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

内容

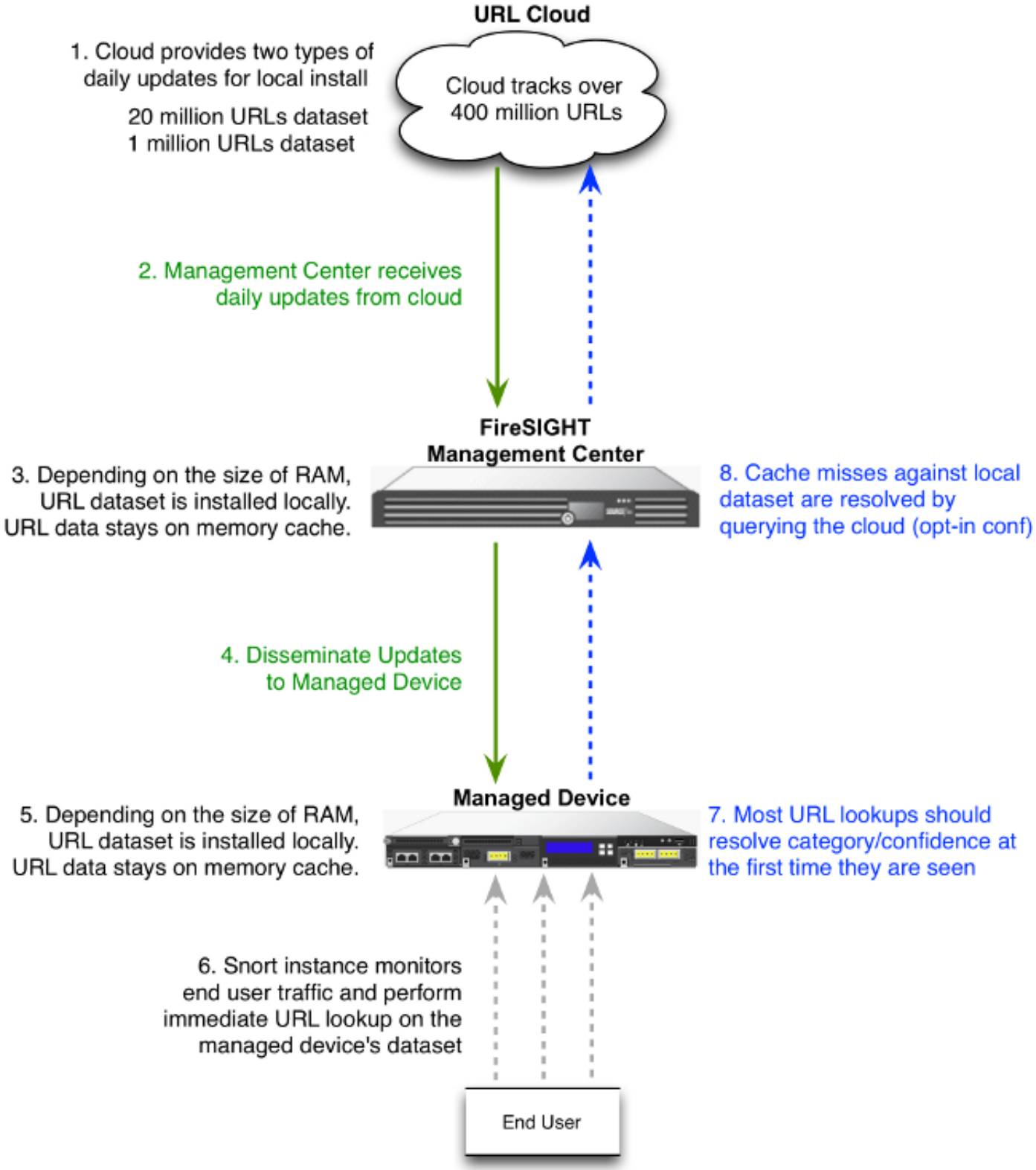
概要

このドキュメントでは、URL フィルタリングに関連する一般的な問題について説明します。FireSIGHT Management CenterのURLフィルタリング機能は、監視対象ホストのトラフィックを分類し、レピュテーションに基づいてアクセスコントロールルールに条件を記述できるようにします。

