

Veilige firewall 1010 FTD High Memory veroorzaakt impact op het verkeer

Inhoud

uitgeven

Gebruikers krijgen een gezondheidswaarschuwing voor "Critical Data Plane memory" op het low-end platform Secure Firewall 1010. Dit hoge geheugengebruik voorkomt dat gebruikers verbinding maken met de VPN. Het apparaat kan ook ontoegankelijk worden en niet meer goed functioneren als gevolg van geheugenuitputting.

Zelfs na een reboot gaat het FTD-geheugen onmiddellijk terug naar hoog gebruik, zelfs als de FTD geen verkeer verwerkt.

<#root>

```
firepower# show memory
```

```
Free memory:          216990542 bytes ( 8%)
```

```
Used memory:          2487943528 bytes (92%)
```

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

Geheugengebruikdetails tonen een grote hoeveelheid geheugen gereserveerd in DMA-pool.

<#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 outputs geven ook tal van toenemende dalingen door Snort preprocessor.

```
<#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
```

De uitvoer van de actieve configuratie van het apparaat kan ook meerdere AnyConnect-pakketten aangeven die bijdragen aan het hoge geheugen.

```
<#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
```

milieu

- Cisco Secure Firewall 1010
- Cisco Secure Client (AnyConnect) ingesteld

resolutie

Defect Cisco bug ID CSCwc82675 is permanent opgelost in Firepower versie 10.0.0.

Tijdelijke oplossing:

- Schakel de WebVPN-cache uit
- Verwijder de ongewenste AnyConnect-clientpakketten
- Het VPN-protocol wijzigen van SSL/TLS naar IPSec

Oorzaak

Dit specifieke probleem wordt veroorzaakt door het defect Cisco bug ID CSCwc82675. Het Firepower 1010-platform is een low-end platform met bekende beperkingen bij het uitvoeren van Secure Client (AnyConnect) vanwege de geheugenbeperkingen die kunnen leiden tot een hoog geheugen voor het gegevensvliegtuig na het configureren van meerdere AnyConnect-pakketten zoals vermeld in Cisco bug ID CSCwc82675. De Firepower 1010 is voorzien van 8 GB aan totaal geheugen en besteedt 3 GB van het totale geheugen aan LINA/ASA (DATAPATH) voor verkeersverwerking. Deze apparaten vertonen meestal een verhoogd geheugengebruik omdat LINA een bepaalde hoeveelheid geheugen reserveert voor verkeersverwerking en het niet gemakkelijk aan het systeem vrijgeeft. Dit gedrag is ontworpen en bedoeld voor betere prestaties. Bij VPN-configuraties laat het geheugenverbruik zien dat ongeveer 40% wordt toegewezen aan de DMA-pool, die voornamelijk is gereserveerd voor VPN-bewerkingen. De systeemoverhead is verantwoordelijk voor het totale geheugengebruik. Zelfs zonder verkeer af te handelen, kan een Firepower 1010-platform met een VPN-configuratie een verhoogd geheugengebruik laten zien. Dit geheugengebruik kan maximale niveaus bereiken zodra het verkeer wordt geïntroduceerd in de firewall.

Verwante inhoud

- [Cisco bug ID CSCwc82675](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.