ルールを使用した侵入ポリシーの調整

ここでは、ルールを使用して侵入ポリシーを調整する方法について説明します。

侵入ルールの調整の基本

侵入ポリシーの [ルール（Rules）] ページを使用して、共有オブジェクトルール、標準テキストルール、およびプリプロセッサルールに関するルール状態とその他の設定を構成できます。

ルールは、ルール状態を [イベントを生成する（Generate Events）] または [ドロップしてイベントを生成する（Drop and Generate Events）] に設定することによって有効にします。ルールを有効にすると、システムがそのルールと一致するトラフィックに対するイベントを生成します。ルールを無効にすると、ルールの処理が停止されます。また、インライン展開で [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールによって、一致するトラフィックに対するイベントが生成され、そのトラフィックが破棄されるように、侵入ポリシーを設定できます。パッシブ展開では、[ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールによって、一致するトラフィックに対するイベントが生成されるだけです。

ルールのサブセットを表示するようにルールをフィルタ処理することによって、ルール状態やルール設定を変更するルールのセットを正確に選択できます。

侵入ルールまたはルールの引数がプリプロセッサの無効化を必要とする場合、ネットワーク分析ポリシーの Web インターフェイスでは無効化されたままになりますが、システムは自動的に現在の設定を使用します。

侵入ルールのタイプ

侵入ルールとは、ネットワーク内の脆弱性を不正利用する試みを検出するためにシステムが使用する、指定されたキーワードと引数のセットのことです。システムはネットワークトラフィックを分析する際に、パケットを各ルールに指定された条件に照らし合わせ、データパケットがルールに指定されたすべての条件を満たす場合、そのルールをトリガーします。

侵入ポリシーには以下の構成要素があります。

- 侵入ルール。共有オブジェクト ルールと標準テキスト ルールに分割されます。
- プリプロセッサルール。パケットデコーダの検出オプション、またはシステムに付属のプリプロセッサの 1 つに関連付けられます。

次の表に、以上のルール タイプの属性を要約します。

表 *1*: 侵入ルールのタイプ

タイプ	ジェネレータ ID（GID）	Snort ID（SID）	ソース	コピーの可否	編集の可否
共有オブジェクトルール	3	1000000 未満	Talos インテリジェンスグループ	はい	制限付き
標準テキストルール	1（グローバル ドメインまたはレガシー GID）	1000000 未満	Talos	はい	制限付き
	1000～2000（子孫ドメイン）	1000000 以上	ユーザが作成またはインポート	はい	はい
プリプロセッサルール	デコーダまたはプリプロセッサに固有	1000000 未満	Talos	いいえ	いいえ
		1000000 以上	オプション設定時にシステムにより生成	いいえ	いいえ

Talos によって作成されたルールを変更して保存することはできませんが、変更されたルールのコピーをカスタム ルールとして保存することはできます。ルールで使用される変数またはルール ヘッダー情報（送信元と宛先のポートや IP アドレスなど）を変更できます。

Talos によって作成されるルールには、各デフォルト侵入ポリシー内でデフォルトのルール状態が割り当てられます。ほとんどのプリプロセッサルールがデフォルトで無効になっているため、システムにプリプロセッサ ルールに対するイベントの生成とインライン展開での違反パケットの破棄を行わせる場合は、これらのルールを有効にする必要があります。

マルチドメイン展開では、子孫ドメインで作成されたか、または子孫ドメインにインポートされたカスタムルールの SID の先頭にドメイン番号が追加されます。たとえば、グローバルドメインに追加されたルールに 1000000 以上の SID があり、子孫ドメインに追加されたルールには [ドメイン番号]000000 以上の SID があります。

侵入ルールのライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

侵入ルールの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- 侵入管理者

侵入ポリシー内の侵入ルールの表示

侵入ポリシーでのルールの表示方法を調整でき、複数の条件によってルールをソートできます。特定のルールの詳細を表示して、ルール設定、ルール ドキュメント、およびその他のルール仕様を確認することもできます。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] > [侵入（Intrusion）]**を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（  ） が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルの [ポリシー情報（Policy Information）] の下にある [ルール（Rules）] をクリックします。

ステップ 4 ルールを表示している間、以下を実行できます。

- 侵入ポリシー内のルール フィルタの設定 （18 ページ）の説明に従ってルールをフィルタリングします。
- ソートの基準とするカラムの一番上のタイトルをクリックすることによって、ルールをソートします。
- 侵入ルール詳細の表示 （6 ページ）の説明に従って、侵入ルールの詳細を表示します。
- [ポリシー（Policy）] ドロップダウン リストから階層を選択することによって、異なるポリシー階層のルールを表示します。

[侵入ルール（Intrusion Rules）] ページの列

[侵入ルール（Intrusion Rules）] ページでは、メニュー バーおよび列ヘッダーに同じアイコンが使用されます。たとえば、[ルール状態（Rule State）] メニューでは、ルールリストの [ルール状態（Rule State）] カラムと同じ [イベントの生成（Generate Events）] が使用されます。

表 2 : [Rules] ページの列

見出し	説明
GID	ルールのジェネレータ ID（GID）を表す整数。
SID	ルールの固有識別子として機能する Snort ID（SID）を表す整数。 カスタム ルールの場合、SID は 1000000 以上です。
メッセージ（Message）	このルールによって生成されるイベントに含まれるメッセージ。ルールの名前としても機能します。

見出し	説明
イベントを生成する（Generate Events）	ルールのルール状態。 • **ドロップおよびイベントの生成** • **イベントを生成する** • **無効** 無効なルールのアイコンは、トラフィックをドロップせずにイベントを生成するように設定されたルールのアイコンのグレー表示されたバージョンです。また、ルールのルール状態アイコンをクリックすると、ルール状態を変更できます。
Cisco 推奨ルール状態	ルールの Cisco 推奨ルール状態。
イベント フィルタ	ルールに適用されるイベントしきい値やイベント抑制などのイベント フィルタ。
動的状態	ルールの動的ルール状態。指定されたレート異常が発生した場合に有効になります。
[エラー（Error）]（）	ルールに対して設定されたアラート（現在は SNMP アラートのみ）。
[コメント（Comment）]（  ）	ルールに追加されたコメント。

レイヤのドロップダウンリストを使用して、ポリシー内の他のレイヤの[ルール（Rules）]ページに切り替えることもできます。ポリシーにレイヤを追加しなかった場合にドロップダウンリストに表示される編集可能なビューはポリシーの[ルール（Rules）]ページと、元は`My Changes`という名前だったポリシー階層の [ルール（Rules）] ページだけであることに注意してください。これらのビューの一方を変更すると、もう一方も同じように変更されることにも注意してください。ドロップダウンリストには、読み取り専用の基本ポリシーの[ルール（Rules）]ページも表示されます。

侵入ルールの詳細

[ルールの詳細（Rule Detail）] ビューで、ルールドキュメント、Cisco の推奨事項、およびルールオーバーヘッドを確認できます。また、ルール固有の機能を表示および追加できます。

表 *3*: ルールの詳細

項目	説明
要約（Summary）	ルールの概要。ルール ベースのイベントでは、ルール ドキュメントに概要情報が含まれている場合にこの行が表示されます。
ルール状態（Rule State）	ルールの現在のルール状態。ルール状態が設定された階層も示します。

