描出关于FireSIGHT系统的规则说明

目录

简介

如果FirePOWER设备或NGIPS虚拟设备是订购过量的，您需要收集某其它数据确定设备的哪个组件减速系统。规则描出使FireSIGHT系统生成检测引擎规则和子系统使用多数CPU周期的进一步数据。此条款提供说明关于怎样运行描出在FireSIGHT设备和NGIPS虚拟设备的规则。

先决条件

要求

思科建议您有在FirePOWER设备和虚拟设备型号的知识。

使用的组件

本文档中的信息基于下列硬件和软件版本：

- FirePOWER 7000系列设备、8000系列设备和NGIPS虚拟设备
- 软件版本5.2或以上

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

> 警告：运行描出命令的规则可能影响网络性能。所以您应该运行此命令，只有当思科技术支持要求规则配置文件数据。

运行规则描出的步骤

步骤 1：访问受管理设备的CLI。

步骤 2：运行描出命令partcular时间的以下规则。时间必须是在15和120分钟之间。在以下示例中，脚本运行在15分钟。

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

步骤 3：确认命令的执行。键入**y**并且按回车。

> 警告： 描出命令的规则重新启动检测引擎，能影响检测功能，并且增加CPU利用率。

```
> 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
```

在确认执行以后，规则描出开始。时候完成描出计数下来对零的分钟。

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

一旦完整， shell提示符回来。

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

步骤 4：描出命令的规则生成.tgz文件。您能通过运行以下in命令找到文件shell。

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

步骤 5：提供文件给思科技术支持为进一步分析。