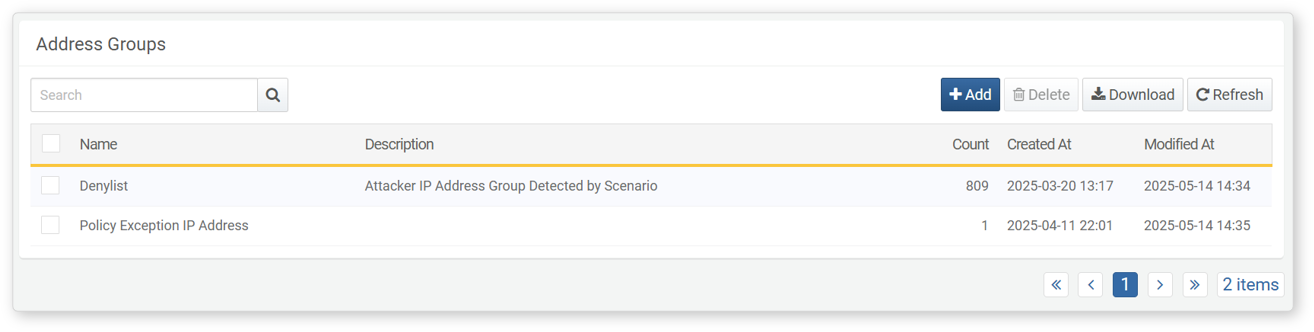
### アドレスグループ

#### 概要

アドレスグループは、IPアドレスを用途別にグループ化して管理するための機能です。アドレスグループは、特定期間に攻撃者や異常なネットワークホストのIPアドレスを登録・管理したり、特定のIPアドレスを検出ルールから除外する目的で利用できます。また、アドレスグループはファイアウォールやIPSなどのネットワークアクセス制御システムのIPブロックリストとしても活用できます。

#### アドレスグループの検索

**ポリシー > アドレスグループ** 画面で、アドレスグループの一覧を表示・検索できます。



* **名前**: アドレスグループの一意な名称
* **説明**: アドレスグループの説明
* **件数**: アドレスグループに登録されているIPアドレスの数
* **作成日時**: アドレスグループが作成された日時
* **最終変更日時**: アドレスグループが最後に変更された日時

特定のアドレスグループを検索する場合は、ツールバーの検索ツールを利用します。検索ツールは、**名前** または **説明** フィールドに入力したキーワードを含むアドレスグループを検索します。大文字・小文字は区別されません。

アドレスグループ一覧のダウンロード

アドレス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。

アドレスグループ一覧の更新

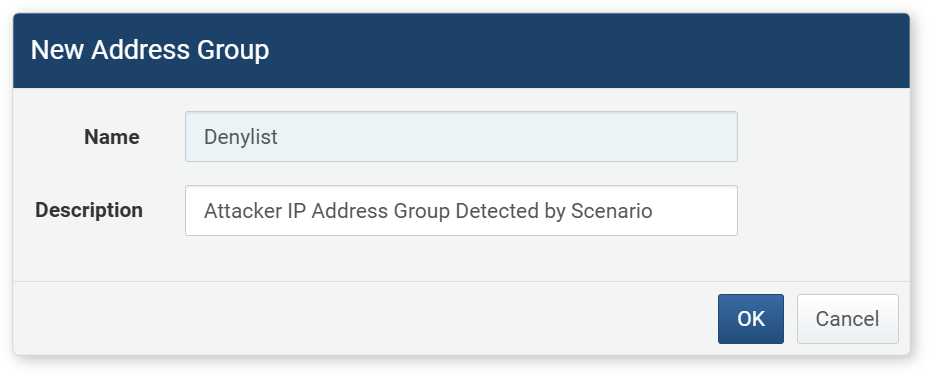
アドレスグループ一覧を最新情報に更新するには、ツールバーの **更新** をクリックします。

#### アドレスグループの追加

アドレスグループを追加するには、以下の手順を実行します。

**ポリシー > アドレスグループ** 画面で、ツールバーの **追加** をクリックします。

**アドレスグループ追加** 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**: アドレスグループ名（最大50文字）
* **説明**: アドレスグループの説明（最大2,000文字）

