IP インプット プロセスで CPU 使用率が高くなる場合のトラブルシューティング

目次

概要

このドキュメントでは、IP インプット プロセスにより CPU 使用率が高くなる場合のトラブルシューティング方法について説明します。

注: このドキュメントは、さまざまな種類の攻撃を防止する戦略は提供しません。

前提条件

要件

このドキュメントの前に、『Cisco ルータの CPU 使用率が高い場合のトラブルシューティング』を読むことを推奨します。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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。 対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

IP Input

Cisco IOS ® ソフトウェアプロセスによって呼出される *IP 入力は* IP パケットのプロセス交換処理します。 IP インプット プロセスで異常に高い CPU リソースが使用されている場合、ルータは多数の IP トラフィックのプロセス スイッチングを行っています。 次の項目を確認してください。

- **割り込みスイッチングが、トラフィックの多数存在するインターフェイス (1 つまたは複数) でディセーブルになっている**割り込みスイッチングとは、プロセス スイッチング以外のスイッチング アルゴリズムを使用することです。 その例としては、ファースト スイッチング、最適スイッチング、Cisco Express Forwarding スイッチングなどがあります (詳細は、『パフォーマンスの調整に関する基本事項』を参照してください)。 **show interfaces switching** コマンドの出力を調べて、どのインターフェイスにトラフィックの負荷がかかっているのかを確認します。 **show ip interface** コマンドを調べると、どのスイッチング方式が各インターフェイスで使用されるのかを確認できます。 そのインターフェイスで割り込みスイッチングを再度有効にします。 通常のファースト スイッチングは、出力インターフェイスで設定されています。 ファースト スイッチングがインターフェイスで設定されている場合、そのインターフェイスから発信されるパケットはファースト スイッチングされます。 Cisco Express Forwarding スイッチングは入力インターフェイスで設定されています。 特定のインターフェイスで Forwarding Information Base (FIB; 転送情報ベース) および隣接関係テーブルのエントリを作成するには、そのインターフェイスにルーティングされるすべてのインターフェイスで Cisco Express Forwarding スイッチングを設定します。
- **同じインターフェイスでファースト スイッチングがディセーブルになっている**インターフェイスに多くのセカンダリ アドレスまたはサブインターフェイスがあり、そのインターフェイスから発信され同じインターフェイス上のアドレス宛てになっているトラフィックが多数存在する場合、それらのパケットはすべてプロセス スイッチングされます。 **この場合、インターフェイスで ip route-cache same-interface をイネーブルにする必要があります。** Cisco Express Forwarding スイッチングを使用する場合に、同じインターフェイスで個別に Cisco Express Forwarding スイッチングをイネーブルにする必要はありません。
- **ポリシー ルーティングを提供するインターフェイスでファースト スイッチングがディセーブルになっている**ルート マップがインターフェイスで設定されており、多くのトラフィックがそのルート マップで処理される場合、ルータがこのトラフィックをプロセス スイッチングします。 **この場合、インターフェイスで ip route-cache policy をイネーブルにする必要があります。** 「Policy Based Routing (PBR) 設定のファスト・スイッチされた」セクションを Policy Based Routing (PBR) 有効に することで述べられる制限をチェックして下さい。
- **割り込みスイッチングを実行できないトラフィックが到着する**これは、リストしたすべてのタイプのトラフィックで発生する可能性があります。 詳細については、リンク項目をクリックしてください。スイッチング キャッシュにまだエントリがないパケットファースト、最適、Cisco Express Forwarding (CEF) のいずれかのスイッチングが設定されたとしても、ファースト スイッチング キャッシュまたは FIB および隣接テーブルで一致するものが存在しないパケットが処理されます。 その後、エントリが適切なキャッシュまたはテーブルで作成されると、同一の基準に一致するすべての後続パケットは、ファースト、最適、CEF のいずれかでスイッチングされます。 通常の状況では、これらの処理されたパケットは高 CPU 使用率の原因にはなりません。 ただし、1) ルータ経由で到達可能なデバイス向けに非常に高い頻度でパケットを生成し、2) 異なる送信元または宛先 IP アドレスを使用するネットワーク内のデバイスが存在する場合、スイッチング キャッシュまたはテーブルでこれらのパケットに一致するものが存在しないので、これらは IP インプット プロセスによって処理されます (NetFlow スイッチングが設定された場合、送信元と宛先 TCP ポートは NetFlow キャッシ

