

# FireSIGHT システムでの URL フィルタリングに関する問題のトラブルシューティング

## 目次

### [概要](#)

### [URL フィルタリング な ルックアップ プロセス](#)

### [Cloud 接続上の問題](#)

### [ステップ 1: ライセンスをチェックして下さい](#)

[ライセンスはインストールされていますか。](#)

[ライセンスは切れますか。](#)

### [ステップ 2: 健全性アラートをチェックして下さい](#)

### [ステップ 3: DNS 設定をチェックして下さい](#)

### [ステップ 4: 必須ポートへの接続をチェックして下さい](#)

### [アクセスコントロールおよび Miscategorization 問題](#)

[問題 1: 選択解除にされた評判レベルとの URL は許可されまじたり/ブロックされます](#)

[ルール処理は割り当てです](#)

[ルール処理はブロックです](#)

### [URL 選択行列](#)

[問題 2: ワイルドカードはアクセスコントロール ルールではたきません](#)

[問題 3: URL カテゴリおよび評判は読み込まれません](#)

### [関連情報](#)

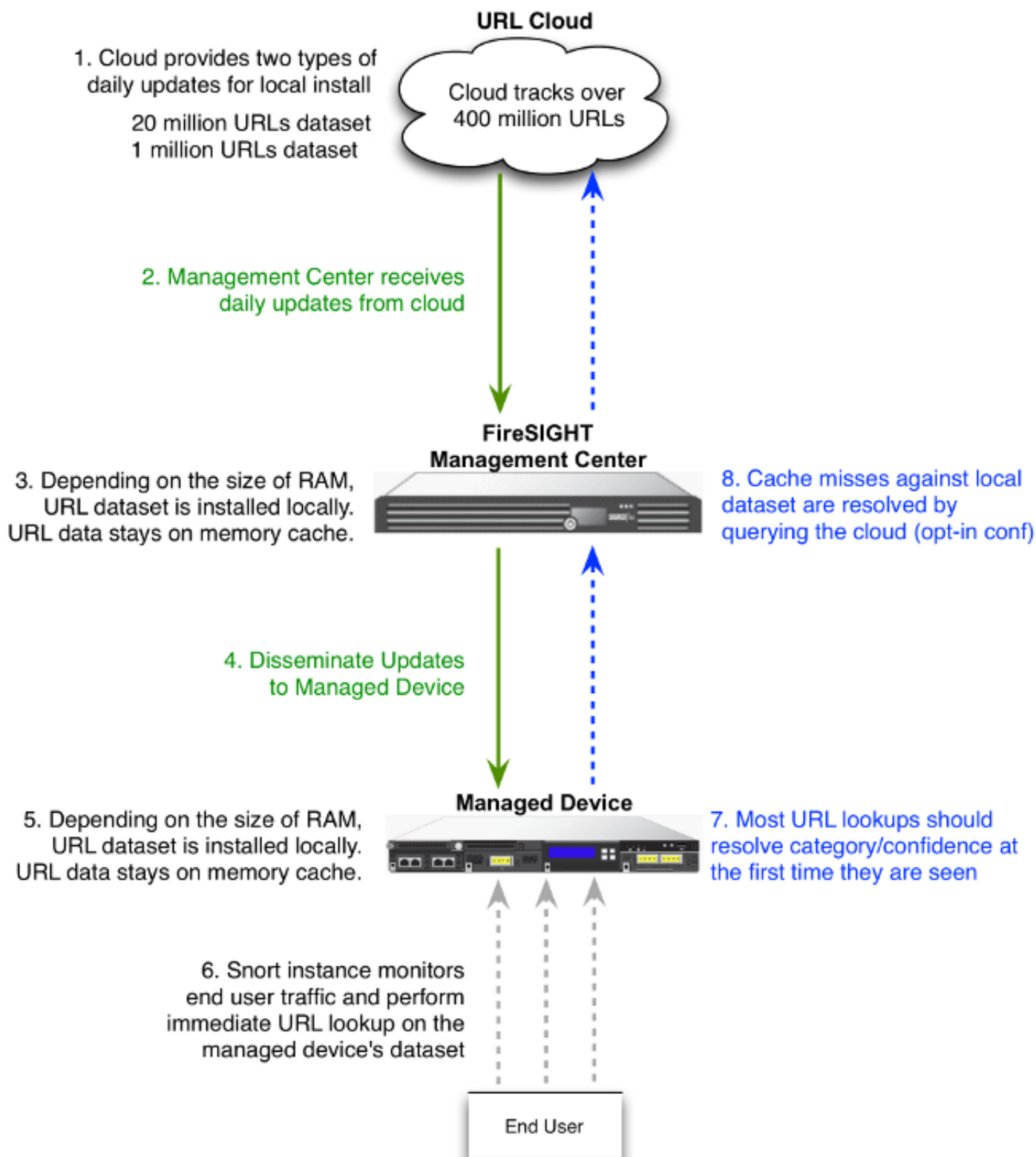
## 概要

この資料は URL フィルタリングにおいてのよくある 問題を記述したものです。FireSIGHT Management Center の URL フィルタリング 機能は監視されたホストのトラフィックを分類し、評判に基づいてアクセスコントロール ルールに条件を書くことを可能にします。

## URL フィルタリング な ルックアップ プロセス

URL ルックアップ プロセスを加速するために、URL フィルタリングは Firepower システムでローカルでインストールされているデータセットを提供します。 アプライアンスで利用可能な メモリ量 (RAM) に依存はそこにデータセットの 2 つの型です:

データセットの型	メモリ要件	
	バージョン 5.3	バージョン 5.4 または それ 以上
20,000,000 の URL データセット	>2GB	>3.4 GB
1,000,000 の URL データセット	<= 2GB	<= 3.4 GB



