Implementación de configuración de plataforma para resolución de problemas de VPN

Contenido

Introducción

Este documento describe cómo organizar e identificar fácilmente los registros de depuración de VPN usando Secure Firewall Management Center y Secure Firewall Threat Defence.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Protección frente a amenazas de firewall (FTD)
- Centro de gestión de firewall seguro (FMC)

- Comprensión básica de la navegación por la GUI de FMC y la CLI de FTD
- Asignación de directiva existente para la configuración de la plataforma

Componentes Utilizados

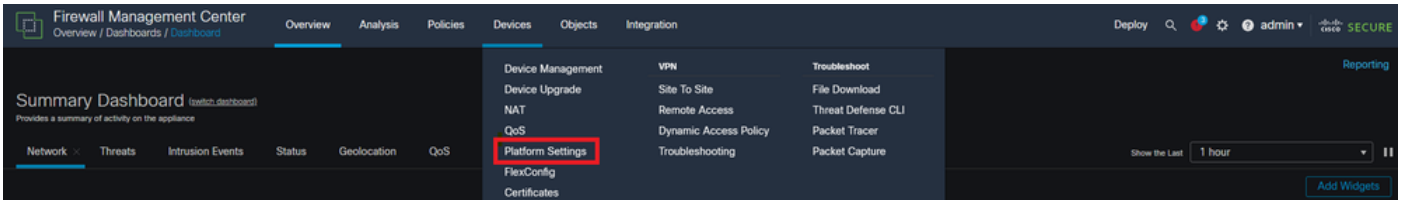
La información de este documento se basa en las siguientes versiones de software y hardware:

- Firewall Management Center versión 7.3
- Firewall Threat Defence versión 7.3

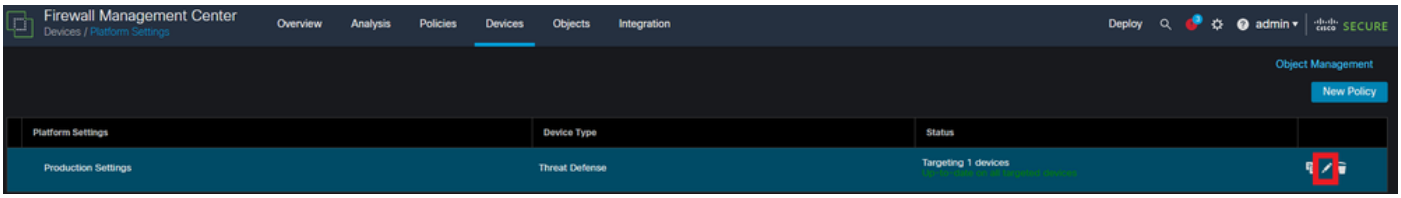
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender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

