

Configurar regras locais personalizadas de Snort no Snort2 no FTD

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração](#)

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

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

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

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

[Etapa 5. Associar Política de Intrusão à Regra de Política de Controle de Acesso \(ACP\)](#)

[Etapa 6. Implantar alterações](#)

[Verificar](#)

[A regra de Snort local personalizada não é acionada](#)

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

[Etapa 2. Solicitação HTTP inicial](#)

[A regra de Snort local personalizada é acionada](#)

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

[Etapa 2. Solicitação HTTP inicial](#)

[Etapa 3. Evento de Intrusão de Confirmação](#)

[Troubleshooting](#)

Introdução

Este documento descreve o procedimento para configurar as Regras locais personalizadas de Snort no Snort2 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:

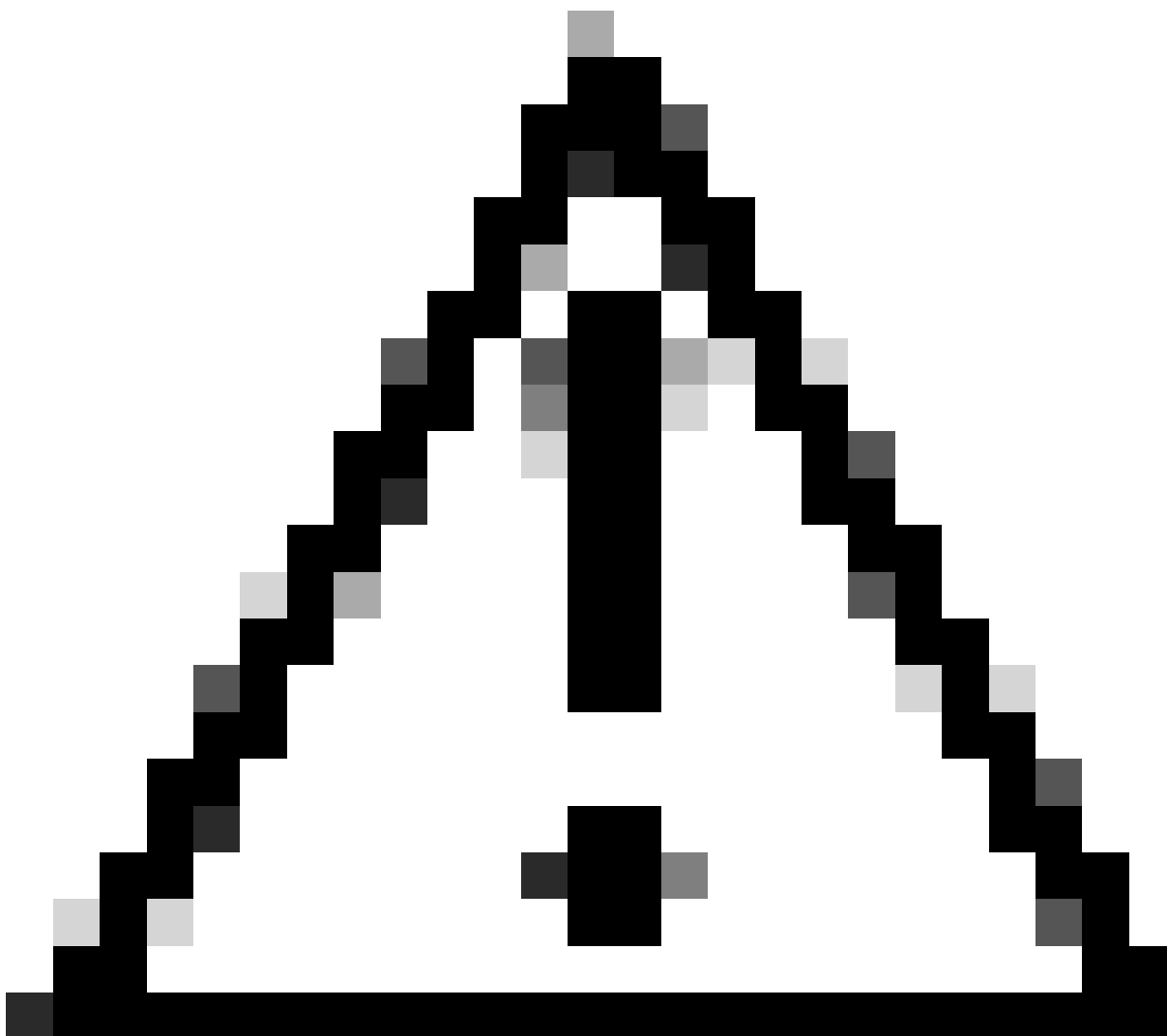
- Cisco Firepower Management Center para VMWare 7.4.1
- Cisco Firepower 2120 7.4.1

