RV320和RV325 VPN路由器上的访问规则配置

目标

访问控制列表(ACL)是阻止或允许流量从特定用户发往或从特定用户发往的列表。访问规则可以配置为始终有效或基于已定义的计划。访问规则根据各种条件进行配置，以允许或拒绝对网络的访问。访问规则根据需要将访问规则应用到路由器的时间进行安排。本文概述并介绍访问规则设置向导，用于确定是否允许流量通过路由器的防火墙进入网络以确保网络中的安全。

适用设备 |固件版本

- RV320双WAN VPN路由器 | V 1.1.0.09(下载最新版本)
- RV325千兆双WAN VPN路由器 | V 1.1.0.09(下载最新版本)

访问规则配置

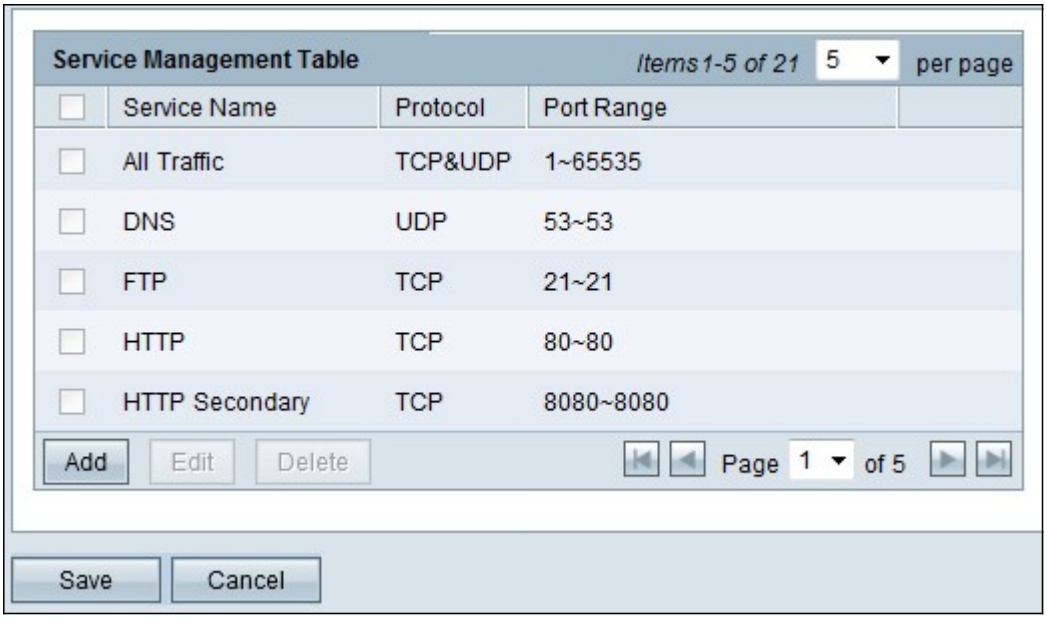
步骤1.登录Web配置实用程序，然后选择Firewall>**Access Rules**。“访*问规则*”页打开：

访问规则表包含以下信息：

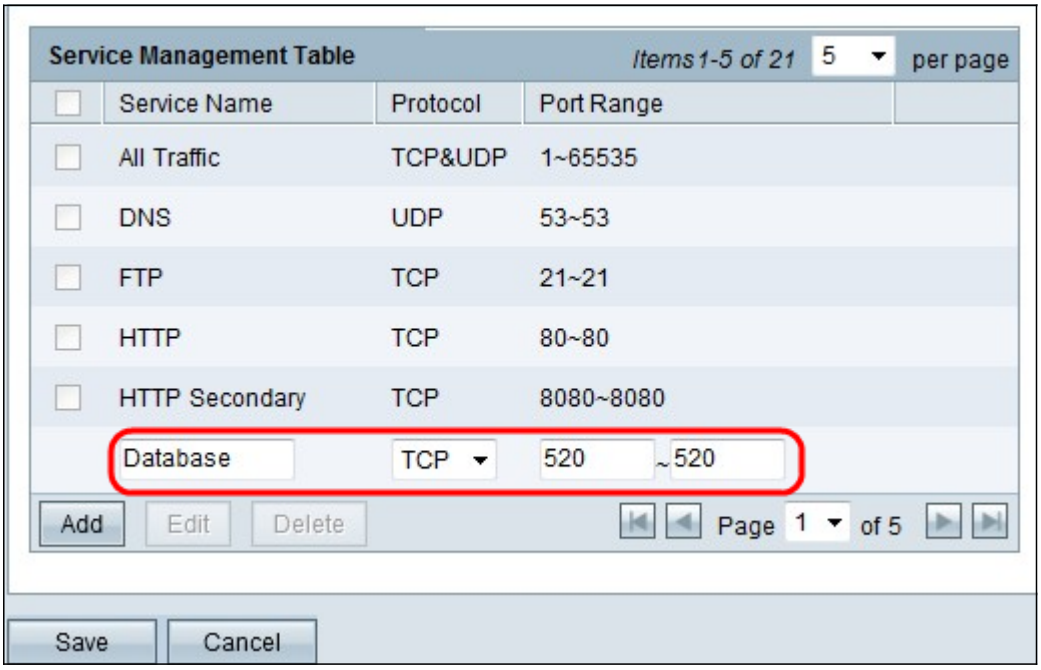
- Priority — 显示访问规则的优先级
- 启用 — 显示访问规则是启用还是禁用
- 操作 — 显示允许或拒绝访问规则。
- 服务 — 显示服务类型。
- SourceInterface — 显示访问规则应用到哪个接口。
- 源 — 显示源设备的IP地址
- 目标 — 显示目标设备的IP地址
- 时间 — 显示应用访问规则的时间
- Day — 显示应用访问规则的一周内

