Configuración Y Verificación De Syslog En El Administrador De Dispositivos Firepower

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Configuraciones](#)
[Verificación](#)
[Troubleshoot](#)

Introducción

Este documento describe cómo configurar Syslog en el Administrador de dispositivos Firepower (FDM).

Prerequisites

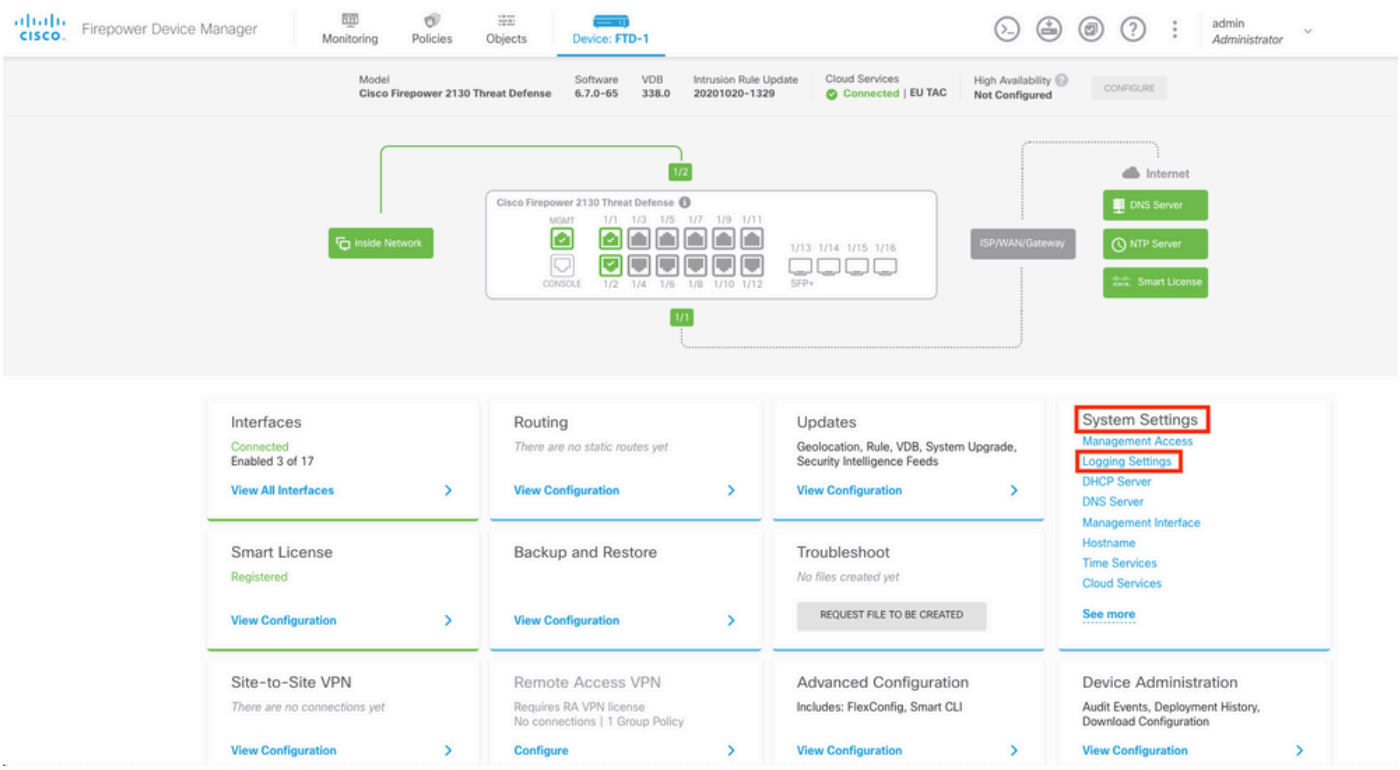
Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

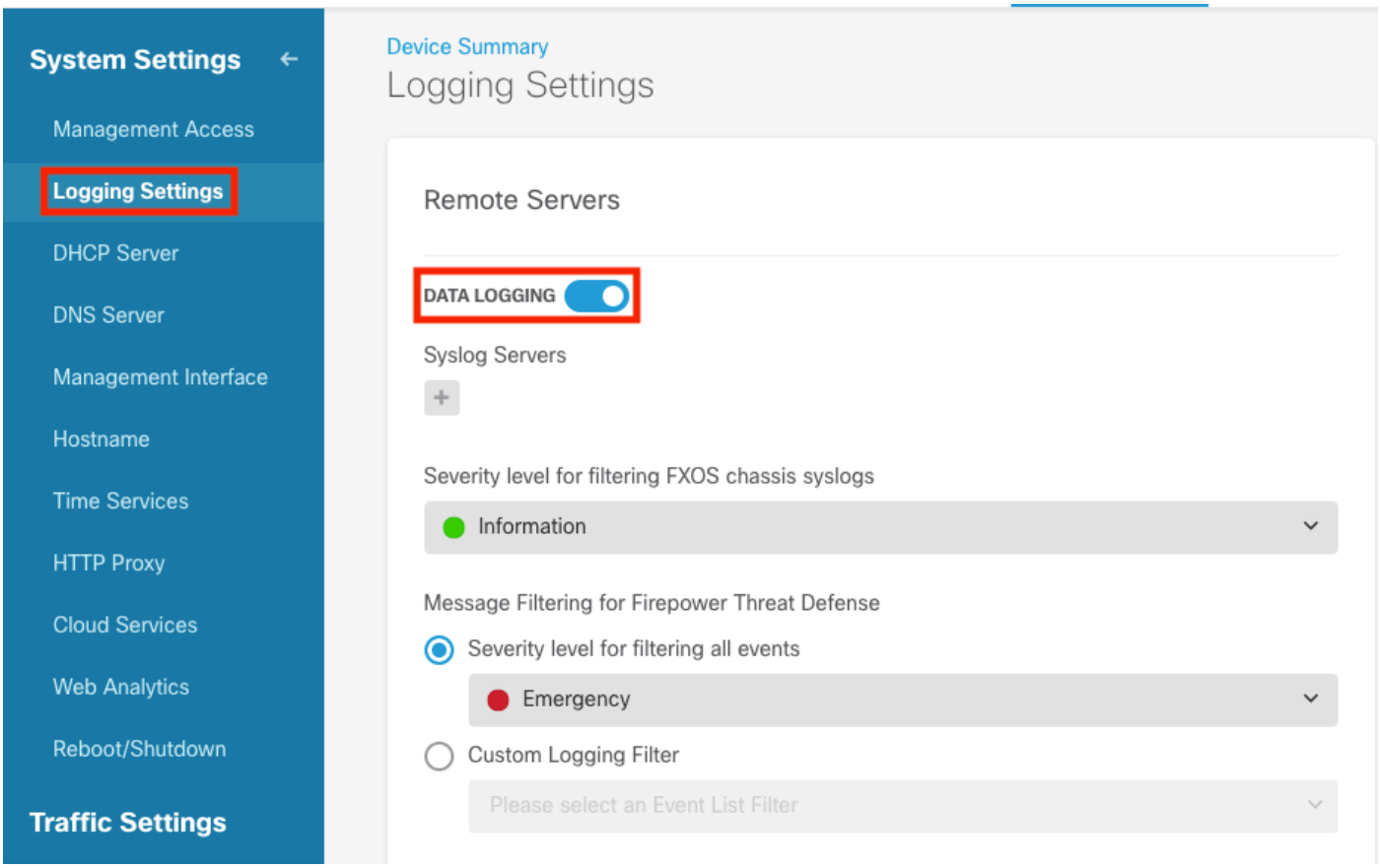
- Firepower Threat Defense
- Servidor Syslog que ejecuta el software Syslog para recopilar datos

