CHAPTER 10

Detector モジュールとゾーンの動作の監視

この章では、Cisco Traffic Anomaly Detector Module（Detector モジュール）とそのゾーンのステータスを監視する方法、およびゾーンのトラフィック フローに関連する問題を診断する方法について説明します。

この章は、次の項で構成されています。

Detector の要約画面の表示

Detector の要約画面（図 10-1 を参照）には、現在の Detector モジュール アクティビティの要約が表示されます。これは、Detector モジュールの WBM に接続したときに最初に表示される画面です。この画面は、インターフェイス内の次の場所から表示できます。

- ナビゲーション ペインで **Detector Summary** をクリックする。
- 情報領域で **Home** をクリックする。

図 10-1　Detector モジュール要約画面

Detector の要約画面には、次の 2 つの領域があります。

- Detector Summary：最近 2 時間に Detector モジュールが処理した受信トラフィック レートの要約をビット / 秒（bps）単位でグラフに示します。

  表 10-1 に、グラフの下に表示される情報の説明を示します。

表 10-1　Detector の要約グラフに含まれるフィールドの説明

フィールド	説明
Min.	最近 2 時間に測定されたトラフィック レートの最小値（bps 単位）。
Max.	最近 2 時間に測定されたトラフィック レートの最大値（bps 単位）。
Avg.	最近 2 時間に測定されたトラフィック レートの平均値（bps 単位）。
Cur.	現在のトラフィック レート（bps 単位）。

- Zones Under Detection：Detector モジュールが現在トラフィックの異常を監視しているゾーンのステータス情報を示します。ゾーン情報は、次の異常検出モードのどちらをアクティブにするかによって異なります。
  - Detect：ゾーンが攻撃を受けている場合、および通常のトラフィック状態にある場合に、ゾーン情報を表示します。
  - Detect and Learn：ゾーンが攻撃を受けている場合にのみ、ゾーン情報を表示します。

  Detector モジュールでは、ゾーンは攻撃を受けた順にリスト表示されます（最後に攻撃を受けたゾーンがリストの最上部に表示されます）。各行の Detector モジュールに表示される情報をクリックすると、関連付けられているゾーンの要約画面を表示できます。

表 10-2 に、検出実行中のゾーンに含まれているフィールドの説明を示します。

表 10-2　異常検出実行中のゾーンに含まれているフィールドの説明

フィールド	説明
Zone	ゾーン名。ゾーン名は、特定のゾーンのステータス画面へのリンクにもなっています。
Activation Time	ゾーン保護がアクティブになった日時。
Attack Start Time	ゾーンに対する攻撃が最後に検出された日時。
#DF	動的フィルタの数。Detector モジュールが動的フィルタを作成するのは異常を検出した場合だけであるため、#DF 値が 0 より大きい場合は、ゾーンに対する攻撃を示します。
#PF	保留動的フィルタの数。インタラクティブ保護モードではなく、自動保護モードでゾーンを実行している場合、画面に N/A と表示されます。
Receive Rate	ゾーンが宛先となっていたトラフィックの現在のレート（bps 単位）。
ゾーン トラフィックの要約のサムネール	最近 30 分間のゾーン トラフィック（bps 単位）の要約を表示するグラフ。

Detector モジュールのグローバル診断ツールの使用

Detector モジュールでは、グローバル イベントの監視およびトラブルシューティングに役立つ診断情報が提供されます。この項は、次の内容で構成されています。

グローバル カウンタの表示

Counters 画面には、Detector モジュールが Detector モジュールの要約画面に表示するカウンタ情報の詳細な分析が提供されます。Counters 画面から、Detector モジュールがトラフィック レートのグラフに表示する情報をフィルタできます。

Detector モジュールのカウンタを表示するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインの **Detector Summary** をクリックします。Detector の要約メニューが表示されます。

ステップ 2　Detector の要約メニューで、**Diagnostics > Counters > Device Counters** を選択します。Counters 画面が表示されます。

デフォルトでは、トラフィック レートのグラフには、最近 2 時間に記録した、bps 単位で測定されたカウンタ情報が表示されます。

ステップ 3　（オプション）Detector モジュールがトラフィック レートのグラフで使用する測定単位を変更します。Graph Type ドロップダウン リストで測定単位を選択します。

- **pps**：パケット / 秒
- **bps**：ビット / 秒

ステップ 4　**Update Graph** をクリックします。Detector モジュールにより、グラフがアップデートされます。

ステップ 5　（オプション）Detector モジュールのカウンタをクリアするには、**Clear Counters** をクリックします。Detector モジュールが現在のカウンタとトラフィック レートをクリアします。カウンタにテスト セッションの情報だけが含まれるようにテストを実行する場合は、Detector モジュールのカウンタをクリアできます。

受信パケットのカウンタは、Detector モジュールが受信して分析したパケットの総数を示します。

表 10-3 に、受信パケットのカウンタに含まれているフィールドの説明を示します。

表 10-3　受信パケットのカウンタに含まれているフィールドの説明

フィールド	説明
Packets	Detector モジュールがリロードされた後のパケットの総数。
Bits	Detector モジュールがリロードされた後のビットの総数。
pps	現在のトラフィック レート（パケット / 秒単位）。
bps	現在のトラフィック レート（bps 単位）。

Detector モジュールのカウンタのクリア

カウンタにテスト セッションの情報だけが含まれるようにテストを実行する場合は、Detector モジュールのカウンタをクリアできます。

Detector モジュールのカウンタをクリアするには、次の手順を実行します。

ステップ 1　ナビゲーション ペインの **Detector Summary** をクリックします。Detector の要約メニューが表示されます。

ステップ 2　Detector の要約メニューで、**Diagnostics > Counters > Device Counters** を選択します。Counters 画面が表示されます。

ステップ 3　**Clear Counters** をクリックします。Detector モジュールが現在のカウンタとトラフィック レートをクリアします。

グローバル受信カウンタのリアルタイムでの表示

Detector モジュールでは、受信パケットのカウンタ情報をリアルタイムで表示できます。受信パケットのカウンタは、Detector モジュールが受信して分析したパケットの総数を示します。

