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は、共同で広範かつ深いパケット検査を提供します。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。システムによって提供されるポリシーは 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った時点で、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。

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。

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。

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

[ポリシー（Policies）] > **[侵入（Intrusion）]** を選択するときに、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を参照してください。上記の表で、侵入ポリシーの名前をクリックすると、各ポリシーのルールを表示できます。

各ポリシーのルールのリストには、アラートまたはドロップに設定されているルールと、明示的に無効にしたルールだけが示されます。デフォルトで無効になっているルールは表示されません。30,000以上のルールがありますが、すべての可能なルールのサブセットのみが表示されます。しかし、最小の有効なルールセットですら、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、スクロールしていくと明らかになります。

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、『Firepower 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 （4 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 Firepower Device Manager ユーザ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 （5 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 は Cisco Talos Intelligence Group（Talos） によって作成されたものです。

アクション

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**：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**：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

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。

メッセージ

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。

- $AIM_SERVERS = ネットワークまたはホストのアドレス 20 個：64.12.24.0/23、64.12.28.0/23、64.12.31.136、64.12.46.140、64.12.161.0/24、64.12.163.0/24、64.12.186.85、64.12.200.0/24、205.188.1.132、205.188.3.0/24、205.188.5.0/24、205.188.7.0/24、205.188.9.0/24、205.188.11.228、205.188.11.253、205.188.11.254、205.188.153.0/24、205.188.179.0/24、205.188.210.203、205.188.248.0/24。

- $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
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。）

ID	コンポーネント
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は、セキュリティインテリジェンスのブラックリストの登録と SSL 復号後、アクセス制御と侵入やファイル検査の前に発生します。

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、システムはアクセス制御ルールで選択した侵入ポリシーに基づいて、異なるネットワーク分析ポリシーを適用します。

システムは、最適な処理が行われるように、侵入やネットワーク分析ポリシーに一致するように試みます。ただし、ネットワーク分析ポリシー（NAP）ルールはアクセス制御ルールで使用されるのと同じトラフィック一致基準を持っていないので、推奨されるガイドラインに従わないと、一致しないポリシーが取得される可能性があります。

システムによる NAP ルールを使用したネットワーク分析ポリシーの選択方法

ネットワーク分析ポリシーを直接割り当てることはできません。代わりに、システムは、アクセス制御ルールで割り当てた侵入ポリシーに基づいて NAP ルールを自動的に生成します。

NAP ルールは、セキュリティゾーンとネットワーク仕様にのみ基づいています。したがって、侵入ポリシーを含むアクセス制御ルールごとに、同じ送信元/送信先のセキュリティ ゾーンとネットワークに、同じ名前のネットワーク分析ポリシーを適用する NAP ルールが作成されます。ポート、URL、ユーザ、およびアプリケーションの基準は無視されます。

これは重要な違いです。ポート、アプリケーション、URL などのレイヤ 4 または 7 基準に基づいて異なる侵入ポリシーを適用できますが、それより高い層の基準はネットワーク分析ポリシーの選択に影響を与えません。

システムは、アクセス制御ルールと同じ順序でNAPルールを順序付けします。システムでは、最初に一致した NAP ルールを使用して、適用するネットワーク分析ポリシーを決定します。

したがって、同じ送信元/送信先ゾーンとネットワーク オブジェクトの組み合わせのトラフィックを許可する制御ルールが複数あるが、別のトラフィック一致基準では異なる場合、システムは重複する複数のNAPルールを生成し、2番目とその後の重複するルールは、トラフィックに一致しなくなります。これらの「重複する」ルールに別の侵入ポリシーを適用する場合、少なくともトラフィックの一部は、侵入およびネットワーク分析ポリシーに一致しなくなります。

たとえば、次のルールについて考えてみます。

1. アクセス ルール 1

   アクション：許可
   [送信元ゾーン（Source zone）]：inside_zone
   [送信元ネットワーク（Source network）]：any
   [送信先ゾーン（Destination zone）]：outside_zone
   [送信先ネットワーク（Destination Network）]：any
   [URLカテゴリ（URL category）]：ソーシャル ネットワーク
   [侵入ポリシー（Intrusion policy）]：接続性よりもセキュリティを優先

2. アクセス ルール 2

   アクション：許可
   [送信元ゾーン（Source zone）]：inside_zone
   [送信元ネットワーク（Source network）]：any
   [送信先ゾーン（Destination zone）]：outside_zone
   [送信先ネットワーク（Destination Network）]：any
   [侵入ポリシー（Intrusion policy）]：バランスのとれたセキュリティと接続性

