



SLK-R620

黑白名单使用说明

SERIALLINK CONFIDENTIAL

目录

简介.....	3
一、 防火墙功能.....	4
1.1. 页面.....	4
1.2. 添加转发规则.....	8
二、 添加白名单.....	10
2.1. 测试部分#1.....	10
2.1.1. 配置规则.....	10
2.1.2. 测试结果.....	13
2.2. 测试部分#2.....	15
2.2.1. 配置规则.....	15
2.2.2. 测试结果.....	20

简介

通过配置防火墙规则可以实现路由器的黑名单功能。要控制下级设备的上网功能，需要按照一定的规制配置才能使其生效。

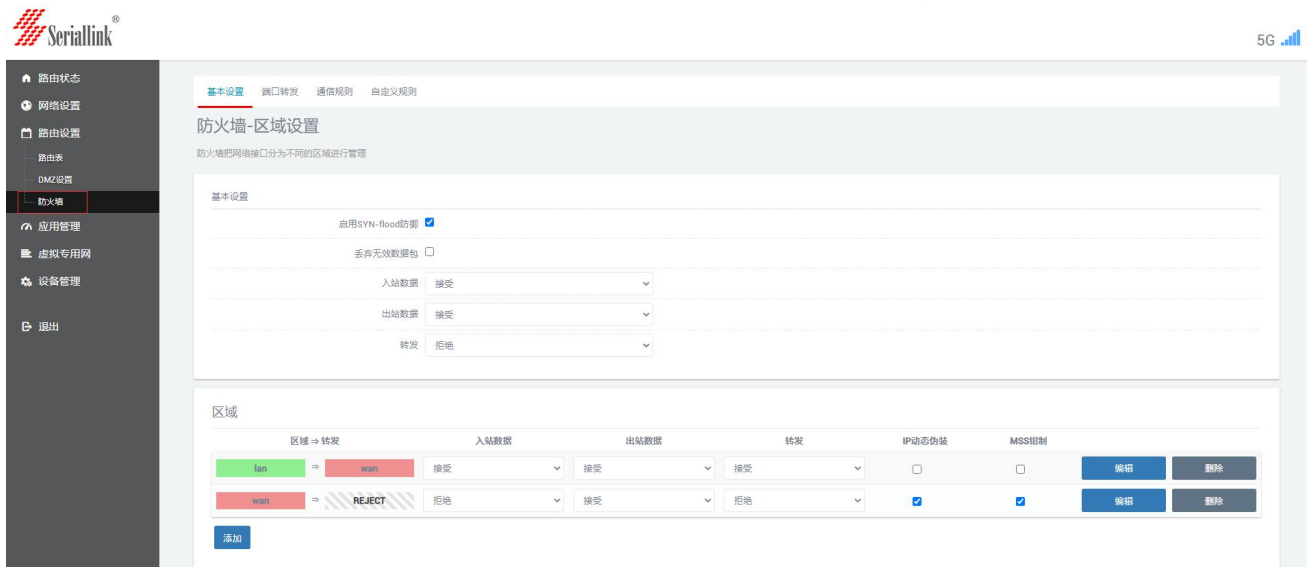
以下部分介绍如何配置黑白名单实现上网自由。

一、防火墙功能

1.1. 页面

① 【路由设置】 ---> 【防火墙】

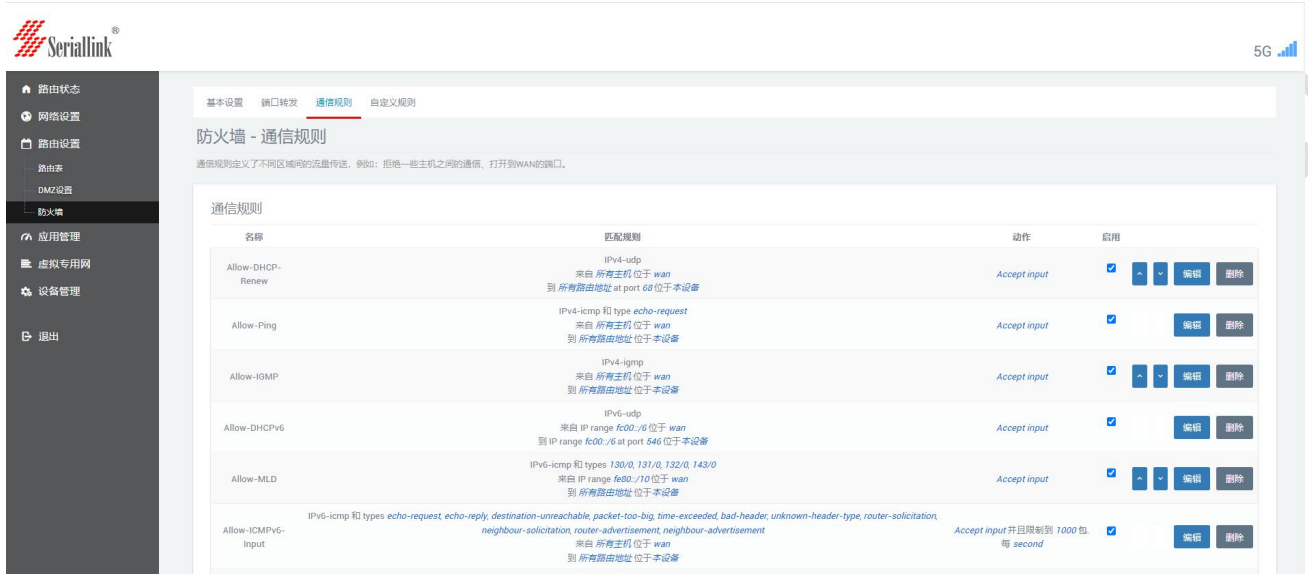
在这里，可以建立包含通用防火墙配置、端口转发和黑白名单等规则。其中，接收代表允许数据通过，拒绝和丢弃代表不允许数据通过；进站数据表示从外部进入 SLK-R620 的数据，出站数据表示从 SLK-R620 出去外部的数据。Lan 区域包含了 SLK-R620 本身、Lan 口的下级设备，wan 区域包含了 4G/5G 和 VPN。



