Configuración de reglas de Snort locales personalizadas en Snort2 en FTD

Contenido

- Introducción
- Prerequisites
  - Requirements
  - Componentes Utilizados
- Antecedentes
- Configurar
  - Diagrama de la red
  - Configuración
    - Paso 1. Confirmar versión de Snort
    - Paso 2. Crear una regla de Snort local personalizada en Snort 2
    - Paso 3. Confirmar regla de Snort local personalizada
    - Paso 4. Cambiar acción de regla
    - Paso 5. Asociar política de intrusión a la regla de política de control de acceso (ACP)
    - Paso 6. Implementar cambios
- Verificación
  - La regla de Snort local personalizada no se activa
    - Paso 1. Establecer el contenido del archivo en el servidor HTTP
    - Paso 2. Solicitud HTTP inicial
  - Se Activa la Regla de Snort Local Personalizada
    - Paso 1. Establecer el contenido del archivo en el servidor HTTP
    - Paso 2. Solicitud HTTP inicial
    - Paso 3. Evento ConfirmIntrusion
- Troubleshoot

Introducción

Este documento describe el procedimiento para configurar las reglas de Snort local personalizado en Snort2 en Firewall Threat Defence (FTD).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Firepower Management Center (FMC)
- Firewall Threat Defence (FTD)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

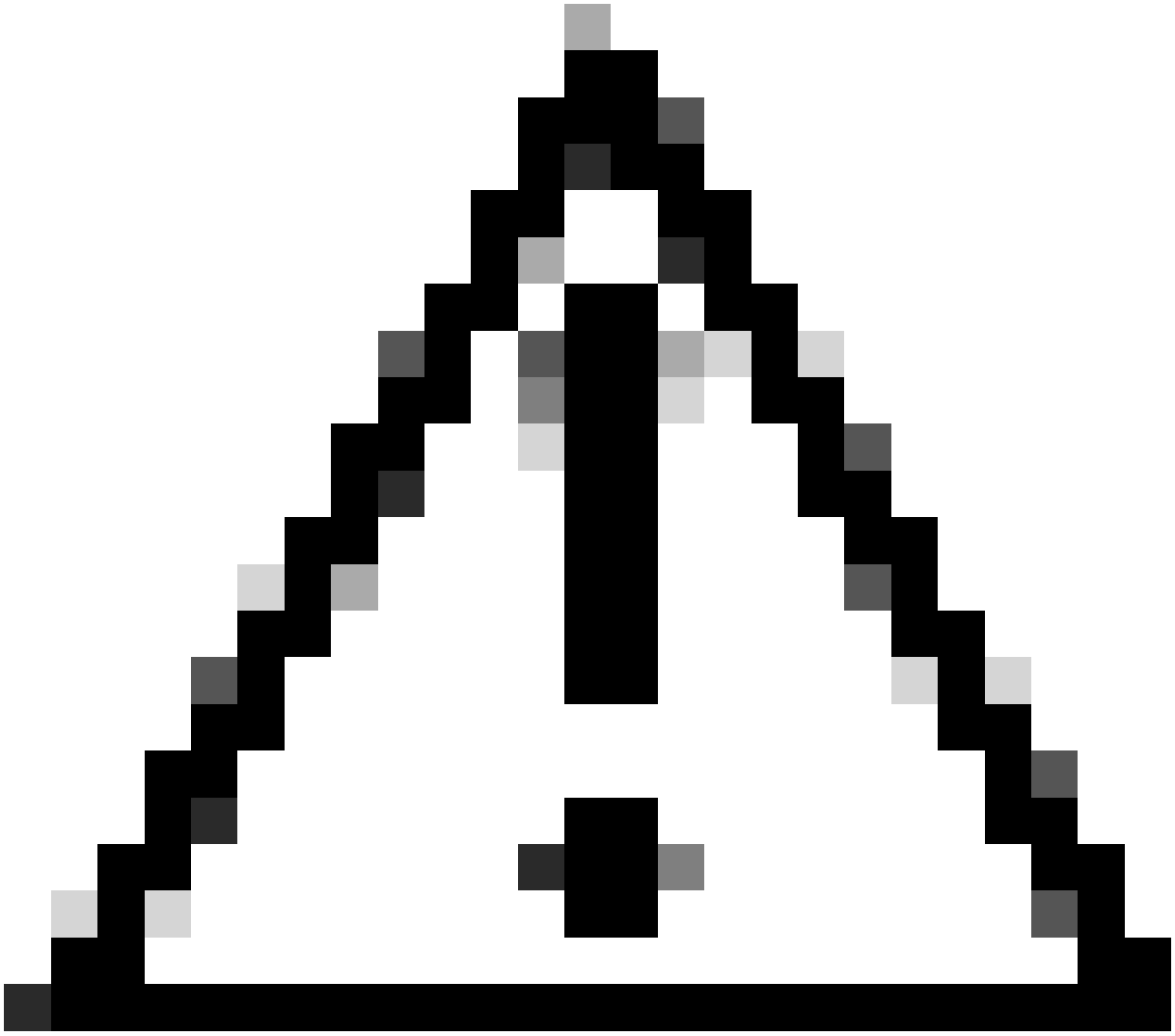
- Cisco Firepower Management Center para VMWare 7.4.1
- Cisco Firepower 2120 7.4.1

