



パッシブ展開における前処理の調整

通常、システムはネットワーク分析ポリシーの静的な設定を使用して、トラフィックの前処理と分析を行います。ただし、適応型プロファイル機能により、トラフィックを得られるホスト情報と関連付けそれに応じてトラフィックを処理することにより、システムはネットワークトラフィックに対応できます。

ホストがトラフィックを受信すると、ホストで実行されているオペレーティングシステムはIPフラグメントを再構成します。再構成に使用する順序は、オペレーティングシステムによって異なります。同様に、各オペレーティングシステムはさまざまな方法でTCPを実装することがあるため、TCPストリームの再構成の方法も異なる可能性があります。プリプロセッサが宛先ホストのオペレーティングシステムで使用されているものとは異なる形式を使用してデータを再構成すると、受信ホストでの再構成時に悪意のある可能性があるコンテンツをシステムが見逃す可能性があります。



ヒント

パッシブ展開の場合、シスコでは、適応型プロファイルを設定することを推奨しています。インライン展開の場合、シスコでは、インライン正規化プリプロセッサの設定で[TCPペイロードの正規化(Normalize TCP Payload)]オプションを有効にすることを推奨しています。詳細については、[インライントラフィックの正規化\(21-6 ページ\)](#)を参照してください。

適応型プロファイルを使用したパケットフラグメントとTCPストリームの再構成の改善に関する詳細については、次のトピックを参照してください。

- [適応型プロファイルについて\(22-1 ページ\)](#)
- [適応型プロファイルの設定\(22-3 ページ\)](#)

適応型プロファイルについて

ライセンス:Protection

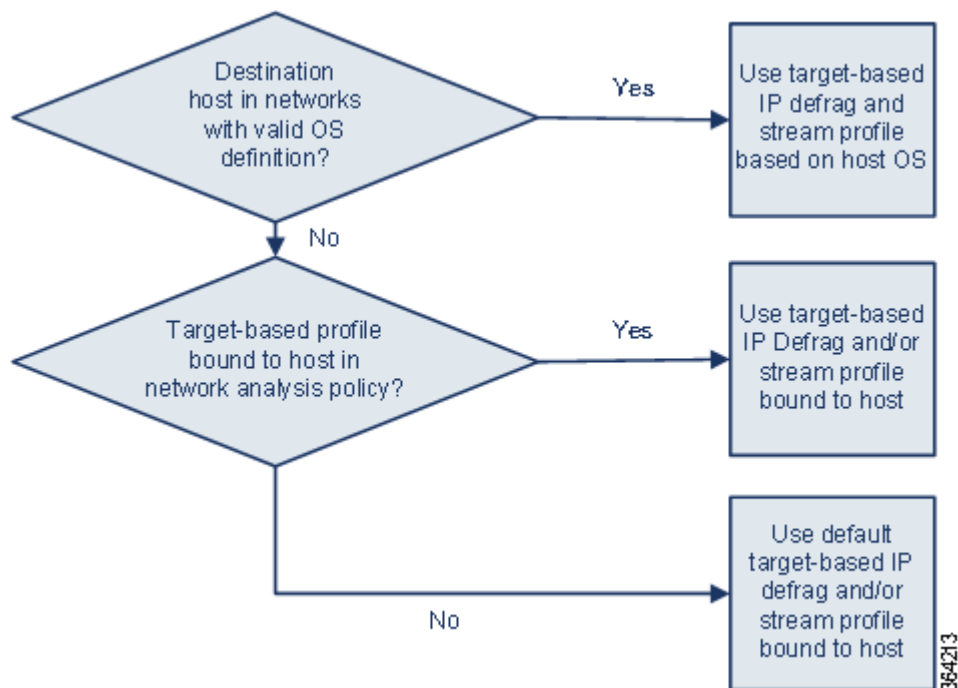
適応型プロファイルは、IP最適化とTCPストリームの前処理に最適なオペレーティングシステムプロファイルの使用を可能にします。適応型プロファイルにより影響を受けるネットワーク分析ポリシーの側面の詳細については、[IPパケットの最適化\(21-12 ページ\)](#)および[TCPストリームの前処理の使用\(21-21 ページ\)](#)を参照してください。

プリプロセッサによる適応型プロファイルの使用

ライセンス:Protection

適応型プロファイルは、ターゲットホストのオペレーティングシステムと同じ方法で、IP パケットの最適化およびストリームの再構成を行うのに役立ちます。その後、侵入ルールエンジンは宛先ホストによって使用されるものと同じ形式でデータを分析します。

