Hoge CPU op DATAPATH en connectiviteitsproblemen op FTD als gevolg van overmatige embryonale verbindingen

Inhoud

uitgeven

Een hoog CPU-gebruik werd waargenomen op FTD-apparaten, wat leidde tot connectiviteitsproblemen en gebruikers belette toegang te krijgen tot kritieke bedrijfstoepassingen. De firewall vertoonde een verhoogd gebruik van datapath en Snort CPU, waarbij gebruikers problemen ondervonden met latentie en intermitterende toegang. Onderzoek bracht een groot aantal embryonale TCP-verbindingen aan het licht, waarbij een aanzienlijk deel afkomstig was van interne beveiligingsscanners, wat resulteerde in uitputting van middelen en verminderde prestaties.

milieu

- Cisco Secure Firewall Firepower Threat Defense (FTD)
- Hardware: Cisco Firepower 1150
- Softwareversie: 7.4.2.3
- Beheerd door: Firepower Management Center (FMC)
- High Availability (HA)-configuratie
- Datapath en Snort CPU consistent op of nabij 100%
- Hoog aantal embryonale TCP-verbindingen door interne scanners
- Recente wijzigingen: configuraties van logboekverzamelaars toegepast en teruggezet; implementatie van toegangsregels; gebeurtenis voor waargenomen failover
- Systemen die sterke verbindingen genereren en worden geïdentificeerd als interne Qualys-scanners

resolutie

Geïdentificeerd hoog CPU-gebruik op DATAPATH gebruikt voor verkeersverwerking.

```
device# show processes cpu-usage sorted non-zero
Hardware:   FPR-1150
Cisco Adaptive Security Appliance Software Version 9.20(2)43
ASLR enabled, text region 562a19048000-562a1e49126d
PC         Thread       5Sec     1Min     5Min   Process
   -          -        99.7%    99.7%    99.7%   DATAPATH-4-22658
   -          -        99.7%    99.7%    99.6%   DATAPATH-3-22657
```

```
   -          -        99.7%    99.6%    99.6%   DATAPATH-2-22656
   -          -        99.6%    99.7%    99.7%   DATAPATH-5-22659
   -          -        97.5%    97.1%    97.1%   DATAPATH-1-22655
   -          -        97.4%    97.1%    97.1%   DATAPATH-0-22654
0x0000562a1b8c55e3   0x0000151e97f523e0     1.1%     1.6%     1.6%   CP Processing
0x0000562a1d408771   0x0000151e97f434a0     0.4%     0.2%     0.0%   Unicorn Proxy Thread
0x0000562a1b6ba40a   0x0000151e97f3cb80     0.3%     0.3%     0.3%   appagent_async_client_receive_thre
0x0000562a1cfebc65   0x0000151e97f43f80     0.1%     0.1%     0.1%   IP SLA Mon Event Processor
0x0000562a1d328a89   0x0000151e97f64240     0.1%     0.1%     0.1%   lina logclient Rx data thread
0x0000562a1d72eb46   0x0000151e97f417a0     0.0%     0.1%     0.0%   cli_xml_request_process
0x0000562a1df983a5   0x0000151e97f69940     0.0%     0.1%     0.0%   Checkheaps
```

Vanuit de FTD CLI werd een output van show conn detail geëxporteerd voor beoordeling van verbindingsstatistieken door interne automatiseringstools.

WAARSCHUWING: De uitvoer van show conn detail van de CLI kan extreem lang zijn als het aantal verbindingen meer dan 100.000 is. Zorg ervoor dat er voldoende tijd is voor deze inzameling.

De disk0 komt overeen met /mnt/disk0/ in de FTD backend. Exporteer het bestand dienovereenkomstig.

```
device# show conn detail | redirect disk0:/shconndetMMDDYY.txt
```

Bekijk de verbindingsstatistieken van de resultaten van het hulpmiddel voor embryonale verbindingen in grote hoeveelheden:

```
Total Emryonic Conns: 121611. This is 87.984% of the total conns (138219)
--
Top-5  Embryonic IPs (SYN, but not SYN/ACK - 'aA' flags) going through the device
IP                                          Count    Percent
------------------------------------------------------------
10.5.30.77                                  81519    33.517%
10.1.30.102                                 40042    16.463%
10.1.212.14                                   907     0.373%
10.1.204.4                                    837     0.344%
10.1.21.122                                   804     0.331%
```

Na het identificeren van de bron-IP's (in dit geval interne beveiligingsscanners), voorkomen dat de bron het verkeer genereert en de verbindingen van de FTD wissen.

```
device# clear conn add 10.5.30.77
4563 connection(s) deleted.
device# show conn count
5936 in use, 465189 most used
Inspect Snort:
```

```
        preserve-connection: 4451 enabled, 0 in effect, 432406 most enabled, 0 most in effect
```

Bewaak CPU-gebruik na mitigatie om te bevestigen dat de oorzaak door verkeer is veroorzaakt.

```
device# show cpu
CPU utilization for 5 seconds = 9%; 1 minute: 28%; 5 minutes: 70%
```

De verkeersconnectiviteit zou weer normaal moeten zijn en de latentie zou niet langer moeten worden waargenomen.

Oorzaak

De hoofdoorzaak van hoge CPU- en connectiviteitsproblemen was overmatige embryonale verbindingen die werden gegenereerd door interne beveiligingsscanners. Deze verbindingen, voornamelijk SYN-pakketten zonder overeenkomstige SYN / ACK-antwoorden, overweldigden de FTD-datapath- en Snort-processen. Het grote aantal onvolledige verbindingen leidde tot uitputting van bronnen, wat resulteerde in een aanhoudend hoog CPU-gebruik, intermitterende connectiviteit en impact op bedrijfskritieke toegang tot toepassingen.

Verwante inhoud

- Cisco Technical Support en downloads

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.