Firepower Device Manager(FDM)でのSyslogの設定と確認

内容

概要

このドキュメントでは、Firepower Device Manager(FDM)内でSyslogを設定する方法について説明します。

前提条件

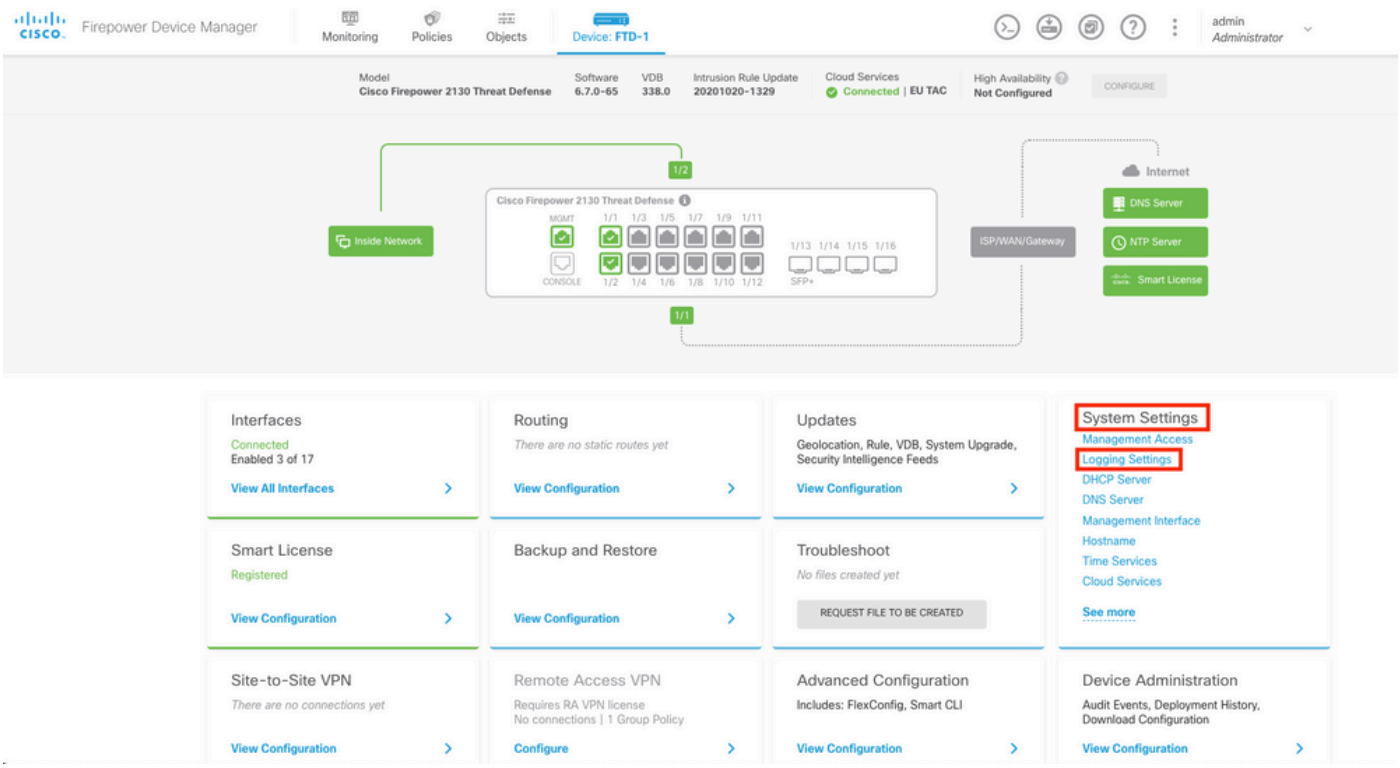
要件

次の項目に関する知識があることが推奨されます。

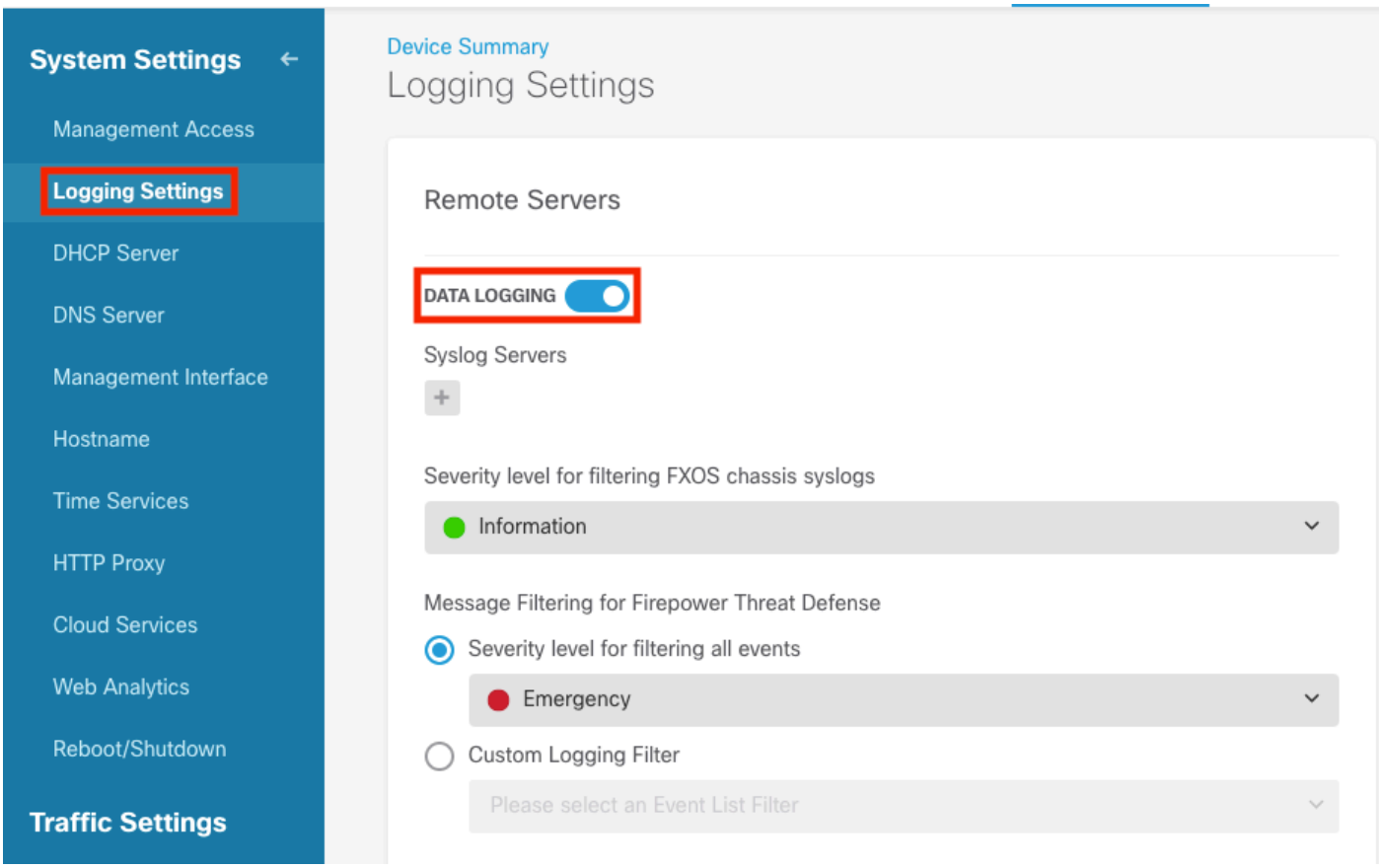
- Firepower脅威防御
- Syslogソフトウェアを実行してデータを収集するSyslogサーバ

設定

ステップ 1：Firepowerデバイスマネージャのメイン画面から、画面の右下隅にある[System Settings]の下の[Logging Settings]を選択します。

