暗号化された可視性エンジン

Encrypted Visibility Engine（EVE）は、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するために使用されます。可視性を実現し、管理者が環境内でアクションを実行してポリシーを適用できるようにします。EVEテクノロジーは、マルウェアの特定と阻止にも使用できます。

Encrypted Visibility Engine の概要

The encrypted visibility engine (EVE) is used to provide more visibility into the encrypted sessions without the need to decrypt them. These insights into encrypted sessions are obtained by Cisco's open-source library that is packaged in Cisco's vulnerability database (VDB). The library fingerprints and analyzes incoming encrypted sessions and matches it against a set of known fingerprints. This database of known fingerprints is also available in the Cisco VDB.

（注） 暗号化された可視性エンジンの機能は、Snort 3 を実行している Firewall Management Center の管理対象デバイスでのみサポートされます。この機能は、Snort 2 デバイスおよび Firewall Device Manager 管理対象デバイスではサポートされていません。

EVE の重要な機能の一部を次に示します。

- EVEから取得した情報を使用して、トラフィックに対してアクセス コントロール ポリシー アクションを実行できます。

- Cisco Secure Firewall に含まれる VDB には、EVE によって高い信頼値で検出された一部のプロセスにアプリケーションを割り当てる機能があります。または、次の目的でカスタムアプリケーション ディテクタを作成できます。
  - EVE で検出されたプロセスを新しいユーザー定義アプリケーションにマッピングする。
  - EVE で検出されたプロセスにアプリケーションを割り当てるために使用されるプロセス確実性の組み込み値を上書きする。

  『Cisco Secure Firewall Management Center デバイス設定ガイド』の「**アプリケーションの検出**」の章にある項「**カスタム アプリケーション ディテクタの設定**」と「**EVE のプロセス割り当ての指定**」を参照してください。
- EVE は、暗号化されたトラフィックで Client Hello パケットを作成したクライアントのオペレーティングシステムのタイプとバージョンを検出できます。
- EVE は、Quick UDP Internet Connections（QUIC）トラフィックのフィンガープリントと分析もサポートします。Client Hello パケットからのサーバー名は、[接続イベント（Connection Events）] ページの [URL] フィールドに表示されます。

注目 Firewall Management Center で EVE を使用するには、デバイスに有効な IPS ライセンスが必要です。IPSライセンスがない場合、ポリシーによって警告が表示され、展開は許可されません。

（注）
- EVE は SSL セッションのオペレーティングシステムのタイプとバージョンを検出できます。アプリケーションやパッケージ管理ソフトウェアの実行など、オペレーティングシステムの通常の使用により、OS検出がトリガーされる可能性があります。クライアントOS検出を表示するには、EVE トグルボタンを有効にすることに加えて、**[ポリシー（Policies）] > [ネットワークの検出（Network Discovery）]** で [ホスト（Hosts）] を有効にする必要があります。ホスト IP アドレスで使用可能なオペレーティングシステムのリストを表示するには、**[分析（Analysis）] > [ホスト（Hosts）] > [ネットワークマップ（Network Map）]** をクリックし、該当するホストを選択します。
- EVE では、カプセル化されたトラフィックの可視性やインサイトは提供されません。

関連リンク

EVE の設定 （4 ページ）
EVE 例外ルールの設定 （8 ページ）

EVE の仕組み

Encrypted Visibility Engine（EVE）は、TLS ハンドシェイクの Client Hello 部分を検査して、クライアントプロセスを識別します。Client Hello は、サーバーに送信される最初のデータパケットです。これにより、ホスト上のクライアントプロセスがよくわかります。このフィンガープリントと、宛先 IP アドレスなどの他のデータが組み合わされて、EVE のアプリケーション識別の基礎となります。TLS セッションの確立で特定のアプリケーション フィンガープリントを識別することで、システムはクライアントプロセスを識別し、適切なアクション（許可/ブロック）を実行することができます。

