增加在RV180和RV180W的访问规则

目标

本文陈列创建在Cisco RV180W无线N VPN防火墙的一个访问规则程序。访问规则设置允许的流量类型允许到网络和流量类型的策略网络的外部去。

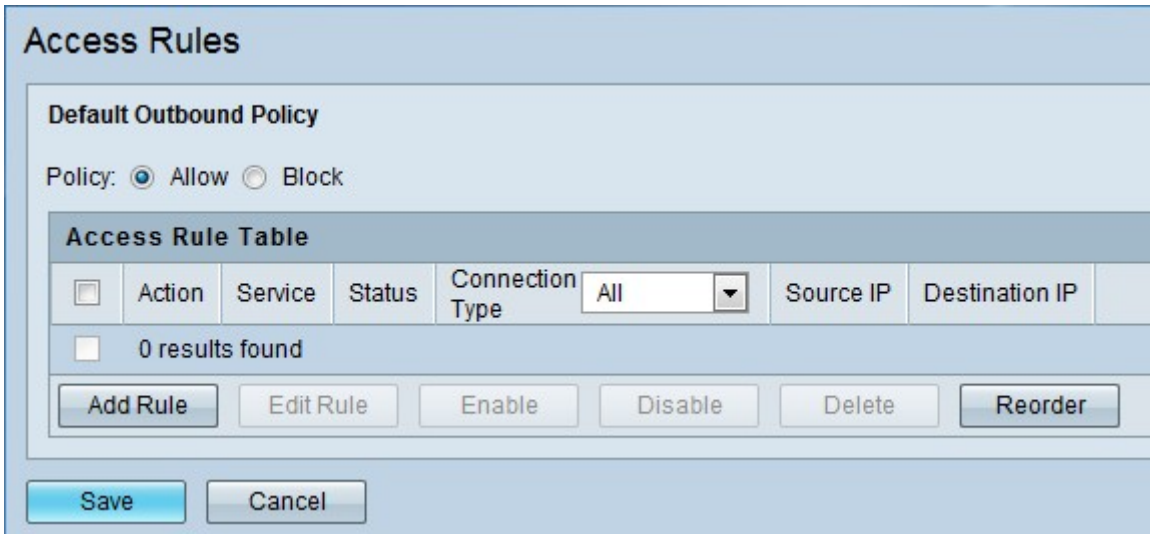
可适用的设备

•RV180
•RV180W

默认出局策略配置

此策略适用于没有由防火墙规则包括配置的数据流。

