

# 端口转发通过在RV180和RV180W的日程表

## 目标

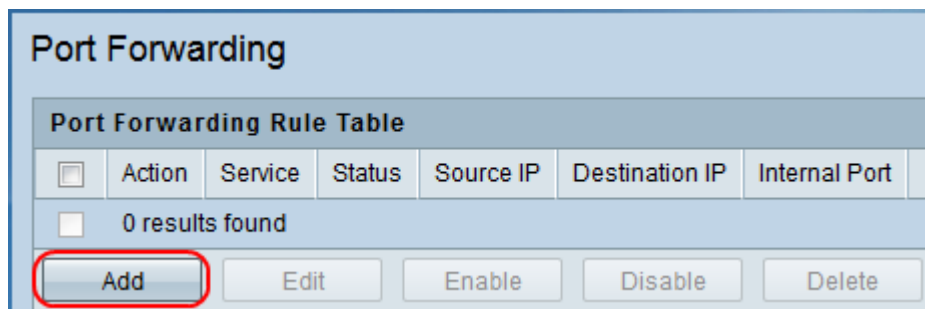
端口转发允许远程计算机(即在互联网的计算机)连接到特定计算机或服务在一个专用的局域网(LAN)内。本文解释如何允许或阻塞根据从一个端口的特定日程表的所有服务数据流在广域网对在LAN的另一个端口。条款说明用户可以根据他们的过滤规则被拒绝。日程表可以根据所有日或时刻做。允许或被拒绝的IP地址可以是指定范围或所有特定IP地址。

## 可适用的设备

- RV180
- RV180W

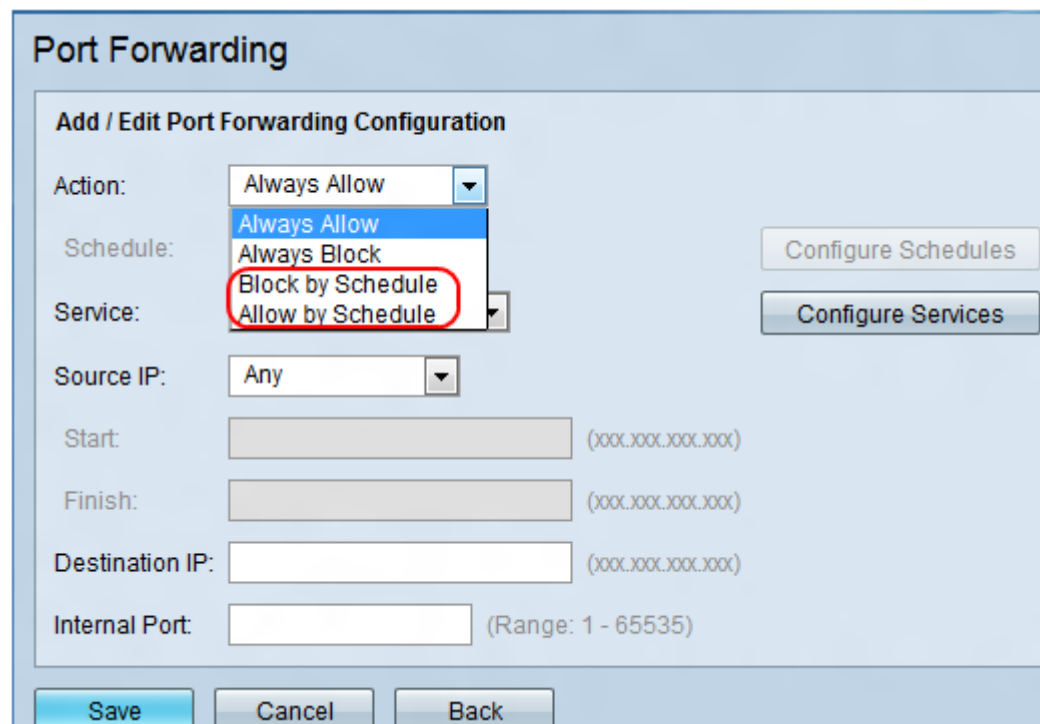
## 允许或阻拦在端口内的交通规则的步骤

第 1 步：在路由器配置工具请选择防火墙>端口转发。端口转发页打开：



The screenshot shows the 'Port Forwarding' configuration page. At the top, there is a section titled 'Port Forwarding Rule Table'. Below this, there is a table with columns: Action, Service, Status, Source IP, Destination IP, and Internal Port. Below the table, it says '0 results found'. At the bottom of the table, there are several buttons: 'Add', 'Edit', 'Enable', 'Disable', and 'Delete'. The 'Add' button is highlighted with a red circle.

