Snort 3 侵入ポリシーを開始するには

この章では、侵入検知と防御のための Snort 3 侵入ポリシーとアクセス制御ルール設定の管理について説明します。

侵入ポリシーの概要

侵入ポリシーは定義済みの侵入検知のセットであり、セキュリティ違反についてトラフィックを検査し、インライン展開の場合は、悪意のあるトラフィックをブロックまたは変更することができます。侵入ポリシーは、アクセス コントロール ポリシーによって呼び出され、システムの最終防御ラインとして、トラフィックが宛先に到達することを許可するかどうかを判定します。

各侵入ポリシーの中核となるのは、侵入ルールです。ルールを有効にすると、ルールに一致するトラフィックに対して侵入イベントが生成されます（さらに、必要に応じてトラフィックがブロックされます）。ルールを無効にすると、ルールの処理が停止されます。

システムによって提供されるいくつかの基本侵入ポリシーにより、Cisco Talos Intelligence Group（Talos）の経験を活用できます。これらのポリシーでは、Talos が侵入ルールとインスペクタルールの状態（有効または無効）を設定し、他の詳細設定の初期設定も行います。

ヒント システム提供の侵入ポリシーとネットワーク分析ポリシーには同じような名前が付けられていますが、異なる設定が含まれています。たとえば、「Balanced Security and Connectivity」ネットワーク分析ポリシーと「Balanced Security and Connectivity」侵入ポリシーは連携して動作し、どちらも侵入ルールのアップデートで更新できます。ただし、ネットワーク分析ポリシーは主に前処理オプションを管理し、侵入ポリシーは主に侵入ルールを管理します。

カスタム侵入ポリシーを作成すると、以下を実行できます。

- ルールを有効化/無効化することに加え、独自のルールを作成して追加し、検出を調整する。
- ネットワーク上で検出されたオペレーティングシステム、サーバー、およびクライアントアプリケーションプロトコルをそれらの資産を保護するために明確に書き込まれたルールに関連付けるには、Secure Firewall の推奨事項を使用します。

侵入ポリシーは一致するパケットをドロップして、侵入イベントを生成できます。侵入またはプリプロセッサのドロップルールを設定するには、その状態を [ブロック（Block）] に設定します。

留意事項として、侵入ポリシーを調整する場合（特にルールを有効化して追加する場合）、一部の侵入ルールでは、最初に特定の方法でトラフィックをデコードまたは前処理する必要があります。侵入ポリシーによって検査される前に、パケットはネットワーク分析ポリシーの設定に従って前処理されます。必要なインスペクタを無効にすると、システムは自動的に現在の設定でインスペクタを使用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではインスペクタは無効のままになります。

注意 前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する**必要があります**。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、**高度な**タスクです。

カスタム侵入ポリシーを設定した後、それを 1 つ以上のアクセス コントロール ルールまたはアクセス 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ることによって、カスタム侵入ポリシーをアクセスコントロール設定の一部として使用できます。これによって、システムは、最終宛先に渡す前に、特定の許可されたトラフィックを侵入ポリシーによって検査します。変数セットを侵入ポリシーと組み合わて使用することにより、ホーム ネットワークと外部ネットワークに加えて、必要に応じてネットワーク上のサーバを正確に反映させることができます。

デフォルトでは、暗号化ペイロードの侵入インスペクションは無効化されます。これにより、侵入インスペクションが設定されているアクセス コントロール ルールと暗号化された接続を照合する際の誤検出が減少し、パフォーマンスが向上します。

追加のサポートと情報については、「Snort 3 侵入ポリシーの概要」ビデオを参照してください。

ネットワーク分析と侵入ポリシーの前提条件

Snort検査エンジンが侵入およびマルウェア分析のトラフィックを処理できるようにするには、Firewall Threat Defense デバイスに対して IPS ライセンスを有効にする必要があります。

ネットワーク分析、侵入ポリシーを管理し、移行タスクを実行するには、管理者ユーザーである必要があります。

カスタム Snort 3 侵入ポリシーの作成

手順

ステップ 1 **Policies** > **Access Control heading** > **Intrusion**を選択します。

ステップ 2 [ポリシーの作成（Create Policy）] をクリックします。

ステップ 3 [名前（Name）] に一意の名前を入力し、オプションで [説明（Description）] を入力します。

ステップ 4 [検査モード（Inspection Mode）] を選択します。

選択したアクションによって、侵入ルールでブロックしてアラートを発生させるか（**防御**モード）、またはアラートを発生させるのみにするか（**検出**モード）が決まります。

