

# Configure o encaminhamento de portas e o disparo de portas nos roteadores RV160 e RV260

## Table Of Contents

- [Objetivo](#)
- [Dispositivos aplicáveis | Versão do firmware](#)
- [Introduction](#)
- [Configurar o encaminhamento de porta](#)
- [Configurar disparo de porta](#)

## Objetivo

O objetivo deste artigo é mostrar a você como configurar o encaminhamento de portas e o disparo de portas nos roteadores RV160 e RV260.

## Dispositivos aplicáveis | Versão do firmware

RV160 | 1.0.00.13

RV260 | 1.0.00.13

## Introduction

O encaminhamento de portas e o disparo de portas são recursos que permitem que alguns usuários da Internet tenham acesso a recursos específicos em sua rede, enquanto protegem os recursos que você deseja manter privados.

O encaminhamento de portas permite o acesso público a serviços em dispositivos de rede na LAN (Local Area Network, rede local) abrindo uma porta específica ou intervalo de portas para um serviço, como FTP (File Transfer Protocol, protocolo de transferência de arquivos). O encaminhamento de portas abre um intervalo de portas para serviços como jogos na Internet que usam portas alternativas para se comunicar entre o servidor e o host da LAN.

O disparo de portas permite que uma porta ou intervalo de portas especificado abra para o tráfego de entrada após o usuário enviar o tráfego de saída pela porta de disparo. O disparo de portas permite que o dispositivo monitore os dados de saída para números de porta específicos. O dispositivo recorda o endereço IP do cliente que enviou os dados correspondentes. Quando os dados solicitados retornam pelo dispositivo, os dados são enviados ao cliente apropriado usando o endereçamento IP e as regras de mapeamento de porta.

Para obter mais informações sobre o encaminhamento de portas e o disparo de portas, clique [aqui](#).

## Configurar o encaminhamento de porta

Para configurar o encaminhamento de portas, siga estas etapas:

Etapa 1. Faça login no utilitário de configuração da Web. Insira o nome de usuário e a senha do roteador e clique em **Login**. O nome do usuário e a senha padrão são cisco.

Neste artigo, usaremos o RV260 para configurar o encaminhamento de portas. A configuração pode variar dependendo do modelo usado.



## Router

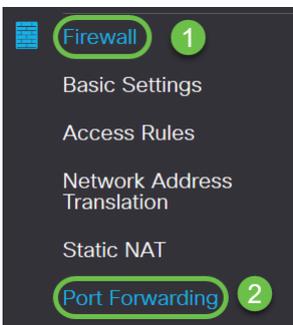
Username **1**

Password **2**

English ▼

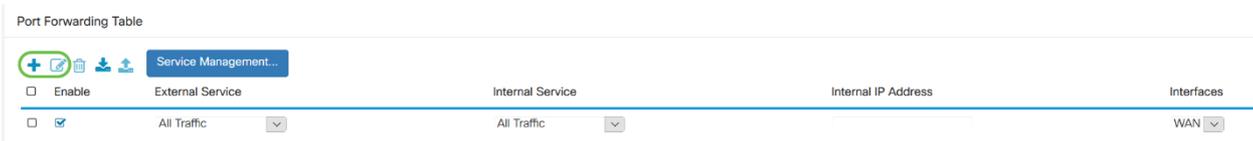
Login **3**

Etapa 2. Clique em **Firewall > Port Forwarding (Firewall > Encaminhamento de porta)**.



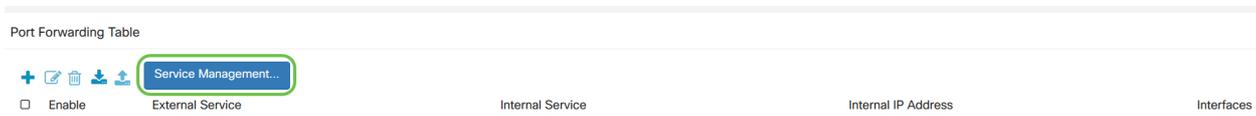
Etapa 3. Na Tabela de encaminhamento de portas, clique no **ícone adicionar** ou selecione a linha e clique no **ícone editar**) e configure o seguinte:

<b>Enable</b>	<b>Marque Habilitar para habilitar o encaminhamento de portas</b>
Serviço externo	Selecione um serviço externo na lista suspensa. (Se um serviço não estiver listado, você pode adicionar ou modificar a lista seguindo as instruções na seção Gerenciamento de serviços)
Serviço interno	Selecione um serviço interno na lista suspensa. (Se um serviço não estiver listado, você pode adicionar ou modificar a lista seguindo as instruções na seção Gerenciamento de serviços)
Endereços IP internos	Insira os endereços IP internos do servidor
Interfaces	Selecione a interface na lista suspensa para aplicar o encaminhamento de portas em



Para adicionar ou editar uma entrada na lista Serviço, siga estas etapas:

Etapa 4. Clique em **Gerenciamento de serviços**.



