FireSIGHT システムでの URL フィルタリングの設定例

目次

概要

このマニュアルでは、FireSIGHT システム上で URL フィルタリングを設定する手順について説明します。 FireSIGHT 管理センターの URL フィルタリング機能を使用すると、モニタされたホストからの暗号化されない URL リクエストに基づいてネットワークをトラバースするトラフィックを判断するためにアクセス コントロール ルールの条件を記述することができます。

前提条件

要件

このドキュメントでは、URL フィルタリング ライセンスおよびポートに対するいくつかの特定の要件について説明します。

URL フィルタリング ライセンスの要件

FireSIGHT 管理センターでは、URL 情報の更新について定期的にクラウドにコンタクトするための URL フィルタリング ライセンスが必要です。 URL フィルタリング ライセンスがない状態でもアクセス コントロール ルールのカテゴリおよびレピュテーション ベースの URL 条件を追加することができます。 ただし、最初に URL フィルタリング ライセンスを FireSIGHT 管理センターに追加し、ポリシー適用対象のデバイス上で有効にするまでアクセス コントロール ポリシーを適用できません。

URL フィルタリング ライセンスが期限切れになると、カテゴリおよびレピュテーション ベースの URL 条件を持つアクセス コントロール ルールは URL のフィルタリングを停止し、FireSIGHT 管理センターはクラウド サービスにコンタクトしなくなります。 URL フィルタリングのライセ

ンスがない場合、許可するかブロックするように個々の URL または URL のグループを設定することができますが、ネットワーク トラフィックをフィルタするために URL カテゴリまたはレピュテーション データは使用することはできません。

ポート要件

SireSIGHT システムはクラウド サービスと通信するためにポート 443/HTTPS および 80/HTTP を使用します。 ポート 443/HTTPS は双方向で開き、ポート 80/HTTP へのインバウンド アクセスを FireSIGHT 管理センター上で許可する必要があります。

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。

- FirePOWER アプライアンス： 7000 シリーズ、8000 シリーズ
- 次世代侵入防御システム（NGIPS）仮想アプライアンス
- 適応型セキュリティ アプライアンス（ASA）FirePOWER
- Sourcefire 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。

