Configuration et vérification de Syslog dans le Gestionnaire de périphériques Firepower

Table des matières

Introduction

Ce document décrit comment configurer Syslog dans Firepower Device Manager (FDM).

Conditions préalables

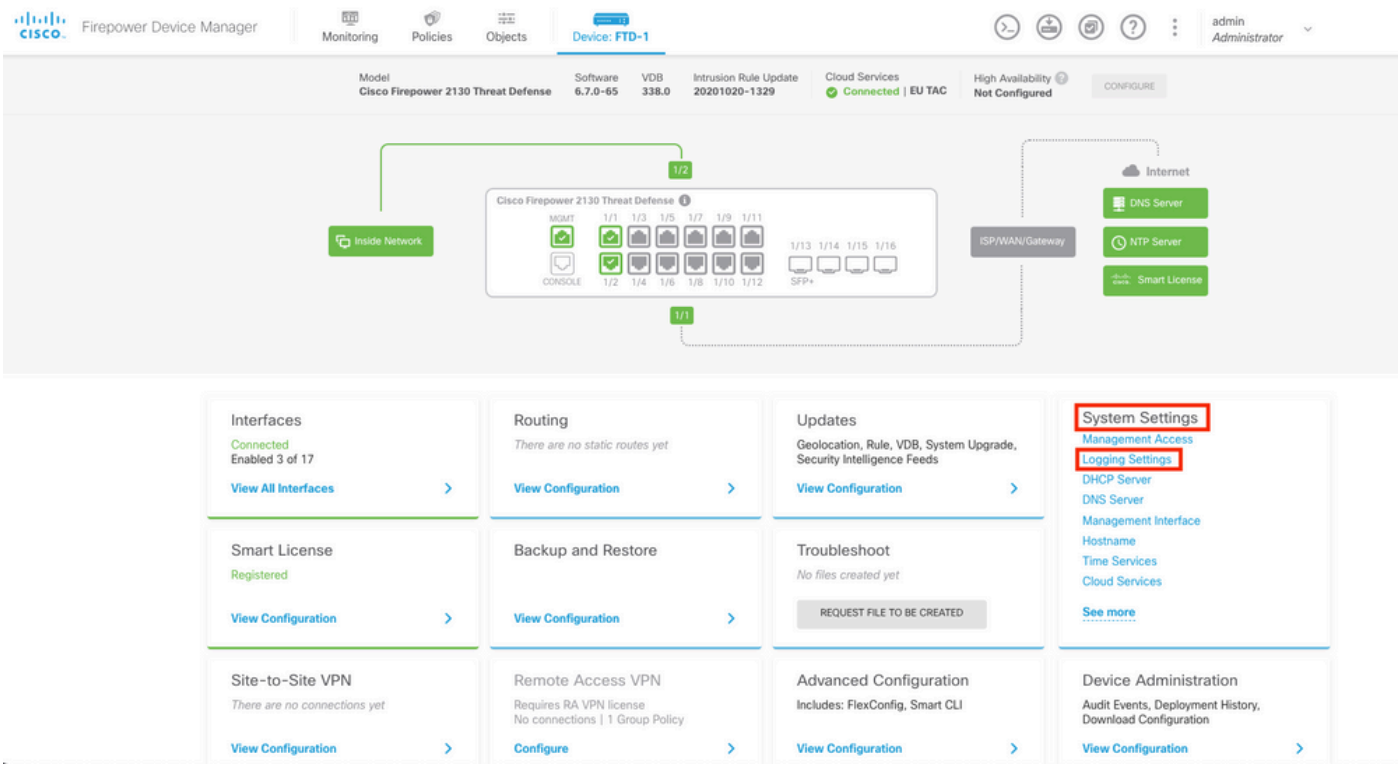
Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

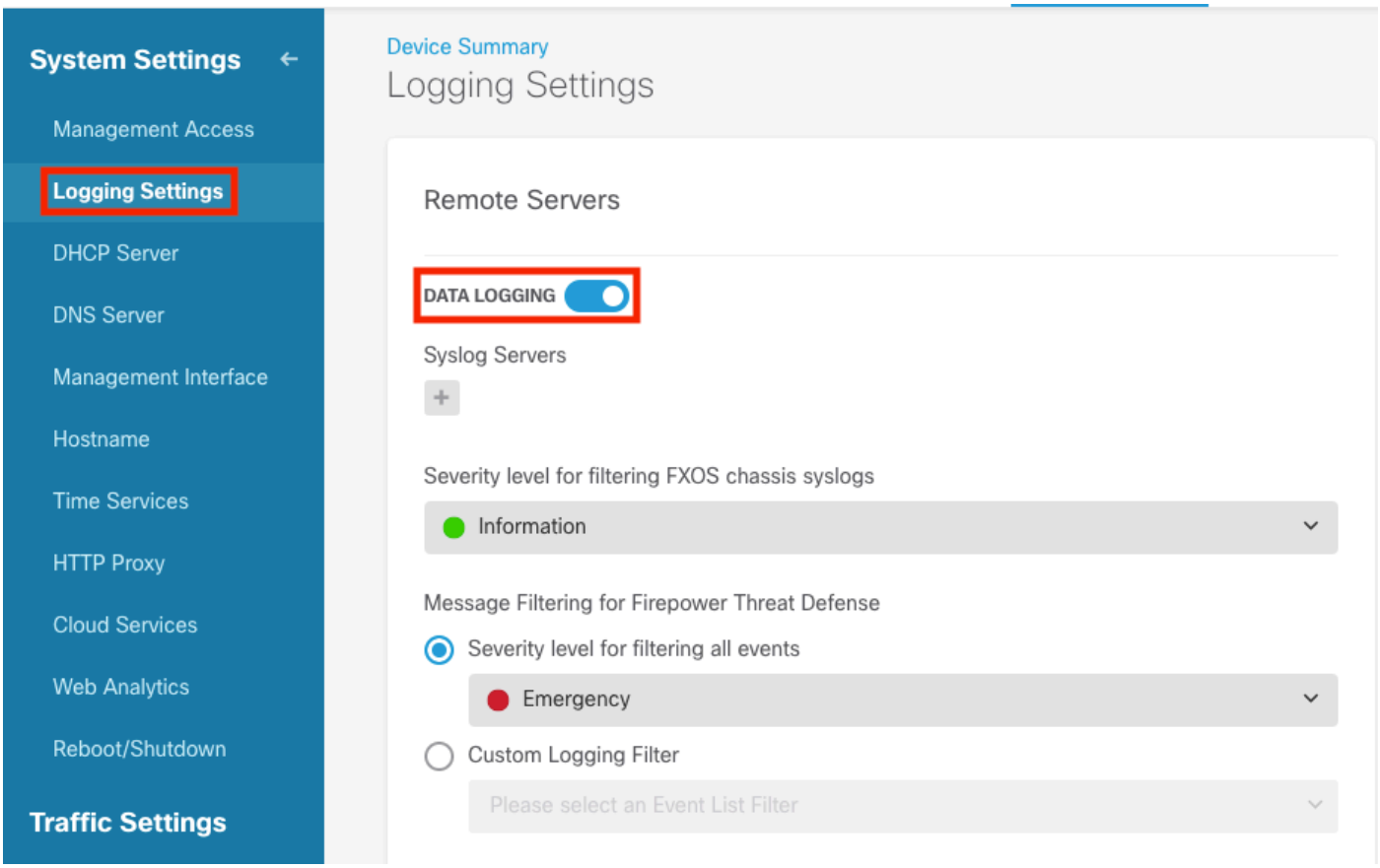
- Firepower Threat Defense
- Serveur Syslog exécutant le logiciel Syslog pour collecter des données