#### アドレスグループの編集

アドレスグループを編集するには、以下の手順を実行します。

編集したいアドレスグループ名を一覧からクリックします。

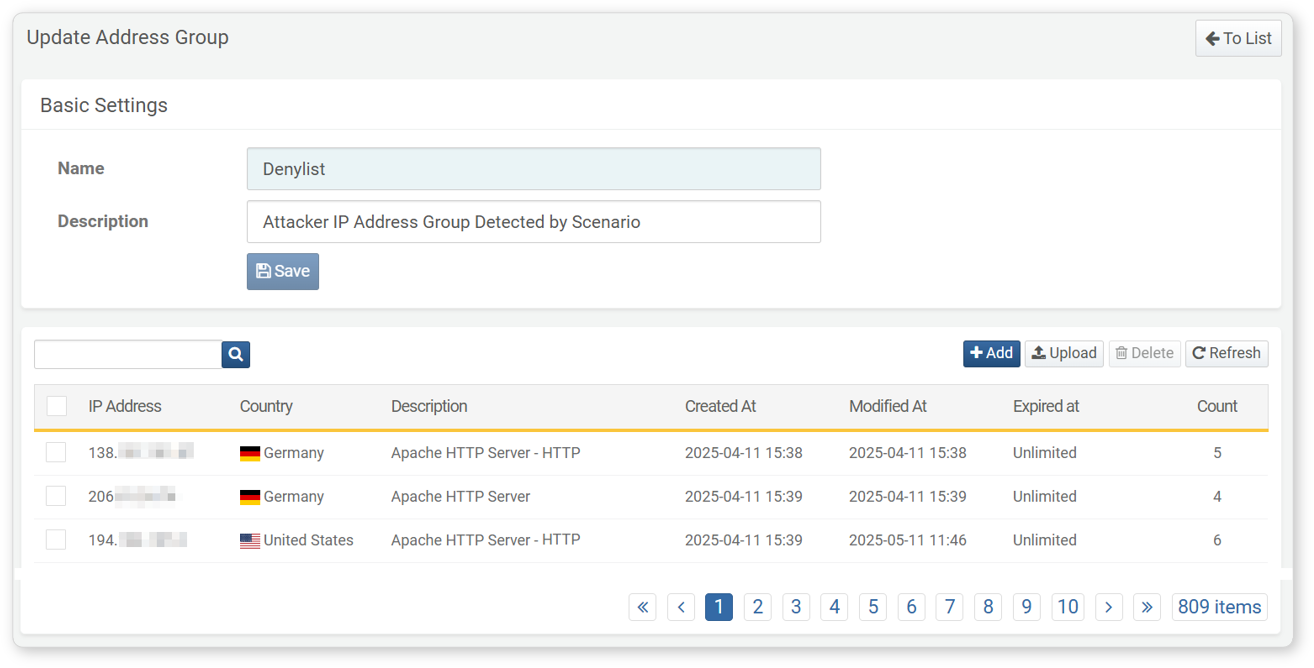
**アドレスグループ編集** 画面で情報を修正し、**保存** をクリックします。

アドレスグループ内のIPアドレス検索

アドレスグループ内の特定IPアドレスを表示・検索するには、以下の手順を実行します。

[アドレスグループ](https://docs.logpresso.comnull) 一覧で、対象のアドレスグループ名をクリックします。

**アドレスグループ編集** 画面で、IPアドレス一覧を表示または検索します。



* **IPアドレス**: アドレスグループに登録されたIPアドレス
* **国情報**: 内蔵の [geoip-lookup](https://docs.logpresso.comnull) コマンドで判定された国情報
* **説明**: IPアドレスの説明。ストリームルールやバッチルールによる登録の場合、検出ルール名が記録されます。
* **登録日時**: IPアドレスが初めて登録された日時
* **最終登録日時**: 直近の登録日時。再登録された場合、この値が更新されます。
* **有効期限**: 保持期間満了時にアドレスグループから削除される日時
* **再登録回数**: IPアドレスが再登録された回数

