Regras locais do Snort do costume em um sistema de Cisco FireSIGHT

Índice

Introdução

Uma regra local feita sob encomenda em um sistema de FireSIGHT é uma regra padrão feita sob encomenda do Snort que você importe em um formato de arquivo de texto ascii de uma máquina local. Um sistema de FireSIGHT permite que você importe regras locais usando a interface da WEB. As etapas para importar regras locais são muito diretas. Contudo, para escrever uma regra local ótima, um usuário exige o conhecimento aprofundado no Snort e nos protocolos de rede.

A finalidade deste documento é fornecê-lo alguns pontas e auxílio escrever uma regra local feita sob encomenda. As instruções em criar regras locais estão disponíveis no *manual dos usuários do Snort,* que está disponível em snort.org. Cisco recomenda que você transfere e lê os usuários manuais antes que você escreva uma regra local feita sob encomenda.

> Nota: As regras fornecidas em um pacote da atualização da regra de Sourcefire (SRU) são criadas e testadas pela inteligência e pelo grupo de investigação de Segurança de Cisco Talos, e apoiadas pelo centro de assistência técnica da Cisco (TAC). O tac Cisco não fornece o auxílio na escrita ou em ajustar uma regra local feita sob encomenda, contudo se você experimenta quaisquer edições com a funcionalidade da importação da regra de seu sistema de FireSIGHT, contacte por favor o tac Cisco.

> **aviso:** Um costume deficientemente escrito regra local pode impactar o desempenho de um sistema de FireSIGHT que possa conduzir à degradação do desempenho da toda a rede. Se você está experimentando quaisquer problemas de desempenho em sua rede, e há algumas regras locais feitas sob encomenda do Snort permitidas em seu sistema de FireSIGHT, Cisco recomenda-o desabilitar aquelas regras locais.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento em regras do Snort e no sistema de FireSIGHT.

Componentes Utilizados

A informação neste documento é baseada nestes versão de hardware e software:

- O centro de gerenciamento de FireSIGHT (igualmente conhecido como o centro da defesa)
- Versão de software 5.2 ou mais atrasado

Trabalho com as regras locais feitas sob encomenda

Regras do Local da importação

Antes que você comece, você deve certificar-se de que as regras no arquivo não contêm nenhuns caracteres de escape. O importador da regra exige todas as regulamentações aduaneiras ser importado usando a codificação ASCII ou de UTF-8.

O seguinte procedimento explica como importar regras padrão locais do texto de uma máquina local:

