在Firepower设备管理器中配置并验证系统日志

目录

简介

本文档介绍如何在Firepower设备管理器(FDM)中配置系统日志。

先决条件

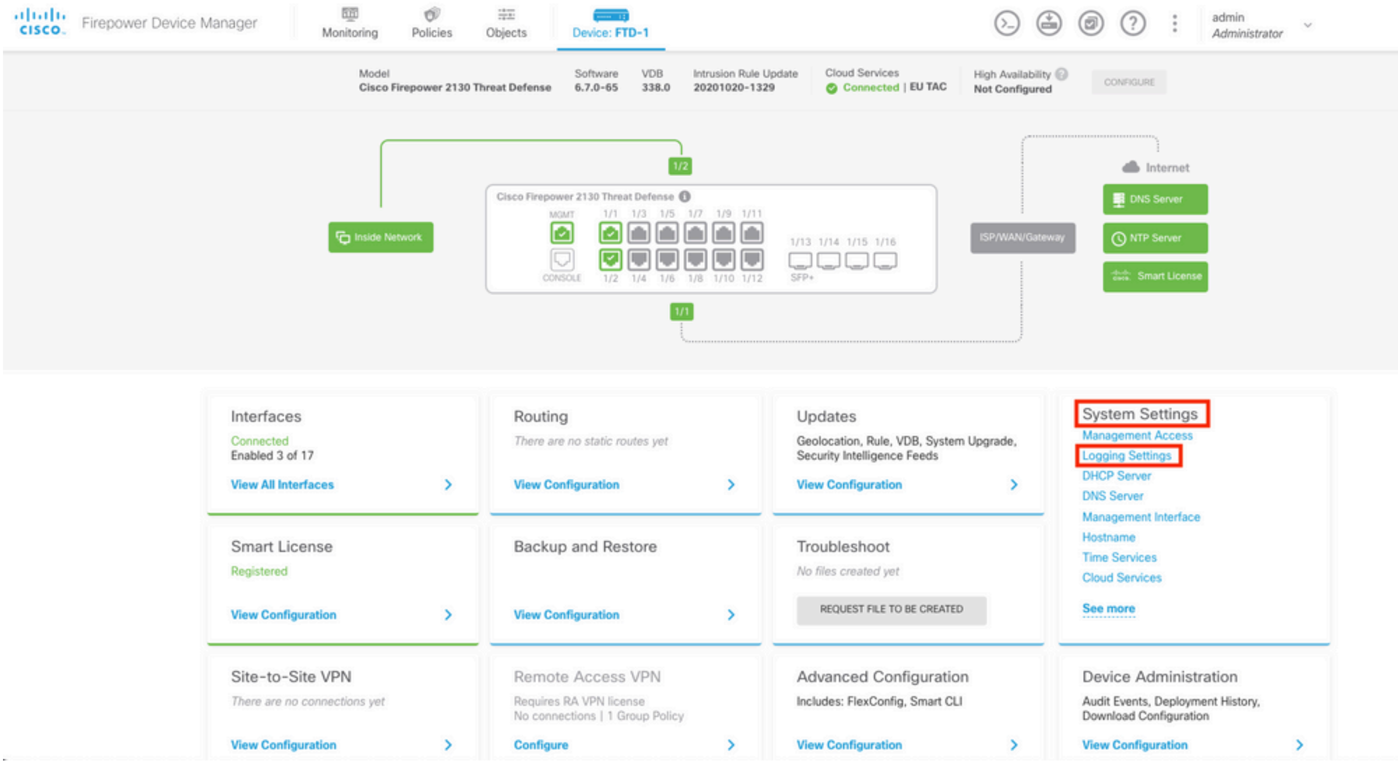
要求

Cisco 建议您了解以下主题：

- Firepower威胁防御
- 运行Syslog软件以收集数据的Syslog服务器

配置

步骤1:在Firepower设备管理器主屏幕中，选择屏幕右下角System Settings下的Logging Settings。



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

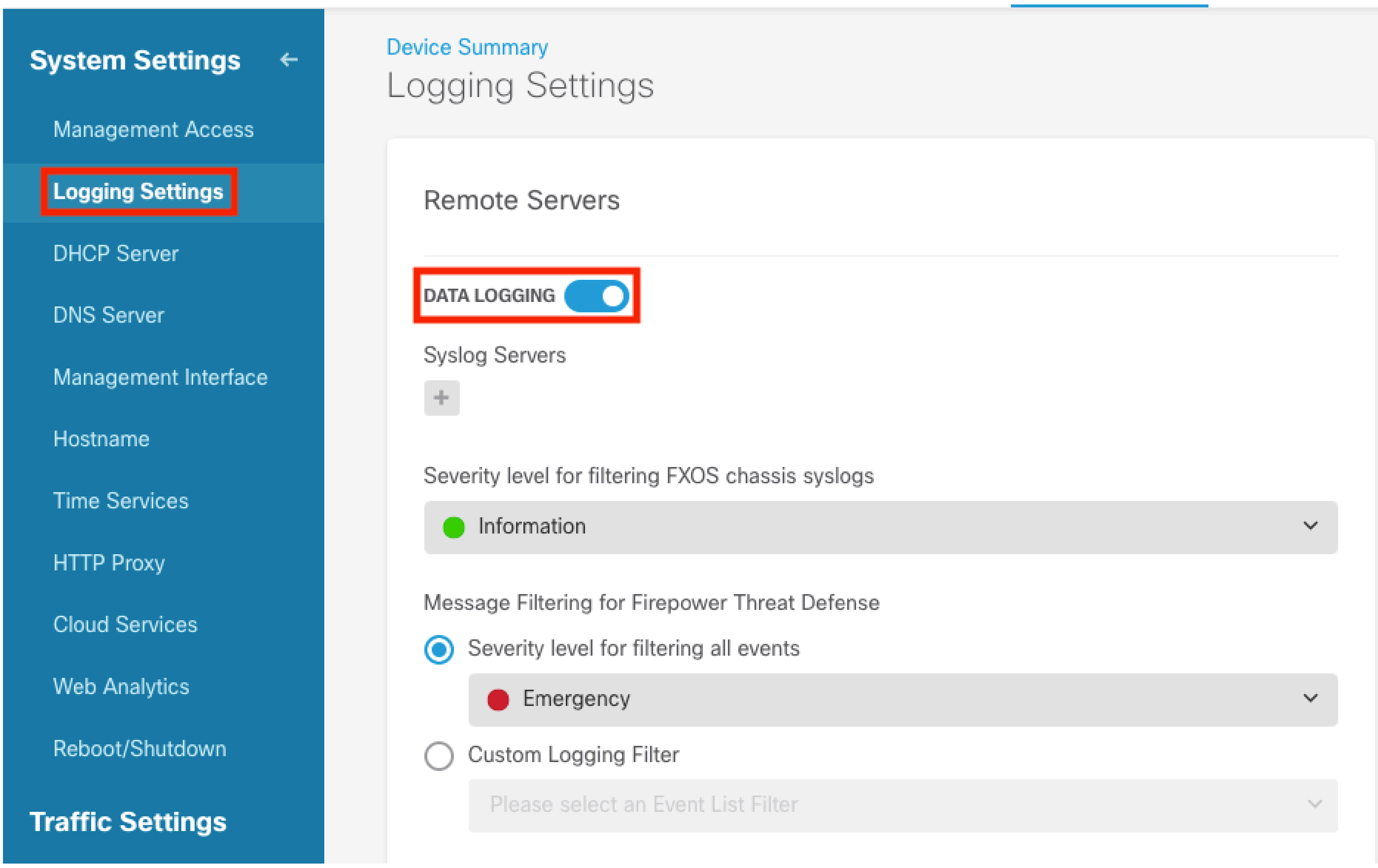
Site-to-Site VPN
There are no connections yet
View Configuration

