

# Configuración de reglas de Snort locales personalizadas en Snort3 en FTD

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Diagrama de la red](#)

[Configuración](#)

[Método 1. Importación de Snort 2 a Snort 3](#)

[Paso 1. Confirmar versión de Snort](#)

[Paso 2. Creación o edición de una regla de Snort local personalizada en Snort 2](#)

[Paso 3. Importar reglas de Snort locales personalizadas de Snort 2 a Snort 3](#)

[Paso 4. Cambiar acción de regla](#)

[Paso 5. Confirmar regla de Snort local personalizada importada](#)

[Paso 6. Asociar política de intrusiones con regla de política de control de acceso \(ACP\)](#)

[Paso 7. Implementar cambios](#)

[Método 2. Cargar un archivo local](#)

[Paso 1. Confirmar versión de Snort](#)

[Paso 2. Crear una regla de Snort local personalizada](#)

[Paso 3. Cargar la regla de snort local personalizada](#)

[Paso 4. Cambiar acción de regla](#)

[Paso 5. Confirmar la regla de Snort local personalizada cargada](#)

[Paso 6. Asociar política de intrusiones con regla de política de control de acceso \(ACP\)](#)

[Paso 7. Implementar cambios](#)

[Verificación](#)

[Paso 1. Establecer el contenido del archivo en el servidor HTTP](#)

[Paso 2. Solicitud HTTP inicial](#)

[Paso 3. Confirmar evento de intrusión](#)

[Preguntas frecuentes](#)

[Troubleshoot](#)

[Referencia](#)

---

## Introducción

Este documento describe el procedimiento para configurar las reglas de Snort local personalizado en Snort3 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.

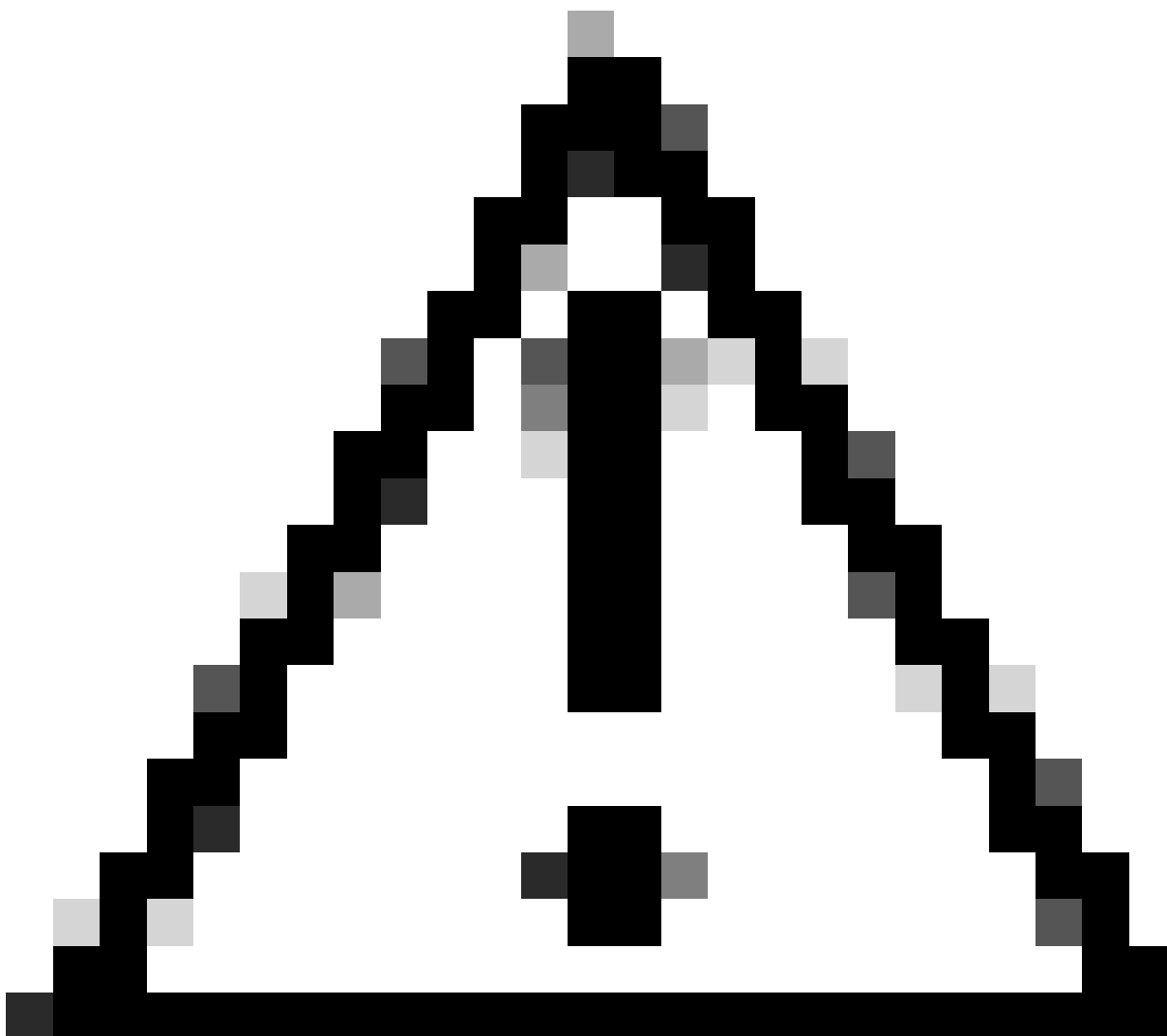
- Cisco Firepower Management Center para VMWare 7.4.1
- Cisco Firepower 2120 7.4.1