（注）　カウンタ情報をリアルタイムに表示するには、クライアントに Java Runtime Environment（JRE）をインストールしておく必要があります（第 1 章「製品の概要」の「Java 2 Runtime Environment のインストール」の項を参照）。

カウンタをリアルタイムで表示するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインの **Detector Summary** をクリックします。Detector の要約メニューが表示されます。

ステップ 2　Detector の要約メニューで **Diagnostics > Counters > Real time counters** を選択します。Real Time Counters 画面が表示されます。

ステップ 3　（オプション）トラフィック レートのグラフで Detector モジュールが使用する測定単位を変更するには、次のいずれかの Graph Type オプションを選択します。

- **bps**：ビット / 秒
- **pps**：パケット / 秒

Detector モジュールにより、トラフィック レートのグラフがアップデートされます。

イベント ログの表示

Detector モジュールは、検出されているゾーンおよび Detector モジュールの動作に関連するシステム アクティビティとイベントを自動的に記録します。Detector モジュールのログを表示して、Detector モジュールのアクティビティを確認および追跡できます。

表 10-4 に、イベントの重大度レベルの説明を示します。

表 10-4　イベント ログの重大度レベル

イベントのレベル	説明
Emergencies	システムが使用不能
Alerts	ただちに対処が必要
Critical	深刻な状態
Errors	エラー状態
Warnings	警告状態
Notifications	通常、ただし注意が必要
Informational	情報メッセージ
Debugging	デバッグ メッセージ

（注）　イベント　　ログに表示されるのは、ゾーンに関係するイベントとその重大度レベル（Emergency、Alert、Critical、Error、Warning、または Notification）のみです。ゾーンのイベント ログの詳細については、「ゾーンのイベント ログの表示」の項を参照してください。

イベント ログの内容を表示するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインの **Detector Summary** をクリックします。Detector の要約メニューが表示されます。

ステップ 2　Detector の要約メニューで、**Diagnostics > Event log** を選択します。Events 画面が表示されます。イベント テーブルの上にあるナビゲーション ツールを使用して、イベントをスクロールします。

ステップ 3　（オプション）次のオプションのいずれかを選択し、イベント テーブルに表示するイベントを制御します。

- **Show all Events**：すべての重大度レベルのイベントを表示します。
- **Show events with severity level**：選択した重大度レベルのイベントだけを表示します（表 10-4 を参照）。

ステップ 4　**Filter Events** をクリックします。Detector モジュールにより、イベント テーブルがアップデートされます。

デバイス リソースの監視

Detector モジュールがシステム ステータスの分析と監視に使用しているリソースの概要を表示できます。

Detector モジュールのリソースのリストを表示するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインで **Detector Summary** をクリックします。Detector の要約メニューが表示されます。

ステップ 2　Detector の要約メニューで、**Diagnostics > Device Resources** を選択します。Detector モジュールの Device Resources 画面が表示されます。

表 10-5 に、Device Resources 画面に含まれるフィールドの説明を示します。

表 10-5　Device Resources 画面に含まれるフィールドの説明

フィールド	説明
Host CPU1	CPU1 が user mode、system mode、niced tasks、および idle になっている CPU 時間の割合。niced tasks はシステム時間とユーザ時間にもカウントされるので、CPU 使用率合計は 100 % を超えることがあります。
Flash space usage	Detector モジュールが使用している割り当て済みフラッシュ スペースの割合。 フラッシュ スペースの使用率がディスクの最大キャパシティの約 75 % に達すると、Detector モジュールはシステム ログに警告メッセージを表示し、トラップを送信します。 フラッシュの使用率がディスクの最大キャパシティの 80 % に達すると、Detector モジュールは情報を消去して、使用しているディスク スペースを約 75 % まで削減します。 Detector モジュールのレコードをネットワーク サーバに定期的に保存して、古いレコードを削除することをお勧めします。 フラッシュ スペースの使用率が 80 % に達した場合、ゾーン攻撃レポートをネットワーク サーバにエクスポートしてから、古い攻撃レポートを削除できます（「攻撃レポートのエクスポート」および「攻撃レポートの削除」の項を参照）。
Accelerator card memory usage	アクセラレータ カードが使用しているメモリの割合。 アクセラレータ カードのメモリ使用率が 85 % を超える場合、Detector モジュールは SNMP トラップを生成します。大きな値は、Detector モジュールが大量のトラフィックを監視していることを示す場合があります。

