CHAPTER 11

DDoS 攻撃の識別と防御

概要

この章では、Distributed-DoS（DDoS; 分散型 DoS）攻撃を識別して防御するための SCE プラットフォームの機能について説明し、攻撃フィルタ モジュールの設定手順およびモニタリング手順を示します。

攻撃のフィルタリングと検出

攻撃フィルタリング

SCE プラットフォームには、DDoS 攻撃を検出し、これらの攻撃から防御するための高度な機能が備わっています。

攻撃フィルタリングは、特定 IP 攻撃ディテクタを使用して実行されます。特定 IP 攻撃ディテクタは、IP アドレス（または IP アドレスのペア）、プロトコル（TCP、UDP、ICMP、その他）、宛先ポート（TCP、UDP）、インターフェイス、および方向のそれぞれの組み合わせについて、SCE プラットフォームで、フローのレート（オープンされているものの合計と一時停止されているものの合計）を追跡します。レートがユーザ設定基準を満たすと、攻撃として認識され、設定済みのアクションを実行することができます（レポートする、ブロックする、サブスクライバに通知する、SNMP トラップを送信するなど）。

このメカニズムはデフォルトでイネーブルにされ、各攻撃タイプに対して個々にディセーブルにしたりイネーブルにしたりすることができます。

攻撃タイプには次の 32 種類があります。

- **1**：宛先ポートに関係なく、サブスクライバ側の特定の IP アドレスからの TCP フロー
- **2**：宛先ポートに関係なく、サブスクライバ側の特定の IP アドレスへの TCP フロー
- **3 ～ 4**：1 、2 と同じだが、方向が逆（サブスクライバのネットワーク）
- **5**：サブスクライバ側の特定の IP アドレスからネットワーク側の特定の IP アドレスへの TCP フロー
- **6**：5 と同じだが、方向が逆（ネットワーク側からサブスクライバ側へ）
- **7 ～ 12**：1 ～ 6 と同じだが、攻撃のすべてのフローに対して共通の特定の宛先ポート（1 ～ 6 はポートレスの攻撃タイプで、7 ～ 12 はポートベースの攻撃タイプ）
- **13 ～ 24**：1 ～ 12 と同じだが、TCP ではなく UDP
- **25 ～ 28**：1 ～ 4 と同じだが、TCP ではなく ICMP
- **29 ～ 32**：1 ～ 4 と同じだが、TCP ではなく他のプロトコル

特定の攻撃フィルタリング

特定の攻撃タイプに対する特定の IP 攻撃フィルタがイネーブルにされている場合、登録済みのエンティティごとに次の 2 つのレートが測定されます。

- 新規フローのレート
- 疑わしいフローのレート（疑わしいフローとは、一般的に、SCOS によって適切な確立（TCP の場合）が認められないか、または 1 つのパケットのみ（他のすべてのプロトコルの場合）が認められるフロー）

各 IP アドレスに対して個別に（シングル サイド）、また、IP アドレス ペア（該当するフローの送信元と宛先）に対しても、別のレート測定機能が維持されるので、特定の IP がある特定の IP を攻撃しているとき、IP アドレスのこのペアにより、1 つの障害（デュアル サイド）が定義されます。

次のいずれかの条件が存在する場合、これらの 2 つのメトリックに基づいて、特定 IP 攻撃が宣言されます。

- 新規フロー レートが特定のしきい値を超えた場合
- 疑わしいフローのレートが設定されているしきい値を超え、新しい総フローのレートに対する疑わしいフローのレートの割合が、設定されているしきい値を超えた場合

レートがこの基準を満たさなくなり、攻撃の終了が宣言された場合

特定の攻撃フィルタリングは、次の 2 つの手順で設定されることに注意してください。

- 特定の攻撃タイプに対する IP フィルタリングをイネーブルにします。
- 該当する攻撃タイプに対する攻撃ディテクタを設定します。各攻撃ディテクタでは、攻撃と、攻撃が検出された場合に実行されるアクションのしきい値が指定されます。

  特定の攻撃ディテクタに加え、ユーザ定義のしきい値およびアクションを使用して設定できるデフォルト ディテクタが存在するか、またはシステム デフォルトが残っています。

さらに、ユーザは、特定の状況での攻撃フィルタリングを実行または停止するために、設定済みの攻撃ディテクタを上書きできます。

選択された攻撃タイプに対する特定の IP フィルタリングは、次のパラメータでイネーブルにできます。これらのパラメータでは、次のケースに対して 32 のどの攻撃タイプがフィルタ処理されるかが制御されます。

- **プロトコル**：TCP、UDP、ICMP、その他。
- **攻撃の方向**：次の 1 つか 2 つの IP アドレスによってのみ、攻撃の方向を識別できます。
  - **シングル サイド**：攻撃は、送信元の IP アドレスまたは宛先アドレスのいずれかによってのみ、識別されます。

  フィルタ定義では、特定のサイドを指定することができます。または、両サイドのうちのどちらのサイドであるかに関係なく、いずれかのシングル サイドの攻撃を含めることができます。
  - **デュアル サイド**（TCP プロトコルおよび UDP プロトコルのみ）：攻撃は、送信元と宛先の両方の IP アドレスで識別されます。つまり、特定の IP が特定の IP を攻撃した場合、これは、2 つの別々の障害としてではなく、1 つの障害として検出されます。
- **宛先ポート**（TCP プロトコルおよび UDP プロトコルのみ）：ポートベースまたはポートレスの検出に対して特定の IP 検出をイネーブルにするかディセーブルにするかを定義します。1 つまたは複数の固定の宛先ポートが含まれる TCP 攻撃または UDP 攻撃に対するポートベースの検出をイネーブルにします。

  ポートベースの検出に対する宛先ポートのリストは、別に設定されます （「特定の攻撃ディテクタ」（P.11-13）を参照）。

攻撃の検出

特定の IP の検出は、次のパラメータで識別されます。

- 特定の IP アドレス（またはデュアル サイド検出の場合は 2 つの IP アドレス）
- プロトコル：TCP、UDP、ICMP、その他
- ポート：1 つの固定宛先ポートが含まれる TCP 攻撃または UDP 攻撃
- サイド：攻撃パケットの送信元インターフェイス（サブスクライバまたはネットワーク）
- 攻撃の方向：1 つの IP アドレスが指定された場合、IP アドレスは、攻撃元または攻撃先の IP アドレス

最大で 1000 の独立した攻撃を、同時に識別できます。

攻撃を識別したあと、次のいずれかのアクションを実行するようにシステムを設定できます。

- **レポート**：デフォルトでは、攻撃の開始と終了が常にレポートされます。
- **ブロック**：攻撃期間中は、すべての攻撃トラフィックがブロックされます（IP アドレスが攻撃元か攻撃先かにより、トラフィックが、攻撃 IP アドレスから、または、攻撃 IP アドレスへのものになります）。

- **通知**：サブスクライバ通知。識別された IP アドレスが、特定のサブスクライバのコンテキストに対応する場合、そのサブスクライバに対し、攻撃されていること（または、そのサブスクライバのネットワーク上のコンピュータが攻撃を生成していること）を、HTTP リダイレクトで通知するようにシステムを設定できます。
- **アラーム**：それぞれの攻撃が「開始」および「停止」されるたびに、SNMP トラップが生成されます。

攻撃の検出と処理について、ユーザが設定できます。この章では、攻撃の検出を設定してモニタリングする方法について説明します。

攻撃検出のしきい値

攻撃の定義に使用される　3 つのしきい値があります。これらのしきい値は、各 IP アドレスまたはアドレスのペア、プロトコル、インターフェイス、攻撃の方向について、SCE プラットフォームによって維持される測定機能に基づいています。

- **オープン フロー レート**：トラフィックが認められたフロー。新規フローが認められたすべてのパケットは、このフローがオープン フローであることを宣言するのに十分です。

  レートは、新規フローで 1 秒あたりで測定されます。
- **疑わしいフローのレート**：疑わしいフローとは、オープンされたが、確立フローになっていないフローです。

  レートは、新規フローで 1 秒あたりで測定されます。
- **疑わしいフローのレート**：オープン フローのレートに対する疑わしいフローのレートの割合。

前述の説明のとおり、次のいずれかの条件が存在する場合、特定 IP 攻撃が宣言されます。

- オープン フロー レートがしきい値を超えた場合。
- 疑わしいフローのレートがしきい値を超え、疑わしいフローのレートがしきい値を超えた場合。

各攻撃タイプの値には、別に設定されたデフォルト値があります。

該当するプロトコルでは、一般的に、疑わしいフロー レートのしきい値は、ポートベースの検出について、ポートレス検出より小さく設定する必要があります。これは、該当する IP アドレスと共通の宛先ポートでのフローは、次のとおり 2 回測定されるからです。

