Syslog configureren en controleren in Firepower Device Manager

Inhoud

Inleiding

In dit document wordt beschreven hoe u Syslog kunt configureren in Firepower Device Manager (FDM).

Voorwaarden

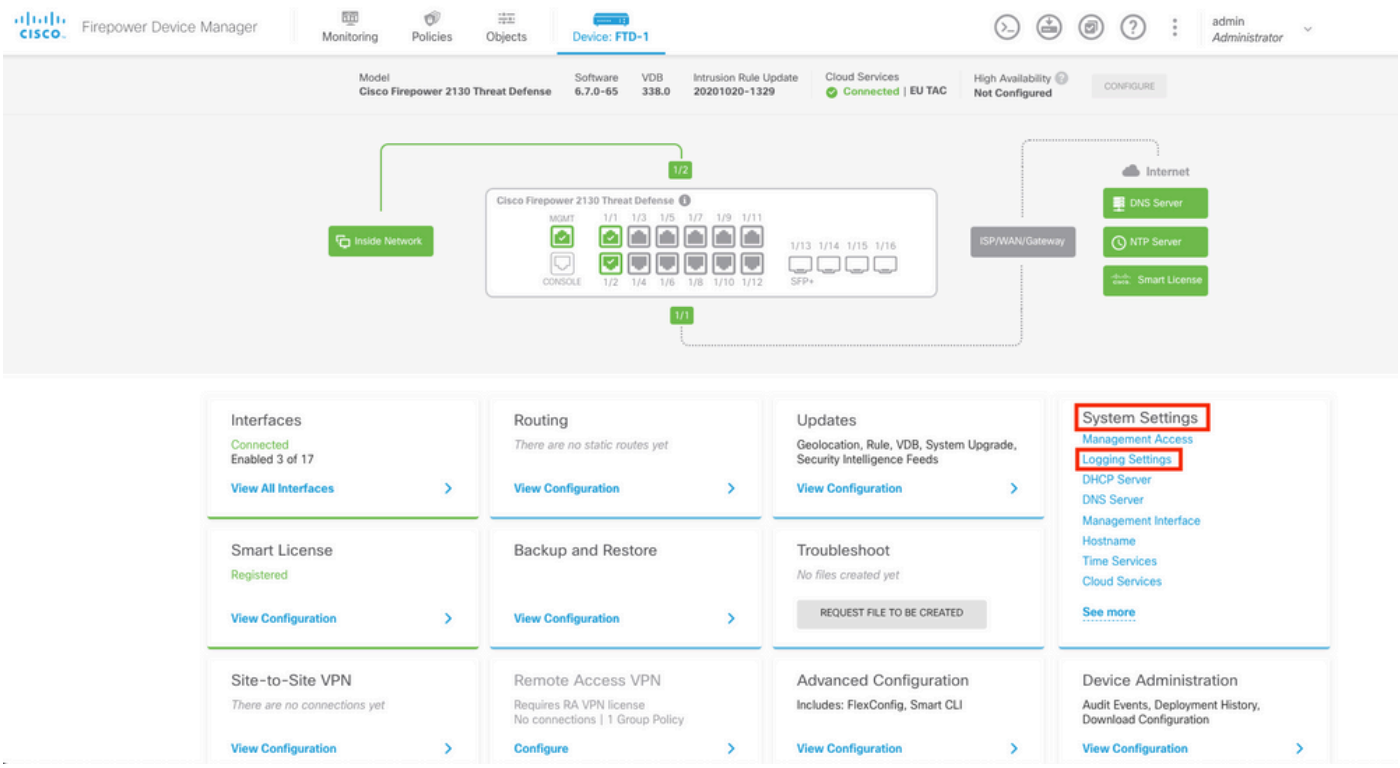
Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

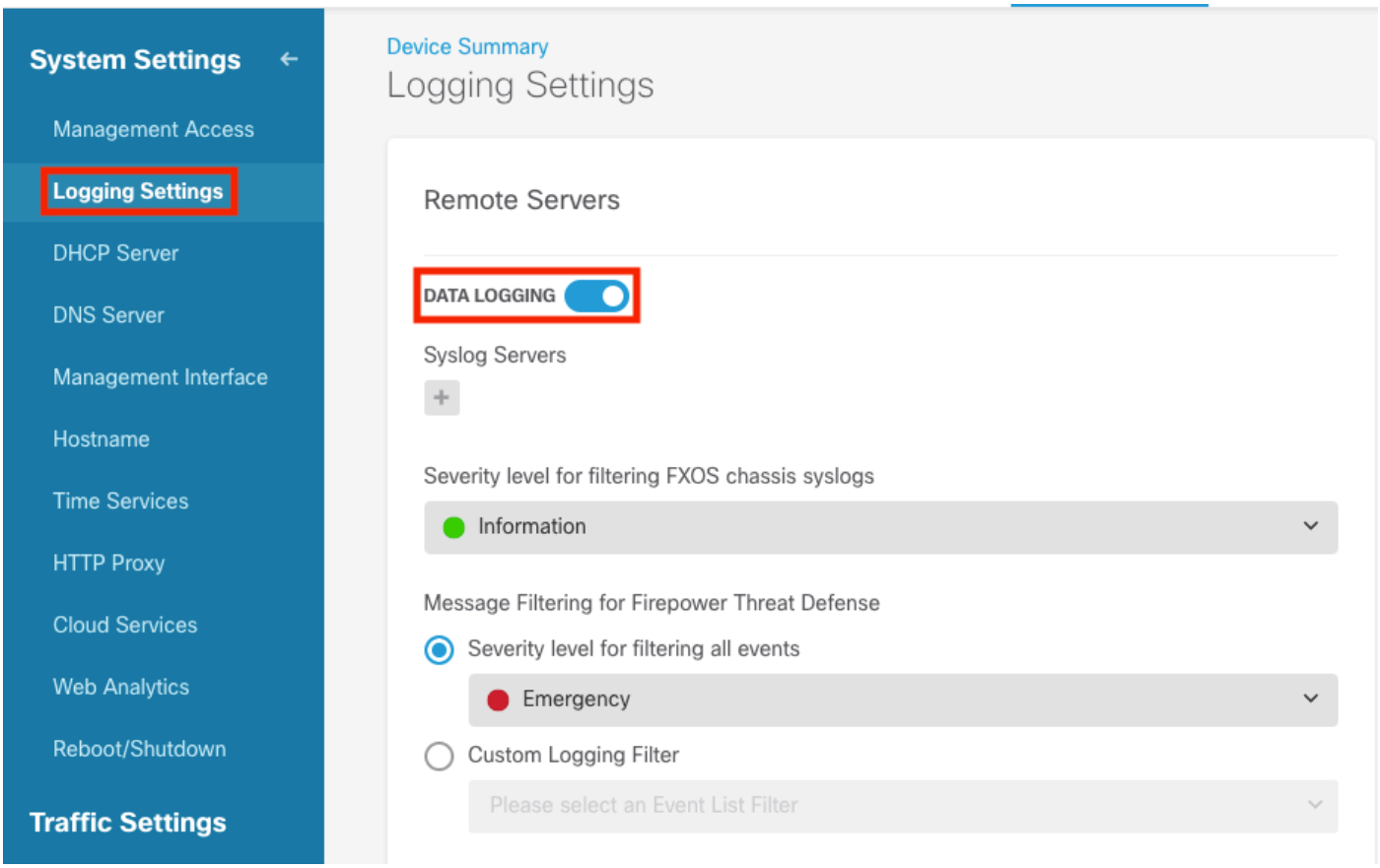
- Firepower Threat Defence
- Syslog Server waarop Syslog-software wordt uitgevoerd om gegevens te verzamelen

