Configuración de acciones de reglas adicionales de Snort 3 en FMC

Contenido

Introducción

Este documento describe la compatibilidad de Firepower Management Center (FMC) con la función de acciones de regla adicionales de Snort 3 añadida en la versión 7.1.

Antecedentes

Aunque Firepower Threat Defence (FTD) admite siete acciones de regla de política de intrusiones Alert/Disable/Block/Reject/Rewrite/Pass/Drop en la versión 7.0, FMC solo admitió tres acciones de regla de Snort 3: "Alert", "Disable" y "Block".

Desde Firepower 7.1.0, FMC admite la configuración de nuevas acciones de regla.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:
· Conocimiento de código abierto Snort
· Firepower Management Center (FMC) 7.1.0+
· Firepower Threat Defense (FTD) 7.0.0+

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.
· Este documento se aplica a todas las plataformas Firepower que ejecutan Snort 3
· Cisco Firepower Threat Defense Virtual (FTD), que ejecuta la versión de software 7.4.2
· Firepower Management Center Virtual (FMC), que ejecuta la versión de software 7.4.2

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.

Detalles de la función

Las nuevas acciones de regla de Snort 3 añadidas y sus descripciones son las siguientes:

Pass: No se genera ningún evento, lo que permite que el paquete pase sin que ninguna regla de Snort posterior realice una evaluación adicional.

Abandonar: Genera eventos, descarta paquetes coincidentes y no bloquea más tráfico en esta conexión.

Rechazar: Genera eventos, descarta paquetes coincidentes, bloquea más tráfico en esta conexión y envía el reinicio TCP o el puerto ICMP inalcanzable a los hosts de origen y destino.

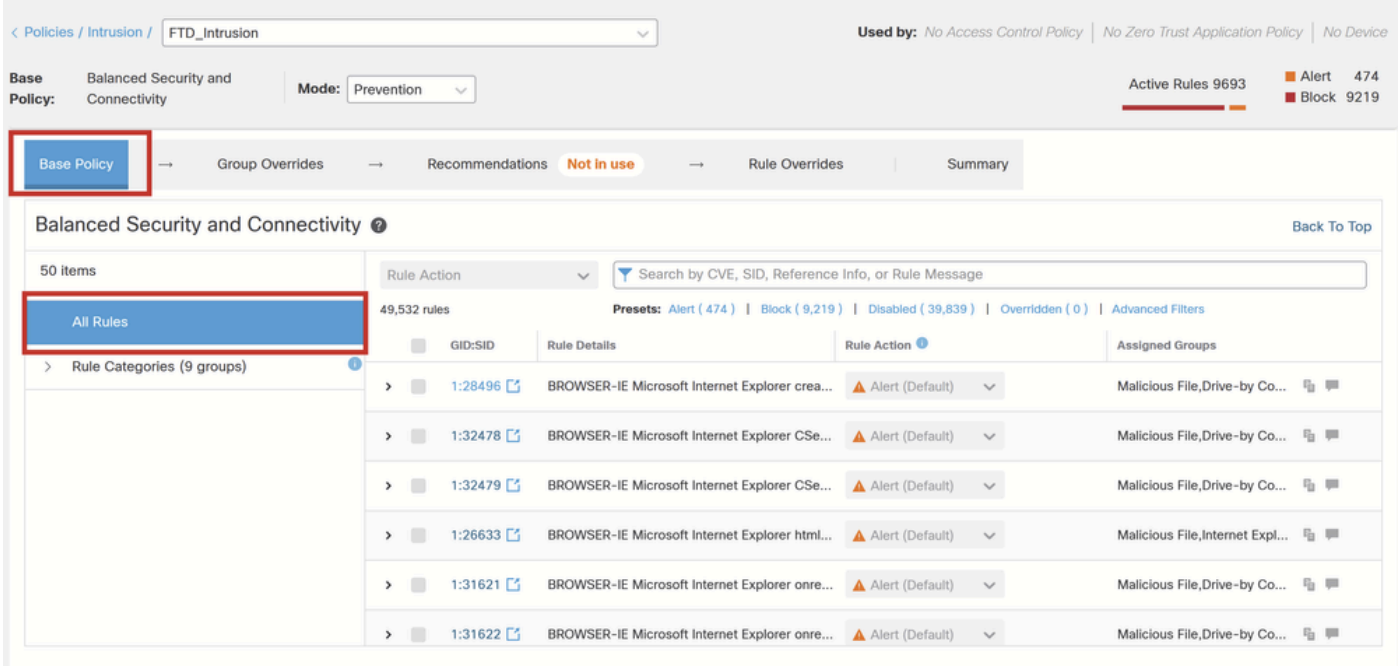
Reescritura: Genera eventos y sobrescribe el contenido del paquete basándose en la opción de reemplazo de la regla.

