インタラクティブ検出モード

ゾーン検出をイネーブルにした場合、Cisco Traffic Anomaly Detector Module（Detector モジュール）はゾーンのトラフィックを分析し、超過したポリシーのしきい値を検索します。ポリシーのしきい値を超過したことを検出すると、トラフィックを分析し、トラフィックを処理するためのフィルタのセット（動的フィルタ）を作成します。動的フィルタは、自動またはインタラクティブのどちらでもアクティブにできます。この章では、インタラクティブ検出モードについて説明します。この章には、次の主な項があります。

概要

DDoS 攻撃が開始されると、Detector モジュールのポリシーは動的フィルタを作成します。ゾーンがインタラクティブ検出モードである場合、Detector モジュールはこのような動的フィルタをアクティブにせず、ユーザの決定を待ちます。このようなフィルタは、保留動的フィルタと呼ばれます。推奨事項は、フィルタを生成したポリシーに応じた保留フィルタのサマリーです。この情報には、推奨事項を提示したポリシーの名前、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が含まれています。どの保留動的フィルタを受け入れるか、無視するか、または自動アクティベーションに向けるかを決定することにより、攻撃が進行しているときに講じる対策をより強く制御できます。

Guard は、インタラクティブ検出モードである限り、保留動的フィルタの生成を続けて、ゾーンを検出します。ゾーンの検出中いつでもインタラクティブ検出モードをアクティブにできますが、Guard がインタラクティブ検出モードで、ゾーンに対する DDoS 攻撃が進行中である場合にだけ、推奨事項およびその保留動的フィルタを表示できます。インタラクティブ検出モードは、ゾーンを定義するときや、ゾーン検出をアクティブにする前または後に設定できます。

1000 個を超える保留動的フィルタがある場合、Detector モジュールは次のように動作します。

- ゾーンを非アクティブにして自動検出モードで再度アクティブにするよう指示するエラー メッセージを表示する。
- ゾーンのログ　ファイルおよびレポートに推奨事項を記録してから、推奨事項を廃棄する。

新しい推奨事項が利用可能になっても、Detector モジュールは通知を表示しません。推奨事項を追跡するには、次のいずれかを行います。

- ゾーン設定モードで **show** コマンドを使用して、ゾーンのステータスを表示する。
- **event monitor** コマンドを使用して、新しい保留動的フィルタの作成時に通知を受け取る。
- 外部 syslog サーバを使用して、新しい保留動的フィルタの通知を受け取る。

いつでもインタラクティブ検出モードを停止して、自動検出モードに戻ることができます。Detector モジュールは、インタラクティブ検出モード中の決定をすべて無視し、現在の保留動的フィルタをすべて受け入れます。ポリシーは、動的フィルタを自動的に生成してアクティブにするという役割を再開します（第 7 章「ポリシー テンプレートとポリシーの設定」を参照してください）。

インタラクティブ検出モードのアクティブ化

既存のゾーンのインタラクティブ検出モードをアクティブにするには、ゾーン設定モードで **interactive** と入力します。

インタラクティブ検出モードに設定された新しいゾーンを作成するには、設定モードで次のコマンドを入力します。

zone *new-zone-name* **interactive**

new-zone-name 引数には、新しいゾーンの名前を指定します。ゾーン名は英数字の文字列とし、必ず英字で入力を開始してください。スペースは使用できません。また、63 文字以内で入力してください。

次の例を参考にしてください。

```
user@DETECTOR-conf# zone scannew interactive
```

インタラクティブ検出モードに設定された新しいゾーンが、デフォルト ゾーン テンプレートで作成されます。

インタラクティブ検出モードの非アクティブ化

インタラクティブ検出モードを非アクティブにするには、**no interactive** コマンドを使用します。インタラクティブ検出モードを非アクティブにすると、ポリシーのインタラクティブ ステータスが **always-accept** になります。

推奨事項の表示

ゾーンのすべての推奨事項のリスト、保留動的フィルタのリスト、または特定の推奨事項を表示するには、**show recommendations** コマンドを使用します。次のコマンドを入力します。

show recommendations [*recommendation-id*] [**pending-filters**]

表 8-1 で、**show recommendations** コマンドのキーワードと引数について説明します。

表 8-1　show recommendations コマンドのキーワードと引数

パラメータ	説明
recommendation-id	（オプション）特定の推奨事項の ID。
pending-filters	（オプション）特定の推奨事項の保留フィルタのリストを表示します。

次の例を参考にしてください。

```
user@DETECTOR-conf-zone-scannet# show recommendations
```

表 8-2 で、**show recommendations** コマンド出力のフィールドについて説明します。

表 8-2　show recommendations コマンドのフィールド説明

フィールド	説明
ID	推奨事項の識別番号。
Policy	推奨事項を作成したポリシー。
Threshold	超過したポリシーしきい値。
Detection date	推奨事項が作成された日時。
Attack flow	攻撃フローの特性。この特性は、プロトコル番号、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポートを含み、トラフィックが断片化されているかどうかを示します。**Any** は、断片化されているトラフィックと断片化されていないトラフィックの両方があることを示します。

表 8-2　show recommendations コマンドのフィールド説明（続き）

フィールド	説明
Min current rate	最小攻撃レート（pps）。 複数の保留動的フィルタを持つ推奨事項の場合、最小攻撃レートの保留動的フィルタのレートが表示されます。
Max current rate	最大攻撃レート（pps）。 複数の保留動的フィルタを持つ推奨事項の場合、最大攻撃レートの保留動的フィルタのレートが表示されます。
No. of pending-filters	ポリシーしきい値の超過が発生したために作成された保留動的フィルタの数。
Recommended action	推奨されているアクション。推奨事項を受け入れると、このアクションが実行されます。

