侵入ポリシー

次のトピックでは、侵入ポリシーと密接に関連付けられているネットワーク分析ポリシー（NAP）について説明します。侵入ポリシーには、脅威についてトラフィックをチェックし、攻撃が判明したトラフィックをブロックするルールが含まれます。ネットワーク分析ポリシーは、トラフィックを正規化してプロトコルの異常を識別することによってさらに検査するためにトラフィックの準備を行う、トラフィックの前処理を制御します。

前処理と侵入検査を非常に密接に関連しているため、1 つのパケットを調べるネットワーク分析と侵入ポリシーはお互いを補完する必要があります。

侵入ポリシーとネットワーク分析ポリシーについて

ネットワーク分析ポリシーと侵入ポリシーは、共同で侵入の脅威を検出し、防ぎます。

- ネットワーク分析ポリシー（NAP）では、トラフィックの復号化および前処理の方法について、特に侵入の試行を示す可能性がある異常なトラフィックをさらに評価できるよう、制御します。
- 侵入ポリシーでは、侵入ルールと呼ばれる侵入やプリプロセッサのルールを使用し、パターンに基づいて攻撃がないかデコードされたパケットを調べます。ルールでは、脅威となるトラフィックを防いで（ドロップして）イベントを生成したり、単に検出（警告）してイベントの生成のみを行うことができます。

システムがトラフィックを分析するとき、ネットワーク分析の復号化および前処理のフェーズは、侵入防御のフェーズより前に、個別に発生します。ネットワーク分析ポリシーと侵入ポリシーを一緒に使用すると、広範囲で詳細なパケットインスペクションを行うことができます。このポリシーは、ホストとそのデータの可用性、整合性、機密性を脅かす可能性のあるネットワーク トラフィックの検知、通知および防御に役立ちます。

システム定義のネットワーク分析および侵入ポリシー

システムには、相互に補完して動作する、同じ名前のネットワーク分析と侵入ポリシーのいくつかのペアが含まれています。たとえば「バランスのとれたセキュリティと接続性」という名前の NAP と侵入ポリシーの両方があり、一緒に使用されることを意図しています。システム提供のポリシーは、Cisco Talos Intelligence Group（Talos）によって設定されます。これらのポリシーに対して Talos は侵入とプリプロセッサルールの状態を設定し、プリプロセッサの最初の設定とその他の高度な設定を行います。

新たな脆弱性が既知になると、Talos は侵入ルールの更新をリリースします。これらのルール更新により、システム付属のネットワーク分析ポリシーや侵入ポリシーが変更され、侵入ルールやプリプロセッサルールの新規作成または更新、既存ルールのステータスの変更、デフォルトのポリシー設定の変更が実施されます。ルールの更新はまた、システム提供のポリシーからルールを削除、新しいルールのカテゴリを提供、デフォルトの変数セットを変更できます。

手動で、ルールデータベースを更新したり、定期的な更新スケジュールを設定できます。有効にするには更新を展開する必要があります。システムデータベースの更新についての詳細は、システム データベースの更新を参照してください。

次にシステム提供のポリシーについて示します。

[バランスのとれたセキュリティと接続性（Balanced Security and Connectivity）] ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、速度と検出の両方を目的として作成されています。これらを一緒に使用すると、ほとんどの種類のネットワークおよび展開に適した出発点として機能します。[バランスのとれたセキュリティと接続性（Balanced Security and Connectivity）] ネットワーク分析ポリシーがデフォルトとして使用されます。

[セキュリティよりも接続性を優先（Connectivity Over Security）] ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、接続性、すべてのリソースを取得する機能が、ネットワークインフラストラクチャのセキュリティよりも優先されるネットワーク向けに作られています。この侵入ポリシーは、[接続性よりもセキュリティを優先（Security over Connectivity）] ポリシー内で有効になっているルールよりもはるかに少ないルールを有効にします。トラフィックをブロックする最も重要なルールだけが有効にされます。

[接続性よりもセキュリティを優先（Security over Connectivity）] ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、ネットワークインフラストラクチャのセキュリティがユーザの利便性より優先されるネットワーク向けに作られています。この侵入ポリシーは、正式なトラ

フィックに対して警告またはドロップする可能性のある膨大な数のネットワーク異常侵入ルールを有効にします。

[最大検出（Maximum Detection）] ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、ネットワークインフラストラクチャのセキュリティが、運用に対する影響が大きい、[接続性よりもセキュリティを優先（Security Over Connectivity）] ポリシーで考慮されるセキュリティよりもさらに重視されるネットワーク向けに作られています。たとえば、この侵入ポリシーでは、マルウェア、エクスプロイトキット、古い脆弱性や一般的な脆弱性、および既知の流行中のエクスプロイトを含め、多数の脅威カテゴリのルールを有効にします。

検査モード：防御と検出

デフォルトでは、侵入防御システム（IPS）を実装するため、すべての侵入ポリシーが防御モードで動作します。防御インスペクションモードでは、トラフィックを切断するアクションの侵入ルールと接続が一致する場合、接続は能動的にブロックされます。

一方、ネットワーク上で侵入ポリシーの影響をテストするには、侵入検知システム（IDS）を実装する「検出」にモードを変更します。このインスペクションモードでは、ドロップルールはアラートルールと同様に扱われます。この場合、一致する接続が通知されますが、アクションの結果がブロックされ、実際に接続がブロックされることはありません。

侵入ポリシーごとにインスペクションモードを変更するため、防御と検出を混在させることができます。

侵入ルールおよびプリプロセッサ ルール

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。

システムには、Cisco Talos Intelligence Group（Talos） によって作成された次のタイプのルールが含まれています。

- 侵入ルール。共有オブジェクト ルールおよび標準のテキスト ルールに細分されます。
- プリプロセッサルール。プリプロセッサと、ネットワーク分析ポリシーのパケットデコーダ検出オプションが関連付けられたルールです。デフォルトではほとんどのプリプロセッサ ルールは無効です。

ここでは、侵入ルールについてより詳細に説明します。

侵入ルール属性

侵入ポリシーを表示すると、脅威を特定するために利用できるすべての侵入ルールのリストが示されます。

各ポリシーのルールのリストは同じです。異なる点は、各ルールに設定されたアクションです。30,000 を超えるルールがあるため、リスト全体をスクロールするには時間がかかります。ルールは、リストをスクロールしていくと順に表示されます。

次に、各ルールを定義する属性を示します。

> (シグニチャの説明)

左の列の [>] ボタンをクリックして、署名の説明を開きます。説明は、トラフィックとルールを照合するために、Snort インスペクション エンジンによって使用されます。コードの説明はこのドキュメントの範囲外ですが、『Management Center Configuration Guide』で詳しく説明しています。http://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html からご使用のソフトウェアのバージョン用のブックを選択してください。侵入ルールの編集についての情報を探します。

署名には、特定の項目の変数が含まれています。詳細については、「デフォルトの侵入変数セット （5 ページ）」を参照してください。

GID

ジェネレータ識別子（ID）。この数は、ルールを評価し、イベントを生成する、システムコンポーネントを示します。1 は標準テキスト侵入ルール、3 は共有オブジェクト侵入ルールを示します（これらのルールタイプの違いは Firewall Device Manager ユーザーにとって意味はありません）。これらは、侵入ポリシーを設定するときに対象となる主なルールです。その他の GID の詳細については、ジェネレータ識別子 （6 ページ）を参照してください。

SID

Snort 識別子（ID）。署名 ID とも呼ばれます。1000000 より小さい Snort ID が Cisco Talos Intelligence Group（Talos） によって作成されました。

操作（Action）

選択した侵入ポリシーでのこのルールの状態。各ルールに対し、このポリシー内のルールのデフォルトアクションに「（デフォルト）」が追加されます。ルールをデフォルトの設定に戻すには、このアクションを選択します。指定できるアクションは、次のとおりです。

- [アラート（Alert）]：このルールがトラフィックと一致するとイベントを作成しますが、接続はドロップしません。
- [ドロップ（Drop）]：このルールがトラフィックと一致するとイベントを作成し、接続をドロップします。
- [無効（Disabled）]：このルールではトラフィックは一致しません。イベントは生成されません。

