FireSIGHT系统上的规则分析说明

目录

简介

如果FirePOWER设备或NGIPS虚拟设备超订用，您需要收集一些额外数据以确定设备的哪个组件正在减慢系统速度。规则分析使FireSIGHT系统能够生成更多数据，以了解检测引擎的规则和子系统使用的CPU周期最多。本文提供有关如何在FireSIGHT设备和NGIPS虚拟设备上运行规则分析的说明。

先决条件

要求

思科建议您了解FirePOWER设备和虚拟设备型号。

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
- 5.2 或更高软件版本

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**：运行规则分析命令可能会影响网络性能。因此，您应仅在思科技术支持请求规则分析数据时运行此命令。

运行规则分析的步骤

步骤 1：访问受管设备的CLI。

步骤 2：在特定时间运行以下规则分析命令。时间必须介于15到120分钟之间。在以下示例中，脚本运行15分钟。

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

步骤 3：确认命令的执行。键入y并按Enter。

警告： 规则分析命令可重新启动检测引擎，这可能影响检测功能并增加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
```

确认执行后，规则分析开始。完成分析的时间会减少到零分钟。

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

完成后，shell提示符将返回。

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

步骤 4：规则分析命令生成.tgz文件。在shell中运行以下命令可以找到该文件。

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

步骤 5：向思科技术支持提供文件以供进一步分析。