Configurar e verificar o Syslog no Gerenciador de dispositivos do Firepower

Contents

Introduction

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

Prerequisites

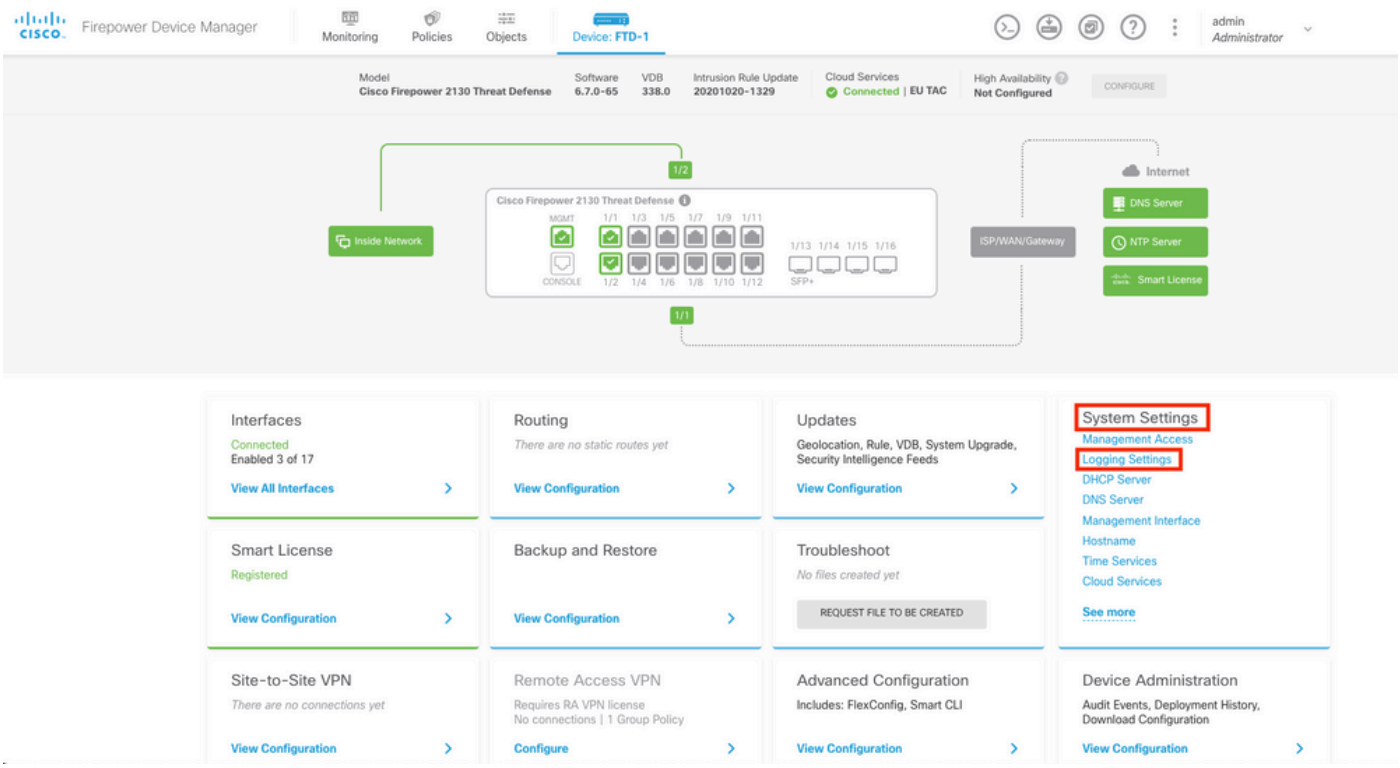
Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

