

Esaurimento blocco memoria FTD firewall protetto che causa la perdita di traffico

Sommario

Problema

Perdita intermittente del traffico e interruzioni del routing su un FTD Secure Firewall 2110 utilizzando il protocollo EIGRP (Enhanced Interior Gateway Routing Protocol). Questo porta a cali di dipendenza e perdita di connettività Internet. Sintomi correlati all'esaurimento dei blocchi di memoria (dimensioni dei blocchi 80 e 9472), con conseguenti perdite di pacchetti di datapath e impatto sul control plane. Inoltre, non viene generato alcun file di arresto anomalo o di base per il problema poiché non viene attivato il riavvio.

L'esaurimento del blocco di memoria provoca l'arresto dell'unità FTD dell'elaborazione del traffico.

<#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

Le interruzioni ASP sull'FTD hanno mostrato conteggi elevati per le interruzioni "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

Dispatch queue tail drops (dispatch-queue-limit)	1582611
---	----------------

Sono inoltre disponibili numerosi timeout per il riassettaggio dei frammenti:

<#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

I blocchi assegnati mostrano tutti la stessa allocazione e indicano l'impatto del difetto Cisco, ID bug CSCws19823. (Eseguire il comando `terminal pager 20` prima di eseguire per limitare l'output)

<#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							

Un'analisi delle connessioni sull'FTD conferma che la maggior parte delle connessioni in entrata sono traffico SMB (TCP/445) sull'interfaccia FTD. (eseguire `terminal pager 20` prima dell'esecuzione per limitare l'output)

<#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 1  
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
```

Ambiente

- Cisco Secure Firewall FPR2110-NGFW-K9 Firewall Threat Defense (FTD) versione 7.4.3 (prima)
- Traffico SMB (TCP/445) ispezionato dal firewall

Risoluzione

Soluzione immediata

1. Configurare un criterio di prefiltro per ignorare l'ispezione del traffico SMB su tutte le interfacce rilevanti, in particolare l'interfaccia FTD in cui il traffico SMB entra nel 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. Cancella le connessioni SMB esistenti e reimposta i contatori dei blocchi

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

3. Eseguire questo comando per monitorare gli incrementi dei blocchi non riusciti:

```
show blocks
```

Correzione permanente

1. Eseguire l'aggiornamento a Cisco Secure Firewall Threat Defense versione 7.0.9, 7.2.1, 7.4.4 o 7.6.0.
2. Dopo l'aggiornamento alla versione fissa, monitorare l'utilizzo dei blocchi di memoria per confermare la stabilizzazione e verificare che non si verifichi un ulteriore esaurimento dei blocchi.
3. Una volta aggiornato alla versione fissa, il traffico SMB può essere rimosso in modo sicuro dal prefiltro, se lo si desidera, in quanto il difetto sottostante è stato risolto.

Comandi per la risoluzione dei problemi

Questi comandi diagnostici sono stati utilizzati per analizzare i modelli di allocazione dei blocchi di 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.snapshot.txt
```

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

Causa

Il problema è causato da un difetto software noto come Cisco bug ID CSCws19823 in Cisco Secure Firewall Threat Defense, dove volumi elevati di traffico SMB (TCP/445) ispezionato potrebbero causare l'esaurimento di dimensioni del blocco di memoria pari a 80, con conseguente perdita di pacchetti di datapath ed effetti secondari come l'instabilità EIGRP e la perdita di traffico. Il difetto si verifica quando il traffico delle PMI viene sottoposto a un'ispezione completa.

Contenuto correlato

- [ID bug Cisco CSCws19823 - riduzione dei blocchi 80, 1550 e 9472 rilevato su ASA/FTD 2100 quando viene inviato il traffico multicanale per PMI](#)
- [Supporto tecnico Cisco e download](#)

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).