セキュアファイアウォール1010 FTDの高メモリがトラフィックへの影響を引き起こす

内容

お問い合わせ内容

ローエンドプラットフォームのセキュアファイアウォール1010では、ヘルスモニタの警告「Critical Data Plane memory」が表示されます。この高いメモリ使用率により、ユーザはVPNに接続できません。また、メモリの枯渇により、デバイスにアクセスできなくなり、正常に機能しなくなる可能性があります。

リブート後でも、FTDがトラフィックを処理していなくても、FTDメモリはすぐに使用率の高い状態に戻ります。

<#root>

```
firepower# show memory

Free memory:         216990542 bytes ( 8%)

Used memory:        2487943528 bytes (92%)


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

メモリ使用量の詳細は、DMAプールで予約されている大量のメモリを示します。

<#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ドロップ出力は、Snortプリプロセッサによる多数のドロップの増加も示しています。

<#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
```

デバイスのrunning-config出力に、高メモリの一因となる複数のAnyConnectパッケージが示されている場合もあります。

<#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

- 製品：Cisco Secure Firewall 1010
- Cisco Secure Client(AnyConnect)が設定されている

解決策

不具合のCisco Bug ID CSCwc82675は、Firepowerバージョン10.0.0では永続的に解決されています。

回避策：

- Webvpnキャッシュの無効化
- 不要なAnyConnectクライアントパッケージの削除
- VPNプロトコルをSSL/TLSからIPSecに変更する

原因

この特定の問題は、不具合のCisco Bug ID CSCwc82675が原因で発生します。Firepower 1010プラットフォームは、Secure Client(AnyConnect)の実行時にメモリの制約が原因で既知の制限があるローエンドプラットフォームです。Cisco Bug ID CSCwc82675で説明されているように、複数のAnyConnectパッケージを設定した後でデータプレーンメモリが高くなる可能性があります。Firepower 1010は8 GBの総メモリでプロビジョニングされ、トラフィック処理用に総メモリの3 GBをLINA/ASA(DATAPATH)専用に割り当てます。これらのデバイスでは、LINAがトラフィック処理のために一定量のメモリを予約し、それをシステムに簡単に解放しないため、通常、メモリ使用量が増加します。この動作は設計によるものであり、より良いパフォーマンスを目的としています。VPN設定では、メモリ消費は約40 %がDMAプールに割り当てられていることを示します。これは主にVPN運用のために予約されています。システムのオーバーヘッドは、総メモリ使用量を占めます。トラフィックを処理しなくても、VPN構成のFirepower 1010プラットフォームでメモリ使用率が上昇することがあります。このメモリ使用量は、トラフィックがファイアウォールに入ると、最大レベルに達する可能性があります。

関連コンテンツ

- Cisco Bug ID CSCwc82675

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。