تكوين syslog والتحقق من صحته في FirePOWER Device Manager

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين syslog داخل FirePOWER Device Manager (FDM).

المتطلبات الأساسية

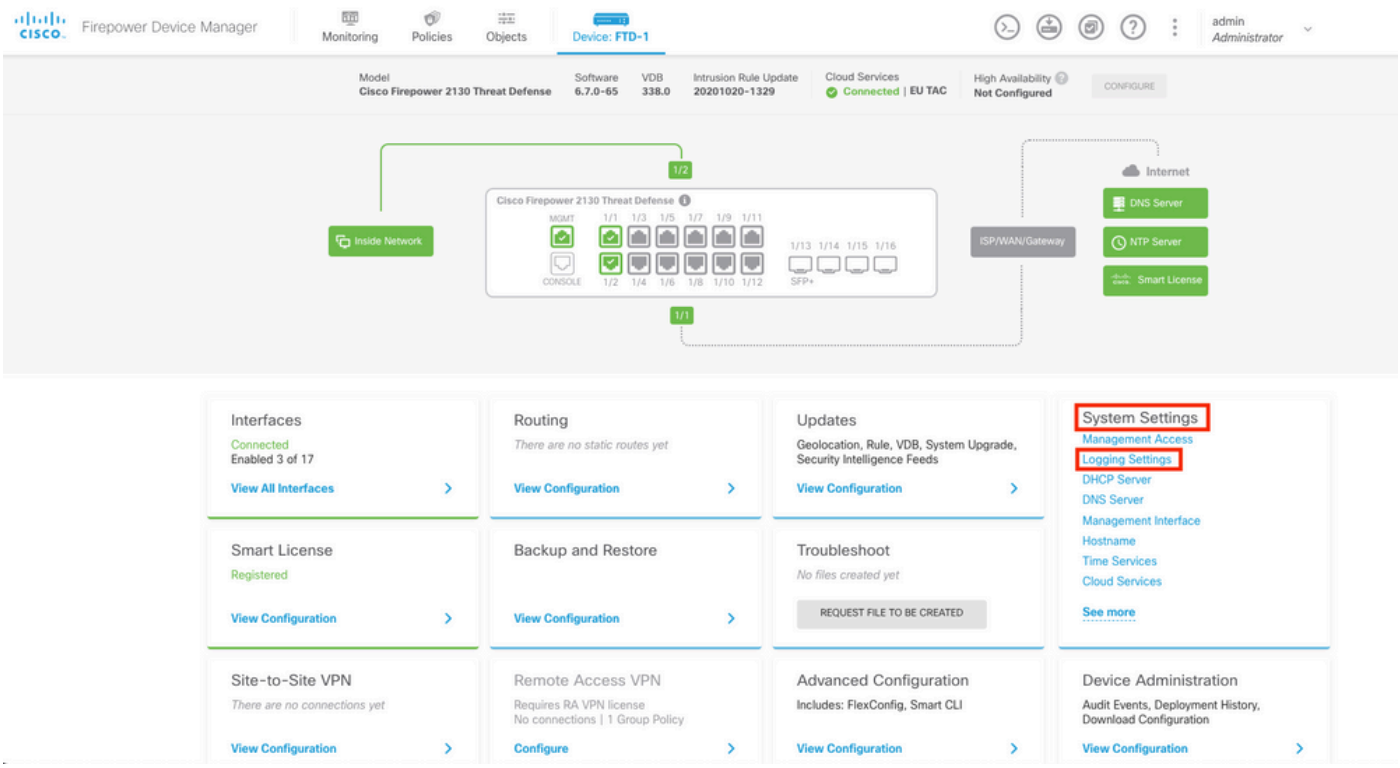
المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

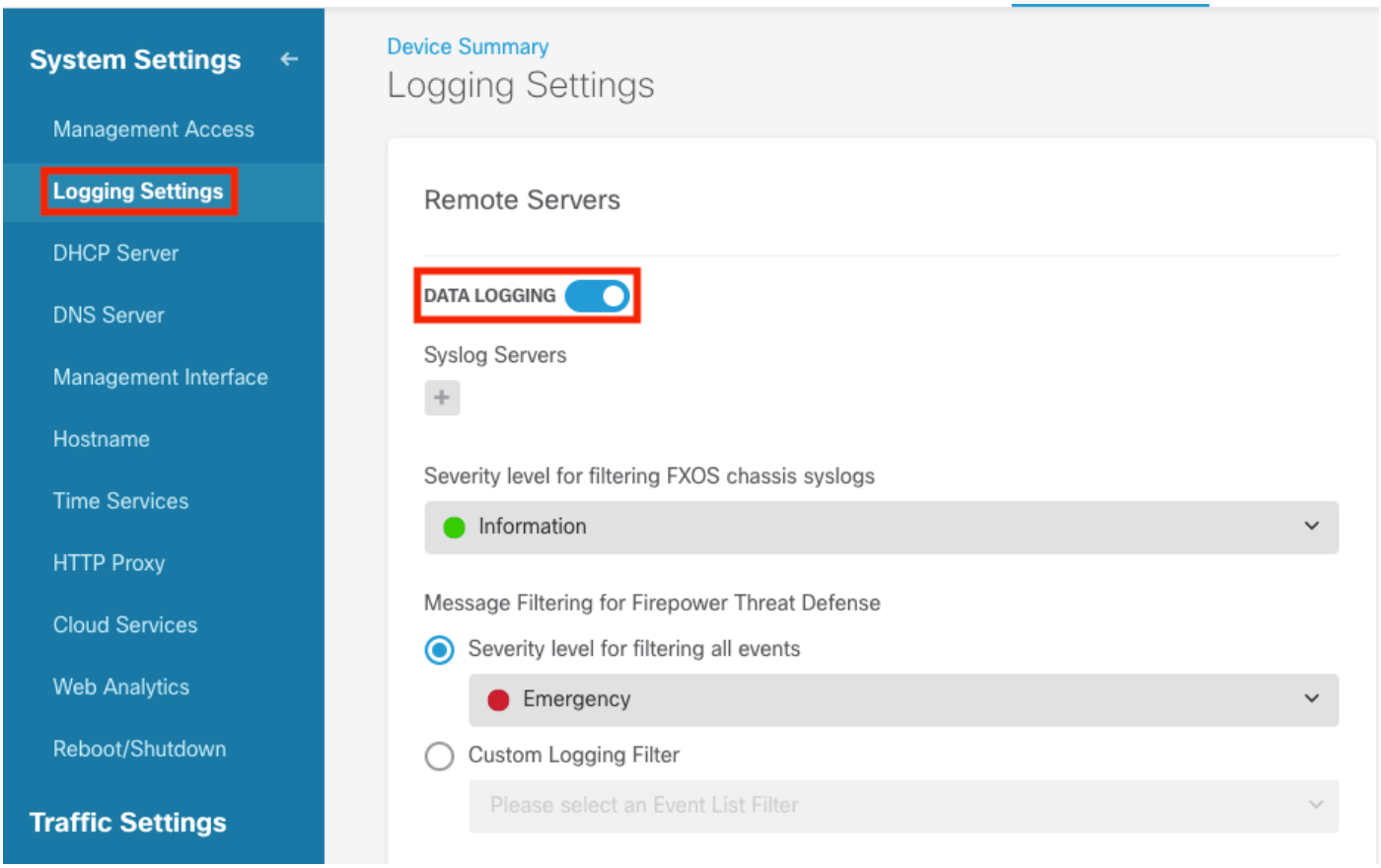
- Firepower Threat Defense
- Syslog Server الذي يشغل برنامج syslog لجمع البيانات

