Firepower Device Manager에서 Syslog 구성 및 확인

목차

소개

이 문서에서는 FDM(Firepower Device Manager) 내에서 Syslog를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

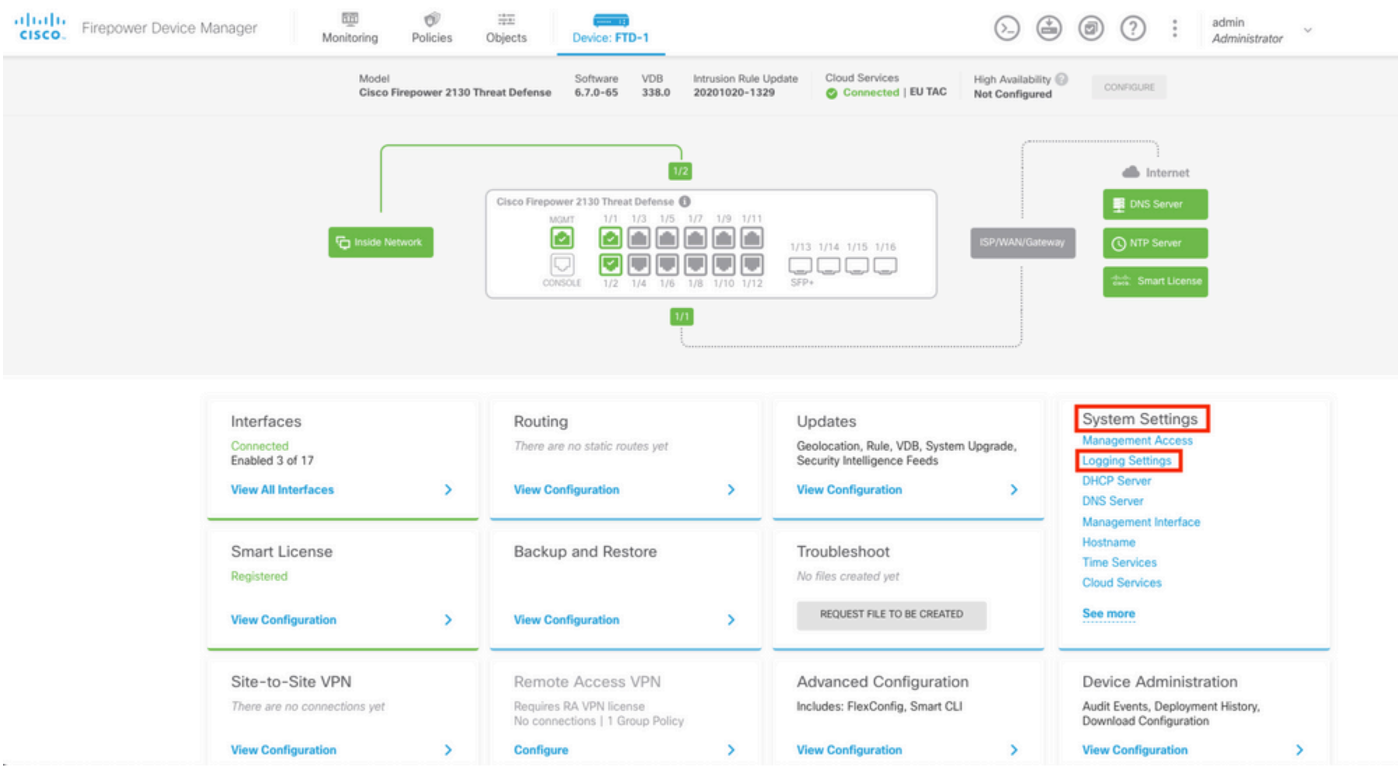
요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Firepower 위협 방어
- 데이터를 수집하기 위해 Syslog 소프트웨어를 실행하는 Syslog 서버

설정

1단계. 기본 Firepower Device Manager(Firepower 디바이스 관리자) 화면의 오른쪽 아래에 있는 System Settings(시스템 설정) 아래에서 Logging Settings(로깅 설정)를 선택합니다.



Model: Cisco Firepower 2130 Threat Defense | Software: 6.7.0-65 | VDB: 338.0 | Intrusion Rule Update: 20201020-1329 | Cloud Services: Connected | EU TAC | High Availability: Not Configured

Interfaces
Connected
Enabled 3 of 17
View All Interfaces >

Routing
There are no static routes yet
View Configuration >

Updates
Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds
View Configuration >

System Settings
Management Access
Logging Settings
DHCP Server
DNS Server
Management Interface
Hostname
Time Services
Cloud Services
See more

Smart License
Registered
View Configuration >

Backup and Restore
View Configuration >

Troubleshoot
No files created yet
REQUEST FILE TO BE CREATED

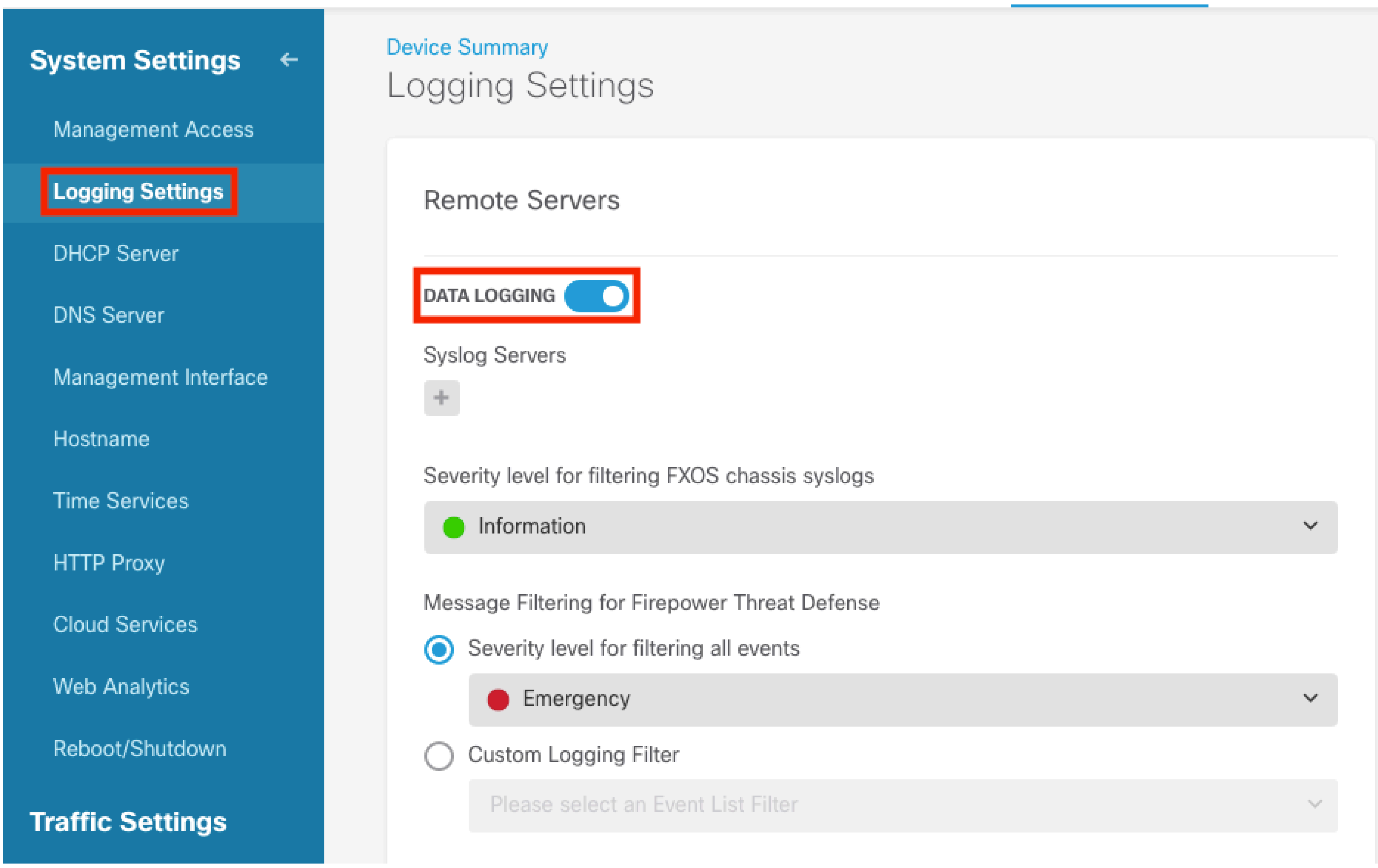
Site-to-Site VPN
There are no connections yet
View Configuration >

