



## インタラクティブ検出モードの 使用方法

Cisco Traffic Anomaly Detector モジュール (Detector モジュール) をアクティブにして、次のいずれかの動作モードでゾーン異常検出を実行できます。

- 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。ただし、動的フィルタをアクティブにはしません。代わりに Detector モジュールは、動的フィルタを推奨処置としてグループ化します。ユーザは、これらの推奨事項を確認して、推奨事項を受け入れるか、無視するか、または自動アクティベーションの対象にするかを決定できます。

この章では、インタラクティブ検出モード、および2つの動作モードの切り替え方法について説明します。

この章には、Detector モジュールの関連製品である Cisco Guard (Guard) についての記述がありません。Guard は、DDoS 攻撃 (分散型サービス拒絶攻撃) を検出して軽減するデバイスです。Guard は、ゾーントラフィックが通過する際に攻撃トラフィックをドロップして正常なトラフィックをネットワークに戻し、ゾーントラフィックをクリーンにします。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できます。また、Detector モジュールは Guard とゾーン設定を同期させることができます。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。

- [インタラクティブ検出モードについて](#)
- [インタラクティブ検出モードと異常検出のアクティブ化](#)
- [インタラクティブ検出モードのゾーンの設定](#)
- [推奨事項の表示](#)
- [推奨事項の管理](#)
- [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について

ゾーンに対して DDoS 攻撃が開始されると、ゾーン ポリシーによって動的フィルタが作成されま  
す。ゾーンがインタラクティブ検出モードで動作するように設定した場合、Detector モジュールは  
動的フィルタを自動的にアクティブにせず、どのようなアクションを取るかをユーザが決定するの  
を待ちます。ユーザの決定を待つフィルタは、*保留動的フィルタ*と呼ばれます。保留動的フィルタ  
は生成元のポリシーに応じてグループ化され、そのグループは Detector モジュールの*推奨事項*と  
して表示されます。この推奨事項には、次の情報が提供されます。

- 保留動的フィルタの作成の元になるポリシーの名前についての情報など、保留フィルタの要約
- 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
- 推奨アクション

ゾーン設定でインタラクティブ検出モードをイネーブルにすると、ゾーンに対する攻撃中に  
Detector モジュールで実行されるアクションを制御できます。ユーザは、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の対象にするかを決定します。ゾーン  
をインタラクティブ検出モードで動作するように設定できるのは、ゾーンの定義時、ゾーン保護を  
アクティブにする前、またはゾーン検出をアクティブにした後です。

Detector モジュールは、インタラクティブ検出モードになっており、かつゾーンが攻撃を受けてい  
る限り、保留動的フィルタの生成を続けます。ゾーンの異常検出中は、いつでもインタラクティブ  
検出モードをイネーブルにできます。

Detector モジュールでは最大 1,000 までの保留動的フィルタを管理できます。保留動的フィルタの  
数がこの上限に到達すると、次のアクションが実行されます。

- 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、推奨事項を削除する。

ゾーンの保護中は、ゾーンが攻撃を受けている場合でも、いつでもインタラクティブ検出モードか  
ら自動保護モードに切り替えることができます。攻撃中に自動保護モードに切り替えると、次のア  
クションが実行されます。

- ユーザが推奨事項を受け入れた結果として追加された動的フィルタが保持される。
- 自動保護モードに切り替える前に従わなかった推奨事項に関連付けられた保留動的フィルタ  
がすべて受け入れられる。
- ポリシーによって生成される新しい動的フィルタがすべて自動的に受け入れられる。

## インタラクティブ検出モードと異常検出のアクティブ化

この項では、インタラクティブ検出モードで Detector モジュールをアクティブにするために必要な手順の概要を説明します。各手順には、タスクを完了するために必要な CLI コマンドが含まれています。

インタラクティブ検出モード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** 次のうち適切なコマンドを使用して、新しいゾーンまたは既存のゾーンがインタラクティブ検出モードで動作するように設定します。

