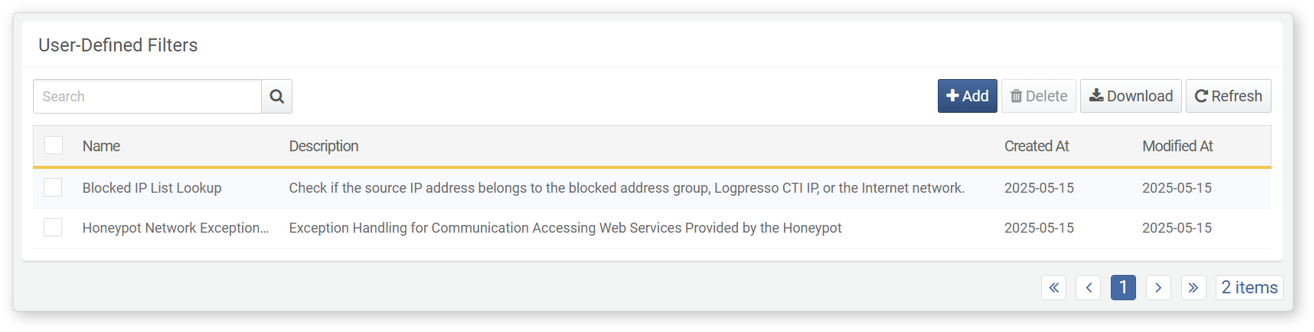
### ユーザー定義フィルター

#### 概要

ユーザー定義フィルターは、データ分析および検出のために特定のフィルタ条件を検出ルールに適用できる機能です。これらのフィルターは、繰り返し使用される複雑な条件をモジュール化し、複数の検出ルールで同じ条件を簡単に適用できるようにします。これにより、ストリームルールおよびバッチルールの両方で効率的なフィルタリングが実現します。

#### ユーザー定義フィルターの検索

**ポリシー > ユーザー定義フィルター** でユーザー定義フィルターの一覧を表示または検索できます。



* **名前**：ユーザー定義フィルターの一意な名称
* **説明**：ユーザー定義フィルターの説明
* **作成日時**：ユーザー定義フィルターが作成された日時
* **最終修正日時**：ユーザー定義フィルターが最後に修正された日時

特定のフィルターを検索するには、ツールバーの検索ツールを使用します。検索ツールは、入力したキーワードが**名前**または**説明**フィールドに含まれるユーザー定義フィルターを検索します。検索は大文字・小文字を区別しません。

