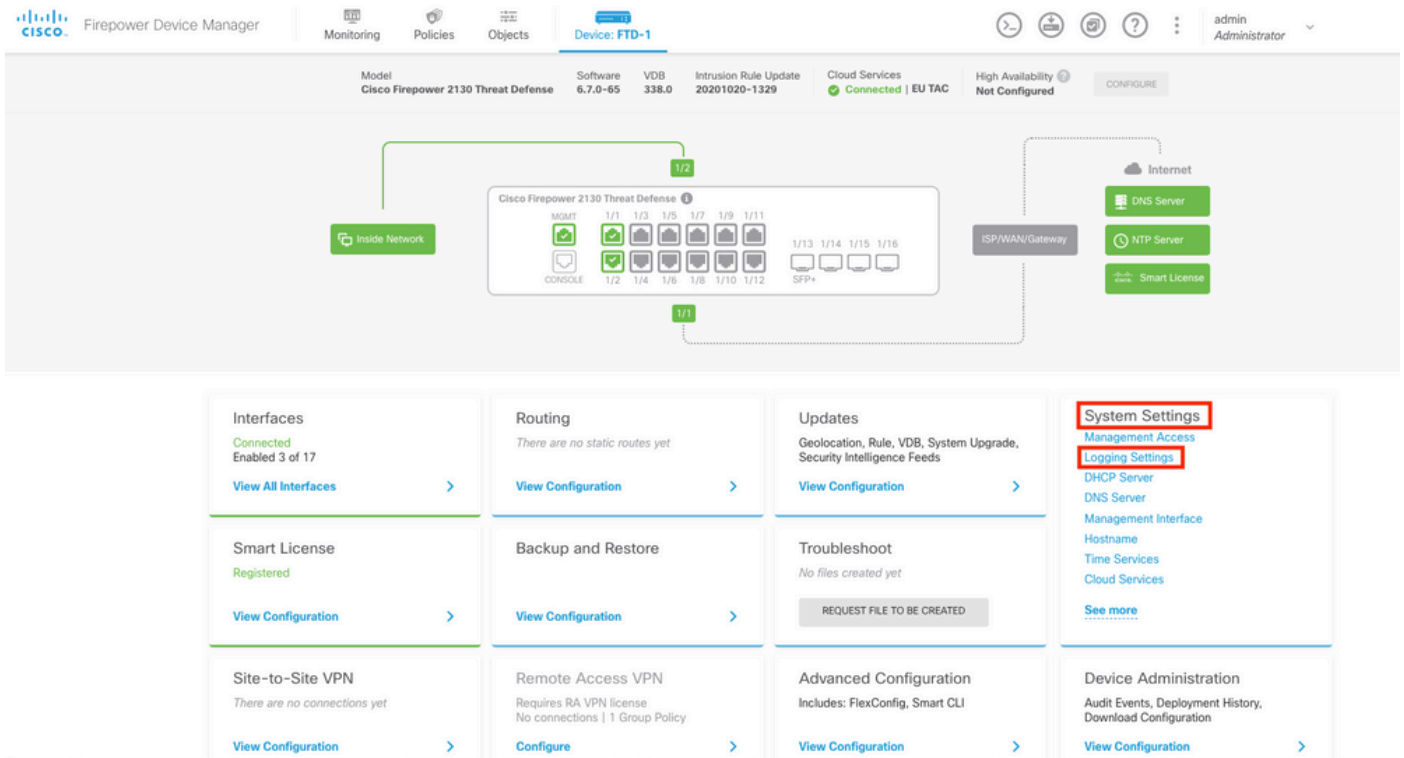
Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

