使用Web用户界面下载数据包数据（PCAP文件）

目录

简介

使用Web用户界面，可以下载触发Snort规则的数据包。本文提供了使用Sourcefire FireSIGHT管理系统的Web用户界面下载数据包捕获数据（PCAP文件）的步骤。

先决条件

要求

思科建议您了解Sourcefire FirePOWER设备和虚拟设备型号。

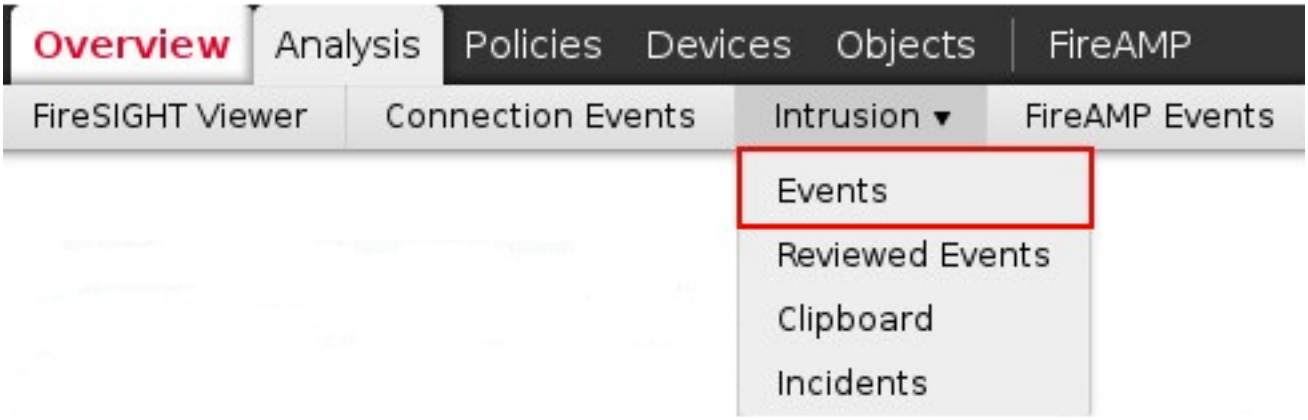
使用的组件

本文档中的信息基于运行软件版本5.2或更高版本的Sourcefire FireSIGHT管理中心（也称为防御中心）。

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：登录Sourcefire防御中心或管理中心，然后导航至Intrusion Events页面，如下所示：



步骤 2：使用此复选框，选择要下载数据包捕获数据（PCAP文件）的事件。

步骤 3：滚动到页面底部，然后：

- 点击Download Packet（下载数据包）下载触发选定入侵事件的数据包
- 点击Download All Packets以下载在当前受限视图中触发入侵事件的所有数据包

  注意：下载的数据包将另存为PCAP。 如果要分析数据包捕获，则需要下载并安装能够读取PCAP文件的软件。

步骤 4：出现提示时，将PCAP文件保存到硬盘。