Instruções de criação de perfis de regras no sistema FireSIGHT

Contents

Introduction

Se um dispositivo FirePOWER ou NGIPS Virtual estiver com excesso de assinaturas, você precisará coletar alguns dados adicionais para determinar qual componente do dispositivo está retardando o sistema. O perfil de regras permite que um sistema FireSIGHT gere mais dados sobre quais regras e subsistemas do mecanismo de detecção estão usando a maioria dos ciclos da CPU. Este artigo fornece as instruções sobre como executar o perfil de regras em dispositivos FireSIGHT e NGIPS Virtual Appliance.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento sobre o dispositivo FirePOWER e os modelos de dispositivos virtuais.

Componentes Utilizados

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

- Dispositivos FirePOWER 7000 Series, dispositivos 8000 Series e dispositivos virtuais NGIPS
- Versão do software 5.2 ou 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.

> **aviso:** A execução do comando de criação de perfil de regra pode afetar o desempenho da rede. Portanto, você deve executar esse comando somente se o Suporte Técnico da Cisco

solicitar dados de perfil de regras.

Etapas para executar o perfil da regra

Passo 1: Acesse a CLI do dispositivo gerenciado.

Passo 2: Execute o seguinte comando de criação de perfil de regra para uma determinada hora. O tempo deve estar entre 15 e 120 minutos. No exemplo a seguir, o script é executado por 15 minutos.

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

Passo 3: Confirme a execução do comando. Digite **y** e pressione **Enter**.

> **Aviso**: o comando de criação de perfil de regra reinicia o mecanismo de detecção, o que pode afetar a funcionalidade de detecção e aumentar a utilização da 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
```

Após confirmar a execução, o perfil da regra é iniciado. O tempo para concluir o perfil é reduzido para zero minutos.

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

Depois de concluído, o prompt do shell volta.

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

Passo 4: O comando de criação de perfil de regra gera um arquivo .tgz. você pode encontrar o arquivo executando o seguinte comando no shell.

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

Passo 5: Forneça o arquivo ao Suporte Técnico da Cisco para análise posterior.