（注）
防御モードを選択する前に、多くの誤検出の原因となるルールを特定できるように、ブロックルールのみにアラートを発生させることができます。

ステップ 5 [ベースポリシー（Base Policy）] を選択します。

システム提供のポリシーまたは既存のポリシーをベースポリシーとして使用できます。

ステップ 6 [保存（Save）] をクリックします。

新しいポリシーにはベースポリシーと同じ設定項目が含まれています。

次のタスク

ポリシーをカスタマイズするには、Snort 3 侵入ポリシーの編集 （3 ページ）を参照してください。

Snort 3 侵入ポリシーの編集

Snort 3 ポリシーを編集している間、すべての変更は即座に保存されます。変更を保存するための追加のアクションは必要ありません。

手順

ステップ 1 **Policies** > **Access Control heading** > **Intrusion** を選択します。

ステップ 2 [侵入ポリシー（Intrusion Policies）] タブが選択されていることを確認します。

ステップ 3 設定する侵入ポリシーの横にある [Snort 3バージョン（Snort 3 Version）] をクリックします。

ステップ 4 ポリシーを編集します。

- モードの変更：検査モードを変更するには、[モード（Mode）] ドロップダウンをクリックします。

注意
検査モードは、Snort 3 バージョンのポリシーでのみ変更されます。既存の検査モードは Snort 2 バージョンでそのまま保持されます。つまり、Snort 2 バージョンと Snort 3 バージョンのポリシーの検査モードは異なることになります。そのため、このオプションは注意して使用することを推奨します。

- [防御（Prevention）]：トリガーされたブロックルールはイベント（アラート）を作成し、接続をドロップします。
- [検出（Detection）]：トリガーされたブロックルールはアラートを生成します。

  防御モードに入る前に、検出モードを選択できます。たとえば、防御モードを選択する前に、多くの誤検出の原因となるルールを特定できるように、ブロックルールでアラートのみを生成することができます。

ステップ 5 侵入ポリシーのデフォルト設定を定義する [ベースポリシー（Base Policy）] レイヤをクリックします。

- 検索ルール：検索フィールドを使用して表示をフィルタ処理します。GID、SID、ルールメッセージ、または参照情報を入力できます。たとえば、GID:1; SID:9621 はルール 1:962 のみを表示し 、SID:9621,9622,9623 は異なる SID を持つ複数のルールを表示します。[検索（Search）] テキストボックス内をクリックして、次のオプションのいずれかを選択することもできます。
  - フィルタ [アクション = アラート（Action = Alert）] または [アクション：ブロック（Action: Block）] を適用する
  - [無効なルール（Disabled Rules）] フィルタを適用する
  - [カスタム/ユーザ定義ルール（Custom/User Defined Rules）] を表示する
  - GID、SID、または GID:SID でフィルタ処理する
  - CVE でフィルタ処理する
  - コメントでフィルタ処理する

- フィルタ処理されたルールの表示：[プリセット（Presets）]のいずれかをクリックすると、アラート、ブロック、無効などに設定されているルールが表示されます。

  オーバーライドされたルールは、ルールアクションがデフォルトアクションから別のアクションに変更されたルールを示します。変更すると、元のデフォルトアクションに戻す場合でも、ルールアクションのステータスは[オーバーライド済み（Overridden）]になります。ただし、[ルールアクション（Rule Action）]ドロップダウンリストから[デフォルトに戻す（Revert to default）]を選択すると、[オーバーライド済み（Overridden）]ステータスが削除されます。

  [高度なフィルタ（Advanced Filters）]は、Lightweight Security Package（LSP）のリリース、侵入の分類、およびMicrosoftの脆弱性に基づくフィルタオプションを提供します。

- ルールドキュメントの表示：ルールのTalosマニュアルを表示するには、ルールIDまたは[ルールマニュアル（Rule Documentation）]アイコンをクリックします。

- ルールの詳細の表示：ルールの詳細を表示するには、ルール行の**Expand Arrow**（›）アイコンをクリックします。

- ルールコメントを追加：[コメント（Comments）]列で**Comment**（💬）をクリックし、ルールに対してコメントを追加します。

ステップ6 グループのオーバーライド：ルールグループのすべてのルールカテゴリが一覧表示される[グループのオーバーライド（Group Overrides）]レイヤをクリックします。Description、Overrides、Enabled Groupsなどを含むトップレベルの親ルールグループが表示されます。親ルールグループは更新できず、読み取り専用です。リーフルールグループのみを更新できます。各ルールグループで、最後のリーフグループまでトラバースできます。各グループ全体で、ルールグループを上書き、包含、および除外できます。リーフルールグループでは、次のことができます。