Remote Access VPN
Requires RA VPN license
No connections | 1 Group Policy
Configure >

Advanced Configuration
Includes: FlexConfig, Smart CLI
View Configuration >

Device Administration
Audit Events, Deployment History, Download Configuration
View Configuration >

2단계. System Settings(시스템 설정) 화면의 왼쪽 메뉴에서 Logging Settings(로깅 설정)를 선택합니다.



Logging Settings

Remote Servers

DATA LOGGING ●

Syslog Servers
+

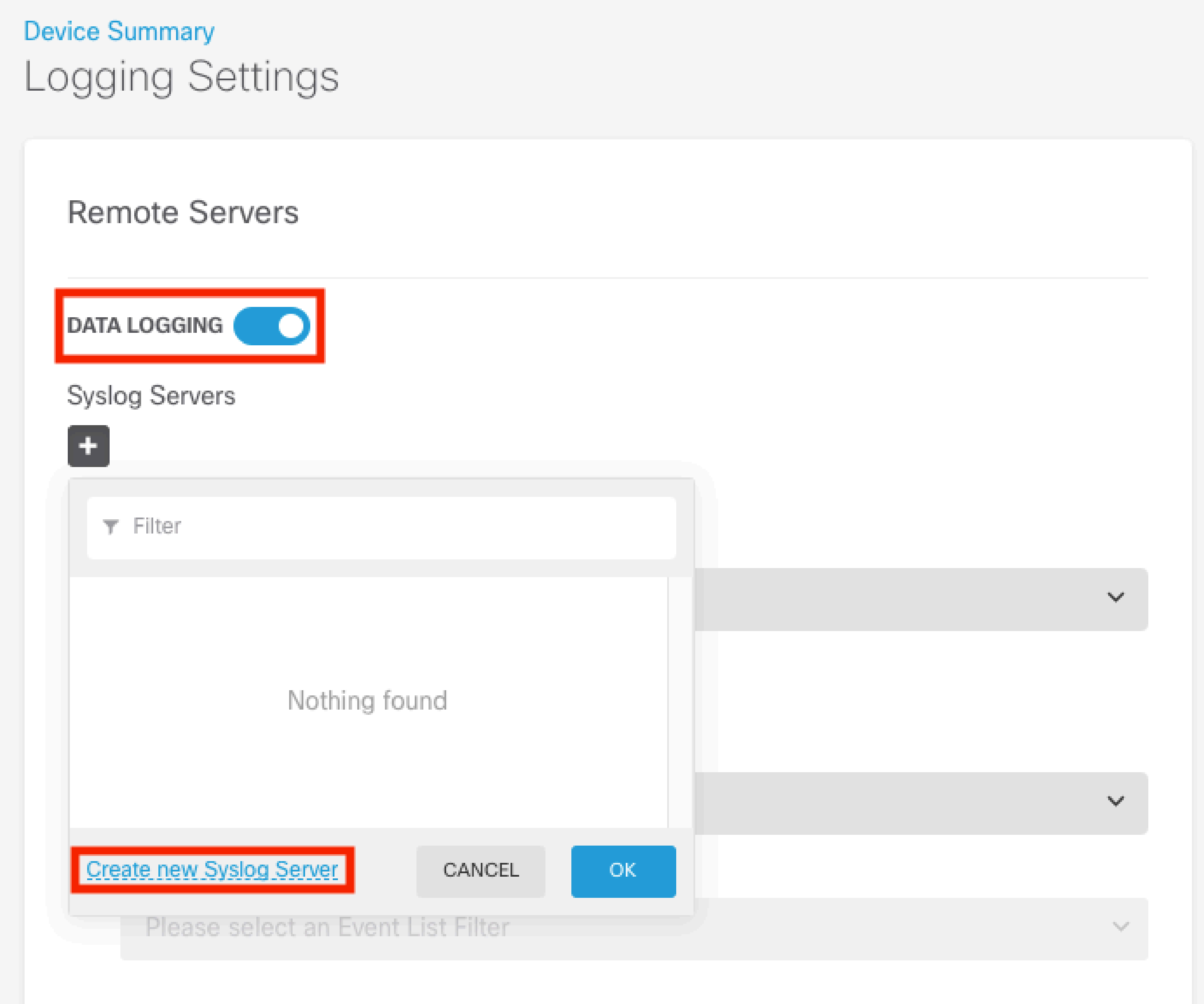
Severity level for filtering FXOS chassis syslogs
● Information

Message Filtering for Firepower Threat Defense
● Severity level for filtering all events
● Emergency
○ Custom Logging Filter
Please select an Event List Filter

