

排解由於MTU更大（封包過大）而捨棄封包的疑難問題

目錄

[簡介](#)

[驗證](#)

[組態](#)

簡介

任何網路中的封包的MTU可能大於預設大小1518位元組。這可能會導致封包在Snort處理之前，在受管裝置的介面被捨棄。因此，在FireSIGHT管理中心的Web使用者介面上將沒有相應的事件。本文描述如何驗證資料包過大導致的資料包丟棄，以及如何更改FireSIGHT系統上的預設MTU設定。

驗證

若要判斷是否由於MTU大小而發生捨棄，請執行以下步驟：

1. 通過安全外殼(SSH)登入到受管裝置，然後運行以下命令：

```
> show portstats
```

輸出示例：

```

> show portstats
====Port: s1p1====
LateCollisions           0
Collisions               0
BadCRC                   0
RxErrorFrameReceived    0
Jabber                   0
Oversize                 0
Fragments                0
Undersize                 0
ReceiveFIFOOverrun      0
FCReceived               0
FCSent                   0
SentMultiple             0
BroadcastFramesSent     0
MulticastFramesSent     0
ExcessiveCollisions     0
UnicastFramesSent       0
Frames1024toMaxOctets   893517976
Frames512to1023Octets  386326257
Frames256to511Octets   311216343
Frames128to255Octets   816262625
Frames65to127Octets    9596711850
Frames64Octets          6063772443
MulticastFramesReceived 1061719547
BroadcastFramesReceived 475460322
SentDeferred             0
GoodUnicastFramesReceived 16530627625
CRCErrorsSent           0
BadOctetsReceived       0
GoodOctetsReceived      3052120191917
GoodOctetsSent          0

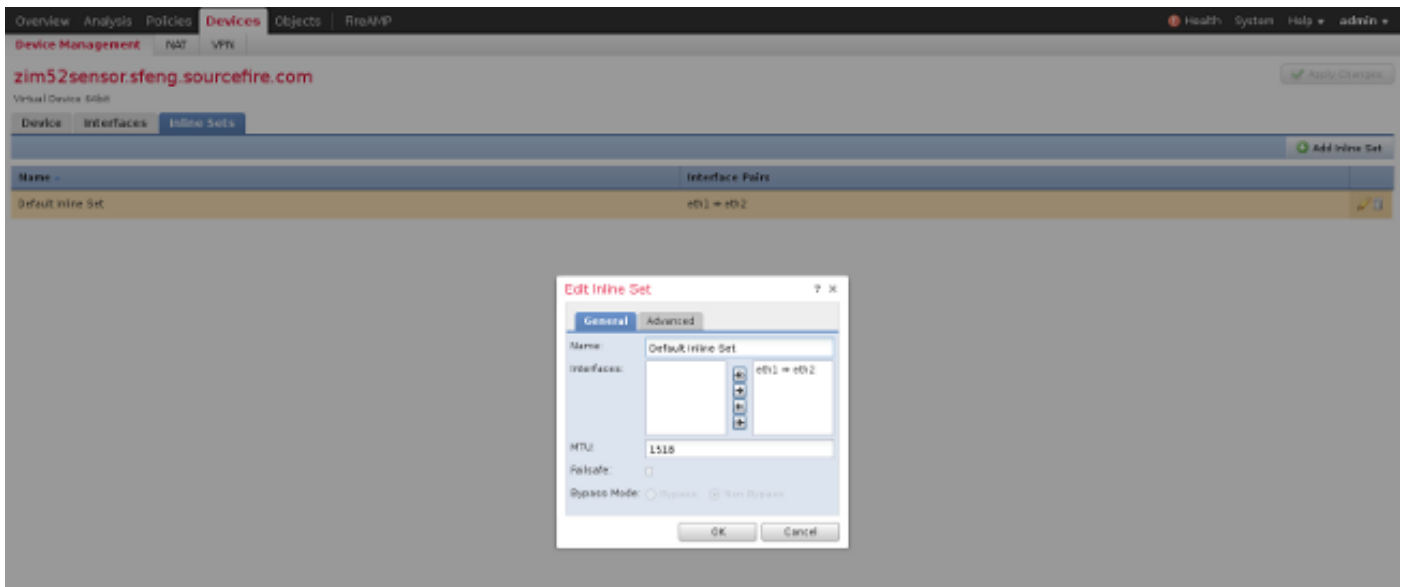
```

2. 檢查每個埠的 *Oversize* 資料包。驗證數字是否為零或更高。例如，上面的螢幕截圖顯示埠 s1p1 的超大計數器為零。此檢查可讓您知道哪些連線埠正在接收超大封包。

組態

如果受管裝置的介面看到過大的資料包，則必須增加介面上的 MTU。若要變更 MTU，請依照以下步驟操作：

1. 登入到 FireSIGHT 管理中心的 Web 使用者介面。
2. 導覽至 **Devices > Device Management**。
3. 按一下 **Inline Sets** 頁籤，然後按一下要更改的內聯集旁的 **Edit**。
4. 根據網路的流量型別，將 **MTU** 欄位設定為適當的數字。



4. 儲存並應用更改。