

# Firewall seguro FTD Bloqueo de memoria Agotamiento que causa caídas de tráfico

## Contenido

---

## Problema

La pérdida intermitente de tráfico y la interrupción del routing se producen en un FTD Secure Firewall 2110 mediante el protocolo de routing de gateway interior mejorado (EIGRP). Esto provoca caídas de adyacencia y la pérdida de conectividad a Internet. Los síntomas se correlacionaron con el agotamiento del bloque de memoria (tamaño de bloque 80 y 9472), lo que resultó en caídas de paquetes de ruta de datos e impacto en el plano de control. Además, no se genera ningún archivo crash o core para el problema, ya que no se activa ningún reinicio.

El agotamiento del bloque de memoria hace que la unidad FTD detenga el procesamiento del tráfico.

```
<#root>
```

```
firepower#
```

```
show blocks
```

| SIZE | MAX  | LOW  | CNT  | FAILED |
|------|------|------|------|--------|
| 0    | 2700 | 2650 | 2700 | 0      |
| 4    | 200  | 199  | 200  | 0      |

```
80 24000 0 0 2200668
```

|      |      |      |      |   |
|------|------|------|------|---|
| 256  | 6072 | 3011 | 3178 | 0 |
| 1550 | 7386 | 4013 | 4719 | 0 |
| 2048 | 600  | 572  | 600  | 0 |
| 2560 | 900  | 889  | 900  | 0 |
| 4096 | 100  | 100  | 100  | 0 |
| 8192 | 100  | 97   | 100  | 0 |

```
9472 10000 0 2668 1
```

|       |     |     |     |   |
|-------|-----|-----|-----|---|
| 16384 | 100 | 100 | 100 | 0 |
| 65664 | 16  | 16  | 16  | 0 |

Las caídas de ASP en el FTD mostraron grandes recuentos de caídas "Dispatch queue tail drops (dispatch-queue-limit)":

<#root>

firepower#

**show asp drop**

Frame drop:

|                                                         |          |
|---------------------------------------------------------|----------|
| First TCP packet not SYN (tcp-not-syn)                  | 12357166 |
| Packet is blacklisted by snort (snort-blacklist)        | 1159498  |
| Fragment reassembly failed (fragment-reassembly-failed) | 53865    |

|                                                         |                |
|---------------------------------------------------------|----------------|
| <b>Dispatch queue tail drops (dispatch-queue-limit)</b> | <b>1582611</b> |
|---------------------------------------------------------|----------------|

También hay muchos tiempos de espera de reensamblado de fragmentos:

<#root>

firepower#

**show fragment**

Interface: outside

Configuration: Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual  
Run-time stats: Queue: 0, Full assembly: 1916508

**Drops:**

Size overflow: 0,

**Timeout: 6217,**

Chain overflow: 0, Fragment queue threshold exceeded: 47611,  
Small fragments: 0, Invalid IP len: 0,  
Reassembly overlap: 0, Fraghead alloc failed: 0,  
SGT mismatch: 0, Block alloc failed: 0,  
Invalid IPV6 header: 0, Passenger flow assembly failed: 0  
Cluster reinsert collision: 0

Todos los bloques asignados muestran la misma asignación e indican el impacto del defecto de ID de bug de Cisco CSCws19823. (ejecute el comando `terminal pager 20` antes de ejecutar para limitar la salida)

<#root>

firepower#

**show blocks assigned**

Class size 2, size 80

| Block              | allocd_by          | freed_by           | data size | alloccnt | dup_cnt | oper loc |
|--------------------|--------------------|--------------------|-----------|----------|---------|----------|
| 0xa800000100058c80 | 0x000000aaad8556ac | 0x000000aaad2cefb8 | 183       | 17310    | 0       |          |

**alloc cvmx\_api\_pdts\_send\_to\_host**

|                    |                    |                    |     |      |   |  |
|--------------------|--------------------|--------------------|-----|------|---|--|
| 0xa800000100059400 | 0x000000aaad8556ac | 0x000000aaad2cefb8 | 183 | 3748 | 0 |  |
|--------------------|--------------------|--------------------|-----|------|---|--|

**alloc cvmx\_api\_pdts\_send\_to\_host**

|                    |                    |                    |     |       |   |  |
|--------------------|--------------------|--------------------|-----|-------|---|--|
| 0xa800000100059b80 | 0x000000aaad8556ac | 0x000000aaad2cefb8 | 182 | 74639 | 0 |  |
|--------------------|--------------------|--------------------|-----|-------|---|--|

**alloc cvmx\_api\_pdts\_send\_to\_host**

|                    |                    |                    |     |       |   |  |
|--------------------|--------------------|--------------------|-----|-------|---|--|
| 0xa80000010005a300 | 0x000000aaad8556ac | 0x000000aaad7cf0e8 | 183 | 23610 | 0 |  |
|--------------------|--------------------|--------------------|-----|-------|---|--|

