Configurar ações adicionais de regra do Snort 3 no FMC

Contents

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.

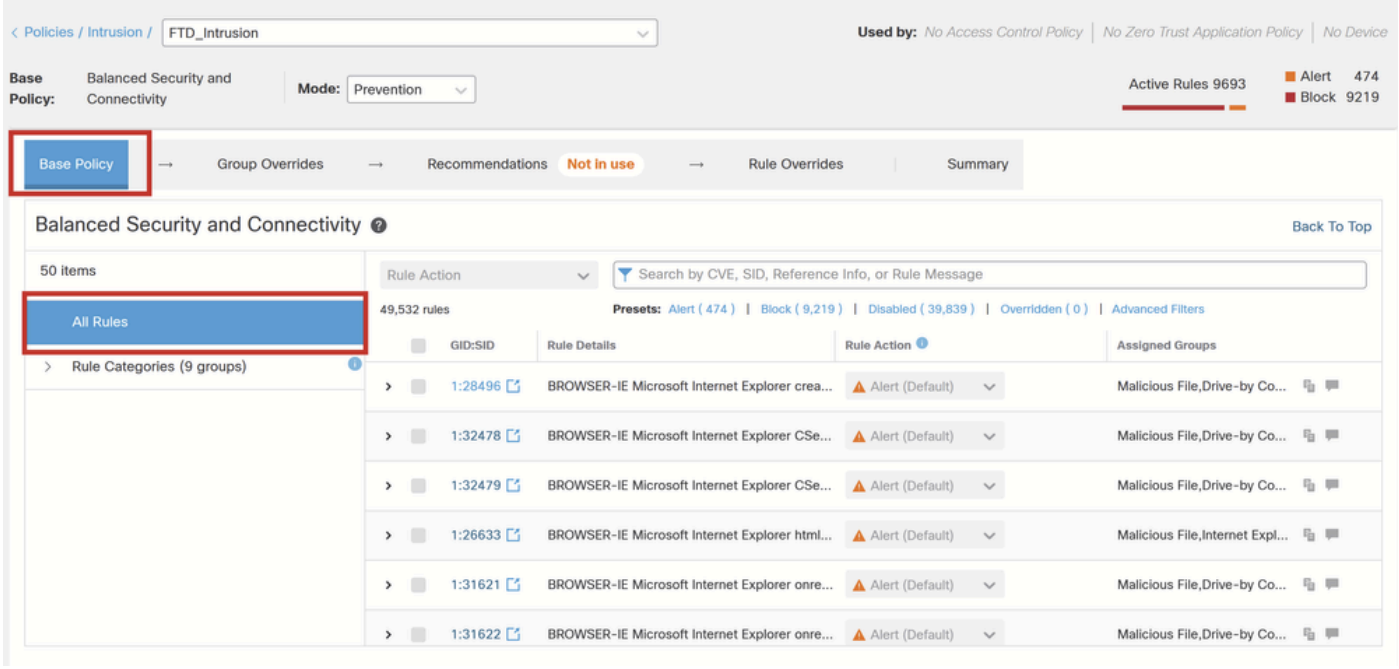
Reescrever: Gera eventos e sobregrava o conteúdo do pacote com base na opção de substituição na regra.

Passo a Passo do FMC

Para exibir as regras do Snort 3 em uma política de intrusão, navegue paraFMC Policies > Access Control > Intrusion,depois clique na opção Versão do Snort 3 no canto superior direito da política, como mostrado na imagem:

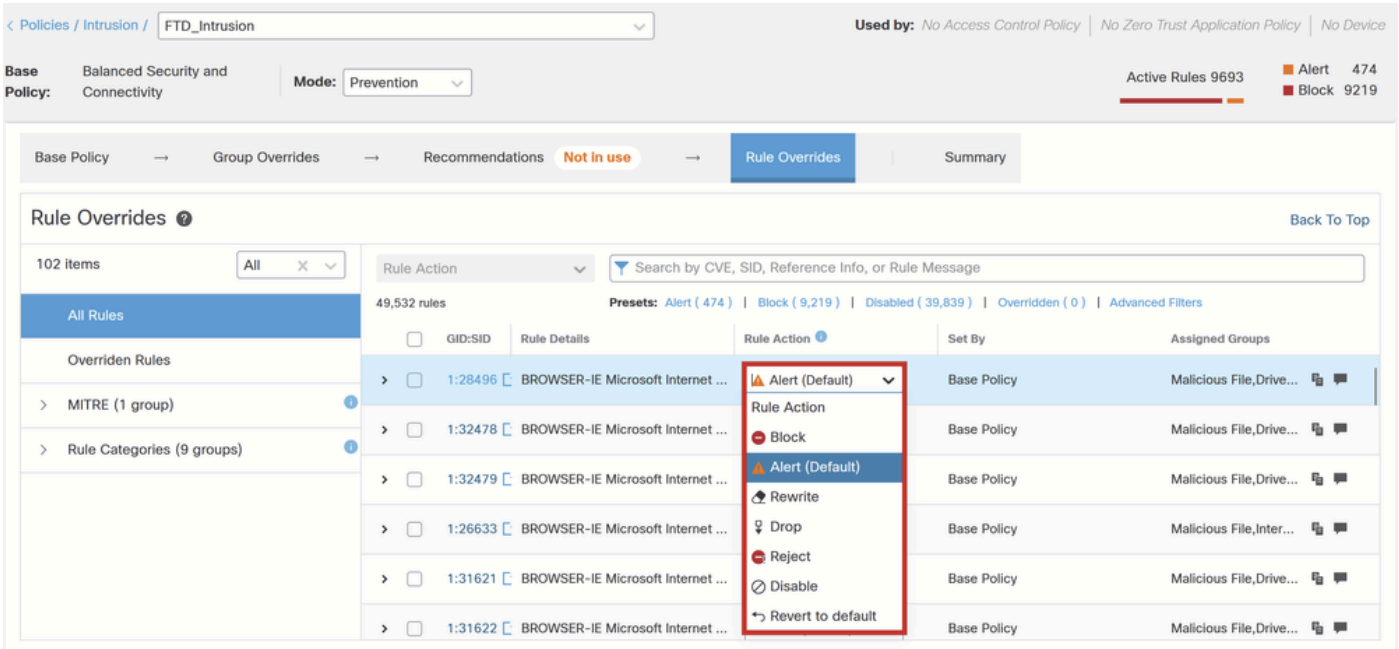
Versão do Snort 3

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

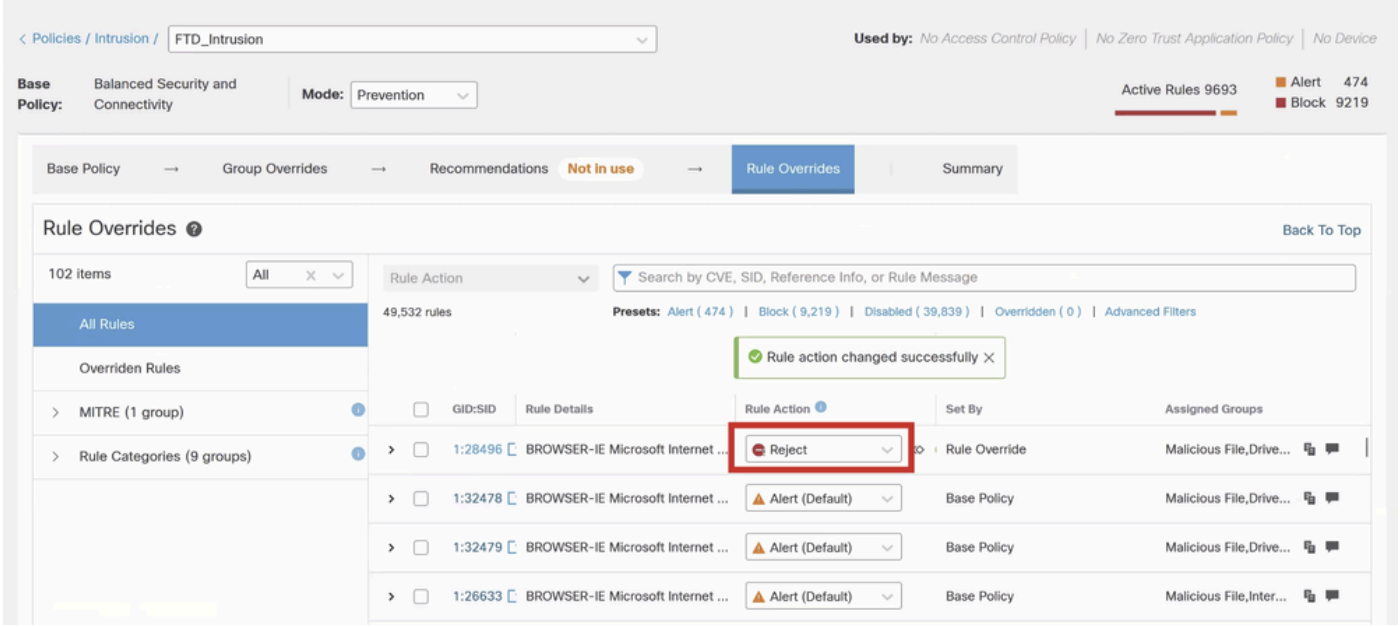


Política básica

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.

