

FireSIGHT システムでの URL フィルタリングの設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[URL フィルタリング ライセンスの要件](#)

[ポート要件](#)

[使用するコンポーネント](#)

[設定](#)

[FireSIGHT 管理センター上の URL フィルタリング](#)

[管理デバイス上の URL フィルタリング](#)

[ブロックされた URL カテゴリからの特定のサイトの除外](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

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

FireSIGHTシステムは、クラウドサービスとの通信にポート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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

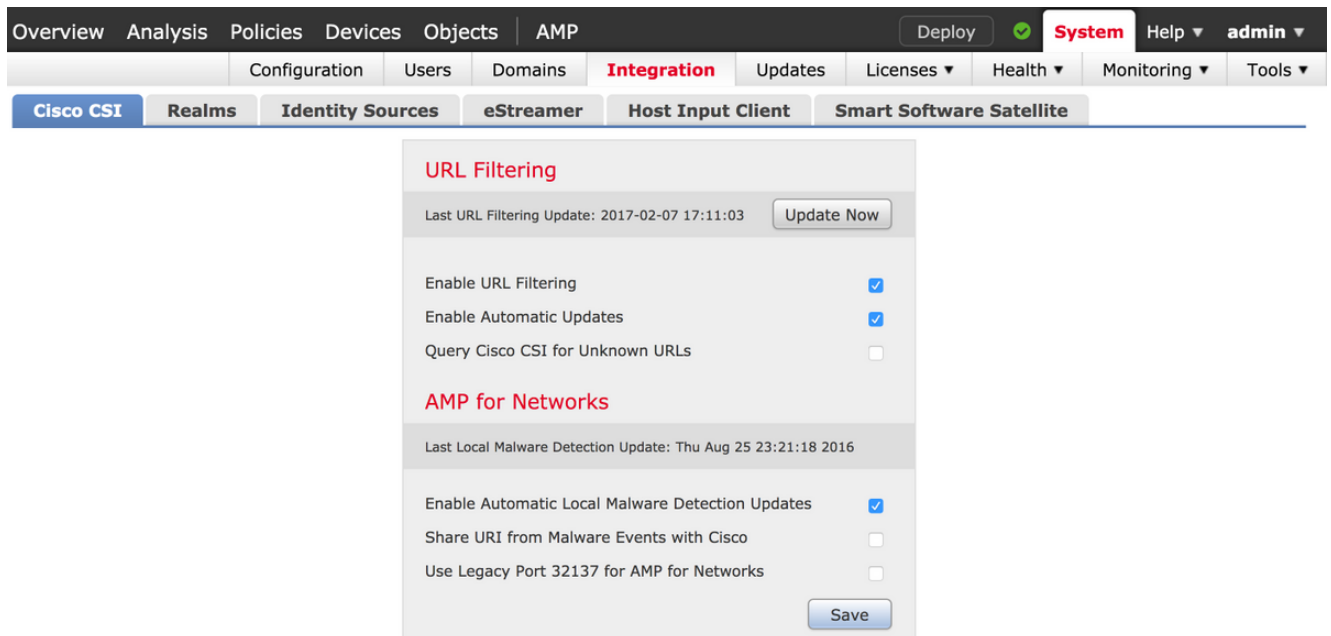
設定

FireSIGHT 管理センター上の URL フィルタリング

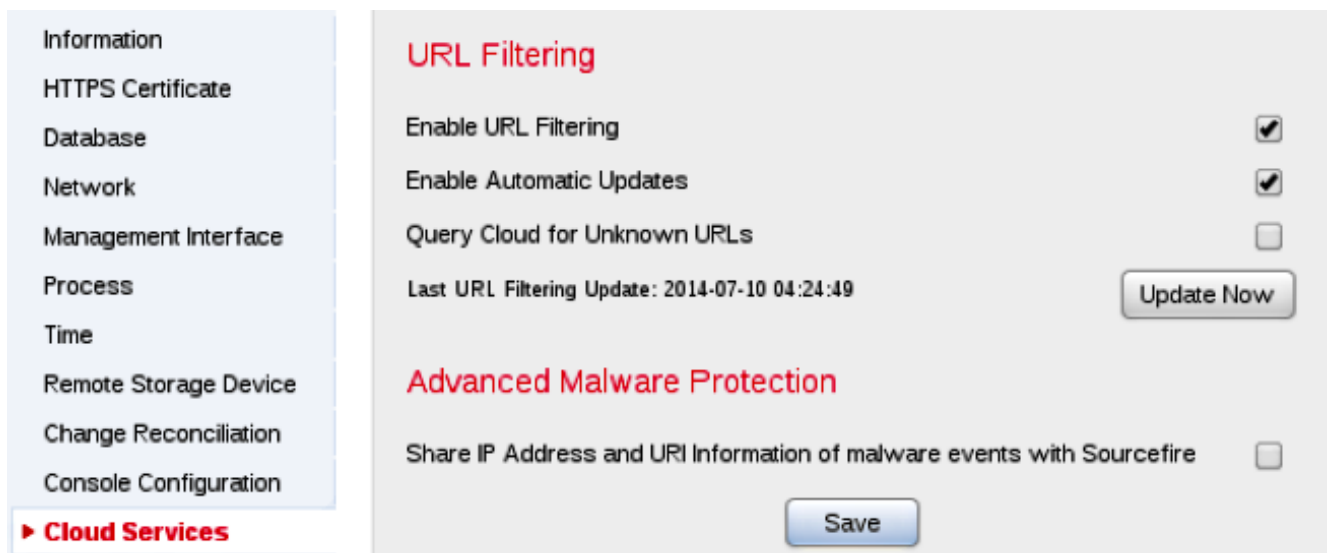
URL フィルタリングを有効にするには、これらのステップを完了します。

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. ナビゲーションは、実行するソフトウェアバージョンによって異なります。

バージョン6.1.xでは、[System] > [Integration] > [Cisco CSI] を選択します。



バージョン5.xでは、**System > Local > Configuration**の順に選択します。[Cloud Services] を選択します。



