CVR100W VPNルータでのアクセスルールの設定

目的

アクセスコントロールリスト(ACL)は、パケットがルータインターフェイスで許可されるか拒否されるかを制御するリストです。ACLは、常に有効になるように、または定義されたスケジュールに基づいて設定されます。CVR100W VPNルータでは、セキュリティを強化するためにアクセスルールを設定できます。

このドキュメントの目的は、CVR100W VPNルータでアクセスルールを設定する方法を示すことです。

該当するデバイス

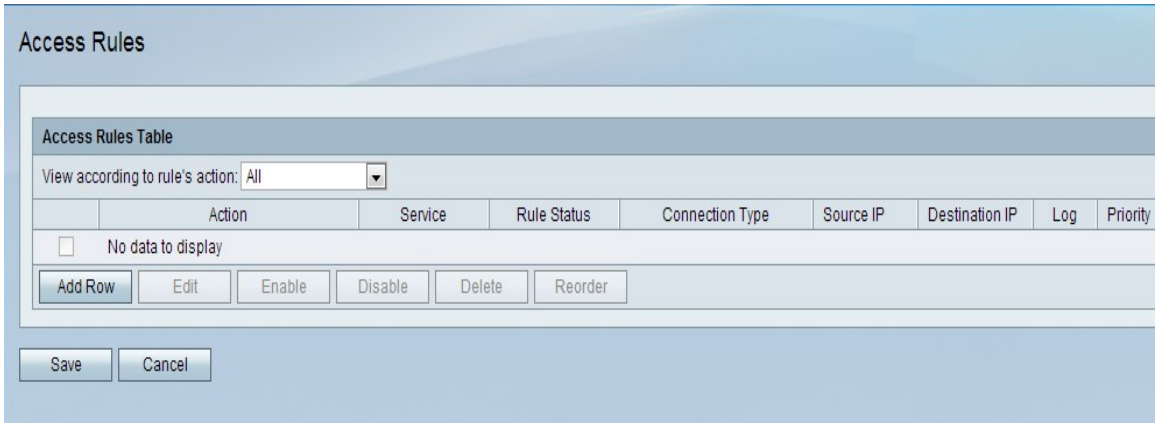
- CVR100W VPNルータ

[Software Version]