服务管理

步骤1.单击**Service Management**添加新服务。“服务*管理*”表页打开：



步骤2.单击**Add**添加新服务。



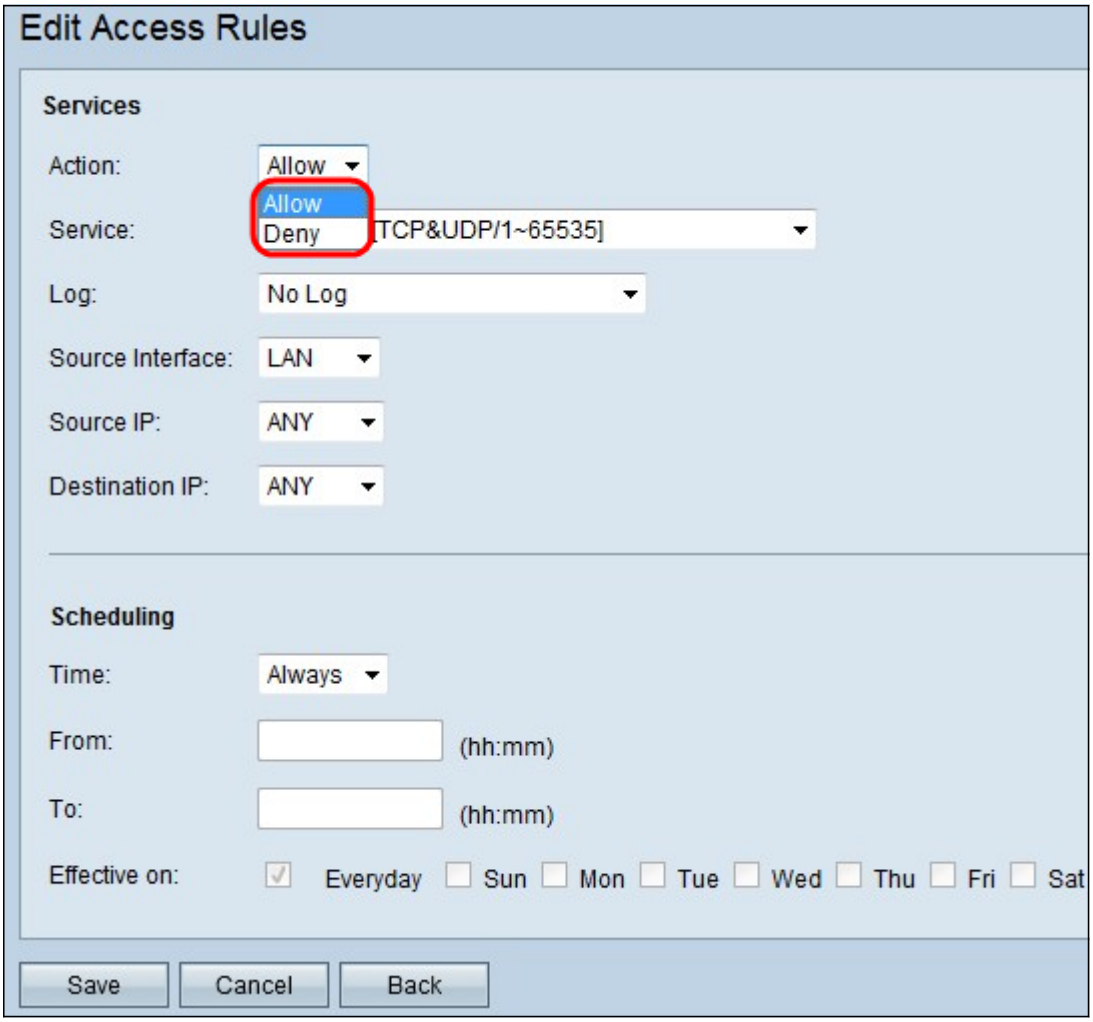
步骤3.配置以下字段。

- 服务名称 — 根据您的要求，为服务指定名称
- 协议(Protocol) — 为服务选择协议TCP或UDP
- 端口范围 — 根据您的要求输入端口号范围，端口号必须在范围(1-65536)内。

