CHAPTER 10

Guard およびゾーンの動作の監視

この章では、Cisco Guard（Guard）とそのゾーンのステータスを監視するためのタスクを実行する方法、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できる統計ツール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。

Guard 要約画面の表示

Guard 要約画面（図 10-1 を参照）には、現在の Guard のアクティビティに関する要約が示されます。この画面は、Guard の WBM に接続するときに最初に表示されます。Guard 要約画面には、インターフェイス内の次の場所からアクセスできます。

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

図 10-1　Guard 要約画面

Guard 要約画面には、次の 2 つの領域があります。

- Guard Summary：最近 2 時間に Guard が処理したトラフィックの要約をビット / 秒（bps）単位でグラフに示します。保護されているゾーンに Guard が転送した正当なトラフィックは、緑色で表示されます。Guard が検出した悪意のあるトラフィックは、赤色で表示されます。

  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　Guard 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）。

  この情報は、正当なトラフィックと悪意のあるトラフィックに分けて表示されます。

- Currently Protected Zones：Guard が現在保護しているゾーンのステータス情報。ゾーン情報は、次のゾーン保護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。
  - Protect：ゾーンが攻撃を受けていて、通常のトラフィック状態にあるときにゾーン情報を表示します。
  - Protect 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。

Guard 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）。Guard が各行に表示する情報をクリックすると、関連するゾーンの要約画面を表示できます。

表 10-2 に、現時点で保護されているゾーンに含まれるフィールドの説明を示します。

表 10-2　現時点で保護されているゾーンに含まれ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。Guard 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。
Legitimate Rate	Guard がゾーンに転送した正当なトラフィックの現時点でのレート（bps 単位）。
Malicious Rate	ゾーンをターゲットとした悪意のあるトラフィックの現時点でのレート（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。正当なトラフィックのレートは緑色で表示されます。悪意のあるトラフィックのレートは赤色で表示されます。

Guard のグローバル診断ツールの使用

Guard 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、Guard が Guard 要約画面に表示するカウンタ情報の詳細な分析が表示されます。Counters 画面では、Guard 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。

Guard 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 **Guard Summary** をクリックします。Guard の要約メニューが表示されます。

ステップ 2　Guard 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、グラフには最近 2 時間の正当なトラフィックと悪意のあるトラフィックが bps 単位で表示されます。

ステップ 3　（オプション）トラフィック レートのグラフに Guard が表示するカウンタ情報を追加する場合、対象のカウンタの隣にあるチェックボックスをオンにします。グラフからカウンタ情報を削除する場合、対象のカウンタの隣にあるチェックボックスをオフにします。

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

Guard は、次のトラフィック カウンタを表示できます。

- Legitimate：Guard がゾーンに転送した正当なトラフィック。
- Malicious：ゾーンを宛先とする悪意のあるトラフィック。悪意のあるトラフィックは、ドロップされたパケットとスプーフィング パケット（ここにはゾンビ パケットも含まれます）の合計です。
- Received：Guard が受信して処理したパケット。受信されたパケットは、正当なトラフィックと悪意のあるトラフィックの合計です。
- Dropped：Guard が攻撃の一部と見なし、ドロップしたパケット。
- Replied：正当なトラフィックの一部であるか攻撃の一部であるかを確認するために、スプーフィング防止機能またはゾンビ防止機能による処理の一環として、開始側のクライアントに応答が送信されたパケット。
- Spoofed：Guard によってスプーフィング パケットと見なされ、ゾーンに転送されなかったパケット。スプーフィング パケットは、応答された（返送された）パケットのうち、応答を受信しなかったパケットです。スプーフィング パケットにはゾンビ パケットが含まれます。

ステップ 5　（オプション）グラフに表示する情報の対象期間を変更するには、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。Guard 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 6　（オプション）トラフィック レートのグラフで Guard 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、**Update Graph** をクリックします。Guard により、グラフがアップデートされます。

測定単位は次のいずれかです。

- pps：パケット / 秒
- bps：ビット / 秒

ステップ 7　（オプション）Guard のカウンタをクリアするには、**Clear Counters** をクリックします。

Guard 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、Guard のカウンタをクリアできます。

表 10-3 に、各カウンタに含まれるフィールドの説明を示します。

表 10-3　カウンタ レポートに含まれるカウンタのフィールドの説明

フィールド	説明
Shown in Graph	トラフィック レートのグラフに表示されるカウンタ情報のタイプ。
Packets	Guard がリロードされた後のパケットの総数。
Bits	Guard 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（ビット / 秒単位）。

グラフの下には、さまざまな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。

Guard 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、Guard のカウンタをクリアできます。

Guard 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 **Guard Summary** をクリックします。Guard の要約メニューが表示されます。

ステップ 2　Guard の要約メニューで、**Diagnostics > Counters > Device Counters** を選択します。Guard 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。Guard 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。

Guard のカウンタのリアルタイムでの表示

Guard では、グローバル カウンタ情報をリアルタイムに表示できます。

（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 Java 2 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 **Guard Summary** をクリックします。Guard の要約メニューが表示されます。

ステップ 2　Guard 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 レートのグラフの表示を変更する場合は、表示するトラフィック カウンタのタイプ（Show in Graph の下）の隣にあるチェックボックスをオンにします。Guard 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。

Guard は、次のトラフィック カウンタを表示できます。

- Legitimate：Guard がゾーンに転送した正当なトラフィック。
- Malicious：ゾーンを宛先とする悪意のあるトラフィック。悪意のあるトラフィックは、ドロップされたパケットとスプーフィング パケット（ここにはゾンビ パケットも含まれます）の合計です。
- Received：Guard が受信して処理したパケット。受信されたパケットは、正当なトラフィックと悪意のあるトラフィックの合計です。
- Dropped：Guard が攻撃の一部と見なし、ドロップしたパケット。
- Replied：正当なトラフィックの一部であるか攻撃の一部であるかを確認するために、スプーフィング防止メカニズムまたはゾンビ防止メカニズムによる処理の一環として、開始側のクライアントに応答が送信されたパケット。
- Spoofed：Guard によってスプーフィング パケットと見なされ、ゾーンに転送されなかったパケット。スプーフィング パケットは、応答された（返送された）パケットのうち、応答を受信しなかったパケットです。スプーフィング パケットにはゾンビ パケットが含まれます。