ユーザー定義フィルター一覧のダウンロード

ユーザー定義フィルター一覧をローカルPCにダウンロードするには、ツールバーの**ダウンロード**をクリックします。

ユーザー定義フィルター一覧の更新

最新情報にリストを更新するには、ツールバーの**更新**をクリックします。

#### ユーザー定義フィルターの追加

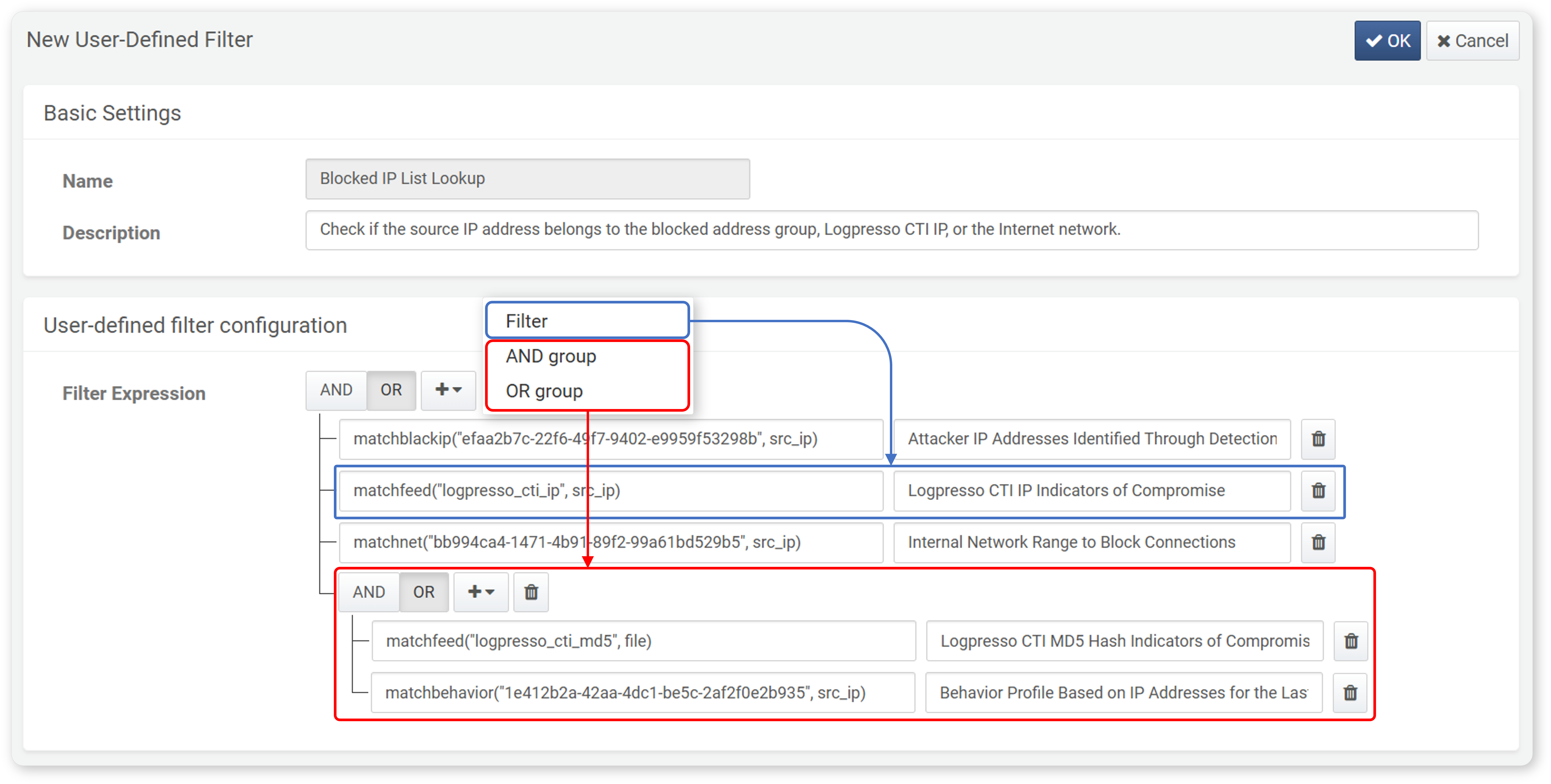
ユーザー定義フィルターを追加するには、以下の手順に従います。

**ポリシー > ユーザー定義フィルター** に移動し、ツールバーの**追加**をクリックします。

**ユーザー定義フィルター追加**画面で、**名前**および**説明**を入力します。

* **名前**：ユーザー定義フィルターの一意な名称（最大50文字）。作成後は変更できません。
* **説明**：ユーザー定義フィルターの説明（最大2,000文字）。

**ユーザー定義フィルター設定**で**フィルター式**を入力し、**OK**をクリックします。



* 初期状態では、フィルター式の入力欄が1つ表示されます。Logpressoクエリ言語で記述したブール式と説明（各最大1,000文字）を入力してください。
* 「+」をクリックすると、フィルター式またはサブフィルター式グループを追加できます。グループは最大3階層までネスト可能です。
* **AND**または**OR**をクリックして、フィルター式の論理演算を指定します。
* フィルター式またはグループを削除するには、右側のゴミ箱アイコンをクリックします。

