RV042、RV042G、およびRV082 VPNルータでのデュアルWAN接続の設定

目的

ワイドエリアネットワーク(WAN)は、複数のLANで構成されるネットワークです。RVルータは、両方のWANポートを同時に使用できるデュアルWAN機能をサポートしています。WAN接続は、継続的なインターネット接続を確保するためのフェールオーバー設定としても設定できます。デュアルWAN機能をさらに最適化するために、RVルータはプロトコルバインディングを使用します。プロトコルバインディングにより、特定のトラフィックを特定のWANポート経由で送信できます。

この記事では、RV042、RV042G、およびRV082 VPNルータでデュアルWANを設定する方法について説明します。

適用可能なデバイス

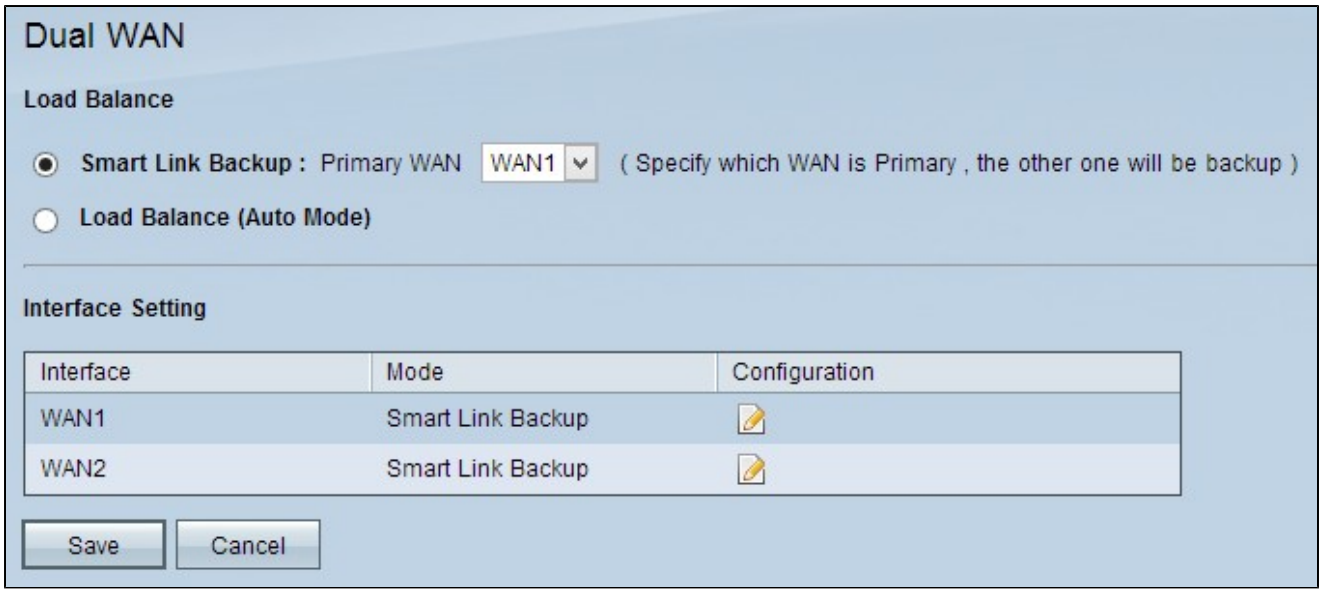
- RV042
- RV042G
- RV082

[Software Version]

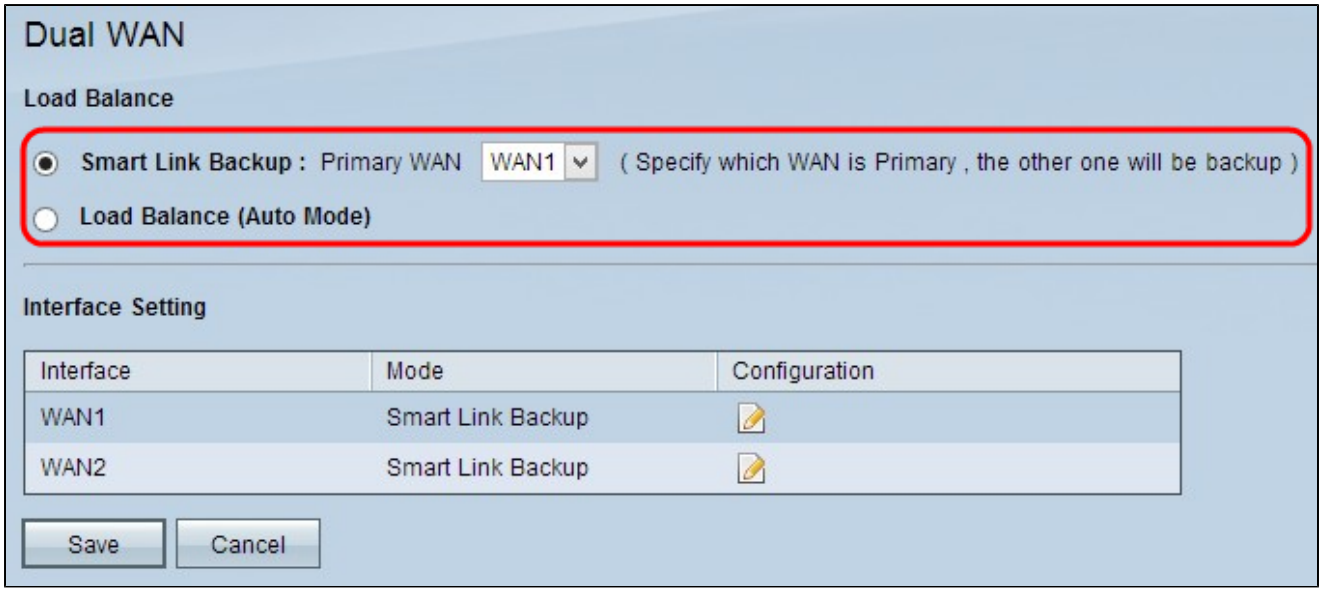
- v4.2.1.02

デュアルWANの設定

ステップ 1：Router Configuration Utilityにログインして、System Management > Dual WANの順に選択します。Dual WANページが開きます。



Load Balance



ステップ 1：適切なWANモードをクリックして、WAN接続を管理します。

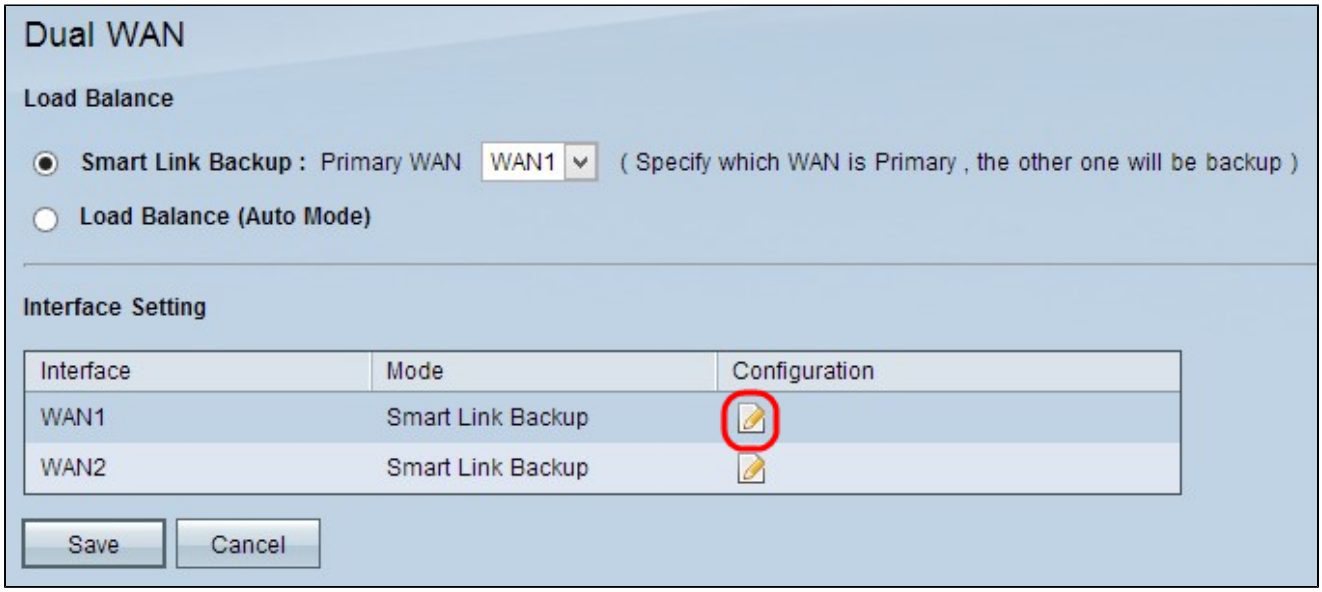
・ スマートリンクバックアップ：このオプションは、RVルータで継続的なWAN接続を確保します。プライマリWANが接続を失うと、バックアップWANが引き継ぎます。Primary WANドロップダウンリストから、プライマリWANとして指定されているWANを選択します。

