Sichere Firewall 1010 FTD - hoher Speicher verursacht Beeinträchtigung des Datenverkehrs

Inhalt

Problem

Die Benutzer erhalten eine Warnmeldung auf dem Systemmonitor für den "kritischen Datenebenenspeicher" auf der einfachen Plattform Secure Firewall 1010. Diese hohe Speichernutzung verhindert, dass Benutzer eine Verbindung zum VPN herstellen. Das Gerät kann auch unzugänglich werden und aufgrund von Speichererschöpfung nicht mehr richtig funktionieren.

Selbst nach einem Neustart wird der FTD-Speicher sofort wieder hochgefahren, selbst wenn der FTD keinen Datenverkehr verarbeitet.

<#root>

```
firepower# show memory

Free memory:         216990542 bytes ( 8%)

Used memory:        2487943528 bytes (92%)


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

Details zur Speichernutzung zeigen eine große Menge an Speicher an, die im DMA-Pool reserviert ist.

<#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-Drop-Ausgaben zeigen außerdem zahlreiche inkrementelle Drops durch den Snort-Präprozessor an.

<#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
```

Die Ausgabe von running-config des Geräts kann auch auf mehrere AnyConnect-Pakete hinweisen, die zum hohen Arbeitsspeicher beitragen.

<#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
```

Umwelt

- Produkt: Cisco Secure Firewall 1010
- Konfiguration des Cisco Secure Client (AnyConnect)

Auflösung

Der Fehler Cisco bug ID CSCwc82675 wurde in Firepower Version 10.0.0 behoben.

Problemumgehung:

- Deaktivieren des WebVPN-Caches
- Löschen Sie die unerwünschten AnyConnect Client-Pakete
- Ändern des VPN-Protokolls von SSL/TLS in IPSec

Ursache

Dieses spezielle Problem wird durch den Defekt Cisco Bug-ID CSCwc82675 verursacht. Die Firepower 1010-Plattform ist eine Low-End-Plattform mit bekannten Einschränkungen bei der Ausführung von Secure Client (AnyConnect) aufgrund ihrer Speicherbeschränkungen, die nach der Konfiguration mehrerer AnyConnect-Pakete, wie in Cisco Bug-ID CSCwc82675 erwähnt, zu einem hohen Arbeitsspeicher auf Datenebene führen können. Die Firepower 1010 wird mit 8 GB Arbeitsspeicher, davon 3 GB für LINA/ASA (DATAPATH) zur Datenverkehrsverarbeitung Diese Geräte weisen in der Regel eine erhöhte Speichernutzung auf, da LINA eine bestimmte Speichermenge für die Datenverkehrsverarbeitung reserviert und diese nicht einfach an das System überträgt. Dieses Verhalten ist von der Konstruktion her und für eine bessere Leistung bestimmt. Bei VPN-Konfigurationen zeigt die Speicherbelegung, dass ca. 40 % dem DMA-Pool zugewiesen sind, der hauptsächlich für VPN-Vorgänge reserviert ist. Der System-Overhead berücksichtigt die gesamte Speichernutzung. Auch ohne die Verarbeitung von Datenverkehr kann eine FirePOWER 1010-Plattform mit VPN-Konfiguration eine erhöhte Speichernutzung aufweisen. Diese Speichernutzung kann die Höchstgrenze erreichen, wenn Datenverkehr in die Firewall

eingeführt wird.

Verwandte Inhalte

- Cisco Bug-ID CSCwc82675

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.