Configurations

Étape 1. Dans l'écran Main Firepower Device Manager (Gestionnaire principal de périphériques Firepower), sélectionnez Logging Settings (Paramètres de journalisation) sous System Settings (Paramètres système) dans le coin inférieur droit de l'écran.



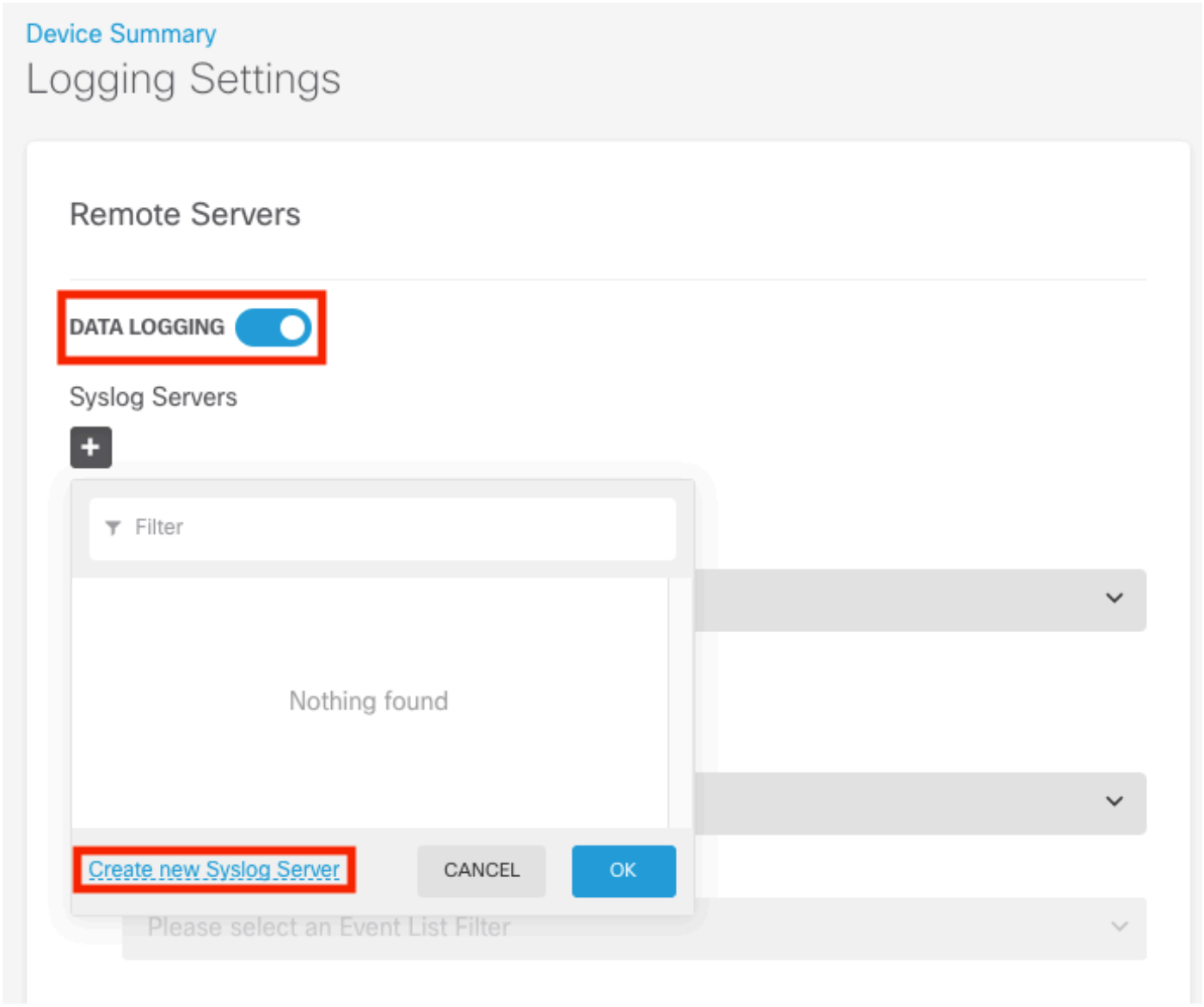
Étape 2. Dans l'écran System Settings (Paramètres système), sélectionnez Logging Settings (Paramètres de journalisation) dans le menu de gauche.