Tutorial sobre FMC

Para ver las reglas de Snort 3 en una política de intrusiones, vaya aFMC Policies > Access Control > Intrusion,continuación y haga clic en la opción Snort 3 Version en la esquina superior derecha de la política, como se muestra en la imagen:

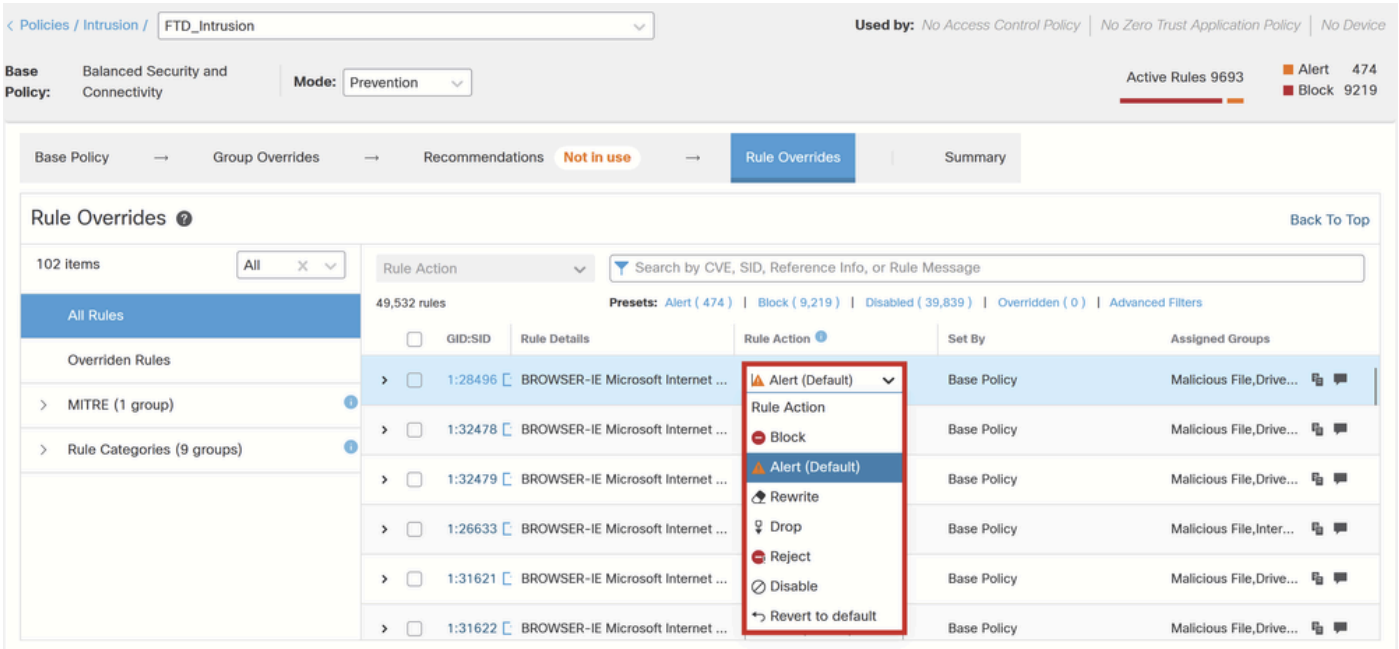
Versión de Snort 3

Haga clic en Base Policy > All Rules, puede ver las acciones predeterminadas de todas las reglas de Snort 3 definidas por el sistema.

