Configuración y prueba de la política de archivos de AMP mediante FDM

Contenido

Introducción

Este documento describe cómo configurar y probar una política de protección frente a malware avanzado (AMP) mediante Firepower Device Manager (FDM).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Administrador de dispositivos Firepower (FDM)
- Firepower Threat Defense (FTD)

Componentes Utilizados

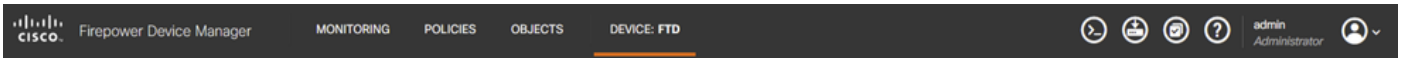
- FTD virtual de Cisco versión 7.0 gestionada mediante FDM
- Licencia de evaluación (la licencia de evaluación se utiliza con fines de demostración. Cisco recomienda adquirir y utilizar una licencia válida)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Instrucciones

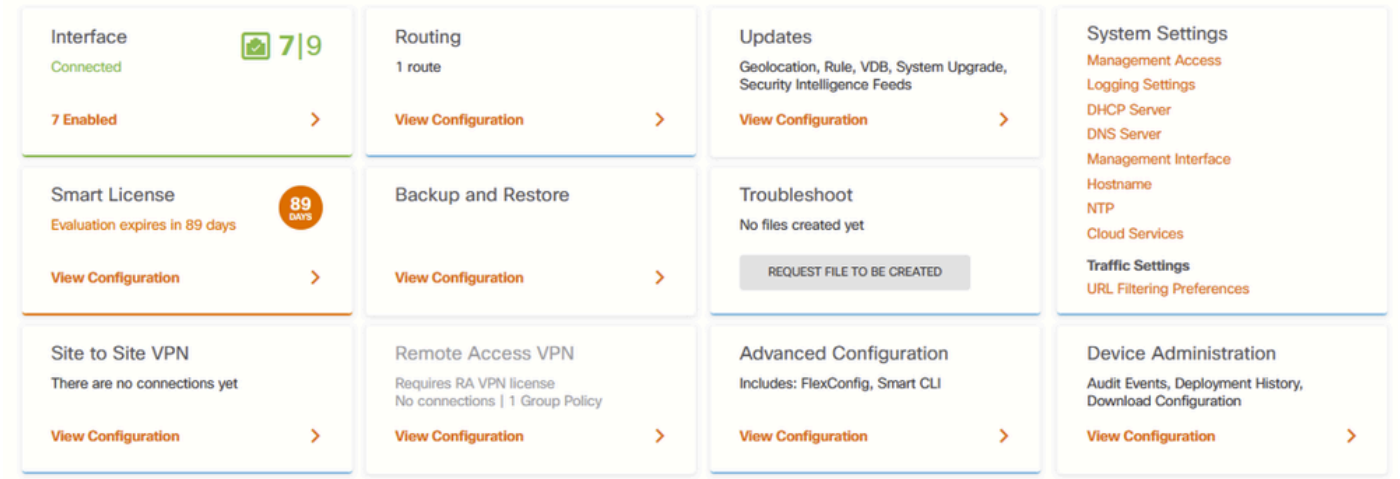
Licencias

1. Para habilitar la licencia de malware, navegue hasta la página DEVICE en la GUI de FDM.



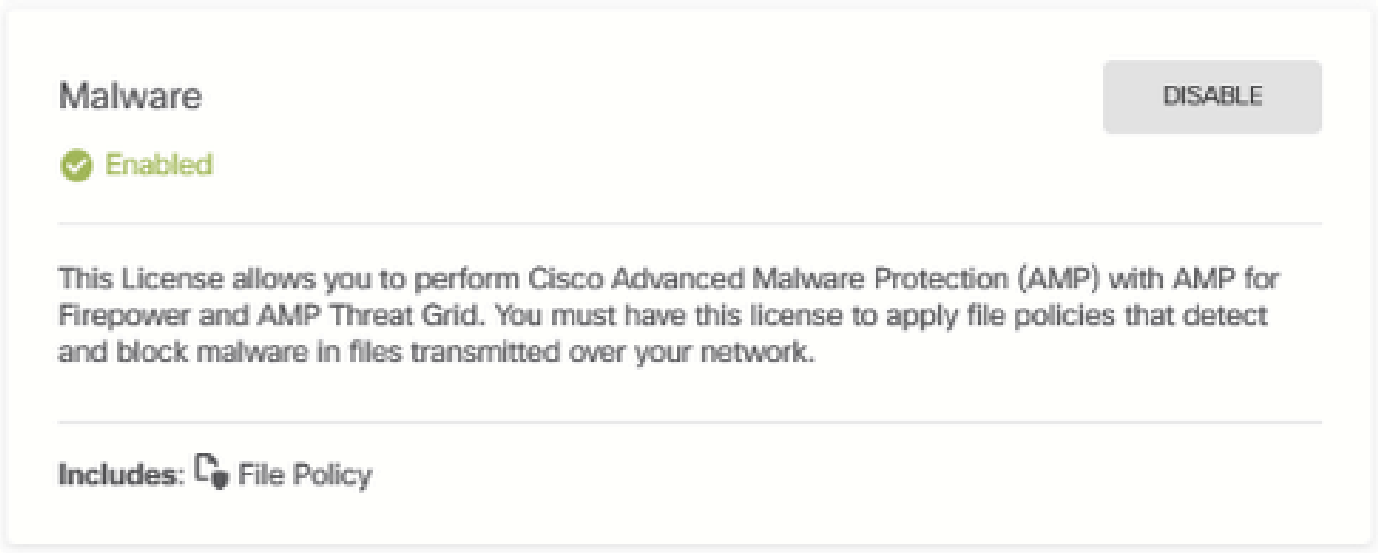
Ficha Dispositivo de FDM

2. Busque el cuadro Smart License y haga clic en View Configuration.



Página Dispositivo FDM

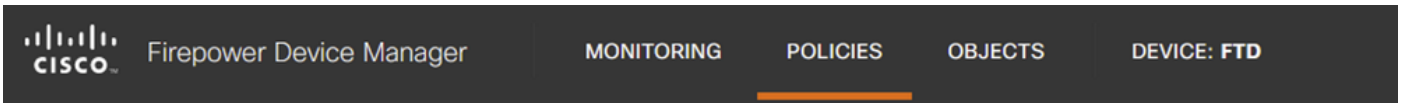
3. Active la licencia con el nombre Malware.