Configuraciones

Paso 1. En la pantalla principal del administrador de dispositivos de Firepower, seleccione la configuración de registro en Configuración del sistema en la esquina inferior derecha de la pantalla.



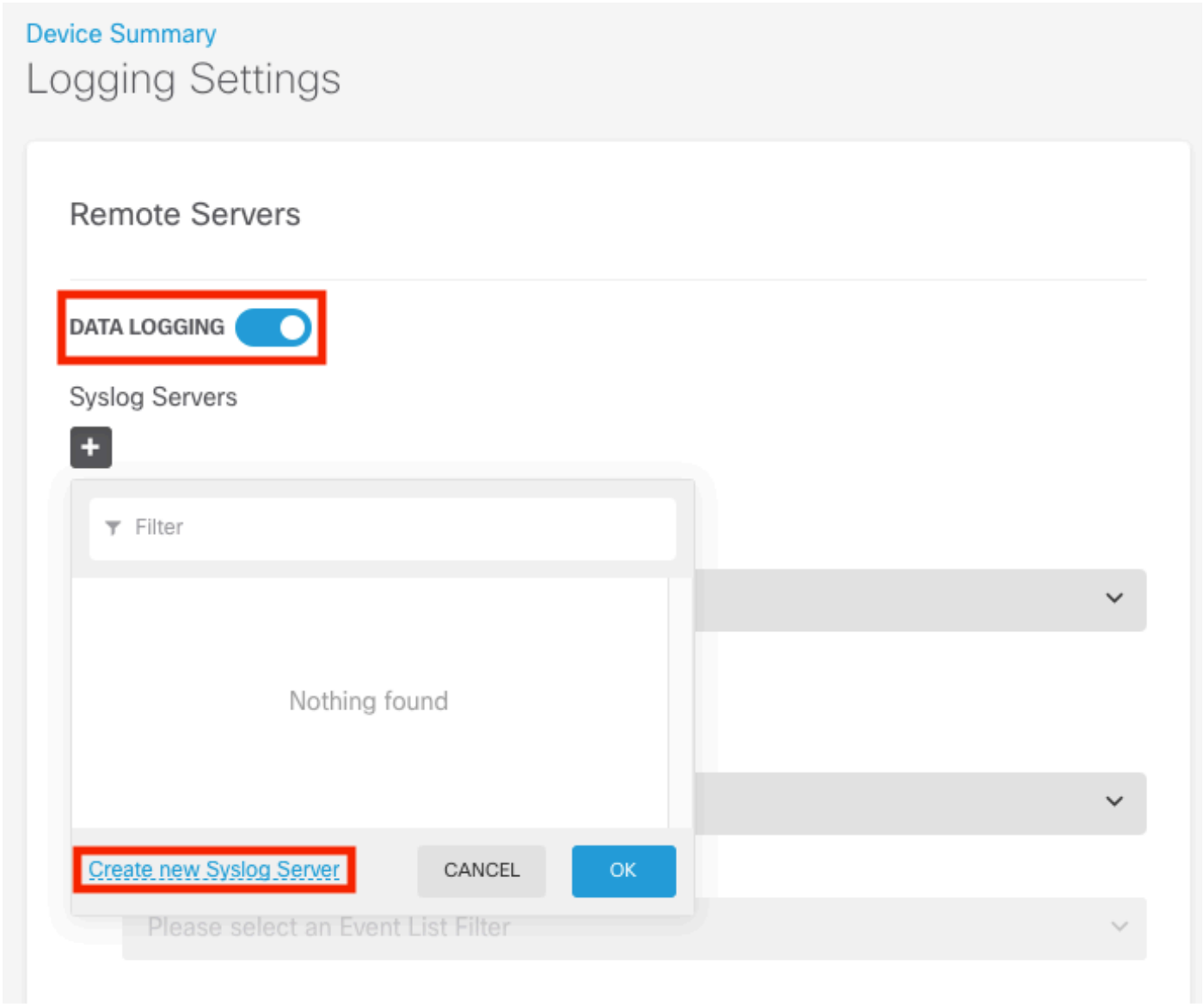
Paso 2. En la pantalla System Settings (Parámetros del sistema), seleccione Logging Settings (Parámetros de registro) en el menú de la izquierda.



