Configure Port Forwarding and Port Triggering in RV160 and RV260 Routers

Table of Contents

Objective

The objective of this article is to show you how to configure port forwarding and port triggering on the RV160 and RV260 Routers.

Applicable Devices | Firmware Version

RV160 | 1.0.00.13

RV260 | 1.0.00.13

Introduction

Port forwarding and port triggering are features that allow some internet users to have access to specific resources on your network, while protecting the resources that you want to keep private.

Port forwarding allows public access to services on network devices on the Local Area Network (LAN) by opening a specific port or port range for a service, such as file transfer protocol (FTP). Port forwarding opens a port range for services such as internet gaming that uses alternate ports to communicate between the server and the LAN host.

Port triggering allows a specified port or port range to open for inbound traffic after user sends outbound traffic through the trigger port. Port triggering allows the device to monitor outgoing data for specific port numbers. The device recalls the IP address of the client that sent the matching data. When the requested data returns through the device, the data is sent to the proper client using the IP addressing and port mapping rules.

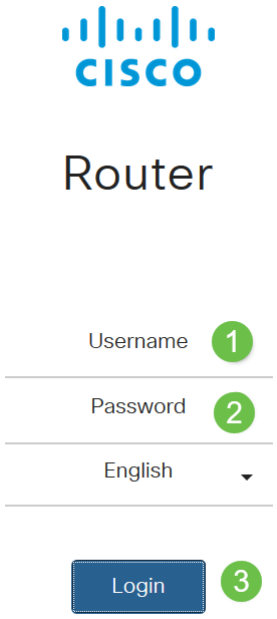
For more information on port forwarding and port triggering, click here.

Configure Port Forwarding

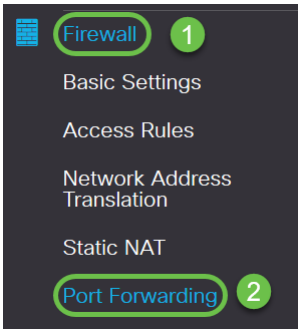
To configure port forwarding, follow these steps:

Step 1. Log in to the web configuration utility. Enter the username and password for the router and click **Login**. The default username and password is *cisco*.

In this article, we will be using the RV260 to configure port forwarding. The configuration may vary depending on the model you use.

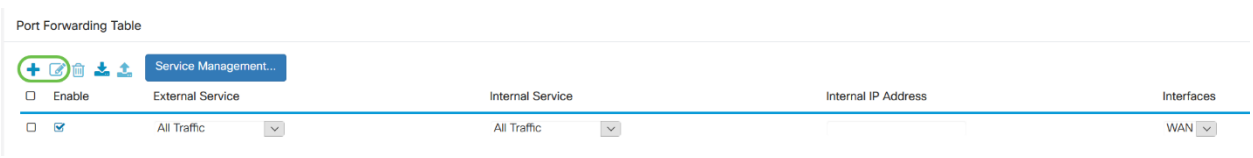


Step 2. Click **Firewall > Port Forwarding**.



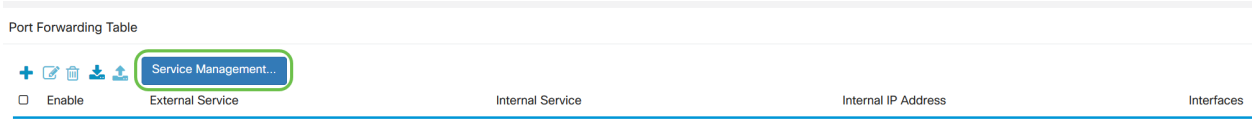
Step 3. In the Port Forwarding Table, click **add icon** or select the row and click **edit icon**) and configure the following:

Enable	**Check Enable to enable port forwarding**
External Service	Select an external service from the drop-down list. (If a service is not listed, you can add or modify the list by following the instructions in the Service Management section)
Internal Service	Select an internal service from the drop-down list. (If a service is not listed, you can add or modify the list by following the instructions in the Service Management section)
Internal IP Addresses	Enter the internal IP addresses of the server
Interfaces	Select the interface from the drop-down list, to apply port forwarding on



To add or edit an entry on the Service list, follow these steps:

Step 4. Click **Service Management**.



