解释Firepower威胁防御TCP连接标志（连接建立和拆卸）

目录

简介

本文档介绍如何通过Firepower威胁防御(FTD)排除TCP连接故障。

先决条件

要求

Cisco 建议您了解以下主题：

- TCP通信协议基础知识。
- FTD CLI的基本知识。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

排除TCP连接故障

对通过FTD的TCP连接进行故障排除时，为每个连接显示的连接标志提供了大量有关通过FTD的TCP连接状态的信息。此信息可用于对FTD的问题以及网络中其他位置的问题进行故障排除。

```
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.
```

由于所有FTD接口的安全级别均为0，因此接口在 show conn 输出基于接口编号。具体而言，首先显示虚拟平台接口编号(VPIF)较高的接口。

```
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
```

您可以从的输出中看到接口VPIF值 show interface detail 命令。

```
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
```

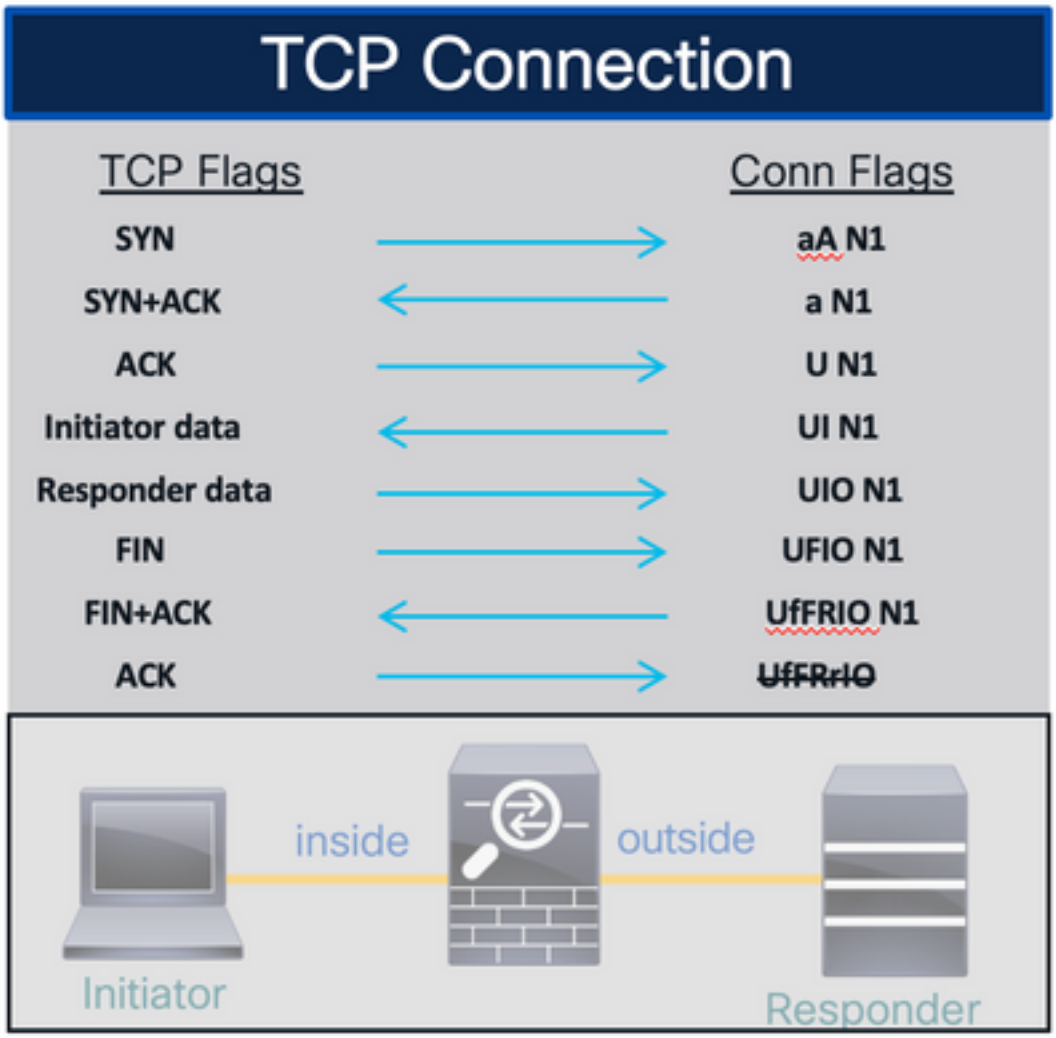
此 show conn long和 show conn detail命令提供有关连接的发起方和响应方的详细信息。

```
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
```

