FireSIGHT システムを使用したビデオ ストリーミング トラフィックの検出

目次

概要

ネットワークのビデオ トラフィックを検出するには、FireSIGHTシステムのアクセス制御機能とURLフィルタリング機能を使用できます。 このドキュメントでFireSIGHTシステムをこのように設定する方法について説明します。

前提条件

要件

このドキュメントの手順は、制御ライセンスおよびURLフィルタ ライセンスはFireSIGHT Management Centerにインストールされている必要があります。

使用するコンポーネント

このドキュメントの情報は、次のハードウェアとソフトウェアのバージョンに基づいています。

- FireSIGHT 管理センター
- ソフトウェア バージョン 5.2 以降

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

ビデオ トラフィックのストリーミングも検出

アプリケーション フィルタの使用方法

アクセス制御ポリシー機能はトラフィックをすべきブロック、信頼またはオンかどうかを判断するためにフィルタとしてアプリケーションを使用できるようになります。 ビデオ アプリケーションをフィルタを使用してトラフィックをストリーミングを検出するには、次の手順を実行します:

ステップ 1： 環境に適したゾーン、ネットワークと運用を使用してアクセス コントロール ルールを作成します。

ステップ 2： [Applications] タブを選択します。 アプリケーション フィルタ セクションで多く**の選択肢が**あります。

手順 3： アプリケーション フィルタ セクション**で**検索フィルタを200で使用できるアプリケーション**のマルチメディア (** TV/video) という名前のスクロールします。 1つのアプリケーション、またはアプリケーションすべてを選ぶことができます。 このフィルタのすべてのアプリケーションを選択してもRule]ボタンに、**フィルタ]**に一致するすべての**アプリケーションを選択**します。

> **ヒント**： アプリケーションを理解するために、各アプリケーション*の右側*にある情報アイコンをクリックします。 これはアプリケーションの説明、リスク、タイプ、ビジネス関連性などを提供。

ステップ 4： また、アプリケーション (フィルタ)]**セクション**の下にあるタグのカテゴリを**表示する**ことができます。 マルチメディア (**TV/video) の**カテゴリ**にリストされていないもので、追加する他**のアプリケーションの提供、ビデオ会議、UDPプロトコル、Webカメラ、ストリーミング ビデオ**の共有などのさまざまなタグを**検索します。

ステップ 5： マネージド デバイスにアクセス制御ポリシーを保存して再適用します。

> **ヒント**： 新しいアプリケーション タイプは脆弱性データベース (VDBアップデートに追加されます。 カテゴリ、以前のアプリケーションに最新の機能を検出するために現在の割り当てからバージョンが保持されます。

URL フィルタリングの使用方法

また、ビデオのURLフィルタリングを使用してトラフィックをストリーミングを検出できます。 アクセス コントロール ルールを追加するときには、次の手順を実行してください:

ステップ 1： [URLs] タブを選択します。

ステップ 2： [Streaming Media] カテゴリを選択します。 既知のリスクが高く、に関係するメディア レピュテーション レベルを**選択**できます。 これは新しいURLが、定期的に更新する必要があるURLフィルタリング データベースに追加され、新しいビデオ トラフィックをストリーミングを検出できるようになります。

手順 3： ルールを追加した後、アクセス制御ポリシーを保存してマネージド デバイスに再度適用します。

トラフィックをストリーミング ビデオの録画

アプリケーションまたはURLフィルタを設定したら、これらの接続を追跡するログを有効にすることができます。 そのために、録音**タブを選択します**。

トラフィックをストリーミング ビデオをブロックするアクセス コントロール ルールを設定して接続を**行うための接続の開始時点**でログを選択します。 フローのネットワーク接続と期間に使用中のビデオ タイプについて生成するルールを行うには接続の**終了にログを選択します**。

> **注:** UDPアプリケーションはコネクションレス型なので、1時間が送信元と宛先のUDPトラフィックなしで通過までUDPセッションは完了とは見なされません。