インライン正規化プリプロセッサの有効化とACK 前および ACK 後検査について

内容

はじめに

このドキュメントでは、インライン正規化プリプロセッサを有効にする方法について説明し、インライン正規化の2つの高度なオプションの違いと影響を理解するのに役立ちます。

前提条件

要件

Cisco FirepowerシステムとSnortに関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、Cisco FireSIGHT Management CenterおよびFirepowerアプライアンスに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

インライン正規化プリプロセッサは、インライン展開を使用して攻撃者が検出を回避できる可能性を最小限に抑えるために、トラフィックを正規化します。正規化は、パケットのデコード直後

に他のプリプロセッサの前に行われ、パケットの内部層から外部に向かって進みます。インライン正規化ではイベントは生成されませんが、他のプリプロセッサで使用できるようにパケットが準備されます。

インライン正規化プリプロセッサが有効になっている状態で侵入ポリシーを適用すると、Firepowerデバイスはインライン展開を使用していることを確認するために次の2つの条件をテストします。

- バージョン5.4以降では、ネットワーク分析ポリシー(NAP)でインラインモードが有効になっており、侵入ポリシーがトラフィックをドロップするように設定されている場合、侵入ポリシーでインライン時のドロップも設定されています。バージョン5.3以前では、侵入ポリシーでDrop when Inlineオプションが有効になっています。

- ポリシーは、インライン（またはfailopenを使用したインライン）インターフェイスセットに適用されます。

したがって、インライン正規化プリプロセッサの有効化と設定に加えて、次の要件が満たされていることを確認する必要があります。満たされていない場合、プリプロセッサはトラフィックを正規化しません。

- インライン展開では、トラフィックをドロップするようにポリシーを設定する必要があります。

- ポリシーをインラインセットに適用する必要があります。

インライン正規化の有効化

このセクションでは、バージョン5.4以降およびバージョン5.3以前でインライン正規化を有効にする方法について説明します。

バージョン5.4以降でインライン正規化を有効にする

プリプロセッサ設定のほとんどは、バージョン5.4以降のNAPで構成されます。NAPでインライン正規化を有効にするには、次の手順を実行します。

1. FireSIGHT Management CenterのWeb UIにログインします。

2. [Policies] > [Access Control] に移動します。

3. ページの右上の領域にあるNetwork Analysis Policyをクリックします。

4. 管理対象デバイスに適用するネットワーク分析ポリシーを選択します。

5. 鉛筆アイコンをクリックして編集を開始すると、Edit Policyページが表示されます。

6. 画面の左側にあるSettingsをクリックすると、Settingsページが表示されます。

7. Transport/Network Layer Preprocessor領域でInline Normalizationオプションを見つけます。

8. この機能をイネーブルにするには、Enabledオプションボタンを選択します。

インライン正規化が行われるようにするには、インライン正規化を使用するNAPをアクセスコントロールポリシーに追加する必要があります。NAPは、アクセスコントロールポリシーのAdvancedタブから追加できます。

その後、アクセス制御ポリシーを検査デバイスに適用する必要があります。

注：バージョン5.4以降では、特定のトラフィックに対してインライン正規化を有効にし、他のトラフィックに対してそれを無効にすることができます。特定のトラフィックに対して有効にする場合は、ネットワーク分析ルールを追加し、トラフィック基準とポリシーをインライン正規化が有効になっているものに設定します。グローバルに有効にする場合は、デフォルトのネットワーク分析ポリシーをインライン正規化が有効になっているポリシーに設定します。