- 自システムによって：ポートベース攻撃を検出する場合
- 同じ IP アドレスと異なる宛先ポートのフローとともに：ポートレス攻撃を検出する場合

ポートベース攻撃が発生した場合で、フローのレートが両方のしきい値（ポートベースのしきい値とポートレスのしきい値）より大きい場合、ポートレス攻撃の前にポートベース攻撃を検出することが必要です。同様に、このしきい値は、双方向 IP 検出のためと、単方向 IP 検出のために小さくする必要があります。

これらのしきい値について、あらかじめ設定されているデフォルトを上書きする値をユーザ側で定義できます。また、（アクセス リストおよびポート リストを使用して）IP アドレス別とポート別に固有のしきい値を設定することも可能です。このようにして、ネットワーク エンティティのタイプ（サーバファーム、DNS サーバ、または大企業カスタマー）別に異なった検出基準を設定できます。

攻撃の処理

攻撃の処理は、次のように設定できます。

- **アクションの設定：**

- レポート：攻撃パケットを通常どおり処理し、攻撃が発生したことをレポートします。
- ブロック：攻撃パケットは SCE プラットフォームにより廃棄されるため、攻撃先にパケットが到達することはありません。

どのアクションを設定するかにかかわらず、すべての攻撃で 2 つのレポートが生成されます。1 つはいつ攻撃の開始が検出されたかで、もう 1 つはいつ攻撃の終了が検出されたかです。

- **サブスクライバ通知の設定（通知）：**
  - イネーブル：サブスクライバの IP アドレスが攻撃された、または攻撃されていることが検出されると、そのサブスクライバに通知します。
  - ディセーブル：サブスクライバには攻撃を通知しません。
- **SNMP トラップ送信の設定（アラーム）：**
  - アラーム：攻撃の開始時と終了時に SNMP トラップが送信されます。

    SNMP トラップには、次の情報フィールドが含まれます。

    特定の IP アドレス、または、

    プロトコル（TCP、UDP、ICMP、その他）。

    検出された IP アドレスが存在する**インターフェイス**（ユーザまたはネットワーク）。以降、攻撃「サイド」と呼びます。

    攻撃の方向（IP アドレスが攻撃元または攻撃先のどちらであるか）。

    違反したしきい値のタイプ（open- flows / ddos- suspected- flows、「attack- start」トラップのみ）。

    違反したしきい値の値（「attack- start」トラップのみ）。

    実行したアクション（report、block）：検出後に SCE プラットフォームがどのようなアクションを行ったかを表します。

    ブロックまたはレポートされた攻撃フローの数：攻撃中に検出されたフローの総数を表します（「attack- stop」トラップのみ）。
  - ディセーブル：SNMP トラップは送信されません。

サブスクライバ通知

攻撃が識別された場合、IP アドレスがサブスクライバ側で検出され、サブスクライバにマッピングされていると、攻撃に関する情報がアプリケーションに通知されます。これにより、アプリケーションはこのサブスクライバの HTTP 要求を、攻撃を通知するサーバにリダイレクトして、攻撃についてサブスクライバにオンラインで通知できます。

また、TCP トラフィックをブロックする場合は、指定されたポートをブロックしないようにシステムを設定して、このリダイレクションを有効にできます。このポートは、ブロック禁止と見なされます。

サブスクライバ通知が正常に動作するのは、SCE プラットフォームに現在ロードされている Service Control アプリケーションによってサポートされていて、なおかつ、この機能をアクティブ化するようにアプリケーションが設定されている場合に限られます。使用中のアプリケーションが攻撃のサブスクライバ通知をサポートしているかどうかを確認する方法、およびアプリケーションで攻撃のサブスクライバ通知をイネーブルにする方法については、該当する Service Control アプリケーションのマニュアルを参照してください。

ハードウェア フィルタリング

SCE プラットフォームには、ソフトウェアによるものとハードウェアによるものの、2 つの攻撃処理方法があります。攻撃は、通常、ソフトウェアによって処理されます。これにより、SCE プラットフォームでは、攻撃フローを正確に測定し、攻撃の終了をただちに検出することができます。

ただし、非常に強い攻撃は、ソフトウェアによって正常に処理することはできません。ソフトウェアによって攻撃が適切に処理できなかった場合、その結果発生する CPU での高い負荷のため、SCE プラットフォームによって提供されるサービスに悪影響が及ぼされます（通常のトラフィック分類および制御）。したがって、ソフトウェアに障害を発生させる脅威となるソフトウェアは、ハードウェアによって自動的にフィルタ処理されます。

攻撃のフィルタ処理にハードウェアが使用される場合、ソフトウェアでは、攻撃パケットについて把握しておらず、したがって次のような副次的な影響が発生します。

- 攻撃フロー数が、ソフトウェアによって非常に小さく見積もられます。これは、CLI（show interface linecard attack-filter current-attacks）によってレポートされる攻撃中のフローの総数が、実際の数より非常に小さくなります。
- 同様に、レポートされる攻撃フロー レート（これも CLI によってレポートされる）も、実際のレートより非常に小さくなります。0 というレートは、通常、ソフトウェアによって測定されます。
- 攻撃終了の検出には、非常に大きな遅延が発生します。攻撃終了の検出は、2 つの上限によって制限されます。
  - 1 つ目の上限は、次のように、設定されているアクションに依存します。
  - レポート：8 分の遅延。
  - ブロック：64 分の遅延。
  - 遅延の 2 つ目の上限は、攻撃の実際の時間の長さよりも 1 分長い値です（たとえば、3 分間続いていた攻撃の終了の検出の遅延の最大は、4 分間）。
- 次に、これらの 2 つの上限に関連するやり取りの例を示します。
  - 2 分間続いている攻撃については、設定されているアクションに関係なく、終了の検出の最大遅延は 3 分間
  - 設定されたアクションが「レポート」である、2 時間続いている攻撃については、終了の検出の最大遅延は 8 分間
  - 設定されたアクションが「ブロック」である、2 時間続いている攻撃については、終了の検出の最大遅延は 64 分間

ハードウェア攻撃フィルタリングは自動プロセスで、ユーザは設定できません。ただし、攻撃レポート機能でのハードウェア攻撃フィルタリングの影響のため、ハードウェア処理がいつアクティブであるかを認識し、ハードウェア フィルタリングのモニタリングが重要であることを認識することが重要です。これを行うには、次の 2 つの方法があります（「攻撃フィルタリングのモニタリング」（P.11-20）を参照）。

- **show interface linecard attack-filter current-attacks** コマンドの「*HW-filter*」フィールドをチェックします。
- 攻撃ログ ファイルの「*HW-filter*」フィールドをチェックします。

攻撃ディテクタの設定

シスコの攻撃検出メカニズムは、攻撃ディテクタと呼ばれる特殊なエンティティの定義および設定によって制御されます。

「デフォルト」と呼ばれる攻撃ディテクタが 1 つあり、これは常にイネーブルです。そのほかに、デフォルトでディセーブルに設定されている 99 の攻撃ディテクタ（1 ～ 99 の番号付き）があります。各ディテクタ（デフォルトおよびディテクタ 1 ～ 99）は、可能性がある 32 のあらゆる攻撃について、それぞれ異なるアクションおよびしきい値を使用して設定できます。

ディテクタ 1 ～ 99 がディセーブルの場合、デフォルトの攻撃ディテクタの設定により、攻撃の検出に使用されるしきい値と、攻撃が検出された際に SCE プラットフォームが実行するアクションが決まります。攻撃タイプごとに、異なるしきい値およびアクションのセットを指定できます。また、サブスクライバ通知および SNMP トラップ（アラーム）についても、同じ粒度でイネーブルまたはディセーブルに設定できます。

デフォルトの攻撃ディテクタは、SCE プラットフォームを通過する大部分のトラフィックに対する、SCE プラットフォームの望ましい動作を反映した値に設定する必要があります。ただし、SCE プラットフォームを通過するすべてのトラフィックに同じ値のセットを使用することはできません。一部のネットワーク エンティティは、他のネットワーク要素から送信されるとき、通常のトラフィックであっても、その特性によって攻撃と見なされる場合があるからです。次に、一般的な例を 2 つ示します。

- DNS サーバは、多くの短い DNS クエリーの送信先になります。これらのクエリーは一般に UDP フローであり、各フローが 2 つのパケット（要求および応答）で構成されています。これらのフローはパケット数が 3 未満のため、SCE プラットフォームは、通常、DNS サーバに対してオープンされたすべての UDP フローを DDoS の疑いのあるフローと見なします。DNS サーバはピーク時には 1 秒ごとに何百もの DNS 要求を処理することがあるため、protocol = UDP および direction = attack-destination については、DDoS の疑いのあるフローのしきい値を適切に設定する必要があります。1 秒あたりのこのしきい値を 1000 にすると、DNS サーバに適していると考えられます。一方、他の大部分のネットワーク要素については、このような大量の UDP フローのレートの宛先になるのは、攻撃される可能性があるため、このしきい値は不適切です。したがって、すべてのトラフィックに 1000 というしきい値を設定するのは得策ではありません。
- SCE プラットフォームのサブスクライバ側には、それぞれ複数のコンピュータをインターネット経由で接続し、コンピュータごとに異なる IP アドレスを使用している一般家庭サブスクライバが数多く存在すると考えられます。さらに、NAT を使用して何百台ものコンピュータを 1 つの IP アドレスで代表させている企業サブスクライバもいくつか存在すると考えられます。企業サブスクライバの IP アドレスでは、一般家庭サブスクライバの IP アドレスよりも、明らかに多くのフローがトラフィックに含まれます。これら 2 つのケースに同じしきい値は適用できません。