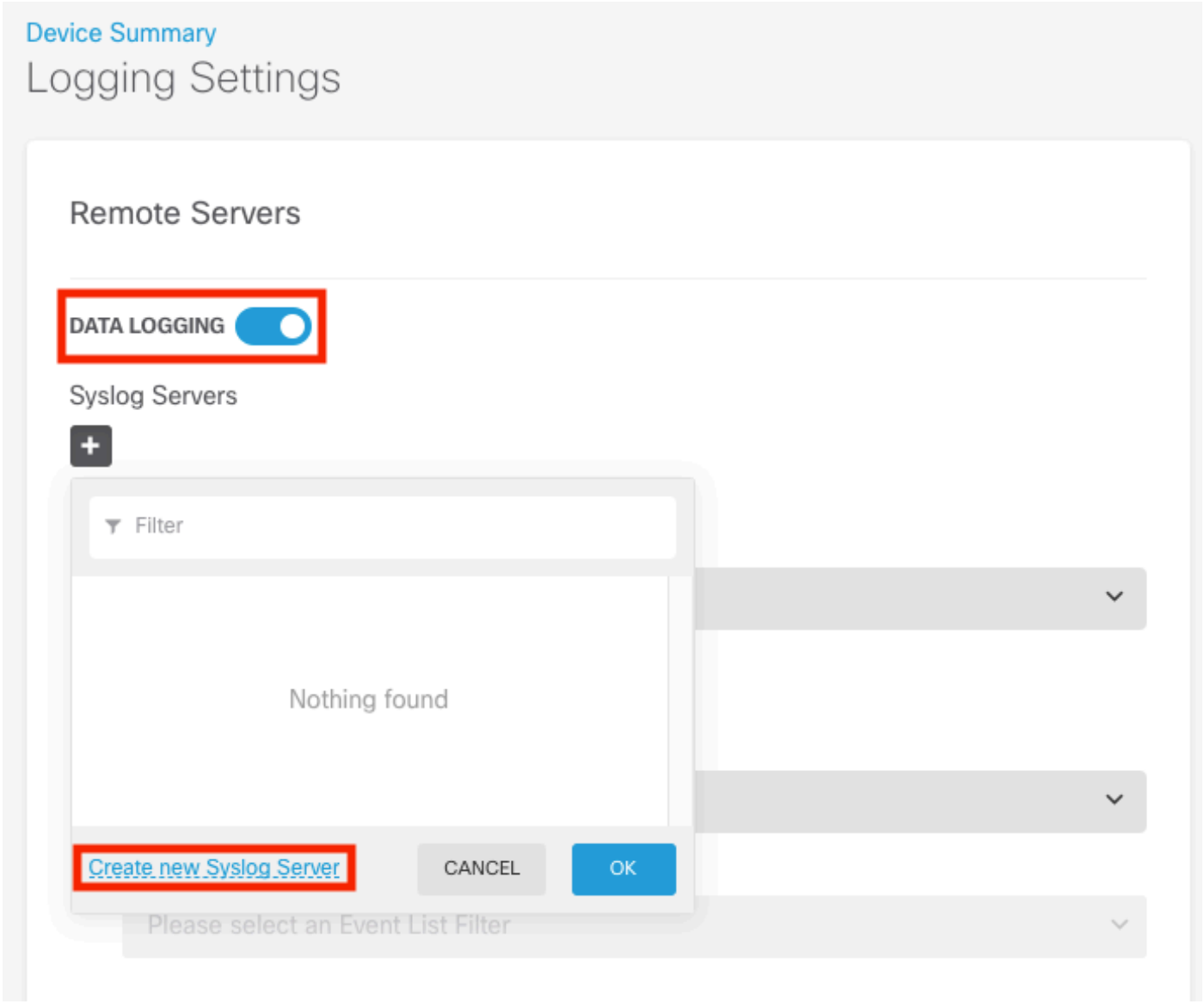


ステップ 2：[System Settings]画面で、左側のメニューから[Logging Settings]を選択します。

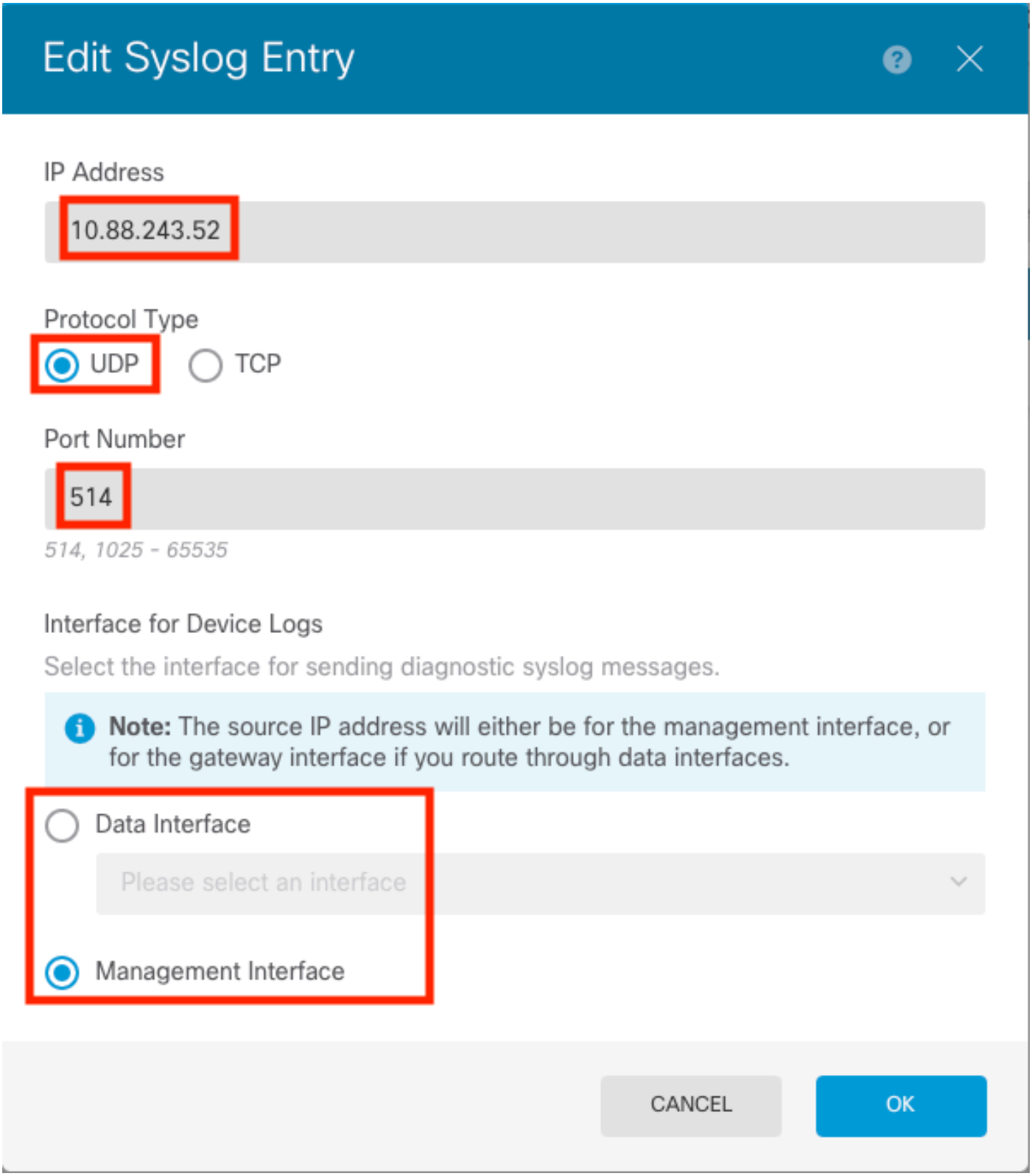


ステップ 3：Syslog Serversの下の+記号を選択して、Data