ASAのパフォーマンス問題の監視とトラブルシューティング

内容

はじめに

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)のパフォーマンスを監視およびトラブルシューティングするために使用するコマンド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、バージョン 8.3 以降を稼働する Cisco 適応型セキュリティ アプライアンス（ASA）に基づいています。

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、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

表記法

表記法の詳細については、『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。

パフォーマンス問題のトラブルシューティング

パフォーマンスの問題をトラブルシューティングするには、このセクションで説明する基本部分を確認します。

注：ご使用のシスコデバイスの、show コマンドの出力データがあれば、Cisco CLI Analyzerを使用して今後予想される障害と修正を表示できます。Cisco CLIアナライザ（登録ユーザ専用）は、特定のshow コマンドをサポートします。Cisco CLI Analyzerを使用するには、シスコの登録ユーザであり、シスコアカウントにログインし、ブラウザでJavaScriptを有効にしている必要があります。

速度とデュプレックスの設定

セキュリティ アプライアンスは、インターフェイスの速度とデュプレックスの設定を自動的に検出するようにあらかじめ設定されています。ただし、自動ネゴシエーションプロセスが失敗し、速度またはデュプレックスのいずれかのミスマッチ（およびパフォーマンスの問題）が発生する原因となる状況がいくつかあります。ミッション クリティカルなネットワーク インフラストラクチャの場合、シスコがインターフェイスごとに速度とデュプレックス モードを手動でハードコーディングするため、エラーが発生する可能性はありません。通常、これらのデバイスは移動しないため、適切に設定すれば変更する必要はありません。

どのようなネットワーク デバイスでも、リンク速度は検出可能ですが、デュプレックスはネゴシエートする必要があります。2台のネットワークデバイスが速度とデュプレックスを自動ネゴシエートするように設定されている場合、それらのデバイスは速度とデュプレックス機能をアドバタイズするフレーム(Fast Link Pulse(FLP)と呼ばれる)を交換します。未対応のリンク パートナーにとっては、これらのパルスは通常の 10 Mbps フレームのように見えます。パルスをデコードできるリンク パートナーにとっては、FLP にはリンク パートナーが提供できる速度とデュプレックスの設定がすべて含まれています。FLP を受信した端末はそのフレームに対する確認応答を返し、各デバイスは互いに速度およびデュプレックスを、それぞれ実現可能な最高の状態に合わせます。一方のデバイスが自動ネゴシエーションをサポートしていない場合、他方のデバイスはFLPを受信し、並行検出モードに移行します。相手の速度を感知するために、デバイスはパルス長を聞き、その長さに基づいて速度を設定します。ここで、デュプレックスの設定の際に問題が生じます。デュプレックスはネゴシエートする必要があるため、自動ネゴシエートするように設定されているデバイスは他のデバイスの設定を判別できず、そのためIEEE 802.3u規格に従ってデフォルトの半二重に設定します。

たとえば、ASAインターフェイスを自動ネゴシエーションに設定し、100 Mbpsで全二重にハードコードされているスイッチにASAインターフェイスを接続すると、ASAからFLPが送信されます。ただし、スイッチは速度とデュプレックスがハードコードされているため応答せず、自動ネゴシエーションには参加しません。スイッチから応答を受信しないため、ASAは並行検出モードに移行し、スイッチが送信するフレームのパルス長を検出します。つまり、ASAはスイッチが100 Mbpsに設定されていることを検出し、これに基づいてインターフェイス速度を設定します。しかし、スイッチは FLP を交換しないため、ASA はスイッチが全二重で動作できるかどうかを検出できず、自身のインターフェイス デュプレックスを、IEEE 803.2u 規格に従って半二重に設定します。スイッチは100 Mbpsの全二重にハードコードされていて、ASAは（実際に）100 Mbpsの半二重に自動ネゴシエートしたばかりで、その結果デュプレックスのミスマッチが生じ、パフォーマンスに深刻な問題が発生する可能性があります。

速度またはデュプレックスの不一致は、通常、問題のあるインターフェイスでエラー カウンタの値が増加することによって判明します。最もよくあるエラーは、フレーム、Cyclic Redundancy Check（CRC; 巡回冗長検査）、およびラントです。これらの値がインターフェイスで増加している場合は、速度/デュプレックスの不一致またはケーブル配線の問題のいずれかが発生しています。この問題を解決してから、他の作業を行う必要があります。

例

<#root>

Interface GigabitEthernet0/0 "outside", is up, line protocol is up Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec Auto-Duplex(Full-duplex), A

157 runts

, 0 giants

379 input errors, 107 CRC, 273 frame

, 0 overrun, 0 ignored, 0 abort 0 pause input, 0 resume input 0 L2 decode drops 121 packets output, 774

CPU Utilization

CPU使用率が高い場合は、次の手順を実行してトラブルシューティングを行います。

- show xlate count の接続カウントが低いことを確認します。
- メモリ ブロックが正常であることを確認します。
- ACL の数値が高いことを確認します。
- show memory detailコマンドを発行し、ASAで使用されているメモリが正常な使用率であることを確認します。
- show processes cpu-hogおよびshow processes memoryのカウントが正常であることを確認します。
- セキュリティ アプライアンスの Inside または Outside に存在するすべてのホストが、ブロードキャスト/マルチキャスト トラフィックとなり得る悪意のあるトラフィックまたは大量のトラフィックを生成して、高い CPU 使用率を発生させる可能性があります。この問題を解決するには、アクセス リストを設定してホスト間（エンド ツー エンド）のトラフィックを拒否し、使用率を確認します。
- ASA インターフェイスでデュプレックスおよび速度の設定を確認します。リモートインターフェイスとの設定が一致しないと、CPU使用率が高くなる可能性があります。

次の例では、速度の不一致により *input error* と *overruns* の値が高くなっている状態が示されています。エラーを確認するには、show interface コマンドを使用します。

<#root>

```
Ciscoasa#
```

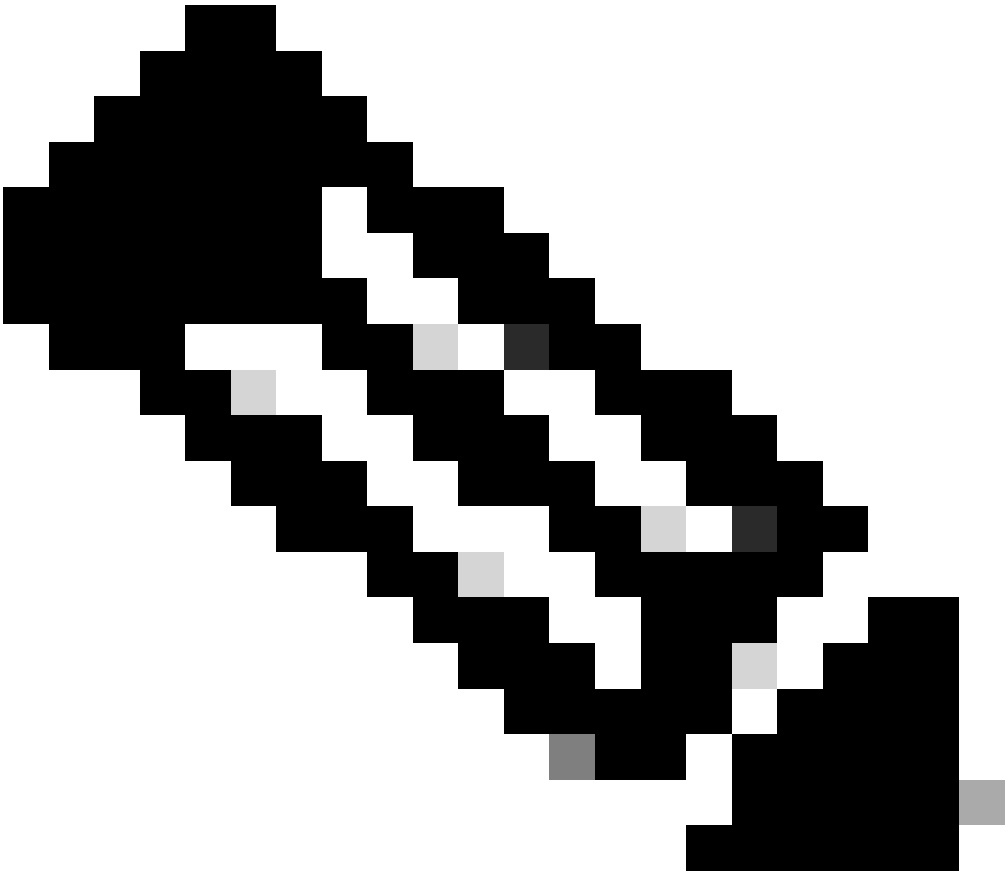
sh int GigabitEthernet0/1

```
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
 Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
       Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
       Input flow control is unsupported, output flow control is unsupported
       MAC address 0013.c480.b2b8, MTU 1500
       IP address 192.168.17.4, subnet mask 255.255.255.0
       311981 packets input, 20497296 bytes, 0 no buffer
       Received 311981 broadcasts, 157 runts, 0 giants
```

