侵入ポリシーの使用を開始するには

ここでは、侵入ポリシーの使用を開始する方法について説明します。

侵入ポリシーの基本

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的な侵入ポリシーにより、Talos インテリジェンス グループの経験を活用できます。これらのポリシーでは、Talos が侵入およびプリプロセッサ 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。
- Cisco推奨機能を使用して、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、それらのアセットを保護するために作成されたルールに関連付ける。
- 外部アラート、センシティブ データの前処理、グローバル ルールのしきい値設定など、さまざまな詳細設定を設定する。
- レイヤを構成要素として使用し、複数の侵入ポリシーを効率的に管理する。

インライン展開では、侵入ポリシーによってトラフィックを変更したりブロックすることができます。

- 廃棄ルールを使用すると、一致した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廃棄ルールを設定するには、そのステータスを [ドロップしてイベントを生成する（Drop and Generate Events）] に設定します。
- 侵入ルールでは、`replace` キーワードを使用して悪意のあるコンテンツを置き換えることができます。

侵入ルールがトラフィックに影響を与えるようにするには、廃棄ルールおよびコンテンツを置き換えるルールを適切に設定し、さらに管理対象デバイスを適切にインライン展開する（つまり、インライン インターフェイス セットを設定する）必要があります。最後に、侵入ポリシーのドロップ動作（[インライン時にドロップ（Drop when Inline）] 設定）を有効にします。

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。必要なプリプロセッサを無効にすると、システムは自動的に現在の設定でプリプロセッサを使用します。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プリプロセッサ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。

侵入ポリシーのためのライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

侵入ポリシーの要件と前提条件

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

侵入ポリシーの管理

[侵入ポリシー（Intrusion Policy）] ページ（**[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[侵入（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。

- ポリシーが最後に変更された日時（ローカル時間）とそれを変更したユーザー
- [インライン時にドロップ（Drop when Inline）] 設定が有効になっているかどうか。この設定が有効な場合、インライン展開でトラフィックをドロップしたり変更することができます。インライン展開は、ルーテッドインターフェイス、スイッチドインターフェイス、トランスペアレントインターフェイス、あるいはインラインインターフェイスのペアを使用してデバイスに展開される設定です。
- 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
- ポリシーに保存されていない変更があるかどうか、およびポリシーを現在編集している人（いれば）に関する情報

手順

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

ステップ 2 侵入ポリシーを管理します。

- [比較（Compare）]：**[ポリシーの比較（Compare Policies）]** をクリックします（「ポリシーの比較」を参照）。
- 作成：[ポリシーの作成（Create Policy）] をクリックします。次を参照してください。
  - Snort 2 ポリシーの場合は、カスタム Snort 2 検査ポリシーの作成 （5 ページ）。
  - Snort 3 ポリシーの場合は、最新バージョンの『Cisco Secure Firewall Management Center Snort 3 Configuration Guide』の「*Creating a Custom Snort 3 Intrusion Policy*」トピック。
- 削除：削除するポリシーの横にある [削除（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。
- 編集：次を選択します。
  - [Snort 2バージョン（Snort 2 Version）]。Snort 2 侵入ポリシーの編集 （6 ページ）を参照してください。
  - [Snort 3バージョン（Snort 3 Version）]。最新バージョンの『Cisco Secure Firewall Management Center Snort 3 Configuration Guide』の「*Editing Snort 3 Intrusion Policies*」トピックを参照してください。

  代わりに [表示（View）]（  ） 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。

- エクスポート：別の Secure Firewall Management Center にインポートするために、侵入ポリシーをエクスポートするには、[YouTube EDU]（） をクリックします。Cisco Secure Firewall Management Center アドミニストレーション ガイド の 「エクスポート構成」を参照してください。
- [展開（Deploy）]：**[展開（Deploy）]** > **[展開（Deployment）]** をクリックします（設定変更の展開 を参照）。
- レポート：[レポート（Report）]（） をクリックします（現在のポリシーレポートの生成 を参照）。

カスタム侵入ポリシーの作成

新しい侵入ポリシーを作成する場合は、一意の名前を付けて基本ポリシーを指定し、ドロップ動作を指定する必要があります。

基本ポリシーは侵入ポリシーのデフォルト設定を定義します。新しいポリシーの設定の変更は、基本ポリシーの設定を変更するのではなく、オーバーライドします。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。

カスタム Snort 2 検査ポリシーの作成

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[侵入（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。別のポリシー内に未保存の変更が存在する場合は、[Intrusion Policy] ページに戻るかどうか尋ねられたときに [Cancel] をクリックします。

[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 [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。

ステップ 5 [基本ポリシー（Base Policy）] で最初の基本ポリシーを選択します。

システム提供のポリシーまたは別のカスタム ポリシーを基本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。

関連トピック

レイヤでの侵入ルール
競合と変更：ネットワーク分析ポリシーと侵入ポリシー

Snort 2 侵入ポリシーの編集

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[侵入（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 2バージョン（Snort 2 Version）] をクリックします。