步骤2.点击添加创建转发规则的端口。端口转发配置页打开：



The screenshot shows the 'Add / Edit Port Forwarding Configuration' page. The 'Action' dropdown is set to 'Always Allow'. The 'Schedule' dropdown is open, showing options: 'Always Allow', 'Always Block', 'Block by Schedule', and 'Allow by Schedule'. The 'Block by Schedule' option is highlighted with a red circle. There are also buttons for 'Configure Schedules' and 'Configure Services'. Below the dropdowns, there are input fields for 'Source IP' (set to 'Any'), 'Start', 'Finish', 'Destination IP', and 'Internal Port' (with a range of 1 - 65535). At the bottom, there are 'Save', 'Cancel', and 'Back' buttons.

步骤3.选择由日程表允许或由从动作下拉列表的日程表阻拦。

### Port Forwarding

**Add / Edit Port Forwarding Configuration**

Action:  ▾

Schedule:  ▾ Configure Schedules

Service:  ▾ Configure Services

Source IP:  ▾

Start:  (xxx.xxx.xxx.xxx)

Finish:  (xxx.xxx.xxx.xxx)

Destination IP:  (xxx.xxx.xxx.xxx)

Internal Port:  (Range: 1 - 65535)

步骤4.点击**配置**日程表定义日程表。日程表页打开：

### Schedules

These schedules can be applied to Firewall Access Rules and Port Forwarding Rules

Schedule Table				
<input type="checkbox"/>	Name	Start Time	End Time	Days
<input type="checkbox"/>	0 results found			
<span style="border: 1px solid red; border-radius: 50%; padding: 2px;">Add</span> <input type="button" value="Edit"/> <input type="button" value="Delete"/>				

步骤5.点击**添加**添加日程表。

### Schedules

**Add / Edit Schedules Configuration**

Name:

**Time**

All Day

Start Time:  :   
HH mm

End Time:  :   
HH mm

**Repeat**

Everyday

Sun  Mon  Tue  Wed  Thu  Fri  Sat

步骤6. 输入日程表名字(例如周末或假日)在名称字段。

### Schedules

**Add / Edit Schedules Configuration**

Name:

**Time**

All Day

Start Time:  :   
HH mm

End Time:  :   
HH mm

**Repeat**

Everyday

Sun  Mon  Tue  Wed  Thu  Fri  Sat

第 7 步：在时间字段下**整天**请检查(以便所有服务数据流可以被阻塞或允许整天不特定小时或分钟)或选择特定小时，并且分钟从开始计时和结束时间下拉列表。

### Schedules

**Add / Edit Schedules Configuration**

Name:

**Time**

All Day

Start Time:  :   
HH mm

End Time:  :   
HH mm

**Repeat**

Everyday

Sun  Mon  Tue  Wed  Thu  Fri  Sat

第8步。在重复字段，如果要选择日程表的，特定日请留给每天被不选定。

### Schedules

**Add / Edit Schedules Configuration**

Name:

**Time**

All Day

Start Time:  :   
HH mm

End Time:  :   
HH mm

**Repeat**

Everyday

Sun  Mon  Tue  Wed  Thu  Fri  Sat

第9步。检查对应的复选框在您要阻塞或允许服务数据流的日子。

步骤10. 点击“Save”保存日程表，并且以下页打开：

## Schedules

Operation succeeded

These schedules can be applied to Firewall Access Rules and Port Forwarding Rules

Schedule Table					
<input type="checkbox"/>	Name	Start Time	End Time	Days	
<input checked="" type="checkbox"/>	Weekend	00:00	23:59	Sunday, Saturday	

