# ASA インターフェイス オーバーラン カウンタのエラーのトラブルシューティング

## 内容



## 概要

このドキュメントでは、「オーバーラン」エラー カウンタと、ネットワークでのパフォーマンスの問題やパケット損失の問題を調査する方法について説明します。管理者は適応型セキュリティ アプライアンス（ASA）の **show interface コマンドの出力に表示されるエラーに気付く場合があります。**

## 前提条件

### 要件

このドキュメントに特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内容は、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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、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。

## 問題

ASA インターフェイスのエラー カウンタ「overrun」は、ネットワーク インターフェイスでパケットが受信されたにもかかわらず、インターフェイス FIFO キューにパケットを保存するために使用可能なスペースがなかった回数を追跡します。そのため、パケットは破棄されます。このカウンタの値は、**show interface コマンドで確認できます。**

問題を表示する出力例：

```
ASA# show interface GigabitEthernet0/1
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
Full-Duplex(Full-duplex), 1000 Mbps(1000 Mbps)
Input flow control is unsupported, output flow control is off
MAC address 0026.0b31.0c59, MTU 1500
IP address 10.0.0.113, subnet mask 255.255.0.0
580757 packets input, 86470156 bytes, 0 no buffer
Received 3713 broadcasts, 0 runts, 0 giants
2881 input errors, 0 CRC, 0 frame, 2881 overrun, 0 ignored, 0 abort
0 pause input, 0 resume input
0 L2 decode drops
905828 packets output, 1131702216 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops, 0 tx hangs
input queue (blocks free curr/low): hardware (255/230)
output queue (blocks free curr/low): hardware (255/202)
```

上記の例では、ASAが起動した後、またはカウンタを手動でクリアするためにコマンド**clear interfaceを入力した**後で、2881のオーバーランドがインターフェイスで確認されています。

# インターフェイス オーバーランの原因

通常、インターフェイス オーバーランのエラーは、次の要因の組み合わせによって発生します。

- ソフトウェア レベル：ASA ソフトウェアがインターフェイス FIFO キューのパケットを取り出す速度が遅すぎます。これにより FIFO キューがいっぱいになり、新しいパケットが廃棄されてしまいます。
- ハードウェア レベル：パケットがインターフェイスに到着する速度が速すぎるため、ASA ソフトウェアがパケットを引き出す前に FIFO キューがいっぱいになってしまいます。通常、パケットのバーストにより、FIFOキューが短時間で最大キャパシティまで満たされます。

# インターフェイス オーバーランの原因をトラブルシューティングする手順

この問題のトラブルシューティングを行い、対処する手順は次のとおりです。

1. ASA で CPU ホグが発生しているかどうか、また CPU ホグが問題の一因となっているかどうかを確認します。長期的または頻繁な CPU ホグを緩和するように努めてください。
2. インターフェイスのトラフィック レートを理解し、ASA がトラフィック プロファイルによってオーバーサブスクライブされたのかどうかを確認します。
3. 断続的なトラフィック バーストが原因で問題が発生するかどうかを確認します。その場合、ASA インターフェイスおよび隣接スイッチポートでフロー制御を実装します。

# 考えられる原因と解決方法

## ASA の CPU が着信パケット（CPU Hog）を処理するために定期的に過度のビジー状態になる

ASAプラットフォームは、ソフトウェアのすべてのパケットを処理し、すべてのシステム機能(syslog、Adaptive Security Device Manager(ASDM)接続、アプリケーションインスペクションなど)を処理するメインCPUコアを使用して、着信パケットを処理します。ソフトウェアのプロセスによって CPU が必要以上に長く保持される場合、プロセスが CPU を「ホグ状態」にするため、ASA で CPU ホグ イベントとして記録されます。CPU ホグのしきい値はミリ秒単位で設定されており、各ハードウェア アプライアンス モデルによって異なります。しきい値は、ハードウェア プラットフォームの CPU 処理能力とデバイスが処理できる潜在的なトラフィック レートを考慮して、インターフェイス FIFO キューがいっぱいになるまでにどのくらいの時間がかかるかに基づいています。