Configuraties

Stap 1. Selecteer in het scherm Main Firepower Device Manager de instellingen voor vastlegging onder de Systeeminstellingen in de rechterbenedenhoek van het scherm.



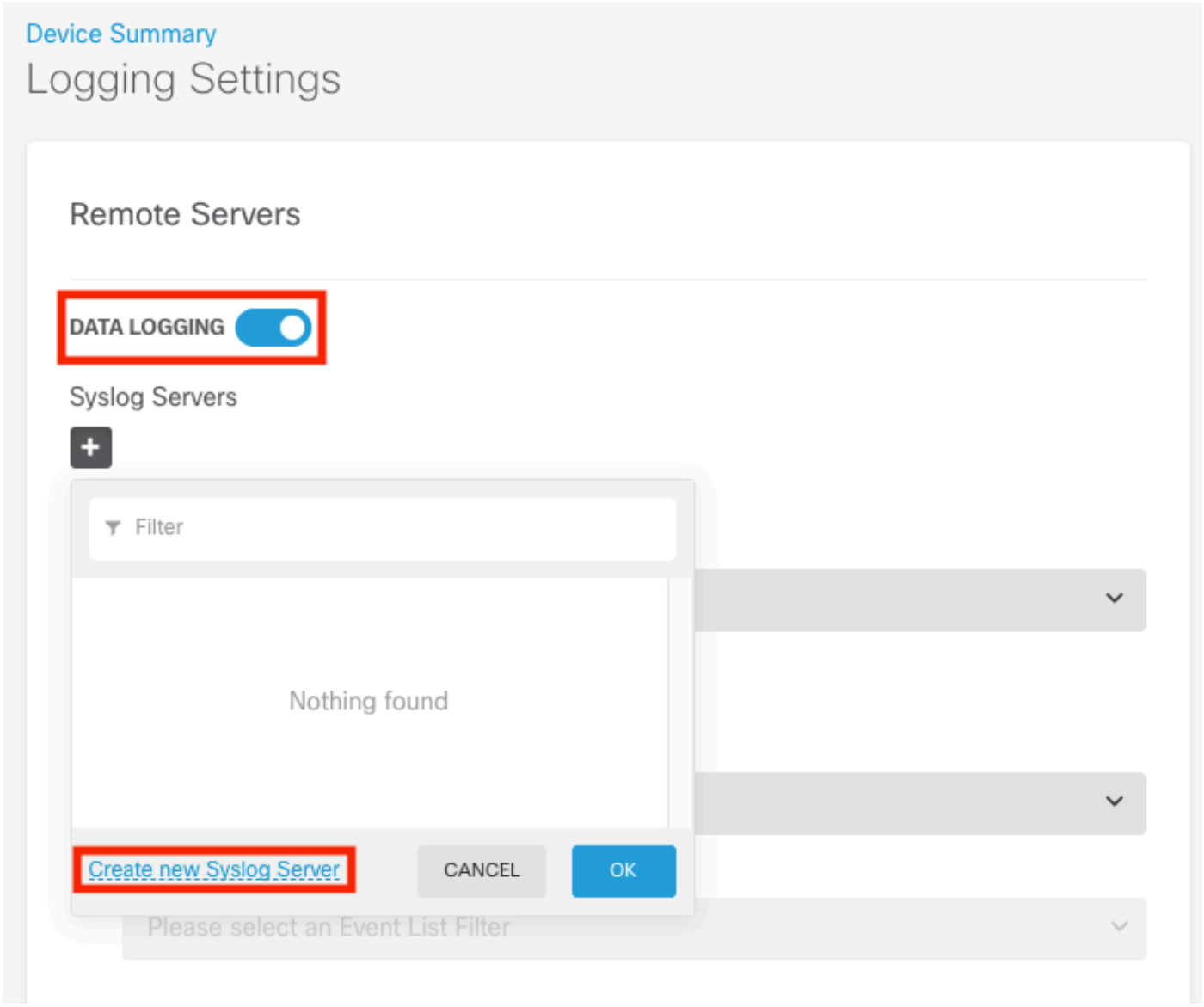
Stap 2. Selecteer in het scherm Systeeminstellingen de instellingen voor vastlegging in het linker menu.



