RV130およびRV130Wのアクセスルールの追加と設定

目的

ネットワークデバイスは、アクセスルールを備えた基本的なトラフィックフィルタリング機能を提供します。アクセスルールは、プロトコル、送信元と宛先のIPアドレス、またはネットワーク設定に基づいて、許可ルールまたは拒否ルール（パケットの転送または廃棄）を指定するアクセスコントロールリスト(ACL)の単一のエントリです。

このドキュメントの目的は、RV130およびRV130Wでアクセスルールを追加および設定する方法を示すことです。

適用可能なデバイス

- RV130
- RV130W

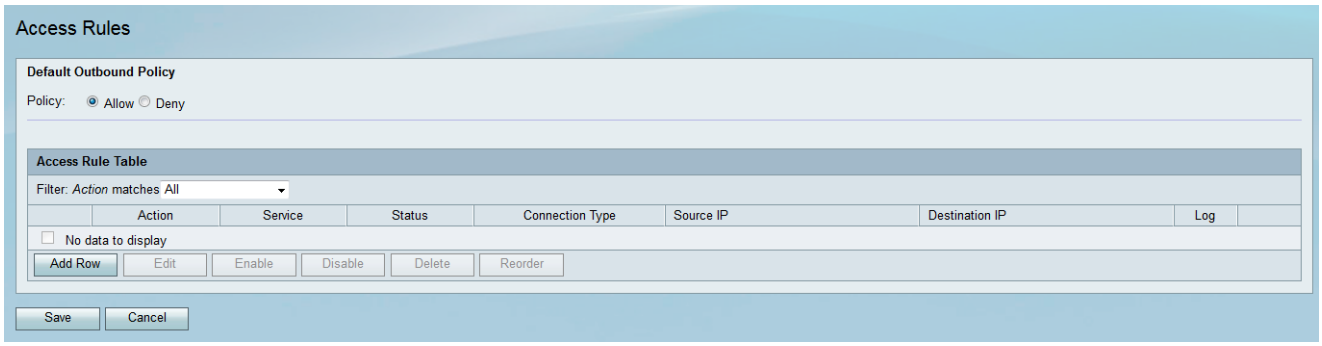
ソフトウェアのバージョン

•Version 1.0.1.3

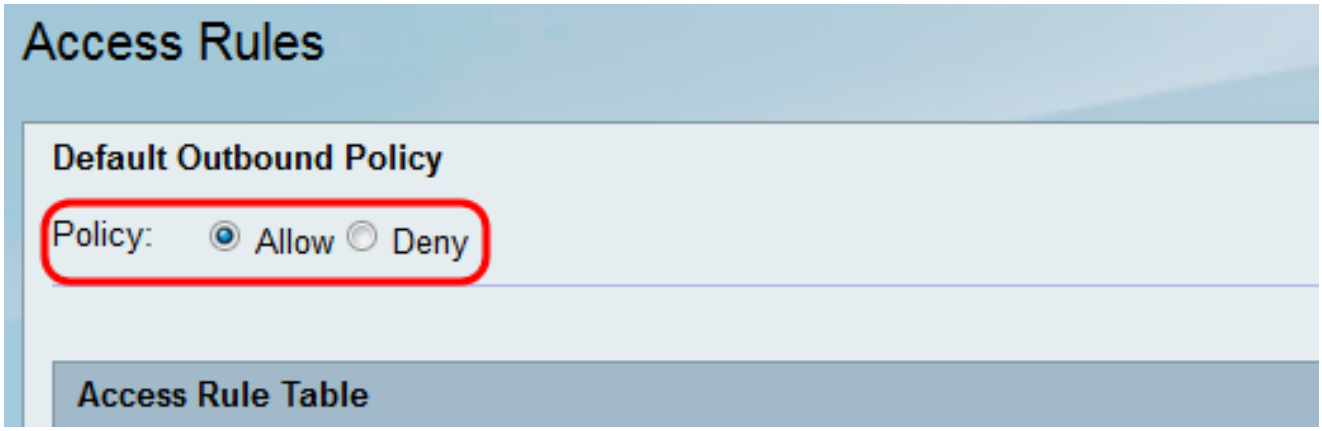
アクセスルールの追加と設定

デフォルトのアウトバウンドポリシーの設定

ステップ 1：Web設定ユーティリティにログインし、Firewall > Access Rulesの順に選択します。アクセスルールページが開きます。



ステップ 2：Default Outbound Policyエリアで、目的のオプションボタンをクリックして、発信トラフィックのポリシーを選択します。ポリシーは、アクセスルールまたはインターネットアクセスポリシーが設定されていないときはいつでも適用されます。デフォルト設定はAllowで、インターネットへのすべてのトラフィックの通過を許可します。

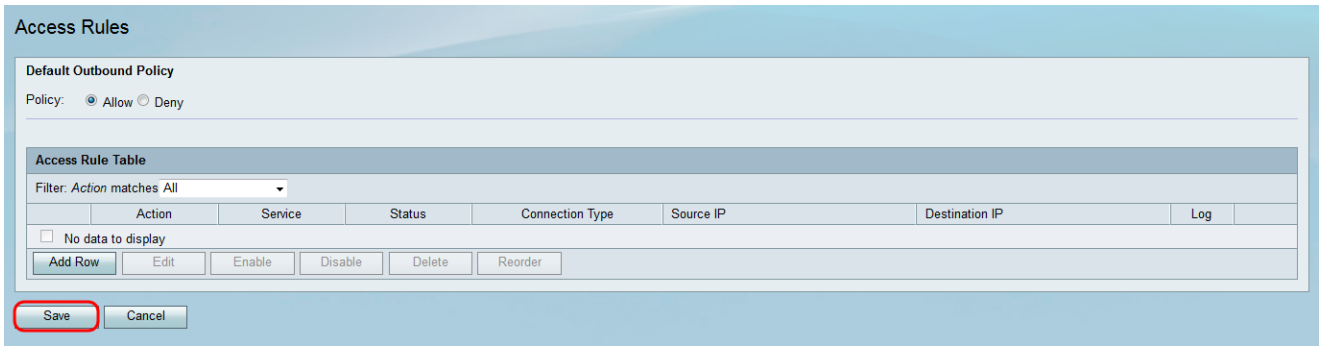


使用可能なオプションは、次のように定義されます。

- Allow:LANからインターネットに送信されるすべてのタイプのトラフィックを許可します。

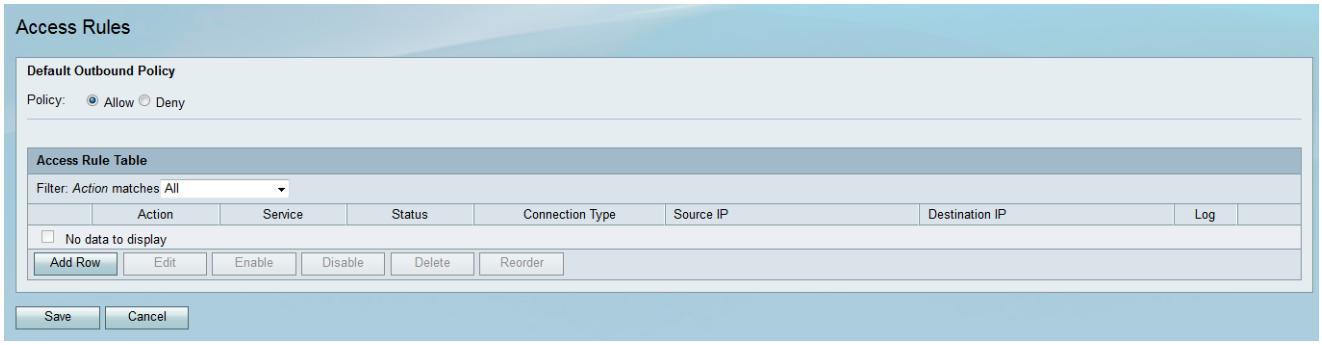
- Deny — LANからインターネットに送信されるすべてのタイプのトラフィックをブロックします。