ステータス（Status）

Snort 2 ルールの場合、[ステータス（Status）] は個別の列になっています。ルールに対するデフォルトのアクションを変更すると、この列に「上書き済み」と表示されます。それ以外の場合は、この列は空です。

Snort 3 ルールの場合、[上書き済み（Overridden）] ステータスは [アクション（Action）] 属性の下部に表示されます（変更した場合）。

メッセージ（Messages）

これはルールの名前で、ルールによってトリガーされたイベントにも表示されます。メッセージは通常、署名が一致した脅威を識別します。それぞれの脅威の詳細についてインターネットで検索できます。

デフォルトの侵入変数セット

侵入ルールの署名には、特定の項目の変数が含まれます。変数のデフォルト値を次に示します。$HOME_NET と $EXTERNAL_NET が最もよく使用される変数です。プロトコルはポート番号とは別々に指定されるため、ポート変数は数字のみです。

- $DNS_SERVERS = $HOME_NET（任意の IP アドレスを示します）。
- $EXTERNAL_NET = 任意の IP アドレス。
- $FILE_DATA_PORTS = $HTTP_PORTS、143、110。
- $FTP_PORTS = 21、2100、3535。
- $GTP_PORTS = 3386、2123、2152。
- $HOME_NET = 任意の IP アドレス。
- $HTTP_PORTS = 次の番号の 144 個のポート：36、80 ～ 90、311、383、443、555、591、593、631、666、801、808、818、901、972、1158、1212、1220、1414、1422、1533、1741、1830、1942、2231、2301、2381、2578、2809、2980、3029、3037、3057、3128、3443、3507、3702、4000、4343、4848、5000、5117、5222、5250、5450、5600、5814、6080、6173、6767、6988、7000、7001、7005、7071、7080、7144、7145、7510、7770、7777 ～ 7779、8000、8001、8008、8014、8015、8020、8028、8040、8060、8080 ～ 8082、8085、8088、8118、8123、8161、8180 ～ 8182、8222、8243、8280、8300、8333、8344、8400、8443、8500、8509、8787、8800、8888、8899、8983、9000、9002、9060、9080、9090、9091、9111、9290、9443、9447、9710、9788、9999、10000、11371、12601、13014、15489、19980、23472、29991、33300、34412、34443、34444、40007、41080、44449、50000、50002、51423、53331、55252、55555、56712。
- $HTTP_SERVERS = $HOME_NET（任意の IP アドレスを示します）。
- $ORACLE_PORTS = 任意。
- $SHELLCODE_PORTS = 180。
- $SIP_PORTS = 5060、5061、5600。
- $SIP_SERVERS = $HOME_NET（任意の IP アドレスを示します）。
- $SMTP_SERVERS = $HOME_NET（任意の IP アドレスを示します）。
- $SNMP_SERVERS = $HOME_NET（任意の IP アドレスを示します）。

- $SQL_SERVERS = $HOME_NET（任意の IP アドレスを示します）。
- $SSH_PORTS = 22。
- $SSH_SERVERS = $HOME_NET（任意の IP アドレスを示します）。
- $TELNET_SERVERS = $HOME_NET（任意の IP アドレスを示します）。

ジェネレータ識別子

ジェネレータ識別子（GID）は、侵入ルールを評価し、イベントを生成するサブシステムを識別します。標準のテキスト侵入ルールのジェネレータ ID は 1、共有オブジェクト侵入ルールのジェネレータ ID は 3 です。また、各種プリプロセッサに対して複数のルール セットがあります。次の表で、GID について説明します。

表 *1:* ジェネレータ *ID*

ID	コンポーネント
1	標準テキスト ルール。
2	タグ付きパケット。 （タグ付きセッションからパケットを生成するタグジェネレータのルール。）
3	共有オブジェクト ルール。
102	HTTP デコーダ。
105	バック オリフィス探知機。
106	RPC デコーダ。
116	パケット デコーダ。
119、120	HTTP インスペクト プリプロセッサ （GID 120 ルールは、サーバ固有の HTTP トラフィックに関連しています）。
122	ポートスキャン ディテクタ。
123	IP 最適化。
124	SMTP デコーダ。 （SMTP 動詞に対するエクスプロイト。）
125	FTP デコーダ。
126	Telnet デコーダ。
128	SSH プリプロセッサ。

ID	コンポーネント
129	ストリーム プリプロセッサ。
131	DNS プリプロセッサ。
133	DCE/RPC プリプロセッサ。
134	ルール遅延、パケット遅延。 （これらのルールのイベントは、ルール遅延中断（SID 1）または侵入ルールのグループの再有効化（SID 2）のとき、またはパケット遅延のしきい値を超えた（SID 3）ためにシステムがパケットの検査を中止したときに生成されます）。
135	レートベースの攻撃ディテクタ。 （ネットワーク上のホストへの過剰な接続。）
137	SSL プリプロセッサ。
138、139	機密データ プリプロセッサ。
140	SIP プリプロセッサ。
141	IMAP プリプロセッサ。
142	POP プリプロセッサ。
143	GTP プリプロセッサ。
144	Modbus プリプロセッサ。
145	DNP3 プリプロセッサ。

ネットワーク分析ポリシー

ネットワーク分析ポリシーはトラフィック前処理を制御します。プリプロセッサは、トラフィックを正規化し、プロトコル異常を識別することにより、トラフィックがさらに検査されるように準備します。ネットワーク分析関連の前処理が行われるのは、セキュリティインテリジェンスによるドロップとSSL復号の後ですが、アクセス制御と侵入またはファイル検査の前です。

デフォルトでは、システムは [バランスのとれたセキュリティと接続性（Balanced Security and Connectivity）] ネットワーク分析ポリシーを使用して、アクセス制御ポリシーによって処理されるすべてのトラフィックを前処理します。ただし、アクセス制御ルールで侵入ポリシーを設定する場合、システムは、適用される最も積極的な侵入ポリシーに一致するネットワーク分析ポリシーを使用します。たとえば、アクセス制御ルールで [接続性よりセキュリティを優先（Security over Connectivity）] ポリシーと [バランスのとれたセキュリティと接続性（Balanced Security and Connectivity）] ポリシーの両方を使用する場合、システムはすべてのトラフィックに対して [接続性よりセキュリティを優先（Security over Connectivity）] NAP を使用します。

Snort 3 カスタム侵入ポリシーの場合、この割り当ては、侵入ポリシーに割り当てられた基本テンプレートポリシーに従って行われます。

侵入ポリシーのためのライセンス要件

アクセス制御ルールの侵入ポリシーを適用するには、**Threat**ライセンスを有効にする必要があります。ライセンスの設定については、オプションライセンスの有効化または無効化を参照してください。

ネットワーク分析ポリシーには追加ライセンスは必要ありません。

アクセス制御ルールでの侵入ポリシーの適用

侵入ポリシーをネットワークトラフィックに適用するには、トラフィックを許可するアクセス制御ルール内でポリシーを選択します。侵入ポリシーを直接指定しません。

保護するネットワークの相対的なリスクに基づいた可変の侵入保護を提供する別の侵入のポリシーを割り当てることができます。たとえば、内部ネットワークと外部ネットワーク間のトラフィックには、より厳しい [接続性よりもセキュリティを優先（Security over Connectivity）] ポリシーを使用する場合があります。一方で、内部ネットワーク間のトラフィックに対しては、より緩やかな [セキュリティよりも接続性を優先（Connectivity over Security）] ポリシーを適用する場合があります。

また、すべてのネットワークに対して同じポリシーを使用することで、構成を簡略化することもできます。たとえば、[バランスのとれたセキュリティと接続性（Balanced Security and Connectivity）] ポリシーは、接続に過度に影響を与えずに良好な保護を提供するための設計です。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]** を選択します。

ステップ 2 トラフィックを**許可**する、新しいルールを作成するか、既存のルールを編集します。

既定のアクションを許可する場合は、既定のアクションで侵入ポリシーを指定することもできます。

トラフィックを信頼またはブロックするルールに侵入ポリシーを適用することはできません。

ステップ 3 [侵入ポリシー（Intrusion Policy）] タブをクリックします。

ステップ 4 **[侵入ポリシー（Intrusion Policy）]** > **[オン（On）]** を選択し、トラフィックの照合に使用する侵入検査ポリシーを選択します。

