# 通過Sourcefire FirePOWER和虛擬裝置檢測鏈路聚合流量

## 目錄



## 簡介

鏈路聚合已由IEEE在802.3ad 802.3ax上標準化。鏈路聚合的常見實現包括EtherChannel、鏈路聚合控制協定(LACP)、埠聚合協定(PAgP)等。本文介紹Sourcefire裝置如何處理鏈路聚合流量。

## 必要條件

### 需求

思科建議您瞭解Sourcefire FirePOWER裝置型號、虛擬裝置型號、鏈路聚合控制協定(LACP)、EtherChannel和埠聚合協定(PAgP)。

## 支援鏈路聚合

Sourcefire裝置能夠與任何標準鏈路聚合實施配合使用，因為鏈路聚合協定不會向資料包本身新增任何額外資料。在實施Sourcefire裝置和任何鏈路聚合協定之間沒有已知問題。

### 注意事項

在連結聚合部署中部署Sourcefire裝置時，需要考慮以下幾點：

1. 如果Sourcefire裝置處於被動模式，並且同一檢測引擎正在監視EtherChannel的所有鏈路，則鏈路聚合配置並不重要。
2. 如果單個檢測引擎僅監控某些鏈路，或者裝置部署為內聯裝置，則建議配置鏈路聚合以同時使

用源MAC地址和目標MAC地址。這將避免與非同步路由相關的效能問題。
3. Snort能夠順利處理連結彙總流量。 但是，Snort無法解碼交換機之間傳送的鏈路聚合控制資料包。
4. EtherChannel中的負載平衡方法基於每個流量流，而不是基於每個幀或資料包，因此這些流量是獲得負載均衡的原因。在EtherChannel中配置「源IP和目標IP」可能會影響Sourcefire snort例項間的負載平衡。僅當執行的雜湊導致可供選擇的IP集較有限時，才會出現這種情況。使用「源MAC和目標MAC」有助於負載分配。

# 已知問題

在5.3.1.1之前和之前（包括5.3.1.1之前）的所有版本上報告了LACP上的以下已知問題：

在某些情況下，對訪問控制策略、入侵策略、網路發現策略或裝置配置應用更改，或者安裝入侵規則更新或漏洞資料庫(VDB)更新，會導致系統在快速模式下使用鏈路聚合控制協定(LACP)的流量中發生中斷。解決方法是在慢速模式下配置LACP鏈路。(112070)

# 相關檔案

- 《 FireSIGHT系統版本5.3.1.1發佈說明》