L'elevata memoria Secure Firewall 1010 FTD provoca un impatto sul traffico

Sommario

Problema

Sulla piattaforma di fascia bassa Secure Firewall 1010, gli utenti ricevono un avviso di Health Monitor relativo alla "memoria del piano dati critico". Questo elevato utilizzo della memoria impedisce agli utenti di connettersi alla VPN. Il dispositivo può inoltre diventare inaccessibile e smettere di funzionare correttamente a causa dell'esaurimento della memoria.

Anche dopo un riavvio, la memoria FTD torna immediatamente all'uso elevato anche se l'FTD non gestisce traffico.

<#root>

```
firepower# show memory

Free memory:         216990542 bytes ( 8%)

Used memory:        2487943528 bytes (92%)


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

Nei dettagli sull'utilizzo della memoria viene visualizzata una grande quantità di memoria riservata nel pool DMA.

<#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% )
```

Gli output di tipo drop ASP indicano anche numerose cadute incrementali da parte del preprocessore Snort.

<#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
```

L'output del comando running-config del dispositivo può anche indicare più pacchetti AnyConnect che contribuiscono alla quantità di memoria elevata.

<#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
```

Ambiente

- Prodotto: Cisco Secure Firewall 1010
- Cisco Secure Client (AnyConnect) configurato

Risoluzione

L'ID bug Cisco CSCwc82675 è stato risolto in modo permanente in Firepower versione 10.0.0.

Soluzione temporanea:

- Disabilita la cache Webvpn
- Elimina i pacchetti client Anyconnect indesiderati
- Modificare il protocollo VPN da SSL/TLS a IPSec

Causa

Questo problema specifico è causato da un difetto dell'ID bug Cisco CSCwc82675. La piattaforma Firepower 1010 è una piattaforma di fascia bassa con limitazioni note nell'esecuzione di Secure Client (AnyConnect) a causa dei vincoli di memoria che possono causare un'elevata quantità di memoria del piano dati dopo la configurazione di più pacchetti AnyConnect, come indicato nell'ID bug Cisco CSCwc82675. Firepower 1010 ha 8 GB di memoria totale e dedica 3 GB di memoria totale a LINA/ASA (DATAPATH) per l'elaborazione del traffico. Questi dispositivi in genere mostrano un elevato utilizzo della memoria perché LINA riserva una certa quantità di memoria per l'elaborazione del traffico e non la rilascia facilmente al sistema. Questo comportamento è stato progettato appositamente per migliorare le prestazioni. Con le configurazioni VPN, il consumo di memoria indica che circa il 40% è allocato al pool DMA, che è principalmente riservato per le operazioni VPN. Il sovraccarico del sistema tiene conto dell'utilizzo totale della memoria. Anche senza gestire il traffico, una piattaforma Firepower 1010 con una configurazione VPN può mostrare un elevato utilizzo della memoria. Questo utilizzo della memoria può raggiungere i livelli massimi una volta che il traffico viene introdotto nel firewall.

Contenuto correlato

- ID bug Cisco CSCwc82675

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).