- ルールグループの検索：検索フィールドを使用してキーワードを入力し、ルールグループを検索します。
- 左側のパネルで、ルールグループを検索するためのプリセット フィルタ オプションのいずれかを選択できます。
  - [すべて（All）]：すべてのルールグループを表示します。
  - [除外（Excluded）]：除外されたグループを表示します。
  - [含む（Included）]：含まれているグループを表示します。
  - [オーバーライド（Overridden）]：設定がオーバーライドされたルールグループを表示します。
- ルールグループのセキュリティレベルの設定：左側のペインで必要なルールグループに移動し、クリックします。システム定義のルール設定に基づいてセキュリティレベルを引き上げるか、または引き下げるには、ルールグループの[セキュリティレベル（Security Level）]の横にある[編集（Edit）]をクリックします。

[セキュリティレベルの編集（Edit Security Level）] ダイアログボックスには、[デフォルトに戻す（Revert to Default）] をクリックするオプションがあります。これにより、行った変更が元に戻ります。

Firewall Management Center は、設定されたセキュリティレベルのルールグループのルールアクションを自動的に変更します。[ルールのオーバーライド（Rule Overrides）] レイヤで、セキュリティレベルを変更するたびに、[事前設定（Presets）] の [ブロックルール（Block Rules）] と [無効ルール（Disabled Rules）] の数に注意してください。

- セキュリティレベルを一括変更して、特定のルールカテゴリ内のすべてのルールグループのセキュリティレベルを変更できます。セキュリティレベルの一括変更は、複数のルールグループを含むルールグループに適用されます。ルールグループの一括更新後も、その中の関連するルールグループのセキュリティレベルを更新できます。

  ルールグループ内で [混在（mixed）] セキュリティレベルとすることができます。[混在（mixed）] は、子グループに親ルールグループ内のセキュリティレベルが混在していることを示します。

- ルールグループを含めるまたは除外する：表示されるルールグループは、システムによって提供される基本の侵入ポリシーに関連付けられているデフォルトのルールグループです。侵入ポリシーにルールグループを含めたり、除外したりできます。除外されたルールグループは侵入ポリシーから削除され、そのルールはトラフィックに適用されません。Firewall Management Center にカスタムルールをアップロードする方法については、ルールグループへのカスタムルールの追加を参照してください。

  ルールグループを除外するには、次の手順を実行します。

  1. [ルールグループ（Rule Groups）] ペインに移動し、除外するルールグループを選択します。
  2. 右側のペインで [除外（Exclude）] ハイパーリンクをクリックします。
  3. [除外（Exclude）] をクリックします。

  アップロードされたカスタムルールまたは以前に除外されたルールグループを使用して 1 つまたは複数の新しいルールグループを含めるには、次の手順を実行します。

  1. ルール グループ フィルタ ドロップダウン リストの横にある **Add** (+) をクリックします。
  2. ルールグループの横にあるチェックボックスをオンにして、追加するグループをすべて選択します。
  3. [保存（Save）] をクリックします。

- リーフルールグループの場合、[オーバーライド（Override）] 列ヘッダーの下にあるアイコンをクリックして、ルールアクションの証跡を表示します。これは、侵入ルールのベースポリシーおよびグループのオーバーライドのために割り当てることができる、オーバーライドされたルールアクションのシーケンスを示しています。ルールアクションは、ベースポリシー構成またはユーザーグループのオーバーライドから取得できます。ユーザーグ

ループのオーバーライドは、この2つの間の優先順位を取得します。優先順位は、ルールグループに割り当てられた、オーバーライドされた最終的なアクションを参照します。

- [ルールカウント（Rule Count）] 列ヘッダーの下にあるルールカウント（数）をクリックして、ルールグループの一部であるルールの概要を表示します。

ステップ 7 **推奨事項**：シスコが推奨するルールを生成して適用する場合は、[推奨事項（Recommendations）] レイヤをクリックします。推奨事項は、ホストのデータベースを使用して、既知の脆弱性に基づいてルールを有効または無効にします。

ステップ 8 **ルールのオーバーライド**：[ルールのオーバーライド（Rule Overrides）] レイヤをクリックして、アラート、ブロック、無効、オーバーライド済み、書き換え、パス、ドロップ、または拒否に設定されているルールを表示する、いずれかのプリセットを選択します。

