

يف هتحص نم ققحتلاو syslog نيوكت FirePOWER Device Manager

تايوت حمل

[قمدملا](#)

[قيساسألا تابلطت ملا](#)

[تابلطت ملا](#)

[تان نيوكت ملا](#)

[قحصلا نم ققحت ملا](#)

[اهجالص او اءاخألا فاشكتسا](#)

قمدملا

FirePOWER Device Manager (FDM) لخد syslog نيوكت ةيفيك دننتملا اذه حضوي

قيساسألا تابلطت ملا

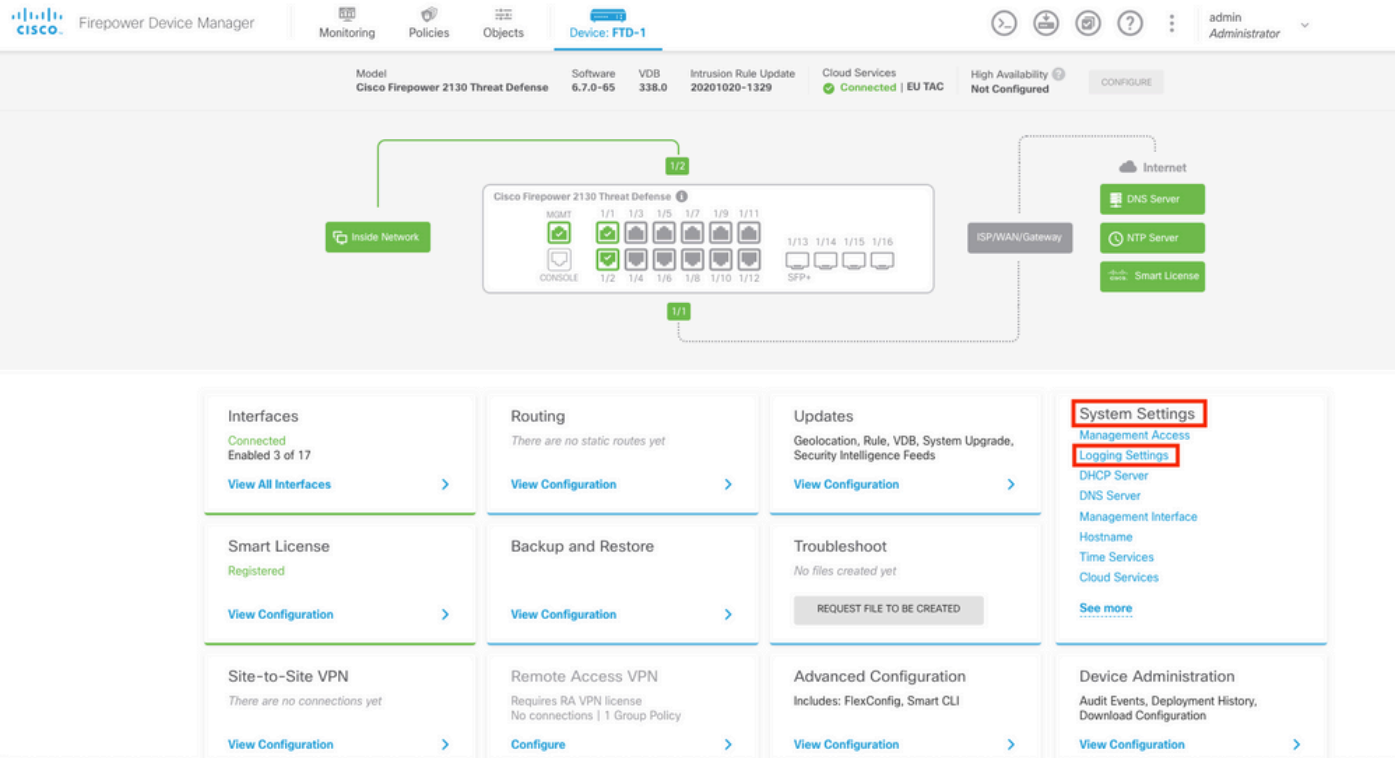
تابلطت ملا

ةيلاتلا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco ي صوت:

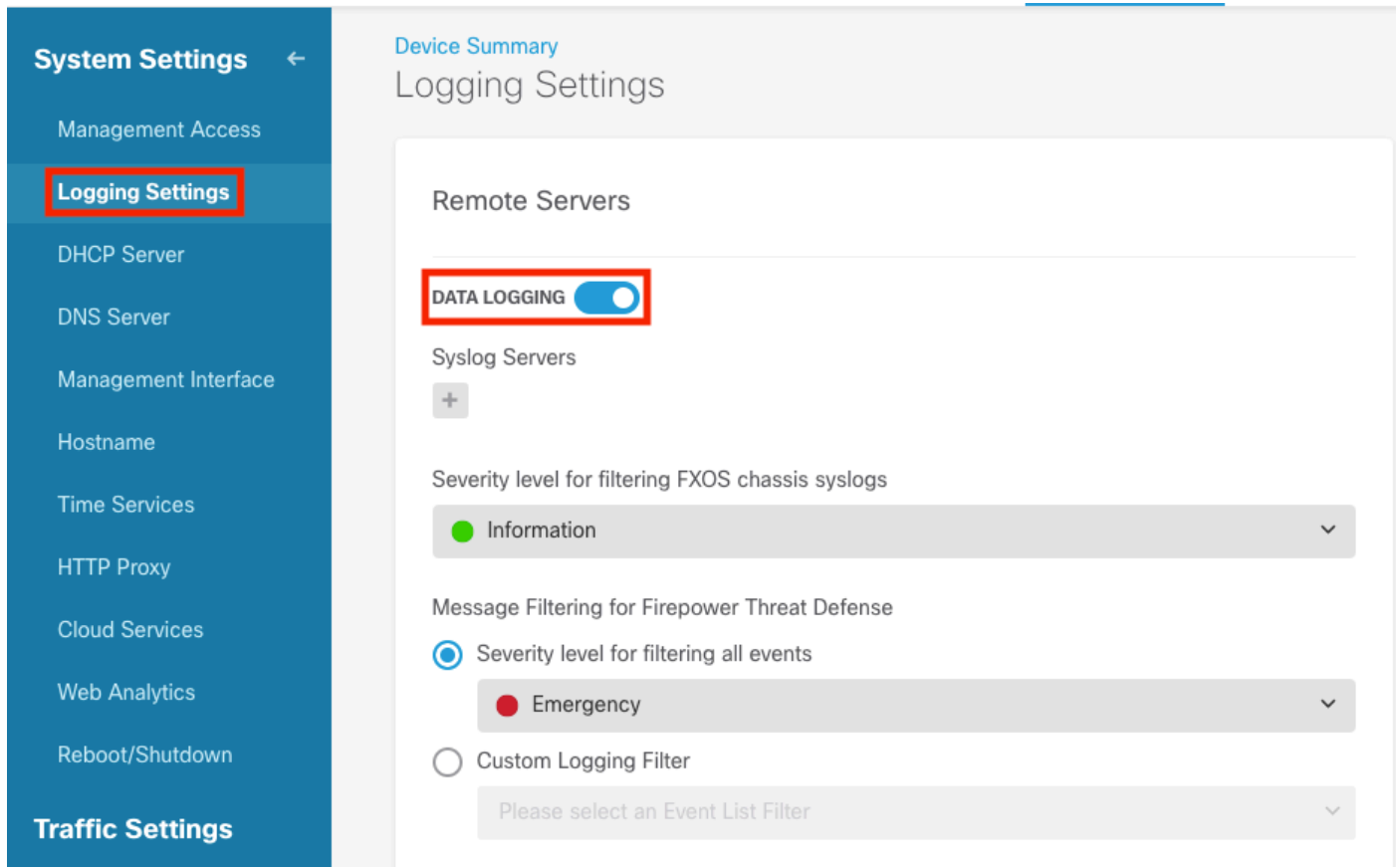
- Firepower Threat Defense
- Syslog Server جم انرب لغشي يذلا

تان نيوكت ملا

لفسأ ليجستلا تاداعإ ددح، FirePOWER ةزهجأ ةرادإل ةيسيئرلا ةشاشلا نم 1. ةوطخلا ةشاشلا نم نميألا يلفسلا نكرلا يف ماظنلا تاداعإ



يُرسِل الةمئاقال ي ف ليجستل ادادع| دح، ماطنل ادادع| ةشاش ي ف 2. ةوطخل



مداوخ لفس + ةمالع ديدحت لال خ نم تانايبال ليجست ليدبت لوحمل نييعت ب مق 3. ةوطخل Syslog.

