

Syslog configureren en controleren in Firepower Device Manager

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Configuraties](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

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

Voorwaarden

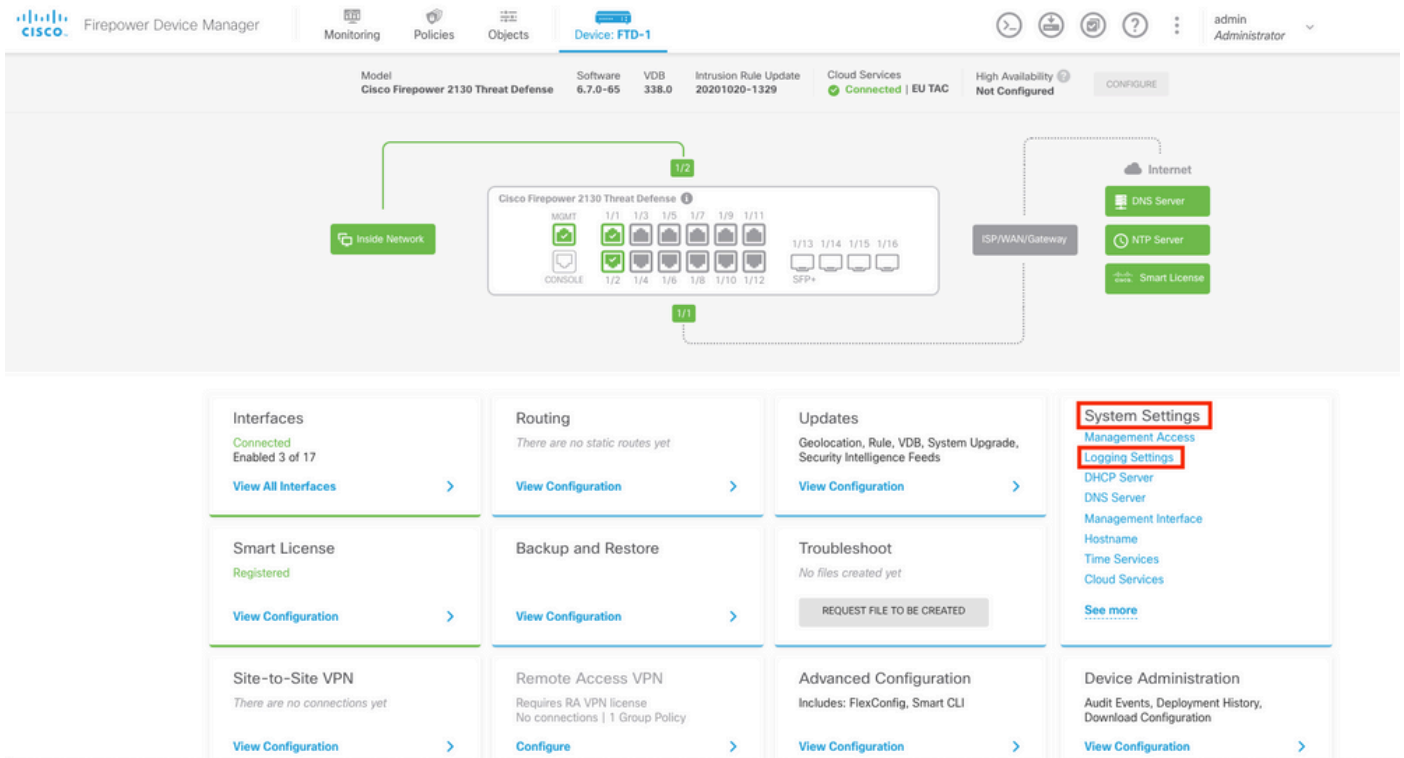
Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

