



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、ネットワーク分析ポリシーと侵入ポリシーの概要を示します。

- [ネットワーク分析ポリシーと侵入ポリシーの基本 \(1 ページ\)](#)
- [ポリシーが侵入についてトラフィックを検査する仕組み \(2 ページ\)](#)
- [システム提供およびカスタムのネットワーク分析ポリシーと侵入ポリシー \(8 ページ\)](#)
- [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 \(16 ページ\)](#)
- [競合と変更: ネットワーク分析および侵入ポリシー \(17 ページ\)](#)

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、Firepower 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。

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っており、これにより、ユーザは指定された値を使用してネットワーク環境を正確に反映できます。

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、別にネットワーク分析（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。これらのポリシーは、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、アラート、防御に役立ちます。

Firepower システムには、同様の名前（Balanced Security and Connectivity など）が付いた複数のネットワーク分析ポリシーと侵入ポリシーが付属しており、それらは相互に補完して連携します。システム付属のポリシーを使用することで、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 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。

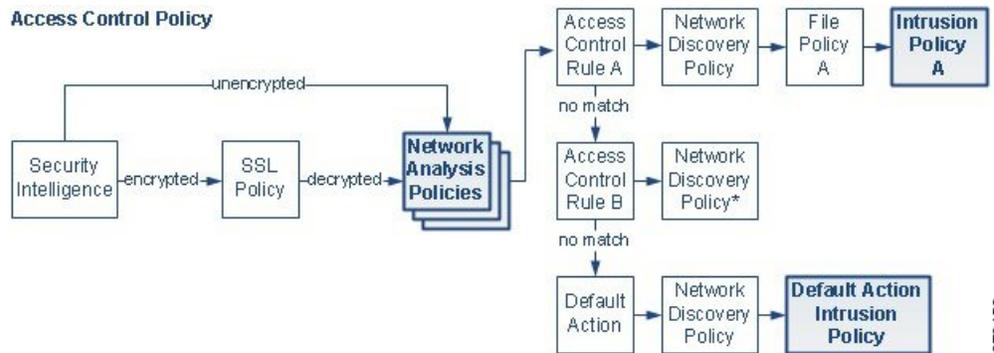
また、カスタムのネットワーク分析ポリシーや侵入ポリシーも作成できます。カスタムポリシーの設定を調整することで、各自にもっとも役立つ方法でトラフィックを検査できます。これによって、管理対象デバイスのパフォーマンスが向上し、ユーザは生成されたイベントにさらに効率的に対応できるようになります。

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。

ポリシーが侵入についてトラフィックを検査する仕組み

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（復号化と前処理）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ネットワーク向け AMP 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を示しています。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。



373458

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ッサイベント（総称的に「侵入イベント」とも呼ばれる）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含んでいる可能性を示唆しています。



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、暗号化ペイロードの侵入およびファイルインスペクションは無効化されます。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、いくつかの前処理（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。

復号化、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化された後
- 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。まず、最初の3つのTCP/IPレイヤを経由するパケットがデコードされ、続いて、標準化、前処理、プロトコルの異常の検出が行われます。

- パケットデコーダは、パケットヘッダーとペイロードを、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、パケットヘッダーからさまざまな異常動作を検出します。
- 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に向けてパケットを準備し、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 と DNP3 のプリプロセッサは、トラフィックの異常を検出し、データを侵入ルールに提供します。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バース攻撃など、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について、前処理を制御します。最初に、デフォルトでは **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、トラフィックはアクセスコントロールルール（設定されている場合）によって評価されます。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

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）。

ポリシーが侵入についてトラフィックを検査する仕組み (2 ページ) の図は、インラインの侵入防御およびネットワーク向け AMP 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、これを設定する必要はありません。
- 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は一致したトラフィックを許可します。次に、トラフィックはネットワーク検出ポリシーによって検査されてから、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、有効にする侵入ルールとプリプロセッサルールの選択および設定方法を管理することです。

侵入ルールと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。システムが各ルール内で指定された条件とパケットを照らし合わせます。そして、パケットデータとルール内で指定されたすべての条件が一致した場合に、ルールがトリガーとして使用されます。

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。

- 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：ネットワーク分析ポリシーのプリプロセッサおよびパケットデコード検出オプションに関連付けられています。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とき、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してい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。Firepower 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、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。

変数セット

システムが侵入ポリシーを使用してトラフィックを評価する場合、システムは関連付けられた変数セットを使用します。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。上級ユーザはカスタム変数セットを作成して、1つ以上のカスタム侵入ポリシーと組み合わせることができます。

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 Firepower 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、システムは復号化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。以降、パケットを検査する侵入ポリシーで付随するデコーダルールが有効な場合は、システムによってプリプロセッサイベントが生成されます。