・ ロードバランス：両方のWAN接続を同時に使用します。これにより、RVルータで使用可能な帯域幅が増加します。

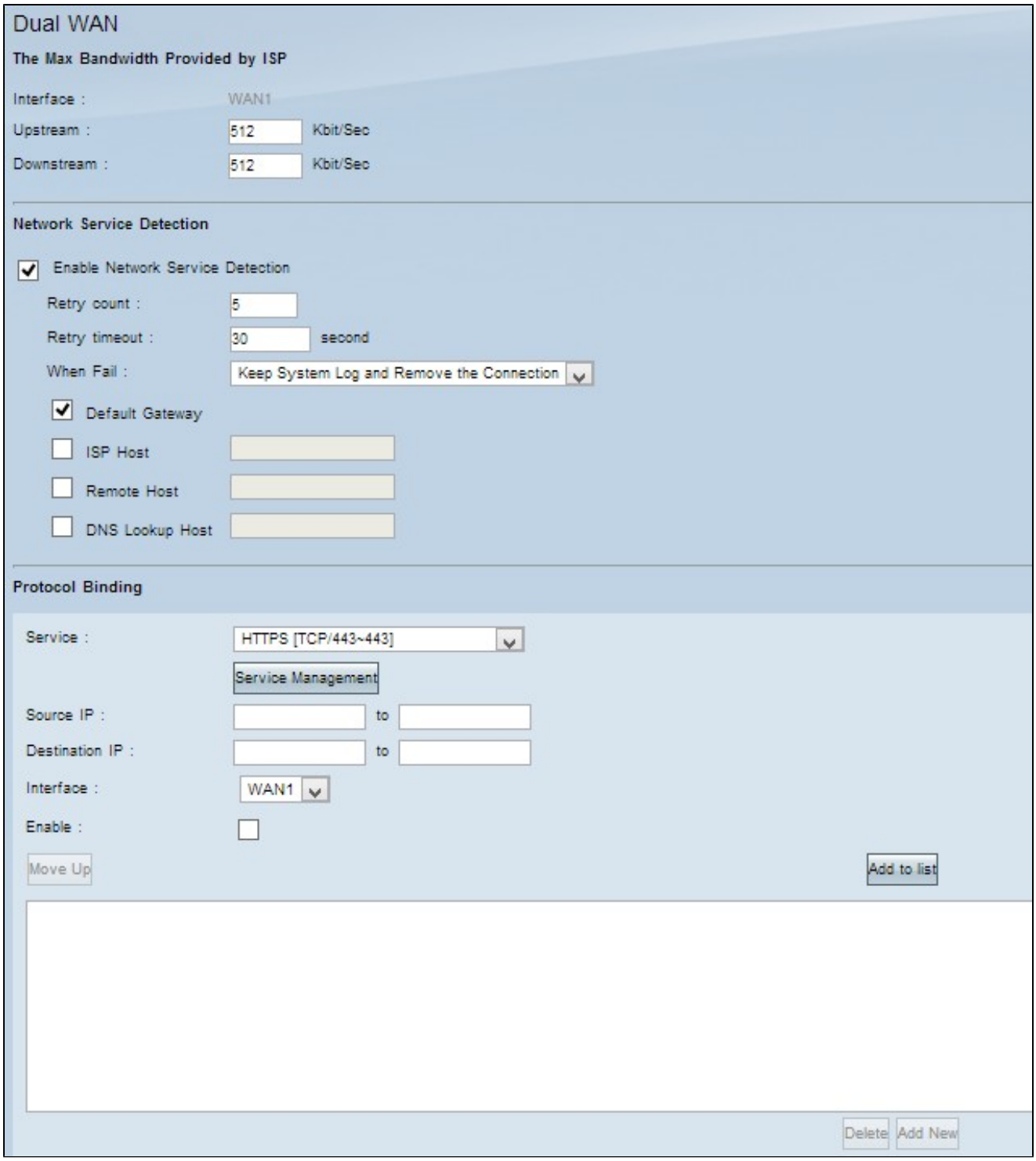
ステップ 2：[Save] をクリックして、設定を保存します。

WANの編集

注：最大帯域幅管理についての詳細は、『RV042、RV042GおよびRV016 VPNルータでのレート制御帯域幅管理』の「レート制御タイプの帯域幅」および『RV042およびRV042Gでのプライオリティ帯域幅管理』の「プライオリティタイプの帯域幅」を参照してください。



ステップ 1：Configurationボタンをクリックして、適切なWANインターフェイスを編集し、デュアルWANの設定を編集します。Dual WANページが開きます。



上記のウィンドウについては、次のサブセクションを参照してください。

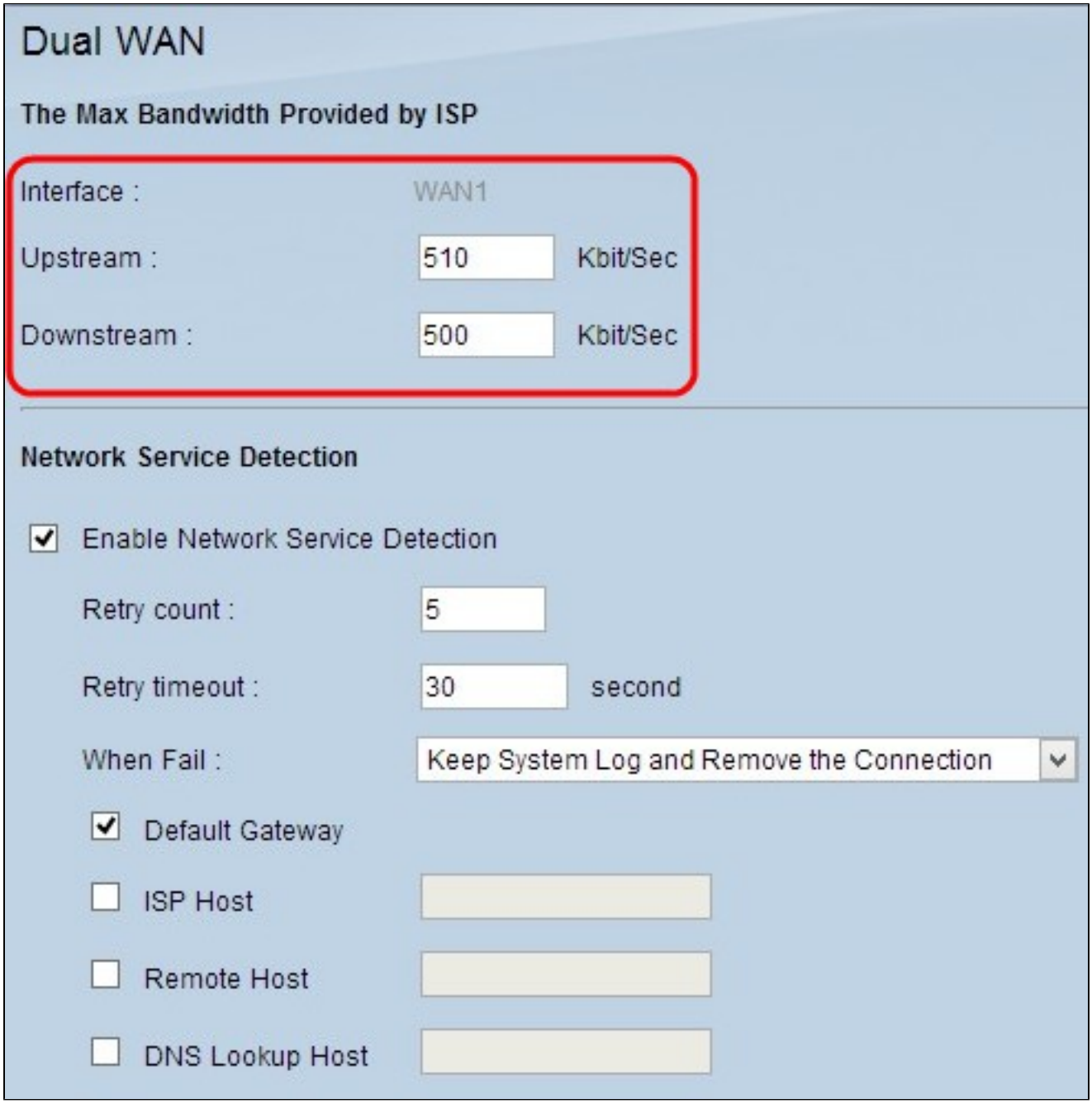
・ WAN帯域幅：指定したWANインターフェイスの帯域幅を設定する方法。

・ ネットワークサービス検出 — WAN接続を検出するためのpingテストの実行方法。

・ Manage Protocol Binding：指定されたWANインターフェイスのプロトコルバインディングを設定する方法。プロトコルバインディングにより、特定のトラフィックにどの

