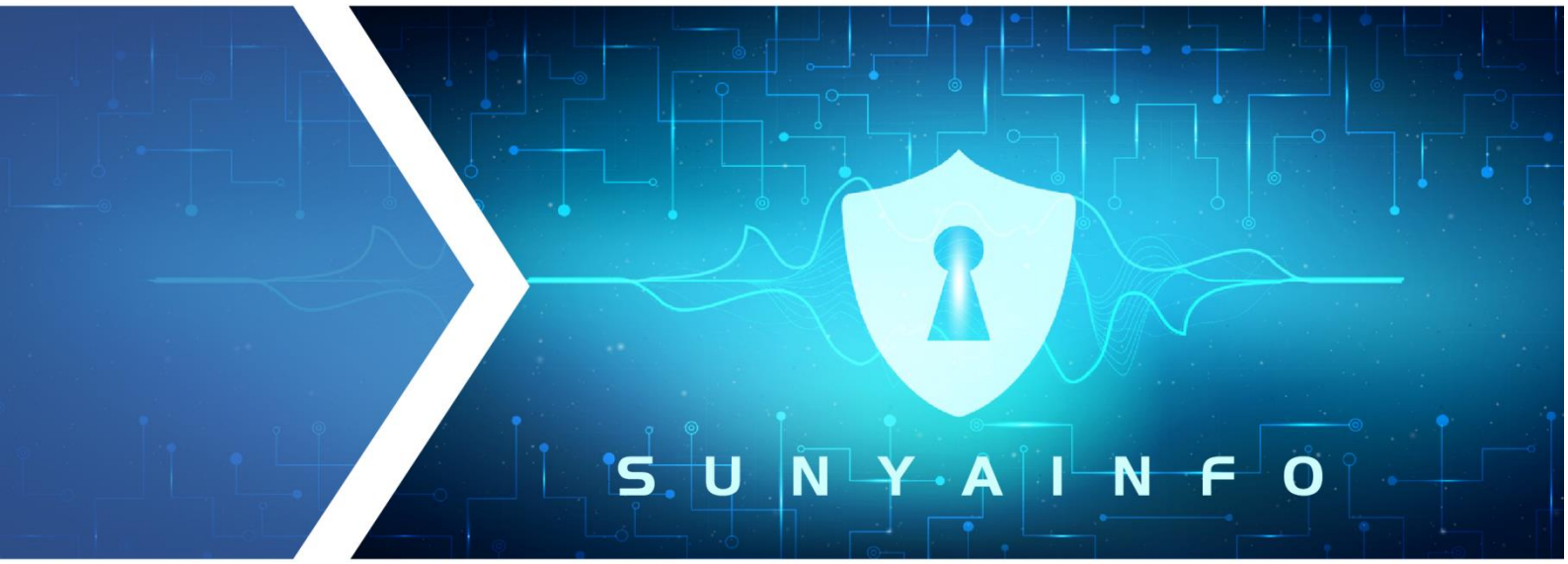


上元信安下一代防火墙(V4.0)

Web 用户手册

上元信安
领先的云计算安全专家

北京市海淀区上地三街金隅嘉华大厦E座2层
电话：400-067-0050
www.sunyainfo.com

版权声明

修订记录

日期	修订版本	修改记录	修改人
2021 年 10 月 20 日	ASG4.0_Release_V1	首次发布	孟方贞、刘惠、邓凯元

目录

前言

本用户手册对上元信安下一代防火墙（NGFW）的配置和使用做了详细的介绍。该手册仅供用户使用参考，并不确保涵盖所有使用场景。手册中的配置信息仅存在指导用户配置的意义，使用时一切以实际为准。

适用读者

本手册主要适用于期望了解上元信安下一代防火墙(NGFW)的主要功能及使用方法的读者，阅读本手册的读者尽量对以下知识领域有一定了解：

- TCP/IP 网络协议
- 常见数据库、服务器、防火墙设备基本操作配置
- DDOS、SQL 注入、暴力破解等网络安全知识

约定

格式约定

格式	说明
黑体字	对于 web 界面中的菜单以及页签的出现必须使用黑体字表示，例如：通过“**策略>防火墙策略>策略分析**”菜单打开页面。
< >	点击操作必须使用<>,例如：“点击<**新建**>按钮”
>	介绍操作步骤时用于隔离操作对象使用>，例如：通过“**策略>防火墙策略>策略分析**”菜单打开页面。

符号约定

符号	解释说明

注意	有此标记的文本表示有潜在的风险，若忽视这些文本可能会导致设备损坏、数据丢失、性能下降、功能失效等不可预知的结果。
提示	有此标记的文本表示正文的附加信息，是对正文的强调以及补充。

获得帮助

使用过程中如遇任何问题，请致电服务热线 400-067-0050。

官网：http://www.sunyainfo.com

地址：北京市海淀区上地三街金隅嘉华大厦 E 座 2 层

产品简介

当前，随着云计算、大数据、5G、人工智能等技术的发展，世界正在进入一个万物互联的时代。人们在享受新技术带来便利的同时，也正遭受信息泄漏、病毒木马、网络滥用、非法入侵、钓鱼邮件、网络勒索、APT 攻击等各种威胁。网络及 IT 设施的规模越来越庞大、架构越来越复杂，导致传统的防御体系失效，管理和维护的成本急剧上升。

上元信安下一代防火墙(NGFW)正是在此背景下产生，它提供应用层防火墙、入侵防护、防病毒、反 APT、DOS 防护、内容过滤、URL 过滤、VPN、智能带宽管理、上网行为管控与审计等多重安全特性；同时，它全面适配云环境，支持主流的公有云、私有云及虚拟化平台；全特性支持 RESTful API，具备高效的协同联动能力，包括沙箱联动、威胁情报联动、态势感知联动、EDR 联动、IDS 联动，等，提供立体化防护能力。

此外，上元信安下一代防火墙(NGFW)全面支持 SD-WAN 理念及架构，具备智能化云端管理的能力，设备支持零接触上线，可通过云端管理平台实现对业务配置统一编排、设备集中运维、状态实时监控及可视化，最大程度的简化了运维管理的工作，大大的节省了资金和人力投入。

由此可见，上元信安下一代防火墙(NGFW)不仅能防护传统网络边界，还适用于内网、数据

中心、公有云、私有云等场景，并能实现云、网、边、端的全面协同防护。

第一章 入门指南

用户可通过运行 Internet 浏览器的任何计算机使用 HTTP 或一个安全的 HTTPS 连接，便能够配置并管理下一代防火墙设备（NGFW）。在进行 Web 管理前，必须配置下一代防火墙设备使其能够接受来自指定接口的 HTTP 或 HTTPS 管理。

推荐使用 Mozilla22.0 及以上版本、chrome27.0 浏览器，最佳显示分辨率为 1920×1080。

1.1. 初始配置

出厂的设备有默认的配置。这些默认配置保证了用户不需要进行额外配置就能够通过 CLI 或 Web 对下一代防火墙设备进行管理、配置。CLI 包括 Console、SSH。Web 包括 HTTP、HTTPS。管理接口（MGT）的默认地址配置为 192.168.1.200/24。

1.1.1. 默认管理员

系统默认的管理员用户为 admin，密码为 admin。用户可以使用这个管理员账号从任何地址登录设备，并且使用设备的所有功能。

系统默认的审计员用户为 audit，密码为 admin.audit。用户可以使用这个账号对日志系统进行审计。

系统默认的用户管理员用户为 useradmin，密码为 admin.user。用户可以使用这个账号配置系统管理员。

1.1.2. CLI 管理

请参考以下步骤搭建上元信安下一代防火墙（NGFW）的 Console 口配置环境：

1. 用标准 RS-232 电缆将 PC 的串口与防火墙的 Console 口连接起来。

2. 在 PC 上运行终端仿真程序（如系统的超级终端、SecureCRT 等），并按如下表所示设置参数：

参数	数值
波特率	9600 bit/s
数据位	8
奇偶校验	无
停止位	1
数据流控制	无
参数	数值

3. 打开电源开关，设备会进行自检并且自动进行初始化配置。如果系统启动成功，会出现登录提示入账户名和密码并敲击回车即可进入 CLI 配置界面。

1.1.1. Web 管理

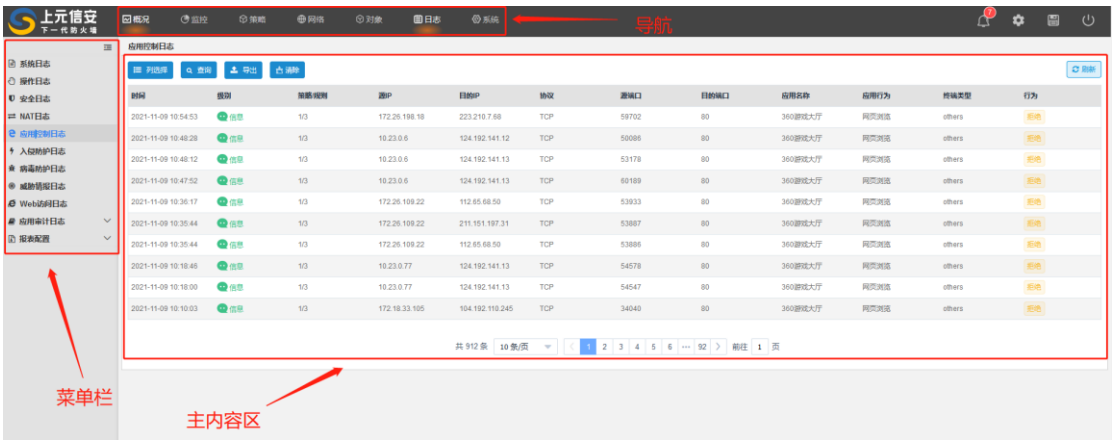
用户可通过 MGT 接口登录到设备的 WebUI 进行初始配置。参考以下步骤：

1. 将 PC 的 IP 地址设置为与 192.168.1.1/24 同网段的 IP 地址，并用网线将 PC 设备和 MGT 接口连接起来。

2. PC 使用浏览器输入 https://192.168.1.200 并敲击回车，会显示设备的登录页面；输入账户名和密码即可进入 Web 管理界面。

1.2. 系统菜单

Web 系统菜单由**导航条**、**菜单栏**、和**主内容区**页面组成，每个导航标签里有相应的一个或多个子项目。当点击一个导航页，如监控。左侧显示菜单项目，右侧为主内容区。



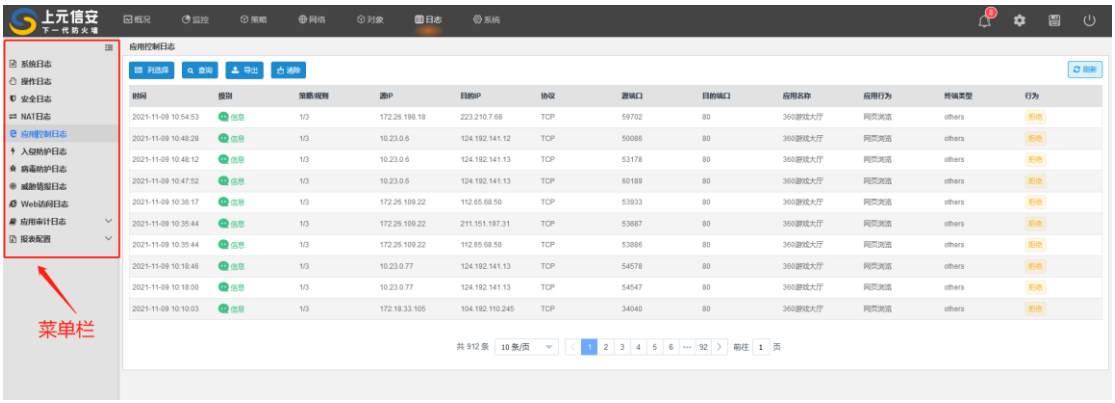
1.2.1. 导航

导航提供了下一代防火墙设备的信息统计和主要配置选项。

导航标签	说明
概况	系统相关的一些关键信息展示。包括状态、接口、流量、在线用户等概要信息显示，方便直接查看。
监控	一些数据统计结果的显示，包括用户流量、设备健康信息等。
策略	策略相关配置。包括用户策略、应用策略、防护策略、协议、流量策略等。
网络	网络相关配置。接口、路由、DNS、IPSEC 等。
对象	对象相关配置。包括用户、关键字，应用、服务、地址、时间，设备健康检查、CA 证书等。
日志	类别日志查询。包括系统、安全、NAT、应用控制、入侵防御、病毒防护日志。
系统	系统功能配置。包括管理员配置、可用性、系统维护等。

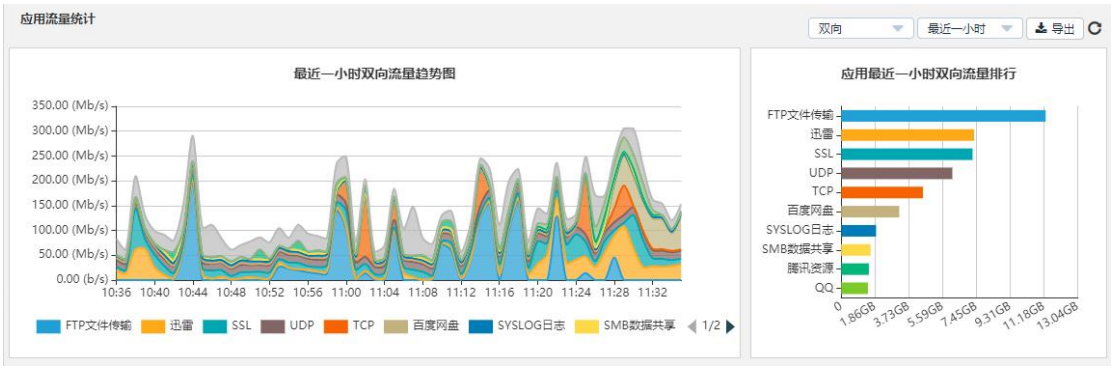
1.2.2. 菜单栏

除“**概况**”之外，其他导航页面左侧都有可折叠的浮动“**菜单栏**”。菜单栏中可以选择不同的配置项目进行细节配置或查看。



1.2.3. 主内容区

主内容区是显示配置和信息的界面，在不同导航项目中有不同的表现形式。在“监控”导航标签下，监控信息主要以图表的形式直观的展现出来，不同项目信息以不同颜色加以显示，方便查看。



应用名称	上行流量	下行流量	总流量	操作
FTP文件传输	2.39GB	8.88GB	11.27GB	
迅雷	229.51MB	7.10GB	7.32GB	
SSL	656.61MB	6.60GB	7.24GB	
UDP	6.10GB	27.49MB	6.13GB	
TCP	3.74GB	780.33MB	4.50GB	
百度网盘	3.07GB	130.37MB	3.20GB	
SYSLOG日志	1.81GB	115.76MB	1.92GB	
SMB数据共享	720.83MB	938.28MB	1.62GB	
腾讯资源	140.89MB	1.39GB	1.52GB	
QQ	1.28GB	201.44MB	1.47GB	

在“**日志**”，“**策略**”，“**网络**”等导航标签下，信息主要以表格的形式展现，更加贴近用户的使用习惯。

时间	级别	策略/规则	源IP	目的IP	协议	源端口	目的端口	应用名称	应用行为	终端类型	行为
2021-10-19 11:39:06	信息	1/1	211.101.36.78	10.244.0.1	UDP	23161	514	SYSLOG日志	网络协议	PC	允许
2021-10-19 11:39:06	信息	1/1	172.18.12.10	10.244.0.1	UDP	45471	514	SYSLOG日志	网络协议	PC	允许
2021-10-19 11:39:06	信息	1/1	10.23.0.6	172.17.0.194	TCP	62983	443	SSL	网络协议	Android	允许
2021-10-19 11:39:06	信息	1/1	10.23.0.92	103.235.46.211	TCP	56611	80	百度通行证	登录	IOS	允许
2021-10-19 11:39:06	信息	1/1	211.101.36.78	8.8.8.8	UDP	31595	53	DNS	网络协议	PC	允许
2021-10-19 11:39:06	信息	1/1	192.168.130.90	8.8.8.8	UDP	51724	53	DNS	网络协议	PC	允许
2021-10-19 11:39:06	信息	1/1	172.17.112.66	114.114.114.114	UDP	40172	53	DNS	网络协议	PC	允许
2021-10-19 11:39:06	信息	1/1	211.101.36.78	8.8.8.8	UDP	40356	53	DNS	网络协议	PC	允许
2021-10-19 11:39:06	信息	1/1	172.17.112.66	8.8.8.8	UDP	40172	53	DNS	网络协议	PC	允许
2021-10-19 11:39:06	信息	1/1	211.101.36.78	8.8.8.8	UDP	47265	53	DNS	网络协议	PC	允许

共 2618 条 10 条/页 1 2 3 4 5 6 ··· 262 前往 2 页

第二章 概况

概况作为 Web 首页，展示了设备当前的基本信息，包括系统基本信息、实时流量信息、系统信息、授权状态、在线管理员、应用统计等。用户可以通过概况页面迅速了解当前设备的基本信息以及运行情况。

2.1. 主页面板

主页面板默认显示以下窗口模块：系统基本信息、实时流量信息、系统信息、授权信息、在线管理员、应用流量信息、系统日志信息。在页面右上角点击图标自定义主页面板的页面布局。

2.1.1. 系统基本信息

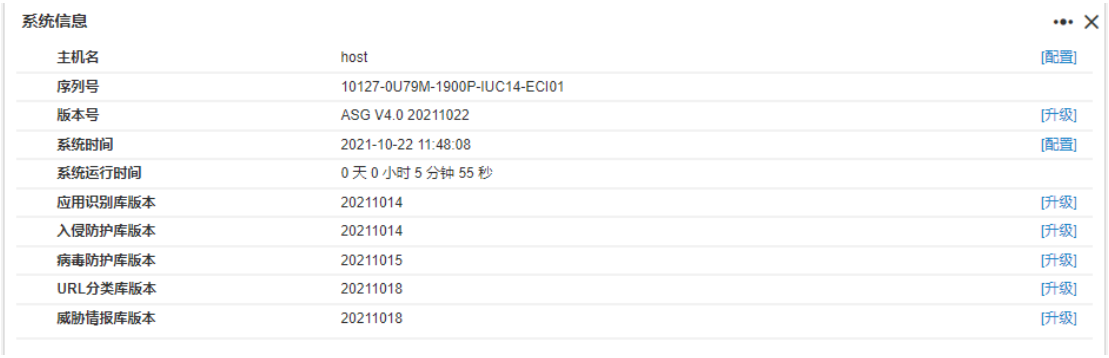
在导航栏点击“**概况**”，进入概况页面。查看设备**基本信息**展示。

设备基本信息的相关信息及详细说明如下：

相关信息	说明
在线用户	当前在线用户统计，具体用户请参考在线用户统计。
连接数	当前连接数统计，具体连接请参考会话监控。
今日事件	统计今日的安全事件，具体请参考“**日志>安全日志**”。
CPU	显示加载页面时当前 CPU 占用率。
内存	显示加载页面时当前内存占用率。
硬盘/CF 卡	显示加载页面时当前硬盘/CF 卡使用率，当设备有硬盘时，显示硬盘使用率，当设备无硬盘时，显示 CF 卡使用率。

2.1.2. 系统信息

在导航栏点击“**概况**”，进入概况页面。查看**系统信息**展示。



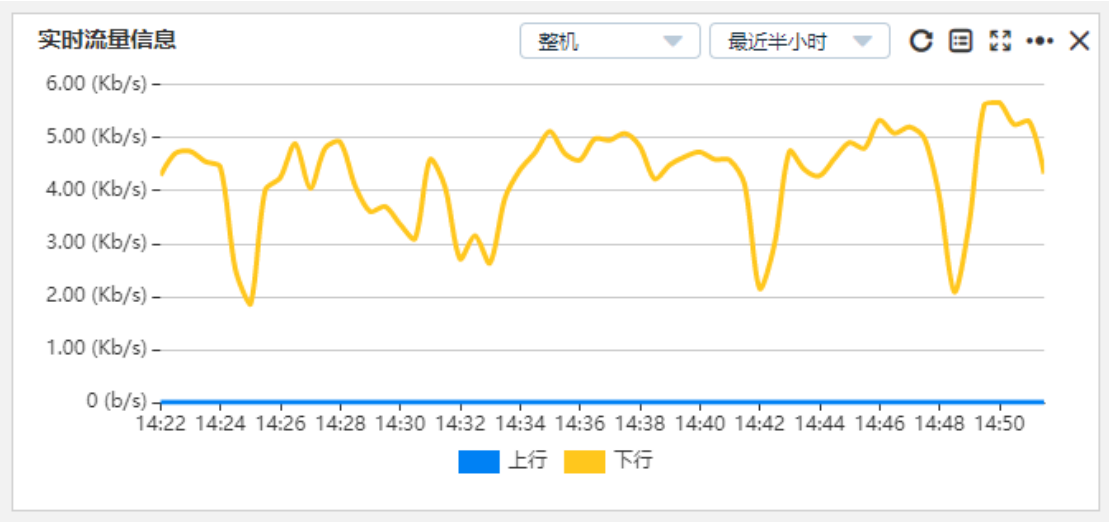
系统信息的相关信息及详细说明如下：

相关信息	说明
主机名	用户可通过主机名称区分设备。
序列号	设备的唯一序列号，出厂时设定，无法修改。
版本号	当前设备运行系统软件的版本号。
系统时间	该设备的系统日期和时间。
系统运行时间	系统从上次启动后不间断运行的时长。
应用识别库版本	当前应用特征库版本号。
入侵防护库版本	当前入侵防护特征库版本号。
病毒防护库版本	当前病毒防护特征库版本号。
URL 分类库版本	当前 URL 分类特征库版本号。
威胁情报库版本	当前威胁情报特征库版本号。

特征库会定期发布更新，可以对各类防护特征库进行升级，升级方式请参考升级与重启。

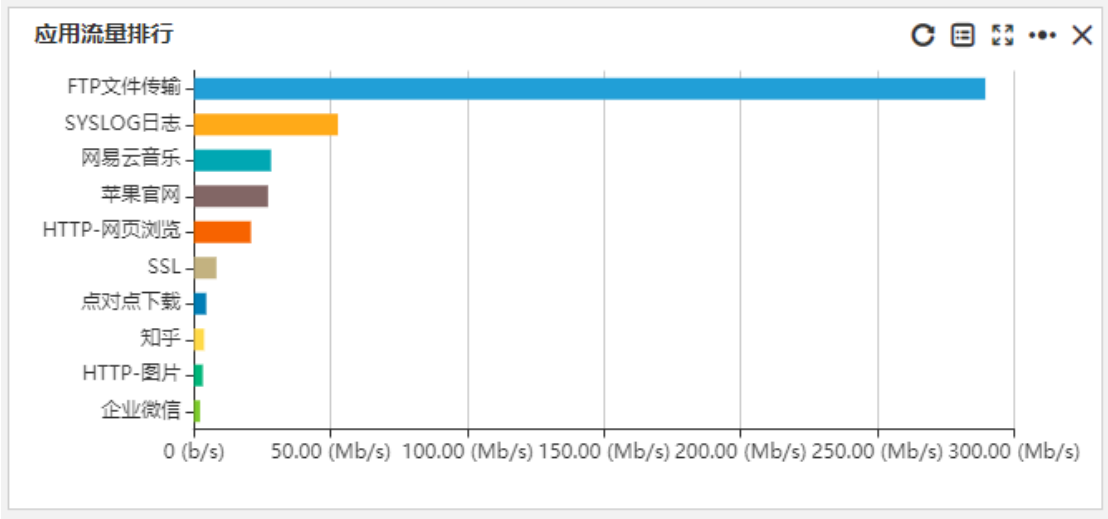
2.1.3. 实时流量信息

在导航栏点击“**概况**”，进入概况页面。查看设备**实时流量信息**展示。默认显示整机最近半小时的上行、下行流量；支持显示整机或单个接口流量；支持显示最近半小时、一小时、三小时、一天、一周、一月流量显示；用户点击图标刷新；用户点击图标切换图表和列表显示方式；用户点击图标扩大图表。



2.1.4. 应用流量信息

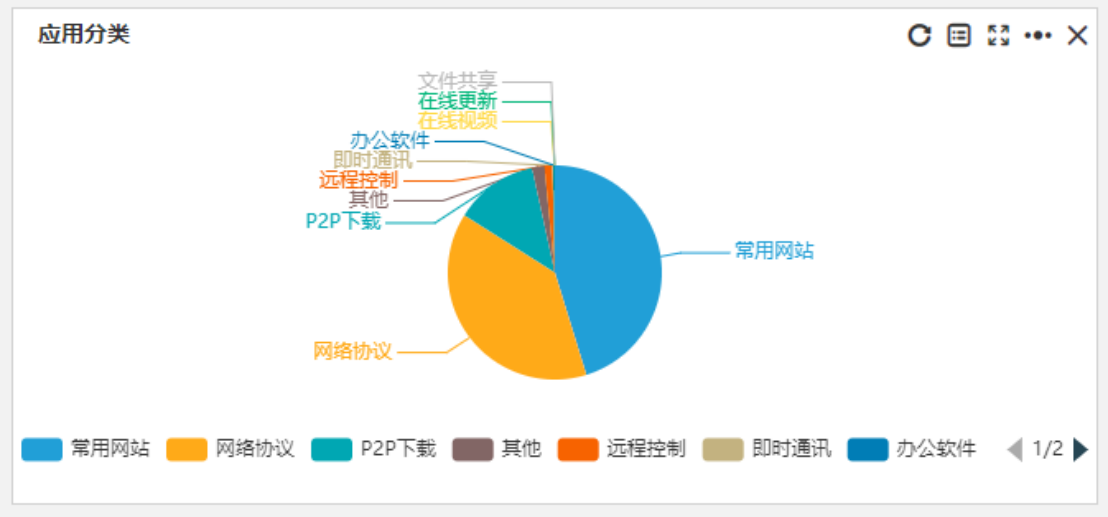
在导航栏点击“**概况**”，进入概况页面。查看**应用流量信息**展示，显示当前系统应用流量排行。用户点击图标刷新；用户点击图标可切换列表和图表显示方式；用户点击图标扩大图表。



有关应用的更多信息，请参考应用。

2.1.5. 应用分类信息

在导航栏点击“**概况**”，进入概况页面。查看**应用分类信息**展示，显示系统处理的流量按应用类别所产生的排名，用户可在右上角点击图标切换图表和列表显示方式，用户点击图表扩大图表。



2.1.6. 授权信息

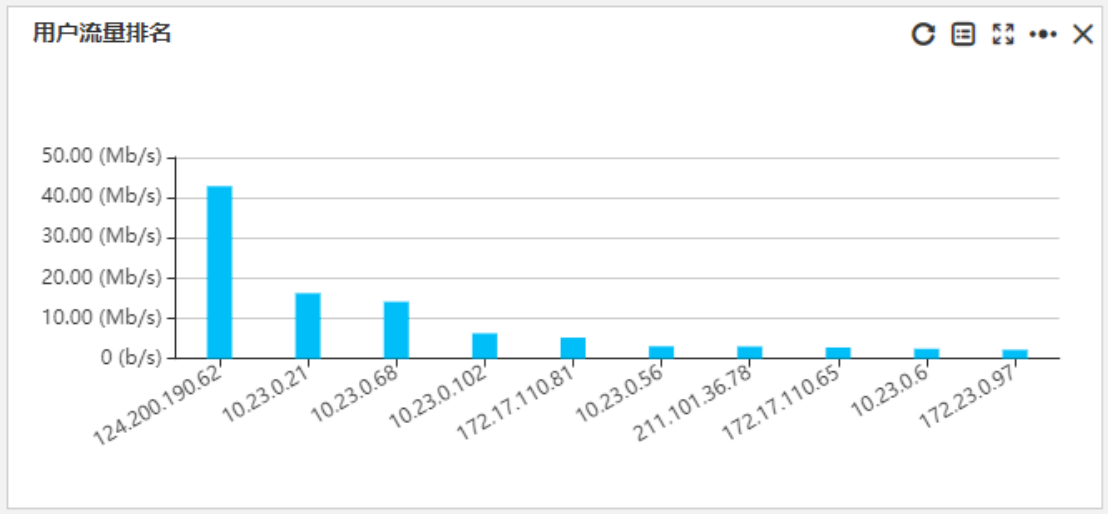
在导航栏点击“**概况**”，进入概况页面。查看**授权信息**展示。用户点击图标前往授权页

面授权/激活。

如需升级授权信息，请参考授权。

2.1.7. 用户流量排名

在导航栏点击“**概况**”，进入概况页面。查看**用户流量排名**展示，显示所有通过设备访问网络的用户所产生的上下行流量排名。用户点击图标刷新；用户可在右上角点击图标切换图表和列表显示方式；用户点击图标扩大图表。



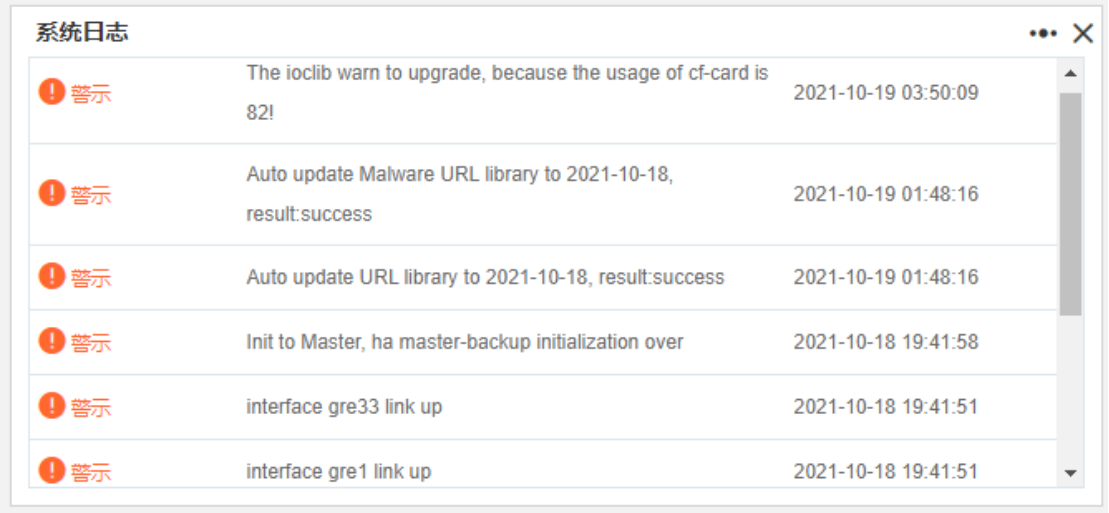
有关用户和用户组的更多信息，请参考用户对象。

2.1.8. 在线管理员

在导航栏点击“**概况**”，进入概况页面。查看**在线管理员**展示，显示在线管理员的用户名、管理地址、访问方式和登录时间。

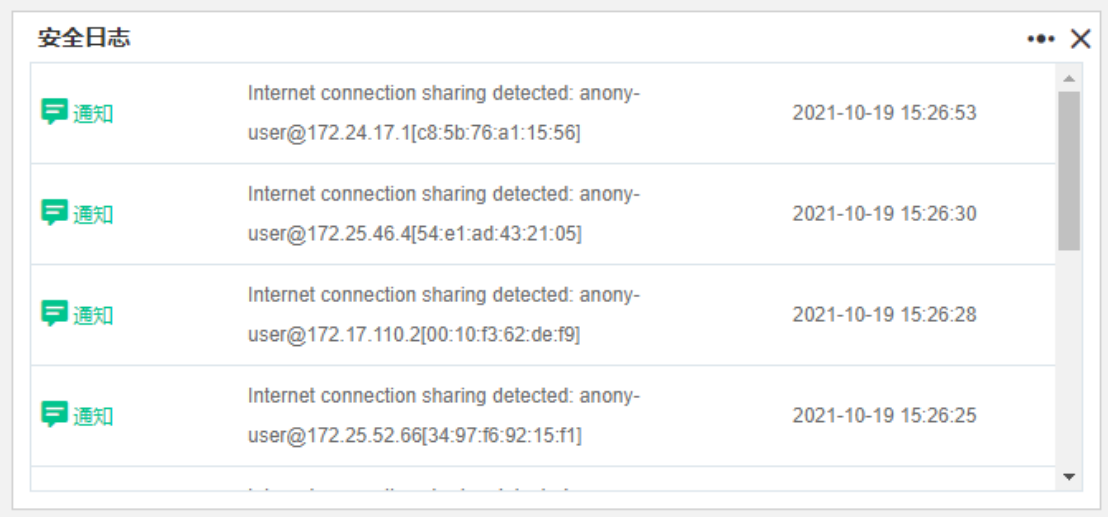
2.1.9. 系统日志信息

在导航栏点击“**概况**”进入概况页面。查看**系统日志信息**展示，显示最近 10 条系统日志信息（只显示警示及以上级别日志）。



2.1.10. 安全日志信息

在导航栏点击“**概况**”，进入概况页面。查看**安全日志信息**展示，显示安全日志的最近 10 条日志信息（显示信息及信息以上级别的日志）。



有关安全日志配置的更多信息，请参考“**日志>安全日志**”。

第三章 监控

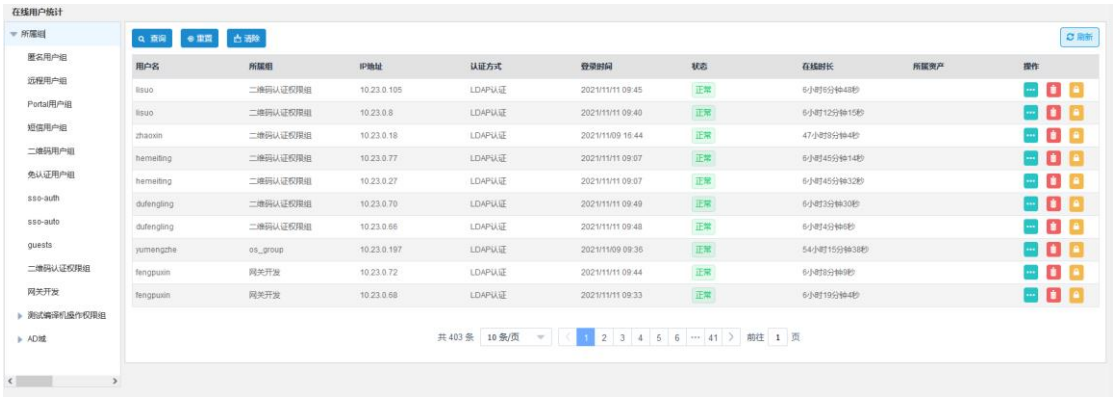
监控分为系统监控、流量分析和安全分析。收集三个维度的曲线图信息，通过这些信息可以判断其工作状况是否正常，给排查问题、进行大数据分析提供必要的信息。

3.1. 系统监控

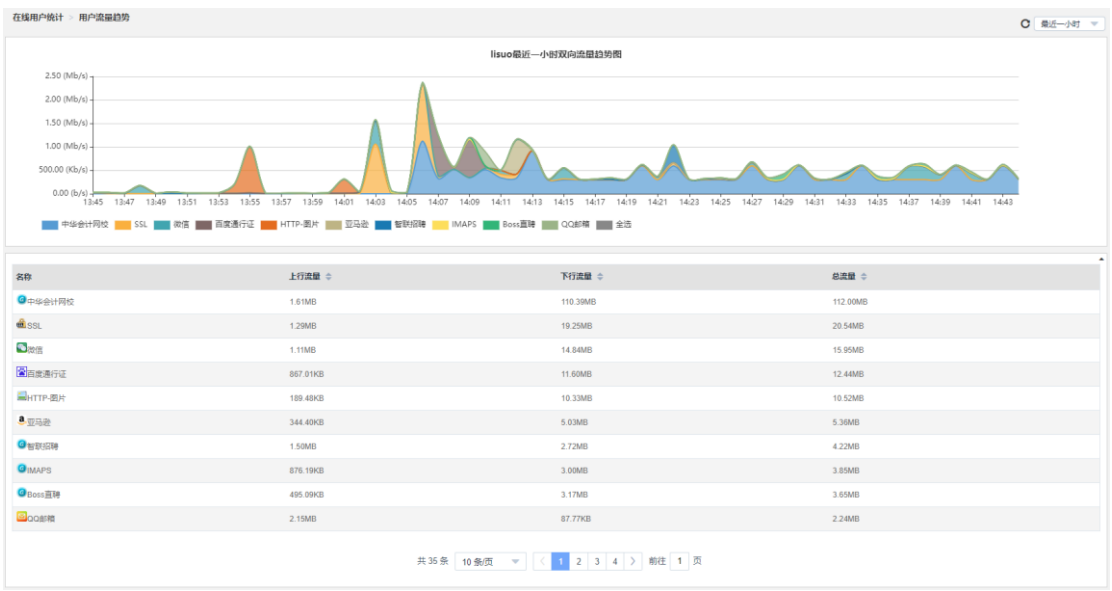
通过系统监控功能，可监控设备当前在线用户、接口信息、设备健康、健康检查等信息。

3.1.1. 在线用户统计

在系统菜单点击“**监控>系统监控>在线用户统计**”，进入**在线用户统计**页面，查看设备上所有用户。



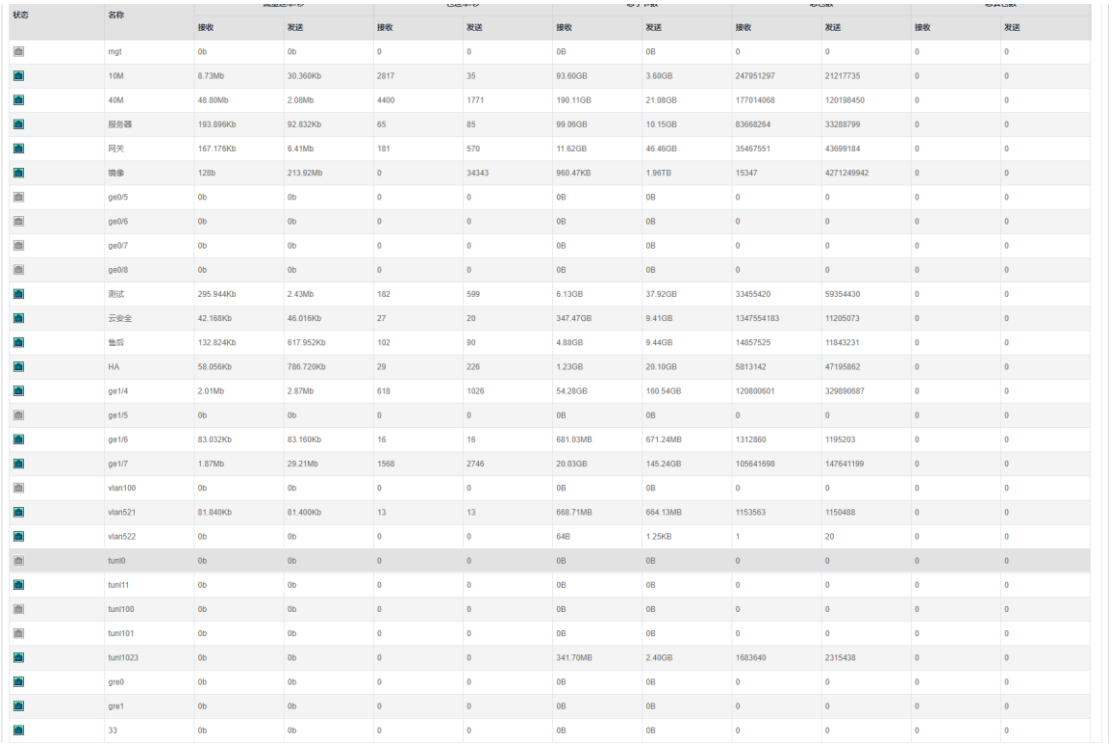
在**在线用户统计**页面右侧“**操作**”栏点击 查看该用户的流量统计。



在**在线用户统计**页签右侧“**操作**”栏点击可以冻结该用户，被冻结后的用户在冻结时间内无法通过防火墙上网。

3.1.2. 接口信息统计

在系统菜单点击“**监控>系统监控>接口信息统计**”，进入**接口信息统计**页面，查看设备所有接口的信息统计内容。



状态	名称										
		接收	发送	接收	发送	接收	发送	接收	发送	接收	发送
	mgt	0b	0b	0	0	0B	0B	0	0	0	0
	10M	8.73Mb	30.360Kb	2817	35	93.60GB	3.60GB	247951297	21217735	0	0
	40M	48.80Mb	2.08Mb	4400	1771	190.11GB	21.08GB	177014068	120198450	0	0
	服务器	193.896Kb	92.832Kb	65	85	99.06GB	10.15GB	83668264	33288799	0	0
	网关	167.176Kb	6.41Mb	181	570	11.62GB	46.46GB	35467551	43699184	0	0
	镜像	128b	213.92Mb	0	34343	960.47KB	1.96TB	15347	4271249942	0	0
	ge0/5	0b	0b	0	0	0B	0B	0	0	0	0
	ge0/6	0b	0b	0	0	0B	0B	0	0	0	0
	ge0/7	0b	0b	0	0	0B	0B	0	0	0	0
	ge0/8	0b	0b	0	0	0B	0B	0	0	0	0
	测试	295.944Kb	2.43Mb	182	599	6.13GB	37.92GB	33455420	59354430	0	0
	云安全	42.168Kb	46.016Kb	27	20	347.47GB	9.41GB	1347554183	11205073	0	0
	集团	132.824Kb	617.952Kb	102	90	4.88GB	9.44GB	14857525	11843231	0	0
	HA	58.056Kb	786.720Kb	29	226	1.23GB	20.10GB	5813142	47195862	0	0
	ge1/4	2.01Mb	2.87Mb	618	1026	54.28GB	160.54GB	120800601	329890687	0	0
	ge1/5	0b	0b	0	0	0B	0B	0	0	0	0
	ge1/6	83.032Kb	83.160Kb	16	16	681.03MB	671.24MB	1312860	1195203	0	0
	ge1/7	1.87Mb	29.21Mb	1568	2746	20.83GB	145.24GB	105641698	147641199	0	0
	vlan100	0b	0b	0	0	0B	0B	0	0	0	0
	vlan521	81.840Kb	81.400Kb	13	13	668.71MB	664.13MB	1153563	1150488	0	0
	vlan522	0b	0b	0	0	64B	1.25KB	1	20	0	0
	tun0	0b	0b	0	0	0B	0B	0	0	0	0
	tun11	0b	0b	0	0	0B	0B	0	0	0	0
	tun100	0b	0b	0	0	0B	0B	0	0	0	0
	tun101	0b	0b	0	0	0B	0B	0	0	0	0
	tun1023	0b	0b	0	0	341.70MB	2.40GB	1683640	2315438	0	0
	gre0	0b	0b	0	0	0B	0B	0	0	0	0
	gre1	0b	0b	0	0	0B	0B	0	0	0	0
	33	0b	0b	0	0	0B	0B	0	0	0	0

接口信息统计的配置项与详细说明如下：

配置项	说明
自动刷新时间	通过点击<**自动刷新**>下拉菜单，选择统计数据的时间范围，可选范围：10 秒、30 秒、300 秒。默认是禁用，禁用就是不进行自动刷新。

点击<**清除计数**>按钮可以清除全部接口计数。

3.1.3. 设备健康统计

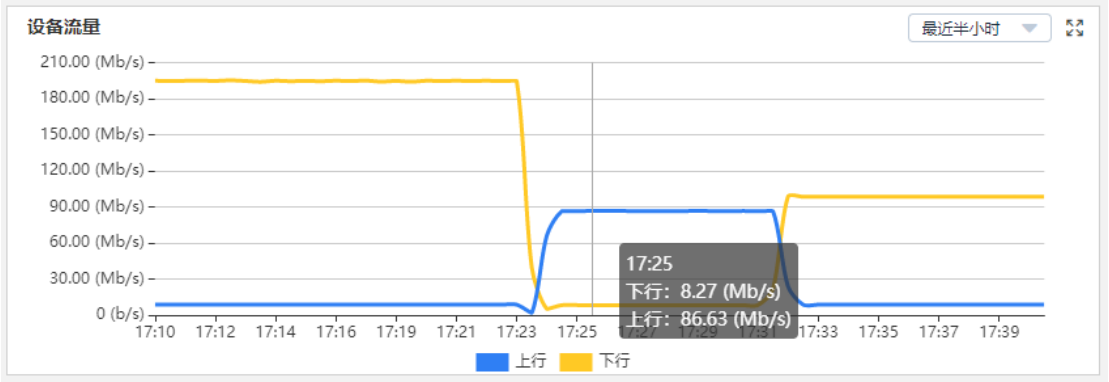
设备健康统计用于展示一定时间段内设备系统资源占用情况，如：通过设备的上下行流量大小、设备连接数、CPU 利用率及内存利用率，用户可根据需要查看不同时间段内设备健康情况。

在系统菜单点击“**监控>系统监控>设备健康统计**”，进入**设备健康统计**配置页面，可直观查看到所有设备健康统计信息，默认所有信息统计时间为最近半小时。

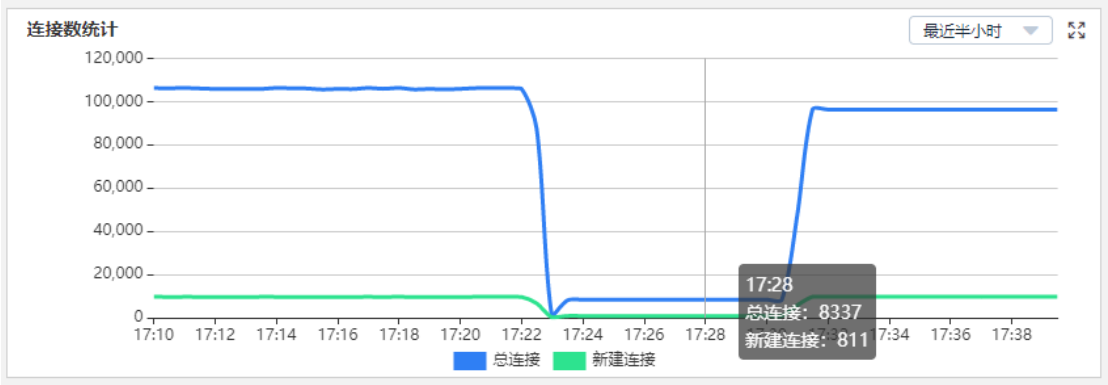
设备健康统计的配置项与详细说明如下：

配置项	说明
时间段	通过点击<**最近半小时**>下拉菜单，选择统计数据的时间范围，可选范围：最近半小时；最近一小时；最近三小时；最近一天；最近一周；最近一月。

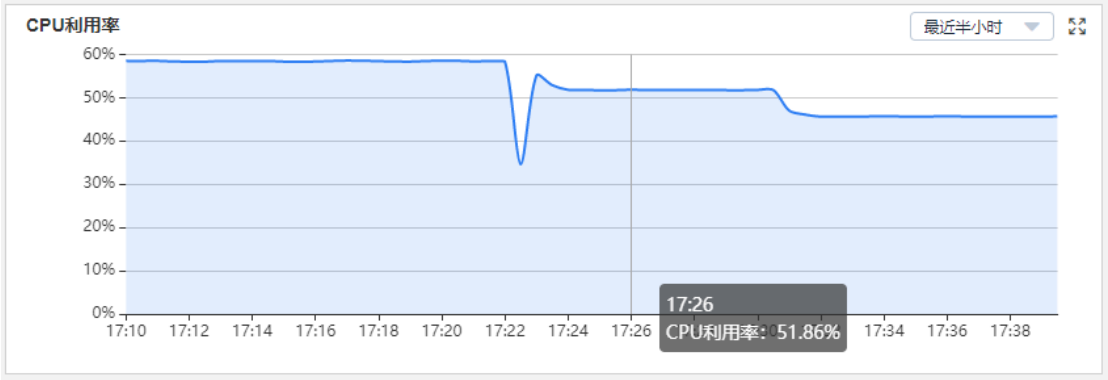
设备流量：统计选定时间内通过设备的上下行流量，可通过点击<**最近半小时**>下拉菜单查看可选时间段，切换时间段可变更查询范围，可通过点击<**上行**><**下行**>按钮，进行单独展示上行或下行流量。



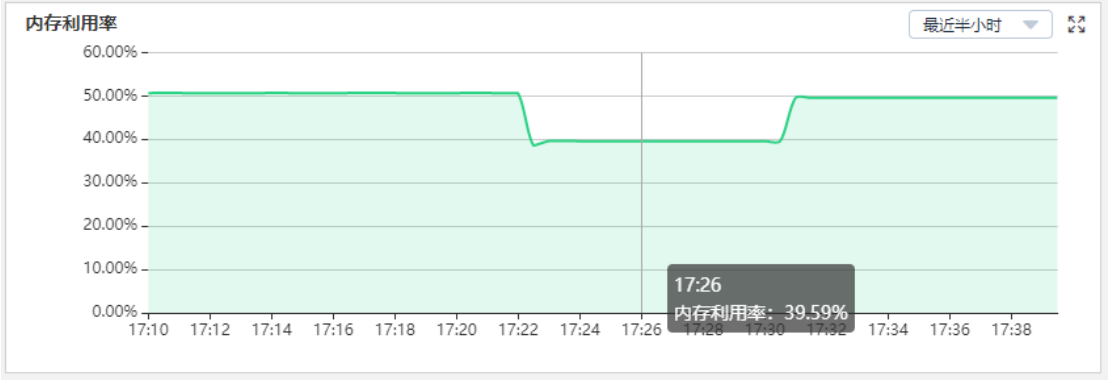
连接数统计：统计选定时间内设备中存在的连接数，包括总连接及新建连接数，可通过点击<**最近半小时**>下拉菜单查看可选时间段，切换时间段可变更查询范围，可通过点击<**总连接**><**新建连接**>按钮，进行单独展示总连接或新建连接。



CPU 利用率：统计选定时间内设备 CPU 占用情况，可通过点击<**最近半小时**>下拉菜单查看可选时间段，切换时间段可变更查询范围。



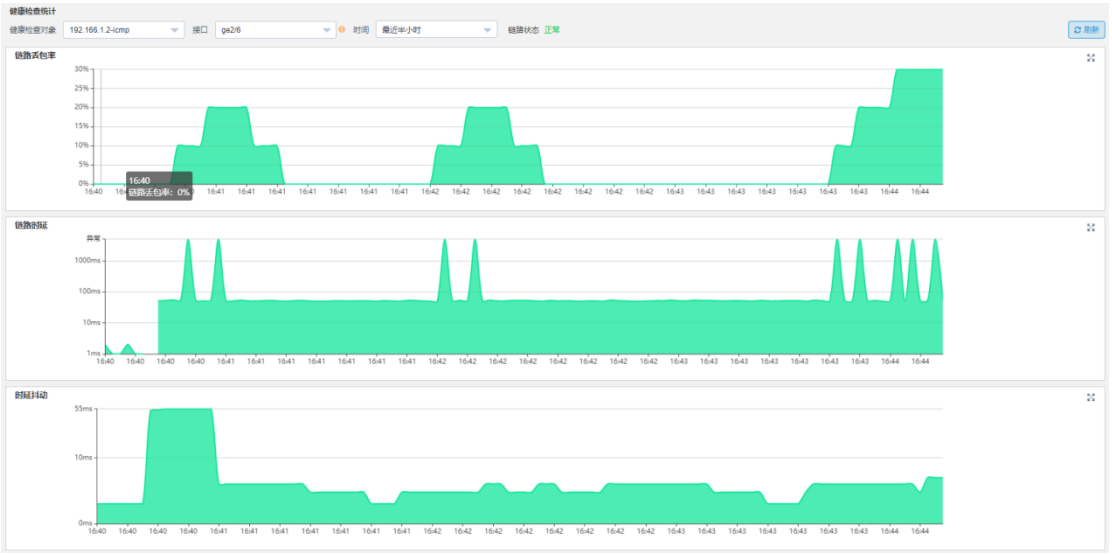
内存利用率：统计选定时间内设备内存占用情况，可通过点击<**最近半小时**>下拉菜单查看可选时间段，切换时间段可变更查询范围。



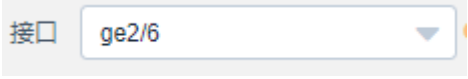
3.1.4. 健康检查统计

健康检查统计可对具体健康检查对象进行监控，统计被监控对象的链路丢包率、链路延时及延时抖动，以图表形式进行展示，可使用户直观的看到所选健康检查对象的链路状态。

在系统菜单点击“监控>系统监控>健康检查统计”，进入健康检查统计配置页面，可根据需求选择被引用的健康检查对象，根据出接口、统计时间，进行相应的图表展示。

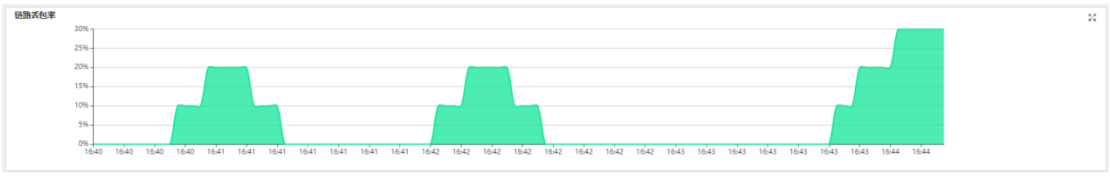


健康检查统计的配置项与详细说明如下：

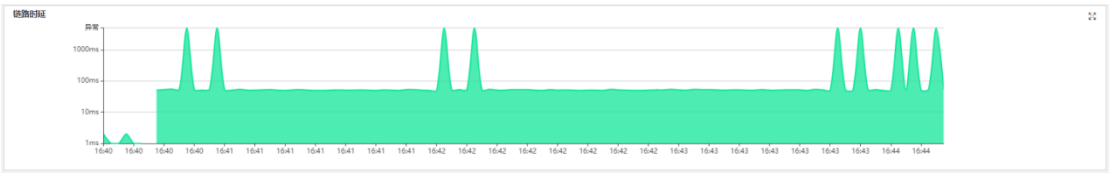
配置项	说明
健康检查对象	下拉菜单，可根据需求选择具体要查询的对象，默认展示健康检查对象中第一条记录。 
接口	下拉菜单，可根据需求选择被路由/HA 引用的出接口，默认展示第一个出接口 
时间	下拉菜单，可根据需求选择需要查询的时间段，默认展示为“最近半小时”，可选时间段：最近半小时；最近一小时；最近一天；最近一

	周。 
链路状态	显示当前链路状态，分为正常、异常和未被引用三种状态 

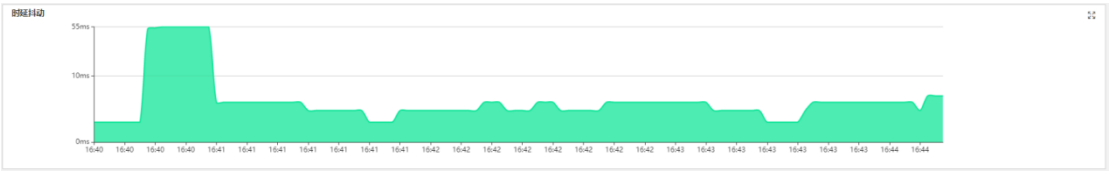
链路丢包率：以百分比为单位展示所选健康检查对象，在所选时间段内的具体丢包情统计到的百分比及具体统计时间，绘制图表进行展示。



链路延时：以 ms 为单位展示所选健康检查对象，在所选时间端内通信延时情况，并根据延时情况及时间段，绘制图表进行展示。



延时抖动：以 ms 为单位展示所选健康检查对象，在所选时间端内通信延时抖动情况，并根据延时抖动及抖动发生的时间段，绘制图表进行展示。



3.2. 流量分析

通过流量分析功能，可监控应用流量控制策略的生效情况和会话信息的统计情况。应用流量控制策略，可监控统计通过防火墙设备应用的流量信息，用户可以查看通过设备的流量模型以及流量分布，管理员可以根据这些数据分析后按需合理规划策略。会话信息监控是统计设备上所有的会话，并可根据参数定制进行查询；包括会话统计、会话监控、会话流

量统计，其中流量统计需要打开流量统计开关才可统计，开关位于一体化策略。

3.2.1. 应用流量统计

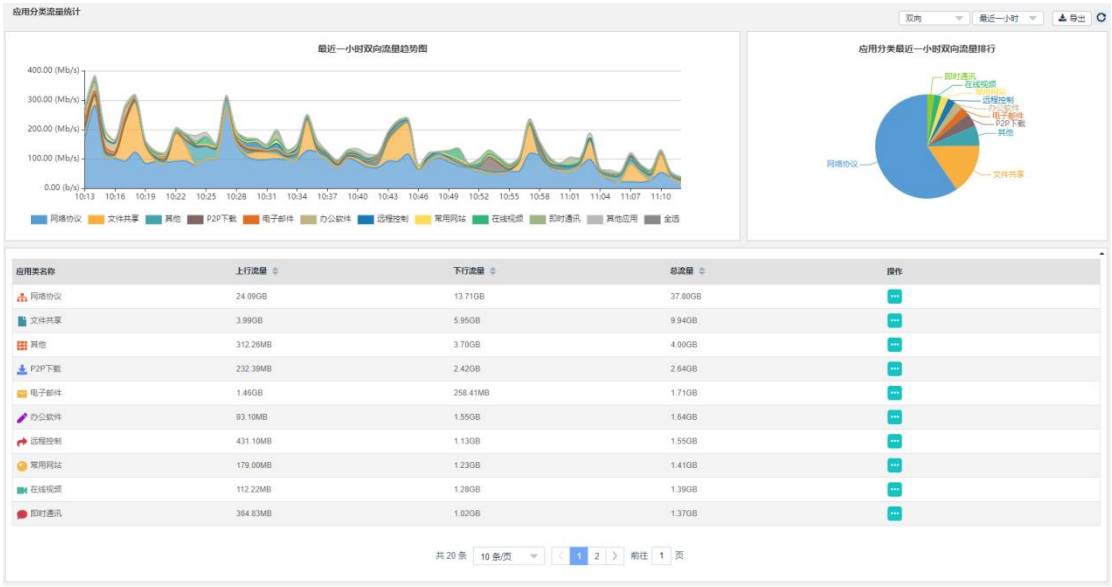
在系统菜单点击“**监控>流量统计>应用流量统计**”，进入**应用流量统计**页面，展示的是一段时间内的应用流量统计情况。

通过页面右上角的下拉框，既可以对统计的时间范围进行调整，包括最近一小时、最近一天、最近一周；又可以对流量的类型进行调整，包括双向、上行、下行；还可以通过<**导出**>按钮对统计信息进行 PDF 导出，通过刷新按钮对当前统计内容进行刷新。

在**应用流量统计**页面，点击操作列的**操作**按钮进入应用访问趋势页面，展示单个应用流量在一段时间内所有用户访问的的统计情况。

3.2.2. 应用分类流量统计

在系统菜单点击“**监控>流量统计>应用分类流量统计**”，进入**应用分类流量统计**页面，展示的是一段时间内的应用分类流量统计情况。

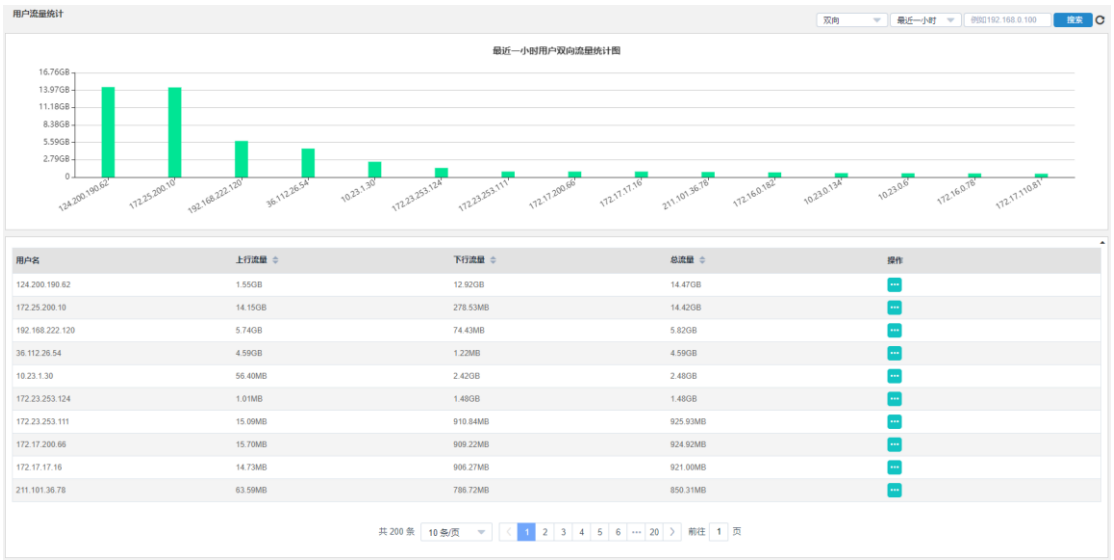


通过页面右上角的下拉框，既可以对统计的时间范围进行调整，包括最近一小时、最近一天、最近一周；又可以对流量的类型进行调整，包括双向、上行、下行；还可以通过<**导出**>按钮对统计信息进行 PDF 导出，通过刷新按钮对当前统计内容进行刷新。

在**应用分类流量统计**页面，点击操作列的**操作**按钮进入应用访问趋势页面，展示单个应用分类流量在一段时间内所有用户访问的的统计情况。

3.2.3. 用户流量统计

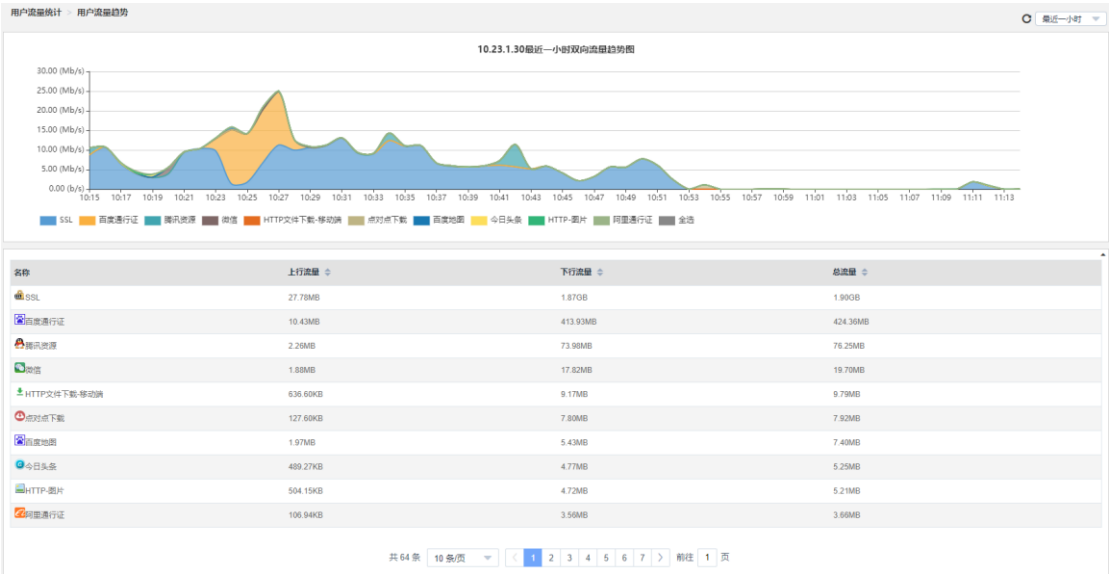
在系统菜单点击“**监控>流量统计>用户流量统计**”，进入**用户应用流量统计**页面，查看设备上所有用户的应用流量统计信息。



通过页面右上角的下拉框，既可以对统计的时间范围进行调整，包括最近一小时、最近一

天、最近一周；又可以对流量的类型进行调整，包括双向、上行、下行；还可以通过刷新按钮对当前统计内容进行刷新。通过右上角的<**搜索**>，搜索单个用户，查看更加详细信息。

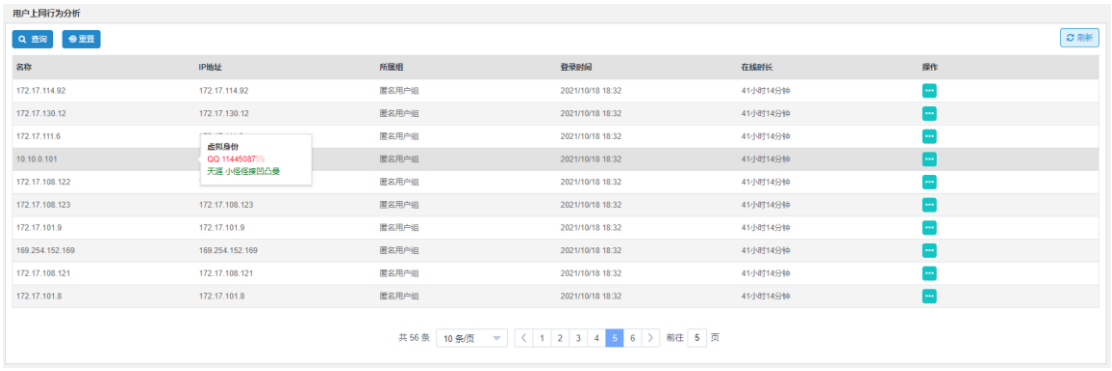
点击页面中用户列表操作列中的**操作**按钮，可以查看单个用户更加详细的流量统计信息。



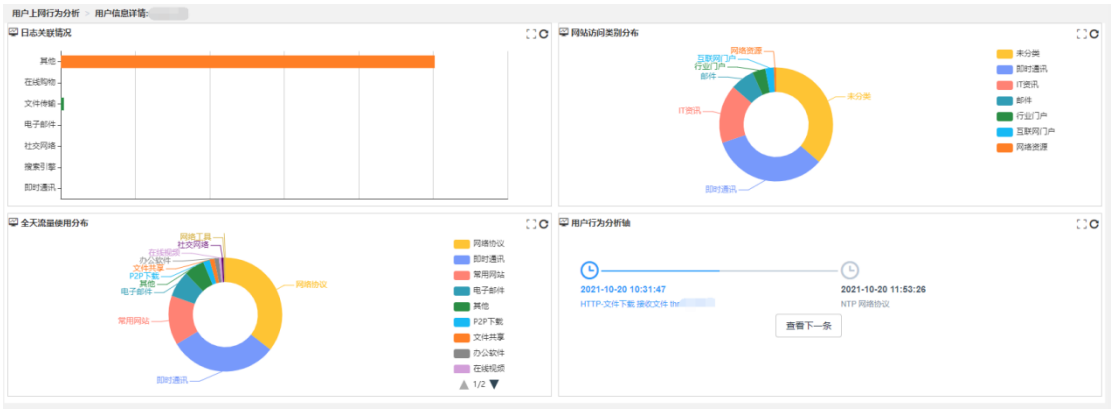
3.2.4. 用户上网行为分析

在系统菜单点击“**监控>流量统计>用户上网行为分析**”，进入**用户上网行为统计**页面，查看设备上所有用户的上网行为统计信息。

用户在登录 qq 后，鼠标放置在用户名称上，会有悬浮框展示用户的虚拟身份。虚拟身份支持 qq 账号、天涯论坛账号等。



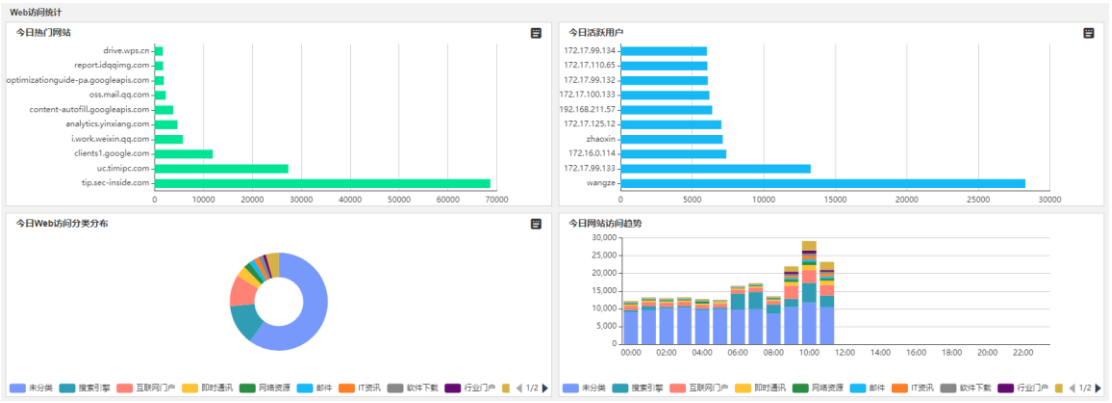
点击操作列的**操作**按钮，进入用户信息详情页面，展示日志关联情况、全天流量使用分布、网站访问类别分布、用户行为分析轴。



3.2.5. Web 访问统计

Web 统计可以统计查看今日热门网站、今日活跃用户、Web 访问分类分布、网站访问趋势等信息。

在系统菜单点击“**监控>流量统计>Web 访问统计**”，进入 **Web 访问统计**页面，可以查看今日热门网站、今日活跃用户、今日 Web 访问分类分布、今日网站访问趋势等。

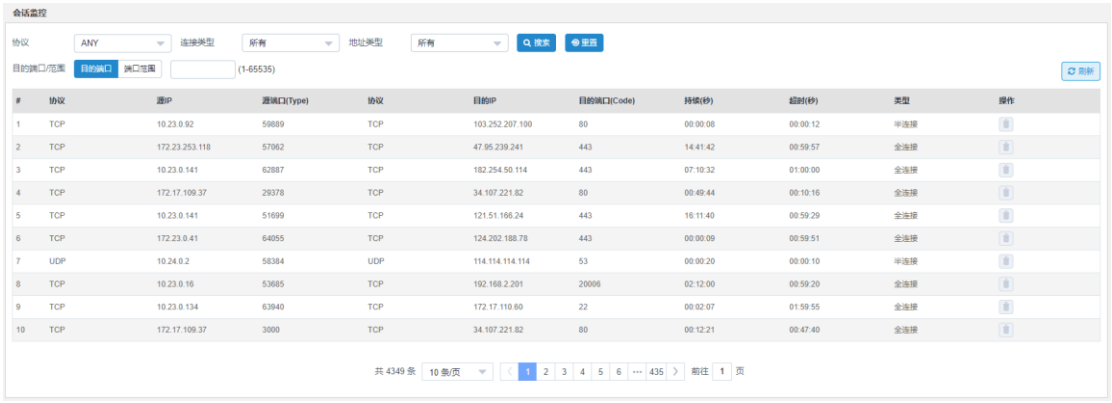


3.2.6. 会话统计

在系统菜单点击“**监控>流量分析>会话统计**”查看会话统计，可查看每个通过设备 IP 的连接数。可基于源 IPv4 统计、源 IPv6 统计、目的 IPv4 统计、目的 IPv6 统计、目的端口统计，默认为基于源 IPv4 统计；当前统计项超过 50 时，只统计前 50 项，按连接数多少排序。

3.2.7. 会话监控

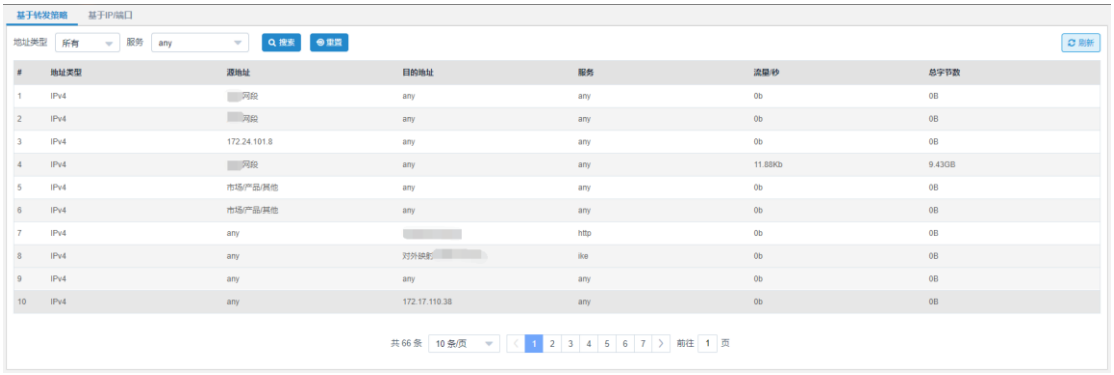
在系统菜单点击“**监控>流量分析>会话监控**”查看会话监控；可查看设备上监控到的会话及连接状态。



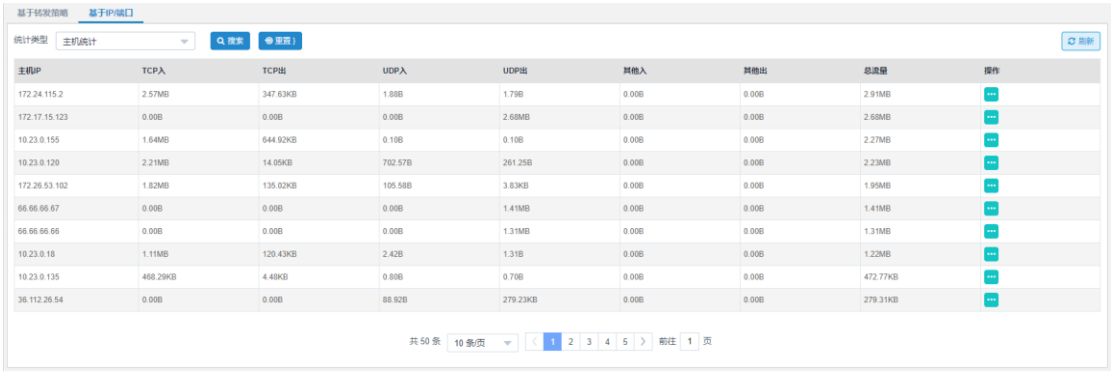
3.2.8. 会话流量统计

在系统菜单点击“**监控>流量分析>会话流量统计**”查看流量统计页面，查看设备基于策略或 IP/接口的转发流量统计。

点击<**基于转发策略**>查看设备基于策略的转发流量统计。



点击<**基于 IP/端口**>查看设备基于策略或 IP/接口的转发流量统计。

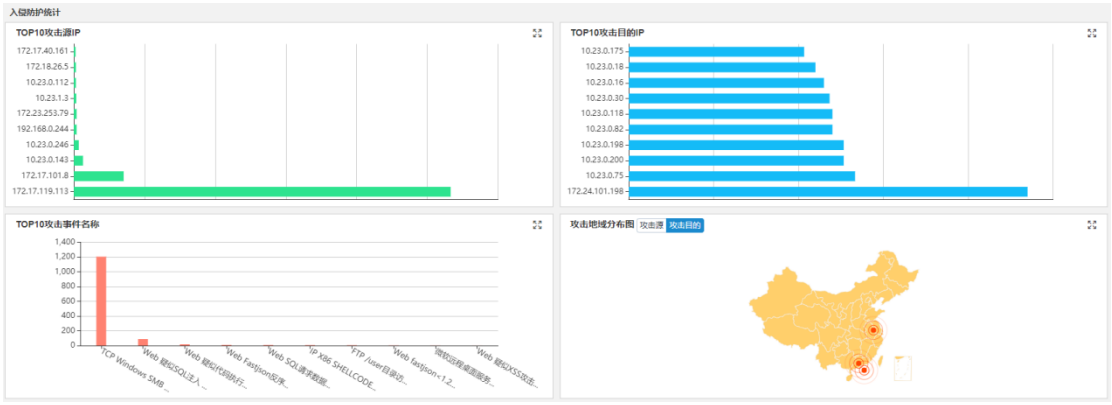


3.3. 安全分析

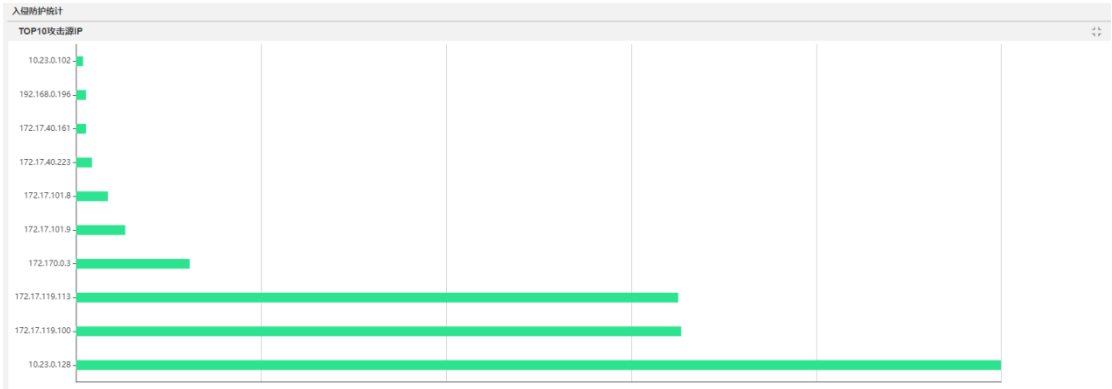
通过安全分析功能，可监控入侵防护、病毒防护和威胁情报的统计数据。管理员可以根据这些分析数据按需合理规划安全策略，防止设备遭受攻击。

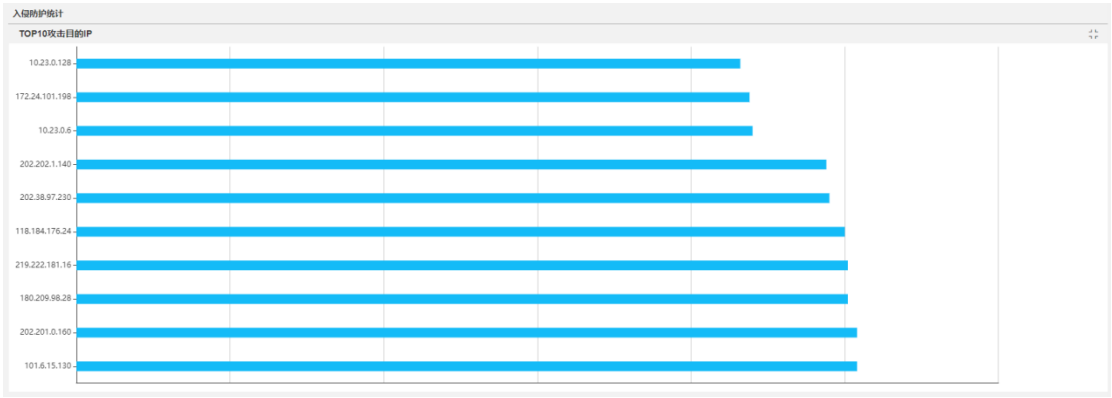
3.3.1. 入侵防护统计

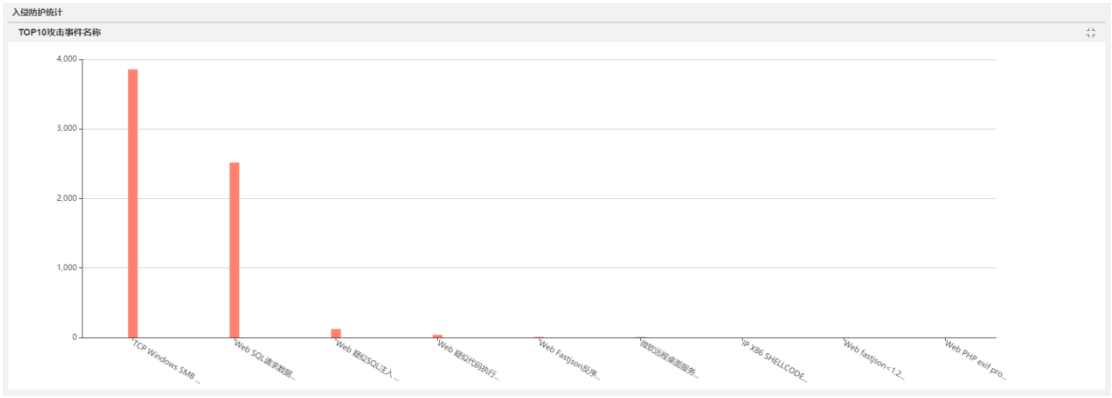
在系统菜单选择 “**监控>安全分析>入侵防护统计**”查看入侵防护统计。在入侵防护统计中统计排行前十的攻击源 IP、目的 IP、攻击事件名称，以及对攻击源和目的 IP 的所在地显示。



