CHAPTER 12

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、アタック フィルタ モジュールの設定手順およびモニタ手順を示します。

攻撃のフィルタリングおよび攻撃の検出

攻撃のフィルタリング

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。

攻撃のフィルタリングは、特定 IP のアタック ディテクタを使用して実行されます。特定 IP のアタック ディテクタでは、SCE プラットフォームの（オープンしていて、疑いのあるすべての）フローレートを IP アドレスの各組み合わせ（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 に関する）、インターフェイスおよび方向について、追跡します。ユーザが設定した基準を満たすレートは攻撃と見なされ、設定したアクションが実行されます（レポートおよびブロック、サブスクライバへの通知、SNMP トラップの送信）。

このメカニズムはデフォルトでイネーブルで、攻撃タイプ別にディセーブルおよびイネーブルに設定できます。

攻撃タイプには、32 種類あります。

- **1**：サブスクライバ側の特定の IP アドレスからの TCP フロー（宛先ポートに関係なく）
- **2**：サブスクライバ側の特定の IP アドレスへの TCP フロー（宛先ポートに関係なく）
- **3-4**：1 および 2 と同じ。ただし、逆方向（サブスクライバ 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。ただし、逆方向（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。ただし、攻撃のすべてのフローに共通する特定の宛先ポートを持つ（1 ～ 6 はポートレス攻撃タイプ、7 ～ 12 は、ポートベースの攻撃タイプ）
- **13-24**：1 ～ 12 と同じ。ただし、TCP ではなく UDP に対する攻撃
- **25-28**：1 ～ 4 と同じ。ただし、TCP ではなく ICMP に対する攻撃
- **29-32**：1 ～ 4 と同じ。ただし、TCP ではなくその他のプロトコルに対する攻撃

特定攻撃のフィルタリング

特定の攻撃タイプについて特定 IP の攻撃フィルタがイネーブルである場合、定義されたエンティティごとに次の 2 つのレートが測定されます。

- 新しいフローのレート
- 疑いのあるフローのレート（通常、疑いのあるフローとは SCOS が適切な確立を確認しなかったフロー [TCP]、または 1 つのパケットしか確認できなかったフロー [他のすべてのプロトコル] です）

それぞれのレート メートルは IP アドレス別に（片側）および IP アドレスのペア（所定のフローの送信元および宛先）で維持されるため、特定 IP が特定 IP を攻撃している場合、この IP アドレスのペアが 1 つのインシデントを定義します（両側）。

これらの 2 つのメトリックに基づいて、次のいずれかの状態が発生した場合に、特定 IP 攻撃が宣言されます。

- 新しいフローのレートが特定のしきい値を超過している。
- 疑いのあるフローのレートが設定されたしきい値を超過していて、疑いのあるフロー レートの新しいフローの合計レートに対する割合が設定されたしきい値を超過している。

レートがこの基準に達さなくなると、攻撃の終了が宣言されます。

特定の攻撃フィルタリングは、2 つの手順で設定されます。

- 特定の攻撃タイプに関する特定の IP フィルタリングのイネーブル化。
- 関連する攻撃タイプに関するアタック ディテクタの設定。各アタック ディテクタは、攻撃および攻撃が検出された場合に実行するアクションを定義するしきい値を指定します。

  特定のアタック ディテクタのほかに、デフォルトのディテクタがあります。ここでは、ユーザが定義したしきい値およびアクションが設定されるか、またはシステム デフォルトが保持されます。

さらに、ユーザは設定されたアタック ディテクタを手動で上書きして、特定の状況での攻撃フィルタリングを強制実行または防止できます。

選択した攻撃タイプに関する特定の IP フィルタリングは、次のパラメータによりイネーブル化されます。これらのパラメータは、32 種類の攻撃タイプのどれをフィルタリング対象とするかを制御します。

- **Protocol**：TCP、UDP、ICMP、またはその他
- **Attack direction**：攻撃方向が、1 つのみの IP アドレス、または 2 つの IP アドレスで識別されます。
  - **single side**：攻撃は、送信元 IP アドレスまたは宛先アドレスのどちらか一方で識別されます。

