

# Configurar regras locais personalizadas de Snort no Snort3 no FTD

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Diagrama de Rede](#)

[Configuração](#)

[Método 1. Importar do Snort 2 para o Snort 3](#)

[Etapa 1. Confirmar versão do Snort](#)

[Etapa 2. Crie ou edite uma regra de Snort local personalizada no Snort 2](#)

[Etapa 3. Importar regras locais personalizadas de Snort 2 para Snort 3](#)

[Etapa 4. Ação da regra de alteração](#)

[Etapa 5. Confirmar Importação de Regra de Snort Local Personalizada](#)

[Etapa 6. Associar Política de Intrusão à Regra de Política de Controle de Acesso \(ACP\)](#)

[Passo 7. Implantar alterações](#)

[Método 2. Carregar um arquivo local](#)

[Etapa 1. Confirmar versão do Snort](#)

[Etapa 2. Crie uma regra de Snort local personalizada](#)

[Etapa 3. Carregar a regra de Snort local personalizada](#)

[Etapa 4. Ação da regra de alteração](#)

[Etapa 5. Confirmar upload da regra de Snort local personalizada](#)

[Etapa 6. Associar Política de Intrusão à Regra de Política de Controle de Acesso \(ACP\)](#)

[Passo 7. Implantar alterações](#)

[Verificar](#)

[Etapa 1. Definir Conteúdo do Arquivo no Servidor HTTP](#)

[Etapa 2. Solicitação HTTP inicial](#)

[Etapa 3. Confirmar evento de intrusão](#)

[Perguntas frequentes](#)

[Troubleshooting](#)

[Referência](#)

---

## Introdução

Este documento descreve o procedimento para configurar as Regras locais personalizadas de Snort no Snort3 no Firewall Threat Defense (FTD).

## Pré-requisitos

## Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

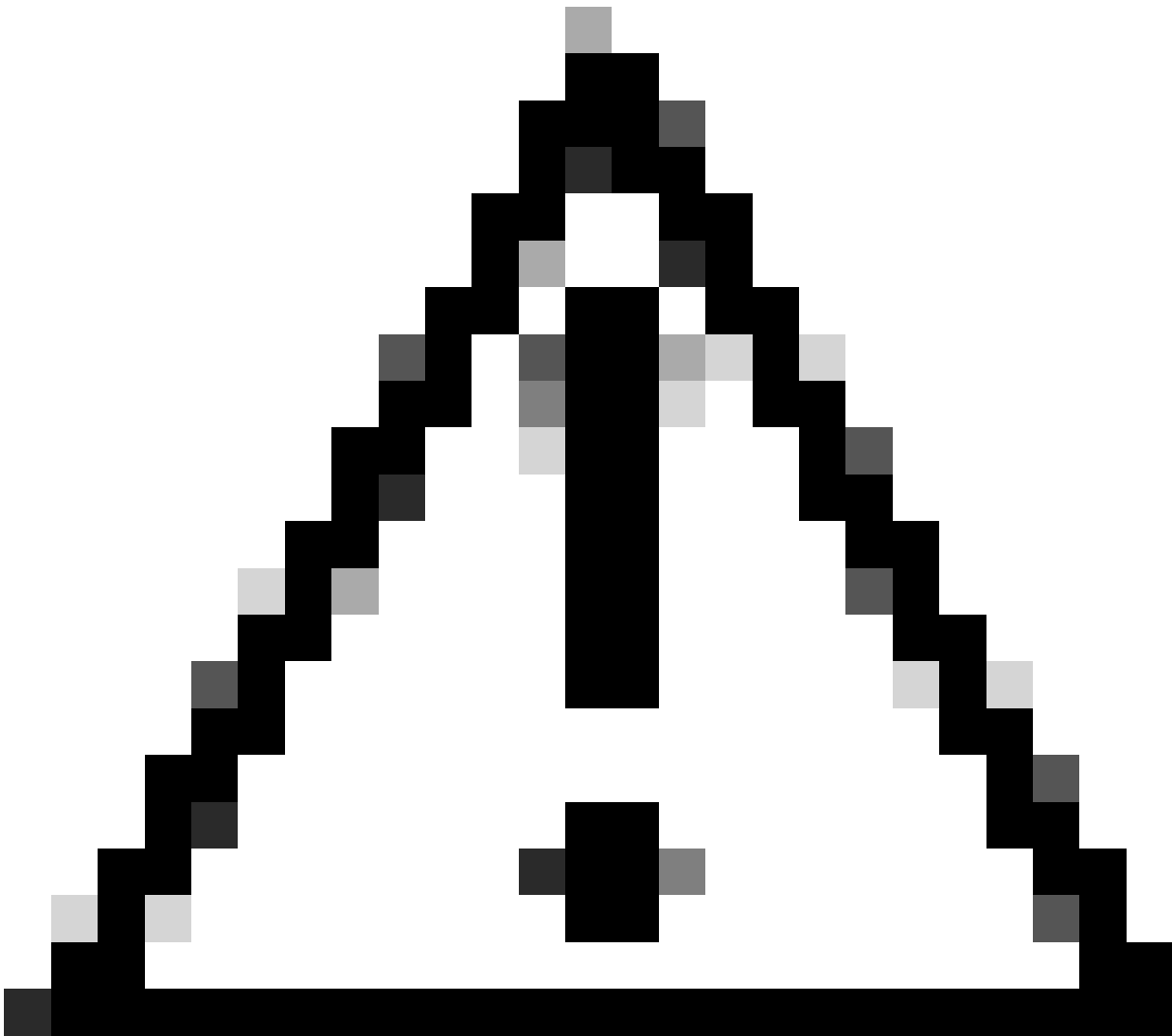
- Cisco Firepower Management Center para VMWare 7.4.1
- Cisco Firepower 2120 7.4.1

