ゾーン保護のアクティブ化

ゾーン保護は、Cisco Guard 上で次の 2 つの方法のいずれかでアクティブにできます。

- Cisco Traffic Anomaly Detector などの外部トリガー デバイスを使用して、自動的にアクティブにする
- Guard の CLI または WBM を使用して、手動でアクティブにする

ゾーンをどのように設定したかに応じて、Guard は、ゾーン名や、宛先変更されたトラフィックから抽出する情報に基づいてゾーン保護をアクティブにします。保護をアクティブにする方式として、次のものを使用できます。

- ゾーン名 : Guard は、ゾーン名に基づいてゾーン保護をアクティブにします。
- IP アドレス : Guard は、ゾーンの一部である IP アドレスまたはサブネットで構成された外部からの攻撃の兆候を受信した場合に、ゾーン保護をアクティブにします。
- パケット : Guard は、データベースでゾーンのパケットを受信した場合に、ゾーン保護をアクティブにします。
- IP アドレスまたはパケット : Guard は、ゾーンを宛先とするトラフィック（パケット）を受信した場合、またはゾーンのアドレス範囲の一部である IP アドレスまたはサブネットで構成される外部からの攻撃の兆候を受信した場合に、ゾーン保護をアクティブにします。

保護のアクティベーション方法の詳細については、第 4 章「ゾーンの作成と設定」の「保護のアクティベーション方式」の項を参照してください。

ゾーン保護がアクティブになると、Guard はゾーンのポリシーをトラフィック フローに適用します。異常なトラフィックがポリシーのしきい値を超過して（攻撃があったことを示す）、ポリシーのアクションが実行されると、Guard は動的フィルタの作成を開始して攻撃を管理します。Guard は、当該トラフィックのための動的フィルタを作成する必要がなくなると、攻撃が終了したと判断します。

この章では、WBM を使用して Guard 上でゾーン保護をアクティブにし、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。

- ゾーン保護のオプション
- ゾーン保護の管理
- 動的フィルタの管理
- ゾーンの動作モードの変更

ゾーン保護のオプション

Guard には、ゾーン保護を実行するためのオプションが複数用意されています。たとえば、Guard にゾーン保護動作のすべての面を管理させることも、攻撃の進行中に Guard を監視して指示を与えることもできます。

この項では、ゾーン保護に関する次の情報について説明します。

- オンデマンド保護
- Protect および Protect and Learn
- 自動およびインタラクティブ ゾーン動作モード

オンデマンド保護

オンデマンド保護は、ゾーンの定義後すぐに Guard が提供するタイプの保護です。ゾーン定義プロセスを開始するために選択するゾーン テンプレートには、一連の定義済みのポリシーおよびオンデマンド保護のユーザ フィルタが含まれています。次の状況の場合、ゾーン保護にはオンデマンド保護を使用します。

- Guard にラーニング プロセスを実行させる時間がない場合
- ラーニング プロセス中にゾーンで攻撃が発生した場合

ゾーン テンプレートのポリシーのデフォルトしきい値は、Guard がトラフィックの異常を識別したときに、Guard のスプーフィング防止機能がすぐにアクティブになる値に設定されています。Guard は、オンデマンド保護を使用しているときはゾーンのトラフィックをラーニングしないため、Guard はゾーンのトラフィック パターンに関する知識を特に持っていません。そのため、送信元 IP アドレスからのトラフィックのブロック（ドロップ）に使用されるしきい値は、比較的高い値に設定されています。Guard がゾーンのトラフィックに関する知識を特に持たないため、オンデマンド保護では、スプーフィングを利用しない攻撃を軽減する場合にはユーザの介入が必要になります。オンデマンド保護を使用するゾーンに対して攻撃が進行している間は、ゾーンの正当なトラフィックと悪意のあるトラフィックのレートを監視して、Guard の軽減アクションを確認してください。

ゾーンのトラフィックを Guard がラーニングすることを許可した場合、Guard は、オンデマンド保護に使用されるゾーンの設定のポリシーを、ゾーン用に個別に作成するポリシーで置き換えます。