## Cloud 接続上の問題

### ステップ 1: ライセンスをチェックして下さい

ライセンスはインストールされていますか。

FireSIGHT Management Center に最初に URL フィルタリング な ライセンスを追加するまでポリシーによって目標とされるデバイスで、そして有効にするそれをアクセスコントロール ポリシーを適用できないどんなに URL フィルタリング な ライセンスなしでアクセスコントロール ルール

にカテゴリおよび評判ベースの URL 状態を追加できます。

## ライセンスは切れますか。

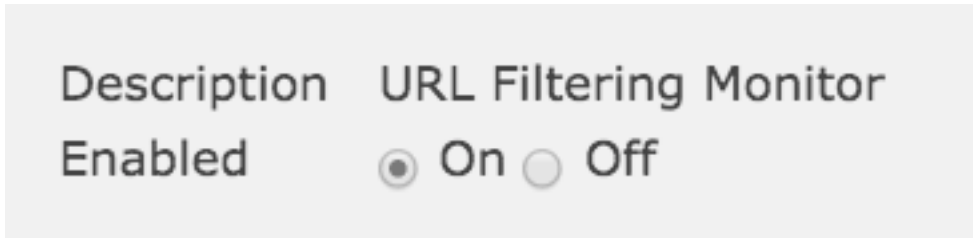
URL フィルタリング ライセンスが期限切れになると、カテゴリおよびレピュテーション ベースの URL 条件を持つアクセス コントロール ルールは URL のフィルタリングを停止し、FireSIGHT 管理センターはクラウド サービスにコンタクトしなくなります。

ヒント： 学ぶために [SireSIGHT システム構成例で URL フィルタリングを](#) SireSIGHT システムの URL フィルタリング な 機能を有効にし 管理対象装置の URL フィルタリング な ライセンスを適用する方法を読んで下さい。

## ステップ 2： 健全性アラートをチェックして下さい

FireSIGHT Management Center と Cisco 間の URL フィルタリング な モニタ モジュールトラック通信はシステムが一般に参照された URL の URL フィルタリング ( カテゴリおよび評判 ) データを得るところで、曇ります。URL フィルタリング な モニタ モジュールはまた FireSIGHT Management Center と URL フィルタリング を有効にした 管理対象装置間の通信をトラッキングします。

URL フィルタリング な モニタ モジュールを有効にするために、**健康ポリシー 設定** ページに、選択します **URL フィルタリング な モニタ** を行って下さい。ヘルス ステータス テストのためのモジュールの使用を有効にするために **イネーブルになったオプションのための ON オプション・ボタン** をクリックして下さい。設定に実施されてほしい場合 FireSIGHT Management Center に健康政策を適用して下さい。