1. Alcance a página do **editor da regra** navegando às **políticas > ao editor da intrusão > da regra**.

2. Clique **regras de importação**. A página das **atualizações da regra** publica-se.

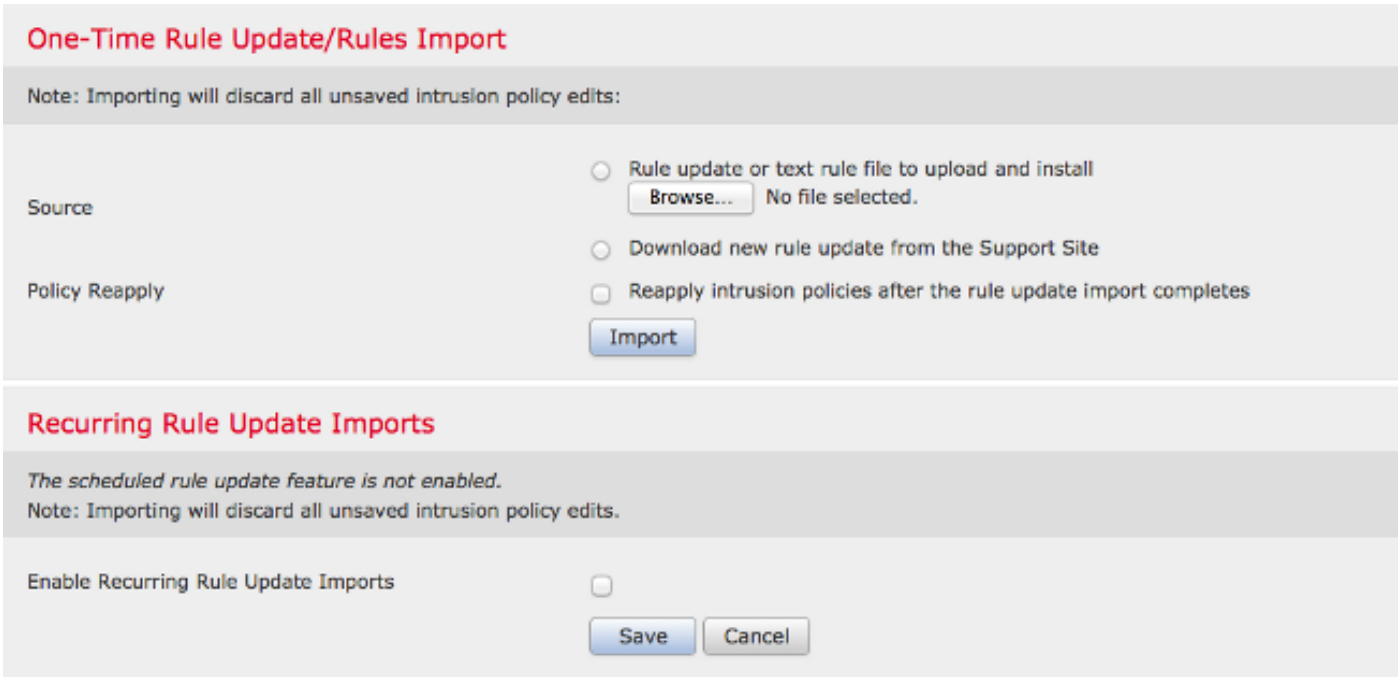


Figura: Um tiro de tela da regra atualiza a página

3. Selecione a **atualização da regra ou o arquivo da regra do texto a transferir arquivos pela rede e instalar** e o clique **consultam** para selecionar o arquivo da regra.

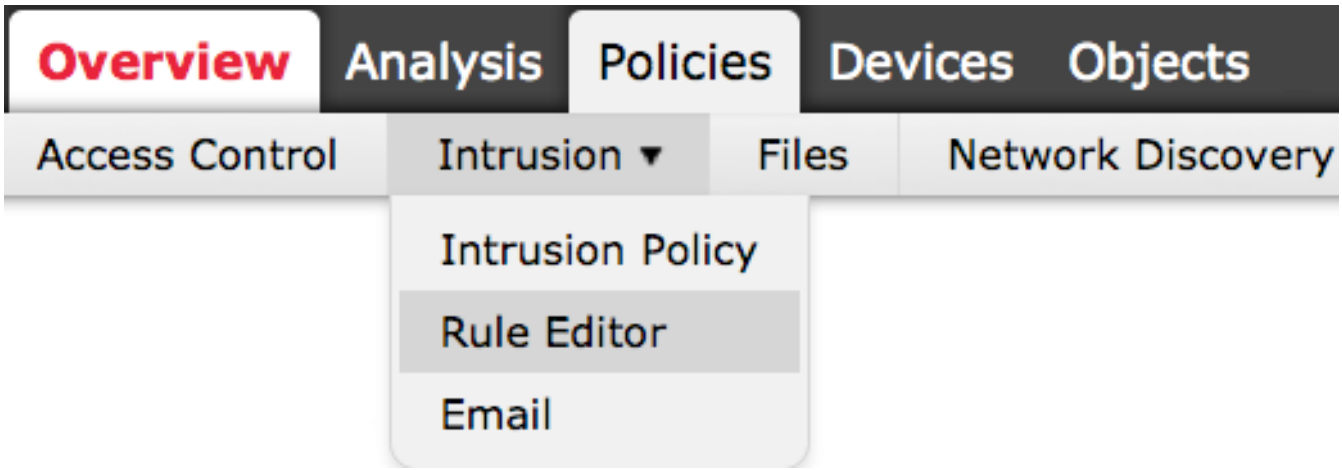
> Nota: Todas as regras transferidas arquivos pela rede salvar na categoria **local da regra**.

4. **Importação do** clique. O arquivo da regra é importado.

> Cuidado: Os sistemas de FireSIGHT não usam a regra nova ajustada para a inspeção. Para ativar uma regra local, você precisa de permiti-la na política da intrusão, e aplica então a política.

