

RV34xシリーズルータでのポート転送/ポートトリガー/NATの設定

目的

ポートフォワーディングとポートトリガーの目的を説明し、RV34xシリーズルータでこれらの機能を設定する手順を示します。

- ポートフォワーディングとポートトリガーの比較
- ポートフォワーディングおよびポートトリガーの設定
- ネットワークアドレス変換(NAT)の設定

該当するデバイス

- RV34xルータシリーズ

[Software Version]

- 1.0.01.17

ポートフォワーディングとポートトリガーの比較

これらの機能により、一部のインターネットユーザはネットワーク上の特定のリソースにアクセスでき、プライベートなリソースを保護できます。これを使用する場合の例を次に示します。web/eメールサーバ、アラームシステム、およびセキュリティカメラのホスティング（ビデオをオフサイトのコンピュータに返送するため）ポート転送は、指定されたサービスの着信トラフィックに反応してポートを開きます。

これらのポートのリストと説明は、セットアップウィザードの[Service Management]セクションに情報を入力すると設定されます。これらの設定では、ポートフォワーディングとポートトリガーの両方に同じポート番号を使用することはできません。

ポート転送

ポート転送は、着信トラフィックに反応してサービスの特定のポートを開くことによって、ローカルエリアネットワーク(LAN)上のネットワークデバイス上のサービスへのパブリックアクセスを可能にするテクノロジーです。これにより、パケットが目的の宛先に対する明確なパスを持つようになります。これにより、ダウンロード速度が速くなり、遅延が短くなります。これは、ネットワーク上の1台のコンピュータに設定されます。特定のコンピュータのIPアドレスを追加する必要があり、変更できません。

これは、選択した特定の範囲のポートを開き、変更しないスタティック操作です。これは、設定されたポートが常にオープンであるため、セキュリティリスクを増大させる可能性があります。

割り当てられたデバイスのポートでドアが常に開いていることを想像してみてください。

ポートトリガー

ポートトリガーはポート転送に似ていますが、もう少し安全です。違いは、トリガーポートがその特定のトラフィックに対して常にオープンであるとは限らないことです。LAN上のリソースがトリガーポートを介して発信トラフィックを送信した後、ルータは指定されたポートまたはポート範囲を介して着信トラフィックをリッスンします。トリガーされたポートは、アクティビティが存在しない場合に閉じられ、セキュリティが強化されます。もう1つの利点は、ネットワーク上の複数のコンピュータが異なる時刻にこのポートにアクセスできることです。したがって、事前にトリガーするコンピュータのIPアドレスを知る必要はありません。これは自動的に行われます。

誰かにパスを与えると思いますが、そこにドアの男が入るたびにパスをチェックし、次のパスを持つ人が到着するまでドアを閉めます。

ポートフォワーディングおよびポートトリガーの設定

ポート転送

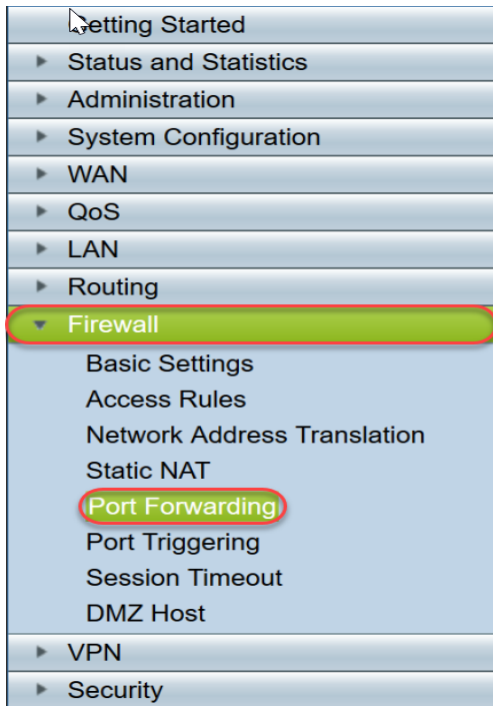
ポート転送を設定するには、次の手順を実行します。

ステップ1: Web設定ユーティリティにログインします。検索/アドレスバーにルータのIPアドレスを入力します。ブラウザから、Webサイトが信頼できないという警告が表示されることがあります。Webサイトに移動します。この手順の詳細については、[ここをクリックしてください](#)。

