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

目次

概要

このドキュメントでは、Cisco Adaptive Security Appliance（ASA）のパフォーマンスの監視とトラブルシューティングを行うために使用できる ASA 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、コマンドを使用する前に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。

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: Ciscoデバイスからの**表示コマンド**の出力がある場合、潜在的な問題および修正を表示するために Cisco CLI アナライザ（登録ユーザのみ）を使用できます。 Cisco CLI アナライザはある種のshowコマンドをサポートします。 Cisco CLI アナライザを使用する場合、登録ユーザである必要があります Cisco アカウントにログオンしブラウザの内で有効に なる JavaScript がなければなりません。

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、いくつかの原因によってオート 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どちらかのミスマッチが発生する（そのためにパフォーマンス上の問題を引き起こされる）ことがあります。 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、このようなデバイスは移動することがないため、適切に設定してある場合は、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、ネットワーク デバイスは速度およびデュプレックスの能力をアドバタイズするフレーム（Fast Link Pulse（FLP; ファスト リンク パルス）と呼ばれます）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 を受け取って、並行検出モードに移行します。 パートナーの速度を検知するため、デバイスではパルスの長さをリッスンし、それに従っ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。 しかし、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に応答せず、自動ネゴシエーションには参加しません。 スイッチからの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知します。 つまり、ASA はスイッチが 100 Mbps に設定されていることを検知し、それに応じて自身の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 は規定どおりに 100 Mbps の半二重に自動ネゴシエートしたため、二重モードが一致しなくなり、パフォ

ーマンスの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

```
Interface GigabitEthernet0/0 "outside", 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
       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, 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)
```

CPU 使用率

CPU の使用率が高い場合は、次の手順でトラブルシューティングを行います。

1. show xlate count の接続カウントが低いことを確認します。
2. メモリ ブロックが正常であることを確認します。
3. ACL の数値が高いことを確認します。
4. 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。
5. 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。

6. 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。

7. 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設定が一致しないと、CPU の使用率が増加す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。

```
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: **ip verify reverse-path interface** CPU これは、高 CPU 使用率の問題が発生した FWSM に適用されます。

8. 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。

9. 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。

10. 高 CPU 使用率は、Cisco Bug ID CSCsq48636 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: 上記で提供される解決策で問題を解決できない場合、必要に応じて ASA プラットフォームをアップグレードします。 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とおよび能力の詳細は、『Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスのデータ シート』を参照してください。 詳細については、TAC（登録ユーザ専用）にお問

い合わせください。

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。

- **イベントのロギング**： イベント ロギングは、大量のメモリを消費する場合があります。 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 ソフトウェアで確認されている問題のため、メモリの消費量が高くなる場合があります。 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。
- **デバッグの有効化**： 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 インターフェイスにブロッキング ポートがあると、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。
- **脅威検出**： 脅威検出機能は、さまざまな脅威についての異なるレベルでの統計情報の収集とスキャニング脅威検出で構成され、この機能によってホストがスキャンを実行するタイミングを決定します。 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ときに、デフォルトのポート パラメータの多くは望ましい値になっていません。 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、トランキングを無効に、PortFast を有効に、それぞれ設定してください。

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ネゴシエートしようとしている場合、これらのフレームが問題の原因になることがあります。 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、デフォルトではチャネリングが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、リンクのオート ネゴシエーションに関する問題の原因になることがあります。 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。 以上の理由から、ASA に接続するすべてのスイッチ ポートで PortFast を有効にすることが推奨されます。

> **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。

```
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)
```

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。

```
Ciscoasa#show xlate

5 in use, 5 most used

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

NAT from any:192.168.1.10 to any:172.16.1.1/24

    flags s idle 277:05:26 timeout 0:00:00
```

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。

```
Ciscoasa#clear xlate
```

```
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 コマンドを使用して global [ip address] キーワードを指定します。

NAT のための ASA の設定例を次に示します。

```
Ciscoasa#show xlate
0 in use, 1 most used
```

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。

```
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。

```
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。

```
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、ソフトウェア ダウンロード（登録ユーザ専用）のページからダウンロードできます。

Kiwi Enterprises などの一部のベンダーから、 Windows 2000 や Windows XP などの各種 Windows プラットフォームに対応する 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。

次に、例を示します。