- 新しいゾーン：ゾーン設定モードで **zone new-zone-name interactive** コマンドを入力します。  
user@DETECTOR-conf# **zone scannet interactive**
- 既存のゾーン：ゾーン設定モードで **interactive** コマンドを入力します。  
user@DETECTOR-conf-zone-scannet# **interactive**

詳細については、[P.10-4](#) の「[インタラクティブ検出モードのゾーンの設定](#)」を参照してください。

**ステップ 2** (オプション) **event monitor** コマンドを使用すると、新しい推奨事項が使用可能になったときに Detector モジュールが通知を表示するように設定できます。

```
user@DETECTOR# event monitor
```

外部の 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信することや、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手動で表示することもできます。

**ステップ 3** **learning** コマンドを使用して、Detector モジュールをアクティブにし、ゾーントラフィックパターンをラーニングします。ラーニングプロセスの詳細については、[第 8 章「ゾーントラフィックの特性のラーニング」](#)を参照してください。

**ステップ 4** **detect** コマンドを使用して、ゾーン異常検出をアクティブにします。

```
user@DETECTOR-conf-zone-scannet# detect
```

詳細については、[第 9 章「ゾーントラフィック異常の検出」](#)を参照してください。

**ステップ 5** **show recommendations** コマンドを使用して、新しい推奨事項とその保留動的フィルタを表示します。

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

詳細については、[P.10-5](#) の「[推奨事項の表示](#)」を参照してください。

**ステップ 6** **recommendation** コマンドを使用して新しい推奨事項を管理する方法を決定します。推奨事項を受け入れるか、無視するか、または Detector モジュールに対して推奨事項を自動的にアクティブにするよう指示するかを決定できます。

```
user@DETECTOR-conf-zone-scannet# recommendation 135 accept
```

詳細については、[P.10-7](#) の「[推奨事項の管理](#)」を参照してください。

**ステップ7** `no interactive` コマンドを使用すると、インタラクティブ検出モードをいつでも非アクティブにできます。Detector モジュールは、新しい動的フィルタを自動的にアクティブにできます。

```
user@DETECTOR-conf-zone-scanner# no interactive
```

詳細については、[P.10-9](#) の「インタラクティブ検出モードの非アクティブ化」を参照してください。

---

## インタラクティブ検出モードのゾーンの設定

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` コマンドを使用します。

次の例は、既存のゾーンに対してインタラクティブ検出モードをアクティブにする方法を示しています。

```
user@DETECTOR-conf-zone-scanner# 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を作成するには、設定モードで次のコマンドを使用します。

```
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。

次の例は、新しいゾーンを作成し、インタラクティブ検出モードに設定する方法を示しています。

```
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。詳細については、[P.5-5](#) の「新しいゾーンの作成」を参照してください。

## 推奨事項の表示

ゾーン設定モードで次のコマンドを入力すると、すべての推奨事項のリスト、保留動的フィルタのリスト、およびゾーンに固有の推奨事項を表示できます。

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

表 10-1 に、`show recommendations` コマンドのキーワードと引数を示します。

表 10-1 show recommendations コマンドのキーワードと引数

パラメータ	説明
<code>recommendation-id</code>	(オプション) 特定の推奨事項の ID。
<code>pending-filters</code>	(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。

次の例は、すべての推奨事項のリストを表示する方法を示しています。

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

表 10-2 に、`show recommendations` コマンド出力のフィールドを示します。

表 10-2 show recommendations コマンド出力のフィールドの説明

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。この特性には、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、宛先ポートが含まれています。トラフィックが断片化されているかどうかを示しています。 <b>any</b> の値は、断片化された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。
Min current rate	最小攻撃レート (パケット / 秒)。 複数の保留動的フィルタを持つ推奨事項の場合、保留動的フィルタの最小レートが表示されます。
Max current rate	最大攻撃レート (パケット / 秒)。 複数の保留動的フィルタを持つ推奨事項の場合、保留動的フィルタの最大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	推奨処置。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 10-3 に、`show recommendations pending-filters` コマンド出力のフィールドを示します。

表 10-3 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 (パケット / 秒)。
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。この特性には、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、宛先ポートが含まれています。トラフィックが断片化されているかどうかを示しています。 <b>any</b> の値は、断片化された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。
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 (パケット / 秒)。
Current rate	現在の攻撃レート (パケット / 秒)。
Recommended action	推奨処置。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。この特性には、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、宛先ポートが含まれています。トラフィックが断片化されているかどうかを示しています。 <b>any</b> の値は、断片化された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。

Detector モジュールでは、次の場合に、ワイルドカードとしてのアスタリスク (\*) がパラメータのいずれかに表示されます。

- 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)

Detector モジュール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。

次の例は、推奨事項 135 の保留動的フィルタを表示する方法を示しています。