ステップ 4　（オプション）トラフィック レートのグラフで Guard 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。

- pps：パケット / 秒
- bps：ビット / 秒

Guard 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。

表 10-4 に、リアルタイム カウンタに含まれるフィールドの説明を示します。

表 10-4　リアルタイム カウンタに含まれるフィールドの説明

フィールド	説明
Shown in Graph	トラフィック レートのグラフに表示されるカウンタ情報のタイプ。
Packets	Guard が再びアクティブにされた後のパケットの総数。
Bits	Guard が再びアクティブに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（ビット / 秒単位）。

Guard イベント ログの表示

Guard は、保護されているゾーンおよび Guard 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。Guard のログを表示して、Guard のアクティビティを確認および追跡できます。

表 10-5 に、イベントの重大度レベルの説明を示します。

表 10-5　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 **Guard Summary** をクリックします。Guard の要約メニューが表示されます。

ステップ 2　Guard 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）イベント テーブルに表示するイベントを制御するには、次のオプションのいずれかを選択します。

- **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 10-5 を参照）。

ステップ 4　**Filter Events** をクリックします。

Guard 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

Guard 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。

Guard 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 ペインの **Guard Summary** をクリックします。Guard の要約メニューが表示されます。

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

表 10-6 に、Device Resources 画面に含まれるフィールドの説明を示します。

表 10-6　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。
Host CPU2	CPU2 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。
Disk space usage	Guard が使用している割り当て済みディスク スペースの割合。 ディスク 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、Guard 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。 ディスク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、Guard 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。 Guard 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。 ディスク 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）。

表 10-6　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 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、Guard は SNMP トラップを生成します。大きな値は、Guard 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。
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、Guard は SNMP トラップを生成します。大きな値は、Guard 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。
Top proxy usage	使用しているプロキシ ポートの割合。詳細については、「ゾーンのプロキシ使用率の表示」の項を参照してください。
Anomaly detection engine used memory	Guard 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、Guard 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。Guard は、アクティブな動的フィルタの数と、Guard 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、Guard 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、Guard 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、Guard 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	Guard 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。
- ゾーン保護が現在イネーブルの場合は、ナビゲーション ペインの **Protected Zones** 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（**Guard Summary > Zones > Zone list**）から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。次の各項で、この画面について説明します。

- ゾーンのステータス画面の機能ボタンについて
- 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の機能ボタンについて

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。

- Protect & Learn : ゾーンの Protect and Learn 機能をアクティブにします。Protect and Learn 機能を使用すると、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、ゾーンを保護することができます。この機能は、ゾーンのメイン メニューで **Protection > Protect** を選択し、**Learning > Tune Thresholds** を選択するのと同じです（順序は重要でありません）。

- Protect : ゾーン保護をアクティブにします。この機能は、ゾーンのメイン メニューで **Protection > Protect** を選択するのと同じです。

ゾーン保護または Protect 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。これは、ゾーンのメイン メニューで **Protection > Deactivate** を選択するのと同じ操作です。

  Protect and Learn 機能がイネーブルの場合、**Deactivate** をクリックすると、ゾーン保護、ラーニング プロセス、またはその両方の動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。この機能は、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、「現在の攻撃の詳細表示」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。
- Guard がゾーン保護を実行する方法 : Guard がゾーンに対して自動保護モードで動作するか、インタラクティブ保護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、「自動およびインタラクティブ ゾーン動作モード」および「自動保護モードまたはインタラクティブ保護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です。動作状態は、Protected、Protected/Tuning Thresholds、Inactive、Constructing Policy、または Tuning Thresholds のいずれかです。
- 新しい推奨事項の通知：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、ゾーンに関連する最近 2 時間のトラフィック レートが bps 単位で表示されます。Guard がゾーンに転送した正当なトラフィックは、緑色で表示されます。ゾーンがターゲットとなっていた、Guard がドロップした悪意のあるトラフィックは、赤色で表示されます。

表 10-7 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 10-7　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 テーブルは、ゾーンの現在の動作に関する情報を提供し、次の情報を示します。

- Active Dynamic filters：アクティブになっている動的フィルタの数。Guard 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。動的フィルタの詳細については、第 9 章「ゾーン保護のアクティブ化」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保護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。動的フィルタの詳細については、第 9 章「ゾーン保護のアクティブ化」の「動的フィルタの管理」の項を参照してください。Guard の推奨事項の詳細については、第 9 章「ゾーン保護のアクティブ化」の「動的フィルタに関する Guard の推奨事項の管理」の項を参照してください。
- Proxy usage：Guard が使用しているプロキシ ポートの割合。詳細については、「ゾーンのプロキシ使用率の表示」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：ゾーン保護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。Guard は、イベントをゾーンのイベント ログと Guard イベント ログにも記録します。

ゾーンの診断ツールの使用

Guard 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。

ゾーンのプロキシ使用率の表示

Guard は、ゾーンごとにプロキシ使用率を監視します。Guard は、TCP の強化認証プロセスおよび DNS 認証プロセスでプロキシ IP アドレスを使用します。Guard がこれらのプロセスを実行する能力は、プロキシ単位で制限されている TCP ポートの数によって制限されます。使用可能なプロキシ ポートがないと、Guard は新しい接続を認証して開くことができなくなり、結果的に接続はドロップされます。この問題を防ぐため、1 つのゾーンまたはすべてのアクティブなゾーンが使用しているプロキシ ポートの割合を監視することができます。

プロキシ使用率を表示するには、次の項を参照してください。

- デバイス リソースの監視：すべてのアクティブなゾーンのプロキシ使用率を表示します。
- ゾーンのステータス画面の表示：ゾーンのプロキシ使用率情報を表示します。