バージョン5.3以前でインライン正規化を有効にする

侵入ポリシーでインライン正規化を有効にするには、次の手順を実行します。

1. FireSIGHT Management CenterのWeb UIにログインします。

2. Policies > Intrusion > Intrusion Policiesの順に移動します。

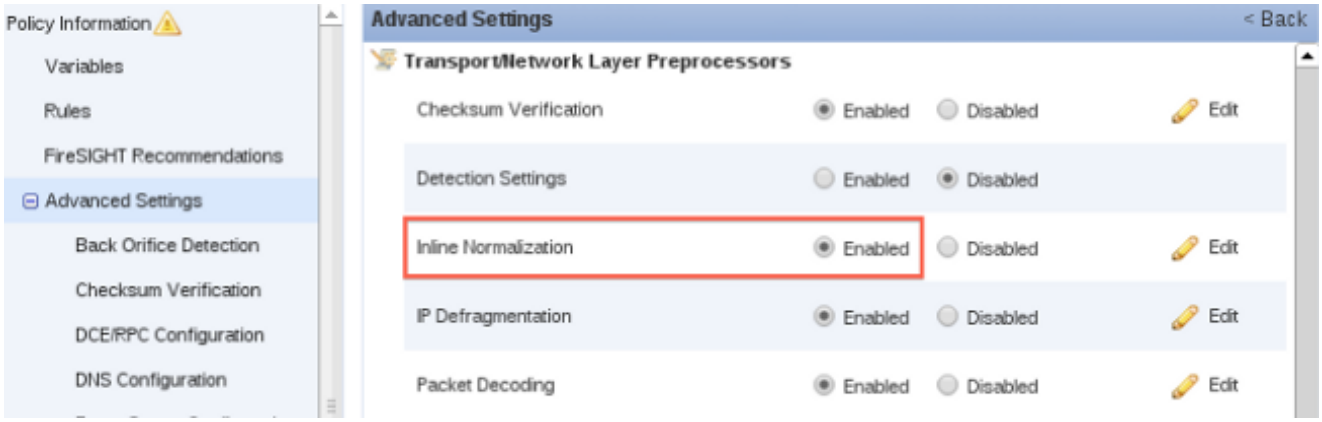
3. 管理対象デバイスに適用する侵入ポリシーを選択します。

4. 鉛筆アイコンをクリックして編集を開始すると、Edit Policyページが表示されます。

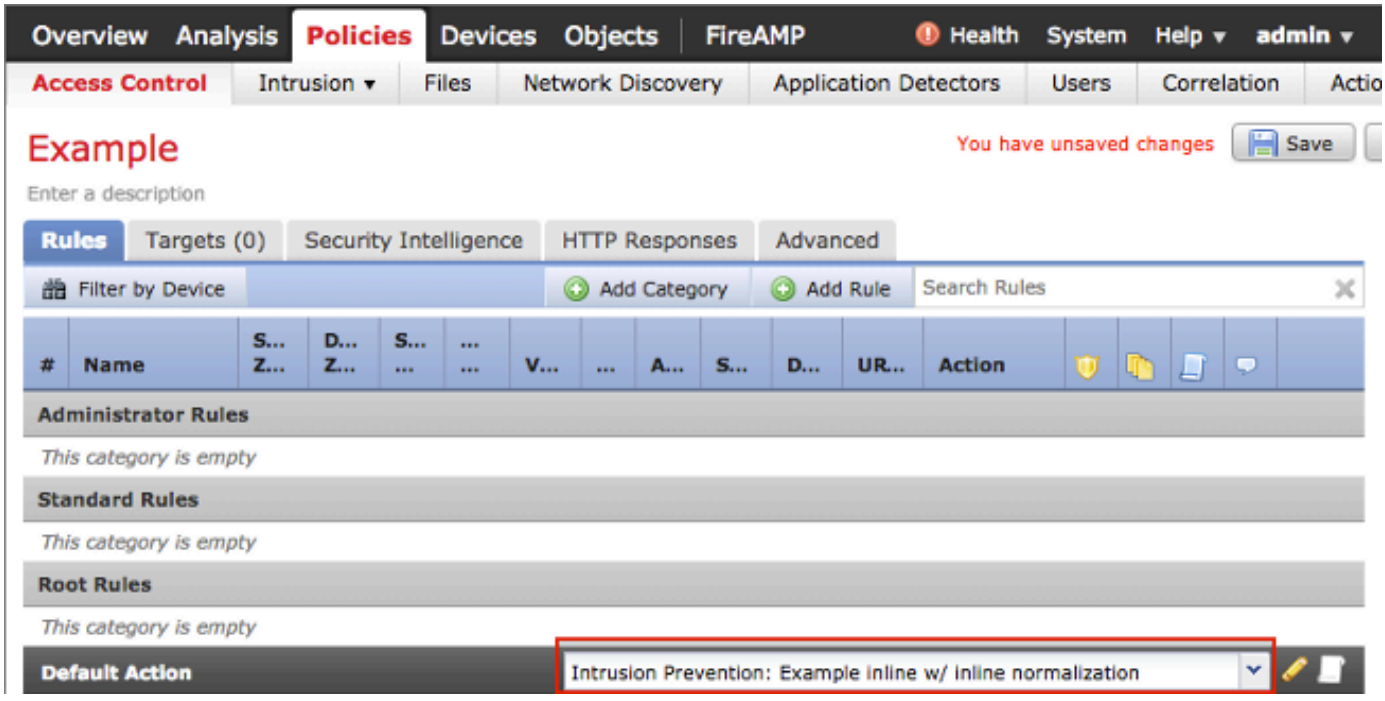
5. Advanced Settingsをクリックすると、Advanced Settingsページが表示されます。