設定

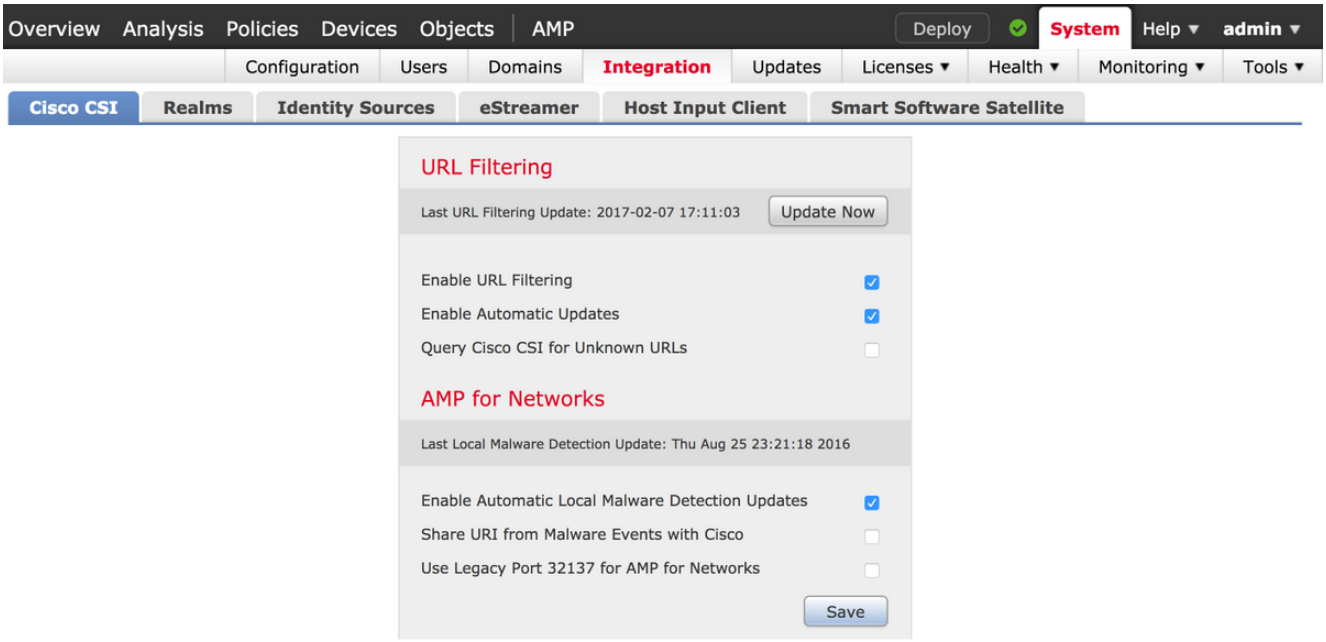
FireSIGHT 管理センター上での URL フィルタリングの有効化

URL フィルタリングを有効にするには、これらのステップを完了します。

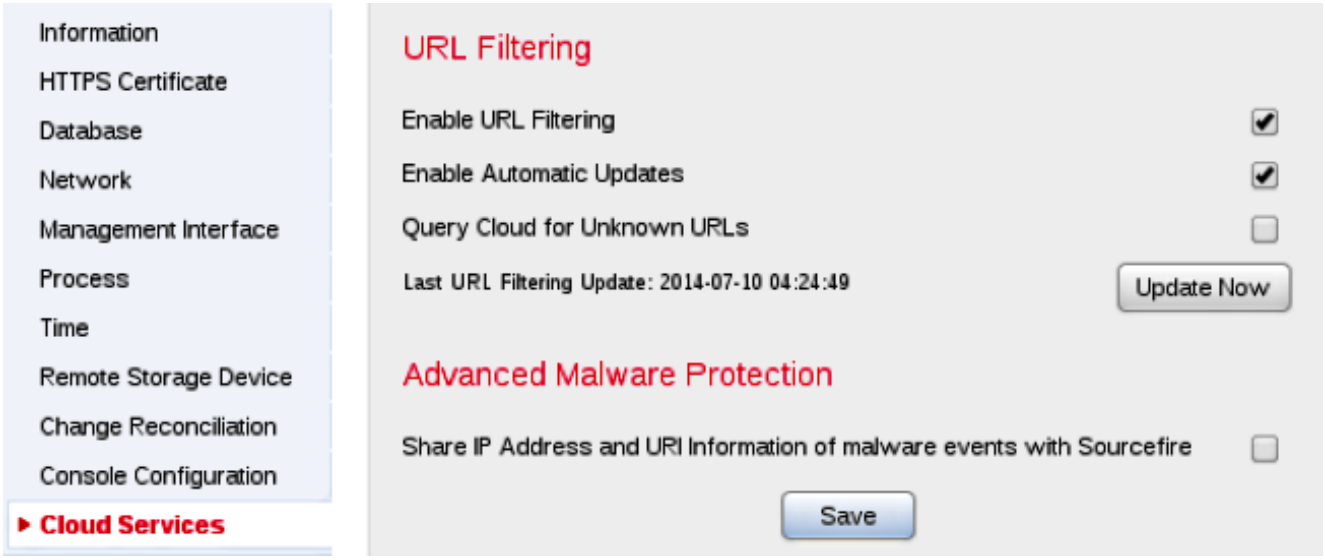
1. FireSIGHT 管理センターの Web ユーザ インターフェイスにログインします。

2. 実行するソフトウェア バージョンに基づくナビゲーションは異なっています:

   バージョン 6.1.x で、**システム > 統合 > Cisco CSI を**選択して下さい。



バージョン 5.x で、**システム > ローカル > 設定を**選択して下さい。 **Cloud サービスを**選択して下さい。



3. URL フィルタリングを有効に するために**イネーブル URL フィルタリング な** チェックボックスをチェックして下さい。
4. 任意で、自動アップデートをイネーブルにするために**イネーブル自動 Updates チェックボックスを**チェックして下さい。 このオプションは、システムが定期的にクラウド サービスに接続して、アプライアンスのローカル データ セットに含まれる URL データの更新を取得できるようにします。