ゾーンが使用しているプロキシ ポートの割合を減らすには、次のアクションのいずれか 1 つを実行します（優先順位順に記載）。

- プロキシ IP アドレスの数を増やす：このアクションをお勧めします。詳細については、『*Guard Configuration Guide*』を参照してください。
- ゾーン ポリシーのしきい値を再設定する：ポリシーのしきい値を上げて、強力な保護レベルを必要とする送信元 IP アドレスの数を減らします。詳細については、第 8 章「ゾーンのポリシーの管理」の「ポリシーのパラメータの変更」の項を参照してください。
- ゾーンを TCP_NO_PROXY ゾーンにする：GUARD_TCP_NO_PROXY ゾーン テンプレートを使用してゾーンを再作成および再設定します。このゾーン テンプレートは、強力な保護レベルを使用しません。詳細については、第 4 章「ゾーンの作成と設定」の「ゾーンの作成」の項を参照してください。

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、ゾーン保護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ことで、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。

デフォルトでは、グラフには最近 2 時間の正当なトラフィックと悪意のあるトラフィックが bps 単位で表示されます。

ステップ 3　（オプション）トラフィック レートのグラフの表示を変更する場合は、表示するカウンタの隣にあるチェックボックスをオンにします。

ステップ 4　**Update Graph** をクリックします。Guard 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。

Guard は、次のトラフィック カウンタを表示できます。

- Legitimate：Guard がゾーンに転送した正当なトラフィック。
- Malicious：ゾーンを宛先とする悪意のあるトラフィック。悪意のあるトラフィックは、ドロップされたパケットとスプーフィング パケット（ここにはゾンビ パケットも含まれます）の合計です。
- Received：Guard が受信して処理したパケット。受信されたパケットは、正当なトラフィックと悪意のあるトラフィックの合計です。
- Dropped：Guard が攻撃の一部と見なし、ドロップしたパケット。
- Replied：正当なトラフィックの一部であるか攻撃の一部であるかを確認するために、スプーフィング防止メカニズムまたはゾンビ防止メカニズムによる処理の一環として、開始側のクライアントに応答が送信されたパケット。
- Spoofed：Guard によってスプーフィング パケットと見なされ、ゾーンに転送されなかったパケット。スプーフィング パケットは、応答された（返送された）パケットのうち、応答を受信しなかったパケットです。スプーフィング パケットにはゾンビ パケットが含まれます。

ステップ 5　（オプション）Graph Period ドロップダウン リストで期間を選択して、グラフに表示する期間を変更します。

ステップ 6　**Update Graph** をクリックします。Guard 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 7　（オプション）トラフィック レートのグラフで Guard 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。測定単位は次のいずれかです。

- pps：パケット / 秒
- bps：ビット / 秒

ステップ 8　**Update Graph** をクリックします。Guard により、グラフがアップデートされます。

ステップ 9　（オプション）Guard のカウンタをクリアするには、**Clear Counters** をクリックします。Guard 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。

- Shown in Graph：カウンタをグラフに表示するかどうかを指定します。
- Counter：使用可能なカウンタのタイプ。
- Packets：Guard 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：Guard 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。

この項は、次の内容で構成されています。

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 フローを分析する必要があります。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。

- 受信したパケットと正当なパケットの数が 0 より大きい場合は、Guard へのゾーン トラフィックの宛先変更が適切に機能していることを示します。
- 受信したパケットの数が正当なパケットの数を上回り、悪意のあるパケットの数が 0 より大きい場合は、ゾーンが攻撃を受け、ゾーン保護が適切に機能していることを示します。ゾーンが攻撃されているかどうかを確認するには、ゾーンの要約画面を参照して、Guard が攻撃を処理するために動的フィルタを作成しているかどうかを確認します（「ゾーンのステータス画面の表示」の項を参照）。

ネットワーク トラフィックに関する経験と知識に基づいて、次のガイドラインに従ってください。

- ドロップ パケットが存在している場合は、信頼された送信元 IP アドレスが動的フィルタによってブロックされていないかどうかを確認してください。信頼されたトラフィックが Guard を通過できるようにするため、信頼された送信元 IP アドレスからのトラフィックにバイパス フィルタを設定できます（第 5 章「ゾーン フィルタの設定」の「バイパス フィルタの管理」の項を参照）。
- 非常に大量の IP フローをドロップする動的フィルタをポリシーが作成した場合は、正当だと思われる送信元 IP アドレスがしきい値を上回るレートでトラフィックを送信し、そのフローをフィルタがブロックしていないかどうかを確認する必要があります。ポリシーのしきい値を大きくするか、ポリシーを非アクティブにしてポリシーが追加の動的フィルタを作成しないよう防止することができます。ゾーン ポリシーの設定については、第 8 章「ゾーンのポリシーの管理」を参照してください。
- 受信したパケットの現在のレート（pps または bps）が 0 である場合、または正当なパケットの数が長期間にわたって変化しない場合、問題が発生している恐れがあります。トラブルシューティング情報については、「ゾーン トラフィックの問題の分析」の項を参照してください。

ゾーン トラフィックの問題の分析

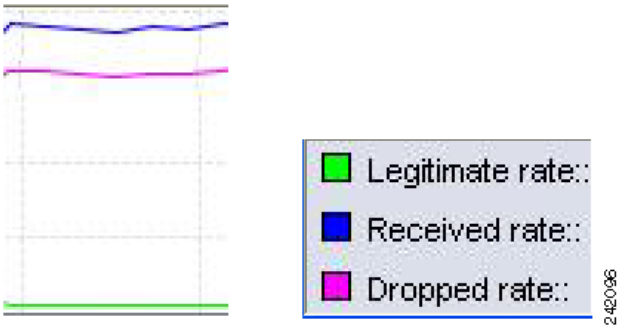
受信トラフィック カウンタ（パケットまたはビット）または正当トラフィック カウンタ（パケットまたはビット）が 0 になっている場合は、次の状況のいずれかまたは両方を示す可能性があります。

- ゾーンが宛先となっているパケットを Guard が受信していない（受信トラフィック カウンタ = 0）：ゾーン トラフィックの宛先変更またはネットワーク設定に問題があることを示しています。
- Guard は宛先変更されたゾーン トラフィックを受信しているが、パケットがゾーンに転送されるのをブロックしている（長期間にわたって、受信トラフィック カウンタが 0 より大きく、正当なトラフィックの現在のレート（pps および bps）が 0 になっている）：正当なトラフィックが悪意のあるトラフィックとして誤認識され、Guard によってドロップされていることを示します。

