侵入防御の概要

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と防御のため、FireSIGHT システムを展開できます。*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、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。

FireSIGHT システムは、以下の設定に応じて、侵入検知システムとしても侵入防御システムとしても機能します。

- 管理対象デバイスをネットワークに接続する方法：インラインラインまたはアウトオブバンド
- デバイスのインターフェイス セットを設定する方法：パッシブ、インライン、スイッチド、またはルーテッド
- [Drop and Generate Events] に設定されたルールのドロップ動作：有効または無効

デバイスが展開され、ニーズに合わせて設定された後に、FireSIGHT システムは複数のメカニズムを使用して、攻撃者が開発したさまざまなエクスプロイトを見つけようとします。その後、さまざまなツールを使用して、侵入イベントを分析し、それに対応することができます。

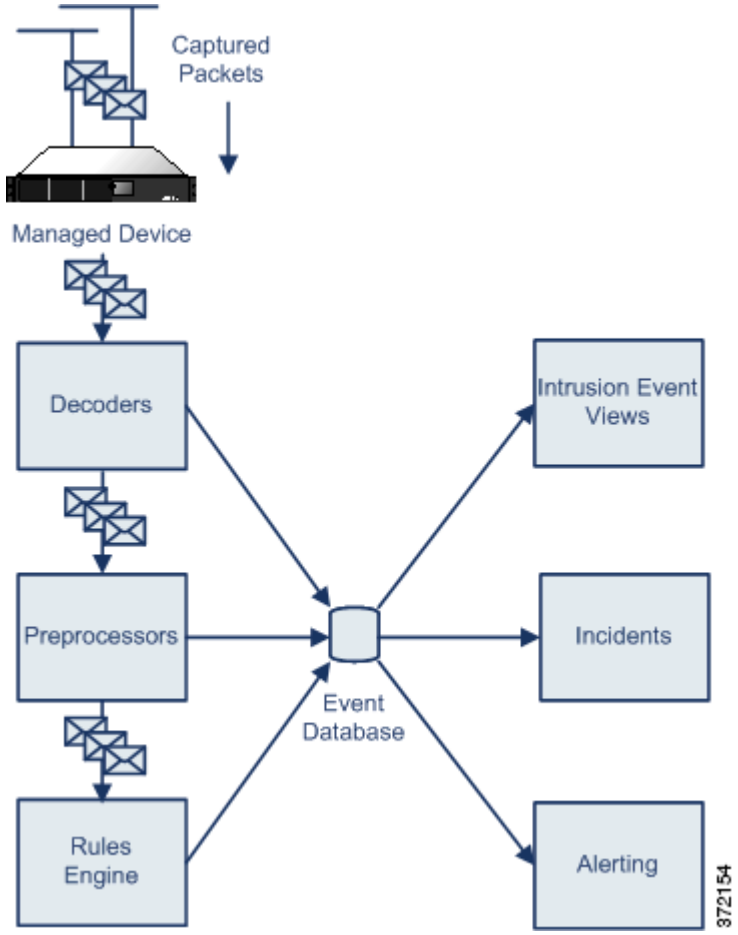
侵入の検知

パケット デコーダとプリプロセッサは、侵入の試みを示す可能性のある異常なトラフィックを検出し、付随するデコーダとプリプロセッサのルールが有効にされている場合は、検出された異常をレポートします。次に、復元化されたパケットを侵入ルールが検査し、パターンに基づいて攻撃を検出します。侵入ルールとプリプロセッサを同時に使用すると、シグニチャベースのシステムよりも広範囲で詳細なパケット インスペクションが提供され、より効果的に侵入を識別するために役立ちます。

シスコの脆弱性調査チーム（VRT）は、シスコ ルール アップデートと呼ばれる、新しい侵入ルールを含めることができるアップデートを定期的に発行して、最近リリースされた攻撃が常に検知の対象となるようにします。