EVE は、5,000 を超えるクライアントプロセスを識別できます。システムは、アクセス制御ルールの基準として使用するために、多数のこれらのプロセスをクライアントアプリケーションにマッピングします。これにより、システムは TLS 復号を有効にすることなく、これらのアプリケーションを識別して制御することができます。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することで、EVE テクノロジーを使用して、アウトバウンド復号を使用せずに暗号化された悪意のあるトラフィックを識別してブロックすることもできます。

機械学習（ML）テクノロジーにより、シスコは 10 億を超える TLS フィンガープリントと 10,000 を超えるマルウェアサンプルを毎日処理し、EVE フィンガープリントを作成および更新しています。これらの更新は、その後、シスコの脆弱性データベース（VDB）パッケージを使用してお客様に配信されます。

EVE は、フィンガープリントを認識できない場合、クライアントアプリケーションを識別し、IP アドレス、ポート、サーバー名などの接続先の詳細情報を使用して最初のフローの脅威スコアを推定します。この時点で、フィンガープリントのステータスはランダム化され、デバッグログで確認できます。同じフィンガープリントを持つ後続のフローの場合、EVE は再分析をスキップし、フィンガープリントのステータスをラベルなしとしてマークします。EVE の低い、または非常に低いスコアしきい値に基づいてトラフィックをブロックする場合、最初のフローはブロックされます。ただし、アプリケーションのフィンガープリントがキャッシュされると、その後のフローは許可されます。

侵害の兆候イベント

ホストの暗号化された可視性エンジン検出の侵害の兆候（IoC）イベントにより、非常に高いマルウェアの確実性レベルで、EVE によって報告された接続イベントをチェックできます。IoC イベントは、悪意のあるクライアントを使用してホストから生成された暗号化セッションに対してトリガーされます。悪意のあるホストの IP アドレス、MAC アドレス、OS 情報などの情報と、不審なアクティビティのタイムスタンプを表示できます。

接続イベントで示される、暗号化された可視性脅威の確実性スコアが「非常に高い」となっているセッションは、IoC イベントを生成します。**[ポリシー（Policies）]** > **[ネットワーク検出（Network Discovery）]** から [ホスト（Hosts）] を有効にする必要があります。 Firewall Management Center では、次の場所から IoC イベントの存在を表示できます。

- **[分析（Analysis）]** > **[侵害の兆候（Indications of Compromise）]**

- **[分析（Analysis）]** > **[ネットワークマップ（Network Map）]** > **[侵害の兆候（Indications of Compromise）]** > チェックする必要があるホストを選択します。

  [接続イベント（Connection Events）] ページでは、IoC が生成されるセッションのプロセス情報を表示できます。**[分析（Analysis）]** > **、[接続ヘッダー（Connections Header）]** > **[イベント（Events）]** の順に選択し、**[接続イベント（Connection Events）]** ページにアクセスします。**[接続イベントのテーブルビュー（Table View of Connection Events）]** タブで、[Encrypted Visibility] と [IoC] フィールドを手動で選択する必要があることに注意してください。

EVE の QUIC フィンガープリント

Snort は、EVE に基づいて Quick UDP Internet Connections（QUIC セッション）内のクライアントアプリケーションを識別できます。QUIC フィンガープリントでは次を実行できます。

- 復号を有効にせずに QUIC でアプリケーションを検出する。
- 復号を有効にせずにマルウェアを特定する。
- サービスアプリケーションを検出する。QUIC プロトコルで検出されたサービスに基づいて、アクセスコントロールルールを割り当てることができます。

EVE の設定

手順

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 **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（EVE）** の横にある **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 [アプリケーション検出にEVEを使用（Use EVE for Application Detection）]：このトグルボタンはデフォルトで有効になっています。つまり、EVE はクライアント アプリケーションをプロセスに割り当てることができます。

