Konfiguration und Überprüfung des Syslog im FirePOWER Geräte-Manager

Inhalt

Einleitung

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

Voraussetzungen

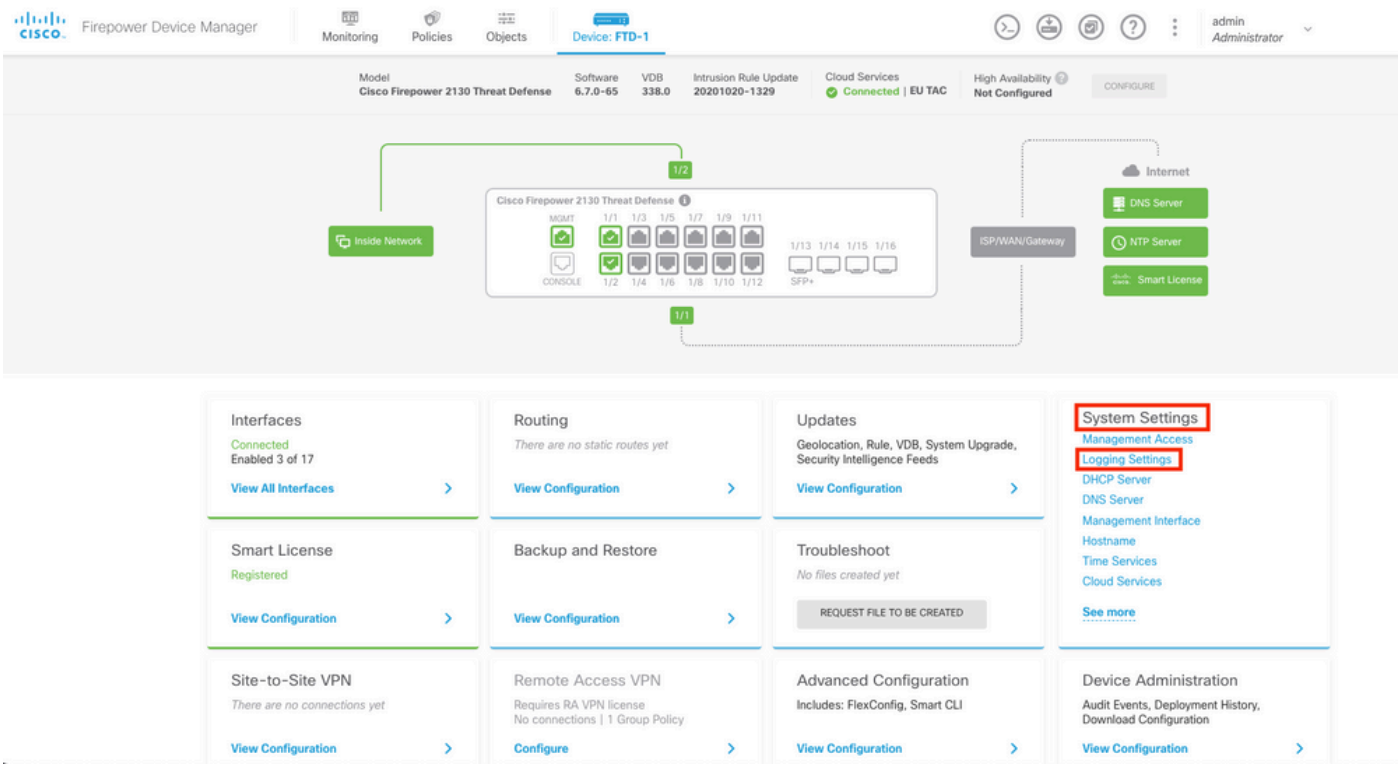
Anforderungen

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

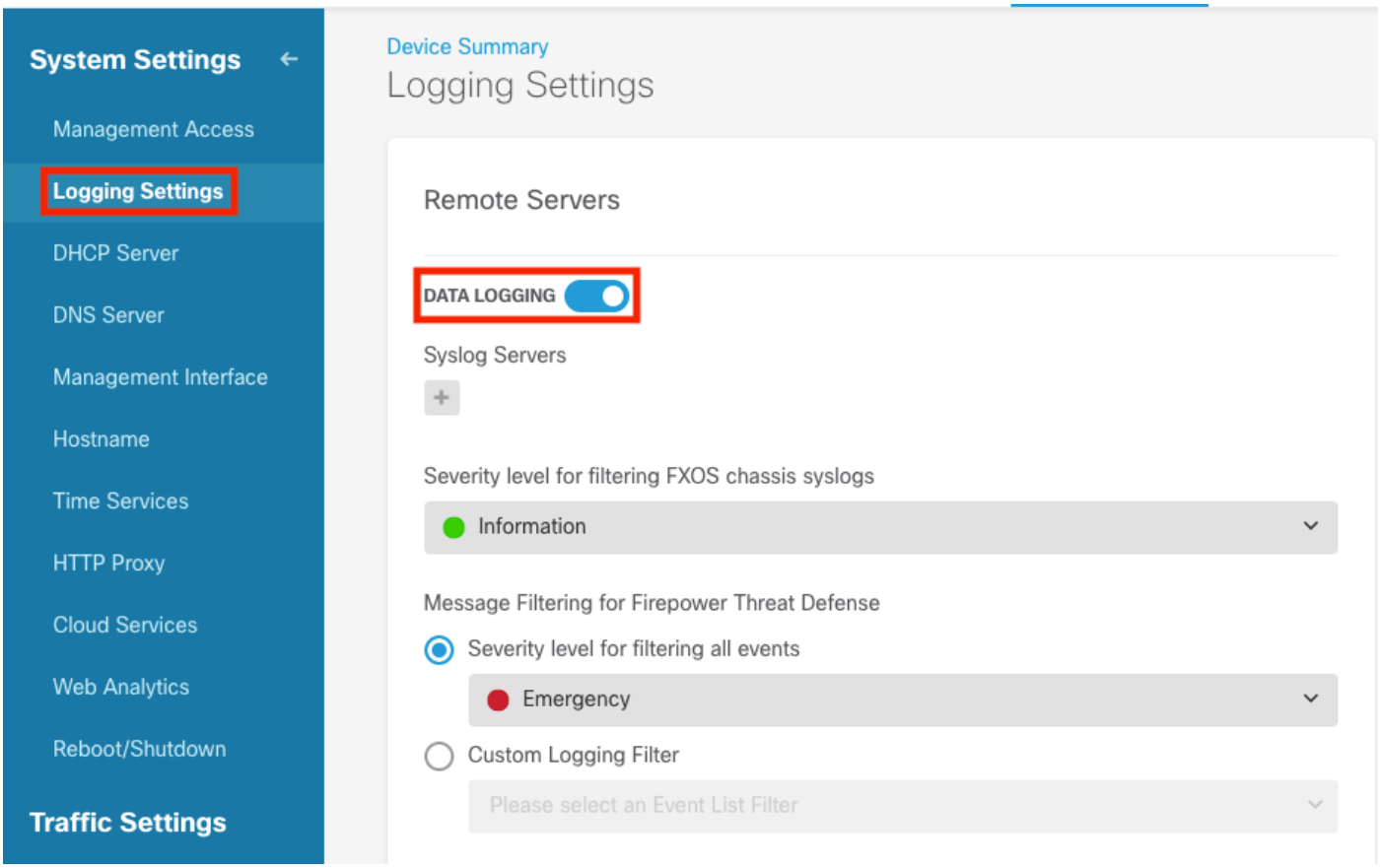
- FirePOWER Threat Defence