```
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）とそれ以上に重要な 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なものです。

```
logging on
logging host <ip_address_of_syslog_server> logging trap debugging
```

このメッセージを受信している場合は、ASA に対して service reset inbound コマンドを発行します。 ASA は通知なくパケットをドロップする代わりに、 このコマンドにより、ASA ではセキュリティ ポリシーによって拒否されるすべての着信接続がただちにリセットされるようになります。 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

SNMP を使用した Cisco ASA のパフォーマンスの監視は、企業での導入時に推奨される方法です。 Cisco ASA は SNMP バージョン 1、2c、および 3 によるネットワークの監視をサポートします。

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、『Cisco ASA での SNMP の設定』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。 この一覧から、次の MIB がパフォーマンスの監視に役立ちます。

- CISCO-FIREWALL-MIB ---- フェールオーバーに有用なオブジェクトが含まれています。
- CISCO-PROCESS-MIB ---- CPU 使用率に有用なオブジェクトが含まれています。
- CISCO-MEMORY-POOL-MIB ---- メモリ オブジェクトに有用なオブジェクトが含まれています。

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は、ユーザのアクセス元や、ユーザが有効なホストかどうかを判断するために、逆 DNS ルックアップを使用することがあります。 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

```
% nslookup 198.133.219.25
25.219.133.198.in-addr.arpa     name = www.cisco.com.
```

すると、その IP アドレスに割り当てられているデバイスの DNS 名を示す応答が受信されます。 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。 フロー制御用のポーズ フレームをイネーブルにすると、このような問題の発生を抑制できます。 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。

```
hostname(config)#interface tengigabitethernet 1/0

hostname(config-if)#
flowcontrol send on
```

詳細は、「物理インターフェイスのイネーブル化とイーサネット パラメータの設定」を参照してください。

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、さまざまな処理を 1 つの CPU で行っています。 たとえば、パケットの処理やコンソールへのデバッグ メッセージの出力などがあります。 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。 CPU を最も多く使用するプロセスはおそらく暗号化です。そのため、ASA が暗号化されたトンネルに大量のトラフィックを送る場合は、より高速な ASA や、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 のロギングまたは Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）のロギング（ロギング ヒストリ）のレベルを、5（通知）以下に設定する必要があります。 さらに、**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。

また、Cisco Adaptive Security Device Manager（ASDM）の [Monitoring] タブにはグラフがあり、ASA の CPU 使用率を経時的に表示できます。 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