7186 input errors, 0 CRC, 0 frame, 7186 overrun

```
, 0 ignored, 0 abort
       0 pause input, 0 resume input
       0 L2 decode drops
       121 packets output, 7744 bytes, 0 underruns
       0 pause output, 0 resume output
       0 output errors, 0 collisions, 1 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 (255/249)
       output queue (blocks free curr/low): hardware (255/254)
```

この問題を解決するには、対応するインターフェイスの速度を *auto* に設定します。

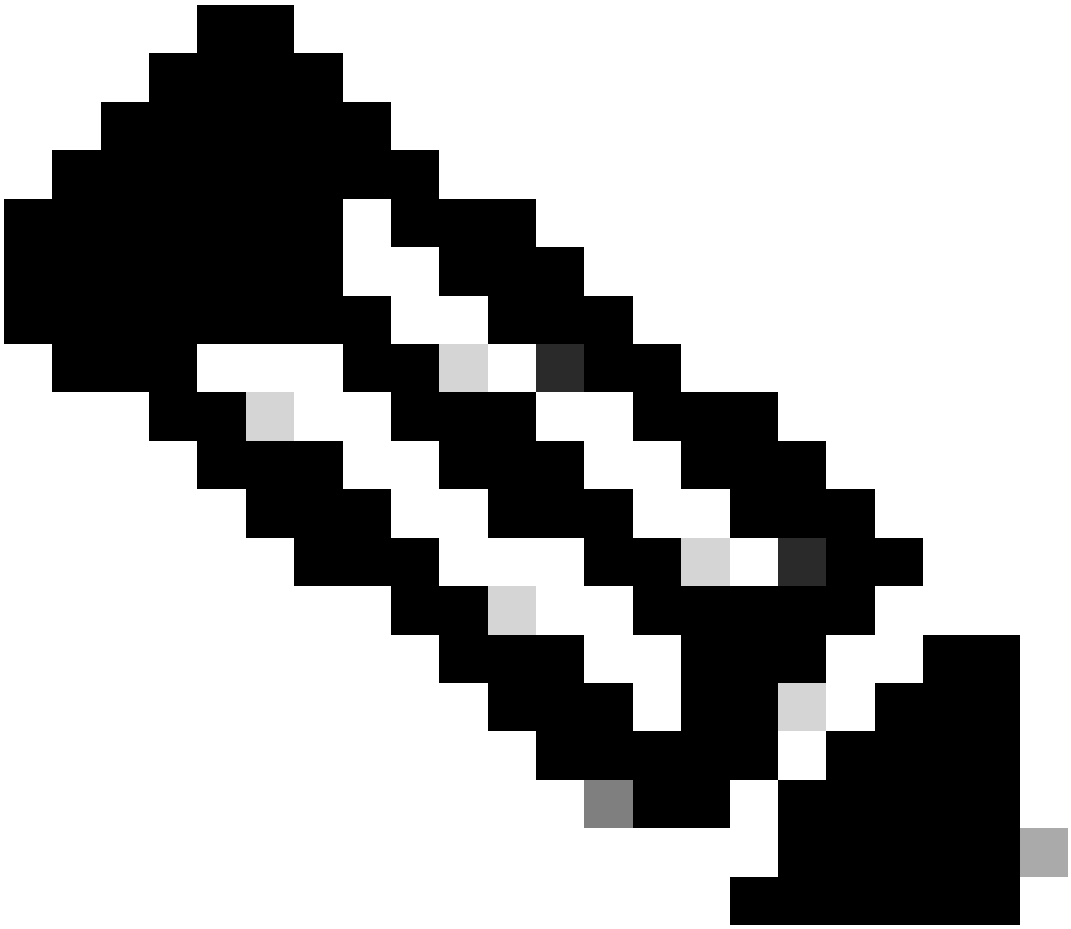


注：シスコでは、すべてのインターフェイスでip verify reverse-path interfaceコマンドを有効にすることを推奨します。これにより、有効な送信元アドレスを持たないパケットがドロップされ、CPU使用率が低下します。これは、FWSMでCPU使用率が高くなる問題が発生している場合に適用されます。

- CPU の使用率が高くなるもう 1 つの原因として可能性があるのは、マルチキャスト ルートの過多です。ASAが受信するマルチキャストルートが多すぎるかどうかを確認するには、show mrouteコマンドを発行します。

- ネットワークでサービス拒絶攻撃が発生しているかどうかを確認するには、show local-hostコマンドを使用します。これは、ネットワークでのウイルス攻撃を示す場合があります。

- CPUの高使用は、Cisco Bug ID CSCsq48636（登録ユーザ専用）が原因で発生する可能性があります。詳細は、Cisco Bug ID CSCsq48636（登録ユーザ専用）を参照してください。



注：シスコの内部ツールおよびバグ情報にアクセスできるのは、登録ユーザのみです。

注：前述の解決策で問題が解決しない場合は、要件に基づいてASAプラットフォームをアップグレードしてください。適応型セキュリティアプライアンスプラットフォームの機能についての詳細は、『セキュリティアプライアンス用のシスコセキュリティモジュール』を参照してください。詳細については、TAC(シスコテクニカルサポート)にお問い合せください。

高メモリ使用率

次に、高いメモリ使用率について可能性のある原因と解決策を示します。

- **イベントロギング：**イベント口ギングは大量のメモリを消費する可能性があります。この問題を解決するには、syslog サーバのような外部サーバをインストールし、すべてのイベントをそこに記録します。

- **メモリリーク：**セキュリティアプライアンスソフトウェアの既知の問題により、メモリの消費量が高くなる可能性があります。この問題を解決するには、セキュリティ アプライアンス ソフトウェアをアップグレードします。

- **Debugging Enabled:**デバッグは大量のメモリを消費する可能性があります。この問題を解決するには、`undebug all` コマンドでデバッグを無効にします。

- **ブロッキングポート：**セキュリティアプライアンスのOutsideインターフェイス上のブロッキングポートは、指定されたポートを通過するパケットをブロックするためにセキュリティアプライアンスが大量のメモリを消費する原因となります。この問題を解決するには、問題のトラフィックを ISP 側でブロックします。

- **脅威の検出：**脅威の検出機能は、さまざまな脅威に対して収集されたさまざまなレベルの統計情報と、スキャンされた脅威の検出で構成されます。この検出によって、ホストがスキャンを実行するタイミングが決まります。**消費するメモリを少なくするには、この機能をオフにします**。

PortFast、チャネリング、およびトランキング

Catalyst オペレーティング システム（OS）が稼働する Cisco スイッチなどの多くのスイッチが、デフォルトで、プラグアンドプレイ デバイスとして設計されています。そのため、ASAをスイッチに接続する場合、デフォルトのポートパラメータの多くは望ましくありません。たとえば、Catalyst OS が稼働するスイッチでは、デフォルトのチャネリングがオートに、トランキングがオートに、PortFast が無効に、それぞれ設定されています。Catalyst OSが稼働するスイッチにASAを接続する場合は、チャネリングを無効にし、トランキングを無効にして、PortFastを有効にします。

