多个公共IP的配置在非敏感区域(DMZ) RV042、RV042G和RV082 VPN路由器的

客观

非敏感区域(DMZ)是组织的一个内部网络，安排可用一个不信任的网络。根据安全， DMZ下跌在委托的和不信任的网络之间。DMZ的维护帮助改进安全ofto组织的内部网络。当访问控制表(ACL)一定对接口时，其访问控制元素(ACE)规则被运用于到达该接口的信息包。不匹配其中任一在访问控制表的ACE的信息包被匹配对动作是丢弃不匹配信息包的默认规则。

本文目标将显示您如何配置DMZ端口允许多个公共IP地址和定义IP的访问控制表(ACL)在路由器设备。

可适用的设备

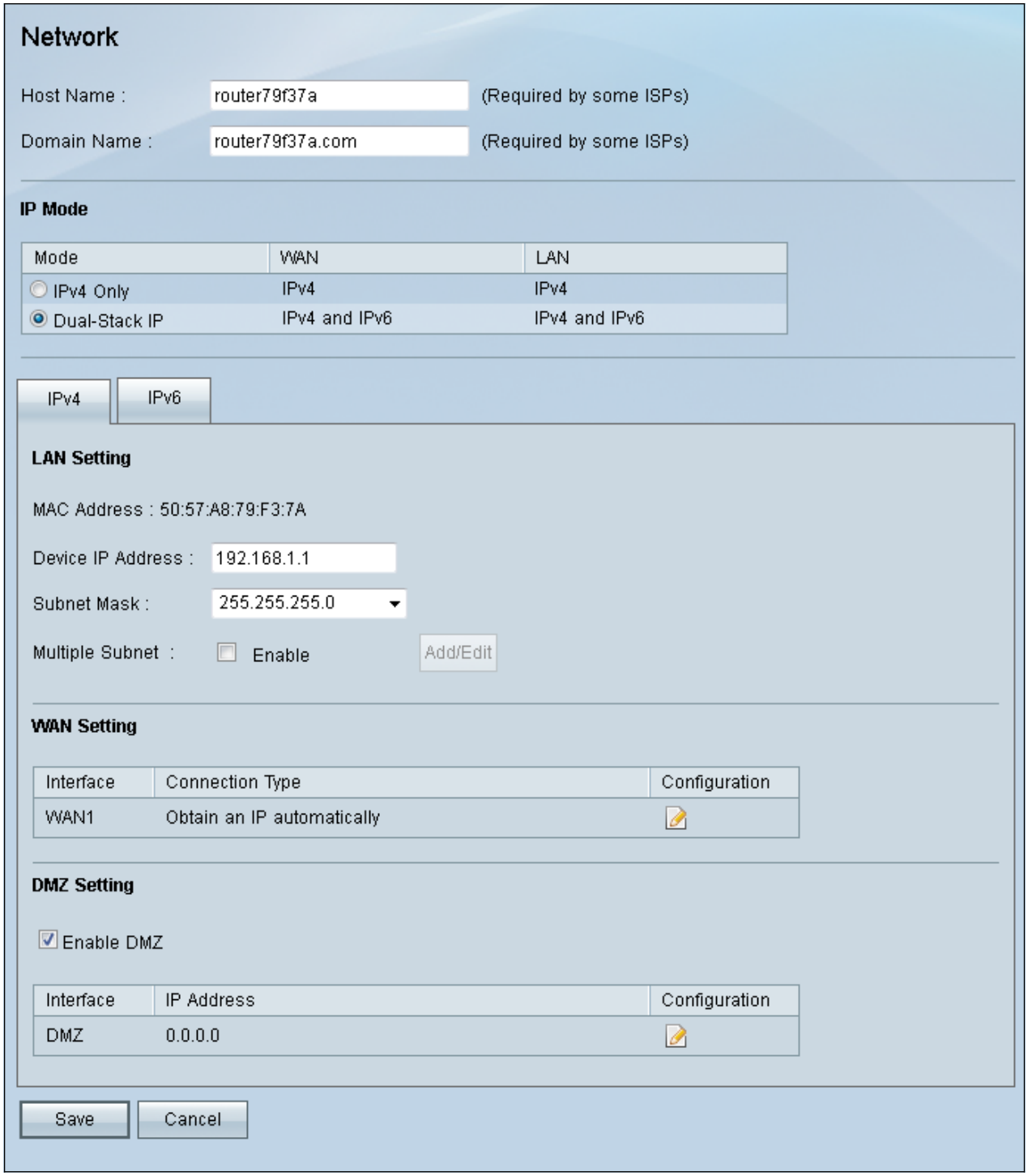
- RV042
- RV042G
- RV082

软件版本

- v4.2.2.08

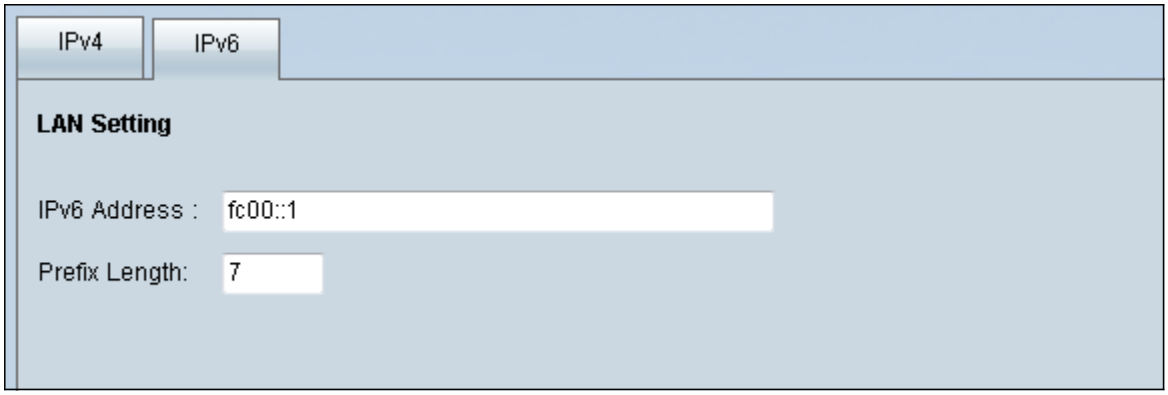
非军事区配置

步骤1.日志到Web配置实用工具页里和选择**设置>网络**。*网络*页打开：



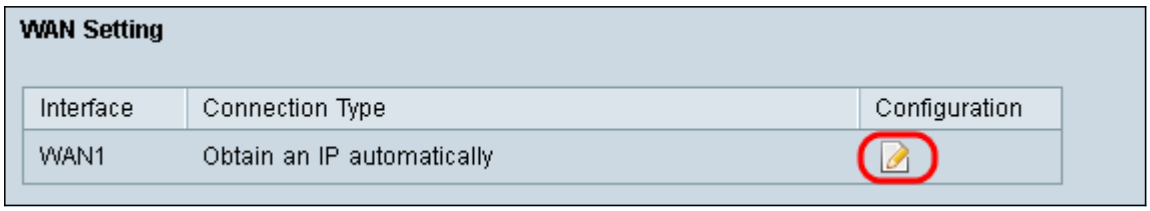
Step 2.在*Mode字段的IP中，请*点击**Dual-Stack IP**单选按钮对enable (event) IPv6地址的配置。

