

版本: V2.0



目录

简介		;
<i></i> `,	防火墙功能	ł
	11. 页面	ł
	1.2. 添加转发规则	3
二、	添加白名单10)
	2.1. 测试部分#110)
	2.1.1. 配置规则)
	2.1.2. 测试结果	3
	2.2. 测试部分#2	5
	2.2.1. 配置规则	5
	2.2.2. 测试结果)



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。



防火墙功能

SLK-R620 黑白名单使用说明

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;入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。

Veriallink®											
DUTIUTTIIK											
財本	基本设置 第二转发 通信规则 自定义规则										
设置	防火墙-区域设置										
	防火墙把网络接口分为不同的区域进行管理										
22	***·八···										
9548	臺平设置 自用SYN-flood訪問										
专用网	丢弃无效数据包	0									
管理	入站数据	接受			~						
	出站数据	接受			~						
	转发	拒绝			~						
	区域										
	区域⇒转发	入车	鐵据		出站数据		结发	IP动态伪装	MSS钳制		
	lan ⇒ wan	接受	~	接受	*	接受	*	0		编辑	删除
	Wan ⇒ REJECT	拒绝	~	接受	~	拒绝	~			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	
 ▲ 路由状态 ④ 网络设置 二 路由设置 希由表 	基本设置 第日转发 通信规则 自定的 防火墙 - 通信规则 通信规则如义了不同区域间的运量传送,例如:拒	URD9 8—49主約之2回約3勝何、177750WAAM2380□。				
DMZ设置 防火清 (7) 应用管理	通信规则	匹配规则	动作	启用		
■ 虚拟专用网 ✿ 设备管理	Allow-DHCP- Renew	IPv4-udp 来自 <i>所有主机位</i> 于 wan 到 <i>所有面曲地</i> 就 at port 60位于本设备	Accept input	✓ ▲ ▲ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	創除	
₿- 退出	Allow-Ping	IP-4-icnp 31 type echo-request 来自 許容正的で wan 到 所有質問地址位于本设备	Accept input	✓	删除	
	Allow-IGMP	119-4-ignp 来自,将海王建位于 wan 到,所有關語地址位于本记备	Accept input	✓ ▲ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★	删除	
	Allow-DHCPv6	마사-udp 来自 IP range fc00-26 년구 wan 到 IP range fc00-26 dt port 846 位子 구 2018	Accept input	☑ 编辑	删除	
	Allow-MLD	IPv6-iemp fil types 130(0, 137(0, 132(0, 143/0) 用 im range face: 2070 GET wan 到 所有面白地址 位于本设备	Accept input		删除	
	IPv6-icmp 和 types e Allow-ICMPv6- Input	ho-request echo-regly, destination-unreachable, paddet-too-big, time-acceeded, bad-header, unknown-header-type, router-solicitation neighbour-solicitation router-solverisament, neighbour-advertisement 来自 所有運用地址 位于本途番	Accept input并且限制到 1000 包。 毎 second	マ 編編	翻除	



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。

名称	匹配规则	动作	启用			
Allew DUOD	IPv4-udp			-		_
Allow-DHCP-	来自 <i>所有主机</i> 位于 wan	Accept input	~	~	编辑	删除
Reliew	到 所有路由地址 at port 68 位于本设备			_		
	IPv4-icmp 和 type <i>echo-request</i>		-			
Allow-Ping	来自 <i>所有主机</i> 位于 wan	Accept input			编辑	删除
	到 所有路由地址位于本设备				- Charles -	, morat
	IPv4-iqmp					
Allow-IGMP	来自 <i>所有主机</i> 位于 wan	Accept input		~	编辑	删除
	到 所有路由地址 位于本设备					
	IPv6-udp					
Allow-DHCPv6	来自 IP range fc00::/6 位于 wan	Accept input			编辑	删除
	到 IP range fc00::/6 at port 546 位于本设备					
	IPv6-icmp #1 types 130/0, 131/0, 132/0, 143/0		-	-		
Allow-MLD	来自 IP range <i>fe80::/10</i> 位于 <i>wan</i>	Accept input		~	/ 编辑	删除
	到 所有路由地址位于本设备					
	IPv6-icmp 和 types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header,					
Allow-ICMPv6-	unknown-header-type, router-solicitation, neighbour-solicitation, router-advertisement, neighbour-advertisement	Accept input 并且限制到			1040	00120
Input	来自 所有主机 位于 wan	1000包.每 second			编辑	删除
	到 所有路由地址位于本设备					
	IPv6-icmp 和 types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header,					
Allow-ICMPv6-	unknown-header-type	Accept forward 并且限制到			1019	INIRA
Forward	来自 <i>所有主机</i> 位于 wan	1000包.每 second			编辑	删际
	到所有主机位于所有区域					
Allaw IDOas	任何 esp		-			
Allow-IPSec-	来自 <i>所有主机</i> 位于 wan	Accept forward			编辑	删除
ESP	到 <i>所有主机</i> 位于 Ian					
	任何 udp			-		
Allow-ISAKMP	来自 <i>所有主机 位于 wan</i>	Accept forward		^	编辑	删除
	到 <i>所有主机</i> port 500 位于 Ian					