Step 5. In the *Service Management* click **Add icon** or select a row and click **Edit icon.**

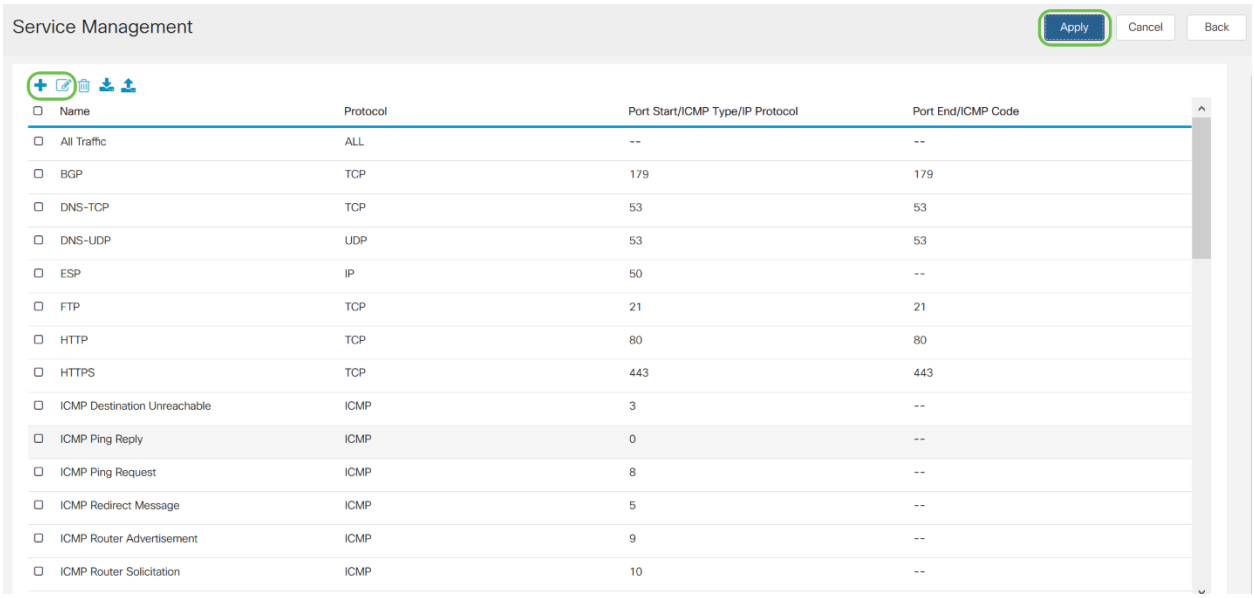
Configure the following:

Application Name - Name of the service or application.

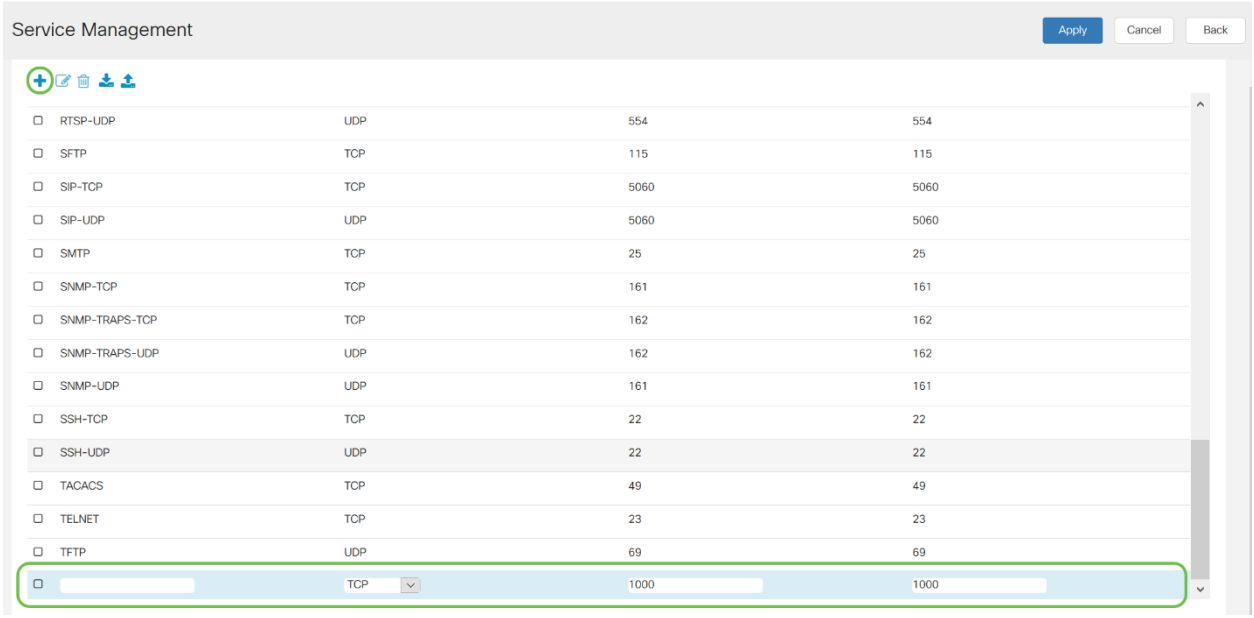
Protocol - Required protocol. Refer to the documentation for the service that you are hosting.