チャネリング（Fast EtherChannel または Giga EtherChannel とも呼ばれます）は、複数の物理ポートを 1 つの論理グループにバインドし、リンク全体のスループットを向上させるために使用されます。ポートを自動チャネリングに設定すると、ポートは、チャネルの一部かどうかを判断するために、リンクがアクティブになると、Port Aggregation Protocol（PAgP; ポート集約プロトコル）フレームを送出します。相手側のデバイスがリンクの速度とデュプレックスを自動的にネゴシエートしようとすると、これらのフレームが問題を引き起こす可能性があります。また、ポートのチャネリングがオートに設定されていると、リンクのアップ後、ポートがトラフィックの転送を始める前に、さらにおよそ 3 秒の遅延が発生します。

注:Catalyst XLシリーズスイッチでは、チャネリングはデフォルトでオートに設定されていません。このため、ASAに接続するすべてのスイッチポートでチャネリングを無効にする必要があります。

トランキング（一般的なトランキング プロトコルでは Inter-Switch Link（ISL; スイッチ間リンク）または Dot1q）では、複数の Virtual LAN（VLAN; 仮想 LAN）が単一のポート（またはリンク）に結合されます。通常、トランキングは 2 台のスイッチの双方で複数の VLAN が定義されているときにスイッチ間で使用されます。ポートが自動トランキングに設定されると、ポートでは、接続先のポートがトランキングを要求しているかどうかを判断するために、リンクがアップになると、Dynamic Trunking Protocol（DTP）フレームを送出します。これらのDTPフレームは、リンクの自動ネゴシエーションで問題を引き起こす可能性があります。スイッチ ポートでトランキングがオートに設定されていると、リンクのアップ後、ポートがトラフィックの転送を始める前に、さらにおよそ 15 秒の遅延が加わります。

PortFast（Fast Start とも呼ばれます）は、スイッチ ポートにレイヤ 3 デバイスが接続されていることをスイッチに通知するオプションです。ポートでは、デフォルトでの 30 秒間（15 秒のリッスンと 15 秒の学習）の待機が行われず、スイッチでは、リンクがアップした直後にポートが「フォワーディング」状況にされます。PortFast を有効にしてもスパニング ツリーが無効にならないことを理解することが重要です。そのポートのスパニング ツリーはまだ有効になっています。PortFast を有効にすると、リンクの他端に接続されている別のスイッチやハブ（レイヤ 2 専用デバイス）はないことのみが、スイッチに通知されます。スイッチでは、通常の 30 秒間の遅延が省略され、そのポートをアップした場合にレイヤ 2 ループが発生するかどうかの判定が試みられます。そのため、リンクがアップした後も、スイッチは引き続きスパニング ツリーに参加しています。ポートからは Bridge Packet Data Units（BPDU）が送出され、スイッチはそのポートで BPDU をリッスンしています。これらの理由から、ASAに接続するすべてのスイッチポートでPortFastを有効にすることを推奨します。

注:Catalyst OSリリース5.4以降にはset port host <mod>/<port>コマンドが組み込まれており、これを使用してチャネリングの無効化、トランキングの無効化、およびPortFastの有効化が1回のコマンドで実行できます。

ネットワーク アドレス変換（NAT）

各 NAT または NAT オーバーロード（PAT）セッションには、*xlate* と呼ばれる変換スロットが割り当てられます。これらの xlate は、xlate に影響する NAT ルールの変更を行った後でも存在する場合があります。このため、変換を受けるトラフィックによって、変換スロットの減少または予期しない動作のいずれか一方または両方が発生する場合があります。ここでは、セキュリティ アプライアンスの xlate を表示およびクリアする方法を説明します。

注意：セキュリティアプライアンスでxlateをグローバルにクリアすると、デバイスを通過するすべてのトラフィックのフ

⚠ ローが一瞬中断する場合があります。

Outside インターフェイスの IP アドレスを使用する PAT に対する ASA の設定の例を次に示します。

object network OBJ_GENERIC_ALL subnet 0.0.0.0 0.0.0.0 nat (inside,outside) source dynamic OBJ_GENERIC_ALL interface

セキュリティ アプライアンスを通過するトラフィックは、ほとんどが NAT の対象になります。セキュリティアプライアンスで使用されている変換を表示するには、show xlate コマンドを使用します。

<#root>

Ciscoasa#

show xlate

```
 5 in use, 5 most used Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice NA
```

変換スロットは、キーの変更を行った後でも残っている場合があります。セキュリティアプライアンス上の現在の変換スロットをクリアするには、clear xlateコマンドを発行します。

<#root>

Ciscoasa#

clear xlate

<#root>

Ciscoasa#

show xlate

0 in use, 1 most used

clear xlateコマンドは、xlateテーブルから現在のダイナミックトランスレーションをすべてクリアします。特定のIP変換をクリアするには、clear xlateコマンドとglobal [ip address]キーワードを使用できます。

NAT のための ASA の設定例を次に示します。

object network inside-net subnet 0.0.0.0 0.0.0.0 object network outside-pat-pool range 10.10.10.10 10.10.10.100 nat (inside,outside) source dynamic inside

内部の10.2.2.2から外部のグローバルな10.10.10.10への変換に対するshow xlateの出力に注意してください。

<#root>

Ciscoasa#

show xlate

2 in use, 2 most used

Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice

TCP PAT from inside:10.2.2.2/1429 to any:10.10.10.10/64768 flags ri idle 62:33:57 timeout 0:00:30

TCP PAT from inside:10.5.5.5/1429 to any:10.10.10.11/64768 flags ri idle 62:33:57 timeout 0:00:30

10.10.10.10 のグローバル IP アドレスに対する変換をクリアします。

<#root>

Ciscoasa# clear xlate global 10.10.10.10

この例では、Inside の 10.2.2.2 から Outside のグローバルな 10.10.10.10 への変換がなくなります。

<#root>

Ciscoasa#

show xlate

1 in use, 2 most used

Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice

TCP PAT from inside:10.5.5.5/1429 to any:10.10.10.11/64768 flags ri idle 62:33:57 timeout 0:00:30

Syslog

syslog を使用すると、ASA に関する問題をトラブルシューティングできます。Cisco では、ASA Firewall Syslog Server（PFSS）と呼ばれる Windows NT 対応の syslog サーバを無償で提供しています。PFSSは、Cisco Technical Support & Downloadsからダウンロードできます。

その他の複数のベンダーでは、Windows 2000やWindows XPなどの各種Windowsプラットフォームに対応したsyslogサーバが提供されています。UNIX および Linux では、ほとんどのマシンで syslog サーバがデフォルトでインストールされています。

syslog サーバを設定するときは、ASA から syslog サーバにログが送信されるように ASA を設定してください。

例：

<#root>

logging on logging host <ip_address_of_syslog_server> logging trap debugging

注：この例では、デバッグ（レベル7）とより重要なsyslogをsyslogサーバに送信するようにASAを設定しています。これらの ASA ログは最も詳細なログであるため、問題のトラブルシューティングを行うときにのみ使用してください。通常の運用では、ログ レベルを警告（レベル 4）またはエラー（レベル 3）に設定してください。

パフォーマンスが低下する問題がある場合は、テキスト ファイルの syslog を開き、パフォーマンスの問題に関係する送信元 IP アドレスを探します（UNIX を使用している場合は、syslog を grep して送信元 IP アドレスを探せます）。外部サーバが TCP ポート 113（Identification Protocol（Ident）の場合）で内部 IP アドレスへのアクセスを試みているものの、ASA がパケットを拒否していることを示すメッセージをチェックします。メッセージは次の例のようになります。

%ASA-2-106001: Inbound TCP connection denied from 10.64.10.2/35969 to 192.168.110.179/113 flags SYN

このメッセージを受信した場合は、service resetinboundコマンドをASAに発行します。ASAは通知せずにパケットをドロップするのではなく、このコマンドを実行すると、ASAはセキュリティポリシーによって拒否されているすべての着信接続をただちにリセットします。サーバでは、Ident パケットの TCP 接続がタイムアウトするのを待つのではなく、ただちにリセット パケットが受信されるようになります。

SNMP

企業への導入に推奨される方法は、SNMPを使用してCisco ASAのパフォーマンスを監視することです。Cisco ASAでは、SNMPバ

ージョン1、2c、3でこれがサポートされています。

セキュリティ アプライアンスを設定して、ネットワーク管理サーバ（NMS）にトラップを送信したり、NMS を使用して、セキュリティ アプライアンスの MIB を参照することができます。MIB は定義の集合であり、セキュリティ アプライアンスは定義ごとに値のデータベースを保持します。これに関する詳細は、『CLI 8.4および8.6を使用したCisco ASA 5500シリーズ設定ガイド』を参照してください。