- Syslog-Server mit Syslog-Software zur Datenerfassung

Konfigurationen

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



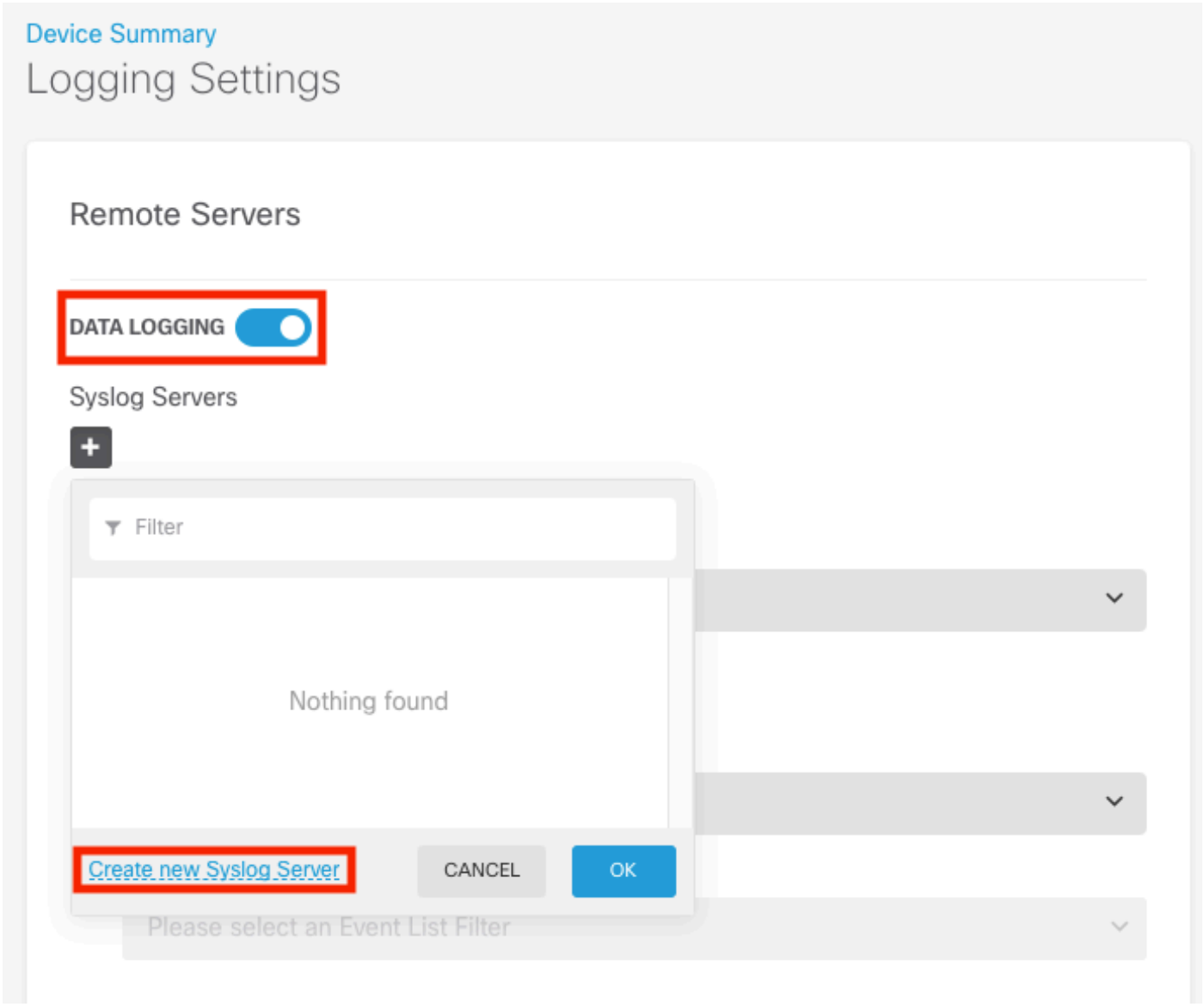
Schritt 2: Wählen Sie im Bildschirm "System Settings" (Systemeinstellungen) im Menü auf der linken Seite die Option Logging Settings (Protokollierungseinstellungen) aus.



