奇固科威 HKW-NF500 防火墙系统
用户手册 V1.5.8

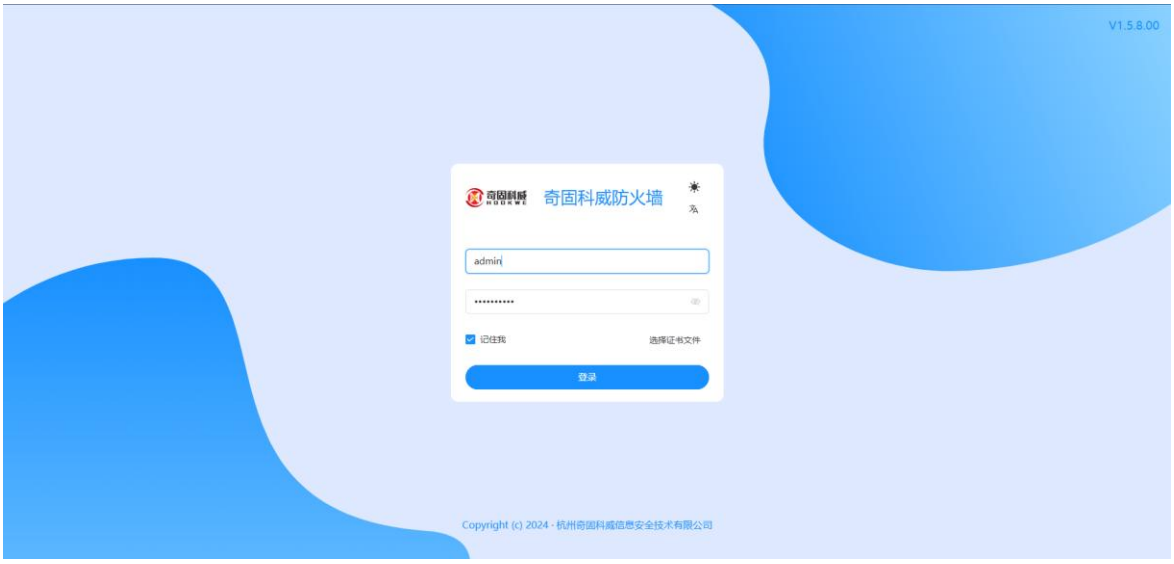
杭州奇固科威信息安全技术有限公司

2024 年 8 月

目 录

登录界面

用网线连接设备 eth0 口，将自己电脑 IP 地址改成 192.168.0.0/24 网段内的地址，打开谷歌或者 IE.11 浏览器，在网址中输入 https://192.168.0.178。



管理员：用户名 admin，密码 Linkqi@123

本系统分为三种权限：管理员、操作员，审计员

1 主界面

1.1 首页

权限:(管理员)

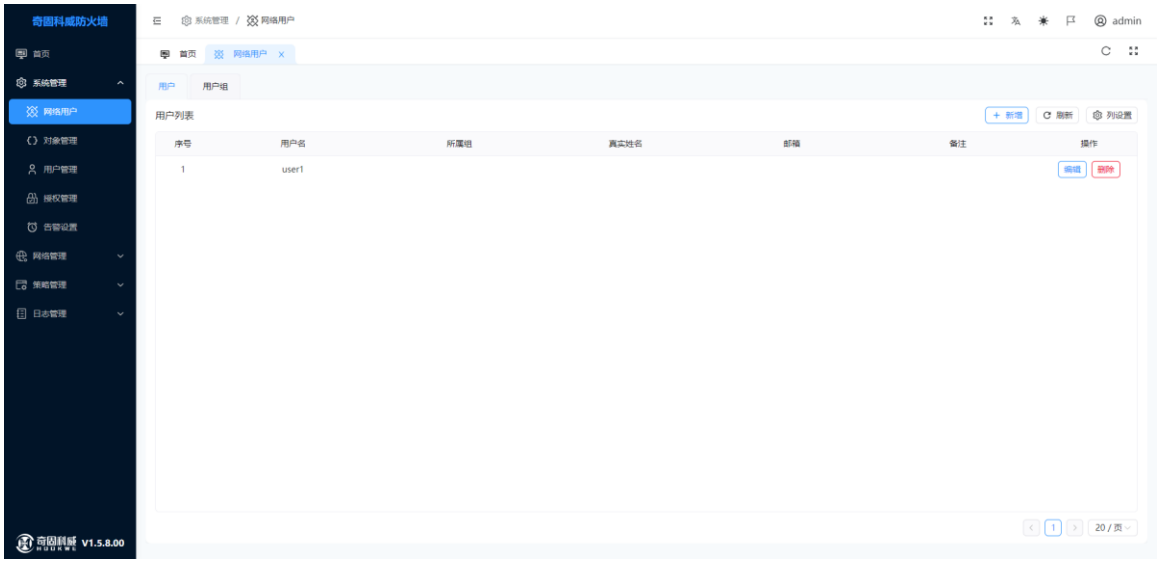
首页对系统的信息、系统资源详情信息进行展示。

1.2 系统管理

1.2.1 网络用户

1.2.1.1 用户

权限:(管理员)



用户角色防火墙策略允许管理员根据为用户分配的角色允许或限制用户的网络访问。用户角色防火墙可以更好地缓解威胁，提供更多信息丰富的取证资源，改进记录存档以确保合规性，并增强常规访问配置。

支持认证方式

认证方式		说明
本地认证	用户名/密码	通过用户名和密码进行认证。需要从防火墙管理员处获取用户名和密码。

当防火墙的**安全策略**开启时，用户类型选择网络用户时， 需要认证才可以使用网络。，

配置项	说明
用户名	用户名
密码	用户密码（数字大小写字母特殊符号如何而成，最少三种组合）
确认密码	确认密码
所属组	指用户组
真实名称	-
邮箱	-
备注	备注信息

新增

点击新增按钮，设置需要新增的用户名，密码等。点击保存创建成功。如下图

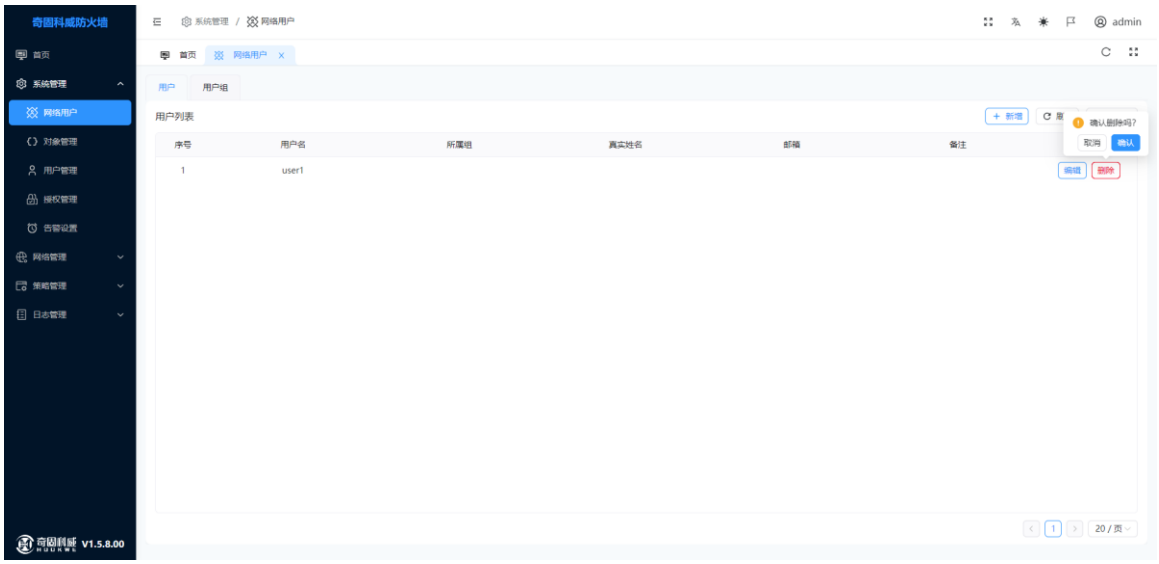
注：所属组关联用户组

编辑

点击列表中的编辑按钮，可以当前项进行修改操作。如下图

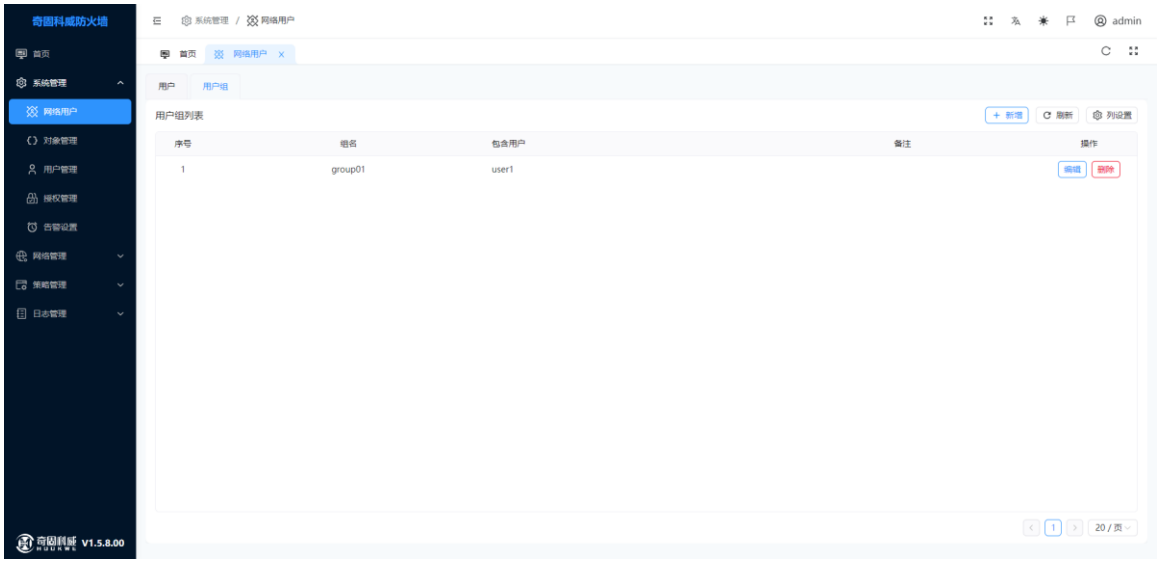
删除

点击列表中的删除进行删除。此操作不可逆，点击后确认后删除该条数据。如下图



1.2.1.2 用户组

权限:(管理员)



防火墙中的用户组织结构是现实中的组织结构的映射，是基于用户进行访问控制的基础

配置项	说明
组名	-
包含用户	指网络用户-
备注	备注信息

新增

点击新增按钮，设置需要新增的组名。点击保存创建成功。如下图

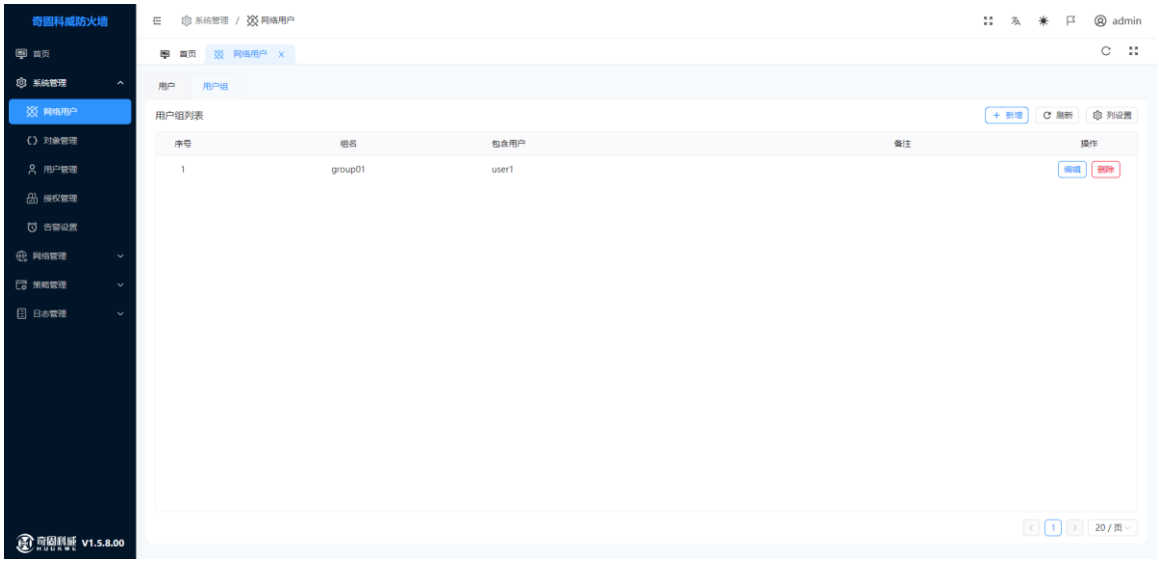
注：包含用户指网络用户

编辑

点击列表中的编辑按钮，可以当前项进行修改操作。如下图

删除

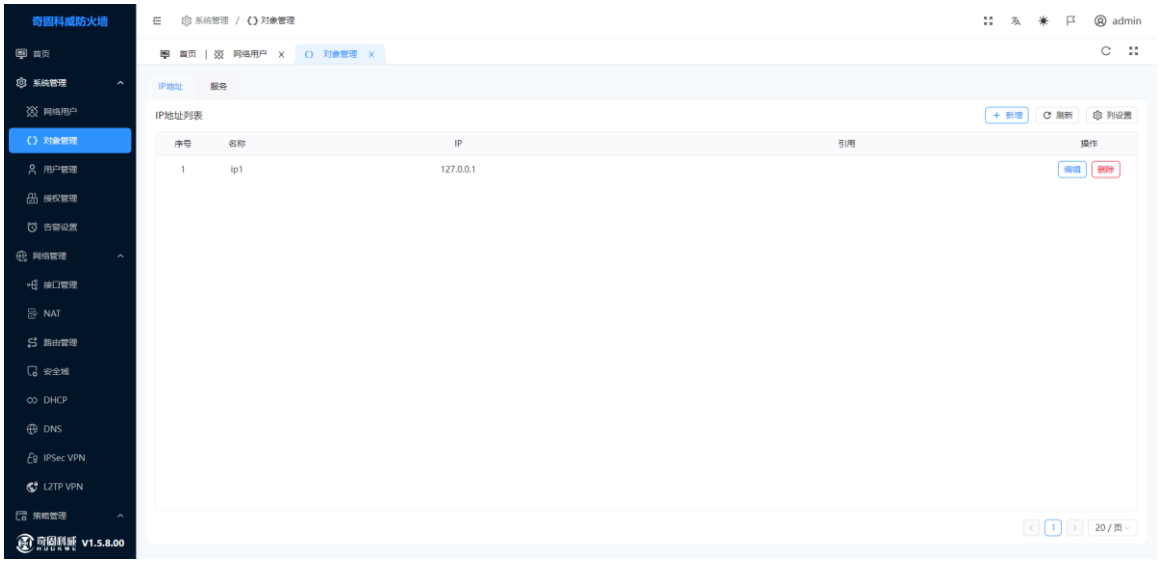
点击列表中的删除进行删除。此操作不可逆，点击后确认后删除该条数据。如下图



1.2.2 对象管理

1.3 IP 地址

权限:(管理员)



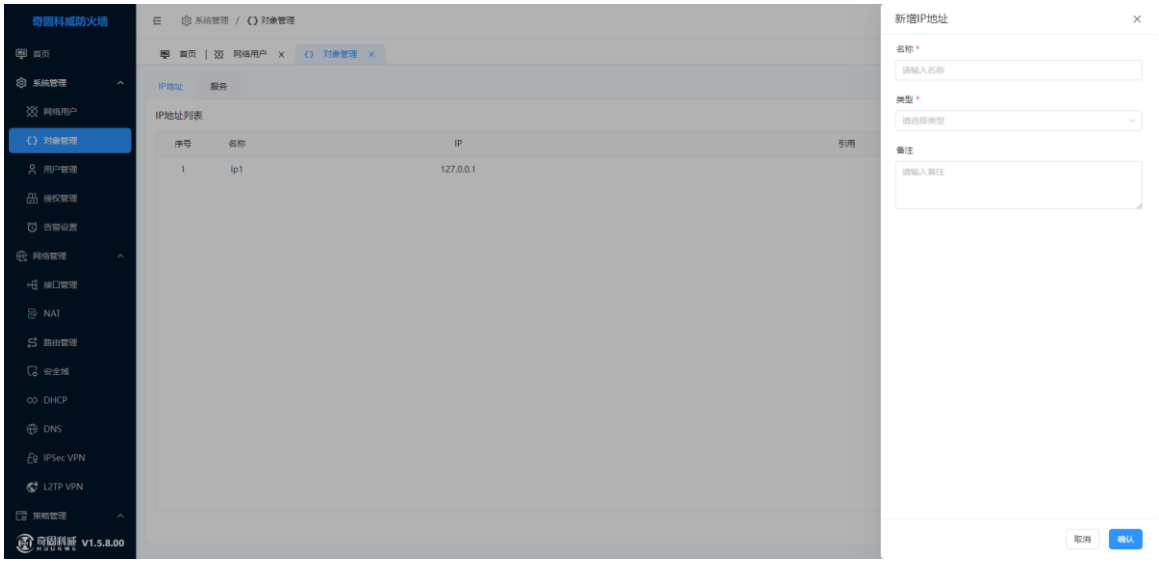
IP 地址是指一段连续的 IP 地址，即从起始 IP 到结束 IP 之间的若干 IP 主机对象或单个 IP 地址对象

配置项	说明
名称	用户名
类型	支持 IP 地址和 IP 范围
IP 地址	类型为 IP 地址时，只允许单 IP
开始地址	类型为 IP 范围时，开始 IP-
结束地址	类型为 IP 范围时、结束 IP-
备注	备注信息

新增

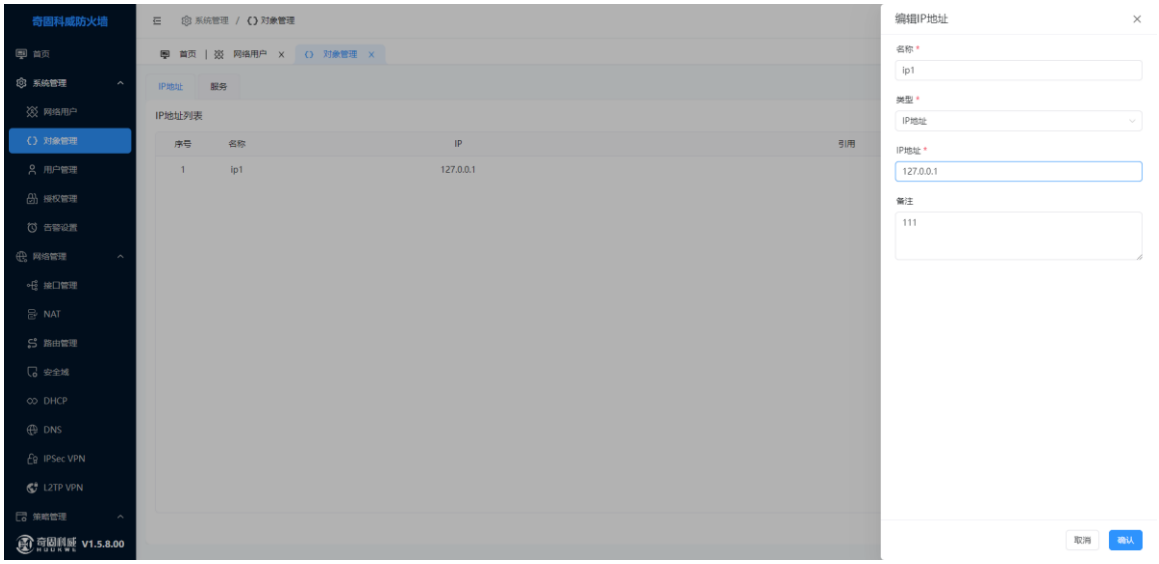
点击新增按钮，设置需要新增的名称，类型等。点击保存创建成功。如下图

注： 类型可选 IP 地址和 IP 范围 可以创建单 IP 或者 IP 区间



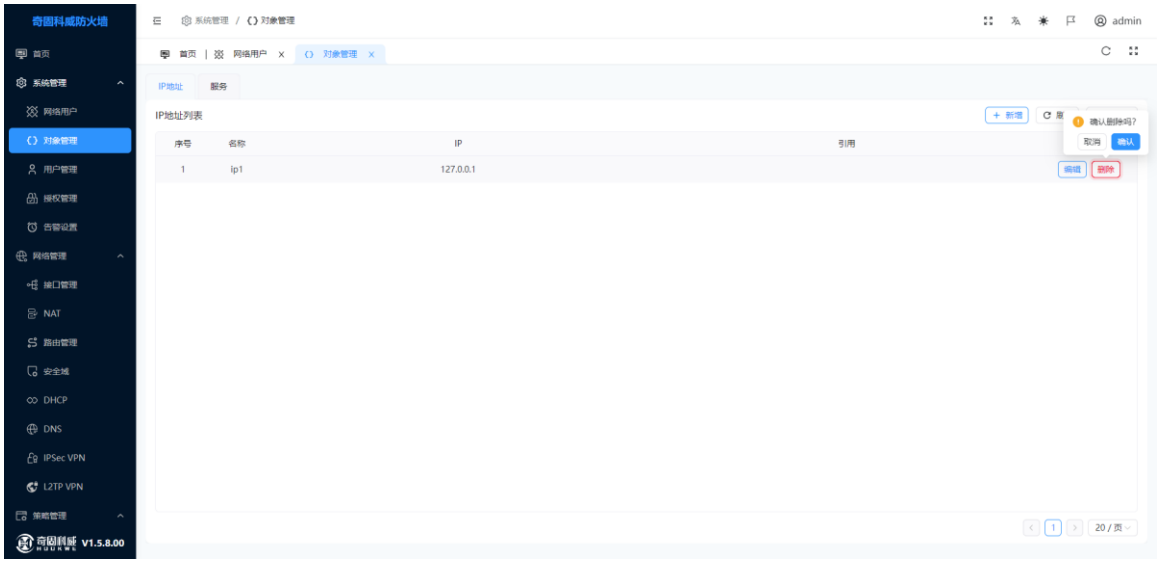
编辑

点击列表中的编辑按钮，可以当前项进行修改操作。如下图

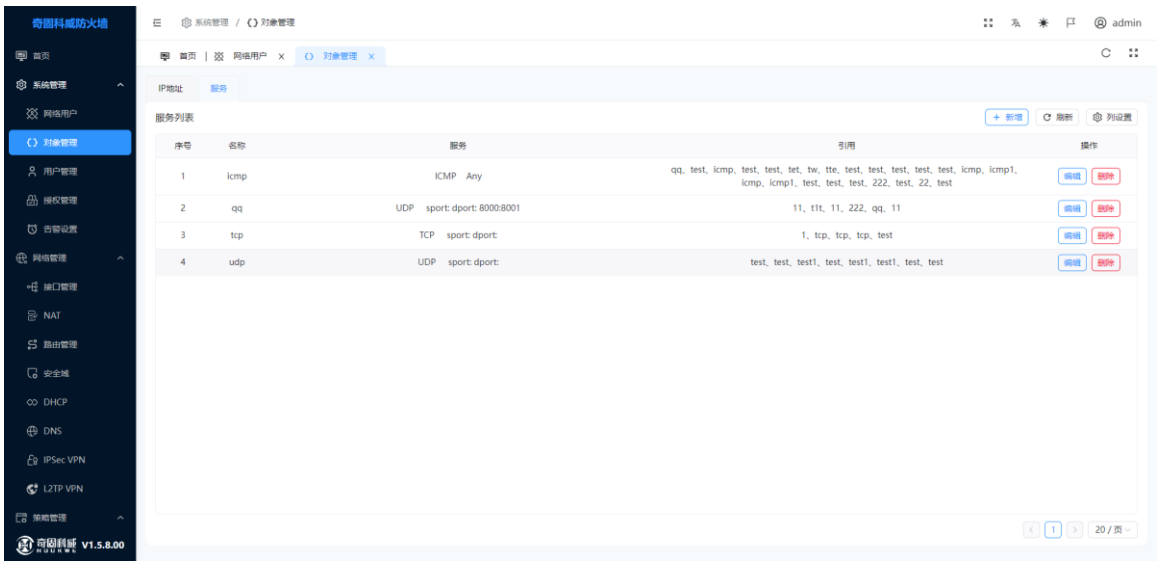


删除

点击列表中的删除进行删除。此操作不可逆，点击后确认后删除该条数据。如下图



1.3.1.1 服务



配置项	说明
名称	用户名
协议	下方注释
类型	下方注释
备注	备注信息

注：

协议可选'ICMP', 'ICMP6', 'TCP', 'UDP'

'ICMP'可选类型

'Any'、'ECHO_and_ECHOREPLY'、'INFO_REQUEST_and_INFO_REPLY'、'TIMESTAMP_and_TIMESTAMPREPLY'、'ADDRESS_and_ADDRESSREPLY'、'ROUTER_ADVERTISEMENT'、'ROUTER_SOLICITATION'、'DEST_UNREACH'、'SOURCE_QUENCH'、'REDIRECT'、'TIME_EXCEEDED'、'PARAMETERPROB'

