

# ASA吞吐量 and 連線速度故障排除和分析資料包捕獲

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[故障排除方法](#)

[資料分析](#)

[常見問題](#)

[將ASA連線到相鄰裝置的介面上的速度和雙工值配置錯誤](#)

[將流量傳送到IPS模組](#)

[ASA對TCP MSS選項的修改會導致效能稍有下降](#)

[相關資訊](#)

## 簡介

本文檔介紹如何對思科自適應安全裝置(ASA)吞吐量和連線速度問題進行故障排除。

## 必要條件

### 需求

本文件沒有特定需求。

### 採用元件

本檔案中的資訊是根據思科調適型安全裝置(ASA)。

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。

## 背景資訊

某些客戶在首次部署ASA或測試新連線時可能會遇到問題。問題在於，流經ASA的連線的TCP吞吐量比ASA不在連線路徑中時低得多 ( 或者連線速度比在網路上實施ASA之前慢得多 )。

例如，客戶可能會用ASA 5505或ASA 5510替換低端D-Link路由器 ( 或其他路由裝置 )；但是，一旦更換路由器，連線速度就會大大降低。客戶可能會向Cisco TAC提出問題，因為他們認為ASA導致連線速度降低。

## 故障排除方法

當網路上有封包遺失或封包延遲時，TCP流量會減慢。為了瞭解問題的確切原因，資料必須顯示線路上該連線的實際TCP資料包，以及網路可能會如何影響這些資料包。通常情況下，網路管理員在執行特定操作（例如FTP檔案傳輸或線上速度測試）時收到有關該問題的警報。通常，問題會再次出現。因此，管理員可以收集所需資料以查詢根本原因。

為了收集所需的資料，應在測試之前和之後從ASA運行**show tech**命令。此命令顯示配置和資料包統計資訊(主要來自**show service-policy**)，還顯示介面錯誤是否增加。

需要雙向、同時的資料包捕獲（從連線經過的兩個ASA介面獲取）以完全診斷問題的原因。

有關如何將資料包捕獲應用到ASA的示例，請參閱以下文檔：

- [排除通過PIX和ASA的連線故障](#)
- [TAC安全播客第#1集 — 使用ASA資料包捕獲實用程式進行故障排除](#)

## 資料分析

收集所需資料後，您可以使用資料包捕獲，確定可能已出現以下哪一個問題：

- 來自外部主機的资料包在到達ASA的外部介面之前被丟棄或延遲。
- ASA延遲或丟棄資料包。
- 資料包在內部網路中的某個位置被延遲或丟棄。

**附註：**此分析假設資料從外部介面上的主機傳送到內部介面上的主機。

以下影片示範了如何對封包擷取進行分析：

*TCP資料流聚合*是此問題特有的技術考慮因素，因為當您使用ASA上的某些功能時，防火牆會完全合併通過它的TCP資料流。

例如，如果ASA發現網路上的缺失資料包（因為ASA未收到該資料包），它將代表另一個TCP端點傳送缺失資料的ACK。這種情況最為常見。如果ASA發現不按順序到達的資料包，則ASA對資料包重新排序，並以正確的順序將其傳送給接收者。如果沒有網路丟棄或資料包重新排序，啟用此功能不會有任何副作用。如果任一TCP終端傳送的所有資料包都成功通過網路和ASA，您將不知道此功能已啟用，因為它不會對資料包流執行操作。只有當網路上的TCP連線出現故障時，此功能才會進一步降低網路流量的速度。對ASA而言，合併TCP流的行為非常耗費資源。對於網路上丟棄的每個資料包，ASA不僅必須傳送TCP資料包請求重新傳輸該資料包，還必須緩衝資料包丟失後傳送方繼續傳送的資料包。

## 常見問題

### 將ASA連線到相鄰裝置的介面上的速度和雙工值配置錯誤

當裝置被ASA替換時，通常會發生此問題。如果ASA介面上的速度和雙工值與相鄰裝置上的值不同，則該介面會發生丟包。檢查ASA介面以及相鄰介面上的速度和雙工值。

檢查ASA的**show interface**輸出，查詢作為此問題症狀的明顯錯誤：

```
Interface Ethernet0/0 "Outside", is up, line protocol is up
```

```
Hardware is i82546GB rev03, BW 100 Mbps
Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
MAC address 0019.2f58.c324, MTU 1500
IP address 192.168.222.122, subnet mask 255.255.255.252
124047996 packets input, 35340918453 bytes, 0 no buffer
Received 3 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 L2 decode drops
156918660 packets output, 40931551514 bytes, 0 underruns
1 output errors, 4286634 collisions, 0 interface resets
0 babbles, 123332 late collisions, 4752834 deferred
0 lost carrier, 0 no carrier
input queue (curr/max blocks): hardware (0/0) software (0/0)
output queue (curr/max blocks): hardware (0/245) software (0/0)
Traffic Statistics for "Outside":
124047995 packets input, 33107957301 bytes
157041993 packets output, 38195084709 bytes
103480 packets dropped
1 minute input rate 2140 pkts/sec, 477200 bytes/sec
1 minute output rate 2630 pkts/sec, 396763 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 2152 pkts/sec, 525496 bytes/sec
5 minute output rate 2701 pkts/sec, 421215 bytes/sec
5 minute drop rate, 0 pkts/sec
```

## 將流量傳送到IPS模組

當ASA配置為向IPS模組傳送流量時，ASA上會使用TCP流合併功能。有關TCP資料流合併功能的詳細資訊，請參閱本文檔的[資料分析部分](#)。

## ASA對TCP MSS選項的修改會導致效能稍有下降

預設情況下，ASA將SYN資料包中的TCP MSS選項設定為1380。因此，TCP端點不應傳輸大於1380位元組的TCP區段。該值低於通常的預設值1460位元組，表示TCP效能下降了約6%(6%)。效能可能會提高，因為您增加了ASA上的最大MSS設定或禁用了MSS調整。修改ASA上的預設命令之前，如果資料包被進一步封裝在某個位置的路徑中，請瞭解與潛在分段相關的風險。

有關詳細資訊，請參閱Cisco ASA 5500系列命令參考的[sysopt connection tcpmss](#)部分。

## 相關資訊

- [Cisco ASA 5500系列命令參考，8.2](#)
- [技術支援與文件 - Cisco Systems](#)