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。

# Seriallink®			5G .
		刘 所有随用燃起位于本设备	
 ▲ 路由状态 ④ 网络设置 ▲ 路由设置 	Allow-ICMPv6- Input	IPvG-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, regiphour-advertisement, regiphour-advertisem	剑臆
路由表 DMZ设置	Allow-ICMPv6- Forward	IPvG-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	
の应用管理	Allow-IPSec-ESP	任何 #10 来自 所有主机位于 war Accept forward 【 编辑 另 所有主机位于 fan	
■ 虚拟专用网 ✿ 设备管理	Allow-ISAKMP	任何10月 来自后将主张位于wart Accept forward C o Little 到 <i>所有主先</i> (10年) Accept forward C o Little	刷除
₿ 退出	打开路由器端口:		
	名称	h议 外部桌口	
	新建进入规则	TCP+UDP v XXXX	
	新建转发规则:		
	名称	還区域 目标区域	
	新建转发规则	lan ▼ wan ▼ 活加开编辑.	



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】

本设置 端口转发 通信规则 自定义规则		
ī火墙 - 通信规则 - (未命名规则	山)	
页面可以更改通信规则的高级设置,比如:需匹配的源:	上机和目标主机。	
Rule is enabled	禁用	
名称	自定义名称	
限制地址	IPv4 和 IPv6	v
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: 🛃	lžtp: 题 pptp: 题 opempn. 灵 gre: ④ gre_static 灵 ·
目标地址	所有	v
目标端口	所有	



	任何 🗸	协议
	any 🗸	匹配ICMP类型
	lan: lan:	源区域
	所有	源MAC地址
	192.168.2.59 (40:8D:5C:7A:F3:F7) 🗸	源地址
	所有	源端口
pptp: 🛅 openvpn: 🐊 gre: (奎) gre_static: 🐊 🔹	wan: wan: 🐙 wan6: 🐙 modem: 🛃 12tp:	目标区域
	所有	目标地址
	所有	目标適口
	接受 🗸	动作
		附加参数
	传递到iptables的额外参数。小心使用!	

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 <i>所有主机</i> 位于 wan 到 <i>所有路由地址</i> 位于本设备	Accept input			编辑	删除
Allow-IGMP	IPv4-igmp 来自 <i>所有主机</i> 位于 wan 到 <i>所有路由地址</i> 位于 <i>本设备</i>	Accept input	^	*	编辑	副除
Allow-DHCPv6	IPv6-udp 来自 IP range <i>fc00:::/6</i> 位于 <i>wan</i> 到 IP range <i>fc00::/6</i> at port <i>546</i> 位于 <i>本设备</i>	Accept input			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 <i>wan</i> 到 <i>所有路由地址</i> 位于 <i>本设备</i>	Accept input	^	-	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 所有許加位于 wan 到 所有路由地址 位于本设备	Accept input 并且限制到 1000 包.每 second			编辑	删附
Allow-ICMPv6- Forward	IPv6-icmp 和 types <i>echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header,</i> 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	^	~	编辑	删附
Allow-IPSec- ESP	任何 esp 来自 <i>所有主机</i> 位于 wan 到 <i>所有主机</i> 位于 lan	Accept forward			编辑	删除
Allow-ISAKMP	任何 udp 来自 <i>所有主机</i> 位于 wan 到 <i>所有主机</i> port <i>500</i> 位于 lan	Accept forward	^	•	编辑	删附
自定义名称	任何 交通 来自 IP <i>192.168.2.59</i> 位于 <i>Ian</i> 到 <i>所有主机</i> 位于 wan	Accept forward			编辑	删附



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】

5 I	体设置 端口转发 通信	調測 自定义规则				
a 防	火墙 - 通信规则					
	规则定义了不同区域间的流量 (五/言切回)	传送,例如:拒绝一些主机之间	间的通信、打开到WAN的商口。			
里	名称		匹配规则		动作	启用
用网 里				尚无任何配置		
	打开路由器端口: 名称	协议	外部端口			
	新建转发规则:	201714	1000			
	新建转发规则	an ~	awica 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 PC1 的 IP 地址: 192.168.2.59
- ⑤【动作】选择【接收】, 允许 PC1 通过 SLK-R620 网络