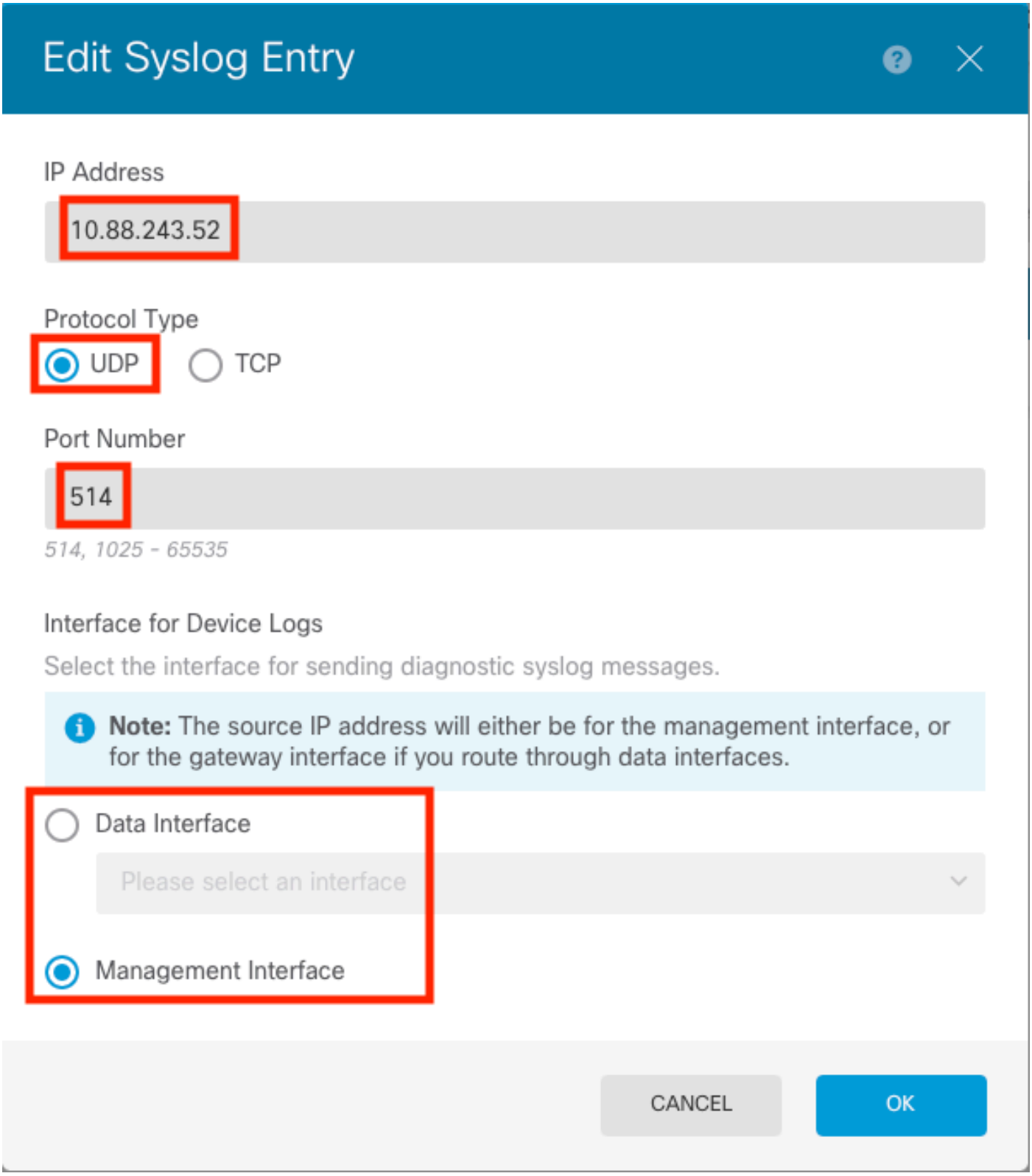
Étape 3. Définissez le commutateur à bascule Journalisation des données en sélectionnant le signe + sous Serveurs Syslog.

Étape 4. Sélectionnez Ajouter un serveur Syslog. Vous pouvez également créer l'objet Serveur

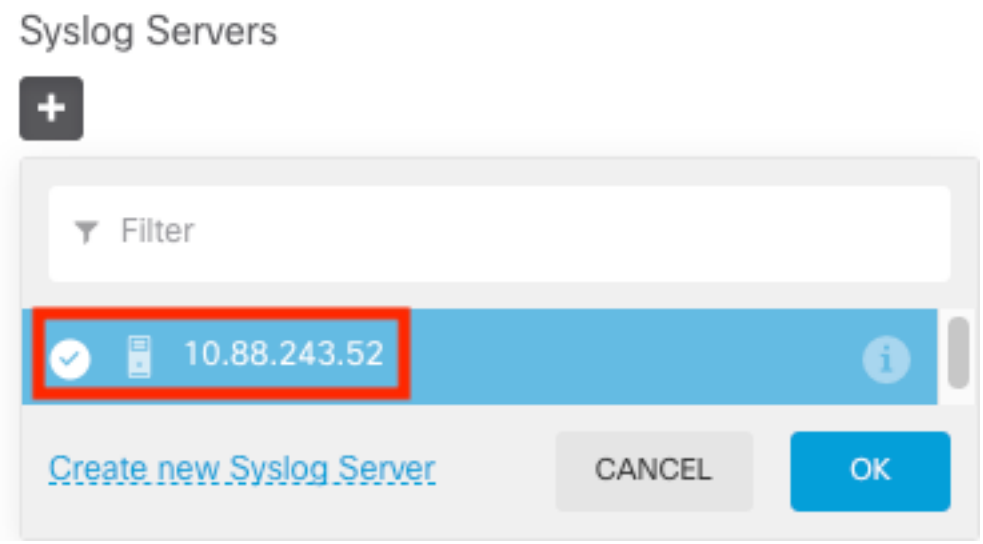
Syslog dans Objets - Serveurs Syslog.



