アダプティブ 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

次のことを行うには、アダプティブプロファイルを有効にする必要があります。

- マルウェア保護（AMP）を含むアプリケーションとファイルの制御を実行し、侵入ルールがサービスメタデータを使用できるようにします。

⚠

注意 アクセスコントロールルールでマルウェア防御（AMP）を含むアプリケーション/ファイル制御を実行し、侵入ルールで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 （5 ページ）の説明に従ってアダプティブプロファイルを有効（デフォルトの状態）にする**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ライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

アダプティブプロファイルの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

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。adaptive profile updates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。

Profile updatesは、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 システムか固有のホストに構築したプロファイルのいずれかに適用されます。ただし、Profile updatesは、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。

10.6.0.0/16 サブネット向けにprofile updates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 Firewall 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とシスコの推奨ルール

adaptive profile updates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。シスコの推奨ルール機能は、設定する個々の侵入ポリシーに適用されます。

シスコの推奨ルールと同様に、profile updates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、シスコの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、profile updates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。

シスコの推奨ルールでは、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、Profile updates 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、シスコの推奨ルールでは、結果として、無効化されたルールを有効にできます。これに対して、Profile updates では、侵入ポリシーですでに有効になっているルールの適用のみに影響を与えます。Profile updates はルール状態を変更することはありません。

profile updatesとシスコの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、Profile updates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

シスコ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）

このオプションを有効にする必要があるのは、次の場合です。

- アクセスコントロールルールでマルウェア保護（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

このオプションは、デフォルトで有効です。

（注） Snort 3 でアダプティブプロファイルを有効にするには、[有効化（Enable）] オプションと [プロファイル更新の有効化（Enable Profile Updates）] オプションの両方を選択する必要があります。

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。

Snort 3 でアダプティブプロファイルが有効になっている場合は、これを有効にする必要があります。

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、Firewall 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 profile updates 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。IPv4 と IPv6 がサポートされます。

デフォルト値（**0.0.0.0/0**）は、すべてのネットワークにアダプティブプロファイルの更新を適用します。

関連トピック

トラフィック識別の前に通過するパケットのインスペクション
変数セット

適応型プロファイルの設定

パッシブ展開では、adaptive profile updates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。

始める前に

アクセス コントロール ポリシーには、ホスト/サービスの検出を実行できるように有効になっている、ネットワーク検出ポリシーが必要です。または、ホストデータをサードパーティのソースからインポートする必要があります。

手順

ステップ 1 アクセス制御ポリシーエディタで、変更するポリシーの [編集（Edit）]（✎） をクリックします。

ステップ 2 **[詳細（More）] > [詳細設定（Advanced Settings）]** の順にクリックし、[検出拡張の設定（Detection Enhancement Settings）] セクションの横にある [編集（Edit）]（✎） をクリックします。

代わりに [表示（View）]（👁） が表示される場合、設定は先祖ポリシーから継承されており、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、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 3 適応型プロファイルのオプション （4 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 4 [OK] をクリックします。

ステップ 5 [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展開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 再起動のシナリオ

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。