URLフィルタリングルックアッププロセス

URLルックアッププロセスを高速化するために、URLフィルタリングはFirepowerシステムにローカルにインストールされたデータセットを提供します。アプライアンスで使用可能なメモリ(RAM)の量に応じて、次の2種類のデータセットがあります。

データセットのタイプ	メモリ要件	
	バージョン5.3	バージョン5.4以降
2,000万のURLデータセット	>2 GB	>3.4 GB
100万のURLデータセット	<= 2 GB	3.4 GB未満



クラウド接続の問題

ステップ 1：ライセンスの確認

ライセンスがインストールされているか

URLフィルタリングライセンスなしで、カテゴリとレピュテーションベースのURL条件をアクセスコントロールルールに追加できますが、最初にURLフィルタリングライセンスをFireSIGHT Management Centerに追加し、ポリシーの対象となるデバイスで有効にするまで、アクセスコン

トロールポリシーを適用できません。

ライセンスの期限が切れていますか。

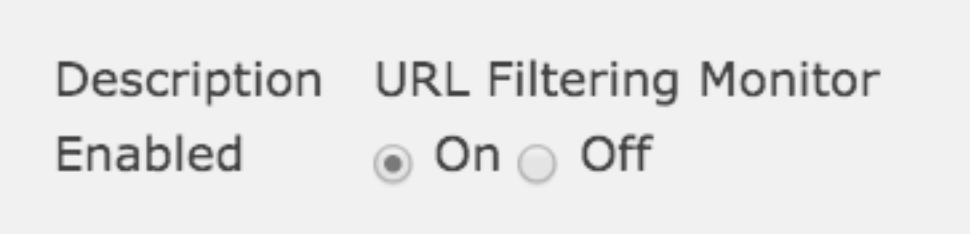
URL フィルタリング ライセンスが期限切れになると、カテゴリおよびレピュテーション ベースの URL 条件を持つアクセス コントロール ルールは URL のフィルタリングを停止し、FireSIGHT 管理センターはクラウド サービスにコンタクトしなくなります。

> **ヒント**：FireSIGHTシステムでURLフィルタリング機能を有効にし、管理対象デバイスにURLフィルタリングライセンスを適用する方法については、『FireSIGHTシステムでのURLフィルタリングの設定例』を参照してください。

ステップ 2：ヘルスアラートの確認

URL Filtering Monitorモジュールは、FireSIGHT Management Centerとシスコのクラウド間の通信を追跡します。システムは、よくアクセスするURLのURLフィルタリング（カテゴリおよびレピュテーション）データを取得します。URLフィルタリングモニタモジュールは、FireSIGHT Management Centerと、URLフィルタリングを有効にした管理対象デバイス間の通信も追跡します。

URLフィルタリングモニタモジュールを有効にするには、**Health Policy Configuration**ページに移動し、**URL Filtering Monitor**を選択します。モジュールをヘルスステータステストで使用できるようにするには、[Enabled] オプションの[On] オプションボタンをクリックします。設定を有効にするには、FireSIGHT Management Centerに正常性ポリシーを適用する必要があります。



- **Critical Alert**:FireSIGHT Management Centerがクラウドと正常に通信できない場合、またはクラウドから更新を取得できない場合、そのモジュールのステータス分類は*Critical*に変わります。
- **警告アラート**：FireSIGHT Management Centerがクラウドと正常に通信すると、Management Centerが新しいURLフィルタリングデータを管理対象デバイスにプッシュできない場合、モジュールのステータスは*警告*に変わります。

ステップ 3：DNS設定の確認

FireSIGHT Management Centerは、クラウドのルックアップ中にこれらのサーバと通信します。

```
database.brightcloud.com
service.brightcloud.com
```

ファイアウォールで両方のサーバが許可されていることを確認したら、FireSIGHT Management Centerで次のコマンドを実行し、Management Centerが名前を解決できるかどうかを確認します。

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

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

ステップ 4：必要なポートへの接続の確認

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。

Management Centerが正常にnslookupを実行できることを確認したら、telnetを使用してポート80とポート443への接続を確認します。URLデータベースはdatabase.brightcloud.comのポート443でダウンロードされますが、不明なURLクエリはservice.brightcloud.comのポート80で実行されます。

```
telnet database.brightcloud.com 443
telnet service.brightcloud.com 80
```

次に、database.brightcloud.comへのtelnet接続が成功した例を示します。

```
Connected to database.brightcloud.com.
Escape character is '^]'.
```