Centro de gestión de firewall

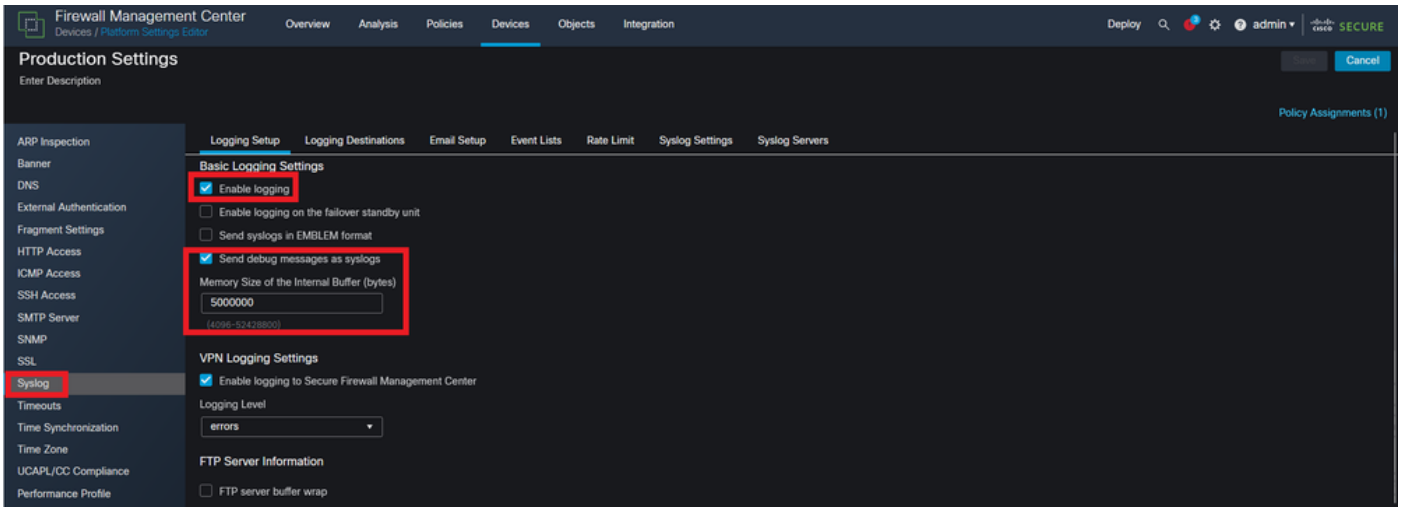
Vaya a . Devices > Platform Settings



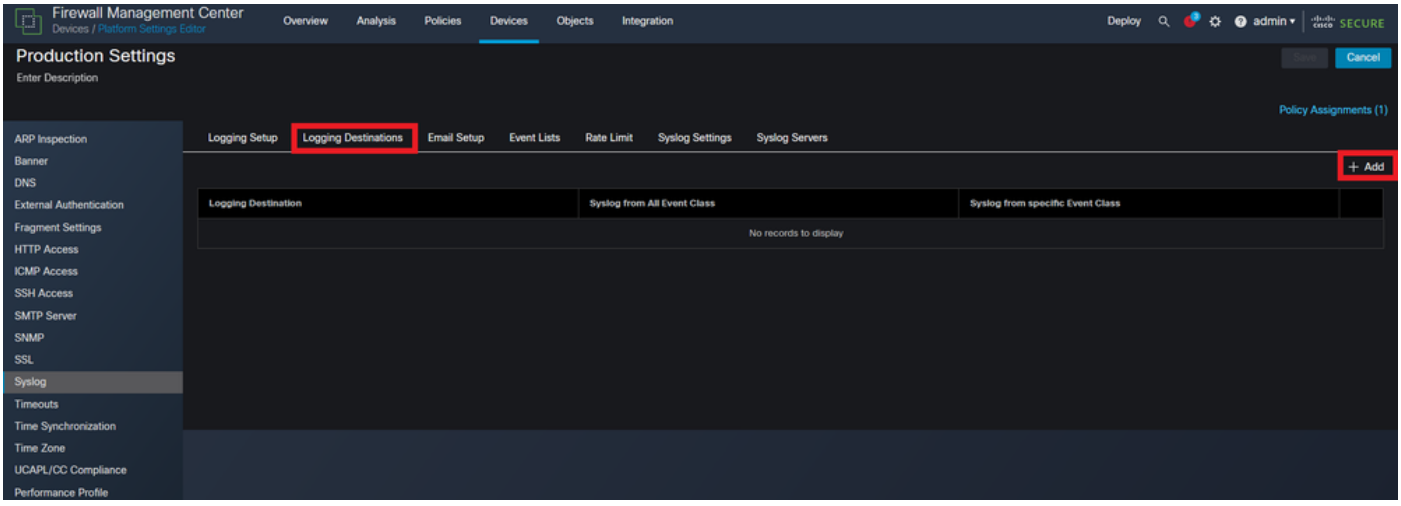
Haga clic en el **pencil** símbolo situado entre copy y delete icon.



Desplácese hasta Syslogen la columna izquierda de opciones y asegúrese de que **Enable Logging**, y **Send debug messages as syslog** están activados. Además, asegúrese de que Memory Size of the Internal Buffer se ha establecido un valor adecuado para la resolución de problemas.