このような特殊なケースを SCE プラットフォームが異なった方法で取り扱えるようにするため、非デフォルトの攻撃ディテクタ 1 ～ 99 を設定できます。非デフォルトの攻撃ディテクタでも、デフォルトの攻撃ディテクタと同様に、攻撃タイプごとに、異なるアクションおよびしきい値のセットを指定できます。ただし、非デフォルトの攻撃ディテクタに効力を持たせるには、このようなディテクタをイネーブルにして、Access Control List（ACL; アクセス制御リスト）を割り当てる必要があります。ACL によって許可された IP アドレスについてのみ、この種の攻撃ディテクタに設定されたアクションおよびしきい値が有効になります。非デフォルトの攻撃ディテクタには、その目的を記述したラベル（「DNS servers」、「Server farm」など）を付けることができます。

非デフォルトの攻撃ディテクタは、攻撃タイプに限って有効です。そのため、デフォルトの攻撃ディテクタの設定を、非デフォルトの攻撃ディテクタの設定に重複して組み込む必要がありません。次に、具体的な例を示します。SCE プラットフォームのサブスクライバ側に存在する、ある HTTP サーバに着信する要求が多いため、着信 TCP フロー レートのしきい値を大きな値に設定した非デフォルトの攻撃ディテクタを使用する必要があります。この目的で、攻撃ディテクタ 4 を使用すると仮定します。この攻撃ディテクタをイネーブルにし、この HTTP サーバの IP アドレスを許可する ACL を割り当てます。また、サブスクライバを UDP 攻撃から保護するために、デフォルトの攻撃ディテクタは、ネットワークから着信する UDP 攻撃をブロックするように設定されていると仮定します（デフォルトの設定では、攻撃をレポートするだけでブロックしません）。HTTP サーバがネットワークからの UDP 攻撃を受けた場合には、デフォルトの攻撃ディテクタの設定が、この HTTP サーバについても有効になります。攻撃ディテクタ 4 は、UDP 攻撃には対応していないからです。

非デフォルトの攻撃ディテクタと、32 の攻撃タイプのそれぞれについて、4 つの設定可能な設定があります。

- しきい値
- アクション
- サブスクライバ通知
- アラーム

これらの 4 つの各設定は、（値または値のセットで）設定されている場合と、設定されていない場合があります。デフォルトの状態は、これらのすべてが設定されていません。

攻撃タイプごとにイネーブルに設定した攻撃ディテクタの集合と、デフォルトの攻撃ディテクタは、1 つのデータベースを形成します。このデータベースによって、攻撃を検出するしきい値および実行するアクションが決まります。プラットフォームが潜在的な攻撃を検出すると、次のアルゴリズムを使用して、攻撃検出のしきい値を判断します。

- イネーブルに設定された攻撃ディテクタを、番号の小さい順にスキャンします。
- 攻撃ディテクタに指定された ACL によって IP アドレスが許可され、なおかつ、該当する攻撃タイプに対してしきい値が設定されている場合、その攻撃ディテクタで指定されるしきい値を使用します。そうでない場合、次の攻撃ディテクタをスキャンします。
- IP アドレスとプロトコルの組み合わせに一致する攻撃ディテクタがない場合、デフォルトの攻撃ディテクタを使用します。

残りの設定であるアクション、サブスクライバ通知、アラームに対して使用する値を決定する際には、同じロジックが適用されます。使用する値は、攻撃タイプについて特定の設定がある、イネーブルで番号が最も小さい攻撃ディテクタで指定されているアクションです。このような攻撃ディテクタが存在しない場合には、デフォルトの攻撃ディテクタの設定が使用されます。

攻撃ディテクタを設定してイネーブルにするには、ここで説明するコマンドを使用します。

- [no] attack-filter protocol *protocol* attack-direction *direction*
- attack-detector (default| *number*) protocol *protocol* attack-direction *direction* side *side* action *action* [open-flows *number* suspected-flows-rate *number* suspected-flows-ratio *number*]
- attack-detector (default| *number*) protocol *protocol* attack-direction *direction* side *side* (notify-subscriber|don't-notify-subscriber)
- attack-detector (default| *number*) protocol *protocol* attack-direction *direction* side *side* (alarm|no-alarm)
- default attack-detector (default| *number*) protocol *protocol* attack-direction *direction* side *side*
- default attack-detector default
- default attack-detector *number*
- default attack-detector (all-numbered|all)

- attack-detector *number* access-list comment
- attack-detector *number* (TCP-dest-ports|UDP-dest-ports) (all|(*port1 [port2 …]*))
- [no] attack-filter subscriber-notification ports *port1*

特定 IP 検出をイネーブルにするには

特定 IP 検出は、デフォルトでは、すべての攻撃タイプについてディセーブルです。ユーザは、次のオプションによって、特定の、定義済みの状況のみについて、特定 IP 検出をイネーブルまたはディセーブルに設定できます。

- 選択されたプロトコルのみ。
- TCP プロトコルおよび UDP プロトコルについては、ポートベース検出のみ、または、ポートレス検出のみ。
- 選択された攻撃の方向については、すべてのプロトコルに対して、または、選択されたプロトコルに対して。

オプション

次のオプションを使用できます。

- **protocol**：特定 IP 検出がイネーブルまたはディセーブルにされる特定のプロトコル。
  - デフォルト：すべてのプロトコル（プロトコルの指定なし）
- **attack direction**：シングル サイドまたはデュアル サイドの攻撃に対して特定 IP 検出をイネーブルまたはディセーブルにするかどうかを定義します。
  - デフォルト：すべての方向
- **宛先ポート**（TCP プロトコルおよび UDP プロトコルのみ）：ポートベースまたはポートレスの検出に対して特定の IP 検出をイネーブルにするかディセーブルにするかを定義します。
  - デフォルト：ポートベースおよびポートレスの両方
- 設定済みの特定 IP 検出をディセーブルにするには、このコマンドの **no** 形式を使用します。

特定 IP 検出をイネーブルにするには

ステップ 1　SCE(config if)# プロンプトで、**attack-filter [protocol (((TCP|UDP) [dest-port (specific|not-specific|both)])|ICMP|other)] [attack-direction (single-side-source|single-side-destination|single-side-both|dual-sided|all)]** と入力し、**Enter** キーを押します。

TCP プロトコルのみの場合にすべての攻撃方向で特定 IP 検出をイネーブルにするには

ステップ 1　SCE(config if)# プロンプトで、**attack-filter protocol TCP** と入力し、**Enter** キーを押します。

TCP プロトコルのポートベース検出のみの場合にデュアル サイド攻撃で特定 IP 検出をイネーブルにするには

ステップ 1　SCE(config if)# プロンプトで、**attack-filter protocol TCP dest-port specific attack-direction dual-sided** と入力し、**Enter** キーを押します。

TCP、UDP、ICMP 以外のプロトコルの場合にすべての攻撃方向で特定 IP 検出をディセーブルにするには

ステップ 1　SCE(config if)# プロンプトで、**no attack-filter protocol other** と入力し、**Enter** キーを押します。

ICMP の場合に送信元 IP によって定義されたシングル サイド攻撃で特定 IP 検出をディセーブルにするには

ステップ 1　SCE(config if)# プロンプトで、**no attack-filter protocol ICMP attack-direction single-side-source** と入力し、**Enter** キーを押します。