ルータのユーザ名とパスワードを入力し、[Log In]をクリックします。デフォルトのユーザ名とパスワードはciscoです。

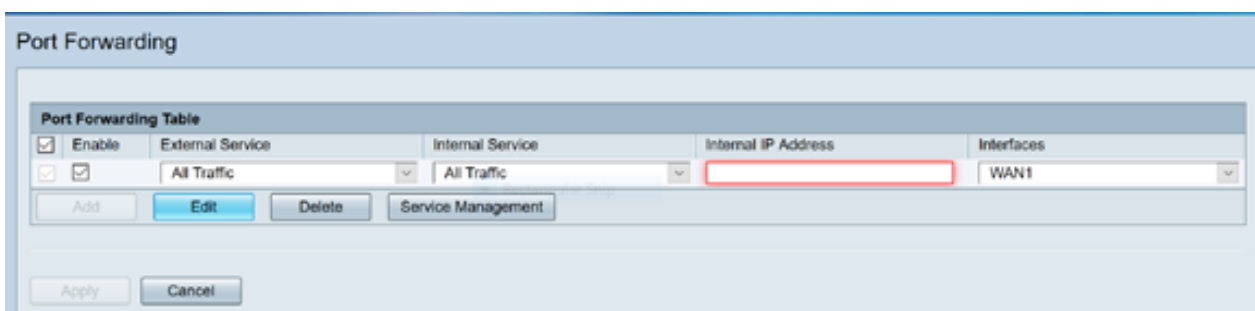


ステップ2 : 左側のメインメニューで、[Firewall] > [Port Forwarding]をクリックします



ポート転送テーブルで、[追加]をクリックするか、行を選択し、[編集]をクリックして次の項目を設定します。

外部サービス	ドロップダウンリストから外部サービスを選択します。(サービスがリストされ Management]セクションの手順に従ってリストを追加または変更できます)。
内部サービス	ドロップダウンリストから内部サービスを選択します。(サービスがリストされ Management]セクションの手順に従ってリストを追加または変更できます)。
内部IPアドレス	サーバの内部IPアドレスを入力します。
インターフェイス	ポートフォワーディングを適用するインターフェイスをドロップダウンリストから
ステータス	ポート転送ルールを有効または無効にします。



たとえば、ある企業がLAN上でWebサーバ(内部IPアドレス192.0.2.1)をホストするとします。HTTPトラフィックのポート転送ルールを有効にできます。これにより、インターネットからそのネットワークへの要求が許可されます。IPアドレス192.0.2.1に転送するポート番号80(HTTP)を設定し、外部ユーザからのすべてのHTTP要求を192.0.2.1に転送します。これは、ネットワーク内のその特定のデバイスに対して設定されます。

ステップ3:[Service Management]をクリックします。

[Service Table]で、[Add]をクリックするか、行を選択し、[Edit]をクリックして次の項目を設定します。

- [Application Name] : サービスまたはアプリケーションの名前
- プロトコル : 必須プロトコル。ホスティングしているサービスのマニュアルを参照してください
- Port Start/ICMP Type/IP Protocol : このサービス用に予約されているポート番号の範囲
- Port End : このサービス用に予約されているポートの最後の番号

Service Management

Service Table				
<input type="checkbox"/>	Application Name	Protocol *	Port Start/ICMP Type/IP Protocol	Port End
<input type="checkbox"/>	SMTP	TCP	25	25
<input type="checkbox"/>	SNMP-TCP	TCP	161	161
<input type="checkbox"/>	SNMP-TRAPS-TCP	TCP	162	162
<input type="checkbox"/>	SNMP-TRAPS-UDP	UDP	162	162
<input type="checkbox"/>	SNMP-UDP	UDP	161	161
<input type="checkbox"/>	SSH-TCP	TCP	22	22
<input type="checkbox"/>	SSH-UDP	UDP	22	22
<input type="checkbox"/>	TACACS	TCP	49	49
<input type="checkbox"/>	TELNET	TCP	23	23
<input type="checkbox"/>	TFTP	UDP	69	69
<input checked="" type="checkbox"/>	<input type="text" value=""/>	TCP	<input type="text" value="10000"/>	<input type="text" value="10000"/>

* When a service is in use by Port Forwarding / Port Triggering settings, this service can not apply ICMP/IP on the Protocol Type.

