はじめに

シスコ Event Streamer（eStreamer とも称されます）により、外部のクライアント アプリケーションに Firepower システムイベントをストリーミングできます。Management Center からのホストデータ、検出データ、相関データ、コンプライアンスのホワイト リスト データ、侵入データ、ユーザ アクティビティ データ、ファイル データ、マルウェア データ、接続データをストリーミングでき、また、7000 および 8000 シリーズのデバイスからの侵入データをストリーミングできます。

eStreamer は、NGIPSv、Firepower Services、Firepower Threat Defense Virtual、Firepower Threat Defense には対応していない点にご注意ください。これらのデバイスからのイベントをストリーミングするには、そのデバイスが報告する Management Center 上で eStreamer を設定できます。

eStreamer では、カスタム アプリケーション層プロトコルを使用して接続されたクライアント アプリケーションとの通信を行います。eStreamer の目的は、単にクライアントが要求されたデータを戻すことであるため、このガイドは、主に、リクエストされたデータの eStreamer 形式について記述しています。

eStreamer クライアントを作成し、Firepower システムと統合するには 3 つの主要な手順があります:

1. eStreamer アプリケーション プロトコルを使用してメッセージをManagement Center または管理対象デバイスと交換するクライアント アプリケーションを作成します。eStreamer SDK には、参照クライアント アプリケーションが含まれます。
2. クライアント アプリケーションに必要なイベントのタイプを送信するために Management Center またはデバイスを設定します。
3. クライアント アプリケーションを Management Center またはデバイスに接続し、データの交換を開始します。

このガイドでは、eStreamer バージョン 6.1 クライアント アプリケーションを正常に作成し、実行するのに必要な情報を提供します。

eStreamer バージョン 6.1 の主要な変更点

Firepower システム展開を バージョン 6.1 にアップグレードする場合、次に示す変更に注意してください。これらの変更の一部では、eStreamer クライアントを更新する必要があります。

- 以下のブロックが追加されました:
  - ポリシー UUID をセンサー名およびポリシー名にマッピングするために、アクセス コントロール ポリシー メタデータ ブロック 6.0+（4-209 ページ）が追加されました。

- 以下のメタデータ レコードが追加されました:
  - アクセス コントロール ポリシー メタデータ (4-28 ページ)
  - プレフィルタ ポリシー メタデータ (4-30 ページ)
  - トンネルまたはプレフィルタのルールのメタデータ (4-31 ページ)
- 次のブロックを置き換えました:
  - 接続統計データ ブロック 6.0.x (B-198 ページ) を接続統計データ ブロック 6.1+ (4-123 ページ) に置き換えてプレフィルター フィールドおよびトンネル フィールドを追加しました。
  - 接続チャンク データ ブロック 5.1.1 ～ 6.0.x (B-147 ページ) を6.1+ の接続チャンク データ ブロック (4-104 ページ) に置き換えて、元のクライアント IP フィールドを追加しました。
  - ユーザ ログイン情報データ ブロック 6.0.x (B-112 ページ) をユーザ ログイン情報データ ブロック 6.1+ (4-199 ページ) に置き換えて、ポート フィールドとトンネリング フィールドを追加しました。

このガイドの使用方法

eStreamer サービスは、最高レベルで Firepower システムから要求元のクライアントにデータをストリーミングするメカニズムです。このサービスでは、次のデータ カテゴリをストリーミングできます:

- 侵入イベント データおよび追加のイベント データ
- 相関 (コンプライアンス) イベント データ
- 検出イベント データ
- ユーザ イベント データ
- イベントのメタデータ
- ホスト情報
- マルウェア イベント データ

本書では、主に、eStreamer から戻されるデータ構造について説明します。本書の各章は、次のとおりです:

- eStreamer アプリケーション プロトコルについて (2-1 ページ)。この章では、eStreamer 通信の概要、eStreamer クライアント アプリケーションの作成に関する要件の詳細を記述し、eStreamer サービスとのコマンドの送受信に使用される 4 種類のメッセージについて説明します。
- 侵入および相関データ構造の概要 (3-1 ページ)。この章では、侵入検出コンポーネントと相関コンポーネントによって作成されたイベント データを戻すのに使用されるデータ形式および侵入イベントや関連付けイベントを表すのに使用されるデータ形式について説明します。
- 検出と接続データ構造の概要 (4-1 ページ)。この章では、検出データ、ユーザ データ、接続イベント データを戻すために使用されるデータ形式について説明します。
- ホスト データ構造の概要 (5-1 ページ)。この章では、ホスト情報要求メッセージを受信すると完全なホスト情報データを戻すために eStreamer が使用するデータ形式について説明します。

- eStreamer の設定（6-1 ページ）。この章では、Management Center または管理対象デバイスでの eStreamer の設定方法について説明します。この章では、eStreamer コマンド ライン スイッチについても説明し、手動で eStreamer サービスを開始し、停止する方法、および eStreamer を自動的に開始させるために Management Center または管理対象デバイスを設定する方法を提示します。
- データ構造の例（A-1 ページ）。この章では、2 進数形式の eStreamer メッセージ パケットの例を示します。
- レガシー データ構造の概要（B-1 ページ）。この章では、現在出荷されている製品では使用されていませんが、旧クライアントが使用する可能性があるレガシー データ構造の構造について説明します。

前提条件

本ガイドの情報を理解するには、一般に Firepower システムの機能と名称、およびコンポーネントの機能、特に、これらのコンポーネントが生成するさまざまなタイプのイベント データに精通している必要があります。精通していない製品またはその製品固有の用語は、ほとんどが *Firepower eStreamer 統合ガイド* に記述されています。

