CHAPTER 9

異常の検出のアクティブ化

この章では、WBM を使用して異常検出をアクティブにする方法について説明します。ユーザがゾーンの異常検出をアクティブにすると、Cisco Traffic Anomaly Detector Module（Detector モジュール）は、受信するゾーンのトラフィックのコピーにゾーンのポリシーを適用します。トラフィックの異常によってポリシーのしきい値の超過が発生し（攻撃の兆候が示され）、ポリシーのアクションがトリガーされると、Detector モジュールは、ユーザに通知を送信するか、Cisco Anomaly Guard（Guard）をアクティブにします。

Detector モジュールの付属製品である Guard は Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃を検出および軽減するデバイスです。攻撃トラフィックをドロップし、正当なトラフィックをネットワークに再注入することで、トラフィックがゾーンを通過するときにゾーン トラフィックをクリーニングします。Detector モジュールは、ゾーンが攻撃を受けていると判断したときに、Guard の攻撃軽減サービスをアクティブにすることができます。また、Detector モジュールはゾーンの設定を Guard と同期させることもできます。Guard の詳細については、『*Cisco Anomaly Guard Module Configuration Guide*』または『*Cisco Guard Configuration Guide*』を参照してください。

この章は、次の項で構成されています。

異常検出のアクティベーションのオプションについて

Detector モジュールには、異常の検出を実行するためのオプションがいくつか用意されています。たとえば、異常検出動作のすべての面を Detector モジュールで管理するように設定したり、攻撃の進行中に Detector モジュールを監視し、指示したりできます。

この項は、次の内容で構成されています。

Detect と Detect and Learn

ゾーンの異常検出をアクティブにする場合、Detector モジュールでは次のオプションを選択できます。

- Detect：ゾーンのトラフィックを分析し、トラフィックの異常を検出すると、動的フィルタの作成を開始します。
- Detect and Learn：ゾーンのトラフィックに異常がないかどうか分析すると同時に、ラーニング プロセスのしきい値調整フェーズを開始します。しきい値調整フェーズ用にトラフィックを分析する間、Detector モジュールはゾーン設定のポリシーのしきい値を、新しいしきい値の情報で自動的に調整します。トラフィックの分析中に攻撃を検出した場合、Detector モジュールは、攻撃トラフィックのしきい値をラーニングしないよう、しきい値調整フェーズを停止します。

自動動作モードとインタラクティブ動作モード

Detector モジュールでは、次のいずれかの動作モードでゾーン トラフィックの異常を検出するように設定できます。

- 自動検出モード：攻撃中に作成した動的フィルタを自動的にアクティブにします。
- インタラクティブ検出モード：攻撃中に動的フィルタを作成しますが、アクティブにしません。代わりに、Detector モジュールは動的フィルタを*推奨事項*としてグループ化します。ユーザは推奨事項を確認して、受け入れるか、無視するか、または自動アクティベーションに誘導するかを決定します。

異常の検出の管理

この項では、ゾーン トラフィックの異常の検出を手動でアクティブまたは非アクティブにする方法について説明します。

この項は、次の内容で構成されています。

異常の検出のアクティブ化

ゾーンの異常の検出をアクティブにするには、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 メニューとゾーンのステータス画面が表示されます。

ステップ 2　次のいずれかの方法で、異常の検出をアクティブにします。

- Detect のみをアクティブにするには、**Detect** をクリックするか、ゾーンのメイン メニューで **Detection > Detect** を選択します。
- Detect and Learn をアクティブにするには、**Detect & Learn** をクリックします。

Detector モジュールがトラフィック フローの分析を開始して、トラフィックの異常を検出します。

ナビゲーション ペインの Under Detection ゾーン リストにゾーン名が追加され、Recent Events テーブルには、*検出が実行されているゾーン*の詳細なリストとともに、*検出開始*のイベント タイプが表示されます。

ゾーンのステータス アイコンが検出  に変更されます。

トラフィック異常の検出の確認

ゾーンのステータス画面からトラフィックのカウンタを表示すると、異常の検出プロセスが正常に動作しているかどうかを確認できます。

ナビゲーション ペインで、検出実行中のゾーンをクリックしてゾーンのステータス画面を表示します。次の条件を満たしている場合、異常の検出が機能しています。

- Recent Events テーブルに、*検出が実行されているゾーン*の詳細なリストとともに、*検出開始*のイベント タイプが表示される。
- Traffic Rate テーブルの受信トラフィック レートが 0 より大きい値を示す。