Cisco ASA 対応のサポートされているすべての MIB は、『ASA の MIB サポート一覧』で確認できます。このリストから、次のMIBはパフォーマンスを監視する際に役立ちます。

- CISCO-FIREWALL-MIB ----フェールオーバーに役立つオブジェクトが含まれています。
- CISCO-PROCESS-MIB ---- CPU使用率に役立つオブジェクトが含まれています。
- CISCO-MEMORY-POOL-MIBには、メモリオブジェクトに役立つオブジェクトが----まれています。

逆 DNS ルックアップ

ASA でパフォーマンスが低下する場合は、ASA が使用している外部アドレスに対応した Domain Name System Pointer（DNS PTR）レコード（逆 DNS ルックアップ レコードとも呼ばれます）が、権威 DNS サーバ上にあることを確かめてください。このレコードには、グローバル ネットワーク アドレス変換（NAT）プール（または、インターフェイスでオーバーロードしている場合は ASA Outside インターフェイス）内のすべてのアドレスと、すべてのスタティック アドレス、および内部アドレス（それらのアドレスで NAT を使用していない場合）が含まれます。File Transfer Protocol（FTP；ファイル転送プロトコル）やTelnetサーバなどの一部のアプリケーションでは、DNS逆引き参照を使用して、ユーザの送信元と、ユーザが有効なホストであるかどうかを判別できます。逆 DNS ルックアップが解決しない場合は要求がタイムアウトするため、パフォーマンスが低下します。

これらのホストに対応するPTRレコードが存在することを確認するには、PCまたはUNIXマシンからnslookup コマンドを発行し、インターネットへの接続に使用するグローバルIPアドレスを指定します。

例

<#root>

```
% nslookup 192.168.219.25
 10.219.133.198.in-addr.arpa name = www.cisco.com.
```

そのIPアドレスに割り当てられたデバイスのDNS名を含む応答を受信する必要があります。応答がない場合は、DNS の管理者に連絡し、自分の各グローバル IP アドレスに対応した PTR レコードを追加するように依頼してください。

インターフェイスでのオーバーラン

トラフィック バーストが発生している場合、バーストが NIC の FIFO バッファまたは受信リング バッファのバッファリング容量を超えると、パケットがドロップされる可能性があります。フロー制御のポーズフレームを有効にすると、この問題を軽減できます。ポーズ (XOFF) および XON フレームは、FIFO バッファ使用量に基づいて、NIC ハードウェアによって自動的に生成されます。バッファ使用量が高ウォーター マークを超えると、ポーズ フレームが送信されます。フロー制御用のポーズ (XOFF) フレームをイネーブルにするには、次のコマンドを使用します。

<#root>

hostname(config)#

```
interface tengigabitethernet 1/0
 hostname(config-if)#
flowcontrol send on
```

show コマンド

show cpu usage

show cpu usageコマンドは、ASAのCPUにかかっているトラフィックの負荷を調べる際に使用します。トラフィックのピーク時、あるいはネットワークのサージや攻撃の発生時には、CPU 使用率が急激に上昇することがあります。

ASAは、パケットを処理し、デバッグメッセージをコンソールに出力するなど、さまざまなタスクを処理するための単一のCPUを備えています。プロセスにはそれぞれに目的があり、他のプロセスよりも多くの CPU 時間を必要とするプロセスもあります。おそらく暗号化が最もCPUを集中的に使用するプロセスです。そのため、ASAが暗号化されたトンネルを介して大量のトラフィックを渡す場合は、より高速なASA、VPN 3000などの専用VPNコンセントレータを検討する必要があります。VAC は、ASA の CPU から暗号化と復号化の負荷を取り除き、カード上のハードウェアで実行します。これにより、ASA でトリプル DES（168 ビット暗号化）を使用する 100 Mbps のトラフィックを暗号化/復号化することが可能になります。

大量のシステム リソースを消費する可能性のあるもう 1 つのプロセスとして、ロギングがあります。この理由から、ASA のコンソール、モニタ、およびバッファの ロギングを無効にすることを推奨します。問題のトラブルシューティングを行う際にはこれらの処理を有効にしても構いませんが、日常の運用では（特に CPU の処理能力が不足している場合）無効にしてください。また、syslogまたはSimple Network Management Protocol(SNMP)ロギング（ロギング履歴）をレベル5（通知）以下に設定することも推奨されます。また、no logging message <syslog_id> コマンドを使用して、特定のsyslogメッセージIDを無効にすることもできます。

Cisco Adaptive Security Device Manager(ASDM)のMonitoring タブには、ASAのCPU使用率を時間の経過とともに表示できるグラフもあります。このグラフを使用して、ASA の負荷を判定できます。

show cpu usage コマンドを使用すると、CPU使用率の統計情報を表示できます。

例

<#root>

Ciscoasa#

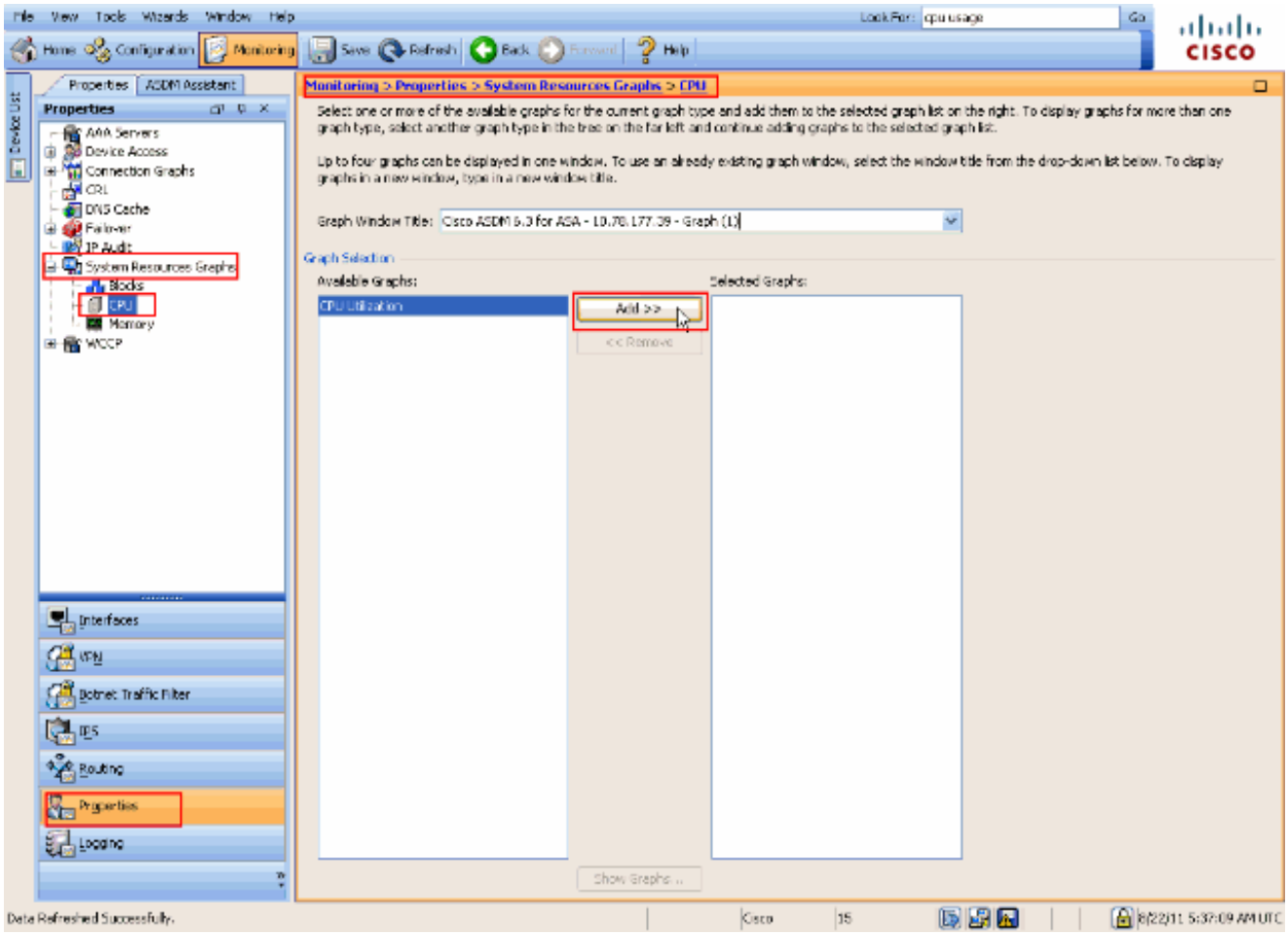
show cpu usage

```
 CPU utilization for 5 seconds = 1%; 1 minute: 2%; 5 minutes: 1%
```

