

RV34x シリーズ ルータのポート フォワーディング/ポート Triggering/NAT を設定して下さい

目標

誘発するポート フォワーディングおよびポートの目的を説明し、RV34x シリーズ ルータのこれらの機能を設定する指示を提供して下さい。

- ポート フォワーディングおよびポート 誘発の比較
- ポート フォワーディングおよびポート 誘発の設定
- ネットワーク アドレス変換 (NAT) の設定

適当なデバイス

- RV34x ルータシリーズ

[Software Version]

- 1.0.01.17

ポート フォワーディングおよびポート 誘発の比較

これらの機能はプライベートにしておきたいと思うことリソースを保護している間何人かのインターネットユーザをネットワークの特定のリソースにアクセスできる割り当てます。これが使用される時いくつかの例: Web をホストして/サーバ、警報 システムおよび保安用カメラを E-メールを送って下さい (ビデオをに offsite 送り返すためコンピュータ)。ポート フォワーディングは指定 サービスのための受信 トラフィックに応じてポートをオープンにします。

Setup ウィザードのサービス マネジメント セクションで情報を入力するときこれらのポートのリストおよび記述は設定されます。ポート両方フォワーディングおよびポート 誘発のためにセットこれら、同じ ポート数を使用できない時。

ポート フォワーディング

ポート フォワーディングはテクノロジーですローカルエリア・ ネットワーク (LAN) のネットワーク デバイスのサービスに受信 トラフィックに応じてサービスのための特定のポートをオープンにすることによってパブリックアクセスを許可する。これはパケットにより速いダウンロード速度およびより低いレイテンシーを可能にする意図されたデスティネーションにクリア パスがあることを確認します。これはネットワークの単一のコンピュータのために設定されます。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。

これは選択する開き、変更しない特定のポート範囲を静的なオペレーションです。これは設定されたポートが開いている常にのでセキュリティリスクを高めるかもしれません。

割り当てられたことドアがそのデバイスにそのポートで開いている常にことを想像して下さい。

ポート誘発

ポート誘発はポート フォワーディングに類似したややセキュアでありではない。違いはトリガー ポートがその特定のトラフィックのために開いていない常にことです。LAN のリソースがトリガー ポートを通して送信トラフィックを送信した後、ルータは特定のポートがポート範囲を通して受信トラフィックを聞き取ります。誘発されたポートはセキュリティに追加するアクティビティがないとき閉じます。もう一つの利点はネットワーク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。従って、それ自動的にしますこれをそれを先立って誘発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。

誰かにパスを与えているあなたについて考えて下さいしかしそこにパスを持つ次の人が着くまでいつもドアを入力し、閉じるパスをチェックするそこにドアボーイです。

ポート フォワーディングおよびポート誘発の設定

ポート フォワーディング

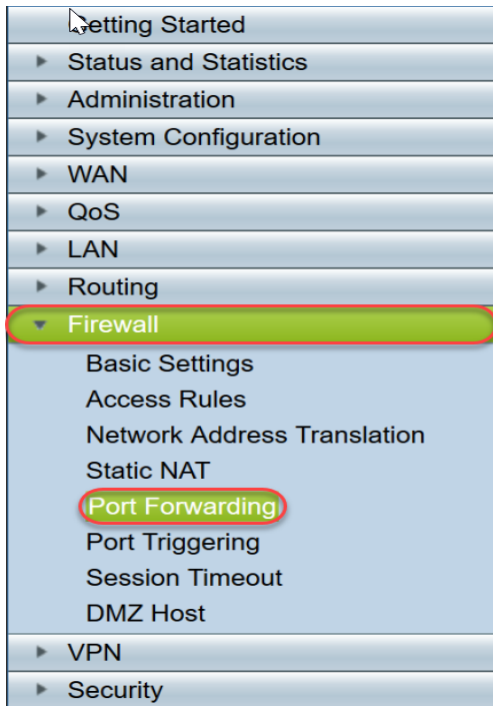
ポート フォワーディングを設定するために、次の手順に従って下さい:

