Verificar una lista de SID personalizada de los sensores Firepower utilizando CLI y GUI de FMC

Introducción

Este documento describe cómo obtener una lista SID personalizada del módulo Firepower Threat Defense (FTD) o FirePOWER mediante CLI y la GUI de FMC. La información de SID se puede encontrar en la GUI de FMC si navega a ***Objetos > Reglas de intrusión***. En algunos casos, es necesario obtener una lista de SID disponibles de la CLI.

prerrequisitos

Requisitos

Cisco recomienda conocer estos temas:

- Cisco Firepower Threat Defense (FTD)
- Cisco ASA con FirePOWER Services
- Cisco Firepower Management Center (FMC)
- conocimiento básico de Linux

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software:'

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico.Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada).Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Una ***regla de intrusión*** es un conjunto de palabras clave y argumentos que el sistema utiliza para detectar intentos de explotar vulnerabilidades en su red. A medida que el sistema analiza el tráfico de red, compara los paquetes con las condiciones especificadas en cada regla. Si los datos del paquete coinciden con todas las condiciones especificadas en una regla, la regla se activa. Si una regla es una regla de alerta, genera un evento de intrusión. Si es una regla de paso, ignora el tráfico. Para una regla de caída en una implementación en línea, el sistema descarta el paquete y genera un evento. Puede ver y evaluar eventos de intrusión desde la consola web de Firepower Management Center.

Firepower System proporciona dos tipos de reglas de intrusión: ***reglas de objeto compartidas*** y ***reglas de texto estándar***. El Grupo de Investigación e Inteligencia de Seguridad Talos de Cisco

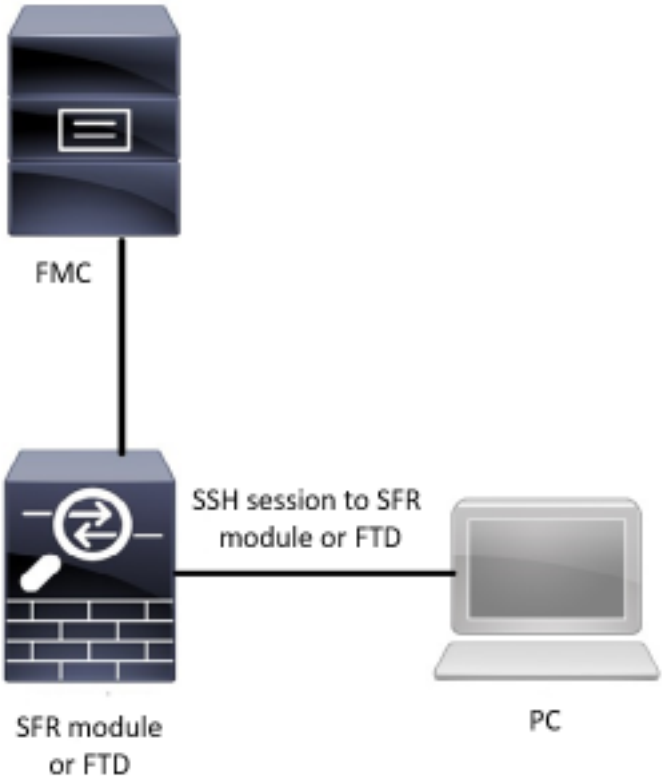
(Talos) puede utilizar reglas de objetos compartidos para detectar ataques contra vulnerabilidades de formas que las reglas de texto estándar tradicionales no pueden. No es posible crear reglas de objetos compartidos. Cuando las reglas de intrusión se escriben por su cuenta, se debe crear una regla de texto estándar. Reglas de texto estándar personalizadas para ajustar los tipos de eventos que probablemente verá. Al escribir reglas y especificar el mensaje de evento de la regla, puede identificar más fácilmente el tráfico que indica ataques y evasiones de políticas.

Cuando habilita una regla de texto estándar personalizada en una directiva de intrusión personalizada, tenga en cuenta que algunas palabras clave y argumentos de regla requieren que el tráfico primero se descodifice o se procese previamente de una determinada manera.