CPU ホグは 5505、5510、5520、5540、および 5550 などのシングルコア ASA でのインターフェイス オーバーラン エラーの原因となる場合があります。100 ミリ秒以上にわたる長いホグでは、比較的低いトラフィック レベルおよび非バースト トラフィック レートにおいて特にオーバーランが発生する可能性があります。この問題は、いずれかの CPU コアがプロセスによってホグ状態になっても、その他のコアが Rx リングのパケットを引き出せるため、マルチコア システムでは大きく影響しません。

デバイスのしきい値を超えるホグは、次に示すように ID 711004 で syslog を生成します。

```
20132614:40:42:%ASA-4-711004:60= sshPC = 90b0155= 20132614:40:42:%ASA-4-711004:60= sshPC =
90b0155= 0x090b0155 0x090bf3b6 0x090b3b84 0x090b3f6e 0x009 0b4459 0x090b44d6 0x08c46fcc
0x09860ca0 0x080fad6d 0x080efa5a 0x080f0a1c0x0806922c
```

また、CPU ホグ イベントはシステムによって記録されます。**show proc cpu-hog コマンドの出力は、次のフィールドを表示します。**

- Process：CPU をホグ状態にしたプロセスの名前。
- PROC_PC_TOTAL：このプロセスが CPU をホグ状態にした合計回数。
- MAXHOG：そのプロセスにおいて、発生した最も長い CPU ホグのミリ秒単位の時間。
- LASTHOG：最後のホグが CPU を保持したミリ秒単位の時間。
- LASTHOG At：CPU ホグが最後に発生した時間。
- PC：CPU ホグ発生時のプロセスのプログラム カウンタ値。（Cisco Technical Assistance Center（TAC）向けの情報）
- Call stack：CPU ホグ発生時のプロセスのコール スタック。（Cisco TAC 向けの情報）

この例では、**show proc cpu-hog コマンドの出力を示します。**

ASA#

**show proc cpu-hog**

```
Process:    ssh, PROC_PC_TOTAL: 1, MAXHOG: 119, LASTHOG: 119
LASTHOG At: 12:25:33 EST Jun 6 2012
PC:         0x08e7b225 (suspend)

Process:    ssh, NUMHOG: 1, MAXHOG: 119, LASTHOG: 119
```

```
LASTHOG At: 12:25:33 EST Jun 6 2012
PC:         0x08e7b225 (suspend)
Call stack: 0x08e7b225 0x08e8a106 0x08e7ebf4 0x08e7efde 0x08e7f4c9 0x08e7f546 0x08a7789c
            0x095a3f60 0x080e7e3d 0x080dcfa2 0x080ddf5c 0x0806897c

CPU hog threshold (msec): 10.240
Last cleared: 12:25:28 EST Jun 6 2012
ASA#
```

ASA SSH プロセスによって、2012 年 6 月 6 日の 12:25:33 EST に 119 ミリ秒の間 CPU が専有されました。

インターフェイスでオーバーランエラーが継続的に増加する場合は、**show proc cpu-hogコマンドの出力を調べ**て、CPU hogイベントがインターフェイスオーバーランカウンタの増加と相関するかどうかを確認します。CPUホグがインターフェイスオーバーランのエラーの原因となることがわかった場合は、Bug Toolkitでバグを検索するか、Cisco TACでケースを提起することをお勧めします。**show tech-support command コマンドの出力には、show proc cpu-hog コマンドの出力も含まれます。**

## 処理されるトラフィック プロファイルが定期的に ASA をオーバーサブスクライブする

トラフィック プロファイルによっては、ASA を通過するトラフィックが処理するには多過ぎるため、オーバーランが発生する場合があります。

トラフィック プロファイルは、（その他の要素に加えて）次のもので構成されます。

- パケット サイズ
- パケット間のギャップ（パケット レート）
- プロトコル：一部のパケットは ASA のアプリケーション検査の対象となり、他のパケットよりも多くの処理が必要です。

