目录

简介

当检测在您的受监视网段时的新的主机FireSIGHT系统生成事件。它可能有较少信心不正确地检测操作系统或服务，或者。如果事件被标记作为*未知*，意味着分析流量，但是操作系统不匹配其中任一已知指纹。本文提供清单和建议最小化*未知*事件。

先决条件

本文档中的信息基于下列硬件和软件版本：

- FireSIGHT系统、火力伊莱克斯和NGIPS虚拟伊莱克斯
- 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。

故障排除列表

如果您的FireSIGHT系统生成在待定或在UNKNOWN状态的事件，您能遵从下面步骤开始排除故障此问题：

> **注意**：*未认出的*主机不是相同的象*未知主机*。*未认出的*主机是系统未收集足够的信息识别他们的操作系统的主机。

排除故障清单	**建议**
1. 什么VDB版本安装在FireSIGHT管理中心？	最新的VDB版
2. 什么是您的FireSIGHT许可证主机限制？多少台主机由FireSIGHT检测？	如果主机限制。
3. 离开多少的跳主机从FireSIGHT受管理设备查找？	越高在主机和

4. 有没有在主机和受管理设备之间的任何轴向设备？	任何轴向设备 主机的原始T
5. 受管理设备监控在任何异步路由网络的流量？	如果FireSIG
6. 有没有用于任何服务的任何非标准端口？有没有配置的任何自定义编码器寻址非标准端口？	不正确地配置

其它数据

如果所有上述建议按照，但是仍有未知，等待或未认出的主机找到，则我们将需要分析以下 data:

1. 全双工会话流量

从不正确地识别或者被标记作为未知或待定的主机的全双工会话流量。

2. 排除故障文件

排除故障从FireSIGHT管理中心和受管理设备的文件。显示受管理设备的位置的网络图或拓扑是有用。

3. 数据包捕获(PCAP)

受管理设备接收的数据包跟在主机产生的数据包可能不同。如果任何报头正在修改的轴向设备存在主机和受管理设备之间，它发生。所以，捕获从两端的PCAP -主机和受管理设备最好的，准许比较从两个PCAPs的报头。数据包之间的所有不匹配能导致服务或主机的错误辨识。