

Configurar e verificar o Syslog no Gerenciador de dispositivos do Firepower

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Configurações](#)

[Verificar](#)

[Troubleshoot](#)

Introduction

Este documento descreve como configurar o Syslog no Firepower Device Manager (FDM).

Prerequisites

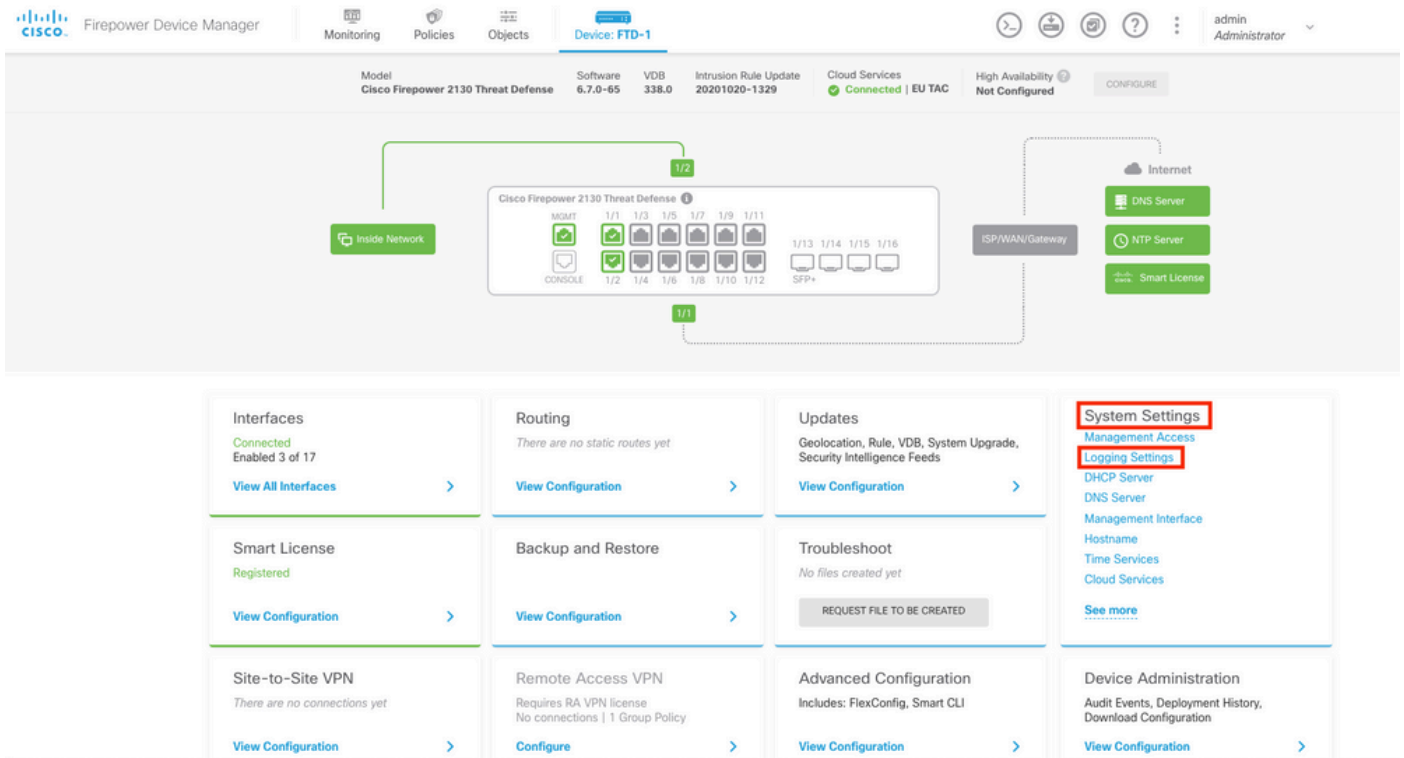
Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