步骤4.单击“**保存**”以保存更改

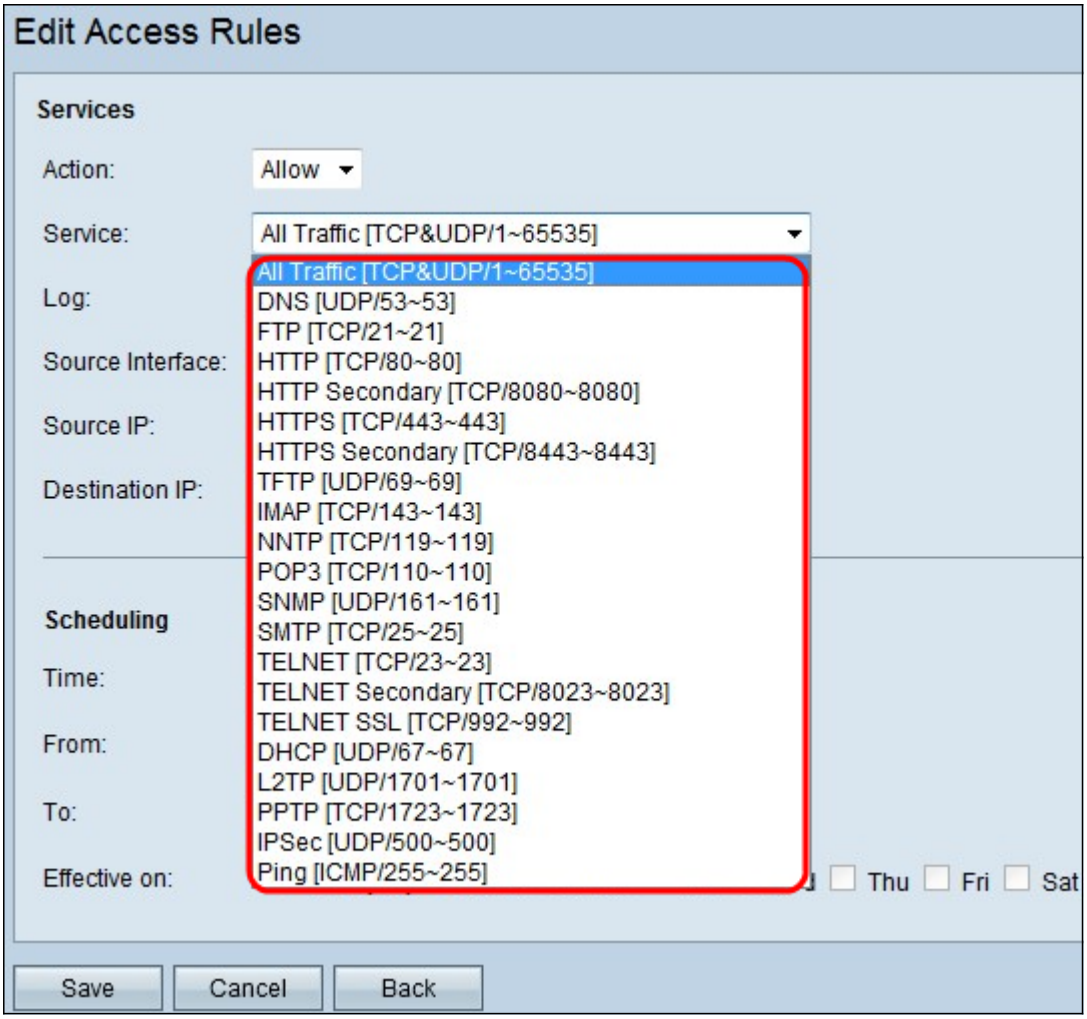
IPv4上的访问规则配置

步骤1.单击**Add**以配置新的访问规则。系统将显示*"编辑访问规*则"窗口。

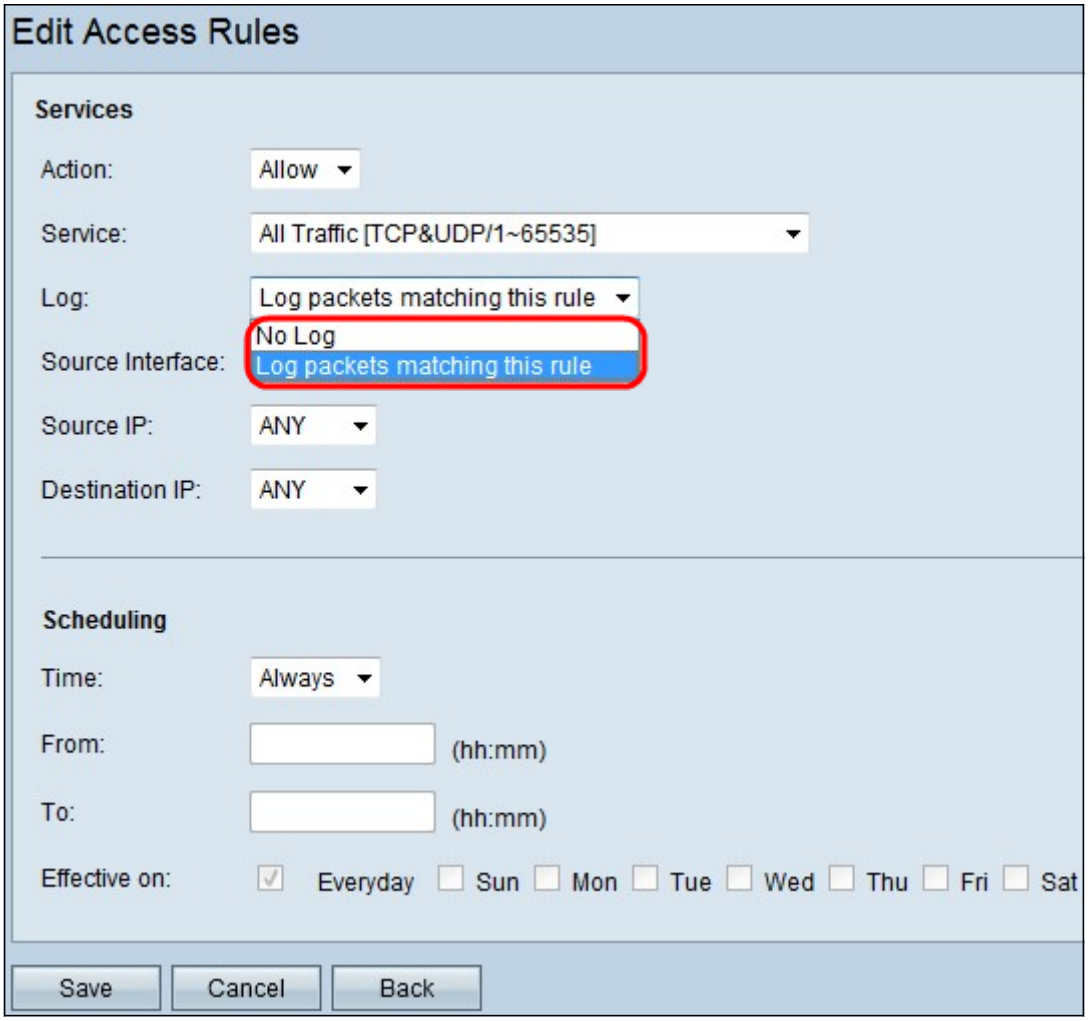


步骤2.从Action下拉列表中选择适当的选项，以允许或限制要设置的规则的流量。访问规则根据各种值限制对网络的访问。

- 允许 — 允许所有流量。
- 拒绝 — 限制所有流量。

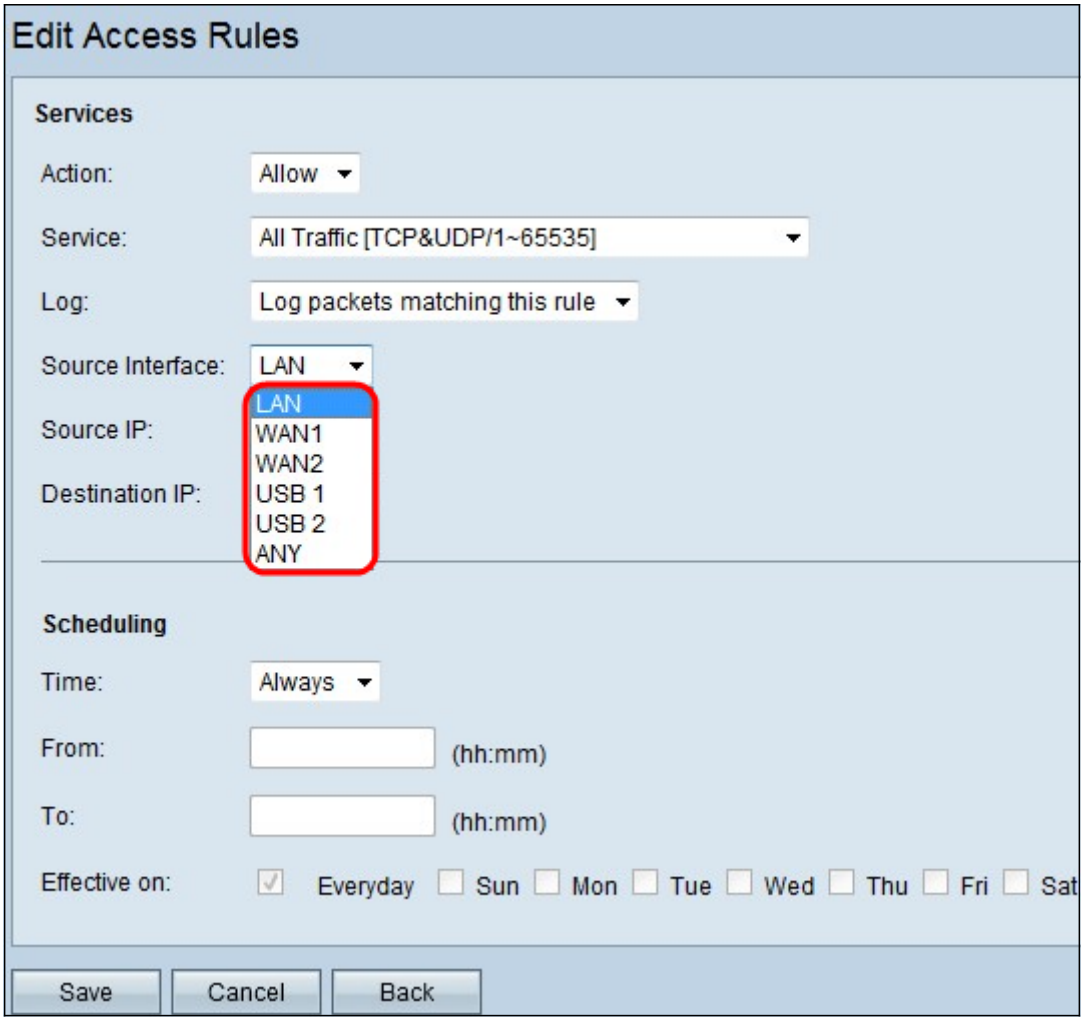