区域 -> 转发	进站数据	出站数据	转发	IP动态伪装	MSS控制	操作
lan -> wan	接受	接受	接受	<input type="checkbox"/>	<input type="checkbox"/>	编辑 删除
wan -> REJECT	拒绝	接受	拒绝	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	编辑 删除

② 【路由设置】 ---> 【防火墙】 ---> 【通信规则】

需要设置路由黑白名单时，可通过添加通信规则实现。需要注意的是，在保留基本设置默认不变的情况下，仅通过【通信规则】添加规则实现黑白名单也是可以生效的。



Seriallink 5G

基本设置 端口转发 通信规则 自定义规则

防火墙 - 通信规则

通信规则定义了不同区域间的流量传递。例如：拒绝一些主机之间的通信，打开到WAN的端口。

名称	匹配规则	动作	启用
Allow-DHCP-Renew	IPv4-udp 来自 所有主机 位于 wan 到 所有路由地址 位于本设备	Accept input	<input checked="" type="checkbox"/>
Allow-Ping	IPv4-icmp 和 type echo-request 来自 所有主机 位于 wan 到 所有路由地址 位于本设备	Accept input	<input checked="" type="checkbox"/>
Allow-IGMP	IPv4-igmp 来自 所有主机 位于 wan 到 所有路由地址 位于本设备	Accept input	<input checked="" type="checkbox"/>
Allow-DHCPv6	IPv6-udp 来自 IP range fc00::/6 位于 wan 到 IP range fc00::/6 位于本设备	Accept input	<input checked="" type="checkbox"/>
Allow-MLD	IPv6-icmp 和 types 130/0, 131/0, 132/0, 143/0 来自 IP range fe80::/10 位于 wan 到 所有路由地址 位于本设备	Accept input	<input checked="" type="checkbox"/>
Allow-ICMPv6-Input	IPv6-icmp 和 types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type, router-solicitation, neighbour-solicitation, router-advertisement, neighbour-advertisement 来自 所有主机 位于 wan 到 所有路由地址 位于本设备	Accept input 并且限制到 1000 包/秒	<input checked="" type="checkbox"/>

③【路由设置】---->【防火墙】---->【通信规则】---->【通信规则列表】

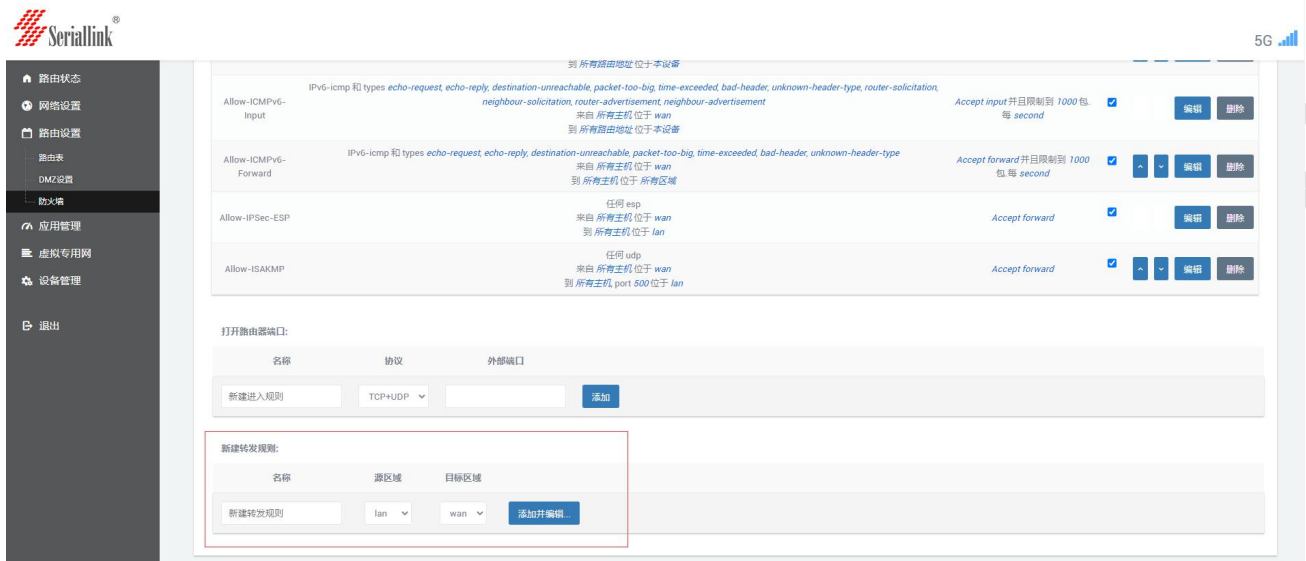
可通过通信规则列表查看得到已添加的通信规则。要注意，**SLK-R620** 默认具备正常运行所需的通讯规则，这些规则不影响后续的黑白名单配置和生效，务必不要删除。