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 compatibilidad con Snort 3 en la defensa contra amenazas con el centro de gestión comienza en la versión 7.0. Para dispositivos nuevos y recreados de la versión 7.0 y posteriores, Snort 3 es el motor de inspección predeterminado.

Este documento proporciona un ejemplo de cómo personalizar las reglas de Snort para Snort 3, así como un ejemplo práctico de verificación. Específicamente, se le presenta cómo configurar y verificar una política de intrusión con una regla Snort personalizada para descartar paquetes HTTP que contienen una cadena determinada (nombre de usuario).



Precaución: la creación de reglas de Snort locales personalizadas y la prestación de soporte para ellas quedan fuera de la cobertura de soporte 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.

---

## Diagrama de la red

Este documento presenta la configuración y verificación de la regla de Snort local personalizado en Snort3 en este diagrama.

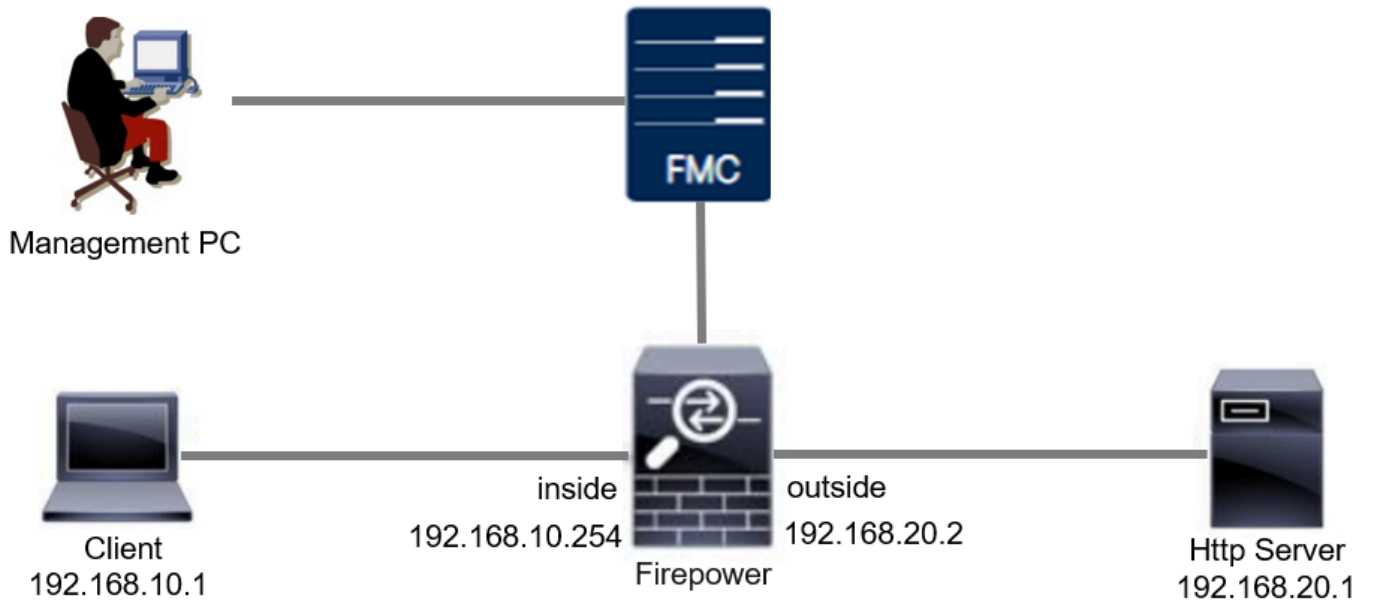


Diagrama de la red

## 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).



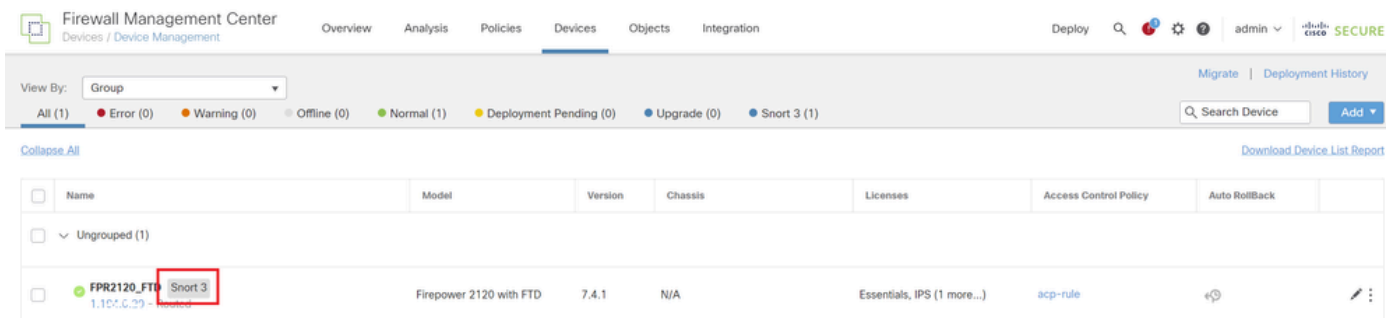