侵入への対応

パケットがセグメントを通過するとき、管理対象デバイスは一連のデコーダとプリプロセッサ、そしてその後にルール エンジン使用して、そのパケットを収集して分析します。デバイスは侵入の可能性を識別すると、*侵入イベント*を生成します。これは、エクスプロイトの日付、時刻、タイプ、および攻撃のターゲットとソースに関するコンテキスト情報を示すデータです。デバイスがパッシブ展開されている場合を除いて、システムは可能性のある侵入をブロックしたり、パケット内の有害なコンテンツを置き換えたりすることができます。パケットベースのイベントの場合、イベントをトリガーしたパケットのコピーも記録されます。



FireSIGHT システムの展開がネットワークの保護にどのように役立つかについての詳細は、以下の項を参照してください。

- 「トラフィックを分析する方法について」（P.17-3）
- 「侵入イベント データの分析」（P.17-7）
- 「侵入イベントの応答の使用」（P.17-7）
- 「侵入防御の展開について」（P.17-8）
- 「カスタム侵入ポリシーの利点」（P.17-10）

トラフィックを分析する方法について

ライセンス：Protection

システムは、受賞歴のある Snort® テクノロジーを使用して、ネットワーク トラフィックを分析し、侵入イベントを生成します。これは、特定のネットワーク セグメントをモニタするデバイスに適用される侵入ポリシーに違反したトラフィックの記録です。イベント アナリストは、イベントを確認して、それらがネットワークの観点から重要かどうかを判別できます。

侵入イベントは、以下から生成できます。

- Ethernet II デコーダなど、リンク層のデコーダ
- IP デコーダなど、ネットワーク層のデコーダ
- TCP デコーダなど、トランスポート層のデコーダ
- HTTP Inspect プリプロセッサなど、アプリケーション層デコーダまたはプリプロセッサ
- ルール エンジン

イベントには、以下のような情報が含まれます。

- イベントが生成された日時
- イベントの優先順位
- ネットワーク検出を使用するとき、イベントに関連付けられた影響フラグ
- インライン展開、スイッチド展開、またはルーテッド展開で、イベントを発生されたパケットがドロップしたかどうか、またはドロップする可能性があったかどうか
- イベントを生成したデバイスの名前
- イベントを発生させたパケットのプロトコル
- イベントの送信元 IP アドレスおよびポート
- イベントの宛先 IP アドレスおよびポート
- 送信元ホストにログインしたユーザの名前
- ICMP のタイプとコード（ICMP トラフィックの場合）
- イベントを生成した FireSIGHT システム コンポーネント（ルール、デコーダ、プリプロセッサなど）
- イベントの簡単な説明
- イベントを生成したルールの分類
- ホストがメンバーとなっている VLAN

侵入イベントに含まれる情報の完全なリストと説明については、「侵入イベントについて」（P.18-8）を参照してください。

注　共有オブジェクト ルールによって生成されたイベントの場合、ルール自体が使用可能ではありません。

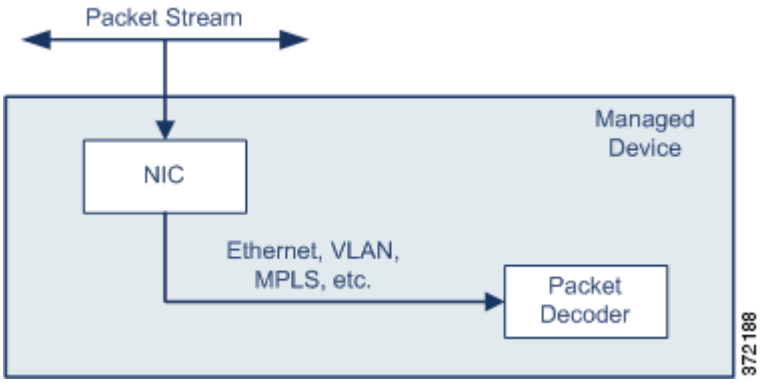
以下の項では、システムが情報を取得して処理する方法について詳しく説明します。

- 「パケットの検出と復号化」（P.17-4）
- 「パケットの処理」（P.17-5）
- 「イベントの生成」（P.17-6）

パケットの検出と復号化

ライセンス：Protection

パケットを検査する前に、パケットをネットワークから検出する必要があります。次の図では、どのようにシステムがパケットをスニファで取り込み、さらに分析する前に復号化するかを示しています。



