

# Configurar ações adicionais de regra do Snort 3 no FMC

## Contents

---

[Introdução](#)

[Informações de Apoio](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Detalhes do recurso](#)

[Passo a Passo do FMC](#)

---

## Introdução

Este documento descreve o suporte do Firepower Management Center (FMC) para o recurso adicional de ações de regra do Snort 3 adicionado na versão 7.1.

## Informações de Apoio

Embora o Firepower Threat Defense (FTD) suporte sete ações de regra de política de intrusão Alerta/Desativar/Bloquear/Rejeitar/Regravar/Passar/Descartar no 7.0, o FMC suportou apenas três ações de regra do Snort 3: "Alert" (Alerta), "Disable" (Desativar) e "Block" (Bloquear).

A partir do Firepower 7.1.0, o FMC oferece suporte para configurar novas ações de regra.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento do Snort de código aberto
- Firepower Management Center (FMC) 7.1.0+
- Firepower Threat Defense (FTD) 7.0.0+

### Componentes Utilizados

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

- Este documento se aplica a todas as plataformas Firepower que executam o Snort 3
- Cisco Firepower Threat Defense Virtual (FTD), que executa a versão 7.4.2 do software
- Firepower Management Center Virtual (FMC), que executa a versão 7.4.2 do software

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.

## Detalhes do recurso

As novas ações de regra do Snort 3 adicionadas e suas descrições são as seguintes:

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

**Soltar:** Gera evento, descarta o pacote correspondente e não bloqueia mais tráfego nesta conexão.

**Reject:** Gera evento, descarta o pacote correspondente, bloqueia mais tráfego nesta conexão e envia a reinicialização do TCP ou a porta ICMP inalcançável para os hosts origem e destino.

**Reescrever:** Gera eventos e sobregrava o conteúdo do pacote com base na opção de substituição na regra.

## Passo a Passo do FMC

Para exibir as regras do Snort 3 em uma política de intrusão, navegue para [FMC Policies > Access Control > Intrusion](#), depois clique na opção **Versão do Snort 3** no canto superior direito da política, como mostrado na imagem:



Versão do Snort 3

Clique em [Base Policy > All Rules](#), você pode ver as ações padrão de todas as regras do Snort 3 definidas pelo sistema.

< Policies / Intrusion / FTD\_Intrusion

Used by: No Access Control Policy | No Zero Trust Application Policy | No Device

Base Policy: Balanced Security and Connectivity Mode: Prevention

Active Rules 9693 Alert 474 Block 9219

Base Policy → Group Overrides → Recommendations Not in use → Rule Overrides | Summary

### Balanced Security and Connectivity

50 items

All Rules

49,532 rules

Presets: Alert ( 474 ) | Block ( 9,219 ) | Disabled ( 39,839 ) | Overridden ( 0 ) | Advanced Filters

GID:SID	Rule Details	Rule Action	Assigned Groups
1:28496	BROWSER-IE Microsoft Internet Explorer crea...	Alert (Default)	Malicious File,Drive-by Co...
1:32478	BROWSER-IE Microsoft Internet Explorer CSe...	Alert (Default)	Malicious File,Drive-by Co...
1:32479	BROWSER-IE Microsoft Internet Explorer CSe...	Alert (Default)	Malicious File,Drive-by Co...
1:26633	BROWSER-IE Microsoft Internet Explorer html...	Alert (Default)	Malicious File,Internet Expl...
1:31621	BROWSER-IE Microsoft Internet Explorer onre...	Alert (Default)	Malicious File,Drive-by Co...
1:31622	BROWSER-IE Microsoft Internet Explorer onre...	Alert (Default)	Malicious File,Drive-by Co...

Política básica

Para alterar a ação da regra para qualquer uma dessas novas ações de regra, navegue até Substituições de regra > Todas as regras e selecione a ação da regra no menu suspenso para a regra selecionada.