'ICMP6'可选类型

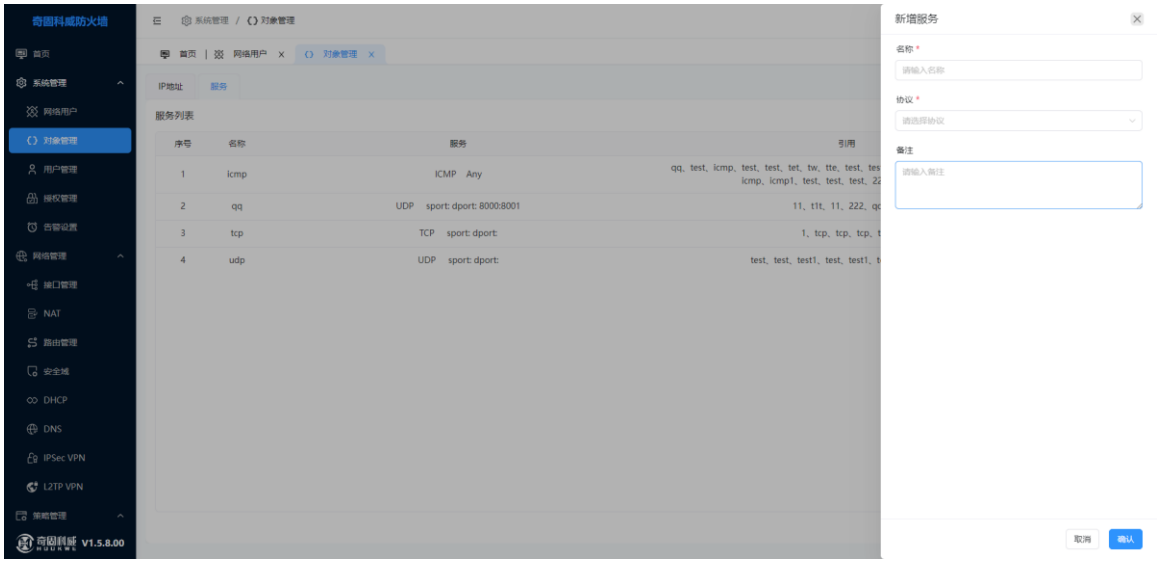
'Any'、'DST_UNREACH'、'PACKET_TOO_BIG'、'TIME_EXCEEDED'、'PARAM_PROB'、'ECHO_and_ECHOREPLY'

'TCP'类型 与 UDP 类型

Tcp 需要配置源端口 目的端口 可以配置单端口或者端口区间

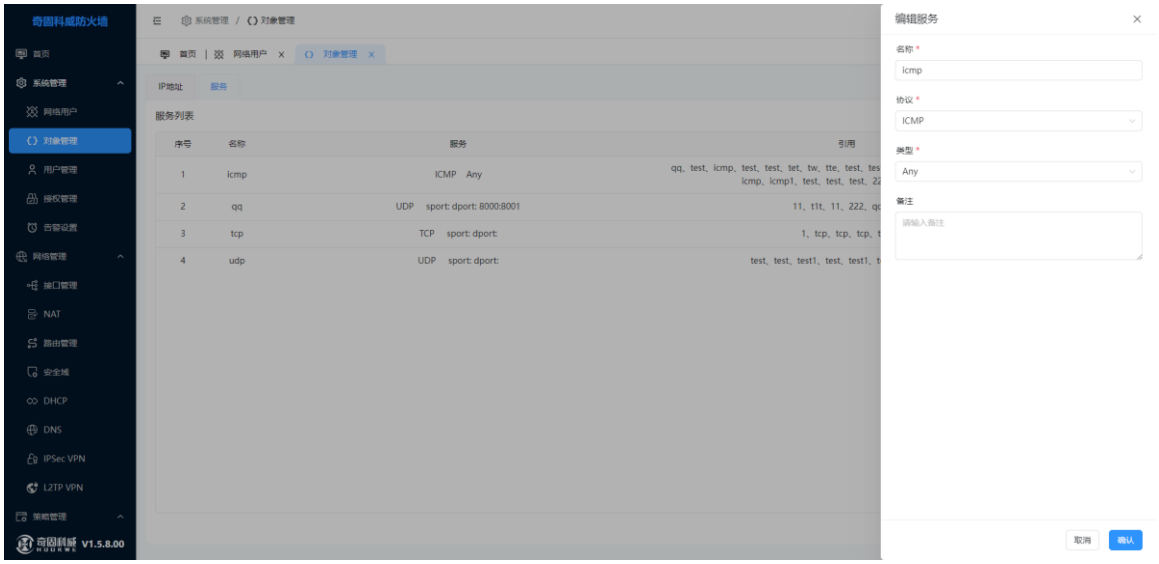
新增

点击新增按钮，设置需要新增的名称，类型等。点击保存创建成功。如下图



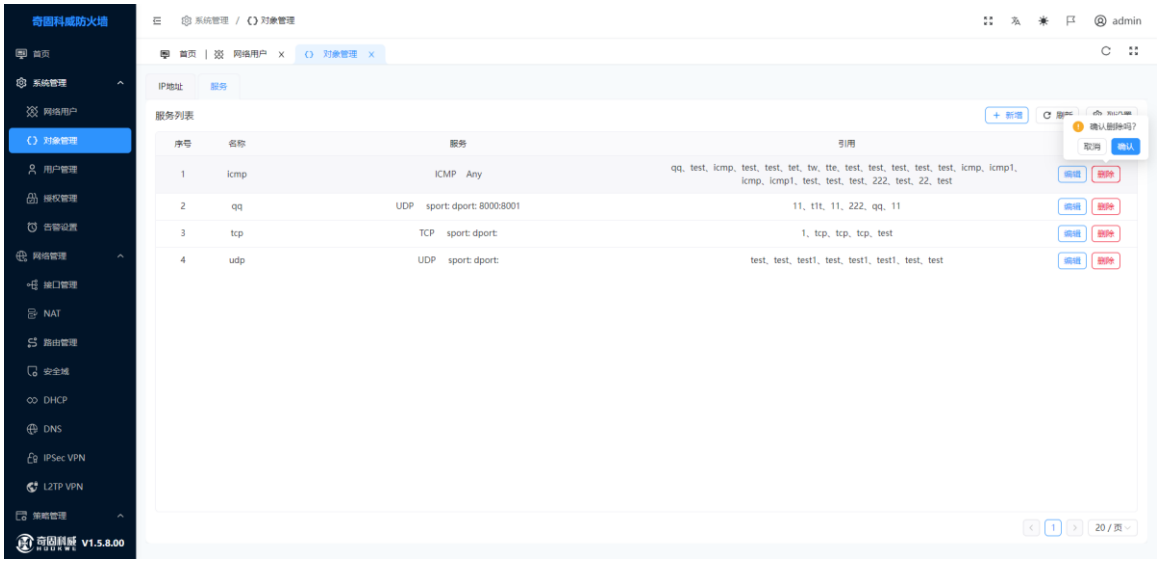
编辑

点击列表中的编辑按钮，可以当前项进行修改操作。如下图



删除

点击列表中的删除进行删除。此操作不可逆，点击后确认后删除该条数据。如下图



1.3.2 用户管理

权限:(管理员)

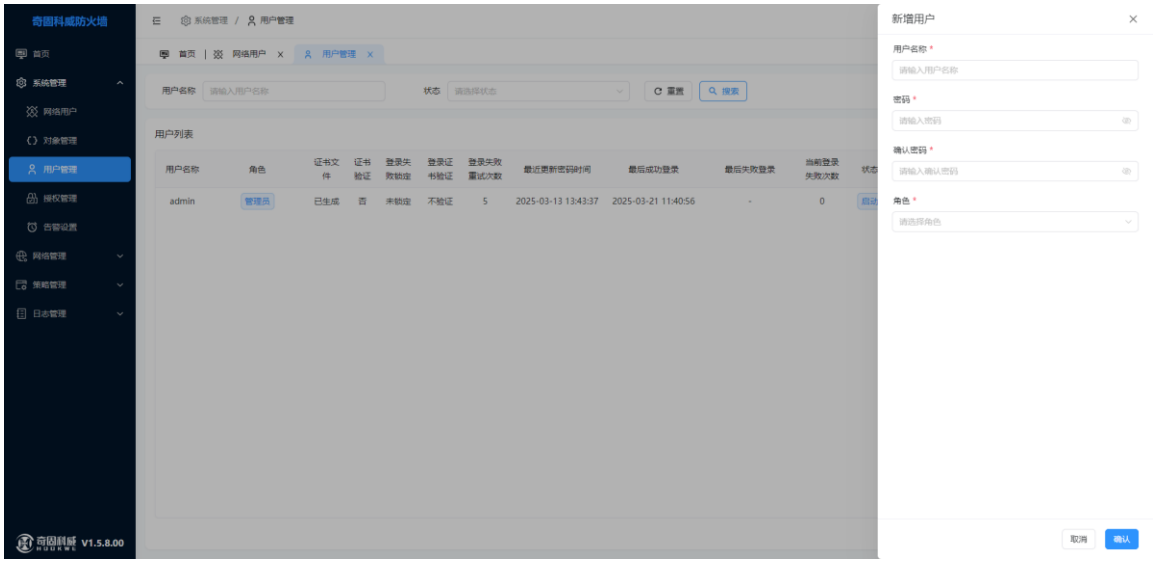
管理当前系统下所有用户。包含功能新增、编辑、删除、解锁、生成证书

配置项	说明
名称	用户名
密码	用户密码（数字大小写字母特殊符号如何而成，最少三种组合）
确认密码	二次确认密码

角色	支持管理源、审计员、操作员-
登录失败次数	允许最大失败登录次数
状态	控制用户能否登录
登录证书验证	当生成证书后，支持登录证书认证

新增

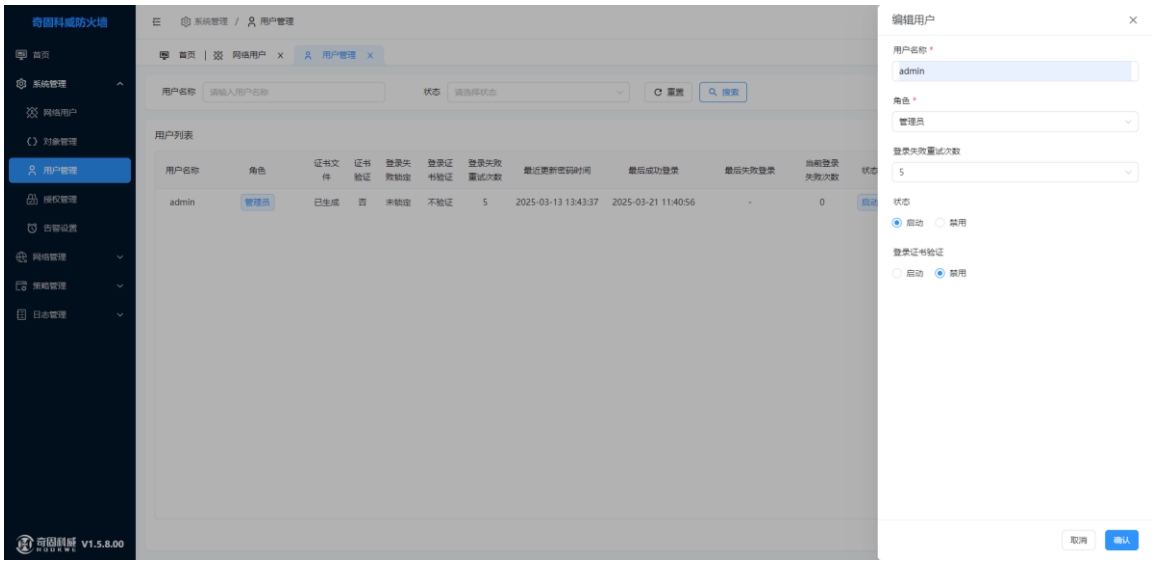
点击新增按钮，设置需要新增的用户名，选择角色，创建密码等。点击保存创建成功。如下图



编辑

点击列表中的编辑按钮，可以当前项进行修改操作。如下图

注： 用户名不可修改



删除用户

点击用户列表中的删除进行删除。此操作不可逆，点击后直接删除该用户。如下图

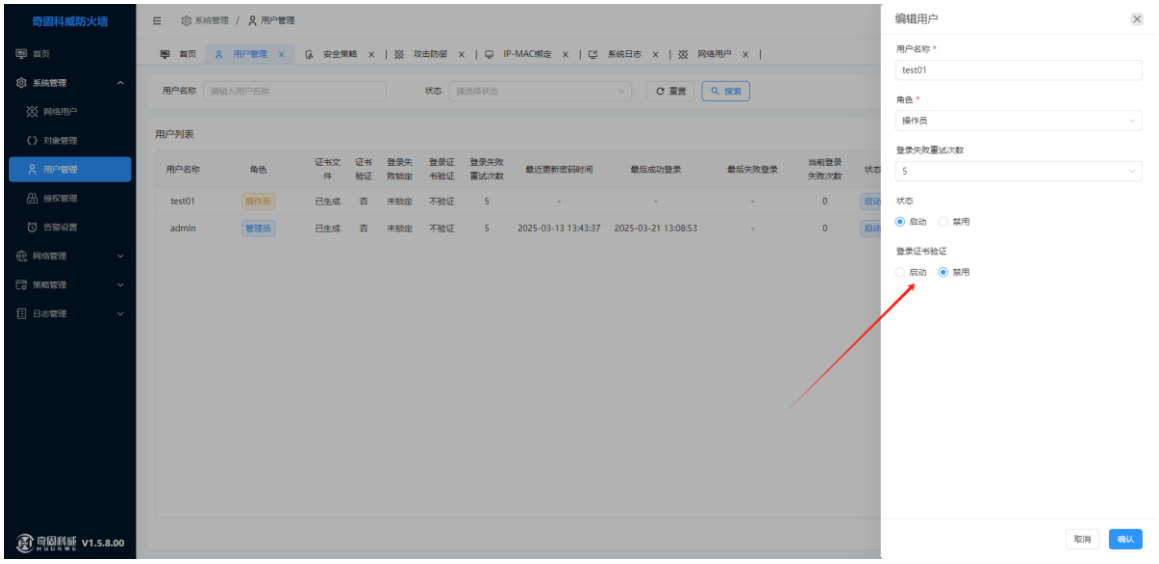
证书

如果希望安全登录使用，可以采取采方式，

1. 生成证书

   注：生成证书后会下载一个文件，该文件请妥善保管，后续如修改证书认证，那么则需要上传认证，才可登录

2. 修改启动证书验证即可

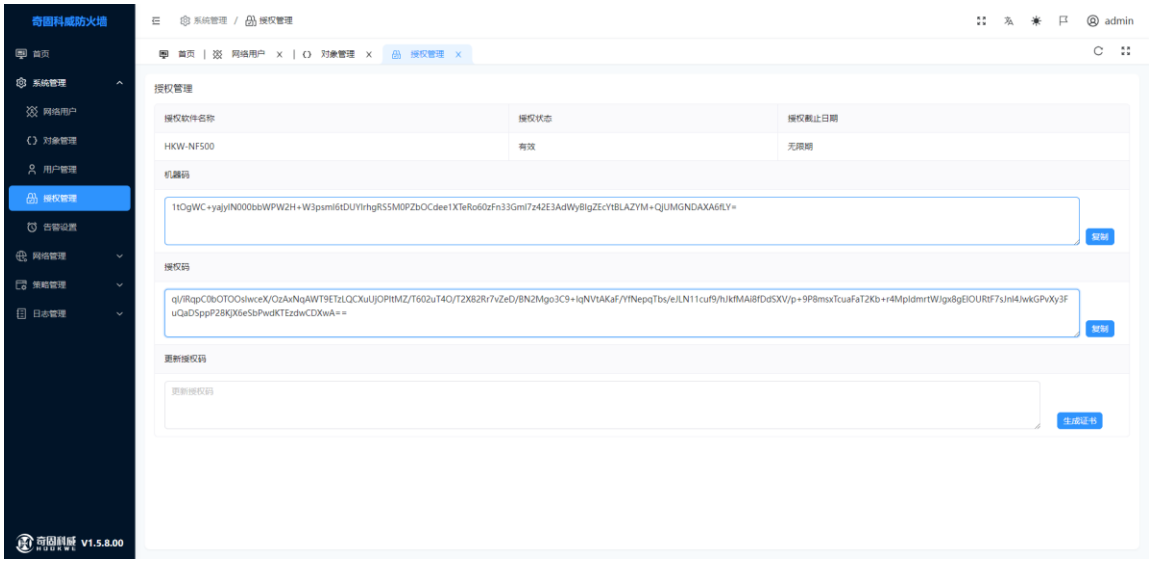


解锁

账户多次错误登录被锁定，需要解锁才可以继续使用

1.3.3 授权管理

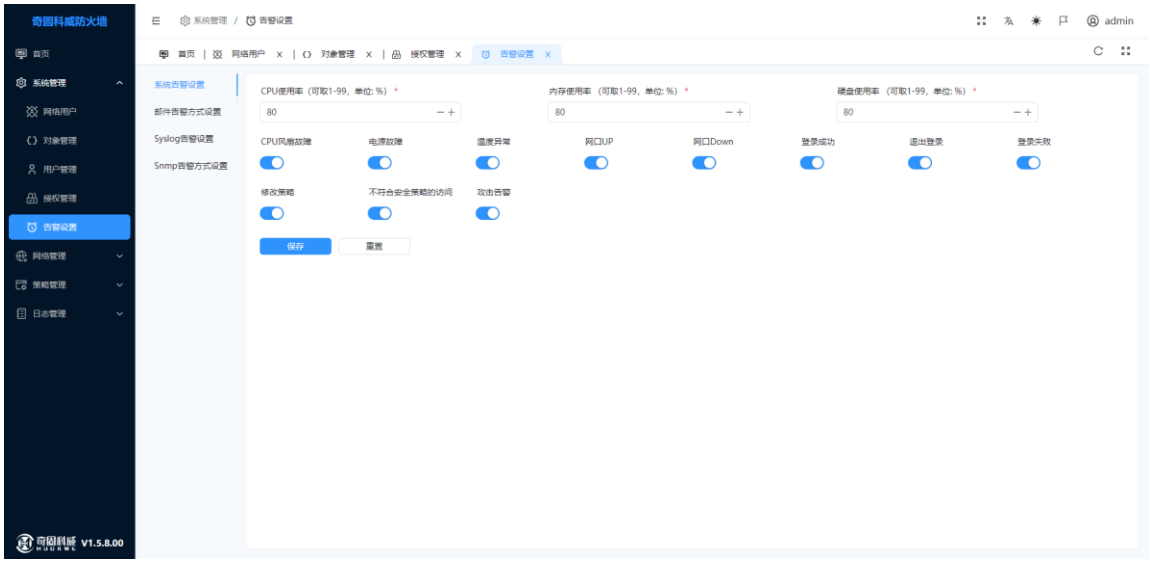
配置项	说明
更新授权码	需要通过系统认证试用期方可使用



可以对当前的授权状态，授权截止日期等进行查看，如系统未授权则通过更新授权码获得权限

1.3.4 告警设置

1.3.4.1 系统告警设置

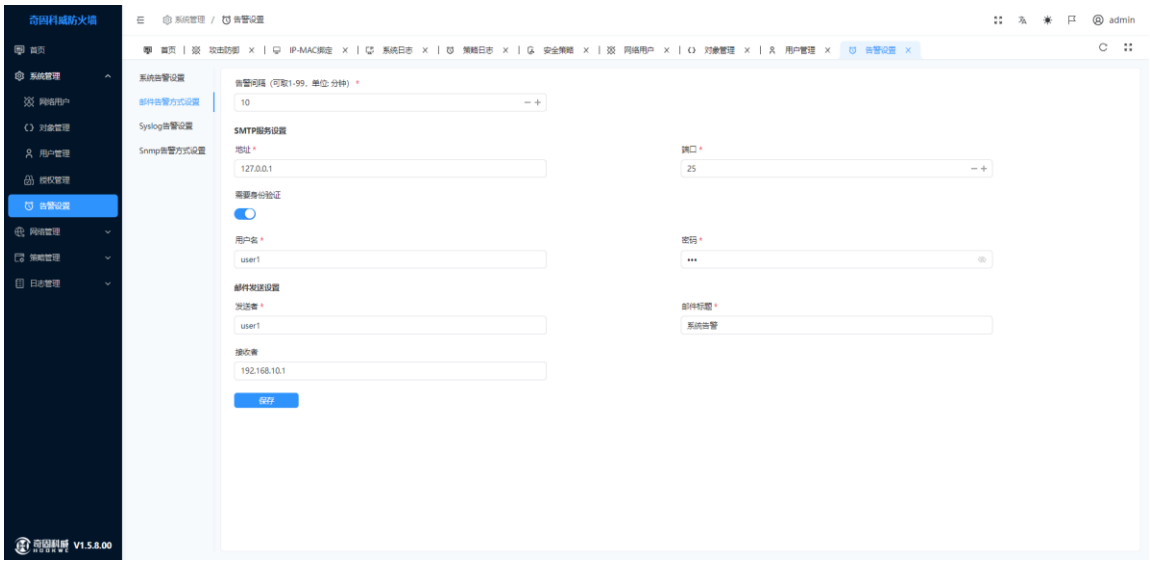


主要对系统的 cpu 使用率，内存使用率，硬盘使用率以及事件进行配置，如果超出设置上限，则开始告警通知。

配置项	说明
CPU 使用率	可取 1-99 ， 单位%

内存使用率	可取 1-99 ， 单位%
硬盘使用率	可取 1-99 ， 单位%
CPU 风扇故障	是否告警，开启/关闭-
电源故障	-是否告警，开启/关闭-
温度异常	-是否告警，开启/关闭-
网口 UP	-是否告警，开启/关闭-
网口 Down	-是否告警，开启/关闭-
登录成功	-是否告警，开启/关闭-
登录失败	-是否告警，开启/关闭-
修改策略	-是否告警，开启/关闭-
不符合安全策略访问	-是否告警，开启/关闭-
攻击告警	-是否告警，开启/关闭-

1.3.4.2 邮件告警方式设置

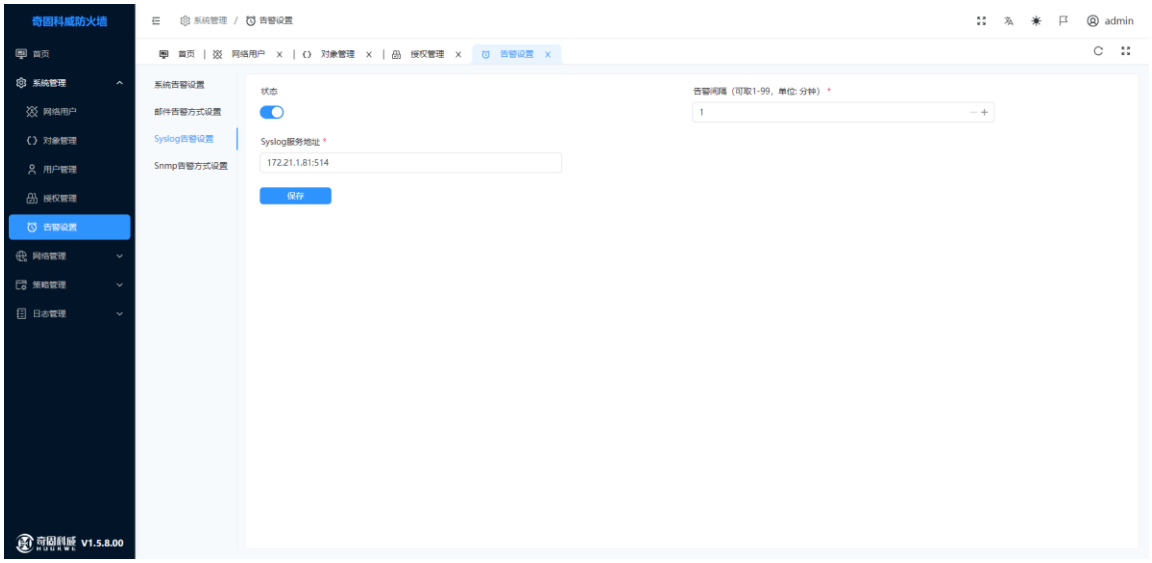


通过配置，当出现告警时，会将通知推送到对应的邮箱上

配置项	说明
告警间隔	1-99 分钟

地址	smtp 的服务地址
端口	默认 465
需要身份验证	开启后需要用户名，密码认证
用户名	-
密码	-
发送者	发送人邮箱
邮件标题	邮件的标题
接受者	当出现资源告警，入侵告警后通知的邮箱

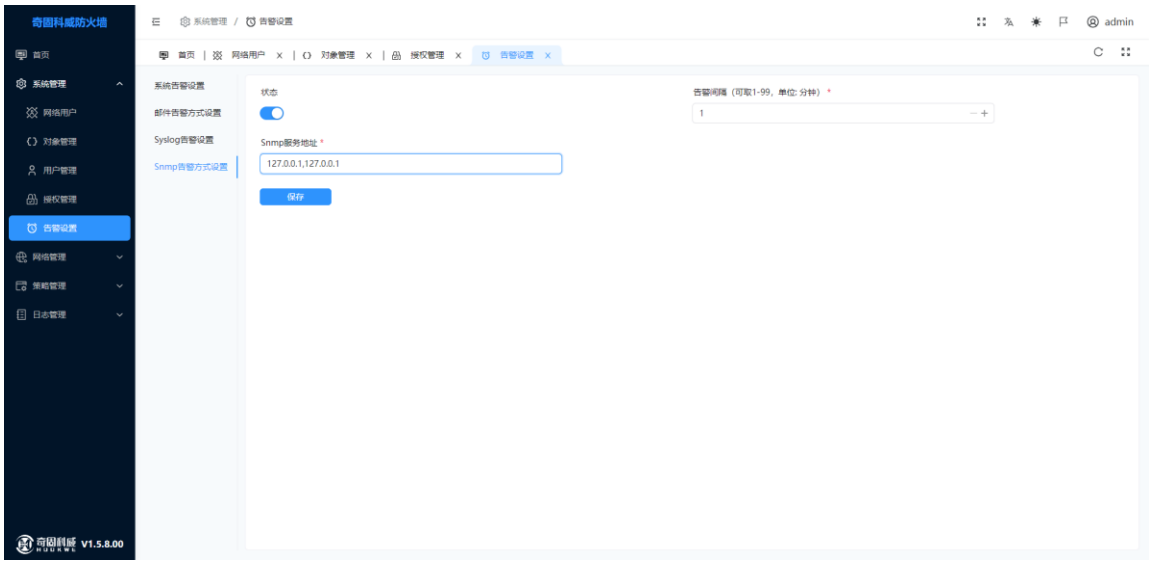
1.3.4.3 Syslog 告警设置



通过配置，当出现告警时，会将通知，推送到对应的 Syslog 服务上

配置项	说明
状态	是否使用，默认关闭
告警间隔	1-99
syslog 服务地址	syslog 的服务地址（上限为 5 个，不可重复）

1.3.4.4 Snmp 告警方式设置

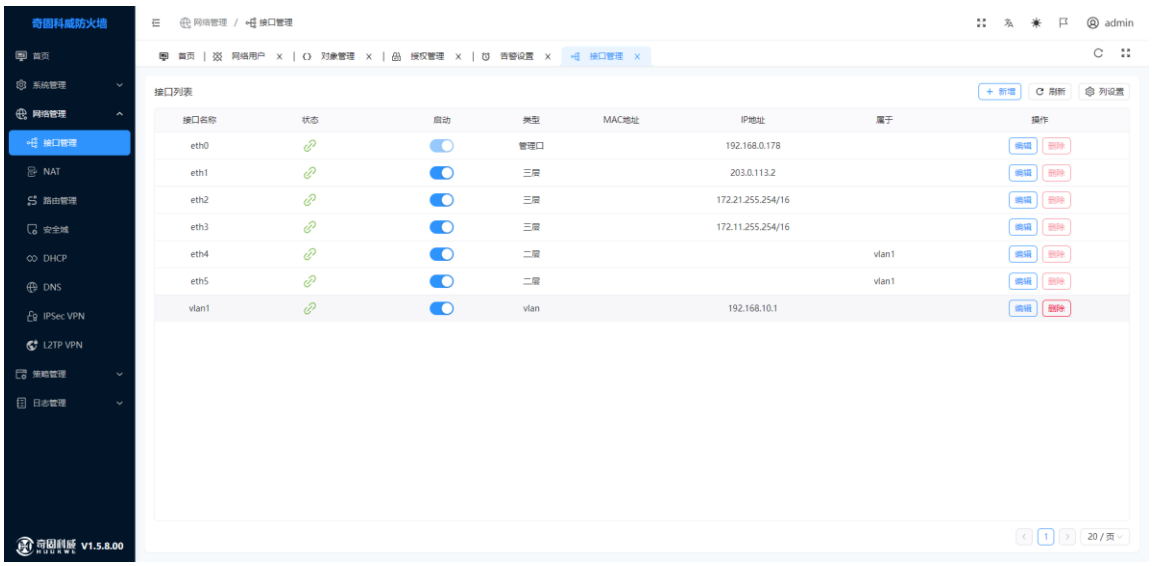


通过配置，当出现告警时，会将通知推送到对应的 snmp 服务上

配置项	说明
管理接口配置	通过配置管接口用来配置当前系统的 IP 配置
启动监听	启动后会启动防火墙和审计检引擎（实际根据功能配置），对当前网口上的所有数据包（实际根据功能配置），进行检测
设置	针对当前网口进行配置，

