Verifique uma lista SID personalizada dos sensores Firepower usando CLI e FMC GUI

Introduction

Este documento descreve como obter uma lista SID personalizada do Firepower Threat Defense (FTD) ou do módulo FirePOWER usando CLI e FMC GUI. As informações de SID podem ser encontradas na GUI do FMC se você navegar para ***Objetos > Regras de intrusão***. Em alguns casos, é necessário obter uma lista de SIDs disponíveis na CLI.

Prerequisites

Requirements

A Cisco recomenda que você conheça estes tópicos:

- Cisco Firepower Threat Defense (FTD)
- Cisco ASA com Serviços FirePOWER
- Cisco Firepower Management Center (FMC)
- conhecimento básico do Linux

Componentes Utilizados

As informações neste documento são baseadas na seguinte versão de software:

- Firepower Management Center 6.6.0
- Firepower Threat Defense 6.4.0.9
- Módulo FirePOWER 6.2.3.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Uma ***regra de intrusão*** é um conjunto de palavras-chave e argumentos que o sistema usa para detectar tentativas de explorar vulnerabilidades na sua rede. À medida que o sistema analisa o tráfego de rede, ele compara pacotes com as condições especificadas em cada regra. Se os dados do pacote corresponderem a todas as condições especificadas em uma regra, a regra será acionada. Se uma regra for uma regra de alerta, ela gerará um evento de invasão. Se for uma regra de passagem, ela ignora o tráfego. Para uma regra de queda em uma implantação em linha, o sistema descarta o pacote e gera um evento. Você pode visualizar e avaliar eventos de invasão no console da Web do Firepower Management Center.

O sistema Firepower oferece dois tipos de regras de intrusão: ***regras de objeto compartilhado*** e ***regras de texto padrão***. O Cisco Talos Security Intelligence and Research Group (Talos) pode usar regras de objeto compartilhado para detectar ataques contra vulnerabilidades de maneiras

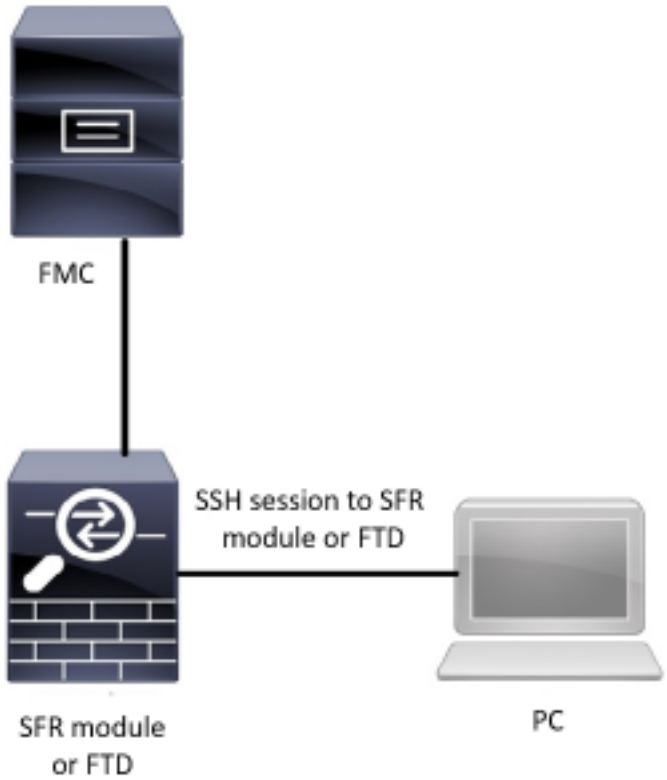
que as regras de texto padrão tradicionais não podem. Não é possível criar regras de objeto compartilhado. Quando as regras de intrusão são são são escritas por si, a regra de texto padrão deve ser criada. Regras de texto padrão personalizadas para ajustar os tipos de eventos que você provavelmente verá. Ao escrever regras e especificar a mensagem de evento da regra, você pode identificar mais facilmente o tráfego que indica ataques e evasões de política.

Ao habilitar uma regra de texto padrão personalizada em uma política de invasão personalizada, lembre-se de que algumas palavras-chave e argumentos de regra exigem que o tráfego seja decodificado ou pré-processado primeiro de uma certa maneira.