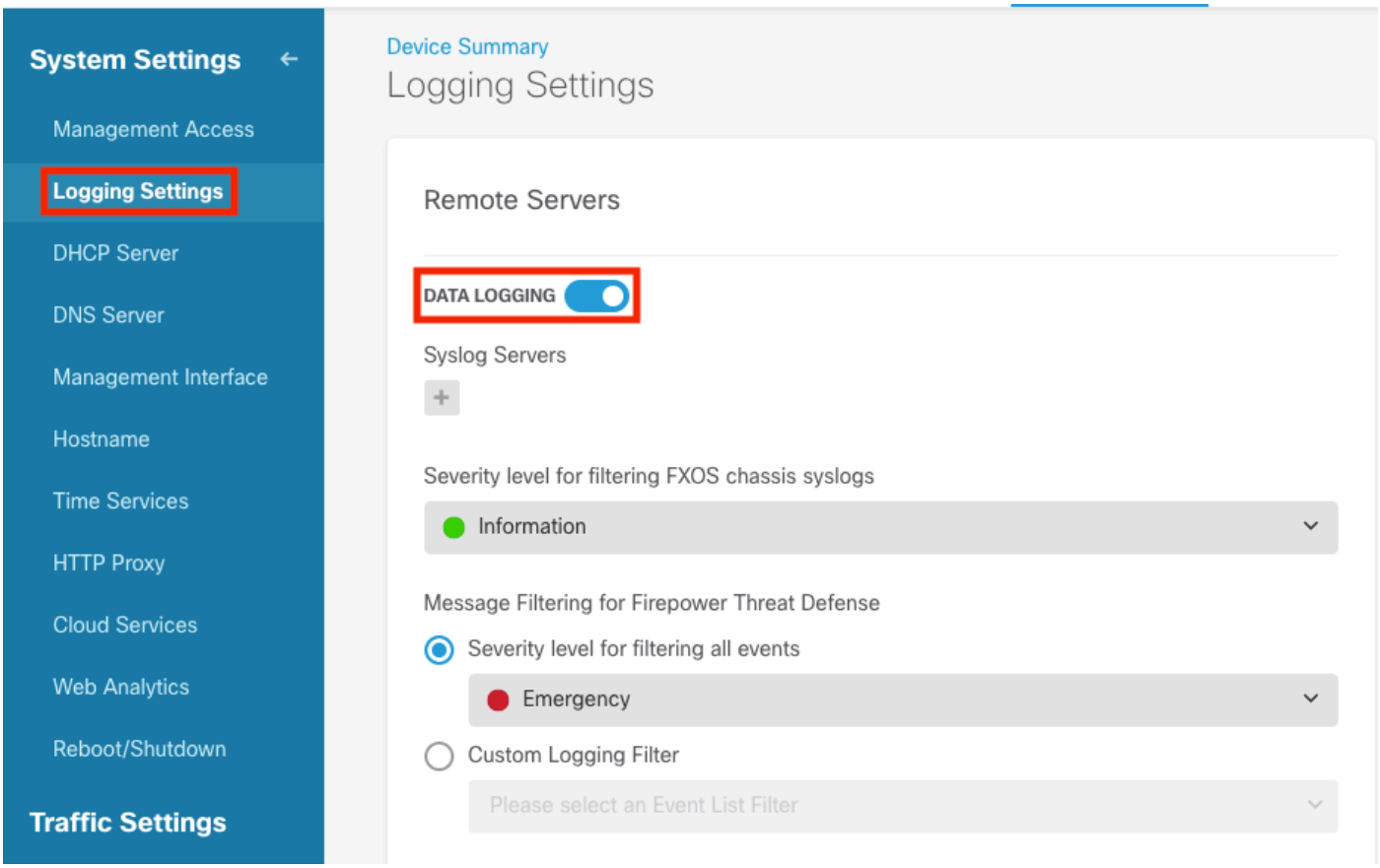
- Firepower Threat Defense
- Servidor Syslog que executa o software Syslog para coletar dados

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.



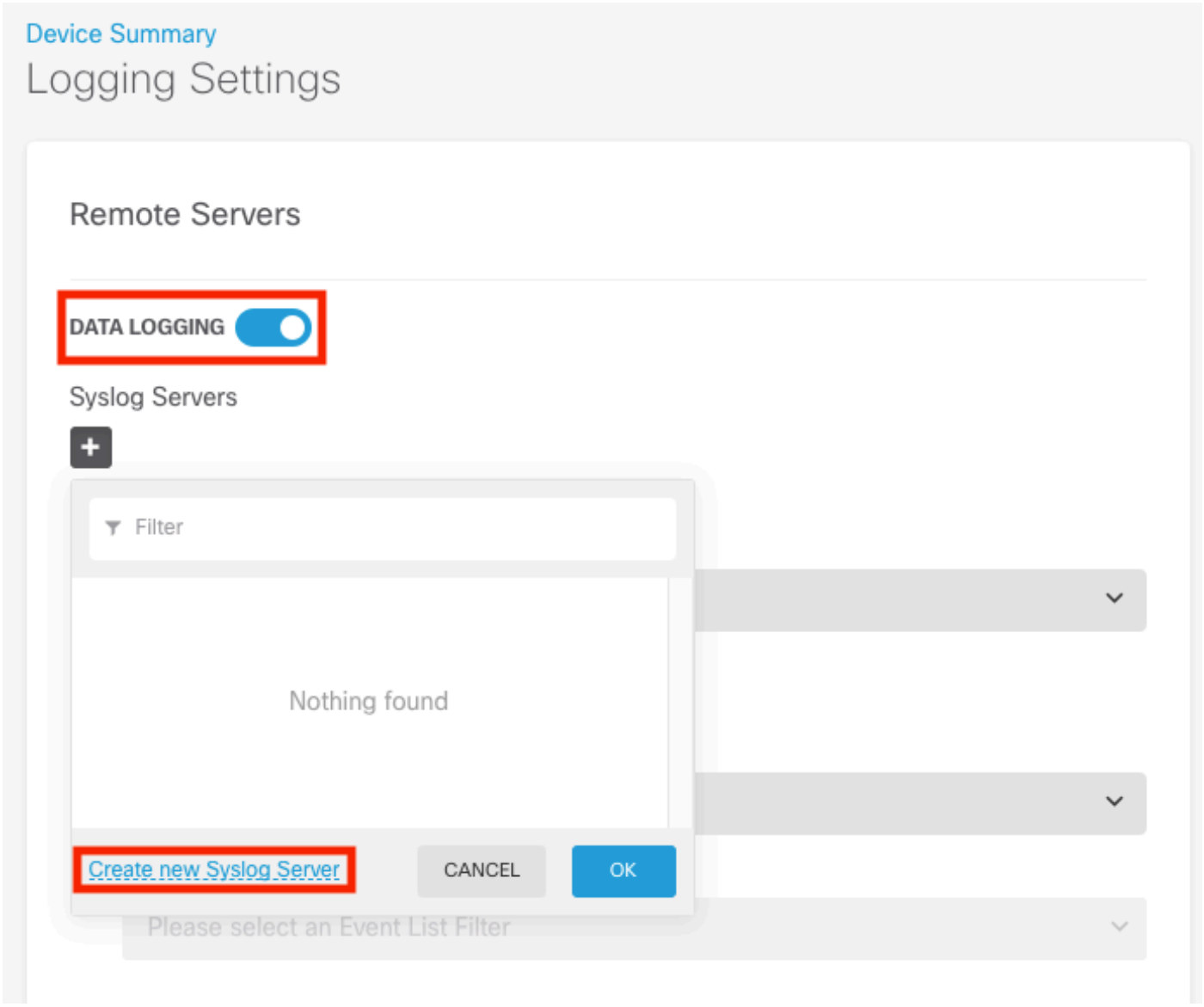
Etapa 2. Na tela Configurações do sistema, selecione Configurações de registro no menu à esquerda.