Add Edit Delete

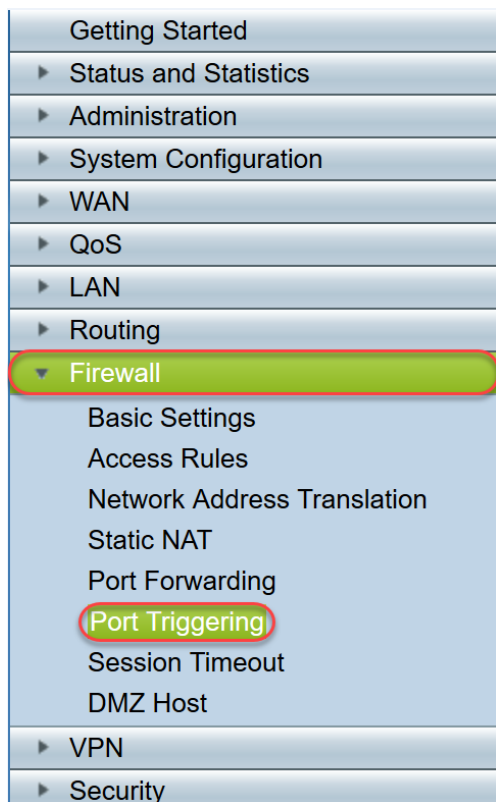
Apply Back Cancel

ステップ4:[Apply]をクリックします

ポートトリガー

ポートトリガーを設定するには、次の手順を実行します。

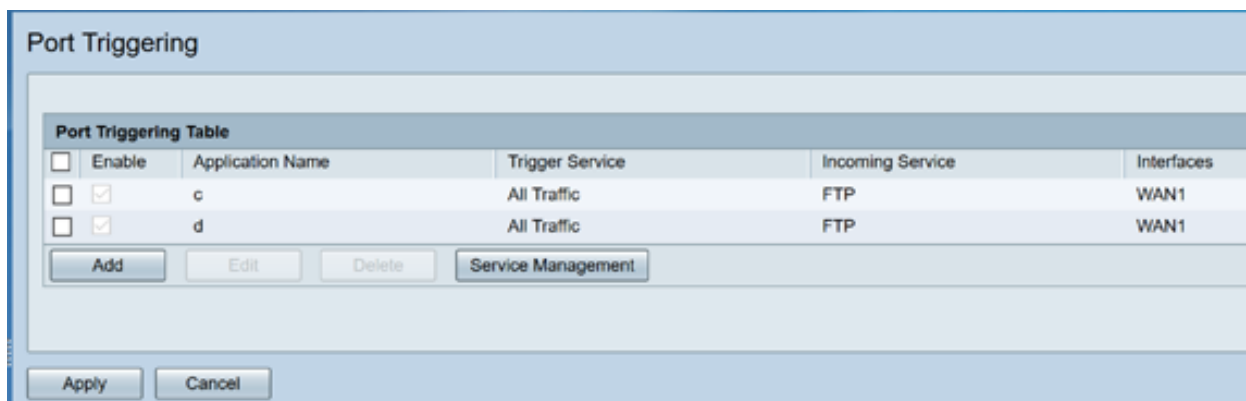
ステップ1:Web設定ユーティリティにログインします。左側のメインメニューで、[Firewall] > [Port Triggering] をクリックします



ステップ2：ポートトリガータブルにサービスを追加または編集するには、次のように設定します。

アプリケーション名	アプリケーションの名前を入力します。
トリガーサービス	ドロップダウンリストからサービスを選択します。(サービスがリストされていない場合は[サービス管理]セクションの手順に従ってリストを追加または変更できます)。
着信サービス	ドロップダウンリストからサービスを選択します。(サービスがリストされていない場合は[サービス管理]セクションの手順に従ってリストを追加または変更できます)。
インターフェイス	ドロップダウンリストからインターフェイスを選択します。
ステータス	ポートトリガールールを有効または無効にします。