Uma *regra local personalizada* em um sistema Firepower é uma regra de Snort padrão personalizada que você importa em um formato de arquivo de texto ASCII de uma máquina local. Um sistema Firepower 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 exige conhecimento profundo do Snort e dos protocolos de rede.

> **aviso:** Certifique-se de usar um ambiente de rede controlado para testar as regras de intrusão que você escreve antes de usar as regras em um ambiente de produção. Regras de invasão mal escritas podem afetar seriamente o desempenho do sistema

Diagrama de Rede



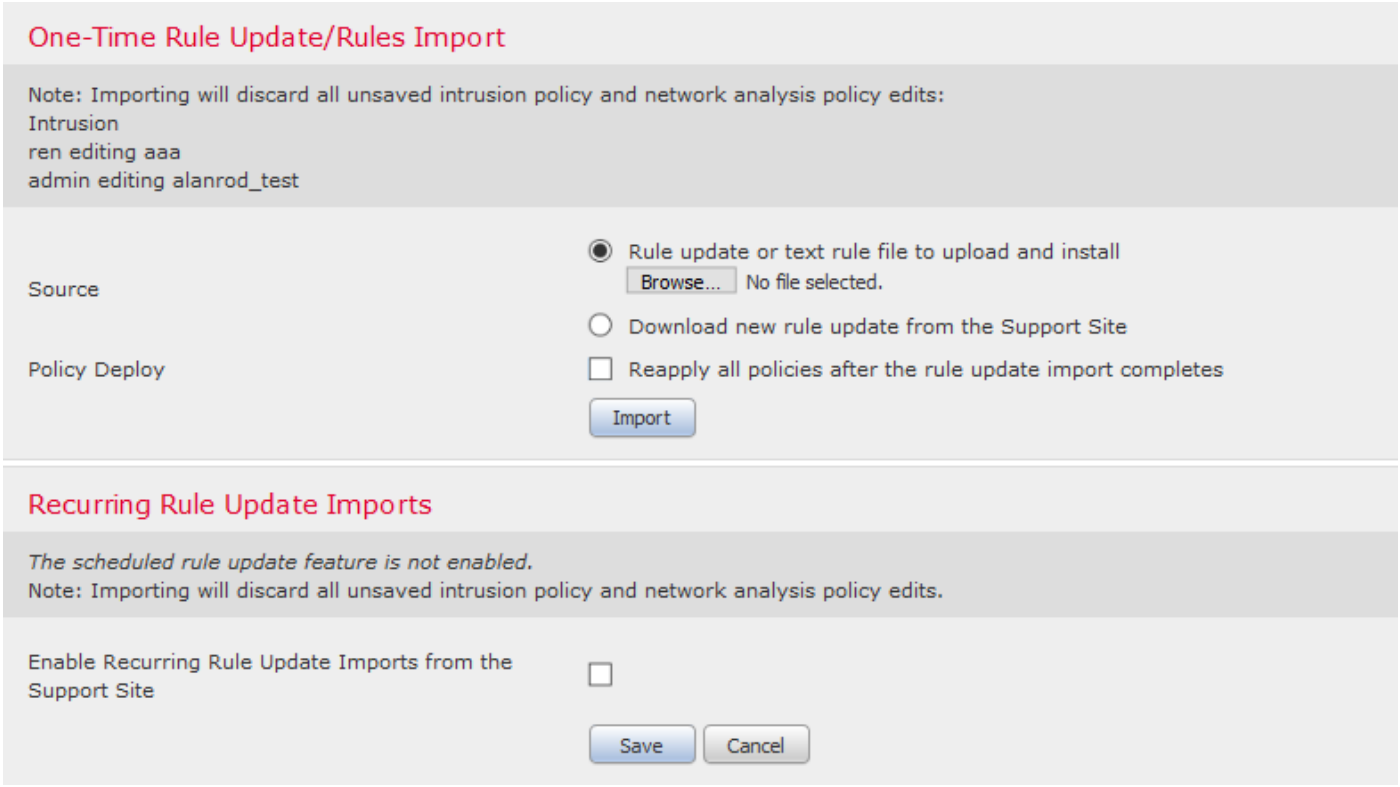
Configurar

Importar regras locais

Antes de começar, é necessário certificar-se de que as regras listadas no seu arquivo personalizado não contêm caracteres especiais. O importador de regras exige que todas as

regras personalizadas sejam importadas usando a codificação ASCII ou UTF-8. O procedimento mostrado abaixo explica como importar regras de texto padrão local de uma máquina local.

