



ネットワーク分析ポリシーと侵入ポリシーの概要

以下のトピックでは、Snort 検査エンジンの概要、およびネットワーク分析ポリシーと侵入ポリシーを示します。

- [ネットワーク分析ポリシーと侵入ポリシーの基本 \(1 ページ\)](#)
- [ポリシーがトラフィックで侵入を検査する方法 \(3 ページ\)](#)
- [システム提供およびカスタムネットワーク分析ポリシーと侵入ポリシー \(8 ページ\)](#)
- [ネットワーク分析ポリシーと侵入ポリシーのライセンス要件 \(16 ページ\)](#)
- [ネットワーク分析と侵入ポリシーの要件と前提条件 \(17 ページ\)](#)
- [ナビゲーション ウィンドウ: ネットワーク分析と侵入ポリシー \(17 ページ\)](#)
- [競合と変更: ネットワーク分析ポリシーと侵入ポリシー \(18 ページ\)](#)

ネットワーク分析ポリシーと侵入ポリシーの基本

ネットワーク分析ポリシーと侵入ポリシーは、システムの侵入検知および防御機能の一部として連携して動作します。

- 侵入検知という用語は、一般に、ネットワーク トラフィックへの侵入の可能性を受動的にモニタおよび分析し、セキュリティ分析用に攻撃データを保存するプロセスを指します。これは「IDS」とも呼ばれます。
- 侵入防御という用語には、侵入検知の概念が含まれますが、さらにネットワークを通過中の悪意のあるトラフィックをブロックしたり変更したりする機能も追加されます。これは「IPS」とも呼ばれます。



- (注)
- Snort 3 および SSL 復号または TLS サーバーアイデンティティを使用している場合は、**防止**モードでネットワーク分析ポリシー (NAP) を構成する必要があります。Snort 3 NAP が検知モードの場合、SSL 機能は動作しません。
 - 侵入ポリシー (IPS) とネットワーク分析ポリシー (NAP) を同じ設定にすることを強くお勧めします。IPS が検出モードの場合、NAP を検出モードに設定します。逆の場合も同様です。

侵入防御の展開では、システムがパケットを検査するときに次のことが行われます。

- **ネットワーク分析ポリシー**は、トラフィックのデコードと前処理の方法を管理し、特に、侵入を試みている兆候がある異常なトラフィックについて、さらに評価できるようにします。
- **侵入ポリシー**では侵入およびプリプロセッサルール (総称的に「侵入ルール」とも呼ばれる) を使用し、パターンに基づき、デコードされたパケットを検査して攻撃の可能性を調べます。侵入ポリシーは変数セットとペアになり、それによって名前付き値を使用してネットワーク環境を正確に反映することができます。

ネットワーク分析ポリシーと侵入ポリシーは、どちらも親のアクセス コントロール ポリシーによって呼び出されますが、呼び出されるタイミングが異なります。システムでトラフィックが分析される際には、侵入防御 (追加の前処理と侵入ルール) フェーズよりも前に、別途ネットワーク分析 (デコードと前処理) フェーズが実行されます。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。

システムには、同様の名前 (Balanced Security and Connectivity など) が付いたいくつかのネットワーク分析ポリシーおよび侵入ポリシーが付属しており、それらは互いに補完しあい、連携して動作します。システム付属の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、プリプロセッサおよび他の詳細設定の初期設定も提供します。

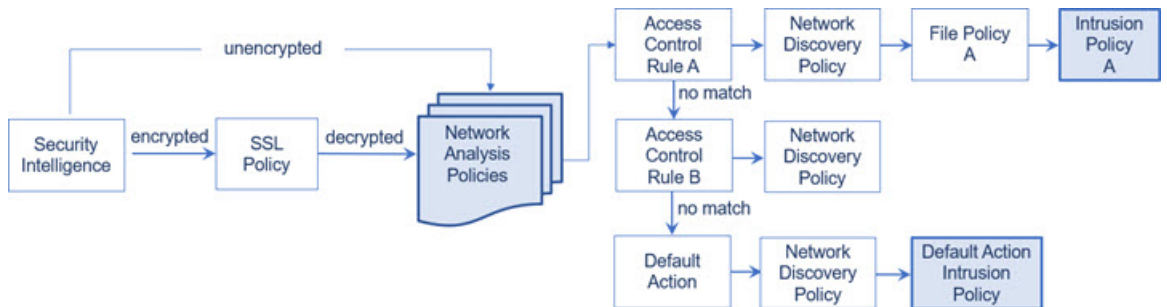
また、カスタムのネットワーク分析ポリシーや侵入ポリシーも作成できます。カスタムポリシーの設定を調整することで、各自に最も役立つ方法でトラフィックを検査できます。これによって、管理対象デバイスのパフォーマンスが向上し、ユーザは生成されたイベントにさらに効率的に対応できるようになります。

Web インターフェイスで同様のポリシーエディタを使用し、ネットワーク分析ポリシーや侵入ポリシーを作成、編集、保存、管理します。いずれかのタイプのポリシーを編集するときには、Web インターフェイスの左側にナビゲーションパネルが表示され、右側にさまざまな設定ページが表示されます。

ポリシーがトラフィックで侵入を検査する方法

アクセスコントロールの展開の一部としてシステムがトラフィックを分析すると、ネットワーク分析（復号と前処理）フェーズが侵入防御（侵入ルールおよび詳細設定）フェーズとは別にその前に実行されます。

次の図は、インラインの侵入防御およびマルウェア防御 展開におけるトラフィック分析の順序を簡略化して示しています。アクセスコントロールポリシーが他のポリシーを呼び出してトラフィックを検査するしくみ、およびそれらのポリシーが呼び出される順序が示されています。ネットワーク分析ポリシーと侵入ポリシーの選択フェーズは強調表示されています。



インライン展開（つまり、ルーテッド、スイッチド、トランスペアレントインターフェイスまたはインラインインターフェイスのペアを使用して関連設定がデバイスに展開される展開）では、システムは上図のプロセスのほぼすべての段階において、追加のインスペクションなしでトラフィックをブロックすることができます。セキュリティインテリジェンス、SSLポリシー、ネットワーク分析ポリシー、ファイルポリシー、および侵入ポリシーのすべてで、トラフィックをドロップまたは変更できます。唯一の例外として、パッシブにパケットを検査するネットワーク検出ポリシーは、トラフィックフローに影響を与えることができません。

