La mémoire élevée du pare-feu sécurisé 1010 FTD a un impact sur le trafic

Table des matières

Problème

Les utilisateurs reçoivent un avertissement de surveillance de l'état de la « mémoire du plan de données critique » sur la plate-forme bas de gamme Secure Firewall 1010. Cette utilisation élevée de la mémoire empêche les utilisateurs de se connecter au VPN. Le périphérique peut également devenir inaccessible et cesser de fonctionner correctement en raison d'un épuisement de la mémoire.

Même après un redémarrage, la mémoire FTD redevient immédiatement très utilisée, même si le FTD ne gère aucun trafic.

<#root>

```
firepower# show memory

Free memory:         216990542 bytes ( 8%)

Used memory:        2487943528 bytes (92%)


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

Les détails d'utilisation de la mémoire indiquent une grande quantité de mémoire réservée dans le 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% )
```

Les sorties d'abandon ASP indiquent également de nombreuses abandons incrémentés par le préprocesseur 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 sortie running-config du périphérique peut également indiquer plusieurs packages AnyConnect qui contribuent à la mémoire élevée.

<#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
```

Environnement

- Produit : Cisco Secure Firewall 1010
- Client sécurisé Cisco (AnyConnect) configuré

Résolution

L'ID de bogue Cisco CSCwc82675 a été définitivement résolu dans Firepower version 10.0.0.

Solution de contournement:

- Désactiver le cache Webvpn
- Supprimer les packages client Anyconnect indésirables
- Remplacer le protocole VPN SSL/TLS par IPSec

Motif

Ce problème spécifique est causé par le défaut Cisco bug ID CSCwc82675. La plate-forme Firepower 1010 est une plate-forme bas de gamme avec des limitations connues lors de l'exécution de Secure Client (AnyConnect) en raison de ses contraintes de mémoire qui peuvent entraîner une mémoire élevée du plan de données après la configuration de plusieurs packages AnyConnect comme mentionné dans le bogue Cisco ID CSCwc82675. Le Firepower 1010 est provisionné avec 8 Go de mémoire totale et dédié 3 Go de la mémoire totale à LINA/ASA (DATAPATH) pour le traitement du trafic. Ces périphériques affichent généralement une utilisation élevée de la mémoire, car LINA réserve une certaine quantité de mémoire pour le traitement du trafic et ne la libère pas facilement dans le système. Ce comportement est conçu pour offrir de meilleures performances. Avec les configurations VPN, la consommation de mémoire montre qu'environ 40 % est alloué au pool DMA, qui est principalement réservé aux opérations VPN. La surcharge système tient compte de l'utilisation totale de la mémoire. Même sans gérer le trafic, une plate-forme Firepower 1010 avec une configuration VPN peut afficher une utilisation élevée de la mémoire. Cette utilisation de la mémoire peut atteindre des niveaux maximaux une fois que

le trafic est introduit dans le pare-feu.

Autres informations utiles

- ID de bogue Cisco CSCwc82675

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.