Snort 2 と Snort 3 の切り替え

Snort は製品の主要インスペクションエンジンです。Snort のバージョンは自由に切り替えることができますが、Snort 2.0 の一部の侵入ルールは Snort 3.0 に存在しない場合があり、その逆の場合もあります。これらのルールのいずれか 1 つのルールアクションを変更した場合、Snort 3 に切り替えて Snort 2 に戻るか、再度 Snort 3 に戻ると、その変更は保持されません。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は保持されます。Snort 3 と Snort 2 のルール間マッピングは 1 対 1 または 1 対多にすることができるため、変更の保存はベストエフォートベースで行われることに注意してください。

Snort バージョンを変更すると、システムは自動展開を実行して変更を実装します。タスクリストに進行状況が表示されます。これらのタスクは、Snortバージョンの変更と自動展開（Snortバージョン切り替え）です。展開と、Snort の停止と再起動が必要なため、VPN を含むすべての既存の接続がドロップされ、再確立する必要があります。これにより、一時的なトラフィック損失が発生します。

（注） Snort のバージョンを切り替えようとして失敗した場合、破棄できない保留中の変更が残り、後続の切り替えを試みることができなくなります。この場合は、ToggleInspectionEngine API を使用して切り替えを完了する必要があります。これは API Explorer から使用できます。bypassPendingChangeValidation 属性を TRUE に設定する必要があります。

始める前に

現在有効になっている Snort のバージョンを確認するには、次の手順を使用するか、**[ポリシー（Policies）] > [侵入（Intrusion）]** を選択します。テーブルの上にある [Snortバージョン（Snort Version）] 行を探します。現在のバージョンは、完全なバージョン番号の最初の番号です。たとえば、2.9.17-95 は Snort 2 バージョンです。

デバイスがエアギャップネットワークにある場合は、バージョンを切り替える前に、新しいバージョン用の最新のルールパッケージを手動でアップロードすることを検討してください。

2.0 にダウングレードすると、作成したカスタム侵入ポリシーはすべて、カスタムポリシーで使用される基本ポリシーに変換されます。可能なかぎり、ルール アクション オーバーライドは保持されます。複数のカスタムポリシーが同じ基本ポリシーを使用する場合は、最も多くのアクセス制御ポリシーで使用されるカスタムポリシーのオーバーライドが保持され、その他のカスタムポリシーのオーバーライドは失われます。これらの「重複」ポリシーを使用していたアクセス制御ルールは、最もよく使用されるカスタムポリシーから作成された基本ポリシーを使用するようになります。すべてのカスタムポリシーが削除されます。カスタムポリシーを、後でインポートできるように保存しておくには、Snort 3 に切り替えた後に、Firewall Threat Defense API を使用して設定をエクスポートします。

Snort のバージョンを切り替えるには、保留中の変更を展開する必要があります。

手順

ステップ 1 [デバイス（Device）] を選択してから、[更新（Updates）] のサマリーで [設定の表示（View Configuration）] をクリックします。

[侵入ルール（Intrusion Rule）] グループを確認します。Snort の現在のバージョンが表示されます。

ステップ 2 [侵入ルール（Intrusion Rule）] グループで、[Snort 3.0へのアップグレード（Upgrade to Snort 3.0）] または [Snort 2.0へのダウングレード（Downgrade to Snort 2.0）] をクリックして、Snort のバージョンを変更できます。

ステップ 3 アクションを確認するプロンプトが表示されたら、最新の侵入ルールパッケージを取得するオプションを選択し、[はい（Yes）] をクリックします。

最新のルールパッケージを入手することをお勧めします。システムはアクティブな Snort バージョンのパッケージのみをダウンロードするため、切り替え先の Snort バージョン用の最新パッケージがインストールされている可能性は低くなります。

侵入ポリシーを編集するには、バージョンを切り替えるタスクが完了するまで待つ必要があります。

侵入イベントの Syslog の設定

侵入ポリシーの外部 syslog サーバを設定して Syslog サーバに侵入イベントを送信できます。サーバに送信される侵入イベントを取得するために侵入ポリシーで Syslog サーバを設定する必要があります。アクセス ルールで syslog サーバを設定し、侵入イベントではなく、接続イベントのみ syslog サーバに送信します。

複数の syslog サーバーを選択する場合、イベントは各サーバーに送信されます。

侵入イベントのメッセージ ID は 430001 です。

手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** の順に選択します。

ステップ 2 **[ログ設定の編集（Edit Logging Settings）]** ボタン（⚙）をクリックして syslog を設定します。

ステップ 3 [侵入イベント送信先（Send Intrusion Events To）] の下にある [+] ボタンをクリックして、syslog サーバーを定義するサーバーオブジェクトを選択します。必要なオブジェクトが存在しない場合は、[新しい Syslog サーバーの作成（Create New Syslog Server）] をクリックして作成します。

ステップ 4 [OK] をクリックします。

侵入ポリシーの管理（Snort 3）

Snort 3 を検査エンジンとして使用する場合は、独自の侵入ポリシーを作成し、それらを目的に応じてカスタマイズすることができます。システムには、同じ名前の Cisco Talos Intelligence Group（Talos）定義のポリシーに基づく事前定義されたポリシーが付属しています。これらのポリシーを編集することもできますが、基盤となる Talos ポリシーに基づいて独自のポリシーを作成し、ルールアクションを調整する必要がある場合にはそれを変更することをお勧めします。

これらの各事前定義ポリシーには同じ侵入ルール（署名とも呼ばれます）のリストが含まれていますが、各ルールに対して実行する操作は異なります。たとえば、あるポリシーでは有効化され、別のポリシーでは無効化されるルールがあります。

適用されている特定のルールであまりにも誤検出が多く、そのルールでブロックして欲しくないトラフィックがブロックされている場合、安全性の低い侵入ポリシーに切り替えることなく、ルールを無効にできます。または、トラフィックをドロップせずに、一致すると警告するように変更することもできます。

逆に、特定の攻撃に対して保護する必要があるにもかかわらず、関連するルールが選択した侵入ポリシーで無効になっている場合は、より安全なポリシーに変更せずに、ルールを有効にすることができます。

侵入に関連するダッシュボードおよびイベント ビューアを使用して（両方、[モニタリング（Monitoring）]ページ）、侵入ルールがトラフィックに与えている影響を評価します。警告や削除に設定された侵入ルールに一致したトラフィックに対してのみ、侵入イベントや侵入データが表示されることに注意してください。無効になっているルールは評価されません。

（注） Snort 2 に切り替える場合、カスタムポリシーを作成できなくなり、侵入ポリシーの使用方法も少し異なります。このトピックの代わりに、侵入ポリシーの管理（Snort 2） （26 ページ）を参照してください。

手順

ステップ 1 **[ポリシー（Policies）] > [侵入（Intrusion）]** を選択します。

テーブルの上に表示されている Snort のバージョンが 3.x であることを確認します。

ステップ 2 次のいずれかを実行します。

- [検索/フィルタ（Search/Filter）] ボックスを使用してポリシーを検索します。名前でのみ検索できます。
- 歯車アイコン（⚙）をクリックし、syslog サーバーへのロギングを有効にします。侵入イベントの Syslog の設定 （10 ページ）を参照してください。

- [+] をクリックし、新しいポリシーを作成します。カスタム侵入ポリシーの設定（Snort 3）（12 ページ）を参照してください。
- 編集アイコン（）をクリックしてポリシーのプロパティとルールを表示し、それらを編集します。侵入ポリシーのプロパティの表示または編集（Snort 3）（13 ページ）を参照してください。
- 削除アイコン（）をクリックしてポリシーを削除します。

カスタム侵入ポリシーの設定（Snort 3）

事前定義ポリシーがニーズに合わない場合は、新しい侵入ポリシーを作成してルールの動作をカスタマイズできます。一般に、事前定義ポリシーを変更するのではなく、事前定義ポリシーに基づいてカスタムポリシーを作成することをお勧めします。これにより、カスタマイズによって必要な結果が得られない場合に、Cisco Talos 定義のポリシーの一つを簡単に実装できます。