同様に、プロセスの各ステップで、パケットによってシステムがイベントを生成する場合があります。侵入およびプリプロセスイベント（総称して「侵入イベント」と呼ばれることもある）は、パケットまたはそのコンテンツがセキュリティリスクを表す可能性を示しています。



ヒント SSL インスペクションの設定で暗号化トラフィックの通過が許可されている場合や、SSL インスペクションが設定されていない場合について、この図は、そのような場合のアクセスコントロールルールによる暗号化トラフィックの処理を反映していません。デフォルトでは、暗号化されたペイロードの侵入インスペクションとファイルインスペクションは無効になっています。これにより、侵入およびファイルインスペクションが設定されたアクセスコントロールルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。

単一の接続の場合は、図に示すように、アクセスコントロールルールよりも前にネットワーク分析ポリシーが選択されますが、一部の前処理（特にアプリケーション層の前処理）はアクセスコントロールルールの選択後に実行されます。これは、カスタムネットワーク分析ポリシーでの前処理の設定には影響しません。

復号、正規化、前処理：ネットワーク分析ポリシー

デコードと前処理を実行しないと、プロトコルの相違によりパターンマッチングを行えなくなるので、侵入についてトラフィックを適切に評価できません。これらのトラフィック処理タスクは、以下のタイミングでネットワーク分析ポリシーによる処理の対象となります。

- 暗号化トラフィックがセキュリティ インテリジェンスによってフィルタリングされた後
- 暗号化トラフィックがオプションの SSL ポリシーによって復号された後
- ファイルまたは侵入ポリシーによってトラフィックを検査できるようになる前

ネットワーク分析ポリシーは、フェーズでのパケット処理を制御します。最初に、システムは最初の3つのTCP/IP層を通ったパケットを復号し、次にプロトコル異常の正規化、前処理、および検出に進みます。

- パケット デコーダは、パケット ヘッダーやペイロードを、プリプロセッサや以降の侵入ルールで簡単に使用できる形式に変換します。TCP/IP スタックの各レイヤのデコードは、データリンク層から開始され、ネットワーク層、トランスポート層へと順番に行われます。パケット デコーダは、パケット ヘッダーのさまざまな異常動作も検出します。
- インライン展開では、インライン正規化プリプロセッサは、攻撃者が検出を免れる可能性を最小限にするために、トラフィックを再フォーマット（正規化）します。その他のプリプロセッサや侵入ルールによる検査用にパケットを準備し、システムで処理されるパケットがネットワーク上のホストで受信されるパケットと同じものになるようにします。



(注) パッシブな展開の場合、シスコでは、ネットワーク分析レベルでインライン正規化を行うのではなく、アクセス コントロール ポリシー レベルで、アダプティブプロファイルの更新を有効にすることを推奨しています。

- ネットワーク層とトランスポート層のさまざまなプリプロセッサは、IPフラグメントを悪用する攻撃を検出したり、チェックサム検証を実行したり、TCP および UDP セッションの前処理を実行したりします。

トランスポートおよびネットワーク プリプロセッサの一部の詳細設定は、アクセス コントロール ポリシーのターゲット デバイスで処理されるすべてのトラフィックにグローバルに適用されます。これらの詳細設定は、ネットワーク分析ポリシーではなくアクセス コントロール ポリシーで設定します。

- 各種のアプリケーション層プロトコル デコーダは、特定タイプのパケット データを侵入ルールエンジンで分析可能な形式に正規化します。アプリケーション層プロトコルのエンコードを正規化することにより、システムはデータ表現が異なるパケットに同じコンテンツ関連の侵入ルールを効果的に適用し、大きな結果を得ることができます。
- Modbus、DNP3、CIP、および s7commplus SCADA プリプロセッサは、トラフィックの異常を検出し、侵入ルールにデータを提供します。Supervisory Control and Data Acquisition

(SCADA) プロトコルは、製造、水処理、配電、空港、輸送システムなどの工業プロセス、インフラストラクチャプロセス、および設備プロセスからのデータをモニタ、制御、取得します。

- 一部のプリプロセッサでは、Back Orifice、ポートスキャン、SYNフラッドおよび他のレートベース攻撃など、特定の脅威を検出できます。

侵入ポリシーで、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する機密データプリプロセッサを設定することに注意してください。

新たに作成されたアクセスコントロールポリシーでは、1つのデフォルトネットワーク分析ポリシーが、同じ親アクセスコントロールポリシーによって呼び出されるすべての侵入ポリシー向けのすべてのトラフィックの前処理を制御します。初期段階では、デフォルトで[バランスの取れたセキュリティと接続 (Balanced Security and Connectivity)] ネットワーク分析ポリシーが使用されますが、別のシステム付属ポリシーやカスタムネットワーク分析ポリシーに変更できます。より複雑な展開では、上級ユーザは、一致するトラフィックの前処理にさまざまなカスタムネットワーク分析ポリシーを割り当てることによって、特定のセキュリティゾーン、ネットワーク、VLAN に合わせてトラフィックの前処理オプションを調整できます。

アクセスコントロールルール：侵入ポリシーの選択

最初の前処理の後、アクセスコントロールルール（ある場合）はトラフィックを評価します。ほとんどの場合、パケットが一致した最初のアクセスコントロールルールがそのトラフィックを処理することになります。ユーザは一致したトラフィックをモニタ、信頼、ブロック、または許可することができます。

アクセスコントロールルールでトラフィックを許可すると、ディスカバリ データ、マルウェア、禁止ファイル、侵入について、この順序でトラフィックを検査できます。アクセスコントロールルールに一致しないトラフィックは、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よって処理されます。デフォルトアクションでは、ディスカバリ データと侵入についても検査できます。



- (注) どのネットワーク分析ポリシーによって前処理されるかに関わらず、すべてのパケットは、設定されているアクセスコントロールルールと上から順に照合されます（したがって、侵入ポリシーによる検査の対象となります）。

