適応型プロファイル

ここでは、適応型プロファイルの設定方法について説明します。

アダプティブ プロファイルについて

アダプティブプロファイルを使うと、次の操作を実行できます。

- アクセス コントロール ルールは AMP を含むアプリケーション制御およびファイル制御が可能になり、侵入ルールはサービス メタデータを使用できるようになります。

  注意 アクセス コントロール ルールが AMP を含むアプリケーション制御およびファイル制御を行い、侵入ルールがサービス メタデータを使用するためには、適応型プロファイルの設定 （4 ページ）で説明されているように、アダプティブ プロファイルが**必ず**有効になっている（デフォルト状態）必要があります。

- パッシブ展開では、アダプティブプロファイルの更新を有効にして、宛先ホストのオペレーティング システムに従って IP トラフィックに最適化とリアセンブルを行います。

  （注） インライン展開では、アダプティブプロファイルの更新を有効にする代わりに、インライン正規化プリプロセッサを設定し、[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ます。

アダプティブプロファイルの更新

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。アダプティブプロファイルの更新では、ネットワーク検出で検出したホスト情報またはサードパーティからインポートしたホスト情報に合わせて、システムが処理動作を変更します。

プロファイルの更新ネットワーク分析ポリシーに手動で設定可能なターゲットベース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リアセンブル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 プロファイルは、選択したデフォルト 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のいずれかに適用されます。プロファイルの更新では、ターゲット ホストのホスト プロファイル内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えを行います。

10.6.0.0/16 サブネット向けにプロファイルの更新を設定し、Linux にデフォルトの IP 最適化ターゲットベース ポリシーを設定するシナリオを考えてみます。設定を構成する Firepower Management Center 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。

- システムが 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 フラグメントのリアセンブルを行います。
- システムが 10.6.0.0/16 サブネット上にあるホスト B からのトラフィックを検出すると、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 データを取得します。システムは、このオペレーティング システムに基づいたプロファイルを使用し、ホスト B を宛先とするトラフィックを最適化します。

アダプティブプロファイルの更新および Firepower 推奨ルール

アダプティブ プロファイルの更新機能は、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。Firepower 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。

Firepower 推奨ルールと同様に、プロファイルの更新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、Firepower 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、プロファイルの更新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。

Firepower 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、プロファイルの更新は侵入ポリシーを変更しません。プロファイル更新に基づくルールの処理は、パケット単位で行われます。

さらに、Firepower 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。プロファイルの更新は、対照的に、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。プロファイルの更新がルール状態を変更することはありません。

プロファイルの更新と Firepower 推奨ルールは組み合わせて使用できます。侵入ポリシーを展開すると、プロファイルの更新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。

関連トピック

Firepower 推奨ルールについて

適応型プロファイルのオプション

有効（Enable）

次のことを可能にします。

- アクセス コントロール ルールで AMP を含めたアプリケーションとファイルの制御を実行する
- 侵入ルールでサービス メタデータを使用する

プロファイルの更新を有効にする（Enable Profile Updates）

パッシブ展開で、プロファイルの更新を有効にして、ネットワーク マップでホストが使用するオペレーティング システムのプロファイルに応じて IP トラフィックがデフラグおよびリアセンブルされるようにします。

アダプティブ プロファイル - 属性の更新間隔（Adaptive Profiles - Attribute Update Interval）

プロファイルの更新を有効にすると、Firepower Management Center から管理対象デバイスに対するネットワーク マップ データの同期の頻度を分単位で制御することができます。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。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でパフォーマンスを向上させることができます。

アダプティブ プロファイル - ネットワーク（Adaptive Profiles - Networks）

任意で、プロファイルの更新を有効にすると、IP アドレス、アドレス ブロック、およびネットワーク変数のカンマ区切りリストに対する プロファイルの更新 を制限して、パフォーマンスを向上させることができます。ネットワーク変数を使用すると、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ている変数セットの変数の値が使用されるようになります。たとえば、**192.168.1.101**、**192.168.4.0/24**、**$HOME_NET** というように入力することができます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上位ポリシーでプロファイルの更新を有効にして適用する場合、Cisco では、デフォルトのネットワークの制約 **0.0.0.0/0** を保持するか、または値 any を指定してネットワーク変数を使用することをお勧めしています。この設定により、すべてのサブドメインのすべてのモニタ対象ホストに プロファイルの更新 が適用されるようになります。

関連トピック

デフォルトの侵入ポリシー
Firepower システムの IP アドレス表記法
変数セット

適応型プロファイルの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

パッシブ展開では、アダプティブ プロファイルの更新を設定することをお勧めします。インライン展開の場合、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します。

注意 アクセス コントロール ルールが AMP を含むアプリケーション制御およびファイル制御を行い、侵入ルールがサービス メタデータを使用するためには、この手順で説明されているように、アダプティブ プロファイルが**必ず**有効になっている（デフォルト状態）必要があります。アダプティブ プロファイルを有効化または無効化すると 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。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® の再起動によるトラフィックの動作を参照してください。

手順

ステップ 1 アクセス コントロール ポリシー エディタで [詳細（Advanced）] タブをクリックし、[検出拡張の設定（Detection Enhancement Settings）] セクションの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する（Inherit from base policy）] をオフにして、編集を有効にします。

ステップ 2 適応型プロファイルのオプション（3 ページ）の説明に従って適応型プロファイルのオプションを設定します。

ステップ 3 [OK] をクリックします。

ステップ 4 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の導入を参照してください。

関連トピック

インライン正規化プリプロセッサ
Snort® の再起動シナリオ