访问在RV215W的规则配置

客观

RV215W允许访问规则的配置强化安全。这些访问控制列表(ACL)是阻塞或允许从被发送的数据流到/从某些用户的列表。可以实际上配置他们是一直或根据被定义的日程表。

此条款说明如何配置在RV215W的访问规则。

可适用的设备

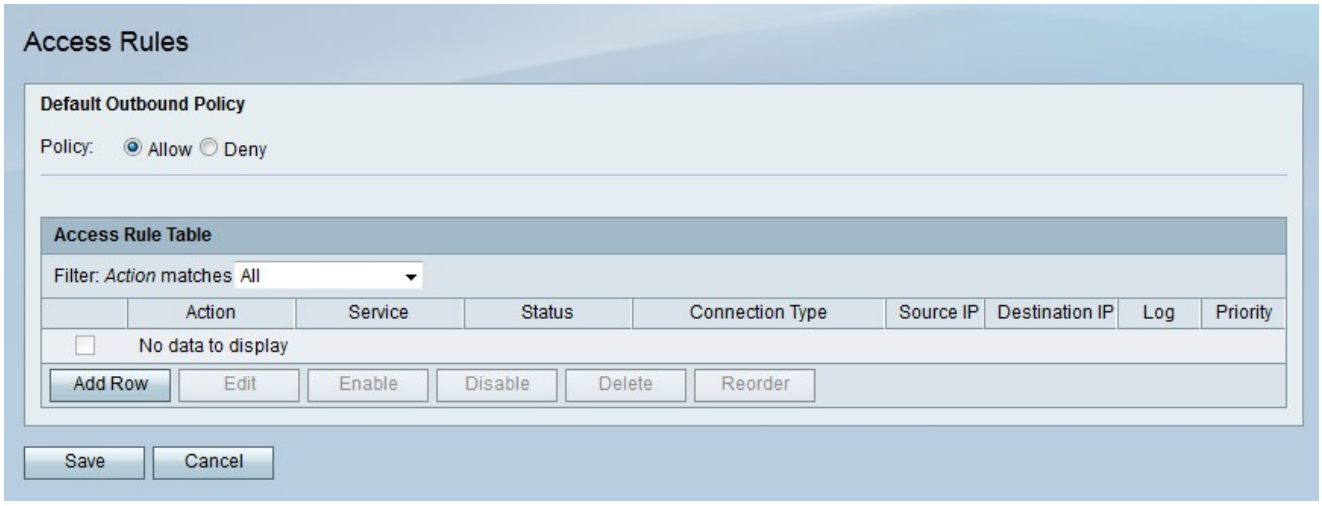
•RV215W

软件版本

•1.1.0.5

访问规则

步骤1.登陆到Web配置工具并且选择**防火墙>Access规则**。*访问规则*页打开：

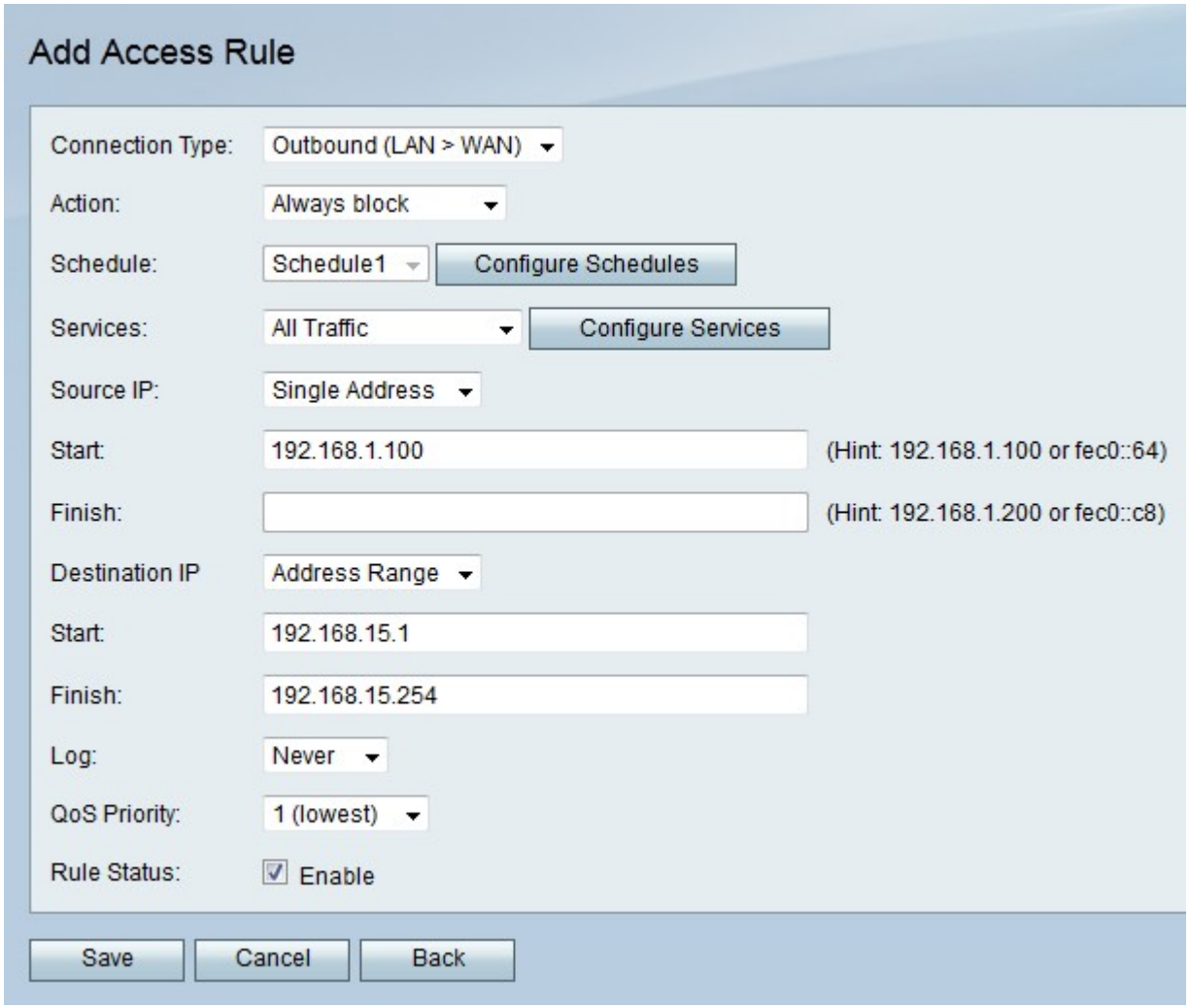


步骤2.点击对应于在Policy字段的期望默认出局策略的单选按钮。默认出局策略确定出局流量是否允许或被否决。使用它，每当没有访问规则或互联网访问策略被配置对用户的IP地址。

步骤3.点击**"Save"**。

增加访问规则

步骤1.点击**Add行**增加一个新的访问规则。添加访问规则页打开：



Step 2.从连接类型下拉列表请选择规则的种类创建。

- outbound (LAN >广域网) —规则影响来自安全的LAN并且去不安全的广域网的信息包。
- 入站(广域网> LAN) —规则影响来自不安全的广域网并且去获取LAN的信息包。
- 入站(广域网> DMZ) —规则影响来自不安全的广域网并且去DMZ的信息包。DMZ是从广域网分离LAN提供安全一个被添加的层的网段。

第3.步。从动作下拉列表请选择将适用于规则的动作。

- 总是块—总是阻拦信息包。
- 总是请准许—总是允许信息包。
- 由日程表的块—根据一个指定的日程表的阻拦信息包。
- 由日程表允许—允许根据一个指定的日程表的信息包。