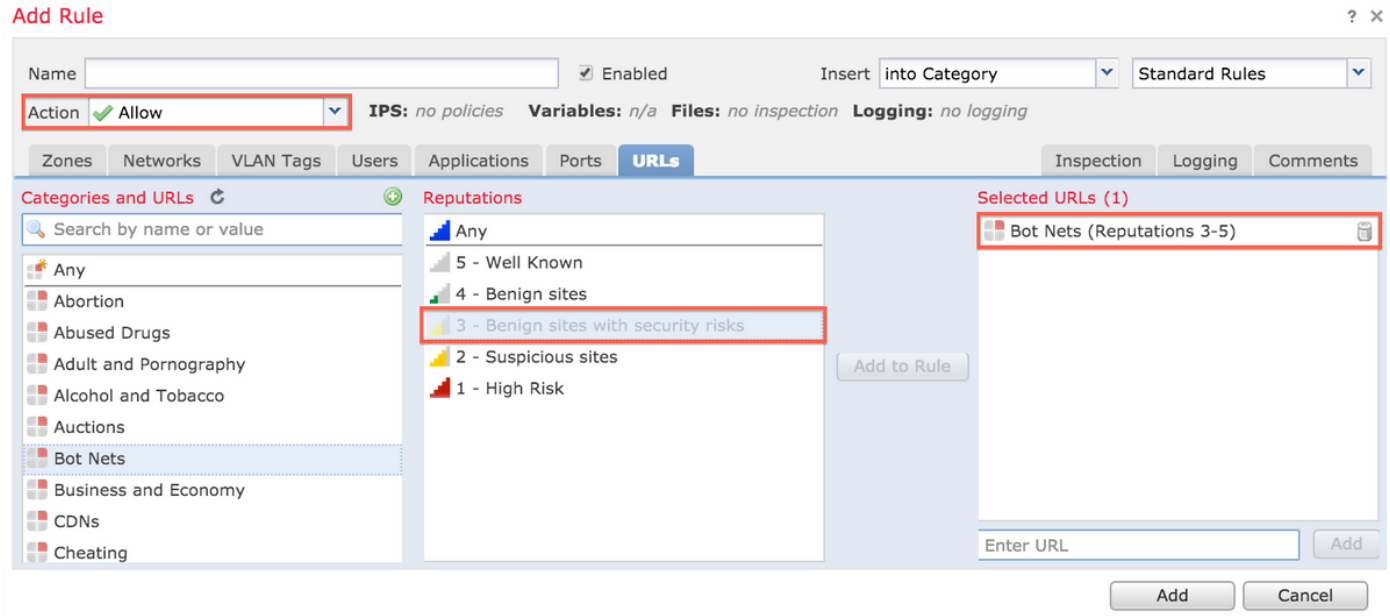
アクセス制御と誤分類の問題

問題 1：レピュテーションレベルが選択されていないURLは許可/ブロックされる

URLが許可またはブロックされているのに、アクセスコントロールルールでそのURLのレピュテーションレベルを選択していない場合は、このセクションを読んで、URLフィルタリングルールの動作を理解してください。