التكوينات

الخطوة 1. من الشاشة الرئيسية لإدارة أجهزة FirePOWER، حدد إعدادات التسجيل أسفل إعدادات النظام في الركن السفلي الأيمن من الشاشة.

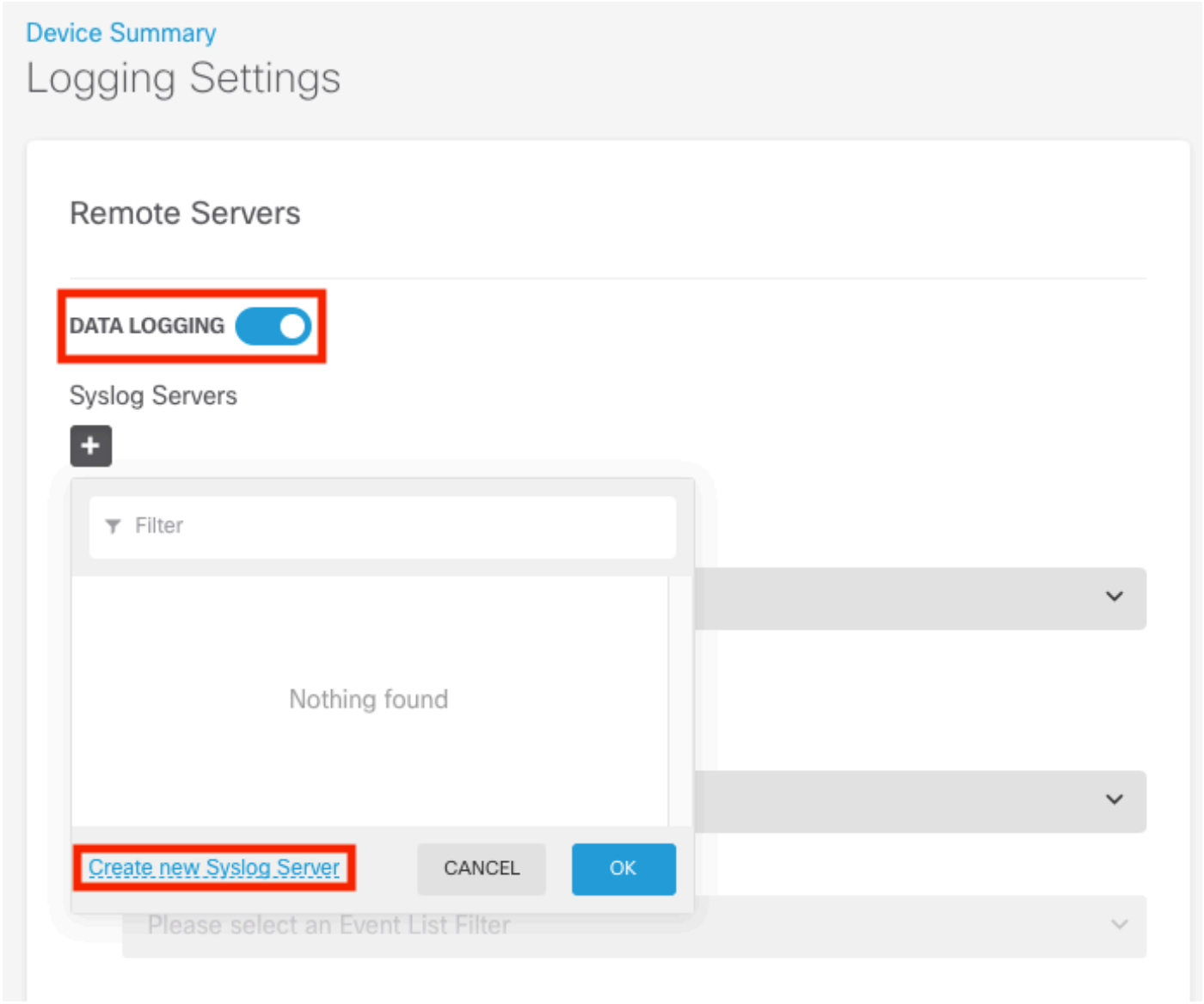


الخطوة 2. في شاشة إعدادات النظام، حدد إعدادات التسجيل في القائمة اليسرى.