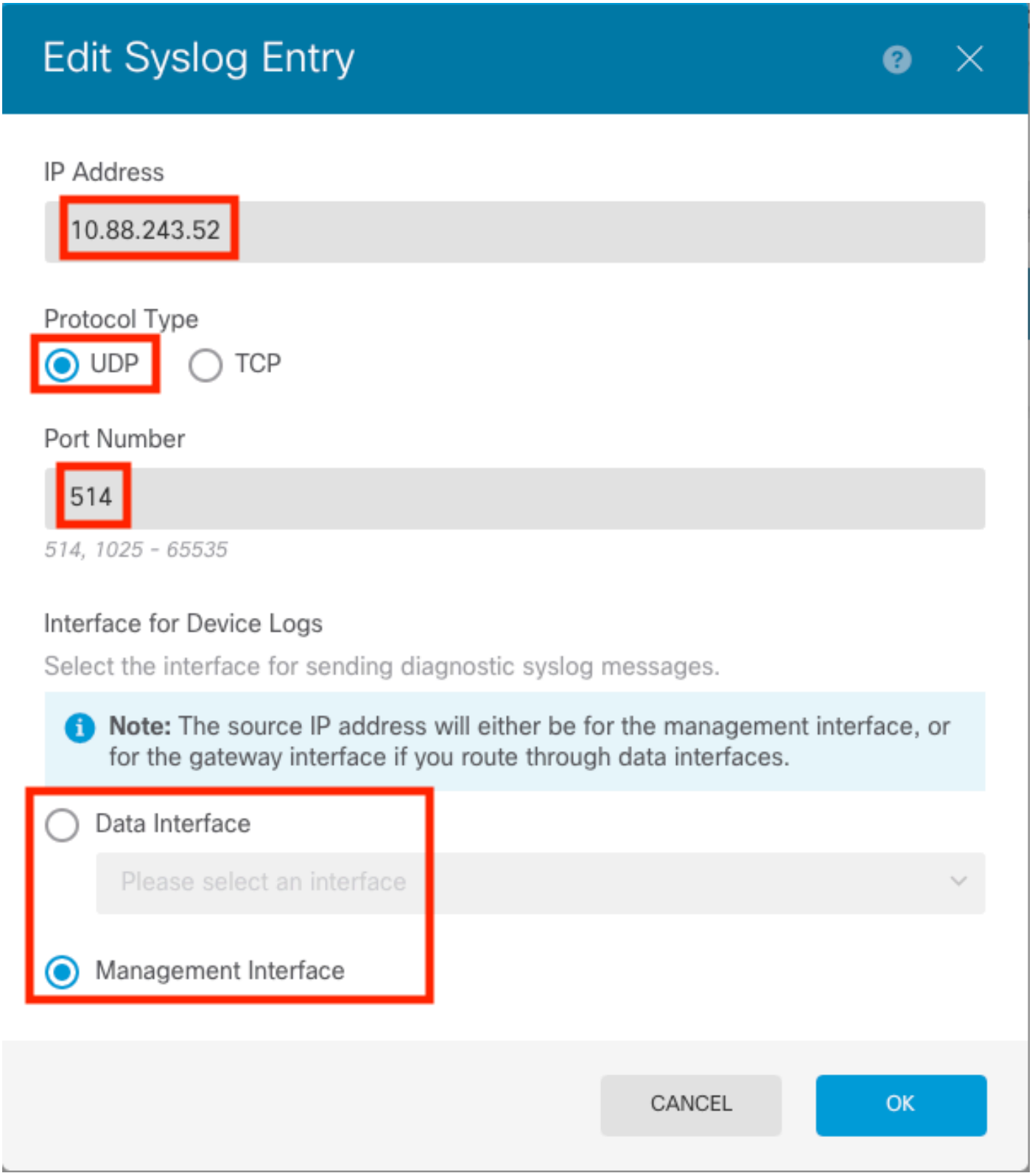
Etapa 3. Defina o switch de alternância Registro de dados selecionando o sinal + em Servidores Syslog.