Nota: A partir de ahora, no es posible agregar reglas de Snort local personalizadas desde la página Todas las reglas de Snort 3 en la GUI de FMC. Debe utilizar el método introducido en este documento.

---

## Método 1. Importación de Snort 2 a Snort 3

### Paso 1. Confirmar versión de Snort

Navegue hasta Dispositivos>Administración de dispositivos en FMC, haga clic en FichaDispositivo. Confirme que la versión del snort es Snort3.



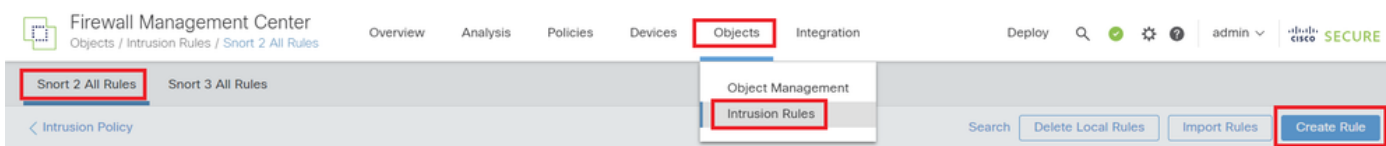
Versión de Snort

## Paso 2. Creación o edición de una regla de Snort local personalizada en Snort 2

Vaya a Objetos > Reglas de intrusión > Snort 2 All Rules on FMC. Haga clic en el botón Create Rule (Crear regla) para agregar una regla de snort local personalizada, o vaya a Objects > Intrusion Rules > Snort 2 All Rules > Local Rules on FMC, haga clic en el botón Edit para editar una regla de snort local personalizada existente.

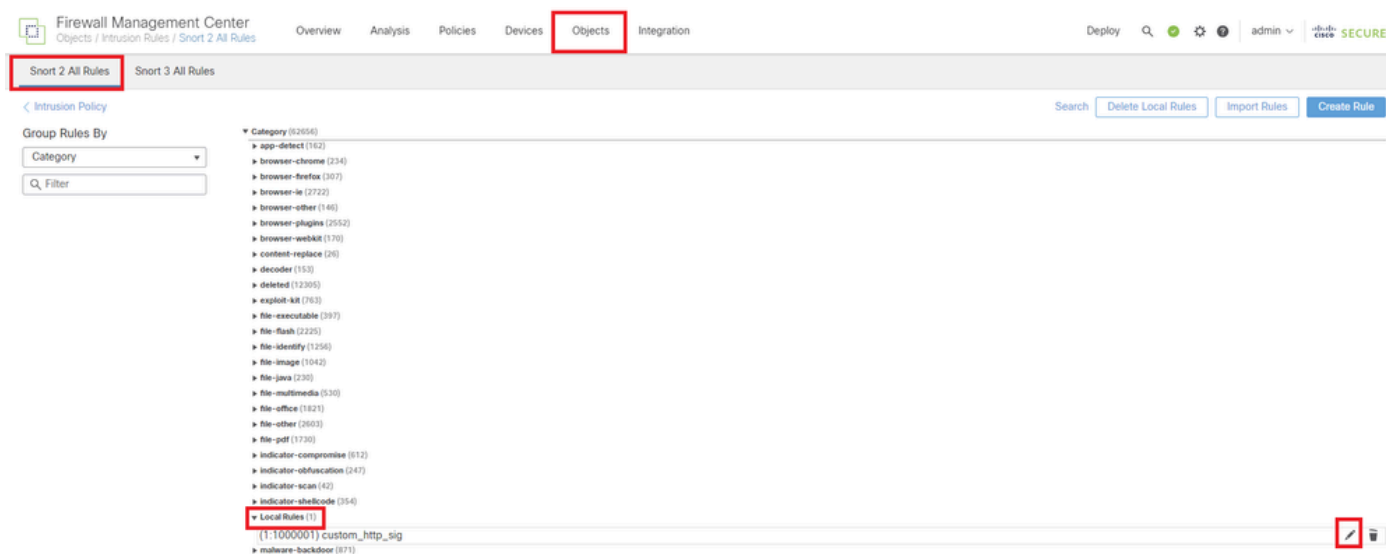
Para obtener instrucciones sobre cómo crear reglas de Snort locales personalizadas en Snort 2, consulte [Configuración de reglas de Snort locales personalizadas en Snort2 en FTD](#).