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.

Antecedentes

La regla de Snort local personalizada hace referencia a una regla definida por el usuario que se puede crear e implementar dentro del sistema de detección y prevención de intrusiones de Snort integrado en el FTD. Cuando se crea una regla Snort local personalizada en Cisco FTD, básicamente se define un nuevo patrón o conjunto de condiciones que el motor Snort puede observar. Si el tráfico de red coincide con las condiciones especificadas en la regla personalizada, Snort puede realizar la acción definida en la regla, como generar una alerta o descartar el paquete. Los administradores utilizan reglas Snort locales personalizadas para hacer frente a amenazas específicas que no están cubiertas por los conjuntos de reglas generales.

En este documento, se explica cómo configurar y verificar una regla de Snort local personalizada diseñada para detectar y descartar paquetes de respuesta HTTP que contengan una cadena específica (nombre de usuario).

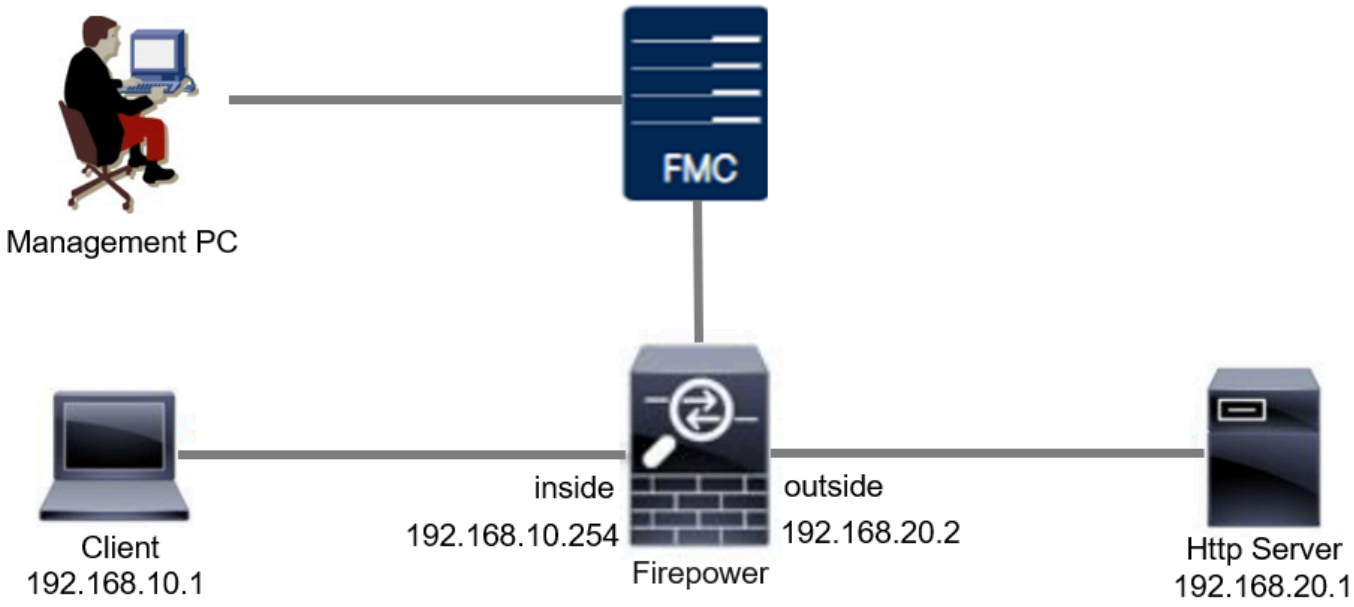


Precaución: la creación de reglas de Snort locales personalizadas y la prestación de asistencia para ellas quedan fuera de la cobertura de asistencia del TAC. Por lo tanto, este documento sólo se puede utilizar como referencia y solicite que cree y administre estas reglas personalizadas según su propio criterio y responsabilidad.