Etapa 5. No *Gerenciamento de serviços*, clique no **ícone Adicionar** ou selecione uma linha e clique no **ícone Editar**.

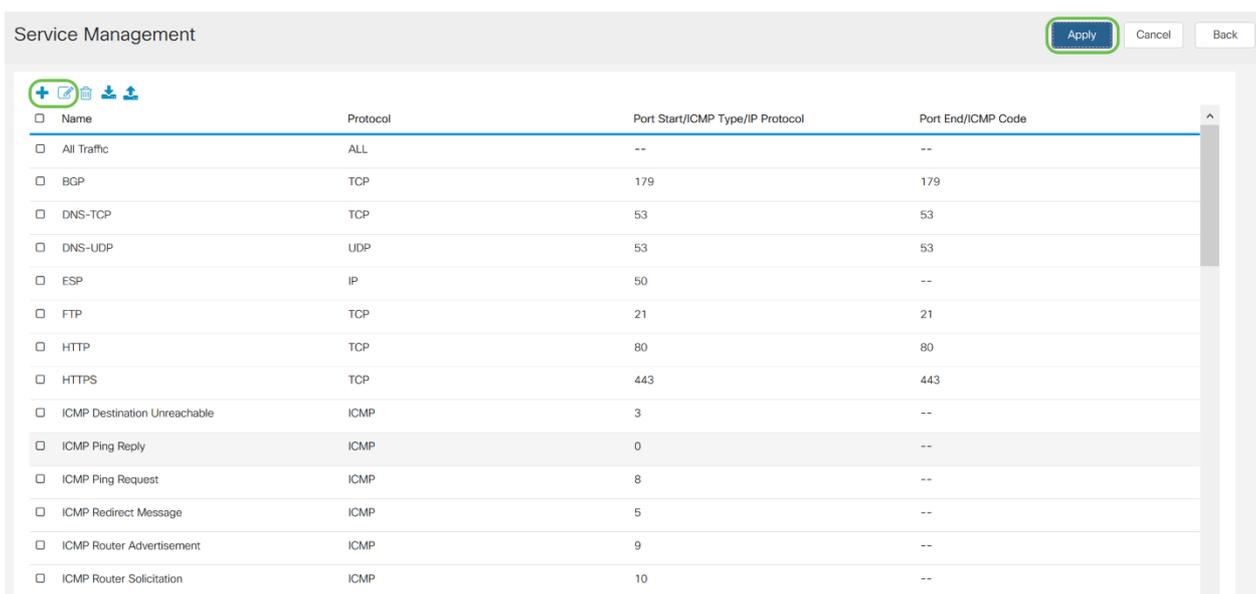
Configure o seguinte:

**Application Name** - Nome do serviço ou aplicativo.

**Protocolo** - Protocolo obrigatório. Consulte a documentação do serviço que você está hospedando.

**Port Start/ICMP Type/IP Protocol** - Intervalo de números de porta reservados para este serviço.

**Porta final** - último número da porta reservada para esse serviço.



Para adicionar um serviço, clique no **ícone de adição** e configure Nome, Protocolo, Início da porta/Tipo/IP de ICMP e Código de fim/ICMP da porta.

Service Management

Apply Cancel Back

Name	Protocol	Port Start	Port End
<input type="checkbox"/> RTSP-UDP	UDP	554	554
<input type="checkbox"/> SFTP	TCP	115	115
<input type="checkbox"/> SIP-TCP	TCP	5060	5060
<input type="checkbox"/> SIP-UDP	UDP	5060	5060
<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 type="checkbox"/> <input type="text"/>	TCP	1000	1000

Para editar um serviço, selecione uma linha e clique no ícone de edição para configurar os campos conforme mostrado abaixo.