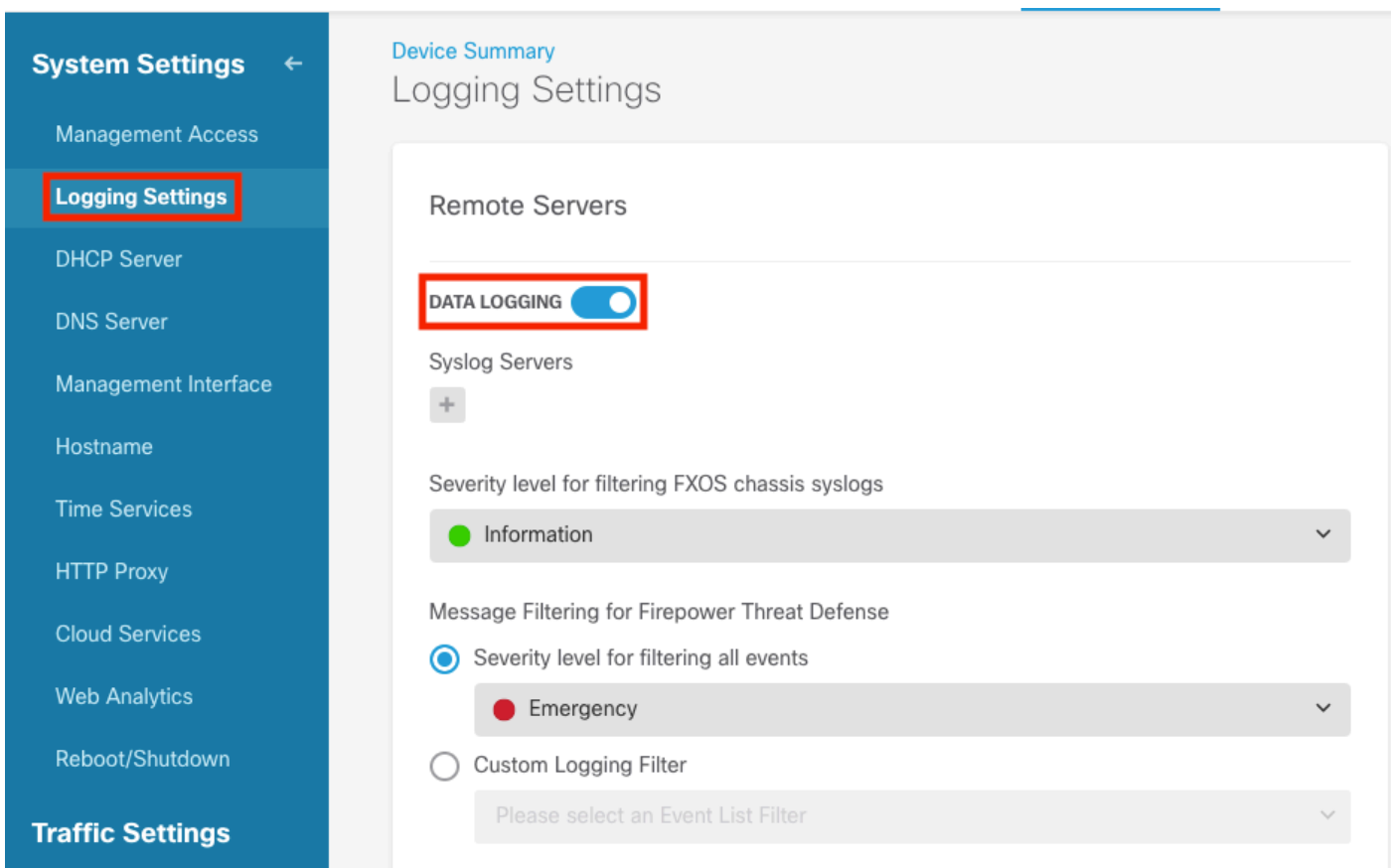
- Firepower Threat Defense
- Servidor Syslog que executa o software Syslog para coletar dados

Configurações

Etapa 1. Na tela principal do Gerenciador de dispositivos do Firepower, selecione as Configurações de registro em Configurações do sistema, no canto inferior direito da tela.