```
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 モジュールに設定できます。また、ポリシーによって推奨事項が生成されないよう Detector モジュールに設定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検出モードで、DDoS 攻撃が進行中の場合、推奨事項を生成し続けます。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。

ゾーン ポリシーは、次のアクションを取ることができます。

- **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同様に受け入れられます。重複する推奨事項は Detector モジュールで削除されます。

ゾーンの推奨事項を決定するには、ゾーン設定モードで次のコマンドを使用します。

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

表 10-4 に、**recommendation** コマンドの引数とキーワードを示します。

表 10-4 **recommendation** コマンドの引数とキーワード

パラメータ	説明
<i>recommendation-id</i>	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。
<b>pending-filters</b> <i>pending-filter-id</i>	(オプション) 特定の保留動的フィルタの ID を指定します。
<i>decision</i>	推奨事項に対するアクション。指定できる値は、次のとおりです。 <ul style="list-style-type: none"> <li>• <b>accept</b> : 特定の推奨事項を受け入れます。保留動的フィルタは、アクティブな動的フィルタになります。</li> <li>• <b>always-accept</b> : 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、自動的にアクティブな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 モジュールはこのような推奨事項を表示しなくなります。</li> <li>• <b>always-ignore</b> : 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 モジュールが推奨事項を表示しなくなります。</li> </ul>

表 10-4 recommendation コマンドの引数とキーワード (続き)

パラメータ	説明
<i>timeout</i>	<p>(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。</p> <ul style="list-style-type: none"> <li>• <b>forever</b> : 検出が有効である限り、推奨事項によって生成された動的フィルタをアクティブにします。このタイムアウトがデフォルトです。詳細については、<a href="#">P.6-15</a> の「動的フィルタの設定」を参照してください。</li> <li>• <b>new-timeout</b> : 定義した期間中、ポリシーによって生成された動的フィルタをアクティブにします。この期間は秒で測定されます。詳細については、<a href="#">P.6-15</a> の「動的フィルタの設定」を参照してください。</li> </ul>

次の例は、推奨事項 135 を受け入れる方法を示しています。

```
user@DETECTOR-conf-zone-scannet# recommendation 135 accept
```

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。ポリシーのインタラクティブステータスを設定することで、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。詳細については、[P.7-22](#) 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。

Detector モジュールは、**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.7-15](#) の「ポリシーの状態の変更」を参照してください。

次の例では、`dns_tcp/53/analysis` のインタラクティブステータスを **always-accept** に設定しています。

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



## 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、ゾーン設定モードで **no interactive** コマンドを使用します。ユーザがインタラクティブ検出モードを非アクティブにすると、Detector モジュールはすべての新しい動的フィルタを自動的にアクティブにし、ポリシーのインタラクティブステータスを **always-accept** に設定します（ゾーン ポリシーの表示方法の詳細については、[P.7-26](#) の「[ポリシーの表示](#)」を参照）。

次の例は、ゾーン `scannet` のインタラクティブ検出モードを非アクティブにする方法を示しています。

```
user@DETECTOR-conf-zone-scannet# no interactive
```

■ インタラクティブ検出モードの非アクティブ化