

RV215W上的访问规则配置

目标

RV215W允许配置访问规则以提高安全性。这些访问控制列表(ACL)是阻止或允许某些用户发送或发送流量的列表。它们可以配置为始终有效或基于定义的计划。

本文介绍如何在RV215W上配置访问规则。

适用设备

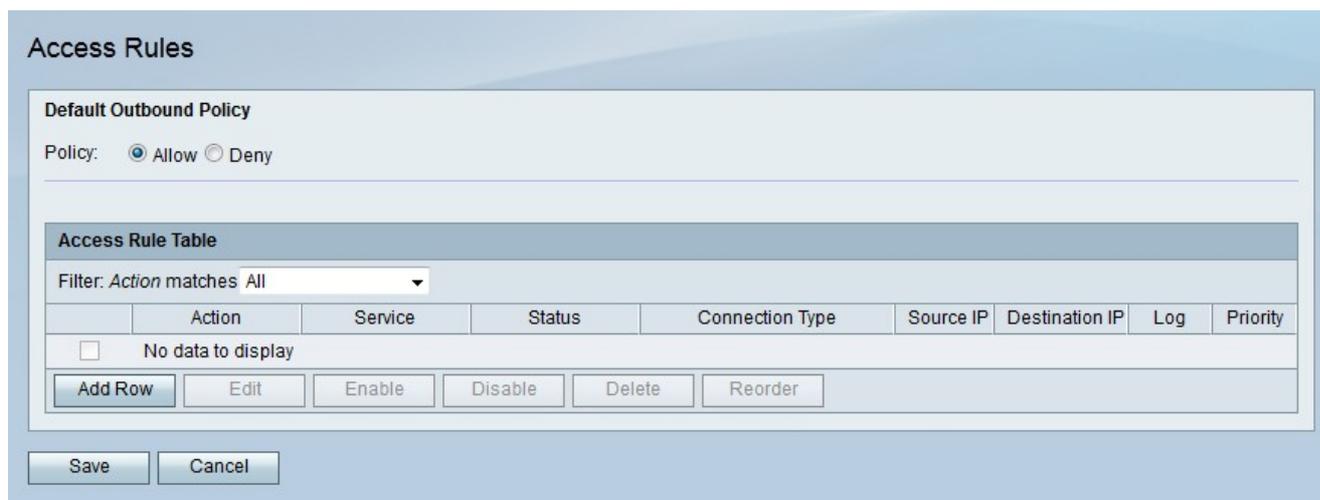
·RV215W

软件版本

·1.1.0.5

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”页打开：



Access Rules

Default Outbound Policy

Policy: Allow Deny

Access Rule Table

Filter: Action matches All

Action	Service	Status	Connection Type	Source IP	Destination IP	Log	Priority
No data to display							

No data to display

Add Row Edit Enable Disable Delete Reorder

Save Cancel

步骤2.点击与Policy字段中所需的默认出站策略对应的单选按钮。默认出站策略确定是允许还是拒绝出站流量。当没有为用户的IP地址配置访问规则或互联网访问策略时，会使用它。

步骤3.单击“保存”。

添加访问规则

步骤1.单击Add Row以添加新访问规则。系统将打开“添加访问规则”页：

Add Access Rule

Connection Type: Outbound (LAN > WAN) ▼

Action: Always block ▼

Schedule: Schedule1 ▼

Services: All Traffic ▼

Source IP: Single Address ▼

Start: 192.168.1.100 (Hint: 192.168.1.100 or fec0::64)

Finish: (Hint: 192.168.1.200 or fec0::c8)

Destination IP: Address Range ▼

Start: 192.168.15.1

Finish: 192.168.15.254

Log: Never ▼

QoS Priority: 1 (lowest) ▼

Rule Status: Enable

步骤2.从Connection Type下拉列表中选择要创建的规则类型。

- 出站(LAN > WAN) — 该规则影响来自安全LAN并转到不安全WAN的数据包。
- 入站(WAN > LAN) — 该规则影响来自不安全WAN并转到安全LAN的数据包。
- 入站(WAN > DMZ) — 该规则影响来自不安全WAN并进入DMZ的数据包。DMZ是将LAN与WAN分隔开来的网段，可提供更高的安全层。

