"；增強型應用和URL檢測"；時，排除FTD資料包丟棄(tcp-not-syn)故障在具有非對稱流量流的內聯介面上啟用

目錄

問題

使用內嵌介面集設定的防火牆威脅防禦(FTD)裝置捨棄具有加速安全路徑(ASP)捨棄原因tcp-not-syn的TCP返回流量。這在TLS伺服器身份發現(TSID)功能啟用後立即發生，特別是啟用「增強型應用和URL檢測」選項。在較舊的Firewall Management Center(FMC)版本中，該選項稱為「早期應用程式檢測和URL分類」。 傳迴路徑上的TCP SYN-ACK封包會被轉送原始SYN的相同FTD裝置捨棄，因此無法建立TCP作業階段。

該問題表現為廣泛的TCP連線故障，不限於TLS流量。啟用此功能時會觀察到以下症狀：

- 返迴路徑上的TCP SYN-ACK封包會以ASP drop reason tcp-not-syn 遭捨棄。
- 新TCP作業階段不會顯示在FTD連線表中。
- 高ASP捨棄計數器的累積速度很快，如該輸出在功能啟用後約10分鐘捕獲的圖所示：

```
<#root>
device#

show asp drop


Frame drop:
 Flow is denied by configured rule (acl-drop)                                  1

 First TCP packet not SYN (tcp-not-syn)                                    34802


 TCP RST/FIN out of order (tcp-rstfin-ooo)                                     4
 Dst MAC L2 Lookup Failed (dst-l2_lookup-fail)                               995
 Dropped pending packets in a closed socket (np-socket-closed)                 3
 TCP Proxy probe reset injected (tcp-proxy-probe-rst-injected)                 1
 TCP Proxy probe receive drop (tcp-proxy-probe-tcp-probe-drop)                 1
```

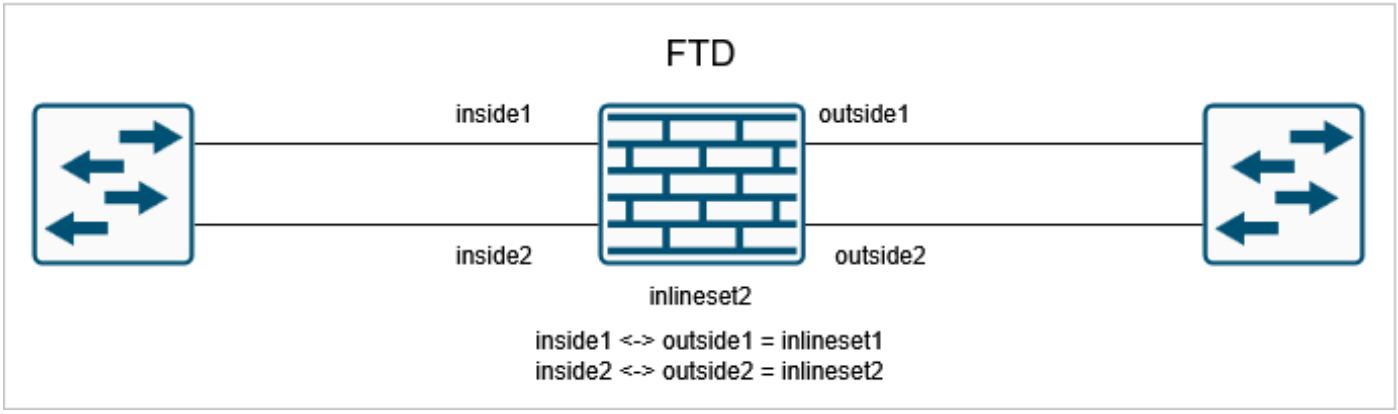
```
 Blocked or blacklisted by the reputation preprocessor (reputation)           1

Last clearing: 16:50:21 CEST Oct 24 2026 by enable_1
```