- [設定者（Set By）] 列には、状態（ベースポリシー）ごとのデフォルトのセット、またはグループのオーバーライド、ルールのオーバーライド、または推奨事項ごとに変更されたルールの状態が表示されます。[すべてのルール（All Rules）]（左ペイン）の [設定者（Set By）] 列には、優先順位に基づいたルールアクションのオーバーライドアクションの証跡が表示されます。ルールアクションの優先順位は、[ルールのオーバーライド（Rule Override）] > [推奨事項（Recommendations）] > [グループのオーバーライド（Group Override）] > [ベースポリシー（Base Policy）] です。
- [ルールアクション（Rule Action）] の変更：ルールアクションを変更するには、次のいずれかを選択します。
  - 一括編集：1 つまたは複数のルールを選択し、[ルールアクション（Rule Action）] ドロップダウンリストから必要なアクションを選択し、[保存（Save）] をクリックします。

    （注）
    ルールアクションの一括変更は、最初の 500 個のルールでのみサポートされます。

  - 単一ルールの編集：[ルールアクション（Rule Action）] 列のドロップダウンリストからルールアクションを選択します。

  ルールアクションは次のとおりです。

  - [ブロック（Block）]：イベントを生成し、現在の一致するパケットと、この接続内の後続のすべてのパケットをブロックします。
  - [アラート（Alert）]：一致するパケットのイベントのみを生成し、パケットまたは接続をドロップしません。
  - [無効（Disabled）]：このルールとトラフィックを照合しません。イベントは生成されません。
  - [デフォルトに戻す（Revert to default）]：システムのデフォルトアクションに戻します。
  - [成功（Pass）]：イベントは生成されず、後続の Snort ルールによる以降の評価なしでパケットが通過できます。

（注）
[成功（Pass）] アクションは、カスタムルールでのみ使用でき、システム提供のルールでは使用できません。

- [ドロップ（Drop）]：イベントを生成し、一致するパケットをドロップし、この接続でそれ以上のトラフィックをブロックしません。
- [拒否（Reject）]：イベントを生成し、一致するパケットをドロップし、この接続で後続のトラフィックをブロックして、TCP プロトコルの場合は TCP リセットを送信元および接続ホストに送信します。

  クライアントまたはサーバーに関連するさまざまなファイアウォールモードおよびIPアドレスまたは送信元または宛先での拒否の動作：Snort は、ルーティングされた、インライン、およびブリッジされたインターフェイスの場合、クライアントとサーバーの両方に RST パケットを送信します。Snort は 2 つの RST パケットを送信します。クライアント方向の RST パケットでは、送信元がサーバーの IP に設定され、宛先がクライアントの IP に設定されます。サーバー方向の RST パケットでは、送信元がクライアントの IP に設定され、宛先がサーバーの IP に設定されます。
- [書き換え（Rewrite）]：ルールの置き換えオプションに基づいて、イベントを生成し、パケットの内容を上書きします。

IPS ルールアクションのロギングについては、「ルールアクションのロギング （9 ページ）」を参照してください。

[対応（React）] ルールがある場合は、アラートアクションに変換されます。

ステップ 9 ポリシーに対する現在の変更の全体像を表示するには、[概要（Summary）] レイヤをクリックします。[ポリシーの概要（policy summary）] ページには次の情報が表示されます。

- ポリシーのルール分布、つまり、アクティブなルール、無効なルールなど。
- ポリシーをエクスポートし、侵入ポリシーのレポートを生成するオプション。
- ベースポリシーの詳細。
- 推奨事項を生成するオプション。
- オーバーライドしたグループのリストを表示するグループオーバーライド。
- オーバーライドしたルールのリストを表示するルールオーバーライド。
- [概要（Summary）] レイヤで、[?] アイコンをクリックして、Snort レイヤリングの概念を説明する Snort ヘルパーガイドのポップアップウィンドウを開きます。

ベースポリシーを変更するには、侵入ポリシーのベースポリシーの変更 （10 ページ）を参照してください。

（注）

[**Objects** > **Intrusion Rules**] に移動し、[Snort 3すべてのルール（Snort 3 All Rules）] タブをクリックして、すべての侵入ルールグループをトラバースできます。親ルールグループには、関連する子グループとルール数がリストされます。