システムはパケットを検出すると、それらをパケット デコーダに送信します。パケット デコーダは、パケット 見出しやペイロードを、プリプロセッサやルール エンジン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は、次の表で説明されているように、データリンク層から開始してネットワーク層とトランスポート層へと、交互に復号化されます。

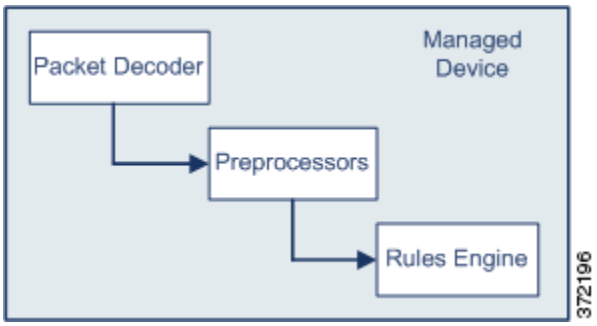
表 17-1　復号化されたパケット

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） • ポイントツーポイント プロトコル（PPP） • Point-to-Point Protocol over Ethernet（PPPoE） • 総称ルーティング カプセル化（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 トンネリング プロトコル（GTP）
トランスポート	• Transmission Control Protocol（TCP） • ユーザ データグラム プロトコル（UDP）

パケットの処理

ライセンス：Protection

パケットは、最初の 3 つの TCP/IP 層によって復号化された後、プリプロセッサに送られます。そこでは、アプリケーション層でトラフィックが標準化されて、プロトコルの異常が検出されます。プリプロセッサを通過した後、パケットはルール エンジンに送られます。ルール エンジンは、パケット 見出しやペイロードを検査して、それらによって共有オブジェクト ルールや標準テキスト ルールがトリガーされるかどうかを判別します。



使用する環境に適するように、プリプロセッサやプリプロセッサ オプションを有効または無効にすることができます。たとえば、プリプロセッサの 1 つは HTTP トラフィックを正規化します。ネットワークはに Microsoft Internet Information Services（IIS）を使用する Web サーバが含まれ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して、システム処理のオーバーヘッドを軽減できます。

ルール エンジンは、プリプロセッサからのパケットを検査する際に、以下の 3 つのトラックを必要とします。

- ルール オプティマイザ
- マルチルール検索エンジン
- イベント セレクタ

プリプロセッサの詳細については、「侵入ポリシーの詳細設定の使用」（P.22-1）を参照してください。

ルール オプティマイザは、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の基準に基づいて、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。パケットがルール エンジンに着信すると、各パケットに適用する適切なルールのサブセットが選択されます。

ルールのサブセットが選択された後に、マルチルール検索エンジンが、以下のように 3 つの異なる種類の検索を実行します。

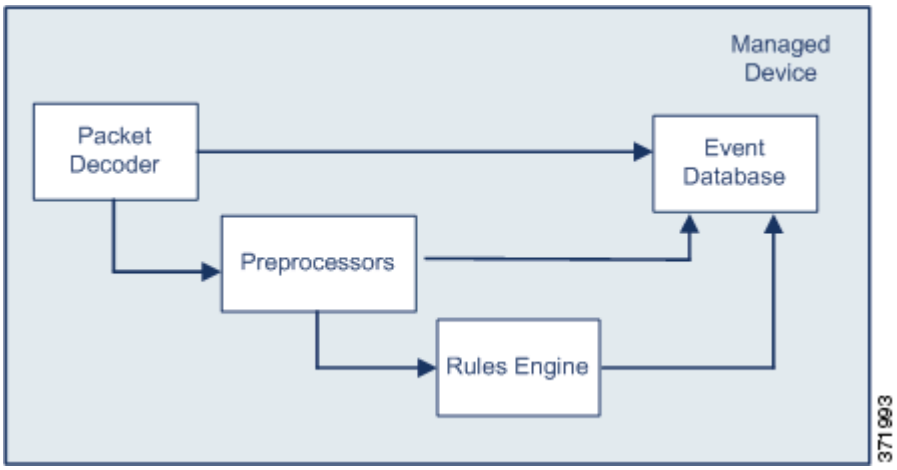
- プロトコル フィールド検索は、アプリケーション プロトコル内の特定のフィールドでの一致を検索します。
- 汎用コンテンツ検索は、パケット ペイロードの ASCII またはバイナリ バイトでの一致を検索します。
- パケット異常検索は、特定のコンテンツを含むかどうかではなく、確立されたプロトコルに違反しているパケット 見出しやペイロードを検索します。