  フィルタ定義には、特定の側が指定されるか、またはどちらの側でもいずれか一方の攻撃が含まれる（both）場合があります。
  - **dual side**（TCP および UDP プロトコルのみ）：攻撃は送信元および宛先 IP アドレスの両方で識別されます。つまり、特定 IP が特定 IP を攻撃する場合、2 つの個別のインシデントではなく、1 つのインシデントとして検出されます。
- **Destination port**（TCP 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検出について、特定 IP の検出がイネーブルまたはディセーブルであるかを定義します。宛先ポート（または複数のポート）が固定された TCP/UDP 攻撃について、ポートベース検出をイネーブルにします。

  ポートベース検出の宛先ポートのリストは、個別に設定されます（「特定のアタック ディテクタ」（P.12-13）を参照）。

攻撃の検出

特定 IP の検出は、次のパラメータを使用して識別されます。

- 特定の IP アドレス（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：宛先ポートが固定されている TCP/UDP 攻撃
- 側：攻撃パケットの送信元であるインターフェイス（サブスクライバ/ネットワーク）
- 攻撃方向：1 つの IP アドレスが指定されている場合、この IP アドレスは攻撃の送信元アドレスまたは宛先アドレスです。

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、攻撃の開始と終了は常にレポートされます。
- **ブロック**：攻撃が持続している間、すべての攻撃トラフィックはブロックされます（IP アドレスが攻撃の送信元か宛先かに応じて、トラフィックはその IP アドレスで送信または受信されます）。
- **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**：攻撃が開始または中止されるたびに、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しきい値は、2 つあります。これらのしきい値は、SCE プラットフォームにより 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、および攻撃方向別に維持されるメートルに基づきます。

- **オープン フロー レート**：いくらかのトラフィックが確認されたフロー。新しいフローでパケットが確認された場合は、このフローがオープン フローであると宣言できます。

  レートは、新しいフローで秒単位で測定されます。

- **疑いのあるフロー レート**：疑いのあるフローとは、オープンであるのに、未確立であるフローのことです。

  レートは、新しいフローで秒単位で測定されます。

- **疑いのあるフローの比率**：疑いのあるフロー レートのオープン フロー レートに対する比率。

上記で説明したように、次のいずれかの状態が発生した場合に、特定 IP の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過している。
- 疑いのあるフロー レートおよび疑いのあるフローの比率がしきい値を超過している。

攻撃タイプごとの値では、デフォルト値がそれぞれに設定されています。

一般的に、所定のプロトコルにおいて、疑いのあるフロー レートのしきい値はポートレス検出よりポートベース検出に対する方が小さくなるよう設定されなければなりません。これは、所定の IP アドレスおよび共通の宛先ポートを持つフローでは、次のように測定が 2 回行われるからです。

- フロー自体による：ポートベース攻撃を検出する目的
- IP アドレスが同じで宛先ポートが異なるフローとともに：ポートレス攻撃を検出する目的

ポートベース攻撃が発生して、フロー レートが両方のしきい値（ポートベース しきい値およびポートレス しきい値）を超えた場合、ポートベース攻撃がポートレス攻撃より先に検出されることが望まれます。同様に、このしきい値は、シングル IP 検出よりデュアル IP 検出に対する方が小さくなるよう設定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、特定の IP アドレスおよびポートについて特定のしきい値を設定することもできます（アクセス リストおよびポート リストを使用して）。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ドロップされるため、宛先に到達しません。

  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）：**
- イネーブル：SNMP トラップが、攻撃の開始時および終了時に送信されます。

  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「側」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** [「attack- start」トラップのみ]
  - **実行したアクション**（レポート、ブロック）：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、指定し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。このときこのポートを、ブロック禁止に設定できます。

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、攻撃処理方法が 2 つあります（ハードウェアまたはソフトウェアによる）。通常、攻撃はソフトウェアによって処理されます。これにより、SCE プラットフォームは攻撃フローを正確に測定でき、攻撃が終了したことを直ちに検出できます。

ただし、かなり強い攻撃の場合、ソフトウェアではうまく処理できません。ソフトウェアが攻撃を十分に処理できない場合、結果として CPU 負荷が高くなり、SCE プラットフォームにより提供されるサービス（通常のトラフィック分類および制御）に悪影響が及びます。そのため、ソフトウェアを圧倒するおそれがある攻撃は、ハードウェアにより自動的にフィルタリングされます。