通信规则 **在不清楚这些规则的定义下，务必不要删除!!!**

名称	匹配规则	动作	启用
Allow-DHCP-Renew	IPv4-udp 来自 所有主机 位于 wan 到 所有路由地址 at port 68 位于本设备	Accept input	<input checked="" type="checkbox"/> ↑ ↓ 编辑 删除
Allow-Ping	IPv4-icmp 和 type echo-request 来自 所有主机 位于 wan 到 所有路由地址 位于本设备	Accept input	<input checked="" type="checkbox"/> 编辑 删除
Allow-IGMP	IPv4-igmp 来自 所有主机 位于 wan 到 所有路由地址 位于本设备	Accept input	<input checked="" type="checkbox"/> ↑ ↓ 编辑 删除
Allow-DHCPv6	IPv6-udp 来自 IP range fc00::/6 位于 wan 到 IP range fc00::/6 at port 546 位于本设备	Accept input	<input checked="" type="checkbox"/> 编辑 删除
Allow-MLD	IPv6-icmp 和 types 130/0, 131/0, 132/0, 143/0 来自 IP range fe80::/10 位于 wan 到 所有路由地址 位于本设备	Accept input	<input checked="" type="checkbox"/> ↑ ↓ 编辑 删除
Allow-ICMPv6-Input	IPv6-icmp 和 types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type, router-solicitation, neighbour-solicitation, router-advertisement, neighbour-advertisement 来自 所有主机 位于 wan 到 所有路由地址 位于本设备	Accept input 并且限制到 1000 包/每 second	<input checked="" type="checkbox"/> 编辑 删除
Allow-ICMPv6-Forward	IPv6-icmp 和 types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type 来自 所有主机 位于 wan 到 所有主机 位于 所有区域	Accept forward 并且限制到 1000 包/每 second	<input checked="" type="checkbox"/> ↑ ↓ 编辑 删除
Allow-IPSec-ESP	任何 esp 来自 所有主机 位于 wan 到 所有主机 位于 lan	Accept forward	<input checked="" type="checkbox"/> 编辑 删除
Allow-ISAKMP	任何 udp 来自 所有主机 位于 wan 到 所有主机, port 500 位于 lan	Accept forward	<input checked="" type="checkbox"/> ↑ ↓ 编辑 删除

④【路由设置】---->【防火墙】---->【通信规则】---->【新建转发规则】

页面往下可以找到【新建转发规则】，通过建立转发规则，便可以实现黑白名单功能。



The screenshot shows the Seriallink web interface for configuring firewall rules. The left sidebar contains navigation options: 路由状态, 网络设置, 路由设置, 路由表, DMZ设置, 防火墙, 应用管理, 虚拟专用网, 设备管理, and 退出. The main content area displays a list of existing rules and a section for creating new rules.

名称	协议	外部端口
新建进入规则	TCP+UDP	

新建转发规则:

名称	源区域	目标区域
新建转发规则	lan	wan

1.2. 添加转发规则

① 点击【添加并编辑】

新建转发规则:

名称	源区域	目标区域	
新建转发规则	lan	wan	添加并编辑...

② 在跳转的新页面内，自定义规则【名称】

③ 【协议】选择【任何】

④ 【源地址】选择或填写允许/禁止通过 SLK-R620 网络的 IP 地址

⑤ 【动作】选择【接收】、【丢弃】或【拒绝】

【接收】：允许该 IP 地址通过 SLK-R620 网络

【丢弃】和【拒绝】：禁止该 IP 地址通过 SLK-R620 网络

⑥ 点击【保存并应用】

基本设置 端口转发 通信规则 自定义规则

防火墙 - 通信规则 - (未命名规则)

本页面可以更改通信规则的高级设置，比如：需匹配的源主机和目标主机。

Rule is enabled 禁用

名称	自定义名称
限制地址	IPv4 和 IPv6
协议	任何
匹配ICMP类型	any
源区域	lan: lan
源MAC地址	所有
源地址	192.168.2.59 (40:8D:5C:7A:F3:F7)
源端口	所有
目标区域	wan: wan, wan6, modem, l2tp, pptp, openvpn, gre, gre_static
目标地址	所有
目标端口	所有

协议	任何
匹配ICMP类型	any
源区域	lan: lan: ***
源MAC地址	所有
源地址	192.168.2.59 (40:8D:5C:7A:F3:F7)
源端口	所有
目标区域	wan: wan: *** wan6: *** modem: *** l2tp: *** pptp: *** openvpn: *** gre: () gre_static: ***
目标地址	所有
目标端口	所有
动作	接受
附加参数	

传递到iptables的额外参数。小心使用!

[返回至概况](#)
[保存并应用](#)

⑦在跳转回到通信规则的页面上，可以找到刚添加的转发规则，这表示规则添加成功并生效。

Allow-Ping	IPv4-icmp 和 type <i>echo-request</i> 来自 所有主机 位于 wan 到 所有路由地址 位于本设备	Accept input	<input checked="" type="checkbox"/>	编辑 删除
Allow-IGMP	IPv4-igmp 来自 所有主机 位于 wan 到 所有路由地址 位于本设备	Accept input	<input checked="" type="checkbox"/>	编辑 删除
Allow-DHCPv6	IPv6-udp 来自 IP range <i>fc00::/6</i> 位于 wan 到 IP range <i>fc00::/6</i> at port 546 位于本设备	Accept input	<input checked="" type="checkbox"/>	编辑 删除
Allow-MLD	IPv6-icmp 和 types <i>130/0, 131/0, 132/0, 143/0</i> 来自 IP range <i>fe80::/10</i> 位于 wan 到 所有路由地址 位于本设备	Accept input	<input checked="" type="checkbox"/>	编辑 删除
Allow-ICMPv6-Input	IPv6-icmp 和 types <i>echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type, router-solicitation, neighbour-solicitation, router-advertisement, neighbour-advertisement</i> 来自 所有主机 位于 wan 到 所有路由地址 位于本设备	Accept input 并且限制到 1000 包/每 second	<input checked="" type="checkbox"/>	编辑 删除
Allow-ICMPv6-Forward	IPv6-icmp 和 types <i>echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type</i> 来自 所有主机 位于 wan 到 所有主机 位于 所有区域	Accept forward 并且限制到 1000 包/每 second	<input checked="" type="checkbox"/>	编辑 删除
Allow-IPSec-ESP	任何 esp 来自 所有主机 位于 wan 到 所有主机 位于 lan	Accept forward	<input checked="" type="checkbox"/>	编辑 删除
Allow-ISAKMP	任何 udp 来自 所有主机 位于 wan 到 所有主机, port 500 位于 lan	Accept forward	<input checked="" type="checkbox"/>	编辑 删除
自定义名称	任何 交通 来自 IP 192.168.2.59 位于 lan 到 所有主机 位于 wan	Accept forward	<input checked="" type="checkbox"/>	编辑 删除