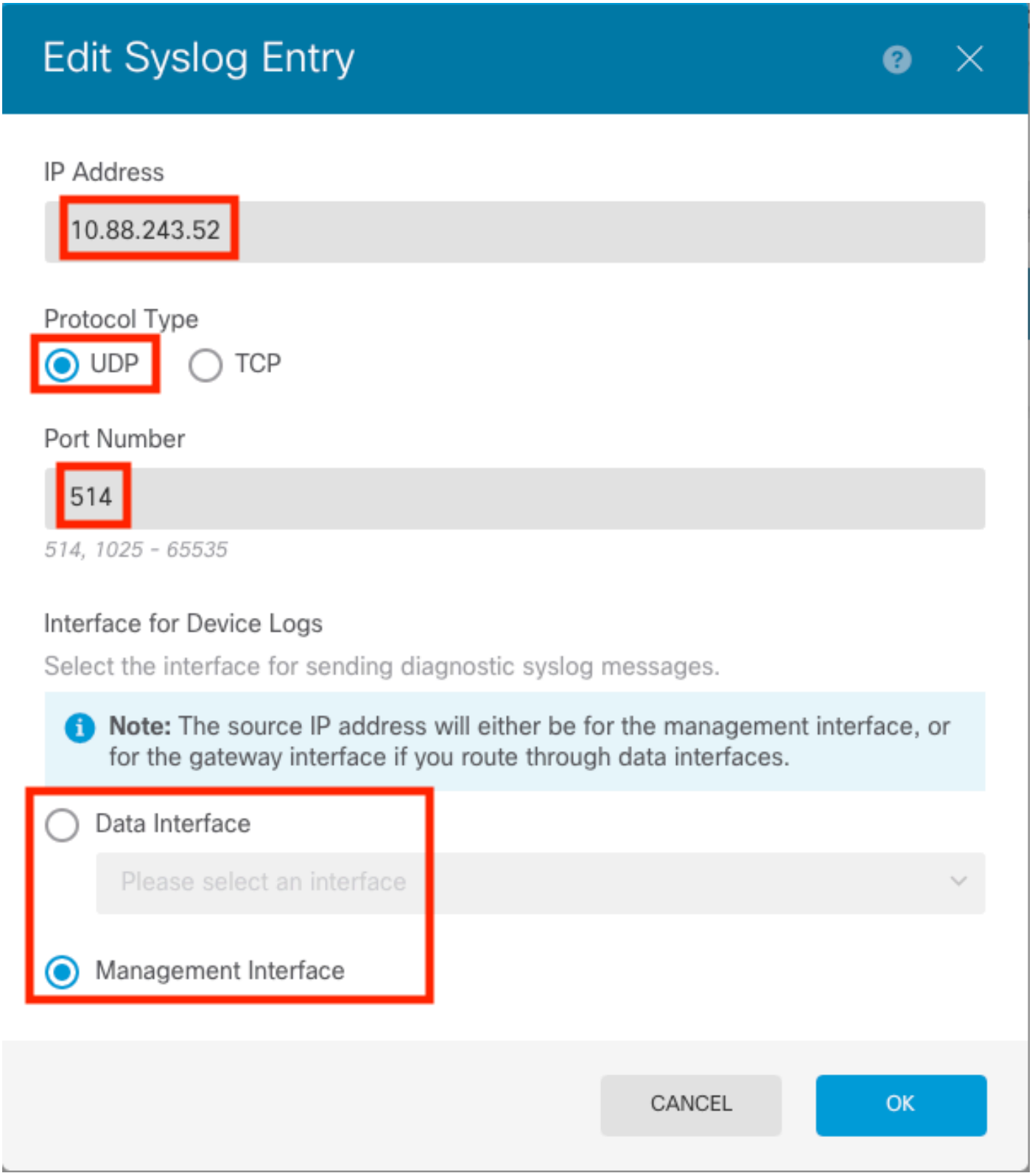


الخطوة 3. قم بتعيين المحول تبديل تسجيل البيانات من خلال تحديد علامة + أسفل خوادم Syslog.

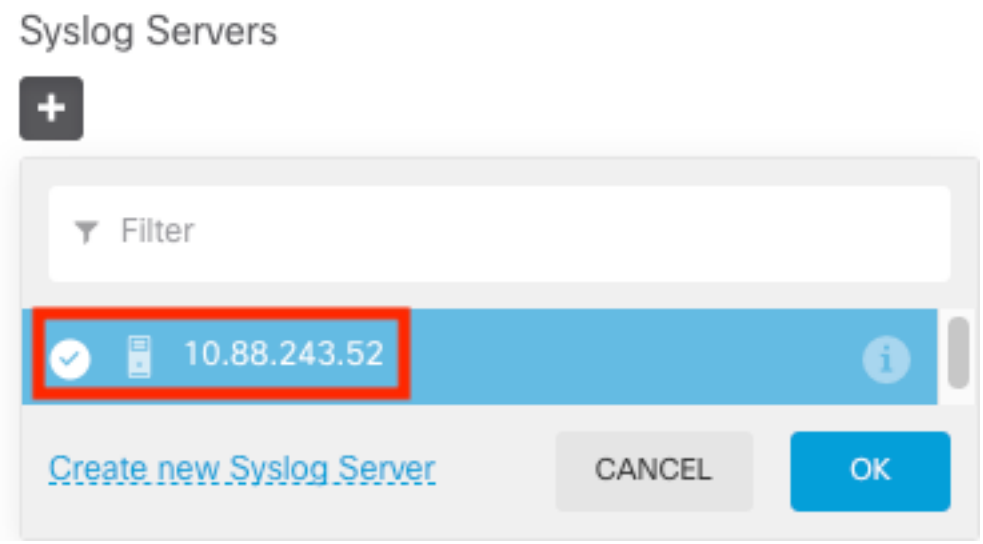
الخطوة 4. حدد إضافة خادم syslog. بدلا من ذلك، يمكنك إنشاء كائن خادم syslog في الكائنات - خوادم syslog.



