

解釋Firepower威脅防禦TCP連線標誌 (連線建立和拆卸)

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[排除TCP連線故障](#)

[FTD TCP連線旗標](#)

[TCP連線標誌值](#)

簡介

本檔案介紹如何透過Firepower威脅防禦(FTD)對TCP連線進行疑難排解。

必要條件

需求

思科建議您瞭解以下主題：

- 瞭解TCP通訊協定的基本知識。
- FTD CLI的基本知識。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

排除TCP連線故障

對透過FTD的TCP連線進行排解疑難時，每個連線顯示的連線旗標會提供透過FTD的TCP連線狀態的豐富資訊。此資訊可用於排除FTD的問題以及網路中其他地方的問題。

Disclaimer: The information in this document was created based on FTD devices on version 7.0 in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

由於所有FTD介面的安全等級均為0，因此介面的順序如下 `show conn` 輸出基於介面編號。具體而言，首先顯示具有更高虛擬平台介面編號(VPIF)的介面。

Disclaimer : The **show conn** output can be too long, hence it is recommended to use 'terminal pager' or write into a file saved in disk0: such as 'show conn | redirect filename.txt'

```
firepower# show conn
3 in use, 22 most used
Inspect Snort:
preserve-connection: 3 enabled, 0 in effect, 22 most enabled, 0 most in effect
```

```
TCP ISP2 192.168.50.14:35518 Inside 192.168.45.130:22, idle 0:10:00, bytes 7164, flags UIO N1
TCP ISP2 192.168.50.14:80 Inside 192.168.45.130:54554, idle 0:00:13, bytes 0, flags U N1
TCP Inside 192.168.45.130:34070 ISP1 10.31.104.78:3128, idle 0:00:02, bytes 1187822, flags UIO
N1
```

您可以從的輸出中看到介面VPIF值 show interface detail指令。

```
firepower# show interface detail | i Interface number is|Interface
Interface GigabitEthernet0/0 "ISP1", is up, line protocol is up
Control Point Interface States:
  Interface number is 3
Interface config status is active
Interface state is active
Interface GigabitEthernet0/1 "Inside", is up, line protocol is up
Control Point Interface States:
  Interface number is 4
Interface config status is active
Interface state is active
Interface GigabitEthernet0/2 "DMZ", is up, line protocol is up
Control Point Interface States:
  Interface number is 5
Interface config status is active
Interface state is active
Interface GigabitEthernet0/3 "ISP2", is up, line protocol is up
Control Point Interface States:
  Interface number is 6
Interface config status is active
Interface state is active
```

其 show conn long和 show conn detail命令提供有關連線的啟動器和響應器的詳細資訊。

```
firepower# show conn long
3 in use, 22 most used
Inspect Snort:
preserve-connection: 3 enabled, 0 in effect, 22 most enabled, 0 most in effect
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,
B - TCP probe for server certificate,
b - TCP state-bypass or nailed,
C - CTIQBE media, c - cluster centralized,
D - DNS, d - dump, E - outside back connection, e - semi-distributed,
F - initiator FIN, f - responder FIN,
G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,
i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
k - Skinny media, L - decap tunnel, M - SMTP data, m - SIP media
N - inspected by Snort (1 - preserve-connection enabled, 2 - preserve-connection in effect)
n - GUP, O - responder data, o - offloaded,
P - inside back connection, p - passenger flow
q - SQL*Net data, R - initiator acknowledged FIN,
R - UDP SUNRPC, r - responder acknowledged FIN,
T - SIP, t - SIP transient, U - up,
V - VPN orphan, v - M3UA W - WAAS,
w - secondary domain backup,
```

X - inspected by service module,
 x - per session, Y - director stub flow, y - backup stub flow,
 Z - Scansafe redirection, z - forwarding stub flow

