Regras locais personalizadas de Snort em um sistema Cisco FireSIGHT

Contents

Introduction

Uma regra local personalizada em um sistema FireSIGHT é uma regra Snort padrão personalizada que você importa em um formato de arquivo de texto ASCII de uma máquina local. Um sistema FireSIGHT permite importar regras locais usando a interface da Web. As etapas para importar regras locais são muito simples. No entanto, para escrever uma regra local ideal, um usuário precisa de conhecimento profundo sobre o Snort e os protocolos de rede.

A finalidade deste documento é fornecer algumas dicas e ajuda para escrever uma regra local personalizada. As instruções sobre a criação de regras locais estão disponíveis no *Manual de usuários do Snort,* disponível em snort.org. A Cisco recomenda que você baixe e leia o Manual do usuário antes de escrever uma regra local personalizada.

> **Note**: As regras fornecidas em um pacote Sourcefire Rule Update (SRU) são criadas e testadas pelo Cisco Talos Security Intelligence and Research Group e têm suporte do Cisco Technical Assistance Center (TAC). O Cisco TAC não oferece assistência para escrever ou ajustar uma regra local personalizada. No entanto, se você tiver algum problema com a funcionalidade de importação de regras do seu sistema FireSIGHT, entre em contato com o Cisco TAC.

> **aviso:** Uma regra local personalizada mal escrita pode afetar o desempenho de um sistema FireSIGHT, o que pode levar à degradação do desempenho de toda a rede. Se você estiver tendo problemas de desempenho na rede e algumas regras locais personalizadas do Snort estiverem ativadas no sistema FireSIGHT, a Cisco recomenda que você desative essas regras locais.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento sobre as regras do Snort e o sistema FireSIGHT.

Componentes Utilizados

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

- O FireSIGHT Management Center (também conhecido como Defense Center)
- Versão do software 5.2 ou posterior

Como Trabalhar com as Regras Locais Personalizadas

Importar regras locais

Antes de começar, certifique-se de que as regras no arquivo não contenham caracteres de escape. O importador de regras requer que todas as regras personalizadas sejam importadas usando a codificação ASCII ou UTF-8.

O procedimento a seguir explica como importar regras de texto padrão locais de uma máquina local:

1. Acesse a página **Rule Editor** navegando para **Policies > Intrusion > Rule Editor**.

2. Clique em **Importar Regras**. A página **Atualizações de regras** é exibida.

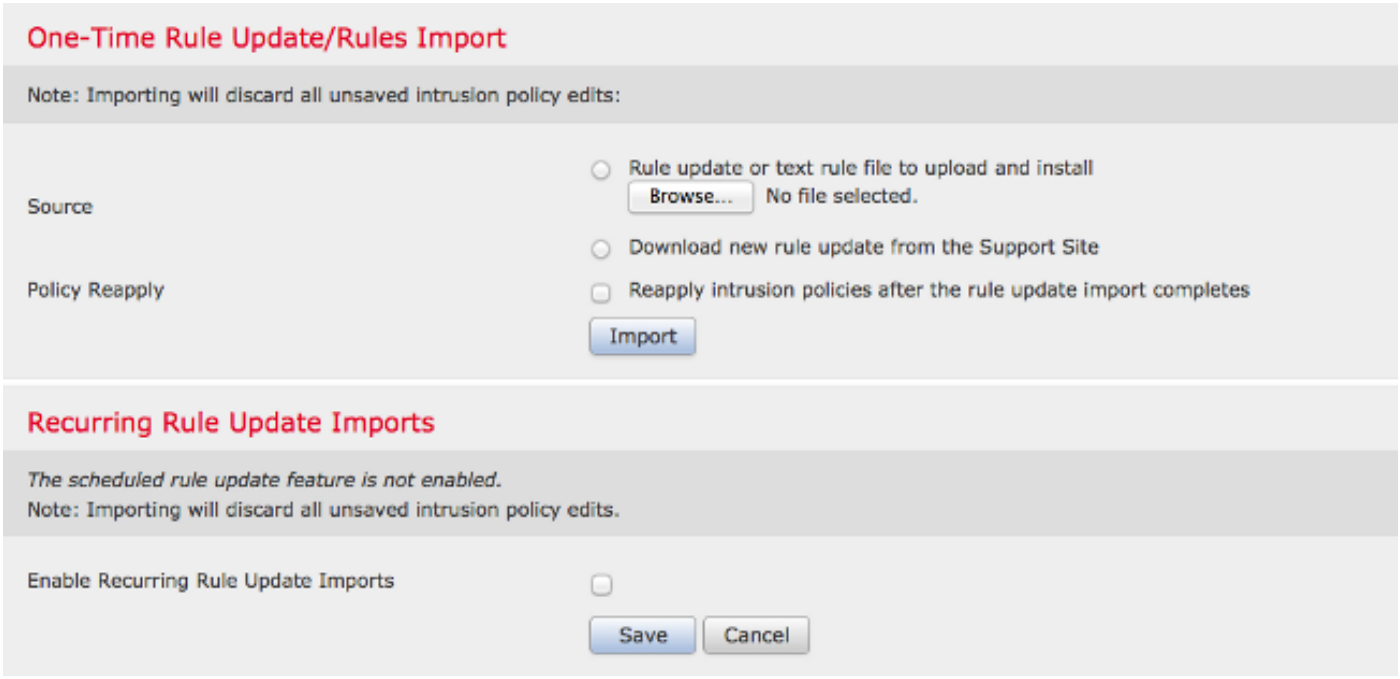


Figura: Uma captura de tela da página Atualizações de regras

3. Selecione **Atualização de regra ou arquivo de regra de texto para carregar e instalar** e clique em **Procurar** para selecionar o arquivo de regra.

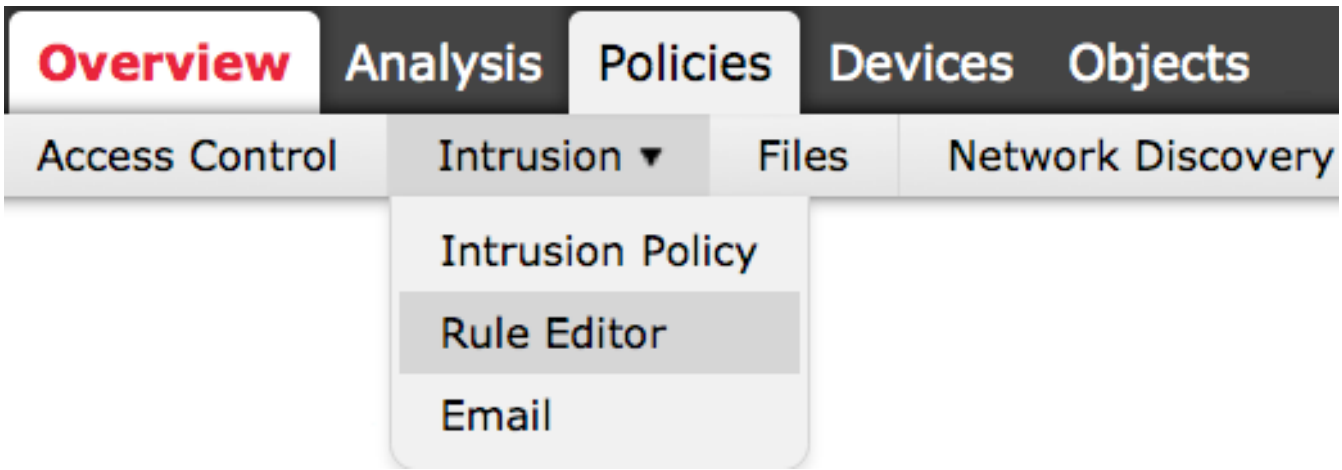
> **Note**: Todas as regras carregadas são salvas na categoria **regra local**.

4. Clique em **Importar**. O arquivo de regras é importado.

> **Caution**: Os sistemas FireSIGHT não usam o novo conjunto de regras para inspeção. Para ativar uma regra local, você precisa ativá-la na Política de intrusão e, em seguida, aplicar a política.