ステップ 3：[Save] をクリックして、設定を保存します。

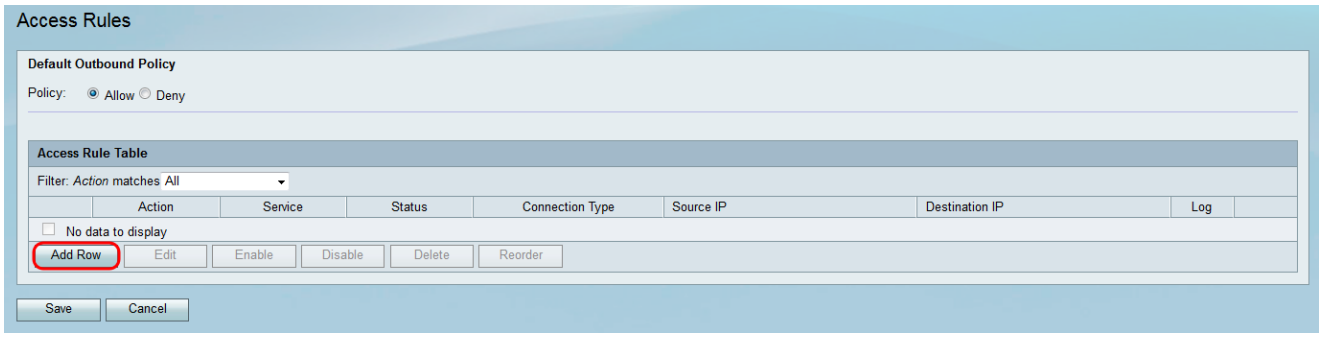


アクセスルールの追加

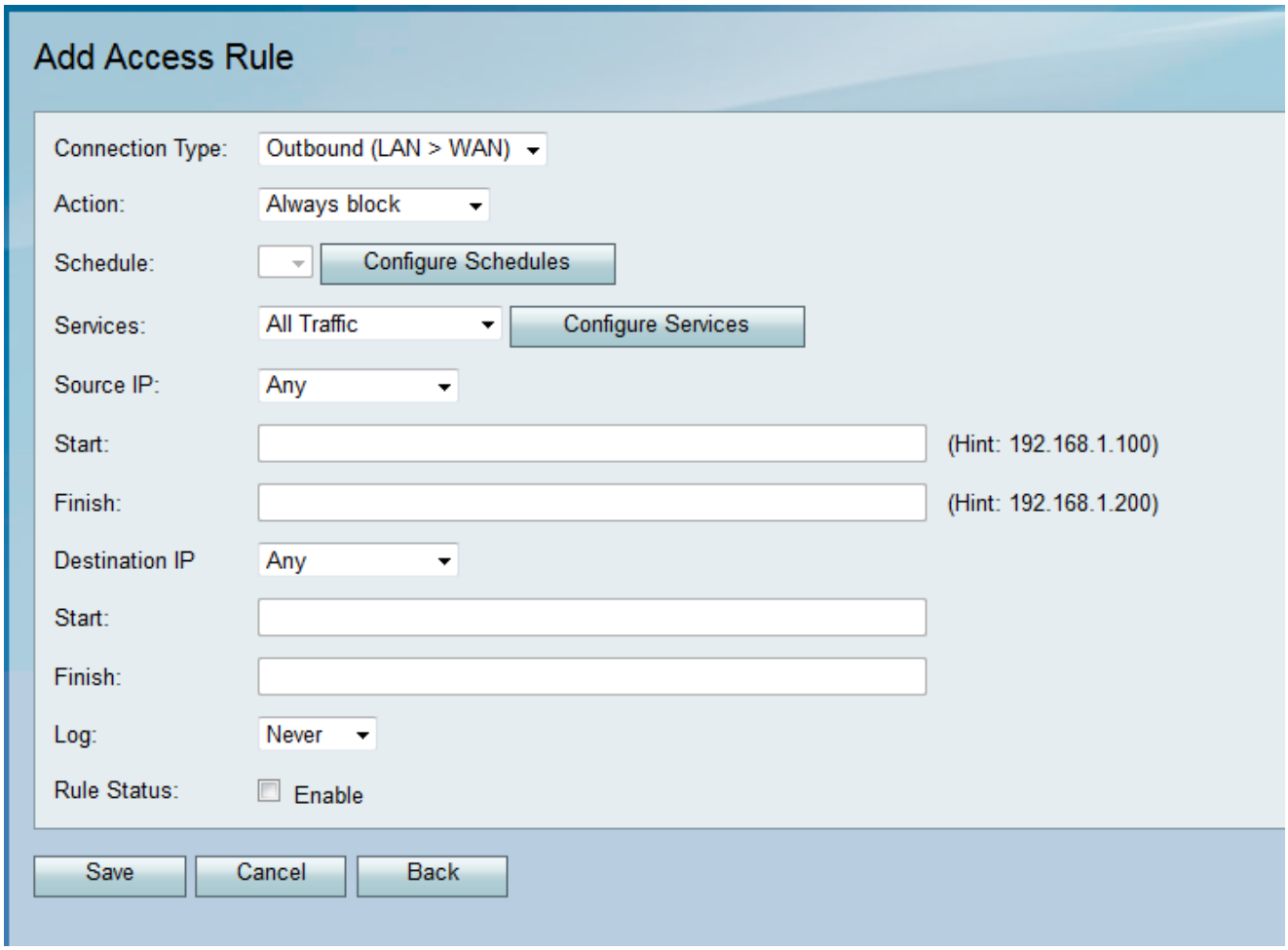
ステップ 1：Web設定ユーティリティにログインし、Firewall > Access Rulesの順に選択します。「アクセスルール」ウィンドウが開きます。



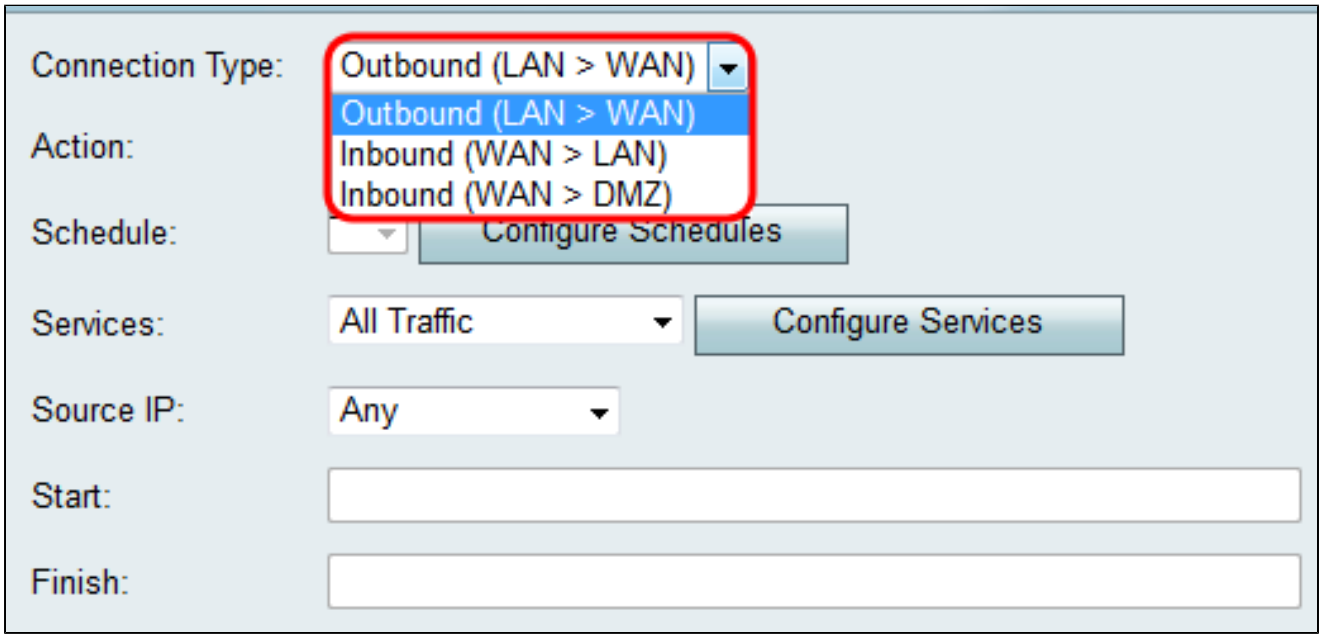
ステップ 2：新しいアクセスルールを追加するには、Access Rule TableでAdd Rowをクリックします。



アクセスルール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、ルールが適用されるトラフィックのタイプを選択します。