項目	説明
Cisco の推奨事項（Cisco Recommendation）	Cisco の推奨事項が生成されている場合は、推奨されるルール状態を表すアイコンがあります。[侵入ルール（Intrusion Rules）] ページの列 （4 ページ）を参照してください。ルールを有効にすることが推奨されている場合、システムは推奨事項をトリガーしたネットワーク アセットまたは設定も示します。
ルールのオーバーヘッド	システム パフォーマンスに対するルールの潜在的影響とルールが誤検出を引き起こす確率。脆弱性にマップされていないローカル ルールにはオーバーヘッドが割り当てられていません。
しきい値	このルールに現在設定されているしきい値と、ルールのしきい値を追加するための機能。
抑制（Suppressions）	このルールに現在設定されている抑制設定と、ルールの抑制を追加するための機能。
動的状態（Dynamic State）	このルールに現在設定されているレート ベースのルール状態と、ルールの動的ルール状態を追加するための機能。
アラート（Alerts）	このルールに設定されている SNMP アラートと、ルールのアラートを追加するための機能。
説明	このルールに追加されたコメントと、ルールのコメントを追加するための機能。
資料	Talos インテリジェンス グループによって提供される現在のルールのルール ドキュメント。必要に応じて、[ルール ドキュメンテーション（Rule Documentation）] をクリックして、ルールの詳細を表示します。

侵入ルール詳細の表示

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] > [侵入（Intrusion）]**を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（  ） が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ペインで [ルール（Rules）] をクリックします。

ステップ 4 ルールの詳細を表示したいルールをクリックし、ページの下部にある [詳細の表示（Show details）] をクリックします。
侵入ルールの詳細 （5 ページ）で説明されているように、ルールの詳細が表示されます。

ステップ 5 ルールの詳細から、以下を設定できます。

- アラート：侵入ルールの SNMP アラートの設定 （9 ページ）を参照してください。
- コメント：侵入ルールへのコメントの追加 （10 ページ）を参照してください。
- ダイナミック ルールの状態：[ルール詳細（Rule Details）] ページからの動的ルール状態の設定 （8 ページ）を参照してください。
- しきい値：侵入ルールのしきい値の設定 （7 ページ）を参照してください。
- 抑制：侵入ルールの抑制の設定 （8 ページ）を参照してください。

侵入ルールのしきい値の設定

[ルールの詳細（Rule Detail）] ページで、ルールの単一のしきい値を設定できます。しきい値を追加すると、ルールの既存のしきい値が上書きされます。

無効な値を入力するとフィールドに [復元（Revert）] が表示される点に注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

手順

ステップ 1 侵入ルールの詳細で、[しきい値（Thresholds）] の横にある [追加（Add）] をクリックします。

ステップ 2 [タイプ（Type）] ドロップダウンリストから、設定するしきい値のタイプを選択します。

- 指定された期間あたりのイベントインスタンス数に通知を制限する場合は、[制限（Limit）] を選択します。
- 指定された期間あたりのイベント インスタンス数ごとに通知を提供する場合は、[しきい値（Threshold）] を選択します。
- 指定されたイベントインスタンス数に達した後で、期間あたり 1 回ずつ通知を提供する場合は、[両方（Both）] を選択します。

ステップ 3 [追跡対象（Track By）] ドロップダウンリストから、[送信元（Source）] または [宛先（Destination）] を選択し、イベント インスタンスが送信元 IP アドレスまたは宛先 IP アドレスのどちらによって追跡されるかを指定します。

ステップ 4 [カウント（Count）] フィールドに、しきい値として使用するイベント インスタンスの数を入力します。

ステップ 5 [秒数（Seconds）] フィールドに、イベント インスタンスを追跡する期間（秒数）を指定する数値を入力します。

ステップ 6 [OK] をクリックします。

ヒント [イベントフィルタリング（Event Filtering）] カラムのルールの横に [イベントフィルタ（Event Filter）] が表示されます。ルールに複数のイベントフィルタを追加すると、イベントフィルタの数が表示されます。

侵入ルールの抑制の設定

侵入ポリシーのルールに対して 1 つ以上の抑制を設定できます。

無効な値を入力するとフィールドに[復元（Revert）] アイコンが表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

手順

ステップ 1 侵入ルールの詳細で、[抑制（Suppressions）] の横にある [追加（Add）] をクリックします。

ステップ 2 [抑制タイプ（Suppression Type）] ドロップダウンリストから、次のいずれかのオプションを選択します。

- 選択したルールのイベントを完全に抑制する場合は、[ルール（Rule）] を選択します。
- 指定した送信元 IP アドレスから送信されるパケットによって生成されるイベントを抑制する場合は、[送信元（Source）] を選択します。
- 指定した宛先 IP アドレスに送信されるパケットによって生成されるイベントを抑制する場合は、[宛先（Destination）] を選択します。

ステップ 3 抑制タイプとして [送信元（Source）] または [宛先（Destination）] を選択した場合は、[ネットワーク（Network）] フィールドに IP アドレス、アドレス ブロック、またはそれらの任意の組み合わせで構成されたカンマ区切りのリストを入力します。

侵入ポリシーがアクセス コントロール ポリシーのデフォルト アクションに関連付けられている場合は、デフォルトアクション変数セットでネットワーク変数を指定または列挙することもできます。

ステップ 4 [OK] をクリックします。

ヒント 抑制するルールの横にある [イベントフィルタリング（Event Filtering）] カラムのルールの横に [イベントフィルタ（Event Filter）] が表示されます。ルールに複数のイベントフィルタを追加した場合は、フィルタ上の数字がフィルタの数を示します。

[ルール詳細（Rule Details）] ページからの動的ルール状態の設定

1 つのルールに対して 1 つ以上の動的ルール状態を設定できます。最初に表示される動的ルール状態に最も高いプライオリティが割り当てられます。2 つの動的ルール状態が競合している場合は、最初のアクションが実行されます。

動的ルール状態はポリシー固有です。

無効な値を入力するとフィールドに[復元（Revert）] が表示される点に注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

手順

ステップ 1 侵入ルールの詳細で、[動的状態（Dynamic State）] の横にある [追加（Add）] をクリックします。

ステップ 2 [追跡対象（Track By）] ドロップダウンリストから、ルール一致の追跡方法を指定するオプションを選択します。

- 特定の送信元または送信元のセットからのそのルールのヒット数を追跡する場合は、[送信元（Source）] を選択します。
- 特定の宛先または宛先のセットへのそのルールのヒット数を追跡する場合は、[宛先（Destination）] を選択します。
- そのルールのすべての一致を追跡する場合は、[ルール（Rule）] を選択します。

ステップ 3 [追跡対象（Track By）] を [送信元（Source）] または [宛先（Destination）] に設定した場合は、[ネットワーク（Network）] フィールドに追跡する各ホストのアドレスを入力します。

ステップ 4 [レート（Rate）] の横で、攻撃レートを設定する期間あたりのルール一致の数を指定します。

- [カウント（Count）] フィールドで、しきい値として使用するルール一致の数を指定します。
- [秒（Seconds）] フィールドで、攻撃を追跡する期間を表す秒数を指定します。

ステップ 5 [新しい状態（New State）] ドロップダウンリストから、条件が満たされたときに実行する新しいアクションを選択します。

ステップ 6 [タイムアウト（Timeout）] フィールドに値を入力します。

タイムアウトが発生すると、ルールが元の状態に戻ります。新しいアクションがタイムアウトしないようにする場合は、0 を入力します。

ステップ 7 [OK] をクリックします。

ヒント [動的状態（Dynamic State）] カラムのルールの横に動的状態（  ）が表示されます。ルールに複数の動的ルール状態フィルタを追加した場合は、フィルタ上の数字がフィルタの数を示します。

侵入ルールの SNMP アラートの設定

[ルールの詳細（Rule Detail）] ページで、ルールの SNMP アラートを設定できます。

手順

侵入ルールの詳細で、[アラート（Alerts）] の横にある [SNMP アラートの追加（Add SNMP Alert）] をクリックします。

ヒント [アラート（Alerting）] カラムのルールの横にアラート [エラー（Error）] （  ） が表示されます。ルールに複数のアラートを追加した場合は、アラートの数が表示されます。

侵入ルールへのコメントの追加

手順

ステップ 1 侵入ルールの詳細で、[コメント（Comments）] の横の [追加（Add）] をクリックします。

ステップ 2 [コメント（Comments）] フィールドに、ルール コメントを入力します。

ステップ 3 [OK] をクリックします。

ヒント システムは [コメント（Comments）] カラムのルールの横に [コメント（Comment）] （  ） を表示します。ルールに複数のコメントを追加した場合は、コメント上の数字がコメントの数を示します。