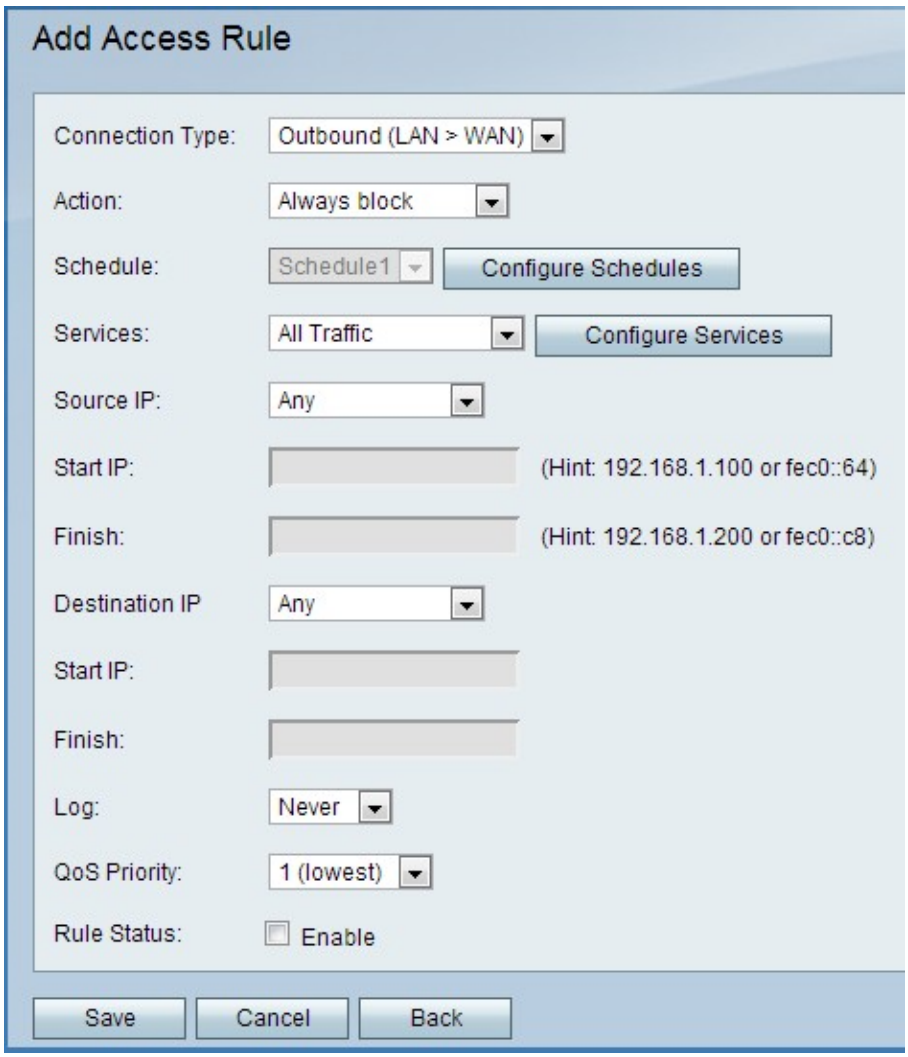
•1.0.1.19

アクセスルール

ステップ1:Web構成ユーティリティにログインし、**[Firewall] > [Access Control] > [Access Rules]を選択します。**「*アクセス規則*」ページが開きます。



ステップ2:[行の追**加]をクリック**して、新しいアクセスルールを追加します。「*アクセス規則の追*加」ページが開きます。



ステップ3:[Connection Type]ドロップダウンリストから、作成するルールのタイプを選択します。

・ アウトバウンド(LAN > WAN)：このオプションは、セキュアLANからセキュアでないWANへのパケットに影響します。

・ インバウンド(WAN > LAN)：このオプションは、非セキュアWANからセキュアLANへのパケットに影響します。

・ インバウンド(WAN > DMZ)：このオプションは、安全でないWANからDMZへのパケットに影響します。DMZは、LANとWANを分離してセキュリティ層を提供するネットワークのセグメントです。

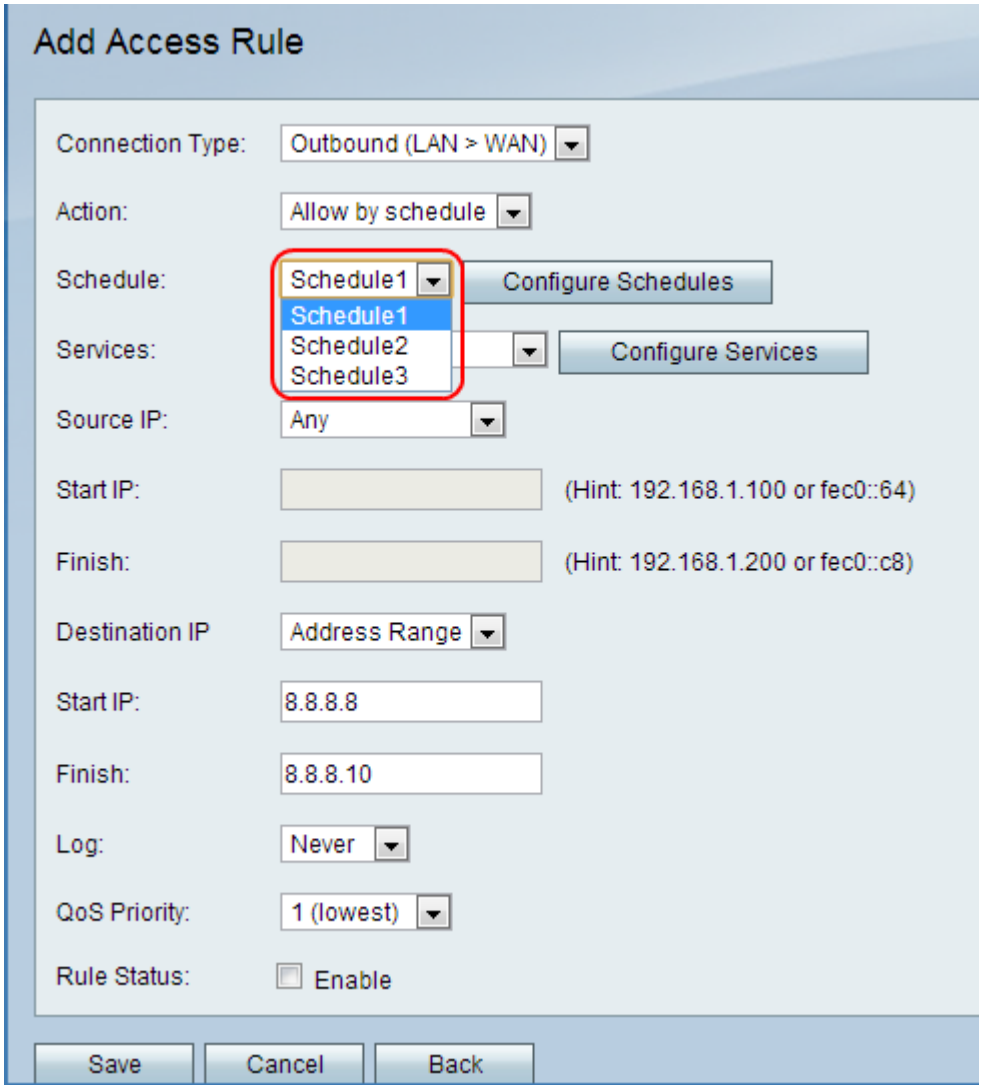
ステップ4:[Action（アクション）]ドロップダウンリストから、ルールに適用するアクションを選択します。