Port Start/ICMP Type/IP Protocol - Range of port numbers reserved for this service.

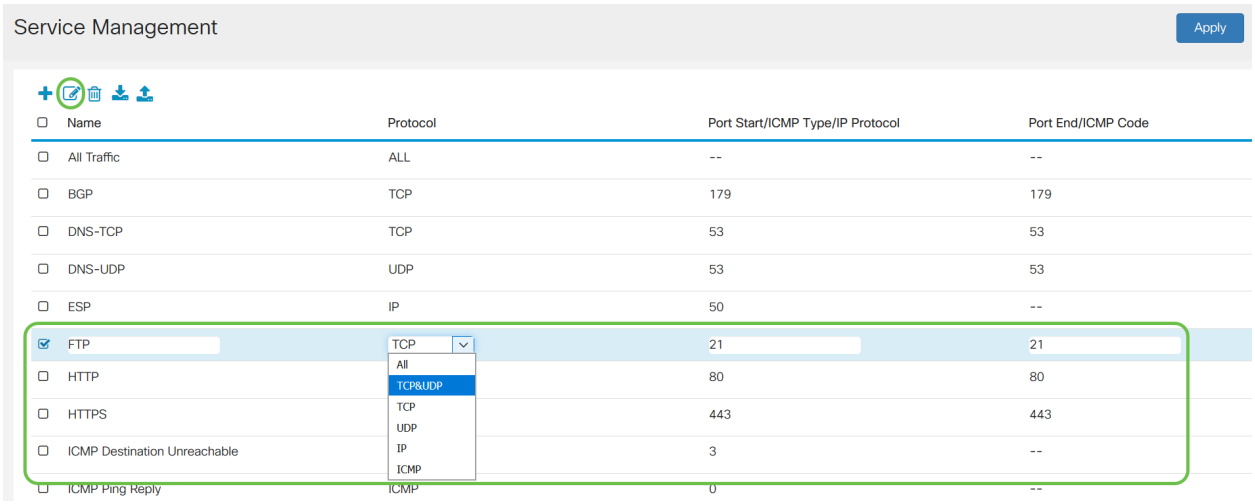
Port End - Last number of the port reserved for this service.



To add a service, click on the **plus icon** and configure Name, Protocol, Port Start/ICMP Type/IP Protocol and Port End/ICMP Code.

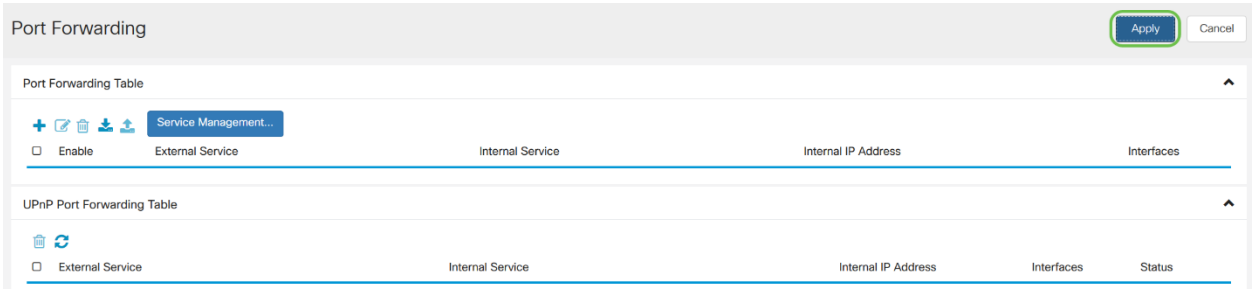


To edit a service, select a row and click on the **edit icon** to configure the fields as shown below.