Una *regla local personalizada* en un sistema Firepower es una regla estándar personalizada de Snort que se importa en un formato de archivo de texto ASCII desde una máquina local. Un sistema Firepower permite importar reglas locales mediante la interfaz web. Los pasos para importar reglas locales son muy simples. Sin embargo, para escribir una regla local óptima, un usuario necesita un conocimiento profundo de Snort y los protocolos de red.

> Advertencia: Asegúrese de utilizar un entorno de red controlado para probar cualquier regla de intrusión que escriba antes de utilizar las reglas en un entorno de producción. Las reglas de intrusión mal escritas pueden afectar seriamente el rendimiento del sistema

Diagrama de la red



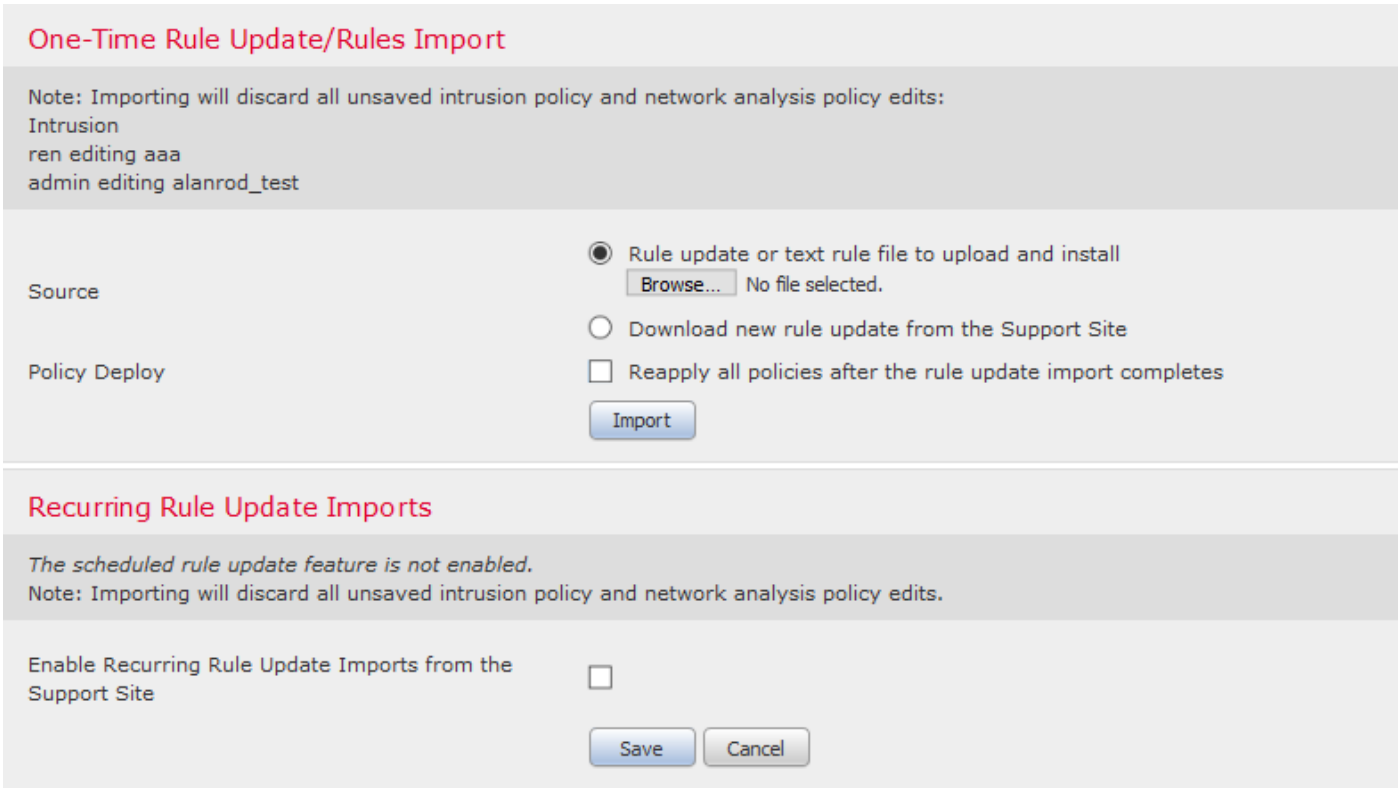
Configurar

Importar reglas locales

Antes de empezar, debe asegurarse de que las reglas enumeradas en el archivo personalizado

no contienen caracteres especiales. El importador de reglas requiere que se importen todas las reglas personalizadas mediante codificación ASCII o UTF-8. El procedimiento que se muestra a continuación explica cómo importar reglas de texto estándar locales desde una máquina local.