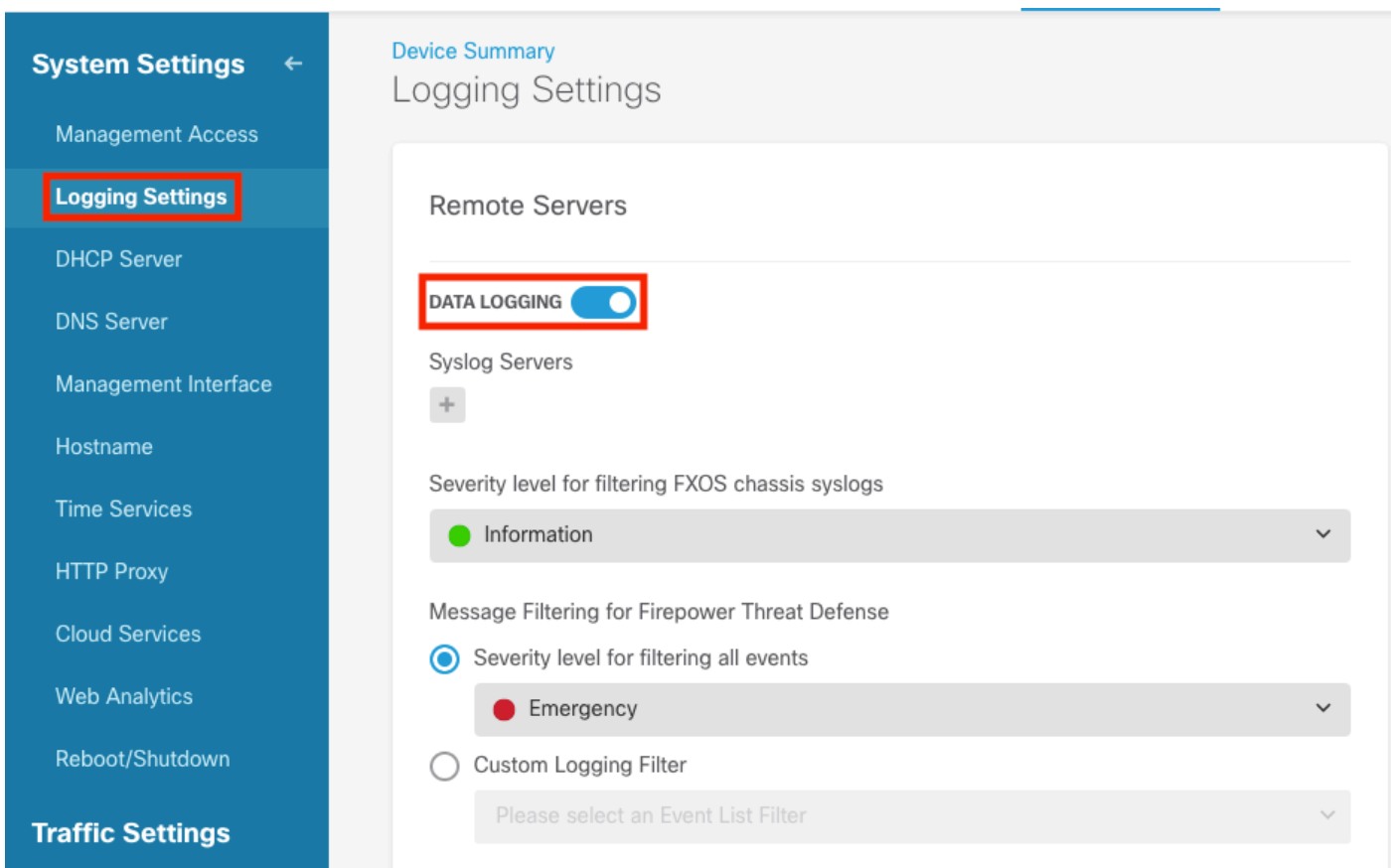
- Firepower Threat Defence
- Syslog Server waarop Syslog-software wordt uitgevoerd om gegevens te verzamelen