Protect および Protect and Learn

WBM を使用してゾーン保護を手動でアクティブにすると、Guard で次のゾーン保護オプションを利用できるようになります。

- Protect : Guard 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。
- Protect and Learn : Guard は、ゾーンのトラフィックに異常がないかどうかを分析すると同時に、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でトラフィックを分析しながら、Guard はゾーン設定のポリシーのしきい値を新しいしきい値情報で自動的に調整します。Guard は、トラフィックの分析中に攻撃を検出すると、攻撃を管理している間、しきい値調整フェーズを一時停止します。ゾーンに対する攻撃が終了すると、Guard はしきい値調整フェーズをゾーン保護とともに再開します。

自動およびインタラクティブ ゾーン動作モード

攻撃の進行中、Guard は 2 つの動作モードのいずれかで動作します。作成する動的フィルタを自動的にアクティブにするモードと、動的フィルタをアクティブにするかどうかをシステム管理者が決定するまで待機するモードです。ゾーン設定を定義する場合、次のいずれかの設定を選択して、ゾーンの動作モードを設定します。

- **Automatic operation mode** : Guard は、作成する動的フィルタをユーザの操作なしで自動的にアクティブにします。
- **Interactive operation mode** : Guard が推奨する動的フィルタをアクティブにするか、無視するかについて、システム管理者が選択します。インタラクティブ ゾーン動作モードを使用すると、Guard が継続的に攻撃を分析し、提案される動的フィルタをキューイングするので、ゾーン保護の手段をシステム管理者が決定できます。

ゾーン設定のゾーンの動作モード設定は、いつでも変更することができます。

ゾーン保護の管理

この項では、ゾーン保護を手動でアクティブ化または非アクティブ化する手順について説明します。また、ゾーン保護をアクティブ化した後でトラフィックの宛先変更および保護を確認できる情報についても説明します。

この項では、次の手順について説明します。

ゾーン保護のアクティブ化

ゾーン保護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、ゾーン保護をアクティブにします。

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

次の処理が実行されます。

- Guard　は、ゾーン　トラフィックを自身に宛先変更し、異常についてトラフィック フローの分析を開始します。正当なトラフィックは、その目的の宛先へと転送されるネットワークに再び注入されます。悪意のあるトラフィックは Guard によってフィルタリングされ、ドロップされます。
- 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  から保護  に変更されます。
- Recent Events テーブルに、保護されるゾーンの詳細なリストとともに、保護開始のイベント タイプが表示されます。

オンデマンド保護のアクティブ化

オンデマンド保護を使用すると、Guard がゾーン固有のトラフィック パターンをラーニングして必要な変更をゾーンの設定に加える前でも、ゾーンを保護することができます。オンデマンド保護を使用する場合、選択するゾーン テンプレートのデフォルト設定値を使用して、攻撃を処理する新しいゾーンを特別に作成します。次のいずれかの状況に当てはまる場合、ゾーンのオンデマンド保護が必要となることがあります。

- Guard が、ラーニング プロセスのポリシー構築またはしきい値調整を実行中である
- Guard が Protect and Learn モードにあるが、ゾーンのトラフィック特性をまだラーニングしていない
- ゾーンのトラフィックを表さないと判断したポリシーのしきい値を受け入れている

オンデマンド保護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　攻撃を処理する新しいゾーンを作成します（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）。

ステップ 2　ナビゲーション　ペインで、作成した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 3　次のいずれかの方法で、ゾーン保護をアクティブにします。

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

次の処理が実行されます。

- Guard　は、ゾーン　トラフィックを自身に宛先変更し、異常についてトラフィック フローの分析を開始します。正当なトラフィックは、その目的の宛先へと転送されるネットワークに再び注入されます。悪意のあるトラフィックは Guard によってフィルタリングされ、ドロップされます。
- 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  から保護  に変更されます。

- Recent Events テーブルに、保護されるゾーンの詳細なリストとともに、保護開始のイベント タイプが表示されます。

ステップ 4　ゾーンのトラフィック パターンを分析します（第 10 章「Guard およびゾーンの動作の監視」の「ゾーンのカウンタの表示」の項を参照）。

ゾーン トラフィックの宛先変更および保護の確認

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、ゾーンのトラフィックが正常に Guard に宛先変更され、保護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。