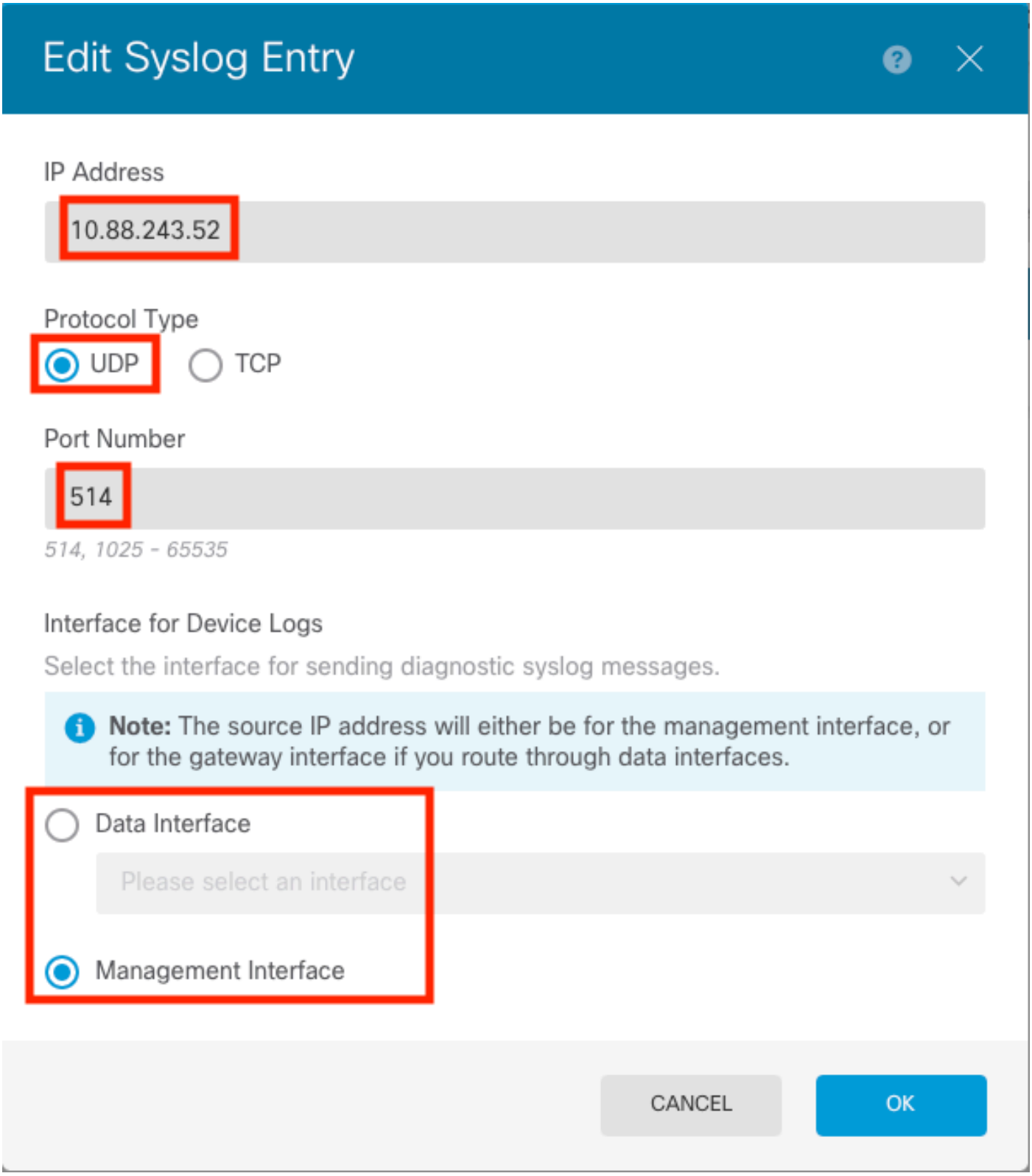
Paso 3. Establezca el interruptor de alternancia Registro de datos seleccionando el signo + en Servidores Syslog.

Paso 4. Seleccione Agregar servidor Syslog. Como alternativa, puede crear el objeto Servidor

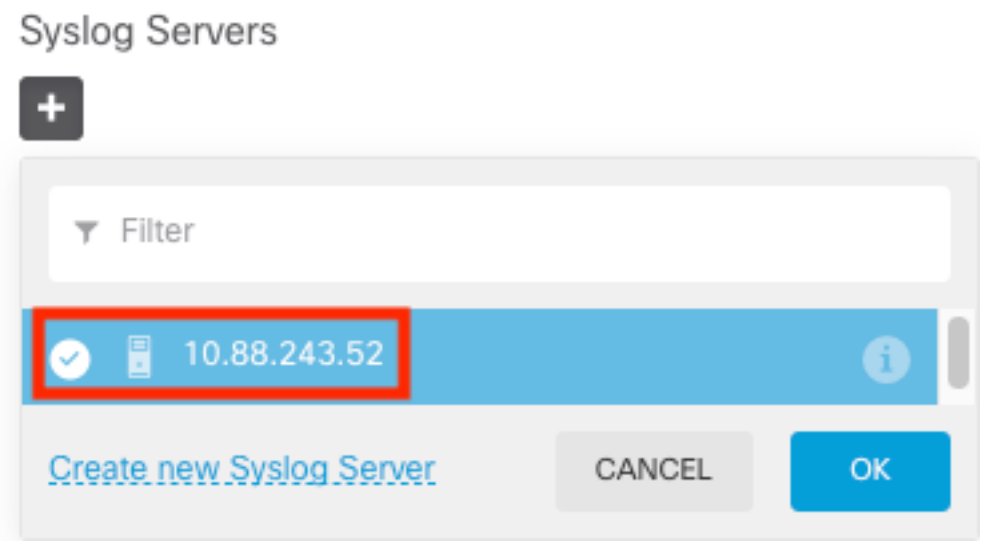
Syslog en Objetos - Servidores Syslog.



