安全防火牆1010 FTD高記憶體導致流量影響

目錄

問題

在低端平台安全防火牆1010上，使用者會遇到針對「關鍵資料平面記憶體」的運行狀況監視器警告。這種高記憶體利用率會阻止使用者連線到VPN。裝置也可能因記憶體耗盡而無法訪問並停止正常工作。

即使重新開機後，FTD記憶體也會立即恢復為高使用率，即使FTD未處理流量也是如此。

<#root>

```
firepower# show memory

Free memory:         216990542 bytes ( 8%)

Used memory:        2487943528 bytes (92%)


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

記憶體使用詳細資訊顯示DMA池中預留的大量記憶體。

<#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% )
```

ASP丟棄輸出還指示Snort前處理器執行多次遞增丟棄。

<#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
```

裝置的運行配置輸出還可能指示多個導致高記憶體的AnyConnect軟體包。

<#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
```

環境

- 產品:思科安全防火牆1010
- 已配置Cisco Secure Client(AnyConnect)

解析

Firepower 10.0.0版中已永久解決缺陷Cisco錯誤ID CSCwc82675。

因應措施：

- 禁用Webvpn快取
- 刪除不需要的Anyconnect客戶端軟體包
- 將VPN協定從SSL/TLS更改為IPSec

原因

此特定問題是由思科錯誤ID CSCwc82675缺陷導致的。Firepower 1010平台是低端平台，在運行Secure Client(AnyConnect)時存在已知限制，因為其記憶體限制可能會在配置多個AnyConnect程式包(如思科錯誤ID CSCwc82675中所述)後導致高資料平面記憶體。Firepower 1010調配了8GB的總記憶體，並將3GB的總記憶體分配給LINA/ASA(DATAPATH)以進行流量處理。這些裝置通常顯示提升的記憶體使用率，因為LINA保留特定數量的記憶體以進行流量處理，但不會輕易將其釋放到系統。此行為是設計行為，旨在獲得更好的效能。對於VPN配置，記憶體消耗顯示大約40%分配給DMA池，該池主要保留用於VPN操作。系統開銷佔記憶體使用總量。即使不處理流量，具有VPN配置的Firepower 1010平台也可顯示更高的記憶體使用率。將流量引入防火牆後，此記憶體使用率可能會達到最高水準。

相關內容

- 思科錯誤ID CSCwc82675

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）。