6. Transport/Network Layer Preprocessor領域でInline Normalizationオプションを見つけます。

7. この機能をイネーブルにするには、Enabledオプションボタンを選択します。



インライン正規化用に設定した侵入ポリシーは、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として追加する必要があります。



その後、アクセス制御ポリシーを検査デバイスに適用する必要があります。

IPv4、IPv6、Internet Control Message Protocol Version 4(ICMPv4)、ICMPv6、およびTCPトラフィックを任意の組み合わせで正規化するために、インライン正規化プリプロセッサを設定できます。各プロトコルの正規化は、そのプロトコルの正規化が有効になったときに自動的に行われます。

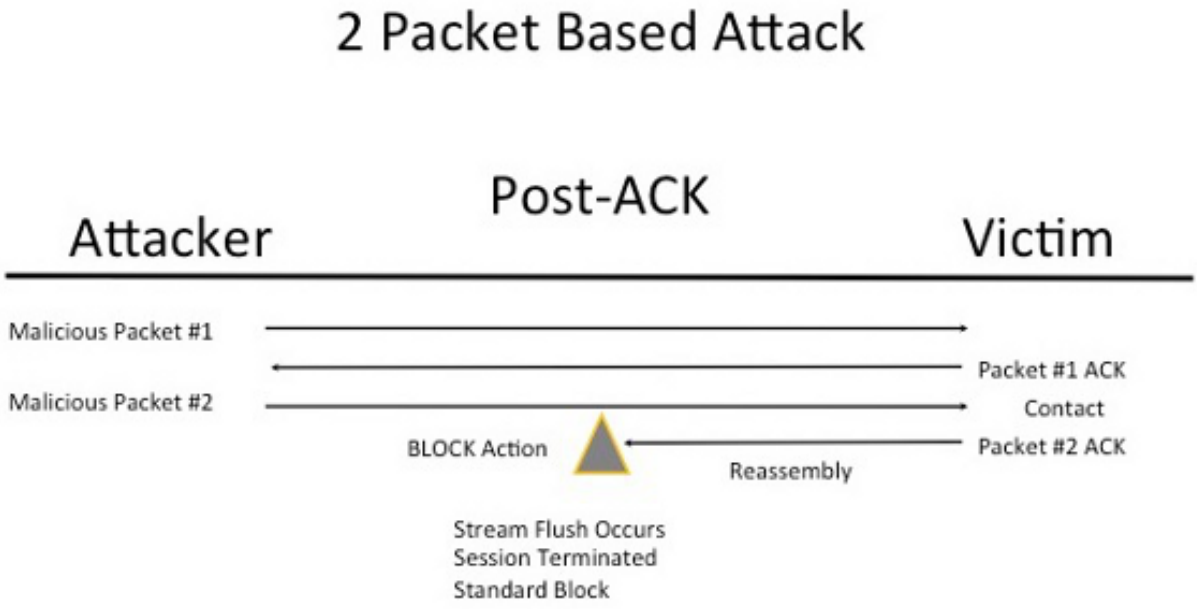
Post-ACKインスペクションとPre-ACKインスペクションの有効化

インライン正規化プリプロセッサを有効にした後、Normalize TCP Payloadオプションを有効にするために設定を編集できます。インライン正規化プリプロセッサのこのオプションは、2つの異なる検査モードを切り替えます。