表 10-5　Device Resources 画面に含まれるフィールドの説明（続き）

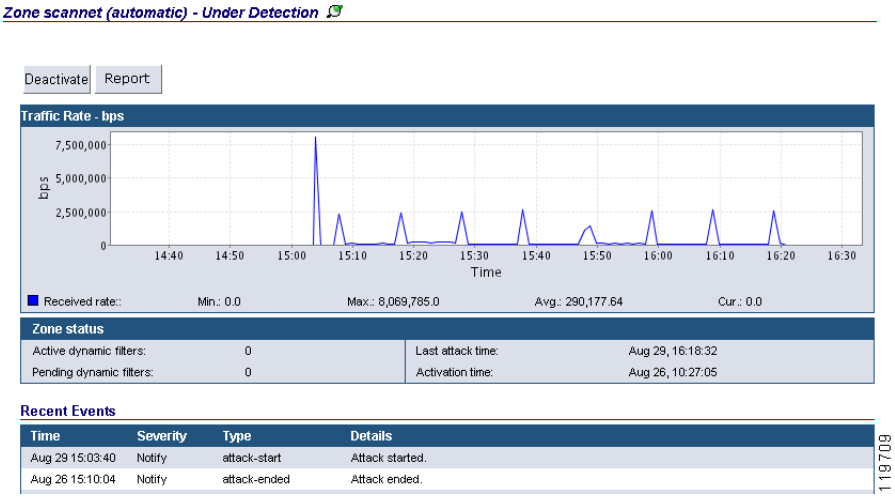
フィールド	説明
Accelerator card CPU utilization	使用しているアクセラレータ カードの CPU の割合。 アクセラレータ カードの CPU 使用率が 85 % を超える場合、Detector モジュールは SNMP トラップを生成します。大きな値は、Detector モジュールが大量のトラフィックを監視していることを示す場合があります。
Anomaly detection engine used memory	Detector モジュールの統計エンジンが使用するメモリの割合を指定します。異常検出エンジンのメモリ使用率は、アクティブなゾーンの数、各ゾーンが監視するサービスの数、Detector モジュールが監視している非スプーフィング トラフィックの量の影響を受けます。 異常検出エンジンのメモリ使用率が 90 % を超える場合、アクティブなゾーンの数を減らすことを強くお勧めします。
Dynamic filters used	すべてのゾーンでアクティブになっている動的フィルタの総数。Detector モジュールは、アクティブな動的フィルタの数と、Detector モジュールがサポートしている総数 150,000 の動的フィルタのうちアクティブな動的フィルタの割合を表示します。アクティブな動的フィルタの数が 150,000 に達した場合、Detector モジュールは重大度レベル EMERGENCY の SNMP トラップを生成します。アクティブな動的フィルタの数が 135,000 に達した場合、Detector モジュールは重大度レベル WARNING の SNMP トラップを生成します。 大きな値は、Detector モジュールが DDoS 攻撃の大量のトラフィックを監視していることを示す場合があります。
Number of zones	Detector モジュールに定義されているゾーンの総数。
Number of attacked zones	ゾーン保護がアクティブになっていて、攻撃を受けているゾーンの総数。
Number of active zones	ゾーン保護またはゾーン ラーニングがアクティブになっているゾーンの総数。

ゾーンのステータス画面の表示

ゾーンのステータス画面（図 10-2 を参照）には、ゾーン動作のステータスの要約が示されます。この画面には、次の方法で移動できます。

- ナビゲーション ペインの All Zones リストでゾーン名をクリックする。
- ゾーンの異常検出が現在イネーブルの場合は、ナビゲーション ペインの Under Detection リストからゾーン名をクリックする。
- ゾーンの特定の画面のナビゲーション パスで、**Zone** をクリックする。
- ゾーンのリスト（**Detector Summary > Zones > Zone list**）でゾーン名をクリックする。

図 10-2　ゾーンのステータス画面



ゾーンのステータス画面は 4 つの領域（ゾーンのステータス バー、ゾーンのトラフィック レートのグラフ、ゾーンのステータス テーブル、ゾーンの最近のイベント テーブル）に分割されています。次の項で説明します。

- ゾーンのステータス バーについて
- ゾーンのトラフィック レートのグラフについて
- ゾーンのステータス テーブルについて
- ゾーンの最近のイベント テーブルについて

ゾーンのステータス画面には、機能ボタンがあります。WBM では、ゾーンの現在の動作モードに応じて、異なる機能ボタンが表示されます。

ゾーンがスタンバイの場合、次の機能ボタンが表示されます。

- Detect & Learn：Detect and Learn 機能をアクティブにします。この機能により、Detector モジュールはラーニング プロセスのしきい値調整フェーズの実行中に、ゾーン トラフィックの異常を検出できます。このボタンを使用することは、ゾーンのメイン メニューで **Detection > Detect** を選択し、**Learning > Tune Thresholds** を選択する（この順序は重要でありません）のと同じです。
- Detect：ゾーンの異常検出をアクティブにします。このボタンを使用することは、ゾーンのメイン メニューで **Detection > Detect** を選択するのと同じです。

ゾーンの異常検出または Detect and Learn 機能が現在イネーブルの場合、次の機能ボタンが表示されます。

- Deactivate：ゾーン保護を非アクティブにします。このボタンを使用することは、ゾーンのメイン メニューで **Detection > Deactivate** を選択するのと同じです。

  Detect and Learn 機能がイネーブルの場合、**Deactivate** をクリックすると、ゾーン異常検出、ラーニング、またはその両方の操作を非アクティブにするオプションを使用できます。
- Report：現在の攻撃レポートへのリンクを提供します。このボタンを使用することは、ゾーンのメイン メニューで **Diagnostics > Attack reports > Attack Summary** を選択し、現在の攻撃（識別番号（#）が *Curr* になっている攻撃）をクリックするのと同じです。Report ボタンは、進行中の攻撃がある場合のみ使用できます。詳細については、「攻撃レポートの詳細について」の項を参照してください。

ゾーンのステータス バーについて

ゾーンのステータス バーは、ゾーンのステータス画面の最上部に表示され、現在操作しているゾーンのステータスをすばやく参照することができます。ゾーンのステータス バーでは、次の情報が提供されます。

- ゾーンの名前。
- Detector モジュールがゾーンの異常検出を実行するモード：Detector モジュールがゾーンに対して自動検出モードで動作するか、インタラクティブ検出モードで動作するかを示します。ゾーンの動作モード設定の詳細については、第 9 章「異常の検出のアクティブ化」の「自動動作モードとインタラクティブ動作モード」および「自動検出モードまたはインタラクティブ検出モードのアクティブ化」の項を参照してください。
- ゾーンの動作状態：ゾーンの現在の動作状態を示します。動作ステータスは、Under Detection、Under Detection/Tuning Thresholds、Inactive、Constructing Policy、または Tuning Thresholds です。
- 新しい推奨事項：新しい動的フィルタの推奨事項が利用可能になっており、推奨事項を受け入れるか、無視するか、自動アクティベーションに誘導するかを確認し、決定できることを示します。この通知が利用可能なのは、ゾーンの動作モードがインタラクティブに設定されている場合のみです。