次のASA機能を使用して、ASAのトラフィックプロファイルを識別できます。

- NetFlow - ASAは、NetFlowバージョン9レコードをNetFlowコレクタにエクスポートするように設定できます。その後、トラフィック プロファイルの詳細を理解するために、このデータを分析できます。

- SNMP - ASAインターフェイスのトラフィックレート、CPU、接続レート、および変換レートを追跡するために、SNMPモニタリングを使用します。その後、情報を分析して、トラフィックパターンと時間の経過とともに変化する方法を理解できます。オーバーランの増加と相関関係のあるトラフィック レートの上昇があるかどうか、そのトラフィックの上昇の原因を調べてみてください。TAC ではネットワークのデバイスが誤動作し（設定ミスやウイルス感染が原因で）、トラフィックのフラッディングが定期的に生成される問題が報告されています。

## 断続的なパケット バーストによる ASA インターフェイス FIFO キューのオーバーサブスクライブ

CPU が FIFO からパケットを引き出す前に、NIC に到着するパケットのバーストにより FIFO がいっぱいになる可能性があります。通常、この問題を解決するために実行できる多くはありませんが、ネットワークでQoSを使用してトラフィックバーストを平滑化したり、ASAと隣接スイッチポートのフロー制御を行ったりすることで、緩和できます。

フロー制御は、ASAのインターフェイスが隣接デバイス（スイッチポートなど）にメッセージを送信できるようにして、短時間トラフィックの送信を停止するように指示する機能です。これは

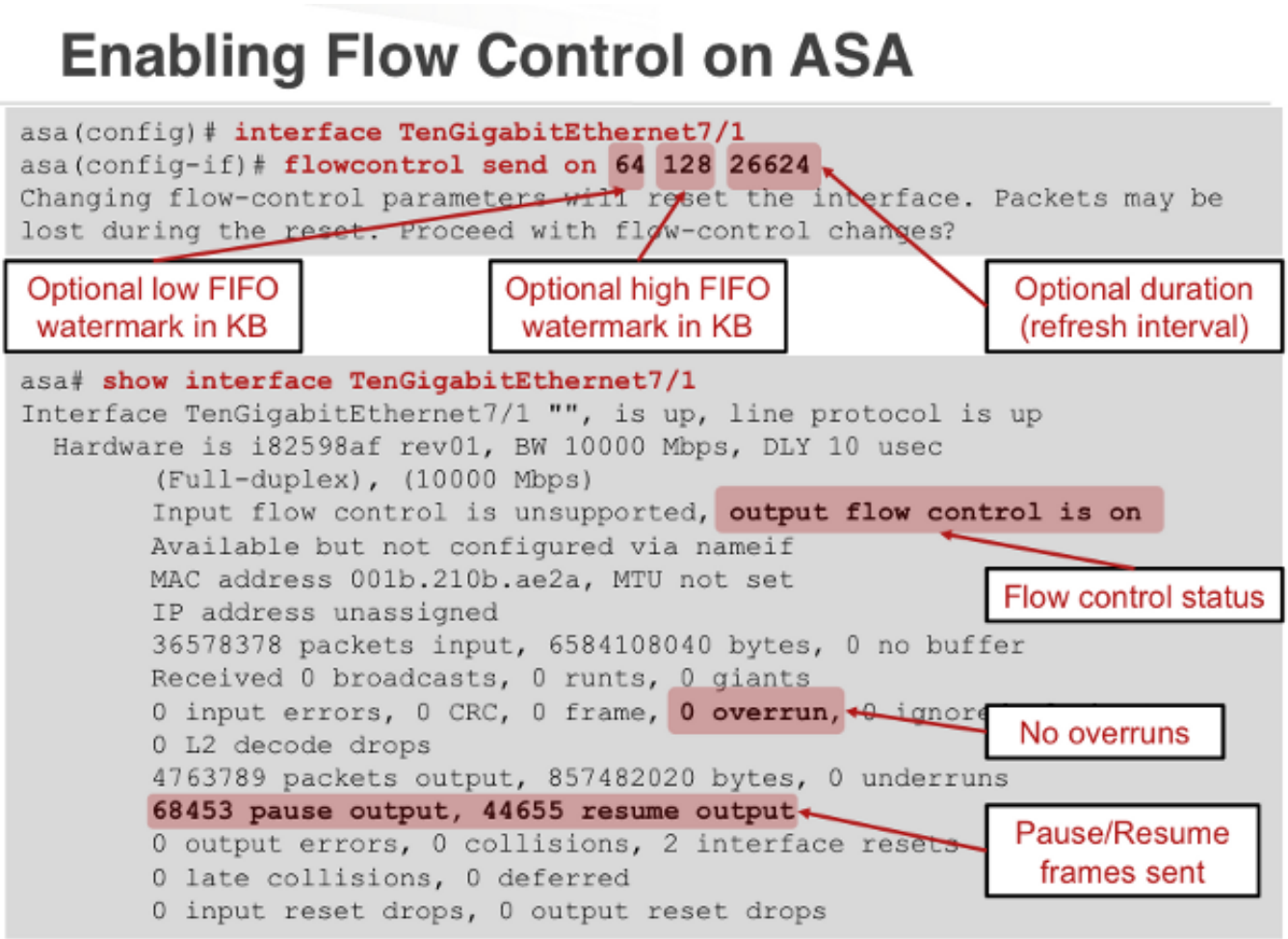
FIFO が特定の上限に達すると実行されます。ある程度まで FIFO が解放されたら、ASA NIC は再開フレームを送信し、スイッチポートはトラフィックの送信を続行します。通常、隣接するスイッチポートにはより多くのバッファ スペースがあり、受信方向側で ASA が処理するよりも送信時にパケットのバッファリングに優れているため、この方法が適切です。