Licencia de malware

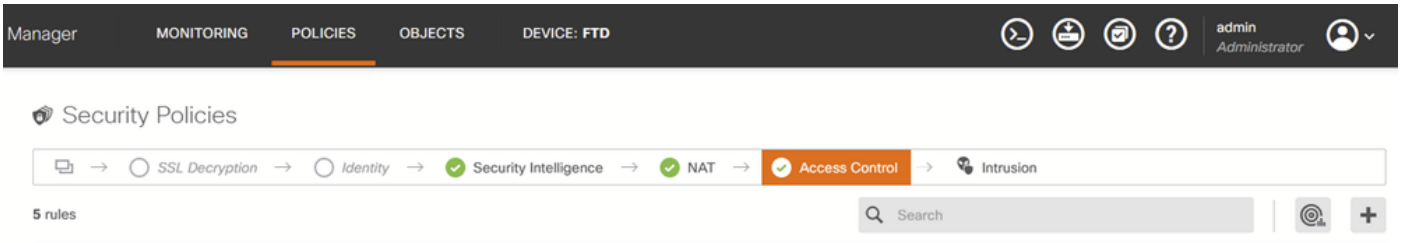
Configuración

1. Acceda a la página POLÍTICAS de FDM.



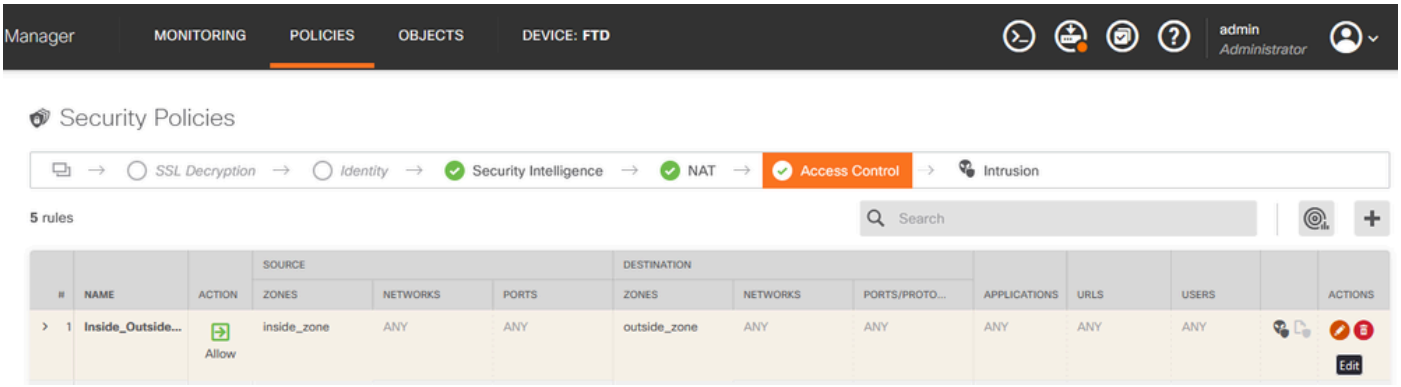
Ficha Directivas de FDM

2. En Políticas de seguridad, navegue hasta la sección Control de acceso.



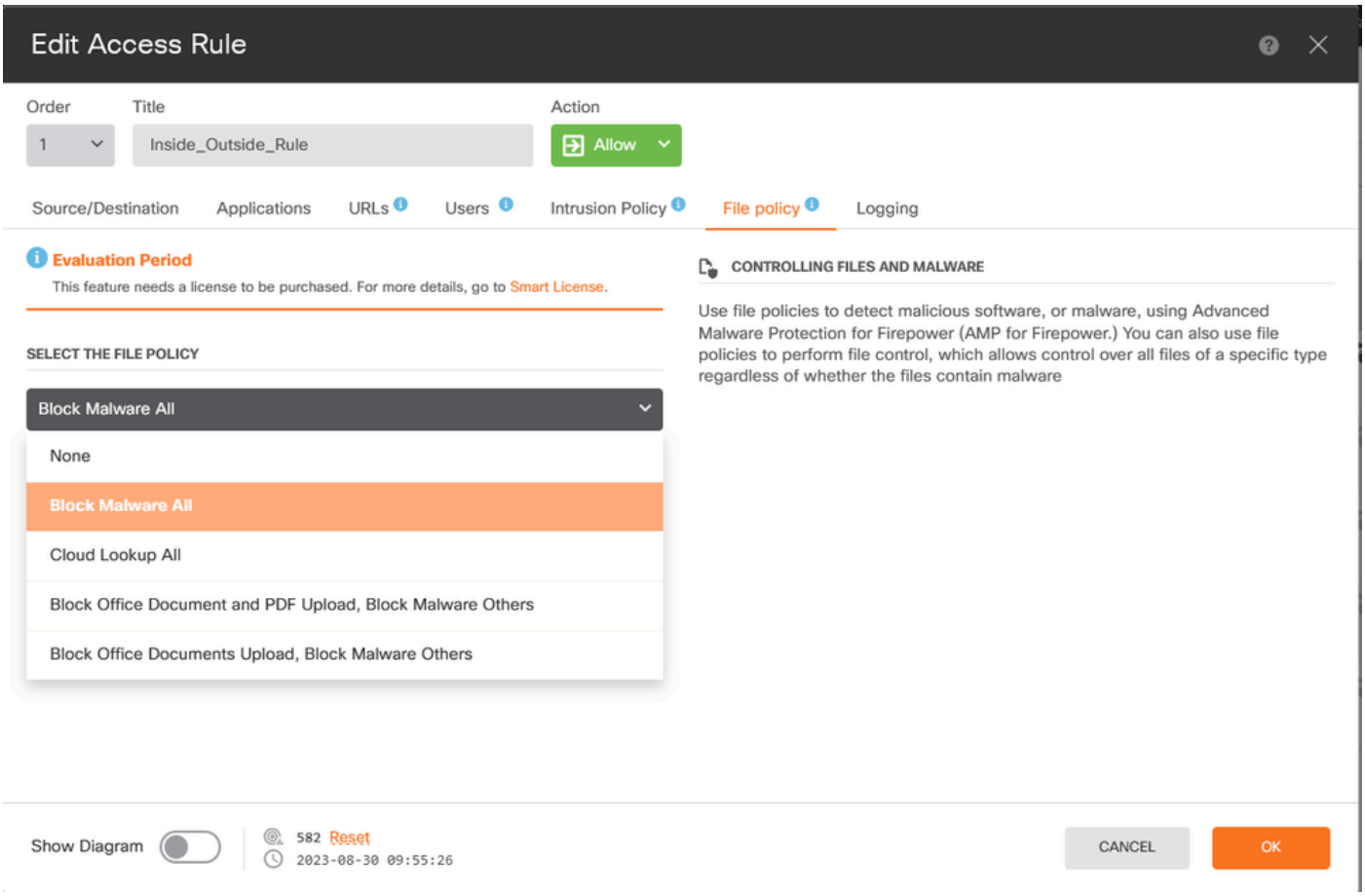
Ficha Control de acceso a FDM

3. Busque o cree una regla de acceso para configurar la política de archivos. Haga clic en el editor de Access Rule. Para obtener instrucciones sobre cómo crear una regla de acceso, consulte este enlace.



Regla de control de acceso de FDM

4. Haga clic en la sección Política de Archivos en la Regla de Acceso y seleccione la opción preferida Política de Archivos del menú desplegable. Haga clic en Aceptar para guardar los cambios en la regla.

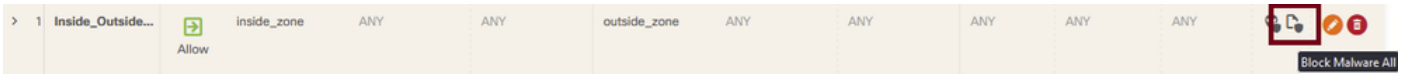


Ficha Directiva de archivo de regla de control de acceso de FDM

5. Confirme que la política de archivos se ha aplicado a la regla de acceso comprobando si el icono Política de archivos está activado.