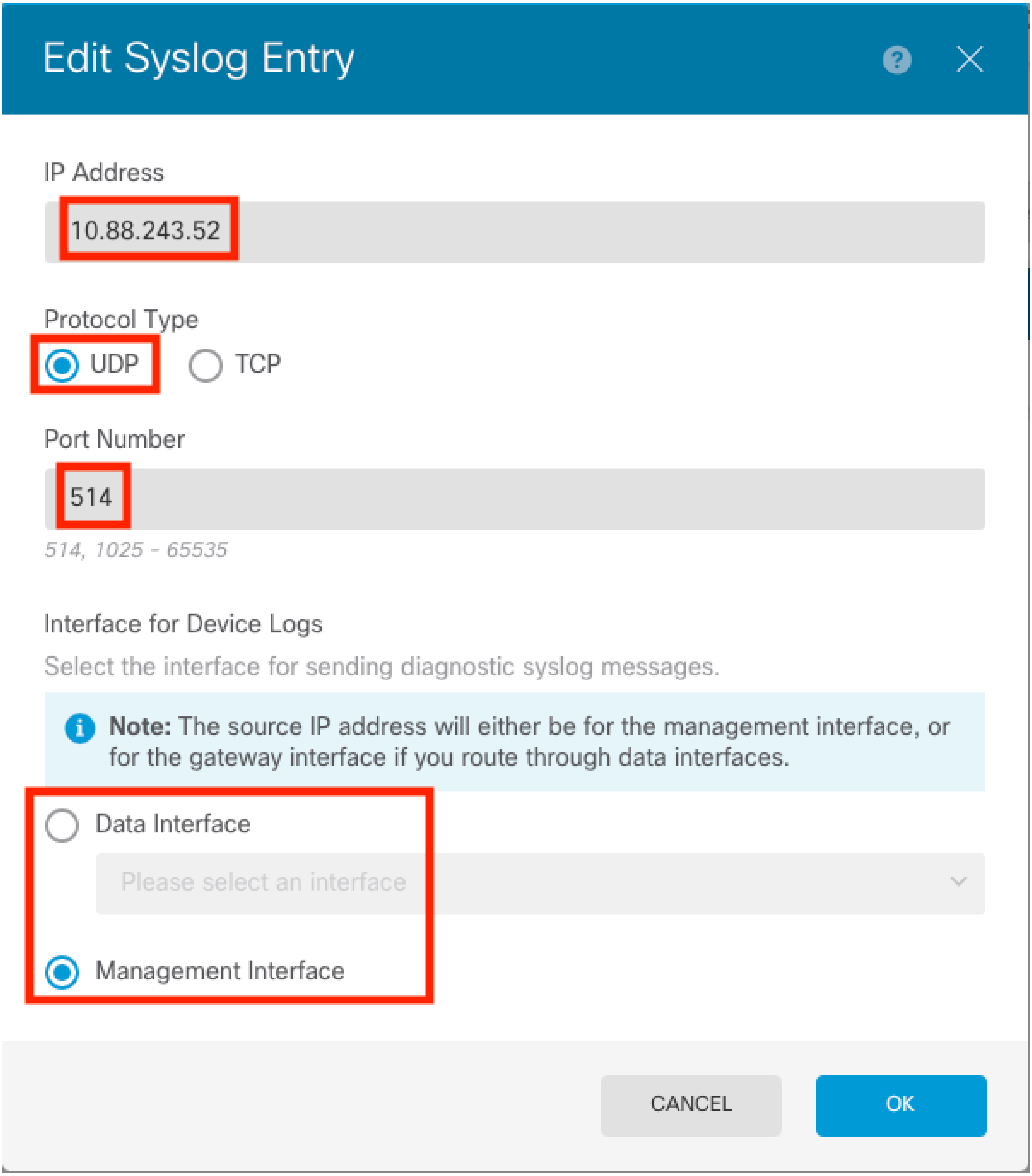
3단계. Syslog Servers(Syslog 서버) 아래에서 + 기호를 선택하여 데이터 로깅 토글 스위치를 설정합니다.

4단계. Add Syslog Server(Syslog 서버 추가)를 선택합니다. 또는 Objects - Syslog Servers(개체 -

Syslog 서버)에서 Syslog 서버 개체를 생성할 수 있습니다.



5단계. Syslog 서버의 IP 주소와 포트 번호를 입력합니다. Data Interface(데이터 인터페이스)의 라디오 버튼을 선택하고 OK(확인)를 선택합니다.



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.

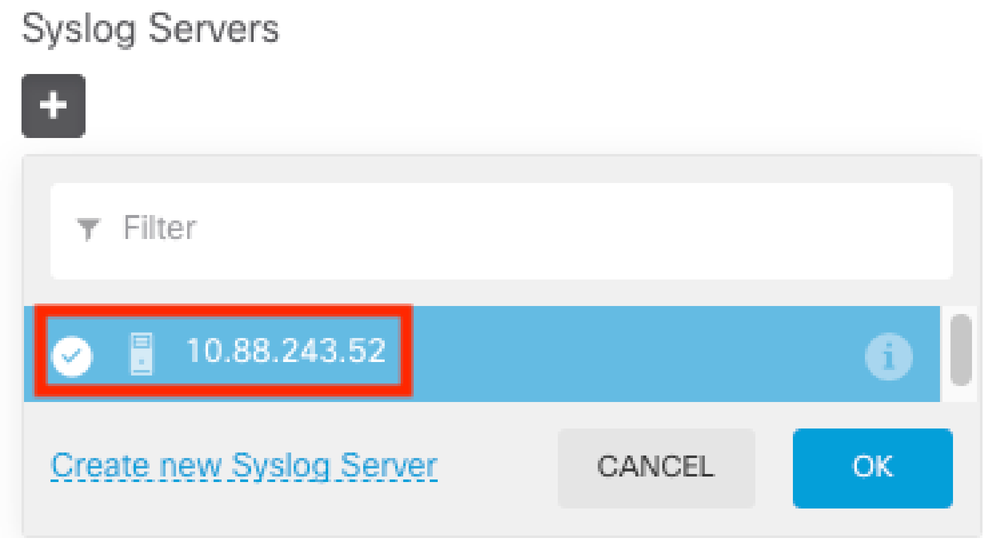
Note: The source IP address will either be for the management interface, or for the gateway interface if you route through data interfaces.