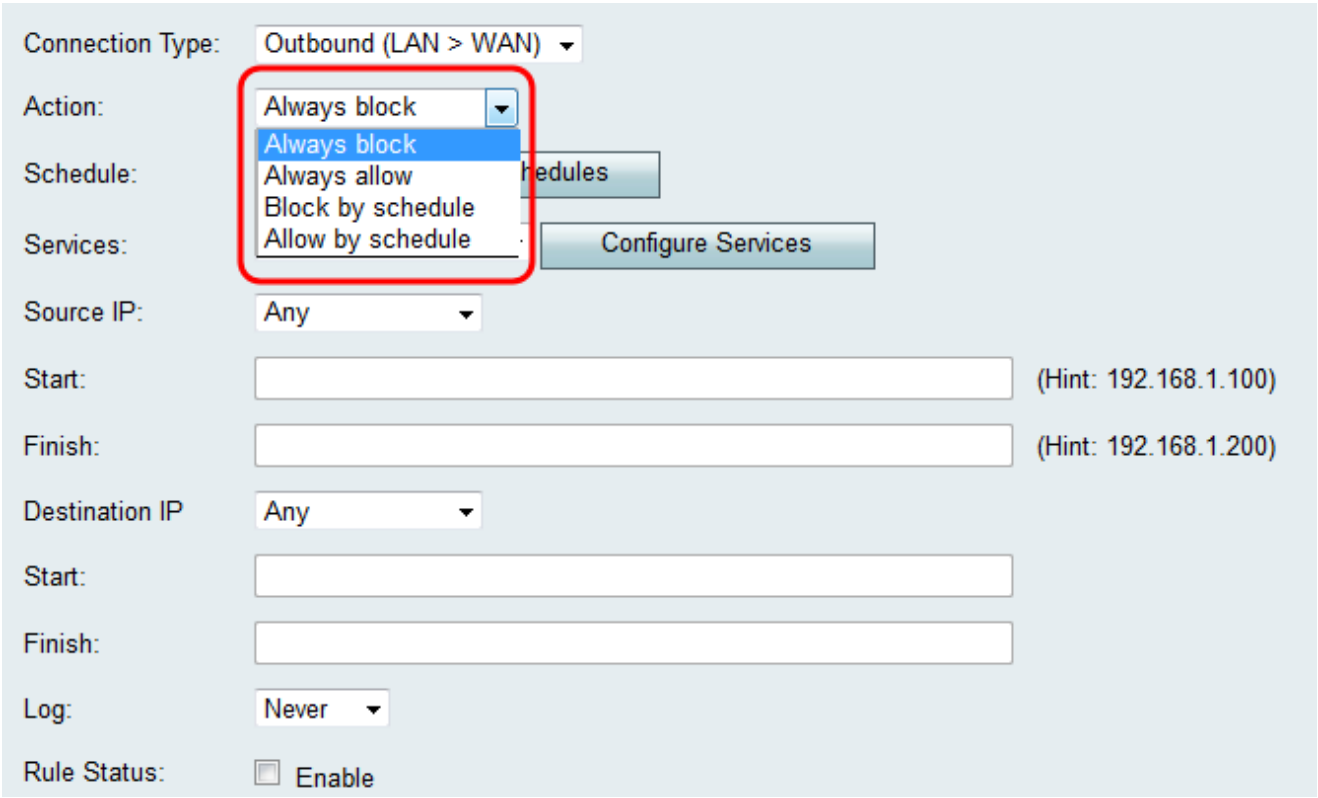
使用可能なオプションは、次のように定義されます。

・アウトバウンド(LAN > WAN)：このルールは、ローカルネットワーク(LAN)から到達してインターネット(WAN)に送信されるパケットに影響します。

・インバウンド(WAN > LAN)：このルールは、インターネット(WAN)からローカルネットワーク(LAN)に着信するパケットに影響します。

・インバウンド(WAN > DMZ)：このルールは、インターネット(WAN)から来て非武装地帯(DMZ)サブネットワークに入るパケットに影響します。

ステップ 4：Actionドロップダウンリストから、ルールが一致した場合に実行されるアクションを選択します。



使用可能なオプションは、次のように定義されます。

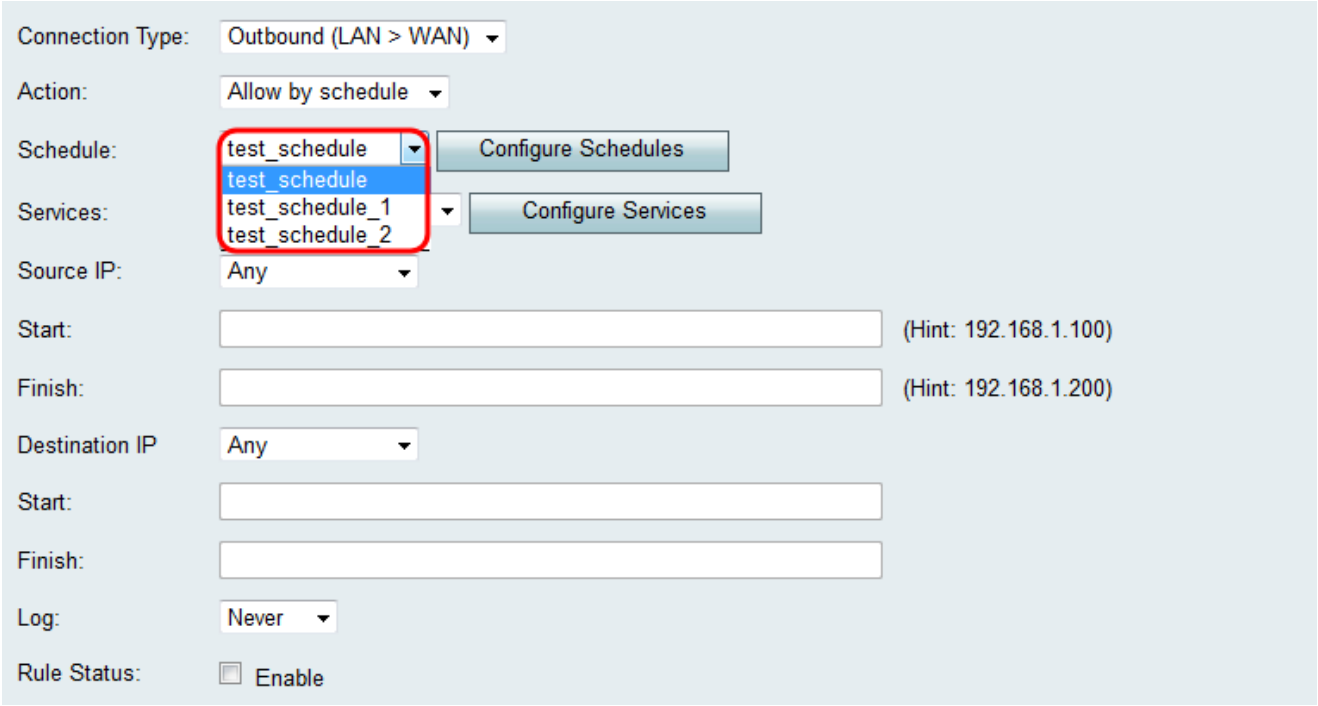
・ Always Block：条件が一致する場合は常にアクセスを拒否します。ステップ 6 に進みます。

・ Always Allow：条件が一致する場合は常にアクセスを許可します。ステップ 6 に進みます。

・スケジュールによるブロック：事前設定されたスケジュールで条件が一致した場合、アクセスを拒否します。

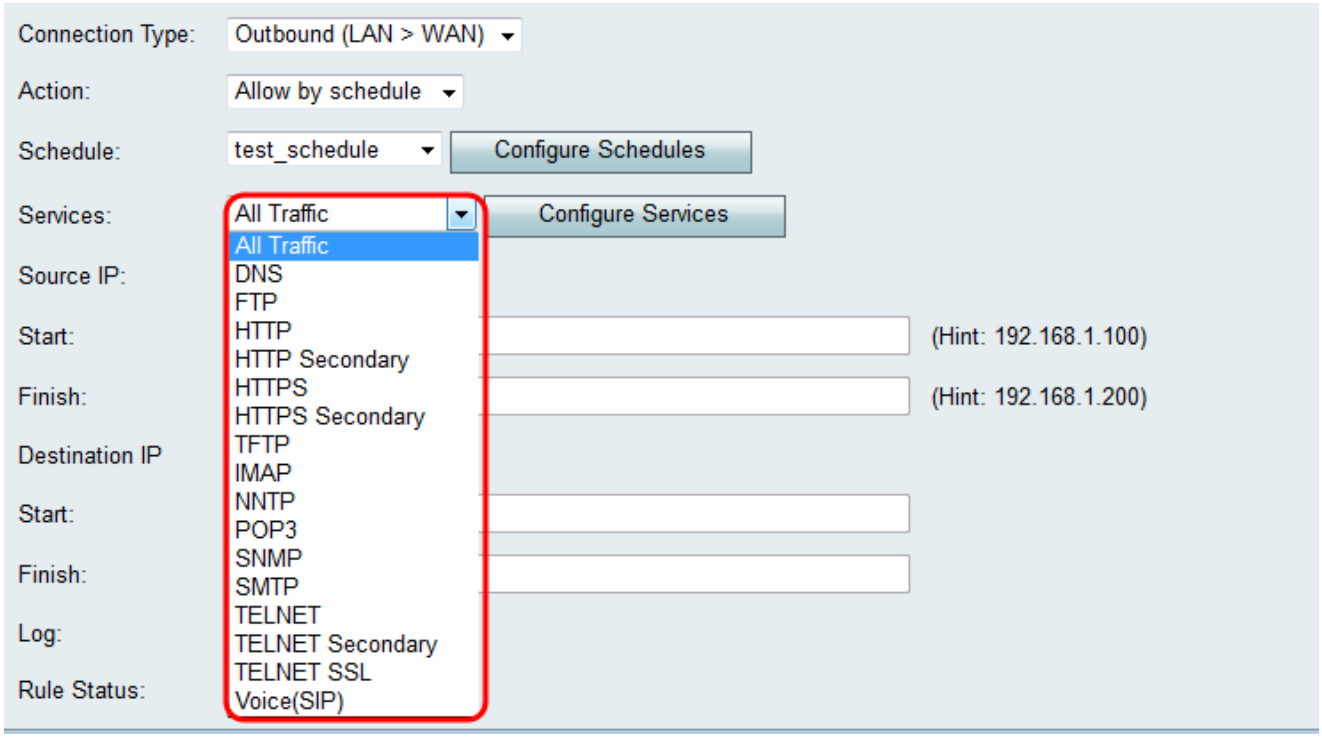
・スケジュールによる許可：事前設定されたスケジュールで条件が一致する場合にアクセスを許可します。

ステップ 5：手順4でBlock by scheduleまたはAllow by scheduleを選択した場合は、Scheduleドロップダウンリストから適切なスケジュールを選択します。



注：スケジュールを作成または編集するには、[スケジュールの構成]をクリックします。詳細およびガイドラインについては、『RV130およびRV130Wでのスケジュールの設定』を参照してください。