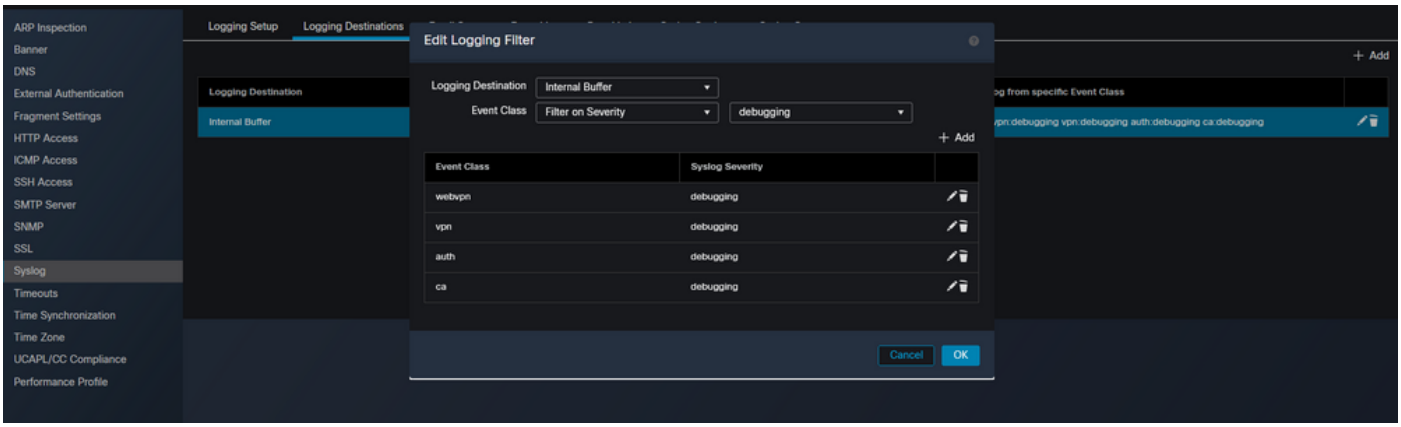


Haga **Logging Destinations** clic en y, a continuación, en **+Add**.



En esta sección, el destino del registro es una preferencia del administrador y **Internal Buffer** se

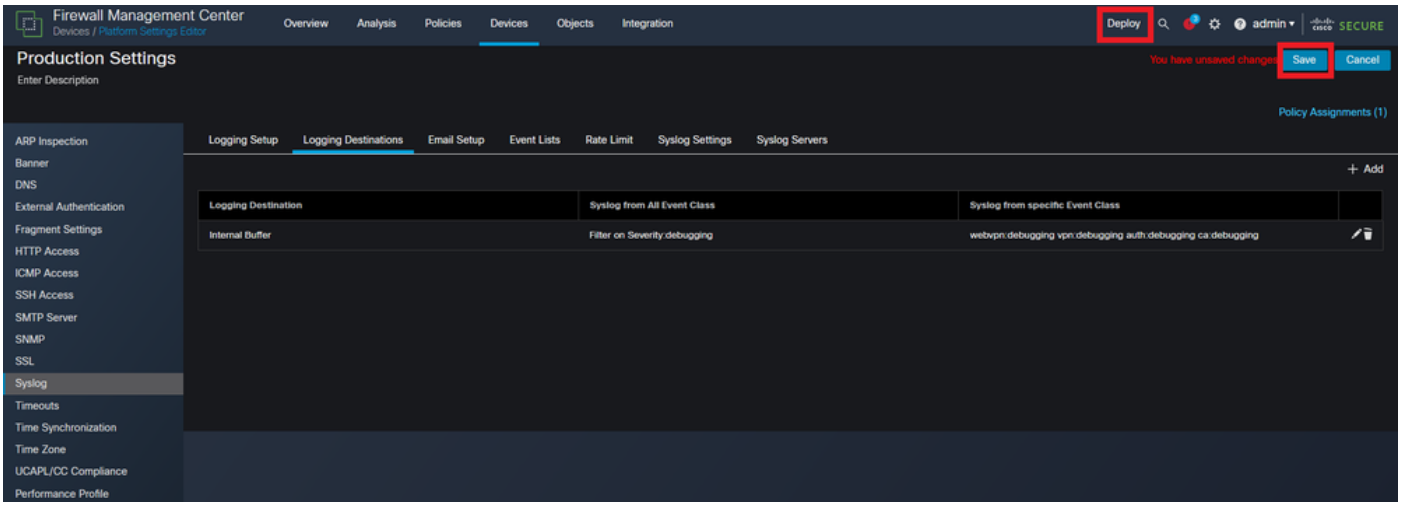
utiliza. Cambie **Event Class** a Una **Filter on Severity and debugging**. vez que se haya completado esto, haga clic en +Add y elija webvpn, vpn, auth, y caall con la gravedad Syslog de debugging. Este paso permite al administrador filtrar estos resultados de depuración a un mensaje syslog específico de 711001. Estos resultados se pueden modificar según el tipo de solución de problemas. Sin embargo, los elegidos en este ejemplo cubren los problemas más comunes relacionados con el sitio a sitio, el acceso remoto y AAA VPN.



Cree clases de eventos y filtros para los debugs.