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

第二步：在“系统设置”屏幕上，选择左侧菜单中的“日志记录设置”。



Device Summary
Logging Settings

Remote Servers

DATA LOGGING ●

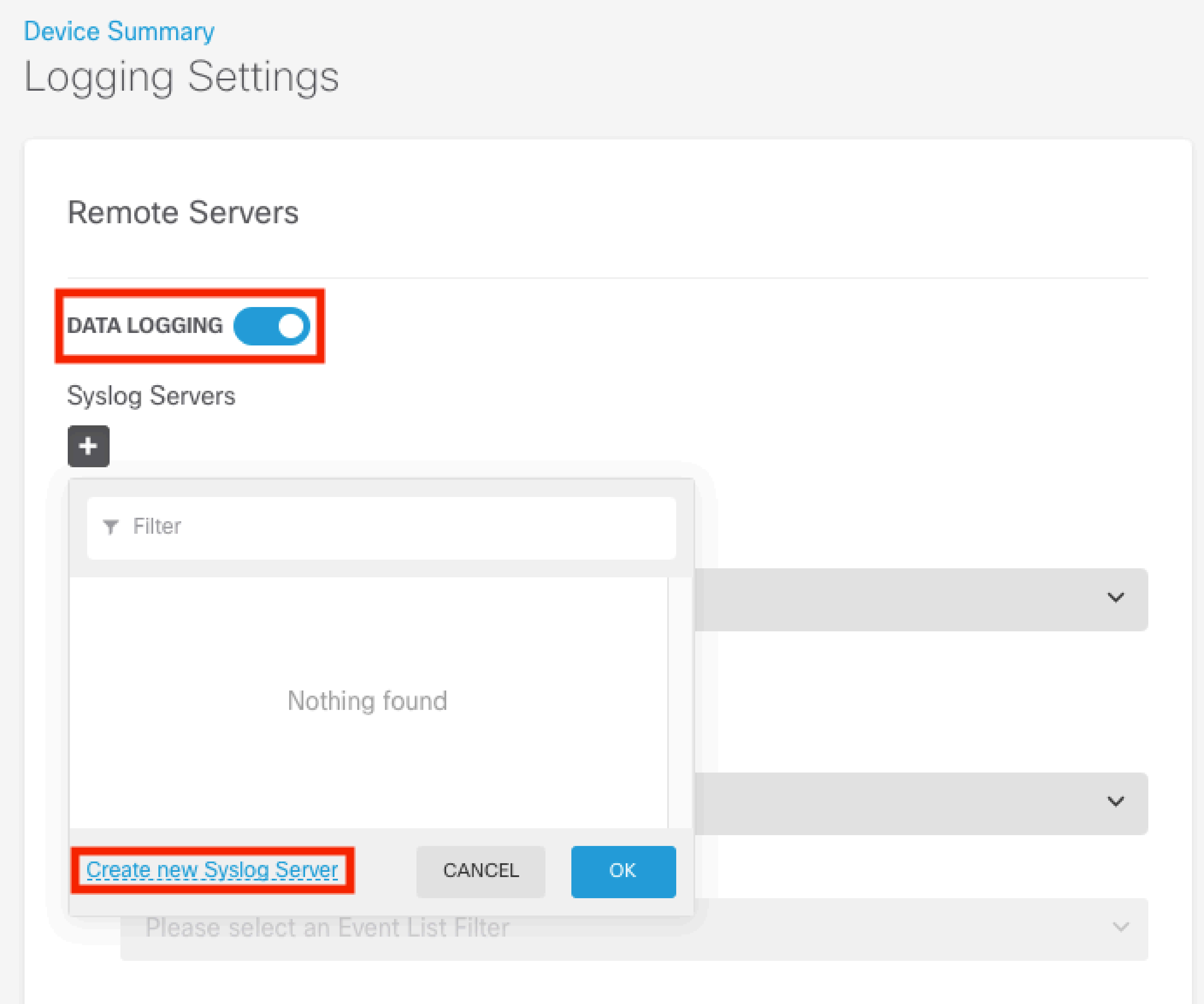
Syslog Servers
+

Severity level for filtering FXOS chassis syslogs
● Information

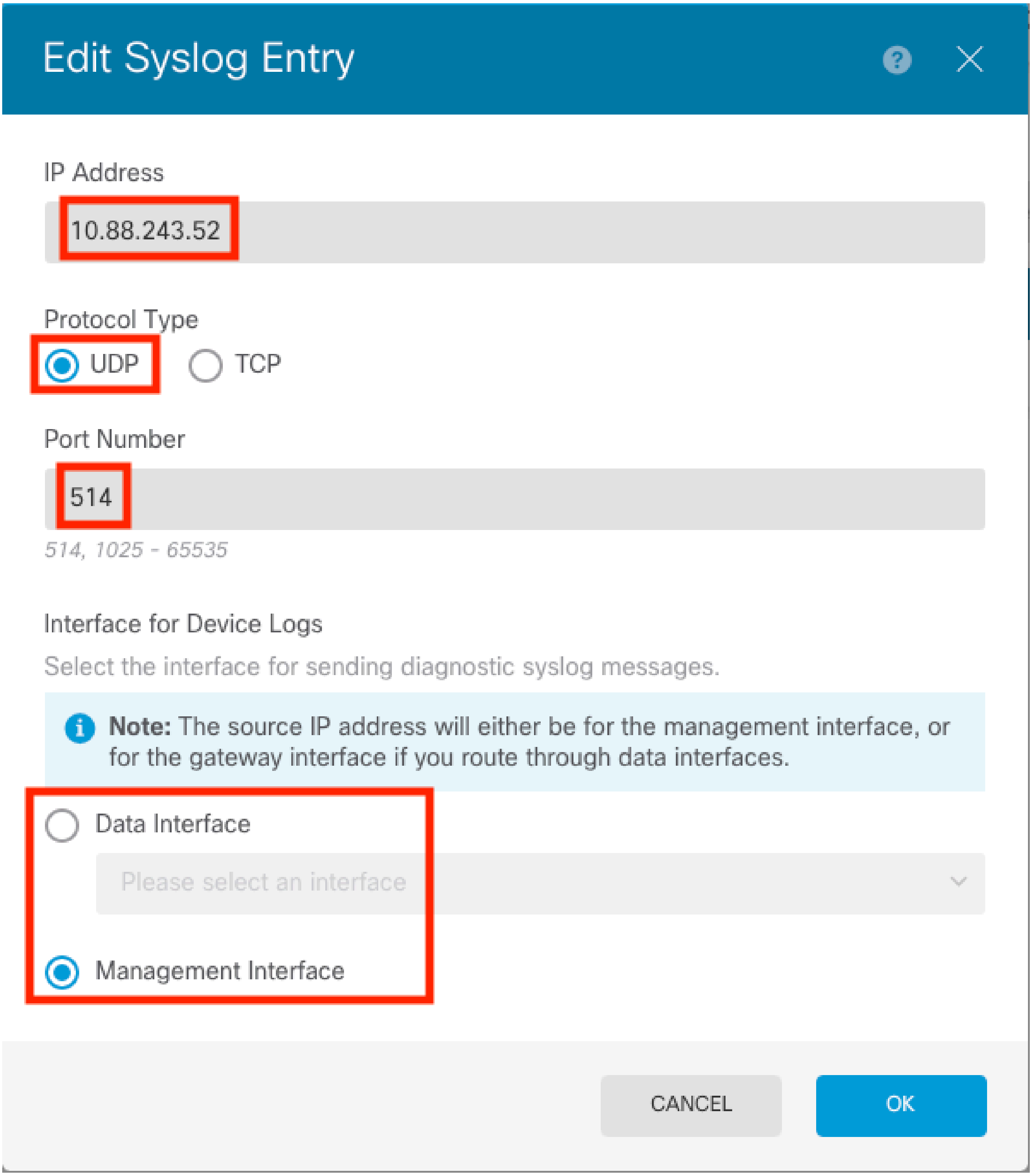
Message Filtering for Firepower Threat Defense
● Severity level for filtering all events
● Emergency
○ Custom Logging Filter
