ネットワーク分析ポリシーと侵入ポリシーについて

ネットワーク分析ポリシーと侵入ポリシーは、ASA FirePOWER モジュール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。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、ネットワークを通過する悪意のあるトラフィックをブロックまたは変更する機能も加味されます。

ネットワーク分析ポリシーと侵入ポリシーについて

ASA FirePOWER モジュールは、ネットワーク分析ポリシーと侵入ポリシーを使用して侵入検知と防御機能を処理します。

侵入防御展開では、システムがパケットを検査するときに、以下が実行されます。

- 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（総称して「侵入ポリシー 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いるため、名前付き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

ネットワーク分析ポリシーと侵入ポリシーについて

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。

ASA FirePOWER モジュールには、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、それらのポリシーは相互に補完して連携します。システムによって提供されるポリシーを使用することで、シスコ脆弱性調査チーム（VRT）の経験を活用できます。これらのポリシーでは、VRT 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 ポリシー内の設定は、ユーザにとって最も意味のある方法でトラフィックを検査するように調整できます。

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、ユーザ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。

この章では、ネットワーク分析ポリシーおよび侵入ポリシーによって管理される各種設定の概要、ポリシーが連携してトラフィックを検査し、ポリシー違反のレコードを生成するしくみ、および、ポリシーエディタの基本的な操作方法について説明します。また、カスタムポリシーとシステム付属ポリシーを比較して、それらの使用上の利点と制約についても説明します。侵入防御展開をカスタマイズするには、以下の該当する手順を参照してください。

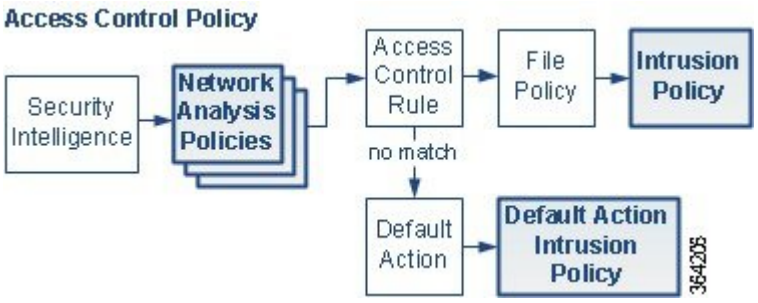
- 変数セットの操作には、ネットワーク環境を正確に反映させるためのシステムの侵入変数の設定方法が記載されています。カスタムポリシーを使用しない場合でも、デフォルトの変数セットのデフォルト変数を変更することを強く推奨します。上級ユーザはカスタム変数セットを作成して、1 つ以上のカスタム侵入ポリシーと組合わせることができます。
- 侵入ポリシーについて では、単純なカスタム侵入ポリシーを作成および編集する方法について説明します。
- 侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御には、親アクセス コントロール ポリシーに侵入ポリシーを関連付け、侵入ポリシーを使用して目的のトラフィックのみを検査するためのシステムの設定方法が記載されています。また、侵入ポリシーの高度なパフォーマンス オプションの設定方法も記載されています。
- ネットワーク分析ポリシーまたは侵入ポリシー レイヤでのレイヤの使用では、大規模な組織や複雑な展開環境で、ポリシー階層と呼ばれる構成要素を使用して、複数のネットワーク分析ポリシーや侵入ポリシーをより効率的に管理する方法が説明されています。

ポリシーが侵入の有無についてトラフィックをどのように検査するかについて

ライセンス：Protection

システムがアクセス コントロール展開の一部としてトラフィックを分析する際には、侵入防御（侵入ルールと詳細設定）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。

次の図は、インラインの侵入防御および高度なマルウェア防御（AMP）展開におけるトラフィック分析の順序を簡略的に示しています。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。



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 リスクを含んでいる可能性を示しています。

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方法に**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

ライセンス：Protection

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ってパターンマッチングを行えなくなるので、侵入についてシステムでトラフィックを適切に評価できなくなります。ポリシーが侵入の有無についてトラフィックをどのように検査するかについて （3 ページ）の図に示すように、ネットワーク分析ポリシーは、次のように、これらのトラフィック処理タスクを制御します。

- 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

- 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化し、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。
- 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。詳細については、
- 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、一致した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 ゾーンおよびネットワークに合わせてトラ