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

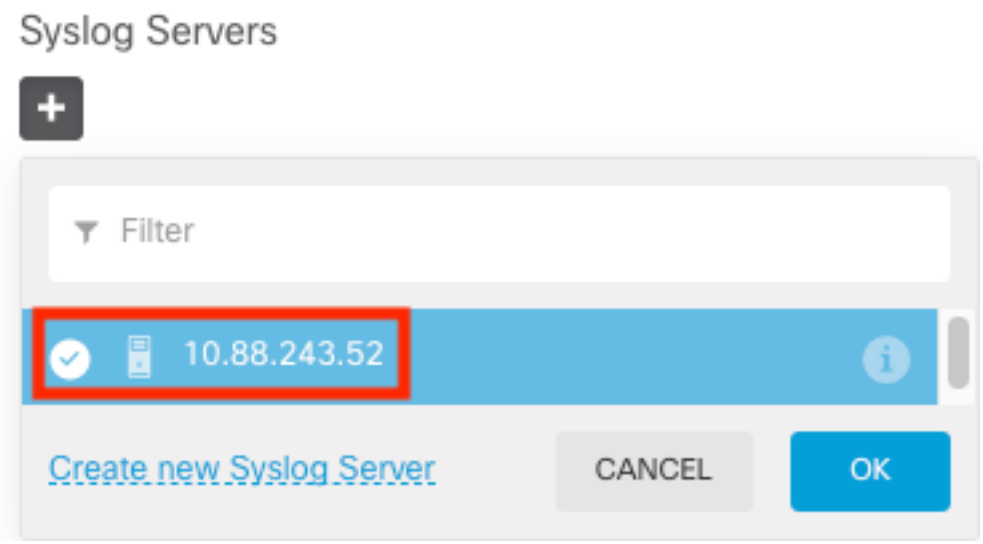
criar o objeto Servidor Syslog em Objetos - Servidores Syslog.



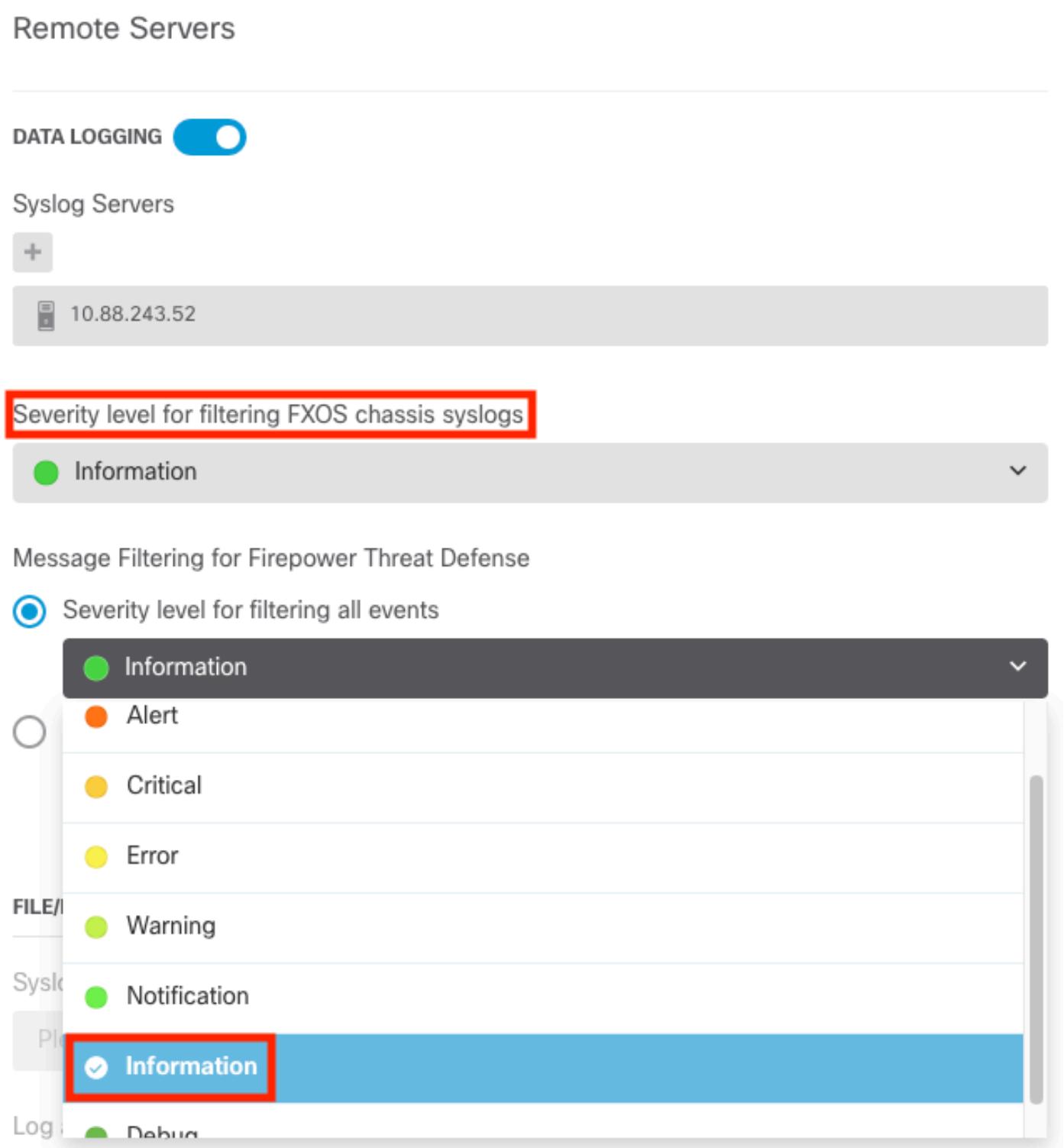
Etapa 5. Insira o endereço IP do Servidor Syslog e o número da porta. Selecione o botão de opção Interface de Dados e selecione OK.