ステップ 1. Web コンフィギュレーションユーティリティへのログイン。検索/アドレスバーでルータのための IP アドレスを入力して下さい。ブラウザは Web サイトが信頼できないこと警告を発するかもしれません。Web サイトに進んで下さい。 [このステップのより多くの指導に関しては、ここをクリックして下さい。](#)

ルータのためのユーザ名 および パスワードを入力し、『Log In』 をクリックして下さい。デフォルトのユーザ名およびパスワードは cisco です。

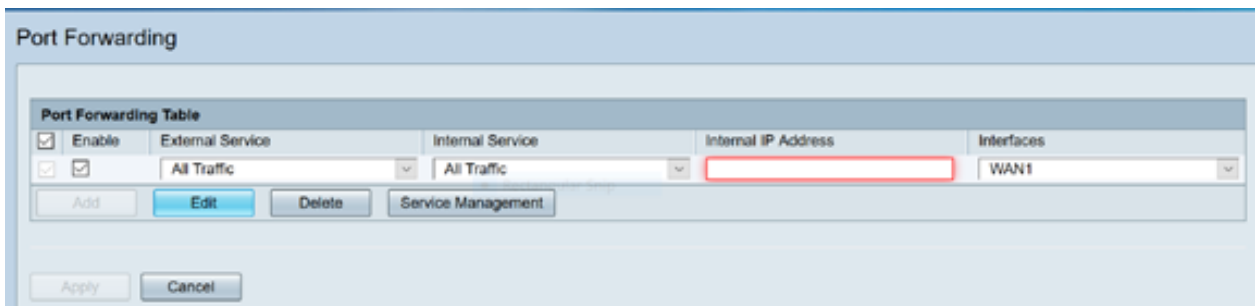


ステップ 2. From は左側のメイン メニュー、ファイアウォール > ポート フォワーディング をクリックします



ポート フォワーディング表で、『Add』 をクリック しか、または行を選択し、次を設定する ために『Edit』 をクリック して下さい:

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て下さい。 サービスがリストさ ていなければ (、サービス マネジメント セクションの手順に従うことによっ てリ トを追加するか、または修正できます。)
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て下さい。 サービスがリストさ ていなければ (、サービス マネジメント セクションの手順に従うことによっ てリ トを追加するか、または修正できます。)
内部 IP アドレス	サーバの内部 IP アドレスを入力して下さい。
インターフェイス	ポート フォワーディングを適用するためにドロップダウン リストからインターフ ィイスを、選択して下さい。
ステータス	ポート フォワーディング ルールを有効に するか、または無効に して下さい。



たとえば、会社は LAN の Webサーバを (192.0.2.1 の内部 IP アドレスと) ホストします。 HTTP トラフィックのためのポート フォワーディング ルールは有効に することができます。 これはそのネットワークにインターネットからの要求を可能にします。 会社は第 80 (HTTP) 転送されるべき IP アドレス 192.0.2.1 に設定 します、そして外部利用者からす べての HTTP 要求は 192.0.2.1 に転送されます。 それはネットワークのその特定のデバイ スのために設定されます。

ステップ 3 サービス管理をクリックして下さい

サービス表で、『Add』をクリックし、または行を選択し、次を『Edit』をクリックし、設定して下さい:

- アプリケーション名-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。ホストしていることサービスのためのドキュメントを参照して下さい
- ポート Start/ICMP Type/IP プロトコル-このサービスのために予約されるポート番号の範囲
- ポート端-このサービスのために予約済みのポートの最後の数

The screenshot shows the 'Service Management' interface. It features a 'Service Table' with columns for 'Application Name', 'Protocol *', 'Port Start/ICMP Type/IP Protocol', and 'Port End'. The table lists various services like SMTP, SNMP, SSH, TACACS, TELNET, and TFTP. Below the table, there is a form to add a new service. The form has a checked checkbox, a text input field (highlighted with a red box), a protocol dropdown menu set to 'TCP', and two numeric input fields for 'Port Start' (10000) and 'Port End' (10000). Below the form, there are buttons for 'Add', 'Edit', and 'Delete'. At the bottom, there are buttons for 'Apply', 'Back', and 'Cancel'. A note at the bottom of the form states: '* When a service is in use by Port Forwarding / Port Triggering settings, this service can not apply ICMP/IP on the Protocol Type.'