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

Regra de Snort Local Personalizada refere-se a uma regra definida pelo usuário que você pode criar e implementar no sistema de detecção e prevenção de intrusão Snort integrado ao FTD. Ao criar uma regra Snort local personalizada no Cisco FTD, você está essencialmente definindo um novo padrão ou conjunto de condições que o mecanismo Snort pode observar. Se o tráfego de rede corresponder às condições especificadas em sua regra personalizada, o Snort poderá executar a ação definida na regra, como gerar um alerta ou descartar o pacote. Os administradores usam regras locais personalizadas do Snort para lidar com ameaças específicas não cobertas pelos conjuntos de regras gerais.

Neste documento, você é apresentado como configurar e verificar uma Regra de Snort Local Personalizada projetada para detectar e descartar pacotes de resposta HTTP contendo uma string específica (nome de usuário).

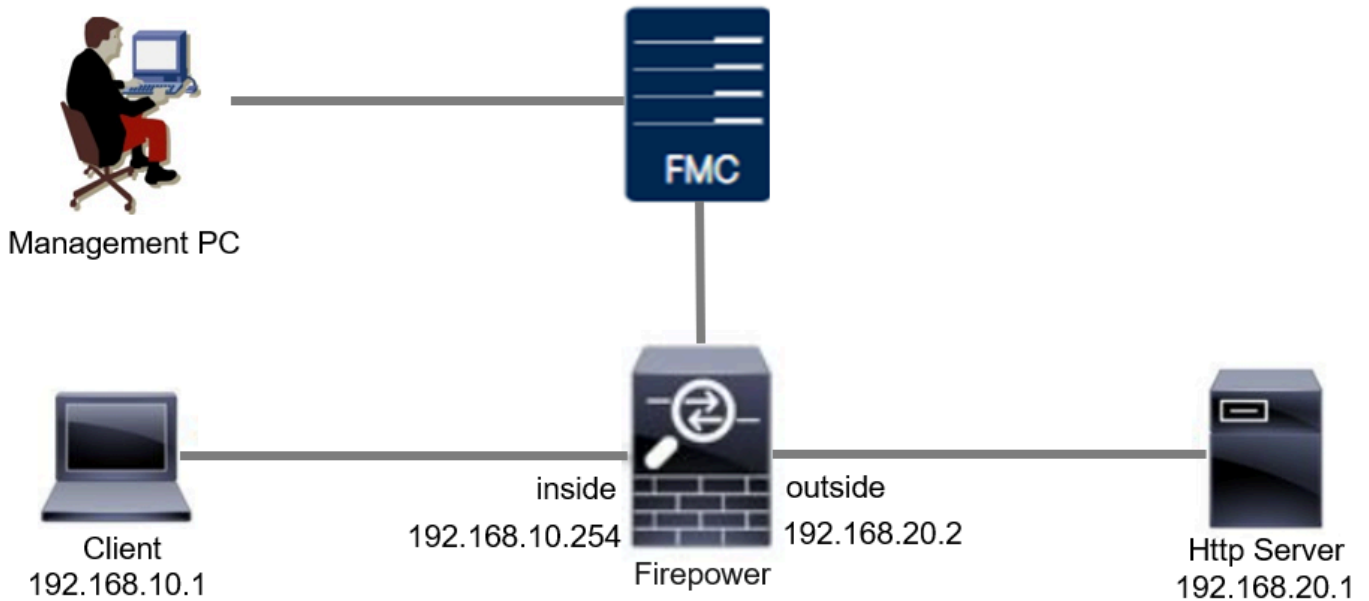


Cuidado: a criação de regras locais personalizadas de Snort e o fornecimento de suporte a elas não faz parte da cobertura de suporte do TAC. Portanto, este documento pode ser usado apenas como referência e peça que você crie e gerencie essas regras personalizadas a seu próprio critério e responsabilidade.