步骤3.点击位于*LAN的*IPv6选项*setting字段*能配置在IPv6地址的DMZ。

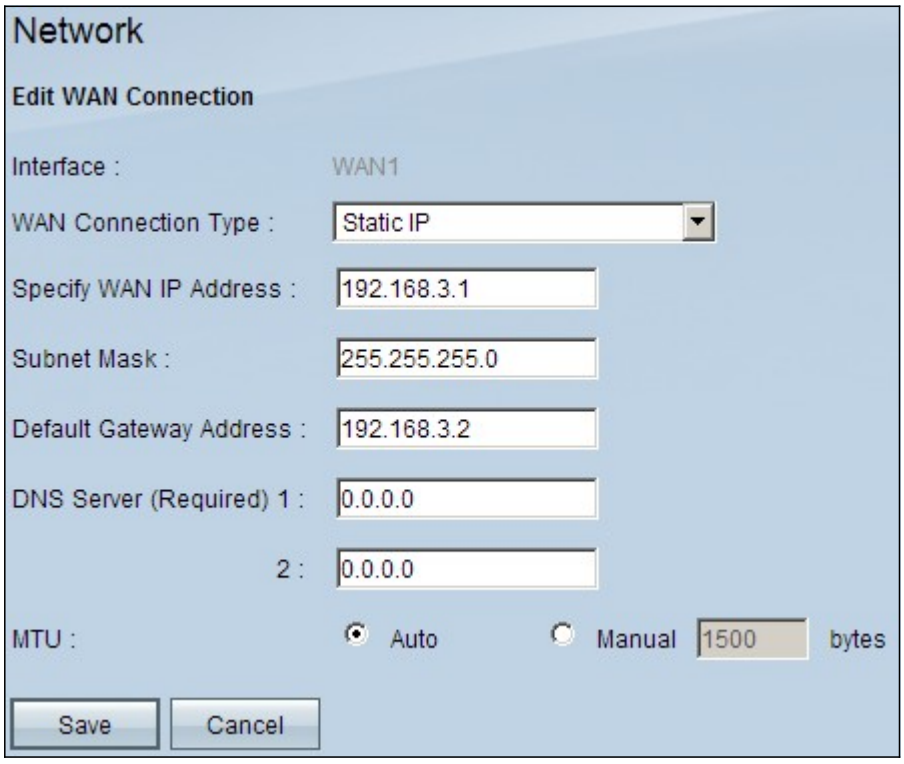


步骤下来4.Scroll对设置区域的DMZ和点击**DMZ**复选框对enable (event) DMZ

第 5 步：在*setting字段的广域网中请*点击**编辑按钮**编辑WAN1设置的IP静态。



*网络*页打开：



步骤6.从*WAN连接类型*下拉列表选择**静态IP**。

步骤7.输入在*IP Address字段的指定广域网的系统汇总页*显示的广域网IP地址。

步骤8.输入子网掩码地址在*子网掩码*字段。

步骤9.输入默认网关地址在*默认网关地址*字段。

步骤10.输入在*DNS服务器的系统汇总页*显示的DNS服务器地址*(需要) 1个*字段。

Note: DNS服务器地址2是可选的。

步骤11.选择最大传输单元(MTU)是**自动**或**指南**。如果选择指南请输入手工的MTU的字节。

步骤12。点击**Save选项**保存您的设置。

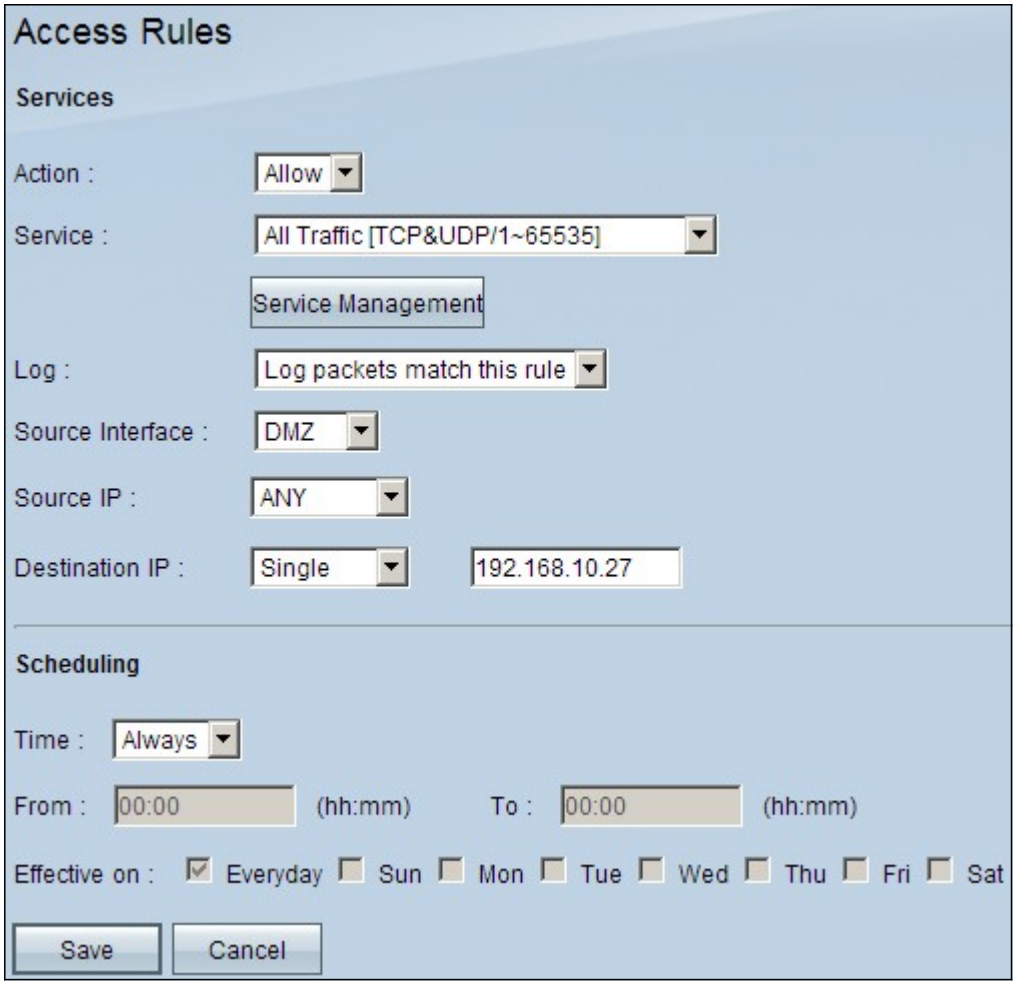
ACL定义

步骤1.日志到Web配置实用工具页里和选择**防火墙>Access规则**。*访问规则*页打开：

Note:当您进入时*访问规定*默认访问规则不可能被编辑的页。

步骤2.点击**Add按钮**增加一个新的访问规则。