   注: クラウド サービスは一般的に 1 日あたりのデータを一度アップデートするが、自動更新を有効に する場合 FireSIGHT Management Center に情報が現在常にであることを 30 分毎に確認させます。 毎日の更新は小規模である傾向がありますが、最終更新日から 5 日以上経過している場合、新しい URL フィルタリング データのダウンロードに最長で 20 分かかる場合があります。 一度更新がダウンロードされると、更新自体を実行するのに最大 30 分かかります。

5. 任意で、未知 URL のためにクラウド サービスを問い合わせるために未知 URL チェックボックスの**未知 URL があるようにクエリ Cloud を**確認して下さい。 このオプションは、監視

対象ネットワーク上で誰かがローカル データ セットに存在しない URL を参照しようとしたときに、システムが Sourcefire クラウドを照会できるようにします。 クラウドが URL のカテゴリまたはレピュテーションを識別できない場合、または FireSIGHT 管理センターがクラウドに接続できない場合、その URL はカテゴリまたはレピュテーション ベースの URL 条件を含むアクセス コントロール ルールと一致しません。

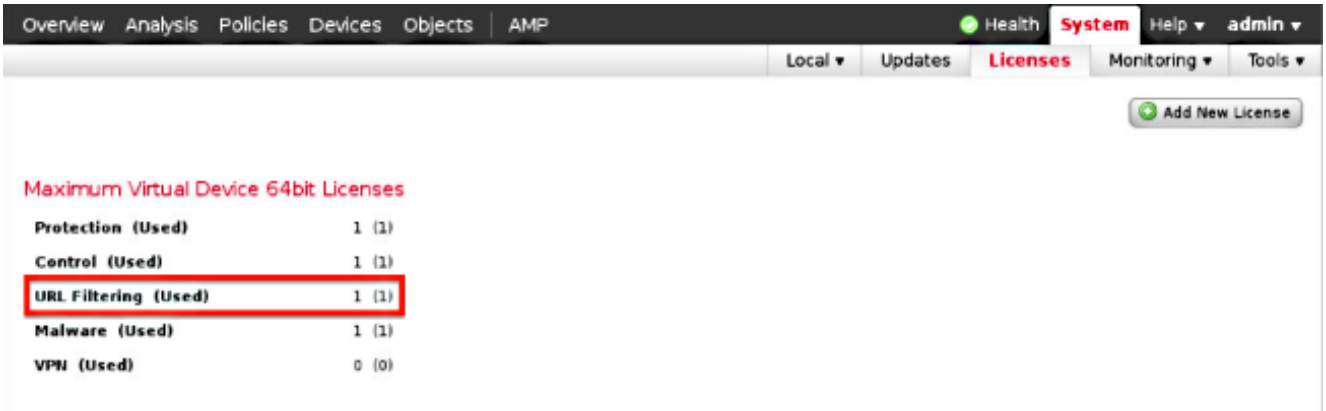
注: URL に手動でカテゴリやレピュテーションを割り当てることはできません。 プライバシー上の理由などで、未分類の URL を Sourcefire クラウドでカタログ化したくない場合は、このオプションを無効にします。

6. [Save] をクリックします。 URL フィルタリング設定が保存されます。

注: URL フィルタリングが最後に有効になってから経過した時間に応じて、または URL フィルタリングを今回初めて有効にしたかどうかによって、FireSIGHT 管理センターがクラウド サービスから URL フィルタリング データを取得します。

