

FireSIGHT システムでの URL フィルタリングの設定例

目次

[はじめに](#)

[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

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ります:

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。

The screenshot shows the Cisco AMP configuration page. At the top, there are navigation tabs: Overview, Analysis, Policies, Devices, Objects, AMP, Integration, Updates, Licenses, Health, Monitoring, and Tools. Below these are sub-tabs: Cisco CSI, Realms, Identity Sources, eStreamer, Host Input Client, and Smart Software Satellite. The main content area is divided into two sections:

- URL Filtering:**
 - Last URL Filtering Update: 2017-02-07 17:11:03 (Update Now button)
 - Enable URL Filtering:
 - Enable Automatic Updates:
 - Query Cisco CSI for Unknown URLs:
- AMP for Networks:**
 - Last Local Malware Detection Update: Thu Aug 25 23:21:18 2016
 - Enable Automatic Local Malware Detection Updates:
 - Share URI from Malware Events with Cisco:
 - Use Legacy Port 32137 for AMP for Networks:

A Save button is located at the bottom right of the configuration area.

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。

This screenshot shows the same configuration page as above, but with the left sidebar expanded. The 'Cloud Services' option is highlighted in red. The main content area shows the following settings:

- URL Filtering:**
 - Enable URL Filtering:
 - Enable Automatic Updates:
 - Query Cloud for Unknown URLs:
 - Last URL Filtering Update: 2014-07-10 04:24:49 (Update Now button)
- Advanced Malware Protection:**
 - Share IP Address and URI Information of malware events with Sourcefire:

A Save button is located at the bottom right of the configuration area.

- 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。
- 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。

- 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。

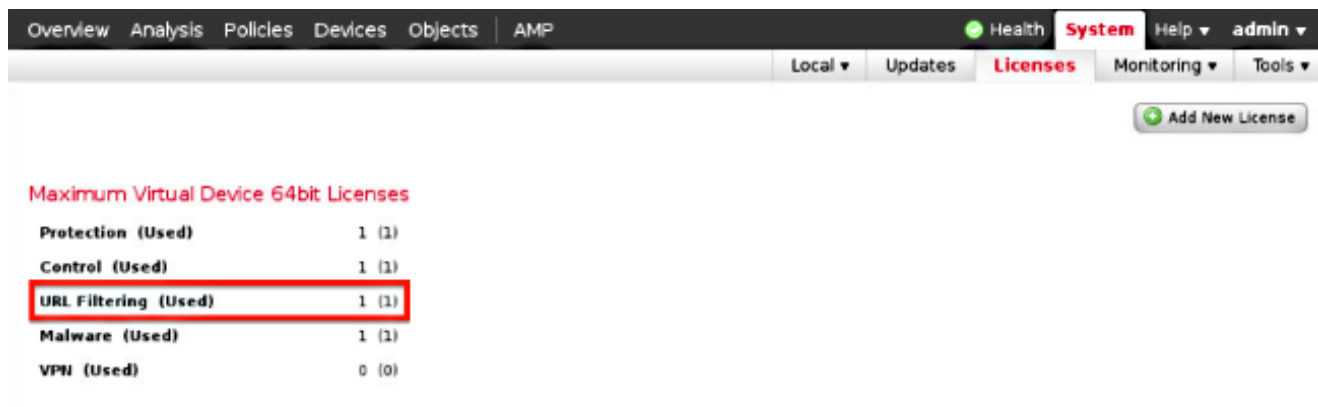
注: URL に手動でカテゴリやレピュテーションを割り当てることはできません。プライバシー上の理由などで、未分類の URL を Sourcefire クラウドでカタログ化したくない場合は、このオプションを無効にします。

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。



The screenshot shows the 'Licenses' page in the FireSIGHT management console. The navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'AMP'. The 'Licenses' tab is active. Below the navigation bar, there is a table titled 'Maximum Virtual Device 64bit Licenses' with the following data:

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

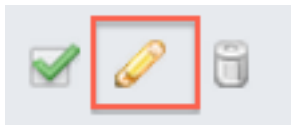
2. [Devices] > [Device Management] ページに移動して、URL フィルタリング ライセンスがトラフィックをモニタするデバイス上に適用されるかどうかを検証します。



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' tab is active. Below the navigation bar, there is a table with 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 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。

Overview Analysis Policies **Devices** Objects | FireAMP

Device Management NAT VPN

ASA FirePOWER

ASA5545

Device Interfaces

License ? X

Capabilities

Protection:

Control:

Malware:

URL Filtering:

Save >>

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**

 **Apply 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. オブジェクト > オブジェクト管理ページに行ってください。
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ください。
[URL Objects] ウィンドウが表示されます。

URL Objects



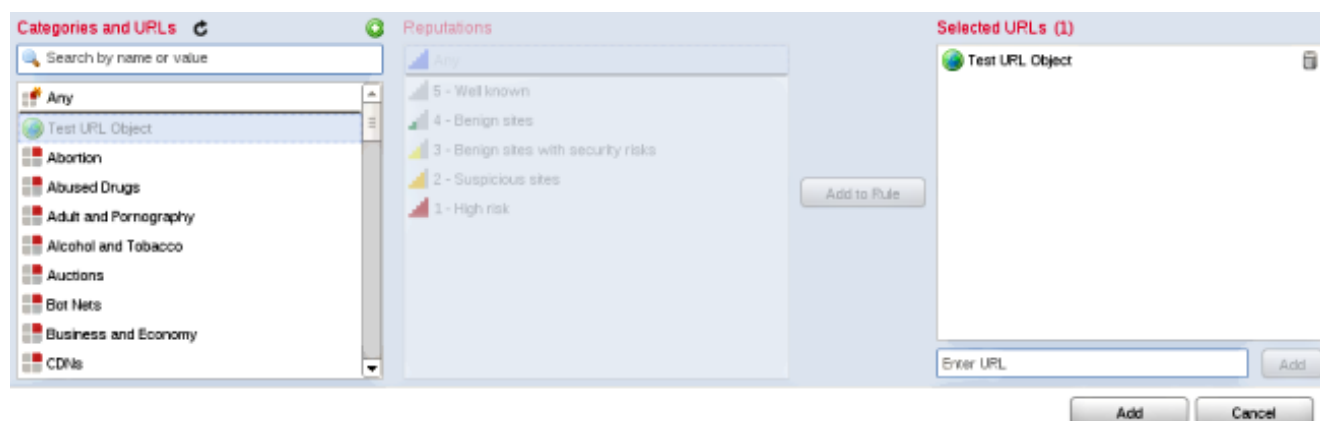
Name:	<input type="text" value="Test URL Object"/>
URL:	<input type="text" value="http://www.cisco.com"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	



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

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ください。
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](#)