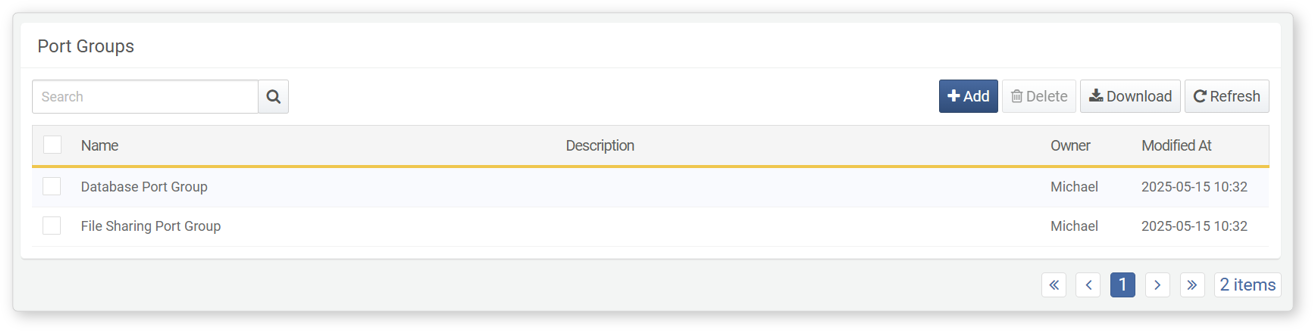
### ポートグループ

#### 概要

ポートグループは、TCPおよびUDP通信で使用されるポート番号をトピックごとにグループ化し、検出ポリシーに適用できる機能です。特定ポートへのアクセス検知や異常行動の分析に利用されます。

#### ポートグループの検索

**ポリシー > ポートグループ** で、ポートグループの一覧を表示または検索できます。



* **名前**: ポートグループの一意な名称
* **説明**: ポートグループに関する詳細情報
* **所有者**: ポートグループを追加したユーザー
* **最終更新日**: ポートグループの作成または最終更新日時

特定のポートグループを一覧から探す場合は、ツールバーの検索ツールを利用してください。検索ツールは、**名前** または **説明** に入力したキーワードを含むポートグループを検索します。大文字・小文字は区別されません。