Please select an Event List Filter

第三步：选择Syslog Servers下的+号设置Data Logging切换开关。

第四步：选择Add Syslog Server。或者，您可以在Objects - Syslog Servers中创建系统日志服务器对象。



第五步：输入系统日志服务器的IP地址和端口号。选择“数据接口”的单选按钮，然后选择“确定”。



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.

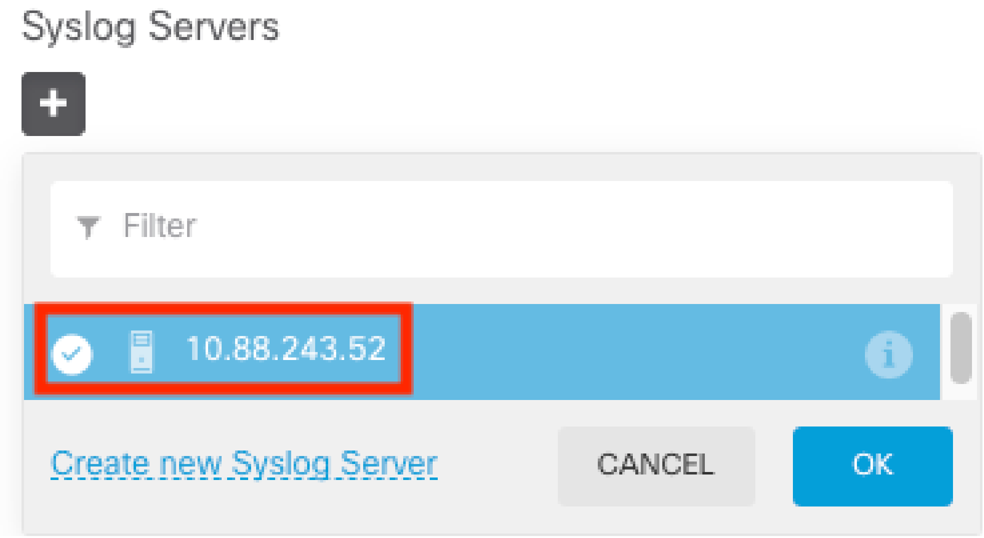
Note: The source IP address will either be for the management interface, or for the gateway interface if you route through data interfaces.