ステップ 4 ルール コメントを削除するには、ルール コメント セクションで [削除（Delete）] をクリックします。侵入ポリシーの変更がコミットされずにコメントがキャッシュされている場合にだけコメントを削除できます。

次のタスク

- 設定変更を展開します設定変更の展開を参照してください。

侵入ポリシー内の侵入ルール フィルタ

[ルール（Rules）] ページに表示するルールは、1 つの基準または 1 つ以上の基準の組み合わせに基づいてフィルタ処理できます。

ルール フィルタ キーワードは、ルール状態やイベント フィルタなどのルール設定を適用するルールを見つけやすくします。[ルール（Rules）] ページのフィルタ パネルで必要な引数を選択することによって、キーワードでフィルタ処理すると同時に、キーワードの引数を選択することができます。

侵入ルール フィルタの注意事項

作成したフィルタが [フィルタ（Filter）] テキストボックスに表示されます。フィルタ パネルでキーワードとキーワード引数をクリックしてフィルタを作成できます。複数のキーワードを選択した場合は、システムがそれらを AND ロジックを使用して結合し、複合検索フィルタを生成します。たとえば、[カテゴリ（Category）] で [プリプロセッサ（preprocessor）] を選択し

てから、**[ルール コンテンツ（Rule Content）] > [GID]** の順に選択して、「116」と入力すると、プリプロセッサ ルールで、**かつ**、GID が 116 のすべてのルールを取得する「`Category: "preprocessor" GID:"116"`」というフィルタが返されます。

[カテゴリ（Category）]、[Microsoft 脆弱性（Microsoft Vulnerabilities）]、[Microsoft ワーム（Microsoft Worms）]、[プラットフォーム特有（Platform Specific）]、[プリプロセッサ（Preprocessor）]、および [優先度（Priority）] の各フィルタ グループを使用すれば、カンマで区切られたキーワードの複数の引数を送信できます。たとえば、[カテゴリ（Category）] から [os-linux] と [os-windows] を選択すると、`os-linux` カテゴリまたは `os-windows` カテゴリ内のルールを取得する「`Category:"os-windows,os-linux"`」というフィルタを作成できます。

フィルタパネルを表示するには、**表示アイコン** をクリックします。

フィルタパネルを非表示にするには、**非表示アイコン** をクリックします。

侵入ポリシー ルール フィルタ構築のガイドライン

ほとんどの場合、フィルタを作成するときに、侵入ポリシー内の [ルール（Rules）] ページの左側にあるフィルタ パネルを使用して必要なキーワード/引数を選択できます。

フィルタ パネルでは、ルール フィルタがルール フィルタ グループに分類されます。多くのルール フィルタ グループにサブ基準が含まれているため、探している特定のルールを簡単に見つけることができます。一部のルール フィルタには、展開して個別のルールにドリルダウンするための複数のレベルが設定されています。

フィルタ パネル内の項目は、場合によって、フィルタ タイプ グループを表したり、キーワードを表したり、キーワードの引数を表したりします。次の点に注意してください。

- キーワード（[ルール設定（Rule Configuration）]、[ルール コンテンツ（Rule Content）]、[プラットフォーム特有（Platform Specific）]、および [優先度（Priority）]）以外のフィルタ タイプ グループ見出しを選択すると、そのグループが展開されて使用可能なキーワードが一覧表示されます。

  基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ条件とする引数を指定するためのポップアップ ウィンドウが表示されます。

  そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

  たとえば、フィルタ パネルの **[ルール設定（Rule Configuration）] > [推奨（Recommendation）]** で [ドロップしてイベントを生成する（Drop and Generate Events）] をクリックすると、「`Recommendation:"Drop and Generate Events"`」がフィルタ テキスト ボックスに追加されます。その後で、**[ルール設定（Rule Configuration）] > [推奨（Recommendation）]** で [イベントを生成する（Generate Events）] をクリックすると、フィルタが「`Recommendation:"Generate Events"`」に変更されます。

- キーワード（[カテゴリ（Category）]、[分類（Classifications）]、[Microsoft 脆弱性（Microsoft Vulnerabilities）]、[Microsoft ワーム（Microsoft Worms）]、[優先度（Priority）]、および [ルール アップデート（Rule Update）]）になっているフィルタ タイプ グループ見出しを選択すると、使用可能な引数が一覧表示されます。

このタイプのグループから項目を選択すると、適用される引数とキーワードがすぐにフィルタに追加されます。キーワードがすでにフィルタ内に存在していた場合は、そのグループに対応するキーワードの既存の引数が置き換えられます。

たとえば、フィルタ パネルの [カテゴリ（Category）] で [os-linux] をクリックすると、「`Category:"os-linux"`」がフィルタ テキストボックスに追加されます。その後で、[カテゴリ（Category）] で [os-windows] をクリックすると、フィルタが「`Category:"os-windows"`」に変更されます。

- [ルール コンテンツ（Rule Content）] の下の [参照（Reference）] はキーワードであり、その下に特定の参照 ID タイプが列挙されます。参照キーワードのいずれかを選択すると、引数を指定するためのポップアップ ウィンドウが表示され、キーワードが既存のフィルタに追加されます。キーワードがすでにフィルタ内で使用されていた場合は、既存の引数が指定した新しい引数に置き換えられます。

  たとえば、フィルタパネルで **[ルールコンテンツ（Rule Content）]** > **[参照（Reference）]** > **[CVE ID]** の順にクリックすると、ポップアップウィンドウが開いて CVE ID を指定するよう求められます。「`2007`」と入力すると、「`CVE:"2007"`」がフィルタ テキストボックスに追加されます。別の例では、フィルタパネルで **[ルールコンテンツ（Rule Content）]** > **[参照（Reference）]** の順にクリックすると、ポップアップウィンドウが開いて、参照を指定するよう求められます。「`2007`」と入力すると、「`Reference:"2007"`」がフィルタ テキストボックスに追加されます。

- 複数のグループからルール フィルタ キーワードを選択した場合は、各フィルタ キーワードがフィルタに追加され、既存のキーワードが維持されます（同じキーワードの新しい値で上書きされなかった場合）。

  たとえば、フィルタ パネルの [カテゴリ（Category）] で [os-linux] をクリックすると、「`Category:"os-linux"`」がフィルタ テキストボックスに追加されます。その後で、[Microsoft 脆弱性（Microsoft Vulnerabilities）] で [MS00-006] をクリックすると、フィルタが「`Category:"os-linux" MicrosoftVulnerabilities:"MS00-006"`」に変更されます。

- 複数のキーワードを選択した場合は、システムがそれらを AND ロジックを使用して結合し、複合検索フィルタを生成します。たとえば、[カテゴリ（Category）] で [プリプロセッサ（preprocessor）] を選択してから、**[ルール コンテンツ（Rule Content）]** > **[GID]** の順に選択して、「`116`」と入力すると、プリプロセッサ ルールで、**かつ**、GID が 116 のすべてのルールを取得する「`Category: "preprocessor" GID:"116"`」というフィルタが返されます。

- [カテゴリ（Category）]、[Microsoft 脆弱性（Microsoft Vulnerabilities）]、[Microsoft ワーム（Microsoft Worms）]、[プラットフォーム特有（Platform Specific）]、および [優先度（Priority）] の各フィルタ グループを使用すれば、カンマで区切られたキーワードの複数の引数を送信できます。たとえば、[カテゴリ（Category）] から [os-linux] と [os-windows] を選択すると、`os-linux` カテゴリまたは `os-windows` カテゴリ内のルールを取得する「`Category:"os-windows,app-detect"`」というフィルタを作成できます。

複数のフィルタ キーワード/引数のペアで同じルールが取得される場合があります。たとえば、ルールが **dos** カテゴリでフィルタ処理された場合と **High** 優先度でフィルタ処理された場合はともに、DOS Cisco attempt rule（SID 1545）が表示されます。

