Instrucciones para la creación de perfiles de reglas en el sistema FireSIGHT

Contenido

Introducción

Si se sobresuscribe un appliance FirePOWER o un appliance virtual NGIPS, debe recopilar algunos datos adicionales para determinar qué componente del dispositivo está ralentizando el sistema. La creación de perfiles de reglas permite a un sistema FireSIGHT generar más datos sobre las reglas y subsistemas del motor de detección que utilizan la mayoría de los ciclos de CPU. En este artículo se proporcionan instrucciones sobre cómo ejecutar la generación de perfiles de reglas en el appliance FireSIGHT y el appliance virtual NGIPS.

Prerequisites

Requirements

Cisco recomienda que conozca los dispositivos FirePOWER y los modelos de appliances virtuales.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

- Appliances FirePOWER serie 7000, appliances de la serie 8000 y appliances virtuales NGIPS
- Software versión 5.2 o posterior

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. If your network is live, make sure that you understand the potential impact of any command.

> **Advertencia:** La ejecución del comando de definición de perfiles de reglas puede afectar al rendimiento de la red. Por lo tanto, debe ejecutar este comando sólo si el Soporte Técnico

de Cisco solicita datos de perfiles de reglas.

Pasos para ejecutar perfiles de reglas

Paso 1: Acceda a la CLI del dispositivo administrado.

Paso 2: Ejecute el siguiente comando de definición de perfiles de reglas durante un tiempo determinado. El tiempo debe estar entre 15 y 120 minutos. En el siguiente ejemplo, el script se ejecuta durante 15 minutos.

```
> system support run-rule-profiling 15
```

Paso 3: Confirme la ejecución del comando. Escriba **y** y presione **Enter**.

> **Advertencia**: el comando de definición de perfiles de reglas reinicia el motor de detección, lo que puede afectar a la funcionalidad de detección y aumentar la utilización de la CPU.

```
> system support run-rule-profiling 15

You are about to profile
 DE    Primary Detection Engine (94854a60-cb17-11e3-a2f5-8de07680f9f3)
 Time  15 minutes

WARNING!!  Detection Engine will be restarted.
Intrusion Detection / Prevention will be affected

Please confirm by entering 'y': y
```

Después de confirmar la ejecución, comienza la creación de perfiles de reglas. El tiempo para completar la generación de perfiles se reduce a cero minutos.

```
Restarting DE for profiling...done
Profiling for 15 more minutes...
```

Una vez completado, el mensaje del shell vuelve.

```
Restarting DE for profiling...done
Profiling...done
Restarting DE with original configuration...in progress
>
```

Paso 4: El comando de generación de perfiles de regla genera un archivo .tgz. puede encontrar el archivo ejecutando el siguiente comando en el shell.

```
> system file list
May 12 15:53 99364308 profiling.94854a60-cb17-11e3-a2f5-8de07680f9f3.1399909945.tgz
```

Paso 5: Proporcione el archivo al Soporte Técnico de Cisco para un análisis adicional.