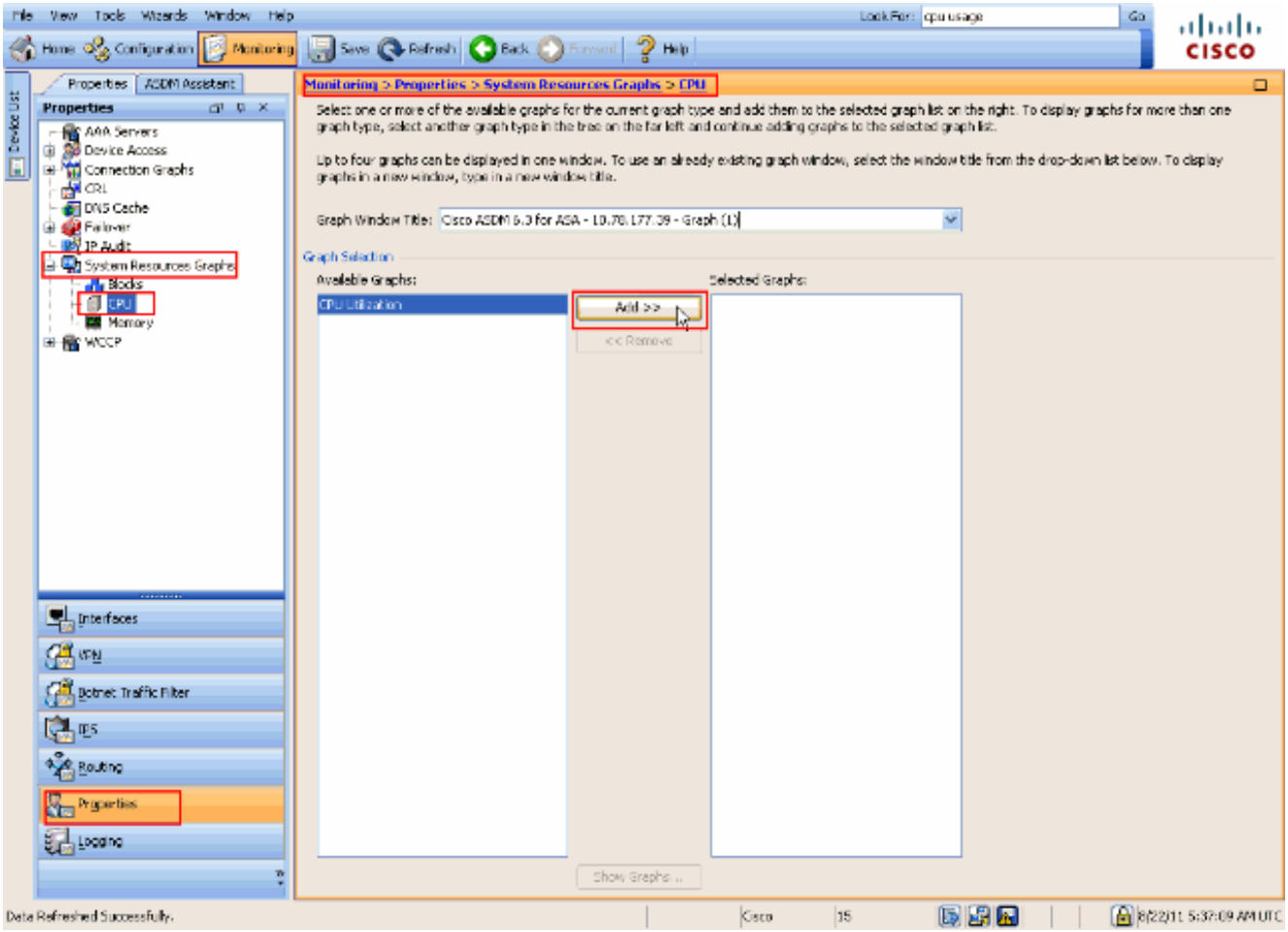
```
Ciscoasa#show cpu usage

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

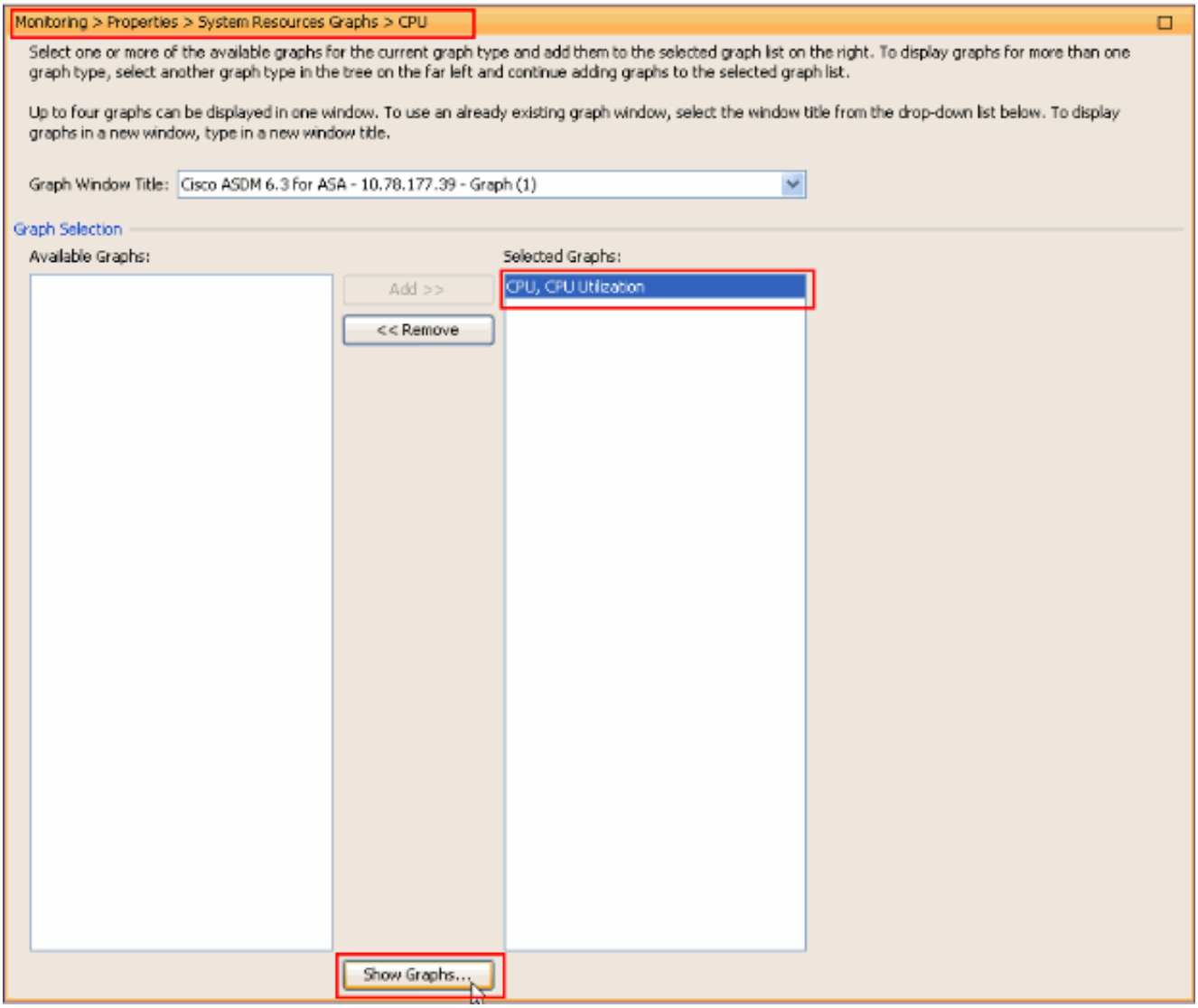
ASDM での CPU 使用率の表示

ASDM で CPU 使用率を表示するには、次の手順を実行します。

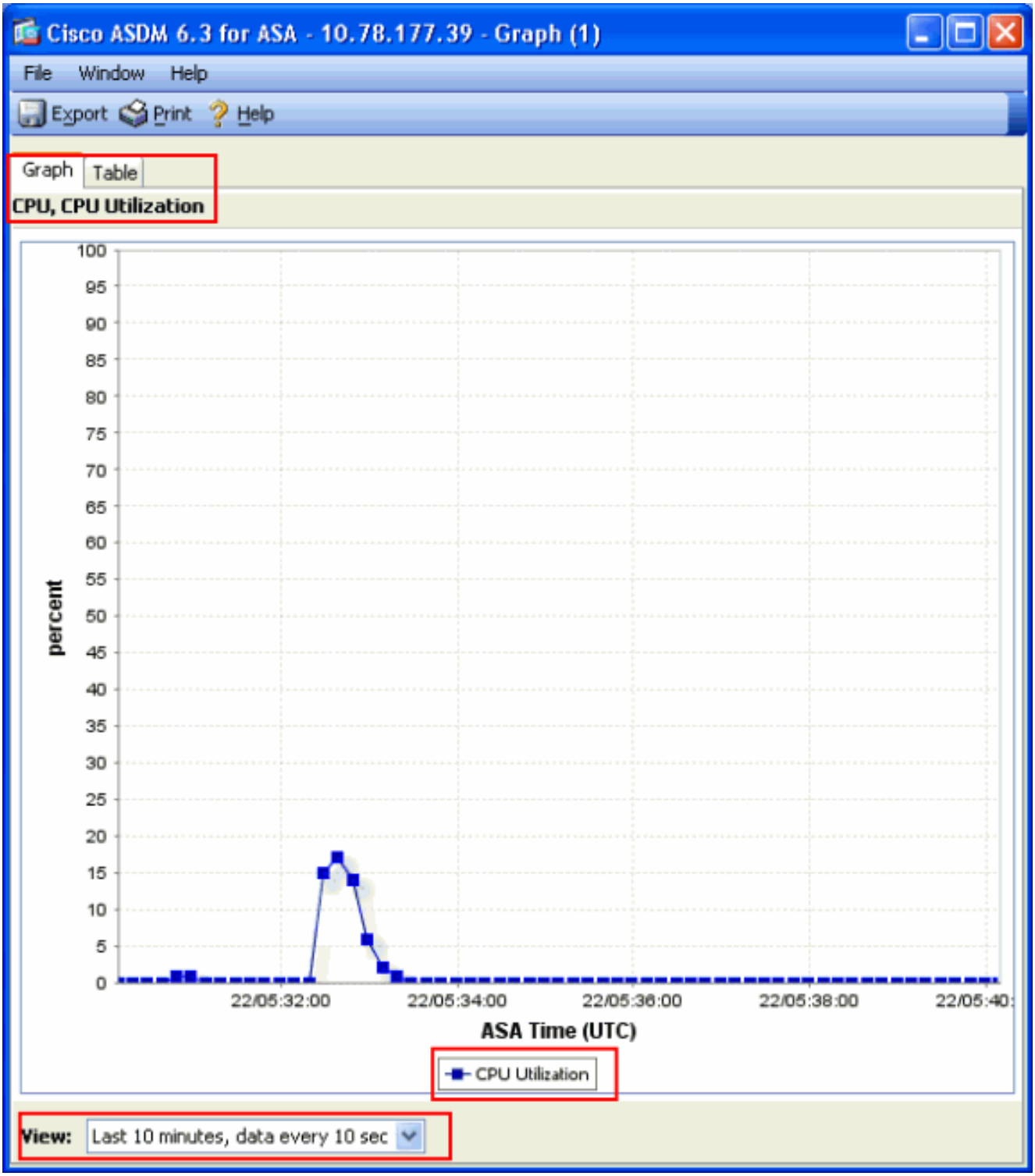
1. ASDM で [Monitoring] > [Properties] > [System Resources Graphics] > [CPU] の順に移動し、[Graph Window Title] を選択します。 次に、[Available Graphs] の一覧から [Add] をクリックして、必要なグラフを選択します。



2. 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。 このグラフではさまざまなビューを使用することができ、[View] ドロップダウン リストからビューを選択することで変更できます。 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、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ります。

例