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

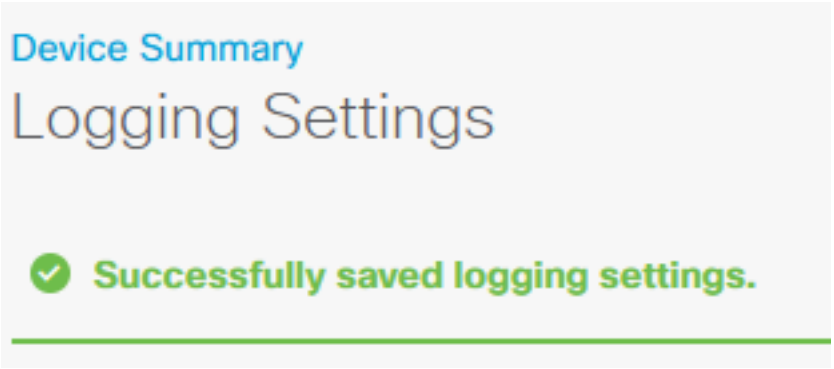


Passo 7. Selecione o botão de opção Nível de severidade para filtrar todos os eventos e selecione o nível de registro desejado.



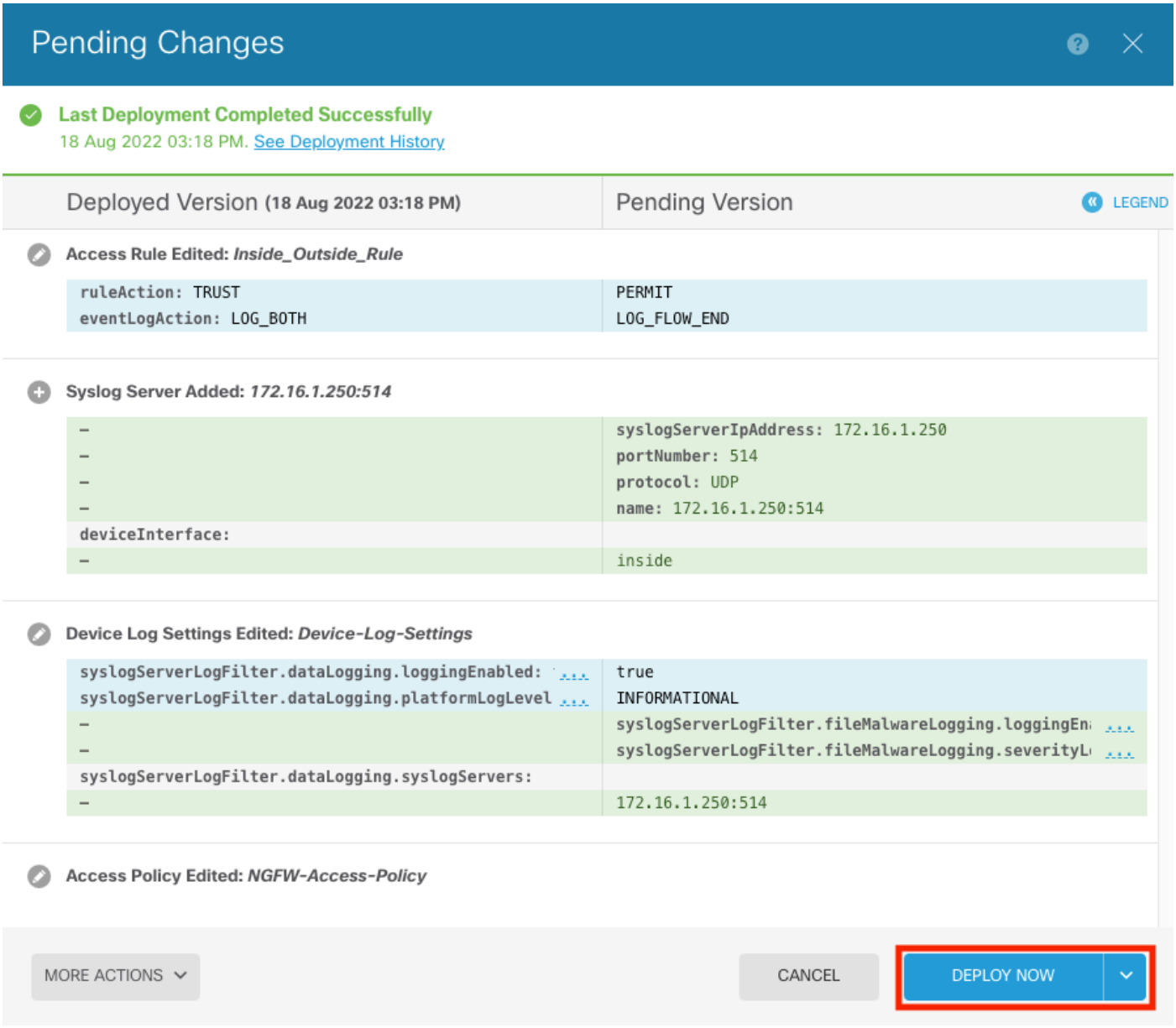
Etapa 8. Selecione Salvar na parte inferior da tela.

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



Etapa 10. Implante as novas configurações.

