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を使用すると、トラフィックをホスト情報と関連付けて、それに応じてトラフィックを処理することにより、システムをネットワーク トラフィックに適応させることができます。

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（24-7 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

ライセンス：Protection

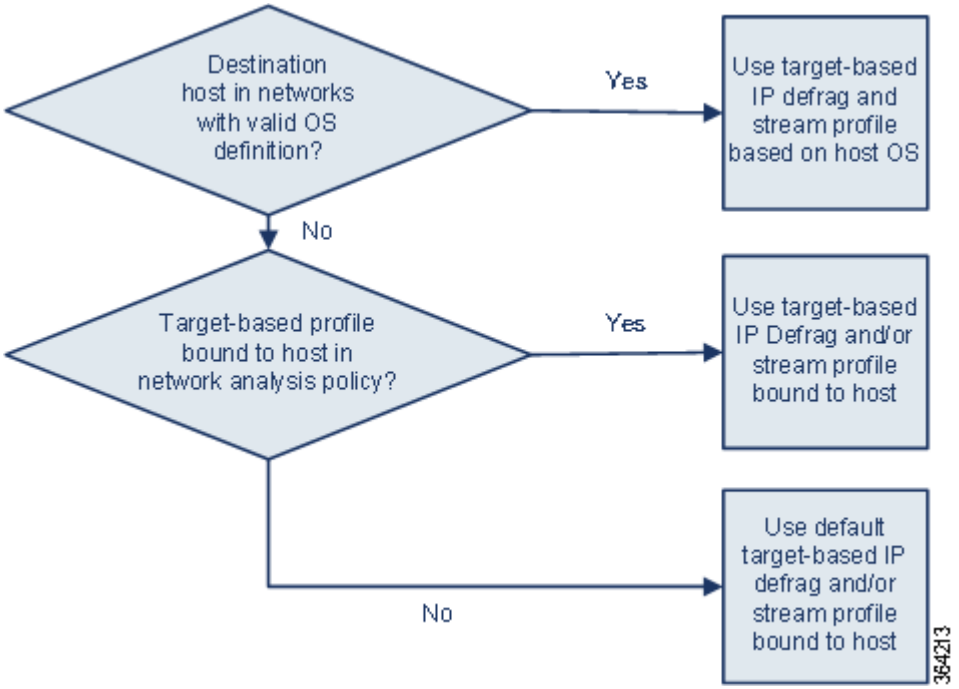
適応型プロファイルは、IP 最適化と TCP ストリームの前処理に最適なオペレーティング システム プロファイルの使用を可能にします。適応型プロファイルにより影響を受けるネットワーク分析ポリシーの側面の詳細については、IP パケットのデフラグ（24-13 ページ）およびTCP ストリームの前処理の使用（24-23 ページ）を参照してください。

プリプロセッサでの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によって、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 パケットが最適化され、ストリームが再構成されます。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 システムに応じて、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 サブネットに適応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。ここでホスト B は、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 パケットのデフラグ（24-13 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（24-23 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。適応型プロファイルを正常に使用するには、そのネットワークがデバイスによってモニタされるセグメント内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（20-1 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：

手順 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。

手順 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。

手順 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。

手順 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。

手順 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。

手順 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。

手順 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、変数セットの操作（2-15 ページ）を参照してください。

手順 8　[OK] をクリックして設定内容を維持します。