

在RV0xx上允许或阻止IPv6中的服务流量

目标

本文档介绍如果请求来自特定计算机，如何根据特定计划允许或阻止任何服务流量。本文解释可以根据IP地址拒绝用户。可以根据任何一天或时间制定时间表。允许或拒绝的IP地址可以是特定范围或任何特定IP地址。

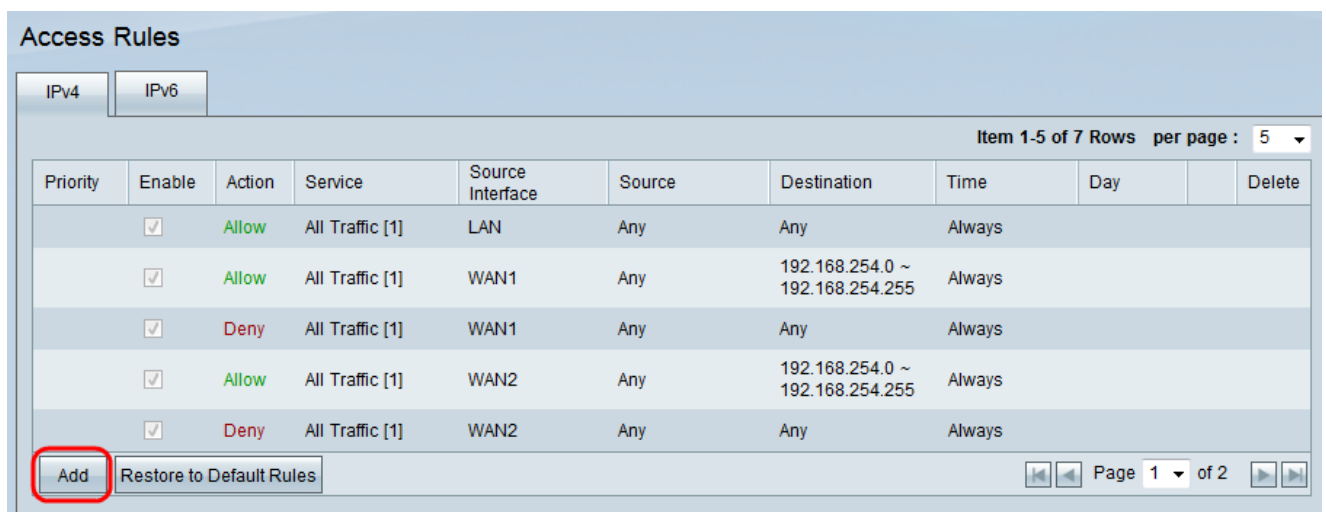
适用设备

- RV016
- RV082
- RV042
- RV042G

允许或阻止服务流量的步骤

配置服务的步骤

步骤1:登录路由器配置实用程序并选择Firewall > Access Rules。Access Rules页面打开：



The screenshot shows the 'Access Rules' configuration page for IPv6. The page has tabs for 'IPv4' and 'IPv6', with 'IPv6' selected. The table below lists the current rules:

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Delete
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	WAN1	Any	192.168.254.0 ~ 192.168.254.255	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always		
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	WAN2	Any	192.168.254.0 ~ 192.168.254.255	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always		

At the bottom left, there is an 'Add' button (highlighted with a red circle) and a 'Restore to Default Rules' button. The bottom right shows navigation controls and 'Page 1 of 2'.

第二步：单击Add以创建服务流量计划。将打开访问规则页面：

Access Rules

Services

Action :

Service :
 [TCP&UDP/1~65535]

Log :

Source Interface :

Source IP :

Destination IP :

Scheduling

Time :

From : (hh:mm) To : (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

第三步：在Action下拉列表中，选择Allow以允许流量跟随，或选择Deny以阻止流量。

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP :

Scheduling

Time :

From : (hh:mm)

Effective on : Ev Mon Tue Wed Thu Fri Sat

- All Traffic [TCP&UDP/1~65535]
- DNS [UDP/53~53]
- FTP [TCP/21~21]
- HTTP [TCP/80~80]
- HTTP Secondary [TCP/8080~8080]
- HTTPS [TCP/443~443]
- HTTPS Secondary [TCP/8443~8443]
- TFTP [UDP/69~69]
- IMAP [TCP/143~143]
- NNTP [TCP/119~119]
- POP3 [TCP/110~110]
- SNMP [UDP/161~161]
- SMTP [TCP/25~25]
- TELNET [TCP/23~23]
- TELNET Secondary [TCP/8023~8023]
- TELNET SSL [TCP/992~992]
- DHCP [UDP/67~67]
- L2TP [UDP/1701~1701]
- PPTP [TCP/1723~1723]
- IPSec [UDP/500~500]

第四步：从服务(Service)下拉列表中选择服务。

注意：如果服务下拉列表中未提及特定服务，请点击服务管理(Service Management)。

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP :

Scheduling

Time :

From : (hh:mm) To : (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

第五步：从日志下拉列表中选择一个选项。

·记录与此规则匹配的数据包 — 记录与访问规则匹配的传入数据包。

·不记录 — 不记录与访问规则匹配的传入数据包。

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP :

Scheduling

Time :

From : (hh:mm) To : (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

第六步：从Source Interface下拉列表中选择一个接口。源接口是从中发起流量的接口。

- LAN — 局域网。它将计算机紧密连接到网络（例如办公大楼或学校）中。
- WAN1 — 广域网。这可以连接网络中大面积的计算机。这可以是连接一个地区甚至一个国家的任何网络。企业和政府用它来连接其他位置。
- WAN2 — 与WAN1相同，只是它是第二个网络。
- DMZ — 允许外部流量访问网络上的计算机，而不暴露局域网。
- ANY — 允许使用任何接口。

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP :

Scheduling

Time :

From : (hh:mm) To : (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

步骤 7.从Source IP下拉列表中选择一个选项来指定源IP地址。

- Any — 任何IP地址都将用于转发流量。下拉列表右侧没有任何字段可用。
- 单一 — 使用单个IP地址转发流量。在下拉列表右侧的字段中输入所需的IP地址。
- 范围 — 范围IP地址将用于转发流量。在下拉列表右侧的字段中输入所需的IP地址范围。

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP :

Scheduling

Time :

From : (hh:mm) To : (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

步骤 8从Destination IP下拉列表中选择一个选项来指定目标IP地址。

- Any — 任何IP地址都将用于转发流量。下拉列表右侧没有任何字段可用。
- 单一 — 使用单个IP地址转发流量。在下拉列表右侧的字段中输入所需的IP地址。
- 范围 — 范围IP地址将用于转发流量。在下拉列表右侧的字段中输入所需的IP地址范围。

配置调度的步骤

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP :

Scheduling

Time :

From :
 (hh:mm) To : (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

步骤1:从时间(Time)下拉列表中选择时间选项。

·始终 — 此选项将允许或阻止您的服务流量在整个一周内传输。

·时间间隔 — 此选项将允许或阻止您的服务流量在特定日期或特定时间某天。

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP :

Scheduling

Time :

From : (hh:mm) To : (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

第二步：在From字段和To字段中输入特定时间，以指定允许或阻止服务流量的时间。

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP :

Scheduling

Time :

From : (hh:mm) To : (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

第三步：保持日常复选框处于默认选中状态，以允许或阻止服务流量在每天的特定时间，或取消选中日常复选框以选择要允许或阻止服务流量的天数。

第四步：单击Save以保存配置的访问规则。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。