WANインターフェイスが使用されるかが決まります。

WAN帯域幅



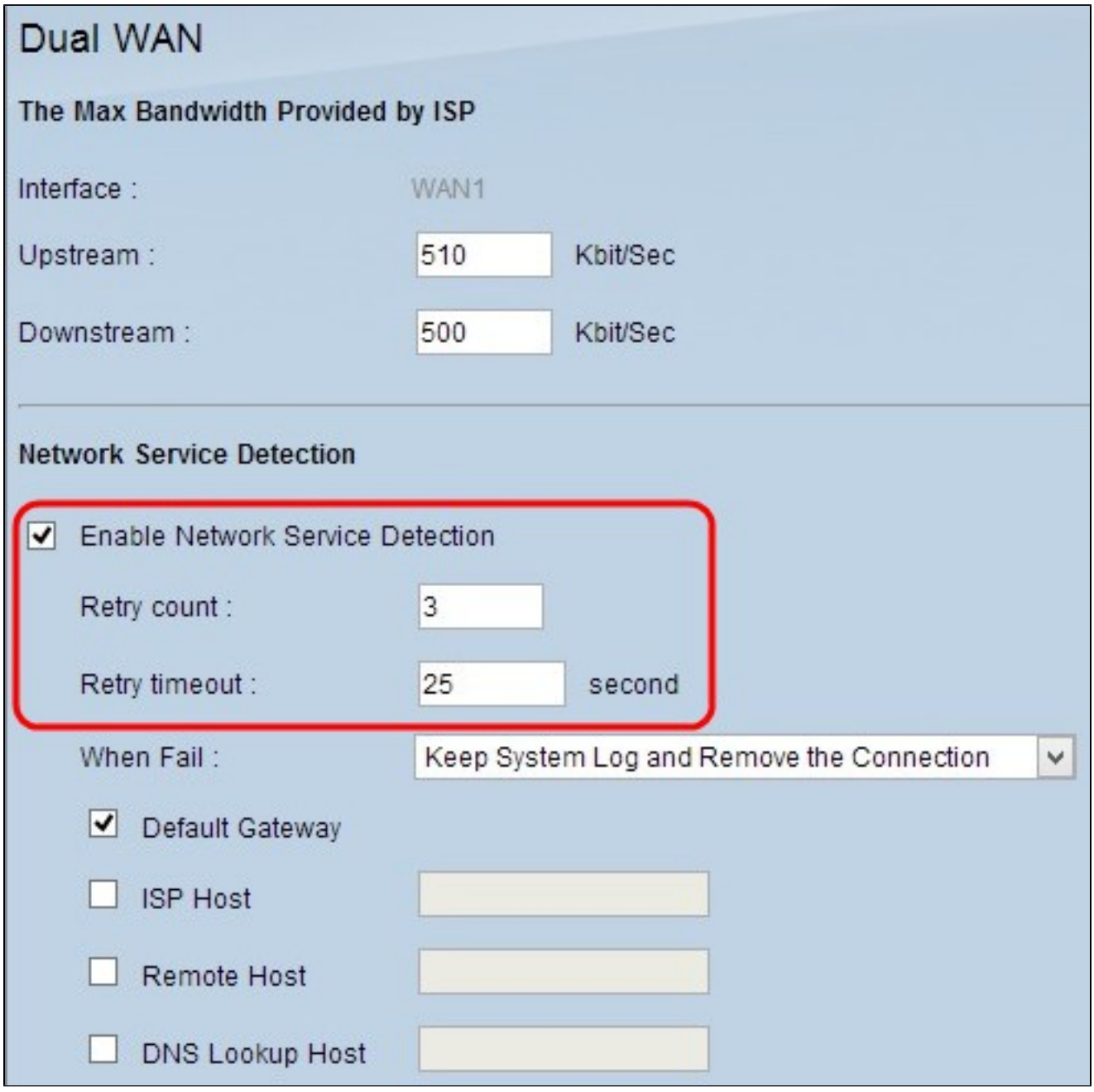
Interfaceフィールドには、指定したWANのインターフェイスが表示されます。

ステップ 1：Upstreamフィールドに、アップロードの最大帯域幅をキロビット/秒で入力します。アップストリーム帯域幅は、ネットワークがインターネットサービスプロバイダー(ISP)にデータを送信する最大帯域幅です。 デフォルトのアップストリーム帯域幅は512 kbit/秒です。

ステップ 2：Downstreamフィールドに、ダウンロードの最大帯域幅をキロビット/秒で入力します。ダウンストリーム帯域幅は、インターネットサービスプロバイダー(ISP)がネットワークにデータを送信する際の最大帯域幅です。デフォルトのダウンストリーム帯域幅は512 kbit/秒です。

ステップ 3：[Save] をクリックして、設定を保存します。

ネットワークサービスの検出

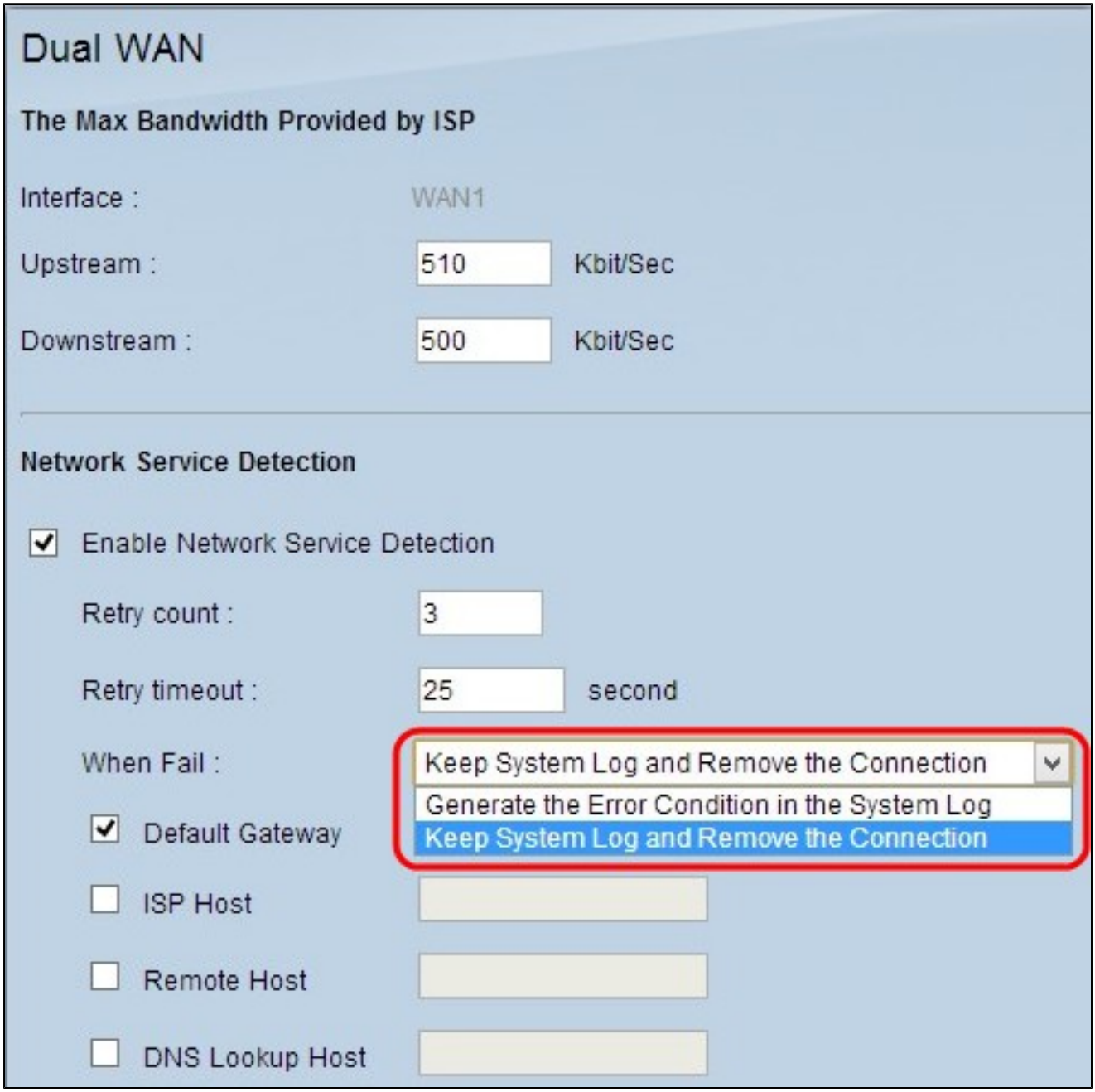


ステップ 1：RVルータが接続を検出できるようにするには、Enable Network Service Detectionにチェックマークを付けます。これは、設定されたIPアドレスへのpingテストによ