Agregue una nueva regla de snort local personalizada como se muestra en la imagen.



Agregar una nueva regla personalizada

Edite una regla existente de snort local personalizado como se muestra en la imagen. En este ejemplo, edita una regla personalizada existente.



Editar una regla personalizada existente

Introduzca la información de firma para detectar paquetes HTTP que contengan una cadena

específica (nombre de usuario).

- Mensaje: custom\_http\_sig
- Acción: alerta
- Protocolo: tcp
- flujo: establecido, al cliente
- content: username (Raw Data)

Firewall Management Center  
Objects / Intrusion Rules / Create

Overview Analysis Policies Devices **Objects** Integration

Deploy Search Upload Update Intrusion

Snort 2 All Rules Snort 3 All Rules

Edit Rule 1:1000000:3 (Rule Comment)

Message: custom\_http\_sig

Classification: Unknown Traffic

Action: alert

Protocol: tcp

Direction: Bidirectional

Source IPs: any Source Port: any

Destination IPs: any Destination Port: any

Detection Options

flow: Established To Client

content: username

Raw Data

Save Save As New

Introduzca la información necesaria para la regla

### Paso 3. Importar reglas de Snort locales personalizadas de Snort 2 a Snort 3

Navigate hasta Objetos > Reglas de intrusión > Reglas de Snort 3 > Todas las reglas en FMC, haga clic en Convertir reglas de Snort 2 e Importar de la lista desplegable Tareas.

Firewall Management Center  
Objects / Intrusion Rules / Snort 3 All Rules

Overview Analysis Policies Devices **Objects** Integration

Deploy Search Upload Update Intrusion

Snort 2 All Rules Snort 3 All Rules

Intrusion Policy

All Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Actions Search by CVE, SID, Reference Info, or Rule Message Tasks

50,094 rules

<input type="checkbox"/>	OID:SID	Info	Rule Action	Assigned Groups
<input type="checkbox"/>	148:2	(cip) CIP data is non-conforming to ODVA standard	Disable (Default)	Builtins
<input type="checkbox"/>	133:3	(dce_smb) SMB - bad SMB message type	Disable (Default)	Builtins

Upload Short 3 rules

Convert Snort 2 rules and Import

Convert Snort 2 rules and download

Add Rule Groups

Importar regla personalizada a Snort 3

Verifique el mensaje de advertencia y haga clic en OK.

## Convert Snort 2 rules and import



The Snort 2 local rules are not auto-converted to the Snort 3 version, as Snort 3 rules are written differently compared to Snort 2 rules. This action will convert all Snort 2 local rules to Snort 3 rules. All the enabled rules per the Snort 2 version of the policy will be added into different groups and enabled in the corresponding Snort 3 version of the policy.

Cancel

OK

Mensaje de advertencia

Navegue hasta Objetos > Reglas de Intrusión > Reglas de Snort 3 All en FMC, haga clic en Todas las Reglas de Snort 2 Convertidas Globales para confirmar la Regla de Snort Local Personalizada importada.

The screenshot shows the Firewall Management Center interface. The breadcrumb path is 'Objects / Intrusion Rules / Snort 3 All Rules'. The 'Objects' tab is selected. The 'Snort 3 All Rules' section is active. The 'Local Rules / All Snort 2 Converted Global' group is selected, showing a description: 'Group created for custom rules enabled in snort 2 version'. A search bar is present with the text 'Search by CVE, SID, Reference Info, or Rule Message'. A notification box states 'The custom rules were successfully imported X'. Below the notification is a table with the following data:

<input type="checkbox"/>	GID:SID	Info	Rule Action	Assigned Groups	Alert Configuration
<input type="checkbox"/>	2000:1000000	custom_http_sig	Disable (Default)	All Snort 2 Converted Glo...	None

Confirmar regla personalizada importada

### Paso 4. Cambiar acción de regla

Haga clic en Por política de intrusión según la acción de regla de la regla personalizada de destino.



**All Rules**

- Local Rules (1 group)
- All Snort 2 Converted Global
- MITRE (1 group)
- Rule Categories (9 groups)

**Local Rules / All Snort 2 Converted Global**

**Description** Group created for custom rules enabled in snort 2 version

Rule Actions  Tasks

1 rule

✔ The custom rules were successfully imported ✕

	GID:SID	Info	Rule Action	Assigned Groups	Alert Configuration
>	2000:1000000	custom_http_sig	<div style="border: 1px solid #ccc; padding: 2px;"> <span>⊗ Disable (Default) (Overridden)</span>  <span>🛑 Block</span>  <span>⚠ Alert</span>  <span>🔧 Rewrite</span>  <span>⬇ Drop</span>  <span>🟢 Pass</span>  <span>🚫 Reject</span>  <span>⊗ Disable (Default)</span>  <span>↩ Revert to default</span>  <span style="border: 2px solid red; padding: 2px;">Per Intrusion Policy</span> </div>	All Snort 2 Converted Glo...	None

Cambiar acción de regla

En la pantalla Edit Rule Action, ingrese la información para Policy y Rule Action.