ハードウェアが攻撃のフィルタリングに使用される場合、ソフトウェアでは攻撃パケットについて認識していないため、次の副次的な悪影響が生じます。

- ソフトウェアが見積もる攻撃フロー数が、かなり少なくなります。これにより、CLI（show interface linecard attack-filter current-attacks）がレポートする攻撃フローの総数が、実際の数よりもかなり少なくなります。
- 同様に、（CLI が）レポートする攻撃フロー レートも実際のレートよりかなり低くなります。通常、ソフトウェアでは 0（ゼロ）のレートが測定されます。
- 攻撃終了の検出にかなりの遅延が生じます。攻撃終了の検出における遅延は、2 つの上限により制限されます。
  - 1 つめの上限は、次のように設定されたアクションごとに異なります。
  - レポート：8 分以下の遅延
  - ブロック：64 分以下の遅延
  - 遅延に対する 2 番めの上限は、実際の攻撃時間より 1 分多くなります（たとえば、3 分間持続する攻撃の終了を検出する場合の最大遅延は、4 分となります）。
- 次に、これらの 2 つの上限が相互作用する例を示します。
  - 2 分間持続している攻撃の場合、終了を検出する場合の最大遅延は、設定されたアクションに関係なく、3 分となります。
  - 設定されたアクションが「レポート」で、2 時間持続している攻撃の場合、終了を検出する場合の最大遅延は、8 分となります。
  - 設定されたアクションが「ブロック」で、2 時間持続している攻撃の場合、終了を検出する場合の最大遅延は、64 分となります。

ハードウェアの攻撃フィルタリングは自動プロセスのため、ユーザによる設定はできません。ただし、ハードウェアの攻撃フィルタリングが攻撃レポート及ぼす影響があるため、いつハードウェア処理が実行されるかを認識することが重要となります。そのため、ハードウェア フィルタリングのモニタリングが不可欠です。方法には 2 つあります（「攻撃フィルタリングをモニタする方法」（P.12-20）を参照）。

- **show interface linecard attack-filter current-attacks** コマンドで [*HW-filter*] フィールドを確認します。
- 攻撃ログ ファイルの [*HW-filter*] フィールドを確認します。

アタック ディテクタの設定

シスコの攻撃検出メカニズムは、アタック 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」と呼ばれるアタック 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 のアタック 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、32 の可能な攻撃タイプすべてについて、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、デフォルトのアタック 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、それぞれ異なるしきい値およびアクションのセットを設定できます。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。

デフォルトのアタック 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 未満なので、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毎秒何百もの DNS 要求を処理することがあるので、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。このしきい値を 1000 フロー / 秒にすれば、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、このような大きなレートの UDP フローの宛先になるのは、攻撃される可能性があるので、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を適用できません。

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、非デフォルトのアタック ディテクタ 1 ～ 99 を設定できます。非デフォルトのアタック ディテクタでも、デフォルトのアタック ディテクタと同様に、すべての攻撃タイプごとに、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、非デフォルトのアタック 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 コントロール 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、この種のアタック 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。非デフォルトのアタック 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。

非デフォルトのアタック ディテクタは、特別に設定された攻撃タイプに対してのみ有効です。そのため、デフォルトのアタック ディテクタの設定を、非デフォルトのアタック 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ので、着信 TCP フロー レートのしきい値を大きい値に設定した非デフォルトのアタック ディテクタを使用しなければなりません。この目的で、アタック ディテクタ 4 を使用すると仮定します。このアタック 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、デフォルトのアタック 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、デフォルトのアタック 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。アタック ディテクタ 4 は、UDP 攻撃には対応していないからです。

非デフォルトの各アタック ディテクタには、32 の攻撃タイプそれぞれについて、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 4 つの設定について、それぞれ設定（1 つの値または値のセットにより）または未設定のどちらでも可能です。デフォルト ステートは、すべての設定に関して未設定です。

アタックのタイプごとにイネーブルに設定したアタック ディテクタの集合と、デフォルトのアタック 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アタック ディテクタを、番号の小さい順にスキャンします。
- アタック 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、そのアタック 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、次のアタック 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アタック ディテクタがない場合、デフォルトのアタック ディテクタを使用します。

残りの設定（アクション、サブスクライバ通知、およびアラーム）で使用される値を決定する場合にも、同じ論理が適用されます。使用される値は、攻撃タイプに対する値が設定されていて、最も小さい値で番号付けされたイネーブルなアタック ディテクタが指定する値です。このようなアタック ディテクタが存在しない場合には、デフォルトのアタック ディテクタの設定が使用されます。

アタック ディテクタを設定してイネーブルにするには、次の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 の検出をイネーブルにする方法