1.4 网络管理

1.4.1 接口配置



接口管理主要是围绕网口进行管理配置

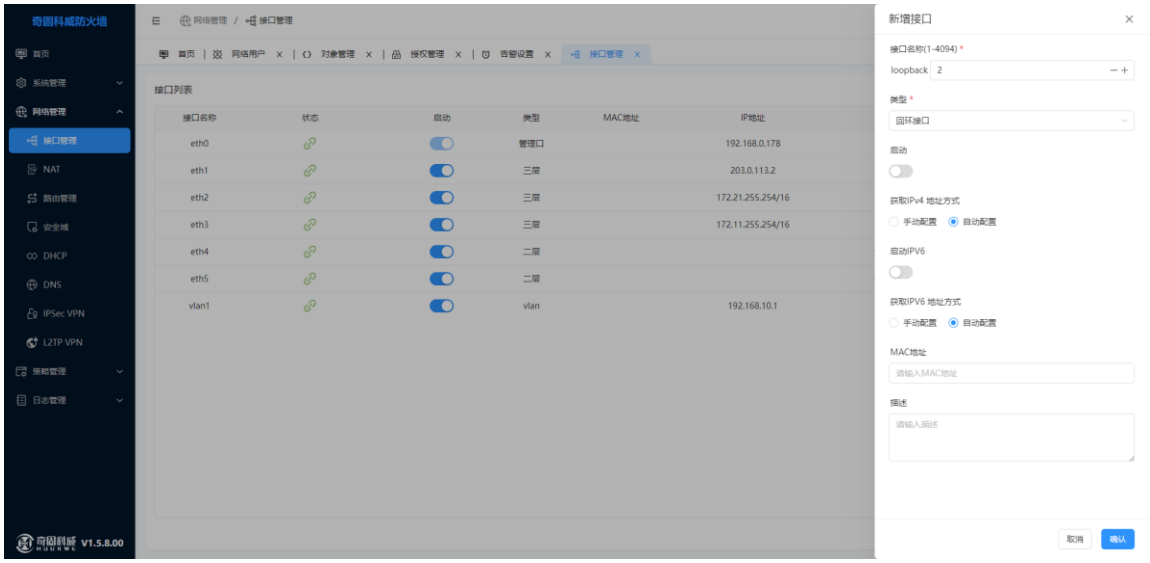
配置项	说明
接口名称	-
类型	Vlan、回环接口可新增 管理口、三层、二层不可新增
启动	启动/关闭
获取 IPv4 地址方式	手动/自动
类型	
启动 IPv6	-
获取 IPv6 地址方式	手动/自动
IPv4	-
IPv6	-
Mac	-
模式	二层支持 Access / Trunk
Navtive vlan	可选 Vlan
从属 vlan	可选 Vlan

描述	描述信息

新增

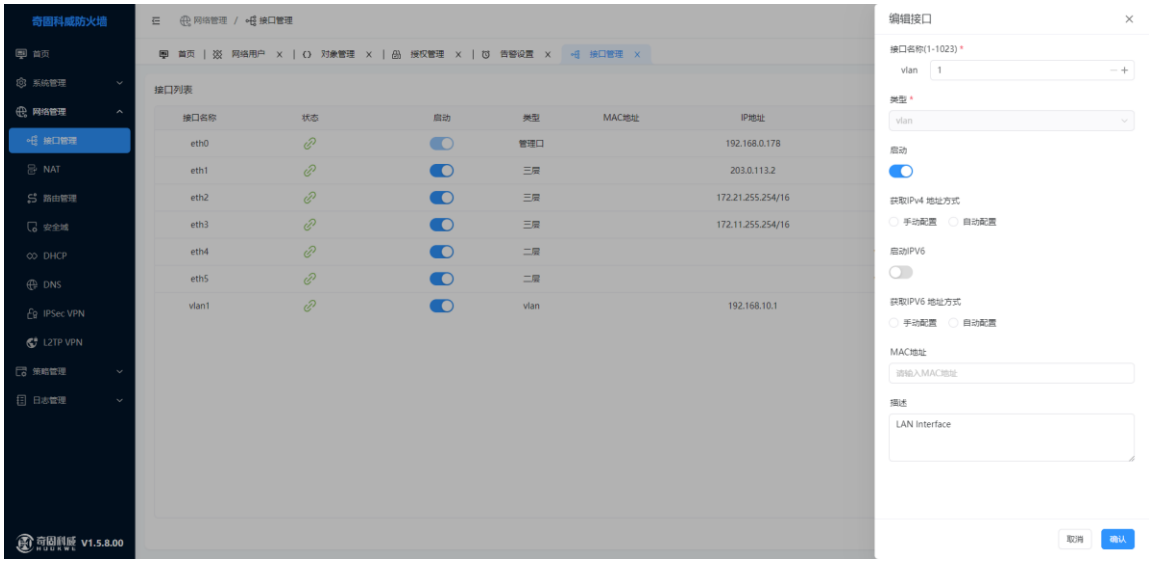
点击新增按钮，设置需要新增的接口名称、类型等。点击保存创建成功。如下图

注： 类型可选回环接口与 vlan 接口



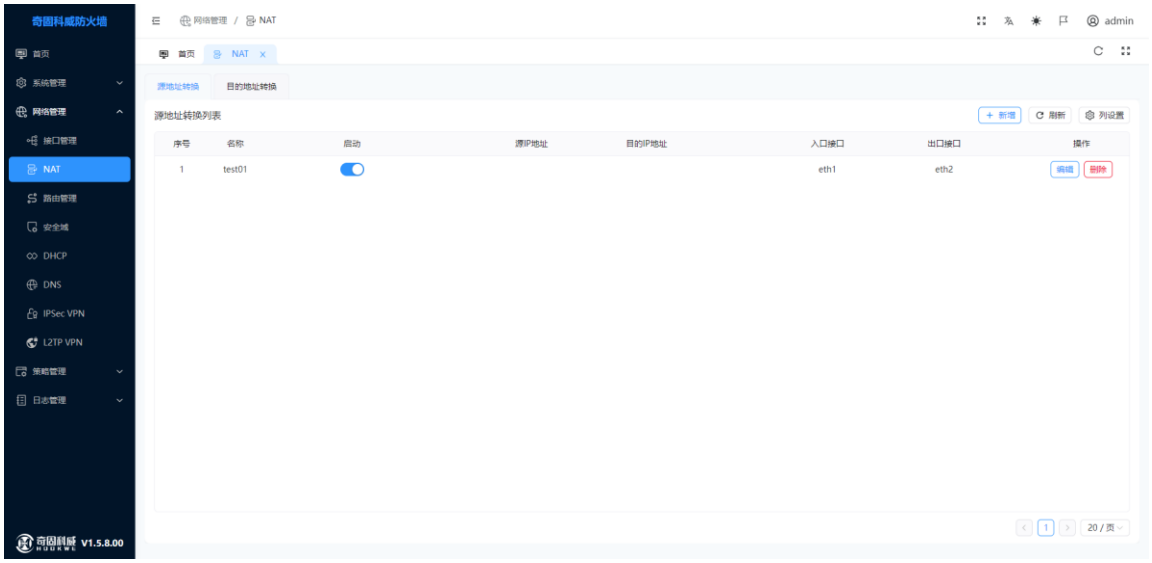
编辑

点击列表中的编辑按钮，可以当前项进行修改操作。如下图



1.4.2 NAT

1.4.2.1 源地址转换



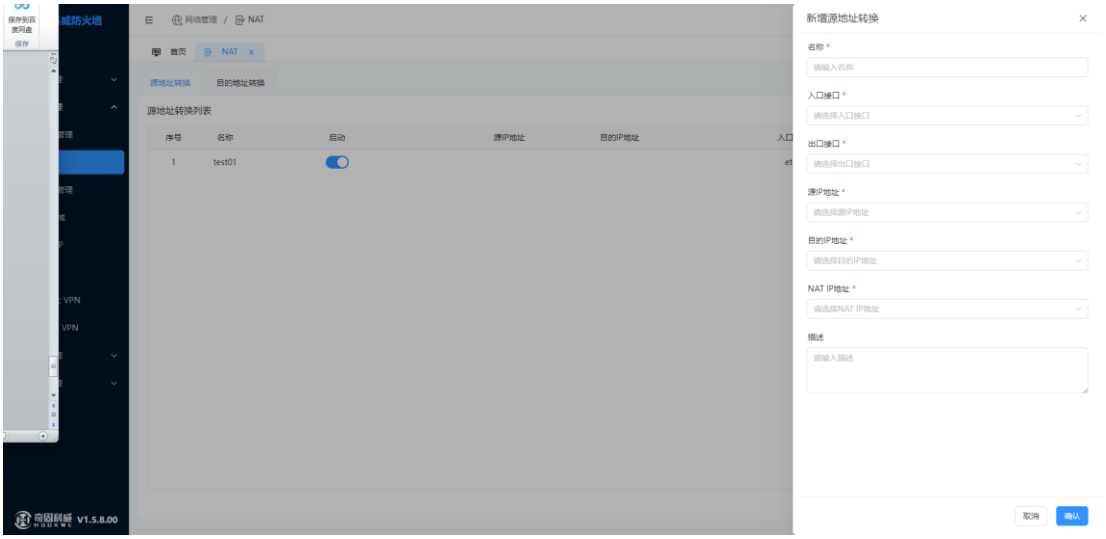
源地址转换可完成私有 IP 地址到公有 IP 地址的转换，使内网用户访问外网。

根据映射的 IP 地址数量， SNAT 可分为：单 IP 地址转换为单 IP 地址，多 IP 地址转换为单 IP 地址，多 IP 地址转换为多 IP 地址。

配置项	说明
名称	–
入口接口	可选 接口
出口接口	可选 接口
源 IP 地址	支持任意或列表 IP 对象（指对象管理下 IP 地址）或 IP 地址
目的 IP 地址	支持任意或列表 IP 对象（指对象管理下 IP 地址）或 IP 地址
NAT IP 地址	支持列表 IP 对象（指对象管理下 IP 地址）或 IP 地址
描述	描述信息

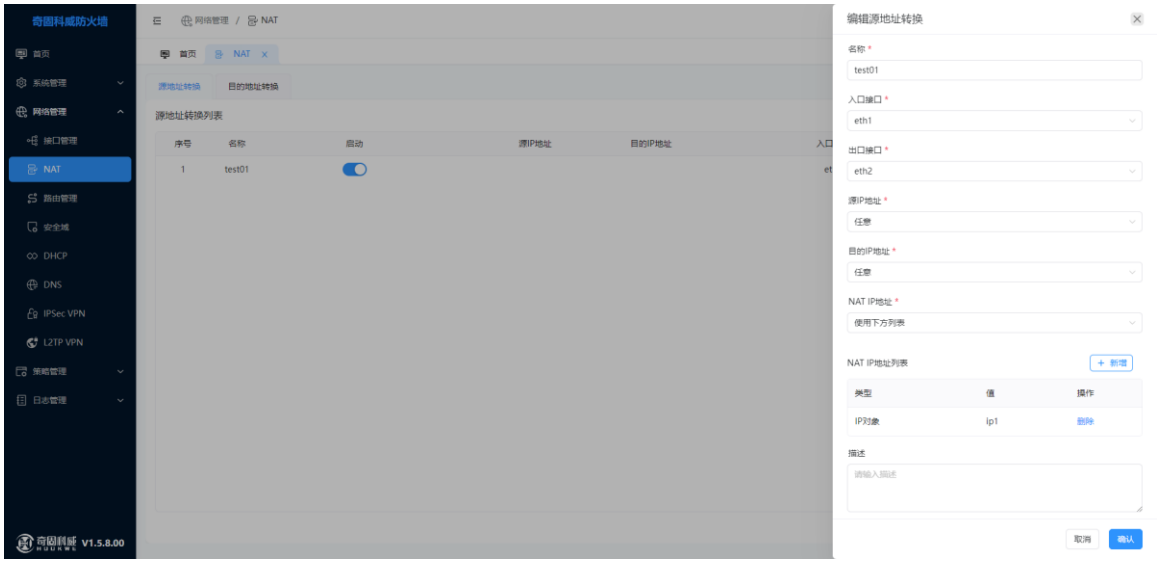
新增

点击新增按钮，设置需要新增的名称，入口接口、出口接口、源 IP 地址，目的 IP 地址、NAT IP 地址等。点击保存创建成功。如下图



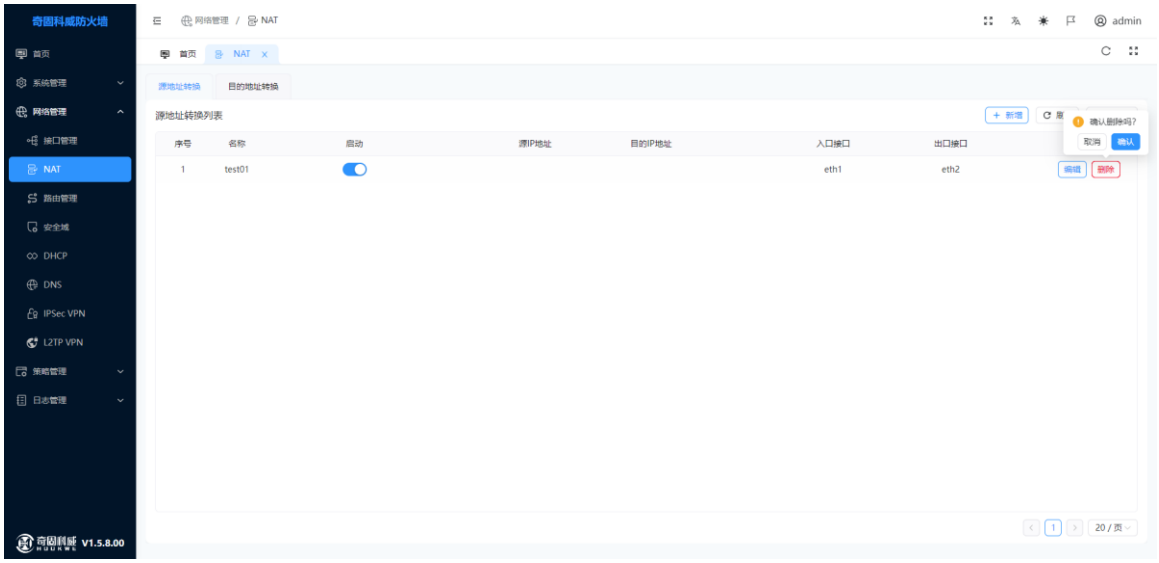
编辑

点击列表中的编辑按钮，可以当前项进行修改操作。如下图

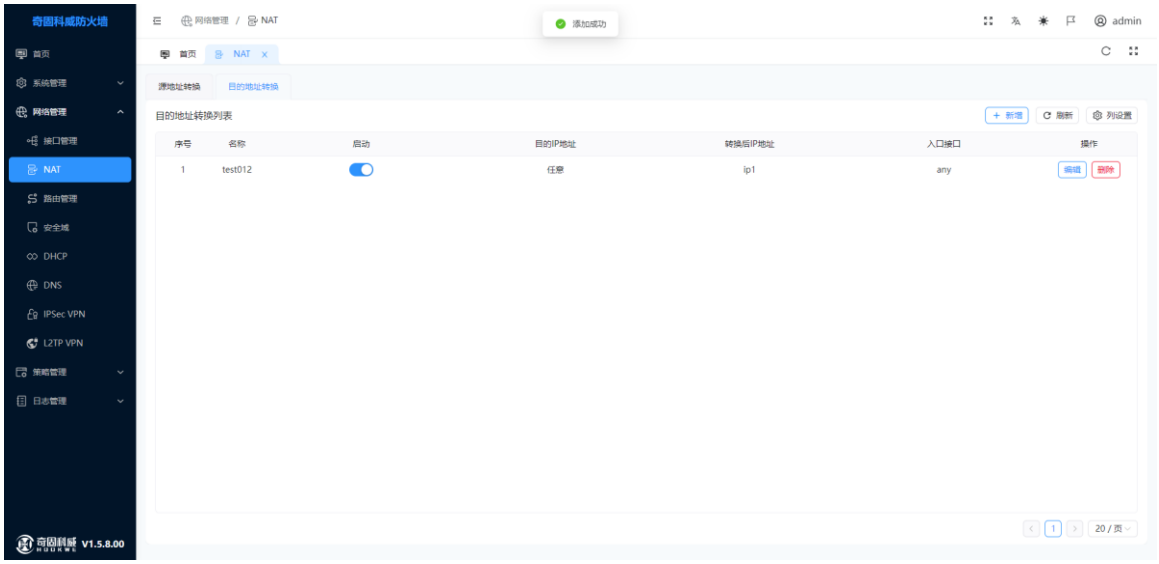


删除

点击列表中的删除进行删除。此操作不可逆，点击后确认后删除该条数据。如下图



1.4.2.2 目的地址转换



目的地址转换可完成公有 IP 地址到私有 IP 地址的转换，能够减小内网被外网攻击的可能性。 根据映射的 IP 地址数量， DNAT 可分为： 单 IP 地址转换为单 IP 地址。 单 IP 地址转换为多 IP 地址。

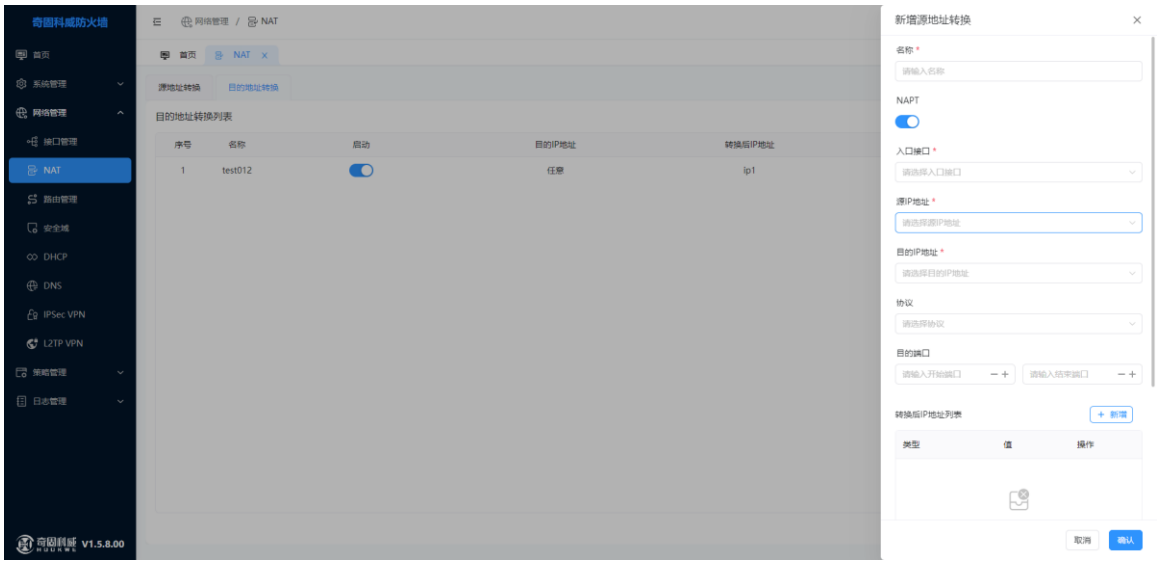
配置项	说明
名称	–
入口接口	可选 接口
NAPT	开启/关闭
源 IP 地址	支持任意或列表 IP 对象（指对象管理下 IP 地址）或 IP 地址

目的 IP 地址	支持任意或列表 IP 对象（指对象管理下 IP 地址）或 IP 地址
目的端口	第一个 开始端口 第二个 结束端口
转换后 IP 地址列表	支持列表 IP 对象（指对象管理下 IP 地址）或 IP 地址
协议	支持 TCP 与 UDP
转换后地址	第一个 开始端口 第二个 结束端口
协议	支持 TCP 与 UDP
描述	描述信息

新增

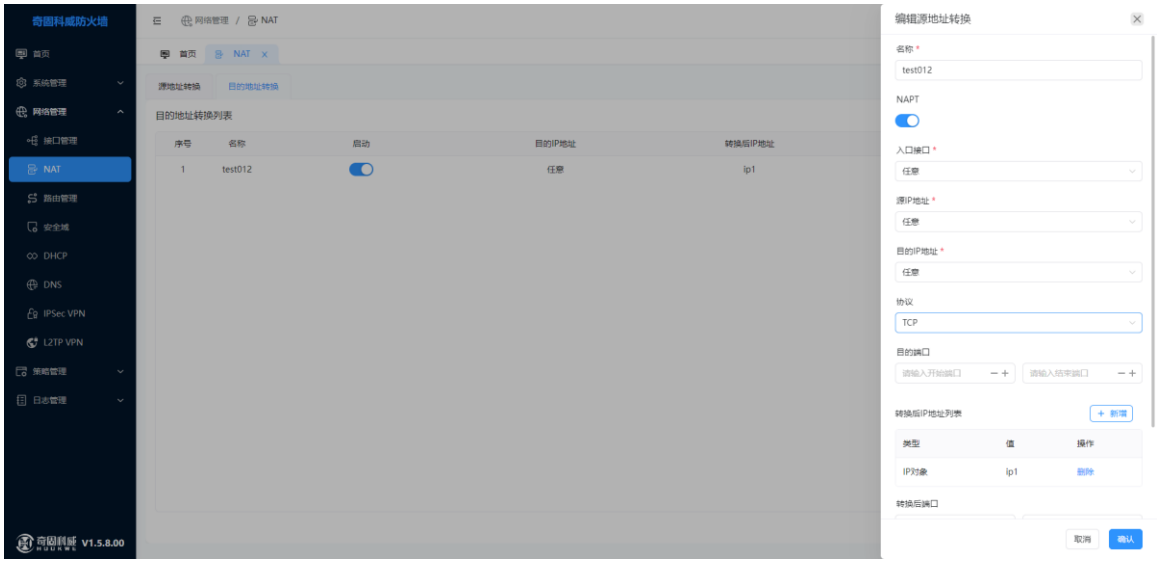
点击新增按钮，设置需要新增的名称，入口接口、源 IP 地址，目的 IP 地址、NAT IP 地址等。点击保存创建成功。如下图