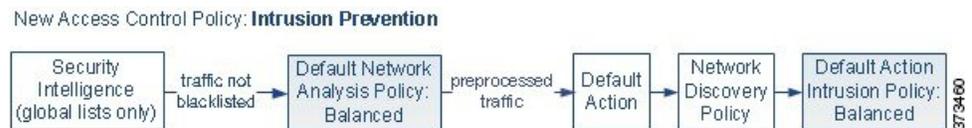
- IP最適化プリプロセッサが重複する一連のIPフラグメントを検出した場合、プリプロセッサはこれを潜在的な攻撃と解釈し、付随するプリプロセッサルールが有効な場合はシステムによってプリプロセッサ イベントが生成されます。
- 侵入ルールエンジン内では、ほとんどの標準テキストルールおよび共有オブジェクトルールはパケットによってトリガーされた場合に侵入イベントを生成するように記述されます。

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のネットワーク分析ポリシーと侵入ポリシー

Firepower システムを使用してトラフィック フローを管理する最初のステップの1つは、新しいアクセス コントロール ポリシーを作成することです。デフォルトでは、新たに作成されたアクセスコントロールポリシーは、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。前処理および侵入防御のフェーズが強調表示されています。



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。最初は、システム付属の *Balanced Security and Connectivity* ネットワーク分析ポリシーがデフォルトになります。
- 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、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（グローバルなホワイトリストとブラックリストのみ）を使用し、SSLポリシーによる暗号化トラフィックの復号化や、アクセス コントロール ルールによるネットワーク トラフィックの特別な処理や検査を実行しません。

侵入防御展開を調整するために実行できる簡単な手順は、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。Firepower 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

Firepower 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、Cisco Talos Intelligence Group (Talos) 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)。これらのルールアップデートにより、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、侵入ルールとプリプロセッサルールの新規作成または更新、既存ルールの状態の変更、および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して扱います。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。

Firepower 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、**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。

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、正規のトラフィックにアラートを発したり、それらのトラフィックを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。

No Rules Active 侵入ポリシー

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 ネットワーク分析とカスタム侵入ポリシーの利点

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、組織のネットワークのセキュリティニーズに完全に合致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に焦点を当てたビューを提供できます。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最終的なベース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が影響を受けると、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。

ユーザが作成するカスタムポリシーに加えて、システムには、初期インラインポリシーと初期パッシブポリシーという2つのカスタム侵入ポリシーと2つのネットワーク分析ポリシーが用意されています。これらのポリシーは、該当する「Balanced Security and Connectivity」ポリシーを基本ポリシーとして使用します。両者の唯一の相違点はドロップ動作です。インラインポリシーではトラフィックのブロックと変更が有効化され、パッシブポリシーでは無効化されます。これらのシステム提供のカスタムポリシーは編集して使用できます。

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デコーダを調整できる方法には次のものがあります。

- モニタ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します。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なままになります。

- 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を特定したり、Telnet、HTTP、SMTP トラフィックをデコードするポートを特定できます。

複雑な環境内の上級ユーザの場合は、複数のネットワーク分析ポリシーを作成して、それぞれが異なる方法でトラフィックを処理するように調整できます。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。（ASA FirePOWER モジュールでは、VLAN に応じて前処理を制限することはできません）。



(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。

侵入防御の展開をカスタマイズするために、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異なる方法で処理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であることを確認し、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。
- Firepower 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、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。

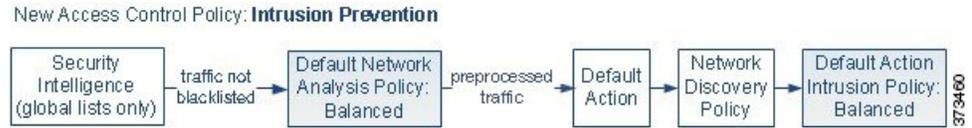
- 機密データ プリプロセッサは、ASCII テキストのクレジットカード番号や社会保障番号などの機密データを検出します。特定の脅威（Back Orifice 攻撃、何種類かのポートスキャン、および過剰なトラフィックによってネットワークを過負荷状態に陥らせようとするレートベース攻撃）を検出するプリプロセッサは、ネットワーク分析ポリシーで設定します。
- グローバルしきい値を設定すると、侵入ルールに一致するトラフィックが、指定期間内に特定のアドレスまたはアドレス範囲で送受信される回数に基づいて、イベントが生成されます。これにより、大量のイベントによってシステムに過剰な負荷がかかることを回避できます。
- 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。前処理および侵入防御のフェーズが強調表示されています。



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なままになります。



- (注) プリプロセッサを無効化してパフォーマンスを向上させるには、どの侵入ポリシーでもプリプロセッサを要求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。(ただし、ASA FirePOWER VLAN による前処理を制限できません)。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、ルールに一致したトラフィックの前処理を制御するネットワーク分析ポリシーが関連付けられています。