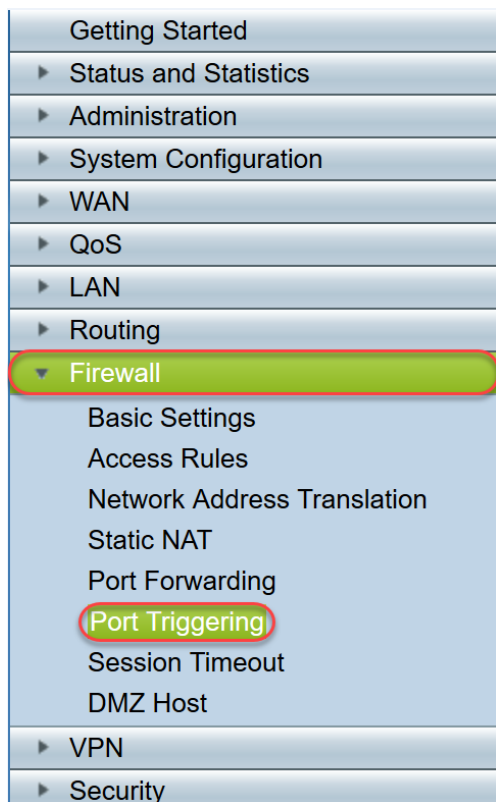
Application Name	Protocol *	Port Start/ICMP Type/IP Protocol	Port End
<input type="checkbox"/> SMTP	TCP	25	25
<input type="checkbox"/> SNMP-TCP	TCP	161	161
<input type="checkbox"/> SNMP-TRAPS-TCP	TCP	162	162
<input type="checkbox"/> SNMP-TRAPS-UDP	UDP	162	162
<input type="checkbox"/> SNMP-UDP	UDP	161	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

ステップ 4. 『Apply』 をクリックして下さい

ポート誘発

誘発するポートを設定するために次の手順に従って下さい:

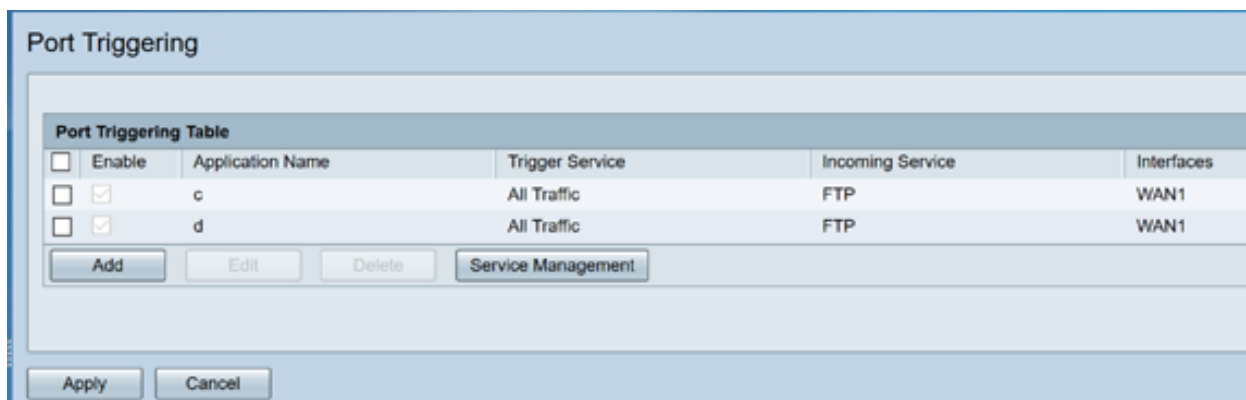
ステップ 1. Log Web コンフィギュレーションユーティリティに。左側のメインメニューから、ファイアウォール > ポート誘発をクリックして下さい



ステップ 2.To は表を誘発するポートにサービスを設定します次を追加するか、または編集します:

アプリケーション名	アプリケーションの名前を入力して下さい。
サービスを誘発して下さい	ドロップダウン リストからサービスを選択して下さい。 サービスがリストなければ (、サービス マネジメント セクションの手順に従うことによっ追加するか、または修正できます。)
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て下さい。 サービスがリストなければ (、サービス マネジメント セクションの手順に従うことによっ追加するか、または修正できます。)
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て下さい。
ステータス	ルールを誘発するポートを有効に するか、または無効にして下さい。

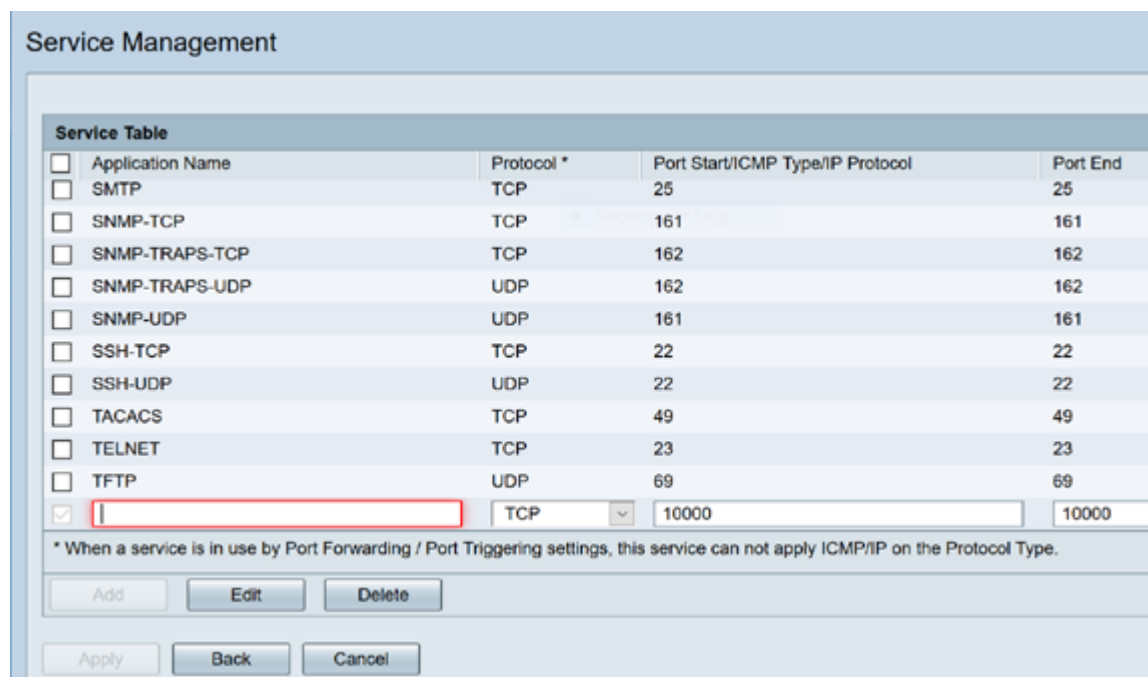
(または行を選択し、 『Edit』 をクリックし、) 『Add』 をクリックして下さい次の情報を入力して下さい:



ステップ 3. Service リストのエントリを追加するか、または編集するためにサービス管理を、クリックして下さい。

サービス表で、次を『Add』 をクリックしか、または編集し、設定して下さい:

- アプリケーション 名-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。 ホストしていることサービスのためのドキュメントを参照して下さい
- ポート Start/ICMP Type/IP プロトコル-このサービスのために予約されるポート 番号の範囲
- ポート端-このサービスのために予約済みのポートの最後の数



The screenshot shows the 'Service Management' window. It contains a 'Service Table' with the following columns: Application Name, Protocol *, Port Start/ICMP Type/IP Protocol, and Port End. The table lists several services, with the last row being a new entry with a red border around the 'Application Name' field, which is currently empty. The 'Protocol' is set to 'TCP' and the 'Port End' is '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'.

