EVEの脅威の確実性スコアに基づいてトラフィックをブロックする

Encrypted Visibility Engine について

Encrypted Visibility Engine（EVE）を使用すると Transport Layer Security（TLS）暗号化を使用するクライアント アプリケーションとプロセスを識別できます。EVE は、復号せずに暗号化されたセッションの可視性を高めます。EVE の結果に基づいて、管理者は環境内のトラフィックにポリシーアクションを適用できます。また、EVE を使用してマルウェアを特定して阻止することもできます。

利点

管理者は EVE の脅威スコアを活用し、調整して、悪意のある暗号化トラフィックをブロックできます。着信トラフィックが悪意のある可能性がある場合は、脅威スコアに基づいて、接続をブロックするように EVE を設定できます。

ビジネスシナリオの例

大規模な企業ネットワークで、主要な侵入検知および防御システムとして Snort 3 を使用しているとします。セキュリティへの脅威が急速に進化する状況では、堅牢なネットワークセキュリティ対策の採用が必要かつ重要です。セキュリティチームは EVE を使用して、完全な中間

者（MITM）復号を実装することなく、暗号化されたトラフィックの検査を強化します。EVE テクノロジーは、既知の悪意のあるプロセスのフィンガープリントを使用して、マルウェアを特定して阻止します。ネットワーク管理者は、設定されたブロックしきい値に基づいて、悪意のある可能性がある接続をブロックするために、EVE のブロックトラフィックしきい値を柔軟に設定できる必要があります。

前提条件

- Management Center 7.4.0 以降を実行している必要があり、管理対象 Threat Defense も 7.4.0 以降である必要があります。
- 有効な侵入防御システム（IPS）ライセンスがあり、Snort 3 が検出エンジンであることを確認します。

ワークフローの概要

1. EVE は着信トラフィックを分析し、着信トラフィックがマルウェアであるかどうかを判定します。
2. EVE が着信トラフィックを特定の信頼度でマルウェアであると検出した場合、そのトラフィックをブロックするように EVE を設定できます。
3. パケットのマルウェア確率または脅威スコアが最初にチェックされ、脅威スコアが設定済みのブロックしきい値と比較されます。
4. 脅威スコアが設定済みのしきい値よりも高い場合、EVE はトラフィックをブロックします。
5. 脅威スコアが設定済みのしきい値よりも小さい場合、EVE はアクションを実行しません。

EVE でのブロックしきい値の設定

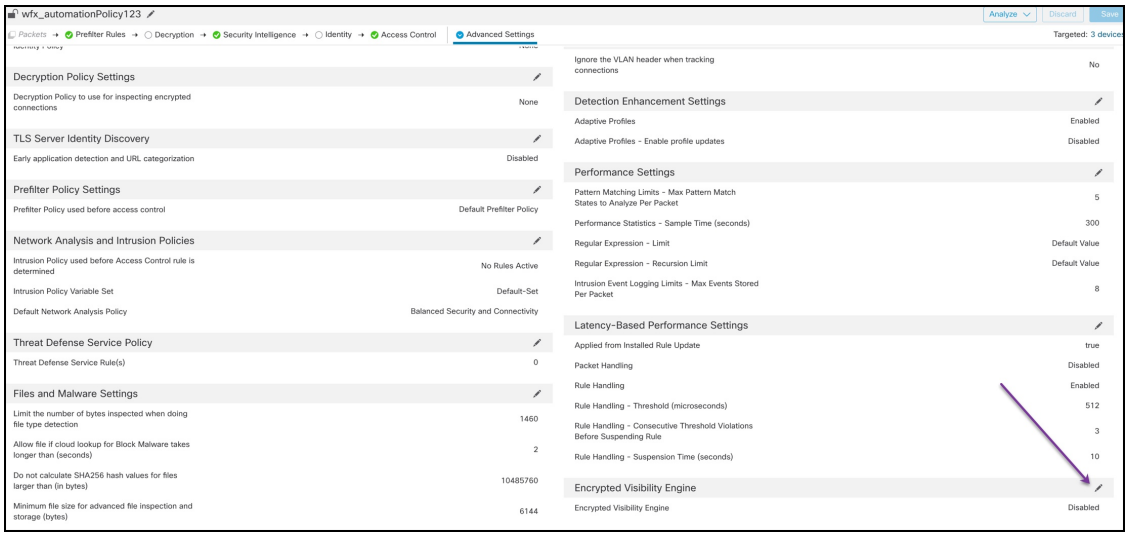
この手順では、90% 以上の EVE の脅威の確実性スコアに基づいて、悪意のある可能性があるトラフィックをブロックする方法を示します。