  図 10-3 に、ゾーンが宛先となっているほぼすべてのトラフィックがドロップされる状況を示します。Guard が作成した動的フィルタにドロップ アクション フィルタがないかどうかを確認し、次のガイドラインに従ってください。

  - ドロップ アクションを持つ動的フィルタを削除する。
  - ドロップ アクションを持つ動的フィルタを作成したポリシーを非アクティブにして、ポリシーがドロップ アクションを持つ動的フィルタを作成できないようにする。このアクションを実行しない場合、動的フィルタを削除するとドロップ アクション フィルタが再度表示され、Guard は引き続き同じトラフィック タイプを検出します。

図 10-3　問題の分析：Rcv >0、Legitimate = 0



注意　ポリシーを非アクティブにすると、Guard がポリシーをトラフィック フローに適用しなくなるため、ゾーン保護のレベルが低下する場合があります。

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。Guard 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

Guard では、ゾーンのカウンタ情報をリアルタイムに表示することができます。

（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）。

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 レートのグラフの表示を変更する場合は、表示するトラフィック カウンタのタイプ（Show in Graph の下）の隣にあるチェックボックスをオンにします。Guard 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。

Guard は、次のトラフィック カウンタを表示できます。

- Legitimate：Guard がゾーンに転送した正当なトラフィック。
- Malicious：ゾーンを宛先とする悪意のあるトラフィック。悪意のあるトラフィックは、ドロップされたパケットとスプーフィング パケット（ここにはゾンビ パケットも含まれます）の合計です。
- Received：Guard が受信して処理したパケット。受信されたパケットは、正当なトラフィックと悪意のあるトラフィックの合計です。
- Dropped：Guard が攻撃の一部と見なし、ドロップしたパケット。
- Replied：正当なトラフィックの一部であるか攻撃の一部であるかを確認するために、スプーフィング防止メカニズムまたはゾンビ防止メカニズムによる処理の一環として、開始側のクライアントに応答が送信されたパケット。
- Spoofed：Guard によってスプーフィング パケットと見なされ、ゾーンに転送されなかったパケット。スプーフィング パケットは、応答された（返送された）パケットのうち、応答を受信しなかったパケットです。スプーフィング パケットにはゾンビ パケットが含まれます。

ステップ 4　（オプション）トラフィック レートのグラフで Guard 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

Guard 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。

ゾーンのトラフィックと問題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」および「ゾーン トラフィックの問題の分析」の項を参照してください。

ゾーンのイベント ログの表示

Guard 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。Guard のログを表示して、Guard のアクティビティを確認および追跡できます。

表 10-8 に、さまざまなイベントの重大度レベルの説明を示します。

表 10-8　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

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）イベント テーブルに表示するイベントを制御するには、次のオプションのいずれかを選択します。

- **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 10-8 を参照）。

ステップ 4　**Filter Events** をクリックします。Guard 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

Guard では、ゾーンで Guard が検出した攻撃を分析できるようにするために、ゾーンごとのハイレベルな攻撃要約レポート（図 10-4 を参照）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。Guard は、攻撃の進行中に情報を記録し、そのデータをさまざまな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。Guard は、攻撃のデータもグラフ形式で表示します。

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。

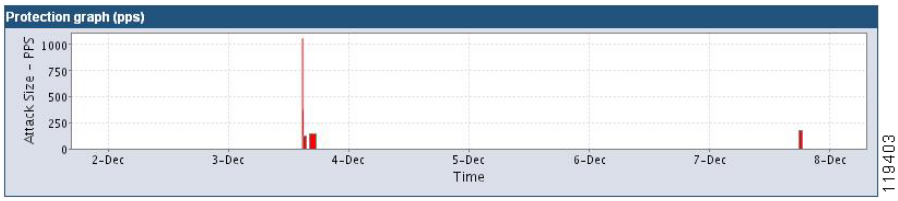
ステップ 2　ゾーンのメイン メニューで、**Diagnostics > Attack Reports > Attack Summary** を選択します。Attacks Summary 画面が表示されます。デフォルトでは、レポートに先月分の攻撃情報が表示されます。

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。

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

- 保護のグラフ：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 10-4　ゾーン保護の要約レポート：保護のグラフ



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 10-9 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 10-9　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

フィールド	説明
Attacks Mitigated	軽減された攻撃の数。
Attacks Duration	軽減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悪意のある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て、Guard が受信したトラフィックの総量。
Total Blocked	ゾーンが宛先となっていて、Guard がドロップしたトラフィックの総量。
Legitimate vs. Malicious Traffic	ゾーンの総トラフィックについて、悪意のあるトラフィック（赤色で表示）と正当なトラフィック（青色で表示）の割合を表示する円グラフ。

- 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。

  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表示」の項を参照）。

表 10-10 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 10-10　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
#	軽減された攻撃の識別番号（ID）。Guard は、進行中の攻撃に Curr という値を表示します。
Start time	軽減された攻撃の発生日時。
Duration	軽減された攻撃の持続期間（時、分、および秒）。
Type	軽減された攻撃のタイプ。表示される値は次のいずれかです。 • Client Attack：スプーフィング以外のすべてのトラフィック異常。 • Malformed Packets：悪意のある不正形式パケットと見なされたすべてのトラフィック異常。 • Spoofed：スプーフィングされた送信元からの DDoS 攻撃と見なされたトラフィック異常。 • User Defined：ユーザ フィルタが処理したすべての異常。これらのフィルタは、デフォルト設定で動作することも、ユーザが動作を設定することもできます。 • Zombie：ゾンビが発信元であると見なされたトラフィック異常。 • Hybrid：特性の異なる複数の攻撃で構成された攻撃。 • Traffic Anomaly：短期間のみ検出され、軽減を必要としなかった異常。
Peak (pps)	攻撃レートの最大値（パケット / 秒単位）。
Received Pkts	攻撃の進行中に Guard が処理した、ゾーンが宛先となっていたパケットの総数。
Legitimate vs. Malicious Traffic	攻撃進行中の総トラフィックについて、悪意のあるトラフィック（赤色で表示）と正当なトラフィック（青色で表示）の割合を表示する円グラフ。