マルチルール検索エンジンは、パケットを検査した後に、トリガーされたすべてのルールに対してイベントを生成してイベント キューに追加します。イベント セレクタは、キュー内のイベントに優先順位を付け、イベント データベースにイベントをロギングします。これらは、侵入イベント統計情報および侵入イベント レポートに示される侵入イベントです。

イベントの生成

ライセンス：Protection

パケットは、パケット デコーダ、プリプロセッサ、およびルール エンジンによって評価されます。プロセスの各ステップで、パケットはシステムにイベントを生成させることができます。これは、パケットやそのコンテンツがネットワークのセキュリティに対するリスクとなる可能性があること、または自分のネットワーク内から攻撃が発生する場合には、自分のネットワークか外部ネットワークのどちらかのセキュリティに対するリスクとなる可能性があることを示しています。



たとえば、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）より小さい IP パケットを受け取ると、デコーダはこれを異常なトラフィックと解釈して、付随するデコーダ ルールが有効なときにはイベントを生成します。同様に、前処理ステップで、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 ルールが有効なときにはイベントを生成します。同じ種類の反応は、ほとんどのルールがパケットによってトリガーされるとイベントを生成するように記述されている、ルール エンジン内でも生じます。

データベース内の各イベントには、攻撃の可能性に関する 2 つの情報ソースが含まれています。1 つ目はイベント 見出しと呼ばれ、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付と時刻に関する情報を含んでいます。2 つ目はパケット ログで、復号化されたパケット 見出しとパケット ペイロードのコピーを含んでいます。

侵入イベント データの分析

ライセンス：Protection

システムが侵入イベントを蓄積しているとき、ユーザは攻撃の可能性の分析を開始できます。FireSIGHT システムには、侵入イベントを検討し、それらがネットワーク環境やセキュリティ ポリシーの観点から重要かどうかを評価するために必要なツールが備わっています。これらのツールは次のとおりです。

- 管理対象デバイスの現在のアクティビティの概要を示す、[Intrusion Event Statistics] ページ

  詳細については、「侵入イベントの統計の表示」（P.18-2）を参照してください。
- 選択した任意の期間を対象に生成できる、テキストベースのレポートやグラフィカル レポート。ユーザが独自のイベント レポートを設計して、それらがスケジュールされた間隔で実行されるように設定することもできます。

  詳細については、「レポートの操作」（P.44-1）を参照してください。
- 攻撃に関連したイベントやパケット データの収集に使用できる、インシデント処理ツール。調査と対応のトラッキングに役立つように、注釈を追加することもできます。

  詳細については、「インシデント対応」（P.19-1）を参照してください。
- 侵入イベントをドリルダウンして、さらに調査するイベントを識別するために使用可能な、定義済みのワークフローとカスタム ワークフロー

  詳細については、「ワークフローの概要と使用」（P.47-1）および「侵入イベントの操作」（P.18-1）を参照してください。

侵入イベントの応答の使用

ライセンス：Protection

攻撃に基づいて侵入イベントを生成することに加えて、アラート メカニズムの広範なリストを使用し、特定の攻撃についてはユーザに即時に通知されるようにすることができます。反対に、重要なシステムに影響を与える可能性が小さいイベントを抑制することや、アラートが出される前に到達する必要のあるイベント数を示すしきい値を設定することもできます。

