### サブネットグループ

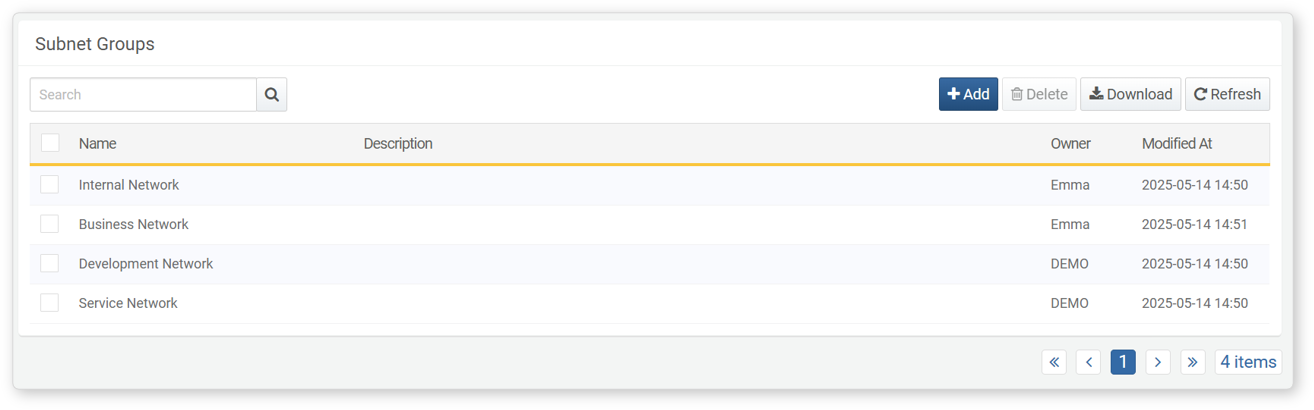
#### 概要

サブネットはグループ単位で管理でき、検出ポリシーに適用できます。一般的に、サブネットグループはサブネットの定義、ネットワーク境界のアクティビティ監視、またはポリシー例外の処理に使用されます。

本機能はIPv4アドレスのみをサポートします。

#### サブネットグループの検索

**ポリシー > サブネットグループ** でサブネットグループの一覧を確認できます。



* **名前**: サブネットグループの一意な名称
* **説明**: サブネットグループの説明
* **所有者**: サブネットグループを追加したユーザー
* **最終更新日時**: サブネットグループの作成または最終更新日時

#### サブネットグループ一覧のダウンロード

サブネットグループ一覧をファイルとしてローカル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。

#### サブネットグループ一覧の更新

サブネットグループ一覧を最新情報に更新するには、ツールバーの **更新** をクリックします。

#### サブネットグループ内のサブネット検索

**サブネットグループの編集** 画面では、ツールバーの検索ツールを利用できます。単一のIPアドレス、空白文字、キーワードの組み合わせで検索が可能です。空白文字の使用有無によって検索動作が異なります。

検索語に空白文字が含まれない場合:

* **IPアドレスのみ**: 入力したIPアドレスを含むサブネットを表示します。
* **キーワードのみ**: **名前** または **説明** にキーワードが含まれるサブネットを表示します。

検索語に1つ以上の空白文字が含まれる場合:

* **IPアドレスとキーワード**: IPアドレスを含み、かつ **名前** または **説明** にキーワードが含まれるサブネットを表示します。検索語として使用できるIPアドレスは1つのみです。
* **複数キーワード**: **名前** または **説明** にすべてのキーワードが含まれるサブネットを表示します。

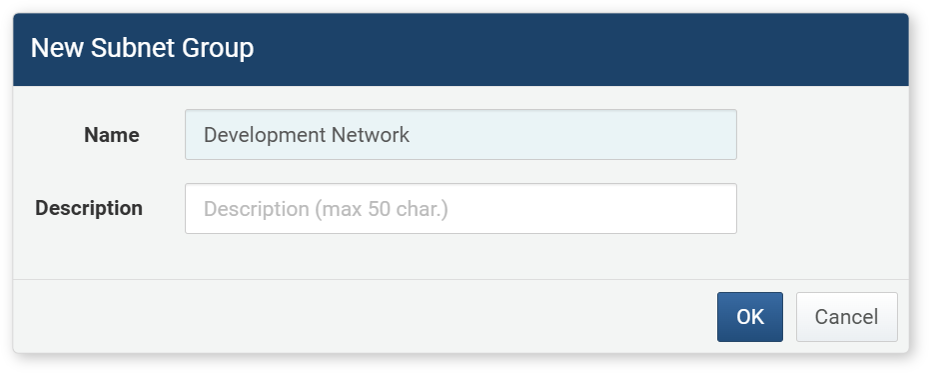
検索は大文字・小文字を区別しません。

#### サブネットグループの追加

サブネットグループを追加するには:

**[サブネットグループ](section-subnet-group#outline3)** 一覧で、ツールバーの **追加** をクリックします。

**サブネットグループの追加** ダイアログで必要な値を入力または選択し、**OK** をクリックします。



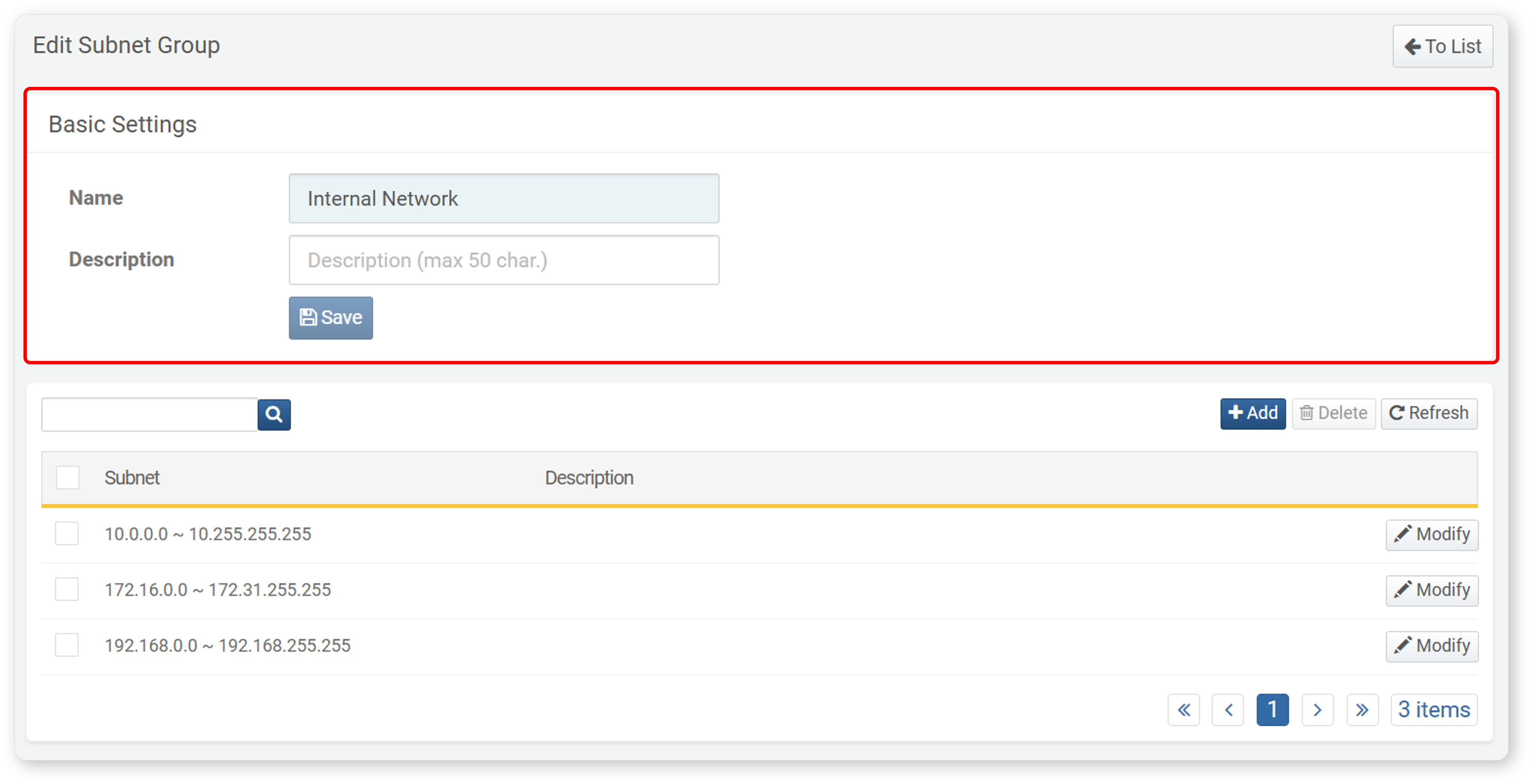
* **名前**: サブネットグループの一意な名称（最大50文字）
* **説明**: サブネットグループの説明（最大50文字）