ポートグループ一覧のダウンロード

ポートグループ一覧をローカル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。

ポートグループ一覧の更新

最新情報でポートグループ一覧を更新するには、ツールバーの **更新** をクリックします。

#### ポートグループの追加

ポートグループを追加するには、以下の手順に従います。

**ポリシー > ポートグループ** で、ツールバーの **追加** をクリックします。

**ポートグループ追加** ダイアログで必要事項を入力し、**OK** をクリックします。

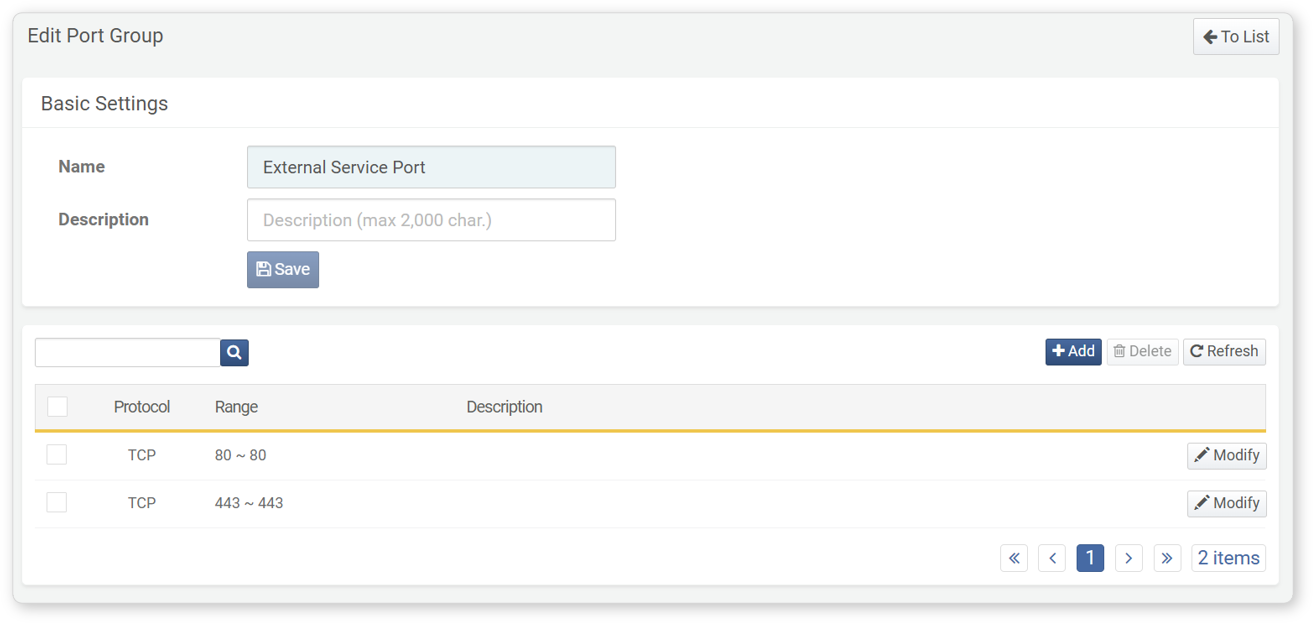
* **名前**: ポートグループ名（最大50文字）
* **説明**: 詳細説明（最大2,000文字）