ゾーンのトラフィック レートのグラフについて

ゾーンのトラフィック レートのグラフには、最近 2 時間に受信した、bps 単位で測定されたトラフィックのレートが表示されます。

表 10-6 に、ゾーンのトラフィック レートのグラフの下に表示されるフィールドの説明を示します。

表 10-6　ゾーンのトラフィック レートのグラフの下に表示されるフィールドの説明

フィールド	説明
Min	最近 2 時間に測定されたトラフィック レートの最小値（bps 単位）。
Max	最近 2 時間に測定されたトラフィック レートの最大値（bps 単位）。
Avg	最近 2 時間に測定されたトラフィック レートの平均値（bps 単位）。
Cur	現在のトラフィック レート（bps 単位）。

ゾーンのステータス テーブルについて

ゾーンのステータス テーブルでは、ゾーンの現在の動作に関する情報が提供されます。このテーブルには次の情報が含まれています。

- Active Dynamic filters：アクティブになっている動的フィルタの数。Detector モジュールがゾーンのトラフィックに異常を検出した場合、アクティブな動的フィルタの数は 1 より大きくなります。

  Dynamic Filters 画面を表示するには、**Active Dynamic filters** をクリックします。動的フィルタの使用の詳細については、第 9 章「異常の検出のアクティブ化」の「動的フィルタの管理」の項を参照してください。

- Pending dynamic filters：保留動的フィルタの数。保留動的フィルタの数は、ゾーンがインタラクティブ検出モードになっていて新しい推奨事項がある場合は、1 より大きくなります。

  Recommendations 画面を表示するには、**Pending Dynamic filters** をクリックします。Detector モジュールの推奨事項の詳細については、第 9 章「異常の検出のアクティブ化」の「動的フィルタに対する Detector モジュールの推奨事項の管理」の項を参照してください。

- Last attack time：ゾーンが最後に攻撃を受けた日時。
- Activation time：ゾーンの異常の検出がアクティブになった日時。

ゾーンの最近のイベント テーブルについて

最近のイベント テーブルには、*notify* 以上の重大度を持つ、報告されるゾーン イベントが表示されます。また、Detector モジュールは、ゾーンのイベント ログおよび Detector モジュールのイベント ログにもイベントを記録します。

ゾーンの診断ツールの使用

Detector モジュールでは、ゾーン イベントの監視およびトラブルシューティングに役立つ診断情報が提供されます。この項は、次の内容で構成されています。

ゾーンのカウンタの表示

ゾーンのカウンタを利用すると、ゾーン固有のトラフィック情報を分析してゾーンのステータスを確認し、ゾーンの異常の検出が適切に機能しているかどうかを判断できます。ゾーンのカウンタのグラフ表示の期間を変更すると、ゾーン保護がどのように進行しているかを確認できます。

ゾーンのカウンタ情報を表示するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューで、**Diagnostics > Counters > Zone Counters** を選択します。ゾーンの Counters 画面が表示されます。

ステップ 3　（オプション）グラフに表示する期間を変更します。Graph Period ドロップダウン リストで期間を選択し、**Update Graph** をクリックします。Detector モジュールにより、グラフがアップデートされます。

デフォルトでは、トラフィック レートのグラフには、最近 2 時間に記録したカウンタ情報が表示されます。

ステップ 4　（オプション）トラフィック レートのグラフで Detector モジュールが使用する測定単位を変更するには、Graph Type ドロップダウン リストで測定単位を選択します。

- **pps**：パケット / 秒
- **bps**：ビット / 秒

ステップ 5　**Update Graph** をクリックします。Detector モジュールにより、グラフがアップデートされます。

ステップ 6　（オプション）Detector モジュールのカウンタをクリアするには、**Clear Counters** をクリックします。Detector モジュールが現在のカウンタとトラフィック レートをクリアします。カウンタにテスト セッションの情報だけが含まれるようにテストを実行する場合は、ゾーンのカウンタをクリアできます。

Zone Current Counters/Rates テーブルには、次の情報が表示されます。

- Packets：Detector モジュールが最後にリロードされた後に、ゾーンが宛先として指定されたパケットの総数。
- Bits：Detector モジュールが最後にリロードされた後に、ゾーンが宛先として指定されたビットの総数。
- pps：ゾーンが宛先となっているトラフィックの現在のレート（パケット / 秒単位）。
- bps：ゾーンが宛先となっているトラフィックの現在のレート（ビット / 秒単位）。

トラフィック レートのグラフの下には、カウンタを識別するための凡例が表示されます。また、選択した期間における各カウンタの最小レート、最大レート、および平均レートが表示されます。

トラフィック フローを分析するためのゾーンのカウンタの使用

トラフィックがアクティブなゾーンに適切に送信されているかどうかを判断するには、トラフィック フローの分析が重要です。次の情報では、トラフィック フローの分析方法、発生する可能性のある問題の認識方法、およびその解決策について説明しています。

- 受信パケットの数が 0 より大きい場合は、トラフィック フローがゾーンに適切に送信されていることを示します。
- 受信パケットの数が 0 の場合は、次の状況のいずれかに該当している可能性があります。
  - Detector モジュールまたは他のゾーンで受信したパケットの現在のレート（pps または bps）も 0 の場合は、トラフィックのキャプチャの設定に問題があるか、1 つまたは複数のゾーンが宛先となっているトラフィックが Detector モジュールがインストールされたスイッチまたはルータに到達する前にブロックされている可能性があります。
  - Detector モジュールまたは他のゾーンで受信したパケットの現在のレート（pps または bps）が 0 より大きい場合は、ゾーンにバイパス フィルタが定義されていないことを確認してください。

ゾーンのカウンタのクリア

カウンタにテスト セッションの情報だけが含まれるようにテストを実行する場合は、ゾーンのカウンタをクリアできます。

ゾーンのカウンタをクリアするには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューで、**Diagnostics > Counters > Zone Counters** を選択します。ゾーンの Counters 画面が表示されます。

