

在RV130和RV130W上添加和配置访问规则

目标

网络设备通过访问规则提供基本的流量过滤功能。访问规则是访问控制列表(ACL)中的单个条目，根据协议、源和目标IP地址或网络配置指定允许或拒绝规则（转发或丢弃数据包）。

本文档旨在向您展示如何在RV130和RV130W上添加和配置访问规则。

适用设备

- RV130
- RV130W

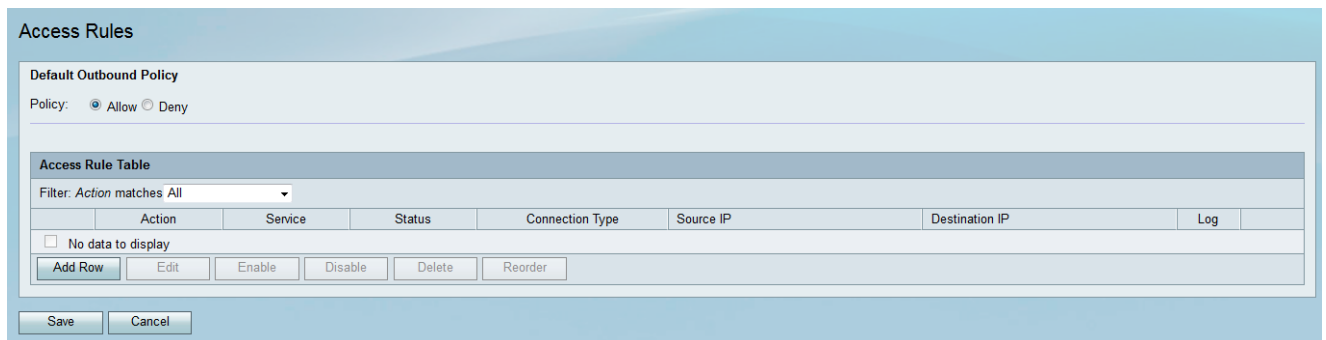
软件版本

- 1.0.1.3 版

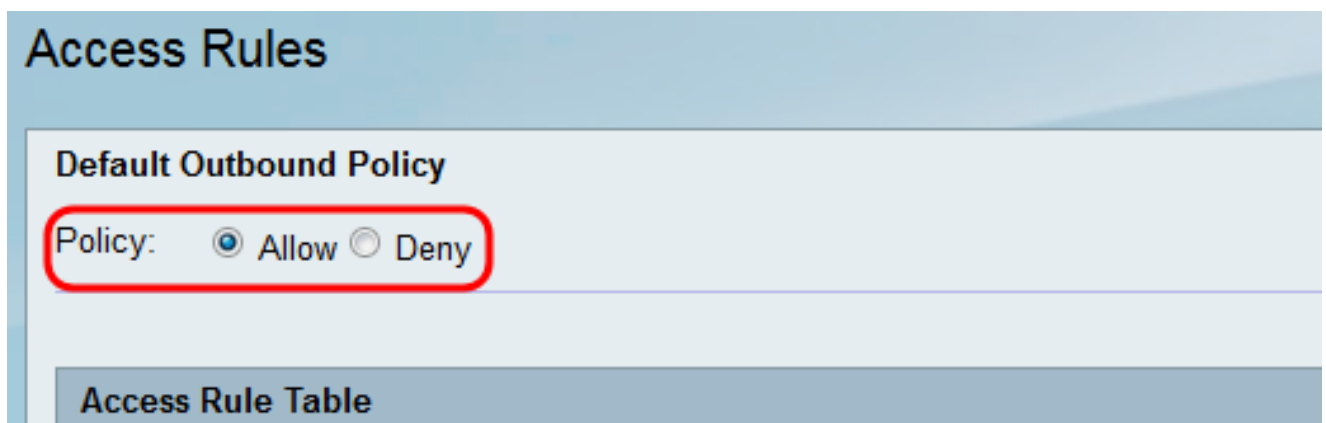
添加和配置访问规则

设置默认出站策略