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

O suporte para Snort 3 em defesa contra ameaças com o centro de gerenciamento começa na versão 7.0. Para dispositivos novos e recriados da versão 7.0 e posterior, o Snort 3 é o mecanismo de inspeção padrão.

Este documento fornece um exemplo de como personalizar as regras do Snort para o Snort 3, bem como um exemplo prático de verificação. Especificamente, você é apresentado a configurar e verificar uma Política de intrusão com uma regra Snort personalizada para descartar pacotes HTTP que contenham uma determinada string (nome de usuário).



Cuidado: a criação de regras locais personalizadas de snort e o fornecimento de suporte a elas não faz parte da cobertura de suporte do TAC. Portanto, este documento pode ser usado apenas como referência e peça que você crie e gerencie essas regras personalizadas a seu próprio critério e responsabilidade.

---

## Diagrama de Rede

Este documento introduz a configuração e a verificação da regra de Snort local personalizada no Snort3 neste diagrama.

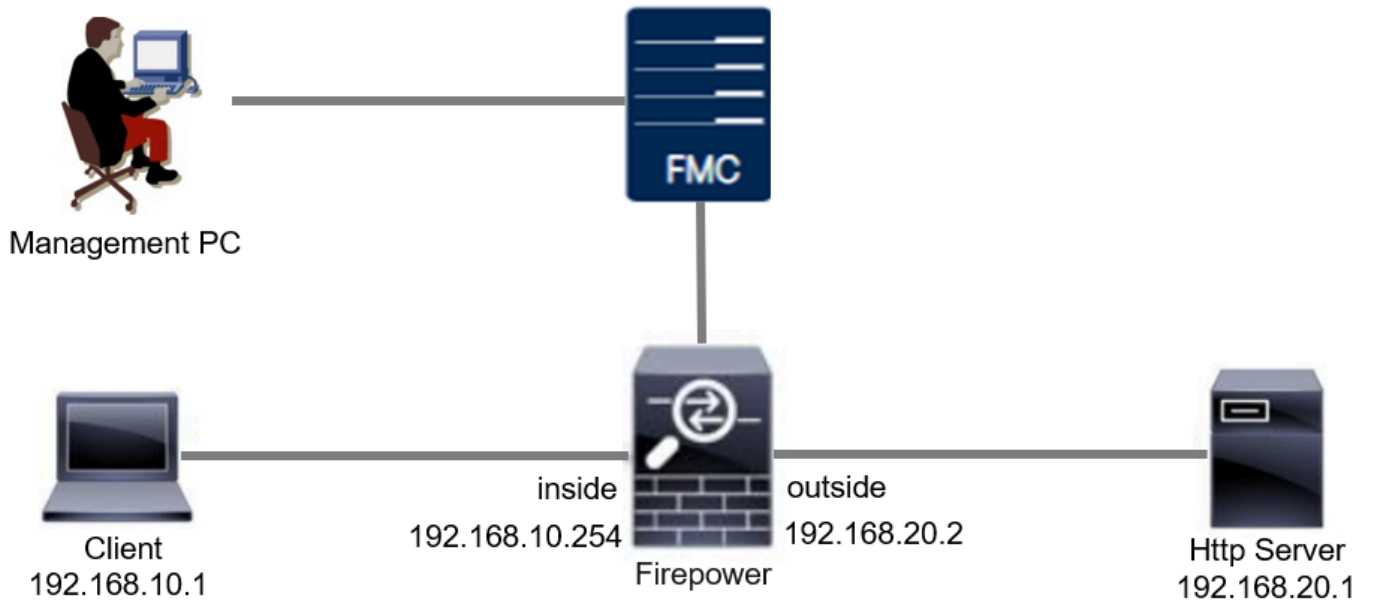


Diagrama de Rede

## Configuração

Esta é a configuração da Regra de Snort Local Personalizada para detectar e descartar pacotes de resposta HTTP contendo uma string específica (nome de usuário).