ステップ 3　**Clear Counters** をクリックします。Detector モジュールが現在のゾーンのカウンタとトラフィック レートをクリアします。

ゾーンのカウンタのリアルタイムでの表示

Detector モジュールでは、ゾーンのカウンタ情報をリアルタイムで表示できます。

（注）　カウンタ情報をリアルタイムに表示するには、クライアントに JRE をインストールしておく必要があります（第 1 章「製品の概要」の「Java 2 Runtime Environment のインストール」の項を参照）。

ゾーンのカウンタ情報をリアルタイムに表示するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューで、**Diagnostics > Counters > Real Time Counters** を選択します。ゾーンの Real time counters/Rates 画面が表示されます。

ステップ 3　（オプション）トラフィック レートのグラフで Detector モジュールが使用する測定単位を変更するには、次のいずれかの Graph Type オプションを選択します。

- **bps**：ビット / 秒
- **pps**：パケット / 秒

Detector モジュールにより、トラフィック レートのグラフがアップデートされます。

ゾーン トラフィックを分析するためのカウンタ情報の使用については、「トラフィック フローを分析するためのゾーンのカウンタの使用」の項を参照してください。

ゾーンのイベント ログの表示

Detector モジュールは、システム アクティビティとイベントを自動的に記録します。Detector モジュールのログを表示して、Detector モジュールのアクティビティを確認および追跡できます。

ゾーンのイベント ログの内容を表示するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューで、**Diagnostics > Event log** を選択します。ゾーンの Events 画面が表示されます。

ステップ 3　（オプション）次のオプションのいずれかを選択し、イベント テーブルに表示するイベントを制御します。

- **Show all Events**：各重大度レベルのイベントを表示します（使用可能なイベントのレベルのリストは表 10-4 を参照）。
- **Show events with severity level**：選択した重大度レベルのイベントだけを表示します。

ステップ 4　**Filter Events** をクリックします。Detector モジュールにより、イベント テーブルがアップデートされます。

攻撃の要約レポートの表示

Detector モジュールでは、ゾーンで Detector モジュールが検出した攻撃を分析できるようにするために、ゾーンごとの高レベルな要約レポートを提供しています。このレポートは、ユーザが定義した期間中にゾーンが受けた DDoS 攻撃を要約したものです。Detector モジュールは、攻撃の進行中に情報を記録し、そのデータをカテゴリ別に編成します。このレポートには、攻撃の総数および強さに関する詳細、および各攻撃の簡単な要約が示されます。Detector モジュールは、攻撃のデータをグラフ形式でも表示します。

ゾーン攻撃の要約レポートを表示するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューで、**Diagnostics > Attack Reports > Attack Summary** を選択します。Attacks Summary 画面が表示されます。デフォルトでは、レポートに先月分の攻撃情報が表示されます。

ステップ 3　(オプション）攻撃レポートの期間を変更します。表示する期間の日付を **Period from** および **to** に入力し、**Get Reports** をクリックします。日付は手動で入力することも、各フィールドの右側にあるカレンダー アイコンをクリックし、カレンダー ポップアップ ウィンドウから選択することもできます。

Attack Summary Report 画面は、次の領域で構成されています。

- 検出のグラフ：ユーザが定義した期間中に発生した攻撃の要約がグラフ形式で提示されます。

図 10-3　ゾーンでの検出の要約レポート：検出のグラフ

X 軸は、攻撃が発生した期間を表示しています。Y 軸は、平均の攻撃レートをパケット / 秒（pps）単位で表示しています。各攻撃は 1 つのバーで表されています。マウス カーソルをいずれかの攻撃バーの上に数秒間置いておくと、平均の攻撃レートが表示されます。

攻撃の詳細を表示するには、グラフで攻撃バーをクリックし、攻撃レポートを開きます（「攻撃レポートの詳細の表示」の項を参照）。

- 攻撃に関する統計情報のテーブル：ゾーンに対する攻撃の数、およびユーザが定義した期間中に発生した攻撃の集計情報が示されます。

  表 10-7 に、攻撃に関する統計情報のテーブルに含まれるフィールドの説明を示します。

表 10-7　攻撃に関する統計情報のテーブルに含まれているフィールドの説明

フィールド	説明
Attacks Detected	検出された攻撃の数。
Attacks Duration	検出された攻撃の持続期間の集計。
Max. Traffic Rate	ゾーンが宛先となっていたトラフィックの最大レート。
Total Rx	ゾーンが宛先となっていたトラフィックの合計レート。

- 攻撃ごとの要約テーブル：定義した期間中にゾーンが受けた DDoS 攻撃のリストがテーブルで示されます。攻撃ごとの要約テーブルに現在表示されている情報を削除（「攻撃レポートの削除」の項を参照）、または攻撃レポートの内容をエクスポート（「攻撃レポートのエクスポート」の項を参照）できます。

  表 10-8 に、攻撃ごとの要約テーブルのカラムに含まれるフィールドの説明を示します。

表 10-8　要約レポートに含まれるフィールドの説明

フィールド	説明
#	検出された攻撃の識別番号（ID）。Detector モジュールは、進行中の攻撃に *Curr* という値を表示します。
Start time	検出された攻撃の発生日時。
Duration	検出された攻撃の持続期間（時、分、および秒）。
Type	検出された攻撃のタイプ。表示される値は次のいずれかです。 • Tcp connections：データを保持している（または保持していない）、異常な数の TCP 同時接続が検出されたフロー。 • HTTP：異常な HTTP トラフィック フロー。 • Tcp incoming：ゾーンがサーバである場合に、TCP サービスへの攻撃が検出されたフロー。 • Tcp outgoing：ゾーンがクライアントである場合に、ゾーンが開始した接続に対する SYN-ACK 攻撃など、クライアントがゾーンであるように見える検出済み攻撃フロー。 • Unauthenticated tcp：Detector のスプーフィング防止機能が認証できなかった検出済みフロー。たとえば、ACK フラッド、FIN フラッド、その他の未認証パケットによるフラッドなどです。 • DNS (UDP)：攻撃的な DNS-UDP プロトコル フロー。 • DNS (TCP)：攻撃的な DNS-TCP プロトコル フロー。 • UDP：攻撃的な UDP プロトコル フロー。 • Non tcp/udp protocols：TCP/UDP 以外の攻撃的なプロトコル フロー。 • Fragments：異常な量の断片化トラフィックが検出されたフロー。 • Hybrid：特性の異なる複数の攻撃で構成された攻撃。 • IP scan：送信元 IP アドレスが、ゾーンの多数の宛先 IP アドレスにアクセスしようとして開始した検出済みフロー。 • port scan：送信元 IP アドレスが、ゾーンの多数のポートにアクセスしようとして開始した検出済みフロー。 • user detected：ユーザ定義によって検出された異常フロー。 • worm_tcp：TCP/IP プロトコルを介したワーム攻撃。
Peak (pps)	攻撃レートの最大値（パケット / 秒単位）。
Received Pkts	攻撃進行中に Detector モジュールが処理した、ゾーンが宛先となっていたパケットの総数。