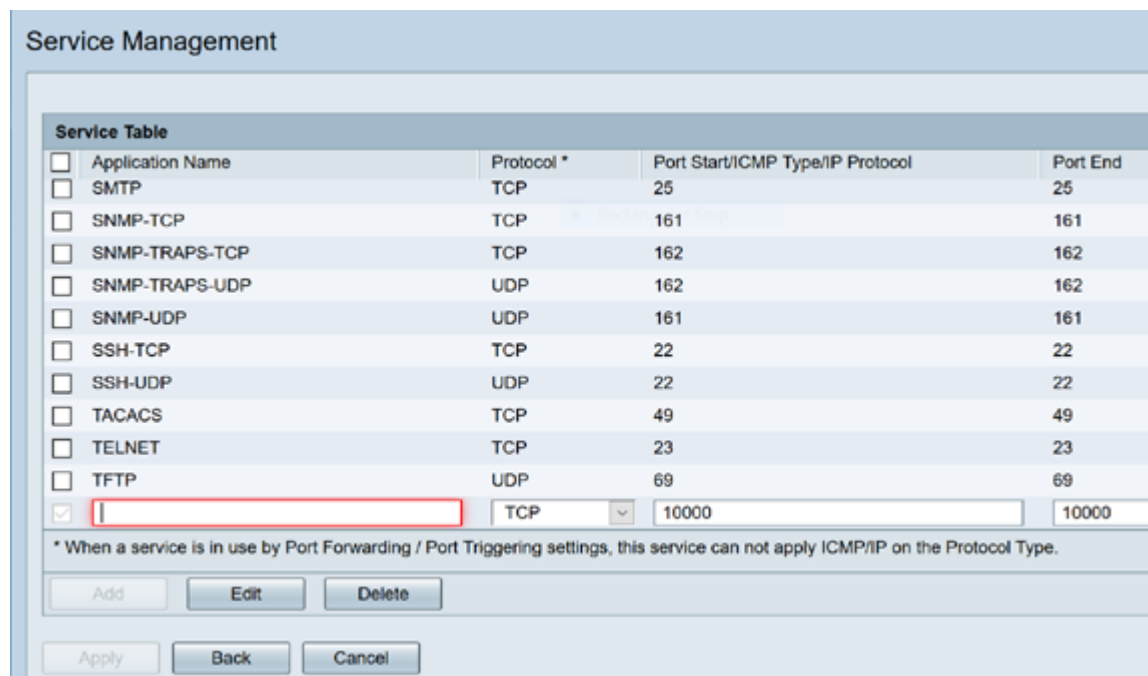
[追加]をクリックし(または行を選択して[編集]をクリック)、次の情報を入力します。



ステップ3：[サービス管理]をクリックし、[サービス]リストのエントリを追加または編集します。

[Service Table]で、[Add]または[Edit]をクリックして、次の項目を設定します。

- [Application Name] : サービスまたはアプリケーションの名前
- プロトコル : 必須プロトコル。ホスティングしているサービスのマニュアルを参照してください
- Port Start/ICMP Type/IP Protocol : このサービス用に予約されているポート番号の範囲
- Port End : このサービス用に予約されているポートの最後の番号



The screenshot shows the 'Service Management' window. It contains a 'Service Table' with the following data:

Application Name	Protocol *	Port Start/ICMP Type/IP Protocol	Port End
<input type="checkbox"/> SMTP	TCP	25	25
<input type="checkbox"/> SNMP-TCP	TCP	161	161
<input type="checkbox"/> SNMP-TRAPS-TCP	TCP	162	162
<input type="checkbox"/> SNMP-TRAPS-UDP	UDP	162	162
<input type="checkbox"/> SNMP-UDP	UDP	161	161
<input type="checkbox"/> SSH-TCP	TCP	22	22
<input type="checkbox"/> SSH-UDP	UDP	22	22
<input type="checkbox"/> TACACS	TCP	49	49
<input type="checkbox"/> TELNET	TCP	23	23
<input type="checkbox"/> TFTP	UDP	69	69
<input checked="" type="checkbox"/>	TCP	10000	10000

Below the table, there is a note: '* When a service is in use by Port Forwarding / Port Triggering settings, this service can not apply ICMP/IP on the Protocol Type.'

At the bottom, there are buttons for 'Add', 'Edit', 'Delete', 'Apply', 'Back', and 'Cancel'.