（注） Talos インテリジェンスグループ がルール更新メカニズムを使用してルール フィルタを追加または削除する場合があります。

[ルール（Rules）] ページのルールは、共有オブジェクト ルール（ジェネレータ ID 3）または標準テキスト ルール（ジェネレータ ID 1、グローバル ドメインまたはレガシー GID（1000 ～ 2000）、子孫ドメイン）のいずれかになります。次の表に、さまざまなルール フィルタの説明を示します。

表 *4:* ルール フィルタ グループ

フィルタ グループ	説明	複数の引数をサポートするか	見出し	リスト内の項目
ルール設定（Rule Configuration）	ルールの設定に基づいてルールを検索します。	非対応	グループ	キーワード
ルール コンテンツ（Rule Content）	ルールの内容に基づいてルールを検索します。	非対応	グループ	キーワード
カテゴリ（Category）	ルール エディタで使用されるルール カテゴリに基づいてルールを検索します。ローカル ルールはローカル サブグループに表示されることに注意してください。	対応	キーワード	引数
分類（Classifications）	ルールによって生成されるイベントのパケット画面内に表示される攻撃分類に基づいてルールを検索します。	非対応	キーワード	引数
Microsoft 脆弱性（Microsoft Vulnerabilities）	Microsoft セキュリティ情報番号に従ってルールを検索します。	対応	キーワード	引数
Microsoft ワーム（Microsoft Worms）	Microsoft Windows ホストに影響する特定のワームに基づいてルールを検索します。	対応	キーワード	引数

フィルタ グループ	説明	複数の引数をサポートするか	見出し	リスト内の項目
プラットフォーム特有（Platform Specific）	オペレーティング システムの特定のバージョンとの関連性に基づいてルールを検索します。 ルールが複数のオペレーティング システムまたは 1 つのオペレーティング システムの複数のバージョンに影響する場合があることに注意してください。たとえば、SID 2260 を有効にすると、Mac OS X、IBM AIX、およびその他のオペレーティング システムの複数のバージョンに影響します。	対応	キーワード	引数 サブリストからいずれかの項目を選択すると、引数に修飾子が追加されることに注意してください。
プリプロセッサ（Preprocessors）	個別のプリプロセッサのルールを検索します。 プリプロセッサが有効になっている場合にプリプロセッサ オプションに対するイベントを生成し、インライン展開では、違反パケットをドロップします。するためには、そのオプションに関連付けられたプリプロセッサ ルールを有効にする必要があることに注意してください。	対応	グループ	サブグループ
プライオリティ（Priority）	高、中、および低の優先度に基づいてルールを検索します。 ルールに割り当てられた分類によってその優先度が決定されます。これらのグループは、さらにルール カテゴリに分類されます。ローカル ルール（つまり、ユーザがインポートまたは作成したルール）は優先度グループに表示されないことに注意してください。	対応	キーワード	引数 サブリストからいずれかの項目を選択すると、引数に修飾子が追加されることに注意してください。
ルール更新（Rule Update）	特定のルール更新を通して追加または変更されたルールを検索します。ルール更新ごとに、更新内のすべてのルール、更新でインポートされた唯一の新しいルール、または更新によって変更された唯一の既存のルールを表示します。	非対応	キーワード	引数

侵入ルール構成フィルタ

[ルール（Rules）]ページに表示されたルールをいくつかのルール構成設定でフィルタ処理できます。たとえば、ルール状態が推奨ルール状態と一致しない一連のルールを表示する場合は、[推奨と一致しない（Does not match recommendation）] を選択することによってルール状態をフィルタ処理できます。

基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ条件とする引数を指定できます。そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

たとえば、フィルタ パネルの **[ルール設定（Rule Configuration）]** > **[推奨（Recommendation）]** で [ドロップしてイベントを生成する（Drop and Generate Events）] をクリックすると、「`Recommendation:"Drop and Generate Events"`」がフィルタ テキスト ボックスに追加されます。その後で、**[ルール設定（Rule Configuration）]** > **[推奨（Recommendation）]** で [イベントを生成する（Generate Events）] をクリックすると、フィルタが「`Recommendation:"Generate Events"`」に変更されます。

侵入ルール コンテンツ フィルタ

[Rules] ページに表示されたルールをいくつかのルール コンテンツ項目でフィルタ処理できます。たとえば、ルールの SID を検索することによって、ルールをすばやく取得できます。特定の宛先ポートに送信されるトラフィックを検査するすべてのルールを検索することもできます。

基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ条件とする引数を指定できます。そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

たとえば、フィルタ パネルの [ルール コンテンツ（Rule Content）] で [SID] をクリックすると、ポップアップ ウィンドウが開いて SID の入力が促されます。「`1045`」と入力すると、「`SID:"1045"`」がフィルタ テキスト ボックスに追加されます。その後で、再度 [SID] をクリックして、SID フィルタを「`1044`」に変更すると、フィルタが「`SID:"1044"`」に変更されます。

表 *5:* ルール コンテンツ フィルタ

フィルタ	検索するルールの内容
メッセージ（Message）	メッセージ フィールドで指定された文字列を含む。
SID	指定された SID がある。
GID	指定された GID がある。
参照（Reference）	参照フィールドで指定された文字列を含む。また、特定のタイプの参照および指定された文字列でフィルタリングすることもできます。
操作（Action）	`alert` または `pass` から開始する。
プロトコル（Protocol）	選択されたプロトコルを含む。
方向（Direction）	ルールに、指定された方向設定が含まれているかどうかに基づく。

フィルタ	検索するルールの内容
ソース IP（Source IP）	ルール内の送信元 IP アドレス宛先に指定されたアドレスまたは変数を使用する。有効な IP アドレス、CIDR ブロック/プレフィックス長、または $HOME_NET や $EXTERNAL_NET などの変数を使用してフィルタ処理できます。
宛先 IP（Destination IP）	ルール内の送信元 IP アドレス宛先に指定されたアドレスまたは変数を使用する。有効な IP アドレス、CIDR ブロック/プレフィックス長、または $HOME_NET や $EXTERNAL_NET などの変数を使用してフィルタ処理できます。
ソース ポート	指定された送信元ポートを含む。ポート値は、1 ～ 65535 の整数またはポート変数にする必要があります。
接続先ポート（Destination port）	指定された宛先ポートを含む。ポート値は、1 ～ 65535 の整数またはポート変数にする必要があります。
ルールのオーバーヘッド	選択されたルールのオーバーヘッドがある。
メタデータ	一致するキーと値のペアを含むメタデータがある。たとえば、HTTP アプリケーション プロトコルに関連するメタデータを使用したルールを検索するには、「metadata:"service http"」と入力します。

侵入ルール カテゴリ

システムは、ルールが検出するトラフィックのタイプに基づいてカテゴリにルールを配置します。[ルール（Rules）] ページで、ルール カテゴリでフィルタ処理することによって、カテゴリ内のすべてのルールにルール属性を設定できます。たとえば、ネットワーク上に Linux ホストが存在しない場合は、**os-linux** カテゴリでフィルタ処理してから、表示されたすべてのルールを無効にすることによって、**os-linux** カテゴリ全体を無効にすることができます。

カテゴリ名の上にポインタを移動すると、そのカテゴリ内のルールの数を表示できます。

（注） Talos インテリジェンス グループ がルール更新メカニズムを使用してルール カテゴリを追加または削除する場合があります。

侵入ルールのフィルタ コンポーネント

フィルタ パネルでフィルタをクリックしたときに入力される特殊なキーワードとその引数を変更するようにフィルタを編集できます。[ルール（Rules）] ページのカスタム フィルタはルール エディタで使用されるものと同様に機能しますが、フィルタ パネルを通してフィルタを選択したときに表示される構文を使用して、[ルール（Rules）] ページのフィルタに入力されたキーワードのいずれかを使用することもできます。今後使用するキーワードを決定するには、右側のフィルタ パネルで該当する引数をクリックします。フィルタ キーワードと引数構文がフィルタ テキストボックスに表示されます。キーワードのカンマ区切りの複数の引数は [カテ

