增加并且配置在RV130和RV130W的访问规则

客观

网络设备提供基本流量过滤功能访问规则。访问规则是指定许可证在访问控制表(ACL)的单个条目或拒绝根据协议、源和目的地IP地址或者网络配置(转发或丢弃信息包)的规则。

本文目标将显示您如何增加和配置在RV130和RV130W的一个访问规则。

可适用的设备

•RV130

•RV130W

软件版本

•版本1.0.1.3

增加并且配置访问规则

设置默认出局策略

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：

Step 2.在*默认出局策略*地区中，请点击期望单选按钮选择出局流量的一个策略。策略适用，每当没有被配置的访问规则或互联网访问策略。默认设置是**准许**，允许所有数据流到互联网通过通过。

可用的选项被定义如下：

- 准许—允许出去从LAN的所有流量类型到互联网。
- 拒绝—拦截出去从LAN的所有流量类型到互联网。

步骤3.点击**"Save"**保存设置。

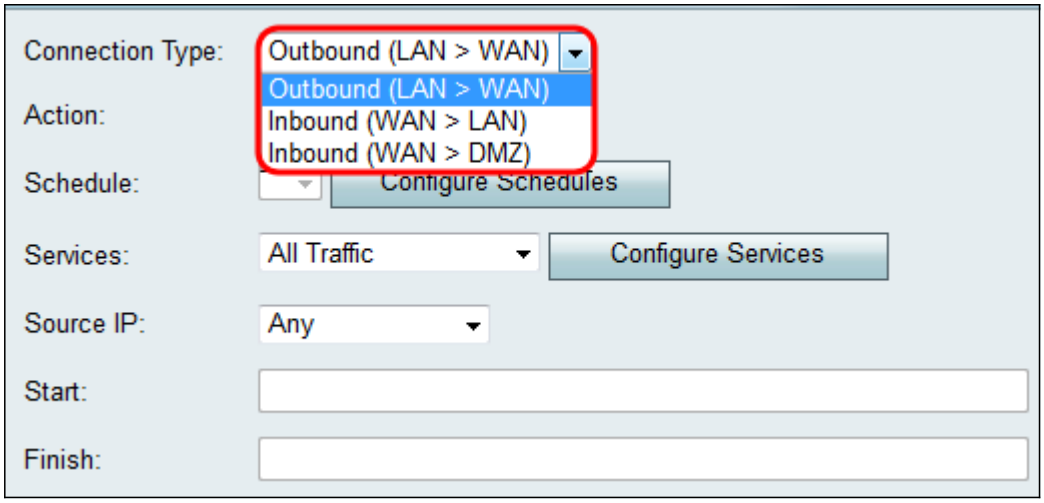
增加访问规则

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*窗口打开：

步骤2.点击**Add行**在*访问规则表里*增加一个新的访问规则。

*添加访问规则*页打开：

第 3 步：从*连接类型*下拉列表，请选择规则适用的流量类型。



可用的选项被定义如下：

•outbound (LAN >广域网) —规则影响来自本地网络的信息包(LAN)并且出去到互联网(广域网)。

•入站(广域网> LAN) —规则影响来自互联网的信息包(广域网)并且进入本地网络(LAN)。

•入站(广域网> DMZ) —规则影响来自互联网的信息包(广域网)并且进入非敏感区域(DMZ)子网络。

第 4 步：从*动作*下拉列表，当规则被匹配时，请选择应采取的措施。