Loggingトグルスイッチを設定します。

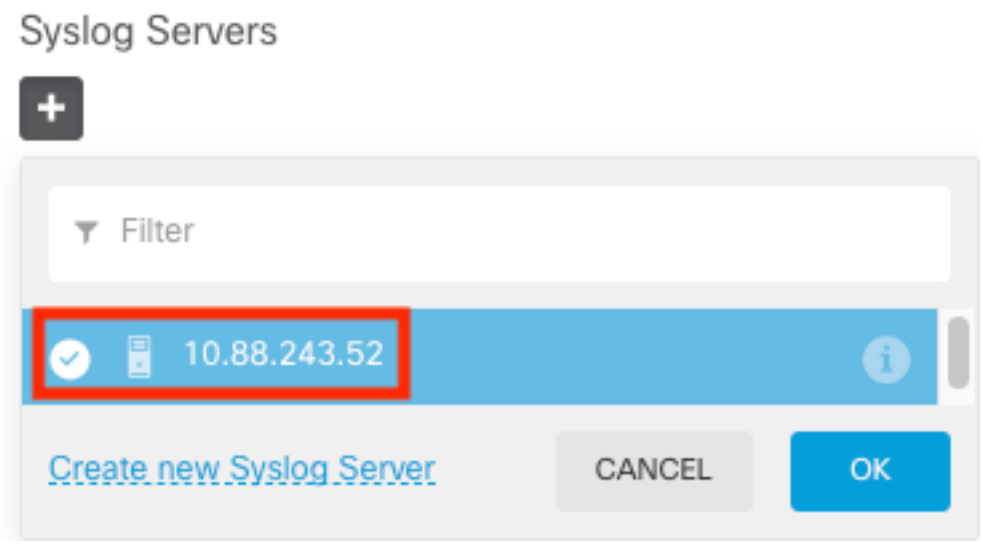
ステップ 4：[Add Syslog Server]を選択します。または、[Objects] - [Syslog Servers]でSyslog Serverオブジェクトを作成することもできます。