手順 6：Servicesドロップダウンリストから、アクセスルールが適用されるサービスのタイプを選択します。



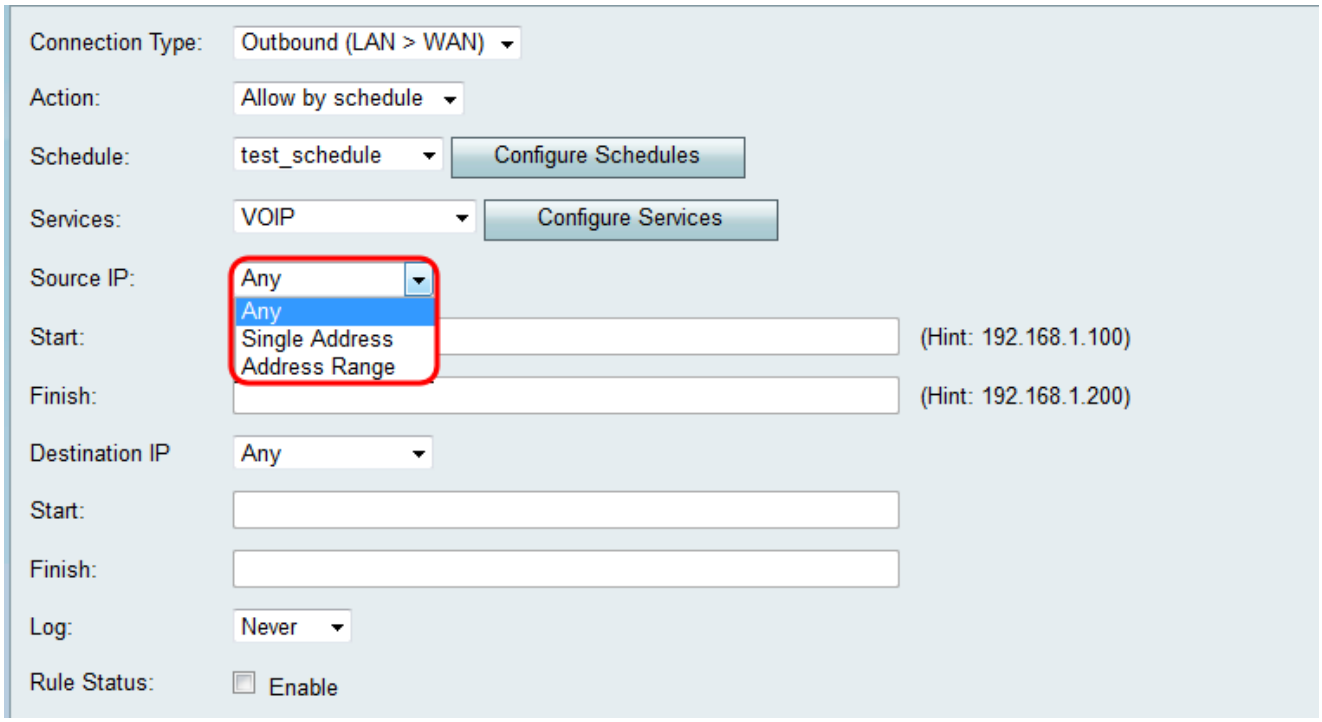
注：サービスを追加または編集する場合は、Configure Servicesをクリックします。詳細とガイドラインについては、『RV130およびRV130Wでのサービス管理の設定』を参照してください。

発信トラフィックの送信元および宛先IPの設定

アクセスルールの追加のステップ3で接続タイプとしてアウトバウンド(LAN > WAN)が選択されている場合は、このセクションの手順に従います。

注：アクセスルールの追加のステップ3でインバウンド接続タイプを選択した場合は、次のセクションに進んでください。 着信トラフィックの送信元および宛先IPの設定』を参照してください。

ステップ 1：Source IPドロップダウンリストから、送信元IPの定義方法を選択します。発信トラフィックの場合、送信元IPはファイアウォール規則が適用されるアドレス (LAN内) を指します。



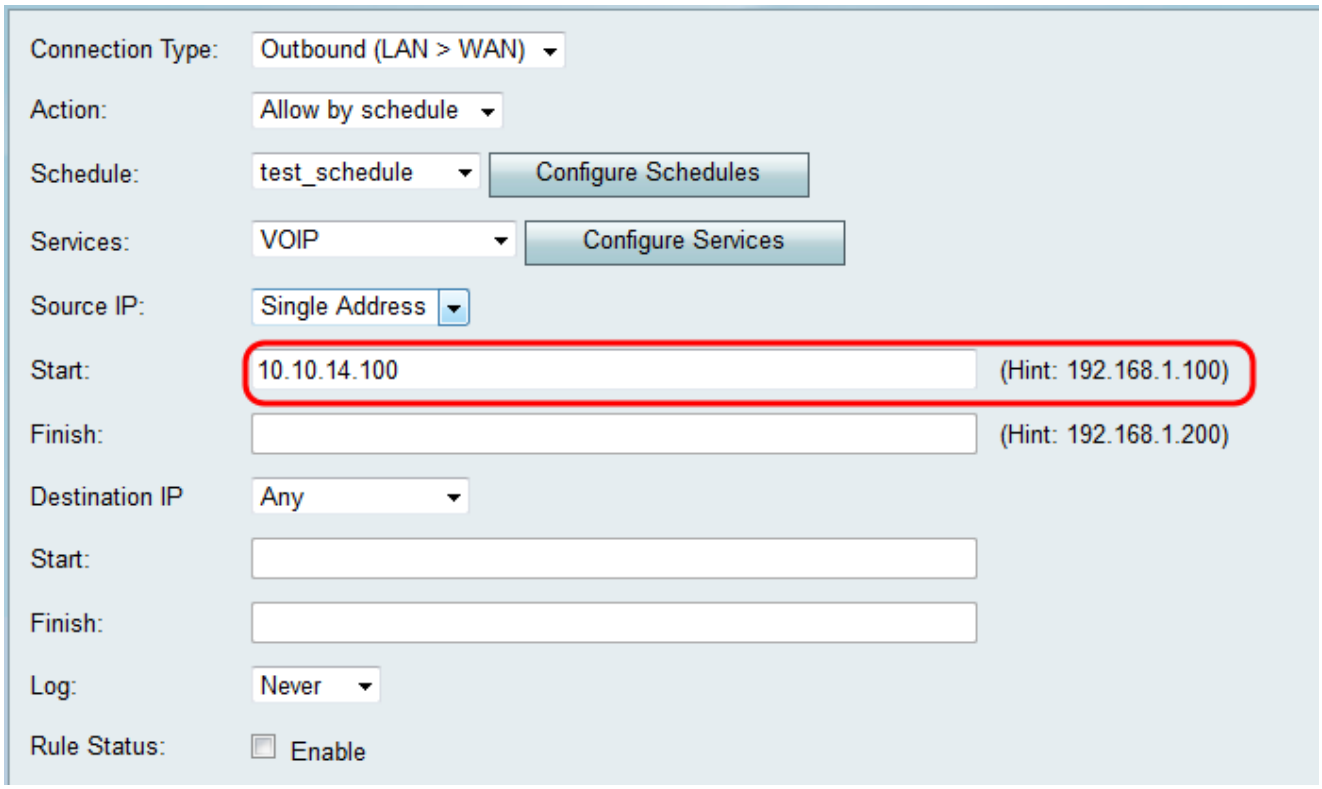
使用可能なオプションは、次のように定義されます。

・ Any：ローカルネットワーク内の任意のIPアドレスから発信されたトラフィックに適用されます。したがって、「開始」フィールドと「終了」フィールドは空白のままにします。このオプションを選択した場合は、ステップ4に進みます。

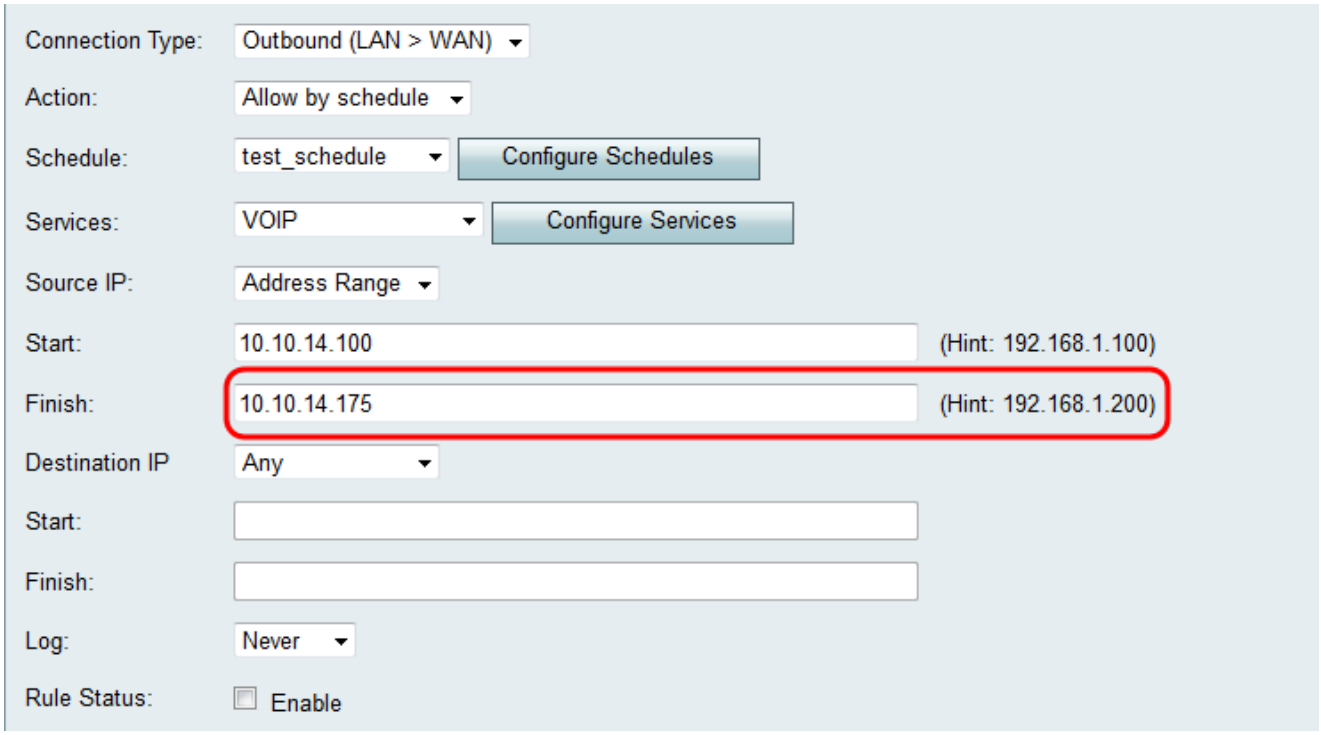
・ Single Address：ローカルネットワーク内の単一のIPアドレスから発信されたトラフィックに適用されます。StartフィールドにIPアドレスを入力します。

・アドレス範囲：ローカルネットワークのIPアドレスの範囲から発信されたトラフィックに適用されます。範囲を設定するには、範囲の開始IPアドレスをStartフィールドに入力し、終了IPアドレスをFinishフィールドに入力します。