可用的选项被定义如下：

•总是块—，如果条件被匹配，总是请拒绝访问。跳到第6.步。

•总是请准许—，如果条件被匹配，总是请允许访问。跳到第6.步。

•由日程表的块—在一个预先配置的日程表期间，如果条件被匹配请拒绝访问。

•由日程表允许—在一个预先配置的日程表期间，如果条件被匹配请允许访问。

第 5 步：如果**由日程表**选择了**块**或**由**在第4步的**日程表允许**，从*日程表*下拉列表请选择适当的日程表。

Note:要创建或编辑日程表，请点击**配置日程表**。参考*配置在RV130和RV130W的日程表*欲知更多信息和指南。

步骤6.选择访问规则申请从*服务*下拉列表的服务类型。

Note:如果要添加或编辑服务，请点击**配置服务**。参考*服务在RV130和RV130W的管理配置*欲知更多信息和指南。

配置出局流量的来源和目的地IP

请遵从在此部分的步骤，如果**outbound (LAN >广域网)**选择了作为连接类型第3步*增加访问规则。*

Note:如果一种Inbound连接类型在第3步选择了增加访问规则，请跳到下个部分： *配置Inbound数据流的来源和目的地IP*。

步骤1.选择您如何希望定义从*来源IP*下拉列表的来源IP。对于出局流量，来源IP是指地址或地址(在LAN)防火墙规则将适用。

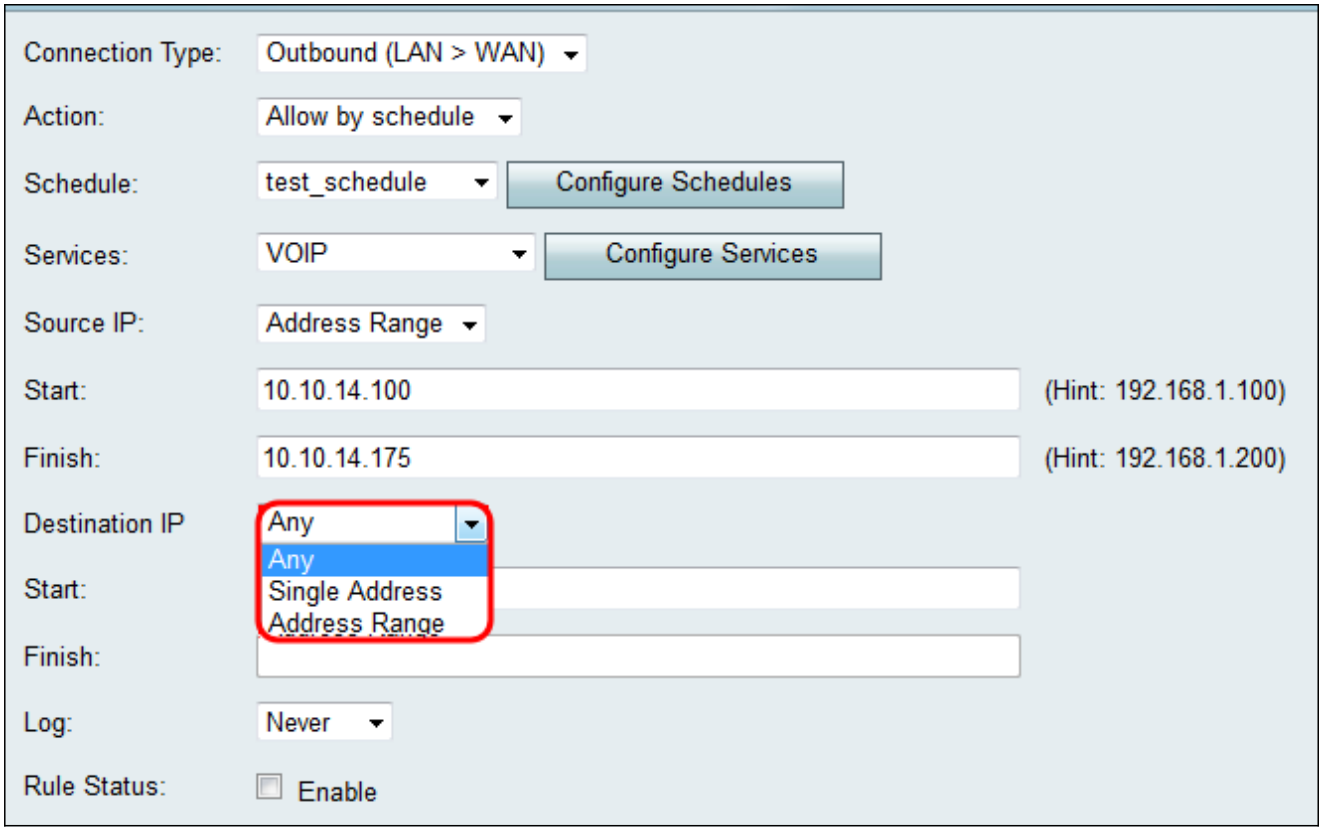
可用的选项被定义如下：

- 其中任一—适用于起源从所有IP地址于本地网络的数据流。所以，请留下*启动*和*完成*字段留空。如果选择此选项，请跳到第4步。
- 单个地址—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IP地址。
- 地址范围—适用于起源从IP地址的范围于本地网络的数据流。输入范围的开始的IP地址在*Start字段*和结束IP地址在*Finish字段*为了设置范围。