步骤1.登录Web配置实用程序，然后选择Firewall > Access Rules。“访问规则”页打开：



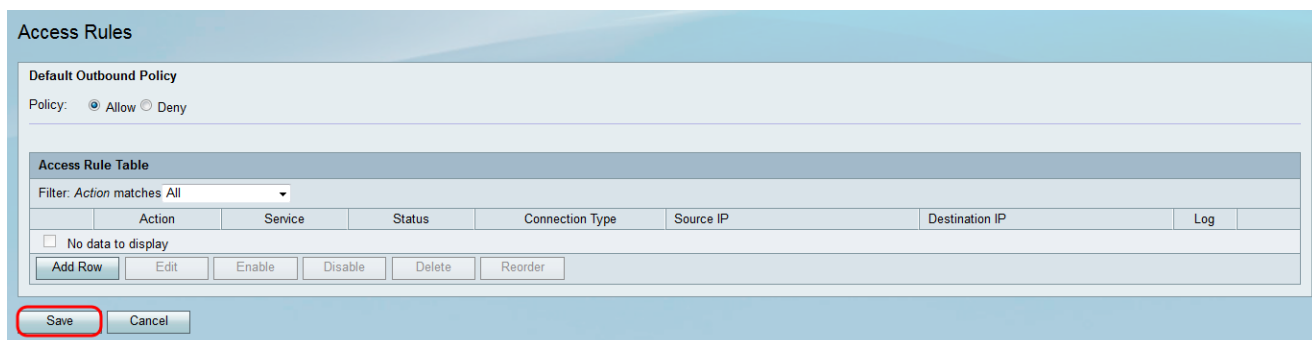
步骤2.在Default Outbound Policy区域中，单击所需的单选按钮以选择出站流量的策略。当未配置访问规则或互联网访问策略时，会应用该策略。默认设置为**Allow**，它允许所有到Internet的流量通过。



可用选项定义如下：

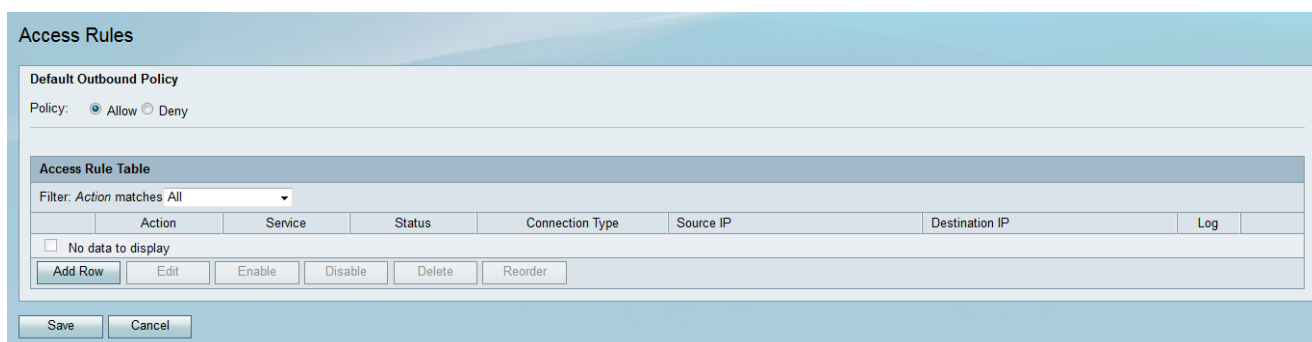
- 允许 — 允许所有类型的流量从LAN流向Internet。
- 拒绝 — 阻止从LAN传出到Internet的所有类型的流量。