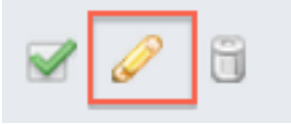
管理デバイス上の URL フィルタリング ライセンスの適用

1. URL フィルタリング ライセンスが FireSIGHT 管理センターにインストールされているかどうかを確認します。 [System] > [Licenses] ページに移動してライセンスのリストを検索します。

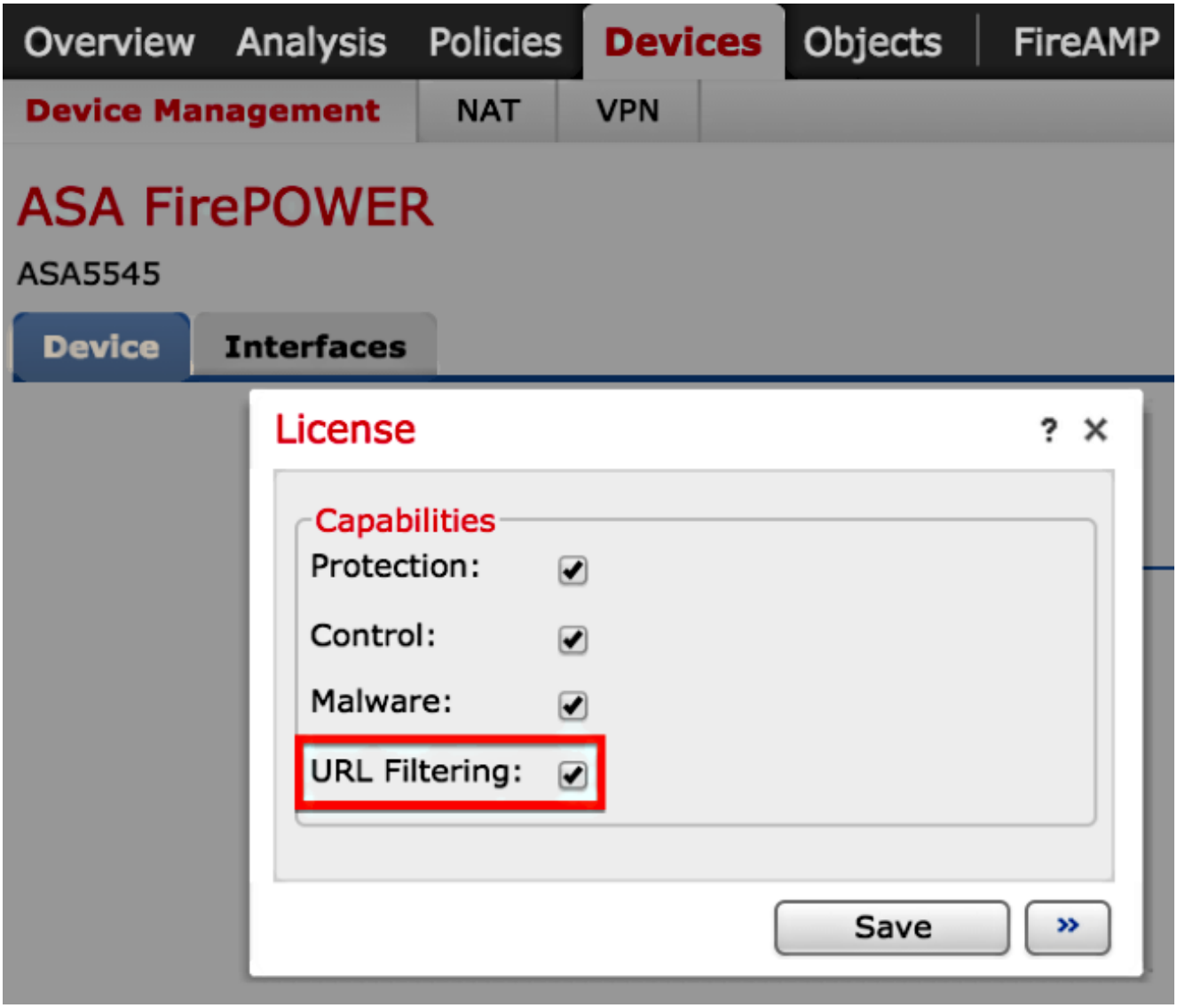


2. [Devices] > [Device Management] ページに移動して、URL フィルタリング ライセンスがトラフィックをモニタするデバイス上に適用されるかどうかを検証します。

