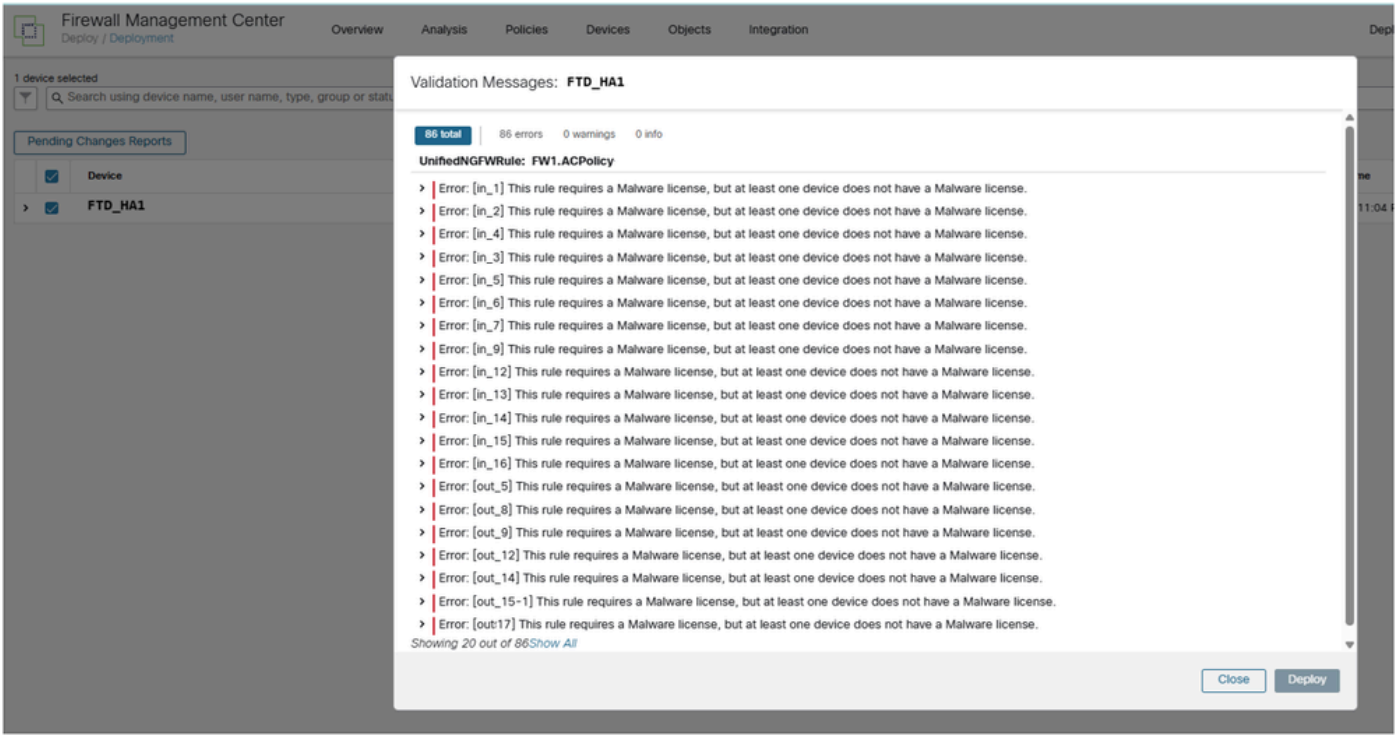
Solución de problemas de error de licencia de malware en la implementación de políticas FTD

Contenido

Problema

Al intentar realizar cambios de políticas en Cisco Secure Firewall Management Center (FMC), aparece un mensaje de error que indica que "esta regla requiere una licencia de malware, pero al menos un dispositivo no tiene una licencia de malware". Este error impide que los cambios de configuración e implementación de políticas se apliquen a los dispositivos de firewall afectados.