・ Always Block：常にパケットをブロックします。

・ Always Allow：常にパケットを許可します。

・ スケジュールでブロック：指定されたスケジュールに基づいてパケットがブロックされます。

・ Allow by schedule：指定されたスケジュールに基づいてパケットが許可されます。



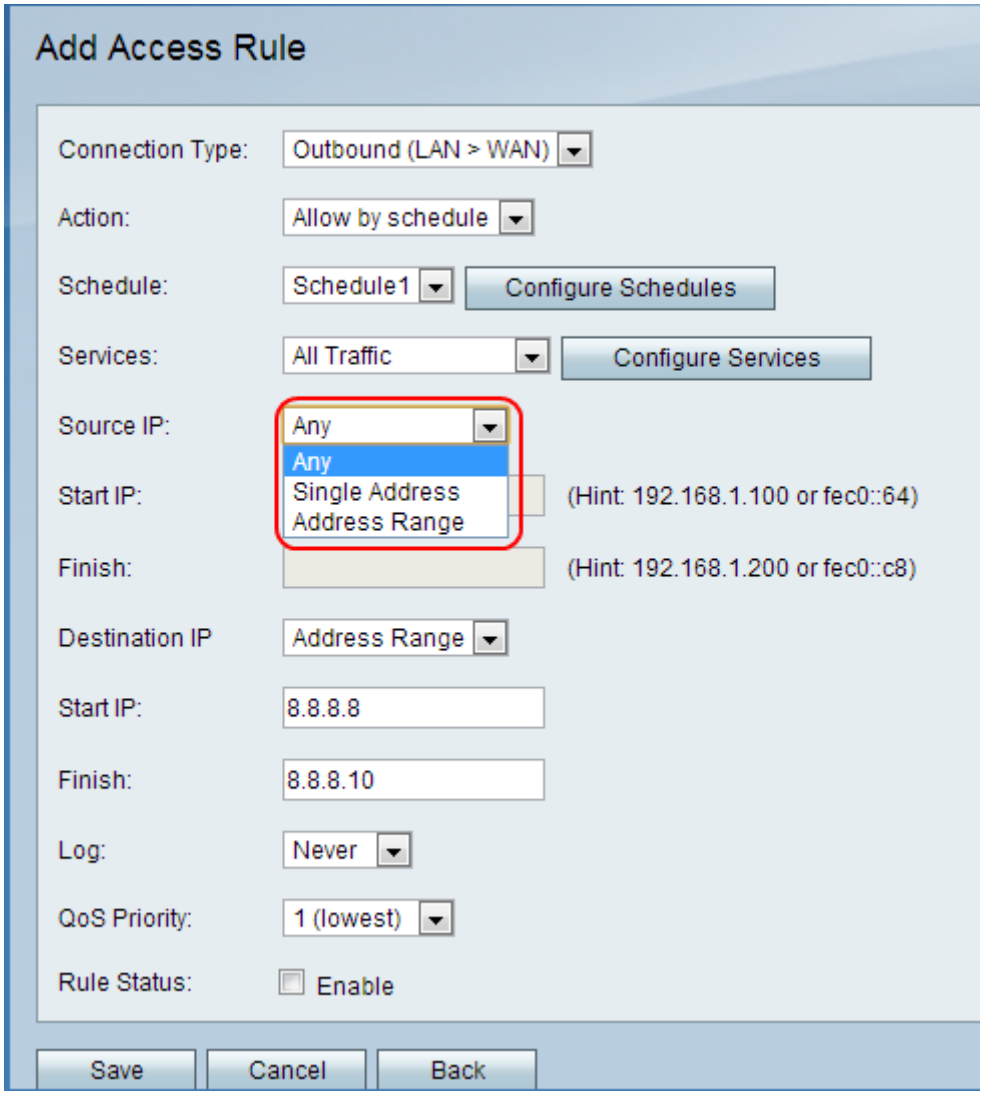
ステップ5:[Schedule（スケジュール）]ドロップダウンリストから、ルールに適用するスケジュールを選択します。