この場合、2 つの NAP ルールがあります。

1. NAP ルール 1

   [送信元ゾーン（Source zone）]：inside_zone
   [送信元ネットワーク（Source network）]：any
   [送信先ゾーン（Destination zone）]：outside_zone
   [送信先ネットワーク（Destination Network）]：any
   [ネットワーク分析ポリシー（Network analysis policy）]：接続性よりもセキュリティを優先

2. NAP ルール 2

   [送信元ゾーン（Source zone）]：inside_zone
   [送信元ネットワーク（Source network）]：any
   [送信先ゾーン（Destination zone）]：outside_zone
   [送信先ネットワーク（Destination Network）]：any
   [ネットワーク分析ポリシー（Network analysis policy）]：バランスのとれたセキュリティと接続性

両方のNAPルールには同じ一致基準があるために、システムは[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を、アクセス制御ルール 1 または 2 のいずれかに一致するトラフィックに適用します。ただし、アクセス制御ルール 2 に一致するほとんどのトラフィックは、バランスのとれた侵入ポリシーを使用します。したがって、アクセス制御ルール2に一致するトラフィックは、NAPおよび侵入ポリシーに一致しません。

（注） アクセス制御ポリシーで 1 つの侵入ポリシーを使用する場合、システムはデフォルトのポリシーと同じ名前のネットワーク分析ポリシーを設定するだけで、NAPルールは生成しません。それ以外の場合は、デフォルトのネットワーク分析ポリシーとしてバランスのとれたポリシーを設定します。他のNAPルールが適用されない場合はデフォルトのポリシーが適用されます。これは侵入ポリシーを割り当てていないゾーンとネットワークの組み合わせでは一般的です。

NAP の処理を最適化する侵入のポリシーを適用するためのベスト プラクティス

適したネットワーク分析ポリシーを得るために侵入ポリシーの割り当て方法を決定する際は、次の推奨事項を考慮してください。

- 同じ侵入ポリシーを常に使用する場合、同じ名前のネットワーク分析ポリシーをデフォルトとして設定し、常に適した侵入ポリシーおよびネットワーク分析ポリシーを取得します。
- 特定のトラフィックに対して異なる侵入ポリシーを使用する必要がある場合は、送信元/送信先のセキュリティ ゾーンとネットワーク オブジェクトの同じ組み合わせに対し常に同じ侵入ポリシーを使用します。これにより NAP ルールは、すべての関連付けられているアクセス制御ルールに対し同じ名前のネットワーク分析ポリシーを割り当てることが保証されます。

  たとえば、network_one の inside_zone から outside_zone への一部のトラフィックに対し、[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必要があると決定した場合、同じ送信元/送信先ゾーンとネットワーク仕様を持つアクセス制御ルールごとに 、[接続性よりもセキュリティを優先（Security over Connectivity）] ポリシーを割り当てます。

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、[脅威（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と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。

侵入ポリシーの管理

Firepower Device Manager では、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。

ただし、ルールが侵入ポリシーでデフォルトで無効な場合は、一致したトラフィックをドロップまたは警告するように変更することはできません。有効なポリシーまたは以前無効にしたポリシーでのみ、アクションを変更できます。

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。

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。

異なるネットワークに対して異なるポリシーを使用する場合は、同じ送信元/送信先のセキュリティ ゾーンを使用するすべてのルールに同じポリシーを適用し、ネットワーク オブジェクトが条件に一致する場合に最良の結果を得ることになります。詳細については、NAP の処理を最適化する侵入のポリシーを適用するためのベスト プラクティス （9 ページ）を参照してください。

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。

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。

侵入ルールのアクションの変更

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。

指定されたポリシーの中で、ルールの既定のアクションは、それが有効な場合のみ、つまりアラートまたはドロップに設定されていれば変更できます。既定のアクションを変更すると、誤検出が多すぎるルールを無効できます。またはルールが一致するトラフィックをアラートまたはドロップするかどうかを変更できます。

（注） 既定のアクションを変更すると、次回侵入ルールデータベースが更新された際に、システムがルールをデフォルトから選択したアクションにリセットします。その時点で、選択が新しいデフォルトとなり、ステータスにはアクションが上書き済みとして表示されなくなります。

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。

各ポリシーのルールのリストには、アラートまたはドロップに設定されているルールと、明示的に無効にしたルールのみが示されます。デフォルトで無効になっているルールは表示されません。

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。

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 [接続イベント送信先（Send Connection Events To）] フィールドをクリックして、syslog サーバを定義するサーバ オブジェクトを選択します。必要なオブジェクトがすでに存在しない場合、[Syslogサーバの新規作成（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）] への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