- サブゾーン レポート：サブゾーンのリストを表示します。サブゾーンは、ゾーンの一部（送信元ゾーンのすべての IP アドレス範囲を含まないゾーン）を保護するために Guard が作成したゾーンです。サブゾーンの保護が終了すると、Guard はサブゾーンを消去します。サブゾーンの攻撃レポートを表示するには、サブゾーン名をクリックします。サブゾーンの追加情報については、第 4 章「ゾーンの作成と設定」の「サブゾーンについて」の項を参照してください。

攻撃レポートの詳細表示

Guard を使用して、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、ユーザによる指示またはタイムアウト パラメータのアクションによって保護が終了するまでの、攻撃の詳細が示されています。

Guard 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。

この項は、次の内容で構成されています。

- 過去の攻撃レポートの詳細表示

- 現在の攻撃の詳細表示

過去の攻撃レポートの詳細表示

過去のゾーン攻撃のレポートの詳細を表示するには、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。ゾーンのステータス画面とゾーンのメイン　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、前月の攻撃情報が示されます。

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　次のいずれかの方法で、攻撃レポートの詳細を表示します。

- 保護のグラフの攻撃バーをクリックします。
- 攻撃ごとの要約テーブルに表示されている攻撃のいずれかのフィールドをクリックします。

Attack report 画面が表示されます。

現在の攻撃の詳細表示

ゾーンに対する攻撃が進行中の場合、Guard は、攻撃を受けているゾーンのステータス画面上に Report ボタンを表示します。

ゾーンの現在の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、攻撃を受けているゾーンを選択します。ゾーンのステータス画面とゾーンのメイン メニューが表示されます。

ステップ 2　次のいずれかの方法で、ゾーンの現在の攻撃レポートを表示します。

- ゾーンのステータス画面の **Report** をクリックします。
- ゾーンのメイン メニューで **Diagnostics > Attack Reports > Attack Summary** を選択し、攻撃ごとの要約テーブルにある、進行中の攻撃のいずれかのフィールドをクリックします。Guard は、進行中の攻撃の識別番号（#）に Curr という値を表示します。

攻撃レポートの詳細について

この項では、詳細な攻撃レポートにおいて、Guard が表示する以下の情報について説明します。

- 一般的な攻撃情報について
- 攻撃に関する統計情報について
- ドロップまたは返送されたパケットに関する情報について

一般的な攻撃情報について

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。Guard 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について

攻撃に関する統計情報テーブルには、次のタイプのパケットに関する情報が示されます。

- Received：Guard が受信した、ゾーンが宛先となっているトラフィック。
- Forwarded：Guard がゾーンに転送した正当なトラフィック。
- Replied：Guard のスプーフィング防止機能およびゾンビ防止機能による処理の一環として、クライアントに送信されたトラフィック。
- Dropped：ゾーンが宛先となっていて、Guard によってドロップされたパケットの総数。

表 10-11 に、各パケット タイプに含まれる情報の説明を示します。

表 10-11　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。
%	受信したパケットの中で、このパケットが占める割合。

トラフィック レートは、「一般的な攻撃情報について」の項のドロップダウン リストで選択した単位で表示されます。

ドロップまたは返送されたパケットに関する情報について

ドロップまたは返送されたパケットのテーブルには、Guard が悪意のあるトラフィックとして識別し、ドロップまたは応答（返送）したパケットに関する統計情報が示されます。パケットは、パケットを識別した Guard の機能に基づいて分類されています。

テーブルの行には、次の Guard の機能が表示されます。

- Rate Limiter：ゾーンのレート リミッタによって、またはレート リミッタが設定されていたユーザ フィルタによってドロップされたパケット。レート リミッタの設定の詳細については、第 4 章「ゾーンの作成と設定」の「ゾーン テンプレートからのゾーンの作成」の項を参照してください。
- Flex-content filter：フレックスコンテンツ フィルタによってドロップされたパケット。フレックスコンテンツ フィルタの使用の詳細については、第 5 章「ゾーン フィルタの設定」の「フレックスコンテンツ フィルタの管理」の項を参照してください。
- User filter：ユーザ フィルタによってドロップされたパケット。ユーザ フィルタの使用の詳細については、第 5 章「ゾーン フィルタの設定」の「ユーザ フィルタの管理」の項を参照してください。
- Dynamic filter：動的フィルタによってドロップされたパケット。動的フィルタの使用の詳細については、第 9 章「ゾーン保護のアクティブ化」の「動的フィルタの管理」の項を参照してください。
- Spoofed：Guard によってスプーフィング パケットまたは発信元がゾンビであるパケットと見なされ、ゾーンに転送されなかったパケット。スプーフィング パケットは、応答が受信されなかったパケットです。
- Malformed：形式が不正であると Guard が判断したため、ドロップされたゾーン宛てのパケット。

表 10-12 に、各パケット タイプに含まれる情報の説明を示します。

表 10-12　ドロップまたは返送されたパケットに含まれるフィールドの説明

フィールド	説明
Total	ドロップまたは返送されたパケットの総数。
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。
%	ドロップまたは返送された合計パケットがパケット数に占める割合。

トラフィック レートは、「一般的な攻撃情報について」の項のドロップダウン リストで選択した単位で表示されます。

検出された異常に関する情報について

検出された異常のテーブルには、Guard 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、Guard 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。Guard では、タイプとフロー パラメータ（送信元 IP アドレスや宛先ポートなど）が同じトラフィック異常を 1 つのタイプとしてまとめます。

表 10-13 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 10-13　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）。
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：Guard 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。 • SIP (UDP)：VoIP セッションの確立に Session Initiation Protocol（SIP）over UDP を使用する、検出済み Voice over IP（VoIP）異常フロー。
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というステータス。**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 1 つにワイルドカードとしてアスタリスク（*）が使用される場合、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した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 10-14 に、Guard が提供する異常の詳細情報の説明を示します。