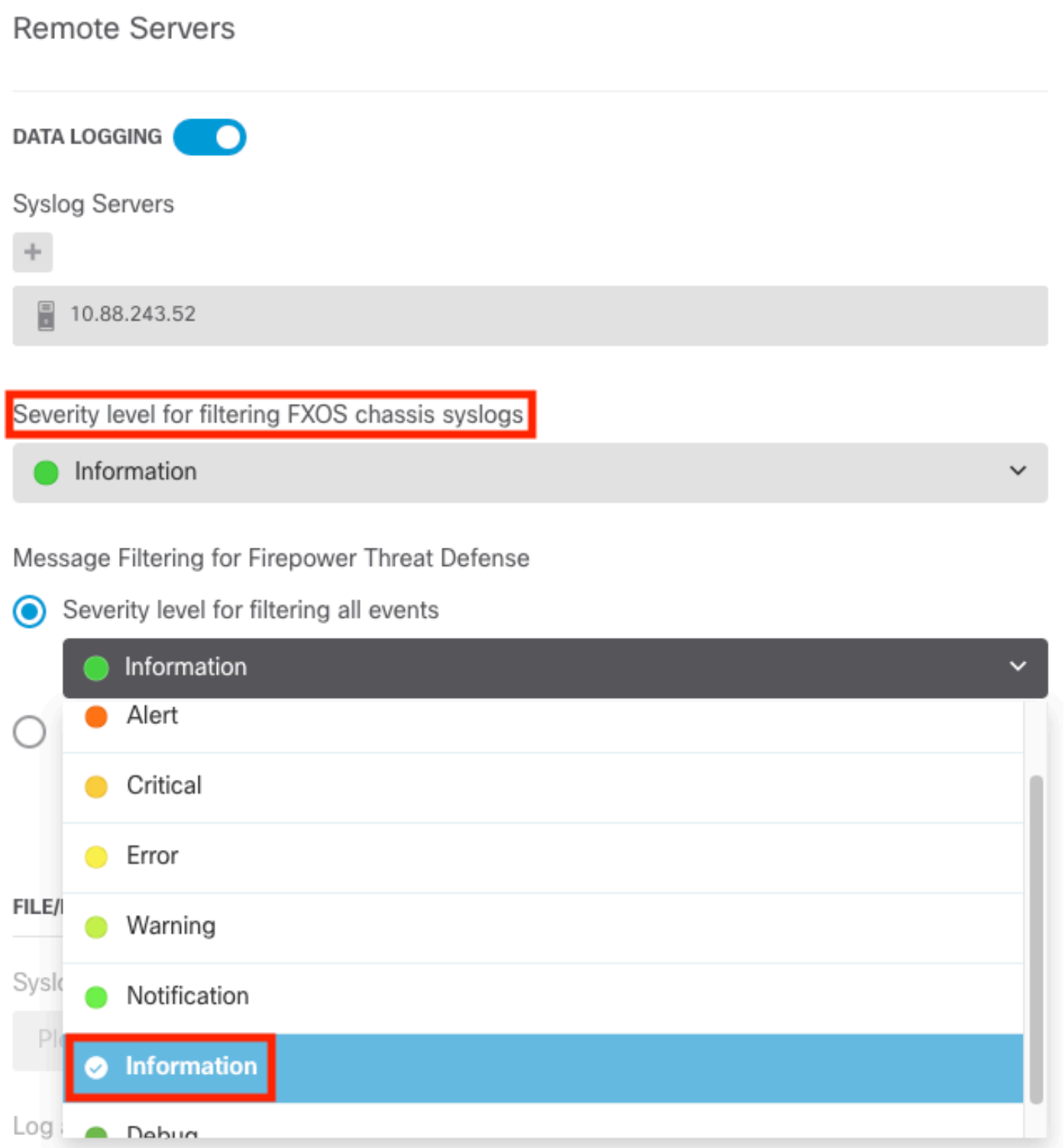
الخطوة 5. دخلت العنوان من ك syslog نادل ورقم أيسر. حدد زر الخيار لواجهة البيانات وحدد موافق.



الخطوة 6. بعد ذلك، حدد خادم syslog الجديد وحدد موافق.

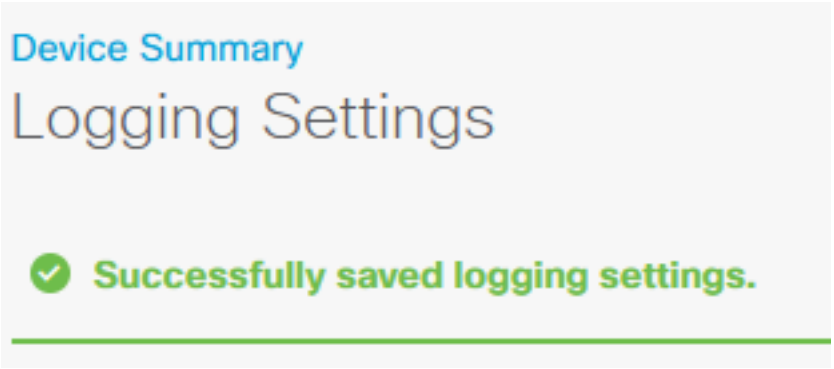


الخطوة 7. حدد مستوى الخطورة لتصفية كل الأحداث الراديو، وحدد مستوى التسجيل الذي تريده.