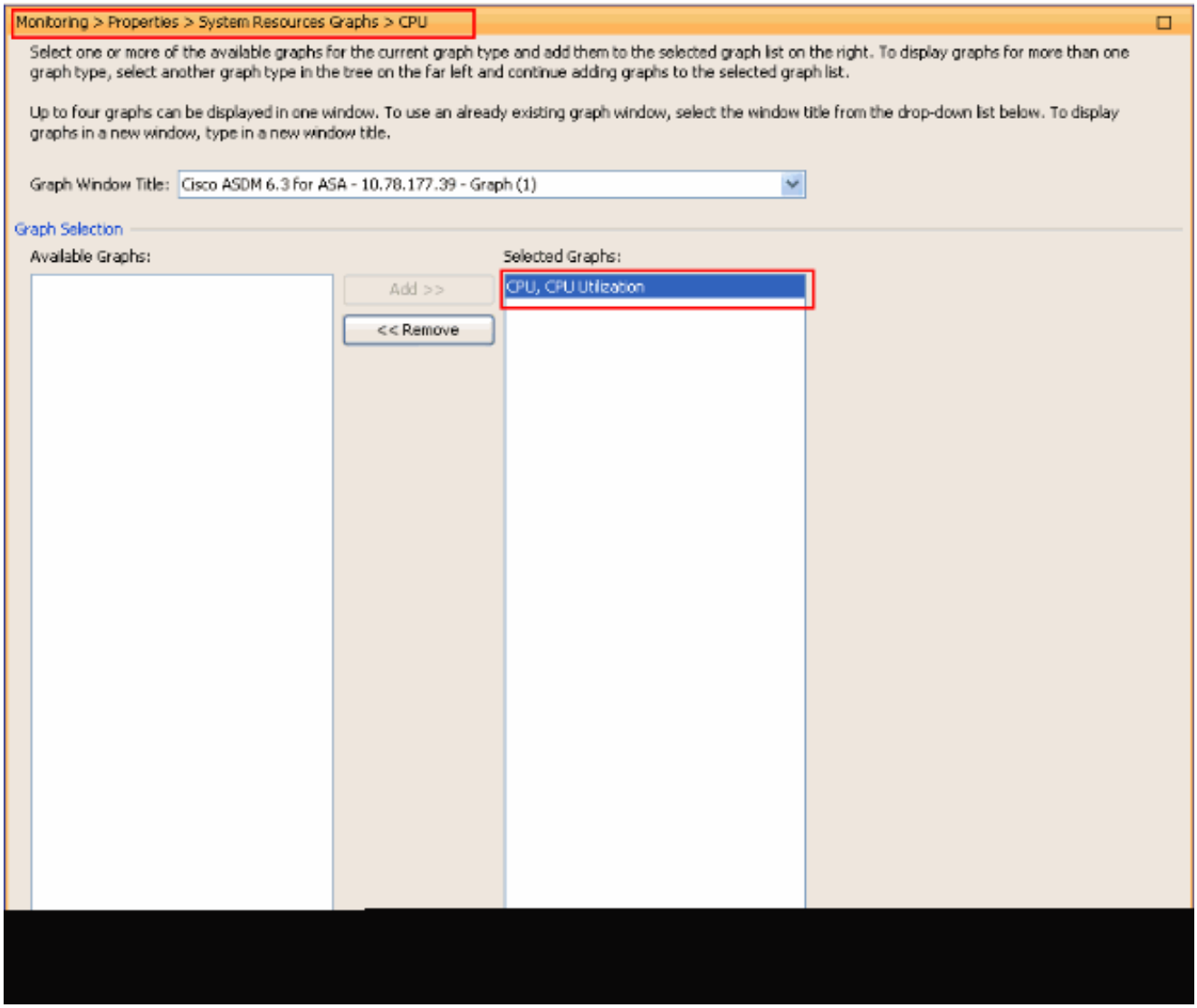
ASDMでのCPU使用率の表示

ASDM で CPU 使用率を表示するには、次の手順を実行します。

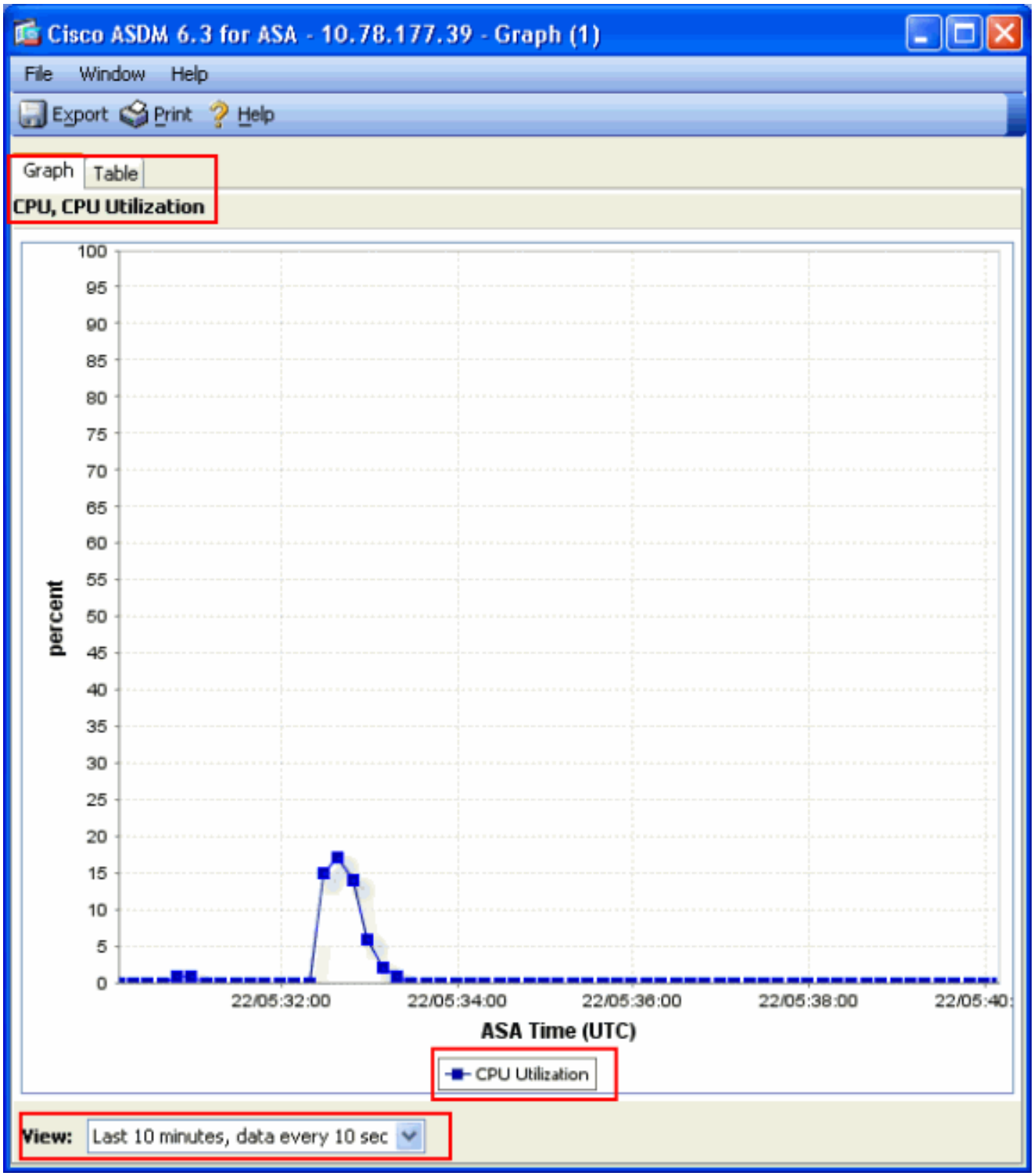
- ASDMでMonitoring > Properties > System Resources Graphics > CPU に移動し、**Graph Window Titleを選択します。次に**、[Available Graphs] **の一覧から [Add] をクリックして、必要なグラフを選択します。**