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。

ルールグループのレポート

ルールグループは、生成された侵入イベントに反映され、MITRE の戦術と手法も呼び出されます。MITRE の戦術と手法の列と、侵入イベントの非 MITRE ルールグループの列があります。侵入イベントにアクセスするには、Firewall Management Center で **Analysis** > **Intrusions** > **Events** に移動し、[イベントのテーブルビュー（Table View of Events）] タブをクリックします。[統合されたイベント（Unified Events）] ビューアに侵入イベントフィールドを表示することもできます。[分析（Analysis）] タブで、[統合されたイベント（Unified Events）] をクリックします。

[侵入イベント（Intrusion Events）] ページに、ルールグループのレポート用に次のフィールドが追加されます。以下の列を明示的に有効にする必要があることに注意してください。

- MITRE ATT&CK
- ルールグループ

これらのフィールドの詳細については、『Cisco Secure Firewall Management Center Administration Guide, 7.3』の「Intrusion Event Fields」セクションを参照してください。

ルールアクションのロギング

Firewall Management Center 7.2.0 以降、[侵入イベント（Intrusion Events）] ページの [インライン結果（Inline Result）] 列のイベントには、ルールに適用された IPS アクションと同じ名前が表示されるため、ルールに一致するトラフィックに適用されたアクションを確認できます。

IPS アクションについて、次の表に、[侵入イベント（Intrusion Events）] ページの [インライン結果（Inline Result）] 列と、[統合されたイベント（Unified Events）] ページの [侵入イベントタイプ（Intrusion Event Type）] の [アクション（Action）] 列に表示されるイベントを示します。

IPS アクション（Snort 3）	**インライン結果 - Firewall Management Center 7.1.0 以前**	**インライン結果 - Firewall Management Center 7.2.0 以降**
アラート（Alert）	成功（Pass）	アラート（Alert）
ブロック（Block）	Dropped/Would Have Dropped/Partially Dropped	Block/Would Block/Partial Block

IPS アクション（Snort 3）	インライン結果 - Firewall Management Center 7.1.0 以前	インライン結果 - Firewall Management Center 7.2.0 以降
削除（Drop）	Dropped/Would have dropped	Drop/Would drop
拒否（Reject）	Dropped/Would have dropped	Reject/Would reject
書き換え（Rewrite）	許可（Allow）	書き換え（Rewrite）

重要

- [置換（Replace）]オプションのないルールの場合、**書き換え**アクションは「**Would Rewrite**」と表示されます。
- また、[置換（Replace）] オプションが指定されているが、IPS ポリシーが検出モードであるか、デバイスがインライン TAP/パッシブモードである場合に、**書き換え**アクションは「**Would Rewrite**」と表示されます。

（注） 後方互換性の場合（Firewall Management Center 7.2.0 が Firewall Threat Defense 7.1.0 デバイスを管理している）、言及されているイベントは、[成功（Pass）]がイベントの[アラート（Alert）]として表示されるアラート IPS アクションにのみ適用されます。他のすべてのアクションについては、Firewall Management Center 7.1.0 のイベントが適用されます。

侵入ポリシーのベースポリシーの変更

別のシステム提供のポリシーまたはカスタム ポリシーを基本ポリシーとして使用できます。

最大 5 つのカスタム ポリシーをチェーンすることができます。5 つのうちの 4 つのポリシーで事前に作成されたポリシーが基本ポリシーとして使用され、5つ目のポリシーでシステムによって提供されたポリシーをベースとして使用する必要があります。

手順

ステップ 1 **Policies** > **Access Control heading** > **Intrusion** を選択します。

ステップ 2 設定する侵入ポリシーの横にある **Edit** (✎) をクリックします。

ステップ 3 [ベースポリシー（Base Policy）] ドロップダウンリストからポリシーを選択します。

ステップ 4 [保存（Save）] をクリックします。

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。

Snort 2 と Snort 3 のベースポリシーのマッピングの表示

（注） Snort 2 は、Threat Defense バージョン 7.7ではサポートされていません。7.7 より前のバージョンでサポートされている Snort 2 機能については、ご使用の Firewall Threat Defense のバージョンに対応する Firewall Management Center のガイドを参照してください。

手順

ステップ 1 **Policies** > **Access Control heading** > **Intrusion**を選択します。

ステップ 2 [侵入ポリシー（Intrusion Policies）] タブが選択されていることを確認します。

ステップ 3 [IPS マッピング（IPS Mapping）] をクリックします。

ステップ 4 [IPSポリシーマッピング（IPS Policy Mapping）] ダイアログボックスで、[マッピングの表示（View Mappings）] をクリックして、Snort 3 から Snort 2 への侵入ポリシーのマッピングを表示します。