3. URLフィルタリングを有効にするには、[Enable URL Filtering] チェックボックスをオンにします。
4. 必要に応じて、[Enable Automatic Updates] チェックボックスをオンにして、自動更新を有効にします。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通常、1日に1回データを更新しますが、自動更新を有効にすると、情報が常に最新であることを確認するためにFireSIGHT Management Centerが30分ごとにチェックを行います。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. 必要に応じて、[Query Cloud for Unknown URLs for Unknown URLs] チェックボックスをオンにして、不明なURLのクラウドサービスを照会します。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。

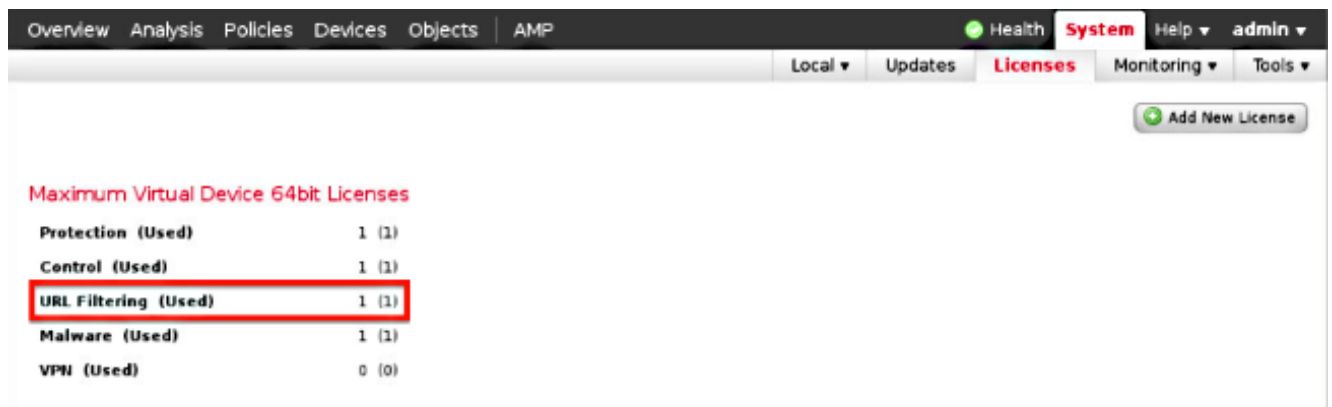
注：URL に手動でカテゴリやレピュテーションを割り当てることはできません。プライベート上の理由などで、未分類の URL を Sourcefire クラウドでカタログ化したくない場合は、このオプションを無効にします。

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

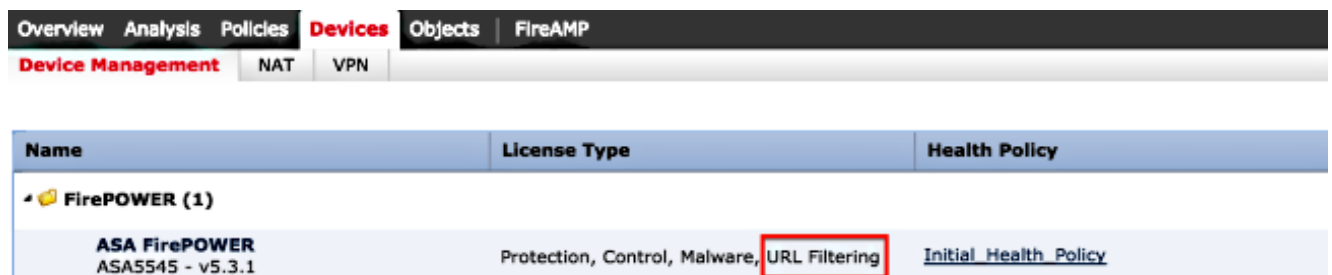
1. URL フィルタリング ライセンスが FireSIGHT 管理センターにインストールされているかどうかを確認します。[System] > [Licenses] ページに移動してライセンスのリストを検索します。