Observação: a partir de agora, não é possível adicionar regras locais personalizadas de snort na página Snort 3 All Rules na GUI do FMC. Você deve usar o método introduzido neste documento.

---

## Método 1. Importar do Snort 2 para o Snort 3

### Etapa 1. Confirmar a versão do Snort

Navegue até Dispositivos>Gerenciamento de dispositivos no FMC e clique em Devicetab. Confirme se a versão do Snort é Snort3.

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
FPR2120_FTD 1.10.0.29	Firepower 2120 with FTD	7.4.1	N/A	Essentials, IPS (1 more...)	acp-rule	

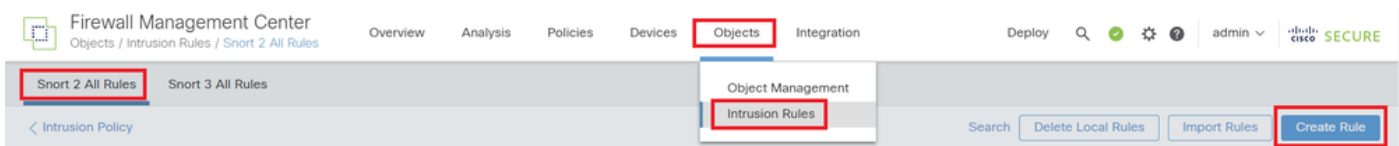
Versão do Snort

## Etapa 2. Crie ou edite uma regra de Snort local personalizada no Snort 2

Navegue até Objetos > Regras de intrusão > Snort 2 All Rules no FMC. Clique no botão Criar regra para adicionar uma regra de snort local personalizada ou Navegue até Objetos > Regras de intrusão > Snort 2 Todas as regras > Regras locais no FMC, clique no botão Editar para editar uma regra de snort local personalizada existente.

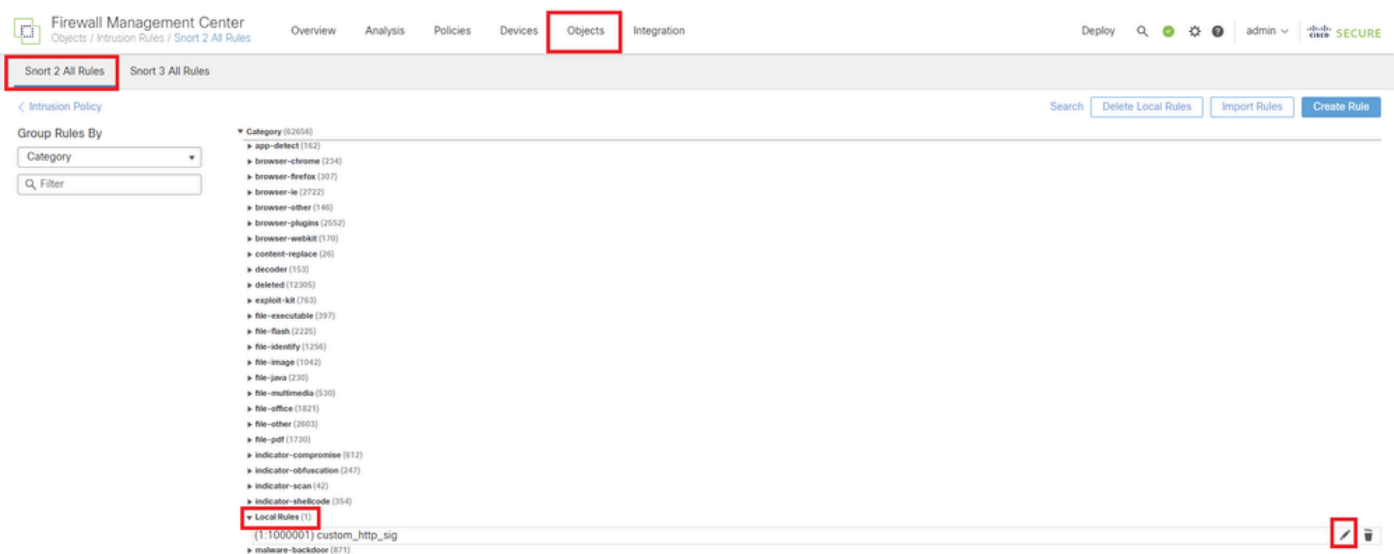
Para obter instruções sobre como criar Regras de Snort Local Personalizadas no Snort 2, consulte [Configurar Regras de Snort Local Personalizadas no Snort2 no FTD](#).