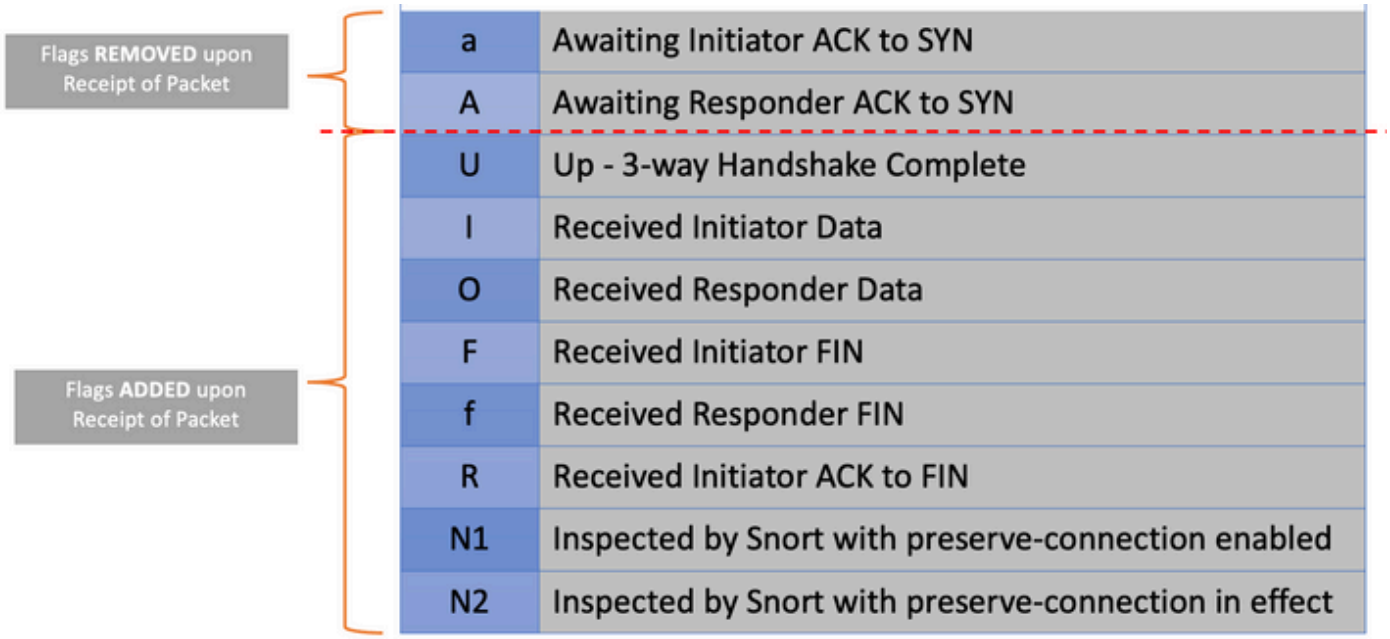
FTD TCP连接标志

此表显示了TCP状态机不同阶段的FTD TCP连接标志。在FTD中，入站和出站连接的连接标志相同，因为安全级别始终为“0”。 在FTD上使用 **show conn**命令可以查看这些标志。



TCP连接标志值

此表显示接收数据包时删除和添加的TCP连接标志。



要查看连接中所有可能的标志，请使用 **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
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。