○ Data Interface

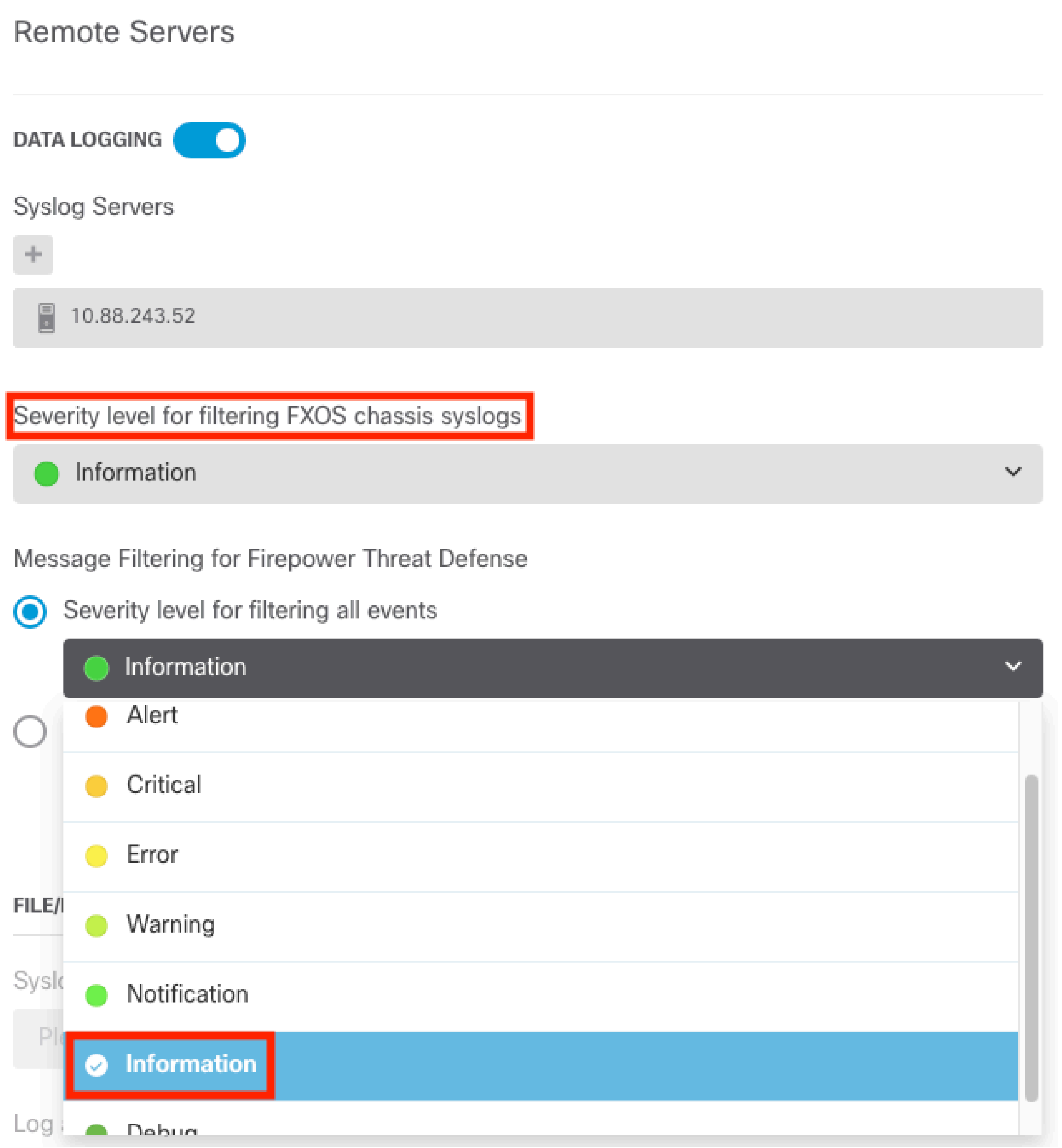
Please select an interface

● Management Interface

第六步：接下来，选择新的Syslog服务器，然后选择OK。



步骤 7.选择Severity level for filtering all events单选按钮并选择所需的日志记录级别。



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

FILE/I

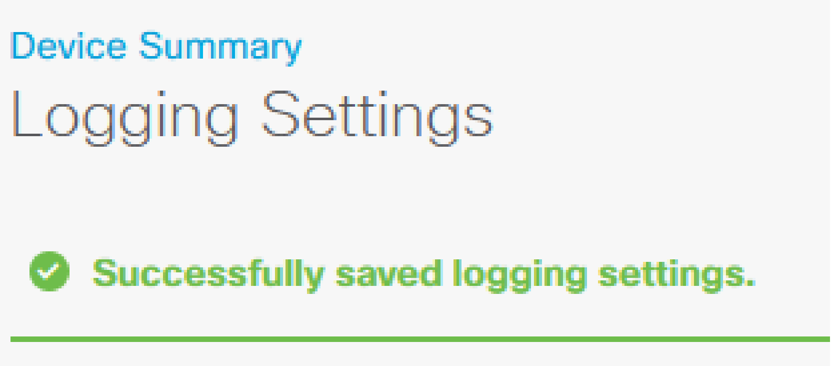
Sysl

Pl

Log

步骤 8选择屏幕底部的Save。

步骤 9验证设置是否成功。

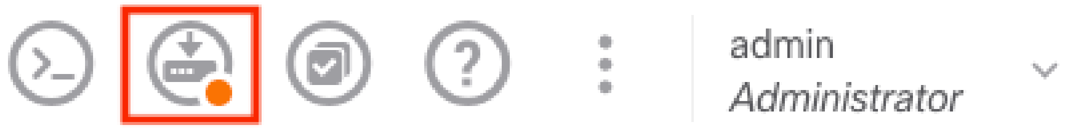


Device Summary

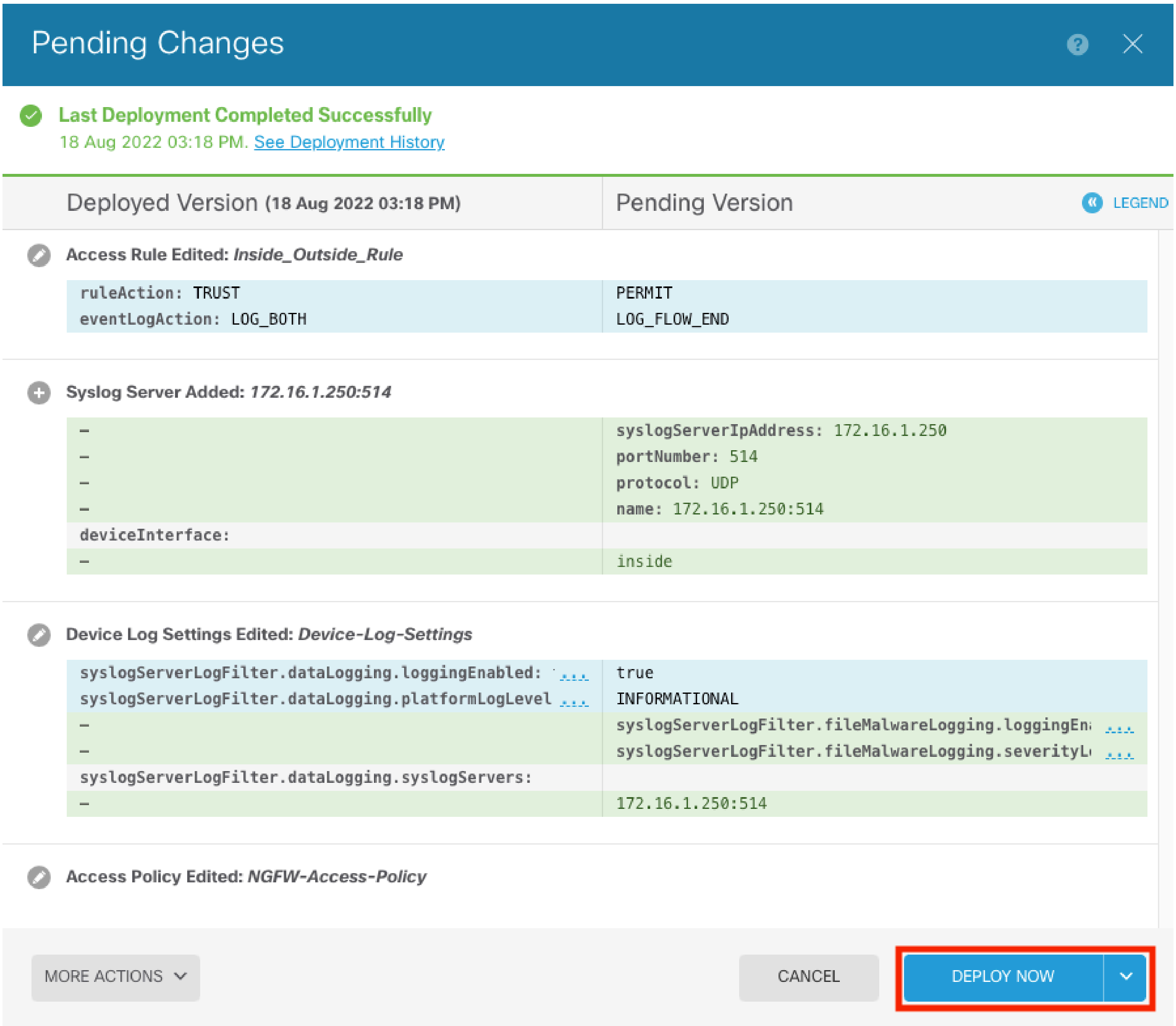
Logging Settings

Successfully saved logging settings.