Service Management

Apply

Name	Protocol	Port Start/ICMP Type/IP Protocol	Port End/ICMP Code
<input type="checkbox"/> All Traffic	ALL	--	--
<input type="checkbox"/> BGP	TCP	179	179
<input type="checkbox"/> DNS-TCP	TCP	53	53
<input type="checkbox"/> DNS-UDP	UDP	53	53
<input type="checkbox"/> ESP	IP	50	--
<input checked="" type="checkbox"/> FTP	TCP	21	21
<input type="checkbox"/> HTTP	All	80	80
<input type="checkbox"/> HTTPS	TCP&UDP	443	443
<input type="checkbox"/> ICMP Destination Unreachable	TCP	3	--
<input type="checkbox"/> ICMP Ping Reply	UDP	0	--
<input type="checkbox"/> ICMP Ping Reply	IP	0	--
<input type="checkbox"/> ICMP Ping Reply	ICMP	0	--

Neste exemplo, o serviço FTP é selecionado.

Etapa 6. Clique em Apply.

Port Forwarding

Apply Cancel

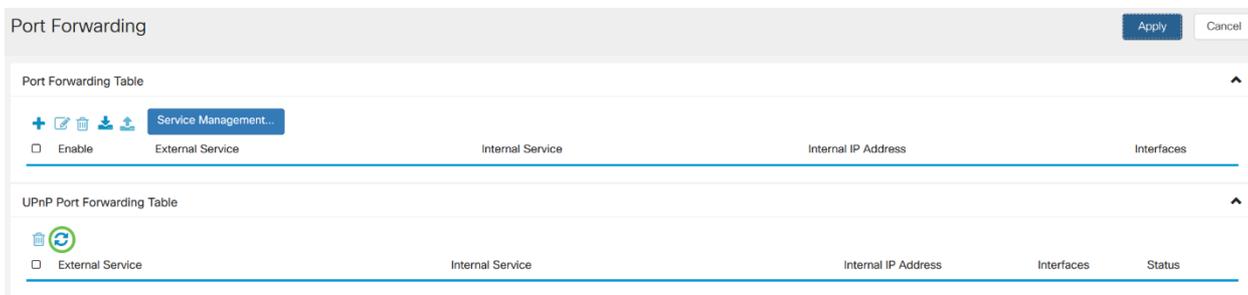
Port Forwarding Table

Enable	External Service	Internal Service	Internal IP Address	Interfaces
<input type="checkbox"/>				

UPnP Port Forwarding Table

External Service	Internal Service	Internal IP Address	Interfaces	Status
<input type="checkbox"/>				

Passo 7. Na Tabela de Encaminhamento de Portas Universal Plug and Play (UPnP), clique no ícone de atualização para atualizar os dados. As regras de encaminhamento de portas para UPnP são adicionadas dinamicamente pelo aplicativo UPnP.



## Configurar disparo de porta

Para configurar o disparo de portas, siga estas etapas:

Etapa 1. Faça login no utilitário de configuração da Web. Insira o nome de usuário e a senha do roteador e clique em **Login**. O nome do usuário e a senha padrão são cisco.



### Router

Username **1**

---

Password **2**

---

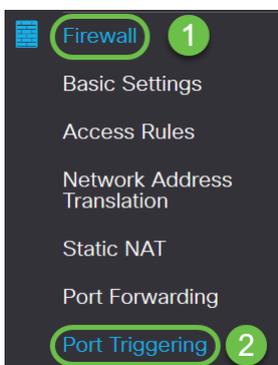
English **3**

---

Login **3**

Neste artigo, usaremos o RV260 para configurar o disparo de portas. A configuração pode variar dependendo do modelo usado.

Etapa 2. Clique em **Firewall > Port Triggering (Firewall> Disparo de portas)**.