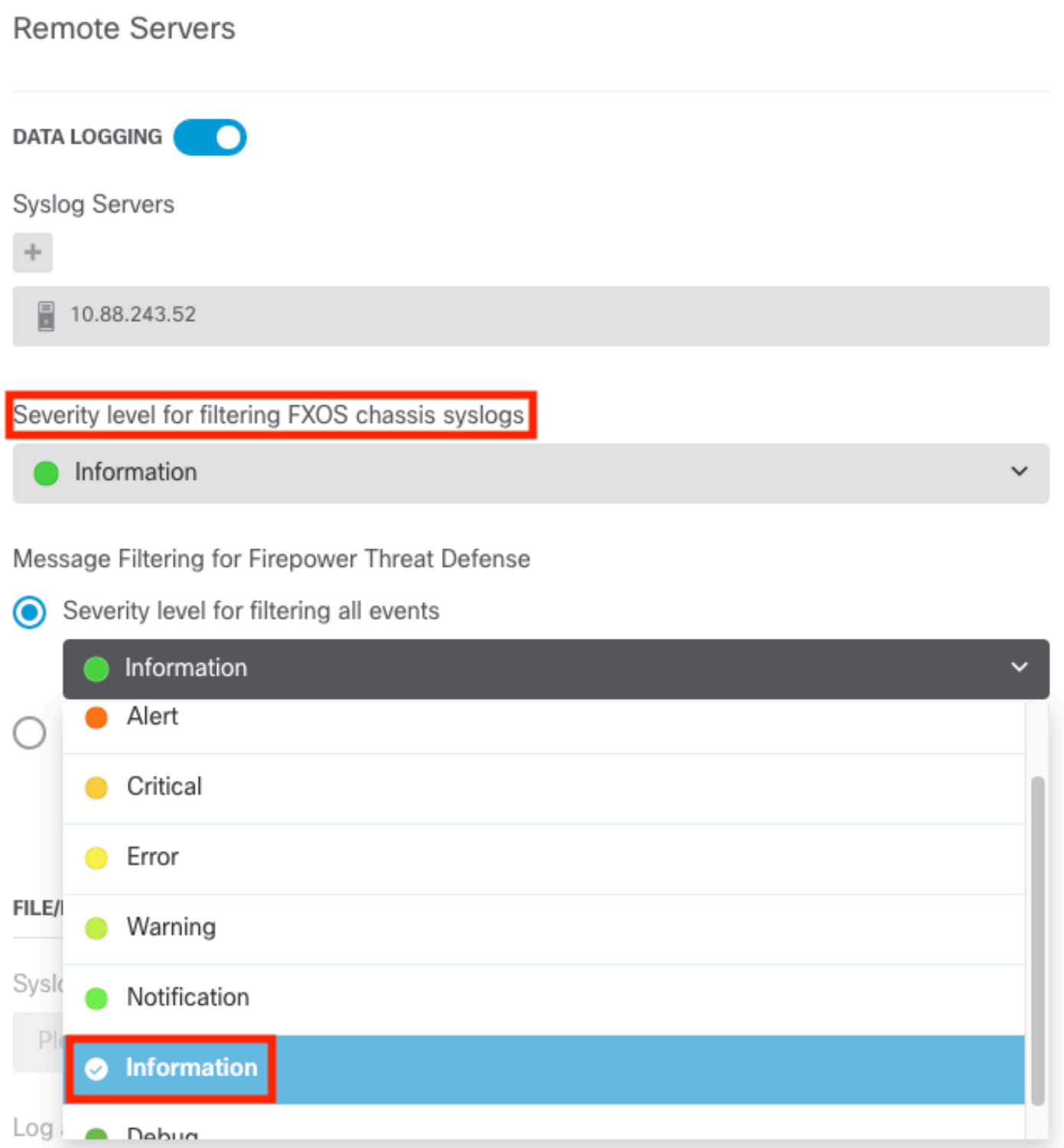
Paso 5. Introduzca la dirección IP del servidor Syslog y el número de puerto. Seleccione el botón de opción de Interfaz de datos y seleccione Aceptar.



Paso 6. A continuación, seleccione el nuevo servidor Syslog y haga clic en Aceptar.

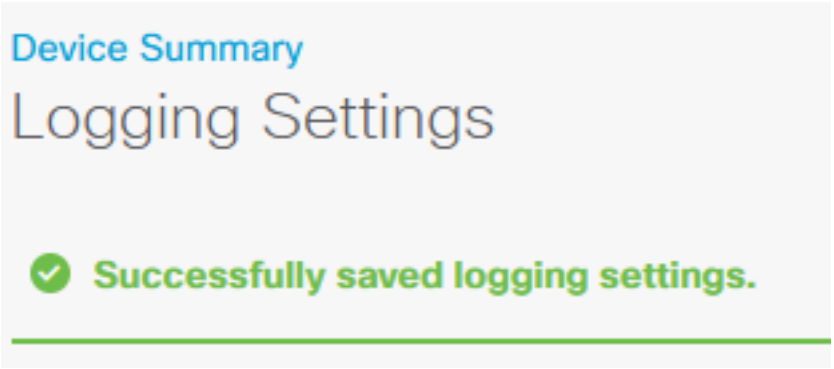


Paso 7. Seleccione el botón de opción Nivel de gravedad para filtrar todos los eventos y seleccione el nivel de registro que desee.