環境

- 平台:Cisco Firepower 4115。其他平台也可能受到影響。
- FTD軟體版本：7.6.4.其他軟體版本也可能會受到影響。
- FMC軟體版本：10.1.0.其他軟體版本也可能會受到影響。
- 具有內嵌介面集的FTD。
- FTD至少有兩個內嵌介面對：inlineset1和inlineset2（或有兩個不同的FTD，各有一個內嵌集）。
- 環境中存在非對稱流量：TCP SYN會透過outside1介面進入，而對應的TCP SYN-ACK會透過同一FTD裝置上的outside2介面返回。
- FTD上啟用TSID功能。

拓撲



解析

建議透過內嵌FTD介面停止tcp-not-syn捨棄和復原TCP連線的解決方案是停用TSID中的「Enhanced application and URL Detection」選項。這允許TCP狀態旁路在內聯介面集上保持活動狀態，這是適應環境中的非對稱流量所必需的。

在FMC中禁用「增強型應用和URL檢測」

導覽至：策略>訪問控制> [您的訪問控制策略] >高級> TLS伺服器身份發現。取消選中或停用「Enhanced application and URL Detection」複選框，然後將策略部署到受影響的FTD裝置。

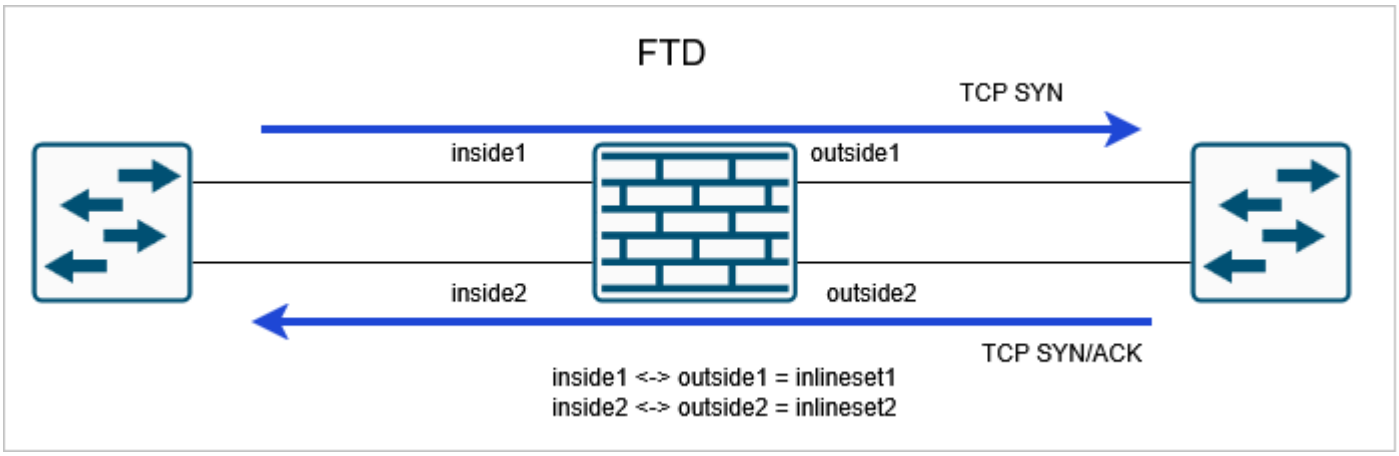
禁用此功能後，新的會話將顯示在連線表中，確認TCP連線是否成功完成了三次握手。

附註：禁用TSID後，FTD無法再在TLS 1.3會話中看到伺服器證書。應用規則和URL規則匹配加密流量時流量的準確性較低。

原因

tcp-not-syn drops的根本原因在於FTD中內嵌介面集的TLS伺服器身分探索功能和TCP狀態略過之間的不相容性。

預設情況下，對於透過FTD上內嵌介面的流量，會啟用TCP狀態略過。TCP狀態略過設計為允許非對稱流量（其中TCP連線的轉送和返迴路徑可以經過不同的介面甚至不同的裝置）通過，而不需執行FTD強制執行嚴格的TCP狀態追蹤。在存在路由不對稱的環境中，這是必要行為：