تانايلال ي ف syslog مداخ نئاك ءاشن كنكمي، كلذ نم ال دب. syslog مداخ ةفاض| دح 4. ةوطخل syslog مداوخ.

Logging Settings

Remote Servers

DATA LOGGING

Syslog Servers



Filter

Nothing found

[Create new Syslog Server](#)

CANCEL

OK

Please select an Event List Filter

ددحو تانايبلا ةهجاول رايخل رز ددح .رسيأ مقررولدان syslog ك نم ناوعلا تلخد .5 ةوطخل ا قفاوم .

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

قفاوم ددحو ديدجالا syslog مداخ ددح، كلذ دعب 6 ةوطخلا

Syslog Servers



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

[Create new Syslog Server](#)

يذلل لئجستل لئوتسم ددو، وئدارلأ شادألأ لك ةئفصلل ةرولأل لئوتسم ددو. 7 ةولألأ
هءرل.

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

ةشاشلا لفسأ يف ظفح ددح. 8 ةوطخل

SAVE

تادادعالا حاجن نم ققحت. 9 ةوطخل

Device Summary

Logging Settings

✔ Successfully saved logging settings.

ةدي دجل تادادعإلإ رشن 10 ةوطخلإ



9

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 | LEGEND |
|-------------------------------------------------------------------|----------------------------------------------------------|--------|
| 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 ▾

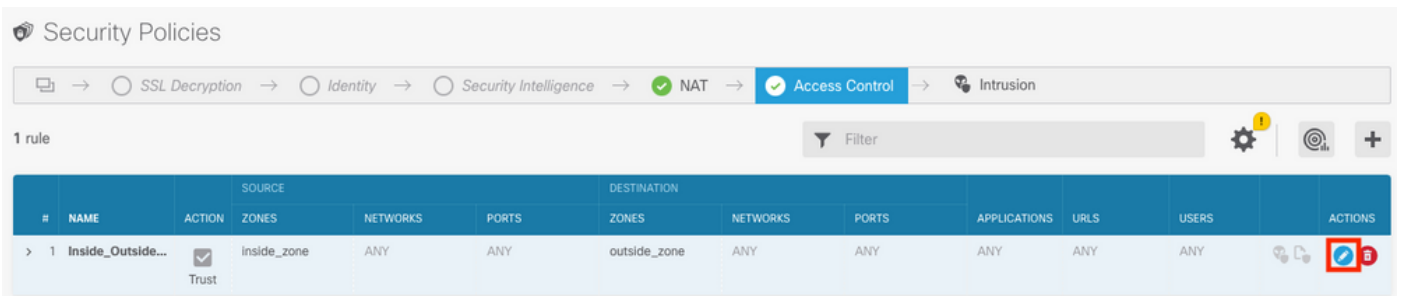
ي.رأختا

لوصول ي ف مكحتللا جهنل لوصول ي ف مكحتللا دعاوق نيي عت نكم ي ،كلذ ي ة فاضلأب
syslog مداخ ي ل لوخدلا ليحستل