（注） 攻撃の詳細を表示するには、攻撃ごとの要約テーブルのいずれかの行をクリックします（「攻撃レポートの詳細の表示」の項を参照）。

攻撃レポートの詳細の表示

Detector モジュールでは、Attacks Summary 画面に一覧表示される攻撃レポートの詳細を表示できます。攻撃レポートには、最初の動的フィルタが作成された時点からユーザによる指示があるまで、または新しい動的フィルタが追加されないように定義された期間が終了するまでの、攻撃の詳細が示されています。

Detector モジュールは、攻撃の進行中に情報を記録し、そのデータをカテゴリ別に編成します。過去および現在の攻撃の詳細を表示できます。

攻撃レポートを表示するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューで、**Diagnostics > Attack Reports > Attack Summary** を選択します。Attacks Summary 画面が表示されます。

ステップ 3　（オプション）攻撃レポートの期間を変更するには、表示する期間の日付を **Period from** および **to** に入力し、**Get Reports** をクリックします。日付は手動で入力することも、各フィールドの右側にあるカレンダー アイコンをクリックし、カレンダー ポップアップ ウィンドウから選択することもできます。

ステップ 4　検出グラフで攻撃バーをクリックします。Attack Report 画面が表示されます。

攻撃ごとの要約テーブルに含まれている、攻撃のいずれかのフィールドもクリックできます。

Detector モジュールは、進行中の攻撃の識別番号（#）に *Curr* という値を表示します。

ゾーンへの攻撃が進行中である場合、Detector モジュールでは、攻撃を受けているゾーンのステータス画面に、Report ボタンが表示されます。**Report** ボタンをクリックすると、Detector モジュールが現在の攻撃に関して収集している情報が表示されます。

攻撃レポートの詳細について

攻撃レポートには、次のセクションにまとめられたデータ フィールドとデータ テーブルがあります。

- 一般的な攻撃情報
- 攻撃に関する統計情報
- 検出された異常

一般的な攻撃情報

攻撃レポートの最初のセクションには、攻撃の日時に関する情報（攻撃の開始日時、終了日時、および持続期間を含む）が示されます。

レポートの詳細を表示するには、**i** または **Show details for all events** をクリックします。

カウンタは、レートを除いてすべて整数値です。画面の一般的な攻撃情報領域から、統計情報の測定単位を選択することができます。

統計情報の測定単位を変更するには、次の手順を実行します。

ステップ 1　Statistics units ドロップダウン リストから、使用する目的の単位を選択します。

ステップ 2　**Set units** をクリックします。Detector モジュールにより、表示がアップデートされます。

攻撃に関する統計情報

攻撃に関する統計情報には、受信したパケットに関する情報が示されます。

表 10-9 に、攻撃に関する統計情報について提供される情報の説明を示します。

表 10-9　攻撃に関する統計情報

フィールド	説明
Total	このカテゴリに該当するパケットの総数。
Max Rate	測定されたパケット レートの最大値。
Average Rate	パケット レートの平均値。

トラフィック レートは、一般的な攻撃領域のドロップダウン リストで選択した単位で表示されます（「一般的な攻撃情報」の項を参照）。

検出された異常

検出された異常のテーブルには、Detector モジュールがゾーンのトラフィックで検出した異常の詳細が示されます。動的フィルタの生成が必要となった場合、Detector モジュールはトラフィックを異常があるものと分類します。このような異常はあまり発生しないか、または体系的な DDoS 攻撃となる可能性があります。Detector モジュールでは、タイプとフロー パラメータ（送信元 IP アドレスまたは宛先ポートなど）が同じトラフィック異常を 1 つのトラフィック異常タイプとしてまとめます。