第11.步。在您实现然后点击**添加**增加规则到日程表的日程表旁边检查复选框。

## Port Forwarding

### Add / Edit Port Forwarding Configuration

Action:

Schedule:

Service:

Source IP:

Start:  (xxx.xxx.xxx.xxx)

Finish:  (xxx.xxx.xxx.xxx)

Destination IP:  (xxx.xxx.xxx.xxx)

Internal Port:  (Range: 1 - 65535)

步骤12。从日程表下拉列表选择日程表。

### Port Forwarding

**Add / Edit Port Forwarding Configuration**

Action:

Schedule:

Service:

Source IP:

Start:

Finish:

Destination IP:

Internal Port:  (Range: 1 - 65535)

AIM  
 BGP  
 BOOTP\_CLIENT  
 BOOTP\_SERVER  
 CU-SEEME:UDP  
 CU-SEEME:TCP  
 DNS:UDP  
 DNS:TCP  
 FINGER  
 FTP  
 HTTP  
 HTTPS  
 ICMP-TYPE-3  
 ICMP-TYPE-4  
 ICMP-TYPE-5  
 ICMP-TYPE-6  
 ICMP-TYPE-7  
 ICMP-TYPE-8  
 ICMP-TYPE-9  
 ICMP-TYPE-10

第13步。从服务下拉列表选择服务。

### Port Forwarding

**Add / Edit Port Forwarding Configuration**

Action:

Schedule:

Service:

Source IP:

Start:

Finish:

Destination IP:

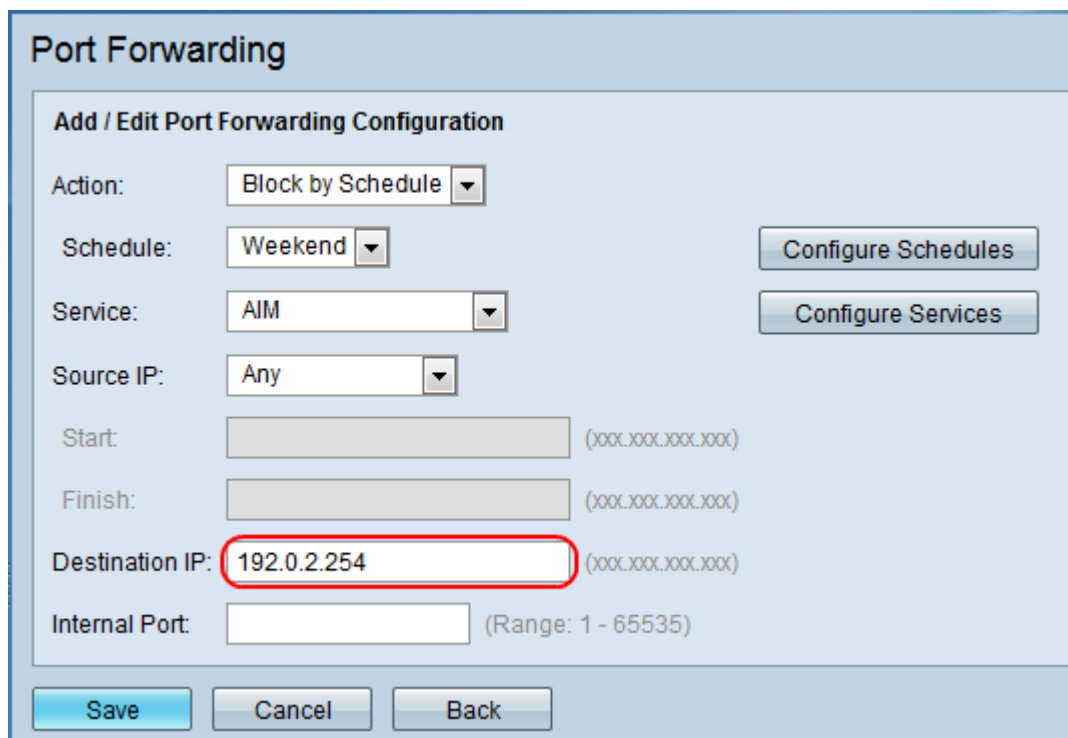
Internal Port:  (Range: 1 - 65535)