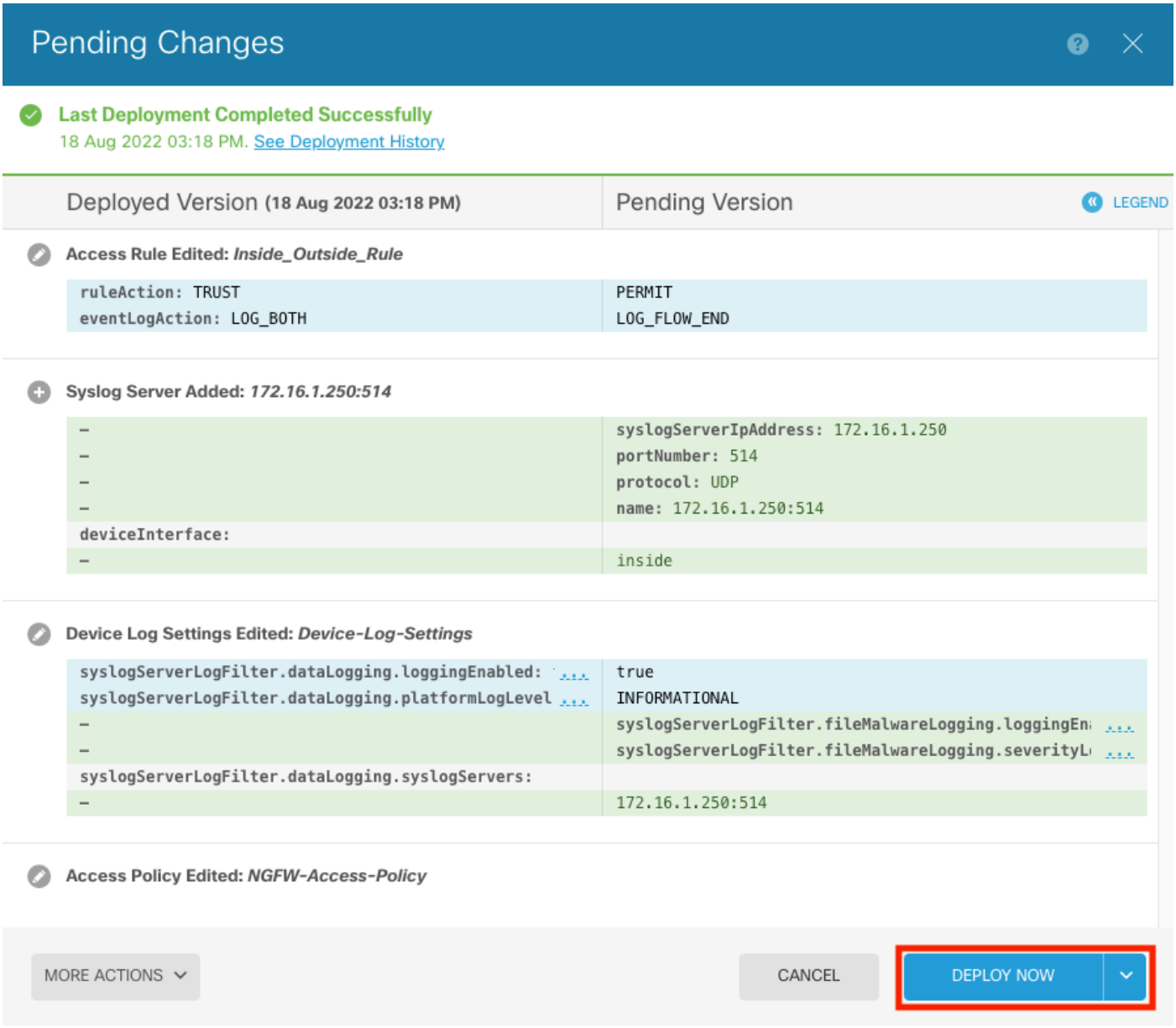
الخطوة 8. حدد حفظ في أسفل الشاشة.

الخطوة 9. تحقق من نجاح الإعدادات.



الخطوة 10. نشر الإعدادات الجديدة.

و

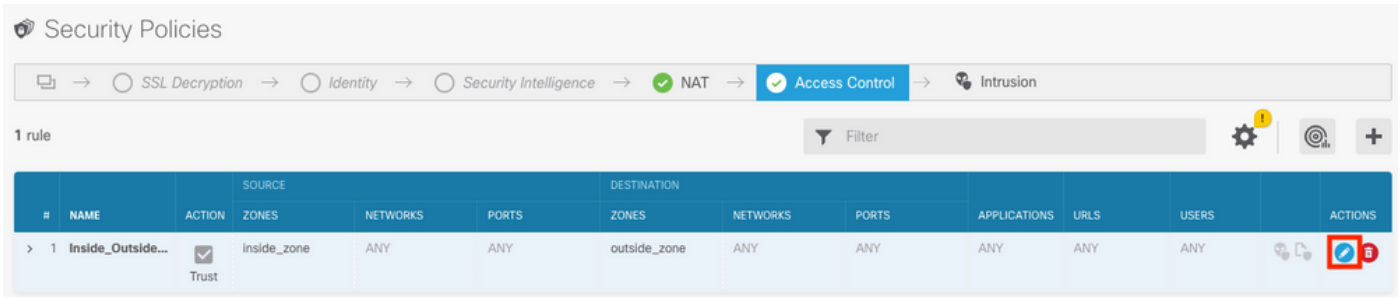


اختياري.