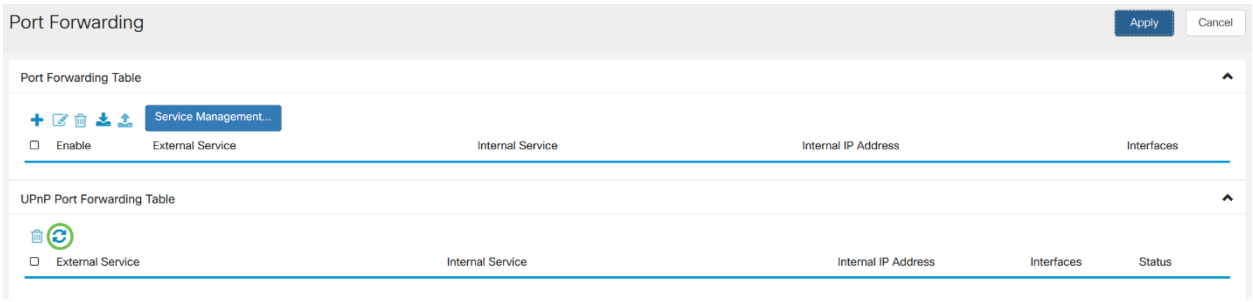


In this example, FTP service is selected.

Step 6. Click **Apply**.



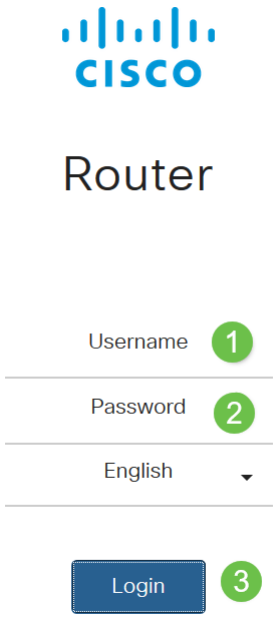
Step 7. In the Universal Plug and Play (UPnP) Port Forwarding Table, click the **refresh icon** to refresh the data. The port forwarding rules for UPnP are dynamically added by the UPnP application.



Configure Port Triggering

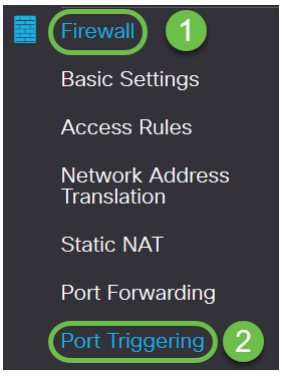
To configure port triggering, follow these steps:

Step 1. Log in to the web configuration utility. Enter the username and password for the router and click **Login**. The default username and password is *cisco*.



In this article, we will be using the RV260 to configure port triggering. The configuration may vary depending on the model you use.

Step 2. Click **Firewall > Port Triggering**.

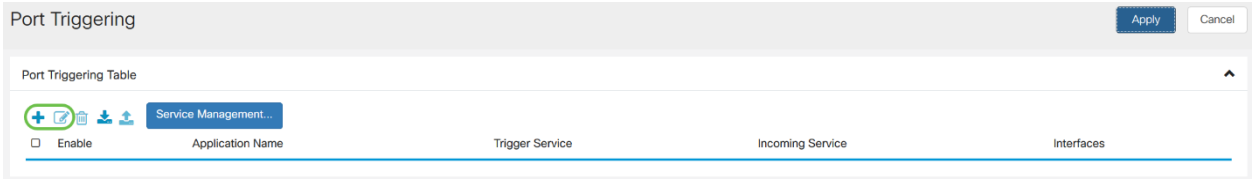


Step 3. To add or edit a service to the port triggering table, configure the following:

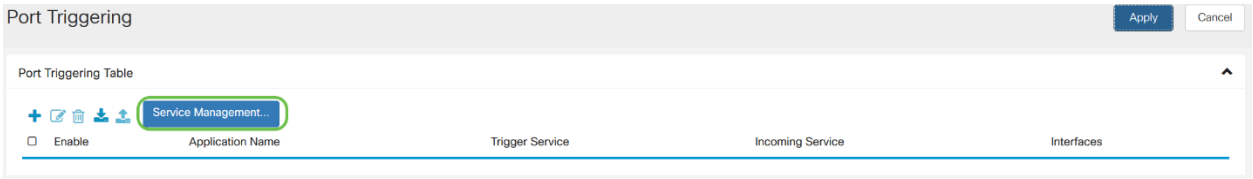
Click **add icon** (or select the row and click **edit icon** and enter the information:

Enable **Check to enable port triggering**

Application Name	Enter the name of the application
Trigger Service	Select a service from the drop-down list (If a service is not listed, you can add or modify the list by following the instructions in the Service Management section)
Incoming Service	Select a service from the drop-down list (If a service is not listed, you can add or modify the list by following the instructions in the Service Management section)
Interfaces	Select the interface from the drop-down list



Step 4. Click **Service Management** to add, or edit an entry on the Service list.