って実行されます。

ステップ 2：Retry Countフィールドに、RVルータが設定されたIPアドレスにpingを試行する回数を入力します。デフォルト値は 5 です。

ステップ 3：Retry Timeoutフィールドに、RVルータがpingの間に待機する時間（秒）を入力します。デフォルト時間は30秒です。

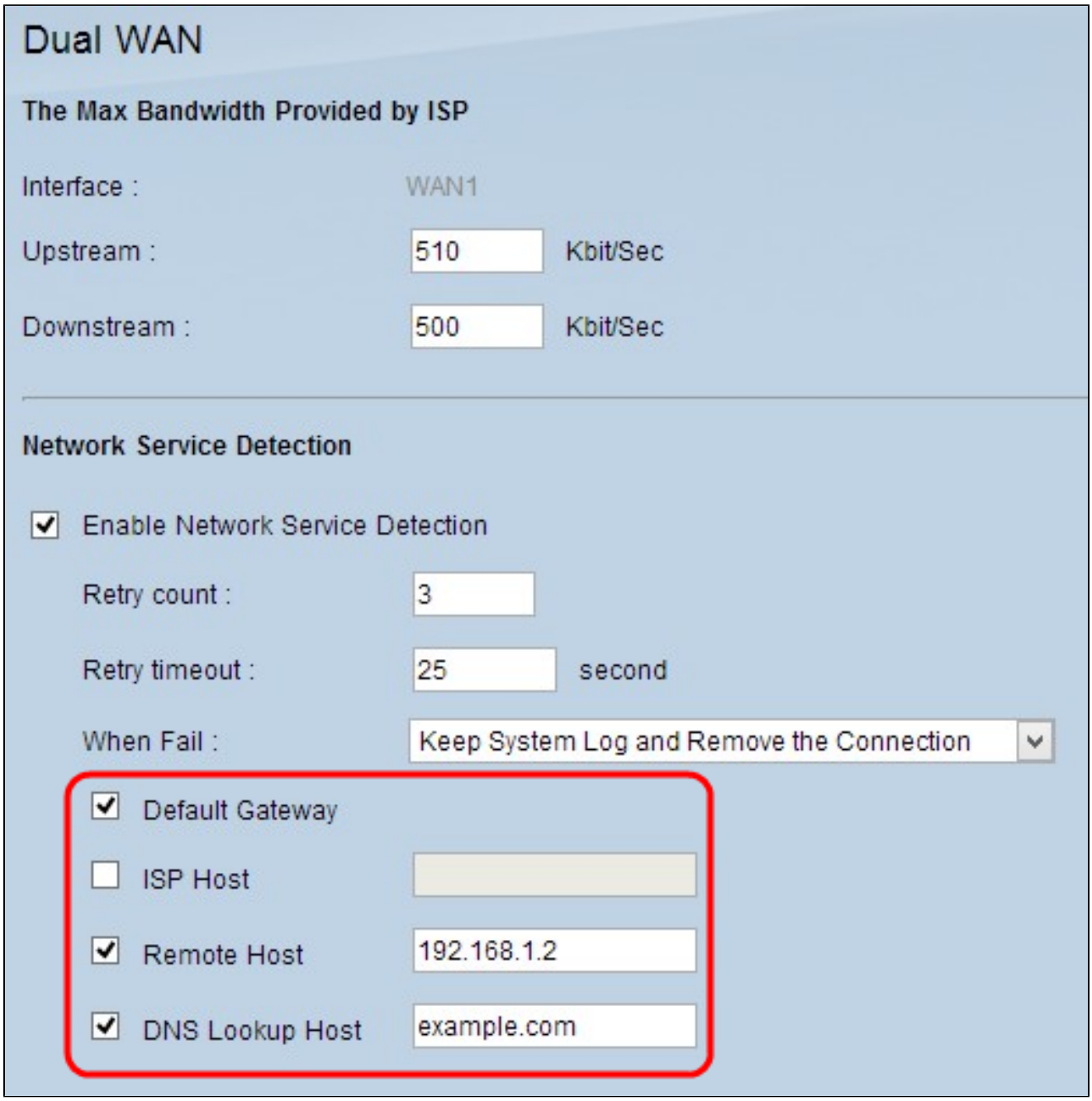


ステップ 4：When Failドロップダウンリストから、pingテストが失敗したときに実行するアクションを選択します。

・ システムログの保持と接続の削除：フェールオーバーが発生し、バックアップWANイン

ターフェイスが制御を行います。プライマリWANへの接続が回復すると、プライマリWANが制御を再開します。

・システムログでエラー状態を生成：障害がシステムログに記録され、フェールオーバーは発生しません。



ステップ 5：pingテストのためにpingを実行する場所のチェックボックスをオンにします。

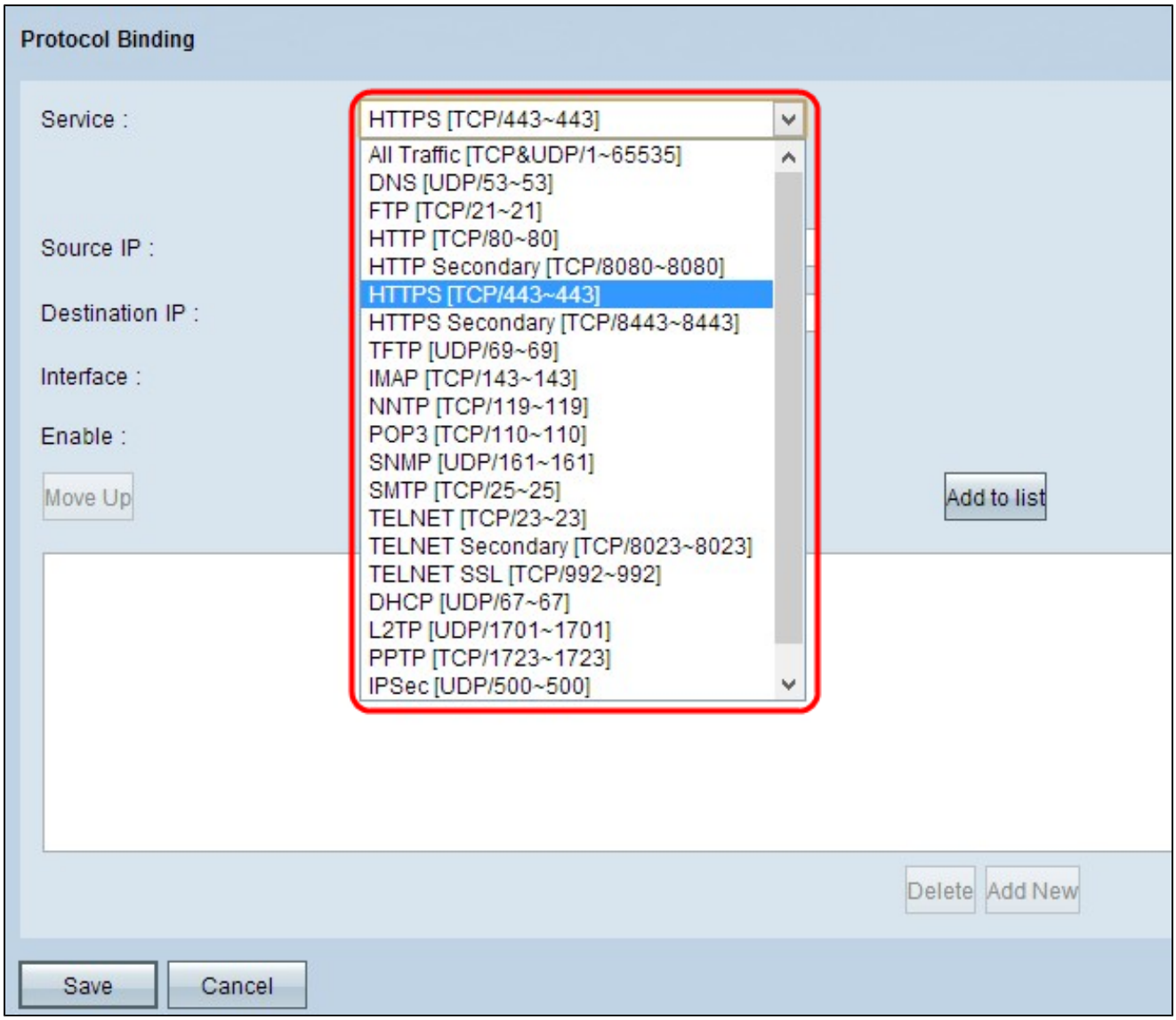
・デフォルトゲートウェイ：RV320は設定されたデフォルトゲートウェイに対してpingを実行します。

