FireSIGHT可能會錯誤地識別主機，或者將事件標籤為「掛起」或「未知」

目錄

簡介

FireSIGHT系統在檢測到受監控網段上的新主機時生成事件。它可能會錯誤地檢測到作業系統或服務，或檢測結果不太可靠。如果事件標籤為*Unknown*，則表示已分析流量，但作業系統不匹配任何已知指紋。本文檔提供最小化未知事件的清單*和建*議。

必要條件

本檔案中的資訊是根據以下硬體和軟體版本：

- FireSIGHT系統、FirePOWER裝置和NGIPS虛擬裝置
- 軟體版本5.2或更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

疑難排解清單

如果您的FireSIGHT系統正在生成處於掛起或未知狀態的事件，可以按照以下步驟開始解決此問題：

> **注意**：未*識別*的主機與未知主機*不*相同。*未識*別的主機是系統尚未收集到足夠資訊來識別其作業系統的主機。

	建議

	最新的VDB版本包含更多指紋資訊。始終建議在FireSIGHT管理中心上安裝最新版本。
主機？	如果主機限制超過，FireSIGHT系統會在新資料傳入時修剪最早的資料。可以將系統策略配置
	主機與受管裝置之間的跳數越高，主機離裝置越遠，因此流量被修改的可能性就越大，並且
	任何線上裝置（如防火牆、NAT裝置、負載平衡器和代理伺服器）的存在都可以修改原始TC
	如果FireSIGHT系統監視非同步路由流量，它可能無法看到完整的會話。
非標準埠進行編址？	配置不當的自定義解碼器可能與預設解碼器衝突。

其他資料

如果按照以上所有建議，但仍然找不到未知、待定或未識別的主機，則需要分析以下資料和冒號；

1.完整會話流量

來自主機且未正確識別或標籤為未知或待定的完整會話流量。

2.疑難排解檔案

對FireSIGHT管理中心和受管裝置中的檔案進行故障排除。顯示受管裝置位置的網路圖或拓撲將很有幫助。

3.封包擷取(PCAP)

受管裝置接收的資料包可能與主機上生成的資料包不同。如果主機和受管裝置之間存在任何修改內聯裝置的報頭，就會發生這種情況。因此，最好從兩端（主機和受管裝置）捕獲PCAP，這樣就可以比較兩個PCAP的報頭。資料包之間的任何不匹配都可能導致服務或主機標識錯誤。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。