[ポリシーがトラフィックで侵入を検査する方法 \(3 ページ\)](#) の図は、インラインの侵入防御およびマルウェア防御 展開でデバイスを通過する、次のようなトラフィックのフローを示しています。

- アクセスコントロールルール A により、一致したトラフィックの通過が許可されます。次にトラフィックは、ネットワーク検出ポリシーによるディスカバリ データの検査、ファイルポリシー A による禁止ファイルおよびマルウェアの検査、侵入ポリシー A による侵入の検査を受けます。

- アクセスコントロールルール B も一致したトラフィックを許可します。ただし、このシナリオでは、トラフィックは侵入（あるいはファイルまたはマルウェア）について検査されないため、ルールに関連付けられている侵入ポリシーやファイルポリシーはありません。通過を許可されたトラフィックは、デフォルトでネットワーク検出ポリシーによって検査されます。したがって、この設定を行う必要はありません。
- このシナリオでは、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で、一致したトラフィックを許可しています。次に、トラフィックはネットワーク検出ポリシー、さらにその後侵入ポリシーによって検査されます。アクセスコントロールルールまたはデフォルトアクションに侵入ポリシーを関連付けるときに、必要に応じて、別の侵入ポリシーを使用できます。

ブロックされたトラフィックや信頼済みトラフィックは検査されないため、図の例には、ブロックルールや信頼ルールは含まれていません。

侵入インスペクション：侵入ポリシー、ルール、変数セット

トラフィックが宛先に向かうことを許可する前に、システムの最終防御ラインとして侵入防御を使用できます。侵入ポリシーは、セキュリティ違反に関するトラフィックの検査方法を制御し、インライン展開では、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。侵入ポリシーの主な機能は、どの侵入ルールおよびプリプロセッサルールを有効にしてどのように設定するかを管理することです。

侵入ルールおよびプリプロセッサルール

侵入ルールはキーワードと引数のセットとして指定され、ネットワーク上の脆弱性を悪用する試みを検出します。システムは侵入ルールを使用してネットワークトラフィックを分析し、トラフィックがルールの条件に合致しているかどうかをチェックします。システムは各ルールで指定された条件をパケットに照らし合わせます。ルールで指定されたすべての条件にパケットデータが一致する場合、ルールがトリガーされます。

システムには、Talos インテリジェンスグループ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。

- 共有オブジェクト侵入ルール：コンパイルされており、変更できません（ただし、送信元と宛先のポートや IP アドレスなどのルールヘッダー情報を除く）。
- 標準テキスト侵入ルール：ルールの新しいカスタムインスタンスとして保存および変更できます。
- 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。プリプロセッサルールはコピーまたは編集できません。ほとんどのプリプロセッサルールはデフォルトで無効になっています。プリプロセッサを使用してイベントを生成し、インライン展開では、違反パケットをドロップします。するにはそれらを有効にする必要があります。

システムで侵入ポリシーに従ってパケットを処理する際には、最初にルール オプティマイザが、基準（トランスポート層、アプリケーションプロトコル、保護されたネットワークへの入

出力方向など)に基づいて、サブセット内のすべてのアクティブなルールを分類します。次に、侵入ルールエンジンが、各パケットに適用する適切なルールのサブセットを選択します。最後に、マルチルール検索エンジンが3種類の検索を実行して、トラフィックがルールに一致するかどうかを検査します。

- プロトコルフィールド検索は、アプリケーションプロトコル内の特定のフィールドでの一致を検索します。
- 汎用コンテンツ検索は、パケットペイロードのASCIIまたはバイナリバイトでの一致を検索します。
- パケット異常検索では、特定のコンテンツが含まれているかどうかではなく、確立されたプロトコルに違反しているパケットヘッダーやペイロードが検索されます。

カスタム侵入ポリシーでは、ルールを有効化および無効化し、独自の標準テキストルールを記述および追加することで、検出を調整できます。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、それらの資産を保護するために作成されたルールに関連付けることもできます。

変数セット

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を使用します。セット内の大部分の変数は、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アドレスと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。

システムには、定義済みのデフォルト変数から構成される1つのデフォルト変数セットが含まれています。システム提供の共有オブジェクトルールと標準テキストルールは、これらの定義済みのデフォルト変数を使用してネットワークおよびポート番号を定義します。たとえば、ルールの大半は、保護されたネットワークを指定するために変数 `$HOME_NET` を使用して、保護されていない（つまり外部の）ネットワークを指定するために変数 `$EXTERNAL_NET` を使用します。さらに、特殊なルールでは、他の定義済みの変数がしばしば使用されます。たとえば、Webサーバーに対するエクスプロイトを検出するルールは、`$HTTP_SERVERS` 変数および `$HTTP_PORTS` 変数を使用します。



ヒント システム提供の侵入ポリシーを使用する場合でも、シスコでは、デフォルトセットの主要なデフォルト変数を変更すること強く推奨します。ネットワーク環境を正確に反映する変数を使用すると、処理が最適化され、システムによって疑わしいアクティビティに関連するシステムをモニタできます。高度なユーザは、1つ以上のカスタム侵入ポリシーとペアリングするために、カスタム変数セットを作成して使用できます。

関連トピック

[定義済みデフォルト変数](#)

侵入イベントの生成

侵入されている可能性を特定すると、システムは侵入イベントまたはプリプロセッサイベント（まとめて侵入イベントと呼ばれることもあります）を生成します。管理対象デバイスは Management Center にイベントを送信します。ここで、集約データを確認し、ネットワーク アセットに対する攻撃を的確に把握できます。インライン展開では、管理対象デバイスは、有害であると判明しているパケットをドロップまたは置き換えることができます。

データベース内の各侵入イベントにはイベントヘッダーがあり、イベント名と分類、送信元と宛先の IP アドレス、ポート、イベントを生成したプロセス、およびイベントの日時に関する情報、さらに攻撃の送信元とそのターゲットに関するコンテキスト情報が含まれています。パケットベースのイベントの場合、システムは復号されたパケットヘッダーとイベントをトリガーしたパケット（複数の場合あり）のペイロードのコピーもログに記録します。

