Filtrar regras de Snort com base nas versões SRU e LSP de dispositivos Firepower gerenciados pelo FMC

Contents

Introdução

Este documento descreve como filtrar regras de snort com base na versão Cisco Secure Rule Update (SRU) e Link State Packet (LSP) de dispositivos firepower gerenciados pelo Firepower Management Center (FMC).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

Componentes Utilizados

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

- Este artigo se aplica a todas as plataformas Firepower
- O Cisco Firepower Threat Defense (FTD), que executa a versão 7.0.0 do software
- Firepower Management Center Virtual (FMC) que executa a versão de software 7.0.0

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

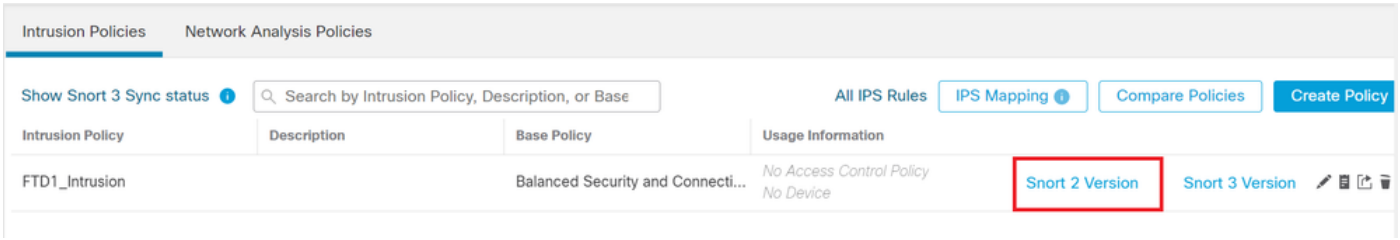
No contexto dos sistemas de detecção de intrusão (IDS) e sistemas de prevenção de intrusão (IPS), "SID" significa "ID de assinatura" ou "ID de assinatura Snort".

Um Snort Signature ID (SID) é um identificador exclusivo atribuído a cada regra ou assinatura dentro de seu conjunto de regras. Essas regras são usadas para detectar padrões ou comportamentos específicos no tráfego de rede que podem indicar atividade mal-intencionada ou ameaças à segurança. Cada regra é associada a um SID para permitir fácil referência e gerenciamento.

Para obter informações sobre o Snort de código aberto, visite o site do SNORT.

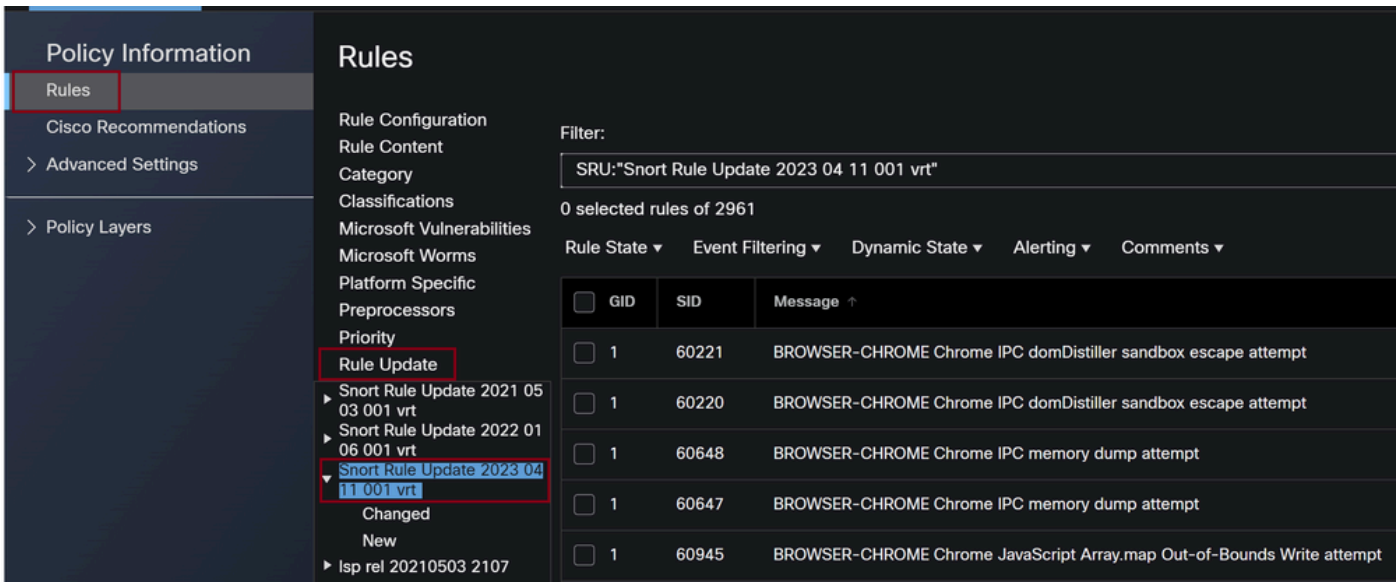
Procedimento para filtrar regras do Snort