- 必要なグラフの名前が　[Selected Graphs] **セクションに追加したら、[Show Graphs] をクリックします。**



次の図は、ASDM 上の　**CPU 使用率のグラフを示します**。このグラフの異なるビューが使用可能で、[ビュー]ドロップダウンリストからビューを選択すると変更できます。必要に応じて、この出力を印刷したり、コンピュータに保存したりすることができます。



出力の説明

show cpu usage 出力の各フィールドの説明を次の表に示します。

フィールド	説明
CPU utilization for 5 seconds	最後の 5 秒間の CPU 使用率。
1 minute	CPU 使用率の 5 秒間のサンプルを最後の 1 分間で平均したもの。
5 分	CPU 使用率の 5 秒間のサンプルを最後の 5 分間で平均したもの。

show traffic

show traffic コマンドは、特定の時間内にASAを通過するトラフィックの量を示します。この結果は、コマンドが最後に発行されてから経過した時間間隔に基づきます。正確な結果を得るには、最初に **clear traffic** コマンドを発行し、1 ~ 10分待ってからshow traffic コマンドを発行します。show trafficコマンドを発行して、1 ~ 10分待ってから再度このコマンドを発行することもできますが、有効なのは2回目に発行したコマンドの出力だけです。

show trafficコマンドを使用すると、ASAを通過するトラフィックの量を調べることができます。インターフェイスが複数ある場合、コマンドは最も多くのデータを送受信しているインターフェイスの判別に役立ちます。インターフェイスが2つあるASAアプライアンスでは、Outsideインターフェイスの着信トラフィックと発信トラフィックの合計が、Insideインターフェイスの着信トラフィックと発信トラフィックの合計に等しくなる必要があります。

例

<#root>

Ciscoasa#

show traffic

```
 outside: received (in 124.650 secs): 295468 packets 167218253 bytes 2370 pkts/sec 1341502 bytes/sec tra
```

いずれかのインターフェイスが定格スループットに近づいている場合、またはそれに達している場合は、より高速なインターフェイスにアップグレードするか、またはそのインターフェイスに対して流入または流出するトラフィックの量を制限する必要があります。そうしないと、パケットが廃棄される可能性があります。**show interface**のセクションで説明されているように、インター

フェイスカウンタを調べることでスループットを判断できます。

show perfmon

show perfmonコマンドは、ASAが検出しているトラフィックの量とタイプを監視するために使用します。このコマンドは、1 秒あたりの変換（xlates）および接続（conn）の数を調べる唯一の手段です。接続はさらに TCP 接続と User Datagram Protocol（UDP; ユーザ データグラム プロトコル）接続とに分かれます。このコマンドが生成する出力については、**「出力の説明」を参照してください**。

例

PERFMON STATS Current Average Xlates 18/s 19/s Connections 75/s 79/s TCP Conns 44/s 49/s UDP Conns 31/s 30/s URL Access 27/s 30/s URL Serve

出力の説明

show perfmon 出力の各フィールドの説明を次の表に示します。

フィールド	説明
Xlates	1 秒間に生成された変換の数
接続	1 秒間に確立された接続の数
TCP Conns	1 秒あたりの TCP 接続の数
UDP Conns	1 秒あたりの UDP 接続の数
URL Access	1 秒間にアクセスされた URL（Web サイト）の数

URL Server Req	1秒あたりにWebsenseおよびN2H2に送信される要求の数です(filter コマンドが必要)
TCP Fixup	ASA が 1 秒間に転送する TCP パケットの数
TCPIntercept	スタティックに設定されている初期制限を超えた、1 秒あたりの SYN パケットの数
HTTP Fixup	ポート80を宛先とする1秒あたりのパケット数(fixup protocol httpコマンドが必要)
FTP Fixup	1 秒間に検出された FTP コマンドの数
AAA Authen	1 秒あたりの認証要求の数
AAA Author	1 秒あたりの認可要求の数
AAA Account	1 秒あたりのアカウンティング要求の数

show blocks

show cpu usageコマンドとともにshow blocksコマンドを使用すると、ASAが過負荷状態になっているかどうかを判定できます。

パケットブロック(1550および16384バイト)

ASA のインターフェイスに到着したパケットは入力インターフェイス キューに入れられ、最終的に OS に渡されてブロックに格納されます。イーサネット パケットの場合は 1550 バイトのブロックが使用されます。パケットが 66 MHz ギガビット イーサネット カードに到達した場合は 16384 バイトのブロックが使用されます。ASA は、アダプティブ セキュリティ アルゴリズム（ASA）に基づいてパケットを許可するか拒否するかを判断し、パケットを処理してから、発信インターフェイスの出力キューに渡します。ASA がトラフィックの負荷をサポートできない場合は、使用可能な 1550 バイト ブロック（66 MHz GE の場合は 16384 バイト ブロック）の数が 0 に近づきます（コマンド出力の CNT カラムに示されます）。CNT カラムが 0 になると、ASA は 8192 個を上限として、より多くのブロックを割り当てようとします。使用可能なブロックがなくなると、ASA はパケットを廃棄します。

フェールオーバー ブロックおよび syslog ブロック（256 バイト）

256 バイト ブロックは、主にステートフル フェールオーバー メッセージ用に使用されます。アクティブ ASA はパケットを生成してスタンバイ ASA に送り、変換テーブルおよび接続テーブルを更新します。バーストトラフィックが発生している間は、作成または削除される接続の割合が高くなり、使用可能な256バイトブロックの数が0になることがあります。この低下は、1 つ以上の接続がスタンバイ ASA に対して更新されていないことを示します。この場合、ステートフル フェールオーバー プロトコルによって、失われた変換または接続が次の機会に捕捉されるため、通常このような状態は許容されます。ただし、256 バイト ブロックの CNT カラムが長い間 0 または 0 付近に留まっている場合は、ASA が処理している 1 秒あたりの接続数が原因で、ASA は変換テーブルおよび接続テーブルの同期を維持できません。この問題が絶えず発生する場合は、ASA をより高速なモデルにアップグレードしてください。

ASA から送出される syslog メッセージも 256 バイト ブロックを使用しますが、これらは通常 256 バイト ブロックのプールを使い切るほど大量に送出されることはありません。CNT カラムで 256 バイト ブロックの数が 0 付近を示している場合は、ログをデバッグ (レベル 7) で syslog サーバに記録していないかどうかを確かめます。これは ASA 設定の logging trap 行に示されます。デバッグのために追加情報が必要な場合を除き、ロギングを通知 (レベル5) 以下に設定することをお勧めします。

例

<#root>

Ciscoasa#

show blocks

```
 SIZE MAX LOW CNT 4 1600 1597 1600 80 400 399 400 256 500 495 499 1550 1444 1170 1188 16384 2048 1532 1
```