Configuraties

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



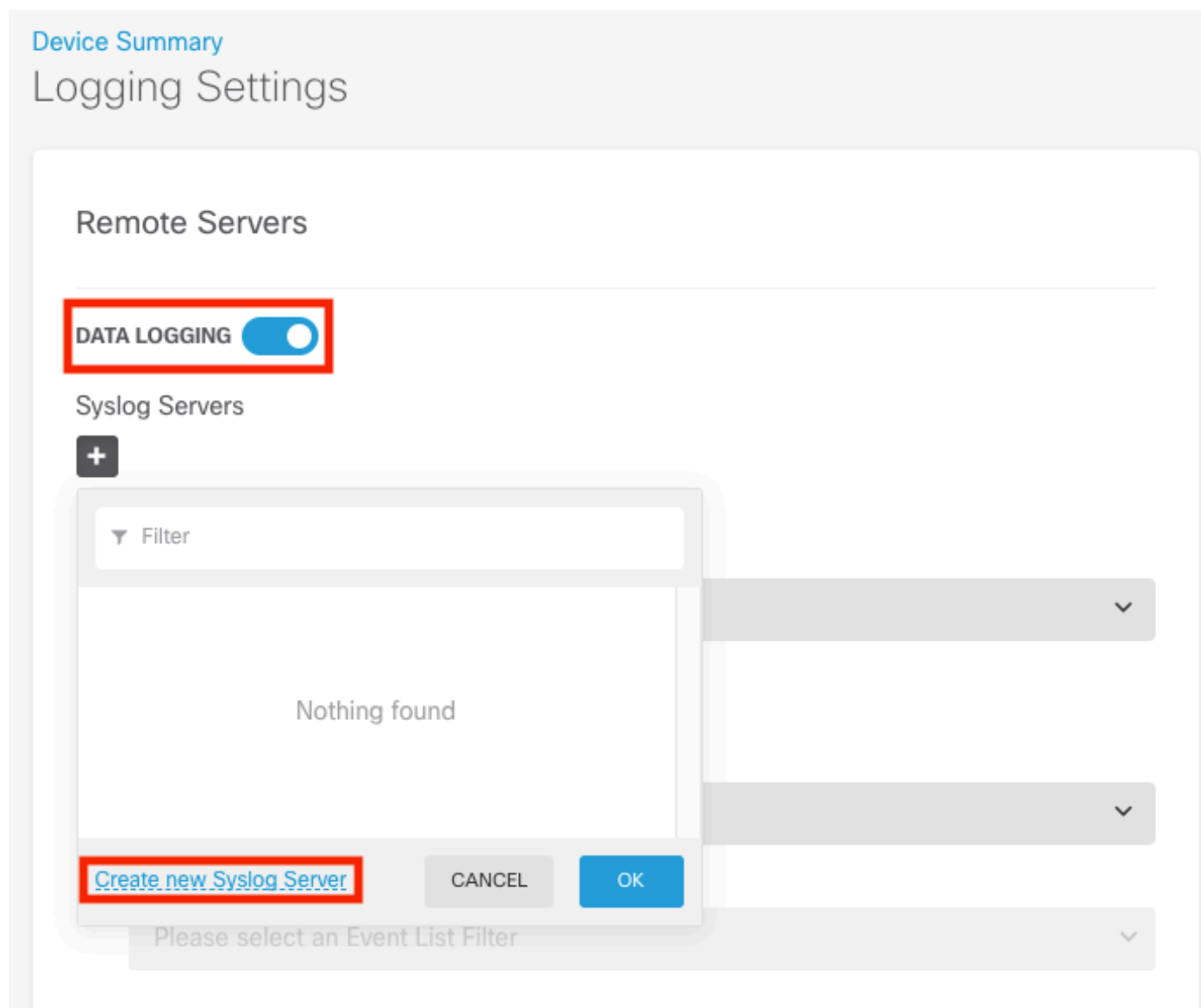
Step 2. Selecteer in het scherm Systeeminstellingen de instellingen voor vastlegging in het linker menu.



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

Step 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.