Configurar

Diagrama de Rede

Este documento introduz a configuração e a verificação da Regra de Snort Local Personalizada no Snort2 neste diagrama.



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).

Etapa 1. Confirmar versão do Snort

Navegue até Devices > Device Management no FMC e clique na guia Device. A confirmação da versão de snort é Snort2.

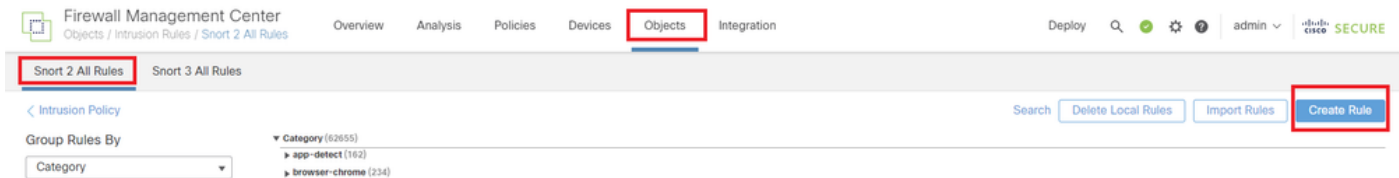
The screenshot shows the Cisco Firewall Management Center (FMC) interface. The 'Devices' tab is selected, and the 'Device' sub-tab is active. The configuration for device FPR2120_FTD is displayed. The 'Inspection Engine' is set to 'Snort 2'.

Section	Property	Value	
General	Name:	FPR2120_FTD	
	Transfer Packets:	Yes	
	Troubleshoot:	Logs CLI Download	
	Mode:	Routed	
	Compliance Mode:	None	
	TLS Crypto Acceleration:	Enabled	
	Device Configuration:	Import Export Download	
	OnBoarding Method:	Registration Key	
	License	Essentials:	Yes
		Export-Controlled Features:	Yes
Malware Defense:		Yes	
IPS:		Yes	
Carrier:		No	
URL:		No	
Secure Client Premier:		No	
System	Model:	Cisco Firepower 2120 Threat Defense	
	Serial:	J4N0111C7J2	
	Time:	2024-04-06 01:26:12	
	Time Zone:	UTC (UTC+0:00)	
Inspection Engine	Inspection Engine:	Snort 2	
	Health	Status: ●	
Management	Remote Host Address:	1.1.1.1	