デフォルトの攻撃ディテクタを設定するには

デフォルトの攻撃ディテクタの値を設定するには、これらのコマンドで次のパラメータを使用します。

- 攻撃処理アクション
- しきい値
- サブスクライバ通知
- SNMP トラップの送信

特定の攻撃タイプについて固有の攻撃ディテクタを定義すると、その攻撃ディテクタによってデフォルト 攻撃ディテクタが上書きされます。

オプション

次のオプションを使用できます。

- **attack-detector**：設定中の攻撃ディテクタ。この場合は、デフォルトの攻撃ディテクタです。
- **protocol**：デフォルトの攻撃ディテクタが適用されるプロトコルを定義します。
- **attack-direction**：デフォルトの攻撃ディテクタを、シングル サイド攻撃に適用するかデュアル サイド攻撃に適用するかを定義します。
- **destination port**（TCP プロトコルおよび UDP プロトコルのみ）：デフォルトの攻撃ディテクタを、ポートベース検出に適用するかポートレス検出に適用するかを定義します。
- **side**：デフォルトの攻撃ディテクタを、サブスクライバ側からの攻撃に適用するかネットワーク側からの攻撃に適用するかを定義します。
- **action**：デフォルト アクション
  - **report**（デフォルト）：攻撃ログに書き込むことによって、攻撃の開始と終了をレポートします。
  - **block**：この攻撃の一部である今後のすべてのフローをブロックし、SCE プラットフォームがパケットを廃棄します。
- **Thresholds**：
  - **open-flows-rate**：オープン フローのレートに対するデフォルトのしきい値。
    suspected-flows-rate：疑わしい DDoS フローのレートに対するデフォルトのしきい値。
  - **suspected-flows-ratio**：オープン フローのレートに対する疑わしいフローのレートの割合のデフォルトのしきい値。
- デフォルトでサブスクライバ通知をイネーブルまたはディセーブルにするには、適切なキーワードを使用します。
  - **notify-subscriber**：サブスクライバ通知をイネーブルにします。
  - **don't-notify-subscriber**：サブスクライバ通知をディセーブルにします。
- デフォルトで SNMP トラップの送信をイネーブルまたはディセーブルにするには、適切なキーワードを使用します。
  - **alarm**：SNMP トラップの送信をイネーブルにします。
  - **no-alarm**：SNMP トラップの送信をディセーブルにします。

デフォルト アクションおよび（任意で）デフォルトしきい値を定義するには

デフォルト

デフォルトの攻撃ディテクタに対するデフォルト値は、次のとおりです。

- アクション：レポート

- しきい値：攻撃タイプにより多様
- サブスクライバ通知：ディセーブル
- SNMP トラップの送信：ディセーブル

ステップ 1　SCE(config if)# プロンプトで、**attack-detector default protocol (((TCP|UDP) [dest-port (specific|not- specific|both)]) |ICMP|other|all) attack-direction (single-side-source|single-side-destination|single-side-both|dual-sided|all) side (subscriber|network|both) [action (report|block)] [open-flows-rate** *number* **suspected-flows-rate** *rate* **suspected-flows-ratio** *ratio***]** と入力し、**Enter** キーを押します。

定義済みの攻撃タイプに対して、デフォルト 攻撃ディテクタを設定します。

ステップ 2　SCE(config if)# プロンプトで、**attack-detector default protocol (((TCP|UDP) [dest-port (specific|not- specific|both)])|ICMP|other|all) attack-direction (single-side-source|single-side-destination|single-side-both|dual-sided|all) side (subscriber|network|both) (notify-subscriber|don't-notify-subscriber)** と入力し、**Enter** キーを押します。

定義済みの攻撃タイプに対して、デフォルトで、サブスクライバ通知をイネーブルまたはディセーブルにします。

攻撃タイプは、ステップ 1 と同様に定義する必要があります。

ステップ 3　SCE(config if)# プロンプトで、**attack-detector default protocol (((TCP|UDP) [dest-port (specific|not- specific|both)]) |ICMP|other|all) attack-direction (single-side-source|single-side-destination|single-side-both|dual-sided|all) side (subscriber|network|both) (alarm|no-alarm)** と入力し、**Enter** キーを押します。

定義済みの攻撃タイプに対して、デフォルトで、SNMP トラップ送信をイネーブルまたはディセーブルにします。

攻撃タイプは、ステップ 1 と同様に定義する必要があります。

攻撃タイプの選択済みのセットでシステム デフォルトに戻すには

ユーザが定義したアクション、しきい値、サブスクライバ通知のデフォルト値を削除し、攻撃タイプの選択済みのセットに対する SNMP トラップの送信を取り消し、システムのデフォルト設定に戻すには、ここで説明するコマンドを使用します。

ステップ 1　SCE(config if)# プロンプトで、**default attack-detector default protocol (((TCP|UDP) [dest-port (specific|not- specific|both)])|ICMP|other|all) attack-direction (single-side-source|single-side-destination|single-side-both|dual-sided|all) side (subscriber|network|both)** と入力し、**Enter** キーを押します。

定義済みの攻撃タイプについて、システム デフォルトに戻します。

すべての攻撃タイプでシステム デフォルトを元に戻すには

ステップ 1　SCE(config if)# プロンプトで、**default attack-detector default** と入力し、**Enter** キーを押します。

定義済みの攻撃タイプについて、システム デフォルトに戻します。

特定の攻撃ディテクタ

攻撃タイプの選択済みのセットに対応する特定の攻撃ディテクタで、しきい値、アクション、およびサブスクライバ通知の設定を定義するには、ここで説明するコマンドを使用します。

オプション

プロトコル、攻撃方向、サイドの組み合わせごとに、特定の攻撃ディテクタを設定できます。SCE プラットフォームは、最大 100 の攻撃ディテクタをサポートします。各攻撃ディテクタは、1 ～ 100 の番号で識別されます。各ディテクタを、ディセーブル（デフォルト）またはイネーブルに設定できます。イネーブルの攻撃ディテクタには、次のパラメータを設定する必要があります。

- **access-list**：指定された攻撃ディテクタに関連付けられている Access Control List（ACL）の数。ACL により、このディテクタで選択される IP アドレスが識別されます （「ACL」を参照）。
  - 双方向 IP 検出では、ACL との一致に宛先 IP アドレスが使用されます。
  - この攻撃ディテクタによって許可されるすべての IP アドレスを示すには、「none」キーワードを使用します。

  このオプションは、コマンドを使用してポート リストを定義する場合に役に立ち、必要な設定は、すべての IP アドレスに対して設定する必要があります。
- **comment**：文書化の目的で使用します。

イネーブルにする攻撃ディテクタには、そのほかに次の設定値も含めることができます。

- **TCP-port-list/UDP-port-list**：指定されたプロトコルの宛先ポート リスト。TCP プロトコルと UDP プロトコルは、特定のポートのみに対して設定することができます。これは、プロトコルごとに指定された宛先ポートのリストです。

  異なる 15 までの TCP ポート数と、異なる 15 までの UDP ポート数を指定できます。

  同じプロトコル（TCP/UDP）でポートベース（特定の宛先ポートを検出するなど）の攻撃タイプにのみ影響が及ぼされる攻撃ディテクタについて、TCP/UDP ポート リストを設定します。他の攻撃タイプの設定は、設定されるポート リストの影響を受けません。

攻撃ディテクタごとに、各攻撃タイプに対して次の設定が可能です。各設定は、「not configured」状態（デフォルト）か、特定の値を設定できます。

- **action**：アクション
  - **report**（デフォルト）：攻撃ログに書き込むことによって、攻撃の開始と終了をレポートします。

  - **block**：この攻撃の一部である今後のすべてのフローをブロックし、SCE プラットフォームがパケットを廃棄します。
- **Thresholds**：
  - **open-flows-rate**：オープン フローのレートに対するデフォルトのしきい値。
    suspected-flows-rate：疑わしい DDoS フローのレートに対するデフォルトのしきい値。
  - **suspected-flows-ratio**：オープン フローのレートに対する疑わしいフローのレートの割合のデフォルトのしきい値。
- デフォルトでサブスクライバ通知をイネーブルまたはディセーブルにするには、適切なキーワードを使用します。
  - **notify-subscriber**：サブスクライバ通知をイネーブルにします。
  - **don't-notify-subscriber**：サブスクライバ通知をディセーブルにします。
- デフォルトで SNMP トラップの送信をイネーブルまたはディセーブルにするには、適切なキーワードを使用します。
  - **alarm**：SNMP トラップの送信をイネーブルにします。
  - **no-alarm**：SNMP トラップの送信をディセーブルにします。

特定の攻撃ディテクタをイネーブルにして ACL を割り当てるには

ステップ 1　SCE(config if)# プロンプトで、**attack-detector** *number* **access-list (***aclnumber* **|none) [comment** *comment***]** と入力し、**Enter** キーを押します。

攻撃ディテクタをイネーブルにして、それに特定の ACL を割り当てます。

特定の攻撃ディテクタのアクションおよび（任意で）しきい値を定義するには

ステップ 1　SCE(config if)# プロンプトで、**attack-detector** *number* **protocol (((TCP|UDP) [dest-port (specific|not- specific|both)])|ICMP|other|all) attack-direction (single-side-source|single-side-destination|single-side-both|dual-sided|all) side (subscriber|network|both) [action (report|block)] [open-flows-rate** *number* **suspected-flows-rate** *rate* **suspected-flows-ratio** *ratio*」と入力し、**Enter** キーを押します。

指定された攻撃ディテクタのアクションを定義します。

特定の攻撃ディテクタにサブスクライバ通知を定義するには

特定の攻撃ディテクタおよび攻撃タイプの選択済みのセットについて、サブスクライバ通知を設定するには、ここで説明するコマンドを使用します。

ステップ 1　SCE(config if)# プロンプトで、**attack-detector** *number* **protocol (((TCP|UDP) [dest-port (specific|not- specific|both)])|ICMP|other|all) attack-direction (single-side-source|single-side-destination|single-side-both|dual-sided|all) side (subscriber|network|both) (notify-subscriber|don't-notify-subscriber)** と入力し、**Enter** キーを押します。