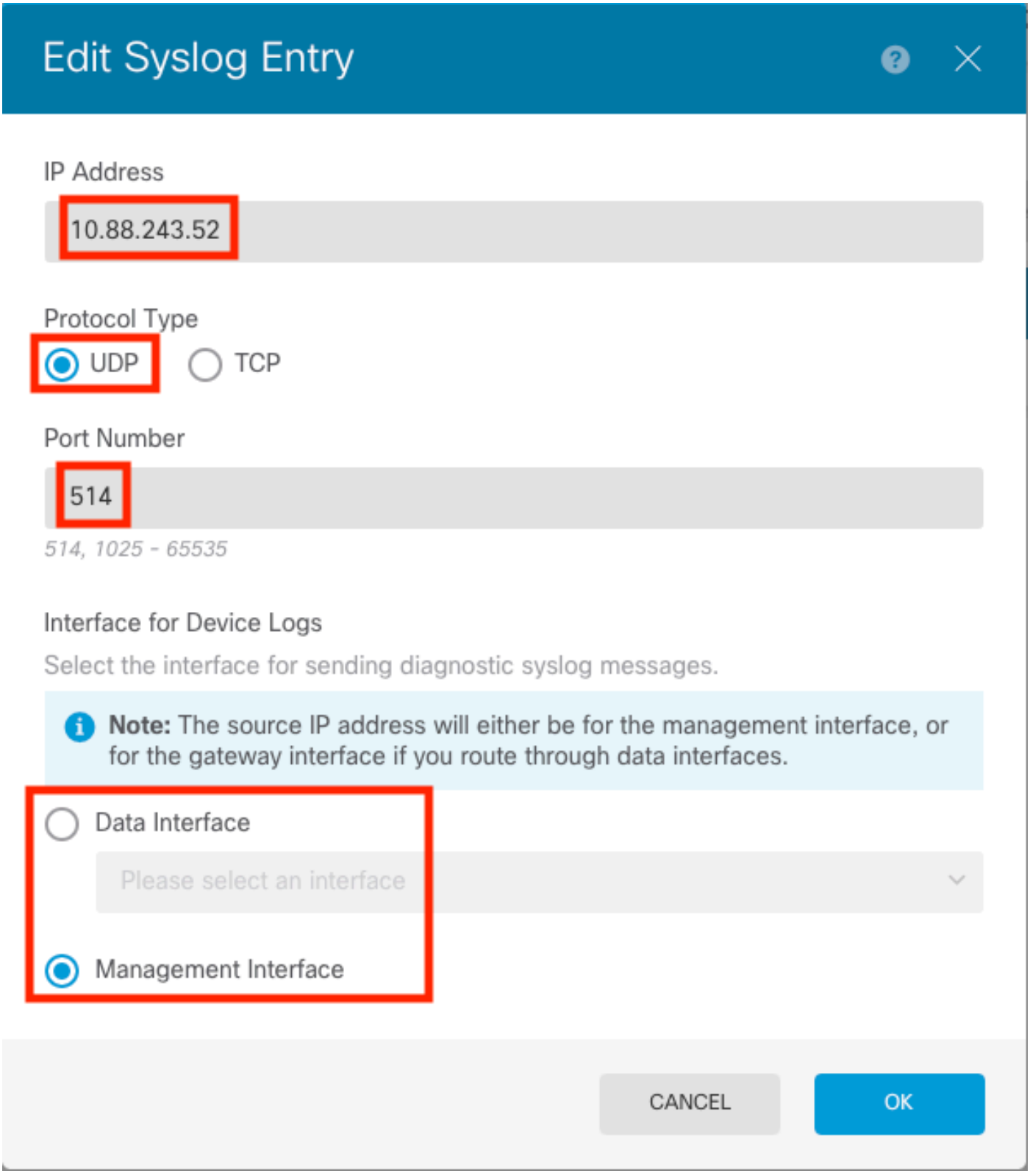
Stap 3. Stel de switch voor de schakelen voor gegevensvastlegging in door het +-teken te selecteren onder Syslog-servers.

Stap 4. Selecteer Syslog Server toevoegen. U kunt ook het object Syslog Server in Objecten -

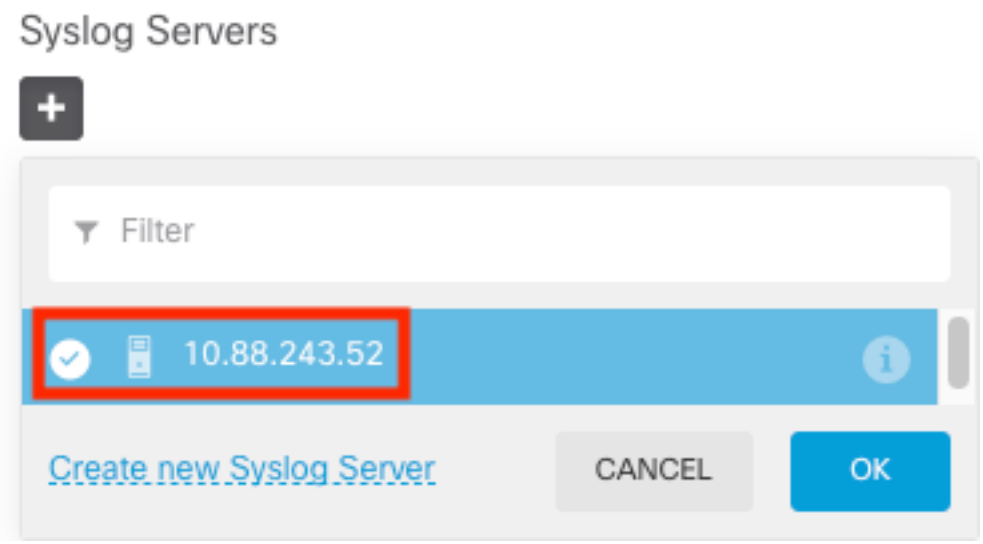
Syslog Servers maken.