Step 5. In the *Service Management*, click **add icon** or select the row and click **edit icon.**

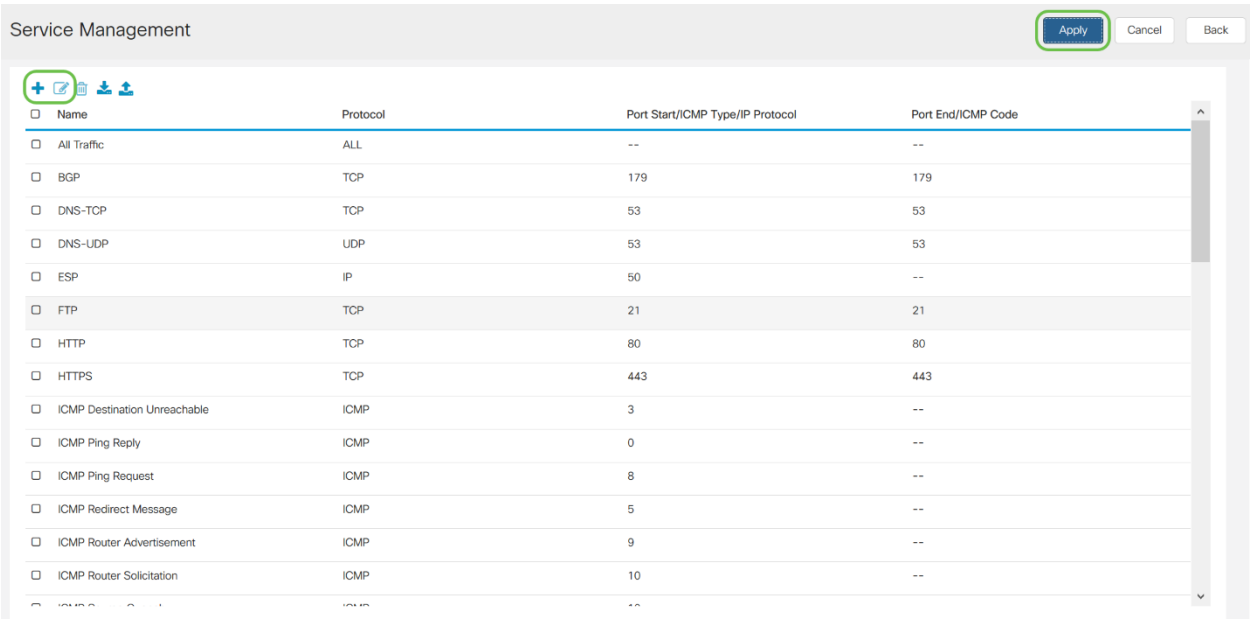
Configure the following:

Application Name - Name of the service or application.

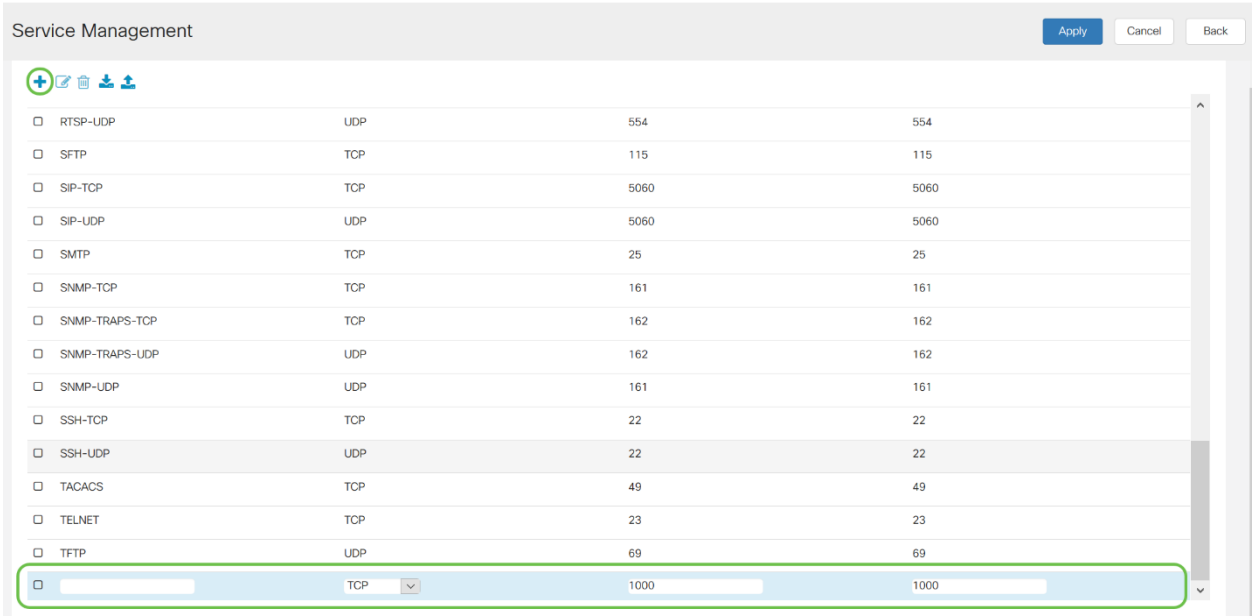
Protocol - Required protocol. Refer to the documentation for the service that you are hosting.