Edit Syslog Entry



IP Address

10.88.243.52

Protocol Type

UDP TCP

Port Number

514

514, 1025 - 65535

Interface for Device Logs

Select the interface for sending diagnostic syslog messages.

i Note: The source IP address will either be for the management interface, or for the gateway interface if you route through data interfaces.

Data Interface

Please select an interface

Management Interface

CANCEL

OK

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

Syslog Servers



Filter

<input checked="" type="checkbox"/>		10.88.243.52	
-------------------------------------	--	--------------	--

[Create new Syslog Server](#) CANCEL OK

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

Remote Servers

DATA LOGGING

Syslog Servers



10.88.243.52

Severity level for filtering FXOS chassis syslogs

Information

Message Filtering for Firepower Threat Defense

Severity level for filtering all events

Information

Alert

Critical

Error

Warning

Notification

Information

Debug

Stap 8. Selecteer Opslaan onder op het scherm.

SAVE

Stap 9. Controleer of de instellingen zijn geslaagd.

Device Summary

Logging Settings

✔ Successfully saved logging settings.

Stap 10. Implementeer de nieuwe instellingen.



en

Pending Changes

✔ Last Deployment Completed Successfully
18 Aug 2022 03:18 PM. [See Deployment History](#)

Deployed Version (18 Aug 2022 03:18 PM)	Pending Version
Access Rule Edited: <i>Inside_Outside_Rule</i>	
ruleAction: TRUST	PERMIT
eventLogAction: LOG_BOTH	LOG_FLOW_END
+ Syslog Server Added: 172.16.1.250:514	
-	syslogServerIpAddress: 172.16.1.250
-	portNumber: 514
-	protocol: UDP
-	name: 172.16.1.250:514
deviceInterface:	
-	inside
Device Log Settings Edited: <i>Device-Log-Settings</i>	
syslogServerLogFilter.dataLogging.loggingEnabled: true	true
syslogServerLogFilter.dataLogging.platformLogLevel: INFORMATIONAL	INFORMATIONAL
-	syslogServerLogFilter.fileMalwareLogging.loggingEn: true
-	syslogServerLogFilter.fileMalwareLogging.severityL: true
syslogServerLogFilter.dataLogging.syslogServers:	
-	172.16.1.250:514
Access Policy Edited: <i>NGFW-Access-Policy</i>	

MORE ACTIONS ▾ CANCEL **DEPLOY NOW** ▾

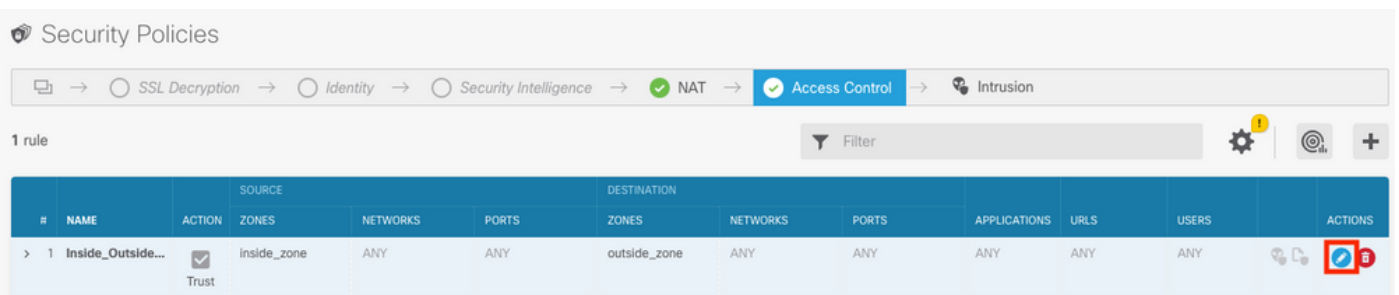
Optioneel.