ゴリ（Category）] と [優先度（Priority）] のフィルタ タイプでしかサポートされないことに注意してください。

引用符内のキーワードと引数、文字列、およびリテラル文字列と一緒に、複数のフィルタ条件を区切るスペースを使用できます。ただし、正規表現、ワイルドカード文字、および除外文字（!）、「大なり」記号（>）、「小なり」記号（<）などの特殊な演算子をフィルタに含めることはできません。キーワードなし、キーワードの先頭文字の大文字表記なし、または引数の周りの引用符なしの検索語を入力すると、検索が文字列検索として扱われ、[カテゴリ（Category）]、[メッセージ（Message）]、および [SID] の各フィールドで指定された単語が検索されます。

`gid` キーワードと `sid` キーワードを除くすべての引数と文字列が部分文字列として扱われます。`gid` と `sid` の引数は、完全一致のみを返します。

各ルール フィルタに、次の形式で 1 つ以上のキーワードを含めることができます。

`keyword:"argument"`

ここで、Keyword は侵入ルール フィルタ グループ内のキーワードのいずれかで、argument は二重引用符で囲まれ、キーワードに関連した特定のフィールド内で検索される単一の大文字と小文字が区別されない英数字文字列です。キーワードは先頭文字を大文字にして入力する必要があることに注意してください。

`gid` と `sid` を除くすべてのキーワードの引数が部分文字列として扱われます。たとえば、引数 `123` によって `"12345"`、`"41235"`、`"45123"` などが返されます。`gid` と `sid` の引数は完全一致のみを返します。たとえば、`sid:3080` は `SID 3080` のみを返します。

各ルール フィルタに、1 つ以上の英数字文字列を含めることもできます。文字列はルールの [メッセージ（Message）] フィールド、Snort ID（SID）、およびジェネレータ ID（GID）を検索します。たとえば、文字列 `123` は、ルール メッセージ内の文字列 `"Lotus123"` や `"123mania"` などを返し、`SID 6123` や `SID 12375` なども返します。部分的な SID を検索するには、1 つ以上の文字列を使ってフィルタ処理できます。

すべての文字列では大文字と小文字が区別されず、部分的な文字列として扱われます。たとえば、文字列 `ADMIN`、`admin`、または `Admin` はすべて、「`admin`」、「`CFADMIN`」、「`Administrator`」などを返します。

文字列を引用符で囲むと、完全一致を返すことができます。たとえば、引用符付きのリテラル文字列 `"overflow attempt"` は完全一致のみを返しますが、引用符なしの 2 つの文字列 `overflow` と `attempt` で構成されるフィルタは `"overflow attempt"`、`"overflow multipacket attempt"`、`"overflow with evasion attempt"` などを返します。

複数のキーワード、文字列、またはその両方をスペースで区切って任意に組み合わせて入力することで、フィルタリングの結果を絞り込むことができます。結果には、すべてのフィルタ条件に一致するルールが含まれます。

複数のフィルタ条件を任意の順序で入力できます。たとえば、次のフィルタはそれぞれ同じルールを返します。

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`

- `login cve:200 attempt url:at`

侵入ルール フィルタの使用

侵入ポリシー内の [ルール（Rules）] ページの左側にあるフィルタ パネルから事前定義のフィルタ キーワードを選択できます。フィルタを選択すると、ページに、すべての一致するルールが表示されるか、どのルールも一致しなかったことが表示されます。

フィルタにキーワードを追加してさらに絞り込むことができます。入力されたフィルタは、ルールデータベース全体を検索して、一致するすべてのルールを返します。前回のフィルタ結果がページに表示されている状態でフィルタを入力すると、そのページの内容が消去され、代わりに新しいフィルタの結果が返されます。

また、フィルタを選択したとき、または、フィルタを選択後にその中の引数値を変更したときに指定したものと同じキーワードと引数の構文を使用してフィルタを入力することもできます。キーワードなし、キーワードの先頭文字の大文字表記なし、または引数の周りの引用符なしの検索語を入力すると、検索が文字列検索として扱われ、[カテゴリ（Category）]、[メッセージ（Message）]、および [SID] の各フィールドで指定された単語が検索されます。

侵入ポリシー内のルール フィルタの設定

[ルール（Rules）]ページで、ルールのサブセットを表示するようにルールをフィルタ処理できます。その後で、いずれかのページ機能を使用できます。これには、コンテキストメニューで使用可能な機能の選択も含まれます。これは、特定のカテゴリのすべてのルールのしきい値を設定する場合などに便利です。フィルタ処理されている場合もされていない場合も、リスト内のルールで同じ機能を使用できます。たとえば、新しいルール状態を、フィルタ処理されたリスト内のルールまたはフィルタ処理されていないリスト内のルールに適用できます。

すべてのフィルタのキーワード、キーワード引数、および文字列では大文字と小文字が区別されません。フィルタ内に存在するキーワードの引数をクリックすると、既存の引数が置き換えられます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[侵入（Intrusion）]**を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（  ） が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 次に示す方法を個別に使用したり、組み合わせて使用することでフィルタを作成します。

- [フィルタ（Filter）] テキスト ボックスに値を入力して、Enter キーを押します。
- 事前定義されたキーワードのいずれかを展開します。たとえば、[ルール設定（Rule Configuration）] をクリックします。

- キーワードをクリックして、プロンプトが表示されたら引数の値を指定します。次に例を示します。
  - [ルール設定（Rule Configuration）] の下で、[ルール状態（Rule State）] をクリックし、ドロップダウンリストから [イベントの生成（`Generate Events`）] を選択して、[OK] をクリックします。
  - [ルール設定（Rule Configuration）] の下で、[コメント（Comment）] をクリックし、フィルタ条件として使用するコメント テキストの文字列を入力して、[OK] をクリックします。
  - [カテゴリ（Category）] の下で、[アプリ検出（app-detect）] をクリックします。システムは、これを引数の値として使用します。
- キーワードを展開して、引数の値をクリックします。たとえば、[ルール状態（Rule State）] を展開して、[イベントの生成（Generate Events）] をクリックします。

侵入ルールの状態

侵入ルールの状態により、個々の侵入ポリシー内のルールを有効または無効にできるだけでなく、モニタ対象の条件によってルールがトリガーされたときにシステムが実行するアクションを指定できます。

各デフォルト ポリシーの侵入ルールとプリプロセッサ ルールのデフォルト状態は、Talos インテリジェンスグループが設定します。たとえば、ルールを Security over Connectivity デフォルト ポリシーでは有効にして、Connectivity over Security デフォルト ポリシーでは無効にすることができます。Talos がルール更新を使用してデフォルト ポリシー内の 1 つ以上のルールのデフォルト状態を変更する場合もあります。ルール更新での基本ポリシーの更新を許可すると、ポリシーの作成時に使用されたデフォルトポリシー（または基礎となるデフォルトポリシー）のデフォルト状態が変更されたときの、そのポリシー内のルールのデフォルト状態の変更も許可することになります。ただし、ルール状態を変更している場合は、ルール更新でその変更が上書きされないことに注意してください。

侵入ルールを作成すると、そのルールは、ポリシーの作成時に使用されたデフォルトポリシー内のルールのデフォルト状態を継承します。

侵入ルールの状態オプション

侵入ポリシーでは、ルールの状態を次の値に設定できます。

イベントを生成する（Generate Events）

システムで特定の侵入試行を検出して、一致したトラフィックが見つかった時点で侵入イベントを生成する場合。悪意のあるパケットがネットワークを通過してルールをトリガーすると、そのパケットが宛先に送信され、システムが侵入イベントを生成します。悪意のあるパケットはその対象に到達しますが、イベント ロギングによって通知されます。