手順

ステップ 1 **[ポリシー（Policies）] > [侵入（Intrusion）]** を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいポリシーを作成するには、[+] をクリックします。
- 既存のポリシーを編集するには、そのポリシーの編集アイコン（）をクリックします。ポリシーの詳細が表示されたら、ページの上部にあるポリシープロパティのセクションの [編集（Edit）] リンクをクリックします。

ステップ 3 ポリシーの [名前（Name）] を入力し、必要に応じて、説明を入力します。

ステップ 4 ポリシーの [検査モード（Inspection Mode）] を設定します。

- [防止（Prevention）]：侵入ルールのアクションが常に適用されます。切断ルールに一致する接続はブロックされます。
- [検出（Detection）]：侵入ルールはアラートのみを生成します。切断ルールに一致する接続はアラートメッセージを生成しますが、接続はブロックされません。

ステップ 5 ポリシーの [基本テンプレート（Base Template）] を選択します。

基本テンプレートはCisco Talosによって提供されます。ポリシーの詳細を表示するには、それぞれの情報アイコンをクリックします。新しいルールパッケージがインストールされると、ポリシー名が変更される場合があり、新しいポリシーも表示されることに注意してください。

- [最大検出（Cisco Talos）（Maximum Detection (Cisco Talos)）]：このポリシーはセキュリティを最重要としています。ネットワーク接続とスループットは保証されず、誤検出が発生する可能性があります。このポリシーは、高度なセキュリティを要するエリアでのみ使用する必要があります。また、アラートを調査し、その有効性を判別できるように、セキュリティモニターを準備する必要があります。
- [接続性よりもセキュリティを優先（Cisco Talos）（Security Over Connectivity (Cisco Talos)）]：このポリシーはセキュリティに重点を置いており、ネットワーク接続とスループットが犠牲になる場合があります。トラフィックはより綿密に検査され、より多くのルールが評価されるため、理に適った範囲内での、誤検出と遅延の増加の両方が予期されます。
- [バランスのとれたセキュリティと接続性（Cisco Talos）（Balanced Security and Connectivity (Cisco Talos)）]：（デフォルト）このポリシーは、ネットワーク接続およびスループットとセキュリティニーズの間での微妙なバランスの確立を試みます。このポリシーは、[接続性よりもセキュリティを優先（Security Over Connectivity）]ほど厳格ではありませんが、通常のトラフィックの中断を減少させながら、ユーザーのセキュリティを保持しようとします。
- [セキュリティよりも接続性を優先（Cisco Talos）（Connectivity Over Security (Cisco Talos)）]：このポリシーは、ネットワーク接続とスループットに重点を置いており、セキュリティが犠牲になる場合があります。トラフィックは綿密に検査されず、評価されるルール数は少なくなります。
- [アクティブなルールなし（Cisco Talos）（No Rules Active (Cisco Talos)）]：このポリシーは、一般的なプリプロセッサ設定を指定する基本ポリシーですが、ルールや組み込みアラートは有効になっていません。適用するポリシーのみを有効にする場合は、このポリシーをベースとして使用します。

ステップ 6 [OK] をクリックします。

侵入ポリシーリストに戻ります。これで、新しいポリシーを表示し、必要に応じてルールアクションを調整することができます。

侵入ポリシーのプロパティの表示または編集（Snort 3）

[侵入ポリシー（Intrusion Policy）] ページには、事前定義されたポリシーとユーザー定義のポリシーの両方を含むポリシーのリストとその説明が表示されます。ポリシーを編集するには、まずポリシーのプロパティを表示する必要があります。

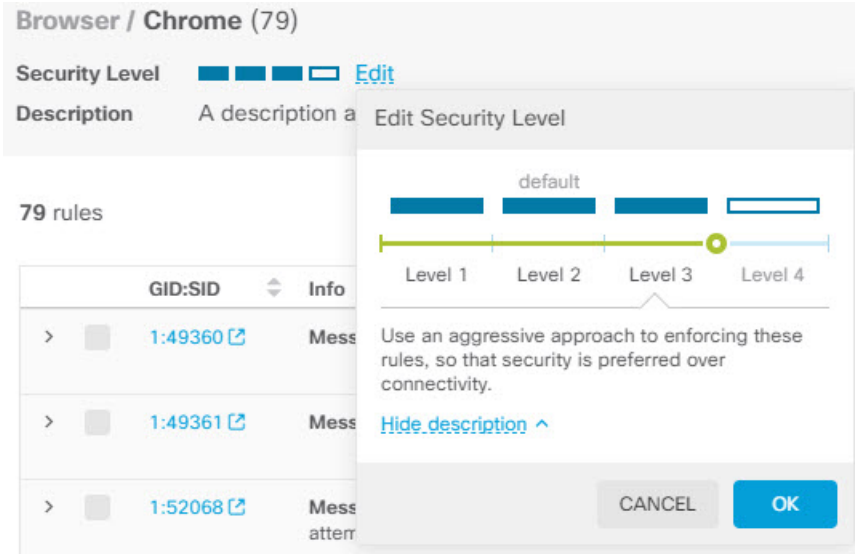
手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** を選択します。

ステップ 2 ポリシーの編集アイコン（  ）をクリックします。

ポリシーには、次のセクションが含まれています。

- [ポリシー名（Policy Name）] ドロップダウンリスト。
  - ドロップダウンリストから選択することで別のポリシーに簡単に切り替えたり、戻るボタン（）をクリックしてポリシーのリストに戻ることができます。
  - このポリシーを削除するには、ポリシー名の横にある削除アイコン（  ）をクリックします。
- [一般プロパティ（General Properties）]。このセクションには、侵入モード、基本ポリシー、および説明が示されます。これらのプロパティまたはポリシー名を変更するには、[編集（Edit）] をクリックします。
- [ルールグループ（Rule Group）] の目次。このリストには、ポリシーにアクティブなルールがあるすべてのルールグループが表示されます。グループには階層があり、親グループには、より大きな親グループ内のルールのサブセットを編成する子グループが含まれます。各グループはルールの論理的な集合であり、特定のルールが複数のグループに含まれる場合があります。
  - 現在ポリシーにアクティブなルールがないグループを追加するには、**[+]>[既存のルールグループの追加（Add Existing Rule Group）]** をクリックして、そのグループを選択します。侵入ポリシーのルールグループの追加または削除（Snort 3）（16 ページ）を参照してください。
  - グループのセキュリティレベルを変更するには、リストから子グループを選択します。ルールリストが変更され、セキュリティレベルが上部に表示され、グループ内のルールが下に一覧表示されます。セキュリティレベルの横にある [編集（Edit）] リンクをクリックし、新しいレベルを選択します。各セキュリティレベルに関する情報を取得するには、編集時に [説明の表示（View Description）] をクリックします。レベルを変更すると、アクティブなルールが（および特定のルールのアクションも）変更される可能性があることに注意してください。よりセキュアなレベルでは、アクティブなルールが多くなり、ドロップアクションを持つルールが多くなる傾向があります。[OK] をクリックして変更を確定します（セキュリティレベルはカスタムルールグループには適用されません）。



- グループ内のすべてのルールを削除するには、リストから子グループを選択します。次に、グループ名の右端にある [除外（Exclude）] リンクをクリックし、グループを除外することを確認します。グループを除外すると、グループ内のすべてのルールが無効になるだけです。グループは削除されません。

  ただし、グループに、有効になっている他のグループと共有しているルールが含まれている場合、共有ルールでは、現在もアクティブであるグループによって適用されるアクションがすべて保持されます。すべての場合において、グループメンバーシップに関係なく、個々のルールに対して最も積極的な設定が保持されます。

- カスタムルールの新しいカスタムルールグループを追加するには、**[+]>[カスタムルールのアップロード（Upload Custom Rules）]**をクリックします。詳細については、カスタム侵入ルールのアップロード （22 ページ）を参照してください。

- カスタムルールグループの名前または説明を変更するには、[編集（Edit）] をクリックします。

- カスタムルールグループを削除するには、[削除（Delete）] をクリックします。詳細については、「カスタム侵入ルールとルールグループの管理 （21 ページ）」を参照してください。

- カスタムルールグループに新しいカスタムルールを追加するには、ルールテーブルの上にある [+] をクリックします。個別のカスタム侵入ルールの設定 （25 ページ）を参照してください。