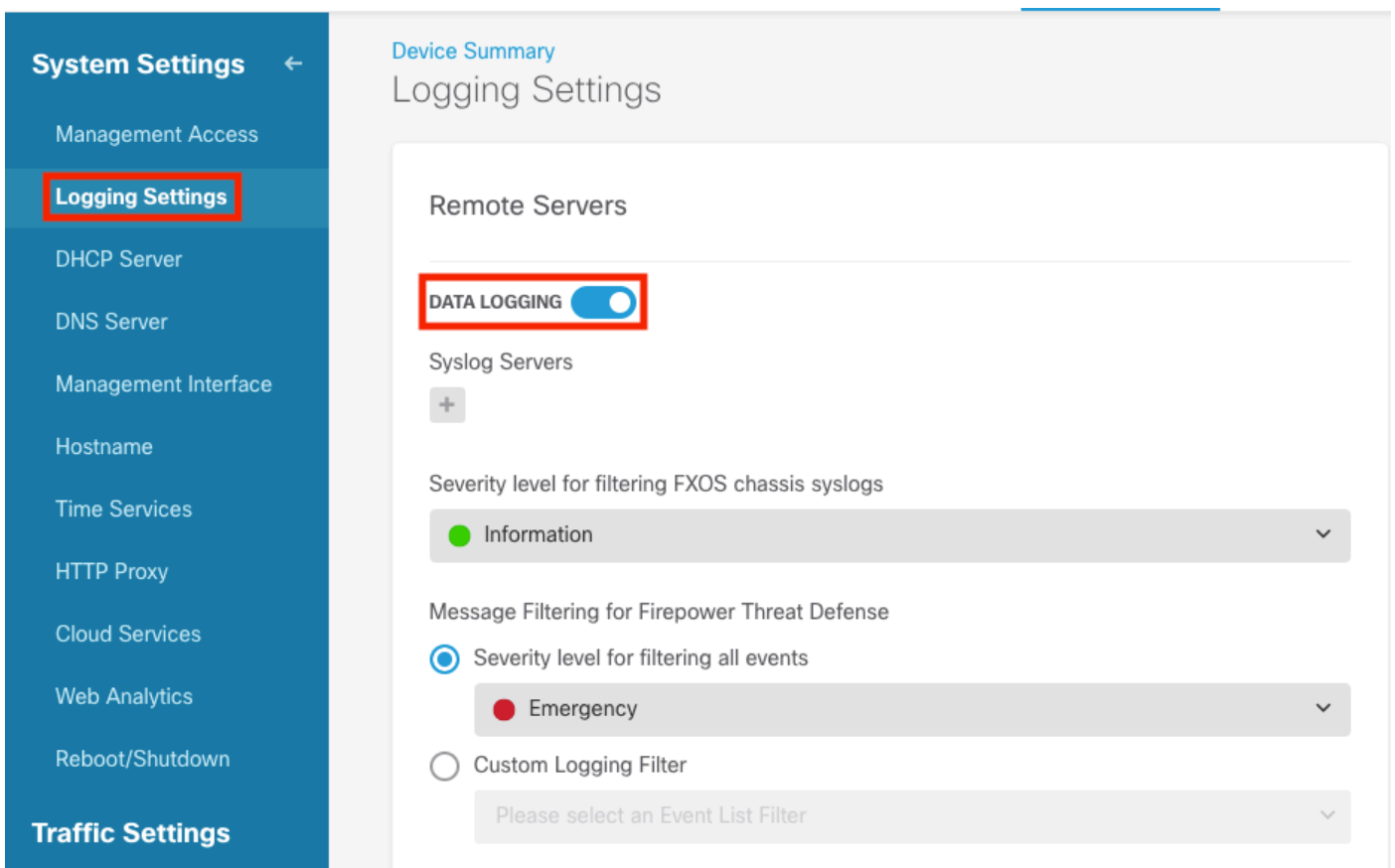
- FirePOWER Threat Defence
- Syslog-Server mit Syslog-Software zur Datenerfassung

Konfigurationen

Schritt 1: Wählen Sie im Hauptbildschirm des FirePOWER Geräte-Managers die Protokollierungseinstellungen unter den Systemeinstellungen in der rechten unteren Ecke des Bildschirms aus.



Schritt 2: Wählen Sie im Bildschirm "System Settings" (Systemeinstellungen) im Menü auf der linken Seite die Option Logging Settings (Protokollierungseinstellungen) aus.



Schritt 3: Legen Sie den Umschalter für die Datenprotokollierung fest, indem Sie unter Syslog Servers (Syslog-Server) das Zeichen + auswählen.

Schritt 4: Wählen Sie Syslog-Server hinzufügen aus. Alternativ können Sie das Syslog-

Serverobjekt unter Objekte - Syslog-Server erstellen.