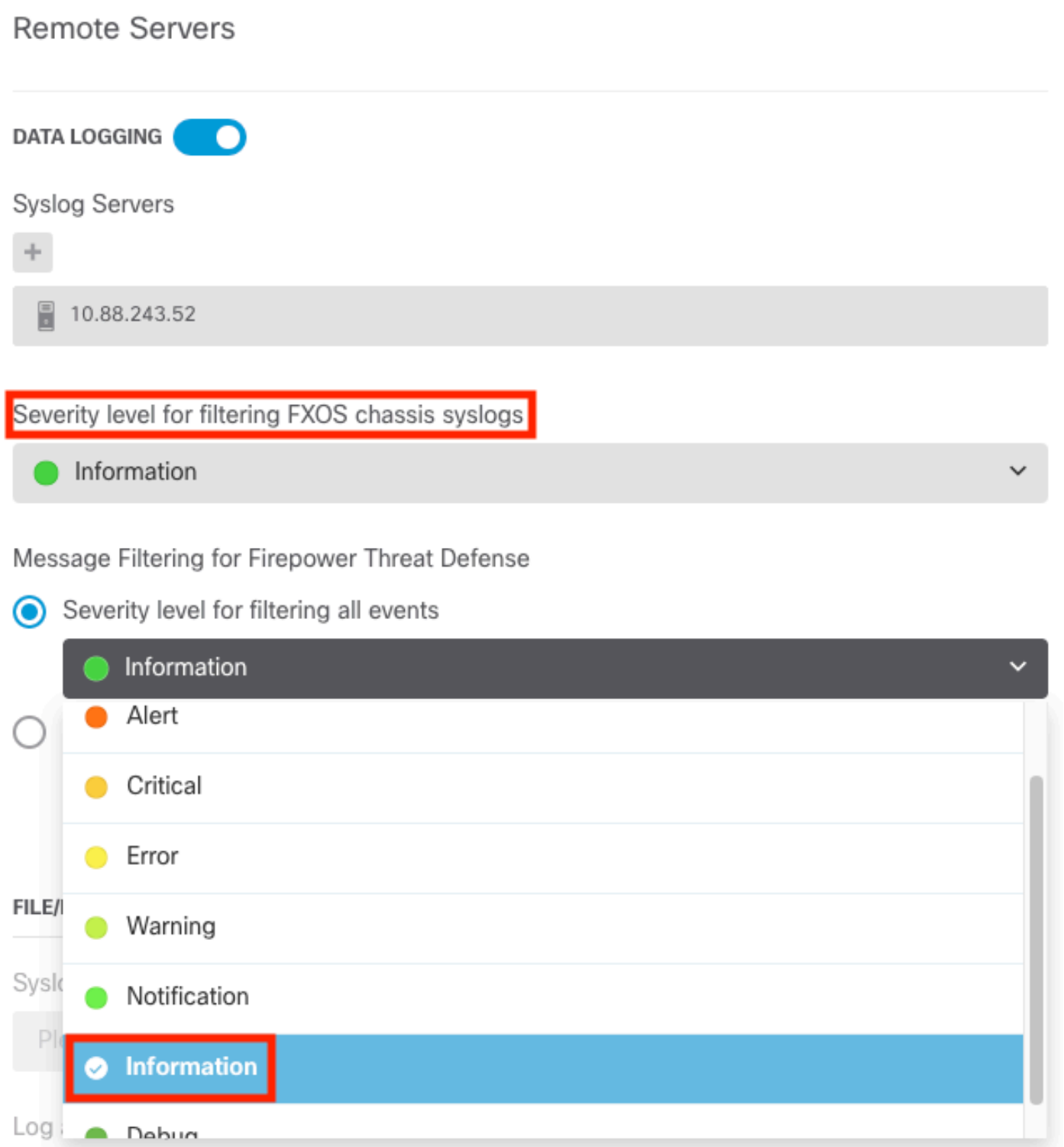
Stap 5. Voer het IP-adres van uw Syslog-server en poortnummer in. Selecteer het keuzerondje voor Data Interface en selecteer OK.



Stap 6. Selecteer vervolgens de nieuwe Syslog-server en selecteer OK.

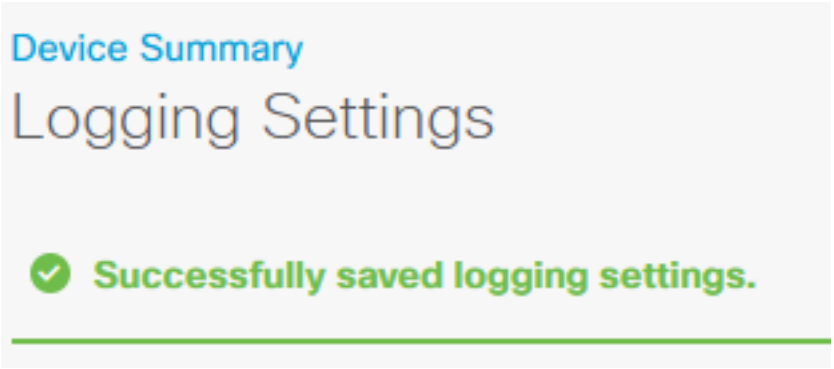


Stap 7. Selecteer het niveau van de Ernst voor het filteren van alle gebeurtenissen radioknop en selecteer uw gewenst registratieniveau.



