Interpretación de los indicadores de conexión TCP de Firepower Threat Defence (compilación y eliminación de conexiones)

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Solucionar problemas de conexiones TCP](#)
[Indicadores de conexión TCP de FTD](#)
[Valores del indicador de conexión TCP](#)

Introducción

Este documento describe cómo resolver problemas de conexiones TCP a través de Firepower Threat Defence (FTD).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico del protocolo de comunicación TCP.
- Conocimiento básico de la CLI de FTD.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Solucionar problemas de conexiones TCP

Cuando se solucionan problemas de conexiones TCP a través del FTD, los indicadores de conexión que se muestran para cada conexión proporcionan una gran cantidad de información sobre el estado de las conexiones TCP a través del FTD. Esta información se puede utilizar para solucionar problemas con el FTD, así como problemas en otras partes de la red.

```
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.
```

Dado que todas las interfaces FTD tienen un nivel de seguridad de 0, el orden de la interfaz en el show conn el resultado se basa en el número de interfaz. Específicamente, la interfaz con un número de interfaz de plataforma virtual (VPIF) más alto se muestra en primer lugar.

```
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
```

Puede ver el valor VPIF de la interfaz desde el resultado de show interface detailcomando.

```
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
```

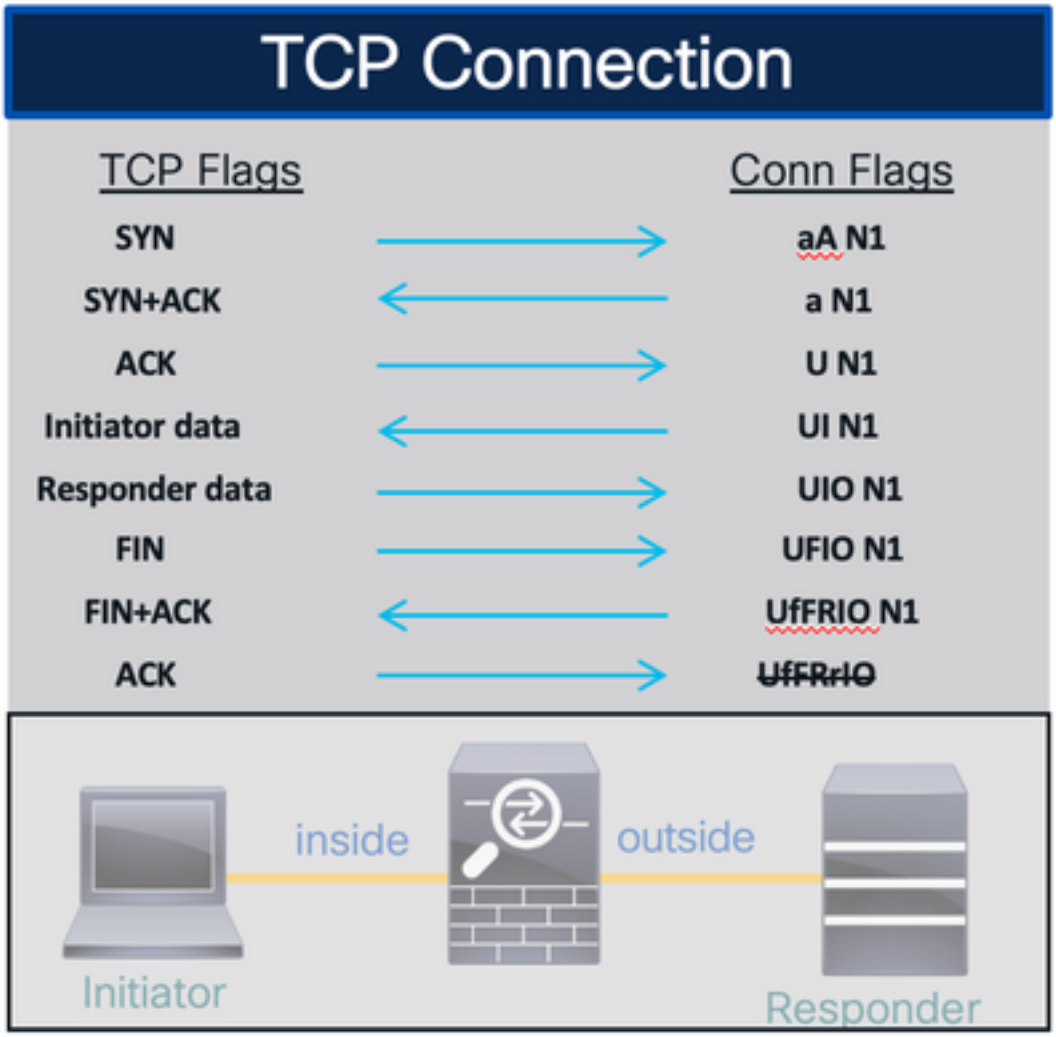
show conn longy show conn detailproporcionan detalles sobre el iniciador y el respondedor de la conexión.

```
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
```

Indicadores de conexión TCP de FTD

Esta tabla muestra los indicadores de conexión TCP de FTD en diferentes etapas de la máquina de estado TCP. En FTD, los indicadores de conexión son los mismos para las conexiones entrantes y salientes, ya que los niveles de seguridad son siempre '0'. Estos indicadores se pueden ver con el comando **show conn** en el FTD.



Valores del indicador de conexión TCP

Esta tabla muestra los indicadores de conexión TCP que se eliminan y se agregan al recibir un paquete.

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

Para ver todos los indicadores posibles en una conexión, utilice el 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
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).