Versão do Snort

Etapa 2. Crie uma regra de Snort local personalizada no Snort 2

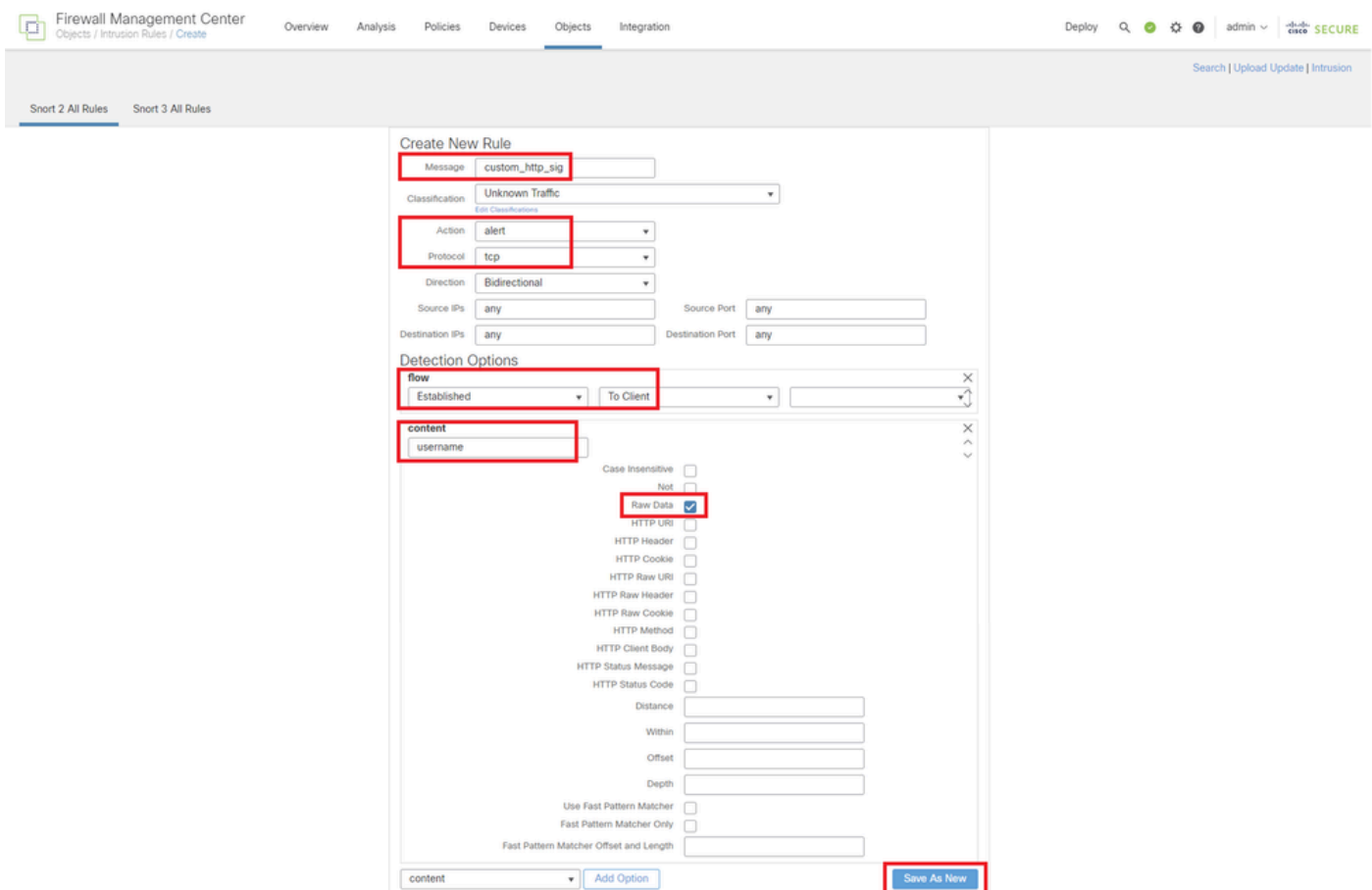
Navegue até Objects > Intrusion Rules > Snort 2 All Rules no FMC, clique no botão Create Rule.



Criar Regra Personalizada

Insira as informações necessárias para a Regra de Snort Local Personalizada.

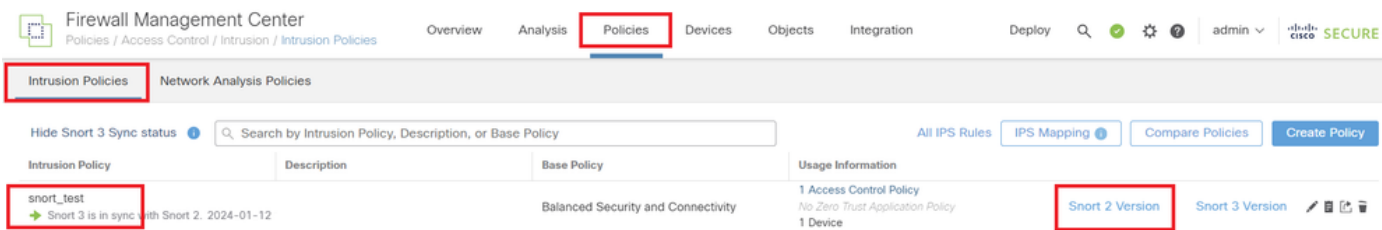
- Intrusão : custom_http_sig
- Ação : alerta
- Protocolo : tcp
- fluxo : Estabelecido, Para o cliente
- conteúdo : nome de usuário (dados brutos)



