A alta memória do Secure Firewall 1010 FTD causa impacto no tráfego

Contents

Problema

Os usuários experimentam um aviso do monitor de integridade para "Memória de plano de dados críticos" na plataforma de baixo custo Secure Firewall 1010. Essa alta utilização de memória impede que os usuários se conectem à VPN. O dispositivo também pode se tornar inacessível e parar de funcionar corretamente devido à exaustão da memória.

Mesmo após uma reinicialização, a memória FTD volta imediatamente para alta utilização, mesmo que o FTD não esteja manipulando nenhum tráfego.

<#root>

```
firepower# show memory

Free memory:         216990542 bytes ( 8%)

Used memory:        2487943528 bytes (92%)


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

Os detalhes de uso da memória mostram uma grande quantidade de memória reservada no 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% )
```

As saídas de queda ASP também indicam várias quedas incrementais pelo pré-processador 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
```

A saída running-config do dispositivo também pode indicar vários pacotes do AnyConnect que contribuem para a alta memória.

<#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

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

Resolução

O defeito do ID de bug da Cisco CSCwc82675 foi resolvido permanentemente no Firepower versão 10.0.0.

Solução:

- Desativar o cache do Webvpn
- Excluir os pacotes do Anyconnect Client indesejados
- Alterar o protocolo VPN de SSL/TLS para IPSec

Causa

Esse problema específico é causado pelo defeito da ID de bug da Cisco CSCwc82675. A plataforma Firepower 1010 é uma plataforma de baixo custo com limitações conhecidas ao executar o Secure Client (AnyConnect) devido a suas restrições de memória, que podem resultar em alta memória do plano de dados após a configuração de vários pacotes do AnyConnect, conforme mencionado na ID de bug da Cisco CSCwc82675. O Firepower 1010 é fornecido com 8 GB de memória total e dedica 3 GB da memória total ao LINA/ASA (DATAPATH) para processamento de tráfego. Esses dispositivos normalmente mostram um uso elevado de memória porque o LINA reserva uma certa quantidade de memória para o processamento de tráfego e não a libera para o sistema facilmente. Esse comportamento é intencional e se destina a melhorar o desempenho. Com as configurações de VPN, o consumo de memória mostra que aproximadamente 40% é alocado para o pool de DMA, que é reservado principalmente para operações de VPN. A sobrecarga do sistema é responsável pelo uso total da memória. Mesmo sem lidar com o tráfego, uma plataforma Firepower 1010 com uma configuração de VPN pode

mostrar o uso elevado de memória. Esse uso de memória pode atingir níveis máximos depois que o tráfego é introduzido no firewall.

Conteúdo relacionado

- ID de bug Cisco CSCwc82675

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.