表 10-14　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.：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。アクション フローは、特定の送信元 IP アドレス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.：断片化特性

軽減された攻撃に関する情報について

軽減された攻撃のテーブルには、ゾーンを保護するために Guard が実行したアクションと、ゾーンに有害であると判明し、軽減された攻撃が示されます。攻撃については、「検出された異常に関する情報について」の項で説明します。Guard は、同じタイプおよびフロー パラメータを持つ軽減アクションをグループ化し、まとめて表示します。

表 10-15 に、軽減された攻撃のテーブルに含まれるフィールドの説明を示します。

表 10-15　軽減された攻撃のテーブルに含まれるフィールドの説明

フィールド	説明
#	軽減された攻撃に Guard によって割り当てられた識別番号。
Start time	軽減された攻撃の発生日時。
Duration	軽減された攻撃の持続期間（時、分、および秒）。
Attack Type	軽減された攻撃のタイプ。表示される値は次のいずれかです。 • Spoofed : スプーフィングされた送信元 IP からの DDoS 攻撃と見なされたトラフィック異常。 • Client Attack : 未認証の送信元 IP アドレスからの DDoS 攻撃と見なされたトラフィック異常。 • User Defined : ユーザ フィルタによって処理された異常など、ユーザ定義のフィルタによって検出された DDoS 攻撃。ユーザ フィルタの使用の詳細については、第 5 章「ゾーン フィルタの設定」の「ユーザ フィルタの管理」の項を参照してください。 • Zombie : ゾンビが発信元である DDoS 攻撃と見なされたトラフィック異常。 • Malformed Packets : 悪意のある不正形式パケットによる DDoS 攻撃と見なされたトラフィック異常。 保護レベル（Basic または Strong）がカッコの中に示されます。
Triggering rate	軽減された攻撃のトラフィック レート。トリガー レートは、クライアント攻撃またはユーザ定義攻撃にのみ適用されます。スプーフィングおよび不正な形式のパケットを利用した攻撃には適用されません。
% Threshold	ポリシーしきい値に対する割合で表した、軽減された攻撃のレート。
Anomaly Flow	軽減された異常トラフィック 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。
Action flow	Guard による攻撃軽減後のトラフィック フローの特性。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。
Dropped	攻撃の軽減中にドロップされたトラフィック。
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（「軽減された攻撃の詳細の表示」の項を参照）。

パラメータの 1 つにワイルドカードとしてアスタリスク（*）が使用される場合、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。

軽減された攻撃の詳細の表示

軽減された攻撃の詳細のテーブルには、Guard が攻撃の軽減に使用した機能に関する追加情報が示されます。

軽減された攻撃の詳細のテーブルを表示するには、軽減された攻撃のテーブルで、対象となる攻撃の Details カラムにある **i** をクリックします。

表 10-16 に、軽減された攻撃の詳細テーブルに Guard が表示する情報の説明を示します。

表 10-16　軽減された攻撃の詳細テーブルに含まれるフィールドの説明

フィールド	説明
Start time	軽減された攻撃の発生日時。
End time	アクティブになった動的フィルタの満了日時。
Rate (pps)	レート（パケット / 秒単位）。 • Thresh：軽減された攻撃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	軽減された検出済みフローに関する次の情報が示されます。 • 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.：断片化特性 • Type：検出された異常のタイプ
Action flow	軽減機能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宛先 IP アドレスの特定の宛先ポートを示すのに対して、アクション フローは特定の宛先 IP アドレスのすべての宛先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.：断片化特性

応答された IP の要約情報について

応答された IP の要約には、スプーフィングおよび非スプーフィング送信元 IP アドレスのリストが示され、次の 2 つのテーブルで構成されています。

- Replied IP Summarization - attack start
- Replied IP Summarization - total attack

応答された IP の要約の 2 つのテーブルを使用して、攻撃期間中に攻撃の送信元の場所が変更されたかどうか、つまり攻撃開始時にある場所から始まり、攻撃中に別のサブネットに移ったかどうかを判断できます。

ゾーンが大規模なスプーフィング攻撃の犠牲になっている場合、攻撃者が使用するサブネットが、応答された IP の要約結果に表示される可能性は最も高くなります。Guard は、スプーフィング防止プロセスを通過するすべてのトラフィック（応答されたトラフィック）に対して応答された IP の要約を実行するので、要約結果には、非スプーフィング IP アドレスも含まれることがあります。Guard は非スプーフィング トラフィックに対しては数分に 1 回だけ認証を実行しますが、スプーフィング トラフィックの認証は継続的に試みているので、応答された IP の要約には、スプーフィング IP アドレスの方がより頻繁に表示されます。

応答された IP の要約テーブルは、スプーフィング IP アドレスの情報を示す唯一の攻撃レポートのテーブルです。ただし、非スプーフィング攻撃のパケットは動的フィルタによりドロップされるので、軽減された攻撃のテーブルに、非スプーフィング攻撃の IP アドレスも表示されることがあります。

表 10-17 に、攻撃レポートのこのセクションに含まれるフィールドの説明を示します。

表 10-17　応答された IP の要約テーブルに含まれるフィールドの説明

フィールド	説明
Subnet	スプーフィングまたは非スプーフィング パケットの IP アドレス。
Subnet Mask	スプーフィングまたは非スプーフィング パケットのサブネット マスク。
Weight(%)	Guard が記録したサンプルの総数における、そのサブネット IP アドレスからのサンプルの割合。
Unique Addresses	そのサブネットに属する一意のアドレスの数。

Guard は、パケットダンプ自動キャプチャ機能をイネーブルにした場合にのみ、応答された IP の要約情報を攻撃レポートに表示します(第 11 章「ネットワーク トラフィックの監視と攻撃シグニチャの抽出」の「自動パケットダンプ キャプチャのイネーブル化」の項を参照)。応答されたパケットダンプ キャプチャ ファイルには、クライアントを認証しようとして Guard が発行した、応答されたパケットのみが含まれています。このため、応答された IP の要約は、記録されたパケットの宛先 IP アドレスから取得されます。応答された IP の要約のレポート結果を正確なものにするため、そのゾーンに対する攻撃中、パケットダンプ キャプチャ機能をイネーブルのままにしておく必要があります。攻撃中にパケットダンプ キャプチャ機能をディセーブルにすると、応答された IP の要約情報は正確でなくなるか、存在しなくなることがあります。