注：手順4で[常にブロック]または[常に許可]オプションを選択すると、ドロップダウンリストが淡色表示されます。

ステップ6:（オプション）ファイアウォールスケジュールを設定するには、[スケジュール**の設定]をクリックします**。スケジュールを設定するには、「*CVR100W VPNルータのファイアウォールスケジュール管理」を参照してください*。

ステップ7:[Services（サービス）]ドロップダウンリストから、許可またはブロックするサービスを選択します。ドロップダウンリストには、CVR100W VPNルータで使用可能なデフォルトサービスが含まれています。サービスは、使用中のプロトコルのタイプと、それが適用されるポートを決定します。

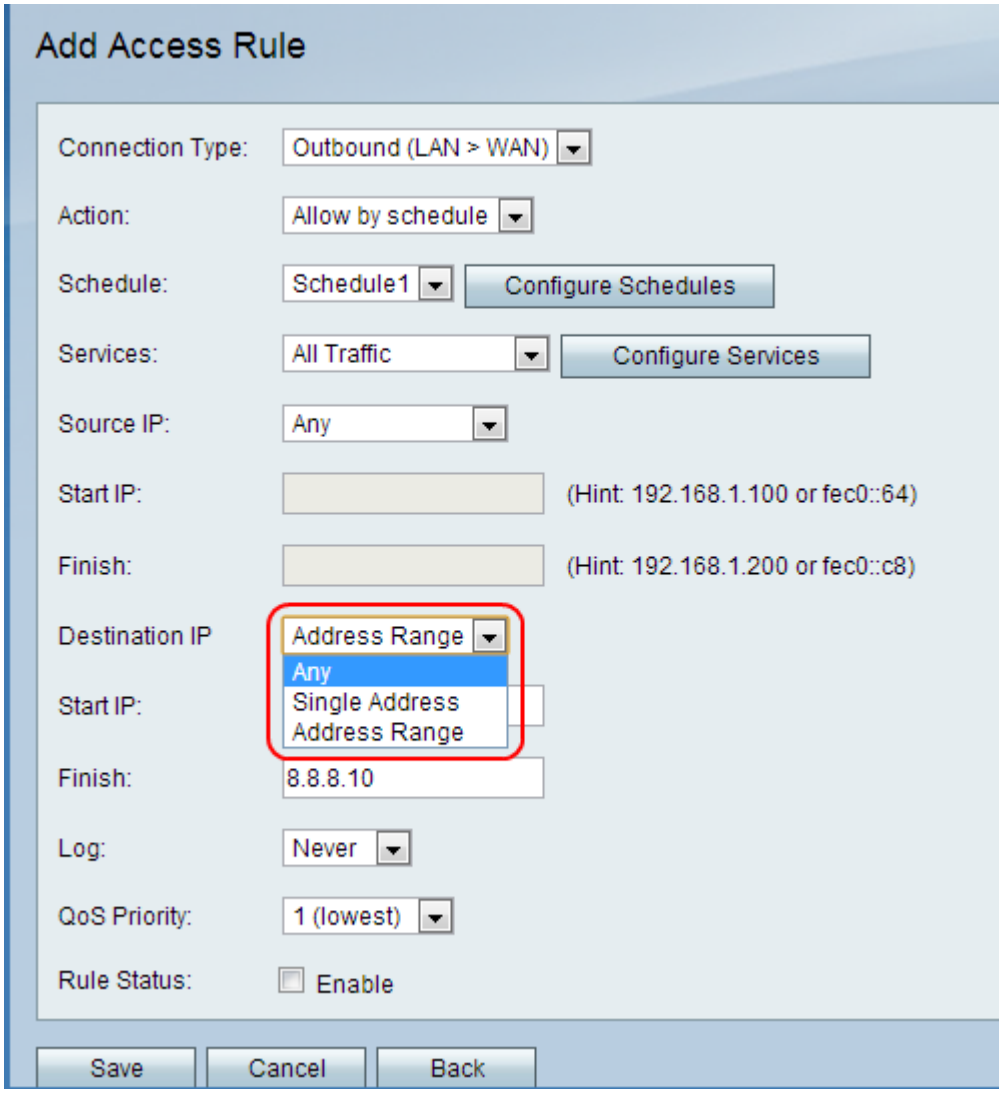
ステップ8:（オプション）サービスを設定するには、[サービスの設定(Configure Services)]をクリックします。サービスを設定するには、「*CVR100W VPNルータのサービス管理」を参照してください*。