異常の検出の非アクティブ化

異常の検出を非アクティブにするには、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、検出中のゾーンをクリックします。ゾーンのメイン メニューとゾーンのステータス ページが表示されます。

ステップ 2　次のいずれかの方法で、異常の検出を非アクティブにします。

- ゾーンのステータス画面で **Deactivate** をクリックします。
- ゾーンのメイン メニューで **Detection > Deactivate** を選択します。

Detect 機能がイネーブルの場合、Detector モジュールはゾーン トラフィックの分析を停止し、ゾーンのステータスがスタンバイ  に変更されます。

Detect and Learn 機能がイネーブルの場合は、Deactivate ウィンドウが表示されます（ステップ 3 に進みます）。

ステップ 3　**Stop Detection** チェックボックスをオンにします。

ステップ 4　（オプション）**Stop Learning** チェックボックスをオンにしてラーニング プロセスのしきい値調整フェーズを停止し、Deactivate ウィンドウで次のいずれかのオプションを選択して、Detector モジュールが新しいしきい値を処理する方法を定義します。

- **Reject**：しきい値調整フェーズの現在の結果を無視します。
- **Accept**：しきい値調整フェーズの現在の結果を、ゾーンの設定に使用します。使用するしきい値の選択方法を定義します。

  表 9-1 に、しきい値の選択方法のパラメータの説明を示します。

表 9-1　しきい値の選択方法

パラメータ	説明
Threshold selection method	受け入れるしきい値を選択する方法。ドロップダウン リストから、次のいずれかのオプションを選択します。 • Accept new thresholds：ラーニング プロセスの結果をゾーンの設定に保存します。 • Accept max. thresholds：ポリシーの現在のしきい値とラーニングしたしきい値とを比較し、値の大きい方をゾーンの設定に保存します。これがデフォルトの方法です。 • Accept weighted thresholds：次の公式に基づいて、保存するポリシーのしきい値を計算します。 新しいしきい値 = (ラーニングしたしきい値 * 重み + 現在のしきい値 * (100 - 重み)) / 100 Weight フィールドに重み値を入力します。 • Keep current thresholds：ラーニング プロセスの提案されたしきい値をすべて拒否します。ポリシーは、現在のしきい値を保持します。
Weight	Detector モジュールが新しいしきい値の計算に使用する重みを定義します。このオプションは、Accept weighted thresholds という方法を選択した場合にだけアクティブになります。次の式に、Detector モジュールが使用する重み値を入力します。 新しいしきい値 = (ラーニングしたしきい値 * 重み + 現在のしきい値 * (100 - 重み)) / 100

ステップ 5　**OK** をクリックして、選択内容を確認します。

Detector モジュールはゾーン トラフィックの分析を停止し、ナビゲーション ペインの Under Detection リストからゾーン名が削除されます。

動的フィルタの管理

動的フィルタは、必要な保護レベルをトラフィック フローに適用し、攻撃の対処法を定義します。Detector モジュールは、フローがゾーン ポリシーのしきい値を超えた場合にゾーン トラフィックに異常を検出し、動的フィルタを作成して、このフィルタ セットをゾーンのトラフィックおよび特定の DDoS 攻撃に合せて継続的に調整します。ゾーンで攻撃が発生している場合にのみ、動的フィルタを表示および管理できます。Detector モジュールは、異常検出がアクティブになっていて、ゾーンが攻撃を受けている場合にのみ、動的フィルタを作成するからです。

攻撃中に手動でゾーンの異常検出を制御するには、攻撃中に動的フィルタを追加または削除します。Detector モジュールは、攻撃が終了するとすべての動的フィルタを削除します。Detector モジュールは、すべてのゾーンで最大 150,000 の動的フィルタを同時にアクティブにします。

この項は、次の内容で構成されています。

動的フィルタのリストの表示

動的フィルタ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、検出実行中のゾーンを選択します。ゾーンのメイン メニューとゾーンのステータス画面が表示されます。

ステップ 2　次のいずれかの方法で、動的フィルタのリストを表示します。

- ゾーンのメイン メニューで **Detection > Dynamic filters** を選択します。
- ゾーンのステータス テーブルで **Active Dynamic filters** をクリックします。