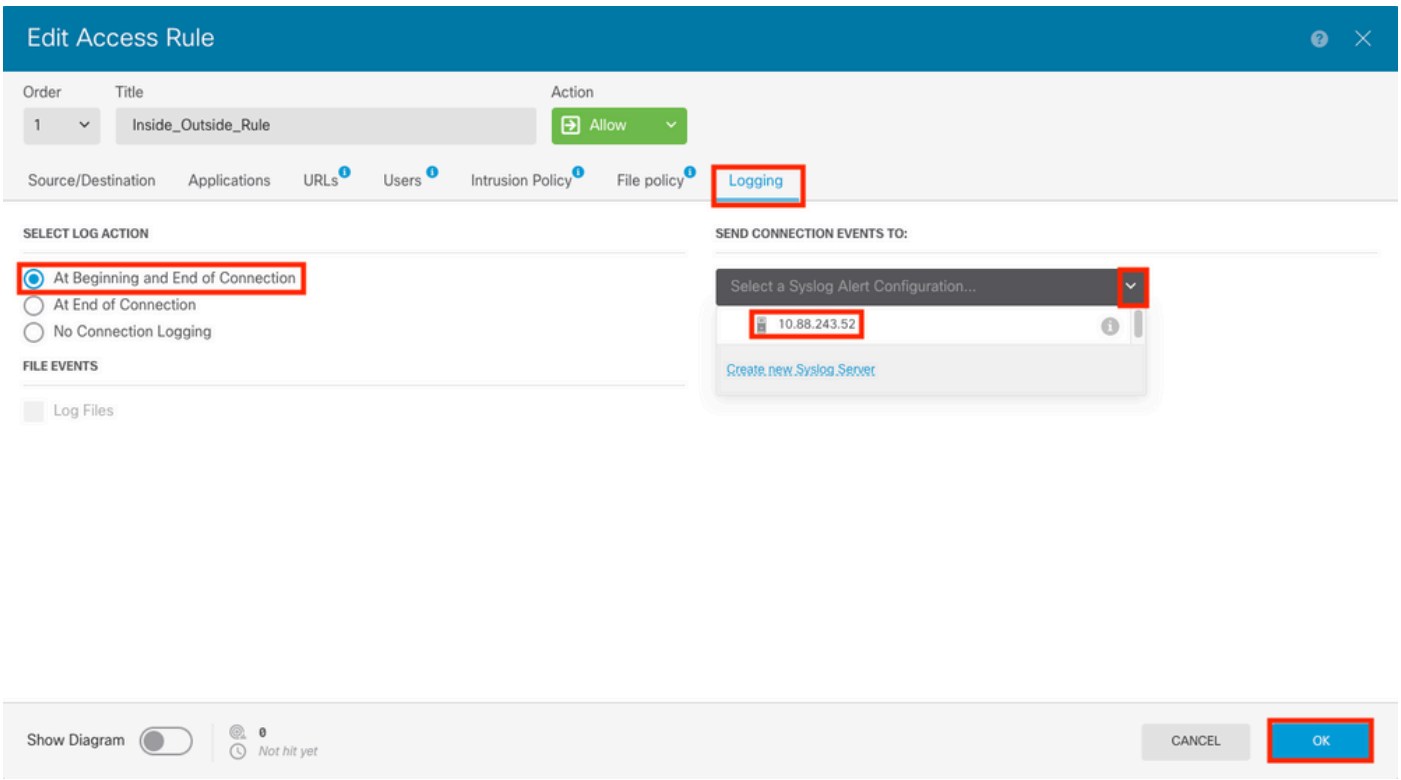
بالإضافة إلى ذلك، يمكن تعيين قواعد التحكم في الوصول لنهج التحكم في الوصول لتسجيل الدخول إلى خادم syslog:

الخطوة 1. انقر فوق الزر سياسات في أعلى الشاشة.

الخطوة 2. قم بالمرور فوق الجانب الأيمن من قاعدة ACP لإضافة تسجيل وتحديد أيقونة القلم الرصاص.



الخطوة 3. حدد علامة التبويب تسجيل، حدد زر الخيار ل عند نهاية الاتصال، حدد السهم المنسدل تحت تحديد تكوين تنبيه Syslog، حدد على خادم Syslog وحدد موافق.