E

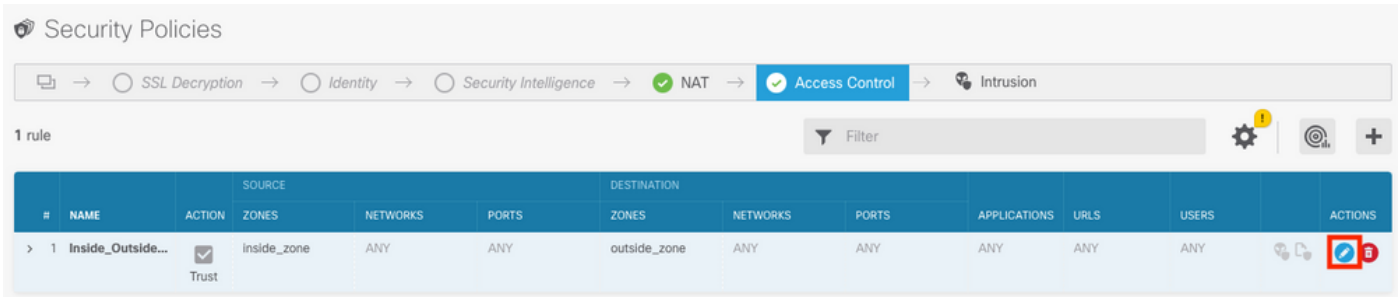


OPCIONAL.

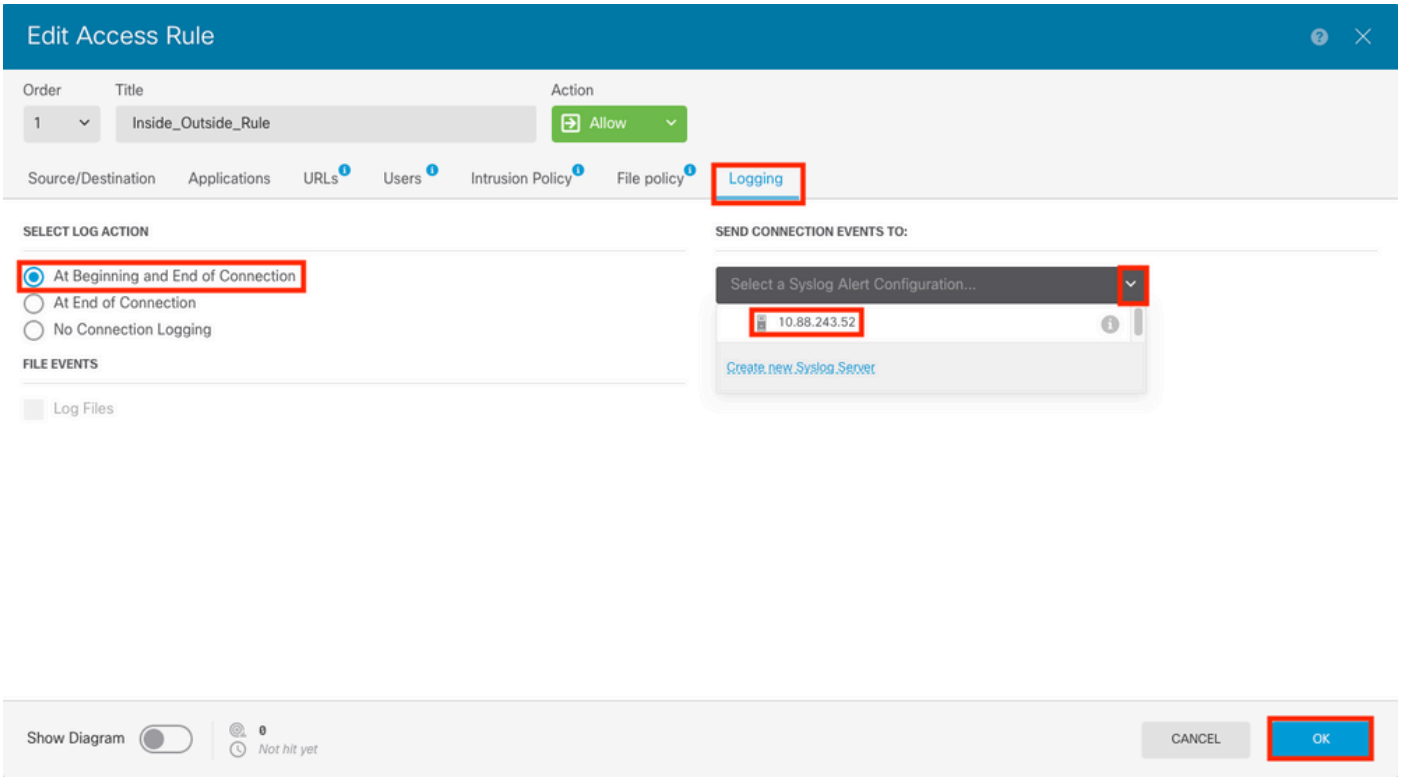
Além disso, as regras de controle de acesso da política de controle de acesso podem ser configuradas para fazer login no servidor Syslog:

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.



