過剰な初期接続が原因の、DATAPATHでのCPU高使用とFTDでの接続の問題

内容

お問い合わせ内容

FTDデバイスで高いCPU使用率が確認されたため、接続の問題が発生し、ユーザが重要なビジネスアプリケーションにアクセスできなくなります。 ファイアウォールでデータパスとSnortのCPU使用率が上昇し、ユーザに遅延と断続的なアクセスの問題が発生しました。 調査の結果、大量の初期TCP接続が確認され、大部分が内部セキュリティスキャナから発信されているため、リソースが枯渇し、パフォーマンスが低下していることが判明しました。

環境

- Cisco Secure Firewall Firepower Threat Defense(FTD)
- ハードウェア：Cisco Firepower 1150
- ソフトウェアバージョン：7.4.2.3
- 管理者：Firepower Management Center(FMC)
- ハイアベイラビリティ(HA)設定
- DatapathおよびSnort CPUの使用率は常に100 %またはそれに近い
- 内部スキャナによる初期TCP接続数が多い
- 最近の変更：ログコレクタの設定の適用と復元、アクセスルールの導入、確認されたフェールオーバーイベント
- 高い接続を生成するシステムは、内部Qualysスキャナとして識別されます。

解決策

「トラフィック処理に使用されるDATAPATHでの高いCPU使用率」を確認。

```
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
```

FTD CLIから、内部オートメーションツールによる接続統計を確認するためにshow conn detailの出力がエクスポートされました。

注意：接続カウントが100,000を超える場合、CLIからのshow conn detailの出力は非常に長くなる可能性があります。 この収集に十分な時間が割り当てられていることを確認します。

disk0はFTDバックエンドの/mnt/disk0/ディレクトリに対応します。 必要に応じてファイルをエクスポートします。

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

初期接続ツールの結果から得られた接続統計を大量に確認します。

```
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%
```

送信元IP（この場合は内部セキュリティスキャナ）を特定した後、送信元がトラフィックを生成しないようにし、その接続をFTDからクリアします。

```
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
```

緩和後にCPU使用率を監視して、原因がトラフィックによって引き起こされたものであることを確認します。

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

トラフィックの接続が通常の状態に戻り、遅延が観察されなくなります。

原因

CPUの高使用と接続の問題の根本原因は、内部セキュリティスキャナによって生成された過剰な初期接続でした。 対応するSYN/ACK応答のない主にSYNパケットであるこれらの接続は、FTDデータパスおよびSnortプロセスを圧倒しました。 不完全な接続が大量に発生すると、リソースが枯渇し、CPU使用率が高い状態が続いたり、接続が断続的になったり、ビジネスクリティカルなアプリケーションアクセスに影響が及ぶことがあります。

関連コンテンツ

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。