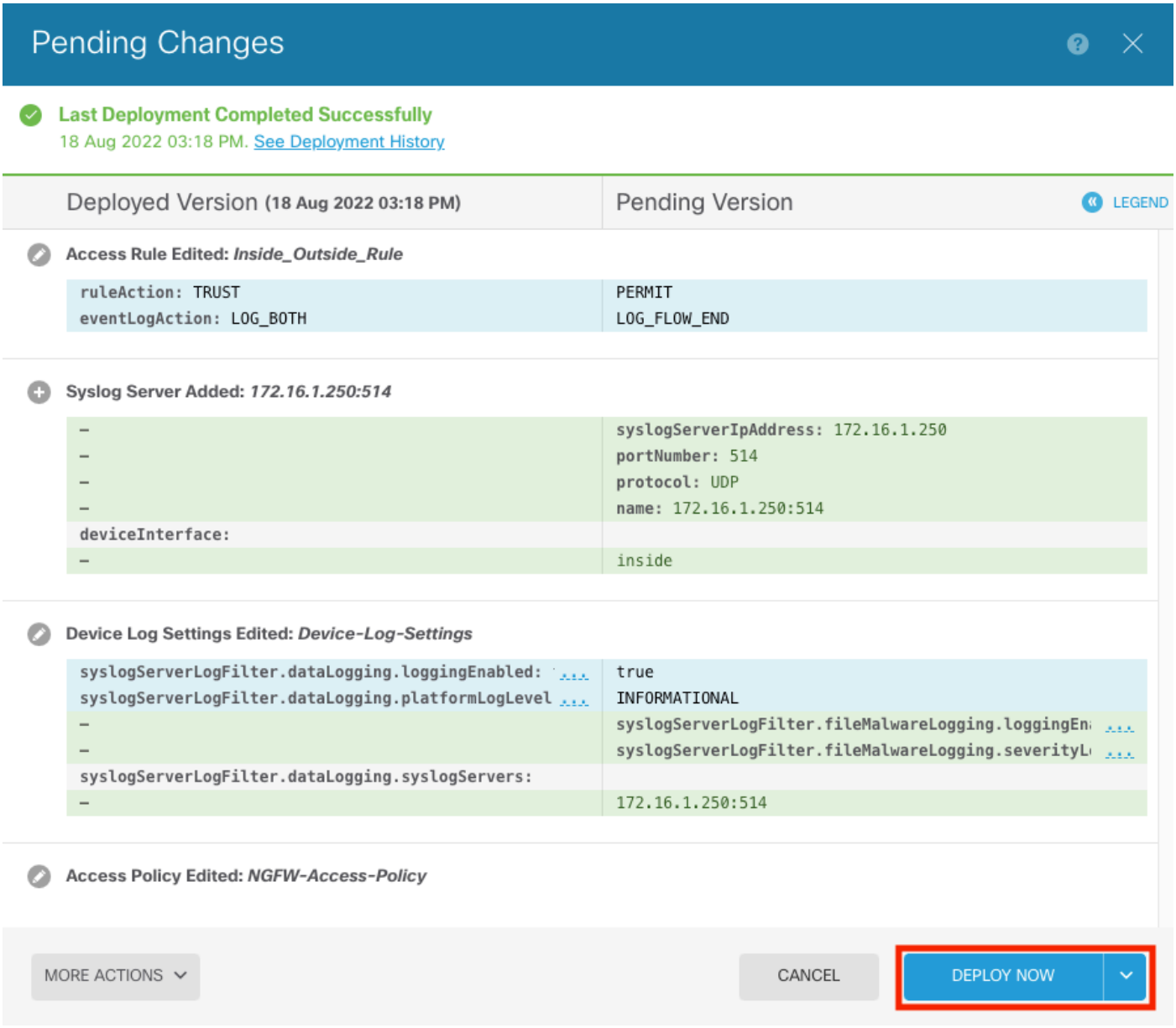
Paso 8. Seleccione Guardar en la parte inferior de la pantalla.

Paso 9. Compruebe que la configuración se ha realizado correctamente.



Paso 10. Implementar la nueva configuración.

Y

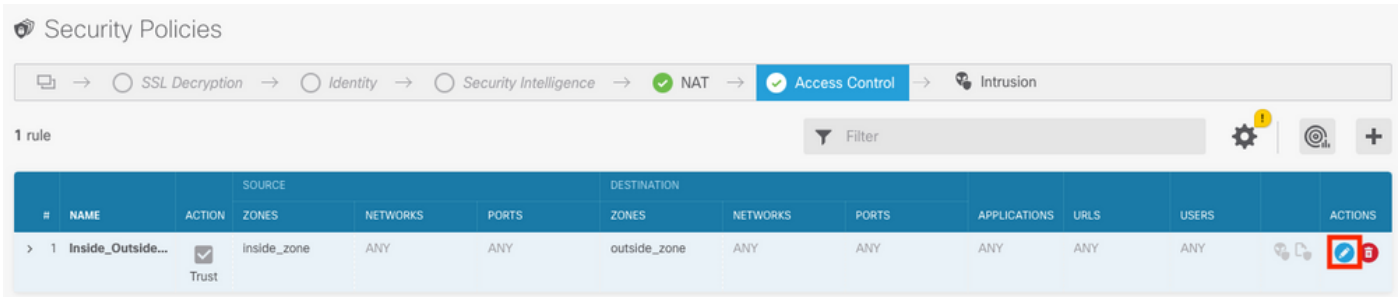


OPCIONAL.