ステップ 5 [OK] をクリックします。

Snort 2 のルールと Snort 3 の同期

Snort 2 のバージョン設定とカスタムルールが保持され、Snort 3 に引き継がれるための同期機能が Firewall Management Center によって提供されます。同期することで、過去数か月または数年にわたって変更または追加されている可能性がある、Snort 2 ルールのオーバーライド設定とカスタムルールを Snort 3 バージョンで複製できます。このユーティリティは、Snort 2 バージョンのポリシー設定を Snort 3 バージョンと同期して、同様の対象範囲で開始するのに役立ちます。

（注） Snort 2 は、Threat Defense バージョン 7.7ではサポートされていません。7.7 より前のバージョンでサポートされている Snort 2 機能については、ご使用の Firewall Threat Defense のバージョンに対応する Firewall Management Center のガイドを参照してください。

Firewall Management Center を 6.7 より前のバージョンから 7.0 以降のバージョンにアップグレードすると、設定が同期されます。Firewall Management Center が新しい 7.0 移行のバージョンの

場合、より高いバージョンにアップグレードできますが、アップグレード中にコンテンツは同期されません。

デバイスを Snort 3 にアップグレードする前に、Snort 2 バージョンで変更が行われた場合は、このユーティリティを使用して Snort 2 バージョンから Snort 3 バージョンに最新の同期を行うことができ、同様の対象範囲で開始できます。

（注） Snort 3 への移行時に、Snort 3 バージョンのポリシーを別個に管理し、通常の運用としてこのユーティリティを使用しないことを推奨します。

重要
- Snort 2 ルールのオーバーライドとカスタムルールのみが Snort 3 にコピーされ、その逆は行われません。Snort 2 と Snort 3 のすべての侵入ルールの 1 対 1 のマッピングが見つからない場合があります。次の手順を実行すると、両方のバージョンに存在するルールのルールアクションに対する変更が同期されます。
- 同期では、カスタムまたはシステムによって提供されるルールのしきい値と抑制の設定は Snort 2 から Snort 3 に移行されません。

手順

ステップ 1 **Policies** > **Access Control heading** > **Intrusion** を選択します。

ステップ 2 [侵入ポリシー（Intrusion Policies）] タブが選択されていることを確認します。

ステップ 3 [Snort 3 の同期ステータスの表示（Show Snort 3 Sync status）] をクリックします。

ステップ 4 同期していない侵入ポリシーを特定します。

ステップ 5 [同期（Sync）] アイコン **Snort out-of-Sync** (🔶) をクリックします。

（注）
侵入ポリシーの Snort 2 と Snort 3 バージョンが同期されている場合、[同期（Sync）] アイコンが、青**Snort in-Sync** (🔷) で表示されます。

ステップ 6 サマリーを読み、必要に応じてサマリーのコピーをダウンロードします。

ステップ 7 [再同期（Re-Sync）] をクリックします。

（注）
- 同期された設定は、Snort 3 侵入エンジンがデバイスに適用され、展開が成功した後にのみ適用されます。
- Snort 2 カスタムルールは、システム付属のツールを使用して Snort 3 に変換できます。Snort 2 カスタムルールがある場合は、[カスタムルール（Custom Rules）] タブをクリックし、

画面の指示に従ってルールを変換します。詳細については、単一の侵入ポリシーの Snort 2 カスタムルールの Snort 3 への変換を参照してください。

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。

侵入ポリシーの管理

[侵入ポリシー（Intrusion Policy）] ページ（**Policies** > **Access Control heading** > **Intrusion**）では、次に示す情報とともに、現在のカスタム侵入ポリシーを表示できます。

- トラフィックの検査に侵入ポリシーを使用しているアクセス コントロール ポリシーとデバイスの数
- マルチドメイン展開では、ポリシーが作成されたドメイン

（注） Snort 2 は、Threat Defense バージョン 7.7ではサポートされていません。7.7 より前のバージョンでサポートされている Snort 2 機能については、ご使用の Firewall Threat Defense のバージョンに対応する Firewall Management Center のガイドを参照してください。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **Policies** > **Access Control heading** > **Intrusion**を選択します。

ステップ 2 侵入ポリシーを管理します。

- 作成：[ポリシーの作成（Create Policy）] をクリックします。カスタム Snort 3 侵入ポリシーの作成 （3 ページ）を参照してください。
- 削除：削除するポリシーの横にある **Delete**（ ）をクリックします。別のユーザが保存していないポリシーの変更がある場合は、システムによって確認と通知のプロンプトが表示されます。[OK] をクリックして確認します。