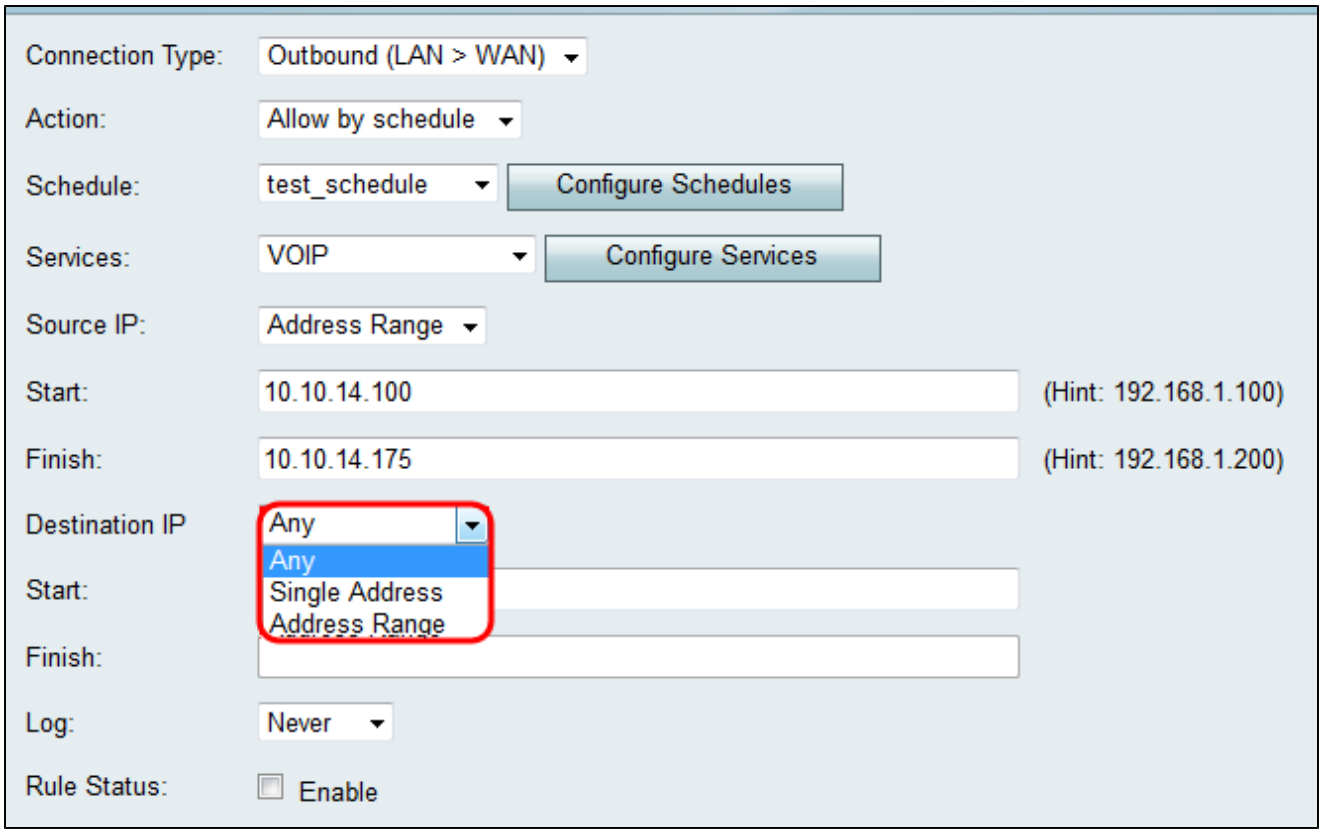
ステップ 2：ステップ1でSingle Addressを選択した場合は、アクセスルールに適用されるIPアドレスをStartフィールドに入力し、ステップ4に進みます。ステップ1でAddress Rangeを選択した場合は、アクセスルールに適用される開始IPアドレスをStartフィールドに入力します。



ステップ 3：ステップ1でAddress Rangeを選択した場合は、アクセスルールのIPアドレス範囲をカプセル化する終了IPアドレスをFinishフィールドに入力します。



ステップ 4：Destination IPドロップダウンリストから、宛先IPの定義方法を選択します。発信トラフィックの場合、宛先IPは、ローカルネットワークからのトラフィックが許可または拒否される（WAN内の）アドレスを指します。



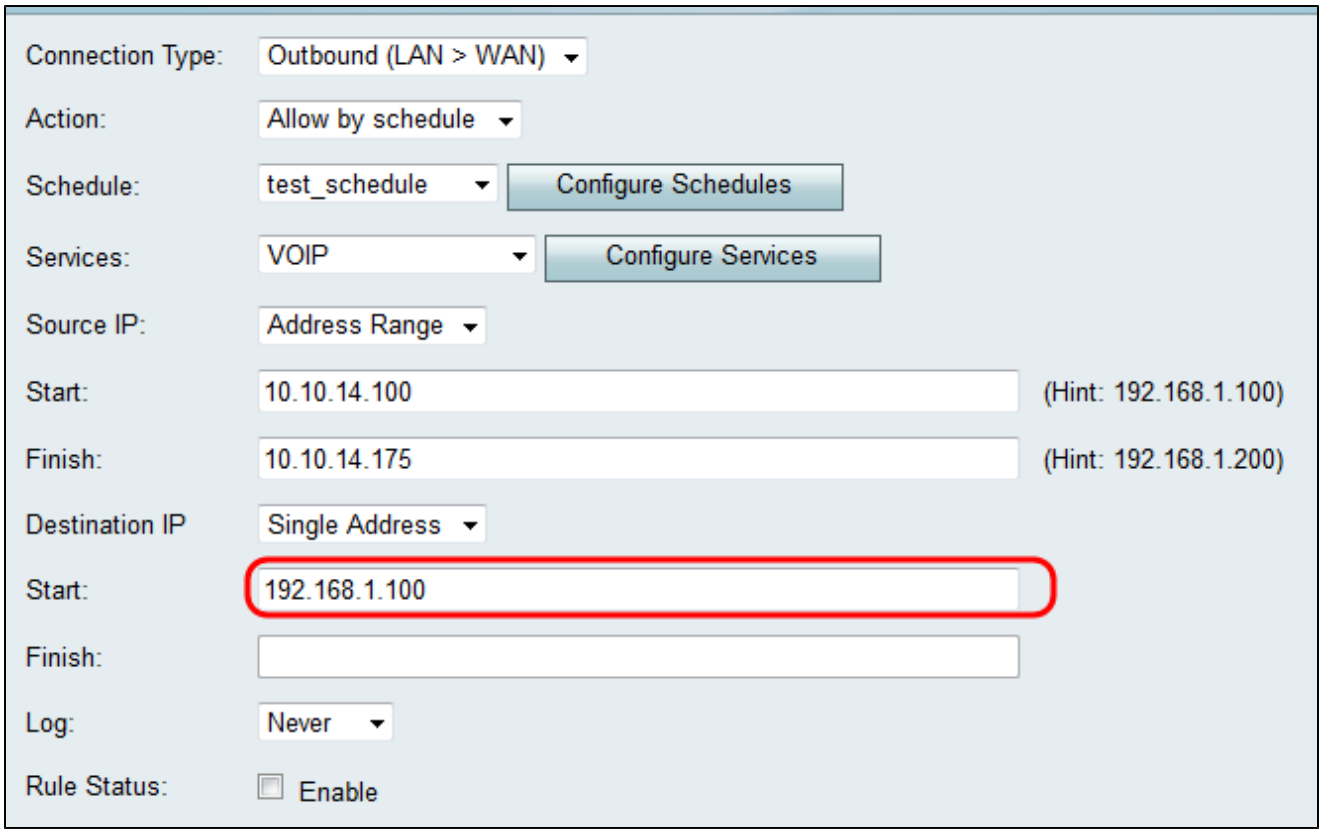
使用可能なオプションは、次のように定義されます。

・ Any：パブリックインターネット内の任意のIPアドレスに向かうトラフィックに適用されます。したがって、「開始」フィールドと「終了」フィールドは空白のままにします。

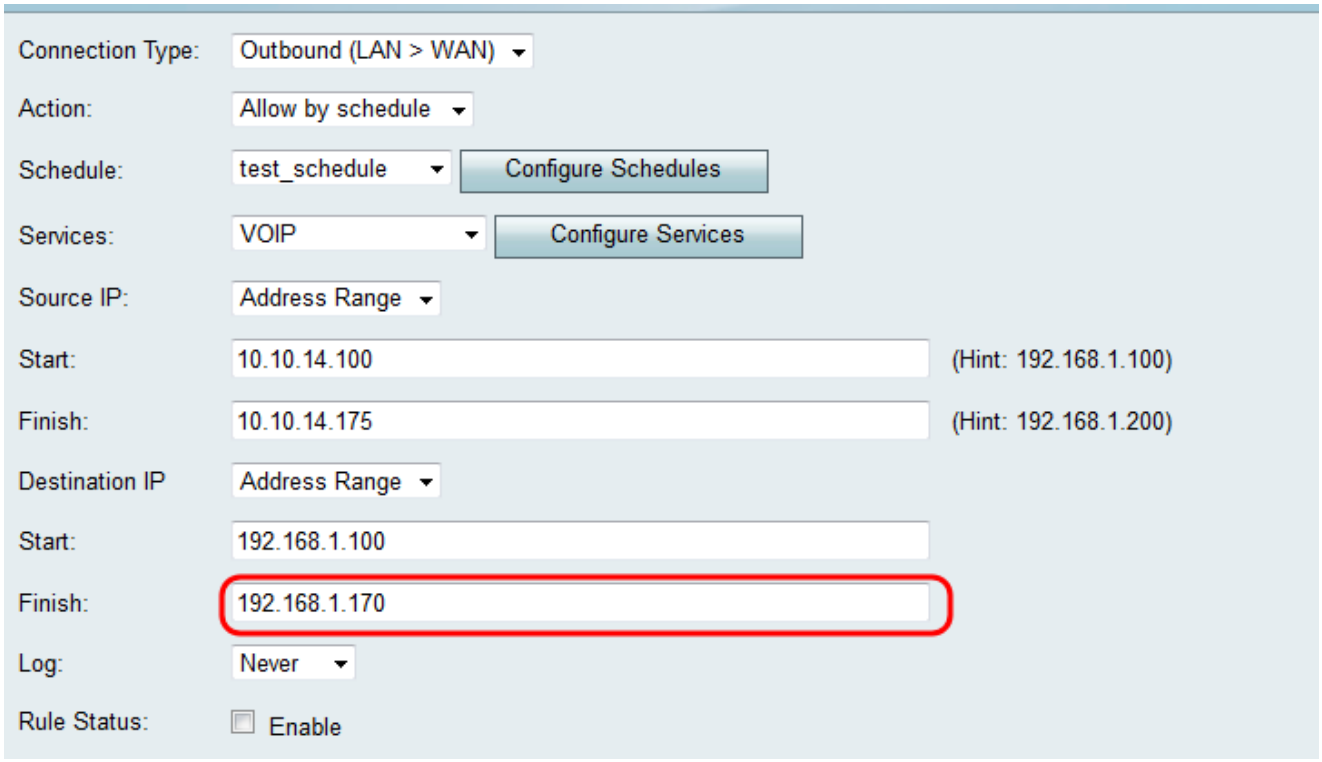
・ Single Address：パブリックインターネット内の単一のIPアドレス宛てのトラフィックに適用されます。StartフィールドにIPアドレスを入力します。