検出された HTTP ゾンビに関する情報について

HTTP ゾンビ攻撃が検出されたことを示すインジケータは、一般的な攻撃情報セクションに表示されます（図 10-5 および「一般的な攻撃情報について」の項を参照）。

図 10-5　検出された HTTP ゾンビ

検出された HTTP ゾンビのリストを表示するには、**i** または **Show HTTP detected zombies** をクリックします。このタイプのトラフィック異常に関する詳細については、「HTTP ゾンビ リストの表示」の項を参照してください。

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　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、シャープ記号（#）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、Guard 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**：使用する転送プロトコルとして、次のいずれかを選択します。

    FTP：File Transport Protocol（ファイル転送プロトコル）を指定します。

SFTP：Secure File Transport Protocol（セキュア ファイル転送プロトコル）を指定します。

SCP：Secure Copy Protocol を指定します。

SFTP および SCP は、Secure Shell（SSH）に依存してセキュアな転送を提供します。そのため、SFTP サーバまたは SCP サーバに攻撃レポートをエクスポートする前に、セキュアな通信のために Guard で使用するキーを設定していない場合、パスワードを入力するように Guard から求められます。SFTP および SCP 用のキーは、Guard CLI を使用しないと設定できません。

- **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。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、Guard はパスワードを入力するように求めます。

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　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、シャープ記号（#）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。Guard が攻撃レポートを削除します。

HTTP ゾンビ リストの表示

HTTP ゾンビ リストを使用すると、ゾーンのトラフィックを分析し、攻撃を開始したゾンビのリストを表示できます。ゾンビに対してアクションを実行できます。

HTTP ゾンビ 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 > HTTP Zombies** を選択します。HTTP ゾンビ リストの画面が表示されます。

表 10-18 に、Guard が HTTP ゾンビ テーブルに表示する情報の説明を示します。

表 10-18　HTTP ゾンビ リストに含まれるフィールドの説明

フィールド	説明
IP	ゾンビの IP アドレス。
Start Time	ゾンビの接続が最初に識別された日時。
Duration	ゾンビ攻撃の持続期間。
“get” Requests	ゾンビによって送信された HTTP GET 要求の数。

ポリシーの統計情報のテーブルの表示

1 つまたは一連のゾーン ポリシーを通過するトラフィックのレートを表示できます。サービスのタイプおよび量がゾーンのトラフィックを表しているかどうかを判断できます。Guard は、ポリシーによって測定された最高レートでゾーンに転送されたトラフィック フローを表示します。レートは、トラフィックのサンプルに基づいて計算されます。

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）画面上でフィルタを設定し、選択したポリシーを次のように表示します。

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. 使用する画面フィルタを設定し、**OK** をクリックします。表 10-19 に、Policy Filter ウィンドウに表示される画面フィルタ パラメータの説明を示します。目的の表示パラメータを、対応するドロップダウン リストから選択します。

   複数のフィルタ パラメータを変更するには、Policy Filter ウィンドウの一番上のパラメータから開始して、下方向に順に変更していきます。

（注）　フィルタ パラメータを 1 つ変更すると、そのパラメータの下にあるすべてのパラメータが、デフォルト設定に自動的にリセットされます。

表 10-19　ポリシーのフィルタ パラメータ

パラメータ	表示する項目
Policy template	選択したポリシー テンプレートに基づいて作成されたポリシー。
Service	選択したサービスのために作成されたポリシー。
Protection level	選択した保護レベルを持つポリシー。

表 10-19　ポリシーのフィルタ パラメータ（続き）

パラメータ	表示する項目
Type	選択したパケット タイプを持つポリシー。
Policy	選択したキーを持つポリシー。
State	選択した動作状態になっているポリシー。
Action	選択したアクションを使用して設定されているポリシー。
Policies	現在の設定のポリシー、またはスナップショット（使用可能な場合）のポリシー。

指定した基準を満たす、ポリシーのリストの一部が表示されます。選択したパス、状態、およびアクションの詳細が 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、5 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。

- PPS Rate：パケット / 秒単位でトラフィック レートを測定するポリシーを通過した、トラフィックのレート。
- PPH Rate：パケット / 時間単位でトラフィック レートを測定するポリシーを通過した、トラフィックのレート。PPH ポリシーの詳細については、第 8 章「ゾーンのポリシーの管理」の「ゾーンのポリシーについて」の項を参照してください。
- 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 ポリシーおよび次のパケット タイプについてのみ表示されます。
  - 分析保護モジュールの in_nodata_conns
  - 強化保護モジュールの in_conns
- 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。

表 10-20 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 10-20　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	ポリシーが監視するサービス。
Level	Guard がトラフィック フローに適用した保護レベル。指定可能な値は、Analysis、Basic、および Strong です。

表 10-20　ポリシーの統計情報（続き）

フィールド	説明
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。 • auth_tcp_pkts：TCP ハンドシェイクを受けたパケット。 • auth_udp_pkts：UDP 認証を受けたパケット。 • in_conns：ゾーンへの着信接続。 • 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。 • num_sources：ゾーンが宛先になっている、Guard のスプーフィング防止機能によって認証済みの TCP 送信元 IP アドレスの数。 • 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（パケット / 秒単位）。 • reqs_pph：データ ペイロードを含んだ要求パケット（パケット / 時間単位）。 • syns：同期パケット（パケット / 秒単位の TCP SYN フラグ付きパケット）。 • syns_pph：同期パケット（パケット / 時間単位の TCP SYN フラグ付きパケット）。 • 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 フラグ付きパケットの数と FIN フラグ付きパケットの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	ポリシー名。
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）。 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：プロトコル番号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の IP アドレスに宛てたトラフィック）。 • 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）。
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、最も大きい値が最上部に表示されます。