ゾーンのステータス画面を表示するには、ナビゲーション ペインでゾーンをクリックします。ゾーンのステータス画面に次の項目が表示される場合、トラフィックの宛先変更が機能しています。

- Traffic Rate テーブルの正当なトラフィック レートが 0 より大きい値を示します。
- Recent Events テーブルに、保護されるゾーンの詳細なリストとともに、保護開始のイベント タイプが表示されます。

悪意のあるトラフィック レートが 0 より大きい場合、攻撃が進行中であることを示します。攻撃の進行中にゾーン保護が適切に機能していることを確認するには、ゾーンのステータス画面で次のことを確認します。

- ゾーンのステータス　テーブルに示されているアクティブな動的フィルタの数が 0 より大きい。
- Traffic Rate テーブルに示されている正当なトラフィック レートが 0 より大きい。

ゾーンに対する攻撃がなく、疑わしいトラフィックの兆候もない場合、Guard はすべての宛先変更されたトラフィックを正当なトラフィックと見なし、ゾーンに転送します。正当なトラフィックのカウンタは、その後 Received トラフィック カウンタと同じになります。Received トラフィック カウンタの表示、およびその他の Guard 診断ツールの使用の詳細については、第 10 章「Guard およびゾーンの動作の監視」を参照してください。

ゾーン保護の非アクティブ化

ゾーンに対する攻撃がなく、ゾーンの異常の検出を他のソースに依存しているときは、ゾーン保護を非アクティブにして、Guard へのトラフィックの宛先変更を終了することができます。

ゾーン保護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、保護されている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　ゾーンのステータス画面および攻撃レポート画面で、ゾーン保護を非アクティブにする前に、ゾーンが現在攻撃されていないことを確認します。

ステップ 3　次のいずれかの方法で、ゾーン保護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 **Protection > Deactivate** を選択します。

次の処理が実行されます。

- Guard は、ゾーン トラフィックの自身への宛先変更を停止します。
- 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、保護  からスタンバイ  に変更されます。
- Recent Events テーブルに、保護されないゾーンの詳細なリストとともに、保護停止のイベント タイプが表示されます。

動的フィルタの管理

Guard が動的フィルタを作成するのは、システム管理者がゾーン保護をアクティブにし、Guard がトラフィックの異常を検出した後のみです。このため、保護されているゾーンで攻撃が発生している場合、動的フィルタの表示および管理だけを実行できます。

動的フィルタは有効期間が限定されています。動的フィルタのタイムアウトが満了すると、Guard は動的フィルタを非アクティブにするかどうかを決定します。Guard が動的フィルタを非アクティブにしないと決定した場合、フィルタのアクティベーション タイムアウトが新たにゼロから再びカウントされます。Guard は、次のいずれかの条件に当てはまる場合、動的フィルタを非アクティブにします。

- ゾーンにおける悪意のあるトラフィックの合計レート（スプーフィングされたトラフィックとドロップされたトラフィックの合計）が、Malicious-rate termination threshold 以下である。
- 動的フィルタのアクションが to-user-filter でない（フィルタのレート カウンタに N/A と表示されていない）場合で、Filter-rate termination threshold が次の両方の値以上である。
  - 動的フィルタの現在のトラフィック レート
  - ユーザが設定した期間内における動的フィルタの平均トラフィック レート

攻撃中に手動でゾーン保護を制御するには、攻撃中に動的フィルタを追加または削除します。Guard 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、保護されている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 **Protection > 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
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。
Activation	フィルタがアクティブになった日時。
Expiration	フィルタの満了時間。フィルタの有効期限が満了すると、Guard は動的フィルタの終了基準に従って、その動的フィルタを非アクティブにするかどうかを決定します。Guard でその動的フィルタがまだ必要となる場合、動的フィルタは次の期限まで引き続きアクティブになります。
Src IP	動的フィルタの適用対象となる送信元 IP アドレス。
Protocol	動的フィルタの適用対象となるプロトコルの番号。
Dst Port	動的フィルタの適用対象となる宛先ポート。
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。