- Política: snort\_test
- Acción de regla: BLOQUEAR



Nota: Las acciones de regla son:

**Bloquear:** genera eventos, bloquea el paquete coincidente actual y todos los paquetes subsiguientes de esta conexión.

**Alerta:** genera solo eventos para paquetes coincidentes y no descarta paquetes ni conexiones.

**Rewrite:** genera el evento y sobrescribe el contenido del paquete basándose en la opción de reemplazo de la regla.

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

**Drop:** 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 de TCP si es un protocolo TCP a los hosts de origen y

---

destino.

Desactivar: no coincide con el tráfico de esta regla. No se genera ningún evento.

Predeterminado: vuelve a la acción predeterminada del sistema.

Edit Rule Action

2000:100... | custom\_http\_sig

All Policies  Per Intrusion Policy

Policy: snort\_test Rule Action: BLOCK

Add Another

Comments (optional): Provide a reason to change if applicable

Cancel Save

Editar acción de regla

### Paso 5. Confirmar regla de Snort local personalizada importada

Navegue hasta Políticas > Políticas de intrusión en FMC, haga clic en Snort 3 Version correspondiente a la política de intrusión de destino en la fila.

Firewall Management Center

Policies / Access Control / Intrusion / Intrusion Policies

Overview Analysis Policies Devices Objects Integration Deploy Search admin | Cisco SECURE

Intrusion Policies Network Analysis Policies

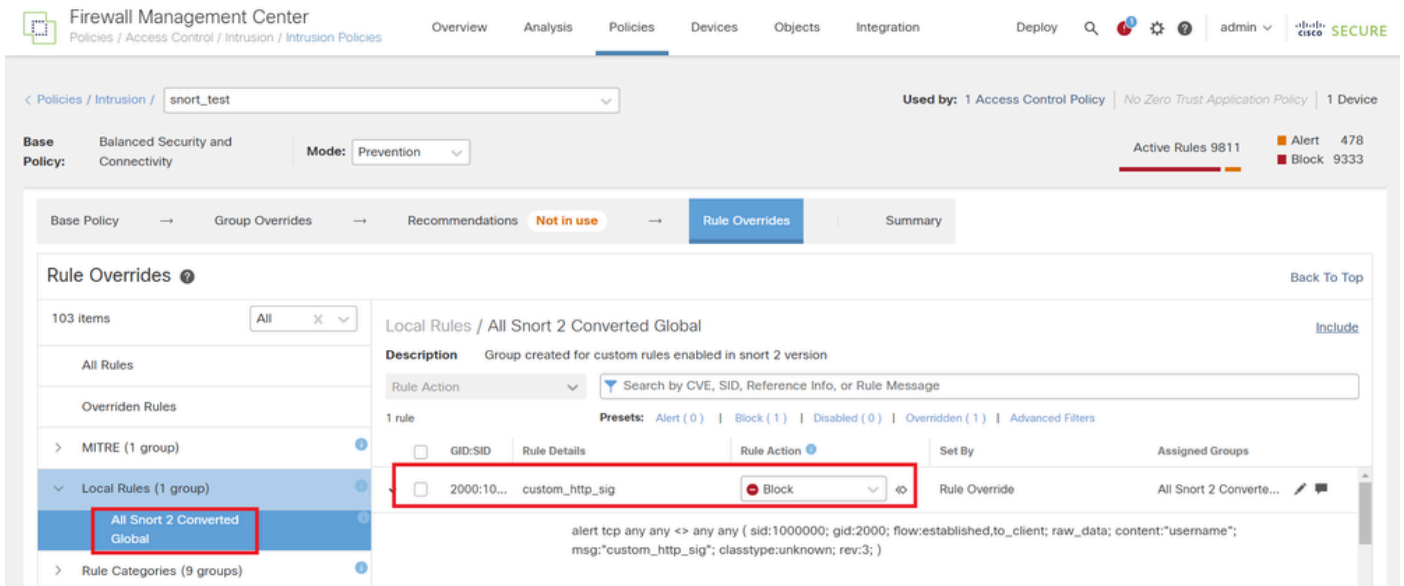
Hide Snort 3 Sync status Search by Intrusion Policy, Description, or Base Policy All IPS Rules IPS Mapping Compare Policies Create Policy

Intrusion Policy	Description	Base Policy	Usage Information
snort_test	Snort 3 is in sync with Snort 2. 2024-01-12	Balanced Security and Connectivity	1 Access Control Policy No Zero Trust Application Policy 1 Device