Para exibir os SIDs de regra do Snort 2, navegue até FMC Policies > Access Control > Intrusion, em seguida, clique na opção SNORT2 no canto superior direito, conforme mostrado na imagem:

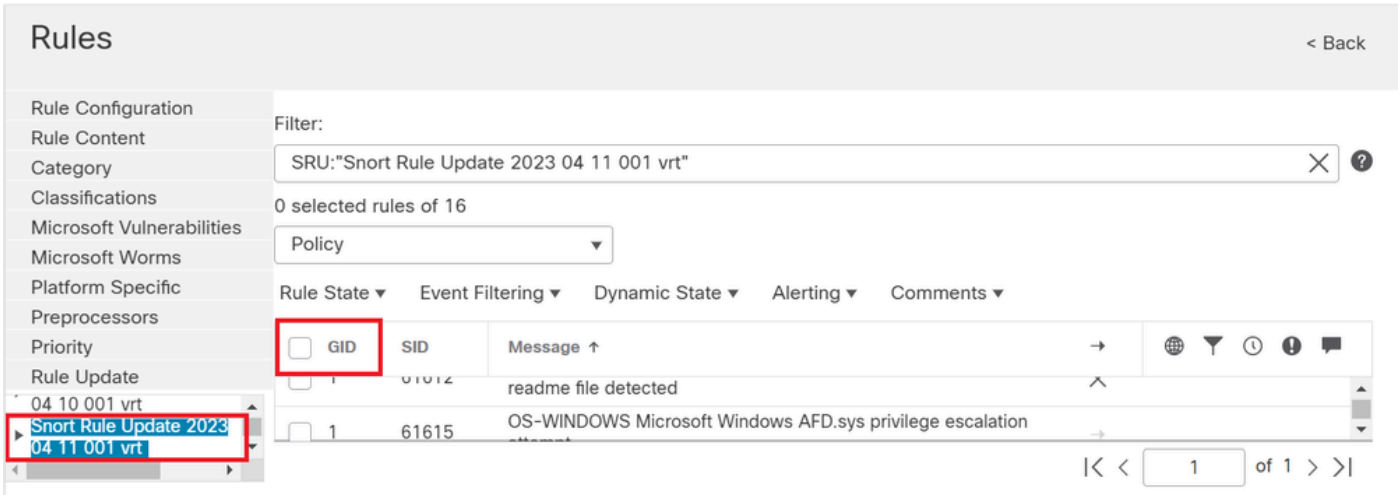


Snort 2

Navegue até Rules > Rule Update e selecione a data mais recente para filtrar o SID.