接続イベントまたは統合イベントの [暗号化された可視性フィンガープリント（Encrypted Visibility Fingerprint）] 列ヘッダーに EVE のフィンガープリント情報が追加されます。収集された EVE データをさらに分析する場合は、フィンガープリント情報を右クリックしてドロップダウンメニューを開くことができます。メニューで、**[Encrypted Visibility Engineプロセス分析を表示（View Encrypted Visibility Engine Process Analysis）]** をクリックして、Cisco Secure

Firewall アプリケーション検出器のサイトに移動し、フィンガープリント、VDB バージョンなどの詳細を確認します。同じフィンガープリント文字列を持つ異なる行と、それらに関連付けられている潜在的なプロセス名およびその拡散度が表示されます。拡散度は、データ収集システム内の特定のフィンガープリントに関連付けられたプロセスの頻度を示します。プロセス名を選択し、[リクエストの送信（Submit Request）] をクリックすると、EVE のプロセス検出の不一致に関するフィードバックを送信することができます。たとえば、検出されたプロセス名が送信されているトラフィックと一致しない場合や、特定のフィンガープリントについてプロセス名がまったく検出されない場合に、リクエストを送信できます。

[Cisco Secure Firewallアプリケーション検出器（Cisco Secure Firewall Application Detectors）] ページで追加の詳細を表示するためのアクセス権は、現在、シスコ以外の電子メールアドレスを持つユーザーは利用できません。

[アプリケーション検出にEVEを使用（Use EVE for Application Detection）] トグルボタンを無効にした場合：

- AppID で識別されたクライアントがプロセスに割り当てられ、EVE プロセスとスコアは表示されますが、EVE で検出されたプロセスからアプリケーションへのマッピングはなく、アクションも実行されません。イベントの詳細は、[接続イベント（Connection Events）] または [統合イベント（Unified Events）] で確認できます。接続イベントの違い（アプリケーションの割り当ての有無）を確認するには、[クライアントアプリケーション（Client Application）] 列ヘッダーを確認します。
- 接続イベントまたは統合イベントの [暗号化された可視性フィンガープリント（Encrypted Visibility Fingerprint）] フィールドは空です。

ステップ 7 、**[脅威の確実性レベルに基づくマルウェアプロセスをブロック（Block Malware Processes Based on Threat Confidence Level）]** トグルボタンを有効にして、EVE の脅威の確実性レベルに基づいて、プレフィックス 「*malware_*」 という悪意のあるクライアントプロセスをブロックします。

デフォルトのブロックしきい値は 99% で、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、トラフィックはブロックされます。
- 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。

（注）
EVE がトラフィックをブロックした場合、**[接続イベント（Connection Events）]** ページの **[理由（Reason）]** 列のヘッダーに **[Encrypted Visiblity ブロック（Encrypted Visiblity Block）]** と表示されます。

ステップ 8 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（[非常に低い（Very Low）] ～ [非常に高い（Very High）] の範囲）。

ステップ 9 今後さらに細かく制御するため、**[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 脅威確実性レベルを割り当てることができるようになりました。デフォルトのブロックしきい値は 99% です。

注意
最適なパフォーマンスを確保するために、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。

Encrypted Visibility Engine イベントを表示する

[Encrypted Visibility Engine] を有効にして、アクセス コントロール ポリシーを展開すると、システムを介してライブトラフィックの送信を開始できます。**[接続イベント（Connection Events）]** ページまたは **[統合（Unified Events）]** ページではログに記録された接続イベントを表示できま。

Firewall Management Center の接続イベントにアクセスするには、次の手順を実行します。

手順

ステップ 1 **[分析（Analysis）]** > **[接続ヘッダー（Connections Header）]** > **[イベント（Events）]** の順に選択します。
ステップ 2 [接続イベントのテーブルビュー（Table View of Connection Events）] タブをクリックします。

[統合イベント（Unified Events）] ページでは、接続イベントも確認できます。**[分析（Analysis）]** > **[統合イベント（Unified Events）]** の順に選択し、**[統合イベント（Unified Events）]** ページにアクセスします。