Paso 1. Acceda a la pestaña **Reglas de importación** navegando hasta **Objetos > Reglas de intrusión > Reglas de importación.** La página **Actualización de reglas** aparece como se muestra en la siguiente imagen:



Paso 2. Seleccione **Actualización de reglas o archivo de reglas de texto para cargar e instalar** y haga clic en **Examinar** para seleccionar el archivo de reglas personalizado

> Nota: Todas las reglas cargadas se guardan en la categoría **de regla local**

Paso 3. Haga clic en **Importar**. Se importa el archivo de regla

> **Nota**: Los Firepower Systems no utilizan el nuevo conjunto de reglas para la inspección. Para activar una regla local, debe activarla en la directiva de intrusiones y, a continuación, aplicar la directiva.

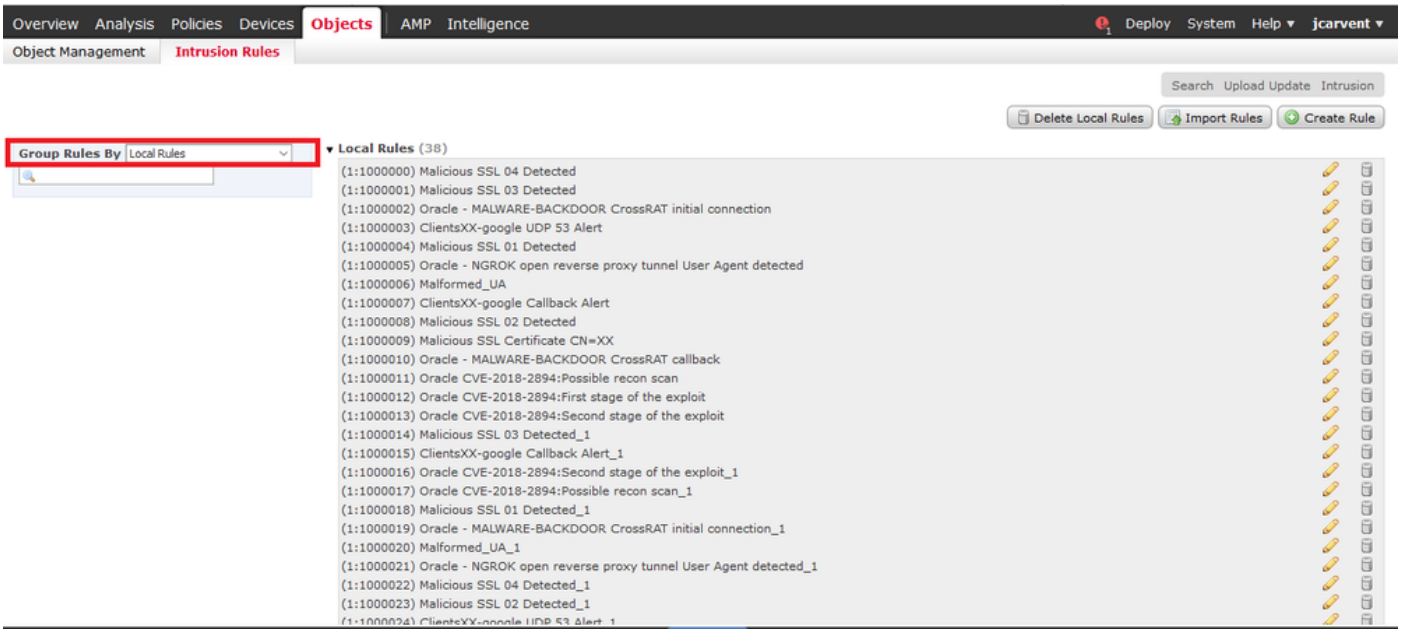
Verificación

Desde la GUI de FMC

1. Ver reglas locales importadas desde la GUI de FMC

Paso 1. Vaya a **Objetos > Reglas de intrusión**

Paso 2. Seleccionar **reglas locales** de **reglas de grupo**



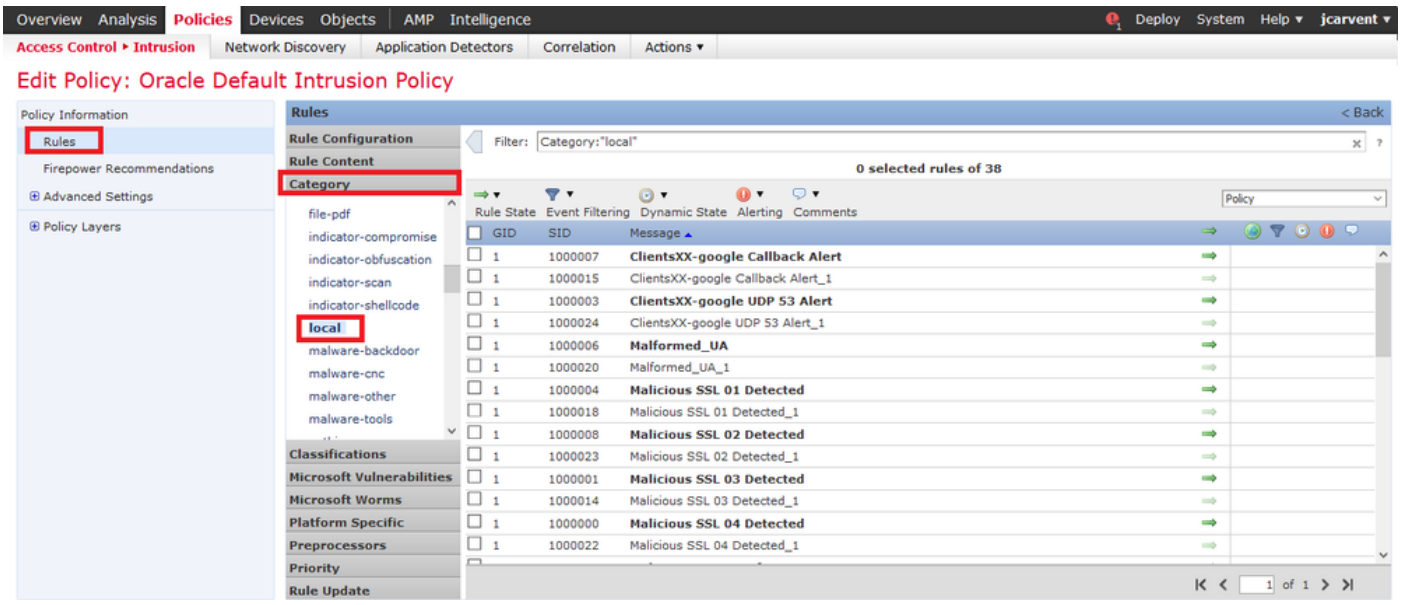
De forma predeterminada, Firepower System establece las reglas locales en un estado desactivado. Estas reglas locales deben establecer manualmente el estado de las reglas locales antes de poder utilizarlas en la política de intrusiones.