ステップ 4 ポリシーを編集します。

- 基本ポリシーの変更：[基本ポリシー（Base Policy）] ドロップダウン リストから基本ポリシーを選択します。基本ポリシーの変更を参照してください。
- 詳細設定の構成：ナビゲーション パネルで [詳細設定（Advanced Settings）] をクリックします。侵入ポリシーの詳細設定 （11 ページ）を参照してください。
- Cisco 推奨ルールの設定：ナビゲーションパネルで **[Cisco推奨事項（Cisco Recommendations）]** をクリックします。Cisco 推奨事項の生成と適用を参照してください。
- インライン展開でのドロップ動作：[インライン時にドロップ（Drop when Inline）] をオンまたはオフにします。インライン展開でのドロップ動作の設定 （10 ページ）を参照してください。
- 推奨ルール状態によるルールのフィルタ：推奨を生成した後、各推奨タイプの横にある [表示（View）] をクリックします。すべての推奨を表示するには、[推奨される変更の表示（View Recommended Changes）] をクリックします。
- 現在のルール状態によるルールのフィルタ：ルール状態タイプ（イベントを生成する、ドロップしてイベントを生成する）の横にある [表示（View）] をクリックします。侵入ポリシー内の侵入ルール フィルタを参照してください。
- ポリシー階層の管理：ナビゲーション パネルで、[ポリシー層（Policy Layers）] をクリックします。レイヤ管理を参照してください。
- 侵入ルールの管理：[ポリシー情報（Policy Information）] をクリックします。侵入ポリシー内の侵入ルールの表示を参照してください。
- 基本ポリシーの設定の表示：[基本ポリシーの管理（Manage Base Policy）] をクリックします。基本レイヤを参照してください。

ステップ 5 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）] を選択して、[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

Cisco 推奨事項の生成と適用
レイヤでの侵入ルールの設定
競合と変更：ネットワーク分析ポリシーと侵入ポリシー

侵入ポリシーの変更

新しい侵入ポリシーを作成すると、そのポリシーには基本ポリシーと同じ侵入ルールと詳細設定が付与されます。

システムは、ユーザごとに1つのセキュリティ ポリシーをキャッシュします。侵入ポリシーの編集中に、メニューまたは別のページへのパスを選択すると、そのページから移動しても、変更内容はシステム キャッシュに残ります。

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。

ヒント システム提供の侵入ポリシーを使用する場合であっても、正確にネットワーク環境を反映するためにシステムの侵入変数を設定することを**強く**推奨します。少なくとも、デフォルトセットにあるデフォルトの変数を変更します。

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。システム提供の侵入ポリシーを使用することで、Talosインテリジェンスグループの経験を活用できます。これらのポリシーでは、Talosは侵入ルールおよびプリプロセッサ 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 コントロール 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 Secure Firewall Management Center に保存します。また、システムはアクセス コントロール 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を Secure Firewall Management Center データベースに自動的にロギングします。

関連トピック

定義済みデフォルト変数

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。アクセス コントロール ルールのコンポーネント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またはカスタムの**侵入ポリシー**を選択するか、またはアクセス 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インスペクションを無効にするには [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。

関連トピック

変数セット

Snort 再起動のシナリオ

インライン展開でのドロップ動作

実際にトラフィックを変更せず、使用している設定がインライン展開（つまり、ルーテッド、スイッチド、またはトランスペアレントインターフェイス、あるいはインラインインターフェイスペアを使用して、関連する設定がデバイスに展開されている）でどのように機能するかを評価する場合は、ドロップ動作を無効にすることができます。その場合、システムは侵入イベントを生成しますが、廃棄ルールをトリガーしたパケットをドロップしません。結果を確認したら、ドロップ動作を有効化できます。

パッシブ展開またはタップモードでのインライン展開では、ドロップ動作に関わらず、システムはトラフィックに影響を与えることはできません。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は [イベントを生成する（Generate Events）] に設定されたルールと同様に動作します。システムは侵入イベントを生成しますが、パケットをドロップすることはできません。

（注） ファイルのブロックアクションにより、ブロックまたは保留中のファイルポリシーによるパケットの判定が発生し、その後、同じパケットで IPS イベントが生成されたとします。その場合、IPS ポリシーが検出モード（IDS）であっても、IPS イベントは Would have dropped ではなく Dropped としてマークされます。

（注） FTP を介してマルウェアの転送をブロックするには、マルウェア防御 を正しく設定するだけでなく、アクセス コントロール ポリシーのデフォルトの侵入ポリシーで [インライン時にドロップ（Drop when Inline）] を有効にする必要があります。

侵入イベントを表示する際に、ワークフローにインライン結果を含めることができます。インライン結果は、トラフィックが実際にドロップされたのか、あるいはドロップが想定に過ぎなかったのかを示します。

インライン展開でのドロップ動作の設定

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[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）]（👁） 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 ポリシーのドロップ動作を設定します。