步骤3.从“服务”下拉列表中选择需要过滤的适当服务。



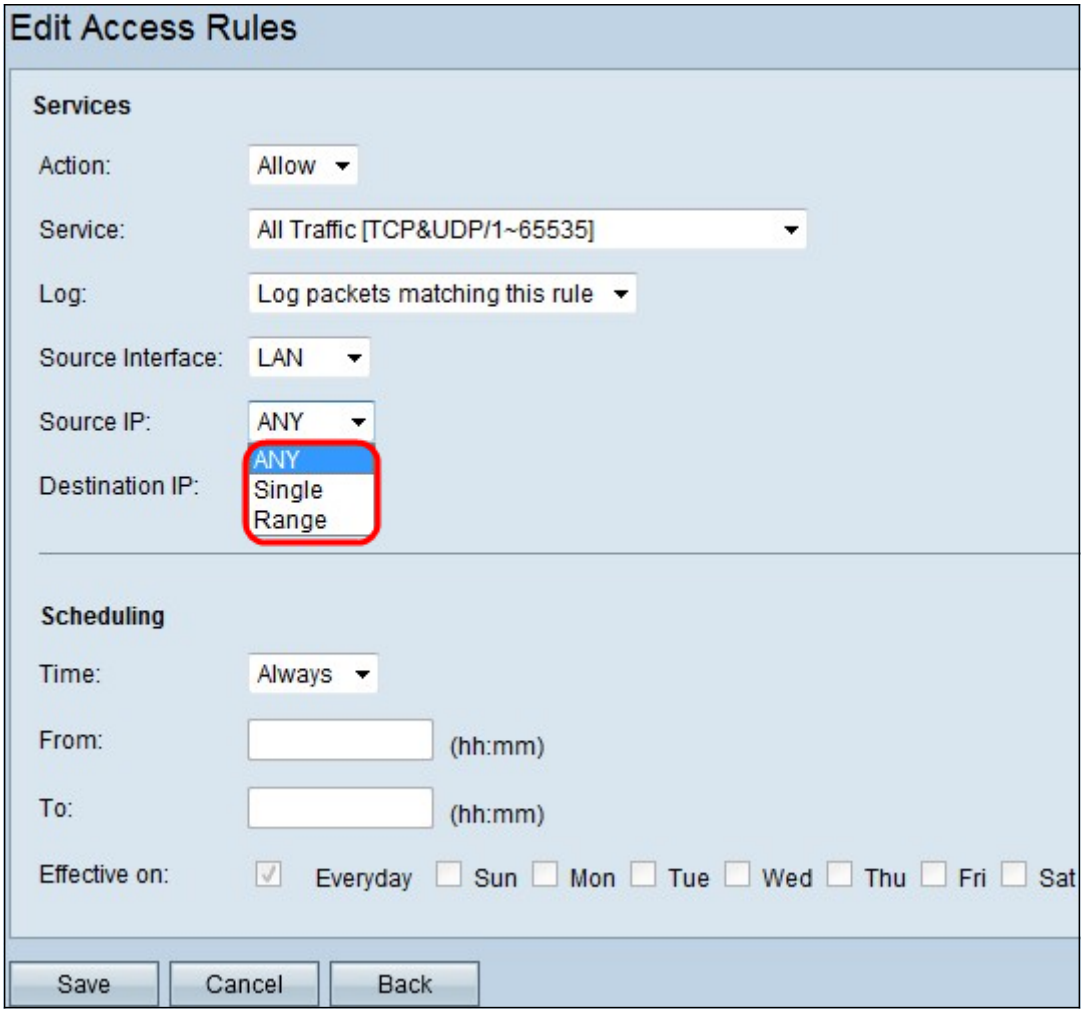
步骤4.从Log下拉列表中选择适当的Log选项。log选项确定设备是否保留与访问规则集对应的流量日志。

- 与此访问规则匹配的日志数据包 — 路由器会保留跟踪所选服务的日志。
- 不记录 — 路由器不保留访问规则的日志。



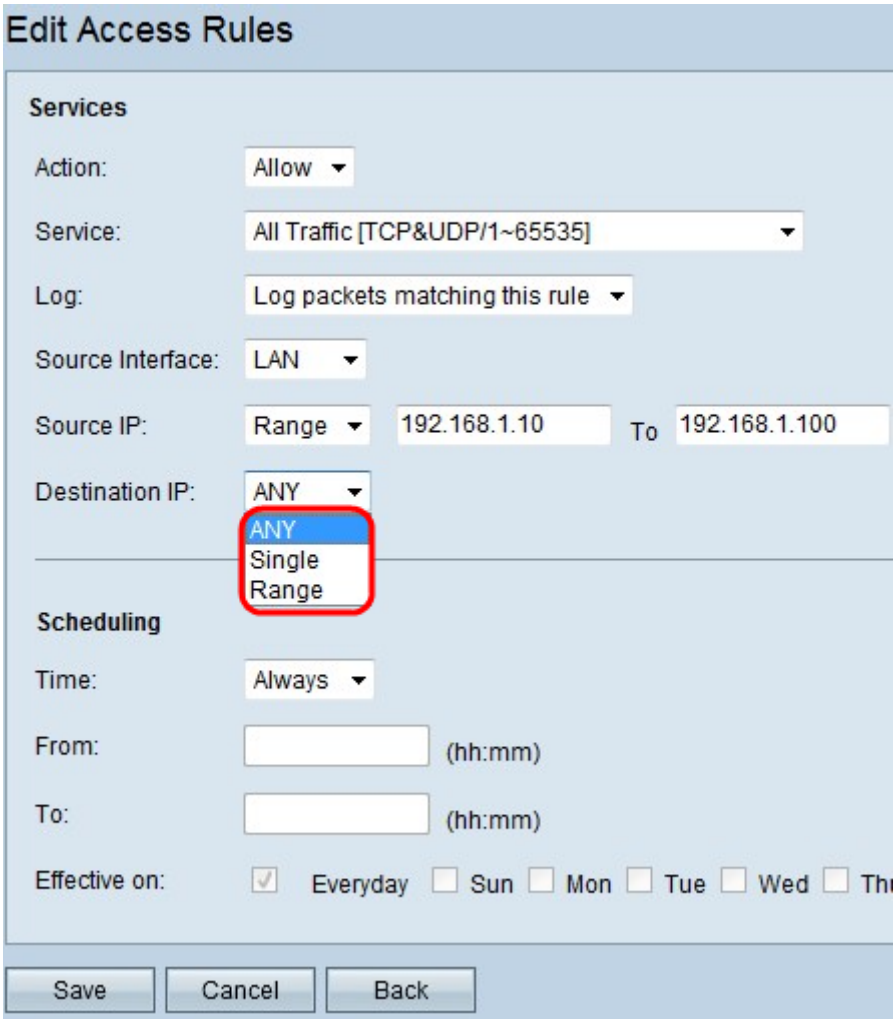
步骤5.从Interface下拉列表中，选择适当的源接口。此接口是实施访问规则的位置。