点击统计右上角的图标，能够放大显示选择的统计类型。

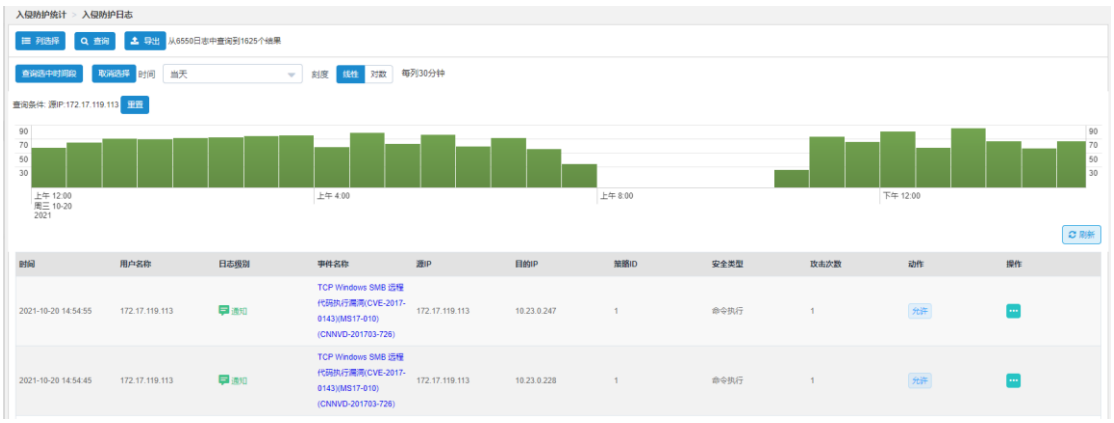






点击统计右上角的图标，能够返回整体显示统计页面。

点击统计显示的单个统计对象能够链接到入侵防护统计日志界面，并过滤出当前用户相关的日志详细内容。



3.3.2. 入侵防护统计列表

在系统菜单选择 “**监控>安全分析>入侵防护统计列表**”查看防护统计列表。防护统计列表根据选择统计周期对发生的事件类型进行统计。

防护统计列表配置项及详细说明如下：

配置项	说明
统计周期	统计周期可以选择当天、最近 7 天、最近 30 天、最近 60 天、最近 90 天和自定义。 选择自定义时需要在新输入框中选择开始和结束时间，作为一个时间范围段，选择的时间不能是未来的时间。

3.3.3. 病毒防护统计

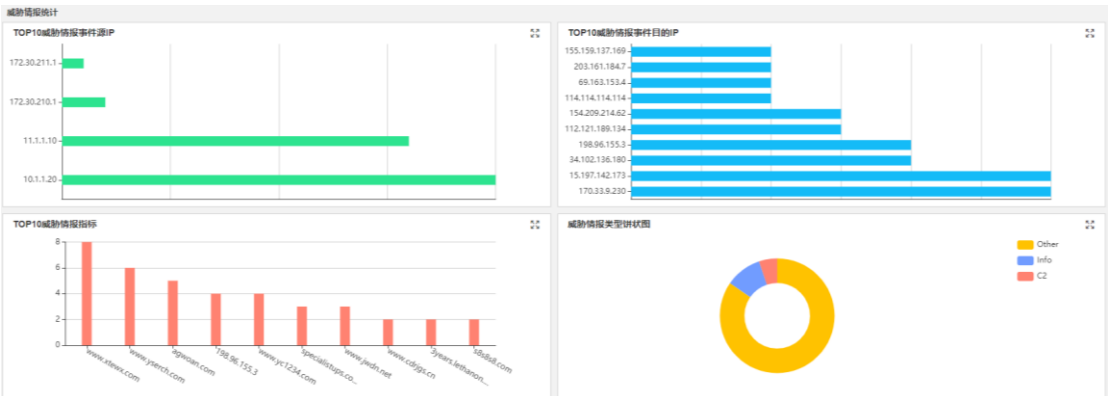
在系统菜单栏点击“**监控>安全分析>病毒防护统计**”，进入**病毒防护统计**页面。分别列出了 TOP10 病毒源 IP、TOP10 病毒目的 IP、TOP10 病毒事件名称信息。

3.3.4. 病毒沙箱防护统计

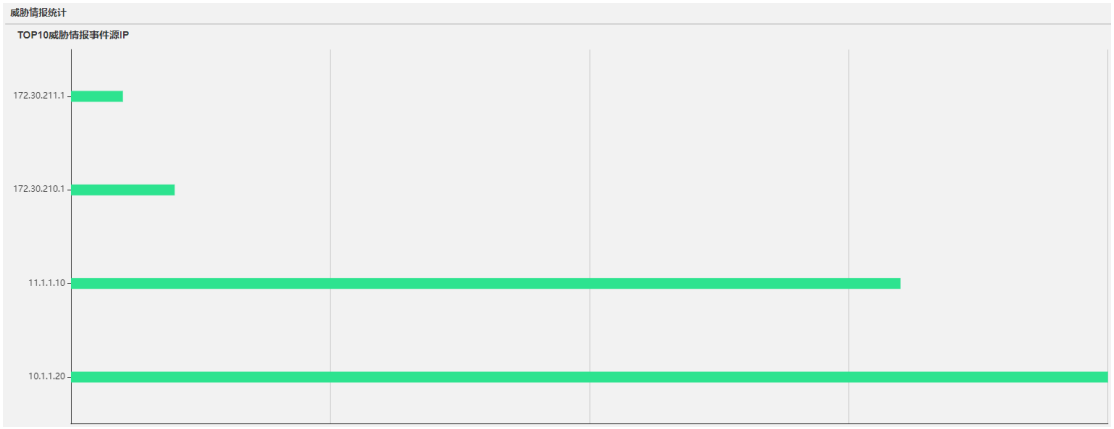
在系统菜单栏点击“**监控>安全分析>病毒沙箱防护统计**”，进入**沙箱防护统计**页面。分别列出了沙箱检测结果统计、沙箱样本类型统计、沙箱检测状态列表。

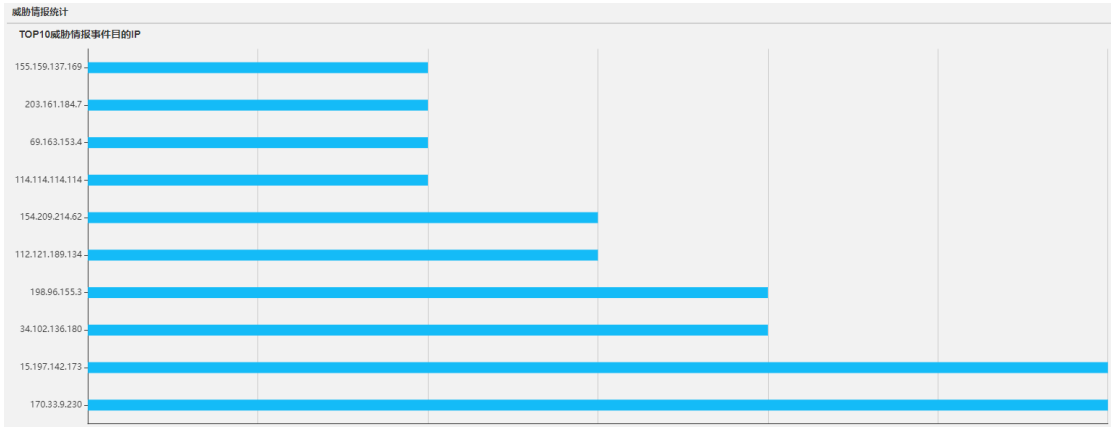
3.3.5. 威胁情报统计

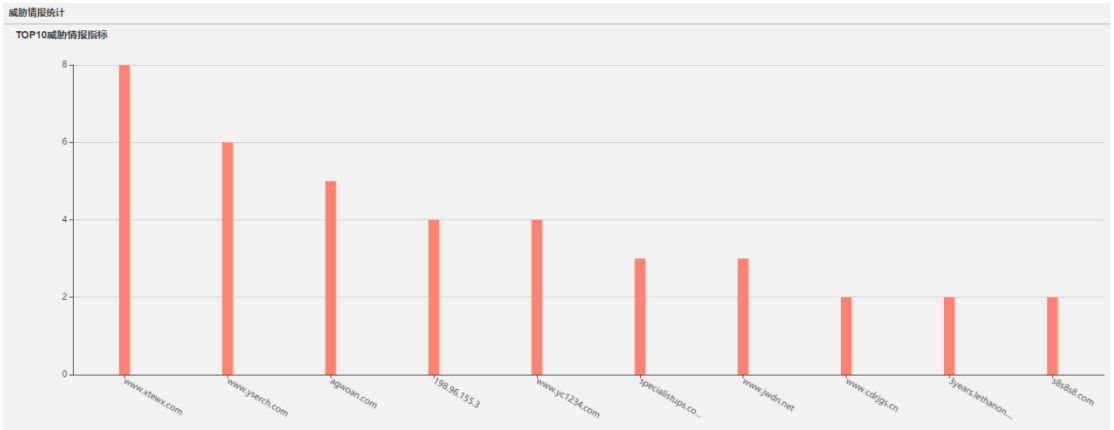
在系统菜单选择“**监控>安全分析>威胁情报统计**”查看威胁情报统计。在威胁情报统计中统计排行前十的威胁情报源 IP、目的 IP、威胁情报指标，以及对威胁情报类型的比例显示。

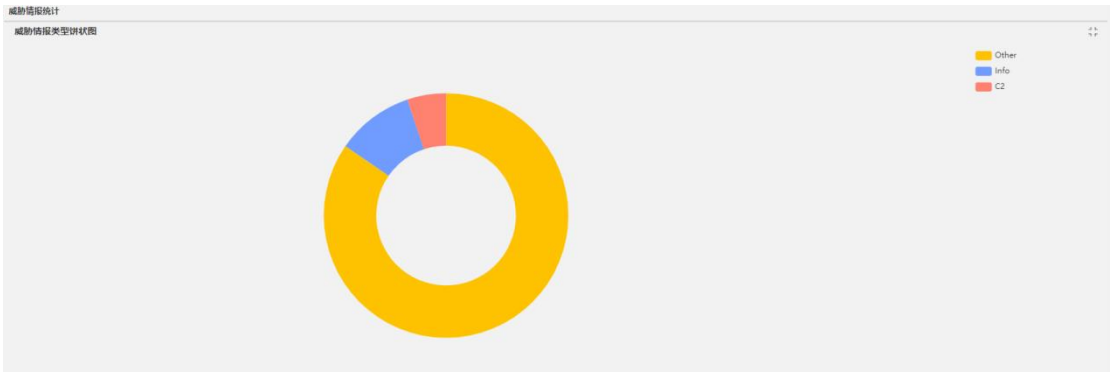


点击统计右上角的图标，能够放大显示选择的统计类型。


威胁情报统计
TOP10威胁情报事件源IP
172.30.211.1
172.30.210.1
11.1.1.10
10.1.1.20

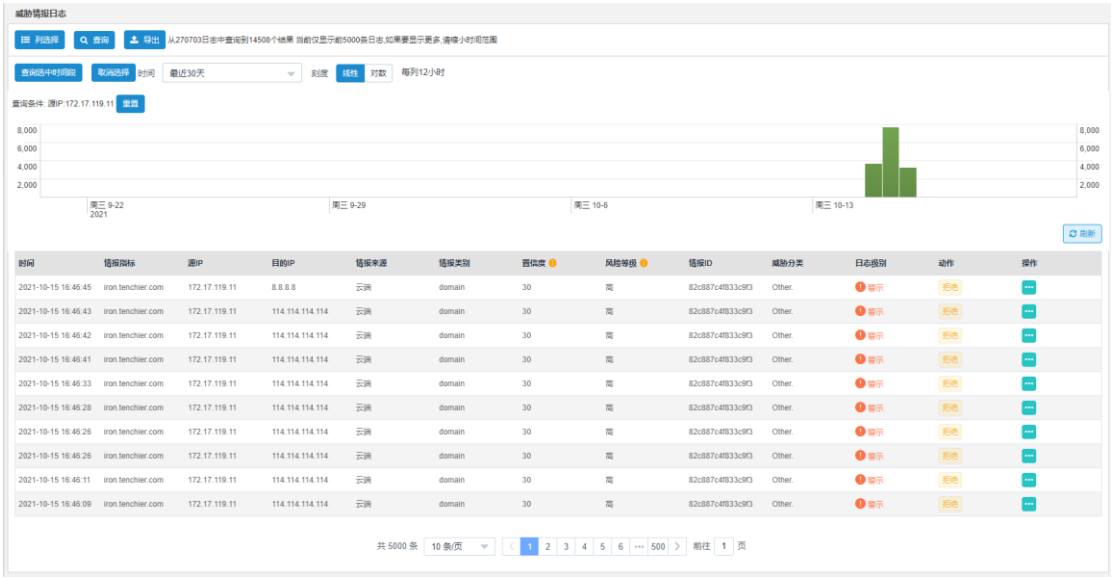

威胁情报统计
TOP10威胁情报事件目的IP
155.159.137.169
203.161.184.7
69.163.153.4
114.114.114.114
154.209.214.62
112.121.189.134
198.96.155.3
34.102.136.180
15.197.142.173
170.33.9.230


威胁情报统计
TOP10威胁情报指标
8
6
4
2
0
www.xtewx.com
www.yserch.com
agwoan.com
198.96.155.3
www.yc1234.com
specialistups.co...
www.jwdn.net
www.cdjtgs.cn
3years.lethanon...
s8s8s8.com



点击统计右上角的图标，能够返回整体显示统计页面。

点击统计显示的单个统计值能够连接到威胁情报统计日志界面，并过滤出当前统计相关的日志详细内容。



3.3.6. 威胁情报统计列表

在系统菜单选择“监控>安全分析>威胁情报统计列表”，进入威胁情报统计列表页面，查看威胁情报统计列表。

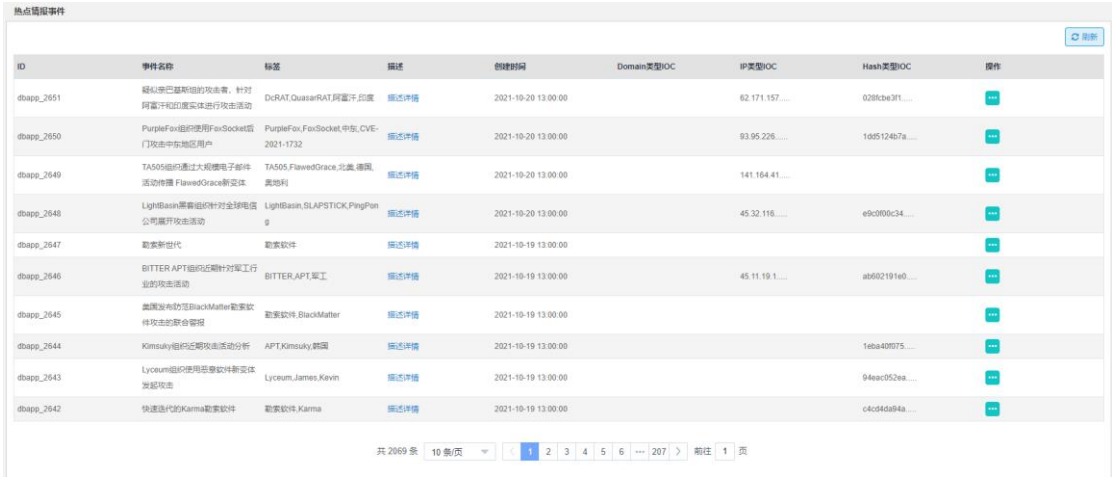
威胁情报统计列表配置项及详细说明如下：

配置项	说明
统计周期	统计周期可以选择当天、最近 7 天、最近 30 天、最近 60 天、最近 90 天。
类型	威胁情报的统计类型包含威胁类型、源 IP、目的 IP、情报指标、情报来源、风险等级、情报类别、情报 ID、情报 HASH。 威胁类型：是指当前威胁的分类，例如 C2、Exploit、Scanner 等。 源 IP：触发威胁情报的源 IP。 目的 IP：触发威胁情报的目的 IP。 情报指标：威胁情报的具体信息，比如：IP、URL、域名。 情报来源：识别威胁情报的来源，包括：自定义情报库、安恒云端情报库、本地恶意 URL 情报库。 风险等级：自定义情报库和本地情报库的风险等级为高、中、低 3 个等级。云端库风险等级为严重、高、中、低、可疑、安全、未知七个等级。 情报类别：是指情报的分类，包含公网 IP、DNS 域名、HTTP URL。 情报 ID：用于识别云端情报库的唯一标识。 情报 HASH：用于识别为风险数据的唯一标识。

3.3.7. 热点情报事件

在系统菜单选择“**统计>威胁情报统计>热点情报事件**”，进入**热点情报事件**页面，查看热点情报事件。

热点情报事件包含当前及时更新的安全热点事件，以及该事件包含的威胁情报内容。



点击“**操作**”列的按钮，可以查看热点事件相关的日志信息，链接到威胁情报日志页面，并过滤显示热点事件相关日志。

第四章 策略

4.1. 防火墙策略

防火墙策略是对经过设备的流量进行转发、阻断及其他高级安全检测的策略。为了对数据流进行统一控制，方便用户配置和管理，下一代防火墙设备引入了一体化策略的概念。

一体化策略是防火墙系统最核心的功能之一。在没有配置任何一体化策略的情况下，对于经过设备的所有数据包，其缺省为不开启策略匹配，且状态为丢弃。

通过配置一体化策略能够对经过设备的数据流进行有效的控制和管理。当设备收到数据报文时，把该报文的方向、源地址、目的地址、协议、端口等信息和用户配置的策略匹配，决定是否建立这条数据流，并且把这条流和匹配的策略关联起来，从而确定如何处理该流的后续报文，实现允许、丢弃，决定哪些用户和数据能进出，以及它们进出的时间。

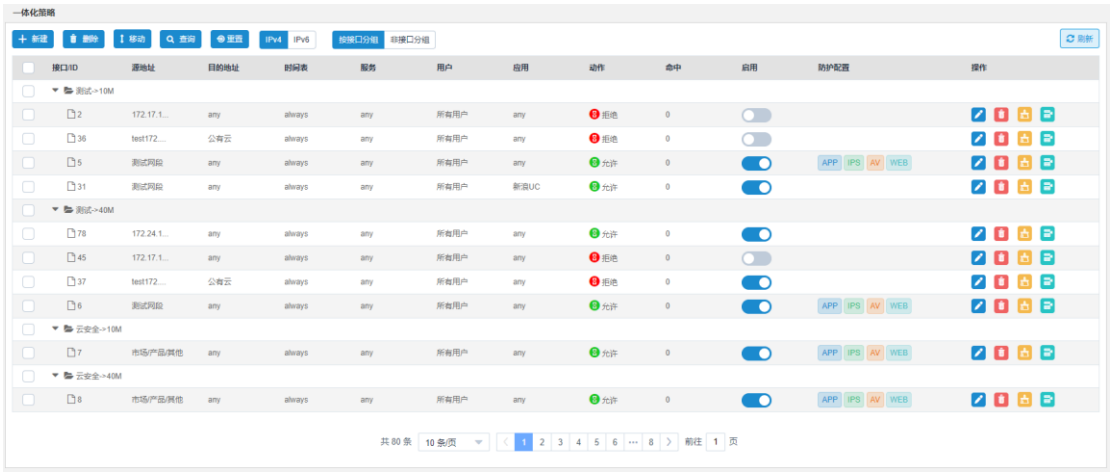
同时，在一体化策略中还可以根据匹配结果，对符合规则的报文实行策略引用的防护配置模板中设置的安全防护检查。

一体化策略遵循在相同入、出接口时从上往下的原则，只对通过设备的数据包进行处理，对于设备本身发出的数据包不进行限制。

4.1.1. 一体化策略

一体化策略同时支持 IPv4 和 IPv6 两种协议栈。一体化策略从源接口/安全域、目的接口/安全域、源地址、目的地址、服务、用户、应用以及时间表八元组，对数据包进行控制。配置多条一体化策略时，设备将按照策略顺序依次匹配所有策略条目。

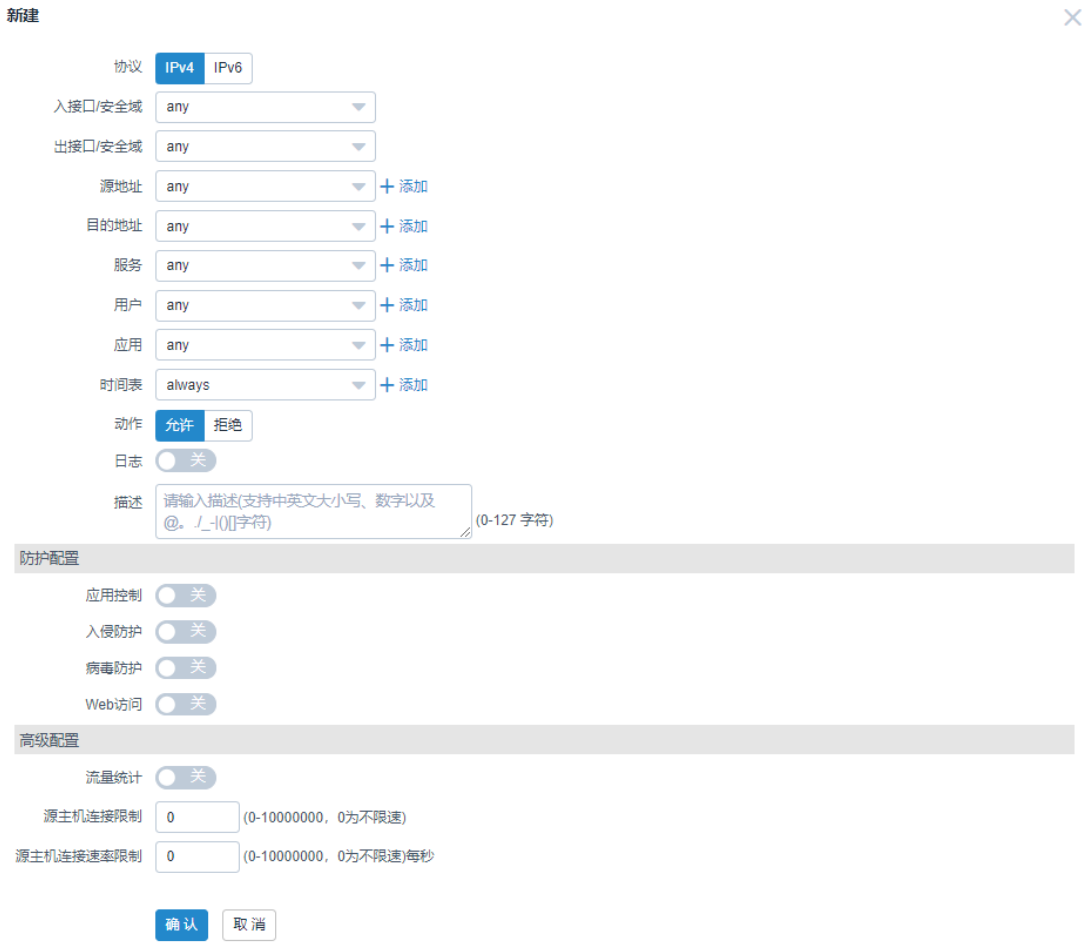
在系统菜单中点击“**策略>防火墙策略>一体化策略**”，进入**一体化策略**配置页面。



一体化策略的操作项及说明如下：

操作项	说明
新建	新建策略。
删除	删除策略。
移动	移动策略顺序。
查询	根据源地址、目的地址、服务、动作来查询策略。
重置	重置查询。
IPv4/IPv6	区分 IPv4 和 IPv6 协议栈的显示。
按接口分组/非接口分组	按接口分组将相同入接口、出接口分为一组，非接口分组不显示入接口、出接口，只显示一体化策略 ID。
启用	启用或禁用策略。
操作	可对该策略进行的操作，包括编辑、删除、清除和插入。

用户可在**一体化策略**页面下点击<**新建**>创建新的一体化策略。



一体化策略的配置项及详细说明如下：

配置项	说明
基础配置	
协议	一体化策略分为 IPv4 和 IPv6 两种类型，数据包匹配相应协议类型的一体化策略。
入接口/安全域	数据流匹配的入接口/安全域。有关接口和安全域配置的更多信息，请参考接口和安全域。
出接口/安全域	数据流匹配的出接口/安全域。有关接口和安全域配置的更多信息，请参考接口和安全域。
源地址	数据流的源地址，可以引用已定义的某个地址对象或地址组，any 表示源地址为任意。

目的地址	数据流的目的地址，可以引用已定义的某个地址对象或地址对象组，any 表示目的地址为任意。
服务	数据流的服务属性，包括协议、源端口和目的端口，可以引用系统预定义服务、自定义的服务对象或服务对象组，any 表示服务为任意，请参考服务。
用户	数据流中源 IP 地址所对应用户对象。any 表示用户为任意。
应用	数据流中匹配的应用对象，any 表示应用为任意。
时间表	策略生效的时间，可以引用已配置的时间，always 表示所有时间。
动作	对符合匹配条件的数据流执行的动作。
日志	数据流命中产生相关日志。
描述	一体化策略的描述，长度限制为 127 个字符。
防护配置	
应用控制	支持引用应用控制策略，请参考应用。
入侵防护	支持引用入侵防护策略，请参考入侵防护。
病毒防护	支持引用病毒防护策略，请参考病毒防护。
Web 访问	支持引用 Web 访问策略，请参考 Web 访问审计。
高级配置	
流量统计	统计匹配该策略的流量，在系统菜单中点击“**监控>流量分析>应用流量统计**”进行查看，请参考流量分析。
源主机连接限制	对匹配该条策略的流，根据源地址连接数进行限制。
源主机连接速率限制	对匹配该策略的流，根据源地址连接速率进行限制。

一体化策略同时支持 IPv6，在系统菜单中点击“**策略>防火墙策略>一体化策略**”，按协议分组选择 IPv6。

用户可在**一体化策略**页面下点击<**新建**>创建新的一体化策略。

注意：

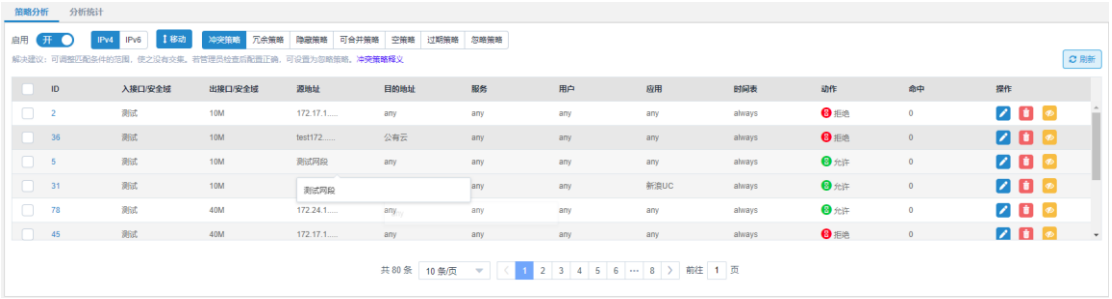
IPv6 不支持引用应用对象。

4.1.2. 策略分析

下一代火墙对当前配置的 IPv4 及 IPv6 一体化策略进行策略分析，检查出冲突策略、冗余策略、隐藏策略、可合并策略、空策略、过期策略和忽略策略，方便管理员维护和管理。

4.1.2.1. 策略分析

在系统菜单中点击“策略>防火墙策略>策略分析>策略分析”进入策略分析配置页签。



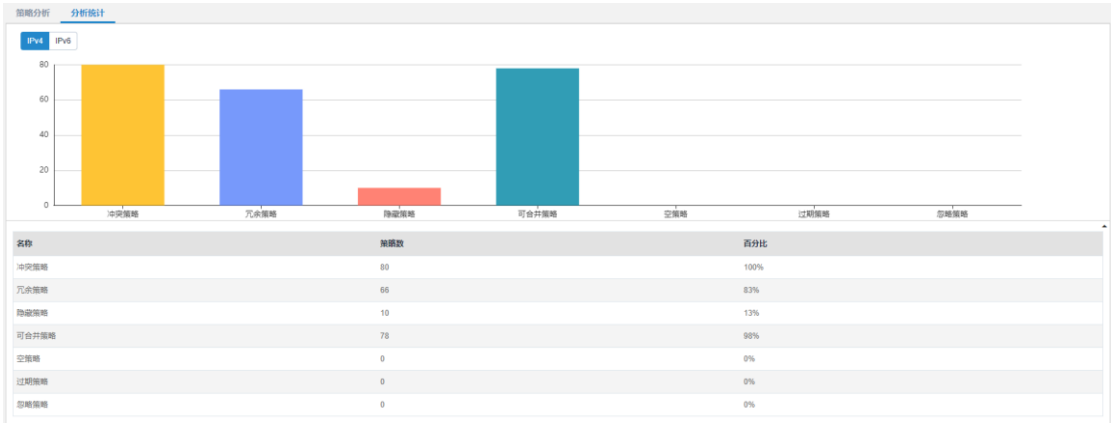
策略分析的配置项及详细说明如下：

配置项	说明
启用	启用或禁用策略分析功能。
IPv4/IPv6	区分 IPv4 和 IPv6 的策略分析页面。
移动	移动某条一体化策略。
刷新	刷新页面。
操作	可对该策略进行的操作，包括编辑、删除和忽略。

策略分析同时支持 IPv6 一体化策略的实时分析，在系统菜单中点击“**策略>防火墙策略>策略分析>策略分析**”进入**策略分析**页签，选择 IPv6 协议。

4.1.2.2. 分析统计

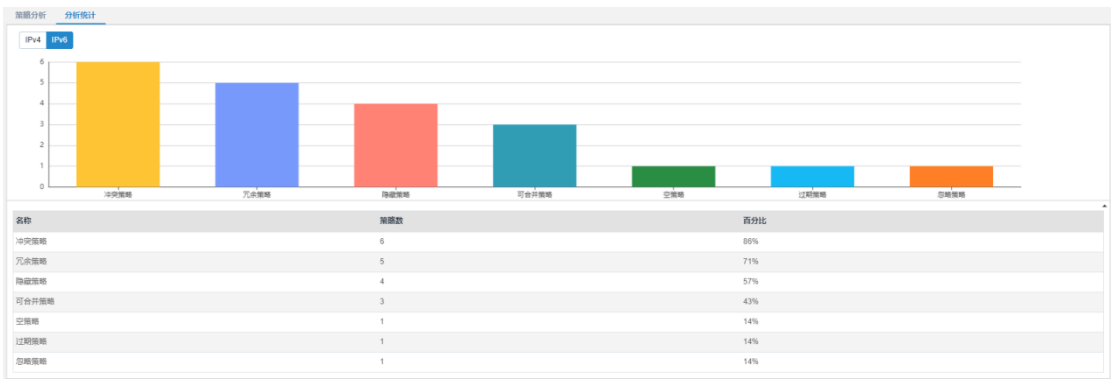
在系统菜单中点击“**策略>防火墙策略>策略分析>分析统计**”进入**分析统计**配置页签。



分析统计的显示项及说明如下：

显示项	说明
冲突策略	不区分匹配的前后顺序，若 A 策略和 B 策略存在数据流交集（非包含和被包含关系），且 A、B 策略的行为不同，则 A 和 B 互为冲突策略。
冗余策略	根据匹配的前后顺序（先匹配 A 策略后匹配 B 策略），如果 A 策略匹配的所有数据流会被 B 策略包含，删除 A 策略不会对其余策略产生影响，且 A、B 策略行为相同，则 A 策略会被认定为冗余策略。
隐藏策略	根据匹配的前后顺序（先匹配 A 策略后匹配 B 策略），如果 B 策略匹配的所有数据流会被 A 策略包含，且 A、B 策略行为相同，则 B 策略会被认定为隐藏策略。
可合并策略	不区分匹配的前后顺序，策略内元组信息只有一项不同（且可合并），则认定为可合并策略。
空策略	当策略中匹配的任何一个对象为空时，该策略会被认定为空策略。
过期策略	策略匹配的时间范围已经不会再次出现。
忽略策略	手动忽略不进行匹配的策略。

分析统计同时支持 IPv6 一体化策略的实时分析，在系统菜单中点击“**策略>防火墙策略>策略分析>分析统计**”进入**分析统计**页签，选择 IPv6 协议。



注意：

用户在新建或编辑一体化策略后，策略分析实时分析新建或编辑策略对已有策略产生的影响。

4.1.3. 黑名单

下一代防火墙支持全局地址黑名单功能。黑名单功能支持配置的时间有效性。如果某条数据流的 IP 地址匹配黑名单表项，则在该配置的时间内，该数据流被丢弃。

4.1.3.1. 黑名单

在系统菜单点击“**策略>防火墙策略>黑名单>黑名单**”进入**黑名单**配置页签。

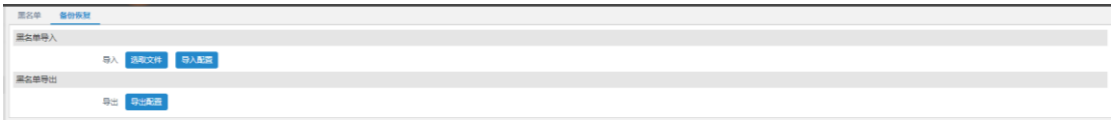
在**黑名单**页签，点击<**新建**>创建新的黑名单。

黑名单配置项及详细说明如下：

配置项	说明
地址类型	支持 IPv4 和 IPv6 两种地址类型。
源 IP	报文的源 IP 地址。
生命周期	可以设置时间 5 分钟、10 分钟、15 分钟、30 分钟、1 小时、2 小时、4 小时，或永久。

4.1.3.2. 备份恢复

在系统菜单点击“**策略>防火墙策略>黑名单>备份恢复**”进入黑名单导入导出页签。



备份恢复配置项及详细说明如下：

配置项	说明
导入	点击选取文件自动打开本地目录，选取要导入的文件后，点击导入配置，黑名单导入成功。
导出	点击导出配置，导出现有的黑名单列表的所有内容。

4.2. 用户策略

下一代防火墙支持用户认证、用户资源管理、用户防暴力破解、用户限额策略等功能。通过

配置用户策略，可以对用户的网络访问进行详细的管控。

4.2.1. 用户认证

下一代防火墙支持用户认证策略，可以指定符合条件的用户，只有通过设置的认证方式认证成功后，才能访问具体的对应资源。

在系统菜单点击“**策略>用户策略>用户认证**”进入**用户认证**页面，可以实现对用户认证的新建、修改、删除和移动。

在**用户认证策略**页签下点击<**新建**>创建新的用户认证策略，或在右侧“操作”列点击 编辑已有的用户认证策略。

用户认证策略配置项及详细说明如下：

配置项	说明
入接口	选择用户认证策略所应用的入接口。
源地址	选择用户认证策略所应用的源地址。有关地址对象配置的更多信息，请参考地址。
出接口	选择用户认证策略所应用的出接口。
目的地址	选择用户认证策略所应用的目的地址。有关地址对象配置的更多信息，请参考地址。
时间表	选择用户认证策略生效时间。有关时间配置的更多信息，请参考时间。
共享接入检测	选择开启关闭共享接入检测。
动作	认证方式包括允许、本地认证、Portal 认证、单点认证、二维码认证、短信认证、免认证、混合认证。有关认证方式的更多信息，请参考用户认证。

用户认证策略按照从上到下的顺序依次匹配，如需修改策略匹配顺序，可勾选需要移动的用户认证策略，点击<**移动**>，选择目标位置完成策略移动后更换匹配顺序。

4.2.2. 用户资源

为了对用户以及用户可访问的资源做精细化的管控，可以配置用户资源策略，授权不同用户访问合法的用户资源。

在系统菜单点击“**策略>用户策略>用户资源**”，进入**用户资源**配置页面，查看设备上已有的全部用户资源策略。设备将按照从上到下的顺序依次匹配所有的用户资源策略。

在用户资源策略页面，点击<**新建**>按钮创建新的用户资源策略，或在“操作”列点击编辑按钮修改已有的用户资源策略。

用户资源策略配置项及详细说明如下：

配置项	说明
状态	默认开启状态，点击状态开关可禁用该策略。
日志	默认关闭，命中该策略后，不会产生安全日志；点击日志开关可开启，命中该策略后，会产生日志。在系统菜单点击“**日志>安全日志**”，进入**安全日志**页面，查看日志的详细信息。
资源对象	可以在下拉框中，选择已创建的资源对象和资源组。在策略匹配过程中，会首先进行资源对象的匹配，有关资源对象配置的更多信息，请参考资源对象、资源组。
用户	可以在下拉框中，选择已创建的用户和用户组。在策略匹配过程中，命中资源对象后，会进行用户的匹配，有关用户配置的更多信息，请参考用户、

	用户组。
时间表	可以在下拉框中，选择已创建的时间对象。在系统时间不在时间对象的时间范围内，该策略选择资源对象中的服务，不再对外提供服务。有关时间表配置的更多信息，请参考绝对时间、周期时间。

4.2.3. 用户防暴力破解

下一代防火墙支持用户防爆力破解功能，当监测到 SSL VPN、IPSec-VPN、Portal 认证、远程认证、本地认证等认证行为后，对认证失败次数进行监控，当一分钟内连续失败次数达到阈值后，会进行认证 IP 的锁定，从而避免非法人员利用工具破解用户密码，给用户资产带来不可预计的损失。

4.2.3.1. 用户防暴力破解

在系统菜单点击“**策略>用户策略>用户防暴力破解>用户防暴力破解**”，进入**用户防暴力破解**配置页签，“启用”用户同名登录和同 IP 登录，看到如下配置。

用户防暴力破解配置项及详细说明如下：

配置项	说明

同 IP 用户登录	默认关闭状态，开启同名用户登录开关后，显示连续出错、锁定时间配置项。同名用户登录只关注同一用户的连续认证失败次数，在锁定 IP 时，只锁定达到连续出错次数的最后一次的 IP 地址。
连续出错	默认值为 5，当一分钟内同一用户认证失败次数达到连续出错次数，该 IP 地址会被锁定；当用户认证成功后，认证失败的次数会自动清空；当 IP 地址被解锁后，认证失败的次数会自动清空；当同名用户登录和同 IP 用户登录都关闭后，认证失败的次数会自动清空。
锁定时间	默认时间为 1 分钟，当 IP 被锁定时，锁定时间即是这里设置的时长。修改锁定时间，不会对已锁定的 IP 的锁定时间生效，只会对下一次锁定 IP 时生效。
同 IP 用户登录	默认关闭状态，开启同名用户登录开关后，显示连续出错、锁定时间配置项。同 IP 用户登录不仅关注用户的连续失败次数，还关注认证失败的 IP 地址。当有多个 IP 地址认证失败同一用户时，只有每个 IP 认证失败次数达到连续出错次数，才会将该 IP 地址锁定。

4.2.3.2. 用户锁定

完成**用户防暴力破解**配置后，在系统菜单点击“**策略>用户策略>用户防暴力破解>用户锁定**”，切换到**用户锁定**页签，查看锁定的 IP 地址，点击操作列的解绑按钮，对锁定的用户进行解绑。

提示：

同名用户登录统计认证失败次数的顺序在同 IP 用户登录之前。

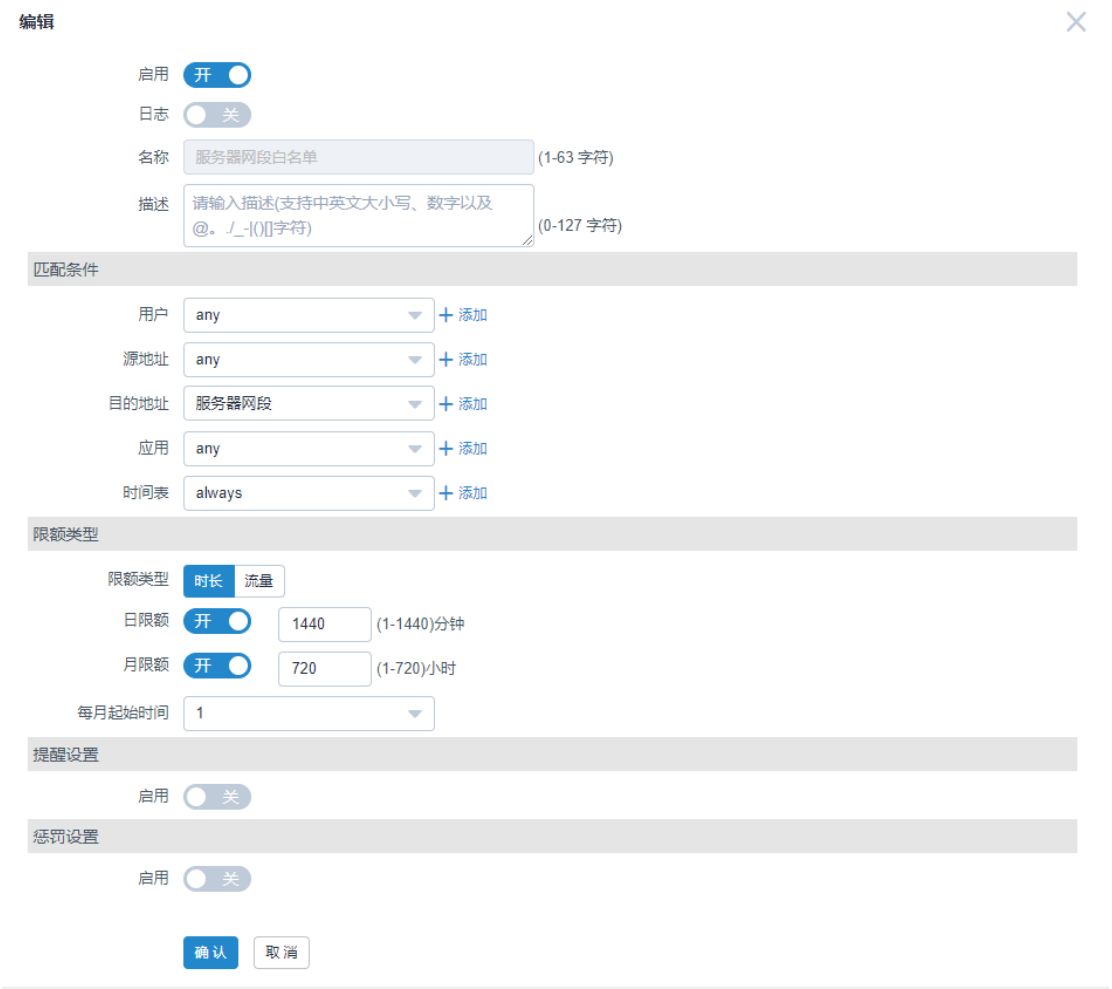
4.2.4. 用户限额

用户限额策略用于监控及控制用户的上网时长或流量，达到阈值后对用户进行惩罚限速或禁止其上网。

4.2.4.1. 用户限额

在系统菜单点击“**策略>用户策略>用户限额>用户限额**”，进入**用户限额**配置页签，查看本设备已有的全部用户限额策略。设备将按照从上到下的顺序，依次匹配所有的用户限额策略。

在用户限额策略页面，点击<**新建**>按钮创建新的用户限额策略，或点击已有用户限额策略的编辑按钮修改已有的用户限额策略。



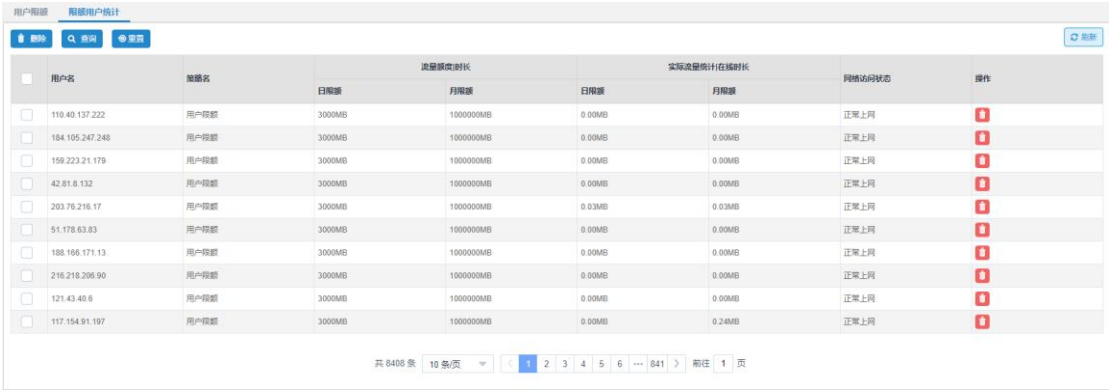
用户限额策略配置项及详细说明如下：

配置项	说明
启用	默认开启，关闭启用开关后，策略禁用，无法生效。
日志	默认关闭，开启日志开关后，能够产生用户上线、推送提醒消息、惩罚用户、用户下线的系统日志。点击系统菜单“**日志>系统日志**”，进入**系统日志**页面，查看系统日志详细信息。
名称	输入策略的名称。
描述	输入策略的描述信息（可选）。
匹配条件	基于用户、源/目的地址、时间、应用等条件对流量进行匹配，对匹配的流量执行策略中指定的限额措施。有关上述对象配置的更多信息，请参考用户对象、地址、应用、时间。

限额类型	● **时长**–统计用户的上网时长。 ● **流量**–统计用户的上网流量大小。 ● **日限额**-用户每日上网流量/时长的最大值，超过此值，会按照惩罚设置进行惩罚。 ● **月限额**-用户每月上网流量/时长的最大值，超过此值，会按照惩罚设置进行惩罚。 ● **每月起始时间**–清空本月所有用户流量/时长的时间点。
提醒设置	默认关闭状态，开启该功能后，用户上网流量或时长达到指定阈值时，设备将按照间隔时间，定期向用户重新定向到提醒页面。
惩罚设置	默认关闭状态，开启后设置用户达到上网流量或时长限额后的惩罚措施及惩罚时长，0 代表时间无限制，包括将该用户的所有后续流量都引流到惩罚通道，或禁止用户上网。有关惩罚通道配置的更多信息，请参考惩罚通道。

4.2.4.2. 限额用户统计

完成**用户限额**配置后，在系统菜单点击“**策略>用户策略>用户限额>限额用户统计**”，进入**限额用户统计**配置页签，查看限额用户的上网流量或上网时长统计。



4.3. 应用控制与审计

下一代防火墙支持对用户的应用访问行为进行详细的控制和审计。

4.3.1. 应用控制

应用控制是针对应用软件进行有效管理，通过配置控制规则对应用分类、应用组、预定义应用、自定义应用通过应用行为、内容、选项、关键字、动作、级别、时间 7 个参数来管理控制。

应用控制功能作为策略模板，需要被一体化策略引用才能生效，配置请参考“防火墙策略”。

在系统菜单点击“**策略>应用控制与审计>应用控制**”，进入**应用控制**配置页面。点击<**新建**>创建新的应用控制，或在右侧“操作”列点击图标编辑已有应用控制数据。也可以点击复制应用控制数据。

应用控制模板配置项及详细说明如下：

配置项	说明
启用	开启应用控制规则。
应用	支持自定义应用和应用组以及预定义应用分类。
应用行为	支持所有应用行为，默认是 any。
内容	设置应用的具体内容，默认是 any。
选项	对应用的具体内容选择包含或者不包含。
关键字	配置应用控制规则匹配的自定义关键字，默认是 any。
动作	为以上匹配规则选择“允许”或“拒绝”。
级别	为匹配以上控应用制规则的应用设定日志级别，支持 7 种日志级别：紧

	急、告警、严重、错误、警示、通知、信息。
时间	对具体应用发生的时间进行设定。
确认	提交控制规则配置内容。

配置完成后点击<**确认**>后，触发应用控制配置后，点击“**日志>应用控制日志**”选择配置的控制规则内容日志可查看控制日志信息。

4.3.2. 应用审计

应用审计是针对应用的审计监测，在模块用户上网行为统计、共享接入检测等功能使用过程中，需开启应用审计功能。审计内容主要包括：即时通讯、搜索引擎、社交网络、电子邮件、文件传输、在线购物、其他应用。

在系统菜单点击“**策略>应用控制与审计>应用审计**”，进入**应用审计**配置页面。点击<**新建**>创建新的应用审计配置，或在右侧“操作”列点击图标编辑已有应用审计数据。

应用审计配置项及详细说明如下：

配置项	**说明**
用户	默认为 any，可点击下拉框选择用户组。可以点击<**添加**>按钮创建用

	户。
地址	默认为 any，可点击下拉框选择地址对象。可以点击<**添加**>按钮创建地址对象。
审计内容	可直接勾选审计内容。点击<**更多选项**>可勾选其他应用。

配置完成后点击<**确认**>后，触发应用审计配置后，点击“**日志>应用审计日志**”选择配置的审计内容日志可查看审计日志信息。

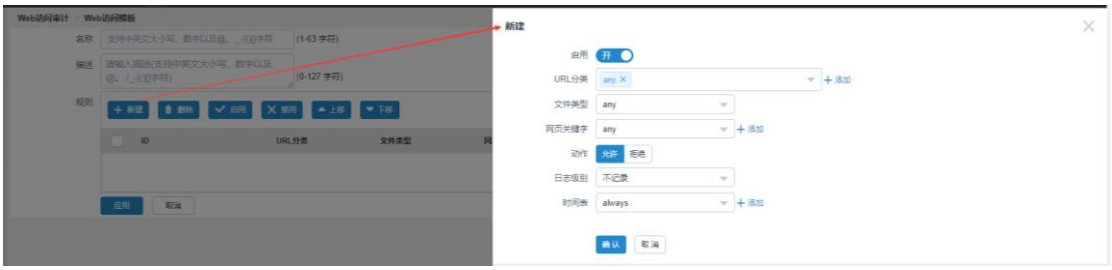
提示：

配置应用审计前，请先进行日志过滤配置，开启对应模块的日志记录。

4.3.3. Web 访问审计

Web 访问审计用于对通过 HTTP 协议的应用进行审计，可以对通过防火墙设备上网的用户访问 HTTP 的网页进行精细化的控制。

在系统菜单点击“**策略>应用控制与审计>Web 访问审计**”，进入 **Web 访问审计**页面，点击<**新建**>创建新的 Web 访问模板，点击控制规则里的<**新建**>创建控制规则。



返回 **Web 访问审计**页面，“操作”列点击图标编辑已有 Web 访问审计数据（规则内容）。也可以点击复制 Web 访问审计数据。

Web 访问审计配置项及相关参数详细说明如下：

配置项	说明
启用	配置开启 Web 访问审计。
URL 类型	配置 Web 访问审计匹配 URL 的类型，可选预定义 URL 分类自定义 URL 分类。
文件类型	配置 Web 访问审计匹配的自定义文件类型。
网页关键字	配置 Web 访问审计匹配的自定义关键字。
动作	为以上匹配规则选择“允许”或“拒绝”。
日志级别	为以上审计内容的设定日志级别，支持 7 种日志级别：紧急、告警、严重、错误、警示、通知、信息。
时间表	配置 Web 访问审计匹配的自定义时间，默认是”always”任意时间。
确定	提交 Web 访问审计配置。

在 Web 访问模板里，勾选具体规则列，点击 上移 下移 按钮可以对具体规则顺序进行上移和下移，点击 启用 禁用 按钮可以对规则进行开启和关闭，勾选多个规则列，点击 删除 按钮可以对勾选规则列进行删除。

4.3.4. 白名单

应用控制与审计支持用户 IP 地址白名单和 URL 白名单，符合白名单的 IP 地址用户或被访

问的 URL 地址，将不再进行应用控制和审计。

4.3.4.1. 白名单

在系统菜单点击“策略>应用控制与审计>白名单>白名单”，进入白名单配置页签。

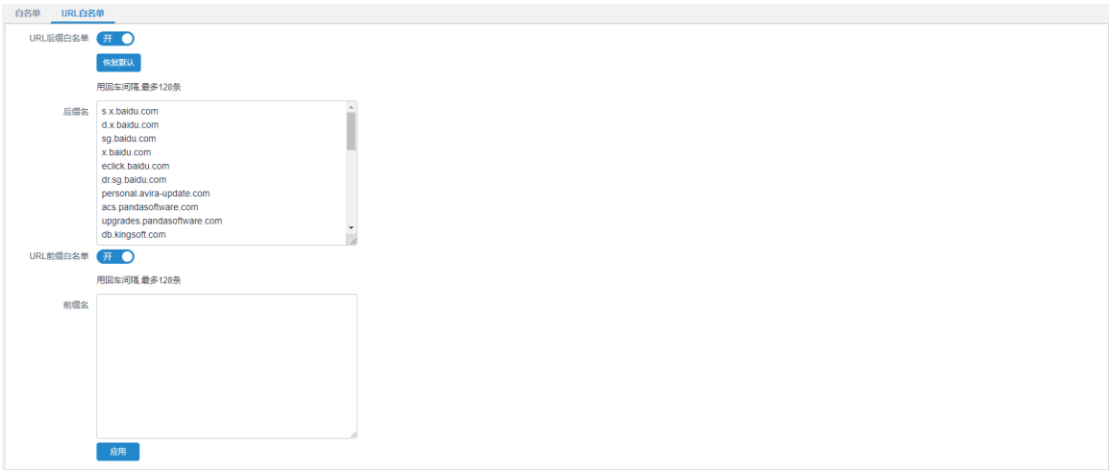
在白名单页签，点击<新建>创建新的白名单。

白名单配置项及详细说明如下：

配置项	说明
用户	白名单用户，默认为 any，点击下拉列表可选择用户组。点击<添加>可创建用户。
地址	白名单生效地址对象，默认为 any，点击下拉列表可选择地址对象。点击<添加>可创建地址。

4.3.4.2. URL 白名单

在系统菜单点击“策略>应用控制与审计>白名单>URL 白名单”，进入 URL 白名单配置页签。



URL 白名单配置项及详细说明如下：

配置项	说明
URL 后缀白名单	启用或禁用 URL 后缀白名单。
后缀名	自定义 URL 后缀白名单，最多可以支持 128 条。
恢复默认	恢复为默认的 URL 后缀白名单。
URL 前缀白名单	启动或禁用 URL 前缀白名单。
前缀名	自定义 URL 前缀白名单，最多可以支持 128 条。

4.4. 入侵防护

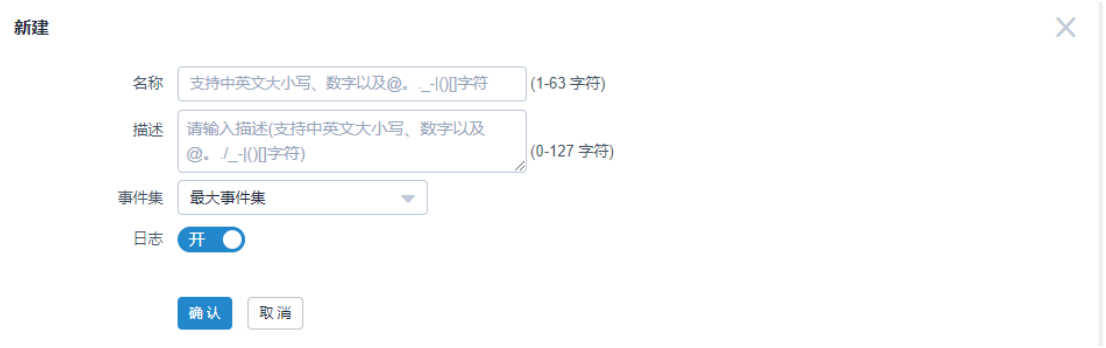
下一代防火墙支持入侵防护功能，支持对常见入侵事件进行检测和防护，也可根据用户自定义协议事件进行检测和防护。入侵防护征库可定期升级，升级方式请参考“升级与重启”。

入侵防护功能作为策略模板，需要被一体化策略引用才能生效，配置请参考“防火墙策略”。

4.4.1. 入侵防护模板

在系统菜单点击“**策略>入侵防护>入侵防护模板**”，进入**入侵防护模板**页面。

点击<**新建**>创建新的入侵防护策略，或点击右侧“操作”列图标编辑已有入侵防护模板，也可以点击复制入侵防护策略。



配置项	说明
名称	入侵防护模板名称。
描述	对入侵防护模板的描述。
事件集	选择入侵防护模板要引用的事件集。
日志	开关按钮，按钮状态切换为开时，触发入侵防护模板会产生日志，日志产生后，可通过菜单进入“**日志>入侵防护日志**”查看日志详细内容。

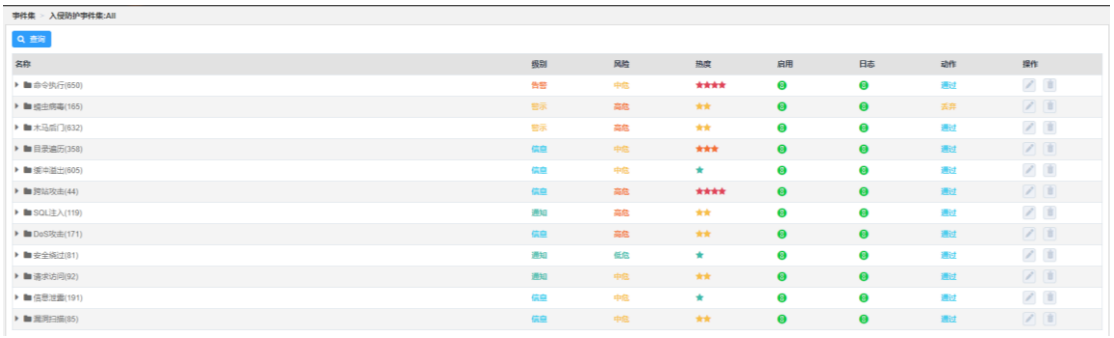
4.4.2. 事件集

事件集用于设定对哪些事件进行攻击检测。当开启了入侵防护功能后，用户的流量会与事件集中的攻击特征做匹配，若能匹配成功则认为是入侵攻击流量，攻击流量会根据策略配置的动作处理。

在系统菜单点击“**策略>入侵防护>事件集**”，进入**事件集**配置页面，可查看当前系统中存在的所有入侵防护事件合集，系统默认提供最大、常规、应用及攻击四种事件集。默认事件集

不允许删除，不支持用户修改默认事件集中内容，默认事件集仅支持修改防护级别，自定义事件集如被引用，不支持删除。点击对应事件集按钮，可查看当前事件集中包含的全部事件组及详细信息。

事件集中详细事件组如下：



在事件集页面通过点击<**新建**>按钮可创建事件集，或点击右侧操作列的按钮，对事件组进行编辑。

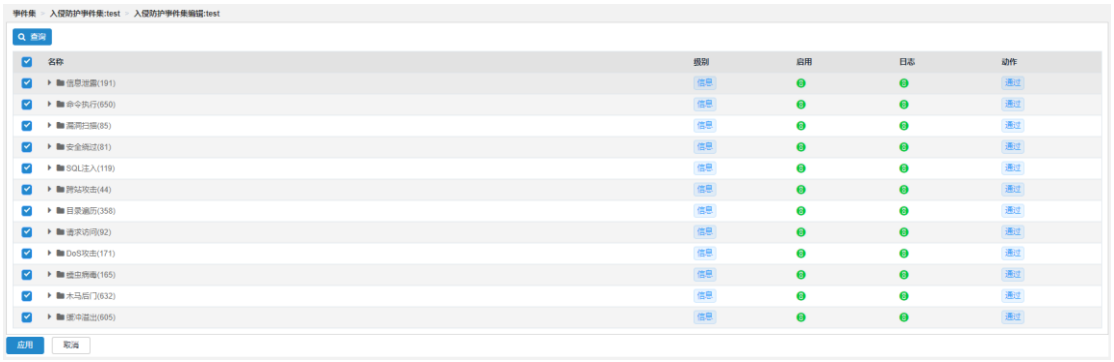
事件集的配置项与详细说明如下：

配置项	说明
名称	事件集名称。

描述	对事件集的描述。
防护级别	事件集的防护级别，分为低、中、高三个等级。

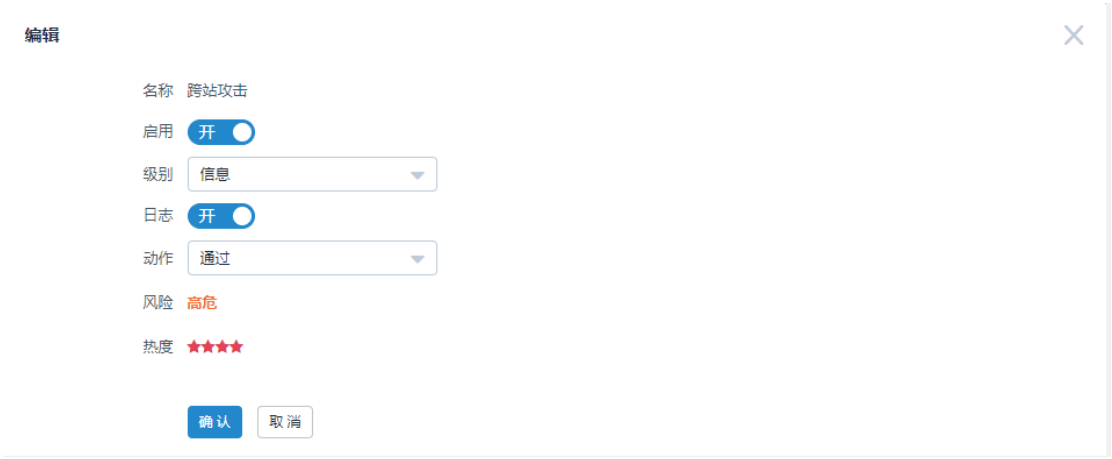
创建事件集成功后，会自动跳转至新增事件集目录下，点击<**添加**>按钮，可选择需要增加的事件组。

通过勾选复选框，选择需要添加到事件集中的防护事件，点击下方<**确认**>按钮可保存当前选择的内容。



编辑事件组/安全事件：新建事件集并选择事件组后，可根据需求对当前事件集内拥有的事件组或安全事件进行编辑。

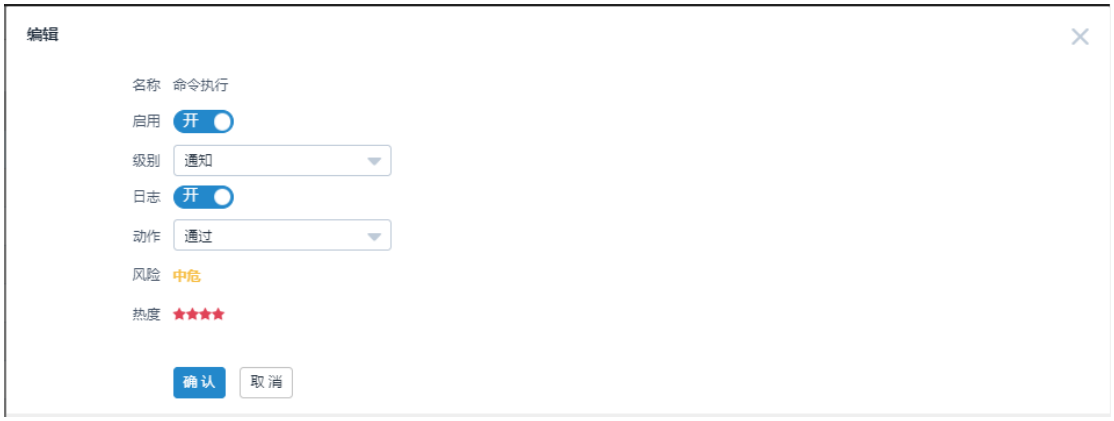
在事件集目录下，点击事件集右侧按钮，进行到事件组页面，点击右侧按钮，对事件组进行编辑。



事件组的配置项与详细说明如下：

配置项	说明
名称	展示当前正在编辑的事件组名，不允许编辑。
启用	开关按钮，按钮状态切换为开时，事件组被启用。
级别	当前事件组被触发后，上报的日志级别，分为信息、通知、警示及告警四个等级。
日志	开关按钮，按钮状态切换为开时，触发事件组会产生日志，日志产生后，可通过菜单进入“**日志>入侵防护日志**”查看日志详细内容。
动作	事件组被触发后，要执行的动作，包括通过、重置、丢弃、阻断会话及阻断源地址五种。
风险	展示当前事件组内事件的平均危险等级，仅作展示，不允许更改。
热度	展示当前事件组内事件被触发的平均可能性，仅作展示，不允许更改。

在自定义事件集目录下，点击事件集右侧按钮，进入自定义事件组，点击自定义事件组名称前的按钮展开事件组，查看组内具体事件，点击具体事件右侧按钮，可对单个事件进行编辑。



4.4.3. IPS 自定义规则

下一代防火墙支持用户自定义 IPS 规则，基于报文的协议类型、协议字段、字段内容设置匹配条件，对匹配到规则的报文执行允许或拒绝操作，实现入侵防御。

在系统菜单点击“**策略>入侵防护>IPS 自定义规则**”，进入 **IPS 自定义规则**页面，显示设备上配置的所有 IPS 自定义规则，在该页面可以对 IPS 自定义规格进行新建、查看、修改、删除、导入和导出。

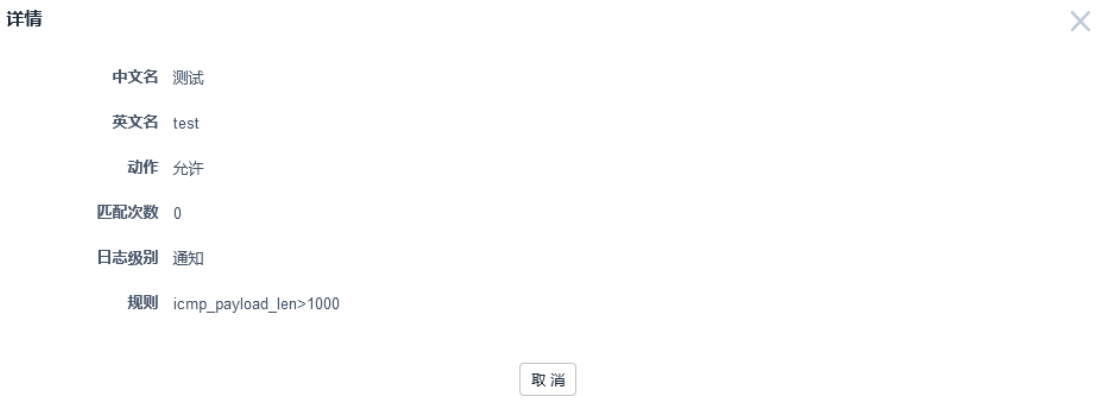
在 **IPS 自定义规则**页面点击<**新建**>创建新的 IPS 自定义规则，或在右侧“操作”列点击图标修改已有的 IPS 自定义规则。

IPS 自定义规则配置项及详细说明如下：

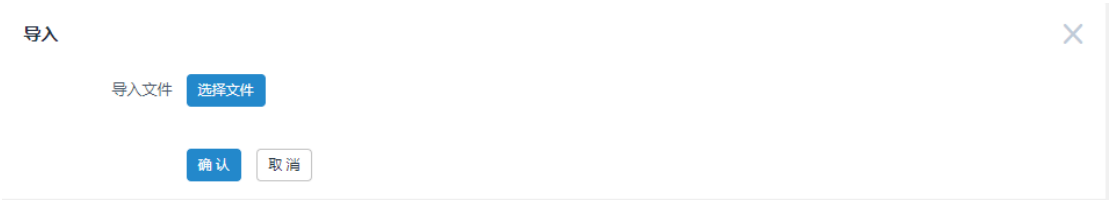
配置项	说明

中文名	配置自定义IPS规则的中文名。
英文名	配置自定义 IPS 规则的英文名。
动作	选择对命中该条规则报文所执行的动作，包括允许和拒绝。
日志级别	选择命中规则后所生成的日志级别，包括信息、通知、警示和告警 4 个级别。
协议类型	选择规则所匹配的报文协议类型。目前设备支持对 IP、UDP、TCP、ICMP、ICMPv6、HTTP、FTP 等 7 种协议类型进行匹配，每种协议类型的具体匹配内容各不相同，请以产品实际界面的选项为准。
协议字段配置	每个协议字段可以包含最多 5 个匹配条件，，配置内容长度 1-256 字符匹配条件之间逻辑关系为“或”和“与”。

在 **IPS 自定义规则**页面选中某一个 IPS 自定义规则点击，在弹出的页面可以查看 IPS 自定义规则的详细信息。



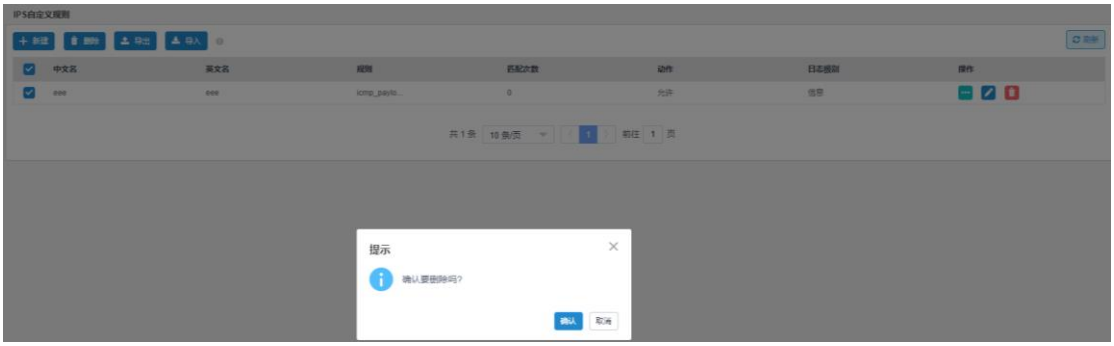
在 **IPS 自定义规则**页面点击<**导入**>，在弹出的页面选择 IPS 自定义规则配置文件，可以实现 IPS 自定义规则的导入。



在 **IPS 自定义规则**页面点击<**导出**>，在弹出的页面点击保存，可以实现 IPS 自定义规则的导

出。

在 IPS 自定义规则页面选中某一个选中要删除的 IPS 自定义规则，点击<删除>或者点击规则后图标，在弹出界面点击确定可以实现 IPS 自定义规则的删除。



提示：

对自定义 IPS 规则最后一次修改 5min 后生效。

4.4.4. 设备联动

下一代防火墙支持设备联动功能，可以添加联动设备，将本设备检测出的入侵事件源 IP 地址，自动添加到联动设备的黑名单列表中。本功能需要联动设备支持对应功能接口。

在系统菜单点击“策略>入侵防护>设备联动”，进入设备联动配置页面，可看到设备联动开关，默认设备联动开关为关闭状态，需要点击按钮，将按钮置为状态，才可添加配置，增加配置完成后，点击<确认>按钮即可保存配置。

设备联动的配置项与详细说明如下：

配置项	说明
启用	启用后可添加配置，且功能生效。
IP 地址	联动设备的 IP 地址。
端口	联动功能所用端口号。
用户名	联动设备登陆所用的用户名。
密码	联动设备登陆所用密码。

4.4.5. 日志合并

当具有相同源目 IP 的攻击在短时间内大量产生，日志数量会迅速增大，且频繁更新，不利于管理/运维人员监控。日志合并功能可将一定时间内，符合一定要求的日志进行合并，规避了上述问题的产生。

在系统菜单点击“**策略>入侵防护>日志合并**”，进入**日志合并**配置页面，可查看到日志合并功能全部配置内容。

开启日志合并：点击按钮，将按钮置为状态；根据需求选择合并选项及合并间隔，点击确认按钮保存配置。

日志合并的配置项与详细说明如下：

配置项	说明
启用	启用后可添加配置，且功能生效。
合并选项	单选框，可选内容包括源地址，目的地址，源目的地址三种，攻击日志会根据所选条件进行合并。
合并间隔	单选框，可选内容包括三十秒，一分钟，五分钟三种，用于决定合并多长时间内符合条件的日志。

4.5. 病毒防护

下一代防火墙支持病毒检测防护，支持对常用协议类型（HTTP、FTP、IMAP、SMTP、POP3）进行病毒扫描及防护，也可指定文件类型和自定义文件类型对病毒进行扫描和防护。

在系统菜单点击“**对象>防护配置模板>病毒防护**”，点击可查看设备支持的病毒数量。病毒特征库可定期升级，升级方式请参考“升级与重启”。

病毒防护功能作为策略模板，需要被一体化策略引用才能生效，配置请参考“防火墙策略”。

4.5.1. 病毒防护模板

在系统菜单点击“**策略**>**病毒防护**>**病毒防护模板**”，进入**病毒防护模板**配置页面，点击<**新建**>创建新的病毒防护策略。

返回病毒防护模板页面，右侧“操作”列点击图标编辑已有病毒防护策略的描述、事件集、日志内容。也可以点击复制病毒防护策略。

病毒防护配置项及详细说明如下：

配置项	说明
名称	支持中英文大小写、数字以及部分的特殊字符，长度范围 1-63 字符。
描述	支持中英文大小写、数字以及部分的特殊字符，长度范围 0-127 字符。
沙箱检测	支持第三方沙箱服务器启用和关闭，点击沙箱配置进入沙箱配置页面，详细配置（参考“策略>病毒防护>病毒沙箱配置”配置）。
协议	支持 HTTP、FTP、SMTP、IMAP、POP3 五种协议。
动作	匹配规则后选择“通过”或“阻断”。
确认	提交病毒防护策略的配置。

4.5.2. 扫描文件设定

默认扫描文件不开启，我们能够对启用的文件类型的病毒文件进行扫描，提高效率。开启扫描所有文件，除文件类型支持之外的病毒类型，也可进行扫描，开启 tar 文件扫描可能会影响性能。

4.5.2.1. 扫描文件设定

在系统菜单点击“策略>病毒防护>扫描文件设定>扫描文件设定”，进入扫描文件设定配置页签。

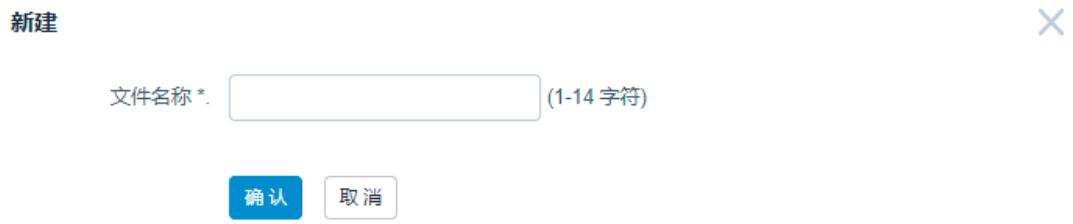
扫描文件配置项及详细说明如下：

配置项	说明
扫描文件	启用扫描所有文件，即对所有文件进行病毒扫描。

4.5.2.2. 文件类型

在系统菜单点击“策略>病毒防护>扫描文件>文件类型”，进入文件类型配置页签。可以新建指定的文件类型，也可以通过启用/禁用扫描列表项对指定文件类型进行病毒扫描。

点击<新建>创建新的文件类型



文件类型显示配置项及详细说明如下：

配置项	说明
文件名称	新建指定的文件类型。
启用	启用/禁用扫描列表项对指定文件类型进行病毒扫描。
操作	新建的文件类型可以进行删除操作

4.5.3. 病毒白名单

白名单就是指允许访问或者允许通过的文件 MD5 值名单，如果设立了白名单，则在白名单中的 MD5 值相同的文件，不会被识别为病毒，认为是安全的。

在系统菜单栏点击“**策略>病毒防护>病毒白名单**”，进入**病毒白名单**配置页面，配置如下：

点击<**新建**>新建病毒白名单，或在右侧“操作”列点击图标编辑修改已有的文件 MD5 值。

4.5.4. 病毒沙箱配置

系统支持与专用沙箱(Sandbox)系统进行联动，沙箱技术可以更为有效地帮助企业防御 APT 攻击，为一些不可靠的程序提供试验而不影响系统运行的环境，有时也被称作沙盒。

在系统菜单栏点击“**策略>病毒防护>病毒沙箱配置**”，进入**病毒沙箱配置**页面，配置如下：

沙箱配置项及详细说明如下：

配置项	说明
启用	是否启用沙箱检测。
服务器（主）	与主服务器联动的通讯地址（威胁检测服务器），如果配置域名，需要在防火墙上配置 DNS 服务器（参考“系统>系统设置>DNS”配置），保证防火墙与 DNS 服务器通讯正常。
服务器（备）	与备服务器联动的通讯地址（威胁检测服务器）。
端口	与服务器联动时目的主机端口。

4.6. 其他防护

下一代防火墙还支持对 APP 防护、DOS 防护、防暴力破解等常见网络攻击，通过检测这些网络攻击报文特征和流量行为，进行告警提示以及阻断攻击行为，保护用户网络资源安全。

4.6.1. ARP 防护

ARP（Address Resolution Protocol）即地址解析协议，是根据 IP 地址获取物理地址的一个 TCP/IP 协议。ARP 协议是 TCP/IP 协议集的数据链路层协议，主要用于在局域网环境下，IP 地址到网络设备的物理地址（MAC）的转换。作为 TCP/IP 协议栈中的一个重要成

员，其设计同样是建立在局域网内各计算机相互信任的基础之上的。由于种种原因，ARP 协议在设计之初，仅处于对传输效率的考虑，而缺乏必要的身份认证和鉴别机制，导致其具有相当脆弱的安全性能。ARP 攻击是一种典型的欺骗类型，其实质就是利用了 ARP 协议本身的安全缺陷和漏洞来进行攻击的。

ARP 攻击可以简单分为两类：

1. ARP 欺骗攻击，攻击和通过伪造 IP 和 MAC 地址实现 ARP 欺骗。

2. ARP 泛洪（Flood），攻击者伪造大量 ARP 报文在同网段内进行广播，导致网关 ARP 表项被占满，合法用户的 ARP 无法正常学习，导致合法用户无法正常访问外网。

下一代防火墙的 ARP 防护功能可以有效识别 ARP 欺骗攻击和 ARP Flood 攻击，配合 ARP 绑定、接口限速、学习控制等措施，有效防范 ARP 攻击造成对的危害。

4.6.1.1. ARP 欺骗防护

在系统菜单点击“**策略>其他防护>ARP 防护>ARP 欺骗防护**”，进入 **ARP 欺骗防护**配置页签。

ARP 欺骗防护配置项及详细说明如下：

配置项	说明
报文有效性检查	开启此功能后，对于源 MAC 地址和以太网报文头中的源 MAC 地址不一致、ARP 应答报文中的目的 MAC 为全 0、全 1 或和以太网报文头中的目的 MAC 地址不一致、ARP 报文中的源目 IP 地址为全 0、全 1 或者组播 IP 地址的 ARP 报文丢弃。对应有日志产生，可通过“**日志>安全日志**”查看。
用户合法性检查	开启用户合法性检查后，只要是不匹配 ARP 绑定表的报文都将被丢弃。有关 ARP 绑定配置的更多信息，请参考 ARP 绑定。对应有日志产生，可通过“**日志>安全日志**”查看。

DHCP 窥探	DHCP 窥探开启后，设备会监听 DHCP-REQUEST 报文，DHCP-ACK 报文记录到 DHCP-SNOOPINGBIND 表中，发送 ARP 报文会对比此表中信息，不一致报文丢弃。对应有日志产生，可通过“**日志>安全日志**”查看。
ARP 网关保护	● **接口**-选择保护接口。 ● **网关地址**-添加需要保护的网关 IP 地址。 接口配置网关保护后，收到 ARP 报文如源 IP 为此接口保护 IP，丢弃报文，不学习 ARP；对应有日志产生，可通过“**日志>安全日志**”查看。

4.6.1.2. ARP Flood 防护

在系统菜单点击“**策略>其他防护>ARP 防护>ARP Flood 防护**”，进入 **ARP Flood 防护**配置页签。

ARP Flood 防护配置项及详细说明如下：

配置项	说明
ARP 报文源 MAC 限制速率	设置每秒钟基于源 MAC 收到的 ARP 报文数量阈值，可输入范围为 1-10000，超过该值将会认定发生了 ARP Flood 攻击。对应有日志产生，可通过“**日志>安全日志**”查看。
ARP 报文接口限制速率	设置每秒钟基于接口收到的 ARP 报文数量阈值，可输入范围为 1-10000，超过该值将会认定发生了 ARP Flood 攻击。对应有日志产生，可通过“**日志>安全日志**”查看。
保护 MAC 白名单	设置不用限制速率的源 MAC 加入白名单。

提示：

同时配置源 MAC 和接口限速时，判断收到的 ARP 报文的源 MAC 是否为信任 MAC（信任 MAC 是 ARP 绑定表、DHCP-Snooping 表、ARP 表中已存在的），是信任 MAC 基于源 MAC 限速，非信任 MAC 基于接口限速。

4.6.1.3. ARP 学习控制

在系统菜单点击“**策略>其他防护>ARP 防护>ARP 学习控制**”，进入 **ARP 学习控制**配置页签。

ARP 学习控制配置项及详细说明如下：

配置项	说明
ARP 表项修改保持	开启此开关后，收到需要修改已有的 ARP 报文信息时在 10s 内不会进行修改。
ARP 表项主动确认	开启此功能时，收到如与已有的信息不同需要修改的 ARP 报文，会进行主动确认机制，发一条单播的请求报文，在 10s 内收到单播回复为正常报文，否则不修改 ARP 表。
ARP 表项动态配额	配置动态配额后，配置接口被动学习表项超过所设置数量后，将不再学习，丢掉收到的 ARP 报文；对应有日志产生，可通过“**日志>安全日志**”查看。 ● **接口**-选择需要配置 ARP 学习控制的接口。 ● **动态配额**-配置学习范围，可下发范围为 0-10000；当配置为 0 时，只可主动学习，被动学习失败。