Encrypted Visibility Engine は、接続を確立するクライアントプロセスとクライアントのオペレーティングシステム（OS）を特定し、プロセスにマルウェアが含まれているかどうかを示します。

[接続イベント（Connection Events）] ページでは、 Encrypted Visibility Engine に追加されたこれらの列を明示的に有効化する必要があります。

- **EVEプロセス名**
- **EVEプロセスの確実性スコア**
- **EVE脅威の確実性**
- **EVE脅威の確実性スコア**
- **[Detection Type]**

これらのフィールドの詳細については、*Cisco Secure Firewall Management Center Administration Guide* の「接続およびセキュリティ関連接続」イベントフィールドを参照してください。

（注）
プロセスにアプリケーションが割り当てられている場合、**[接続イベント（Connection Events）]** ページの **[検出タイプ（Detection Type）]** 列には、**Encrypted Visibility Engine** が表示されます。これは、クライアントアプリケーションが Encrypted Visibility Engine で特定されたことを示します。アプリケーションをプロセス名に割り当てないと、**[検出タイプ（Detection Type）]** 列には、**AppID** が表示されます。これは、クライアントアプリケーションと特定したエンジンが、AppID であることを示します。

EVE ダッシュボードの表示

次のダッシュボードでは、EVE 分析情報を表示できます。

始める前に

- アクセス コントロール ポリシーの **[詳細設定（Advanced Settings）]**で、**[Encrypted Visisibility Engine（EVE）]** を有効にする必要があります。
- **[検出されたプロセスとの接続（Connections with Detected Process）]** および **[悪意のあるプロセス（Malicious Processes）]** ウィジェットを表示するには、デバイスで Firewall Threat Defense バージョン 7.7 以降が実行されている必要があります。

手順

ステップ 1 **[概要（Overview）]** > **[ダッシュボード（Dashboards）]** の順に選択し、**[ダッシュボード（Dashboards）]** をクリックします。

ステップ 2 **[概要ダッシュボード（Summary Dashboard）]** ウィンドウで、**[Encrypted Visibility Engine]** タブをクリックします。

ステップ 3 次のダッシュボードを表示できます。

- **[検出されたプロセス（Discovered Processes）]**：ネットワークと接続数で使用される上位クライアントプロセスを表示します。テーブルのプロセス名をクリックすると、[接続イベント（Connection Events）]ページのフィルタリングされたビューが表示されます。このビューはプロセス名でフィルタリングされています。
- **[脅威の確実性（Threat Confidence）]**：確実性レベル別に接続を表示します。テーブル内の脅威の信頼レベルをクリックすると、[接続イベント（Connection Events）]ページのフィルタリングされたビューが表示されます。このビューは、信頼レベルによってフィルタリングされています。

- **[検出されたプロセスを使用して接続（Connections with Detected Process）]**：EVE がクライアントプロセスを識別した接続の総数を表示します。
- **[悪意のあるプロセス（Malicious Processes）]**：EVE が識別した悪意のあるクライアントプロセスの数を、高いおよび非常に高い脅威の確実性レベルで表示します。

EVE 例外ルールの設定

Encrypted Visibility Engine（EVE）例外ルールを作成して、EVE のブロックアクションをバイパスすることで、信頼できる接続とサービスの継続性を維持できます。プロセス名、送信元および宛先 IP アドレス/FQDN およびダイナミックオブジェクトなどの属性を例外ルールに追加できます。たとえば、信頼ネットワークに対する EVE のブロック判定をバイパスできます。バイパスされたネットワーク内のすべての接続は、脅威の確実性レベルに基づいて EVE のブロック判定から除外されます。

手順

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 **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（EVE）** の横にある **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)] トグルボタンをクリックして有効にします。

ステップ 6 **[EVE 脅威確実性レベル（EVE threat confidence level）]** トグルボタンに基づいて ブロックを有効化し、EVE の脅威確実性レベルに基づいてトラフィックをブロックします。