ドロップおよびイベントの生成（Drop and Generate Events）

システムで特定の侵入試行を検出して、その攻撃を含むパケットをドロップし、一致したトラフィックが見つかった時点で侵入イベントを生成する場合。悪意のあるパケットはその対象に到達せず、イベント ロギングによって通知されます。

このルール状態に設定されたルールはイベントを生成しますが、パッシブ展開ではパケットをドロップしないことに注意してください。システムがパケットをドロップするには、侵入ポリシーで[インライン時にドロップ（Drop when Inline）]も有効にして、デバイスインラインを展開する必要があります。

無効（Disable）

システムで一致するトラフィックを評価しない場合。

（注） [イベントを生成する（Generate Events）] または [ドロップおよびイベントの生成（Drop and Generate Events）] オプションのいずれかを選択すると、ルールが有効になります。[無効（Disable）] を選択すると、ルールが無効になります。

シスコでは、侵入ポリシー内のすべての侵入ルールを有効に**しない**ことを**強く**推奨しています。すべてのルールが有効になっている場合は、管理対象デバイスのパフォーマンスが低下する可能性があります。代わりに、できるだけネットワーク環境に合わせてルールセットを調整してください。

侵入ルール状態の設定

侵入ルール状態は、ポリシー固有です。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[侵入（Intrusion）]**を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（👁） が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ヒント このページには、有効なルールの総数、[イベントを生成する（Generate Events）] に設定された有効なルールの総数、および [ドロップしてイベントを生成する（Drop and Generate Events）] に設定された有効なルールの総数が表示されます。また、パッシブ展開では、[ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールで行われるのはイベントの生成のみであることにも注意してください。

ステップ 3 ナビゲーションウィンドウで、[ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。

ステップ 4 ルール状態を設定する 1 つ以上のルールを選択します。

ステップ 5 次のいずれかを実行します。

- **[ルール状態（Rule State）] > [イベントを生成する（Generate Events）]**
- **[ルール状態（Rule State）] > [ドロップおよびイベントの生成（Drop and Generate Events）]**
- **[ルール状態（Rule State）] > [無効（Disable）]**

ステップ 6 最後のポリシー確定後にこのポリシーで行った変更を保存するには、ナビゲーションパネルで [ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開を参照してください。

侵入ポリシーの侵入イベント通知フィルタ

侵入イベントの重要度は、発生頻度、送信元 IP アドレス、または宛先 IP アドレスに基づいて設定できます。イベントが特定の回数発生するまで注意が必要ない場合もあります。たとえば、何者かがサーバにログインしようとしても、特定の回数失敗するまで、気にする必要はありません。一方、ほんの少数の発生を見れば、広範な問題があることを理解できる場合もあります。たとえば、Web サーバに対して DoS 攻撃が行われた場合は、少数の侵入イベントの発生を確認しただけで、その状況に対処しなければならないことが分かります。同じイベントが何百回も確認されれば、システムの機能が麻痺します。

侵入イベントしきい値

指定された期間内にイベントが生成された回数に基づいて、システムが侵入イベントを記録して表示する回数を制限するための個別のルールのしきい値を侵入ポリシー単位で設定できます。これにより、大量の同じイベントが原因で機能が麻痺するのを避けることができます。共有オブジェクトのルール、標準テキスト ルール、またはプリプロセッサ ルールごとにしきい値を設定できます。

侵入イベントしきい値の設定

しきい値を設定するには、最初にしきい値のタイプを指定します。

表 *6:* しきい値設定オプション

オプション	説明
制限（Limit）	指定された数のパケット（count 引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、イベントを記録して表示します。たとえば、タイプを [制限（Limit）] に、[カウント（Count）] を 10 に、[秒（Seconds）] を 60 に設定し、14 個のパケットがルールをトリガーとして使用した場合、システムはその 1 分の間に発生した最初の 10 個を表示した後、イベントの記録を停止します。
しきい値（Threshold）	指定された数のパケット（count 引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、1 つのイベントを記録して表示します。イベントのしきい値カウントに達し、システムがそのイベントを記録した後、時間のカウンタは再び開始されることに注意してください。たとえば、タイプを [しきい値（Threshold）] に、[カウント（Count）] を 10 に、[秒（Seconds）] を 60 に設定して、ルールが 33 秒間で 10 回トリガーされたとします。システムは、1 個のイベントを生成してから、[秒（Seconds）] と [カウント（Count）] のカウンタを 0 にリセットします。次の 25 秒間にルールがさらに 10 回トリガーされたとします。33 秒でカウンタが 0 にリセットされたため、システムが別のイベントを記録します。
両方（Both）	指定された数（カウント）のパケットがルールをトリガーとして使用した後で、指定された期間ごとに 1 回イベントを記録して表示します。たとえば、タイプを [両方（Both）] に、[カウント（Count）] を 2 に、[秒（Seconds）] を 10 に設定した場合、イベント数は以下のようになります。 • ルールが 10 秒間に 1 回トリガーされた場合、システムはイベントを生成しません（しきい値が満たされていない）。 • ルールが 10 秒間に 2 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回目にトリガーとして使用されたときにしきい値が満たされる）。 • ルールが 10 秒間に 4 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回目にトリガーとして使用されたときにしきい値に達し、それ以降のイベントは無視される）。

次に、トラッキングを指定します。これにより、イベントしきい値が送信元 IP アドレス単位と宛先 IP アドレス単位のどちらで計算されるかが決まります。

表 *7: IP* しきい値設定オプション

オプション	説明
ソース（Source）	送信元 IP アドレス単位でイベント インスタンス カウントを計算します。
接続先（Destination）	宛先 IP アドレス単位でイベント インスタンス カウントを計算します。

最後に、しきい値を定義するインスタンスの数と期間を指定します。

表 *8*:インスタンス/時間のしきい値設定オプション

オプション	説明
カウント（Count）	しきい値を満たすために必要な、追跡するIPアドレス単位で指定された期間単位のイベントインスタンスの数。
秒（Seconds）	カウントがリセットされるまでの秒数。しきい値タイプを [制限（limit）] に、トラッキングを [送信元IP（Source IP）] に、[カウント（count）] を [10] に、[秒（seconds）] を [10] に設定した場合は、システムが指定された送信元ポートから 10 秒間に発生した最初の 10 のイベントを記録して表示します。最初の 10 秒で 7 個のイベントだけが発生した場合、システムはそれらを記録して表示します。最初の 10 秒で 40 個のイベントが発生した場合、システムは 10 個を記録して表示し、10 秒経過してからカウントを再度開始します。

侵入イベントのしきい値設定は、単独で使用することも、レート ベースの攻撃防御、`detection_filter` キーワード、および侵入イベント抑制のいずれかと組み合わせて使用することもできます。

ヒント 侵入イベントのパケット ビューでしきい値を追加することもできます。

関連トピック

detection_filter キーワード

侵入イベントしきい値の追加と変更

侵入ポリシーの1つ以上の特定のルールにしきい値を設定できます。既存のしきい値設定を個別にまたは同時に変更することもできます。それぞれに1つずつのしきい値を設定できます。しきい値を追加すると、ルールの既存のしきい値が上書きされます。

また、侵入ポリシーに関係したすべてのルールとプリプロセッサ生成イベントにデフォルトで適用されるグローバルしきい値を変更することもできます。

無効な値を入力するとフィールドに**復元**が表示されます。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

ヒント 複数の CPU を搭載した管理対象デバイスでグローバルしきい値または個別のしきい値を設定すると、予想より多くのイベントが生成される場合があります。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] > [侵入（Intrusion）]**を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（） が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ナビゲーション（navigation）] ペインの [ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。

ステップ 4 しきい値を設定するルールを選択します。

ステップ 5 [イベントのフィルタリング（Event Filtering）] > [しきい値（Threshold）] を選択します。 >

ステップ 6 [タイプ（Type）] ドロップダウン リストからしきい値のタイプを選択します。

ステップ 7 [追跡対象（Track By）] ドロップダウンリストから、イベントインスタンスが [送信元（Source）] IP アドレスまたは [宛先（Destination）] IP アドレスのどちらによって追跡されるかを選択します。