Adicione uma nova Regra de Snort Local Personalizada conforme mostrado na imagem.



Adicionar uma nova regra personalizada

Edite uma Regra de Snort Local Personalizada existente conforme mostrado na imagem. Neste exemplo, edita uma regra personalizada existente.



Editar uma regra personalizada existente

Digite as informações de assinatura para detectar pacotes HTTP contendo uma string específica

(nome de usuário).

- Mensagem : custom\_http\_sig
- Ação : alerta
- Protocolo : tcp
- fluxo : Estabelecido, Para o cliente
- conteúdo : nome de usuário (dados brutos)

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

Inserir informações necessárias para a regra

### Etapa 3. Importar regras locais personalizadas de Snort 2 para Snort 3

Navegue até Objects > Intrusion Rules > Snort 3 All Rules > All Rules no FMC, clique em Convert Snort 2 rules and Import na lista suspensa Tasks.

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 Back To Top

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

Rule Actions	Info	Rule Action	Assigned Groups
50,094 rules			
<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 Snort 3 rules

Convert Snort 2 rules and Import

Convert Snort 2 rules and download

Add Rule Groups

Importar regra personalizada para o Snort 3

Verifique a mensagem de aviso e clique em 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

Mensagem de aviso

Navegue até Objects > Intrusion Rules > Snort 3 All Rules no FMC, clique em All Snort 2 Converted Global para confirmar a Custom Local Snort Rule importada.

The screenshot shows the FireWall Management Center interface. The breadcrumb path is Objects > Intrusion Rules > Snort 3 All Rules. The left sidebar shows a tree view with 'Local Rules (1 group)' expanded, and 'All Snort 2 Converted Global' selected. The main content area shows the details for this rule group, including a description and a table of rules. A success message 'The custom rules were successfully imported' is displayed in a green box. The table below shows one rule with the following details:

GID:SID	Info	Rule Action	Assigned Groups	Alert Configuration
2000:1000000	custom_http_sig	Disable (Default)	All Snort 2 Converted Glo...	None

Confirmar Regra Personalizada Importada

### Etapa 4. Ação da regra de alteração

Clique em Por política de intrusão de acordo com a Ação da regra da regra 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 ✕

<input type="checkbox"/>	GID:SID	Info	Rule Action	Assigned Groups	Alert Configuration
<input checked="" type="checkbox"/>	2000:1000000	custom_http_sig	<div style="border: 1px solid blue; padding: 2px;">                     Disable (Default) <small>(Overridden)</small>                      Block                      Alert                      Rewrite                      Drop                      Pass                      Reject                      Disable (Default)                      Revert to default                      Per Intrusion Policy                 </div>	All Snort 2 Converted Glo...	None

Ação da regra de alteração

Na tela Editar ação da regra, digite as informações para a política e ação da regra.

- Política : snort\_test
- Ação da regra : BLOQUEAR



Observação: as ações de regra são:

**Bloquear**— Gera evento, bloqueia o pacote correspondente atual e todos os pacotes subsequentes nesta conexão.

**Alerta**— Gera somente eventos para o pacote correspondente e não descarta o pacote ou a conexão.

**Regravação**— Gera evento e sobregrava o conteúdo do pacote com base na opção de substituição da regra.

**Aprovado**— Nenhum evento é gerado, permite que o pacote passe sem avaliação adicional por quaisquer regras de Snort subsequentes.

**Eliminação**— Gera evento, elimina o pacote correspondente e não bloqueia mais tráfego nesta conexão.

**Rejeitar**— Gera evento, descarta o pacote correspondente, bloqueia mais tráfego nesta conexão e envia a reinicialização do TCP se for um protocolo TCP para os hosts origem e

---

destino.

Desabilitar — Não corresponde o tráfego desta regra. Nenhum evento é gerado.

Padrão — Reverte para a ação padrão do 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

Ação Editar regra

## Etapa 5. Confirmar Importação de Regra de Snort Local Personalizada

Navegue para **Policies > Intrusion Policies** no FMC, clique em **Snort 3 Version** correspondente à **Intrusion Policy** de destino na linha.