⑥点击【保存并应用】

	Billy	
青 - 通信规则 - (木命名规)	则)	
使成過激制制的高級後輩,比如:高些動物的	·王司(和日标王司)。	
Rule is enabled	#用	
5H	5 PC1	
限制因	IPv4 和 IPv6	v
物的	任何	v
匹替BCMP类型	any	× •
遵区域	lan: lan: 🚟	
源MAC18b	所有	v
源地址	192.168.2.59 (40:8D:5C:7A:F3:F7)	×
济靖口	所有	
目标区域	wan: wan: 💯 wanis 💯 modern 🛃	Cability Color and Cability Ca
日标地址	前有	v
日初前口	所有	
尼日	接受	v
用此口参考	t	
	传递到iptables的额外参数。小心使用!	

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。

ADIE MORT							
名称	现现无面型	动作	启用				
PC1	任何 交通 来自 IP <i>192.168.2.59</i> 位于 <i>Ian</i> 到 <i>所有主机</i> 位于 wan	Accept forward		^	× 1	編輯	删除
50							



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】

名称	协议	外部端口	
新建进入规则	TCP+UDP 🛩	添加	
建转发规则:			
建转发规则: 名称	源区域	目标区域	

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】

基本设置 黄口转发 通信规则 自定义规则		
防火墙 - 通信规则 - (未命名规则	ال)	
本页面可以更改通信规则的高级设置,比如:高匹配的源于	E机和目标主机。	
Rule is enabled	第月	
名称	白名単	
限制地址	IPv4 #⊡ IPv6 ✓	
协议	任何 🖌	
匹配CMP类型	any 🗸 🗸	1
源区域	lan: Ian: Man	
源MACI包址	所有 イ	
源地址	所有・・	
透流口	新有	
日标区域	wan: wan 👷 wanß 👷 moden: 🚊 12tp.	80 Star (a) Solution (b) Solution (c) Sol
日标地址	所有 イ	
日标演口	所有	
动作	振逸 ~	
附加参数		
	传递到iptables的额外参数。小心使用!	
100124502		gtaum a

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。

名称	尼亚省合共和国	动作	启用				
PC1	任母交通 来自1P 192.168.2.59 位于 Ian 到 <i>所有主机</i> 位于 wan	Accept forward	•	*	*	編輯	翻時
白谷单	任何交通 来自 所用主机位于 Ian 到 所用主机位于 wan	Refuse forward	2			編	創造

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】:

名称	UERSTRUE	动作	启用					
PC1	任何 交遷 来自 IP 192 168.2.59 位于 /an 到 所有主机位于 wan	Accept forward	8	•	*	1	8	删除
PC3	任何交通 来員 IP 192.168.2.222 位于 Jan 到 <i>所有主机</i> 位于 wan	Accept forward	2			\$	i i	题除
白石単	任何 交通 来自 <i>所有主机</i> 位于 <i>lan</i> 到 <i>所有主机</i> 位于 <i>wan</i>	Refuse forward		^	*	i ii	8	删除



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

雨

C:\Users\Administrator>ping www.baidu.com 在 Ping www.a.shifen.com [14.215.177.38] 具有 32 字节的数据: 自 14.215.177.38 的回复: 字节=32 时间=9ms TTL=54 来百百百日 14.215.177.38 的 Ping 统计 数据包:已发送 = 4,已 ⊤信息: 見接收 = 4, 丢失 = 0 (0% 丢失), 为单位): E 为单 的估计时间 9ms, = 9ms, 平均 = 9ms



③PC2 上网络配置如下

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	192.168.2.69	
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	

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: 无法连到端口。 来自 192.168.2.1 的回复: 无法连到端口。 来自 192.168.2.1 的回复: 无法连到端口。 来自 192.168.2.1 的回复: 无法连到端口。 来自 192.168.2.1 的回复: 无法连到端口。
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】

W Seriallink®				5G 🖬
 ▲ 路由状态 ④ 网络设置 	基本设置 施口转发 通信规则 自定义规则			
苗 路由设置 路由表	防火墙 - 通信规则 通信规则定义了不同区编问的流量传送,例如:拒绝一些主机之间的通信、打3	F到wan的端口。		
DMZ设置	通信规则			
 ▲ 应用管理 ■ 虚拟专用网 	名称	匹配規則 尚无任何面	动作	肩用
✿ 设备管理	打开路由器端口:			
	名称 协议 外音 新进计入初则 TCP4IIIP ×	総口 (表tro		
	新建輸发規则:	NUS.		
	名称 遊区域 目标区域	來 initiastt		
		2004/11/00000		