提示：

统计的为被动学习表项的数量，不会统计本机主动学习的表项数量。

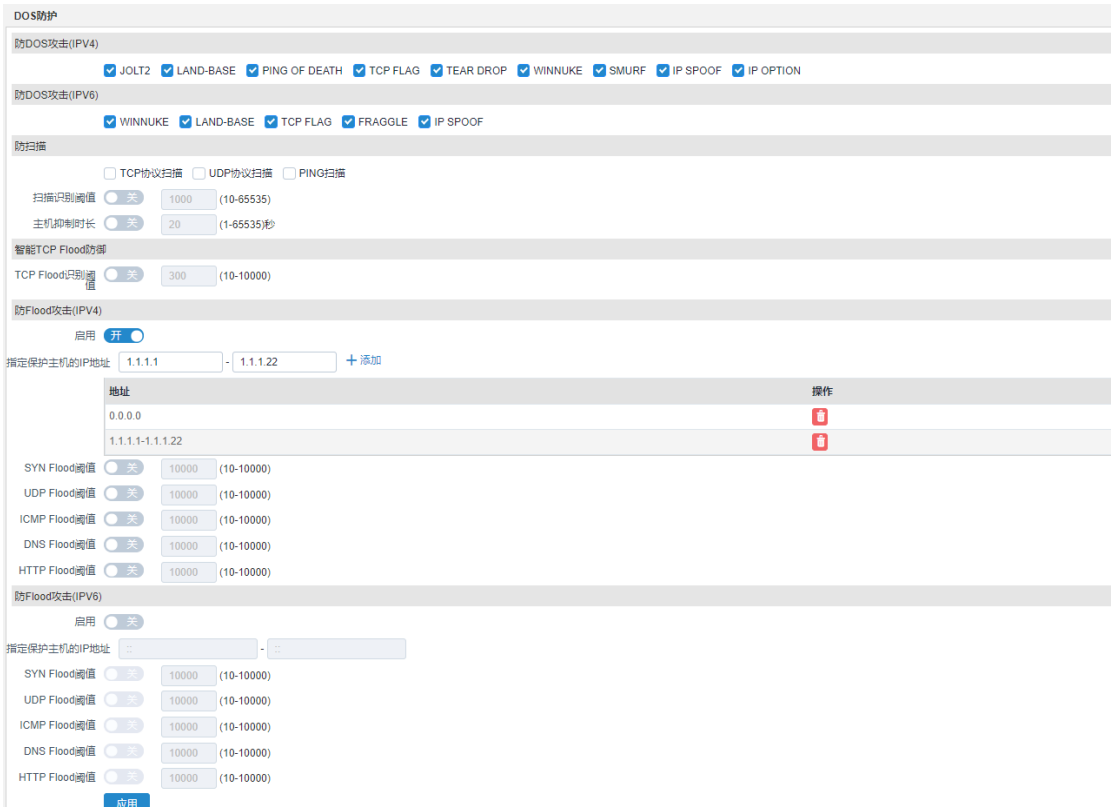
4.6.2. DOS 防护

防 DOS(Denial of Service)攻击设计的目标就是要使设备能够阻止外部的恶意攻击，同时还能使内网正常地与外界通信。不仅保护设备，更要保护内网。当遭受到攻击时，向用户进行报警提示。

4.6.2.1. 防 DOS 攻击

异常包攻击是一种常见的单包攻击，这类攻击虽然破坏力强大，但是只要掌握了攻击的特性，就可以对这些报文（包含 IPv4 与 IPv6 报文）进行拦截并产生告警日志提示。常见的异常攻击主要包括 JOLT2、LAND-BASE、PING OF DEATH、TCP-FLAG、TEAR DROP、WINNUKE、SMURF、IP SPOOF、IP OPTION、FRAGGLE 等。下一代防火墙设备通过检查报文中的攻击行为特征，可以支持对异常包攻击进行有效的防御。

在系统菜单点击“**策略>其他防护>DOS 防护**”，进入 **DOS 防护**配置页面，勾选“**防 DOS 攻击(IPV4)**”和“**防 DOS 攻击(IPV6)**”功能项下对应需要阻断的异常包类型（默认关闭），选择完成后请在此页页底点击<**确认**>，使配置生效。



防 DOS 攻击（IPV4/IPV6）的配置项详细说明如下 ：

配置项	说明
JOLT2	通过向目的主机发送报文偏移加上报文长度超过 65535 的报文，使目的主机处理异常而崩溃。 配置了防 JOLT2 攻击功能后，设备可以检测出 JOLT2 攻击，丢弃攻击报文、将攻击者加入黑名单并根据配置输出告警日志信息。
LAND-BASE	通过向目的主机发送目的地址和源地址相同的报文，使目的主机消耗大量的系统资源，从而造成系统崩溃或死机。 配置了防 LAND-BASE 攻击功能后，设备可以检测出 LAND-BASE 攻击，丢弃攻击报文、将攻击者加入黑名单并根据配置输出告警日志信息。
PING OF DEATH	通过向目的主机发送长度超过 65535 的 ICMP 报文，使目的主机发生处理异常而崩溃。 配置了防 PING OF DEATH 攻击功能后，设备可以检测出 PING OF DEATH 攻击，丢弃攻击报文、将攻击者加入黑名单并根据配置输出告警日志信息。
TCP FLAG	通过向目的主机发送错误的 TCP 标识组合报文，浪费目的主机资源。 配置了防 TCP FLAG 攻击功能后，设备可以检测出 TCP FLAG 攻击，丢弃攻击报文、将攻击者加入黑名单并根据配置输出告警日志信息。
TEAR DROP	通过向目的主机发送报文偏移重叠的分片报文，使目的主机发生处理异常而崩溃。 配置了防 TEAR DROP 攻击功能后，设备可以检测出 TEAR DROP 攻击，丢弃攻击报文、将攻击者加入黑名单并根据配置输出告警日志信息。
WINNUKE	通过向目的主机的 139、138、137、113 端口发送 TCP 紧急标识位 URG 为 1 的带外数据报文，使系统处理异常而崩溃。 配置了防 WINNUKE 攻击功能后，设备可以检测出 WINNUKE 攻击，丢弃攻击报文、将攻击者加入黑名单并根据配置输出告警日志信息。
SMURF	通过使用将回复地址设置成受害网络的广播地址的 ICMP 应答请求

	(PING)数据包，来淹没受害主机，最终导致该网络的所有主机都对此 ICMP 应答请求做出答复，导致网络阻塞。 配置了防 SMURF 攻击功能后，设备可以检测出 SMURF 攻击，丢弃攻击报文、将攻击者加入黑名单并根据配置输出告警日志信息。
IP SPOOF	防护 IP 地址欺骗攻击，暂时用反向路由过滤来实现，如果反向路由不存在或者反向路由查询结果是存在，但是该 IP 为目的地址的数据包离开设备的接口和收到报文的接口不一致，则认为是攻击。 配置了防 SMURF 攻击功能后，设备可以检测出 SMURF 攻击，丢弃攻击报文并根据配置输出告警日志信息。
IP OPTION	攻击者检查 IP 包中的选项域，使用这个规则选项搜索 IP 包头的特定选项（例如源路由），利用可信用户对服务器进行攻击。由于 UDP 协议 面向非连接，因此更容易被利用 配置了防 IP OPTION 攻击功能后，设备可以检测出 IP OPTION 攻击，丢弃攻击报文、将攻击者加入黑名单并根据配置输出告警日志信息。
FRAGGLE	攻击者可以向攻击目标所在的网络发送 UDP 报文，报文的源地址为被攻击主机的地址，目的地址为被攻击主机所在子网的广播地址或子网网络地址，目的端口号为 7 或 19。子网中启用了此功能的每个系统都会向被攻击主机发送回应报文，从而产生大量的流量，占满带宽，导致受害网络的阻塞或受害主机的崩溃。 即使子网上没有启动这些功能的系统也将产生一个 ICMP 不可达消息，因而仍然消耗带宽。若攻击者将 UDP 报文的源端口改为 19，目的端口为 7，这样会不停地产生大量回应报文，其危害性更大。 配置了防 FRAGGLE 攻击功能后，设备可以检测出 FRAGGLE 攻击，丢弃攻击报文、将攻击者加入黑名单并根据配置输出告警日志信息。

4.6.2.2. 防扫描

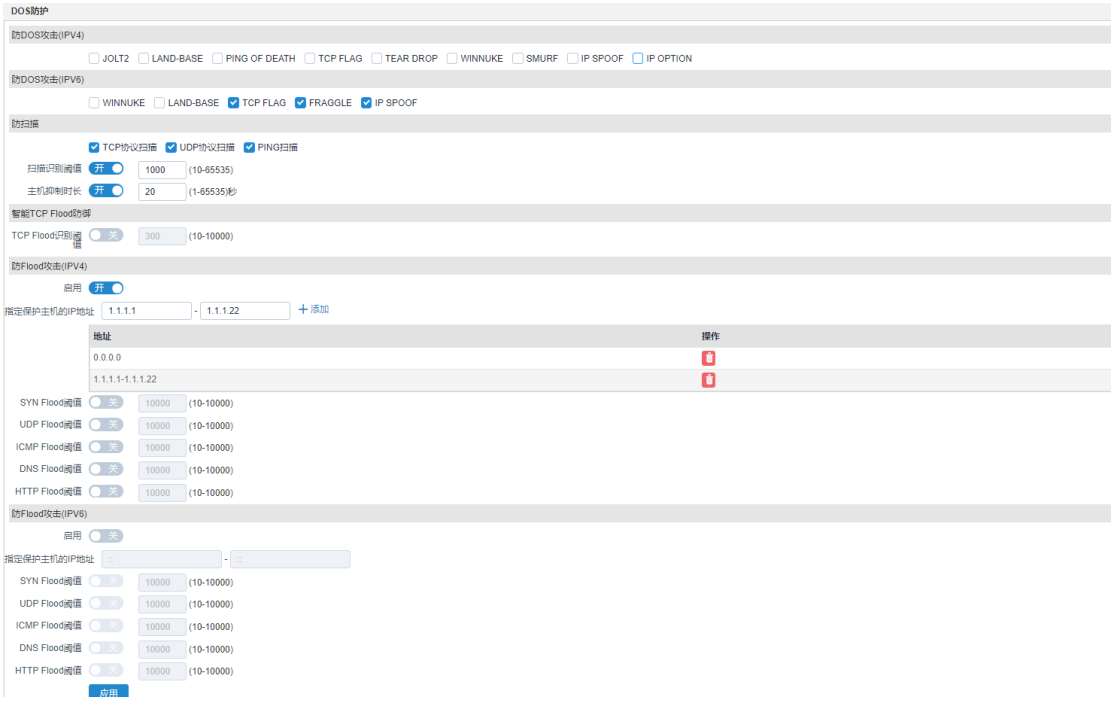
扫描也是网络攻击的一种，攻击者在发起网络攻击之前，攻击者通过对 IP 地址进行扫描探测网络结构，以确定攻击目标，也可通过对端口进行扫描探测网络结构，以确定攻击目标，而一个开放的端口通常意味着某种应用。

常见的扫描主要有：

- TCP 协议扫描：攻击者通过对 TCP 端口进行扫描探测网络结构，以确定攻击目标。
- UDP 协议扫描：攻击者通过对 UDP 端口进行扫描探测网络结构，以确定攻击目标。
- PING 扫描：攻击者通过对 IP 地址进行扫描探测网络结构，以确定攻击目标。

下一代防火墙设备可以有效防范以上几类扫描，从而阻止外部的恶意攻击，保护设备和内网。当检测到此类扫描探测时，向用户进行报警提示并根据配置判断是否将该攻击者源 IP 加入黑名单。

在系统菜单点击“**策略>其他防护>DOS 防护**”，进入 **DOS 防护**配置页面，勾选“**防扫描**”功能项下对应需要防护的扫描行为，并设置扫描识别阈值、主机抑制时长， 选择完成后请在此页页底点击<**确认**>，使配置生效。



防扫描的配置项及详细说明如下：

配置项	说明
TCP 协议扫描	根据实际网络情况，当受到 TCP 扫描攻击时，勾选复选框启用 TCP 协议扫描防护，可以配置防 TCP 扫描。 当一个源 IP 地址在 1 秒内将含有 TCP SYN 片段的 IP 封包发送给位于相同目标 IP 地址的不同端口数量大于配置的阈值时，即认为其进行了端口扫描，系统将其标记为 TCP SCAN，并在配置的阻断时间内

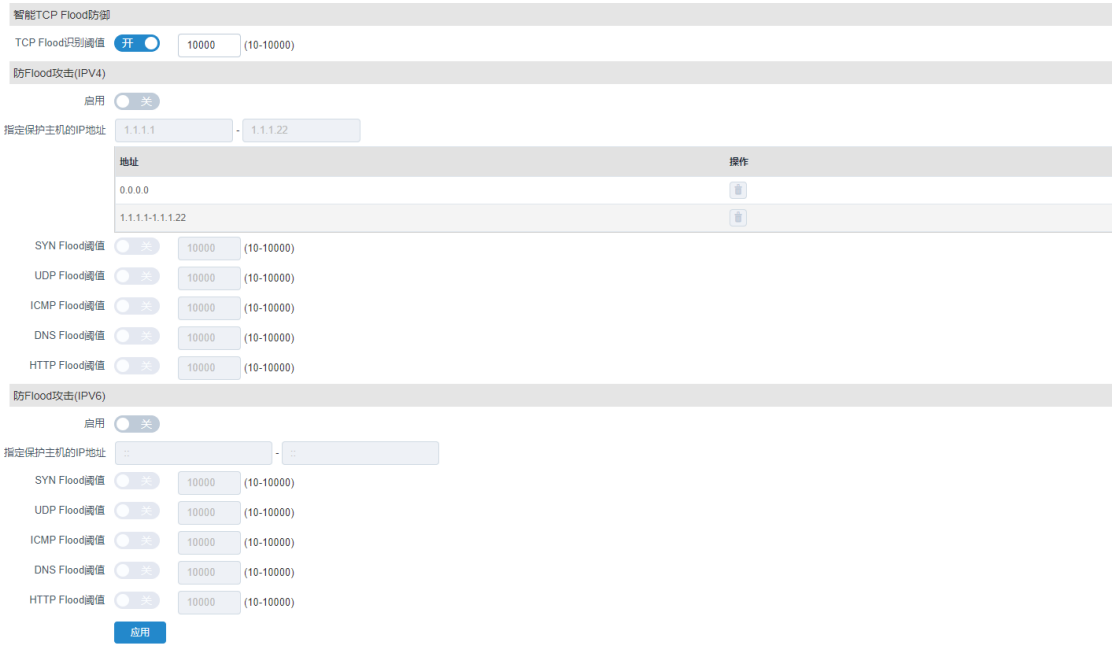
	拒绝来自于该台源主机的所有其它 TCP SYN 包。 启用防 TCP 扫描，可能会占用比较多的内存。
UDP 协议扫描	根据实际网络情况，当受到 UDP 扫描攻击时，勾选复选框启用 UDP 协议扫描防护，可以配置防 UDP SCAN 扫描。 当一个源 IP 地址在 1 秒内将含有 UDP 的 IP 封包发送给位于相同目标 IP 地址的不同端口数量大于配置的阈值时，即进行了一次端口扫描，系统将其标记为 UDP SCAN，并在配置的阻断时间内拒绝来自于该台源主机的所有其它 UDP 包。 启用防 UDP 扫描，可能会占用比较多的内存。
PING 扫描	根据实际网络情况，当受到 PING 扫描攻击时，勾选复选框启用 PING 扫描防护，可以配置防 PING 扫描。 当一个源 IP 地址在 1 秒内发送给不同主机的 ICMP 封包超过门限值时，即进行了一次地址扫描。此方案的目的是将 ICMP 封包（通常是应答请求）发送给各个主机，以期获得至少一个回复，从而查明目标地址。下一代防火墙设备在内部记录从某一远程源地点发往不同地址的 ICMP 封包数目。当某个源 IP 被标记为地址扫描攻击，则系统在配置的阻断时间内拒绝来自该主机的其它更多 ICMP 封包。 启用防 PING 扫描，可能会占用比较多的内存。
扫描识别阈值	防扫描功能的扫描识别门限，超过阈值时，该源 IP 被标记为扫描攻击，来自于该台源主机的所有其它攻击包都被阻断，缺省配置为 1000，选值范围为 10-65535。
主机抑制时长	设置防扫描功能的阻断时间，当系统检测到扫描攻击时，在配置的时长内拒绝来自于该台源主机的所有其它攻击包，缺省配置为 20 秒，选值范围为 1-65535 秒。

4.6.2.3. 防 Flood 攻击

TCP Flood 即 SYN Flood 攻击，是众多 DOS 攻击形式的一种方式。SYN Flood 利用 TCP 协议的缺陷，向服务器端发送大量伪造的 TCP 连接请求之后，自身不再做出应答，使得服务器端的资源迅速耗尽，从而无法及时处理其它正常的服务请求，严重的时候甚至会导致服务器系统的崩溃。

下一代防火墙设备的智能 TCP Flood 防御采用了业界最新的 syncookie 技术，在很少占用系统资源的情况下，可以有效地抵御 SYN Flood 对受保护服务器的攻击。

在系统菜单点击“**策略>其他防护>DOS 防护**”，进入 **DOS 防护**配置页面，开启“**智能 TCP Flood 防御**”功能项并设置对应 TCP Flood 识别阈值，选择完成后请在此页页底点击<**确认**>，使配置生效。



智能 TCP Flood 防御的配置项及详细说明如下：

配置项	说明
TCP Flood 识别阈值	配置 TCP 半连接的阈值，即防 TCP Flood 攻击的启动门限，选值范围为 10-10000。

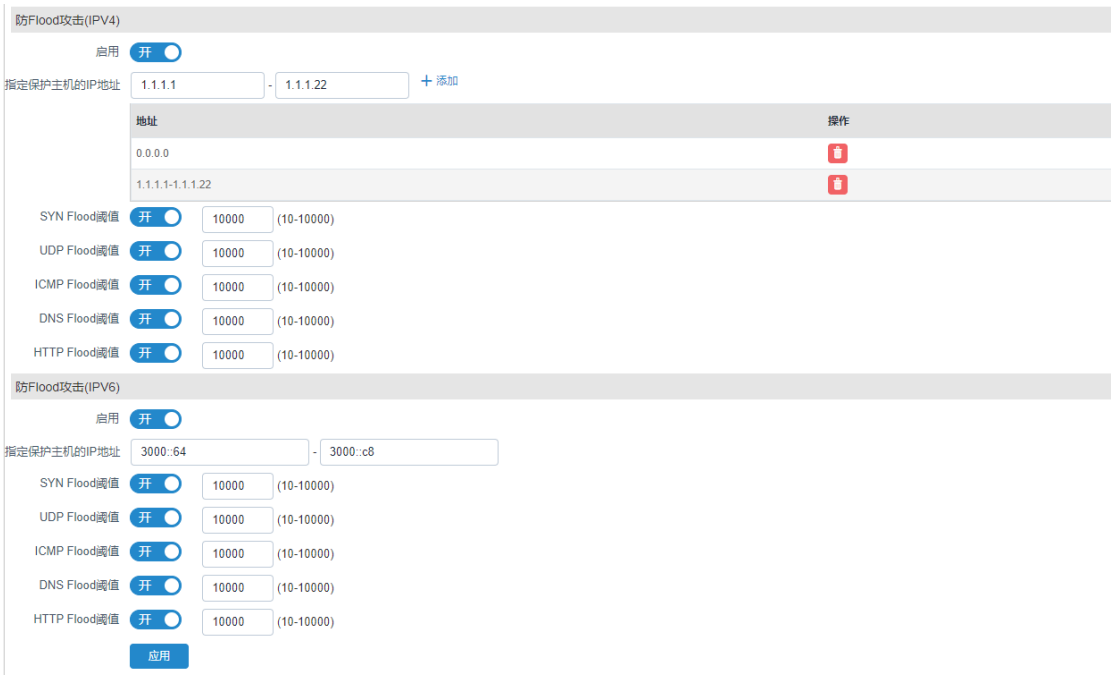
常见的 Flood 攻击（IPv4/IPv6）有以下几类：

- SYN Flood 攻击，由于资源的限制，TCP/IP 协议栈只能允许有限个 TCP 连接。SYN Flood 攻击者向服务器发送伪造源地址的 SYN 报文，服务器在回应 SYN ACK 报文后，由于目的地址是伪造的，因此服务器不会收到相应的 ACK 报文，从而在服务器上产生一个半连接。若攻击者发送大量这样的报文，被攻击服务器上会出现大量的半连接，耗尽其系统资源，使正常的用户无法访问，直到半连接超时。
- ICMP Flood 攻击，ICMP Flood 攻击是指，攻击者在短时间内向特定目标发送大量的 ICMP 请求报文，使其忙于回复这些请求，致使目标系统负担过重而不能处理正常的业

务。

- UDP Flood 攻击，UDP Flood 攻击是指，攻击者在短时间内向特定目标发送大量的 UDP 报文，致使目标系统负担过重而不能处理正常的业务。
- DNS Flood 攻击，向目标 DNS 服务器发送大量伪造的域名（如随机生成或不存在的域名）解析请求，被 攻击的 DNS 服务器在处理这类域名解析请求时会消耗大量资源，导致正常的域名解析服务超时。
- HTTP Flood 攻击，攻击者向目标服务器发送大量的 HTTP 请求报文，这些请求报文中一般都包含设计数据库操作的 URI(Uniform Resource Identifer，统一资源标识符)或其他消耗系统资源的 URI，目的是为了造成目标服务器资源耗尽，无法效应正常请求。

在系统菜单点击“**策略>其他防护>DOS 防护**”，进入 **DOS 防护**配置页面，开启“**防 Flood 攻击(IPV4)**”或“**防 Flood 攻击(IPV6)**”功能项总开关，输入需要保护主机的 IP 地址后点击<**添加**>，选择需要开启的 Flood 功能并设置对应阈值，配置完成后请在此页页底点击<**确认**>，使配置生效。



防 Flood 攻击(IPV4/IPV6)的配置项及详细说明如下：

配置项	说明
指定保护主机的 IP 地址	配置需要被保护的主机的 IP 地址， IPV4 功能输入地址范围

	后需点击<**添加**>按钮，IPV6 功能直接输入地址范围即可，要求输入的地址范围内主机不能超过 65535 个，且不输入保护的 IP 地址，默认不会任何主机进行保护。
SYN Flood 阈值	配置 SYN Flood 的阈值，即防 SYN Flood 攻击的启动门限，默认阈值为 10000，选值范围为 10-10000。
UDP Flood 阈值	配置 UDP Flood 的阈值，即防 UDP Flood 攻击的启动门限，默认阈值为 10000，选值范围为 10-10000。
ICMP Flood 阈值	配置 ICMP Flood 的阈值，即防 ICMP Flood 攻击的启动门限，默认阈值为 10000，选值范围为 10-10000。
DNS Flood 阈值	配置 DNS Flood 的阈值，即防 DNS Flood 攻击的启动门限，默认阈值为 10000，选值范围为 10-10000。
HTTP Flood 阈值	配置 HTTP Flood 的阈值，即防 HTTP Flood 攻击的启动门限，默认阈值为 10000，选值范围为 10-10000。

4.6.3. 防暴力破解

暴力破解也可称为穷举法、枚举法，是一种比较流行的密码破译方法，也就是将密码进行一一推算直到找出正确的密码为止。

多数情况下用户可以通过在网络中部署具有防暴力破解模块防火墙设备来过滤、抑制试图破解密码的流量，设备短时间内收到客户端发起的大量的登录行为后。可以判断为暴力破解密码行为。防暴力破解就是当监测统计到基于 HTTP, FTP,TELNET 等协议的登录攻击行为后，对该攻击行为进行处理，从而避免非法用户破解用户密码，给用户资产带来不可预计的损失。

在系统菜单点击“**策略>其他防护>防暴力破解**”进入**防暴力破解**的配置页面。

提示：

使用防暴力破解功能时需在一体化策略中开启病毒防护配置后方可正常使用。

防暴力破解的配置项及详细说明如下：

配置项	说明
启用	点击启用开关，将状态设置为“开”启用防暴力破解功能。
服务	点击<**添加**>按钮，在弹出页面内选择服务类型及触发阈值。目前设备支持的服务类型包括 TELNET、HTTP、POP3、SMTP、IMAP、FTP、RLOGIN。
攻击者加入黑名单	点击启用开关，将状态设置为“开”启用此功能，会将检测到的暴力破解攻击者加入到黑名单进行阻断。
时间	选择将检测到的暴力破解攻击者加入黑名单进行阻断的时间。

4.7. 威胁情报

随着各种攻击技术和手段的持续提升，传统的安全检测手段对付 APT 攻击严重不足；攻防双方力量不均衡和信息不对称的博弈，都推动着设备厂商从传统的威胁响应方式进化至网络空间的安全解决方案。

下一代防火墙支持威胁情报联动功能，可以实时获取威胁情报，并应用威胁情报对通过的流

量进行威胁检测和防护，准确发现内部失陷主机，结合威胁情报提供的丰富上下文信息，帮助组织挖掘攻击特点、更快地采取安全防范措施。基于大数据关联分析得到的威胁情报可以推动组织快速了解内部的威胁信息，从而帮助企业提前做好安全防范、快速进行攻击检测与响应、更高效的进行事后攻击溯源。

4.7.1. 情报策略

在系统菜单点击“**策略>威胁情报>情报策略**”，进入**情报策略**页面，可以对情报策略类型、信誉值和日志级别进行设置。

情报策略类型配置项及详细说明如下：

配置项	说明
公网 IP	是否禁止访问情报库内公网IP。
DNS 域名	是否禁止访问情报库内域名，表现为解析 DNS 失败。
HTTP URL	是否禁止访问情报库内 HTTP URL，同时不阻断同一域名下其余访问。

情报策略信誉值设置配置项及详细说明如下：

配置项	说明
记录日志	信誉值高于此阈值则记录日志，记录日志的信誉值要配置比拒绝并记录日志的信誉值低，默认信誉值大于 20 记录日志。
拒绝并记录日志	信誉值高于此阈值则阻断并记录日志，默认信誉值大于 80 阻断并记录日志。

情报策略日志级别设置配置项及详细说明如下：

配置项	说明
级别高	设置级别高情报策略的记录日志级别，记录日志级别必须高于级别中和级别低情报策略的记录日志级别，告警级别可选：紧急、告警、严重、错误和警示，默认为警示。
级别中	设置级别中情报策略的记录日志级别，记录日志级别必须高于级别低情报策略的记录日志级别、低于级别高情报策略的记录日志级别，告警级别可选：告警、严重、错误、警示和通知，默认为通知。
级别低	设置级别低情报策略的记录日志级别，记录日志级别必须低于于级别高和级别低的情报策略的记录日志级别，告警级别可选：严重、错误、警示、通知和信息，默认为信息。


提示：

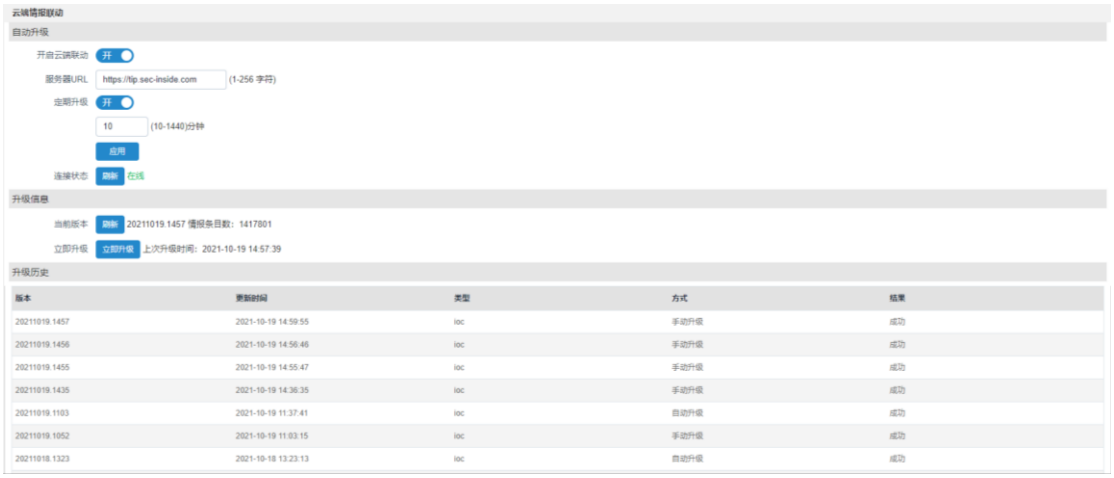
对有带硬盘的设备威胁情报日志在“日志>威胁情报日志”中查看详细信息。

对不带有硬盘的设备威胁情报日志在“日志>安全日志”中查看详细信息。

4.7.2. 云端情报联动

设备支持与云端威胁情报库的联动。开启云端情报联动后，设备可以实时获取威胁情报信息，并应用威胁情报进行威胁检测，准确发现内部失陷主机，更快速进行攻击检测与响应，更高效进行事后攻击溯源。

在系统菜单点击“**策略>威胁情报>云端情报联动**”，进入**云端情报联动**页面，可以对云端情报联动相关参数进行设置。



云端情报联动配置项及详细说明如下：

配置项	说明
开启云端联动	配置开启云端情报联动。
服务器 URL	配置云端情报库的地址，默认为 https://tip.sec-inside.com。
定期升级	配置云端情报库是否定期升级以及定期升级的间隔时间，间隔时间可以配置为 1-60min。
链接状态	显示设备和云端情报库的链接状态。
当前版本	显示当前云端情报库的版本信息以及云端情报库的情报条目数。
检查更新	检测云端情报库是否有版本更新。
立即升级	手动升级云端情报库，并显示最新一次升级时间。

重新注册	重新在云端情报库注册。
升级历史	查看云端情报库升级历史。

4.7.3. 云端情报查询

在系统菜单点击“**策略>威胁情报>云端情报查询**”，进入**云端情报查询**页面，可以对在云端情报库查询特定域名、IP 地址在云端情报库存储的相关信息。

提示：

仅有带硬盘的设备类型支持该功能。

4.7.4. 自定义情报

在系统菜单点击“**策略>威胁情报>自定义情报**”，进入**自定义情报**页面，显示设备上配置的所有自定义情报信息，在该页面可以对自定义情报的新建、删除和查看。

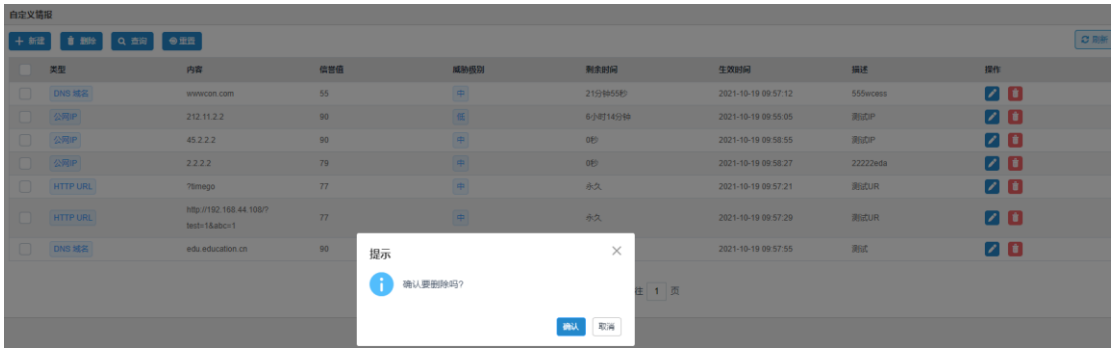
在**自定义情报**页面点击<**新建**>创建新的自定义情报规则，或在右侧“操作”列下点击进入图标修改已有的自定义情报规则。

自定义情报新建配置项及详细说明如下：

配置项	说明
类型	自定义情报类型配置，可选 IP、域名、URL。
信誉值	自定义情报信誉值配置，可配置范围 1-100.

生效时间	自定义情报生效时间配置，可配置范围 1-999min,999 代表永久。
威胁级别	自定义情报威胁级别配置，可选高中低三种，对应产生日志级别。
描述	自定义情报描述信息配置。

在**自定义情报**页面选中想要删除的某一条自定义情报，点击<**删除**>或者点击自定义情报后的图标，在弹出界面点击确定，实现自定义情报的删除。



4.8. 风险扫描

支持对指定的 IP 地址/地址段/子网进行端口扫描和弱密码扫描，可以探测网络资产，发现安全风险，支持查看扫描结果。

4.8.1. 端口扫描

端口扫描功能用来扫描网络电脑开放的网络连接端。确定有哪些服务运行在哪个连接端，以及用以评估网络系统安保；系统管理员可以利用端口扫描来探测工作环境中未经批准使用的服务器。

4.8.1.1. 端口扫描

在系统菜单点击“**策略>风险扫描>端口扫描>端口扫描**”，进入**端口扫描**配置页签。

在**端口扫描**页签，点击<**新建**>创建新的端口扫描任务，在右侧“操作”列点击图标编辑修改已有的端口扫描任务，或在右侧“操作”列点击 图标立即扫描已有任务。

端口扫描任务配置项及详细说明如下：

配置项	说明
名称	配置端口扫描任务名称。1-31 字符支持中英文大小写、数字以及@。.-| () []字符。
描述	配置端口扫描任务描述信息。
类型	支持 IPv4、IPv6 类型选择。
IP 地址类型	支持主机、子网、范围类型选择，IP 地址类型下发输入框输入主机或子网或范围的配置，点击<**添加**>按钮(最大扫描 IP 个数是 500)。
资产发现同步	开启资产发现同步开关。端口扫描结束后在资产管理中可查看到资产记录。
模糊端口	开启端口模糊端口开关。开启后常用端口扫描、自定义端口扫描不

	可选择。
常用端口扫描	下拉列表选择常用端口。共 24 个常用端口选择，可多选，双击取消选中。
自定义端口扫描	开启自定义端口扫描开关。自定义端口输入框输入配置（范围 1-65535，例如 3，5-10）。
扫描类型	支持立即执行、定期执行选择。

提示：

开启资产发现同步，端口扫描到的资产在资产管理中可查看到资产记录。

4.8.1.2. 端口扫描结果

端口扫描结果功能针对端口扫描任务结束的返回结果，主要记录每项任务的开始时间、结束时间、执行结果、扫描结果。

在系统菜单点击“**策略>风险扫描>端口扫描>端口扫描结果**”进入**端口扫描结果**页签。在右侧“操作”列点击 图标可查看扫描结果详细信息，点击 图标删除端口扫描结果，点击 图标下载端口扫描结果到本地。

4.8.2. 弱密码扫描

弱密码扫描是用来扫描网络中服务器或者终端ftp、ssh、telnet、smtp等服务使用的密码是否安全，以及用以评估网络系统安全等级；系统管理员可以利用弱密码扫描来探测工作环境中服务器密码等级，保障网络环境安全。

4.8.2.1. 弱密码扫描

在系统菜单点击“**策略>风险扫描>弱密码扫描>弱密码扫描**”，进入**弱密码扫描**配置页签，查看设备上已有的弱密码扫描任务。

在**弱密码扫描**页签，点击<**新建**>创建新的弱密码扫描任务，或在“操作”列下点击图标修改已有的任务。

提示：

正在执行中的任务无法点击编辑。

弱密码扫描任务配置项及详细说明如下：

配置项	说明
名称	配置弱密码扫描任务的名称，支持中英文大小写、数字以及@。._-|()[]字符,长度范围为 1-31 字符。
描述	配置弱密码扫描任务的描述，支持中英文大小写、数字、空格以及@。./_-|()[]字符,长度范围为 0-127 字符。
类型	选择弱密码扫描目标的类型，可选择 IPv4 或 IPv6 任一类型。
IP 地址类型	设置扫描的目的地址，可以为主机地址或地址段范围，在输入框中输入地址后点击<**添加**>按钮，将其加入配置项数据中。
服务类型	选择扫描的服务（可多选）。目前支持的服务类型包括 ftp、ssh、telnet、smtp、rlogin、imap、pop3、mssql、mysql、postgresql、vnc。
扫描方式	选择一种扫描方式。快速扫描使用相对精简的密码字典文件，全面扫描使用相对全面的密码字典文件，自定义扫描需用户自行选择用户名和密码字典文件。有关字典文件配置的更多信息，请参考字典功能。
空密码检测	开启后检测任务目标地址及服务是否存在空密码的账号。
用户名和密码相同检测	开启后检测任务目标地址及服务是否用户名与密码相同的账号。
扫描类型	选择扫描任务的执行时间，可以是立即执行或在指定的时间开始执行。

4.8.2.2. 弱密码扫描结果

扫描任务完成后可在系统菜单点击“**策略>风险扫描>弱密码扫描>弱密码扫描结果**”，进入**弱密码扫描结果**页签，查看设备上扫描状态完成后对应产生的弱密码扫描结果信息。在右侧“操作”列点击图标可查看扫描结果详细信息，点击图标删除端口扫描结果，点击图标下载端口扫描结果到本地。

4.8.2.3. 字典

在系统菜单点击“**策略>风险扫描>弱密码扫描>字典**”，进入**字典**页签，查看设备上已有的弱密码扫描字典文件。系统内置了一个默认用户名字典与两个密码字典，系统字典无法被修改与删除。

在**字典**页签，点击<**新建**>创建新的自定义字典，或在“操作”列下点击图标修改已有的自定义字典。

字典的配置项及详细说明如下：

配置项	说明
名称	配置自定义字典的名称，支持中英文大小写、数字以及@。._-|()[]字

	符,长度范围为 1-63 字符。
描述	配置自定义字典的描述，支持中英文大小写、数字、空格以及@。./_-|()[]字符,长度范围为 0-127 字符。
字典内容	配置字典内容信息，当字典被弱密码扫描引用后，将对字典内容进行轮询调用，格式要求内容以回车分隔,注意每条内容不能超过 15 个字符,并且不能超过 50 条记录。

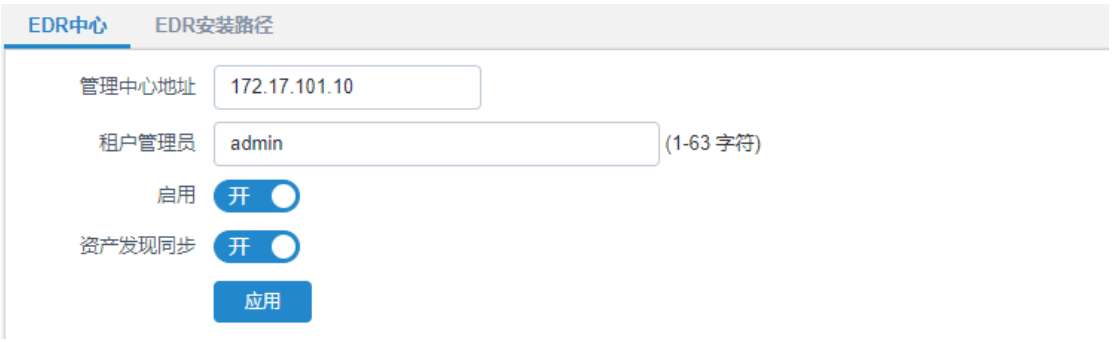
4.9. EDR 策略

下一代防火墙支持与安恒 EDR 的联动：下一代防火墙定期从配置的 EDR 管理控制中心获取数据，可获知网络主机的 EDR 安装信息及 EDR 防护状态，并根据配置的 EDR 联动策略向未安装 EDR 或者中毒的主机推送提示信息，或禁止其上网。

4.9.1. EDR 中心

4.9.1.1. EDR 中心

在系统菜单选择“策略>EDR 联动>EDR 中心>EDR 中心”，进入 EDR 中心配置页签。



EDR 中心配置配置项及详细说明如下：

配置项	说明
管理中心地址	输入安恒管理中心的 IP 地址。
租户管理员	输入租户管理员账号，该账号是 EDR 管理中心上配置。
启用	EDR 联动功能是否开启。

资产发现同步	EDR 发现的设备是否同步到资产管理模块。

4.9.1.2. EDR 安装类路径

在系统菜单选择“策略>EDR 联动>EDR 中心配置>EDR 安装路径”，进入 EDR 安装路径配置页签。

EDR 安装路径配置项及详细说明如下：

配置项	说明
用户定义 EDR 安装路径	当终端未安装 EDR 客户端时，设备给终端推送的自定义的 EDR 客户端安装链接，让用户能够顺利安装 EDR 客户端。

4.9.2. EDR 联动

在系统菜单选择“策略>EDR 联动>EDR 联动”，进入 EDR 联动配置页面。

在 EDR 联动策略页签下点击<新建>创建 EDR 联动策略规则，或者在右侧“操作”列下点击图标修改已有的 EDR 联动策略规则。

EDR 联动策略配置项及详细说明如下：

配置项	说明
启用	该条策略是否启用。
源地址	对终端的源地址进行限制，选择地址对象，仅支持 IP 地址对象，地址对象配置参考对象中地址对象的创建。
目的地址	对终端的源地址进行限制，选择地址对象，仅支持 IP 地址对象。
动作	对不满足条件的终端的操作策略，一共有三种策略： ● **始终允许**-允许被管控的终端通信，不做限制。 ● **EDR 管控并允许**-会通过 HTTP 给被管控终端推送客户端下载链接，客户端的数据会转发，不做限制。 ● **EDR 管控**-会通过 HTTP 给被管控终端推送客户端下载链接，客户端未安装 EDR 客户端前，数据不能通过防火墙转发。

4.9.3. EDR 资产列表

在系统菜单选择“**策略>EDR 联动>EDR 资产列表**”，进入 **EDR 资产列表**配置页面，EDR 管理中心同步给设备安装过 EDR 客户端的信息在本页面显示。

EDR 资产列表中可以查看安装了 EDR 客户端的终端的 IP 地址，操作系统，当前设备可用性状态，在线状态，中毒状态，并可通过按钮给中毒的设备临时放行。

4.10. NAT 策略

NAT即网络地址转换，用于私有地址向公有地址的转换，以解决公有IP地址短缺的问题。这种通过使用少量的全球IP地址（公网IP地址）代表较多的私有IP地址的方式，将有助于减缓可用的IP地址空间的枯竭。后来随着NAT技术的发展及应用的不断深入，NAT更被证明是一项非常有用的技术，可用于多种用途，如：提供了单向隔离，具有很好的安全特性；可用于目标地址的映射，使公有地址可访问配置私有地址的服务器；另外还可用于服务器的负载均衡和地址复用等。

下一代防火墙支持源NAT、目的NAT、静态NAT、跨协议NAT四种NAT功能。

4.10.1. 源 NAT

源 NAT 是基于源地址的转换，主要用于内网访问外网，有效减少对公网 IP 地址的使用，使得多个内网用户可以使用一个公网 IP 来实现访问公网。

在系统菜单点击“**策略>NAT 策略>源 NAT**”，进入**源 NAT** 配置页面，查看设备上已有的源 NAT 策略。设备依据从上往下的顺序依次匹配源 NAT 策略。点击图标修改策略的启用/禁用状态，点击图标编辑修改已有的策略，点击图标清除对应策略的命中数，点击图标复制策略。

用户可以选中特定策略后点击<**移动**>，指定目标位置策略 ID，移动到目标位置策略 ID 之前或者之后。

也可以点击<**查询**>按钮，指定转换类型、源地址、目的地址、服务来查询已有的源 NAT 策略。

点击<**新建**>，建立新的源 NAT 策略。

源 NAT 策略的配置项及详细说明如下：

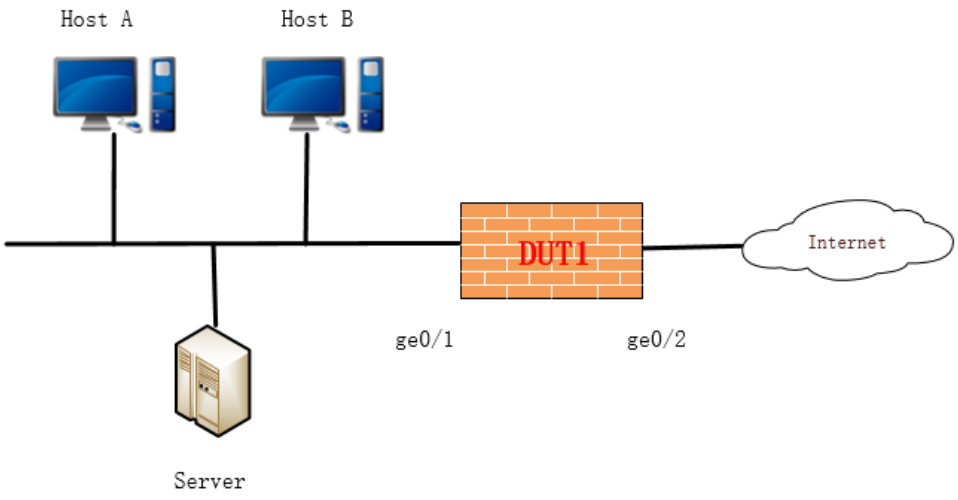
配置项	说明
转换类型	设备支持 IPv4 协议类型地址之间的互转，以及 IPv6 协议类型地址之间的互转。
UID	NAT 策略的 UID 与 HA 配置中主主模式下的单元 ID 有关，两处 ID 设置一致时，创建的或者同步过来的 NAT 策略才会在本设备生效，否则策略不生效。有关 HA 配置的更多信息，请参考 HA 配置。
源地址	NAT 规则匹配的源地址，可以是地址对象或地址组。有关地址对象配置的更多信息，请参考地址。
目的地址	NAT 规则匹配的目的地址，可以是地址对象或地址组。有关地址对象配置的更多信息，请参考地址。
服务	NAT 规则匹配的服务，可以是预定义服务对象、自定义服务对象或服务组。有关服务对象配置的更多信息，请参考服务。

出接口	流量出设备的接口。
转换后源地址	需要转换成的源地址，可以是出接口地址或地址池地址。选择的地址池地址类型必须与转换类型一致。有关地址池配置的更多信息，请参考 NAT 地址池。
描述	对该转换规则的描述，最长不得超过 127 个字符。
日志	开启后匹配该策略的流量可产生日志。在系统菜单点击“**系统>日志设定>日志过滤**”，进入**日志过滤**页面，开启 NAT 策略本地日志，具体请参考日志过滤。在系统菜单点击“**日志>NAT 日志**”，进入 NAT 日志页面，查看日志的详细信息。

4.10.1.1. 源 NAT 配置示例

组网需求

如下图所示，公司拥有 200.1.1.1/24 到 200.1.1.5/24 五个外网地址，内网地址为 192.168.2.0/24 网段，要求实现内网地址可以使用 200.1.1.1/24 和 200.1.1.3/24 三个地址访问外网。



配置步骤

1. 在系统菜单点击“**对象>地址对象>地址对象**”，进入**地址对象**配置页面，点击<**新建**>，创建以下地址对象：

2. 在系统菜单点击“**策略>NAT 策略>NAT 地址池**”，进入 NAT 地址池配置页面，点击<**新建**>，创建以下地址池：

3. 在系统菜单点击“策略>NAT 策略>源 NAT”，进入源 NAT 配置页面，点击<新建>，创建以下源 NAT 策略：

4. 配置完成后内网主机可以直接访问外网。

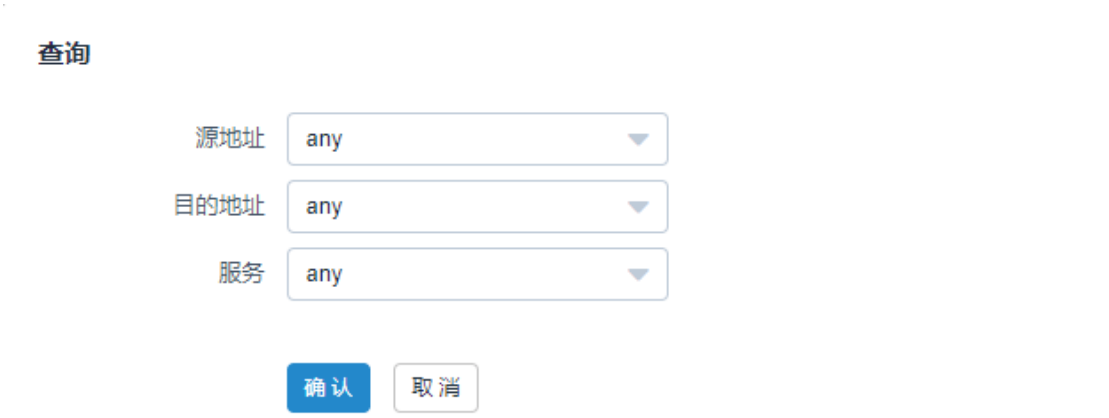
4.10.2. 目的 NAT

目的 NAT 是基于目的地址的转换，主要用于外网访问内网。

在系统菜单点击“策略>NAT 策略>目的 NAT”，进入目的 NAT 配置页面，查看设备上已有的目的 NAT 策略。设备依据从上往下的顺序依次匹配目的 NAT 策略。。点击图标修改策略的启用/禁用状态，点击图标编辑修改已有的策略，点击图标清除对应策略的命中数，点击图标复制策略。

用户可以选中特定策略后点击<移动>，指定目标位置策略 ID，移动到目标位置策略 ID 之前或者之后。

也可以点击<**查询**>按钮，指定源地址、目的地址、服务来查询已有的目的 NAT 策略。



点击<**新建**>，建立新的目的 NAT 策略。

目的 NAT 策略的配置项及详细说明如下：

配置项	说明
UID	NAT 策略的 UID 与 HA 配置中主主模式下的单元 ID 有关，两处 ID 设置一致时，创建的或者同步过来的 NAT 策略才会在本设备生效，否则策略不生效。有关 HA 配置的更多信息，请参考 HA 配置。
源地址	NAT 规则匹配的源地址，可以是地址对象或地址组。有关地址对象配置的更多信息，请参考地址。
目的地址	NAT 规则匹配的目的地址，可以是地址对象或地址组。有关地址对象配置的更多信息，请参考地址。
服务	NAT 规则匹配的服务，可以是预定义服务对象、自定义服务对象或服务组。有关服务对象配置的更多信息，请参考服务。
入接口	流量进入设备的接口。
转换后目的地址	需要转换成的目的地址。选择的地址池地址类型必须与转换类型一

	致。有关地址池配置的更多信息，请参考 NAT 地址池。
转换后端口	转换为指定的 IP 地址+端口。
描述	对该转换规则的描述，最长不得超过 127 个字符。
日志	开启后，并且点击系统菜单“**系统>日志设定>日志过滤**”，进入**日志过滤**页面，开启 NAT 策略本地日志，具体请参考日志过滤。在系统菜单点击“**日志>NAT 日志**”，进入 NAT 日志页面，查看日志的详细信息。

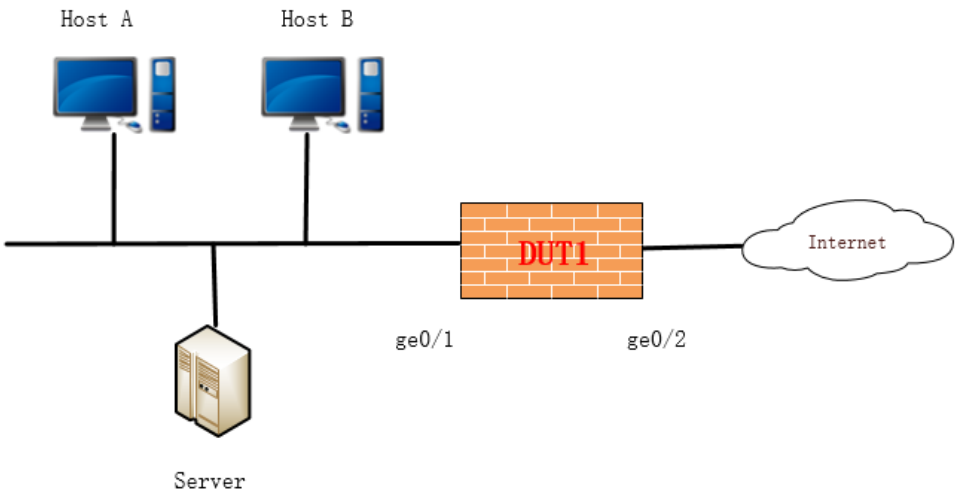
注意：

目的 NAT 会将匹配到的流中的目的地址全部转换，因此一般匹配规则中不配置 any。

4.10.2.1. 目的 NAT 配置示例

组网需求

如下图所示，公司内网拥有一台服务器对外提供 HTTP 服务，其内网地址为 192.168.2.4/24，服务端口为 TCP80 端口，对外开放的 IP 地址为 200.2.1.1/24，对外开放的服务端口为 TCP8080 端口，要求在外网可以直接访问内网服务器。



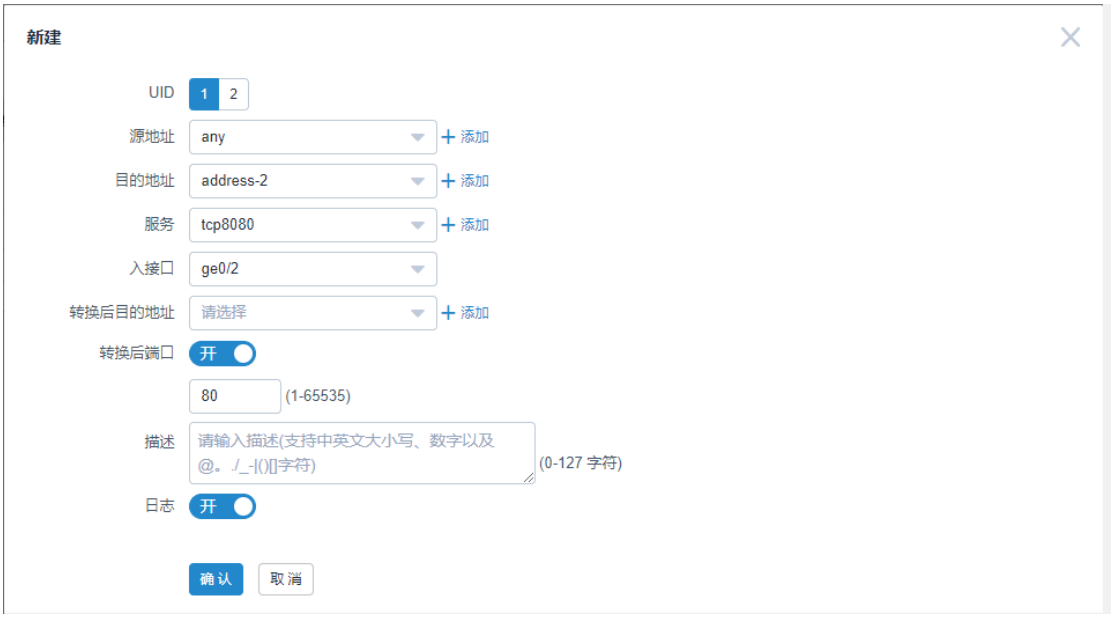
配置步骤

1. 在系统菜单点击“对象>地址对象>地址对象”，进入地址对象配置页面，点击<新建>，创建以下地址对象：

2. 在系统菜单点击“策略>NAT 策略>NAT 地址池”，进入 NAT 地址池配置页面，点击<新建>，创建以下地址池：

3. 在系统菜单点击“对象>服务对象>自定义服务”，进入自定义服务配置页面，点击<新建>，创建以下服务对象：

4. 在系统菜单点击“策略>NAT 策略>目的 NAT”，进入目的 NAT 配置页面，点击<新建>，创建以下目的 NAT 策略：



5. 配置完成后外网主机可以直接访问内网服务器。

4.10.3. 静态 NAT

静态 NAT 是一对一的双向地址映射。在这种情况下，被映射的内部主机可以主动访问外部，外部也可以主动访问这台内部主机，相当于在内、外网之间建立了一条双向通道。

在系统菜单点击“**策略>NAT 策略>静态 NAT**”，进入**静态 NAT** 配置页面，查看设备上已有的静态 NAT 策略。设备依据从上往下的顺序依次匹配静态 NAT 策略。点击图标修改策略的启用/禁用状态，点击图标编辑修改已有的策略，点击图标清除对应策略的命中数，点击图标复制策略。

用户可以选中特定策略后点击<**移动**>，指定目标位置策略 ID，移动到目标位置策略 ID 之前或者之后。

也可以点击<**查询**>按钮，指定转换类型、外部地址、内部地址来查询已有的静态 NAT 策略。

点击<**新建**>，建立新的静态 NAT 策略。

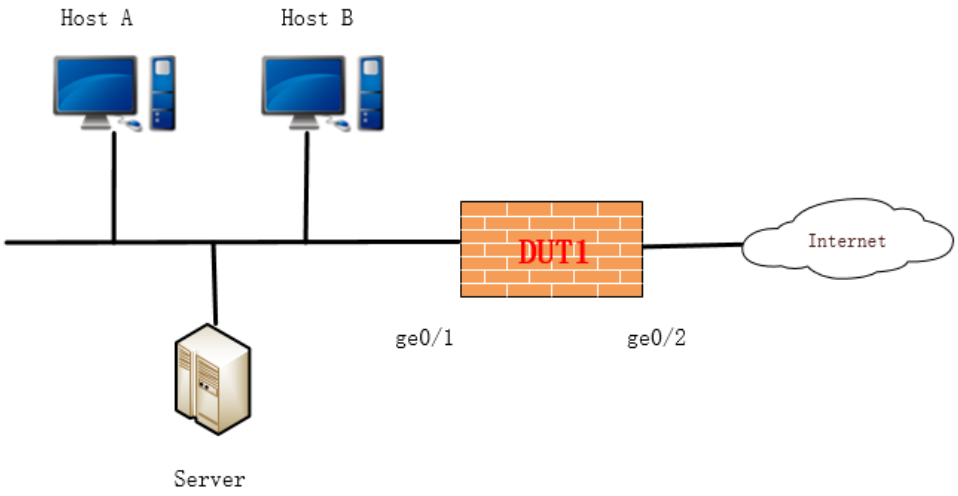
静态 NAT 策略的配置项及详细说明如下：

配置项	说明
UID	NAT 策略的 UID 与 HA 配置中主主模式下的单元 ID 有关，两处 ID 设置一致时，创建的或者同步过来的 NAT 策略才会在本设备生效，否则策略不生效。有关 HA 配置的更多信息，请参考 HA 配置。
转换类型	设备支持 IPv4 to IPv4 协议类型的地址之间的互转，以及 IPv6 to IPv6 协议类型地址之间的互转。
外部地址	需要转换的外部地址。
内部地址	需要转换的内部地址。
接口	和外网相连的接口。
描述	对该转换规则的描述，最长不得超过 127 个字符。
日志	开启后，并且在系统导航栏“**系统>日志过滤**”中开启 NAT 策略本地日志，具体请参考日志过滤。在系统菜单点击“**日志>NAT 日志**”，进入 NAT 日志页面，查看日志的详细信息。

4.10.3.1. 静态 NAT 配置示例

组网需求

如下图所示，公司拥有外网地址 200.3.1.1/24，有一台内网服务器地址为 192.168.3.1/24，要求实现内网服务器可以使用 200.3.1.1/24 访问外网，外网也可以直接访问内网服务器。



配置步骤

1. 在系统菜单点击“策略>NAT 策略>静态 NAT”，进入静态 NAT 配置页面，点击<新建>，创建以下静态 NAT 策略：

2. 配置完成后内网服务器可以直接访问外网，外网主机也可以访问到内网服务器。

4.10.4. 跨协议 NAT

跨协议转换，即 IPv4 与 IPv6 协议地址的互转功能，主要是为了满足用户实现不同网络协议栈之间的互访需求，实现两种协议栈的无缝衔接，从而可达到从 IPv4 网络环境逐步向 IPv6 网络环境过渡的效果。

目前下一代防火墙设备实现了 NAT46，即 IPv4 端发起请求，将其转换为 IPv6 地址，以及 NAT64，即 IPv6 端发起请求，将其转换为 IPv4 地址的转换功能。并在此基础上提供了多种转换方式，可根据用户的实际环境选取合理的转换方式，实现 IPv4 网络与 IPv6 网络之间的互访。跨协议 NAT 分为 NAT46 和 NAT64 两种转换类型，目前设备提供三种转换方式：IVI 转换、嵌入地址转换以及地址池转换。

4.10.4.1. IVI 转换方式

IVI 转换方式是由中国教育和科研计算机网（CERNET）提出的一种无状态的地址映射方式，通过使用指定的前缀，可实现 IPv4 与 IPv6 地址之间的互相转换。IVI 转换方式支持 NAT46 和 NAT64。

在系统菜单点击“**策略>NAT 策略>跨协议 NAT**”，进入**跨协议 NAT** 配置页面，点击<**新建**>，建立新的跨协议 NAT 策略，转换方式选择 IVI。

IVI 转换方式的跨协议 NAT 策略的配置项及详细说明如下：

配置项	说明
转换类型	设备支持 NAT46 地址之间的互转，以及 NAT64 地址之间的互转。
UID	NAT 策略的 UID 与 HA 配置中主主模式下的单元 ID 有关，两处 ID 设置一致时，创建的或者同步过来的 NAT 策略才会在本设备生效，否则策略不生效。有关 HA 配置的更多信息，请参考 HA 配置。
转换方式	包括 IVI、嵌入地址转换和地址池三种转换方式，这里选择 IVI。
源地址	NAT 规则匹配的源地址，可以是地址对象或地址组。有关地址对象配置的更多信息，请参考地址。
目的地址	NAT 规则匹配的目的地址，可以是地址对象或地址组。有关地址

	对象配置的更多信息，请参考地址。
服务	NAT 规则匹配的服务，可以是预定义服务对象、自定义服务对象或服务组。有关服务对象配置的更多信息，请参考服务。
入接口	流量入设备的接口。
源地址类型	● **指定源地址前缀**-源地址根据配置的前缀，采用 IVI 转换规则进行转换必须为 32 位掩码。 ● **转换后源地址**-源地址从指定的地址池中选取，或者转换为出接口地址。
指定目的地址前缀	目的地址根据配置的前缀，采用 IVI 转换规则进行转换，必须为 32 位掩码。
日志	开启后命中该策略的流量可产生日志。在系统导航栏“**系统>日志过滤**”中开启 NAT 策略本地日志，具体请参考日志过滤。在系统菜单点击“**日志>NAT 日志**”，进入 NAT 日志配置页面，查看日志的详细信息。
响应邻居请求/响应 ARP	该规则是否响应对应的 ARP 请求或者邻居请求。(该开关控制的 NAT46 规则响应 ARP 请求的范围，以及 NAT64 规则响应邻居请求的范围由匹配的目的地址对象和入接口来决定)。
描述	对该转换规则的描述，最长不得超过 127 个字符。

4.10.4.2. 嵌入地址转换方式

嵌入地址转换方式，只能被用在 NAT64 的情形。转换后的目标地址是根据用户配置的前缀，从原有的 IPv6 的目标地址中取出前缀后的 32 位地址作为转换后地址。源地址转换可指定 NAT 地址池，或者直接转换为出接口地址。

在系统菜单点击“**策略>NAT 策略>跨协议 NAT**”，进入**跨协议 NAT** 配置页面，点击<**新建**>，建立新的跨协议 NAT 策略，转换方式选择**嵌入地址**。

嵌入地址转换方式的跨协议 NAT 策略的配置项及详细说明如下：

配置项	说明
转换类型	设备支持 NAT46 地址之间的互转，以及 NAT64 地址之间的互转。嵌入地址转换必须配置 NAT64。
UID	NAT 策略的 UID 与 HA 配置中主主模式下的单元 ID 有关，两处 ID 设置一致时，创建的或者同步过来的 NAT 策略才会在本设备生效，否则策略不生效。有关 HA 配置的更多信息，请参考 HA 配置。
转换方式	包括 IVI、嵌入地址转换和地址池三种转换方式，这里选择嵌入地址。
源地址	NAT 规则匹配的源地址，可以是地址对象或地址组。有关地址对象配置的更多信息，请参考地址。
目的地址	NAT 规则匹配的目的地址，可以是地址对象或地址组。有关地址对象配

	置的更多信息，请参考地址。
服务	NAT 规则匹配的服务，可以是预定义服务对象、自定义服务对象或服务组。有关服务对象配置的更多信息，请参考服务。
入接口	流量入设备的接口。
转换后源地址	源地址从指定的地址池中选取，或者转换为出接口地址。
目的地址前缀	从 IPv6 目的地址中配置的前缀之后，读取嵌入的 32 位 IPv4 地址作为转换后的目的地址（前缀最长为 96 位）。
日志	开启后该规则可产生日志。在系统菜单点击“**日志>NAT 日志**”查看日志的详细信息。
响应邻居请求	该规则是否响应对应的邻居请求。(该开关控制的 NAT64 规则响应邻居请求的范围由匹配的目的地址对象和入接口来决定)。
描述	对该转换规则的描述，最长不得超过 127 个字符。

4.10.4.3. 地址池转换方式

NAT64 和 NAT46 都可以使用地址池转换方式，该方式是指转换后的目的地址都从指定的地址池中选取，源地址也可从指定的地址池中选取，或者直接转换为出接口地址。

在系统菜单点击“**策略>NAT 策略>跨协议 NAT**”，进入**跨协议 NAT** 配置页面，，点击<**新建**>，建立新的跨协议 NAT 策略，转换方式选择**地址池**。

地址池转换方式的跨协议 NAT 策略的配置项及详细说明如下：

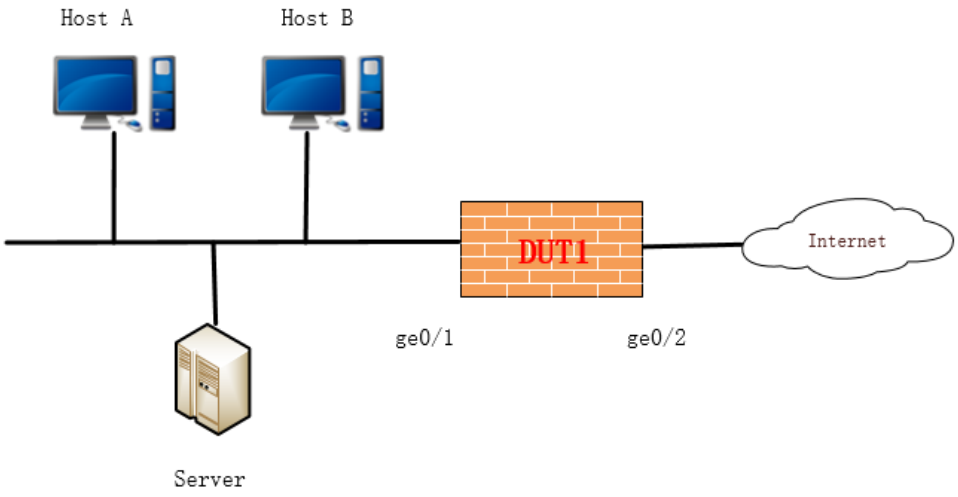
配置项	说明
转换类型	设备支持 NAT46 地址之间的互转，以及 NAT64 地址之间的互转。
UID	NAT 策略的 UID 与 HA 配置中主主模式下的单元 ID 有关，两处 ID 设置一致时，创建的或者同步过来的 NAT 策略才会在本设备生效，否则策略不生效。有关 HA 配置的更多信息，请参考 HA 配置。
转换方式	包括 IVI、嵌入地址转换和地址池三种转换方式，这里选择地址池。
源地址	NAT 规则匹配的源地址，可以是地址对象或地址组。有关地址对象配置的更多信息，请参考地址。
目的地址	NAT 规则匹配的目的地址，可以是地址对象或地址组。有关地址对象配置的更多信息，请参考地址。

服务	NAT 规则匹配的服务，可以是预定义服务对象、自定义服务对象或服务组。有关服务对象配置的更多信息，请参考服务。
入接口	流量入设备的接口。
转换后源地址	源地址从指定的地址池中选取，或者转换为出接口地址。
转换后目的地址	目的地址从指定的地址池中选取。
日志	开启后该规则可产生日志。在系统菜单点击“**日志>NAT 日志**”，进入 **NAT 日志**配置页面，查看日志的详细信息。
响应邻居请求/响应 ARP	该规则是否响应对应的 ARP 请求或者邻居请求。(该开关控制的 NAT46 规则响应 ARP 请求的范围，以及 NAT64 规则响应邻居请求的范围由匹配的目的地址对象和入接口来决定)。
描述	对该转换规则的描述，最长不得超过 127 个字符。

4.10.4.4. NAT46 跨协议转换配置示例

组网需求

如下图所示，公公司内部局域网为 IPv4 网络，需要通过应用设备访问另外一个 IPv6 网络类型局域网中的一个 FTP 站点。该站点的地址为 2010::80/64，公司内部网段为 10.0.0.0/24。下一代防火墙作为核心路由，串行接入网络。



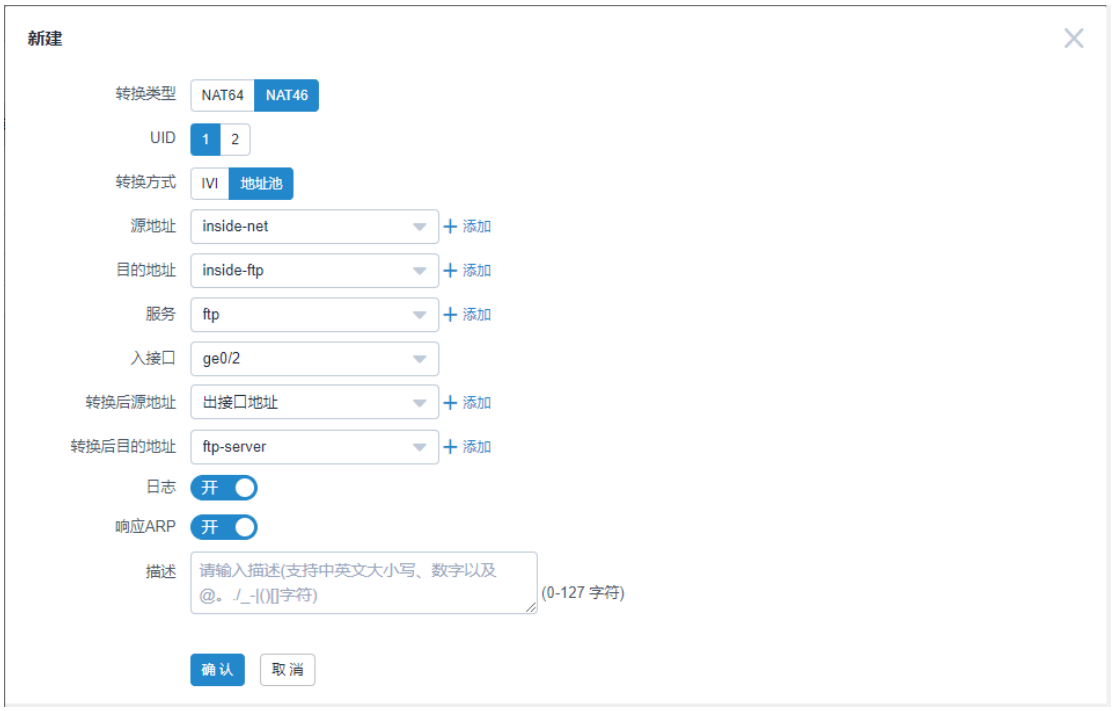
配置步骤

1. 在系统菜单点击“**对象>地址对象>地址对象**”，进入**地址对象**配置页面，点击<**新建**>，创建以下地址对象：

2. 在系统菜单点击“**对象>地址对象>地址对象**”，进入**地址对象**配置页面，点击<**新建**>，创建以下地址对象，该地址将作为 FTP 服务器在内网的映射地址，不能与内网任何一台 PC 的地址冲突：

3. 在系统菜单点击“**策略>NAT 策略>NAT 地址池**”，进入 **NAT 地址池**配置页面，点击<**新建**>，创建以下地址池：

4. 在系统菜单点击“策略>NAT 策略>跨协议 NAT”，进入跨协议 NAT 配置页面，点击<新建>，创建以下 NAT46 策略：



5. 配置完成后可以实现跨协议访问。

4.10.5. NAT 地址池

地址池是用于 NAT 地址转换的 IP 地址集合，用户可根据自己拥有的合法 IP 地址数目、内网主机数目以及实际应用情况，定义合适的地址池。在 NAT 地址转换的过程中，设备将会从地址池中挑选一个 IP 地址做为报文转换后的源 IP 地址。同时，NAT 地址池通过向服务器持续发送 ICMP、TCP 探测报文，及时发现服务器的失活、关闭问题，避免正常的用户流量被引流到失活、关闭的服务器。

在系统菜单点击“策略>NAT 策略>NAT 地址池”，进入 NAT 地址池配置页面，查看已有的 NAT 地址池。

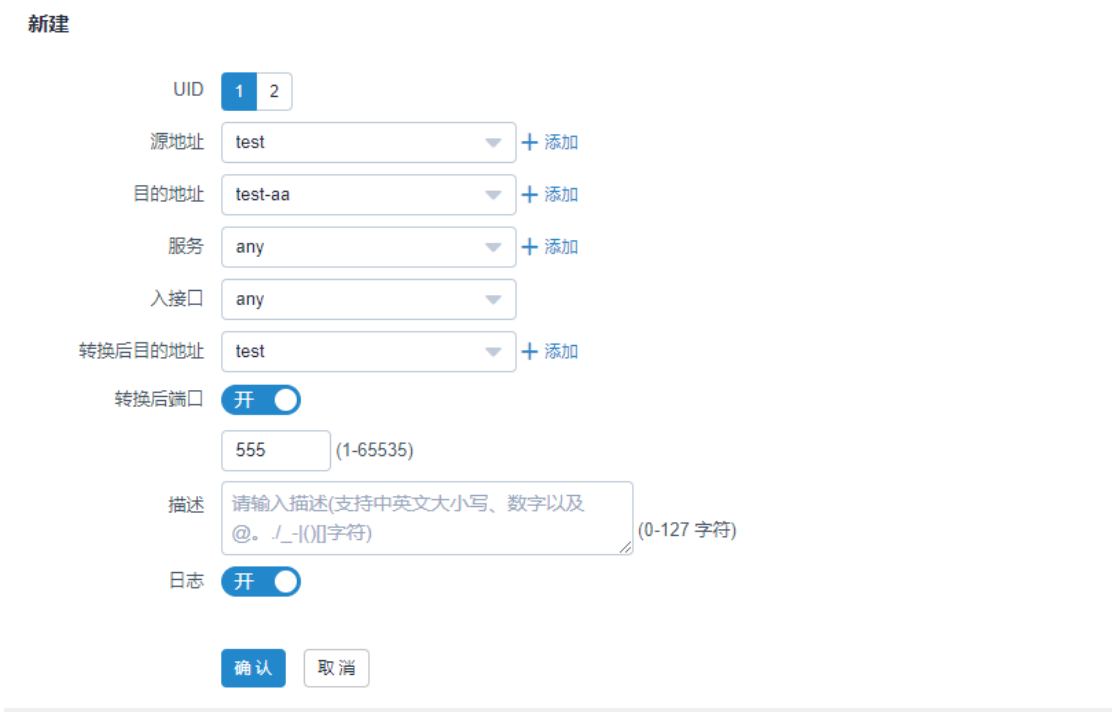
在 NAT 地址池页面，点击<**新建**>按钮创建新的 NAT 地址池，或点击操作列的编辑按钮修改已有的 NAT 地址池。

NAT 地址池配置项及详细说明如下：

配置项	说明
名称	NAT 地址池名称。
描述	NAT 地址池描述信息，非必填项。
选择算法	默认使用源目的地址哈希，可选择轮询、源地址保持。
类型	默认使用无，可选择 ICMP、TCP HALF OPEN。

	● ICMP-只需要配置间隔、最大重试次数、超时时间。设备通过 ICMP 报文对服务器进行探测，只可以探测服务器是否失活，无法探测服务是否关闭。 ● TCP HALF OPEN-需要配置间隔、最大重试次数、超时时间、端口。设备通过 TCP 三次握手的 SYN 报文对服务器进行探测，不仅可以探测服务器是否失活，还可以探测服务是否关闭。
间隔	默认 16，探测报文发送的时间间隔。
最大重试次数	默认 3，探测报文未收到回应，判断探测地址失活、关闭的连续探测次数。探测报文在超时时间范围内没有收到回应，会按照间隔时间进行下次探测，当连续多次都没有在超时时间范围都收到回应，在连续次数达到最大重试次数后，探测地址被判断为不可达地址。
超时时间	默认 5，探测报文未收到回应时，判断此次探测失败的最大超时时间，探测报文连续多次在超时时间范围内没有收到回应，且连续次数达到最大重试次数，探测地址被判断为不可达地址。
端口	只有类型为 TCP HALF OPEN，才会有此配置项，默认 80，即 HTTP 服务，端口代表需要进行探测的服务端口，如：80 对应 HTTP 服务，21 对应 FTP 服务，53 对应 DNS 服务。
协议类型	默认 IPv4，可切换成 IPv6，在输入框输入探测的地址范围。

完成以上配置项后，在系统菜单点击“**策略>NAT 策略>目的 NAT**”，进入**目的 NAT** 配置页面，点击<**新建**>创建新的 NAT 策略，或点击操作列的编辑按钮，修改已有的 NAT 策略，配置项转换后目的地址引用该 NAT 地址池。



在系统菜单点击“策略>NAT 策略>NAT 地址池”，进入地址池探测结果页签，查看 NAT 地址池的探测结果。

提示：

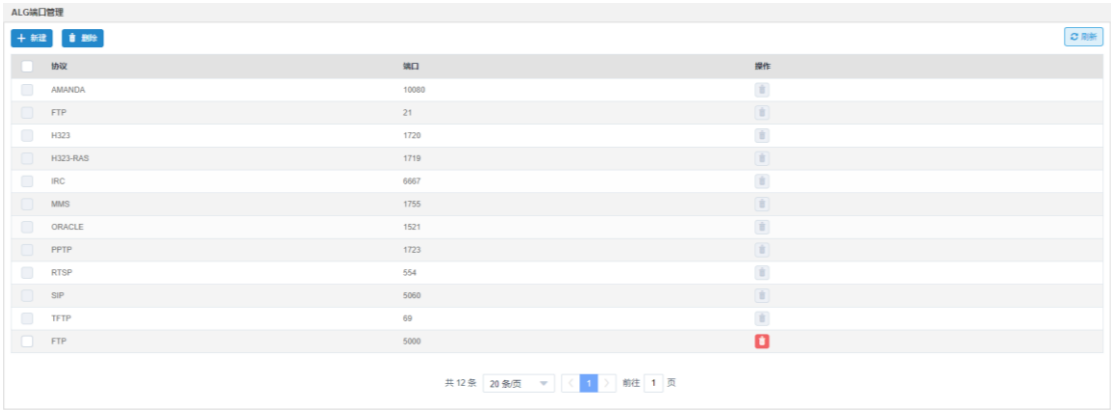
NAT 地址池的探测范围最大 1024 个地址。NAT 地址池不支持 IPv6 地址探测。NAT 地址池只有被目的 NAT 引用后，才会进行地址探测。

4.10.6. ALG 端口管理

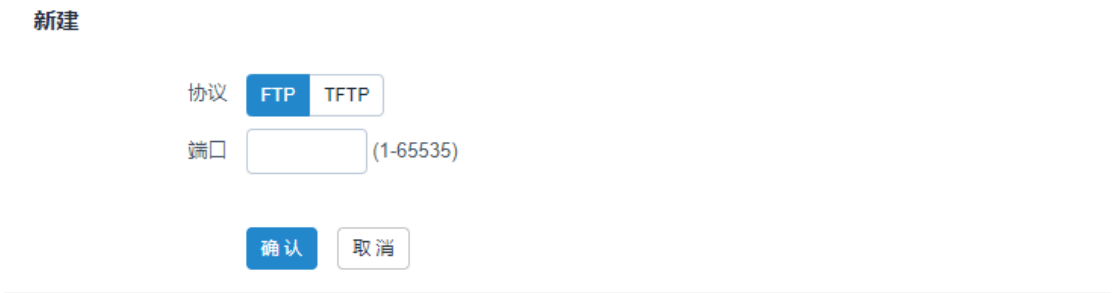
某些场景下，服务器有时会改变所提供服务对应的监听端口号，下一代防火墙可根据用户自定义的 ALG 端口号，正确识别报文中端口号所对应的服务类型。

例如，某个 FTP 服务器除了开放 21 端口监听请求之外，也开放了 1000 端口监听 FTP 请求；当设备接收到一个报文的目的端口号为 1000 时，要识别出该报文为一个 FTP 相关报文，这时就需要设备对 ALG 的端口进行一定的处理。

在系统菜单点击“**策略>NAT 策略>NAT 端口管理**”，进入 **NAT 端口管理**配置页面，显示设备上已有的 NAT 端口管理配置。FTP 协议的 21 号端口和 TFTP 协议的 69 号端口为设备出厂时内置，不可删除或编辑。点击 图标可以删除其他的 NAT 端口管理配置，但不可以进行编辑修改。



点击<**新建**>，建立新的 NAT 端口管理。



NAT 端口管理的配置项及详细说明如下：

配置项	说明
协议	选择协议类型，可选择 FTP 或 TFTP。
端口	选择协议的监听端口号，可选端口的范围为 1-65535。

4.11. 流控策略

下一代防火墙支持流控策略，对通过的流量，基于应用、服务、用户、地址对象等条件进行分析和控制，对各种网络流量实施精细化管控和优化。系统通过以下流程实现流量控制：在选定的物理线路/虚拟线路上划分出不同的虚拟通道，每条通道承载不同的用户或服务流量，根据实际业务需求对虚拟通道执行带宽限制。

4.11.1. 线路设置

线路是流量进出设备的接口，在系统菜单点击“**策略>流控策略>线路设置**”，进入**线路设置**配置页面，查看设备已有的线路。

在线路设置页面，点击<**新建**>按钮创建新的线路，或在操作列点击编辑按钮修改已有的线路。

线路设置配置项及详细说明如下：

配置项	说明
状态	默认开启，关闭状态开关，线路及线路下的所有流控策略全部禁用。
名称	线路名称。
绑定接口	选择线路的绑定接口，只可以绑定物理接口、VLAN、tunl 口，且每个接口只能绑定到一个线路。
带宽限制（出）	设置线路的出站方向的带宽限制。
带宽限制（入）	设置线路的入站方向的带宽限制。

4.11.2. 流控策略

系统以通道为单位对出入物理线路的流量进行划分，并根据通道的策略配置对通道内的流量进行管控。为方便用户配置，系统支持多级通道，即线路中的每个通道还可以包含子通道。用户可以通过多级通道的方式将不同属性的流量限制在一定的带宽内，保障重要的用户或应用优先使用线路带宽。