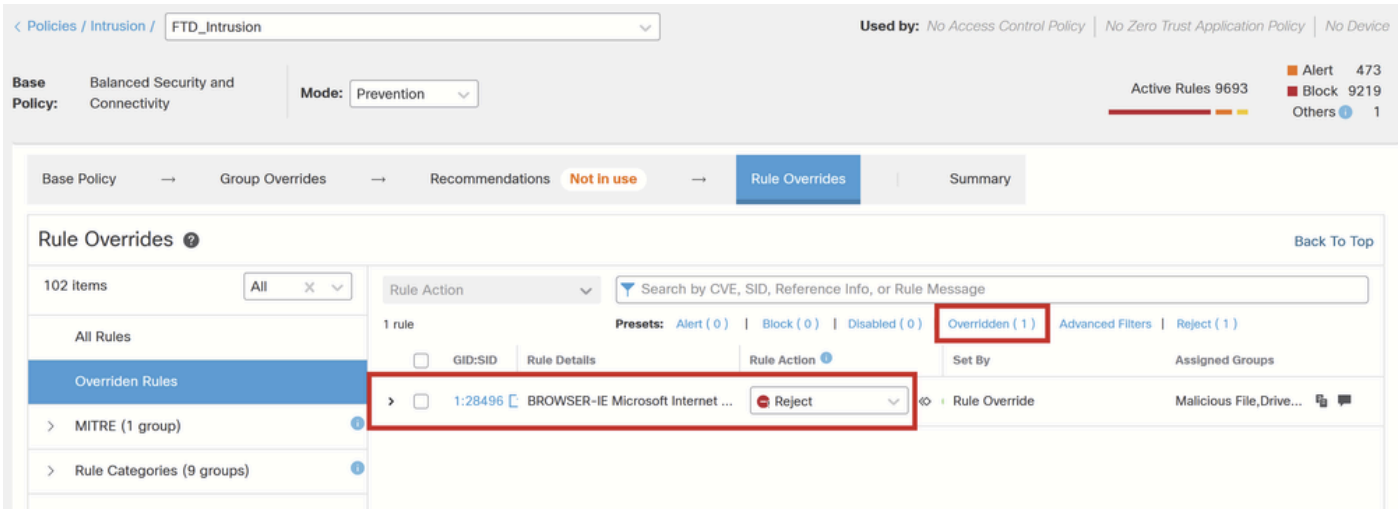


Ações de Regra Adicionais



Como alterar a ação da regra

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



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.