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

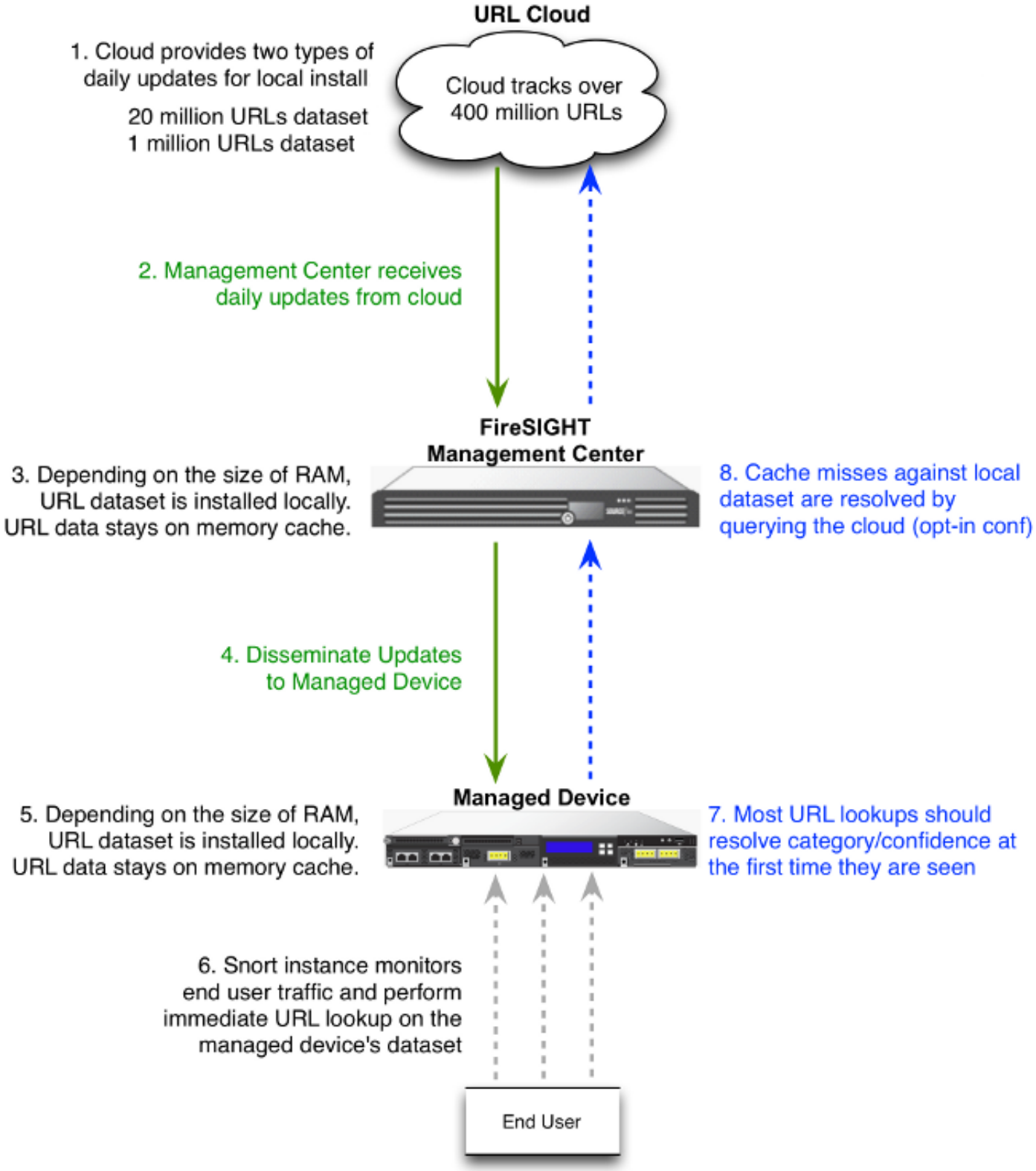
概要

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制御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 システムで口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制御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制御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。