在系统菜单点击“**策略>流控策略>流控策略**”，进入**流控策略**配置页面，并点击线路名称左侧的展开按钮，展示线路下所有的流控策略。

在流控策略页面，首先鼠标点击线路名称，然后点击<**新建**>按钮创建新的流控策略，或点击操作列的编辑按钮修改已有的流控策略。

流控策略配置项及详细说明如下：

配置项	说明
启用	默认开启，关闭启用开关后，该策略及该策略下的所有子通道全部禁用。
线路名称	流控策略的名称。
上一级	显示新建流控策略所属的线路或流控策略，不可操作项。
级别	选择流控策略的优先级，如果子通道的保障带宽未将父通道的最大带宽用满，同时，子通道的实际流量超过该子通道的保障带宽，可以借用父通道剩余的带宽。优先级越高，越有可能借用到父通道的剩余带宽。
带宽设定	设置通道的上下行最大带宽及保障带宽。 最大带宽不能超过其上级通道的最大带宽。 保障带宽是为流控策略预留的带宽，不会被其他流控策略占用。保障带宽不能超过其上级流控策略/线路的保障带宽，也不能超过该流控策略的最大带宽，当多个同级流控策略的保障带宽之和大于等于上一级流控策略的保障带宽，此处设置的保障带宽会自动按比例调整。
每终端限速	根据 IP 地址或用户对终端的上下行流量进行限速。
匹配条件	基于用户、源/目的地址、时间、应用等条件对流量进行匹配，对匹配的流量执行策略中指定的流量控制措施。有关上述对象配置的更多信息，请参考用户、地址、应用、时间。

4.11.3. 流量监控

流量监控是查看设备上所有线路、流控策略的带宽及实时流量情况。在系统菜单点击“**策略>流控策略>流量监控**”，进入**流量监控**页面，查看流量监控的最新情况。

4.11.4. 排除策略

排除策略是指不对流控策略中指定的用户或地址执行流量控制。在系统菜单点击“**策略>流控策略>排除策略**”，进入**排除策略**配置页面，查看设备已有的排除策略。

在排除策略页面，点击<**新建**>按钮并选择需要排除的用户和地址。

有关用户和地址对象配置的更多信息，请参考用户和地址。

提示：

排除策略中的地址和用户是“与”的关系，即只对地址范围内的用户生效。

4.11.5. 惩罚通道

惩罚通道是用户上网流量或时长超过设置阈值时进行惩罚限速处理的通道。惩罚通道不依赖于线路及接口，只能被用户限额策略引用，当用户达到用户限额阈值时流量才会被引流到相应的惩罚通道。

在系统菜单点击“**策略>用户策略>惩罚通道**”，进入**惩罚通道**配置页面，查看设备已有的惩罚通道。

在惩罚通道页面，点击<**新建**>按钮创建新的惩罚通道，或点击编辑按钮修改已有惩罚通道。

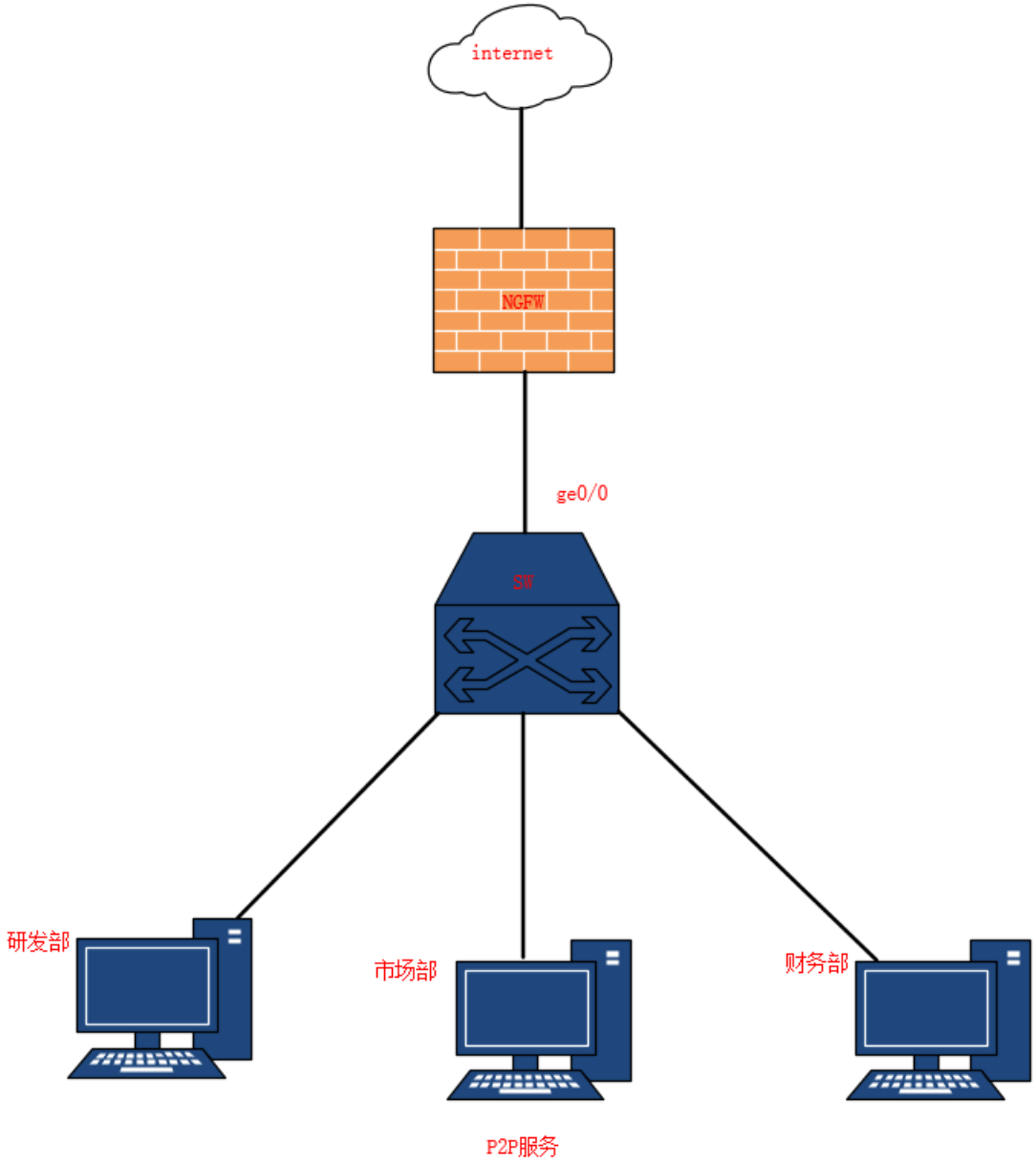
惩罚通道配置项及详细说明如下：

配置项	说明
名称	惩罚通道名称。
带宽设定	设置惩罚通道的出站、进站方向的带宽限制。
每终端限速	根据 IP 地址或用户对终端的上下行流量进行限速。

4.11.6. 流控策略配置实例

组网需求

如下图所示，限制研发部、市场部 P2P 访问的上下行带宽为 2M，同时每用户的 P2P 流量限制 100Kb，上级父节点上下行带宽设置为 1G；同时针对研发部进行带宽保障，上下行保障带宽均配置为 4M，最大带宽 6M。

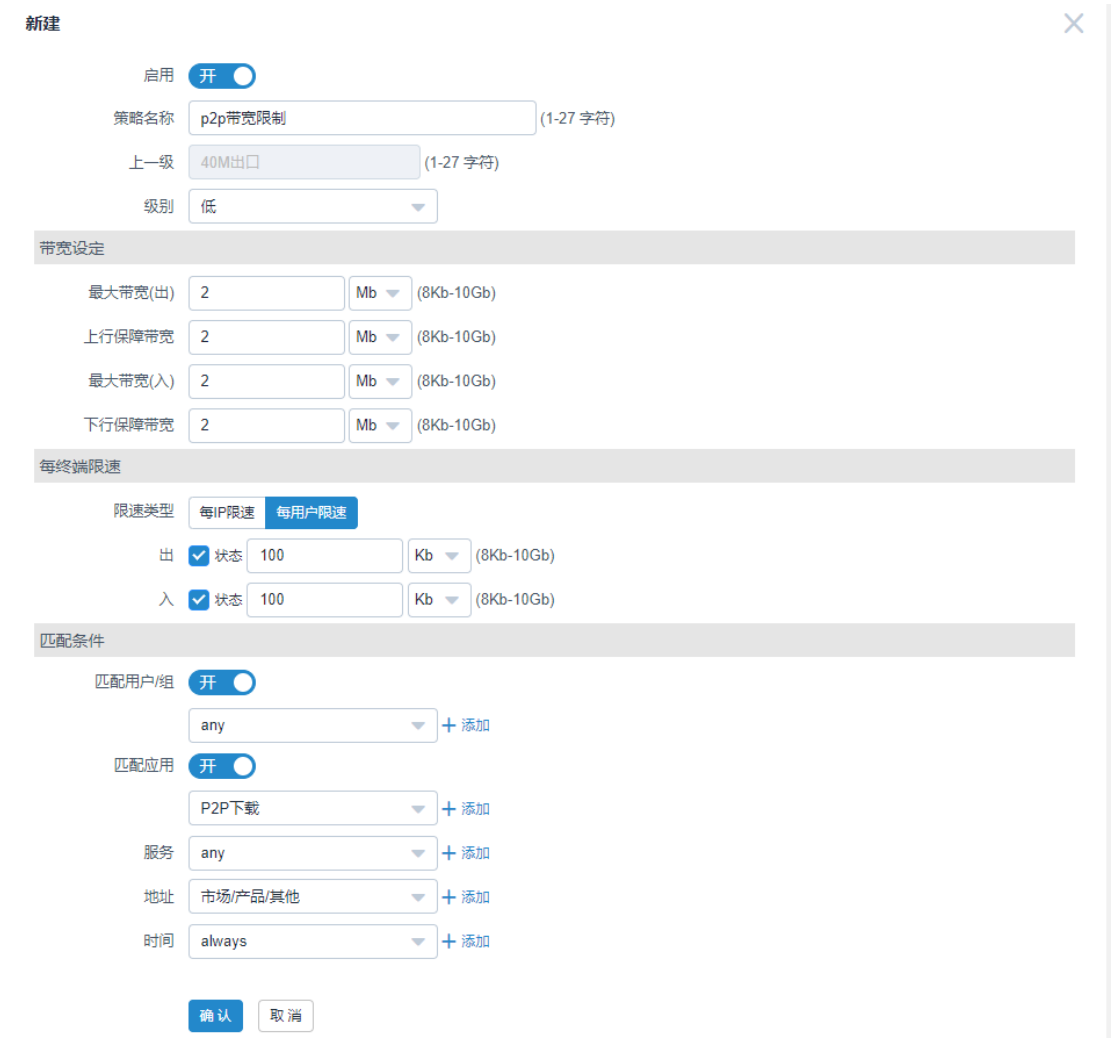


配置步骤

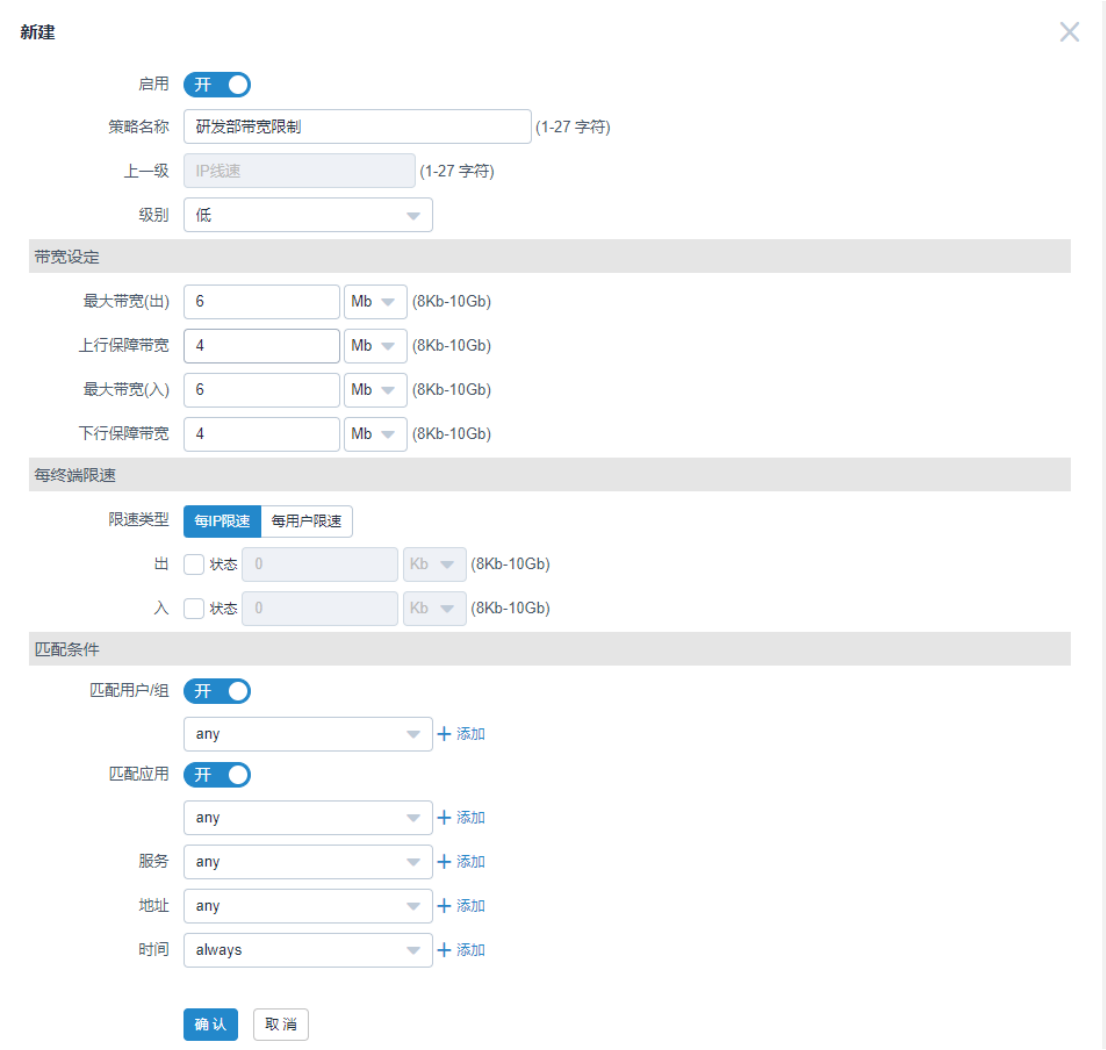
1. 配置研发部、市场部、财务部的 IP 地址及地址组（略）。

2. 在系统菜单点击“**策略>流控策略>线路设置**”，点击<**新建**>按钮创建以下线路：

3. 在系统菜单点击“**策略>流控策略>流控策略**”，鼠标点击步骤 2 创建的线路名称，点击<**新建**>按钮创建研发部、市场部 P2P 访问的流控策略：



4. 重复步骤 3 的操作步骤，创建研发部带宽保障的流控策略：



5. 配置完成后，在系统菜单点击“**策略>流控策略>流量监控**”，确认 P2P 访问的最大流量为 2M，研发部流量为 4M-6M 之间。

4.12. 协议管理

下一代防火墙支持协议连接超时管理功能，以保护设备的连接资源。

本系统默认配置下，TCP 协议的全连接，默认超时时间是 1 小时，UDP 协议为 30 秒。有些应用程序在全连接建立后，报文只会根据实际的数据进行交互，而没有保活机制，往往会导致连接超时删除，后续的数据无法通过设备。协议管理功能提供了设置特定服务超时时间的功能，可以解决这种需要长时间空闲连接的问题。

在系统菜单点击“**策略>协议管理**”显示已配置的协议管理配置

在系统菜单点击<**新建**>或按钮进入协议管理配置界面，用户可以根据需求配置协议超时时间。

协议管理配置项及详细说明如下：

配置项	说明
名称	协议管理条目自定义命名。
协议	选择该协议管理的协议类型，TCP 或 UDP。
端口	填写该协议对应的业务端口。
超时时间	<1-65535>，单位为分钟。
描述	对该协议管理进行注释说明。

提示：

配置协议管理后，对新建的连接才会生效。

第五章 网络

5.1. 接口

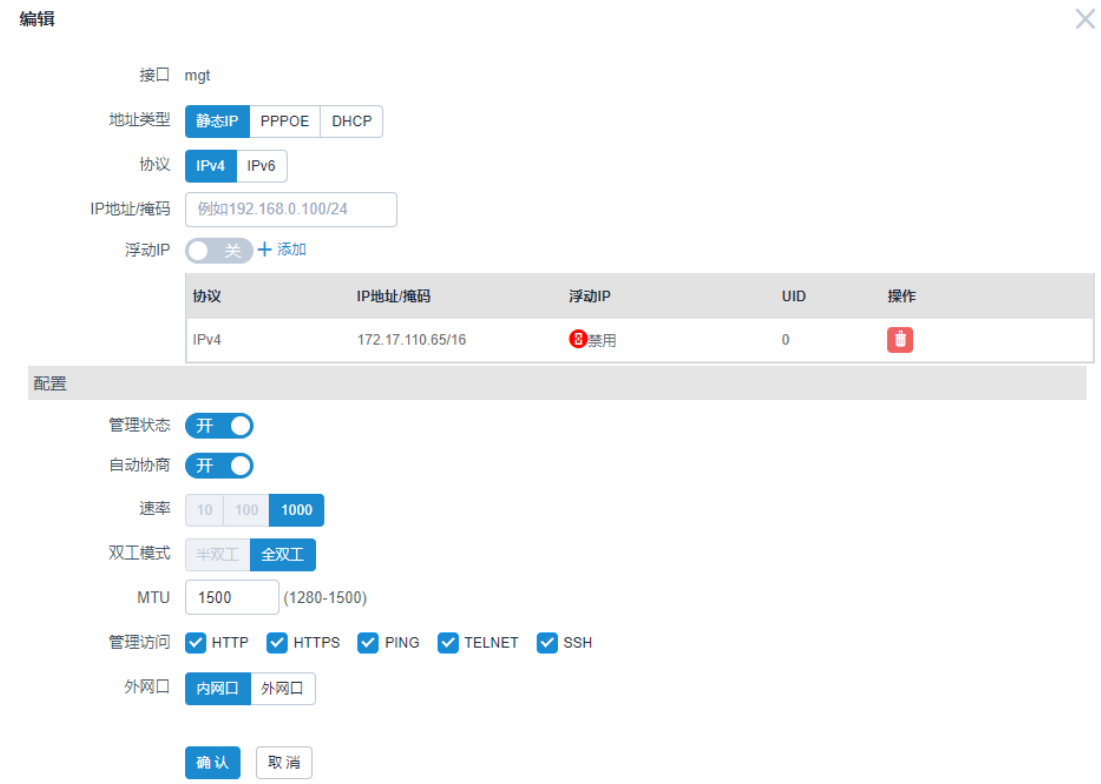
5.1.1. 物理接口

物理接口为设备板载口及扩展卡所支持接口，用户不能对物理接口进行删除操作，也不支持更改接口 mac 地址。物理接口根据速率可分为千兆口及万兆口，千兆口使用 ge1/0 形式进行展示，万兆口使用 xge1/0 方式进行展示。用户可根据需要，对接口进行编辑，更改接口配置。

物理接口分为管理口，双机冗余口及业务口。管理口特殊命名为“mgt”，双机冗余口特殊命名为“eha”。管理口和双机冗余口不会进行转发。

在系统菜单点击“**网络>接口>物理接口**”，进入**物理接口**配置页面，可查看设备上所有物理接口及状态信息。

选择需要修改配置的接口，点击右侧按钮进入接口编辑页。



物理接口的配置项与详细说明如下：

配置项	说明
接口	除 mgt 口外的物理接口名称，支持更改。
地址类型	IP 获取方式，支持三种方式，静态 IP，PPPOE 获取，DHCP 获取。 ● 静态 IP-手动指定静态的接口主 IP 地址和掩码及从属 IP 地址和掩码，如 192.168.1.1/24，这种模式可以避免 IP 地址发生变化。主地址是接口的主要通信地址，优先级最高；从属 IP 地址是接口第二优先级的通信地址。 ● PPPOE-将物理接口配置为 PPPoE 客户端。PPPOE 是以太网上点对点协议（Point-to-Point Protocol over Ethernet）的缩写，在为客户端分配 IP 地址的同时，可以对客户端进行接入控制、验证以及计费。 用户名-PPPOE 拨号的用户名，通常由 ISP 服务商提供。 密码-PPPOE 拨号的密码，通常由 ISP 服务商提供。 指定 IP-要求 PPPOE 服务器分配的固定地址。

	更新网关-开启后由 PPPOE 服务器重新获取网关地址。 更新 DNS-开启后由 PPPOE 服务器重新获取 DNS。 ● DHCP-将物理接口配置为 DHCP 客户端，自动从 DHCP 服务器获取 IP 地址。DHCP 是动态主机配置协议（Dynamic Host Configuration Protocol）的缩写，能够自动为客户端分配适当的 IP 地址以及相关网络参数，从而简化网络管理。 优先级-配置 DHCP 优先级，范围 1-255，数字越小，优先级越高，即系统优先分配优先级数值小的 DHCP 地址。 更新网关-开启后由 DHCP 服务器重新获取网关地址。 更新 DNS-开启后由 DHCP 服务器重新获取 DNS。
协议	支持配置 IPv4 及 IPv6 两种协议类型 IP，通过点击页签进行切换当前 IP 类型，IPv6 仅支持静态地址类型。
IP 地址/掩码	IPv4 地址格式，例如：A.B.C.D/M。IPv6 地址格式，例如：2000::1/64。
浮动 IP	开关按钮，打开后需选择 UID。
添加按钮	选择协议；输入 IP 地址/掩码；选择是否设置浮动 IP 后，点击添加可将 IP 地址添加到表格。
配置	
管理状态	默认开启，开启后接口被软件层面启用。
自动协商	默认开启，自协商速率及双工模式。
速率	关闭自动协商后可进行配置，万兆口不支持修改速率。
双工模式	关闭自协商后可进行配置，支持半双工，全双工两种模式。
MTU	指定接口可发送报文最大长度，范围是 1280-1500。
管理访问	当前接口支持其它设备连接的方法，管理口支持：HTTP、HTTPS、PING、TELNET、SSH。 业务口额外增加支持 BGP、SSLVPN、OSPF、RIP、DNS、WEBAUTH。
外网口	接口属性，分为内网口及外网口两种，用于流量上下行统计。

注意：

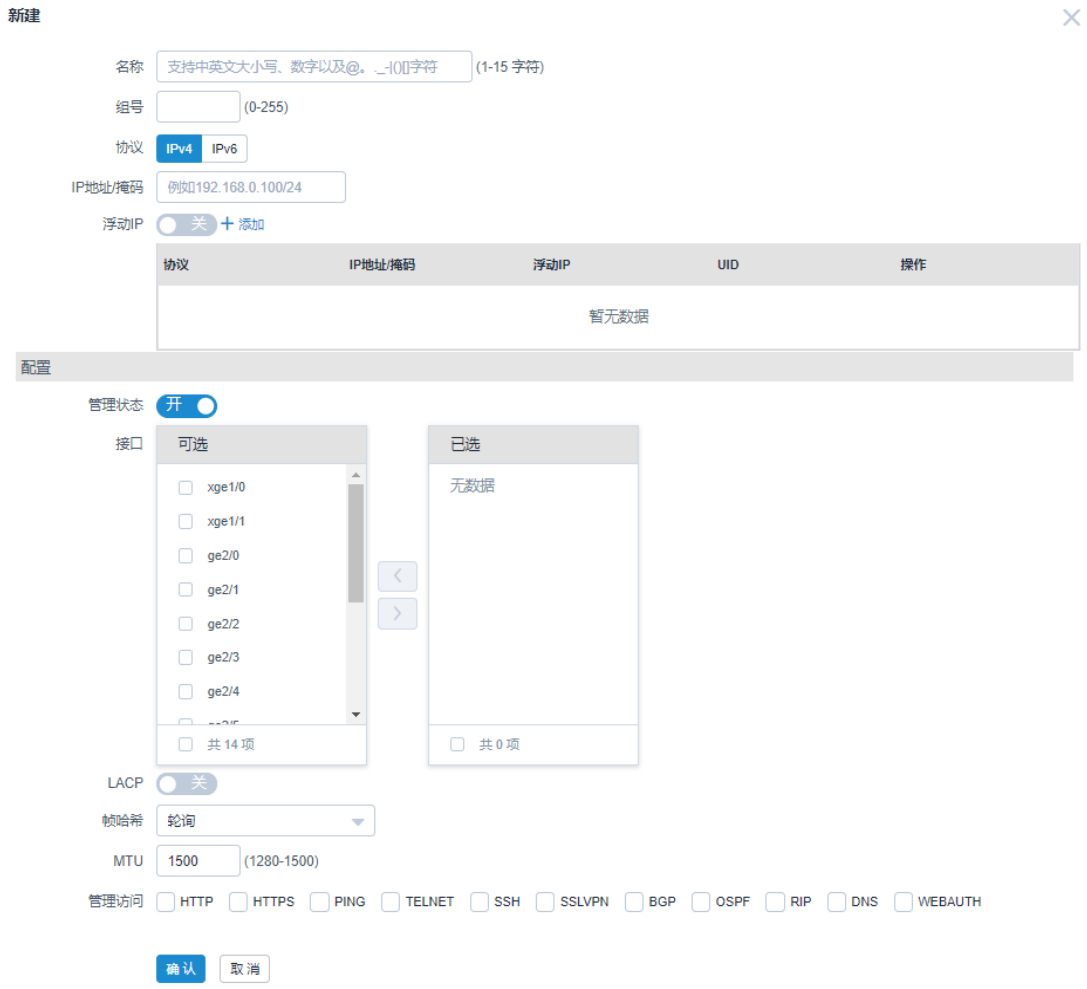
只有物理接口协商模式为非自协商时，速率、双工模式才是可配置项，当物理接口为光口时，协商模式变成灰色，即不可改状态。

5.1.2. 聚合接口

聚合接口是多个物理接口的集合，将多个物理接口进行捆绑，生成一个新逻辑接口，用于提升网络带宽，此外，流量同时由多个绑定的物理接口进行传输，具有链路冗余作用，其中一条或多条链路出现故障，剩余链路可继续工作分担流量。

在系统菜单点击“**网络>接口>聚合接口**”，进入**聚合接口**配置页面，显示设备上所有聚合口及接口状态信息。

用户可对聚合接口进行新建、修改、删除操作。在**聚合接口**页面点击<**新建**>创建新聚合接口，或选中一个聚合接口点击进行接口配置修改。



聚合接口的配置项与详细说明如下：

配置项	说明
名称	指定聚合接口名称。
组号	指定聚合接口 ID，范围是 0-255。
协议	支持 IPv4 及 IPv6 两种协议。
IP 地址/掩码	IPv4 地址格式，例如：A.B.C.D/M。IPv6 地址格式，例如：2000::1/64。
浮动 IP	开关按钮，打开后需选择 UID。
添加按钮	选择协议；输入 IP 地址/掩码；选择是否设置浮动 IP 后，点击添加可将 IP 地址添加到表格。

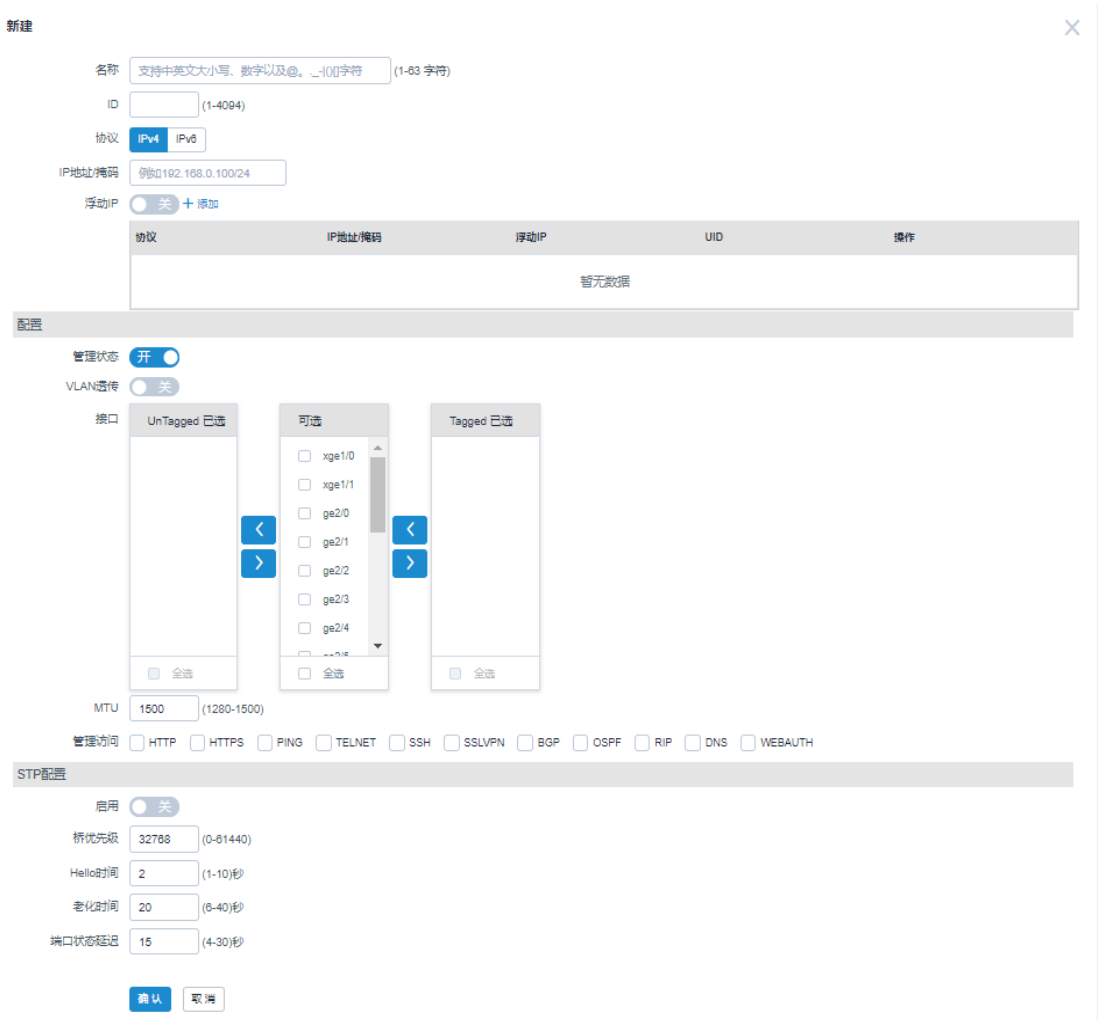
配置	
管理状态	默认开启，开启后接口被软件层面启用。
接口	左侧为全部物理口，选中后移动到右侧，表示需要绑定的物理口。
LACP	勾选后开启 LCAP 协议，默认关闭。
帧哈希	根据所选项进行帧哈希操作，默认为轮询，支持：轮询；源/目的 IP 哈希；源/目的 MAC 哈希；目的 IP 哈希；源 IP 哈希；源 MAC 哈希；目的 MAC 哈希。
MTU	指定接口可发送报文最大长度，范围是 1280-1500.
管理访问	当前接口支持其它设备连接的方法，支持：HTTP、HTTPS、PING、TELNET、SSH、SSLVPN、BGP、OSPF、RIP、DNS、WEBAUTH。

5.1.3. VLAN

VLAN（Virtual Local Area Network，虚拟局域网）是建立在物理网络基础上的逻辑子网。在一个物理局域网内，用户可将局域网内的设备分割为几个各自独立的群组，群组内部的设备之间可以自由通讯，而不同群组之间的设备通讯必须通过三层路由转发；通过这种方式，一个物理局域网被划分为多个相互隔离的局域网，这些不同的群组称为 VLAN。

在系统菜单点击“**网络>接口>VLAN**”，进入 **VLAN** 配置页面，可以看到设备上所有 VLAN 口及其状态信息。

用户可以对 VLAN 执行新建、编辑、删除操作。在 **VLAN** 页面点击<**新建**>创建新 VLAN，或点击编辑指定 VLAN。



VLAN 的配置项与详细说明如下：

配置项	说明
名称	指定 VLAN 接口名称。
ID	指定 VLAN ID，范围是 1-4094。
协议	支持 IPv4 及 IPv6 两种协议。
IP 地址/掩码	IPv4 地址格式，例如：A.B.C.D/M。IPv6 地址格式，例如：2000::1/64。
浮动 IP	开关按钮，打开后需选择 UID。

添加按钮	选择协议；输入 IP 地址/掩码；选择是否设置浮动 IP 后，点击添加可将 IP 地址添加到表格。
配置	
管理状态	默认开启，开启后接口被软件层面启用。
VLAN 透传	开启后可支持 VLAN 透明传输。
接口	左侧为全部可选接口，选中后移动到右侧，表示需要加入 VLAN 的接口。
MTU	指定接口可发送报文最大长度，范围是 1280-1500。
管理访问	当前接口支持其它设备连接的方法，支持：HTTP、HTTPS、PING、TELNET、SSH、SSLVPN、BGP、OSPF、RIP、DNS、WEBAUTH。
STP 配置	
启用	开关按钮，打开后启用 STP 功能。
桥优先级	生成树桥优先级，默认 32768，支持范围 0-61440。
Hello 时间	默认 2 秒，支持范围 1-10 秒。
老化时间	默认 20 秒，支持范围 6-40 秒。
端口状态延迟	默认 15 秒，支持范围 4-30 秒。

5.1.4. GRE 接口

GRE (Generic Routing Encapsulation，通用路由封装)是在网络上建立直接点对点连接的一种方法，目的是简化单独网络之间的连接。GRE 实现机制简单，对隧道两端的设备负担小。GRE 隧道可以通过 IPv4 网络连通多种网络协议的本地网络，有效利用了原有的网络架构，降低成本。

在系统菜单点击“**网络>接口>GRE 接口**”，进入 **GRE 接口**配置页面，可以查看设备中所有 GRE 接口及基本配置信息。

用户可对 GRE 接口进行新建、编辑、删除操作。在 **GRE 接口**页面点击<**新建**>创建新 GRE 接口，或点击编辑指定 GRE 接口。

GRE 接口的配置项与详细说明如下：

配置项	说明
GRE 组号	指定 GREID，范围是 0-2047。
名称	根据需要给接口定义一个名字。
IP 地址/掩码	GRE 接口 IP 地址，格式为 A.B.C.D/M。
隧道源地址	关闭时需选择隧道源接口，开启时可输入隧道源地址。
隧道源接口/隧道源地址	源接口为本地出接口，地址为本地连接对端设备的 IP。

动态 IP	关闭时需配置隧道对端地址，开启后无需配置隧道对端地址。
隧道对端地址	对端设备连接本端设备所用的 IP 地址。
隧道标示	标示隧道，范围是 1-9999。
Keep alive 间隔	开启后隧道持续时间，范围是 1-86400。
TTL	IP 包被路由器丢弃之前允许通过的最大网段数量,范围是 0-255。
MTU	指定接口可发送报文最大长度，范围是 1280-1420。
管理访问	当前接口支持其它设备连接的方法，支持：HTTP、HTTPS、PING、TELNET、SSH、SSLVPN、BGP、OSPF、RIP、DNS、WEBAUTH。

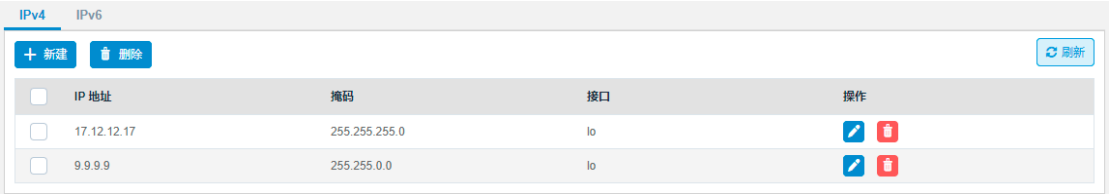
5.1.5. 环回接口

环回口习惯被称为 Loopback 接口，是逻辑虚拟接口。Loopback 接口创建后，除非手工关闭该接口，否则其永远处于 up 状态。由于其稳定性较高，可用于建立路由邻居，隧道连接，测试网络连通性等。

在系统菜单点击“网络>接口>环回接口”，进入环回接口配置页面，可以查看设备上所有环回接口及基本信息，环回接口支持配置 IPv4 及 IPv6 两种。

5.1.5.1. IPv4

在系统菜单点击“网络>接口>环回接口>IPv4”，进入 IPv4 页签，可以查看设备上所有环回接口及基本信息。



5.1.5.2. IPv6

在系统菜单点击“网络>接口>环回接口>IPv6”，进入 IPv6 页签，可以查看设备上所有环回接口及基本信息。

用户可对环回接口进行新建、编辑、删除操作。在**环回接口**页面点击<**新建**>创建新环回接口，或点击编辑指定环回接口。

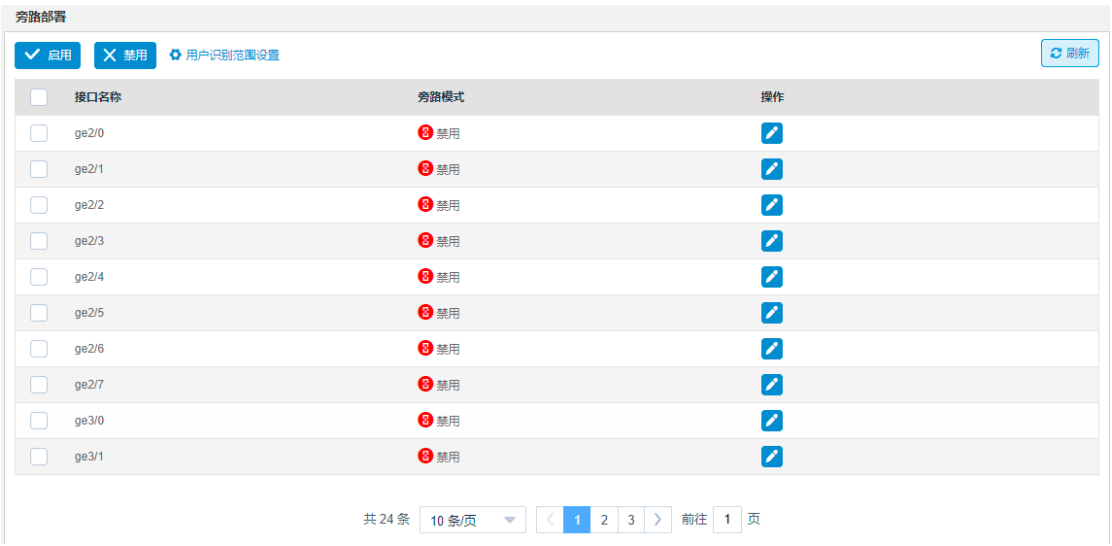
环回接口的配置项与详细说明如下：

配置项	说明
IP 地址	IPv4 地址或 IPv6 地址。
掩码	IPv4 环回口新建时需要填写掩码，IPv4 的地址格式为 A.B.C.D；IPv6 地址格式，例如：2000::1/64。
接口	默认选择 lo 口。

5.1.6. 旁路部署

在此工作模式中，网络的流量不会直接流经设备，而是由其它网络设备把需要检测的流量镜像一份给系统。在这种部署模式下，旁路设备不会影响网络的正常运行，但可以通过与防火墙联动等手段来阻断攻击。需要注意，开启旁路功能的接口，不会进行流量转发，仅用作流量安全监测。

在系统菜单点击“**网络**>**接口**>**旁路部署**”，进入**旁路部署**配置页面。



用户可对单个或多个接口进行旁路功能的启用或禁用，多个接口同时操作需要进行勾选后点击上方<**启用**><**禁用**>按钮，单个接口操作点击右侧进行，“用户识别范围设置”按钮支持修改用户识别范围，在旁路模式下，默认监测所有流量，用户可自己制定内网用户的 IP 地址监测范围。

用户识别范围设置展示如下：

用户识别范围设置的配置项与详细说明如下：

配置项	说明
识别范围	默认为 any，可点击下拉框选择识别范围的地址对象。可以点击<**添加**>按钮创建地址对象。

旁路接口配置展示如下：

接口旁路的配置项与详细说明如下：

配置项	说明
接口名称	选择的接口名称。
旁路模式	开关按钮，打开后接口开启旁路模式。

5.1.7. 端口镜像

端口镜像可以将一个或多个接口的数据流量复制到指定接口来实现对网络的监控。端口镜像功能是对网络流量监控的一个有效的安全手段，对监控流量的分析可以进行安全性的检查，同时也能及时地在网络发生故障时进行准确的定位。

在系统菜单点击“**网络>接口>端口镜像**”，进入**端口镜像**配置页面，查看设备上已有的端口镜像配置。点击图标编辑修改相应的端口镜像的配置。

点击<**新建**>，建立新的端口镜像。

端口镜像的配置项及详细说明如下：

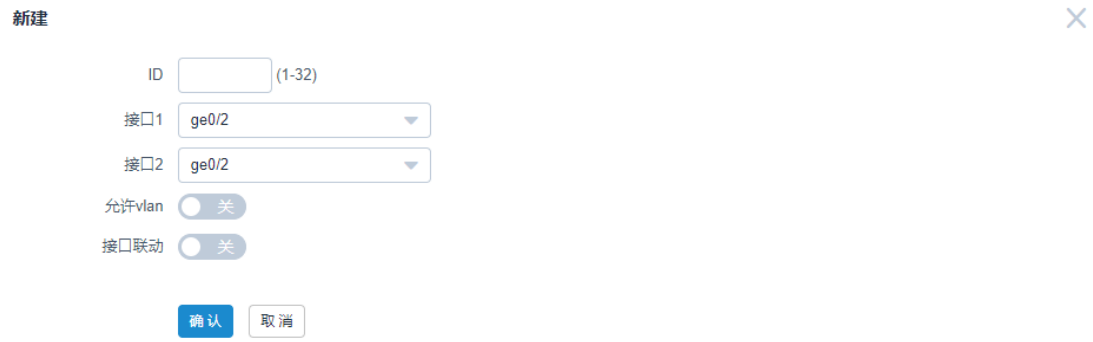
配置项	说明
名称	端口镜像规则的名称。
源接口	选择端口镜像的源接口，此接口上的流量将会被镜像到监控接口。
监控接口	选择端口镜像的监控接口（不可选择在线业务接口）。
规则类型	选择端口镜像的规则类型： ● **入流量**-镜像源接口的入流量。 ● **出流量**-镜像源-接口的出流量。 ● **双向流量**-镜像源接口的双向流量。

5.1.8. 虚拟网线

虚拟网线用于将设备上两个物理接口对应的子网直接连接到一起，被连接的两个子网之间可以直接进行二层通信。对于用户来说，虚拟网线是透明的，不影响已有网络结构。

在系统菜单点击“**网络>接口>虚拟网线**”，进入**虚拟网线**配置页面，查看设备上已有的虚拟网线配置。点击图标编辑修改相应的虚拟网线的配置。

点击<**新建**>，建立新的虚拟网线。



虚拟网线的配置项及详细说明如下：

配置项	说明
ID	新建虚拟网线的 ID。
接口 1	加入虚拟网线的第一个物理接口。
接口 2	加入虚拟网线的第二个物理接口。
允许 VLAN	不开启允许 VLAN，默认 tag/untag 报文都可以通过。开启允许 VLAN 之后，需要配置相应的 VLAN 允许范围,可填写范围为 0-4094，只能通过配置范围之内的 tag 或 untag 报文。
接口联动	开启接口联动后，接口 1、接口 2 中任意一个接口 DOWN 掉之后，另一个口也会自动 DOWN 掉。

5.2. 安全域

安全域是一组具有相同安全保护需求，并相互信任的接口组。可以在一个域中加入多个接口，但是一个接口只能属于一个域。如果一个接口被包含在某个域中，就不能单独对该接口进行配置。

在系统菜单点击“**网络>安全域**”，进入**安全域**界面，可以查看当前配置的安全域条目。

在主内容区点击<**新建**>创建新安全员，或编辑指定安全域，用户可以对安全域内的接口进行绑定或移出。

安全域配置项及详细说明如下：

配置项	说明
名称	安全域条目自定义命名。
域内接口互访	默认数据转发需要配置访问控制策略允许，当开启了域内接口互访功能后，该域内接口成员间的互访不会匹配访问控制策略而是直接转发。
接口成员	安全域作为接口组，表示该组下包含哪些成员。
可选	可以加入该安全域的接口成员。

已选	已经或即将加入该安全域的接口成员。

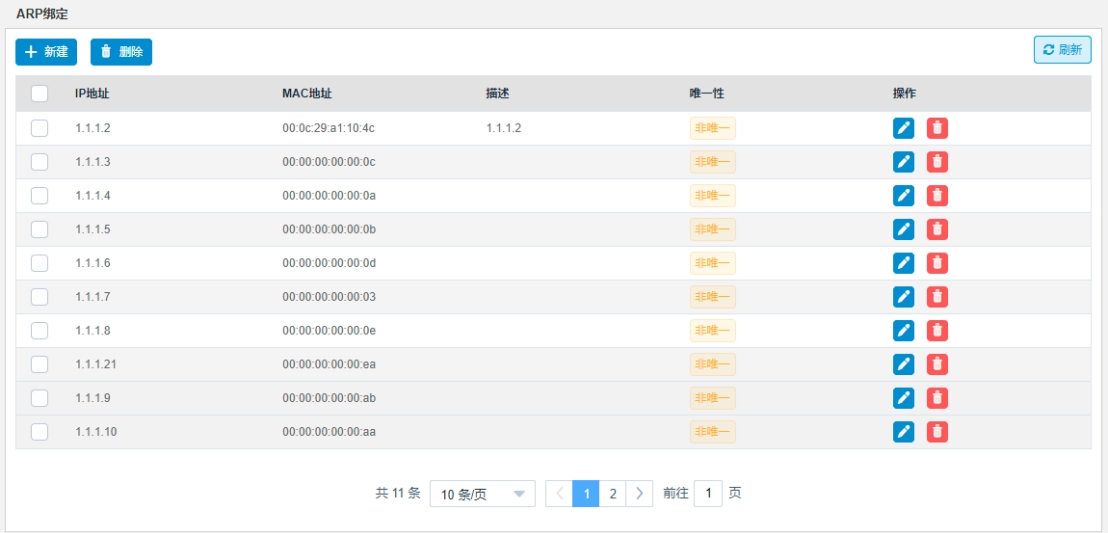
5.3. ARP

IP 数据包常通过以太网发送。以太网设备并不识别 32 位 IP 地址，它们是以 48 位以太网地址(MAC 地址)传输以太网数据包的。因此，IP 驱动器必须把 IP 地址转换成 MAC 地址。在这两种地址之间存在着某种静态的或算法的映射，常常需要查看一张表。地址解析协议(Address Resolution Protocol，ARP)就是用来确定这些映象的协议。
通常设备的 ARP 表是动态从网络中获得，但有很多场景需要在无法获得外界 ARP 的情况下向外发生数据，这就需要 ARP 功能来完成。

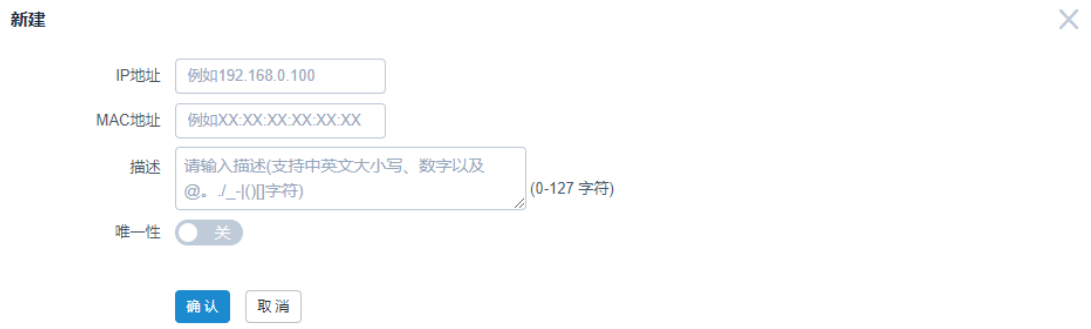
5.3.1. ARP 绑定

ARP 绑定是强制绑定某 IP 地址与某 MAC 地址的功能，通过该功能可以完成黑洞路由、直接发送 IP 数据等功能。

在系统菜单点击“**网络>ARP>ARP 绑定**”，进入 **ARP 绑定**配置页面，查看已有的 ARP 绑定。



在 ARP 绑定页面，点击<**新建**>按钮创建新的 ARP 绑定，或点击操作列的操作按钮修改已有的 ARP 绑定。



ARP 绑定配置项及详细说明如下：

配置项	说明
IP 地址	ARP 绑定的 IP 地址。
MAC 地址	ARP 绑定的 MAC 地址。
描述	ARP 绑定的描述信息，非必填项。
唯一性	默认关闭，开启唯一性开关后，同一个 IP 地址只能被一个 MAC 地址绑定，同一个 MAC 地址只能被一个 IP 地址绑定。

5.3.2. ARP

在系统菜单点击“网络>ARP>ARP”，进入 ARP 页面，查看设备上通过 ARP 学习到的所有 IP 地址及 MAC 地址。

在 ARP 页面，点击操作列的绑定按钮，对学习到的 IP 地址、MAC 地址进行绑定。点击操

作列的解绑按钮，对已绑定的 IP 地址、MAC 地址进行解绑。

5.3.3. 备份恢复

在系统菜单点击“**网络>ARP>备份恢复**”，进入**备份恢复**配置页面，进入备份恢复。

在**备份恢复**页面，点击<**导出**>按钮，可以将 ARP 绑定中的 IP-MAC 绑定表导出为 TXT 文件。

在**备份恢复**页面中，点击<**选择文件**>按钮，选择导入的 IP-MAC 绑定的配置文件，点击<**导入**>按钮，将选择的配置文件导入到系统配置中。

提示：

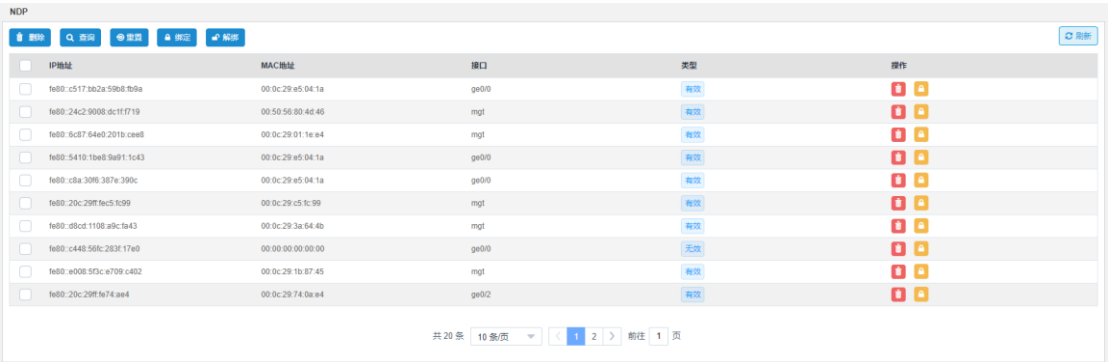
导入的 IP-MAC 绑定的配置文件，支持新建 IP-MAC 绑定和编辑已有的 IP-MAC 绑定。

5.4. NDP

NDP（Neighbor Discovery Protocol，邻居发现协议）在 IPv6 协议体系中占有重要的位置。IPv6 那些明显优于 IPv4 的特性，都依赖于 NDP 来实现。当一个 IPv6 节点在网络上新出现时，直接相连的链路上的其它 IPv6 节点可以通过邻居发现协议发现这个新节点，进而获得它的链路层地址。IPv6 节点也能通过邻居发现协议来查找路由器，维护处于活动状态的邻居节点的可达性信息。

5.4.1. NDP

在系统菜单点击“网络>NDP>NDP”，进入 NDP 配置页面，查看已有的 NDP。



在 NDP 页面，点击操作列的绑定按钮，对学习到的 IP 地址、MAC 地址进行绑定。点击操作列的解绑按钮，对已绑定的 IP 地址、MAC 地址进行解绑。

5.4.2. IP-MAC 绑定

IP-MAC 绑定是强制绑定某 IP 地址与某 MAC 地址的功能，通过该功能可以完成黑洞路由、直接发送 IP 数据等功能。

在系统菜单点击“**网络>NDP>IP-MAC 绑定**”，进入 **IP-MAC 绑定**配置页面，查看已有的 NDP 的 IP-MAC 绑定。

完成上述查看后点击<**新建**>可创建新的 IP-MAC 绑定条目。点击图标编辑修改相应的 IP-MAC 的配置。

IP-MAC 绑定配置项及详细说明如下：

配置项	说明
IP 地址	设置 IP-MAC 绑定中需要绑定的 IPv6 地址。
MAC 地址	设置 IP-MAC 绑定中需要绑定的 MAC 地址。
描述	NDP 绑定的描述信息，非必填项。
唯一性	默认关闭，开启唯一性开关后，同一个 IP 地址只能被一个 MAC 地址绑定，同一个 MAC 地址只能被一个 IP 地址绑定。

5.5. DHCP

本模块提供两种 DHCP 服务功能：DHCP 服务器和 DHCP Relay。设备作为 DHCP 客户端时,其配置请参考接口配置。

DHCP 服务器:DHCP 的全称是动态主机配置协议(Dynamic RG-WALL Configuration Protocol)。设备可以作为 DHCP Server，用于实现对网络中 IP 地址的动态分配和集中管理。动态分配是指当 DHCP 客户端第一次从 DHCP Server 租用到 IP 地址后，并非永久的使用该地址，只要租约到期，客户端就要释放(Release)这个 IP 地址以给其它工作站使用。为了实现 IP 地址的动态分配，必须设置 DHCP Server 拥有一个 IP 地址范围，用来分配给用户，这个用来分配给客户端的地址范围也叫 IP 地址池（IP Pool）。当客户端第一次登录到网络时，它会向网络广播一个 DHCP DISCOVER 消息，此时由于客户端还不知道自己属于哪一个网络，所以封包的来源地址为 0.0.0.0，目的地址则为 255.255.255.255。由于网络上可能不止一个 DHCP

服务器，凡是具有有效 IP 地址信息的 DHCP 服务器均从各自还没有租出的地址中选择一个空闲 IP，然后将该提议回应给客户端。客户端从接收到的第一个提议中选定 IP 地址信息，并广播一条租用地址的消息请求。由发出该提议的 DHCP 服务器响应该消息，确认已接受请求并开始租用，客户端收到确认后开始使用此地址。

DHCP Relay:DHCP 中继代理是用来将一个网段的 DHCP 请求转发给其它网段的 DHCP Server，由其它网段的 DHCP Server 分配 IP 地址。DHCP 中继代理存在的原因是因为 DHCP 客户端还没有 IP 环境设定,这时由 DHCP Relay 来接管客户的 DHCP 请求然后将 DHCP 消息传递给 DHCP Server，再将 DHCP 服务器的应答消息传给客户端，客户端获得 IP 地址。当然也可以在每一个网段之中安装 DHCP Server 但这样的话设备成本会增加而且管理上面也比较分散。

5.5.1. 服务

在系统菜单点击“**网络>DHCP>服务**”，进入**服务**页面，查看设备接口上启用的 DHCP 服务。

DHCP 服务配置项及详细说明如下：

配置项	说明
接口名称	显示需要配置 DHCP 服务的接口名称。
IP	该物理接口的 IP 地址。
类型	选择 DHCP 服务类型： ● **空**-不在接口上启用 DHCP 服务。 ● **DHCP 中继代理**-在接口上启用 DHCP 中继代理服务，并指定 DHCP 服务器 IP。代理从指定的 DHCP 服务器请求 IP 地址，并中继转发给接口。 ● **DHCP 服务器**-在接口上启用 DHCP 服务器服务。

DHCP 服务器	DHCP 服务器的 IP 地址。

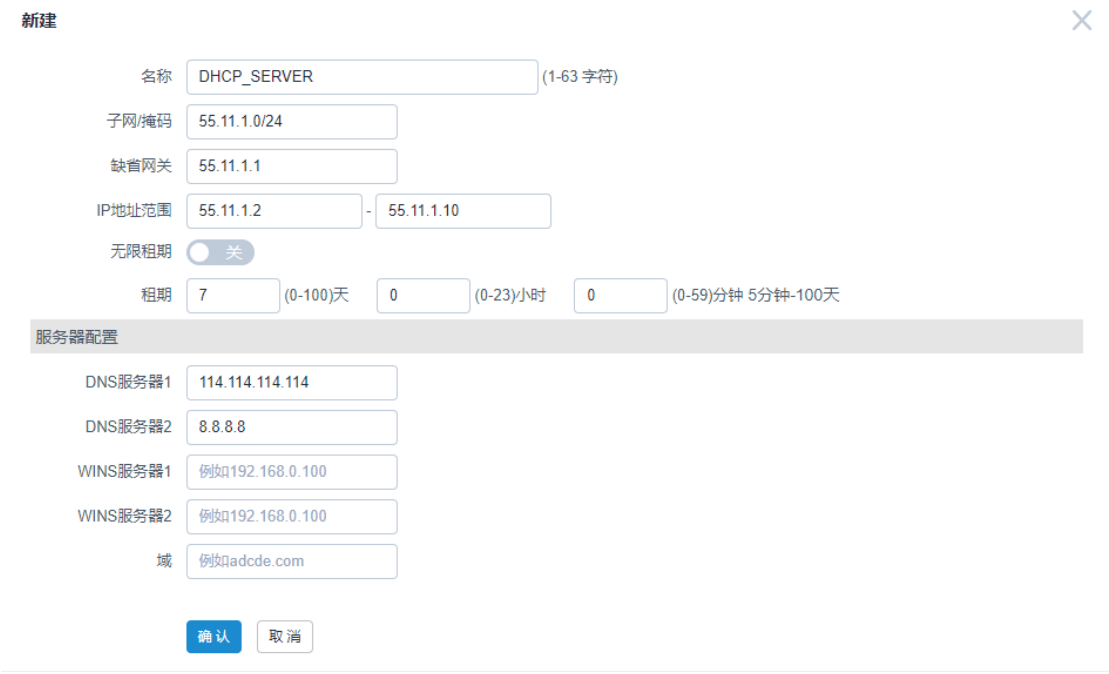
在“服务”页面的右侧“操作”栏中点击图标编辑指定接口下的 DHCP 的服务类型。

在编辑页面中，“类型”选择“DHCP 服务器”点击确认，如下图：

5.5.2. 服务器

在系统菜单点击“**网络>DHCP>服务器**”，进入**服务器**页面，显示出设备上配置的所有 DHCP 服务器。

完成上述查看后点击**<新建>**按钮创建新的 DHCP 服务器，或者在右侧操作栏中点击图标修改已存在的 DHCP 服务器配置。



DHCP 服务器配置项及详细说明如下：

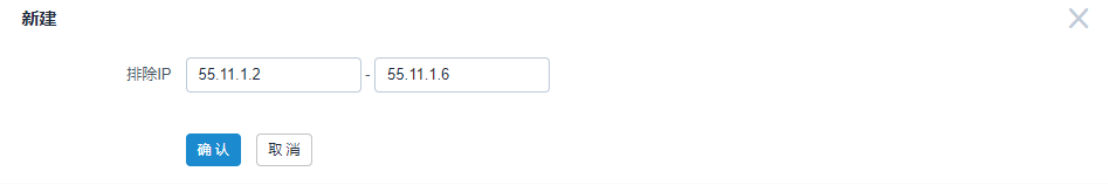
配置项	说明
名称	新建 DHCP 服务器的名称。
子网/掩码	DHCP 服务器的子网网段及掩码。
网关	DHCP 服务器的网关 IP 地址。
IP 地址范围	IP 地址池的范围。
租期	设置 DHCP 服务器所分配 IP 地址的租期时间，单位可以为天、小时、分钟，也可以配置为无限租期，如果不配置无限租期，租期到期后，客户端需要重新向 DHCP 服务器申请 IP 地址。
名称	新建 DHCP 服务器的名称。
服务器配置	
DNS 服务器 1	DHCP 服务器的主 DNS 服务器 IP 地址。
DNS 服务器 2	DHCP 服务器的备 DNS 服务器 IP 地址。
WINS 服务器 1	DHCP 服务器的主 WINS 服务器 IP 地址。

WINS 服务器 2	DHCP 服务器的备 WINS 服务器 IP 地址。
域	DHCP 服务器的域.

5.5.3. 排除范围

在系统菜单点击“**网络>DHCP>排除范围**”，进入**排除范围**配置页面，显示设备上配置的所有的 IP 地址排除范围，排除范围内的 IP 地址不能被分配下发。

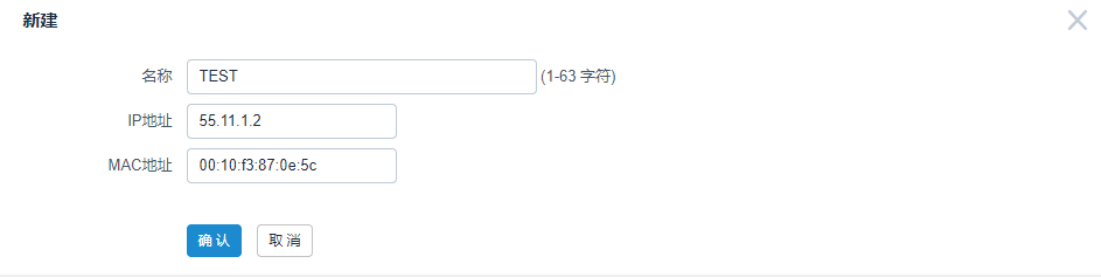
完成上述查看后点击<**新建**>创建新的 IP 地址排除范围，或者在右侧的操作栏中点击图标可修改已存在 IP 地址范围。



5.5.4. IP-MAC 绑定

在系统菜单点击“**网络>DHCP>IP-MAC 绑定**”，显示设备上配置的所有的 IP-MAC 绑定情况，该功能将用户的 IP 地址与 MAC 地址绑定在一起，当 DHCP 客户端由于关机、租期到期等原因。重新向服务器申请 IP 地址时，服务器会根据 IP-MAC 绑定将固定的 IP 地址分配给该客户端，该功能方便了网络管理员对进入网络的客户端设备进行管理。

完成上述查看后点击<新建>可创建新的 IP-MAC 绑定条目。



IP-MAC 绑定配置项及详细说明如下：

配置项	说明
名称	设置 IP-MAC 绑定的名称。
IP 地址	设置 IP-MAC 绑定中需要绑定的 IP 地址。
MAC 地址	设置 IP-MAC 绑定中需要绑定的 MAC 地址。

5.5.5. 监视器

在系统菜单点击“网络>DHCP>监视器”，进入监视器页面，查看到所有已分配出去的 IP 地址，其中还包括 MAC 地址、起始时间、结束时间等信息。

5.5.6. 备份恢复

在系统菜单点击“网络>DHCP>备份恢复”，进入备份恢复页面，看到 IP-MAC 绑定导入与 IP-MAC 绑定导出等功能。

点击<**导出**>按钮，将 IP-MAC 绑定表导出为 TXT 文件。

点击<**选择文件**>按钮，选择导出的 TXT 文件，再点击<**导入**>按钮，将 IP-MAC 绑定表导入。

5.6. DNS

DNS（Domain Name System，域名系统），因特网上作为域名和 IP 地址相互映射的一个分布式数据库，能够使用户更方便的访问互联网，而不用去记住能够被机器直接读取的 IP 数串。通过主机名，最终得到该主机名对应的 IP 地址的过程叫做域名解析（或主机名解析）。

5.6.1. DNS 服务器

DNS 服务器用来提供内网用户的域名解析功能。配置设备用来监听 DNS 报文的本地地址以及 DNS 转发器的地址。

在系统菜单点击“**网络>DNS>DNS 服务器**”，进入 **DNS 服务器**页面，进行 DNS 服务器的基础配置。

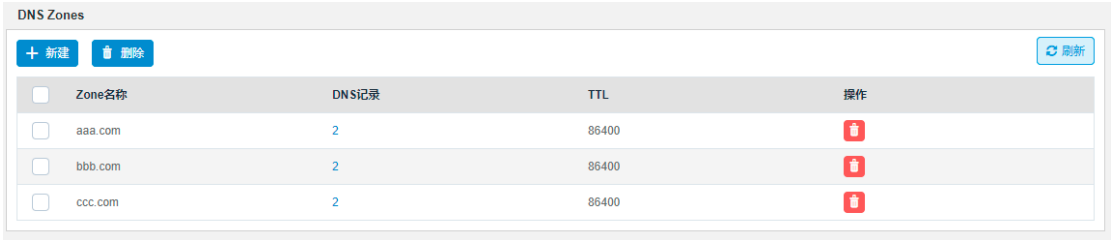
DNS 服务器配置项及详细说明如下：

配置项	说明
监听地址	可以勾选配置本地接口的 IP 地址来实现设备对于 DNS 报文的监听处理，接口包括：物理接口、聚合接口、GRE 接口、VLAN 接口、IPSec 隧道接口、SSL VPN 接口。
DNS 转发器地址	配置 DNS 转发器地址，主要实现本地 DNS 无法正常解析到的请求，转发给另一个已经配置好的 DNS 服务器。

5.6.2. DNS Zones

DNS 区域(ZONE)是 DNS 域名空间中连续的树，将域名空间按照需要划分为若干较小的管理单位。例如在 CCTV 中设置一个 DNS 服务器，这个 DNS 服务器将完成域名空间“cctv.com”下的域名解析工作，我们称这是一个区域。在 DNS 服务器中，必须先建立区域，在区域中建立子域，在区域或者子域中添加主机记录。一台 DNS 服务器可以管理一个或多个区域，而一个区域也可以由多台 DNS 服务器来管理。

在系统菜单点击“网络>DNS>DNS Zones”，进入 DNS Zones 页面，显示设备上配置的所有 DNS Zones 信息，在该页面可以对 DNS Zones 进行新建、查看和删除。



在 DNS Zones 页面下点击<新建>，进入到 DNS Zones 的配置中，进行 Zone 名称、SOA 记录服务器、NS 记录服务器的配置、点击<下一步>，可以配置 DNS Zone 的记录信息的配置，支持 A、NS、CNAME、MX、TXT、PTR、AAAA 记录的配置。

DNS Zone 新建页配置项及详细说明如下：

配置项	说明
Zone 名称	DNS Zone 名称配置。
SOA 记录信息主服务器	配置 SOA 记录服务器的地址。
TTL	设置有效地址解析记录的默认缓存时间。

NS 记录信息域名服务器	配置 NS 域名服务器的地址。

DNS Zone 下一步页配置项及详细说明如下：

配置项	说明
名称	配置 DNS 记录名称。
类型	配置 DNS 记录类型，可以选择 A、NS、CNAME、MX、TXT、PTR、AAAA 记录的配置。 A 记录：A 记录是用来指定主机名（或域名）对应的 IPV4 地址记录。 NS 记录：NS 记录是域名服务器记录，用来指定该域名由哪个 DNS 服务器来进行解析。 MX 记录：MX 记录是邮件交换记录，它指向一个邮件服务器，用于电子邮件系统发邮件时根据收信人的地址后缀来定位邮件服务器。 CNAME 记录：CNAME 别名记录，允许将多个名字映射到同一台计算机。 TXT 记录：一般指某个主机名或域名的说明。 AAAA 记录：AAAA 记录是用来指定主机名（或域名）对应的 IPV6 地址记录。

在 **DNS Zones** 页面下点击已有的 DNS Zones 的“DNS 记录”列下的数字，进入对应 DNS Zones 的 **DNS 记录**页面显示该 DNS Zones 下记录信息，在该页面可可以对 DNS Zones 的记录进行新建、查看和删除。

进入需要配置的 DNS Zone 的 **DNS 记录页面**点击<**新建**>，进入 DNS 记录创建，支持 A、NS、CNAME、MX、TXT、PTR、AAAA 记录的配置。

5.6.3. DNS 代理

DNS代理（或DNS透明代理）可以将主机发起的DNS请求转发到指定的DNS服务器上进行域名解析，并将DNS服务器返回的解析结果转发到主机。

使用DNS代理功能后，当DNS服务器的地址发生变化时，只需改变DNS代理上的配置，无需改变局域网内每个主机的配置，从而简化了网络管理。

DNS代理功能可以设置算法、优先级及权重完成DNS代理的负载均衡策略，最终实现对链路带宽资源的合理利用。

在系统菜单点击“**网络>DNS>DNS 代理**”进入 **DNS 代理**页面，显示设备上配置的所有 DNS 代理信息，在该页面可以实现对 DNS 的新建、修改和删除。

在 **DNS 代理**页面下点击<**新建**>创建新的 DNS 代理规则，或在右侧的“操作”列下点击图标修改的已有的 DNS 代理规则。

DNS 代理新建以及修改的配置项及详细说明如下：

配置项	说明
接口	选择 DNS 代理的出接口。
主服务器	配置 DNS 代理主 DNS 服务器地址。
备服务器	配置 DNS 代理备 DNS 服务器地址。
优先级	配置 DNS 代理优先级，可选范围为 1-32。
权重	配置 DNS 代理权重，可选范围为 1-100。

在 **DNS 代理**页面下点击<**DNS 配置**>，进入到 **DNS 配置**页面，可以对 DNS 代理功能的启用，算法和会话保持时间进行配置。

DNS 配置的配置项及详细说明如下：

配置项	说明
启用	配置 DNS 代理功能是否生效，该功能为全局配置。
算法	对 DNS 代理算法进行配置，支持三种算法：权重、优先级、流量。 基于权重算法： 根据权重值的比例转发 DNS 请求。例如，A 链路设置权重值 1，B 链路设置权重值 2，则 A 和 B 链路转发的 DNS 请求比例为 1:2。 基于优先级算法： 选择当前优先级值最小的 DNS 代理规则，各规则优先字段不允许重复且必须配置。例如，A 链路设置优先级 1，B 链路设置优先级 2，则 DNS 请求由 A 链路转发，此时链路 B 不转发 DNS 请求；当 A 线路发生故障后，继续由 B 链路转发 DNS 请求。 基于流量算法： 以各规则权重值做为分母，以当前接口速率做为分子分别相除计算链路的均衡值，选用当前均衡值最小的 DNS 代理规则。例如，A 链路均衡值为 1，B 链路均衡值为 2，则 DNS 请求由 A 链路转发，此时链路 B 不转发 DNS 请求；当 A 线路均衡值大于链路 B 时，继续由 B 链路转发 DNS 请求。
会话保持时间	配置 DNS 代理会话保持时间，可选参数为 15-1440min。 保证同一个源 IP 的 DNS 请求在一定时间内到同一台 DNS 服务器解析，设备保存有 DNS 代理缓存表，在会话保持时间内，存在表中 DNS 映射将不再匹配代理规则，直接使用上次代理服务器做 DNS 解析。

5.6.4. 特定域名解析

特殊域名需要指定到特定的 DNS 服务器才能解析。例如，域名 www.baidu.com 和 map.baidu.com 的 DNS 请求需要使用 DNS 服务器 2.2.2.2 进行解析。

在系统菜单点击“**网络>DNS>特定域名解析**”，进入**特定域名解析**页面，显示设备上配置的所有特定域名解析信息，在该页面可以实现对特定域名解析的新建、查询、修改和删除。

在**特定域名解析**页面下点击<**新建**>创建新的特定域名解析规则，或在右侧“**操作**”列下点击图标修改已有的特定域名解析规则。

特定域名解析配置项及详细说明如下：

配置项	说明
域名	配置特定域名信息。最多可以输入 255 个字符，可填入数字英文大小写字符、“-”、“.”，每级域名不超过 63 个字符。
主 DNS 服务器	配置特定域名解析的主 DNS 服务器地址。
备 DNS 服务器	配置特定域名解析的备 DNS 服务器地址。

在**特定域名解析**页面下点击<**查询**>可以对特定域名解析的主备 DNS 服务配置进行查询。

5.7. DDNS

动态域名解析（Dynamic DNS，简称 DDNS）是动态更新 DNS 服务器上域名和 IP 地址之间的对应关系，保证通过域名解析到正确的地址。防火墙通过 PPPOE 等方式接入互联网，由于每次获取到的 IP 是不同的，所以用户若通过此接口访问内网只能每次获取此接口的 IP

地址，这样不便于用户的使用。DNS 只是提供了域名和 IP 地址之间的静态对应关系，当 IP 地址发生变化时，DNS 无法动态的更新域名和 IP 地址之间的对应关系，从而导致访问失败。

在使用 DDNS 功能之前，用户需要在 DDNS 服务提供商进行注册，以获取动态域名。目前下一代防火墙支持花生壳、阿里云、公云和 freedns 服务商。

在系统菜单点击“**网络>DDNS**”，进入 **DDNS** 配置页面，可以实现对 DDNS 的新建、修改、删除和刷新。

在 **DDNS** 功能页面下点击<**新建**>创建新的 DDNS 服务条目，或在右侧“**操作**”列下点击图标编辑已有的 DDNS 服务条目。

DDNS 服务配置项及详细说明如下：

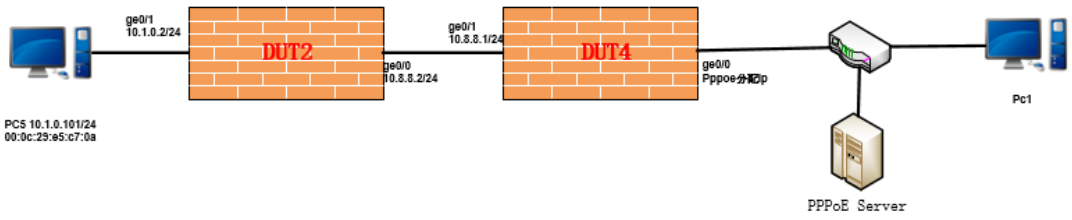
配置项	说明

启用	服务开启/关闭，说明：关闭 DDNS 服务只会将服务关闭，不会删除该接口上的 DDNS 配置。
接口	选择设备上应用 DDNS 服务的接口。
服务商	选择 DDNS 服务供应商。支持花生壳、阿里云、公云和 freedns。
域名	指定从 DDNS 服务商申请到的动态域名。
用户名	指定服务商上注册的用户名。
密码	指定用户名对应的密码。
日志	开启日志开关可记录 DDNS 日志。
更新间隔	指定 DDNS 请求更新间隔时间。启用 DDNS 的接口会定期向 DDNS 服务器发送请求更新动态 IP 地址与域名之间的绑定。默认 300 秒，支持范围 60-7200 秒。

5.7.1. DDNS 配置示例

组网需求

如下图所示，ge0/0 为通过 PPPOE 分配得到的 IP 地址，PC5 提供 HTTP 服务，要求通过 DDNS 实现域名 IP 动态绑定，通过目的 NAT 实现内网 HTTP 服务的地址映射，在 ge0/0 口 IP 地址发生变化时，仍可通过域名方式正常访问内网 HTTP 服务：



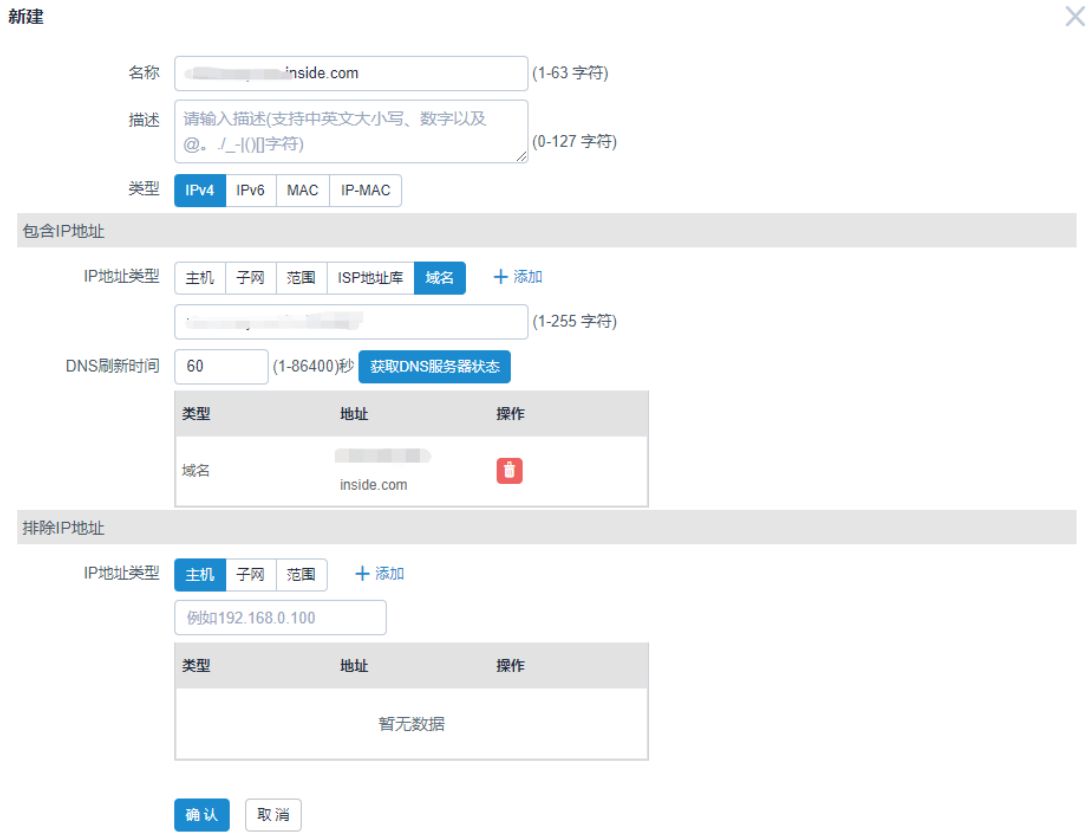
配置步骤

1. 在系统菜单点击“**系统>系统设置>DNS**”，进入 **DNS** 配置页面，按如下方式进行配置：

2. 在系统菜单点击“网络>DDNS”，进入 DDNS 配置页面，点击<新建>按如下方式进行配置：

3. 创建成功后，设备将于所配置服务商，此处为花生壳进行连接，并根据配置的更新间隔发送更新报文，显示当前更新的公网 IP 地址：

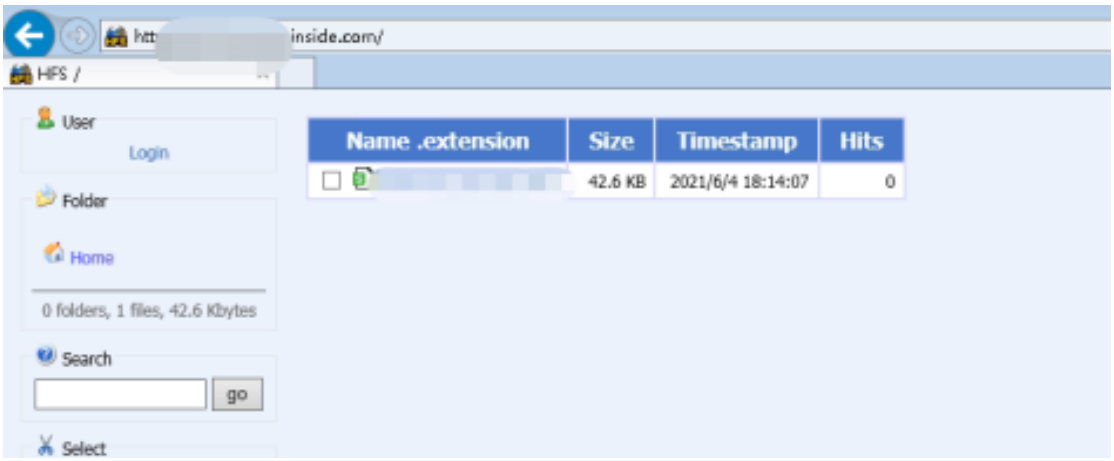
4. 在系统菜单点击“对象>地址>地址对象”，进入地址对象配置页面，点击<新建>将域名配置为步骤 2 所输入域名，即****inside.com，如下所示：



5. 在系统菜单点击“策略>NAT 策略>NAT 地址池”，进入 NAT 地址池配置页面，点击<新建>创建如下地址池：

6. 在系统菜单点击“策略>NAT 策略>目的 NAT”，进入目的 NAT 配置页面，点击<新建>创建如下目的 NAT 规则：

7. 创建完成后，在 Internet 访问 http://***inside.com，可正常访问内网的 HTTP 服务器，当外网口 IP 地址发生变更后，通过域名访问内网 HTTP 服务器正常：



5.8. IPv4 路由

路由是通过互联的网络将数据从源地址传输到目的地址的行为。通常路由器或其他路由设备使用路由选择协议动态的发现互联网中的网络，找出最佳数据传输路径，以最高效率将数据通过网络送达到目的地址。

5.8.1. 路由表

在系统菜单中点击“路由>IPv4 路由>路由表”，进入路由表页面。

路由表的显示项及详细说明如下：

显示项	说明
类型	路由的类型。
目的地址	指定路由的目的 IP 地址，格式为掩码长度或者点分十进制。
下一跳/出接口	指定路由的下一跳地址或者出接口。
权重	设置静态路由的权重，范围 1 到 100。如果存在多个下一跳，权重越大，该条路由命中的概率就越大。
距离	指定路由的管理距离，范围 1 到 255。管理距离是指路由协议的路由可信度。每种路由协议按可靠性从高到低依次分配一个信任等级，这个信任等级就叫管理距离。正常情况下，管理距离越小，优先级就越高，也就是可信度越高。对于两种不同的路由协议到同一个目的地的路由信息，路由器首先根据管理距离决定相信哪一个协议。
持续时间	路由持续的时长。
状态	路由的有效性。