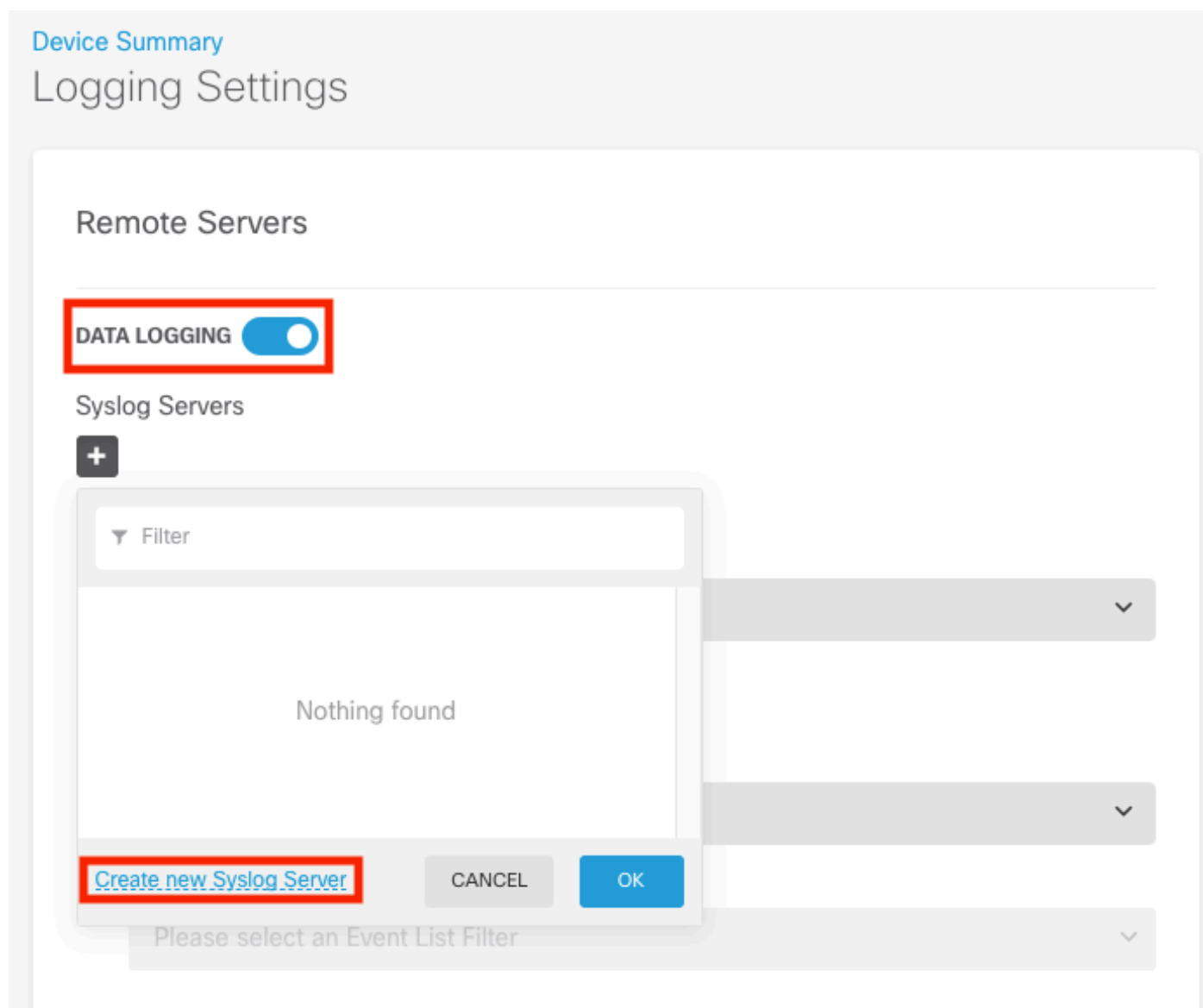
Etapa 2. Na tela Configurações do sistema, selecione Configurações de registro no menu à esquerda.