```
Ciscoasa#show traffic
outside:
        received (in 124.650 secs):
                295468 packets  167218253 bytes
                2370 pkts/sec   1341502 bytes/sec
        transmitted (in 124.650 secs):
                260901 packets  120467981 bytes
                2093 pkts/sec   966449 bytes/sec
inside:
        received (in 124.650 secs):
                261478 packets  120145678 bytes
                2097 pkts/sec   963864 bytes/sec
        transmitted (in 124.650 secs):
                294649 packets  167380042 bytes
                2363 pkts/sec   1342800 bytes/sec
```

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

```
Ciscoasa#show traffic
outside:
        received (in 124.650 secs):
                295468 packets  167218253 bytes
                2370 pkts/sec   1341502 bytes/sec
        transmitted (in 124.650 secs):
                260901 packets  120467981 bytes
                2093 pkts/sec   966449 bytes/sec
inside:
        received (in 124.650 secs):
                261478 packets  120145678 bytes
                2097 pkts/sec   963864 bytes/sec
        transmitted (in 124.650 secs):
                294649 packets  167380042 bytes
                2363 pkts/sec   1342800 bytes/sec
```

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
Connections	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 秒間に Websense および N2H2 に送られた要求の数（**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の数（**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 blocks コマンドは、show cpu usage コマンドとともに使用することで、ASA が過負荷状態になっているかどうかを判定できます。

パケット処理ブロック（1550 バイトおよび 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。 バースト性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るため、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。 デバッグ目的で詳細な情報が必要な場合以外は、ログの通知レベルを 5 以下に設定することを推奨いたします。

例