Configurar

Diagrama de la red

Este documento presenta la configuración y verificación de la regla de Snort local personalizado en Snort2 en este diagrama.

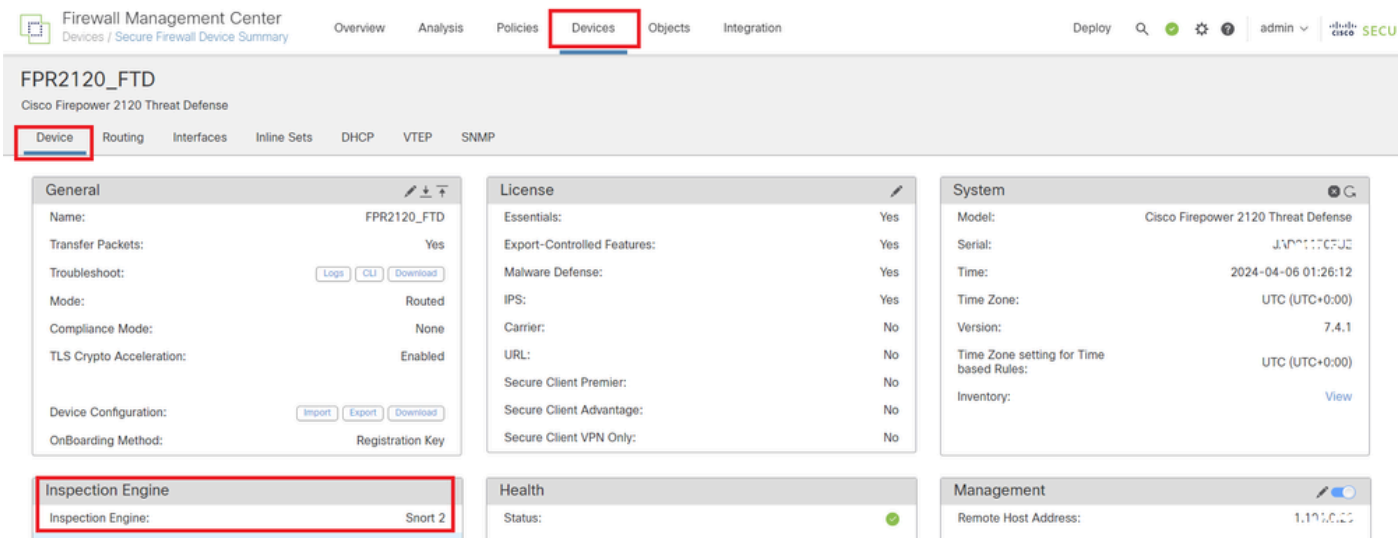


Configuración

Esta es la configuración de la regla de snort local personalizada para detectar y descartar paquetes de respuesta HTTP que contienen una cadena específica (nombre de usuario).

Paso 1. Confirmar versión de Snort

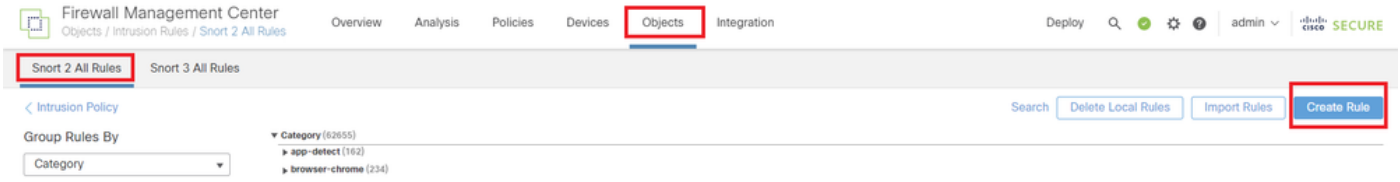
Vaya a Dispositivos > Administración de dispositivos en FMC, haga clic en la pestaña Dispositivo. Confirmación de que la versión del snort es Snort2.



Versión de Snort

Paso 2. Crear una regla de Snort local personalizada en Snort 2

Navegue hasta Objetos > Reglas de intrusión > Snort 2 All Rules en FMC, haga clic en el botón Create Rule.