○ Data Interface

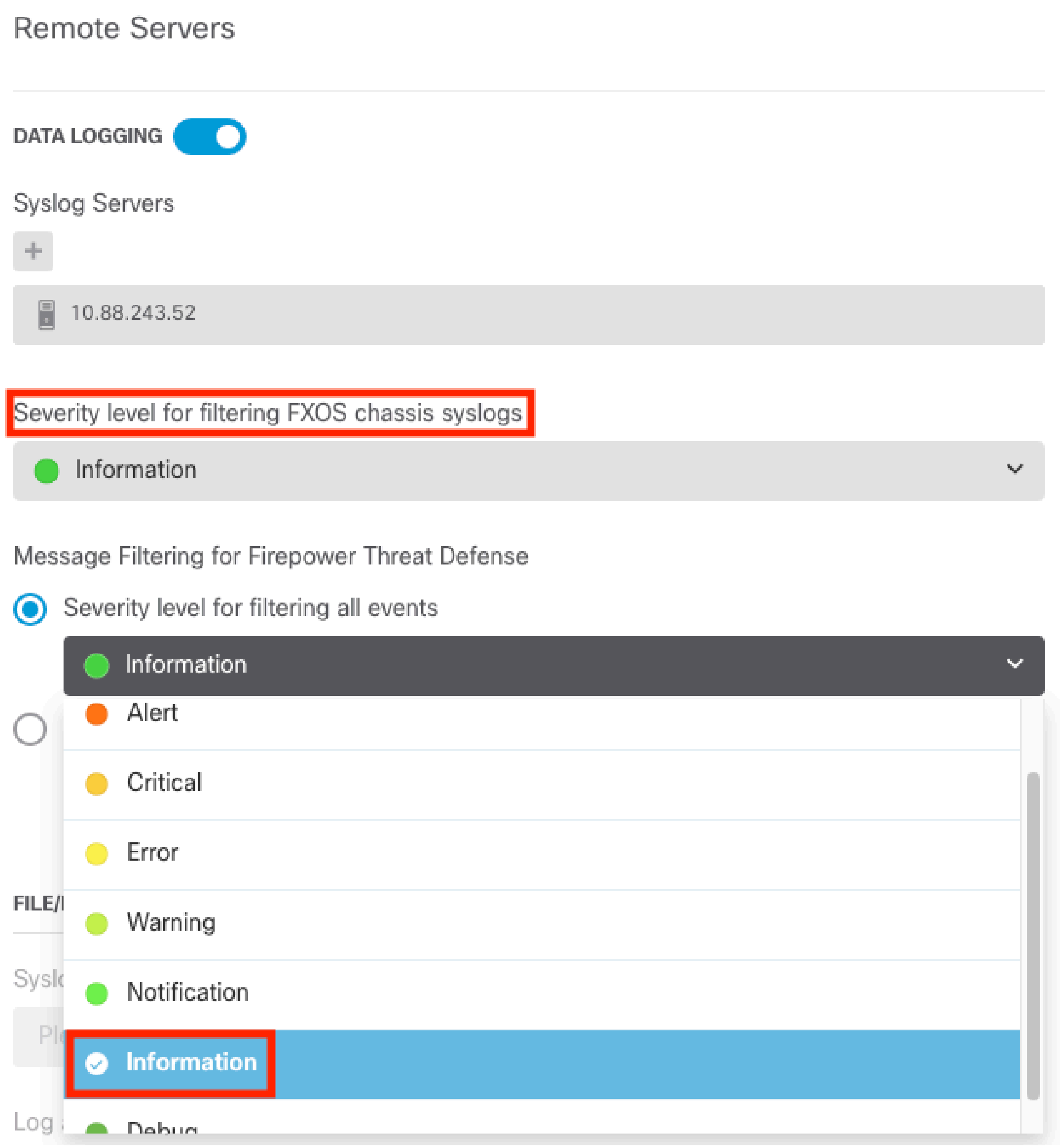
Please select an interface

● Management Interface

6단계. 그런 다음 새 Syslog 서버를 선택하고 OK를 선택합니다.



7단계. Severity level for filtering all events 라디오 버튼을 선택하고 원하는 로깅 수준을 선택합니다
.



Remote Servers

DATA LOGGING

Syslog Servers

+

10.88.243.52

Severity level for filtering FXOS chassis syslogs

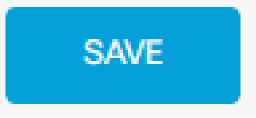
● Information

Message Filtering for Firepower Threat Defense

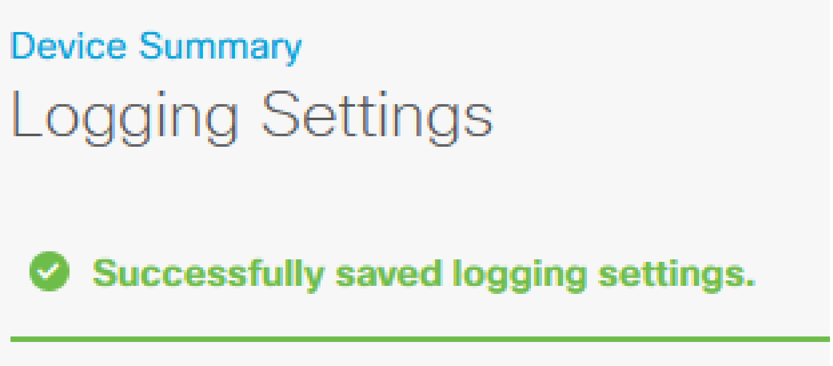
◉ Severity level for filtering all events

● Information

8단계. 화면 하단의 저장을 선택합니다.



9단계. 설정이 성공했는지 확인합니다.

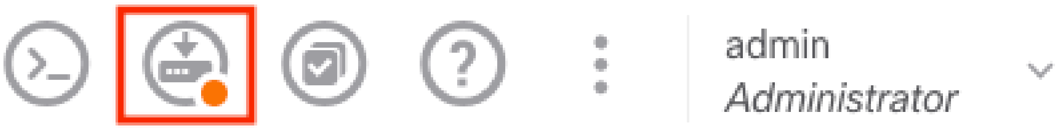


Device Summary

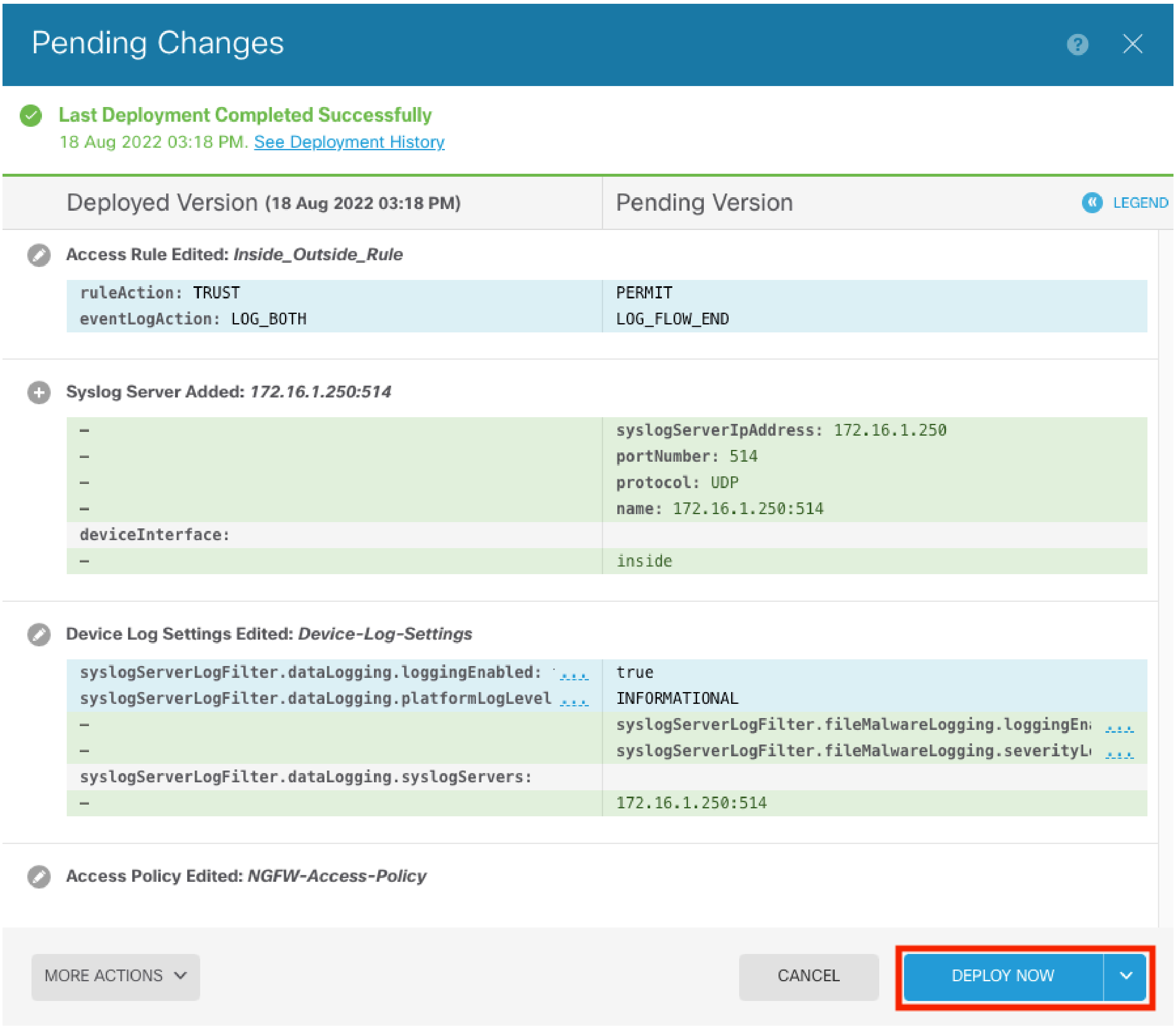
Logging Settings

Successfully saved logging settings.