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"/>	TCP	10000	10000

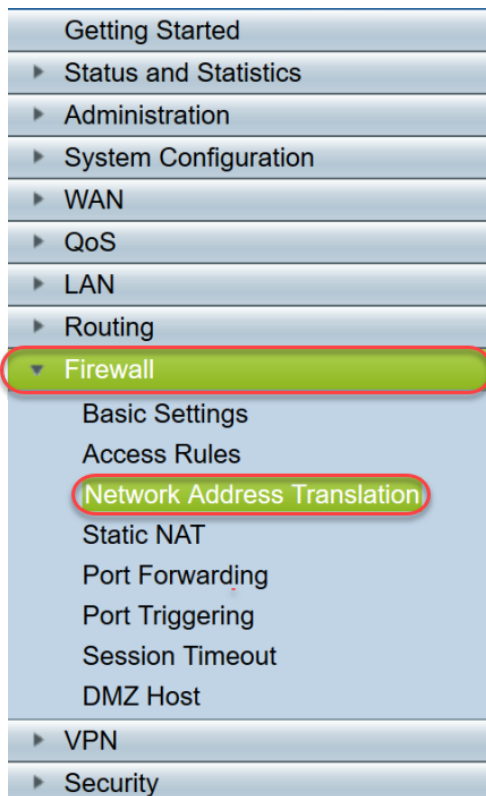
ステップ 4Apply をクリックします。

ネットワーク アドレス変換 (NAT)

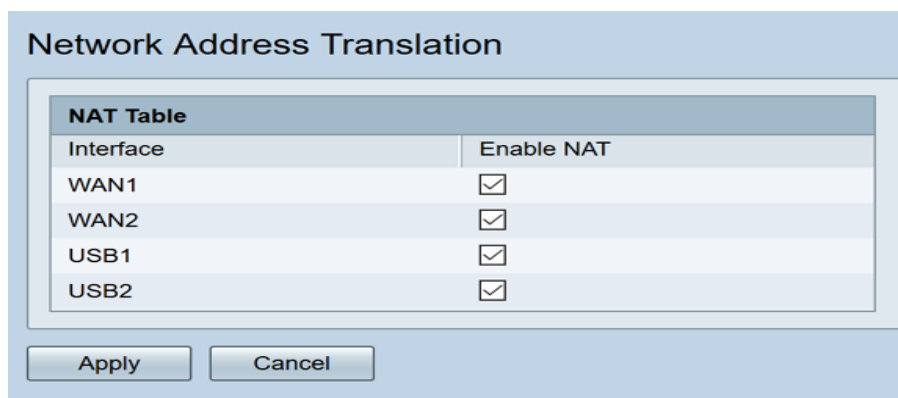
ネットワーク アドレス変換 (NAT) はパブリックネットワークに接続することを未登録 IP アドレスの私用 IP ネットワークが可能にします。これはほとんどのネットワークの一般に設定されたプロトコルです。NAT は公共 IP アドレスにパケットがパブリックネットワークに転送される前に内部ネットワークの私用 IP アドレスを変換します。これは内部ネットワークの多数のホストが公共 IP アドレスの限られた数を通してインターネットにアクセスするようにします。これはまた私用 IP アドレスが保存された非表示であるのであらゆる悪意のある不正侵入かディスカバリから私用 IP アドレスの保護を助けます。

NAT を設定するために、次の手順に従って下さい

ステップ 1.Click ファイアウォール > ネットワーク アドレス変換 (NAT)



呼び出します。NAT 表では、有効になるためにリストの各適切なインターフェイスがあるように有効 NAT を確認して下さい



ステップ 3. 『Apply』 をクリックして下さい

誘発する設定されたポート フォワーディング、ポートおよび NAT が正常に今あります。

他のリソース

- [スタティック NAT の設定には、ここをクリックして下さい](#)
- [ルータについての多くの質問に対する回答に関しては、RV3xx シリーズを含んで、ここをクリックして下さい](#)
- [RV34x シリーズの FAQ に関しては、ここをクリックして下さい](#)
- [RV345 および RV345P に関する詳細については、ここをクリックして下さい](#)
- [RV34x シリーズのサービス管理の設定に関する詳細については、ここをクリックして下さい](#)

表示して下さいこの技術情報に関するビデオを...

[Cisco からの他の Tech Talk を表示するためにここをクリックして下さい](#)