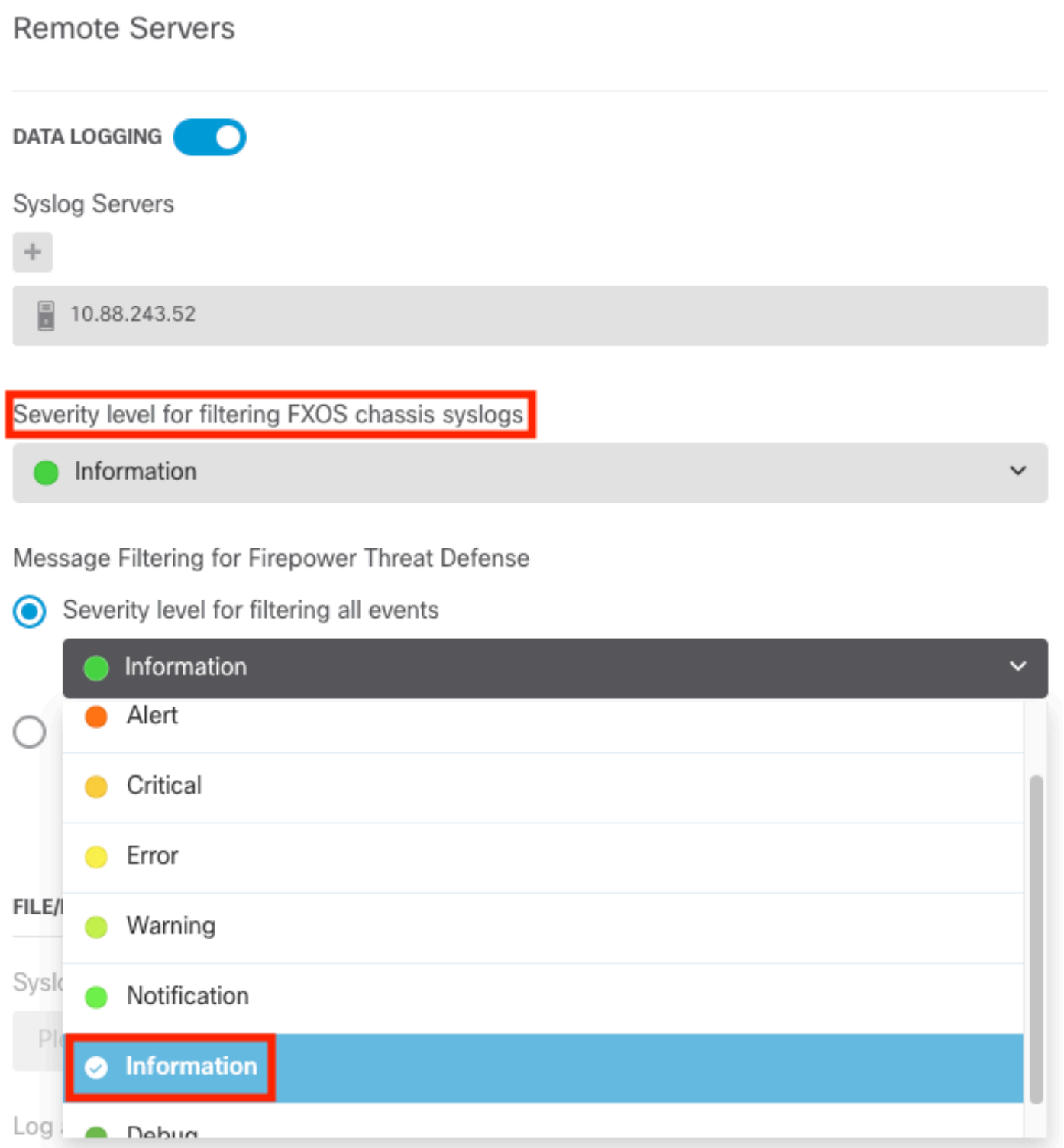
ステップ 5：SyslogサーバのIPアドレスとポート番号を入力します。Data Interfaceのオプションボタンを選択し、OKを選択します。



