Secure Firewall 1010 FTD High Memory Causes Traffic Impact (CSCwc82675)

Contents

Issue

Users experience a health monitor warning for "Critical Data Plane memory" on the low-end platform Secure Firewall 1010. This high memory utilization prevents users from connecting to the VPN. The device can also become inaccessible and stop functioning properly due to memory exhaustion.

Even after a reboot, the FTD memory goes immediately back up to high usage even if the FTD is handling no traffic.

<#root>

```
firepower# show memory

Free memory:         216990542 bytes ( 8%)

Used memory:        2487943528 bytes (92%)


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

Memory usage details show a large amount of memory reserved 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 also indicate numerous incrementing drops by 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
```

The running-config output of the device can also indicate multiple AnyConnect packages which contribute to the high memory.

<#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
```

Environment

- Product: Cisco Secure Firewall 1010
- Cisco Secure Client (AnyConnect) configured

Resolution

Defect Cisco bug ID CSCwc82675 has been permanently resolved in Firepower version 10.0.0.

Workaround

- Disable the Webvpn cache
- Delete the unwanted Anyconnect Client Packages
- Change the VPN protocol from SSL/TLS to IPSec

Cause

This specific issue is caused by defect Cisco bug ID CSCwc82675. The Firepower 1010 platform is a low-end platform with known limitations when running Secure Client (AnyConnect) due to its memory constraints which can result in high data plane memory after configuring multiple AnyConnect packages as mentioned in Cisco bug ID CSCwc82675. The Firepower 1010 is provisioned with 8GB of total memory and dedicates 3GB of the total memory to LINA/ASA (DATAPATH) for traffic processing. These devices typically show elevated memory usage because LINA reserves a certain amount of memory for traffic processing and does not release it to the system easily. This behavior is by design and intended for better performance. With VPN configurations, the memory consumption shows that approximately 40% is allocated to the DMA pool, which is mainly reserved for VPN operations. The system overhead accounts for total memory usage. Even without handling traffic, a Firepower 1010 platform with a VPN configuration can show elevated memory usage. This memory usage can reach maximum levels once traffic is introduced to the firewall.

Related Content

- Cisco bug ID CSCwc82675