Snort 2 Version Snort 3 Version

Confirmar regla personalizada importada

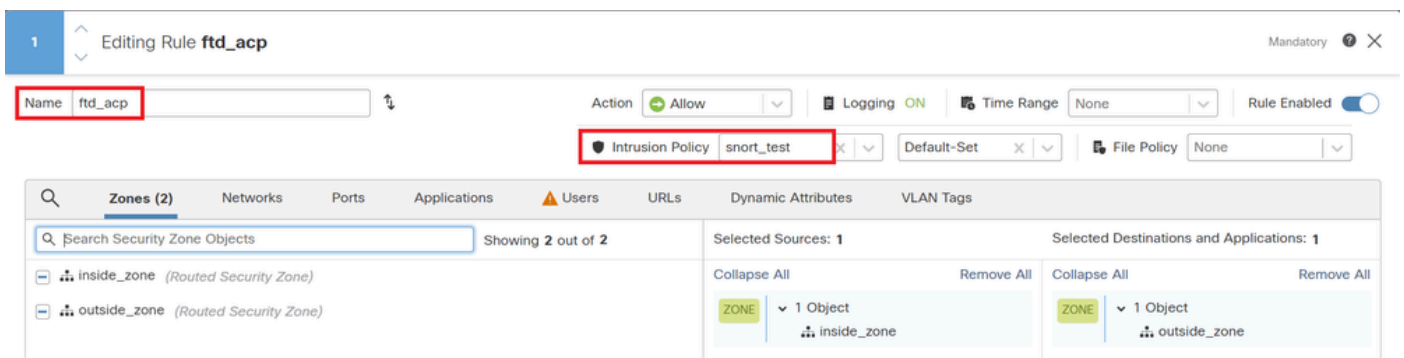
Haga clic en Local Rules > All Snort 2 Converted Global para comprobar los detalles de la Custom Local Snort Rule.



Confirmar regla personalizada importada

## Paso 6. Asociar política de intrusiones con regla de política de control de acceso (ACP)

Navegue hasta Políticas>Control de Acceso en FMC, asocie la Política de Intrusión con ACP.



Asociar con Regla ACP

## Paso 7. Implementar cambios

Implemente los cambios en FTD.



Implementar cambios

## Método 2. Cargar un archivo local

### Paso 1. Confirmar versión de Snort

Igual que en el paso 1 del método 1.

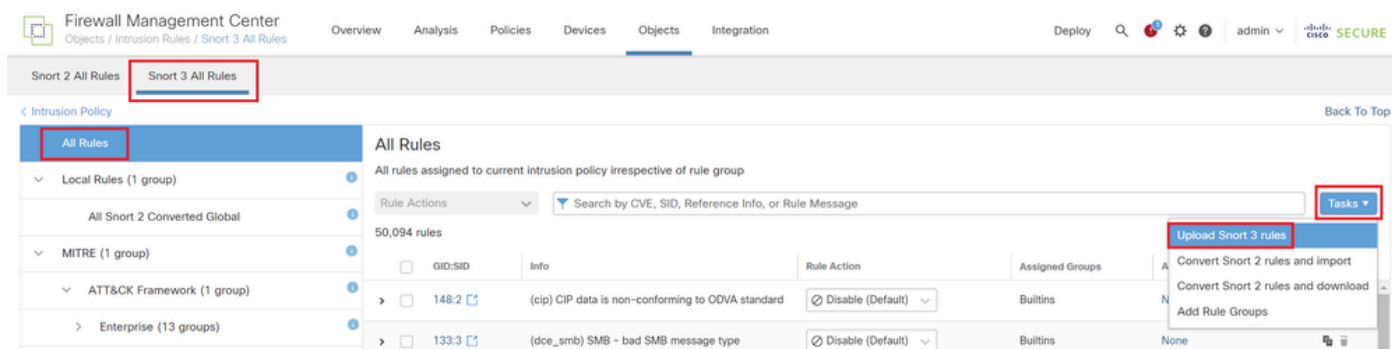
### Paso 2. Crear una regla de Snort local personalizada

Cree manualmente una regla de Snort local personalizada y guárdela en un archivo local denominado custom-rules.txt.

```
alert tcp any any <> any any ( sid:1000000; flow:established,to_client; raw_data; content:"username"; m
```