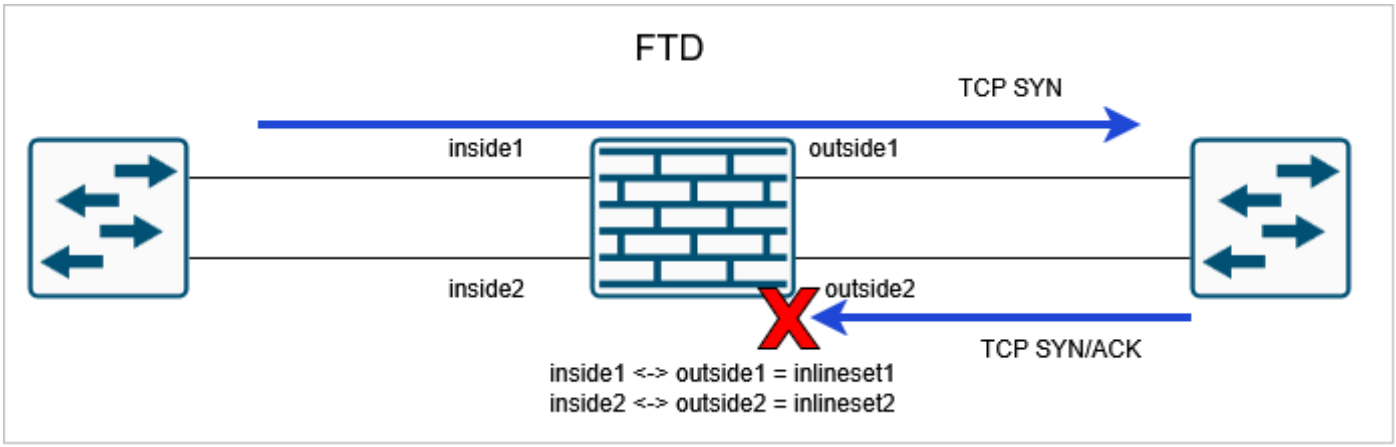


停用TSID時，透過FTD內嵌集的非對稱TCP流。

但是，當啟用其中任一功能時，FTD系統都會覆寫TCP狀態略過，並開始在內嵌介面流量上執行完整的TCP狀態檢查：

- TLS Server Identity Discovery下的「Enhanced application and URL Detection」選項。
- 任何活動的TLS/SSL解密策略。

一旦執行TCP狀態檢查，FTD會追蹤完整的TCP交握序列。在具有非對稱路由的環境中(例如，TCP SYN封包是透過outside1介面退出，但對應的TCP SYN-ACK透過同一裝置上的outside介面返回),FTD不會將SYN-ACK識別為屬於已知的、追蹤的TCP作業階段。由於SYN-ACK到達的介面與預期的不同，且在該介面上未看到對應的SYN，因此FTD將其分類為未知連線的非SYN封包，並使用ASP捨棄原因tcp-not-syn將其捨棄。



啟用TSID時，通過FTD內嵌集的非對稱TCP流。

相關內容

- 思科錯誤ID CSCwp84746 — 文檔：TLS伺服器身份發現與內嵌集介面上的TCP狀態旁路不相容
- 思科錯誤ID CSCwx42897 — DOC:TLS伺服器身份發現會覆蓋內嵌集介面上的TCP狀態旁路，導致TCP流量被丟棄(tcp-not-syn)
- 思科錯誤ID CSCwx42901 — 啟用「早期應用檢測和URL分類」(TSID)時新增警告，表示在內嵌集介面上禁用TCP狀態略過

- Cisco文檔 — TCP狀態繞行指南（包括TLS伺服器身份發現限制）
- 案例研究 — 通過內嵌集的非對稱流量
- 思科技術說明 — 如何生成FTD和FMC故障排除捆綁包
- 思科技術支援與下載

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）。