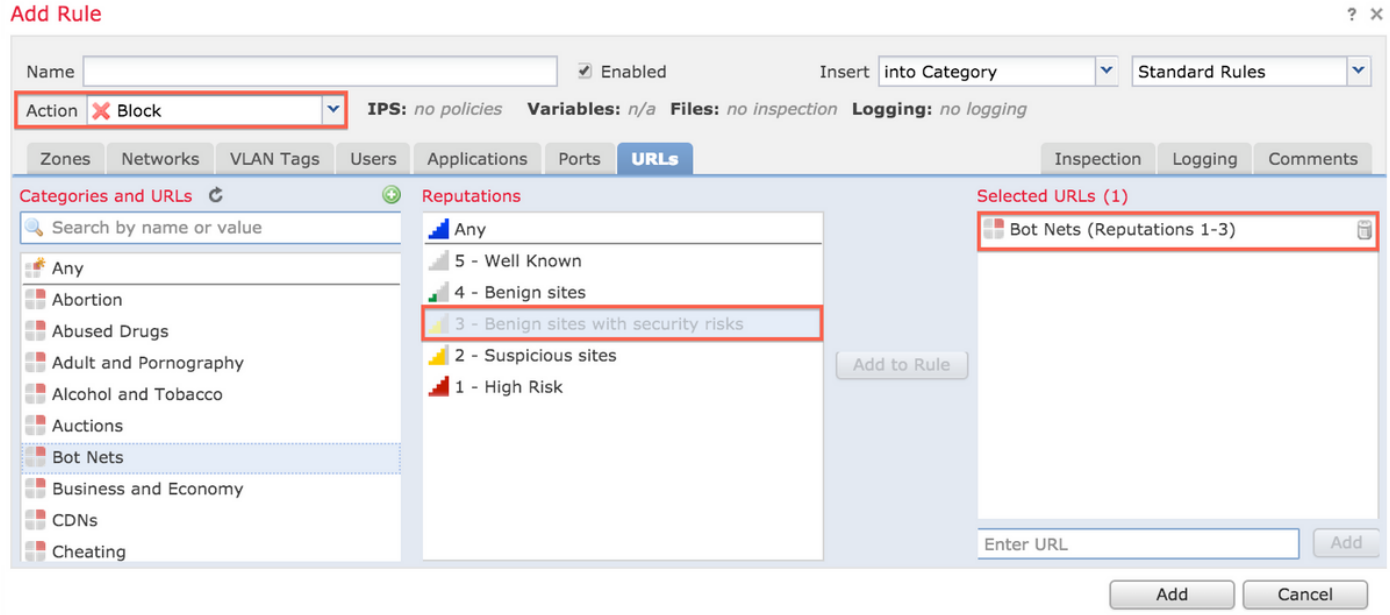
ルールアクションは許可です

レピュテーション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場合、レピュテーションレベルを選択すると、最初に選択したレベルよりも安全性の低いレピュテーションレベルもすべて選択されます。たとえば、*セキュリティリスクのある良性サイト*（レベル3）を許可するルールを設定すると、自動的に*良性サイト*（レベル4）および*よく知られている*（レベル5）サイトも許可されます。



ルールアクションがブロック

レピュテーション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場合、レピュテーションレベルを選択すると、最初に選択したレベルよりも厳しいレピュテーションレベルもすべて選択されます。たとえば、*セキュリティリスクのある良性サイト*（レベル3）をブロックするルールを設定すると、*疑わしいサイト*（レベル2）および*高リスク*（レベル1）のサイトも自動的にブロックされます。



URL選択マトリックス

選択したレピュテーションレベル	選択したルールアクション **高リスク**	**不審なサイト**	**セキュリティリスクのある良性サイト**	**良**
1 – 高リスク				
2 – 疑わしいサイト	Block			
3 – セキュリティリスクのある良性サイト	Block	Block		
4 – 良性サイト	Block	Block	Block	
5 – よく知られている	Block	Block	Block	Blo

問題 2：アクセス制御規則でワイルドカードが機能しない

FireSIGHTシステムは、URL条件でのワイルドカードの指定をサポートしていません。この状態は、cisco.comで警告に失敗する可能性があります。

```
*cisco*.com
```

また、不完全なURLが他のトラフィックと一致する場合も、望ましくない結果を引き起こします。URL条件で個々のURLを指定する場合は、影響を受ける可能性がある他のトラフィックを慎重に考慮する必要があります。たとえば、cisco.comを明示的にブロックするシナリオを考えてみます。ただし、部分文字列の照合は、cisco.comをブロックするとsanfrancisco.comもブロックされることを意味します。これは意図していない可能性があります。

URLを入力するときは、ドメイン名を入力し、サブドメイン情報を省略します。たとえば、www.cisco.comではなくcisco.comと入力します。 Allowルールでcisco.comを使用する場合、ユーザは次のURLのいずれかを参照できます。

```
http://cisco.com
http://cisco.com/newcisco
http://www.cisco.com
```

問題 3：URLカテゴリとレピュテーションが入力されていない

URLがローカルデータベース内になく、そのURLがトラフィック内で初めて見られる場合は、カテゴリまたはレピュテーションが設定されていない可能性があります。これは、未知のURLが初めて見られたときに、ACルールと一致しないことを意味します。 一般的にアクセスされるURLのURLルックアップは、最初にURLが表示されたときに解決しないことがあります。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、5.4.1.1で修正されています。

関連情報

- FireSIGHTシステムでの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