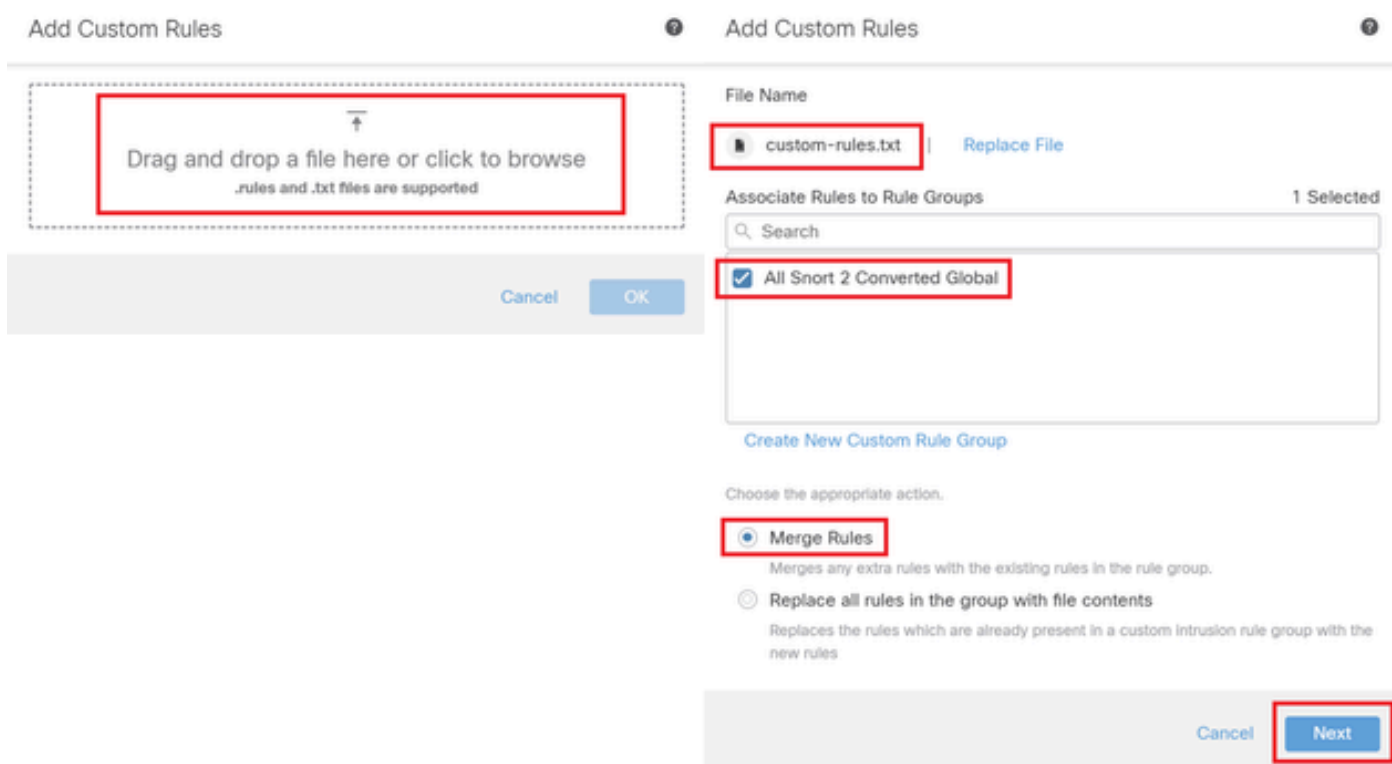
### Paso 3. Cargar la regla de snort local personalizada

Navegue hasta Objetos > Reglas de intrusión > Reglas de Snort 3 > Todas las reglas en FMC, haga clic en Cargar reglas de Snort 3 de la lista desplegable Tareas.



Cargar regla personalizada

En la pantalla Add Custom Rules (Agregar reglas personalizadas), arrastre y suelte el archivo local custom-rules.txt, seleccione los Rule Groups y Appropriate Action (Combinar reglas en este ejemplo) y, a continuación, haga clic en el botón Next.



Agregar regla personalizada

Confirme que el archivo de regla local se ha cargado correctamente.

## Add Custom Rules



### Summary

✓ 1 new rule

2000:1000000

Download the summary file.

Back

Finish

Confirmar resultado de carga

Navegue hasta Objetos > Reglas de Intrusión > Reglas de Snort 3 All en FMC, haga clic en Todas las Reglas de Snort 2 Convertidas Globales para confirmar la Regla de Snort Local Personalizada cargada.

The screenshot shows the Firewall Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Objects' tab is active, and the 'Snort 3 All Rules' sub-tab is selected. The main content area displays a list of rule groups on the left, including 'Local Rules (1 group)', 'MITRE (1 group)', 'ATT&CK Framework (1 group)', 'Enterprise (13 groups)', and 'Rule Categories (9 groups)'. The 'Local Rules / All Snort 2 Converted Global' group is expanded, showing a table with one rule. The rule has a 'GID:SID' of '2000:1000000' and an 'Info' field containing the rule signature: 'alert tcp any any -> any any ( sid:1000000; gid:2000; flow.established,to\_client; raw\_data; content:"username"; msg:"custom\_http\_sig"; classtype:unknown; rev:3; )'. The 'Rule Action' is set to 'Disable (Default)'. The 'Assigned Groups' and 'Alert Configuration' columns are also visible.

Detalle de la regla personalizada

Paso 4. Cambiar acción de regla

Igual que en el paso 4 del método 1.

Paso 5. Confirmar la regla de Snort local personalizada cargada

Igual que en el paso 5 del método 1.

Paso 6. Asociar política de intrusiones con regla de política de control de acceso (ACP)

Igual que en el paso 6 del método 1.

Paso 7. Implementar cambios

Igual que en el paso 7 del método 1.