#### サブネットグループの編集

サブネットグループを編集するには:

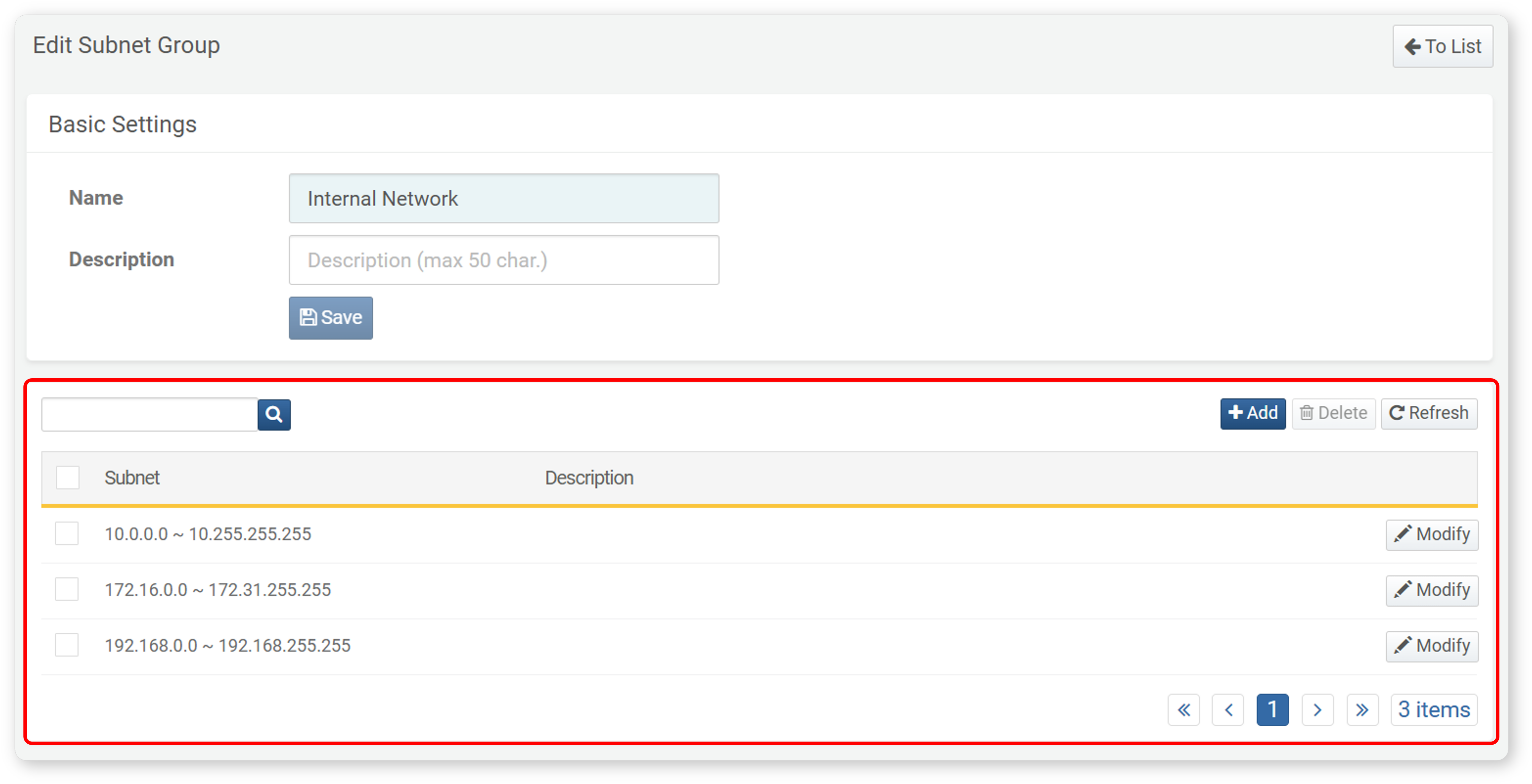
**[サブネットグループ](section-subnet-group#outline3)** 一覧で、編集したいサブネットグループの **名前** をクリックします。