#### ポートグループの編集

ポートグループを編集するには、以下の手順に従います。

**[ポートグループ](section-port-group#outline3)** 一覧で、編集したいポートグループ名をクリックします。

**ポートグループ編集** 画面で内容を修正し、**保存** をクリックします。



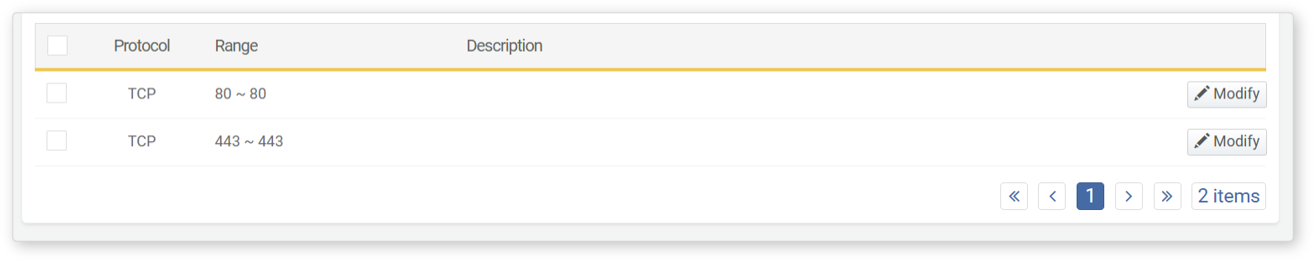
ポートの検索

ポートグループ内に登録された特定のポートを検索するには、以下の手順に従います。

**[ポートグループ](section-port-group#outline3)** 一覧で、検索したいポートグループをクリックします。

**ポートグループ編集** 画面で登録済みポートの一覧を確認できます。

* **プロトコル**: トランスポート層プロトコル（TCP、UDP）
* **範囲**: ポート番号範囲
* **説明**: ポートの説明



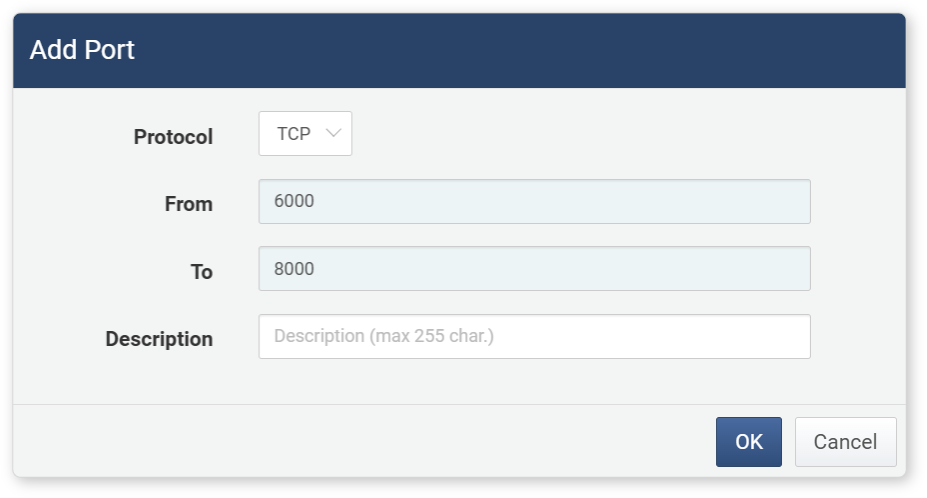
**ポートグループ編集** 画面では検索機能も利用できます。検索ツールは、**範囲** または **説明** に入力したキーワードを含むポートを検索します。大文字・小文字は区別されません。

ポートの追加

ポートグループにポートを追加するには、以下の手順に従います。

**ポートグループ編集** 画面で、ツールバーの **追加** をクリックします。

**ポート追加** ダイアログでポート情報を入力し、**OK** をクリックします。



* **プロトコル**: ポートのプロトコル（選択肢: TCP、UDP／デフォルト: TCP）
* **開始**: 開始ポート番号（0～65,535）
* **終了**: 終了ポート番号（0～65,535）。単一ポートを登録する場合は、**開始** と **終了** に同じ番号を入力してください。
* **説明**: 詳細説明（最大255文字）

ポートの編集

ポートグループに登録されたポートを編集するには、以下の手順に従います。

**ポートグループ編集** 画面で、編集したいポートの行の **編集** をクリックします。

**ポート編集** ダイアログで内容を修正し、**OK** をクリックします。

ポートの削除

ポートグループから登録済みポートを削除するには、以下の手順に従います。

**ポートグループ編集** 画面で、削除したいポート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。

**ポート削除** ダイアログで削除対象のポートを確認し、**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。

#### ポートグループの活用

ポートグループは、以下の方法で活用できます。

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アドレスがアドレスグループに既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。