Dynamic Filters 画面が表示されます。

動的フィルタのテーブルには、動的フィルタを作成したポリシーに従ってフィルタリングされる動的フィルタが示され、進行中の攻撃に関する情報が表示されます。表 9-2 に、動的フィルタのテーブルに表示される情報の説明を示します。

表 9-2　動的フィルタに含まれているフィールドの説明

フィールド	説明
Created by	動的フィルタを作成したポリシー。ポリシーの名前をクリックすると、ポリシーの詳細が表示されます。
Activation	動的フィルタがアクティブになった日時。
Expiration	フィルタの有効期限が満了する時刻。この時刻を過ぎると、動的フィルタは削除されます。
Src IP	フィルタが処理するトラフィックの送信元 IP アドレス。

表 9-2　動的フィルタに含まれているフィールドの説明（続き）

フィールド	説明
Dst IP	動的フィルタの適用対象となる宛先 IP アドレス。 Detector モジュールは、宛先 IP アドレスと、ゾーンに設定された Protect-IP state の値に基づいて、Guard 上で保護をアクティブにします。
Protocol	フィルタが処理するトラフィックのプロトコル番号。
Dst Port	フィルタが処理するトラフィックの宛先ポート。
Fragments	トラフィック フローの断片化設定。攻撃ストリームに、断片化されたパケットが含まれているかどうかを指定します。
Action	動的フィルタが実行するアクション。
Rate (pps)	このフィルタに対して測定された現在のトラフィック レート（パケット / 秒単位）。
Details	このフィルタに関する追加情報が存在することを示します。**i** をクリックすると、追加情報が表示されます。

Src IP、Protocol、および Dst Port は特定のものでなくても問題ありません。アスタリスク（*）は、フィルタがすべてのフィールド値に対して処理を実行すること、または複数の値がフィルタに一致したことを示します。

特定の動的フィルタの詳細の表示については、「動的フィルタの詳細の表示」の項を参照してください。

動的フィルタの詳細の表示

特定の動的フィルタの詳細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、検出実行中のゾーンを選択します。ゾーンのメイン メニューとゾーンのステータス画面が表示されます。

ステップ 2　次のいずれかの方法で、動的フィルタのリストを表示します。

- ゾーンのメイン メニューで **Detection > Dynamic filters** を選択します。
- ゾーンのステータス テーブルで **Active Dynamic filters** をクリックします。

Dynamic Filters 画面が表示されます。

ステップ 3　詳細を表示する動的フィルタの Details カラムにある **i** をクリックします。Dynamic Filter Details 画面が表示されます。

Dynamic Filter Details 画面には、次の情報を表示する 3 つのテーブルがあります。

- 動的フィルタを作成したポリシー。
- 攻撃フローに関する情報。
- 動的フィルタを作成したトリガーに関する情報。表 9-3 に、トリガーのパラメータの説明を示します。

表 9-3　トリガーに含まれているフィールドの説明

フィールド	説明
Policy Threshold	攻撃フローによって超過したポリシーのしきい値。
Triggering rate	動的フィルタの作成原因となった攻撃の概算レート。

動的フィルタの追加

ゾーンに対する攻撃中に、動的フィルタを追加して、ゾーンの異常検出を管理できます。リモート Guard リストに定義された Guard をアクティブにしてゾーンを保護するよう、動的フィルタを設定することができます。動的フィルタの宛先 IP アドレスは、ゾーンに設定された Protect-IP state およびアドレス範囲に一致する必要があります。一致しない場合、リモート Guard のアクティベーションは失敗します。次のいずれかの方法で、リモート Guard 上でゾーン保護をアクティブにするように動的フィルタを設定できます。

- リモート Guard 上で、ゾーン全体に対してゾーン保護をアクティブにする：ゾーン全体に対してゾーン保護をアクティブにするには、Destination IP フィールドにアスタリスク（*）を入力するか、フィールドをブランクのままにします。

  ゾーンの Protect-IP state を Entire Zone または Policy type に設定する必要があります。
- リモート Guard 上で、ゾーンの IP アドレス範囲内の特定の IP アドレスのみ、ゾーン保護をアクティブにする：特定の IP アドレスに対してゾーン保護をアクティブにするには、Destination IP フィールドにその IP アドレスを入力します。