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

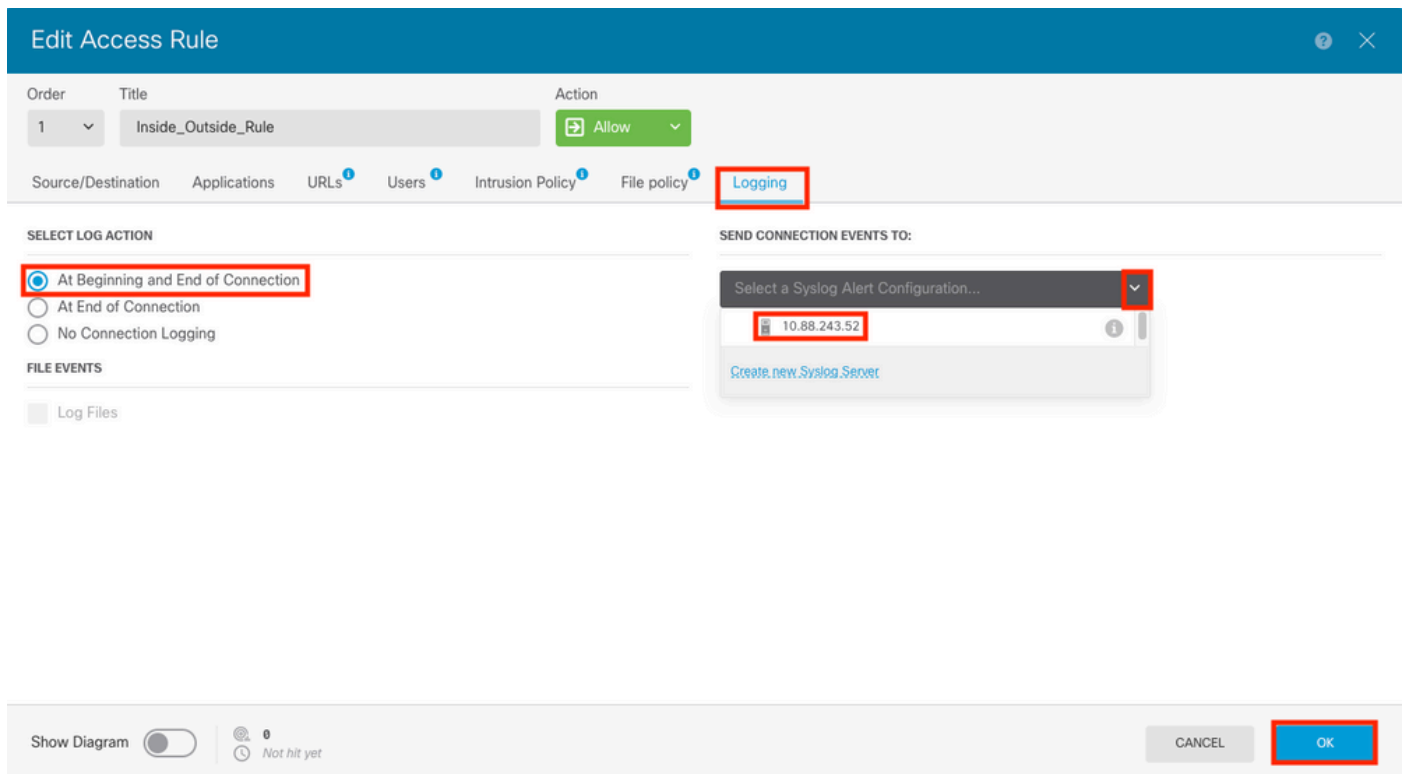
Stap 1. Klik op de knop **Beleid** boven aan het scherm.