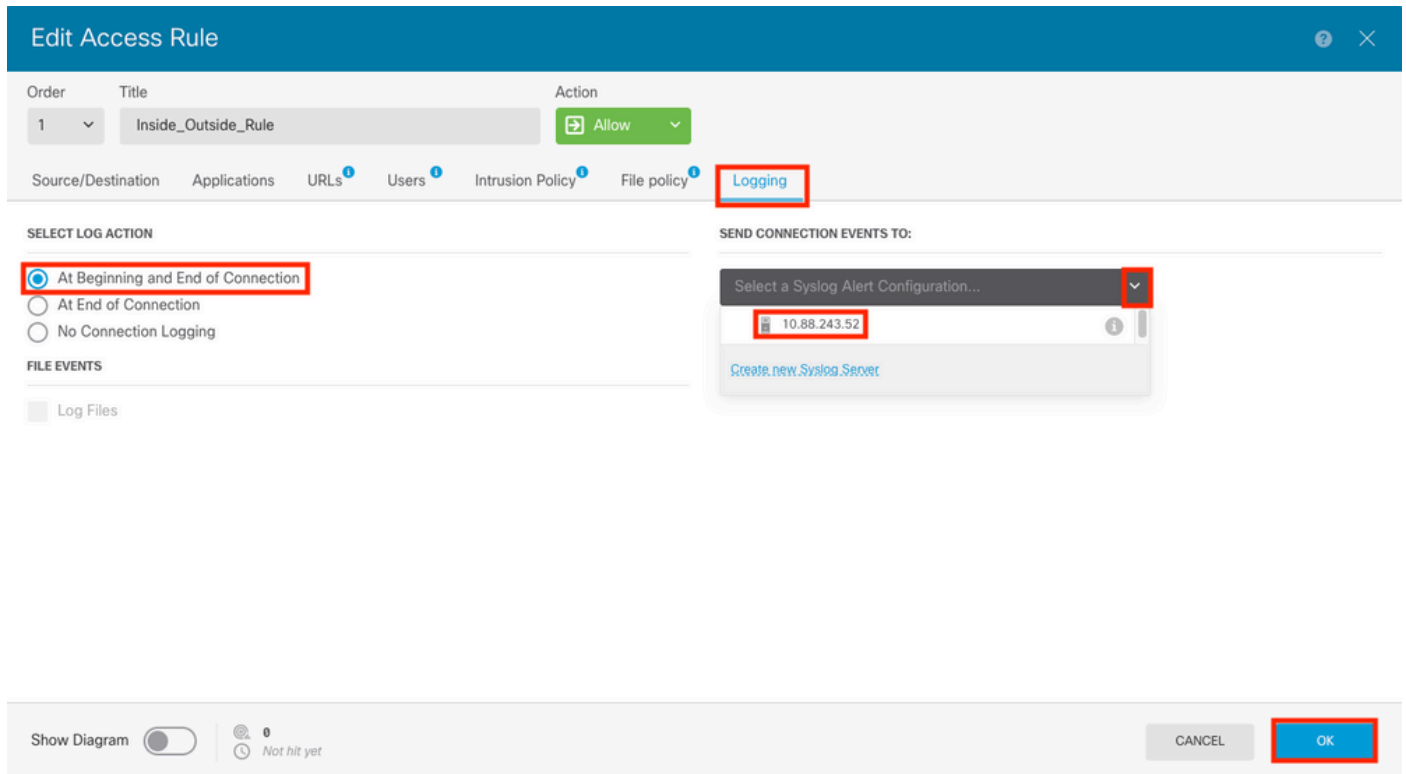
ة.شاشلا يلع ي ف تاسايس رزلا قوف رونا 1. ةوطخللا



ةنوقيأ ديحتو ليحست ة فاضلأ ACP ةدعاوق نم نميألا بنأجللا قوف رورملأب مق 2. ةوطخللا
صاصرلا ملقلا



مهسللا دح ،لاصتالا ةياهن دنع ل رايخللا رز دح ،ليحست بيوبتلا ةمالع دح 3. ةوطخللا
ق.فاوم دحو Syslog مداخ يلع دح ،Syslog هيبن ننيوكت ديحت تحت لدسنملا