特定の攻撃ディテクタにサブスクライバ通知を定義します。

特定の攻撃ディテクタに SNMP トラップ設定を定義するには

攻撃タイプの選択済みのセットに対応する特定の攻撃ディテクタで、SNMP トラップの送信をイネーブルまたはディセーブルにするには、ここで説明するコマンドを使用します。

ステップ 1　SCE(config if)# プロンプトで、**attack-detector** *number* **protocol (((TCP|UDP) [dest-port (specific|not- specific|both)])|ICMP|other|all) attack-direction (single-side-source|single-side-destination|single-side-both|dual-sided|all) side (subscriber|network|both) (alarm|no-alarm)** と入力し、**Enter** キーを押します。

特定の攻撃ディテクタに SNMP トラップ設定を定義します。

特定の攻撃ディテクタで TCP プロトコルまたは UDP プロトコルの宛先ポートを定義するには

特定の攻撃ディテクタについて、TCP プロトコルまたは UDP プロトコルの宛先ポートのリストを定義するには、ここで説明するコマンドを使用します。

ステップ 1　SCE(config if)# プロンプトで、**attack-detector** *number* **TCP-port-list**|**UDP-port-list (all**|(*port1* [*port2, port3...*]) と入力し、**Enter** キーを押します。

特定のプロトコルと攻撃ディテクタにポートを定義します。

ユーザ定義の値を削除するには

攻撃タイプの選択済みのセットに対応する特定の攻撃ディテクタで、アクション、しきい値、サブスクライバ通知を削除し、SNMP トラップの送信を取り消すには、ここで説明するコマンドを使用します。

該当する攻撃タイプでこれらの設定を削除すると、デフォルトの「not configured」状態に戻されます。これは、この攻撃タイプの攻撃に対する応答の決定に、攻撃ディテクタが参加しないことを意味します。

ステップ 1　SCE(config if)# プロンプトで、**default attack-detector** *number* **protocol (((TCP|UDP) [dest-port (specific|not- specific|both)])|ICMP|other|all) attack-direction (single-side-source|single-side-destination|single-side-both|dual-sided|all) side (subscriber|network|both)** と入力し、**Enter** キーを押します。

指定された攻撃ディテクタのアクションを定義します。

特定の攻撃ディテクタをディセーブルにするには

特定の攻撃ディテクタをディセーブルにし、すべてのプロトコル、攻撃方向およびサイドで、デフォルトのアクション、しきい値、サブスクライバ通知の設定を削除するには、ここで説明するコマンドを使用します。

ステップ 1　SCE(config if)# プロンプトで、**default attack-detector** *number* と入力し、**Enter** キーを押します。

指定された攻撃ディテクタをディセーブルにします。

非デフォルトのすべての攻撃ディテクタをディセーブルにするには

非デフォルトのすべての攻撃ディテクタをディセーブルにし、デフォルト値を使用するよう設定するには、ここで説明するコマンドを使用します。

ステップ 1　SCE(config if)# プロンプトで、**default attack-detector all-numbered** と入力し、**Enter** キーを押します。

非デフォルトのすべての攻撃ディテクタをディセーブルにします。

すべての攻撃ディテクタをディセーブルにするには

すべての攻撃ディテクタをディセーブルにし、デフォルト値を使用するよう設定するには、ここで説明するコマンドを使用します。

ステップ 1　SCE(config if)# プロンプトで、**default attack-detector all** と入力し、**Enter** キーを押します。

すべての攻撃ディテクタをディセーブルにします。

攻撃ディテクタの設定例

次の設定では、ICMP 攻撃の検出に使用するデフォルトのユーザ しきい値を変更するとともに、2 つの DNS サーバ（10.1.1.10 および 10.1.1.13）が攻撃されているという誤認を防ぐために、UDP 攻撃に関するしきい値の大きい攻撃ディテクタを設定しています。

ステップ 1　SCE(config)# プロンプトで、**interface linecard 0** と入力し、**Enter** キーを押します。

ラインカード インターフェイス コンフィギュレーション モードを開始します。

ステップ 2　SCE(config if)# プロンプトで、**attack-detector default protocol** *ICMP* **attack-direction** *single-side-source* **action** *report* **open-flow-rate** *1000* **suspected-flows-rate** *100* **suspected-flows-ratio** *10* と入力し、**Enter** キーを押します。

デフォルトの ICMP しきい値およびアクションを設定します。

ステップ 3　SCE(config if)# プロンプトで、**attack-detector 1 access-list 3 UDP-ports-list** *53* **comment** *"DNS servers"* と入力し、**Enter** キーを押します。

攻撃ディテクタ #1 をイネーブルにし、それに ACL #3 を割り当て、UDP 宛先ポートのリストに 1 つのポート、ポート 53 を定義します。

ステップ 4　SCE(config if)# プロンプトで、**attack-detector 1 protocol UDP dest-port** *specific* **attack-direction** *single-side-destination* **action report open-flow-rate** *1000000* **suspected-flows-rate** *1000000* と入力し、**Enter** キーを押します。

攻撃ディテクタ #1 にしきい値およびアクションを定義します。

ステップ 5　SCE(config if)# プロンプトで、**attack-detector 1 protocol UDP dest-port specific attack-direction** *single-side-destination* **side** *subscriber* **notify-subscriber** と入力し、**Enter** キーを押します。

攻撃ディテクタ #1 で、サブスクライバ通知がイネーブルにされます。

ステップ 6　SCE(config if)# プロンプトで、**exit** と入力し、**Enter** キーを押します。

ラインカード インターフェイス コンフィギュレーション モードを終了します。

ステップ 7　攻撃ディテクタに割り当てられた ACL #3 を設定します。

```
SCE(config)# access-list 3 permit 10.1.1.10
SCE(config)# access-list 3 permit 10.1.1.13
```

サブスクライバ通知の設定

サブスクライバ通知は、サブスクライバにマッピングされた IP アドレスに関連する現在の攻撃について、サブスクライバにリアルタイムで通知する機能です。サブスクライバ通知は、前述の方法に従って、攻撃ディテクタ レベルで設定します。また、該当する Service Control アプリケーションのユーザガイドの説明に従って、SCE プラットフォームにロードしたアプリケーションでイネーブル化および設定されている必要があります。

現在のソリューションでは、SCE プラットフォームはサブスクライバから発信された HTTP フローをプロバイダーのサーバ（サブスクライバが攻撃を受けていることを通知する）にリダイレクトすることで、サブスクライバに攻撃を通知します。これにより、block アクションを設定した、サブスクライバから発信された TCP 攻撃についての問題が生じます。通常このような攻撃は、HTTP リダイレクションを使用してサブスクライバに通知することはできません。サブスクライバから発信される HTTP フローはすべて TCP フローであるため、これらは他の攻撃フローとともにブロックされるからです。HTTP リダイレクトを効率的に使用するために、上記のような状況が発生しても、サブスクライバから特定の TCP ポートに発信される TCP フローがブロックされないようにする CLI コマンドがあります。

サブスクライバ通知ポートを設定するには

サブスクライバ通知ポートとして使用するポートを定義できます。SCE プラットフォームのサブスクライバ側からこのポートへの TCP トラフィックは攻撃フィルタによってブロックされないため、このポートは常にサブスクライバ通知のために使用できます。

オプション

次のオプションを使用できます。

- **portnumber**：サブスクライバ通知ポートとして使用するポートの番号

ステップ 1　SCE(config if)# プロンプトで、**attack-filter subscriber-notification ports** *portnumber* と入力し、**Enter** キーを押します。

サブスクライバ通知ポートを削除するには

ステップ 1　SCE(config if)# プロンプトで、**no attack-filter subscriber-notification ports** と入力し、**Enter** キーを押します。

攻撃の検出の停止と実行

攻撃ディテクタを設定すると、SCE プラットフォームは自動的に攻撃を検出し、設定に従って攻撃に対処します。ただし、デバッグを行うときや、SCE プラットフォームの攻撃ディテクタの設定変更が短時間でできる作業ではないときなど、手動で介入することが望ましい場合があります。次に例を示します。

- SCE プラットフォームが攻撃を検出したが、それが本当のアラームではないことがわかっている場合。この場合、ユーザが行うべき適切な措置は、（該当する IP 範囲全体で、または特定の IP アドレスかポートについて）しきい値を大きくすることです。しかし、この作業には時間がかかる場合があります。また、攻撃へのアクションが「block」と指定されている場合には、この特定の攻撃についてブロック アクションをとりあえず停止させ、設定変更はあとで、必要な変更を正しくプランニングする時間があるときに行うことが望まれます。

  このような場合には、後述する **dont-filter** コマンドを使用します。

- ISP で、あるサブスクライバがネットワーク側から UDP 攻撃を受けているという通知がありました。ISP は、このサブスクライバへのすべての UDP トラフィックをブロックすることで、サブスクライバをこの攻撃から保護したいと考えますが、不都合なことに SCE プラットフォームは攻撃を認識していません （あるいは、プラットフォームは攻撃を認識していますが、設定されているアクションが「block」ではなく「report」です）。