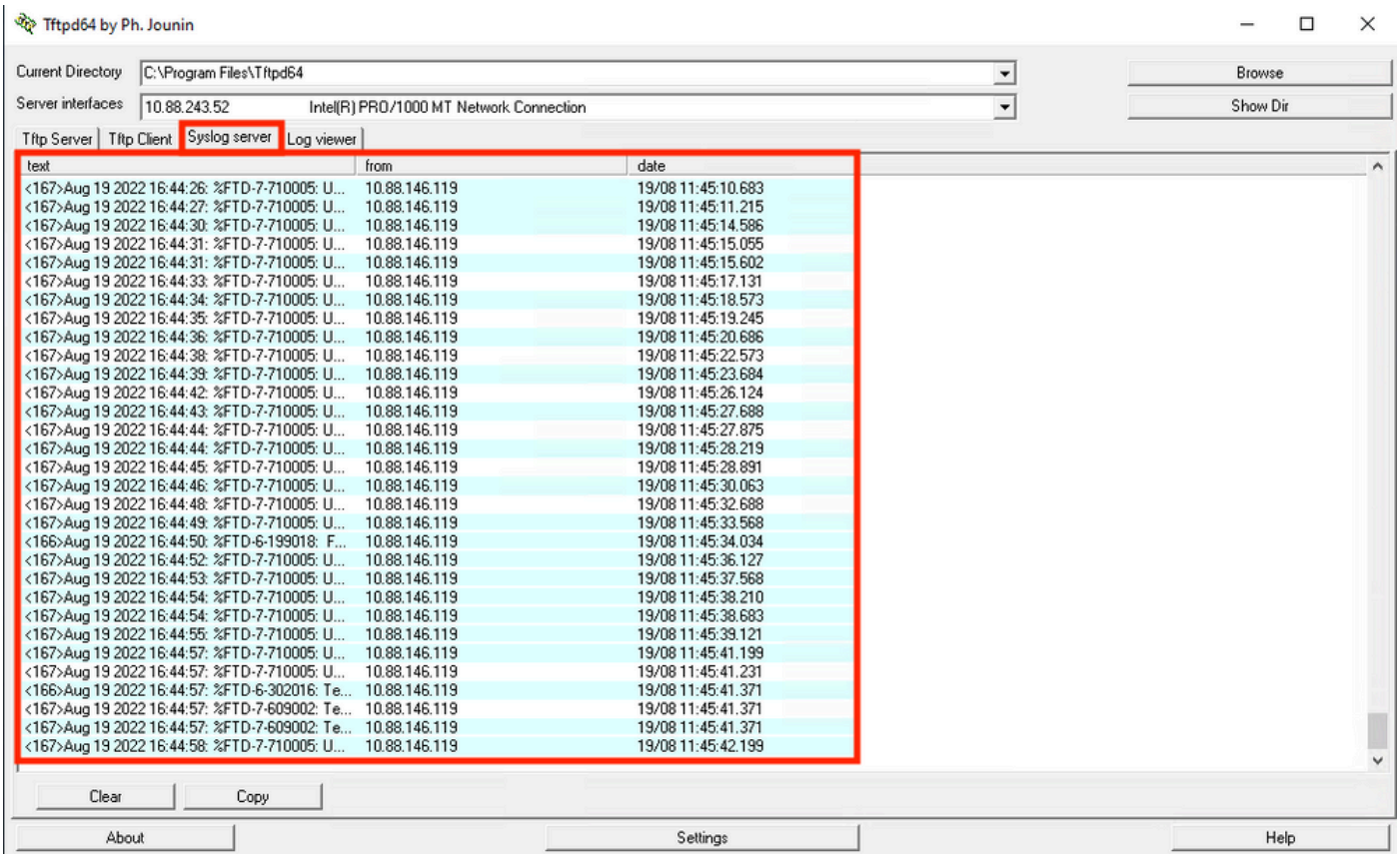
Etapa 4. Implante as alterações de configuração.

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.