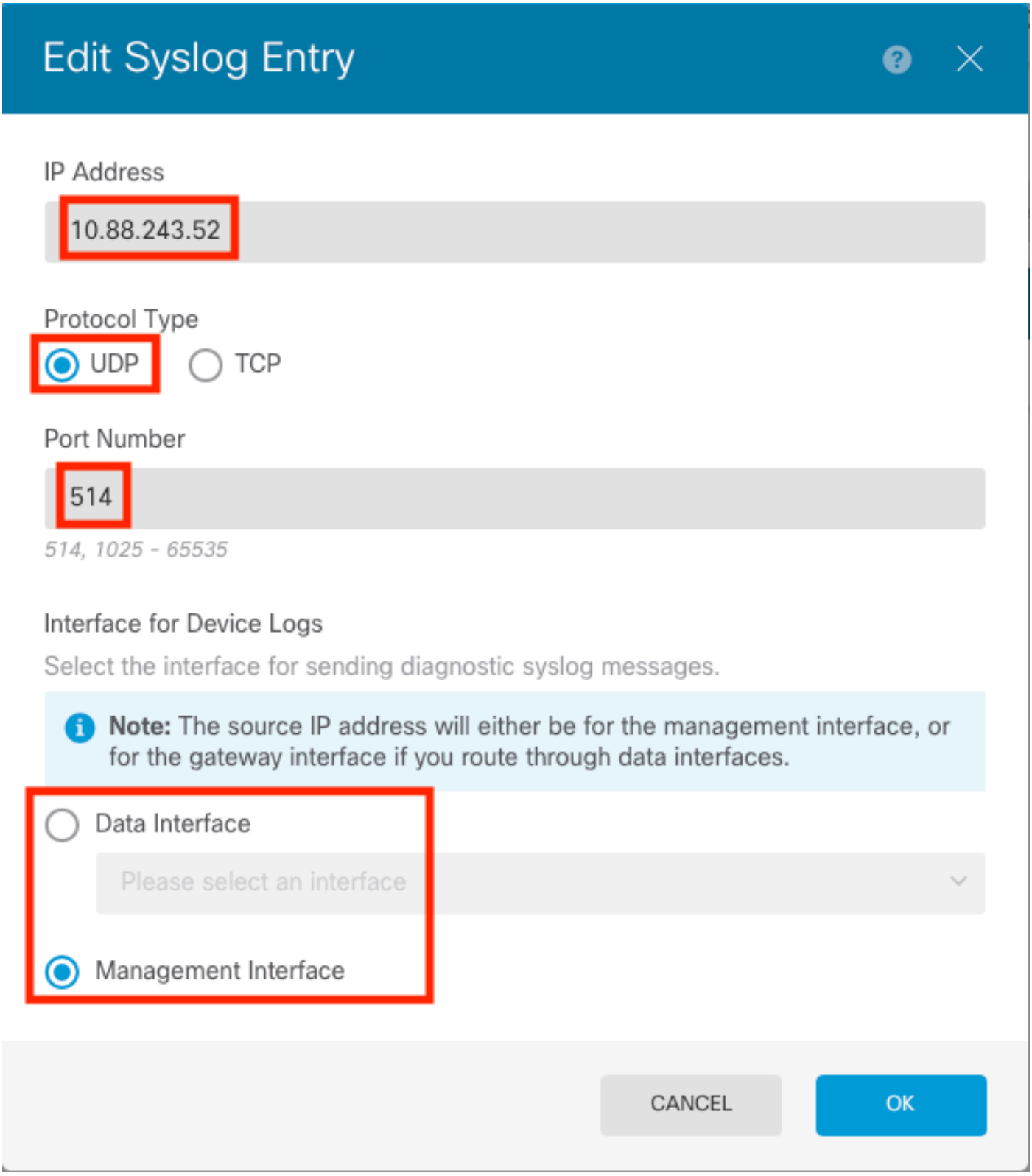
Schritt 3: Legen Sie den Umschalter für die Datenprotokollierung fest, indem Sie unter Syslog Servers (Syslog-Server) das Zeichen + auswählen.