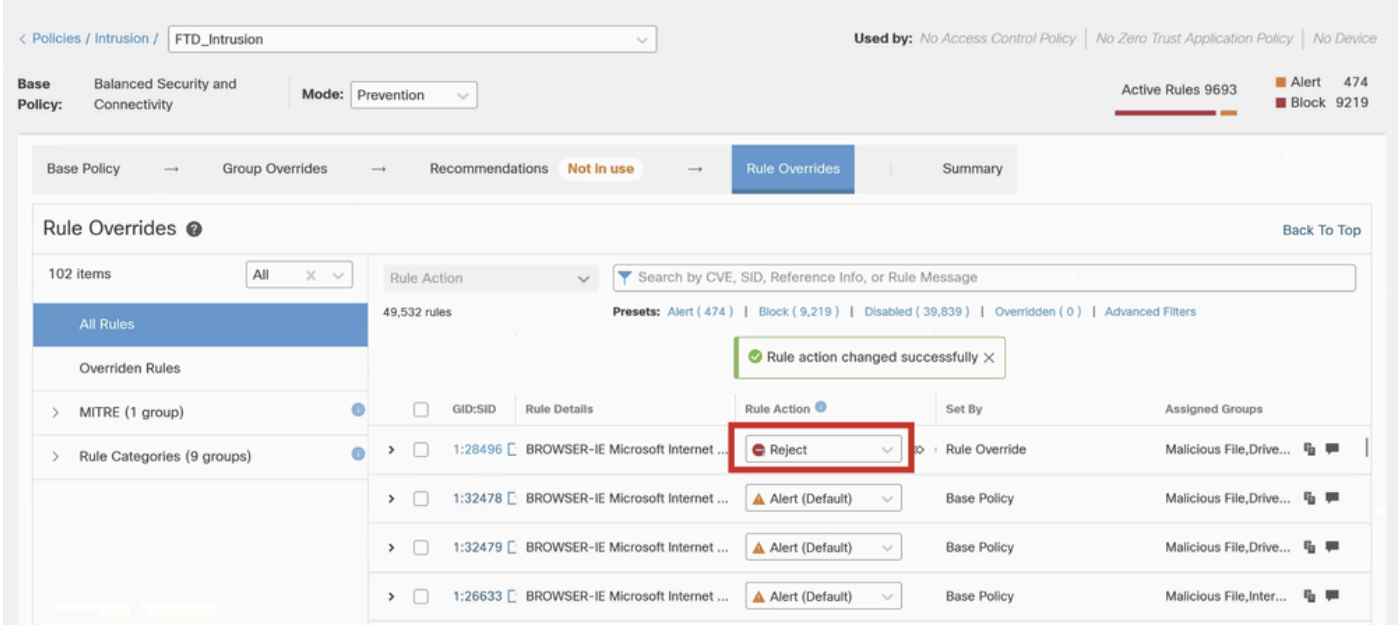


Política básica

Para cambiar la acción de regla a cualquiera de estas nuevas acciones de regla, navegue hasta Anulaciones de regla > Todas las reglas y seleccione la acción de regla del menú desplegable para la regla seleccionada.

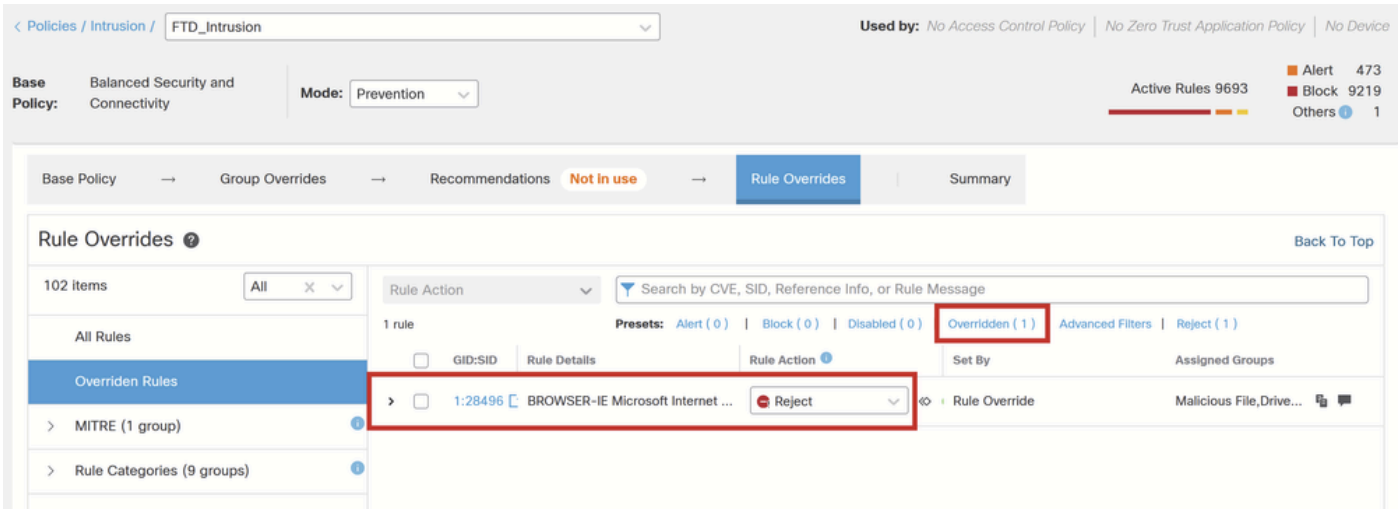


Acciones de regla adicionales



Cambio de la acción de regla

Las reglas anuladas se pueden encontrar en Rule Overrides > Overridden Rules.



Reglas anuladas

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).