Regras do Local da vista

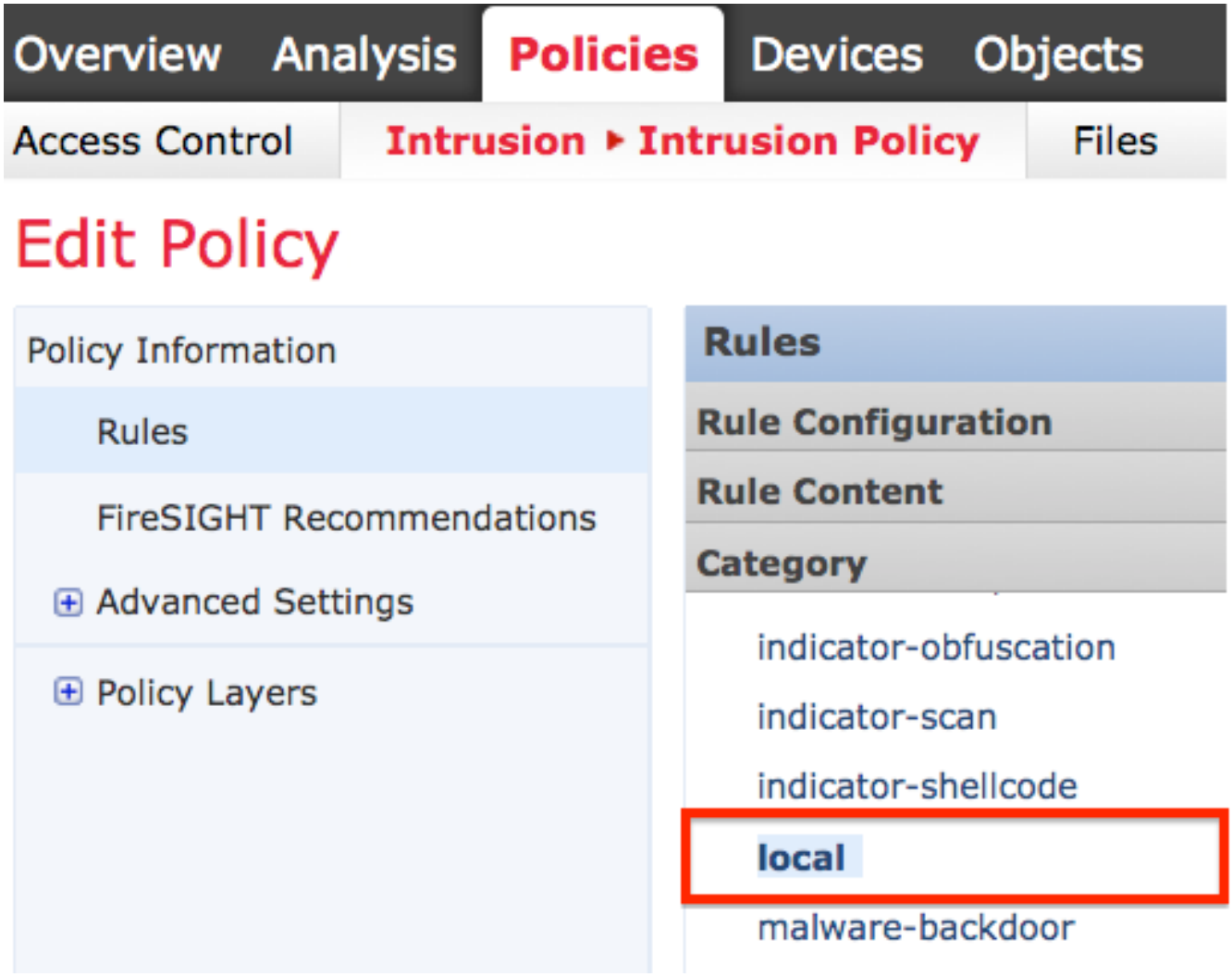
- Para ver o número de revisão para uma regra local atual, navegue à página do **editor da regra** (**políticas > editor da intrusão >** da **regra**).



