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、トラフィックをホスト情報と関連付けて処理することにより、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、シスコではアダプティブ 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 [Normalize TCP Payload] オプションを有効にすることを推奨しています。

アダプティブ プロファイルについて

ライセンス：Protection

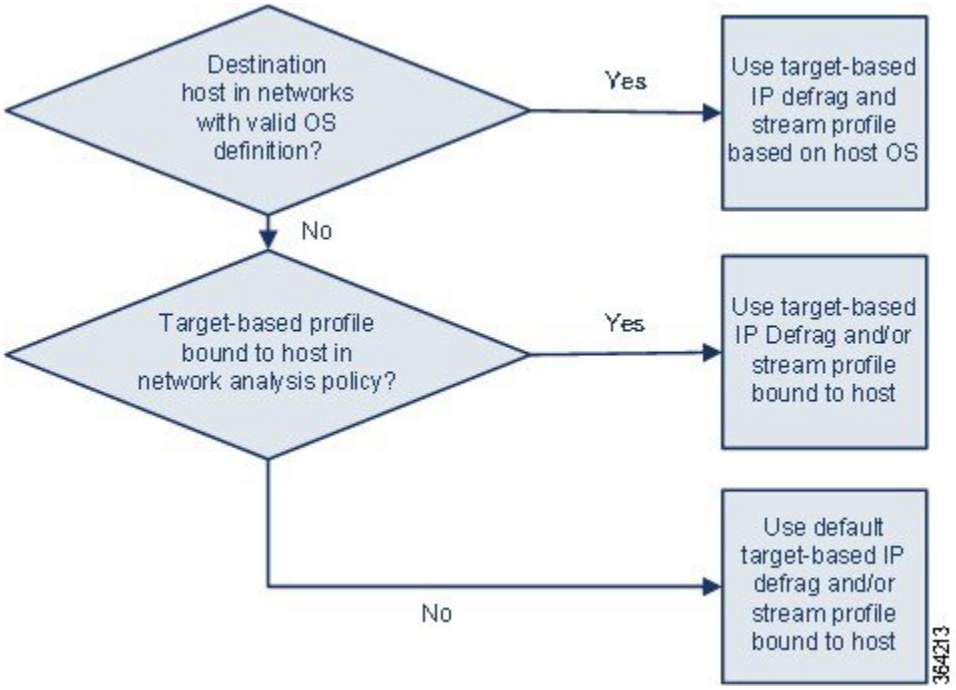
アダプティブ プロファイルは、IP 最適化と TCP ストリームの前処理に最適なオペレーティング システム プロファイルの使用を可能にします。

プリプロセッサでのアダプティブ 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 サブネットにアダプティブ プロファイルを設定し、Linux にデフォルトの IP 最適化ターゲット 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。ただし、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。

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。

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
```

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、アダプティブ 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。

適合型プロファイルの設定：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。
[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 [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 [Detection Enhancement Settings] の横にある編集アイコンをクリックします。
[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 [Adaptive Profiles - Enabled] を選択して、アダプティブ プロファイルを有効にします。

ステップ 6 必要に応じて、[Adaptive Profiles - Attribute Update Interval] フィールドに、同期に必要な経過時間（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 [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。