下载数据包数据(PCAP文件)使用网页用户界面

目录

简介

使用网页用户界面，您能下载触发喷鼻息规则的数据包。条款提供步骤下载数据包捕获数据(PCAP文件)使用Sourcefire FireSIGHT管理系统的网页用户界面。

先决条件

要求

思科建议您有在Sourcefire FirePOWER设备和虚拟设备型号的知识。

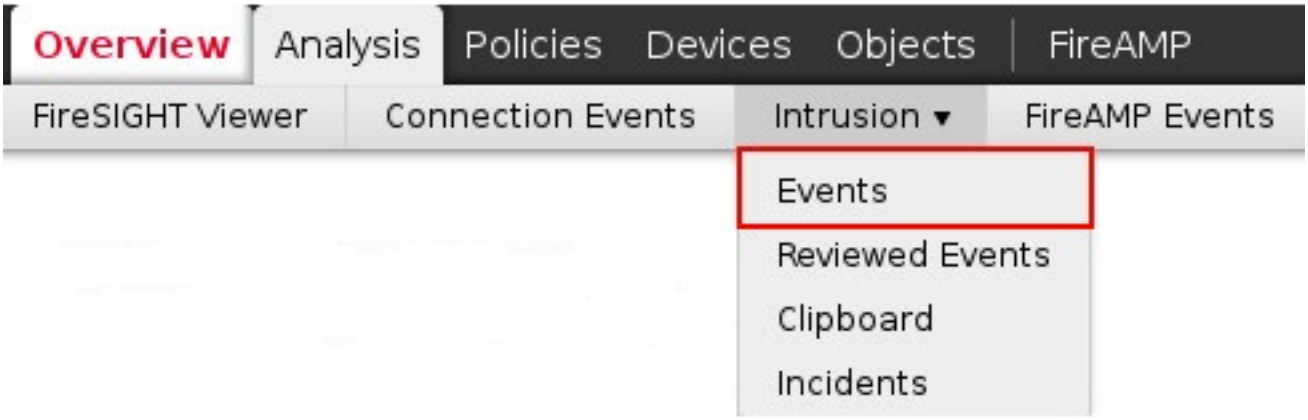
使用的组件

关于本文的信息根据Sourcefire FireSIGHT管理中心，亦称防御中心，运行软件版本5.2或更加极大。

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。

下载PCAP文件的步骤

步骤 1：Sourcefire防御中心或管理中心的洛金，和导航对入侵事件页作为如下：



步骤 2：使用复选框，请选择您希望下载数据包捕获数据的事件(PCAP文件)。

步骤 3：移动到页和的底部：

- 点击下载数据包下载触发选定入侵事件的数据包
- 点击下载所有信息包下载触发在当前限制条件的视图的入侵事件的所有信息包

  注意：下载的数据包将保存作为PCAP。 如果要分析数据包捕获，您将需要下载和安装能够读PCAP文件的软件。

步骤 4：当提示，请保存PCAP文件到您的硬盘驱动器。