Firewall Management Center

Policies / Access Control / Intrusion / Intrusion Policies

Overview Analysis Policies Devices Objects Integration Deploy

Intrusion Policies Network Analysis Policies

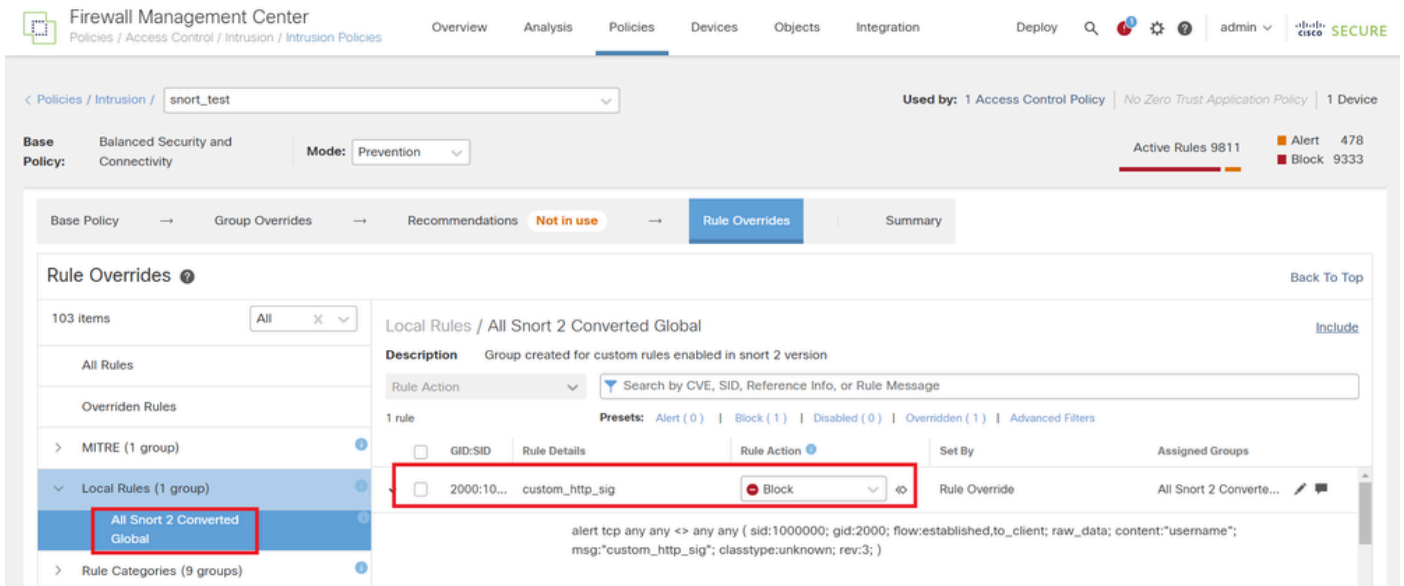
Hide Snort 3 Sync status Search by Intrusion Policy, Description, or Base Policy All IPS Rules IPS Mapping Compare Policies Create Policy

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 Regra Personalizada Importada

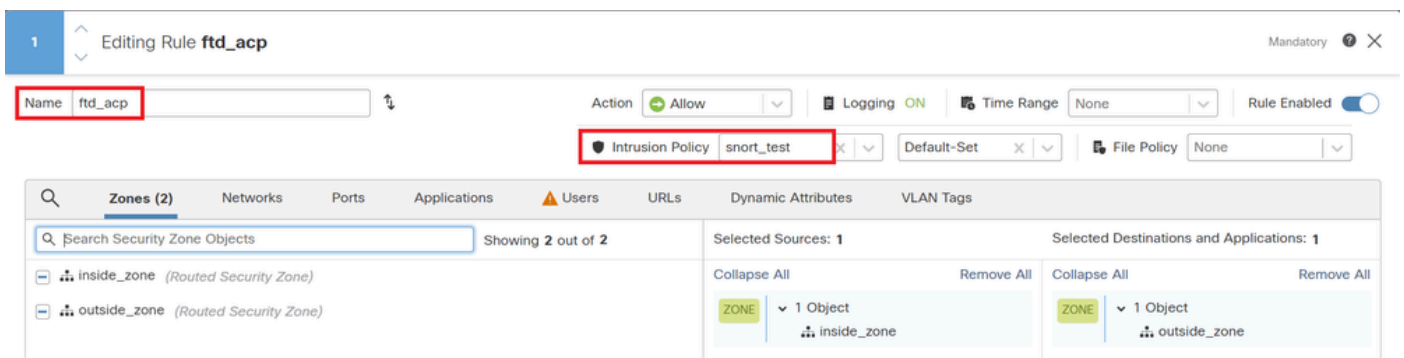
Clique em **Local Rules > All Snort 2 Converted Global** para verificar os detalhes da **Custom Local Snort Rule**.



Confirmar Regra Personalizada Importada

## Etapa 6. Associar Política de Intrusão à Regra de Política de Controle de Acesso (ACP)

Navegue para Políticas > Access Control FMC, associe Intrusion Policy ao ACP.



Associar à Regra de ACP

## Passo 7. Implantar alterações

Implante as alterações no FTD.



Implantar alterações

## Método 2. Carregar um arquivo local

### Etapa 1. Confirmar versão do Snort

O mesmo que na etapa 1 do método 1.