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

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（Edit）]（✎）をクリックします。

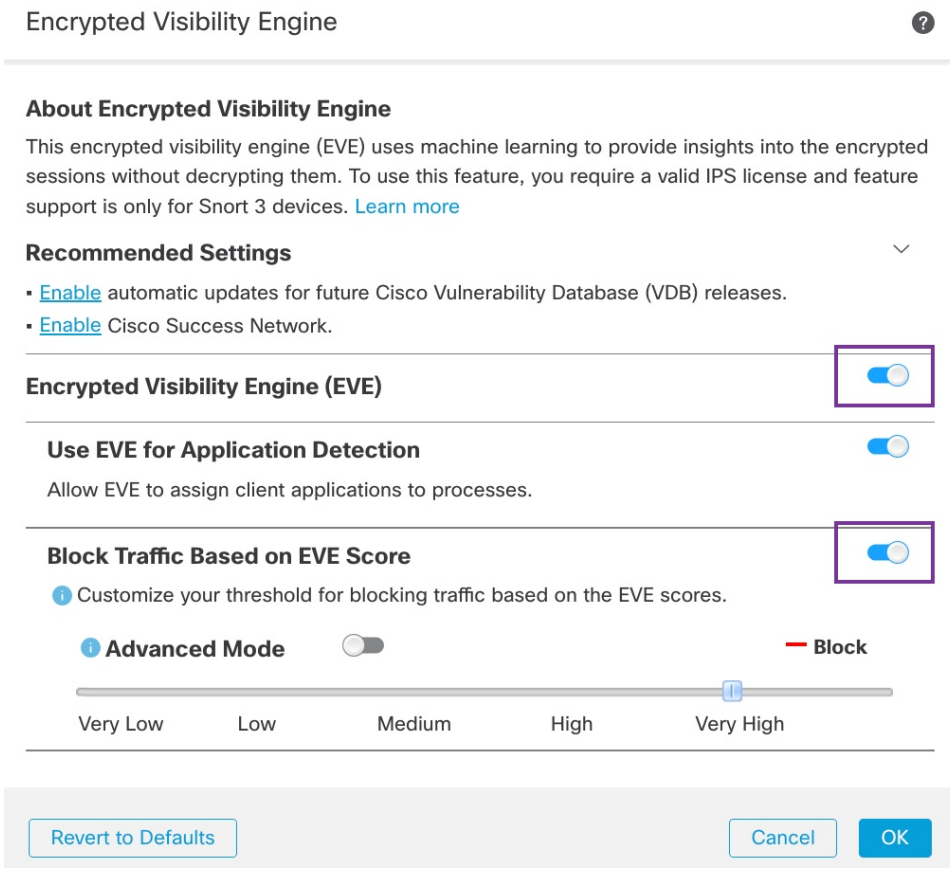
ステップ 3 パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [詳細設定（Advanced Settings）] を選択します。

ステップ 4 [Encrypted Visibility Engine] の横にある [編集（Edit）]（✎）をクリックします。



ステップ 5 [Encrypted Visibility Engine] ページで、[Encrypted Visibility Engine (EVE)] トグルボタンを有効にします。

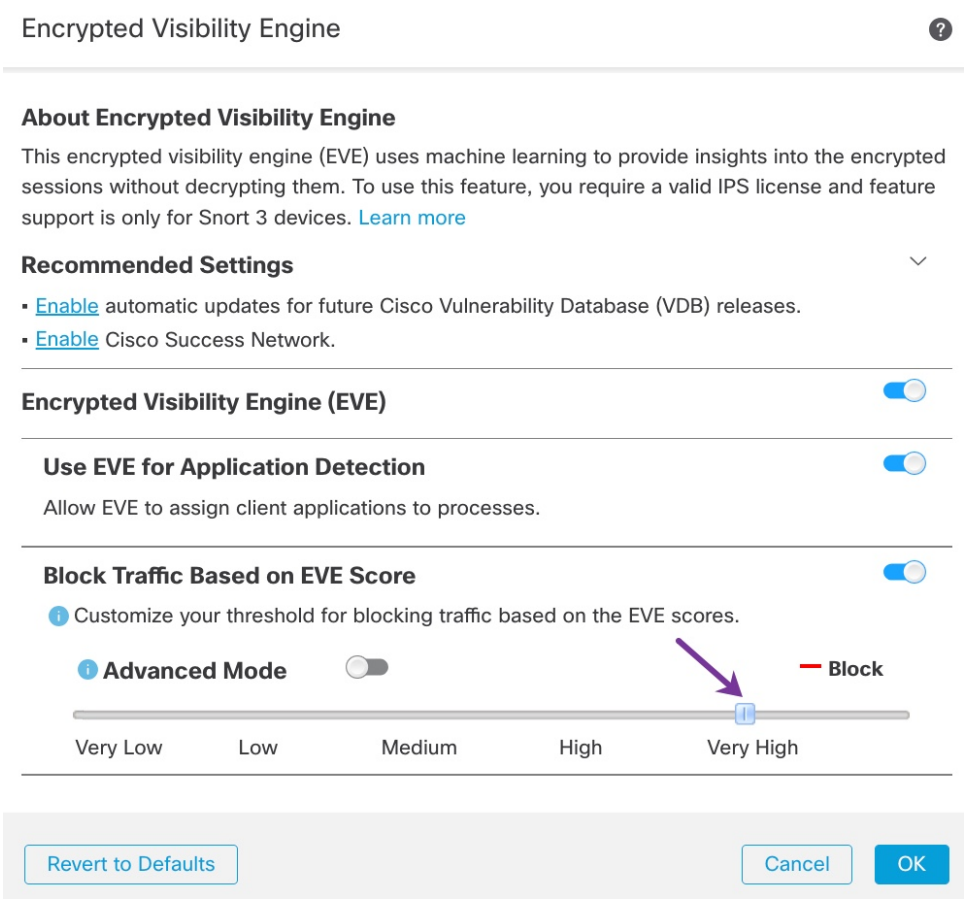
ステップ 6 [EVEスコアに基づいてトラフィックをブロック（Block Traffic Based on EVE Score）] トグルボタンを有効にします。潜在的な脅威である着信トラフィックは、デフォルトでブロックされます。