Description URL Filtering Monitor  
Enabled  On  Off

- **重要な アラート**: FireSIGHT Management Center がとうまく交信するか、またはクラウドからアップデートを取得しなければ **重要**へのそのモジュール変更のためのステータス分類。
- **警告アラート**: FireSIGHT Management Center がクラウドとうまく交信する場合、モジュール状況は管理センターが管理対象装置に新しい URL フィルタリング データを押すことができないかどうか **警告**に変更します。

## 手順 3： DNS 設定をチェックして下さい

FireSIGHT Management Center はクラウド ルックアップの間にこれらのサーバと通信します:

database.brightcloud.com  
service.brightcloud.com

サーバが両方ともファイアウォールで割り当てられることを確かめたら、FireSIGHT Management Center のこれらのコマンドを実行し、管理センターが名前を変換できるかどうか確認して下さい:

```
admin@FireSIGHT:~$ sudo nslookup database.brightcloud.comadmin@FireSIGHT:~$ sudo nslookup
```

service.brightcloud.com

## ステップ 4： 必須ポートへの接続をチェックして下さい

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。

管理センターは正常な nslookup 行えることを確認したらポート 80 および telnet のポート 443 への接続を確認して下さい。URL データベースはポート 443 の database.brightcloud.com と未知 URL クエリはポート 80 の service.brightcloud.com で行われるが、ダウンロードされます。

```
admin@FireSIGHT:~$ sudo nslookup service.brightcloud.com
```

この出力は database.brightcloud.com へ正常な Telnet の例です。

```
admin@FireSIGHT:~$ sudo nslookup service.brightcloud.com
```

## アクセスコントロールおよび Miscategorization 問題

### 問題 1： 選択解除にされた評判レベルとの URL は許可されまじたり/ブロックされます

注意すれば URL は許可されるか、がまたはブロックされます、アクセスコントロール ルールのその URL の水平な評判を読みます URL フィルタリング ルールがどのようにはたらくか理解するためにこのセクションを選択しませんでした。