ステップ9:[Source IP]ドロップダウンリストから、ルールが適用される送信元IPアドレスを選択します。

- Any：このオプションは、すべての送信元IPアドレスにルールを適用します。
- Single Address：このオプションは、1つのIPアドレスにルールを適用します。[Start IP]フィールドに送信元IPアドレスを入力します。
- アドレス範囲：このオプションは、IPアドレスの範囲にルールを適用します。[Start IP]フィールドにアドレス範囲の開始IPアドレスを入力し、[Finish IP]フィールドにアドレス範囲の終了IPアドレスを入力します。

注：[Any]オプションを選択すると、[Start IP]フィールドは淡色表示されます。また、[Any]または[Single Address]オプションを選択すると、[Finish]フィールドが淡色表示されます。



ステップ10:[Destination IP]ドロップダウンリストから、ルールが適用される宛先IPアドレスを選択します。

・ Any：このオプションは、すべての送信元IPアドレスにルールを適用します。

・ Single Address：このオプションは、1つのIPアドレスにルールを適用します。[Start IP]フィールドに宛先IPアドレスを入力します。

・ アドレス範囲：このオプションは、IPアドレスの範囲にルールを適用します。[Start IP]フィールドにアドレス範囲の開始IPアドレスを入力し、[Finish IP]フィールドにアドレス範囲の終了IPアドレスを入力します。

注：[Any]オプションを選択すると、[Start IP]フィールドは淡色表示されます。また、[Any]または[Single Address]オプションを選択すると、[Finish]フィールドが淡色表示されます。

ステップ11:[Log]ドロップダウンリストから、ログオプションを選択します。ログは、監査およびセキュリティ管理に使用されるシステムレコードを生成します。

・ Never：ログを無効にします。

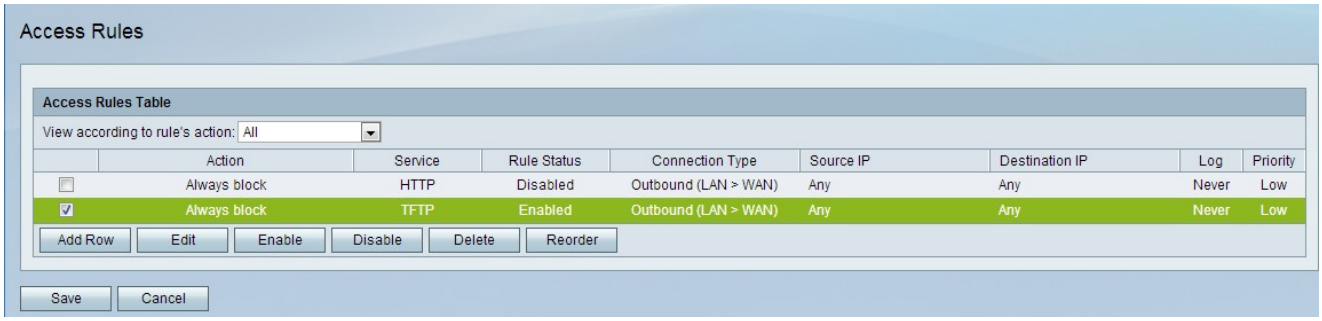
・ 常に：パケットがルールに一致すると、常にログが作成されます。

ステップ12:[QoS Priority]ドロップダウンリストから、ルールの発信IPパケットのプライオリティを選択します。プライオリティ1は最低で、プライオリティ4は最高です。優先順位