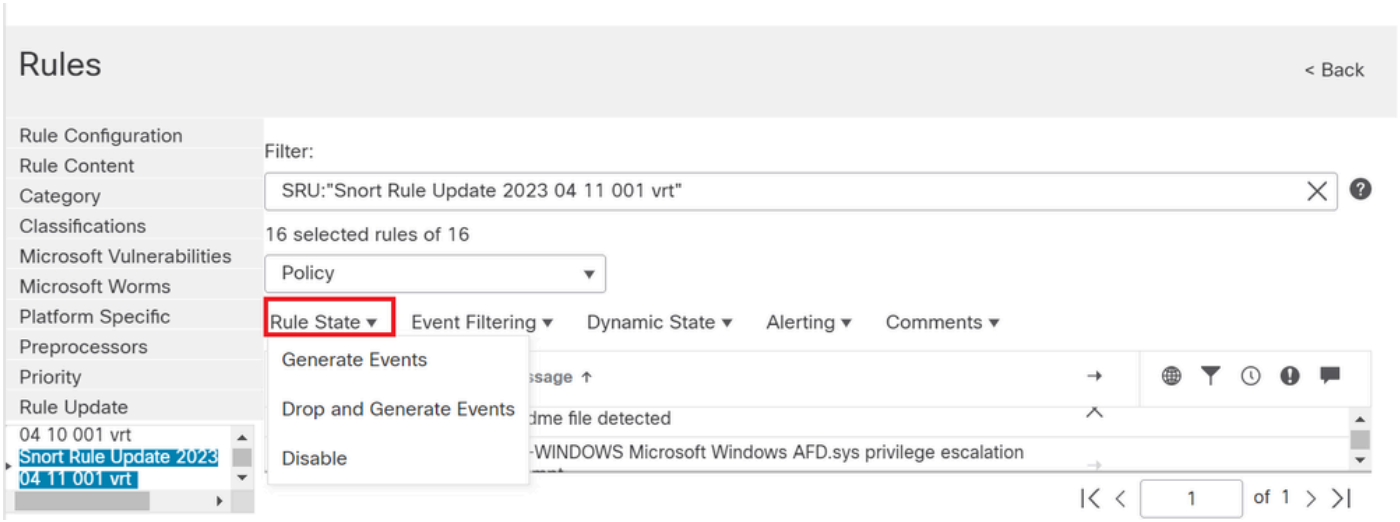


Atualização de regra



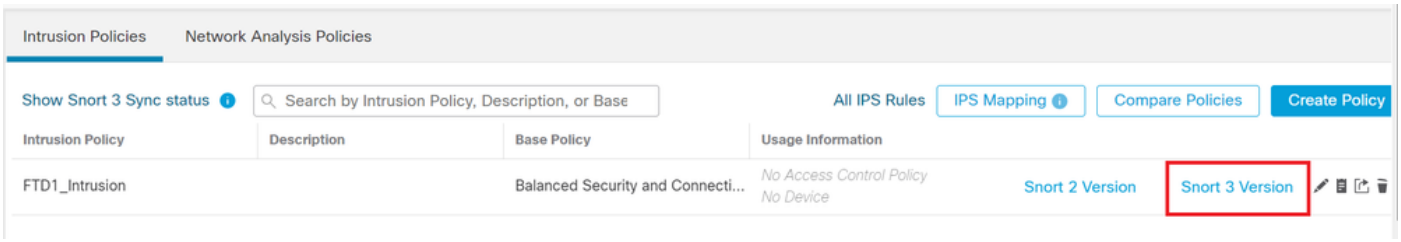
Sids disponíveis sob regras de snort

Selecione uma opção necessária em Rule State conforme mostrado na imagem.