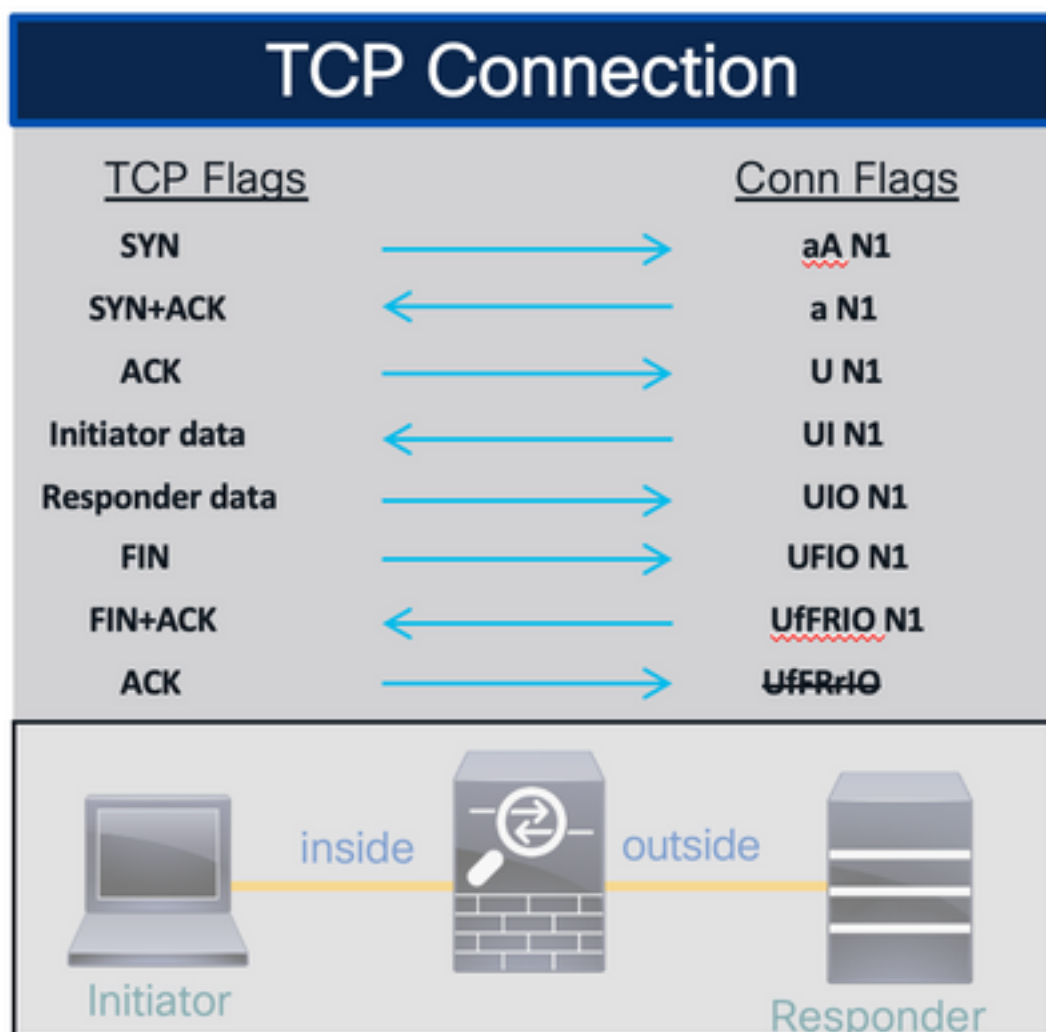
TCP ISP2: 192.168.50.14/35518 (192.168.50.14/35518) Inside: 192.168.45.130/22
 (192.168.45.130/22), flags UIO N1, idle 9m13s, uptime 9m17s, timeout 1h0m, bytes 7164
Initiator: 192.168.50.14, Responder: 192.168.45.130
 Connection lookup keyid: 168317598

TCP ISP2: 192.168.50.14/80 (192.168.50.14/80) Inside: 192.168.45.130/54554
 (192.168.45.130/54554), flags U N1, idle 0s, uptime 10s, timeout 1h0m, bytes 0
Initiator: 192.168.45.130, Responder: 192.168.50.14
 Connection lookup keyid: 168367034

TCP Inside: 192.168.45.130/34070 (192.168.45.130/34070) ISP1: 10.31.104.78/3128
 (10.31.104.78/3128), flags UIO N1, idle 0s, uptime 46s, timeout 1h0m, bytes 617331
Initiator: 192.168.45.130, Responder: 10.31.104.78
 Connection lookup keyid: 168227654

FTD TCP連線旗標

下表顯示TCP狀態機不同階段的FTD TCP連線旗標。在FTD中，傳入和傳出連線的連線旗標是相同的，因為安全級別一律為「0」。在FTD上使用 **show conn**命令可以看到這些旗標。



TCP連線標誌值

此表顯示了在收到資料包時刪除和新增的TCP連線標誌。

Flags REMOVED upon Receipt of Packet	a	Awaiting Initiator ACK to SYN
	A	Awaiting Responder ACK to SYN
Flags ADDED upon Receipt of Packet	U	Up - 3-way Handshake Complete
	I	Received Initiator Data
	O	Received Responder Data
	F	Received Initiator FIN
	f	Received Responder FIN
	R	Received Initiator ACK to FIN
	N1	Inspected by Snort with preserve-connection enabled
	N2	Inspected by Snort with preserve-connection in effect

要檢視連線中所有可能的標誌，請使用 **show conn detail** 命令。

```
firepower# show conn detail
1 in use, 22 most used
Inspect Snort:
preserve-connection: 1 enabled, 0 in effect, 22 most enabled, 0 most in effect
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,
B - TCP probe for server certificate,
b - TCP state-bypass or nailed,
C - CTIQBE media, c - cluster centralized,
D - DNS, d - dump, E - outside back connection, e - semi-distributed,
F - initiator FIN, f - responder FIN,
G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,
i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
k - Skinny media, L - decap tunnel, M - SMTP data, m - SIP media
N - inspected by Snort (1 - preserve-connection enabled, 2 - preserve-connection in effect)
n - GUP, O - responder data, o - offloaded,
P - inside back connection, p - passenger flow
q - SQL*Net data, R - initiator acknowledged FIN,
R - UDP SUNRPC, r - responder acknowledged FIN,
T - SIP, t - SIP transient, U - up,
V - VPN orphan, v - M3UA W - WAAS,
w - secondary domain backup,
X - inspected by service module,
x - per session, Y - director stub flow, y - backup stub flow,
Z - Scansafe redirection, z - forwarding stub flow
```

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）。