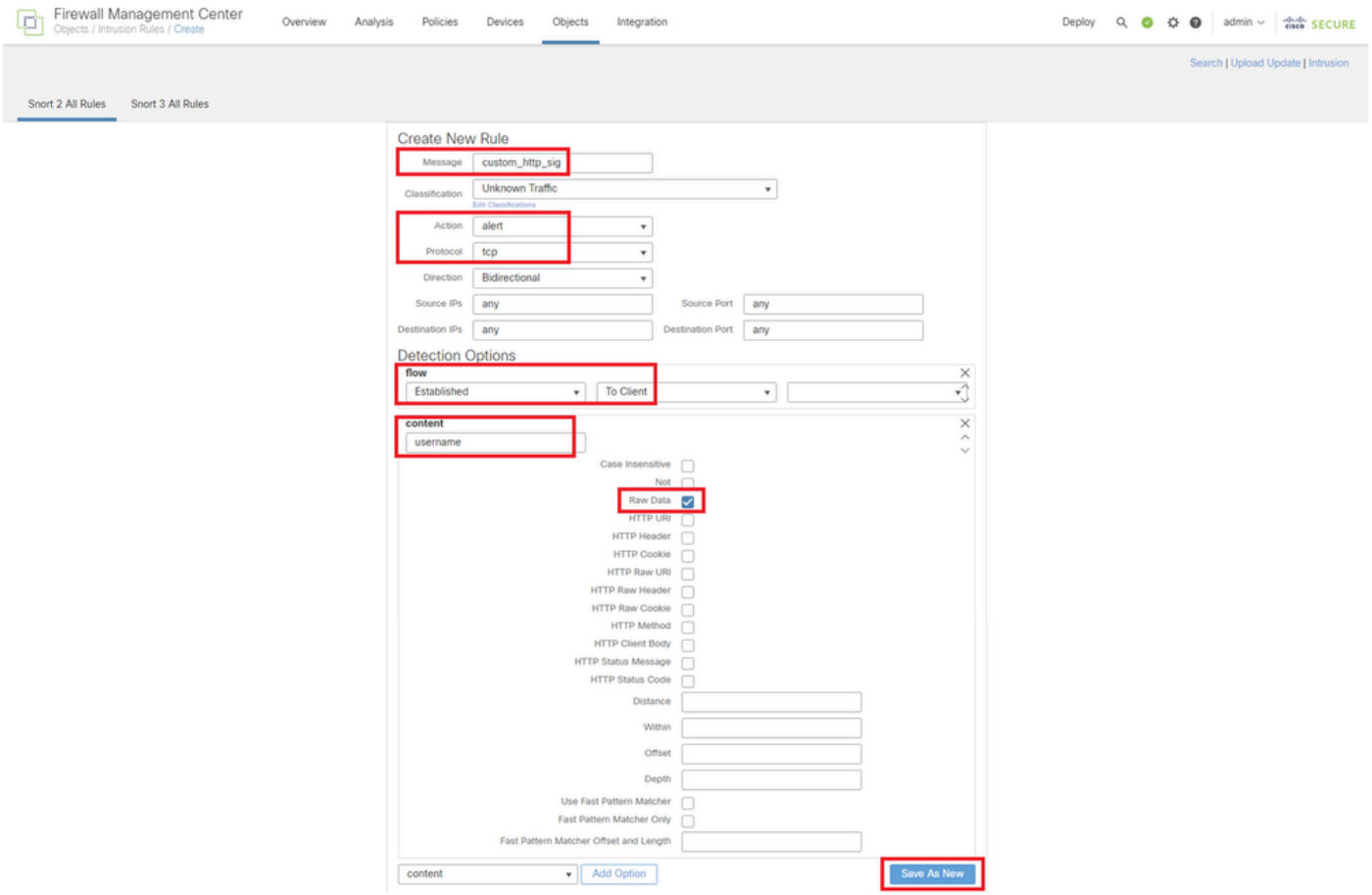


Crear regla personalizada

Introduzca la información necesaria para la regla de snort local personalizado.

- Intrusión: custom_http_sig
- Acción: alerta
- Protocolo: tcp
- flujo: establecido, al cliente

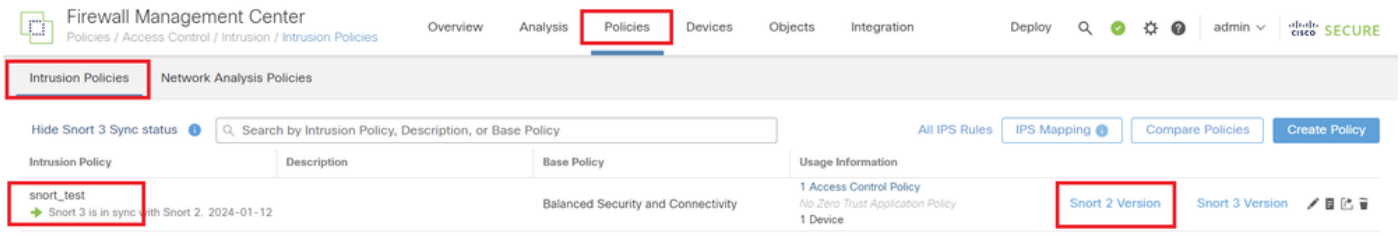
- content: username (Raw Data)



