La memoria alta de FTD de Secure Firewall 1010 provoca un impacto en el tráfico

Contenido

Problema

Los usuarios experimentan una advertencia del monitor de estado para la "memoria del plano de datos críticos" en la plataforma de gama baja Secure Firewall 1010. Esta alta utilización de memoria impide que los usuarios se conecten a la VPN. El dispositivo también puede volverse inaccesible y dejar de funcionar correctamente debido al agotamiento de la memoria.

Incluso después de un reinicio, la memoria FTD vuelve inmediatamente a un uso alto, incluso si el FTD no maneja tráfico.

<#root>

```
firepower# show memory

Free memory:         216990542 bytes ( 8%)

Used memory:        2487943528 bytes (92%)


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

Los detalles de uso de memoria muestran una gran cantidad de memoria reservada en el grupo 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% )
```

Las salidas de caídas de ASP también indican numerosas caídas en aumento por parte del preprocesador 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
```

La salida running-config del dispositivo también puede indicar varios paquetes de AnyConnect que contribuyen a la memoria alta.

<#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
```

Entorno

- Producto: Cisco Secure Firewall 1010
- Cisco Secure Client (AnyConnect) configurado

Resolución

El ID de bug de Cisco CSCwc82675 defectuoso se ha resuelto permanentemente en la versión 10.0.0 de Firepower.

Solución alternativa:

- Desactivar la caché de Webvpn
- Elimine los paquetes de cliente Anyconnect no deseados
- Cambiar el protocolo VPN de SSL/TLS a IPSec

Causa

Este problema específico se debe a un defecto en el ID de error de Cisco CSCwc82675. La plataforma Firepower 1010 es una plataforma de gama baja con limitaciones conocidas al ejecutar Secure Client (AnyConnect) debido a sus limitaciones de memoria, que pueden dar lugar a una memoria de plano de datos elevada después de configurar varios paquetes de AnyConnect, como se menciona en el ID de error de Cisco CSCwc82675. El Firepower 1010 cuenta con 8 GB de memoria total y dedica 3 GB de la memoria total a LINA/ASA (DATAPATH) para el procesamiento del tráfico. Estos dispositivos suelen mostrar un uso elevado de la memoria porque LINA reserva una cierta cantidad de memoria para el procesamiento del tráfico y no la libera al sistema fácilmente. Este comportamiento se ha diseñado y está pensado para mejorar el rendimiento. Con las configuraciones VPN, el consumo de memoria muestra que aproximadamente el 40% está asignado al grupo DMA, que se reserva principalmente para operaciones VPN. La sobrecarga del sistema tiene en cuenta el uso total de memoria. Incluso sin gestionar el tráfico, una plataforma Firepower 1010 con una configuración VPN puede mostrar un

uso elevado de la memoria. Este uso de memoria puede alcanzar niveles máximos una vez que el tráfico se introduce en el firewall.

Contenido relacionado

- ID de bug de Cisco CSCwc82675

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).