デフォルトでは、特定 IP 検出はすべての攻撃タイプに関してイネーブルです。ユーザは、次のオプションに基づいて、特定 IP 検出を特定の定義された状況についてのみ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についてのみ。
- TCP および UDP プロトコルで、ポートベースまたはポートレス検出についてのみ。
- 選択された攻撃方向について、すべてのプロトコルまたは選択されたプロトコルに関して。

オプション

次のオプションを使用できます。

- **protocol**：特定 IP 検出をイネーブルまたはディセーブルにする特定のプロトコル。
  - デフォルト：すべてのプロトコル（プロトコルは指定されません）
- **attack direction**：特定 IP 検出が、片側または両側攻撃についてイネーブルかディセーブルかを定義します。
  - デフォルト：すべての方向
- **destination port**（TCP 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検出について、特定 IP の検出がイネーブルまたはディセーブルであるかを定義します。
  - デフォルト：ポートベースまたはポートレスの両方
- 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方法

ステップ 1　SCE(config if)# プロンプトに、**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)]** を入力して、**Enter** キーを押します。

すべての攻撃方向の TCP プロトコルについてのみ特定 IP 検出をイネーブルにする方法

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

両側攻撃のポートベース検出についてのみ特定 IP 検出をイネーブルにする方法

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

すべての攻撃方向の TCP、UDP、および ICMP 以外のプロトコルの特定 IP 検出をディセーブルにする方法

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

送信元 IP によって定義される片側攻撃に対して ICMP の特定 IP 検出をディセーブルにする方法

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

デフォルトのアタック ディテクタを設定する方法

デフォルトのアタック ディテクタで以下のパラメータに関して値を設定するには、次のコマンドを使用します。

- 攻撃処理のアクション
- 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対して定義された特定のアタック ディテクタは、設定済みのデフォルト アタック ディテクタを上書きします。

オプション

次のオプションを使用できます。

- **attack-detector**：設定されるアタック ディテクタ。この場合は、デフォルトのアタック ディテクタ。
- **protocol**：デフォルトのアタック ディテクタが適用するプロトコルを定義します。
- **attack-direction**：デフォルトのアタック ディテクタが片側の攻撃または両側の攻撃のどちらに対して適用されるかを定義します。
- **destination port**（TCP および UDP プロトコルのみ）：デフォルトのアタック ディテクタがポートベース検出またはポートレス検出のどちらに適用されるかを定義します。
- **side**：デフォルトのアタック ディテクタがサブスクライバ側かネットワーク側のどちらからの攻撃に適用されるかを定義します。
- **action**：デフォルト アクション
  - **report**（デフォルト）：攻撃の開始、終了時を攻撃ログに書き込むことにより、レポートします。
  - **block**：SCE プラットフォームは、この攻撃の一部であるすべての継続フローをブロックして、パケットをドロップします。
- **しきい値**：
  - **open-flows-rate**：オープン フロー レートに関するデフォルトのしきい値
    suspected-flows-rate：疑いのある DDoS フローのレートに関するデフォルトのしきい値
  - **suspected-flows-ratio**：疑いのあるフロー レートのオープン フロー レートに対する比率に関するデフォルトのしきい値
- サブスクライバ通知をデフォルトでイネーブルまたはディセーブルにするには、該当する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。
- SNMP トラップの送信をデフォルトでイネーブルまたはディセーブルにするには、該当する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。

デフォルトのアクションおよび任意でデフォルトのしきい値を定義する方法

デフォルト

デフォルトのアタック ディテクタのデフォルト値は、次のとおりです。

- アクション：レポート
- しきい値：攻撃タイプにより異なります。
- 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)# プロンプトに、**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*」を入力して、**Enter** キーを押します。

定義した攻撃タイプにデフォルトのアタック ディテクタが設定されます。

ステップ 2　SCE(config if)# プロンプトに、**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)** を入力して、**Enter** キーを押します。

定義した攻撃タイプに対して、デフォルトでのサブスクライバ通知がイネーブルまたはディセーブルになります。

攻撃タイプは、ステップ 1 と同じように定義されている必要があります。

ステップ 3　SCE(config if)# プロンプトに、**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)** を入力して、Enter キーを押します。

定義した攻撃タイプに対して、デフォルトでの SNMP トラップの送信がイネーブルまたはディセーブルになります。

攻撃タイプは、ステップ 1 と同じように定義されている必要があります。

選択した攻撃タイプのセットをシステムのデフォルト設定に戻す方法

選択された攻撃タイプのセットについて、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、および SNMP トラップ送信のデフォルト値を削除して、システムのデフォルト設定に戻すには、次のコマンドを使用します。