二、添加白名单

设定 SLK-R620 的 IP 地址为 192.168.2.1，下接两台 PC 分别是 PC1:192.168.2.59 和 PC2:192.168.69；下面展示如何添加【白名单】并记录测试结果。分两部分，部分#1，允许 PC1 通过 SLK-R620 访问外网，不允许 PC2 通过 SLK-R620 访问外网，测试过程和结果记录在 2.1.中；部分#2，允许 PC1 通过 SLK-R620 仅可以访问公网 IP:106.55.45.169 和 118.26.68.91，测试过程和结果记录在 2.2.中。

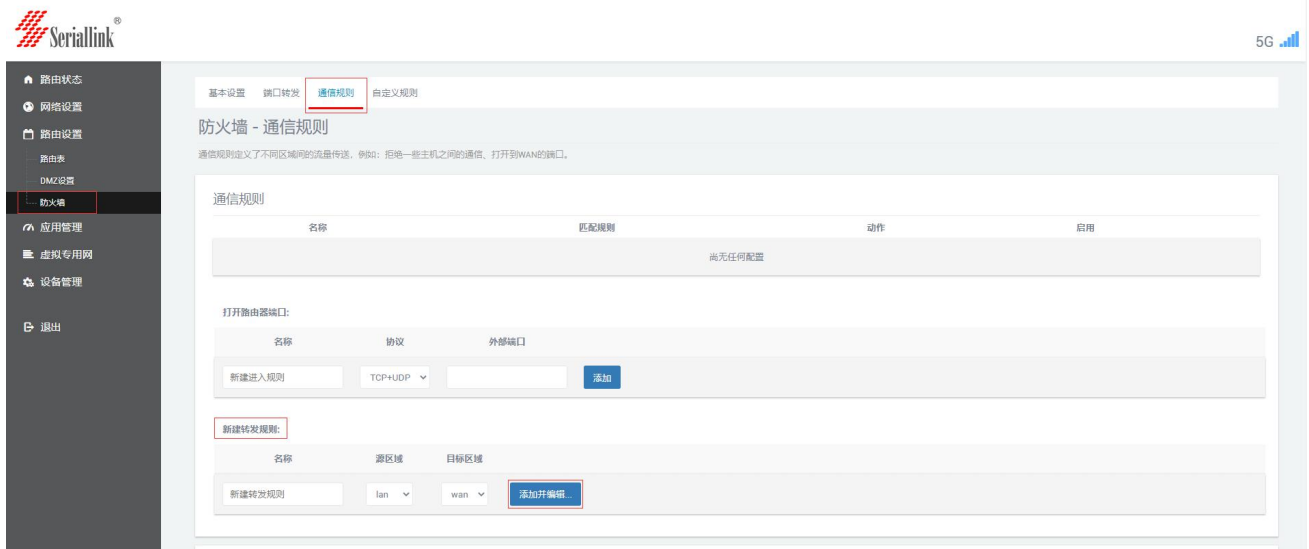
2.1. 测试部分#1

2.1.1. 配置规则

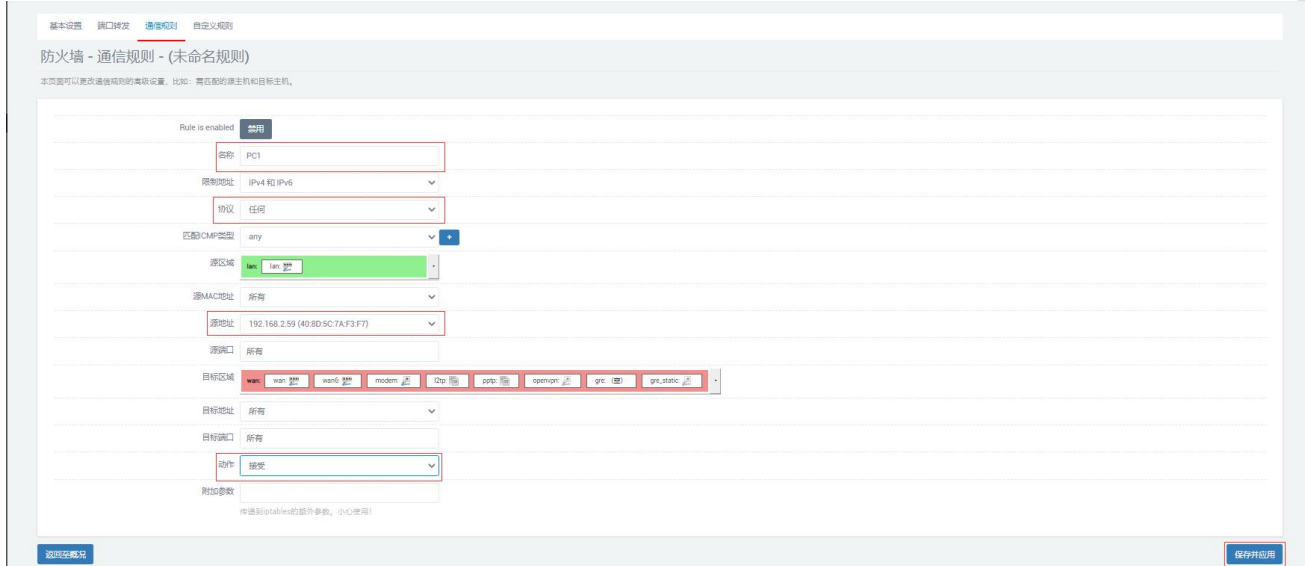
1) 允许某个设备通过 SLK-R620 网络

① 【路由设置】-- 【防火墙】-- 【通信规则】

往下找到【新建转发规则】，点击【添加并编辑】



- ②在跳转的新页面内，自定义规则【名称】
- ③【协议】选择【任何】
- ④【源地址】选择 PC1 的 IP 地址：192.168.2.59
- ⑤【动作】选择【接受】，允许 PC1 通过 SLK-R620 网络
- ⑥点击【保存并应用】



基本设置 端口转发 通信规则 自定义规则

防火墙 - 通信规则 - (未命名规则)