  ゾーンの Protect-IP state を Only Dst IP（宛先 IP アドレスのみ）に設定する必要があります。

リモート Guard リストは、CLI を使用しないと設定できません。CLI の使用の詳細については、『*Cisco Traffic Anomaly Detector Configuration Guide*』を参照してください。

ゾーンの Protect-IP state の詳細については、第 4 章「ゾーンの作成と設定」の「Guard ゾーンの設定」の項を参照してください。

動的フィルタを追加するには、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、検出中のゾーンを選択します。ゾーンのメイン メニューとゾーンのステータス画面が表示されます。

ステップ 2　次のいずれかの方法で、動的フィルタのリストを表示します。

- ゾーンのメイン メニューで **Detection > Dynamic filters** を選択します。
- ゾーン ステータス ページのゾーンのステータス テーブルで、**Active Dynamic filters** をクリックします。

Dynamic filters 画面が表示されます。

ステップ 3　**Add** をクリックします。Add Dynamic Filter 画面が表示されます。

ステップ 4　表 9-4 の説明に従って、動的フィルタのパラメータを定義します。

表 9-4　動的フィルタに含まれているフィールドの説明

フィールド	説明
Destination IP	Detector モジュールは、宛先 IP アドレスと、ゾーンに設定された Protect-IP state の値に基づいて、リモート Guard 上で保護をアクティブにします。ブランクのままにするか、すべての IP アドレスを表すアスタリスク（*）を入力します。
Action	トラフィックがフィルタに一致した場合に Detector モジュールが実行するアクション。Detector モジュールは、remote-activate アクションのみをサポートしています。このアクションでは、リモート Guard リストに定義したリモート Guard をアクティブにしてゾーンを保護できます。リモート Guard リストを設定するには CLI を使用します。Detector モジュールの CLI へのアクセスと使用の詳細については、『*Cisco Traffic Anomaly Detector Module Configuration Guide*』を参照してください。
Timeout (Sec)	フィルタがアクティブである最短時間。次のいずれかのフィルタ タイムアウト オプションを選択します。 • Forever チェックボックスをオンにして、無期限を指定します。 • seconds チェックボックスをオンにして、時間を秒単位で入力します。

ステップ 5　**OK** をクリックして動的フィルタをアクティブにします。

動的フィルタの削除

動的フィルタは削除できますが、フィルタの削除は限られた期間のみ有効です。これは、攻撃トラフィックの変化に従って Detector モジュールが新しい動的フィルタを設定し続けるからです。Detector モジュールが不要な動的フィルタを作成しないようにするには、「不要な動的フィルタの作成の防止」の項を参照してください。

動的フィルタを削除するには、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、検出実行中のゾーンを選択します。ゾーンのメイン メニューとゾーンのステータス画面が表示されます。

ステップ 2　次のいずれかの方法で、動的フィルタのリストを表示します。

- ゾーンのメイン メニューで **Detection > Dynamic filters** を選択します。
- ゾーンのステータス テーブルで **Active Dynamic filters** をクリックします。

Dynamic filters 画面が表示されます。

ステップ 3　削除する動的フィル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　**Delete** をクリックして、動的フィルタを削除します。

不要な動的フィルタの作成の防止

次のいずれかのアクションを実行して、Detector モジュールで不要な動的フィルタが作成されないよう防止できます。

- 動的フィルタを作成するポリシーを非アクティブにする。ポリシーの動作状態の変更の詳細については、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。動的フィルタのリストを表示して、不要な動的フィルタを作成したポリシーを特定するには、「動的フィルタのリストの表示」の項を参照してください。
- 目的のトラフィック フロー用のバイパス フィルタを設定する。バイパス フィルタの設定の詳細については、第 5 章「ゾーンのフィルタの設定」の「バイパス フィルタの管理」の項を参照してください。
- 不要な動的フィルタを作成したポリシーのしきい値を大きくする。ポリシーのしきい値の変更については、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。

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

ゾーン トラフィックの異常を検出するときに Detector モジュールが次のいずれかのモードで動作するよう設定することによって、ゾーンの動的フィルタのアクティベーションを制御できます。

- 自動検出モード：Detector モジュールは、ゾーンに対してフィルタを作成するとただちに動的フィルタをアクティブにします。この動作モードはデフォルトです。
- インタラクティブ検出モード：Detector モジュールは、ゾーンに対して作成する動的フィルタを自動的にアクティブにしません。代わりに、動的フィルタを保存し、推奨事項としてグループ化します。ユーザは、推奨事項を確認して、どの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決定します。