自動アラートの詳細については、「侵入ルールの外部アラートの設定」（P.31-1）を参照してください。

以下のツールを使用して、侵入イベントに対する自動応答をセットアップできます。

- SNMP、電子メール、および Syslog 用に設定できる自動アラート

  詳細については、「侵入ルールの外部アラートの設定」（P.31-1）を参照してください。
- 防御センターで、特定の侵入イベントに応答してそれを修復するために使用できる、自動化された相関ポリシー

  詳細については、「修復の設定」（P.41-1）を参照してください。

侵入防御の展開について

ライセンス：Protection

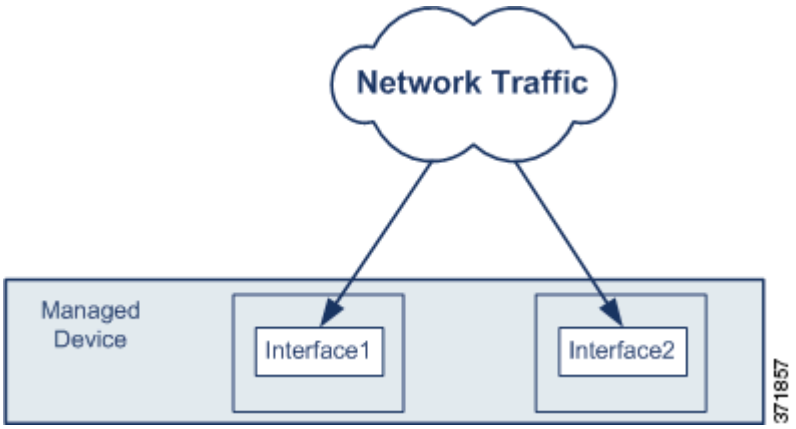
管理対象デバイスにパッシブ展開を設定して、デバイスが、パケット ストリームからアウトオブバンド トラフィックを検知するようにできます。同様に、インライン展開、スイッチド展開、またはルーテッド展開を設定して、侵入ポリシーを使用してパケットをドロップするように設定することにより、損害を与えることが知られているパケットをドロップまたは置換できます。

管理対象デバイスごとに侵入ポリシーをカスタマイズして、ネットワークの特定の部分にあるホストのセキュリティに影響を与える可能性のある攻撃に対してのみ、イベントを生成することができます。どのルールがアラートを出さないか、どのルールがイベントを生成するか、そしてパッシブ展開以外の場合には、どのルールがイベントを生成すると共に悪意のあるトラフィックをドロップするかを指定できます。

どのタイプのシステムの場合でも、センシング インターフェイスをネットワークの適切なセグメントに接続して、それらのインターフェイスをインターフェイス セットに追加します。これらのインターフェイスはステルス モードに設定されているので、ネットワーク上の他のデバイスからは、そのデバイス自体がネットワークにまったく接続されていないように認識されます。また、インターフェイスは無差別モードで設定されているので、トラフィックの宛先には関係なく、ネットワーク セグメントのすべてのトラフィックを検出します。この設定で、デバイスはネットワーク セグメントのトラフィックをすべて認識できますが、そのデバイス自体は表示されません。

アウトオブバンド展開とインライン展開、スイッチド展開、またはルーテッド展開との、展開としての主な違いは、各システムで使用されるインターフェイス セットに基づくものです。アウトオブバンド展開はパッシブ インターフェイス セットを使用しますが、インライン展開、スイッチド展開、またはルーテッド展開はインライン セットを使用します。パッシブ インターフェイス セットのインターフェイスは、インライン セットのインターフェイス ペア間をトラフィックがフローする際に、モニタ対象のセグメントのトラフィックを受動的に分析します。

