

Configure and Verify Syslog in Firepower Device Manager

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Configurations](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes how to configure Syslog within the Firepower Device Manager (FDM).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Firepower Threat Defense
- Syslog Server running Syslog Software to collect data

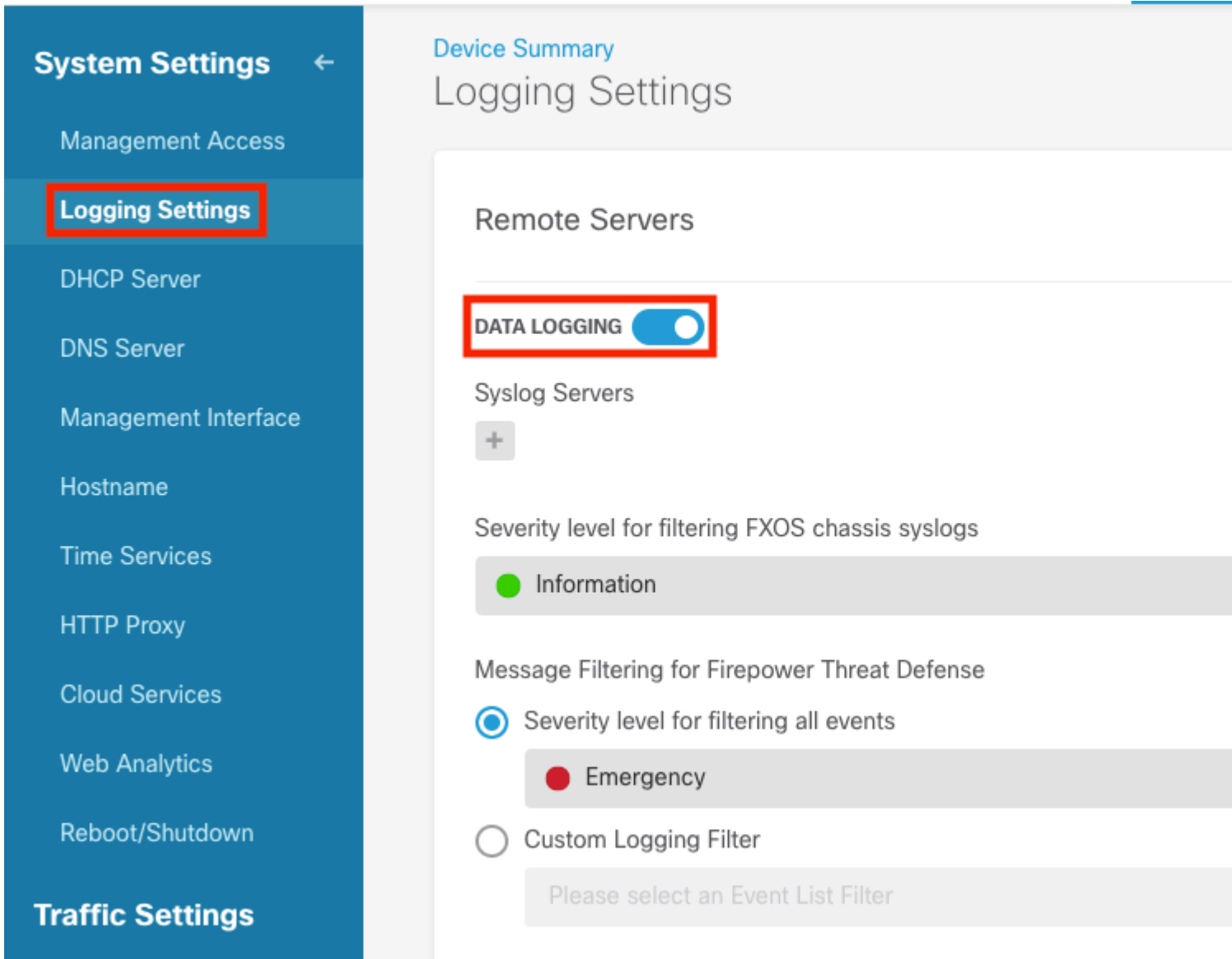
Configurations

Step 1. From the Main Firepower Device Manager screen, select the Logging Settings under the System Settings in the lower right-hand corner of the screen.



Interfaces Connected Enabled 3 of 17 View All Interfaces	Routing <i>There are no static routes yet</i> View Configuration	Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration
Smart License Registered View Configuration	Backup and Restore View Configuration	Troubleshoot <i>No files created yet</i> REQUEST FILE TO BE CREATED
Site-to-Site VPN <i>There are no connections yet</i> View Configuration	Remote Access VPN Requires RA VPN license No connections 1 Group Policy Configure	Advanced Configuration Includes: FlexConfig, Smart CLI View Configuration

Step 2. On the System Settings screen, Select the Logging Settings in the left-hand menu.