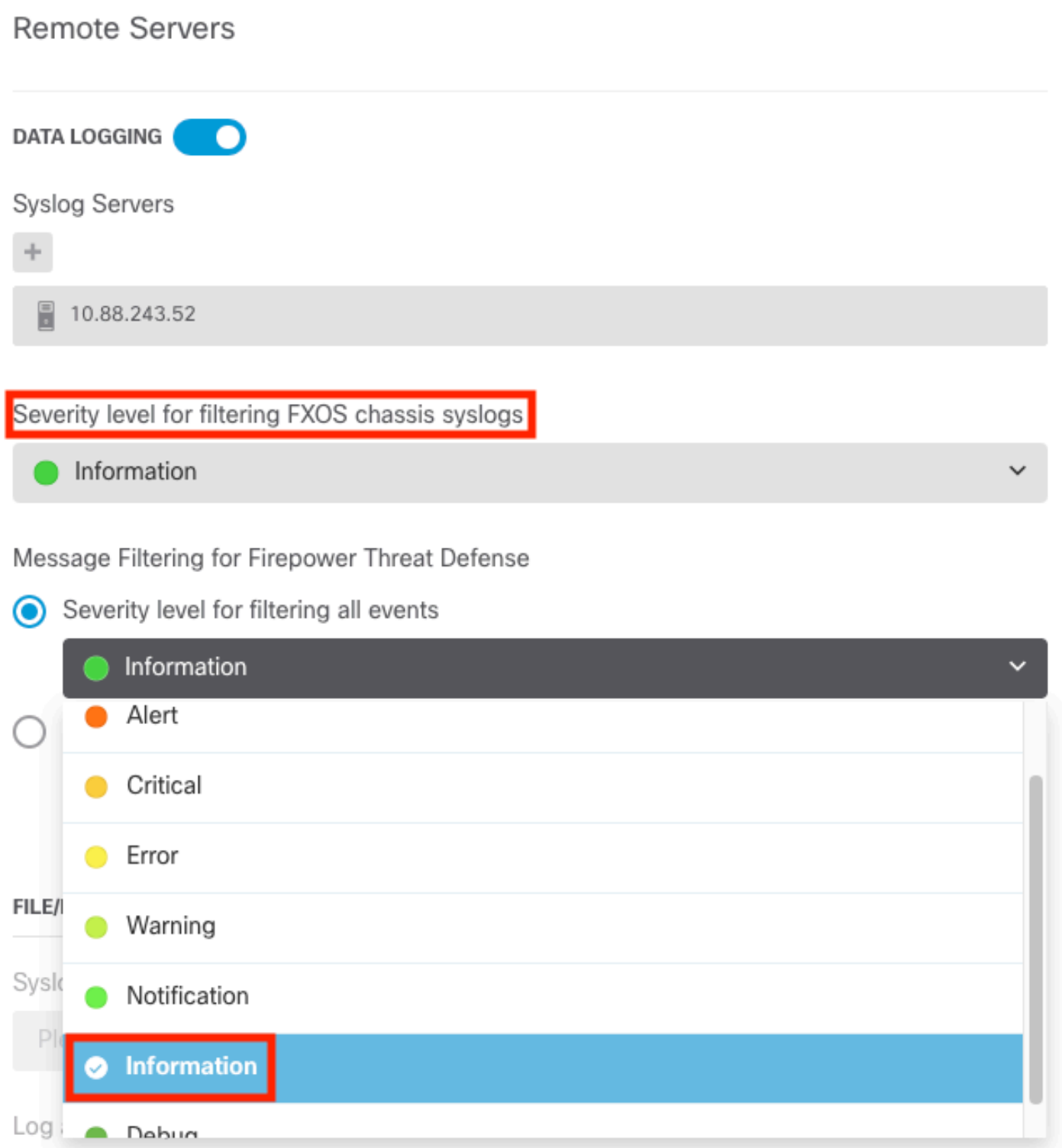
Étape 5. Saisissez l'adresse IP de votre serveur Syslog et le numéro de port. Sélectionnez la case d'option Interface de données, puis cliquez sur OK.



Étape 6. Sélectionnez ensuite le nouveau serveur Syslog, puis cliquez sur OK.

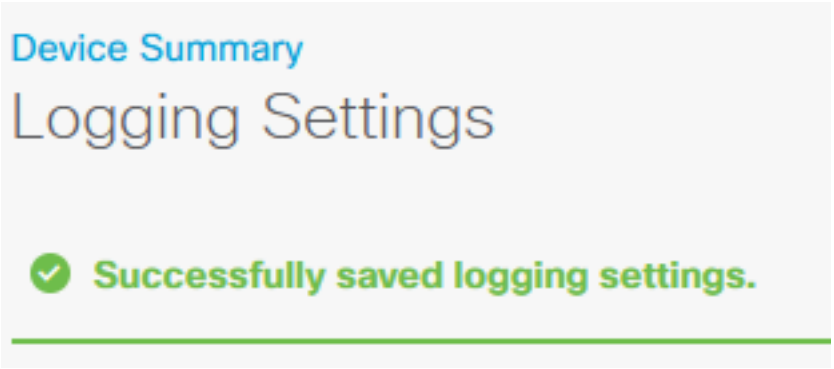


Étape 7. Sélectionnez la case d'option Niveau de gravité pour le filtrage de tous les événements et sélectionnez le niveau de journalisation souhaité.



