ASA のスループットと接続速度のトラブルシューティングおよびパケット キャプチャの分析

要約

概要

このドキュメントでは、Cisco 適応型セキュリティ アプライアンス（ASA）のスループットと接続速度の問題をトラブルシューティングする方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco Adaptive Security Appliance（ASA）に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

初回の ASA 導入時や、新しい接続のテスト時に問題が発生することがあります。 これは、ASA を通過するフローの速度が、接続パス内に ASA がない場合よりも低下する（つまり、ネットワークに ASA を実装する前よりも接続速度が低下する）という TCP 接続スループットの問題です。

たとえば、お客様が口ーエンドの D リンク ルータを ASA 5505 または ASA 5510 に交換したところ、 ルータの交換後に接続速度が著しく低下することがあります。 お客様は、接続速度が低下した原因は ASA にあると考えて、Cisco TAC にサービス リクエストを送信します。

機能情報

トラブルシューティング方法

TCP フローの速度は、ネットワークでパケット損失やパケット遅延が生じると低下します。 問題の真の原因を把握するためには、その接続の実際の TCP パケットの状態とそれがネットワークに及ぼす影響をデータで確認する必要があります。 通常、ネットワーク管理者は、FTP ファイル転

送やオンライン速度テストなど、特別なアクションを実行したときに、問題についての警告を受けます。 これらの問題のほとんどは再現可能です。 したがって、管理者は根本原因を見つけるために必要なデータを収集できます。

必要なデータを収集するためには、テストの前後に ASA から **show tech** コマンドを実行します。 このコマンドを使用すると、設定とパケット統計情報 (主として **show service-policy**)が表示され、またインターフェイスのエラー数が増えているかどうかもわかります。

問題の原因を完全に診断するには、双方向の同時パケット キャプチャ (接続に使用される 2 つの ASA インターフェイスから取得) が必要です。

ASA へのパケット キャプチャの適用例については、次のドキュメントを参照してください。

- PIX および ASA を経由した接続のトラブルシューティング
- TAC セキュリティ ポッドキャスト エピソード #1 - ASA パケット キャプチャ ユーティリティを使用したトラブルシューティング

データ分析

必要なデータの収集後にパケット キャプチャを使用すれば、発生した問題が次のどれであるのか判断できます。

- 外部ホストからのパケットが ASA の外部インターフェイスに到達する前に、パケットのドロップまたは遅延が生じている
- ASA によってパケットの遅延またはドロップが発生している
- 内部ネットワークのどこかでパケットの遅延またはドロップが発生している

注: この分析では、データは外部インターフェイス上のホストから内部インターフェイス上のホストに送信されていると想定しています。

このビデオには、パケット キャプチャに対する分析の実行例が示されています。

*TCP ストリーム結合*は、この問題に関する技術的な考察対象となります。ASA の特定の機能を使用すると、ファイアウォールが ASA を通過する TCP ストリームを完全に結合するからです。

たとえば、ASA があるパケットを受信せず、ネットワーク上でパケット損失が生じたことを発見した場合、ASA は他方の TCP エンドポイントの代わりに損失データの ACK を送信します。 これは最も一般的な例です。 ASA は、順序が乱れて到着したパケットを発見すると、パケットの順序を修正し、正しい順序で受信側に渡します。 ネットワーク ドロップやパケット順序の入れ替えがなければ、この機能を有効にしても影響はありません。 すべてのパケットがどちらかの TCP エンドポイントから送信され、正常にネットワークと ASA を通過した場合、何かアクションが実行されることはないため、ユーザはこの機能が有効になっていることに気付かないと考えられます。 つまり、ネットワーク上の TCP 接続に問題が生じた場合だけこの機能が有効になり、ネットワーク トラフィックの速度が低下します。 TCP ストリームの結合は ASA にとって非常にリソース負荷の高い動作です。 ネットワークでパケット ドロップが生じるたびに、ASA はそのパケットの再送信を求める TCP パケット要求を送信するだけでなく、失われたパケットの後に送信側から送られたパケットのバッファリングも行う必要があります。

一般的な問題

ASA と隣接デバイスを接続するインターフェイスの速度とデュプレックス値の誤設定

この問題は、デバイスを ASA に交換した場合によく発生します。 ASA インターフェイスの速度とデュプレックス値が隣接デバイスの値と異なっていると、そのインターフェイスでパケット ドロップが生じます。 ASA インターフェイスおよび隣接インターフェイスの速度とデュプレックスの値を確認してください。

ASA の **show interface** 出力で、この問題による現象と明らかに考えられるエラーがないか確認します。

```
Interface Ethernet0/0 "Outside", is up, line protocol is up
Hardware is i82546GB rev03, BW 100 Mbps
Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
MAC address 0019.2f58.c324, MTU 1500
IP address 192.168.222.122, subnet mask 255.255.255.252
124047996 packets input, 35340918453 bytes, 0 no buffer
Received 3 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 L2 decode drops
156918660 packets output, 40931551514 bytes, 0 underruns
1 output errors, 4286634 collisions, 0 interface resets
0 babbles, 123332 late collisions, 4752834 deferred
0 lost carrier, 0 no carrier
input queue (curr/max blocks): hardware (0/0) software (0/0)
output queue (curr/max blocks): hardware (0/245) software (0/0)
Traffic Statistics for "Outside":
124047995 packets input, 33107957301 bytes
157041993 packets output, 38195084709 bytes
103480 packets dropped
1 minute input rate 2140 pkts/sec, 477200 bytes/sec
1 minute output rate 2630 pkts/sec, 396763 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 2152 pkts/sec, 525496 bytes/sec
5 minute output rate 2701 pkts/sec, 421215 bytes/sec
5 minute drop rate, 0 pkts/sec
```

IPS モジュールにトラフィックを送信 して下さい

IPS モジュールにトラフィックを送信するように ASA が設定されている場合は、ASA で TCP ストリーム結合機能が動作します。 TCP ストリーム結合機能の詳細については、このドキュメントの「データ分析」セクションを参照してください。

ASA の TCP MSS オプションの変更によるわずかなパフォーマンスの低下

デフォルトで、ASA の SYN パケットの TCP MSS オプションは 1380 に設定されます。 そのため、TCP エンドポイントは 1380 バイトを超える TCP セグメントを送信しません。 この値は一般的なデフォルト値である 1460 バイトよりも小さく、これによって TCP パフォーマンスが約 6 % 低下します。 ASA の最大 MSS 値を大きくするか、MSS 調整機能を無効にすると、パフォーマンスが改善される可能性があります。 ただし、ASA のデフォルト コマンドを変更する前に、パスのどこかでパケットがさらにカプセル化される場合の潜在的なフラグメンテーションとそのリスクを十分に理解する必要があります。

詳細については、『Cisco ASA 5500 シリーズ コマンド リファレンス』の「***sysopt connection tcpmss***」セクションを参照してください。

FAQ

関連情報

- Cisco ASA 5500 シリーズ コマンド リファレンス 8.2
- テクニカルサポートとドキュメント - Cisco Systems