- ISP Host:RVルータがpingを実行するISPホストのIPを入力します。
- Remote Host — RVルータがpingを実行するリモートホストのIPを入力します。
- DNS Lookup Host:pingを実行するルータのホスト名またはドメイン名を入力します。

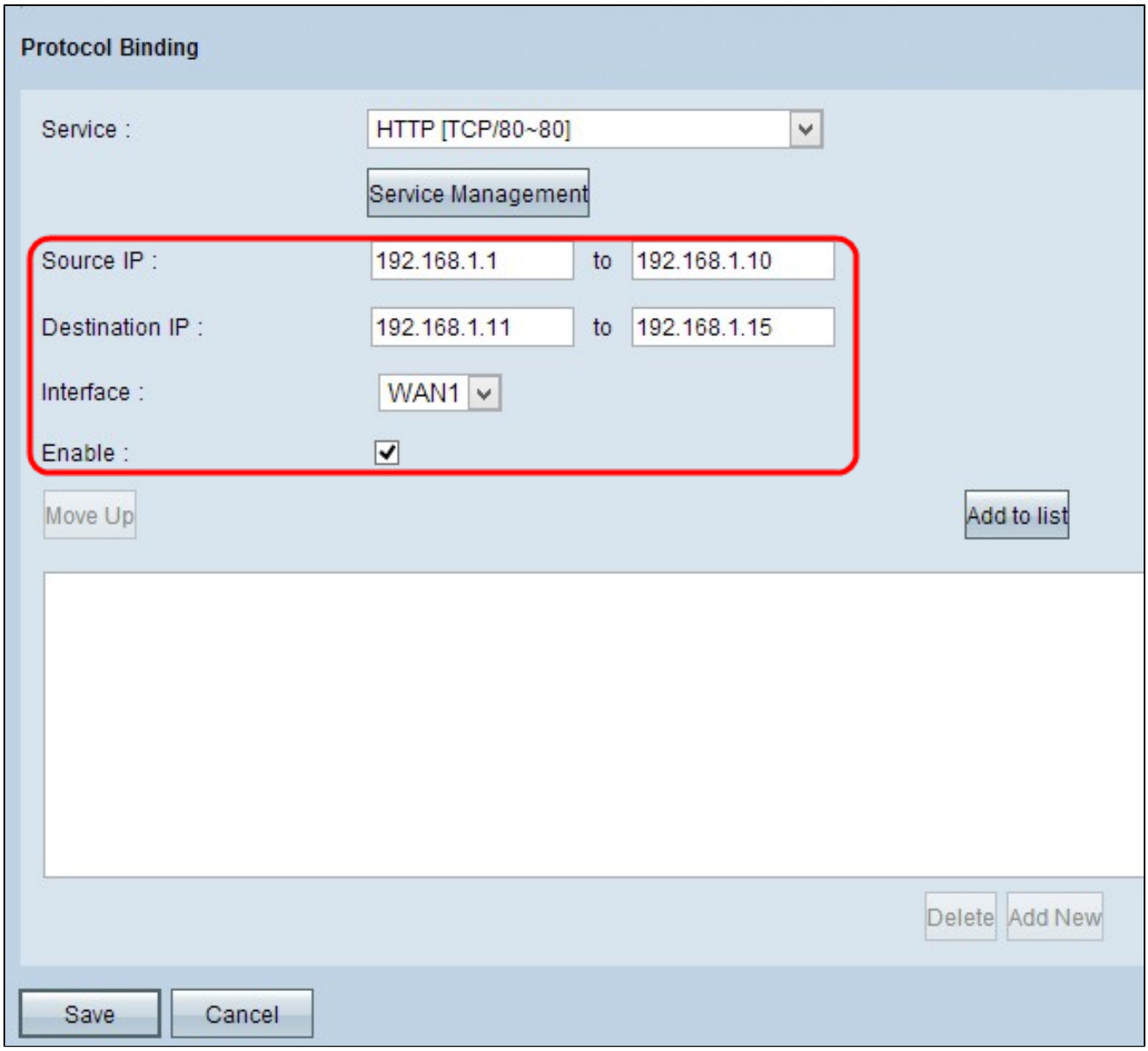
手順 6：[Save] をクリックします。

プロトコルバインドの管理

プロトコルバインディングは、特定のWANインターフェイスを介して特定のトラフィックを送信するために使用される機能です。トラフィックのタイプに一致し、設定済みの送信元IPアドレスから設定済みの宛先アドレスに送信されるトラフィックは、プロトコルバインディングルールの設定済みWANインターフェイスを介して送信されます。プロトコルバインディングは、デュアルWANモードがロードバランスとして設定されている場合にのみ使用できます。



ステップ 1：Serviceドロップダウンリストから、プロトコルバインディングに適用するトラフィックのタイプを選択します。



ステップ 2：Source IPフィールドに、プロトコルバインディングに適用する送信元IPアドレスを入力します。

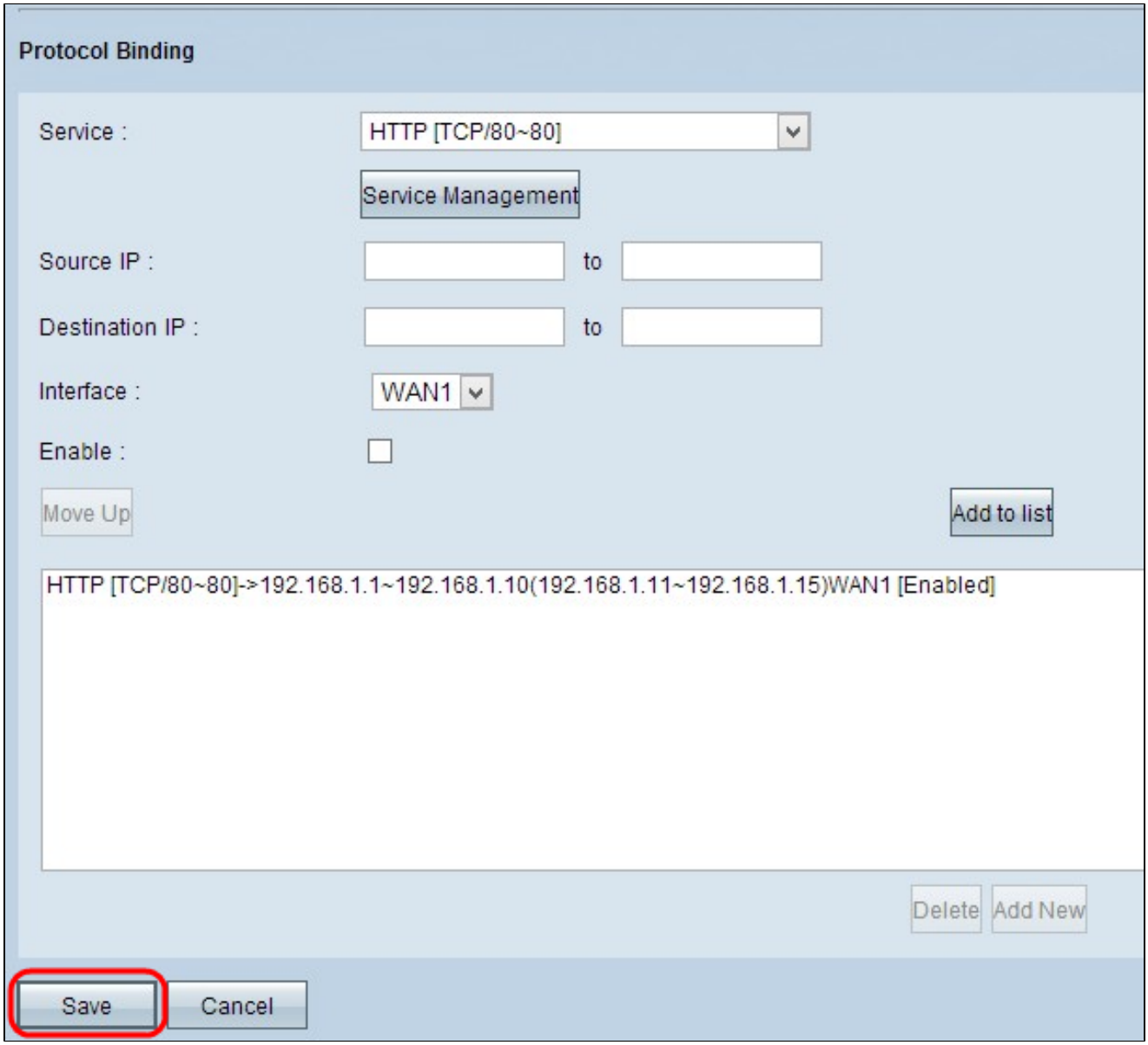
ステップ 3：Destination IPフィールドに、プロトコルバインディングに適用する宛先IPアドレスを入力します。

