CHAPTER 11

インタラクティブ保護モードの使用方法

Cisco Anomaly Guard Module（Guard 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保護を実行できます。

- 自動保護モード：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。
- インタラクティブ保護モード：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 Guard 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、インタラクティブ保護モード、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。

この章は、次の項で構成されています。

インタラクティブ保護モードについて

ゾーンに対して DDoS 攻撃（分散型サービス拒絶攻撃）が開始されると、ゾーン ポリシーによって攻撃を軽減するための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保護モードで動作するように設定した場合、Guard 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 Guard 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保護モードをイネーブルにすると、攻撃の進行中に Guard モジュールで実行される軽減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保護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、またはゾーン保護をアクティブにした後です。

Guard モジュールは、ゾーンをインタラクティブ保護モードで保護していて、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。ゾーンの保護中は、いつでもインタラクティブ保護モードをイネーブルにできます。

Guard 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保護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。

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保護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。

インタラクティブ保護モードのイネーブル化とゾーン保護のアクティブ化

この項では、次のタスクを実行するために必要な手順の概要を説明します。

- ゾーンがインタラクティブ保護モードで動作するように設定する。
- ラーニング プロセスをイネーブルにして、Guard モジュールがゾーン トラフィックをラーニングできるようにする。
- ゾーン保護をアクティブにする。

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。

ゾーンがインタラクティブ保護モードで動作するように設定して、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　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保護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@GUARD-conf# zone scannet interactive
  ```

  P.11-5 の「インタラクティブ保護モード用に設定された新しいゾーンの作成」を参照してください。
- 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@GUARD-conf-zone-scannet# interactive
  ```

  P.11-5 の「インタラクティブ保護モード用の既存のゾーンの設定」を参照してください。

ステップ 2　（オプション）グローバル モードで **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 Guard モジュールが通知を表示するように設定できます。

```
user@GUARD# 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、ステップ 5 のように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。Guard モジュールの推奨事項を表示する方法の詳細については、P.11-6 の「Guard モジュールの推奨事項の追跡」を参照してください。

ステップ 3　（オプション）Guard モジュールがまだゾーン トラフィックをラーニングしておらず、ゾーンが攻撃を受けていない場合は、ラーニング プロセスを実行します。ラーニング プロセスの詳細については、第 9 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。

Guard モジュールがすでにゾーン トラフィックをラーニングしたか、またはオンデマンド保護に対するゾーンを作成した場合は、このステップを省略します。オンデマンド保護の詳細については、P.10-3 の「オンデマンド保護のアクティブ化」を参照してください。

ステップ 4　ゾーン設定モードで **protect** コマンドを使用して、ゾーン保護をアクティブにします。

```
user@GUARD-conf-zone-scannet# protect
```

詳細については、第 10 章「ゾーンの保護」を参照してください。

ステップ 5　ゾーン設定モードで **show recommendations** コマンドを使用して、ゾーンが攻撃を受けているときに Guard モジュールの推奨事項と保留動的フィルタを表示します。

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

詳細については、P.11-6 の「show コマンドを使用した推奨事項の表示」を参照してください。

ステップ 6　ゾーン設定モードで **recommendation** コマンドを使用して、推奨事項の管理方法を指定します。新しい推奨事項を受け入れるか、無視するか、または Guard モジュールで自動的にアクティブにするかを決定できます。

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

詳細については、P.11-8 の「推奨事項の管理」を参照してください。

ゾーン設定モードで **no interactive** コマンドを使用すると、インタラクティブ保護モードをいつでも非アクティブにできます。詳細については、P.11-10 の「インタラクティブ保護モードの非アクティブ化」を参照してください。

ゾーンをインタラクティブ保護モードで動作するように設定

新しいゾーンを作成する際に、インタラクティブ保護モードで動作するように設定できます。また、既存のゾーンの設定を変更して、インタラクティブ保護モードでの動作をイネーブルにすることもできます。

この項では、次のトピックについて取り上げます。

- インタラクティブ保護モード用に設定された新しいゾーンの作成
- インタラクティブ保護モード用の既存のゾーンの設定

インタラクティブ保護モード用に設定された新しいゾーンの作成

新しいゾーンを作成して、ゾーン保護をアクティブにしたときにインタラクティブ保護モードで動作するように設定するには、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、インタラクティブ保護モードで動作するように設定された新しいゾーンを作成する方法を示しています。

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

新しいゾーンは Guard モジュールのデフォルトのゾーン テンプレートで作成されます。詳細については、P.6-4 の「新しいゾーンの作成」を参照してください。

ゾーン保護をアクティブにしたときにインタラクティブ保護モードで動作するように既存のゾーンを設定するには、次の例に示すように、ゾーン設定モードで **interactive** コマンドを使用します。