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

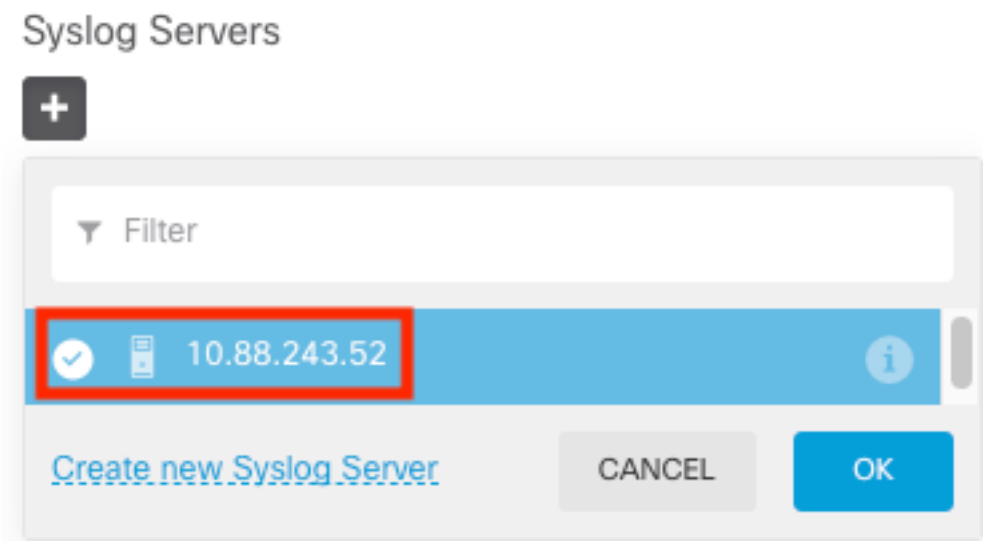
Serverobjekt unter Objekte - Syslog-Server erstellen.



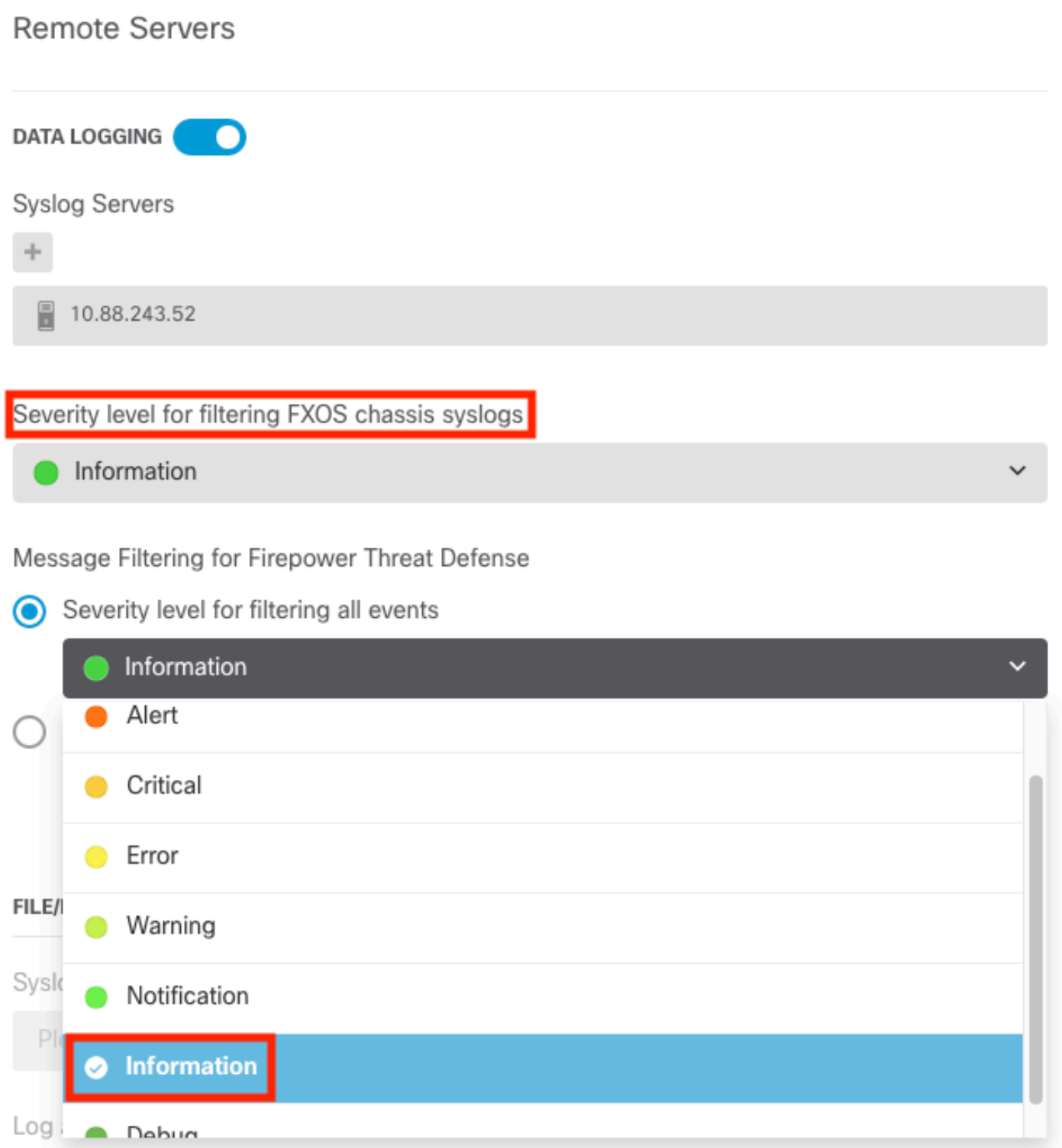
Schritt 5: Geben Sie die IP-Adresse Ihres Syslog-Servers und die Portnummer ein. Aktivieren Sie das Optionsfeld Datenschnittstelle, und wählen Sie OK aus.