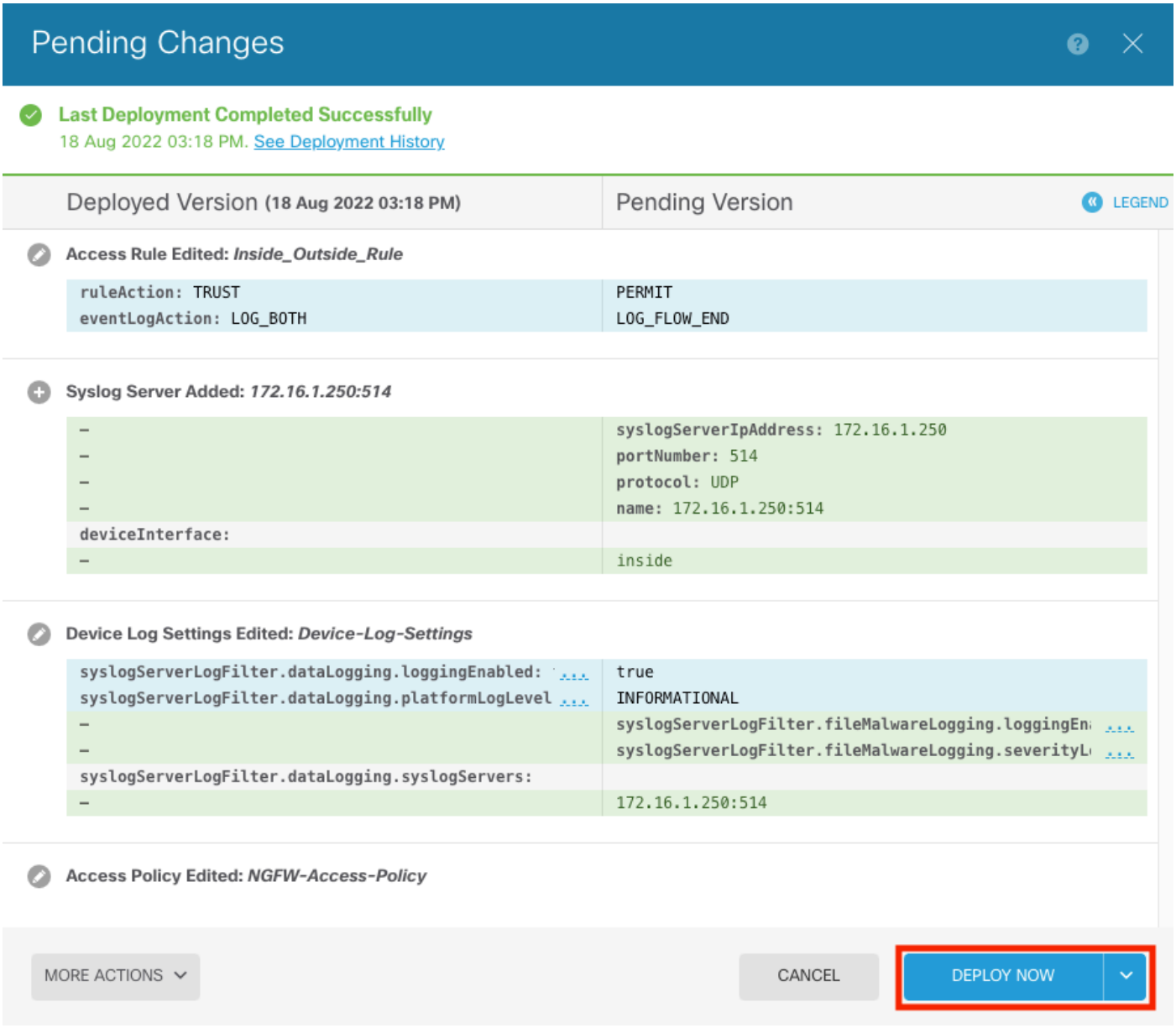
Stap 8. Selecteer Opslaan onder op het scherm.

Stap 9. Controleer of de instellingen zijn geslaagd.



Stap 10. Implementeer de nieuwe instellingen.

en

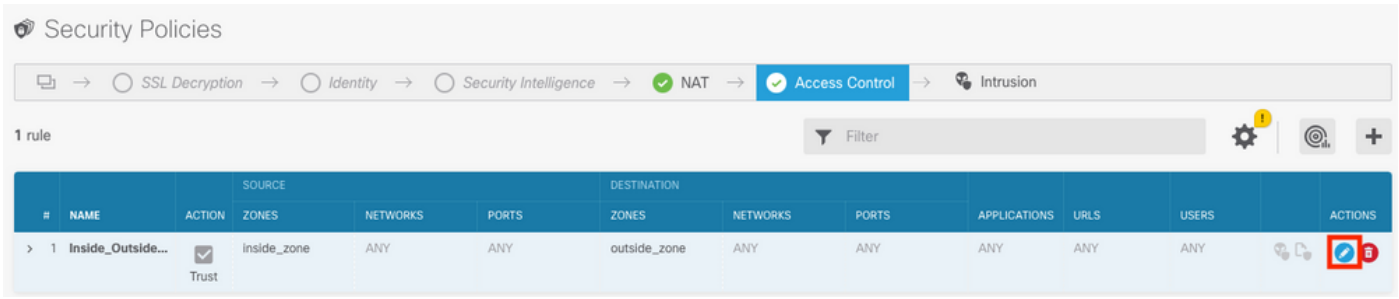


Optioneel.