出力の説明

show blocks出力の各カラムの説明を次の表に示します。

カラム	説明

SIZE	ブロック プールのサイズ (バイト) 。それぞれのサイズは、特定のタイプを表しています。
MAX	指定したバイト ブロックのプールで使用可能なブロックの最大数。起動時に、最大限のブロック数がメモリから切り分けられます。通常、最大ブロック数は変化しません。例外として、256 バイトおよび 1550 バイトのブロックでは、適応型セキュリティ アプライアンスが必要なときにさらに多くのブロックを動的に作成することが可能で、最大 8192 個まで作成できます。
LOW	低基準値。この数は、適応型セキュリティ アプライアンスの電源がオンになった時点、またはブロックが (clear blocks コマンドで) 最後にクリアされた時点から、このサイズの使用可能なブロックが最も少なくなったときの数を示しています。LOW カラムが 0 である場合は、先行のイベントでメモリがいっぱいになったことを示します。
CNT	特定のサイズのブロック プールで現在使用可能なブロックの数。CNT カラムが 0 である場合は、メモリが現在いっぱいであることを意味します。

show blocks出力のSIZE行の値の説明を次の表に示します。

SIZE の値	説明
0	dupb ブロックで使用されます。
4	DNS、ISAKMP、URL フィルタリング、uauth、TFTP、TCP モジュールなどのアプリケーションの既存ブロックを複製します。また、このサイズのブロックは、通常、ドライバにパケットを送信するコードなどで使用できます。
80	TCP 代行受信で確認応答パケットを生成するために、およびフェールオーバー hello メッセージに使用されます。
256	ステートフルフェールオーバーのアップデート、syslog口ギング、およびその他のTCP機能に使用されます。これらのブロックは、主にステートフル フェールオーバーのメッセージに使用されます。アクティブ適応型セキュリティ アプライアンスはパケットを生成してスタンバイ適応型セキュリティ アプライアンスに送り、変換テーブルおよび接続テーブルを更新します。バーストトラフィックでは、高い割合で接続が作成または切断されるため、使用可能なブロック数が0になることがあります。この状況は、1 つ以上の接続がスタ

	ンバイ適応型セキュリティ アプライアンスに対して更新されていないことを示します。ステートフルフェールオーバープロトコルは、失われた変換または接続を次回に捕捉します。256バイトブロックのCNTカラムが長い間0または0付近に留まっている場合、適応型セキュリティアプライアンスでは、1秒あたりに処理される接続数のために、変換テーブルと接続テーブルの同期の維持に苦慮します。適応型セキュリティ アプライアンスから送出される syslog メッセージもまた 256 バイト ブロックを使用しますが、これらは通常 256 バイト ブロックのプールを使い切るほど大量に送出されることはありません。CNT カラムで 256 バイト ブロックの数が 0 付近を示している場合は、ログをデバッグ (レベル 7) で syslog サーバに記録していないかどうかを確かめます。これは、適応型セキュリティ アプライアンス設定の logging trap 行に示されます。デバッグのために追加情報が必要な場合を除き、ロギングは通知 (レベル5) 以下に設定することをお勧めします。
1550	適応型セキュリティアプライアンスを介して処理されるイーサネットパケットの保存に使用されます。パケットが適応型セキュリティアプライアンスインターフェイスに入ると、入力インターフェイスキューに配置され、オペレーティングシステムに渡されてブロックに配置されます。適応型セキュリティアプライアンスは、セキュリティポリシーに基づいてパケットを許可するか拒否するかを決定し、パケットを処理してから発信インターフェイスの出力キューに渡します。適応型セキュリティアプライアンス(ASA)がトラフィックの負荷に対応しようと努力している場合、使用可能なブロックの数が0に近づくことがあります (コマンド出力のCNTカラムに示されています) 。CNT カラムが 0 になると、適応型セキュリティ アプライアンスは 8192 個を上限として、より多くのブロックを割り当てようとします。使用可能なブロックがなくなると、適応型セキュリティ アプライアンスはパケットをドロップします。
16384	64 ビット 66 MHz のギガビット イーサネット カード (i82543) にのみ使用されます。イーサネット パケットの詳細については、1550 の説明を参照してください。
2048	制御の更新に使用される制御フレームまたはガイド付きフレーム。

show memory

show memoryコマンドは、ASAの物理メモリ(RAM)の合計と、現在使用可能なバイト数を表示します。この情報を使用するには、まず ASA がメモリを使用する方法を理解する必要があります。ASA は、ブート時に OS をフラッシュから RAM にコピーし、RAM から OS を実行します (ルータとまったく同様です) 。次に、ASA は自身のスタートアップ コンフィギュレーションをフラッシュからコピーして RAM に格納します。最後にASAは、show blocksのセクションで説明されているように、ブロックプールを作成するためにRAMを割り当てます。この割り当てが完了すると、ASA で追加の RAM が必要になるのは、コンフィギュレーションのサイズが増えた場合だけです。このほか、ASA は変換エントリと接続エントリも RAM に格納します。

通常の動作中は、ASAの空きメモリの変化はごくわずかです（あったとしてもごくわずかです）。通常、メモリ不足になる必要があるのは、攻撃を受けて何十万もの接続がASAを通過する場合だけです。接続をチェックするには、show conn count コマンドを発行します。このコマンドは、ASAを経由した接続の現在数と最大数を表示します。ASA がメモリ不足になると、最終的に ASA はクラッシュします。クラッシュが発生する前に、syslog(%ASA-3-211001)にメモリ割り当てエラーメッセージが表示される場合があります。

攻撃が原因でメモリ不足に陥っている場合は、シスコテクニカルサポートチームに連絡してください。

例

<#root>

Ciscoasa#

show memory

Free memory: 845044716 bytes (79%) Used memory: 228697108 bytes (21%) ------------- ---------------- T

show xlate

show xlate countコマンドは、ASAを経由した変換の現在数と最大数を表示します。変換とは内部アドレスから外部アドレスへのマッピングで、1 対 1 のマッピング（Network Address Translation（NAT; ネットワーク アドレス変換）と同じ）または多数対 1 のマッピング（Port Address Translation（PAT; ポート アドレス変換）と同じ）になります。このコマンドはshow xlateコマンドのサブセットで、ASA経由の各変換を出力します。コマンド出力に表示される「in use」の変換は、コマンドの発行時点でASA内に存在するアクティブな変換の数を表します。「most used」は、ASAの電源オン以降にASA上に存在した変換の最大数を表します。

注:1つのホストが複数の接続をさまざまな宛先に対して持つことができますが、変換は1つだけです。xlate のカウントが内部ネットワークのホスト数よりも極端に多い場合には、内部ホストのいずれかが侵入されている可能性があります。侵入された内部ホストは、送信元アドレスをスプーフィングして ASA からパケットを送出します。

注： vpnclientの設定が有効で、内部ホストがDNS要求を送出していると、show xlateコマンドで1つの固定変換に対して複数のxlateを表示できます。

例

<#root>

Ciscoasa#

show xlate count

 84 in use, 218 most used

<#root>

Ciscoasa(config)#

show xlate

 3 in use, 3 most used Flags: D - DNS, d - dump, I - identity, i - inside, n - no random, o - outside,

TCP PAT from inside:10.1.1.15/1026 to outside:192.168.49.1/1024 flags ri idle 62:33:57 timeout 0:00:30

UDP PAT from 10.1.1.15/1028 to outside:192.168.49.1/1024 flags ri idle 62:33:57 timeout 0:00:30

ICMP PAT from inside:10.1.1.15/21505 to outside:192.168.49.1/0 flags ri idle 62:33:57 timeout 0:00:30

最初のエントリは、Inside ネットワークのホスト ポート（10.1.1.15, 1026）から Outside ネットワークのホスト ポート（192.168.49.1, 1024）への TCP PAT です。「r」というフラグは、変換がポート アドレス変換であることを示しています。「i」というフラグは、変換が Inside アドレス ポートに適用されることを示します。

2番目のエントリは、内部ネットワーク上のホストポート(10.1.1.15、1028)から外部ネットワーク上のホストポート(192.168.49.1、1024)へのUDPポートアドレス変換(PAT)です。「r」というフラグは、変換がポート アドレス変換であることを示しています。「i」というフラグは、変換が Inside アドレス ポートに適用されることを示します。

3番目のエントリは、内部ネットワークのホストICMP ID(10.1.1.15, 21505)から外部ネットワークのホストICMP ID(192.168.49.1, 0)へのICMPポートアドレス変換です。「r」というフラグは、変換がポート アドレス変換であることを示しています。「i」というフラグは、変換が Inside アドレス ICMP ID に適用されることを示します。