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

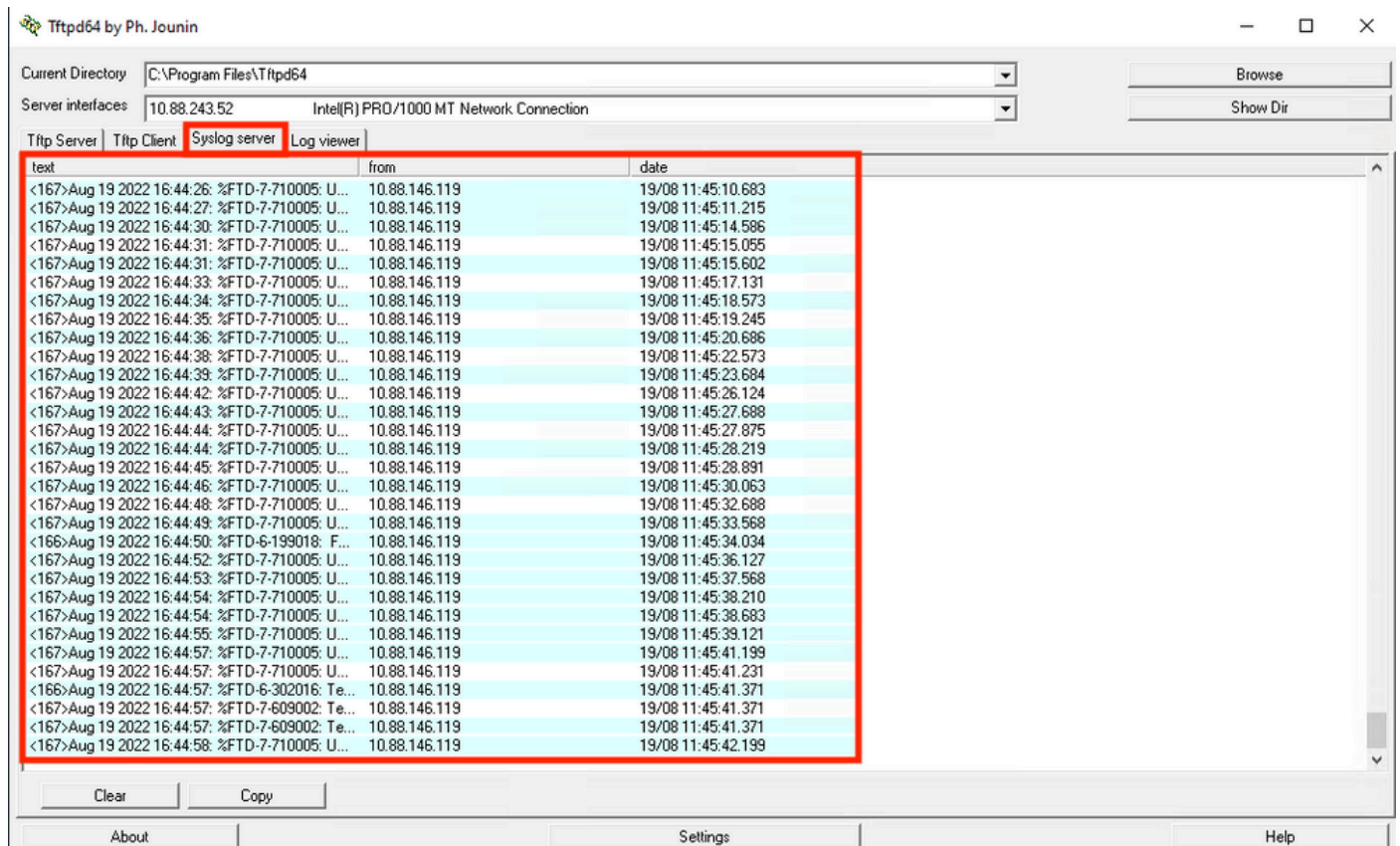
Stap 1. Nadat de taak is voltooid, kunt u de instellingen controleren in de FTD CLI Clish Mode met behulp van de opdracht **Show in werking stelt**-configuratievastlegging.

```
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

