

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

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[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](#)

[トラフィックをストリーミング ビデオの録画](#)

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

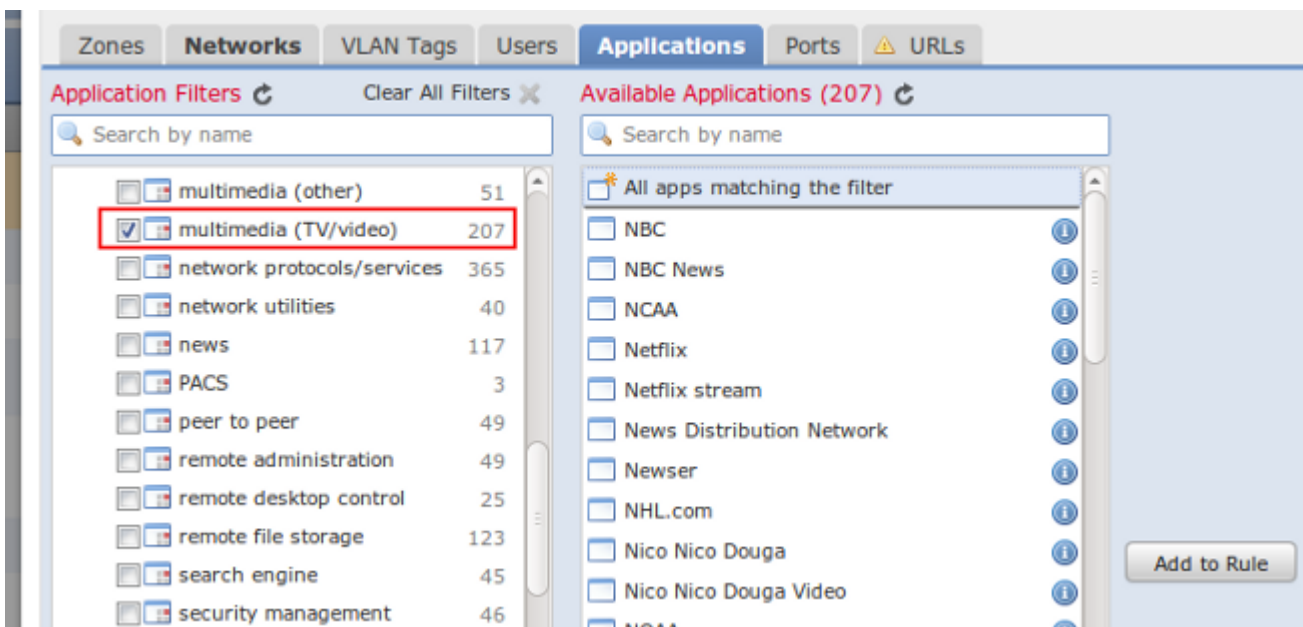
アクセス制御ポリシー機能はトラフィックをすべきブロック、信頼またはオンかどうかを判断するためにフィルタとしてアプリケーションを使用できるようになります。ビデオアプリケーションをフィルタを使用してトラフィックをストリーミングを検出するには、次の手順を実行します:

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。

ステップ 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で使用す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。