Step 2.如果选择了在Step1的**单个地址**，请输入将适用于访问规则在*Start字段的*IP地址，然后跳到第4.步。如果选择了在Step1的**地址范围**，请输入将适用于访问规则在*Start字段的*一个开始的IP地址。

第 3 步：如果选择了在Step1的**地址范围**，请输入在*Finish字段将*封装访问规则的IP地址范围的结束IP地址。

步骤4.选择您如何希望定义从*目的地IP*下拉列表的目的地IP。对于出局流量，目的地IP是指地址或地址(在广域网)数据流从本地网络允许或被否决。



可用的选项被定义如下：

- 其中任一—适用于数据流朝向往所有IP地址在公共互联网里。所以，请留下*启动*和*完成*字段留空。
- 单个地址—适用于数据流朝向往单个IP地址在公共互联网里。在*Start字段*输入IP地址。
- 地址范围—适用于数据流朝向往IP地址的范围在公共互联网里。输入范围的开始的IP地址在*Start字段*和结束IP地址在*Finish字段*为了设置范围。

第 5 步：如果选择了在第4步的**单个地址**，请输入将适用于访问规则在*Start字段的*IP地址。如果选择了在第4步的**地址范围**，请输入将适用于访问规则在*Start字段的*一个开始的IP地址。

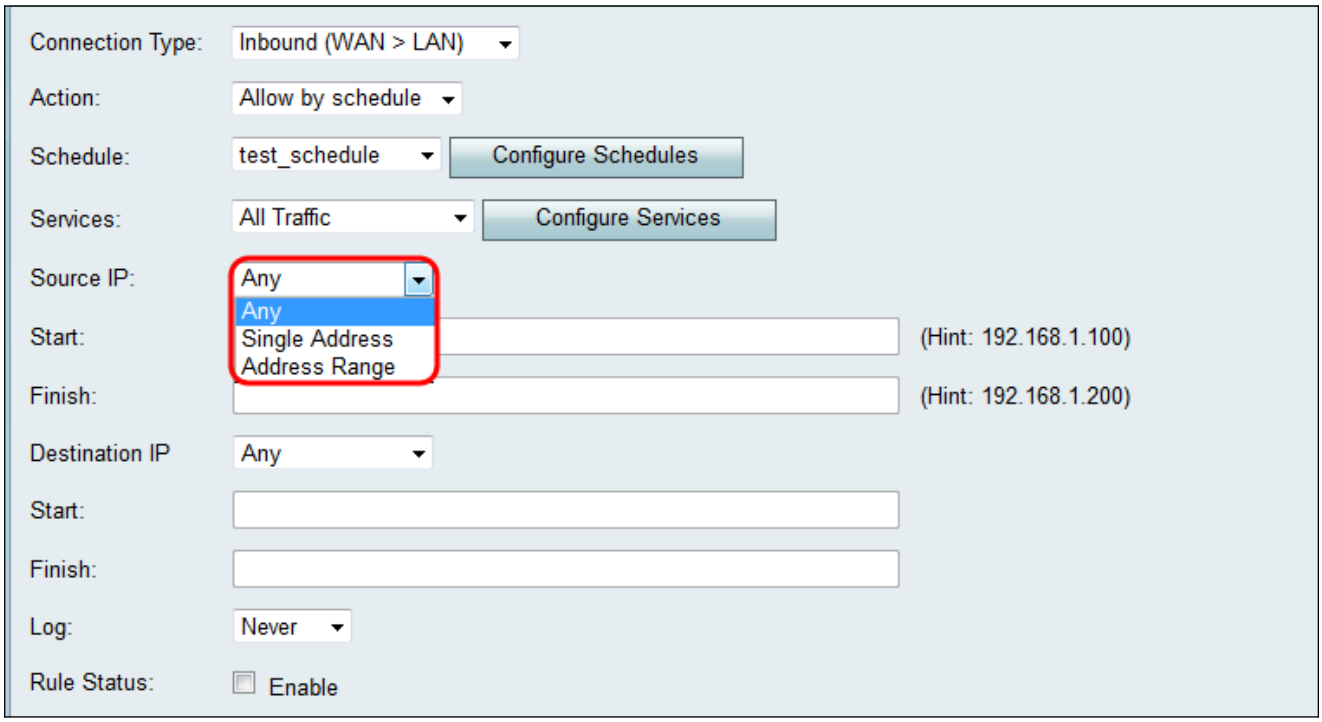
第6.步。如果选择了在第4步的**地址范围**，请输入在*Finish字段将*封装访问规则的IP地址范围的结束IP地址。