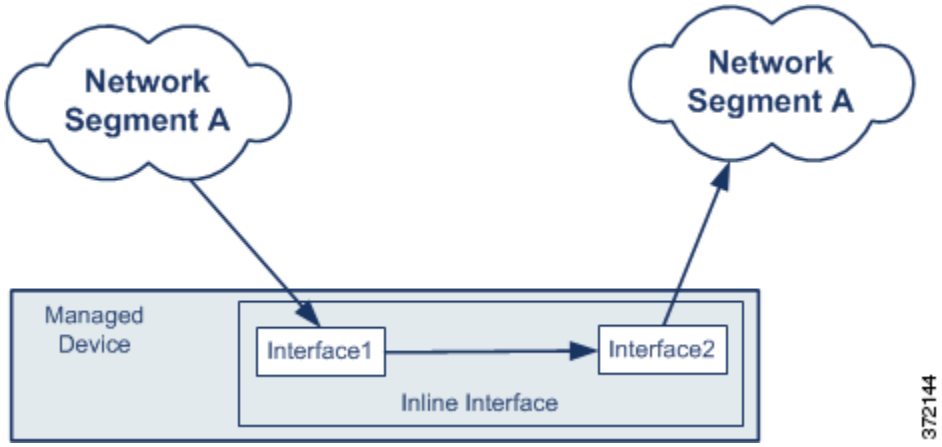
次の図に、2 つのパッシブ インターフェイス セットと共に、パッシブ展開された管理対象デバイスの例を示します。各インターフェイスは、異なるネットワーク セグメントをモニタします。



アウトオブバンドのトラフィックを検知することにより、デバイスの検知用の帯域幅と計算能力のほぼすべてを、トラフィックのモニタリング、データグラムとストリームの再構成、パケットの標準化、異常の検出、および侵入の可能性のアラートに使用することができます。さらに、インターフェイスがアウトオブバンドで展開され、ステルス モードで稼動しているので、攻撃者がその存在を認識することはほぼなくなり、攻撃のターゲットとなる可能性は小さくなります。

それと比較してインライン展開では、インライン インターフェイス セットを使用する管理対象デバイスを設定します。これを行うには、デバイスをネットワークに接続して、デバイスのネットワーク インターフェイス間でトラフィックがフローするようにします。インターフェイス セットがインラインとして設定されている場合、インターフェイスは無差別モードにも設定されるので、トラフィックの宛先には関係なく、ネットワーク セグメントのすべてのトラフィックが検出されます。デバイスはネットワーク セグメントのトラフィックをすべて認識できますが、そのデバイス自体は表示されません。ただし、インターフェイス セットがインラインで展開されている場合、疑わしいパケットをドロップしたり、カスタムの標準テキスト ルールでは、パケット ペイロードの悪意のある部分をより無害なコンテンツで置き換えたりするルールを設定できます。

たとえば、次の図はインラインで展開されたデバイスを示します。デバイスは、単一のネットワーク セグメントをモニタする 2 つのネットワーク インターフェイスを含む、インターフェイス セットを使用します。



パッシブ インターフェイス セットを使用するデバイスと同様に、インライン インターフェイス セットを使用するデバイスは、トラフィックの宛先には関係なく、インターフェイス セット内のインターフェイスをパススルーするトラフィックすべてを認識できます。ただし、トラフィックはインターフェイス間をフローするので、ユーザは疑わしいパケットを変更したりブロックしたりできます。たとえば、ネットワークが攻撃される可能性のある既知のエクスプロイトがペイロードに含まれているパケットが、デバイスによって検出された場合、そのパケットをドロップするようにシステムを設定できます。この場合、悪意のあるパケットは、意図されたターゲットに到達しません。

インライン展開では、ペイロードの一部を独自に選択したコンテンツに置き換えることもできます。デバイスが `bin/sh` を含むパケット（shellcode 攻撃を示す場合が多い）を検出する簡単な例を検討します。この文字列の全部または一部を正確に同じ文字数で置き換える、カスタムの侵入ルールを作成することができます。たとえば、`bin/sh` を `foo/sh` に置き換えてからパケットを宛先に送ると、shellcode 攻撃は失敗し、パケットが変更されたことは攻撃者に知られません。

この結果を、同じトラフィックが受動的に検査された場合の結果と比較してください。このシナリオでは、同じルールによってエクスプロイトが検出されますが、パケットをドロップするオプションはなく、その存在をアラートすることだけが可能です。

