異常の検出のアクティブ化

ゾーンの異常検出をアクティブにすると、Detector は取得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るポリシーのしきい値の超過（攻撃を示すもの）が発生し、ポリシーのアクションがトリガーされると、Detector はユーザに通知を送信するか、Cisco Guard をアクティブにします。この章では、WBM を使用してゾーンの異常の検出をアクティブにし、管理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。

異常の検出のオプション

Detector には、異常検出を実行するための複数のオプションが用意されています。たとえば、異常検出処理のあらゆる面を Detector で管理することも、ユーザが攻撃の進行中に自分で Detector を監視し、指示を出すこともできます。

この項は、異常の検出に関する次の情報で構成されています。

Detect と Detect and Learn

WBM を使用してゾーンの異常検出を手動でアクティブにする場合、Detector では次のオプションを選択できます。

- Detect：Detector は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：Detector はゾーンのトラフィックに異常がない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。Detector は、しきい値調整フェーズのためのトラフィック分析を実行しながら、ゾーンの設定のポリシーのしきい値を新しいしきい値の情報に合せて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すると、Detector はしきい値調整フェーズを一時停止します。ゾーンへの攻撃が終了すると、Detector は異常の検出に加えてしきい値調整フェーズを再開します。

自動動作モードとインタラクティブ動作モード

攻撃の進行中に、Detector は 2 つの動作モードのいずれかで動作し、作成した動的フィルタを自動的にアクティブにするか、または動的フィルタをアクティブにするかどうかをユーザが決定するのを待ちます。ゾーンの設定を定義するときに、次のいずれかの設定を選択して、Detector の動作モードを設定します。

- **Automatic operation mode** : Detector は、作成した動的フィルタをユーザの操作なしでアクティブにします。
- **Interactive operation mode** : Detector が作成した動的フィルタをアクティブにするか無視するかをユーザが選択します。インタラクティブ動作モードを使用すると、Detector で攻撃の分析と提案された動的フィルタのキューイングを継続しながら、ユーザが異常の検出措置を決定することができます。

ゾーンの設定の動作モード設定値は、いつでも変更することができます。

異常の検出の管理

この項の手順では、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。

この項では、次の手順について説明します。

異常の検出のアクティブ化

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。

- ゾーンのステータス画面の **Detect & Learn** または **Detect** をクリックします。
- ゾーンのメイン メニューの **Detection > Detect** を選択します。

次の処理が実行されます。

- Detector が、トラフィック異常についてトラフィック フローの分析を開始します。
- ゾーンの名前が、ナビゲーション ペインの Under Detection ゾーン リストに追加されます。
- ゾーンのステータス アイコンが、スタンバイ  から検出  に変更されます。
- 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 タイプが表示されます。
- Traffic Rate テーブルの受信トラフィック レートが 0 より大きい値を示します。

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、検出実行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、異常の検出を非アクティブにします。

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

次の処理が実行されます。

- Detector はゾーンのトラフィックの分析を停止します。
- ゾーンの名前が、ナビゲーション ペインの Protected Zones リストから削除されます。
- ゾーンのステータス アイコンが、検出  からスタンバイ  に変更されます。
- Recent Events テーブルに、検出が実行されていないゾーンの詳細なリストとともに、検出停止のイベント タイプが表示されます。

動的フィルタの管理

Detector はゾーンの異常の検出をアクティブにした後、動的フィルタだけを作成し、Detector は攻撃を検出します。したがって、ゾーン上で攻撃が発生したとき、動的フィルタの表示および管理だけを実行できます。

攻撃中に手動でゾーンの異常の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 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。

この項では、次の手順について説明します。

- 動的フィルタのリストの表示
- 動的フィルタの詳細の表示
- 動的フィルタの追加
- 動的フィルタの削除
- 不要な動的フィルタの作成の防止

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 メニューの **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。

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基づいてフィルタリングされた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 9-1 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 9-1　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発信元 IP アドレスを指定します。
Dst IP	動的フィルタの適用対象となる宛先 IP アドレス。 Detector は、宛先 IP アドレスに基づいた Cisco Guard 上の保護とゾーンに対して設定された Protect-IP state の値をアクティブ化します。
Protocol	フィルタが処理するトラフィックのプロトコル番号を指定します。
Dst Port	フィルタが処理するトラフィックの宛先ポートを指定します。
Fragments	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	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 レートを pps で指定します。
Details	このフィルタに関する追加情報が存在す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。

任意のパラメータの * という値は、次のいずれかを示します。

- 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。

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 メニューの **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　目的の動的フィルタの 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 つのテーブルが含まれています。

