DATAPATH上的CPU高，以及FTD上因初期連線過多導致的連線問題

目錄

問題

FTD裝置上觀察到高的CPU使用率，導致連線問題和防止使用者存取關鍵業務應用程式。防火牆顯示資料路徑和Snort CPU使用率上升，使用者遇到延遲和間歇存取問題。調查顯示大量雛形TCP連線，其中相當大部份來自內部安全掃描器，導致資源耗盡和效能降低。

環境

- 思科安全防火牆Firepower威脅防禦(FTD)
- 硬體：Cisco Firepower 1150
- 軟體版本:7.4.2.3
- 管理者：Firepower Management Center (FMC)
- 高可用性(HA)配置
- Datapath和Snort CPU始終穩定在100%或接近100%
- 內部掃描器導致大量初始TCP連線
- 最近的更改：已應用並還原日誌收集器配置；訪問規則部署；觀察到的故障切換事件
- 生成確定為內部Qualys掃描器的高連線的系統

解析

已確定用於流量處理的DATAPATH上的CPU使用率高。

```
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
```

在FTD CLI中，已匯出show conn detail輸出，以供內部自動化工具檢視連線統計資訊。

注意：如果連線計數超過100,000，則CLI的show conn detail輸出可能會非常長。請確保為此集合分配了足夠的時間。

disk0與FTD後端中的/mnt/disk0/目錄對應。請相應地匯出檔案。

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

檢視從早期連線工具的結果中獲得的連線統計資訊，以獲得大量早期連線：

```
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%
```

識別來源IP後（在本案例中為內部安全掃描器），防止來源產生流量並從FTD清除其連線。

```
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
```

在緩解後監控CPU利用率，以確認原因是由流量引發的。

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

流量連線應恢復正常，不應再觀察延遲。

原因

高CPU和連線問題的根本原因是內部安全掃描器生成的過多初期連線。這些連線（主要是沒有相應SYN/ACK響應的SYN資料包）不堪重負FTD資料路徑和Snort進程。大量不完整連線導致資源耗盡，導致CPU利用率持續高、連線間歇性中斷，並影響關鍵業務應用程式訪問。

相關內容

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。