步骤 10部署新设置。



和



Pending Changes

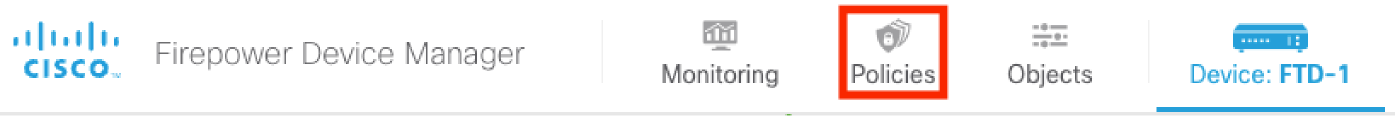
Last Deployment Completed Successfully
18 Aug 2022 03:18 PM. See Deployment History

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***	

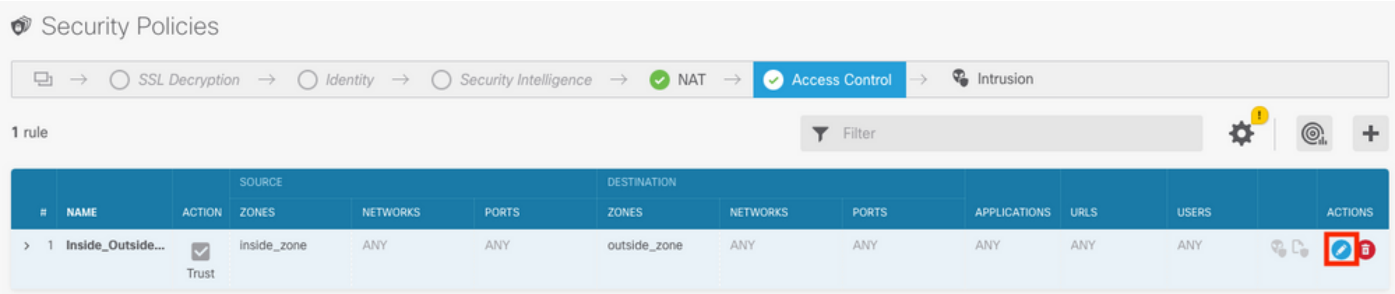
可选。

此外，可以将访问控制策略访问控制规则设置为登录系统日志服务器：

步骤1:点击屏幕顶部的Policies（策略）按钮。



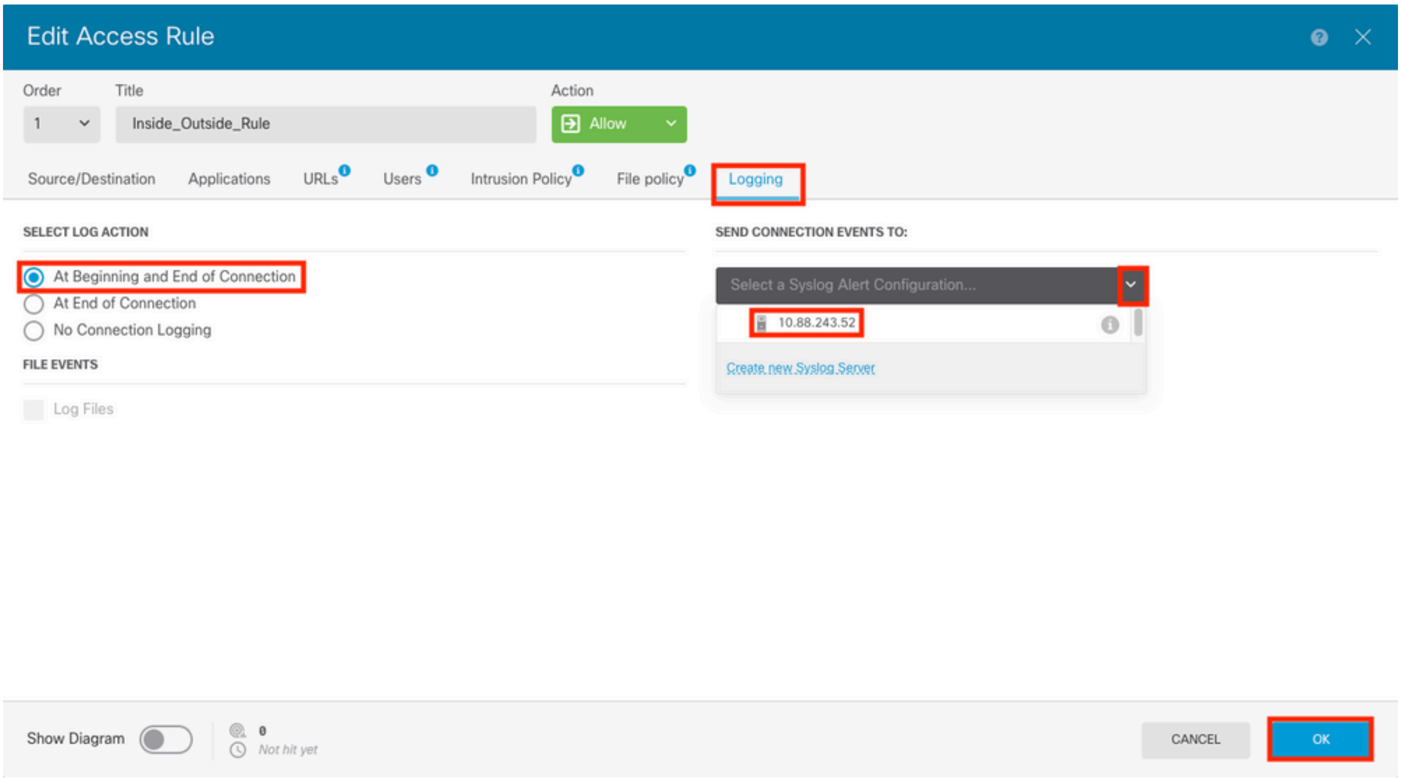
第二步： 将鼠标悬停在ACP规则的右侧以添加日志记录并选择铅笔图标。


Security Policies
SSL Decryption → Identity → Security Intelligence → NAT → Access Control → Intrusion
Filter