10단계. 새 설정을 구축합니다.



및



Pending Changes

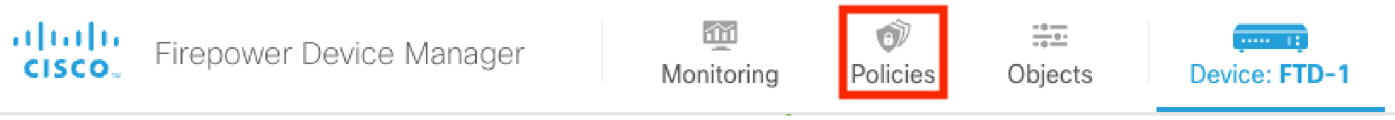
Last Deployment Completed Successfully
18 Aug 2022 03:18 PM. See Deployment History

Deployed Version (18 Aug 2022 03:18 PM)	Pending Version
Access Rule Edited: ***Inside_Outside_Rule***	
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: ***Device-Log-Settings***	
syslogServerLogFilter.dataLogging.loggingEnabled: ...	true
syslogServerLogFilter.dataLogging.platformLogLevel ...	INFORMATIONAL
–	syslogServerLogFilter.fileMalwareLogging.loggingEn ...
–	syslogServerLogFilter.fileMalwareLogging.severityL ...
syslogServerLogFilter.dataLogging.syslogServers:	
–	172.16.1.250:514
Access Policy Edited: ***NGFW-Access-Policy***	

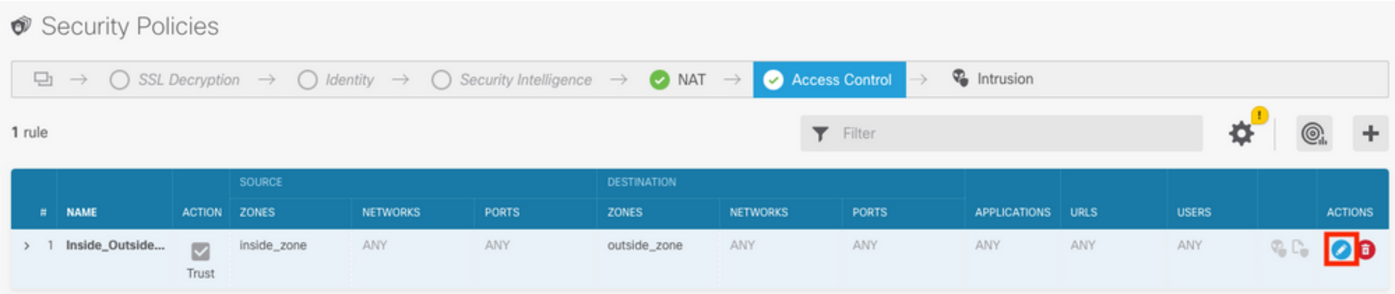
선택 사항.

또한 액세스 제어 정책 액세스 제어 규칙은 Syslog 서버에 로그인하도록 설정할 수 있습니다.

1단계. 화면 상단의 Policies(정책) 버튼을 클릭합니다.

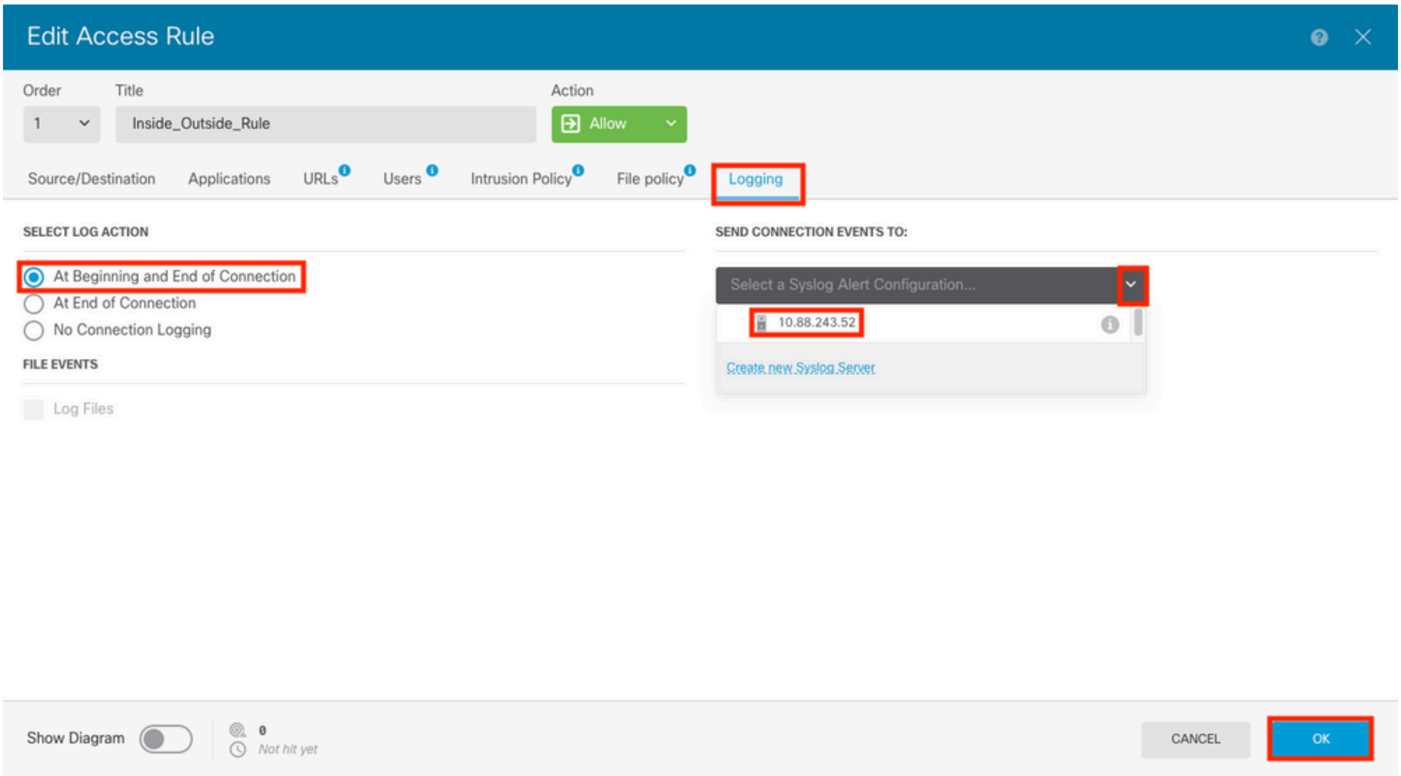


2단계. 로깅을 추가하려면 ACP 규칙의 오른쪽에 마우스 커서를 놓고 연필 아이콘을 선택합니다.



			SOURCE			DESTINATION						
#	NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS	APPLICATIONS	URLS	USERS	ACTIONS
1	Inside_Outside...	Trust	inside_zone	ANY	ANY	outside_zone	ANY	ANY	ANY	ANY	ANY	

3단계. Logging(로깅) 탭을 선택하고 At End of Connection(연결 종료 시)의 라디오 버튼을 선택한 다음 Select a Syslog Alert Configuration(Syslog 경고 컨피그레이션 선택) 아래의 드롭다운 화살표를 선택하고 Syslog Server(Syslog 서버)에서 Select(선택)를 선택한 다음 OK(확인)를 선택합니다.