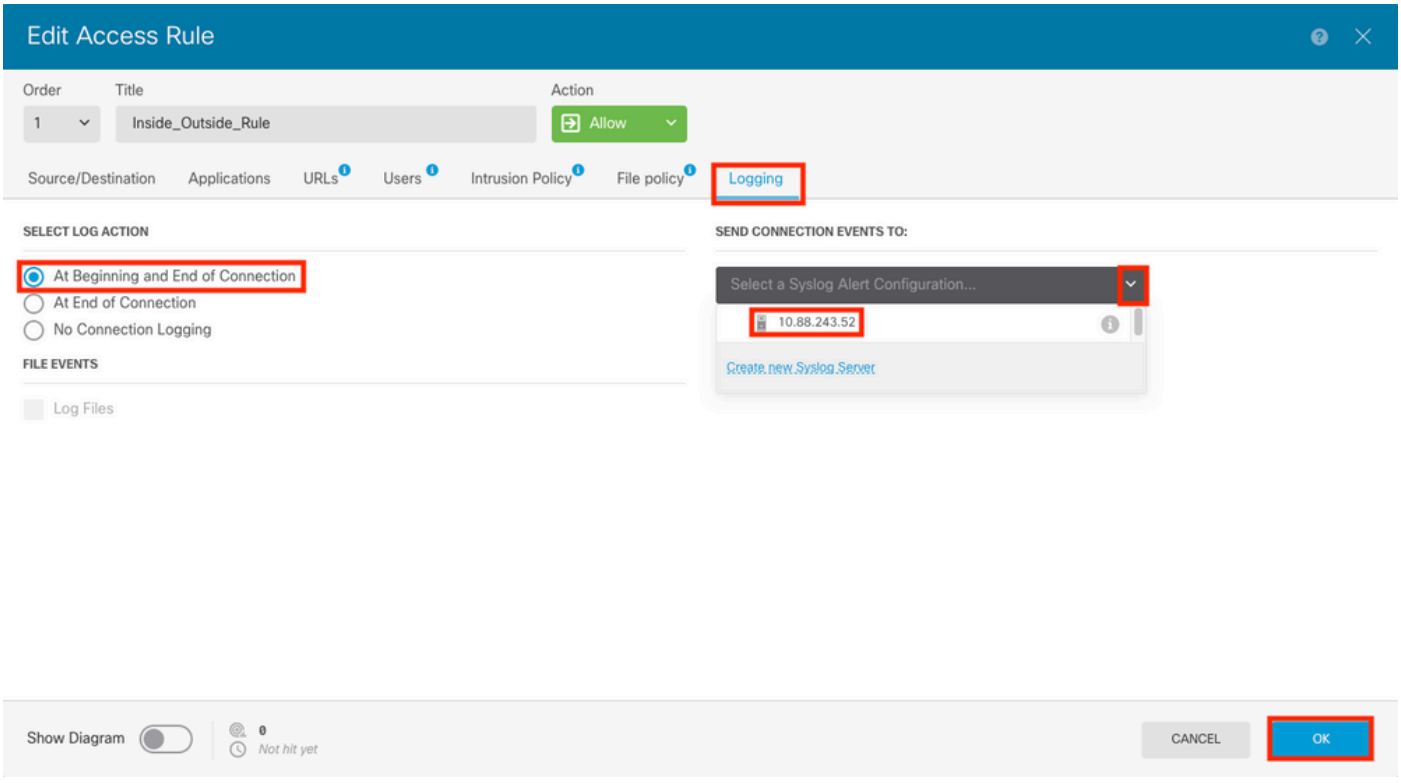
Bovendien kunnen de toegangscontroleregels voor het toegangsbeleid worden ingesteld om in te loggen op de Syslog-server:

Stap 1. Klik op de knop Beleid boven aan het scherm.

Stap 2. Beweeg over de rechterkant van de ACS-regel om logboekregistratie toe te voegen en selecteer het potloodpictogram.



Stap 3. Selecteer het tabblad Vastlegging, selecteer de keuzerondje voor Aan het einde van de verbinding, selecteer de pijl van de vervolgkeuzelijst onder Selecteer een Syslog Alert Configuration, selecteer op de Syslog-server en selecteer OK.