ドロップの統計情報のテーブルの表示

ドロップの統計情報のテーブルを使用すると、進行中の攻撃について、ドロップされたパケットの持続期間をレートおよびカウンタごとに表示できます。

ドロップ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 > Drop Statistics** を選択します。Drop Statistics 画面が表示されます。

ステップ 3　（オプション）表示される統計情報の測定単位を変更するには、ドロップダウン リストから目的の測定単位を選択し、**Set units** をクリックします。

ドロップされたパケットは、パケット タイプに基づいて 2 つのテーブルに表示されます。

表 10-21 にドロップ統計情報テーブルの内容の説明を、表 10-22 にスプーフィング統計情報テーブルの内容の説明を示します。

表 10-21　ドロップの統計情報

タイプ	説明
Total dropped	ドロップされたトラフィックの総量。
Dynamic filters	動的フィルタによってドロップされたトラフィックの量。
User filters	ユーザ フィルタによってドロップされたトラフィックの量。
Flex filter	フレックスコンテンツ フィルタによってドロップされたトラフィックの量。
Rate limit	ユーザ フィルタのレート リミット パラメータと、ドロップされたゾーンのレート リミットによって定義されたパケット。
Incoming TCP unauthenticated basic	基本的な TCP スプーフィング防止機能が認証に失敗し、ドロップされたトラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。
Incoming TCP unauthenticated-strong	強力な TCP スプーフィング防止機能によって認証されなかったためにドロップされたトラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。
Outgoing TCP unauthenticated	TCP スプーフィング防止機能によって認証されなかったためにドロップされた、ゾーンで開始された接続。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。
UDP unauthenticated-basic	基本的なスプーフィング防止機能によって認証されなかったためにドロップされた UDP トラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。

表 10-21　ドロップの統計情報（続き）

タイプ	説明
UDP unauthenticated-strong	強力なスプーフィング防止機能によって認証されなかったためにドロップされた UDP トラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。
Other protocols unauthenticated	Guard のスプーフィング防止機能が認証に失敗し、ドロップされた TCP および UDP 以外のトラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。
TCP fragments unauthenticated	Guard のスプーフィング防止機能によって認証されなかったためにドロップされた、断片化された TCP パケット。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。
UDP fragments unauthenticated	Guard のスプーフィング防止機能によって認証されなかったためにドロップされた、断片化された UDP パケット。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。
Other protocols fragments unauthenticated	Guard のスプーフィング防止機能によって認証されなかったためにドロップされた、TCP および UDP 以外の断片化されたパケット。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。
DNS malformed replies	Guard の保護機能によってドロップされた不正な形式の DNS 応答。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内で不正な形式のパケットとしてカウントされます。
DNS spoofed replies	Guard のスプーフィング防止機能によってドロップされた、ゾーンで開始された接続に応答する着信 DNS パケット。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。
DNS short queries	Guard の保護機能によってドロップされた短い（不正な形式の）DNS クエリー。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内で不正な形式のパケットとしてカウントされます。
Non DNS packets to/from DNS port	Guard の保護機能がドロップした、DNS ポートを宛先または送信元とする非 DNS トラフィック。攻撃レポートでは、このようなパケットは Malicious Packets Statistics テーブル内で不正な形式のパケットとしてカウントされます。
Bad packets to proxy addresses	Guard の保護メカニズムによってドロップされた、Guard のプロキシ IP アドレス宛ての不正形式トラフィック。
TCP anti-spoofing mechanisms related pkts	Guard の TCP スプーフィング防止機能が実行した副次的な動作が原因でドロップされたパケットの数。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内で不正な形式のパケットとしてカウントされます。
DNS anti-spoofing mechanisms related pkts	Guard の DNS スプーフィング防止機能が実行した副次的な動作が原因でドロップされたパケットの数。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内で不正な形式のパケットとしてカウントされます。

表 10-21　ドロップの統計情報（続き）

タイプ	説明
Anti-spoofing internal errors	Guard のスプーフィング防止機能のエラーのためにドロップされたパケットの数。攻撃レポートでは、このようなパケットは Packets テーブルでカウントされます。
Land attack	送信元 IP アドレスと宛先 IP アドレスが同じであるためにドロップされたパケットの数。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内で不正な形式のパケットとしてカウントされます。
Malformed packets	ヘッダーの形式が不正だったためにドロップされたパケットの数。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内で不正な形式のパケットとしてカウントされます。
Malformed SIP packets	不正な形式であるために Guard の保護機能がドロップした Session Initiation Protocol（SIP）over UDP パケット。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。
SIP anti-spoofing features related pkts	Guard のスプーフィング防止機能が、副次的な動作が原因でスプーフィングされていると見なしてドロップした SIP over UDP パケットの数。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内で不正な形式のパケットとしてカウントされます。

表 10-22　スプーフィングの統計情報

タイプ	説明
Total spoofed	スプーフィングされたトラフィックの総量。
Spoofed incoming TCP basic	基本的な TCP スプーフィング防止機能が認証に失敗したトラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。
Spoofed incoming TCP strong	強力な TCP スプーフィング防止機能が認証に失敗したトラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。
Spoofed outgoing TCP basic	基本的な TCP スプーフィング防止機能が認証に失敗した、ゾーンが開始した接続トラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。
Spoofed outgoing TCP strong	強力な TCP スプーフィング防止機能が認証に失敗した、ゾーンが開始した接続トラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。
Spoofed incoming DNS	着信 Domain Name System（DNS）（クエリー）スプーフィング防止機能が認証に失敗したトラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。
Spoofed outgoing DNS basic	発信 DNS（応答）基本スプーフィング防止機能が認証に失敗したトラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。

表 10-22　スプーフィングの統計情報（続き）

タイプ	説明
Spoofed outgoing DNS strong	発信 DNS（応答）強化スプーフィング防止機能が認証に失敗したトラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。
Spoofed zombie	ゾンビ スプーフィング防止機能が認証に失敗したトラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。
Spoofed incoming SIP	着信 SIP over UDP スプーフィング防止機能が認証に失敗したトラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。