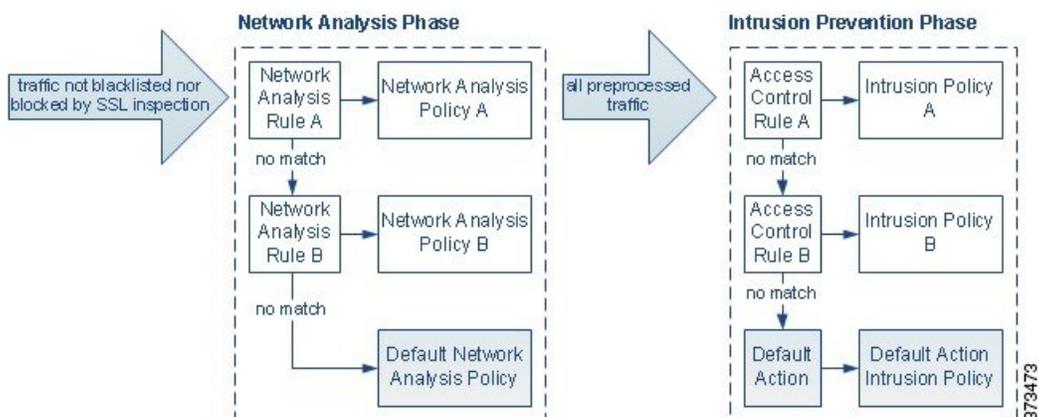


- ヒント** アクセス コントロール ポリシーの詳細設定としてネットワーク分析ルールを設定します。Firepower システムの他のタイプのルールとは異なり、ネットワーク分析ルールは、ネットワーク分析ポリシーに含まれるのではなく、ネットワーク分析ポリシーを呼び出します。

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。ネットワーク分析ルールに一致しなかったトラフィックは、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、アクセス コントロールルール独自のプロセスで引き続きアクセス 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**。適切なネッ

トワーク分析ポリシーと侵入ポリシーを呼び出して特定の packets を評価するように、注意してアクセス コントロール ポリシーを設定する必要があります。

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 インスペクション 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とデフォルトアクションの侵入ポリシーは強調表示されています。



このシナリオでは、アクセス コントロール ポリシーは、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で設定されています。

- ネットワーク分析ルール A は、ネットワーク分析ポリシー A とトラフィックとの照合を前処理します。その後、このトラフィックを侵入ポリシー A によって検査できます。
- ネットワーク分析ルール B は、ネットワーク分析ポリシー B とトラフィックとの照合を前処理します。その後、このトラフィックを侵入ポリシー B によって検査できます。
- 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、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ている侵入ポリシーによってこのトラフィックを検査できます。

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設定された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。その後、トラフィックは侵入ポリシー A により検査されます。
- 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。その後、トラフィックは侵入ポリシー B により検査されます。
- 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。その後、トラフィックは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制御するポリシーペアを意図していた場合に、誤って、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。このような理由から、ネットワーク分析ルールとカスタム 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。

単一の接続の場合、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、いくつかの前処理（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方法に影響しません。

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。



ナビゲーションパネルは境界線によって複数のポリシー設定項目リンクに分割されており、ポリシー層との直接対話により（下側）または直接対話なしで（上側）ポリシー設定項目を設定できます。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、[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。

Policy Information

[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 [Policy Information] の横にポリシー変更アイコン (▲) が表示されます。このアイコンは、変更を保存すると表示されなくなります。

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。

[Firepower の推奨事項 (Firepower Recommendations)] (侵入ポリシーのみ)

侵入ポリシーの [Firepower の推奨事項 (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、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。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のみ) と Advanced Settings (侵入ポリシーのみ)

ネットワーク分析ポリシーの [Settings] ページでは、プリプロセッサとアクセスプリプロセッサの設定ページを有効または無効にすることができます。[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。

侵入ポリシーの [Advanced Settings] ページでは、詳細設定ページと詳細設定のアクセス設定ページを有効または無効にすることができます。[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

[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レイヤの要約が表示されます。[Policy Layers] リンクを展開すると、ポリシー内のレイヤに関するサマリーページへのサブリンクが表示されます。各レイヤのサブリンクを展開すると、レイヤ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。

競合と変更：ネットワーク分析および侵入ポリシー

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 ([Policies] > [Access Control]、次に [Network Analysis Policy] または [Policies] > [Access Control] > [Intrusion]、次に [Network Analysis Policy]) および [侵入ポリシー (Intrusion Policy)] ページ ([Policies] > [Access Control] > [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。
- 同一ユーザとして複数の Web インターフェイ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し、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を保存できなくなります。

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、最初に特定の方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。ネットワーク分析ルールまたは侵入ポリシーを保存すると、システムは必要な設定を自動的に有効にするか、または警告を発して、設定を無効化してもトラフィックに影響がないことを示します。

- 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ルールアラートを無効化してから、再度保存する必要があります。
- 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化してポリシーを保存することを許可するか、ルールを無効化して再度保存する必要があります。
- 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、インライン正規化プリプロセッサを有効化した場合は、ポリシーを保存できます。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せん。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。

Firepower 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

関連トピック

[ネットワーク解析ポリシーの設定の構成](#)

[侵入ポリシー設定の構成](#)

ネットワーク分析または侵入ポリシーの終了

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか (Any)	いずれか (Any)	Admin/Intrusion Admin

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 (ommit 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。
-