2. Habilitar una regla local desde una política de intrusiones

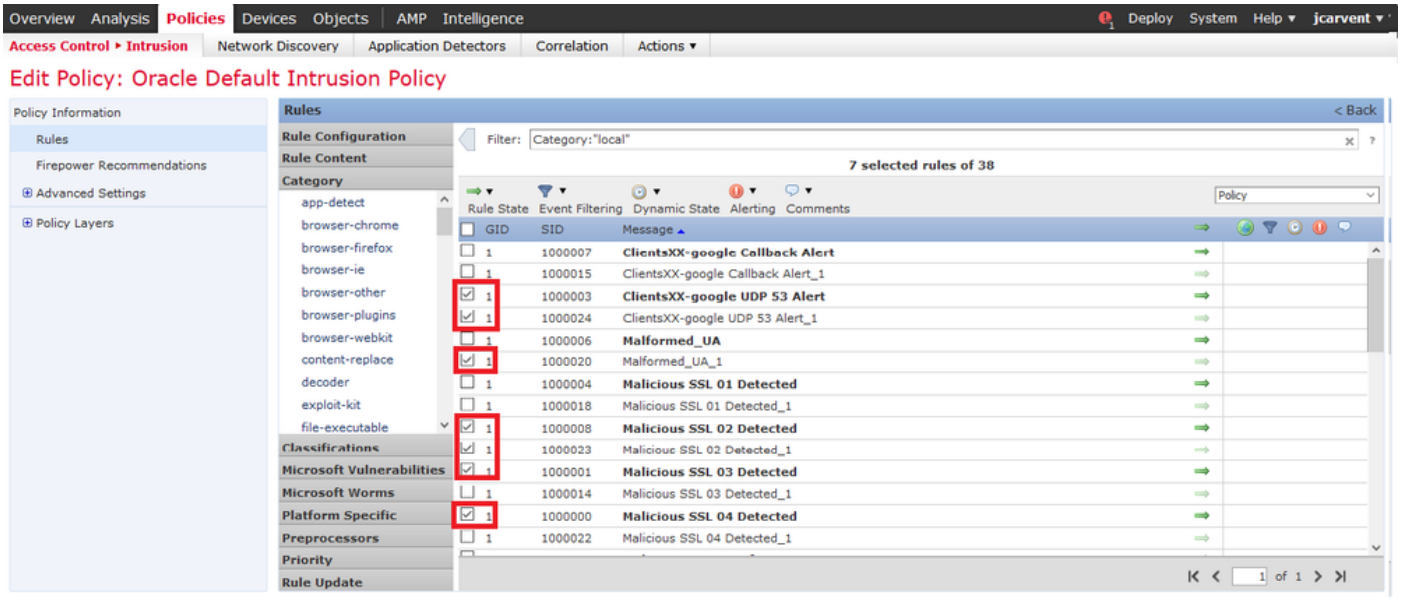
Paso 1. Vaya a la página Editor de políticas bajo **Políticas > Intrusión > Política de intrusiones**

Paso 2. Seleccione **Reglas** en el panel izquierdo

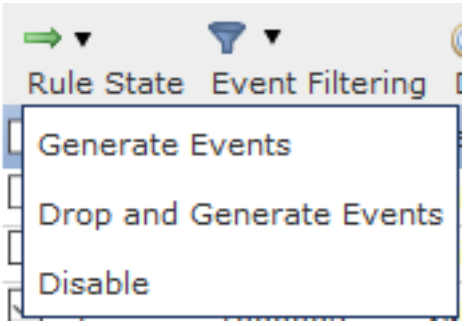
Paso 3. En **Category**, seleccione **local.** Todas las reglas locales deben aparecer si están disponibles:



Paso 4. Seleccione las reglas locales deseadas:



Paso 5. Después de seleccionar las reglas locales deseadas, seleccione un estado en **Estado de regla**



