

Interpretar os sinalizadores de conexão TCP do Firepower Threat Defense (Compilação e Desmontagem da Conexão)

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Solucionar problemas de conexões TCP](#)

[Sinalizadores de Conexão TCP FTD](#)

[Valores de Sinalizador de Conexão TCP](#)

Introduction

Este documento descreve como solucionar problemas de conexões TCP através do Firepower Threat Defense (FTD).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico do Protocolo de Comunicação TCP.
- Conhecimento básico da CLI de FTD.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Solucionar problemas de conexões TCP

Quando você soluciona problemas de conexões TCP por meio do FTD, os sinalizadores de conexão mostrados para cada conexão fornecem uma grande quantidade de informações sobre o estado das conexões TCP por meio do FTD. Essas informações podem ser usadas para solucionar problemas com o FTD, bem como problemas em outros locais da rede.

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.

Como todas as interfaces FTD têm um Nível de segurança 0, a ordem das interfaces no `show conn` a saída é baseada no número da interface. Especificamente, a interface com um número de interface de plataforma virtual (VPIF) maior é mostrada primeiro.

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
```

Você pode ver o valor VPIF da interface na saída de `show interface detail` comando.

```
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
```

O `show conn long` e `show conn detail` fornecem detalhes sobre o Iniciador e o Respondente da conexão.

```
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

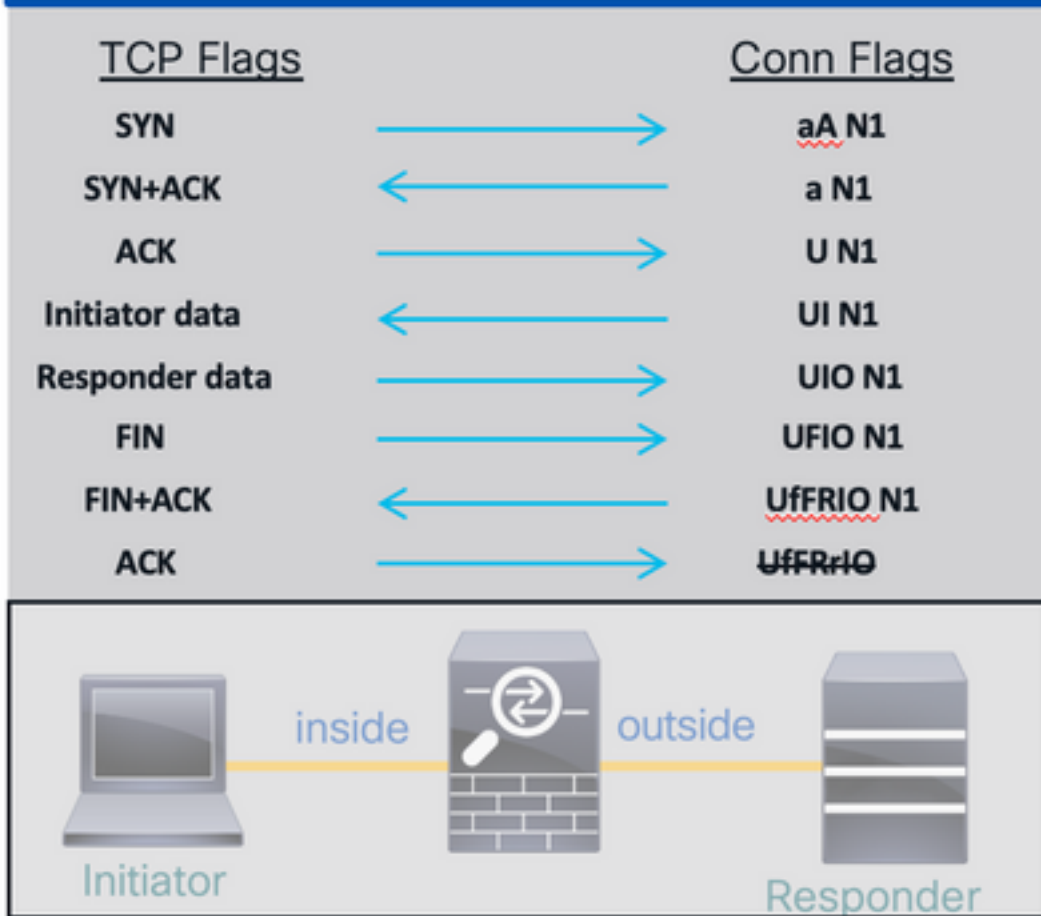
Initiator: 192.168.45.130, Responder: 10.31.104.78

Connection lookup keyid: 168227654

Sinalizadores de Conexão TCP FTD

Esta tabela mostra os sinalizadores de Conexão TCP de FTD em diferentes estágios da máquina de estado TCP. No FTD, os sinalizadores de conexão são os mesmos para conexões de entrada e saída, já que os níveis de segurança são sempre '0'. Esses sinalizadores podem ser vistos com o comando **show conn** no FTD.

TCP Connection



Valores de Sinalizador de Conexão TCP

Esta tabela mostra os Sinalizadores de Conexão TCP que são removidos e adicionados após o recebimento de um pacote.

Flags REMOVED upon Receipt of Packet	Flag	Description
[REMOVED]	a	Awaiting Initiator ACK to SYN
	A	Awaiting Responder ACK to SYN
[ADDED]	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 visualizar todas as flags possíveis em uma conexão, use o 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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.