・アドレス範囲：パブリックインターネットのIPアドレスの範囲に向かうトラフィックに適用されます。範囲を設定するには、範囲の開始IPアドレスをStartフィールドに入力し、終了IPアドレスをFinishフィールドに入力します。

ステップ 5：ステップ4でSingle Addressを選択した場合は、アクセスルールに適用されるIPアドレスをStartフィールドに入力します。ステップ4でAddress Rangeを選択した場合は、アクセスルールに適用される開始IPアドレスをStartフィールドに入力します。



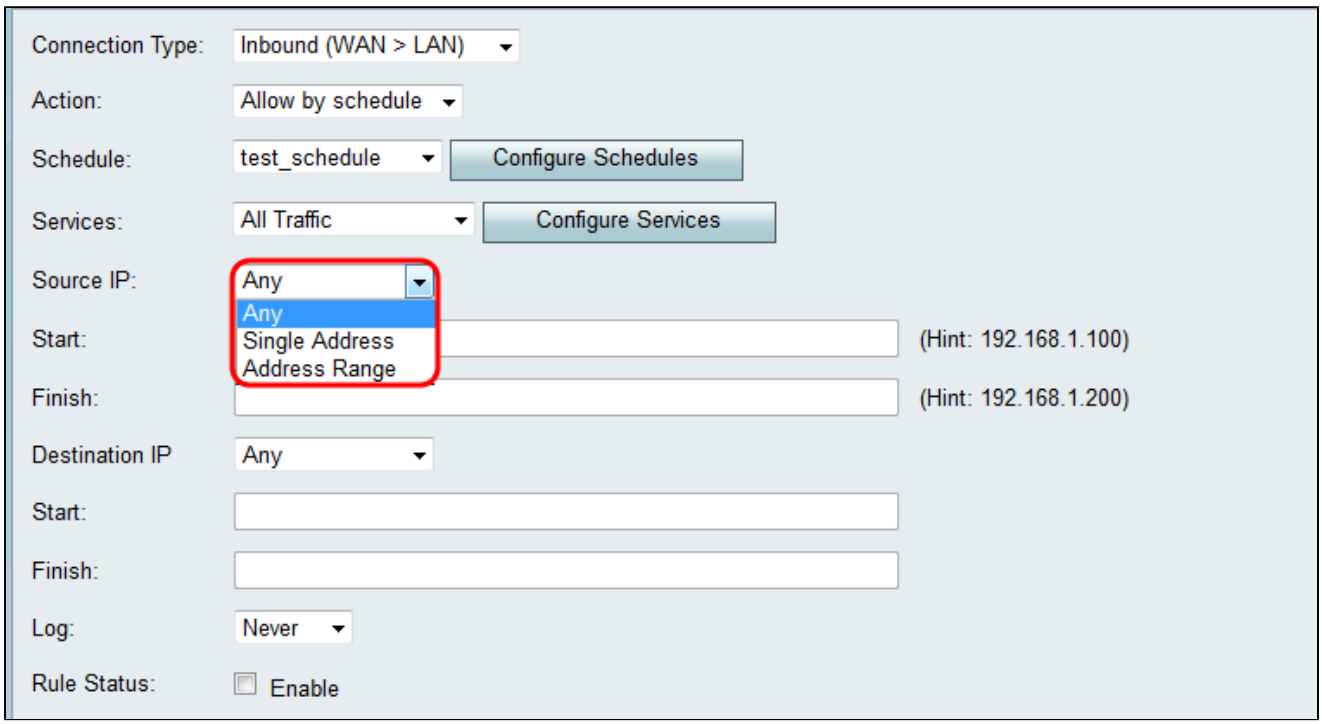
手順 6：ステップ4でAddress Rangeを選択した場合は、アクセスルールのIPアドレス範囲をカプセル化する終了IPアドレスをFinishフィールドに入力します。



着信トラフィックの送信元および宛先IPの設定

アクセスルールの追加のステップ3で着信(WAN > LAN)または着信(WAN > DMZ)を接続タイプとして選択した場合は、このセクションのステップに従います。

ステップ 1：Source IPドロップダウンリストから、送信元IPの定義方法を選択します。着信トラフィックの場合、送信元IPは、ファイアウォール規則が適用されるWAN内のアドレスを指します。



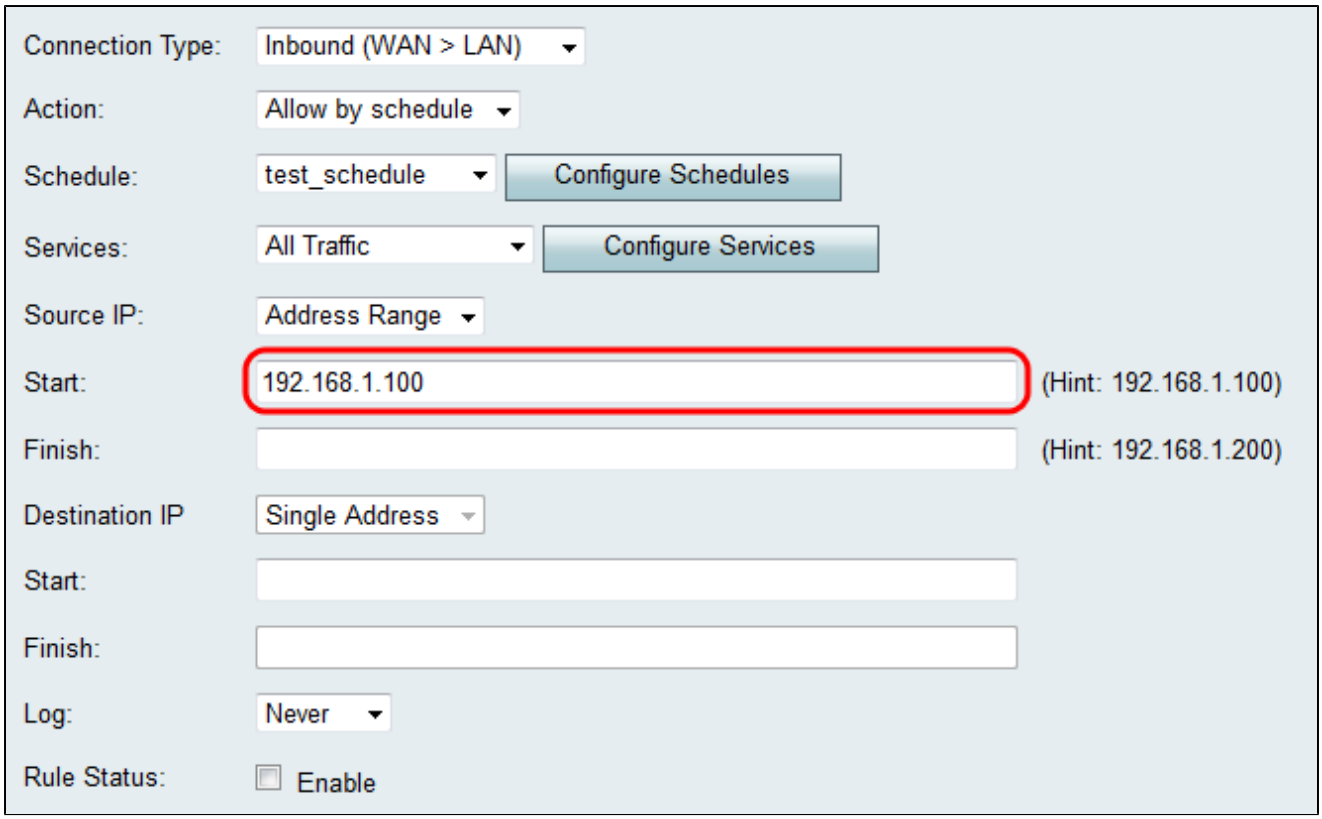
使用可能なオプションは、次のように定義されます。

・ Any：パブリックインターネットの任意のIPアドレスから発信されたトラフィックに適用されます。したがって、「開始」フィールドと「終了」フィールドは空白のままにします。このオプションを選択した場合は、ステップ4に進みます。