ステップ 1　SCE(config if)# プロンプトに、**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)** を入力して、**Enter** キーを押します。

定義した攻撃タイプがシステムのデフォルト設定に戻ります。

すべての攻撃タイプをシステムのデフォルト設定に戻す方法

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

定義した攻撃タイプがシステムのデフォルト設定に戻ります。

特定のアタック ディテクタ

選択された攻撃タイプのセットについて、特定のアタック ディテクタのしきい値、アクション、サブスクライバ通知の設定、および SNMP トラップの送信を定義するには、次のコマンドを使用します。

オプション

プロトコル、攻撃方向、および側の組み合わせごとに、固有のアタック 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 のアタック ディテクタをサポートします。各アタック 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。イネーブルのアタック 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**：指定されたアタック ディテクタに関連付けられた Access-Control List（ACL; アクセス コントロール リスト）の番号。ACL は、このディテクタで選択される IP アドレスを識別します（「ACL の設定」（P.5-19）を参照）。
  - dual-ip 検出の場合、ACL との照合に宛先 IP アドレスが使用されます。
  - このアタック ディテクタがすべての IP アドレスを許可することを示すには、「none」キーワードを使用します。

  このオプションは、ポート リストを定義するコマンドを使用する場合に役立ちます。すべての IP アドレスに対して必要な設定を設定する必要があります。
- **comment**：文書用。

イネーブルにするアタック 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**：指定したプロトコルの宛先ポート リスト。TCP および UDP プロトコルは、指定したポートにのみ設定される場合があります。これは、指定した宛先ポートのプロトコルごとのリストです。

  最大 15 の異なる TCP ポート番号および最大 15 の異なる UDP ポート番号を指定できます。

  所定のアタック ディテクタに TCP/UDP ポート リストを設定すると、同じプロトコル（TCP/UDP）を持つ攻撃タイプ（ポートベース）にのみ影響します（つまり、特定の宛先ポートを検出します）。設定したポート リストは、その他の攻撃タイプの設定には影響しません。

以下は、各アタック ディテクタで攻撃タイプごとに設定可能な設定です。それぞれ、「未設定」ステート（デフォルト）または特定の値により設定するステートのいずれかに設定できます。

- **action**：次のアクション

  - **report**（デフォルト）：攻撃の開始、終了時を攻撃ログに書き込むことにより、レポートします。
  - **block**：SCE プラットフォームは、この攻撃の一部であるすべての継続フローをブロックして、パケットをドロップします。
- **しきい値**：
  - **open-flows-rate**：オープン フロー レートに関するデフォルトのしきい値
    suspected-flows-rate：疑いのある DDoS フローのレートに関するデフォルトのしきい値
  - **suspected-flows-ratio**：疑いのあるフロー レートのオープン フロー レートに対する比率に関するデフォルトのしきい値
- サブスクライバ通知をデフォルトでイネーブルまたはディセーブルにするには、該当する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。
- SNMP トラップの送信をデフォルトでイネーブルまたはディセーブルにするには、該当する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。

特定のアタック ディテクタをイネーブルにして ACL に割り当てる方法

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

アタック ディテクタがイネーブルになり、指定した ACL に割り当てられます。

特定のアタック 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方法

ステップ 1　SCE(config if)# プロンプトに、**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***]** を入力して、**Enter** キーを押します。

指定したアタック ディテクタのアクションが定義されます。

特定のアタック ディテクタのサブスクライバ通知設定を定義する方法

所定のアタック ディテクタおよび選択された攻撃タイプのセットにサブスクライバ通知を設定するには、次のコマンドを使用します。

ステップ 1　SCE(config if)# プロンプトに、**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)** を入力して、**Enter** キーを押します。

指定したアタック ディテクタのサブスクライバ通知設定が定義されます。

特定のアタック ディテクタの SNMP トラップ設定を定義する方法

所定のアタック ディテクタおよび選択された攻撃タイプのセットで SNMP トラップをイネーブルまたはディセーブルにするには、次のコマンドを使用します。

ステップ 1　SCE(config if)# プロンプトに、**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)** を入力して、**Enter** キーを押します。