適応型プロファイルは、次の図に示すように、ターゲットホストのホストプロファイルのオペレーティングシステムに基づいて、適切なオペレーティングシステムプロファイルに切り替わります。



たとえば、10.6.0.0/16 サブネットに適合型プロファイルを設定し、Linux にデフォルトの [IP 最適化 (IP Defragmentation)] ターゲットベースポリシーを設定します。設定を行う ASA FirePOWER モジュールには 10.6.0.0/16 サブネットが含まれています。

デバイスは、10.6.0.0/16 サブネットにないホスト A からのトラフィックを検出すると、Linux ターゲットベースポリシーを使用して IP フラグメントを再構成します。一方、10.6.0.0/16 サブネットにあるホスト B からのトラフィックを検出した場合、デバイスはホスト B のオペレーティングシステムのデータを取得します。このマップでは、ホスト B が Microsoft Windows XP Professional を実行しています。システムは、Windows ターゲットベースプロファイルを使用して、ホスト B に送信されるトラフィックの IP 最適化を実行します。

IP 最適化プリプロセッサの詳細については、[IP パケットの最適化 \(21-12 ページ\)](#) を参照してください。ストリームプリプロセッサの詳細については、[TCP ストリームの前処理の使用 \(21-21 ページ\)](#) を参照してください。

適応型プロファイルの設定

ライセンス:Protection

ホスト情報を使用して IP 最適化および TCP ストリームの前処理に使用するターゲット ベース プロファイルを判別するために、適応型プロファイルを設定できます。

適応型プロファイルを設定する際、適応型プロファイルを特定のネットワークにバインドする必要があります。正常に適応型プロファイルを使用するには、そのネットワークがデバイスでモニタされるセグメントにある必要があります。

IP アドレス、アドレスのブロック、またはアクセス コントロール ポリシーのデフォルトの侵入ポリシーにリンクされた変数セットにおいて、設定された適切な値を使用したネットワーク変数を指定することで、トラフィックの処理に適応型プロファイルが使用される、ネットワーク内のホストを指定できます。詳細については、[アクセス コントロールのデフォルト侵入ポリシーの設定 \(17-1 ページ\)](#)を参照してください。

これらのアドレス指定方法を単独で使用したり、次の例に示すように、IP アドレス、アドレス ブロック、または変数をカンマで区切ったリストとして組み合わせて使用したりすることができます。

```
192.168.1.101, 192.168.4.0/24, $HOME_NET
```

アドレス ブロックの指定の詳細については、[IP アドレスの表記規則 \(1-4 ページ\)](#)を参照してください。



ヒント

any という値の変数を使用するか、またはネットワーク値として 0.0.0.0/0 を指定することにより、適応型プロファイルをネットワーク内のすべてのホストに適用できます。

適応型プロファイルの設定:

- ステップ 1 **[設定 (Configuration)] > [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [ポリシー (Policies)] > [アクセス コントロール ポリシー (Access Control Policy)]** の順に選択します。
[アクセス コントロール ポリシー (Access Control Policy)] ページが表示されます。
- ステップ 2 編集するアクセス コントロール ポリシーの横にある編集アイコン(✎)をクリックします。
アクセス コントロール ポリシー エディタが表示されます。
- ステップ 3 **[詳細設定 (Advanced)]** タブを選択します。
アクセス コントロール ポリシーの詳細設定ページが表示されます。
- ステップ 4 **[検出拡張の設定 (Detection Enhancement Settings)]** の横にある編集アイコン(✎)をクリックします。
[検出拡張の設定 (Detection Enhancement Settings)] ポップアップ ウィンドウが表示されます。
- ステップ 5 **[検出拡張の設定 (Detection Enhancement Settings)]** を選択して、適応型プロファイルを有効にします。
- ステップ 6 必要に応じて、**[適応型プロファイル - 属性の更新間隔 (Adaptive Profiles - Attribute Update Interval)]** フィールドに、データの同期の間隔 (分) を入力します。



(注)

このオプションの値を大きくすると、大規模なネットワークのパフォーマンスを向上できます。

- ステップ 7 **[適応型プロファイル - ネットワーク (Adaptive Profiles - Networks)]** フィールドに、適応型プロファイルを使用するネットワーク内のホストを識別する、特定の IP アドレス、アドレス ブロック、または変数、またはこれらのアドレス指定方法を含むカンマ区切りのリストを入力します。
変数の設定の詳細については、[変数セットの使用 \(2-15 ページ\)](#)を参照してください。
- ステップ 8 **[OK]** をクリックして設定内容を維持します。