3. URL フィルタリング なライセンスがデバイスで加えられない場合、設定を編集するために**鉛筆**アイコンをクリックして下さい。 アイコンは、デバイス名の横にあります。



4. [Devices] タブから、デバイス上で URL フィルタリング ライセンスを有効にできます。



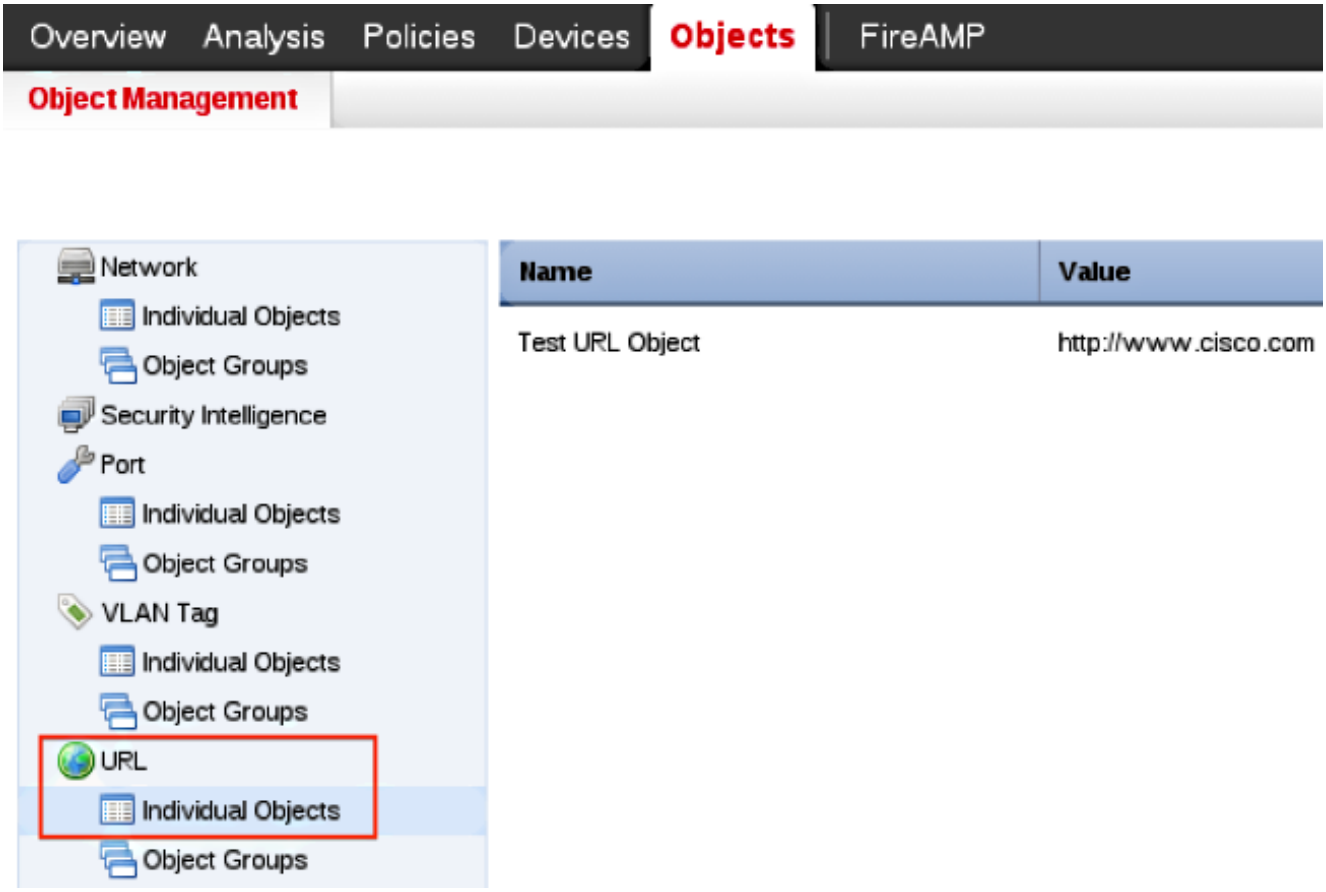
5. ライセンスを有効にして変更を保存した後、[Apply Changes] をクリックして管理デバイス上でライセンスを適用する必要があります。