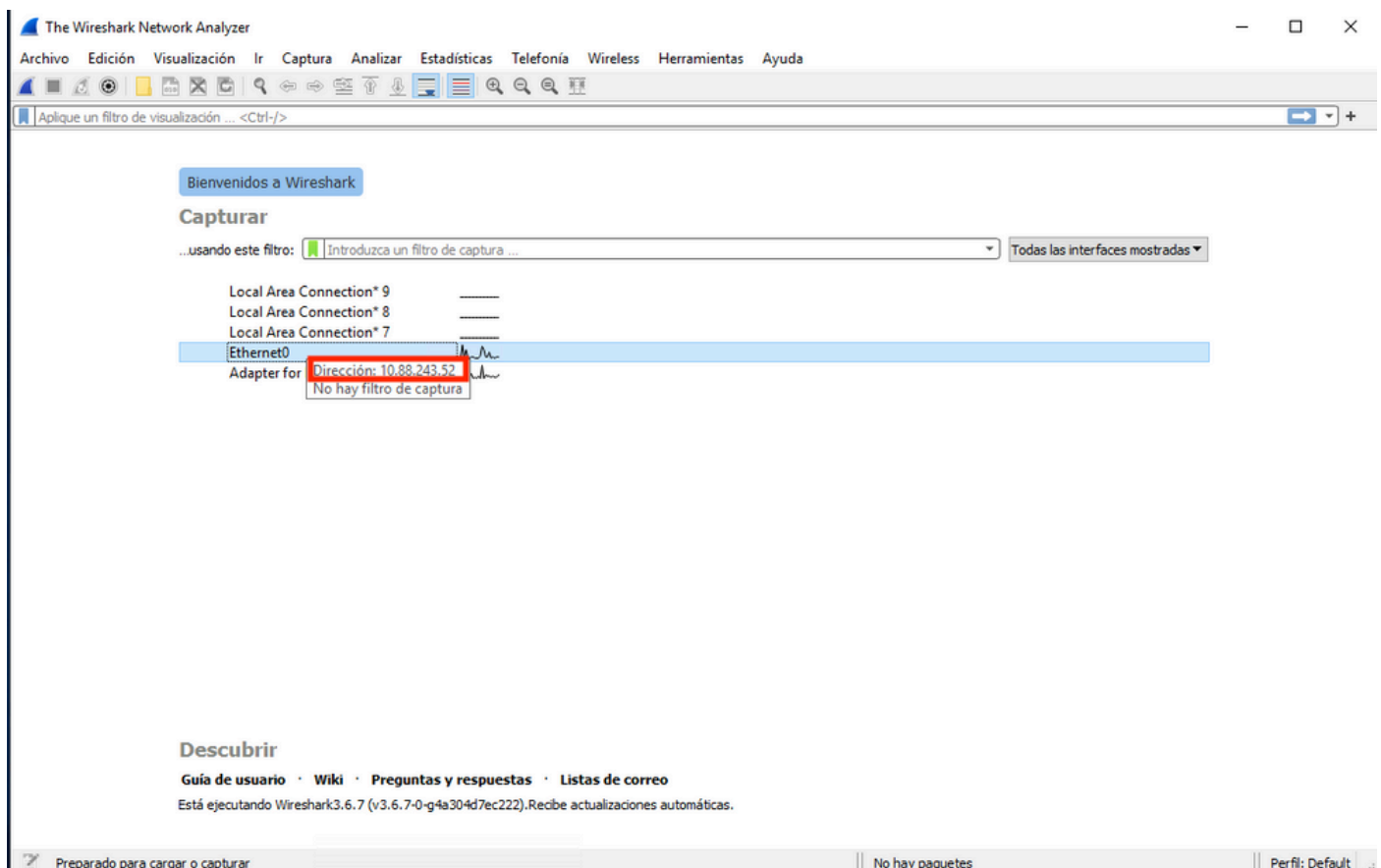
Stap 1. Als de Syslog-berichten op de Syslog-toepassing berichten produceren, voert u een pakketopname uit vanuit de FTD CLI om te controleren of er pakketten zijn. Verander van Clish-modus naar LINA door het commando van de **steemondersteuning diagnostic-client** in te voeren bij de clish-prompt.