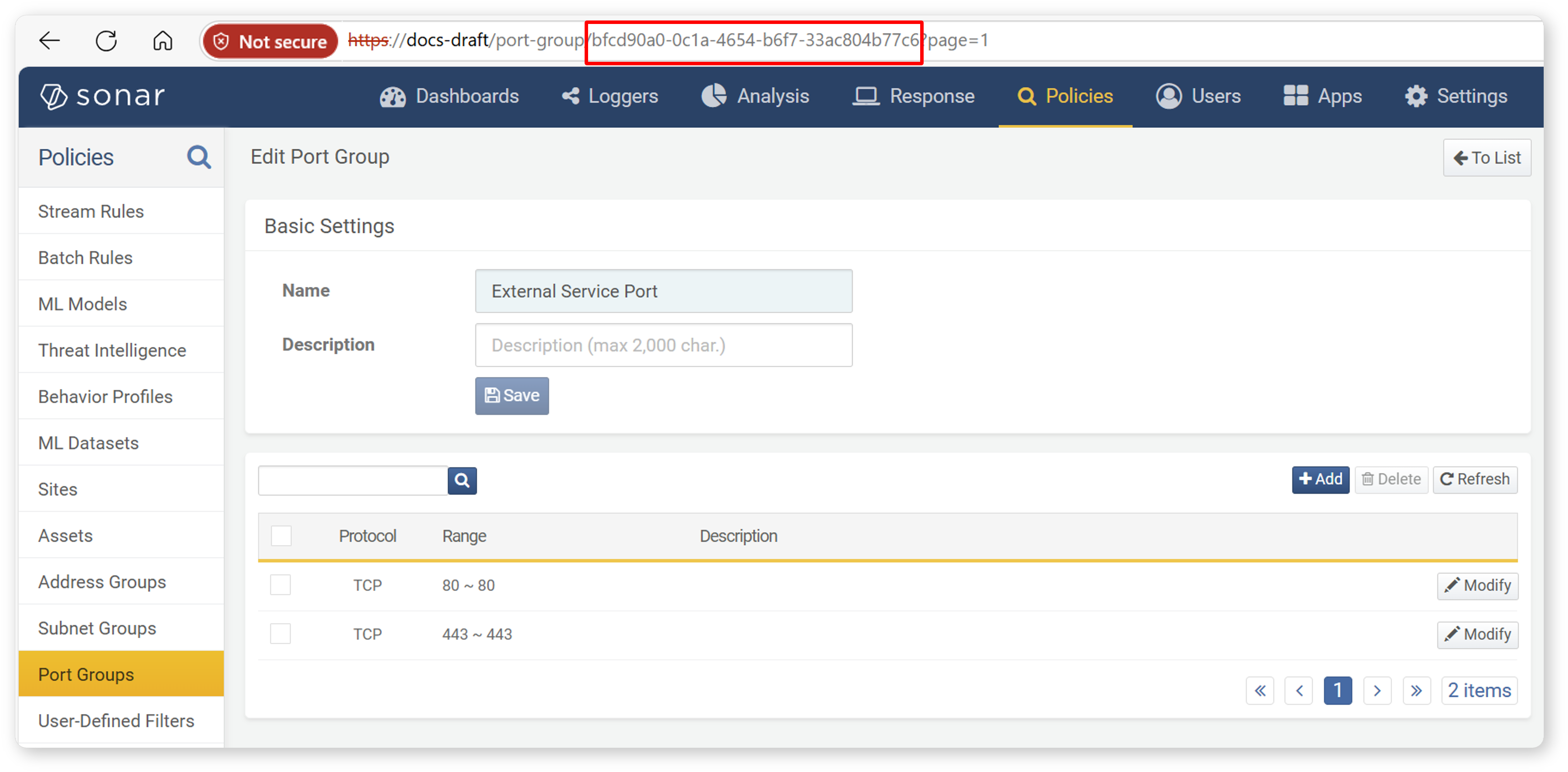
以下の表は、入力フィールドタイプが **PORT** の場合にシナリオビルダーで利用できるポートグループ関連ルールをまとめたものです。詳細は [フィールドタイプ別ルールとパラメータ](https://docs.logpresso.comnull) を参照してください。

|  |  |  |  |
| --- | --- | --- | --- |
| ルール | パラメータ | 範囲 | 説明 |
| ポートグループに含まれる | 対象ポートグループ | ポートグループを選択 | フィールド値がポートグループに含まれる場合にフィルタリング |

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、[matchport](https://docs.logpresso.comnull) コマンドや [matchport()](https://docs.logpresso.comnull) 関数を利用してポー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ポートグループを利用可能です。

[matchport](https://docs.logpresso.comnull) コマンドや [matchport()](https://docs.logpresso.comnull) 関数を利用するには、ポートグループのGUIDが必要です。GUIDはブラウザのアドレスバーで確認できます。



#### ポートグループの削除

ポートグループを削除するには、以下の手順に従います。

**ポートグループ** 一覧で、削除したいポー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。

**ポートグループ削除** ダイアログで削除対象のポートグループを確認し、**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。

バッチルールまたはストリームルールで参照されているポートグループを削除すると、該当ルールが正しく動作しなくなる可能性があります。