特定のIPアドレスを検索する場合は、ツールバーの検索ツールを利用します。検索ツールは、**IPアドレス** または **説明** フィールドに入力したキーワードを含むエントリを検索します。大文字・小文字は区別されます。

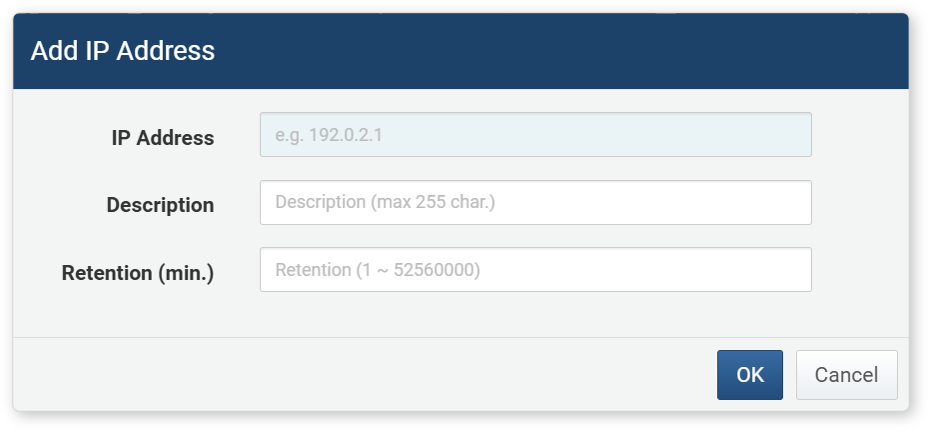
アドレスグループへのIPアドレス追加

アドレスグループにIPアドレスを追加するには、以下の手順を実行します。

[アドレスグループ](https://docs.logpresso.comnull) 一覧で、対象のアドレスグループ名をクリックします。

**アドレスグループ編集** 画面で、ツールバーの **追加** をクリックします。

**IPアドレス追加** ダイアログでIPアドレス情報を入力し、**OK** をクリックします。



* **IPアドレス**: IPv4アドレス
* **説明**: IPアドレスの説明（最大255文字）
* **保持期間（分）**: アドレスグループにIPアドレスを保持する時間。未入力の場合は無期限で保持されます。（範囲：1～52,560,000、約100年）