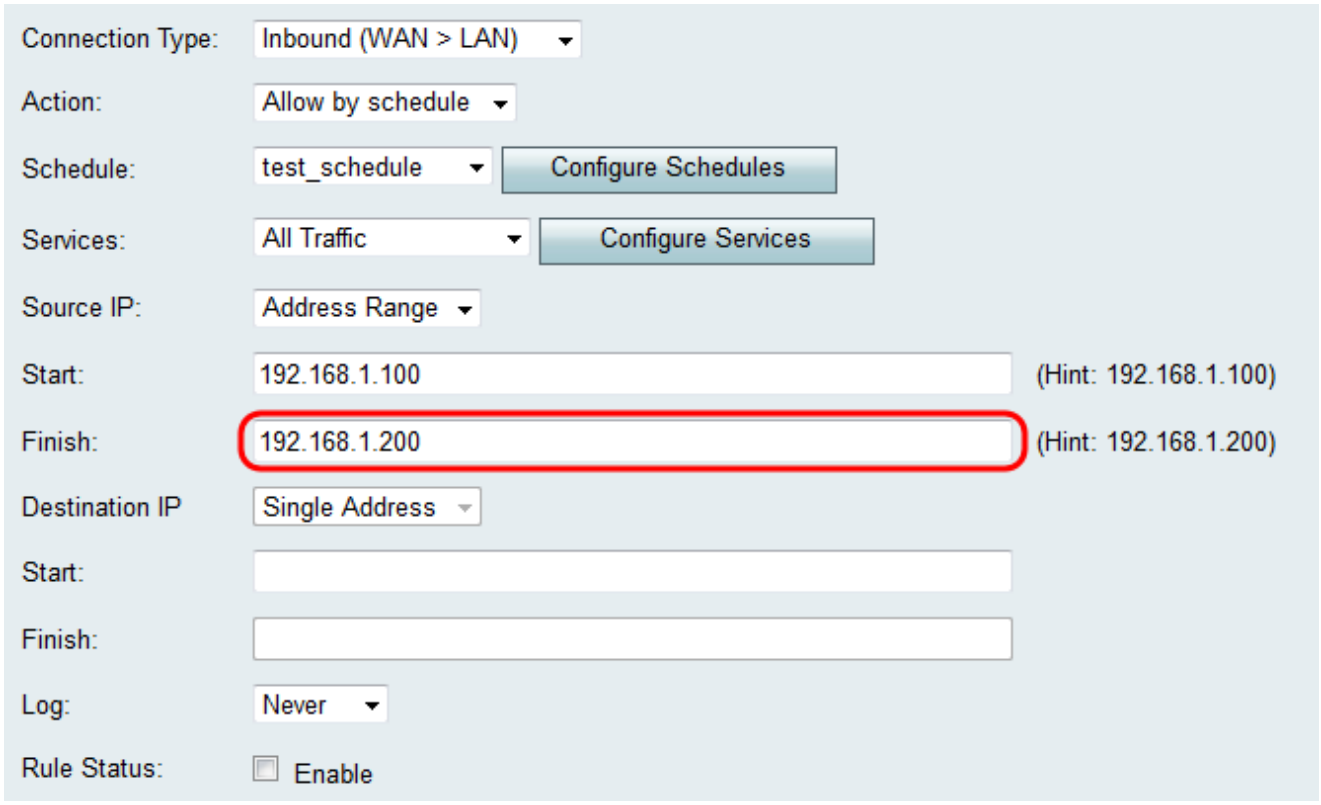
・ Single Address：パブリックインターネットの単一のIPアドレスから発信されたトラフィックに適用されます。StartフィールドにIPアドレスを入力します。

・ アドレス範囲：パブリックインターネットのIPアドレスの範囲から発信されたトラフィックに適用されます。範囲を設定するには、範囲の開始IPアドレスをStartフィールドに入力し、終了IPアドレスをFinishフィールドに入力します。

ステップ 2：ステップ1でSingle Addressを選択した場合は、アクセスルールに適用されるIPアドレスをStartフィールドに入力し、ステップ4に進みます。ステップ1でAddress Rangeを選択した場合は、アクセスルールに適用される開始IPアドレスをStartフィールドに入力します。

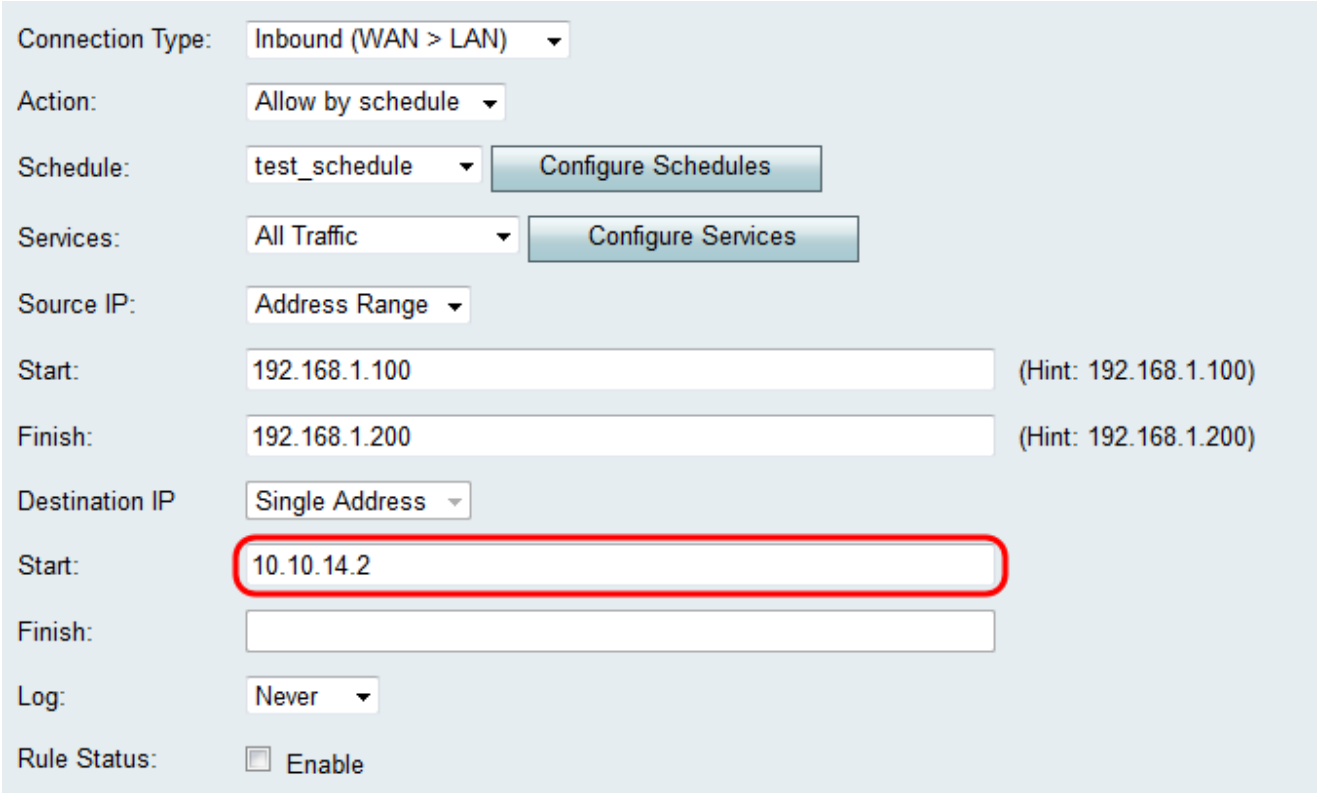


ステップ 3：ステップ1でAddress Rangeを選択した場合は、アクセスルールのIPアドレス範囲をカプセル化する終了IPアドレスをFinishフィールドに入力します。



ステップ 4：StartフィールドのDestination IPドロップダウンリストの下に、Destination IPのSingle Addressを入力します。着信トラフィックの場合、宛先IPは、パブリックインタ

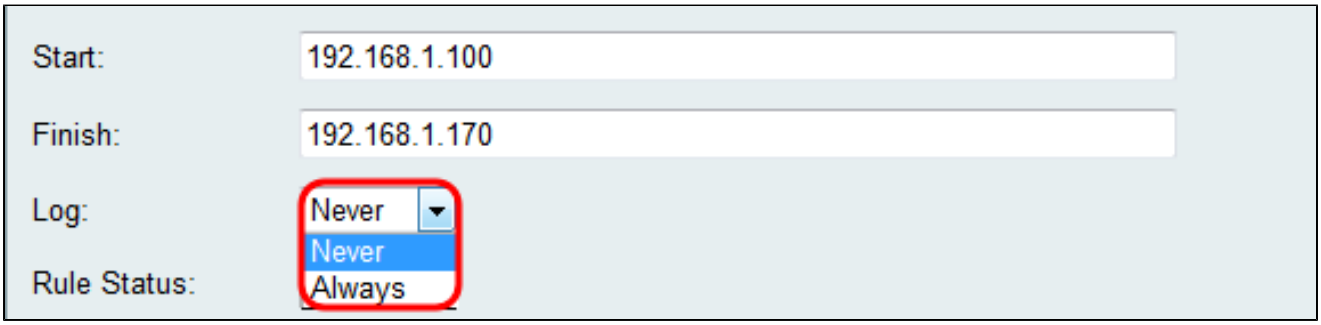
ーネットからのトラフィックが許可または拒否されるアドレス（LAN内）を指します。