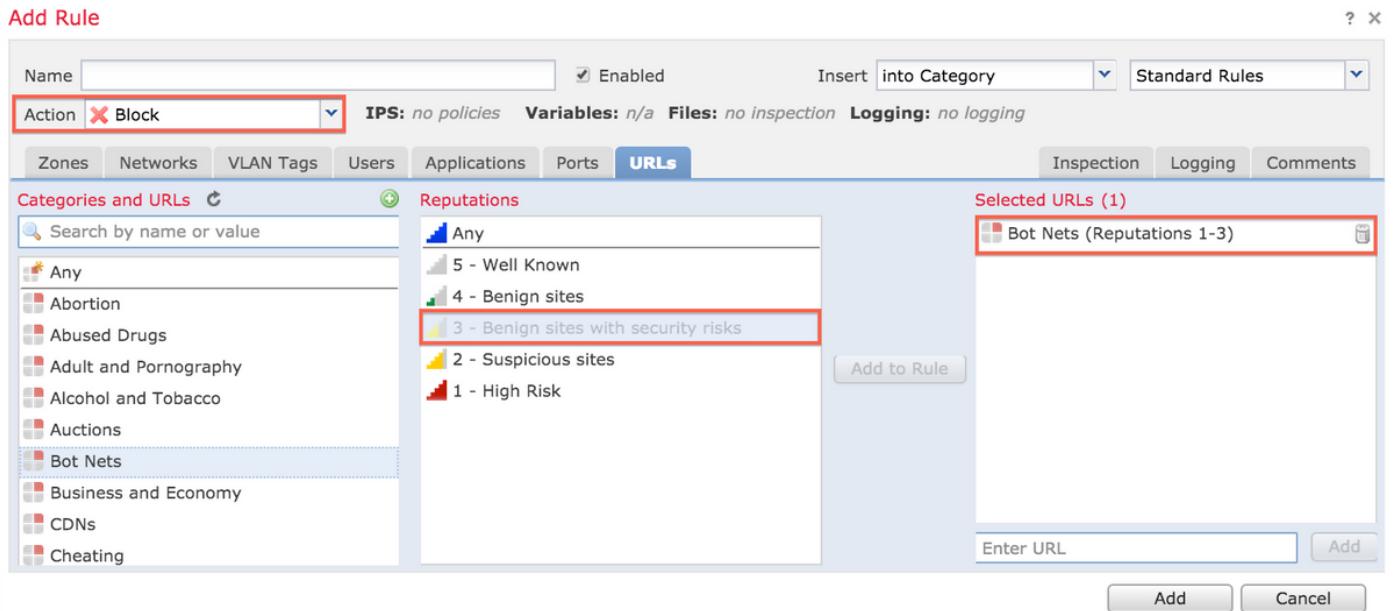
### ルール処理は割り当てです

評判レベルに基づいてトラフィックを許可するルールを作成するとき評判レベルの選択はまた最初に選択したレベルよりセキュア評判レベルすべてをより少なく選択します。たとえば、セキュリティリスク (3) レベルの良性 サイトを許可するルールを設定すればそれはまた自動的に良性サイト (4) レベルをおよびよく知られている可能にします (5) レベル サイト。

The screenshot shows the 'Add Rule' configuration window. The 'Action' is set to 'Allow'. The 'URLs' tab is selected, showing a list of reputation categories. 'Bot Nets' is selected in the 'Categories and URLs' list. In the 'Reputations' list, '3 - Benign sites with security risks' is highlighted. The 'Selected URLs (1)' list contains 'Bot Nets (Reputations 3-5)'. The 'Add' button is visible at the bottom right.

### ルール処理はブロックです

評判レベルに基づいてトラフィックをブロックするルールを作成するとき評判レベルの選択はまた最初に選択したレベルより厳しい評判レベルすべてを選択します。たとえば、セキュリティリスク(3)レベルの良性サイトをブロックするルールを設定すればそれはまた自動的に疑わしいサイト(レベル2)および高いリスク(1)レベルサイトをブロックします。



## URL 選択行列

指定評判レベル	指定ルール処理
1-高いリスク	高いリスク
2-疑わしいサイト	疑わしいサイト
3-セキュリティリスクの良性サイト	セキュリティリスクの良性サイト
4-良性サイト	良性サイト
5-よく知られている	よく知られている

## 問題 2: ワイルドカードはアクセスコントロールルールではたきません

SireSIGHT システムは URL 状態のワイルドカードの仕様をサポートしません。この条件はかもしれません `cisco.com` 警告しないために。

```
admin@FireSIGHT:~$ sudo nslookup service.brightcloud.com
```

さらに、望ましくない結果を引き起こす不完全な URL は他のトラフィックに対して一致するかもしれません。URL 状態のユーザー URL を規定するとき、注意深く影響を受けるかもしれない他のトラフィックを考えて下さい。たとえば、明示的に `cisco.com` ブロックしたいと思うシナリオを考慮して下さい。ただし、部分文字列一致は `cisco.com` ブロックすることがまたインテントではないかもしれない `sanfrancisco.com` ブロックすることを意味します。

URL を入力するとき、ドメイン名を入力し、サブドメイン情報を省略して下さい。たとえば、[www.cisco.com](http://www.cisco.com) よりむしろ `cisco.com` 入力して下さい。割り当てルールで `cisco.com` 使用するとき、ユーザはこれらの URL の何れかにブラウズする可能性があります:

```
admin@FireSIGHT:~$ sudo nslookup service.brightcloud.com
```

## 問題 3: URL カテゴリおよび評判は読み込まれません

URL はトラフィックで見られること URL がローカルデータベースになればおよびそれが最初になら、カテゴリが評判は読み込まれないかもしれません。これは未知 URL が見られる時最初に、AC ルールを一致することを意味します。時々一般に参照された URL のための URL ルックアップは URL が見られる時最初にで解決しないかもしれません。この問題はバージョン 5.3.0.3、5.3.1.2 および 5.4.0.2 で、5.4.1.1 解決されます。

## 関連情報

- [SireSIGHT システムの URL フィルタリングの設定](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)