ステップ 8 [数（Count）] フィールドに値を入力します。

ステップ 9 [秒数（Seconds）] フィールドに値を入力します。

ステップ 10 [OK] をクリックします。

ヒント [イベントフィルタリング（Event Filtering）] カラムのルールの横に [イベントフィルタ（Event Filter）] が表示されます。ルールに複数のイベントフィルタを追加した場合は、フィルタ上の数字がイベントフィルタの数を示します。

ステップ 11 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開を参照してください。

関連トピック

グローバル ルールのしきい値の基本

侵入イベントしきい値の表示と削除

ルールに関する既存のしきい値設定を表示または削除することができます。[ルールの詳細（Rules Details）] ビューを使用してしきい値の既存の設定を表示することによって、それらがシステムに適切かどうかを確認できます。そうでない場合は、新しいしきい値を追加して既存の値を上書きすることができます。

侵入ポリシーによって記録されるすべてのルールとプリプロセッサ生成イベントにデフォルトで適用されるグローバルしきい値を変更することもできます。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] > [侵入（Intrusion）]**を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（👁） が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ナビゲーション（navigation）] ペインの [ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。

ステップ 4 表示または削除する、しきい値が設定された 1 つまたは複数のルールを選択します。

ステップ 5 選択した各ルールのしきい値を削除するには、**[イベントフィルタリング（Event Filtering）] > [しきい値の削除（Remove Thresholds）]** の順に選択します。

ステップ 6 [OK] をクリックします。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開を参照してください。

関連トピック

グローバル ルールのしきい値の基本

侵入ポリシー抑制の設定

特定の IP アドレスまたは IP アドレスの範囲が特定のルールまたはプリプロセッサをトリガーしたときの侵入イベント通知を抑制できます。これは、誤検出を回避するのに役立ちます。たとえば、特定のエクスプロイトのように見えるパケットを伝送しているメールサーバが存在する場合は、そのメールサーバによってトリガーとして使用されたイベントに関するイベント通知を抑制できます。ルールはすべてのパケットに対してトリガーとして使用されますが、本物の攻撃に対するイベントだけが表示されます。

侵入ポリシー抑制タイプ

侵入イベント抑制は、単独で使用することも、レート ベースの攻撃防御、`detection_filter` キーワード、および侵入イベントしきい値構成のいずれかと組み合わせて使用することもできることに注意してください。

ヒント　侵入イベントのパケット ビュー内から抑制を追加できます。また、侵入ルール エディタ ページ（**[オブジェクト（Objects）]** > **[侵入ルール（Intrusion Rules）]**）や任意の侵入イベント ページ（イベントが侵入ルールによってトリガーされた場合）で右クリック コンテキスト メニューを使用して、抑制設定にアクセスすることもできます。

関連トピック

detection_filter キーワード

特定のルールの侵入イベントの抑制

侵入ポリシーのルールに関連する侵入イベント通知を抑制できます。ルールに関する通知が抑制されると、ルールはトリガーとして使用されますが、イベントは生成されません。ルールの 1 つまたは複数の抑制を設定できます。リスト内の最初の抑制に最も高いプライオリティが割り当てられます。2つの抑制が競合している場合は、最初の抑制のアクションが実行されます。

無効な値を入力するとフィールドに [復元（Revert）] が表示される点に注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

手順

ステップ 1　**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[侵入（Intrusion）]**を選択します。

ステップ 2　編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（👁） が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3　ナビゲーション パネルの [ポリシー情報（Policy Information）] の直下にある [ルール（Rules）] をクリックします。

ステップ 4　抑制条件を設定する 1 つまたは複数のルールを選択します。

ステップ 5　**[イベント フィルタリング（Event Filtering）]** > **[抑制（Suppression）]** を選択します。

ステップ 6　[抑制タイプ（Suppression Type）] を選択します。

ステップ 7　抑制タイプとして [送信元（Source）] または [宛先（Destination）] を選択した場合は、[ネットワーク（Network）] フィールドに、IP アドレス、アドレス ブロック、または送信元 IP アドレスまたは宛先 IP アドレスとして指定する変数、あるいは、これらの任意の組み合わせで構成されたカンマ区切りのリストを入力します。

ステップ 8　[OK] をクリックします。

ヒント　抑制するルールの横にある [イベントフィルタリング（Event Filtering）] カラムのルールの横に [イベントフィルタ（Event Filter）] が表示されます。ルールに複数のイベントフィルタを追加した場合は、フィルタ上の数字がイベントフィルタの数を示します。

ステップ 9 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開を参照してください。

抑制条件の表示と削除

既存の抑制条件を表示または削除することもできます。たとえば、メールサーバがエクスプロイトのように見えるパケットを普段から送信しているという理由で、そのメール サーバの IP アドレスから送信されたパケットに関するイベント通知を抑制できます。その後、そのメールサーバが使用停止になり、その IP アドレスが別のホストに再割り当てされたら、その送信元 IP アドレスの抑制条件を削除する必要があります。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] > [侵入（Intrusion）]**を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（👁） が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルの [ポリシー情報（Policy Information）] の直下にある [ルール（Rules）] をクリックします。

ステップ 4 抑制を表示または削除する 1 つまたは複数のルールを選択します。

ステップ 5 次の選択肢があります。

- ルールのすべての抑制を削除するには、**[イベントフィルタリング（Event Filtering）] > [抑制の削除（Remove Suppressions）]**を選択します。
- 特定の抑制設定を削除するには、ルールをクリックして、[詳細の表示（Show Details）] をクリックします。抑制設定を展開して、削除する抑制設定の横にある [削除（Delete）] をクリックします。

ステップ 6 [OK] をクリックします。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開を参照してください。

動的侵入ルール状態

レート ベースの攻撃は、ネットワークまたはホストに過剰なトラフィックを送信することによって、低速化または正規の要求の拒否を引き起こし、ネットワークまたはホストを混乱させようとします。レートベースの防御を使用して、特定のルールの過剰なルール一致に対応してルール アクションを変更することができます。

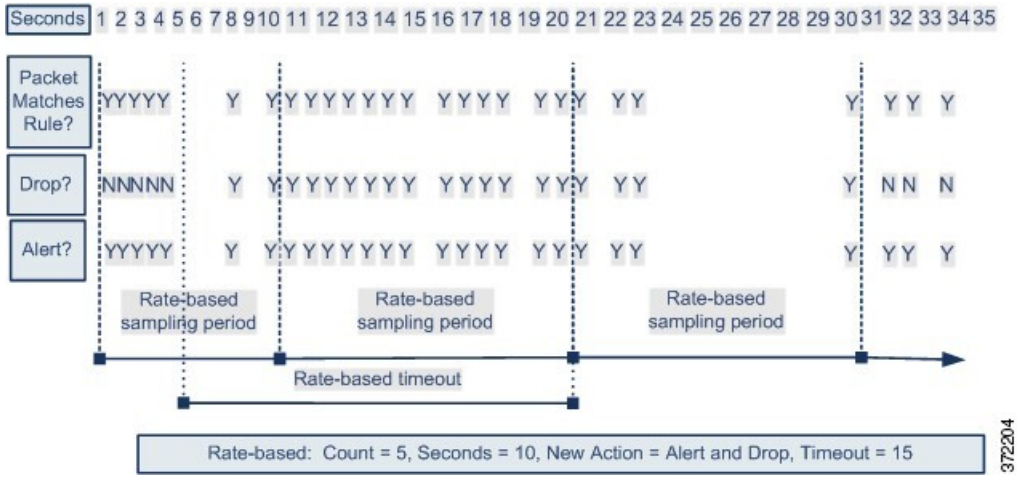
侵入ポリシーにレートベースのフィルタを含めることにより、一定期間においてルールの一致が過剰に発生した時点を検出できます。インライン展開された管理対象デバイス上でこの機能を使用して、指定された時刻のレートベースの攻撃をブロックしてから、ルール一致がイベントを生成するだけでトラフィックをドロップしないルール状態に戻すことができます。