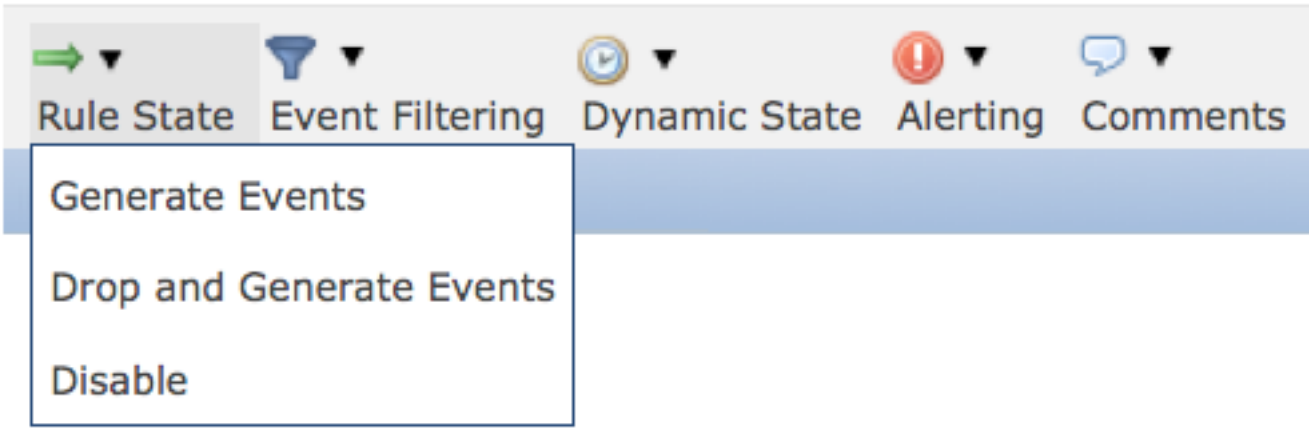
- Na página do editor da regra, clique sobre a categoria **local da regra** para expandir o dobrador, a seguir clique-a **editam** ao lado da regra.
- Todas as regras locais importadas salvar automaticamente na categoria **local da regra**.

Permita regras locais

- Àrevelia, o sistema de FireSIGHT ajusta as regras locais em um estado desabilitado. Você deve manualmente ajustar o estado de regras locais antes que você possa as usar em sua política da intrusão.
- A fim permitir uma regra local, navegue à página do editor de política (**políticas > intrusão > política da intrusão**). Selecione **regras no** painel esquerdo. Sob a **categoria**, selecione o **local**. Todas as regras locais devem aparecer, se disponíveis.



- Após ter selecionado as regras locais desejadas, selecione um estado para as regras.



- Uma vez que o estado da regra é selecionado, clique sobre a opção da **informação sobre a política no** painel esquerdo. Selecione o botão das **mudanças comprometer**. A política da intrusão é validada.

  Nota: A validação da política falha se você permite uma regra local importada que use a palavra-chave suplicada do ponto inicial em combinação com a característica do limiar do evento da intrusão em uma política da intrusão.

Veja as regras locais suprimidas

- Todas as regras locais suprimidas são movidas da categoria local da regra para a categoria suprimida da regra.
- Para ver o número de revisão de uma regra local suprimida, vá à página do **editor da regra**, clique sobre a categoria **suprimida** para expandir o dobrador, a seguir clique o ícone do *lápis* para ver o detalhe da regra na página do **editor da regra**.

Numeração das regras locais

- Você não tem que especificar um gerador (GID); se você faz, você pode especificar somente GID 1 para uma regra padrão do texto ou 138 para uns dados sensíveis ordenam.
- Não especifique um Snort ID (SID) ou o número de revisão ao importar uma regra pela primeira vez; isto evita colisões com os SID de outras regras, incluindo regras suprimidas.
- O centro de gerenciamento de FireSIGHT atribui automaticamente a regulamentação aduaneira disponível seguinte SID de 1000000 ou maior, e um número de revisão de 1.
- Se você tenta importar uma regra da intrusão com SID maior de 2147483647, um erro de validação ocorrerá.
- Você deve incluir SID atribuído pelo IPS e um número de revisão maior do que o número de revisão atual ao importar uma versão actualizado de uma regra local que você importe previamente.
- Você pode restabelecer uma regra local de que você suprima importando a regra usando SID atribuído pelo IPS e um número de revisão maior do que o número de revisão atual. Note que o centro de gerenciamento de FireSIGHT incrementa automaticamente o número de revisão quando você suprimir de uma regra local; este é um dispositivo que permita que você restabeleça regras locais.