フィックの前処理オプションを調整できます。詳細については、システムによって提供されるポリシーとカスタム ポリシーの比較 （9 ページ）を参照してください。

表 *1*：復号化されたパケット

TCP/IP 層	復号化されたパケット
データ リンク	• イーサネット • 仮想ローカル エリア ネットワーク（VLAN） • マルチプロトコル ラベル スイッチング（MPLS）
ネットワーク	• Encapsulated Remote Switched Port Analyzer（ERSPAN）タイプ II、タイプ III • インターネット プロトコル バージョン 4（IPv4） • インターネット プロトコル バージョン 6（IPv6） • Internet Control Message Protocol バージョン 4（ICMPv4） • Internet Control Message Protocol バージョン 6（ICMPv6） • Point-to-Point Protocol (PPP) • Point-to-Point Protocol over Ethernet（PPPoE） • Generic Routing Encapsulation (GRE) • カプセル化セキュリティ プロトコル（ESP） • Teredo トンネリング • GPRS Tunneling Protocol（GTP）
トランスポート	• 伝送制御プロトコル（TCP） • ユーザ データグラム プロトコル（UDP）

アクセス コントロール ルール：侵入ポリシーの選択

ライセンス：Protection

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、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、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）。詳細については、カスタム ポリシーの制限 （14 ページ）を参照してください。

ポリシーが侵入の有無についてトラフィックをどのように検査するかについて （3 ページ）の図は、インラインの侵入防御および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 ルールによって、一致したトラフィックを続行できます。次にトラフィックは、ファイル ポリシーによって禁止ファイルとマルウェアについて検査され、侵入ポリシーによって侵入について検査されます。
- 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ので、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。詳細については、ルール アクションを使用したトラフィック処理とインスペクションの決定およびデフォルトの処理の設定およびネットワーク トラフィックのインスペクションを参照してください。

侵入インスペクション：侵入ポリシー、ルール、変数セット

ライセンス：Protection

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、VRT により作成された次のような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：コンパイルされているため変更できません（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：これは、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 デコーダの検出オプションに関連付けられるルールです。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たり、インライ展開で違反パケットをドロップするには、これらのルール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。

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、関連付けられた変数セットが使用されます。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、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を強く推奨します。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合わせることができます。詳細については、事前定義されたデフォルト変数の最適化を参照してください。

侵入イベントの生成

ライセンス：Protection

システムは侵入の可能性を特定すると、侵入イベントまたはプリプロセッサイベント（総称して「侵入イベント」とも呼ばれる）を生成します。このデータを表示して、ネットワーク アセットに対する攻撃についてさらに理解することができます。インライン展開では、システムは、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きます。

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。

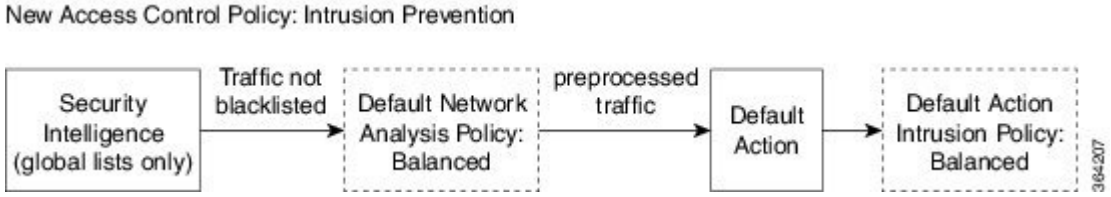
デバイスに侵入イベントが蓄積されると、ユーザは攻撃の可能性について分析を開始できます。システムは、ユーザが侵入イベントを確認し、ネットワーク環境とセキュリティ ポリシーのコンテキストでそのイベントが重要であるかどうかを評価するために必要なツールを提供します。

システムによって提供されるポリシーとカスタム ポリシーの比較

ライセンス：Protection

ASA FirePOWER モジュール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 ポリシーの作成です。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、システムによって提供される Balanced Security and Connectivity 侵入ポリシーによって判定された悪意のないすべてのトラフィックを許可します。
- 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（グローバルブロックなしリストとブロックリストのみ）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、アクセス制御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インスペクションを実行しません。

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。シスコでは ASA FirePOWER モジュールで、これらのポリシーのペアを複数提供しています。

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。

システムによって提供されるポリシーについて

ライセンス：Protection

シスコでは ASA FirePOWER モジュールで、ネットワーク分析ポリシーと侵入ポリシーのペアを複数提供しています。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と侵入ポリシーを使用することで、シスコ脆弱性調査チーム（VRT）の経験を活用できます。これらのポリシーに対して、VRT は侵入およびプリプロセッサ ルールの状態を設定し、プリプロセッサと他の詳細設定の初期設定も行います。システムによって提供されるポリシーをそのまま使用するか、またはカスタム ポリシーのベースとして使用できます。

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、ネットワーク環境を正確に反映するように、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、デフォルトセットの主要なデフォルト変数を変更してください（事前定義されたデフォルト変数の最適化を参照）。