パケット デコーダ、プリプロセッサ、および侵入ルールエンジンはすべて、システムによるイベントの生成を引き起こします。次に例を示します。

- (ネットワーク分析ポリシーで設定された) パケット デコーダが 20 バイト (オプションやペイロードのない IP データグラムのサイズ) 未満の IP パケットを受け取った場合、デコーダはこれを異常なトラフィックと解釈します。パケットを検査する侵入ポリシー内の付随するデコーダルールが有効な場合、システムは後でプリプロセッサ イベントを生成します。
- IP 最適化プリプロセッサが重複する一連の IP フラグメントを検出した場合、プリプロセッサはこれを潜在的な攻撃と解釈して、付随するプリプロセッサルールが有効な場合、システムはプリプロセッサ イベントを生成します。
- 侵入ルールエンジン内では、ほとんどの標準テキストルールおよび共有オブジェクトルールはパケットによってトリガーされた場合に侵入イベントを生成するように記述されます。

データベースに侵入イベントが蓄積されると、ユーザは攻撃の可能性について分析を開始できます。システムは、ユーザが侵入イベントを確認し、ネットワーク環境とセキュリティポリシーのコンテキストでそのイベントが重要であるかどうかを評価するために必要なツールを提供します。

システム提供およびカスタムネットワーク分析ポリシーと侵入ポリシー

新しいアクセス コントロール ポリシーを作成することは、システムを使用してトラフィックフローを管理するための最初のステップの1つです。デフォルトでは、新しく作成されたアクセス コントロール ポリシーは、システムによって提供されるネットワーク分析ポリシーおよび侵入ポリシーを呼び出してトラフィックを検査します。

次の図は、インラインの侵入防御展開で、新たに作成されたアクセス コントロール ポリシーが最初にトラフィックを処理するしくみを示しています。前処理と侵入防御フェーズは強調表示されています。

図 1:新しいアクセス コントロール ポリシー : 侵入防御



以下の点に注意してください。

- デフォルトのネットワーク分析ポリシーによって、アクセス コントロール ポリシーで処理されるすべてのトラフィックの前処理が制御されます。初期段階では、システムによって提供される **Balanced Security and Connectivity** ネットワーク分析ポリシーがデフォルトです。
- 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は、システム付属の **Balanced Security and Connectivity** 侵入ポリシーによる検査に従って、悪意のないトラフィックをすべて許可します。デフォルトアクションはトラフィックの通過を許可するので、侵入ポリシーが悪意のあるトラフィックを検査して潜在的にブロックする前に、検出機能によって、ホスト、アプリケーション、ユーザ データについてトラフィックを検査できます。
- ポリシーは、デフォルトのセキュリティ インテリジェンス オプション（グローバルなブロックリストとブロックなしリストのみ）を使用し、SSL ポリシーによる暗号化トラフィックの復号や、アクセス コントロール ルールを使用したネットワークトラフィックの特別な処理や検査は実行しません。

侵入防御展開を調整するために実行できるシンプルなステップは、システム付属のネットワーク分析ポリシーと侵入ポリシーの別のセットをデフォルトとして使用することです。システムには、これらのポリシーの複数のペアが提供されています。

または、カスタムポリシーを作成して使用することで、侵入防御展開を調整できます。それらのポリシーに設定されているプリプロセッサオプション、侵入ルール、およびその他の詳細設定が、ネットワークのセキュリティ ニーズに適合しない場合があります。設定できるネットワーク分析ポリシーおよび侵入ポリシーを調整することにより、システムがネットワーク上のトラフィックを処理して侵入の有無について検査する方法を非常にきめ細かく設定できます。

システム提供のネットワーク分析ポリシーと侵入ポリシー

システムには、ネットワーク分析ポリシーと侵入ポリシーのペアがいくつか付属しています。システム提供のネットワーク分析ポリシーおよび侵入ポリシーを使用して、**Talos** インテリジェンスグループのエクスペリエンスを活用することができます。これらのポリシーでは、**Talos** が侵入ルールおよびプリプロセッサルールの状態、ならびにプリプロセッサおよび他の詳細設定の初期設定も指定しています。

すべてのネットワークプロファイル、最小トラフィック、または防御ポスタチャに対応したシステム付属ポリシーはありません。これらの各ポリシーは一般的なケースとネットワークのセットアップに対応しているため、これらのポリシーに基づいて適切に調整された防御ポリシーを

策定することができます。システム付属ポリシーは、変更せずにそのまま使用できますが、カスタムポリシーのベースとして使用し、カスタムポリシーを各自のネットワークに合わせて調整することが推奨されます。



ヒント システム付属のネットワーク分析ポリシーと侵入ポリシーを使用する場合でも、ネットワーク環境が正確に反映されるように、システムの侵入変数を設定する必要があります。少なくとも、デフォルトのセットにある主要なデフォルトの変数を変更します。

新しい脆弱性が知られるようになると、Talos が侵入ルールの更新をリリースします（「Snort ルールの更新」とも呼ばれます）。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、侵入ルールやア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。ルールアップデートでは、システム付属のポリシーからルールが削除されたり、新しいルールカテゴリが提供されたり、さらにデフォルトの変数セットが変更されることもあります。

ルール更新によって展開が影響を受けると、Web インターフェイスは影響を受けた侵入ポリシーやネットワーク分析ポリシー、およびそれらの親のアクセスコントロールポリシーを失効したものと扱います。変更を有効にするには、更新されたポリシーを再展開する必要があります。

必要に応じて、影響を受けた侵入ポリシーを（単独で、または影響を受けたアクセスコントロールポリシーと組み合わせて）自動的に再展開するように、ルールの更新を設定できます。これにより、新たに検出されたエクスプロイトおよび侵入から保護するために展開環境を容易に自動的に最新に維持することができます。

前処理の設定を最新の状態に保つには、アクセスコントロールポリシーを再展開する**必要があります**。これにより、現在実行されているものとは異なる、関連するSSLポリシー、ネットワーク分析ポリシー、ファイルポリシーが再展開され、前処理とパフォーマンスの詳細設定オプションのデフォルト値も更新できるようになります。

システムに付属しているネットワーク分析ポリシーと侵入ポリシーのペアは以下のとおりです。

[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。一緒に使用すると、ほとんどの組織および展開タイプにとって最適な出発点となります。ほとんどの場合、システムは Balanced Security and Connectivity のポリシーおよび設定をデフォルトとして使用します。