手順 6：次に、新しいSyslogサーバを選択し、[OK]を選択します。

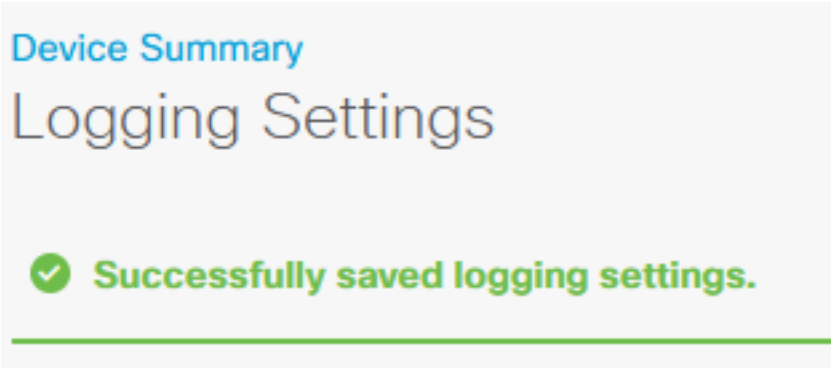


手順 7：[Severity level for filtering all events]オプションボタンを選択し、必要なログレベルを選択します。



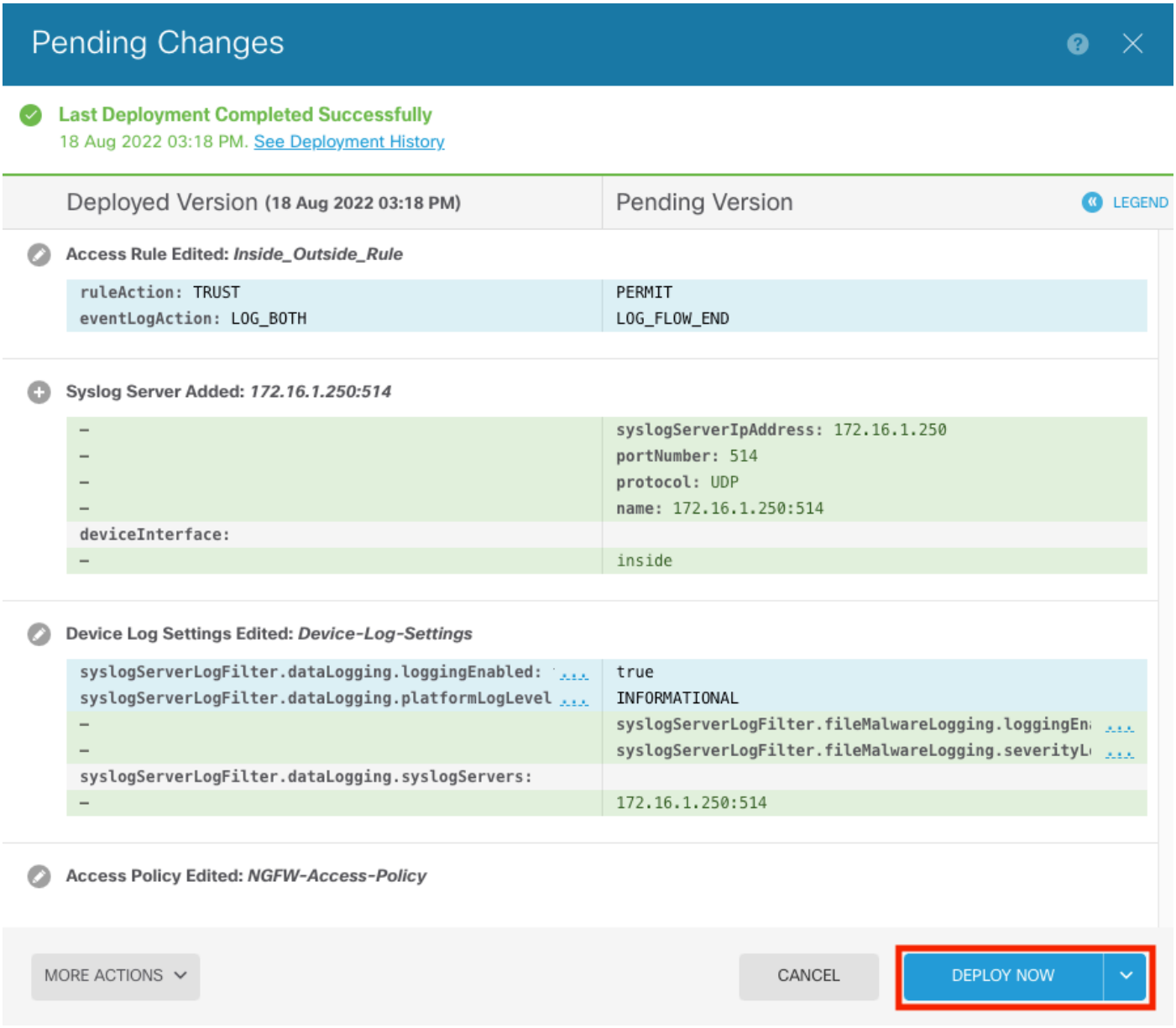
ステップ 8：画面の下部にある[Save]を選択します。

ステップ 9：設定が正常に行われたことを確認します。



ステップ 10：新しい設定を展開します。

および

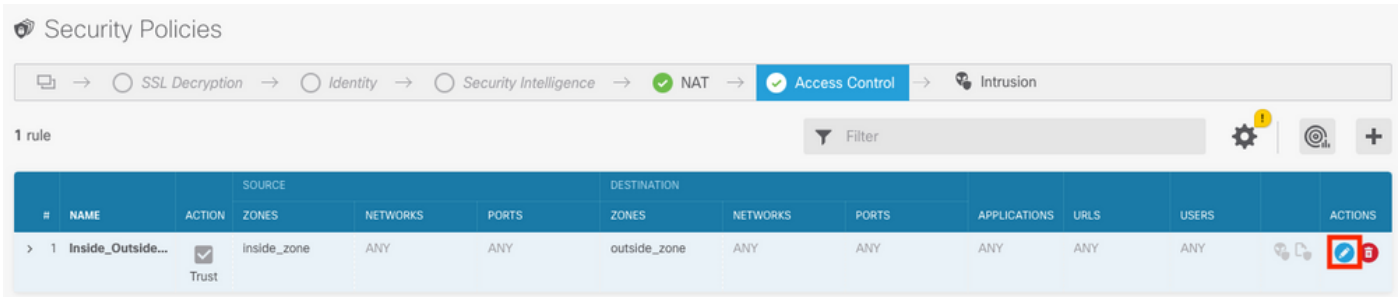


オプション。