Etapa 3. Para adicionar ou editar um serviço à tabela de disparo de portas, configure o seguinte:

Clique no ícone **Adicionar** (ou selecione a linha e clique no ícone **Editar** e insira as informações:

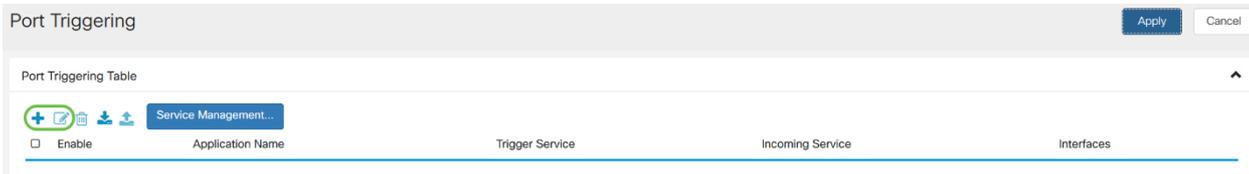
**Enable** Marque para ativar o disparo de portas

Nome do aplicativo Insira o nome do aplicativo

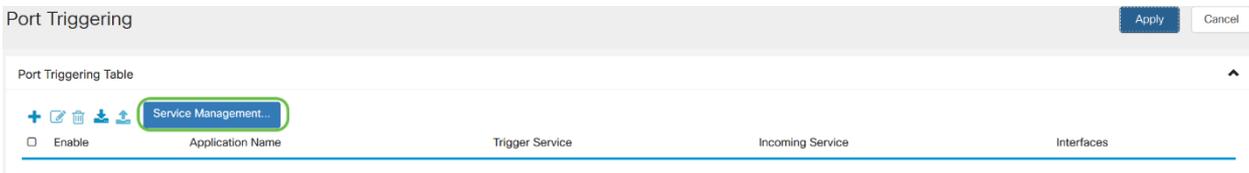
Serviço de disparo Selecione um serviço na lista suspensa (se um serviço não estiver listado, você pode adicionar ou modificar a lista seguindo as instruções na seção Gerenciamento de serviços)

Serviço de entrada Selecione um serviço na lista suspensa (se um serviço não estiver listado, você pode adicionar ou modificar a lista seguindo as instruções na seção Gerenciamento de serviços)

Interfaces Selecione a interface na lista suspensa



Etapa 4. Clique em **Gerenciamento de serviços** para adicionar ou editar uma entrada na lista Serviço.



Etapa 5. No *Gerenciamento de serviços*, clique no **ícone Adicionar** ou selecione a linha e clique no **ícone de edição**.

Configure o seguinte:

**Application Name** - Nome do serviço ou aplicativo.

**Protocolo** - Protocolo obrigatório. Consulte a documentação do serviço que você está hospedando.

**Port Start/ICMP Type/IP Protocol** - Intervalo de números de porta reservados para este serviço.

**Porta final** - último número da porta reservada para esse serviço.

Service Management

Apply Cancel Back

+ [edit] [delete] [download] [upload]

<input type="checkbox"/> Name	Protocol	Port Start/ICMP Type/IP Protocol	Port End/ICMP Code
<input type="checkbox"/> All Traffic	ALL	--	--
<input type="checkbox"/> BGP	TCP	179	179
<input type="checkbox"/> DNS-TCP	TCP	53	53
<input type="checkbox"/> DNS-UDP	UDP	53	53
<input type="checkbox"/> ESP	IP	50	--
<input type="checkbox"/> FTP	TCP	21	21
<input type="checkbox"/> HTTP	TCP	80	80
<input type="checkbox"/> HTTPS	TCP	443	443
<input type="checkbox"/> ICMP Destination Unreachable	ICMP	3	--
<input type="checkbox"/> ICMP Ping Reply	ICMP	0	--
<input type="checkbox"/> ICMP Ping Request	ICMP	8	--
<input type="checkbox"/> ICMP Redirect Message	ICMP	5	--
<input type="checkbox"/> ICMP Router Advertisement	ICMP	9	--
<input type="checkbox"/> ICMP Router Solicitation	ICMP	10	--

Para adicionar um serviço, clique no *ícone de adição* e configure *Nome*, *Protocolo*, *Início da Porta/ICMP Tipo/Protocolo IP* e *Código Final/ICMP da Porta*.

Service Management

Apply Cancel Back

+ [edit] [delete] [download] [upload]

<input type="checkbox"/> RTSP-UDP	UDP	554	554
<input type="checkbox"/> SFTP	TCP	115	115
<input type="checkbox"/> SIP-TCP	TCP	5060	5060
<input type="checkbox"/> SIP-UDP	UDP	5060	5060
<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 type="checkbox"/> <input type="text"/>	TCP <input type="text"/>	1000 <input type="text"/>	1000 <input type="text"/>

Para editar um serviço, selecione uma linha e clique no *ícone de edição* para configurar os campos conforme mostrado abaixo.