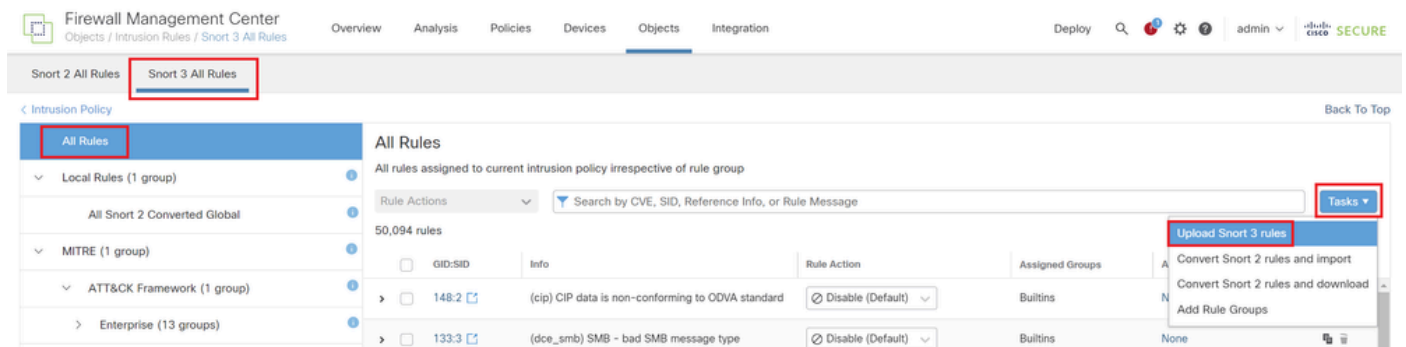
### Etapa 2. Crie uma regra de Snort local personalizada

Crie manualmente uma Regra de Snort Local Personalizada e salve-a em um arquivo local chamado custom-rules.txt.

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

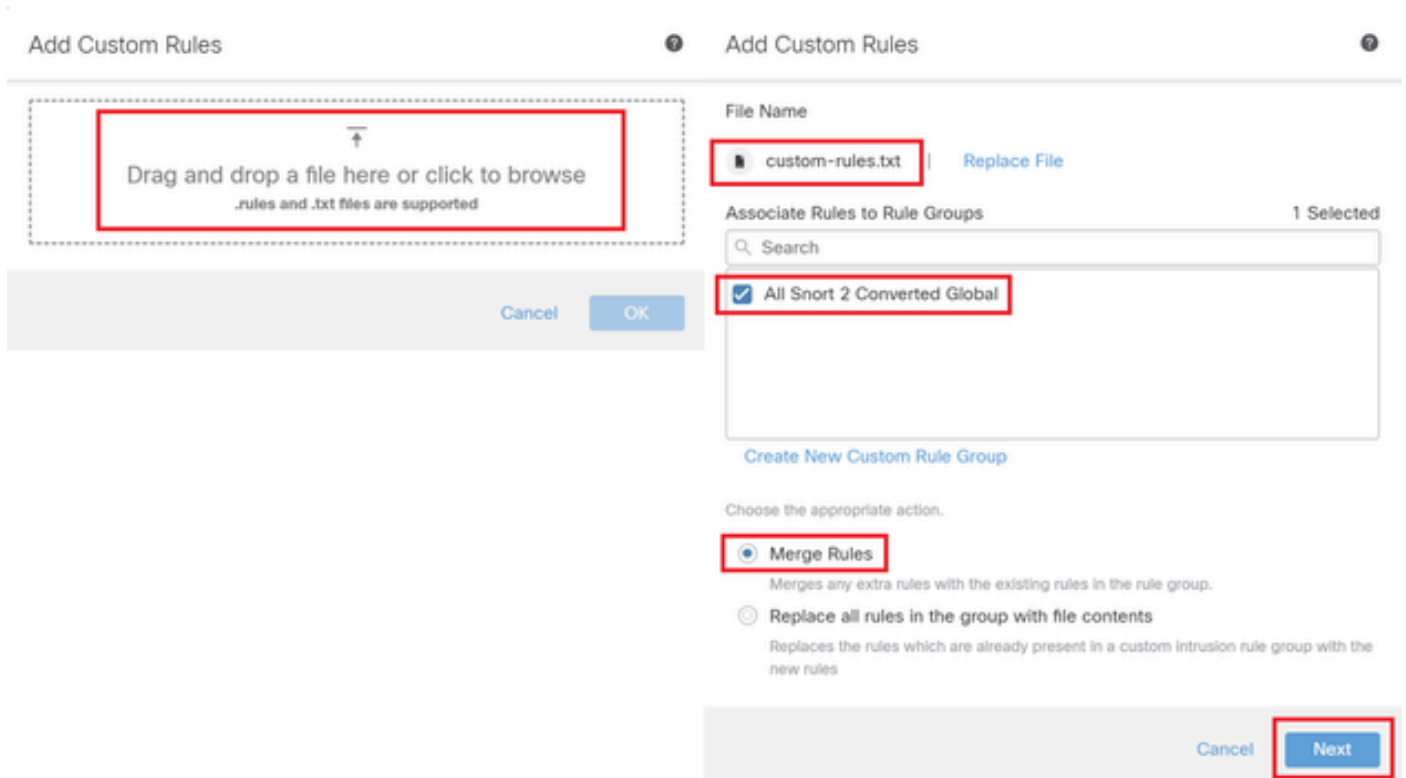
### Etapa 3. Carregar a regra de Snort local personalizada