步骤3.单击“保存”保存设置。

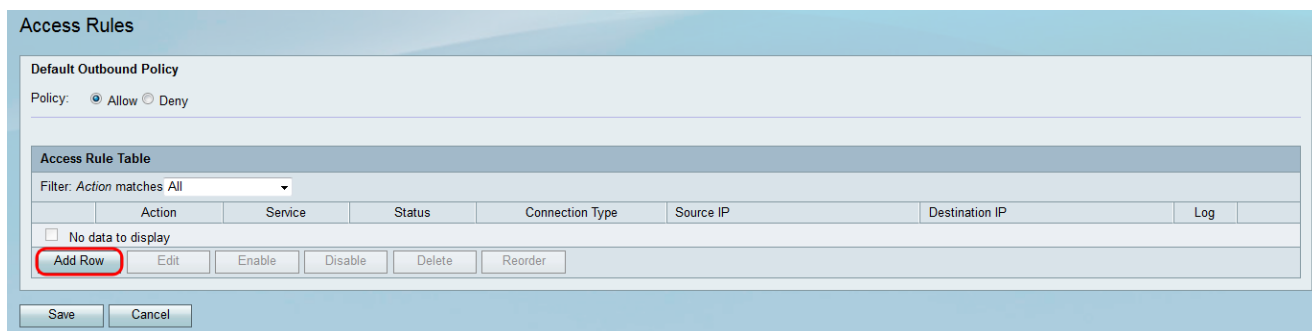


添加访问规则

步骤1.登录Web配置实用程序，然后选择Firewall > Access Rules。“访问规则”窗口打开：



步骤2.单击“访问规则表”中的“添加行”以添加新的访问规则。



系统将打开“添加访问规则”页：

Add Access Rule

Connection Type: Outbound (LAN > WAN) ▾

Action: Always block ▾

Schedule: ▾

Services: All Traffic ▾

Source IP: Any ▾

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status: Enable

步骤3.从Connection Type下拉列表中，选择应用规则的流量类型。

Connection Type: Outbound (LAN > WAN) ▾
Outbound (LAN > WAN)
Inbound (WAN > LAN)
Inbound (WAN > DMZ)

Action:

Schedule: ▾

Services: All Traffic ▾

Source IP: Any ▾

Start:

Finish:

可用选项定义如下：

- 出站(LAN > WAN) — 该规则影响来自本地网络(LAN)和外出到互联网(WAN)的数据包。
- 入站(WAN > LAN) — 该规则影响来自Internet(WAN)并进入本地网络(LAN)的数据包。
- 入站(WAN > DMZ) — 该规则影响来自互联网(WAN)并进入隔离区(DMZ)子网的数据包。

步骤4.从Action下拉列表中，选择匹配规则时要采取的操作。

Connection Type: Outbound (LAN > WAN) ▾

Action: Always block ▾

Schedule: ▾

Services: ▾

Source IP: Any ▾

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status: Enable

可用选项定义如下：

- 始终阻止 — 如果条件匹配，则始终拒绝访问。跳至步骤6。
- 始终允许 — 如果条件匹配，始终允许访问。跳至步骤6。
- 按计划阻止 — 如果条件在预配置计划期间匹配，则拒绝访问。
- 按计划允许 — 如果条件在预配置计划期间匹配，则允许访问。

步骤5.如果在步骤4中**选择按计划阻止或按计划允许**，请从“计划”下拉列表中选择适当的计划。

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: ▾

Source IP: Any ▾

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status: Enable

注意：要创建或编辑计划，请单击“配置计划”。有关详细[信息和指南](#)，请参阅在RV130和RV130W上配置时间表。

步骤6.从“服务”下拉列表中选择访问规则应用的服务类型。

The screenshot shows a configuration page for a firewall rule. The 'Services' dropdown menu is open, displaying a list of service types. The 'All Traffic' option is highlighted in blue. The list includes: All Traffic, DNS, FTP, HTTP, HTTP Secondary, HTTPS, HTTPS Secondary, TFTP, IMAP, NNTP, POP3, SNMP, SMTP, TELNET, TELNET Secondary, TELNET SSL, and Voice(SIP). Other fields on the page include 'Connection Type' (Outbound (LAN > WAN)), 'Action' (Allow by schedule), 'Schedule' (test_schedule), 'Source IP', 'Start' and 'Finish' times for HTTP, HTTPS, and SMTP, and 'Destination IP'.