```
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   1538
```

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 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 ユリティ 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、 ます。
低	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 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 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 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 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、パケットをドライバに送信する ドなどで使用されます。
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 用されます。
256	ステートフル フェールオーバーの更新、syslog 処理、およびその他の TCP 機能に使用されます。 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 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 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。 接続が頻繁に作成または切断される スト トラフィックが発生すると、使用可能なブロックの数が 0 まで低下することがあります。 こ 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 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、不明な変換または接続を次回に捕 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は、適応 キュリティ アプライアンスが処理している 1 秒あたりの接続数が原因で、適応型セキュリティ ア

1550	イアンス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。 適応型セキュリティ アプ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 loggin trap 行に示されます。 ロギングは、デバッグのために詳細な情報が必要となる場合を除いて、Notification（レベル 5）以下に設定することを推奨します。 適応型セキュリティ アプライアンス経由で処理されるイーサネット パケットの格納に使用されまパケットは、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ューに配置され、次にオペレーティング システムに渡されてブロックに配置されます。 適応型セリティ アプライアンスは、パケットを許可するか拒否するかをセキュリティ ポリシーに基づいてし、パケットを発信インターフェイス上の出力キューに配置します。 適応型セキュリティ アプランスがトラフィックの負荷に対応できていない場合は、使用可能なブロックの数が 0 付近で停滞すす（このコマンドの出力の CNT カラムに示されます）。 CNT カラムが 0 になると、適応型セキティ 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。

通常の運用中は、ASA の空きメモリの変動はほとんどないか、あってもごくわずかです。 普通は、攻撃を受けて何十万もの接続が ASA を通過している場合でない限り、メモリ不足にはなりません。 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、メモリ割り当てエラー メッセージ（%ASA-3-211001）が syslog に記録されることもあります。 攻撃が原因でメモリ不足に陥っている場合は、Cisco Technical Assistance Center（TAC）に連絡してください。

例

```
Ciscoasa#
show memory
```

```
Free memory:       845044716 bytes (79%)

Used memory:       228697108 bytes (21%)

------------     ----------------

Total memory:     1073741824 bytes (100%)
```

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 で見られた変換の最大数を表します。

> **注:** 1 台のホストでは、さまざまな宛先への複数の接続を確立できますが、変換は 1 つしか確立できません。 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 が表示される場合があります。

例

```
Ciscoasa#
show xlate count
84 in use, 218 most used
```

```
Ciscoasa(config)#show xlate

3 in use, 3 most used

Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,

       o - outside, r - portmap, s - static

TCP PAT from inside:10.1.1.15/1026 to outside:192.150.49.1/1024 flags ri
```

```
idle 62:33:57 timeout 0:00:30
UDP PAT from 10.1.1.15/1028 to outside:192.150.49.1/1024 flags ri
idle 62:33:57 timeout 0:00:30
ICMP PAT from inside:10.1.1.15/21505 to outside:192.150.49.1/0 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（192.150.49.1, 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、Inside ネットワークのホスト ポート（10.1.1.15, 1028）から Outside ネットワークのホスト ポート（192.150.49.1, 1024）への UDP 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 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（192.150.49.1, 0）への ICMP 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 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。

接続カウントが極端に多い場合は（通常は 50 ~ 100 回）、攻撃を受けていることを示している可能性があります。 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、『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』を参照してください。

例

```
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

```
Ciscoasa#show interface
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
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, 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)
```

また、インターフェイスでエラーが発生していないかどうかをチェックしてください。 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。 ケーブル不良の可能性もあります。 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れば、コリジョン、レイト コリジョン、または遅延パケットがまったく発生しないことに留意してください。 逆に、インターフェイスが半二重に設定されていれば、コリジョンやいくつかのレイト コリジョンがあり、遅延パケットも多少発生しています。 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、入力および出力のパケット カウンタの合計数の 10 % を超えないことが望まれます。 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うち 10 % を ASA がドロップしていることを意味します。 これらのパケットはそれぞれ再送信が必要になります。

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 回発行します。 このとき、1 回目を実行してから 2 回目を実行するまでの間、1 分ほど待ちます。 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:** 個々の ASA プロセスの検査は、このドキュメントの適用範囲外です。ここでは全体を簡単に説明しました。 ASA プロセスの詳細については、『ASA の show processes コマンド』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。 この出力は稼働平均であることに注意してください。 稼働平均で隠されていても、ASA では 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 ギガビット イーサネット カードの場合は 16384 バイト ブロック) で、**show blocks** の出力の現在の CNT カラムが 0 に近い場合は、ASA が著しいビジー状態のためにイーサネット パケットをドロップしている可能性が最も高いと考えられます。 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** コマンドまたは **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 シリーズ適応型セキュリティ アプライアンス
- テクニカルサポート - Cisco Systems