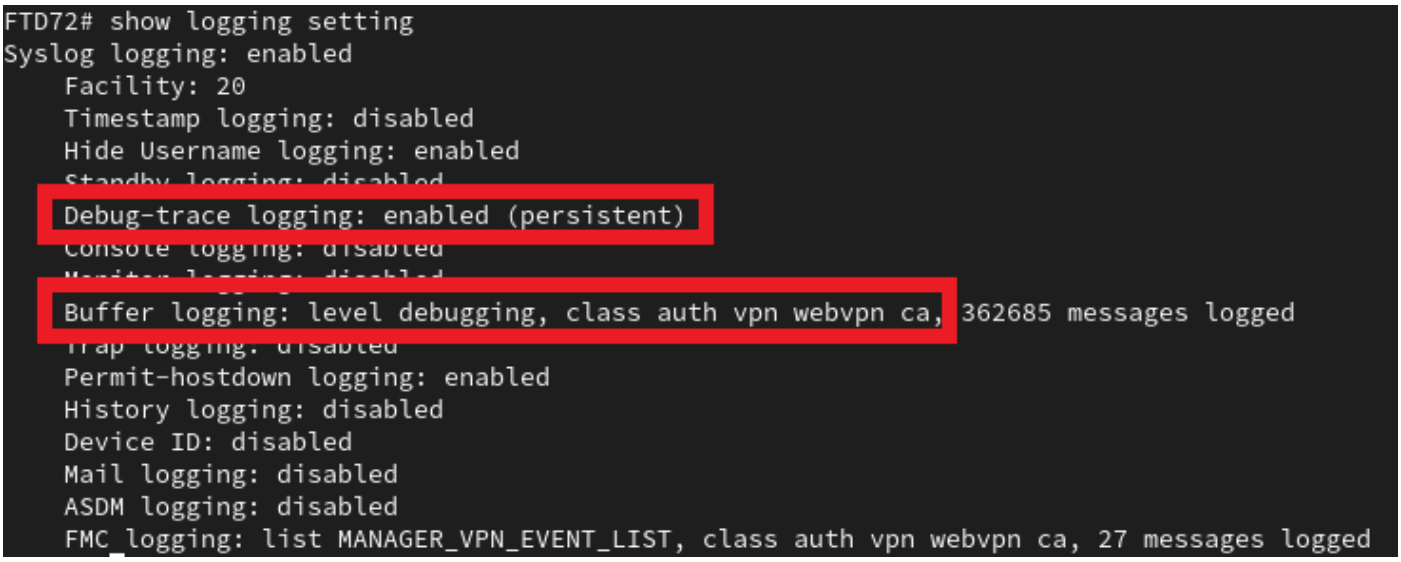
Advertencia: Esto cambia el nivel de registro de búfer a depuración y registra eventos de depuración para las clases especificadas en el búfer interno. Se recomienda utilizar este método de registro para solucionar problemas, y no para un uso a largo plazo.

Choose Save en la parte superior derecha y, a continuación, cambia Deployla configuración.



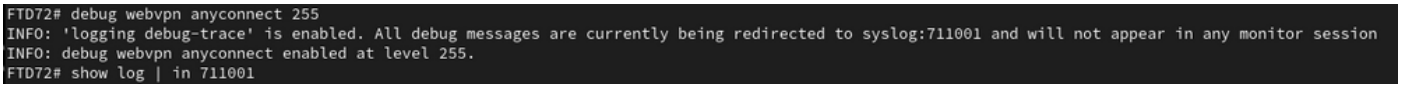
Defensa contra amenazas de firewall

Navegue hasta la CLI de FTD y ejecute el comandoshow logging setting. La configuración refleja los cambios realizados en el CSP. Asegúrese de que el registro de seguimiento de depuración esté habilitado y de que el registro del búfer coincida con las clases y el nivel de registro especificados.



Mostrar la configuración de registro en la CLI de FTD.

Por último, aplique una depuración para asegurarse de que los registros se redirijan a syslog:711001. En este ejemplo, `debug webvpn anyconnect 255` se aplica. Esto activa un aviso de seguimiento de depuración de registro, lo que permite al administrador saber que estas depuraciones se redirigen. Para ver estos debugs, ejecute el comando `show log | in 711001`. Este ID de syslog ahora solo contiene los debugs relevantes de VPN según los aplica el administrador. Los registros existentes se pueden borrar con un buffer de registro despejado.



Muestra que todas las depuraciones de VPN se están redirigiendo a syslog 711001.

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).