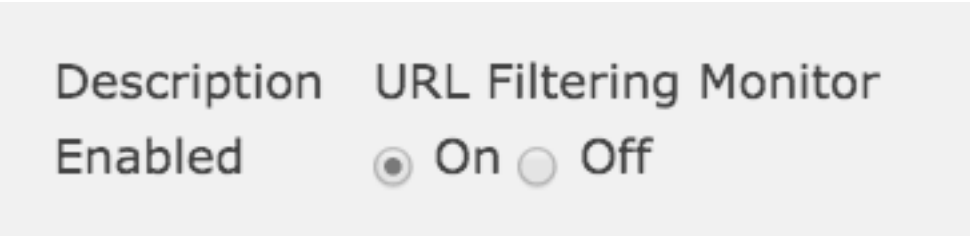
URL フィルタリング ライセンスが期限切れになると、カテゴリおよびレピュテーション ベースの URL 条件を持つアクセス コントロール ルールは URL のフィルタリングを停止し、FireSIGHT 管理センターはクラウド サービスにコンタクトしなくなります。

> **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 なライセンスを加え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 フィルタリングをイネーブル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 モジュールをイネーブルにするために、**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イネーブルにするために**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。



- **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。

ステップ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.com

admin@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
```

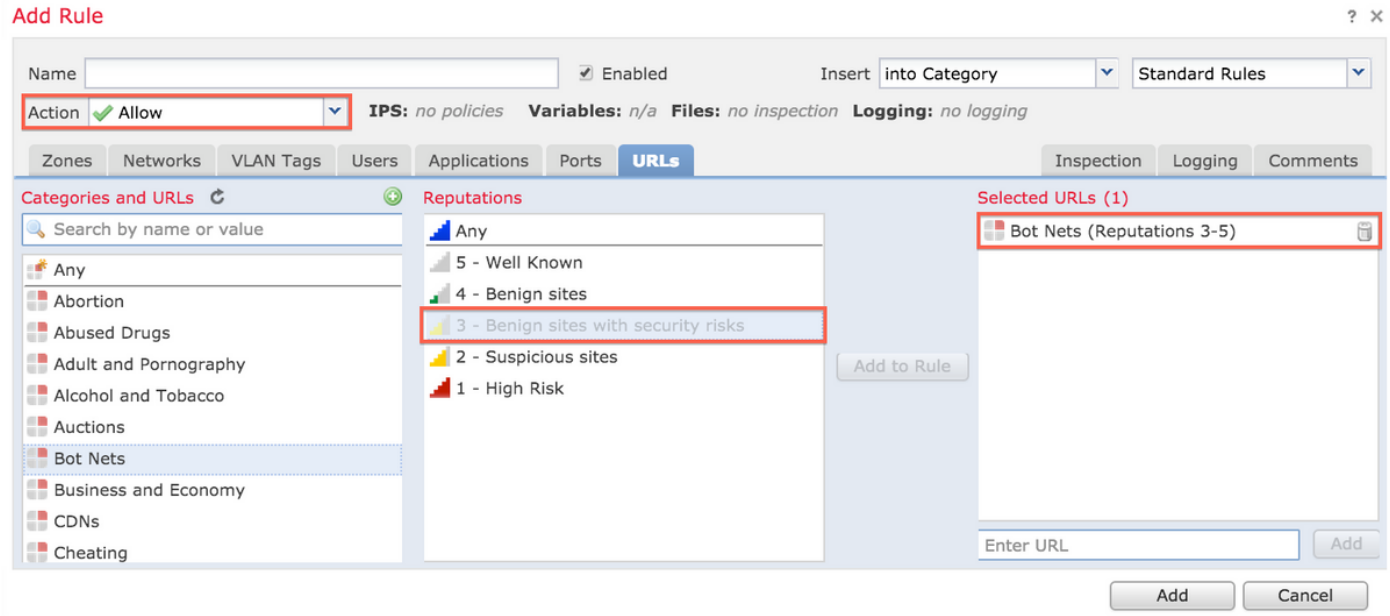
アクセス制御および Miscategorization 問題

問題 1： 選択解除にされた評判レベルとの URL は許可されましたり/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、アクセス制御ルールのその URL の評判レベルを、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。