Introduzca la información necesaria para la regla

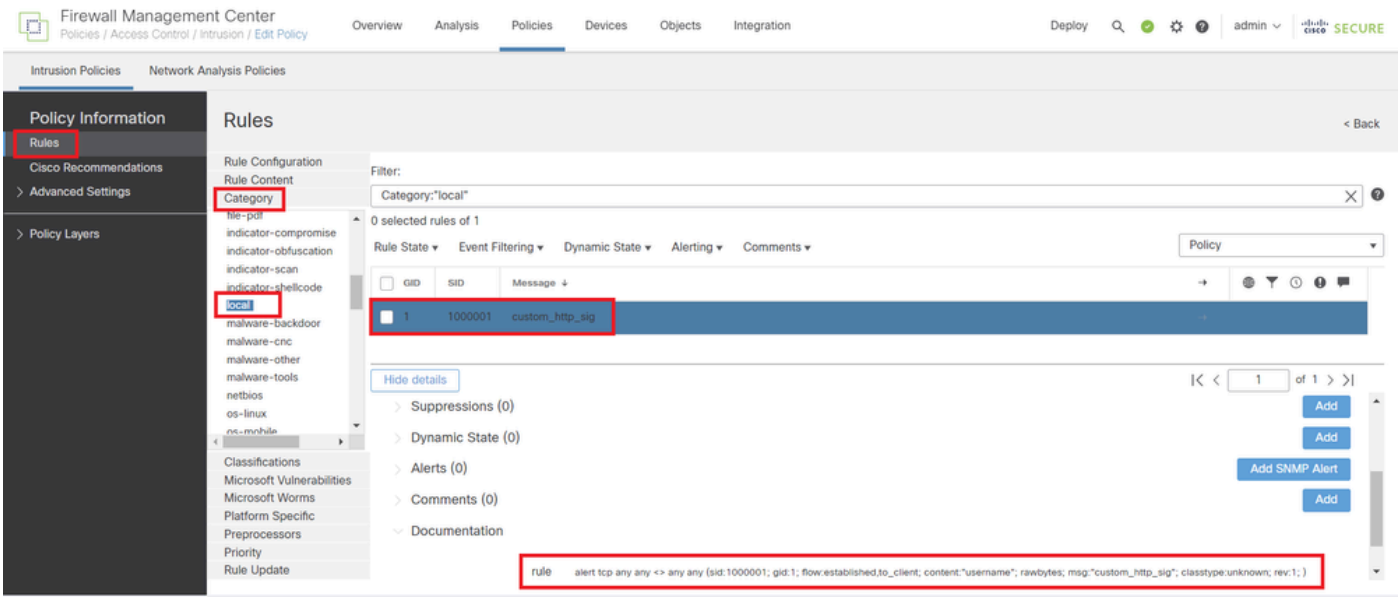
Paso 3. Confirmar regla de Snort local personalizada

Navegue hasta Políticas > Políticas de intrusión en FMC, haga clic en el botón Versión Snort 2.