本页可以更改通信规则的高级设置。比如：需配置源主机和目标主机。

Rule is enabled

名称 PC1

限制地址 IPv4 和 IPv6

协议 任何

匹配CIDR类型 any

源区域 lan

源MAC地址 所有

源地址 192.168.2.59 (40:8D:5C:7A:F3:F7)

源端口 所有

目标区域 wan

目标地址 所有

目标端口 所有

动作 接受

附加参数

返回功能页 保存并应用

⑦在跳转回到通信规则的页面上，可以找到刚添加的转发规则，这表示规则添加成功并生效。

通信规则

名称	匹配规则	动作	启用			编辑	删除
PC1	任何 交通 来自 IP 192.168.2.59 位于 lan 到 所有主机 位于 wan	Accept forward	<input checked="" type="checkbox"/>	^	v	编辑	删除

2) 禁止其他设备通过 SLK-R620 网络

注意，步骤 1) 仅是实现了允许 PC1 通过 SLK-R620 网络，下面还需要添加规则以禁止除 PC1 外的设备通过 SLK-R620 网络。

①同样找到【新建转发规则】，点击【添加并编辑】



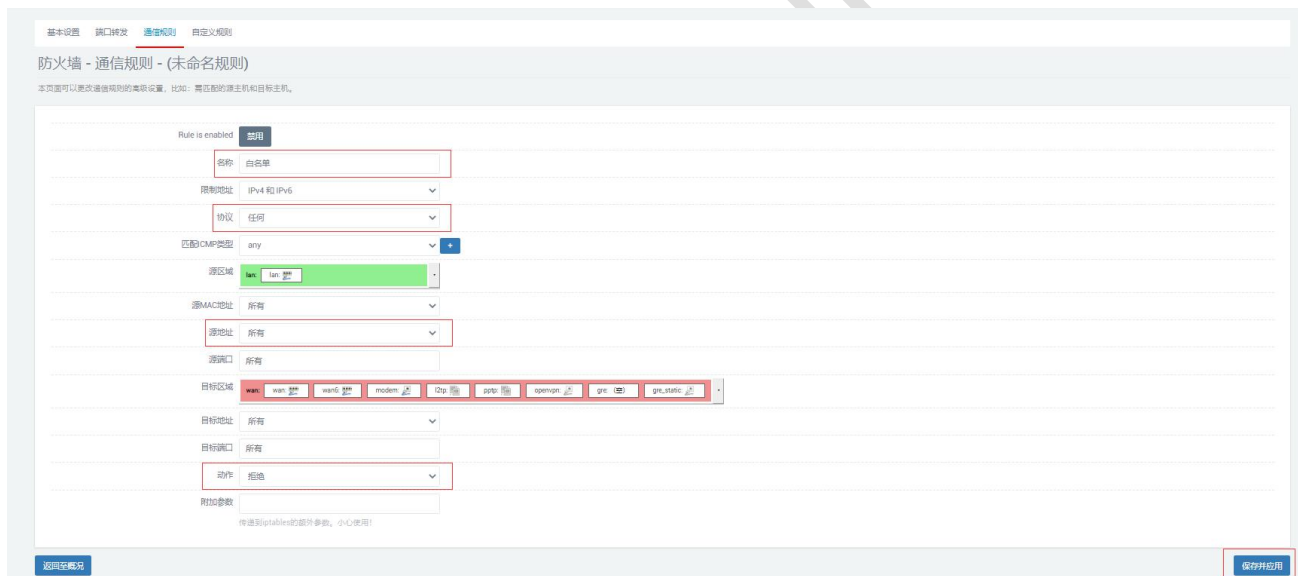
②在跳转的新页面内，自定义规则【名称】

③【协议】选择【任何】

④【源地址】选择【任何】

⑤【动作】选择【拒绝】，禁止其他地址通过 SLK-R620 网络

⑥点击【保存并应用】



⑦在跳转回到通信规则的页面上，可以找到刚添加的两条转发规则，这表示白名单规则添加成功。



注意：需要允许不止一个设备通过 SLK-R620 网络时（如下图，允许 PC1 和 PC3 通过 SLK-R620，禁止其他 PC 通过 SLK-R620 网络），可以添加多个允许不同设备通过 SLK-R620 网络的转发规则，然后点击规则列表的排序按钮（如下图红圈中的图标），调整规则顺序，将下图的【白名单】规则调整至列表末端，并点击【保存并应用】：



2.1.2. 测试结果

①PC1 上网络配置如下



网络连接详细信息

网络连接详细信息(D):

属性	值
连接特定的 DNS 后缀	lan
描述	Realtek PCIe GbE Family Controller #
物理地址	40-8D-5C-7A-F3-F7
已启用 DHCP	否
IPv4 地址	192.168.2.59
IPv4 子网掩码	255.255.255.0
IPv4 默认网关	192.168.2.1
IPv4 DNS 服务器	114.114.114.114 8.8.8.8

②PC1 测试结果

```
C:\Users\Administrator>ping www.baidu.com

正在 Ping www.a.shifen.com [14.215.177.38] 具有 32 字节的数据:
来自 14.215.177.38 的回复: 字节=32 时间=9ms TTL=54
来自 14.215.177.38 的回复: 字节=32 时间=9ms TTL=54
来自 14.215.177.38 的回复: 字节=32 时间=9ms TTL=54
来自 14.215.177.38 的回复: 字节=32 时间=9ms TTL=54

14.215.177.38 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 9ms, 最长 = 9ms, 平均 = 9ms
```

③PC2 上网络配置如下



②PC2 测试结果

```
C:\Users\Administrator>ping www.baidu.com

正在 Ping www.a.shifen.com [14.215.177.38] 具有 32 字节的数据:
来自 192.168.2.1 的回复: 无法连接到端口。
来自 192.168.2.1 的回复: 无法连接到端口。
来自 192.168.2.1 的回复: 无法连接到端口。
来自 192.168.2.1 的回复: 无法连接到端口。

14.215.177.38 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
```