- カスタムルールのグループメンバーシップを編集、複製、削除、または管理するには、ルールの右側にカーソルを合わせ、適切なボタンまたはコマンドをクリックします。詳細については、「個別のカスタム侵入ルールの設定 （25 ページ）」を参照してください。

- [ルールのリスト（List of rules）]。検索フィールドを使用すると、全文検索でルールを検索できます。フィルタリング項目を選択して、GID または SID の任意の組み合わせで検索

したり、（追加した）ユーザー定義のルールのみ表示したり、単にアクション（無効、アラート、ドロップ）に基づいてルールを表示したりもできます。ルールは遅延ロードされるため、フィルタ処理されていないリスト全体のスクロールにはかなりの時間がかかります。リストをフィルタ処理する場合は、更新ボタンをクリックして、フィルタ処理されたビューをリロードしてください。

- ルールのアクションを変更するには、ルールの [アクション（Action）] セルをクリックし、新しいアクションを選択します。アラートのみにする場合は [アラート（Alert）]、一致するトラフィックをブロックする場合は [ブロック（Block）]、ルールを無効にする場合は [無効（Disable）] を選択してください。各ルールのデフォルトアクションが示されます。
- 一度に複数のルールのアクションを変更するには、変更するルールの左の列にあるチェックボックスをクリックし、ルールテーブルの上にある [アクション（Action）] ドロップダウンリストから新しいアクションを選択します。GID:SIDヘッダーのチェックボックスをクリックしてリスト内のすべてのルールを選択します。最大5000のルールを一度に変更できます。
- カスタムルールグループ内のルールを更新するには、[ルールファイルのアップロード（Upload Rule File）] をクリックします。詳細については、「カスタム侵入ルールのアップロード （22 ページ）」を参照してください。
- ルールに関する詳細情報を取得するには、[GID：SID] セルのリンクをクリックします。リンクをクリックすると Snort.org に移動します。
- 一覧表示されるルールを変更するには、ルールグループの目次から子グループ（親グループではなく）をクリックします。ルールグループリストの上部にある [すべてのルール（ALL RULES）] をクリックすると、すべてのルールのリストに戻ることができます。
- ソート順序を変更するには、カラムのテーブルヘッダーをクリックします。ルールのデフォルトのソートは、上書きされたルール、ドロップルール、アラートルールの順です。

侵入ポリシーのルールグループの追加または削除（Snort 3）

侵入ルールはローカルグループで編成されます。グループには階層があり、親グループには関連する子グループが含まれます。ルール自体は子グループにのみ表示されます。親グループは単に組織的な構成要素です。特定のルールが複数のグループに表示される場合があります。

作成したカスタムルールグループは、[ユーザー定義グループ（User Defined Groups）] フォルダにあります。カスタムルールグループには階層がありません。

侵入ポリシーのルールを追加または削除する最も簡単な方法は、グループを追加または削除することです。グループ内のルールは論理的に関連しているため、高い確率で、特定のグループ内のすべてではないにしてもほとんどのルールを使用することになります。

次の手順では、グループを追加し、グループのセキュリティレベルを変更する方法について説明します。

手順

ステップ 1 **[ポリシー（Policies）] > [侵入（Intrusion）]** を選択します。

ステップ 2 変更するポリシーの編集アイコン（  ）をクリックします。

ステップ 3 （グループの追加）ルールグループのリストにグループが表示されない場合は、**[+] > [既存のルールグループの追加（Add Existing Rule Group）]** をクリックして、次の手順を実行します。

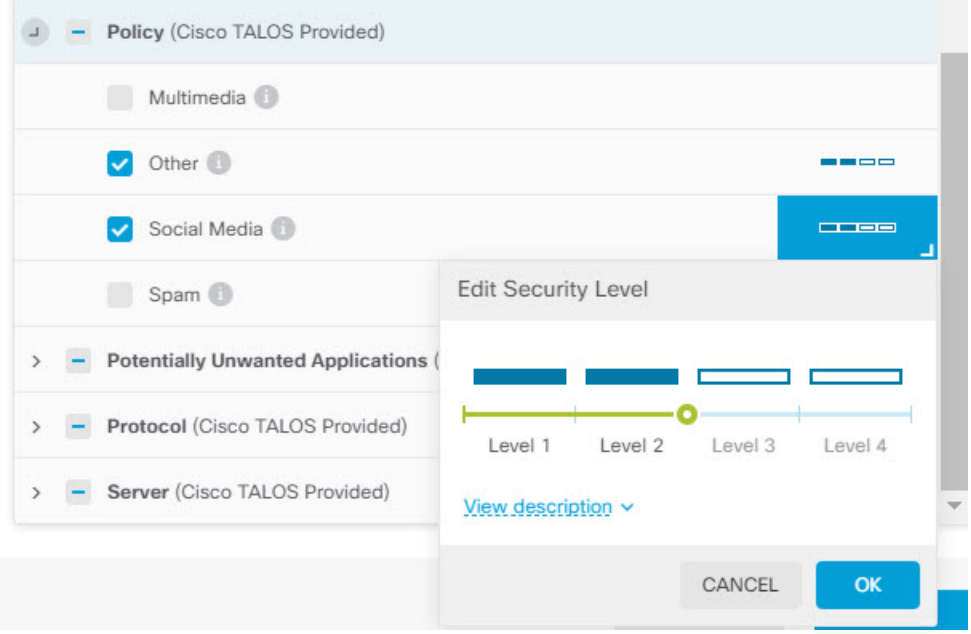
a) 子グループを検索します。

- 親グループ名の横のチェックマークは、その親グループに含まれるすべての子グループがすでに選択されていることを示します。
- 親グループ名の横のマイナス記号は、1 つ以上の子グループがこのポリシーに対して有効なルールを持っていないことを示します。これらは追加できるグループです。
- 子グループ名の横のチェックマークは、そのグループがすでに選択されていることを示します。

b) 追加するグループを選択します（チェックボックスをオンにする）。

c) （オプション、カスタムルールグループには適用されません）各グループには、カスタムポリシーに使用される基本ポリシーに応じたデフォルトのセキュリティレベルがあります。変更する場合は、セキュリティレベルのアイコンをクリックし、新しいレベルを選択して、[OK] をクリックします。

レベル 1 は最も安全性の低いセキュリティ態勢であり、セキュリティよりも接続性が重視されます。一方、レベル 4 は最も積極的なセキュリティ態勢であり、最大のセキュリティを提供します。[説明の表示（View Description）] をクリックすると、選択した各レベルの説明が表示されます。



d) すべての変更が完了するまで、グループの選択（または選択解除）を続けます。

e) [OK] をクリックします。

ステップ 4 （グループの削除）グループに含まれるすべてのルールを無効にするには、次のいずれかの方法を使用できます。

- ルールのリストの上で、グループを選択し、グループ名の右端にある [除外（Exclude）] リンクをクリックします。
- グループを追加する手法を使用しますが、代わりに、不要なグループの選択を解除し（チェックボックスをオフする）、[OK] をクリックします。
- カスタムルールグループを削除して、システムおよびそのルールを使用するすべての侵入ポリシーから完全に削除できます。グループを選択してから、[削除（Delete）] をクリックします。

侵入ルールのアクションの変更（Snort 3）

各侵入ポリシーには同じルールがあります。違いは、各ルールで取られるアクションがポリシーごとに異なる場合があることです。

ルールアクションを変更して、誤検出が多すぎるルールを無効にすることができます。またはルールが、一致するトラフィックのアラートを発するか、そのトラフィックを切断するかどうかを変更できます。また、無効になっているルールを有効にして、一致するトラフィックをアラートまたは切断することもできます。

ルールアクションを変更する最も簡単な方法は、ルールグループのセキュリティレベルを変更することです。グループのセキュリティレベルを変更すると、グループ内のルールのアクションが変更されます。選択するセキュリティ態勢により、これが一部のルールを有効（または無効）にすることを意味する場合もあれば、アクションがアラートとドロップの間で変化する場合もあります。ただし、必要に応じて、個々のルールアクションを変更できます。

（注） 特定のルールのデフォルトアクションは、グループとシビラティ（重大度）の全体的な選択に基づいて決まります。グループのシビラティ（重大度）を変更したり、グループを除外したりすると、ルールのデフォルトアクションが変化する場合があります。