既に登録されているIPアドレスを再度追加した場合、再登録回数が1増加し、説明と保持期間は最新の入力内容で更新されます。

レスポンスターゲット機能で参照されているアドレスグループにIPアドレスが追加されると、システムは即座に同期対象デバイスへブロックリストの更新を要求します。

IPアドレスの削除

アドレスグループからIPアドレスを削除するには、以下の手順を実行します。

**IPアドレス** 一覧で、削除したいIPアドレス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。

**IPアドレス削除** ダイアログで詳細を確認し、**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。

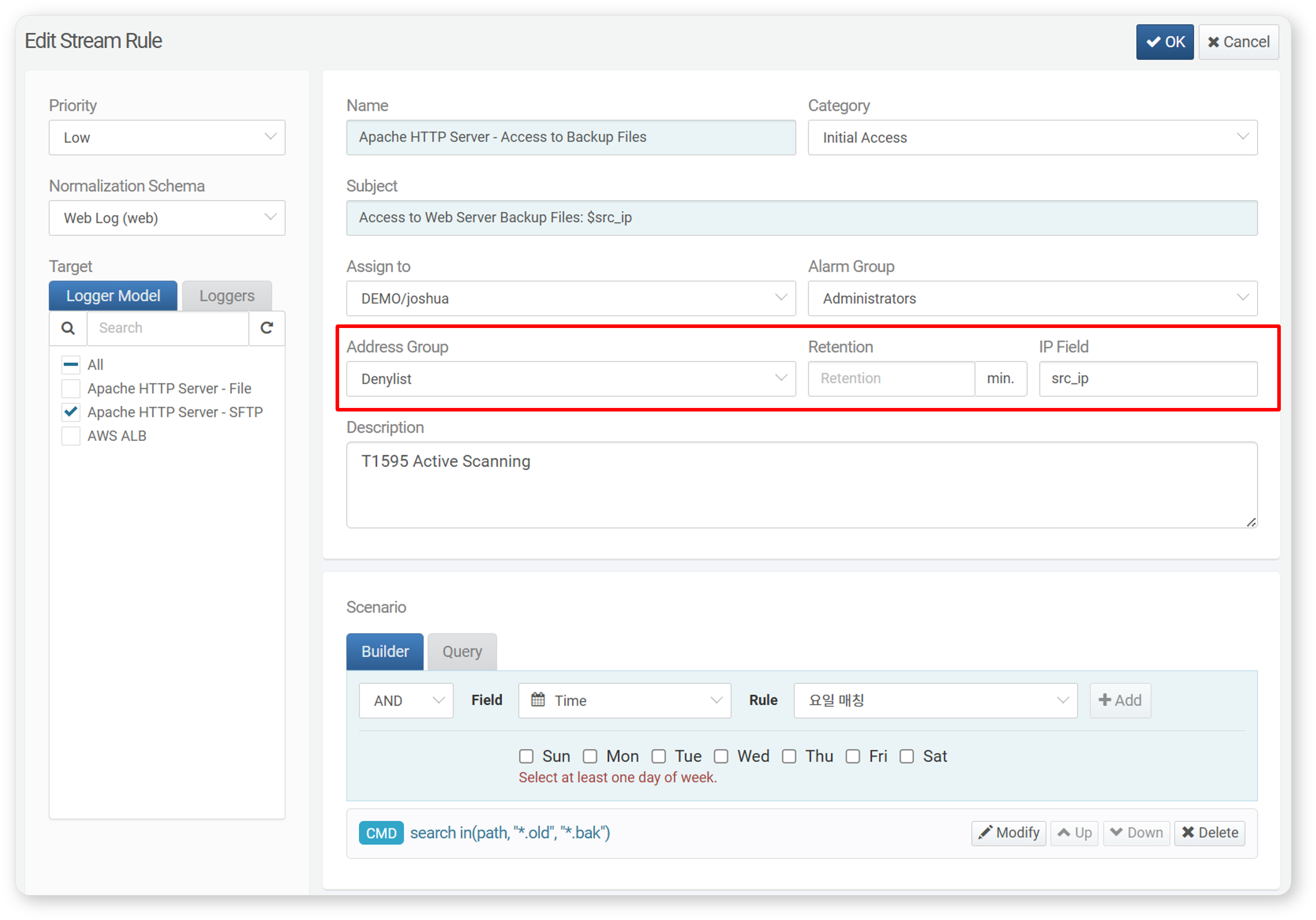
レスポンスターゲット機能で参照されているアドレスグループからIPアドレスが削除されると、システムは即座に同期対象デバイスへブロックリストの更新を要求します。有効期限切れによる削除時も同様です。