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（すべてのリソースに到達可能な）の方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優先される組織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組織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

このポリシーは、Security over Connectivity ポリシー以上にネットワークインフラストラクチャのセキュリティを重視する組織のために作成されています。動作への影響がさらに高くなる可能性があります。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。

[アクティブなルールなし (No Rules Active)] 侵入ポリシー

[アクティブなルールなし (No Rules Active)] 侵入ポリシーでは、すべての侵入ルールと侵入ルールのしきい値を除くすべての詳細設定が無効にされます。このポリシーは、他のシステムによって提供されるポリシーのいずれかで有効になっているルールをベースにするのではなく、独自の侵入ポリシーを作成する場合の出発点を提供します。



(注) 選択されているシステムから提供されるベースポリシーによって、ポリシーの設定が異なります。ポリシー設定を表示するには、ポリシーの横にある [編集 (Edit)] アイコンをクリックしてから、[ベースポリシーの管理 (Manage Base Policy)] リンクをクリックします。

カスタムネットワーク分析ポリシーと侵入ポリシーの利点

システムによって提供されるネットワーク分析ポリシーおよび侵入ポリシーに設定されたプリプロセッサオプション、侵入ルール、およびその他の詳細設定は、組織のセキュリティニーズに十分に対応しない場合があります。

カスタム侵入ポリシーを作成すると、環境内のシステムのパフォーマンスを向上させ、ネットワークで発生する悪意のあるトラフィックやポリシー違反を重点的に観察できるようになります。設定できるカスタムポリシーを作成および調整することにより、システムがネットワーク上のトラフィックを処理して侵入の有無について検査する方法を非常にきめ細かく設定できます。

すべてのカスタムポリシーには基本ポリシー (別名「基本レイヤ」) があり、それによって、ポリシー内のすべてのコンフィギュレーションのデフォルト設定が定義されます。レイヤは、複数のネットワーク分析ポリシーまたは侵入ポリシーを効率的に管理するために使用できる構成要素です。

ほとんどの場合、カスタムポリシーはシステム付属のポリシーに基づきますが、別のカスタムポリシーを使用することもできます。ただし、すべてのカスタムポリシーには、ポリシーチェーンの根本的な基礎としてシステム付属ポリシーが含まれています。システム付属のポリ

シーはルールアップデートによって変更される可能性があるため、カスタムポリシーを基本として使用している場合でも、ルールアップデートをインポートするとポリシーに影響が及びます。ルール更新によって展開に影響を受けると、Web インターフェイスは影響を受けたポリシーを失効として扱います。

カスタム ネットワーク分析ポリシーの利点

デフォルトでは、1つのネットワーク分析ポリシーによって、アクセスコントロールポリシーで処理されるすべての暗号化されていないトラフィックが前処理されます。これは、侵入ポリシー（および侵入ルールセット）に関係なく、すべてのパケットが同じ設定に基づいてデコードされ、処理されることを意味します。

初期段階では、システムによって提供される **Balanced Security and Connectivity** ネットワーク分析ポリシーがデフォルトです。前処理を調整する簡単な方法は、デフォルトとしてカスタム ネットワーク分析ポリシーを作成して使用することです。

使用可能な調整オプションはプリプロセッサによって異なりますが、プリプロセッサおよびコードを調整できる方法には次のものがあります。

- モニターしているトラフィックに適用されないプリプロセッサを無効にできます。たとえば、HTTP Inspect プリプロセッサは HTTP トラフィックを正規化します。ネットワークに Microsoft インターネット インフォメーション サービス (IIS) を使用する Web サーバが含まれていないことが確実な場合は、IIS 特有のトラフィックを検出するプリプロセッサ オプションを無効にすることで、システム処理のオーバーヘッドを軽減できます。



(注) カスタム ネットワーク分析ポリシーでプリプロセッサが無効化されているときに、パケットを有効な侵入ルールまたはプリプロセッサルールと照合して評価するために、プリプロセッサを使用する必要がある場合、システムはプリプロセッサを有効化して使用します。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。

- 必要に応じて、特定のプリプロセッサのアクティビティを集中させるポートを指定します。たとえば、DNS サーバの応答や暗号化 SSL セッションをモニタするための追加ポートや、Telnet、HTTP、RPC トラフィックを復号するポートを特定できます。

複雑な環境での高度なユーザの場合は、複数のネットワーク分析ポリシーを作成し、それぞれがトラフィックを別々に前処理するように調整することができます。さらに、トラフィックのセキュリティゾーン、ネットワーク、または VLAN に応じて前処理が制御されるようにこれらのポリシーを設定できます。



(注) カスタム ネットワーク分析ポリシー（特に複数のネットワーク分析ポリシー）を使用して前処理を調整することは、高度なタスクです。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、単一の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が相互補完することを許可する場合は、注意する必要があります。

カスタム侵入ポリシーの利点

侵入防御を実行するように初期設定して、新規にアクセス コントロール ポリシーを作成した場合、そのポリシーでは、デフォルトアクションはすべてのトラフィックを許可しますが、最初にシステム付属の **Balanced Security and Connectivity** 侵入ポリシーでトラフィックをチェックします。アクセス コントロール ルールを追加するか、またはデフォルト アクションを変更しない限り、すべてのトラフィックがその侵入ポリシーによって検査されます。

侵入防御展開をカスタマイズするために、複数の侵入ポリシーを作成し、それぞれがトラフィックを異なる方法で検査するように調整できます。次に、どのポリシーがどのトラフィックを検査するかを指定するルールを、アクセス コントロール ポリシーに設定します。アクセス コントロール ルールは単純でも複雑でもかまいません。セキュリティゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求されたURL、またはユーザなど、複数の基準を使用してトラフィックを照合および検査します。

侵入ポリシーの主な機能は、次のように、どの侵入ルールおよびプリプロセッサルールを有効にしてどのように設定するかを管理することです。

- 各侵入ポリシーで、環境に適用されるすべてのルールが有効になっていることを確認し、環境に適用されないルールを無効化することによって、パフォーマンスを向上させます。インライン展開では、どのルールによって悪質なパケットをドロップまたは変更するかを指定できます。
- Cisco 推奨機能を使用すると、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作成されたルールに関連付けることができます。
- 必要に応じて、既存のルールの変更や、新しい標準テキストルールの作成により、新たなエクスプロイトの検出やセキュリティ ポリシーの適用が可能です。