ステップ 4：Interfaceドロップダウンリストから、トラフィックが通過するインターフェイスを選択します。

ステップ 5：Enableフィールドのチェックボックスをオンにして、プロトコルバインディングを有効にします。

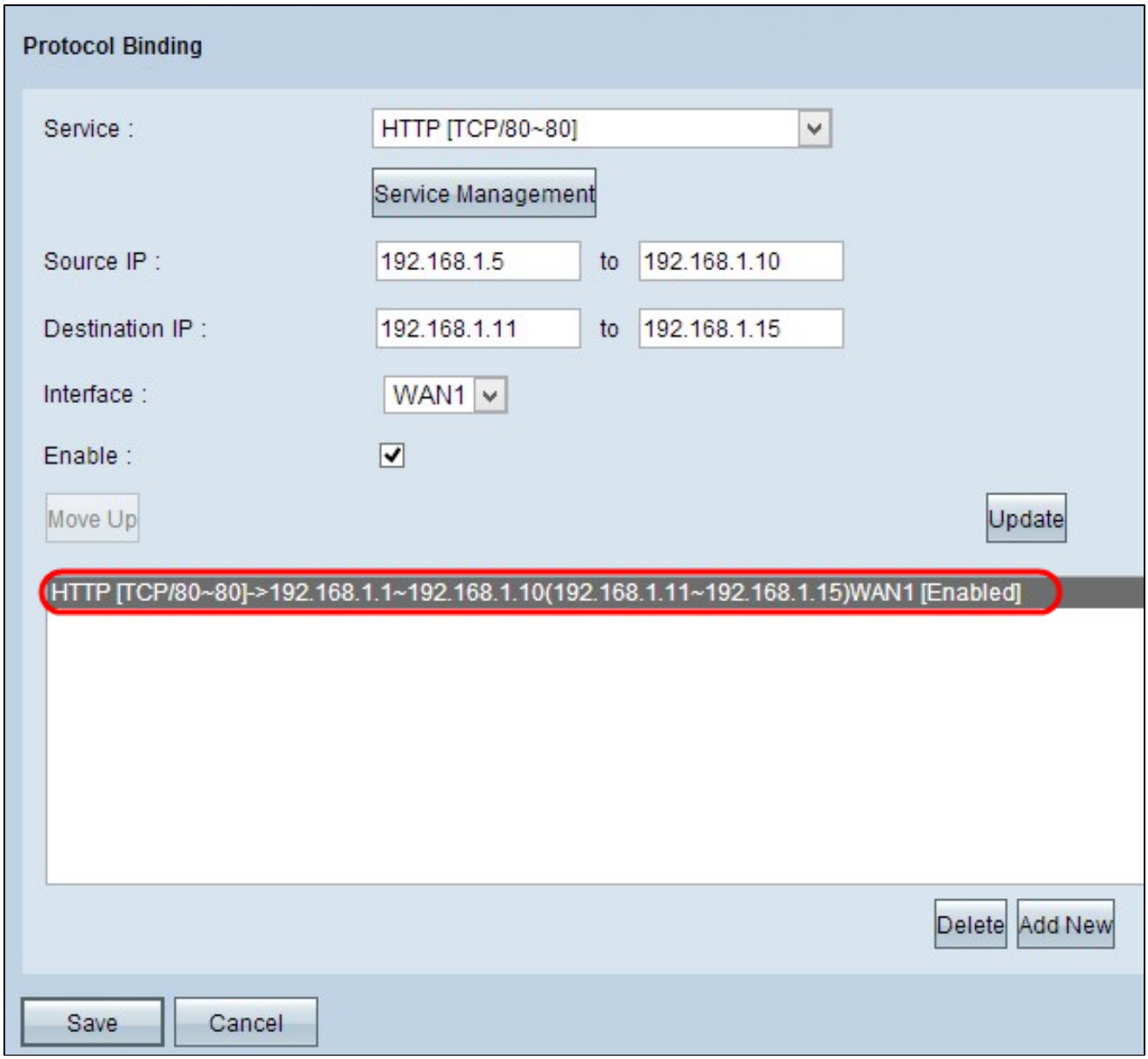
注：サービスを追加するには、Service Managementをクリックします。サービスの追加方法の詳細については、「サービス管理」のセクションを参照してください。

手順 6：Add to Listをクリックして、テーブルに追加します。



手順 7：[Save] をクリックします。プロトコルバインディングの設定が行われます。

プロトコルバインディングの編集

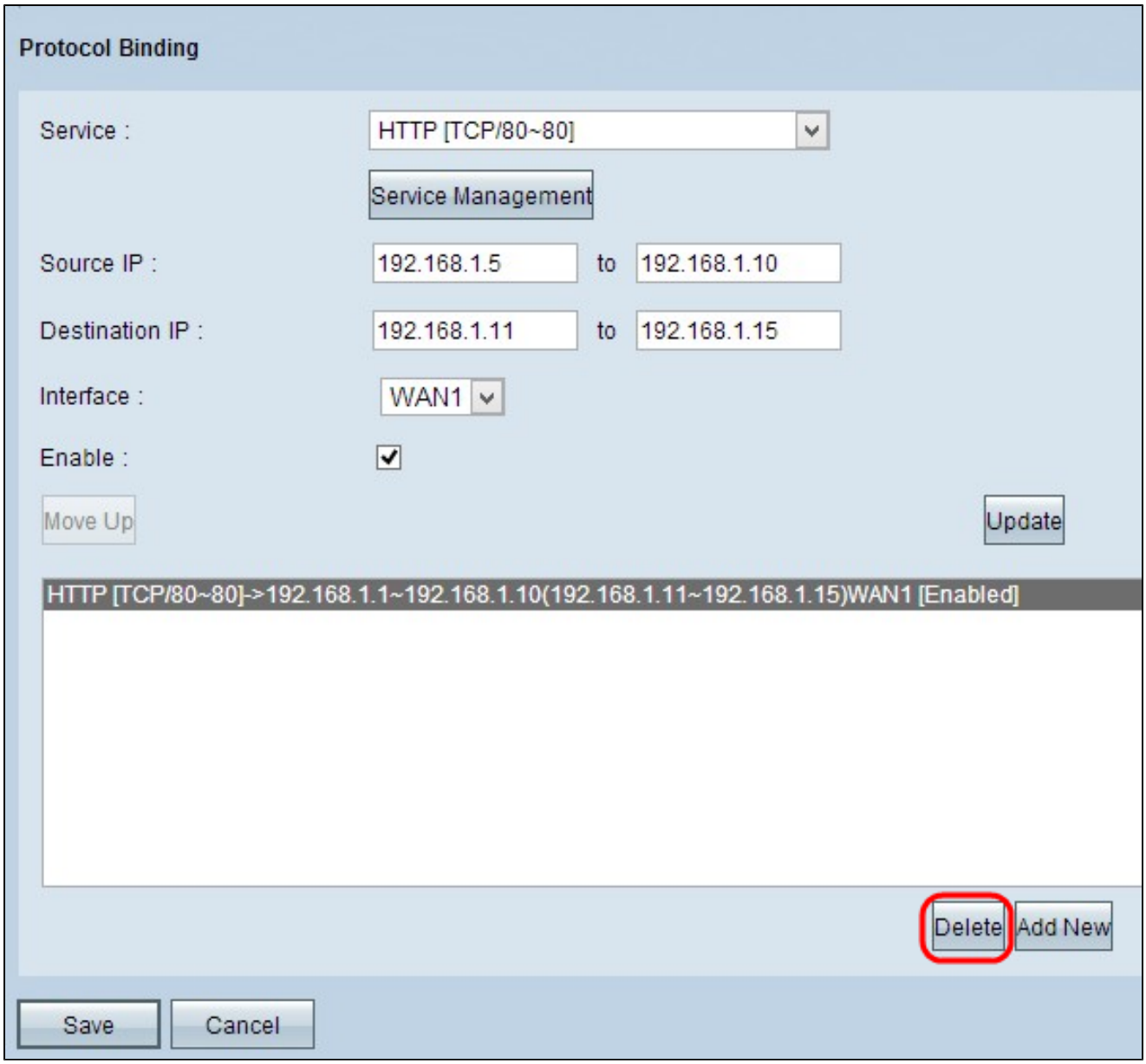


ステップ 1：編集するプロトコルバインディングをテーブルからクリックし、必要な情報を変更します。アップデート方法の詳細については、「プロトコルバインディングの追加」セクションを参照してください。