Icono

de



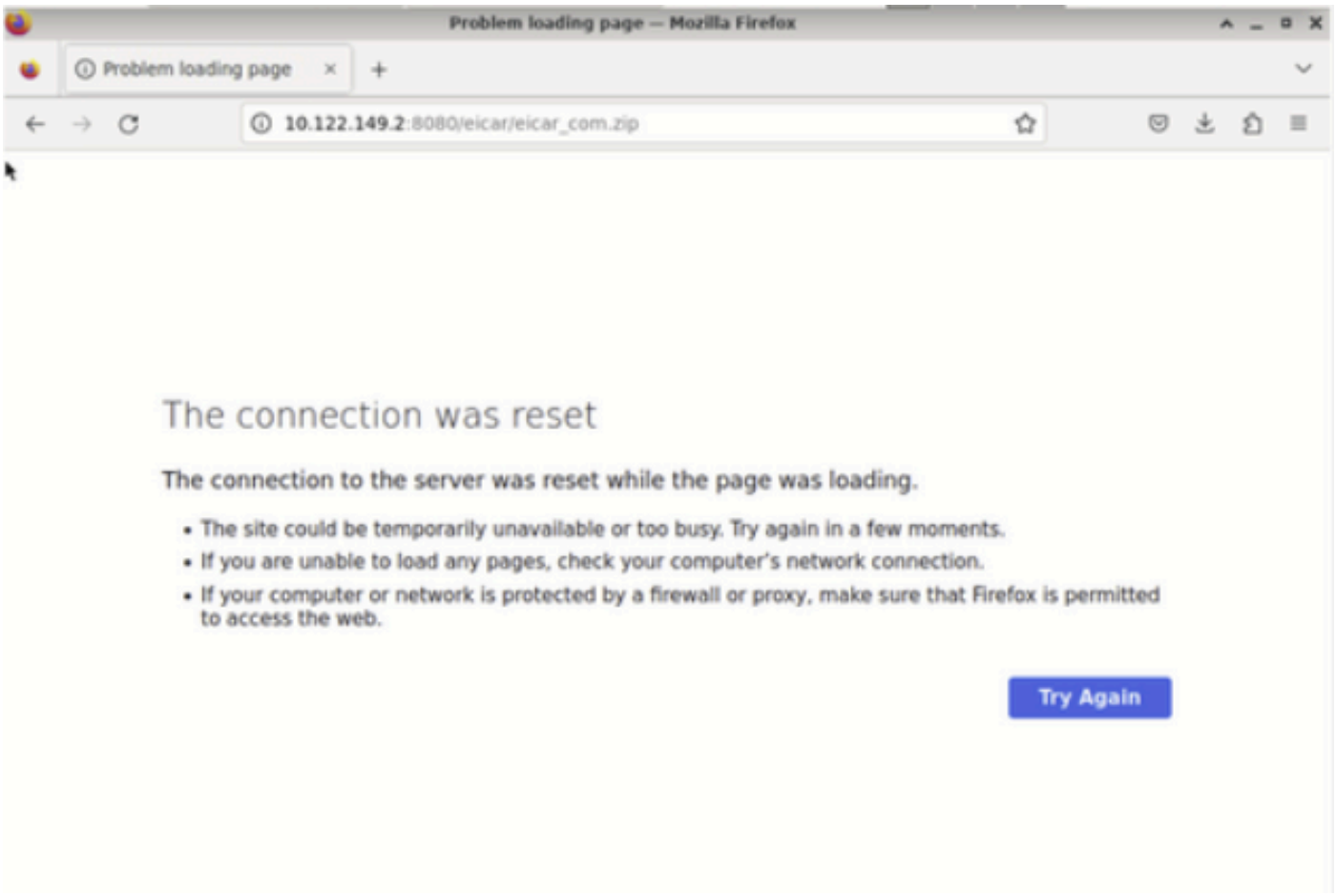
directiva de archivos habilitado

6. Guarde e implemente los cambios en el dispositivo administrado.

Prueba

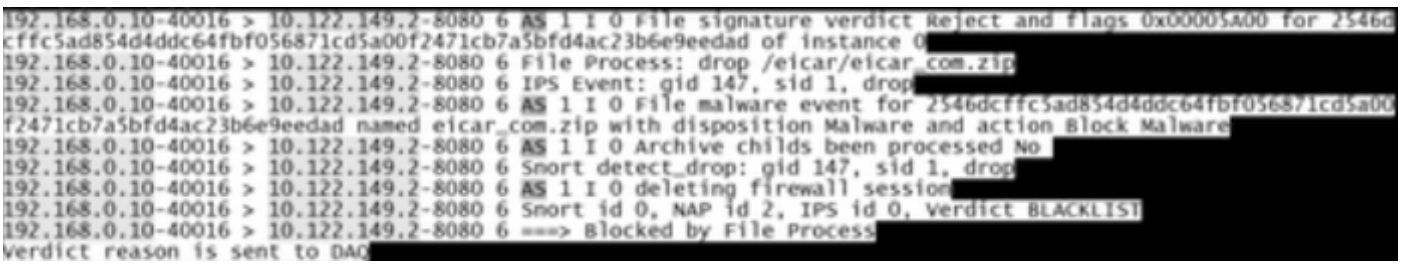
Para verificar que la política de archivos configurada para la protección frente a malware funciona, utilice estos intentos de escenario de prueba para descargar un archivo de prueba de malware desde el navegador web de un host final.

Como se muestra en esta captura de pantalla, no se puede descargar un archivo de prueba de malware desde el navegador web.



Prueba de descarga del navegador

Desde la CLI de FTD, el seguimiento de compatibilidad del sistema muestra que el proceso de archivo bloqueó la descarga del archivo. Para obtener instrucciones sobre cómo ejecutar un seguimiento de soporte del sistema a través de la CLI de FTD, consulte este enlace.



Prueba de seguimiento de compatibilidad del sistema

Esto confirma que la configuración de la política de archivos bloqueó correctamente el malware.

Resolución de problemas

En caso de que el malware no se bloquee correctamente al utilizar las configuraciones anteriores, consulte estas sugerencias de solución de problemas:

1. Compruebe que la licencia de malware no ha caducado.

2. Confirme que la regla de control de acceso está dirigida al tráfico correcto.

3. Confirme que la opción de política de archivos seleccionada es correcta para el tráfico dirigido y la protección contra malware deseada.

Si el problema sigue sin resolverse, póngase en contacto con el TAC de Cisco para obtener asistencia adicional.

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).