Confirmar regla personalizada

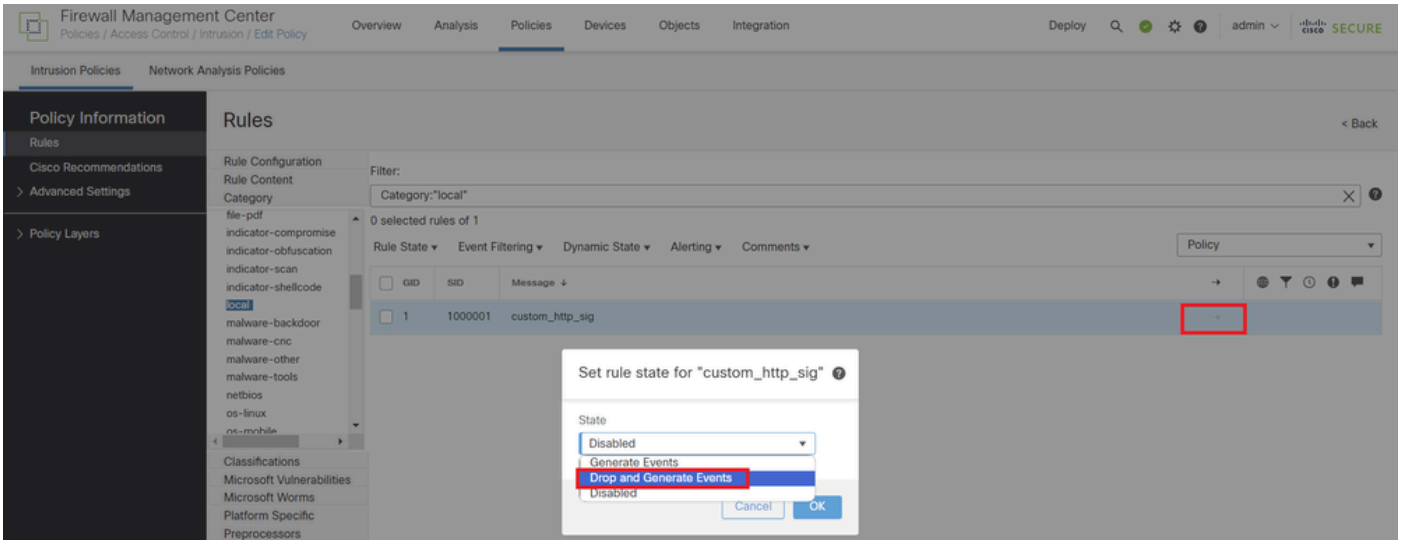
Navegue hasta Reglas > Categoría > local en FMC, confirme los detalles de la Regla de Snort Local Personalizada.



Detalle de la regla personalizada

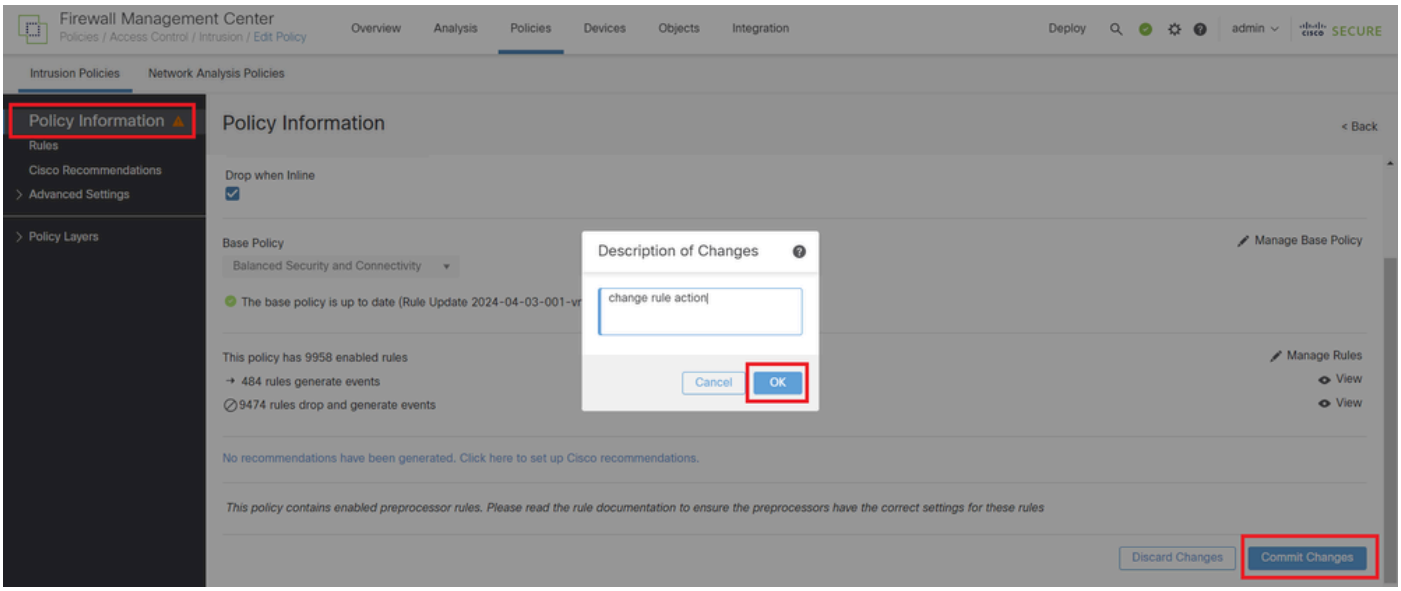
Paso 4. Cambiar acción de regla

Haga clic en el botón State, establezca el State en Drop and Generate Events y haga clic en el botón OK.