#### アドレスグループの活用

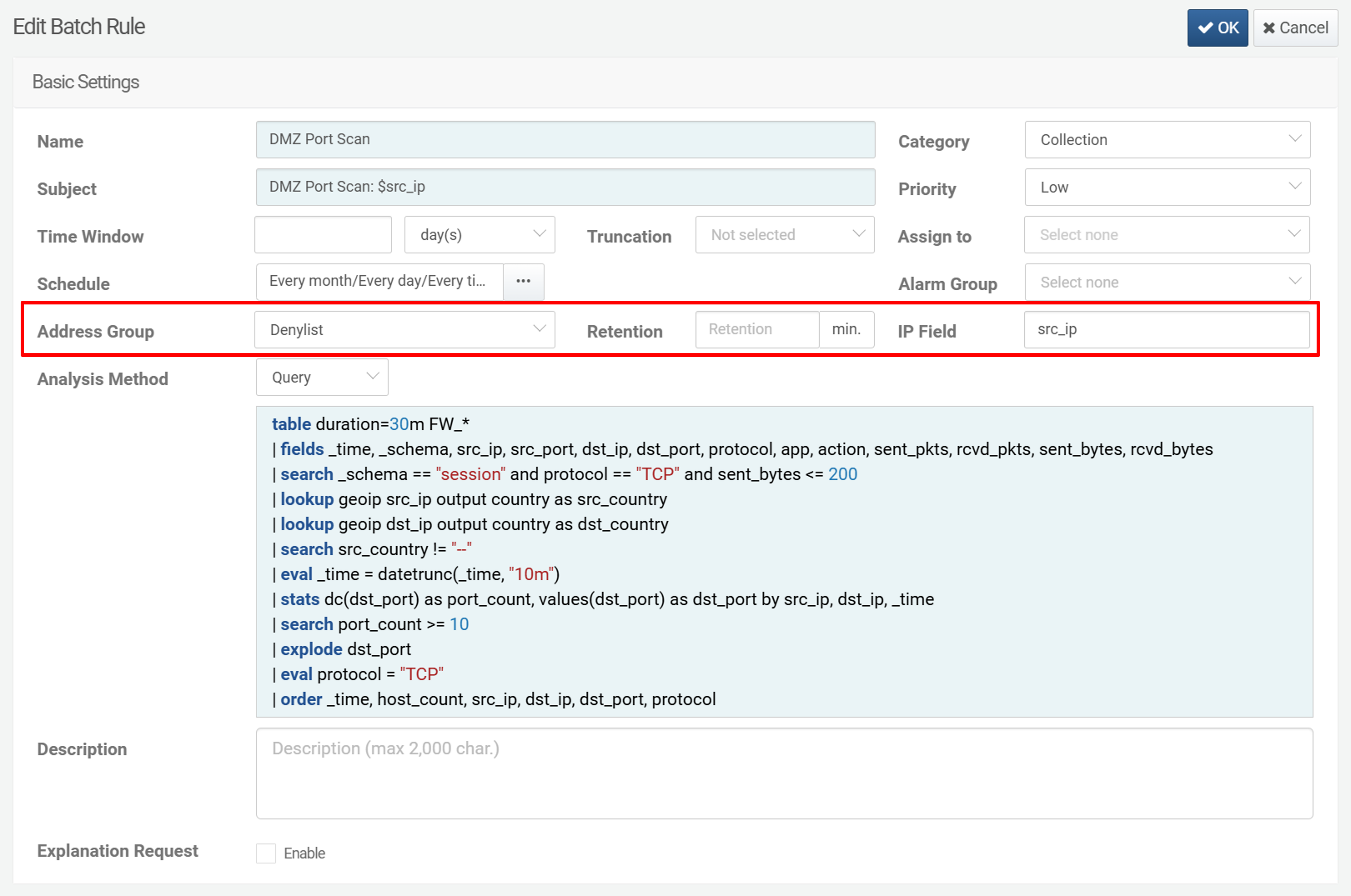
脅威検出および管理

ストリームルールやバッチルールで悪性IPアドレスを追加したり、検出された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を比較できます。

* 悪性IPアドレスの追加ストリームルールを利用して、疑わしい悪性IPアドレスを自動的にアドレスグループへ登録できます。

****

バッチ検出でも同様に動作します。



* アドレスグループとのIPアドレス比較（シナリオビルダー）シナリオビルダーを利用して、検出されたIPアドレスが特定のアドレスグループに既に登録されているかを判定する検出ルールを作成できます。