- LAN — 访问规则仅影响LAN流量。
- WAN 1 — 访问规则仅影响WAN 1流量。
- WAN 2 — 访问规则仅影响WAN 2流量。
- Any — 访问规则影响设备任何接口中的所有流量。



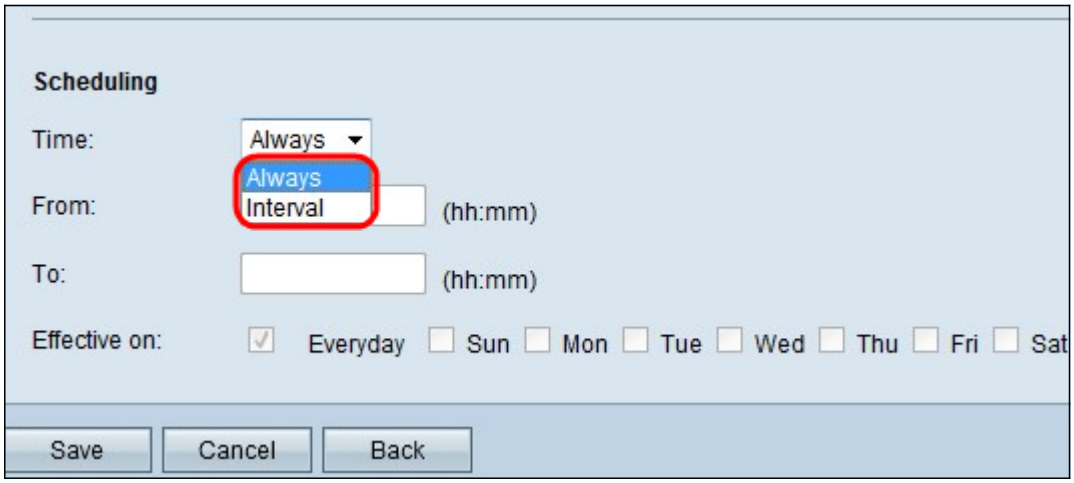
步骤6.从Source IP下拉列表中选择访问规则应用到的相应源IP类型。

- Any — 设备网络的任何IP地址都已应用规则。
- 单个 — 设备网络上只有一个指定IP地址应用了该规则。在相邻字段中输入所需的IP地址。
- 范围 — 只有设备网络上指定的IP地址范围才应用了规则。如果选择范围，则需要在相邻字段中输入该范围的第一个和最后一个IP地址。



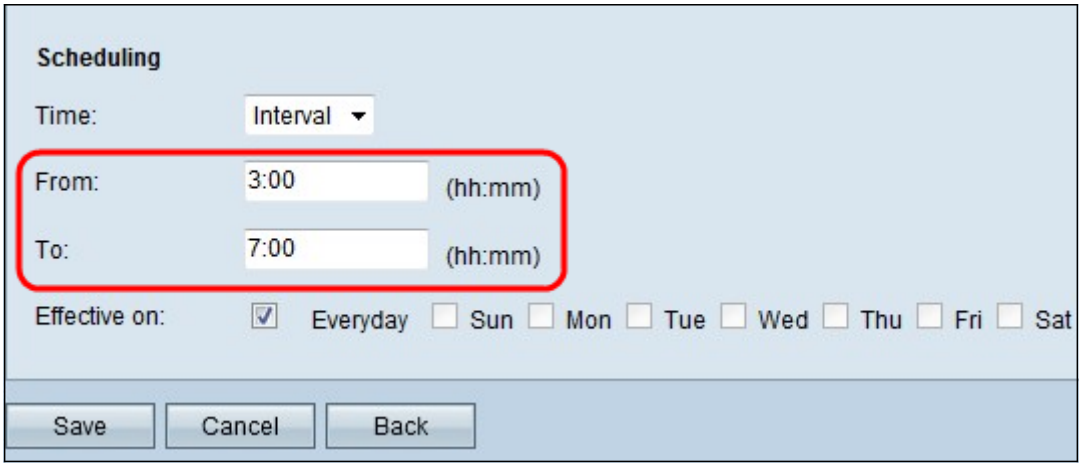
步骤7.从可用下拉列表中选择应用访问规则的相应目标IP类型。

- Any — 任何目标IP地址都应用了规则。
- 单个 — 仅单个指定的IP地址应用了规则。在相邻字段中输入所需的IP地址。
- 范围 — 只有设备网络外部的指定IP地址范围才应用了规则。如果选择范围，则需要在相邻字段中输入该范围的第一个和最后一个IP地址。



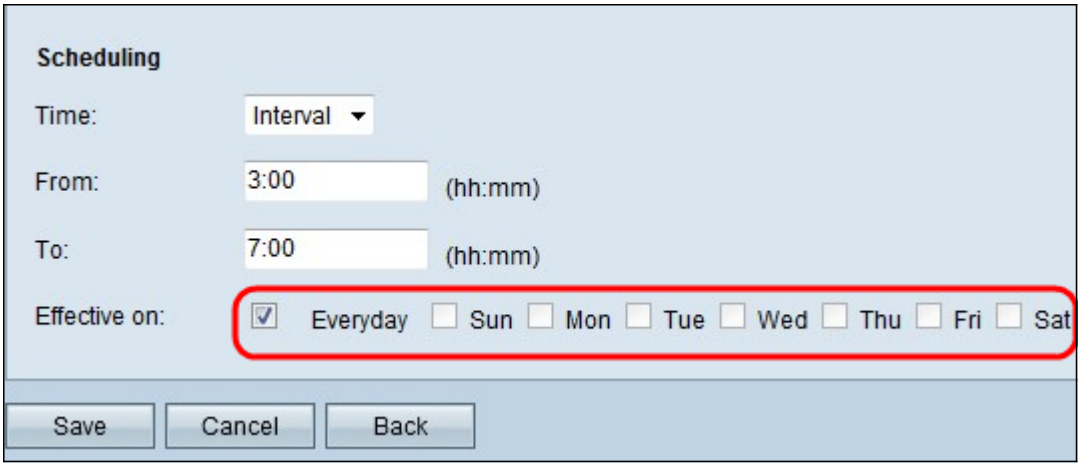
节省时间:默认情况下，时间设置为Always。如果要将访问规则应用于特定时间或日，请按照步骤8到步骤11。否则，请跳至步骤12。