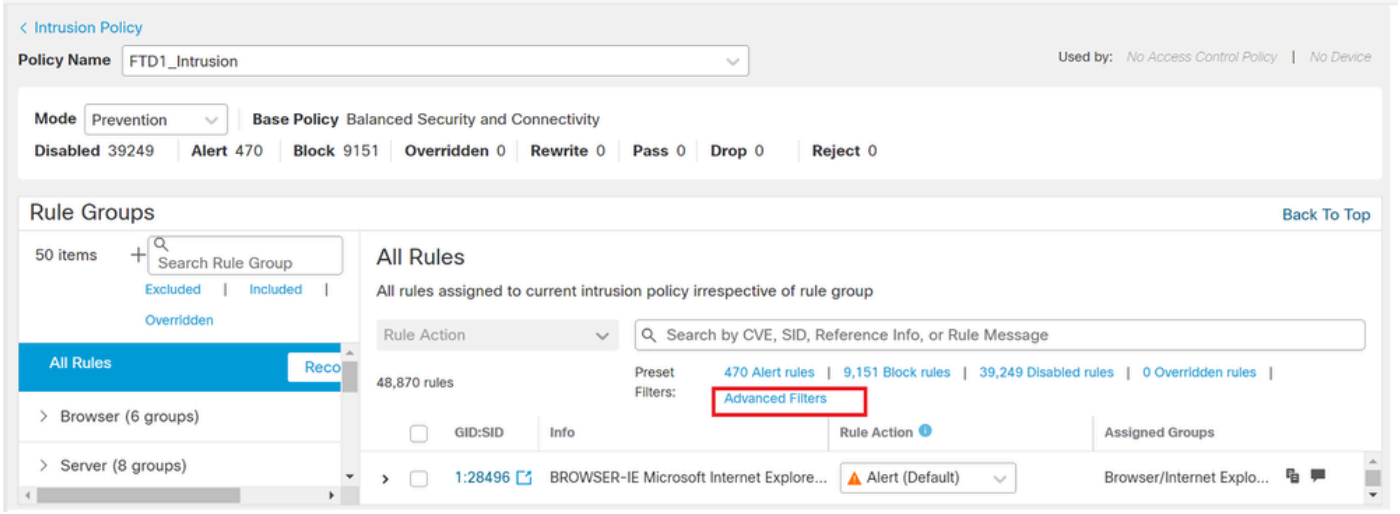
Seleção de estados de Regra

Para exibir os SIDs de regra do Snort 3, navegue até FMC Policies > Access Control > Intrusion e, em seguida, clique na opção SNORT3 no canto superior direito, conforme mostrado na imagem:

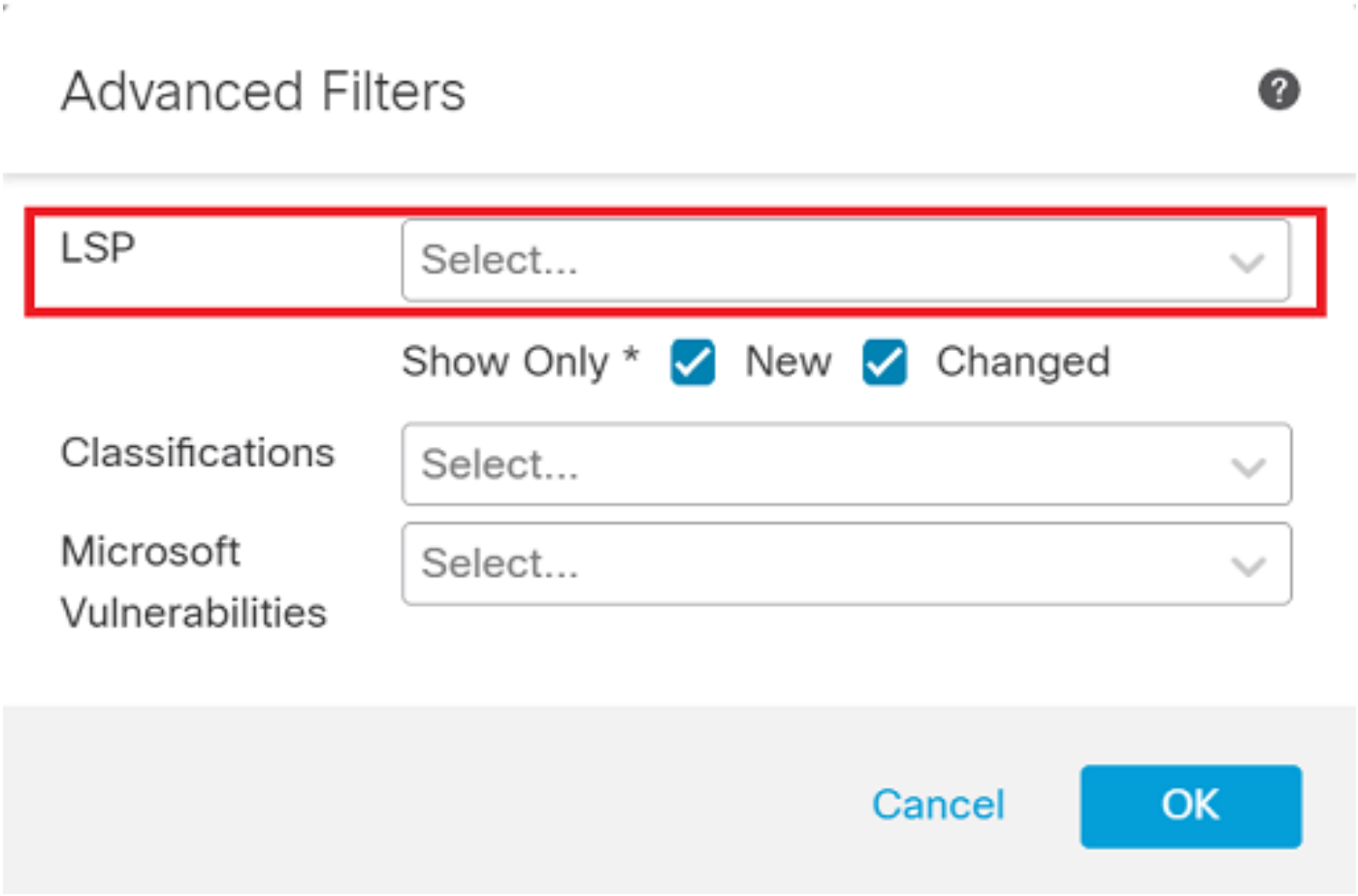


Snort 3

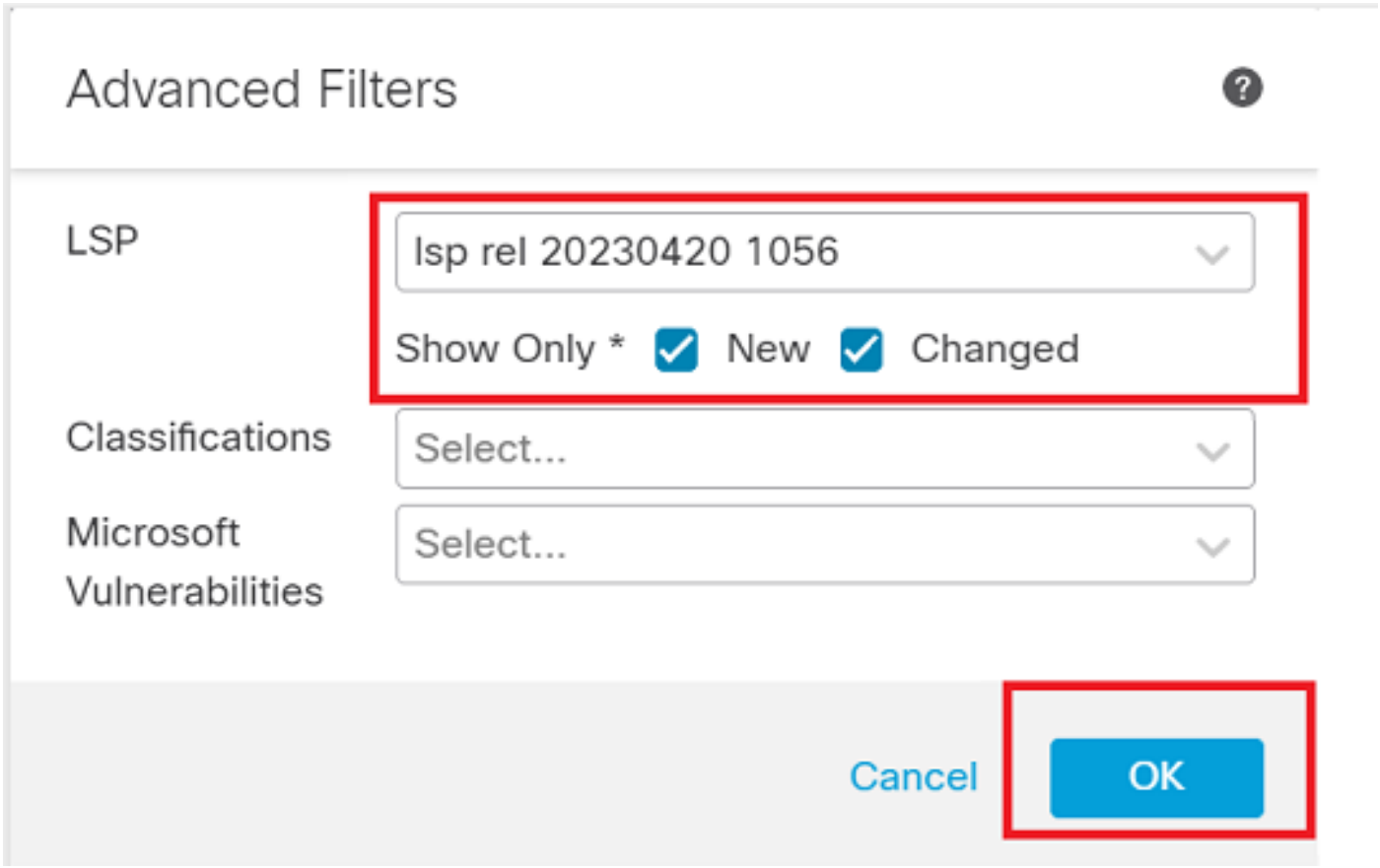
Navegue até Advanced Filters e selecione a data mais recente para filtrar o SID como mostrado na imagem.



3 filtros Snort