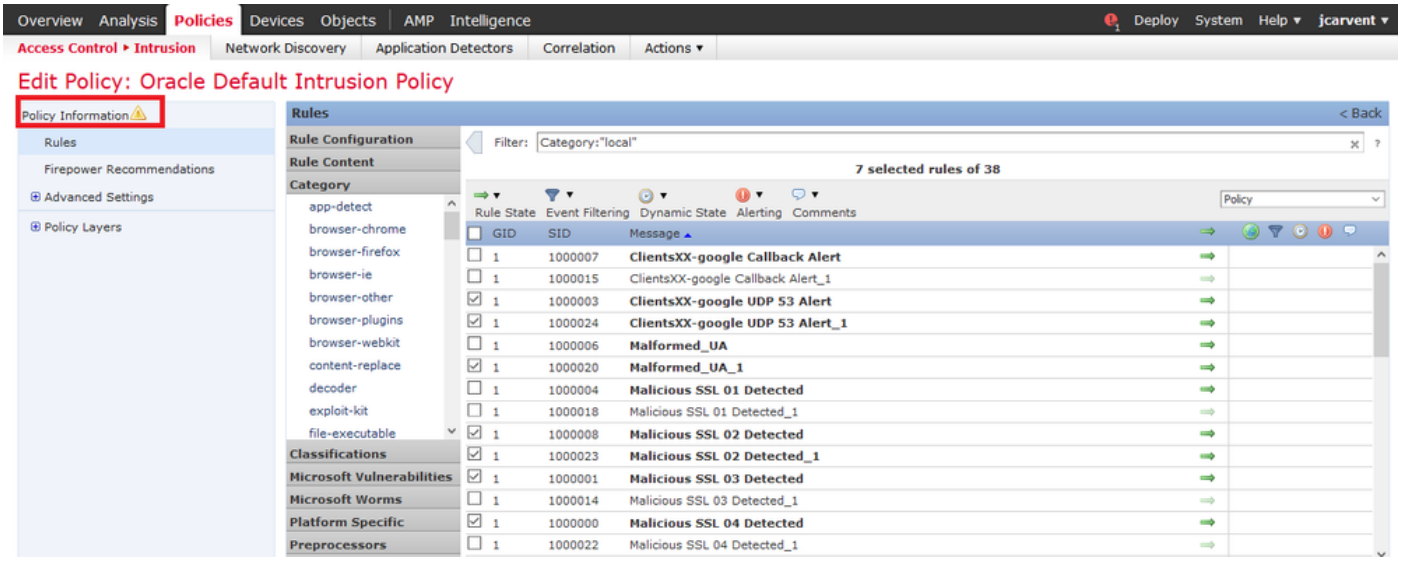
Las opciones disponibles son las siguientes:

- Generar eventos: Habilitar la regla y generar un evento

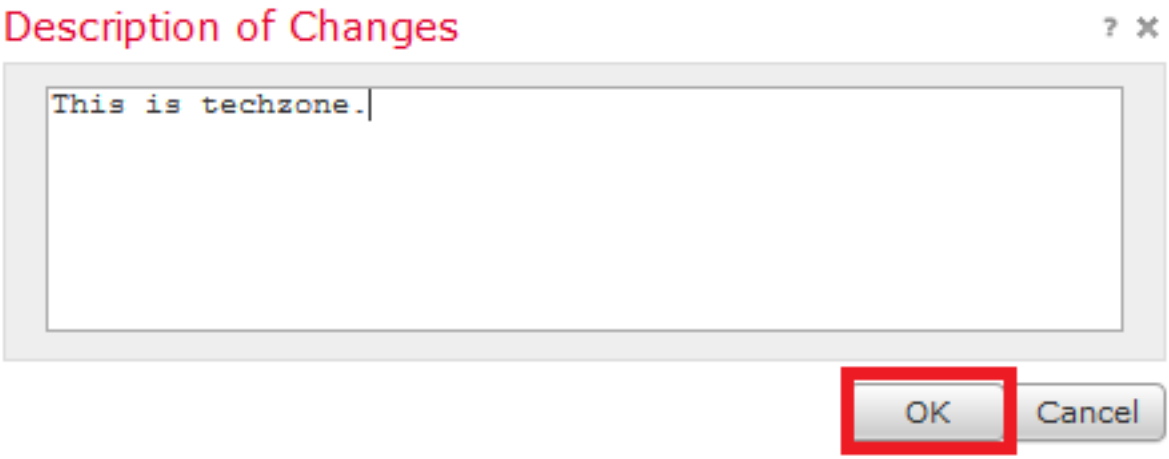
- Eliminar y generar eventos: Habilite la regla, descarte el tráfico y genere un evento

-Inhabilitar: No habilitar la regla, no hay eventos

Paso 6. Una vez seleccionado el estado de regla, haga clic en el opción **Información de política** en el panel izquierdo



Paso 7. Seleccione el botón **Registrar cambios** y proporcione una breve descripción de los cambios. Haga clic en **Aceptar** más tarde. Se valida la política de intrusiones.



> **Nota**: La validación de la política falla si se habilita una regla local importada que utiliza la palabra clave de umbral obsoleta en combinación con la característica de umbral de evento de intrusión en una política de intrusión.