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

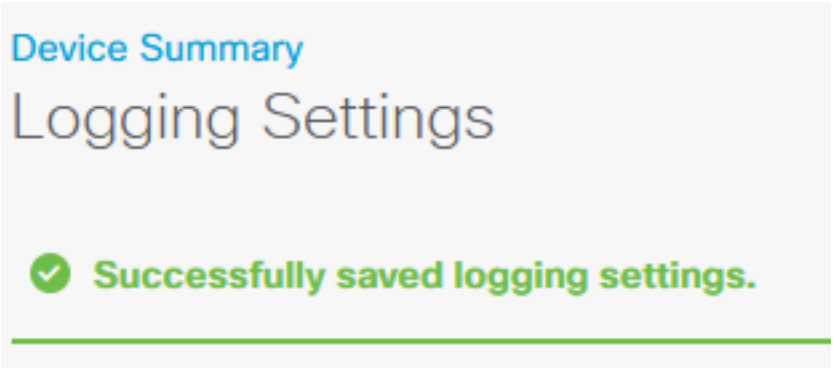


Schritt 7. Aktivieren Sie das Optionsfeld Schweregrad zum Filtern aller Ereignisse, und wählen Sie die gewünschte Protokollierungsebene aus.



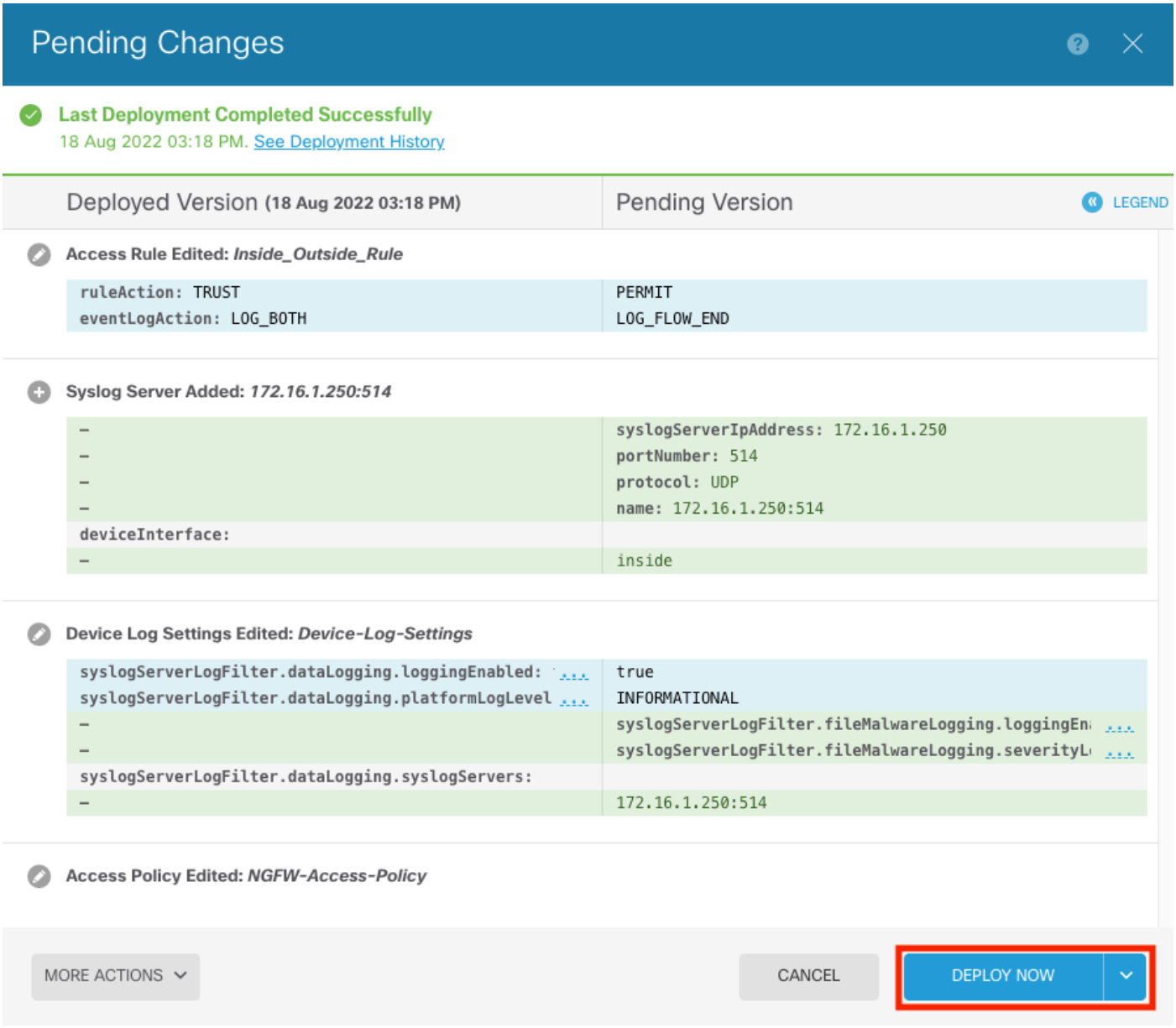
Schritt 8: Wählen Sie unten im Bildschirm Speichern aus.