配置Inbound数据流的来源和目的地IP

请遵从在此部分的步骤，如果**入站(广域网> LAN)**或**入站(广域网> DMZ)**选择了作为连接类型第3步*增加访问规则*。

步骤1.选择您如何希望定义从*来源IP*下拉列表的来源IP。对于Inbound数据流，来源IP是指地

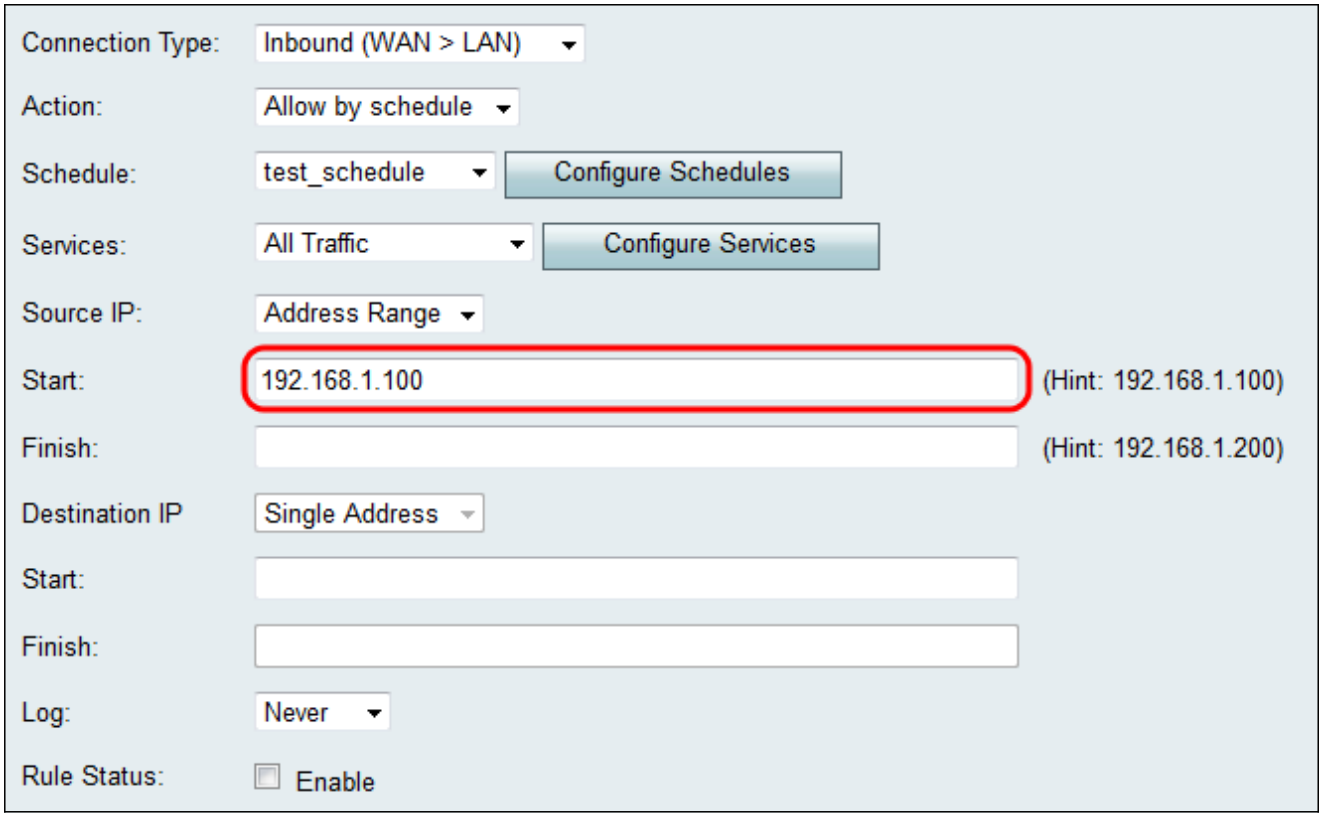
址或地址(在广域网)防火墙规则将适用。



可用的选项被定义如下：

- 其中任一—适用于起源从所有IP地址在公共互联网里的数据流。所以，请留下*启动*和*完成*字段留空。如果选择此选项，请跳到第4步。
- 单个地址—适用于起源从单个IP地址在公共互联网里的数据流。在*Start字段*输入IP地址。
- 地址范围—适用于起源从IP地址的范围在公共互联网里的数据流。输入范围的开始的IP地址在*Start字段*和结束IP地址在*Finish字段*为了设置范围。