異常検出の動作モードは、ゾーンの設定の一部として設定します。動作モードの設定値は、ゾーンが攻撃を受けているときを含め、いつでも変更できます。

この項は、次の内容で構成されています。

自動検出モードのアクティブ化

ゾーンを自動検出モードでアクティブにするには、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 メニューとゾーンのステータス画面が表示されます。

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

ステップ 3　**Config** をクリックします。Config 画面が表示されます。

ステップ 4　Operation Mode パラメータ ドロップダウン リストから、**automatic** を選択します。

ステップ 5　**OK** をクリックします。Detector モジュールが、ゾーンの設定を新しい動作モード設定でアップデートします。ゾーンの動作が現在アクティブになっている場合、Detector モジュールは、すべての保留および新規の動的フィルタを自動的にアクティブにします。

インタラクティブ検出モードのアクティブ化

ゾーンをインタラクティブ検出モードでアクティブにするには、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 メニューとゾーンのステータス画面が表示されます。

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

ステップ 3　**Config** をクリックします。Config 画面が表示されます。

ステップ 4　Operation Mode パラメータ ドロップダウン リストから、**interactive** を選択します。

ステップ 5　**OK** をクリックします。Detector モジュールが、ゾーンの設定を新しい動作モード設定でアップデートします。異常の検出が現在アクティブになっている場合、Detector モジュールは攻撃を検出すると推奨事項を作成します。

保留動的フィルタの数が 1000 を超えた場合の対応

保留動的フィルタの数が 1000 を超えた場合、Detector モジュールは次のアクションを実行します。

- エラー　メッセージを表示して、ゾーンを非アクティブにしてから自動検出モードで再度アクティブにするよう指示する。
- 推奨事項をゾーンのログ ファイルに記録してから破棄する。

Detector モジュールの保留動的フィルタが 1000 個を超える場合にゾーン トラフィックの異常を検出するには、次の手順を実行してゾーンに自動検出モードを設定する必要があります。

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 メニューとゾーンのステータス画面が表示されます。

ステップ 2　**Deactivate** をクリックします。Detector モジュールは異常の検出を停止し、すべての保留動的フィルタを削除します。

ステップ 3　ゾーンのメイン メニューで **Configuration > General** を選択します。General 画面が表示されます。

ステップ 4　**Config** をクリックします。Config 画面が表示されます。

ステップ 5　Operation Mode ドロップダウン リストから **automatic** を選択し、**OK** をクリックします。ゾーンの設定が、新しい異常検出設定でアップデートされます。

ステップ 6　**Protect** をクリックします。Detector モジュールが自動検出モードの動作を開始し、動的フィルタを作成してそのすべてをアクティブにします。

動的フィルタに対する Detector モジュールの推奨事項の管理

インタラクティブ検出モードでゾーンの異常の検出を実行する場合、Detector モジュールは、攻撃の進行中に作成した動的フィルタのリストを生成します。このリストの動的フィルタは、*保留動的フィルタ*と呼ばれます。Detector モジュールは、保留動的フィルタを作成したポリシーに従って保留動的フィルタをグループ化し、Detector モジュールの*推奨事項*としてユーザに提示します。

この推奨事項は、保留フィルタの要約と、保留動的フィルタの作成の元になるポリシーの名前、ポリシーのアクティベーションの原因となったトラフィック異常に関するデータ、保留動的フィルタの数、および推奨アクションについての情報を提供します。ユーザは、Detector モジュールの推奨事項（関連付けられた保留動的フィルタをすべて含む）に対応することも、個々の保留動的フィルタに対応することもできます。

この項は、次の内容で構成されています。

推奨事項の表示

Detector モジュールでは、新しい推奨事項が使用可能になると、次の場所に推奨事項のアイコン  が表示されます。

- ナビゲーション ペインにある、**All Zones** リストのゾーン アイコンの隣
- ナビゲーション ペインにある、**Under Detection** リストのゾーン アイコンの隣
- ゾーン ステータス ページにあるゾーン ステータス バー
- ゾーン リストのテーブル

Detector モジュールに新しい推奨事項がある場合は、保留動的フィルタの数が 0 より大きくなっています。Detector モジュールは、ゾーン ステータス画面にある保留動的フィルタの数をゾーン ステータス テーブルに表示します。