Exibir regras locais

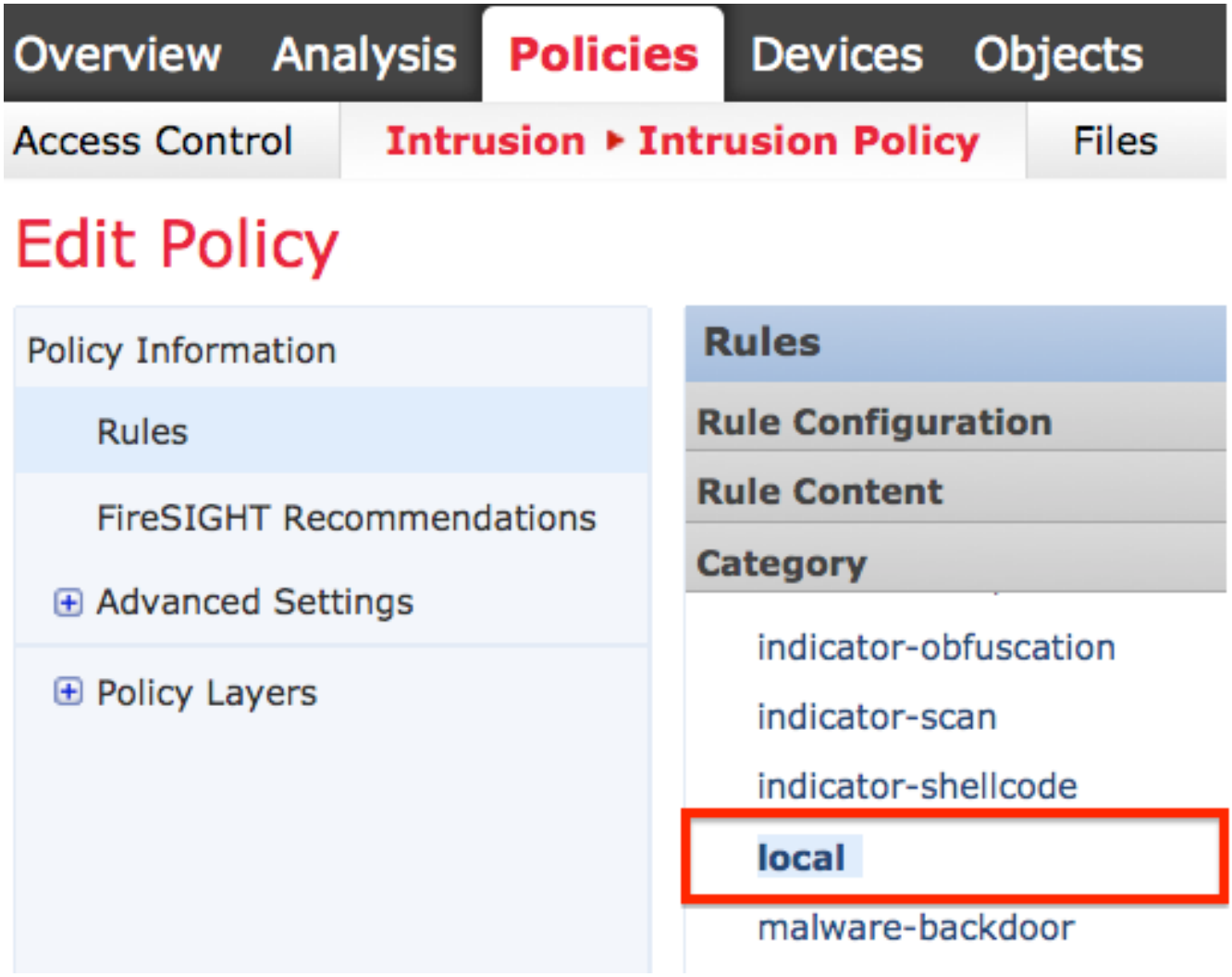
- Para exibir o número de revisão de uma regra local atual, navegue até a página **Editor de regras** (**Políticas** > **Intrusão** > **Editor de regras**).