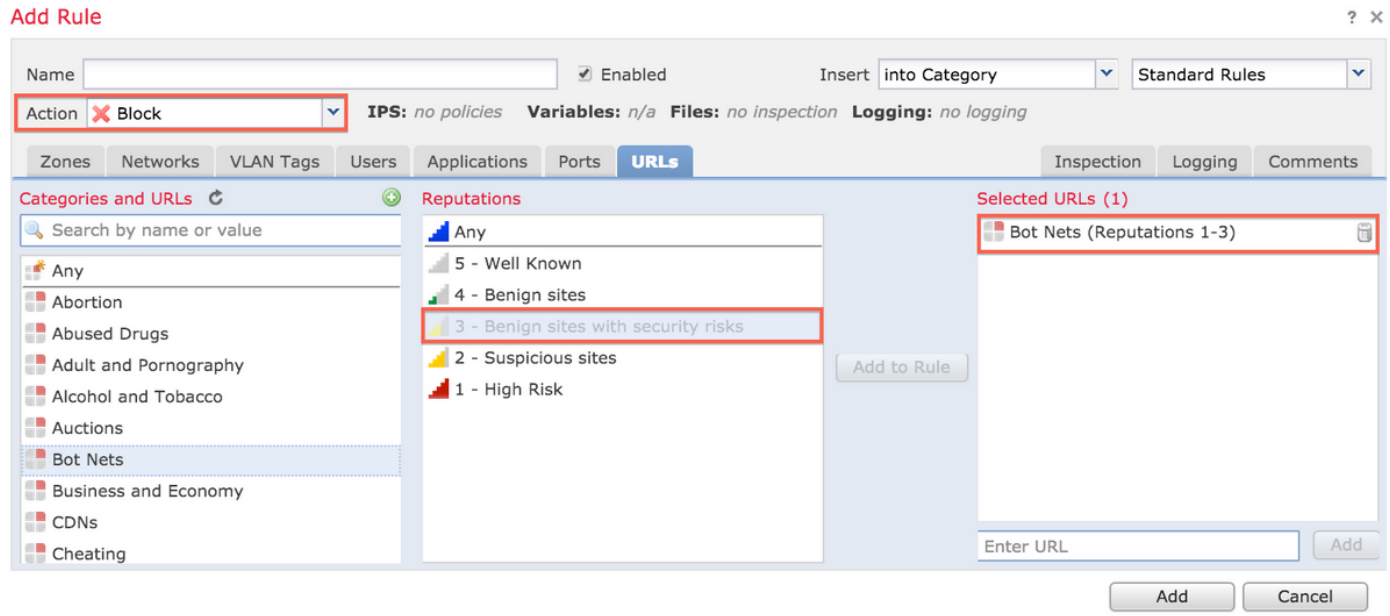
ルール操作は割り当てです

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の良性サイト*を設定すれば（許可するルールを 3）水平な、それはまた自動的に*良性サイト*を可能にします（4）水平な、*よく知られた*（水平な 5）サイト。



ルール操作はブロックです

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の良性サイト*を設定すれば（ブロックするルールを 3）水平な、それはまた自動的に*疑わしいサイト*をブロックします（2）および*高いリスク*（水平な 1）サイト水平な。



URL 選択行列

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

問題 2： ワイルドカードはアクセス制御ルールではたらきません

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 しないことを。

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

さらに、不完全な URL は望ましくない結果を引き起こす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` よりもむしろ `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ければおよびそれが最初になら、カテゴリか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