Any  
 Single Address  
 Address Range

步骤14。从来源IP下拉列表选择选项。

- 其中任一——规则适用于起源从所有IP地址于本地网络的数据流。
- 单个地址——规则适用于起源从单个IP地址于本地网络的数据流。在Start字段输入地址。

•地址范围—规则适用于起源的数据流从位于地址范围的IP地址。输入开始的IP地址在Start字段和结束IP地址在Finish字段。



**Port Forwarding**

**Add / Edit Port Forwarding Configuration**

Action:

Schedule:

Service:

Source IP:

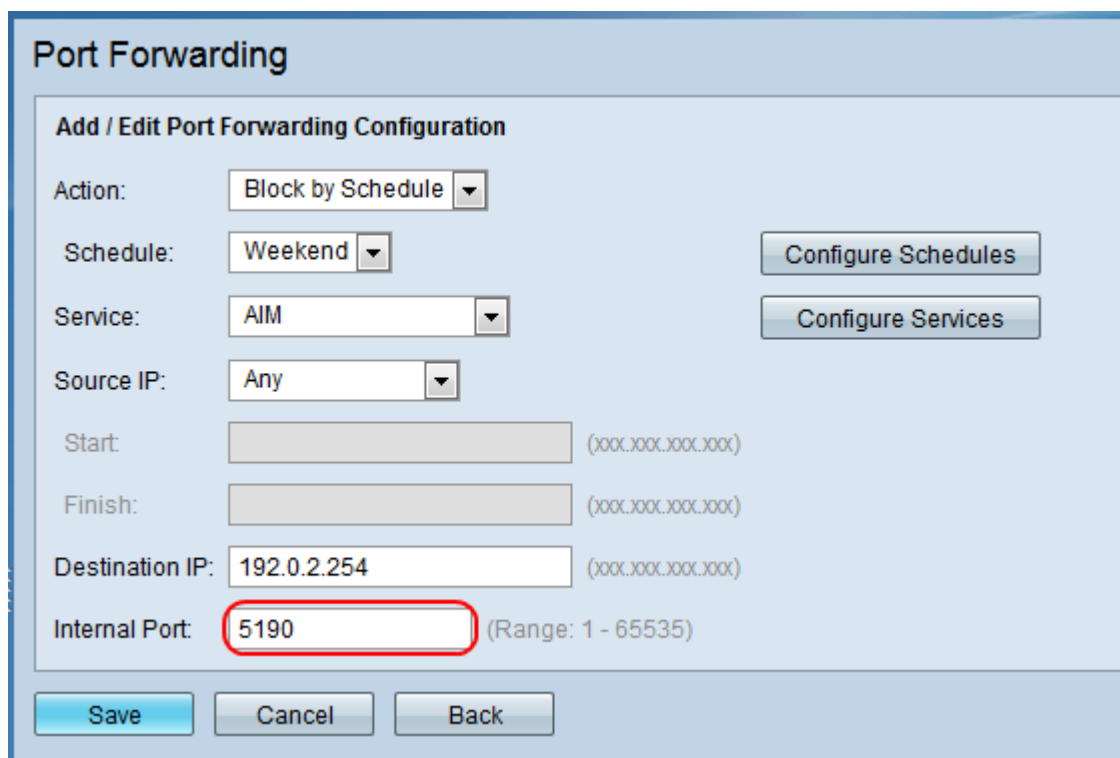
Start:  (xxx.xxx.xxx.xxx)

Finish:  (xxx.xxx.xxx.xxx)

Destination IP:  (xxx.xxx.xxx.xxx)

Internal Port:  (Range: 1 - 65535)

第15步。输入目的地IP地址在应该发送满足规则的数据流的目的地IP字段。



**Port Forwarding**

**Add / Edit Port Forwarding Configuration**

Action:

Schedule:

Service:

Source IP:

Start:  (xxx.xxx.xxx.xxx)

Finish:  (xxx.xxx.xxx.xxx)

Destination IP:  (xxx.xxx.xxx.xxx)

Internal Port:  (Range: 1 - 65535)

第16步。在内部Port字段输入端口号对应该转发哪数据流。

第17步。点击“Save”保存端口转发规则。