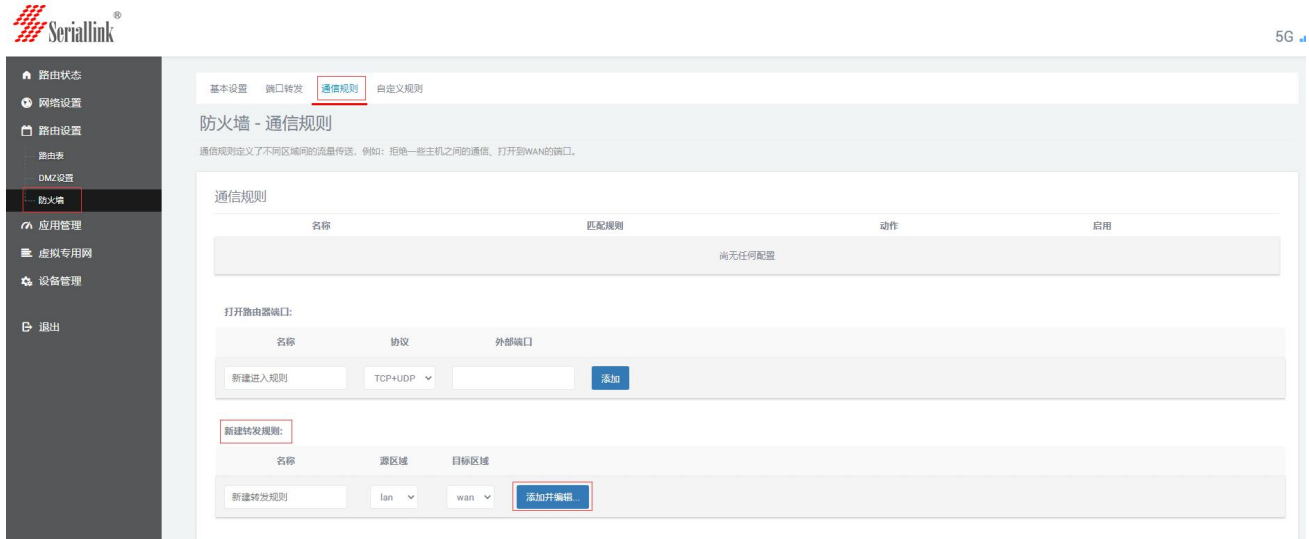
2.2. 测试部分#2

2.2.1. 配置规则

1) 添加允许 PC1:192.168.2.59 访问 106.55.45.169 规则

① 【路由设置】 -- 【防火墙】 -- 【通信规则】

往下找到【新建转发规则】，点击【添加并编辑】



②在跳转的新页面内，自定义规则【名称】

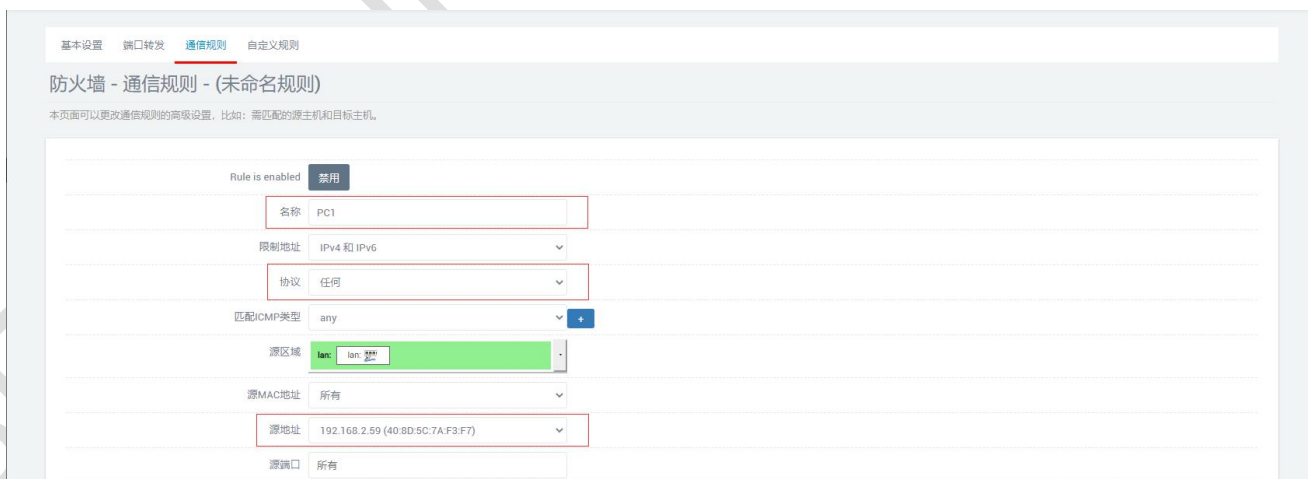
③【协议】选择【任何】

④【源地址】选择 PC1 的 IP 地址：192.168.2.59

⑤【目标地址】填写 106.55.45.169

⑥【动作】选择【接收】，允许 PC1 通过 SLK-R620 网络访问 106.55.45.169

⑦点击【保存并应用】



目标区域 wan wan6 modem l2tp pptp openvpn gre gre_static

目标地址 106.55.45.169

目标端口 所有

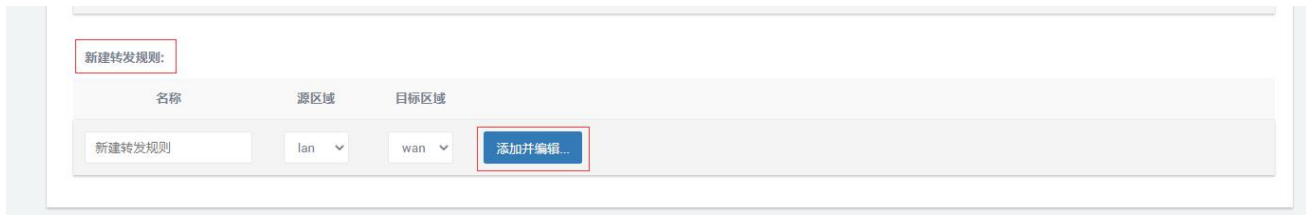
动作 接受

附加参数
传递到iptables的额外参数。小心使用!