Device Summary
Logging Settings

Remote Servers

DATA LOGGING

Syslog Servers

+

Filter

Nothing found

[Create new Syslog Server](#) CANCEL OK

Please select an Event List Filter

Schritt 5: Geben Sie die IP-Adresse Ihres Syslog-Servers und die Portnummer ein. Aktivieren Sie das Optionsfeld Datenschnittstelle, und wählen Sie OK aus.

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

Schritt 6: Wählen Sie anschließend den neuen Syslog-Server aus, und wählen Sie OK aus.

Syslog Servers



Filter

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

[Create new Syslog Server](#) CANCEL OK

Schritt 7. Aktivieren Sie das Optionsfeld Schweregrad zum Filtern aller Ereignisse, und wählen Sie die gewünschte Protokollierungsebene aus.

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

Schritt 8: Wählen Sie unten im Bildschirm Speichern aus.

SAVE

Schritt 9: Überprüfen Sie, ob die Einstellungen erfolgreich waren.

Device Summary

Logging Settings

✔ Successfully saved logging settings.

Schritt 10. Bereitstellen der neuen Einstellungen



und

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** ▾

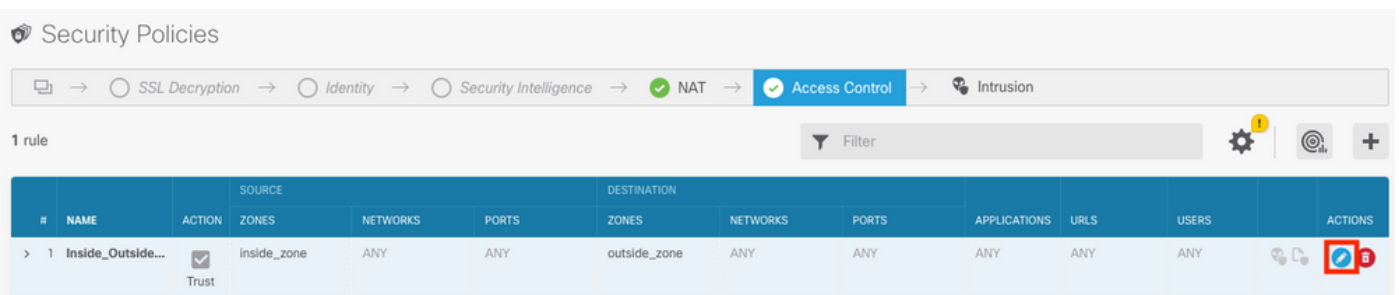
OPTIONAL.

Darüber hinaus können die Zugriffskontrollregeln der Zugriffskontrollrichtlinie so festgelegt werden, dass sie sich beim Syslog-Server anmelden:

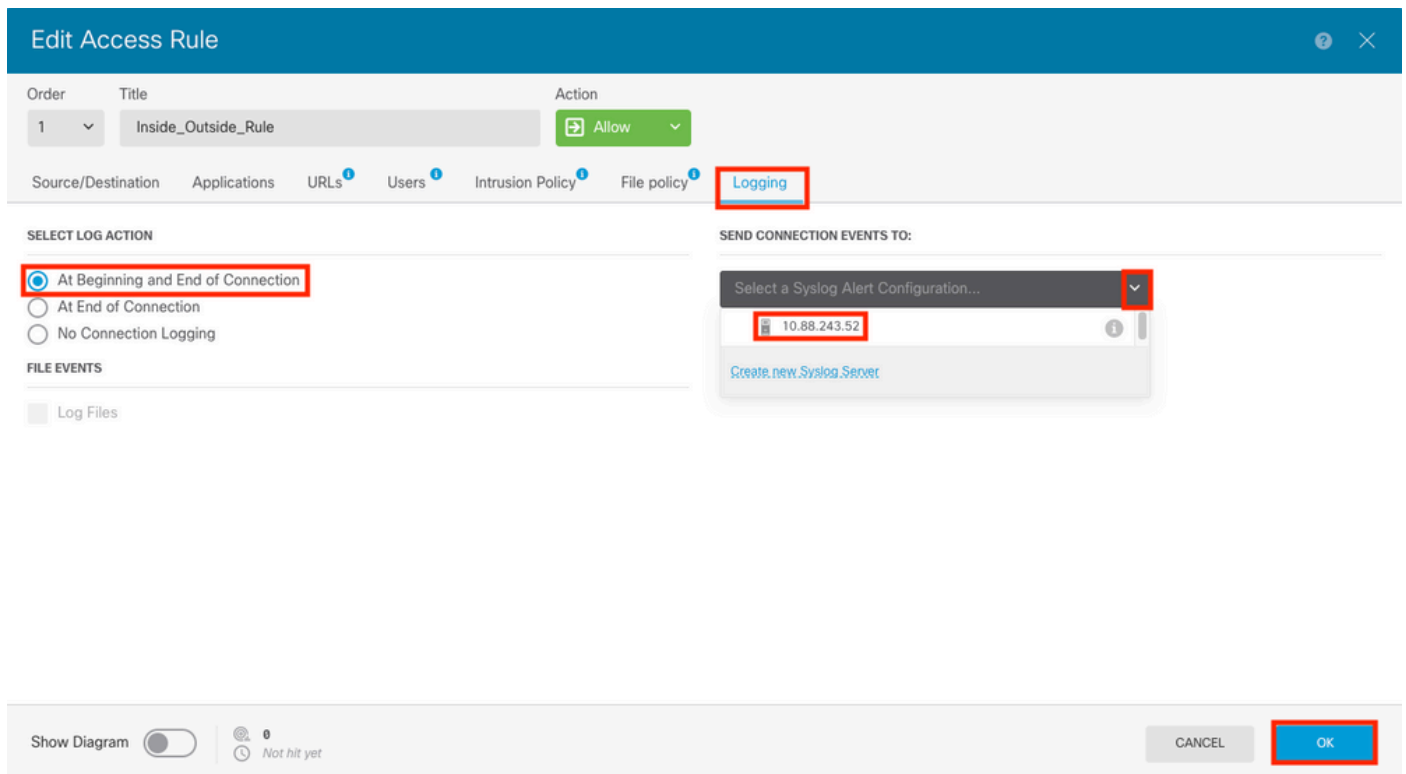
Schritt 1: Klicken Sie oben im Bildschirm auf die Schaltfläche "Richtlinien".



Schritt 2: Bewegen Sie den Mauszeiger über die rechte Seite der ACP-Regel, um die Protokollierung hinzuzufügen, und wählen Sie das Bleistiftsymbol aus.



Schritt 3: Wählen Sie die Registerkarte Protokollierung aus, aktivieren Sie das Optionsfeld bei Verbindungsende, wählen Sie den Dropdown-Pfeil unter Syslog-Warmeldungskonfiguration auswählen aus, wählen Sie auf dem Syslog-Server aus, und wählen Sie OK aus.