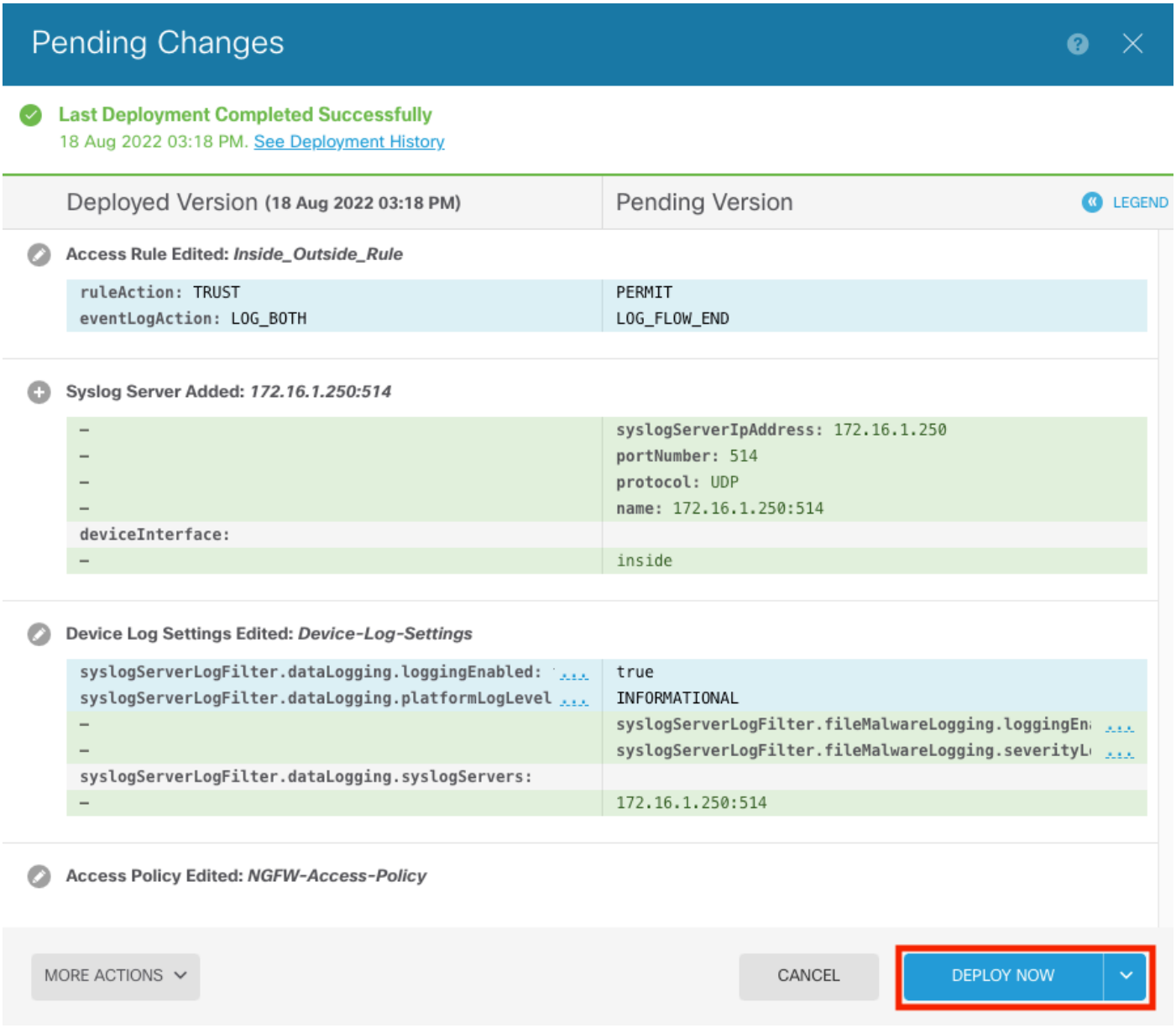
Étape 8. Sélectionnez Enregistrer en bas de l'écran.

Étape 9. Vérifiez que les paramètres ont réussi.



Étape 10. Déployez les nouveaux paramètres.

ET

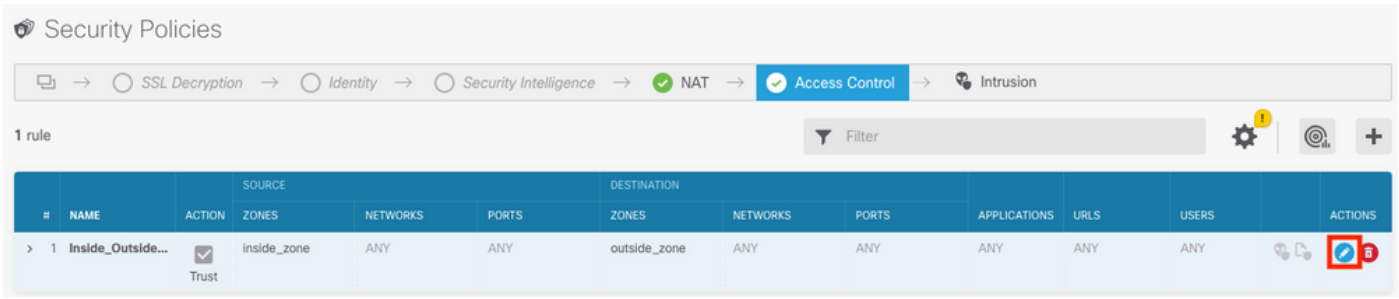


FACULTATIF.

