

보안 방화벽 FTD 메모리 블록 소진으로 트래픽 감소

목차

문제

EIGRP(Enhanced Interior Gateway Routing Protocol)를 사용하는 Secure Firewall 2110 FTD에서 간헐적인 트래픽 손실 및 라우팅 중단이 발생합니다. 이로 인해 드민턴이 저하되고 인터넷 연결이 끊깁니다. 메모리 블록 소진과 관련된 증상(블록 크기 80 및 9472)으로, 데이터 경로 패킷 삭제 및 컨트롤 플레인 영향이 발생합니다. 또한 재부팅이 트리거되지 않으므로 이 문제에 대한 크래시 또는 코어 파일이 생성되지 않습니다.

메모리 블록이 고갈되면 FTD 유닛에서 트래픽 처리를 중지합니다.

<#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

FTD의 ASP 삭제에서 "Dispatch queue tail drops (dispatch-queue-limit)" 삭제에 대한 개수가 많았습니다.

<#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
---	----------------

프래그먼트 재결합 시간 초과도 많습니다.

<#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

할당된 모든 블록은 결함 Cisco 버그 ID CSCws19823의 영향을 나타내는 동일한 할당을 표시합니

다. 출력을 제한하기 위해 실행하기 전에 terminal pager 20 명령을 실행하십시오.

<#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

FTD의 연결을 검토하면 수신 연결의 대부분이 FTD 인터페이스의 SMB(TCP/445) 트래픽임을 확인할 수 있습니다. (출력을 제한하기 위해 실행하기 전에 터미널 페이지 20 실행)

<#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 2202
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
```

환경

- Cisco Secure Firewall FPR2110-NGFW-K9 FTD(Firewall Threat Defense) 버전 7.4.3(처음 확인)
- 방화벽에서 검사 중인 SMB(TCP/445) 트래픽

해결

즉각적인 해결

1. 모든 관련 인터페이스, 특히 SMB 트래픽이 방화벽으로 들어가는 FTD 인터페이스에서 SMB 트래픽에 대한 검사를 우회하도록 사전 필터 정책을 구성합니다.

```
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. 기존 SMB 연결을 지우고 차단 카운터를 재설정합니다.

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

3. 이 명령을 실행하여 실패한 블록 증가를 모니터링합니다.

```
show blocks
```

영구 수정

1. Cisco Secure Firewall Threat Defense 버전 7.0.9, 7.2.11, 7.4.4 또는 7.6.0으로 업그레이드합니다.
2. 고정 릴리스로 업그레이드한 후 메모리 블록 사용률을 모니터링하여 안정화를 확인하고 추가 메모리 블록 소진이 발생하지 않는지 확인합니다.
3. 고정 버전으로 업그레이드한 후에는 기본 결함이 해결되었으므로 원하는 경우 SMB 트래픽을 사전 필터에서 안전하게 제거할 수 있습니다.

사용된 트러블슈팅 명령

다음 진단 명령을 사용하여 메모리 블록 할당 패턴을 분석했습니다.

```
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
```

원인

이 문제는 Cisco Secure Firewall Threat Defense에서 알려진 소프트웨어 결함 Cisco 버그 ID CSCws19823으로 인해 발생합니다. 이 경우 대량의 검사된 SMB(TCP/445) 트래픽이 메모리 블록 크기 80에 고갈되어 데이터 경로 패킷이 삭제되고 EIGRP 불안정 및 트래픽 손실과 같은 2차 영향이 발생할 수 있습니다. SMB 트래픽이 전체 검사를 받을 때 결함이 발생합니다.

관련 콘텐츠

- [Cisco 버그 ID CSCws19823 - 80, 1550 및 9472는 SMB 멀티채널 트래픽이 전송될 때 ASA/FTD 2100에서 나타나는 고갈 현상 차단](#)
- [Cisco 기술 지원 및 다운로드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.