の高いキューのパケットは、優先順位の低いキューのパケットよりも先に転送されます。

ステップ13:[Rule Status]フィールドの[**Enable**]チェックボックスをオンにして、ルールを有効にします。

ステップ14:[**Save**]をクリックします。



ステップ15:（オプション）アクセスルールテーブルでアクセスルールを編集するには、エントリのチェックボックスをオンにし、[**Edit**]をクリックし、必要なフィールドを編集して、[**Save**]をクリックします。

ステップ16:（オプション）アクセスルールテーブルのアクセスルールエントリを削除するには、エントリのチェックボックスをオンにし、[削除]をクリックし、[**保存**]をクリックします。

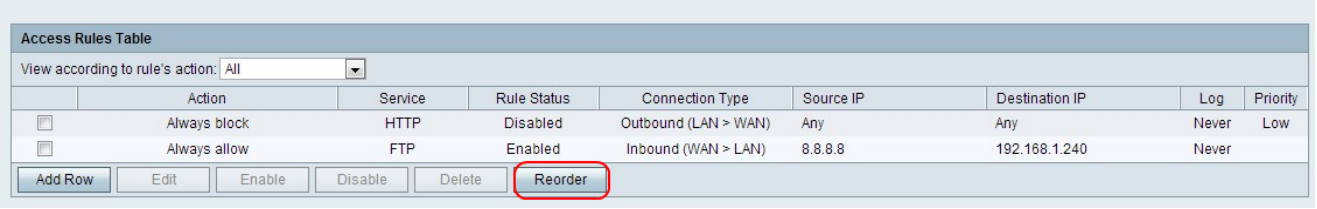
注：編集または削除する前に保存する必要があることを示すプロンプトが表示されます。

ステップ17:（オプション）アクセスルールテーブルでアクセスルールエントリを有効にするには、エントリのチェックボックスをオンにし、[有効にする]をクリックし、[**保存**]をクリックします。

ステップ18:（オプション）アクセスルールテーブルのアクセスルールエントリを無効にするには、エントリのチェックボックスをオンにし、[無効にする]をクリックし、[**保存**]をクリックします。

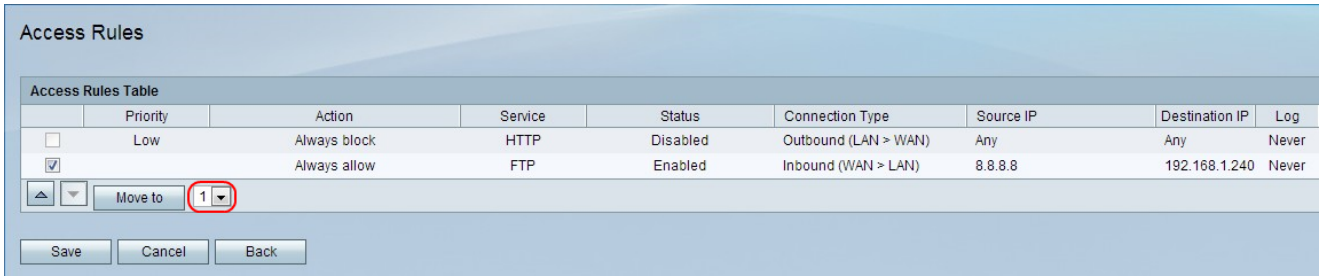
アクセスルールの並べ替え

アクセスルールは、アクセスルールテーブルに特定の順序で表示されます。 順序は、ルールの適用方法を示します。テーブルの最初のルールが適用される最初のルールです。その後、リストの2番目のルールが適用されます。リオーダー機能は、CVR100W VPNルータの重要なオプションです。



ステップ1:[並べ替え]をクリックして、アクセスルールを並べ替えます。

ステップ2：並べ替えるアクセスルールのチェックボックスをオンにします。



ステップ3：ドロップダウンリストから、指定したルールを移動する位置を選択します。

ステップ4:[Move to]をクリックしてルールの順序を変更します。ルールがテーブル内の指定された位置に移動します。

注：上矢印ボタンと下矢印ボタンを使用して、アクセスルールを並べ替えることができます。

ステップ5:[Save]をクリックします。