ステップ 7 [例外ルールの追加（Add Exception Rule）] をクリックし、以下の属性を 1 つ以上追加します。

a) [プロセス名（Process Name）] タブで、EVE で識別されたプロセス名を入力し、ウィンドウの右側にある [プロセスに追加（Add to Process）] をクリックします。

同じ例外ルールに複数のプロセス名を追加できます。プロセス名に基づく EVE 例外リストは、EVE で識別されるプロセス名でのみ機能します。この名前では、大文字と小文字やスペースの有無が区別されます。

b) [ネットワークオブジェクト（Network Objects）] タブで、次のいずれかを実行します。

- リストから 1 つ以上の IP アドレスまたは FQDN を選択し、[送信元ネットワークに追加（Add to Source Network）] または [宛先ネットワークに追加（Add to Destination Network）] をクリックします。

- **[選択した送信元ネットワーク（Selected Source Network）]** または **[選択した接続先ネットワーク（Selected Destination Network）]** で、IP アドレスを手動入力し、**Add** (＋) アイコンをクリックして、それを選択したネットワークに追加します。

c) [ダイナミック属性（Dynamic Attributes）] タブでダイナミックオブジェクトを選択し、[選択したダイナミックオブジェクト（Selected Dynamic Objects）] リストに追加します。

ダイナミックオブジェクトの作成または操作の詳細については、『Secure Firewall Management Center デバイス設定ガイド』の「初めてのダイナミックオブジェクトの作成」または「ダイナミックオブジェクトの操作」セクションを参照してください。

d) （任意）すべてのタブで使用可能な [コメント（Comment）] フィールドに、EVE 例外ルールに必要な属性を追加する理由を入力できます。

ステップ 8 [保存（Save）] をクリックして EVE 例外ルールを保存します。

ステップ 9 アクセス コントロール ポリシーをデバイスに保存して展開します。

（注） 接続が例外ルールに一致すると、EVE のブロック判定がバイパスされます。EVE のアクションは、**[接続イベント（Connection Events）]** または **[統合イベント（Unified Events）]** ページで表示できます。[理由（Reason）] 列ヘッダーでは、このような EVE がバイパスされたトラフィックの識別に対して、[EVE除外（EVE Exempted）] と表示されます。

統合イベントからの例外ルールの追加

[統合イベント（Unified Events）] ページを使用すると、EVE がブロックする接続の例外ルールを追加することができます。

始める前に

例外リストは、Threat Defense バージョン 7.6.0 以降のみでサポートされます。

手順

ステップ 1 **[分析（Analysis）]** > **[統合イベント（Unified Events）]** をクリックします。

ステップ 2 **[Encrypted Visibilityブロック（Encrypted Visibility Block）]**が理由として指定されている**[理由（Reason）]** 列のセル内で、**Ellipsis**( ) アイコンをクリックします。

ステップ 3 ドロップダウンリストから [EVE例外ルールの追加（Add EVE Exception Rule）] を選択します。

ステップ 4 表示されている [暗号化された可視性エンジン（Encrypted Visibility Engine）] ウィンドウで、ルールが例外リストの一番下に自動的に追加されます。設定を保存して展開する前に、追加したルールを確認して変更することができます。

イベントエンリッチメント

MITRE ATT&CK のコンテキスト エンリッチメントは、Talos 分類と Encrypted Visibility Engine（EVE）から行われます。Talos と EVE の両方のエンリッチメントが、Talos 分類を使用して伝達されます。EVE エンリッチメントは、EVE が有効になっている場合に機能します。EVE の有効化の詳細については、「EVE の設定 （4 ページ）」を参照してください。

[接続イベント（Connection Events）] ページでは、エンリッチメントが行われたイベントコンテンツの一部として追加された、以下の列ヘッダーを表示できます。以下の列を明示的に有効にする必要があります。

- **MITRE ATT&CK**
- その他のエンリッチメント（Other Enrichment）

これらのフィールドの詳細については、*Cisco Secure Firewall Management Center Administration Guide* の「接続およびセキュリティ関連の接続」イベントフィールドを参照してください。

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。