  コントロールが淡色表示されている場合、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。

- 侵入ポリシーの詳細の編集：編集するポリシーの横にある **Edit**（✎）をクリックします。侵入ポリシーの [名前（Name）]、[検査モード（Inspection Mode）]、および [ベースポリシー（Base Policy）] を編集できます。
- 侵入ポリシー設定の編集：[Snort 3 バージョン（Snort 3 Version）] をクリックします。Snort 3 侵入ポリシーの編集 （3 ページ）を参照してください。
- エクスポート：侵入ポリシーをエクスポートして別の Firewall Management Center にインポートする場合は、[エクスポート（Export）] をクリックします。最新バージョンの『*Cisco Secure Firewall Management Center Configuration Guide*』の「*Exporting Configurations*」トピックを参照してください。
- 展開：**[展開（Deploy）] > [展開（Deployment）]** を選択します。設定変更の展開を参照してください。
- レポート：[レポート（Report）] をクリックします。最新バージョンの『*Cisco Secure Firewall Management Center Configuration Guide*』の「*Generating Current Policy Reports*」トピックを参照してください。ポリシーバージョンごとに 1 つずつ、2 つのレポートを生成します。

侵入防御を実行するためのアクセスコントロールルール設定

アクセス コントロール ポリシーは、複数のアクセス コントロール ルールを侵入ポリシーに関連付けることができます。侵入インスペクションを許可アクセス コントロール ルールまたはインタラクティブ ブロック アクセス コントロール ルールに設定でき、これによって、トラフィックが最終宛先に到達する前に、異なる侵入インスペクションプロファイルをネットワーク上のさまざまなタイプのトラフィックと照合できます。

システムは侵入ポリシーを使用してトラフィックを評価するたびに、関連する変数セット使用します。セット内の変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先の IP アドレスおよびポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制および動的ルール状態にある IP アドレスを表すこともできます。

システムによって提供される侵入ポリシーとカスタム侵入ポリシーについて

システムには複数の侵入ポリシーが付属しています。システムによって提供される侵入ポリシーを使用することで、Cisco Talos インテリジェンスグループ（Talos）の経験を活用できます。これらのポリシーでは、Talos は侵入ルールとプリプロセッサルールの状態を設定し、詳細設定の初期設定も提供します。システムによって提供されるポリシーをそのまま使用するか、またはカスタム ポリシーのベースとして使用できます。カスタム ポリシーを作成すれば、環境内のシステムのパフォーマンスを向上させ、ネットワーク上で発生する悪意のあるトラフィックやポリシー違反に焦点を当てたビューを提供できます。

接続イベントおよび侵入イベントのロギング

アクセス制御ルールによって呼び出された侵入ポリシーが侵入を検出すると、侵入イベントを生成し、そのイベントをManagement Centerに保存します。また、システムはアクセス制御ルールのロギング設定に関係なく、侵入が発生した接続の終了も Management Center データベースに自動的にロギングします。

アクセス コントロール ルール設定と侵入ポリシー

1 つのアクセス コントロール ポリシーで使用可能な一意の侵入ポリシーの数は、ターゲットデバイスのモデルによって異なります。より強力なデバイスは、より多数のポリシーを処理できます。侵入ポリシーと変数セットの固有の**ペア**はすべて、1 つのポリシーと見なされます。異なる侵入ポリシーと変数セットのペアをそれぞれの許可ルールおよびインタラクティブ ブロック ルール（およびデフォルト アクション）と関連付けることができますが、ターゲットデバイスが設定されたとおりに検査を実行するのに必要なリソースが不足している場合は、アクセス コントロール ポリシーを展開できません。

侵入防御を実行するアクセスコントロールルールの設定

このタスクを実行するには、管理者、アクセス管理者、またはネットワーク管理者である必要があります。

手順

ステップ 1 アクセス コントロール ポリシー エディタで新しいルールを作成するか、既存のルールを編集します。最新バージョンの『*Cisco Secure Firewall Management Center Configuration Guide*』の「*Access Control Rule Components*」を参照してください。

ステップ 2 ルール アクションが [許可（Allow）]、[インタラクティブ ブロック（Interactive Block）]、または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] に設定されていることを確認します。