Etapa 3. Defina o switch de alternância Registro de dados selecionando o sinal + em Servidores Syslog.

Etapa 4. Selecione Add Syslog Server (Adicionar servidor Syslog). Como alternativa, você pode

criar o objeto Servidor Syslog em Objetos - Servidores Syslog.



Etapa 5. Insira o endereço IP do Servidor Syslog e o número da porta. Selecione o botão de opção Interface de Dados e selecione 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

Etapa 6. Em seguida, selecione o novo servidor Syslog e selecione OK.

Syslog Servers



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

[Create new Syslog Server](#) CANCEL OK

Passo 7. Selecione o botão de opção Nível de severidade para filtrar todos os eventos e selecione o nível de registro desejado.

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

Etapa 8. Selecione Salvar na parte inferior da tela.

SAVE

Etapa 9. Verifique se as configurações foram bem-sucedidas.

Device Summary

Logging Settings

✔ Successfully saved logging settings.

Etapa 10. Implante as novas configurações.



E

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** ▾

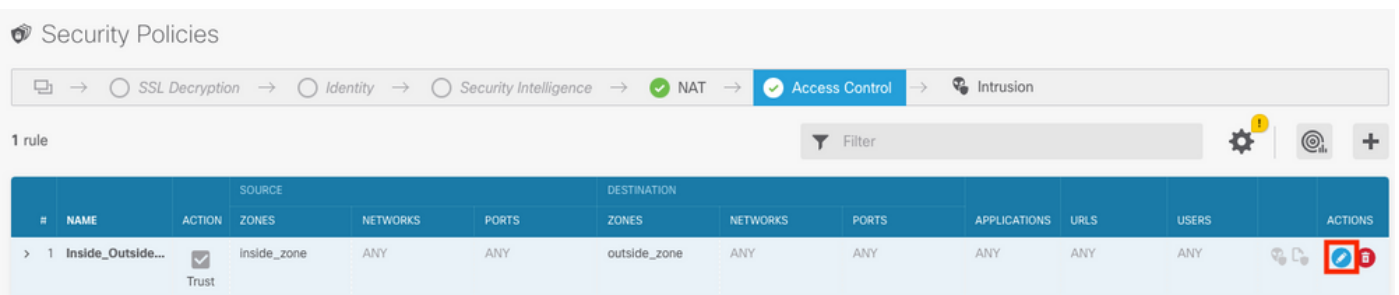
OPCIONAL.

Além disso, as regras de controle de acesso da política de controle de acesso podem ser configuradas para fazer login no servidor Syslog:

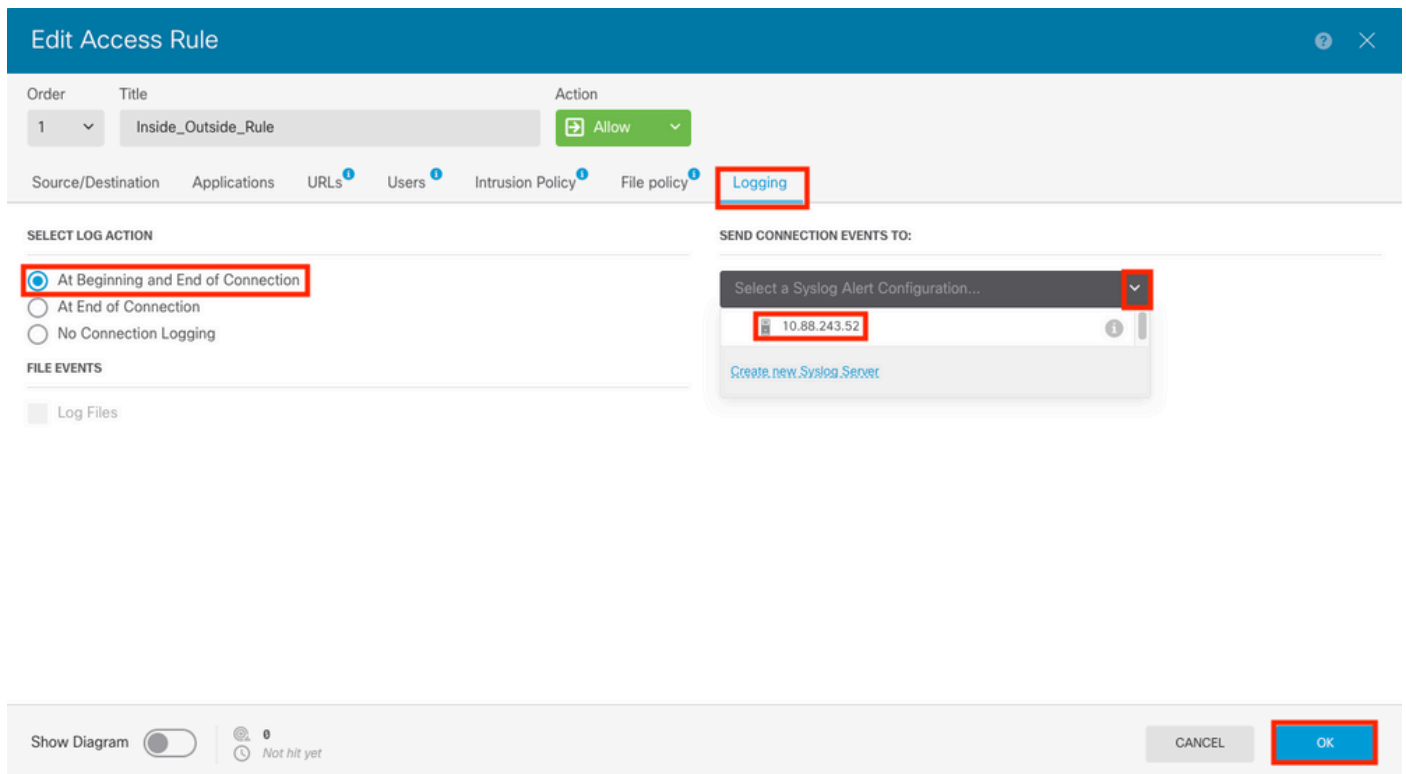
Etapa 1. Clique no botão Policies (Regras) na parte superior da tela.



Etapa 2. Passe o mouse sobre o lado direito da regra de ACP para adicionar logs e selecione o ícone do lápis.



Etapa 3. Selecione a guia Registro, selecione o botão de opção No fim da conexão, selecione a seta suspensa em Selecionar uma configuração de alerta de Syslog, selecione no servidor Syslog e selecione OK.



Etapa 4. Implante as alterações de configuração.