Order: 1
Title: Inside_Outside_Rule
Action: Allow

SELECT LOG ACTION

● At Beginning and End of Connection
○ At End of Connection
○ No Connection Logging

FILE EVENTS

□ Log Files

SEND CONNECTION EVENTS TO:

Select a Syslog Alert Configuration...

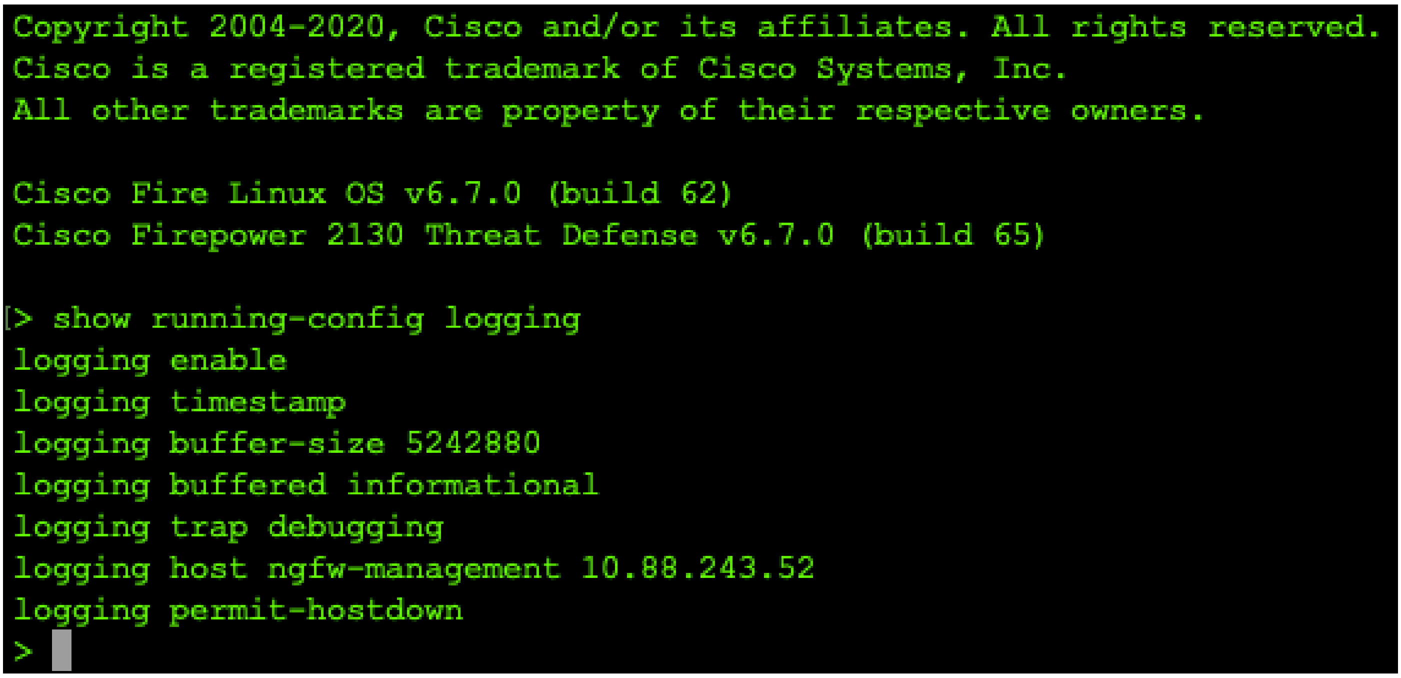
10.88.243.52

0
Not hit yet

4단계. 컨피그레이션 변경 사항을 구축합니다.

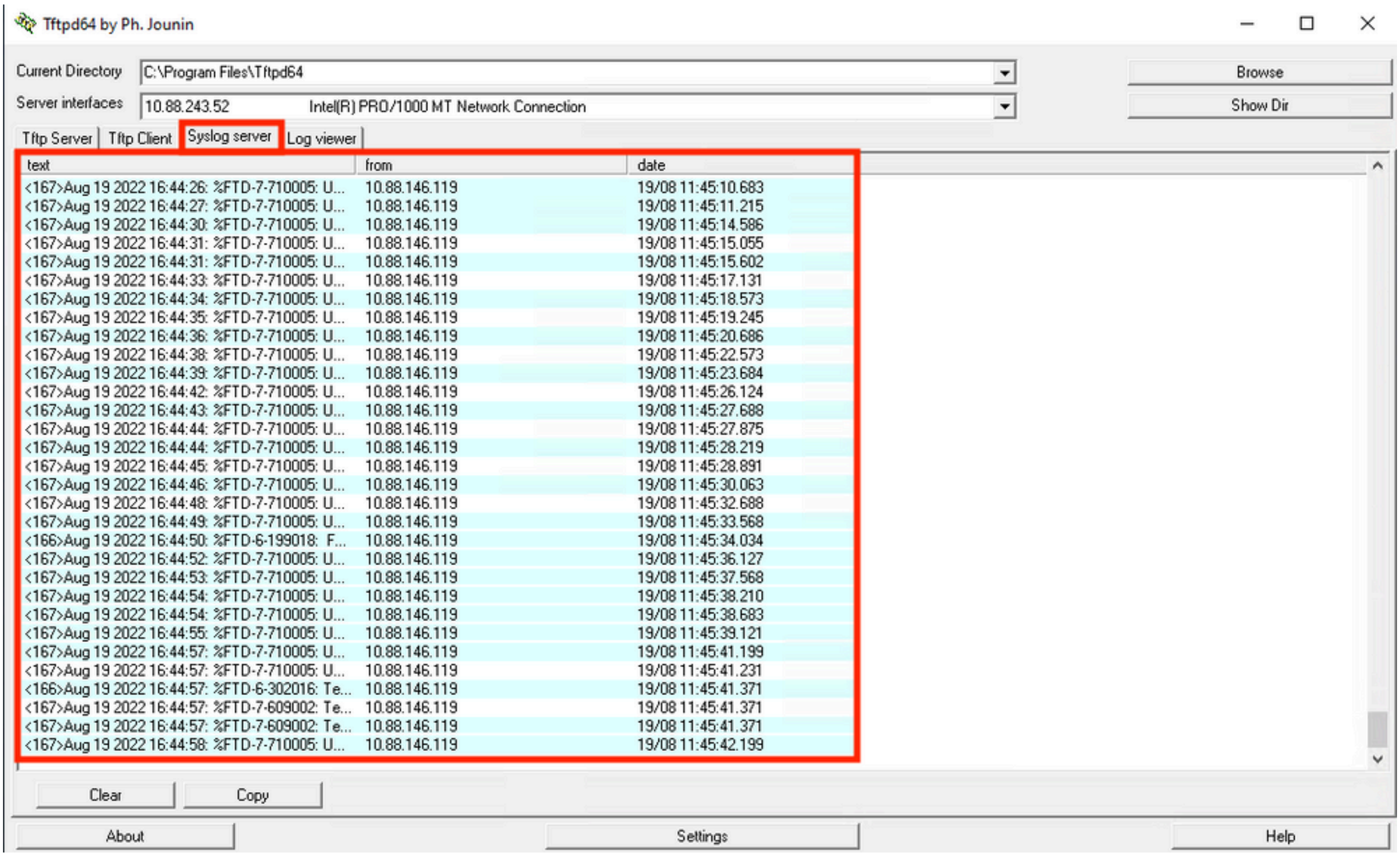
다음을 확인합니다.