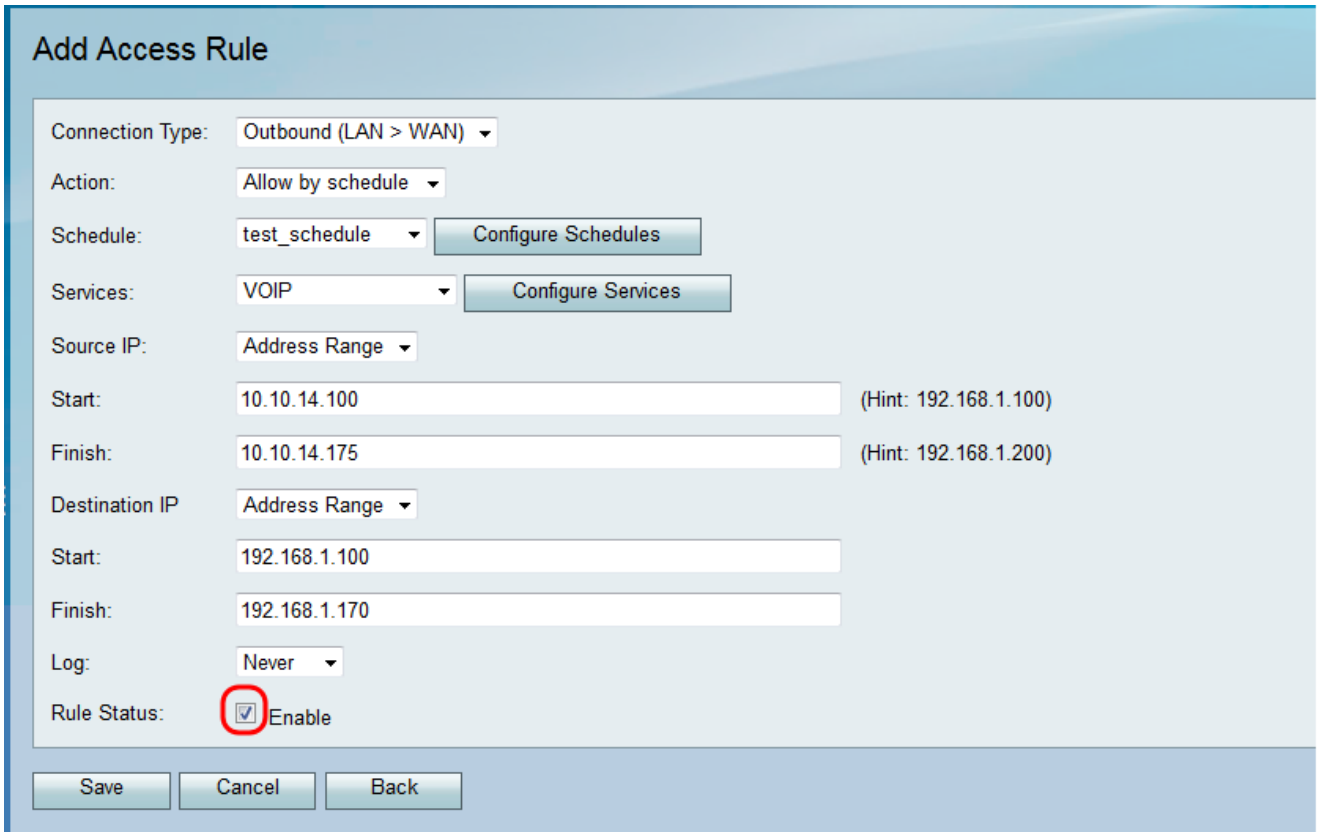
注：アクセスルールの追加のステップ3で接続タイプとしてインバウンド(WAN > DMZ)が選択されている場合、宛先IPの単一アドレスは、有効なDMZホストのIPアドレスで自動的に設定されます。

アクセスルールのロギングと有効化

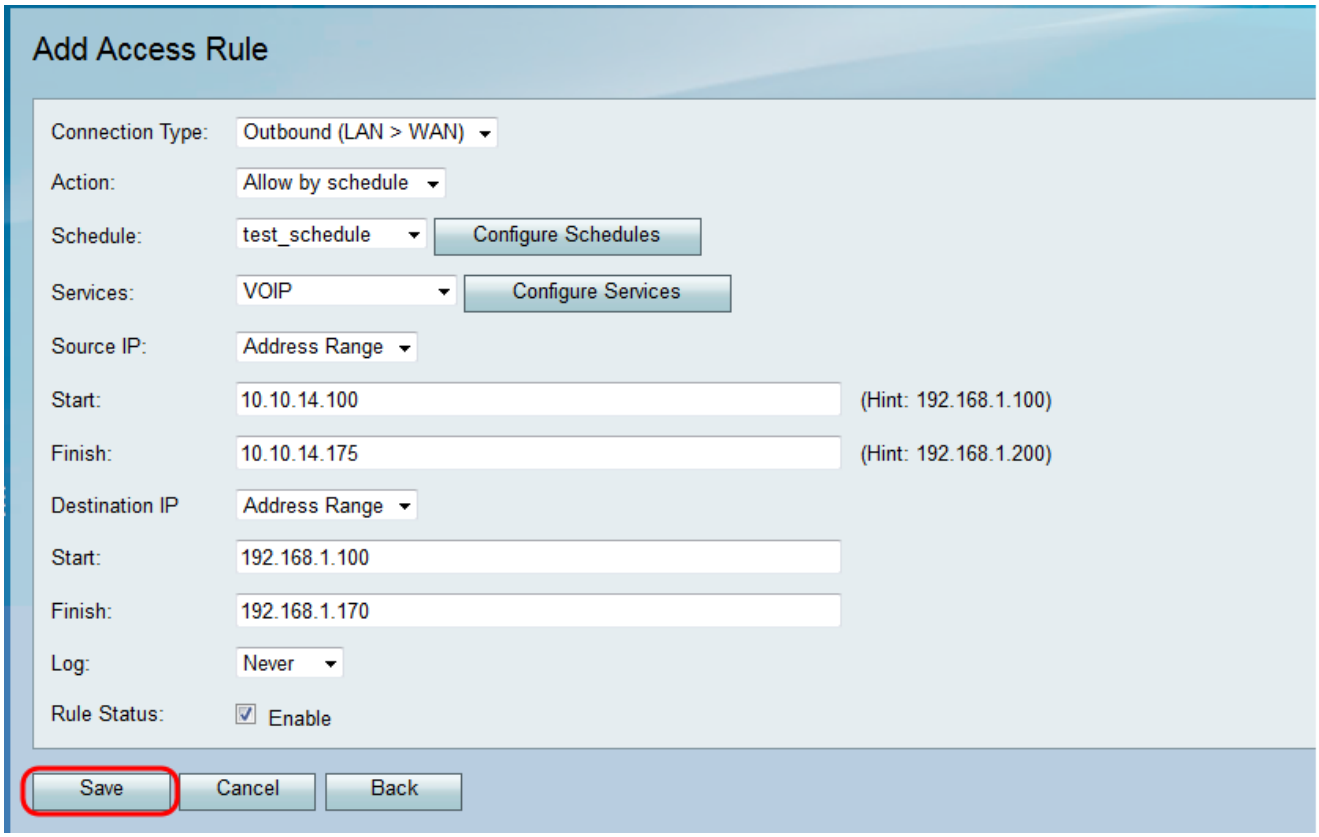
ステップ 1：パケットがルールに一致するたびにルータでログが作成されるようにするには、Logドロップダウンリストでalwaysを選択します。ルールが一致したときにロギングが行われないようにする場合は、Neverを選択します。



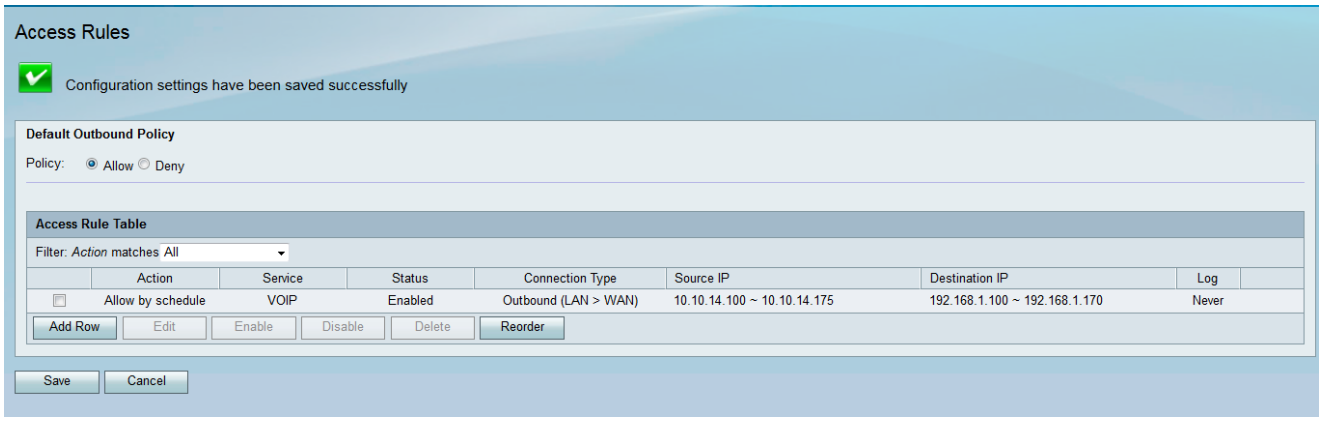
ステップ 2：アクセスルールを有効にするには、Enableチェックボックスにチェックマークを付けます。



ステップ 3：Saveをクリックして設定を保存します。



アクセスルールテーブルが、新しく設定されたアクセスルールで更新されます。


Access Rules
Configuration settings have been saved successfully
Default Outbound Policy
Policy: Allow Deny
Access Rule Table
Filter: Action matches All
Action
Service
Status
Connection Type
Source IP
Destination IP
Log
Allow by schedule
VOIP
Enabled
Outbound (LAN > WAN)
10.10.14.100 ~ 10.10.14.175
192.168.1.100 ~ 192.168.1.170
Never
Add Row
Edit
Enable
Disable
Delete
Reorder
Save
Cancel

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。