第4.步。从日程表下拉列表请选择日程表适用于规则。

第5.步。从服务下拉列表请选择服务准许或阻拦。

Note:点击**配置服务**配置在*服务管理*页的日程表。

第6.步。从来源IP下拉列表请选择规则阻拦或允许信息包自的IP原地址。

- 其中任一—规则适用于所有IP原地址。

•单个地址—输入规则在Start字段适用的单个IP地址。

•地址范围—输入规则适用于在启动和完成字段IP地址的范围。

第7.步。从目的地IP下拉列表请选择规则阻拦或允许信息包的目的地IP地址。

•其中任一—规则适用于所有目的地IP地址。

•单个地址—输入规则适用于在Start字段的单个IP地址。

•地址范围—输入规则适用于在启动和完成字段IP地址的范围。

第8.步。从日志下拉列表请选择日志选项。日志是使用安全管理的生成的系统记录。

•从未—功能失效日志。

•总是— RV215W创建一本日志，每当信息包匹配规则。

第9.步。从QoS优先级下拉列表请选择规则的outbound IP信息包的优先级。当优先级四最高时，优先级一是最低的。在更加高优先级的队列的信息包在那些前将被发送在更加低优先级的队列。

第10.步。检查在规则Status字段的**Enable (event)**对enable (event)规则。

步骤11.点击**"Save"**。

重新命令访问规则