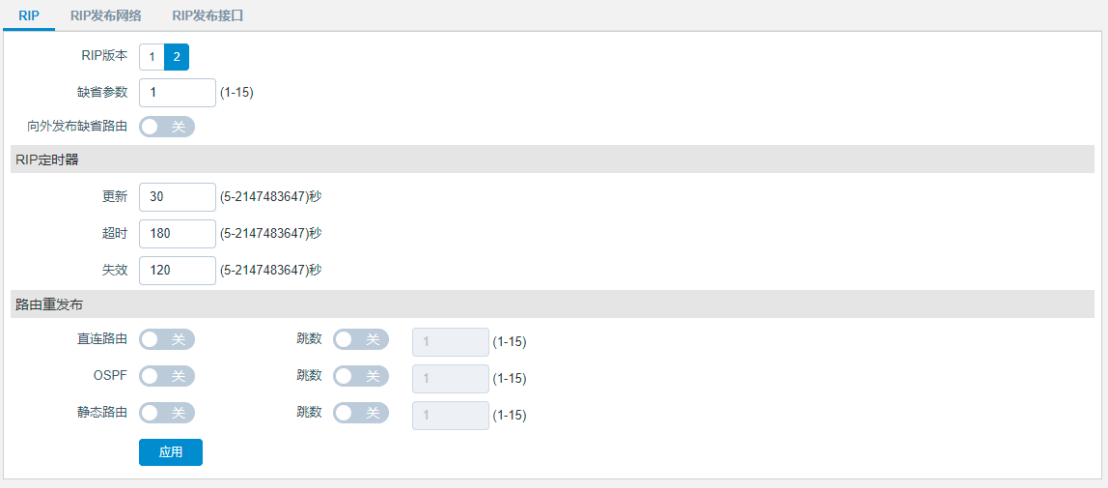
5.8.2. RIP

RIP 协议是一种基于 D-V 算法（又称为 Bellmen-Ford 算法）的内部动态路由协议（即 IGP, Interior Gateway Protocol）,它通过 UDP 数据报交换路由信息。D-V 算法又称为距离向量算法,这种算法在 ARPARNET 早期就用于计算机网络的路由的计算。RIP 协议在目前已成为路由器、主机路由信息传递的标准之一，是使用最广泛的 IGP 之一，被大多数 IP 路由器商业卖主广泛使用。RIP 协议被设计用于使用同种技术的中小型网络，因此适应于大多数的校园网和使用速率变化不是很大的连续的地区性网络。对于更复杂的环境，一般不使用 RIP 协议。

RIP 协议使用路由权即跳数来衡量到达目标主机的距离，RIP 协议使用两种形式的报文：路径信息请求报文和路径信息响应报文。在路由器端口第一次启动时，将会发送请求报文。路径信息响应报文包含了实际的路由信息，以每 30 秒的间隔发送给相邻端口。在 RIP 协议中，还使用了水平分割、毒性逆转机制来防止路由环的形成，并且使用触发更新和路由超时机制确保路由的正确性。

5.8.2.1. RIP

在系统菜单中点击“网路>IPv4 路由>RIP>RIP”，进入 RIP 协议配置页签。



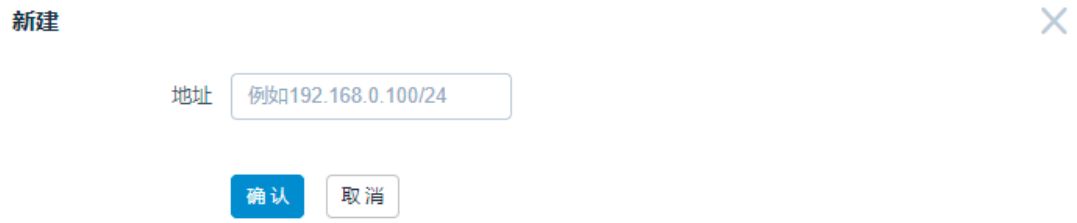
RIP 全局的配置项及详细说明如下：

配置项	说明
基础配置	
RIP 版本	选择 RIP 版本。
缺省参数	设置重发布路由的缺省跳数。
向外发布缺省路由	设置是否产生缺省路由并发布出去。
RIP 定时器	
更新	设置定时更新的触发时间，单位为秒。
超时	设置超时定时器的触发时间，单位为秒。
失效	设置垃圾收集定时器的触发时间，单位为秒。
路由器重发布	
直连路由	设置是否重发布直连路由。
OSPF	设置是否重发布 OSPF 路由。
静态路由	设置是否重发布静态路由。
跳数	三种重发布类型进行重发布时的度量。

5.8.2.2. RIP 发布网络

在系统菜单中点击“网路>IPv4 路由>RIP>RIP 发布”，进入 RIP 发布网络页签。

用户可在 RIP 发布网络页签，点击<新建>创建发布网络。



RIP 发布网络的配置项及详细说明如下：

配置项	说明
地址	对应要宣告的地址和子网掩码。

5.8.2.3. RIP 发布接口

在系统菜单中点击“网络>IPv4 路由>RIP>RIP 发布接口”，进入 RIP 发布接口页签。

用户可在 RIP 发布接口页签，点击<新建>创建发布接口。

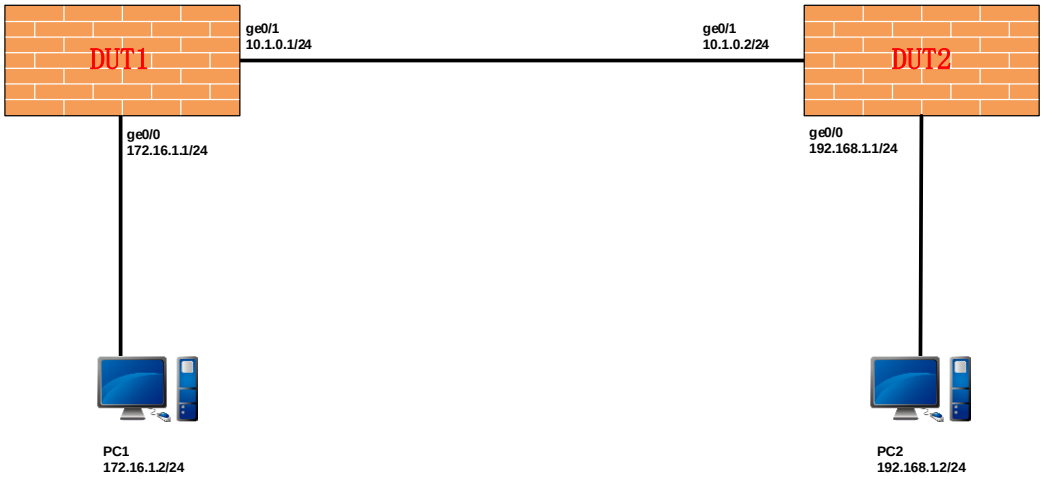
RIP 发布接口的配置项及详细说明如下：

配置项	说明
接口名称	需要进行配置的接口名。
发送版本	接口的发送报文版本。
接收版本	接口的接收报文版本。
认证算法	接口的认证类型：none、text、md5。

5.8.2.4. RIP 配置示例

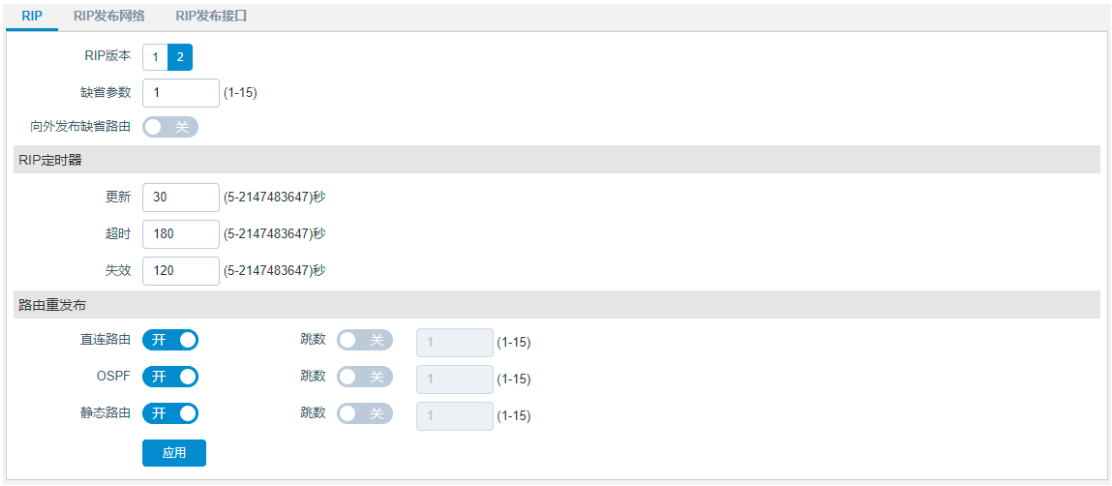
组网需求

如下图所示，配置接口 IP 地址，要求设备 DUT1 在 ge0/0 和 ge0/1 接口上启用 RIP 协议，设备 DUT2 在接口 ge0/0 和 ge0/1 上启用 RIP 协议，两台设备的互连接口收发报文的版本都设置为 2。PC1 ping PC2 的 IP 地址可通。

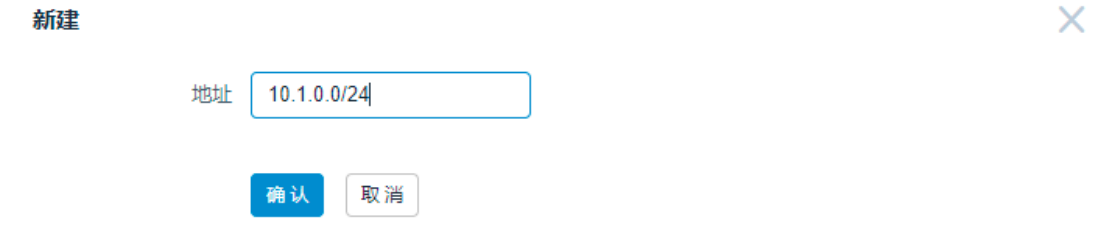


配置步骤

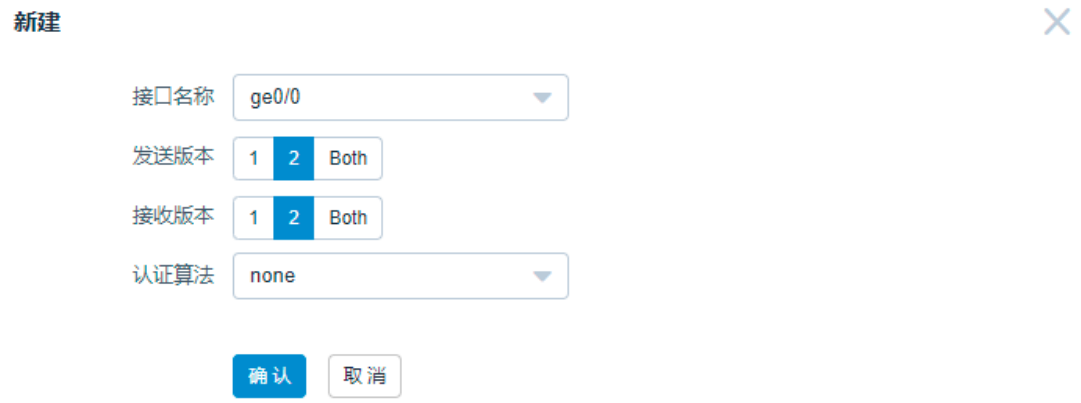
1. 在设备 DUT1 上，在系统菜单中点击“网络>IPv4 路由>RIP>RIP”，进入 RIP 配置页签配置 RIP 协议参数信息，具体信息请参考下图：



2. 在设备 DUT1 上，在系统菜单中点击“网络>IPv4 路由>RIP>RIP 发布网络”，进入 RIP 发布网络页签分别配置网络 10.1.0.0/24，172.16.1.0/24，具体信息请参考下图：



3. 在设备 DUT1 上，在系统菜单中点击“网络>IPv4 路由>RIP>RIP 发布接口”，进入 RIP 发布接口页签，点击<新建>分别在 ge0/0 和 ge0/1 接口上启用 RIP 协议并选择版本 2，具体信息请参考下图：



4. 设备 DUT2 请参考 DUT1 配置方法。

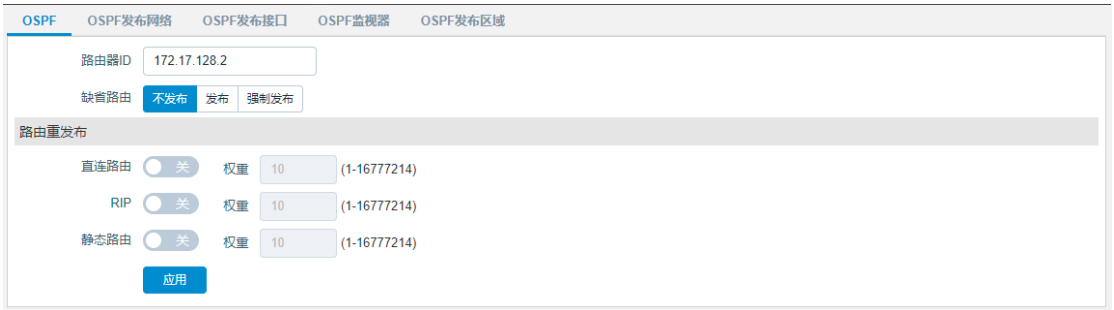
5. 配置完成后，在 PC1 上使用 ping 命令验证 PC2 可达。

5.8.3. OSPF

OSPF（开放最短路径优先协议，Open Shortest Path First）是 IETF 组织开发的一个基于链路状态的内部网关协议，其最重要的特点之一是快速收敛：在网络拓扑结构发生变化时会立即发送更新报文，在自治系统（AS）中同步变化信息。OSPF 协议可支持大规模网络，允许将自治系统的网络划分为区域进行管理，从而减少 CPU 和内存使用率；此外 OSPF 使用最短路径树算法计算路由，算法本身可以保证不会生成自环路由。

5.8.3.1. OSPF

在系统菜单点击“网络>IPv4 路由>OSPF>OSPF”，进入 OSPF 页签，显示 OSPF 功能配置信息。



OSPF 的配置项及详细说明如下：

配置项	说明
路由器 ID	指定 OSPF 路由器 ID，默认取值为设备上接口状态 UP 的物理接口中最大的 IP 地址作为设备的路由器 ID。路由器 ID 可手动修改，不同设备的路由器 ID 请配置不同值。格式为点分十进制 IP 格式。
缺省路由	设置是否向邻接设备下发缺省路由信息，默认为**不发布**。 开启此功能为**发布**状态时，如果系统中存在缺省路由时，才会向邻居设备发布缺省路由信息。 开启此功能为**强制发布**状态时，如果系统中不存在缺省路由也会向邻居设备发布缺省路由信息。
路由重发布	
直连路由	开启此功能后，设备会通过 OSPF 协议重发布本系统中的直连路由信息给邻居设备，重发布时可指定此类路由的权重值。
RIP	开启此功能后，设备会通过 OSPF 协议重发布本系统中的 RIP 路由信息给邻居设备，重发布时可指定此类路由的权重值。
静态路由	开启此功能后，设备会通过 OSPF 协议重发布本系统中的静态路由信息给邻居设备，重发布时可指定此类路由的权重值。

5.8.3.2. OSPF 发布网络

在系统菜单点击“网络>IPv4 路由>OSPF>OSPF 发布网络”，进入 OSPF 发布网络页签，显示设备上的所有 OSPF 发布的网络信息。

在 OSPF 发布网络页面下，点击<新建>按钮，创建新的 OSPF 发布网络信息，或在右侧“操作”列下点击图标修改已有的 OSPF 发布网络配置。

OSPF 发布网络的配置项及详细说明如下：

配置项	说明
网络	配置系统中需要启用 OSPF 协议的网络信息，格式为“IP 地址/掩码”，例如 192.168.0.100/24。
区域	指定发布的网络所对应的 OSPF 协议的区域 ID，格式为“0-4294967295 或 IP 地址”。只有区域 ID 相同，启用了 OSPF 协议的设备之间才可能成为邻居。

5.8.3.3. OSPF 发布接口

在系统菜单点击“网络>IPv4 路由>OSPF>OSPF 发布接口”，进入 OSPF 发布接口页签，显示设备上的所有 OSPF 发布的接口信息。

在 OSPF 发布接口页面下，点击<新建>按钮，创建新的 OSPF 发布接口信息，或在右侧“操作”列下点击图标修改已有的 OSPF 发布接口配置。

OSPF 发布接口的配置项及详细说明如下：

配置项	说明
接口	选择需要开启 OSPF 协议的接口。
优先级	配置接口的优先级，默认值为 1，优先级值范围为 0-255。优先级值为 0 时不参与选举指定路由器\备份指定路由器，当优先级值非 0 时，具有高优先级值的设备会被选为网络中的指定路由器。
发送开销	发送报文的开销值（cost）。默认值为 0，优先级值范围为 0-65535。0 表示根据接口类型和速率自动计算。
网络类型	接口的 OSPF 网络类型，支持配置 Broadcast（广播）、Point-to-Point（点到点）类型，默认类型为 Broadcast。
认证算法	OSPF 邻居协商时认证类型。支持配置的算法有 None（不认证）、

	Text（明文认证）、MD5（密文认证），默认算法为 None。
计时	
Hello 间隔	Hello 报文发送间隔时间。Hello 报文来用进行 OSPF 邻居发现、定期发送 Hello 报文进行邻居状态保活。默认值为 10 秒，范围为 1-65535 秒。
重传间隔	LSA（链路状态通告）消息重传间隔时间。默认值为 5 秒，范围为 3-65535 秒。
Dead 间隔	邻居路由器失效间隔时间，如果接口在指定的 Dead 间隔时间内没有收到邻居发来的 Hello 报文，则认为邻居已经失效。默认值为 40 秒，范围为 1-65535 秒。
发送延迟	LSA（链路状态通告）消息发送延迟时间。默认值为 1 秒，范围为 1-65535 秒。

5.8.3.4. OSPF 监视器

在系统菜单点击“网络>IPv4 路由>OSPF>OSPF 监视器”，进入 OSPF 监视器页签，显示设备上的所有 OSPF 邻居状态信息。

OSPF 监视器的信息项及详细说明如下：

信息项	说明
邻居路由器 ID	对端邻居设备的路由器 ID 信息。
邻居路由器地址	对端邻居设备建立邻居使用的 IP 地址。
优先级	对端邻居设备的优先级。
系统状态	邻居建立状态信息及路由器信息。
超时	Dead 间隔剩余时间。

接口	与对端设备建立邻居使用的接口。

5.8.3.5. OSPF 发布区域

在系统菜单点击“网络>IPv4 路由>OSPF>OSPF 发布区域”，进入 OSPF 发布区域页签，显示设备上的所有 OSPF 发布区域信息。

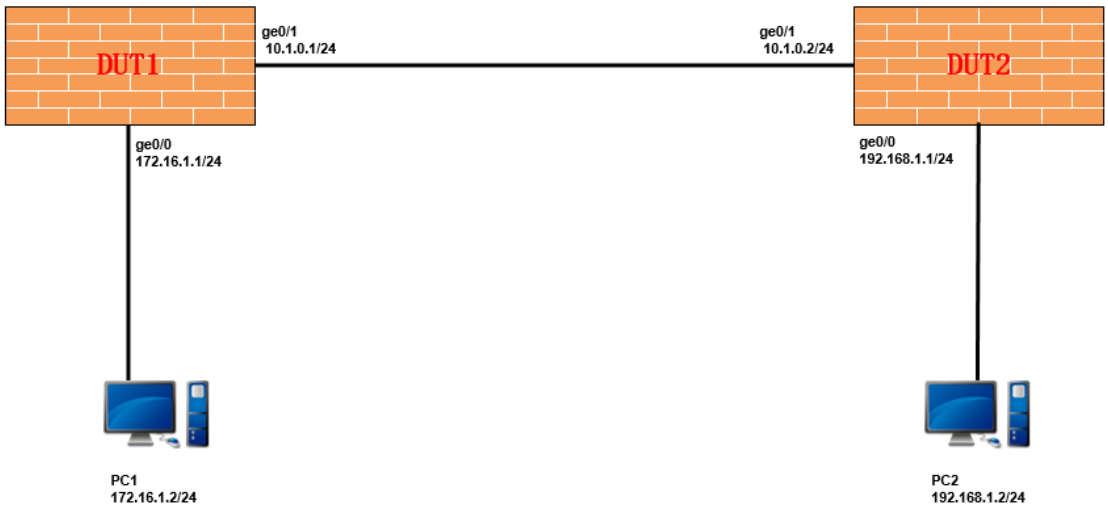
OSPF 发布区域的信息项及详细说明如下：

信息项	说明
发布区域	OSPF 的发布网络的区域
认证算法	OSPF 发布区域的认证算法。例如：None（不认证）、Text（明文认证）、MD5（密文认证）

5.8.3.6. OSPF 配置示例

组网需求

如下图所示， DUT1 是 PC1 的网关设备、DUT2 是 PC2 的网关设备。要求设备 DUT1 与 DUT2 启用 OSPF 协议，DUT1 设备上能学习到 192.168.1.0/24 网段的 OSPF 路由，DUT2 设备上能学习到 172.16.1.0/24 网段的 OSPF 路由，PC1 ping PC2 的 IP 地址可通。



配置步骤

1. 在设备 DUT1 上，在系统菜单点击“网络>IPv4 路由>OSPF>OSPF”，进入 OSPF 页签配置 OSPF 协议参数信息，具体信息请参考下图并点击<应用>：

2. 在设备 DUT1 上，在系统菜单点击“网络>IPv4 路由>OSPF>OSPF 发布网络”，进入 OSPF 发布网络页签点击<新建>按钮配置需要新建的 OSPF 发布网络信息，具体信息请参考下图并点击<确认>：

3. 在设备 DUT1 上，在系统菜单点击“**网络>IPv4 路由>OSPF>OSPF 发布接口**”，进入 **OSPF 发布接口**页签点击<**新建**>按钮配置需要新建的 OSPF 发布接口信息，具体信息请参考下图并点击<**确认**>：

4. DUT2 设备请参考 DUT1 设备配置方法。

5. 配置完成后，PC1 对 PC2 进行 ping 测试，PC 间访问可以互通。

5.8.4. BGP

BGP（Border Gateway Protocol）是一种不同自治系统的路由器之间进行通信的外部网关协议(Exterior Gateway Protocol，EGP)，其主要功能是在不同的自治系统(Autonomous Systems，AS)之间交换网络可达信息，并通过协议自身机制来消除路由环路。

BGP 使用 TCP 协议作为传输协议，通过 TCP 协议的可靠传输机制保证 BGP 的传输可靠性。

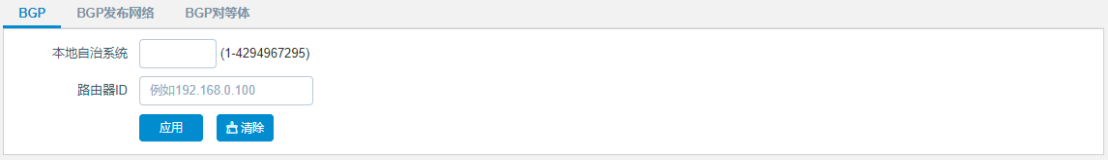
运行 BGP 协议的 Router 称为 BGP Speaker，建立了 BGP 会话连接(BGP Session)的 BGP Speaker 之间被称作对等体(BGP Peers)。BGP speaker 之间建立对等体的模式有两种：

IBGP(Internal BGP)和 EBGP(External BGP)。IBGP 是指在相同 AS 内建立的 BGP 连接，EBGP 是指在不同 AS 之间建立的 BGP 连接。二者的作用简而言之就是：EBGP 是完成不同 AS 之间路由信息的交换，IBGP 是完成路由信息在本 AS 内的过渡。

5.8.4.1. BGP

BGP 协议需要路由器 ID，作为本路由器在自治系统中的唯一标识。一般在协议任务启动后，下一代防火墙设备会选择状态 up 的接口地址大的作为本路由器 ID，也可以指定一个路由器 ID。

在系统菜单中点击“网络>IPv4 路由>BGP>BGP”，进入 BGP 配置页签。



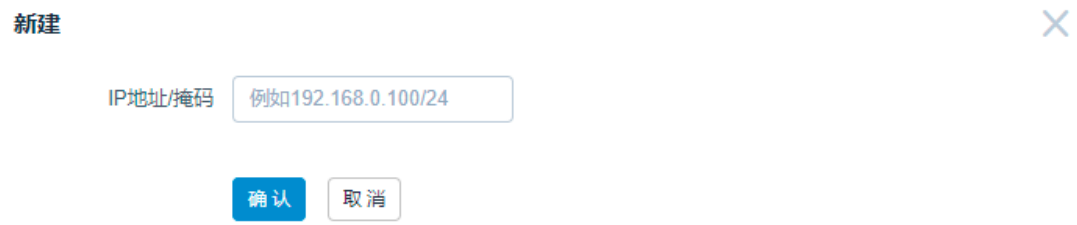
BGP 的配置项及详细说明如下：

配置项	说明
本地自治系统	本地自治系统的 ID，用户指定。
路由器 ID	指定路由器 ID。如果不输入，点击确认后系统会自动选取路由器 ID。

5.8.4.2. BGP 发布网络

在系统菜单中点击“网络>IPv4 路由>BGP>BGP 发布网络”，进入 BGP 发布网络配置页签。

用户可在 BGP 发布网络页签点击<新建>，创建发布网络。



BGP 发布网络的配置项及详细说明如下：

配置项	说明
IP 地址/掩码	对应要宣告的地址和子网掩码。

5.8.4.3. BGP 对等体

在系统菜单中点击“网络>IPv4 路由>BGP>BGP 对等体”，进入 BGP 对等体配置页签。

用户可在 BGP 对等体页签点击<新建>，创建 BGP 对等体。

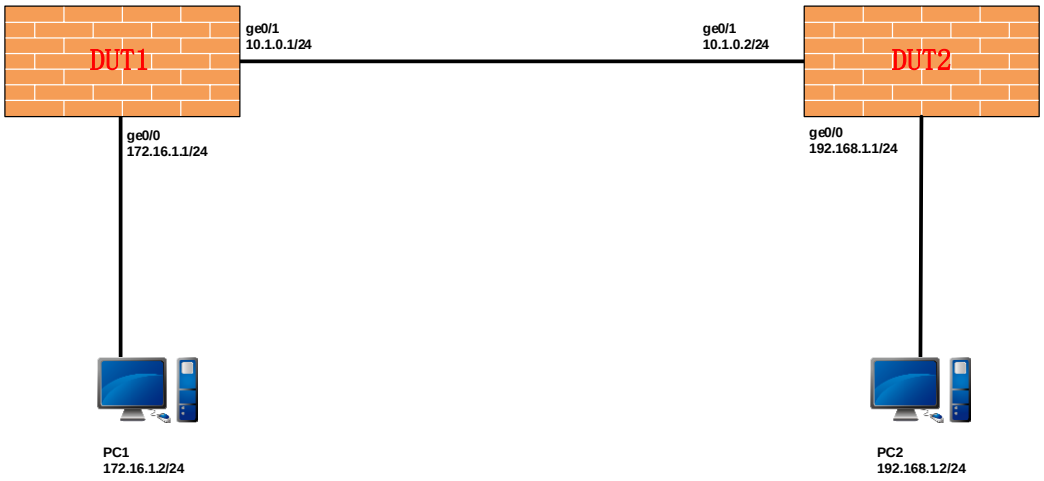
BGP 对等体的配置项及详细说明如下：

配置项	说明
IP 地址	远端对等体的地址。
远端 AS	远端对等体的自治系统的 ID。

5.8.4.4. BGP 配置示例

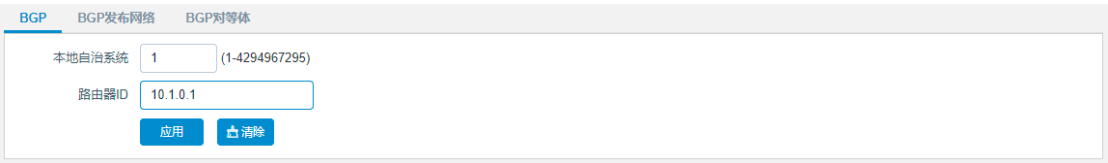
组网需求

如下图所示，配置接口 IP 地址，要求设备 DUT1 在 ge0/1 接口上启用 BGP 协议，设备 DUT2 在接口 ge0/1 上启用 BGP 协议。PC1 ping PC2 的 IP 地址可通。

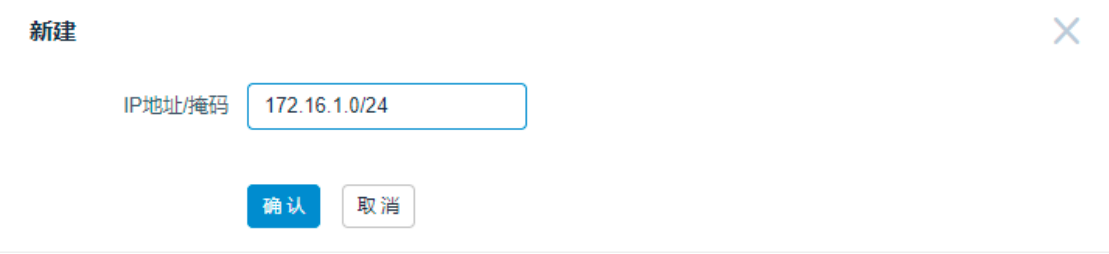


配置步骤

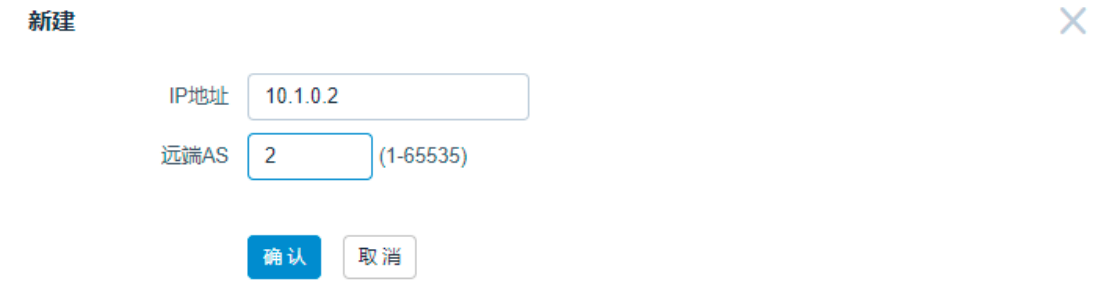
1. 在设备 DUT1 上，在系统菜单中点击“网络>IPv4 路由>BGP>BGP”，进入 BGP 配置页签，具体信息请参考下图：



2. 在设备 DUT1 上，在系统菜单中点击“网络>IPv4 路由>BGP>BGP 发布网络”，进入 BGP 发布网络页签，配置网络 172.16.1.0/24，具体信息请参考下图：



3. 在设备 DUT1 上，在系统菜单中点击“网络>IPv4 路由>BGP>BGP 对等体”，进入 BGP 对等体页签，点击<新建>IP 地址和远端 AS，具体信息请参考下图：



4. 设备 DUT2 请参考 DUT1 配置方法。

5. 配置完成后，在 PC1 上使用 ping 命令验证 PC2 可达。

5.8.5. 静态路由

静态路由是用户在设备的路由表中手动添加的固定路由，适用于网络规模较小、拓扑结构固定的网络环境中。静态路由的优点是简单、高效、可靠、几乎不增加 CPU 负载。在所有路由中，静态路由的优先级最高，静态路由与动态路由发生冲突时，系统会以静态路由为准。

在系统菜单中点击“网络配置>IPv4 路由>静态路由”，进入静态路由页面。

用户可在**静态路由**页面下，点击<**新建**>，创建新的静态路由，或在右侧“操作”列下点击图标修改已有的静态路由配置。

静态路由的配置项及详细说明如下：

配置项	说明
IP 地址/掩码	指定静态路由的目的 IP 地址及掩码。
下一跳类型	指定静态路由的下一跳地址的类型。
下一跳地址/出接口	指定静态路由下一跳地址或者出接口。
权重	设置静态路由的权重，范围 1 到 100。如果存在多个下一跳负载均衡，权重越大，该条路由命中的概率就越大。
距离	指定静态路由的管理距离，范围 1 到 255。管理距离是指路由协议的路由可信度。每种路由协议按可靠性从高到低依次分配一个信任等级，这个信任等级就叫管理距离。正常情况下，管理距离越小，优先级就越高，也就是可信度越高。对于两种不

	同的路由协议到同一个目的地的路由信息，下一代防火墙设备首先根据管理距离决定相信哪一个协议。
健康检查	设置对静态路由下一跳的健康检查，根据探测到的结果更新路由表中对应路由条目的有效性。

5.8.6. 策略路由

策略路由（Policy Based Routing）是指在决定一个 IP 报文的下一跳转发地址时，不是简单的根据目的或源 IP 地址决定，而是基于预先配置的策略将报文转发到指定的接口。接口启用策略路由后，将对该接口接收到的所有报文进行检查，符合用户定义策略的报文按照该策略中定义的操作进行处理，不符合任何策略的报文按照其他路由转发进行处理。

在系统菜单中点击“**网络>IPv4 路由>策略路由**”，进入**策略路由**页面。

用户可在**策略路由**页面下，点击<**新建**>，添加策略路由，或在右侧“操作”列下点击图标 修改已有的策略路由。

策略路由的配置项及详细说明如下：

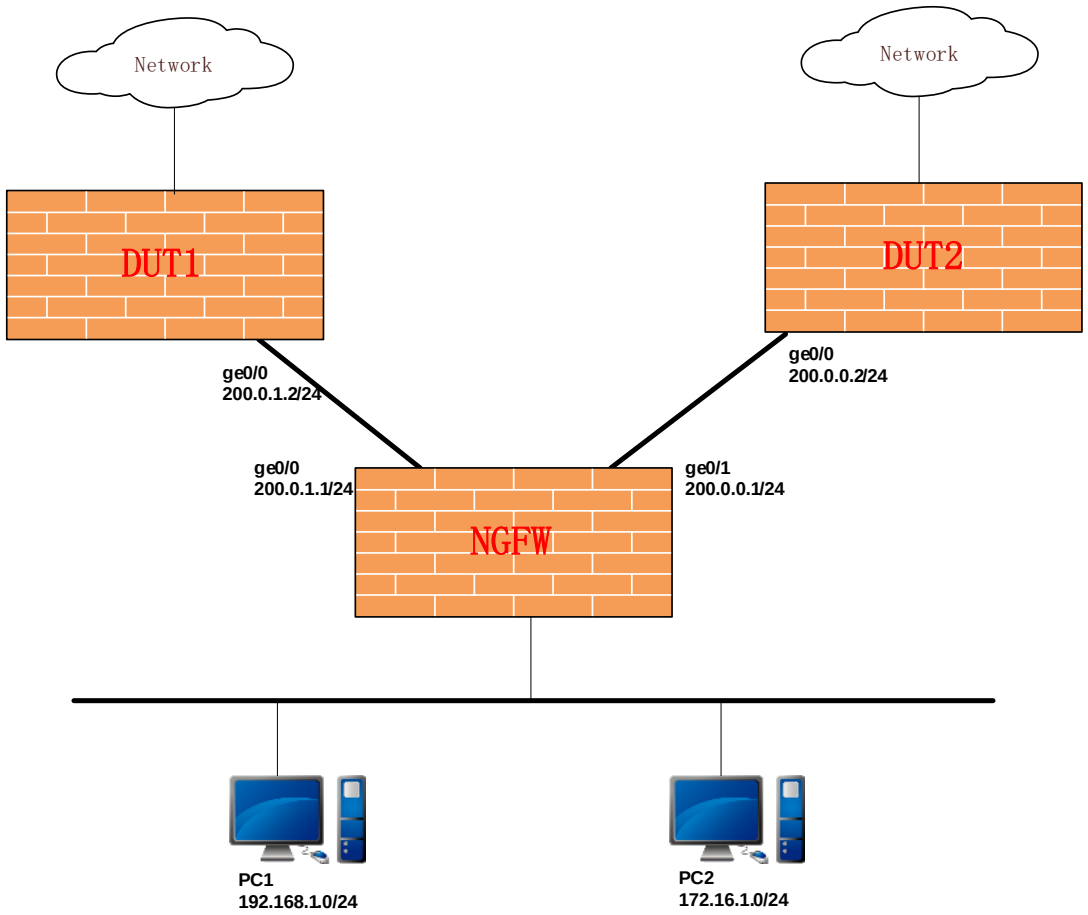
配置项	说明
启用	启用或者禁用策略路由。
入接口	指定策略路由的入接口。
源地址	指定策略路由规则的源地址，可以为 IP 地址、地址范围、主机地址或域名。有关地址配置的更多信息，请参考地址。
目的地址	指定策略路由规则的目的地址，可以为 IP 地址、地址范围、主机地址或域名。有关地址配置的更多信息，请参考地址。
用户	指定策略路由规则的用户对象，可以为用户或用户组。有关用户配置的更多信息，请参考用户对象。
服务	指定策略路由规则的服务对象，可以为服务或服务组。有关服务配置的更多信息，请参考服务。
应用	指定策略路由规则的应用对象。
时间表	指定策略路由的生效时间。请参考时间。

下一跳信息	
类型	支持选择网关或出接口。
网关	支持填写网关或出接口。
健康检查	设置对策略路由下一跳的健康检查，根据探测到的结果更新路由表中对应路由条目的有效性。
权重	设置静态路由的权重，范围 1 到 255。如果存在多个下一跳负载均衡，权重越大，该条路由命中的概率就越大。
多路径选择	可选根据源 IP 或根据连接进行哈希计算下一跳。

5.8.6.1. 策略路由配置示例

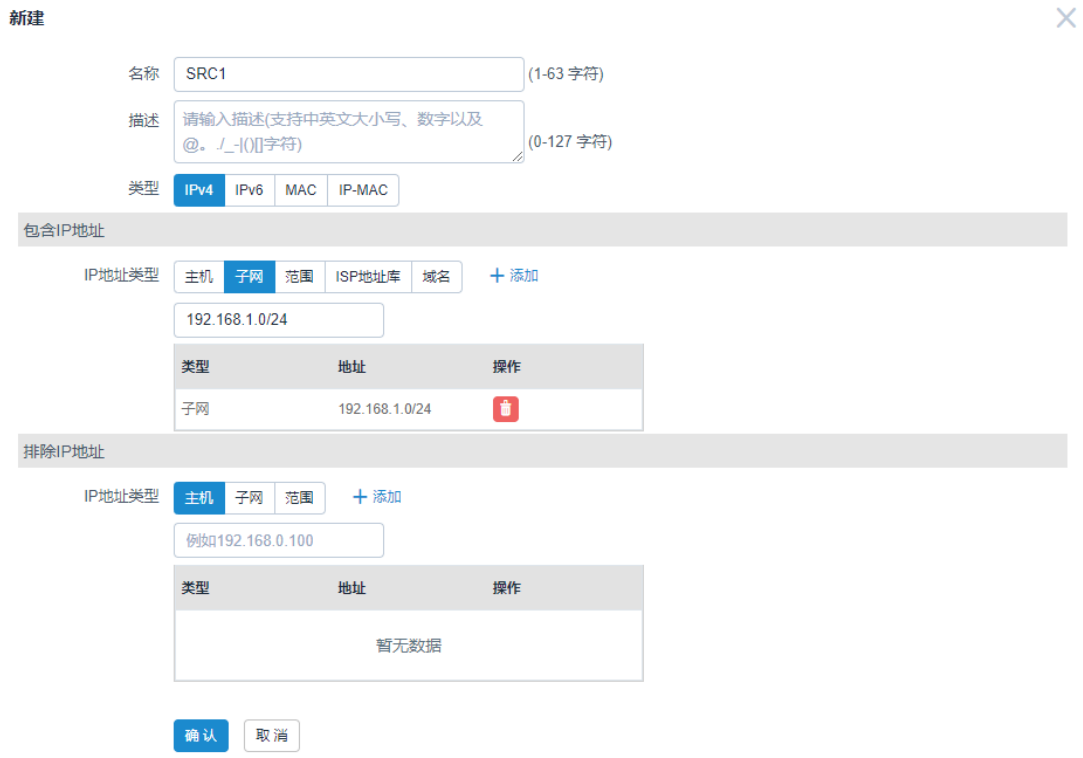
组网需求

如下图所示，配置接口 IP 地址，要求将来自 192.168.1.0/24 网段的数据包发至设备 DUT1 200.0.1.2 上，将来自 172.16.1.0/24 网段的数据包发至设备 DUT2 200.0.0.2 上。

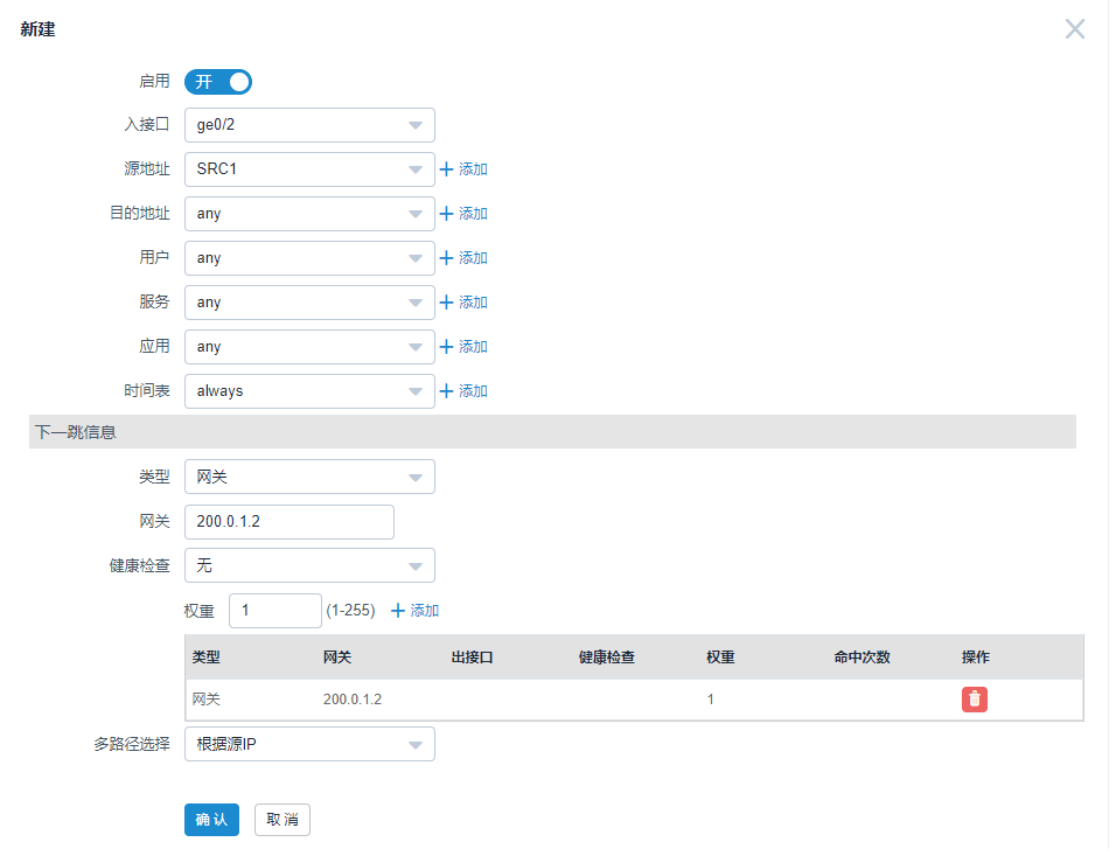


配置步骤

1. 在系统菜单中点击“**对象>地址>地址对象**”，进入**地址对象**页面，点击<**新建**>，创建 192.168.1.0/24 的地址对象，具体信息请参考下图：



2. 在系统菜单中点击“网络>IPv4 路由>策略路由”，进入策略路由页面，点击<新建>，创建策略路由，具体信息请参考下图：



3. 重复上述步骤配置 192.168.1.0/24 地址对象 SRC2 和对应的策略路由条目。

4. 配置完成后，查看策略路由表确认已有以下策略路由条目：

5. PC1 从 RouterA 访问外网，PC2 通过 RouterB 访问外网。

5.8.7. ISP 路由

一些用户会申请多条 ISP 线路进行流量负载均衡。在这种业务场景下，如果通过 ISPA 的线路访问 ISP 的服务器，网速会降低。针对该问题，下一代防火墙设备提供 ISP 路由功能，使不同 ISP 流量走专有路由，从而提高网络速度。

配置 ISP 路由，配置以 ISP 地址库名称为目的地址的 ISP 路由。下一代防火墙设备提供了多个预定义 ISP 地址库，分别是 ISP_INTL.dat、ISP_CERNET.dat、ISP_CT.dat、ISP_UNICOM.dat、ISP_CTT.dat、ISP_CMCC.dat。

在系统菜单中点击“**网络>IPv4 路由>ISP 路由**”，进入 **ISP 路由**页面，用户可以在此页面新建、编辑或删除 ISP 路由。

用户可在 **ISP 路由**页面下，点击<**新建**>按钮，创建新的 ISP 路由，或在右侧“操作”列下点击图标修改已有的 ISP 路由配置。

ISP 路由的配置项及详细说明如下：

配置项	说明
启用	启用或禁用 ISP 路由。
ISP 地址库	选择 ISP 路由所使用的 ISP 地址库。

类型	指定下一跳类型，可以为网关的 IP 地址或出接口（只能是隧道或 PPPoE 接口）。
网关/出接口	选择 ISP 路由的网关或出接口。
健康检查	设置对 ISP 路由下一跳的健康检查，根据探测到的结果更新路由表中对应路由条目的有效性。
权重	设置 ISP 路由的权重，取值范围 1-255。如果一条 ISP 路由匹配多个下一跳，系统会按照权重值比例分配流量。
多路径选择	可选根据源 IP 或根据连接进行哈希计算下一跳。

5.9. IPv6 路由

IPv6 是 Internet Protocol Version 6 的缩写，是 IETF 组织设计的用于替代现行版本 IP 协议（IPv4）的下一代 IP 协议。IPv4 地址只有 32 位，最大的问题在于网络地址资源有限，严重制约了互联网的应用和发展。IPv6 地址为 128 位，不仅能解决网络地址资源数量的问题，而且支持更多的服务类型，解决了多种设备接入互联网的障碍。

5.9.1. 路由表

在系统菜单中点击“网络>IPv6 路由>路由表”，进入路由表页面。

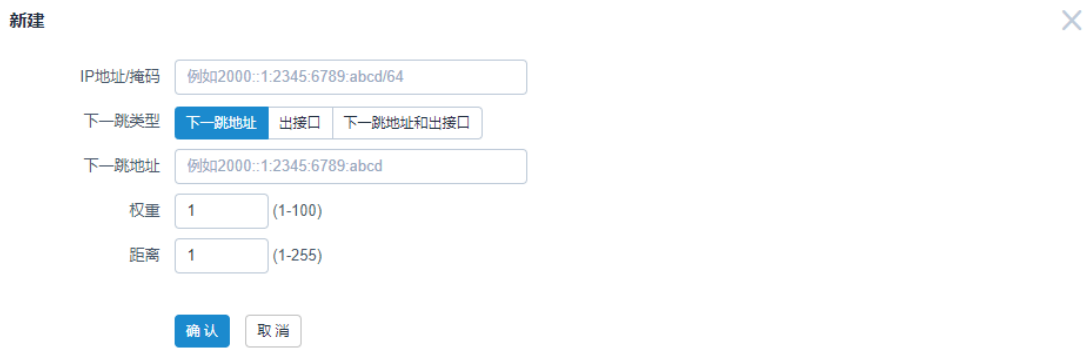
网关支持通过以下几种方式获取 IPv6 路由：

- IPv6 静态路由，指定目的网段和下一跳即可生成 IPv6 路由
- IPv6 路由通告
- 直连路由

5.9.2. 静态路由

在系统菜单中点击“网络>IPv6 路由>静态路由”，进入静态路由页面，显示设备上的所有 IPv6 静态路由。

在静态路由页面下点击<新建>创建新的 IPv6 静态路由，点击图标修改已有的静态路由。。



IPv6 静态路由的配置项及详细说明如下：

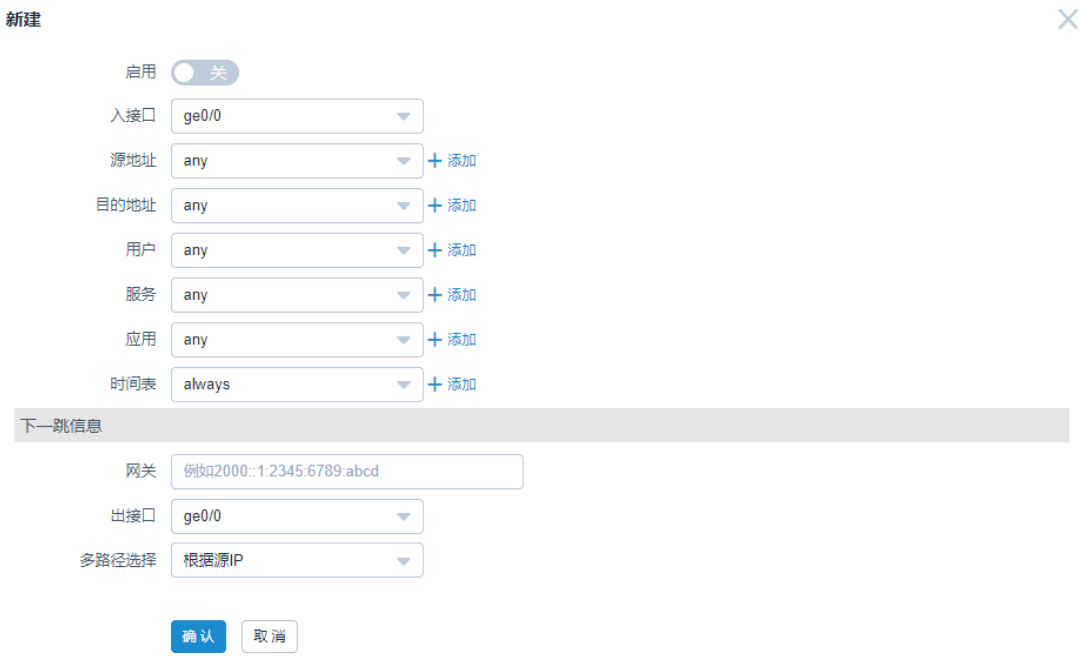
配置项	说明
IP 地址/掩码	设定 IPv6 静态路由的目的 IP 地址及掩码。
下一跳类型	支持选择下一跳地址、出接口以及下一跳地址和出接口。
下一跳地址/出接口	设置 IPv6 静态路由的下一跳或出接口或者下一跳和出接口。
权重	设置静态路由的权重，范围 1 到 100。如果存在多个下一跳负载均衡，权重越大，该条路由命中的概率就越大。
距离	指定路由的管理距离，范围 1 到 255。管理距离是指路由协议的路由可信度。每种路由协议按可靠性从高到低依次分配一个信任等级，这个信任等级就叫管理距离。正常情况下，管理距

	离越小，优先级就越高，也就是可信度越高。对于两种不同的路由协议到同一个目的地的路由信息，路由器首先根据管理距离决定相信哪一个协议。

5.9.3. 策略路由

在系统菜单中点击“网络>IPv6 路由>策略路由”，进入策略路由页面。

在策略路由页面下点击<新建>添加策略路由，点击图标修改已有的策略路由。



策略路由的配置项及详细说明如下：

配置项	说明
启用	启用或者禁用策略路由。

入接口	指定策略路由的入接口。
源地址	指定策略路由规则的源地址，可以为 IP 地址、地址范围、主机地址或域名。有关地址配置的更多信息，请参考地址。
目的地址	指定策略路由规则的目的地址，同源地址配置。
用户	指定策略路由规则的用户对象，可以为用户或用户组。有关用户配置的更多信息，请参考用户对象。
服务	指定策略路由规则的服务对象，可以为服务或服务组。有关服务配置的更多信息，请参考服务。
应用	指定策略路由规则的应用。
时间表	指定策略路由的生效时间。请参考时间。
下一跳信息	
网关	支持填写网关下一跳。
出接口	支持填写出接口。
多路径选择	可选根据源 IP 或根据连接进行哈希计算下一跳。

5.9.4. OSPF v3

OSPFv3 是 OSPF 版本 3 的简称，是在 OSPFv2 基础上开发的用于 IPv6 网络的路由协议。随着 IPv6 网络的建设，同样需要动态路由协议为 IPv6 报文的转发提供准确有效的路由信息。基于此，IETF 在保留了 OSPFv2 优点的基础上针对 IPv6 网络修改形成了 OSPFv3。OSPFv3 主要用于在 IPv6 网络中提供路由功能，是 IPv6 网络中路由技术的主流协议。

5.9.4.1. OSPF v3

在系统菜单点击“网络>IPv6 路由>OSPF v3>OSPF v3”，进入 OSPF v3 页签，显示 OSPF v3 功能配置信息。

OSPF v3 的配置项及详细说明如下：

配置项	说明
路由器 ID	指定 OSPF 路由器 ID，不同设备的路由器 ID 请配置不同值。格式为点分十进制 IP 格式。
路由重发布	
直连路由	开启此功能后，设备会通过 OSPF v3 协议重发布本系统中的 IPv6 直连路由信息给邻居设备。
静态路由	开启此功能后，设备会通过 OSPF v3 协议重发布本系统中的 IPv6 静态路由信息给邻居设备。

5.9.4.2. OSPF v3 发布接口

在系统菜单点击“网络>IPv4 路由>OSPF v3>OSPF v3 发布接口”，进入 OSPF v3 发布接口页签，显示设备上的所有 OSPF v3 发布的接口信息。

在 OSPF v3 发布接口页面下点击<新建>按钮创建新的 OSPF v3 发布接口信息。

OSPF v3 发布接口的配置项及详细说明如下：

配置项	说明
接口	选择需要开启 OSPF v3 协议的接口。
发布区域	指定发布的网络所对应的 OSPF v3 协议的区域，格式为“IP 地址”。只有发布区域相同，启用了 OSPF v3 协议的设备之间才可能成为邻居。

5.9.4.3. OSPF v3 监视器

在系统菜单点击“网络>IPv6 路由>OSPF v3>OSPF v3 监视器”，进入 OSPF v3 监视器页签，显示设备上的所有 OSPF v3 邻居状态信息。

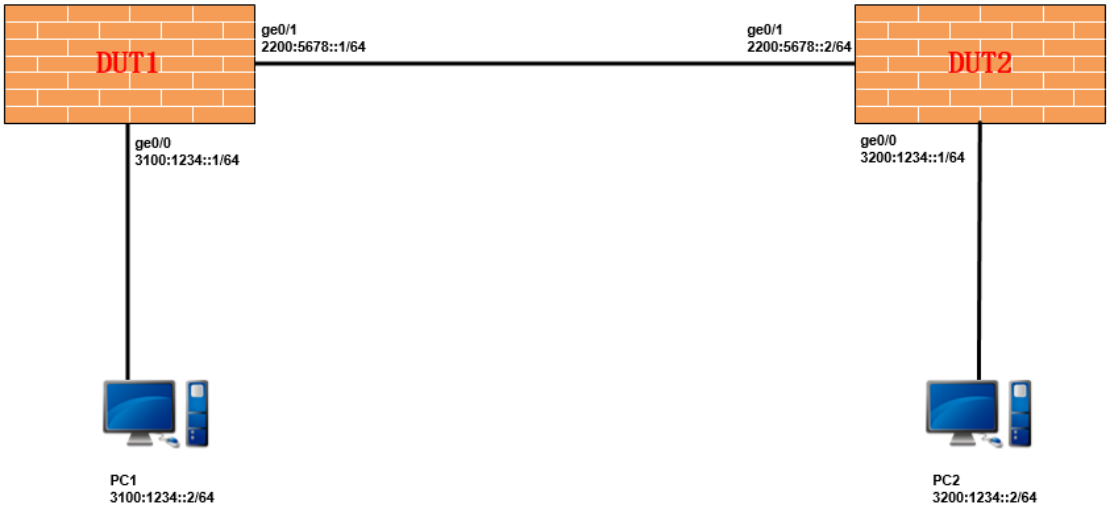
OSPF v3 监视器的信息项及详细说明如下：

信息项	说明
邻居路由器 ID	对端邻居设备的路由器 ID 信息。
优先级	对端邻居设备的优先级。
系统状态	邻居建立状态信息及路由器信息。
持续时间	邻居表项生成后的的保持时间。
接口	与对端设备建立邻居使用的接口。

5.9.4.4. OSPF v3 配置示例

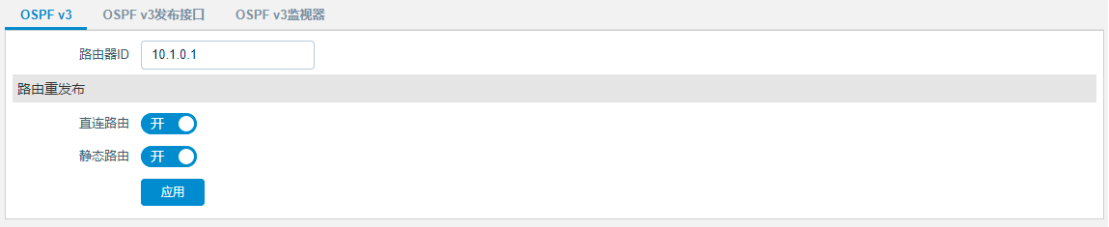
组网需求

如下图所示， DUT1 是 PC1 的网关设备、DUT2 是 PC2 的网关设备。要求设备 DUT1 与 DUT2 启用 OSPF v3 协议，DUT1 设备上能学习到 3200:1234::/64 网段的 OSPF v3 路由，DUT2 设备上能学习到 3100:1234::/64 网段的 OSPFv3 路由，PC1 ping6 PC2 的 IPv6 地址可通。

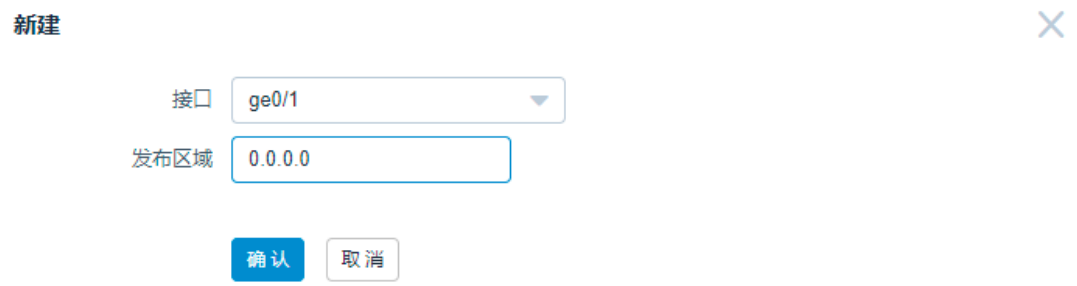


配置步骤

1. 在设备 DUT1 上，在系统菜单点击“网络>IPv6 路由>OSPF v3>OSPF v3”，进入 OSPF v3 页签配置 OSPF v3 协议参数信息，具体信息请参考下图并点击<确认>：



2. 在设备 DUT1 上，在系统菜单点击“网络>IPv6 路由>OSPF v3>OSPF v3 发布接口”，进入 OSPF v3 发布接口页签点击<新建>按钮配置需要新建的 OSPF 发布网络信息，具体信息请参考下图并点击<确认>：



3. DUT2 设备请参考 DUT1 设备配置方法。

4. 配置完成后，PC1 对 PC2 进行 ping6 测试，PC 间访问可以互通。

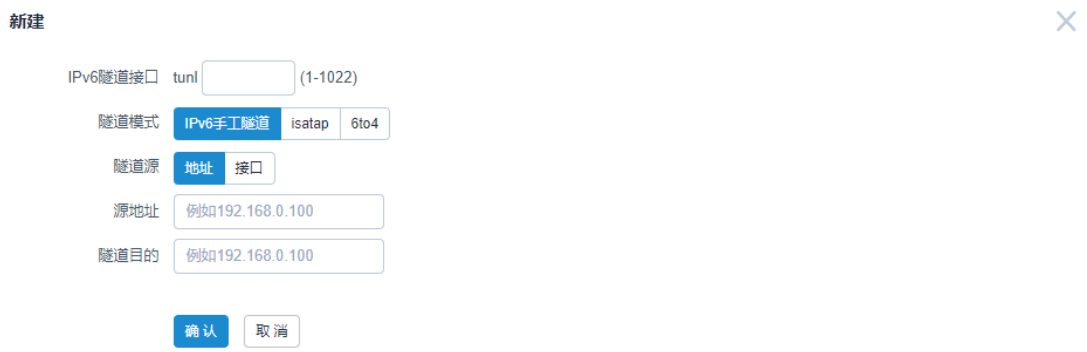
5.10. IPv6 隧道

IPv6 隧道包括手动隧道、6to4 隧道和 ISATAP 隧道，其隧道机制是将 IPv6 数据报文前封装上 IPv4 的报文头，通过隧道（Tunnel）使 IPv6 报文穿越 IPv4 网络，实现隔离的 IPv6 网络的互通。这种把 IPv4 网络当成链路层的 IPv6 隧道，又称为 IPv6 over IPv4 隧道。

5.10.1. IPv6 隧道配置

在系统菜单点击“网络>IPv6 隧道>IPv6 隧道配置”，进入 IPv6 隧道配置页面，显示设备上的所有 IPv6 隧道配置信息。

在 IPv6 隧道配置页面下点击<新建>按钮创建新的 IPv6 隧道配置，或在右侧“操作”列下点击图标修改已有的 IPv6 隧道配置。



IPv6 隧道配置的配置项及详细说明如下：

配置项	说明

IPv6 隧道接口	指定 IPv6 隧道接口的名称，格式为 tunl+ID，ID 范围为 1-1022。
隧道模式	选择 IPv6 隧道的模式。目前设备支持三种隧道模式，分别为 IPv6 手工隧道、isatap 隧道和 6to4 隧道。 ● **IPv6 手工隧道**-是在隧道两端的设备上通过人工配置而创建的，它需要静态指定隧道的源 IPv4 地址和目的 IPv4 地址。 ● **ISATAP 隧道**-定义在 RFC4214，是一种 IPv6 自动隧道技术，主要用于 IPv4 网络中的双栈主机通过 ISATAP 隧道访问 IPv6 网络的场景，它需要只需要指定隧道的源 IPv4 地址。同时需要在隧道接口配置一个主 IPv6 地址，也可以只配置主 IPv6 地址前缀信息，同时点击**生成 EUI-64<开关>**，设备会根据 IPv6 地址前缀与源 IPv4 地址计算出一个 ISATAP 地址。 ● **6to4 隧道**-也是一种将多个 IPv6 孤岛通过 IPv4 网络互连的技术。to4 隧道只需要配置隧道源地址，隧道的终点也是由设备自动生成。同样，它也使用了一种特殊的地址格式，称为 6to4 地址。
隧道源	指定隧道源地址获取的方式，目前支持手动指定隧道源地址、从指定接口上获取地址作为隧道源地址两种方式。

5.10.2. IPv6 隧道接口

在系统菜单点击“**网络>IPv6 隧道>IPv6 隧道接口**”，进入 **IPv6 隧道接口**页面，显示设备上的所有 IPv6 隧道接口信息。在“操作”列下点击图标修改已有的 IPv6 隧道接口信息。

IPv6 隧道接口的信息项及详细说明如下：

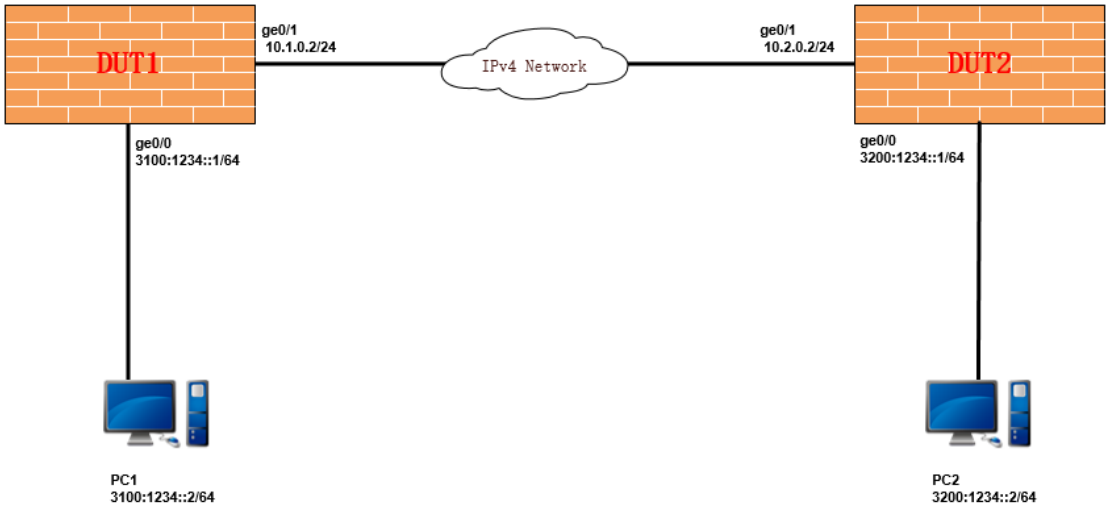
信息项	说明
名称	IPv6 隧道配置配置完成后产生对应的 IPv6 隧道接口，名称即为 IPv6 隧

	道配置创建使用的对应名称，格式为 tunl+ID。
IPv4 地址	IPv6 隧道接口上如果配置了 IPv4 地址，在此处进行显示。
IPv6 地址	IPv6 隧道接口上如果配置了 IPv6 地址，在此处进行显示。
隧道模式	IPv6 隧道接口所对应的 IPv6 隧道配置使用的隧道模式。
连接状态	当前此 IPv6 隧道接口的状态，显示分别为 UP/DOWN 两种。
管理状态	点击“管理状态”列下图标可人为控制 IPv6 隧道接口的状态（图标蓝色为 UP、灰色为 DOWN）。

5.10.3. IPv6 隧道配置示例

组网需求

如下图所示，PC1 与 DUT1、PC2 与 DUT2 均通过 IPv6 网络互通，DUT1 与 DUT2 通过 IPv4 网络互通。现需要通过 IPv6 手工隧道，使 PC1 与 PC2 的 IPv6 网络互通。



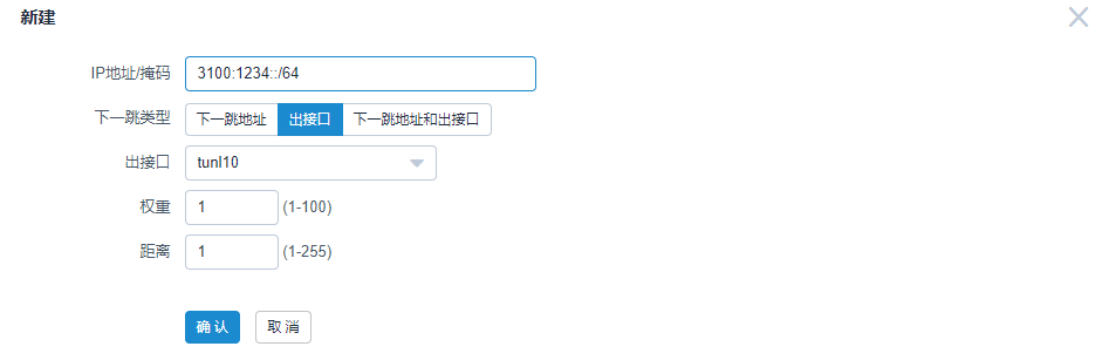
配置步骤

1. 在设备 DUT1 上，在系统菜单点击“网络>IPv6 隧道>IPv6 隧道配置”，点击<新建>按钮创建 IPv6 隧道，配置隧道源地址为 10.1.0.2、隧道目的 10.2.0.2，具体信息请参考下图：

2. 在设备 DUT2 上，在系统菜单点击“网络>IPv6 隧道>IPv6 隧道配置”，点击<新建>按钮创建 IPv6 隧道，配置隧道源地址为 10.2.0.2、隧道目的 10.1.0.2，具体信息请参考下图：

3. 在设备 DUT1 上，在系统菜单点击“网络>IPv6 路由>静态路由”，点击<新建>按钮创建 IPv6 静态路由，设置目标 IPv6 网络为 3200:1234::/64 的流量通过下一跳出接口 tunl10 发送，具体信息请参考下图：

4. 在设备 DUT2 上，在系统菜单点击“网络>IPv6 路由>静态路由”，点击<新建>按钮创建 IPv6 静态路由，设置目标 IPv6 网络为 3200:1234::/64 的流量通过下一跳出接口 tunl10 发送，具体信息请参考下图：



5. PC1 设置 IPv6 地址为 3100:1234::2/64，默认路由下一跳地址为 3100:1234::1，PC2 设置 IPv6 地址为 3200:1234::2/64，默认路由下一跳地址为 3200:1234::1。

6. 配置完成后，PC1 对 PC2 进行 ping6 测试，PC 间访问可以互通。

5.11. VPN 管理

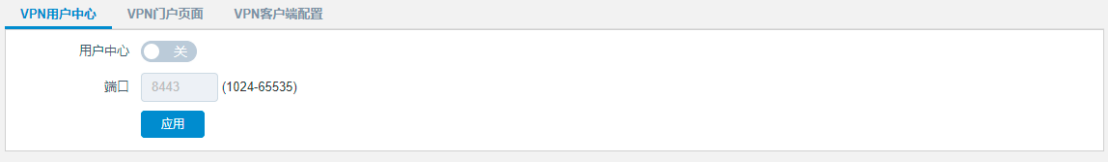
为了提升用户在 VPN 远程办公使用过程中的安全性，在现有用户认证（用户名密码）的基础上，增加动态码认证因素，以此提升 VPN 用户接入认证安全，解决弱身份鉴别可能引发的内网信息泄漏隐患。

5.11.1. VPN 用户中心

VPN 用户中心专为用户提供密码修改、客户端下载和 VPN 帮助文档查看功能。

5.11.1.1. VPN 用户中心

在系统菜单点击“网络>VPN 管理>VPN 用户中心>VPN 用户中心”，进入 VPN 用户中心配置页签。



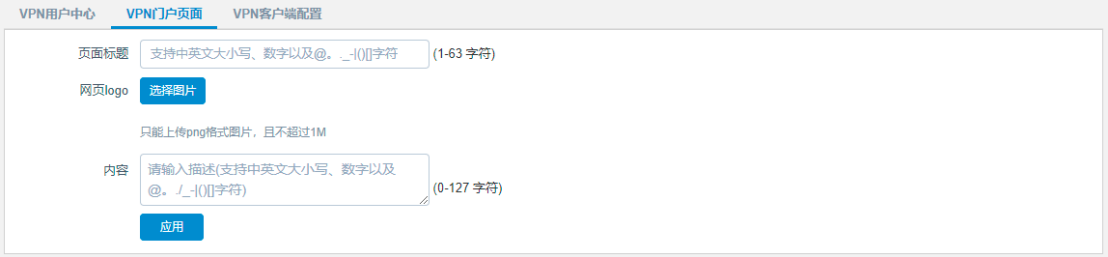
VPN 用户中心配置项及详细说明如下：

配置项	说明
用户中心	用户中心的开关。
端口号	默认端口 8443。

用户中心访问方式为 https://IP 地址:8443，用户可在**账户管理页**修改用户密码，在 **VPN** 页下载 VPN 客户端，在**帮助中心页**查看 VPN 帮助文档。

5.11.1.2. VPN 门户页面

在系统菜单点击“网络>VPN 管理>VPN 用户中心>VPN 门户页面”，进入 VPN 门户页面配置页签。



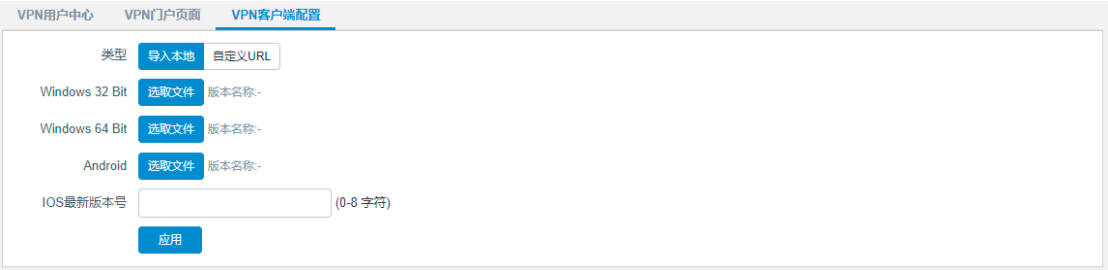
VPN 门户页面配置项及详细说明如下：

配置项	说明
页面标题	设置门户页面的标题内容。
网页 logo	上传显示在门户页面的 logo，仅支持 PNG 格式，文件大小不超过 1M，logo 上传后只能覆盖不能恢复默认。
内容	设置显示在门户页面的公告内容。

5.11.1.3. VPN 客户端配置

在系统菜单点击“网络>VPN 管理>VPN 用户中心>VPN 客户端配置”，进入客户端配置页签。页签分为导入本地和自定义 URL。

在 VPN 客户端配置页签下类型选择“导入本地”显示：

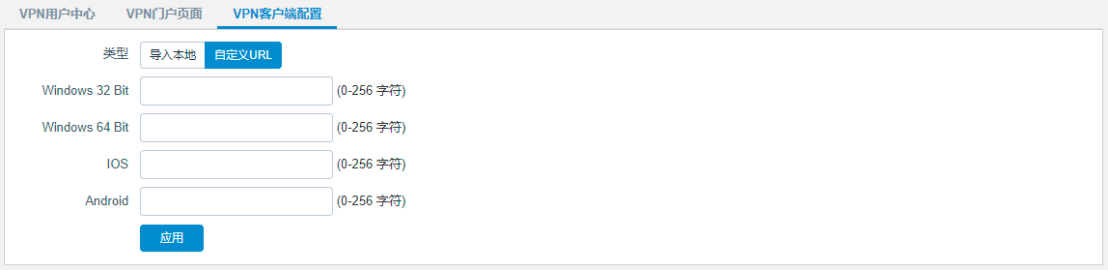


导入本地具体配置项如下：

配置项	说明
类型	选择导入本地后，自定义 URL 内容自动清空。

Windows 32 Bit	导入 Windows 32 位客户端压缩包，只支持 zip 格式，文件大小不超过 15M，压缩包内包含客户端安装包和 readme，客户端安装包命名格式为“VPNCLIENT_WIN32_V11.10_20210519”，readme 包含该安装包的 Version 版本号和 MD5 值。
Windows 64 Bit	导入 Windows 64 位客户端压缩包，只支持 zip 格式，文件大小不超过 15M，压缩包内包含客户端安装包和 readme，客户端安装包命名格式为“VPNCLIENT_WIN64_V11.10_20210519”，readme 包含该安装包的 Version 版本号和 MD5 值。
Android	导入 Android 客户端压缩包，只支持 zip 格式，文件大小不超过 15M，压缩包内包含客户端安装包和 readme，客户端安装包命名格式为“VPNCLIENT_ANDROID_V11.10_20210519”，readme 包含该安装包的 Version 版本号和 MD5 值。
IOS 最新版本号	手动输入版本号，进行客户端版本校验。

在 **VPN 客户端配置**页签下类型选择“自定义 URL”显示：



自定义 URL 配置项及详细说明如下：

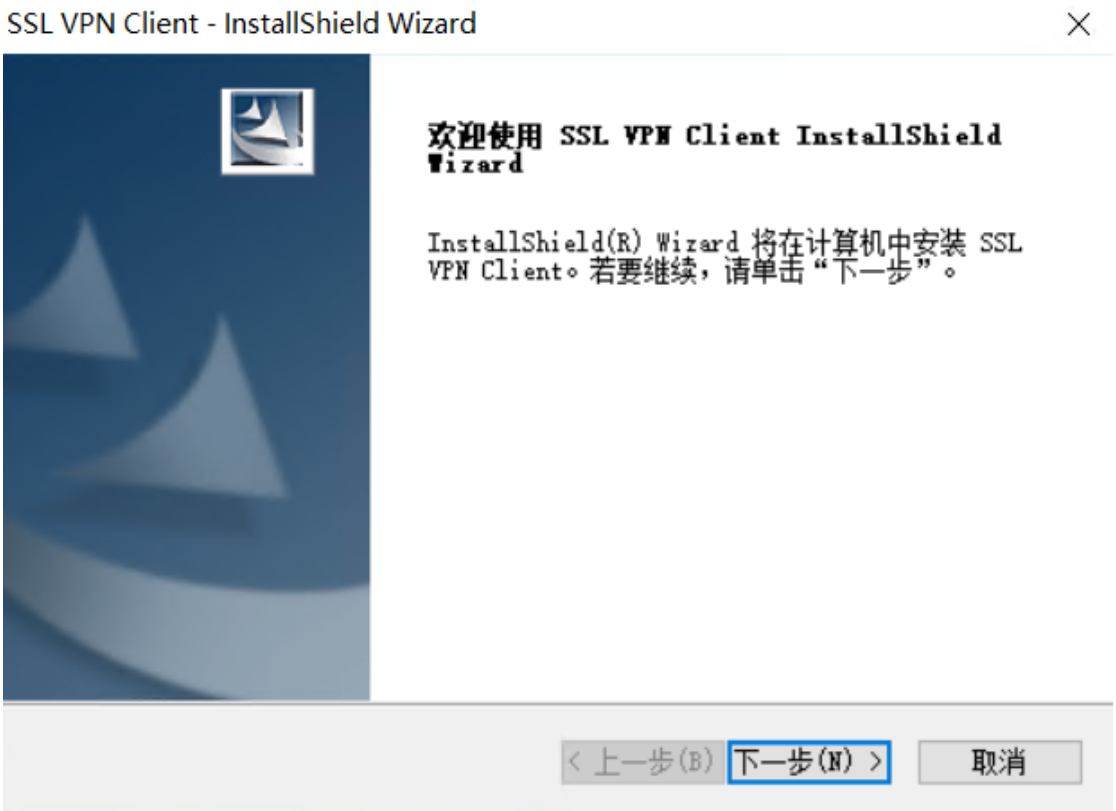
配置项	说明
类型	选择自定义 URL 后，导入本地的客户端自动清除。
Windows 32 Bit	设置 Windows 32 位 VPN 客户端的下载链接，支持 HTTP 和 HTTPS 服务器，用户需自行搭建下载服务器，设备本身不提供此项服务。
Windows 64 Bit	设置 Windows 64 位 VPN 客户端的下载链接，支持 HTTP 和 HTTPS 服务器，用户需自行搭建下载服务器，设备本身不提供此项服务。
IOS	设置 IOS VPN 客户端的下载链接，支持 HTTP 和 HTTPS 服务器，用户

	需自行搭建下载服务器，设备本身不提供此项服务。
Android	设置 Android VPN 客户端的下载链接，支持 HTTP 和 HTTPS 服务器，用户需自行搭建下载服务器，设备本身不提供此项服务。

5.11.1.4. VPN 客户端示例

从 SSL VPN 门户页面下载 SSL VPN 客户端后，参考以下步骤安装、运行客户端：

1. 双击安装包并按照提示安装客户端程序，具体信息请参考下图：



2. 安装完成后，点击运行客户端程序，具体信息请参考下图：

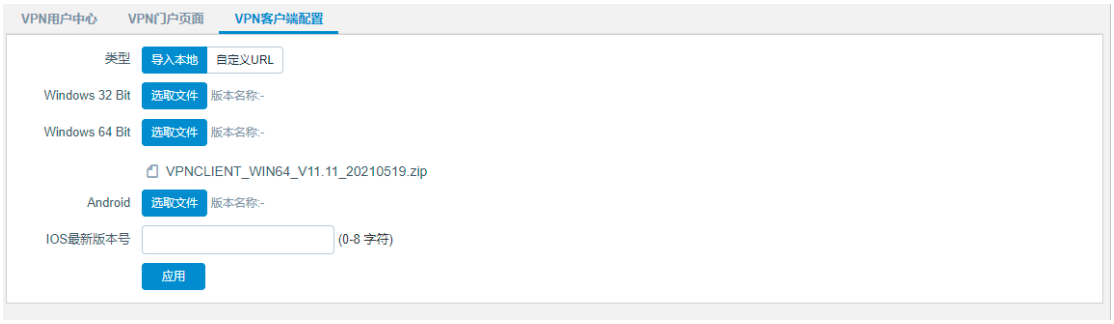
3. 输入服务器地址、服务器端口、用户名、用户密码后，点击<**登录**>，进行连接。