  このような場合には、後述する **force-filter** コマンドを使用します。

CLI の攻撃フィルタリング コマンドを使用すると、次の操作を実行できます。

- 特定の IP アドレスに関連する攻撃のフィルタリングを防止または停止するには、**dont-filter** コマンドを設定します。
- 特定の IP アドレスに関連する攻撃のフィルタリングを（特定のアクションで）実行するには、**force-filter** コマンドを設定します。

攻撃フィルタリングを実行または停止するには、ここで説明するコマンドを使用します。

- [no] attack-filter dont-filter
- [no] attack-filter force-filter

オプション

前述の攻撃ディテクタ オプションに加え、次のオプションを使用できます。

- **ip-address**：攻撃フィルタリングを停止する IP アドレス。

attack -direction がデュアル サイドの場合、送信元側（*source-ip-address*）および宛先側（*dest-ip-address*）の両方で、IP アドレスを設定する必要があります。

攻撃フィルタリングの停止

特定の IP アドレスおよび攻撃タイプについて攻撃フィルタリングを停止するには、**dont-filter** CLI コマンドを実行します。フィルタリングがすでに実行中であれば、その動作が停止されます。攻撃フィルタリングが停止している場合、別の CLI コマンド（**force-filter** または **no dont-filter**）で明示的に復元するまで、停止した状態を続けます。

- 「指定された状況で dont-filter を設定するには」（P.11-19）
- 「指定された状況から dont-filter を削除するには」（P.11-19）
- 「すべての dont-filter を削除するには」（P.11-19）

指定された状況で dont-filter を設定するには

ステップ 1　SCE(config if)# プロンプトで、**attack-filter dont-filter protocol (((TCP|UDP) [dest-port (port-number |not-specific))|ICMP|other) attack-direction (((single-side-source|single-side-destination|single-side-both) (ip** *ip-address* **)|(dual-sided source-ip** *source-ip-address* **destination-ip** *dest-ip-address* **)) side (subscriber|network|both)** と入力し、**Enter** キーを押します。

指定された状況から dont-filter を削除するには

ステップ 1　SCE(config if)# プロンプトで、**no attack-filter dont-filter protocol (((TCP|UDP) [dest-port (port-number |not-specific))|ICMP|other) attack-direction (((single-side-source|single-side-destination|single-side-both) (ip** *ip-address* **)|(dual-sided source-ip** *source-ip-address* **destination-ip** *dest-ip-address* **)) side (subscriber|network|both)** と入力し、**Enter** キーを押します。

すべての dont-filter を削除するには

ステップ 1　SCE(config if)# プロンプトで、**no attack-filter dont-filter all** と入力し、**Enter** キーを押します。

攻撃フィルタリングの強制実行

特定の IP アドレスおよびプロトコルについて、攻撃フィルタリングを強制的に実行できます。強制的な攻撃フィルタリングは、明示的な CLI コマンド（**no force-filter** または **dont-filter**）で取り消すまで続行されます。

- 「指定された状況で force-filter を設定するには」（P.11-20）
- 「指定された状況から force-filter を削除するには」（P.11-20）

- 「すべての force-filter を削除するには」（P.11-20）

指定された状況で force-filter を設定するには

ステップ 1　SCE(config if)# プロンプトで、**attack-filter force-filter action (block|report) protocol (((TCP|UDP) [dest-port (port-number |not-specific))|ICMP|other) attack-direction (((single-side-source|single-side-destination|single-side-both) (ip** *ip-address* **)|(dual-sided source-ip** *source-ip-address* **destination-ip** *dest-ip-address* **)) side (subscriber|network|both)[notify-subscriber]** と入力し、**Enter** キーを押します。

指定された状況から force-filter を削除するには

ステップ 1　SCE(config if)# プロンプトで、**no attack-filter force-filter protocol (((TCP|UDP) [dest-port (port-number |not-specific))|ICMP|other) attack-direction (((single-side-source|single-side-destination|single-side-both) (ip** *ip-address* **)|(dual-sided source-ip** *source-ip-address* **destination-ip** *dest-ip-address* **)) side (subscriber|network|both)** と入力し、**Enter** キーを押します。

すべての force-filter を削除するには

ステップ 1　SCE(config if)# プロンプトで、**no attack-filter force-filter all** と入力し、**Enter** キーを押します。

攻撃フィルタリングのモニタリング

- 「SNMP トラップを使用した攻撃フィルタリングのモニタリング」（P.11-20）
- 「CLI トラップを使用した攻撃フィルタリングのモニタリング」（P.11-22）
- 「攻撃のログ」（P.11-28）

攻撃フィルタリングと攻撃の検出をモニタリングする場合、次の 3 つのオプションがあります。

- CLI の show コマンド
- SNMP の攻撃検出トラップ
- 攻撃のログ

SNMP トラップを使用した攻撃フィルタリングのモニタリング

システムでは、次のように、特定の攻撃検出イベントの開始時トラップが送信され、また、特定の検出イベントの終了時にも、トラップが送信されます。

- STARTED_FILTERING トラップ：攻撃情報を含む文字列
- STOPPED_FILTERING

- 攻撃情報を含む文字列
- 停止理由を含む文字列

攻撃の開始時に送信される attack-information 文字列のフォーマットは、次のとおりです。

- トラフィックで攻撃が検出された場合

```
Attack detected: Attack 'IP-info>from 'side>side, protocol 'protocol>. 'rate1>open
flows per second detected, 'rate2' Ddos-suspected flows per second detected. Action
is: 'action'.
```

- 攻撃が、**force-filter** コマンドの結果として宣言された場合

```
Attack Filter: Forced 'forced-action' 'IP-info' from 'side' side, protocol 'protocol'.
Attack forced using a force-filter command.
```

攻撃の終了時に送信される attack-information 文字列の形式は、次のとおりです。

- トラフィックで攻撃が検出された場合

```
End-of-attack detected: Attack 'IP-info' from 'side' side, protocol 'protocol'. Action
is: 'action' Duration 'duration' seconds, 'total-flows' 'hw-filter'
```

- 攻撃が、**no force-filter** コマンドまたは新しい **don't-filter** コマンドの結果として宣言された場合

```
Attack Filter: Forced to end 'action2' 'IP-info' from 'side' side, protocol
'protocol'. Attack end forced using a 'no force-filter' or a 'don't-filter' command.
```

攻撃の開始時に送信される reason 文字列のフォーマットは、次のとおりです。

- トラフィックで攻撃の終了が検出された場合

```
Detected attack end
```

- 攻撃が、**no force-filter** コマンドまたは新しい **don't-filter** コマンドの結果として宣言された場合

```
Forced attack end
```

情報文字列の（' '）で示されたフィールドに表示される値には、次のものが含まれる可能性があります。

- 'action'
  - Report
  - Block
- 'forced-action' は、設定されている force-filter アクションにより、次の値の 1 つになります。
  - フローのブロック
  - レポート
- 'IP-info' は、攻撃の方向と、検出された IP アドレスが 1 つか 2 つかによって、次のフォーマットの 1 つになります。
  - 送信元 IP アドレス A.B.C.D
  - 発信先 IP アドレス A.B.C.D
  - 送信元 IP アドレス A.B.C.D から発信先 IP アドレス A.B.C.D
- 'side'
  - サブスクライバ
  - ネットワーク

- 'protocol'
  - TCP
  - UDP
  - ICMP
  - その他
- 'rate1' と 'rate2' は数字です。
- 'duration' は数字です。
- 'total-flows' は、攻撃のアクションによって、次の文字列の 1 つです。
  - 'action' がブロックの場合：'number' に表示されている数のフローがブロックされます。
  - 'action' がレポートの場合：攻撃には、'number' に表示されている数のフローが含まれています。
- 'hw-filter'
  - 攻撃がハードウェア フィルタによってフィルタ処理されなかった場合：空の文字列
  - 攻撃がハードウェア フィルタによってフィルタ処理された場合：HW フィルタが使用され、実際の攻撃の長さは前述のレポートより小さく、また、処理されたフローの実際の量は前述のレポートより大きい可能性があります。

CLI トラップを使用した攻撃フィルタリングのモニタリング

- 「特定の攻撃ディテクタの設定を表示するには」（P.11-23）
- 「デフォルトの攻撃ディテクタの設定を表示するには」（P.11-24）
- 「すべての攻撃ディテクタの設定を表示するには」（P.11-25）
- 「フィルタ状態を表示するには（イネーブルまたはディセーブル）」（P.11-25）
- 「設定済みのしきい値とアクションを表示するには」（P.11-25）
- 「現在のカウンタを表示するには」（P.11-27）
- 「現在処理されている攻撃をすべて表示するには」（P.11-27）
- 「すべての既存の force-filter 設定を表示するには」（P.11-27）
- 「すべての既存の don't-filter 設定を表示するには」（P.11-27）
- 「サブスクライバ通知用に選択されたポートのリストを表示するには」（P.11-28）
- 「ハードウェア攻撃フィルタリングがアクティブかどうかを確認するには」（P.11-28）