Etapa 1. Acesse a guia **Import Rules** navegando para **Objects > Intrusion Rules > Import Rules.** A página **Rule Updates** é exibida conforme mostrado na imagem abaixo:



Etapa 2. Selecione o **arquivo de regra de texto ou atualização de regra de texto a ser carregado e instalado** e clique em **Procurar** para selecionar o arquivo de regra personalizada

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

Etapa 3. Clique em **Importar**. O arquivo de regra é importado

> **Observação**: os sistemas Firepower não usam o novo conjunto de regras para inspeção. Para ativar uma regra local, é necessário ativá-la na Política de intrusão e, em seguida, aplicar a política.

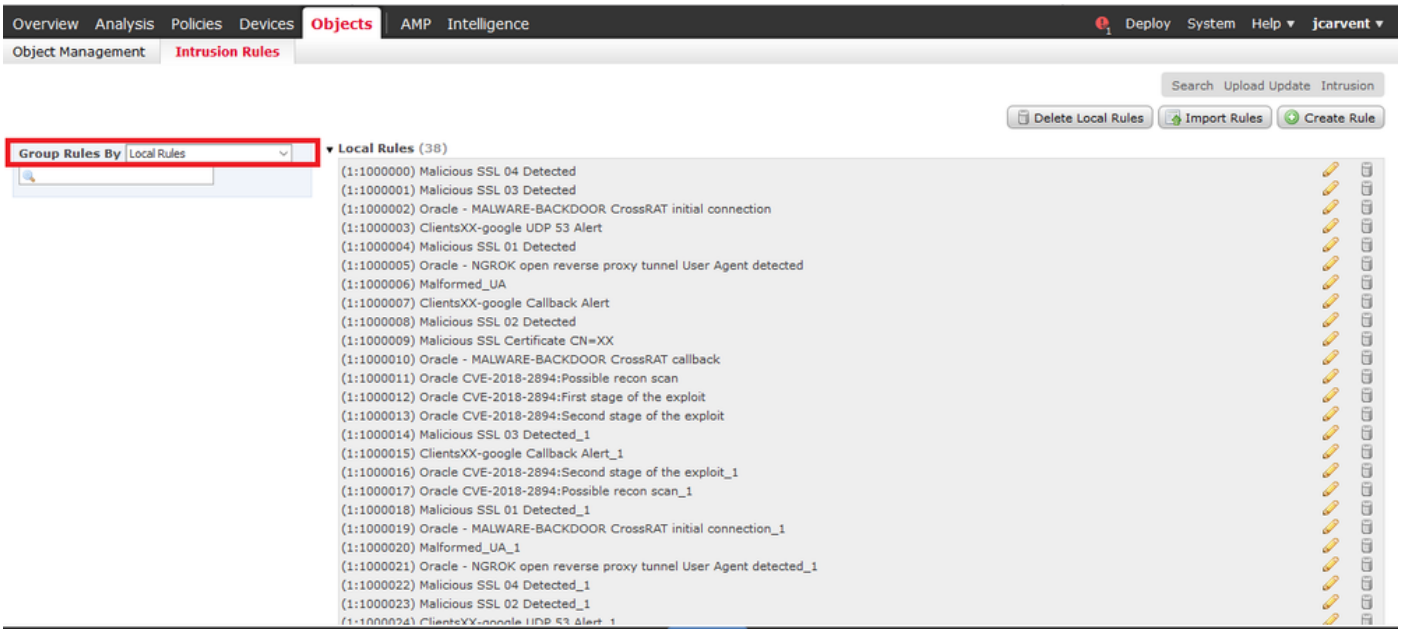
Verificar

na GUI do FMC

1. Exibir regras locais importadas da GUI do FMC

Etapa 1. Navegue até **Objetos > Regras de intrusão**

Etapa 2. Selecionar **Regras Locais** nas **Regras do Grupo**



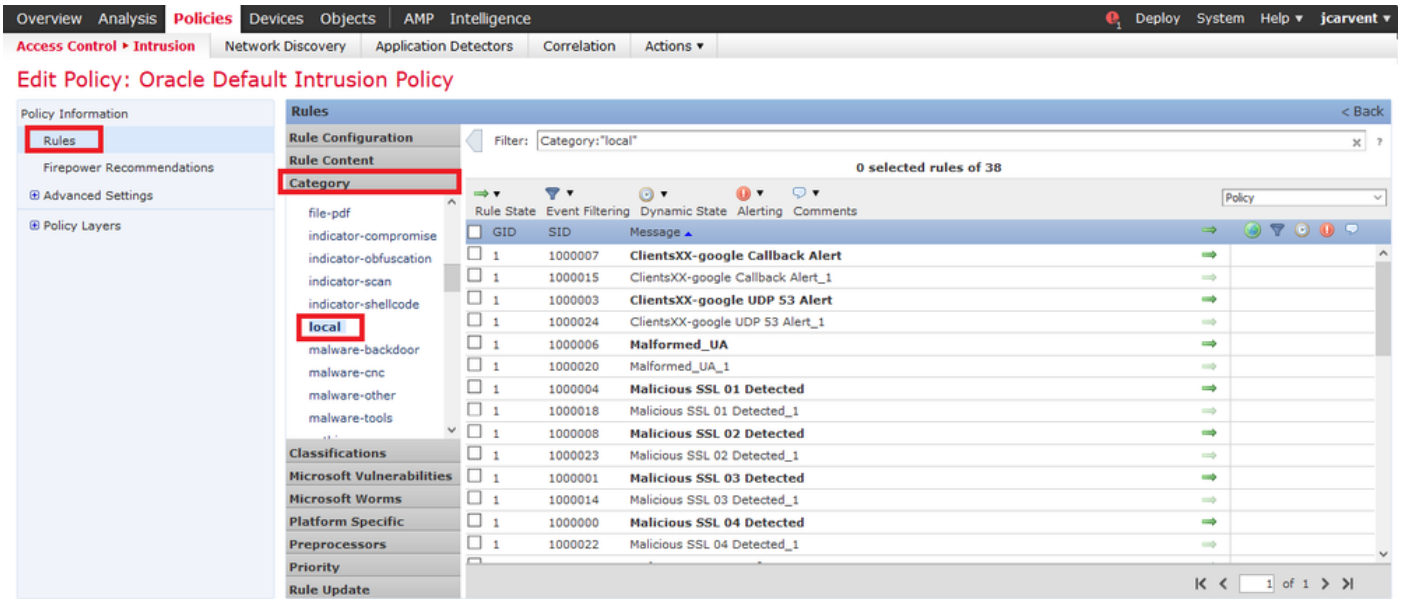
Por padrão, o sistema Firepower define as regras locais em um estado desabilitado. Essas regras locais devem definir manualmente o estado das regras locais para que você possa usá-las em sua política de invasão.