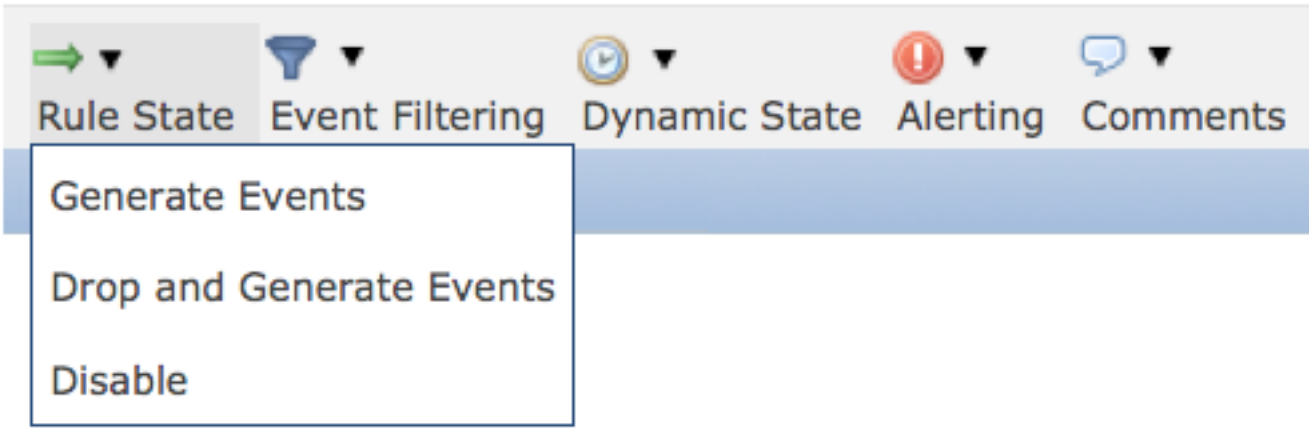
- Na página Editor de regras, clique na categoria **Regra local** para expandir a pasta e clique em **Editar** ao lado da regra.
- Todas as regras locais importadas são salvas automaticamente na categoria **regra local**.

Habilitar regras locais

- Por padrão, o sistema FireSIGHT define as regras locais em um estado desativado. Você deve definir manualmente o estado das regras locais antes de usá-las na política de intrusão.
- Para habilitar uma regra local, navegue até a página Policy Editor (**Policies** > **Intrusion** > **Intrusion Policy**). Selecione **Rules** no painel esquerdo. Em **Categoria**, selecione **local**. Todas as regras locais devem ser exibidas, se disponíveis.



- Depois de selecionar as regras locais desejadas, selecione um estado para as regras.



- Quando o estado da regra for selecionado, clique na opção **Policy Information** no painel esquerdo. Selecione o botão **Confirmar alterações**. A política de intrusão é validada.

  Note: A validação da política falhará se você habilitar uma regra local importada que use a palavra-chave de limite preterida em combinação com o recurso de limite de evento de intrusão em uma política de intrusão.

Exibir as regras locais excluídas

- Todas as regras locais excluídas são movidas da categoria de regra local para a categoria de regra excluída.
- Para exibir o número de revisão de uma regra local excluída, vá para a página **Editor de regras**, clique na categoria **excluído** para expandir a pasta e, em seguida, clique no ícone do **lápis** para exibir os detalhes da regra na página **Editor de regras**.

Numeração das regras locais

- Você não precisa especificar um Gerador (GID); se fizer isso, você poderá especificar apenas GID 1 para uma regra de texto padrão ou 138 para uma regra de dados confidenciais.
- Não especifique um Snort ID (SID) ou número de revisão ao importar uma regra pela primeira vez; isso evita colisões com SIDs de outras regras, inclusive regras excluídas.
- O FireSIGHT Management Center atribui automaticamente o próximo SID de regra personalizada disponível de 1000000 ou maior e um número de revisão 1.
- Se você tentar importar uma regra de intrusão com um SID maior que 2147483647, ocorrerá um erro de validação.
- Você deve incluir o SID atribuído pelo IPS e um número de revisão maior que o número de revisão atual ao importar uma versão atualizada de uma regra local que você tenha importado anteriormente.
- Você pode restabelecer uma regra local que tenha excluído importando a regra usando o SID atribuído pelo IPS e um número de revisão maior que o número de revisão atual. Observe que o FireSIGHT Management Center incrementa automaticamente o número de revisão quando você exclui uma regra local; este é um dispositivo que permite restabelecer regras locais.

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.

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.