攻撃の検出およびフィルタリングをモニタリングするには、ここで説明するコマンドを使用します。

- show interface linecard 0 attack-detector
- show interface linecard 0 attack-filter
- show interface linecard 0 attack-filter query
- show interface linecard 0 attack-filter current-attacks
- show interface linecard 0 attack-filter don't-filter
- show interface linecard 0 attack-filter force-filter
- show interface linecard 0 attack-filter subscriber-notification ports

特定の攻撃ディテクタの設定を表示するには

- 「オプション」（P.11-23）
- 「例：」（P.11-23）

次の情報が表示されます。

- プロトコル側：攻撃ディテクタが、サブスクライバ側から発信される攻撃に適用されるか、または、ネットワーク側から発信される攻撃に適用されるか。
- 方向：デフォルトの攻撃ディテクタを、シングル サイド攻撃に適用するかデュアル サイド攻撃に適用するか。攻撃が検出された場合に実行されるアクション。
- しきい値：
  - open-flows-rate：オープン フローのレートに対するデフォルトのしきい値（1 秒あたりの新しいオープン フロー）
  - suspected-flows-rate：疑わしい DDoS フローのレートに対するデフォルトのしきい値（1 秒あたりの新たな疑わしいフロー）
  - suspected-flows-ratio：オープン フローのレートに対する疑わしいフローのレートの割合のデフォルトのしきい値
- サブスクライバ通知の設定：イネーブルまたはディセーブル
- アラーム：SNMP トラップの送信がイネーブルまたはディセーブル

オプション

次のオプションを使用できます。

- **number**：表示される攻撃ディテクタの数

ステップ 1　SCE> プロンプトで、**show interface linecard 0 attack-detector** *number* と入力し、**Enter** キーを押します。

例：

```
SCE>show interface LineCard 0 attack-detector 1
Detector #1:
Comment: 'Sample'
Access-list: 1
Effective only for TCP port(s) 21,23,80
Effective for all UDP ports
Protocol|Side|Direction  ||Action|     Thresholds                |Sub- |Alarm
|    |           ||      |Open flows|Ddos-Suspected flows|notif|
|    |           ||      |rate      |rate        |ratio  |     |
--------|----|-----------||------|----------|------------|-------|-----|-----
TCP     |net.|source-only||      |          |            |       |     |
TCP     |net.|dest-only  ||      |          |            |       |     |
TCP     |sub.|source-only||      |          |            |       |     |
TCP     |sub.|dest-only  ||      |          |            |       |     |
TCP     |net.|source+dest||      |          |            |       |     |
TCP     |sub.|source+dest||      |          |            |       |     |
TCP+port|net.|source-only||Block |          |         |       |     |Yes
TCP+port|net.|dest-only  ||      |          |            |       |     |
TCP+port|sub.|source-only||Block |          |            |       |     |Yes
TCP+port|sub.|dest-only  ||      |          |            |       |     |
TCP+port|net.|source+dest||      |          |            |       |     |
TCP+port|sub.|source+dest||      |          |            |       |     |
```

```
UDP     |net.|source-only||      |          |            |       |     |
UDP     |net.|dest-only  ||      |          |            |       |     |
UDP     |sub.|source-only||      |          |            |       |     |
UDP     |sub.|dest-only  ||      |          |            |       |     |
UDP     |net.|source+dest||      |          |            |       |     |
UDP     |sub.|source+dest||      |          |            |       |     |
UDP+port|net.|source-only||      |          |            |       |     |
UDP+port|net.|dest-only  ||      |          |            |       |     |
UDP+port|sub.|source-only||      |          |            |       |     |
UDP+port|sub.|dest-only  ||      |          |            |       |     |
UDP+port|net.|source+dest||      |          |            |       |     |
UDP+port|sub.|source+dest||      |          |            |       |     |
ICMP    |net.|source-only||      |          |            |       |     |
ICMP    |net.|dest-only  ||      |          |            |       |     |
ICMP    |sub.|source-only||      |          |            |       |Yes  |
ICMP    |sub.|dest-only  ||      |          |            |       |     |
other   |net.|source-only||      |          |            |       |     |
other   |net.|dest-only  ||      |          |            |       |     |
other   |sub.|source-only||      |          |            |       |     |
other   |sub.|dest-only  ||      |          |            |       |     |
Empty fields indicate that no value is set and configuration from
the default attack detector is used.
SCE#>
```

デフォルトの攻撃ディテクタの設定を表示するには

ステップ 1　SCE> プロンプトで、**show interface linecard 0 attack-detector default** と入力し、**Enter** キーを押します。

例：

```
SCE>show interface LineCard 0 attack-detector default
Default detector:
Protocol|Side|Direction  ||Action|     Thresholds                |Sub- |Alarm
|    |           ||      |Open flows|Ddos-Suspected flows|notif|
|    |           ||      |rate      |rate        |ratio  |     |
--------|----|----------||------|----------|------------|-------|-----|-----
TCP     |net.|source-only||Report|      1000|         500|50     |No   |No
TCP     |net.|dest-only  ||Report|      1000|         500|50     |No   |No
TCP     |sub.|source-only||Report|      1000|         500|50     |No   |No
TCP     |sub.|dest-only  ||Report|      1000|         500|50     |No   |No
TCP     |net.|source+dest||Report|       100|          50|50     |No   |No
TCP     |sub.|source+dest||Report|       100|          50|50     |No   |No
TCP+port|net.|source-only||Report|      1000|         500|50     |No   |No
TCP+port|net.|dest-only  ||Report|      1000|         500|50     |No   |No
TCP+port|sub.|source-only||Report|      1000|         500|50     |No   |No
TCP+port|sub.|dest-only  ||Report|      1000|         500|50     |No   |No
TCP+port|net.|source+dest||Report|       100|          50|50     |No   |No
TCP+port|sub.|source+dest||Report|       100|          50|50     |No   |No
UDP     |net.|source-only||Report|      1000|         500|50     |No   |No
UDP     |net.|dest-only  ||Report|      1000|         500|50     |No   |No
UDP     |sub.|source-only||Report|      1000|         500|50     |No   |No
UDP     |sub.|dest-only  ||Report|      1000|         500|50     |No   |No
UDP     |net.|source+dest||Report|       100|          50|50     |No   |No
UDP     |sub.|source+dest||Report|       100|          50|50     |No   |No
UDP+port|net.|source-only||Report|      1000|         500|50     |No   |No
UDP+port|net.|dest-only  ||Report|      1000|         500|50     |No   |No
UDP+port|sub.|source-only||Report|      1000|         500|50     |No   |No
UDP+port|sub.|dest-only  ||Report|      1000|         500|50     |No   |No
```

```
UDP+port|net.|source+dest||Report|       100|          50|50     |No   |No
UDP+port|sub.|source+dest||Report|       100|          50|50     |No   |No
ICMP    |net.|source-only||Report|       500|         250|50     |No   |No
ICMP    |net.|dest-only  ||Report|       500|         250|50     |No   |No
ICMP    |sub.|source-only||Report|       500|         250|50     |No   |No
ICMP    |sub.|dest-only  ||Report|       500|         250|50     |No   |No
other   |net.|source-only||Report|       500|         250|50     |No   |No
other   |net.|dest-only  ||Report|       500|         250|50     |No   |No
other   |sub.|source-only||Report|       500|         250|50     |No   |No
other   |sub.|dest-only  ||Report|       500|         250|50     |No   |No
SCE#>
```

すべての攻撃ディテクタの設定を表示するには

ステップ 1　SCE> プロンプトで、**show interface linecard 0 attack-detector all** と入力し、**Enter** キーを押します。

フィルタ状態を表示するには（イネーブルまたはディセーブル）

ステップ 1　SCE> プロンプトで、**show interface linecard 0 attack-filter** と入力し、**Enter** キーを押します。

例：

```
SCE>show interface LineCard 0 attack-filter
Enabled state :
------------------
Protocol  |Direction   |State
----------|------------|------------
TCP       |source-only |enabled
TCP       |dest-only   |enabled
TCP       |dest+source |enabled
TCP+port  |source-only |enabled
TCP+port  |dest-only   |enabled
TCP+port  |dest+source |enabled
UDP       |source-only |enabled
UDP       |dest-only   |enabled
UDP       |dest+source |enabled
UDP+port  |source-only |enabled
UDP+port  |dest-only   |enabled
UDP+port  |dest+source |enabled
ICMP      |source-only |enabled
ICMP      |dest-only   |enabled
other     |source-only |enabled
other     |dest-only   |enabled
SCE#>
```

設定済みのしきい値とアクションを表示するには

このコマンドを使用すると、指定された IP アドレス（およびポート）で設定されているしきい値とアクションが表示され、さまざまな特定の攻撃ディテクタ アクセス リスト設定を考慮が入れられます。