侵入ポリシーに対して行えるその他のカスタマイズは次のとおりです。

- 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、数種類のポートスキャン、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。
- グローバルしきい値を設定すると、侵入ルールに一致するトラフィックが、指定期間内に特定のアドレスまたはアドレス範囲で送受信される回数に基づいて、イベントが生成されます。これにより、大量のイベントによってシステムに過剰な負荷がかかることを回避できます。
- また、個々のルールまたは侵入ポリシー全体に対して、侵入イベント通知を抑制し、しきい値を設定することで、大量のイベントによってシステムに過剰な負荷がかかることを回避することもできます。
- 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、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。

カスタム ポリシーの制限

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、単一のパケットを処理および検査する、ネットワーク分析ポリシーと侵入ポリシーが相互補完することを設定で許可する場合は、注意する**必要があります**。

デフォルトでは、システムは、管理対象デバイスでアクセス コントロール ポリシーにより処理されるすべてのトラフィックを、1つのネットワーク分析ポリシーを使用して前処理します。次の図は、インラインの侵入防御展開で、新たに作成されたアクセス コントロール ポリシーが最初にトラフィックを処理するしくみを示しています。前処理と侵入防御フェーズは強調表示されています。

図 2: 新しいアクセス コントロール ポリシー : 侵入防御



アクセス コントロール ポリシーで処理されるすべてのトラフィックの前処理が、デフォルトのネットワーク分析ポリシーによってどのように制御されるのかに注意してください。初期段階では、システムによって提供される **Balanced Security and Connectivity** ネットワーク分析ポリシーがデフォルトです。

前処理を調整する簡単な方法は、デフォルトとしてカスタム ネットワーク分析ポリシーを作成して使用することです。ただし、カスタム ネットワーク分析ポリシーでプリプロセッサが無効化されているときに、前処理されたパケットを有効な侵入ルールまたはプリプロセッサルールと照合して評価する必要がある場合、システムはプリプロセッサを有効化して使用します。ただし、ネットワーク分析ポリシーの **Web ユーザ** 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) プリプロセッサを無効にするパフォーマンス上の利点を得るには、侵入ポリシーでそのプリプロセッサを必要とするルールが有効になっていないことを確認する**必要があります**。

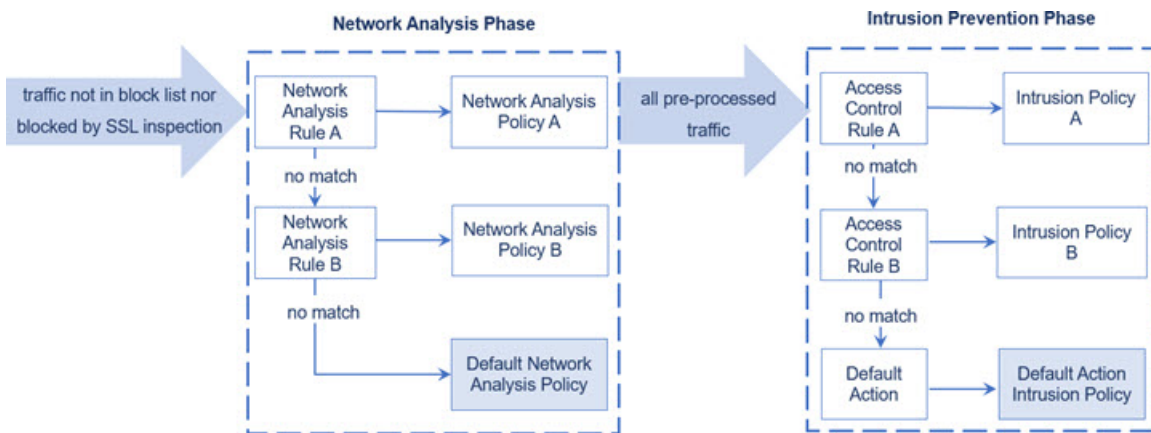
複数のカスタム ネットワーク分析ポリシーを使用する場合は、さらに課題があります。複雑な展開内の上級ユーザの場合は、一致したトラフィックの前処理にカスタム ネットワーク分析ポリシーを割り当てることによって、特定のセキュリティゾーン、ネットワーク、VLAN に合わせて前処理を調整できます。これを実現するには、アクセス コントロール ポリシーにカスタム ネットワーク分析ルールを追加します。各ルールにはネットワーク分析ポリシーが関連付けられており、ルールに一致するトラフィックの前処理を制御します。



ヒント アクセス コントロール ポリシーの詳細設定としてネットワーク分析ルールを設定します。システムの他のタイプのルールとは異なり、ネットワーク分析ルールは、ネットワーク分析ポリシーに含まれているのではなく、それを呼び出します。

システムは、ルール番号の昇順で、設定済みネットワーク分析ルールとパケットを照合します。いずれのネットワーク分析ルールにも一致しないトラフィックは、デフォルトのネットワーク分析ポリシーによって前処理されます。これにより非常に柔軟にトラフィックを前処理できます。ただし、留意すべき点として、パケットがどのネットワーク分析ポリシーによって前処理されるかに**関係なく**、すべてのパケットは、それら独自のプロセスにおいて引き続きアクセス コントロールルールと照合されます（つまり、侵入ポリシーにより検査される可能性があります）。つまり、特定のネットワーク分析ポリシーでパケットを前処理しても、そのパケットが確実に特定の侵入ポリシーで検査されるわけでは**ありません**。アクセスコントロールポリシーを設定するときは、そのポリシーが正しいネットワーク分析ポリシーおよび侵入ポリシーを呼び出して特定のパケットを評価するように、慎重に行う**必要があります**。

次の図は、侵入防御（ルール）フェーズよりも前に、別にネットワーク分析ポリシー（前処理）の選択フェーズが発生するしくみを詳細に示しています。簡略化するために、図では検出フェーズとファイル/マルウェア インспекションフェーズが省かれています。また、デフォルトのネットワーク分析ポリシーおよびデフォルトアクションの侵入ポリシーを強調表示しています。



