適応型プロファイルの使用

通常、システムは侵入ポリシーの静的な設定を使用して、トラフィックの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 パッシブ展開では、シスコは適応型プロファイルの設定を推奨します。インライン展開では、シスコは [Normalize TCP] オプションと [Normalize TCP Payload] オプションを有効にした、インライン正規化プリプロセッサの設定を推奨します。詳細については、「TCP 正規化」（P.26-6）および「インライン正規化の設定」（P.26-7）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：FireSIGHT + 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侵入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」（P.26-12）および「TCP ストリームの前処理の使用」（P.26-21）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。

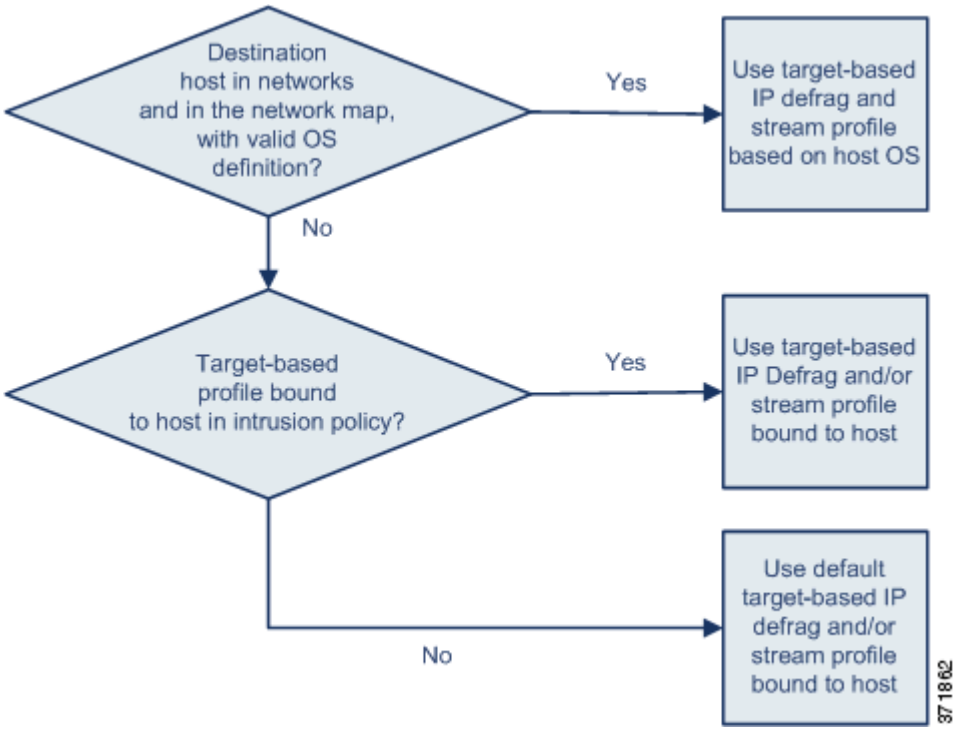
注　コマンドラインのインポート ユーティリティまたはホスト入力 API を使用してサードパーティ製アプリケーションからホスト情報を入力する場合、適応型プロファイルで使用できるように、データを製品の定義にマッピングしておく必要があります。詳細については、「サードパーティ製品マッピングの管理」（P.42-33）を参照してください。

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：FireSIGHT + Protection

適応型プロファイルは、侵入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、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、適応型プロファイルが 10.6.0.0/16 サブネットで有効であり、Linux に対するデフォルトの IP 最適化ターゲット ベース ポリシーを設定した、侵入ポリシーを設定します。ポリシーを設定する防御センターには 10.6.0.0/16 サブネットを含むネットワーク 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 パケットのデフラグ」（P.26-12）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」（P.26-21）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：FireSIGHT + Protection

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、ユーザー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。

同じポリシー内で適応型プロファイルと FireSIGHT 推奨ルールを使用できます。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、「FireSIGHT ルール状態推奨の管理」（P.21-39）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：FireSIGHT + 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、侵入ポリシーを含むアクセス 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の有効化は、アクセス コントロール ポリシーのデフォルト アクションに関連付ける侵入ポリシーでのみ行う必要があります。

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 アクションに関連付けられる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。

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 アドレスの表記法」（P.1-19）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、防御センターのネットワーク 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。

適合型プロファイルの設定：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、続行します。別のポリシーでの未保存の変更の保存方法については、「侵入ポリシー変更のコミット」（P.20-9）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [Advanced Settings] をクリックします。

[Advanced Settings] ページが表示されます。

ステップ 4　[Detection Enhancement] の下の [Adaptive Profiles] が有効かどうかにより、次の 2 つの選択肢があります。

- 設定が有効な場合、[Edit] をクリックします。
- 設定が無効の場合、[Enabled] をクリックした後で、[Edit] をクリックします。

[Adaptive Profiles] ページが表示されます。

ページ下部のメッセージは、設定を含む侵入ポリシー層を示します。詳細については、「侵入ポリシーでのレイヤの使用」（P.23-1）を参照してください。

ステップ 5　必要に応じて、[Attribute Update Interval] フィールドに、防御センターから管理対象デバイスへのネットワーク マップ データの同期に必要な経過時間（分）を入力します。

注　[Attribute Update Interval] 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 6　[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、「変数セットの操作」（P.5-19）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」（P.35-26）を参照してください。

ステップ 7　ポリシーの保存、編集の続行、変更の廃棄、またはシステム キャッシュ内の変更をそのままにした終了を行います。詳細については、「一般的な侵入ポリシー編集操作」の表を参照してください。