下载信息包数据(PCAP文件)使用网页用户界面

Contents

Introduction

使用网页用户界面，您能下载触发喷鼻息规则的信息包。条款提供步骤下载信息包获取数据(PCAP文件)使用Sourcefire FireSIGHT管理系统的网页用户界面。

Prerequisites

Requirements

Cisco建议您有在Sourcefire Firepower设备和虚拟设备型号的知识。

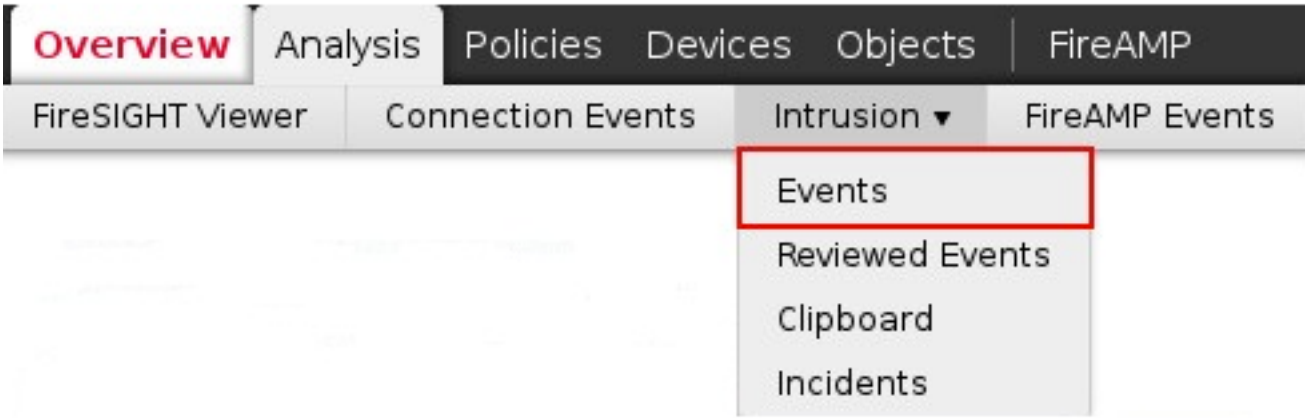
Components Used

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。

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.

下载PCAP文件的步骤

步骤 1：Sourcefire防御中心或管理中心的洛金，和连接对闯入事件页作为如下：



步骤 2：使用复选框，请选择您希望下载信息包获取数据的事件(PCAP文件)。

步骤 3：移动到页和的底部：

- 点击下载信息包下载触发所选的闯入事件的信息包
- 点击下载所有信息包下载触发在当前约束的视图的闯入事件的所有信息包

Note:下载的信息包将被保存作为PCAP。 如果要分析信息包获取，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文件对您的硬盘驱动器。