- 確認応答後（ACK後）
- 事前確認応答(Pre-ACK)

Post-ACKインスペクションについて(「Normalize TCP/Normalize TCP Payload Disabled」)

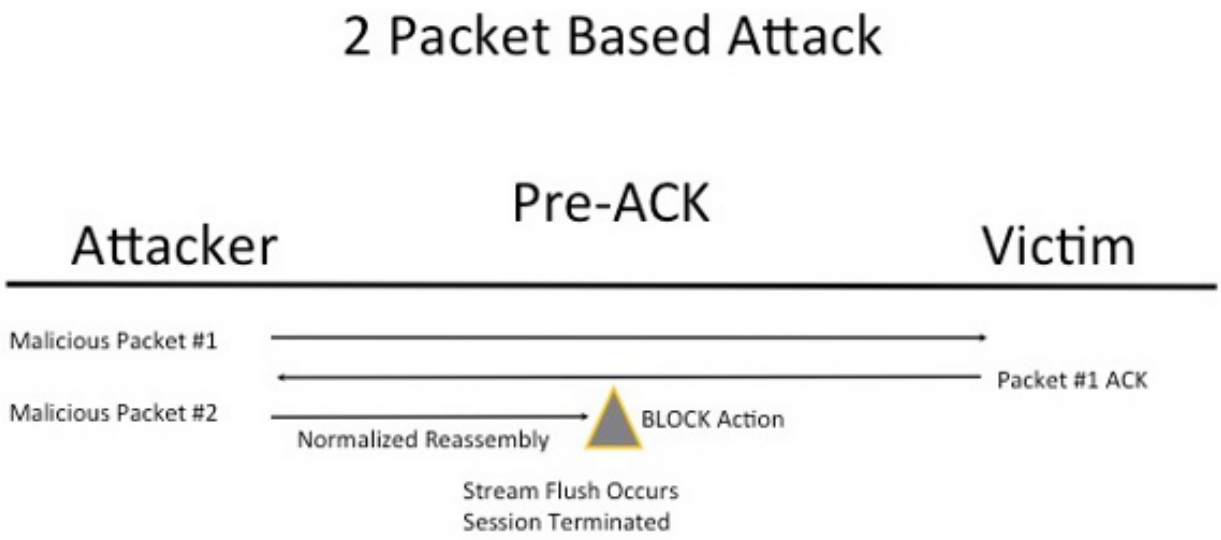
Post-ACKインスペクションでは、攻撃を完了したパケットに対する被害者からの確認応答(ACK)が侵入防御システム(IPS)によって受信された後に、パケットストリームの再構成、フラッシュ（検査プロセスの残りの部分へのハンドオフ）、およびSnortでの検出が行われます。ストリームのフラッシュが発生する前に、攻撃パケットはすでに攻撃対象に到達しています。したがって、アラート/ドロップは、攻撃パケットが被害者に到達した後に発生します。このアクションは、攻撃パケットに対する標的からのACKがIPSに到達すると発生します。



Pre-ACKインスペクションについて（TCPの正規化/TCPペイロードの正規化が有効）

この機能は、TCP回避の労力を最小限に抑えるために、パケットのデコード直後、および他のSnort機能が処理される前にトラフィックを正規化します。これにより、IPSに到達するパケット

が被害者に渡されるパケットと同じであることが保証されます。Snortは、攻撃が被害者に到達する前に攻撃を完了したパケットのトラフィックをドロップします。



Normalize TCPを有効にすると、次の条件に一致するトラフィックもドロップされます。

- 以前にドロップされたパケットのコピーを再送信
- 以前にドロップされたセッションを継続しようとするトラフィック
- 次のTCPストリームプリプロセッサのルールのいずれかに一致するトラフィック：
  - 129:1
  - 129:3
  - 129:4
  - 129:6
  - 129:8
  - 129:11
  - 129:14 ~ 129:19

注：正規化プリプロセッサによって廃棄されるTCPストリームルールのアラートを有効にするには、TCPストリーム設定のステートフル検査の異常機能を有効にする必要があります。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。