注意：如果要添加或编辑服务，请单击“配置服务”。有关详细信息和指南，请参阅[RV130和RV130W上的服务管理配置](#)。

配置出站流量的源和目标IP

如果在添加访问规则的步骤3中选择了出站(LAN > WAN)作为连接类型，请执行本[节中的步骤](#)。

注意：如果在添加访问规则的步骤3中选择了入站连接类型，请跳至下一节：[配置入站流量的源和目标IP](#)。

步骤1.从Source IP下拉列表中选择要如何定义Source IP。对于出站流量，源IP是指防火墙规则将应用到的地址或地址（在LAN中）。

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Any ▾
Any
Single Address
Address Range

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status: Enable

可用选项定义如下：

- 任意 — 适用于源自本地网络中任何IP地址的流量。因此，将“开始”和“完成”字段留空。如果选择此选项，请跳至步骤4。
- 单个地址 — 适用于源自本地网络中单个IP地址的流量。在“开始”字段中输入IP地址。
- 地址范围 — 适用于源自本地网络中IP地址范围的流量。在“开始”字段中输入范围的起始IP地址，在“完成”字段中输入结束IP地址，以设置范围。

步骤2.如果在步骤1中选择**Single Address**，请在Start 字段中输入将应用于访问规则的IP地址，然后跳至步骤4。如果在步骤1中选择**Address Range**，请在“Start ”字段中输入将应用于访问规则的起始IP地址。

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Single Address ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status: Enable

步骤3.如果在步骤1中**选择了Address Range**，请在Finish字段中输入将封装访问规则的IP地址范围的结束IP地址。

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Address Range ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: 10.10.14.175 (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status: Enable

步骤4.从目标IP下拉列表中选择要如何定义目标IP。对于出站流量，目标IP是指允许或拒绝来自本地网络的流量的地址或地址（在WAN中）。

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Address Range ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: 10.10.14.175 (Hint: 192.168.1.200)

Destination IP: Any ▾

Start: Any

Finish: Single Address

Address Range

Log: Never ▾

Rule Status: Enable

可用选项定义如下：

- 任意 — 适用于流向公共互联网中任何IP地址的流量。因此，将“开始”和“完成”字段留空。
- 单个地址 — 适用于流向公共Internet中单个IP地址的流量。在“开始”字段中输入IP地址。
- 地址范围 — 适用于流向公有Internet中的IP地址范围的流量。在“开始”字段中输入范围的起始IP地址，在“完成”字段中输入结束IP地址，以设置范围。

步骤5.如果在步骤4中选择了单个地址，请在“开始”字段中输入将应用于访问规则的IP地址。如果在步骤4中选择地址范围，请在开始字段中输入将应用于访问规则的起始IP地址。

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Address Range ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: 10.10.14.175 (Hint: 192.168.1.200)

Destination IP: Single Address ▾

Start: 192.168.1.100

Finish:

Log: Never ▾

Rule Status: Enable

步骤6.如果在步骤4中选择了Address Range，请在Finish字段中输入将封装访问规则的IP地址范围的结束IP地址。

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Address Range ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: 10.10.14.175 (Hint: 192.168.1.200)

Destination IP: Address Range ▾

Start: 192.168.1.100

Finish: 192.168.1.170

Log: Never ▾

Rule Status: Enable

配置入站流量的源和目标IP

如果在添加访问规则的步骤3中选择入站(WAN > LAN)或入站(WAN > DMZ)作为连接类型，请执行本节中的步骤。

步骤1.从Source IP下拉列表中选择要如何定义Source IP。对于入站流量，源IP是指防火墙规则将应用到的地址或地址（在WAN中）。

Connection Type: Inbound (WAN > LAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: All Traffic ▾