第 1 步：使用在设备的配置工具，请选择**防火墙>Access规则**。*访问规则*窗口打开。



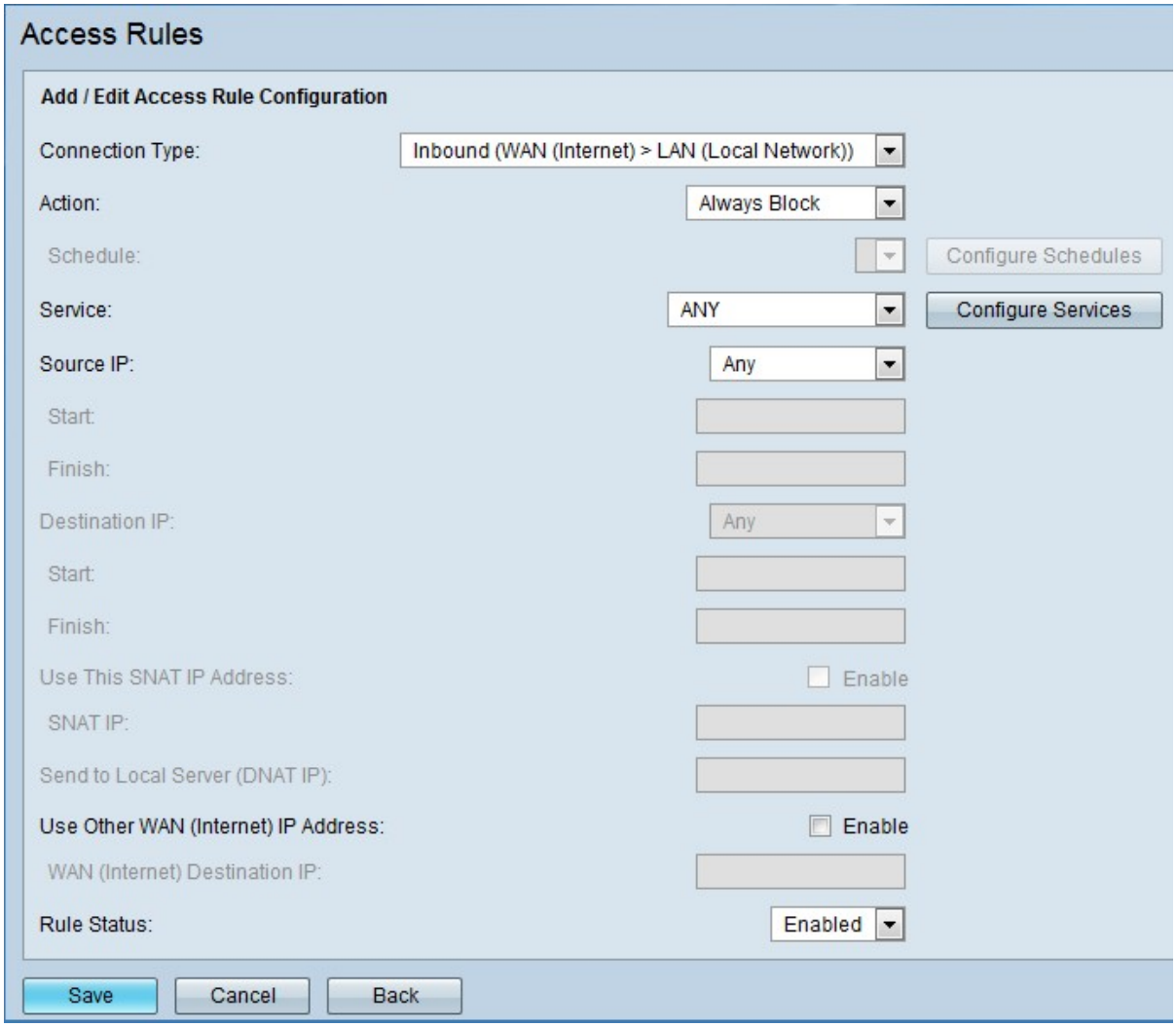
Step 2.在默认出局策略地区下，请点击**允许**或适当地**阻拦**单选按钮。允许对数据流的提供访问从本地网络到互联网。块拒绝对数据流的访问从本地网络到互联网。