ブロックされた URL カテゴリからの特定のサイトの除外

FireSIGHT 管理センターでは、デフォルトの Sourcefire が提供するカテゴリ レーティングを上書きする URL のローカル レーティングを使用できません。 このタスクを実行するには、アクセス コントロール ポリシーを使用する必要があります。 これらの手順は、ブロック カテゴリから特定のサイトを除外するため、アクセス コントロール ルールで URL オブジェクトを使用する方法を説明しています。

1. **オブジェクト > オブジェクト管理**ページに行って下さい。

2. URL のための**個別のオブジェクトを選択し、追加 URL** ボタンをクリックして下さい。
   [URL Objects] ウィンドウが表示されます。

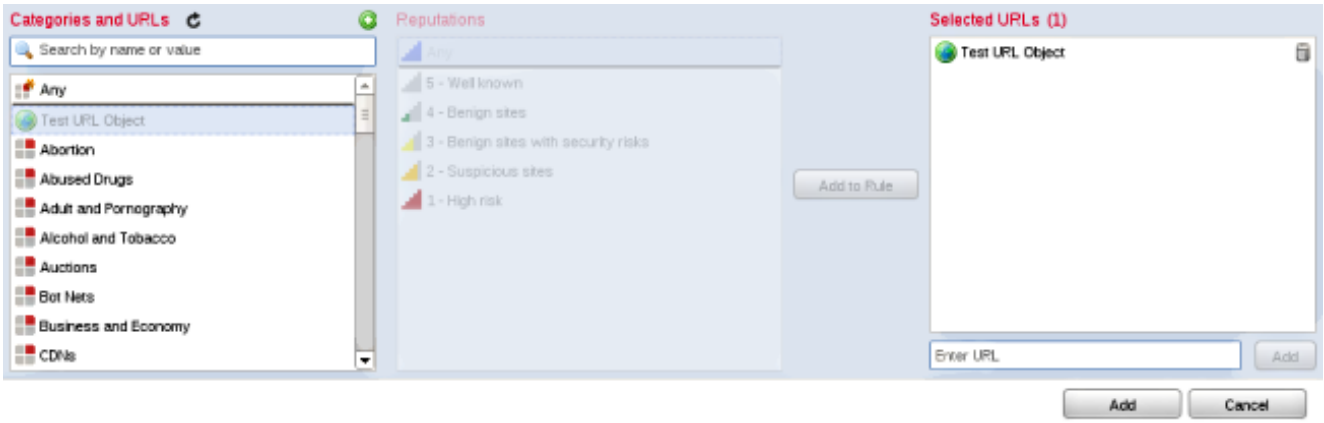


3. 変更を保存した後、**> アクセス制御**『Policies』 を選択 し、アクセス制御ポリシーを編集するために**鉛筆**アイコンをクリックして下さい。

4. [Add Rule] をクリックします。

5. [Allow] アクションで URL オブジェクトをルールに追加し、URL カテゴリ ルールの上位に

配置して、ルール アクションが最初に評価されるようにします。



6. ルールを追加した後、『SAVE』 をクリック し、**適用して下さい。** 新規変更が保存され、アクセス コントロール ポリシーが管理対象アプライアンスに適用されます。

確認

検証またはトラブルシューティング情報については、「関連情報」セクションでリンクされている「**FireSIGHT システム上の URL フィルタリングでのトラブルシューティングの問題**」の記事を参照してください。

トラブルシューティング

検証またはトラブルシューティング情報については、「関連情報」セクションでリンクされている「**FireSIGHT システム上の URL フィルタリングでのトラブルシューティングの問題**」の記事を参照してください。

関連情報

- **FireSIGHT システム上の URL フィルタリングでのトラブルシューティングの問題**
- **テクニカル サポートとドキュメント – Cisco Systems**