新たな脆弱性が発見されると、VRT は侵入ルールのアップデートをリリースします。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。

ルールの更新によって展開が影響を受けると、システム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 ポリシーを失効とマークします。変更を有効にするには、更新されたポリシーを再適用する必要があります。

便宜を図るために、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、自動的に再適用するように、ルール アップデートを設定できます。これにより、展開を自動的に最新な状態に保ち、新たに検出されたエクスプロイトや侵入から保護することができます。

前処理の設定を確実に最新の状態にするには、アクセス コントロール ポリシーを再適用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 ポリシーが再適用され、高度な前処理とパフォーマンス オプションのデフォルト値も更新できます。詳細については、「ルール更新とローカル ルール ファイルのインポート」を参照してください。

シスコでは ASA FirePOWER モジュールで、次のネットワーク分析ポリシーと侵入ポリシーを提供しています。

[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。一緒に使用すると、ほとんどの組織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。

[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。

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詳細設定が無効化されます。このポリシーは、他のシステム付属ポリシーのいずれかで有効になっているルールに基づくのではなく、独自のポリシーを作成する場合の出発点となります。

注意 シスコでは、試験用に別のポリシー Experimental Policy 1 を使用しています。シスコの担当者から指示された場合を除き、このポリシーは使用しないでください。

カスタム ポリシーの利点

ライセンス：Protection

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や侵入ポリシーを効率的に管理するために使用できる基本構成要素です（ネットワーク分析ポリシーまたは侵入ポリシー レイヤでのレイヤの使用を参照）。

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ので、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ポリシーが影響を受けると、モジュールインターフェイスでは影響を受けたポリシーが失効とマークされます。詳細については、ルールアップデートによるシステム付属基本ポリシーの変更を許可するを参照してください。

カスタム ネットワーク分析ポリシーの利点

ライセンス：Protection

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はプリプロセッサが無効に設定されているものの、後にパケットを有効化されている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、自動的に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。

- 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、RPC トラフィックを復号化するポートを特定したりできます。

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。次に、システムがこれらのポリシーを使用し、異なるセキュリティ ゾーンまたはネットワークを使用してトラフィックの前処理を制御するように、システムを設定します。

（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**。詳細については、カスタム ポリシーの制限 （14 ページ）を参照してください。

カスタム侵入ポリシーの利点

ライセンス：Protection

侵入防御を実行するように設定されている、新規に作成されたアクセス コントロール 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、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。システムによって提供されるポリシーとカスタム ポリシーの比較 （9 ページ）の図を参照してください。

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、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。ポリシーが侵入の有無についてトラフィックをどのように検査するかについて （3 ページ）のシナリオは、トラフィックが 2 つの侵入ポリシーの一方によって検査される展開を示しています。

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。詳細については、ルール状態の設定を参照してください。
- 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。詳細については、侵入イベントの記録の制限を参照してください。

- 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。詳細については、ポリシー単位の侵入イベント通知のフィルタ処理を参照してください。
- 侵入イベントに加えて、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。詳細については、侵入ルールに関する外部アラートの設定を参照してください。

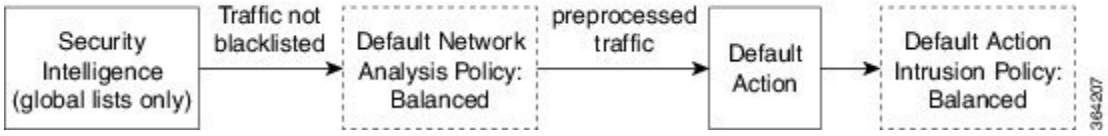
カスタム ポリシーの制限

ライセンス：Protection

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1つのネットワーク分析ポリシーを使用してすべてのトラフィックを前処理します。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。

New Access Control Policy: Intrusion Prevention



デフォルトのネットワーク分析ポリシーがアクセス コントロール ポリシーによって処理されるすべてのトラフィックの前処理を制御する仕組みに注目してください。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、カスタムネットワーク分析ポリシーを作成し、それをデフォルトとして使用することです（カスタム ネットワーク分析ポリシーの利点 （12 ページ）の概要を参照）。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、システムが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にして使用します。この場合、ネットワーク分析ポリシーの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。