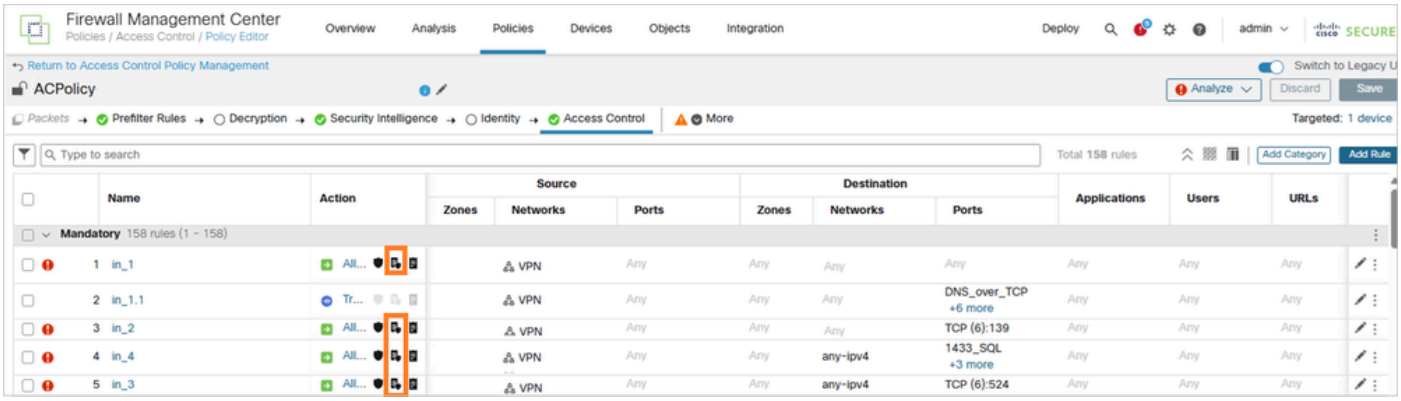


Entorno

- FMC 7.4.2. Otras versiones de software también se ven afectadas.
- FPR1140 ejecuta Firewall Threat Defence (FTD). Otras plataformas también se ven

afectadas.

- FTD utiliza una política de control de acceso (ACP) con la política de archivos activada en una o más reglas.



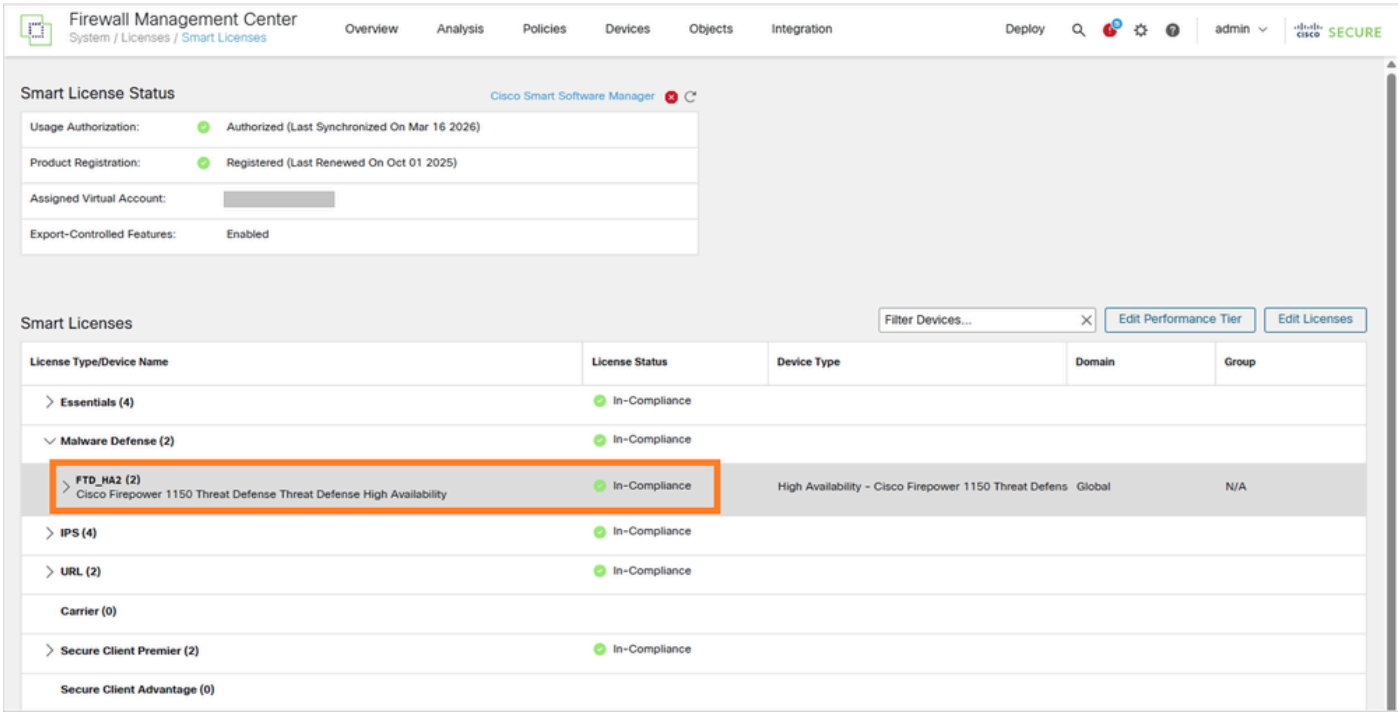
Resolución

La resolución de este error de licencia de malware implica la obtención e instalación de la licencia de Malware necesaria en el dispositivo afectado. Siga estos pasos para resolver el problema:

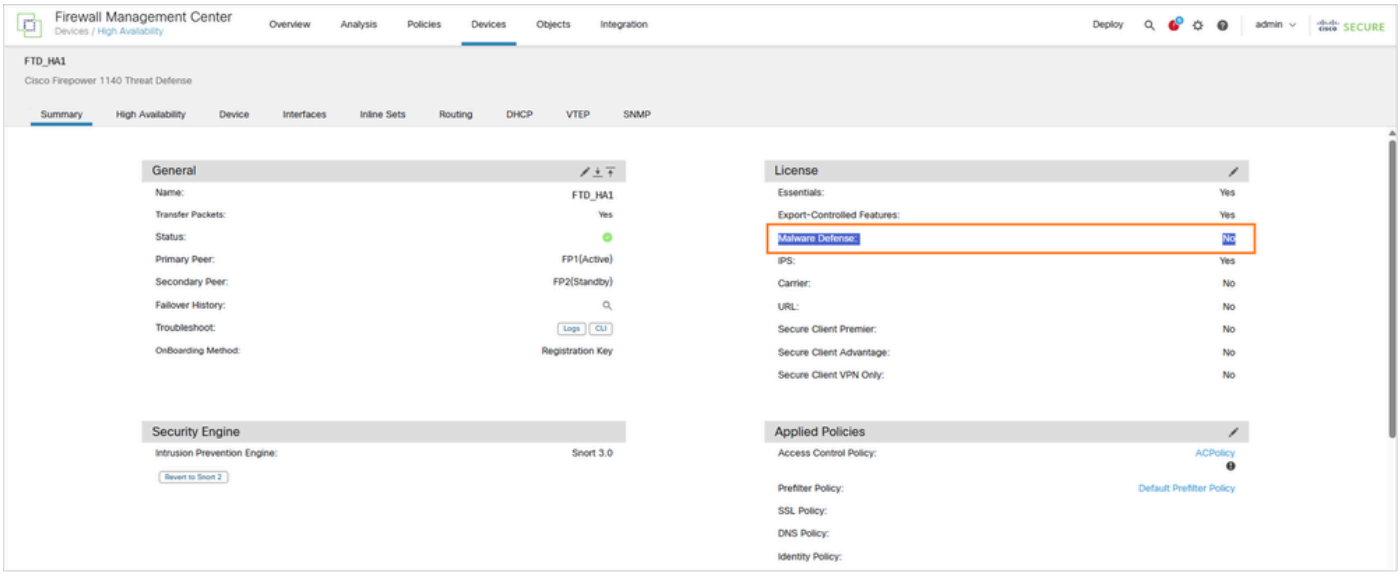
Paso 1. Identificar la brecha de la licencia

Verifique que el dispositivo de firewall afectado tenga políticas de archivos configuradas para utilizar la protección frente a malware avanzado (AMP), pero carezca de la licencia de defensa frente a malware correspondiente. Esto se puede confirmar comprobando la configuración del dispositivo y comparándola con las licencias disponibles.

En este caso, solo el par FTD_HA2 tiene la licencia de malware. El par FTD_HA1 no lo tiene:



El par de firewalls FTD_HA1 tiene la licencia de malware establecida en No:



Paso 2. Obtenga la licencia necesaria

Póngase en contacto con su representante de ventas o partner autorizado de Cisco para obtener la licencia de malware necesaria para el dispositivo afectado. La licencia debe ser adecuada para su modelo de firewall específico y los requisitos de implementación.

Paso 3. Instalación de la licencia de malware

Una vez obtenida la licencia, instálela en el dispositivo afectado mediante el proceso de licencias estándar de Cisco. Normalmente, esto implica aplicar la licencia a través del FMC o directamente en el dispositivo, según la configuración de gestión.

Paso 4. Verificación de la instalación de la licencia

Después de la instalación de la licencia, compruebe que la función de defensa frente a malware esté ahora habilitada correctamente y que se haya borrado el error de licencia.

Paso 5. Prueba de implementación de políticas

Intente implementar de nuevo los cambios de directiva para confirmar que el problema de licencia se ha resuelto y que las operaciones de directiva pueden continuar normalmente.

Causa

El error se produce debido a una discordancia en la validación de licencias en la que las políticas de archivos se configuran para usar la funcionalidad de AMP, pero la licencia de defensa frente a malware correspondiente no se instala ni se activa en el dispositivo de firewall afectado. El FMC aplica el cumplimiento de las licencias e impide la implementación de políticas cuando faltan licencias necesarias, incluso si las políticas están configuradas técnicamente.

Esta validación garantiza que solo se implementen en los dispositivos las funciones con licencia adecuada, lo que mantiene el cumplimiento de los requisitos de licencia de Cisco y evita el uso de funciones sin licencia.

Contenido relacionado

- Soporte técnico y descargas de Cisco

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).