返回至概况 保存并应用

2) 添加禁止 PC1 访问其他外部 IP 地址规则

① 同样找到【新建转发规则】，点击【添加并编辑】



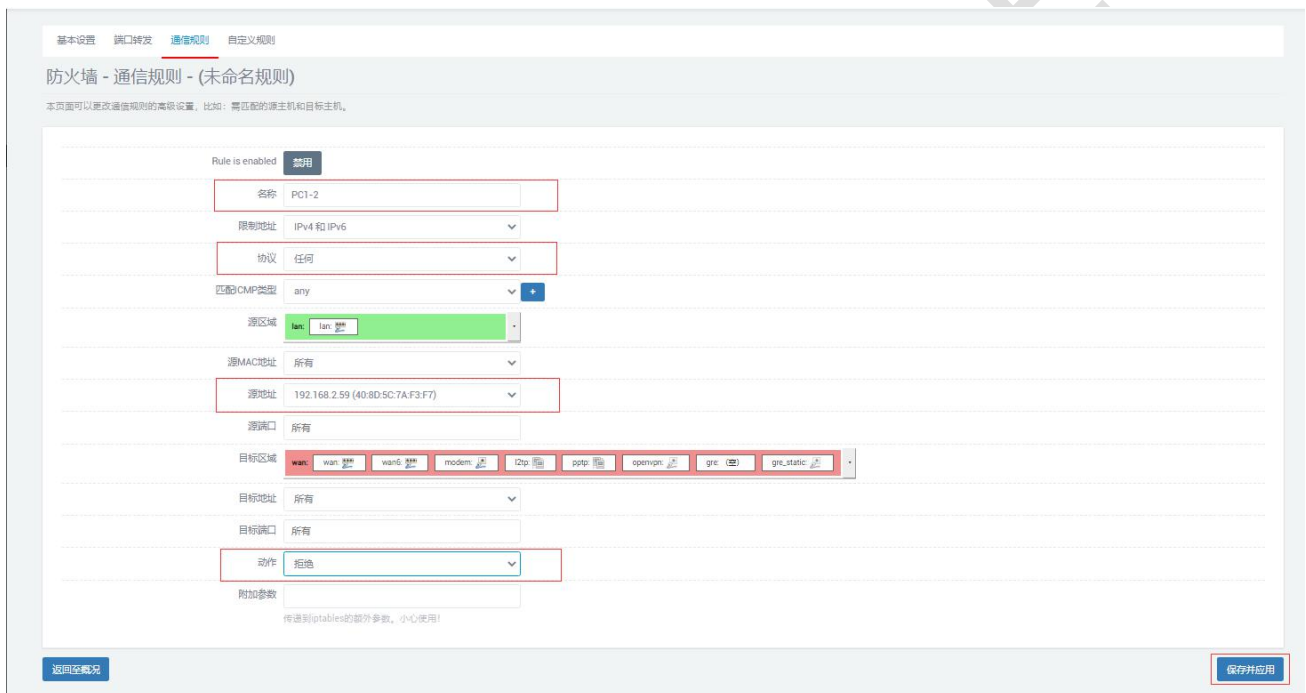
② 在跳转的新页面内，自定义规则【名称】

③ 【协议】选择【任何】

④ 【源地址】选择 PC1 的 IP 地址：192.168.2.59

⑤ 【动作】选择【拒绝】，禁止 PC1 通过 SLK-R620 网络访问其他外部 IP 地址

⑥ 点击【保存并应用】



3) 禁止其他设备通过 SLK-R620 网络

注意，步骤 1) 和 2) 仅是实现了允许 PC1 通过 SLK-R620 网络访问某个外部 IP，下面还需要添加规则以禁止除 PC1 外的设备通过 SLK-R620 网络。