注：支持 UDP 和 TCP 协议



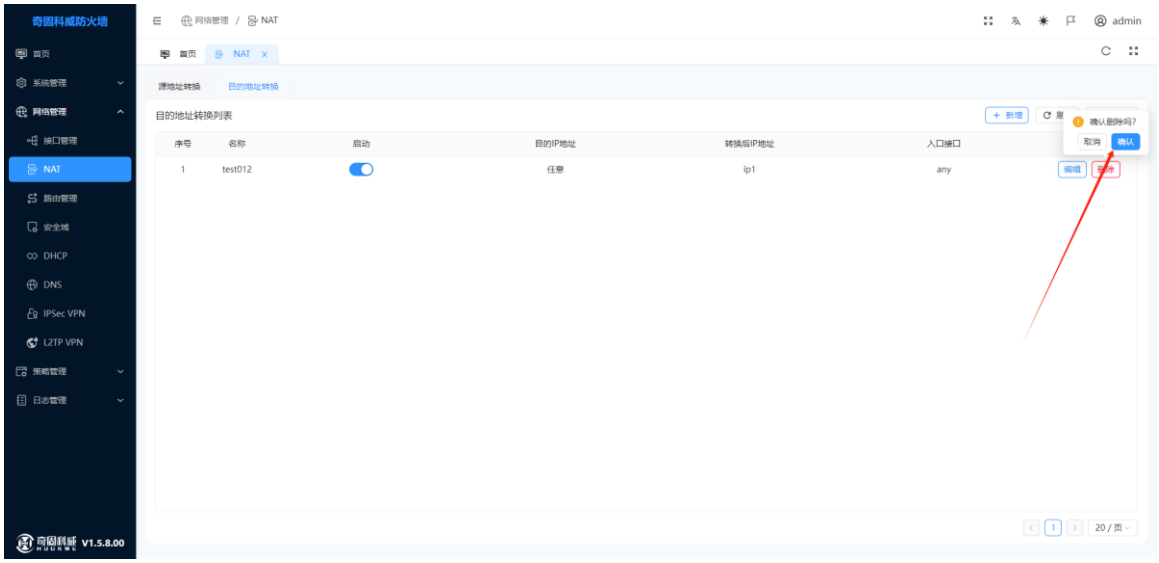
编辑

点击列表中的编辑按钮，可以当前项进行修改操作。如下图



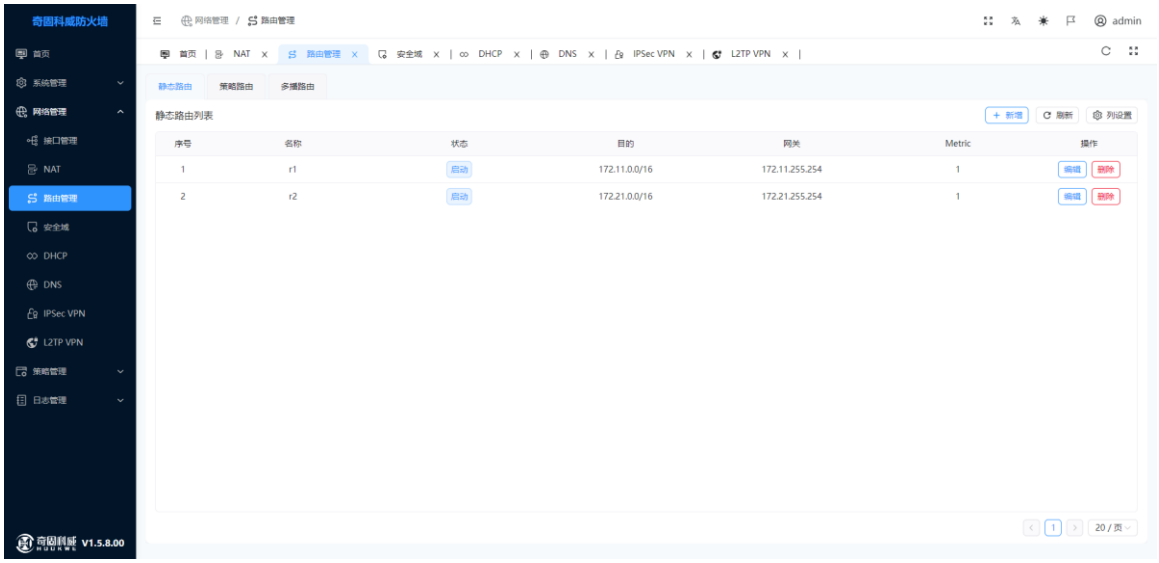
删除

点击列表中的删除进行删除。此操作不可逆，点击后确认后删除该条数据。如下图



1.4.3 路由管理

1.4.3.1 静态路由

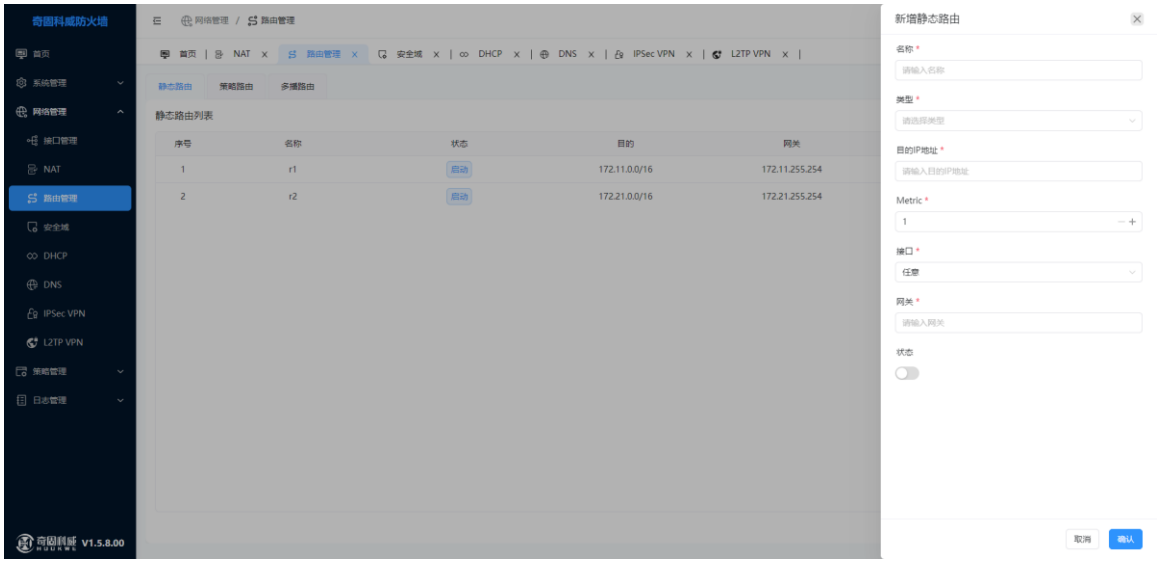


适用于规模较小且不经常变化的网络。由于静态路由不能自动适应网络变化，当网络拓扑结构发生变化时，需手动修改静态路由
信息。

配置项	说明
名称	-
类型	可选 IPv4 / IPv6
目的 IP 地址	根据类型 IPv4 示例：172.11.0.0/16 IPv6 示例： 240e:390:36f:e430:fdc3:d1a2:4213:2021
Metric	可取 1-255
接口	可选接口
网关	网关地址
状态	开启/关闭

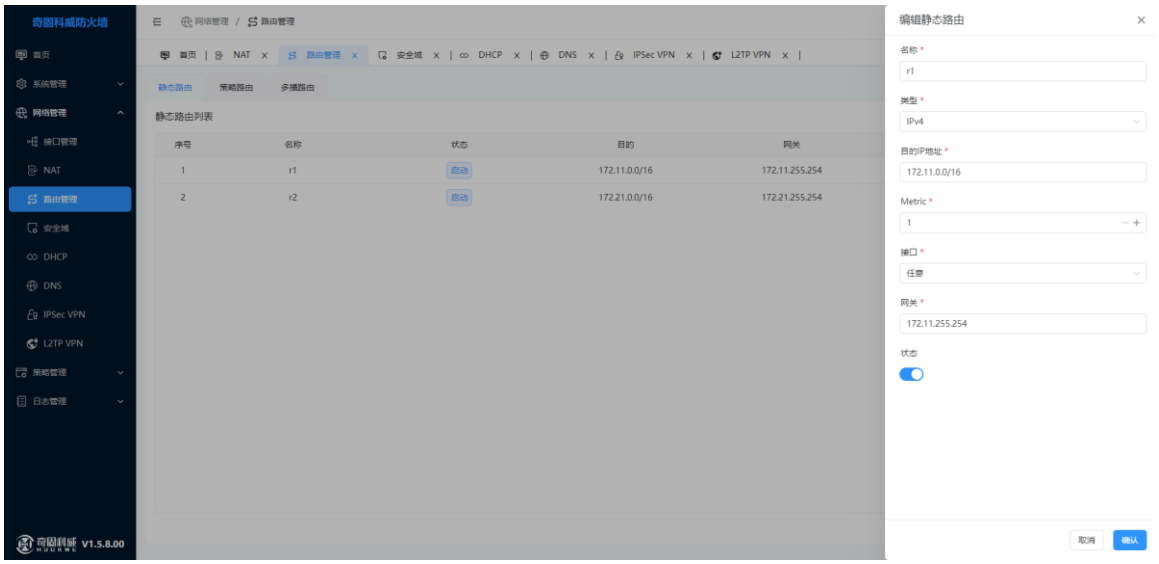
新增

点击新增按钮，设置需要新增的名称、类型、目的 IP 地址、Metric、接口、网关等。点击保存创建成功。如下图



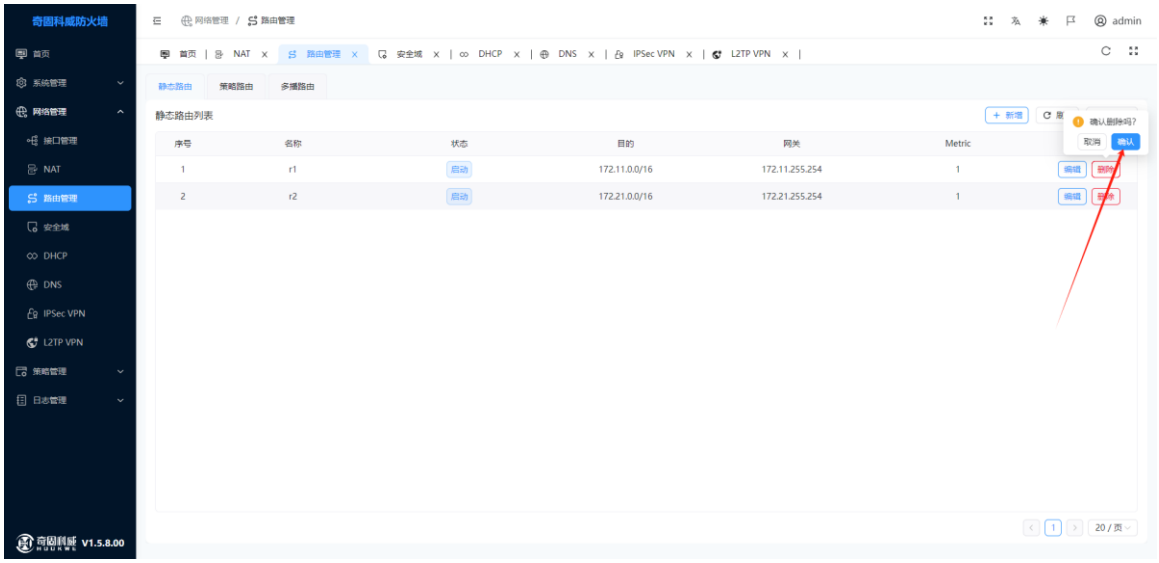
编辑

点击列表中的编辑按钮，可以当前项进行修改操作。如下图

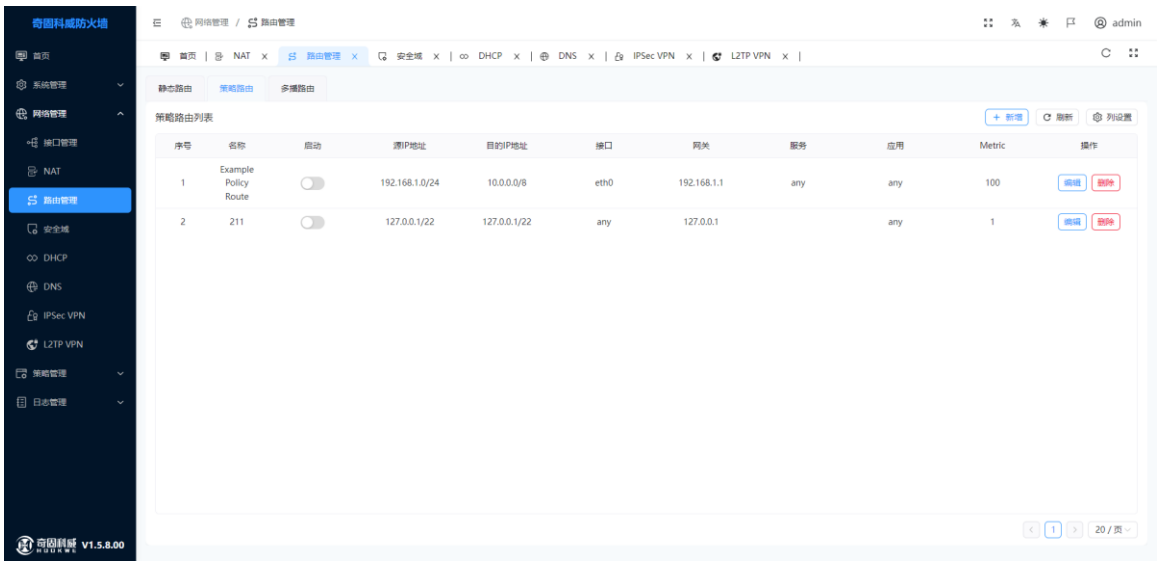


删除

点击列表中的删除进行删除。此操作不可逆，点击后确认后删除该条数据。如下图



1.4.3.2 策略路由



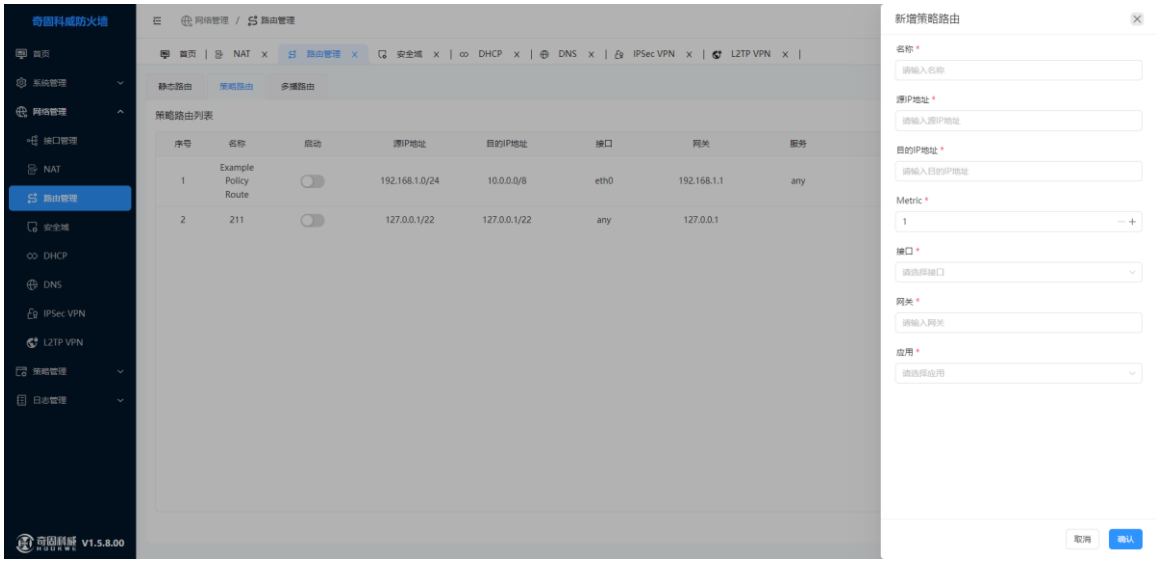
依据用户制定的策略进行路由选择的机制。与静态路由依照数据包的目的地址进行转发的方法不同，策略路由基于数据包的源地址、目的 IP、服务或者应用等信息灵活地进行路由选择。

配置项	说明
名称	-
源 IP 地址	IPv4 示例：172.11.0.0/16
目的 IP 地址	IPv4 示例：172.11.0.0/16
Metric	可取 1-255

接口	可选接口
网关	网关地址
状态	开启/关闭

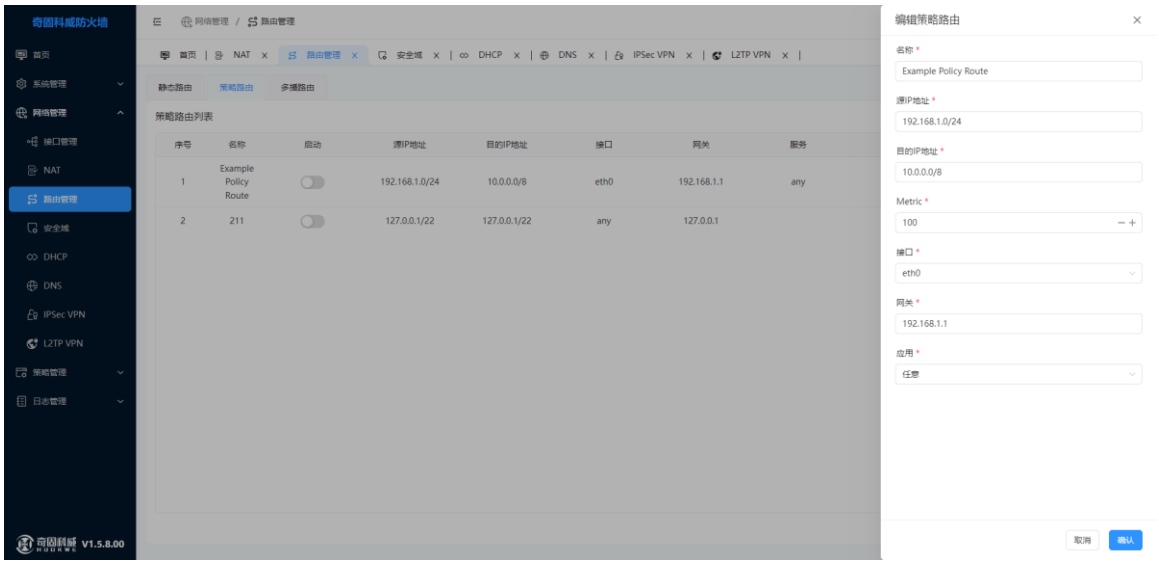
新增

点击新增按钮，设置需要新增的名称、类型、目的 IP 地址、Metric、接口、网关等。点击保存创建成功。如下图



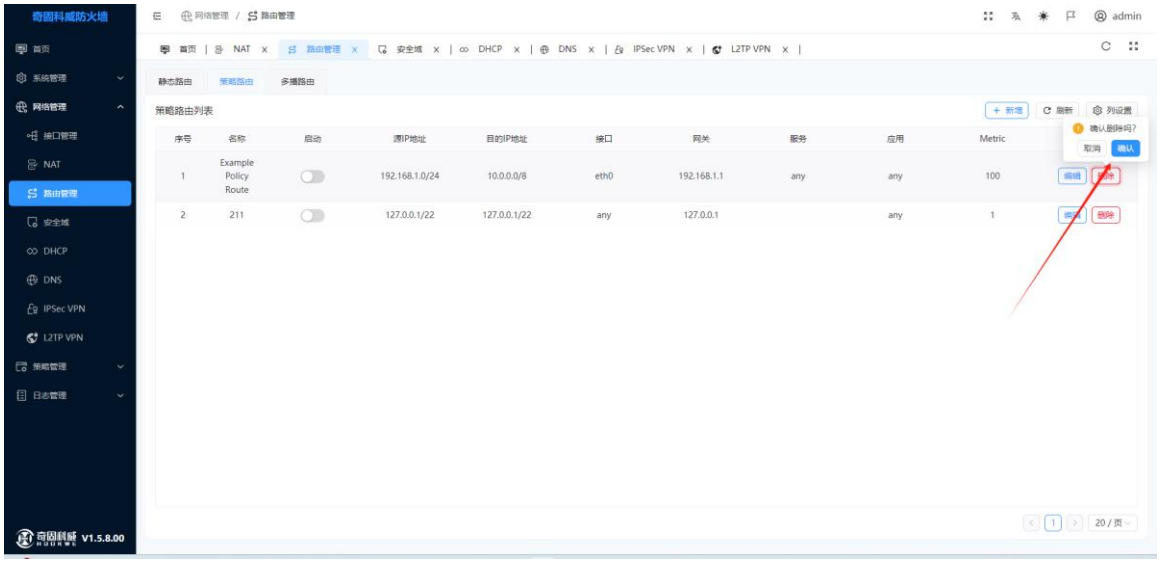
编辑

点击列表中的编辑按钮，可以当前项进行修改操作。如下图

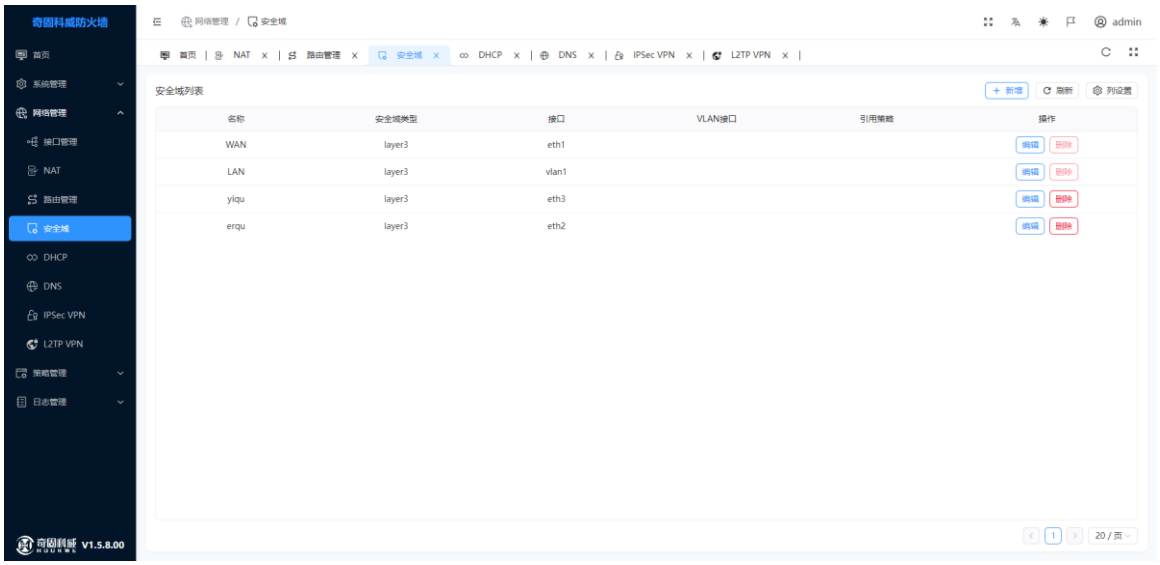


删除

点击列表中的删除进行删除。此操作不可逆，点击后确认后删除该条数据。如下图



1.4.4 安全域



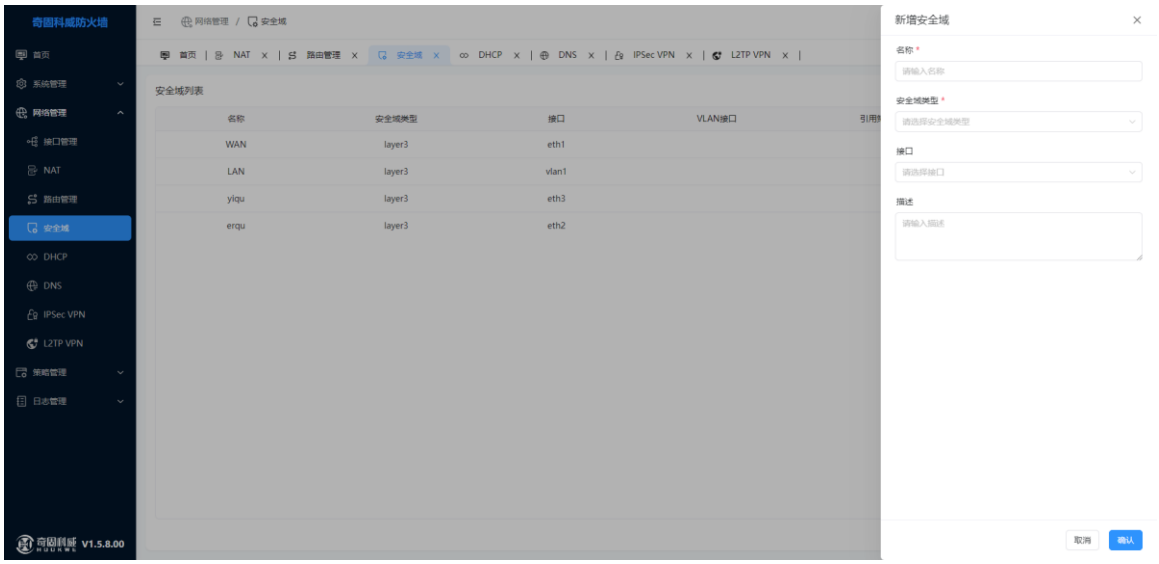
安全域是接口的集合。将接口绑定在一起使得 防火墙可以 对一个逻辑网络进行统一的安全控制