ュ内に対しても確認されます）。 この送信元デバイスは、機能しないデバイスであるか、または、可能性が高いのは、攻撃を行おうとしているデバイスです。(*) グリーニング隣接関係のみ。 隣接関係に関する詳細については Cisco Express Forwarding（CEF） Cisco Express Forwarding（CEF）参照して下さい。ルータが宛先になっているパケット次に示すのは、ルータを宛先とするパケットの例です。非常に高い頻度で到着するルーティング アップデート。 処理が必要な大量のルーティング アップデートがルータに到着した場合、このタスクが CPU を過負荷にする可能性があります。 通常、これは安定したネットワークでは発生しません。 詳細な情報を収集する方法は、設定したルーティング プロトコルに応じて異なります。 **ただし、定期的に show ip route summary コマンドの出力のチェックを始めることもできます。** 値が急速に変われば、ネットワークが不安定であるしるしです。 頻繁なルーティング テーブルの変更は、ルーティング プロトコル処理が増加することを意味し、それが結果として、CPU 使用率の増加を引き起こします。 この問題のトラブルシューティング方法の詳細は、『インターネットワーク トラブルシューティング ガイド』の「TCP/IP のトラブルシューティング」セクションを参照してください。他の種類のルータ宛てのトラフィック。 ルータに誰がログオンしているのかという点と、ユーザの操作を確認します。 誰かがログオンして長い出力を生成するコマンドを発行した場合、「IP インプット」プロセスによる高い CPU 使用率の後には、さらに高い CPU 使用率の Virtual Exec プロセスが続きます。スプーフィング攻撃。 **問題を識別するため、show ip traffic コマンドを発行して、IP トラフィックの量をチェックします。** 問題が存在する場合、ローカルな宛先を持つ受信パケットの数が重要になります。 **次に、show interfaces および show interfaces switching コマンドの出力を調べて、パケットがどのインターフェイスから送られてくるのかを確認します。 受信しているインターフェイスを識別したら、発信インターフェイス上の ip accounting を有効にして、パターンが存在するかどうかを確認します。** 攻撃がある場合、送信元アドレスはほぼすべての場合で異なりますが、宛先アドレスは同じです。 一時的に問題を解決するために、アクセス リストを設定できます（パケットの送信元に最も近いデバイスで行うのが望ましい）が、本当の解決策は、送信元デバイスを追跡して攻撃を停止することです。ブロードキャスト トラフィック**show interfaces** コマンド出力でブロードキャスト パケットの数を確認します。 ブロードキャストの量をインターフェイスで受信されたパケットの合計数と比較すると、ブロードキャストのオーバーヘッドが存在するかどうかがだいたいわかるようになります。 ルータに複数のスイッチが接続された LAN が存在する場合、これは、スパニング ツリーの問題を示すことになります。オプション付き IP パケットプロトコル変換を必要とするパケットマルチリンク ポイントツーポイント プロトコル（Cisco Express Forwarding スイッチングでサポート）圧縮されたトラフィックルータに Compression Service Adapter（CSA）が存在しない場合、圧縮されたパケットはプロセス スイッチングされる必要があります。暗号化されたトラフィックルータに Encryption Service Adapter（ESA）が存在しない場合、暗号化されたパケットはプロセス スイッチングされる必要があります。X.25 暗号化でシリアル インターフェイスを通過するパケットX.25 プロトコル スイートでは、フロー制御が 2 番目の Open System Interconnection（OSI; オープン システム インターコネクション）レイヤで実装されます。

- 直接接続されたサブネット内が宛先となっている（そのため、Address Resolution Protocol（ARP; アドレス解決プロトコル）テーブルにエントリが存在しない）多数のパケットが、きわめて多い頻度で到着する。 このような事態は、ウィンドウ メカニズム上の理由で TCP トラフィックでは発生しないはずですが、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）トラフィックでは発生する可能性があります。 問題を識別するために、推奨される操作を繰り返してスプーフィング攻撃を追跡します。
- 多数のマルチキャスト トラフィックがルータを通過する。 残念ながら、マルチキャスト トラフィックの量を調べる簡単な方法はありません。 **まとまった情報を示す唯一のコマンドは show ip traffic コマンドです。 ただし、ルータでマルチキャスト ルーティングを設定している場合は、ip mroute-cache インターフェイス コンフィギュレーション コマンドでマルチキ**

ャスト パケットのファースト スイッチングをイネーブルにできます（マルチキャスト パケットのファースト スイッチングはデフォルトでオフになっています）。

- ルータが加入過多の状態になっている。 ルータが過剰に使用されていて、この量のトラフィックを処理できない場合、他のルータに負荷を分散させるか、ハイエンド ルータを購入してください。
- IP Network Address Translation（NAT; ネットワーク アドレス変換）がルータ上で設定され、多数の Domain Name System（DNS; ドメイン ネーム システム）パケットがルータを通過する。 送信元または宛先ポート 53（DNS）の UDP または TCP パケットは、常に NAT によってプロセス レベルにパントされます。
- 処理にパントされるその他のパケットの種類が存在する。
- IPデータグラムのフラグメンテーションがあります。 IPデータグラムのフラグメント化すること当然の CPU およびメモリ オーバーヘッドに小さい増加があります。 この問題を解決する方法に関する詳細については GRE および IPSEC においての解決 IP フラグメンテーション、MTU、MSS および PMTUD 問題を参照して下さい。