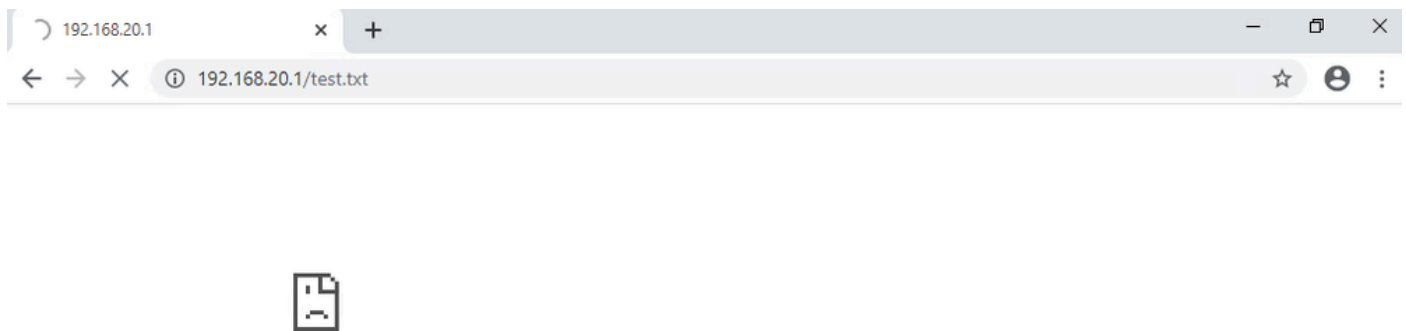
## Verificación

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.

A screenshot of the Fire Management Center (FMC) interface. The 'Analysis' tab is selected. The main area displays 'Events By Priority and Classification' for the period 2024-04-06 13:26:03 to 2024-04-06 14:31:12. A table of events is shown, with one event highlighted. The event details are: Time: 2024-04-06 14:30:48, Priority: low, Impact: Unknown, Inline Result: Block, Reason: custom\_http\_sig (2000:1000000:3), Source IP: 192.168.20.1, Destination IP: 192.168.10.1, Source Port / ICMP Type: 80 (http) / tcp, Destination Port / ICMP Code: 50103 / tcp, Message: custom\_http\_sig (2000:1000000:3), Classification: Unknown Traffic, and Generation: Standard.

Time	Priority	Impact	Inline Result	Reason	Source IP	Source Country	Destination IP	Destination Country	Source Port / ICMP Type	Destination Port / ICMP Code	SSL Status	VLAN ID	Message	Classification	Generation
2024-04-06 14:30:48	low	Unknown	Block	custom_http_sig (2000:1000000:3)	192.168.20.1		192.168.10.1		80 (http) / tcp	50103 / tcp			custom_http_sig (2000:1000000:3)	Unknown Traffic	Standard

Evento de intrusión

Haga clic en la ficha Paquetes y confirme los detalles del evento de intrusión.

The screenshot shows the 'Analysis' tab in the Firewall Management Center. The main heading is 'Events By Priority and Classification'. Below it, there are navigation options: 'Drilldown of Event, Priority, and Classification', 'Table View of Events', and 'Packets'. The 'Event Information' section is expanded, showing details for a rule named 'custom\_http\_sig (2000:1000000:3)'. The event occurred on 2024-04-06 at 14:31:26. The classification is 'Unknown Traffic' with a 'low' priority. The event details include: Ingress Security Zone (outside\_zone), Egress Security Zone (inside\_zone), Device (FPR2120\_FTD), Ingress Interface (outside), and Egress Interface (inside). The source IP is 192.168.20.1, and the destination IP is 192.168.10.1. The source port is 80 (http) / tcp, and the destination port is 50105 / tcp. The HTTP Hostname is 192.168.20.1 and the HTTP URI is /nest.txt. The intrusion policy is snort\_test, the access control policy is acp-rule, and the access control rule is ftd\_acp. The rule definition is: `Rule alert tcp any any <> any any ( sid:1000000; gid:2000; flow:established,to_client; rax_data: content:'username'; msg:'custom_http_sig'; classtype:unknown; rev:3; )`

Detalle del evento de intrusión

## Preguntas frecuentes

P: ¿Qué se recomienda, Snort 2 o Snort 3?

R: En comparación con Snort 2, Snort 3 ofrece velocidades de procesamiento mejoradas y nuevas funciones, lo que la convierte en la opción más recomendada.

P: Después de actualizar de una versión de FTD anterior a la 7.0 a una versión 7.0 o posterior, ¿la versión de snort se actualiza automáticamente a Snort 3 ?

R: No, el motor de inspección permanece en Snort 2. Para utilizar Snort 3 después de la actualización, debe habilitarlo explícitamente. Tenga en cuenta que Snort 2 está planificado para dejar de utilizarse en una futura versión y se recomienda encarecidamente dejar de utilizarlo ahora.

P: En Snort 3, ¿es posible editar una regla personalizada existente?

R: No, no puede editarlo. Para editar una regla personalizada específica, debe eliminar la regla pertinente y volver a crearla.

## Troubleshoot

Ejecute `system support trace` el comando para confirmar el comportamiento en FTD. En este ejemplo, la regla IPS bloquea el tráfico HTTP (2000:1000000:3).

```
<#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:

192.168.10.1 50104 -> 192.168.20.1 80 6 AS=0 ID=4 GR=1-1 Firewall: allow rule, '

**ftd\_acp**

', allow

192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1

**Event**

:

2000:1000000:3

, Action

**block**

192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict: blacklist

192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict Reason:

**ips, block**

Referencia

[Guía de configuración de Cisco Secure Firewall Management Center Snort 3](#)

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).