Step 2.如果选择了在Step1的**单个地址**，请输入将适用于访问规则在*Start字段的*IP地址，然后跳到第4.步。如果选择了在Step1的**地址范围**，请输入将适用于访问规则在*Start字段的*一个开始的IP地址。



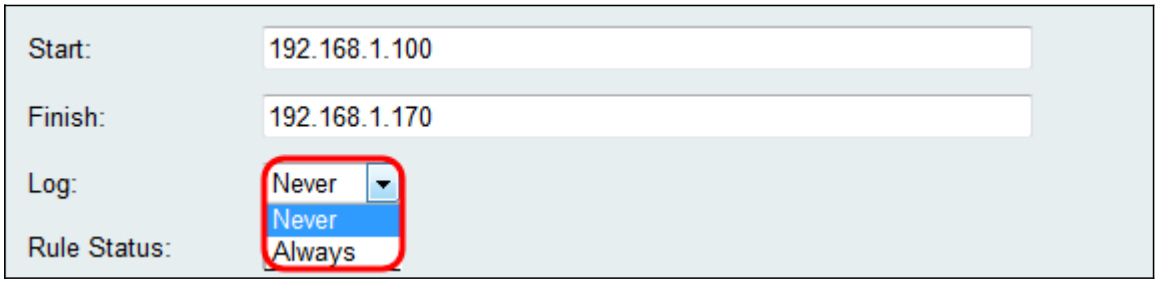
第 3 步：如果选择了在Step1的**地址范围**，请输入在*Finish字段*将封装访问规则的IP地址范围的结束IP地址。

步骤4.在*Start字段*输入目的地IP的单个地址在*目的地IP*下拉列表之下。对于Inbound数据流，目的地IP是指地址(在LAN)数据流从公共互联网允许或被否决。

Note:如果**入站(广域网> DMZ)**选择了作为连接类型第3步*增加访问规则*，目的地IP的单个地址自动地配置有启用DMZ主机的IP地址。

记录和启用访问规则

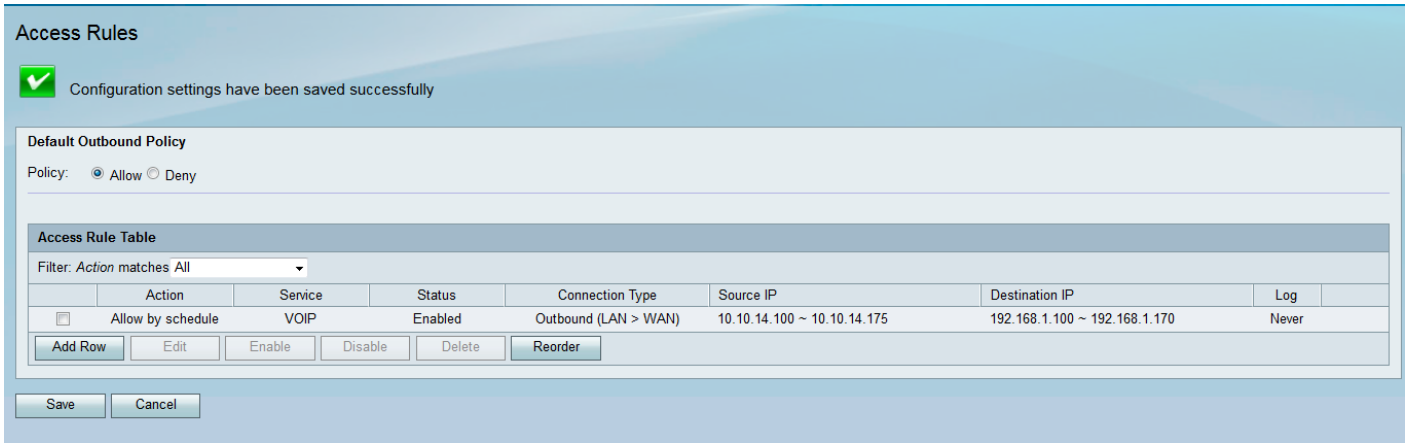
步骤1.**总是请**选择在*日志*下拉列表，如果希望路由器创建日志，每当信息包匹配一个规则。请勿选择，如果请勿希望记录发生，当规则被匹配时。



Step 2.检查**Enable复选框**对enable (event)访问规则。

步骤3.点击“Save”保存您的设置。

*访问规则*表用最近配置的访问规则更新。


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
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
Add Row
Edit
Enable
Disable
Delete
Reorder
Save
Cancel