Hohe CPU bei DATAPATH und Verbindungsprobleme bei FTD aufgrund übermäßiger embryonaler Verbindungen

Inhalt

Problem

Eine hohe CPU-Auslastung wurde auf FTD-Geräten beobachtet, was zu Verbindungsproblemen führte und den Zugriff von Benutzern auf kritische Geschäftsanwendungen verhinderte. Die Firewall wies einen erhöhten Datenpfad und eine erhöhte Snort-CPU-Auslastung auf, wobei Benutzer Latenzprobleme und vorübergehende Zugriffsprobleme aufwiesen. Die Untersuchung ergab eine große Anzahl embryonaler TCP-Verbindungen, wobei ein erheblicher Teil von internen Sicherheitsscannern stammte, was zu Ressourcenauslastung und Leistungseinbußen führte.

Umwelt

- Cisco Secure Firewall FirePOWER Threat Defense (FTD)
- Hardware: Cisco FirePOWER 1150
- Software-Version: 7.4.2.3
- Verwaltet von: Firepower Management Center (FMC)
- Konfiguration für hohe Verfügbarkeit (HA)
- Datapath und Snort CPU konsistent bei oder nahe 100 %
- Hohe Anzahl embryonaler TCP-Verbindungen durch interne Scanner
- Letzte Änderungen: Protokollsammlerkonfigurationen angewendet und zurückgesetzt; Bereitstellung von Zugriffsregeln; beobachtetes Failover-Ereignis
- Systeme, die als interne Qualys-Scanner identifizierte hohe Verbindungen erzeugen

Auflösung

Hohe CPU-Auslastung bei DATAPATH für die Datenverkehrsverarbeitung ermittelt.

```
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
```

Aus der FTD-CLI wurde eine Ausgabe von show conn detail zur Überprüfung der Verbindungsstatistik durch interne Automatisierungstools exportiert.

ACHTUNG: Die Ausgabe von show conn detail aus der CLI kann extrem lang sein, wenn die Anzahl der Verbindungen über 100.000 liegt. Stellen Sie sicher, dass genügend Zeit für diese Sammlung zur Verfügung steht.

Die Datei disk0 entspricht dem Verzeichnis /mnt/disk0/ im FTD-Backend. Exportieren Sie die Datei entsprechend.

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

Überprüfen Sie die Verbindungsstatistiken aus den Ergebnissen des Werkzeugs für embryonale Verbindungen in hohen Mengen:

```
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%
```

Nachdem die Quell-IPs identifiziert wurden (in diesem Fall die internen Sicherheitsscanner), verhindern Sie, dass die Quelle den Datenverkehr erzeugt, und löschen Sie die Verbindungen aus der FTD.

```
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
```

Überwachen Sie die CPU-Auslastung nach der Risikominimierung, um sicherzustellen, dass die Ursache datenverkehrsinduziert war.

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

Die Datenverkehrsverbindung sollte wieder normal sein, und Latenzen sollten nicht mehr beobachtet werden.

Ursache

Die Ursache für hohe CPU- und Verbindungsprobleme waren übermäßige embryonale Verbindungen, die von internen Sicherheitsscannern erzeugt wurden. Diese Verbindungen, in erster Linie SYN-Pakete ohne entsprechende SYN/ACK-Antworten, überlasteten die FTD-Datenpfad- und Snort-Prozesse. Das hohe Volumen an unvollständigen Verbindungen führte zu einer Ressourcenauslastung, die zu einer anhaltend hohen CPU-Auslastung, intermittierenden Verbindungen und Auswirkungen auf den Zugriff geschäftskritischer Anwendungen führte.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.