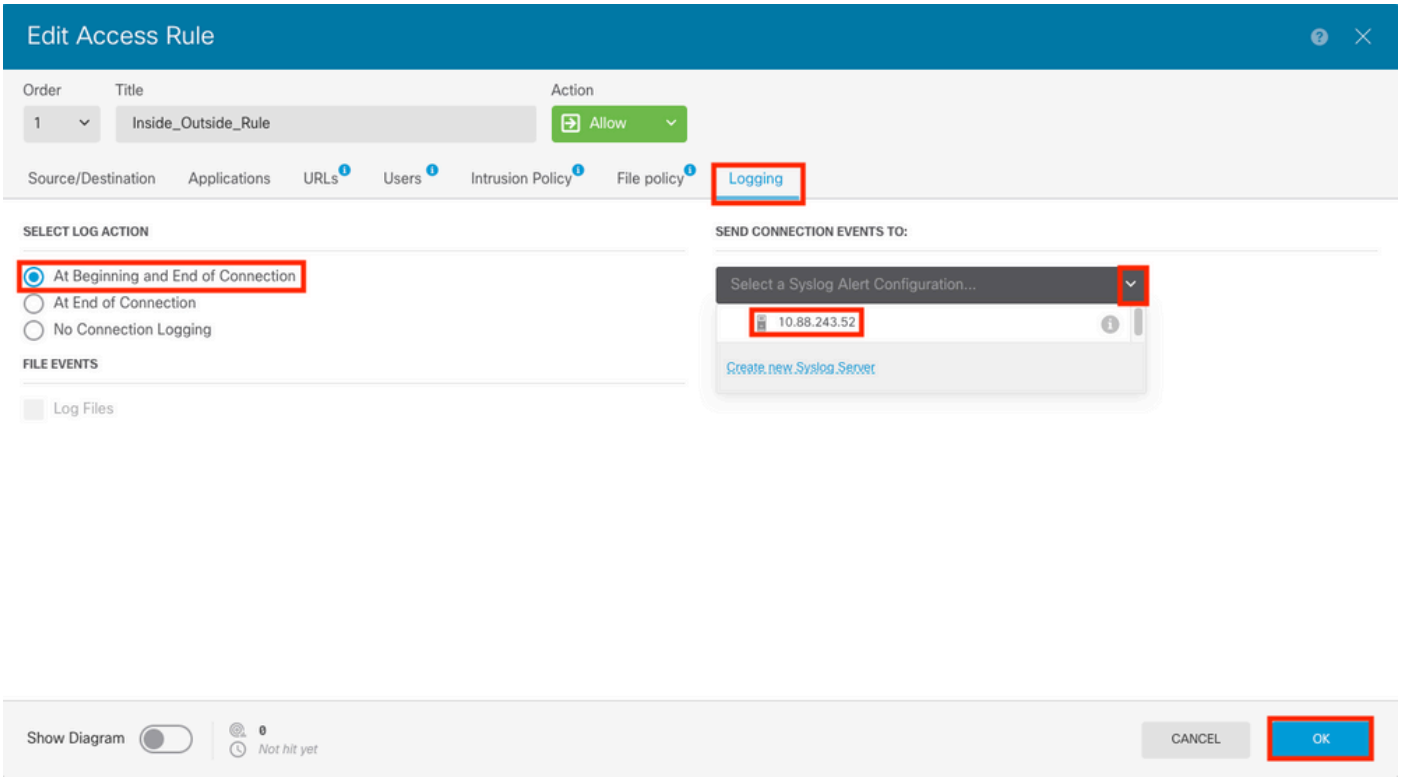
さらに、Syslogサーバにログインするようにアクセスコントロールポリシーのアクセスコントロールルールを設定できます。

ステップ 1：画面上部の[Policies]ボタンをクリックします。

ステップ 2： ACPルールの右側にマウスを移動して、ロギングを追加し、鉛筆アイコンを選択します。



ステップ 3：[Logging]タブを選択し、[At End of Connection]のオプションボタンを選択し、[Select a Syslog Alert Configuration]の下のドロップダウン矢印を選択し、Syslogサーバでを選択して、[OK]を選択します。