步骤8.从下拉列表中选择**Interval**,Access rules are ave stecific times。您需要输入要实施的访问规则的时间间隔。



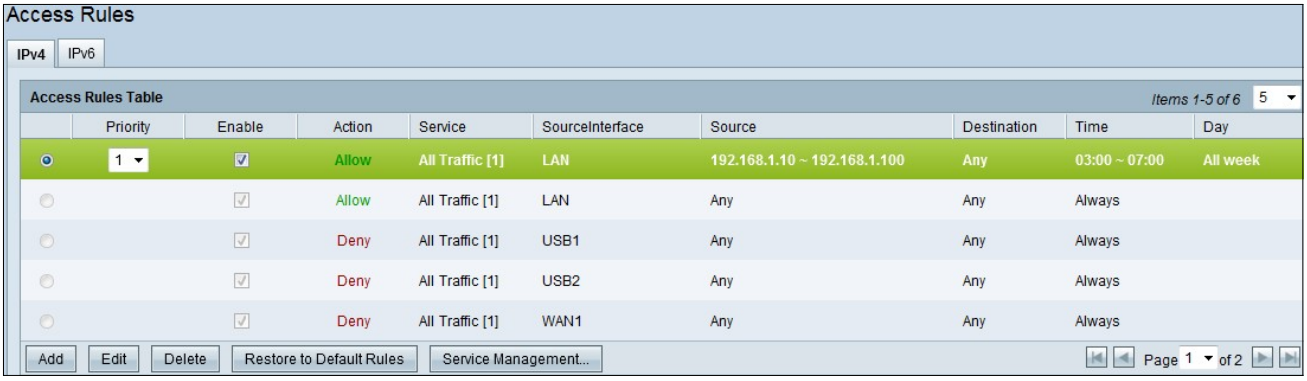
步骤9.在“自”字段中输入开始应用访问列表的时间。时间格式为hh:mm。

步骤10.在“收件人”字段中输入您不再希望应用访问列表的时间。时间格式为hh:mm。



步骤11.选中要应用访问列表的特定天数复选框。

步骤12.单击“**保存**”以保存更改。

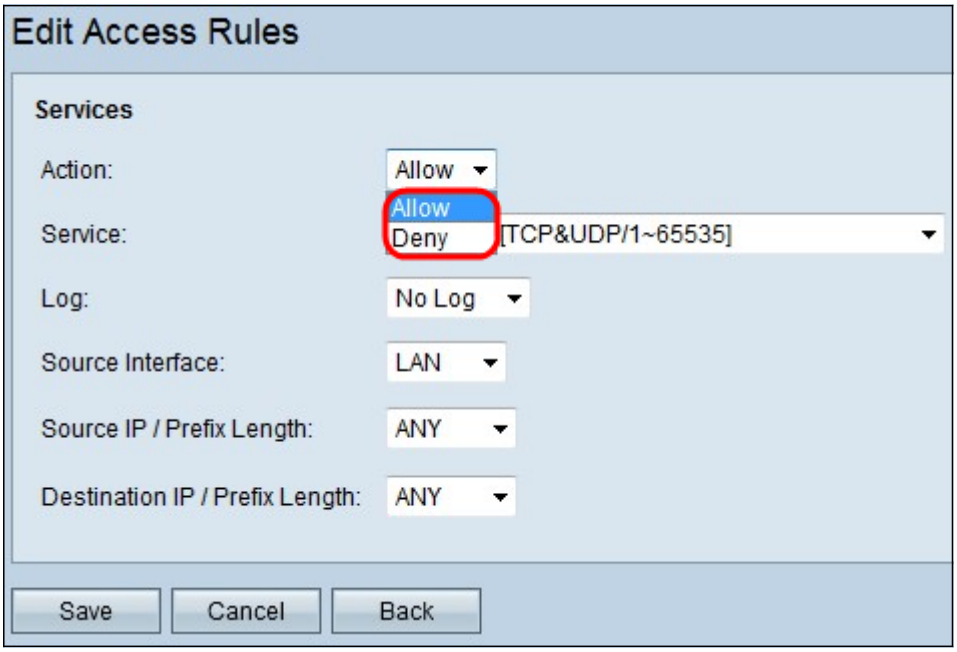


步骤13.（可选）如果要恢复默认规则，请点击Restore to Default Rules（**恢复为默认规则**）。您配置的所有访问规则都会丢失。

IPv6上的访问规则配置

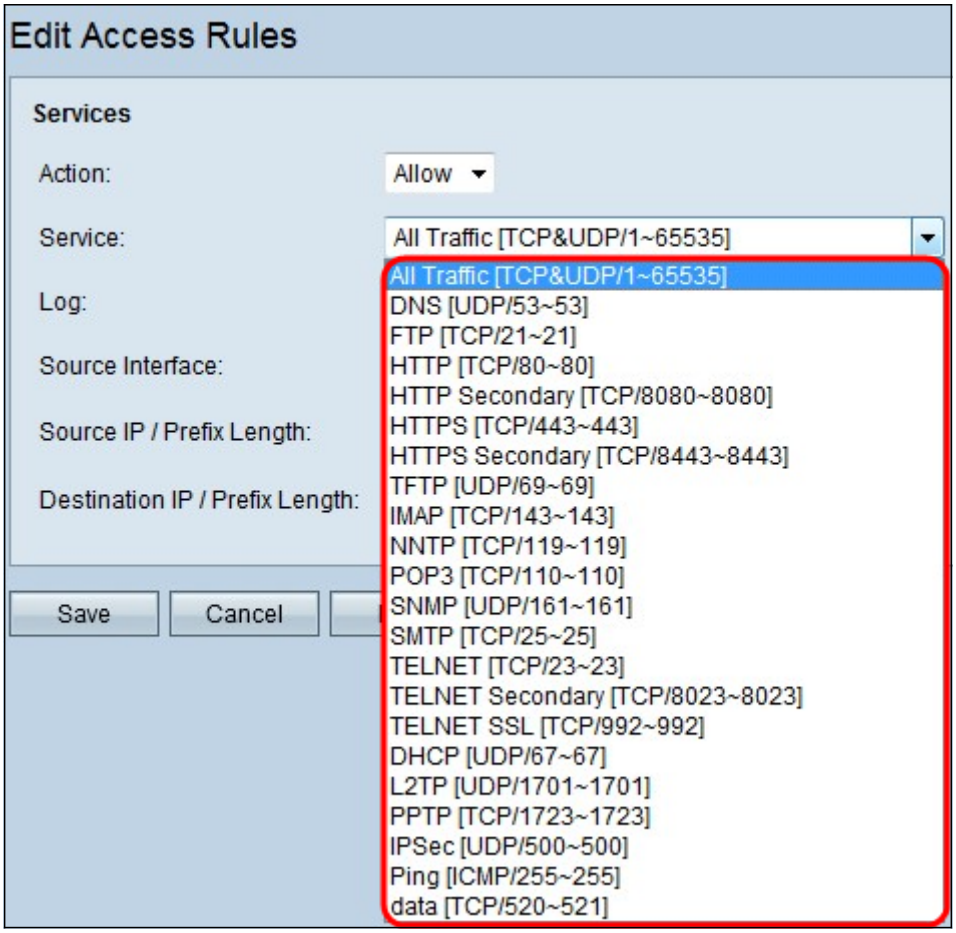
步骤1.点击IPv6选项卡以配置IPv6访问规则。

步骤2.单击Add以添加新的IPv6访问规则。系统将显示*"编辑访问规则"*窗口。