Firepower システムリリース向け製品バージョン

本ガイドでは、バージョン番号を使用してManagement Center および管理対象デバイスによって生成されるイベントのデータ形式を説明します。Firepower システム製品バージョン表には、主要なリリースごとの各製品バージョンを示します。

表 1-1　　Firepower システム製品バージョン

リリース	Management Center のバージョン（Cisco Unified Communications Manager Version）	マスター Management Center バージョン	侵入センサー バージョン	センサー バージョン	管理対象 Device のバージョン
IMS 3.0	管理コンソール 3.0	該当なし	ネットワーク センサー 3.0	該当なし	該当なし
IMS 3.1	管理コンソール 3.1	該当なし	ネットワーク センサー 3.1	無応答（RNA）センサー 1.0	該当なし
IMS 3.2	管理コンソール 3.2	該当なし	ネットワーク センサー 3.2	無応答（RNA）センサー 2.0	該当なし
3D システム 4.0	Management Center 4.0	該当なし	侵入センサー 4.0	無応答（RNA）センサー 3.0	該当なし
3Dシステム 4.5	Management Center 4.5	該当なし	侵入センサー 4.5	無応答（RNA）センサー 3.5	該当なし
3D システム 4.6.1	Management Center 4.6.1	マスター Management Center 4.6.1	該当なし	該当なし	4.6.1

表 1-1　Firepower システム製品バージョン(続き)

リリース	Management Center のバージョン（Cisco Unified Communications Manager Version）	マスター Management Center バージョン	侵入センサー バージョン	センサー バージョン	管理対象 Device のバージョン
3Dシステム 4.7	Management Center 4.7	マスター Management Center 4.7	該当なし	該当なし	4.7
3Dシステム 4.8	Management Center 4.8	マスター Management Center 4.8	該当なし	該当なし	4.8
3D システム 4.8.0.2	Management Center 4.8.0.2	マスター Management Center 4.8.0.2	該当なし	該当なし	4.8.0.2
3Dシステム 4.9	Management Center 4.9	マスター Management Center 4.9	該当なし	該当なし	4.9
3Dシステム 4.9.1	Management Center 4.9.1	マスター Management Center 4.9.1	該当なし	該当なし	4.9.1
3Dシステム 4.10	Management Center 4.10	マスター Management Center 4.10	該当なし	該当なし	4.10
3Dシステム 4.10.1	Management Center 4.10.1	マスター Management Center 4.10.1	該当なし	該当なし	4.10.1
3Dシステム 4.10.2	Management Center 4.10.2	マスター Management Center 4.10.2	該当なし	該当なし	4.10.2
3Dシステム 4.10.3	Management Center 4.10.3	マスター Management Center 4.10.3	該当なし	該当なし	4.10.3
3Dシステム 5.0	Management Center 5.0	該当なし	該当なし	該当なし	5.0
3Dシステム 5.1	Management Center 5.1	該当なし	該当なし	該当なし	5.1
3Dシステム 5.1.1	Management Center 5.1.1	該当なし	該当なし	該当なし	5.1.1
3Dシステム 5.2	Management Center 5.2	該当なし	該当なし	該当なし	5.2
3Dシステム 5.3	Management Center 5.3	該当なし	該当なし	該当なし	5.3
Firepower システム 5.3.1	Management Center 5.3.1	該当なし	該当なし	該当なし	5.3.1

表 1-1　Firepower システム製品バージョン(続き)

リリース	Management Center のバージョン(Cisco Unified Communications Manager Version)	マスター Management Center バージョン	侵入センサー バージョン	センサー バージョン	管理対象 Deviceのバージョン
Firepower システム 5.4	Management Center 5.4	該当なし	該当なし	該当なし	5.4
Firepower システム 6.0	Management Center 6.0	該当なし	該当なし	該当なし	6.0

表記法

eStreamer メッセージ データ タイプの表記法表には、eStreamer メッセージで使用されるさまざまなデータ フィールド形式を説明するために、本書で使用する名前を示します。eStreamer サービスで使用する数値定数は通常、符号なし整数値です。別途注記のない限り、ビット フィールドには下位ビットを使用します。たとえば、フラグ データの 5 ビットを含む 1 バイト フィールドでは、下位 5 ビットにデータが含まれています。

表 1-2　eStreamer メッセージ データ タイプの表記法

データ タイプ	説明
nn-ビット フィールド	nn ビットのビット フィールド
バイト	任意の形式のデータを含む 8 ビット バイト
int8	符号付き 8 ビット バイト
uint8	符号なし 8 ビット バイト
int16	符号付き 16 ビット整数
uint16	符号なし 16 ビット整数
int32	符号付き 32 ビット整数
uint32	符号なし 32 ビット整数
uint64	符号なし 64 ビット整数
string	文字データを格納する可変長フィールド。
[n]	指定されたデータ タイプの n インスタンスを示す上記のデータ タイプに続く配列添字(たとえば、uint8 [4])
変数	さまざまなデータ タイプの収集
BLOB	パケットからキャプチャされるとき、指定されていないタイプ、通常、生データの 2 進数オブジェクト

IP アドレス

シスコデータベースは、2 進数形式の同じフィールドに IPv4 アドレスと IPv6 アドレスを保存します。IPv6 アドレスを取得するには、16 進表記に変換します。例: `20010db80000000000000000000004321`データベースでは、RFC に準拠して 80 ～ 95 ビットに 1 を取り込むことによって IPv4 アドレスを保存し、これによって無効な IPv6 アドレスが生成されます。たとえば IPv4 アドレス 10.5.15.1 は `00000000000000000000FFFF0A050F01` として保存されます。