（注） デフォルトでは、マルウェアがブロックされるしきい値は 99% です。これは、次のことを意味します。

- EVE がトラフィックを 99% 以上の確実性でマルウェアであると検出した場合、EVE はトラフィックをブロックします。
- EVE がトラフィックを 99% 未満の確実性でマルウェアであると検出した場合、EVE は何も実行しません。

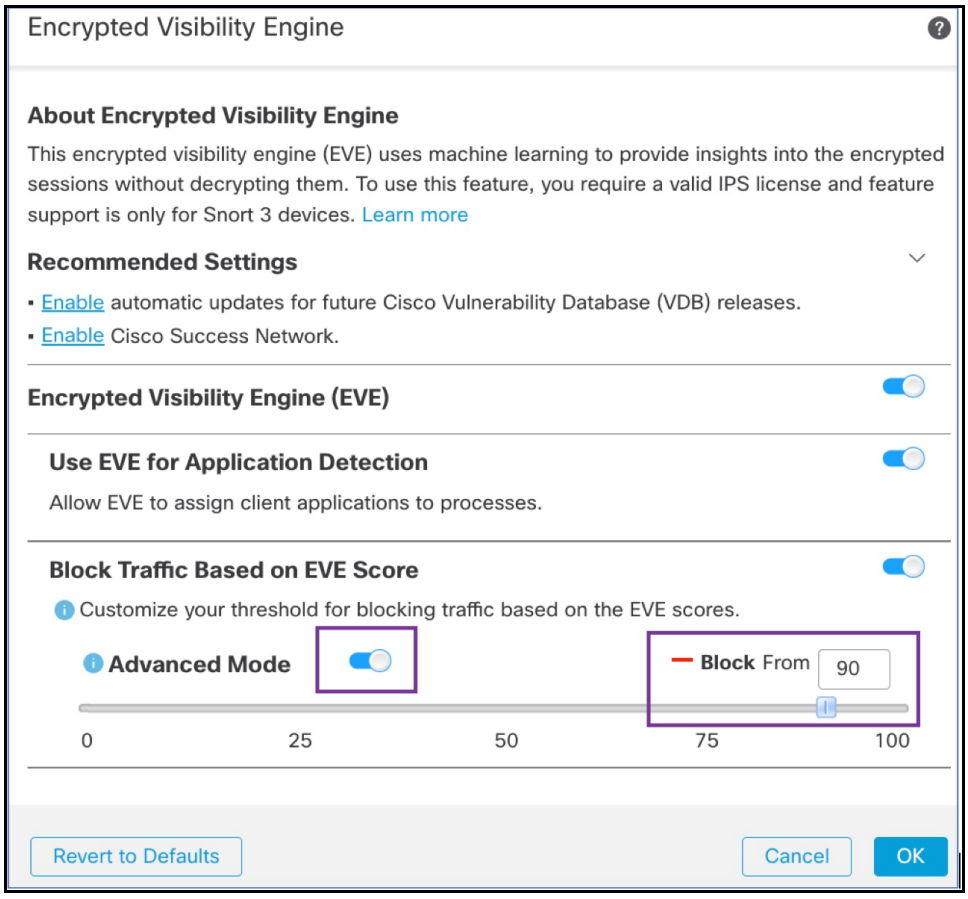
ステップ 7 スライダを使用して、EVE の脅威の確実性に基づいたブロックのしきい値を調整します。この範囲は、[非常に低い（Very Low）] から [非常に高い（Very High）] です。この例では、スライダは [非常に高い（Very High）] に設定されています。