Inside アドレス フィールドは、よりセキュアなインターフェイスからセキュアではないインターフェイスに横断するパケットの送信元アドレスが示されます。逆に、よりセキュアではないインターフェイスからセキュアなインターフェイスに横断するパケットでは、宛先アドレスが示されます。

show conn count

show conn countコマンドは、ASAを経由した接続の現在数と最大数を表示します。「接続」とは、内部アドレスから外部アドレスへのレイヤ 4 情報のマッピングです。ASA が TCP セッションの SYN パケットを受信するか、または UDP セッションの最初のパケットが到達すると、接続が作成されます。TCP セッション ハンドシェイクがクローズするとき、または UDP セッションでタイムアウトが発生したときに、ASA が最後の ACK パケットを受信すると、接続が削除されます。

接続回数が非常に多い（通常の50 ~ 100倍）場合は、攻撃を受けていることを示しています。高い接続カウントによってASAのメモリ不足が発生していないことを確認するには、show memoryコマンドを発行します。攻撃を受けている場合は、スタティック エントリあたりの最大接続数を制限できます。最大初期接続数を制限することも可能です。これにより、内部サーバが攻撃にさらされる事態を回避できます。詳細については、『CLI 8.4および8.6を使用したCisco ASA 5500シリーズ設定ガイド』を参照してください。

例

<#root>

Ciscoasa#

show conn count

```
 2289 in use, 44729 most used
```

show interface

show interface コマンドは、デュプレックスの不一致の問題やケーブルの問題を判別するために役立ちます。また、インターフェイスがオーバーラン状態かどうかを詳しく調べる場合にも役立ちます。ASA が CPU のキャパシティをほとんど使い切ると、1550 バイト ブロックの数が 0 に近づきます（66 MHz ギガビット イーサネット カードの場合は 16384 バイト ブロックの数を見ます

）。 また、別の指標として、インターフェイスの「no buffer」の増加が見られます。no buffer メッセージは、パケットに使用できるブロックがないためにパケットが廃棄されたことにより、インターフェイスがパケットを ASA OS に送信できないことを示します。no bufferの増加が頻繁に発生する場合は、show proc cpuコマンドを発行して、ASAのCPU使用率をチェックします。大きいトラフィック負荷のために CPU 使用率が高い場合は、十分な負荷の処理能力を持つ、より高性能な ASA にアップグレードします。

パケットが初めてインターフェイスに到達すると、パケットは入力ハードウェア キューに置かれます。入力ハードウェア キューがいっぱいになると、パケットは入力ソフトウェア キューに置かれます。パケットは入力キューから渡され、1550 バイト ブロック（66 MHz ギガビット イーサネット インターフェイスの場合は 16384 バイト ブロック）に格納されます。続いて ASA によってパケットの出力インターフェイスが決定され、パケットが該当するハードウェア キューに置かれます。ハードウェア キューがいっぱいになると、パケットは出力ソフトウェア キューに置かれます。いずれかのソフトウェア キューの最大ブロック数が大きくなると、インターフェイスがオーバーラン状態になります。たとえば、ASA に到達するトラフィックが 200 Mbps で、それらすべてが単一の 100 Mbps インターフェイスから送出される場合、発信インターフェイスの出力ソフトウェア キューは高い値を示し、インターフェイスが大量のトラフィックを処理できないことを示します。このような状況が起きている場合は、より高速なインターフェイスにアップグレードしてください。

例

<#root>

Ciscoasa#

show interface

```
 Interface GigabitEthernet0/1 "inside", is up, line protocol is up Hardware is i82546GB rev03, BW 1000
```

また、インターフェイスのエラーを確認する必要もあります。ラント、入力エラー、CRC、またはフレーム エラーが表示される場合は、デュプレックスの不一致が発生している可能性があります。ケーブルに問題がある場合もあります。二重モードに関する問題の詳細は、「速度と二重モードの設定」のセクションを参照してください。各エラー カウンタは、特定のエラーが原因でドロップされたパケットの数を表すことに注意してください。特定のカウンタが頻繁に増加している場合は、ASA のパフォーマンスが低下している可能性が高く、問題の根本的な原因を突きとめる必要があります。

インターフェイスカウンタを確認する際は、インターフェイスが全二重に設定されていると、コリジョン、レイトコリジョン、または遅延パケットが発生しないように注意してください。逆に、インターフェイスが半二重に設定されている場合は、コリジョン、一部のレイトコリジョン、および一部の遅延パケットを受信する必要があります。コリジョン、レイトコリジョン、および遅延パケットの合計数は、入力および出力パケットカウンタの合計の10 %を超えることはできません。コリジョンがトラフィック合計の 10 % を超えている場合は、リンクが過剰に使用されており、全二重へのアップグレードか、またはより高速なもの（10 ~ 100 Mbps）へのアップグレードが必要です。10 %のコリジョンとは、そのインターフェイスを通過するパケットの10 %をASAがドロップすることを意味します。これらの各パケットは再送信する必要があります。

インターフェイスカウンタについての詳細は、『Cisco ASA 5500シリーズ適応型セキュリティアプライアンスのコマンドリファレンス』でinterface コマンドを参照してください。

show processes

ASAの**show processes**コマンドは、コマンドの実行時にASAで実行されているアクティブなプロセスをすべて表示します。この情報は、CPU 時間が過剰に与えられているプロセスと、CPU 時間がまったく与えられていないプロセスを判別する際に役立ちます。この情報を取得するには、 **show processes** コマンドを2回発行して、インスタンスごとに約1分間待機します。問題のプロセスについて、1 回目の出力で表示される Runtime 値から、2 回目の出力で表示される Runtime 値を差し引きます。この結果は、その時間内にプロセスに与えられた CPU 時間の量 (ミリ秒) を示しています。プロセスによっては、特定の間隔で実行されるようにスケジューリングされているものや、処理すべき情報があるときにしか実行されないものがあります。すべてのプロセスの中で Runtime の値が最も大きいのは、おそらく 577poll プロセスです。577poll プロセスはイーサネット インターフェイスをポーリングし、それらのインターフェイスに処理する必要のあるデータがあるかどうかを調べています。

注：各ASAプロセスの調査は、このドキュメントの範囲外です。ここでは全体を簡単に説明します。ASAプロセスの詳細については、『ASA 8.3以降：パフォーマンスの問題の監視とトラブルシューティング』を参照してください。

コマンドの概要

要約すると、ASAにかかっている負荷を明らかにするには、show cpu usageコマンドを使用します。出力は稼働平均であることに注意してください。ASAでは、稼働平均で隠されていても、CPU使用率が瞬発的に上昇している可能性があります。ASA の CPU 使用率が 80 % に達すると、ASA による遅延が徐々に増え、CPU 使用率がおよそ 90 % に達するまで増え続けます。CPU 使用率が 90 % を超えると、ASA はパケットのドロップを始めます。

CPUの使用率が高い場合、CPU時間を最も使用しているプロセスを識別するには、**show processes** コマンドを使用します。この情報を使用して、CPU の使用率の高いプロセス (ロギングなど) が消費する時間を減らします。

CPU使用率が高くないにもかかわらず、パケットがまだ廃棄されていると判断される場合は、show interfaceコマンドを使用して、おそらくデュプレックスの不一致が原因と考えられるASAインターフェイスでのno buffersとcollisionsをチェックします。no buffer カウントが増えているにもかかわらず CPU 使用率が低い場合は、通過するトラフィックをインターフェイスがサポートできていません。

バッファに問題がない場合は、ブロックを調べます。1550バイトブロック(66 MHzギガカードの場合は16384バイトブロック)でshow blocksの出力の現在(CNT)のカラムが0に近い場合、ASAが過度にビジー状態になっているためにイーサネットパケットがドロップされている場合がほとんどです。この場合は、CPU の使用率が急激に上昇します。

ASAを経由した新しい接続に問題がある場合は、show conn countコマンドを使用して、ASA経由での現在の接続数をチェックします。

現在のカウントが高い場合は、show memoryの出力をチェックし、ASAがメモリ不足になっていないことを確認します。メモリ不足の場合は、show conn または show local-host コマンドを使用して接続元を調査し、ネットワークがサービス拒絶攻撃を受けていないかどうかを確認します。

他のコマンドを使用して、ASA を通過するトラフィックの量を測定することもできます。**show traffic** コマンドは、インターフェイスあたりのパケット数およびバイト数の集計を表示します。show perfmonは、ASAが検出しているタイプ別にトラフィックを細分化します。

関連情報

- Cisco ASA 5500-Xシリーズファイアウォール
- 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。