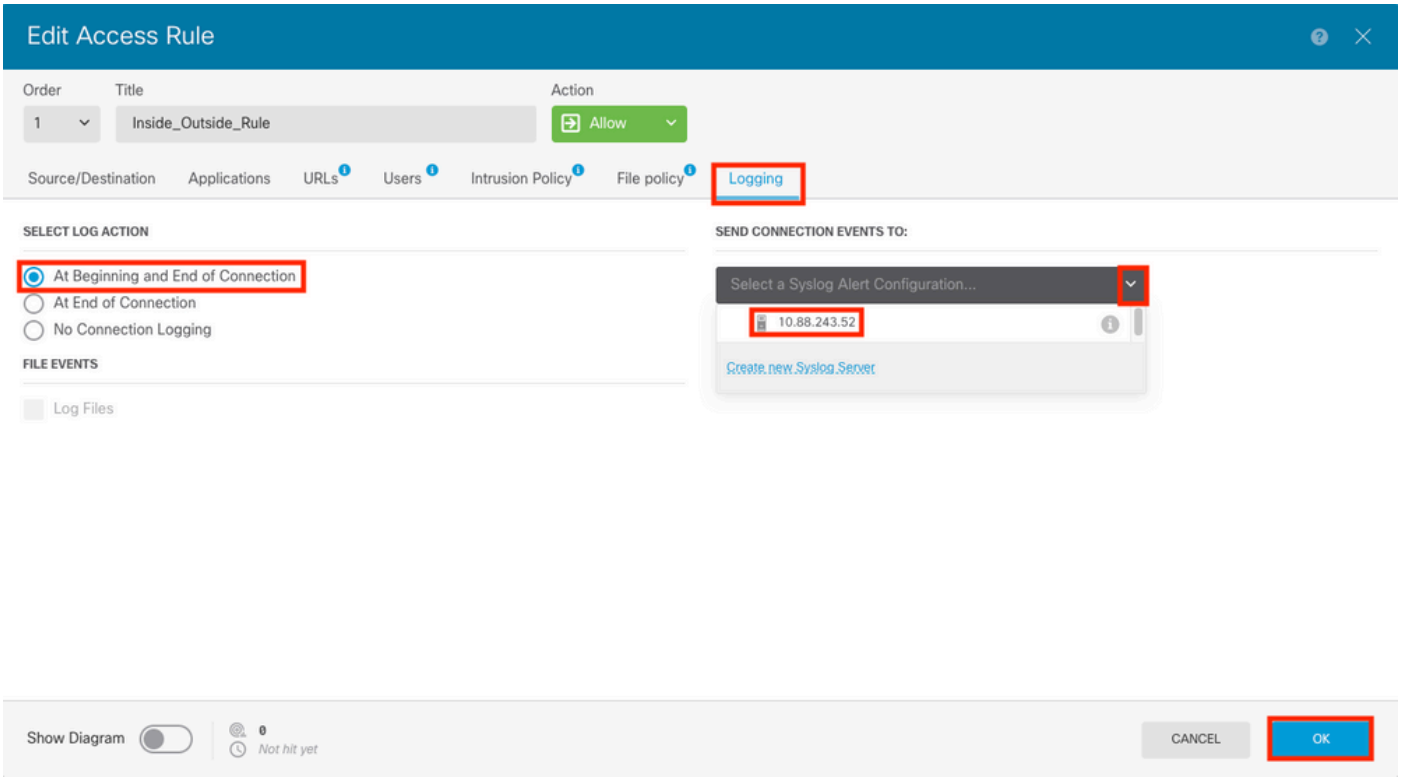
En outre, les règles de contrôle d'accès de la stratégie de contrôle d'accès peuvent être définies pour se connecter au serveur Syslog :

Étape 1. Cliquez sur le bouton Policies en haut de l'écran.

Étape 2. Passez le curseur sur le côté droit de la règle ACP pour ajouter la journalisation et sélectionnez l'icône représentant un crayon.



Étape 3. Sélectionnez l'onglet Logging, sélectionnez la case d'option At End of Connection, sélectionnez la flèche de la liste déroulante sous Select a Syslog Alert Configuration, sélectionnez sur le serveur Syslog et cliquez sur OK.