2. Ativar uma regra local a partir da Política de intrusão

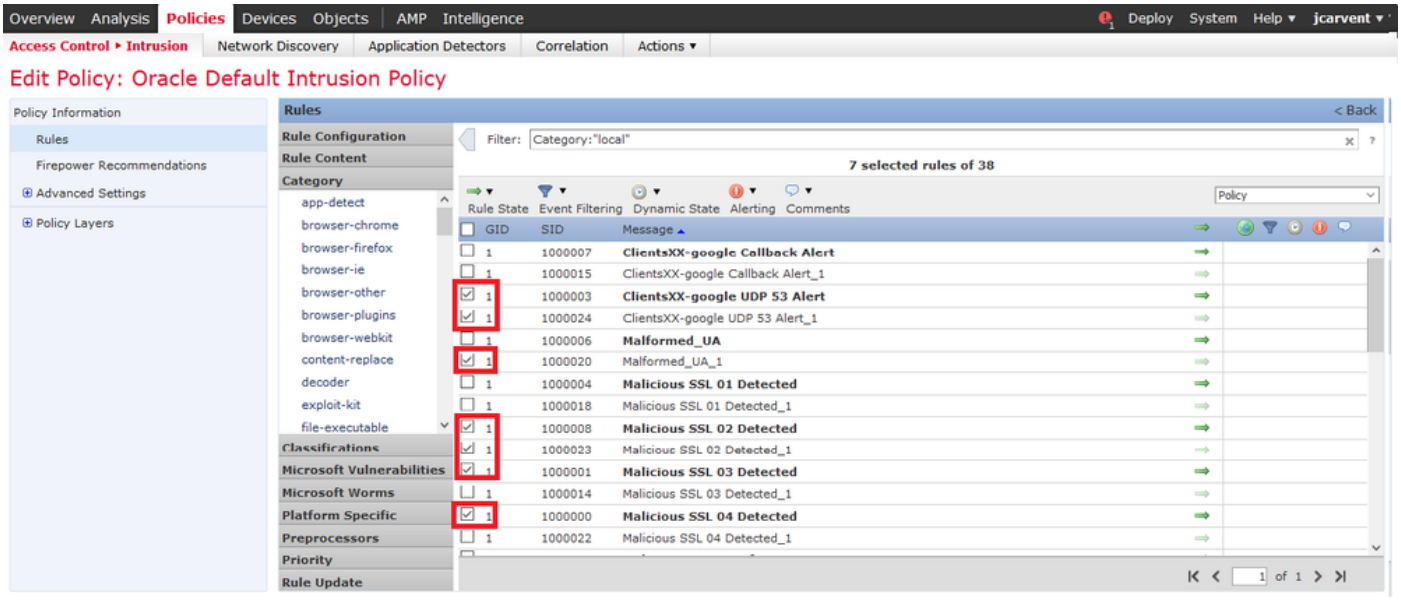
Etapa 1. Navegue até a página Editor de políticas em **Políticas > Intrusão > Política de intrusão**

Etapa 2. Selecione **Regras** no painel esquerdo

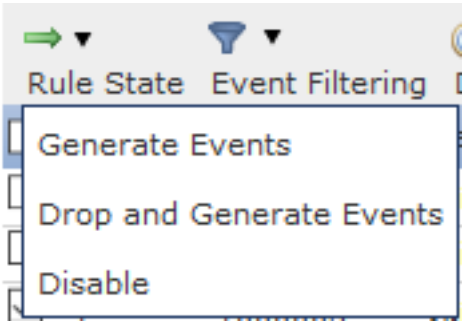
Etapa 3. Em **Categoria**, selecione **local.** Todas as regras locais devem aparecer, se disponíveis:



Etapa 4. Selecione as regras locais desejadas:



Etapa 5. Depois de selecionar as regras locais desejadas, selecione um estado em **Estado da regra**



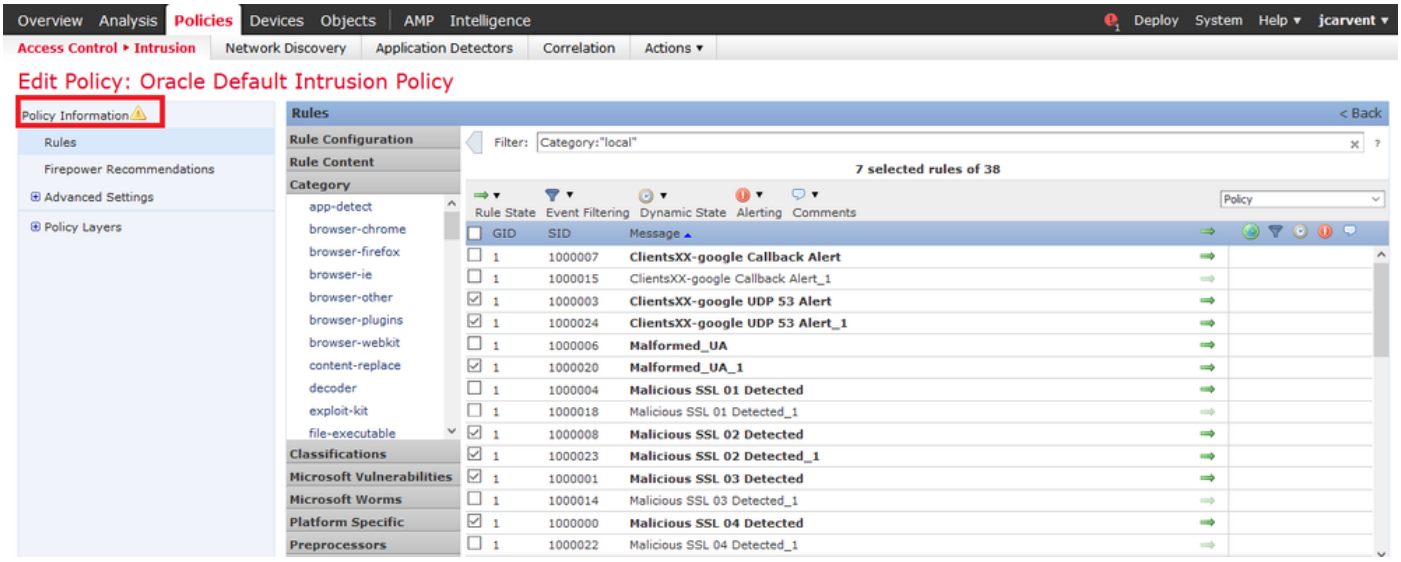
As seguintes operações estão disponíveis:

- Gerar eventos: Ativar a regra e gerar um evento

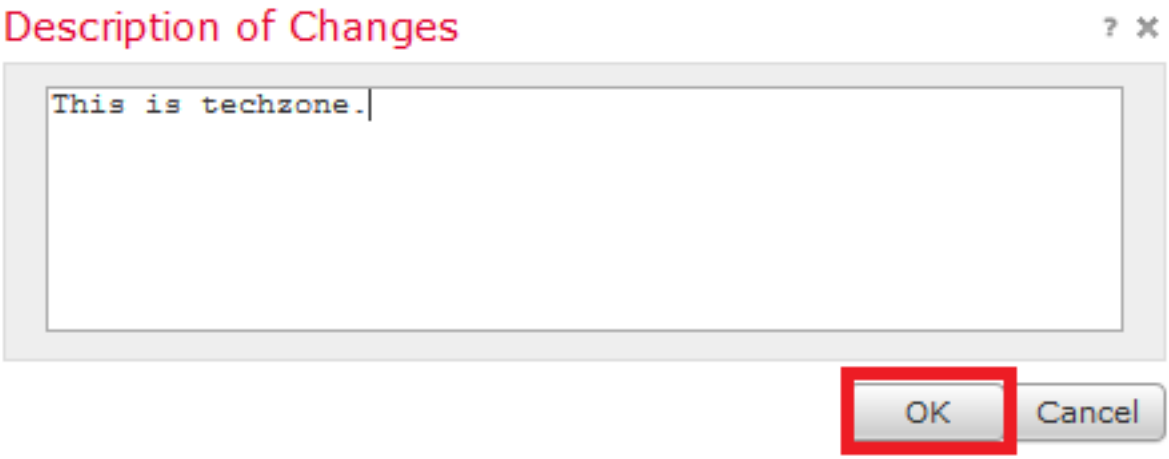
- Soltar e gerar eventos: Ativar a regra, descartar o tráfego e gerar um evento

-Desabilitado: Não habilitar a regra, nenhum evento

Etapa 6. Quando o estado da regra for selecionado, clique no botão Opção **Policy Information (Informações da política**) no painel esquerdo



Passo 7. Selecione o botão **Confirmar alterações** e forneça uma breve descrição das alterações. Clique em **OK** mais tarde. A política de intrusão é validada.



> **Nota**: A validação da política falha se você habilitar uma regra local importada que usa a palavra-chave de limite preterida em combinação com o recurso de limite de evento de intrusão em uma política de invasão.

Etapa 8. Implantar as alterações

Do módulo FTD ou SFR CLI

1. Exibir as regras locais importadas do módulo FTD ou SFR CLI

Etapa 1. Estabelecer uma sessão SSH ou CLI a partir do seu módulo SFR ou FTD

Etapa 2. Navegue até o modo de especialista

```
> expert
admin@firepower:~$
```

Etapa 3. Obter privilégios de administrador

```
admin@firepower:~$ sudo su -
```

Etapa 4. Digite sua senha

```
admin@firepower:~$ sudo su -
Password:
root@firepower:~#
```

Etapa 5. Navegue até **/ngfw/var/sf/detection_engine/UUID/intrusion/**

```
root@firepower:/home/admin# cd /ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-
2369c038cbc9/intrusion/
root@firepower:/ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-2369c038cbc9/intrusion#
```

> **Note**: Se estiver usando o módulo SFR, não use /ngfw/var/sf/detection_engine/*/intrusion path. Uso em instalação **/var/sf/detection_engine/*/intrusion**

Etapa 6. Apresente o seguinte comando

```
grep -Eo "sid:*([0-9]{1,8})" */*local.rules
```

Consulte a imagem abaixo como um exemplo de funcionamento:

```
root@firepower:/ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-2369c038cbc9/intrusion#
grep -Eo "sid:*([0-9]{1,8})" */*local.rules
sid:1000008
sid:1000023
sid:1000007
sid:1000035
sid:1000004
sid:1000000
...
```

Isso listará a lista do SID do cliente que está habilitada pelo módulo FTD ou SFR.