始める前に

カスタムルールグループにはセキュリティレベルがありません。セキュリティレベルの手法を使用して、カスタムルールのルールアクションを変更することはできません。

手順

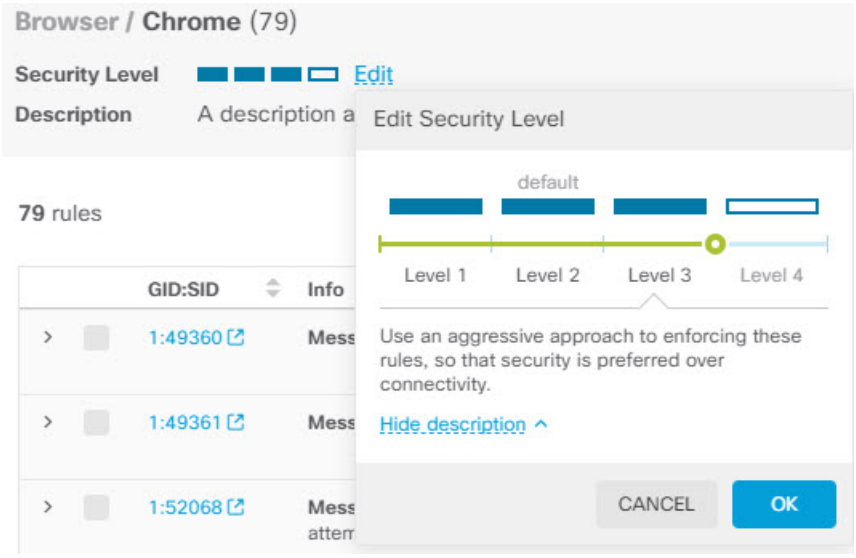
ステップ 1 **[ポリシー（Policies）] > [侵入（Intrusion）]** を選択します。

ステップ 2 ルールアクションを変更するポリシーの表示アイコン（）をクリックします。

ステップ 3 （推奨される方法）グループのセキュリティレベルを変更します。

a) ルールグループリストの子ルールグループをクリックします。

b) ルールのリストの上で、グループのセキュリティレベルの横にある [編集（Edit）] をクリックします。



（注）

グループ内のすべてのルールを無効にする場合は、[編集（Edit）] をクリックしないでください。代わりに、[除外（Exclude）] をクリックし、グループを除外することを確認します。グループは削除されず、そのルールが単に無効になります。残りの手順はスキップしてください。

c) グループの新しいレベルを選択します。[説明の表示（View Description）] をクリックして、選択した各レベルの説明を表示します。

レベル 1 は最も安全性の低いセキュリティ態勢であり、セキュリティよりも接続性が重視されます。一方、レベル 4 は最も積極的なセキュリティ態勢であり、最大のセキュリティを提供します。

d) [OK] をクリックします。

ステップ 4 （手動の方法）1 つ以上のルールのアクションを変更します。

a) 変更するアクションのルールを検索します。

ルール情報内の文字列を検索するには、[検索/フィルター（Search/Filter）] ボックスを使用します。フィルタ処理項目を選択して、GID または SID の任意の組み合わせで検索したり、単にそれらのアクション（無効、アラート、ドロップ）に基づいてルールを表示したりすることもできます。ルールは遅延ロードされるため、フィルタ処理されていないリスト全体のスクロールにはかなりの時間がかかります。リストをフィルタ処理する場合は、更新ボタンをクリックして、フィルタ処理されたビューをリロードしてください。

理想的には、連携して問題に取り組んでいる場合にイベントやシスコ テクニカル サポートから Snort 識別子（SID）とジェネレータ識別子（GID）を取得できます。これにより、ルールを正確に検索できます。

b) アクションを変更するには、次のいずれかを実行します。

- ルールを 1 つずつ変更：ルールの [アクション（Action）] 列をクリックし、必要なアクションを選択します。
  - [アラート（Alert）]：このルールがトラフィックと一致するとイベントを作成しますが、接続はドロップしません。
  - [ドロップ（Drop）]：このルールがトラフィックと一致するとイベントを作成し、接続をドロップします。
  - [無効（Disabled）]：このルールではトラフィックは一致しません。イベントは生成されません。
- 一度に複数のルールを変更：変更するルールのチェックボックスをクリックし、表の上にある [一括（Bulk）] ドロップダウンをクリックして、目的のアクションを選択します。GID:SID ヘッダーのチェックボックスをクリックしてリスト内のすべてのルールを選択します。最大 5000 のルールを一度に変更できます。

カスタム侵入ルールとルールグループの管理

システムには、Cisco Talos Intelligence Group（Talos）によって定義された何千もの侵入ルールが付属しています。追加の攻撃を把握している場合は、カスタム侵入ルールを作成してアップロードし、それらの攻撃をスクリーニングして、アラートを発出したり、攻撃をドロップしたりすることができます。ルールを 1 つずつ作成、編集、削除することもできます。

アップロードするルールの場合、テキストエディタを使用してルールをオフラインで作成します。アップロードする各テキストファイルにカスタムルールのグループを含めることをお勧めします。これにより、ルールへの変更を簡単にアップロードし、新しいルールをカスタムルールグループにマージしたり、ルールを新しい編集済みコピーに置き換えたりできます。

こうしたルールの作成方法の説明は、このドキュメントの対象範囲に含まれていません。Snort 2 ルールを Snort 3 形式に変換する方法など、Snort 用の侵入ルールの作成方法に関する詳細については、https://snort.org/documents のガイドを参照してください。たとえば、https://snort.org/documents/rules-writers-guide-to-snort-3-rules で『*Snort 3*ルールを作成するルール作成者のための手引き』を参照してください。

始める前に

カスタムルールグループは、カスタム侵入ルールのアップロード （22 ページ）で説明されているようにカスタムルールをアップロードするプロセスで作成するか、個々のルールを作成するか、またはルールメンバーシップを管理するときに作成します。グループを作成した後は、グループとその内容を管理できます。

カスタムグループは、グループを作成したときに編集していたポリシーだけでなく、すべての侵入ポリシーで使用できることに注意してください。そのため、グループに加えた変更はすべてのポリシーに対しても加えられます。たとえば、カスタムルールグループを削除すると、そのグループはすべてのポリシーから削除され、どのポリシーでも使用できなくなります。

手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** を選択します。

ステップ 2 ポリシーの編集アイコン（）をクリックします。

いずれかの組み込みポリシーではなくカスタム侵入ポリシーに、カスタムルールを追加することをお勧めします。

ステップ 3 次のいずれかを実行します。

- グループを作成するには、**[+]** > **[カスタムルールのアップロード（Upload Custom Rules）]** をクリックします。カスタム侵入ルールのアップロード （22 ページ）を参照してください。
- グループの名前または説明を編集するには、[ユーザー定義グループ（User Defined Groups）] フォルダのグループ目次でグループを選択します。[編集（Edit）] をクリックして変更を加えることができます。

- ポリシーからグループとそのルールを除外するには、[ユーザー定義グループ（User Defined Groups）] フォルダのグループ目次でグループを選択します。選択後、[除外（Exclude）] をクリックしてグループを削除できます。
- システムからグループを削除するとともに、そのグループを使用するすべてのポリシーを削除するには、[ユーザー定義グループ（User Defined Groups）] フォルダのグループ目次でグループを選択します。さらに [Delete] をクリックします。あるルールが削除されたグループのみに存在する場合、そのルールはシステムからも削除されることに注意してください。他方、削除していない他のカスタムルールグループにも同じルールが存在する場合、そのルールはそれらのグループに残されます。
- グループ内のルールを一括で置換または更新するには、[ユーザー定義グループ（User Defined Groups）] フォルダのグループ目次でグループを選択します。次に、グループのルールテーブルの上にある [アクション（Action）] ドロップダウンリスト横の [ルールファイルのアップロード（Upload Rule File）] をクリックします。このプロセスは、カスタム侵入ルールのアップロード （22 ページ）で説明されたものと同じです。
- 個々のルール、およびルールグループへの割り当てを作成および管理するには、個別のカスタム侵入ルールの設定 （25 ページ）を参照してください。