步骤3.从"操作"下拉列表中选择适当的选项，以允许或限制您需要设置的规则。 访问规则通过允许或拒绝来自特定服务或设备的流量访问来限制对网络的访问。

- 允许 — 允许所有流量。
- 拒绝 — 限制所有流量。

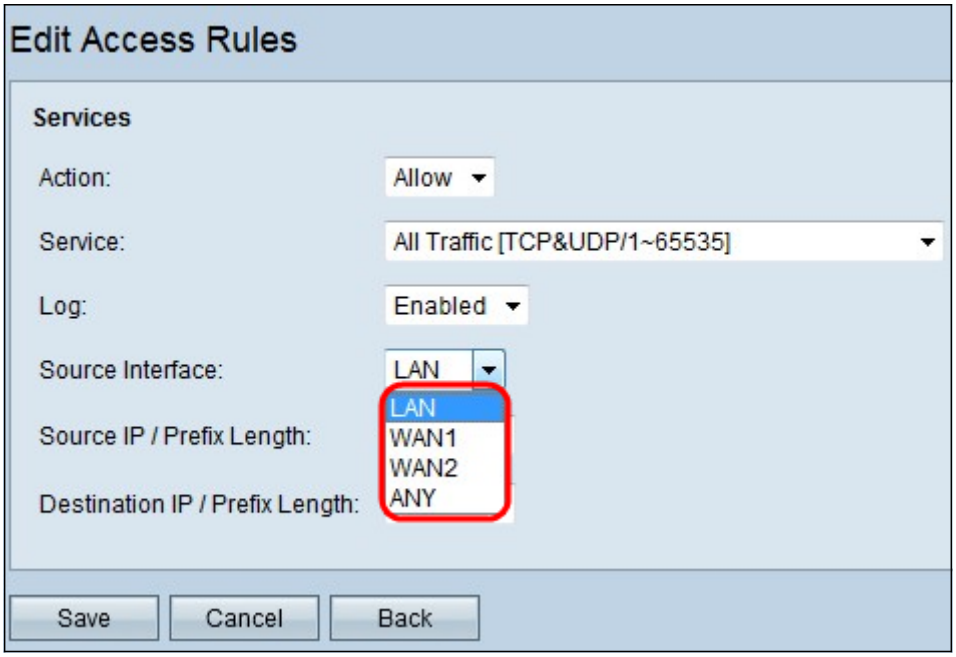


步骤4.从“服务”下拉列表中选择需要过滤的适当服务。

注意：要允许所有流量，请从**服务下拉列表中选择All Traffic [TCP&UDP/1~65535]（如果操作已设置为允许）。**该列表包含您可能想要过滤的所有服务类型。

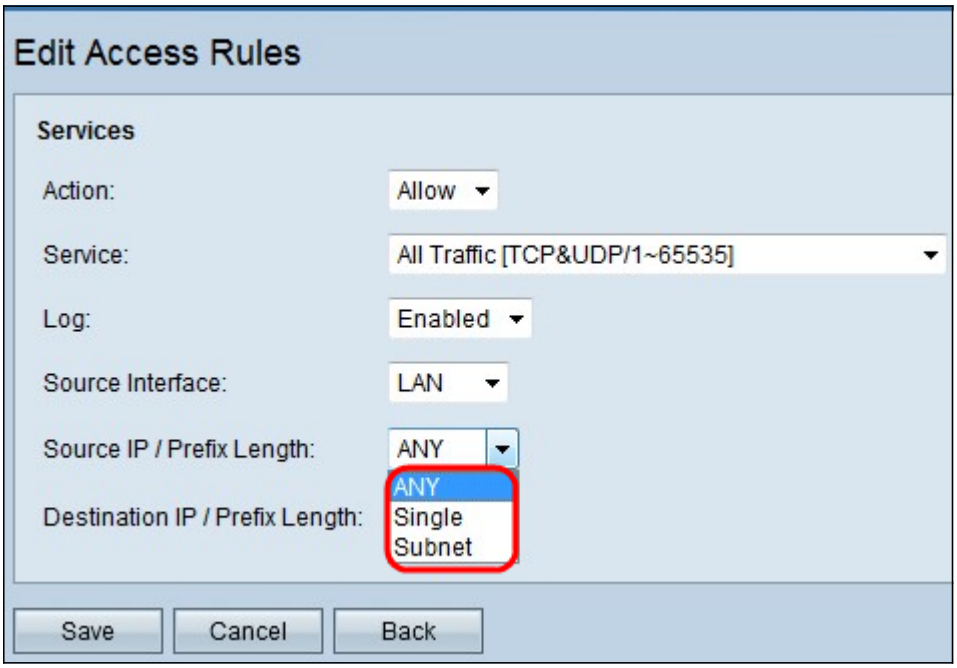
步骤5.从Log下拉列表中选择适当的Log选项。log选项确定设备是否保留与访问规则集对应的流量日志。

- 已启用 — 使路由器能够对已选择的服务保持日志跟踪。
- 非日志 — 禁用路由器以保持日志跟踪。



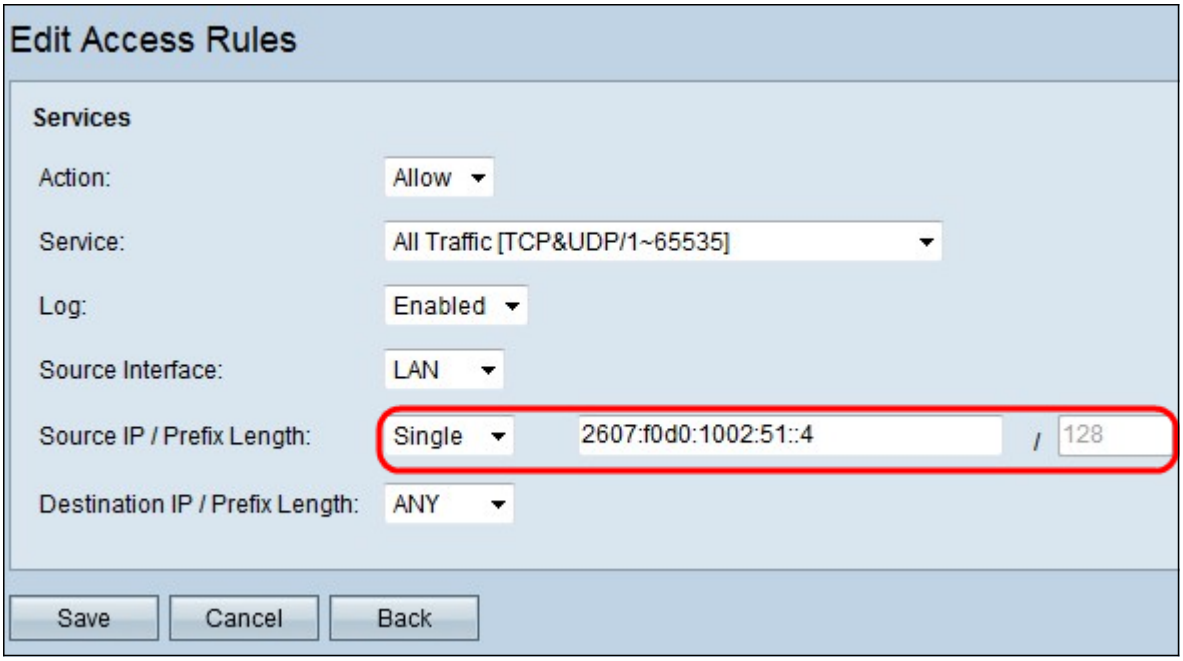
步骤6.点击Interface下拉列表并选择适当的源接口。此接口是实施访问规则的位置。