Paso 8. Implementar los cambios

Desde la CLI del módulo FTD o SFR

1. Ver las reglas locales importadas desde la CLI del módulo FTD o SFR

Paso 1. Establezca una sesión SSH o CLI desde su módulo SFR o FTD

Paso 2. Vaya al modo experto

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

Paso 3. Obtener privilegios de administrador

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

Paso 4. Escriba su contraseña

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

Paso 5. Vaya a **/ngfw/var/sf/detection_Engines/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#
```

> Nota: Si utiliza el módulo SFR, no utilice /ngfw/var/sf/detection_Engines/*/ruta de intrusión. Uso insertado **/var/sf/detection_Engines/*/intrusión**

Paso 6. Introduzca el siguiente comando

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

Consulte la siguiente imagen como ejemplo de funcionamiento:

```
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
...
```

Esto enumerará la lista de SID del cliente que está habilitada por el módulo FTD o SFR.

Troubleshoot

Paso 1. Asegúrese de que la sesión SSH se establece en el módulo SFR o FTD, desde los motores de detección FMC no se muestra

Paso 2. El comando grep -Eo "sid:*([0-9]{1,8})" */*local.rules sólo funcionará en el directorio de intrusiones, el comando no se puede utilizar desde otro directorio

Paso 3. Utilice el comando grep -Eo "sid:*([0-9]{1,8})" */*.rules para obtener una lista SID completa de todas las categorías

Prácticas recomendadas para importar reglas de intrusión locales

Observe las instrucciones al importar un archivo de regla local:

- El importador de reglas requiere que todas las reglas personalizadas se importen en un archivo de texto sin formato codificado en ASCII o UTF-8
- El nombre del archivo de texto puede incluir caracteres alfanuméricos, espacios y no

caracteres especiales distintos del guión bajo (_), punto (.) y guión (-)
- El sistema importa reglas locales precedidas de un carácter de libra (#) único, pero se marcan como eliminadas
- El sistema importa reglas locales precedidas de un carácter de libra (#) y no importa reglas locales precedidas de caracteres de dos libras (##)
- Las reglas no pueden contener caracteres de escape
- No es necesario especificar una ID de generador (GID) al importar una regla local. Si lo hace, especifique sólo GID 1 para una regla de texto estándar
- Al importar una regla por primera vez, haga *no* especifique un ID de Snort (SID) o número de revisión. Esto evita colisiones con SID de otras reglas, incluidas las reglas eliminadas. El sistema asignará automáticamente la regla al siguiente SID de regla personalizada disponible de 1000000 o superior, y un número de revisión de 1
- Si debe importar reglas con SID, los SID deben ser números únicos entre 1,000,000 y 9,999,999
- En una implementación de varios dominios, el sistema asigna SID a reglas importadas de un conjunto compartido utilizado por todos los dominios en el Centro de administración FirePOWER. Si varios administradores importan reglas locales al mismo tiempo, los SID dentro de un dominio individual podrían parecer no secuenciales, porque el sistema asignó los números intervinientes en la secuencia a otro dominio
- Al importar una versión actualizada de una regla local que ha importado previamente, o al restablecer una regla local que ha eliminado, ***debe*** incluir el SID asignado por el sistema y un número de revisión mayor que el número de revisión actual. Puede determinar el número de revisión de una regla actual o eliminada editando la regla

  Nota: El sistema incrementa automáticamente el número de revisión cuando elimina una regla local; se trata de un dispositivo que permite restablecer reglas locales. Todas las reglas locales eliminadas se mueven de la categoría de regla local a la categoría de regla eliminada.

- Importar reglas locales en el Firepower Management Center principal en un par de alta disponibilidad para evitar problemas de numeración de SID
- La importación falla si una regla contiene cualquiera de las siguientes:Un SID es mayor que 2147483647Una lista de puertos de origen o de destino con más de 64 caracteres
- La validación de la política falla si habilita una regla local importada que utiliza la palabra clave ***threshold*** obsoleta en combinación con la característica umbral de evento de intrusión en una política de intrusión
- Todas las reglas locales importadas se guardan automáticamente en la categoría de regla local
- El sistema siempre establece las reglas locales que se importan al estado de regla desactivado. Debe establecer manualmente el estado de las reglas locales antes de poder utilizarlas en la política de intrusiones

Información Relacionada

Aquí hay algunos documentos de referencia relacionados con el SID de snort:

Actualizar reglas de intrusión

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

El editor de reglas de intrusión

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