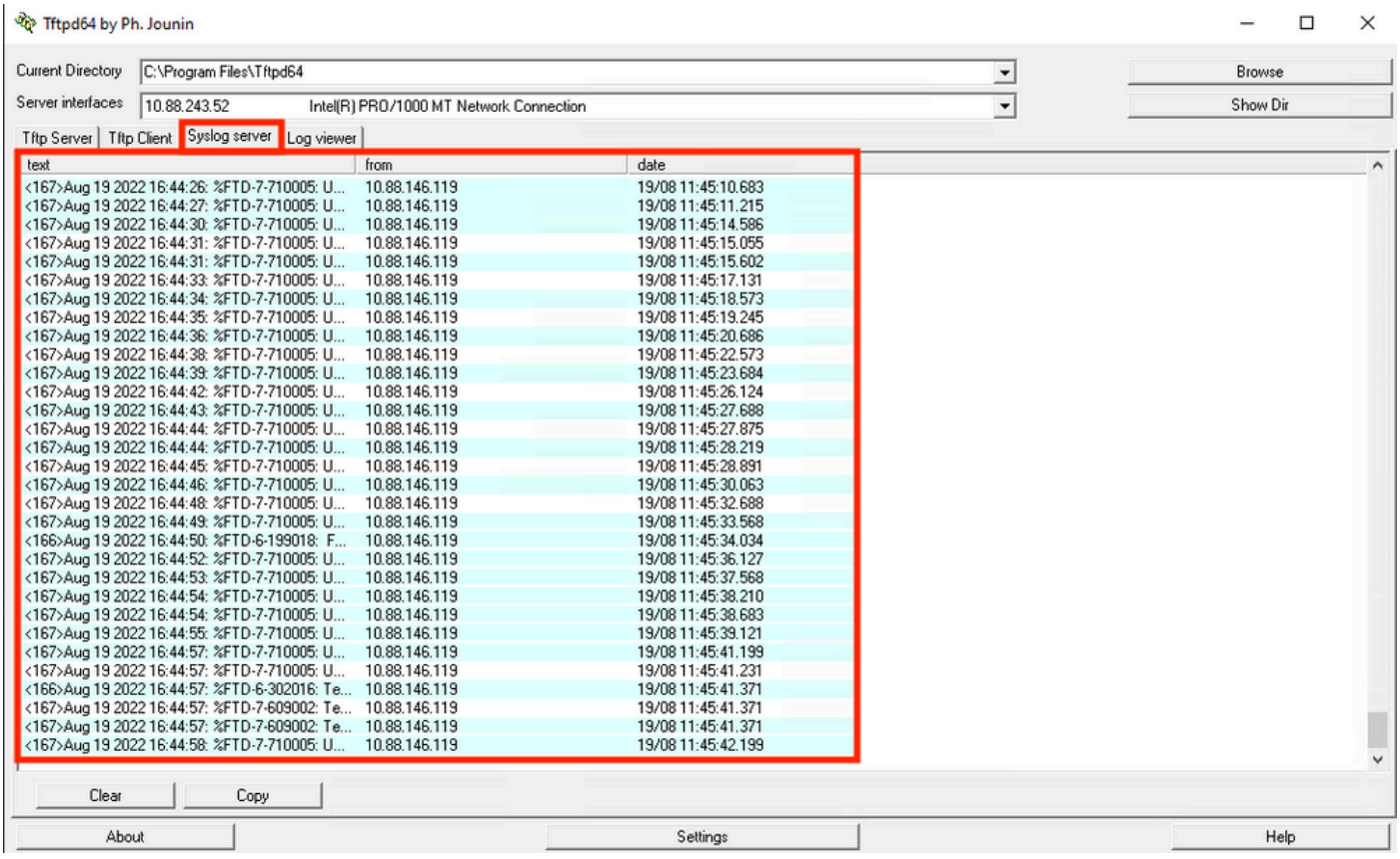
Étape 4. Déployez les modifications de configuration.

