Secure Firewall 1010 FTD 높은 메모리로 인해 트래픽 영향 발생

목차

문제

사용자는 로우엔드 플랫폼 Secure Firewall 1010에서 "Critical Data Plane memory"에 대한 상태 모니터 경고를 경험합니다. 이렇게 메모리 사용률이 높으면 사용자가 VPN에 연결할 수 없습니다. 또한 메모리 소진으로 인해 디바이스에 액세스할 수 없게 되고 제대로 작동하지 않을 수 있습니다.

재부팅 후에도 FTD에서 트래픽을 처리하지 않더라도 FTD 메모리는 즉시 높은 사용량으로 돌아갑니다.

<#root>

```
firepower# show memory

Free memory:          216990542 bytes ( 8%)

Used memory:         2487943528 bytes (92%)


-------------     ------------------
Total memory:        2704934070 bytes (100%)
```

메모리 사용량 세부 정보에는 DMA 풀에 예약된 대량의 메모리가 표시됩니다.

<#root>

```
firepower# show memory detail

Heap Memory:
   Free Memory:
      Heapcache Pool:                       85289152 bytes (  3% )
      Global Shared Pool:                    1675200 bytes (  0% )
      Message Layer Pool:                   14495776 bytes (  1% )
      Message Layer HB Pool:                  197712 bytes (  0% )
      System:                              125170870 bytes (  5% )
   Used Memory:
      Heapcache Pool:                      684365632 bytes ( 25% )
```

```
      Global Shared Pool:                  123629632 bytes (  5% )


Reserved (Size of DMA Pool):        1073741824 bytes ( 40% )


      Reserved for messaging:                2019296 bytes (  0% )
      Reserved for HB messaging:               64432 bytes (  0% )
      MMAP usage:                           39073816 bytes (  1% )
      System Overhead:                     555472872 bytes ( 21% )
-------------------------------------     ----------------
   Total Memory:                          2704934070 bytes ( 100% )
```

또한 ASP 삭제 출력은 Snort 프리프로세서에 의한 여러 개의 증분 삭제를 나타냅니다.

<#root>

```
firepower# show asp drop
.....

  Blocked or blacklisted by the firewall preprocessor (firewall)        14433080


  Blocked or blacklisted by the stream preprocessor (stream)               29325
  Blocked or blacklisted by the session preprocessor (session-preproc)       646
  Blocked or blacklisted by the IPS preprocessor (ips-preproc)                24
  Fragment reassembly failed (fragment-reassembly-failed)                    397
  Packet is blacklisted by snort (snort-blacklist)                       1812129
```

디바이스의 running-config 출력은 또한 높은 메모리에 기여하는 여러 AnyConnect 패키지를 나타낼 수 있습니다.

<#root>

```
firepower# show run | inc anyconnect

 anyconnect image disk0:/csm/cisco-secure-client-win-5.1.8.122-webdeploy-k9.pkg 1 regex "Windows"
 anyconnect image disk0:/csm/cisco-secure-client-macos-5.1.6.103-webdeploy-k9.pkg 2 regex "Mac OS"


 anyconnect profiles all-vpn disk0:/csm/all-vpn.xml
 anyconnect profiles iseposture disk0:/csm/ISEPosture.xml
 anyconnect enable
```

환경

- 제품: Cisco Secure Firewall 1010
- Cisco Secure Client(AnyConnect) 구성

해결

결함 Cisco 버그 ID CSCwc82675이 Firepower 버전 10.0.0에서 영구적으로 해결되었습니다.

해결 방법:

- Webvpn 캐시 비활성화
- 원치 않는 Anyconnect 클라이언트 패키지 삭제
- VPN 프로토콜을 SSL/TLS에서 IPSec으로 변경

원인

이 특정 문제는 결함 Cisco 버그 ID CSCwc82675으로 인해 발생합니다. Firepower 1010 플랫폼은 메모리 제약으로 인해 Secure Client(AnyConnect)를 실행할 때 알려진 제한이 있는 로우엔드 플랫폼이며, Cisco 버그 ID CSCwc82675에서 언급한 대로 여러 AnyConnect 패키지를 구성한 후 데이터 플레인 메모리가 높아질 수 있습니다. Firepower 1010에는 총 메모리 8GB가 프로비저닝되며 총 메모리 중 3GB를 트래픽 처리를 위해 LINA/ASA(DATAPATH)에 할당합니다. LINA는 트래픽 처리를 위해 일정 양의 메모리를 예약하며 시스템에 쉽게 릴리스하지 않기 때문에 이러한 디바이스는 일반적으로 향상된 메모리 사용량을 보여줍니다. 이러한 동작은 설계에 의한 것이며 더 나은 성능을 위해 의도한 것입니다. VPN 컨피그레이션에서 메모리 소비량은 약 40%가 DMA 풀에 할당되어 있으며, 이는 주로 VPN 작업에 사용됩니다. 시스템 오버헤드가 전체 메모리 사용량을 차지합니다. 트래픽을 처리하지 않더라도 VPN 컨피그레이션이 있는 Firepower 1010 플랫폼은 높은 메모리 사용량을 표시할 수 있습니다. 이러한 메모리 사용량은 트래픽이 방화벽에 유입된 후 최대 수준에 도달할 수 있습니다.

관련 콘텐츠

- Cisco 버그 ID CSCwc82675

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.