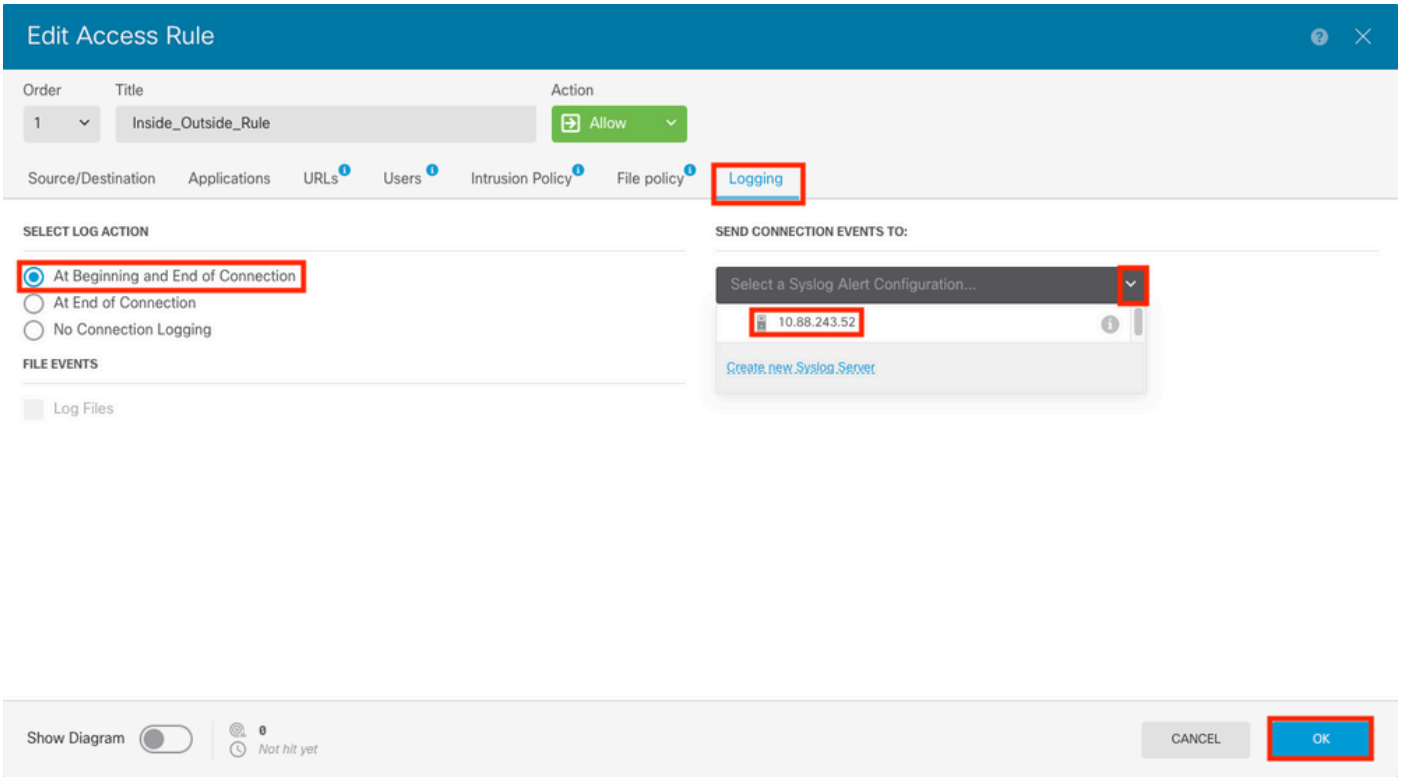
Además, las reglas de control de acceso de la política de control de acceso se pueden configurar para iniciar sesión en el servidor Syslog:

Paso 1. Haga clic en el botón Directivas situado en la parte superior de la pantalla.

Paso 2. Pase el ratón sobre el lado derecho de la regla ACP para agregar el registro y seleccione el icono del lápiz.



Paso 3. Seleccione la ficha Logging (Registro), seleccione el botón de opción At End of Connection (Al final de la conexión), seleccione la flecha desplegable bajo Select a Syslog Alert Configuration (Seleccionar una configuración de alerta de registro del sistema), Select on the Syslog Server (Seleccionar en el servidor de registro del sistema) y Select OK (Aceptar).