1단계. 작업이 완료되면 show running-config logging 명령을 사용하여 FTD CLI Client Mode에서 **설정을** 확인할 수 있습니다.



```
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
>
```

2단계. Syslog 서버로 이동하여 Syslog 서버 애플리케이션이 Syslog 메시지를 수락하는지 확인합니다.



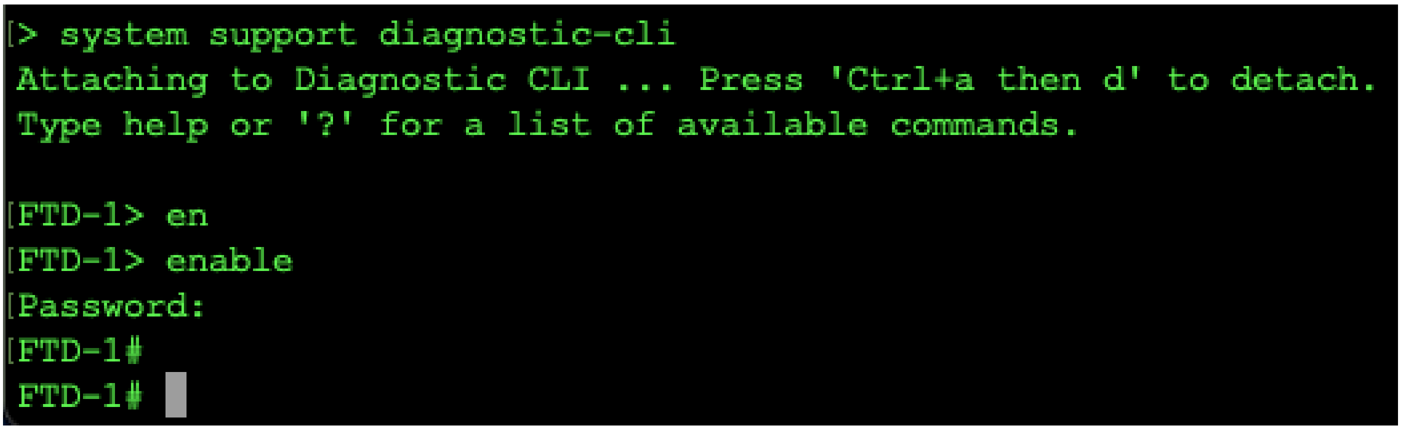
Current Directory: C:\Program Files\Tftpd64

Server interfaces: 10.88.243.52 Intel(R) PRO/1000 MT Network Connection

```
text                                        from           date
<167>Aug 19 2022 16:44:26: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:10.683
<167>Aug 19 2022 16:44:27: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:11.215
<167>Aug 19 2022 16:44:30: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:14.586
<167>Aug 19 2022 16:44:31: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:15.055
<167>Aug 19 2022 16:44:31: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:15.602
<167>Aug 19 2022 16:44:33: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:17.131
<167>Aug 19 2022 16:44:34: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:18.573
<167>Aug 19 2022 16:44:35: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:19.245
<167>Aug 19 2022 16:44:36: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:20.686
<167>Aug 19 2022 16:44:38: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:22.573
<167>Aug 19 2022 16:44:39: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:23.684
<167>Aug 19 2022 16:44:42: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:26.124
<167>Aug 19 2022 16:44:43: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:27.688
<167>Aug 19 2022 16:44:44: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:27.875
<167>Aug 19 2022 16:44:44: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:28.219
<167>Aug 19 2022 16:44:45: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:28.891
<167>Aug 19 2022 16:44:46: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:30.063
<167>Aug 19 2022 16:44:48: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:32.688
<167>Aug 19 2022 16:44:49: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:33.568
<166>Aug 19 2022 16:44:50: %FTD-6-199018:  F...  10.88.146.119  19/08 11:45:34.034
<167>Aug 19 2022 16:44:52: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:36.127
<167>Aug 19 2022 16:44:53: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:37.568
<167>Aug 19 2022 16:44:54: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:38.210
<167>Aug 19 2022 16:44:54: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:38.683
<167>Aug 19 2022 16:44:55: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:39.121
<167>Aug 19 2022 16:44:57: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:41.199
<167>Aug 19 2022 16:44:57: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:41.231
<166>Aug 19 2022 16:44:57: %FTD-6-302016: Te... 10.88.146.119  19/08 11:45:41.371
<167>Aug 19 2022 16:44:57: %FTD-7-609002: Te... 10.88.146.119  19/08 11:45:41.371
<167>Aug 19 2022 16:44:57: %FTD-7-609002: Te... 10.88.146.119  19/08 11:45:41.371
<167>Aug 19 2022 16:44:58: %FTD-7-710005: U...  10.88.146.119  19/08 11:45:42.199
```

문제 해결

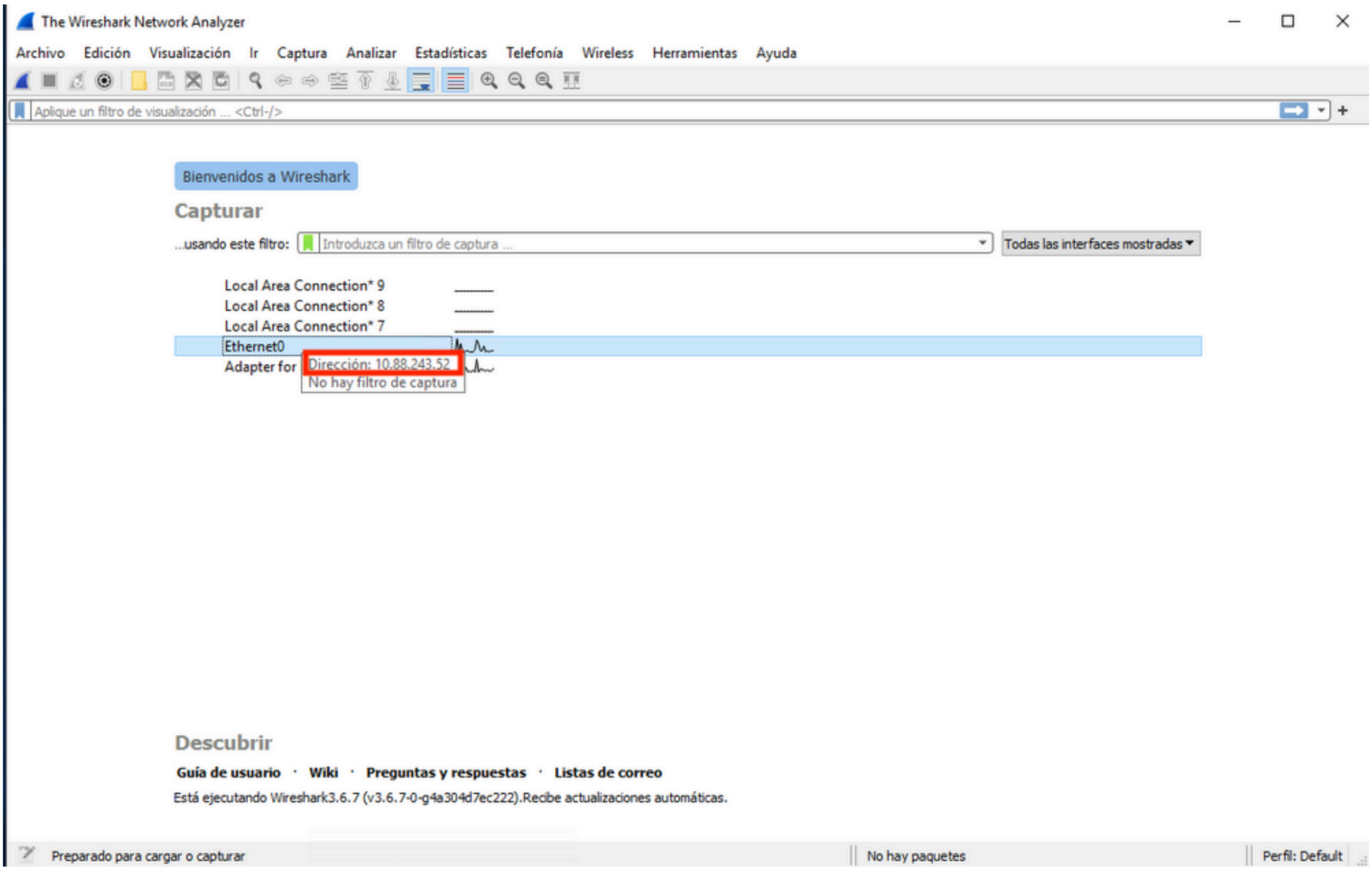
1단계. Syslog 애플리케이션의 Syslog 메시지에서 메시지가 생성되는 경우, FTD CLI에서 패킷 캡처를 수행하여 패킷을 확인합니다. Clish 프롬프트에서 **system support diagnostic-cli 명령을** 입력하여 **Clish 모드**에서 LINA로 변경합니다.