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



Schritt 10. Bereitstellen der neuen Einstellungen

und

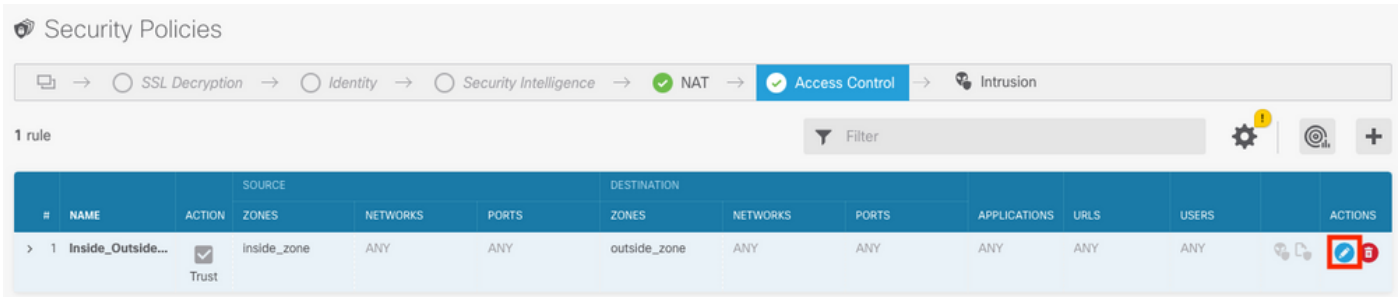


OPTIONAL.

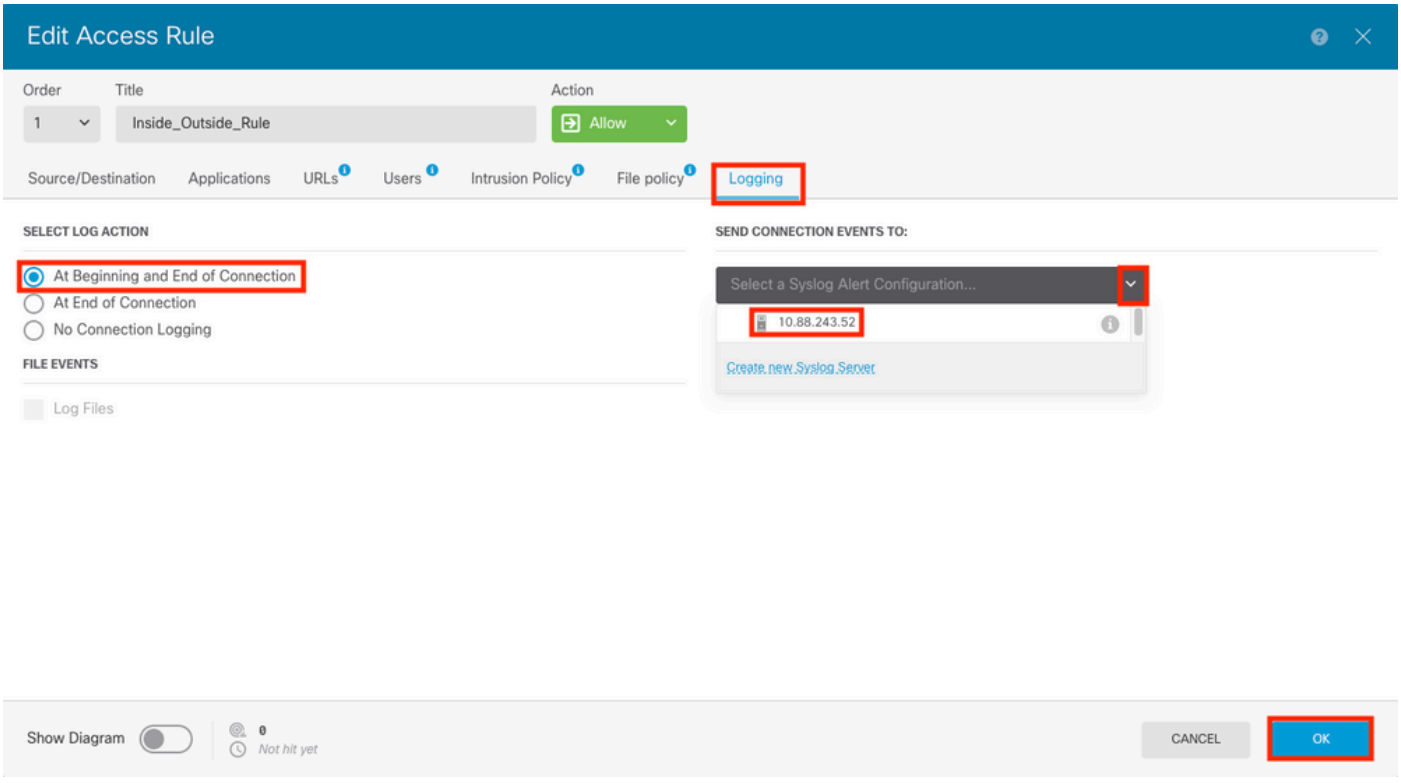
Darüber hinaus können die Zugriffskontrollregeln der Zugriffskontrollrichtlinie so festgelegt werden, dass sie sich beim Syslog-Server anmelden:

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-Warnmeldungskonfiguration auswählen aus, wählen Sie auf dem Syslog-Server aus, und wählen Sie OK aus.