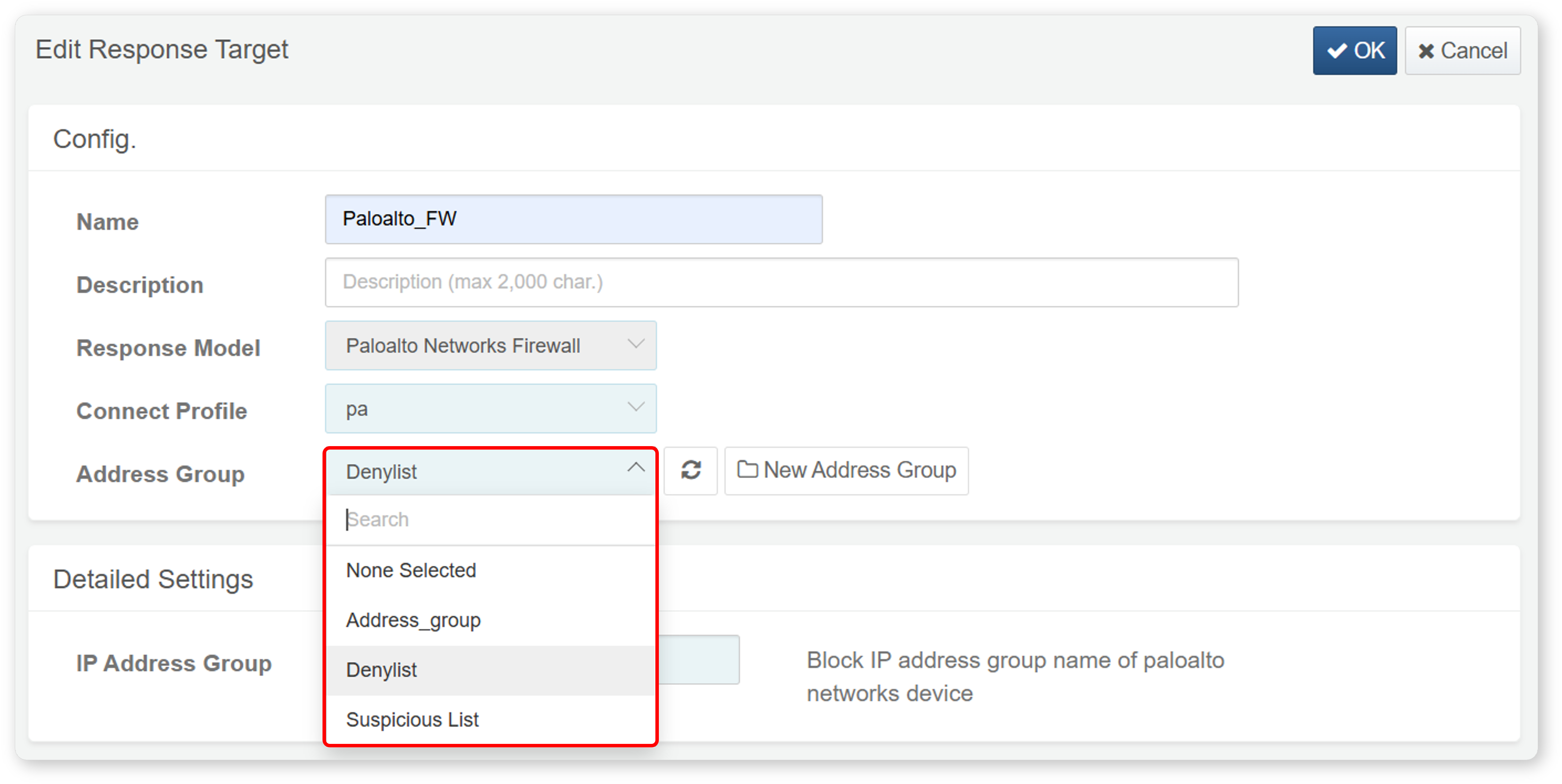
: 下表は、シナリオビルダーで入力フィールドタイプが **IP** の場合に利用できるアドレスグループ関連ルールの一覧です。詳細は [フィールドタイプ別ルールとパラメータ](https://docs.logpresso.comnull) を参照してください。

|  |  |  |  |
| --- | --- | --- | --- |
| ルール | パラメータ | 範囲 | 説明 |
| アドレスグループに含まれるIPアドレス | 対象アドレスグループ | アドレスグループ選択 | アドレスグループに含まれる値をフィルタリングします |

* クエリによるアドレスグループ比較[matchblackip](https://docs.logpresso.comnull) コマンドや [matchblackip()](https://docs.logpresso.comnull) 関数を利用して、疑わしいIPアドレスが既にアドレスグループに含まれているかを判定できます。

自動対応

脅威IPアドレスをブロックリストとしてグループ化し、ファイアウォールやIPSなどのセキュリティシステムと連携して自動的にブロックできます。



#### アドレスグループの削除

アドレスグループを削除するには、以下の手順を実行します。

[アドレスグループ](https://docs.logpresso.comnull) 一覧で、削除したいアドレス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。

**アドレスグループ削除** ダイアログで詳細を確認し、**削除** をクリックします。

ストリームルールやバッチルールで参照されているアドレスグループを削除すると、検出ルールが正しく動作しなくなる場合があります。