重新命令功能是在RV215W的一个重要选项。访问规定的命令在访问规则表里显示指示规则适用的命令。第一个规则在表里是将适用的第一个规则。

步骤1.点击**重新命令**重新命令访问规则。

Step 2.检查您要重新命令访问规则的机箱。

第3.步。从下拉列表请选择您要移动指定的规则向的位置。

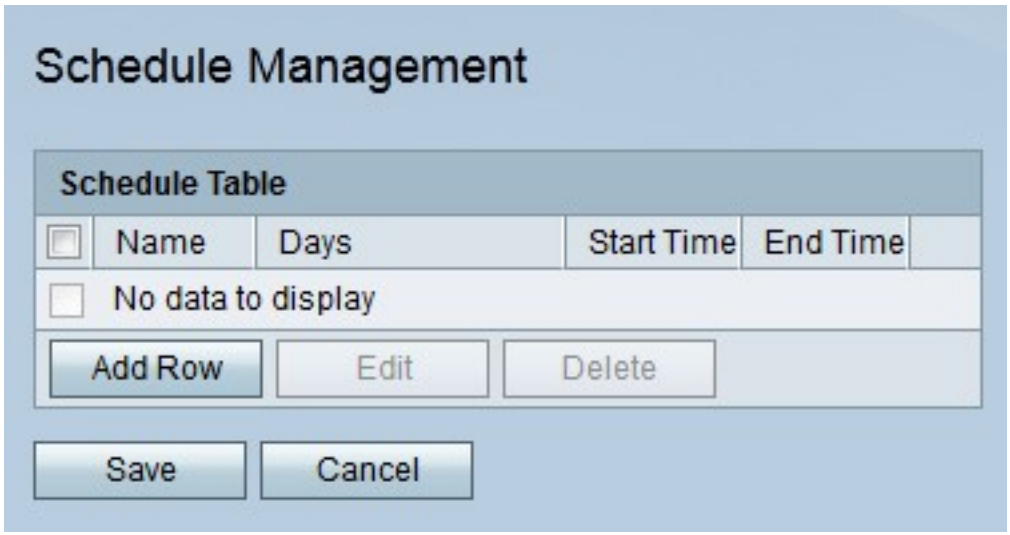
步骤4.点击**移动对**重新命令规则。规则在表里移动向指定的位置。

Note:箭头按钮可能也上上下下用于重新命令访问规则。

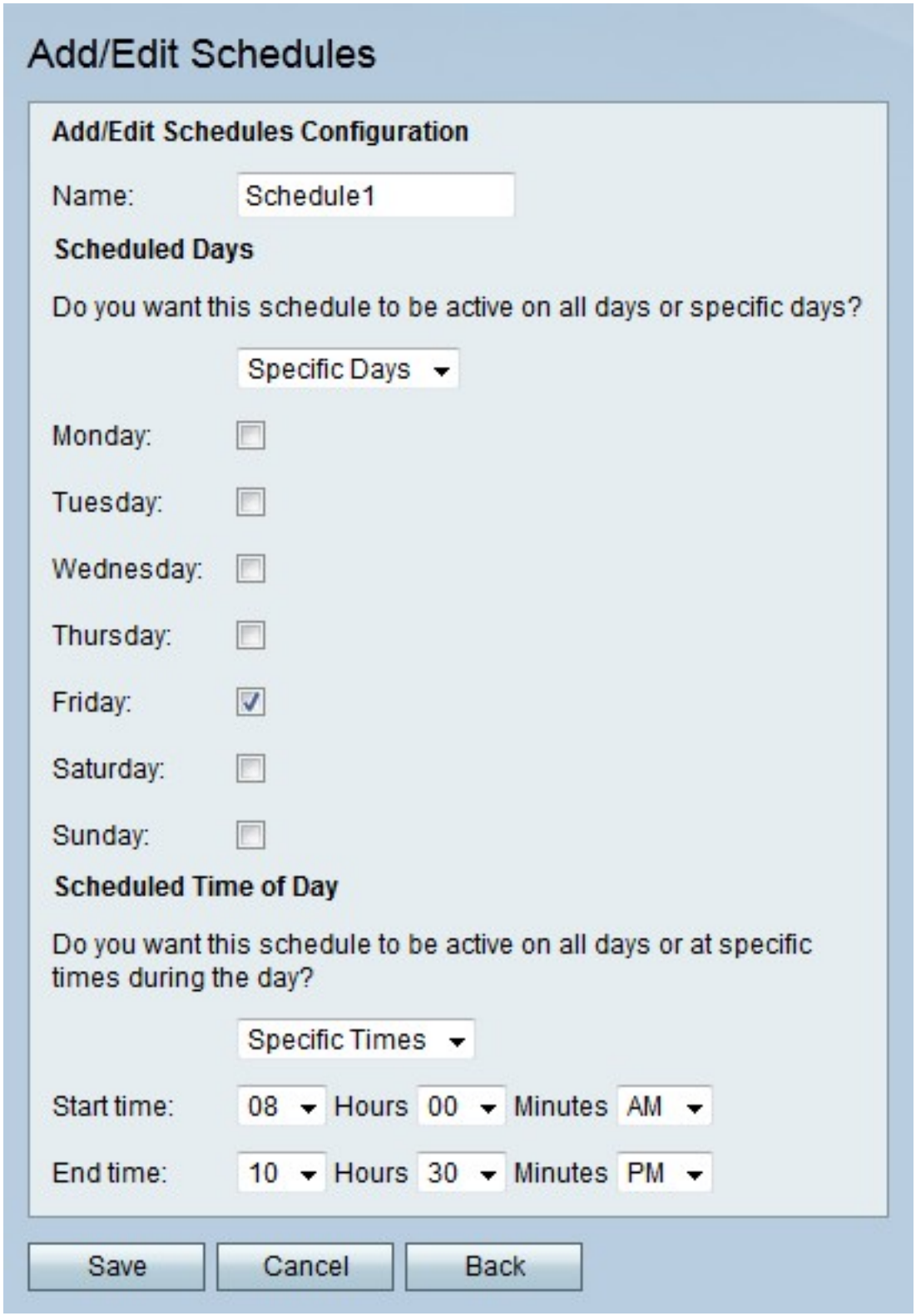
步骤5.点击**"Save"**。

安排管理配置

步骤1.登陆到Web配置工具并且选择**防火墙>日程表管理**。*日程表管理*页打开：



步骤2.点击**Add行**添加一个新的日程表。*添加/编辑*页打开的*日程表*：



步骤3.输入一个名字对于日程表在名称字段。

第4.步。从被安排的几天下拉列表请选择日程表是活跃的日。

- •所有日—日程表为星期的每天是活跃的。
- •特定日—检查日的复选框日程表是活跃的。

第5.步。从被安排的每日定时下拉列表请选择日程表是活跃的时间。

- •所有次—日程表一直是活跃的日。

•特定时间—从一开始时间和结束时间下拉列表选择日程表启动的时间，并且日程表结束的时间。

步骤6.点击“Save”。