指定したアタック ディテクタの SNMP トラップ設定が定義されます。

特定のアタック ディテクタに対する TCP または UDP プロトコルの宛先ポートのリストを定義する方法

TCP または UDP プロトコルの特定ポート検出について、宛先ポートのリストを定義するには、次のコマンドを使用します。

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

指定したプロトコルおよびアタック ディテクタのポート リストが定義されます。

ユーザ定義値を削除する方法

特定のアタック ディテクタおよび選択された攻撃タイプのセットのしきい値、アクション、サブスクライバ通知の設定、および SNMP トラップの送信を削除するには、次のコマンドを使用します。

所定の攻撃タイプでこれらの設定を削除すると、デフォルトの「未設定」ステートに戻されます。これは、アタック ディテクタが、この攻撃タイプの応答の決定に関与していないことを意味します。

ステップ 1　SCE(config if)# プロンプトに、**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)** を入力して、**Enter** キーを押します。

指定した攻撃タイプに構成したアタック ディテクタ設定が削除されます。

特定のアタック ディテクタをディセーブルにする方法

特定のアタック ディテクタをディセーブルにして、すべてのプロトコル、攻撃方向、および側で、デフォルトのアクション、しきい値、およびサブスクライバ通知を使用するように設定する場合は、次のコマンドを使用します。

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

指定したアタック ディテクタがディセーブルになります。

すべての非デフォルトのアタック ディテクタをディセーブルにする方法

すべての非デフォルトのアタック ディテクタをディセーブルにして、デフォルトの値を使用するように設定する場合は、次のコマンドを使用します。

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

すべての非デフォルトのアタック ディテクタがディセーブルになります。

すべてのアタック ディテクタをディセーブルにする方法

すべてのアタック ディテクタをディセーブルにして、デフォルトの値を使用するよ§に設定する場合は、次のコマンドを使用します。

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

すべてのアタック ディテクタがディセーブルになります。

アタック ディテクタの設定例

次のコンフィギュレーションでは、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アタック ディテクタを設定しています。

ステップ 1　SCE(config if)# プロンプトに、**interface linecard 0** を入力して、**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)# プロンプトに、**attack-detector default protocol ICMP attack-direction** *single-side-source* **side** *both* **action** *report* **open-flow-rate** *1000* **suspected-flows-rate** *100* **suspected-flows-ratio** *10* を入力して、**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が設定されます。

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

アタック ディテクタ #1 をイネーブルにして、ACL #3 を割り当てます。

ステップ 4　SCE(config if)# プロンプトに、**attack-detector** *1* **UDP-ports-list** *53* を入力します。

アタック ディテクタ #1 に 1 つのポート（ポート 53 を含む）UDP 宛先ポートのリストを定義します。

ステップ 5　SCE(config if)# プロンプトに、**attack-detector** *1* **protocol UDP dest-port** *specific* **attack-direction** *single-side-destination* **side** *both* **action** *report* **open-flow-rate** *1000000* **suspected-flows-rate** *1000000* を入力して、**Enter** キーを押します。

アタック ディテクタ #1 にしきい値およびアクションが定義されます。

ステップ 6　SCE(config if)# プロンプトに、**attack-detector** *1* **protocol UDP dest-port** *specific* **attack-direction** *single-side-destination* **side** *subscriber* **notify-subscriber** を入力して、**Enter** キーを押します。