< Policies / Intrusion / FTD\_Intrusion

Used by: No Access Control Policy | No Zero Trust Application Policy | No Device

Base Policy: Balanced Security and Connectivity Mode: Prevention

Active Rules 9693 Alert 474 Block 9219

Base Policy → Group Overrides → Recommendations Not in use → Rule Overrides | Summary

### Rule Overrides

102 items

All Rules

49,532 rules

Presets: Alert ( 474 ) | Block ( 9,219 ) | Disabled ( 39,839 ) | Overridden ( 0 ) | Advanced Filters

GID:SID	Rule Details	Rule Action	Set By	Assigned Groups
1:28496	BROWSER-IE Microsoft Internet ...	Alert (Default)	Base Policy	Malicious File,Drive...
1:32478	BROWSER-IE Microsoft Internet ...	Block	Base Policy	Malicious File,Drive...
1:32479	BROWSER-IE Microsoft Internet ...	Alert (Default)	Base Policy	Malicious File,Drive...
1:26633	BROWSER-IE Microsoft Internet ...	Rewrite	Base Policy	Malicious File,Inter...
1:31621	BROWSER-IE Microsoft Internet ...	Drop	Base Policy	Malicious File,Drive...
1:31622	BROWSER-IE Microsoft Internet ...	Reject	Base Policy	Malicious File,Drive...
1:31622	BROWSER-IE Microsoft Internet ...	Disable	Base Policy	Malicious File,Drive...
1:31622	BROWSER-IE Microsoft Internet ...	Revert to default	Base Policy	Malicious File,Drive...

Ações de Regra Adicionais

< Policies / Intrusion / FTD\_Intrusion Used by: No Access Control Policy | No Zero Trust Application Policy | No Device

Base Policy: Balanced Security and Connectivity Mode: Prevention Active Rules 9693 Alert 474 Block 9219

Base Policy → Group Overrides → Recommendations **Not in use** → **Rule Overrides** | Summary

**Rule Overrides** Back To Top

102 items All x v Rule Action Search by CVE, SID, Reference Info, or Rule Message

49,532 rules Presets: Alert ( 474 ) | Block ( 9,219 ) | Disabled ( 39,839 ) | Overridden ( 0 ) | Advanced Filters

✔ Rule action changed successfully ✕

	GID:SID	Rule Details	Rule Action	Set By	Assigned Groups
>	1:28496	BROWSER-IE Microsoft Internet ...	<b>Reject</b>	Rule Override	Malicious File, Drive...
>	1:32478	BROWSER-IE Microsoft Internet ...	Alert (Default)	Base Policy	Malicious File, Drive...
>	1:32479	BROWSER-IE Microsoft Internet ...	Alert (Default)	Base Policy	Malicious File, Drive...
>	1:26633	BROWSER-IE Microsoft Internet ...	Alert (Default)	Base Policy	Malicious File, Inter...

Como alterar a ação da regra

As regras substituídas podem ser encontradas em Substituições de regra > Regras substituídas.

< Policies / Intrusion / FTD\_Intrusion Used by: No Access Control Policy | No Zero Trust Application Policy | No Device

Base Policy: Balanced Security and Connectivity Mode: Prevention Active Rules 9693 Alert 473 Block 9219 Others 1

Base Policy → Group Overrides → Recommendations **Not in use** → **Rule Overrides** | Summary

**Rule Overrides** Back To Top

102 items All x v Rule Action Search by CVE, SID, Reference Info, or Rule Message

1 rule Presets: Alert ( 0 ) | Block ( 0 ) | Disabled ( 0 ) | **Overridden ( 1 )** | Advanced Filters | Reject ( 1 )

	GID:SID	Rule Details	Rule Action	Set By	Assigned Groups
>	1:28496	BROWSER-IE Microsoft Internet ...	Reject	Rule Override	Malicious File, Drive...

Regras Substituídas

## 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.