Interpretare i flag di connessione TCP di Firepower Threat Defense (attivazione e disattivazione della connessione)

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi alle connessioni TCP con Firepower Threat Defense (FTD).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base del protocollo di comunicazione TCP.
- Conoscenze base della CLI FTD.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Risoluzione dei problemi relativi alle connessioni TCP

Quando si risolvono i problemi delle connessioni TCP tramite l'FTD, i flag di connessione mostrati per ciascuna connessione forniscono una serie di informazioni sullo stato delle connessioni TCP tramite l'FTD. Queste informazioni possono essere usate per risolvere i problemi con l'FTD, così come i problemi in altre parti della rete.

```
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.
```

Poiché tutte le interfacce FTD hanno un livello di sicurezza 0, l'ordine dell'interfaccia nel show conn l'output è basato sul numero dell'interfaccia. In particolare, viene mostrata per prima l'interfaccia con un numero VPIF (Virtual Platform Interface Number) più elevato.

```
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
```

È possibile visualizzare il valore VPIF dell'interfaccia dall'output di show interface detail

```
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
```

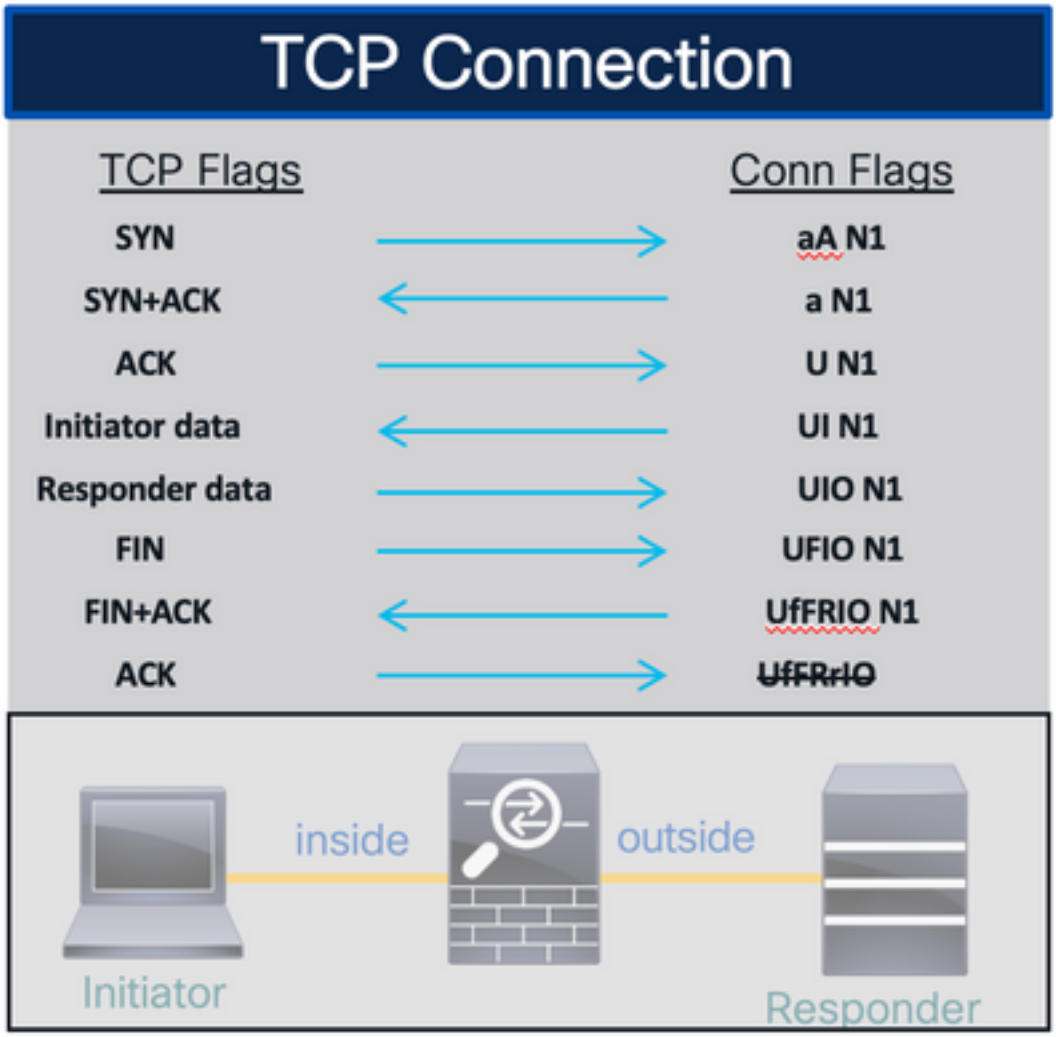
OSPF (Open Shortest Path First) show conn longe show conn detailI comandi forniscono dettagli sull'iniziatore e sul risponditore della connessione.

```
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
```

Flag di connessione TCP FTD

In questa tabella vengono mostrati i flag di connessione TCP FTD nelle diverse fasi della macchina a stati TCP. In FTD, i flag di connessione sono gli stessi per le connessioni in entrata e in uscita, poiché i livelli di protezione sono sempre '0'. Questi flag possono essere visualizzati con il comando **show conn** sull'FTD.



Valori flag connessione TCP

Nella tabella vengono mostrati i flag di connessione TCP che vengono rimossi e aggiunti alla ricezione di un pacchetto.

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

Per visualizzare tutti i possibili flag in una connessione, utilizzare il comando **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
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).