步骤3.从Action下拉列表中选择要应用到规则的操作。

- 始终阻止 — 始终阻止数据包。
- 始终允许 — 始终允许数据包。
- 按计划阻止 — 根据指定的计划阻止数据包。
- 按计划允许 — 根据指定的计划允许数据包。

步骤4.从Schedule下拉列表中选择要应用于规则的计划。

步骤5.从Services下拉列表中选择要允许或阻止的服务。

注意：单击**Configure Services**以在Service Management页上配置计划。

步骤6.从Source IP下拉列表中，选择规则阻止或允许数据包发往的源IP地址。

- 任意 — 规则适用于所有源IP地址。

·单个地址 — 在“开始”字段中输入规则应用到的单个IP地址。

·地址范围 — 在“开始”和“完成”字段中输入规则应用到的IP地址范围。

步骤7.从Destination IP下拉列表中，选择规则阻止或允许数据包到达的目标IP地址。

·任意 — 规则适用于所有目标IP地址。

·单个地址 — 在“开始”字段中输入规则应用到的单个IP地址。

·地址范围 — 在“开始”和“完成”字段中输入规则应用到的IP地址范围。

步骤8.从Log下拉列表中选择日志选项。日志是生成的系统记录，用于安全管理。

·从不 — 禁用日志。

·始终 — 每当数据包与规则匹配时，RV215W都会创建日志。

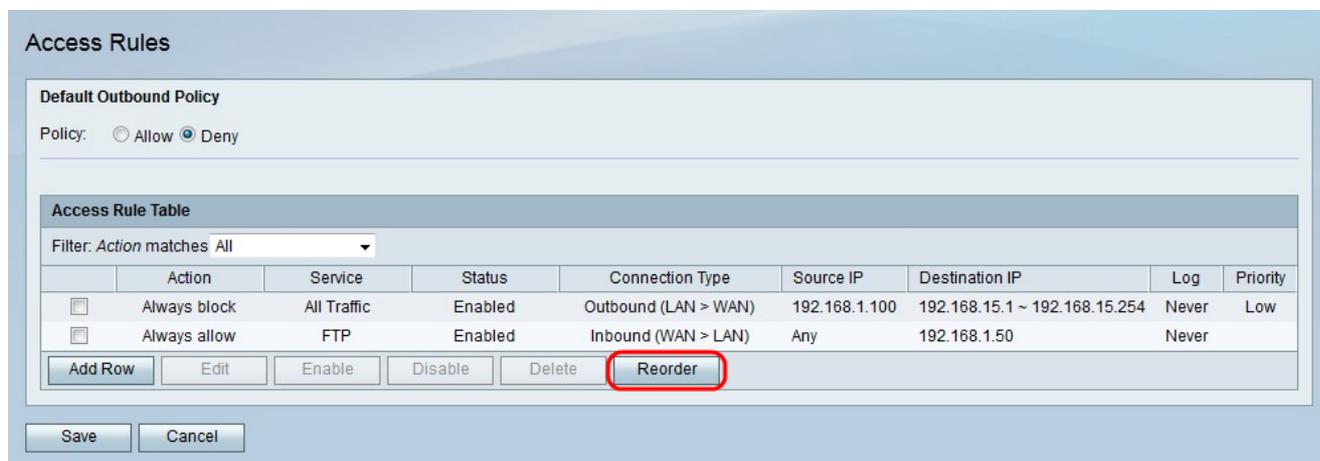
步骤9.从QoS优先级下拉列表中为规则的出站IP数据包选择优先级。优先级1最低，优先级4最高。优先级较高的队列中的数据包将先于优先级较低的队列发送。