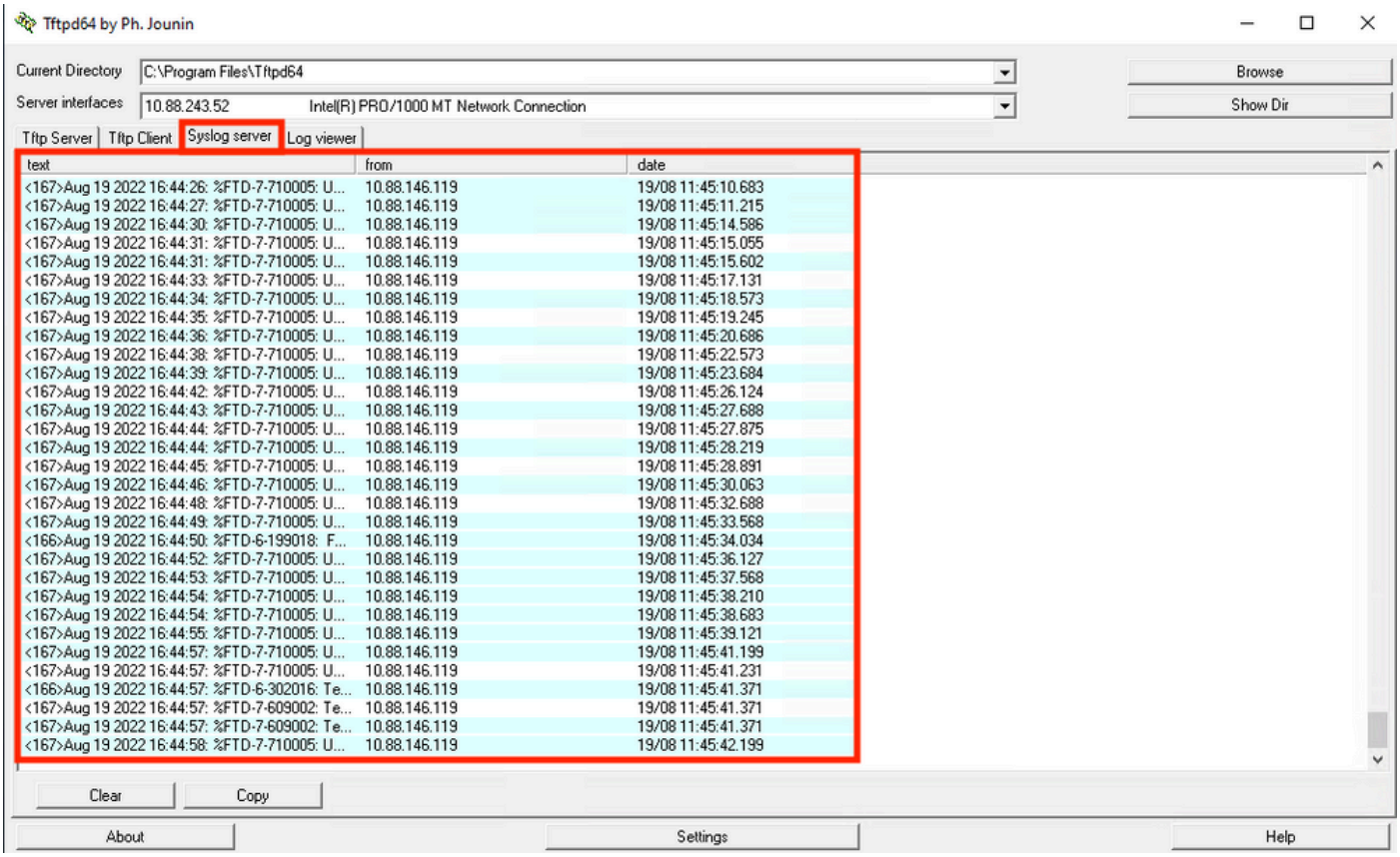
ステップ 4：設定の変更を導入します。

確認

ステップ 1：タスクが完了したら、show running-config loggingコマンドを使用して、FTD CLIのクリックモードの設定を確認できます。

```
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
>
```