このシナリオでは、アクセス コントロール ポリシーに、2つのネットワーク分析ルールとデフォルトのネットワーク分析ポリシーが設定されています。

- Network Analysis Rule A は、一致するトラフィックを Network Analysis Policy A で前処理します。その後、このトラフィックを Intrusion Policy A で検査されるようにすることができます。
- Network Analysis Rule B は、一致するトラフィックを Network Analysis Policy B で前処理します。その後、このトラフィックを Intrusion Policy B で検査されるようにすることができます。

- 残りのトラフィックはすべて、デフォルトのネットワーク分析ポリシーにより前処理されます。その後、このトラフィックを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た侵入ポリシーによって検査されるようにすることができます。

システムはトラフィックを前処理した後、侵入についてトラフィックを検査できます。図では、2つのアクセスコントロールルールとデフォルトアクションが含まれるアクセスコントロールポリシーを示しています。

- アクセスコントロールルール A は、一致したトラフィックを許可します。トラフィックはその後、Intrusion Policy A によって検査されます。
- アクセスコントロールルール B は、一致したトラフィックを許可します。トラフィックはその後、Intrusion Policy B によって検査されます。
- 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は一致したトラフィックを許可します。トラフィックはその後、デフォルトアクションの侵入ポリシーによって検査されます。

各パケットの処理は、ネットワーク分析ポリシーと侵入ポリシーのペアにより制御されますが、このペアはユーザに合わせて調整されません。アクセスコントロールポリシーが誤って設定されているため、ネットワーク分析ルール A とアクセスコントロールルール A が同じトラフィックを処理しない場合を想定してください。たとえば、特定のセキュリティゾーンのトラフィックの処理をポリシーペアによって制御することを意図している場合に、誤まって、異なるゾーンを使用するように2つのルールの条件を設定したとします。この誤設定により、トラフィックが誤って前処理される可能性があります。したがって、ネットワーク分析ルールおよびカスタムポリシーを使用した前処理の調整は、**高度なタスク**です。

単一の接続の場合は、アクセスコントロールルールよりも前にネットワーク分析ポリシーが選択されますが、一部の前処理（特にアプリケーション層の前処理）はアクセスコントロールルールの選択後に実行されます。これは、カスタムネットワーク分析ポリシーでの前処理の設定には影響しません。

ネットワーク分析ポリシーと侵入ポリシーのライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

ネットワーク分析と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

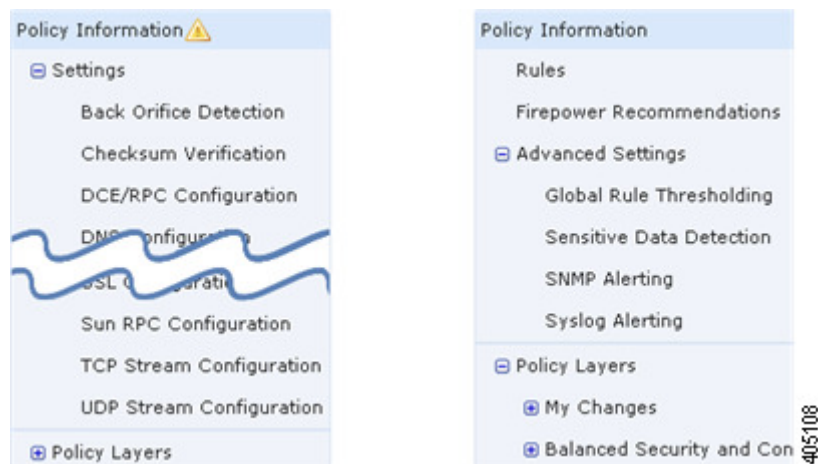
ユーザの役割

- 管理者
- 侵入管理者

ナビゲーションウィンドウ: ネットワーク分析と侵入ポリシー

ネットワーク分析ポリシーと侵入ポリシーは同様の Web インターフェイスを使用して、設定への変更を編集して保存します。

いずれかのタイプのポリシーを編集するときに、Web インターフェイスの左側にナビゲーションパネルが表示されます。次の図は、ネットワーク分析ポリシー（左）および侵入ポリシー（右）のナビゲーションパネルを示しています。



境界線が、ポリシー層との直接対話を使用して構成可能なポリシー設定へのリンク（下側）とポリシー層との直接対話を使用せずに構成可能なポリシー設定へのリンク（上側）にナビゲーションパネルを分割します。いずれかの設定ページに移動するには、ナビゲーションパネル内の名前をクリックします。ナビゲーションパネルで影付きで強調表示されている項目は、現

在の設定ページを示しています。たとえば、上の図では、[ポリシー情報 (Policy Information)] ページがナビゲーションパネルの右側に表示されます。

[ポリシー情報 (Policy Information)]

[ポリシー情報 (Policy Information)] ページには、一般的に使用される設定の設定オプションが表示されます。上記のネットワーク分析ポリシーパネルの図に示すように、ポリシーに未保存の変更がある場合は、ナビゲーションパネルの [ポリシー情報 (Policy Information)] の横にポリシー変更アイコンが表示されます。アイコンは、変更を保存すると消えます。

[ルール (Rules)] (侵入ポリシーのみ)

侵入ポリシーの [ルール (Rules)] ページでは、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のルールステータスとその他の設定項目を設定できます。

Cisco の推奨事項 (侵入ポリシーのみ)

侵入ポリシーの [Cisco の推奨事項 (Cisco Firepower Recommendations)] ページでは、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、各アセットを保護するために作成された侵入ルールに関連付けることができます。これにより、モニタ対象のネットワークの特定ニーズに合わせて侵入ポリシーを調整できます。

[Settings] (ネットワーク分析ポリシー) および [Advanced Settings] (侵入ポリシー)

ネットワーク分析ポリシーの [設定 (Settings)] ページでは、プリプロセッサを有効または無効にしたり、プリプロセッサの設定ページにアクセスしたりできます。[設定 (Settings)] リンクを展開すると、ポリシー内で有効になっているすべてのプリプロセッサの個々の設定ページへのサブリンクが表示されます。