Inserir informações necessárias para a regra

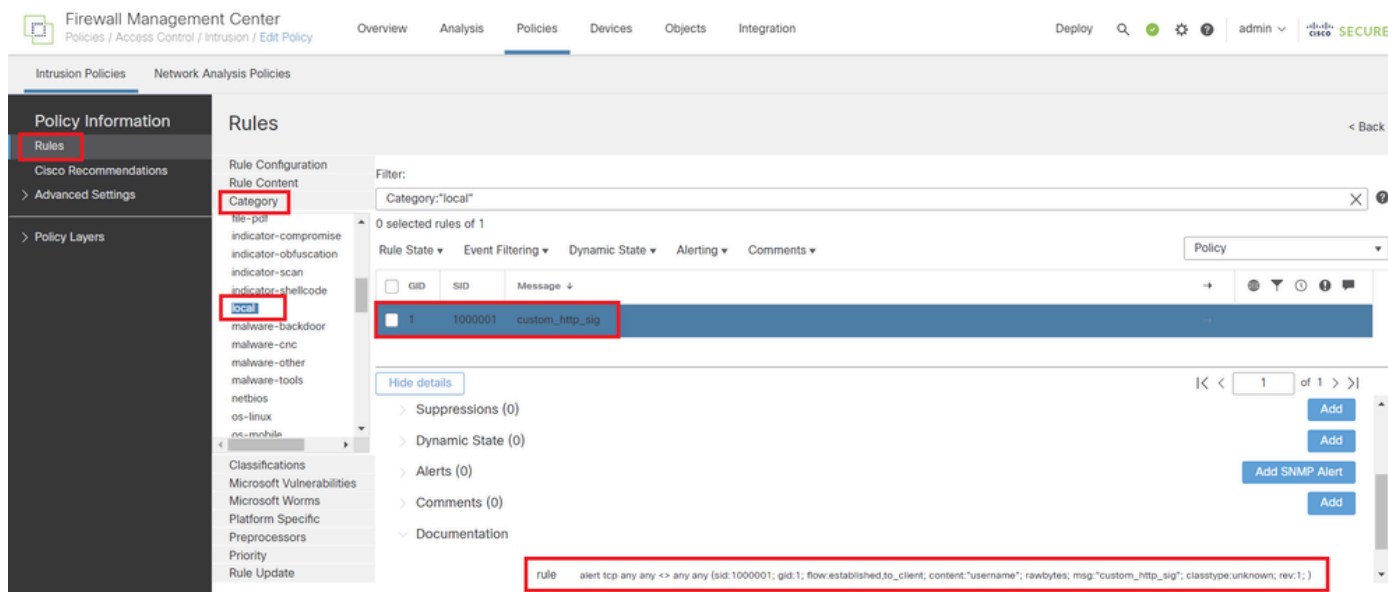
Etapa 3. Confirmar regra de Snort local personalizada

Navegue para Políticas > Intrusion Policies no FMC, clique no botão Snort 2 Version.



Confirmar regra personalizada

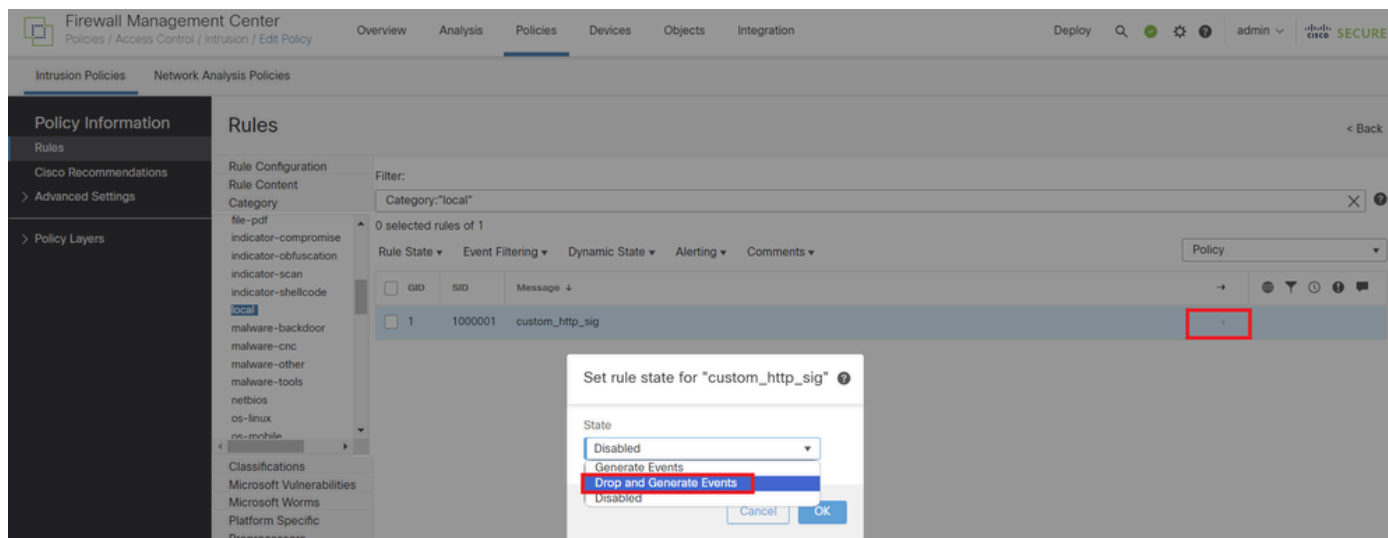
Navegue até Rules > Category > local no FMC e confirme os detalhes de Custom Local Snort Rule.