ステップ 2：Syslogサーバに移動し、SyslogサーバアプリケーションがSyslogメッセージを受け入れていることを確認します。



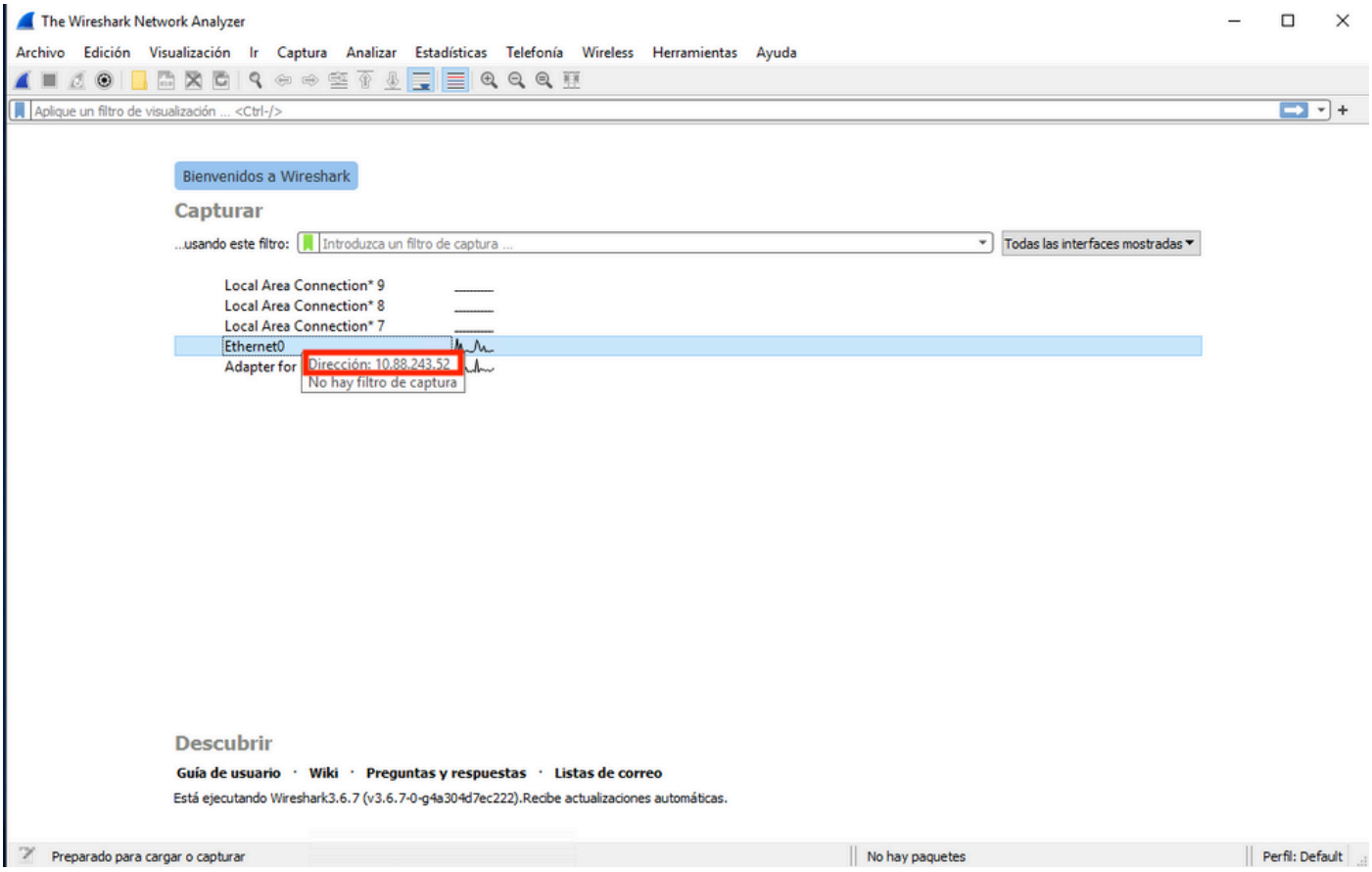
トラブルシュート

ステップ 1：SyslogアプリケーションのSyslogメッセージで何らかのメッセージが生成された場合は、FTD CLIからパケットキャプチャを実行してパケットを確認します。clishプロンプトで**system support diagnostic-cli**コマンドを入力して、ClishモードからLINAに変更します。

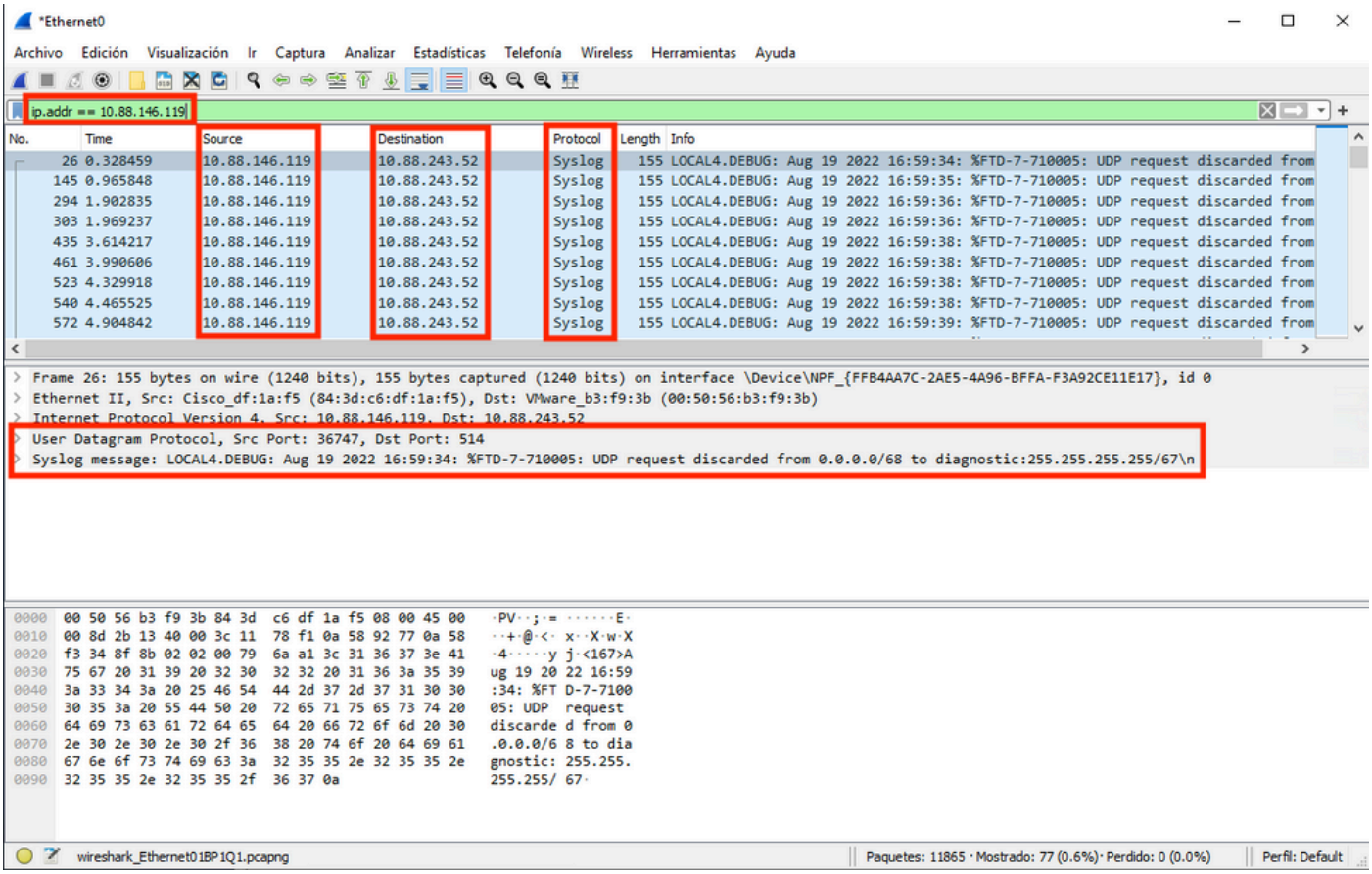
```
[> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

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

ステップ 2：udp 514（tcpを使用している場合はtcp 1468）用に1つのパケットキャプチャを作成します

ステップ 3：通信がSyslogサーバのネットワークインターフェイスカード(NIC)に到達していることを確認します。ロードされたWiresharkまたは別のパケットキャプチャユーティリティを使用します。SyslogサーバのWiresharkのインターフェイスをダブルクリックして、パケットのキャプチャを開始します。



ステップ 4：udp.port==514と入力し、バーの右側にある矢印を選択して、udp 514の上部バーに表示フィルタを設定します。出力から、パケットがSyslogサーバに送信されているかどうかを確認します。



ステップ 5：Syslogサーバアプリケーションにデータが表示されない場合は、Syslogサーバアプリケーション内の設定をトラブルシューティングします。正しいプロトコルがudp/tcpと正しいポート514/1468で使用されていることを確認します。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。