① 同样找到【新建转发规则】，点击【添加并编辑】



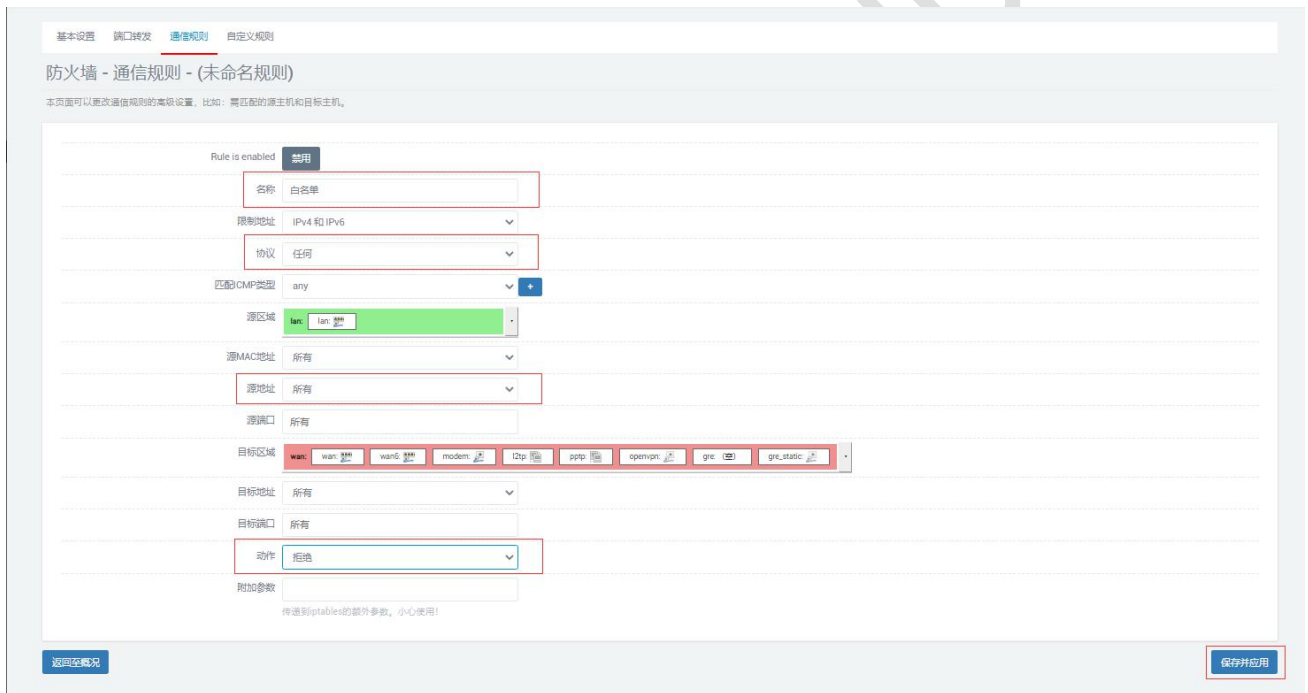
② 在跳转的新页面内，自定义规则【名称】

③ 【协议】选择【任何】

④ 【源地址】选择【任何】

⑤ 【动作】选择【拒绝】，禁止其他地址通过 SLK-R620 网络

⑥ 点击【保存并应用】



4) 最终规则列表如下

【PC1】和【PC1-2】规则表示仅允许 PC1 通过 SLK-R620 网络访问 106.55.45.169,禁止 PC1 访问其他外部 IP,【白名单】规则禁止其他设备通过 SLK-R620 网络访问外网。

名称	匹配规则	动作	启用				
PC1	任何交通 来自 IP 192.168.2.59 位于 lan 到 IP 106.55.45.169 位于 wan	Accept forward	<input checked="" type="checkbox"/>	↑	↓	编辑	删除
PC1-2	任何交通 来自 IP 192.168.2.59 位于 lan 到 所有主机 位于 wan	Refuse forward	<input checked="" type="checkbox"/>			编辑	删除
白名单	任何交通 来自 所有主机 位于 lan 到 所有主机 位于 wan	Refuse forward	<input checked="" type="checkbox"/>	↑	↓	编辑	删除

注意：需要允许设备通过 SLK-R620 网络访问不止一个外部 IP 时（如下图，允许 PC1 通过 SLK-R620 网络访问 106.55.45.169 和 118.26.68.91，禁止其访问其他外部 IP 和禁止其他设备通过 SLK-R620 访问外部网络），可以添加多个允许该设备通过 SLK-R620 网络的转发规则，然后点击规则列表的排序按钮（如下图红圈中的图标），调整规则顺序，将下图的【PC1-禁止】调整至列表倒数第二位和【白名单】规则调整至列表末端，并点击【保存并应用】：

名称	匹配规则	动作	启用				
PC1-允许1	任何交通 来自 IP 192.168.2.59 位于 lan 到 IP 106.55.45.169 位于 wan	Accept forward	<input checked="" type="checkbox"/>	↑	↓	编辑	删除
PC1-允许2	任何交通 来自 IP 192.168.2.59 位于 lan 到 IP 118.26.68.91 位于 wan	Accept forward	<input checked="" type="checkbox"/>			编辑	删除
PC1-拒绝	任何交通 来自 IP 192.168.2.59 位于 lan 到 所有主机 位于 wan	Refuse forward	<input checked="" type="checkbox"/>	↑	↓	编辑	删除
白名单	任何交通 来自 所有主机 位于 lan 到 所有主机 位于 wan	Refuse forward	<input checked="" type="checkbox"/>			编辑	删除

2.2.2. 测试结果

①PC1 上网络配置如下

属性	值
连接特定的 DNS 后缀	
描述	Realtek PCIe GbE Family Controller #
物理地址	40-8D-5C-7A-F3-F7
已启用 DHCP	否
IPv4 地址	192.168.2.59
IPv4 子网掩码	255.255.255.0
IPv4 默认网关	192.168.2.1
IPv4 DNS 服务器	114.114.114.114 8.8.8.8

②PC1 测试结果

```
C:\Users\Administrator>ping 106.55.45.169

正在 Ping 106.55.45.169 具有 32 字节的数据:
来自 106.55.45.169 的回复: 字节=32 时间=7ms TTL=51
来自 106.55.45.169 的回复: 字节=32 时间=7ms TTL=51
来自 106.55.45.169 的回复: 字节=32 时间=7ms TTL=51
来自 106.55.45.169 的回复: 字节=32 时间=7ms TTL=51

106.55.45.169 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 7ms, 最长 = 7ms, 平均 = 7ms

C:\Users\Administrator>ping 118.26.68.91

正在 Ping 118.26.68.91 具有 32 字节的数据:
来自 118.26.68.91 的回复: 字节=32 时间=99ms TTL=50
来自 118.26.68.91 的回复: 字节=32 时间=121ms TTL=50
来自 118.26.68.91 的回复: 字节=32 时间=108ms TTL=50
来自 118.26.68.91 的回复: 字节=32 时间=116ms TTL=50

118.26.68.91 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 99ms, 最长 = 121ms, 平均 = 111ms

C:\Users\Administrator>ping www.baidu.com

正在 Ping www.a.shifen.com [14.215.177.38] 具有 32 字节的数据:
来自 192.168.2.1 的回复: 无法连接到端口。
来自 192.168.2.1 的回复: 无法连接到端口。
来自 192.168.2.1 的回复: 无法连接到端口。
来自 192.168.2.1 的回复: 无法连接到端口。

14.215.177.38 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),

C:\Users\Administrator>ping 14.215.177.38

正在 Ping 14.215.177.38 具有 32 字节的数据:
来自 192.168.2.1 的回复: 无法连接到端口。
来自 192.168.2.1 的回复: 无法连接到端口。
来自 192.168.2.1 的回复: 无法连接到端口。
来自 192.168.2.1 的回复: 无法连接到端口。

14.215.177.38 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
```