CHAPTER 30

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、トラフィックをネットワーク マップから得られるホスト情報と関連付けてから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、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（29-7 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（30-1 ページ）
- 適応型プロファイルの設定（30-3 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（29-13 ページ）および TCP ストリームの前処理の使用（29-22 ページ）を参照してください。

システムはネットワーク検出または Nmap スキャンにより取得するか、またはホスト入力機能により追加されたホスト情報を使用して、処理動作を適応させることができます。

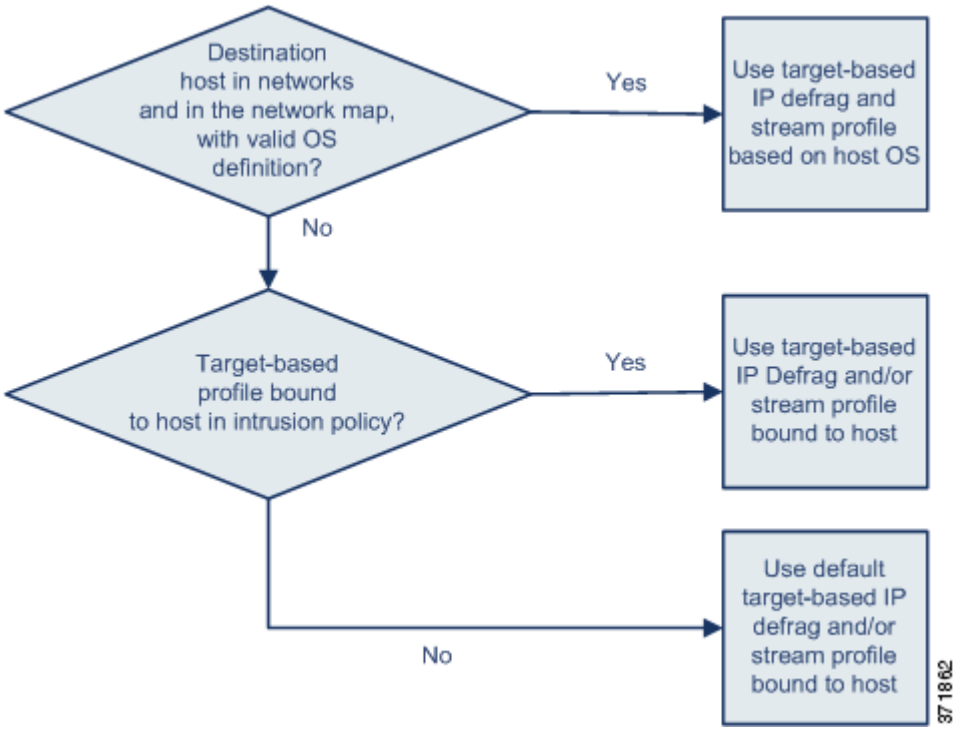
(注)　コマンドラインのインポート ユーティリティまたはホスト入力 API を使用してサードパーティ製アプリケーションからホスト情報を入力する場合、システムが適応型プロファイルで使用できるように、データを製品の定義にマッピングしておく必要があります。詳細については、サードパーティ製品マッピングの管理 (46-33 ページ) を参照してください。

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、ネットワーク分析ポリシーに設定可能なターゲット ベースのプロファイルと同様に、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。

手動で設定されたターゲット ベースのプロファイルは、選択したデフォルトのオペレーティング システム プロファイルまたは特定のホストにバインドしたプロファイルにのみ適用されます。一方、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 Defense Center には 10.6.0.0/16 サブネットが含まれていますネットワーク マップがあります。

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、デバイスはネットワーク マップからホスト B のオペレーティング システムのデータを取得します。このマップには、ホスト B が Microsoft Windows XP Professional を実行していることが記述されています。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（29-13 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（29-22 ページ）を参照してください。

適応型プロファイルと FireSIGHT 推奨ルール

ライセンス：Protection

適応型プロファイルの機能はアクセス コントロール ポリシーの詳細設定で、そのアクセス コントロール ポリシーによって呼び出されるすべての侵入ポリシーにグローバルに適用されます。FireSIGHT 推奨ルールの機能は、設定する個々の侵入ポリシーに適用されます。

FireSIGHT 推奨ルールと同様に、適応型プロファイルはルールのメタデータをホスト情報と比較し、ルールを特定のホストに適用すべきかどうかを判別します。ただし、FireSIGHT 推奨ルールがその情報を使用してルールの有効化または無効化を行うための推奨事項を提供するのに対して、適応型プロファイルはその情報を使用して特定のトラフィックに特定のルールを適用します。

FireSIGHT 推奨ルールでは、提案された変更をルール状態に実装するために、ユーザの対話が必要になります。一方、適応型プロファイルは侵入ポリシーを変更しません。ルールの適応処理はパケット単位で行われます。

さらに、FireSIGHT 推奨ルールによって、無効なルールが有効化される可能性があります。対照的に、適応型プロファイルは、侵入ポリシーですでに有効になっているルールの適用にだけ影響します。適応型プロファイルによってルールの状態が変更されることはありません。

適応型プロファイルと FireSIGHT 推奨ルールを組み合わせて使用できます。侵入ポリシーが適用されると、適応型プロファイルはルールの状態を使用して適用の候補に含めるかどうかを判別し、推奨事項の承認または拒否はそのルール状態に反映されます。両方の機能を使用して、監視対象の各ネットワークに最適なルールを有効化または無効化することができ、特定のトラフィックに対する有効化したルールの適用を最も効率的に行うことができます。

詳細については、ネットワーク資産に応じた侵入防御の調整（33-1 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ネットワーク マップ内にあり、アクセス コントロール ポリシーを適用する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。

（注） 適応型プロファイルを使用するには、保護するネットワークのネットワーク検出ポリシーでホスト検出を有効にし、ネットワーク検出ポリシーを再適用する必要があります。詳細については、ネットワーク検出ポリシーの作成（45-25 ページ）を参照してください。

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 マップ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（25-1 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
```

FireSIGHT システムにおけるアドレス 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（1-24 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、適合型プロファイルをネットワーク マップ内のすべてのホストに適用できます。

また、Defense Center のネットワーク マップ データが管理対象デバイスと同期される頻度を制御することもできます。システムはデータを使用して、トラフィックを処理する際に使用するプロファイルを判別します。

注意 アクセス コントロール ポリシーの適用時に、適合型プロファイルを有効または無効にすると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

適合型プロファイルの設定:

アクセス: Admin/Access Admin/Network Admin

手順 1 [ポリシー（Policies）] > [アクセス制御（Access Control）] を選択します。

[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 - 属性更新間隔（Adaptive Profiles - Attribute Update Interval）] フィールドに、Defense Center から管理対象デバイスへのネットワーク マップ 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　[適合型プロファイル - ネットワーク（Adaptive Profiles - Networks）] フィールドに、適合型プロファイルを使用するネットワーク マップ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（3-19 ページ）を参照してください。ネットワーク マップの設定の詳細については、ネットワーク検出ポリシーの作成（45-25 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。