配置项	说明
名称	-
类型	二层/三层
目的 IP 地址	IPv4 示例：172.11.0.0/16
接口	可选接口
Vlan 接口	从属于的 vlan

描述	描述信息

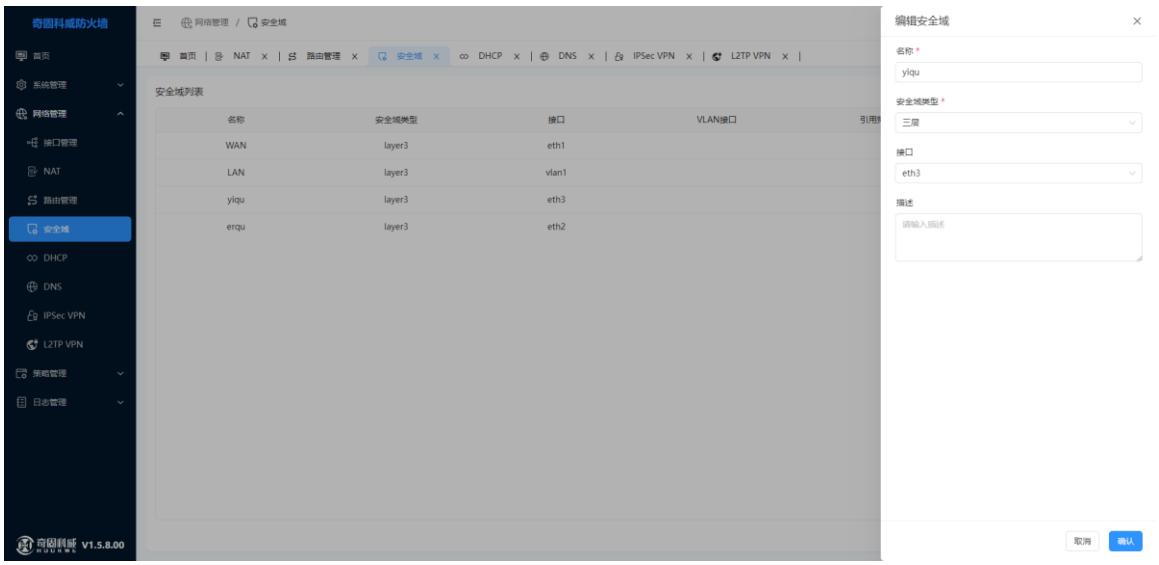
新增

点击新增按钮，设置需要新增的名称、安全域类型、接口等。点击保存创建成功。如下图



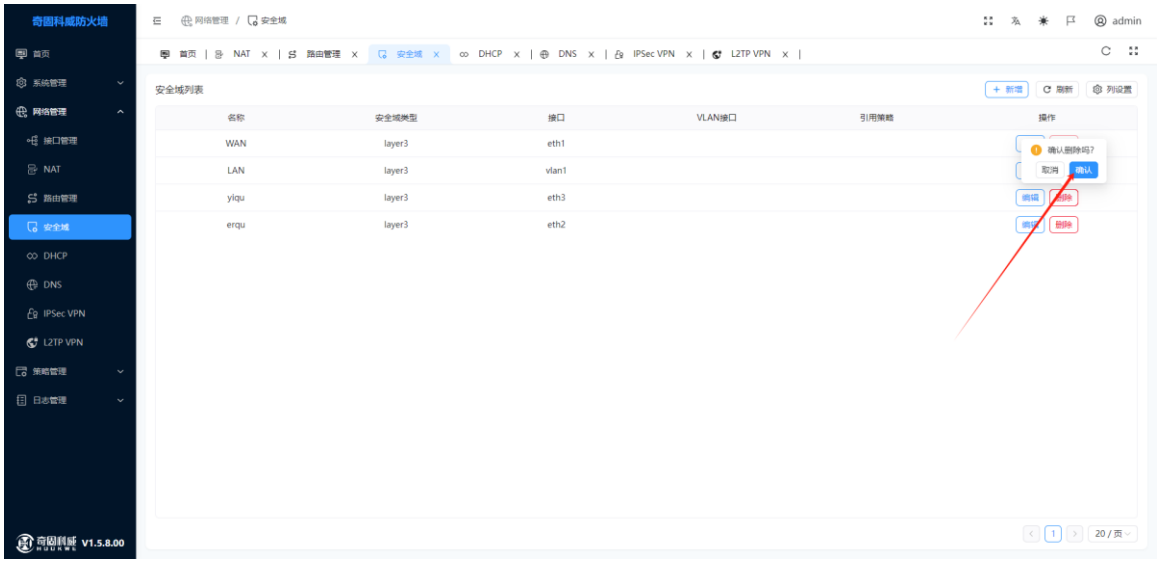
编辑

点击列表中的编辑按钮，可以当前项进行修改操作。如下图



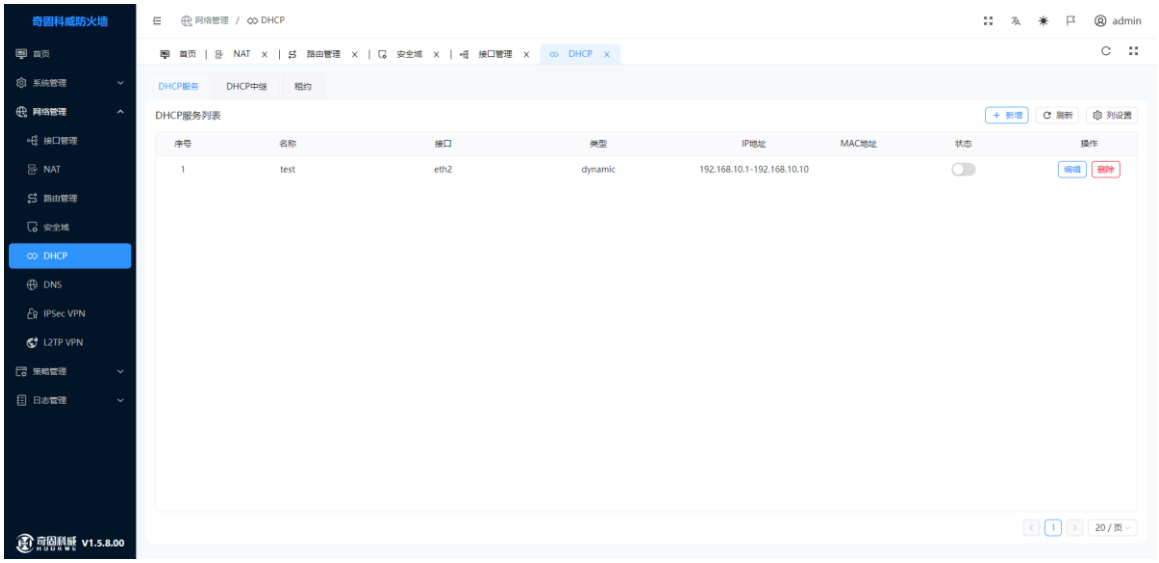
删除

点击列表中的删除进行删除。此操作不可逆，点击后确认后删除该条数据。如下图



1.4.5 DHCP

1.4.5.1 DHCP 服务



动态主机配置协议（Dynamic Host Configuration Protocol，DHCP）是基于 UDP 协议，并采用 CLIENT-SERVER 方式进行数据交互的网络通信协议，其报文格式共有八种，用来为网络中的主机动态地分配 IP 地址。此外，DHCP 还可以确保不使用重复地址和重新分配未使用的地址，并且可以自动为主机连接的子网分配适当的 IP 地址

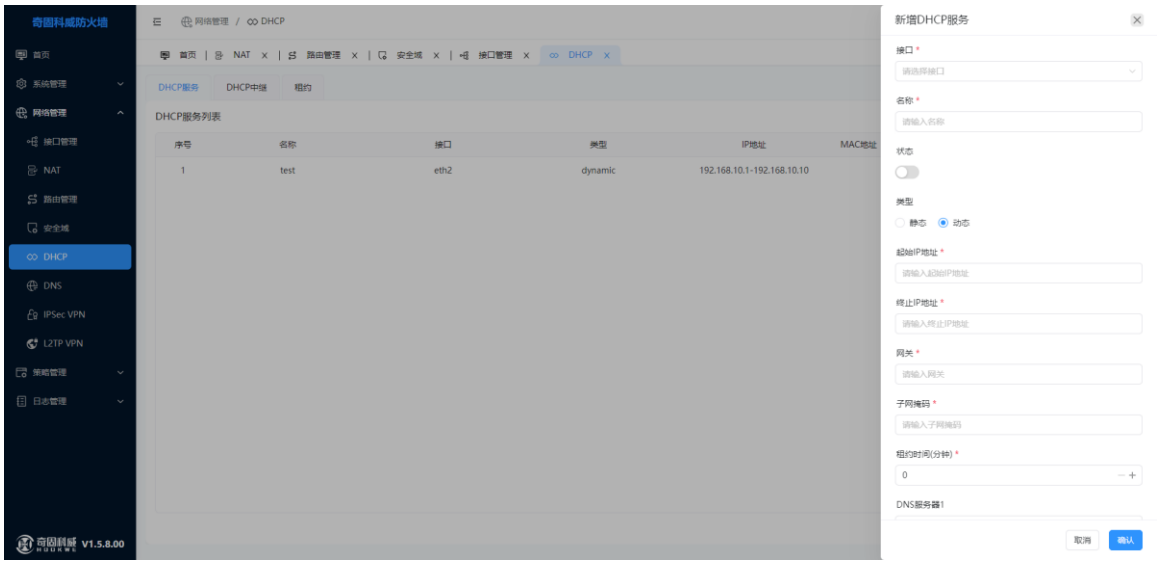
。

配置项	说明

名称	-
接口	可选接口
状态	启动/关闭
类型	静态/动态
起始 IP 地址	IPv4 地址
终止 IP 地址	IPv4 地址
网关	IPv4 地址
子网掩码	-
租约时间	-
IP 地址	IPv4 地址
DNS1 服务器	IPv4 地址
DNS2 服务器	IPv4 地址

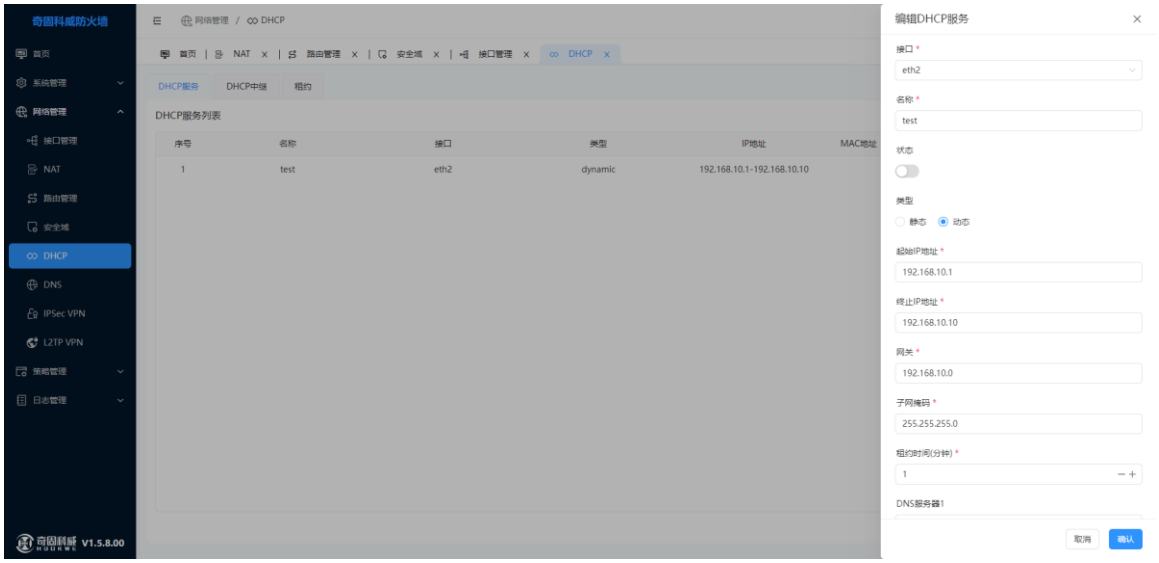
新增

点击新增按钮，设置需要新增的名称、接口、开始结束 IP、网关、子网掩码、租约时间等。点击保存创建成功。如下图



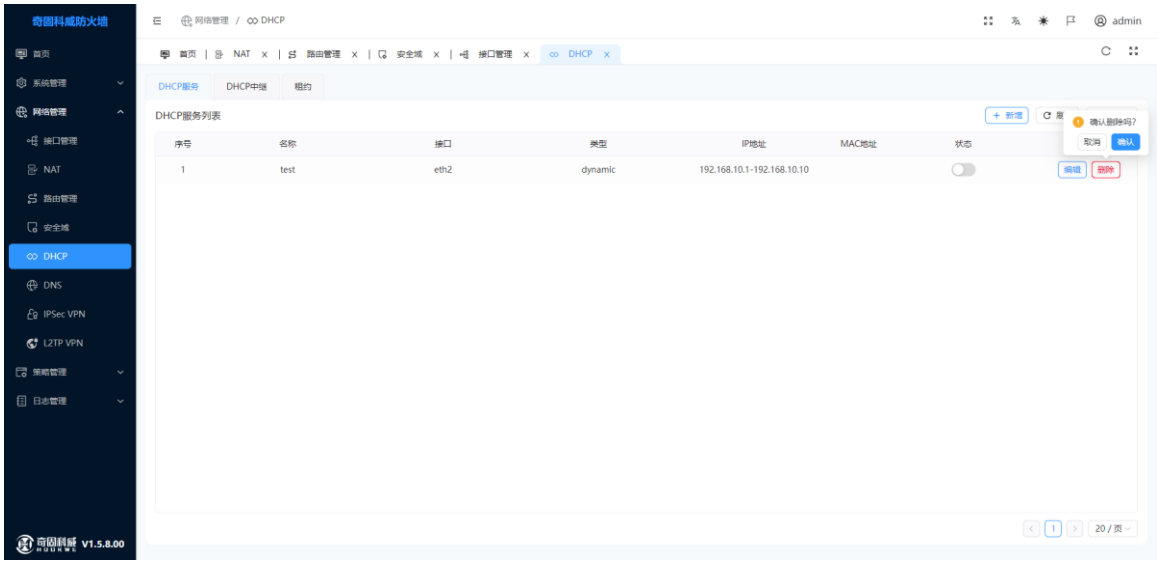
编辑

点击列表中的编辑按钮，可以当前项进行修改操作。如下图

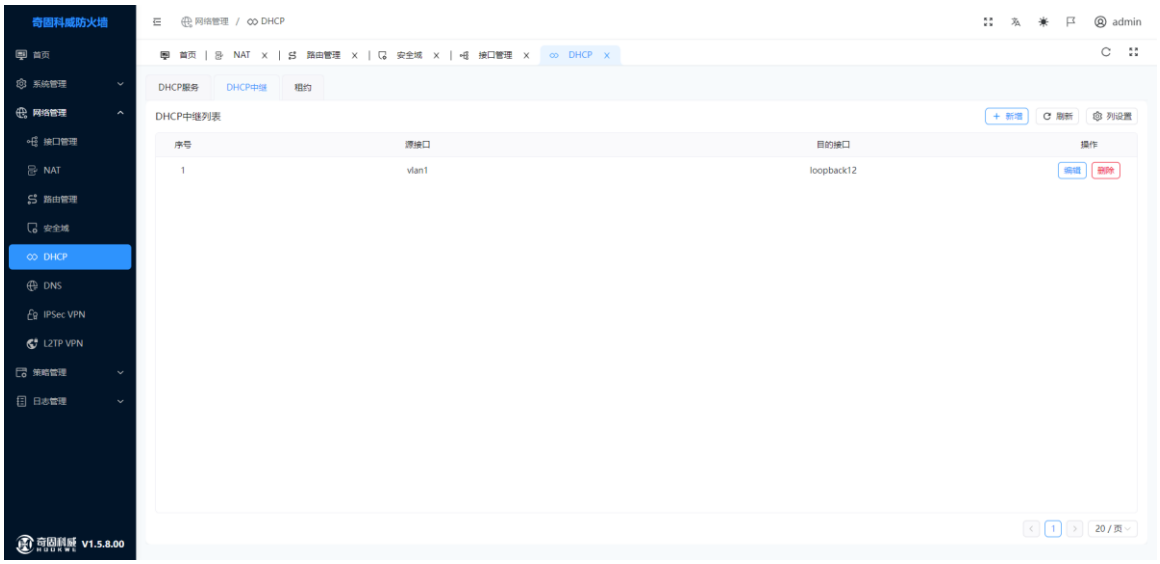


删除

点击列表中的删除进行删除。此操作不可逆，点击后确认后删除该条数据。如下图



1.4.5.2 DHCP 中继

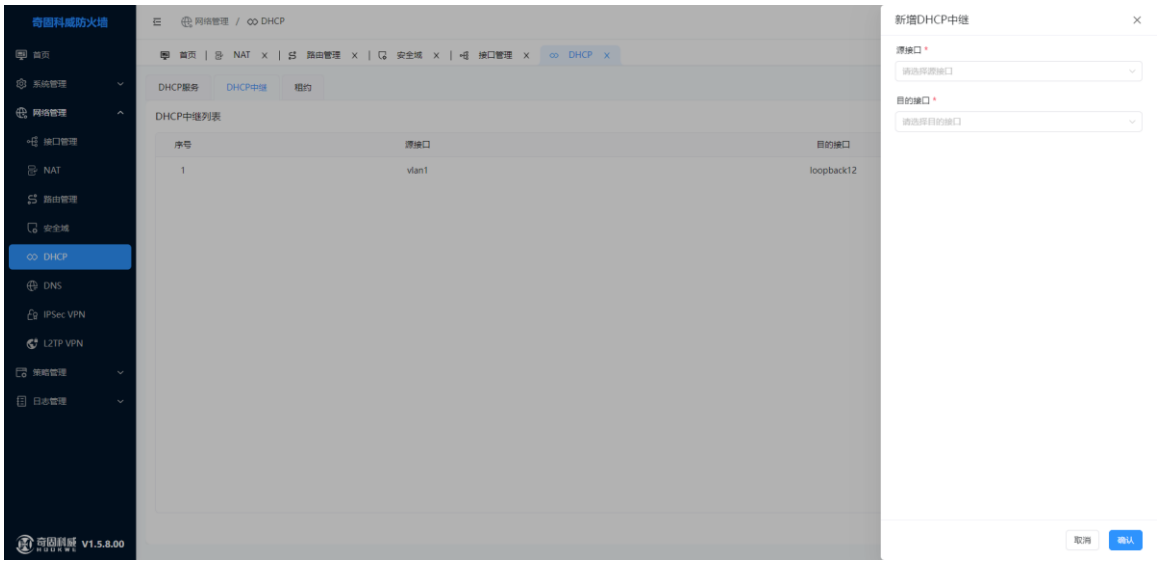


NF 允许操作员将三层接口（包括以太网接口、三层子接口以及 VLAN 接口）配置为 DHCP 中继，接收来自 DHCP 服务器的 DHCP 信息，然后将这些信息转发给任意安全区的 DHCP 客户端。