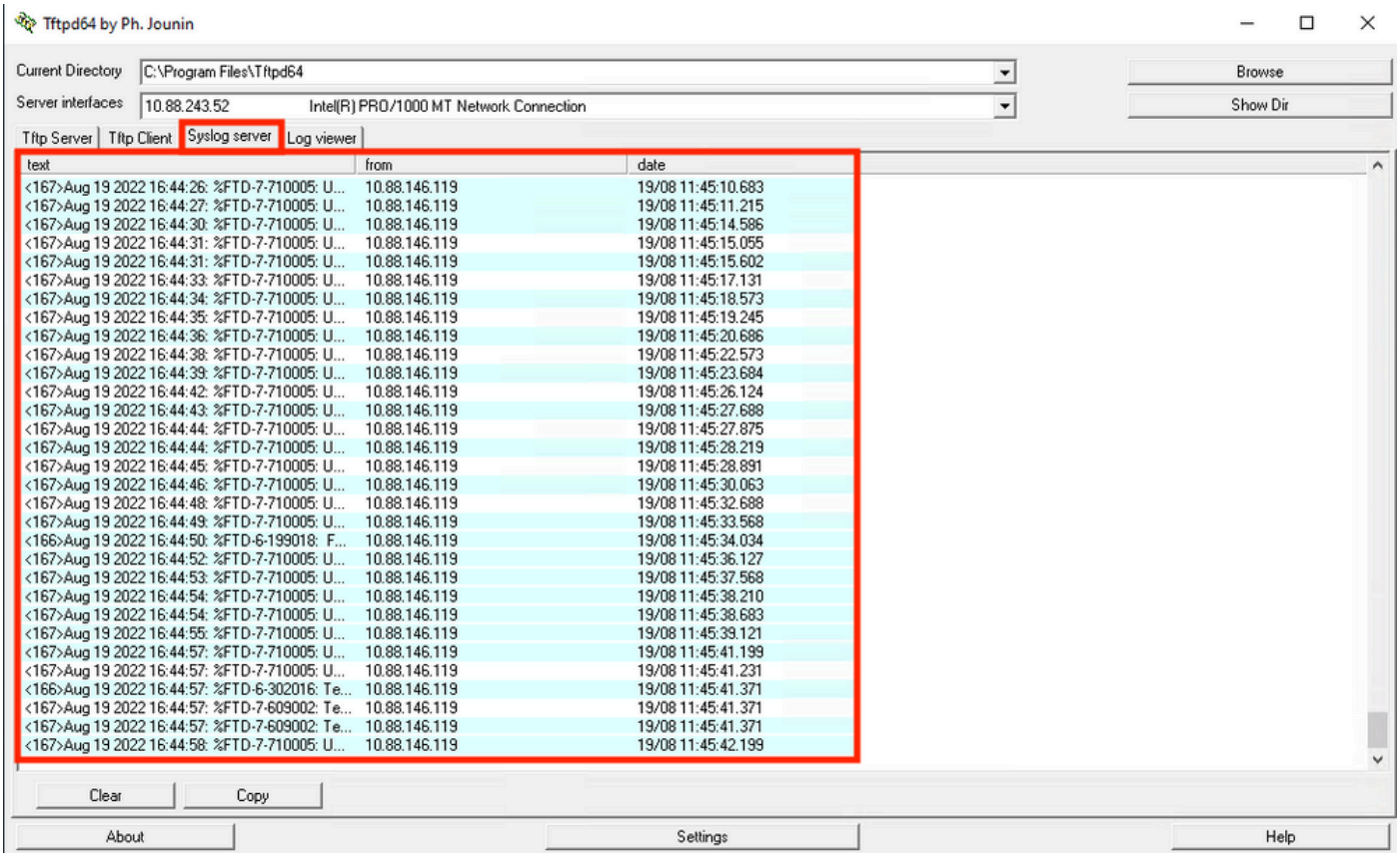
Paso 4. Implemente los cambios de configuración.