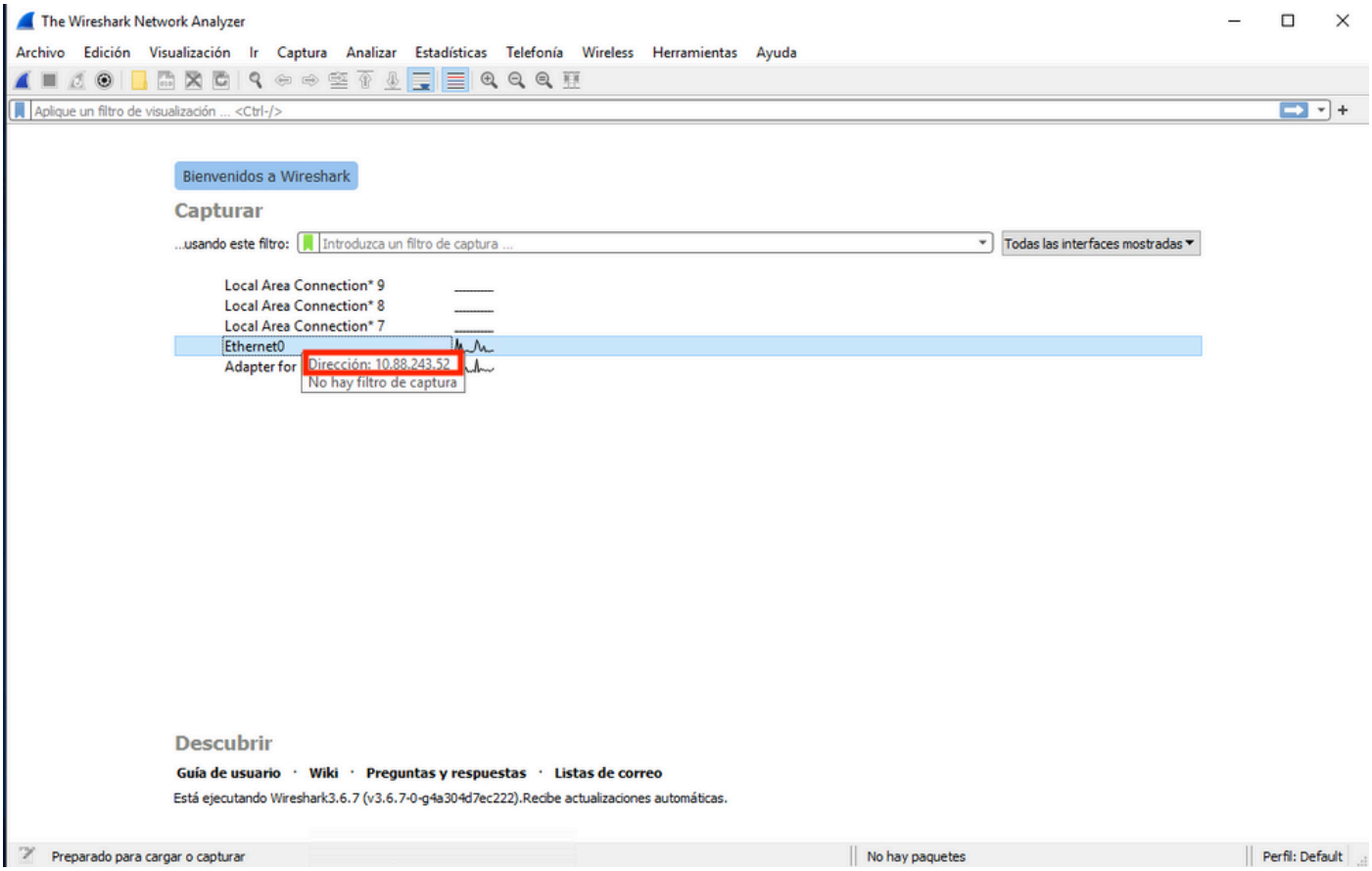
Troubleshoot

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.

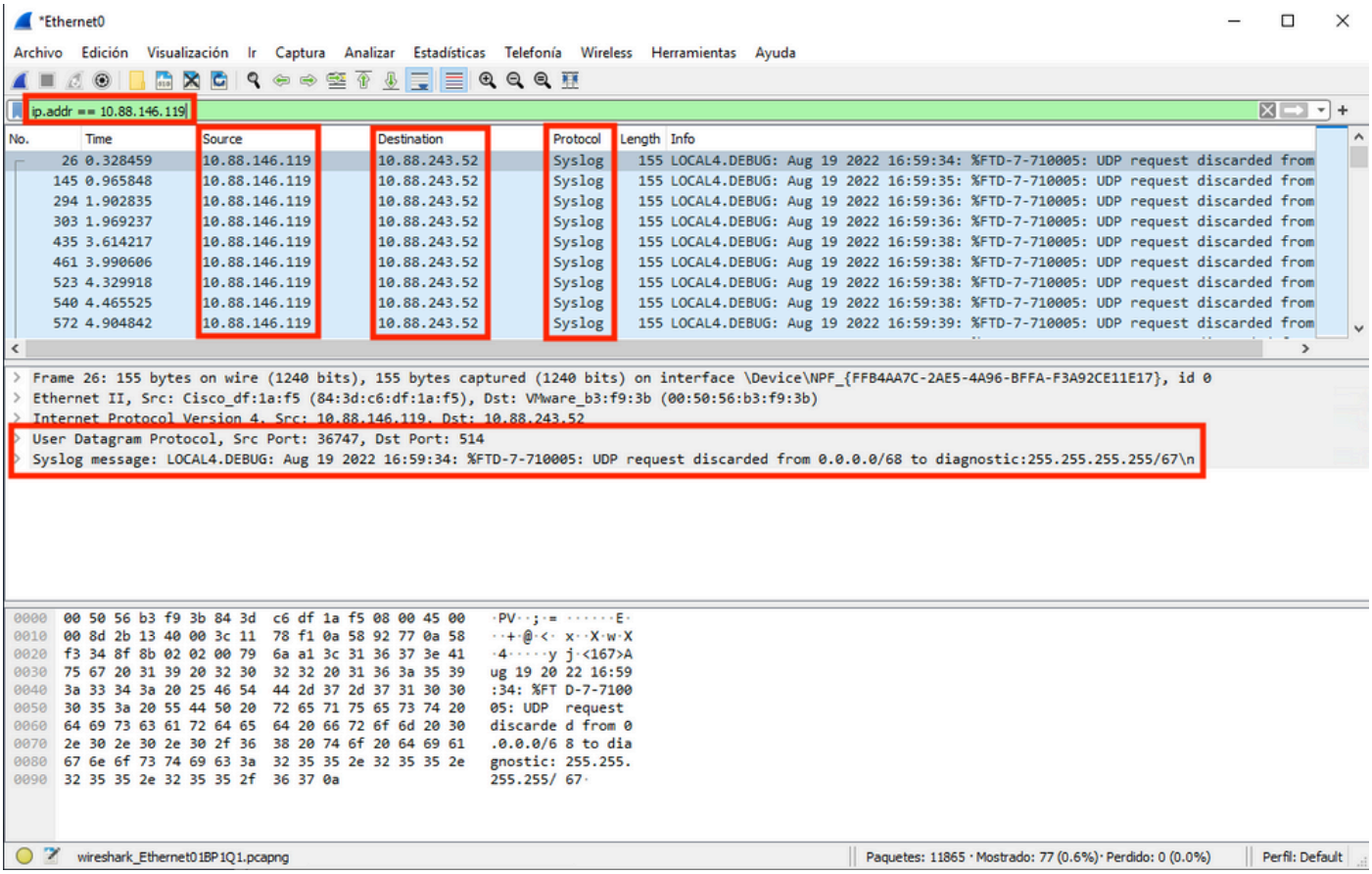
```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

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.



Etapa 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.