```
user@GUARD-conf-zone-scannet# interactive
```

インタラクティブ保護モード用の既存のゾーンの設定

新しいゾーンを作成して、ゾーン保護をアクティブにしたときにインタラクティブ保護モードで動作するように設定するには、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、インタラクティブ保護モードで動作するように設定された新しいゾーンを作成する方法を示しています。

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

新しいゾーンは Guard モジュールのデフォルトのゾーン テンプレートで作成されます。詳細については、P.6-4 の「新しいゾーンの作成」を参照してください。

Guard モジュールの推奨事項の追跡

この項では、Guard モジュールがインタラクティブ保護モードでゾーンを保護する際に作成される推奨事項の追跡に使用できるオプションについて説明します。

この項では、次のトピックについて取り上げます。

show コマンドを使用した推奨事項の表示

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 11-1 に、**show recommendations** コマンドのキーワードと引数を示します。

表 11-1　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@GUARD-conf-zone-scannet# show recommendations
```

表 11-2 に、**show recommendations** コマンド出力のフィールドを示します。

表 11-2　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。**any** 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	パケット / 秒で測定される最小攻撃レート。 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	パケット / 秒で測定される最大攻撃レート。 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。

表 11-2　show recommendations コマンド出力のフィールドの説明（続き）

フィールド	説明
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 11-3 に、**show recommendations pending-filters** コマンド出力のフィールドを示します。

表 11-3　show recommendations pending-filters コマンド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	超過されたパケット / 秒単位のポリシーしきい値。
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。**any** 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。**any** 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。

Guard 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）　Guard モジュールがインタラクティブ保護モードで、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@GUARD-conf-zone-scannet# show recommendations 135 pending-filters
```

イベント ログを使用した保留動的フィルタの通知の受信

Guard モジュールのイベント ログを使用すると、**event monitor** コマンドを実行することで、新しい保留動的フィルタの作成時に通知を受け取ることができます。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こともできます。イベント ログを使用する方法の詳細については、P.13-9 の「Guard モジュールのログの管理」を参照してください。

推奨事項の管理

Guard モジュールがインタラクティブ保護モードでゾーンを保護する場合、Guard モジュールの推奨事項を受け入れるかどうかをユーザが決定します。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アクティブな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 Guard 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 Guard モジュールに設定することもできます。Guard 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、推奨事項を生成し続けます。現在の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。

（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 Guard 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 11-4 に、**recommendation** コマンドの引数とキーワードを示します。

表 11-4　recommendation コマンドの引数とキーワード

パラメータ	説明
recommendation-id	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-filters *pending-filter-id*	（オプション）特定の保留動的フィルタの ID を指定します。

表 11-4　recommendation コマンドの引数とキーワード（続き）

パラメータ	説明
decision	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。 • **accept**：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。 • **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、自動的にアクティブな動的フィルタになります。 **always-accept** を指定すると、推奨事項が表示されなくなります。 • **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、推奨事項が表示されなくなります。
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**：保護が有効である限り、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。このタイムアウトの設定がデフォルトです。詳細については、P.7-21 の「動的フィルタの設定」を参照してください。 • *new-timeout*：指定した期間中、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、P.7-21 の「動的フィルタの設定」を参照してください。

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@GUARD-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、軽減プロセスの制御が可能になり、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.8-23 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。

Guard モジュールでは、**always-accept** および **always-ignore** に指定された推奨事項は表示されません。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、ポリシー設定モードで **state** コマンドを使用します。詳細については、P.8-15 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@GUARD-conf-zone-scannet-policy-/dns_tcp/53/analysis/# interactive-status
always-accept
```

インタラクティブ保護モードの非アクティブ化

インタラクティブ保護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保護モードを非アクティブにすると、Guard 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.8-25 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保護モードを非アクティブにする方法を示しています。

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