#### ユーザー定義フィルターの編集

ユーザー定義フィルターを編集するには、以下の手順に従います。

**ユーザー定義フィルター**一覧で、編集したいフィルターの名前をクリックします。

**ユーザー定義フィルター編集**画面で内容を修正し、**保存**をクリックします。

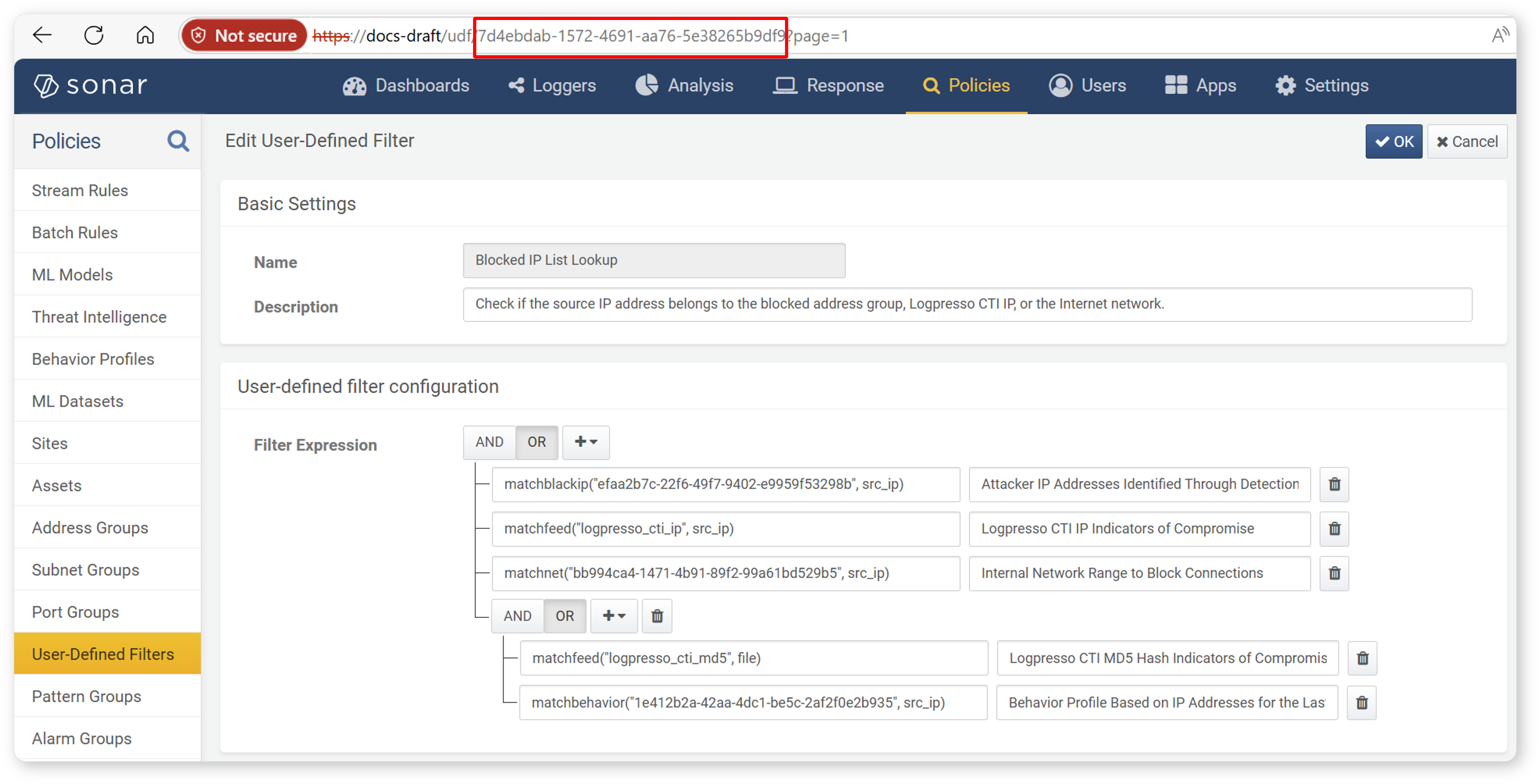
#### ユーザー定義フィルターの利用

クエリでの利用

ユーザー定義フィルターは、クエリ文内で[matchfilter()](https://docs.logpresso.comnull)関数を呼び出すことで適用できます。たとえば、特定のIPアドレスをフィルタリングする場合、以下のようなクエリを使用します。

search matchfilter("ユーザー定義フィルターのGUID")

この関数を利用するには、ユーザー定義フィルターのGUIDを知っておく必要があります。GUIDはブラウザのアドレスバーで確認できます。



#### ユーザー定義フィルターの削除

ユーザー定義フィルターを削除するには、以下の手順に従います。

**ユーザー定義フィルター**一覧で、削除したいフィルターのチェックボックスを選択します。

ツールバーの**削除**をクリックします。

**ユーザー定義フィルター削除**ダイアログで、削除対象のフィルター一覧を確認し、**削除**をクリックします。キャンセルする場合は**キャンセル**をクリックします。

ストリームルールまたはバッチルールで参照されているユーザー定義フィルターを削除すると、検出ルールが正しく動作しなくなる可能性があります。