步骤3.点击**"Save"**保存设置。

访问规则的创建

第 1 步：使用在设备的配置工具，请选择**防火墙>Access规则**。*访问规则*窗口打开。

Step 2.在访问规则表格区域下，请点击**添加规则**按钮。

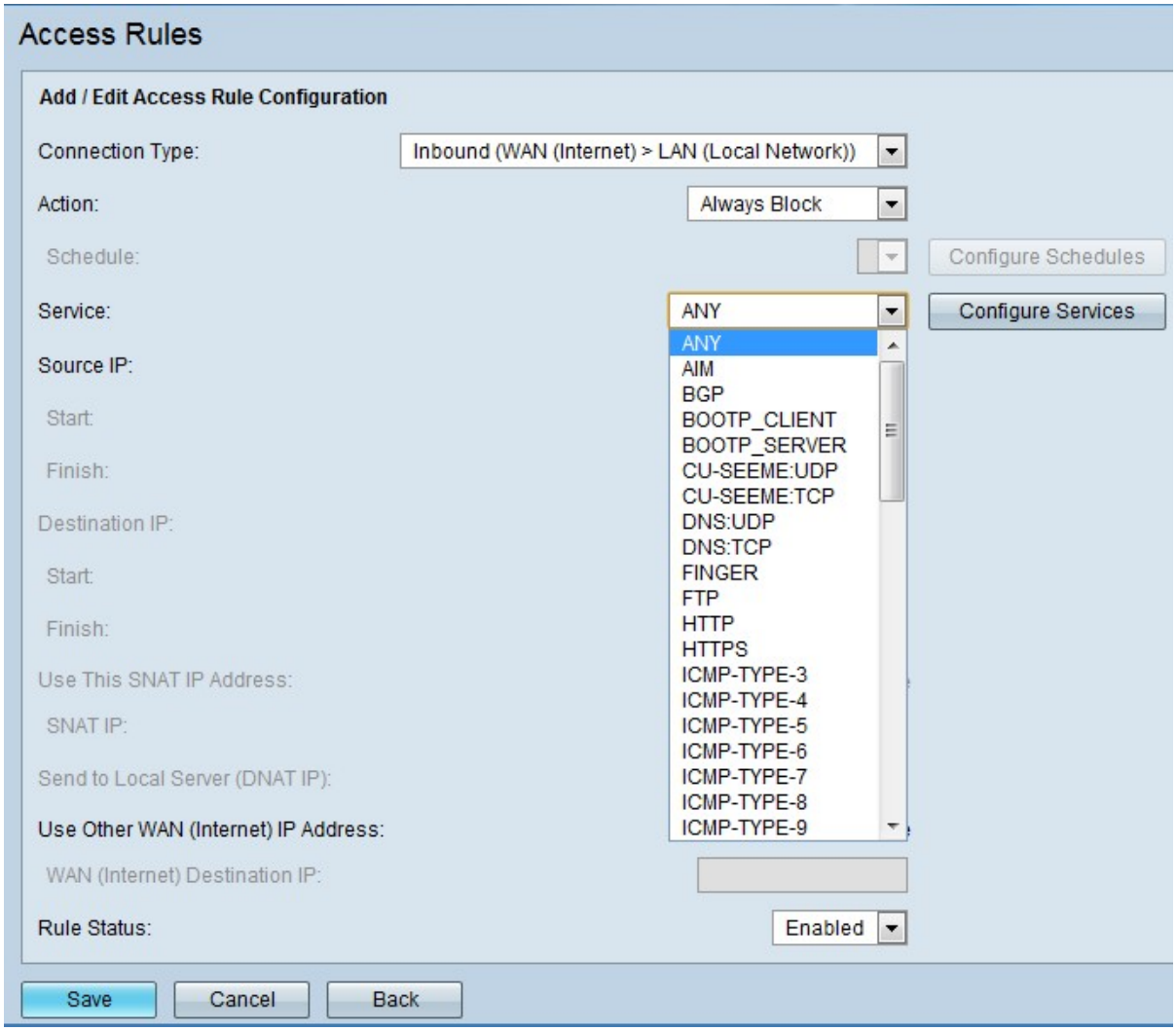


第 3 步：在**连接类型**下拉列表，请选择将由规则包括数据流的适当的目的地。

- 入站—这是来自互联网(广域网)的数据流到内部网络(LAN)。
- outbound —这是来自内部网络(LAN)的数据流到互联网(广域网)。

步骤4.从**动作**下拉列表选择适当的选项。

- 总是块—这永远将否决或阻塞所选的数据流。
- 总是请准许—这永远将允许或允许所选的数据流。
- 由日程表的块否则准许—这根据日程表拦截数据流所选类型。从**日程表**下拉列表选择适当的日程表。
- 由日程表块否则允许—这根据日程表允许数据流所选类型。从**日程表**下拉列表选择适当的日程表。



步骤5.选择适当的服务从**服务**下拉列表允许或阻拦。选择**ANY**，如果规则将适用于所有应用程序和服务或者选择根据需求需要的服务。

第6.步。在来源IP字段请输入防火墙规则将适用的IP地址。

- •其中任一—此规则将适用于起源从所有IP地址于本地网络的数据流。
- •单个地址—此规则将适用于起源从单个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—此规则将适用于起源的数据流从指定的IP地址的范围。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。

第 7 步：对于入站防火墙的配置请访问规则配置以下：

- •目的地网络地址转换—这映射一个公共IP地址用在本地网络的专用IP地址。输入主机在本地网络的机器的IP地址服务器发送到当地服务器领域。
- •请使用其他广域网(互联网) IP地址—多NAT的路由器支援(网络地址转换)。如果检查**使用其他广域网(互联网) IP地址Enable复选框**那么被输入将其aliased公共IP地址用于的IP地址从互联网访问您的本地网络。

选择*启用*对enable (event)规则或*失效*禁用规则和enable (event)从**规则状态**以后请丢弃淹没列表。

outbound防火墙访问规则的配置：

输入防火墙规则在目的地IP字段将适用的IP地址：

•其中任一—此规则将适用于去所有IP地址的数据流。
•单个地址—此规则将适用于去单个IP地址的数据流。在Start字段输入IP地址。
•地址范围—此规则将适用于去指定的范围的数据流IP地址。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。

安全网络地址转换(SNAT)可以通过检查**使用此SNAT IP地址Enable复选框**然后输入适当的IP地址配置映射在专用网络的一个公共IP地址在SNAT IP字段。

选择启用对enable (event)规则或失效禁用规则和enable (event)从**规则状态**以后请丢弃淹没列表。

步骤8.点击**“Save”**保存设置。