4. 成功创建连接后，任务栏将会显示以下图标，具体信息请参考下图：

5. 右键图标会显示客户端设置页面，点击<**关于版本**>即可看到版本号，具体信息请参考下图：

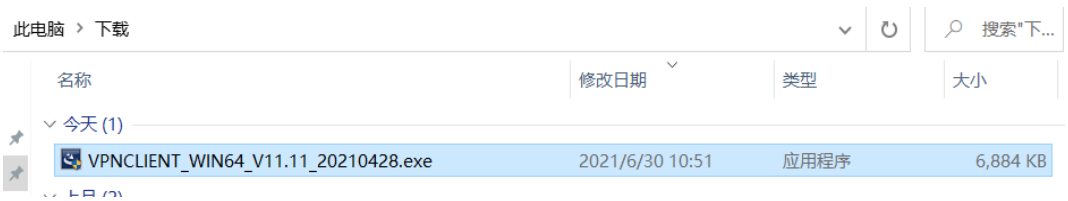
6. 在防火墙的系统菜单中点击“**网络>VPN 管理>VPN 用户中心>VPN 客户端配置**”中选择<

导入本地>上传 V11.11 的压缩包（Windows 64 位为例），具体信息请参考下图：



7. 客户端断开连接，重新登录，会进行版本号校验，具体信息请参考下图：

8. 点击<**下载**>按钮，会自动跳转网页进行下载，具体信息请参考下图：



9. 下载成功后即可直接覆盖安装进行连接。

提示：

卸载 SSL VPN 客户端时建议使用系统控制面板卸载程序进行卸载。

5.11.2. VPN 用户认证

在系统菜单点击“网络>VPN 管理>VPN 用户认证”，进入 VPN 用户认证配置页面。

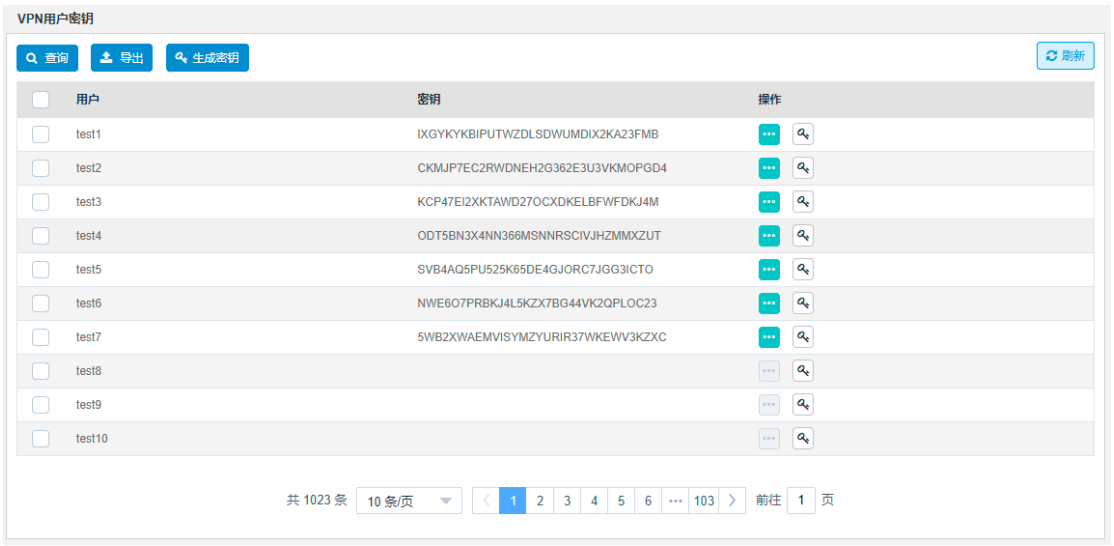
VPN 用户认证配置项及详细说明如下：

配置项	说明
认证模式	默认选中为用户名密码认证。
硬件特征码	默认关闭，表示 VPN 客户端的唯一特征码。
动态口令	默认关闭，动态口令开关。

动态口令的具体配置请参考动态口令。

5.11.3. VPN 用户密钥

在系统菜单点击“网络>VPN 管理>VPN 用户密钥”，进入 VPN 用户密钥管理页面。此页面支持显示本地用户和 LDAP 用户，具体创建用户请参考用户和 LDAP 用户同步。



每个用户默认无密钥，可以点击图标生成密钥，生成密钥后可以点击图标查看二维码，可以使用手机应用（FressOTP 或者 Authenticator）通过密钥或者二维码的方式获取动态口令。

点击<**生成密钥**>可以根据选择的多用户生成密钥。

点击<**刷新**>可以实时刷新用户密钥状态。

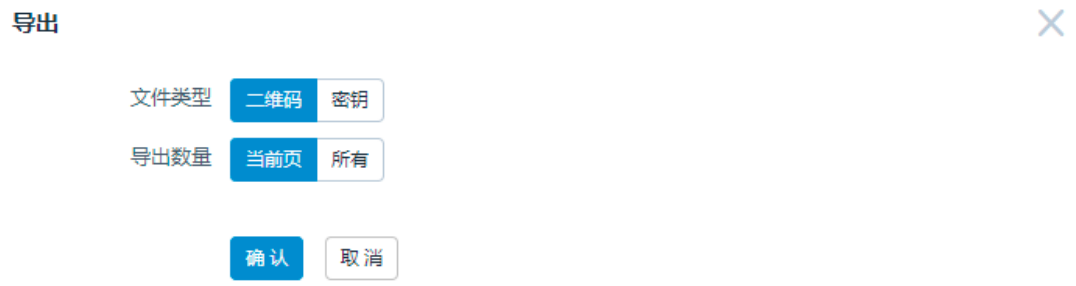
点击<**查询**>可以支持用户和密钥状态来进行查询。

查询内容配置项及详细说明如下：

配置项	说明
用户	
用户	根据用户名进行模糊查询。

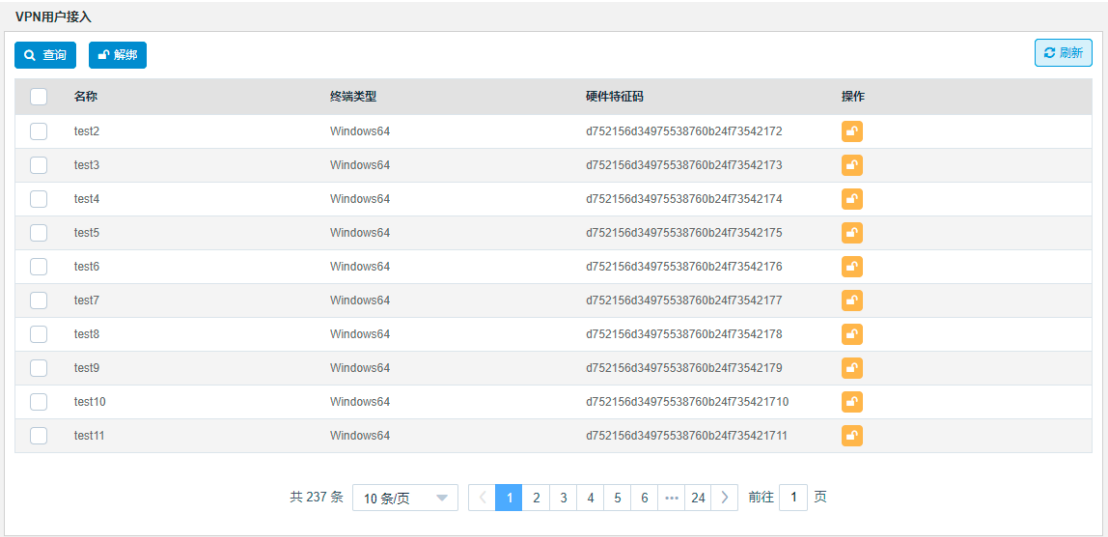
密钥状态	
所有	查询所有用户密钥状态。
已生成	查询已经生成密钥的用户。
未生成	查询未生成密钥的用户。

点击<**导出**>可以根据二维码和密钥进行当前页和所有页的导出。



5.11.4. VPN 用户接入

在系统菜单点击“**网络>VPN 管理>VPN 用户接入**”，进入 **VPN 用户接入**管理页面，显示所有已经连接过的客户端类型和硬件特征码。



点击图标可以单个解绑此用户终端，如果在线则剔除下线。

点击<**解绑**>按钮可以进行多用户多终端的解绑，如果在线则剔除下线。

点击<**刷新**>可以实时刷新用户接入状态。

点击<**查询**>按钮，可以根据用户名和终端类型进行组合查询。

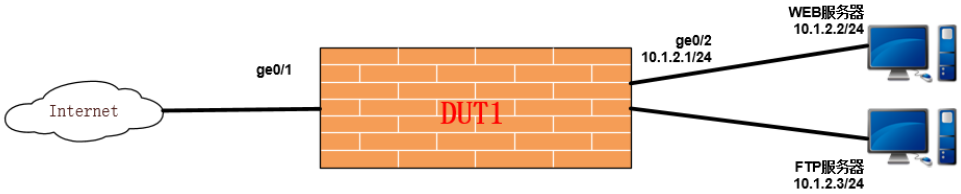
查询内容配置项及详细说明如下：

配置项	说明
名称	通过用户名进行模糊查询。
终端类型	可以根据所有、Android、Windows32、Windows64、IOS 类型进行组合查询。

5.11.5. VPN 动态口令配置示例

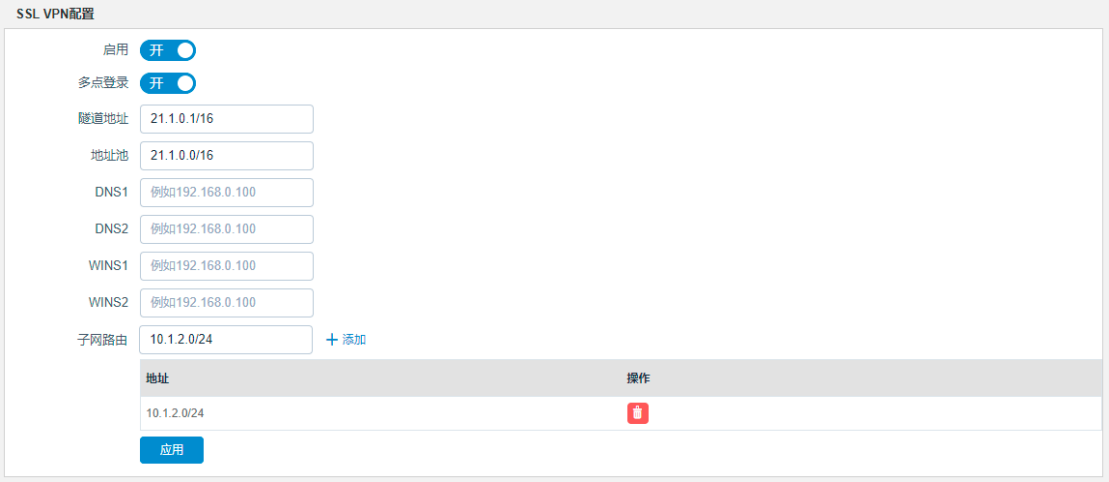
组网需求

如下图所示，设备的 ge0/1 和 ge0/2 接口以路由方式部署在网络中。用户需要设备提供 SSL VPN 服务，并限制特定的互联网用户通过 SSL VPN 访问内网的 Web 和 FTP 服务器。



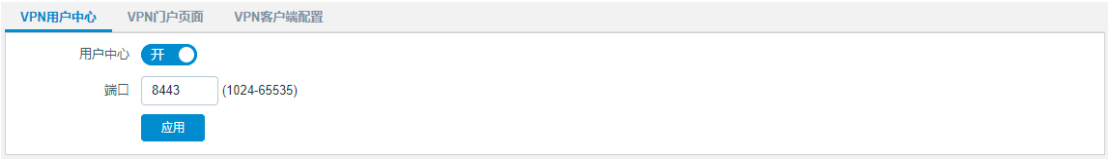
配置步骤

1. 在系统菜单点击“网络>SSL VPN>SSL VPN 配置”，进入 SSL VPN 配置页面，配置 SSL VPN 的配置，具体信息请参考下图：



2. 在系统菜单点击“对象>用户对象>用户”，进入用户页面，点击<新建>创建用户，具体信息请参考下图：

3. 在系统菜单点击“网络>VPN 管理>VPN 用户中心”，进入 VPN 用户中心页签，打开<用户中心>，端口默认为 8443，具体信息请参考下图：



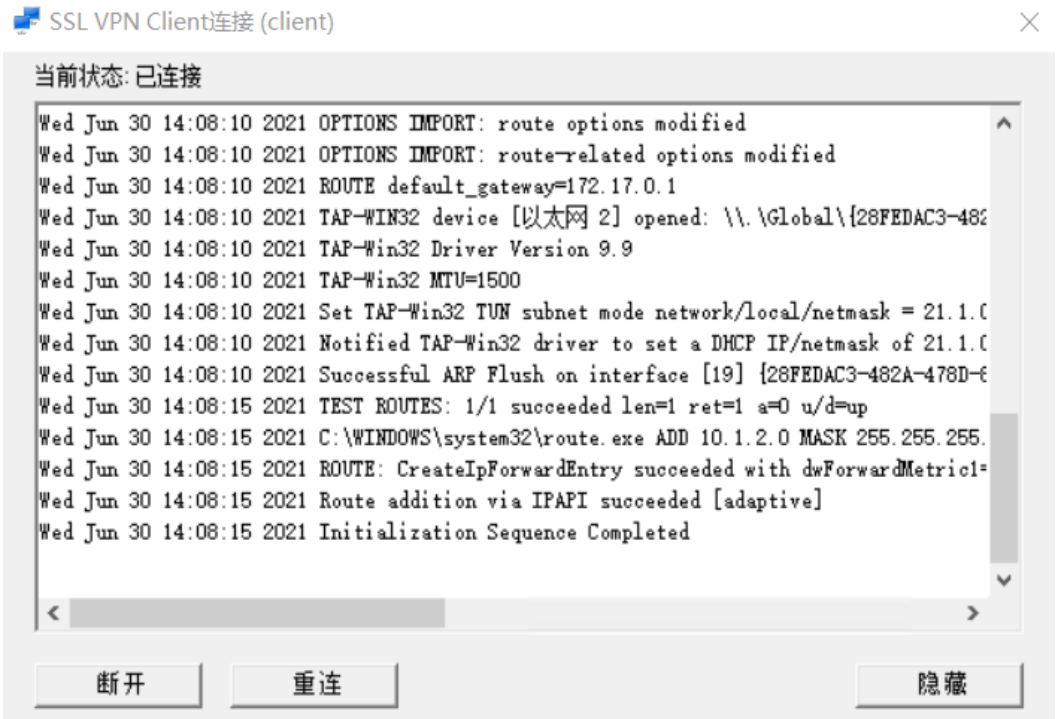
4. 在系统菜单点击“网络>VPN 管理>VPN 用户认证”，进入 VPN 用户认证页面，打开<动态口令>，具体信息请参考下图：

5. 在系统菜单点击“网络>VPN 管理>VPN 用户密钥”，进入 VPN 用户密钥页面，创建用户的密钥，点击图标来生成密钥。

6. 使用手机应用(FreeOTP 或者 Authenticator)输入密钥或者扫描二维码获取动态口令。

7. 获取动态口令后，使用客户端进行<登录>操作，就会弹出“请输入动态口令”的输入框，具体信息请参考下图：

8. 输入动态口令后，点击<**连接**>，显示连接成功则登录成功，具体信息请参考下图：



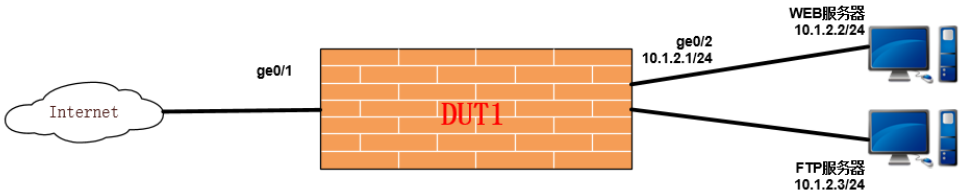
提示：

开启动态口令，设备需要进行时间同步。

5.11.6. VPN 硬件码配置示例

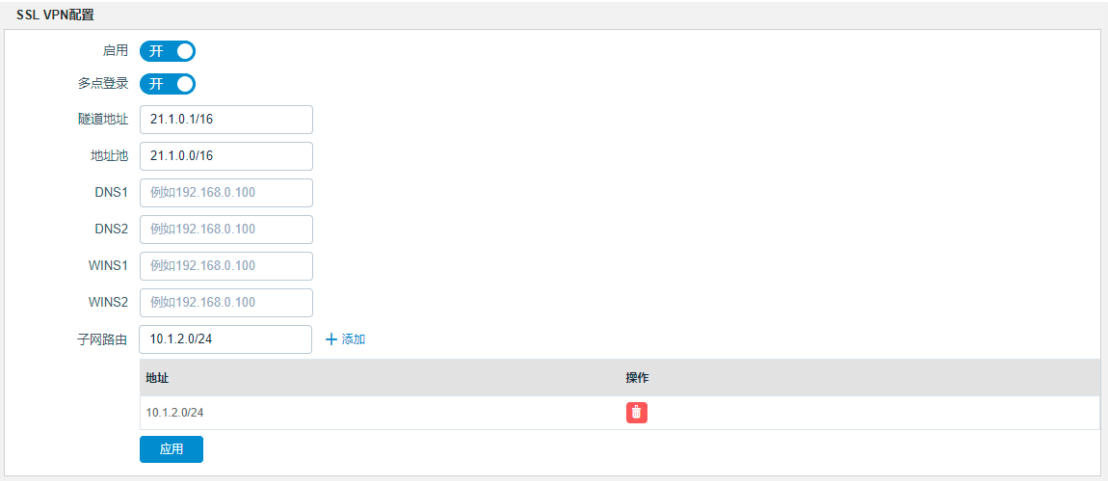
组网需求

如下图所示，设备的 ge0/1 和 ge0/2 接口以路由方式部署在网络中。用户需要设备提供 SSL VPN 服务，并限制特定的互联网用户通过 SSL VPN 访问内网的 Web 和 FTP 服务器。



配置步骤

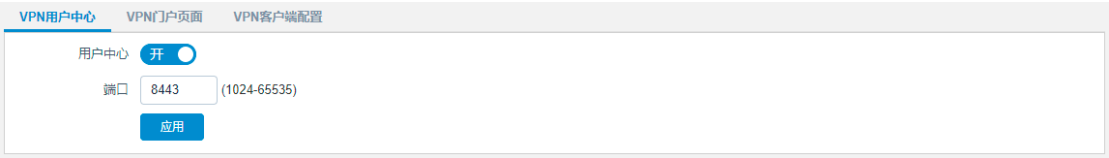
1. 在系统菜单点击“网络>SSL VPN 配置”中配置 SSL VPN 的配置，具体信息请参考下图：



2. 在系统菜单点击“对象>用户对象>用户”，进入用户页面，点击<新建>创建用户，具

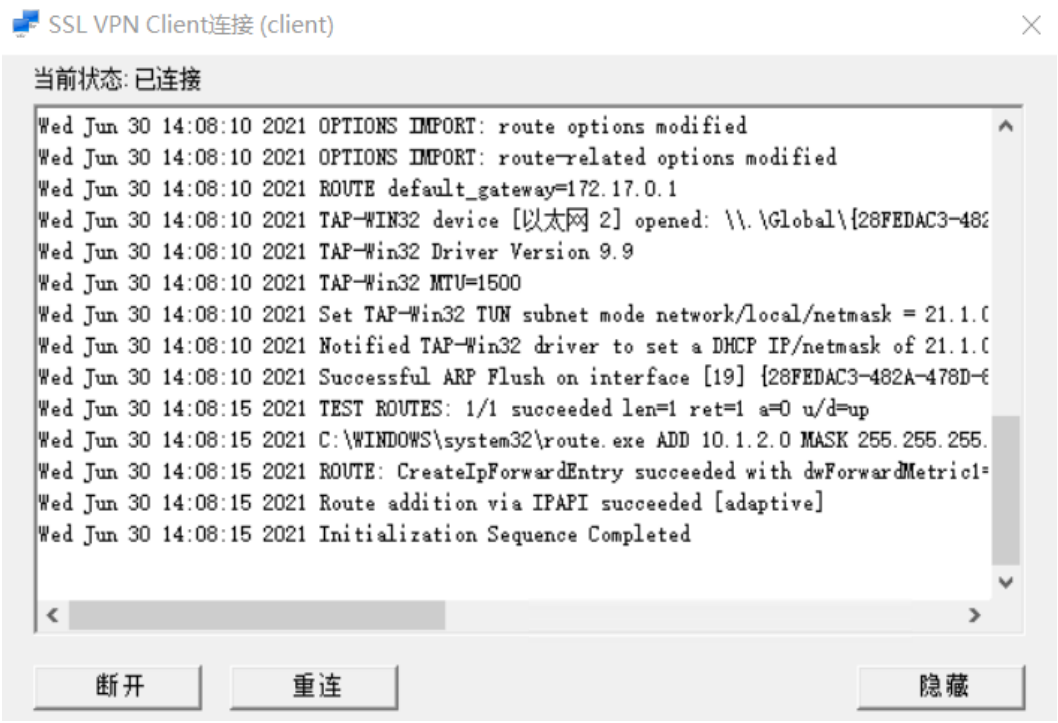
体信息请参考下图：

3. 在系统菜单点击“网络>VPN 管理>VPN 用户中心”，进入 VPN 用户中心页面，打开<用户中心>，端口默认为 8443，具体信息请参考下图：



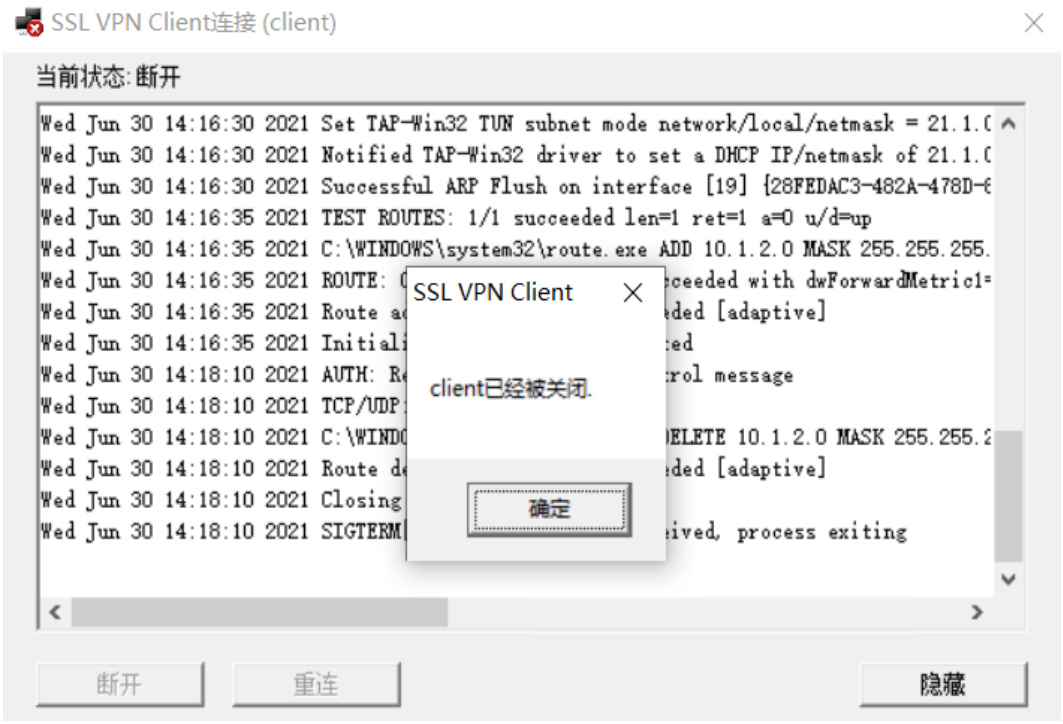
4. 在系统菜单点击“网络>VPN 管理>VPN 用户认证”，进入 VPN 用户认证页面，打开<硬件特征码>，默认接入终端数量为 3，具体信息请参考下图：

5. 使用客户端输入服务器地址、服务器端口、用户名、用户密码后，点击<登录>，客户端连接成功，具体信息请参考下图：



6. 在系统**菜单**点击“**网络>VPN 管理>VPN 用户接入**”，进入 **VPN 用户接入**页面查看，具体信息请参考下图：

7. 设备记录了客户端的终端类型和硬件特征码，点击后，即可剔除客户端，客户端会提示下线，具体信息请参考下图：



5.12. IPSec-VPN

IPSec 用于保护敏感信息在 Internet 上传输的安全性。它在网络层对 IP 数据包进行加密和认证。 IPSec 提供了以下网络安全服务，这些安全服务是可选的，通常情况下，本地安全策略决定了采用以下安全服务的一种或多种。

安全服务包含以下几种：

- 数据的机密性—IPSec 的发送方对发给对端的数据进行加密。
- 数据的完整性—IPSec 的接收方对接收到的数据进行验证以保证数据在传送的过程中
- 没有被修改。
- 数据来源的认证—IPSec 接收方验证数据的起源。
- 抗重播—IPSec 的接收方可以检测到重播的 IP 包丢弃。

使用 IPSec 可以避免数据包的监听、修改和欺骗，数据可以在不安全的公共网络环境下安全的传输，IPSec 的典型运用是构建 VPN。IPSec 使用“封装安全载荷（ESP）”或者“鉴别头（AH）”证明数据的起源地、保障数据的完整性以及防止相同数据包的不断重播；使用 ESP 保障数据的机密性。密钥管理协议称为 ISAKMP ，根据安全策略数据库（SPDB）随 IPSec 使用，用来协商安全联盟（SA）并动态的管理安全联盟数据库。

相关术语解释：

- 鉴别头（AH）：用于验证数据包的安全协议。
- 封装安全有效载荷（ESP）：用于加密和验证数据包的安全协议；可与 AH 配合工作可也以单独工作。
- 加密算法：ESP 所使用的加密算法。
- 验证算法：AH 或 ESP 用来验证对方的验证算法。
- 密钥管理：密钥管理的一组方案，其中 IKE（Internet 密钥交换协议）是默认的密钥自动交换协议。

5.12.1. IPSec 提案

5.12.1.1. 配置 IKE 协商策略

在系统菜单点击“网络>IPSec-VPN>IPSec 提案”，进入 IPSec 提案配置页面，点击<新建>创建 IPSec 一阶段。

IPSec 一阶段配置项及详细说明如下：

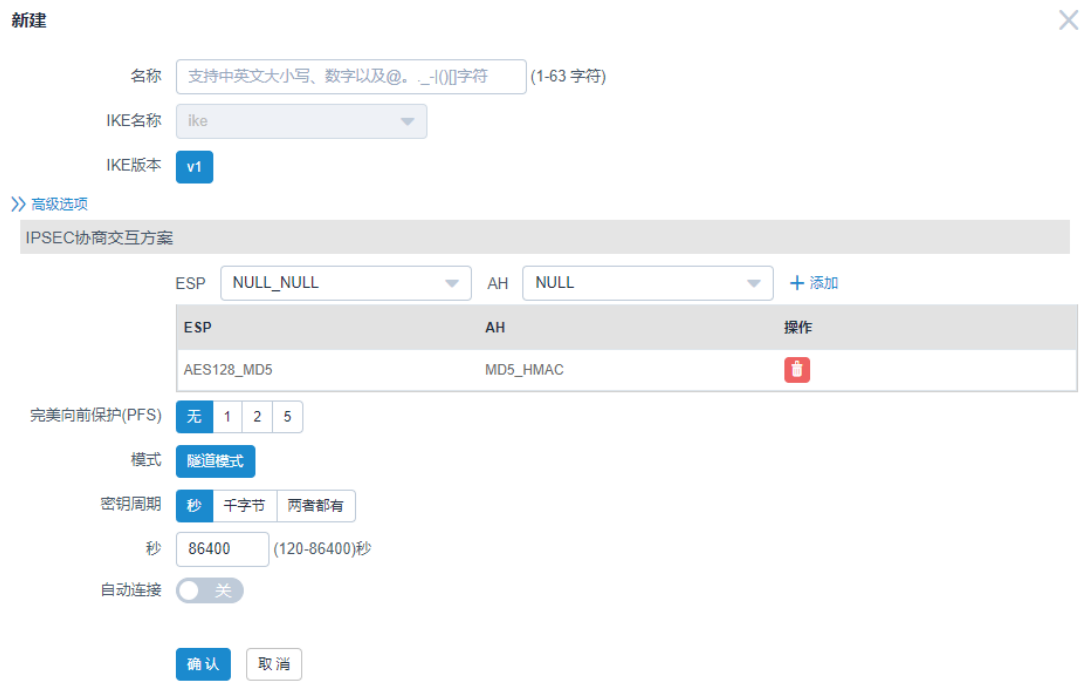
配置项	说明
基本配置	
网关名称	IKE 名称。
IKE 版本	默认选中为 V1
对端网关	指定对端网关。可以有静态 IP、域名、动态三种选择。如果采用域名方式，需启用 DNS 功能并配置正确的 DNS 地址。（DNS 的配置请

	参考 DNS）。
模式	一阶段协商过程中使用的模式，分主模式、野蛮模式和国密模式。
认证方式	指定一阶段认证所采用的方式，有预共享密钥和数字证书两种选择。数字证书的签发和导入请参考本地证书。对端 CA 的导入请参考本地 CA 中心。
高级选项-IKE 协商交互方案 选择第一阶段认证 IKE 协商所使用的加密算法和认证方式，最多可以添加 4 组。	
加密算法	设备目前支持一下加密算法:3DES、SM4、DES、AES（128\192\256 位）。
认证	设备目前支持以下认证方式：MD5、SM3、SHA、SH2-256、SH2-512。
DH 组	指定 DH 交换组。
密钥周期	设置 SA 第一阶段的密钥周期，单位为秒。到达密钥周期后，SA 双方需要重新进行 IKE 协商。默认为 86400 秒
NAT 穿越连接频率	即在穿越 NAT 时，NAT 会话保活报文的发送间隔。默认为 10 秒
本端 ID	设置本端 ID 值，支持 IP、FQDN、USER-FQDN、ASN1DN。其中 FQDN、USER-FQDN 只适用于野蛮模式。ASN1DN 只适用于野蛮模式和国密模式数字证书。
高级选项-对等体状态探测 启用对等体探测（DPD）。启用该功能后，SA 的一端会定期向另一端发送请求报文，检测对端是否存活。	
DPD 检测间隔	设置向对端发送 DPD 请求报文的时间间隔，单位秒。默认为 30 秒
DPD 失败重试间隔	如果发送的 DPD 报文未得到响应，使用 DPD 失败重试间隔时间来发送下一次 DPD 请求报文。DPD 失败重试间隔应小于 DPD 检测间隔，用于快速确认对端是否存活。默认为 5 秒
DPD 失败重试次数	如果在反复发送 DPD 请求报文达到指定的 DPD 失败重试次数后仍没有收到对端的响应报文，系统会判定对端 ISAKMP 网关已经死掉。默认为 5 秒
高级选项-扩展认证	

开启该功能后，设备会对通过 IPSec VPN 客户端接入的用户进行认证，认证的方式有本地认证和远程认证，远程认证需要结合已配置的认证服务器来完成。有关认证服务器的更多信息请参考远程服务器认证。	
高级选项-模式配置 启用允许给远程接入的用户分配地址及下发 DNS、WINS 服务器。	
地址池	选择用于给远程用户分配地址的地址池。有关地址池的更多信息请参考地址。
拨号用户 DNS	指定给远程用户下发的 DNS 服务器 IP 地址。
拨号用户 INS	指定给远程用户下发的 WINS 服务器 IP 地址。
高级选项-本地接口 指定用于建立 IPSec 连接的接口。	

5.12.1.2. 配置 IPSec 协商策略

在系统菜单点击“网络>IPSec-VPN>IPSec 提案”，进入 IPSec 提案配置页面，若存在已经配置好的一阶段 IKE 协商提案，直接点击已创建好的一阶段名称，进入二阶段配置页面，点击〈新建〉。



IPSec 二阶段配置项及详细说明如下：

配置项	说明
基本配置	
名称	设置 IPSec 协商策略名称。
IKE 名称	默认为 IPSec 提案配置的网关名称，不可更改
IKE 版本	默认选中为 V1
高级选项	
IPSec 协商交互方案	添加第二阶段 IPSec 协商的加密方案，包括 ESP 和 AH 所使用的加密算法，最多可添加四组。
完美向前保密（PFS）	选择 PFS 组。启用 PFS 功能后，一个密钥只能访问由它所保护的数据；用于生成密钥的元素一次一换，不能再生成其他密钥；一个密钥被破解，不影响其他密钥的安全性。
模式	目前只支持 IPSec 的隧道模式加密封装。
密钥周期	设置 IPSec SA 的最大有效时间，基于时间、流量或时间+流量的方式计算密钥生存时间。
自动连接	启用自动连接，按照指定的时间间隔，主动发起协商到对端。

注意：

如果发起端同时配置了 AH：md5-hmac 和 AH：null，此时对端不应只配置 AH：null。因为当加密方式存在时，将采取加密方式来进行协商。

5.12.2. IPSec 快速配置

除了上文所述的 IPSec VPN 的典型配置方式，下一代防火墙还提供了快速配置方式，适用于简单化、自动化的 VPN 部署。与典型配置方式相比，快速配置方式隐藏了 IKE 协商策略、IPSec 协商策略和 IPSec 隧道接口的创建，无需配置所要保护的网段，用户可以快速配置做

到“简单部署、快速上线、动态适应”。

在系统菜单点击“网络>IPSec-VPN>IPSec 快速配置”，进入 IPSec 快速配置页面，点击<新建>，配置如下：

IPSec 快速配置项及详细说明如下：

配置项	说明
基本配置	
名称	设置快速 IPSec 策略名称。
节点位置	选择 IPSec 节点的位置，可以是分支节点或中心节点。 ● **分支节点**-本端用作 IPSec VPN 的分支节点，主动向对端发起 IPSec 协商请求。 ● **中心节点**-本端用作 IPSec VPN 的中心节点。中心节点不会主动发起协商。
对端网关	对端设备的 IP 地址。
预共享密钥	用于协商的密钥。

保护网段	本端自动的传递该网段给对端网关，对端网关根据此网段自动生成相应的隧道接口路由。
高级选项	
本端 ID 类型	分为 IP、FQDN、USER-FQDN。
本端 ID	以不同的 ID 类型标识本端 ID。
对端 ID 类型	分为无、FQDN、USER-FQDN。
本地接口	指定用于建立 IPSec 连接的接口。

5.12.3. IPSec 隧道接口

在系统菜单点击“**网络<IPSec-VPN<IPSec 隧道接口**”，进入 **IPSec 隧道接口**配置页面，点击〈**新建**〉，创建 IPSec 隧道接口。

IPSec 隧道接口配置项及详细说明如下：

配置项	说明
IPSec 接口	IPSec 隧道接口名称。
IP 地址/掩码	为 tunnel 接口指定 IPv4 地址。

ike 版本	默认选中为 V1。
IPSec	指定一个已经存在的 IPSec 协商策略。
自动添加路由	是否自动生成 IPSec 的路由。
地址项目	设置受保护的数据流范围。
管理访问	当前接口支持其它设备连接的方法：HTTP；HTTPS；PING；TELNET；SSH；OSPF；RIP；DNS；WEBAUTH；BGP；SSLVPN。

5.12.4. IPSec SA

5.12.4.1. IPSec SA

在系统菜单点击“网络>IPSec-VPN>IPSec SA>IPSec SA”，进入 IPSec SA 页签，查看 IPSec SA 的建立情况。

点击 IPSec SA 监控后的，可以查看 IPSec VPN 相关详细信息。

详情

基本信息

ID	10
名称	DUT2-ipsec
本地网关	10.1.4.2
对端网关	10.1.4.1
状态	1
源网络	10.4.0.2/24
目的网络	10.1.2.2/24

ESP SAs

ESP SA 剩余时间(s)	85312/86400
ESP SA 剩余流量(kb)	0/0/0
SPI(入)	0x087aa492
SPI(出)	0x09e77d12
ESP 封装方式	tunnel
ESP 加密算法	aes128
ESP 认证算法	md5

AH SAs

AH SA 剩余时间(s)	85312/86400
AH SA 剩余流量(kb)	0/0/0
SPI(入)	0x0c3224ad
SPI(出)	0x08f1ac03
AH 封装方式	tunnel
AH 认证算法	md5

失效对端检测

DPD	disable
时间间隔	

取消

5.12.4.2. IKE SA

在系统菜单点击“网络>IPSec-VPN>IPSec SA>IKE SA”，进入 IKE SA 页签，查看 IKE SA 的建立情况。

5.12.4.3. 用户接入监控

在系统菜单点击“网络>IPSec-VPN>IPSec SA>用户接入监控”，进入用户接入监控页签，查看 IOS 客户端通过 IPSec VPN 进行 VPN 连接后的信息。

用户接入监控信息及详细说明如下：

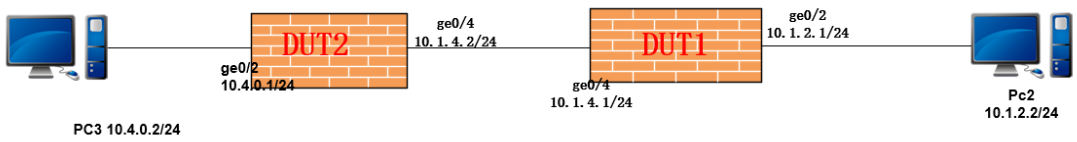
配置项	说明
用户名	SSLVPN 登录所使用的用户名。
虚拟 IP	显示登录 SSLVPN 的客户端拨号后获取的地址池中地址。
接入 IP	显示登录 SSLVPN 的客户端的 IP 地址。
终端类型	显示登录 SSLVPN 的客户端终端类型。
硬件特征码	显示登录 SSLVPN 的客户端的硬件特征码。
在线时长	显示登录 SSLVPN 的客户端拨号成功后的在线时长。
操作	删除 SSLVPN 监控信息，并使该用户强制下线。

5.12.5. 典型 IPSec VPN 配置示例

组网需求

按照下图所示配置接口 IP 地址，DUT2 与 DUT1 建立 IPSec 隧道，使 PC3 能够与 PC2 正常通

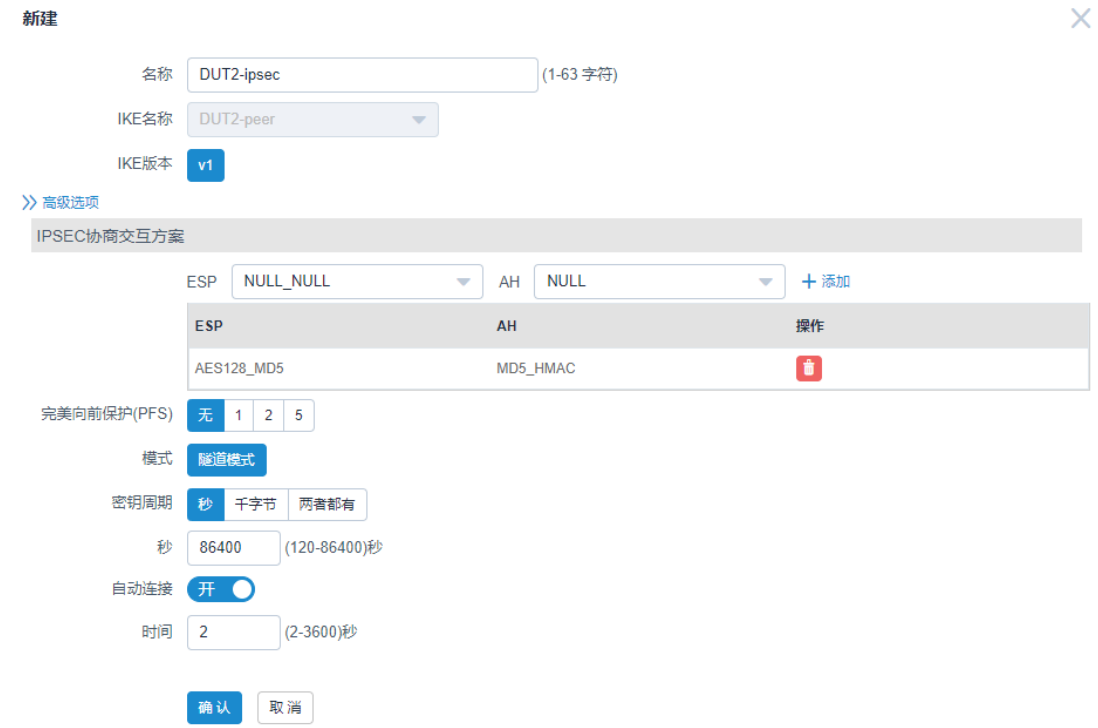
信。



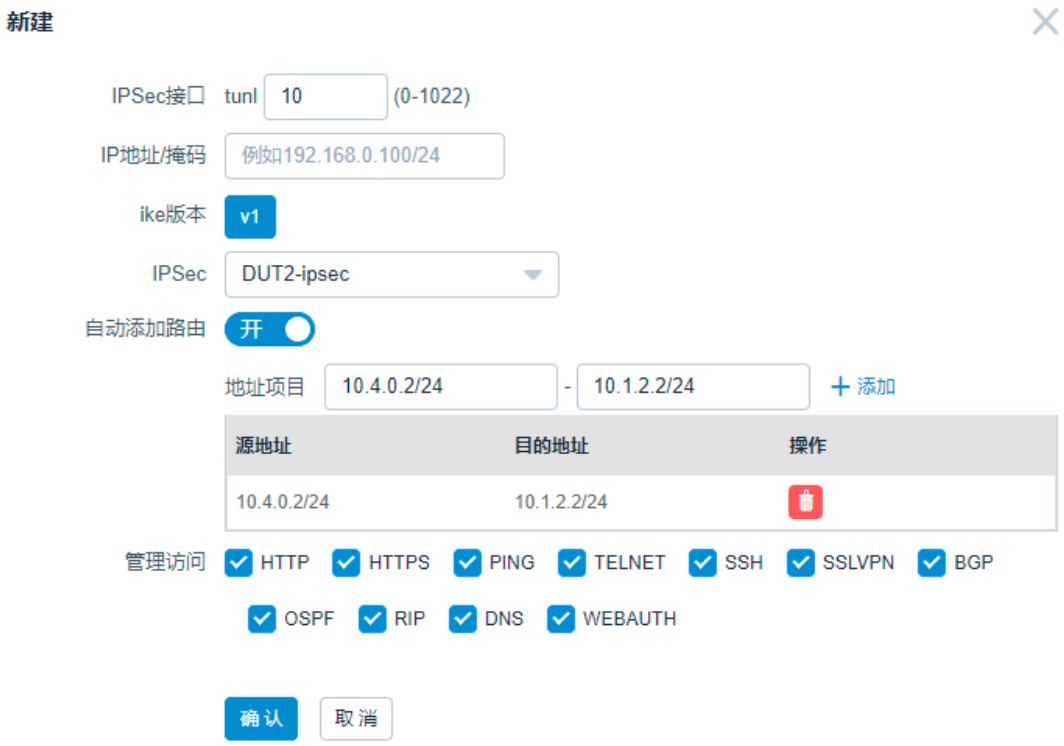
配置步骤

1. 在设备 DUT2 上，在系统菜单点击“网络>IPSec-VPN>IPSec 提案”，进入 IPSec 提案配置页面，点击<新建>，按照下图进行配置：

2. DUT2 点击创建好的一阶段名称<**DUT2-peer**>，配置二阶段，点击<**新建**>，按照下图配置

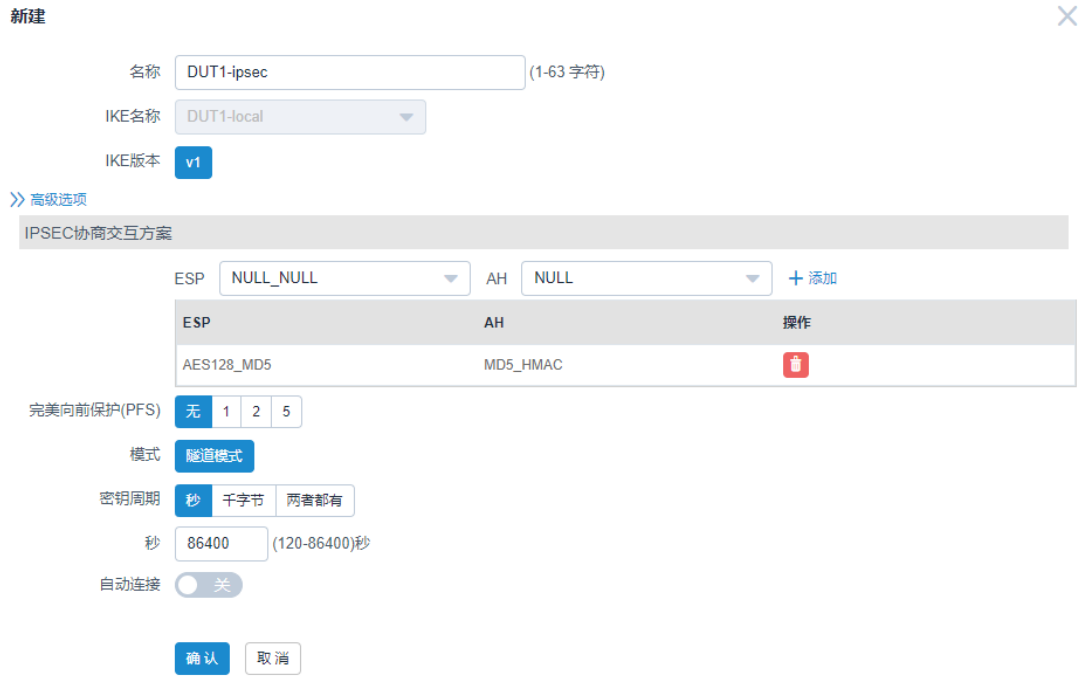


3. 配置完成二阶段后，点击“网络>IPSec-VPN>IPSec 隧道接口”，进入 IPSec 隧道接口配置页面，点击<新建>，按如下图配置：

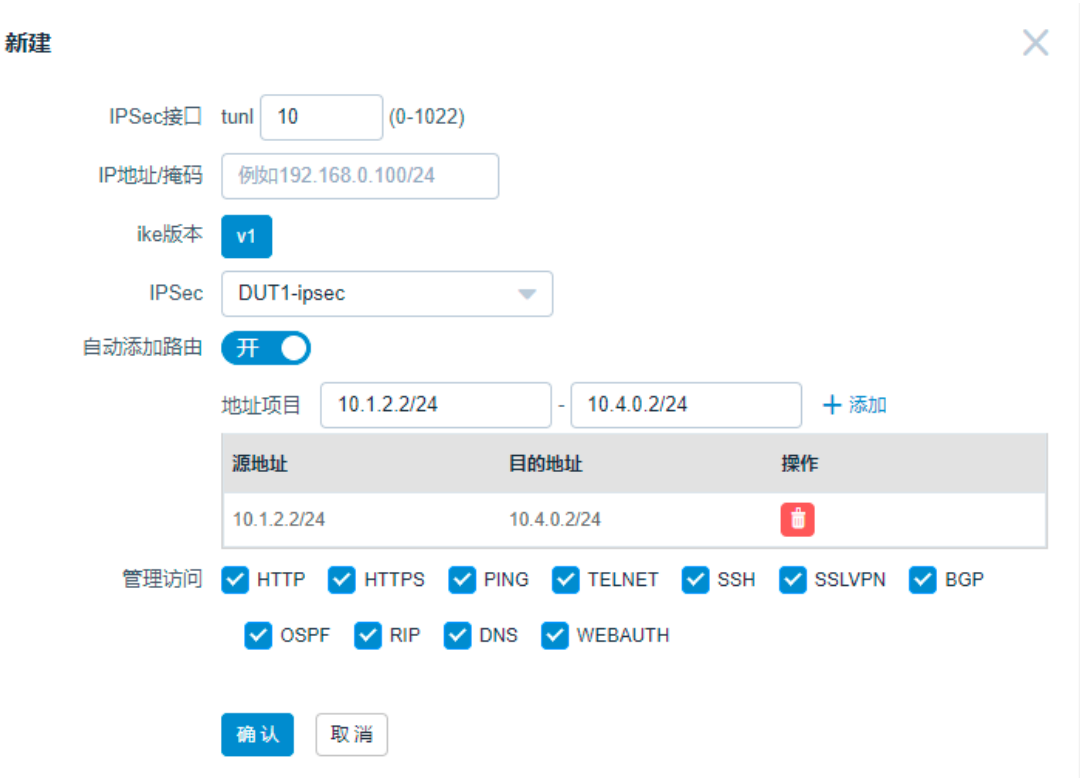


4. 在设备 DUT1 上，在系统菜单点击“网络>IPSec-VPN>IPSec 提案”，进入 IPSec 提案配置页面，点击<新建>，按照下图进行配置：

5. DUT1 点击创建好的一阶段名称<**DUT1-local**>，配置二阶段，点击<**新建**>，按照下图配置：



6. DUT1 配置完成二阶段后，点击“网络>IPSec-VPN>IPSec 隧道接口”，进入 IPSec 隧道接口配置页面，点击<新建>，按下图配置：



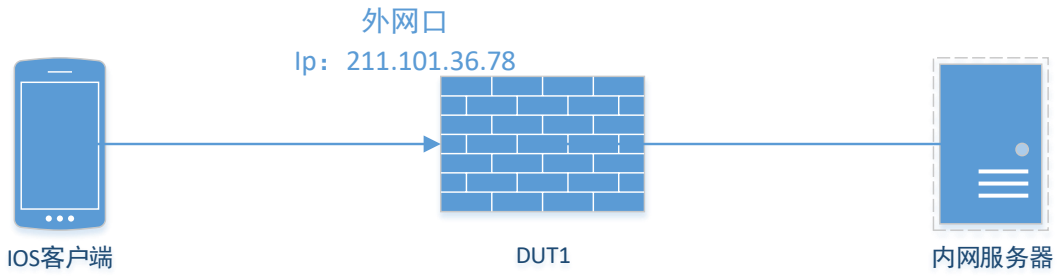
7. 两边设备配置完成后，分别在系统菜单点击“网络>IPSes-VPN>IPSec SA”，进入 IKE SA 和 IPSec SA 配置页签，状态显示连接，表示 IPSec 建立正常。

8. PC3 ping PC2，流量走 IPSec 隧道。

5.12.6. IPSec VPN 客户端配置示例

组网需求

按照下图所示配置接口 IP 地址，IOS 客户端与 DUT1 建立 IPSec 隧道，使 IOS 客户端与内网进行通信。



配置步骤

1. 在设备 DUT1 上，系统菜单点击“网络>IPSec-VPN>IPSec 提案”，进入 IPsec 提案页面，点击<新建>，按照下图进行配置（IOS 客户端仅支持野蛮模式，DH 组仅支持 2，加密算法支持 3DES、DES、AES128、AES192、AES256；认证 MD5、SHA）：


新建
网关名称
ike
(1-63 字符)
IKE版本
v1
对端网关
静态IP地址
动态IP地址
域名
模式
主模式(ID保护)
野蛮模式
国密
认证方式
预共享密钥
数字证书
预共享密钥
••••••
(6-31 字符)
高级选项
IKE协商交互方案
加密算法
3DES
认证
MD5
添加
加密算法
认证
操作
3DES
MD5
DH组
1
2
5
密钥周期
86400
(120-86400)秒
NAT穿越连接频率
10
(10-900)秒
本端ID类型
IP
FQDN
USER-FQDN

2. 配置完提案后，点击<**网关名称**>，并<**新建**>IPSec 二阶段，按照下图进行配置（算法支持 3DES_MD5、3DES_SHA1、AES128_MD5、AES128_SHA1、AES192_MD5、AES192_SHA1、AES256_MD5、AES256_SHA1，PFS 支持无、1、2、5）

3. 系统菜单点击“**网络>IPSec-VPN>IPSec 隧道接口**”，点击<**新建**>，按照下图进行配置：

4. 系统菜单点击“**网络>VPN 管理>VPN 用户中心**”，打开用户中心端口，按照下图进行配置：

5. 系统菜单点击“**对象>用户对象>用户**”，<**新建**>用户，按照下图进行配置：

6. 使用 IOS 客户端输入服务器地址、端口号、预共享密钥、用户名密码即可登录，按照下图进行配置：

7. 首次登录会提示允许添加 VPN 配置，再次输入用户的密码。

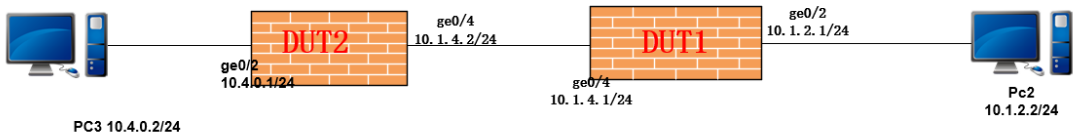
8. 登录成功后，页面可查看连接信息，包括连接时长、已用流量、上下行流速等。

9. 系统菜单点击“**网络>IPSec-VPN>IPSec SA**”，在“**用户接入监控**”页查看连接信息。

5.12.7. 快速 IPSec 配置示例

组网需求

按照下图所示配置接口 IP 地址，DUT2 与 DUT1 建立 IPSec 隧道，使 PC3 能够与 PC2 正常通信。



配置步骤

1. 在设备 DUT2 上，在系统菜单点击“网络>IPSec-VPN>IPSec 快速配置”，进入 IPSec 快速配置页面，点击<新建>，按照下图进行配置：

2. DUT2 配置完成快速配置后，在系统菜单点击“网络>IPSec 隧道接口”，能够看到自动创建的隧道接口：

3. 在设备 DUT1 上，在系统菜单点击“网络>IPSec-VPN>IPSec 快速配置”，进入 IPSec 快速配置页面，点击<新建>，按照下图进行配置：

4. DUT1 配置完成快速配置后，在系统菜单点击“网络>IPSec 隧道接口”，能够看到自动创建的隧道接口如下图：

5. 两边设备配置完成后，分别在系统菜单点击“网络>IPSes-VPN>IPSec SA”，进入 IKE SA 和 IPSec SA 页签，状态显示连接，表示 IPSec 建立正常。

6. PC2 ping PC3，流量走 IPSec 隧道。

5.13. SSL VPN

Secure Socket Layer-安全套接层，俗称 SSL。于 1990 年开发的 SSL 通过提供私密性，信息完整性，身份认证以及私有性来保障 Word Wide Web 通讯的安全。SSL 是一个不依赖于平台和运用程序的协议，是天然的安全远程接入，在方案上，特别是权限控制、应用粒度上有独到之处，成为远程接入领域颇受青睐的选择，目前已经超越了技术范畴，而成为一个安全网络服务框架。

我们的设备使用 IP 方式建立 SSL VPN 远程连接，所有客户端都从服务器获得一个 VPN IP 来

访问内部服务器，需要专用 SSL VPN 客户端软件来帮助建立连接。通信过程中使用 UDP 封装 SSL 协议，协商使用 1194 端口，支持端口映射和 NAT。拥有独立的用户中心页面，访问设备的 8443 端口可以修改用户密码、下载客户端安装文件，并有简明易懂的帮助文档辅助用户安装配置客户端。在使用客户端过程中用户还可以通过客户端的“修改密码”按钮跳转至此用户中心，增强了安全性。

5.13.1. SSL VPN 配置

在系统菜单点击“网络>SSL VPN>SSL VPN 配置”，进入 SSL VPN 配置页面，可以通过配置 SSL VPN 配置项启用 SSL VPN 功能。

SSL VPN 配置项及详细说明如下：

配置项	说明
启用	SSL VPN 功能启用和禁用，控制 SSL VPN 功能开启关闭。
多点登录	开启后同一个用户可以多个 IP 地址登录。
隧道地址	SSLVPN 隧道地址，将作为 VPN 用户网关地址。
地址池	地址池内地址将分配给连接的 VPN 用户。
DNS1	首选 DNS，将下发给拨入的 VPN 用户。
DNS2	备选 DNS,将下发给拨入的 VPN 用户。
WINS1	首选 WINS，将下发给拨入的 VPN 用户。

WINS2	备选 WINS，将下发给拨入的 VPN 用户。
子网路由	作为下发给客户端的路由的目的网段，路由下一跳为隧道地址。

5.13.2. SSL VPN 监控

5.13.2.1. SSL VPN 监控

在系统菜单点击“**网络>SSL VPN>SSL VPN 监控**”，进入 SSL VPN **监控**页签，可以查看已接入的 SSLVPN 用户的详细信息，可通过<**刷新**>按钮刷新最新信息，也可使用<**清除**>按钮清除当前所有的 VPN 在线用户。

SSL VPN 监控信息及详细说明如下：

配置项	说明
用户名	SSLVPN 登录所使用的用户名。
终端类型	显示登录 SSLVPN 的客户端终端类型。
硬件特征码	显示登录 SSLVPN 的客户端的硬件特征码。。
接入 IP	显示登录 SSLVPN 的客户端的 IP 地址。
虚拟 IP	显示登录 SSLVPN 的客户端拨号后获取的地址池中地址。
发送	SSLVPN 发送流量大小。
接收	SSLVPN 接收流量大小。
在线时长	显示登录 SSLVPN 的客户端拨号成功后的在线时长。
操作	删除 SSLVPN 监控信息，并使该用户强制下线。

5.13.2.2. 用户绑定

在系统菜单点击“网络>SSL VPN>SSL VPN 监控>用户绑定”，进入用户绑定页签，可以查看绑定的 SSL VPN 用户与虚拟 IP 的信息。

在用户绑定页签点击<新建>创建用户与虚拟 IP 的绑定关系，虚拟 IP 需要包含在 SSL VPN 配置的地址池中，可通过<删除>按钮删除用户与虚拟 IP 的绑定关系，也可通过<刷新>按钮刷新最新信息。

用户绑定配置项及详细说明如下：

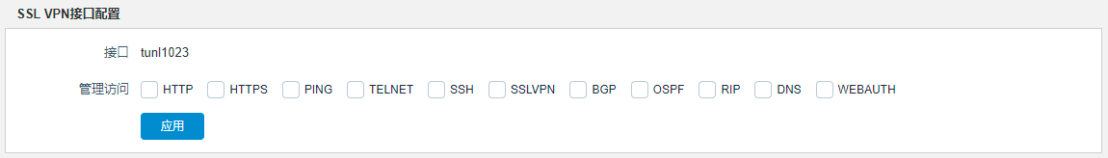
配置项	说明
用户名	SSLVPN 登录所使用的用户名。
虚拟 IP	SSLVPN 用户上线后分配的 IP 地址，地址必须包含在 SSL VPN 配置的地址池中。

注意：

清除和删除 SSLVPN 在线用户会导致用户强制下线，操作时需谨慎。

5.13.3. SSL VPN 接口配置

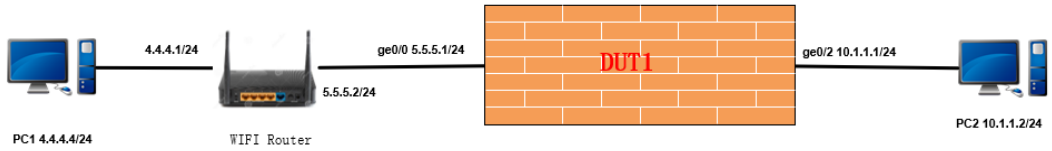
在系统菜单点击“网络>SSL VPN 接口配置”，进入 SSL VPN 接口配置界面，此界面可以配置 SSL VPN 接口的管理访问服务，控制其他地址对此 SSL VPN 接口的服务访问。



5.13.4. SSL VPN 配置示例

组网需求

用户 PC1 通过 SSLVPN Client 拨号后与 DUT1 设备建立 SSLVPN 连接，VPN 建立成功后 PC1 可以成功访问 DUT1 后的内网 PC2。



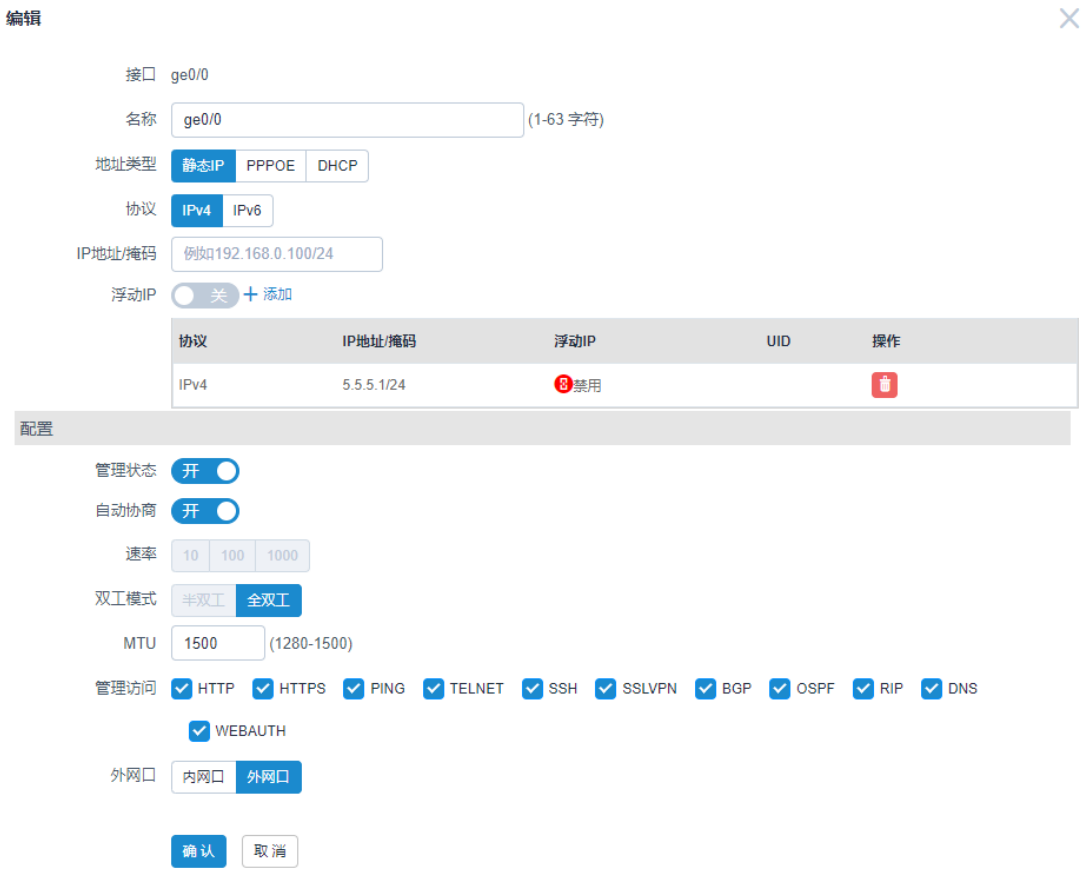
DUT1 ge0/0 地址：5.5.5.1/24，ge0/2 地址：10.1.1.1/24。

Client IP 地址：4.4.4.4/24。

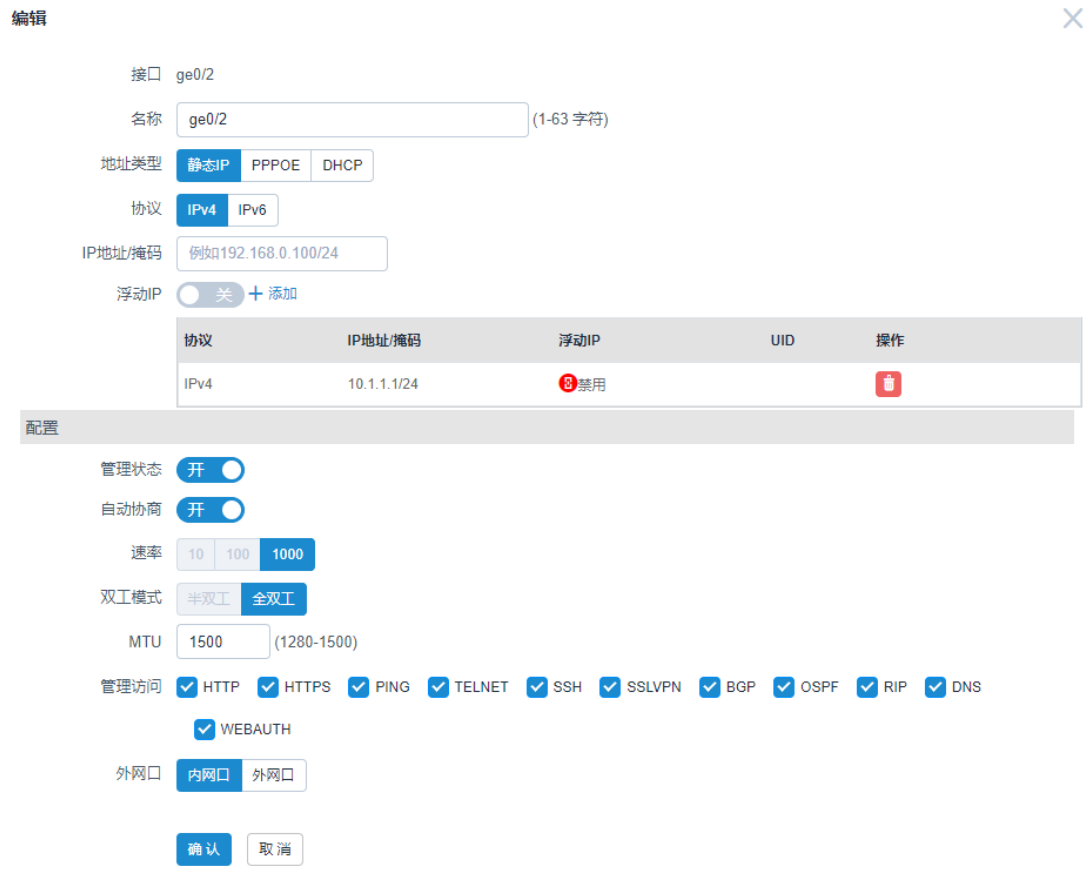
PC2 地址：10.1.1.2/24,默认网关为 10.1.1.1。

配置步骤

1. DUT1:进入“网络>接口配置>物理接口”配置接口,ge0/0 的 IP 地址配置 5.5.5.1/24。

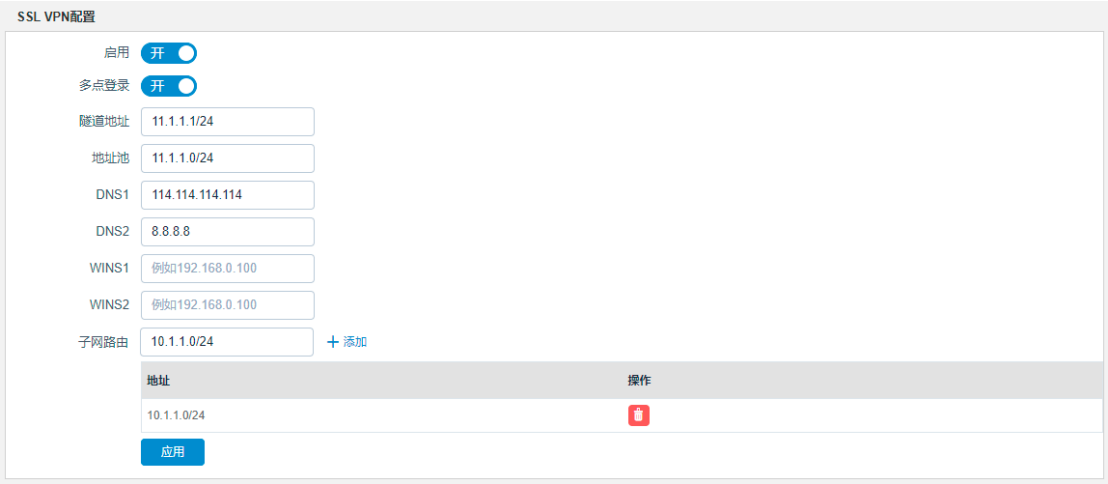


2. ge0/2 的 IP 地址配置为 10.1.1.1/24。



3. 进入“**对象>用户对象>用户**”，点击新建，名称：test 密码为 123456。

4. DUT 配置 SSL VPN，进入“**网络>SSL VPN>SSL VPN 配置**”，打开启用和多点登录开关，输入隧道地址 11.1.1.1/24,地址池 11.1.1.0/24，DNS1 输入 114.114.114.114，DNS2 输入 8.8.8.8，子网路由输入 10.1.1.0/24。



PC 配置

1. 在 PC 上安装客户端。

2. 打开客户端，填写服务器地址 10.1.1.1 及服务器端口号 8443，输入用户名：test，用户密码：123456，点击登录。

3. 登录成功，在监控页面可以查看到 test 用户登录信息。

4. 通过 client 端 PC1 ping PC2 端 IP 地址，可以正常通信。

注意：

SSLVPN 功能要能正常使用需要在 VPN 管理中开启 VPN 用户中心后方可使用。

第六章 对象

6.1. 用户对象

设备提供用户管理功能，支持本地认证、短信认证、二维码认证等多种认证方式，同时支持本地用户、静态绑定和远程用户；可以配置用户组，支持将用户加入用户组中；在访问控制策略、应用控制策略、流控策略、审计等功能中可以引用用户/用户组。

6.1.1. 用户

用户作为系统的一个重要资源，在安全策略、认证等功能上都会相应使用。本系统的用户类型有匿名用户、静态绑定用户、认证用户三种。

- 匿名用户，是指系统未有效识别出来的用户，匿名用户不用配置，系统自动将未识别的用户 IP 作为匿名用户的用户名。
- 静态绑定用户，是指系统根据静态绑定配置识别出的用户。
- 认证用户，是指根据系统配置，需要认证的用户。支持的认证方式：本地、短信认证、访客二维码认证、AD 域单点登录认证、远程认证（LDAP 认证、RADIUS 认证）等，更多信息请参考认证管理。

管理员可根据不同的用户分类采取不同的用户策略，对用户的网络访问等进行权限限制和监控。

在系统菜单点击“**对象>用户对象>用户**”，进入**用户**配置页面，可以实现对用户的新建、修改、删除、查询和重置。

6.1.1.1. 本地认证

在**用户**页面下点击<**新建**>，选择认证类型为“**本地认证**”，或在右侧“操作”列下点击图标修改已有的用户。

本地认证用户配置项及详细说明如下：

配置项	说明
名称	设置用户登录时所使用的的用户名。
启用	开启启用按钮在创建用户成功后立即启用该用户。
认证类型	选择用户的认证类型。
密码	设置用户登录时所使用的本地密码，需配合本地认证功能进行用户身份校验。有关本地认证配置的更多信息，请参考用户认证。
确认密码	校验上面密码输入正确性。

6.1.1.2. 静态绑定

在**用户**页面下点击<**新建**>，选择认证类型为“**静态绑定**”，或在右侧“操作”列下点击图标修改已有的用户。

静态绑定用户配置项及详细说明如下：

配置项	说明
名称	设置用户登录时所使用的的用户名。
启用	开启启用按钮在创建用户成功后立即启用该用户。
认证类型	选择用户的认证类型。
绑定 IP	设置用户的静态绑定 IP，可以为 IP 地址、IP 地址范围，配置多项时需要以回车分隔。 如果上线用户属于绑定范围，则在用户统计中显示的用户名为所设置的名称，显示的认证方式为“**静态绑定**”。 有关在线用户统计的更多信息，请参考在线用户统计。
排除 IP	设置绑定范围内的排除 IP 地址或地址范围，即不应用静态绑定 IP 或地

	址范围。
绑定 IPv6	设置用户的静态绑定 IPv6 地址，可以为 IPv6 地址、IPv6 地址范围，配置多项时需要以回车分隔。
排除 IPv6	设置绑定范围内的排除 IPv6 地址或地址范围，即不应用静态绑定 IPv6 或地址范围。
绑定 MAC	设置用户的静态绑定 MAC 地址。

6.1.1.3. LDAP 认证

在**用户**页面点击<**新建**>，选择认证类型为“**LDAP**”，或在右侧“操作”列下点击图标修改已有的用户。

LDAP 用户配置项及详细说明如下：

配置项	说明
名称	设置用户登录时所使用的的用户名。
启用	开启启用按钮在创建用户成功后立即启用该用户。
认证类型	选择用户的认证类型。
LDAP 服务器	选择用户认证时所需要的 LDAP 服务器。有关于有关 LDAP 服务器配置的更多信息，请参考 LDAP 服务器。

6.1.2. 用户组

在系统菜单点击“**对象>用户对象>用户组**”，进入**用户组**配置页面，可以实现对用户组的新建、修改和删除操作，设备默认有 8 个用户组，不可编辑不可删除。

在**用户组**页面下点击<**新建**>创建新的用户组，或在右侧“操作”列下点击图标修改已有的用户组。此用户组被策略引用时只能编辑不能删除，未被策略引用时可编辑可删除。

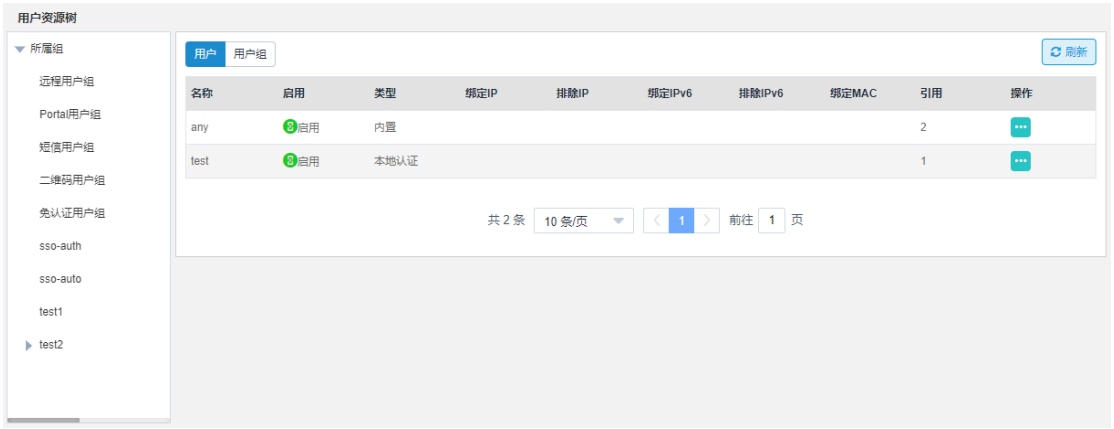
用户组配置项及详细说明如下：

配置项	说明
名称	输入用户组名称。
描述	添加用户组的描述信息（可选）。
成员-可选	选择添加到用户组中的用户或者用户组。
成员-已选	展示用户组包含的用户或用户组，可选择用户或用户组，点击‹从用户组中移除。

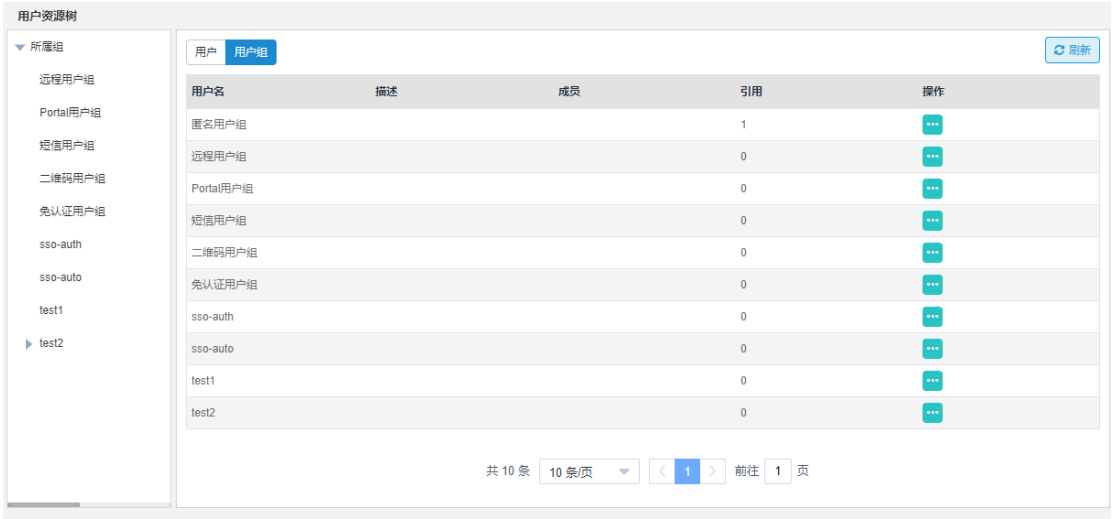
6.1.3. 用户资源树

用户资源树可以将每个用户以树形结构展示层级，支持 32 级层级，更加友好直观的展示。组织结构组包含用户和用户组，用户组可以包含用户和用户组。

在系统菜单点击“**对象>用户对象>用户资源树**”，点击<**用户**>显示设备上已配置的所有用户。



在系统菜单点击“**对象>用户对象>用户资源树**”，点击<**用户组**>显示设备上已配置的所有用户组。



6.1.4. LDAP 用户同步

除了上文所述的手动创建外，下一代防火墙还支持 LDAP 用户同步，将 LDAP 服务器上的用户同步到本地。

在系统菜单点击“**对象>用户对象>LDAP 用户同步**”，进入 **LDAP 用户同步**配置页面，可以实现对 LDAP 用户同步配置的新建、修改、删除、同步和查看详细信息功能。

在 **LDAP 用户同步**页面下点击<**新建**>创建新的 LDAP 用户同步，或在右侧“操作”列下点击图标，修改已有的 LDAP 用户同步配置。

LDAP 用户同步配置项及详细说明如下：

配置项	说明
启用	开启启用按钮启用 LDAP 同步。
LDAP 服务器/名称	选择一个设备上已有的 LDAP 服务器。有关 LDAP 服务器配置的更多信息，请参考 LDAP 服务器。
描述	输入 LDAP 同步任务的描述信息（可选）。
用户组	选择同步用户所属的用户组。
同步类型	同步类型有： ● **按 OU 组织同步**-同步过来的用户将会按照 LDAP 服务器上的设

	置添加到不同的组织结构中。 ● **按安全组同步**-同步过来的用户将会按照 LDAP 服务器上的设置添加到不通的属性组中。如果 LDAP 上同一个用户既属于 OU 又属于某属性组，系统会按照同步顺序保留最后同步的结果。

创建完成后，在用户同步页右侧“操作”列点击图标立即执行 LDAP 用户同步任务；或点击图标显示同步结果。

6.1.5. SNMP 用户同步

SNMP 用户同步作用于跨三层 IP-MAC 绑定，可将三层交换机中 ARP 表同步到设备，对同步来的信息进行 IP 地址和 MAC 地址绑定。

在系统菜单点击“**对象>用户对象>SNMP 用户同步**”，进入 **SNMP 用户同步**配置页面，可对 SNMP 用户同步执行新建、编辑、删除、同步和查看详细信息功能。

在 **SNMP 用户同步**页面下点击<**新建**>创建新的 SNMP 用户同步，或在右侧“操作”列下点击图标修改已有的 SNMP 用户同步任务。

SNMP 用户同步的配置项与详细说明如下：

配置项	说明
启用	开关按钮，打开后 SNMP 用户同步功能开始生效。
名称	用户自定义名称，长度限制为 1-31 字符。
描述	用户自定义字段，长度限制为 0-127 字符。
服务器 IP 地址	需要同步用户的交换机 IP 地址。
团体名	交换机中配置的团体名。
版本号	下拉菜单，目前仅支持 v2c。
任务周期	每间隔多久同步一次，默认 60 秒，范围 5-3600 秒。

创建完成后，在 SNMP 用户同步页右侧“操作”列点击图标立即执行 SNMP 用户同步任务，点击图标显示同步结果。

通过点击右侧按钮，查看同步结果。

通过点击同步结果右侧按钮，查看同步详情。

在同步详情页面，选择需要进行 IP MAC 绑定的条目，点击右侧按钮，可执行绑定操作。

可跳转页面至“对象>用户对象>IP-MAC 绑定”查看被绑定的内容。

6.1.6. IP-MAC 绑定

IP-MAC 绑定功能可对 ARP 欺骗攻击进行防御，启用该功能后，通过设备的 MAC 和 IP 需要和绑定关系保持一致，否则报文将被丢弃。IP-MAC 绑定对二层数据和三层数据生效。

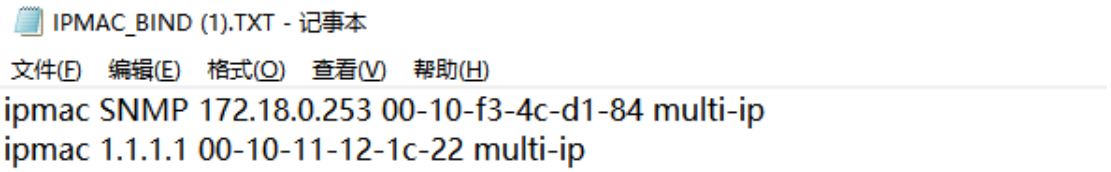
在系统菜单点击“对象>用户对象>IP-MAC 绑定”，进入 IP-MAC 绑定配置页面。可以实现对 IP-MAC 绑定的新建、修改、删除、查询、导入和导出功能。

在 IP-MAC 绑定页面下点击<新建>，或在右侧“操作”列下点击图标修改已有的 IP-MAC 绑定。

IP-MAC 绑定的配置项与详细说明如下：

配置项	说明
IP 地址	需要被绑定的 IP 地址，仅支持 IPv4。
MAC 地址	需要与 IP 相关联的 MAC 地址。
描述	用户自定义字段，长度限制为 0-127 字符。
唯一性	开启或关闭。 不开启唯一性时，只校验 MAC，匹配 MAC 则通过，反之则拒绝。 开启唯一性时，IP 和 MAC 均校验，IP 和 MAC 都匹配才可通过。