Step 3. Set the Data Logging toggle switch, select the + sign under Syslog Servers.

Step 4. Select Add Syslog Server. Alternatively, you can create the Syslog Server object in Objects - Syslog Servers.

Logging Settings

Remote Servers

DATA LOGGING

Syslog Servers



Filter

Nothing found

[Create new Syslog Server](#)

CANCEL

OK

Please select an Event List Filter

Step 5. Enter the IP Address of your Syslog Server and port number. Select the radio button for Data Interface and select 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.

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

Step 6. Next, select the new Syslog server and select OK.

Syslog Servers



Filter

10.88.243.52



[Create new Syslog Server](#)

CANCEL

OK

Step 7. Select the Severity level to filter with the all events radio button and select your desired logging level.

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

Step 8. Select Save at the bottom of the screen.

SAVE

Step 9. Verify the settings were successful.

Device Summary

Logging Settings

✔ Successfully saved logging settings.

Step 10. Deploy the new settings.



And

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: <i>172.16.1.250:514</i>	
-	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
syslogServerLogFilter.dataLogging.platformLogLevel: ...	INFORMATIONAL
-	syslogServerLogFilter.fileMalwareLoggi
-	syslogServerLogFilter.fileMalwareLoggi
syslogServerLogFilter.dataLogging.syslogServers:	
-	172.16.1.250:514
✎ Access Policy Edited: <i>NGFW-Access-Policy</i>	

MORE ACTIONS ▾

CANCEL

DEP

OPTIONAL.

Additionally, the Access Control Policy access control rules can be set to log into the Syslog server:

Step 1. Click on the Policies button at the top of the screen.



Firepower Device Manager



Monitoring



Policies



Objects



Devices

Step 2. Hover over the right-hand side of the ACP rule to add logging and Select the pencil icon.

#	NAME	ACTION	SOURCE			DESTINATION			
			ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS	APPLICATION
> 1	Inside_Outside...	Trust	inside_zone	ANY	ANY	outside_zone	ANY	ANY	ANY

Step 3. Select the Logging tab, Select the radio button for At End of Connection, Select the drop-down arrow under Select a Syslog Alert Configuration, Select on the Syslog Server and Select OK.

Order: 1, Title: Inside_Outside_Rule, Action: Allow

Source/Destination | Applications | URLs | Users | Intrusion Policy | File policy | **Logging**

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

Step 4. Deploy the configuration changes.

Verify

Step 1. After the task completes, you can verify the settings in the FTD CLI Clish Mode with the **show running-config logging** command.

```
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  
>
```

Step 2. Navigate to the Syslog server and verify that the Syslog server application accepts the Syslog messages.

Tftpd64 by Ph. Jounin

Current Directory: C:\Program Files\Tftpd64

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

Tftp Server | Tftp Client | **Syslog server** | Log viewer

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

Clear Copy

About Settings

Troubleshoot

Step 1. If the Syslog messages on the Syslog application produce any messages, perform a packet capture from the FTD CLI to check for packets. Enter the **system support diagnostic-cli** command at the clish prompt to change from Clish mode to Lina.