Detector モジュールの推奨事項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 ペインでゾーンを選択します。ゾーンのメイン メニューとゾーンのステータス画面が表示されます。

ステップ 2　次のいずれかの方法で、推奨事項のリストを表示します。

- ゾーンのメイン メニューで **Detection > Recommendations** を選択します。
- ゾーン ステータス画面のゾーンのステータス テーブルで、**Pending Dynamic filters** をクリックします。

Recommendations 画面が表示されます。

表 9-5 に、推奨事項テーブルに含まれているフィールドの説明を示します。

表 9-5　推奨事項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
ID	Detector モジュールが推奨事項に割り当てた識別番号。
Recommendation	Detector モジュールが推奨するアクション。
Created By	フィルタを作成したポリシー。ポリシーの名前をクリックすると、ポリシーの詳細が表示されます。
# of PFs	推奨事項に関連付けられている保留動的フィルタの数。保留になっている各フィルタは、トラフィック フローがポリシーのしきい値を超過した結果、作成されたものです。数値をクリックすると、推奨事項に関連付けられている保留動的フィルタが表示されます。
Attack flow	攻撃フローに関する情報。攻撃フローに関する次の詳細が提供されます。 • **Src IP**：送信元 IP アドレス。 • **Protocol**：プロトコル番号。 • **Dst Port**：宛先ポート。 • **Dst IP**：宛先 IP アドレス。
Thr.	攻撃フローが超過した、ポリシーのしきい値。
Min.	攻撃レートの最小値。いくつかの保留フィルタを含んでいる推奨事項において、保留動的フィルタの最小のレートが表示されます。
Max.	攻撃レートの最大値。いくつかの保留フィルタを含んでいる推奨事項において、保留動的フィルタの最大のレートが表示されます。
Creation	推奨事項が作成された日時。

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、次の状態であることを示します。

- 値が特定されていない。
- パラメータに対して複数の値が測定されている。それぞれの値を表示するには、すべての保留動的フィルタのリストを確認します。

推奨事項の管理

Detector モジュールの推奨事項をアクティブにするかどうかを決定できます。すべての推奨事項、特定の推奨事項、または特定の保留動的フィルタに対して決定を適用できます。その決定により、ポリシーの保留動的フィルタが動的フィルタになるかどうか、およびその期間が決まります。

特定のポリシーの保留動的フィルタを自動的にアクティブにするよう、Detector モジュールに指示できます。また、ポリシーによって推奨事項が生成されないように Detector モジュールに指示することもできます。

Detector モジュールのポリシーは、ゾーンがインタラクティブ保護モードで、DDoS 攻撃が進行中の場合、推奨事項を継続して作成します。ゾーンのステータスを検証して、さらにアクションが必要かどうかを判断するために推奨事項を管理する場合、ゾーンのステータスを表示することをお勧めします。

推奨事項を管理するには、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 メニューとゾーンのステータス画面が表示されます。

ステップ 2　次のいずれかの方法で、推奨事項のリストを表示します。

- ゾーンのメイン メニューで **Detection > Recommendations** を選択します。
- ゾーン ステータス画面のゾーンのステータス テーブルで、**Pending Dynamic filters** をクリックします。

Recommendations 画面が表示されます。

ステップ 3　Filters timeout ボックスに、フィルタのタイムアウト値を秒単位で入力します。

ステップ 4　受け入れる推奨事項の隣にあるチェックボックスをオンにします。

ステップ 5　次のいずれかの必要なアクションを選択します。

- **accept**：特定の推奨事項を受け入れます。Detector モジュールは、該当の推奨事項に関連付けられている保留動的フィルタをアクティブにします。
- **always-accept**：特定の推奨事項を受け入れます。推奨ポリシーにより新しい推奨事項が生成されると、この決定は必ず自動的に適用されます。保留動的フィルタは、自動的に動的フィルタになります。このアクションを実行すると、Detector モジュールはそのような推奨事項を表示しなくなります。
- **always-ignore**：特定の推奨事項を無視します。動的フィルタも保留動的フィルタも作成されません。この決定は、ポリシーにより作成される将来のすべての推奨事項に自動的に適用されます。推奨事項を常に無視するように決定した場合、Detector モジュールは推奨事項を表示しなくなります。将来の攻撃でポリシーが推奨事項を作成しないようにするには、そのポリシーをディセーブルまたは非アクティブにします（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）。