1 rule

			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	

第三步：选择Logging选项卡，选择At End of Connection的单选按钮，选择Select a Syslog Alert Configuration下的下拉箭头，在Syslog Server上选择，然后选择OK。



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:

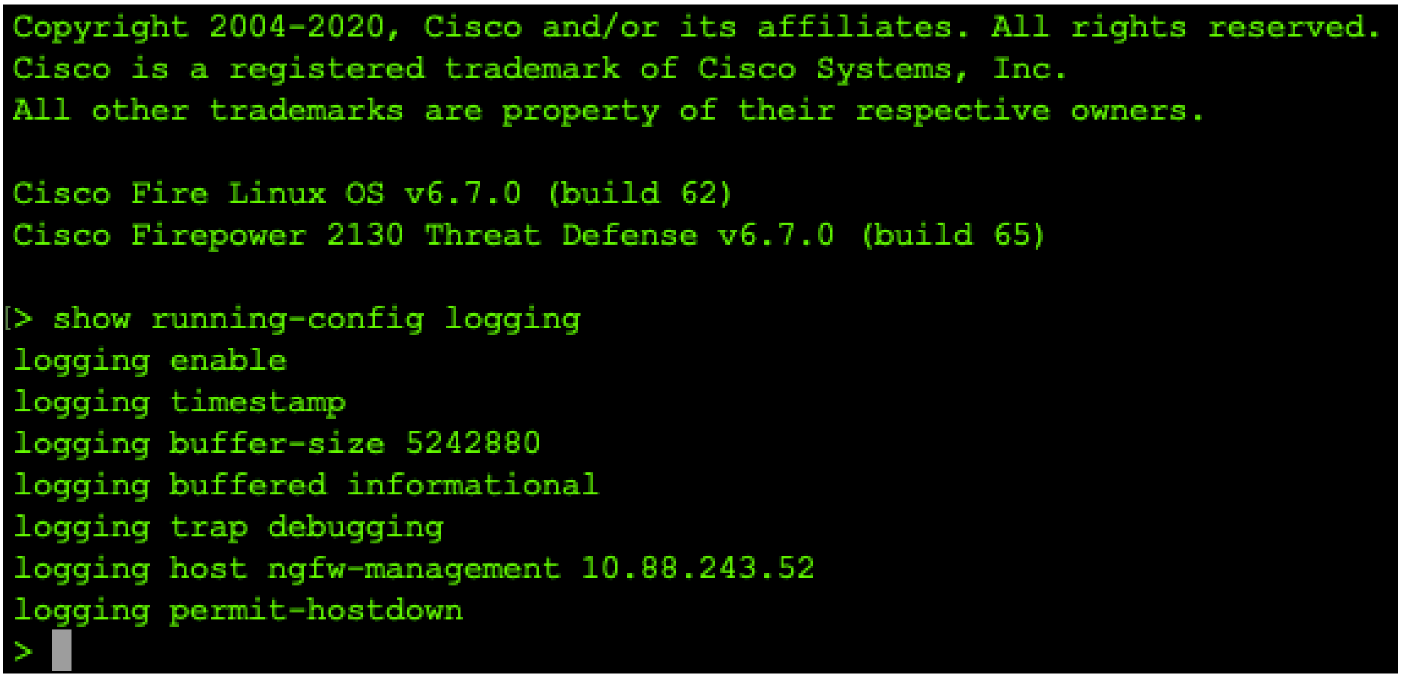
Select a Syslog Alert Configuration...
10.88.243.52
Create new Syslog Server

Show Diagram
0 Not hit yet

第四步：部署配置更改。

验证

步骤1:任务完成后，可以使用show running-config logging命令检验FTD CLI清除模式中的设置。

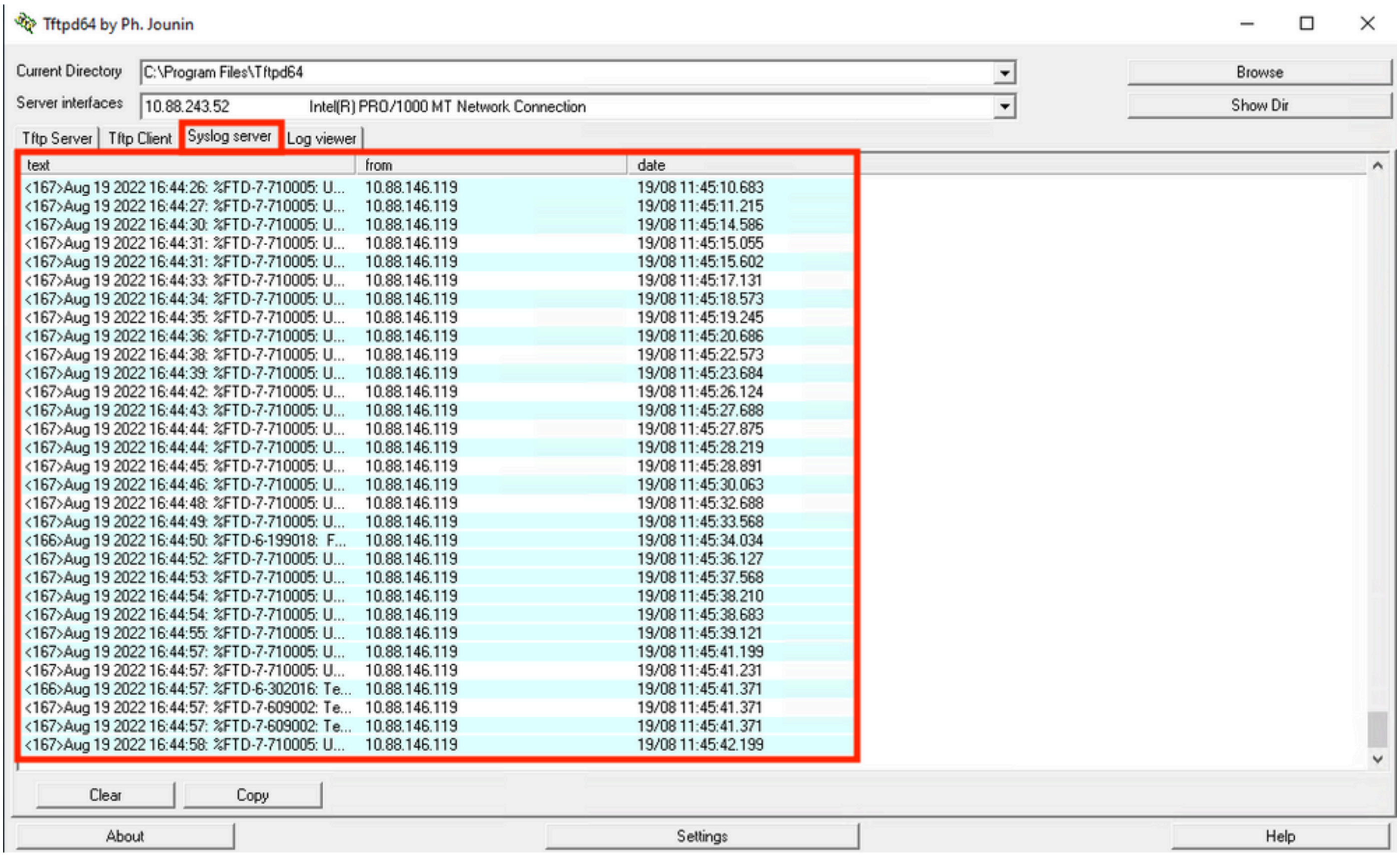


```
Copyright 2004-2020, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

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
>
```