Cambiar la acción de regla

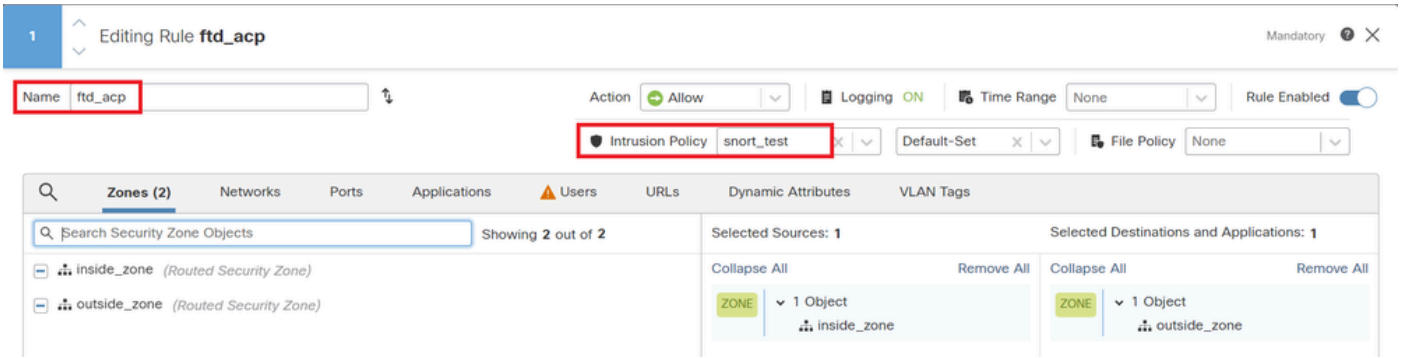
Haga clic en el botón Información de política, haga clic en el botón Registrar cambios para guardar los cambios.



Registrar cambios

Paso 5. Asociar política de intrusiones con regla de política de control de acceso (ACP)

Vaya a Políticas > Control de Acceso en FMC, asocie la Política de Intrusión con ACP.



Asociar con Regla ACP

Paso 6. Implementar cambios

Implemente los cambios en FTD.

Implementar cambios

Verificación

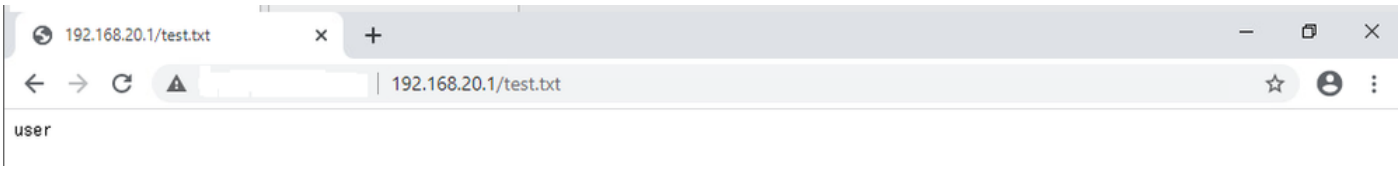
La regla de Snort local personalizada no se activa

Paso 1. Establecer el contenido del archivo en el servidor HTTP

Establezca el contenido del archivo test.txt en el lado del servidor HTTP como usuario.

Paso 2. Solicitud HTTP inicial

Acceda al servidor HTTP (192.168.20.1/test.txt) desde el explorador del cliente (192.168.10.1) y confirme que la comunicación HTTP está permitida.



Solicitud HTTP inicial

Se Activa la Regla de Snort Local Personalizada

Paso 1. Establecer el contenido del archivo en el servidor HTTP

Establezca el contenido del archivo test.txt en el lado del servidor HTTP en username.