Navegue até Objects > Intrusion Rules > Snort 3 All Rules > All Rules no FMC, clique em Upload Snort 3 rules na lista suspensa Tasks.



### Carregar Regra Personalizada

Na tela Adicionar regras personalizadas, arraste e solte o arquivo local custom-rules.txt, selecione os Grupos de regras e a Ação apropriada (Mesclar regras neste exemplo) e clique no botão Avançar.



### Adicionar regra personalizada

Confirme se o arquivo de regras local foi carregado com êxito.

## Add Custom Rules



### Summary

✓ 1 new rule

2000:1000000

[Download the summary file.](#)

[Back](#)

[Finish](#)

Confirmar resultado do upload

Navegue para Objects > Intrusion Rules > Snort 3 All Rules no FMC, clique em All Snort 2 Converted Global para confirmar a regra de snort local personalizada carregada.

The screenshot shows the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes "Overview", "Analysis", "Policies", "Devices", "Objects", and "Integration". The "Objects" tab is selected. The breadcrumb trail is "Objects / Intrusion Rules / Snort 3 All Rules". The main content area is titled "Local Rules / All Snort 2 Converted Global". It shows a list of rules with the following columns: "gid:SID", "Info", "Rule Action", "Assigned Groups", and "Alert Configuration". A single rule is listed with the following details:

gid:SID	Info	Rule Action	Assigned Groups	Alert Configuration
2000:1000000	custom_http_sig	Disable (Default)	All Snort 2 Converted Glo...	None

The rule's alert configuration is shown in a text box below the table:

```
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; )
```

Detalhes da regra personalizada

Etapa 4. Ação da regra de alteração

O mesmo que na etapa 4 do método 1.

Etapa 5. Confirmar upload da regra de Snort local personalizada

O mesmo que na etapa 5 do método 1.

Etapa 6. Associar Política de Intrusão à Regra de Política de Controle de Acesso (ACP)

O mesmo que na etapa 6 do método 1.

## Passo 7. Implantar alterações

O mesmo que na etapa 7 do método 1.

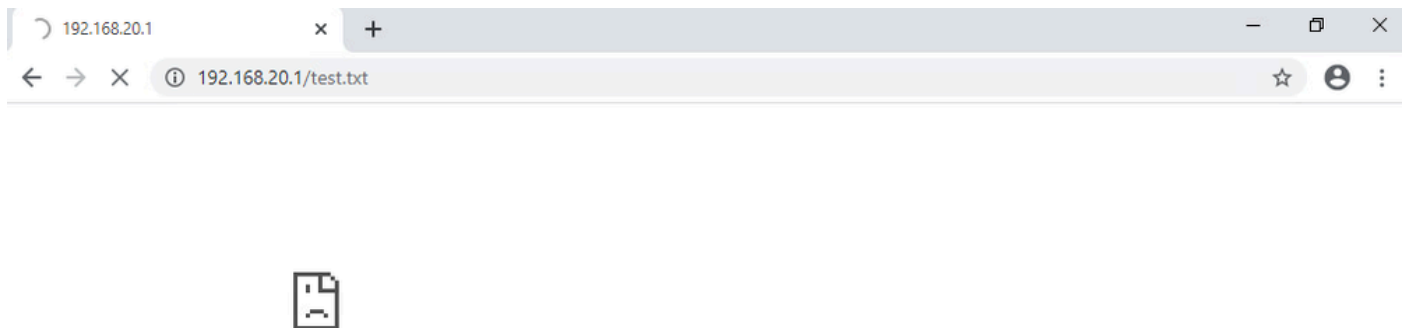
## Verificar

### Etapa 1. Definir Conteúdo do Arquivo no Servidor HTTP

Defina o conteúdo do arquivo test.txt no lado do servidor HTTP como nome de usuário.