配置项	说明
源接口	可选接口
目的接口	可选接口

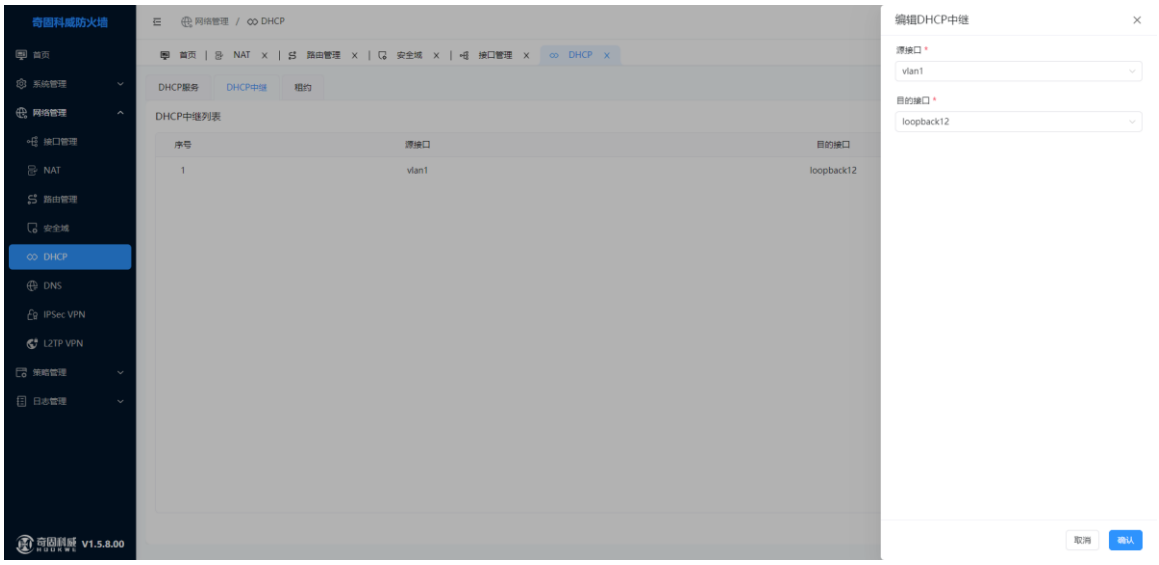
新增

点击新增按钮，设置需要新增的名称、接口、开始结束 IP、网关、子网掩码、租约时间等。点击保存创建成功。如下图



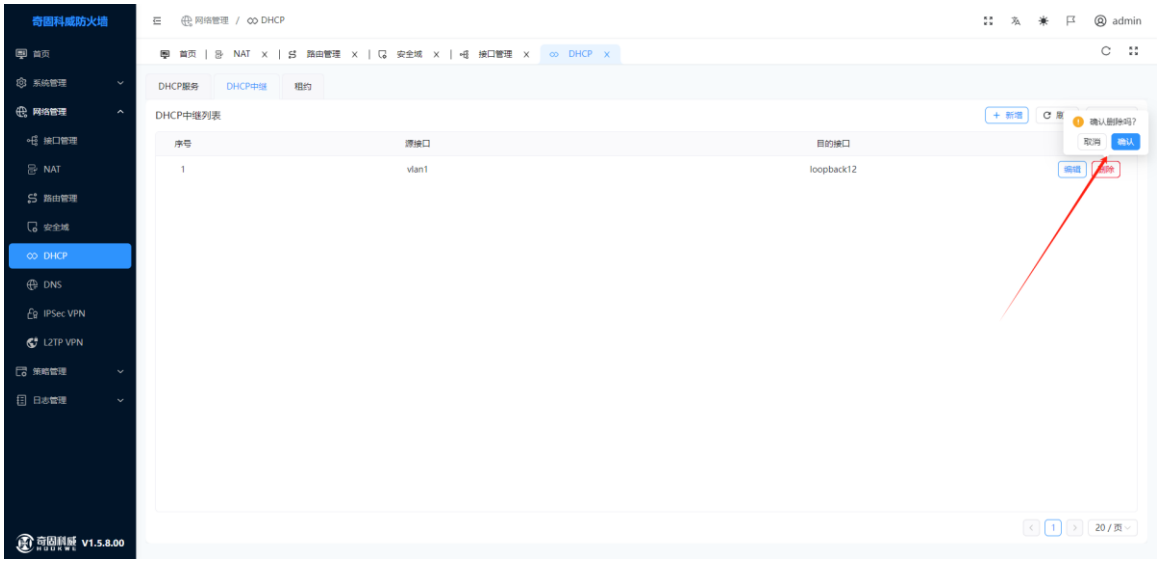
编辑

点击列表中的编辑按钮，可以当前项进行修改操作。如下图

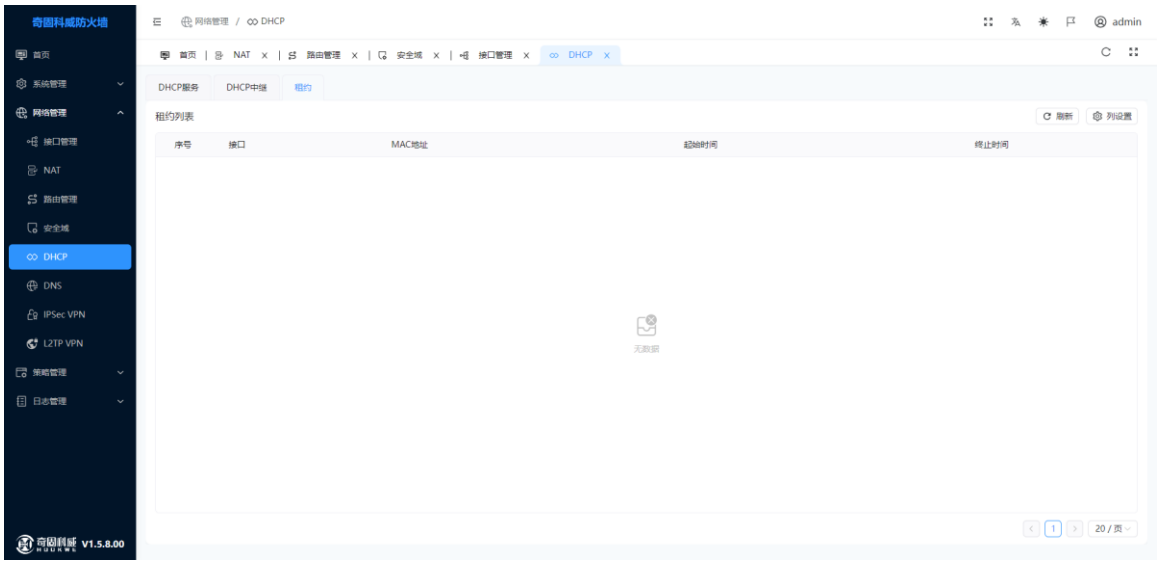


删除

点击列表中的删除进行删除。此操作不可逆，点击后确认后删除该条数据。如下图

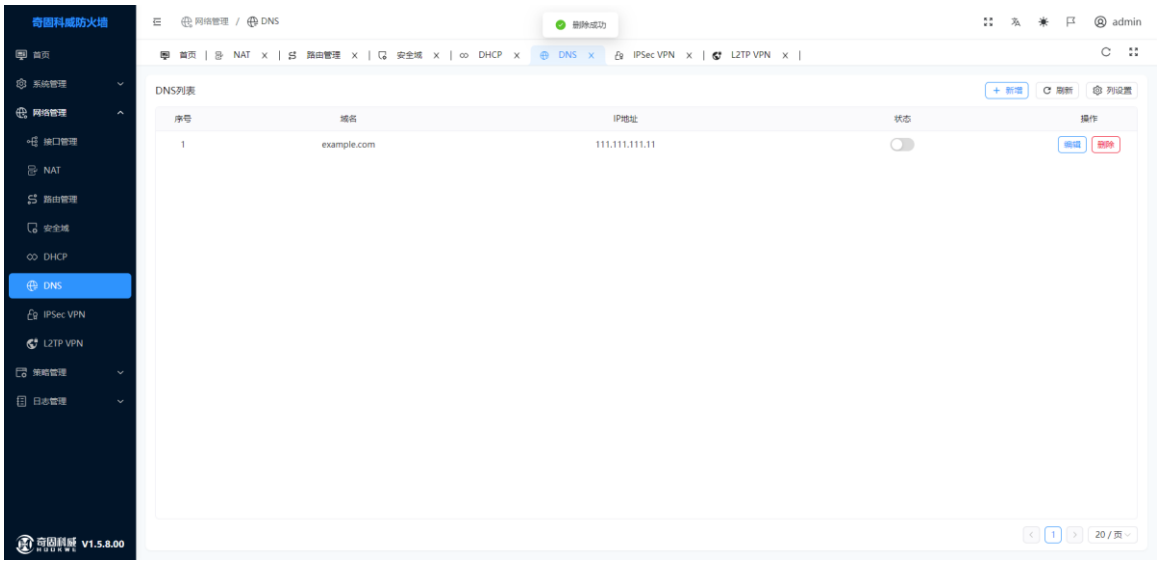


1.4.5.3 租约



当 防火墙充当 DHCP 服务器，并且成功为 DHCP 客户端分配了 IP 地址等网络配置参数时，管理用户可以查看相关的信息。

1.4.6 DNS

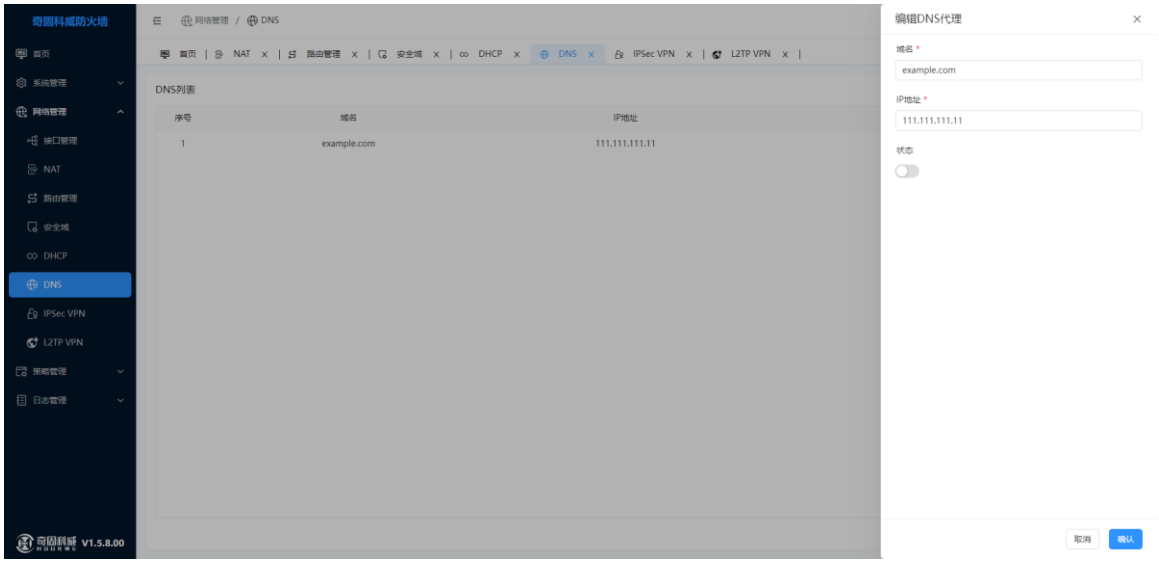


DNS 服务是互联网上非常重要和基础的服务之一，用来确定主机域名和 IP 地址之间的对应 关系

配置项	说明
域名	-
IP 地址	IPv4
状态	开启/关闭

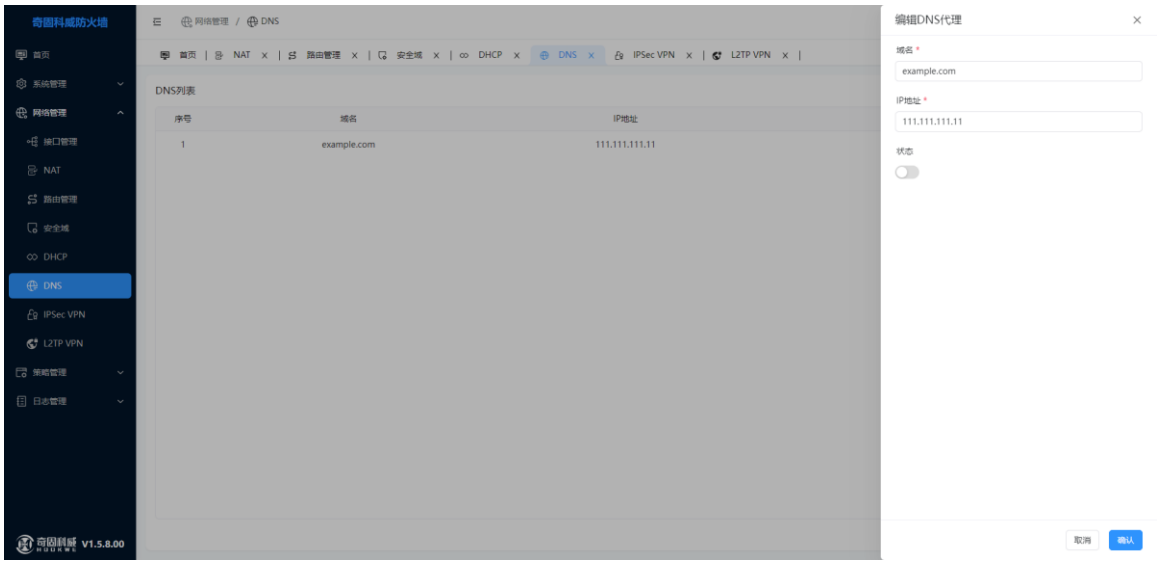
新增

点击新增按钮，设置需要新增的域名、IP 地址等。点击保存创建成功。如下图



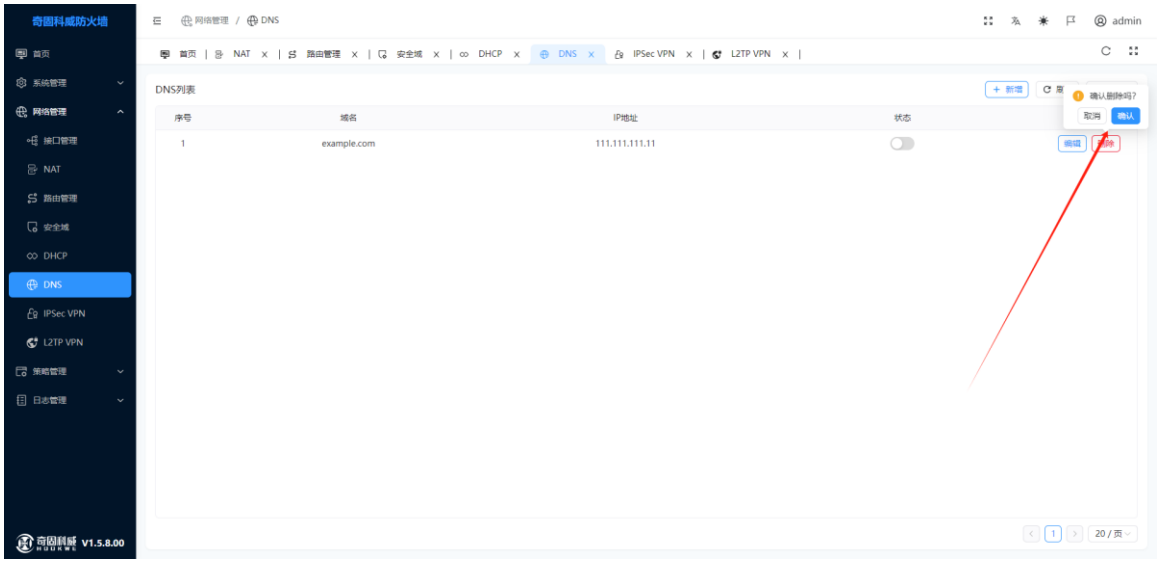
编辑

点击列表中的编辑按钮，可以当前项进行修改操作。如下图



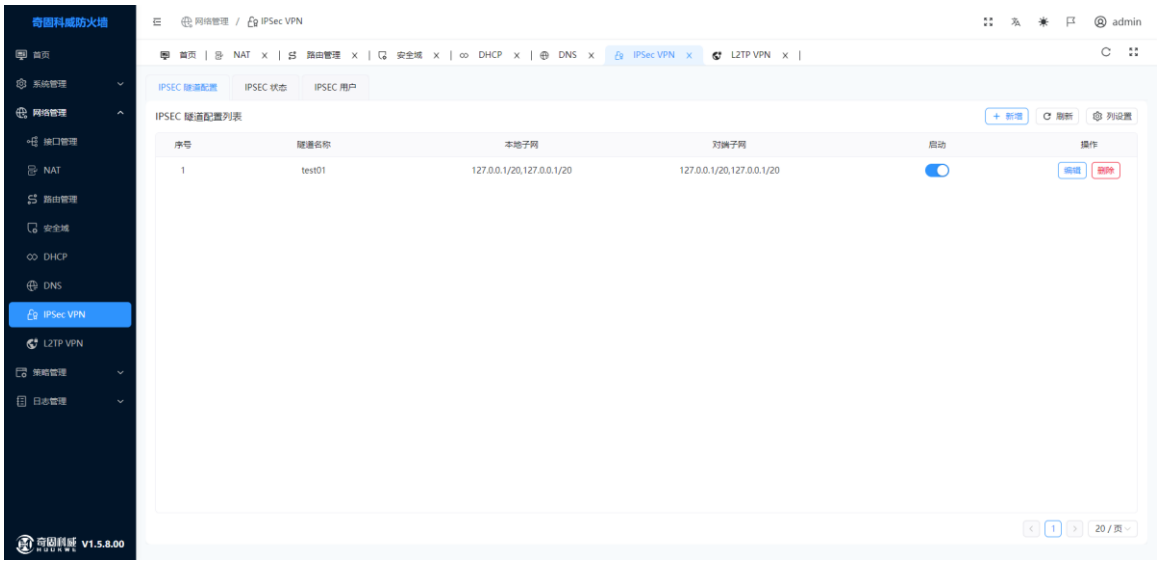
删除

点击列表中的删除进行删除。此操作不可逆，点击后确认后删除该条数据。如下图



1.4.7 IPSec VPN

1.4.7.1 IPSEC 隧道配置

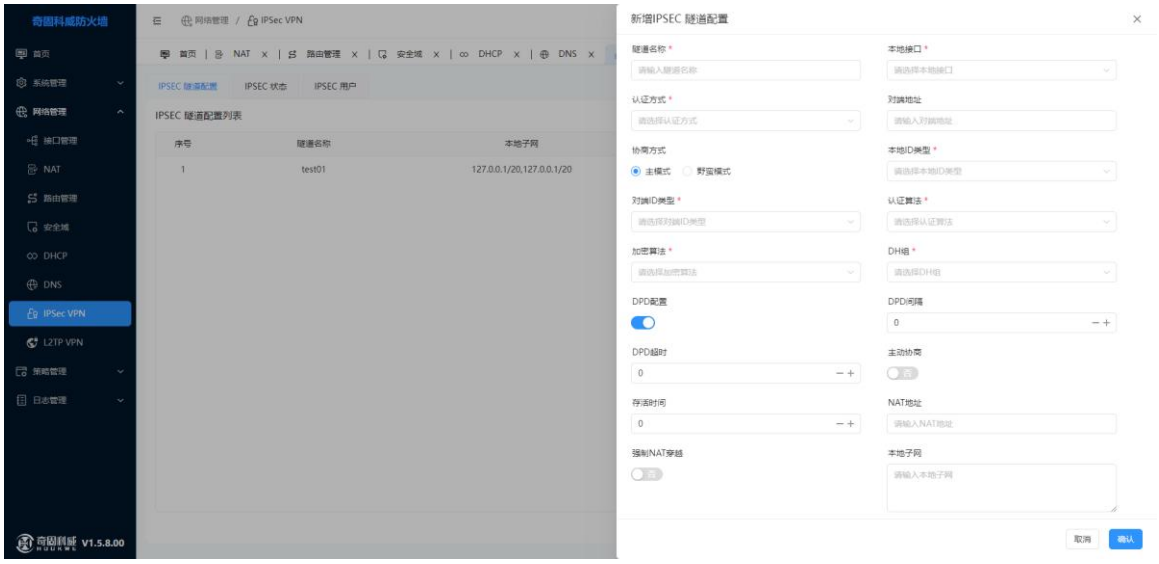


配置项	说明
隧道名称	–
本地接口	可选 接口
认证方式	预共享秘钥
对端地址	IPv4 地址

协商模式	主模式/野蛮模式
本地 ID 类型	IP 地址/域名
本地 IP 地址	根据本地 ID 类型
对端 ID 类型	IP 地址/域名
对端 IP 地址	根据对端 ID 类型
认证算法	MD5 / SHA1
加密算法	支持 '3DES','AES-128','AES-192','AES-256','BLOWFISH','DES'
DH 组	支持 group1, group2, group3
DPD 配置	开启/关闭
DPD 间隔	-
DPD 超时	-
主动协商	开启/关闭
存活时间	-
NAT 地址	IPv4 地址
DH 组	支持 group1, group2, group3
强制 NAT 穿越	是/否
本地子网	支持 IPv4 地址单个或者多个 实例：127.0.0.1/20,127.0.0.1/20
对端子网	支持 IPv4 地址单个或者多个 实例：127.0.0.1/20,127.0.0.1/20
备注	备注信息