アタック ディテクタ #1 で、サブスクライバ通知をイネーブルにします。

ステップ 7　SCE(config if)# プロンプトに、**exit** を入力して、**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 8　アタック ディテクタに割り当てられている ACL #3 が設定されます。

```
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、アタック ディテクタ レベルで設定します。また、『*Cisco Service Control Application for Broadband User Guide*』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の設定方法

ポートを、サブスクライバ通知ポートとして使用されるように定義できます。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ので、これら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数

ステップ 1　SCE(config if)# プロンプトに、**attack-filter subscriber-notification ports** *portnumber* を入力して、**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方法

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

攻撃検出の停止および実行

アタック 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 アタック 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 コマンドを使用して、次の操作を実行できます。

- **dont-filter** コマンドを設定して、指定した IP アドレスに関連する攻撃のフィルタリングを阻止または停止する。
- **force-filter** コマンドを設定して、指定した IP アドレスに関連する攻撃のフィルタリング（特定のアクションを含む）を強制実行する。

攻撃のフィルタリングを実行または停止するには、次の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

前述のアタック 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回避する IP アドレス

  attack -direction が両側である場合、送信元（*source-ip-address*）と宛先（*dest-ip-address*）の両側に 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。

- 「指定した状況に dont-filter 設定を設定する方法」（P.12-19）
- 「指定した状況から dont-filter 設定を削除する方法」（P.12-19）
- 「すべての dont-filter 設定を削除する方法」（P.12-19）

指定した状況に dont-filter 設定を設定する方法

ステップ 1　SCE(config if)# プロンプトに、**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)** を入力して、**Enter** キーを押します。

指定した状況から dont-filter 設定を削除する方法

ステップ 1　SCE(config if)# プロンプトに、**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)** を入力して、**Enter** キーを押します。

すべての dont-filter 設定を削除する方法

ステップ 1　SCE(config if)# プロンプトに、**no attack-filter dont-filter all** を入力して、**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。

- 「指定した状況に force-filter 設定を設定する方法」（P.12-20）
- 「指定した状況から force-filter 設定を削除する方法」（P.12-20）
- 「すべての force-filter 設定を削除する方法」（P.12-20）

指定した状況に force-filter 設定を設定する方法

ステップ 1　SCE(config if)# プロンプトに、**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]** を入力して、**Enter** キーを押します。

指定した状況から force-filter 設定を削除する方法

ステップ 1　SCE(config if)# プロンプトに、**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)** を入力して、**Enter** キーを押します。

すべての force-filter 設定を削除する方法

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

攻撃フィルタリングをモニタする方法

- 「SNMP トラップを使用した攻撃フィルタリングのモニタ」（P.12-21）
- 「CLI コマンドを使用した攻撃フィルタリングのモニタ」（P.12-22）
- 「攻撃ログの表示」（P.12-28）

攻撃フィルタリングおよび検出のモニタには 3 つのオプションがあります。

- CLI show コマンド
- SNMP 攻撃検出トラップ
- 攻撃ログ

SNMP トラップを使用した攻撃フィルタリングのモニタ

システムは、次のように、特定の攻撃検出イベントの開始時、および終了時にトラップを送信します。

- STARTED_FILTERING トラップ：攻撃情報を持つ文字列
- STOPPED_FILTERING
  - 攻撃情報を持つ文字列
  - 停止理由を持つ文字列

攻撃開始時に送信された攻撃情報文字列の形式は、次のとおりです。

- トラフィック内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'.
```

- **force-filter** コマンドの結果として攻撃が明らかになった場合：

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

攻撃終了時に送信された攻撃情報文字列の形式は、次のとおりです。

- トラフィック内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'
```

- **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攻撃の終了が明らかになった場合：

```
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.
```

攻撃開始時に送信された理由文字列の形式は、次のとおりです。

- トラフィック内で攻撃終了が検出された場合：

```
Detected attack end
```

- **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攻撃の終了が明らかになった場合：

```
Forced attack end
```

情報文字列（''）で示されるフィールドに表示される可能性のある値は次のとおりです。

- 'action'
  - Report
  - Block
- 'forced-action' は、設定された force-filter アクションに従い、次の値のいずれかになります。
  - block of flows
  - report
- 'IP-info' は、攻撃の方向および検出された IP アドレスが 1 つか 2 つかによって、次の形式のいずれかになります。
  - IP アドレス A.B.C.D から
  - IP アドレス A.B.C.D で
  - IP アドレス A.B.C.D から 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' は数値です。
- 'duration' は数値です。
- 'total-flows' は、攻撃アクションに従い、次の文字列のいずれかになります。
  - 'action' が block の場合：ブロックされた 'number' フロー
  - 'action' が report の場合：'number' フローで構成される攻撃
- 'hw-filter'
  - 攻撃がハードウェア フィルタでフィルタリングされなかった場合：空の文字列
  - 攻撃がハードウェア フィルタでフィルタリングされた場合：使用される HW フィルタ、実際の攻撃時間は前述のレポートより少なくなる可能性があり、処理される実際のフローの量は前述のレポートより多くなる可能性があります。

CLI コマンドを使用した攻撃フィルタリングのモニタ

攻撃の検出およびフィルタリングをモニタするには、次の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**

指定したアタック ディテクタの設定を表示する方法

- 「オプション」（P.12-23）
- 「例：」（P.12-23）

次の情報が表示されます。

- プロトコル側：アタック ディテクタがサブスクライバ側かネットワーク側のどちらからの攻撃に適用されるか。
- 方向：アタック ディテクタが片側攻撃または両側攻撃のどちらに適用されるか。攻撃が検出された場合に実行するアクション。
- しきい値：
  - open-flows-rate：オープン フロー レート（秒単位の新しいオープン フロー）に関するデフォルトのしきい値
  - suspected-flows-rate：疑いのあるフロー レートのオープン フロー レートに対する比率に関するデフォルトのしきい値
  - suspected-flows-ratio：疑いのあるフロー レートのオープン フロー レートに対する比率に関するデフォルトのしきい値
- サブスクライバ通知：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**：表示するアタック ディテクタの数

ステップ 1　SCE> プロンプトに、**show interface linecard 0 attack-detector** *number* を入力して、**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#>
```