表 10-10 に、それぞれの異常について、提供される情報の説明を示します。

表 10-10　検出された異常に含まれるフィールドの説明

フィールド	説明
#	検出された異常の識別番号（ID）。
Start time	異常を検出した日時。
Duration	異常の持続期間（時、分、および秒）。

表 10-10　検出された異常に含まれるフィールドの説明（続き）

フィールド	説明
Type	検出した異常のタイプ。表示される値は次のいずれかです。 • Tcp_connections：データを保持している（または保持していない）、異常な数の TCP 同時接続が検出されたフロー。 • HTTP：異常な HTTP トラフィック フロー。 • Tcp incoming：ゾーンがサーバである場合に、TCP サービスへの攻撃が検出されたフロー。 • Tcp outgoing：ゾーンがクライアントである場合に、ゾーンが開始した接続に対する SYN-ACK 攻撃など、クライアントがゾーンであるように見える検出済み攻撃フロー。 • Unauthenticated tcp：Detector モジュールのスプーフィング防止機能が認証できなかった検出済みフロー。たとえば、ACK フラッド、FIN フラッド、その他の未認証パケットによるフラッドなどです。 • DNS (UDP)：攻撃的な DNS-UDP プロトコル フロー。 • DNS (TCP)：攻撃的な DNS-TCP プロトコル フロー。 • UDP：攻撃的な UDP プロトコル フロー。 • Non tcp/udp protocols：TCP/UDP 以外の攻撃的なプロトコル フロー。 • Fragments：異常な量の断片化トラフィックが検出されたフロー。 • TCP ratio：各種の TCP パケット（FIN/RST パケットではなく SYN パケットなど）の比率に異常がある検出済みフロー。 • IP scan：送信元 IP アドレスが、ゾーンの多数の宛先 IP アドレスにアクセスしようとして開始した検出済みフロー。 • port scan：送信元 IP アドレスが、ゾーンの多数のポートにアクセスしようとして開始した検出済みフロー。 • user detected：ユーザ定義によって検出された異常フロー。 • worm_tcp：TCP/IP プロトコルを介したワーム攻撃。
Triggering rate	ポリシーのしきい値を超過した異常トラフィックのレート。
% Threshold	ポリシーのしきい値をトリガー レートが上回った割合。
Anomaly Flow	異常なトラフィック フロー。このフローに共通する特性のパラメータが表示されます。この情報には、異常トラフィックのプロトコル番号、トラフィック フローの宛先 IP アドレス、フローのパケット タイプなどのパラメータが含まれています。 異常フローが特定のポートで発生している場合は、dst=*ip address:port* と表示されます。
Details	このフィルタに関する追加情報を表示できるかどうかを示します。**i** をクリックすると、追加情報が表示されます（「検出された異常の詳細の表示」の項を参照）。

パラメータの値がアスタリスク（*）となっている場合は、ワイルドカードとして使用されており、次のいずれかの状態であることを示します。

- 値が特定されていない。
- 異常なパラメータに対して複数の値が測定されている。

任意のパラメータにシャープ記号（#）とそれに続く数字を使用すると、そのパラメータのために測定された値の数を表します。

検出された異常の詳細の表示

検出された異常の詳細のテーブルには、検出された異常に関連する動的フィルタについての追加情報が示されます。

検出された異常の詳細のテーブルを表示するには、検出された異常のテーブルで、トラフィック異常の Details カラムにある **i** をクリックします。

表 10-11 に、Detector モジュールが提供する異常の詳細情報の説明を示します。

表 10-11　検出された異常の詳細に含まれるフィールドの説明

フィールド	説明
Start time	異常を検出した日時。
End time	動的フィルタの満了日時。
Rate (pps)	レート（パケット / 秒単位）。 • Thresh：検出された異常が超過したポリシーのしきい値を示します。 • Triggered：ポリシーのしきい値を超過した異常トラフィックのレートを示します。
Count	動的フィルタが処理したパケットの数。
Detected flow	検出され、動的フィルタの作成原因となった攻撃フローについて、次の情報を示します。 • Prot.：プロトコル番号。 • Src IP：送信元 IP アドレス。 • Src Port：送信元ポート番号。 • Dst IP：宛先 IP アドレス。 • Dst Port：宛先ポート番号。 • frag.：検出されたトラフィック フローの断片化特性。 • Type：検出された異常のタイプ。
Action flow	動的フィルタによって処理されたアクション フローに関する情報。アクション フローは、検出されたフローよりも範囲が広い可能性があります。たとえば、検出されたフローは、特定の送信元 IP の特定の送信元ポートを示すことがあります。アクション フローは、特定の送信元 IP のすべての送信元ポートを示すことがあります。このカラムは、動的フィルタのトラフィック データを表しています。 • Prot.：プロトコル番号。 • Src IP：送信元 IP アドレス。 • Src Port：送信元ポート番号。 • Dst IP：宛先 IP アドレス。 • Dst Port：宛先ポート番号。 • frag.：アクション フローの断片化特性。

攻撃レポートのエクスポート

攻撃レポートをネットワーク サーバにエクスポートするには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューの **Diagnostics > Attack Reports > Attack Summary** を選択します。Attacks Summary 画面が表示されます。

ステップ 3　（オプション）攻撃レポートの期間を変更するには、**Period from** および **to** に日付を入力し、**Get Reports** をクリックします。日付は手動で入力することも、各フィールドの右側にあるカレンダー アイコンをクリックして選択することもできます。

ステップ 4　攻撃ごとの要約テーブルで、エクスポートする攻撃レポートの隣にあるチェックボックスをオンにします。テーブルに表示されているレポートをすべて選択するには、番号記号（#）の隣にあるテーブルのヘッダーのチェックボックスをオンにします。

ステップ 5　**Export** をクリックします。Export File Server Parameters ウィンドウが表示されます。

ステップ 6　Select File Server Parameters フォームで、次のいずれかのオプションから使用するネットワーク サーバを選択して定義します。

- **Use automatic export file server definitions**：CLI コマンド export reports を使用して、Detector モジュールの設定で定義したネットワーク サーバに攻撃レポートをエクスポートします。
- **Use the following server definition**：定義したネットワーク サーバに攻撃レポートをエクスポートします。ネットワーク サーバに関する次の情報を入力します。
  - **Transfer method**：Detector モジュールは、攻撃レポートのエクスポートでのみ File Transfer Protocol（FTP; ファイル転送プロトコル）方式をサポートします。
  - **Address**：ネットワーク サーバの IP アドレス。
  - **Path**：完全パス名。パスを指定しない場合、サーバはユーザのホーム ディレクトリに 1 つ以上のファイルを保存します。
  - **Username**：ネットワーク サーバのログイン名。サーバのログイン名。FTP サーバを定義する場合、username 引数はオプションです。ログイン名を入力しない場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
  - **Password**：（オプション）リモート FTP サーバのパスワード。ユーザ名を入力してパスワードを入力しなかった場合、パスワードを入力するように Detector モジュールから求められます。

ステップ 7　**OK** をクリックして、攻撃レポートをネットワーク サーバにエクスポートします。

攻撃レポートの削除

攻撃レポートを削除するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューの **Diagnostics > Attack Reports > Attack Summary** を選択します。Attacks Summary 画面が表示されます。