The screenshot shows the 'Licenses' page in the FireSIGHT management console. The navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'AMP'. The 'System' tab is active, and the 'Licenses' sub-tab is selected. A table titled 'Maximum Virtual Device 64bit Licenses' displays the following data:

License Type	Used
Protection	1 (1)
Control	1 (1)
URL Filtering	1 (1)
Malware	1 (1)
VPN	0 (0)

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。



The screenshot shows the 'Device Management' page in the FireSIGHT management console. The navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'FireAMP'. The 'Device Management' sub-tab is selected, and the 'NAT' and 'VPN' tabs are visible. A table displays the following data:

Name	License Type	Health Policy
FirePOWER (1)		
ASA FirePOWER ASA5545 - v5.3.1	Protection, Control, Malware, URL Filtering	Initial Health Policy

3. URL フィルタリングライセンスがデバイスに適用されていない場合は、鉛筆アイコンをクリックして設定を編集します。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。

The screenshot shows the ASA FirePOWER management interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'FireAMP'. Below this, there are sub-tabs for 'Device Management', 'NAT', and 'VPN'. The main content area shows 'ASA FirePOWER' and 'ASA5545'. The 'Device' tab is selected, and the 'License' dialog box is open. The dialog box has a title bar with a question mark and a close button. Inside the dialog, under the 'Capabilities' section, there are four checkboxes: 'Protection:', 'Control:', 'Malware:', and 'URL Filtering:'. The 'URL Filtering:' checkbox is checked and highlighted with a red box. At the bottom right of the dialog, there are 'Save' and '>>' buttons.

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。

 You have unapplied changes



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. [Objects] > [Object Management]ページに移動します。
2. URLとして[Individual Objects]を選択し、[Add URL] ボタンをクリックします。[URL Objects] ウィンドウが表示されます。

URL Objects



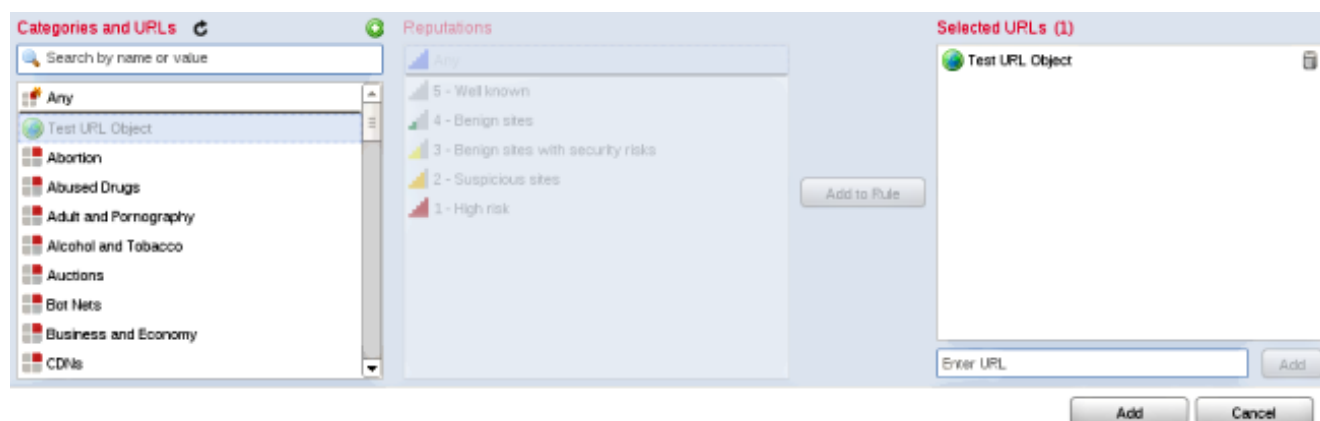
Name:	<input type="text" value="Test URL Object"/>
URL:	<input type="text" value="http://www.cisco.com"/>

A sidebar menu with categories: Network, Security Intelligence, and VLAN Tag. Each category has sub-items for Individual Objects and Object Groups. The 'URL' category is highlighted with a red box.

Name	Value
Test URL Object	http://www.cisco.com

3. 変更を保存したら、[Policies] > [Access Control] を選択し、鉛筆アイコンをクリックしてアクセスコントロールポリシーを編集します。
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. ルールを追加したら、[Save and Apply] をクリックします。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。

トラブルシュート

確認またはトラブルシューティングの情報については、[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](#) 関連情報セクションにリンクされている記事。

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](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。