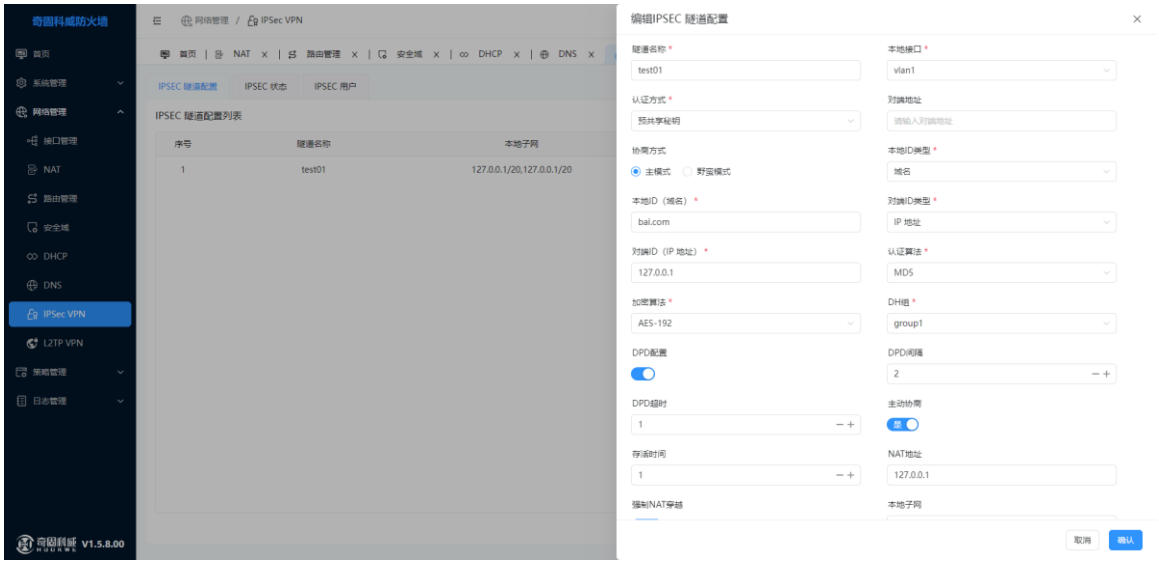
新增

点击新增按钮，设置需要新增的隧道名称、本地接口、认证方式、本地 ID 类型 对端 ID 类型、认证算法、加密算法 DH 组等。点击保存创建成功。如下图



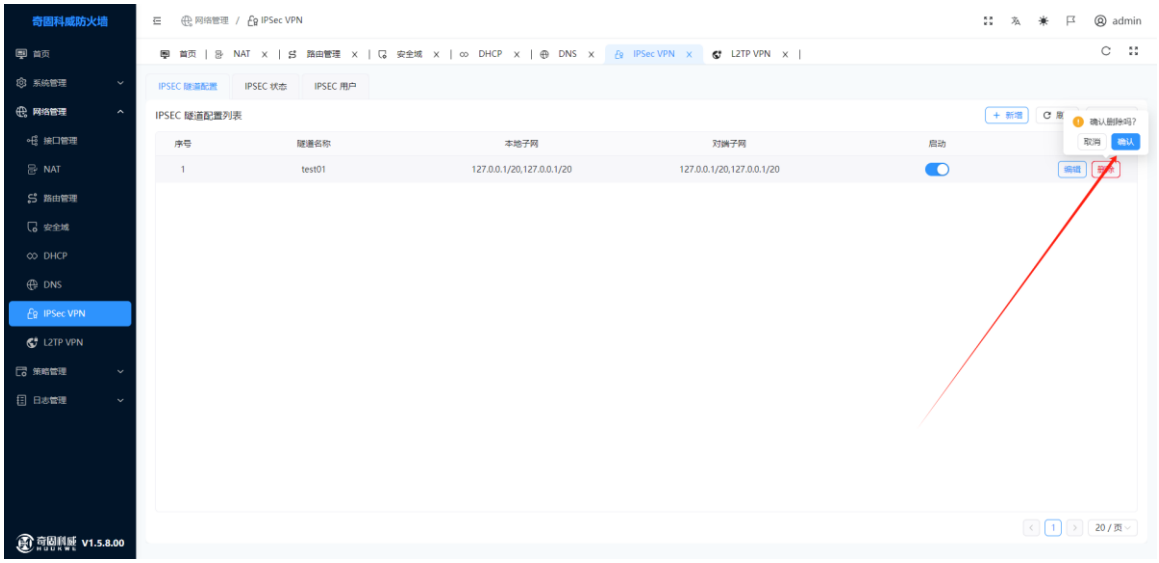
编辑

点击列表中的编辑按钮，可以当前项进行修改操作。如下图

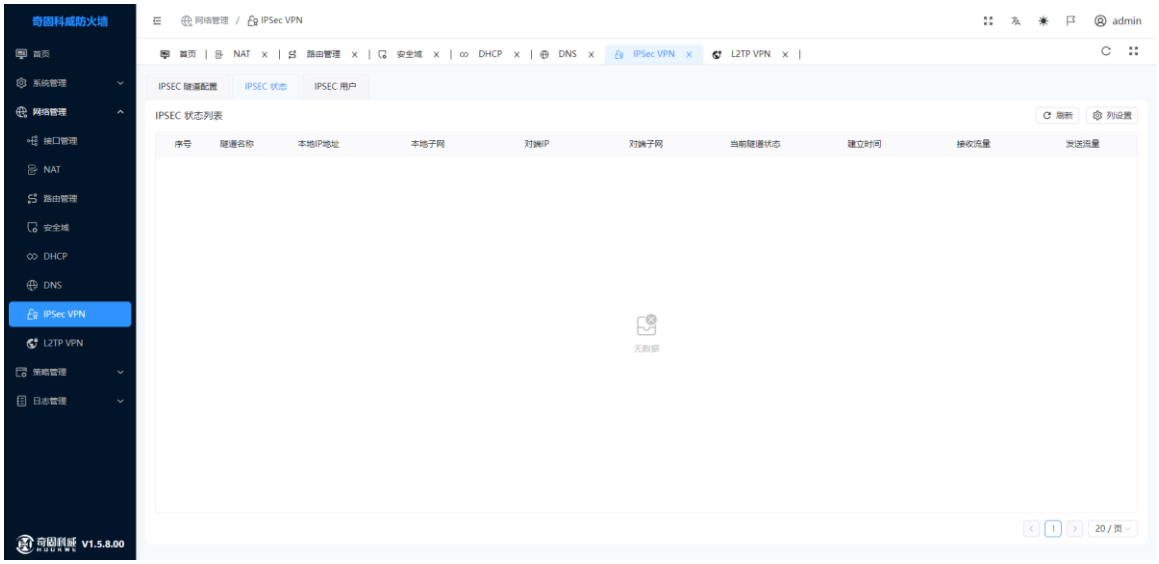


删除

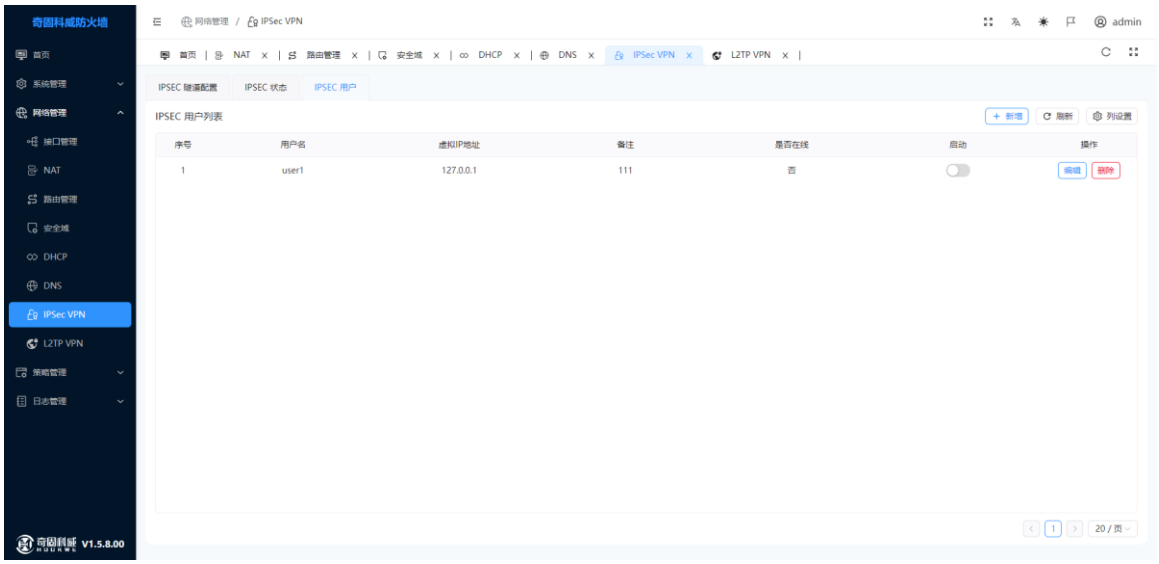
点击列表中的删除进行删除。此操作不可逆，点击后确认后删除该条数据。如下图



1.4.7.2 IPSEC 状态



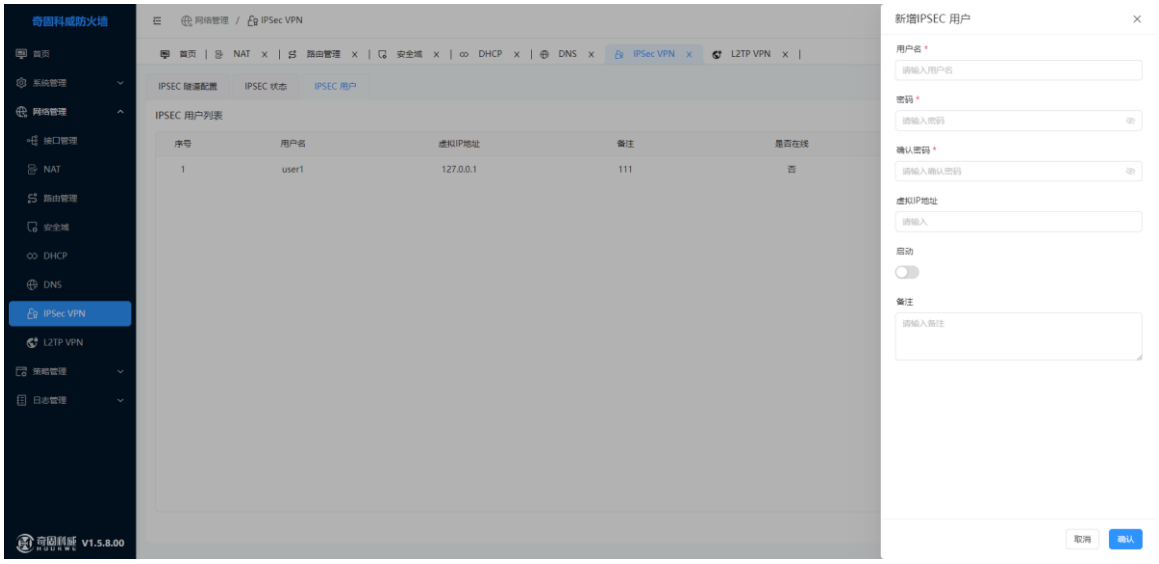
1.4.7.3 IPSEC 用户



配置项	说明
用户名	–
密码	用户密码（数字大小写字母特殊符号如何而成，最少三种组合）
确认密码	确认密码
虚拟 IP 地址	IPv4 地址
备注	备注信息

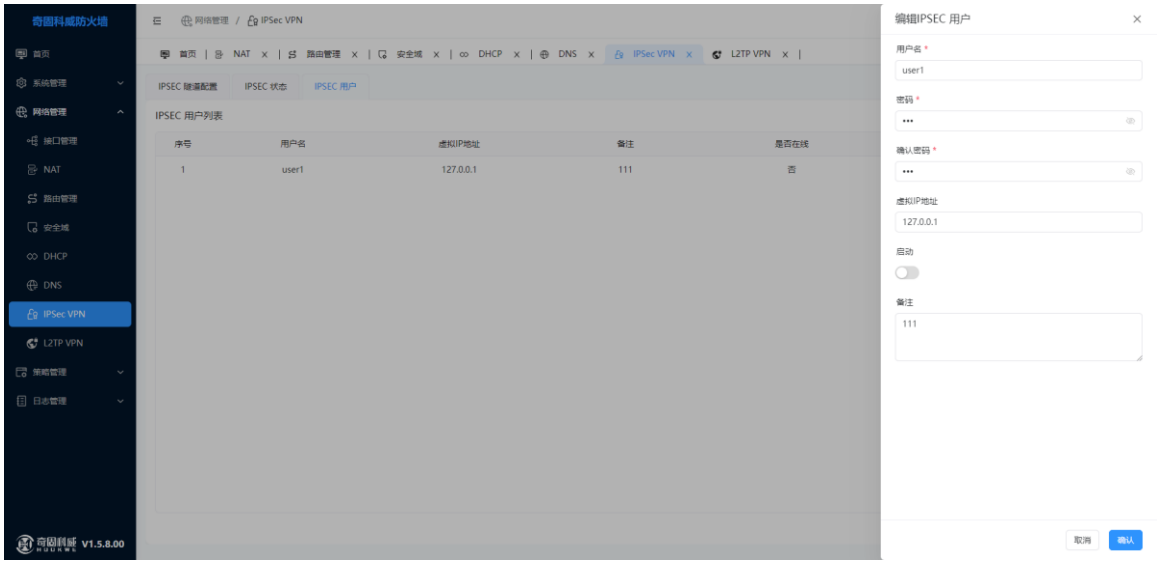
新增

点击新增按钮，设置需要新增的用户名、密码等。点击保存创建成功。如下图



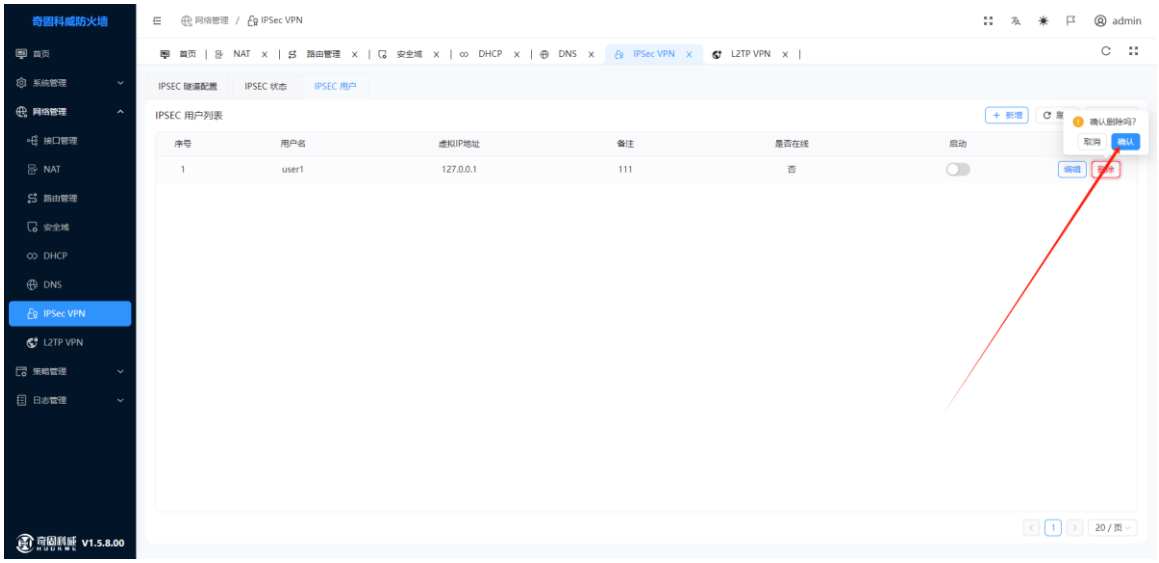
编辑

点击列表中的编辑按钮，可以当前项进行修改操作。如下图



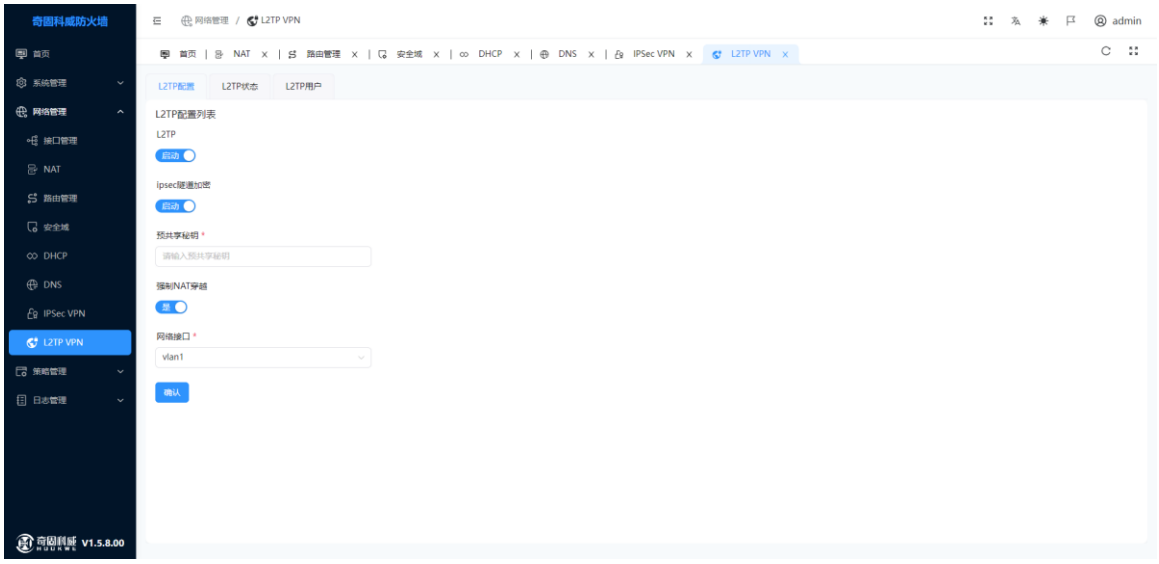
删除

点击列表中的删除进行删除。此操作不可逆，点击后确认后删除该条数据。如下图



1.4.8 L2TP VPN

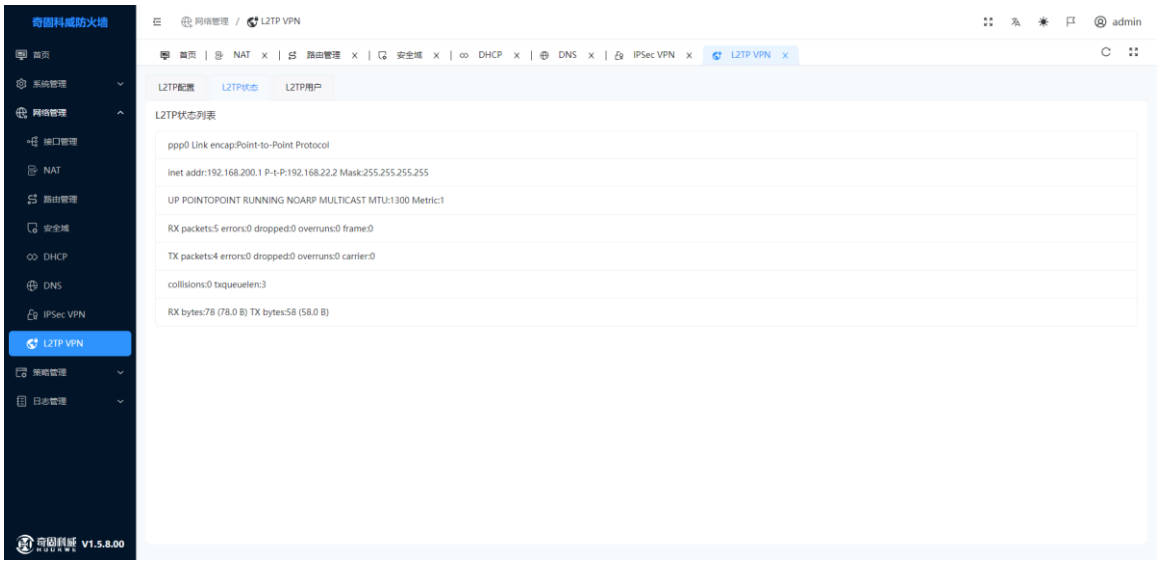
1.4.8.1 L2TP 配置



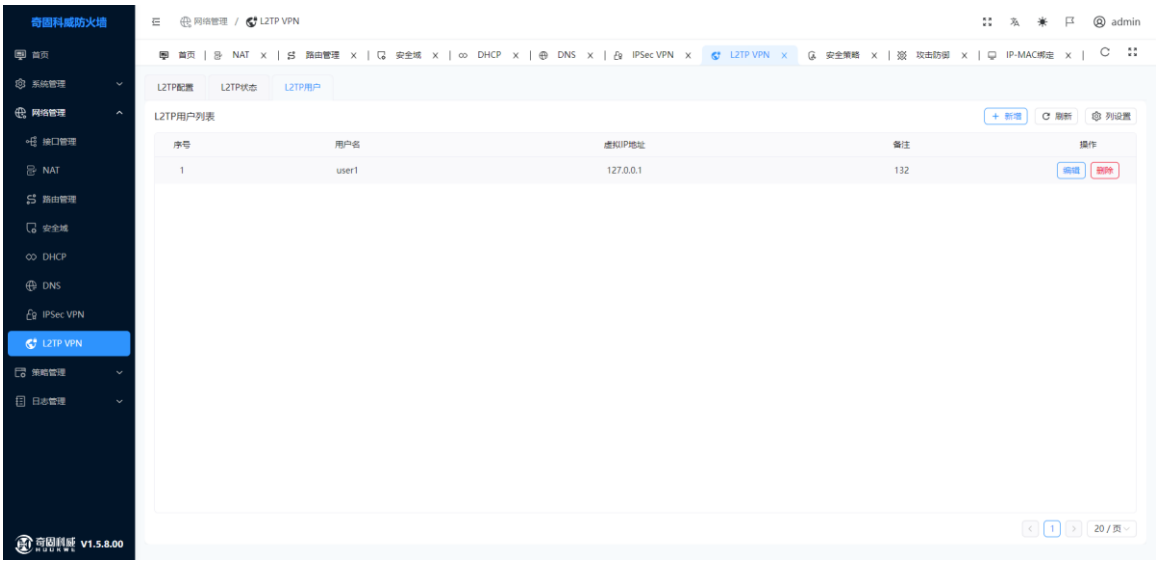
L2TP 是 VPDN（Virtual Private Dial-up Network，虚拟私有拨号网）隧道协议的一种，它是一种对 PPP 链路层数据包进行隧道传输的技术，允许二层链路端点（LAC）和 PPP 会话点（LNS）驻留在通过分组交换网络连接的不同设备上，从而扩展了 PPP 模型，使得 PPP 会话可以跨越帧中继或 Internet 等网络。L2TP 结合了 L2F 和 PPTP 的各自优点，成为 IETF 有关二层隧道协议的工业标准。

配置项	说明
L2TP	启动/关闭
IPSec 隧道加密	启动/关闭
预共享秘钥	-
强制 NAT 穿越	启动/关闭
网络接口	可选接口

1.4.8.2 L2TP 状态



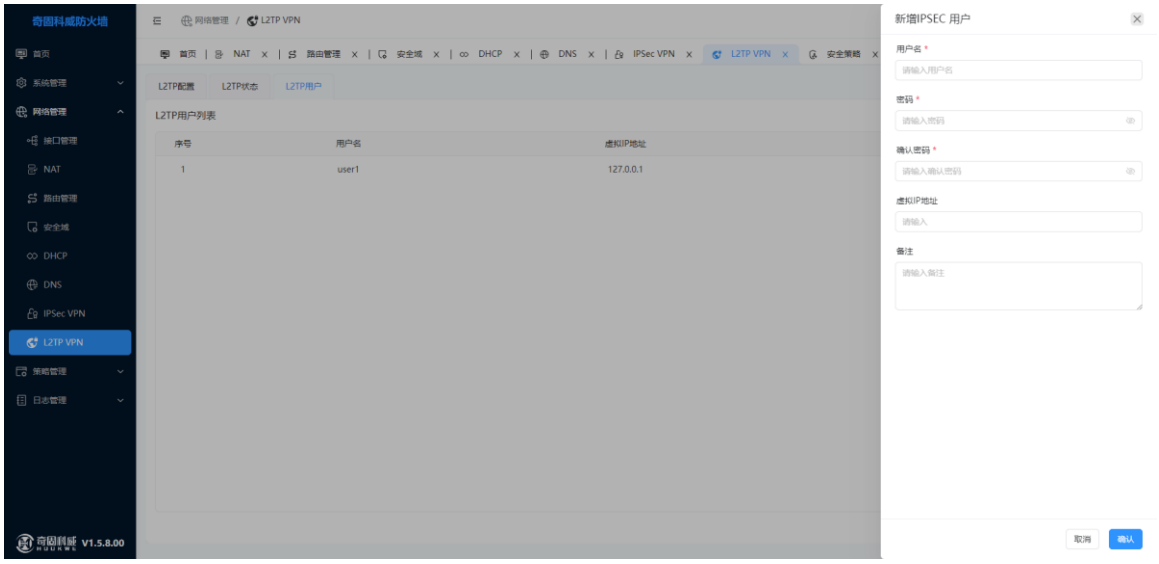
1.4.8.3 L2TP 用户



配置项	说明
用户名	–
密码	用户密码（数字大小写字母特殊符号如何而成，最少三种组合）
确认密码	确认密码
虚拟 IP 地址	IPv4 地址
备注	备注信息

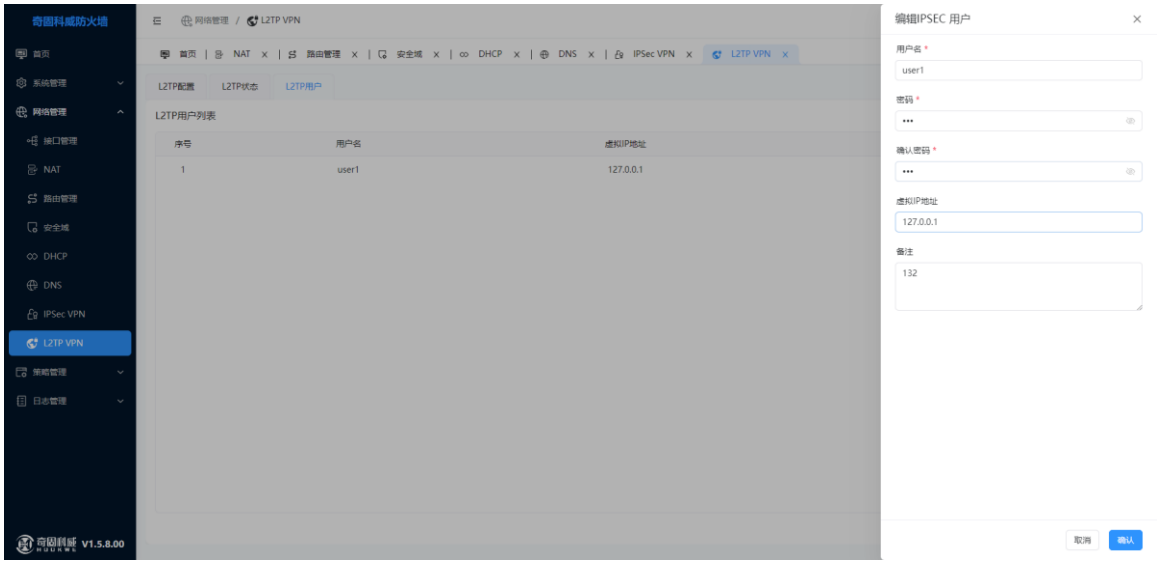
新增

点击新增按钮，设置需要新增的用户名、密码等。点击保存创建成功。如下图



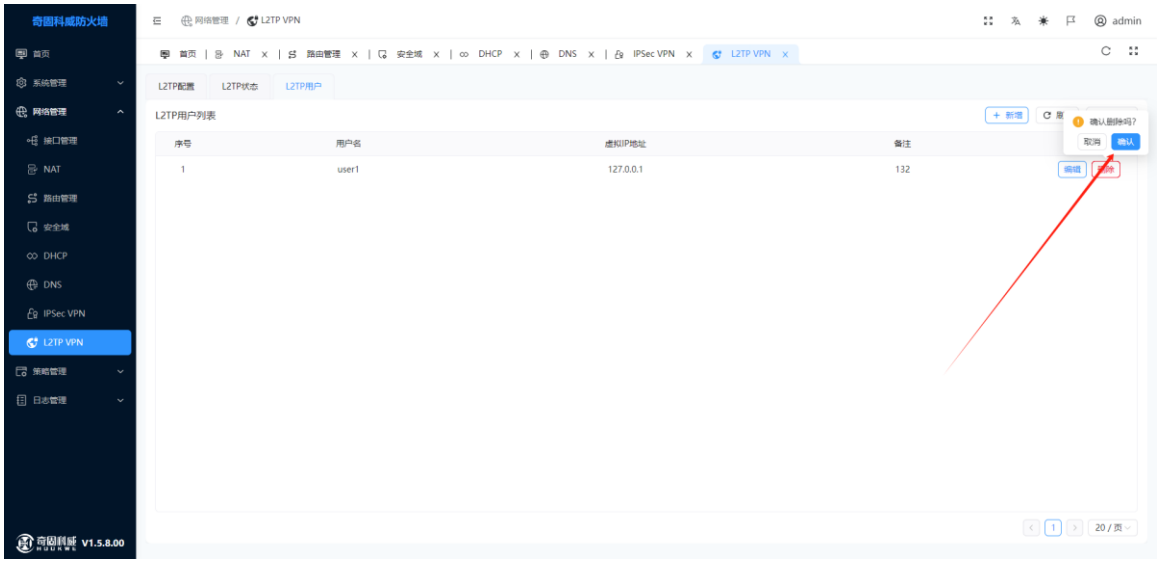
编辑

点击列表中的编辑按钮，可以当前项进行修改操作。如下图



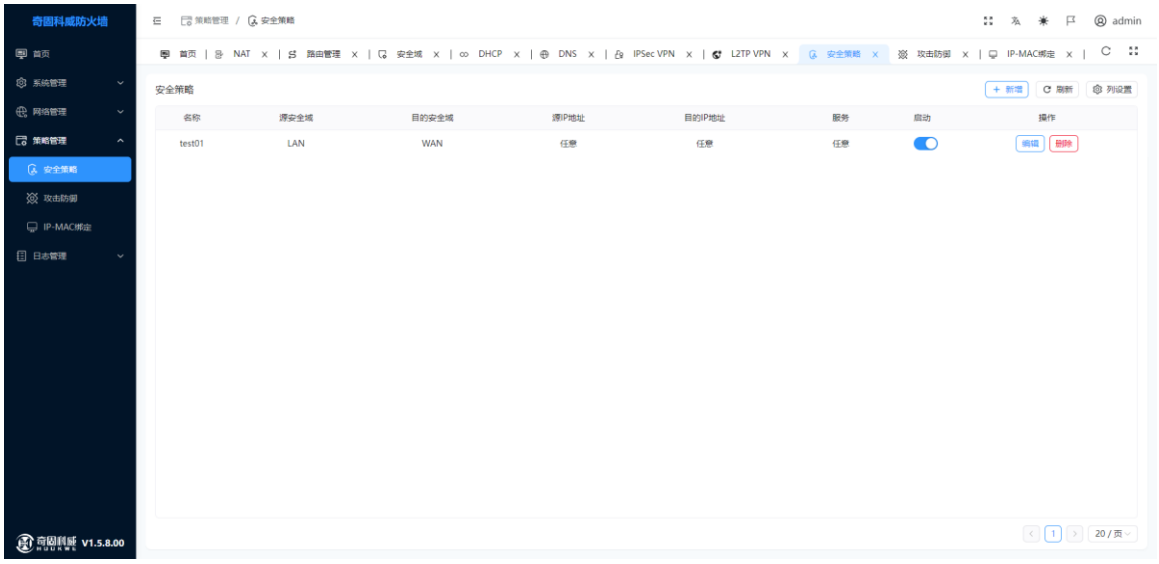
删除

点击列表中的删除进行删除。此操作不可逆，点击后确认后删除该条数据。如下图



1.5 策略管理

1.5.1 安全策略

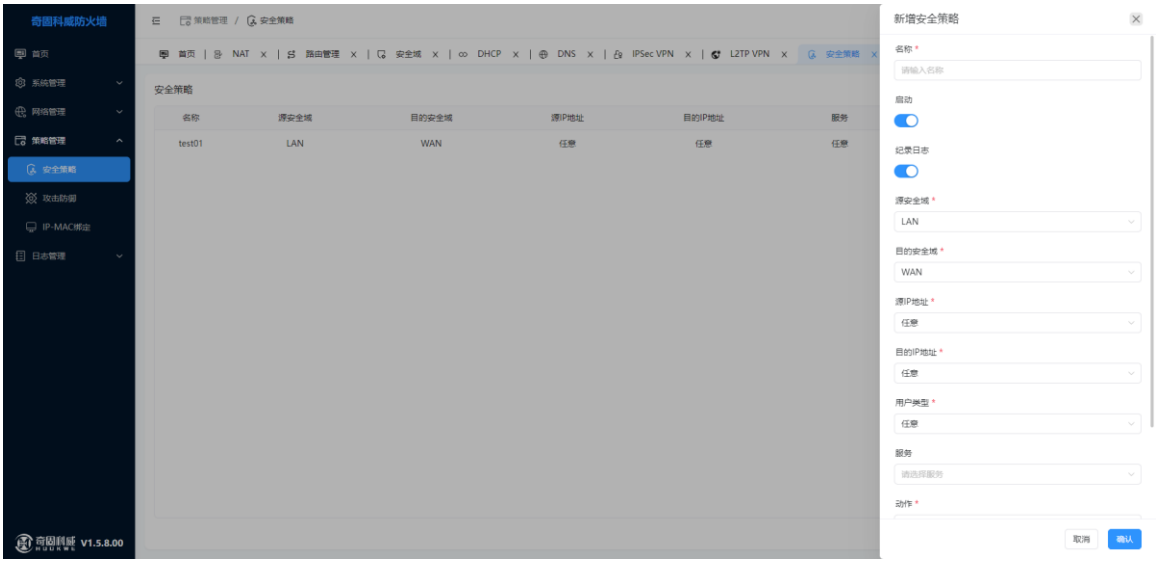


配置项	说明
名称	–
启动	开启/关闭
记录日志	触发策略是否会被记录到策略日志中
源安全域	默认 LAN

目的安全域	-默认 WAN
源 IP 地址	默认 任意， 可选任意 IPv4、IPv6 以及列表（IP 对象（指对象管理下 IP 地址）或 IP 地址）
目的 IP 地址	默认 任意， 可选任意 IPv4、IPv6 以及列表（IP 对象（指对象管理下 IP 地址）或 IP 地址）
用户类型	默认 任意， 任意用户以及列表指定用户
服务	-对应对象管理下服务
动作	允许或拒绝
描述	备注信息