IP インプット プロセスの高 CPU 使用率の理由が何であっても、問題の根本は、IP パケットをデバッグすれば追跡できます。 CPU 使用率がすでに高いので、デバッグ処理は十分に注意して実行する必要があります。 **デバッグ処理によって数多くのメッセージが生成されるので、logging buffered だけを設定してください。**

コンソールにロギングすると、CPU に不必要な割り込みが発生し、CPU の使用率が高くなります。 ホストにロギングすると（またはモニタ ロギング）、インターフェイスにさらにトラフィックが生成されます。

デバッグ処理は、debug ip packet detail exec コマンドで開始できます。 このセッションは、3 ~ 5 秒よりも長く存在できません。 デバッグ メッセージは、ロギング バッファに書き込まれます。 サンプル IPデバッグ セッションのキャプチャはこの資料のサンプル IP パケット デバッギング セッション セクションで提供されます。 不必要な IP パケットの送信元デバイスが見つかった場合、このデバイスをネットワークから切断できるか、ルータにアクセス リストを作成してその宛先からのパケットを廃棄できます。

IP パケット デバッグ セッションのサンプル

設定されたロギング宛先を確認するため、まず **show logging** コマンドを使用します。

```
router#show logging Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns) Console
logging: level debugging, 52 messages logged Monitor logging: level debugging, 0 messages logged
Buffer logging: level debugging, 148 messages logged Trap logging: level informational, 64
message lines logged Logging to 192.168.100.100, 3 message lines logged Logging to
192.168.200.200, 3 message lines logged --More--
```

ロギング バッファ以外のすべてのロギング宛先をディセーブルにして、ロギング バッファをクリアします。

```
router#configure terminal Enter configuration commands, one per line. End with CNTL/Z.
router(config)#no logging console router(config)#no logging monitor router(config)#no logging
192.168.100.100 router(config)#no logging 192.168.200.200 router(config)#^Z router#clear logging
Clear logging buffer [confirm] router#
```

デバッグ出力を読みやすくするために、日時とミリ秒のタイムスタンプをイネーブルにしておきます。

```
router#configure terminal Enter configuration commands, one per line. End with CNTL/Z.
router(config)#service timestamps log datetime msec router(config)#service timestamps debug
datetime msec router(config)#end router#
```

この時点で、デバッグ セッションを開始できます。

```
router#debug ip packet detail IP packet debugging is on (detailed)
```

デバッグは、3 ~ 5 秒よりも長く存在できません。 セッションは、**undebug all** exec コマンドで停止できます。

```
router#undebug all All possible debugging has been turned off
```

結果は、**show logging** exec コマンドで確認できます。

```
router#show logging Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns) Console
logging: disabled Monitor logging: disabled Buffer logging: level debugging, 145 messages logged
Trap logging: level informational, 61 message lines logged Log Buffer (64000 bytes): *Mar 3
03:43:27.320: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.204 (Ethernet0/0), g=10.200.40.1,
len 100, forward *Mar 3 03:43:27.324: ICMP type=8, code=0 *Mar 3 03:43:27.324: IP:
s=192.168.40.53 (Ethernet0/1), d=144.254.2.205 (Ethernet0/0), g=10.200.40.1, len 100, forward
*Mar 3 03:43:27.324: ICMP type=8, code=0 *Mar 3 03:43:27.328: IP: s=192.168.40.53 (Ethernet0/1),
d=144.254.2.206 (Ethernet0/0), g=10.200.40.1, len 100, forward *Mar 3 03:43:27.328: ICMP type=8,
code=0 ...
```

このログは次の内容を示しています。

- パケットは 4 ミリ秒ごとに受信されている
- 送信元 IP アドレスは 192.168.40.53 である
- パケットはインターフェイス Ethernet0/1 上で着信した
- パケットは異なる宛先 IP アドレスを持っている
- パケットはインターフェイス Ethernet0/0 に送信されている
- ネクストホップ IP アドレスは 10.200.40.1 である
- パケットは ICMP 要求（タイプ=8）であったこの例では、IP インプット プロセスの高い CPU 使用率は、IP アドレス 192.168.40.53 からの ping フラッドが原因で発生したことがわかります。SYN フラグの存在がデバッグ出力に示されるため、SYN フラッドもこの方法で簡単に検出できます。

```
*Mar 3 03:54:40.436: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.204
   (Ethernet0/0), g=10.200.40.1, len 44, forward
*Mar 3 03:54:40.440: TCP src=11004, dst=53,
   seq=280872555, ack=0, win=4128 SYN
```

関連情報

- Cisco ルータの CPU 使用率が高い場合のトラブルシューティング
- show processes コマンド
- Catalyst 2900XL/3500XL スイッチでの CPU の高使用率
- パフォーマンス チューニングの基本
- テクニカルサポートとドキュメント - Cisco Systems