Verificación

Paso 1. Una vez completada la tarea, puede verificar la configuración en el modo de suspensión CLI de FTD mediante el 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
>
```

Paso 2. Desplácese hasta el servidor Syslog y compruebe que la aplicación del servidor Syslog acepta mensajes de Syslog.



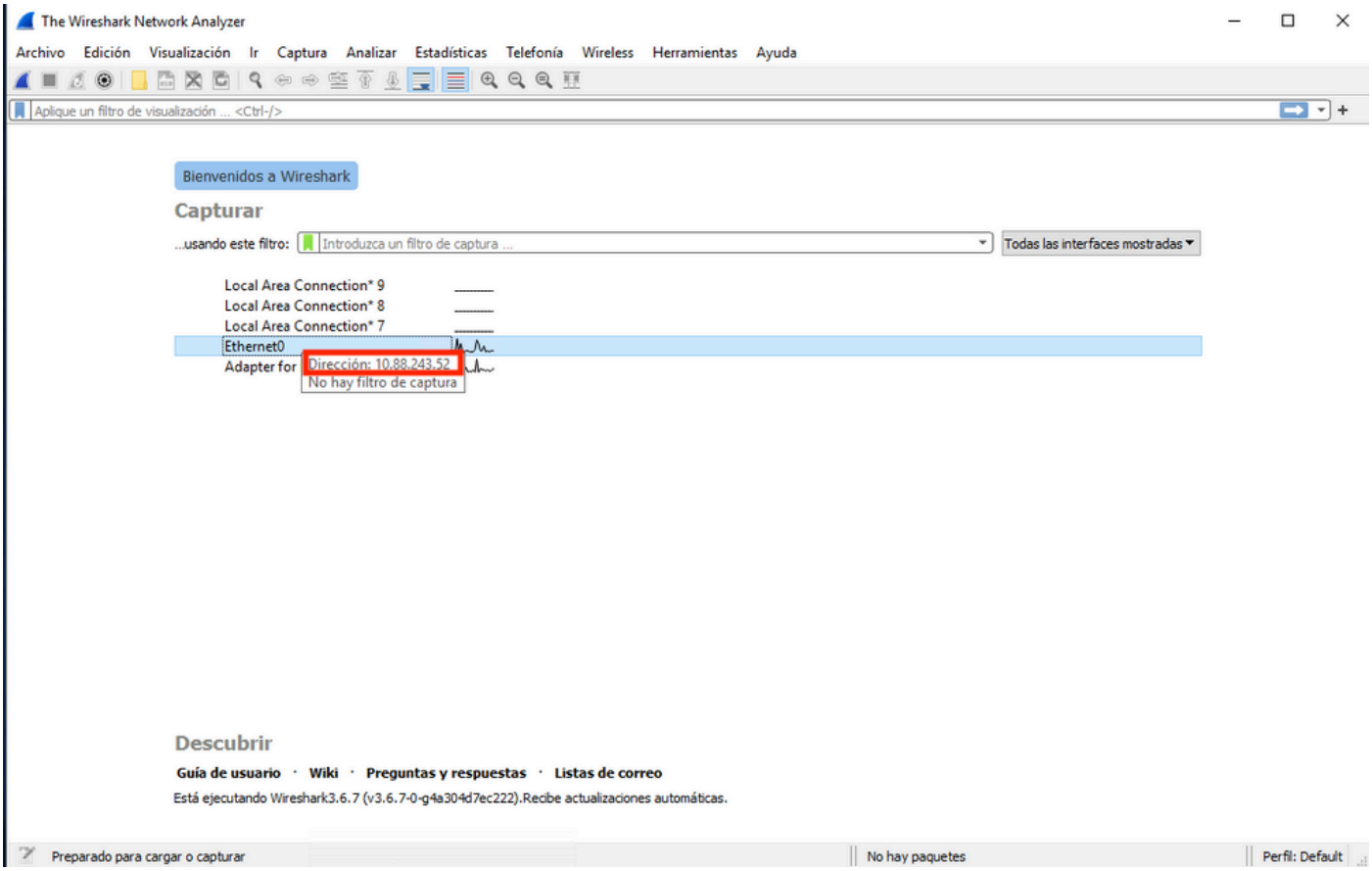
Troubleshoot

Paso 1. Si los mensajes Syslog de la aplicación Syslog generan algún mensaje, realice una captura de paquetes desde la CLI de FTD para comprobar si hay paquetes. Cambie del modo Clish a LINA ingresando el comando **system support diagnostic-cli** en la indicación de clish.

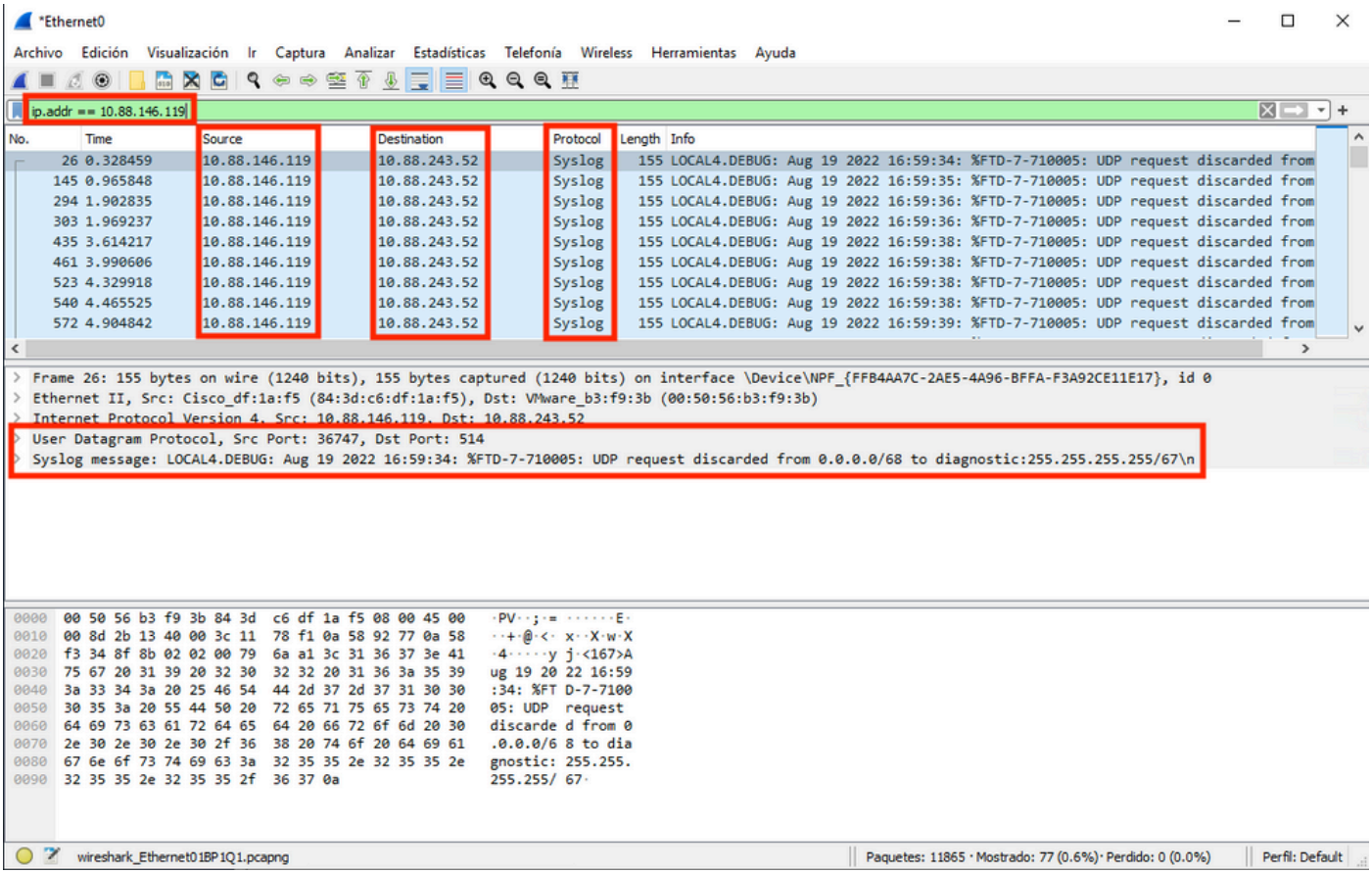
```
[> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

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

Paso 2. Cree una captura de paquetes para su udp 514 (o tcp 1468 si utilizó tcp)

Paso 3. Verifique que la comunicación esté llegando a la tarjeta de interfaz de red en el servidor Syslog. Utilice Wireshark u otra utilidad de captura de paquetes cargada. Haga doble clic en la interfaz de Wireshark para que el servidor Syslog comience a capturar paquetes.



Paso 4. Establezca un filtro de visualización en la barra superior para udp 514. Para ello, escriba udp.port==514 y seleccione la flecha situada a la derecha de la barra. Desde la salida, confirme si los paquetes están llegando al servidor Syslog.



Paso 5. Si la aplicación de servidor Syslog no muestra los datos, solucione el problema en la aplicación de servidor Syslog. Asegúrese de que se esté utilizando el protocolo correcto udp/tcp y el puerto correcto 514/1468.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).