- 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 9-2 に、トリガーのパラメータの説明を示します。

表 9-2　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	ポリシーで定義され、攻撃によって超過したしきい値。
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の検出を実行することができます。リモート Guard リスト（リモート Guard）でゾーンを保護するために定義された Cisco Guard をアクティブにする動的フィルタを設定できます。動的フィルタの宛先 IP アドレスは、Protect-IP state およびゾーンに対して設定されたアドレス範囲に一致している必要があります。一致していなければ、リモート アクティベーションは失敗します。次のいずれかの方法を使用すると、リモート Guard 上の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。

- ゾーン全体に対するリモート Guard 上のゾーン保護のアクティブ化 : ゾーン全体に対するゾーン保護をアクティブにするには、Destination IP フィールドをブランクのままにするか、アスタリスクを入力します。

  ゾーンの Protect-IP state に Entire Zone または Policy タイプを設定する必要があります。
- ゾーン IP アドレス範囲内にある特定の IP アドレスに対するリモート Guard 上のゾーン保護のアクティブ化 : 特定の IP アドレスに対するゾーン保護をアクティブ化するには、Destination IP フィールドに IP アドレスを入力します。

  ゾーンの Protect-IP state に Only Dst IP を設定する必要があります。

CLI を使用した場合に限り、リモート Guard リストを設定できます。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 Protect-IP state の詳細については、P.4-7 の「ゾーン テンプレートからのゾーンの作成」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 メニューの **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。

表 9-3 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 9-3　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 は、Destination IP アドレスに基づいたリモート Guard 上の保護とゾーンに対して設定された Protect-IP state の値をアクティブ化します。ブランクのままにするか、「すべて」を表すアスタリスク（*) を入力します。
Action	特定のトラフィック タイプに対してフィルタが実行するアクションを指定します。フィルタのアクションを Action ドロップダウン リストから選択します。 • **remote-activate :** Detector は、リモート Guard リストでゾーンを保護するために定義されたリモート Guards をアクティブ化します。リモート Guard リストを設定するには、CLI を使用します。Detector の CLI へのアクセスと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。
Timeout (Sec)	フィルタがアクティブである最低限の時間。次のいずれかのオプションを選択します。 • 無期限の場合は、Forever チェックボックスをオンにします。 • 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 4　**OK** をクリックします。Detector が動的フィルタを保存し、アクティブ化します。

動的フィルタの削除

すべての動的フィルタを削除することは可能ですが、削除が有効である期間は限られています。これは、Detector が攻撃の進行中に動的に変化するトラフィックの状態に合せて新しい動的フィルタを設定し続けるためです。

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 メニューの **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　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** をクリックします。Detector により、動的フィルタが削除されます。

不要な動的フィルタの作成の防止

Detector で不要な動的フィルタが作成されないようにするには、次の方法があります。

- 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発見するには、「動的フィルタのリストの表示」の項を参照してください。
- 対象となるトラフィック フローにバイパス 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。

Detector の動的フィルタの推奨事項の管理

インタラクティブ検出モードで異常の検出を実行する場合、Detector は攻撃中に作成する動的フィルタのキューを作成します。キューイングされた動的フィルタは、保留動的フィルタと呼ばれます。Detector は、その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 の推奨事項*としてユーザに表示します。ユーザは、Detector の推奨事項（関連付けられているすべての保留動的フィルタも含めて）に対応することも、各保留動的フィルタに個別に対応することもできます。

この項では、次の手順について説明します。

Detector の推奨事項の表示

Detector では、新しい推奨事項が使用可能になると、Detector の推奨事項アイコン  が表示されます。このアイコンは、次の位置に表示されます。

- 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、Protected Zones 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 に新しい推奨事項がある場合は、ゾーンのステータス画面に表示される保留動的フィルタの数が 0 より大きくなります。

Detector 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 メニューの **Detection > Recommendations** を選択します。
- ゾーンのステータス画面のゾーン ステータス テーブルで、ゾーンのステータス要約にある **Pending Dynamic filters** をクリックします。

Recommendations 画面が表示されます。

表 9-4 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 9-4　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 が推奨事項に割り当てた識別番号。
Recommendation	Detector 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	推奨事項を構成し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。次の情報が提供されます。 • 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。 • Dst IP：攻撃ストリームの宛先 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。いくつかの保留中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。

表 9-4　推奨事項テーブルに含まれているフィールドの説明（続き）

フィールド	説明
Max.	攻撃レートの最大値。いくつかの保留中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。