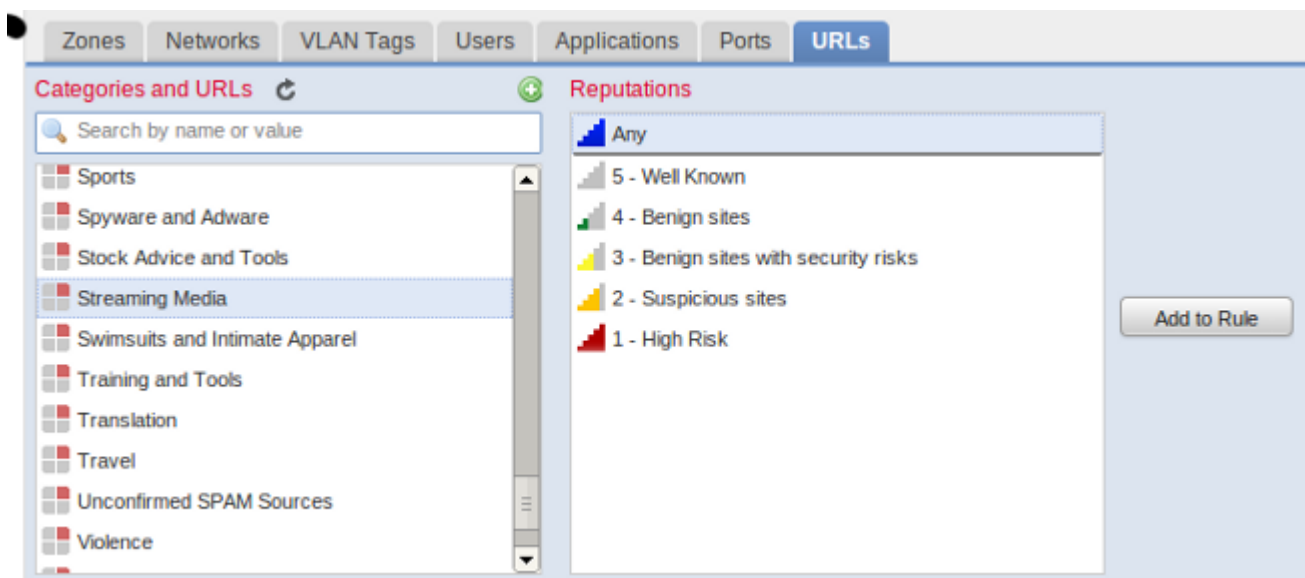
URL フィルタリングの使用方法

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。

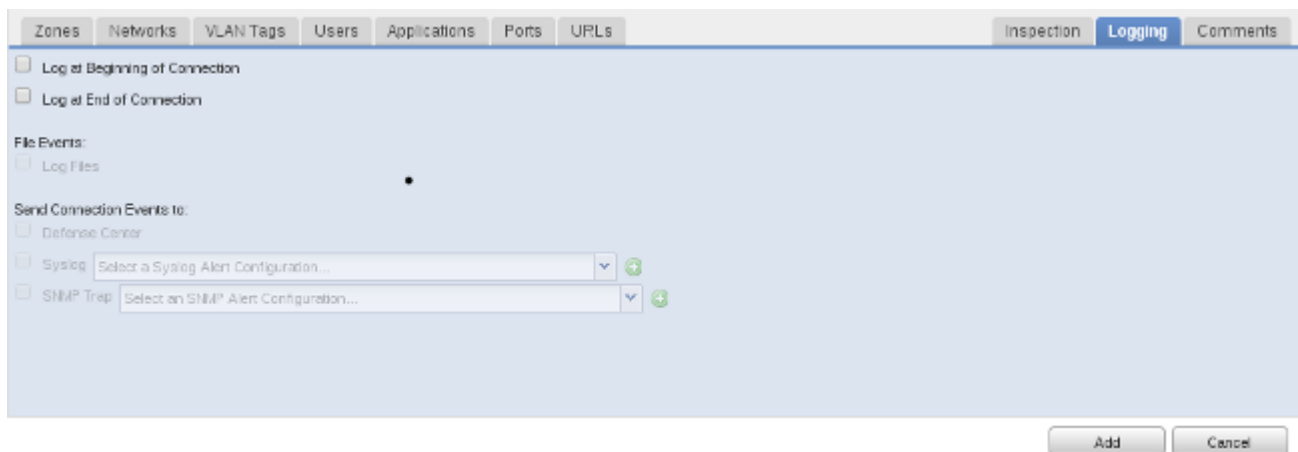
ステップ 2：[Streaming Media] カテゴリを選択します。既知のリスクが高く、に關係するメディアレピュテーションレベルを選択できます。これは新しいURLが、定期的に更新する必要があるURLフィルタリングデータベースに追加され、新しいビデオトラフィックをストリーミングを検出できるようになります。

ステップ 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。