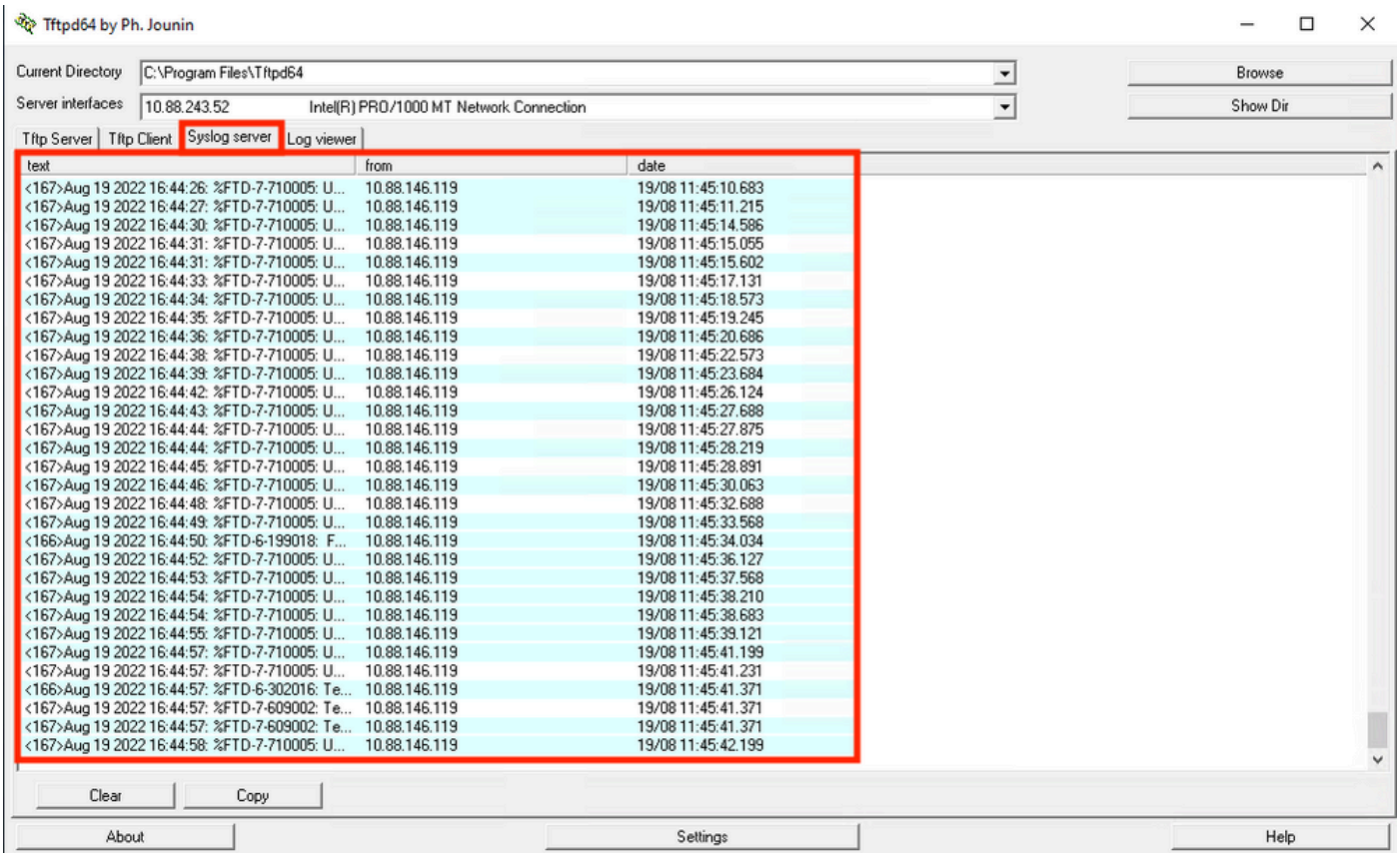
الخطوة 4. قم بنشر تغييرات التكوين.