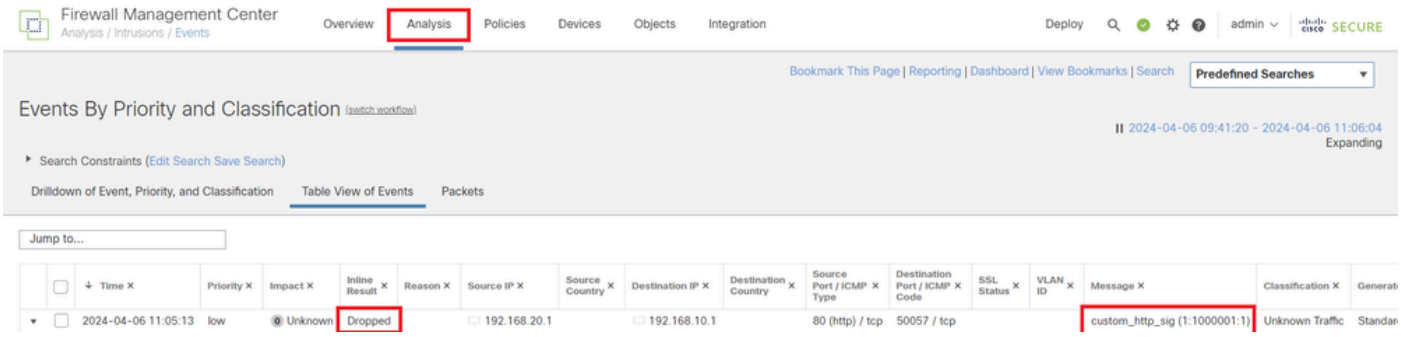
Paso 2. Solicitud HTTP inicial

Acceda al servidor HTTP (192.168.20.1/test.txt) desde el explorador del cliente (192.168.10.1) y confirme que la comunicación HTTP está bloqueada.

Solicitud HTTP inicial

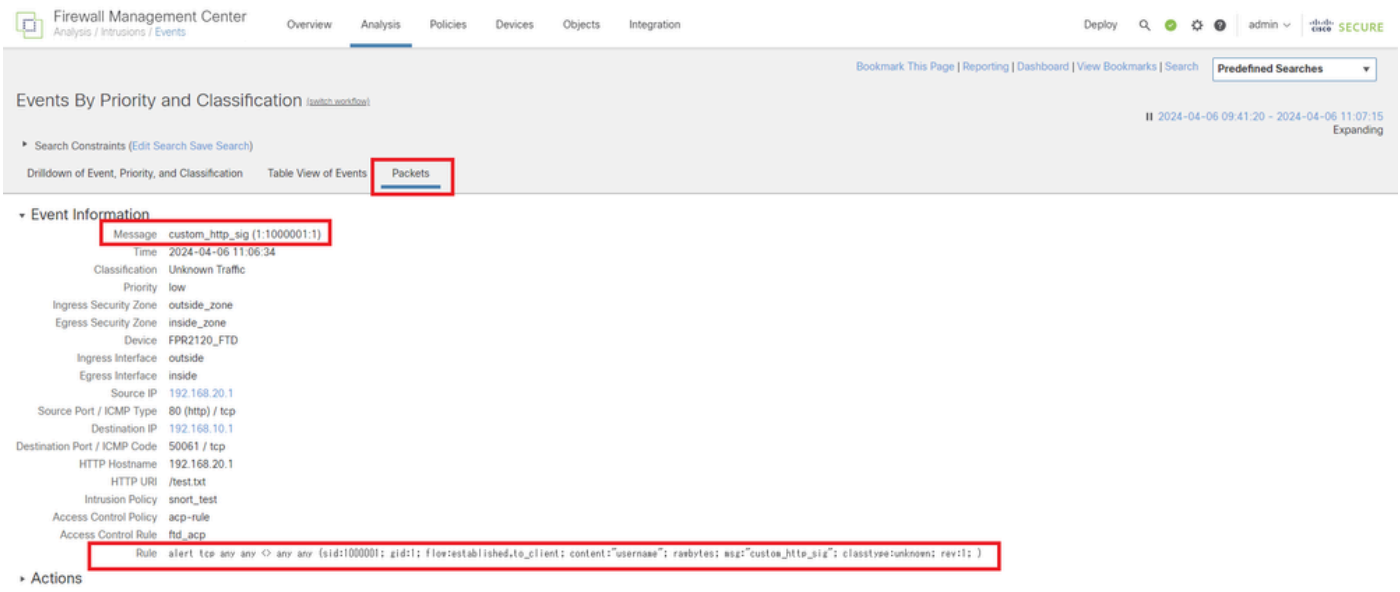
Paso 3. Confirmar evento de intrusión

Navegue hasta Análisis > Intrusiones > Eventos en FMC, confirme que el Evento de Intrusión es generado por la Regla de Snort Local Personalizada.



Evento de intrusión

Haga clic en la pestaña Paquetes, confirme los detalles del evento de intrusión.



Detalle del evento de intrusión

Troubleshoot

Ejecute system support trace el comando para confirmar el comportamiento en FTD. En este ejemplo, la regla IPS bloquea el tráfico HTTP (gid 1, sid 1000001).

```
<#root>

>

system support trace


Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.1
Please specify a client port:
Please specify a server IP address: 192.168.20.1
Please specify a server port:

192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 Firewall: allow rule, '
```

ftd_acp

', allow
192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0

IPS Event

:

gid 1

,

sid 1000001

, drop

192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 Snort id 3, NAP id 2, IPS id 1, Verdict BLOCKFLOW
192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 ===>

Blocked by IPS

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).