第二步：导航到Syslog服务器并验证Syslog服务器应用程序是否接受Syslog消息。



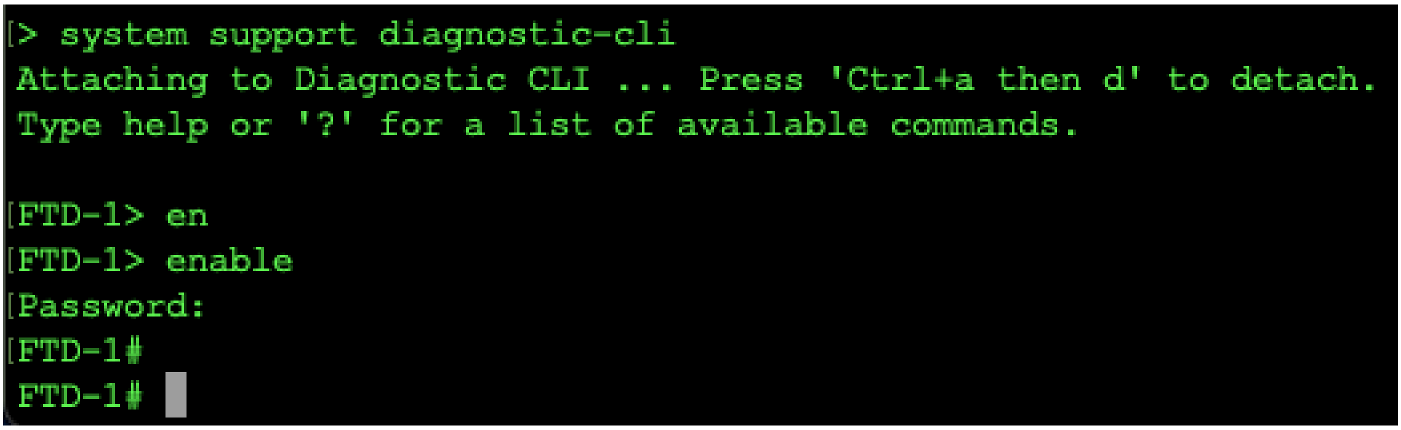
Current Directory: C:\Program Files\Tftpd64

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

故障排除

步骤1:如果Syslog应用程序上的Syslog消息生成任何消息，请从FTD CLI执行数据包捕获以检查数据包。在clish提示符后输入**system support diagnostic-cli**命令，从Clish模式更改为LINA。