ステップ 2：Updateをクリックして、プロトコルバインディングを編集します。

ステップ 3：[Save] をクリックします。プロトコルバインディングの設定が更新されます。

プロトコルバインディングの削除

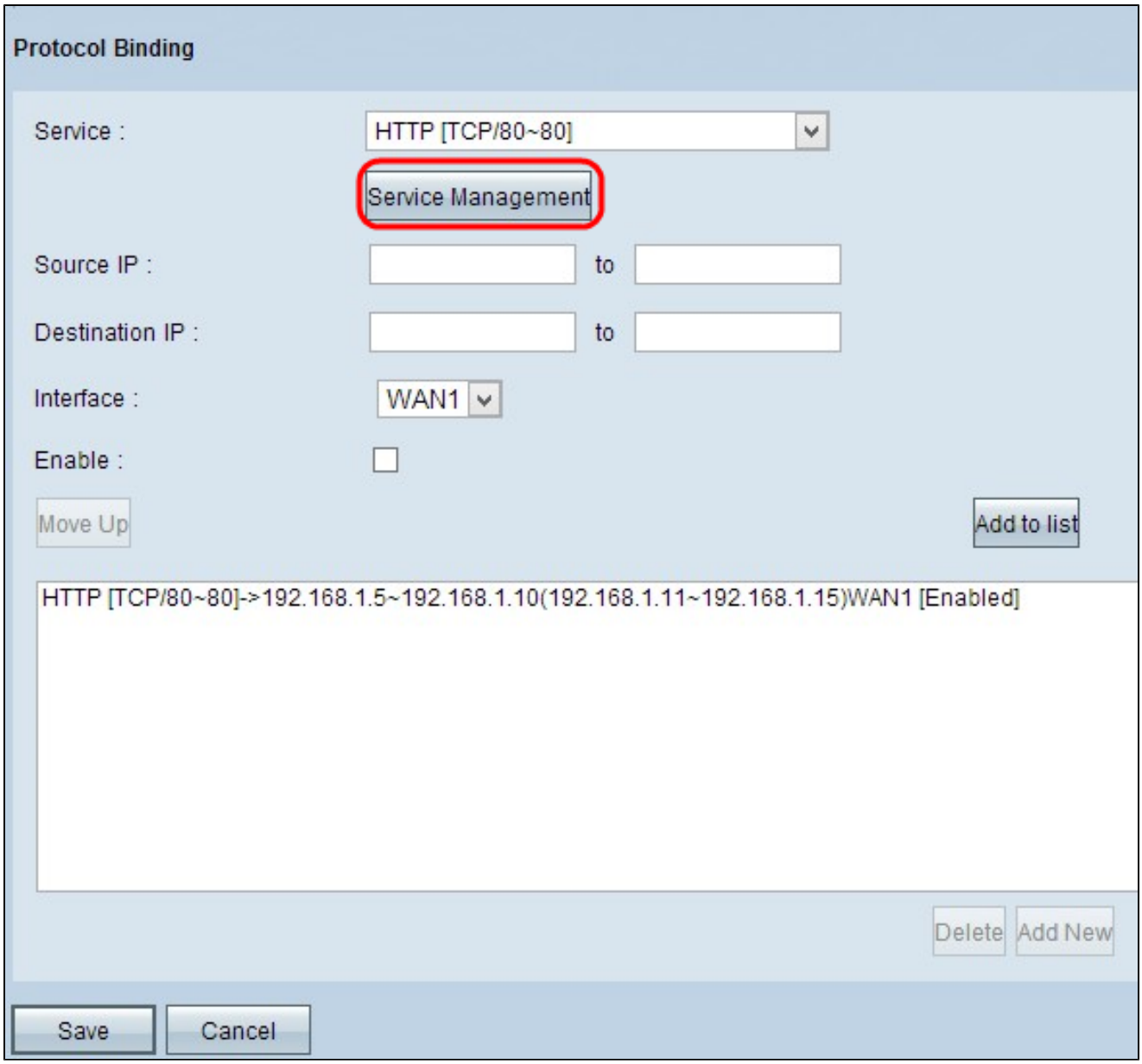


ステップ 1：テーブルから削除するプロトコルバインディングをクリックします。

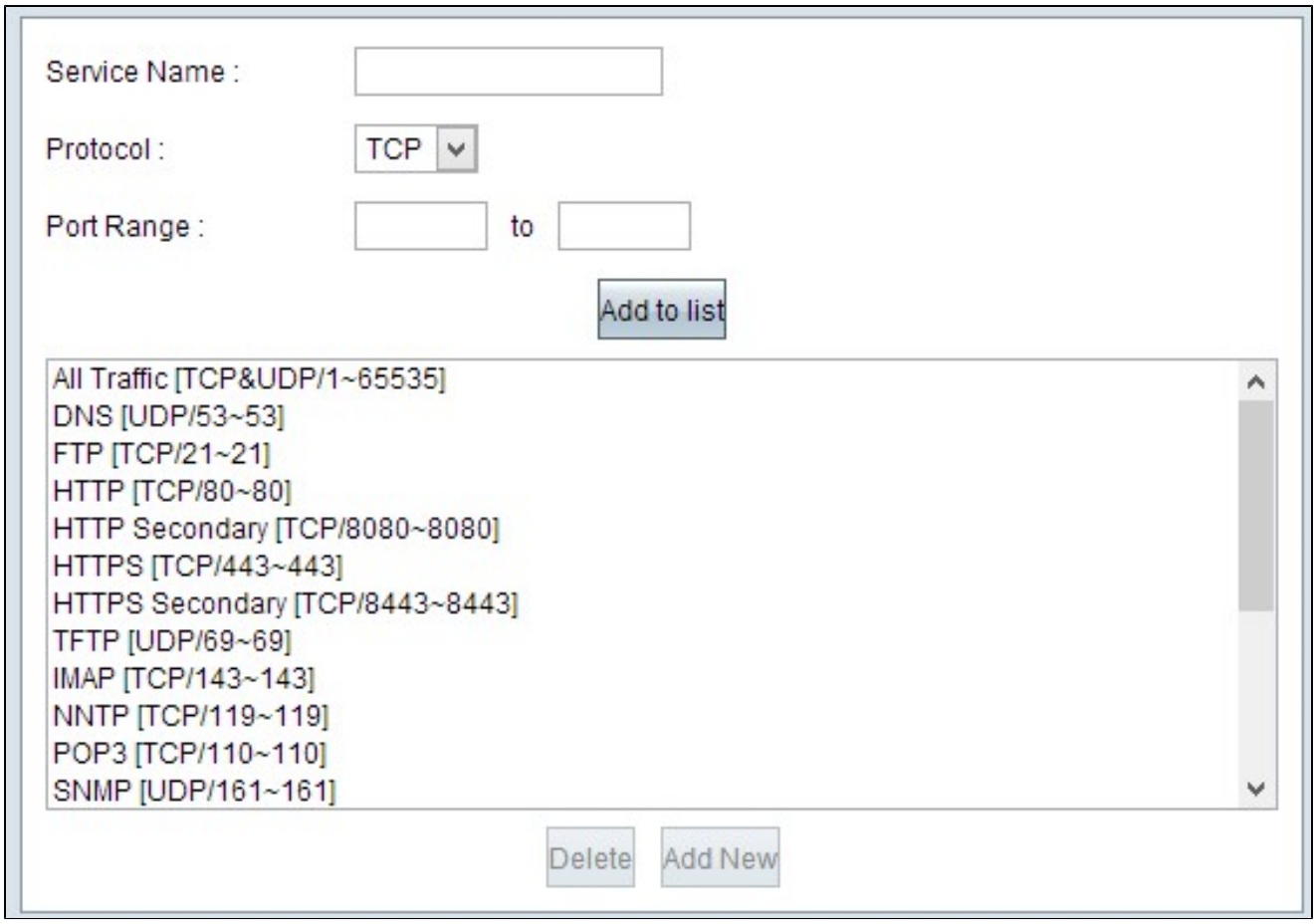
ステップ 2：Protocol Binding TableでDeleteをクリックします。