IP-MAC 绑定关系还支持通过 txt 文件进行导入导出，导出时点击<**导出**>按钮即可，导入时需选择正确内容的 txt 格式文件，格式如下图：



6.2. 用户认证

认证是为了保护系统的隐私数据与资源，使用户合法的访问内部系统的资源。下一代防火墙支持本地认证、短信认证、远程认证、Portal 认证、单点登录等多种认证方式，也支持多种认证方式组合使用，为用户带来高效与便捷。

6.2.1. RADIUS 服务器

在系统菜单点击“**对象>用户认证>RADIUS 服务器**”，进入 **RADIUS 服务器**配置页面，可以实现对 RADIUS 服务器的新建、修改和删除。

在 **RADIUS 服务器**页面下点击<**新建**>创建新的 RADIUS 服务器，或在右侧“操作”列下点击图标修改已有的 RADIUS 服务器配置。

RADIUS 服务器配置项及详细说明如下：

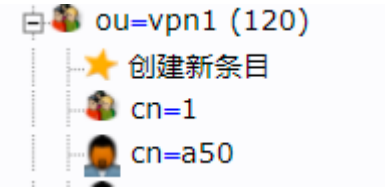
配置项	说明
名称	输入 RADIUS 服务器的名称。
服务器 IP	输入 RADIUS 服务器的 IP 地址。
服务器密码	输入 RADIUS 服务器的认证密码。
端口	输入 RADIUS 服务器的端口号，默认为 1812。

6.2.2. LDAP 服务器

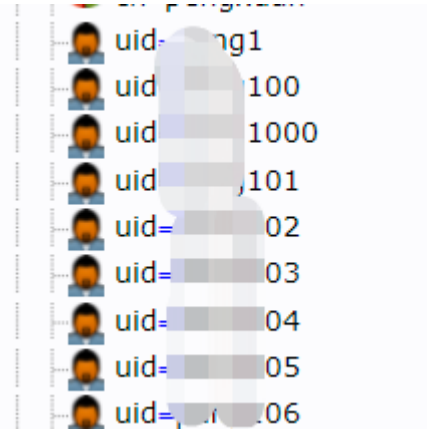
在系统菜单点击“**对象>用户认证>LDAP 服务器**”，进入 **LDAP 服务器**配置页面，可以实现对 LDAP 服务器的新建、修改和删除。

在 **LDAP 服务器**页面下点击<**新建**>创建新的 LDAP 服务器，或在右侧“操作”列下点击图标修改已有的 LDAP 服务器配置。

LDAP 服务器配置项及详细说明如下：

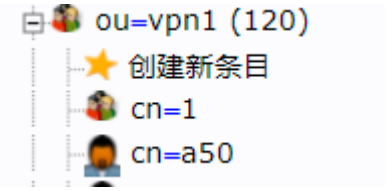
配置项	说明
名称	输入 LDAP 服务器的名称。
服务器类型	可选择 OpenLdap 或 Active Directory
服务器 IP	输入 LDAP 服务器的 IP 地址。
端口	输入 LDAP 服务器的端口号，默认为 389 端口。
区域名	指定 LDAP 服务器的区域名，即 LDAP 服务器收到认证请求时目录查询的起始点。
登录名属性	指 OpenLdap 和 Active Directory 两种登录方式所使用的登录名称属性，包括 cn、uid、sAMAccountName。具体使用如下： 选择 OpenLdap 用户认证方式： ● cn-即 common name，用户使用标识名进行认证，如下所示： 

- uid-即 User ID(Identification），如下所示：

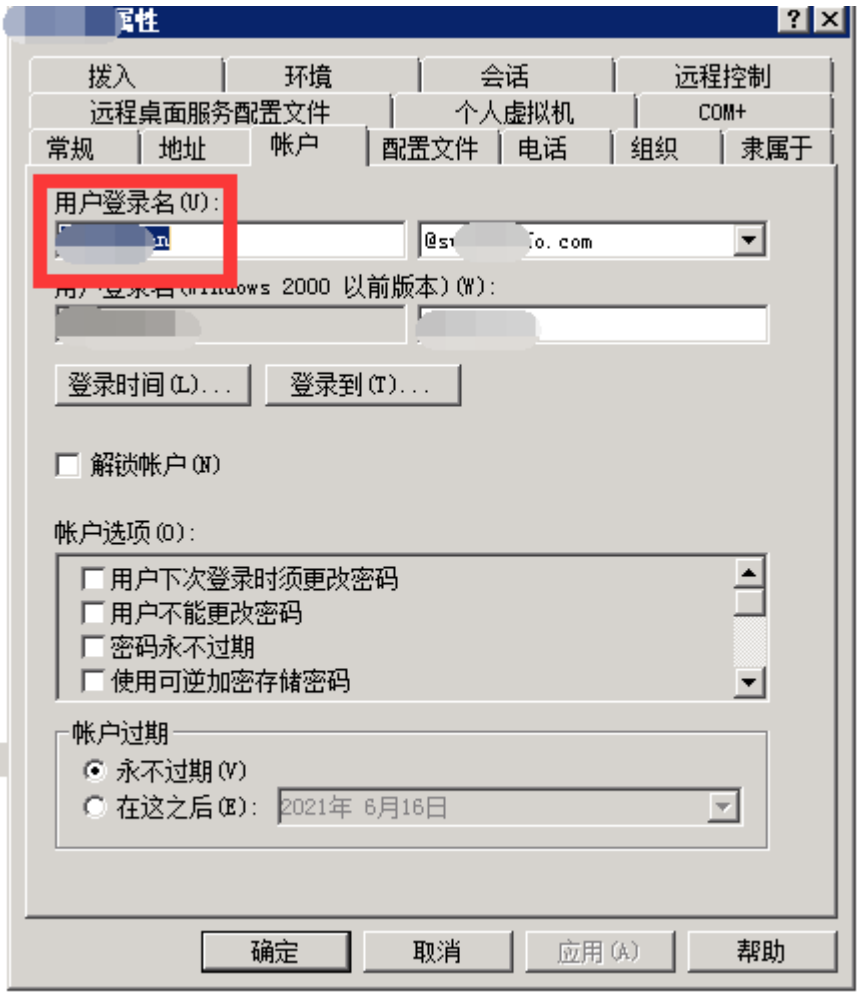


选择 Active Directory 用户认证方式：

- cn-即 common name，用户使用标识名进行认证，如下所示：



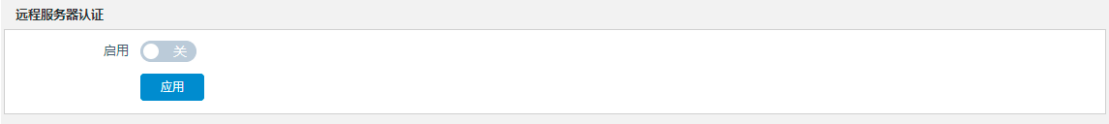
- sAMAccountName-用户使用登录名进行认证，如下所示：

	
管理员	输入 LDAP 服务器的管理员用户名。
密码	输入 LDAP 服务器的管理员密码。

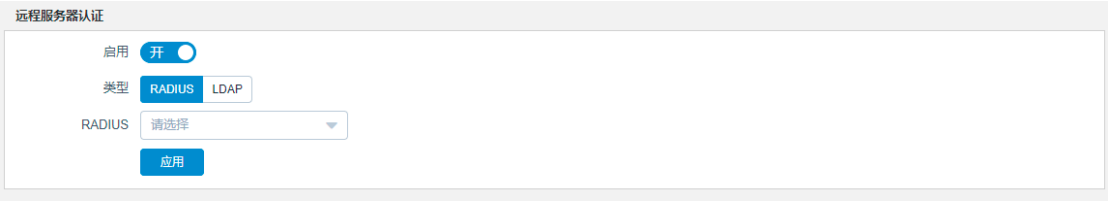
6.2.3. 远程服务器认证

用户认证使用远程服务器配置的认证服务器进行用户名、密码校验，校验通过后可继续访问。

在系统菜单点击“**对象>用户认证>远程服务器认证**”，进入**远程服务器认证**配置页面。



启用后，显示具体认证服务器类型。



远程服务器认证配置项及详细说明如下：

配置项	说明
启用	开启远程服务器认证。开启后可以选择认证服务器类型：RADIUS、LDAP。
类型	支持 RADIUS 和 LDAP 两种远程服务器认证方式。选择认证服务器后，下拉框显示配置的远程服务器名称。

6.2.4. 本地认证

启用本地认证功能后，用户打开浏览器访问 HTTP 页面会被定向到本地认证登录页面，输入正确的用户名和密码即可通过认证。

在系统菜单点击“**对象>认证管理>本地认证**”，进入**本地认证**配置页面。

本地认证配置项及详细说明如下：

配置项	说明
用户登录唯一性检查	
单一账号登录	同一时间只允许同一账号登录。如果出现用户尝试使用同一账号同时登录的情况，可选择踢出已登录用户，或进行同名用户再次登录。
允许重复登录	允许同一账号在多个终端登录。
更多设置	
客户端超时	基于心跳、流量超时两种方式触发超时时间刷新。 心跳超时：浏览器的认证页面定时与设备进行心跳交互，更新超时时间。 流量超时：用户流量经过设备，触发超时时间更新。
强制重登录间隔	**强制用户重新认证时间间隔，对 RADIUS、LDAP 和本地认证的用户生效。**

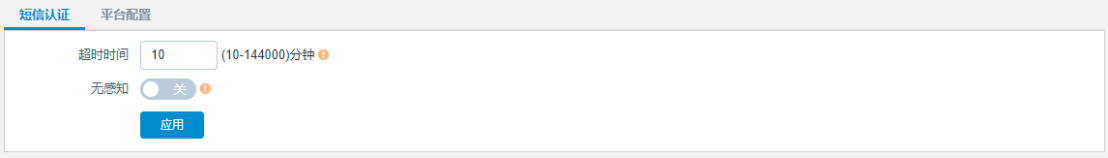
重定向 URL	设置本地认证的跳转页面，即认证成功后继续访问的页面，支持 HTTP 和 HTTPS。

6.2.5. 短信认证

通过短信的方式，进行用户认证。认证后，手机号即用户名。

6.2.5.1. 短信认证

在系统菜单点击“**对象>用户认证>短信认证>短信认证**”，进入**短信认证**配置页签。



短信认证配置项及详细说明如下：

配置项	说明
超时时间	设置客户端超时时间，超过设置时间后仍无流量通过，会强制客户端下线。
开启无感知	开启无感知功能，默认为 480 分钟。
无感知	设置用户无感知时间。在此时间内，通过短信认证的用户下线后重新登录时无需再次认证。

注意：

用户连续一段时间无流量产生，此段时间超过设置的超时时间，用户需要重新认证。

用户第一次认证登录成功开始，在设置的无感知时间范围内，用户下线后再次登录不需要再次认证，无感知时间优于超时时间。

6.2.5.2. 平台配置

在系统菜单点击“对象>用户认证>短信认证>平台配置”，进入平台配置页签。

平台配置的配置项及详细说明如下：

配置项	说明
短信平台	选择短信平台，目前只支持阿里云短信。以下需要输入字段请联系短信平台提供商了解详情： https://www.aliyun.com/product/sms
Access Key ID	输入短信平台获取到的 Access Key ID 值。
Access Key Secret	输入短信平台获取到的 Access Key Secret 值。
签名名称	输入短信平台获取到的签名名称。
模板 CODE	输入短信平台获取到的模板 CODE。

6.2.6. Portal 认证

在用户策略中启用 Portal 认证功能后，未认证用户上网时，设备强制用户登录到特定站点，用户可以免费访问其中的服务。当用户需要使用互联网中的其它信息时，必须在 Portal 网站进行认证，只有认证通过后才可以使用互联网资源。Portal 业务可以提供方便的管理功能，Portal 网站还可以开展广告、业务通知、个性化的业务等。

在系统菜单点击“对象>用户认证>Portal 认证”，进入 Portal 认证配置页面。

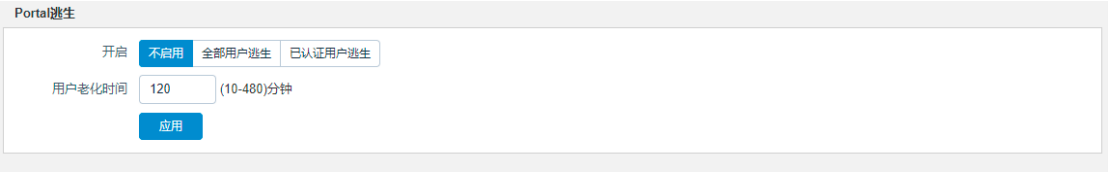
Portal 认证配置项及详细说明如下：

配置项	说明
认证服务器	点击选择一个认证服务器，当前 Portal 认证只支持联动的认证服务器为 RADIUS 服务器。RADIUS 服务器配置请参考 RADIUS 服务器。
portal 服务器	配置 Portal 服务器的 IP 地址信息。
超时时间	用户认证的超时时间，在时间段内没有流量设备会强制用户下线，默认时间为 15 分钟，可配置范围为 1-144000 分钟。
伪 portal 抑制	开启或关闭伪 portal 抑制
认证 URL	Portal 认证时重定向的 URL。

6.2.7. Portal 逃生

在使用 Portal 认证的组网中，用户接入都需要经过 Portal 服务器、认证服务器的认证，认证通过后才可以正常上线。当防火墙设备与 Portal 服务器或认证服务器通信中断后，未认证用户无法正常认证，无法正常使用网络。开启 Portal 逃生功能，当防火墙设备检测到与 Portal 服务器或认证服务器通信中断，利用 Portal 逃生功能机制，让用户仍可以正常的使用网络，并产生健康检查告警日志，通知管理员。

在系统菜单点击“**对象>用户认证>Portal 逃生**”，进入 **Portal 逃生**配置页面。



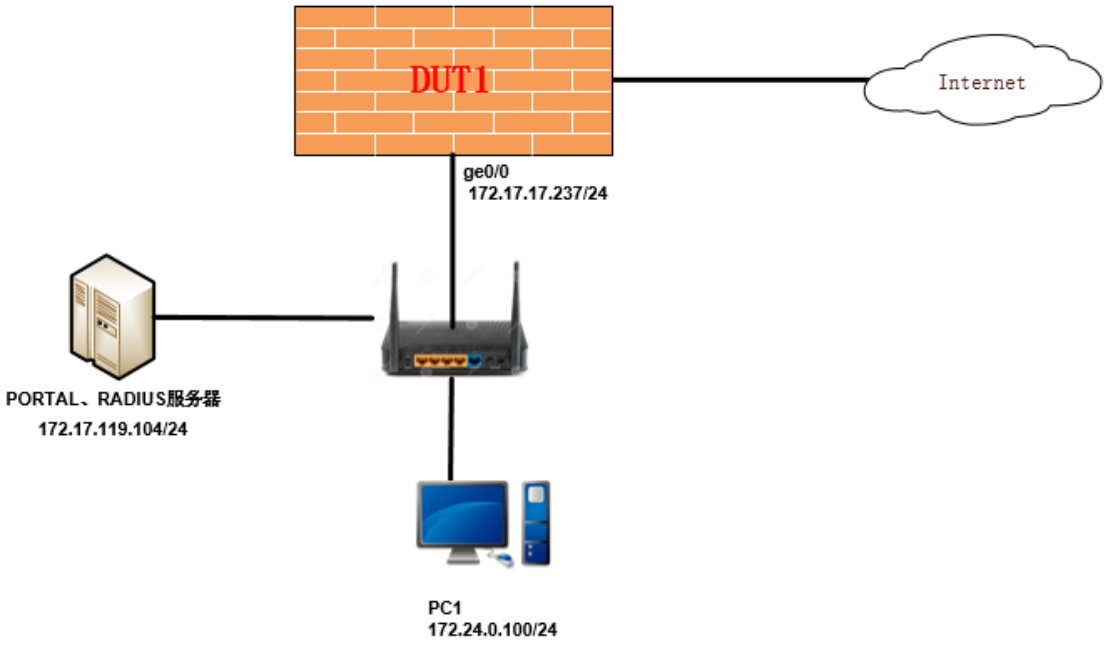
Portal 逃生配置项及详细说明如下：

配置项	说明
开启	开启方式有不启用、全部用户逃生、已认证用户逃生三种，默认为不启用，Portal 逃生功能方式有全部用户逃生、已认证用户逃生两种。选择任意一种即开启 Portal 逃生，自动关联地址探测，地址探测配置请参考健康检查。
用户老化时间	Portal 逃生用户认证上线时间。
地址探测	选择健康检查对象或健康检查组对象。设备会根据健康检查对象或健康检查组对象中的地址探测结果判断是否开启 Portal 逃生功能。

6.2.7.1. Portal 逃生配置示例

组网需求

如下图所示，PC1 进行 Portal 认证通过后可以访问互联网资源，要求当 PORTAL 服务器或 RADIUS 服务器的通讯中断后，已认证用户仍可以通过 Portal 逃生技术正常访问互联网资源。



配置步骤

1. 在系统菜单点击“**对象>地址>地址对象**”，点击<**新建**>创建地址对象，将需要进行 Portal 认证的 PC 网络加入地址对象中，具体信息请参考下图：

2. 在系统菜单点击“**对象>用户认证>RADIUS 服务器**”，点击<**新建**>，创建 RADIUS 服务器，具体信息请参考下图：

3. 在系统菜单点击“**对象>健康检查>健康检查**”，点击<**新建**>创建健康检查对象，对 PORTAL、RADIUS 服务器的地址进行健康检查探测，具体信息请参考下图：

4. 在系统菜单点击“**对象>用户认证>Portal 认证**”，配置 Portal 认证功能参数，具体信息请参考下图：

5. 在系统菜单点击“**对象>用户认证>Portal 逃生**”，配置启用 Portal 已认证用户逃生功能，同时地址探测关联步骤 3 中创建的健康检查对象，具体信息请参考下图：

6. 在系统菜单点击“**策略>用户策略>用户认证**”，点击<**新建**>创建用户认证策略，将 PC 访问互联网资源的流量限制需进行 Portal 认证，具体信息请参考下图：

7. 操作 PORTAL、RADIUS 服务器网段中断，此时 Portal 逃生功能生效，已认证用户可以正常访问互联网资源。

6.2.8. 单点登录

在系统菜单点击“**对象>用户认证>单点登录**”，进入**单点登录**配置页面。

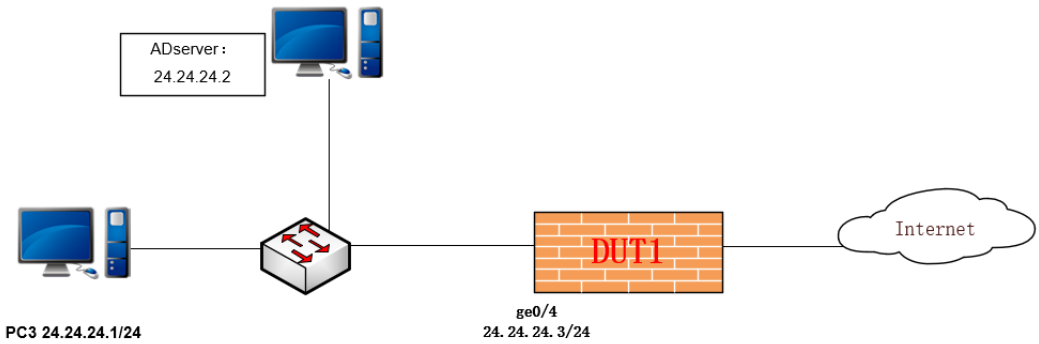
单点登录配置项及详细说明如下：

配置项	说明
启用	打开启用按钮，开启单点登录功能。
单点登录程序	点击下载域单点登录程序，包括登录、注销脚本和配置文件。
会话密钥	设置用于登录到 AD 域的密钥。
本地地址	设备的认证接口 IP 地址。
超时时间	未监测到用户流量的超时时间，指定时间，将用户下线。

6.2.8.1. 单点登录配置示例

组网要求

按照下图所示配置接口 IP 地址，要求 PC3 和 ADsever 互访正常，DUT1 访问外网正常。



配置步骤

1. 在设备 DUT1 上，点击系统菜单“**对象>用户认证>单点登录**”，进入**单点登录**配置页面，点击<**启用**>按钮，点击“下载单点登录程序”，并放到 ADsever 上：

2. 在 DUT1 系统菜单点击“**对象>认证管理>AD 域认证**”，进入 **AD 域认证**配置页面，按照下图进行配置：

3. ADsever 修改好配置文件，将脚本加入到登录和注销脚本目录正常。PC3 加入域账户，重启开机输入加域账户和密码，登录完成后，防火墙收到 PC 上线消息，在系统菜单点击“**监控>系统监控>在线用户统计**”，进入**在线用户统计**页面，点击 sso-auth 用户组，能看到 PC3 用户上线，认证方式为单点登录。

4. 认证成功后，用户之后访问外网无需再进行其他认证。

6.2.9. 动态口令

在系统菜单点击“对象>用户认证>动态口令”，进入动态口令配置页面。

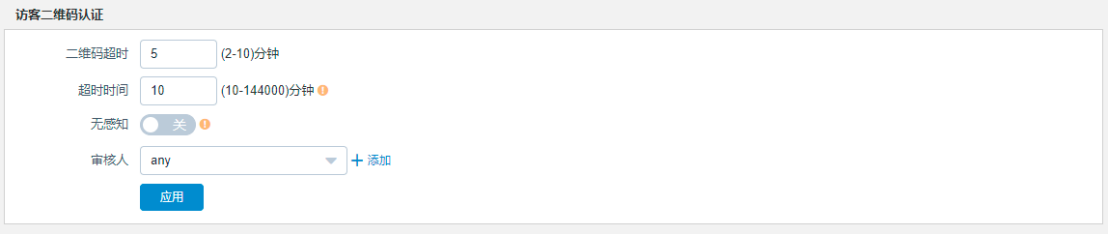
动态口令配置项及详细说明如下：

配置项	说明
模式	支持 TOTP 算法。
动态码长度	支持动态码长度 6 位和 8 位。
算法	目前仅支持 SHA1，且不可选择。
生成间隔	动态口令生成间隔 30-60 秒，默认 30 秒。

6.2.10. 访客二维码认证

启用访客二维码认证功能后，用户打开浏览器访问 HTTP 页面会被定向到访客二维码认证登录页面，必须由已通过认证并有审核权限的用户扫描二维码确认后访客才可以继续访问页面。

在系统菜单点击“对象>用户认证>访客二维码认证”，进入访客二维码认证配置页面。



访客二维码认证配置项及详细说明如下：

配置项	说明
二维码超时	设置认证页面的二维码超时时间。二维码截图超过超时时间后二维码失效，浏览器页面打开二维码不断网连接正常的情况下二维码会自动刷新不失效。
超时时间	设置客户端超时时间，超过设置时间后仍无流量通过，会强制客户端下线。
无感知	设置用户无感知时间。在此时间内，通过短信认证的用户下线后重新登录时无需再次认证。
审核人	选择访客二维码认证的审核人，any 表示任意已通过认证的用户。有关用户配置的更多信息，请参考用户对象。

注意：

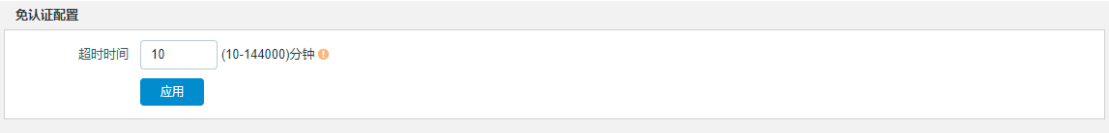
用户连续一段时间无流量产生，此段时间超过设置的超时时间，用户需要重新认证。

用户第一次认证登录成功开始，在设置的无感知时间范围内，用户下线后再次登录不需要再次认证，无感知时间优于超时时间。

6.2.11. 免认证配置

启用免认证功能后，用户打开浏览器访问 HTTP 页面会被定向到免认证页面，无需提供任何认证信息，只需点击<**登录**>即可登录。

在系统菜单点击“**对象>用户认证>免认证配置**”，进入**免认证配置**页面。



免认证配置项及详细说明如下：

配置项	说明
超时时间	设置客户端超时时间，超过设置时间后仍无流量通过，会强制客户端下线。

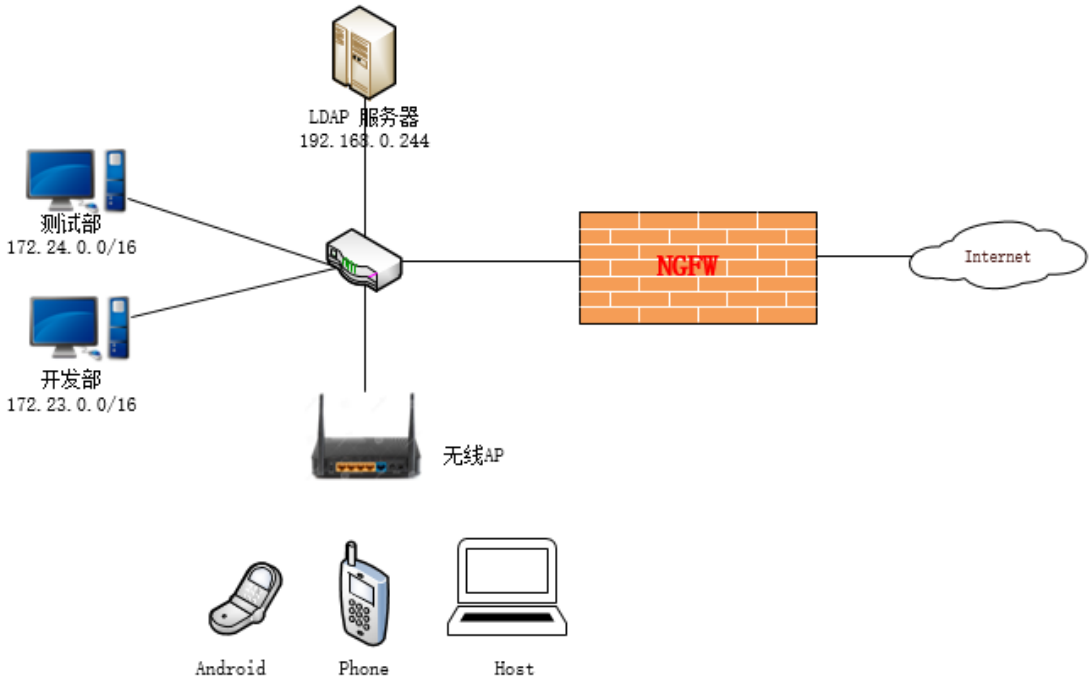
注意：

用户连续一段时间无流量产生，此段时间超过设置的超时时间，用户需要重新认证。

6.2.12. 混合用户认证配置示例

组网需求

如下图所示，公司内网搭建有第三方 LDAP 服务器，用户名存放在 LDAP 服务器上。



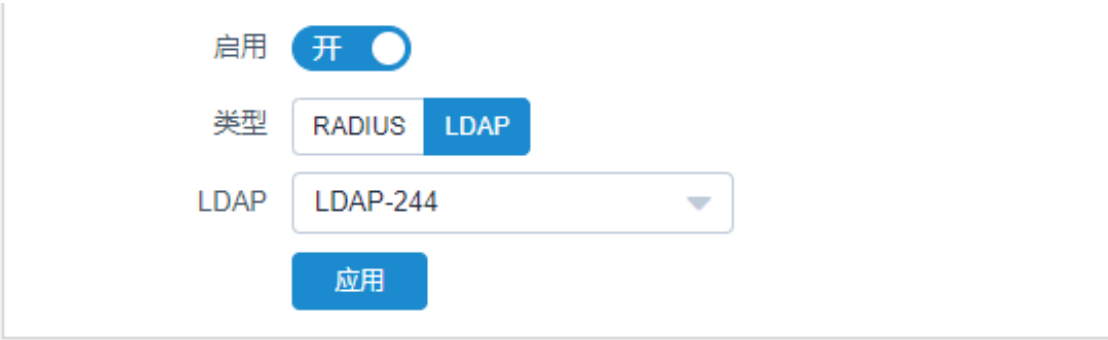
具体要求如下：

- 测试部进行本地认证，用户名密码存储在 LDAP 服务器上。
- 开发部进行短信认证。
- 其他移动终端连接 WiFi 后使用访客二维码认证。

配置步骤

1. 在系统菜单点击“**对象>用户认证>LDAP 服务器**”，点击<**新建**>创建 LDAP 服务器：

2. 在系统菜单点击“**对象>用户认证>远程服务器认证**”开启远程认证，类型为 LDAP，选择步骤 1 新建 LDAP 服务器，如下所示：



3. 在系统菜单点击“**对象>用户认证>短信认证**”配置短信认证配置，如下所示：

4. 在系统菜单点击“**对象>用户认证>访客二维码认证**”配置访客二维码认证配置，如下所示：

5. 在系统菜单点击“**系统>系统设置>DNS**”配置 DNS 服务器可正常访问外网，如下所示：

6. 在系统菜单点击“**对象>地址>地址对象**”新建开发部、测试部和 wifi 用户的地址对象，如下所示：

7. 在系统菜单点击“**策略>防火墙策略>一体化策略**”新建一体化策略，如下所示：

8. 在系统菜单点击“**策略>NAT 策略>源 NAT**”新建源 NAT 策略，用户可通过下一代防火墙正常访问外网，如下所示：

9. 在系统菜单点击“**策略>用户策略>用户认证**”新建测试部、开发部和 WiFi 用户对应用户认证策略，如下所示：

10. 配置完成后，测试部终端发起 HTTP 访问时会弹出如下本地认证页面，用户可以使用本地用户和 LDAP 服务器上的用户名、密码进行认证：

开发部终端发起 HTTP 访问时会弹出如下短信认证页面，用户需输入正确的验证码进行认证：

移动终端连接 WiFi 时会弹出如下访客二维码认证页面，需要认证过并有审核权限的用户进行认证：

审核人识别二维码，输入用户名，认证成功：

11. 在系统菜单点击“**统计>在线用户统计**”查看设备上已录入的远程认证、短信认证和访客二维码认证所有用户：

6.3. 应用

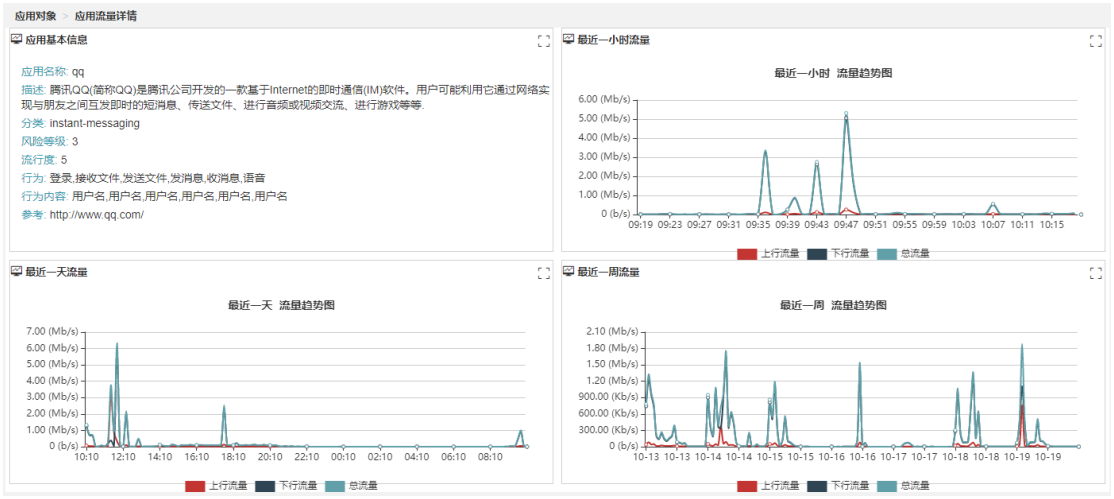
为了方便用户的配置和管理，下一代防火墙中引入了应用对象的概念。在防火墙策略、应用策略、路由策略的等配置中，可以引用应用对象来定义配置生效的条件。应用实际上包括应用对象、应用组两个部分。

- **应用对象**-具体的用户应用，如下载软件、即时通信软件，不需要用户配置。
- **应用分类**-查看预定义应用分组，不需要用户配置。
- **应用组**-需要用户自行配置。
- **自定义应用**-用户可以自己定义应用。

6.3.1. 应用对象

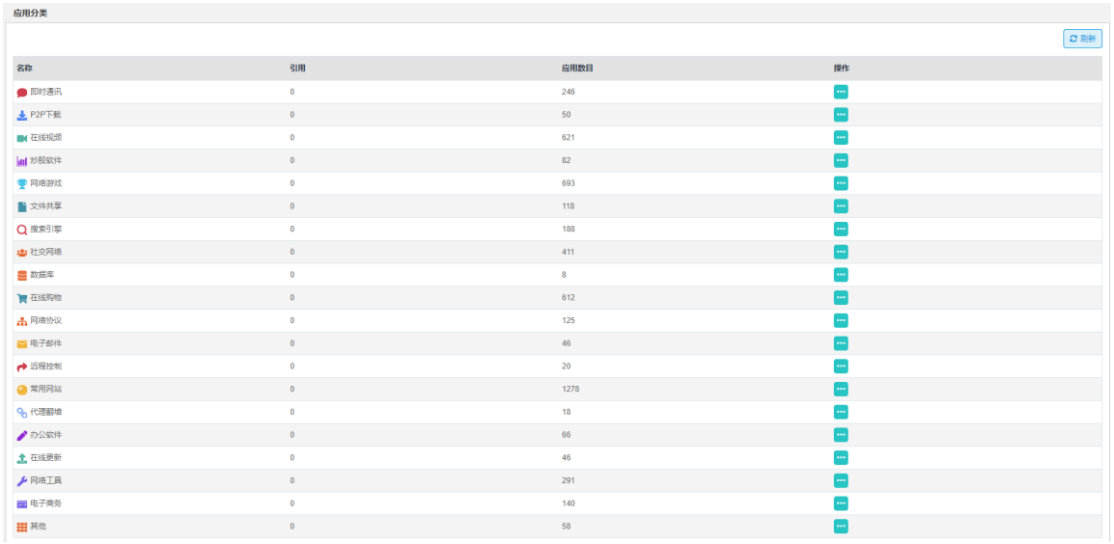
在系统菜单点击“**对象>应用>应用对象**”查看设备上所有预定义应用类别和具体应用信息。

在**应用对象**页面下，点击右侧“操作”列下的，可查看应用对象的应用流量详情。

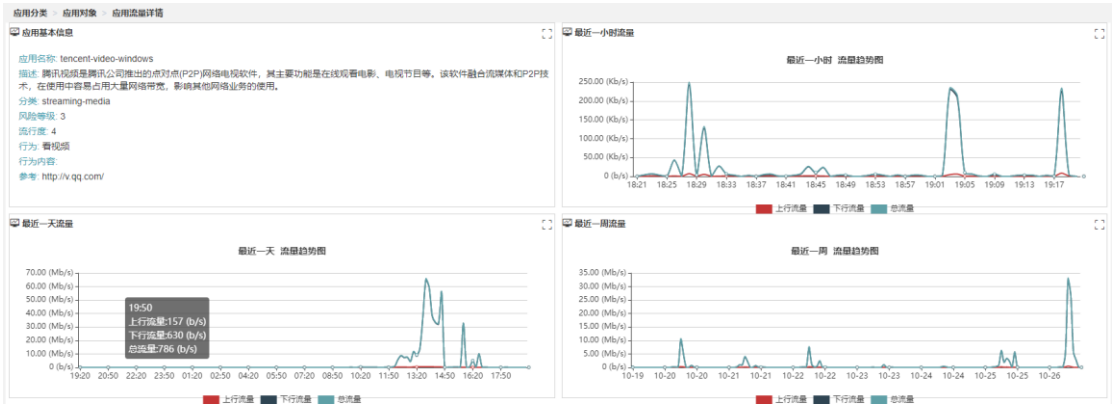


6.3.2. 应用分类

在系统菜单点击“**对象>应用>应用分类**”查看设备上所有的应用对象分类页面。



在**应用分类**页面下，点击“操作”列的…，可跳转到应用对象查看具体的应用流量详情。



6.3.3. 应用组

在系统菜单点击“**对象>应用>应用组**”，进入**应用组**配置页面，可以实现对应用组的新建、修改和删除。

在**应用组**页面下点击<**新建**>创建新的应用组，或在右侧“操作”列点击这个图标修改已有的应用组。

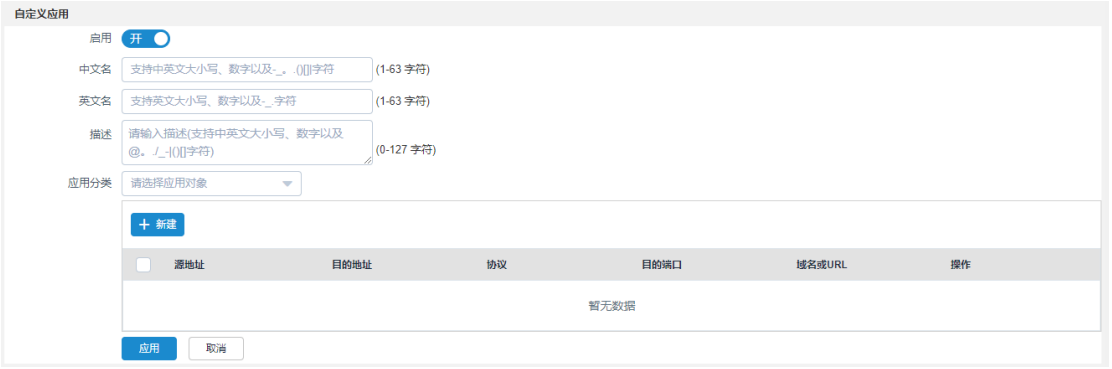
应用组的配置项及详细说明如下：

配置项	说明
名称	为新建应用对象的名称。
描述	输入应用组的描述信息（可选）。
选择应用对象	为系统所支持的所有应用对象。

6.3.4. 自定义应用

在系统菜单点击“**对象>应用>自定义应用**”，进入**自定义应用**配置页面，可以实现对自定义应用的新建、修改和删除。

在**自定义应用**页面下点击<**新建**>创建新的自定义应用，或在右侧“操作”列下点击图标修改已有的自定义应用。



自定义应用的配置项及详细说明如下：

配置项	说明
中文名	输入自定义应用的中文名。

英文名	输入自定义应用的英文名。
描述	输入自定义应用的描述（可选）。
应用分类	选择自定义应用所属的应用组（必选）。
新建	点击<**新建**>，填写自定义应用的源地址、目的地址、协议、目的端口、域名或 URL。设备将根据这些规则信息对自定义应用进行识别。  自定义应用配置项及详细说明如下： ● **源地址**-可选择 any、系统预置的 ISP 的主要地址对象或已经创建好的地址对象组，也可点击<**添加**>，新建 IPv4 地址对象，请参考地址。 ● **目的地址**-可选择 any、系统预置的 ISP 的主要地址对象或已经创建好的地址对象组，也可点击<**添加**>，新建 IPv4 地址对象，请参考地址。 ● **协议**-自定义应用基于 TCP、UDP 两种协议。 ● **目的端口**-配置自定义应用的目的端口范围。 ● **域名或 URL**-配置自定义应用的域名或 URL。

6.4. 地址

为了方便用户的配置和管理，下一代防火墙中引入了地址对象的概念。地址分为地址对象和地址组，地址组是地址对象的集合。在其它功能的配置中(如防火墙策略、NAT 策略、路由策略)，可以引用地址对象来定义配置生效的条件。

6.4.1. 地址对象

在系统菜单点击“**对象>地址>地址对象**”，进入**地址对象**配置页面，可查看设备上已有的地址对象，其中前面 7 个地址对象是设备内置的 IPv4 地址对象，分别是 any(任意地址)、ISP_CMCC.dat（中国移动）、ISP_UNICOM.dat(中国联通)、ISP_CT.dat(中国电信)、ISP_CTT.dat（中国铁通）、ISP_CERNET.dat(教育网)和 ISP_INTL.dat（印度）。用户无法修改或删除内置的 IPv4 地址对象。

在已创建的域名地址对象右侧“操作”列下点击图标查看域名对应的解析地址。

在**地址对象**页面下点击<**新建**>，创建 IPv4 的地址对象，或在右侧“操作”列下点击图标修改已有的地址对象。

IPv4 地址对象配置项及详细说明如下：

配置项	说明
名称	输入 IPv4 地址对象的名称。
描述	输入 IPv4 地址对象的描述信息（可选）。
类型	基于 IPv4 类型的地址对象。
包含 IP 地址	
主机	主机 IPv4 的地址。

	 主机配置项及详细说明如下： ● 输入一个 IPv4 的主机地址。 ● 点击“操作”列下的，可以删除配置的 IPv4 的主机地址。
子网	IPv4 网段地址。  子网配置项及详细说明如下： ● 输入一个 IPv4 的子网。 ● 点击“操作”列下的，可以删除配置的 IPv4 的子网。
范围	IPv4 地址池范围。  范围配置项及详细说明如下： ● 输入一个 IPv4 地址的范围。 ● 点击“操作”列下的，可以删除配置的 IPv4 的范围。
ISP 地址库	系统预置了 ISP 的主要地址信息，ISP 地址库里选择预置的地址信息。

	 选择地址库，点击“添加”。
域名	输入域名，选择 DNS 刷新时间，获取 DNS 服务器状态。  域名配置项及详细说明如下： ● 输入一个域名，点击添加。 ● 选择 DNS 刷新时间，点击<**获取 DNS 服务器状态**>。如未配置 DNS 服务器，根据提示，点击“确认”，跳转到 DNS 配置页面。
排除 IP 地址	设置排除的 IP 地址。

在**地址对象**页面下点击<**新建**>，创建 IPv6 的地址对象。

IPv6 地址对象配置项及详细说明如下：

配置项	说明
名称	输入 IPv6 地址对象的名称。
描述	输入 IPv6 地址对象的描述信息（可选）。
类型	基于 IPv6 类型的地址对象。
包含 IP 地址	
主机	主机 IPv6 的地址。

	 主机配置项及详细说明如下： ● 输入 IPv6 主机地址。 ● 点击“操作”列下的，可以删除配置的 IPv6 的主机地址。
子网	IPv6 网络地址。  子网配置项及详细说明如下： ● 输入一个 IPv6 的子网。 ● 点击“操作”列下的，可以删除配置的 IPv6 的子网地址。
范围	IPv6 地址范围。  范围配置项及详细说明如下： ● 输入一个 IPv6 地址的范围。 ● 点击“操作”列下的，可以删除配置的 IPv6 地址的范围。
排除 IP 地址	设置排除 IPv6 地址类型的主机、子网和范围，即不适用于该对象的地址。

在**地址对象**页面下点击<**新建**>，创建 MAC 的地址对象。

MAC 地址对象配置项及详细说明如下：

配置项	说明
名称	输入 MAC 地址对象的名称。
描述	输入 MAC 地址对象的描述信息（可选）。
类型	基于 MAC 类型的地址对象。
包含 IP 地址	设置 MAC 地址。  MAC 地址配置项及详细说明如下： ● 输入一个 MAC 地址。 ● 点击“操作”列下的，可以删除配置的 MAC 地址。

在**地址对象**页面下点击<**新建**>，创建 IP-MAC 的地址对象。

IP-MAC 地址对象配置项及详细说明如下：

配置项	说明
名称	输入 IP-MAC 地址对象的名称。
描述	输入 IP-MAC 地址对象的描述信息（可选）。
类型	基于 IP-MAC 类型的地址对象。
包含 IP 地址	设置 IP-MAC 地址。 

	IP-MAC 配置项及详细说明如下： ● 输入 IPv4 的地址和 MAC 地址。 ● 点击“操作”列下的，可以删除配置的 IPv4 地址和 MAC 地址。

6.4.2. 地址组

在系统菜单点击“**对象>地址对象>地址组**”，进入**地址组**配置页面，可以实现对地址组的新建、修改和删除。

在**地址组**页面下点击<**新建**>创建新的地址组对象，或在右侧“操作”列点击这个图标修改已有的地址组对象。

地址组配置项及详细说明如下：

配置项	说明
名称	输入地址组对象的名称。
描述	输入地址组对象的描述信息（可选）。
成员	可选择系统默认的地址对象或已创建的地址对象。

6.4.3. 备份恢复

在系统菜单点击“**对象>地址对象>备份恢复**”，可对地址对象进行导入和导出配置。

备份恢复配置项及详细说明如下：

配置项	说明
地址对象导入	导入已有的地址对象信息。
地址对象导出	导出当前的地址对象配置信息。

6.5. 服务

为了方便用户的配置和管理，下一代防火墙中引入了服务对象的概念。在其它功能(如防火墙策略、NAT 策略、路由策略)的配置中，可以引用服务对象来定义配置生效的条件。

服务对象里包括预定义服务，自定义服务，服务组。

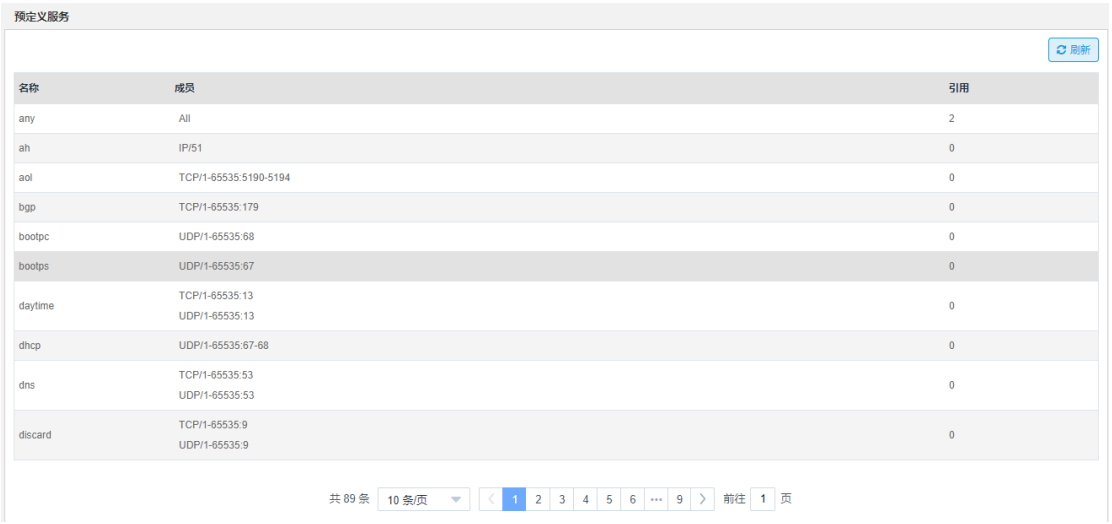
- **预定义服务**-系统预先添加服务，用户不可编辑或删除。
- **自定义服务**-需要用户自行配置添加。

- **服务组**-服务组是服务的集合。

6.5.1. 预定义服务

在系统菜单点击“**对象>服务>预定义服务**”，进入**预定义服务**配置页面，显示设备上所有的预定义服务。预定义服务为设备出厂时内置，不可删除或编辑。

下图是部分系统预定义服务：



6.5.2. 自定义服务

在系统菜单点击“**对象>服务>自定义服务**”，进入**自定义服务**配置页面，可以实现对自定义服务的新建、修改和删除。

在**自定义服务**页面下点击<**新建**>创建新的自定义服务，或在右侧“操作”列点击这个图标修改已有的自定义服务。

自定义服务的配置项及详细说明如下：

配置项	说明
名称	自定义服务的名称。
描述	对自定义服务的描述。
成员	● **协议**-可以自定义的服务协议（TCP，UDP，ICMP，IP）。 ● **源端口**-协议源端口号。 ● **目的端口**-协议目的端口号。

注意：

自定义服务对象若被引用，删除操作框被置灰，不可操作。

6.5.3. 服务组

在系统菜单点击“**对象>服务>服务组**”，进入**服务组**配置页面，显示设备上所有的服务组。

在**服务组**页面下点击<**新建**>创建新的服务组，或在右侧“操作”列点击这个图标修改已有的服务组。

服务组的配置项及详细说明如下：

配置项	说明
名称	服务组的名称。
描述	对服务组的描述。
成员	显示已有的服务对象（包括预定义服务、自定义服务、其他服务组），可从中选择服务对象添加到服务组中。

注意：

服务组对象若被引用，删除操作框被置灰，不可操作。

6.6. 资源

网络环境中，提供访问服务的设备被定义为资源。资源对象是由服务与地址组成，被用户资源策略引用，通过策略配置可以限制这些资源的访问的权限。

6.6.1. 资源对象

在系统菜单点击“**对象>资源对象>资源对象**”，进入**资源对象**配置页面，可以实现对资源对象的新建、修改、删除、查询、导出、导入和重置的功能。

在**资源对象**页面点击<**新建**>创建新的资源对象，或在右侧“操作”列点击这个图标修改已有的资源对象。

资源对象配置项及详细说明如下：

配置项	说明
名称	资源对象名称。
目的地址	默认 any，用来匹配用户流量中的目的地址，有关目的地址配置的更多信息，请参考地址。
服务	默认 any，用来匹配用户流量中的协议，有关服务配置的更多信息，请参考服务。
描述	资源对象的描述信息，非必填。

6.6.2. 资源组

资源组是资源对象的集合，被用户资源策略引用。

在系统菜单点击“**对象>资源>资源组**”，进入**资源组**配置页面，可以实现对资源组的新建、修改、删除、查询和重置的功能。

在**资源组**页面点击<**新建**>创建新的资源组，或在右侧“操作”列点击这个图标修改已有的资源组。

资源组配置项及详细说明如下：

配置项	说明
名称	资源组名称。
成员	选择加入到该资源组的资源对象或资源组。
描述	资源组描述，非必填项。

6.7. 时间

为了方便用户配置和管理，引入了时间的概念，时间分为绝对时间和周期时间，在其它功能的配置中可以引用时间来定义配置生效的条件。

6.7.1. 绝对时间

在系统菜单点击“**对象>时间>绝对时间**”，进入**绝对时间**配置页面，设备出厂时内置名称为 always 的绝对时间数据无法修改或删除。

在**绝对时间**页面点击<**新建**>创建新的绝对时间，或在右侧“操作”列点击这个图标修改已有的绝对时间。

绝对时间配置项及详细说明如下：

配置项	说明
名称	绝对时间名称。
描述	绝对时间描述，非必填项。
开始时间	点击开始时间输入栏选择开始时间。
结束时间	点击结束时间输入栏选择结束时间。

6.7.2. 周期时间

周期时间中可以定义有效时间范围和有效时间段。有效时间范围只能有一个，而有效时间段可以有多个。有效时间段之间为或的关系，满足其中一个即可；有效时间范围和有效时间段之间是与的关系，都满足才生效。

在系统菜单点击“**对象>时间>周期时间**”，进入**周期时间**配置页面，可以实现对周期时间的新建、修改和删除。

在**周期时间**页面点击<**新建**>创建新的周期时间，或在右侧“操作”列点击图标修改已存在的周期时间。

周期时间配置项及详细说明如下：

配置项	说明
名称	周期时间名称。
描述	周期时间描述，非必填。
循环日期	配置循环日志。点击<**新建**>勾选周计划，选择时间；或在“操作”列点击图标修改已存在的循环日期。
设置起止日期	开启设置起止日期开关，选择起始时间、结束时间。

6.8. 关键字

关键字对象主要用于支持设备的关键字过滤功能，在应用控制、Web 访问审计策略中被引用，参与策略的条件匹配。

在系统菜单点击“**对象>关键字**”，进入**关键字**配置页面，可以实现对关键字的新建、修改和删除。

在**关键字**页面点击<**新建**>创建新的关键字对象，或在右侧“操作”列点击图标修改已存在的关键字对象。

关键字配置项及详细说明如下：

配置项	说明
名称	关键字名称。
描述	关键字描述，非必填。
关键字内容	配置关键字内容。关键字以回车分隔，注意每条内容不能超过 63 个字符，并且不能超过 128 条记录。

6.9. URL

URL，统一资源定位符。互联网上的每一个文件、每个网页都有一个唯一的 URL。系统中内置了默认的 URL 库并根据属性进行分类，用户也可以根据需求自定义 URL 对象。URL 对象主要被 Web 访问审计策略引用，参与策略的条件匹配。

6.9.1. 预定义 URL

系统中内置默认的 URL 即预定义 URL。

在系统菜单点击“**对象>URL>预定义 URL**”，进入**预定义 URL** 页面，共 112 种分类。

6.9.2. 自定义 URL

在系统菜单点击“**对象>URL>自定义 URL**”，进入**自定义 URL** 配置页面，可以实现对自定义

URL 的新建、修改和删除。

在**自定义 URL** 页面点击<**新建**>创建新的自定义 URL 对象，或在右侧“操作”列点击图标修改已有的自定义 URL 对象。

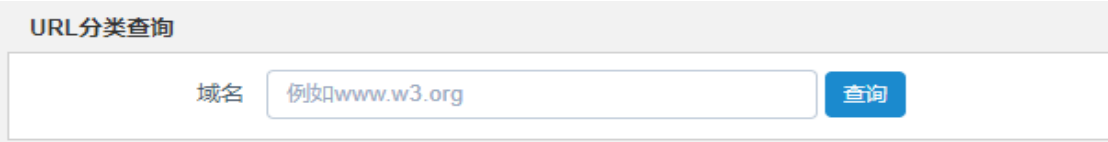
自定义 URL 配置项及详细说明如下：

配置项	说明
名称	自定义 URL 的名称。
描述	自定义 URL 的描述。

内容	自定义 URL 的配置内容。如：www.baidu.com 且 URL 以回车分隔，注意每条 URL 记录不能超过 127 个字符，并且不能超过 64 条 URL 记录。

6.9.3. URL 分类查询

在系统菜单点击“**对象>URL>URL 分类查询**”，进入 **URL 分类查询**配置页面。



在 **URL 分类查询**页面，输入域名点击<**查询**>可查看 URL 为预定义 URL 或自定义 URL 中的分类。

URL 分类查询配置项及详细说明如下：

配置项	说明
域名	配置域名。例如：www.w3.org。

6.10. 文件类型

文件类型对象主要被 Web 访问审计策略引用，参与策略的条件匹配。

在系统菜单点击“**对象>文件类型**”进入**文件类型**配置页面,可以实现对文件类型的新建、修改和删除。

在**文件类型**页面点击<**新建**>创建新的文件类型，或在右侧“操作”列点击图标修改已有的文件类型。

文件类型配置项及详细说明如下：

配置项	说明
名称	文件类型名称。
描述	文件类型描述。
文件类型	配置文件类型。（exe 代表所有后缀为.exe 的文件，各种文件类型以回车分隔,注意每种文件类型不能超过 15 个字符,并且不能超过 32 个文件类型）。

6.11. 资产

该功能所描述的资产为信息资产，资产的信息包括资产 IP、描述、用户、部门、重要度、操作系统、可用服务、来源、状态等等，通过主动添加、被动流量发现和关联功能，实现资产统计。（端口扫描与 EDR 联动添加资产的方式请参考端口扫描与 EDR 策略这两个功能）。

6.11.1. 资产管理

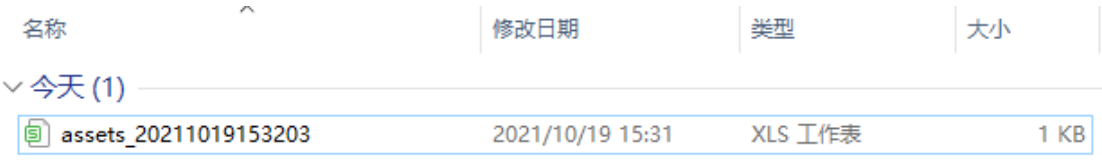
在系统菜单点击“**对象>资产>资产管理**”，显示出设备上统计的所有的资产，可对资产进行新建、编辑、删除、查询、导出和导入功能。

在**资产管理**页面点击<**新建**>创建一个新的资产，或者在右侧“操作”列下点击图标编辑已存在的资产信息。

资产管理配置项及详细说明如下：

配置项	说明
类型	设置资产的 IP 地址类型，分为 IPV4 与 IPV6。
资产 IP	设置资产的 IP 地址。
描述	设置资产的描述信息。
用户	设置资产的用户信息。
部门	设置资产的部门信息。
重要度	设置资产的重要度，支持配置普通资产与核心资产两种类型。
操作系统	设置资产的操作系统，支持配置 windows、linux、unix、ios、android 操作系统。

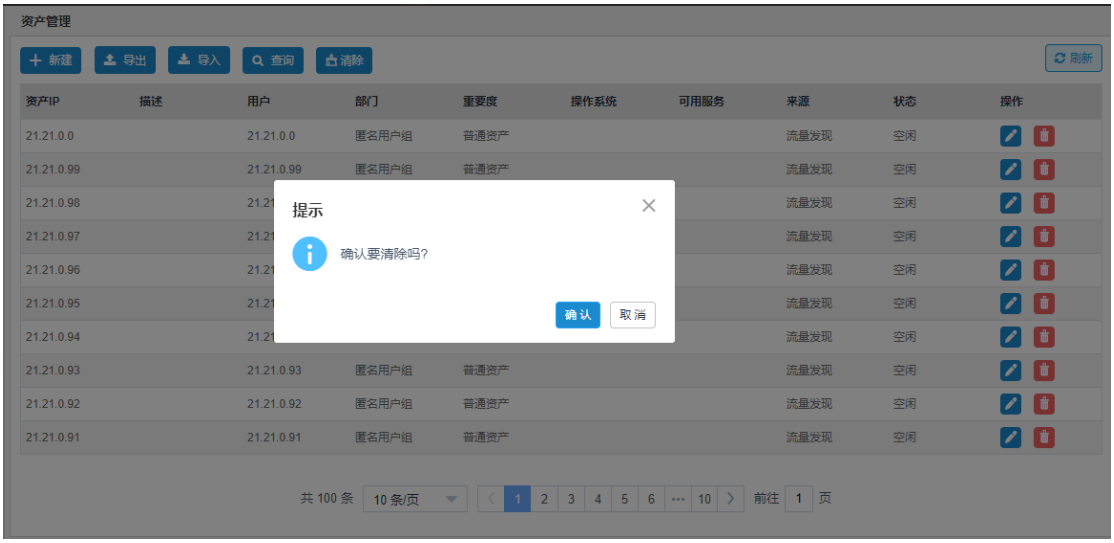
点击<**导出**>，可将已存在的资产全部以表格的形式导出。



点击<**导入**>，选择导出的 csv 文件，可将文件中的资产全部导入。

点击<**查询**>，可以根据资产 IP、描述、用户、部门、重要度、操作系统、可用服务、状态字段来进行精准查询。

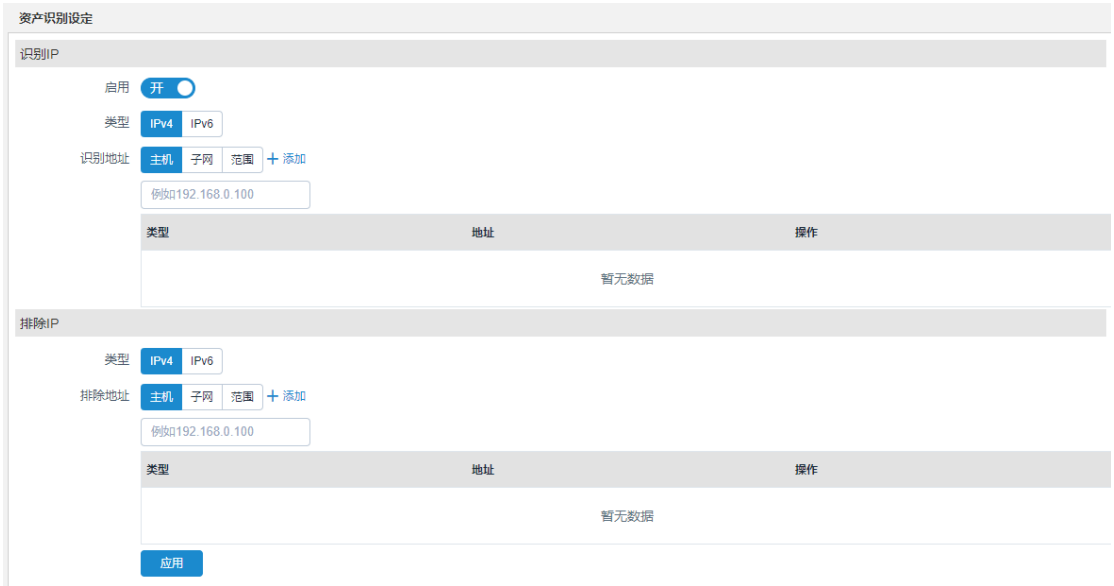
点击<**清除**>，可清除当前所有的资产。



6.11.2. 资产识别设定

该功能主要对流量发现方式统计资产的范围进行限制，用户可以通过配置排除范围与识别范围来精准的统计某地址范围内的资产。

在系统菜单点击“**对象>资产>资产识别设定**”，进入**资产识别设定**配置页面，开启“启用”后可配置识别地址、排除地址。



资产识别设定配置项及详细说明如下：

配置项	说明
启用	资产识别设定功能的开关，开启状态功能生效，关闭状态功能不生效。
类型	设置资产的 IP 地址类型，分为 IPV4 与 IPV6。
识别地址	设置资产的识别地址，支持配置主机、子网与范围三种类型。
排除地址	设置资产的排除地址，支持配置主机、子网与范围三种类型。

6.12. 健康检查

6.12.1. 健康检查

健康检查用来对服务器或者链路进行探测，来获取服务器或者链路的健康状况。一旦发现服务器或链路故障，将执行引用健康检查对象的策略动作。支持的健康检查方式包括：ICMP、TCP HALF OPEN 和 DNS。

在系统菜单点击“**对象>健康检查>健康检查**”，进入**健康检查**配置页面，可以实现对健康检查的新建、修改和删除。

在**健康检查**页面下在点击<**新建**>创建新的健康检查，或在右侧“操作”列下点击图标修改已有的健康检查。

健康检查配置项与详细说明如下：

配置项	说明
名称	设置健康检查的名称。
类型	支持 ICMP、TCP HALF OPEN 和 DNS 三种，默认选择 ICMP。
配置	
间隔	每次发起检查的间隔时间，默认 16 秒，允许范围：1-86400 秒。
最大重试次数	几次后统计结果，默认 3 次，允许范围：1-10 次。
超时时间	多久无回应算作超时，默认 5 秒，允许范围：1-86400 秒。
平均延迟	延迟要小于等于配置的时间，默认 60000 毫秒，允许范围：1-60000 毫秒。
丢包率	丢包率小于配置的百分比，默认 100%，允许范围：1%-100%。

质量采样范围	采集多少次信息来计算结果，默认 10 次，允许范围：10-50 次。
目标 IP 地址类型	仅支持 IPv4 地址类型。
IP 地址	填写需要检查的目标 IP 地址。
端口	当类型选择 TCP HALF OPEN 或 DNS 时才进行展示，输入需要探测的目的端口，允许范围：1-65535。
域名	当类型选择 DNS 时才进行展示，输入需要发起 DNS 探测的目的域名。

6.12.2. 健康检查组

根据需要，可以将多种健康检查组合到一起，形成一个健康检查组，对一个服务器或者链路进行监控。

在系统菜单点击“**对象**>**健康检查**>**健康检查组**”，进入**健康检查组**配置页面，可以实现对健康检查组的新建、修改和删除。

在**健康检查组**页面下点击<**新建**>创建新的健康检查组，或在右侧“操作”列点击这个图标修改已有的健康检查组。

健康检查组配置项与详细说明如下：

配置项	说明
名称	设置健康检查组的名称。
协议类型	仅支持 IPv4 协议类型。
健康检查方法选择	选择需要加入健康检查组的健康检查配置。
有效性	需要匹配已选项中的多少项。
通过的健康检查方法数	有效性要求选择至少时，可输入，默认值为 1，允许范围：1-5。 输入值不能大于已选的健康检查对象数。

6.13. 证书

PKI（公钥基础设施）技术采用证书管理公钥，通过第三方的可信任机构--认证中心 CA(Certificate Authority)，把用户的公钥和用户的其他标识信息（如名称、e-mail、身份证号等）捆绑在一起，在 Internet 网上验证用户的身份。目前，通用的办法是采用建立在 PKI 基础之上的数字证书，通过把要传输的数字信息进行加密和签名，保证信息传输的机密性、真实性、完整性和不可否认性，从而保证信息的安全传输。

设备上的 PKI 本地证书功能是：当设备作为 PKI 客户端时，选择本地证书作为设备的身份标识，并且验证从其他主机接收到的证书的合法性。这相当于 IE 浏览器中的证书项功能。主要包含三项配置：导入用户证书、导入第三方 CA 证书、导入第三方 CA 的 CRL。这三个功能是相对独立又相互联系，即可以根据具体需要，导入不同的本地证书、不同的 CA 证书、不同的 CRL，但要验证某个终端证书时，需要导入该终端证书的 CA 证书、CRL，以便对该终端证书进行验证。

6.13.1. 本地证书

在系统菜单点击“**对象>证书>本地证书**”，进入**本地证书**页面，显示设备上已有的本地证书信息，在该页面可以实现对本地证书的导入、导出、查看和删除。

在**本地证书**页面点击<**导入**>，可以选择三种格式的证书上传。

PKCS12 格式证书上传。

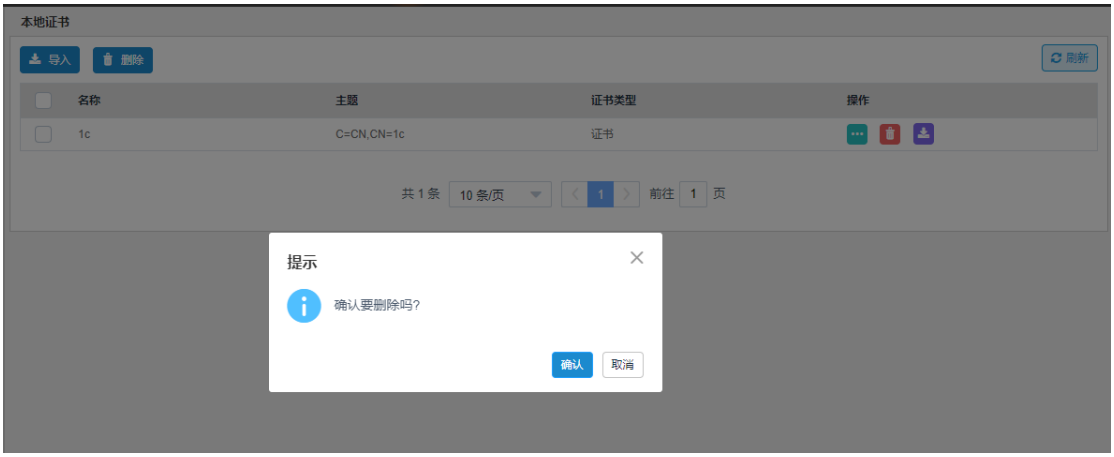
本地证书配置项及详细说明如下：

配置项	说明
类型	可选择上传证书的类型，包括 PKCS12 格式、证书密钥分离格式和证书链三种。
证书文件	数字证书文件位置。
密钥文件	数字证书密钥文件位置。
密码	数字证书的密码。

在**本地证书**页面点击，查看某一个证书的具体信息，显示证书详细信息。

在**本地证书**页面点击，可以导出证书。

在**本地证书**页面选中要删除的证书文件，点击<**删除**>或者点击证书后的，在弹出界面点击确定可以实现证书删除，如果证书前复选框为灰色或者不存在，表明证书正在被引用，无法删除。



6.13.2. 本地 CA 证书

在系统菜单点击“对象>证书>本地 CA 中心”进入本地 CA 中心页面，显示设备上已有的本地 CA 证书信息，在该页面可以实现对本地证书的导入、导出、查看和删除。

在本地 CA 中心页面点击<导入>，导入 CA 中心证书，可以选择两种上传 CA 证书的方式。

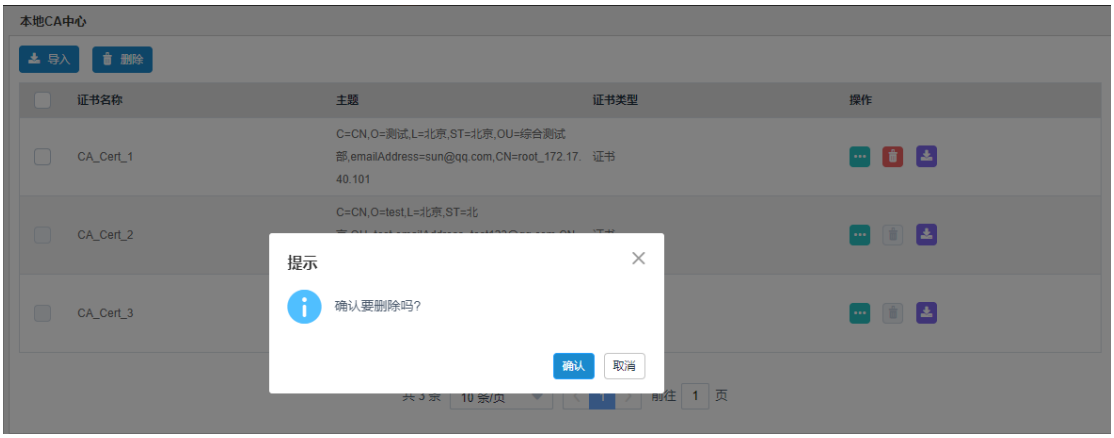
本地 CA 证书配置项及详细说明如下：

配置项	说明
目标位置	选择上传 CA 证书的类型，分别为证书和证书集合。
证书集合	要上传的 CA 证书集合文件位置。

在本地 CA 中心页面点击查看某一个证书的具体信息，显示证书详细信息。

在**本地 CA 中心**页面点击，可以导出证书。

在**本地 CA 中心**页面选中要删除的证书文件，点击<**删除**>或者点击证书后的，在弹出界面点击确定可以实现证书删除，如果证书前复选框为灰色或者不存在，表明证书正在被引用，无法删除。



6.13.3. 导入 CRL

CRL 是证书撤销列表（Certificate Revocation List）的缩写。由于密钥被泄露、 业务终止等原因， CA 可通过撤销证书立即终止证书的使用，在此情况下 CA 需要公布 CRL 来声明该证书是无效的， 并列出不能再使用的证书。

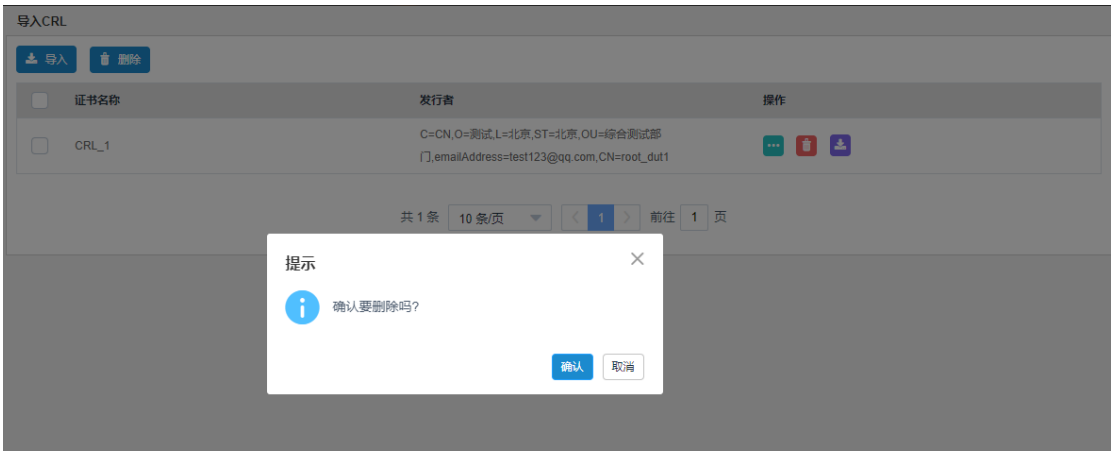
在系统菜单点击“**对象>证书>导入 CRL**”，进入**导入 CRL** 页面，显示设备上已有的 CRL 信息，在该页面可以实现对 CRL 的导入、导出、查看和删除。

在**导入 CRL** 页面点击<**导入**>，导入 CRL。

在**导入 CRL** 页面点击 查看某一个 CRL 证书的具体信息，显示证书详细信息。

在**导入 CRL** 页面点击，可以导出证书。

在**导入 CRL** 页面选中要删除的证书文件，点击<**删除**>或者点击证书后的，在弹出界面点击确定可以实现证书删除，如果证书前复选框为灰色或者不存在，表明证书正在被引用，无法删除。



6.14. CA 中心

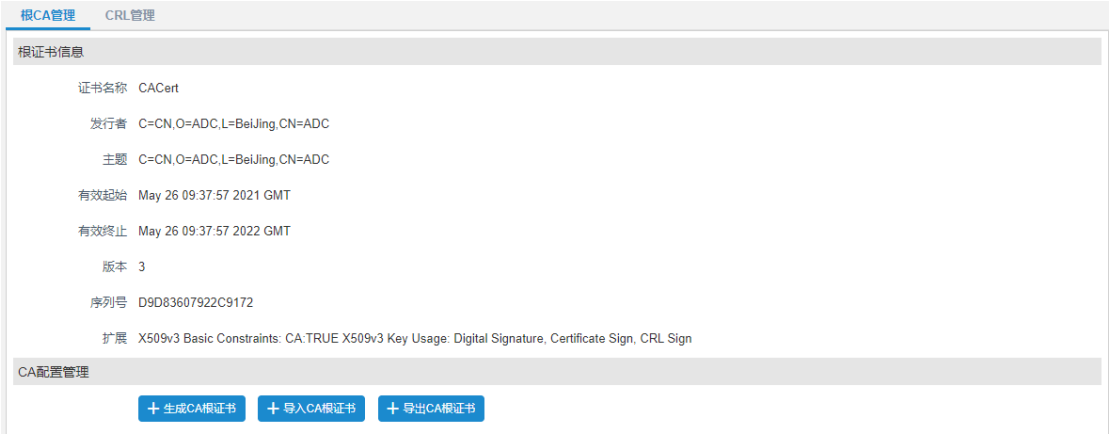
CA 中心又称 CA 机构，即证书授权中心(Certificate Authority)，或称证书授权机构，作为权威的、可信赖的、公正的第三方机构，专门负责发放并管理所有参与网上交易的实体所需的数字证书，承担公钥体系中公钥的合法性检验的责任。它作为一个权威机构，对密钥进行有效地管理，颁发证书证明密钥的有效性，并将公开密钥同某一个实体联系在一起。CA 中心为每个使用公开密钥的用户发放一个数字证书，数字证书的作用是证明证书中列出的用户

合法拥有证书中列出的公开密钥。CA 机构的数字签名使得攻击者不能伪造和篡改证书。

6.14.1. 根 CA 管理

6.14.1.1. 根 CA 管理

在系统菜单点击“**对象>CA 中心>根 CA 管理>根 CA 管理**”，进入**根 CA 管理**页签，可以查看根证书信息、生成 CA 根证书、导入 CA 根证书和导出 CA 根证书。



在**根 CA 管理**页签点击<**生成 CA 根证书**>，在弹出的窗口确认重新生成根 CA 证书，进入证书生成界面。

生成 CA 根证书配置项及详细说明如下：

配置项	说明
CN	证书 common name 信息
部门	证书部门信息。
组织	证书组织信息
位置（城市）	证书位置信息
州/省	证书所属的州或省。
国家/地区	证书国家/地区信息
电子邮件	证书电子邮件信息
有效期	设置证书有效期，范围 1 到 7300 天
密钥算法	设置密钥算法，可选 RSA-1024、RSA-2048 和 SM2-256。

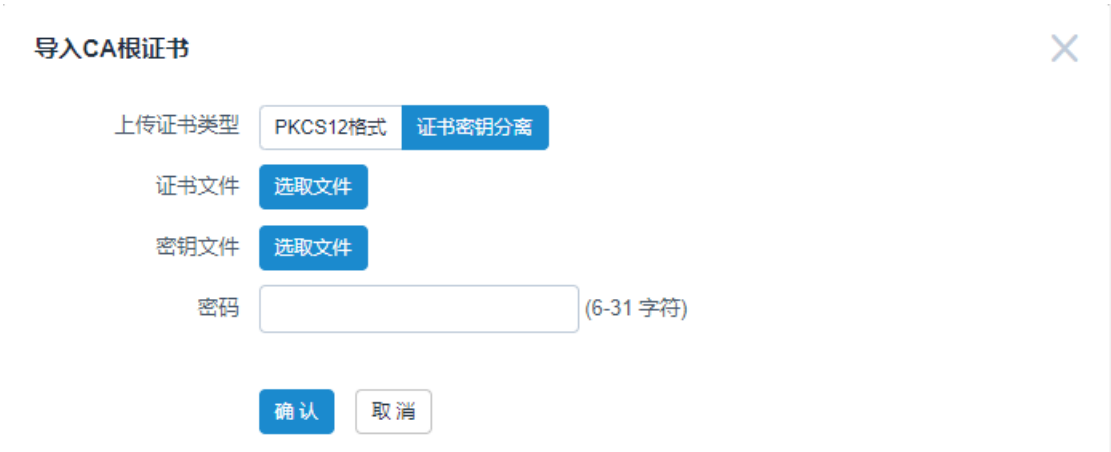
在**根 CA 管理**页签点击<**导入 CA 根证书**>，在弹出的窗口确认重新生成根 CA 证书，进入导入 CA 根证书界面，导入方式分为 PKCS12 格式和证书密钥分离格式两种。

导入 PKCS12 格式根 CA 证书的界面。

导入 PKCS12 格式 CA 根证书配置项及详细说明如下。

配置项	说明
上传证书类型	选择导入 CA 根证书的类型，可选择 PKCS12 格式和证书密钥分离格式两种。
有密钥文件的证书	点击选择证书文件存放的位置。
密码	配置证书文件的密码。

导入证书密钥分离格式 CA 根证书的界面。



导入证书密钥分离格式根 CA 证书配置项及详细说明如下。

配置项	说明
上传证书类型	选择导入 CA 根证书的类型，可选择 PKCS12 格式和证书密钥分离格式两种。

证书文件	点击选择证书文件存放的位置。
密钥文件	点击选择密钥文件存放的位置。
密码	配置密钥文件的密码。

在**根 CA 管理**页签点击<**导出 CA 根证书**>，进入**导出 CA 根证书**界面，可以选择导出为 PEM 格式和 P12 格式两种类型的 CA 证书。其中 PEM 格式证书不包含密钥文件。

PEM 格式证书导出。

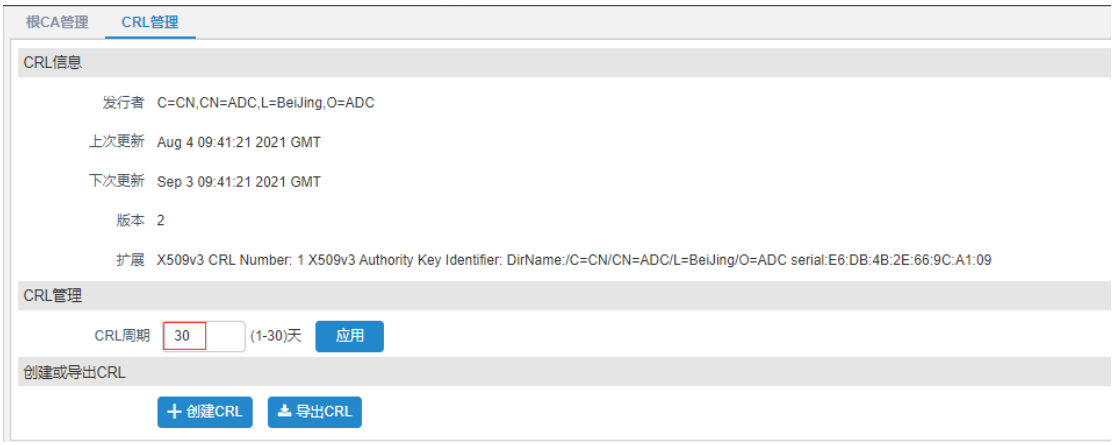
导出 CA 根证书配置项及详细说明如下：

配置项	说明
导出证书类型	选择导出证书的类型，可选择 PEM 格式和 P12 格式两种。
密码	设置导出后 P12 证书的密码，PEM 格式证书不包含密钥文件。

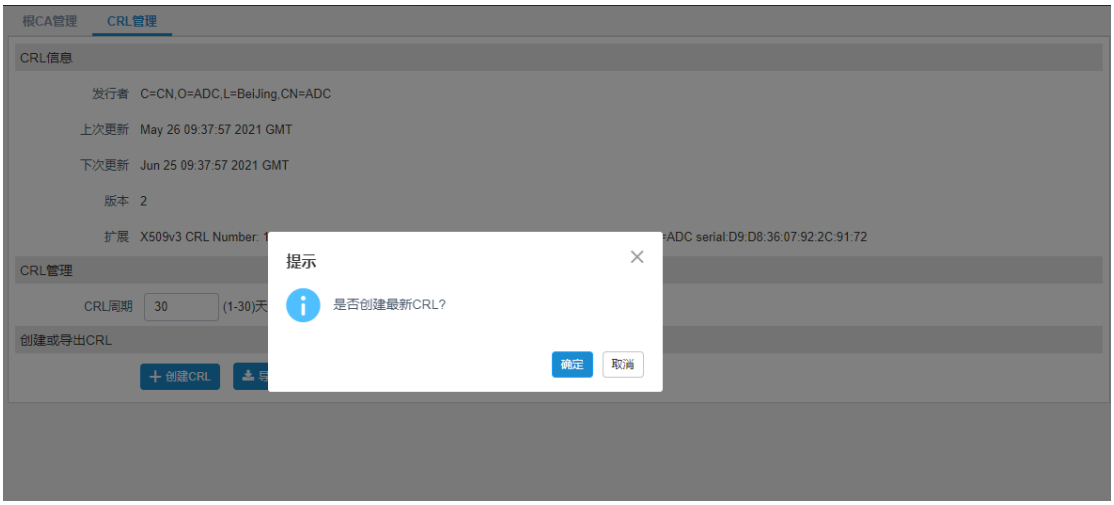
6.14.1.1. CRL 管理

在系统菜单点击“**对象>CA 中心>根 CA 管理>CRL 管理**”，进入 **CRL 管理**页签，可以查看 CRL 信息、配置 CRL 周期、创建和导出 CRL。