侵入ポリシーの [詳細設定 (Advanced Settings)] ページでは、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したりできます。[詳細設定 (Advanced Settings)] リンクを展開すると、ポリシー内で有効になっているすべての詳細設定を個々に設定する設定ページへのサブリンクが表示されます。

[Policy Layers]

[ポリシー層 (Policy Layers)] ページには、ネットワーク分析ポリシーまたは侵入ポリシーを構成する階層の要約が表示されます。[ポリシー層 (Policy Layers)] リンクを展開すると、ポリシー内の階層に関する概要ページへのサブリンクが表示されます。各階層のサブリンクを展開すると、その階層で有効になっているすべてのルール、プリプロセッサ、または詳細設定の設定ページへのサブリンクがさらに表示されます。

競合と変更：ネットワーク分析ポリシーと侵入ポリシー

ネットワーク分析ポリシーや侵入ポリシーを編集するときに、ポリシーに未保存の変更がある場合は、そのことを示すために、ナビゲーションパネルの [ポリシー情報 (Policy Information)]

の横に**ポリシー変更アイコン**が表示されます。変更をシステムに認識させるには、変更を保存（確定）する必要があります。



- (注) 保存後は、変更を反映させるためにネットワーク分析ポリシーまたは侵入ポリシーを展開する必要があります。保存しないでポリシーを展開すると、最後に保存された設定が使用されません。

編集競合の解決

[ネットワーク分析ポリシー (Network Analysis Policy)] ページ ([**ポリシー (Policies)**] > [**アクセス制御 (Access Control)**]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [**Policies**] > [**Access Control**] > [**Intrusion**]、次に [**Network Analysis Policies**] および [侵入ポリシー (Intrusion Policy)] ページ ([**ポリシー (Policies)**] > [**アクセス制御 (Access Control)**] > [**侵入 (Intrusion)**]) には、各ポリシーの未保存の変更の有無、および現在ポリシーを編集中のユーザ情報が表示されます。シスコでは、同時に1人だけがポリシーを編集することを推奨します。同時編集を実行すると、次のようになります。

- ネットワーク分析ポリシーまたは侵入ポリシーを編集しているときに、同時に他のユーザが同じポリシーを編集し、ポリシーへの変更を保存した場合、ポリシーを確定すると、他のユーザの変更が上書きされることを警告するメッセージが表示されます。
- 同じユーザーとして複数の Web インターフェイス インスタンス経由で同じネットワーク分析ポリシーまたは侵入ポリシーを編集集中に、1つのインスタンスの変更を保存すると、他のインスタンスの変更は保存できません。

設定の依存関係の解決

特定の分析を実行する場合、多くのプリプロセッサルールとセキュリティルールでは、最初に特定の手法でトラフィックをデコードまたは前処理するか、他の依存関係を割り当てる必要があります。ネットワーク分析ポリシーまたは侵入ポリシーを保存すると、システムが必要な設定を自動的に有効にするか、または次のように無効な設定はトラフィックに影響しないことが警告されます。

- SNMPルールアラートを追加しても、SNMPアラートを設定しなかった場合は、侵入ポリシーを保存できません。SNMPアラートを設定するか、またはルールアラートを無効にしてから、再度保存します。
- 侵入ポリシーに有効なセンシティブデータルールが含まれているときに、センシティブデータプリプロセッサが有効になっていない場合は、侵入ポリシーを保存できません。システムがプリプロセッサを有効にしてポリシーを保存するように許可するか、またはルールを無効にしてから、再度保存します。
- ネットワーク分析ポリシーで必要なプリプロセッサを無効化しても、まだポリシーを保存できます。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プリプロセッサは無効になっていても、システムは無効になっているプリプロセッサを自動的に現在の設定で使用します。

- ネットワーク分析ポリシーでインラインモードを無効にしても、インライン正規化プリプロセッサが有効になっている場合は、ポリシーを引き続き保存できます。ただし、正規化設定が無視されることが警告されます。インラインモードを無効化すると他の設定が無視されるので、プリプロセッサは、チェックサム検証やレートベース攻撃の防御を含めて、トラフィックを変更またはブロックできます。

ポリシー変更のコミット、破棄、およびキャッシュ

ネットワーク分析ポリシーまたは侵入ポリシーの編集時に、変更を保存しないでポリシーエディタを終了した場合、それらの変更はシステムによってキャッシュされます。変更は、システムからログアウトしたり、システムクラッシュが発生したりした場合でもキャッシュされます。システムキャッシュには、ユーザごとに1つのネットワーク分析ポリシーと1つの侵入ポリシーの未保存の変更しか格納されないため、同じタイプの別のポリシーを編集する場合は、その前に、行った変更を確定または破棄する必要があります。システムは、ユーザが最初のポリシーへの変更を保存せずに別のポリシーを編集したり、侵入ルールの更新をインポートした場合に、キャッシュされた変更内容を破棄します。

ネットワーク分析ポリシーエディタまたは侵入ポリシーエディタの [ポリシー情報 (Policy Information)] ページでポリシーの変更内容をコミットまたは破棄できます。

Secure Firewall Management Center 設定では、以下を制御できます。

- ネットワーク分析ポリシーまたは侵入ポリシーへの変更を確定するときに、それに関するコメントの入力を求めるか (または、コメントの入力を必須とするか)
- 変更内容とコメントを監査ログに記録するか

ネットワーク分析または侵入ポリシーの終了

手順

ネットワーク分析、または侵入ポリシーの拡張エディタを終了するには、以下の方法があります。

- **キャッシュ**：ポリシーを終了し、変更をキャッシュするには、いずれかのメニューを選択するか、別のページへのほかのパスを選択します。終了時に表示される [ページを移動 (Leave page)] をクリックするか、[ページを移動しない (Stay on page)] をクリックして拡張エディタに残ります。
- **破棄**：保存されていない変更を破棄するには、[ポリシー情報 (Policy Information)] ページの [変更の破棄 (Discard Changes)] をクリックし、[OK] をクリックします。
- **保存**：ポリシーの変更を保存するには、[ポリシー情報 (Policy Information)] ページの [変更の確定 (Commit Changes)] をクリックします。プロンプトが表示される場合、コメントを入力し、[OK] をクリックします。

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。