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】

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	1)	
本页面可以更改通信规则的高级设置,比如:需匹配的源主	初和目标主机。	
Rule is enabled	禁 用	
名称	PC1	
限制地址	IPv4和IPv6 v	
协议	任何 *	
匹配ICMP类型	any. 🗸 +	
源区域	lan: Lan: 201	
源MAC地址	所有	
源地址	192.168.2.59 (40.3D.5C.7A.F3.F7) v	
源满口	所有	



		100 C	rząp. juj	ELSE SE	openvpn.	gre: (空) gre		
	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	妠◆参数。小心使用!						
既况								保存并应用
—								
						V		
	7							
	J.							



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】

新I建特权7%1%];					
名称	源区域	目标区域			
新建转发规则	lan 👻	wan 🗸	法加并编辑		

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】

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	数用		
名称	PC1-2		
限制地址	IPv4 ‡∏ IPv6	×	
ibilX	任何	~	
UBCMP类型	any	× +	
源区域	lan: 🔛	•	
源MAC地址	所有	v	
源地址	192.168.2.59 (40:8D:5C:7A:F3:F7)	×	
迴流口	所有		
目标区域	wan: wan 💥 wan6 💥 modem 💒	Tātas 👰 pastas 👰 opensijas 🖉 grē (🖼) grē, static 🎉 🔸	
目标地址	所有	-	
目标满口	所有		
动作	拒绝	~	
附加参数			
	传递到iptables的额外参数。小心使用!		



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】

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【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】

页面可以更改通信规则的高级设置,比如: 素匹配的	的源主机和目标主机。				
Rule is enab	ied 競用				
ŝ	称 白名单				
限制其	助 IPv4 和 IPv6	~			
ta	议 任何	~			
匹配 CMP 禁	部 any	~ +			
源区	Etit lan: 👥				
源MAC地	助有	~			
源地	趾 所有	~			
· 理訓	和 所有				
目标区	tig wan: wan: 👥 wan6: 👥	modem: 🖉 12tp: 🛍 pptp:	openvpn: 🚈 gre: (室) gre_statio	·	
目标地	趾 所有	~			
日标道	印 所有				
2	1作 拒绝	~			
Pdbog	徴				
	传递到iptables的额外参数。小心使用	81			



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。

通信规则								
名称	卫工商已未见到	动作	启用					
PC1	任何 交通 来自 IP 192.168.2.59 位于 Ian 到 IP 106.55.45.169 位于 wan	Accept forward			٠	編	删除	
PC1-2	任何交通 来自 IP 192.168.2.59 位于 Ian 到 所有主机 位于 wan	Refuse forward	2			編輯	創除	
白名単	任何 交通 来旨 <i>所有主机</i> 位于 <i>lan</i> 到 <i>所有主机</i> 位于 <i>wan</i>	Refuse forward		*	•	編	劉除	

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】:

通信规则							
名称	匹省己规则	动作	启用				
PC1-允许1	任何 交通 来自 IP 192 168 2.59 位于 Ian 到 IP 106 55 45 169 位于 wan	Accept forward			•	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				编辑	删除
PC1-拒绝	任何交通 来自 IP <i>192.168.2.59</i> 位于 <i>lan</i> 到 <i>所有主机</i> 位于 <i>wan</i>	Refuse forward	2	^	÷	编辑	删除
白名単	任何 交遷 来自 <i>所有主机</i> 位于 lan 到 <i>所有主机</i> 位于 wan	Refuse forward				编辑	删除



2.2.2. 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		
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 Ping 106.55.45.169 具有 32 字节的数据: 106.55.45.169 的回复: 字节=32 时间=7ms TTL=51 自 来自 自 そ自 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 在 Ping 118.26.68.91 具有 32 字节的数据: 自 118.26.68.91 的回复: 字节=32 时间=99ms TTL=50 自 118.26.68.91 的回复: 字节=32 时间=121ms TTL=50 自 118.26.68.91 的回复: 字节=32 时间=108ms TTL=50 自 118.26.68.91 的回复: 字节=32 时间=116ms TTL=50 来首 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 在 Ping www.a.shifen.com [14.215.177.38] 具有 32 字节的数据: :自 192.168.2.1 的回复: 无法连到端口。 来自 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 Ping 14.215.177.38 具有 32 字节的数据: 192.168.2.1 的回复:无法连到端口。 192.168.2.1 的回复:无法连到端口。 192.168.2.1 的回复:无法连到端口。 192.168.2.1 的回复:无法连到端口。 192.168.2.1 的回复:无法连到端口。 白 自 自 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),