

安全防火牆FTD記憶體塊耗盡導致流量丟棄

目錄

問題

使用增強型內部閘道路由通訊協定(EIGRP)的安全防火牆2110 FTD上會發生間歇性流量遺失和路由中斷。這會導致鄰接關係下降和Internet連線丟失。與記憶體塊耗盡（塊大小80和9472）相關的症狀，導致資料路徑資料包丟棄和控制平面影響。此外，由於未觸發重新啟動，因此不會針對此問題生成崩潰或核心檔案。

記憶體塊耗盡導致FTD裝置停止處理流量。

<#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

FTD上的ASP捨棄顯示「Dispatch queue tail drops(dispatch-queue-limit)」捨棄的計數較大：

```
<#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
---	----------------

此外，還存在許多碎片重組超時：

```
<#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
```

所有指派的區塊都顯示相同的分配結果，表示受到缺陷Cisco錯誤ID CSCws19823的影響。(執行之前，請執行terminal pager 20命令以限制輸出)

<#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_pdt_sen_to_host

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

alloc cvmx_api_pdt_sen_to_host

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

alloc cvmx_api_pdt_sen_to_host

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

alloc cvmx_api_pdt_sen_to_host

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

alloc cvmx_api_pdt_sen_to_host

檢查FTD上的連線可以確認大多數傳入連線是FTD介面上的SMB(TCP/445)流量。(執行之前運行終端
尋呼機20以限制輸出)

<#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
```

環境

- 思科安全防火牆FPR2110-NGFW-K9防火牆威脅防禦(FTD)版本7.4.3 (首次出現)
- 防火牆檢查的SMB(TCP/445)流量

解析

即時解決方法

1. 配置預過濾器策略以繞過所有相關介面上的SMB流量檢查，特別是SMB流量進入防火牆的FTD介面。

```
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. 清除現有SMB連線和重置塊計數器

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

3. 執行此命令以監控失敗的塊增量：

```
show blocks
```

永久修復

1. 升級到思科安全防火牆威脅防禦7.0.9、7.2.11、7.4.4或7.6.0版。
2. 升級至固定版本後，監控記憶體塊利用率以確認穩定性並驗證是否不再發生記憶體塊耗盡。
3. 升級到固定版本後，如有需要，可以從預過濾器安全地刪除SMB流量，因為已解決底層缺陷。
。

使用的疑難排解指令

以下診斷命令用於分析記憶體塊分配模式：

```
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
```

原因

此問題是由思科安全防火牆威脅防禦中的已知軟體缺陷Cisco bug ID CSCws19823引起的，在該缺陷中，大量檢查的SMB(TCP/445)流量可能導致記憶體塊大小80耗盡，導致資料路徑資料包丟棄以及次要影響（如EIGRP不穩定性和流量丟失）。當SMB流量進行完全檢查時，會出現該缺陷。

相關內容

- [思科錯誤ID CSCws19823 — 傳送SMB多通道流量時，ASA/FTD 2100上出現80、1550和9472塊耗盡](#)
- [思科技術支援與下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。