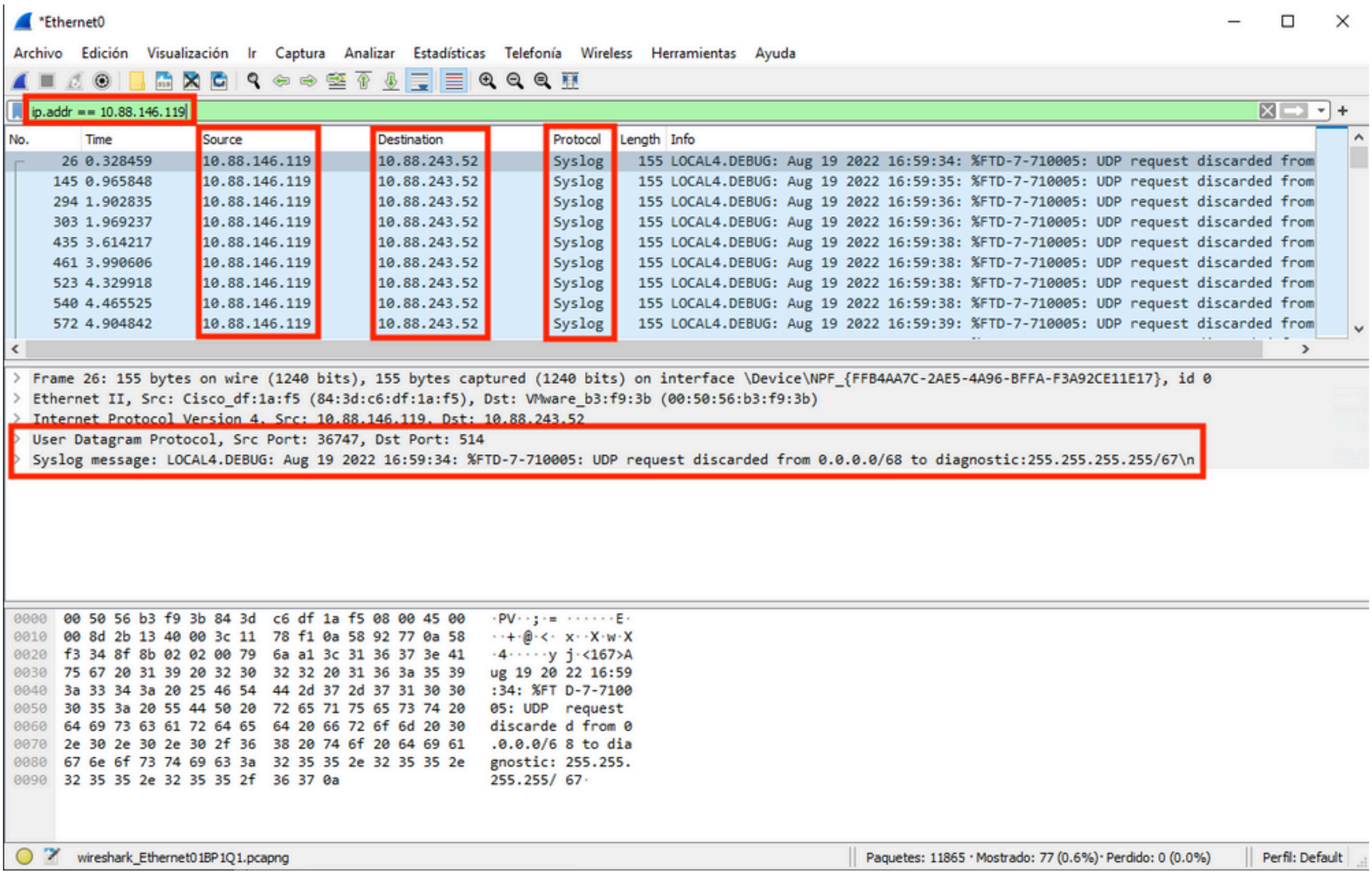
```
[> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

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

2단계. udp 514(또는 tcp를 사용한 경우 tcp 1468)에 대해 하나의 패킷 캡처를 생성합니다.

3단계. 통신이 Syslog 서버의 네트워크 인터페이스 카드에 연결되었는지 확인합니다. 로드된 Wireshark 또는 다른 패킷 캡처 유틸리티를 사용합니다. Wireshark에서 Syslog 서버에 대한 인터페이스를 두 번 클릭하여 패킷 캡처를 시작합니다.


The Wireshark Network Analyzer
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
Aplique un filtro de visualización ... <Ctrl-/>
Bienvenidos a Wireshark
Capturar
...usando este filtro:
Introduzca un filtro de captura ...
Todas las interfaces mostradas
Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 7
Ethernet0
Adapter for
Dirección: 10.88.243.52
No hay filtro de captura
Descubrir
Guía de usuario · Wiki · Preguntas y respuestas · Listas de correo
Está ejecutando Wireshark3.6.7 (v3.6.7-0-g4a304d7ec222).Recibe actualizaciones automáticas.
Preparado para cargar o capturar
No hay paquetes
Perfil: Default

4단계. udp.port==514를 입력하고 막대 오른쪽에 있는 화살표를 선택하여 udp 514의 상단 막대에 표시 필터를 설정합니다. 출력에서 패킷이 Syslog 서버에 도착하는지 확인합니다.



```
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

5단계. Syslog 서버 응용 프로그램에서 데이터를 표시하지 않는 경우 Syslog 서버 응용 프로그램 내의 설정 문제를 해결합니다. 올바른 프로토콜이 udp/tcp 및 올바른 포트 514/1468을 사용하고 있는지 확인합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.