Port Start/ICMP Type/IP Protocol - Range of port numbers reserved for this service.

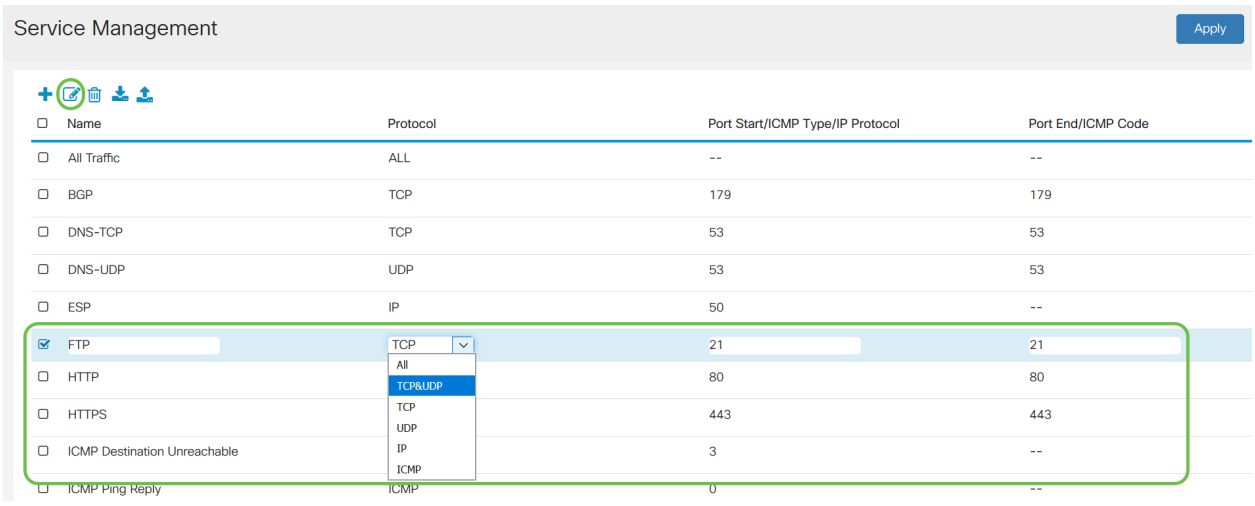
Port End - Last number of the port reserved for this service.



To add a service, click on the *plus icon* and configure *Name, Protocol, Port Start/ICMP Type/IP Protocol and Port End/ICMP Code.*

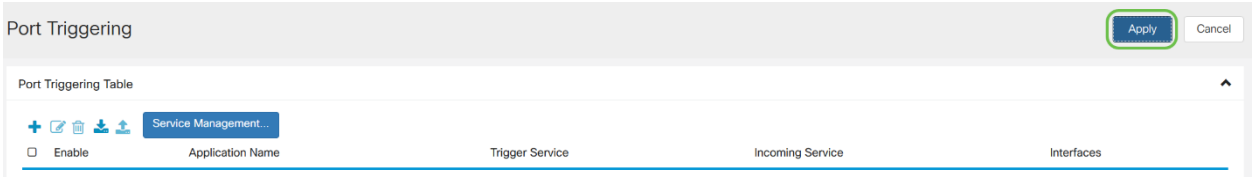


To edit a service, select a row and click on the *edit icon* to configure the fields as shown below.



In this example, FTP service is selected.

Step 6. **Click Apply**.



You have now successfully configured port forwarding/port triggering on the RV160 and RV260 Routers.