

Interpreteer de vlaggen van de TCP-verbinding van de Verdediging van de Firepower Threat Defense (Connection Build-Up en Teardown)

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[TCP-verbindingen oplossen](#)

[FTD TCP-verbindingsvlaggen](#)

[TCP-verbindingsvlagwaarden](#)

Inleiding

Dit document beschrijft hoe u TCP-verbindingen kunt oplossen via Firepower Threat Defence (FTD).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van het TCP-communicatieprotocol.
- Basiskennis van de FTD CLI.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

TCP-verbindingen oplossen

Wanneer u TCP-verbindingen via de FTD verhelpt, verschaft de verbindingsvlaggen die voor elke verbinding worden weergegeven een schat aan informatie over de status van TCP-verbindingen via de FTD. Deze informatie kan worden gebruikt om problemen met de FTD op te lossen, evenals problemen elders in het netwerk.

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.

Aangezien alle FTD-interfaces een beveiligingsniveau van 0 hebben, wordt de interfacevolgorde in de `show conn` de output is gebaseerd op het interfacenummer. In het bijzonder wordt de interface met een hoger Virtual Platform Interface Number (VPIF) als eerste weergegeven.

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
```

U kunt de interface VPIF waarde van de output van zien `show interface detail` uit.

```
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
```

Het `show conn long` en `show conn detail` opdrachten geven informatie over de Initiator en de Responder van de verbinding.

```
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

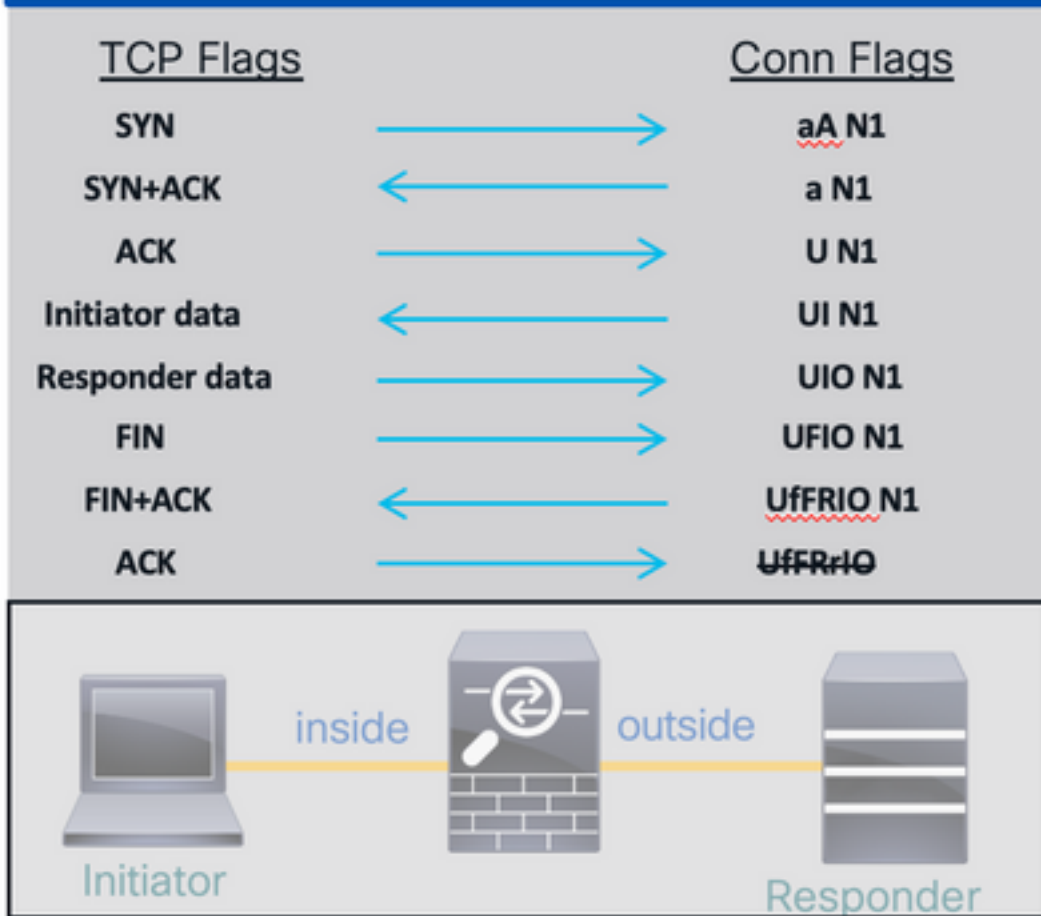
Initiator: 192.168.45.130, Responder: 10.31.104.78

Connection lookup keyid: 168227654

FTD TCP-verbindingvlaggen

Deze tabel toont de FTD TCP Connection-vlaggen in verschillende stadia van de TCP state machine. In FTD zijn de verbindingvlaggen hetzelfde voor inkomende en uitgaande verbindingen, aangezien de veiligheidsniveaus altijd '0' zijn. Deze vlaggen zijn te zien met de opdracht **show conn** op de FTD.

TCP Connection



TCP-verbindingvlagwaarden

Deze tabel toont de TCP-verbindingvlaggen die worden verwijderd en toegevoegd na ontvangst van een pakket.

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

Om alle mogelijke vlaggen in een verbinding te bekijken gebruik de opdracht **show conn detail**.

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.