パラメータの値が * となっている場合は、次のいずれかの状態であることを示します。

- Detector で値を決定できない。
- Detector でそのフィルタのパラメータとして複数の値が測定された。異なる値を表示するには、すべての保留動的フィルタのリストを確認します。

Detector 推奨事項の表示と推奨事項への対応

Detector 推奨事項を表示して推奨事項に対応するには、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 メニューの **Detection > Recommendations** を選択します。
- ゾーンのステータス画面のゾーン ステータス テーブルで、ゾーンのステータス要約にある **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（秒）を入力します。

ステップ 4　目的の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　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 は、その推奨事項に関連付けられた保留動的フィルタをアクティブにします。
- **always-accept**：特定の推奨事項を常に受け入れます。現在の攻撃の間、Detector はその推奨事項を作成したポリシーの推奨事項を自動的に受け入れます。Detector は、**always-accept** 推奨事項を表示しません。
- **always-ignore**：特定の推奨事項を常に無視します。現在の攻撃の間、Detector はその推奨事項を作成したポリシーの推奨事項を自動的に無視します。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）。

  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。

必要に応じて、推奨事項に関連付けられている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 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 メニューの **Detection > Recommendations** を選択します。
- ゾーンのステータス画面のゾーン ステータス テーブルで、ゾーンのステータス要約にある **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　目的の推奨事項の # 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 9-5 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 9-5　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	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。動的フィルタの作成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。

パラメータの値が * となっている場合は、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。
- 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 では、ポリシーが作成した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 メニューの **Detection > Recommendations** を選択します。
- ゾーンのステータス画面のゾーン ステータス テーブルで、ゾーンのステータス要約にある **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　目的の推奨事項の # 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　目的の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。

保留動的フィルタの詳細には、次の情報を表示する 3 つのテーブルが含まれています。

- 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。このテーブルには、攻撃トラフィック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が表示されます。

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 メニューの **Detection > Recommendations** を選択します。
- ゾーンのステータス画面のゾーン ステータス テーブルで、ゾーンのステータス要約にある **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　目的の推奨事項の # 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（秒）を入力します。

ステップ 5　目的の保留動的フィルタ（アクティブにするフィルタ）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** をクリックします。Detector が、選択した保留動的フィルタをアクティブにします。

Detector がゾーンの異常の検出を実行する方法の設定

Detector がゾーンに対する攻撃を検出したときに、どのように動的フィルタをアクティブにするかを設定できます。Detector は、次のいずれかのモードで動作するように設定できます。

- 自動検出モード：Detector は、動的フィルタを作成するとそれらをすべてアクティブにします。
- インタラクティブ検出モード：ユーザは、Detector が攻撃の進行中に作成する動的フィルタの推奨事項に対応する必要があります。Detector の推奨事項をアクティブにするか、無視することができます。

ゾーンの検出モードは、ゾーンの設定の一部として設定します。ゾーンの検出モードの設定は、Detector がゾーンへの攻撃を管理している間も含めて、いつでも変更できます。

この項は、次の情報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 メニューの **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 parameter 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 が、新しい動作モード設定で、ゾーンの設定をアップデートします。その時点でゾーンの動作がアクティブである場合、Detector は保留されている動的フィルタと新しい動的フィルタをすべて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 メニューの **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 parameter 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 が、新しい動作モード設定で、ゾーンの設定をアップデートします。その時点で異常の検出がアクティブである場合、Detector 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 1,000 を超えた場合の対応

ゾーンのステータス画面に表示される保留動的フィルタの数が 1,000 を超えると、Detector は推奨事項の情報をログ ファイルに記録してから、新しい推奨事項の廃棄を開始します。保留動的フィルタの数が 1,000 フィルタを超えた場合は、Detector が実行するゾーンの異常の検出の方法を自動検出モードに変更することをお勧めします。自動検出モードで動作する場合、Detector は動的フィルタを作成するとそれらをすべてアクティブにします。

（注）　保留動的フィルタの数が 1,000 フィルタを超えた場合は、まず、異常の検出を非アクティブにする必要があります。Detector が実行する異常の検出の方法を変更する前に異常の検出を非アクティブにする必要があるのは、この場合のみです。

保留動的フィルタの数が 1,000 フィルタを超えた場合に、Detector が実行する異常検出の方法を自動検出モードに変更するには、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　**Deactivate** をクリックします。Detector 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 メニューの **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 parameter ドロップダウン リストから、**automatic** を選択します。

ステップ 6　**OK** をクリックします。ゾーンの設定が、新しい保護モード設定でアップデートされます。

ステップ 7　**Protect** をクリックします。Detector はゾーンの自動動作を開始し、動的フィルタを作成するとそれらをすべてアクティブにします。