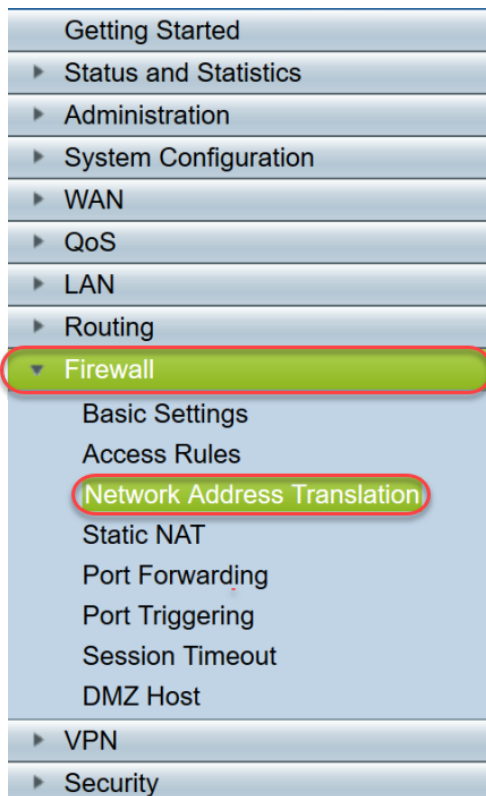
ステップ4:[Apply]をクリックします

ネットワークアドレス変換

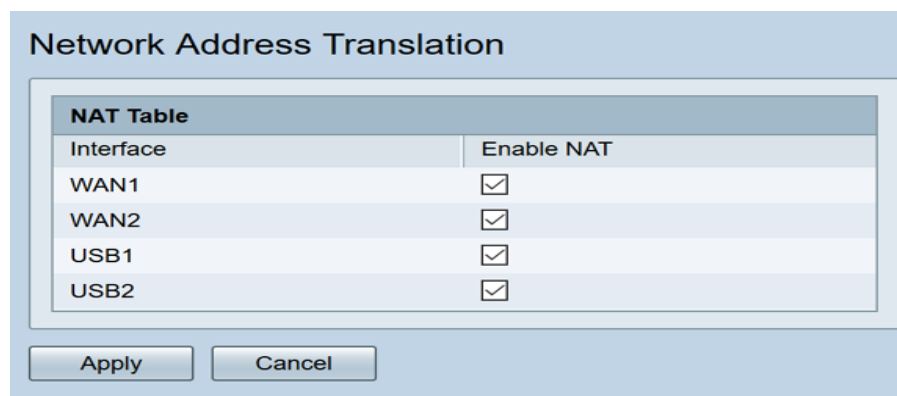
ネットワークアドレス変換(NAT)により、未登録のIPアドレスを持つプライベートIPネットワークをパブリックネットワークに接続できます。これは、ほとんどのネットワークで一般的に設定されているプロトコルです。NATは、パケットがパブリックネットワークに転送される前に、内部ネットワークのプライベートIPアドレスをパブリックIPアドレスに変換します。これにより、内部ネットワーク上の多数のホストが、限られた数のパブリックIPアドレスを使用してインターネットにアクセスできます。また、プライベートIPアドレスは非表示のままであるため、悪意のある攻撃や検出からプライベートIPアドレスを保護することもできます。

NATを設定するには、次の手順を実行します

ステップ1:[Firewall] > [Network Address Translation]をクリックします。



ステップ2:NATテーブルで、リストの該当する各インターフェイスの[Enable NAT]をオンにして、



ステップ3:[Apply]をクリックします

これで、ポート転送、ポートトリガー、およびNATが正しく設定されました。

その他のリソース

- スタティックNATの設定については、[ここをクリックしてください](#)
- RV3xxシリーズを含むルータに関する多くの質問に対する回答については、[ここをクリックしてください](#)
- RV34xシリーズに関するFAQについては、[ここをクリックしてください](#)
- RV345およびRV345Pの詳細については、[ここをクリックしてください](#)
- RV34xシリーズのService Managementの設定の詳細については、[ここをクリックしてください](#)

[この記事に関連するビデオを表示...](#)

[シスコのその他のテクニカルトークを表示するには、ここをクリックしてください](#)