Troubleshoot

Etapa 1. Certifique-se de que a sessão SSH esteja estabelecida no módulo SFR ou FTD, a partir dos mecanismos de detecção do FMC não está listada

Etapa 2. O comando grep -Eo "sid:*([0-9]{1,8})" */*local.rules funcionará somente no diretório de intrusão, o comando não pode ser usado de outro diretório

Etapa 3. Use o comando grep -Eo "sid:*([0-9]{1,8})" */*.rules para obter uma lista SID completa de todas as categorias

Práticas recomendadas para importar regras de intrusão local

Observe as diretrizes ao importar um arquivo de regra local:

- O importador de regras exige que todas as regras personalizadas sejam importadas em um arquivo de texto simples codificado em ASCII ou UTF-8
- O nome do arquivo de texto pode incluir caracteres alfanuméricos, espaços e nenhum

caractere especial além de sublinhado (_), ponto (.) e traço (-)
- O sistema importa regras locais precedidas de um único caractere de libra (#), mas elas são sinalizadas como excluídas
- O sistema importa regras locais precedidas de um único caractere de libra (#) e não importa regras locais precedidas de caracteres de dois quilos (##)
- As regras não podem conter caracteres de escape
- Você não precisa especificar uma ID do gerador (GID) ao importar uma regra local. Se fizer isso, especifique apenas GID 1 para uma regra de texto padrão
- Ao importar uma regra pela primeira vez, faça *não* especificar um ID do Snort (SID) ou número de revisão. Isso evita colisões com SIDs de outras regras, incluindo regras excluídas. O sistema atribuirá automaticamente a regra ao próximo SID de regra personalizada disponível igual ou superior a 1000000 e um número de revisão de 1
- Se você precisar importar regras com SIDs, os SIDs devem ser números únicos entre 1.000.000 e 9.999.999
- Em uma implantação multidomínio, o sistema atribui SIDs a regras importadas de um pool compartilhado usado por todos os domínios no Firepower Management Center. Se vários administradores estiverem importando regras locais ao mesmo tempo, os SIDs dentro de um domínio individual podem parecer não sequenciais, pois o sistema atribuiu os números de intervenção na sequência para outro domínio
- Ao importar uma versão atualizada de uma regra local que você importou anteriormente ou ao reinstalar uma regra local que você excluiu, você ***deve*** incluir o SID atribuído pelo sistema e um número de revisão maior que o número de revisão atual. Você pode determinar o número da revisão de uma regra atual ou excluída editando a regra

  Nota: O sistema incrementa automaticamente o número da revisão quando você exclui uma regra local; este é um dispositivo que permite que você restaure as regras locais. Todas as regras locais excluídas são movidas da categoria de regra local para a categoria de regra excluída.

- Importar regras locais no Firepower Management Center principal em um par de alta disponibilidade para evitar problemas de numeração SID
- A importação falhará se uma regra contiver:Um SID é maior que 2147483647Uma lista de portas de origem ou de destino com mais de 64 caracteres
- Falha na validação da política se você habilitar uma regra local importada que use a palavra-chave ***limite*** preterida em combinação com o recurso de limite de evento de intrusão em uma política de invasão
- Todas as regras locais importadas são salvas automaticamente na categoria de regra local
- O sistema sempre define as regras locais que você importa para o estado de regra desativado. Você deve definir manualmente o estado das regras locais antes de usá-las em sua política de invasão

Informações Relacionadas

Aqui estão alguns documentos para referência relacionados ao SID de snort:

Atualizar regras de intrusão

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-

guide-v60/System_Software_Updates.html#ID-2259-00000356

O Editor de regras de intrusão

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/the_intrusion_rules_editor.html