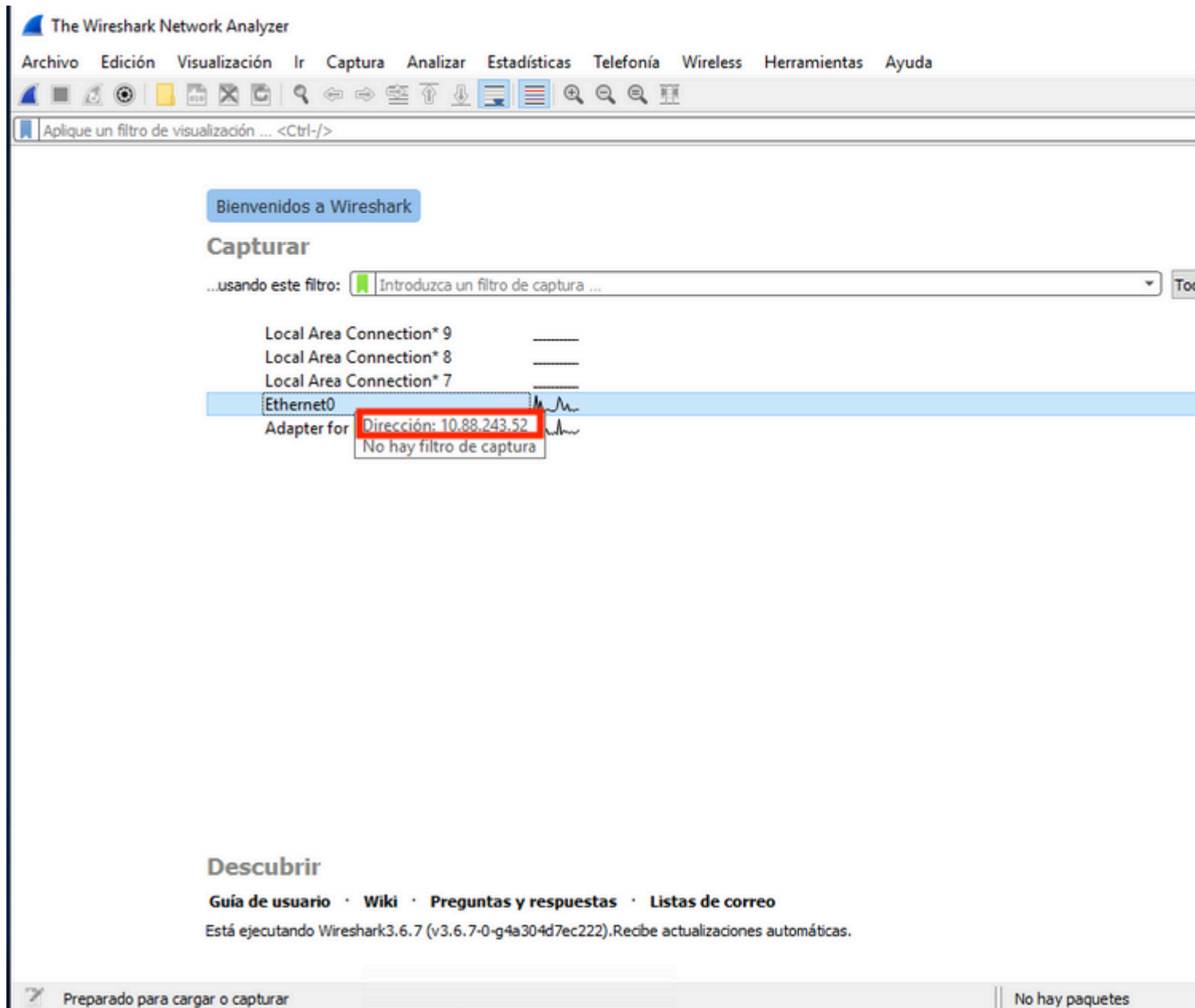
```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

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

Step 2. Create one packet capture for your udp 514 (or tcp 1468 if you used tcp)

Step 3. Verify that the communication gets to the network interface card on the Syslog Server. Use

Wireshark or another packet that captures the utility loaded. Double-click the interface in Wireshark for the Syslog Server to start packet capture.



Step 4. Set a display filter in the top bar for udp 514; type `udp.port==514` and select the arrow to the right of the bar. From the output, confirm whether the packets can make it to the Syslog Server.

*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
145	0.965848	10.88.146.119	10.88.243.52	Syslog	155	LOCAL4.DEBUG: Aug 19 2022 16:59:35: %FTD-7
294	1.902835	10.88.146.119	10.88.243.52	Syslog	155	LOCAL4.DEBUG: Aug 19 2022 16:59:36: %FTD-7
303	1.969237	10.88.146.119	10.88.243.52	Syslog	155	LOCAL4.DEBUG: Aug 19 2022 16:59:36: %FTD-7
435	3.614217	10.88.146.119	10.88.243.52	Syslog	155	LOCAL4.DEBUG: Aug 19 2022 16:59:38: %FTD-7
461	3.990606	10.88.146.119	10.88.243.52	Syslog	155	LOCAL4.DEBUG: Aug 19 2022 16:59:38: %FTD-7
523	4.329918	10.88.146.119	10.88.243.52	Syslog	155	LOCAL4.DEBUG: Aug 19 2022 16:59:38: %FTD-7
540	4.465525	10.88.146.119	10.88.243.52	Syslog	155	LOCAL4.DEBUG: Aug 19 2022 16:59:38: %FTD-7
572	4.904842	10.88.146.119	10.88.243.52	Syslog	155	LOCAL4.DEBUG: Aug 19 2022 16:59:39: %FTD-7

> Frame 26: 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits) on interface \Device\NPF_{FFB4AA7C-2AE5-4A96-B...}

> 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

```

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

```

wireshark_Ethernet01BP1Q1.pcapng Paquetes: 11865 · Mostrad

Step 5. If the Syslog Server Application does not show the data, troubleshoot the setting within the Syslog Server application. Make sure that the correct protocol is used, udp/tcp and the correct port, 514/1468.

Related Information

- [Cisco Technical Support & Downloads](#)