

安全防火墙FTD内存块耗尽导致流量丢弃

目录

问题

在使用增强型内部网关路由协议(EIGRP)的安全防火墙2110 FTD上出现间歇性流量丢失和路由中断。这会导致邻接中断和Internet连接中断。与内存块耗尽（块大小80和9472）相关的症状，导致数据路径数据包丢弃和控制平面影响。此外，由于未触发重启，因此不会针对此问题生成崩溃或核心文件。

内存块耗尽导致FTD单元停止处理流量。

<#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丢包显示“Dispatch queue tail drops(dispatch-queue-limit)”丢弃的计数较大：

```
<#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，还会出现很多分段重组超时：

```
<#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
```

分配的所有块都显示相同的分配表示受缺陷Cisco Bug ID CSCws19823的影响。（在执行之前运行 terminal pager 20命令以限制输出）

<#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_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							

对FTD上的连接进行检查可确认大多数传入连接是FTD接口上的SMB(TCP/445)流量。(执行之前运行终端 寻呼机20以限制输出)

<#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
```

环境

- 思科安全防火墙FPR2110-NGFW-K9防火墙威胁防御(FTD)版本7.4.3 (首次发现)
- 防火墙检查的SMB(TCP/445)流量

分辨率

即时解决方法

1. 配置预过滤器策略以绕过所有相关接口上的SMB流量检查，特别是SMB流量进入防火墙的FTD接口。

```
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. 清除现有SMB连接和重置块计数器

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

3. 执行此命令可监控失败的块增量：

```
show blocks
```

永久性修正

1. 升级到思科安全防火墙威胁防御版本7.0.9、7.2.11、7.4.4或7.6.0。
2. 升级到固定发行版后，监控内存块利用率以确认稳定性并确认不会发生进一步的内存块耗尽。
3. 升级到固定版本后，可以根据需要从预过滤器安全地删除SMB流量，因为基本缺陷已解决。

使用的故障排除命令

以下诊断命令用于分析内存块分配模式：

```
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

此问题是由思科安全防火墙威胁防御中的一个已知软件缺陷Cisco bug ID CSCws19823引起的，在

该缺陷中，大量检查的SMB(TCP/445)流量可能导致内存块大小耗尽80，导致数据路径数据包丢弃和二次影响，例如EIGRP不稳定和流量丢失。当SMB流量进行完全检查时，会出现此缺陷。

相关内容

- [Cisco Bug ID CSCws19823 — 发送SMB多通道流量时，ASA/FTD 2100上显示80、1550和9472块耗尽](#)
- [思科技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。