ステップ 3　（オプション）攻撃レポートの期間を変更するには、**Period from** および **to** に日付を入力し、**Get Reports** をクリックします。日付は手動で入力することも、各フィールドの右側にあるカレンダー アイコンをクリックして選択することもできます。

ステップ 4　攻撃ごとの要約テーブルで、削除する攻撃レポートの隣にあるチェックボックスをオンにします。テーブルに表示されているレポートをすべて選択するには、番号記号（#）の隣にあるテーブルのヘッダーのチェックボックスをオンにします。

ステップ 5　**Delete** をクリックします。Detector モジュールが攻撃レポートを削除します。

ポリシーの統計情報のテーブルの表示

ポリシーの統計情報のテーブルを使用すると、特定のゾーンの各ポリシーを通過するトラフィック フローのレートを表示できます。このテーブルを使用して、正当なトラフィックのみがゾーンに送信されているかどうかを判断して、しきい値を手動で調整できます。

ポリシーの統計情報のテーブルを表示するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューで **Diagnostics > Statistics > Policy Statistics** を選択します。Policies Statistics 画面が表示されます。

ステップ 3　（オプション）表示する情報を次の手順でフィルタリングします。

a. **Set Screen Filter** をクリックします。Policy Filter ウィンドウが表示されます。
b. Policy Filter ウィンドウのドロップダウン リストから、パラメータの値を選択します。
c. **OK** をクリックします。Policy statistics 画面がアップデートされ、選択したパラメータだけが表示されます。選択したパス、およびポリシーごとの最大キーの詳細が Screen Filter フレームに表示されます。

ポリシーの統計情報のテーブルでは、4 つのセクションに情報が表示されます。各セクションの情報は値に基づいてソートされ、最も大きい値が最上部に表示されます。

- Rate：ポリシーを通過するトラフィック フローのレート。
- Ratio：SYN　フラグ付きパケット数と　FIN/RST　フラグ付きパケット数の比率。この情報は、syn_by_fin ポリシーについてのみ表示されます。
- Connections：同時接続または送信元 IP アドレスの数。この情報は、tcp_connections ポリシーおよび in_nodata_conns について表示されます。
- Dst IPs：スキャンされたゾーン宛先 IP アドレスの数。この情報は、worm_tcp ポリシーについて表示されます。

表示された情報の管理を容易にするには、画面フィルタを設定して、利用可能な統計情報のリストの一部のみを表示するようにします。

（注）　いずれかの表示パラメータを変更すると、Detector モジュールは、変更したパラメータの下に表示されているパラメータをすべて自動的に消去します。消去されたパラメータに対して新しい値を入力する必要があります。

表 10-12 に、ポリシーの統計情報に含まれるフィールドの説明を示します。

表 10-12　ポリシーの統計情報

フィールド	説明
Policy template	ポリシーの構築に使用されたポリシー テンプレート。
Service	ポリシーが関連しているサービス。
Level	トラフィック フローの処理に使用されたレベル。
Type	パケット タイプ。表示される値は次のいずれかです。 • auth_pkts：TCP ハンドシェイクまたは UDP 認証を受けたパケット。 • in_nodata_conns：ゾーンへの着信接続のうち、接続時にデータ転送が行われないもの（データ ペイロードのないパケット）。 • in_pkts：ゾーンに着信する DNS クエリー パケット。 • in_unauth_pkts：ゾーンに着信する未認証の DNS クエリー。 • non_estb_conns：不完全な接続。失敗したゾーン着信接続。要求に対する応答がなかった TCP 接続要求（SYN パケット）。 • out_pkts：ゾーンに着信する DNS 応答パケット。 • reqs：データ ペイロードを含んだ要求パケット。 • syns：同期パケット。つまり、TCP SYN フラグの付いたパケット。 • syn_by_fin：SYN フラグ付きパケットと FIN フラグ付きパケット。SYN フラグの付いたパケット数と FIN フラグの付いたパケット数の比率を確認します。 • unauth_pkts：TCP ハンドシェイクを受けていないパケット。 • pkts：同じ保護レベルになっている他のいずれのカテゴリにも該当しない、すべてのパケット タイプ。
Policy	ポリシー識別子。

表 10-12　ポリシーの統計情報（続き）

フィールド	説明
Key	ポリシーの集計に使用されたキー（トラフィックの特性）。 ワームに関連するポリシーでは、キーは、ゾーンのネットワーク アドレスをスキャンする送信元 IP アドレス、コロン、およびスキャンされる宛先ポートで構成されます。たとえば、192.128.100.3:70 となります。 表示される値は次のいずれかです。 • dst_ip：ゾーンの IP アドレスが宛先となっているトラフィック。 • dst_ip_ratio：特定の IP アドレスが宛先となっている SYN フラグ付きパケットと FIN フラグ付きパケットの比率。 • dst_port_ratio：特定のポートが宛先となっている SYN フラグ付きパケットと FIN フラグ付きパケットの比率。 • global：他のポリシー　セクションによって定義された、すべてのトラフィック フローの合計。 • src_ip：送信元 IP アドレスに基づいて集約された、ゾーンが宛先となっているトラフィック。 • dst_port：ゾーンの特定のポートが宛先となっているトラフィック。 • protocol：プロトコルに基づいて集計された、ゾーンが宛先となっているトラフィック。 • src_ip_many_dst_ips：IP スキャニングに使用されるキー。1 つの IP アドレスから多くのゾーン IP アドレスに宛てたトラフィックです。 • src_ip_many_port：ポート スキャニングに使用されるキー。1 つの IP アドレスから多くのゾーンのポートに宛てたトラフィックです。 • scanners：特定の宛先ポート上でゾーンの宛先 IP アドレスをスキャンする送信元 IP アドレスのヒストグラム。
Value	接続のレート、比率、または数。テーブルのセクションに応じて異なります。各セクションの情報は値に基づいてソートされ、最も大きい値が最初に表示されます。