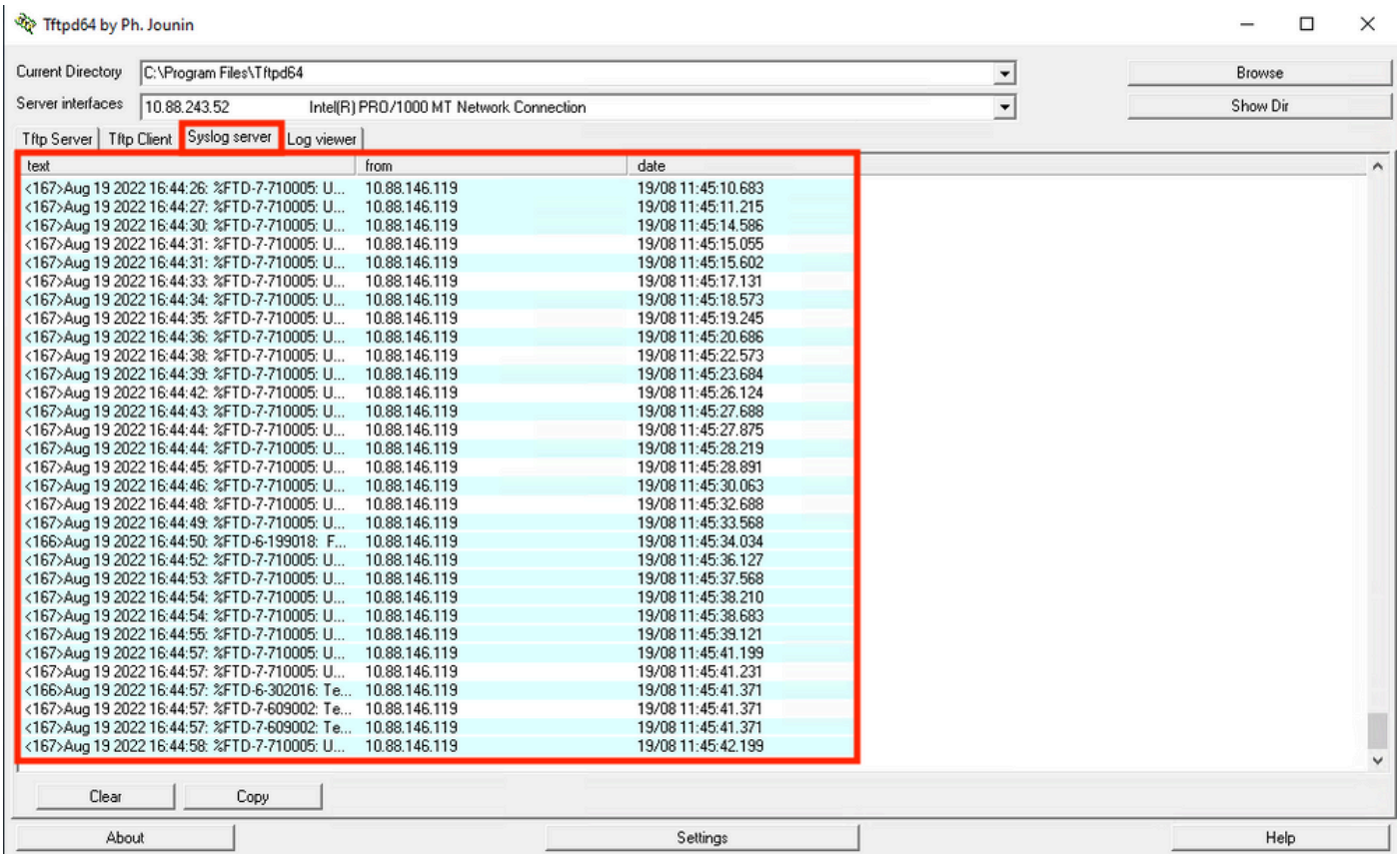
Schritt 4: Bereitstellen der Konfigurationsänderungen

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.