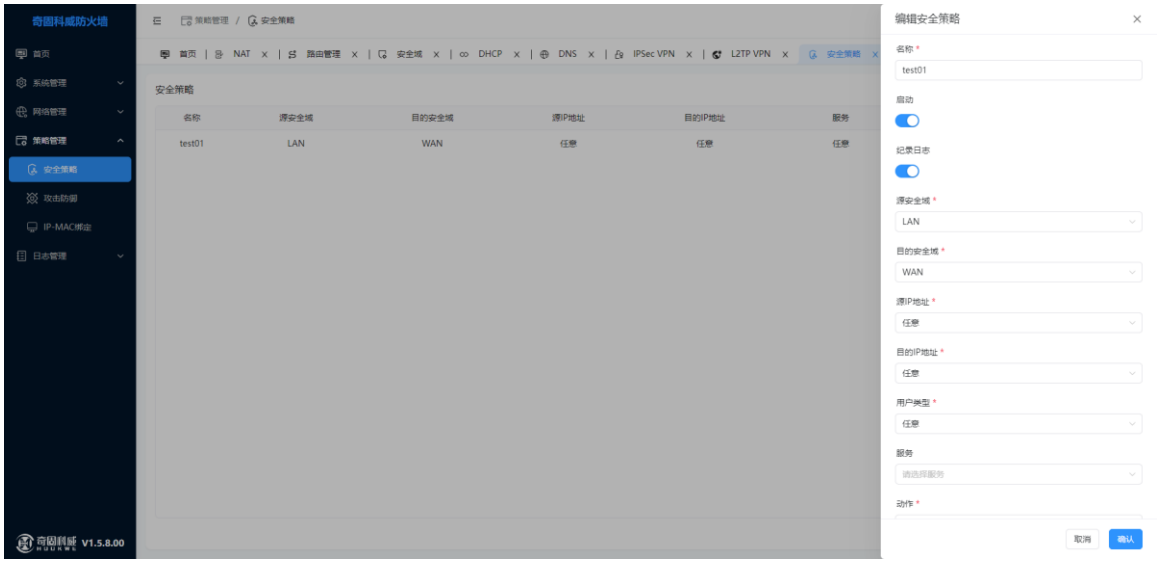
新增

点击新增按钮，设置需要新增的名称、安全域、目的安全域、源 IP 地址、目的 IP 地址、用户类型、动作等。点击保存创建成功。如下图



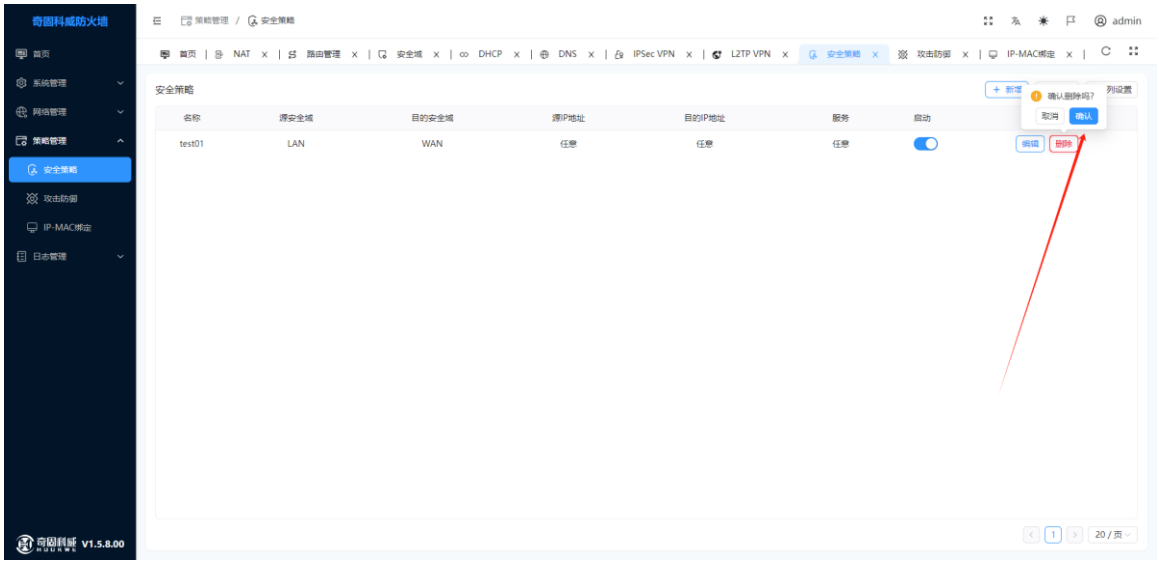
编辑

点击列表中的编辑按钮，可以当前项进行修改操作。如下图



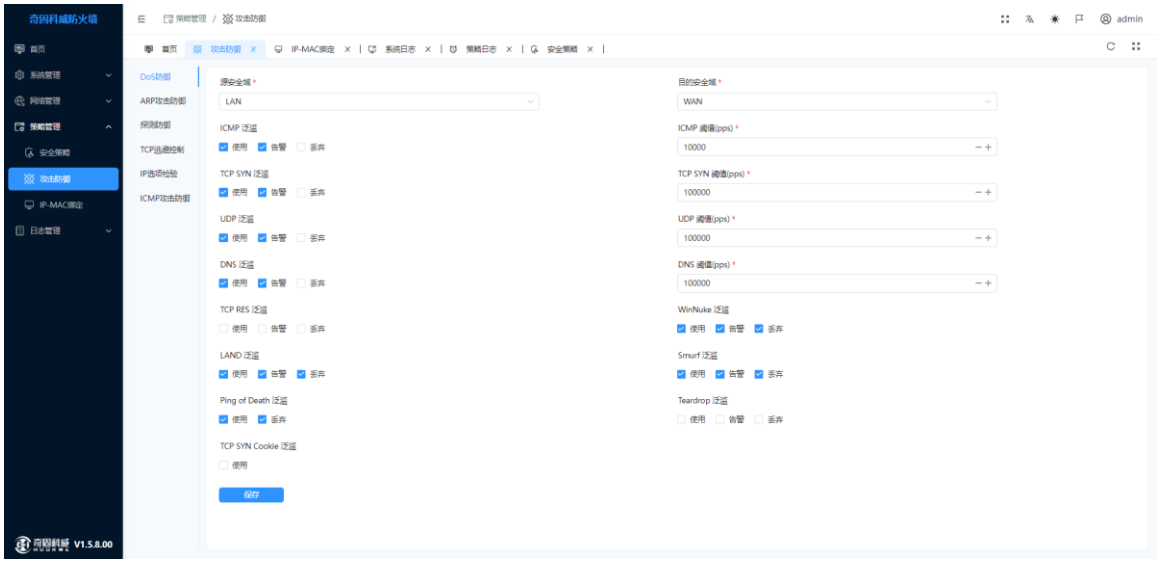
删除

点击列表中的删除进行删除。此操作不可逆，点击后确认后删除该条数据。如下图

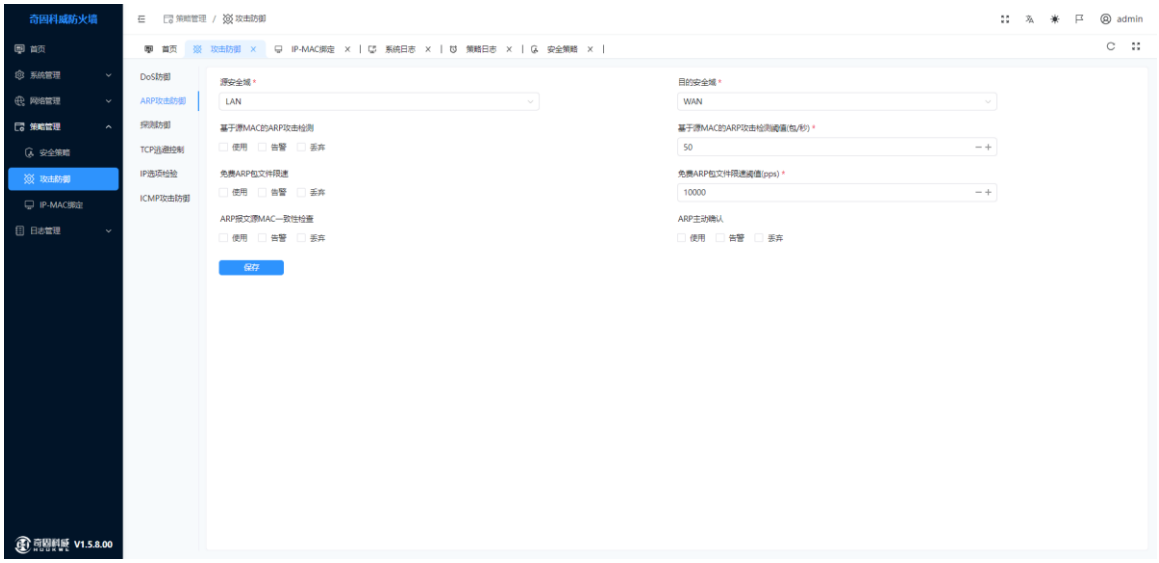


1.5.2 攻击防御

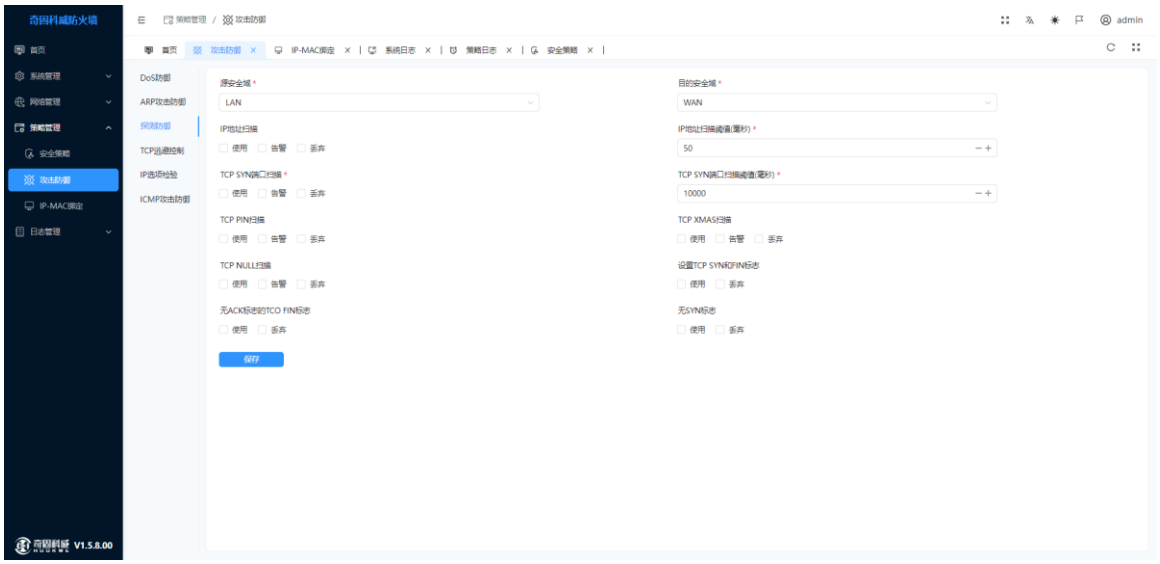
1.5.2.1 DOS 防御



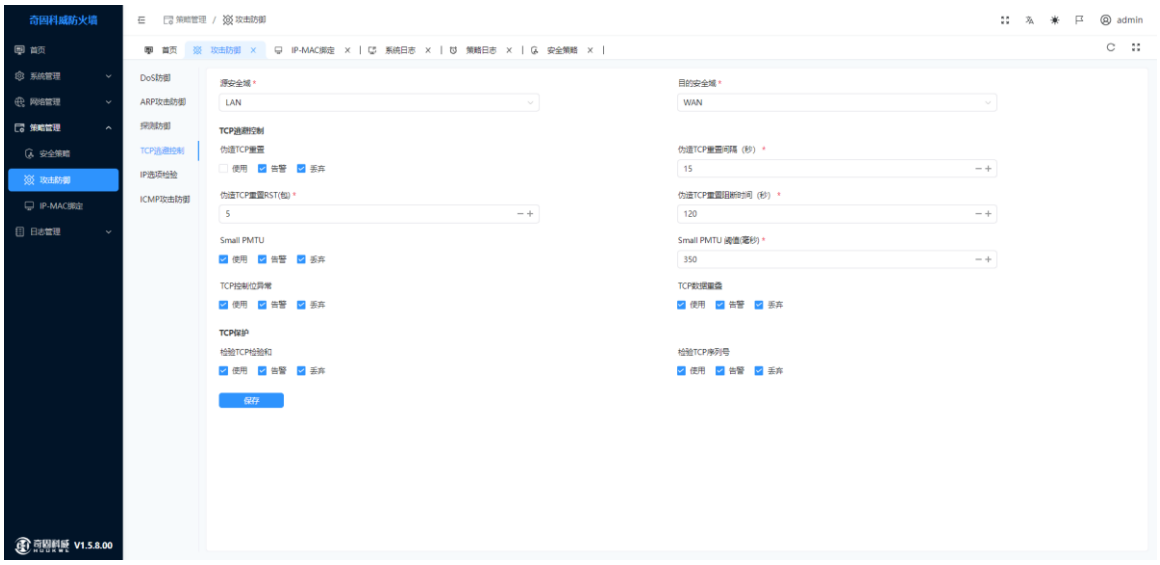
1.5.2.2 ARP 攻击防御



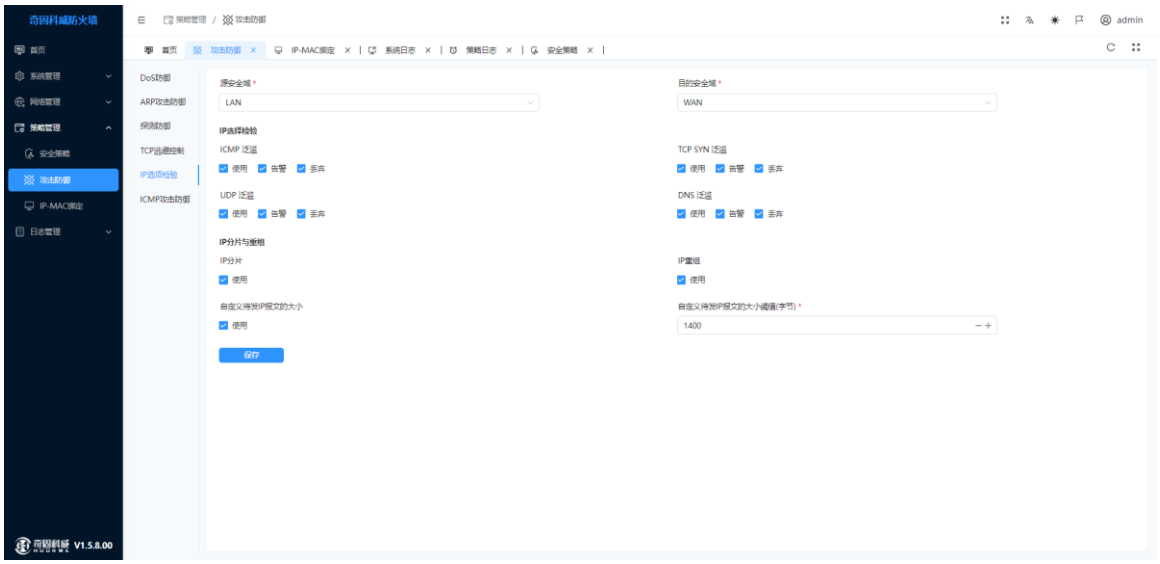
1.5.2.3 探测防御



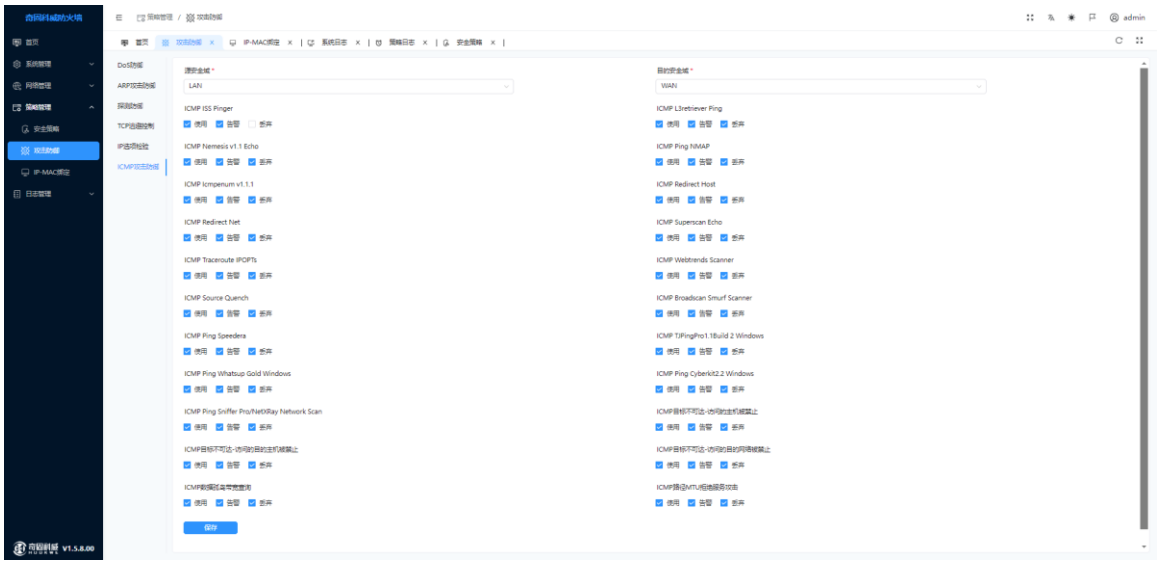
1.5.2.4 TCP 逃避控制



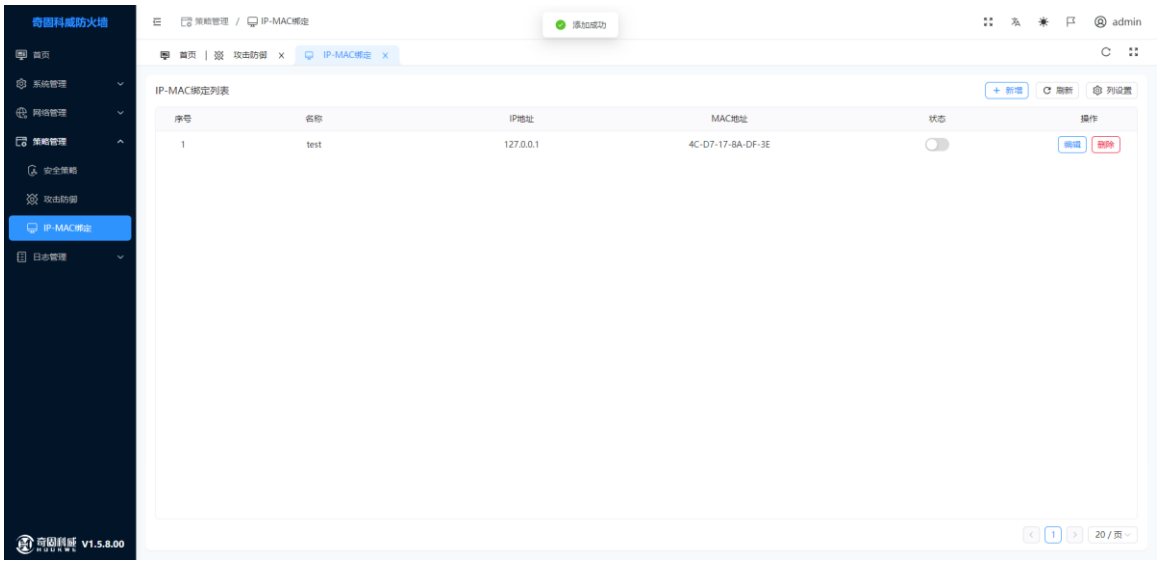
1.5.2.5 IP 选择检验



1.5.2.6 ICMP 攻击防御



1.5.3 IP-MAC 绑定

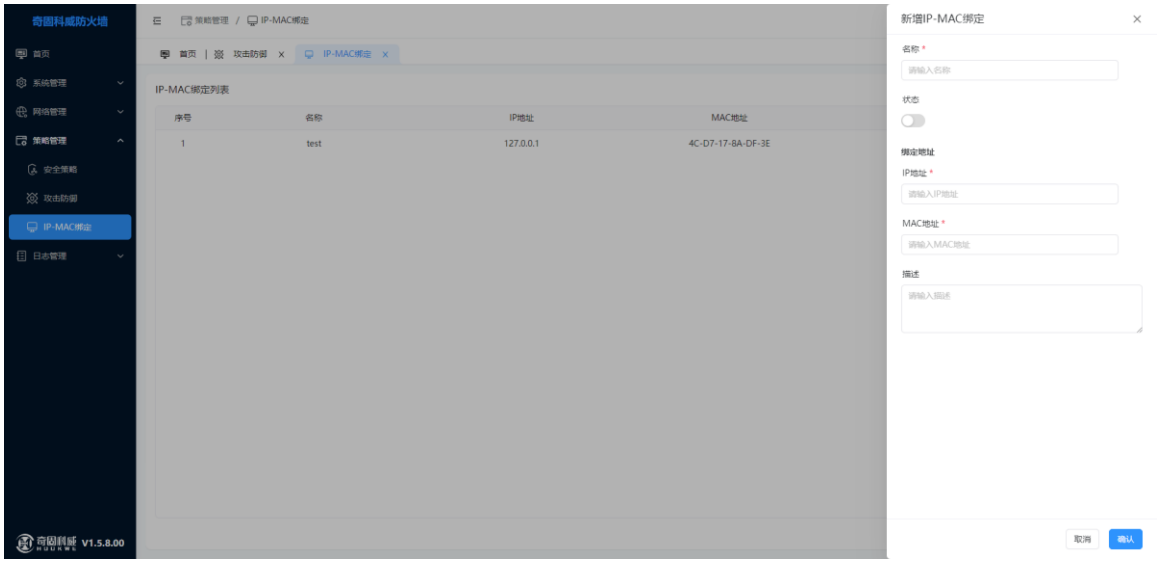


防火墙 的 IP-MAC 地址绑定特性将主机的 IP 地址及其网卡的 MAC 地址绑定到一起，可以 防止非法主机冒用合法主机的 IP 地址。

配置项	说明
名称	-
状态	启动/关闭
IP 地址	静态/动态
MAC 地址	-
描述	描述信息

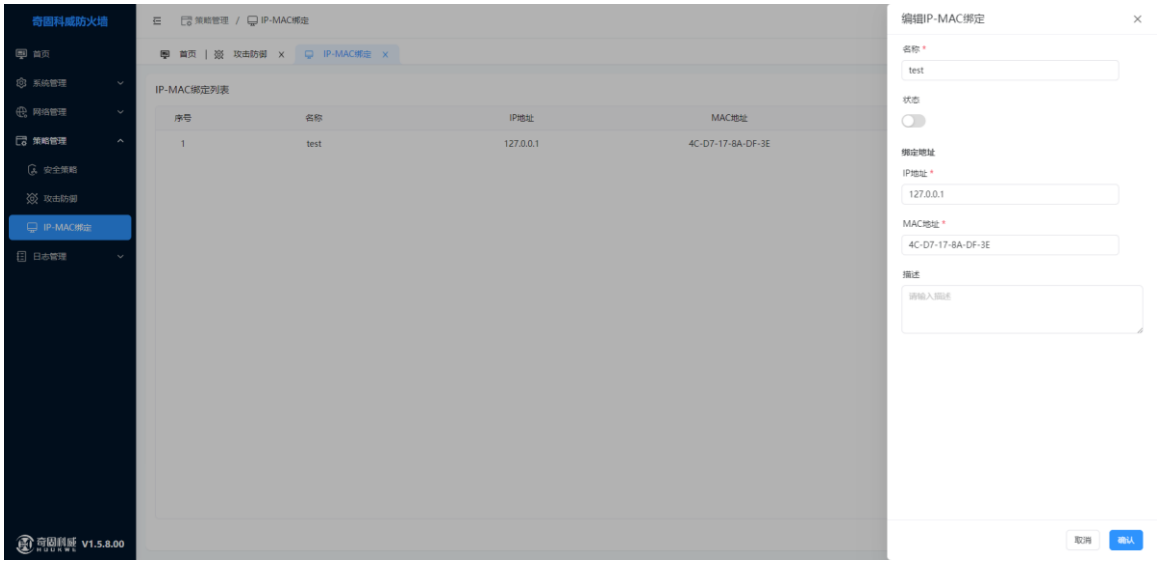
新增

点击新增按钮，设置需要新增的名称、IP 地址、MAC 地址等。点击保存创建成功。如下图



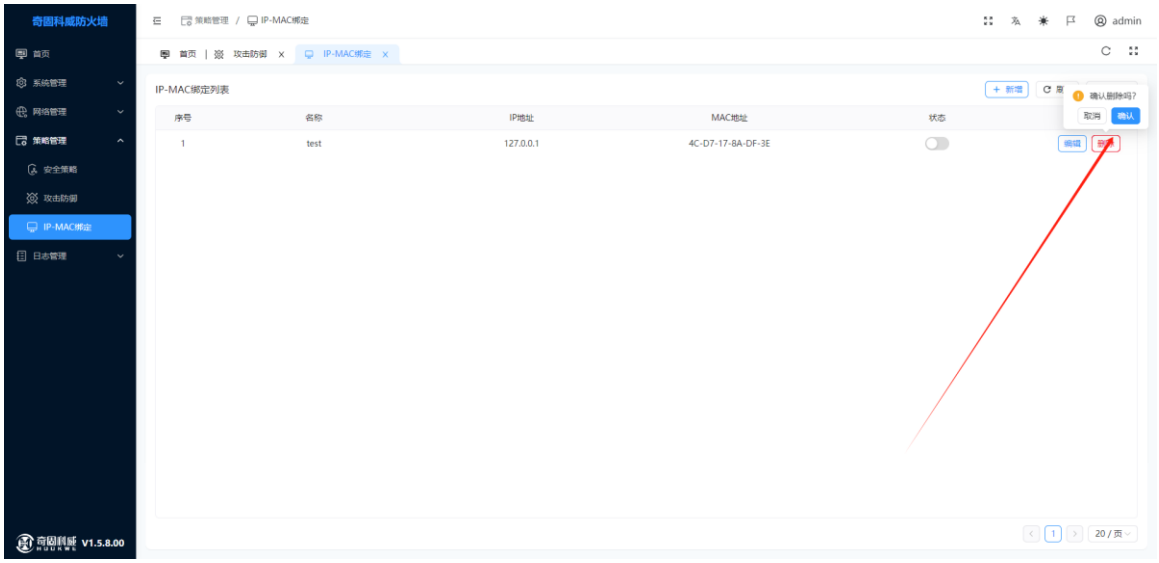
编辑

点击列表中的编辑按钮，可以当前项进行修改操作。如下图



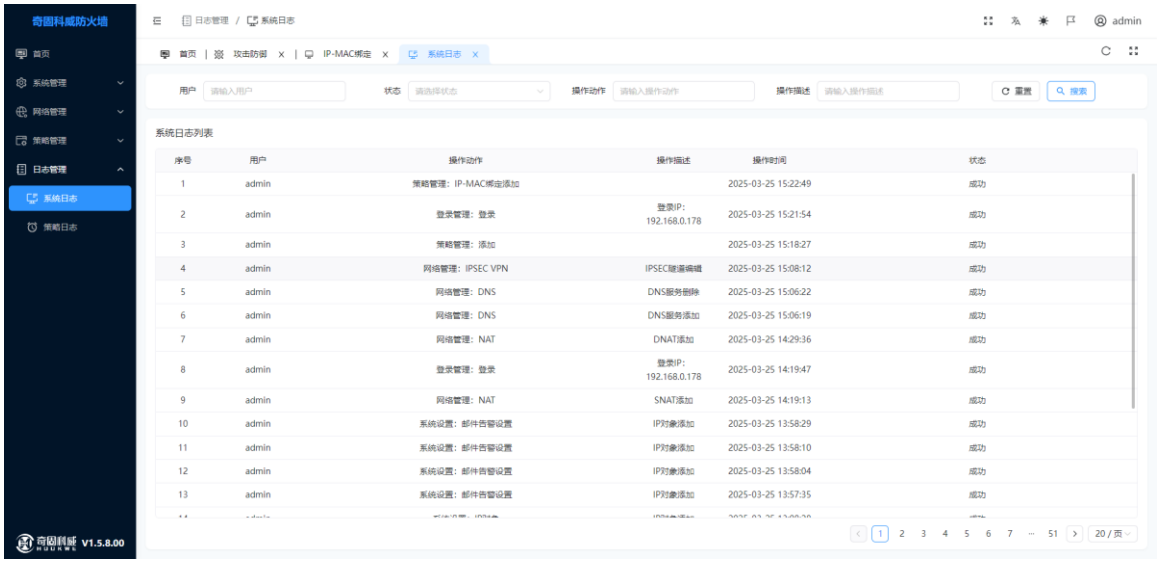
删除

点击列表中的删除进行删除。此操作不可逆，点击后确认后删除该条数据。如下图



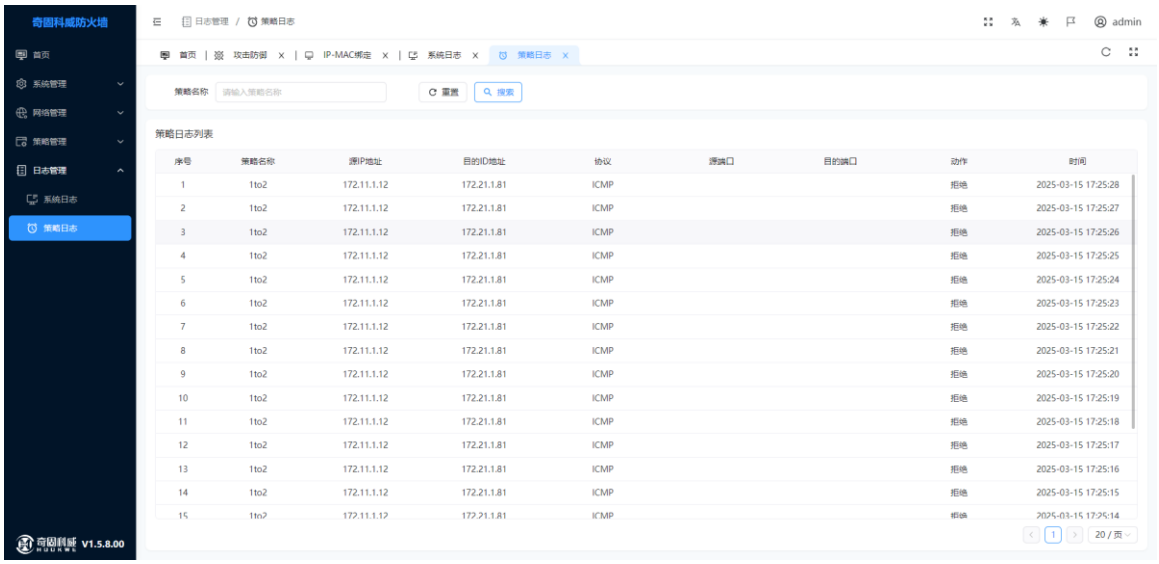
1.6 日志管理

1.6.1 系统日志



记录系统操作日志

1.6.2 策略日志



记录触发策略所生成的所有日志

修改记录

版本	时间
V1.5.8.00	2024/09/03