*访问规则*页当前将显示*服务*和*安排*地区的选项。



步骤3.选择从*动作*下拉列表**允许**允许服务。

步骤4.从*服务*下拉列表选择**所有数据流[TCP&UDP/1~65535]**到enable (event) DMZ的所有服务。

步骤5.选择**日志信息包匹配**从*日志*下拉列表的**此规则**选择匹配访问规则仅的日志。

步骤6.从*源接口*下拉列表选择**DMZ**。这是访问规则的来源。

步骤7.从*来源IP*下拉列表选择其中**任一**。

步骤8.从*目的地IP*下拉列表选择**单个**。

步骤9.输入将提供的目的地的IP地址在*目的地IP*字段的访问规则。

第10.步。在*安排*地区中从*时间*下拉列表**总是请**选择一直做访问规则激活。

Note:如果从*时间*下拉列表**总是**选择，默认情况下访问规则将设置对**每天**在*有效在*字段。

Note:您能通过选择**间隔**选择特定时间时间间隔(哪些访问规则是活跃的)从*时间*下拉列表。然后，您能选择您希望访问规则是活跃的从*有效在*复选框的日。

步骤11.点击**"Save"**保存您的设置。

Note:如果弹出窗口出现请按'好'增加另一个访问规则或者按'取消'返回到访问规则页。

您在上一步创建的访问规则当前显示

步骤12。点击**Edit图标**编辑被创建的访问规则。

第13步。点击**Delete图标**删除被创建的访问规则。