Detalhes da regra personalizada

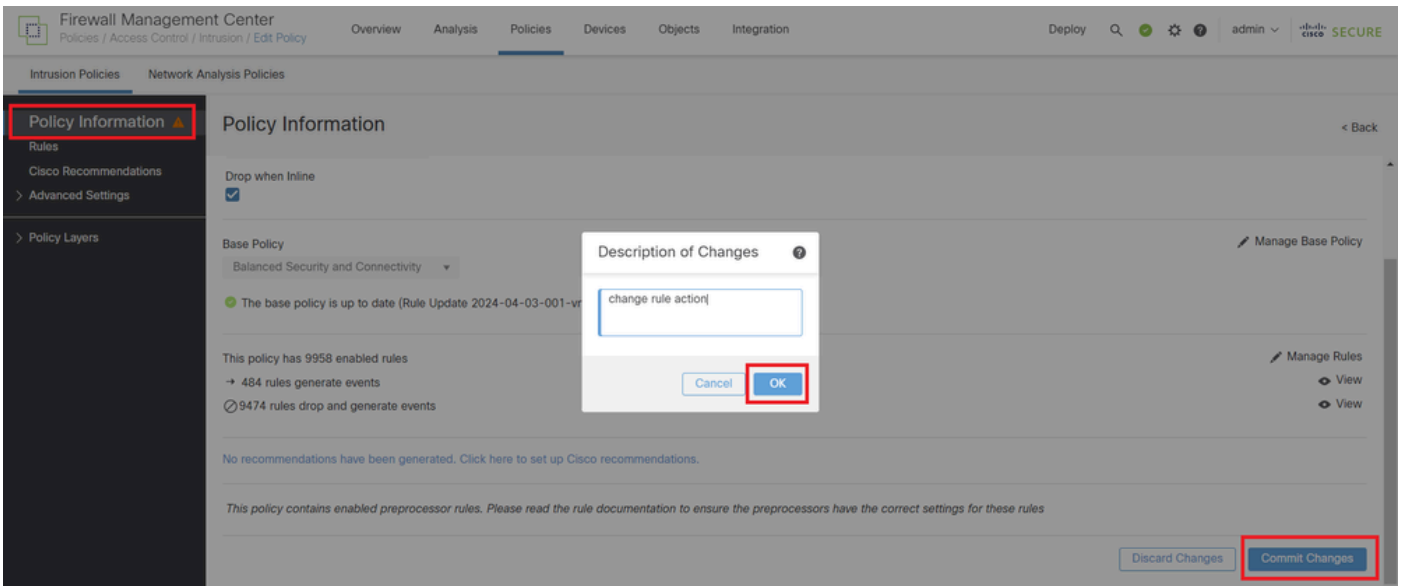
Etapa 4. Ação da regra de alteração

Clique no botão State, defina o estado como Drop and Generate Events e clique no botão OK.