```
[> 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.

*Ethernet0

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

ip.addr == 10.88.146.119

No.	Time	Source	Destination	Protocol	Length	Info
26	0.328459	10.88.146.119	10.88.243.52	Syslog	155	LOCAL4.DEBUG: Aug 19 2022 16:59:34: %FTD-7-710005: UDP request discarded from
145	0.965848	10.88.146.119	10.88.243.52	Syslog	155	LOCAL4.DEBUG: Aug 19 2022 16:59:35: %FTD-7-710005: UDP request discarded from
294	1.902835	10.88.146.119	10.88.243.52	Syslog	155	LOCAL4.DEBUG: Aug 19 2022 16:59:36: %FTD-7-710005: UDP request discarded from
303	1.969237	10.88.146.119	10.88.243.52	Syslog	155	LOCAL4.DEBUG: Aug 19 2022 16:59:36: %FTD-7-710005: UDP request discarded from
435	3.614217	10.88.146.119	10.88.243.52	Syslog	155	LOCAL4.DEBUG: Aug 19 2022 16:59:38: %FTD-7-710005: UDP request discarded from
461	3.990606	10.88.146.119	10.88.243.52	Syslog	155	LOCAL4.DEBUG: Aug 19 2022 16:59:38: %FTD-7-710005: UDP request discarded from
523	4.329918	10.88.146.119	10.88.243.52	Syslog	155	LOCAL4.DEBUG: Aug 19 2022 16:59:38: %FTD-7-710005: UDP request discarded from
540	4.465525	10.88.146.119	10.88.243.52	Syslog	155	LOCAL4.DEBUG: Aug 19 2022 16:59:38: %FTD-7-710005: UDP request discarded from
572	4.904842	10.88.146.119	10.88.243.52	Syslog	155	LOCAL4.DEBUG: Aug 19 2022 16:59:39: %FTD-7-710005: UDP request discarded from

> Frame 26: 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits) on interface \Device\NPF_{FFB4AA7C-2AE5-4A96-BFFA-F3A92CE11E17}, id 0
 > Ethernet II, Src: Cisco_df:1a:f5 (84:3d:c6:df:1a:f5), Dst: VMware_b3:f9:3b (00:50:56:b3:f9:3b)
 > Internet Protocol Version 4, Src: 10.88.146.119, Dst: 10.88.243.52
 > User Datagram Protocol, Src Port: 36747, Dst Port: 514
 > Syslog message: LOCAL4.DEBUG: Aug 19 2022 16:59:34: %FTD-7-710005: UDP request discarded from 0.0.0.0/68 to diagnostic:255.255.255.255/67\n

```

0000  00 50 56 b3 f9 3b 84 3d c6 df 1a f5 08 00 45 00  ·PV·;·= ······E·
0010  00 8d 2b 13 40 00 3c 11 78 f1 0a 58 92 77 0a 58  ·+·@·<·x··X·w·X
0020  f3 34 8f 8b 02 02 00 79 6a a1 3c 31 36 37 3e 41  ·4······y·j·<167>A
0030  75 67 20 31 39 20 32 30 32 32 20 31 36 3a 35 39  ug 19 20 22 16:59
0040  3a 33 34 3a 20 25 46 54 44 2d 37 2d 37 31 30 30  :34: %FT D-7-7100
0050  30 35 3a 20 55 44 50 20 72 65 71 75 65 73 74 20  05: UDP request
0060  64 69 73 63 61 72 64 65 64 20 66 72 6f 6d 20 30  discarde d from 0
0070  2e 30 2e 30 2e 30 2f 36 38 20 74 6f 20 64 69 61  .0.0.0/6 8 to dia
0080  67 6e 6f 73 74 69 63 3a 32 35 35 2e 32 35 35 2e  gnostic: 255.255.
0090  32 35 35 2e 32 35 35 2f 36 37 0a 255.255/ 67·
  
```

wireshark_Ethernet01BP1Q1.pcapng Paquetes: 11865 · Mostrado: 77 (0.6%) · Perdido: 0 (0.0%) Perfil: Default

Step 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.