デフォルトのアタック ディテクタの設定を表示する方法

ステップ 1　SCE> プロンプトに、**show interface linecard 0 attack-detector default** を入力して、**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#>
```

アタック ディテクタの設定をすべて表示する方法

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

フィルタの状態（イネーブルまたはディセーブル）を表示する方法

ステップ 1　SCE> プロンプトに、**show interface linecard 0 attack-filter** を入力して、**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#>
```

設定したしきい値とアクションを表示する方法

各種特定アタック ディテクタのアクセス リストの設定を考慮に入れて、指定した IP アドレス（およびポート）に設定されたしきい値およびアクションを表示するには、次のコマンドを使用します。

オプション

前述のアタック 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 が両側である場合、送信元（*source-ip-address*）と宛先（*dest-ip-address*）の両側に 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> プロンプトに、**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** を入力して、**Enter** キーを押します。

例

例 1

次に、IP アドレス 1 つのクエリーの例を示します。

```
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、指定したポートでの IP アドレス 1 つのクエリーの例を示します。

```
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#>
```

現在のカウンタの表示方法

指定した IP アドレスについて、アタック ディテクタの指定した攻撃タイプに関する現在のカウンタを表示するには、次のコマンドを使用します。

ステップ 1　SCE> プロンプトに、**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** を入力して、**Enter** キーを押します。

現在処理済みの攻撃をすべて表示する方法

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

既存 force-filter 設定をすべて表示する方法

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

既存 don't-filter 設定をすべて表示する方法

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

サブスクライバ通知に選択したポートのリストを表示する方法

ステップ 1　SCE> プロンプトに、**show interface linecard 0 attack-filter subscriber-notification ports** を入力して、**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になっているかどうかを調べる方法

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

このコマンドの出力で HW-filter フィールドを確認します。このフィールドが yes である場合、ユーザは攻撃レポートに誤りがある可能性を考慮に入れる必要があります。

この情報も、攻撃ログ ファイルに表示されます。

```
---|---------------|-----------|------------|----------|------|------|------
---|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|      |      |
---|----------------|-----------|------------|------------|------|------|-------
```

攻撃ログの表示

攻撃ログ

攻撃ログには、特定 IP 検出ごとの攻撃の開始および終了に関するメッセージが含まれます。メッセージは csv 形式です。

攻撃開始の検出に関するメッセージには、次のデータが含まれます。

- IP アドレス（検出された場合は、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（攻撃の送信元または宛先）
- 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、疑いのあるフローレート、疑いのあるフローの比率
- 検出に関するしきい値
- 実行されるアクション

攻撃終了の検出に関するメッセージには、次のデータが含まれます。

- IP アドレス（検出された場合は、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（攻撃の送信元または宛先）
- IP アドレスのインターフェイス
- レポートおよびブロックされた攻撃フロー数
- 実行されるアクション

他のログ ファイルと同様に、2 つの攻撃ログ ファイルがあります。どちらか一方のファイルが最大キャパシティに達するまで攻撃イベントが書き込まれ、その時点でこのファイルに記録されたイベントは一時的にアーカイブされます。もう 1 つのログ ファイルに新しい攻撃イベントが自動的に記録されます。2 番めのログ ファイルが最大キャパシティに達すると、最初のログ ファイルが再び使用され、そのファイルに保存されて一時的にアーカイブされた情報が上書きされます。

次の SNMP トラップは攻撃ログが満杯で、新しいログ ファイルがオープンされたことを示しています。

ST_LINE_ATTACK_LOG_IS_FULL

（注） 大容量の攻撃ログを表示することは推奨できません。大容量のログ ファイルは、コピーしてから表示してください。

攻撃ログの表示方法

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

攻撃ログをファイルにコピーする方法

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

指定したファイルにログ情報が書き込まれます。