Verificar

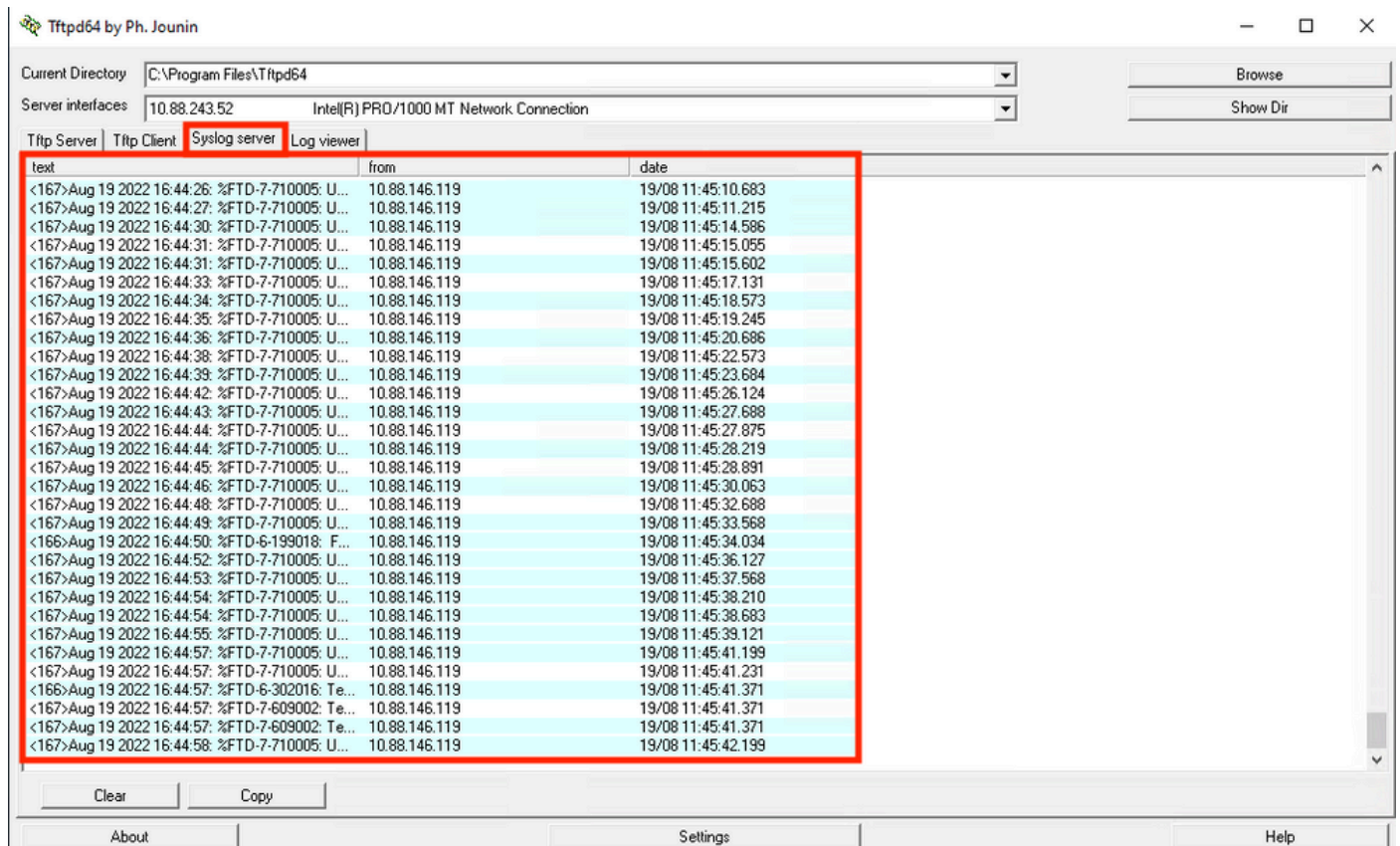
Etapa 1. Após a conclusão da tarefa, você pode verificar as configurações no modo Clish da CLI do FTD usando o comando `show running-config logging`.

```
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
>
```

Etapa 2. Navegue até o servidor Syslog e verifique se o aplicativo do servidor Syslog está aceitando mensagens Syslog.