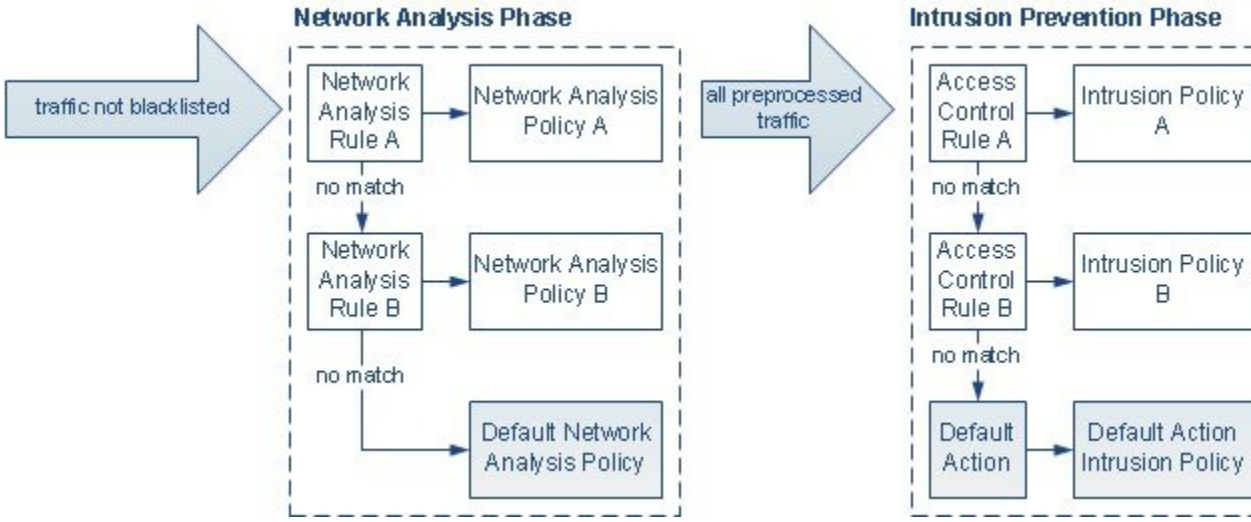
（注） プリプロセッサを無効化してパフォーマンスを向上させるには、どの侵入ポリシーでもプリプロセッサを要求するルールが有効になっていないことを確認する**必要があります**。

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 ゾーンおよびネットワーク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、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。ASA FirePOWER モジュール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、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ー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パケットを評価するように、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 パネルの使用方法

ライセンス：Protection

ネットワーク分析ポリシーと侵入ポリシーは、同様のユーザインターフェイスを使用して、設定に対する変更を編集して保存します。を参照してください。 侵入ポリシーの編集

いずれかのタイプのポリシーを編集するときに、ユーザ 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）と侵入ポリシー（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されているように、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 [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。詳細については、ルールを使用した侵入ポリシーの調整を参照してください。

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。詳細については、侵入ポリシーの詳細設定を参照してください。

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 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。詳細については、ネットワーク分析ポリシーまたは侵入ポリシー レイヤでのレイヤの使用を参照してください。

競合の解決とポリシー変更の確定

ライセンス：Protection

ネットワーク分析ポリシーまたは侵入ポリシーを編集する場合、変更をシステムに認識させるには、その変更を保存（またはコミット）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適用する必要があります。保存しないでポリシーを適用すると、最後に保存された設定が使用されます。侵入ポリシーは個別に再適用できますが、ネットワーク分析ポリシーは親アクセス コントロール ポリシーで適用されます。

編集の競合の解決

[Network Analysis Policy] ページおよび [Intrusion Policy] ページには、各ポリシーの未保存の変更の有無が表示されます。侵入ポリシーの編集を参照してください。

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。同一ユーザとして複数のユーザ 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ユーザ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。詳細については、カスタム ポリシーの制限 （14 ページ）を参照してください。
- 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す。システム キャッシュには、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。最初のポリシーに対する変更を保存せずに別のポリシーを編集した場合や、侵入ルールのアップデートをインポートした場合は、キャッシュされている変更が破棄されます。

ネットワーク分析ポリシーまたは侵入ポリシーのエディタの [Policy Information] ページで、ポリシーの変更をコミットまたは破棄できます。侵入ポリシーの編集を参照してください。

次の表は、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保存または破棄する方法を要約して示しています。

表 *2*: 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の確定

目的	**[Policy Information]** ページでは、次の操作を実行できます
ポリシーへの変更を保存する	[Commit Changes] をクリックします。 任意で、コメントを入力します。[OK] をクリックしてコミットを続行します。
すべての未保存の変更を破棄する	[Discard Changes] をクリックしてから [OK] をクリックし、変更を破棄して、[Intrusion Policy] ページに移動します。変更を破棄しない場合は、[Cancel] をクリックして [Policy Information] ページに戻ります。
ポリシーを終了し、変更をキャッシュする	任意のメニューまたは別のページへの他のパスを選択します。終了時に、表示されたプロンプトで[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）] をクリックして高度なエディタに残ります。