步骤10.在Rule Status字段中选中**Enable**以启用该规则。

步骤11.单击“保存”。

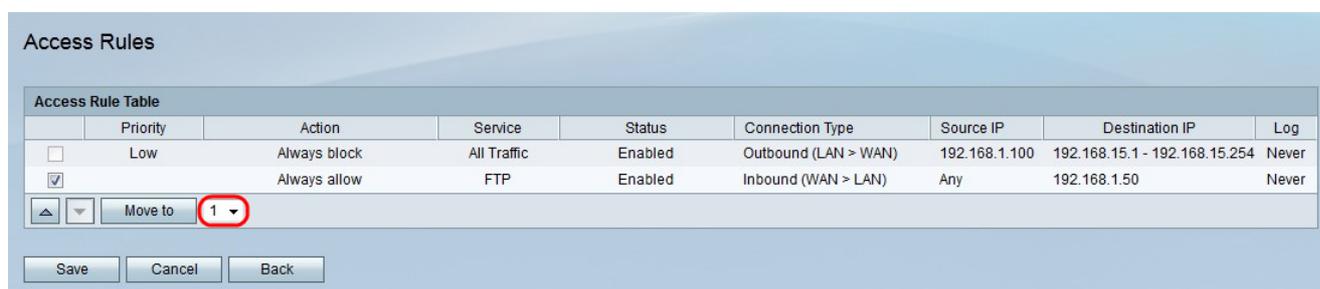
重新排序访问规则

重新排序功能是RV215W的重要选项。访问规则在访问规则表中显示的顺序指示应用规则的顺序。表中的第一个规则是要应用的第一个规则。



步骤1.单击“重新排序”对访问规则重新排序。

步骤2.选中要重新排序的访问规则框。



步骤3.从下拉列表中选择要将指定规则移动到的位置。

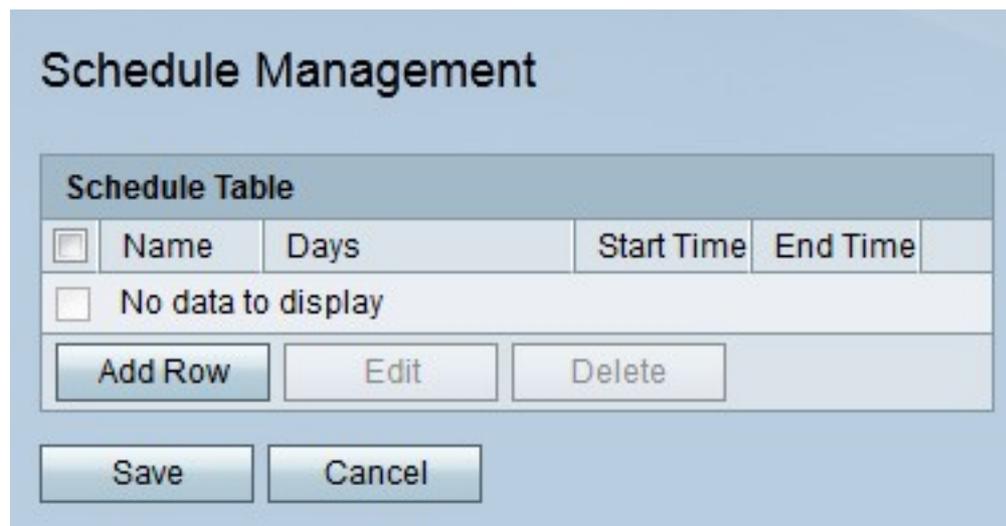
步骤4.单击“移动至”对规则重新排序。规则将移至表中的指定位置。

注意：向上和向下箭头按钮也可用于重新排序访问规则。

步骤5.单击Save。

安排管理配置

步骤1.登录Web配置实用程序，然后选择Firewall > Schedule Management。此时将打开“计划管理”页：



Schedule Table				
<input type="checkbox"/>	Name	Days	Start Time	End Time
<input type="checkbox"/>	No data to display			

步骤2.单击Add Row 以添加新计划。此时将打开“添加/编辑计划”页：

Add/Edit Schedules

Add/Edit Schedules Configuration

Name:

Scheduled Days

Do you want this schedule to be active on all days or specific days?

▼

Monday:

Tuesday:

Wednesday:

Thursday:

Friday:

Saturday:

Sunday:

Scheduled Time of Day

Do you want this schedule to be active on all days or at specific times during the day?

▼

Start time: Hours Minutes

End time: Hours Minutes

Save

Cancel

Back

步骤3.在Name字段中输入计划的名称。

步骤4.从Scheduled Days下拉列表中选择计划处于活动状态的天数。

- All Days — 计划在一周中的每一天都处于活动状态。
- Specific Days — 选中计划处于活动状态的天数复选框。

步骤5.从Scheduled Time of Day下拉列表中选择计划处于活动状态的时间。

- 所有时间 — 计划在一天中的所有时间都处于活动状态。

·特定时间 — 从“开始时间”和“结束时间”下拉列表中选择计划开始时间和计划结束时间。

步骤6.单击“保存”。