Troubleshoot

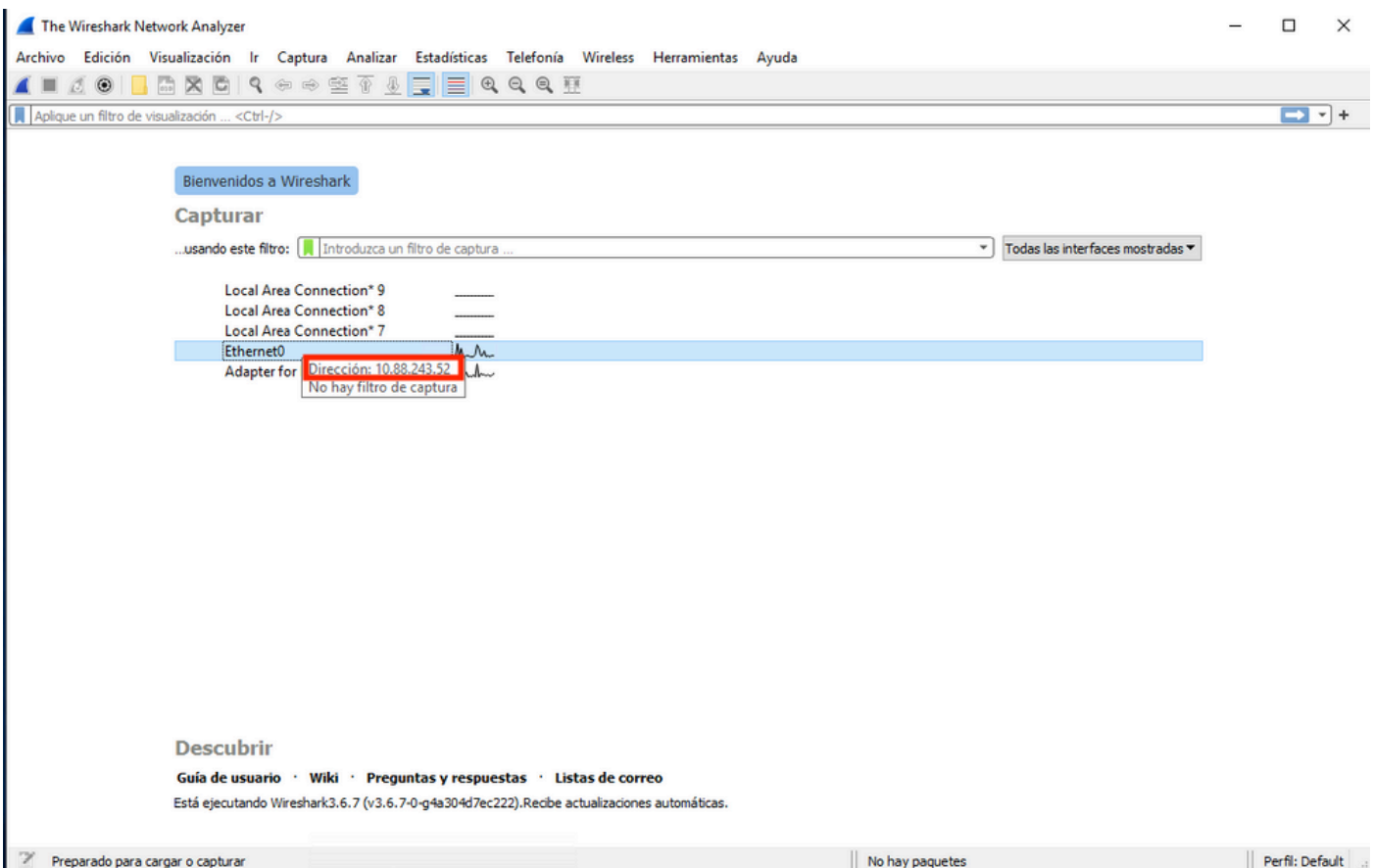
Etapa 1. Se as mensagens de Syslog no aplicativo Syslog produzirem qualquer mensagem, execute uma captura de pacote da CLI do FTD para verificar se há pacotes. Altere do modo Clish para LINA inserindo o comando **system support diagnostic-cli** no prompt do clish.

```
[> 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#
```

Etapa 2. Crie uma captura de pacote para seu udp 514 (ou tcp 1468 se você usou tcp)

Etapa 3. Verifique se a comunicação está fazendo isso com a placa de interface de rede no Servidor Syslog. Use o Wireshark ou outro utilitário de captura de pacotes carregado. Clique duas vezes na interface no Wireshark para que o Servidor Syslog comece a capturar pacotes.



Etapa 4. Defina um filtro de exibição na barra superior para udp 514 digitando **udp.port==514** e selecionando a seta à direita da barra. Na saída, confirme se os pacotes estão chegando ao Servidor Syslog.

*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

Etapas 5. Se o aplicativo Servidor Syslog não estiver mostrando os dados, solucione os problemas da configuração no aplicativo Servidor Syslog. Verifique se o protocolo correto está sendo usado como udp/tcp e a porta correta 514/1468.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.