Alterar a ação da regra

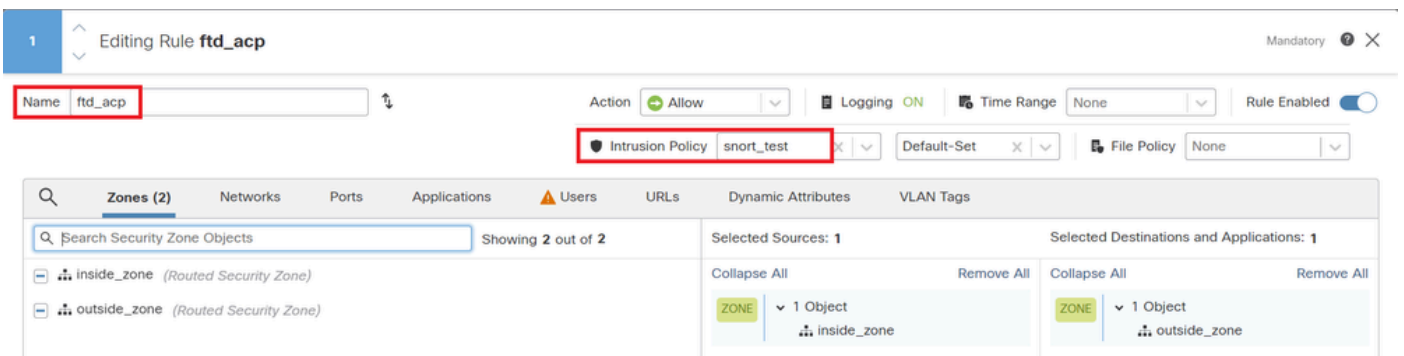
Clique no botão Informações da política, clique no botão Confirmar alterações para salvar as alterações.



Confirmar alterações

Etapa 5. Associar Política de Intrusão à Regra de Política de Controle de Acesso (ACP)

Navegue para Policies > Access Control no FMC, associe Intrusion Policy ao ACP.



Associar à Regra de ACP

Etapa 6. Implantar alterações

Implante as alterações no FTD.



Implantar alterações

Verificar

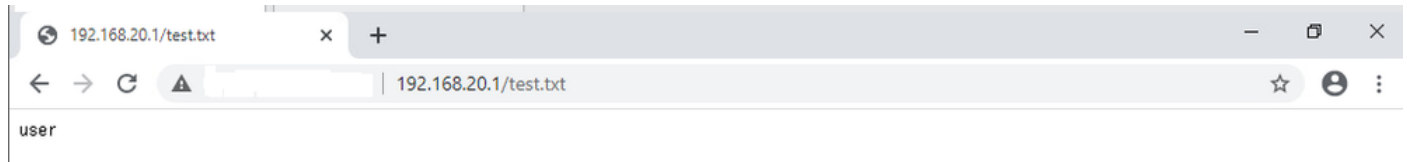
A regra de Snort local personalizada não é acionada

Etapa 1. Definir Conteúdo do Arquivo no Servidor HTTP

Defina o conteúdo do arquivo test.txt no lado do servidor HTTP como 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 é permitida.



Solicitação HTTP inicial

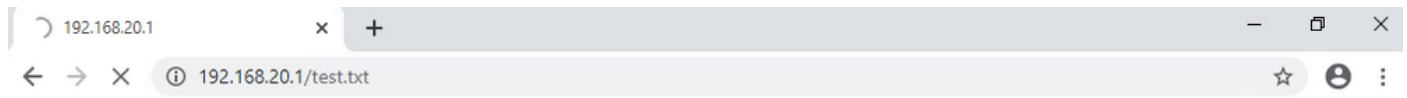
A regra de Snort local personalizada é acionada

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

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 [\[switch workflow\]](#)

II 2024-04-06 09:41:20 - 2024-04-06 11:06:04 Expanding

Search Constraints [\[Edit Search Save Search\]](#)

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

Jump to...

	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	Generate
<input type="checkbox"/>	2024-04-06 11:05:13	low	Unknown	Dropped		192.168.20.1		192.168.10.1		80 (http) / tcp	50057 / tcp			custom_http_sig (1:1000001:1)	Unknown Traffic	Standard

Evento de intrusão

Clique na guia Packets e confirme os detalhes do Intrusion Event.

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 [\[switch workflow\]](#)

II 2024-04-06 09:41:20 - 2024-04-06 11:07:15 Expanding

Search Constraints [\[Edit Search Save Search\]](#)

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

Event Information

Message custom_http_sig (1:1000001:1)

Time 2024-04-06 11:06:34

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 50061 / tcp

HTTP Hostname 192.168.20.1

HTTP URI /test.txt

Intrusion Policy snort_test

Access Control Policy acp-rule

Access Control Rule ftd_acp

Rule alert tcp any any <> any any (sid:1000001; gid:1; flow:established,to_client; content:"username"; rsnbytes; msz:"custom_http_sig"; classtype:unknown; rev:1;)

Actions

Detalhes do evento de intrusão

Troubleshooting

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

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.