### Etapa 2. Solicitação HTTP inicial

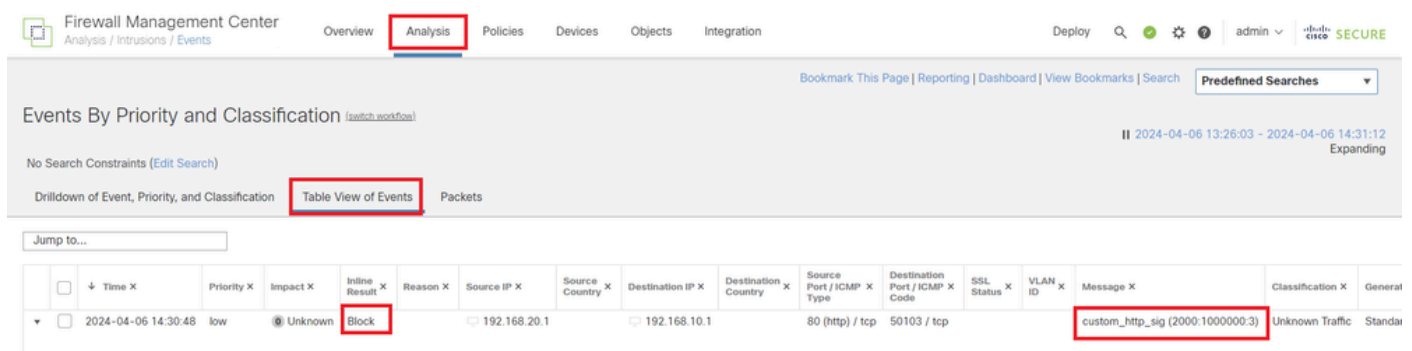
Acesse o Servidor HTTP (192.168.20.1/test.txt) a partir do navegador do cliente (192.168.10.1) e confirme se a comunicação HTTP está bloqueada.



Solicitação HTTP inicial

### Etapa 3. Confirmar evento de intrusão

Navegue até Analysis>Intrusions>Events no FMC, confirme se o evento de intrusão é gerado pela regra de Snort local personalizada.

A screenshot of the Cisco Firewall Management Center (FMC) interface. The 'Analysis' tab is selected. The main area shows 'Events By Priority and Classification' with a table view of events. A single event is listed, which is a 'Block' action triggered by a Snort rule. The event details are as follows:

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	Generated
2024-04-06 14:30:48	low	Unknown	Block		192.168.20.1		192.168.10.1		80 (http) / tcp	50103 / tcp			custom_http_sig (2000:1000000:3)	Unknown Traffic	Standar

Evento de intrusão

Clique em Packetstab, confirme os detalhes do evento de intrusão.

Firewall Management Center  
Analysis / Intrusions / Events

Overview **Analysis** Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin **SECURE**

Bookmark This Page | Reporting | Dashboard | View Bookmarks | Search **Predefined Searches**

Events By Priority and Classification [/search/2003f0a](#)

No Search Constraints [\(Edit Search\)](#)

Drilldown of Event, Priority, and Classification | Table View of Events **Packets**

2024-04-06 13:26:03 - 2024-04-06 14:32:46  
Expanding

Event Information

Message custom\_http\_sig (2000:1000000:3)

Time 2024-04-06 14:31:26

Classification Unknown Traffic

Priority low

Ingress Security Zone outside\_zone

Egress Security Zone inside\_zone

Device FPR2120\_FTD

Ingress Interface outside

Egress Interface inside

Source IP 192.168.20.1

Source Port / ICMP Type 80 (http) / tcp

Destination IP 192.168.10.1

Destination Port / ICMP Code 50105 / tcp

HTTP Hostname 192.168.20.1

HTTP URI /nest.txt

Intrusion Policy snort\_test

Access Control Policy acp-rule

Access Control Rule ftd\_acp

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; )

Actions

Detalhes do evento de intrusão

## Perguntas frequentes

P : Qual das alternativas a seguir é recomendável, Snort 2 ou Snort 3 ?

R: Comparado ao Snort 2, o Snort 3 oferece velocidades de processamento aprimoradas e novos recursos, tornando-o a opção mais recomendada.

P: Após a atualização de uma versão do FTD anterior à 7.0 para uma versão 7.0 ou posterior, a versão do Snort é atualizada automaticamente para o Snort 3 ?

R: Não, o motor de inspeção permanece no Snort 2. Para usar o Snort 3 após a atualização, você deve habilitá-lo explicitamente. Observe que o Snort 2 está planejado para ser substituído em uma versão futura e é altamente recomendável parar de usá-lo agora.

P: No Snort 3, é possível editar uma regra personalizada existente?

R: Não, você não pode editá-lo. Para editar uma regra personalizada específica, você deve excluir a regra relevante e recriá-la.

## Troubleshooting

**Execute** `system support trace` o comando para confirmar o comportamento no FTD. Neste exemplo, o tráfego HTTP é bloqueado pela regra IPS (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

Referência

[Guia de configuração do Cisco Secure Firewall Management Center Snort 3](#)

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.