**サブネットグループの編集** 画面で情報を修正し、**保存** をクリックします。



#### サブネットグループ内のサブネット確認

**[サブネットグループの編集](section-subnet-group#outline8)** 画面で、登録済みのサブネットを確認できます。



* **サブネット**: サブネット情報を表示
* 単一IP（例: 192.0.2.1）
* IP範囲（例: 192.0.2.1 ~ 192.0.2.254）
* CIDRブロック（例: 192.0.2.0/24）
* **説明**: IPアドレスの詳細説明

**サブネットグループの編集** ページでも検索機能が利用でき、**[サブネットグループの検索](section-subnet-group#outline6)** で説明したルールと同様です。ただし、以下の違いがあります。

* 検索対象は選択したサブネットグループ内のIPアドレスに限定されます。
* サブネットには **名前** がないため、説明に検索語が含まれるサブネットのみが表示されます。

サブネットグループへのサブネット追加

サブネットグループにサブネットを追加するには:

**[サブネットグループの編集](section-subnet-group#outline8)** 画面で、ツールバーの **追加** をクリックします。

**サブネットの追加** ダイアログでネットワーク情報を入力し、**OK** をクリックします。選択したネットワークタイプ（**IPアドレス範囲**、**単一IPアドレス**、**CIDR**）によって入力項目が異なります。

* タイプが **IP範囲** の場合:
* **開始**: ネットワーク範囲の最初のIPv4アドレス
* **終了**: ネットワーク範囲の最後のIPv4アドレス
* タイプが **単一IPアドレス** の場合:
* **IPアドレス**: IPv4アドレス
* タイプが **CIDR** の場合:
* **ネットワークアドレス**: IPv4アドレスのホスト部を除いたネットワークアドレス
* **（サブネットマスク）ビット数**: ネットワークアドレスのサブネットマスクビット数（1～32）
* **説明**: ネットワークの詳細説明（最大255文字）

サブネットの編集

サブネットグループに登録されたサブネットを編集するには:

**[サブネットグループの編集](section-subnet-group#outline8)** 画面で、編集したいサブネットの行の **編集** をクリックします。

**サブネットの編集** ダイアログで情報を修正し、**OK** をクリックします。

サブネットの削除

サブネットグループに登録されたサブネットを削除するには:

**[サブネットグループの編集](section-subnet-group#outline8)** 画面で、削除したいネットワーク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。

**サブネットの削除** ダイアログで削除対象のネットワーク一覧を確認し、**削除** をクリックして確定します。キャンセルする場合は **キャンセル** をクリックします。

#### サブネットグループの活用

サブネットグループは以下の方法で利用できます。

シナリオビルダー

**ポリシー > ストリームルール** で、疑わしいIPアドレスが既にアドレスグループに登録されているかどうかを確認するシナリオを構築できます。

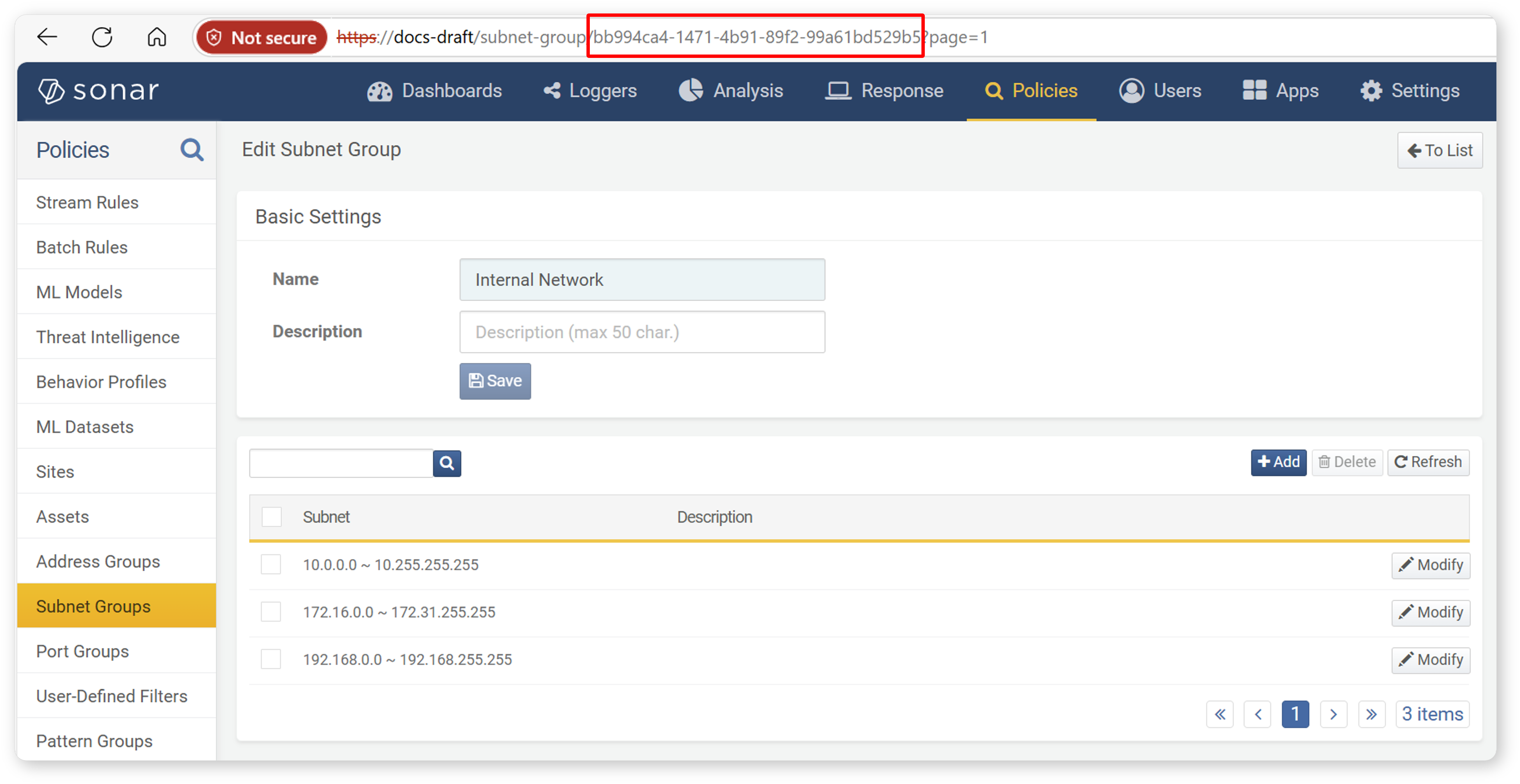
以下の表は、入力フィールドタイプが **IP** の場合にシナリオビルダーで利用可能なサブネット関連ルールをまとめたものです。詳細は [フィールドタイプ別ルールとパラメータ](https://docs.logpresso.comnull) を参照してください。

|  |  |  |  |
| --- | --- | --- | --- |
| ルール | パラメータ | 範囲 | 説明 |
| サブネットグループに含まれるIPアドレス | 対象サブネットグループ | サブネットグループを選択 | 選択したサブネットグループに含まれるフィールド値をフィルタします。 |
|  |  |  |  |

クエリ

**ポリシー > ストリームルール** または **ポリシー > バッチルール** で検出ルールを追加・修正する際、[matchnet](https://docs.logpresso.comnull) コマンドや [matchnet()](https://docs.logpresso.comnull) 関数を利用してサブネットグループを活用できます。クエリ入力をサポートするすべての機能でサブネットグループが利用可能です。

[matchnet](https://docs.logpresso.comnull) コマンドや [matchnet()](https://docs.logpresso.comnull) 関数を利用するには、サブネットグループのGUIDを知る必要があります。GUIDはブラウザのアドレスバーで確認できます。



#### サブネットグループの削除

サブネットグループを削除するには:

**サブネットグループ** 一覧で、削除したいサブネットグループ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。

**サブネットグループの削除** ダイアログで削除対象のサブネットグループ一覧を確認し、**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。

バッチルールやストリームルールで参照されているサブネットグループを削除すると、ルールが正しく動作しなくなる可能性があります。