Schritt 4: Bereitstellen der Konfigurationsänderungen

Überprüfung

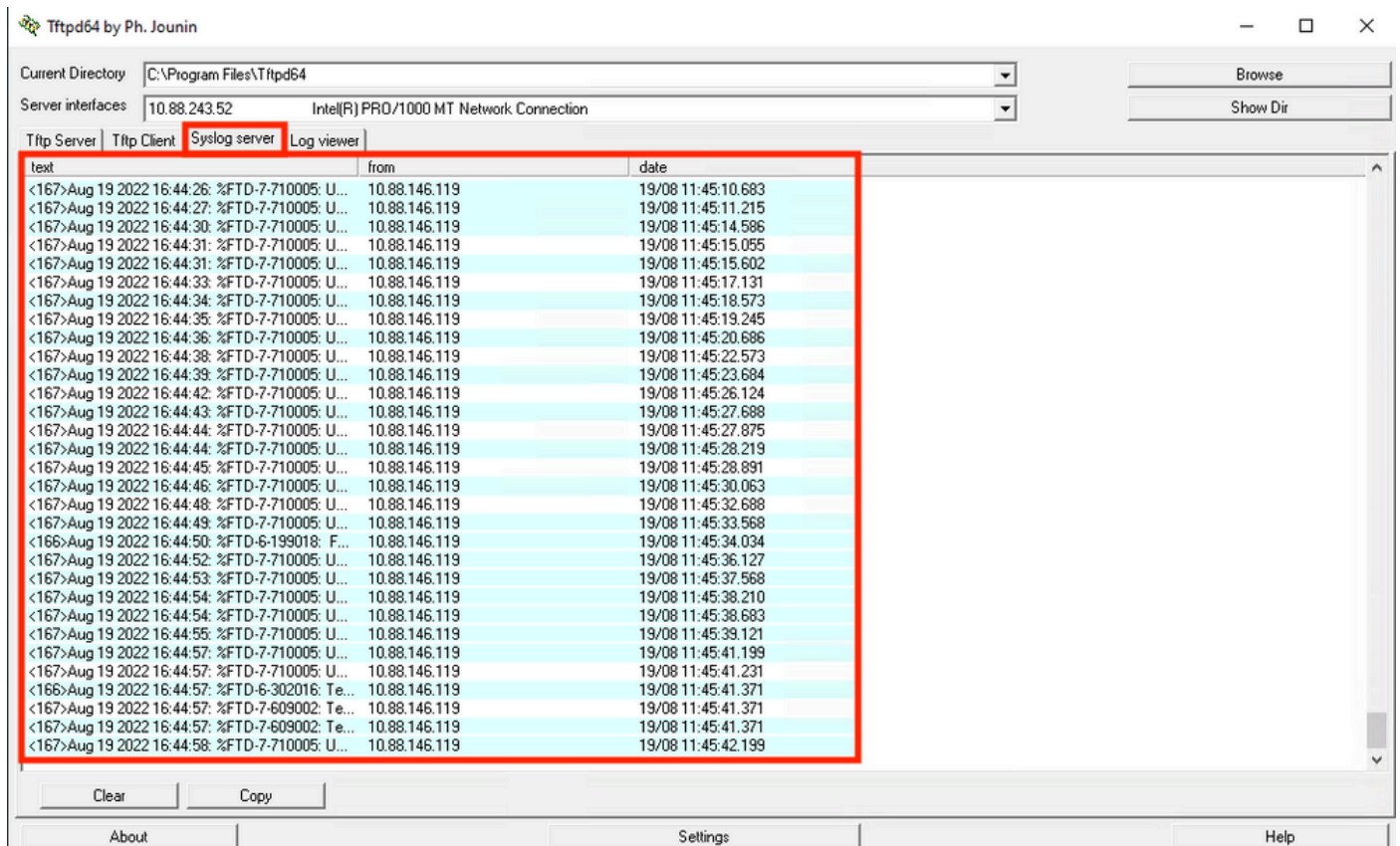
Schritt 1: Nach Abschluss der Aufgabe können Sie die Einstellungen im FTD CLI-Clientmodus mit dem Befehl **show running-config logging** überprüfen.

```
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
>
```

Schritt 2: Navigieren Sie zum Syslog-Server, und stellen Sie sicher, dass die Syslog-Serveranwendung Syslog-Meldungen annimmt.