特定の推奨事項の保留フィルタを表示する前に、すべての推奨事項とその ID のリストを表示するには、**show recommendations** コマンドを使用します。

表 8-3 で、**show recommendations pending-filters** コマンド出力のフィールドについて説明します。

表 8-3　show recommendations pending-filters コマンドのフィールド説明

フィールド	説明
ID	推奨事項の識別番号。
Policy	推奨事項を作成したポリシー。
Threshold	超過したポリシーしきい値（pps）。
Pending-filter-id	保留動的フィルタの識別番号。
Detection date	推奨事項が作成された日時。
Attack flow	攻撃フローの特性。この特性は、プロトコル番号、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポートを含み、トラフィックが断片化されているかどうかを示します。**Any** は、断片化されているトラフィックと断片化されていないトラフィックの両方があることを示します。

表 8-3　show recommendations pending-filters コマンドのフィールド説明

フィールド	説明
Triggering rate	保留動的フィルタの作成をトリガーした攻撃レート（pps）。
Current rate	現在の攻撃レート（pps）。
Recommended action	推奨されているアクション。推奨事項を受け入れると、このアクションが実行されます。
Action flow	保留動的フィルタを受け入れた場合にそのフィルタで処理される、ゾーンへのトラフィック フローの特性。この特性は、プロトコル番号、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポートを含み、トラフィックが断片化されているかどうかを示します。**Any** は、断片化されているトラフィックと断片化されていないトラフィックの両方があることを示します。

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。
- パラメータに対して複数の値が測定された。

（注）　Guard がインタラクティブ検出モードで、ゾーンに対する DDoS 攻撃が進行中である場合にだけ、推奨事項およびその保留動的フィルタを表示できます。

次の例を参考にしてください。

```
user@DETECTOR-conf-zone-scannet# show recommendations 135
pending-filters
```

推奨事項の管理

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行うことができます。その決定によって、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 Detector モジュールに指示することもできます。DDoS 攻撃が続行し、その特性を変更している間、Detector モジュールのポリシーは推奨事項を生成し続けます。

決定を確認するには、決定を行った後にゾーンのステータスを表示します。

ポリシーは、次のアクションを実行します。

- **notify**：ポリシーが Detector の syslog にイベントを記録します。イベントには、しきい値超過が発生したポリシーの詳細が記録されます。
- **remote-activate**：Detector が 1 つまたは複数のリモート Guard をアクティブにし、ゾーンの保護を開始します。

（注）　推奨事項を受け入れると、受け入れた推奨事項と同じまたは受け入れた推奨事項に含まれるフローを持ち、アクションとタイムアウトが同じである、その他の推奨事項も受け入れられます。Detector モジュールは、これらの推奨事項を削除します。

ゾーンの推奨事項に関して決定を行うには、ゾーン設定モードで **recommendation** コマンドを使用します。次のコマンドを入力します。

recommendation *recommendation-id* [**pending-filters** *pending-filter-id*] *decision* [*timeout*]

表 8-4 で、**recommendation** コマンドの引数とキーワードについて説明します。

表 8-4　recommendation コマンドの引数とキーワード

パラメータ	説明
recommendation-id	特定の推奨事項の識別番号。アスタリスク（*****）は、すべての推奨事項を示すワイルドカードです。
pending-filter-id	（オプション）特定の保留動的フィルタの ID。
decision	推奨事項に対して実行するアクション。指定できる値は、次のとおりです。 • **accept**：特定の推奨事項を受け入れます。保留動的フィルタは、動的フィルタになります。 • **always-accept**：特定の推奨事項を受け入れます。この決定は、推奨ポリシーによって新しい推奨事項が生成されると必ず、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 はこ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フィルタも生成されません。この決定は、ポリシーによって生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は、Detector が推奨事項を表示しなくなります。
timeout	（オプション）決定が適用される期間。指定できる値は、次のとおりです。 • **forever**：検出が有効である限り、Detector が、推奨事項によって生成された動的フィルタ（P.6-21 の「動的フィルタの設定」を参照）をアクティブにします。 • *new-timeout*：定義した期間中、Guard が、ポリシーによって生成された動的フィルタ（詳細については、P.6-21 の「動的フィルタの設定」を参照）をアクティブにします。この期間は秒で測定されます。

特定のポリシーまたはポリシーの任意の部分のインタラクティブ ステータスを設定し、ポリシーのその部分が推奨事項と保留動的フィルタを生成するかどうかを決定できます。詳細については、P.7-30 の「ポリシーのインタラクティブ ステータスの設定」を参照してください。この設定により、さらに強力な制御が可能になり、ポリシーをトラフィック フローに、よりよく適合させることができます。

Guard は、**always-accept** および **always-ignore** の推奨事項を表示しません。推奨事項を常に無視するまたは常に受け入れると決定した場合、その決定は、推奨事項を作成したポリシーのインタラクティブ ステータスの一部となります。

ポリシーをディセーブルまたは非アクティブにして、ポリシーが推奨事項と保留動的フィルタを生成しないようにすることができます。ポリシーをディセーブルまたは非アクティブにするには、**state** コマンドを使用します。詳細については、P.7-22 の「ポリシーの状態の変更」を参照してください。

次の例は、*analysis*（分析）検出モジュールを使用する、サービス *53* の *dns_tcp* ポリシー テンプレートのインタラクティブ ステータスを設定しています。

```
user@DETECTOR-conf-zone-scannet-policy-/dns_tcp/53/analysis/#
interactive-status always-accept
```

詳細については、P.7-14 の「ポリシー パスのセクションについて」を参照してください。