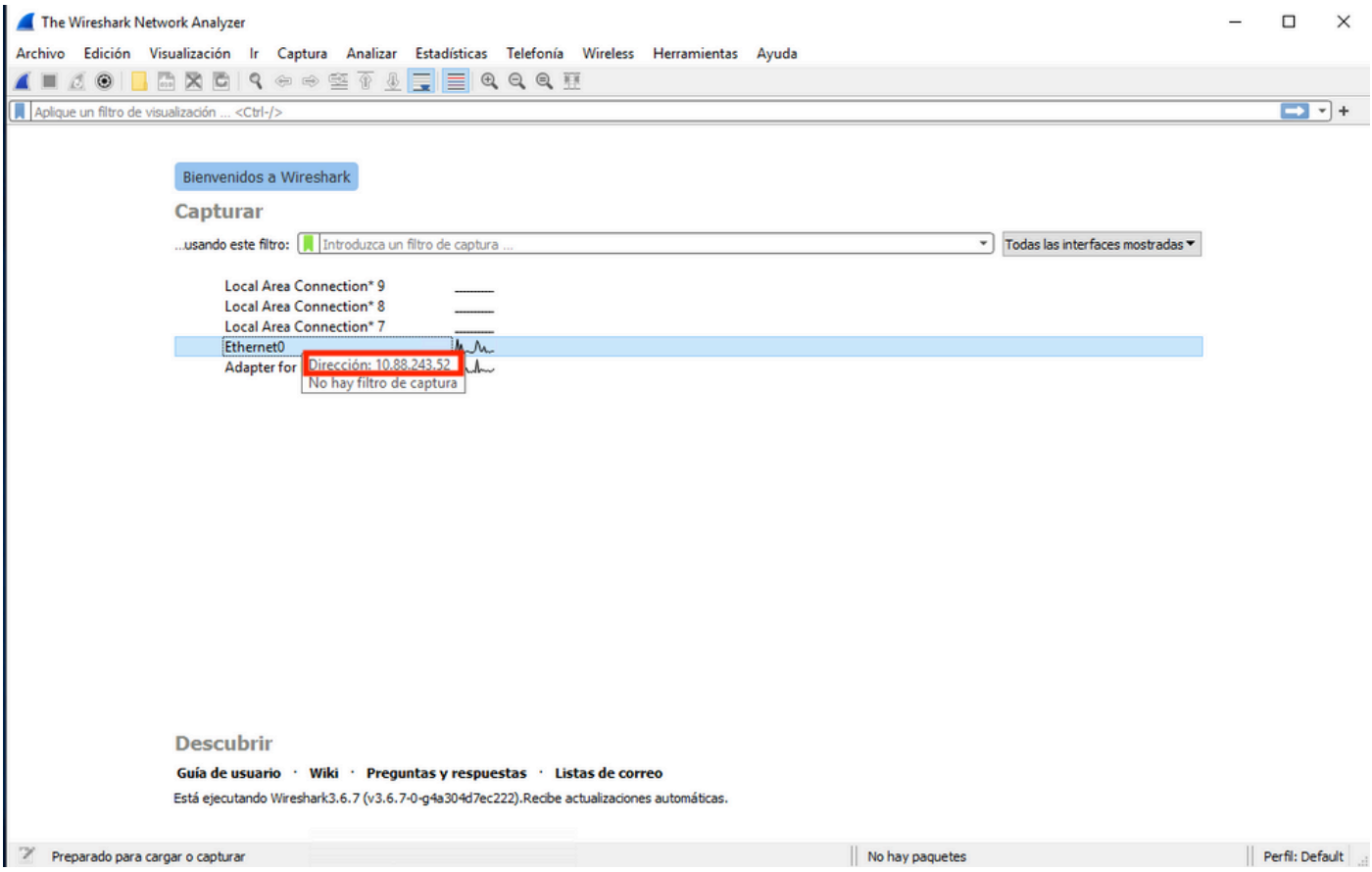
Fehlerbehebung

Schritt 1: Wenn die Syslog-Meldungen der Syslog-Anwendung Meldungen 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.

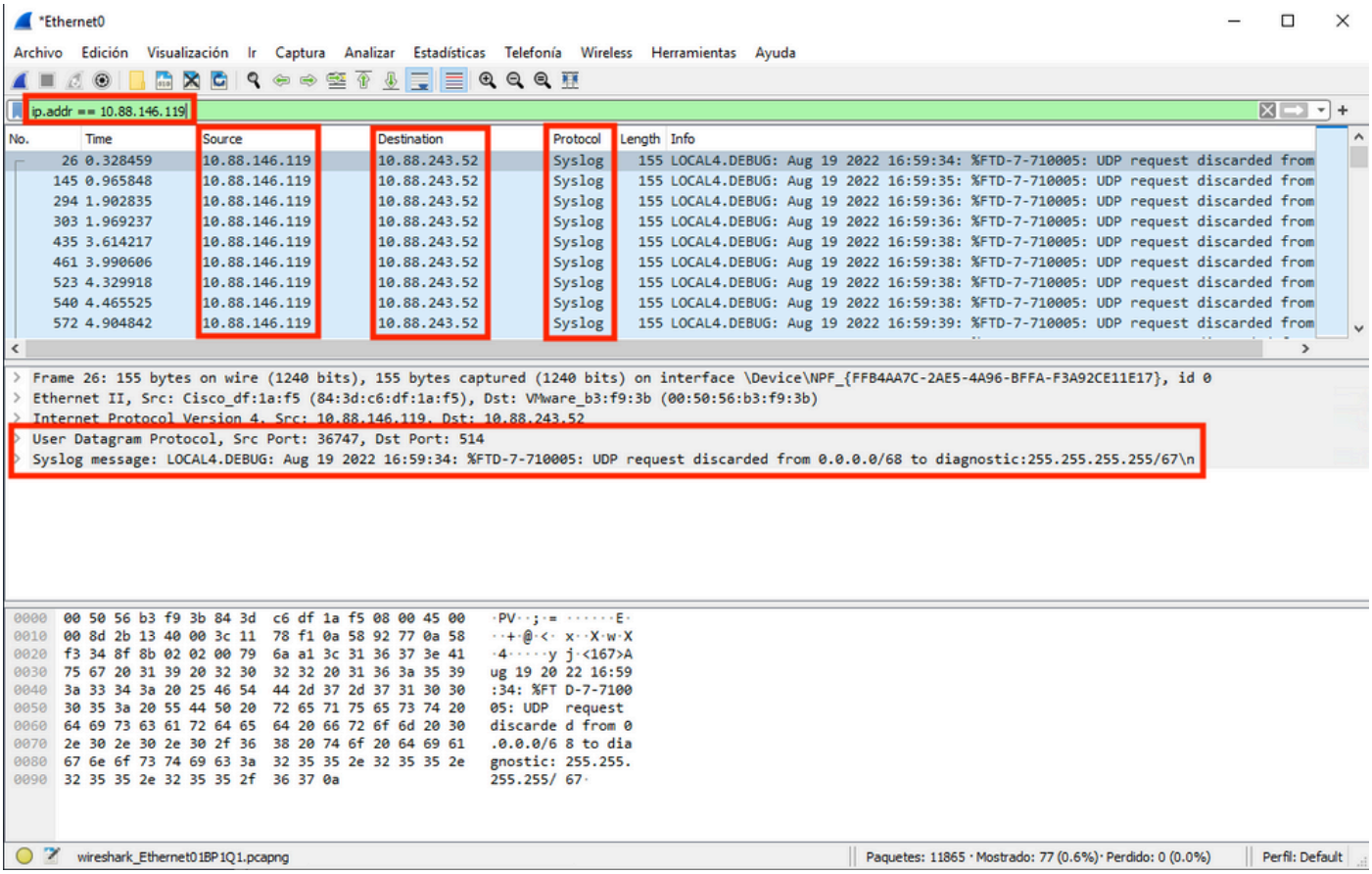
```
[> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

[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.



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.