**alloc cvmx\_api\_pdts\_send\_to\_host**

|                    |                    |                    |     |       |   |  |
|--------------------|--------------------|--------------------|-----|-------|---|--|
| 0xa80000010005aa80 | 0x000000aaad8556ac | 0x000000aaad2cefb8 | 183 | 40731 | 0 |  |
|--------------------|--------------------|--------------------|-----|-------|---|--|

**alloc cvmx\_api\_pdts\_send\_to\_host**

Una revisión de las conexiones en el FTD confirma que la mayoría de las conexiones entrantes son tráfico SMB (TCP/445) en la interfaz FTD. (ejecute `terminal pager 20` antes de ejecutar para limitar la salida)

<#root>

firepower#

**show conn detail**

TCP outside: 10.X.X.49/55970 inside: 10.X.X.73/

445

,  
flags UIO N1, idle 1m13s, uptime 1h52m, timeout 1h0m, bytes 163283, xlate id 0xffe0384b00, flow id  
Initiator: 10.X.X.49, Responder: 10.X.X.73  
Connection lookup keyid: 3616633230  
TCP outside: 10.X.X.72/57775 inside: 10.X.X.214/

445

,  
flags UIO N1, idle 5s, uptime 2h6m, timeout 1h0m, bytes 182005, xlate id 0xffe0384b00, flow id 2202  
Initiator: 10.X.X.72, Responder: 10.X.X.214  
Connection lookup keyid: 3661674758  
TCP outside: 10.X.X.131/54313 inside: 10.X.X.71/

445

,  
flags UIO N1, idle 29s, uptime 9m35s, timeout 1h0m, bytes 26205, xlate id 0xffe0384b00, flow id 224  
Initiator: 10.X.X.131, Responder: 10.X.X.71  
Connection lookup keyid: 1202806582

## Entorno

- Cisco Secure Firewall FPR2110-NGFW-K9 Firewall Threat Defence (FTD) versión 7.4.3 (visto por primera vez)
- El firewall está inspeccionando el tráfico SMB (TCP/445)

## Resolución

### Solución alternativa inmediata

1. Configure una política de filtro previo para omitir la inspección del tráfico SMB en todas las interfaces relevantes, en particular la interfaz FTD donde el tráfico SMB entra en el firewall.

```
access-list CSM_FW_ACL_ line 4 remark rule-id 268459032: PREFILTER POLICY: FTD Prefilter Policy
access-list CSM_FW_ACL_ line 5 remark rule-id 268459032: RULE: SMB-FastPath
access-list CSM_FW_ACL_ line 6 advanced trust tcp ifc outside any any eq 445 rule-id 268459032 eve
```

## 2. Borrar conexiones SMB existentes y restablecer contadores de bloques

```
clear conn port 445 all
clear blocks
```

## 3. Ejecute este comando para monitorear los incrementos de bloque fallidos:

```
show blocks
```

## Corrección permanente

1. Actualice a Cisco Secure Firewall Threat Defence versión 7.0.9, 7.2.11, 7.4.4 o 7.6.0.
2. Después de actualizar a la versión fija, monitoree la utilización del bloque de memoria para confirmar la estabilización y verifique que no se produzca más agotamiento del bloque de memoria.
3. Una vez actualizado a la versión fija, el tráfico SMB se puede eliminar de forma segura del prefiltro si se desea, ya que el defecto subyacente se ha resuelto.

## Comandos de Troubleshooting Utilizados

Estos comandos de diagnóstico se utilizaron para analizar los patrones de asignación de bloques de memoria:

```
show blocks | redirect disk0:/show.blocks.txt
show blocks pool 80 dump | redirect disk0:/show.block.pool.80.dump.txt
show blocks queue history detail | redirect disk0:/show.blocks.Q.history.detail.txt
show blocks queue history core-local | redirect disk0:/show.blocks.Q.hist.core-local.txt
show blocks old core-local | redirect disk0:/show.blocks.old.core-local.txt
```

```
show blocks exhaustion snapshot | redirect disk0:/show.blocks.exhaustion.shapshot.txt
show blocks exhaustion history | redirect disk0:/show.blocks.exhaustion.history.txt
show blocks assigned | redirect disk0:/show.blocks.assigned.txt
```

## Causa

El problema se debe a un defecto de software conocido, Cisco bug ID CSCws19823, en Cisco Secure Firewall Threat Defense, donde los altos volúmenes de tráfico SMB inspeccionado (TCP/445) podrían conducir a un agotamiento del tamaño de bloque de memoria 80, lo que resultaría en caídas de paquetes de ruta de datos y efectos secundarios como inestabilidad EIGRP y pérdida de tráfico. El defecto se produce cuando el tráfico SMB se somete a una inspección completa.

## Contenido relacionado

- [ID de error de Cisco CSCws19823: agotamiento de bloques 80, 1550 y 9472 observado en ASA/FTD 2100 cuando se envía tráfico multicanal SMB](#)
- [Soporte técnico y descargas de Cisco](#)

#### 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).