侵入からの保護と防御を展開することの利点を検討する際には、そのトレードオフとなるものについても評価する必要があります。まず、ネットワーク セグメントのトラフィックと同等以上の帯域幅に対応した管理対象デバイスのモデルを選択する必要があります。また、ネットワーク セグメントのホストの重要度に応じて、オプションのバイパス ネットワーク カードと共に管理対象デバイスを展開することを検討する必要があります。バイパス カードにより、ア

プライアンス自体で障害が生じた場合や電源が失われた場合でも、トラフィックは引き続きインターフェイスをパススルーできるようになります（ただしアプライアンスをリブートする際に少数のパケットは失われる可能性があります）。インライン セットの詳細については、「インライン セットの設定」（P.7-5）を参照してください。展開のオプションの詳細については、管理対象デバイスのインストレーション ガイド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

システムには、パッシブ展開とインライン展開の両方に適したデフォルトの侵入ポリシーが備わっています。ただし、それらのポリシーに設定されたルール、プリプロセッサ オプション、その他の詳細設定は、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。詳細設定とルールを有効にしたり、無効にしたり、それらに特定の設定オプションを指定したりすることで、ポリシーを*調整*できます。詳細設定とルール セット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および検査する方法を非常にきめ細かく設定できます。

たとえば、侵入ポリシーは、プリプロセッサを調整するための以下の方法を提供します。

- モニタしているサブネットの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。
- 必要に応じて、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。
- パケット内で特定の特徴（状態の問題や TCP フラグの特定の組み合わせなど）が検出されたとき、プリプロセッサがイベントを生成するように設定します。
- ネットワーク検出との組み合わせで適応型プロファイルを設定し、ネットワーク検出マップからホストのオペレーティング システムに関する情報を使用して、IP の最適化と TCP ストリームの前処理に最適なターゲットプロファイルに切替えます。

使用可能な調整オプションは、プリプロセッサやその他の詳細設定によって異なることに注意してください。使用可能な詳細設定、それらのオプション、およびそれらによる調整方法の詳細については、「侵入ポリシーの詳細設定の使用」（P.22-1）を参照してください。

さらに、各侵入ポリシー内で、以下のようにしてルールを調整できます。

- 使用するルールの数を減らしてパフォーマンスを改善します。環境に適用できないルールは無効にします。
- 環境に適用可能なルールはすべて有効であることを確認します。
- インライン展開では、どのルールがパケット ストリームから悪意のあるパケットをドロップするかを指定します。

ヒント　ネットワーク検出を使用して、ネットワーク上のオペレーティング システムを識別できます。これにより、どのルールが環境に適用可能であるかをより簡単に識別できます。

侵入ポリシー内で抑制レベルとしきい値を設定して、侵入イベントの通知を受ける頻度を制御することもできます。イベント通知の抑制、および個別のルールまたは侵入ポリシー全体に対するしきい値の設定は選択できます。詳細については、「パケット ビュー内でのしきい値オプションの設定」（P.18-28）、「パケット ビュー内での抑制オプションの設定」（P.18-29）、「ポリシー単位の侵入イベント通知のフィルタ処理」（P.21-25）を参照してください。

システムによって実行されたプロトコル分析、データの正規化、およびトラフィック検査を指定して、この設定全体を保存することにより、エンタープライズ セキュリティのニーズが最もよく満たされるように、ユーザに提供される情報の種類を制御することができます。これはまた、新しい攻撃やエクスプロイトを検出し続けるために、必要な数（多くても少なくても）のポリシーを変更するための簡単なメカニズムを提供します。

また、以下の方法でルールを調整することもできます。

- 必要に応じて、ルール エディタを使用して既存のルールを変更し、ネットワーク インフラストラクチャに対応するようにします。
- 必要に応じて Snort 言語とルール エディタを使用して新しい標準テキスト ルールを作成し、新しいエクスプロイトを検出したりセキュリティ ポリシーを適用したりします。

ルールのキーワード、引数、シンタックス、およびルール セットの調整方法の詳細については、「侵入ルールの概要と作成」（P.32-1）を参照してください。