ننيوكتلا تاريخيغت رشن ب مق 4. ةوطخللا

ةحصلا نم ققحتلا

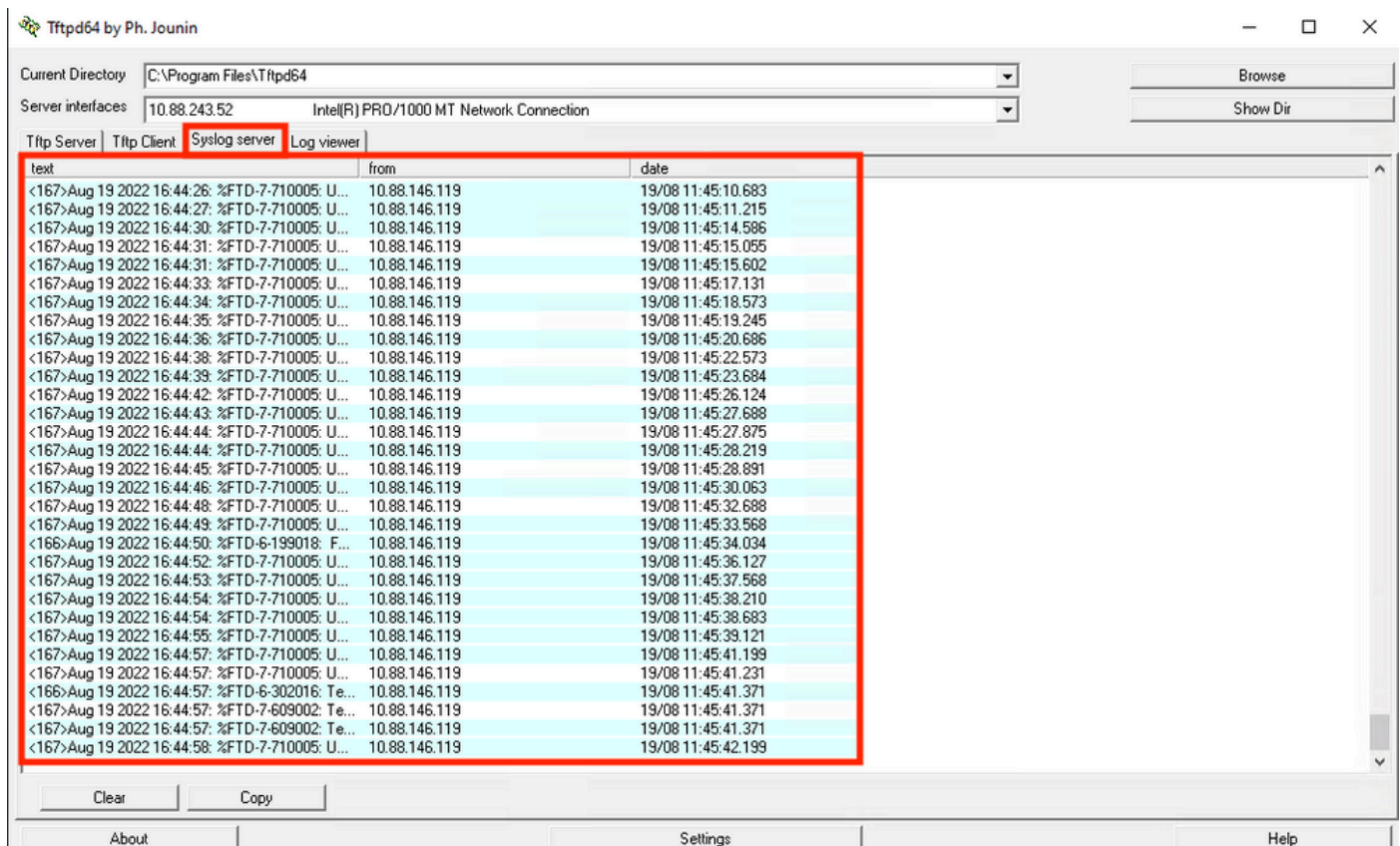
(CLI) رم اوألا رطس ةهجاو عضو يف تادادعإلا نم ققحتلا كنكمي ،ةمهملا لامتك ا دعب 1. ةوطخلا ل show running-config logging رمألا مادختساب FTD ل

```
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
>
```

Syslog لئاسرل Syslog م داخ ققحتو Syslog م داخ ل لقتنا 2. ةوطخلا



اهحالص او ءاطخالا فاشكتسا

نم طاقنلا طبر تنجنا ،ةلاسري ققحتو syslog ل لعل ةلاسر syslog ل لجتني ن 1. ةوطخلا

Wireshark interface showing a packet capture on Ethernet0. The filter is set to `ip.addr == 10.88.146.119`. The packet list shows several Syslog messages from 10.88.146.119 to 10.88.243.52. The selected packet (No. 26) is a Syslog message: LOCAL4.DEBUG: Aug 19 2022 16:59:34: %FTD-7-710005: UDP request discarded from 0.0.0.0/68 to diagnostic:255.255.255.255/67n.

| 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:255.255.255.255/67n

```

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

عاطخألا فاشكتساب مقف ،تانايبال ضرعي Syslog Server قيبت نكي مل اذا 5 ةوطخل
 احي حصلال لوكوتوربال مادختسا نم دكأت . Syslog Server قيبت لخاد احوال صاو
 او 514/1468 احي حصلال ذفن مل او

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ م ف ن م دخت س م ل م عد و ت م م م دقت ل ة م ش ب ل و
م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م م چ ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت م م مچرت م ا ه م د ق ي ي ت ل ا ة ف ا ر ت ح ا ل ا ة مچرت ل ا م ل ا ح ل ا و ه
ل ا ا م ا د ا د ع و چ ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل چ ن ا ل ا دن ت س م ل ا