（注）　特定の推奨事項への対応として決定した **always-ignore** は、その推奨事項の保留動的フィルタを作成したポリシーのインタラクティブ状態を変更することによって変更できます。

推奨事項に関連付けられている保留動的フィルタをすべて受け入れるのではなく、保留動的フィルタの一部を選択して受け入れることもできます。詳細については、「保留動的フィルタの受け入れ」の項を参照してください。

推奨事項の保留動的フィルタの表示

Detector モジュールの推奨事項に関連付けられている保留動的フィルタを表示するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューとゾーンのステータス画面が表示されます。

ステップ 2　次のいずれかの方法で、推奨事項のリストを表示します。

- ゾーンのメイン メニューで **Detection > Recommendations** を選択します。
- ゾーン ステータス画面のゾーンのステータス テーブルで、**Pending Dynamic filters** をクリックします。

Recommendations 画面が表示されます。

ステップ 3　推奨事項の # of PFs（Pending Filters; 保留中のフィルタ）カラムに表示されている数値をクリックします。Pending dynamic filters 画面が表示されます。

表 9-6 に、保留動的フィルタのテーブルに含まれているフィールドの説明を示します。

表 9-6　保留動的フィルタに含まれているフィールドの説明

フィールド	説明
Created by	フィルタを作成したポリシー。ポリシーの名前をクリックすると、ポリシーの詳細が表示されます。詳細については、第 8 章「ゾーンのポリシーの管理」を参照してください。
Activation	フィルタが作成された日時。
Src IP	攻撃ストリームの送信元 IP アドレス。
Protocol	攻撃ストリームのプロトコル番号。
Dst Port	攻撃ストリームの宛先ポート。
Fragments	フィルタの断片化設定で、攻撃ストリームの中に断片化されたパケットが含まれているかどうかを示します。
Action	フィルタが実行するアクション。
Recent rate	フィルタによって測定された現在の攻撃レート。
Rate (pps)	トリガー レート。保留動的フィルタ作成の原因となった攻撃の概算レート。
Details	このフィルタに関する追加情報が存在するかどうかのステータス。**i** をクリックすると、追加情報が表示されます。

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、次の状態であることを示します。

- 値が特定されていない。
- フィルタのパラメータに対して複数の値が測定された。

Detector モジュールでは、ポリシーが作成した保留動的フィルタは少なくともユーザが定義した期間中（フィルタ タイムアウト）はアクティブになります。

保留動的フィルタの詳細の表示

動的フィルタの詳細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 メニューとゾーンのステータス画面が表示されます。

ステップ 2　次のいずれかの方法で、推奨事項のリストを表示します。

- ゾーンのメイン メニューで **Detection > Recommendations** を選択します。
- ゾーン ステータス画面のゾーンのステータス テーブルで、**Pending Dynamic filters** をクリックします。

Recommendations 画面が表示されます。

ステップ 3　推奨事項の # of PFs（Pending Filters; 保留中のフィルタ）カラムに表示されている数値をクリックします。Pending Dynamic Filters 画面が表示されます。

ステップ 4　保留動的フィルタの Details カラムにある **i** をクリックします。Filter Details 画面が表示されます。

Filter Details 画面には、次の情報を表示する 3 つのテーブルがあります。

- フィルタを作成したポリシー。
- 攻撃フロー。
- フィルタ作成のトリガー（攻撃フローが超過したポリシーのしきい値、およびフィルタ作成の原因となった攻撃の概算レートを表示）。

保留動的フィルタの受け入れ

保留動的フィルタを選択的に受け入れるには、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 メニューとゾーンのステータス画面が表示されます。

ステップ 2　次のいずれかの方法で、推奨事項のリストを表示します。

- ゾーンのメイン メニューで **Detection > Recommendations** を選択します。
- ゾーン ステータス画面のゾーンのステータス テーブルで、**Pending Dynamic filters** をクリックします。

Recommendations 画面が表示されます。

ステップ 3　推奨事項の # of PFs（Pending Filters; 保留中のフィルタ）カラムに表示されている数値をクリックします。Pending Dynamic Filters 画面が表示されます。

ステップ 4　Filters timeout ボックスに、動的フィルタのタイムアウト値を秒単位で入力します。

ステップ 5　アクティブにする保留動的フィル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 6　**Accept** をクリックして保留動的フィルタをアクティブにします。