Source IP: Any ▾
Any
Single Address
Address Range

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status: Enable

可用选项定义如下：

·任意 — 适用于来自公共Internet中任何IP地址的流量。因此，将“开始”和“完成”字段留空。如果选择此选项，请跳至步骤4。

·单个地址 — 适用于从公共Internet中的单个IP地址发起的流量。在“开始”字段中输入IP地址。

·地址范围 — 适用于源自公共Internet中IP地址范围的流量。在“开始”字段中输入范围的起始IP地址，在“完成”字段中输入结束IP地址，以设置范围。

步骤2.如果在步骤1中选择**Single Address**，请在Start 字段中输入将应用于访问规则的IP地址，然后跳至步骤4。如果在步骤1中选择了**Address Range**，请在“Start”字段中输入将应用于访问规则的起始IP地址。

Connection Type: Inbound (WAN > LAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: All Traffic ▾

Source IP: Address Range ▾

Start: 192.168.1.100 (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP: Single Address ▾

Start:

Finish:

Log: Never ▾

Rule Status: Enable

步骤3.如果在步骤1中选择了Address Range，请在Finish字段中输入将封装访问规则的IP地址范围的结束IP地址。

Connection Type: Inbound (WAN > LAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: All Traffic ▾

Source IP: Address Range ▾

Start: 192.168.1.100 (Hint: 192.168.1.100)

Finish: 192.168.1.200 (Hint: 192.168.1.200)

Destination IP: Single Address ▾

Start:

Finish:

Log: Never ▾

Rule Status: Enable

步骤4.在Destination IP下拉列表下方的Start字段中，为Destination IP输入Single Address。对于入站流量，目标IP是指允许或拒绝来自公共互联网的流量的地址（在LAN中）。

Connection Type: Inbound (WAN > LAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: All Traffic ▾

Source IP: Address Range ▾

Start: 192.168.1.100 (Hint: 192.168.1.100)

Finish: 192.168.1.200 (Hint: 192.168.1.200)

Destination IP: Single Address ▾

Start: 10.10.14.2

Finish:

Log: Never ▾

Rule Status: Enable

注意：如果在添加访问规则步骤3中选择 *Inbound(WAN > DMZ)* 作为连接类型，则目标IP的 Single Address 会自动配置已启用DMZ主机的IP地址。

记录和启用访问规则

步骤1. 如果希望路由器在数据包与规则匹配时创建日志，请在“Log”下拉列表中选择“Always”。如果希望在规则匹配时永远不会发生日志记录，请选择“从不”。

Start: 192.168.1.100

Finish: 192.168.1.170

Log: ▾
Never
Always

Rule Status: Enable

步骤2. 选中Enable复选框以启用访问规则。

Add Access Rule

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Address Range ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: 10.10.14.175 (Hint: 192.168.1.200)

Destination IP: Address Range ▾

Start: 192.168.1.100

Finish: 192.168.1.170

Log: Never ▾

Rule Status: Enable

步骤3.单击“保存”保存设置。

Add Access Rule

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Address Range ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: 10.10.14.175 (Hint: 192.168.1.200)

Destination IP: Address Range ▾

Start: 192.168.1.100

Finish: 192.168.1.170

Log: Never ▾

Rule Status: Enable

访问规则表将使用新配置的访问规则进行更新。

Access Rules



Configuration settings have been saved successfully

Default Outbound Policy

Policy: Allow Deny

Access Rule Table

Filter: Action matches All

	Action	Service	Status	Connection Type	Source IP	Destination IP	Log
<input type="checkbox"/>	Allow by schedule	VOIP	Enabled	Outbound (LAN > WAN)	10.10.14.100 ~ 10.10.14.175	192.168.1.100 ~ 192.168.1.170	Never