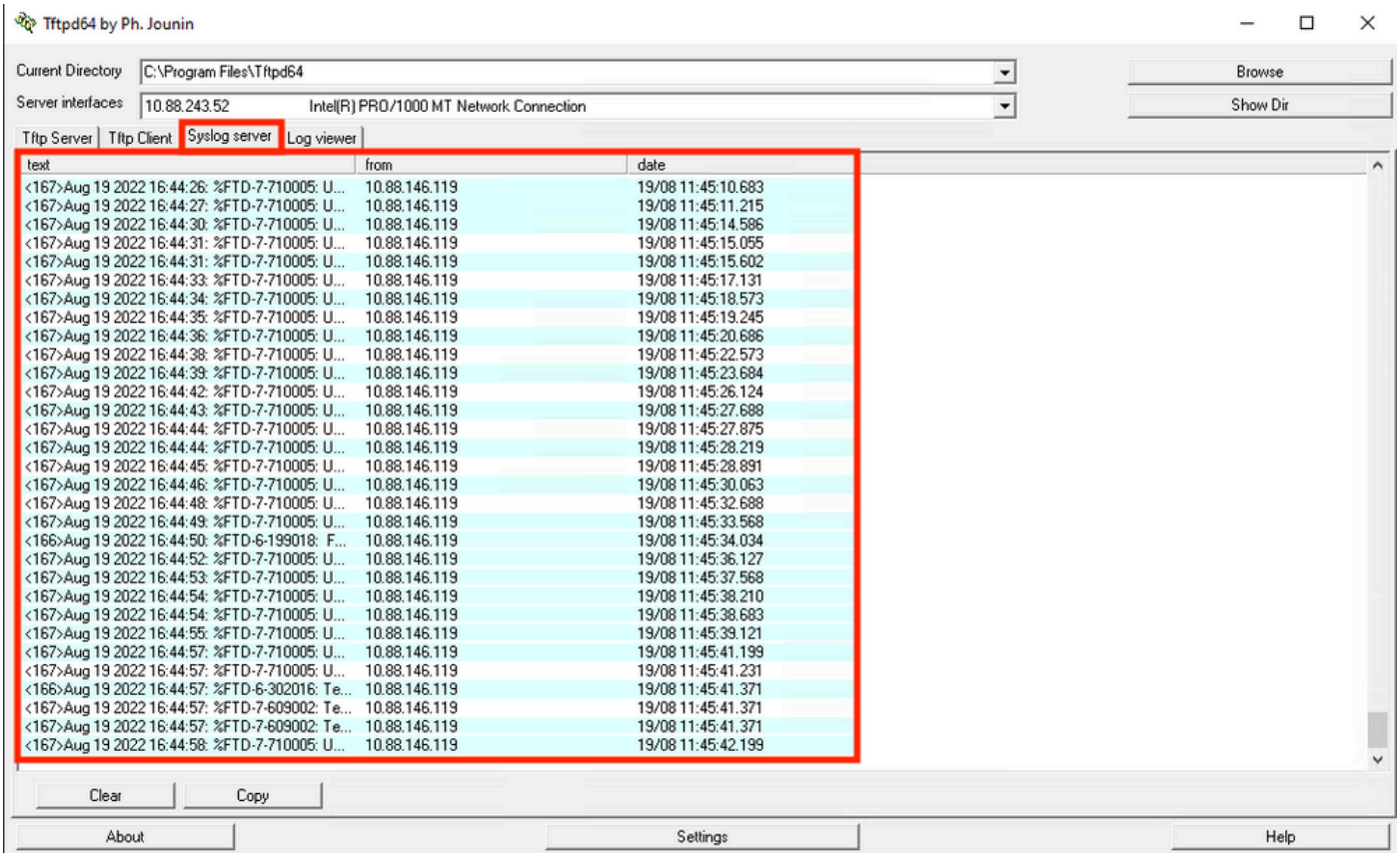
Stap 4. Stel de configuratieveranderingen op.

Verifiëren

Stap 1. Nadat de taak is voltooid, kunt u de instellingen controleren in de FTD CLI Clish Mode met behulp van de opdracht **Show in werking stelt**-configuratievastlegging.

```
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
>
```

Stap 2. Navigeer naar de Syslog-server en controleer of de Syslog-servertoepassing Syslog-berichten accepteert.