- LAN — 访问规则仅影响LAN流量。
- WAN 1 — 访问规则仅影响WAN 1流量。
- WAN 2 — 访问规则仅影响WAN 2流量。
- Any — 访问规则影响设备任何接口中的所有流量。

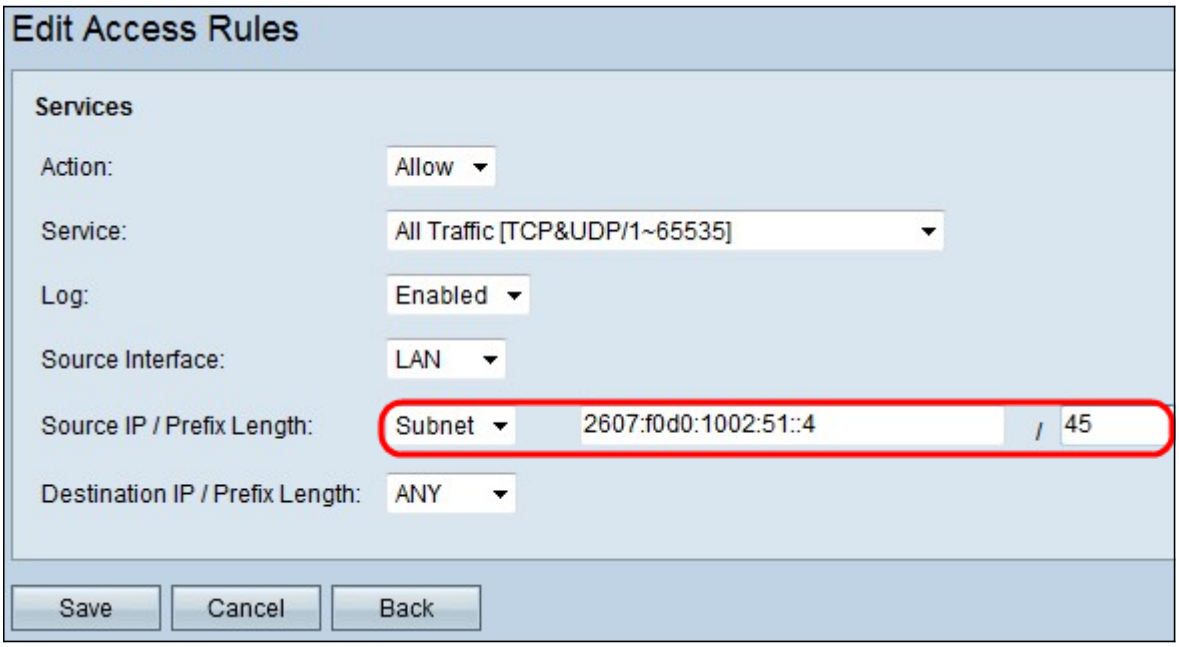


步骤7.从Source IP/ Prefix Length下拉列表中选择访问规则应用到的相应源IP类型。

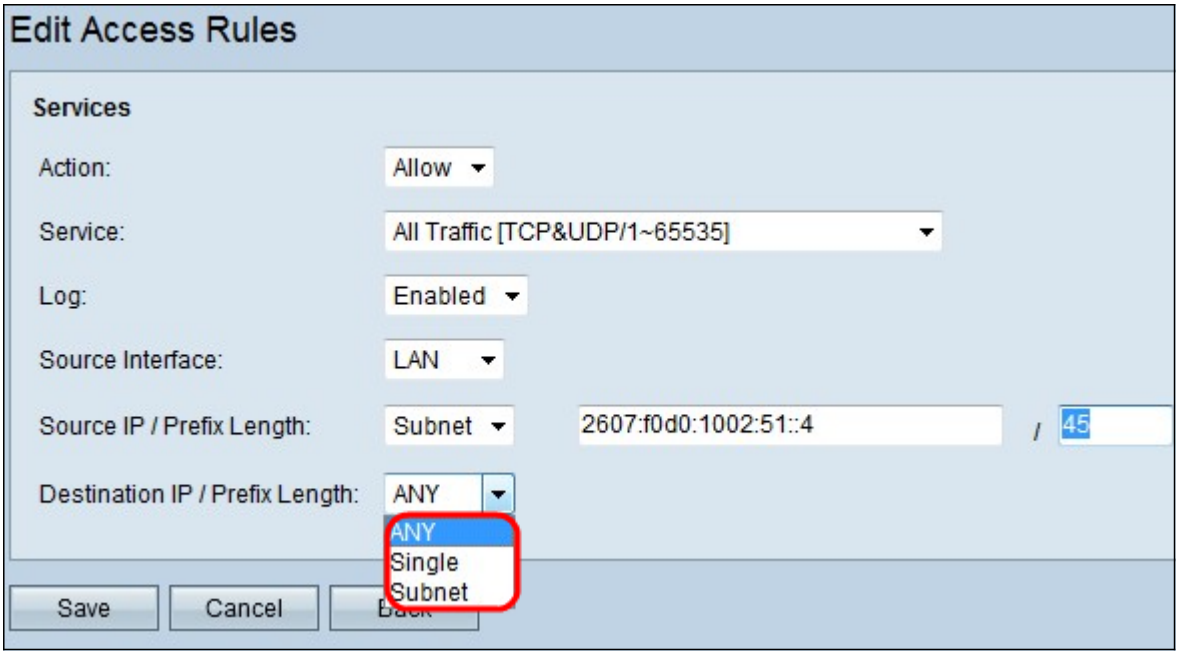
- ANY — 从设备网络接收的任何数据包都应用了规则。



- 单个 — 设备网络中只有一个指定IP地址应用了该规则。在相邻字段中输入所需的IPv6地址。



- 子网 — 只有子网的IP地址才应用该规则。在相邻字段中输入所需子网的IPv6网络地址和前缀长度。



步骤8.从Destination IP / Prefix Length下拉列表中选择访问规则应用到的相应目标IP类型。

- Any — 任何目标IP地址都应用了规则。
- 单个 — 设备网络上只有一个指定IP地址应用了该规则。输入所需的IPv6地址。
- 子网 — 只有子网的IP地址才应用该规则。在相邻字段中输入所需子网的IPv6网络地址和前缀长度。

步骤9.单击“**保存**”以使更改生效。

查看与本文相关的视频……

[单击此处查看思科提供的其他技术讲座]