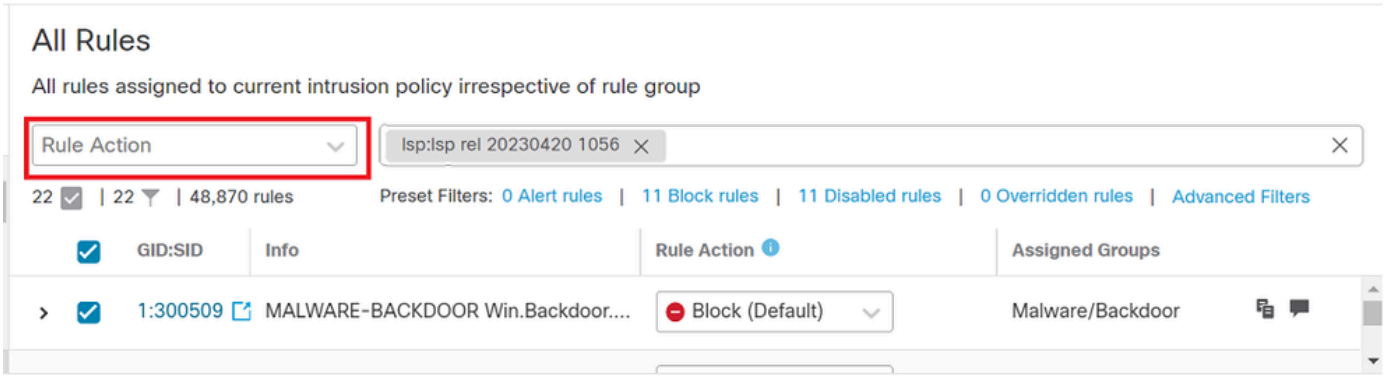
LSP no filtro avançado



versão de LSP

Filtro predefinido para Sid's

Selecione uma opção necessária em Rule state conforme mostrado na imagem.



Ação da regra

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.