ステップ 3 [検査（Inspection）] をクリックします。

ステップ 4 システムによって提供される侵入ポリシーまたはカスタムの侵入ポリシーを選択するか、あるいはアクセス コントロール ルールに一致するトラフィックに対する侵入検査を無効にするには [なし（None）] を選択します。

ステップ 5 侵入ポリシーに関連付けられた変数セットを変更するには、[変数セット（Variable Set）] ドロップダウン リストから値を選択します。

ステップ 6 [保存（Save）] をクリックしてルールを保存します。

ステップ 7 [保存（Save）] をクリックしてポリシーを保存します。

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。

設定変更の展開

設定を変更した後に、影響を受けるデバイスに展開します。

（注） このトピックでは、設定変更を展開する基本的な手順について説明します。手順を進める前に、最新バージョンの『*Cisco Secure Firewall Management Center Configuration Guide*』の「*Deploy Configuration Changes*」トピックを参照し、変更を展開する上での前提条件と影響を理解しておくことを強く推奨します。

注意 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断するSnortプロセスが再開します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。

手順

ステップ 1 Secure Firewall Management Center メニューバーで、[展開（Deploy）] をクリックし、[展開（Deployment）] を選択します。

[GUI]ページには、期限切れの設定を持ち、ステータスが [保留中（Pending）] のデバイスのリストが表示されます。

- [変更者（Modified by）] 列には、ポリシーまたはオブジェクトを変更したユーザーの一覧が表示されます。デバイスリストを展開すると、ポリシーリストごとのポリシーを変更したユーザーが表示されます。

  （注）
  削除されたポリシーおよびオブジェクトのユーザ名は表示されません。

- [インスペクションの中断（Inspect Interruption）] 列には、展開時にデバイスでトラフィック インスペクションの中断が発生する可能性があるかどうかが示されます。

  デバイスのこの列のエントリが空白の場合は、展開時にそのデバイス上でのトラフィック インスペクションが中断されないことを示します。

- [最終変更時刻（Last Modified Time）] 列は、最後に設定変更を行った時刻を示します。
- [プレビュー（Preview）] 列では、次の展開の変更をプレビューできます。

- [ステータス（Status）] 列には、各展開のステータスが表示されます。

ステップ 2 設定変更を展開するデバイスを特定して選択します。

- [検索（Search）] : [検索（Search）] ボックスのデバイス名、タイプ、ドメイン、グループ、またはステータスを検索します。
- [展開（Expand）] : 展開するデバイス固有の設定変更を表示するには、**Expand Arrow (›)** をクリックします。

  デバイスの横にあるチェックボックスをオンにすると、デバイスに加えられ、デバイスの下にリストされているすべての変更が展開のためにプッシュされます。ただし、**Policy selection** ( ) を使用して展開する個々のポリシーや特定の設定を選択し、残りの変更は展開せずに保持することができます。

  （注）
  - [インスペクションの中断（Inspect Interruption）] 列のステータスに [あり（Yes）] と表示され、展開によって Firewall Threat Defense デバイスでインスペクションと、場合によってはトラフィックが中断されるときは、展開されたリストには中断の原因となった特定の設定が **Inspect Interruption** ( ) で示されます。
  - インターフェイスグループ、セキュリティゾーン、またはオブジェクトに変更がある場合、影響を受けるデバイスは、Firewall Management Center で失効として表示されます。これらの変更が有効になるようにするには、これらのインターフェイスグループ、セキュリティゾーン、またはオブジェクトを含むポリシーも、これらの変更とともに展開する必要があります。影響を受けるポリシーは、Firewall Management Center の [プレビュー（Preview）] ページに失効として表示されます。

ステップ 3 [展開（Deploy）] をクリックします。

ステップ 4 展開する変更に関するエラーや警告がシステムによって識別された場合は、[検証メッセージ（Validation Messages）] ウィンドウにその内容が表示されます。完全な詳細を表示するには、警告またはエラーの前にある矢印アイコンをクリックします。

次の選択肢があります。

- [展開（Deploy）] : 警告状態を解決せずに展開を続行します。システムがエラーを確認した場合は続行できません。
- [閉じる（Close）] : 展開せずに終了します。エラーおよび警告状態を解決し、設定の再展開を試行します。

次のタスク

展開中に展開が失敗した場合、その障害がトラフィックに影響を与える可能性があります。ただし、特定の条件によって異なります。展開に特定の設定変更がある場合、展開の失敗によってトラフィックが中断されることがあります。詳細については、最新バージョンの『*Cisco*

Secure Firewall Management Center Configuration Guide』の「Deploy Configuration Changes」のトピック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。