- [インライン時にドロップ（Drop when Inline）] チェックボックスをオンにして、侵入ルールのトラフィックへの適用とイベントの生成を許可します。
- [インライン時にドロップ（Drop when Inline）] チェックボックスをオフにすると、侵入ルールのトラフィックへの適用が禁止されますが、イベントは生成されます。

ステップ 4 [変更を確定（Commit Changes）] をクリックして、最後のポリシーの確定以降に、このポリシーに加えた変更を保存します。

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。

デュアル システム展開でのドロップ動作

ネットワーク内で2つのシステムが連続して接続されている場合、最初のシステムでドロップイベントが発生しても、2番目のシステムでドロップイベントまたは「ドロップ想定」イベントが記録されることは正常です。最初のシステムがファイルの最後のパケットをスキャンするまでにパケットをドロップすることを決定する一方で、2 番目のシステムもトラフィックを調査して「ドロップされる」と識別します。

たとえば、最初のパケットがルールをトリガーする 5 パケット HTTP GET リクエストは、最初のシステムによりブロックされ、最後のパケットのみがドロップされます。2 番目のシステム

は 4 パケットのみを受信し、接続はドロップされますが、2 番目のシステムがセッションをプルーニングしている間に部分的な GET リクエストを最後にフラッシュすると、インライン結果として「ドロップ想定」と同じルールがトリガーされます。

侵入ポリシーの詳細設定

侵入ポリシーの詳細設定を設定するには、特定の専門知識が必要です。デフォルトで有効になる詳細設定や、詳細設定ごとのデフォルトは、侵入ポリシーの基本ポリシーに応じて決まります。

侵入ポリシーのナビゲーション パネルで [詳細設定（Advanced Settings）] を選択すると、ポリシーの詳細設定がタイプ別に一覧表示されます。[詳細設定（Advanced Settings）] ページでは、侵入ポリシーの詳細設定を有効または無効にしたり、詳細設定の設定ページにアクセスすることができます。詳細設定を行うには、それを有効にする必要があります。

詳細設定を無効にすると、サブリンクと [編集（Edit）] リンクは表示されなくなりますが、設定は保持されます。侵入ポリシーの一部の設定（センシティブ データ ルール、侵入ルールの SNMP アラート）では、詳細設定を有効化して適切に設定する必要があります。

詳細設定を変更する場合、変更する設定と、その変更がネットワークに及ぼす可能性のある影響について理解していることが必要です。

特定の脅威の検出

機密データ プリプロセッサは、ASCII テキストのクレジット カード番号や社会保障番号などの機密データを検出します。

特定の脅威（Back Orifice 攻撃、何種類かのポートスキャン、および過剰なトラフィックによってネットワークを過負荷状態に陥らせようとするレートベース攻撃）を検出するプリプロセッサは、ネットワーク分析ポリシーで設定します。

侵入ルールしきい値（Intrusion Rule Thresholds）

グローバル ルールのしきい値を設定すると、しきい値を使用して、システムが侵入イベントを記録したり表示したりする回数を制限できるので、多数のイベントでシステムが圧迫されないようにすることができます。

外部レスポンス（External Responses）

Web インターフェイス内での侵入イベントをさまざまな形式で表示することに加えて、システム ログ（syslog）ファシリティへのロギングを有効にしたり、イベントデータを SNMP トラップサーバーに送信したりできます。ポリシーごとに、侵入イベントの通知限度を指定したり、外部ロギング ファシリティに対する侵入イベントの通知をセットアップしたり、侵入イベントへの外部応答を設定したりできます。

これらのポリシー単位のアラート設定に加えて、各ルールまたはルール グループの侵入イベントを通知する電子メール アラートをグローバルに有効化/無効化できます。どの侵入ポリシーがパケットを処理するかに関わらず、ユーザの電子メール アラート設定が使用されます。

関連トピック

機密データ検出の基本
グローバル ルールのしきい値の基本

侵入検知と防御のパフォーマンス最適化

Firepower システムを使用して侵入検知および防御を実行するものの検出データを利用する必要がない場合は、以下の説明に従って新しい検出を無効にしてパフォーマンスを最適化できます。

始める前に

このタスクを実行するには、次のいずれかのユーザーロールが必要です。

- アクセス制御用の管理者、アクセス管理者、またはネットワーク管理者。
- ネットワーク検出用の管理者または検出管理者。

手順

ステップ 1 ターゲット デバイスに導入したアクセス コントロール ポリシーと関連付けられたルールを変更または削除します。そのデバイスに関連付けられたアクセス制御ルールはいずれも、ユーザ、アプリケーション、または URL の条件を指定できません（アクセスコントロールルールの作成および編集を参照）。

ステップ 2 ターゲット デバイスのネットワーク検出ポリシーからすべてのルールを削除します（ネットワーク検出ルールの設定を参照）。

ステップ 3 変更された設定をターゲット デバイスに導入します（設定変更の展開を参照）。

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。