インタラクティブ推奨モード

Guard は、宛先変更されたゾーン トラフィックを分析して、ポリシーのしきい値超過を探します。ポリシーのしきい値超過を検出すると、結果を分析し、自動的またはインタラクティブにアクティブにできるフィルタのセットを作成します。この章では、インタラクティブ推奨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、Guard 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推奨モードである場合、Guard 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、推奨元のポリシー名、そのポリシーがアクティブになる原因となったトラフィックの異常に関するデータ、保留中のフィルタ数、推奨されるアクションなどが含まれます。どの保留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ブ化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、インタラクティブ推奨モードである限り、保留フィルタの生成を続けて、ゾーンを保護します。ゾーンの保護中いつでもインタラクティブ推奨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推奨モードで、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フィルタを表示できます。ゾーンの定義時、またはゾーン保護の開始前後に、インタラクティブ推奨をゾーンに適用できます。

1000 個を超える保留フィルタがある場合、Guard 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。

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 プロンプトで **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、新しい保留フィルタの通知を受け取る。

いつでもインタラクティブ動作を停止して、自動動作に戻ることができます。Guard は、インタラクティブ モード中の決定をすべて無視し、現在保留中のすべてのフィルタを受け入れます。ポリシーは、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）。

インタラクティブ推奨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推奨モードをアクティブにするには、ゾーン プロンプトで **interactive** と入力します。

インタラクティブ推奨モードの新しいゾーンを作成するには、設定プロンプトで次のように入力します。

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

引数 *new-zone-name* には、新しいゾーンの名前を指定します。ゾーン名は英数字で、英字で開始する必要があり、スペースを使用できず、63 文字を超えることはできません。

次の例を参考にしてください。

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

インタラクティブ推奨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、第 5 章「ゾーンの設定」を参照してください。

インタラクティブ推奨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 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。このコマンドの構文は、次のとおりです。

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。

```
admin@GUARD-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、送信元ポート、宛先 IP、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。
Min current rate	パケット / 秒（pps）で測定された最小攻撃レート。 複数の保留フィルタを持つ推奨事項の場合、最小攻撃レートの保留フィルタのレートが表示されます。
Max current rate	パケット / 秒（pps）で測定された最大攻撃レート。 複数の保留フィルタを持つ推奨事項の場合、最大攻撃レートの保留フィルタのレートが表示されます。
No. of pending-filters	ポリシーのしきい値超過の結果として作成された保留フィルタの数。
Recommended action	推奨されるアクション。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、送信元ポート、宛先 IP、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。
Triggering rate	保留フィルタ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、送信元ポート、宛先 IP、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推奨モードで、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フィルタを表示できます。

次の例を参考にしてください。

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

推奨事項のアクティブ化

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フィルタを自動的にアクティブにするよう Guard 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 Guard 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、Guard 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。

（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、その他の推奨事項が削除されます。

ゾーンの推奨事項に関して決定を行うには、ゾーン プロンプトで **recommendation** コマンドを使用します。このコマンドの構文は、次のとおりです。

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、Guard 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、Guard 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**：保護が有効である限り、Guard が、推奨事項によって生成された動的フィルタ（P.6-19 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.6-19 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.7-26 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.7-20 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）保護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。

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

詳細については、P.7-13 の「ポリシーのセクション」を参照してください。