レートベースの攻撃防止は、異常なトラフィック パターンを識別し、正規の要求に対するそのトラフィックの影響を最小限に抑えようとします。特定の宛先 IP アドレスに送信されるトラフィックまたは特定の送信元 IP アドレスから送信されるトラフィックの過剰なルール一致を識別できます。また、検出されたすべてのトラフィックを通して特定のルールの過剰な一致に対処することもできます。

ルールと一致したすべてのパケットをドロップするのではなく、指定された期間に特定の一致率に達した場合にルールと一致したパケットをドロップするために、ルールを [ドロップしてイベントを生成する（Drop and Generate Events）] 状態に設定しない場合があります。動的ルール状態を使用すれば、ルールのアクションの変更をトリガーするレート、あるレートに達したときに変更すべきアクション、および新しいアクションの継続時間を設定できます。

次の図は、攻撃者がホストにアクセスしようとしている例を示しています。繰り返しパスワードを特定しようとする試みが、レート ベースの攻撃防御が設定されたルールをトリガーします。レート ベースの設定は、ルール一致が 10 秒間に 5 回発生した時点で、ルール属性を [ドロップしてイベントを生成する（Drop and Generate Events）] に変更します。新しいルール属性は 15 秒後にタイムアウトします。

タイムアウト後も、そのパケットは後続のレートベースのサンプリング期間にドロップされることに注意してください。サンプリング レートが現在または前回のサンプリング期間中にしきい値を超えている場合は、新しいアクションが続行されます。新しいアクションは、サンプリング レートがしきい値レートを下回るサンプリング期間の終了後にのみ、[イベントを生成する（Generate Events）] に戻ります。



ダイナミックな侵入ルール状態の設定

侵入ポリシーでは、侵入ルールまたはプリプロセッサ ルールのレート ベースのフィルタを設定できます。レート ベースのフィルタは次の 3 つの要素で構成されます。

- 特定の秒数以内のルール一致のカウントとして設定されるルール一致率
- レートを超えた時点で実行される新しいアクション（[イベントを生成する（Generate Events）]、[ドロップしてイベントを生成する（Drop and Generate Events）]、および [無効（Disable）] の 3 種類がある）
- タイムアウト値として設定されるアクションの継続期間

新しいアクションは、開始されると、レートがその期間内に設定されたレートを下回っても、タイムアウトに達するまで継続されることに注意してください。タイムアウトに達すると、レートがしきい値を下回っていれば、ルールのアクションがルールの初期設定に戻ります。

インライン展開のレートベースの攻撃防御は、攻撃を一時的または永続的にブロックするように設定できます。レート ベースの設定を使用しない場合、[イベントを生成する（Generate Events）] に設定されたルールはイベントを生成しますが、システムはそのようなルールに関するパケットをドロップしません。ただし、攻撃トラフィックが、レートベースの基準が設定されているルールに一致した場合、それらのルールが当初 [イベントのドロップおよび生成（Drop and Generate Events）] に設定されていないとしても、レート アクションがアクティブである期間は、パケットがドロップされる場合があります。

（注） レート ベース アクションでは、無効にされたルールを有効にすることも、無効にされたルールに一致するトラフィックをドロップすることもできません。

同じルールに複数のレート ベース フィルタを定義できます。侵入ポリシーに列挙された最初のフィルタに最も高い優先度が割り当てられます。2 つのレートベースのフィルタ アクション

が競合している場合は、最初のレートベースのフィルタのアクションが実行されることに注意してください。

[ルール（Rule）] ページからの動的ルール状態の設定

1 つのルールに対して 1 つ以上の動的ルール状態を設定できます。最初に表示される動的ルール状態に最も高いプライオリティが割り当てられます。2 つの動的ルール状態が競合している場合は、最初のアクションが実行されます。

動的ルール状態はポリシー固有です。

無効な値を入力するとフィールドに**復元**が表示されます。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

（注） 動的ルール状態は、無効なルールを有効にしたり、無効なルールと一致したトラフィックをドロップしたりできません。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] > [侵入（Intrusion）]**を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（  ） が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ナビゲーション（navigation）] ペインの [ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。

ステップ 4 動的ルール状態を追加する 1 つまたは複数のルールを選択します。

ステップ 5 **[動的状態（Dynamic State）] > [レート ベースのルール状態の追加（Add Rate-Based Rule State）]** を選択します。

ステップ 6 [追跡対象（Track By）] ドロップダウンリストから値を選択します。

ステップ 7 [追跡対象（Track By）] を [送信元（Source）] または [宛先（Destination）] に設定した場合は、[ネットワーク（Network）] フィールドに追跡する各ホストのアドレスを入力します。単一の IP アドレス、アドレス ブロック、変数、またはこれらの任意の組み合わせで構成されたカンマ区切りのリストを指定できます。

ステップ 8 [レート（Rate）] の横で、攻撃レートを設定する期間あたりのルール一致の数を指定します。

- [数（Count）] フィールドに値を入力します。
- [秒数（Seconds）] フィールドに値を入力します。

ステップ 9 [新しい状態（New State）] ドロップダウンリストから、条件が満たされたときに実行する新しいアクションを指定します。

ステップ 10 [タイムアウト（Timeout）] フィールドに値を入力します。

タイムアウトが発生すると、ルールが元の状態に戻ります。新しいアクションのタイムアウトを阻止する場合は、[0] を指定するか、[タイムアウト（Timeout）] フィールドを空白のままにします。

ステップ 11 [OK] をクリックします。

ヒント [動的状態（Dynamic State）] 列のルールの横に [動的状態（Dynamic State）] が表示されます。ルールに複数の動的ルール状態フィルタを追加した場合は、フィルタ上の数字がフィルタの数を示します。

ヒント ルールのセットに対する動的ルール設定を削除するには、[ルール（Rules）] ページでルールを選択して、**[動的状態（Dynamic State）]** > **[レート ベースの状態の削除（Remove Rate-Based States）]** を選択します。また、ルールのルール詳細から個別のレート ベースのルール状態フィルタを削除するには、ルールを選択して、[詳細の表示（Show Details）] をクリックしてから、削除するレート ベースのフィルタのそばにある [削除（Delete）] をクリックします。

ステップ 12 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開を参照してください。

侵入ルールコメントの追加

侵入ポリシーのルールにコメントを追加できます。このようにして追加されたコメントはポリシー専用のコメントとなります。よって、ある侵入ポリシーのルールに追加したコメントは、他の侵入ポリシーでは表示されません。追加したコメントは、侵入ポリシーの[ルール（Rules）] ページ上の [ルールの詳細（Rule Details）] ビューで確認できます。

コメントを含む侵入ポリシーの変更をコミットしてから、ルールの [編集（Edit）] ページで [ルール コメント（Rule Comment）] をクリックしてコメントを表示することもできます。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] > [侵入（Intrusion）]**を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（） が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルの [ポリシー情報（Policy Information）] の直下にある [ルール（Rules）] をクリックします。

ステップ 4 コメントを追加する 1 つまたは複数のルールを選択します。

ステップ 5 [コメント（Comments）] > [ルールコメントの追加（Add Rule Comment）] を選択します。 >

ステップ 6 [コメント（Comments）] フィールドに、ルール コメントを入力します。

ステップ 7 [OK] をクリックします。

ヒント システムは [コメント（Comments）] カラムのルールの横に [コメント（Comment）]（） を表示します。ルールに複数のコメントを追加した場合は、コメント上の数字がコメントの数を示します。

ステップ 8 必要に応じて、コメントの横にある [削除（Delete）] をクリックし、ルールのコメントを削除します。

侵入ポリシーの変更がコミットされずにコメントがキャッシュされている場合にだけコメントを削除できます。侵入ポリシーの変更がコミットされた後は、ルール コメントを削除できなくなります。

ステップ 9 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開を参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。