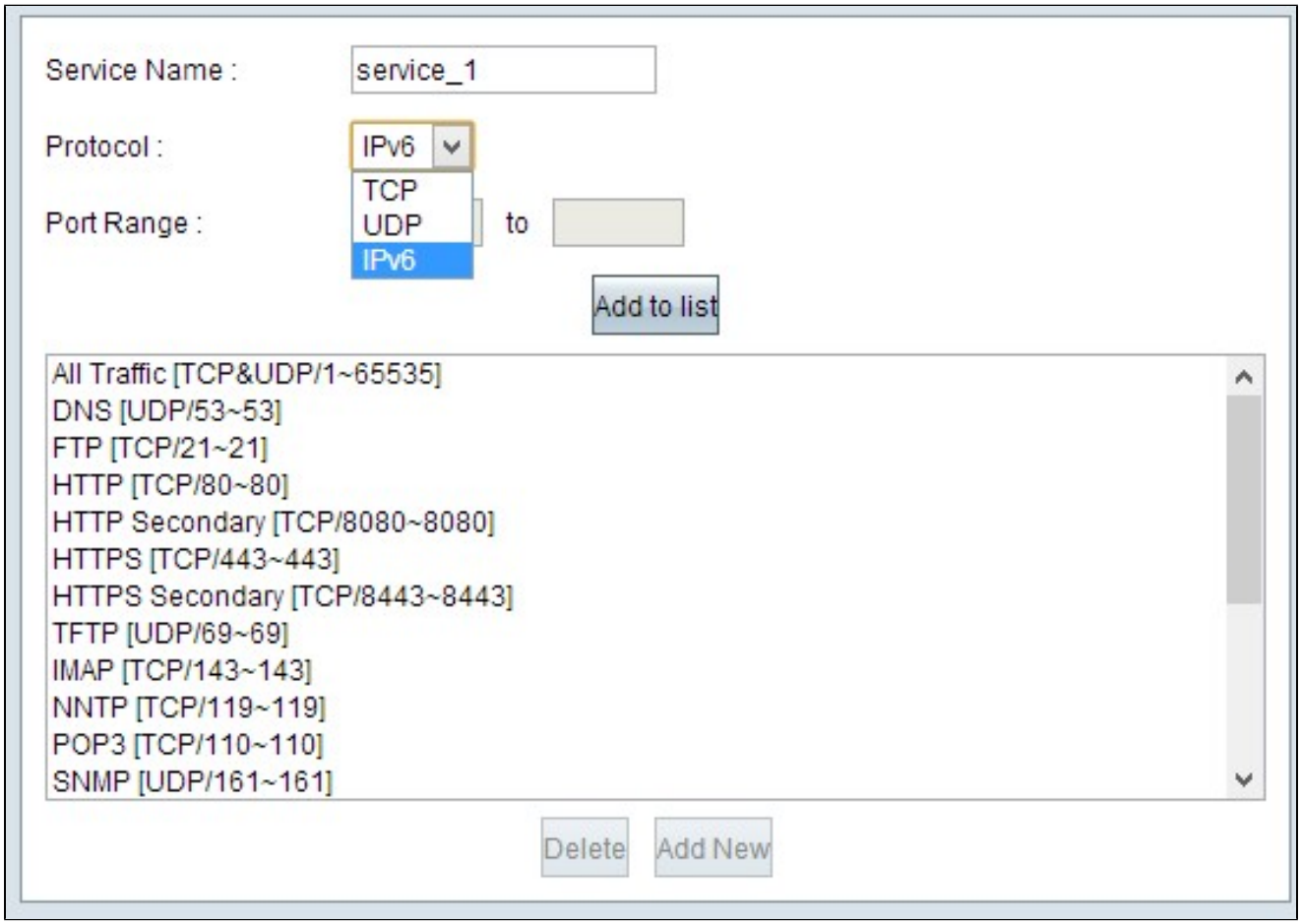
ステップ 3：[Save] をクリックします。プロトコルバインディングの設定が削除されます。

Service Management



ステップ 1：[サービス管理（Service Management）] をクリックします。Service Managementウィンドウが表示されます。


Service Name :
Protocol :
TCP
Port Range :
to
Add to list
All Traffic [TCP&UDP/1~65535]
DNS [UDP/53~53]
FTP [TCP/21~21]
HTTP [TCP/80~80]
HTTP Secondary [TCP/8080~8080]
HTTPS [TCP/443~443]
HTTPS Secondary [TCP/8443~8443]
TFTP [UDP/69~69]
IMAP [TCP/143~143]
NNTP [TCP/119~119]
POP3 [TCP/110~110]
SNMP [UDP/161~161]
Delete
Add New


Service Name :
service_1
Protocol :
IPv6
TCP
UDP
IPv6
Port Range :
to
Add to list
All Traffic [TCP&UDP/1~65535]
DNS [UDP/53~53]
FTP [TCP/21~21]
HTTP [TCP/80~80]
HTTP Secondary [TCP/8080~8080]
HTTPS [TCP/443~443]
HTTPS Secondary [TCP/8443~8443]
TFTP [UDP/69~69]
IMAP [TCP/143~143]
NNTP [TCP/119~119]
POP3 [TCP/110~110]
SNMP [UDP/161~161]
Delete
Add New

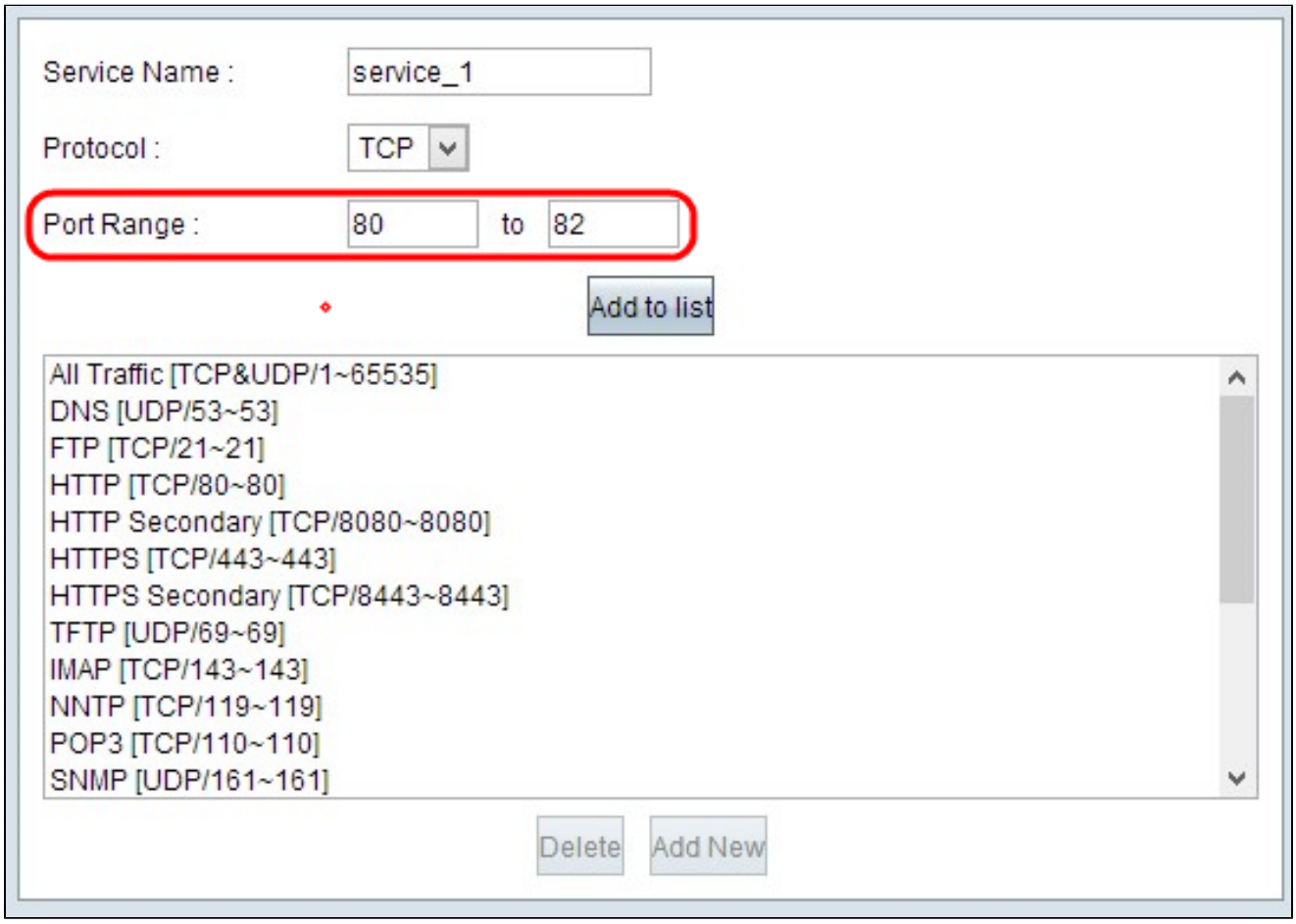
ステップ 2：Service Nameフィールドにサービスの名前を入力します。

ステップ 3：protocolドロップダウンリストから、サービスが使用するプロトコルを選択します。

・ TCP：このサービスはTransmission Control Protocol（TCP；伝送制御プロトコル）パケットを転送します。

・ UDP：このサービスはUser Datagram Protocol（UDP；ユーザデータグラムプロトコル）パケットを転送します。

・ IPv6：このサービスは、すべてのIPv6トラフィックを転送します。



ステップ 4：プロトコルがTCPまたはUDPの場合は、サービス用に予約されているポートの範囲をPort Rangeフィールドに入力します。

ステップ 5：[リストに追加（Add to List）] をクリックします。サービスがサービス管理テーブルに保存されます。

ステップ6: (オプション) 編集するサービスをクリックし、必要な情報を編集して、Saveをクリックします。編集方法の詳細については、前の手順を参照してください。

ステップ7: (オプション) 削除するサービスをクリックし、Deleteをクリックします。

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。