- 「オプション」（P.11-26）
- 「例 1 ：」（P.11-26）

オプション

前述の攻撃ディテクタ オプションに加え、次のオプションを使用できます。

- **ip-address**：情報を表示する IP アドレス。

  attack -direction がデュアル サイドの場合、送信元側（*source-ip-address*）および宛先側（*dest-ip-address*）の両方で、IP アドレスを設定する必要があります。

- **portnumber**：情報を表示するポート番号。

ステップ 1　SCE> プロンプトで、**show interface linecard 0 attack-filter query ((single-sided ip** *ip-address* **)|(dual-sided source-IP** *source-ip-address* **destination-IP** *dest-ip-address* **)) [dest-port portnumber] configured** と入力し、**Enter** キーを押します。

例 1 ：

次に、IP アドレスが 1 つの場合のクエリーの出力例を示します。

```
SCE#>show interface linecard 0 attack-filter query single-sided ip 10.1.1.1 configured
Protocol|Side|Dir.|Action|      Thresholds           |don't- |force-|Sub- |Alarm
|    |    |      |Open flows|Ddos-Susp. flows|filter|filter|notif|
|    |    |      |rate      |rate      |ratio|      |      |     |
--------|----|----|------|----------|----------|-----|----- |------|-----|-----
TCP     |net.|src.|Report|      1000|       500|   50|No    |No    |   No|   No
TCP     |net.|dst.|Report|      1000|       500|   50|No    |No    |   No|   No
TCP     |sub.|src.|Report|      1000|       500|   50|No    |No    |   No|   No
TCP     |sub.|dst.|Report|      1000|       500|   50|No    |No    |   No|   No
UDP     |net.|src.|Report|      1000|       500|   50|No    |No    |   No|   No
UDP     |net.|dst.|Report|      1000|       500|   50|No    |No    |   No|   No
UDP     |sub.|src.|Report|      1000|       500|   50|No    |No    |   No|   No
UDP     |sub.|dst.|Report|      1000|       500|   50|No    |No    |   No|   No
ICMP    |net.|src.|Report|       500|       250|   50|No    |No    |   No|   No
ICMP    |net.|dst.|Report|       500|       250|   50|No    |No    |   No|   No
ICMP    |sub.|src.|Report|       500|       250|   50|No    |No    |  Yes|   No
|    |    |      |          |          |     |      |      |  (1)||
ICMP    |sub.|dst.|Report|       500|       250|   50|No    |No    |   No|   No
other   |net.|src.|Report|       500|       250|   50|No    |No    |   No|   No
other   |net.|dst.|Report|       500|       250|   50|No    |No    |   No|   No
other   |sub.|src.|Report|       500|       250|   50|No    |No    |   No|   No
other   |sub.|dst.|Report|       500|       250|   50|No    |No    |   No|   No
(N) below a value means that the value is set through attack-detector #N.
SCE#>
```

例 2 ：

次に、IP アドレスが 1 つの場合の、指定されたポートでのクエリーの出力例を示します。

```
SCE#>show interface linecard 0 attack-filter query single-sided ip 10.1.1.1 dest-port 21
configured
Protocol|Side|Dir.|Action|      Thresholds           |don't- |force-|Sub- |Alarm
|    |    |      |Open flows|Ddos-Susp. flows|filter|filter|notif|
|    |    |      |rate      |rate      |ratio|      |      |     |
--------|----|----|------|----------|----------|-----|----- |------|-----|-----
TCP+port|net.|src.|Block |      1000|       500|   50|No    |No    |   No|  Yes
|    |    |(1)   |      |          |          |     |      |      |     |  (1)
TCP+port|net.|dst.|Report|      1000|       500|   50|No    |No    |   No|   No
TCP+port|sub.|src.|Block |      1000|       500|   50|No    |No    |   No|  Yes
|    |    |(1)   |      |          |          |     |      |      |     |  (1)
TCP+port|sub.|dst.|Report|      1000|       500|   50|No    |No    |   No|   No
UDP+port|net.|src.|Report|      1000|       500|   50|No    |No    |   No|   No
UDP+port|net.|dst.|Report|      1000|       500|   50|No    |No    |   No|   No
UDP+port|sub.|src.|Report|      1000|       500|   50|No    |No    |   No|   No
UDP+port|sub.|dst.|Report|      1000|       500|   50|No    |No    |   No|   No
(N) below a value means that the value is set through attack-detector #N.
SCE#>
```

現在のカウンタを表示するには

このコマンドを使用すると、特定の IP アドレスに関する攻撃タイプで指定された攻撃ディテクタの現在のカウンタを表示できます。

ステップ 1　SCE> プロンプトで、**show interface linecard 0 attack-filter query ((single-sided ip** *ip-address* **)|(dual-sided source-IP** *source-ip-address* **destination-IP** *dest-ip-address* **)) [dest-port** *portnumber***] current** と入力し、**Enter** キーを押します。

現在処理されている攻撃をすべて表示するには

ステップ 1　SCE> プロンプトで、**show interface linecard 0 attack-filter current-attacks** と入力し、**Enter** キーを押します。

すべての既存の force-filter 設定を表示するには

ステップ 1　SCE> プロンプトで、**show interface linecard 0 attack-filter force-filter** と入力し、**Enter** キーを押します。

すべての既存の don't-filter 設定を表示するには

ステップ 1　SCE> プロンプトで、**show interface linecard 0 attack-filter don't-filter** と入力し、**Enter** キーを押します。

サブスクライバ通知用に選択されたポートのリストを表示するには

ステップ 1　SCE> プロンプトで、**show interface linecard 0 attack-filter subscriber-notification ports** と入力し、**Enter** キーを押します。

ハードウェア攻撃フィルタリングがアクティブかどうかを確認するには

ステップ 1　SCE> プロンプトで、`show interface linecard 0 attack-filter current-attacks` と入力し、**Enter** キーを押します。

このコマンドからの出力は、「HW-filter」フィールドで確認します。このフィールドが「yes」の場合、ユーザは、攻撃のレポートに不正確な情報が含まれている可能性があることを考慮する必要があります。

この情報は、攻撃ログ ファイルにも表示されることに注意してください。

```
|---------------|-----------|------------|----------|------|------|------
|Source IP ->  |Side /     |Open rate / |Handled   |Action|HW-   |force-
|         Dest IP|Protocol   |Susp. rate  |  flows / |      |filter|filter
|               |           |            |Duration  |      |      |
|---------------|-----------|------------|----------|------|------|------
|10.1.1.1       | Subscriber|         523|      4045|Report|No    |No
|               *|TCP        |           0|         9|      |      |
|---------------|-----------|------------|----------|------|------|------
```

攻撃のログ

- 「攻撃ログを表示するには」（P.11-29）
- 「攻撃ログをファイルにコピーするには」（P.11-29）

attack-log には、攻撃の開始と攻撃の終了の各特定 IP 検出について、メッセージが含まれています。メッセージは CSV フォーマットです。

攻撃の開始を検出するメッセージは、次のデータです。

- IP アドレス（検出された場合、アドレスのペア）
- プロトコル ポート番号（検出された場合）
- 攻撃の方向（攻撃元または攻撃先）
- IP アドレスのインターフェイス（サブスクライバまたはネットワーク）
- 攻撃検出時のオープン フロー レート、疑わしいフローのレート、疑わしいフローの割合
- 検出のしきい値
- 実行するアクション

攻撃の終了を検出するメッセージは、次のデータです。

- IP アドレス（検出された場合、アドレスのペア）
- プロトコル ポート番号（検出された場合）
- 攻撃の方向（攻撃元または攻撃先）
- IP アドレスのインターフェイス

- レポートまたはブロックされた攻撃フロー数
- 実行するアクション

他のログとして、2 つの攻撃ログ ファイルがあります。攻撃イベントは、これらのファイルの 1 つが最大容量に達するまで、書き込まれます。この時点で、ファイルに記録されたイベントを指すポインタが、一時的にアーカイブされます。その後、新しい攻撃イベントは代替ログ ファイルに自動的に記録されます。2 番めのログ ファイルが最大容量に達すると、ロギング イベントは最初のログ ファイルに戻され、ファイル内に保存されていた一時的なアーカイブ情報が上書きされます。

次の SNMP トラップは、攻撃ログがいっぱいで、新しいログがオープンされたことを意味します。

ST_LINE_ATTACK_LOG_IS_FULL

（注） 攻撃ログが大きい場合は、その表示の使用は推奨しません。巨大なログはファイルにコピーして表示します。

攻撃ログを表示するには

ステップ 1　SCE# プロンプトで、**more line-attack-log** と入力し、**Enter** キーを押します。

攻撃ログをファイルにコピーするには

ステップ 1　SCE# プロンプトで、**more line-attack-log redirect** *filename* と入力し、**Enter** キーを押します。

ログ情報を指定したファイルに書き出します。