表 9-1　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（続き）

フィールド	説明
Action	フィルタが実行するアクション。動的フィルタには、次のアクションが適用されます。 • **to-user-filters**：トラフィックをユーザ フィルタに転送します。デフォルトのユーザ フィルタを変更した場合は、これらの動的フィルタを処理するユーザ フィルタが存在することを確認してください。 • **filter/strong**：特定のトラフィックに強力な保護スプーフィング防止メカニズムを適用します。 • **filter/drop**：トラフィックをドロップします。 • **block-unauthenticated-basic**：基本的なスプーフィング防止メカニズムを拡張して、認証されなかったトラフィック フローをドロップします。 • **block-unauthenticated-strong**：強力なスプーフィング防止メカニズムを拡張して、認証されなかったトラフィック フローをドロップします。 • **block-unauthenticated-dns**：DNS スプーフィング防止メカニズムにより未認証と定義された、DNS UDP サーバ（プロトコル =UDP、ポート =53）宛てのトラフィック フローをドロップします。 • **redirect/zombie**：ポリシーは、**basic/redirect** のアクションが指定されたすべてのユーザ フィルタの認証を拡張します。
Rate (pps)	攻撃の概算レート（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。

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。

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、保護されている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 **Protection > Dynamic filters** を選択します。
- ゾーンのステータス ページにある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。このリンクは、アクティブな動的フィルタがある場合のみ有効となります。

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、次の攻撃情報に関する説明を示す 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。
- 軽減された攻撃。軽減されたフローは、検出された攻撃フローよりも範囲が広い可能性があります。たとえば、ポート 80 に対するスプーフィング以外の攻撃では、ポート 80 だけでなく、送信元 IP から発信されるすべての TCP トラフィックがブロックされます。
- フィルタを作成したトリガー。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	攻撃トラフィックが超過した、ポリシーのしきい値。
Triggering rate	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保護を実行することができます。

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、保護されている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 **Protection > 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
Source IP	特定の IP アドレスから送信されるトラフィックを動的フィルタに転送します。ブランクのままにするか、「すべて」を表す * を入力します。
Source Subnet	特定のサブネットで送信されるトラフィックを動的フィルタに転送します。サブネットを Source Subnet ドロップダウン リストから選択します。
Protocol	特定のプロトコルで送信されるトラフィックを動的フィルタに転送します。プロトコルはプロトコル番号で指定します。ブランクのままにするか、「すべて」を表す * を入力します。

表 9-3　動的フィルタに含まれているフィールドの説明（続き）

フィールド	説明
Dst Port	特定のポートを宛先とするトラフィックを動的フィルタに転送します。ブランクのままにするか、「すべて」を表す * を入力します。
Fragments	フィルタの操作対象となる特定のトラフィック タイプを指定します。Fragments ドロップダウン リストで、目的のトラフィック タイプを次のいずれかから選択します。 • **without**：動的フィルタは、断片化されていないトラフィックに対して作用します。 • **with**：動的フィルタは、断片化されているトラフィックに対して作用します。 • *：動的フィルタは、断片化されているトラフィックおよび断片化されていないトラフィックに対して作用します。
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。 • **to-user-filters**：特定のトラフィックをユーザが設定したユーザ フィルタに転送します。 • **filter/strong**：指定したトラフィックに強化保護レベルを適用します。 • **filter/drop**：トラフィックをドロップします。 • **block-unauthenticated-basic**：基本保護レベルで認証されなかった未認証のトラフィック フローをドロップします。 • **block-unauthenticated-strong**：強化保護レベルで認証されなかった未認証のトラフィック フローをドロップします。 • **block-unauthenticated-dns**：DNS スプーフィング防止機能で認証されていない、DNS サーバ宛ての未認証トラフィック フローをドロップします。 • **redirect/zombie**：ポリシーは、すべてのユーザ フィルタの認証を拡張し、リダイレクト アクションを備えるフィルタを追加します。

表 9-3　動的フィルタに含まれているフィールドの説明（続き）

フィールド	説明
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　次のいずれかのオプションを選択します。

- **OK**：動的フィルタの情報を保存します。Guard が新しい動的フィルタをアクティブにします。
- **Cancel**：情報を保存せずに Add Dynamic filter 画面を終了します。Dynamic Filters 画面が表示されます。