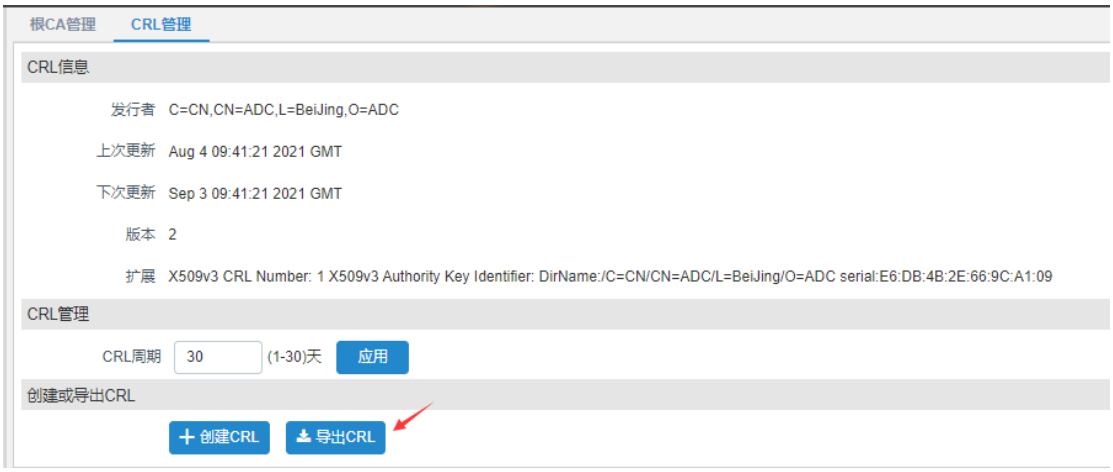
在 **CRL 管理**页签下“**CRL 管理**”中，可以对 CRL 自动更新周期进行配置，CRL 周期配置范围为 1-30 天。



在 **CRL 管理**页签下点击<**创建 CRL**>，在弹出的确认创建最新的 CRL。



在 CRL 管理页签点击<导出 CRL>，可以导出证书。



6.14.2. 用户证书管理

在系统菜单点击“对象>CA 中心>用户证书管理”，进入用户证书管理页面，可以查看用户证书列表，查看特定证书详细信息，进行用户证书的的创建、查看和签发。

在用户证书管理页面点击<新建>，进入证书请求配置页面。

证书请求配置项及详细说明如下：

配置项	说明
证书名称	配置证书的 CN 信息
部门	证书部门信息。
组织	证书组织信息
位置（城市）	证书位置信息
州/省	证书所属的州或省。
国家/地区	证书国家/地区信息
电子邮件	证书电子邮件信息
有效期	设置证书有效期，范围 1 到 7300 天
密钥算法	设置密钥算法，可选 RSA-1024、RSA-2048、SM2-256。

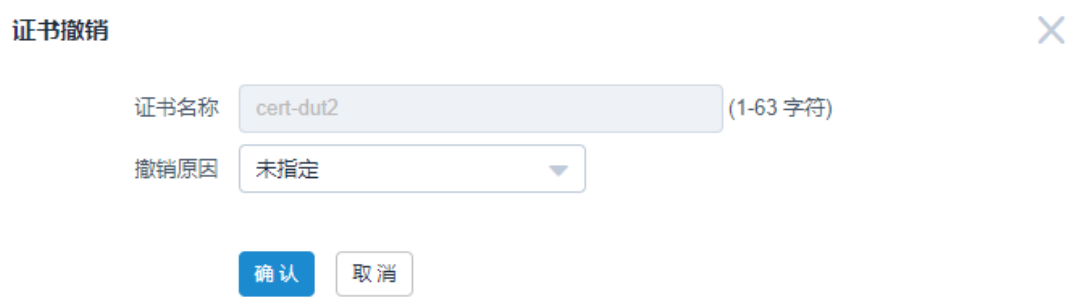
在**用户证书管理**页面选择系统状态为未签发的用户证书请求，点击图标对证书请求进行签发。

证书签发界面。

证书签发配置项及详细说明如下：

配置项	说明
证书名称	需要签发的证书名称。
有限期	设置证书有效期，范围 1-7300 天。
密码	设置证书密码。

在**用户证书管理**页面选择系统状态为正常的用户证书，点击图标，进入证书吊销界面对证书进行撤销。



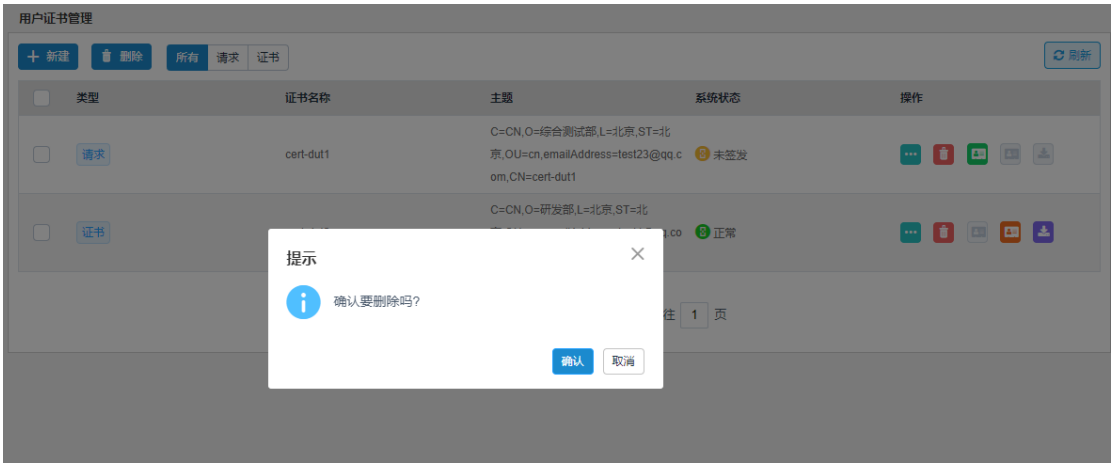
证书撤销配置项及详细说明如下：

配置项	说明
证书名称	需要撤销的证书名称。
撤销原因	配置证书的吊销原因，可选择未指定、密钥泄露、CA 密钥泄露和附属关系改变四种。

在用户证书管理页面选择证书点击，查看某一个证书的具体信息，显示证书详细信息。

在**用户证书管理**页面选择系统状态为正常的证书，点击图标可以导出证书。

在**用户证书管理**页面选中要删除的证书文件，点击<**删除**>或者点击证书后的，在弹出界面点击确定可以实现证书删除。



第七章 系统

7.1. 系统设置

7.1.1. 时间设置

时间设置中可配置当前设备使用的时区及当前时间，可通过手动方式或 NTP 同步方式进行配置。

在系统菜单点击“**系统>系统设置>时间设置**”，进入**时间设置**页面。

手动配置展示如下：

NTP 同步配置展示如下：

时间设置的配置项与详细说明如下：

配置项	说明
系统时间	展示当前系统时间，可刷新查看最新时间。
时区选择	下拉菜单，默认选择 GMT+8:00，可根据需要选择其它时区。
配置方式	支持手动配置及 NTP 同步 2 种方式。
手动配置	可手动选择日期及具体时间。
服务器	配置方式选择 NTP 时可进行展示，填写为 NTP 服务器地址，点击<立即同步>按钮进行直接同步。
同步间隔	定期与 NTP 进行同步，允许范围是 5-65535 分钟。
认证 id	与 NTP 服务器进行认证的 ID，允许范围是 1-1874919423。
认证 key（MD5）	与 NTP 服务器进行认证的 MD5 校验码，允许范围 1-31 字符。

7.1.2. DNS

配置设备自身访问域名所用 DNS，支持配置主备 DNS 服务器，支持检测域名。

在系统菜单点击“**系统>系统设置>DNS**”，进入 **DNS** 配置页面。

DNS 的配置项与详细说明如下：

配置项	说明
首选 dns 服务器	主 DNS 服务器地址。
备选 dns 服务器	备 DNS 服务器地址。
DNS 检测	
检测域名	可输入域名进行检测，检测结果在文本框下方进行展示。

7.1.3. 邮件服务器设置

为减轻设备自身的存储压力，用户可以配置 SMTP 服务器，将日志发送到指定的邮箱。

在系统菜单点击“**系统>系统设置>邮件服务器设置**”，进入**邮件服务器设置**配置页面。

告警邮件配置配置项及详细说明如下：

配置项	说明
服务器	
SMTP 服务器	邮箱服务器地址，如腾讯 SMTP 服务器：smtp.exmail.qq.com。

SMTP 服务器端口	邮箱服务器的端口，默认为 25。
安全连接	默认关闭，如果邮件服务器需要安全连接，则需要开启安全连接。
发件人 E-Mail	告警邮件中的发件人邮箱，必须是 SMTP 服务器的邮箱，且真实存在，可以正常发送邮件。
认证	默认关闭，开启认证开关，可以对 SMTP 用户和密码进行配置。
SMTP 用户	告警邮件的发件人邮箱。
密码	发件人邮箱的登录密码。
测试邮件地址	
测试邮件地址	告警邮件中的收件人邮箱，必须真实存在，可以正常接收邮件。点击<**测试**>按钮，测试邮件地址的收件人邮箱可以收到一封测试邮件。
日志告警	
最短发送间隔	默认 5 分钟，E-Mail 日志消息最短发送的间隔时间。
收件人 E-Mail	收件人邮箱地址，必须真实存在，可以正常接收邮件。多个邮箱地址用分号隔开。

提示：

在“系统-日志设定-日志过滤”中，必须勾选 E-mail 报警。

7.2. 管理员设置

用户可通过管理员设置对登陆设备的管理员进行管理，包括新建删除管理员，查看在线管理员或被阻断用户，生成密钥或二维码等。

7.2.1. 管理员

下一代防火墙支持使用本地用户数据库，支持使用 RADIUS 服务器、LDAP 服务器的用户认证。

选择 RADIUS 认证，用户名和密码与 RADIUS 服务器中的用户名和密码相匹配，则认证通过。

选择 LDAP 认证，用户名和密码与 LDAP 服务器中的用户名和密码相匹配，则认证通过。

未开启三权模式时，使用 admin 账号登陆设备，在系统菜单点击“**系统>管理员设置>管理员**”进入管理员配置页面，开启三权后，使用 useradmin 账号登陆设备，在系统菜单点击“**系统>管理员设置>管理员**”进入管理员配置页面。

用户可对管理员账号进行新建、删除、编辑操作，默认管理员不支持删除。

新建及编辑管理员：点击<**新建**>按钮，弹出框中依照要求输入管理员信息，完成后保存，即创建管理员成功。选中需要修改信息的管理员，点击右侧按钮，可以修改管理员信息。

管理员新建编辑的配置项与详细说明如下：

配置项	说明
名称	用户自定义信息，新建的管理员名称，新建后不可编辑。
描述	用户自定义信息，用于对当前管理员进行说明。
类型	支持密码、RADIUS、LDAP 三种类型管理员。 ● 密码-选择密码表示对于创建的用户，其用户名和密码都保存在本地，然后在密码和确认密码中输入用户自定义的本地用户密码。 ● RADIUS-选择 RADIUS 表示对于创建的用户，本地仅保存用户名，不保存密码，用户需要到指定的 RADIUS 服务器进行认证，该用户需要在 RADIUS 服务器上存在。下拉列表中列出了当前可选的 RADIUS 服务器。 ● LDAP-选择 LDAP 表示对于创建的用户，本地仅保存用户名，不保存密码，用户需要到指定的 LDAP 服务器上进行认证，该用户需要在 LDAP 服务器上存在。下拉列表中列出了当前可选的 LDAP 服务器。
密码	类型选择密码时可输入，用户自定义密码，长度为 6-31 位字符。
确认密码	需要与密码框中所填信息保持一致。
密码周期设置	时间到达填写的周期后，再次登陆时会提示变更密码；全部输入 0 表示密码永不过期。
类型	地址类型，包括 IPv4 及 IPv6 两种。
IP 地址	允许使用该管理员账号登录的 IP，IPv4 地址格式，例如：A.B.C.D/M。IPv6 地址格式，例如：2000::1/64。
Mac 地址	此 IP 对应的 MAC 地址可使用该管理员账号登录，否则不允许使用该管理员账号登录。
接口	使用该管理员账号登录后的流量入口。
添加	按钮，将所输入的 IP 地址，Mac 地址及接口添加到下方表中，表格最多添加 16 条。
开启三权后特殊配置	
权限	开启三权后，管理员按照权限分为配置管理员（admin）、用户管理

	员（useradmin）、审计员（audit）三种。使用默认 useradmin 登陆，可以对管理员进行新建、删除、修改操作，可以根据具体需求，变更管理员读写权限。

7.2.2. 在线管理员

在线管理员中可查看到管理员的登录信息，可以强制管理员下线，也可查看当前被阻断的管理员信息。

7.2.2.1. 在线管理员

在系统菜单点击“**系统>管理员设置>在线管理员>在线管理员**”，进入**在线管理员**配置页签。

选择需要操作的管理员账号，点击按钮，可以将当前用户强制下线。

7.2.2.2. 阻断用户

在系统菜单点击“**系统>管理员设置>在线管理员>阻断用户**”，进入**阻断用户**配置页签。

切换页签到**阻断用户**可以查看当前被阻断的全部用户信息，可将不需要阻断的用户在此目录中删除，点击即可完成操作。

7.2.3. 管理员密钥

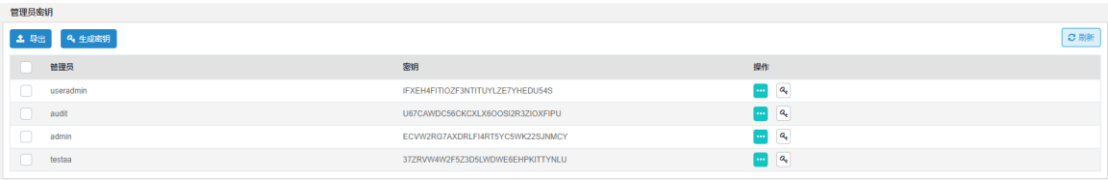
管理员密钥用于管理员辅助认证中动态口令认证，动态口令生成器通过管理员密钥，生成动态口令，用户通过 Web 端登陆设备时，需同时输入正确的账号密码及动态口令才可登陆成功。支持生成管理员密钥及管理员密钥导出功能。

在系统菜单点击“**系统>管理员设置>管理员密钥**”，进入**管理员密钥**配置页面。

支持单个管理员生成密钥及批量生成多个管理员密钥，通过点击按钮可生成单个管理员密钥；通过多选框勾选多个管理员，点击<**生成密钥**>按钮，可批量生成多个管理员密钥。

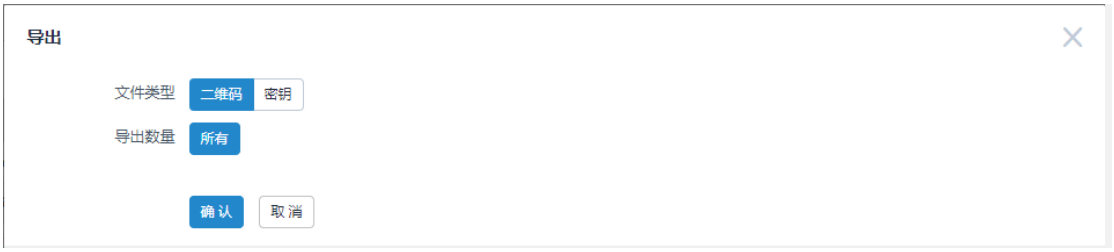
密钥生成后，通过点击按钮，查看二维码。

密钥生成展示如下：



二维码展示如下：

导出密钥：导出功能只支持导出所有已生成密钥的管理员的密钥。点击<**导出**>按钮，弹出框中选择导出的文件类型，点击<**确认**>按钮即可导出完成。



7.2.4. 系统管理设定

系统管理设定中包括配置 Web 端管理（HTTP 和 HTTPS）方式，主机名称，实时保存配置，管理员唯一性检查、登录图形验证码、三权分立模式、页面超时时间、WEB 在线管理员（数量）、管理员最大登录次数、管理员登录失败阻断间隔，及管理员辅助认证的功能。

7.2.4.1. 系统管理设定

在系统菜单点击“**系统>管理员设置>系统管理员设定>系统管理设定**”，进入**系统管理设定**配置页签。

配置项	说明
本地 HTTP 服务管理默认端口	开关按钮，默认状态为开，开启时采用默认的 80 端口进行 HTTP 访问。
本地 HTTP 服务管理端口	当默认端口配置为关时可进行更改，默认信息是 80，自定义时允许范围是 1024-65535。
本地 HTTPS 服务管理默认端口	开关按钮，默认状态为开，开启时采用默认的 443 端口进行 HTTPS 访问。
本地 HTTPS 服务管理端口	当默认端口配置为关时可进行更改，默认信息是 443，自定义时允许范围是 1024-65535。
主机名称	设备名称，默认为 host，可根据需要进行编辑。
实时保存配置	默认为开，打开后可实时保存页面操作。
管理员唯一性检查	开关按钮，默认关闭，开启后只能同时存在一个页面使用管理员账号登陆。
管理员登陆图形验证码	开关按钮，默认开启，开启时 Web 端登陆设备需输入验证

	码。
三权分立模式	开关按钮，默认关闭，开启后需重新登陆，且开启后支持 useradmin 账号及 audit 账号登陆，三种账号拥有不同权限。 ● admin-拥有系统配置，统计信息，日志管理，升级及重启权限。 ● useradmin-拥有管理员配置权限。 ● audit-拥有操作日志审计权限。
页面超时时间	在 Web 无操作的情况下，超过设置的时间，登录用户会自动退出。缺省为 10 分钟，允许范围是 5-480 分钟。
WEB 在线管理员	最多可以同时 Web 登录的管理员个数，默认 10，允许范围是 1-20 个。
管理员最大登录重试次数	管理员可连续登陆失败次数，默认为 5 次，允许范围是 1-60 次。
管理员登陆失败阻断间隔	管理员连续登陆失败超出允许的最大次数后，多久时间内不允许再次登陆，默认为 60 秒，允许范围是 1-3600 秒。

7.2.4.2. 管理员辅助认证

在系统菜单点击“**系统>管理员设置>系统管理员设定>管理员辅助认证**”，进入**管理员辅助认证**配置页签，可查看辅助认证相关配置信息。

系统设置的配置项与详细说明如下：

配置项	说明
动态口令认证	开关按钮，默认关闭，需存在动态口令配置时进行开启，开启后管理员通过页面登陆设备，需输入动态口令。
证书认证	开关按钮，默认关闭，开启后管理员登陆需要进行证书认证，通过后方可登陆成功。

7.3. 高可靠性

高可靠性即 HA（High-Availability），是保证网络高可靠的一种技术方案，防火墙支持两台设备以主-备或主-主两种工作模式运行，满足不同的组网需要。

在主-备工作模式下，只有状态为“主”的设备转发流量，所有流量都被主设备转发，“备”设备不工作，但保持和“主”同样的配置，同时实时监测“主”设备的运行状态，一旦检测到“主”设备出现故障，比如掉电，设备死机等。“备”设备会自动接管“主”设备承担网络流量的转发工作，以保持网络的连通。

在主-主工作模式下，两台设备同时转发流量，流量的分配比例取决于相邻网络设备的路由配置，以及设备上的相关配置，如浮动 IP 等。

两台设备通过用户设置 IP 地址发送心跳报文来检测对端设备的工作状态，同时下一代防火墙产品支持另外三个附加因素可选项：“故障监控”，“链路聚合监控”和“健康检查监控”作为切换条件。正在工作中的主设备如果检测到自己的监控状态比对端的优先级低，则会主动使自己变为“备”状态，所有流量被对端设备接管。在主备工作模式下，可以通过配置的强制模式来决定设备的主备关系。

本章涉及 HA 功能的配置，阐述了如何通过 Web 管理界面配置 HA，实现 HA 功能。

7.3.1. HA 配置

在系统菜单选择“**系统>高可靠性>HA 配置**”，进入 **HA 配置**页面。

HA 配置项及详细说明如下：

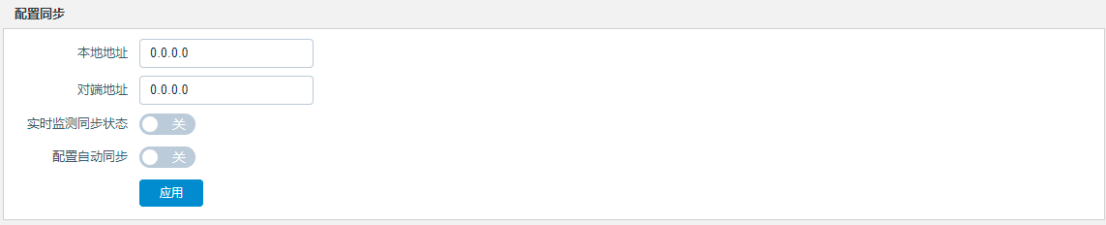
配置项	说明
工作模式	高可靠性的工作模式分主备模式和主主模式，选择禁用为关闭高可靠性功能。
首选通信地址	HA 心跳通信地址，用于发送和接收心跳报文。本地地址必须指定为设备本地的接口地址，推荐使用非业务口地址。
备选通信地址	HA 心跳备用通信地址。指定备选通信地址后，当主选地址故障后，备用地址自动发送 HA 心跳报文。
单元 ID	工作模式选择主主模式时，设备需要设置对应的单元 ID，这是代表设备工作的实例，和设备配置的浮动 IP 的单元 ID 对应，要求参与主主模式的两台设备分别设置 1 和 2，不能设置相同 ID，设置相同会出现 IP 地址冲突。
抢占模式	工作模式选择主备模式时，可以通过抢占模式调整设备的优先级，配置抢占主后，优先级高于对端，主备状态为主。
心跳发送间隔	高可靠性设备之间心跳报文发送间隔，最短 1 秒，最长 3 秒，连续三次没有收到心跳报文，设备按照对端设备异常处理。

7.3.2. 配置同步

HA 功能可实现配置的手动/自动同步，手动同步为当配置完一台设备后，用户可以把本设备上的配置同步到另一台设备上，重启对端设备后生效。自动同步为通过 Web 在主设备上进行配置，非接口相关的配置，能自动同步到备机。既减少了用户配置的工作量，又保证

了两台设备配置相同，出现切换时能保证用户数据传输不中断。

在系统菜单选择“**系统>高可靠性>配置同步**”，进入**配置同步**配置页面。



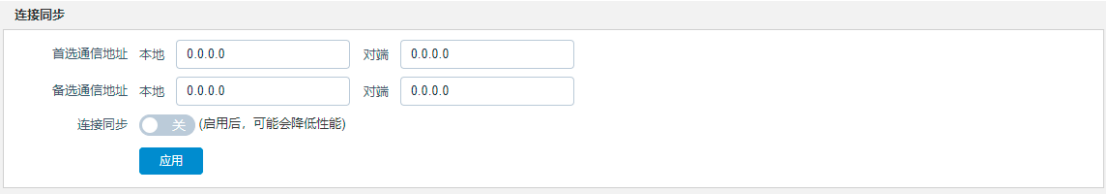
HA 配置同步配置项及详细说明如下：

配置项	说明
本地地址	当前设备连接对端设备的本地接口 IP 地址。
对端地址	当前设备可连接对端设备的对端接口 IP 地址。
实时监测同步状态	开启后每一分钟检查一次配置同步。
配置自动同步	通过 Web 对主设备进行配置时，对端设备能同时更新相关配置。（配置同步的接口需要开启允许 HTTP 流量通过）。

7.3.3. 连接同步

连接同步包括四层流同步，七层会话保持同步，为了保证故障切换时，已经建立的连接不中断，就必须进行连接同步。

在系统菜单选择“**系统>高可靠性>连接同步**”，进入**连接同步**配置页面。



HA 连接同步配置项及详细说明如下：

配置项	说明
首选通信地址	当前设备连接对端时首选通信地址对。
备选通信地址	当前设备连接对端时备选通信地址对。当首选地址不可达时启用。
连接同步	连接同步功能的开启和关闭。

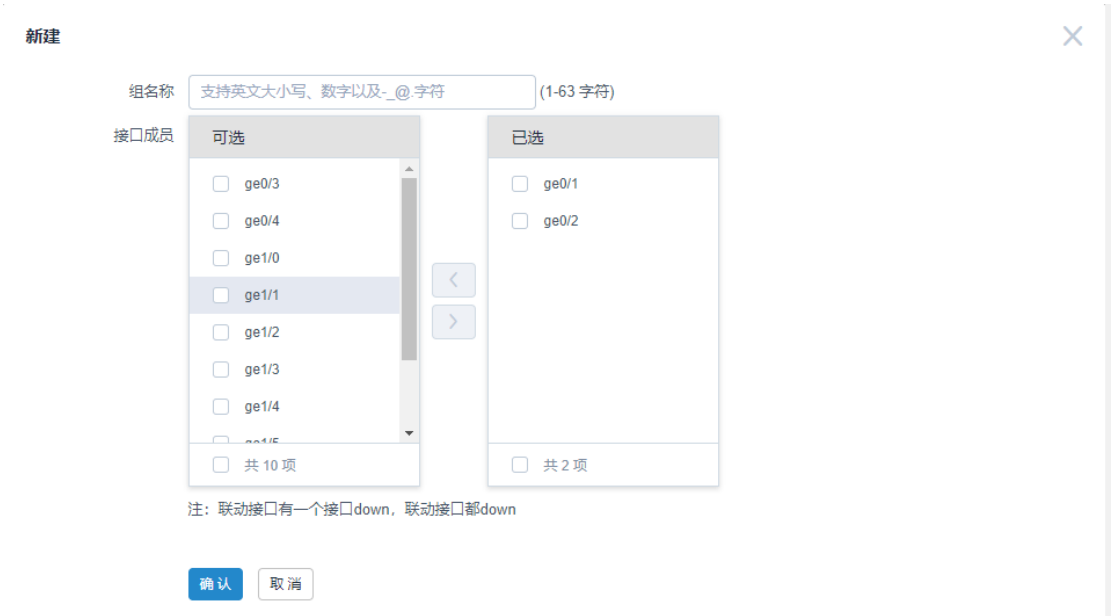
7.3.4. 接口联动

在接口联动组内一个接口 DOWN 掉，组内其他接口都会自动 DOWN。

在系统菜单选择“**系统>高可靠性>接口联动**”，进入**接口联动**配置页面。

接口联动配置完成后，状态栏图标表示接口当前状态为 DOWN，图标表示接口当前状态为 UP，图标为修改配置，图标表示删除该配置项。

在**接口联动**页签下点击<**新建**>创建接口联动配置，或者在右侧“**操作**”列下点击图标修改已有的接口联动配置。



接口联动配置项及详细说明如下：

配置项	说明
组名称	接口联动组名称，只能是英文、数字和字符组合。
接口成员	选择该接口联动组的接口，成员只能是物理接口。

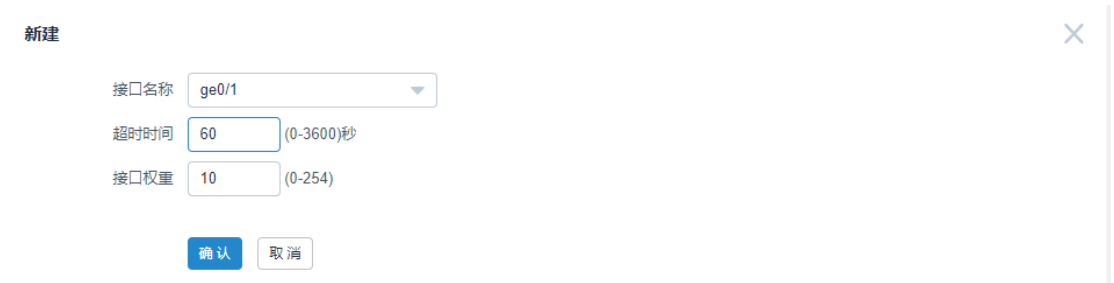
7.3.5. 故障监控

HA 故障检测分接口监控、链路聚合监控和健康检查监控，实时监控设备上的运行状况，当出现监控故障时，触发主备状态切换，保证业务正常转发。

7.3.5.1. 接口监控

在系统菜单选择“**系统>高可靠性>故障监控>接口监控**”，进入**接口监控**配置页签。

在**接口监控**页签下点击<**新建**>创建接口监控配置，或者在右侧“**操作**”列下点击图标修改已有的接口监控配置。



接口监控配置项及详细说明如下：

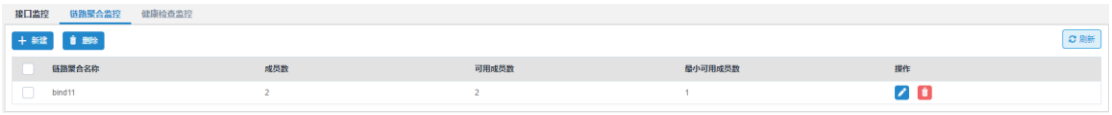
配置项	说明
接口名称	需要监控的物理接口或 VLAN 名称，可以监控用户认为重要的所有 VLAN 和除了管理口之外的物理接口，监控基于物理接口或 VLAN 的 UP/DOWN。建议监控设备上下游直连的接口，这些接口的故障会造成业

	务的中断，必须进行故障切换。
超时时间	监控故障后，等待的超时时间，避免接口短时间内多次 UP/DOWN，引起 HA 状态频繁切换，造成设备不稳定。
接口权重	当接口出现故障时，会从设备的总权重中减去 DOWN 掉接口的权重值，最终权重总值多的为主。

7.3.5.2. 链路聚合监控

链路聚合监控对聚合接口的监控，保证聚合接口能够满足最低使用要求，当聚合口中接口低于最低限制时，报故障，并做 HA 的切换。

在系统菜单选择“**系统>高可靠性>故障监控>链路聚合监控**”，进入**链路聚合监控**配置页签。



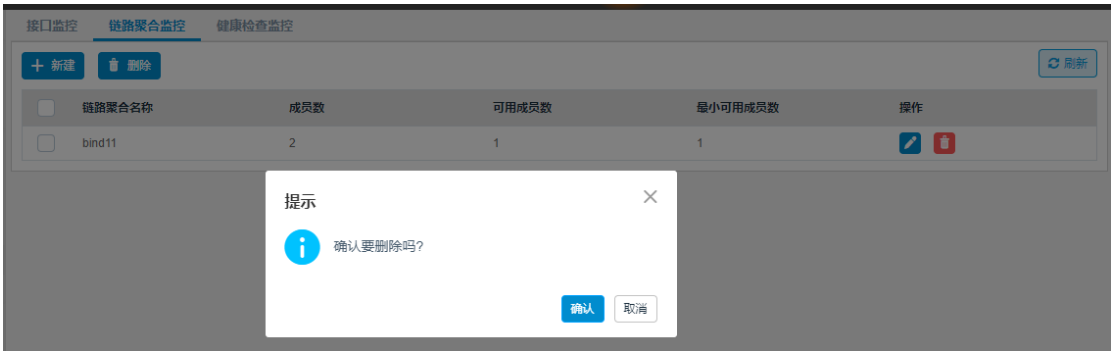
在**链路聚合监控**页签下点击<**新建**>创建链路聚合监控配置，或者在右侧“**操作**”列下点击图标修改已有的链路聚合监控配置。聚合口的配置参考聚合接口配置。

链路聚合监控配置项及详细说明如下：

配置项	说明
链路聚合名称	需要监控的聚合口名称。
最小可用成员数	UP 的成员口个数，当聚合口检测到最小带宽小于设置的成员口个数

	时，聚合口不可用并上报接口故障。

点击图标表示删除，删除配置的聚合口。



7.3.5.3. 健康检查监控

健康检查监控对关键线路的健康状态进行监控，保证关键线路可用，当检测到关键线路（例如 DNS 服务器）异常时，报故障，并做 HA 的切换。

在系统菜单选择“**系统>高可靠性>故障监控>健康检查监控**”，进入**健康检查监控**配置页签。

健康检查监控配置项及详细说明如下：

配置项	说明
健康检查模板	健康检查或健康检查组的名称，通过监控关键线路的健康状态，及时进行 HA 切换，保障业务正常转发，健康检查的配置参考健康检查配置。

7.3.6. HA 监控

7.3.6.1. HA 监控

在系统菜单选择“**系统>高可靠性>HA 监控>HA 监控**”，进入 **HA 监控**配置页签。

HA 监控项及详细说明如下：

监控项	说明
设备名称	主备防火墙设备的名称。
设备状态	根据 HA 监控页面查看当前 HA 的状态，以及是否有异常。
故障统计	接口监控、链路聚合监控、健康检查监控到的异常个数。
接口权重	监控到的所有 UP 接口的权重总和，在故障数都为 0 的情况下，根据接口权重来做主备选择。
系统配置	检查主备防火墙设备配置是否同步，同步显示“相同”，不同步显示“不同”。
软件版本	检查主备防火墙设备软件版本是否相同，相同显示“相同”，不同显示“不同”。

7.3.6.2. 接口监控

在系统菜单选择“**系统>高可靠性>HA 监控>接口监控**”，进入**接口监控**配置页签。

接口监控项及详细说明如下：

监控项	说明
接口名称	监控的接口名称。
超时时间	根据 HA 监控页面查看当前 HA 的状态，以及是否有异常。
接口权重	监控到的 UP 接口的权重数。
监控状态	监控到的接口状态， 表示正常， 表示故障。

7.3.6.3. 链路聚合监控

在系统菜单选择“**系统>高可靠性>HA 监控>链路聚合监控**”，进入**链路聚合监控**配置页签。

链路聚合监控项及详细说明如下：

监控项	说明
链路聚合名称	聚合接口名称。
成员数	聚合接口所包含物理口个数。
最小可用成员数	**故障监控>链路聚合监控**页配置的最小可用成员数。
活动成员数	接口状态为 UP 的物理接口个数。
监控状态	监控到的接口状态， 表示正常， 表示故障。

7.3.6.4. 健康检查监控

在系统菜单选择“**系统>高可靠性>HA 监控>健康检查监控**”，进入**健康检查监控**配置页签。

健康检查监控项及详细说明如下：

监控项	说明
健康检查模板名称	**健康检查**或**健康检查组**页面配置的健康检查名称。
监控状态	监控到的接口状态，表示正常，表示故障。

7.3.6.5. 监控配置

在系统菜单选择“**系统>高可靠性>HA 监控>监控配置**”，进入**监控配置**页签。

健康检查监控项及详细说明如下：

监控项	说明
同步配置到对端	当监控到主备设备配置未同步时，点击**同步配置到对端**按钮可以进行主备设备配置同步。
主备切换	点击**主备切换**按钮，立即进行主备切换。
检测配置	点击**检测配置**按钮，立即进行配置检测

7.4. VRRP

VRRP（Virtual Router Redundancy Protocol，虚拟路由器冗余协议）将可以承担网关功能的路由器加入到备份组中，形成一台虚拟路由器，由 VRRP 的选举机制决定哪台路由器承担转发任务，局域网内的主机只需将虚拟路由器配置为缺省网关。

VRRP 是一种容错协议，在提高可靠性的同时，简化了主机的配置。在具有多播或广播能力的局域网（如以太网）中，借助 VRRP 能在某台设备出现故障时仍然提供高可靠的缺省链路，有效避免单一链路发生故障后网络中断的问题，而无需修改动态路由协议、路由发现协议等配置信息。

VRRP 备份组：

VRRP 将局域网内的一组路由器划分在一起，称为一个备份组。备份组由一个 Master 路由器和多个 Backup 路由器组成，功能上相当于一台虚拟路由器。

虚拟 IP：

虚拟路由器具有 IP 地址。局域网内的主机仅需要知道这个虚拟路由器的 IP 地址，并将其设置为缺省路由的下一跳地址，网络内的主机通过这个虚拟路由器与外部网络进行通信。

备份组中路由器的优先级：

VRRP 根据优先级来确定备份组中每台路由器的角色（Master 路由器或 Backup 路由器）。优先级越高，则越有可能成为 Master 路由器。

备份组中路由器的工作方式：

备份组中的路由器具有以下两种工作方式：

非抢占方式：如果备份组中的路由器工作在非抢占方式下，则只要 Master 路由器没有出现故障，Backup 路由器即使随后被配置了更高的优先级也不会成为 Master 路由器。

抢占方式：如果备份组中的路由器工作在抢占方式下，它一旦发现自己的优先级比当前的 Master 路由器的优先级高，就会对外发送 VRRP 通告报文。导致备份组内路由器重新选举

Master 路由器，并最终取代原有的 Master 路由器。相应地，原来的 Master 路由器将会变成 Backup 路由器。

备份组中路由器的认证方式：

VRRP 提供了两种认证方式：

Text：简单字符认证。在一个有可能受到安全威胁的网络中，可以将认证方式设置为 Text。发送 VRRP 报文的路由器将认证字填入到 VRRP 报文中，而收到 VRRP 报文的路由器会将收到的 VRRP 报文中的认证字和本地配置的认证字进行比较。如果认证字相同，则认为接收到的报文是真实、合法的 VRRP 报文；否则认为接收到的报文是一个非法报文。

MD5：MD5 认证。在一个非常不安全的网络中，可以将认证方式设置为 MD5。发送 VRRP 报文的路由器利用认证字和 MD5 算法对 VRRP 报文进行加密，加密后的报文保存在 Authentication Header（认证头）中。收到 VRRP 报文的路由器会利用认证字解密报文，检查该报文的合法性。

在一个安全的网络中，用户也可以不设置认证方式。

VRRP 定时器：

VRRP 通告报文时间间隔定时器：

用户可以通过设置 VRRP 定时器来调整 Master 路由器发送 VRRP 通告报文的时间间隔。如果 Backup 路由器在等待了 3 个间隔时间后，依然没有收到 VRRP 通告报文，则认为自己是 Master 路由器，并对外发送 VRRP 通告报文，重新进行 Master 路由器的选举。

VRRP 抢占延迟时间定时器：

在性能不够稳定的网络中，Backup 路由器可能因为网络堵塞而无法正常收到 Master 路由器的报文，导致备份组内的成员频繁的进行主备状态转换。用户可以通过设置 VRRP 抢占延迟时间的方法来解决这个问题。

设置了 VRRP 抢占延迟时间后，Backup 路由器会在等待了 3 倍的通告报文时间间隔后，再等待 VRRP 抢占延迟时间。如在此期间还是没有收到 VRRP 通告报文，则此 Backup 路由器将认为自己是 Master 路由器，对外发送 VRRP 通告报文，触发备份组内路由器进行 Master 路

由器的选举。

VRRP 报文格式：

支持 VRRPv2 和 VRRPv3 两种格式的报文。

注意：

虚拟路由器的 IP 地址可以是备份组所在网段中未被分配的 IP 地址，也可以和备份组内的某个路由器的接口 IP 地址相同。

接口 IP 地址与虚拟 IP 地址相同的路由器被称为“IP 地址拥有者”，优先级被强制为 255（最高优先级）。

在同一个 VRRP 备份组中，只允许配置一个 IP 地址拥有者。

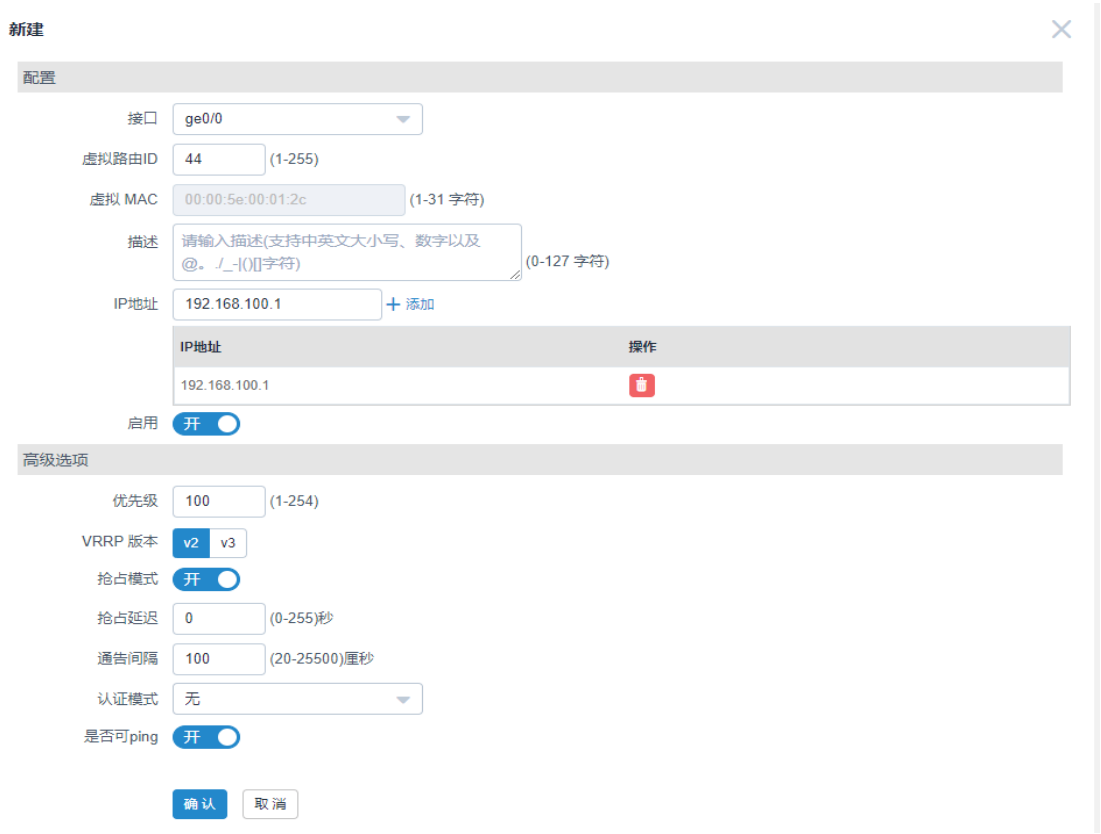
如果接口连接多个子网，则可以为一个备份组配置多个虚拟 IP 地址，以便实现不同子网中路由器的备份。

虚拟 IP 地址不能为全零地址(0.0.0.0)、广播地址(255.255.255.255)、环回地址、非 A/B/C 类地址和其它非法 IP 地址(如 0.0.0.1)。

只有配置的虚拟 IP 地址和接口 IP 地址在同一网段，且为合法的主机地址时，备份组才能够正常工作；否则，如果配置的虚拟 IP 地址和接口 IP 地址不在同一网段，或为接口 IP 地址所在网段的网络地址或网络广播地址，虽然可以配置成功，但是备份组不会生效。

在系统菜单选择“**系统>VRRP**”，进入 VRRP 配置页面。

在 VRRP 页签下点击<**新建**>创建 VRRP 配置，或者在右侧“**操作**”列下点击图标修改已有的 VRRP 配置。



VRRP 配置项及详细说明如下：

配置项	说明
接口	除 mgt 口外的所有接口。
虚拟路由 ID	设置 VRRP 备份组的组号，取值范围 1~255。 在一个接口下，VRID 必须唯一，不能重复；但在不同接口下，可以重复使用。
虚拟 MAC	配置虚拟路由 ID 之后自动生成。
描述	用于管理目的的说明性信息。
IP 地址	备份组的虚拟 IP 地址，点击<**添加**>添加配置的 IP 地址。
启用	是否开启 VRRP 功能。
优先级	VRRP 优先级的取值范围为 1 到 254（数值越大表明优先级越高，优先级高者当选为 Master）。
VRRP 版本	使用 VRRPv2 或 VRRPv3 格式的报文。

抢占模式	是否开启抢占。
抢占延迟	在使能抢占模式的前提下，抢占延迟的可选范围为 0~255 秒。
通告间隔	可选范围为 20~25500 厘秒（1 厘秒=1/100 秒）。
认证模式	在 VRRPv2 版本下，有“无”（不认证），“Text”（简单字符认证）与“MD5”（MD5 认证）三种选择；在 VRRPv3 版本下，没有认证选项。
是否可 ping	按照 VRRP 协议的规定，如果虚拟 IP 与接口上任何真实 IP 都不相同，那么虚拟 IP 是无法 Ping 通的。但很多用户都有 Ping 网关的习惯，所以如果想让虚拟 IP 可以被 Ping，就使能这个选项。

注意：

有时候备份组即使被启用了，但仍然无法工作，因为备份组进入工作状态的前提条件是：

接口处于 UP 状态

接口网线上能检测到载波信号

接口上至少配置了一个真实 IP 地址

备份组至少配置了一个虚拟 IP 地址，当配置的虚拟 IP 地址和接口地址相同时，优先级始终为 255，无需用户配置；IP 地址拥有者始终工作在抢占方式。

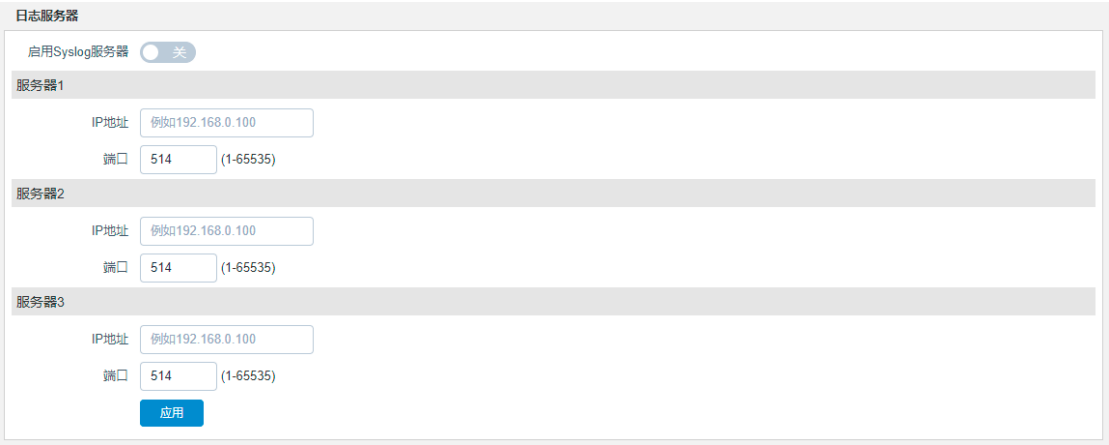
以上条件如果任何一个没有被满足，该备份组都无法进入工作状态。

7.5. 日志设定

7.5.1. 日志服务器

为减轻设备自身的存储压力，用户可以配置日志服务器，将日志发送到指定的 Syslog 服务器。

在系统菜单点击“**系统>日志设定>日志服务器**”，进入**日志服务器**配置页面，配置 Syslog 服务器的 IP 地址和服务端口。



日志服务器配置项及详细信息如下：

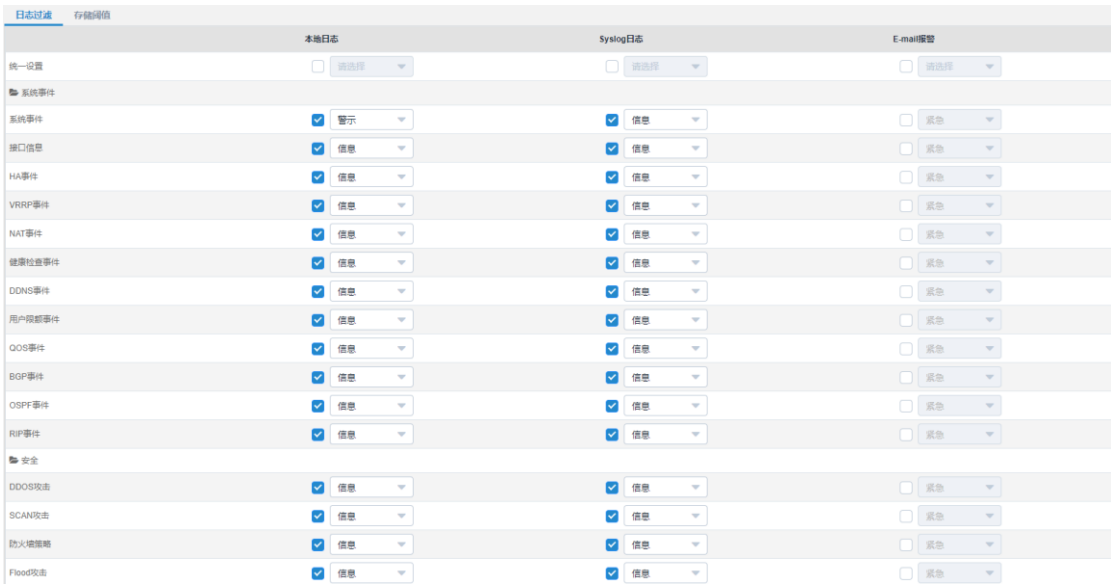
配置项	说明
启用 Syslog 服务器	选中表示启用，不选表示关闭。
IP 地址	Syslog 服务器地址。
端口	Syslog 服务器端口。
服务器 1、服务器 2、服务器 3	表示可以同时将日志发送到 3 个不同的 Syslog 服务器。

7.5.2. 日志过滤

系统日志是一种记录设备运行状况的方式。本设备支持标准的 Syslog 格式、本地日志、以及 E-mail 日志，提供给用户掌握系统运行状况的方法。

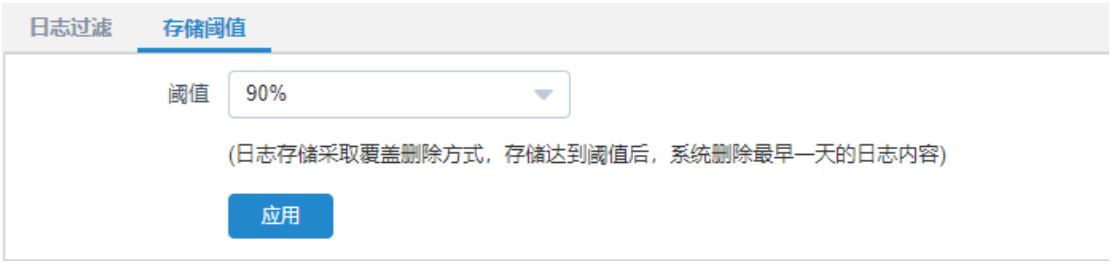
7.5.2.1. 日志过滤

在系统菜单点击“**系统>日志设定>日志过滤>日志过滤**”，进入**日志过滤**配置页签，对系统事件及其对应的本地日志级别、Syslog 日志级别、E-mail 报警级别进行设置。



7.5.2.2. 存储阈值

在系统菜单点击“**系统>日志设定>日志过滤>存储阈值**”，进入**存储阈值**配置页签，设置系统日志自动删除的阈值。



7.5.3. 流日志策略

在系统菜单点击“**系统>日志设定>流日志策略**”，进入**流日志策略**配置页面，查看已有的流日志策略。

在流日志策略页面，点击<**新建**>按钮创建新的的流日志策略，或点击操作列的编辑按钮，修改已有的流日志策略。

流日志策略配置项及详细说明如下：

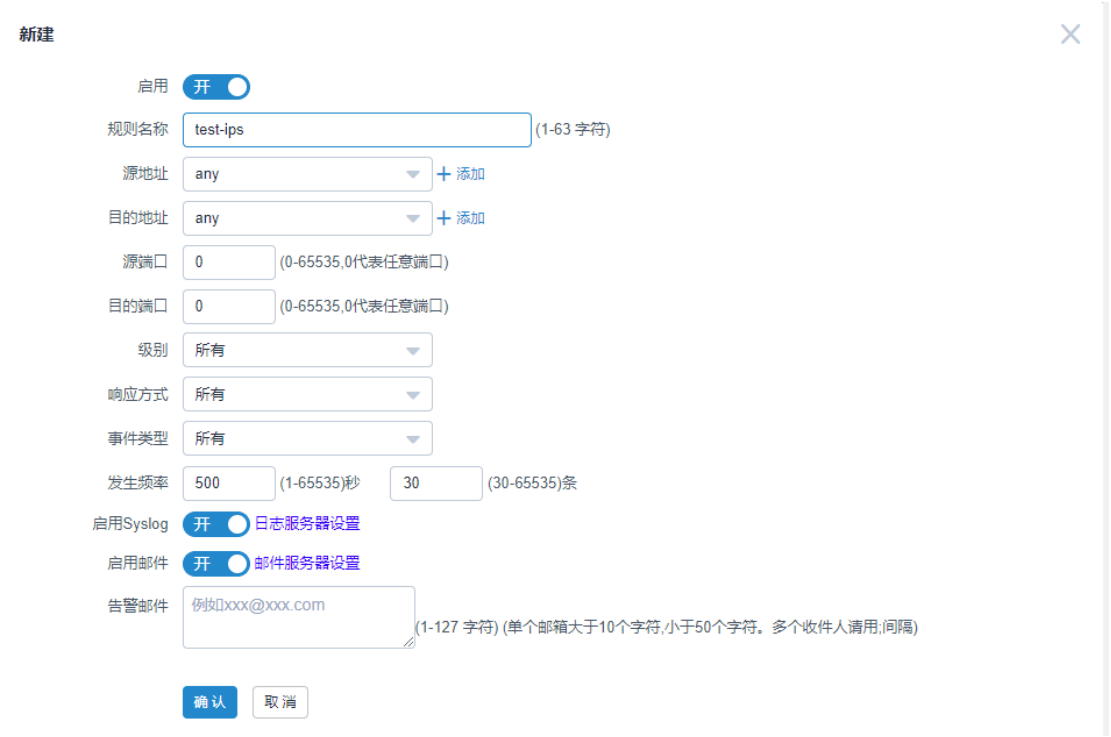
配置项	说明
启用	默认开启，关闭启用开关，策略禁用。
源地址	需要命中策略产生流日志的源地址，有关源地址的更多配置，请参考地址。
日志服务器选择算法	依据所选的算法将日志发送到所配置的 Syslog 服务器，默认使用源地址哈希，可选择轮询调动、广播。
日志服务器 IP 端口	Syslog 日志服务器的 IP 地址和服务端口，可配置多个服务器。

7.5.4. IPS 高阶告警

IPS 高阶告警是对 IPS 告警的一个补充，对指定的 IPS 告警在单位时间内出现次数达到阈值，可以通过日志、邮件方式进行通知用户。

在系统菜单选择“**系统>日志设定>IPS 高阶告警**”，进入 **IPS 高阶告警**配置页面。

在 IPS 高阶高阶页签下点击<**新建**>，创建新的 IPS 高阶告警。或在右侧“**操作**”列下点击 图标修改已有的 IPS 高阶告警规则。



IPS 高阶告警配置项及详细说明如下：

配置项	说明
启用	IPS 高阶告警是否启用的开关。
规则名称	配置 IPS 高阶告警规则名称，不可修改。
源地址	IPS 告警过滤的条件，对满足条件的源 IP 地址进行 IPS 告警过滤。
目的地址	IPS 告警过滤的条件，对满足条件的目的 IP 地址进行 IPS 告警过滤。
源端口	IPS 告警过滤的条件，对满足条件的源端口进行 IPS 告警过滤，范围为 0-65535，0 表示任意端口。
目的端口	IPS 告警过滤的条件，对满足条件的目的端口进行 IPS 告警过滤，范围为 0-65535，0 表示任意端口。

级别	IPS 事件日志的级别，包括：信息、通知、警示、告警。
响应方式	IPS 处理方式，包括：通过、重置、丢弃、阻断会话、阻断源地址。
事件类型	事件类型指 IPS 事件的分类，包含了命令执行、蠕虫病毒、木马后门、目录遍历、缓冲溢出等。
发生频率	IPS 高阶告警的阈值，超过阈值后就会触发 IPS 高阶告警，（1-65535）秒时间内，IPS 告警值达到（30-65535）条后，发送告警邮件和告警日志。
启用 Syslog	是否启用日志服务器的方式通知管理员，配置方式参考 日志服务器 配置。
启用邮件	是否启用邮件的方式通知管理员，配置方式参考 告警邮件配置 配置。
告警邮件	收件人邮箱地址，最多支持 8 个邮箱地址。

选择可以删除单个记录，勾选所有记录，选择可以删除所有记录，选择<**启用**>或者<**禁用**>对启用状态进行修改，选择<**清除**>可以将命中次数清零。

7.6. SNMP

SNMP 是简单网络管理协议（Simple Network Management Protocol）的简称，是标准 IP 网络管理协议。该协议使网络管理员可管理网络中设备，发现目前网络中存在的问题。

在系统菜单点击“**系统**>**SNMP**”进入 **SNMP** 配置页面，共分为 2 个页签，**SNMP** 页签下用于配置 SNMP 基本信息，**SNMP 用户**页签下用于配置 SNMPv3 版本所需要使用的用户及密码等信息。

7.6.1. SNMP 配置

在系统菜单点击“系统>SNMP>SNMP”进入 SNMP 配置页签。

SNMP 的配置项与详细说明如下：

配置项	说明
启用	开关按钮，打开后 SNMP 功能开始生效。
版本	支持 v1，v2c，v3 三个版本，默认三个版本全部开启。
位置	用户自定义字段，可用于标识当前设备所在位置。
trap 地址	接收 trap 消息的服务器端 IPv4 地址。
trap6 地址	接收 trap 消息的服务器端 IPv6 地址。
SNMP 团体	团体字，可以手动设置，默认是 public。

当启用 SNMP v3 版本后，如需采用 v3 版本获取设备信息，设备必须配置 SNMP 用户，并且 SNMP 服务器软件中所设置的用户信息与设备中用户信息必须保持一致。

7.6.2. SNMP 用户

在系统菜单点击“**系统>SNMP>SNMP 用户**”，进入 **SNMP 用户**配置页签。

SNMP 用户的配置项与详细说明如下：

配置项	说明
名称	用户名。
认证算法	默认选择 none，支持 none，MD5，SHA 三种，none 表示无认证。
认证密码	为认证算法设置的密码，输入范围是 8-38 个字符。
加密算法	默认选择 none，支持 none，DES，AES 三种，none 表示无认证算法。
加密密码	默认选择 none，支持 none，DES，AES 三种，none 表示无加密。

7.7. SD-WAN

SD-WAN 软件定义广域网，用于连接广阔地理范围的企业网络、数据中心、互联网应用及云服务。为了解决企业传统跨广域网组网专线费用高、开通周期长，Internet 体验难保障、安全功能薄弱和运维困难的问题。我们推出 SD-WAN 产品及解决方案，为企业提供分支与数据中心、分支与云之间链路按需选择、灵活快捷、安全可靠和简易运维的跨广域网互联解决方案。

在系统菜单点击“**系统>SD-WAN**”，进入 **SD-WAN** 配置页面。

SD-WAN 配置项及详细说明如下：

配置项	说明
启用	打开启用开关。
云端地址	配置云端地址。例 192.168.0.100。
云端端口	默认 9070，不可编辑。
状态上报间隔	配置状态上报间隔。范围 1-600，默认为 10。
绑定码	配置绑定码。范围 1-32 字符。
统计集信息	打开统计集信息开关。
流量统计信息	打开流量统计信息开关。

完成配置项点击<**确认**>，在 **SD-WAN** 页面的**监控**子页面的<**刷新**>按钮可查看云端 IP、代理版本、运行状态。

7.8. 系统维护

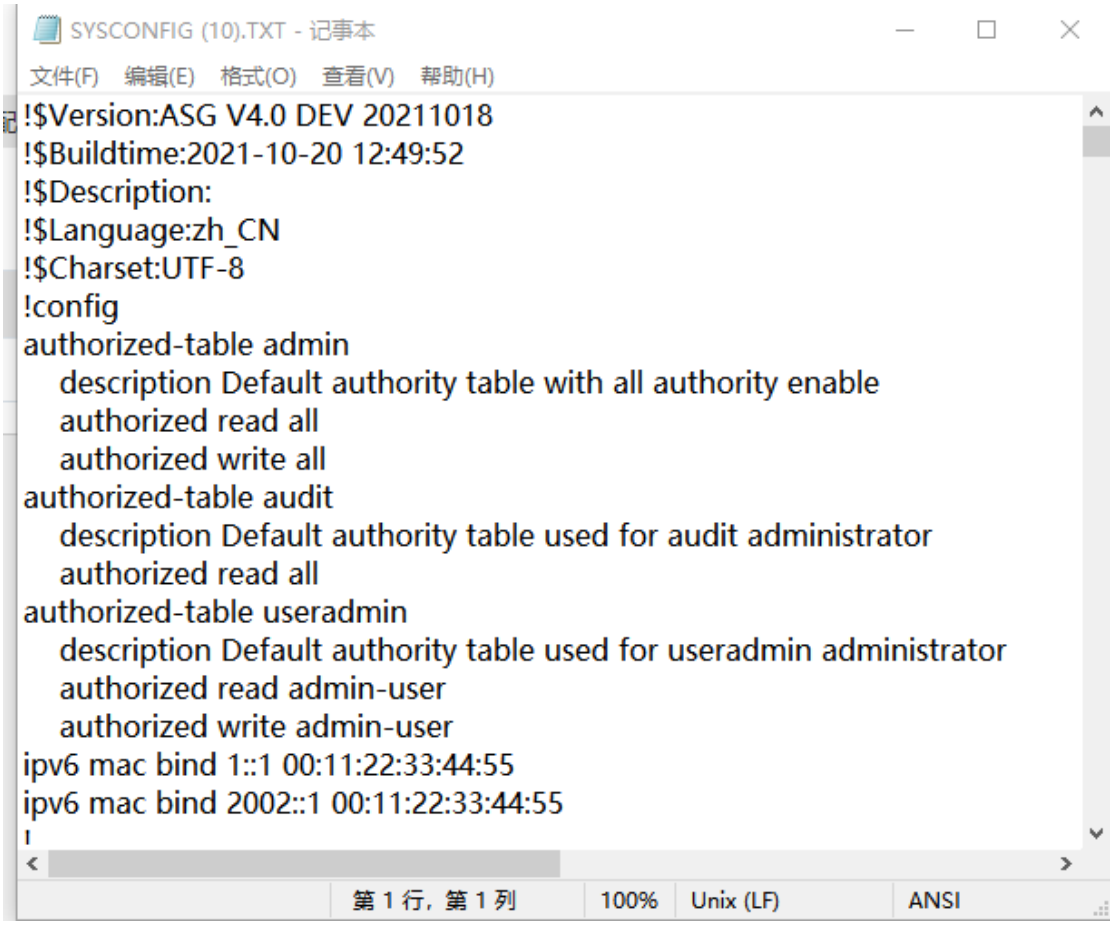
系统维护是为了防止系统在运行过程中发生错误或故障。系统维护包含了配置文件、升级与重启、授权、诊断工具、抓包工具、信息反馈、信息监控、PING 工具、Trace 工具、Token 管理功能。

7.8.1. 配置文件

支持配置文件的导入导出和配置备份功能。

在系统菜单点击“**系统**>**系统维护**>**配置文件**”，进入**配置文件**页面。

配置文件导入导出：点击<**导出**>按钮，可以对设备当前配置进行导出，导出内容为 txt 文本文件。



点击<**选取文件**>按钮，选择保存在 PC 本地的正确配置文件，点击<**导入配置**>按钮可将配置导入设备，导入后的配置文件在设备重启后生效。

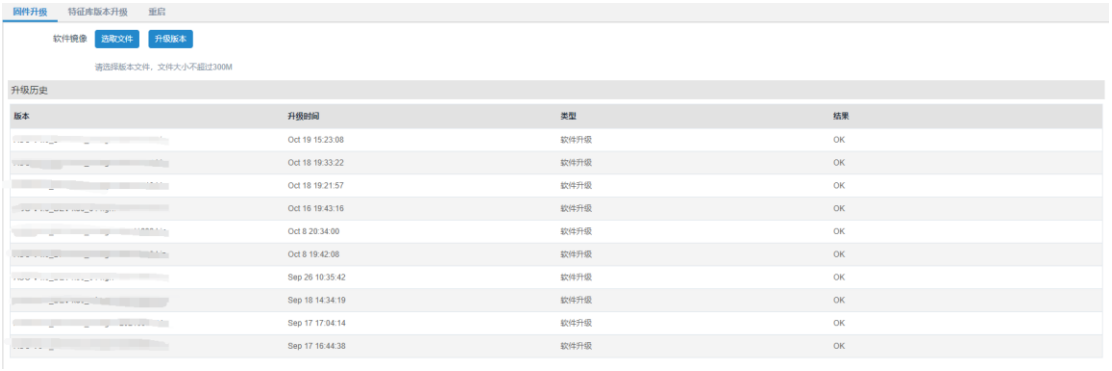
配置备份：点击<**备份**>按钮即可对当前设备中配置进行备份，点击按钮可将配置下载到本地，点击按钮可将当前配置替换为备份的配置。

7.8.2. 升级与重启

支持对设备版本进行升级，支持查看升级记录；同时支持特征库版本自动升级及手动升级，支持在页面上进行重启设备操作以及恢复出厂设置操作。

7.8.2.1. 固件升级

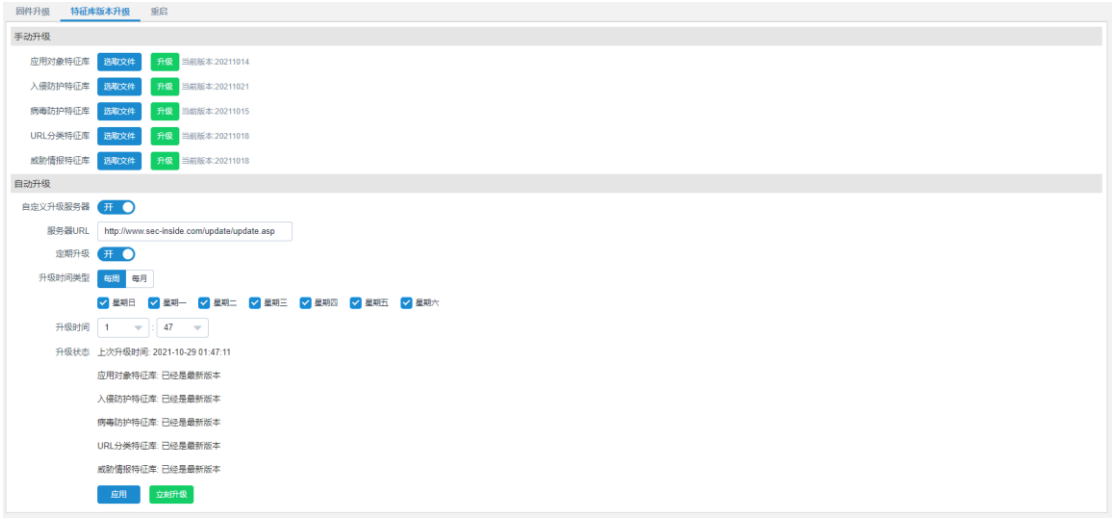
在系统菜单点击“**系统>系统维护>升级与重启>固件升级**”，进入**固件升级**配置页签。



用于升级设备版本，通过点击<**选取文件**>按钮来选择版本文件，点击<**升级版本**>进行开始版本升级操作，升级成功后需重启设备应用新版本，可在下方升级历史中查看设备升级历史记录。

7.8.2.2. 特征库版本升级

在系统菜单点击“**系统>系统维护>升级与重启>特征库版本升级**”，进入**特征库版本升级**页签。



选择需要升级的特征库，点击右侧<**选取文件**>按钮选择特征库文件，选择后点击<**升级**>按钮开始升级操作。

自动升级需指定升级服务器，默认提供升级所用服务器，可根据需要进行修改，可进行定期

升级或立刻升级。

特征库自动升级的配置项与详细说明如下：

配置项	说明
自定义升级服务器	默认关闭，关闭时使用默认服务器地址进行升级，打开后可根据需要自行修改服务器 URL。
服务器 URL	当自定义升级服务器开启时，可进行编辑，支持输入 URL。
定期升级	开启后依据配置的时间，定期进行特征库升级。
升级时间类型	可根据具体需要，选择每周或每月。
升级时间	选择一天内具体升级时间。
升级状态	展示上次升级时间及当前特征库版本是否最新。

7.8.2.3. 重启

在系统菜单点击“**系统>系统维护>升级与重启>重启**”，进入**重启**页签。

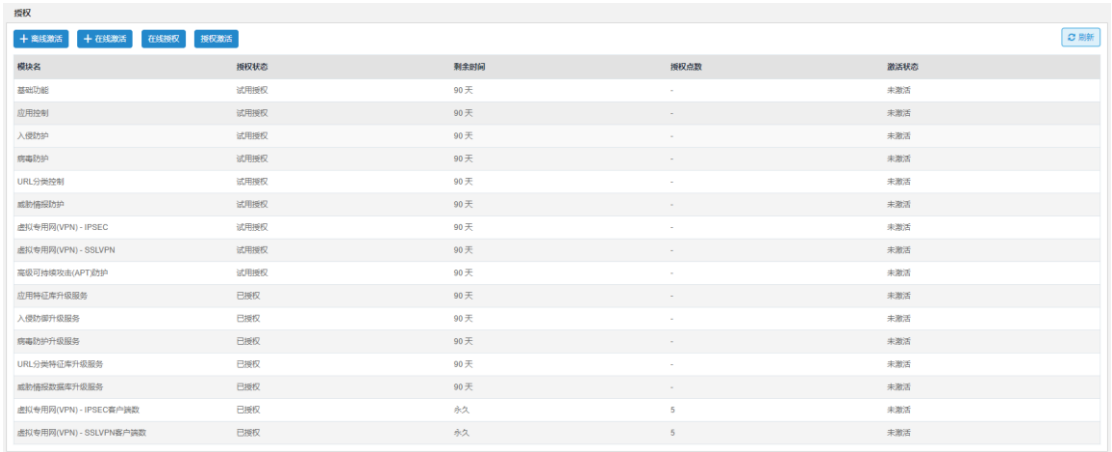
注意：

重启及恢复出厂设置为高危操作，除非必要，否则不建议执行该操作。

7.8.3. 授权

对于系统中的功能模块需经过授权激活才可正常使用。

在系统菜单点击“**系统>系统维护>授权**”，进入**授权**初始页面，支持离线激活、在线激活、在线授权、授权激活。



授权操作及详细说明如下：

操作项	说明
离线激活	设备离线状态下，点击<**离线激活**>，输入授权码，完成离线激活。授权状态为试用授权（默认 90 天）、IPSEC 客户端和 SSLVPN 客户端授权点数为 5，授权状态为未激活。
在线激活	设备在线状态下，点击**在线激活**，选择**自动**或**手动**方式进行激活。
在线授权	设备在线状态下，点击<**在线授权**>，完成在线授权。
授权激活	点击<**授权激活**>对导入的授权进行激活。授权激活后功能生效。**授权激活按**钮点击后自动消失，再次授权无需激活。

7.8.4. 诊断工具

诊断工具主要是为了方便管理员对业务流程进行追踪、调试使用。

7.8.4.1. 诊断工具

在系统菜单点击“**系统>系统维护>诊断工具>诊断工具**”，进入**诊断工具**配置页签。“协议”选项有 ANY、TCP、UDP、ICMP、OTHER，默认显示为 ANY。

诊断工具配置项及详细说明如下：

配置项	说明
协议	点击下拉框选择协议。包含 ANY、TCP、UDP、ICMP、OTHER。
地址类型	地址类型可选择 IPv4、IPv6。
源地址	输入源地址。
目的地址	输入目的地址。
源端口	当“协议”选择 TCP、UDP 时。可选源端口，范围 1-65535；可选端口范围，范围为 1-65535。
目的端口	当“协议”选择 TCP、UDP 时。可选目的端口，范围 1-65535；可选端口范围，范围为 1-65535。
Code	当“协议”选择 ICMP 时。可输入 Code，范围 0-255。
Type	当“协议”选择 ICMP 时。可输入 Type，范围 0-255。
协议号	当“协议”选择 OTHER 时。可输入协议号，范围 0-255。
调试功能	指定查看的功能模块处理结果，可选流信息、NAT。
DEBUG 结果	支持开始 debug，停止 debug，清除 debug 结果。

7.8.4.2. 诊断信息导出

完成**诊断工具**配置，并有 DEBUG 结果后，点击“**系统>系统维护>诊断工具>诊断信息导出**”，进入**诊断信息导出**页签，可以导出诊断信息。

点击<**导出**>按钮，可导出诊断信息到终端本地。

7.8.4.3. 异常信息导出

设备出现异常时，会在**异常信息导出**页面生成异常信息文件方便用户下载并交给专业人士

查看问题原因。

在系统菜单点击“**系统>系统维护>诊断工具>异常信息导出**”，进入**异常信息导出**页签。

设备出现异常时会在**异常信息导出**页面生成数据，点击图标下载文件到本地，点击图标删除数据。

7.8.5. 抓包工具

用户可以使用抓包工具通过指定过滤条件，抓取实际网络中的数据包，便于分析网络状态，追踪网络问题。

在系统菜单点击“**系统>系统维护>抓包工具**”，进入**抓包工具**配置页面。

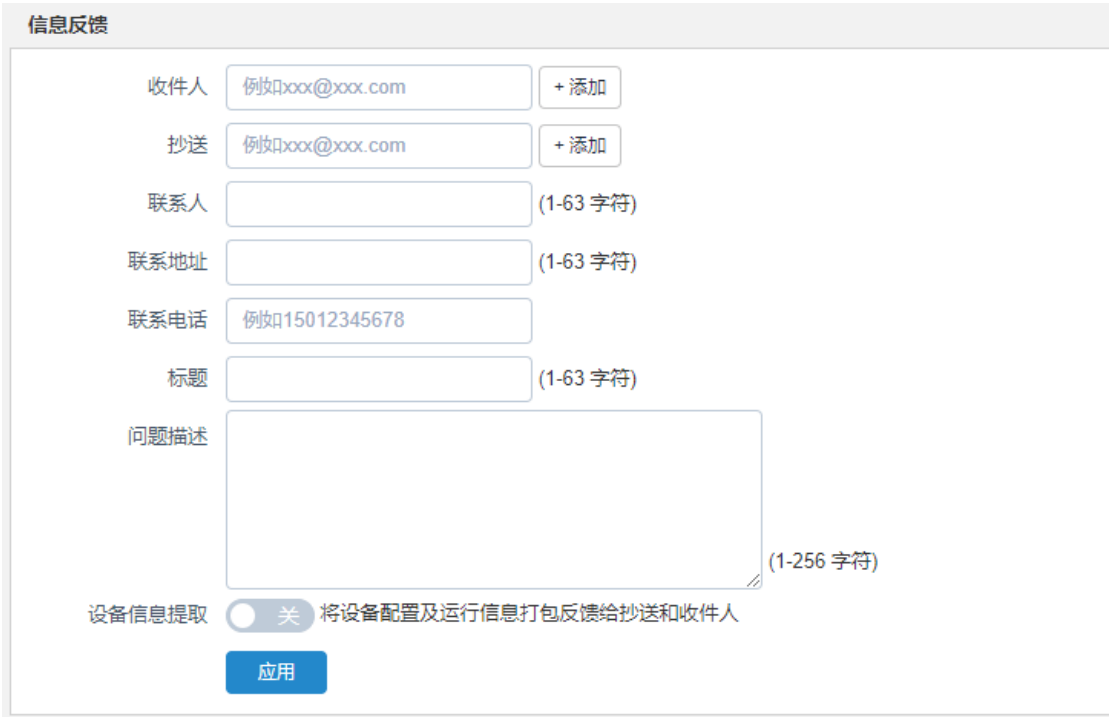
抓包工具配置项及详细说明如下：

配置项	说明
接口	所有接口类型。包括物理口、vlan 口、聚合口、tunl 口、lo 口等。
协议	通过设备的协议类型。包括 ANY、TCP、UDP、ICMP、OTHER，ANY 为所有协议，OTHER 为除 TCP、UDP、ICMP 外的其他协议。
地址类型	IP 地址类型。包括 IPv4、IPv6、所有。
抓包方式	选择抓包方式。包括发送端、接收端、所有 3 个选项。
源地址	IPv4 或 IPv6 的源 IP。地址类型选择<所有>时源地址不需要输入。
目的地址	IPv4 或 IPv6 的目的 IP。地址类型选择<所有>时目的地址不需要输入。
抓包结果	选择抓包结果开始或停止。

生成数据的右侧“操作”列，点击图标可下载数据到本地，点击图标可删除已生成的数据。

7.8.6. 信息反馈

在系统菜单中点击“**系统>系统维护>信息反馈**”，进入**信息反馈**配置页面。



信息反馈配置项及详细说明如下：

配置项	说明
收件人	收件人邮箱地址。点击<**+添加**>按钮，可增加收件人。
抄送	邮箱抄送地址。点击<**+添加**>按钮，可增加抄送人。
联系人	联系人姓名。
联系地址	联系人地址。
联系电话	联系人电话。
标题	邮件标题。
问题描述	本次反馈的问题描述。
设备信息提取	设备信息提取开关。将设备配置及运行信息打包反馈给抄送和收件人。

点击<**应用**>后，收件人可接收到信息反馈邮件。

提示：

配置信息反馈的前提：完成告警邮件配置，且告警邮箱可成功发送邮件。

7.8.7. 信息监控

信息监控主要监控 CPU 占用率、内存占用率、硬盘占用率、流量、连接数、报文大小，这些告警配置如果超过规定值会在本地日志、Syslog 日志、E-mail 报警中产生告警信息，方便用户监控设备。

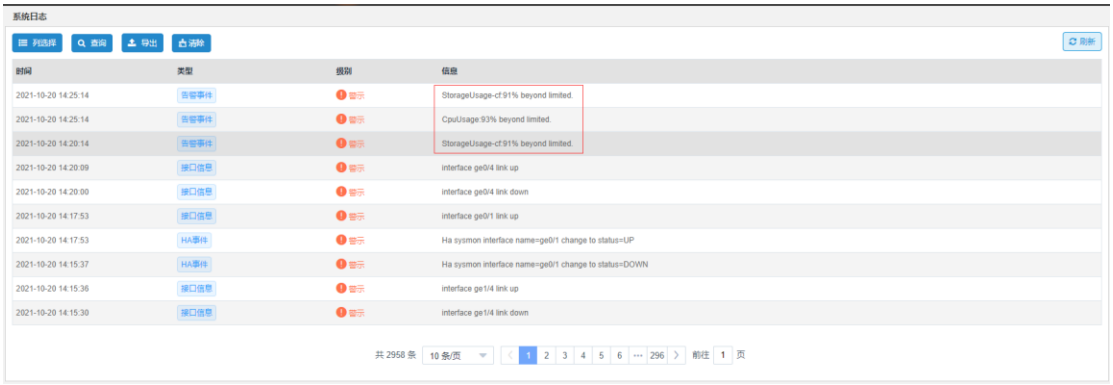
在系统菜单点击“**系统>系统维护>信息监控**”，进入**信息监控**配置页面。

信息监控配置项及详细说明如下：

配置项	说明
CPU 占用率	CPU 占用率配置范围 1-100。可勾选本地日志、Syslog 日志、E-mail 报警。
内存占用率	内存占用率配置范围 1-100。可勾选本地日志、Syslog 日志、E-mail 报警。
硬盘占用率	硬盘占用率配置范围 1-100。可勾选本地日志、Syslog 日志、E-mail 报警。
流量	流量配置范围 0-2000Mb/s。可勾选本地日志、Syslog 日志、E-mail 报警。
连接数	连接数配置范围 0-100000000。可勾选本地日志、Syslog 日志、E-mail 报警。
报文大小	报文大小配置范围 0-65535。可勾选本地日志、Syslog 日志、E-mail 报警。

点击<应用>后设备实际值超过告警配置值后触发告警，点击“**日志>系统日志**”进入**系统日**

志。页面可查看到告警事件。



提示：

在配置信息监控前，完成日志过滤配置。

7.8.8. PING 工具

在系统菜单点击“系统>系统维护>PING 工具”，进入 PING 工具配置页面。

PING 工具配置项及详细说明如下：

配置项	说明
IP 地址	IPv4 地址。
开始/停止/清除	开始 PING 操作/停止 PING 操作/清除 PING 结果。
PING 结果	返回 PING 操作结果。

7.8.9. Trace 工具

用于测试网络上某台主机 host 的跳数及延时情况。

在系统菜单点击“**系统>系统维护>Trace 工具**”，进入 **Trace 工具**配置页面。

Trace 工具配置项及详细说明如下：

配置项	说明
类型	分为 IP 地址、域名两种。
IP 地址/域名	输入 IPv4 地址/域名。
开始/清除	开始 Trace 操作/清除 Trace 结果。
Trace 结果	Trace 结果显示。

提示：

点击<开始>按钮后，请勿切换页面，切换页面 Trace 结果会丢失。

7.8.10. Token 工具

在系统菜单点击“系统>系统维护>Token 管理”，进入 Token 管理配置页面。

在 Token 管理页面，点击<新建>后弹出页面点击<确定>创建新的 Token 数据。在右侧“操作”列点击图标删除数据。