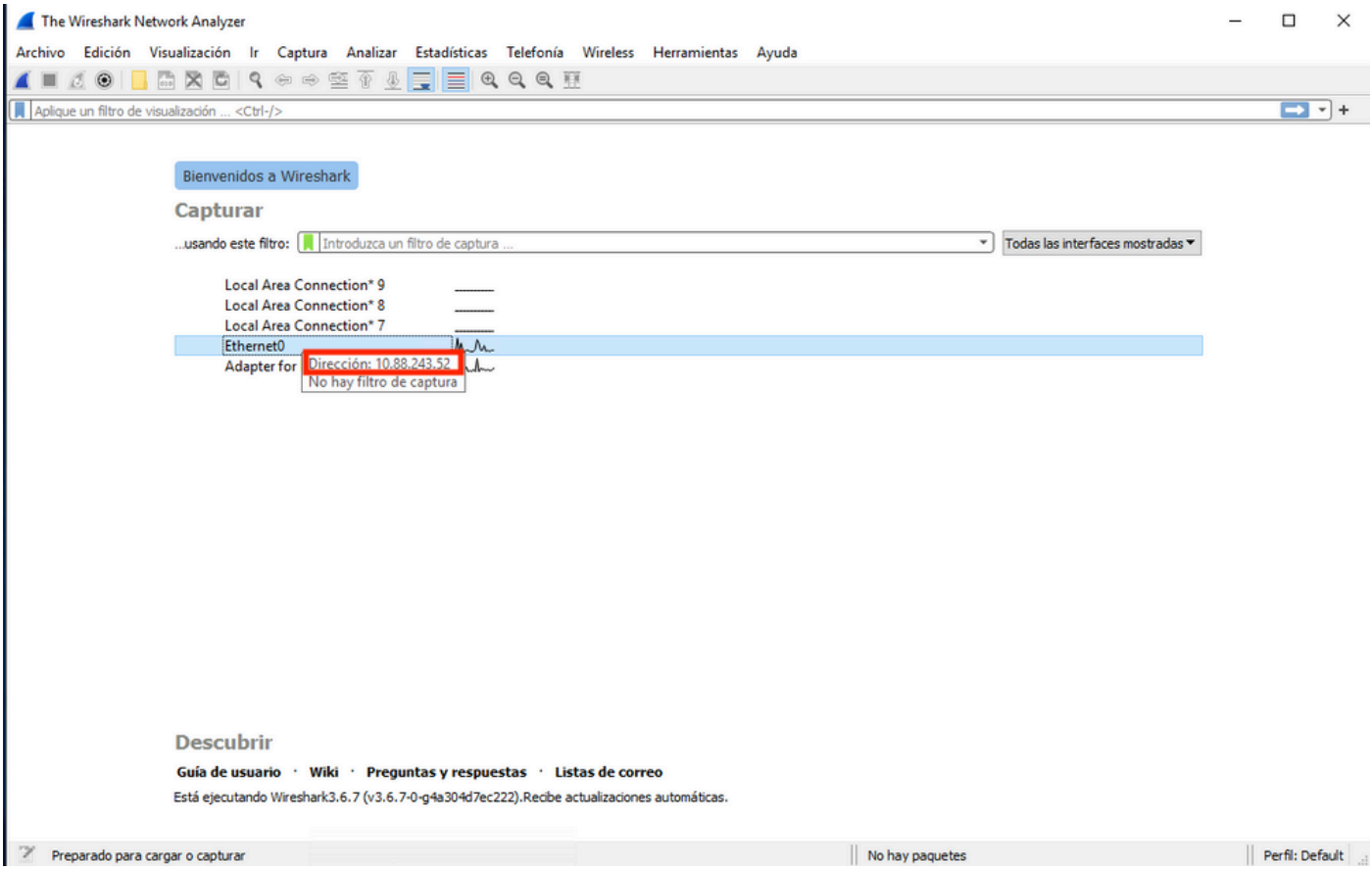
Problemen oplossen

Stap 1. Als de Syslog-berichten op de Syslog-toepassing berichten produceren, voert u een pakketopname uit vanuit de FTD CLI om te controleren of er pakketten zijn. Verander van Clish-modus naar LINA door het commando **van** de **systeemondersteuning diagnostic-client** in te voeren bij de clish-prompt.

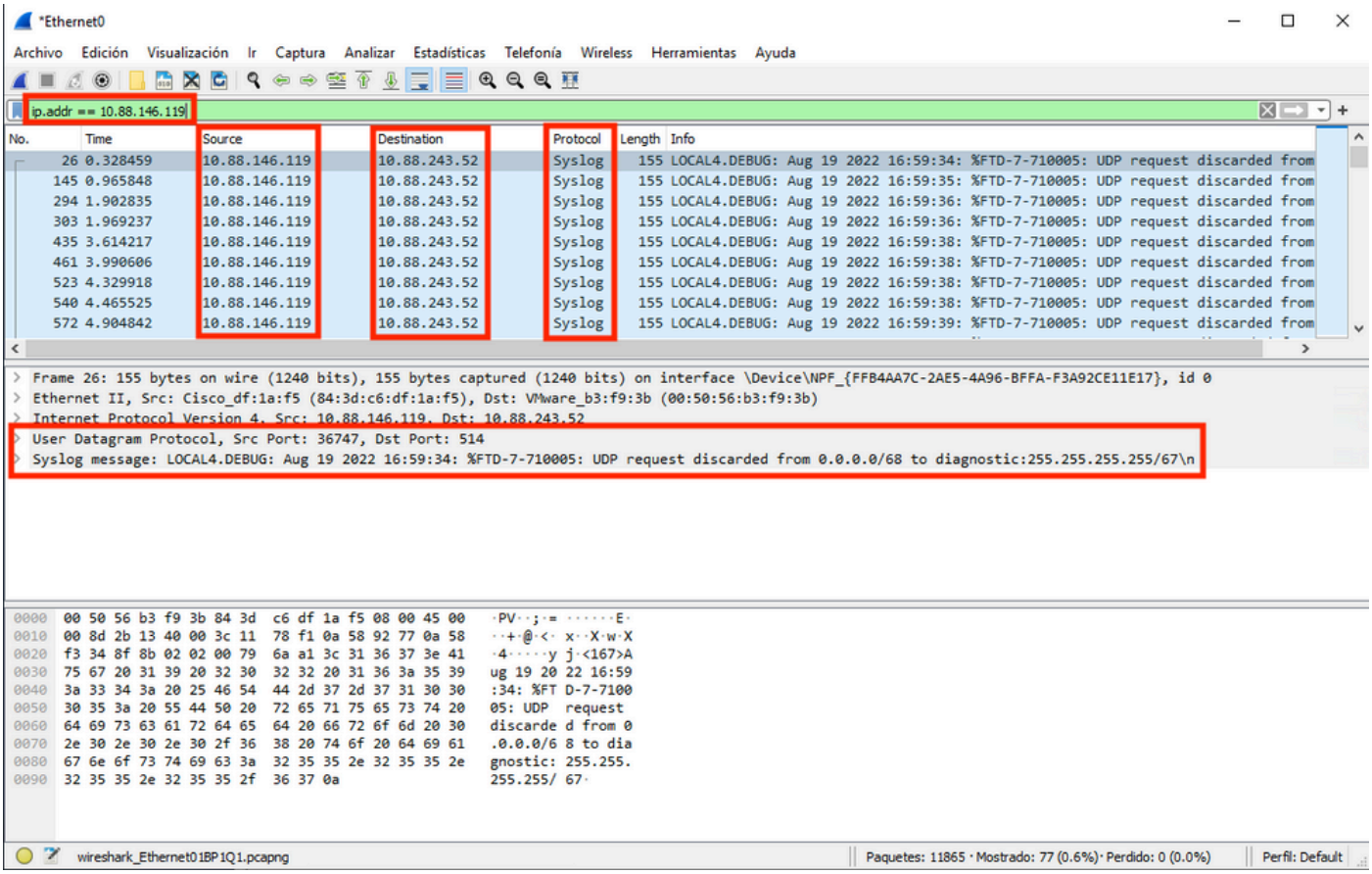
```
[> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

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

Stap 2. Maak één pakketopname voor uw UDP 514 (of TCP 1468 als u TCP gebruikt)

Stap 3. Controleer of de communicatie plaatsvindt naar de netwerkinterfacekaart op de Syslog-server. Gebruik Wireshark of een ander pakketopnameprogramma geladen. Dubbelklik op de interface in Wireshark om te beginnen met het opnemen van pakketten door de Syslog-server.



Stap 4. Stel een weergavefilter in de bovenbalk in voor de udp 514 door de pijl rechts van de balk te typen op udp.port==514. Bevestig vanuit de uitvoer of de pakketten naar de Syslog-server worden verzonden.



Stap 5. Als de Syslog Server-toepassing de gegevens niet toont, kunt u de instelling in de Syslog Server-toepassing oplossen. Zorg ervoor dat het juiste protocol dup/tcp en de juiste poort 514/1468 gebruikt wordt.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.