カスタム侵入ルールのアップロード

現在他のルールでカバーされていない攻撃を把握している場合は、カスタム侵入ルールを作成してアップロードし、それらの攻撃をスクリーニングして、アラートを発出したり、攻撃をドロップしたりすることができます。インポートされたルールのアクションはアラートまたはドロップのいずれかである必要があります。ルールのデフォルトアクションはインポートされたファイルのアクションによって定義されます。インポートしたら、ルールアクションを変更し、必要に応じてルールを無効にすることができます。

これらのルールはオフラインで作成する必要があります。Firewall Device Manager では、ルールファイルをアップロードするだけで、ルールを直接設定するわけではありません。ルールファイルはテキストファイルである必要があります。改行を使用してルールを読みやすい形式にしたり、1 行にルールを入力したりできます。空の行は許可されます。ルールの形式については、snort.org を参照してください。

たとえば、3 つのルールのアップロードファイルは次のようになります。

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (
   msg: "My Custom Rule: EXPLOIT-KIT Styx exploit kit landing page request";
   flow:to_server,established;
   http_raw_uri;
   bufferlen:>100;
   http_uri;
   content:"/i.html?",depth 8; pcre:"/\/i\.html\?[a-z0-9]+\=[a-zA-Z0-9]{25}/";
   flowbits:set,styx_landing;
   metadata: copied from talos sid 29452;
   service:http;
   classtype:trojan-activity;
   gid:1;
```

```
   sid:1000000;
   rev:1;
)

alert tcp $HOME_NET 8811 -> $EXTERNAL_NET any (
   msg:"My Custom rule: MALWARE-BACKDOOR fear1.5/aciddrop1.0 runtime detection - initial
 connection";
   flow:to_client,established;
   flowbits:isset,Fear15_conn.2;
   content:"Drive",nocase;
   metadata:copied from talos sid 7710;
   classtype:trojan-activity;
   gid:1;
   sid:1000001;
   rev:1;
)

alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (
   msg:"My Custom Rule: INDICATOR-COMPROMISE download of a Office document with embedded
 PowerShell";
   flow:to_client,established;
   flowbits:isset,file.doc;
   file_data;
   content:"powershell.exe",fast_pattern,nocase;
   metadata:copied from talos sid 37244;
   classtype:trojan-activity;
   gid:1;
   sid:1000002;
   rev:1;
)
```

手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** を選択します。

ステップ 2 ポリシーの編集アイコン（）をクリックします。

いずれかの組み込みポリシーではなくカスタム侵入ポリシーに、カスタムルールを追加することをお勧めします。

ステップ 3 次のいずれかを実行します。

- グループのリストの上にある **[+]** > **[カスタムルールのアップロード]** をクリックします。
- 作成済みのカスタムルールグループにルールをアップロードする場合は、カスタムルールグループを選択して、グループのルールテーブルの上にある [アクション（Action）] ドロップダウンリストの横にある [ルールファイルのアップロード（Upload Rule File）] をクリックします。

ステップ 4 [参照（Browse）] をクリックしてカスタムルールファイルを選択するか、ファイルを [ファイルのアップロード（Upload File）] ダイアログボックスにドラッグアンドドロップします。

アップロードが完了するまで待ちます。

ステップ 5 競合の処理方法を選択します。

競合は、追加するルールがシステムにすでに存在するルールと同じ場合に発生します。これは、以前にアップロードしたのと同じルールまたは編集したバージョンのルールをアップロードする場合にのみ発生します。

次のオプションのいずれか 1 つを選択します。

（注）
[マージ（Merge）] と [置換（Replace）] は基本的に同じものです。既存のルールに変更を加えるには、アップロードしたルールのリビジョン番号が、アップロード済みのルールのリビジョン番号よりも大きい必要があります。唯一の違いは、[置換（Replace）] オプションを使用すると、アップロードファイルに対象のカスタムルールグループ内のルールがない場合、それらのルールがルールグループから削除されることです。[マージ（Merge）] オプションでは、これらの "欠落している" ルールがそのまま残ります。

- [マージ（Merge）]：アップロードされたファイルのルールのリビジョン番号が大きい場合、アップロードされたファイル内の変更されたルールのうち、選択したグループにも存在するものは、それらの変更がマージされます。変更されていないルール、またはアップロードに対応するルールがないグループ内のルールは変更されません。アップロード内の新しいルールが追加されます。これがデフォルトのオプションです。
- [置換（Replace）]：アップロードされたファイルのルールは、アップロードされたルールのリビジョン番号が大きい場合、選択したグループのルールを置き換えます。アップロードされたファイルに存在しない既存のルールは、グループから削除されます。アップロードされたバージョンのリビジョン番号が同じかそれ以下の既存のルールは変更されません。アップロード内の新しいルールが追加されます。

ステップ 6 [+] をクリックし、アップロードしたルールのカスタムルールグループを選択します。

使用するカスタムルールグループが存在しない場合は、[新しいグループの作成（Create New Group）] をクリックしてすぐに作成します。新しいグループには名前と、必要に応じて説明が必要です。その後、新しいグループを選択できます。

ルールを置き換える場合は、1 つのグループのみを選択できます。ルールをマージする場合は、複数のグループを選択できます。

ステップ 7 [OK] をクリックします。

ファイルがアップロードされ、新しいグループに配置されます。アップロードされたルールの数と、更新、削除、または無視されたルールの数の概要が表示されます。

ファイルにエラーがある場合、アップロードは失敗します。[ダウンロードエラーファイル（Download Error File）] リンクをクリックすると、エラーの詳細情報を取得できます。

グループは、この侵入ポリシーで自動的にアクティブ化されます。グループと新しいルールは他のポリシーに追加できますが、グループとルールが他のポリシーで自動的に有効になることはありません。他のポリシーへのグループの追加については、侵入ポリシーのルールグループの追加または削除（Snort 3）（16 ページ）を参照してください。

個別のカスタム侵入ルールの設定

カスタム侵入ルールは、ファイルアップロードによって一括で行うのではなく、一度に1つずつ設定できます。この方法は、あるルールをすばやく調整する必要がある場合や、一度に少数のルールを作成または変更する必要がある場合に適しています。

侵入ルールを設定する場合は、次の点に注意してください。

- すべてのカスタムルールの GID は 1 である必要があります。
- ルールの SID は、システム内のすべてのルールで一意である必要があります。また、100万（1000000）以上である必要があります。
- ルールを編集する場合は、ルールのバージョンを変更する必要があります。通常、バージョン番号は 1 ずつ増加します。
- Cisco Talos Intelligence Group（Talos）ルールを複製して独自のバージョンのルールを作成できますが、重複する SID を変更して一意にする必要があります。

ルールが適切に形成されていることを確認するためにいくつかの有効性チェックが実行され、問題に関するエラーメッセージが表示されます。ただし、システムはルールが適切かどうかを判断できません。

Snort 2 ルールを Snort 3 形式に変換する方法など、Snort 用の侵入ルールの作成方法に関する詳細については、https://snort.org/documents のガイドを参照してください。たとえば、https://snort.org/documents/rules-writers-guide-to-snort-3-rules で『*Snort 3*ルールを作成するルール作成者のための手引き』を参照してください。

手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** を選択します。

ステップ 2 ポリシーの編集アイコン（）をクリックします。

いずれかの組み込みポリシーではなくカスタム侵入ポリシーに、カスタムルールを追加することをお勧めします。

ステップ 3 次のいずれかを実行します。

- 侵入ルールを追加するには、ルールテーブルの上にある [新しい侵入ルールの追加（Add New Intrusion Rule）] ボタン（+）をクリックします。ルールを追加する場合、新しいルールを含める 1 つ以上のカスタムルールグループを選択する必要があります。必要に応じて、ルールを追加しながら新しいグループを作成できます。
- 既存のルールを複製および編集してルールを追加するには、ルールの右端にマウスを合わせ、[複製（Duplicate）]（）ボタンをクリックします。ボタンは、マウスオーバーでのみ表示されます。カスタムルールの場合、[複製（Duplicate）] コマンドはその他のオプション（...）ボタンの下にあります。

- カスタムルールを編集するには、カスタムルールグループでルールを検索し、ルールの編集（）ボタンをクリックします。編集内容は、ルールが存在するすべてのグループに適用されます。変更を行う場合は、ルールのバージョン番号を少なくとも1つ増やしてください。
- カスタムルールを削除するには、ルールの削除（）ボタンをクリックします。ルールが含まれるすべてのルールグループから、そのルールが削除されます。あるグループから1つのルールだけを削除する場合は、ルールを削除する代わりに [グループ割り当ての管理（Manage Group Assignments）] オプションを使用します。
- ルールを含むグループを変更するには、その他のオプション（...）ボタンをクリックし、[グループ割り当ての管理（Manage Group Assignments）] を選択します。その後、グループを追加または削除できます。変更はグループメンバーシップに影響するだけで、ルールの変更や削除は行いません。

ステップ 4 新しいルールとグループの場合は、ルールをポリシーに追加します。

新しいルールの作成時または既存のルールの編集時に新しいグループを作成すると、そのグループはポリシーに自動的に追加されず、ルールも自動的に有効になりません。編集するポリシーにグループを追加するように求められます。ルールの追加または編集中にグループを追加しない場合は、次のプロセスを使用して後でグループを追加できます。

a) グループの目次の上にある **[+]** > **[既存のルールグループを追加（Add Existing Rule Group）]** をクリックします。
b) [ユーザー定義グループ（User Defined Groups）] フォルダでグループを見つけて選択し、[OK] をクリックします。
c) 目次でグループを選択し、新しいルールがグループ内にあり、目的のアクションがあることを確認します。

侵入ポリシーの管理（Snort 2）

あらかじめ定義された侵入ポリシーのいずれかを適用できます。これらの各ポリシーには同じ侵入ルール（署名とも呼ばれます）の一覧が含まれていますが、各ルールに対して実行する操作は異なります。たとえば、あるルールは1つのポリシーでアクティブになる可能性がありますが、別のポリシーでは無効化されます。

適用されている特定のルールであまりにも誤検出が多く、そのルールでブロックして欲しくないトラフィックがブロックされている場合、安全性の低い侵入ポリシーに切り替えることなく、ルールを無効にできます。または、トラフィックをドロップせずに、一致すると警告するように変更することもできます。

逆に、特定の攻撃に対して保護する必要があるにもかかわらず、関連するルールが選択した侵入ポリシーで無効になっている場合は、より安全なポリシーに変更せずに、ルールを有効にすることができます。

侵入に関連するダッシュボードおよびイベント ビューアを使用して（両方、[モニタリング（Monitoring）]ページ）、侵入ルールがトラフィックに与えている影響を評価します。警告や削除に設定された侵入ルールに一致したトラフィックに対してのみ、侵入イベントや侵入データが表示されることに注意してください。無効になっているルールは評価されません。

ここでは、侵入ポリシーおよびルールの調整について詳しく説明します。

侵入ポリシーのインスペクションモードの設定（Snort 2）

デフォルトでは、侵入防御システム（IPS）を実装するため、すべての侵入ポリシーが防御モードで動作します。防御インスペクションモードでは、トラフィックを切断するアクションの侵入ルールと接続が一致する場合、接続は能動的にブロックされます。

一方、ネットワーク上で侵入ポリシーの影響をテストするには、侵入検知システム（IDS）を実装する「検出」にモードを変更します。このインスペクションモードでは、切断ルールはアラートルールと同様に扱われます。この場合、一致する接続が通知されますが、アクションの結果は「ブロック相当」となり、実際に接続がブロックされることはありません。

侵入ポリシーごとにインスペクションモードを変更するため、防御と検出を混在させることができます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** の順に選択します。

ステップ 2 インスペクションモードを変更する侵入ポリシーのタブをクリックします。

[インスペクションモード（Inspection Mode）] は、ルールテーブルの上に表示されます。

ステップ 3 インスペクションモードの横にある [編集（Edit）] リンクをクリックし、ポリシーのモードを変更して、[OK] をクリックします。

次のオプションがあります。

- [防止（Prevention）]：侵入ルールのアクションが常に適用されます。切断ルールに一致する接続はブロックされます。
- [検出（Detection）]：侵入ルールはアラートのみを生成します。切断ルールに一致する接続はアラートメッセージを生成しますが、接続はブロックされません。

侵入ルールのアクションの変更（Snort 2）

事前定義された各侵入ポリシーには同じルールがあります。違いは、各ルールで取られるアクションがポリシーごとに異なる場合があることです。

ルールアクションを変更して、誤検出が多すぎるルールを無効にすることができます。またはルールが、一致するトラフィックのアラートを発するか、そのトラフィックを切断するかどうかを変更できます。また、無効になっているルールを有効にして、一致するトラフィックをアラートまたは切断することもできます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** の順に選択します。

ステップ 2 変更するルールアクションの侵入ポリシーのタブをクリックします。

事前定義されているポリシーは次のとおりです。

- セキュリティよりも接続性を優先
- バランスのとれたセキュリティと接続性
- 接続性よりもセキュリティを優先
- 最大検出

ステップ 3 変更するアクションのルールを検索します。

ルールは上書き済みが一番上に並べ替えられ、また上書きされたルールのグループ内でアクション順に並べ替えられます。それ以外の場合、ルールは、GID、次に SID で並べ替えられます。

変更するルールを検索するには検索ボックスを使用します。理想的には、連携して問題に取り組んでいる場合にイベントやシスコ テクニカル サポートから Snort 識別子（SID）とジェネレータ識別子（GID）を取得できます。

各ルールの要素の詳細については、侵入ルール属性 （3 ページ）を参照してください。

このリストを検索するには、次の手順を実行します。

a) [検索（Search）] ボックス内でクリックして、[検索属性（search attributes）] ダイアログボックスを開きます。

b) ジェネレータ ID（[GID]）、Snort ID（[SID]）、またはルール [アクション（Action）] の組み合わせを入力し、[検索（Search）] をクリックします。

たとえば [アクション=ドロップ（Action = Drop）] を選択して、一致する接続をドロップするポリシーのすべてのルールを表示できます。検索ボックスの横にあるテキストは、条件に一致するルールの数が表示されます（たとえば「9416 中 8937 ルールが見つかりました」）。

検索条件をクリアするには、検索ボックスの条件の [x] をクリックします。

ステップ 4 ルールの [アクション（Action）] の列をクリックして、必要なアクションを選択します。

- [アラート（Alert）]：このルールがトラフィックと一致するとイベントを作成しますが、接続はドロップしません。

- [ドロップ（Drop）]：このルールがトラフィックと一致するとイベントを作成し、接続をドロップします。
- [無効（Disabled）]：このルールではトラフィックは一致しません。イベントは生成されません。

ルールのデフォルトのアクションは、アクションに加えて「（デフォルト）」と表示されます。デフォルトを変更すると、状態の列にそのルールに対して「上書き済み」と表示されます。

侵入ポリシーのモニタリング

侵入ポリシー統計情報は、[モニタリング（Monitoring）] ページの [攻撃者（Attackers）] および [ターゲット（Targets）] ダッシュボードで確認できます。これらのダッシュボードで情報を表示するには、少なくとも 1 つのアクセス コントロール ルールに侵入ポリシーを適用する必要があります。「トラフィックのモニタリングおよびシステム ダッシュボード」を参照してください。

侵入イベントを表示するには、**[モニタリング（Monitoring）]** > **[イベント（Events）]** を選択して、[侵入（Intrusion）] タブをクリックします。イベントの上にマウスを置き、[詳細の表示（View Details）] リンクをクリックして、詳細情報を表示できます。詳細ページから、[IPSルールの表示（View IPS Rule）] をクリックして、関連する侵入ポリシーのルールへ移動し、そこでルール アクションを変更できます。ルールによりブロックされる適切な接続が多すぎる場合に、アクションをドロップから警告に変更することにより、誤検出の影響を軽減できます。逆に、ルールに対する攻撃トラフィックが多い場合は、アラートルールをドロップルールに変更できます。

侵入ポリシーの syslog サーバーを設定した場合、侵入イベントのメッセージ ID は 430001 です。

侵入ポリシーの例

使用例の章には、次の侵入ポリシーの実装例が含まれています。

- 脅威をブロックする方法
- ネットワーク上のトラフィックをパッシブにモニタする方法

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。

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。