ステップ 8 さらに細かく制御するには、[詳細モード（Advanced Mode）] トグルボタンを有効にします。これで、トラフィックをブロックするための特定の EVE 脅威確実性スコアを割り当てることができるようになりました。デフォルトのしきい値は、99 % です。

ステップ 9 この例では、ブロックしきい値を **90%** に変更します。

注目 ベストプラクティスとして、最適なパフォーマンスを確保するために、ブロックしきい値を 50% 未満に設定しないことを推奨します。



ステップ 10 [OK] をクリックします。

ステップ 11 [保存（Save）] をクリックします。

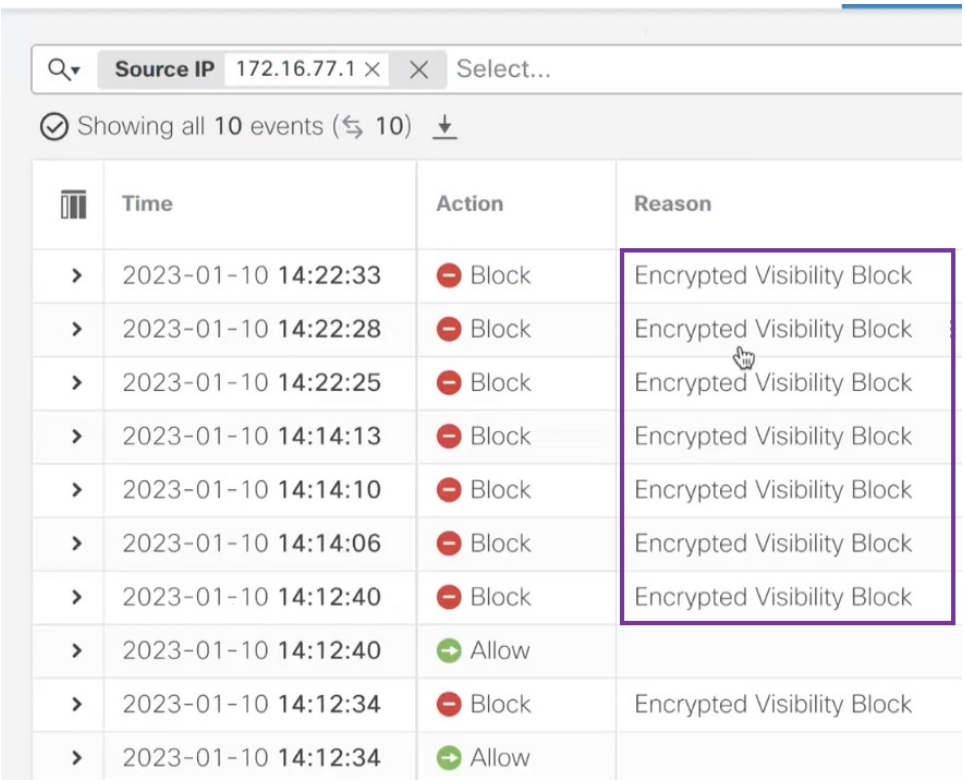
次のタスク

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。

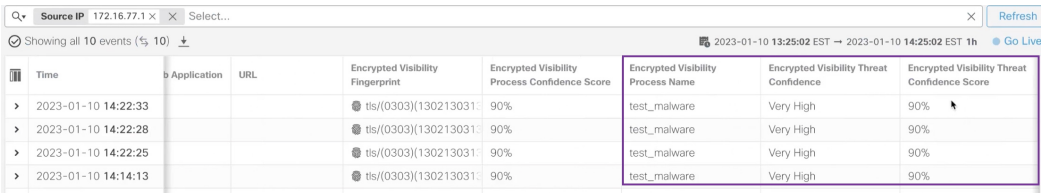
EVE イベントの表示

ステップ 1 ブロックアクションを確認するには、**[分析（Analysis）] > [接続（Connections）] > [イベント（Events）]** の順に選択します。[統合されたイベント（Unified Events）] ビューアからイベントを表示することもできます。

ステップ 2 トラフィックをブロックするように EVE を設定した場合、[理由（Reason）] フィールドには [Encrypted Visibilityブロック（Encrypted Visibility Block）] と表示されます。



ステップ 3 次に、[Encrypted Visibilityプロセス名（Encrypted Visibility Process Name）] が **test_malware**、[Encrypted Visibility脅威の確実性（Encrypted Visibility Threat Confidence）] が [非常に高い（Very High）]、[Encrypted Visibility脅威の確実性スコア（Encrypted Visibility Threat Confidence Score）] が **90%** の例を示します。



その他の参考資料

概念の詳細については、このガイドの「Snort 3 向けの Encrypted Visibility Engine」の章または次のリンクの内容を参照してください。

暗号化された可視性エンジン

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。