トラフィックのマイクロバーストを検出するように、ASA のキャプチャをイネーブルにすることを試みることはできますが、ASA によって処理されてメモリのキャプチャに追加される前にパケットが廃棄されるため、通常は有効ではありません。外部スニファでトラフィック バーストをキャプチャして識別することもできますが、外部スニファがバーストによって圧倒される場合もあります。

## インターフェイス オーバーランを緩和するためにフロー制御をイネーブルにする

フロー制御機能は 10GE インターフェイスではバージョン 8.2(2) 以降、1GE インターフェイスではバージョン 8.2(5) 以降の ASA に追加されています。オーバーランが発生する ASA インターフェイスでフロー制御をイネーブルにする機能は、パケット廃棄の発生を防ぐ有効な技術であることが証明されます。

詳細については、『Cisco ASA 5500 シリーズ コマンド リファレンス 8.2 のフロー制御機能』を参照してください。




*( 図の引用元 : Andrew Ossipov の Cisco Live プレゼンテーション BRKSEC-3021 )*

「output flow control is on」は、ASA によってフロー制御のポーズ フレームが ASA インターフェイスから隣接デバイス ( スイッチ ) に送信されることを意味することに注意してください。「Input flow control is unsupported」は、ASA が隣接デバイスからのフロー制御フレームの受信を

サポートしないことを意味します。

フロー制御の設定例:

```
interface GigabitEthernet0/2

flowcontrol send on

 nameif DMZ interface
 security-level 50
 ip address 10.1.3.2 255.255.255.0
!
```

# 関連情報

- ASA 8.3 以降：パフォーマンスの問題のモニタとトラブルシューティング
- Cisco Liveプレゼンテーション「ファイアウォールパフォーマンスの最大化」: このプレゼンテーションでは、さまざまなASAプラットフォームのアーキテクチャの概要を説明し、パフォーマンスとチューニングに関する情報を提供します。このプレゼンテーションにアクセスするには、にログインしてください。 Ciscolive!365 プレゼンテーション番号BRKSEC-3021を検索します。
- Cisco TACセキュリティポッドキャストエピソード#7「ファイアウォールパフォーマンスの監視」：このポッドキャストエピソードでは、ファイアウォールのパフォーマンスを監視し、パフォーマンスの問題を特定するためのテクニックと方法について説明します。
- テクニカル サポートとドキュメント – Cisco Systems