Vérifier

Étape 1. Une fois la tâche terminée, vous pouvez vérifier les paramètres du mode de configuration CLI FTD à l'aide de la commande 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
>
```

Étape 2. Accédez au serveur Syslog et vérifiez que l'application du serveur Syslog accepte les messages Syslog.



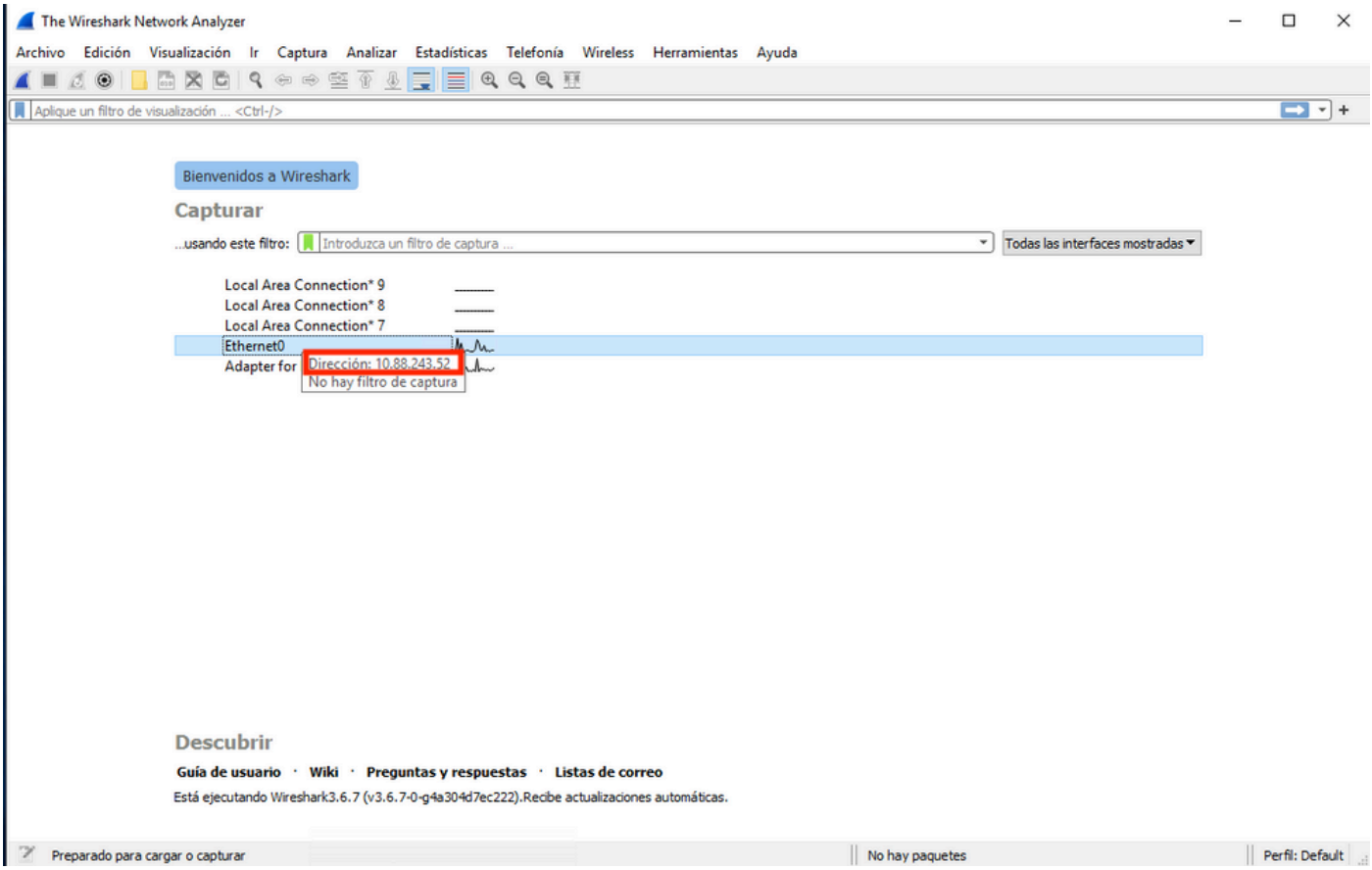
Dépannage

Étape 1. Si les messages Syslog de l'application Syslog produisent des messages, effectuez une capture de paquets à partir de l'interface de ligne de commande FTD pour vérifier la présence de paquets. Passez du mode Clish au mode LINA en entrant la commande **system support diagnostic-cli** à l'invite de commande clish.

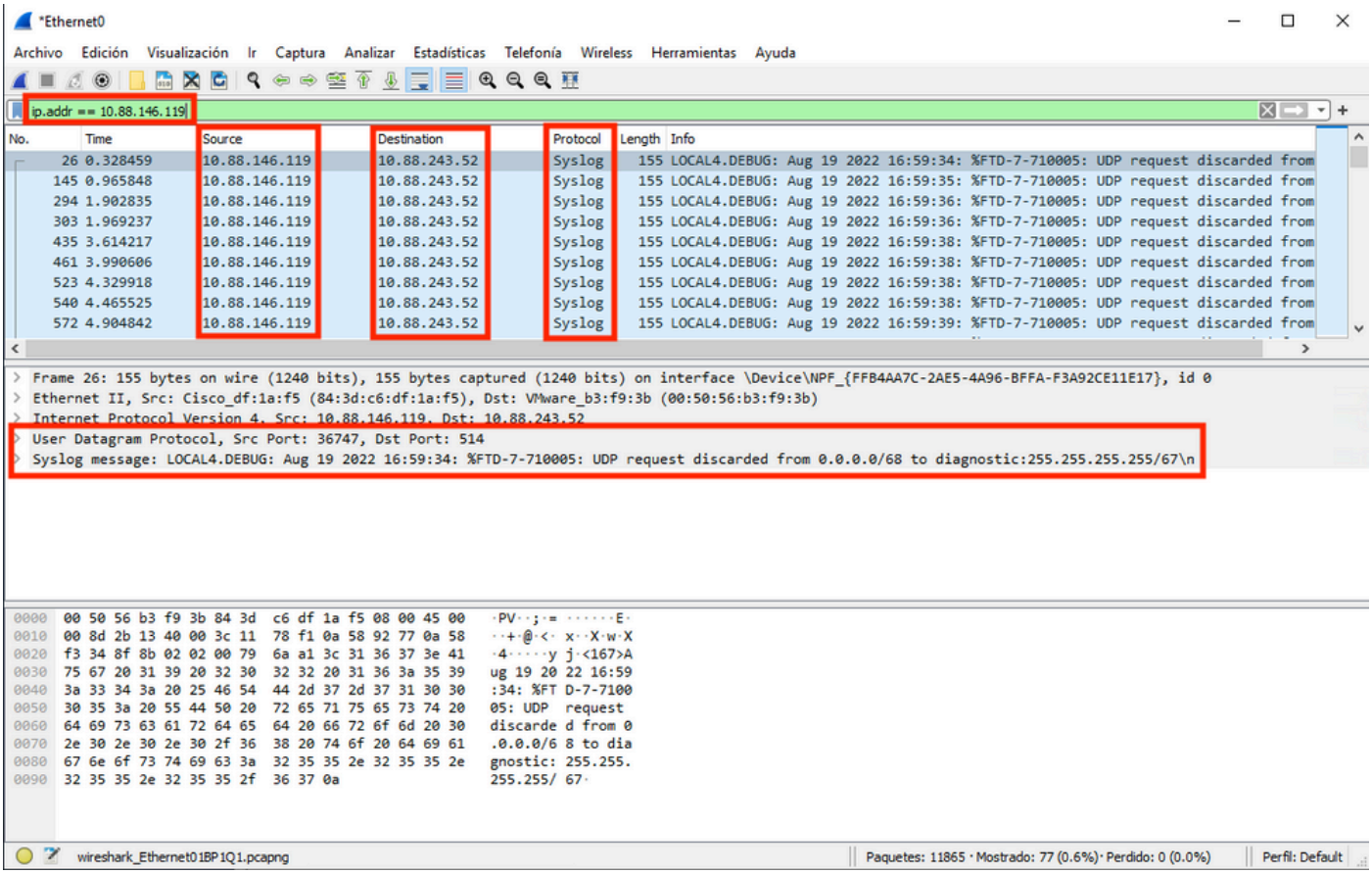
```
[> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

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

Étape 2. Créez une capture de paquets pour votre udp 514 (ou tcp 1468 si vous avez utilisé tcp)

Étape 3. Vérifiez que la communication est établie avec la carte d'interface réseau sur le serveur Syslog. Utilisez Wireshark ou un autre utilitaire de capture de paquets chargé. Double-cliquez sur l'interface dans Wireshark pour que le serveur Syslog commence à capturer des paquets.



Étape 4. Définissez un filtre d'affichage dans la barre supérieure pour udp 514 en tapant udp.port==514 et en sélectionnant la flèche à droite de la barre. À partir du résultat, vérifiez si les paquets sont transmis au serveur Syslog.



Étape 5. Si l'application serveur Syslog n'affiche pas les données, dépannez le paramètre dans l'application serveur Syslog. Assurez-vous que le bon protocole est utilisé avec udp/tcp et le bon port 514/1468.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.