Fehlerbehebung

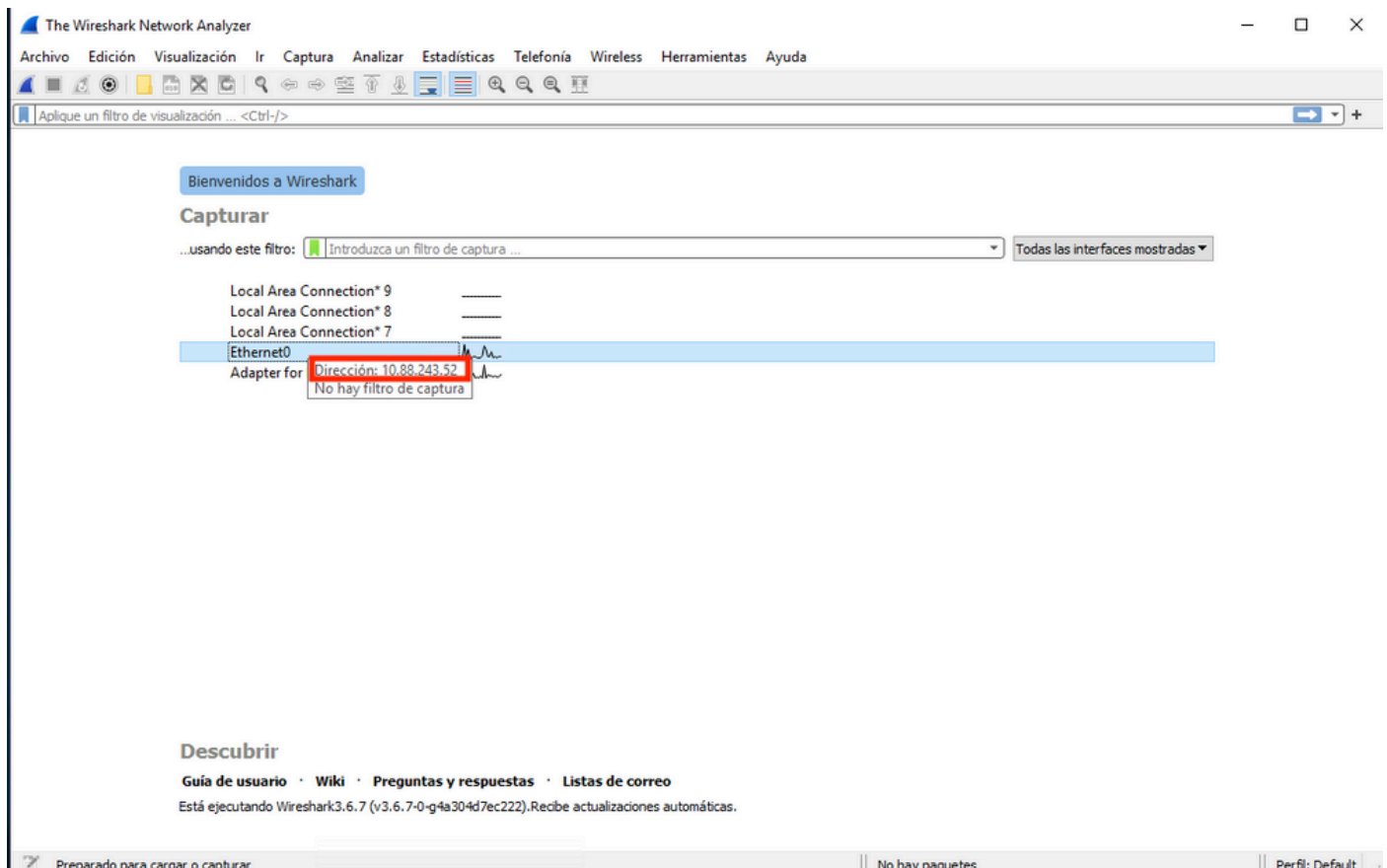
Schritt 1: Wenn die Syslog-Meldungen der Syslog-Anwendung hervorrufen, führen Sie eine Paketerfassung über die FTD-CLI durch, um zu überprüfen, ob Pakete vorhanden sind. Wechseln Sie vom Clientmodus in LINA, indem Sie den Befehl **system support diagnostic-cli** an der Eingabeaufforderung clish eingeben.

```
[> 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#
```

Schritt 2: Erstellen Sie eine Paketerfassung für Ihren UDP 514 (oder TCP 1468, wenn Sie TCP verwendet haben)

Schritt 3: Stellen Sie sicher, dass die Kommunikation mit der Netzwerkschnittstellenkarte auf dem Syslog-Server erfolgt. Verwenden Sie Wireshark oder ein anderes geladenes Dienstprogramm zur Paketerfassung. Doppelklicken Sie auf die Schnittstelle in Wireshark, damit der Syslog-Server mit der Paketerfassung beginnt.



Schritt 4: Legen Sie einen Anzeigefilter in der oberen Leiste für udp 514 fest, indem Sie `udp.port==514` eingeben und den Pfeil rechts neben der Leiste auswählen. Überprüfen Sie anhand der Ausgabe, ob die Pakete den Syslog-Server erreichen.

*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

Schritt 5: Wenn die Syslog-Serveranwendung die Daten nicht anzeigt, beheben Sie die Fehler in der Syslog-Serveranwendung. Stellen Sie sicher, dass das richtige Protokoll udp/tcp und der richtige Port 514/1468 verwendet wird.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.