التحقق من الصحة

الخطوة 1. بعد اكتمال المهمة، يمكنك التحقق من الإعدادات في وضع واجهة سطر الأوامر (CLI) ل FTD باستخدام الأمر 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
>
```

الخطوة 2. انتقل إلى خادم Syslog وتحقق من قبول تطبيق خادم Syslog لرسائل Syslog.



استكشاف الأخطاء وإصلاحها

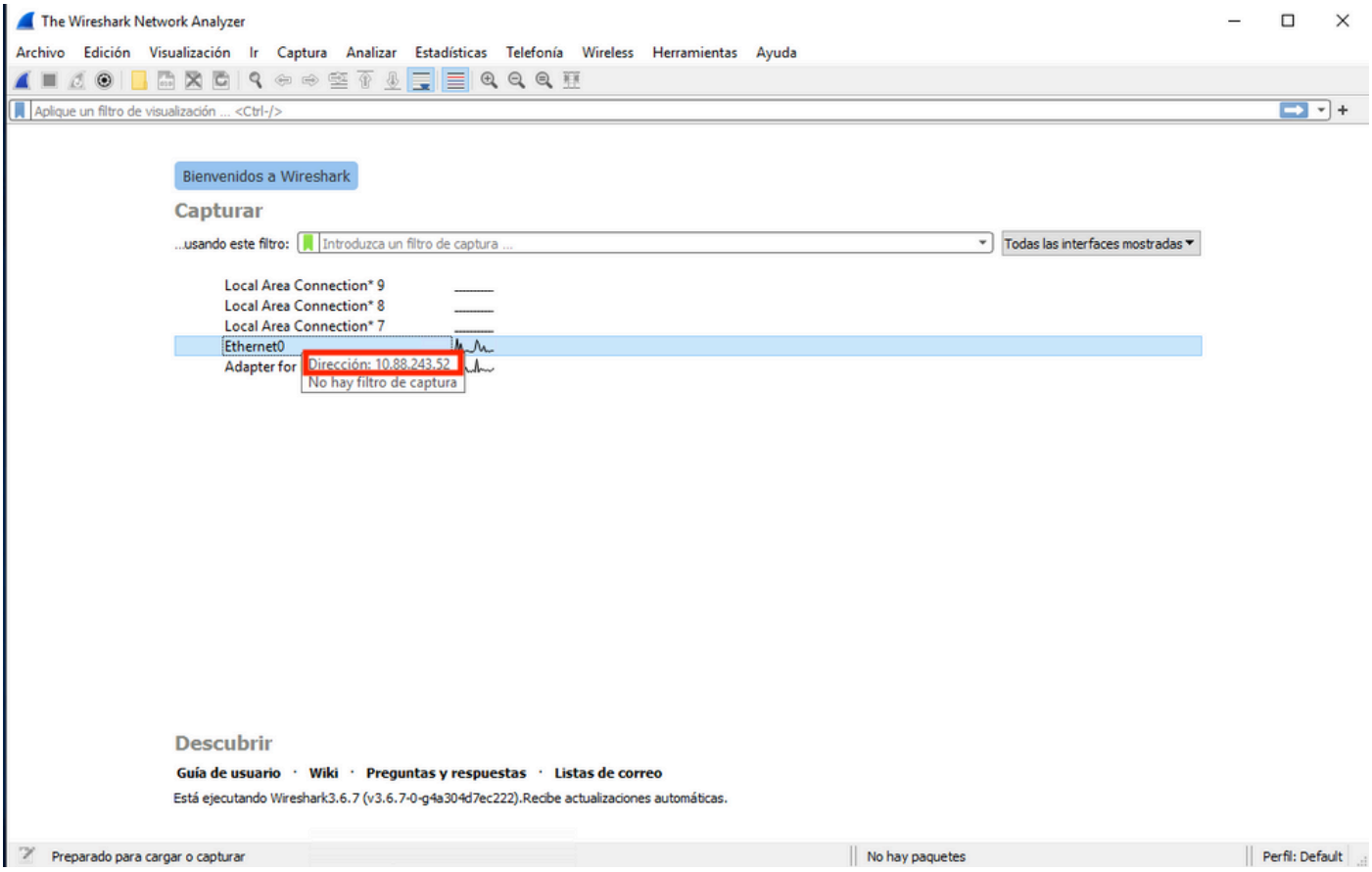
الخطوة 1. إن ينتج ال syslog رسالة على ال syslog تطبيق أي رسالة، أنجزت ربط التقاط من

ال FTD CLI أن يفحص للحزم. قم بالتغيير من وضع Clish إلى LINA من خلال إدخال الأمر **system support diagnostic-cli** في موجه الأمر Clish.

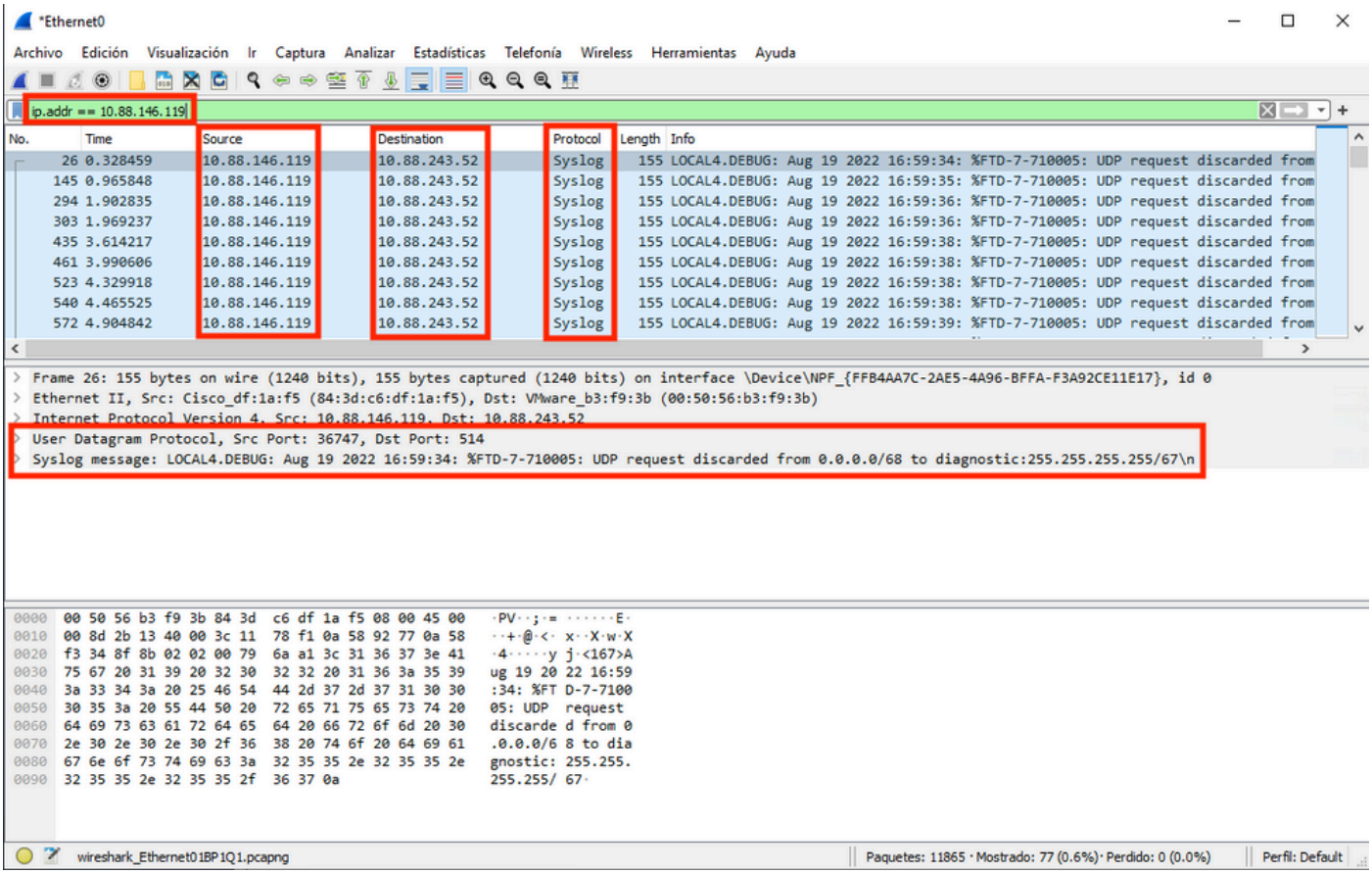
```
[> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

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

الخطوة 2. قم بإنشاء التقاط حزمة واحد ل UDP 514 (أو TCP 1468 إذا كنت تستخدم TCP)

الخطوة 3. تحقق من أن الاتصال يقوم بإرساله إلى بطاقة واجهة الشبكة على خادم syslog. أستخدم Wireshark أو أداة مساعدة أخرى لالتقاط الحزم محملة. انقر نقرا مزدوجا على الواجهة في Wireshark لخادم Syslog لبدء التقاط الحزم.



الخطوة 4. اضبط مرشح عرض في الشريط العلوي ل UDP 514 بالكتابة udp.port==514 وتحديد السهم على يمين الشريط. من الإنتاج، أكدت إن يكون الربط يجعله إلى ال syslog نادل.



الخطوة 5. إذا لم يكن تطبيق Syslog Server يعرض البيانات، فقم باستكشاف الأخطاء وإصلاحها داخل تطبيق Syslog Server. تأكد من إستخدام البروتوكول الصحيح udp/tcp والمنفذ الصحيح 514/1468.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).