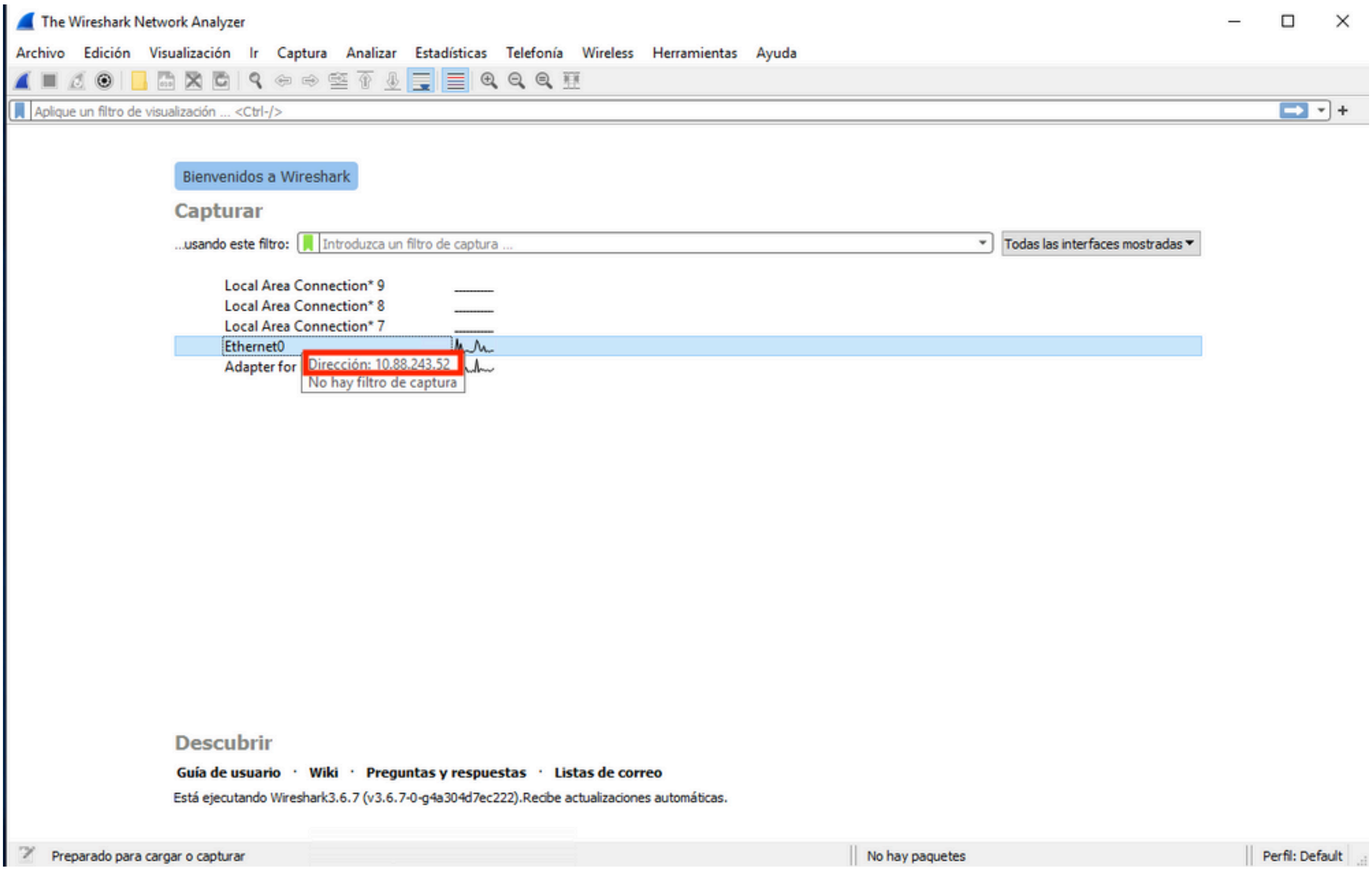


```
[> system support diagnostic-cli
 Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
 Type help or '?' for a list of available commands.

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

第二步：为udp 514创建一个数据包捕获（如果使用tcp，则为tcp 1468）

第三步：验证通信是否正在进行到Syslog服务器上的网络接口卡。使用Wireshark或加载的其他数据包捕获实用程序。双击Wireshark中的接口，让系统日志服务器开始捕获数据包。


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
Todas las interfaces mostradas
Descubrir
Guía de usuario · Wiki · Preguntas y respuestas · Listas de correo

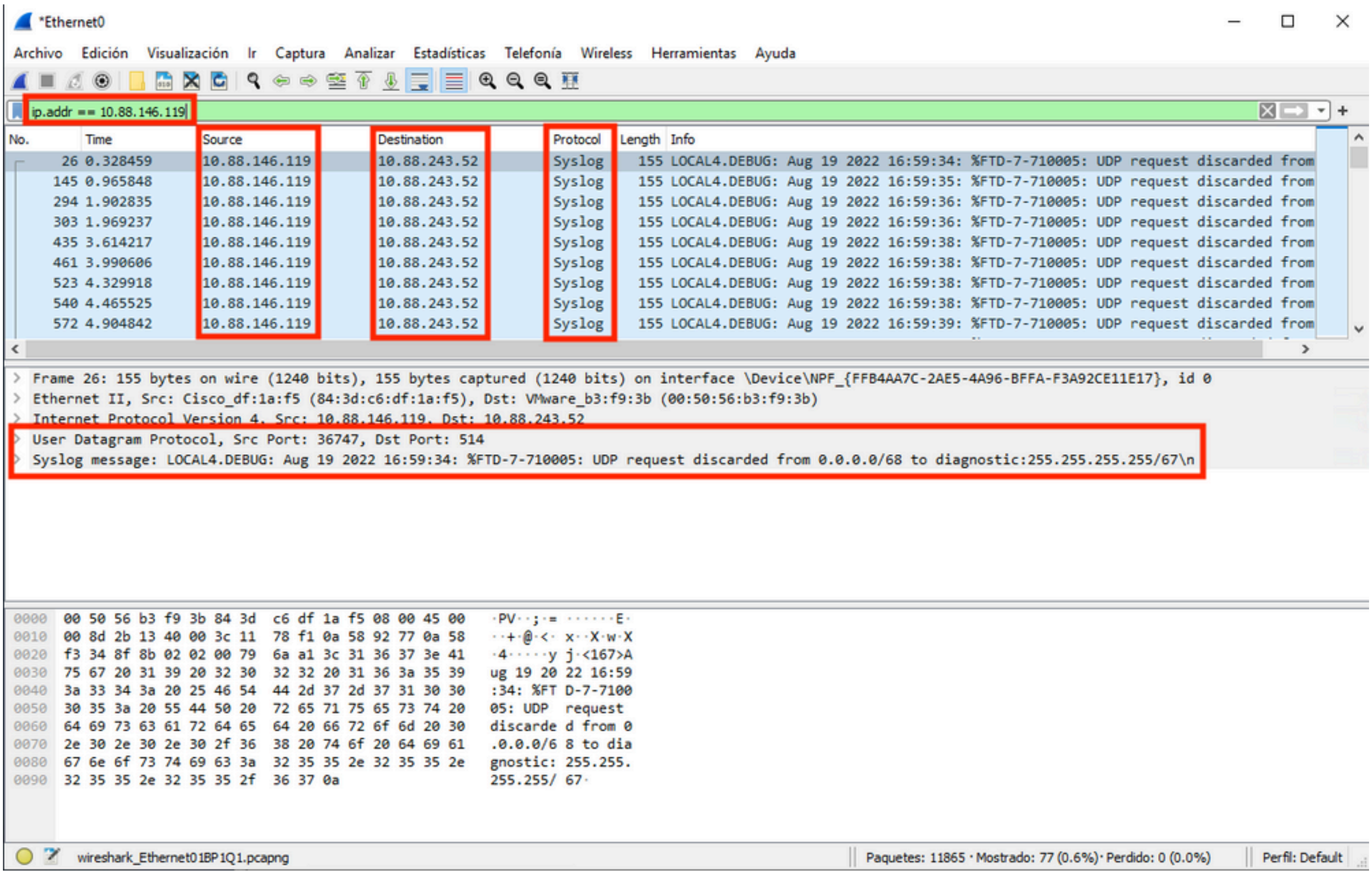
...usando este filtro: Introduzca un filtro de captura ...

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

Está ejecutando Wireshark3.6.7 (v3.6.7-0-g4a304d7ec222).Recibe actualizaciones automáticas.

Preparado para cargar o capturar | No hay paquetes | Perfil: Default

第四步：键入udp.port==514并选择顶部栏右侧的箭头，在顶部栏中为udp 514设置显示过滤器。从输出中，确认数据包是否正在发送到Syslog服务器。


*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
```

第五步：如果Syslog服务器应用程序未显示数据，请排除Syslog服务器应用程序中的设置故障。确保使用的是正确的udp/tcp协议和正确的端口514/1468。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。