動的フィルタの削除

動的フィルタを削除すると、Guard が動的フィルタのアクションをトラフィック フローに適用することを防止できます。攻撃のトラフィック フローで変更がある場合、Guard が新しい動的フィルタを設定し続けるため、動的フィルタの削除が有効である期間は限られています。Guard 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、保護されている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、動的フィルタを表示します。

- ゾーンのメイン メニューの **Protection > Dynamic filters** を選択します。
- ゾーンのステータス画面にある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。Guard が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

ゾーンに転送する必要のあるトラフィックに Guard が動的フィルタを適用している場合は、次のいずれかの操作を実行すると、Guard が不要な動的フィルタを作成することを防止できます。

- 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）。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。
- 目的のトラフィック　フロー用のバイパス　フィルタを設定します（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）。
- 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）。

Guard の動的フィルタ推奨事項の管理

ゾーン保護をインタラクティブ動作モードで実行すると、Guard は、攻撃の進行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。Guard は、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、*Guard 推奨事項*として提示します。Guard 推奨事項（推奨事項に関連付けられているすべての保留動的フィルタを含む）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。

Guard 推奨事項の表示

Guard は、新しい推奨事項が参照可能になると Guard 推奨事項のアイコン  を表示します。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

Guard 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 を超えています。

Guard 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 **Protection > 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	Guard が推奨事項に割り当てた識別番号。
Recommendation	Guard が推奨しているアクション。
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。

- Guard が値を特定できない。
- Guard が、フィルタのパラメータに対して複数の値を測定した。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。

Guard 推奨事項の表示と推奨事項への対応

Guard 推奨事項のリスト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 **Protection > 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。Guard は、こ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**：特定の推奨事項を常に受け入れます。現在の攻撃が進行している間、Guard は、こ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。Guard 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。現在の攻撃が進行している間、Guard は、こ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、「推奨事項の保留動的フィルタの表示」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

Guard 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 **Protection > 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。

Guard 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 **Protection > 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

保留動的フィルタの一部を選択して受け入れるには、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 **Protection > 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。Guard が、選択した保留動的フィルタをアクティブにします。

ゾーンの動作モードの変更

ゾーンに対する攻撃を管理しているときの Guard の動作モードによって、動的フィルタが攻撃の進行中にどのようにアクティブになるかが決まります。Guard は、次のいずれかの動作モードで動作するように設定できます。

- 自動動作モード：Guard は、作成する動的フィルタをすべてアクティブにします。
- インタラクティブ動作モード：攻撃の進行中に Guard が作成する動的フィルタ推奨事項に対応する必要があります。Guard 推奨事項をアクティブ化または無視できます。

ゾーンの動作モードは、ゾーンの設定の一部として設定します。ゾーンの動作モードの設定は、Guard がゾーンに対する攻撃を管理しているときを含めて、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。

ゾーン動作モードの自動への変更

ゾーンの動作モード設定をインタラクティブから自動に変更するには、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　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。Guard が、ゾーンの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。ゾーン保護がアクティブになっている場合、Guard はすべての保留動的フィルタと新しい動的フィルタを自動的にアクティブにします。

ゾーン動作モードのインタラクティブへの変更

ゾーンの動作モード設定を自動からインタラクティブに変更するには、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　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。Guard が、ゾーンの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。ゾーン保護がアクティブになっている場合、Guard は攻撃が検出され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

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、Guard は推奨事項の情報をログ ファイルに記録してから、新しい推奨事項を廃棄し始めます。保留動的フィルタの数が 1,000 フィルタを超える場合は、ゾーンの動作モードを自動に変更することをお勧めします。自動動作モードで動作している場合、Guard は、作成する動的フィルタ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 1000 を超えたときは、動作モードに関して推奨された変更を適用する前に、まずゾーン保護を非アクティブにする必要があります。ゾーンの動作モードを変更する前にゾーン保護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 フィルタを超えたときに、ゾーンの動作モードを自動に変更するには、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。Guard がゾーン保護を停止して、保留動的フィルタをすべて削除します。

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。Guard 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。

ステップ 7　**Protect** をクリックします。Guard がゾーン保護を開始して、作成する動的フィルタをすべてアクティブにします。